Manuel utilisateur

D-Link Corporation

Manuel utilisateur

D-Link Corporation

Publié le 09/01/2008
Copyright © 2007

Note de copyright. Cette publication, ainsi que les photographies, illustrations et logiciels qu'elle contient, est protégée par les lois internationales sur le copyright. Tous droits réservés. Le présent manuel ainsi que les informations qu'il contient ne peuvent être reproduits sans le consentement écrit de leur auteur.

Avis de non-responsabilité. Les informations contenues dans ce document peuvent être modifiées sans avis préalable. Le fabricant ne fait ni cas ni garantie dudit contenu et décline toute garantie de qualité marchande ou d'adéquation à tout usage particulier. Le fabricant se réserve le droit de faire une révision de cette publication et d'apporter des modifications ponctuelles audit contenu sans obligation de sa part d'en informer quiconque.

Limitation de responsabilité. EN AUCUN CAS D-LINK OU SES FOURNISSEURS NE SERONT TENUS POUR RESPONSABLES DES DOMMAGES DE TOUS TYPES (PAR EXEMPLE, PERTE DE BÉNÉFICES, RESTAURATION DU LOGICIEL, ARRÊT DE TRAVAIL, PERTE DE DONNÉES SAUVEGARDÉES OU TOUT AUTRE DOMMAGE COMMERCIAL OU PERTE) DÉCOULANT DE L'APPLICATION, DU MAUVAIS USAGE OU DE LA PANNE D'UN PRODUIT D-LINK, MÊME SI D-LINK EST INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES. DE PLUS, D-LINK NE POURRA ÊTRE TENU POUR RESPONSABLE DES RÉCLAMATIONS FAITES CONTRE LES CLIENTS PAR DES TIERS POUR TOUTE PERTE OU ENDOMMAGEMENT. D-LINK NE SERA EN AUCUN CAS TENU POUR RESPONSABLE DES DOMMAGES DÉPASSANT LE MONTANT VERSÉ PAR L'UTILISATEUR FINAL À D-LINK POUR LE PRODUIT.

Table des matières

Liste des figures

Liste des exemples

Préface

Public visé

Le présent guide de référence s'adresse aux administrateurs responsables de la configuration et de la gestion des Firewalls D-Link qui fonctionnent sous le système d'exploitation NetDefendOS. Ce guide suppose que le lecteur possède certaines connaissances de base sur les réseaux et leur système de sécurité.

Structure du texte et normes

Ce texte est subdivisé en chapitres et sous-sections. Les sous-chapitres numérotés sont consultables dans la table des matières au début du document. Un index est inclus à la fin du document, répertoriant les catégories par ordre alphabétique.

En cliquant sur un lien « Voir chapitre/section » (tel que : voir) contenu dans le corps du texte, vous pouvez directement accéder à la partie en question.

Le texte pouvant apparaître dans l'interface utilisateur du produit est désigné en gras. Lorsqu'un terme est mis en valeur ou introduit pour la première fois, *il peut apparaître en italique.*

Une console d'interaction dans le corps du texte et en dehors d'un exemple apparaîtra dans un encadré au fond gris.

En cliquant sur une adresse Internet dans le texte, vous pouvez ouvrir l'URL spécifiée dans une nouvelle fenêtre du navigateur (certains systèmes ne le permettent pas). Exemple : http://www.dlink.com.

Exemples

Les exemples dans le texte sont indiqués par l'en-tête « Exemple » et apparaissent sur fond gris, comme indiqué ci-dessous. Ils contiennent un exemple de l'interface de ligne de commande et/ou un exemple d'interface Web selon le cas. (Le « CLI Reference Guide » (Guide de référence sur l'interface de ligne de commande) associé fournit des informations sur toutes les commandes de l'interface).

Exemple 1. Exemple de notation

Les informations sur ce que veut illustrer l'exemple sont consultables ici, accompagnées parfois d'une image d'explication.

Interface de ligne de commande
L'exemple d'interface de ligne de commande apparaît ici. L'invite de commande apparaît en premier, suivie de la commande :

```
gw-world:/> somecommand someparameter=somevalue
```

Interface Web

Les exemples d'actions sur l'interface Web sont présentés ici. De manière générale, une liste numérotée montrant les éléments de l'arborescence sur la gauche de l'interface, dans la barre de menu ou dans un menu flottant doit être ouverte, suivie des informations sur les données qui doivent être saisies :

- Sélectionnez Élément X > Élément Y > Élément Z
- Entrez :

DonnéeÉlément1 : donnéevaleur1

DonnéeÉlément2 : valeurdonnée2

Contenu important

Les sections spéciales du texte auxquelles le lecteur doit prêter une attention particulière sont indiquées par des icônes à gauche de la page, suivies d'un petit paragraphe en italique. Voici les différents types de sections disponibles avec l'objectif correspondant :

Remarque
Elle indique une information complémentaire en relation avec le texte qui précède. Elle peut concerner un sujet qui est mis en relief ou qui n'est pas évident ou énoncé explicitement dans le texte précédent.

Conseil
Il indique une information non cruciale, qu'il est utile de connaître dans certains cas mais qu'il n'est pas nécessaire de lire.

Attention
Elle indique les passages où le lecteur doit faire attention à ses actions, un manque de précaution pouvant engendrer une situation indésirable.

Important
Cette section marque un point essentiel que le lecteur doit lire et comprendre.

Avertissement
La lecture de ce passage est essentielle, car l'utilisateur doit être conscient que des problèmes graves peuvent survenir si certaines actions sont ou ne sont pas accomplies.

Chapitre 1. Présentation du produit

Le présent chapitre décrit les principales fonctionnalités de NetDefendOS.

À propos de D-Link NetDefendOS

D-Link NetDefendOS est le firmware, le moteur logiciel qui gère et contrôle tous les produits Firewall D-Link.

Conçu comme un système d'exploitation de sécurité réseau, NetDefendOS se distingue par un haut débit et une grande fiabilité en plus d'un contrôle très précis. Contrairement aux produits reposant sur des systèmes d'exploitation standard (Unix ou Microsoft Windows), NetDefendOS s'intègre en transparence à tous les sous-systèmes, permet de surveiller de manière approfondie toutes les fonctionnalités tout en réduisant la zone d'attaque potentielle, ce qui lui permet d'être moins exposé aux menaces de sécurité.

Du point de vue de l'administrateur, NetDefendOS repose sur une approche conceptuelle visant à visualiser les opérations au moyen d'ensemble de blocs logiques (ou *objets*) qui permettent de configurer le produit de mille-et-une manières. Ce contrôle très précis permet à l'administrateur de répondre aux besoins des cas de figure les plus exigeants en matière de sécurité réseau.

NetDefendOS est un système d'exploitation de réseau puissant doté de nombreuses fonctionnalités. La liste ci-dessous présente les principales fonctionnalités :

Routage IP
: NetDefendOS propose de nombreuses options pour le routage IP, notamment le routage statique, le routage dynamique, ainsi que des fonctions de routage multidiffusion. En outre, NetDefendOS propose des fonctionnalités telles que les LAN virtuels, la surveillance du routage, le proxy-ARP et la transparence. Pour plus d'informations, reportez-vous au *Chapitre 4, Routage*.

Traduction d'adresses
: Pour des raisons de fonctionnalité et de sécurité, NetDefendOS propose une fonction de traduction d'adresses reposant sur des règles. La traduction d'adresses dynamiques (NAT) ainsi que la traduction d'adresses statiques (SAT) est prise en charge et satisfait la plupart des types de besoins en matière de traduction d'adresses. Nous aborderons cette fonctionnalité dans le *Chapitre 7, Traduction d'adresses*.

Firewalls
: Le cœur du produit NetDefendOS propose des firewalls basés sur le filtrage dynamique pour les protocoles courants tels que TCP, UDP et ICMP. En tant qu'administrateur, vous pouvez définir des stratégies détaillées en matière de firewalls, reposant sur les réseaux et interfaces source et de destination, le protocole, les ports, les authentifiants de l'utilisateur, la période de la journée et bien d'autres éléments. La section intitulée « Ensemble de règles IP » décrit comment utiliser les aspects liés aux firewalls de NetDefendOS.

Prévention et détection des intrusions
: Pour atténuer les attaques de la couche d'application qui exploitent des vulnérabilités dans les services et les applications, NetDefendOS propose un puissant moteur de prévention et de détection des intrusions (Intrusion Detection and Prevention). Le moteur IDP repose sur des règles. Il peut exécuter une analyse et une détection très performante des attaques et bloquer ou mettre sur liste noire les hôtes responsables des attaques, si nécessaire. Pour plus de renseignements sur les capacités IDP de NetDefendOS, reportez-vous à la section intitulée « Prévention et détection des intrusions ».

Antivirus
: NetDefendOS intègre une fonctionnalité de passerelle anti-virus. Le trafic qui transite par la passerelle peut être soumis à une analyse antivirus en profondeur et les hôtes responsables des attaques peuvent être, au choix,

bloqués ou mis sur liste noire. La section intitulée « Analyse antivirus » fournit des informations complémentaires sur l'utilisation de la fonctionnalité antivirus intégrée.

Filtrage de contenu Web — NetDefendOS propose divers mécanismes pour le filtrage du contenu Web considéré comme inapproprié d'après vos règles d'utilisation du Web. Le contenu Web peut être bloqué selon la catégorie, les objets malveillants enlevés et les sites Web mis sur liste blanche ou noire, selon de multiples règles. Pour plus d'informations, reportez-vous à la section intitulée « Filtrage de contenu Web ».

Réseau privé virtuel (Virtual Private Network) — Un périphérique qui exécute NetDefendOS est particulièrement approprié pour participer à un réseau privé virtuel. NetDefendOS prend en charge simultanément le VPN IPsec, L2TP et PPTP ; il peut tenir le rôle de serveur ou de client pour tous les types de VPN et peut fournir des règles de sécurité individuelles pour chaque tunnel VPN. Le réseau privé virtuel est traité en détail dans le *chapitre 9, VPN*.

Gestion du trafic — NetDefendOS prend en charge la mise en forme du trafic, les règles aux seuils et les fonctionnalités d'équilibrage du volume de trafic du serveur, ce qui en fait l'outil idéal pour la gestion du trafic. La fonctionnalité de mise en forme du trafic permet une limitation et un équilibrage très précis de la bande passante ; les règles aux seuils permettent de mettre en œuvre différents types de seuils pour avertir ou limiter le trafic du réseau là où c'est nécessaire et l'équilibrage du volume de trafic du serveur permet au périphérique qui exécute NetDefendOS de distribuer les charges de réseau sur plusieurs hôtes. Le *chapitre 10, Gestion du trafic*, fournit des informations plus détaillées sur les différentes capacités de gestion du trafic.

Opérations et maintenance — Pour faciliter la gestion d'un périphérique NetDefendOS, le contrôle administrateur est activé à l'aide d'une interface utilisateur de type Web ou par l'interface de ligne de commande. De plus, NetDefendOS fournit des fonctions très détaillées de consignation et de suivi d'événements ainsi que la prise en charge de la surveillance à l'aide de standards tels que SNMP. Pour plus d'informations, reportez-vous au *chapitre 2, Gestion et Maintenance*.

ZoneDefense — Vous pouvez utiliser NetDefendOS pour contrôler les switches D-Link à l'aide de la fonctionnalité ZoneDefense.

La lecture minutieuse de cette documentation vous permettra de tirer le meilleur parti de votre produit NetDefendOS. En plus de ce document, le lecteur devrait également consulter les volumes additionnels suivants :

NetDefendOS CLI Guide (guide NetDefendOS CLI) qui détaille toutes les commandes console NetDefendOS.

NetDefendOS Log Reference Guide (guide de référence des consignations de NetDefendOS) qui détaille tous les messages du journal d'événements de NetDefendOS.

L'ensemble de ces documents forme la documentation indispensable pour le fonctionnement de NetDefendOS.

Remarque

La haute disponibilité, l'antivirus, le filtrage de contenu Web et ZoneDefense ne sont pas disponibles avec certains modèles, comme cela est précisé dans les chapitres qui se rapportent à ces fonctionnalités.

L'architecture NetDefendOS

Une architecture basée sur l'état

L'architecture NetDefendOS est centrée autour du concept de connexions basées sur l'état. Les routeurs IP ou les switches traditionnels inspectent généralement tous les paquets et effectuent ensuite des décisions relatives au

transfert des données selon les informations trouvées dans les en-têtes des paquets. Avec cette approche, les paquets sont transmis sans se préoccuper du contexte, ce qui évite toute possibilité de détecter et d'analyser des protocoles complexes et renforce les règles de sécurité correspondantes.
Inspection dynamique. NetDefendOS emploie une technique appelée *inspection dynamique*, ce qui signifie qu'il inspecte et transmet le trafic en se basant sur une seule connexion à la fois. NetDefendOS détecte lorsqu'une nouvelle connexion est établie et conserve une faible quantité d'informations ou d'*états* dans sa *table d'état* pendant la durée de cette connexion. Grâce à cette opération, NetDefendOS est capable de comprendre le contexte du trafic réseau, ce qui lui permet notamment d'effectuer une analyse du trafic en profondeur et d'appliquer la gestion de la bande passante.

L'approche d'inspection dynamique propose en outre des performances de débit élevées en plus de l'atout d'une conception hautement évolutive. Le sous-système NetDefendOS qui met en œuvre l'inspection dynamique sera parfois appelé *moteur d'état* NetDefendOS dans la documentation.

Blocs logiques de NetDefendOS

Les blocs logiques de base de NetDefendOS sont les interfaces, les objets logiques ainsi que les différents types de règles (ou ensembles de règles).

Interfaces. Les *interfaces* sont les passages pour le trafic réseau en direction ou en provenance du système. Sans interfaces, un système NetDefendOS n'a aucun moyen de recevoir ou d'envoyer du trafic. Différents types d'interfaces sont pris en charge : les interfaces physiques, les sous-interfaces physiques et les interfaces tunnels. *Les interfaces physiques* correspondent aux ports Ethernet physiques réels ; les *sous-interfaces physiques* incluent les interfaces VLAN et PPPoE, tandis que les *interfaces tunnels* sont utilisées pour recevoir et envoyer le trafic dans les tunnels VPN.

Symétrie d'interface. La conception de l'interface NetDefendOS est symétrique, ce qui signifie que les interfaces du périphérique ne sont pas fixées sur « l'extérieur non sécurisé » ou « l'intérieur sécurisé » d'une topologie réseau. La notion de contenu interne et externe doit être entièrement définie par l'administrateur.

Objets logiques. *Les objets logiques* peuvent être considérés comme des blocs logiques prédéfinis destinés à être utilisés par les ensembles de règles. Le carnet d'adresses, par exemple, contient des objets nommés qui représentent les adresses réseau et hôtes. Les services, qui représentent un protocole spécifique et des combinaisons de ports, constituent d'autres exemples d'objets logiques. Les objets de la passerelle ALG (Application Layer Gateway), utilisés pour définir des paramètres supplémentaires qui concernent des protocoles spécifiques tels que HTTP, FTP, SMTP et H.323, sont également importants.

Ensembles de règles NetDefendOS. Enfin, les règles définies par l'administrateur dans les différents *ensembles de règles* sont utilisées pour réellement mettre en œuvre les règles de sécurité de NetDefendOS. L'ensemble de règles le plus indispensable est l'ensemble de *règles IP*, utilisé aussi bien pour définir la règle de filtrage de la couche 3 (IP) que pour réaliser la traduction d'adresses et l'équilibrage du volume de trafic du serveur. Les règles de mise en forme du trafic définissent la stratégie de gestion de la bande passante, les règles IDP contrôlent le comportement du moteur de prévention des intrusions, etc.

Flux de paquets de base

Cette section décrit le flux de base dans le moteur d'état pour les paquets reçus et transmis par NetDefendOS. Veuillez noter que cette description est simplifiée et ne pourrait s'appliquer entièrement à tous les cas de figure. Le principe de base est toutefois valable pour toutes les applications.

Une trame Ethernet est reçue par l'une des interfaces Ethernet du système. La procédure de validation de la trame Ethernet de base est effectuée et le paquet est ignoré si la trame n'est pas valide.

Le paquet est associé à une interface source. L'interface source est définie comme suit :

Si la trame Ethernet contient un ID de VLAN (identifiant de réseau virtuel), le système vérifie l'existence d'une interface VLAN configurée possédant un ID de VLAN correspondant. S'il en détecte une, celle-ci devient l'interface source pour le paquet. Si aucune interface correspondante n'est trouvée, le paquet est ignoré et l'événement est consigné.

Si la trame Ethernet contient une charge utile PPP, le système vérifie l'existence d'une interface PPPoE

correspondante. S'il en trouve une, celle-ci devient l'interface source pour le paquet. Si aucune interface correspondante n’est trouvée, le paquet est ignoré et l’événement est consigné.

Dans tous les autres cas, l’interface Ethernet réceptrice devient l’interface source pour le paquet.

Le datagramme IP inclus dans le paquet est transmis au vérificateur de cohérence NetDefendOS. Le vérificateur de cohérence effectue un certain nombre de tests pour vérifier que le paquet est sain, parmi lesquels la validation des totaux de contrôle, les indicateurs de protocoles, la longueur du paquet, etc. Si le test de cohérence échoue, le paquet est ignoré et l’événement est consigné.

NetDefendOS tente à présent de répertorier une connexion existante en associant les paramètres du paquet entrant. Un certain nombre de paramètres sont utilisés lors de la tentative de correspondance, notamment l’interface source, les adresses IP source et de destination ainsi que le protocole IP.

Si aucune correspondance n’est trouvée, le système exécute un processus d’établissement de connexion comprenant les étapes suivantes, jusqu’à l’étape 9. Si une correspondance est détectée, le processus de transmission continue à l’étape 10 ci-dessous.

Les règles d’accès sont examinées pour déterminer si l'adresse IP source de la nouvelle connexion est autorisée sur l’interface reçue. Si aucune règle d’accès ne correspond, une résolution de routage inverse est effectuée. En d’autres termes, une interface n’acceptera par défaut que les adresses IP sources appartenant aux réseaux routés par cette interface. Si les règles d’accès ou la résolution de routage inverse déterminent que l’IP source n'est pas valide, le paquet est ignoré et l’événement est consigné.

Un chemin de routage est établi en utilisant la table de routage appropriée. L’interface de destination pour la connexion est à présent déterminée.

Les règles IP sont désormais inspectées dans le but de trouver une règle qui corresponde au paquet. Les paramètres suivants font partie du processus de mise en correspondance :

Interfaces source et de destination

Réseau source et de destination

Protocole IP (par exemple TCP, UDP, ICMP)

Ports TCP/UDP

Types ICMP

Point dans le temps faisant référence à une planification prédéfinie.

Si aucune correspondance ne peut être trouvée, le paquet est ignoré.

Si une règle correspondant à la nouvelle connexion est trouvée, le paramètre « Action » de la règle détermine la manière dont NetDefendOS exploitera cette connexion. Si l’action est « Drop » (Ignorer), le paquet est ignoré et l'événement est consigné en fonction des paramètres de consignation de la règle.

Si l’action est « Allow » (Autoriser), le paquet est autorisé à transiter sur le système. Un état correspondant est ajouté à la table de connexion pour mettre en correspondance les prochains paquets appartenant à la même connexion. De plus, il se peut que l’objet de service qui correspondait au protocole et aux ports IP ait déjà contenu une référence à un objet de la passerelle ALG (Application Layer Gateway). Cette information est consignée dans l’état de manière à ce que NetDefendOS sache que le traitement des couches d’application devra être effectué sur la connexion.

Enfin, l’ouverture de la nouvelle connexion est consignée en fonction des paramètres de consignation de la règle.

Remarque

Il existe en réalité un certain nombre d’actions supplémentaires disponibles, telles que la traduction d’adresses et l’équilibrage de charge du serveur. Le concept de base qui consiste à interrompre et à autoriser le trafic ne change pas.

Les règles de détection et de prévention des intrusions (IDP) sont à présent évaluées d'une manière comparable aux règles IP. Si une correspondance est trouvée, les données IDP sont consignées dans l'état. Grâce à cette opération, NetDefendOS sait que l'analyse IDP est supposée être effectuée sur tous les paquets appartenant à cette connexion.

La règle de mise en forme du trafic et l'ensemble de règles aux seuils sont à présent inspectés. Si une correspondance est trouvée, cette information est consignée dans l'état. Cela permettra une gestion correcte du trafic de la connexion.

Grâce aux informations stockées dans l'état, NetDefendOS sait à présent la manière dont il doit traiter le paquet entrant :

Si l'information ALG existe ou si l'analyse IDP est sur le point d'être effectuée, la charge utile du paquet est prise en charge par le sous-système de pseudo-rassemblement TCP, qui à son tour utilise les différentes passerelles ALG, les moteurs d'analyse de la couche 7 et ainsi de suite, pour analyser ou transformer le trafic en profondeur.

Si le contenu du paquet est encapsulé (comme c'est le cas avec IPsec, L2TP/PPTP ou un autre type de protocole de tunnelisation), alors les listes d'interfaces sont analysées pour rechercher une interface correspondante. Si une interface correspondante est détectée, le paquet est décapsulé et la charge utile (le texte brut) est renvoyée à NetDefendOS, l'interface source étant alors l'interface tunnel correspondante. En d'autres termes, le processus se poursuit à l'étape 3 ci-dessus.

Si les informations sur la gestion du trafic existent, le paquet peut être mis en file d'attente ou être soumis à des actions liées à la gestion du trafic.

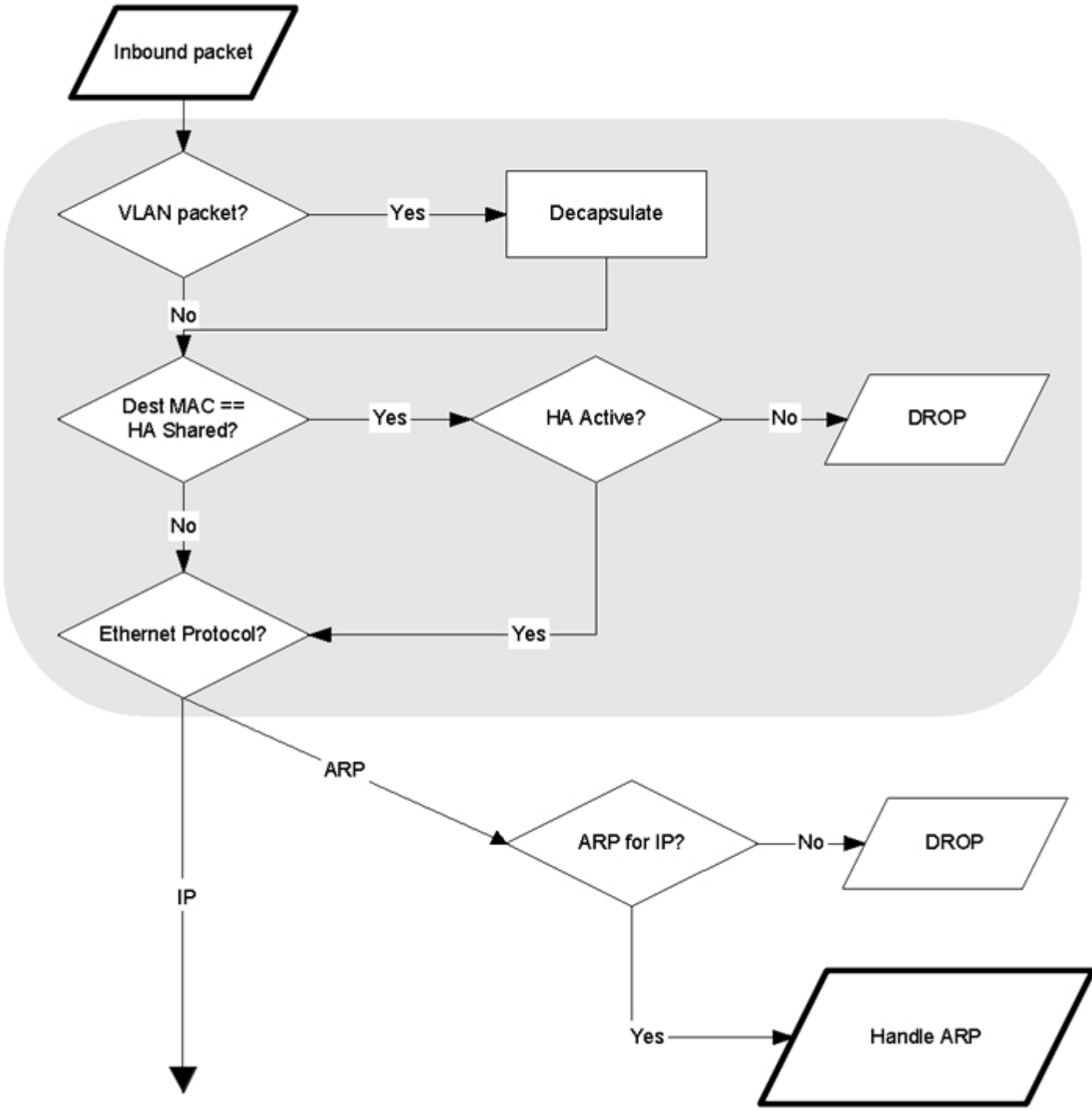
Finalement, le paquet sera transmis à l'interface de destination en fonction de l'état. Si l'interface de destination est une interface tunnel ou une sous-interface physique, des traitements supplémentaires tels que le chiffrement ou l'encapsulation peuvent avoir lieu.

La section suivante fournit un ensemble de schémas qui illustrent le flux de paquets qui traversent NetDefendOS.

Flux de paquets du moteur d'état de NetDefendOS

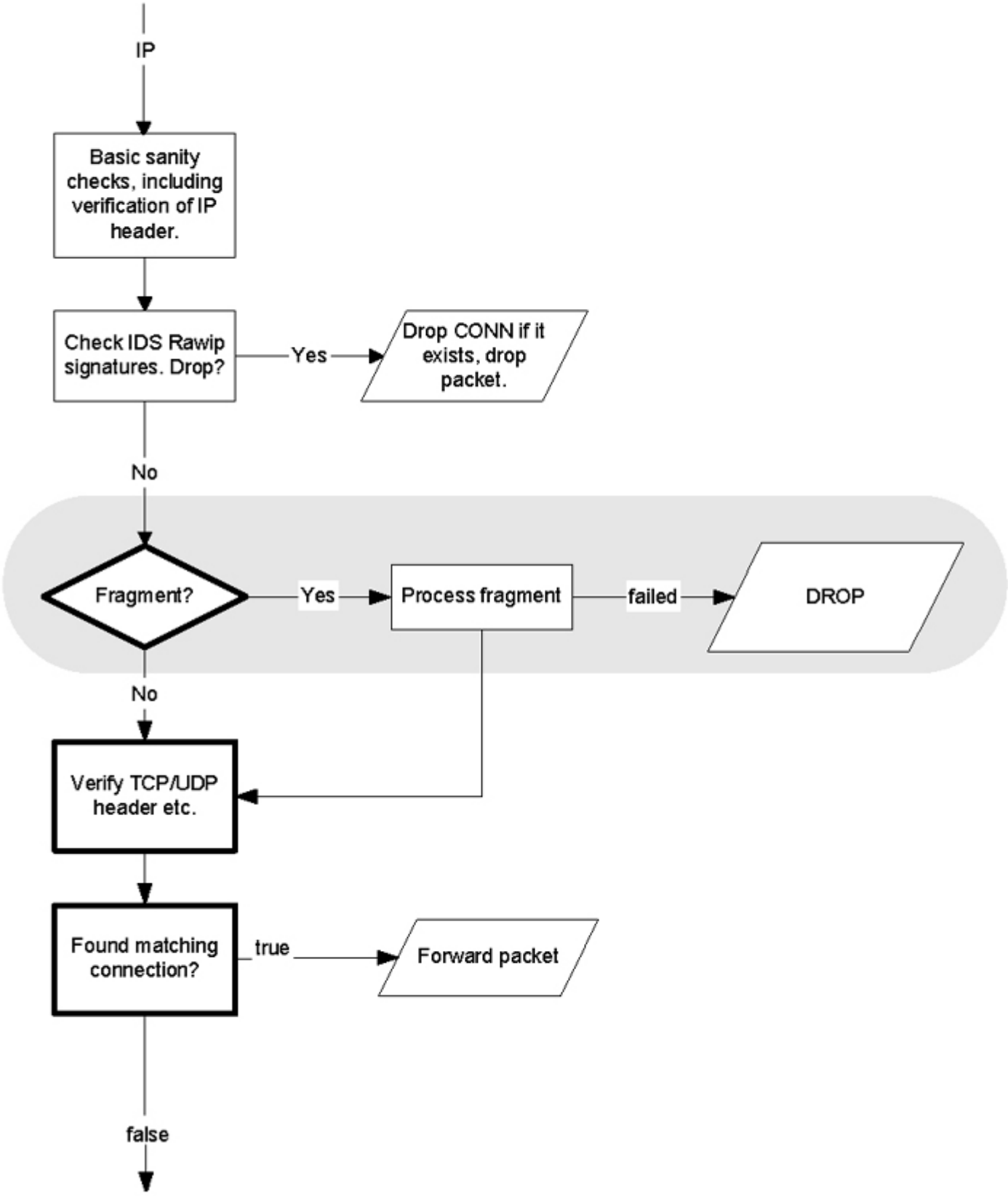
Les schémas de cette section offrent un résumé du flux de paquets qui traverse le moteur d'état de NetDefendOS. Les trois schémas suivants doivent être lus de manière consécutive.

Figure 1.1 Schéma du flux de paquets Partie I



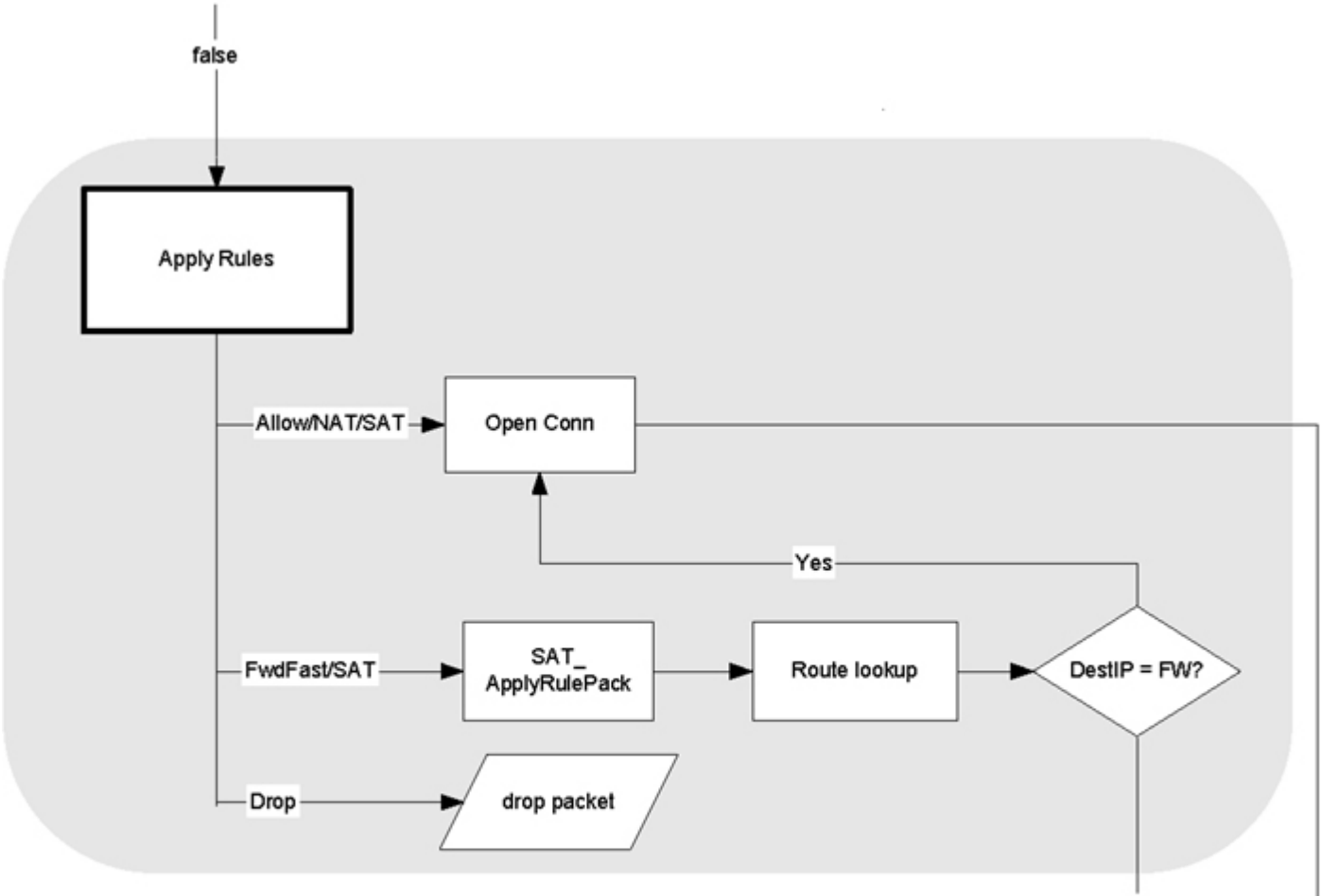
Le flux de paquets se poursuit sur la page suivante.

Figure 1.2 Schéma du flux de paquets Partie II


IP
Basic sanity checks, including verification of IP header.
Check IDS Rawip signatures. Drop?
Yes
Drop CONN if it exists, drop packet.
No
Fragment?
Yes
Process fragment
failed
DROP
No
Verify TCP/UDP header etc.
Found matching connection?
true
Forward packet
false

Le flux de paquets se poursuit sur la page suivante.

Figure 1.3 Schéma du flux de paquets Partie III



Chapitre 2. Gestion et maintenance

Ce chapitre décrit les aspects relatifs à la gestion, à la maintenance et aux opérations sur NetDefendOS.

Gestion de NetDefendOS

Présentation

NetDefendOS est conçu pour apporter un haut niveau de performances et une grande fiabilité. Non seulement il fournit un vaste ensemble de fonctions, mais aussi il permet à l'administrateur de pleinement contrôler tous les détails du système. En d'autres termes, le produit peut être déployé dans les environnements les plus difficiles.

Une bonne compréhension de la manière de configurer NetDefendOS est cruciale pour la bonne utilisation du système. Pour cette raison, cette section présente de façon détaillée le sous-système de configuration et décrit la manière de travailler avec les multiples interfaces de gestion.
Interfaces de gestion. NetDefendOS comprend les interfaces de gestion suivantes :

L'interface utilisateur Web L'*interface utilisateur Web* propose une interface de gestion graphique conviviale et intuitive, accessible depuis un navigateur Web standard.

L'interface de ligne de commande L'*interface de ligne de commande*, accessible en local via un port console série ou à distance via le protocole SSH (Secure Shell), propose le contrôle le plus pointu de tous les paramètres de NetDefendOS.

> **Remarque**
> Microsoft Internet Explorer (version 6 ou supérieure), Firefox et Netscape (version 8 ou supérieure) sont les navigateurs Web recommandés pour l'utilisation de l'interface utilisateur Web. D'autres navigateurs peuvent aussi convenir.

L'accès aux interfaces de gestion distante peut être contrôlé grâce à la stratégie de gestion distante. Ainsi, l'administrateur peut restreindre l'accès au réseau source, à l'interface source et aux authentifiants. Il est possible d'autoriser l'accès à l'interface Web par des administrateurs de certains réseaux et l'accès distant à l'interface de ligne de commande par un administrateur connecté à l'aide d'un tunnel IPSec spécifique.

Par défaut, l'accès à l'interface utilisateur Web est autorisé aux utilisateurs réseau connectés via l'interface LAN du firewall (pour les produits dotés de plusieurs interfaces LAN, LAN1 est l'interface par défaut).

Comptes administrateur par défaut

Par défaut, NetDefendOS a une base de données utilisateur locale : *AdminUsers*, avec un compte utilisateur prédéfini.

Nom d'utilisateur : *admin*. Mot de passe : *admin*.
Ce compte a tous les droits administrateur de lecture/d'écriture.

> **Important**
> Pour des raisons de sécurité, il est recommandé de modifier le mot de passe du compte par défaut aussitôt que possible après connexion au firewall de D-Link.

Création de comptes. Des comptes utilisateur supplémentaires peuvent être créés le cas échéant. Les comptes peuvent appartenir soit au groupe des administrateurs (dans ce cas, ils ont tous les droits administrateur de lecture/d'écriture), soit au groupe des auditeurs (dans ce cas, ils n'ont que les droits de lecture).

Interface de ligne de commande

NetDefendOS contient une *interface de ligne de commande* pour les administrateurs qui préfèrent ou exigent une approche par ligne de commande, ou qui ont besoin d'un contrôle plus précis de la configuration du système.

L'interface de ligne de commande est disponible en local grâce au port console série ou à distance grâce au protocole SSH (Secure Shell).

L'interface de ligne de commande dispose d'un vaste ensemble de commandes qui permettent non seulement l'affichage et la modification des données de configuration, mais aussi l'affichage des données d'exécution et la réalisation des tâches de maintenance du système.

Cette section ne fait qu'un résumé de l'utilisation de l'interface de ligne de commande. Pour plus de précisions sur les lignes de commande, reportez-vous au *CLI Reference Guide* (Guide de référence sur l'interface de ligne de commande), fourni par D-Link.

Console série pour l'accès à l'interface de ligne de commande. Le port console série est un port RS-232 sur le firewall de D-Link, qui permet l'accès à l'interface de ligne de commande grâce à une connexion série sur un PC ou un terminal. Pour localiser le port console série du système D-Link, reportez-vous au Guide de démarrage rapide de D-Link.

Pour utiliser le port console, vous avez besoin des éléments suivants :

Un terminal ou un ordinateur avec un port série et la capacité d'émuler un terminal (par exemple, le logiciel *Hyper Terminal* inclus dans certaines éditions de Microsoft Windows). Le port console série utilise les paramètres par défaut suivants : *9600 bits par seconde, sans parité, 8 bits de données, 1 bit d'arrêt.*

Un câble RS-232 avec les connecteurs appropriés. Un câble RS-232 simulateur de modem est inclus dans le pack.

Pour connecter un terminal au port console, suivez ces étapes :

Paramétrez le protocole du terminal selon la procédure précédemment décrite.

Branchez l'un des connecteurs du câble RS-232 directement sur le port console du matériel.

Branchez l'autre extrémité du câble au terminal ou au port série d'un ordinateur qui exécute le logiciel de communication.

Appuyez sur la touche *Entrée* du terminal. L'invite de connexion de NetDefendOS devrait apparaître sur l'écran du terminal.

Accès SSH à l'interface de ligne de commande. Le protocole SSH (Secure Shell) peut être utilisé pour accéder à l'interface de ligne de commande par le biais du réseau d'un hôte distant. Le SSH est un protocole utilisé à l'origine pour des communications sécurisées sur des réseaux non sécurisés, ce qui implique une forte authentification et l'intégrité des données. Une grande partie des clients SSH sont disponibles gratuitement pour presque toutes les plates-formes matérielles.

NetDefendOS est compatible avec la version 1, 1.5 et 2 du protocole SSH. L'accès SSH est contrôlé par la stratégie de gestion distante de NetDefendOS et désactivé par défaut.

Exemple 2.1. Autorisation de l'accès SSH distant

Cet exemple montre comment vous pouvez autoriser l'accès SSH distant depuis le réseau *lannet* grâce à une interface *lan*, en ajoutant une règle à la stratégie de gestion distante.

Interface de ligne de commande

```
gw-world:/> add RemoteManagement RemoteMgmtSSH ssh Network=lannet Interface=lan
   LocalUserDatabase=AdminUsers
```

Interface Web

Sélectionnez System > Remote Management > Add > Secure Shell Management (Système > Gestion distante > Ajouter > Gestion SSH).

Saisissez le nom de la stratégie de gestion SSH distante (par exemple, *ssh_policy*).

Dans les listes déroulantes, sélectionnez les options suivantes :

User Database (Base de données utilisateur) : AdminUsers (Administrateurs)

Interface : lan

Network (Réseau) : lannet

Cliquez sur OK.

Connexion à l'interface de ligne de commande. Quand l'accès à l'interface de ligne de commande a été établi pour NetDefendOS grâce à une console série ou un client SSH, l'administrateur devra s'identifier sur le système avant de pouvoir exécuter n'importe quelle ligne de commande. Cette étape d'authentification est nécessaire pour assurer que seuls les utilisateurs autorisés peuvent accéder au système et pour fournir des informations utilisateur lors de vérifications.

En accédant à l'interface de ligne de commande, le système répond par une invite de connexion. Saisissez votre nom d'utilisateur et appuyez sur la touche *Entrée*, puis insérez votre mot de passe et appuyez de nouveau sur la touche *Entrée*. Une fois l'authentification réussie, une invite de commande apparaît. Si un message d'accueil a été paramétré, il s'affichera directement après l'authentification.

```
gw-world:/>
```

Pour des raisons de sécurité, il est conseillé de désactiver ou de ne pas personnaliser le message d'accueil de l'interface de ligne de commande.
Modification de l'invite de l'interface de ligne de commande. L'invite de l'interface de ligne de commande par défaut est :

```
Device:/>
```

Device est la référence du firewall de D-Link. Elle peut être personnalisée en *gw-world:/>* par exemple, à l'aide de la ligne de commande :

```
Device:/> set device name="gw-world"
```

Le *CLI Reference Guide* (Guide de référence sur l'interface de ligne de commande) utilise tout du long l'invite de commande *gw-world:/>*.

Remarque

Quand l'invite de ligne de commande est remplacée par une nouvelle valeur, cette valeur apparaît aussi comme le nouveau nom du périphérique dans le nœud supérieur de l'arborescence de l'interface utilisateur Web.

Activation et confirmation des modifications. Si des modifications sont apportées à la configuration en cours par l'interface de ligne de commande, elles ne seront pas enregistrées dans NetDefendOS jusqu'à ce que la commande

```
gw-world:/> activate
```

soit émise.

Immédiatement après la commande *activate*, la commande

```
gw-world:/> commit
```

doit être émise pour rendre ces modifications permanentes. Si une commande *commit* n'a pas été lancée dans une période par défaut de 30 secondes, les modifications seront automatiquement ignorées et l'ancienne configuration sera restaurée.
Déconnexion de l'interface de ligne de commande. Après avoir fini de travailler avec l'interface de ligne de commande, déconnectez-vous afin d'empêcher d'autres personnes de se connecter au système sans autorisation. Déconnectez-vous en utilisant la commande *exit* ou *logout*.

L'interface utilisateur Web

NetDefendOS propose une *interface utilisateur Web* très polyvalente pour la gestion du système par le biais d'un navigateur Internet standard. Ainsi, l'administrateur peut effectuer une gestion distante de pratiquement n'importe quel endroit du monde sans avoir à installer de clients tiers.

Connexion à l'interface Web. Pour accéder à l'interface Web, lancez un navigateur Internet standard et saisissez

l'adresse IP du firewall. L'adresse par défaut du fabricant pour tout firewall D-Link est *192.168.1.1*.

Lors de la première connexion à NetDefendOS, l'administrateur DOIT utiliser le protocole https:// dans l'URL (par exemple, https://192.168.1.1). L'utilisation de HTTPS comme protocole chiffre le nom d'utilisateur et le mot de passe lorsqu'ils sont envoyés vers NetDefendOS.

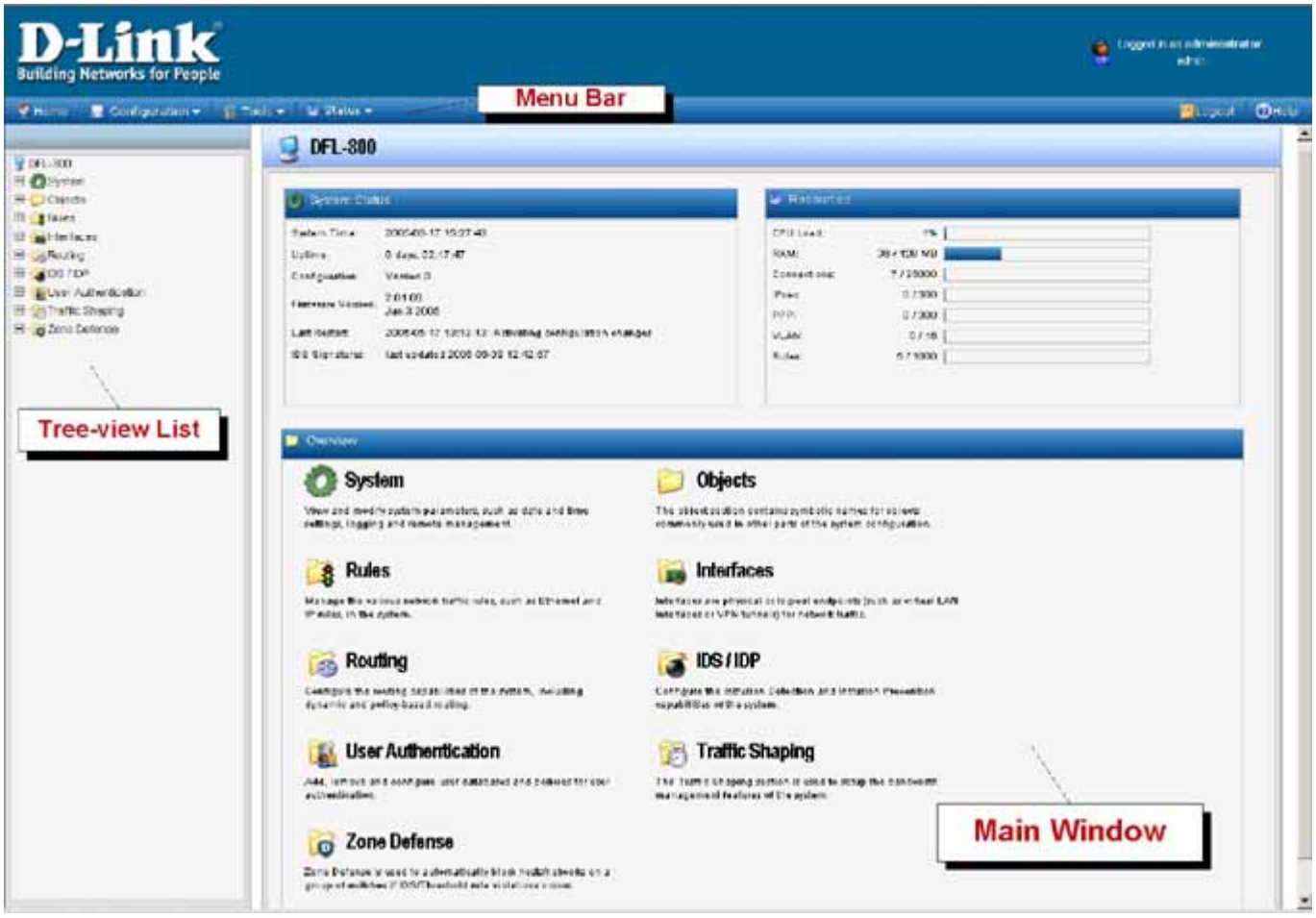
Si la communication avec NetDefendOS est correctement établie, une boîte de dialogue d'authentification de l'utilisateur similaire à celle montrée ci-dessous apparaîtra dans la fenêtre du navigateur.

Saisissez votre nom d'utilisateur et cliquez sur le bouton Login (Connexion). Si les authentifiants de l'utilisateur sont corrects, la page Web principale de l'interface apparaîtra. Cette page dont les parties essentielles sont mises en évidence est présentée ci-dessous.

Prise en charge de plusieurs langues. La boîte de dialogue de connexion de l'interface utilisateur Web offre la possibilité de choisir une autre langue que l'anglais dans l'interface. Cette prise en charge s'appuie sur un ensemble distinct de fichiers de ressources fournis avec NetDefendOS.

Il arrive qu'une mise à niveau de NetDefendOS ne bénéficie temporairement pas d'une traduction complète à cause de contraintes de temps. Dans ce cas, la version originale en anglais sera utilisée comme une solution temporaire.

Interface du navigateur Internet. Sur le côté gauche de l'interface utilisateur Web se trouve une arborescence qui permet de naviguer au travers des différents modules de NetDefendOS. La partie centrale de l'interface utilisateur Web affiche les informations qui concernent ces modules. Les informations sur la performance en cours sont affichées par défaut.



Pour obtenir des informations sur le nom d'utilisateur et le mot de passe par défaut, vous pouvez consulter la section Comptes administrateur par défaut.

Remarque

L'accès à l'interface Web est contrôlé par la stratégie de gestion distante. Par défaut, le système n'autorisera l'accès qu'au réseau interne.

Structure de l'interface. L'interface Web principale est divisée en trois sections majeures :

La barre de menus La barre de menus située en haut de l'interface Web contient des boutons et des menus déroulants utilisés non seulement pour l'exécution des tâches de configuration, mais aussi pour l'accès à divers outils et pages d'état.

Home (Accueil) : renvoie à la première page de l'interface Web.

Configuration

Save and Activate (Enregistrer et activer) : enregistre et active la configuration.

Discard Changes (Ignorer les modifications) : ignore toutes les modifications apportées à la configuration lors de la session en cours.

View Changes (Afficher les modifications) : répertorie les modifications apportées à la configuration depuis la dernière sauvegarde.

Tools (Outils) : contient plusieurs outils utiles à la maintenance du système.

Status (État) : propose diverses pages d'état utilisables lors de diagnostics du système.

Maintenance

Update Center (Centre de mise à jour) : effectuez des mises à jour manuelles ou programmées de la fonction de détection des intrusions et des signatures de virus.

License (Licence) : affichez les détails de la licence ou saisissez le code d'activation.

Backup (Sauvegarde) : sauvegardez la configuration sur votre ordinateur local ou restaurez une sauvegarde téléchargée précédemment.

Reset (Réinitialiser) : redémarrez le firewall ou réinitialisez les paramètres usine par défaut.

Upgrade (Mise à niveau) : mettez à niveau le firmware du firewall.

Navigateur — Le navigateur situé sur le côté gauche de l'interface Web contient une arborescence de la configuration du système. L'arborescence est divisée en plusieurs sections qui correspondent aux principales unités élémentaires de la configuration. L'arborescence peut être développée pour présenter des sections supplémentaires.

Fenêtre principale — La fenêtre principale contient les détails de la configuration et de l'état qui correspondent à la section sélectionnée dans le navigateur ou dans la barre de menus.

Contrôle de l'accès à l'interface Web. Par défaut, l'interface Web n'est accessible que via le réseau interne. Si vous devez autoriser l'accès à d'autres parties du réseau, vous pouvez modifier la stratégie de gestion distante.

Exemple 2.2. Activation de la gestion HTTPS distante

Interface de ligne de commande

```
gw-world:/> add RemoteManagement RemoteMgmtHTTP https
   Network=all-nets Interface=any LocalUserDatabase=AdminUsers HTTPS=Yes
```

Interface Web

Sélectionnez System > Remote Management > Add > HTTP/HTTPS Management (Système > Gestion distante > Ajouter > Gestion HTTP/HTTPS).

Saisissez le nom de la stratégie de gestion HTTP/HTTPS distante (par exemple, *https*).

Cochez la case HTTPS.

Dans les listes déroulantes, sélectionnez les éléments suivants.

User Database (Base de données utilisateur) : AdminUsers (Administrateurs)

Interface : any (toute)

Network (Réseau) : all-nets (tous les réseaux)

Cliquez sur OK.

Attention

L'exemple ci-dessus est donné à titre d'information uniquement. Il n'est jamais recommandé de dévoiler une interface de gestion à quiconque sur Internet.

Déconnexion de l'interface Web. Une fois le travail accompli sur l'interface Web, vous devez toujours vous déconnecter pour empêcher les utilisateurs qui peuvent se servir de votre poste de travail d'avoir un accès non autorisé au système. Déconnectez-vous en cliquant sur le bouton Logout (Déconnexion) à droite de la barre de menus.

Conseil

S'il survient un problème avec l'interface de gestion lors d'une communication via des tunnels VPN, vérifiez la table de routage principale et cherchez une route all-nets (tous les réseaux) vers le tunnel VPN. Si aucune route spécifique n'existe jusqu'à l'interface de gestion, le trafic de gestion en provenance de

NetDefendOS sera automatiquement dirigé vers le tunnel VPN. Si tel est le cas, l'administrateur doit ajouter une route pour diriger le trafic de gestion destiné au réseau de gestion vers la bonne interface.

Utilisation des configurations

La configuration du système s'appuie sur des objets. Chaque objet représente un élément configurable de tout type. Exemples d'objets de configuration : entrées de la table de routage, entrées du carnet d'adresses, définitions du service et règles IP. Chacun a plusieurs propriétés qui constituent les valeurs de cet objet.

Chaque objet de configuration a un type bien défini. Le type détermine les propriétés disponibles pour l'objet de configuration et leurs contraintes. Par exemple, le type *IP4Address* est utilisé pour tous les objets de configuration qui représentent une adresse IPv4 nommée.

Dans l'interface utilisateur Web, les objets de configuration sont organisés en une sorte d'arborescence et classés selon leur type.

Dans l'interface de ligne de commande, les types similaires d'objet de configuration sont regroupés en catégories. Ces catégories sont différentes de la structure utilisée dans l'interface utilisateur Web, afin de permettre un accès plus rapide aux objets de configuration dans l'interface de ligne de commande. Les types *IP4Adress*, *IP4Group* et *EthernetAddress* sont par exemple regroupés dans une catégorie nommée *Address* (Adresse), puisqu'ils représentent tous des adresses différentes. Par conséquent, les objets Ethernet et VLAN sont tous regroupés dans une catégorie nommée *Interface* puisqu'ils sont des objets d'interface. Ces catégories n'ont en fait aucun impact sur la configuration du système. Elles ne font que simplifier l'administration du système.

Les exemples suivants décrivent la manière d'utiliser les objets.

Exemple 2.3. Liste des objets de configuration

Pour identifier tous les objets de configuration existants, vous pouvez créer une liste de ceux-ci. Cet exemple décrit la manière d'établir une liste de tous les objets de service.

Interface de ligne de commande

```
gw-world:/> show Service
```

Une liste de tous les services classés selon leur type respectif s'affiche.

Interface Web

Sélectionnez Objects > Services (Objets > Services).

Une page Web qui répertorie tous les services s'affiche.

Une liste contient les éléments de base suivants.

Add (Ajouter) : le bouton affiche un menu déroulant après avoir cliqué dessus. Le menu répertorie tous les types d'élément de configuration qui peuvent être ajoutés à la liste.

Header (En-tête) : la ligne d'en-tête affiche les titres des colonnes de la liste. Les petites icônes en flèche situées près de chaque titre peuvent être utilisées pour trier la liste dans chaque colonne.

Rows (Lignes) : chaque ligne de la liste correspond à un élément de configuration. De manière générale, chaque ligne débute par le nom de l'objet (si l'élément a un nom), suivi par les valeurs des colonnes de la liste.

Le fait de cliquer à un endroit de la ligne sans lien hypertexte permet de ne sélectionner qu'une seule ligne. Le fond de la ligne devient bleu foncé. Le fait de cliquer avec le bouton droit de la souris sur la ligne fait apparaître un menu grâce auquel les objets peuvent être modifiés, supprimés ou réordonnés.

Exemple 2.4. Affichage d'un objet de configuration

L'opération la plus simple à effectuer sur un objet de configuration est d'afficher son contenu, c'est-à-dire les valeurs des propriétés de cet objet. Cet exemple décrit la manière d'afficher le contenu d'un objet de configuration qui représente le service *telnet*.

Interface de ligne de commande

```
gw-world:/> show Service ServiceTCPUDP telnet

   Property Value
 ---------------- -------
    Name: telnet
 DestinationPorts: 23
    Type: TCP
  SourcePorts: 0-65535
   SYNRelay: No
 PassICMPReturn: No
    ALG: (none)
  MaxSessions: 1000
   Comments: Telnet
```

La colonne Property (Propriété) répertorie les noms de toutes les propriétés de la classe ServiceTCPUDP et la colonne Value (Valeur) répertorie les valeurs des propriétés correspondantes.

Interface Web

Sélectionnez Objects > Services (Objets > Services).

Cliquez sur le lien hypertexte telnet dans la liste.

Une page Web du service telnet s'affiche.

> **Remarque**
> Pour accéder à un objet via l'interface de ligne de commande, vous pouvez omettre le nom de la catégorie et simplement utiliser le nom du type. La ligne de commande de l'exemple ci-dessus peut donc être simplifiée par :
>
> ```
> gw-world:/> show ServiceTCPUDP telnet
> ```

Exemple 2.5. Modification d'un objet de configuration

Pour modifier le fonctionnement de NetDefendOS, vous allez très probablement devoir modifier un ou plusieurs des objets de configuration. Cet exemple décrit la manière de modifier la propriété *Comments* du service *telnet*.

Interface de ligne de commande

```
gw-world:/> set Service ServiceTCPUDP telnet Comments="Modified Comment"
```

Affichez à nouveau l'objet pour vérifier la nouvelle valeur de la propriété :

```
gw-world:/> show Service ServiceTCPUDP telnet

   Property Value
 ---------------- -------
    Name: telnet
 DestinationPorts: 23
    Type: TCP
  SourcePorts: 0-65535
   SYNRelay: No
 PassICMPReturn: No
    ALG: (none)
  MaxSessions: 1000
   Comments: Modified Comment
```

Interface Web

Sélectionnez Objects > Services (Objets > Services).

Cliquez sur le lien hypertexte telnet dans la liste.

Dans la zone de texte Comments (Commentaires), saisissez votre nouveau commentaire.

Cliquez sur OK.

Vérifiez que le nouveau commentaire a bien été mis à jour dans la liste.

Important

Les modifications apportées à un objet de configuration ne seront pas appliquées au système en cours d'exécution tant que vous ne les aurez pas activées et confirmées.

Exemple 2.6. Ajout d'un objet de configuration

Cet exemple décrit la manière dont vous pouvez ajouter un nouvel objet *IP4Address* en créant l'adresse IP 192.168.10.10 dans le carnet d'adresses.

Interface de ligne de commande

```
gw-world:/> add Address IP4Address myhost Address=192.168.10.10
```

Affichez le nouvel objet :

```
gw-world:/> show Address IP4Address myhost

    Property Value
 -------------------- -------------
     Name: myhost
    Address: 192.168.10.10
  UserAuthGroups: (none)
 NoDefinedCredentials: No
    Comments: (none)
```

Interface Web

Sélectionnez Objects > Address Book (Objets > Carnet d'adresses).

Cliquez sur le bouton Add (Ajouter).

Dans le menu déroulant affiché, sélectionnez l'adresse IP4.

Dans la zone de texte Name (Nom), saisissez myhost.

Saisissez 192.168.10.10 dans la zone de texte de l'adresse IP.

Cliquez sur OK.

Vérifiez que la nouvelle adresse IP4 de l'objet a bien été ajoutée à la liste.

Exemple 2.7. Suppression d'un objet de configuration

Cet exemple décrit la manière de supprimer l'objet *IP4Address* récemment ajouté.

Interface de ligne de commande

```
gw-world:/> delete Address IP4Address myhost
```

Interface Web

Sélectionnez Objects > Address Book (Objets > Carnet d'adresses).

Cliquez avec le bouton droit de la souris sur la ligne contenant l'objet myhost.

Dans le menu déroulant affiché, sélectionnez Delete (Supprimer).

La ligne est barrée, ce qui indique qu'elle est en cours de suppression.

Exemple 2.8. Annulation de la suppression d'un objet de configuration

Un objet supprimé peut toujours être restauré avant que la configuration n'ait été activée et confirmée. Cet exemple décrit la manière de restaurer l'objet *IP4Address* précédemment supprimé.

Interface de ligne de commande

```
gw-world:/> undelete Address IP4Address myhost
```

Interface Web

Sélectionnez Objects > Address Book (Objets > Carnet d'adresses).

Cliquez avec le bouton droit de la souris sur la ligne qui contient l'objet myhost.

Dans le menu déroulant affiché, sélectionnez Undo Delete (Annuler la suppression).

Consultation de la liste des objets modifiés. Après avoir modifié plusieurs objets de configuration, vous pouvez avoir envie de consulter une liste des objets modifiés, ajoutés ou supprimés depuis la dernière sauvegarde.

Exemple 2.9. Affichage de la liste des objets de configuration

Cet exemple décrit la manière de répertorier les objets de configuration modifiés.

Interface de ligne de commande

```
gw-world:/> show -changes

 Type   Object
 ------------ ------
 - IP4Address  myhost
 * ServiceTCPUDP telnet
```

Le signe + au début d'une ligne indique que l'objet a été ajouté. Le signe * indique que l'objet a été modifié. Le signe - indique que l'objet est en cours de suppression.

Interface Web

Dans la barre de menus, sélectionnez Configuration > View Changes (Configuration > Afficher les modifications).

Une liste des modifications apparaît.

Activation et confirmation d'une configuration. Après avoir apporté des modifications à une configuration, cette dernière doit être activée pour que les modifications prennent effet sur le système en cours d'exécution. Lors du processus d'activation, la nouvelle configuration est validée et NetDefendOS essaye d'initialiser les sous-systèmes affectés avec les données de la nouvelle configuration.

> **Confirmation des modifications IPSec**
> L'administrateur doit savoir que, si des modifications qui affectent les configurations des tunnels directs sont validées, les connexions de ces tunnels SERONT INTERROMPUES et devront être relancées.

Si la nouvelle configuration est validée, NetDefendOS attendra une courte période (30 secondes par défaut) durant laquelle une connexion avec l'administrateur doit être rétablie. À titre de rappel, si la configuration a été activée via l'interface de ligne de commande grâce à la commande *activate*, une commande *commit* doit être lancée au cours de cette période. Si une connexion perdue ne peut être rétablie ou si la commande *commit* n'a pas été lancée, NetDefendOS reviendra à l'ancienne configuration. Il s'agit d'un mécanisme à sécurité intégrée, notamment capable d'éviter qu'un administrateur distant ne procède au verrouillage.

Exemple 2.10. Activation et confirmation d'une configuration

Cet exemple décrit la manière d'activer et de confirmer une nouvelle configuration.

Interface de ligne de commande

```
gw-world:/> activate
```

Le système valide et commence à utiliser la nouvelle configuration. Lorsque l'invite de commande

```
gw-world:/> commit
```

réapparaît, la nouvelle configuration est désormais confirmée.

Interface Web

Dans la barre de menus, sélectionnez Configuration > Save and Activate (Configuration > Enregistrer et activer).

Cliquez sur OK.

Le navigateur Web essaye automatiquement de se reconnecter à l'interface Web après 10 secondes. Si la connexion s'établit, la gestion distante fonctionne toujours d'après l'interprétation de NetDefendOS. La nouvelle configuration est automatiquement confirmée.

Remarque

La configuration doit être confirmée avant que les modifications ne soient enregistrées. Toutes les modifications apportées à une configuration peuvent être ignorées en omettant l'étape de confirmation.

Événements et consignation

Présentation

La possibilité de consigner et d'analyser les activités du système représente une fonctionnalité essentielle de NetDefendOS. La consignation permet non seulement de surveiller l'état et le bon fonctionnement du système, mais aussi de vérifier l'utilisation du réseau et de faciliter le dépannage.

NetDefendOS définit plusieurs *event messages* (messages d'événements) qui sont générés en conséquence d'événements du système correspondants. Exemples d'événements : établissement ou échec de connexions, réception de paquets corrompus et interruption du trafic selon les règles de filtrage.

Quand un event message (message d'événement) est généré, il peut être filtré et affiché par tous les event receivers (récepteurs d'événements) après configuration. L'administrateur peut configurer plusieurs event receivers (récepteurs d'événements), qui peuvent avoir chacun leur propre event filter (filtre d'événements) personnalisé.

La conception complexe des mécanismes d'événements et de consignation de NetDefendOS garantit que la possibilité de connexion est simple et directe. Parallèlement, le contrôle de toutes les activités du système reste très fin pour les déploiements les plus avancés.

Messages d'événements

NetDefendOS détermine plusieurs centaines d'événements pour lesquels des event messages (messages d'événements) peuvent être générés. Les événements peuvent être : high-level (de haut niveau), customizable (personnalisables), user events (de l'utilisateur), low-level (de bas niveau) ou mandatory system events (obligatoires au système).

Par exemple, l'événement *conn_open* est un événement généralement high-level (de haut niveau), qui génère un event message (message d'événement) chaque fois qu'une nouvelle connexion est établie. En effet, la règle de sécurité correspondante définit que les event messages (messages d'événements) doivent être générés lors de cette connexion.

Exemple d'événement low-level (de bas niveau) : l'événement *startup_normal*, qui génère un event message (message d'événement) obligatoire lorsque le système démarre.

Tous les event messages (messages d'événements) sont établis sur un format commun, qui regroupe la catégorie, la gravité et les actions recommandées. Ces attributs permettent un filtrage facile des messages, dans NetDefendOS avant même leur envoi à un event receiver (récepteur d'événement) ou lors de l'analyse après la consignation et le stockage des messages sur un serveur de consignation externe.

Une liste de tous les event messages (messages d'événements) est consultable dans le *Log Reference Guide* (Guide de référence des événements). Ce guide décrit aussi la structure des event messages (messages d'événements), ainsi que les divers attributs disponibles. La gravité de chaque événement est prédéfinie et classée selon son degré :

Emergency (Urgence)
Alert (Alerte)

Critical (Critique)
Error (Erreur)
Warning (Avertissement)
Notice (Avis)
Info
Debug (Débogage)

Par défaut, tous les messages du niveau Info ou supérieur sont affichés. La catégorie Debug (Débogage) n'est destinée qu'aux dépannages et ne doit être activée que s'il est nécessaire de résoudre un problème. Les messages de tout degré de gravité sont consultables dans le Log Reference Guide (Guide de référence des événements) de NetDefendOS.

Répartition des messages d'événements

Pour répartir et enregistrer les event messages (messages d'événements) générés, il est nécessaire de définir un ou plusieurs event receivers (récepteurs d'événements) qui spécifient *quels* événements choisir et *où* les envoyer.

NetDefendOS peut répartir les event messages (messages d'événements) des façons suivantes :

Memlog Le firewall D-Link a un mécanisme de consignation intégré, du nom de *Memory Log* (Mémoire des événements). Il sauvegarde tous les messages d'événements dans la mémoire et permet de les afficher directement grâce à l'interface Web.

Syslog Le standard de référence pour la consignation d'événements des périphériques réseau. Si d'autres périphériques réseau sont déjà consignés sur les serveurs Syslog, utiliser Syslog avec les messages de NetDefendOS peut simplifier l'administration générale.

Enregistrement vers des hôtes Syslog

Syslog est un protocole standard pour la transmission des données de journal, bien qu'il n'existe pas de format standard pour les messages de consignation eux-mêmes. Le format utilisé par NetDefendOS convient bien aux traitements, filtrages et recherches automatiques.

Bien que les formats exacts de chaque entrée de journal dépendent du mode de fonctionnement d'un récepteur Syslog, la plupart se ressemblent beaucoup. La façon dont les journaux sont lus dépend aussi du mode de fonctionnement du récepteur Syslog. Les daemons Syslog des serveurs UNIX enregistrent généralement des éléments dans des fichiers texte, ligne par ligne.

La plupart des récepteurs Syslog font précéder chaque entrée de journal d'une indication d'horodatage et de l'adresse IP de la machine à l'origine de l'envoi des données de journal.

```
Feb 5 2000 09:45:23 gateway.ourcompany.com
```

Vient ensuite le texte d'envoi choisi par l'expéditeur.

```
Feb 5 2000 09:45:23 gateway.ourcompany.com EFW: DROP:
```

Le texte qui vient ensuite dépend de l'événement survenu.

Afin de faciliter le traitement automatique de tous les messages, NetDefendOS écrit toutes les données de journal en une seule ligne de texte. Toutes les données suivant le texte d'origine est présenté sur le format : *name=value* (nom=valeur). Ainsi, les filtres automatiques permettent de rechercher facilement des valeurs sans partir du fait qu'une donnée spécifique se trouve à un endroit spécifique dans l'entrée de journal.

Remarque

Le champ Prio= des messages Syslog contient les mêmes informations que le champ Severity (Gravité) des messages de journal D-Link. Toutefois, l'ordre de numérotation est inversé.

Exemple 2.11. Activation de l'enregistrement sur un hôte Syslog

Pour activer l'enregistrement de tous les événements dont le niveau de gravité est supérieur ou égal à Notice (Avis) sur un serveur Syslog dont l'adresse IP est 195.11.22.55, suivez les étapes présentées ci-dessous.

Interface de ligne de commande

```
gw-world:/> add LogReceiverSyslog my_syslog IPAddress=195.11.22.55
```

Interface Web

Sélectionnez System > Log and Event Receiver > Add > Syslog Receiver (Système > Journal et récepteur d'événements > Ajouter > Récepteur Syslog).

Spécifiez un nom adapté à l'event receiver (récepteur d'événement). Par exemple : *my_syslog*.

Saisissez l'adresse IP *195.11.22.55*.

Sélectionnez une option appropriée dans la liste « facility ». Le nom « facility » est généralement utilisé comme un paramètre de filtrage pour la plupart des daemons Syslog.

Cliquez sur OK.

Le système enregistre désormais tous les événements dont le niveau de gravité est supérieur ou égal à Notice (Avis) dans le serveur Syslog *195.11.22.55*.

> **Remarque**
> Le serveur Syslog devra peut-être être configuré pour recevoir les messages de consignation de NetDefendOS. Consultez la documentation spécifique du logiciel de votre serveur Syslog afin de le configurer correctement.

Interruptions SNMP

Protocole SNMP. Le SNMP (Simple Network Management Protocol) est un moyen de communication entre un service de messagerie réseau et un périphérique géré. Il définit 3 types de messages : la commande *Read* pour que le service de messagerie réseau examine un périphérique géré, une commande *Write* pour modifier l'état d'un périphérique géré et une commande *Trap* utilisée par les périphériques gérés pour envoyer des messages de manière décalée à un service de messagerie réseau à propos d'un changement d'état.

Interruptions SNMP dans NetDefendOS. NetDefendOS amène le concept d'interruption SNMP une étape plus loin en autorisant l'envoi de n'importe quel message comme une interruption SNMP. En d'autres termes, l'administrateur peut configurer la notification d'événements sur l'interruption SNMP que vous considérez comme étant importante pour l'utilisation d'un réseau.

Le fichier *DFLNNN-TRAP.MIB* (*NNN* représente la référence du firewall) est fourni par D-Link. Il définit les objets SNMP et les types de donnée utilisés pour décrire une interruption SNMP reçue de NetDefendOS.

> **Remarque**
> Il existe un fichier MIB différent pour chaque modèle de firewall D-Link. Assurez-vous d'utiliser le bon fichier.

Pour chaque modèle de firewall D-Link, il existe un objet d'interruption générique appelé *DLNNNosGenericTrap* et utilisé pour chaque interruption (*NNN* représente la référence). Cet objet inclut les paramètres suivants.

System (Système) : système générant l'interruption.

Severity (Gravité) : gravité du message.

Category (Catégorie) : problème rapporté par le sous-système de NetDefendOS.

*ID : i*dentification unique dans la catégorie.

Description : courte description textuelle.

Action : action de NetDefendOS.

Ces informations peuvent faire l'objet de références croisées – *Log Reference Guide* (Guide de référence des événements).

Remarque

NetDefendOS envoie des interruptions SNMP basées sur le standard SNMPv2c, comme le définissent RFC1901, RFC1905 et RFC1906.

Exemple 2.12. Envoi des interruptions SNMP à un récepteur d'interruptions SNMP

Pour permettre l'envoi d'interruptions SNMP pour tous les événements dont le niveau de gravité est supérieur ou égal à Alert (Alerte) à un récepteur d'interruptions SNMP dont l'adresse IP est 195.11.22.55, suivez les étapes ci-dessous.

Interface de ligne de commande

```
gw-world:/> add LogReceiver EventReceiverSNMP2c my_snmp IPAddress=195.11.22.55
```

Interface Web

Sélectionnez Log & Event Receivers > Add > EventReceiverSNMP2c (Journal et récepteurs d'événements > Ajouter > EventReceiverSNMP2c).

Spécifiez le nom de l'event receiver (récepteur d'événements). Par exemple : *my_snmp*.

Saisissez l'adresse IP 195.11.22.55.

Saisissez une chaîne de communauté SNMP si le récepteur d'interruption la requiert.

Cliquez sur OK.

Le système envoie désormais des interruptions SNMP pour tous les événements dont le niveau de gravité est supérieur ou égal à Alert (Alerte) à un récepteur d'interruptions SNMP 195.11.22.55.

Comptabilisation RADIUS

Présentation

Dans un environnement réseau basé sur un grand nombre d'utilisateurs, il est avantageux d'avoir un ou plusieurs serveurs centraux pour conserver les informations des comptes utilisateur et prendre en charge l'identification et les tâches d'autorisation. La base de données centrale se trouvant sur le ou les serveurs dédiés conserve tous les authentifiants des utilisateurs ainsi que le détail des connexions, ce qui réduit de manière significative la complexité de la tâche d'administration. RADIUS (Remote Authentication Dial-in User Service) est un protocole d'authentification, d'autorisation et de comptabilisation (AAA) largement utilisé pour appliquer cette méthode et exploité par NetDefendOS pour mettre en œuvre la comptabilisation des utilisateurs.

Le protocole RADIUS est basé sur une architecture client/serveur. Le firewall D-Link agit comme le client du serveur RADIUS : il crée et envoie des requêtes à des serveurs spéciaux. Dans la terminologie RADIUS, le firewall agit comme le serveur d'accès réseau (NAS). Lors de l'identification de l'utilisateur, le serveur RADIUS reçoit les requêtes, vérifie les informations de l'utilisateur en consultant sa base de données, et accepte ou refuse le client demandé. Dans RFC2866, RADIUS allait jusqu'à se charger de la remise des informations de comptabilisation. Il s'agit du standard suivi par NetDefendOS pour la comptabilisation des utilisateurs. Les avantages d'avoir des serveurs centralisés s'étendent donc à la comptabilisation des connexions utilisateur. (Pour obtenir des détails sur l'utilisation de RADIUS lors de l'authentification NetDefendOS, consultez la section Configuration de l'authentification.)

Messages de comptabilisation RADIUS

Les statistiques, telles que le nombre d'octets émis et reçus et le nombre de paquets émis et reçus, sont mises à jour et stockées tout au long des sessions RADIUS. Toutes les statistiques d'un utilisateur authentifié sont mises à jour chaque fois qu'une connexion relative à cet utilisateur est coupée.

Quand une nouvelle session client est ouverte par un utilisateur qui établit une nouvelle connexion grâce au firewall D-Link, NetDefendOS envoie un message *AccountingRequest* (réponse de comptabilisation) de type START à un serveur spécial pour enregistrer le début d'une nouvelle session. Les informations du compte

utilisateur sont transmises au serveur RADIUS. Le serveur va renvoyer un message d'accusé de réception *AccountingResponse* (réponse de comptabilisation) à NetDefendOS.

Par exemple, quand un utilisateur n'est plus authentifié après sa déconnexion ou l'expiration de la session, un message *AccountingRequest* (requête de comptabilisation) de type STOP sur les statistiques importantes de la session est envoyé par NetDefendOS. Les informations incluses dans ces statistiques sont configurables par l'utilisateur. Le contenu des messages de type START ou STOP est décrit ci-dessous.

Paramètres du message de type START. Les paramètres inclus dans les messages de type START envoyés par NetDefendOS sont les suivants.

Type : signale le début (START) du service dans AccountingRequest (requête de comptabilisation).

ID : identifiant unique pour permettre la concordance d'AccountingRequest (requête de comptabilisation) et d'Acct-Status-Type (Type-état-compt.) défini sur STOP.

User Name (Nom de l'utilisateur) : nom d'utilisateur de la personne authentifiée.

NAS IP Address (Adresse IP NAS) : adresse IP du firewall de D-Link.

NAS Port (Port NAS) : port du NAS sur lequel l'utilisateur était authentifié (il s'agit d'un port physique et non d'un port TCP ou UDP).

User IP Address (Adresse IP de l'utilisateur) : adresse IP de l'utilisateur authentifié. Ce message est envoyé uniquement en cas d'indication sur le serveur d'authentification.

How Authenticated (Mode d'authentification) : mode d'authentification de l'utilisateur. Il peut s'agir soit de *RADIUS* si l'utilisateur s'est authentifié via RADIUS, soit de *LOCAL* si l'utilisateur s'est authentifié via la base de donnée utilisateur locale.

Delay Time (Temps d'attente) : temps d'attente (en secondes) entre l'envoi du paquet d'AccountingRequest (requête de comptabilisation) et la réception de la reconnaissance de l'authentification. Ce temps peut être soustrait au temps d'arrivée sur le serveur afin de trouver le temps approximatif de la génération de ce message AccountingRequest (requête de comptabilisation) par l'événement. Remarque : ce temps ne prend pas en compte les attentes réseau. Le paramètre de la première tentative sera défini sur 0.

Timestamp (Estampille) : nombre de secondes écoulées depuis le 01/01/1970. Elle est utilisée lors de l'envoi du paquet par NetDefendOS.

Paramètres du message STOP. Les paramètres inclus dans les messages STOP envoyés par NetDefendOS sont les suivants.

Type : signale l'arrêt d'une session (STOP) dans AccountingRequest (requête de comptabilisation).

ID : identifiant qui fait correspondre le paquet d'AccountingRequest (requête de comptabilisation) précédemment envoyé avec l'Acct-Status-Type (Type-état-compt.) défini sur START.

User Name (Nom de l'utilisateur) : nom d'utilisateur de la personne authentifiée.

NAS IP Address (Adresse IP NAS) : adresse IP du firewall de D-Link.

NAS Port (Port NAS) : port NAS sur lequel l'utilisateur était authentifié. (Il s'agit d'un port physique et non d'un port TCP ou UDP.)

User IP Address (Adresse IP de l'utilisateur) : adresse IP de l'utilisateur authentifié. Ce message est envoyé uniquement en cas d'indication sur le serveur d'authentification.

Input Bytes (Octets entrants) : nombre d'octets reçus par l'utilisateur. (*)

Output Bytes (Octets sortants) : nombre d'octets émis par l'utilisateur. (*)

Input Packets (Paquets entrants) : nombre de paquets reçus par l'utilisateur. (*)

Output Packets (Paquets sortants) : nombre de paquets émis par l'utilisateur. (*)

Session Time (Durée de la session) : durée de la session en secondes. (*)

Termination Cause (Cause de l'arrêt) : raison pour laquelle la session a été fermée.

How Authenticated (Mode d'authentification) : mode d'authentification de l'utilisateur. Il s'agit soit de *RADIUS* si l'utilisateur s'est authentifié via RADIUS, soit de *LOCAL* si l'utilisateur s'est authentifié via la base de donnée utilisateur locale.

Delay Time (Temps d'attente) : consultez la description ci-dessus.

Timestamp (Estampille) : nombre de secondes écoulées depuis le 01/01/1970. Elle est utilisée lors de l'envoi du paquet par le firewall de D-Link. De plus, deux attributs supplémentaires peuvent être envoyés.

Input Gigawords (Gigawords entrants) : indique le nombre de tours effectués par le compteur d'Input Bytes (Octets entrants). Cet attribut est envoyé uniquement si le compteur a fait un tour et si l'attribut Input Bytes (Octets entrants) est envoyé.

Output Gigawords (Gigawords sortants) : indique le nombre de tours effectués par le compteur d'Output Bytes (Octets sortants). Cet attribut est envoyé uniquement si le compteur a fait un tour et si l'attribut Output Bytes (Octets sortants) est envoyé.

Remarque

Dans la liste ci-dessus, le symbole (*) indique que l'envoi du paramètre est configurable par l'utilisateur.

Messages de comptabilisation d'attente

En plus des messages START et STOP, NetDefendOS peut de manière facultative et périodique envoyer des *Interim Accounting Messages* (Messages de comptabilisation d'attente) pour mettre à jour le serveur de comptabilisation avec l'état en cours d'un utilisateur authentifié. Un *Interim Accounting Message* (Message de comptabilisation d'attente) peut être considéré comme une « capture » des ressources du réseau qu'un utilisateur authentifié a utilisé jusqu'à un moment donné. Grâce à cette fonctionnalité, le serveur RADIUS peut tracer le nombre d'octets et de paquets qu'un utilisateur authentifié a émis et reçu jusqu'au moment où le dernier message a été envoyé.

Un *Interim Accounting Message* (Message de comptabilisation d'attente) contient les valeurs en cours des statistiques d'un utilisateur authentifié. Il contient plus ou moins les mêmes paramètres que le message AccountingRequest (requête de comptabilisation) de type STOP, à l'exception faite que l'*Acct-Terminate-Cause* (Cause-arrêt-compt.) n'est pas incluse (puisque l'utilisateur n'est pas encore déconnecté).

La fréquence des Interim Accounting Messages (Messages de comptabilisation d'attente) peut être configurée soit sur le serveur d'authentification, soit sur NetDefendOS. Le fait d'enclencher ce paramètre dans NetDefendOS remplace ce même paramètre sur le serveur de comptabilisation.

Activation de la fonction de comptabilisation RADIUS

Pour activer la fonction de comptabilisation RADIUS, un certain nombre d'étapes doivent être suivies.

Le serveur de comptabilisation RADIUS doit être spécifié.

Une règle doit être associée à un objet d'authentification utilisateur sur le serveur RADIUS spécifié.

Quelques points importants sont à noter sur cette activation :

La fonction de comptabilisation RADIUS ne fonctionnera pas pour une connexion soumise à une règle *FwdFast* paramétrée dans les règles IP.

Il n'est pas obligatoire d'utiliser un même serveur RADIUS pour l'authentification et la comptabilisation : un serveur peut se charger de l'authentification et un autre peut se charger des tâches de comptabilisation.

Des serveurs RADIUS multiples peuvent être configurés dans NetDefendOS si le serveur principal est

inaccessible.

Sécurité de comptabilisation RADIUS

La communication entre NetDefendOS et n'importe quel serveur de comptabilisation RADIUS est protégée par l'intermédiaire d'un secret partagé. Ce secret n'est jamais envoyé sur le réseau. À la place, un *Authenticator code* (authentificateur) de 16 octets est calculé à l'aide de la fonction de hachage MD5 et utilisé pour authentifier les messages de comptabilisation.

Le secret partagé respecte la casse, peut contenir jusqu'à 100 caractères, et doit être tapé d'exactement la même façon sous NetDefendOS et sur le serveur RADIUS.

Les messages sont envoyés à l'aide du protocole UDP. Le numéro du port par défaut est 1813. Ce paramètre peut être configuré par l'utilisateur.

Comptabilisation RADIUS et haute disponibilité

Dans un cluster de haute disponibilité, les informations de comptabilisation sont synchronisées entre les firewalls D-Link passifs et actifs. En d'autres termes, les informations de comptabilisation sont automatiquement mises à jour sur les deux membres du cluster lorsque la connexion est terminée. L'unité active utilise deux événements de comptabilisation spéciaux pour être synchrone avec l'unité passive.

Un événement AccountingStart est envoyé au membre inactif avec un paramètre de haute disponibilité chaque fois qu'une réponse est reçue de la part du serveur de comptabilisation. Il indique que les informations de comptabilisation doivent être stockées pour chaque utilisateur authentifié.

Un problème avec la synchronisation des informations de comptabilisation peut survenir si les connexions associées à un utilisateur authentifié d'une unité active expirent avant qu'elles ne soient synchronisées avec l'unité passive. Pour résoudre ce problème, un événement spécial AccountingUpdate est envoyé à l'unité passive sur la base d'une temporisation. Cet événement contient les informations de comptabilisation les plus récentes sur les connexions.

Serveurs sans réponse

Une question se soulève lorsqu'un client qui envoie le paquet *AccountingRequest* (réponse de comptabilisation) de type START avec le serveur RADIUS ne donne jamais de réponse. NetDefendOS renverra la requête après une période en secondes spécifiée par l'utilisateur. Cependant, l'utilisateur bénéficiera encore d'un accès authentifié lorsque NetDefendOS essayera de contacter le serveur de comptabilisation.

Après trois tentatives infructueuses, NetDefendOS considère le serveur de comptabilisation comme étant inaccessible. L'administrateur peut utiliser le paramètre avancé AllowAuthIfNoAccountingResponse de NetDefendOS pour déterminer la manière de gérer cette situation. Si ce paramètre est activé, la session de l'utilisateur authentifié ne sera pas affectée. Dans le cas contraire, tous les utilisateurs effectifs seront automatiquement déconnectés même s'ils se sont déjà authentifiés.

Comptabilisation et interruption système

Si le client échoue dans l'envoi du paquet *AccountingRequest* (requête de comptabilisation) RADIUS de type STOP pour une quelconque raison, le serveur de comptabilisation ne pourra plus mettre à jour ses statistiques utilisateur et en déduira probablement que la session est encore active. Cette situation doit être évitée.

Si l'administrateur du firewall D-Link émet une commande d'interruption alors que des utilisateurs authentifiés sont encore connectés, le paquet *AccountingRequest* (requête de comptabilisation) de type STOP ne sera probablement jamais envoyé. Pour éviter cela, NetDefendOS a le paramètre avancé LogOutAccUsersAtShutdown. Ce paramètre permet à l'administrateur de spécifier explicitement que NetDefendOS doit envoyer un message de type STOP pour chaque utilisateur authentifié à tous les serveurs RADIUS configurés avant de lancer l'interruption.

Limitations avec NAT

Le module d'authentification utilisateur de NetDefendOS se base sur l'adresse IP de l'utilisateur. Des problèmes peuvent survenir avec des utilisateurs partageant une même adresse IP.

Cela peut arriver par exemple quand plusieurs utilisateurs sont derrière le même réseau et utilisent NAT pour pouvoir bénéficier d'un accès au réseau grâce à une seule adresse IP externe. En d'autres termes, dès qu'un utilisateur est authentifié, le trafic provenant de l'adresse IP de la passerelle NAT peut être considéré comme provenant de cet utilisateur authentifié, alors qu'il peut provenir d'autres utilisateurs du même réseau. La fonction de comptabilisation RADIUS de NetDefendOS regroupe donc les statistiques de tous les utilisateurs du réseau comme s'il n'en existait qu'un seul.

Surveillance

Surveillance SNMP

Présentation. SNMP (*Simple Network Management Protocol*) est un protocole standard pour la gestion des périphériques réseau. Un client compatible SNMP peut se connecter à un périphérique réseau également compatible avec le protocole SNMP pour lui envoyer des requêtes et la contrôler.

NetDefendOS est compatible avec la version 1 et 2 de SNMP. La connexion peut être établie par tout client compatible SNMP avec des périphériques NetDefendOS. Cependant, seules les opérations de requête sont autorisées pour des raisons de sécurité. NetDefendOS est plus particulièrement compatible avec les opérations de requête SNMP suivantes :

L'opération *GET REQUEST*.

L'opération *GET NEXT REQUEST*.

L'opération *GET BULK REQUEST* (pour les versions 2c de SNMP uniquement).

MIB de NetDefendOS. MIB est une base de données, généralement sous forme d'un fichier, qui définit les paramètres d'un périphérique réseau qu'un client SNMP peut modifier ou auquel il peut envoyer une requête. Le fichier MIB pour un périphérique NetDefendOS est fourni avec le pack standard NetDefendOS sous le nom de fichier *DFLNNN-TRAP.MIB* (*NNN* représente la référence du firewall). Ce fichier doit être transféré sur le disque dur du poste de travail qui va exécuter le client SNMP pour qu'il puisse être importé par le logiciel du client. Lorsque le client fonctionne, le fichier MIB est ouvert pour indiquer les valeurs qui peuvent faire l'objet d'une requête sur un périphérique NetDefendOS.

Définition de l'accès SNMP. L'accès SNMP est défini par un objet *Remote* de NetDefendOS avec un *Mode* de SNMP. L'objet Remote requiert la saisie des éléments suivants.

Interface : interface de NetDefendOS dans laquelle la requête SNMP va arriver.

Network (Réseau) : adresse IP ou réseau source de la requête SNMP.

Community (Communauté) : chaîne de communauté qui garantit la sécurité des mots de passe des accès.

Chaîne de communauté. Pour la version 1 et 2 de SNMP, la sécurité est garantie par la chaîne de communauté, qui ressemble à un mot de passe d'accès SNMP. La chaîne de communauté ne doit pas être facile à deviner et donc être élaborée sur la même base que tout autre mot de passe (à l'aide d'une combinaison de majuscules, de minuscules et de chiffres).

Activation d'une règle IP pour SNMP. Le paramètre avancé SNMPBeforeRules de la section RemoteAdmin (Administrateur distant) contrôle si la configuration de la règle IP surveille tous les accès par clients SNMP. Ce paramètre est désactivé par défaut, mais nous recommandons de toujours l'activer.

La conséquence de l'activation de ce paramètre est d'ajouter une règle invisible en haut de l'ensemble des règles IP, qui autorise automatiquement l'accès au port 161 du réseau et à l'interface définie pour l'accès SNMP. Le port 161 est généralement utilisé pour SNMP et NetDefendOS attend toujours le trafic SNMP sur ce port.

Chiffrement des accès distants. Remarque : lors des accès à la version 1 et 2c de SNMP, la chaîne de communauté est envoyée en texte clair sur le réseau. Cette situation est clairement un cas d'insécurité si un client distant est en communication via Internet. Il est donc conseillé de faire en sorte que les accès distants s'effectuent via un tunnel VPN chiffré ou tout autre moyen de communication au niveau de sécurité équivalent.

Prévention de la surcharge SNMP. Le paramètre avancé SNMPReqLimit restreint le nombre de requêtes SNMP autorisées par seconde. Il peut aider à prévenir des attaques basées sur une surcharge SNMP.

Exemple 2.13. Activation de la surveillance SNMP

Cet exemple active l'accès SNMP par une interface lan interne depuis le réseau mgmt-net, à l'aide de la chaîne de communauté *Mg1RQqR*. (Puisque la gestion du client se fait sur le réseau interne, nous n'avons pas besoin de lui appliquer un tunnel VPN.)

Interface de ligne de commande

```
gw-world:/> add RemoteManagement RemoteMgmtSNMP my_snmp Interface=lan
 Network=mgmt-net SNMPGetCommunity=Mg1RQqR
```

S'il est nécessaire d'activer SNMPBeforeRules (activation par défaut), la commande est alors :

```
gw-world:/> set Settings RemoteMgmtSettings SNMPBeforeRules=Yes
```

Interface Web

Sélectionnez System > Remote Management > Add > SNMP management (Système > Gestion distante > Ajouter > Gestion SNMP).

Pour Remote access (Accès distant), saisissez les éléments suivants.

Name (Nom) : nom adapté

Community (Communauté) : Mg1RQqR

Pour Access Filter (Filtre d'accès), saisissez les éléments suivants.

Interface : lan

Network (Réseau) : mgmt-net

Cliquez sur OK.

S'il est nécessaire d'activer SNMPBeforeRules (activation par défaut), vous trouverez ce paramètre dans System > Remote Management > Advanced Settings (Système > Gestion distante > Paramètres avancés).

Maintenance

Mécanisme de mise à jour automatique

En ce qui concerne les mises à jour automatiques et le filtrage de contenu, des fonctionnalités de NetDefendOS reposent sur des serveurs externes. Le système de prévention et de détection des intrusions ainsi que les modules antivirus requièrent un accès à des bases de données de signatures actualisées pour garantir une protection contre les menaces les plus récentes.

Pour faciliter la fonctionnalité de mise à jour automatique, D-Link assure une infrastructure internationale de serveurs qui fournissent des services de mise à jour pour les firewalls de D-Link. Pour garantir une disponibilité et des temps de réponse courts, NetDefendOS utilise un mécanisme qui sélectionne automatiquement le serveur le plus approprié pour garantir les mises à jour.

Pour plus de détails sur ces fonctionnalités, vous pouvez consulter :

La section Prévention et détection des intrusions

La section Analyse antivirus

La section Filtrage de contenu Web

L'annexe A *Abonnement aux mises à jour de sécurité*

Configuration des sauvegardes et des restaurations

La configuration NetDefendOS d'un firewall D-Link peut être sauvegardée ou restaurée sur demande. Cela peut permettre par exemple de retrouver la « dernière configuration connue pour être bonne » lors d'essais d'autres configurations.

Exemple 2.14. Configuration des sauvegardes et des restaurations

Interface Web
Pour créer une sauvegarde de la configuration en cours d'exécution :

Sélectionnez Tools > Backup (Outils > Sauvegarde).

Téléchargez la configuration, sélectionnez un nom et commencez la sauvegarde.

Pour restaurer une configuration sauvegardée :

Sélectionnez Tools > Backup (Outils > Sauvegarde).

Dans Restore unit's configuration (Restaurer la configuration de l'unité), recherchez la sauvegarde en question.

Cliquez sur Upload configuration (Charger la configuration) et choisissez l'activation de cette configuration.

> **Remarque**
> Les sauvegardes n'incluent que les informations statiques de la configuration du firewall. Les informations dynamiques telles que l'attribution d'un serveur DHCP à une base de données ne sont pas sauvegardées.

Réinitialisation des paramètres usine par défaut

Une restauration des paramètres usine par défaut peut être appliquée pour qu'il soit possible de retourner à l'état du firewall au moment de sa livraison par D-Link. Quand une restauration est appliquée, toutes les données telles que l'IDP et les bases de données antivirus sont perdues et doivent être rechargées.

Exemple 2.15. Réinitialisation complète

Interface de ligne de commande

```
gw-world:/> reset -unit
```

Interface Web

Sélectionnez Maintenance > Reset (Réinitialiser).

Sélectionnez Restore the entire unit to factory defaults (Restaurer l'unité entière aux paramètres usine par défaut), puis confirmez et attendez la fin de la restauration.

Réinitialisation des options du DFL-210/260/800/860 uniquement. Pour réinitialiser le DFL-210/260/800/860, vous devez maintenir appuyé le bouton situé sur le panneau arrière pendant 10 à 15 secondes lors de la mise sous tension de l'unité. Relâchez ensuite le bouton de réinitialisation. Le DFL-210/800 continue le chargement et démarre en mode par défaut, c'est-à-dire avec 192.168.1.1 dans l'interface LAN.

Réinitialisation des options du DFL-1600 et du DFL-2500 uniquement. Appuyez sur n'importe quelle touche du clavier quand le message Press keypad to Enter Setup (Appuyez sur une touche pour entrer dans le menu de configuration) s'affiche. Sélectionnez Reset firewall (Réinitialiser le firewall), confirmez par Yes (Oui), et attendez la fin du processus.

> **Avertissement**
> N'INTERROMPEZ JAMAIS LE PROCESSUS DE RÉINITIALISATION DES PARAMÈTRES USINE PAR DÉFAUT. En cas d'abandon, le firewall de D-Link peut cesser de fonctionner correctement.

Chapitre 3. Fondamentaux

Le présent chapitre décrit les objets logiques fondamentaux qui forment NetDefendOS. Ces objets sont notamment de type adresse, service et programmation. De plus, le présent chapitre explique le mode de fonctionnement des différentes interfaces prises en charge. Il décrit la façon dont les règles de sécurité sont établies et dont les paramètres système de base sont configurés.

Carnet d'adresses

Présentation

Le carnet d'adresses contient des objets nommés qui représentent différents types d'adresses (IP, réseau et Ethernet MAC).

L'utilisation des objets du carnet d'adresses offre trois avantages distincts. Elle augmente la lisibilité, réduit le risque de saisir des adresses réseau incorrectes et facilite la modification des adresses. L'utilisation des objets à la place des adresses numériques vous permet d'effectuer des modifications à un seul emplacement, plutôt que d'avoir à les faire dans chaque partie de la configuration où apparaît l'adresse.

Adresses IP

Les objets *IP Address* servent à définir des noms génériques pour différents types d'adresses IP. En fonction de la spécification de l'adresse, un objet *IP Address* peut représenter un hôte (une adresse IP unique), un réseau ou une plage d'adresses IP.

De plus, vous pouvez employer les objets *IP Address* pour spécifier les authentifiants de l'utilisateur qui seront utilisés par la suite par les différents sous-systèmes d'authentification. Pour plus d'informations, reportez-vous au *chapitre 8, Authentification de l'utilisateur*.

La liste suivante présente les différents types d'adresses qu'un objet *IP Address* peut détenir, outre le format utilisé pour représenter ce type spécifique.

Hôte
: Un hôte unique est représenté simplement par son adresse IP.
Exemple : *192.168.0.14*

Réseau IP
: Un réseau IP est représenté en utilisant le format CIDR (Classless Inter Domain Routing). CIDR utilise une barre oblique et un chiffre (0 à 32) pour indiquer la taille du réseau (masque réseau). */24* correspond à un réseau de classe C avec 256 adresses (masque réseau 255.255.255.0), */27* correspond à un réseau avec 32 adresses (masque réseau 255.255.255.224) et ainsi de suite. Les nombres 0 à 32 correspondent au nombre de binaires dans le masque réseau.

  Exemple : *192.168.0.0/24*

Plage d'adresses IP
: Une plage d'adresses IP est représentée sous la forme *a.b.c.d - e.f.g.h*. Remarque : les plages ne sont pas restreintes aux limites des masques réseau. Elles peuvent inclure toute plage d'adresses IP.

  Exemple : *192.168.0.10-192.168.0.15* représente six hôtes dans l'ordre consécutif.

Exemple 3.1. Ajout d'un hôte IP

Cet exemple ajoute l'hôte IP *wwwsrv1* avec l'adresse IP *192.168.10.16* au carnet d'adresses.

Interface de ligne de commande

```
gw-world:/> add Address IP4Address wwwsrv1 Address=192.168.10.16
```

Interface Web

Sélectionnez Objects > Address Book > Add > IP address (Objets > Carnet d’adresses > Ajouter > Adresse IP).

Spécifiez un nom convenable pour l’hôte IP, par exemple wwwwsrv1.

Saisissez *192.168.10.16* comme adresse IP.

Cliquez sur OK.

Exemple 3.2. Ajout d’un réseau IP

Cet exemple ajoute un réseau IP nommé *wwwsrvnet* avec l'adresse *192.168.10.0/24* au carnet d'adresses.

Interface de ligne de commande

```
gw-world:/> add Address IP4Address wwwsrvnet Address=192.168.10.0/24
```

Interface Web

Sélectionnez Objects > Address Book > Add > IP address (Objets > Carnet d’adresses > Ajouter > Adresse IP).

Spécifiez un nom convenable pour le réseau IP, par exemple *wwwsrvnet.*

Saisissez *192.168.10.0/24* comme adresse IP.

Cliquez sur OK.

Exemple 3.3. Ajout d’une plage d’adresses IP

Cet exemple ajoute une plage d’adresses IP allant de *192.168.10.16* à *192.168.10.21* nommée *wwwservers* :

Interface de ligne de commande

```
gw-world:/> add Address IP4Address wwwservers Address=192.168.10.16-192.168.10.21
```

Interface Web

Sélectionnez Objects > Address Book > Add > IP address (Objets > Carnet d’adresses > Ajouter > Adresse IP).

Spécifiez un nom convenable pour la plage d’adresses IP, par exemple *wwwwservers.*

Saisissez *192.168.10.16-192.168.10.21* comme adresse IP.

Cliquez sur OK.

Exemple 3.4. Suppression d’un objet *Address*

Pour supprimer un objet nommé *wwwsrv1* du carnet d’adresses, procédez comme suit :

Interface de ligne de commande

```
gw-world:/> delete Address IP4Address wwwsrv1
```

Interface Web

Sélectionnez Objects > Address Book (Objets > Carnet d’adresses).

Dans la liste, cliquez avec le bouton droit de la souris sur l’objet *Address wwwsrv1*.

Choisissez Delete (Supprimer) dans le menu

Cliquez sur OK.

Adresses Ethernet

Les objets *Ethernet Address* sont utilisés pour définir des noms génériques pour les adresses Ethernet (également connues sous le nom d'adresses MAC). Ils sont utiles, par exemple, lorsqu'on remplit la table ARP avec des entrées ARP statiques, ou pour d'autres éléments de configuration où l'on préfère utiliser des noms génériques plutôt que des adresses Ethernet numériques.
Lorsque l'on spécifie une adresse Ethernet, on doit utiliser le format *aa-bb-cc-dd-ee-ff*. Les adresses Ethernet sont donc affichées sous ce format.

Exemple 3.5. Ajout d'une adresse Ethernet

L'exemple suivant ajoute l'objet *Ethernet Address* nommé *wwwsrv1_mac* avec l'adresse MAC numérique suivante : *08-a3-67-bc-2e-f2 :*

Interface de ligne de commande

```
gw-world:/> add Address EthernetAddress wwwsrv1_mac Address=08-a3-67-bc-2e-f2
```

Interface Web

Sélectionnez Objects > Address Book > Add > Ethernet Address (Objets > Carnet d'adresses > Ajouter > Adresse Ethernet).

Spécifiez un nom convenable pour l'objet *Ethernet Address*, par exemple *wwwsrv1_mac*.

Saisissez *08-a3-67-bc-2e-f2* comme adresse MAC.

Cliquez sur OK.

Groupes d'adresses

Il est possible de regrouper les objets *Address* pour simplifier la configuration. Considérez un certain nombre de serveurs publics qui doivent être accessibles à partir d'Internet. Les serveurs possèdent des adresses IP qui ne se suivent pas et ne peuvent donc pas être référencées comme une plage d'adresses IP unique. Par conséquent, vous devez créer des objets *IP Address* individuels pour chaque serveur.

Pour ne pas avoir à gérer la création et la maintenance de règles de filtrage séparées autorisant le trafic vers chaque serveur, il est possible de créer un *Groupe d'adresses*, nommé par exemple *Webservers*, avec les hôtes de serveur Web comme membres du groupe. Vous pouvez à présent utiliser une règle unique pour ce groupe et réduire considérablement la charge de travail.

Les objets *Address Group* ne sont pas restreints à posséder des membres du même sous-type. En d'autres termes, les objets *IP host* peuvent être associés aux plages d'adresses, réseaux IP, etc. Toutes les adresses de l'ensemble des membres du groupe sont associées, ce qui engendre véritablement une union des adresses. Par exemple, un groupe contenant deux plages d'adresses IP, l'une possédant les adresses *192.168.0.10 – 192.168.0.15* et l'autre les adresses *192.168.0.14 – 192.168.0.19*, engendrera une plage d'adresses IP unique possédant les adresses *192.168.0.10 - 192.168.0.19*.

N'oubliez pas cependant que pour des raisons évidentes, vous ne pouvez pas associer les objets *IP Address* à des adresses Ethernet.

Objets *Address* générés automatiquement

Pour simplifier la configuration, plusieurs objets *Address* sont générés automatiquement lors de la première exécution du système. Ces objets sont utilisés par d'autres éléments de configuration dès le démarrage.

Les objets *Address* suivants sont générés automatiquement :

Interface Addresses (adresses des interfaces) Pour chaque interface Ethernet du système, deux objets *IP Address* sont prédéfinis, l'un pour l'adresse IP de l'interface en question et l'autre représentant le réseau local pour cette interface.

Les objets adresse IP de l'interface sont nommés *interfacename*_ip et les objets réseau, *interfacename*net. Par exemple, une interface nommée *lan* aura un objet IP

d'interface nommé *lan ip* et un objet réseau nommé *lannet*.

Default Gateway (passerelle par défaut) Un objet *IP Address* nommé *wan gw* est généré automatiquement et représente la passerelle par défaut du système. L'objet wan_gw est utilisé principalement par la table de routage, mais également par le sous-système client DHCP pour stocker les informations sur les adresses de la passerelle récupérées à partir d'un serveur DHCP. Si une adresse de passerelle par défaut a été communiquée pendant la phase d'installation, l'objet wan_gw contiendra cette adresse. Dans le cas contraire, l'objet sera laissé vide (en d'autres termes, l'adresse IP sera 0.0.0.0).

All-nets (tout réseau) L'objet adresse IP *all-nets* est initialisé à l'adresse IP 0.0.0.0/0, qui représente toutes les adresses IP possibles. Cet objet est largement utilisé tout au long de la configuration.

Services

Présentation

Un objet de service fait référence à un protocole IP spécifique avec des paramètres associés. La définition d'un service repose généralement sur l'un des protocoles principaux, tels que TCP ou UDP, avec le(s) numéro(s) de port(s) associé(s). Le service HTTP, par exemple, est défini comme celui qui utilise le protocole TCP avec le port 80 associé.

Toutefois, les objets de service ne sont en aucun cas restreints aux protocoles TCP ou UDP. Vous pouvez les utiliser pour définir des messages ICMP, tout comme n'importe quel protocole IP définissable par l'utilisateur.

Les services sont des objets passifs car ils ne peuvent eux-mêmes entreprendre aucune action dans le système. Au lieu de cela, les objets de service sont fréquemment utilisés dans les différentes règles de sécurité définies par les ensembles de règles. Une règle contenue dans l'ensemble de règles IP peut par exemple utiliser un objet de service en tant que filtre pour décider d'autoriser ou non un quelconque trafic à travers le firewall D-Link. Pour plus d'informations sur l'utilisation des objets de service avec les règles IP, reportez-vous à la section Ensemble de règles IP.

Un nombre important d'objets de service prédéfinis accompagnent NetDefendOS. Ceux-ci comportent des services courants tels que HTTP, FTP, Telnet et SSH. Les services prédéfinis peuvent être utilisés et également modifiés de la même façon que les services définis par l'utilisateur. Toutefois, il est recommandé de NE PAS modifier les services prédéfinis, mais d'en créer plutôt des nouveaux avec les paramètres désirés.

Exemple 3.6. Référencement des services disponibles

Pour effectuer un référencement des services disponibles dans le système :

Interface de ligne de commande

```
gw-world:/> show Service
```

Le résultat sera similaire à la liste suivante :

```
ServiceGroup

 Name   Comments
 ------------ --------------------------------------------------
 all_services All ICMP, TCP and UDP services
 all_tcpudp All TCP and UDP services
 ipsec-suite The IPsec+IKE suite
 l2tp-ipsec L2TP using IPsec for encryption and authentication
 l2tp-raw  L2TP control and transport, unencrypted
 pptp-suite PPTP control and transport

ServiceICMP
...
```

Interface Web

Sélectionnez Objects > Services (Objets > Services).

Exemple 3.7. Visualisation d’un service spécifique

Pour visualiser un service spécifique du système :

Interface de ligne de commande

```
gw-world:/> show Service ServiceTCPUDP echo
```

Le résultat sera similaire à la liste suivante:

```
   Property Value
 ---------------- ----------------
    Name: echo
 DestinationPorts: 7
    Type: TCPUDP (TCP/UDP)
  SourcePorts: 0-65535
 PassICMPReturn: No
    ALG: (none)
  MaxSessions: 1000
   Comments: Echo service
```

Interface Web

Sélectionnez Objects > Services (Objets > Services).

Sélectionnez l’objet de service spécifique dans la liste de contrôle.

Une liste référençant tous les services s’affiche.

Services reposant sur les protocoles TCP et UDP

La plupart des applications utilisent le TCP et/ou l’UDP comme protocoles de transport pour le transfert des données d’applications sur les réseaux IP.

Le TCP (Transmission Control Protocol) est un protocole réservé à la connexion qui inclut, entre autres, des mécanismes garantissant une transmission fiable des données. Le TCP est utilisé par un grand nombre d’applications courantes telles que HTTP, FTP et SMTP, où les transferts exempts d’erreur sont obligatoires.

Pour d’autres types d’applications, tels que les services de diffusion audio et vidéo en continu, où l’on accorde par exemple une grande importance aux performances, on préfèrera utiliser le protocole UDP (User Datagram Protocol). L’UDP est un protocole sans connexion, qui propose très peu de services de récupération d’erreur et entraîne ainsi une surcharge du trafic bien plus faible que le TCP. Pour cette raison, l’UDP est également utilisé pour les services de non-diffusion en continu et il est courant dans ces cas-là que les applications fournissent elles-mêmes les mécanismes de récupération d’erreur.

Pour définir un service TCP ou UDP dans le firewall D-Link, on utilise un objet *Service TCP/UDP*. Ce type d’objet contient, outre un nom unique qui décrit le service, des informations sur le type de protocole (TCP et/ou UDP) et le type de ports source et de destination qui peuvent s’appliquer à ce service.

Les numéros de ports peuvent être spécifiés de différentes manières :

Single Port (port unique)	Pour un grand nombre de services, un seul port de destination suffit. Le protocole HTTP, par exemple, utilise le port de destination 80 dans la plupart des cas. SMTP utilise le port 25, et ainsi de suite. Pour ces types de services, le numéro de port unique est simplement spécifié dans l’objet Service TCP/UDP.
Port Ranges (plages de ports)	Certains services utilisent une plage de ports de destination. Par exemple, le protocole NetBIOS utilisé par Microsoft Windows utilise les ports de destination 137 à 139. Pour définir une plage de ports dans un objet Service TCP/UDP, on utilise le format *mmm-nnn*. Une plage de ports est inclusive, ce qui signifie qu'une plage définie sur 137 à 139 couvre les ports 137, 138 et 139.

Multiple Ports and Port Ranges (ports multiples et plages de ports) Il est également possible de saisir des plages multiples ou des ports individuels, séparés par des virgules. Cela permet de couvrir une vaste plage de ports en n'utilisant qu'un seul objet Service TCP/UDP. Il est, par exemple, possible de couvrir l'ensemble du réseau Microsoft Windows en utilisant la définition de port suivante : 135-139,445. Vous pouvez couvrir HTTP et HTTPS en définissant les ports de destination sur 80,443.

Conseil

Les méthodes de spécification des numéros de ports ci-dessus ne sont pas utilisées uniquement pour les ports de destination. Les définitions de ports source peuvent suivre les mêmes conventions, bien que, généralement, ces derniers soient laissés sur la valeur par défaut 0-65535, qui correspond à tous les ports source possibles.

Exemple 3.8. Ajout d'un Service TCP/UDP

Cet exemple montre comment ajouter un Service TCP/UDP en se servant du port de destination 3306 utilisé par MySQL.

Interface de ligne de commande

```
gw-world:/> add Service ServiceTCPUDP MySQL DestinationPorts=3306 Type=TCP
```

Interface Web

Sélectionnez Objects > Services > Add > TCP/UDP service (Objets > Services > Ajouter > Service TCP/UDP).

Spécifiez un nom convenable pour le service, par exemple *MySQL*.

A présent, saisissez :

Type : TCP

Source : 0-65535

Destination : 3306

Cliquez sur OK.

Outre les informations sur le protocole et le port, les objets de service TCP/UDP contiennent également plusieurs autres paramètres décrits plus en détail dans les autres sections du présent guide de l'utilisateur.

SYN Flood Protection (protection SYN-Flood) Vous pouvez configurer un service TCP pour activer la protection contre les attaques *SYN Flood*. Pour plus de détails sur le fonctionnement de cette fonctionnalité, reportez-vous à la section intitulée « Attaques TCP-SYN-Flood ».

Passing ICMP Errors (ignorer les erreurs ICMP) Si une application utilisateur tente d'ouvrir une connexion TCP derrière le firewall D-Link et que le serveur distant n'est pas actif, un message d'erreur ICMP s'affiche en réponse. Vous pouvez soit ignorer ces erreurs ICMP, soit les autoriser à passer et à retourner vers l'application concernée.

Passerelle ALG (Application Layer Gateway) Vous pouvez rattacher un Service TCP/UDP à une *passerelle ALG* pour activer une inspection approfondie de certains protocoles. Pour plus d'informations, reportez-vous à la section intitulée « Passerelles ALG ».

Max Sessions (sessions maximum). Un paramètre important associé à un Service est le paramètre *Max Sessions (sessions maximum)*. Ce paramètre se voit attribuer une valeur par défaut lorsque le service est associé à une passerelle ALG. La valeur par défaut varie selon la passerelle ALG à laquelle elle est associée. Si la valeur par défaut est 100, cela signifie que seulement 100 connexions sont autorisées au total pour ce service à travers toutes les interfaces.

Pour un service comprenant, par exemple, une passerelle ALG HTTP, la valeur par défaut peut souvent être trop faible si un grand nombre de clients se connectent via le firewall D-Link. Il est par conséquent recommandé d'estimer si une valeur supérieure est exigée pour un cas de figure particulier.

Utilisation de « All Services » (tous les services). Au moment de la configuration des règles de filtrage par service, il est possible d'utiliser le service « grouping_all services » pour se référer à tous les protocoles. Pour se référer uniquement aux protocoles principaux (TCP, UDP et ICMP), on peut utiliser le service « group all_tcpundpicmp ».

Services ICMP

Internet Control Message Protocol (ICMP) est un protocole intégré au protocole IP pour le rapport d'erreurs et la transmission des paramètres de contrôle. Le service PING utilise par exemple ICMP pour tester la connexion Internet.

Le message ICMP est distribué en paquets IP et comporte un *Type de message* qui spécifie le type, c'est-à-dire le format du message ICMP et un *Code* utilisé pour la désignation du message. Le type de message *Destination Unreachable (destination injoignable)* utilise par exemple le paramètre Code pour spécifier la cause exacte de l'erreur.

Les types de messages ICMP que vous pouvez configurer dans NetDefendOS sont répertoriés ci-dessous :

Echo Request (message d'écho) : envoyé par le protocole PING en direction d'une destination pour vérifier la connectivité.

Destination Unreachable (destination injoignable) : la source est informée qu'un problème est survenu lors de la remise du paquet. Il existe des codes allant de 0 à 5 pour ce type :

Code 0 : Net Unreachable (réseau injoignable)

Code 1 : Host Unreachable (hôte injoignable)

Code 2 : Protocol Unreachable (protocole injoignable)

Code 3 : Port Unreachable (port injoignable)

Code 4 : Cannot Fragment (fragmentation impossible)

Code 5 : Source Route Failed (échec de la route source)

Redirect (redirection) : la source est informée qu'une meilleure route existe pour un paquet donné. Les codes assignés sont les suivants :

Code 0 : Redirect datagrams for the network (redirection des datagrammes pour le réseau)

Code 1 : Redirect datagrams for the host (redirection des datagrammes pour l'hôte)

Code 2 : Redirect datagrams for the Type of Service and the network (redirection des datagrammes pour le type de service et le réseau)

Code 3 : Redirect datagrams for the Type of Service and the host (redirection des datagrammes pour le type de service et l'hôte)

Parameter Problem (problème de paramètre) : identifie un paramètre incorrect sur le datagramme.

Echo Reply (réponse à écho) : réponse provenant de la destination, envoyée comme message de réponse à écho.

Source Quenching (extinction de la source) : la source envoie les données trop rapidement pour le récepteur, la mémoire tampon est pleine.

Time Exceeded (temps dépassé) : le paquet a été rejeté car il a mis trop de temps à être transmis.

Services de Protocole IP personnalisés

Les services qui fonctionnent sur le protocole IP et qui assurent les fonctions de la couche d'applications/de transport peuvent être affectés d'un identifiant unique grâce aux *numéros de protocoles IP*. Le protocole IP peut transporter des données pour un certain nombre de protocoles différents. Chacun d'entre eux est identifié par un numéro de protocole IP unique spécifié dans un champ se trouvant dans l'en-tête de l'IP. Par exemple, ICMP, IGMP et EGP possèdent respectivement les numéros de protocoles 1,2 et 8.

NetDefendOS prend en charge ces types de protocoles IP en utilisant le concept de *Services de Protocole IP personnalisés.* Un service de protocole IP personnalisé est une définition de service qui donne un nom à un numéro de protocole IP. Certains des protocoles IP courants, tels que IGMP, sont déjà prédéfinis dans la configuration système de NetDefendOS.

Vous pouvez utiliser une plage de numéros de protocoles IP semblable aux plages de ports TCP/UDP décrites précédemment pour spécifier de multiples applications pour un seul service.

Remarque

Les numéros de protocoles IP affectés actuellement ainsi que les références sont publiées par l'IANA (Internet Assigned Numbers Authority) et peuvent être consultées à l'adresse suivante : http://www.iana.org/assignments/protocol-numbers.

Exemple 3.9. Ajout d'un service de protocole IP

Cet exemple montre comment ajouter un service de protocole IP à l'aide du Virtual Router Redundancy Protocol (protocole de redondance de routeur virtuel, VRRP).

Interface de ligne de commande

```
gw-world:/> add Service ServiceIPProto VRRP IPProto=112
```

Interface Web

Sélectionnez Objects > Services > Add > IP protocol service (Objets > Services > Ajouter > Service de protocole IP).

Spécifiez un nom convenable pour le service, par exemple *VRRP*.

Saisissez 112 dans le contrôle de protocole IP.

Si nécessaire, saisissez *Virtual Router Redundancy Protocol* dans le contrôle des commentaires.

Cliquez sur OK.

Interfaces

Présentation

Une interface est l'un des plus importants blocs logiques de NetDefendOS. L'ensemble du trafic réseau qui traverse le système ou qui s'interrompt dans celui-ci s'effectue à travers une ou plusieurs interfaces.

Une interface peut être considérée comme un passage pour le trafic réseau, vers ou en provenance du système. Donc, lorsque le trafic pénètre le système par une interface, on l'appellera interface *réceptrice* (ou parfois interface *d'entrée*). Par conséquent, lorsque le trafic quitte le système, l'interface utilisée pour expulser le trafic est appelée interface *d'envoi* (ou parfois interface *de sortie*).

NetDefendOS prend en charge un certain nombre de types d'interfaces qui peuvent être réparties en quatre grands groupes, comme suit :

Interfaces physiques

Chaque *interface physique* représente un port physique dans un produit NetDefendOS. L'ensemble du trafic réseau qui émane du système ou qui s'interrompt dans celui-ci traversera donc en fin de compte l'une des interfaces physiques.

Ethernet est le seul type d'interface physique actuellement pris en charge par

NetDefendOS. Pour plus d'informations sur les interfaces Ethernet, reportez-vous à la section intitulée « Ethernet ».

Sous-interfaces physiques

Certaines interfaces nécessitent une mise en association avec une interface physique sous-jacente pour transférer des données. Ce groupe d'interfaces est appelé *Sous-interfaces physiques.*

NetDefendOS prend en charge deux types de sous-interfaces physiques:

Les interfaces VLAN (*Virtual LAN*), comme spécifié par la norme IEEE 802.1Q. Si vous routez des paquets IP via une interface VLAN, ils seront encapsulés dans des trames Ethernet balisées VLAN. Pour plus d'informations sur les interfaces Ethernet, reportez-vous à la section intitulée « VLAN ».

Interfaces *PPPoE* (PPP-over-Ethernet) pour les connexions aux serveurs PPPoE. Pour plus d'informations sur les interfaces PPPoE, reportez-vous à la section intitulée « PPPoE ».

Interfaces tunnels

Les *interfaces tunnels* sont utilisées lorsque le trafic réseau est acheminé par un tunnel qui relie le système et l'autre extrémité du tunnel dans le réseau, avant qu'il soit routé vers sa destination finale.

Pour réaliser la tunnelisation, des en-têtes supplémentaires sont ajoutés au trafic acheminé par le tunnel. De plus, diverses transformations peuvent être appliquées au trafic réseau en fonction du type d'interface tunnel. Lorsque le trafic est routé via une interface IPsec par exemple, la charge utile est généralement chiffrée pour garantir la confidentialité.

NetDefendOS prend en charge les types d'interfaces tunnels suivantes :

Les interfaces *IPsec* sont utilisées comme extrémités pour les tunnels VPN IPsec. Pour plus d'informations sur les interfaces VPN IPsec, reportez-vous à la section intitulée « IPsec ».

Les interfaces *PPTP/L2TP* sont utilisées comme extrémités pour les tunnels PPTP ou L2TP. Pour plus d'informations sur les interfaces PPTP/L2TP, reportez-vous à la section intitulée « PPTP/L2TP ».

Les interfaces *GRE* sont utilisées pour établir des tunnels GRE. Pour plus d'informations sur les interfaces GRE, reportez-vous à la section intitulée « Tunnels GRE ».

Même si les divers types d'interfaces sont très différents dans la manière dont ils sont déployés et la manière dont ils fonctionnent, NetdefendOS considère toutes les interfaces comme des interfaces IP logiques. En d'autres termes, tous les types d'interfaces peuvent être utilisées pratiquement de manière interchangeable dans les différents sous-systèmes et règles. Il en résulte une très grande fiabilité dans le mode de contrôle et de routage du trafic dans le système.

Chaque interface de NetDefendOS se voit attribuer un nom unique pour qu'elle puisse être sélectionnée dans d'autres sous-systèmes. Certains types d'interfaces proposent des noms adaptés par défaut qu'il est possible de modifier si nécessaire, tandis que d'autres types d'interfaces nécessitent un nom défini par l'utilisateur.

Avertissement

Si la définition d'une interface est supprimée de la configuration de NetDefendOS, il est important de commencer par supprimer ou modifier toutes les références à cette interface. Il est conseillé, par exemple, de supprimer ou de modifier les règles contenues dans l'ensemble de règles IP qui font référence à cette interface.

Les interfaces *core* et *any*. De plus, NetDefendOS propose deux interfaces logiques spéciales nommées core et any :

any représente toute les interfaces possibles, y compris les interfaces core

core indique que c'est NetDefendOS lui-même qui se chargera du trafic. Core est par exemple utilisé lorsque le firewall D-Link fonctionne en tant que serveur PPTP ou L2TP ou doit répondre aux requêtes ping ICMP. Si vous définissez l'interface de destination d'une route en tant que *core*, NetDefendOS saura qu'il est lui-même le récepteur final du trafic.

Ethernet

La norme Ethernet IEEE 802.3 permet de raccorder différents périphériques au niveau de points arbitraires ou « ports » à un mécanisme de transport physique (un câble coaxial, par exemple). Avec le protocole CSMA/CD, chaque périphérique connecté par le biais d'Ethernet « écoute » le réseau et envoie des données à un autre périphérique connecté alors qu'aucun autre envoi de données n'est en cours. Si deux périphériques diffusent simultanément, des algorithmes leur permettent de renvoyer les données à différents moments. Les périphériques diffusent des données sous forme de trames et les autres périphériques « écoutent » pour déterminer s'ils sont les destinataires visés par une de ces trames.

Une trame est une suite de bits qui définit le périphérique source et de destination, le flux de données ainsi que les bits de vérification d'erreur. Une pause entre la diffusion de trames individuelles donne du temps aux périphériques pour traiter chaque trame avant l'arrivée de la suivante. Cette pause se réduit progressivement au fur et à mesure que les taux de transmission augmentent, passant de normal à rapide puis à une transmission Ethernet Gigabit.

Chaque interface Ethernet d'un firewall D-Link correspond à un port Ethernet physique du système. Le nombre de ports, leur vitesse de liaison et la façon dont les ports sont mis en place dépend du modèle de matériel.

Remarque

Certains systèmes utilisent un switch de couche 2 pour fournir des ports physiques Ethernet supplémentaires. Ces ports supplémentaires sont considérés comme une interface unique par NetDefendOS.

Noms des interfaces Ethernet. Les noms des interfaces Ethernet sont prédéfinis par le système et sont calqués sur les noms des ports physiques ; un système possédant un port *wan* aura une interface Ethernet nommée wan et ainsi de suite.

Vous pouvez modifier les noms des interfaces Ethernet pour mieux traduire leur utilisation. Par exemple, si une interface nommée *dmz* est connectée à un réseau local (LAN) sans fil, il peut être pratique de renommer cette interface *radio*. Pour la maintenance et la résolution des problèmes, il est recommandé de baliser le port physique correspondant avec le nouveau nom.

Remarque

Le processus de démarrage va énumérer toutes les interfaces Ethernet disponibles. Chaque interface se verra attribuer un nom de la forme *lanN, wanN et dmz*, où N représente le numéro de l'interface si votre firewall D-Link possède plusieurs de ces interfaces. Dans la plupart des exemples de ce guide, « lan » désigne le trafic LAN et « wan » le trafic WAN. Si votre firewall D-Link ne possède pas ces interfaces, remplacez ces références par le nom de l'interface choisie.

Adresses IP Ethernet. Chaque interface Ethernet doit posséder une *Adresse IP Ethernet*, qui peut être soit une adresse statique, soit une adresse fournie par DHCP. L'adresse IP de l'interface est utilisée comme adresse principale pour communiquer avec le système à travers l'interface Ethernet spécifique.

La norme consiste à utiliser les objets adresse IP4 pour définir les adresses des interfaces Ethernet. Ces objets sont normalement générés automatiquement par le système. Pour plus d'informations, reportez-vous à la section intitulée « Objets adresse générés automatiquement ».

Conseil

Vous pouvez spécifier plusieurs adresses IP pour une interface Ethernet en utilisant la fonctionnalité ARP Publish (publication ARP). Pour plus d'informations, reportez-vous à la section intitulée « ARP ».

En plus des adresses IP de l'interface, une adresse *réseau* est également spécifiée pour l'interface Ethernet. L'adresse réseau fournit des informations à NetDefendOS concernant les adresses IP accessibles directement par l'interface, en d'autres termes celles qui résident sur le même segment LAN que l'interface elle-même. Dans la table de routage associée à l'interface, NetDefendOS va créer automatiquement une route directe vers le réseau

spécifié via l'interface en question.
La passerelle par défaut. Si nécessaire, vous pouvez spécifier une adresse de *passerelle par défaut* pour une interface Ethernet. Ce paramètre indique à NetDefendOS comment atteindre les hôtes pour lesquels il n'existe pas aucune route. En d'autres termes, si une adresse de passerelle par défaut a été spécifiée, NetDefendOS va créer automatiquement une route par défaut (réseau de destination *tout réseau*) via l'interface en question en utilisant la passerelle spécifiée. Pour des raisons évidentes, vous ne pouvez affecter qu'une seule interface Ethernet à la fois comme passerelle par défaut.
Utilisation de DHCP sur les interfaces Ethernet. NetDefendOS comprend un client DHCP pour l'affectation dynamique des informations d'adresse. Les informations qui peuvent être définies via DHCP comportent les adresses IP de l'interface, le réseau local auquel est connectée l'interface et la passerelle par défaut.

Toutes les adresses reçues du serveur DHCP sont affectées aux objets adresse IP4 correspondants. De cette manière, vous pouvez utiliser les adresses affectées de manière dynamique de la même manière que les adresses statiques dans l'ensemble de la configuration. Par défaut, les objets utilisés sont les mêmes que ceux définis dans la section intitulée « Objets adresse générés automatiquement ».

Exemple 3.10. Activation de DHCP

Interface de ligne de commande

```
gw-world:/> set Interface Ethernet wan DHCPEnabled=Yes
```

Interface Web

Sélectionnez Interfaces > Ethernet.

Dans la liste, cliquez sur l'objet Ethernet souhaité.

Activez l'option Enable DHCP client (Activer le client DHCP).

Cliquez sur OK.

VLAN

Présentation. Les VLAN (*Virtual LAN*) sont utiles dans plusieurs cas de figure, par exemple, lorsque le filtrage du trafic est nécessaire entre différents VLAN d'une organisation, ou pour toute autre raison, lorsque l'administrateur souhaite augmenter le nombre d'interfaces.

La prise en charge de VLAN par NetDefendOS permet de définir une ou plusieurs *interfaces VLAN* qui seront associées à une interface physique donnée. Celles-ci seront considérées comme des interfaces logiques par NetDefendOS et pourront être traitées comme des interfaces physiques dans les ensembles de règles et les tables de routage.

Fonctionnement VLAN. NetDefendOS est conforme à la norme IEEE 802.1Q relative aux réseaux VLAN. En ce qui concerne le protocole, VLAN fonctionne en ajoutant un ID de VLAN (*Virtual LAN Identifier*) aux en-têtes de trames Ethernet. L'ID du VLAN est un nombre compris entre 0 et 4095 utilisé pour identifier le VLAN spécifique auquel appartient la trame. De cette manière, les trames Ethernet peuvent appartenir à différents VLAN, tout en continuant à partager la même interface physique. Avec NetDefendOS, l'ID du VLAN doit être unique pour l'interface physique et le même ID de VLAN peut être utilisé sur différentes interfaces physiques.

Les paquets reçus à travers les trames Ethernet par une interface physique de NetDefendOS sont examinés pour rechercher un ID de VLAN. Si un ID de VLAN valide est trouvé et qu'une interface VLAN correspondante a été définie pour cette interface, NetDefendOS utilisera l'interface VLAN comme interface source lors du traitement ultérieur avec les ensembles de règles IP.

Si aucun ID de VLAN valide n'est associé à une trame Ethernet reçue par l'interface physique, alors la trame est considérée comme étant reçue par l'interface physique et non par une quelconque interface VLAN pouvant être définie.
Limitations de licence. Le nombre d'interfaces VLAN pouvant être défini pour une installation NetDefendOS est limité par les paramètres de la licence utilisée. Les différents modèles matériels possèdent différentes licences et différentes limitations de VLAN.

Résumé de l'installation du VLAN. Il est important de comprendre que l'administrateur doit considérer une interface VLAN de la même façon qu'une interface physique dans le sens où celles-ci requièrent au moins des règles IP et des routes pour être définies et être capables de fonctionner. Si, par exemple, aucune règle Allow (Autoriser) n'est définie dans l'ensemble de règles IP pour une interface VLAN, alors les paquets qui arrivent sur cette interface seront ignorés. Pour configurer une interface VLAN, procédez comme suit :

Attribuez un nom à l'interface VLAN.

Sélectionnez l'interface physique pour le VLAN.

Attribuez un ID de VLAN unique sur l'interface physique.

Si nécessaire, précisez une adresse IP pour le VLAN.

Si nécessaire, précisez une adresse IP de diffusion pour le VLAN.

Créez la(les) route(s) pour le VLAN dans la table de routage appropriée.

Créez des règles dans l'ensemble de règles IP pour autoriser le trafic à traverser l'interface VLAN.

Exemple 3.11. Définition d'un VLAN

Cet exemple simple définit un VLAN nommé *VLAN10* avec l'ID de VLAN *10*. Notez que cette interface de VLAN utilisera l'adresse IP de l'interface Ethernet correspondante, car aucune adresse IP n'est spécifiée.

Interface de ligne de commande

```
gw-world:/> add Interface VLAN VLAN10 Ethernet=lan Network=all-nets VLANID=10
```

Interface Web

Sélectionnez Interfaces > VLAN > Add > VLAN (Interfaces > VLAN > Ajouter > VLAN).

Saisissez un nom convenable pour le VLAN (dans notre exemple, *VLAN10).*

A présent, saisissez :

Interface : lan

VLAN ID (ID du VLAN) : 10

Cliquez sur OK.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) est un protocole de tunnelisation utilisé pour connecter à Internet plusieurs utilisateurs d'un réseau Ethernet par une interface série commune, telle qu'une ligne DSL unique, un périphérique sans fil ou un modem câble. Tous les utilisateurs d'Ethernet partagent une connexion commune, tandis que le contrôle d'accès peut être effectué en fonction des utilisateurs.

Les FAI demandent souvent aux clients de se connecter à leur service haut débit par PPPoE. En utilisant PPPoE, le fournisseur peut :

mettre en œuvre des contrôles de sécurité et d'accès en utilisant l'authentification par nom d'utilisateur/mot de passe ;

associer les adresses IP à un utilisateur spécifique ;

attribuer automatiquement des adresses IP aux utilisateurs PC (similaire à DHCP). La fourniture d'adresses IP peut se faire par groupe d'utilisateurs.

Présentation de PPP

PPP (Point-to-Point Protocol) est un protocole de communication entre deux ordinateurs qui utilisent une interface série (cas d'un ordinateur personnel connecté sur une ligne téléphonique commutée à un FAI, par exemple). Concernant le modèle OSI, PPP propose un mécanisme d'encapsulation de couche 2 pour autoriser les paquets de n'importe quel protocole à voyager à travers les réseaux IP. PPP utilise le protocole LCP (Link Control Protocol) pour établir des connexions, ainsi que pour la configuration et les tests. Une fois le LCP initialisé, un ou plusieurs NCP (Network Control Protocols) peuvent être utilisés pour transporter du trafic pour une suite de protocoles donnée, de sorte que des protocoles multiples puissent être reliés par la même connexion. Par exemple, les trafics IP et IPX peuvent tous deux partager une liaison PPP.

L'authentification est une option de PPP. Les protocoles d'authentification pris en charge sont : PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) et Microsoft CHAP (versions 1 et 2). Lorsque l'on utilise un protocole d'authentification, au moins l'un des nœuds doit s'authentifier avant que les paramètres de la couche réseau puissent être négociés à l'aide de NCP. Pendant la négociation LCP et NCP, des paramètres optionnels tels que le chiffrement peuvent également être négociés.

Configuration du client PPPoE

L'interface PPPoE. Puisque le protocole PPPoE exécute PPP via Ethernet, le firewall a besoin d'utiliser l'une des interfaces Ethernet normales pour exécuter PPPoE via celle-ci. Chaque tunnel PPPoE est considéré comme une interface logique par NetDefendOS, avec les mêmes capacités de routage et de configuration que les interfaces habituelles, l'ensemble de règles IP étant appliqué à la totalité du trafic. Le trafic réseau qui arrive vers le firewall à travers le tunnel PPPoE utilisera l'interface tunnel PPPoE comme interface source. L'interface tunnel PPPoE sera l'interface de destination pour le trafic sortant. Comme avec toute interface, une ou plusieurs routes sont définies de telle sorte que NetDefendOS puisse identifier les adresses IP en provenance desquelles il doit accepter le trafic et vers lesquelles il doit envoyer le trafic par le tunnel PPPoE. Vous pouvez configurer le client PPPoE de manière à utiliser un nom de service permettant de distinguer les différents serveurs sur le même réseau Ethernet.

Informations relatives à l'adresse IP. PPPoE utilise l'attribution automatique des adresses IP, comme le protocole DHCP. Lorsque NetDefendOS reçoit ces informations relatives à l'adresse IP de la part du FAI, il les stocke dans un objet réseau et les utilise en tant qu'adresse IP de l'interface.

Authentification utilisateur. Si le FAI exige une authentification utilisateur, vous pouvez configurer le nom d'utilisateur et le mot de passe dans NetDefendOS pour un envoi automatique en direction du serveur PPPoE.

Connexion à la demande. Si la connexion à la demande est activée, la connexion PPPoE sera uniquement opérationnelle lorsqu'il y aura du trafic sur l'interface PPPoE. Il est possible de configurer la façon dont le firewall détecte une activité sur l'interface, sur le trafic sortant, le trafic entrant ou les deux. Vous pouvez également configurer la durée d'inactivité avant la déconnexion du tunnel.

Exemple 3.12. Configuration d'un client PPPoE sur l'interface WAN avec routage du trafic via PPPoE

Interface de ligne de commande

```
gw-world:/> add Interface PPPoETunnel PPPoEClient EthernetInterface=wan
   Network=all-nets Username=exampleuser Password=examplepw
```

Interface Web

Sélectionnez Interfaces > PPPoE > Add > PPoE Tunnel (Interfaces > PPPoE > Ajouter > Tunnel PPoE).

Saisissez :

Name (nom) : PPPoEClient (client PPPoE)

Physical Interface (interface physique) : wan

Remote Network (réseau distant) : all-nets (tout-réseau, car l'ensemble du trafic sera routé vers le tunnel)

Service Name (nom du service) : nom de service communiqué par le fournisseur d'accès

Username (nom d'utilisateur) : nom d'utilisateur communiqué par le fournisseur d'accès

Password (mot de passe) : mot de passe communiqué par le fournisseur d'accès

Confirm Password (confirmer le mot de passe) : Retype the password (retapez le mot de passe)
Dans le menu Authentication (authentification), précisez quel protocole d'authentification vous souhaitez utiliser
(s'il n'est pas spécifié, le paramètre par défaut sera utilisé)

Désactivez l'option Enable dial-on-demand (Activer la connexion à la demande)

Dans le menu Advanced (Avancé), si l'option Add route for remote network (Ajouter une route pour le réseau distant) est activée, alors une nouvelle route sera ajoutée pour l'interface

Cliquez sur OK.

Remarque

Pour garantir une connexion point-à-point via Ethernet, chaque session PPP doit connaître l'adresse Ethernet du nœud distant et créer un identifiant de session unique. PPPoE intègre un protocole de détection qui permet ce processus.

Tunnels GRE

Présentation. Le protocole GRE *(Generic Router Encapsulation)* est un simple protocole d'encapsulation qui peut être utilisé chaque fois qu'il est nécessaire d'acheminer le trafic par un tunnel à travers les réseaux et/ou via des périphériques réseau. Le protocole GRE ne propose pas de fonctions de sécurité, mais son utilisation provoque ainsi une surcharge extrêmement faible.

Utilisation du protocole GRE. Le protocole GRE est généralement utilisé pour offrir une méthode permettant de connecter ensemble deux réseaux à travers un troisième réseau tel que Internet. Les deux réseaux reliés communiquent par un protocole commun qui est acheminé par tunnel grâce au protocole GRE par le réseau intermédiaire. Exemples d'utilisation du protocole GRE :

Pour passer à travers un équipement réseau qui bloque un protocole donné.

Pour la tunnelisation du trafic IPv6 via un réseau IPv4.

Lorsqu'un flux de données UDP doit faire l'objet d'un envoi en multidiffusion et qu'il est nécessaire de passer par un périphérique réseau qui ne prend pas en charge la multidiffusion. Le protocole GRE autorise la tunnelisation via le périphérique réseau.

Sécurité et performances du protocole GRE. Un tunnel GRE n'utilise pas de chiffrement pour communiquer et n'est donc pas, par définition, sécurisé. La sécurité doit être assurée par le protocole acheminé par tunnel. L'avantage de ce défaut de chiffrement du protocole GRE sont les hautes performances garanties par la faible surcharge lors du traitement du trafic. Le défaut de chiffrement peut être acceptable dans certaines circonstances si la tunnelisation est effectuée à travers un réseau interne qui n'est pas public.
Configuration du protocole GRE. Comme certains autres tunnels de NetDefendOS tels que le tunnel IPsec, un tunnel GRE est considéré comme une interface logique par NetDefendOS, avec les mêmes capacités de filtrage, de mise en forme du trafic et de configuration qu'une interface standard. Les options du protocole GRE sont :

Adresse IP : adresse IP de l'interface d'envoi. Cette information est facultative et peut rester vide. Si elle est vide, l'adresse IP source sera l'adresse de l'hôte local par défaut : 127.0.0.1.

Réseau à distance : réseau distant auquel sera connecté le tunnel GRE.

Extrémité distante : adresse IP du périphérique distant auquel sera connecté le tunnel.

Utilisation d'une clé de session : si nécessaire, vous pouvez spécifier un numéro unique pour ce tunnel. Ce paramètre autorise plusieurs tunnels GRE à fonctionner entre deux extrémités identiques. La variable *clé de session* permet de les différencier.

Total de contrôle d'encapsulation supplémentaire : le protocole GRE permet un total de contrôle supplémentaire au-delà du total de contrôle IPv4. Cela permet une vérification supplémentaire de l'intégrité des données.

Les paramètres avancés d'une interface GRE sont :

Ajouter automatiquement une route pour un réseau distant : on vérifiera généralement cette option pour que la table de routage soit mise à jour automatiquement. Une solution alternative consiste à créer manuellement la route souhaitée.

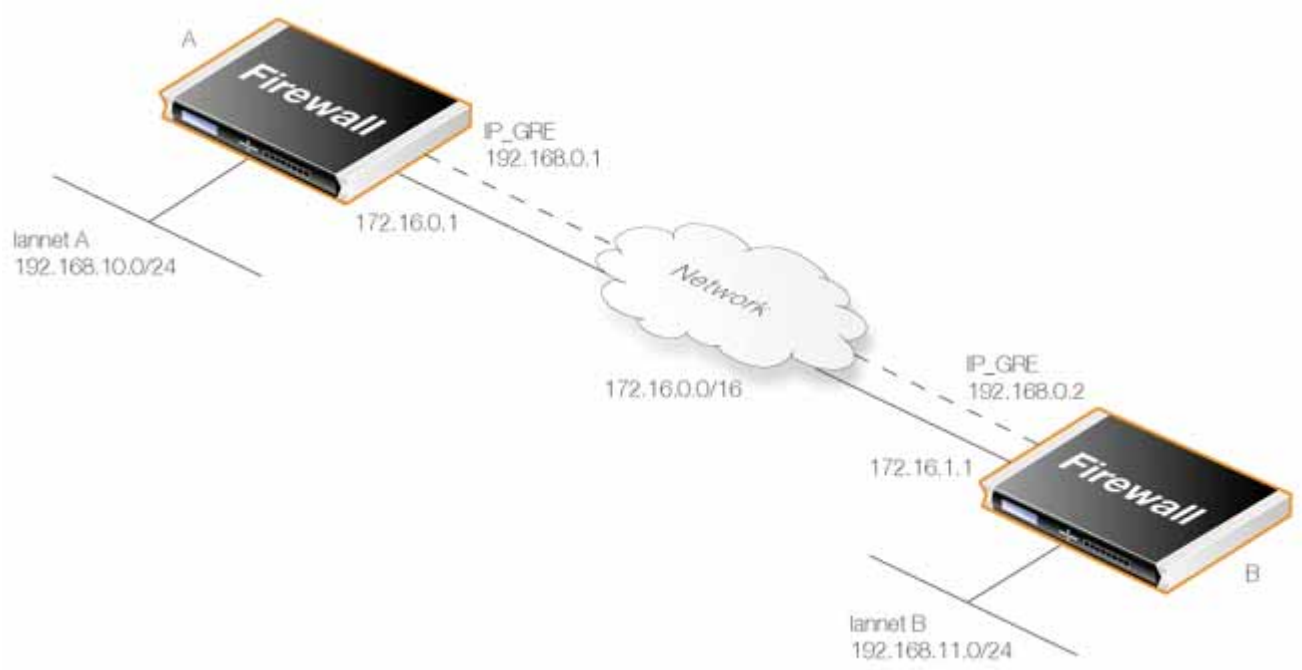
Adresse à utiliser comme IP source : il est possible de spécifier une adresse IP particulière en tant qu'IP de l'interface source pour le tunnel.

Ensemble de règles IP et GRE. Un tunnel GRE établi ne signifie pas automatiquement que l'ensemble du trafic en provenance ou à destination de ce tunnel est autorisé. Bien au contraire, le trafic réseau en provenance du tunnel GRE sera transféré vers l'ensemble de règles IP de NetDefendOS pour être évalué. Le tunnel GRE associé portera le nom de l'interface source du trafic réseau. Ceci est également valable pour le trafic en direction opposée, c'est-à-dire en direction d'un tunnel GRE. De plus, il faut définir une route pour que NetDefendOS identifie les adresses IP qui doivent être acceptées et envoyées par le tunnel.

Exemple de cas de figure GRE. Le schéma ci-dessous illustre un cas de figure GRE type, où deux firewalls D-Link A et B doivent communiquer l'un avec l'autre à travers le réseau interne intermédiaire *172.16.0.0/16*.

Tout le trafic transitant entre A et B est acheminé par tunnel à travers le réseau intermédiaire au moyen d'un tunnel GRE. Le réseau étant interne et non public, aucun chiffrement n'est requis.

Figure 3.1. Exemple de cas de figure GRE



Configuration du firewall D-Link « A ». En supposant que le réseau *192.168.10.0/24* est un réseau lannet sur l'interface lan, voici les étapes de configuration de NetDefendOS sur le firewall A :

Dans le carnet d'adresses, configurez les objets IP suivants :

remote_net_B: 192.168.11.0/24

remote_gw: 172.16.1.1

ip_GRE: 192.168.0.1

Créez un objet tunnel GRE nommé GRE_to_B ayant les paramètres suivants :

Adresse IP : ip_GRE:

Réseau distant : remote_net_B:

Extrémité distante : remote_gw:

Utilisation d'une clé de session : 1

Total de contrôle d'encapsulation supplémentaire : activé

Définissez une route dans la table de routage *principale* qui achemine l'ensemble du trafic vers remote_net_B sur l'interface GRE GRE_to_B. Cette opération n'est pas nécessaire si l'option Add route for remote network (Ajouter une route pour un réseau distant) est activée dans l'onglet Advanced (Avancé), car la route sera alors ajoutée automatiquement.

Créez les règles suivantes dans l'ensemble de règles IP, qui autorisent le trafic à traverser le tunnel :

Nom	Action	Interface src	Réseau src	Interface de dest.	Réseau de dest.	Service
To_B	Autoriser	lan	lannet	GRE_to_B	remote_net_B:	Tous
From_B	Autoriser	GRE_to_B	remote_net_B:	lan	lannet	Tous

Configuration du firewall D-Link « B ». En supposant que le réseau *192.168.10.0/24* est un réseau lannet sur l'interface lan, voici les étapes de configuration de NetDefendOS sur le firewall B :

Dans le carnet d'adresses, configurez les objets IP suivants :

remote_net_A: 192.168.10.0/24

remote_gw: 172.16.0.1

ip_GRE: 192.168.0.2

Créez un objet tunnel GRE nommé GRE_to_A ayant les paramètres suivants :

Adresse IP : ip_GRE:

Réseau distant : remote_net_A:

Extrémité distante : remote_gw:

Utilisation d'une clé de session : 1

Total de contrôle d'encapsulation supplémentaire : activé

Définissez une route dans la table de routage *principale* qui achemine l'ensemble du trafic vers remote_net_A sur l'interface GRE GRE_to_A. Cette opération n'est pas nécessaire si l'option Add route for remote network (Ajouter une route pour un réseau distant) est activée dans l'onglet Advanced (Avancé), car la route sera alors ajoutée automatiquement.

Créez les règles suivantes dans l'ensemble de règles IP, qui autorisent le trafic à traverser le tunnel :

Nom	Action	Interface src	Réseau src	Interface de dest.	Réseau de dest.	Service
To_A	Autoriser	lan	lannet	GRE_to_A	remote_net_A:	Tous
From_A	Autoriser	GRE_to_A	remote_net_A:	lan	lannet	Tous

Groupes d'interfaces

Il est possible de regrouper plusieurs interfaces de NetDefendOS pour former un *Groupe d'interfaces*. Ce groupe logique peut par la suite être soumis à des règles communes et désigné par un nom de groupe dans l'ensemble de règles IP et dans les règles d'authentification utilisateur.

Un groupe peut être composé d'interfaces Ethernet habituelles, d'interfaces VLAN ou de tunnels VPN et les membre d'un groupe ne doivent pas être du même type. Un groupe peut être composé, par exemple, de deux interfaces Ethernet et de quatre interfaces VLAN.

Exemple 3.13. Création d'un groupe d'interfaces

Interface de ligne de commande

```
gw-world:/> add Interface InterfaceGroup examplegroup Members=exampleif1,exampleif2
```

Interface Web

Sélectionnez Interfaces > Interface Groups > Add > InterfaceGroup (Interfaces > Groupes d'interfaces > Ajouter > Groupe d'interfaces).

Saisissez les informations suivantes pour définir le groupe :

Name (nom) : nom du groupe qui sera utilisé ultérieurement.

Security/Transport Equivalent (équivalent sécurité/transport) : lorsque cette option est activée, vous pouvez utiliser le groupe d'interfaces en tant qu'interface de destination dans les règles pour lesquelles les connexions peuvent nécessiter d'être permutées entre les interfaces. Le Route Fail-Over (reprise de routes) et l'OSPF sont des exemples d'applications.

Interfaces : sélectionnez les interfaces à placer dans le groupe

Cliquez sur OK.

ARP

Présentation

ARP (Address Resolution Protocol) est un protocole qui mappe une adresse de protocole de couche réseau vers l'adresse matérielle d'une couche de liaison de données. Il est utilisé pour traduire une adresse IP dans l'adresse Ethernet correspondante. Il fonctionne sur la couche OSI Data Link (couche 2 : consultez l'*Annexe D, La structure OSI*) et est encapsulé par des en-têtes Ethernet pour la transmission.

Un hôte du réseau Ethernet peut communiquer avec un autre hôte uniquement s'il connaît l'adresse Ethernet (adresse MAC) de cet hôte. Des protocoles de plus haut niveau tels que le protocole IP utilisent des adresses IP foncièrement différentes d'un plan d'adressage de plus bas niveau comme les adresses MAC. ARP est utilisé pour retrouver l'adresse MAC d'un hôte grâce à son adresse IP.

Lorsqu'un hôte a besoin de traduire une adresse IP dans l'adresse Ethernet correspondante, il transmet un paquet de requêtes ARP. Le paquet de requêtes ARP contient l'adresse MAC source et les adresses IP source et de destination. Chaque hôte du réseau local reçoit ce paquet. L'hôte avec l'adresse IP de destination spécifiée envoie un paquet de réponses ARP à l'hôte source avec son adresse MAC.

ARP dans NetDefendOS

NetDefendOS propose non seulement une prise en charge standard du protocole ARP, mais ajoute également un certain nombre de contrôles de sécurité au cœur de la mise en œuvre du protocole. Par exemple, NetDefendOS n'acceptera pas par défaut les réponses ARP pour lesquelles le système n'a envoyé aucune requête ARP correspondante. Sans ce type de protection, le système serait vulnérable aux « détournements de connexion ».

NetDefendOS prend en charge à la fois l'ARP dynamique et statique, ce dernier étant disponible en deux modes : Publish et XPublish.

L'*ARP dynamique* est le mode de fonctionnement principal d'ARP, dans lequel NetDefendOS envoie des requêtes ARP à chaque fois qu'il a besoin de traduire une adresse IP en adresse Ethernet. Les réponses ARP sont stockées dans le cache ARP du système.

L'*ARP statique* est utilisé pour verrouiller manuellement une adresse IP sur une adresse Ethernet spécifique. Ce procédé est expliqué plus en détail dans les sections ci-dessous.

Cache ARP

Le *cache ARP* est la table temporaire de NetDefendOS pour stocker le mappage entre les adresses IP et Ethernet. Le cache ARP est vide au démarrage du système et ses entrées seront remplies si besoin.

Le contenu d'un cache ARP typique (minimal) est similaire à la table suivante :

Type	Adresse IP	Adresse Ethernet	Expiration
Dynamique	192.168.0.10	08:00:10:0f:bc:a5	45
Dynamique	193.13.66.77	0a:46:42:4f:ac:65	136
Publié	10.5.16.3	4a:32:12:6c:89:a4	-

Le premier élément de ce cache ARP est une entrée ARP dynamique qui nous apprend que l'adresse IP 192.168.0.10 est mappée sur l'adresse Ethernet 08:00:10:0f:bc:a5. Le second élément mappe de manière dynamique l'adresse IP 193.13.66.77 sur l'adresse Ethernet 0a :46 :42 :4f :ac :65. Enfin, le troisième élément est une entrée ARP statique qui associe l'adresse IP 10.5.16.3 à l'adresse Ethernet 4a :32 :12 :6c :89 :a4.

La troisième colonne de la table, Expiration, est utilisée pour indiquer la durée pendant laquelle l'entrée ARP sera valide. Le premier élément, par exemple, possède une valeur d'expiration de 45, ce qui signifie que cette entrée sera rendue invalide et supprimée du cache ARP après 45 secondes. Si un trafic est envoyé à l'adresse IP 192.168.0.10 après l'expiration, NetDefendOS émet une nouvelle requête ARP.

Le temps d'expiration par défaut pour les entrées ARP dynamiques est de 900 secondes (15 minutes). Vous pouvez le changer en modifiant le paramètre avancé ARPExpire. Le paramètre ARPExpireUnknown précise combien de temps NetDefendOS va garder en mémoire les adresses injoignables. Cette précaution permet de s'assurer que NetDefendOS ne sollicite pas ces adresses en continu. La valeur par défaut pour ce paramètre est de 3 secondes.

Exemple 3.14. Affichage du cache ARP

Vous pouvez afficher le contenu du cache ARP à partir de l'interface de ligne de commande.

Interface de ligne de commande

```
gw-world:/> arp -show

ARP cache of iface lan
 Dynamic 10.4.0.1  = 1000:0000:4009 Expire=196
 Dynamic 10.4.0.165 = 0002:a529:1f65 Expire=506
```

Alignement du cache ARP. Si un hôte de votre réseau a récemment été remplacé par un nouveau matériel tout en conservant la même adresse IP, il est très probable qu'il dispose d'une nouvelle adresse Ethernet. Si NetDefendOS possède une entrée ARP pour cet hôte, l'adresse Ethernet de cette entrée sera invalide, ce qui empêchera les données envoyées vers l'hôte de parvenir à destination.

Après le temps d'expiration ARP, NetDefendOS apprendra évidemment la nouvelle adresse Ethernet de l'hôte demandé, mais il arrive parfois que l'on doive forcer une nouvelle requête manuellement. Le plus simple consiste à *aligner* le cache ARP, opération qui supprime toutes les entrées ARP dynamiques du cache, ce qui force NetDefendOS à émettre de nouvelles requêtes ARP.

Exemple 3.15. Alignement du cache ARP

Cet exemple montre comment aligner le cache ARP à partir de l'interface de ligne de commande.

Interface de ligne de commande

```
gw-world:/> arp -flush
ARP cache of all interfaces flushed.
```

Taille du cache ARP. Par défaut, le cache ARP peut détenir 4 096 entrées ARP à la fois. Cela convient pour la plupart des déploiements, mais il se peut que vous deviez parfois ajuster cette valeur, par exemple lorsque plusieurs LAN très volumineux sont connectés directement au firewall. Vous pouvez le faire en modifiant le paramètre avancé ARPCacheSize.

Les « tables de hachage » sont utilisées pour localiser des entrées dans le cache ARP. Pour une efficacité maximale, un hachage doit être deux fois plus grand que la table qu'il indexe, donc si le LAN à connexion directe le plus volumineux contient 500 adresses IP, la table de hachage ARP doit comporter au moins 1 000 entrées. L'administrateur peut modifier le paramètre avancé ARPHashSize pour traduire des besoins réseau spécifiques. La valeur par défaut pour ce paramètre est 512.

Le paramètre ARPHashSizeVLAN est similaire au paramètre ARPHashSize mais il affecte la taille de hachage pour les interfaces VLAN uniquement. La valeur par défaut est 64.

Entrées ARP statiques et publiées

NetDefendOS prend en charge la définition d'entrées ARP statiques (association statique d'adresses IP aux adresses Ethernet) ainsi que la publication d'adresses IP avec une adresse Ethernet spécifique.

Entrées ARP statiques. Les éléments ARP statiques peuvent être utiles lorsqu'un périphérique signale une adresse Ethernet incorrecte en réponse aux requêtes ARP. Certains ponts entre les postes de travail, comme les modems radio, peuvent rencontrer ce type de problèmes. Vous pouvez également les utiliser pour verrouiller une adresse IP sur une adresse Ethernet spécifique dans le but d'augmenter la sécurité ou pour éviter le déni de service lorsque des utilisateurs pirates se trouvent dans un réseau. Notez toutefois qu'une telle protection s'applique uniquement aux paquets envoyés en direction de cette adresse IP, et non aux paquets envoyés à partir de celle-ci.

Exemple 3.16. Définition d'une entrée ARP statique

Cet exemple va créer un mappage statique entre l'adresse IP *192.168.10.15* et l'adresse Ethernet *4b:86:f6:c5:a2:14* sur l'interface *lan*.

Interface de ligne de commande

```
gw-world:/> add ARP Interface=lan IP=192.168.10.15 Mode=Static
 MACAddress=4b-86-f6-c5-a2-14
```

Interface Web

Sélectionnez Interfaces > ARP > Add > ARP (ARP > Ajouter > ARP).

Dans les listes déroulantes, sélectionnez les options suivantes :

Mode : Static (statique)

Interface : lan

Saisissez les paramètres suivants :

Adresse IP : 192.168.10.15

MAC (Adresse MAC) : 4b-86-f6-c5-a2-14

Cliquez sur OK.

Entrées ARP publiées. NetDefendOS prend en charge la *publication* d'entrées ARP, ce qui signifie que vous pouvez définir des adresses IP (et, si nécessaire, des adresses Ethernet) pour une interface. NetDefendOS propose alors des réponses ARP pour les requêtes ARP qui se rapportent à ces adresses IP.

Ce processeur a deux utilités majeures :

Donner l'impression que l'interface de NetDefendOS possède plusieurs adresses IP.

Aider l'équipement réseau proche répondant aux requêtes ARP de manière incorrecte. Cet usage est toutefois moins courant.

Le premier usage est pratique lorsque plusieurs plages IP distinctes se trouvent sur un seul LAN. Les hôtes de chaque plage IP peuvent alors utiliser une passerelle de leur propre plage lorsque ces adresses de passerelles sont publiées sur l'interface NetDefendOS correspondante.

Un autre usage consiste à publier plusieurs adresses sur une interface externe, ce qui permet à NetDefendOS d'adresser de manière statique les communications vers ces adresses et de les transmettre en direction des serveurs internes qui possèdent des adresses IP privées.

Il existe deux modes de publication : Publish et XPublish. La différence entre les deux est que Xpublish « ment » quant à l'adresse Ethernet de l'expéditeur se trouvant dans l'en-tête Ethernet ; celle-ci est définie de manière à être identique à l'adresse Ethernet publiée plutôt qu'à l'adresse Ethernet réelle de l'interface Ethernet. Si une adresse Ethernet publiée est identique à l'adresse Ethernet de l'interface, il n'y aura pas de différence si vous sélectionnez Publish ou XPublish. Dans les deux cas, le résultat sera le même.

Conseil

Dans la configuration des entrées ARP, les adresses peuvent uniquement être publiées une à la fois. Toutefois, vous pouvez utiliser la fonctionnalité ProxyARP pour gérer la publication de réseaux entiers (reportez-vous à la section nommée « ARP Proxy »).

Paramètres ARP avancés

Cette section présente certains paramètres avancés du protocole ARP. Dans la plupart des cas, vous n'avez pas besoin de modifier ces paramètres, mais pour certains déploiements, des modifications peuvent être requises. La plupart se trouvent dans WebUI, via ARP > Advanced Settings (ARP > Paramètres avancés).

Diffusion et multidiffusion. Les requêtes et les réponses ARP qui contiennent des adresses de diffusion ou multidiffusion ne sont, en général, jamais correctes, à l'exception de certains périphériques d'équilibrage du volume de trafic et de redondance, qui utilisent des adresses à multidiffusion de la couche matérielle.

Le comportement par défaut de NetDefendOS consiste à ignorer et à consigner de telles requêtes et réponses ARP. Vous pouvez toutefois le changer en modifiant les paramètres avancés ARPMulticast et ARPBroadcast.

Réponses ARP non sollicitées. Il est tout à fait possible pour un hôte présent sur le LAN d'envoyer une réponse ARP au firewall, même si aucune requête ARP correspondante n'a été effectuée. Selon les spécifications ARP, le récepteur doit accepter ce type de réponses ARP. Toutefois, étant donné que ce processus peut faciliter le détournement de connexions locales, NetDefendOS ignore et consigne normalement ces réponses.

Vous pouvez changer ce comportement en modifiant le paramètre avancé UnsolicitedARPReplies.

Requêtes ARP. La spécification ARP déclare qu'un hôte doit mettre à jour son cache ARP avec les données des requêtes ARP reçues des autres hôtes. Toutefois, étant donné que cette procédure peut faciliter le détournement de connexions locales, NetDefendOS ne l'autorise pas.

Pour rendre ce comportement compatible avec la spécification RFC 826, l'administrateur peut modifier le paramètre avancé ARPRequests. Même lorsque le paramètre ARPRequests est défini sur « Drop » (Ignorer), ce qui signifie que le paquet est rejeté sans être stocké, le système va tout de même répondre à ce paquet, à condition que d'autres règles acceptent la demande.

Modifications du cache ARP. NetDefendOS propose quelques paramètres qui contrôlent la façon de modifier le cache ARP.

Une réponse ou une requête ARP reçue peut modifier un élément existant du cache ARP. Le fait d'autoriser cette opération peut permettre le détournement de connexions locales. Toutefois, si on ne l'autorise pas, cela peut causer des problèmes si, par exemple, un adaptateur réseau est remplacé, car NetDefendOS n'acceptera pas la nouvelle adresse tant que l'entrée du cache ARP précédente n'a pas expiré.

Vous pouvez régler les paramètres avancés ARPChanges pour modifier le comportement. Le comportement par défaut de NetDefendOS consiste à autoriser les modifications, mais elles sont dans ce cas toutes consignées.

On rencontre une situation similaire lorsque les informations contenues dans les réponses ou dans les requêtes ARP coïncident avec les entrées statiques du cache ARP. Cela n'est, bien sûr, jamais autorisé. Toutefois, la modification du paramètre avancé StaticARPChanges autorise l'administrateur à spécifier si oui ou non de telles situations doivent être consignées.

IP expéditeur 0.0.0.0. Il est possible de configurer la façon dont NetDefendOS traite les requêtes ARP qui possèdent l'IP expéditeur 0.0.0.0. De tels IP expéditeur ne sont jamais valides en réponse, mais les unités réseau

qui n'ont pas encore détecté leur adresse IP posent parfois des requêtes ARP avec un IP expéditeur « non spécifié ». Normalement, ces réponses ARP sont ignorées et consignées, mais vous pouvez changer ce comportement en modifiant le paramètre avancé ARPQueryNoSenderIP.

Correspondance des adresses Ethernet. Par défaut, NetDefendOS exige que l'adresse de l'expéditeur au niveau Ethernet soit conforme à l'adresse Ethernet indiquée par les données ARP. Si ce n'est pas le cas, la réponse sera ignorée et consignée. Vous pouvez changer ce comportement en modifiant le paramètre avancé ARPMatchEnetSender.

L'ensemble de règles IP

Règles de sécurité

Caractéristiques des règles. Les *règles* de sécurité NetDefendOS conçues par l'administrateur décident de la façon dont le trafic peut traverser un firewall D-Link. Dans NetDefendOS, les règles sont définies par différents *ensembles de règles* NetDefendOS. Ces ensembles de règles partagent une manière commune de spécifier les critères de filtrage qui déterminent le type de trafic auquel elles vont s'appliquer. Cet ensemble de critères comprend :

Une interface source	Interface ou groupe d'interfaces qui reçoit le paquet au niveau du firewall D-Link. Il peut aussi s'agir d'un tunnel VPN.
Un réseau source	Réseau contenant l'adresse IP source du paquet. Il peut s'agir d'un objet IP NetDefendOS qui définit une adresse IP unique ou une plage d'adresses.
Une interface de destination	Interface ou groupe d'interfaces par lequel le paquet quitte le firewall D-Link. Il peut aussi s'agir d'un tunnel VPN.
Un réseau de destination	Réseau auquel appartient l'adresse IP de destination du paquet. Il peut s'agir d'un objet IP NetDefendOS qui définit une adresse IP unique ou une plage d'adresses.
Un service	Type de protocole auquel appartient le paquet. Les objets de service définissent un type de protocole/de port, par exemple, HTTP ou ICMP. Vous pouvez également définir des services personnalisés (reportez-vous à la section Services pour plus d'informations).

Les ensembles de règles de NetDefendOS, qui utilisent tous les mêmes paramètres de filtrage, comprennent les éléments suivants :

Les règles IP.

Les « pipe rules » ou règles de tuyau (reportez-vous à la section intitulée « Mise en forme du trafic »).

Les politiques d'acheminement en fonction de règles (reportez-vous à la section intitulée « Acheminement en fonction de règles »).

Les règles IDP (reportez-vous à la section intitulée « Prévention et détection des intrusions »).

Les règles d'authentification – réseau/interface source uniquement (reportez-vous au *chapitre 8, Authentification utilisateur*).

Spécification d'une interface ou d'un réseau. Au moment de spécifier le critère de filtrage dans l'un des ensembles de règles mentionnés ci-dessus, vous pouvez utiliser trois options utiles prédéfinies :

Pour un réseau source ou de destination, l'option « all-nets » (tout-réseau) équivaut à l'adresse IP 0.0.0.0/0, ce qui implique que toute adresse IP est acceptable.

Pour une interface source ou de destination, vous pouvez utiliser l'option « Any » afin que NetDefendOS ne s'occupe pas de l'interface à destination ou en provenance de laquelle transite le trafic.

Vous pouvez définir l'interface de destination en tant que « core ». Cela signifie que le trafic, par exemple un *Ping*

ICMP, est destiné au firewall D-Link lui-même et que c'est NetDefendOS qui va lui répondre.

Règles IP. L'*ensemble de règles IP* est le plus important de ces ensembles de règles de sécurité. Il définit la fonction essentielle de filtrage des paquets de NetDefendOS, en régulant ce qui est autorisé ou non à traverser le firewall D-Link et, si nécessaire, la façon dont s'appliquent les traductions d'adresses comme NAT.

Il existe deux approches possibles pour définir comment doit être traité le trafic qui traverse NetDefendOS :

Sauf autorisation spécifique, tout est refusé

Sauf refus spécifique, tout est autorisé

Pour permettre la meilleure sécurité possible, la première de ces approches est adoptée par NetDefendOS et l'action « Drop » (Ignorer) est la règle par défaut de l'ensemble de règles IP, ce qui signifie que l'ensemble du trafic est refusé. Pour permettre tout trafic (notamment les réponses de NetDefendOS aux requêtes *Ping* ICMP), l'administrateur doit définir des règles IP qui autorisent le trafic à traverser le firewall D-Link.

Bien que le rejet des paquets est réalisé sans qu'une règle IP spécifique existe, il est recommandé, à des fins de consignation, qu'une règle IP Drop avec consignation activée soit placée comme dernière règle dans l'ensemble de règles IP.

Évaluation des règles IP

Lorsqu'une nouvelle connexion TCP/IP est établie à travers le firewall D-Link, la liste des règles IP est examinée de haut en bas jusqu'à ce qu'une règle correspondant aux paramètres de la nouvelle connexion soit trouvée. L'action de la règle est alors exécutée.

Si l'action l'autorise, l'établissement de la nouvelle connexion se poursuit. Une nouvelle entrée (ou un *état)* représentant la nouvelle connexion est ensuite ajoutée à la table d'état interne de NetDefendOS, ce qui permet de surveiller les connexions ouvertes et actives qui utilisent le firewall D-Link. Si l'action est Drop (Ignorer) ou Reject (Rejeter), alors la nouvelle connexion est refusée.

Filtrage dynamique. Après l'évaluation de l'ouverture de la connexion par la règle initiale, les prochains paquets appartenant à cette connexion n'auront pas à être examinés individuellement par l'ensemble de règles. Au lieu de cela, un algorithme particulièrement efficace recherche chaque paquet dans la table pour déterminer s'il appartient à une connexion déjà établie.

Cette approche est appelée *filtrage dynamique* et ne s'applique pas seulement aux protocoles dynamiques tels que TCP mais également aux protocoles statiques tels que UDP et ICMP, au moyen de « pseudo-connexions ». Cette approche signifie que l'examen avec l'ensemble de règles IP est uniquement effectué lors de la phase initiale d'ouverture de connexion. La taille de l'ensemble de règles IP a par conséquent un effet négligeable sur le débit global.

Le premier principe de correspondance. Si plusieurs règles correspondent aux mêmes paramètres, la première règle de correspondance dans un balayage de haut en bas est celle qui décide de la manière dont la connexion va être gérée.

Les règles SAT sont une exception car elles reposent sur un appariement avec une seconde règle pour fonctionner. Après avoir rencontré une règle SAT correspondante, la recherche va se poursuivre pour trouver une seconde règle qui corresponde (pour plus d'informations, reportez-vous à la section « Traduction d'adresses statiques »).

Trafic non-correspondant. Les paquets entrants qui ne correspondent à aucune règle de l'ensemble de règles et qui ne possèdent pas de connexion correspondante dans la table d'état seront automatiquement soumis à l'action « Drop » (Ignorer). Pour être plus explicite, une règle finale appelée DropAll, possédant une action « Drop » (Ignorer) configurée sur *all-nets* comme réseau source/de destination et *all* comme interface source/de destination, devrait exister dans l'ensemble de règles.

Actions des règles IP

Une règle se compose de deux parties : les paramètres de filtrage et la mesure à prendre si une correspondance existe avec ces paramètres. Comme décrit ci-dessus, les paramètres de toute règle NetDefendOS, notamment les règles IP, sont :

Une interface source

Un réseau source

Une interface de destination

Un réseau de destination

Un service

L'élément *service* d'une règle IP est également important car si un objet de la passerelle ALG (*Application Layer Gateway*) doit être appliqué au trafic, il doit être associé à un objet de service (reportez-vous à la section « Passerelle ALG »).

Lorsqu'une règle IP est déclenchée par une correspondance, l'une des *actions* suivantes peut se produire :

Autoriser Le paquet est autorisé à passer. Étant donné que la règle est appliquée uniquement à l'ouverture d'une connexion, une entrée est établie dans la « table d'état » pour enregistrer l'ouverture d'une connexion. Le reste des paquets attribués à cette connexion traversera le « moteur dynamique » de NetDefendOS.

FwdFast Laisse le paquet traverser le firewall D-Link sans configurer d'état qui lui soit spécifique dans la table d'état. Cela signifie que le processus de filtrage dynamique est évité et est, par conséquent, moins sécurisé que les règles Allow ou NAT. La durée de traitement des paquets est également plus lente que pour les règles Allow car chaque paquet est comparé à l'ensemble de règles tout entier.

NAT La règle NAT fonctionne comme la règle Allow, mais avec la traduction dynamique d'adresse (NAT) activée (pour une description détaillée, reportez-vous à la section intitulée « Traduction dynamique des adresses réseau » du *chapitre 7, Traduction d'adresses*).

SAT Cette action commande à NetDefendOS de procéder à la traduction d'adresse statique. Une règle SAT nécessite toujours une règle Allow, NAT ou FwdFast correspondante en plus de l'ensemble de règles (pour une description détaillée, reportez-vous à la section intitulée « Traduction d'adresse statique » du *chapitre 7, Traduction d'adresse*).

Drop (Ignorer) Cette action commande à NetDefendOS d'ignorer immédiatement le paquet. Il s'agit d'une version « impolie » de l'action Reject (Rejeter), car aucune réponse n'est envoyée à l'expéditeur. Elle est souvent préférable car elle ne donne, au pirate potentiel, aucune information sur ce qui est arrivé à leurs paquets.

Reject (Rejeter) Cette action fonctionne comme l'action Drop (Ignorer), mais retourne un message « TCP RST » ou « ICMP Injoignable », qui informe l'ordinateur expéditeur que le paquet a été rejeté. Il s'agit d'une version « polie » de l'action Drop (Ignorer).

Connexions bidirectionnelles. Une erreur courante lors de la configuration des règles IP est de définir deux règles, l'une pour le trafic allant dans un sens et l'autre pour le trafic rentrant dans l'autre sens. En fait, presque toutes les règles IP autorisent un flux de trafic *bidirectionnel* une fois que la connexion initiale est configurée. Le réseau source et l'interface source dans la règle correspondent à la source de la requête de connexion initiale. Une fois qu'une connexion est autorisée et établie, le trafic peut alors circuler dans chaque direction.

L'exception à ce flux bidirectionnel sont les règles FwdFast. Si l'action FwdFast est utilisée, alors la règle n'autorisera pas le trafic à revenir de la destination à la source. Si un flux bidirectionnel est exigé, alors deux règles FwdFast sont requises, c'est-à-dire une pour chaque direction. C'est également le cas lorsqu'une règle FwdFast est utilisée avec une règle SAT.

Utilisation de Reject (Rejeter). Dans certaines situations, l'action Reject (Rejeter) est recommandée, plutôt que l'action Drop (Ignorer), car une réponse polie est exigée par NetDefendOS. Un exemple d'une telle situation est la réponse au protocole d'identification de l'utilisateur IDENT.

Modification des entrées de l'ensemble de règles IP

Après avoir ajouté différentes règles à l'ensemble de règles, vous pouvez cliquer avec le bouton droit de la souris

sur la ligne de votre choix dans l'interface Web pour la modifier.

Un menu contextuel apparaît avec les options suivantes :

Modifier — Autorise la modification du contenu de la règle.

Supprimer — Supprime définitivement la règle de l'ensemble de règles.

Activer/Désactiver — Permet de désactiver la règle en la conservant dans l'ensemble de règles. Lorsque cette option est définie sur « Désactiver », la ligne de l'ensemble de règles n'affectera pas le trafic et apparaîtra grisée dans l'interface utilisateur. Vous pouvez la réactiver à tout moment.

Options de déplacement — La dernière section du menu contextuel permet de déplacer la règle à un autre emplacement dans l'ensemble de règles, afin de lui affecter une priorité différente.

Programmation

Dans certains cas de figure, il peut être utile de contrôler non seulement quelle fonctionnalité est activée, mais également à quel moment cette fonctionnalité est utilisée.

La politique informatique d'une entreprise peut, par exemple, stipuler que le trafic Web en provenance d'un service spécifique est uniquement autorisé à sortir du service pendant les heures normales de bureau. Un autre exemple : l'authentification qui utilise une connexion VPN spécifique est autorisée uniquement les jours de semaine avant midi.

NetDefendOS répond à cette en fournissant des objets *programmation*, ou simplement des *programmes*, que vous pouvez sélectionner et utiliser avec différents types de règles de sécurité pour obtenir un contrôle en fonction du temps. Cette fonctionnalité n'est en aucun cas limitée aux règles IP, mais est valide pour la plupart des types de règles, notamment les règles de mise en forme du trafic et les règles de détection et de prévention des intrusions (IDP). Un objet *programme* est, en d'autres termes, un composant très puissant qui peut autoriser une régulation détaillée des périodes d'activation ou de désactivation des fonctions de NetDefendOS.

Un objet *programme* vous permet d'indiquer plusieurs plages horaires pour chaque jour de la semaine. De plus, il est possible de spécifier des dates de début et de fin qui imposeront des contraintes supplémentaires à la programmation. Par exemple, vous pouvez définir le programme suivant : le lundi et le mardi, de 8 h 30 à 10 h 40 et de 11 h 30 à 14 h, le vendredi, de 14 h 30 à 17 h.

Important

Étant donné que les programmes dépendent de la date et de l'heure exacte, il est très important que la date et l'heure du système soient correctement paramétrées. De préférence, la synchronisation de l'heure a également été activée pour s'assurer que les règles planifiées seront activées et désactivées au bon moment. Pour plus d'informations, reportez-vous à la section « Configuration de la date et de l'heure ».

Exemple 3.17. Configuration d'une règle planifiée

Cet exemple crée un objet programme pour les heures de bureau en semaine et l'associe à une règle IP qui autorise le trafic HTTP.

Interface de ligne de commande

```
gw-world:/> add ScheduleProfile OfficeHours Mon=8-17 Tue=8-17 Wed=8-17 Thu=8-17
   Fri=8-17

gw-world:/> add IPRule Action=NAT Service=http SourceInterface=lan
   SourceNetwork=lannet DestinationInterface=any
   DestinationNetwork=all-nets Schedule=OfficeHours
   name=AllowHTTP
```

Interface Web

Sélectionnez Objects > Schedules > Add > Schedule (Objets > Programmation > Ajouter > Programme).

Saisissez les paramètres suivants :

Name (nom): OfficeHours (heures de bureau)

Dans la liste, sélectionnez de 8 h à 17 h, du lundi au vendredi.

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez les paramètres suivants :

Name (nom): AllowHTTP (autoriser HTTP)

Dans les listes déroulantes, sélectionnez les options suivantes :

Action : NAT

Service: http

Schedule (programmation) : OfficeHours (heures de bureau)

SourceInterface (interface source) : lan

SourceNetwork lannet (réseau source lannet)

DestinationInterface (interface de destination) : any (toutes)

DestinationNetwork (réseau de destination) : all-nets (tout réseau)

Cliquez sur OK.

Certificats X.509

NetDefendOS prend en charge des certificats numériques conformes à la norme ITU-T X.509. Cela implique l'utilisation d'une hiérarchie de certificats X.509 avec une cryptographie à clé publique utilisée pour la distribution de clés et l'authentification d'entités.

Présentation

Un certificat X.509 est une preuve d'identité numérique. Il crée un lien entre une identité et une clé publique dans le but de définir si une clé publique appartient réellement au propriétaire supposé. Par ce processus, il empêche l'interception des données transférées par un tiers malveillant qui pourrait poster une fausse clé avec le nom et l'identifiant utilisateur d'un destinataire souhaité.

Certificats des tunnels VPN. L'usage prédominant des certificats dans NetDefendOS concerne les tunnels VPN. La façon la plus simple et la plus rapide de sécuriser les extrémités d'un tunnel est d'utiliser des clés pré-partagées (PSK). La complexité d'utilisation des clés PSK augmente avec la taille des réseaux VPN. Les certificats sont un moyen de mieux gérer la sécurité dans les réseaux plus importants.

Composants des certificats. Un certificat comprend les éléments suivants :

Une clé publique : l'identité de l'utilisateur, par exemple son nom ou son identifiant utilisateur.

Les signatures numériques : Une déclaration qui stipule que les informations contenues dans le certificat ont été approuvées par une autorité de certification.

En combinant les informations ci-dessus, un certificat est une clé publique comprenant une identification, couplée à un cachet de certification d'un organisme agrée.
Autorités de certification. Une *autorité de certification* (AC) est une entité agrée qui délivre des certificats à d'autres entités. L'autorité de certification signe numériquement tous les certificats qu'elle délivre. Une signature de l'autorité de certification vérifie l'identité du propriétaire du certificat et garantit que le certificat n'a pas été falsifié par un tiers.

Une autorité de certification se charge de vérifier que les informations de chaque certificat qu'elle délivre sont correctes. Elle doit également s'assurer que l'identité du certificat correspond à l'identité du propriétaire du certificat.

Une AC peut également délivrer des certificats à d'autres AC. Cela entraîne une hiérarchie de certificats sous forme d'arbre. L'AC située au plus haut de la hiérarchie est appelée l'AC racine. Dans cette hiérarchie, chaque AC est signée par l'AC située juste au-dessus, à l'exception de l'AC racine qui est généralement signée par elle-même.

Un chemin de certification fait référence au chemin de certificats allant d'un certificat à un autre. Lors du processus de vérification de la validité d'un certificat d'utilisateur, le chemin entier partant du certificat d'utilisateur jusqu'au certificat du nœud agrée doit être examiné avant que la validité du certificat d'utilisateur ne soit établie.

Le certificat AC est identique à n'importe quel certificat, hormis le fait qu'il autorise la clé privée correspondante à signer d'autres certificats. Si la clé privée de l'AC est altérée, toute l'AC est également altérée, y compris tous les certificats qu'elle a signés.

Durée de validité. Un certificat n'est pas valide indéfiniment. Chaque certificat contient les dates de validité du certificat. Lorsque cette période de validité arrive à expiration, le certificat ne peut plus être utilisé et un nouveau certificat doit être délivré.

Listes de révocation de certificats. Une liste de révocation de certificats (CRL) contient une liste de tous les certificats qui ont été annulés avant leur date d'expiration. Ces cas de figure peuvent se présenter pour plusieurs raisons, notamment lorsque les clés du certificat ont été altérées de quelque manière que ce soit ou que le propriétaire du certificat a perdu les droits d'authentification qui utilisent ce certificat. Cela peut arriver, par exemple, si un employé a quitté l'entreprise qui a délivré le certificat.

Une CRL est régulièrement publiée sur un serveur auquel peuvent accéder tous les utilisateurs de certificats, au moyen des protocoles LDAP ou HTTP.

Les certificats contiennent souvent un champ de points de distribution CRL, qui spécifie l'emplacement à partir duquel la liste de révocation de certificats peut être téléchargée. Dans certains cas, les certificats ne contiennent pas ce champ. Dans ces cas-là, l'emplacement de la liste CRL doit être configuré manuellement.

L'AC met à jour sa CRL à un intervalle donné. La longueur de cet intervalle dépend de la configuration de l'AC. Généralement, elle varie entre une heure et plusieurs jours.

Approbation des certificats. Lorsqu'on utilise des certificats, NetDefendOS fait confiance à toute personne qui détient un certificat signé par une AC donnée. Avant qu'un certificat soit approuvé, la validité du certificat est vérifiée de la manière suivante :

Construction d'un chemin de certification jusqu'à la racine AC agréée.

Vérification des signatures de tous les certificats contenus dans le chemin de certification.

Recherche de chaque certificat dans la liste CRL afin de vérifier qu'aucun des certificats n'a été révoqué.

Listes d'identification. En plus de vérifier les signatures des certificats, NetDefendOS utilise également des listes d'identification. Une liste d'identification est une liste qui mentionne toutes les identités distantes qui possèdent un accès autorisé par un tunnel VPN spécifique, à condition que la procédure de validation du certificat décrite ci-dessus ait abouti.

Réutilisation des certificats racine. Dans NetDefendOS, les certificats racines doivent être considérés comme des entités globales qui peuvent être réutilisées entre les tunnels VPN. Même si un certificat racine est associé à un tunnel VPN dans NetDefendOS, il peut toujours être réutilisé avec le nombre d'autres tunnels VPN différents que l'on souhaite.

Certificats X.509 dans NetDefendOS

Les certificats X.509 peuvent être chargés sur le firewall D-Link pour être utilisés lors des authentifications IKE/IPsec, Webauth, etc. Deux types de certificats peuvent être chargés : les certificats auto-signés et les certificats distants appartenant à un nœud distant ou un serveur AC.

Exemple 3.18. Chargement d'un certificat X.509

Il peut s'agir d'un certificat auto-signé ou d'un certificat appartenant à un nœud distant ou à un serveur AC.

Interface Web

Sélectionnez Objects > Authentication Objects > Add > Certificate (Objets > Objets d'authentification > Ajouter > Certificat).

Spécifiez un nom convenable pour le certificat.

Sélectionnez l'une des options suivantes :

Upload self-signed X.509 Certificate (charger un certificat X.509 auto-signé)

Upload a remote certificate (charger un certificat distant)

Cliquez sur OK et suivez les instructions.

Exemple 3.19. Association de certificats X.509 à des tunnels IPsec

Pour associer un certificat importé à un tunnel IPsec.

Interface Web

Sélectionnez Interfaces > IPsec.

Affichez les propriétés du tunnel IPsec.

Sélectionnez l'onglet Authentication (Authentification).

Sélectionnez l'option Certificat X509.

Sélectionnez la passerelle et les certificats racine corrects.

Cliquez sur OK.

Configuration de la date et de l'heure

Pour assurer le bon fonctionnement de NetDefendOS, il est important de configurer correctement la date et l'heure. Les règles planifiées, les mises à jour automatiques de l'IDP et des bases de données antivirus, ainsi que d'autres fonctionnalités du produit exigent que l'horloge système soit réglée avec précision. De plus, les messages de consignation sont horodatés pour indiquer l'instant où se produit un événement spécifique. Cela suppose non seulement une horloge qui fonctionne, mais aussi qu'elle est correctement synchronisée avec les autres périphériques du réseau.

Pour garantir une date et une heure précises, NetDefendOS utilise une horloge matérielle en temps réel intégrée. Cette horloge est également équipée d'une pile de sauvegarde qui la protège contre les coupures de courant temporaires. De plus, NetDefendOS prend en charge les *protocoles de synchronisation horaire*, reposant sur des requêtes envoyées à des serveurs externes spécifiques, pour ajuster automatiquement l'horloge.

Paramètres de date et heure généraux

Date et heure actuelles. L'administrateur peut configurer la date et l'heure manuellement. Cela est recommandé lorsqu'une nouvelle installation de NetDefendOS est lancée pour la première fois.

Exemple 3.20. Configuration de la date et de l'heure actuelles

Pour ajuster la date et l'heure actuelles, suivez les étapes ci-dessous :

Interface de ligne de commande

```
gw-world:/> time -set YYYY-mm-DD HH:MM:SS
```

Où YYYY-mm-DD HH :MM :SS représente les nouvelles date et heure. Notez l'ordre de présentation de la date : l'année, puis le mois et enfin le jour. Pour régler la date et l'heure sur le 27 avril 2007, 9 h 25, la commande sera :

```
gw-world:/> time -set 2007-04-27 09:25:00
```

Interface Web

Sélectionnez System > Date and Time (Système > Date et heure).

Cliquez sur Set Date and Time (Ajuster la date et l'heure).

Ajustez l'année, le mois, le jour et l'heure à l'aide des commandes déroulantes.

Cliquez sur OK.

Remarque

Dès qu'elles sont définies, NetDefendOS applique les nouveaux paramètres de date et heure.

Fuseaux horaires. Le monde est divisé en un certain nombre de fuseaux horaires, l'Heure de Greenwich (GMT) à Londres à la longitude 0 étant utilisée comme fuseau de référence. Tous les autres fuseaux horaires situés à l'Est et à l'Ouest de la longitude 0 sont définis comme étant GMT plus ou moins un nombre d'heures entier. Tous les emplacements comptabilisés comme étant à l'intérieur d'un fuseau horaire donné posséderont alors la même heure locale, qui sera donnée par un nombre entier représentant le décalage horaire par rapport à GMT.

Le fuseau horaire de NetDefendOS correspond au fuseau horaire dans lequel se trouve physiquement le firewall D-Link.

Exemple 3.21. Configuration du fuseau horaire

Pour régler le fuseau horaire de NetDefendOS sur GMT + 1 heure, suivez les étapes ci-dessous :

Interface de ligne de commande

```
gw-world:/> set DateTime Timezone=GMTplus1
```

Interface Web

Sélectionnez System > Date and Time (Système > Date et heure).

Sélectionnez (GMT+01:00) dans la liste déroulante des fuseaux horaires.

Cliquez sur OK.

Passage à l'heure d'été. De nombreuses régions observent le passage à l'heure d'été (*Daylight Saving Time, DST*), ce qui signifie que les horloges sont avancées pour la période estivale. Malheureusement, les principes qui régulent le passage à l'heure d'été varient suivant les pays et il existe, dans certains cas, des différences au sein d'un même pays. Pour cette raison, NetDefendOS ne sait pas automatiquement quand il doit passer à l'heure d'été. Vous devez saisir cette information manuellement si vous souhaitez utiliser le passage à l'heure d'été.

Deux paramètres régissent le passage à l'heure d'été ; la période DST et le décalage DST. La période de l'heure d'été indique à quelles dates débute et se termine le passage à l'heure d'été. Le décalage de l'heure d'été indique le nombre de minutes qui doit être ajouté à l'horloge pendant la période de l'heure d'été.

Exemple 3.22. Activer le passage à l'heure d'été

Pour activer le passage à l'heure d'été, suivez les étapes ci-dessous :

Interface de ligne de commande

```
gw-world:/> set DateTime DSTEnabled=Yes
```

Interface Web

Sélectionnez System > Date and Time (Système > Date et heure).

Cochez la case Enable daylight saving time (Activer le passage à l'heure d'été).

Cliquez sur OK.

Serveurs horaires

L'horloge matérielle utilisée par NetDefendOS peut parfois accélérer ou ralentir après une certaine période d'activité. Il s'agit d'un comportement normal dans la plupart des équipements informatiques et réseau qui peut être résolu en utilisant des *Serveurs horaires*.

NetDefendOS peut ajuster l'horloge automatiquement en fonction des informations reçues de la part d'un ou plusieurs serveurs horaires qui offrent une heure ultra-précise, en utilisant généralement les horloges atomiques. L'utilisation de serveurs horaires est fortement recommandée car elle garantit que NetDefendOS alignera son heure et sa date sur celles des autres périphériques réseau.

Protocoles de synchronisation de l'heure. Les *protocoles de synchronisation de l'heure* sont des méthodes normalisées qui permettent de récupérer les informations concernant l'heure sur les serveurs horaires externes. NetDefendOS prend en charge les protocoles de synchronisation horaire suivants :

SNTP - Défini par la norme RFC 2030, le SNTP (Simple Network Time Protocol) est une forme allégée du protocole NTP (RFC 1305). Il est utilisé par NetDefendOS pour interroger les serveurs NTP.

UDP/TIME - Le Time Protocol (UDP/TIME) est une ancienne méthode qui fournit un service de synchronisation horaire via Internet. Ce protocole propose une heure et une date indépendantes de tout site et lisibles par la machine. Le serveur renvoie l'heure en secondes depuis le 1er janvier 1900, à minuit.

La plupart des serveurs horaires publics exécutent le protocole NTP et sont accessibles via SNTP.

Configuration des serveurs horaires. Jusqu'à trois serveurs horaires peuvent être configurés pour lancer des requêtes visant à récupérer les informations d'heure. L'utilisation de plusieurs serveurs permet d'éviter les situations où un serveur injoignable entraîne l'échec du processus de synchronisation du temps. NetDefendOS interroge toujours l'ensemble des serveurs horaires configurés et calcule une heure moyenne en fonction de toutes les réponses. Des moteurs de recherche Internet peuvent être utilisés pour établir la liste des serveurs horaires accessibles au plus grand nombre.

Important

Assurez-vous qu'un serveur DNS externe est configuré de manière à ce que les URL des serveurs horaires puissent être traduites (reportez-vous à la section « Recherche DNS »). Cette opération n'est pas requise si vous utilisez des adresses IP de serveurs.

Exemple 3.23. Activation de la synchronisation du temps via SNTP

Dans cet exemple, la synchronisation du temps est configurée de façon à utiliser le protocole SNTP pour communiquer avec les serveurs NTP du Swedish National Laboratory for Time and Frequency. Les URL du serveur NTP sont *ntp1.sp.se* et *ntp2.sp.se*.

Interface de ligne de commande

```
gw-world:/> set DateTime TimeSynchronization=custom TimeSyncServer1=dns:ntp1.sp.se
   TimeSyncServer2=dns:ntp2.sp.se TimeSyncInterval=86400
```

Web Interface

Sélectionnez System > Date and Time (Système > Date et heure).

Cochez la case Enable time synchronization (Autoriser la synchronisation du temps)

Saisissez :

Time Server Type (type de serveur horaire) : SNTP

Primary Time Server (serveur horaire primaire) : ntp1.sp.se

Secondary Time Server (serveur horaire secondaire) : ntp2.sp.se

Cliquez sur OK.

> **Remarque**
> Si le paramètre TimeSyncInterval n'est pas spécifié lorsque l'interface de ligne de commande est utilisée pour paramétrer l'intervalle de synchronisation, la valeur par défaut de 86 400 secondes (1 jour) est appliquée.

Exemple 3.24. Déclenchement manuel de la synchronisation du temps

Vous pouvez déclencher la synchronisation du temps via l'interface de ligne de commande. Le résultat ci-dessous montre une réponse typique.

Interface de ligne de commande

```
gw-world:/> time -sync
Attempting to synchronize system time...

Server time: 2007-02-27 12:21:52 (UTC+00:00)
Local time: 2007-02-27 12:24:30 (UTC+00:00) (diff: 158)

Local time successfully changed to server time.
```

Réglage du temps maximum. Pour éviter les situations où un serveur horaire défectueux provoque la mise à jour de l'horloge avec une heure extrêmement imprécise, vous pouvez paramétrer une valeur de *réglage maximale* (en secondes). Si la différence entre l'heure actuelle de NetDefendOS et l'heure reçue à partir d'un serveur horaire est supérieure à cette valeur de réglage maximale, alors la réponse du serveur horaire sera rejetée. Supposons par exemple que la valeur de réglage maximale est de 60 secondes et que l'heure actuelle de NetDefendOS est 16 h 42 min 35 s. Si la réponse d'un serveur horaire est 16 h 43 min 38 s, alors la différence est de 63 secondes. Cette valeur est supérieure à la valeur de réglage maximale donc aucune mise à jour n'est effectuée pour cette réponse.

Exemple 3.25. Modification de la valeur de réglage maximale

Interface de ligne de commande

```
gw-world:/> set DateTime TimeSyncMaxAdjust=40000
```

Web Interface

Sélectionnez System > Date and Time (Système > Date et heure).

Pour définir le décalage de temps maximal qu'un serveur est autorisé à ajuster, entrez la durée maximale en secondes qu'un serveur est autorisé à ajuster.

Cliquez sur OK.

Il peut parfois être nécessaire de remplacer le réglage maximal, par exemple lorsque la synchronisation du temps vient juste d'être activée et que la différence de durée initiale est supérieure à la valeur de réglage maximale. Il est alors possible de forcer manuellement une synchronisation et d'ignorer le paramètre de réglage maximal.

Exemple 3.26. Forcer la synchronisation du temps

Cet exemple démontre comment forcer la synchronisation du temps, en remplaçant le paramètre de réglage maximal.

Interface de ligne de commande

```
gw-world:/> time -sync -force
```

Intervalles de synchronisation. L'intervalle entre chaque tentative de synchronisation peut être ajusté si nécessaire. La valeur par défaut est de 86 400 secondes (1jour), ce qui signifie que le processus de synchronisation

s'exécute une fois toutes les 24 heures.

Serveurs horaires D-Link. L'utilisation des serveurs horaires propres à D-Link est une option de NetDefendOS ; c'est la méthode préconisée pour synchroniser l'horloge du firewall. Ces serveurs communiquent avec NetDefendOS via le protocole SNTP.

Lorsque l'option serveur D-Link est sélectionnée, un ensemble de valeurs prédéfinies sont utilisées pour la synchronisation.

Exemple 3.27. Activation du serveur D-Link NTP

Pour activer l'utilisation du serveur D-Link NTP :

Interface de ligne de commande

```
gw-world:/> set DateTime TimeSynchronization=D-Link
```

Web Interface

Sélectionnez System > Date and Time (Système > Date et heure).

Sélectionnez le bouton radio D-Link TimeSync Server.

Cliquez sur OK.

Comme mentionné ci-dessus, il est important de configurer un serveur DNS externe pour que les URL du serveur horaire D-Link puissent être traduites durant le processus d'accès.

Recherche DNS

Un serveur DNS peut traduire un *Fully Qualified Domain Name* (FQDN) en adresse IP numérique correspondante. Les FQDN sont des noms de domaines textuels non ambigus qui spécifient une position de nœud unique dans l'arbre hiérarchique du Système de Noms de Domaines (DNS) Internet. La résolution FQDN autorise la modification de l'adresse IP physique réelle tandis que le FQDN peut rester identique.

La différence entre une URL (*Uniform Resource Locator*) et un FQDN est que l'URL intègre, outre le FQDN, le protocole d'accès. Le protocole « *http//:»* peut par exemple être spécifié pour les pages du World Wide Web.

Les FQDN sont utilisés dans de nombreux aspects d'une configuration NetDefendOS où les adresses IP sont inconnues ou lorsqu'il s'avère plus judicieux d'utiliser la résolution DNS à la place des adresses IP statiques.

Pour réaliser la résolution DNS, NetDefendOS possède un client DNS intégré qui peut être configuré pour utiliser jusqu'à trois serveurs DNS.

Exemple 3.28. Configuration des serveurs DNS

Dans cet exemple, le client DNS est configuré pour utiliser un serveur DNS primaire et un serveur DNS secondaire, possédant respectivement les adresses 10.0.0.1 et 10.0.0.2.

Interface de ligne de commande

```
gw-world:/> set DNS DNSServer1=10.0.0.1 DNSServer2=10.0.0.2
```

Web Interface

Sélectionnez System > DNS (Système > DNS).

Saisissez les paramètres suivants :

Primary DNS (DNS principal) : 10.0.0.1

Secondary DNS (DNS secondaire) : 10.0.0.2

Cliquez sur OK.

Chapitre 4. Routage

Le présent chapitre décrit comment configurer le routage IP sous NetDefendOS.

Présentation

Les fonctionnalités de routage IP font partie des possibilités les plus fondamentales de NetDefendOS : tout paquet IP qui navigue dans le système est soumis à au moins une décision de routage à un moment donné et une configuration adaptée du routage est cruciale pour que le système de NetDefendOS fonctionne comme prévu.

NetDefendOS prend en charge les types de mécanismes de routage suivants :

Routage statique.

Routage dynamique.

De plus, NetDefendOS prend en charge la *surveillance du routage* pour accomplir le routage et la redondance des liens avec possibilité de fail-over (basculement).

Routage statique

Le *Routage statique* constitue la forme de routage la plus basique. Le terme « statique » se rapporte au fait que les entrées de la table de routage sont ajoutées manuellement et sont donc permanentes (ou statiques) de nature.

Cette approche manuelle fait du routage statique la méthode la plus appropriée aux plus petits déploiements de réseaux, au sein desquels les adresses sont presque toutes fixes et où le nombre de réseaux connectés sont limités. Cependant, pour des réseaux plus étendus (ou bien lorsque la topologie du réseau est complexe), les tâches de maintenance manuelle des tables de routage statique seraient trop longues et problématiques. Dans ces cas de figure, le routage dynamique est donc recommandé.
Pour plus d'informations sur les capacités de routage dynamique de NetDefendOS, veuillez consulter la section intitulée « Routage dynamique ». Notez cependant que même si vous choisissez de déployer un routage dynamique pour votre réseau, vous devez quand même comprendre les principes du routage statique et la manière dont il s'applique à NetDefendOS.

Principes de base du routage

Le routage IP est le mécanisme utilisé dans les réseaux TCP/IP pour transmettre les paquets IP de leur source jusqu'à leur destination, en passant par de nombreux nœuds intermédiaires, le plus souvent désignés comme des routeurs ou des firewalls. Dans chaque routeur, une *table de routage* indique où le prochain paquet doit être envoyé. Une table de routage se compose généralement de plusieurs *routes*. Chaque route contient en principe un réseau de destination, une interface vers laquelle transférer le paquet et éventuellement l'adresse IP de la prochaine passerelle se trouvant sur le chemin de la destination.

Les images ci-dessous illustrent le déploiement typique d'un firewall D-Link, ainsi que la représentation de la table de routage associée.

Route n°	Interface	Destination	Passerelle
1	lan	192.168.0.0/24	
2	dmz	10.4.0.0/16	
3	wan	195.66.77.0/24	
4	wan	all-nets (tout réseau)	195.66.77.4

La table de routage ci-dessus fournit les informations suivantes :

Route n°1 : tous les paquets allant vers les hôtes du réseau 192.168.0.0/24 doivent être envoyés via l'interface lan. Comme aucune passerelle n'est spécifiée pour cette route, l'hôte est supposé se situer sur le segment du réseau dédié à l'interface lan.

Route n°2 : tous les paquets allant vers les hôtes du réseau 10.4.0.0/16 doivent être envoyés via l'interface dmz. De même, aucune passerelle n'est spécifiée pour cette route.

Route n°3 : tous les paquets allant vers les hôtes du réseau 195.66.77.0/24 sont envoyés via l'interface wan. Aucune passerelle n'est requise pour atteindre les hôtes.

Route n°4 : tous les paquets allant vers n'importe quel hôte (*all-nets* correspond à tous les hôtes) sont envoyés via l'interface wan vers les passerelles dont l'adresse IP est 195.66.77.4. Cette passerelle va donc consulter sa table de routage pour savoir où transmettre les paquets. Une route dont la destination est *all-nets* (tout réseau) est souvent considérée comme la *route par défaut* puisqu'elle va correspondre à tous les paquets pour lesquels aucune route spécifique n'a été déterminée.

Lors de l'évaluation d'une table de routage, l'ordre des routes est important. En général, les routes les plus *spécifiques* d'une table de routage sont évaluées en premier. En d'autres termes, si deux routes ont des réseaux de destination qui se chevauchent, le réseau le plus limité sera évalué en premier par rapport à un réseau plus étendu. Dans l'exemple ci-dessus, un paquet dont l'adresse IP de destination est 192.168.0.4 correspond théoriquement à la première et à la dernière route. Cependant, la première route correspond davantage. L'évaluation s'arrête donc ici et le paquet est transmis en fonction de cette donnée.

Routage statique

Cette section décrit comment le routage est appliqué dans NetDefendOS et présente la manière de configurer le routage statique.

NetDefendOS prend en charge plusieurs tables de routage. Une table par défaut appelée « main » est prédéfinie et est toujours présente dans NetDefendOS. Cependant, l'administrateur peut définir des tables de routage supplémentaires et complètement indépendantes pour bénéficier d'un routage alternatif.

Ces tables de routage supplémentaires définies par l'utilisateur sont utiles pour mettre en œuvre un *Policy Based Routing* (routage basé sur des règles). Ceci signifie que l'administrateur peut établir des règles dans l'ensemble de règles IP qui déterminent quelles tables de routage se chargeront de quel type de trafic (voir la section intitulée « Routage basé sur des règles »).

Le mécanisme de Route lookup (recherche de route). Le mécanisme de Route lookup (recherche de route) de NetDefendOS présente quelques différences par rapport au mode de fonctionnement d'autres routeurs. Pour beaucoup de routeurs chez lesquels les paquets IP sont transférés sans contexte (c'est-à-dire que le transfert est dépourvu d'état), la table de routage est analysée à chaque fois que le routeur reçoit un paquet IP. Dans NetDefendOS, les paquets sont transmis pourvus d'un état. Le processus de recherche de route est donc étroitement intégré dans le mécanisme d'inspection dynamique de NetDefendOS.

Quand un paquet IP est reçu sur n'importe laquelle des interfaces, la table de connexion est consultée pour vérifier si une connexion qui correspond au paquet reçu n'est pas déjà établie. Si une connexion existante est trouvée, l'entrée de la table de connexion informe de la direction du paquet et évite ainsi toute recherche dans la table de routage. Cette solution est bien plus efficace que les recherches traditionnelles sur table de routage. C'est aussi l'une des raisons qui explique les hautes performances de transmission de NetDefendOS.

Si aucune connexion n'est établie, la table de routage est consultée. Il est important de comprendre que la recherche de route est effectuée avant l'évaluation des différentes sections de règles. Ainsi, l'interface de destination est connue au moment où NetDefendOS décide si la connexion doit être autorisée ou ignorée. Cette méthode permet un contrôle plus fin des règles de sécurité.

Désignation des routes dans NetDefendOS. NetDefendOS désigne les routes de manière légèrement différente par rapport à la plupart des autres systèmes, mais sa méthode est plus facile à comprendre, ce qui peut éviter les erreurs.

Beaucoup d'autres produits n'utilisent pas l'interface spécifique dans la table de routage, mais spécifient l'adresse IP de l'interface. La table de routage ci-dessous provient d'un poste de travail Microsoft Windows XP :

```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 13 d4 51 8d dd ...... Intel(R) PRO/1000 CT Network
0x20004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
```

```
===========================================================================
Active Routes:
Network Destination  Netmask  Gateway  Interface Metric
   0.0.0.0   0.0.0.0 192.168.0.1 192.168.0.10  20
   10.0.0.0  255.0.0.0 10.4.2.143 10.4.2.143  1
  10.4.2.143 255.255.255.255 127.0.0.1  127.0.0.1  50
 10.255.255.255 255.255.255.255 10.4.2.143 10.4.2.143  50
  85.11.194.33 255.255.255.255 192.168.0.1 192.168.0.10  20
  127.0.0.0  255.0.0.0 127.0.0.1  127.0.0.1  1
  192.168.0.0 255.255.255.0 192.168.0.10 192.168.0.10  20
  192.168.0.10 255.255.255.255 127.0.0.1  127.0.0.1  20
 192.168.0.255 255.255.255.255 192.168.0.10 192.168.0.10  20
  224.0.0.0  240.0.0.0 10.4.2.143 10.4.2.143  50
  224.0.0.0  240.0.0.0 192.168.0.10 192.168.0.10  20
 255.255.255.255 255.255.255.255 10.4.2.143 10.4.2.143  1
 255.255.255.255 255.255.255.255 192.168.0.10 192.168.0.10  1
Default Gateway:  192.168.0.1
===========================================================================
Persistent Routes:
None
```

La même table de routage sous NetDefendOS ressemble à ceci :

```
Flags Network   Iface Gateway  Local IP Metric
----- ----------------- -------- -------------- --------- ------
  192.168.0.0/24  lan        20
  10.0.0.0/8   wan        1
  0.0.0.0/0   wan  192.168.0.1    20
```

Le mode de désignation des routes est plus facile à lire et à comprendre sous NetDefendOS. Un autre avantage de cette notation est que vous pouvez spécifier une passerelle pour une route particulière sans qu'une route ne couvre l'adresse IP de la passerelle, ou malgré le fait que la route qui couvre l'adresse IP de la passerelle passe normalement par une autre interface.

Il convient aussi de mentionner que NetDefendOS vous permet de spécifier les routes pour des destinations qui ne sont pas alignées sur des masques de sous-réseau traditionnels. En d'autres termes, il est parfaitement légitime de spécifier une route pour les plages d'adresses de destination comprises entre 192.168.0.5 et 192.168.0.17 et une autre route pour les adresses 192.168.18 à 192.168.0.254. Cette fonctionnalité rend NetDefendOS vraiment approprié au routage dans des topologies de réseau très complexes.

Affichage de la table de routage. Il est important de bien distinguer la table de routage active dans le système et la table de routage que vous configurez. La table de routage que vous configurez ne contient que les routes que vous avez ajoutées manuellement (les routes statiques). Le contenu de la table de routage active, quant à lui, varie selon plusieurs facteurs. Par exemple, si le routage dynamique a été activé, la table de routage sera alimentée de routes connues lors des échanges avec les autres routeurs du réseau. De plus, les fonctionnalités telles que le fail-over (basculement) des routes modifient parfois l'apparence de la table de routage active.

Exemple 4.1. Affichage de la table de routage

Cet exemple indique comment afficher le contenu de la table de routage configurée et de la table de routage active.

Interface de ligne de commande

Pour afficher la table de routage configurée :

```
gw-world:/> cc RoutingTable main

gw-world:/main> show

Route

 # Interface Network Gateway  Local IP
 - --------- -------- ------------ --------
 1 wan  all-nets 213.124.165.1 (none)
 2 lan  lannet (none)   (none)
 3 wan  wannet (none)   (none)
```

Pour afficher la table de routage active, saisissez :

```
gw-world:/> routes

Flags Network   Iface   Gateway   Local IP  Metric
----- ----------------- ------------- --------------- -------------- ------
  192.168.0.0/24  lan           0
  213.124.165.0/24 wan           0
  0.0.0.0/0   wan   213.124.165.1     0
```

Interface Web

Pour afficher la table de routage configurée :

Sélectionnez Routing > Routing Tables (Routage > Tables de routage).

Cliquez avec le bouton droit de la souris sur la table de routage principale (*main*) figurant dans la liste.

Dans le menu, sélectionnez Edit (Modifier).

La fenêtre principale répertorie les routes configurées.

Pour afficher la table de routage active, sélectionnez l'élément Routes dans le menu déroulant Status (État) de la barre de menu. La fenêtre principale affiche la table de routage active.
Routes *du noyau*. NetDefendOS alimente automatiquement la table de routage active avec les *routes du noyau*. Ces routes ont pour but d'indiquer au système où diriger le trafic qui est destiné au système lui-même. Une route est ajoutée pour chaque interface du système. En d'autres termes, deux interfaces nommées lan et wan, dont les adresses IP sont respectivement 192.168.0.10 et 193.55.66.77, vont créer les routes suivantes :

Route n°	Interface	Destination	Passerelle
1	noyau	192.168.0.10	
2	noyau	193.55.66.77	

Lorsque le système reçoit un paquet IP dont l'adresse de destination est l'une des adresses IP des interfaces, le paquet sera acheminé vers l'interface du noyau. En d'autres termes, le traitement est assuré par NetDefendOS lui-même.

Une route du noyau est aussi ajoutée pour toutes les adresses à multidiffusion :

Route n°	Interface	Destination	Passerelle
1	noyau	224.0.0.0/4	

Pour inclure les routes du noyau lorsque vous affichez la table de routage active, vous devez spécifier une option dans la commande de routage.

Exemple 4.2. Affichage des routes du noyau

Cet exemple indique comment afficher les routes du noyau dans la table de routage active.

Interface de ligne de commande

```
gw-world:/> routes -all

Flags Network   Iface   Gateway   Local IP  Metric
----- ----------------- ------------- --------------- -------------- ------
  127.0.0.1   core   (Shared IP)      0
  192.168.0.1  core   (Iface IP)      0
  213.124.165.181 core   (Iface IP)      0
  127.0.3.1   core   (Iface IP)      0
  127.0.4.1   core   (Iface IP)      0
  192.168.0.0/24  lan           0
  213.124.165.0/24 wan           0
  224.0.0.0/4  core   (Iface IP)      0
  0.0.0.0/0   wan   213.124.165.1     0
```

Interface Web

Sélectionnez l'élément Routes dans le menu déroulant Status (État) de la barre de menu.

Cochez Show all routes (Afficher toutes les routes), puis cliquez sur le bouton Apply (Appliquer).

La fenêtre principale affiche la table de routage active, y compris les routes du noyau.

Conseil

Pour plus d'informations sur la restitution des commandes de **routage** de l'interface de ligne de commande, veuillez consulter le *CLI Reference Guide* (Guide de référence sur l'interface de ligne de commande).

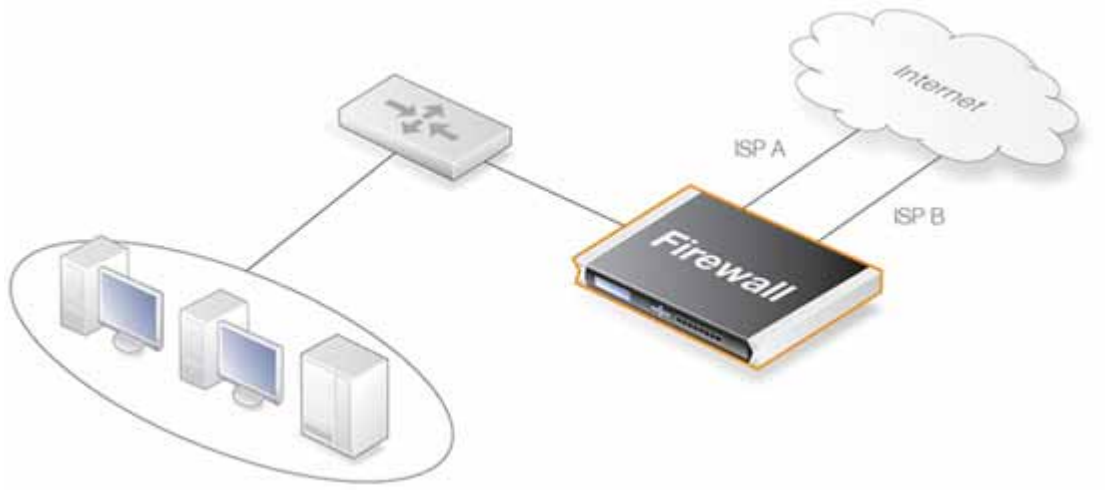
Basculement de route

Présentation. Les firewalls D-Link sont souvent déployés dans des endroits critiques où leur disponibilité et leur connectivité sont cruciales. Par exemple, une société dont le fonctionnement repose massivement sur l'accès à Internet, peut voir ses activités gravement interrompues si une connexion à l'Internet échoue.

Par conséquent, il est fréquent d'avoir une connexion Internet de secours en faisant appel à un Fournisseur d'Accès Internet (FAI) secondaire. Les accès Internet des deux FAI utilisent souvent des méthodes de connexion différentes pour prévenir tout point commun d'échec.

Pour simplifier les scénarios tels que les multiples FAI, NetDefendOS offre une fonctionnalité de *failover* (basculement) *de route*. Ainsi, si une route échoue, le trafic sera automatiquement *basculé* vers une route alternative. La fonctionnalité de *fail-over* (basculement) *de route* de NetDefendOS s'applique avec la fonctionnalité de *surveillance du routage*, par laquelle NetDefendOS surveille la disponibilité des routes et commute le trafic sur une route alternative en cas d'échec de la route principale.

Figure 4.1. Scénario de basculement de route pour un accès ISP



Configuration du basculement de route. La surveillance du routage doit être activée « route par route ». Pour activer la fonction de basculement de route dans un scénario comportant une route préférée et une route de sauvegarde, il faut activer la surveillance du routage sur la route préférée. Cette fonction n'a pas besoin d'être activée sur la route de sauvegarde puisque aucune route ne lui est associée pour tout basculement. Pour une route dont la surveillance du routage est activée, vous devez choisir parmi deux méthodes de surveillance :

Interface Link Status (État de liaison de l'interface) NetDefendOS surveille l'état de liaison de l'interface spécifiée sur la route. Tant que l'interface est active, la route apparaît comme étant en bon état de fonctionnement. Cette méthode permet de vérifier que l'interface est attachée physiquement et que le câblage fonctionne correctement. Cette méthode a la réponse à l'échec la plus rapide, puisque tout changement de l'état de liaison est tout de suite notifié.

Gateway Monitoring (Surveillance des passerelles) Si une passerelle spécifique a été spécifiée comme étant le prochain saut pour une route, la surveillance de l'accessibilité de cette passerelle se fait par envoi périodique de requêtes ARP. Tant que la passerelle répond à ces requêtes, la route apparaît comme étant en bon état de

fonctionnement.

Configuration de la métrique d'une route. Lors de la spécification des routes, l'administrateur doit configurer manuellement une *métrique* des routes. La métrique est un entier positif qui indique une préférence dans le choix de la route à emprunter vers la destination donnée. Lorsque deux routes conduisent à la même destination, NetDefendOS sélectionne celle qui possède la valeur métrique la plus basse pour envoyer les données (si les deux routes ont la même métrique, la route trouvée en premier dans la table de routage sera empruntée).

Une route principale préférée doit avoir une métrique basse (par exemple « 10 ») et une route secondaire de basculement doit avoir une métrique plus élevée (par exemple « 20 »).

Routes de basculement multiples. Il est possible de spécifier plusieurs routes de basculement. Par exemple, il est possible d'associer à une route principale deux routes de basculement au lieu d'une seule. Dans ce cas, la métrique doit être différente pour chacune des trois routes. Par exemple : « 10 » pour la route principale, « 20 » pour la première route de basculement et « 30 » pour la seconde route de basculement. La surveillance du routage doit être activée dans la table de routage pour les deux premières routes, mais pas pour la dernière (avec la métrique la plus élevée) puisqu'elle n'a pas de route associée vers laquelle basculer.

Processus de basculement. Lorsque la surveillance détermine qu'une route n'est pas disponible, NetDefendOS marque la route comme désactivée et inspecte le basculement de route pour rechercher de nouvelles connexions ou des connexions existantes. Dans le cas de connexions déjà établies, une recherche de route est effectuée pour déterminer la prochaine route qui correspond le mieux. Les connexions commutent alors vers la nouvelle route. Dans le cas de nouvelles connexions, la recherche de route ignore les routes désactivées et la prochaine route qui correspond le mieux est empruntée à leur place.

Le tableau ci-dessous définit deux routes par défaut. Elles ont toutes deux une destination « Tout réseau », mais n'utilisent pas la même passerelle. La première, la route principale, a la métrique la plus basse. La surveillance du routage est activée. Pour la seconde, la route alternative, la surveillance du routage n'est pas nécessaire puisque aucune route de basculement ne lui est associée.

Route n°	Interface	Destination	Passerelle	Métrique	Surveillance
1	wan	Tout réseau	195.66.77.1	10	Activée
2	wan	Tout réseau	193.54.68.1	20	Désactivée

Lorsqu'une connexion vers un hôte sur Internet est sur le point d'être établie, la recherche de route choisira la route qui a la métrique la plus basse. Si le routeur principal WAN échoue, NetDefendOS le détectera et la première route sera désactivée. Par conséquent, une nouvelle recherche de route est effectuée et la seconde route est sélectionnée.

Réactivation des routes. Même si une route a été désactivée, NetDefendOS continuera de vérifier son état. Si la route est de nouveau disponible, elle sera réactivée et les connexions existantes lui seront automatiquement ré-attribuées.

Groupement de l'interface de routage. Lors de l'utilisation de la surveillance du routage, il est important de vérifier si le fail-over (basculement) vers une autre route provoquera des modifications dans l'interface de routage. Au vu de cette possibilité, il est nécessaire de prendre quelques précautions pour s'assurer que les règles et les connexions existantes seront maintenues.

Pour illustrer ce problème, analysez la configuration suivante :
D'abord, une règle IP traduit les adresses réseau (NAT) de tout le trafic HTTP à destination de l'Internet par l'interface wan :

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	NAT	lan	lannet	wan	Tout réseau	http

Par conséquent, la table de routage contient la route par défaut suivante :

Route n°	Interface	Destination	Passerelle	Métrique	Surveillance

Route n°	Interface	Destination	Passerelle	Métrique	Surveillance
1	wan	Tout réseau	195.66.77.1	10	Désactivée

On ajoute maintenant une route secondaire qui emprunte une connexion DSL de sauvegarde. La surveillance du routage est désactivée. La nouvelle table de routage ressemble à ceci :

Route n°	Interface	Destination	Passerelle	Métrique	Surveillance
1	wan	Tout réseau	195.66.77.1	10	Activée
2	dsl	Tout réseau	193.54.68.1	20	Désactivée

Notez que la surveillance du routage est active pour la première route et non pas pour la route de basculement de sauvegarde.

Tant que la route wan préférée agira correctement, tout fonctionnera comme prévu. La surveillance du routage fonctionne également, donc la route secondaire sera activée si la route wan échoue.

Il existe cependant certains problèmes avec cette configuration : si un basculement de route est effectué, la route par défaut utilisera alors l'interface dsl. Quand une nouvelle connexion HTTP est établie depuis le réseau Internet, une recherche de route est effectuée. Sa réponse est une interface de destination dsl. Les règles IP sont donc évaluées, mais la règle NAT d'origine part du principe que l'interface de destination est wan. La nouvelle connexion est donc ignorée par l'ensemble de règles.

De plus, toute connexion existante qui correspond à la règle NAT est aussi ignorée à cause du changement d'interface de destination. Cette situation n'est clairement pas souhaitable.

Pour contourner ce problème, les interfaces de destination potentielles doivent être regroupées dans un *groupe d'interfaces* et l'indicateur de l'équivalent sécurité/transport doit être activé pour ce groupe. Le groupe d'interfaces est désormais utilisé comme interface de destination lors de la configuration des règles. Pour plus d'informations sur les groupes, veuillez consulter la section intitulée « Groupe d'interfaces ».
Génération d'ARP gratuite. Par défaut, NetDefendOS génère une requête ARP gratuite lorsqu'un basculement de route survient, de sorte à informer les systèmes environnants qu'un changement de route a été effectué. Ce comportement peut être contrôlé via le paramètre avancé RFO_GratuitousARPOnFail.

Proxy ARP

Comme expliqué précédemment dans la section intitulée « ARP », le protocole ARP facilite le mappage entre une adresse IP et l'adresse MAC d'un nœud sur un réseau Ethernet. Cependant, il arrive qu'un réseau exécutant Ethernet soit divisé en deux parties, avec un seul appareil de routage tel que le Firewall D-Link. Dans ce cas, NetDefendOS peut répondre lui-même aux requêtes ARP dirigées vers le réseau, vers la partie du firewall D-Link qui utilise la fonctionnalité connue sous le nom de proxy ARP.

Par exemple, l'hôte A d'un sous-réseau envoie une requête ARP pour trouver l'adresse MAC de l'adresse IP de l'hôte B sur un autre réseau séparé. La fonctionnalité de proxy ARP suppose que NetDefendOS réponde à cette requête ARP à la place de l'hôte B. NetDefendOS envoie sa propre adresse MAC comme s'il était l'hôte de destination. Après réception de la réponse, l'hôte A envoie les données directement à NetDefendOS qui, dans son rôle de proxy, les transmettra vers l'hôte B. Durant cette procédure, l'appareil peut examiner et filtrer les données.

Diviser un réseau Ethernet en deux parties distinctes est une application courante d'une fonctionnalité proxy ARP d'un firewall D-Link. L'accès aux deux parties doit être contrôlé. Dans ce cas, NetDefendOS peut surveiller et réguler tout le trafic transitant entre les deux parties.

Remarque
Seul le proxy ARP peut fonctionner pour les interfaces Ethernet et VLAN.

Routage basé sur des règles

Présentation

Le *Policy-based Routing* (Routage basé sur des règles) est une extension du routage standard décrit ci-dessus. Il offre aux administrateurs une flexibilité accrue lors de la mise en œuvre de règles de décision de routage et permet de définir des règles pour que les tables de routage alternatives soient utilisées.

Le routage normal transmet des paquets selon l'adresse IP de destination dérivée de routes statiques ou d'un protocole de routage dynamique. Par exemple, lors de l'utilisation d'OSPF, la route choisie pour les paquets est le chemin de plus bas coût (le plus court) dérivé d'un calcul SPF. Le routage basé sur des règles implique que les routes choisies pour le trafic peuvent être basées sur des paramètres spécifiques de trafic.

Le routage basé sur des règles peut autoriser :

Un routage basé sur la source	Une table de routage supplémentaire peut être nécessaire, selon la source du trafic. Quand les services Internet sont assurés par plusieurs FAI, le routage basé sur des règles peut router le trafic provenant de différents groupes d'utilisateurs au travers de différentes routes. Par exemple, le trafic provenant d'une catégorie d'adresses peut être routé par un FAI et le trafic provenant d'une autre catégorie d'adresses routé par un autre FAI.
Un routage basé sur le service	Une table de routage supplémentaire peut être nécessaire, en fonction du service. Le routage basé sur des règles peut router un protocole donné tel que le HTTP à travers des proxys tels que les caches Web. Les services spécifiques peuvent également être routés vers un FAI spécifique de sorte que l'ensemble du trafic HTTP soit géré par un seul FAI.
Un routage basé sur l'utilisateur	Une table de routage supplémentaire peut être nécessaire, selon l'identité de l'utilisateur ou le *groupe* auquel l'utilisateur appartient. Cette solution est particulièrement utile dans des *réseaux métropolitains à fournisseur indépendant*, où tous les utilisateurs partagent le même cœur de réseau actif, mais où chacun peut choisir un FAI différent en souscrivant à des fournisseurs différents.

La mise en application du routage basé sur des règles dans NetDefendOS a deux fondements :

Une ou plusieurs *Policy-based Routing Tables* (Tables de routage basées sur des règles), alternatives et définies par l'utilisateur, en complément de la table de routage principale standard par défaut.

Une ou plusieurs *Policy-based routing rules* (Règles de routage), qui déterminent quelle table de routage est à utiliser pour quel trafic.

Tables de routage basées sur des règles

NetDefendOS dispose d'une table de routage standard par défaut, appelée « main ». En plus de cette table principale, il est possible de définir une ou plusieurs tables de routage alternatives supplémentaires (les tables de routage basées sur des règles sont parfois appelées « tables de routage *alternatives* » dans la présente section).

Les tables de routage alternatives contiennent les mêmes informations de désignation des routes que la table de routage « *main* », à l'exception d'un paramètre supplémentaire *ordering* défini pour chacune d'elles. Ce paramètre détermine la manière dont est effectuée la recherche de route à l'aide des tables alternatives et de la table principale. Ce procédé est décrit plus loin, dans la section intitulée « Le paramètre Ordering ».

Règles de routage

Une règle parmi l'ensemble de règles de routage peut déterminer quelle est la table de routage à utiliser. Une règle de routage peut être déclenchée par le type de service (HTTP par exemple) conjointement avec l'interface source ou de destination et le réseau source ou de destination.

Lors d'une recherche dans les règles, c'est la première règle correspondante trouvée qui est activée.

Sélection de la table de routage basée sur des règles

Lorsqu'un paquet qui correspond à une nouvelle connexion arrive, la table de routage est choisie de la manière

suivante :

Une recherche dans les règles de PBR doit être effectuée, mais il faut pour cela que l'interface de destination du paquet soit déterminée, ce qui suppose une recherche dans la table de routage « *main* ». Il est donc important qu'une correspondance soit trouvée pour le réseau de destination ou au moins qu'une route « tout réseau » par défaut existe, qui pourrait s'associer à tous les éléments pour lesquels aucune correspondance explicite n'a été trouvée.

Une règle de routage est ensuite recherchée, qui correspond à l'interface source ou de destination du paquet, au réseau source ou de destination du paquet ainsi qu'à son service. Si une règle correspondante est trouvée, la table de routage à utiliser est déterminée. Si aucune règle en PRB n'est trouvée, la table « *main* » sera dans ce cas utilisée.

Une fois que la table de routage correspondante a été localisée, le système vérifie l'adresse IP source afin de s'assurer qu'elle appartient bien à l'interface réceptrice. Les règles d'accès sont d'abord examinées pour voir si elles peuvent effectuer cette vérification (pour plus d'informations sur cette fonctionnalité, consultez la section intitulée « Règles d'accès »). S'il n'y a aucune règle d'accès ou qu'aucune correspondance avec les règles ne peut être trouvée, une recherche inversée est effectuée dans la table de routage sélectionnée à l'aide de l'adresse IP source. Si la vérification échoue, un message d'erreur de règle d'accès par défaut est alors généré.

À cet instant, la recherche de route est effectuée à partir de la table de routage sélectionnée pour déterminer l'interface de destination du paquet. Le paramètre *ordering* est utilisé pour déterminer la procédure de recherche réelle. Les options de cette procédure sont décrites dans la section suivante. Pour mettre en œuvre des systèmes virtuels, l'option d'ordering *Only* doit être utilisée.

La connexion est alors soumise à l'ensemble de règles IP normal. Si une règle SAT est rencontrée, une traduction d'adresses sera effectuée. Le choix de la table à utiliser est effectué avant la traduction d'adresses et la recherche de route est effectuée avec la nouvelle adresse. Notez que la recherche de route d'origine permettant de trouver l'interface de destination à utiliser pour toutes les recherches de règles était effectuée avec l'adresse originale non traduite.)

Si l'ensemble de règles IP le permet, la nouvelle connexion est ouverte dans la table d'état de NetDefendOS et le paquet est transmis par cette connexion.

Le paramètre *Ordering*

Une fois la table de routage de la nouvelle connexion sélectionnée et s'il s'agit d'une table de routage alternative, le paramètre *Ordering* associé à la table en question est utilisé pour décider de la manière elle doit être combinée avec la table de routage principale pour rechercher la route appropriée. Les trois options disponibles sont :

Default (Par défaut) : le comportement par défaut consiste à rechercher d'abord la route dans la table principale. Si aucune route correspondante n'est trouvée ou que la route par défaut est trouvée (la route avec la destination tout réseau 0.0.0.0/0), la recherche est poursuivie dans la table alternative. Si aucune correspondance n'est trouvée dans la table alternative, la route par défaut de la table de routage principale sera utilisée.

First (En premier) : ce comportement implique de rechercher d'abord la route de connexion dans la table alternative. Si aucune route correspondante n'est trouvée, la recherche est poursuivie dans la table principale. Dans le cas contraire, la route tout réseau par défaut sera comptabilisée comme correspondance dans la table alternative.

Only (Uniquement) : cette option ignore l'existence de toute autre table que la table alternative. Ainsi, la recherche n'est effectuée que sur cette table. Une des applications de cette option est de permettre à l'administrateur de dédier une table de routage à un ensemble d'interfaces. L'option only (Uniquement) est utilisée pour créer des systèmes virtuels, puisqu'elle peut dédier une table de routage à un ensemble d'interfaces.

Les deux premières options peuvent être vues comme une combinaison de la table alternative et de la table principale, qui assigne une route si une correspondance est trouvée dans chacune des deux tables.

Important : apparition de la destination tout réseau dans la table principale

Une erreur courante avec le routage basé sur des règles est l'absence de route par défaut avec une interface de destination tout réseau dans la table de routage principale. S'il n'existe aucune correspondance exacte, l'absence d'une route tout réseau par défaut implique l'échec de la connexion.

Exemple 4.3. Création d'une table de routage basée sur des règles

Dans cet exemple, nous créons une table de routage basée sur des règles appelée « TestPBRTable ».

Interface Web

Sélectionnez Routing > Routing Tables > Add > RoutingTable (Routage > Tables de routage > Ajouter > Table de routage).

Entrez :

Name (Nom) : TestPBRTable

Pour l'Ordering, sélectionnez l'une des options suivantes :

First (En premier) : la table de routage créée est consultée en premier. Si cette recherche échoue, elle se poursuivra dans la table de routage principale.

Default (Par défaut) : la table de routage principale est consultée en premier. Si la seule correspondance est la route par défaut (*tout réseau*), la table de routage créée sera consultée. Si la recherche dans la table de routage créée échoue, alors la recherche dans son intégralité aura échoué.

Only (Uniquement) : la table de routage créée est la seule à être consultée. Si cette recherche échoue, elle ne se poursuivra pas dans la table de routage principale.

Si l'option Remove Interface IP Routes (Supprimer les routes IP de l'interface) est activée, les routes de l'interface par défaut sont supprimées, c'est-à-dire les routes dirigées vers l'interface du *noyau* (qui sont des routes vers NetDefendOS lui-même).

Cliquez sur OK.

Exemple 4.4. Création de la route

Après avoir défini la table de routage « TestPBRTable », nous allons à présent lui ajouter des routes.

Interface Web

Sélectionnez Routing > Routing Tables > TestPBRTable > Add > Route (Routage > Tables de routage > TestPBRTable > Ajouter > Route).

Entrez :

Interface : l'interface à router.

Network (Réseau) : le réseau à router.

Gateway (Passerelle) : la passerelle vers laquelle envoyer les paquets.

Local IP Address (Adresse IP locale) : l'adresse IP spécifiée ici est automatiquement publiée sur l'interface correspondante. Cette adresse est aussi utilisée comme adresse d'envoi pour les requêtes ARP. Si aucune adresse n'est spécifiée, l'adresse IP de l'interface du firewall sera utilisée.

Metric (Métrique) : spécifie la métrique de cette route (Plus particulièrement utilisée lors de scénarios de basculement de routes.

Cliquez sur OK.

Exemple 4.5 Configuration du routage basé sur des règles

Cet exemple illustre un scénario de FAI multiples, où il est normal d'utiliser un routage basé sur des règles. On considère que :

Chaque FAI vous donne un réseau IP de sa propre gamme de réseaux. Considérons un scénario à deux FAI, où le réseau 10.10.10.0/24 appartient au FAI A et le réseau 20.20.20.0/24 appartient au FAI B. Les passerelles des FAI sont respectivement 10.10.10.1 et 20.20.20.1.

Pour plus de facilité, toutes les adresses de ce scénario sont des adresses publiques.

Ceci est une structure simplissime : il n'y a pas de sous-réseau explicite entre les passerelles des FAI et le firewall D-Link.

Dans un réseau indépendant de tout fournisseur d'accès, les clients auront probablement une adresse IP qui appartient à un des FAI. Dans un scénario à organisation unique, des serveurs accessibles au public seront configurés avec deux adresses IP séparées : une pour chaque FAI. Cependant, cette différence importe peu pour la configuration des règles de routage.

Notez que pour cette organisation unique, la connexion Internet fournie par plusieurs FAI est normalement meilleure via le protocole BGP, qui permet de ne plus se soucier des différentes plages d'adresses IP et des règles de routage. Cette solution n'est malheureusement pas toujours possible, c'est pourquoi le routage basé sur des règles devient une nécessité.

Nous allons configurer la table de routage principale pour utiliser le FAI A et ajouter une table de routage « r2 » qui utilise la passerelle par défaut du FAI B.

Interface	**Réseau**	**Passerelle**	**Proxy ARP**
lan1	10.10.10.0/24		wan1
lan1	20.20.20.0/24		wan2
wan1	10.10.10.1/32		lan1
wan2	20.20.20.1/32		lan1
wan1	Tout réseau	10.10.10.1	

Voici le contenu de la table de routage basée sur des règles r2 :

Interface	**Réseau**	**Passerelle**
wan2	Tout réseau	20.20.20.1

Le paramètre Ordering de la table r2 est défini sur Default (Par défaut), ce qui implique qu'elle sera consultée si la recherche dans la table de routage principale trouve la route par défaut (*tout réseau*).

Voici le contenu des règles de routage :

Interface source	**Plage source**	**Interface de destination**	**Plage de destination**	**Service**	**Table de transfert VR**	**Table de retour VR**
lan1	10.10.10.0/24	wan2	Tout réseau	TOUS	r2	r2
wan2	Tout réseau	lan1	20.20.20.0/24	TOUS	r2	r2

Pour configurer ce scénario :

Interface Web

Ajoutez les routes trouvées dans la liste des routes de la table de routage principale, comme montré précédemment.

Créez une table de routage nommée « r2 » et assurez-vous que le paramètre ordering est défini sur « Default » (Par défaut).

Ajoutez la route trouvée dans la liste des routes de la table de routage « r2 », comme montré précédemment.

Ajoutez deux règles VR selon la liste des règles montrée précédemment.

Sélectionnez Routing > Routing Rules > Add > Routing Rule (Routage > Règles de routage > Ajouter > Règle de routage).

Entrez les informations trouvées dans la liste des règles affichée précédemment.

Répétez la procédure pour ajouter la deuxième règle.

Remarque
Les règles de l'exemple ci-dessus sont ajoutées pour les connexions entrantes et sortantes.

Routage dynamique.

Présentation du routage dynamique

Le routage dynamique est différent du routage statique en ce sens que le firewall D-Link s'adapte automatiquement aux changements de topologie du réseau et à son trafic. NetDefendOS s'enquiert d'abord auprès des réseaux connectés directement, puis cherche des informations supplémentaires sur la route auprès des autres routeurs. Les routes détectées sont classées et celles qui conviennent le mieux pour les destinations sont ajoutées dans la table de routage. Ces informations sont ensuite envoyées vers les autres routeurs.

Le routage dynamique répond instantanément aux mises à jour, mais il présente l'inconvénient d'être plus prédisposé à certains problèmes tels que les boucles de routage. Sur Internet, deux types d'algorithmes de routage dynamique sont utilisés : l'algorithme Distance Vector (DV) et l'algorithme Link State (LS). Le type d'algorithme choisi détermine la procédure suivie par le routeur pour sélectionner la route optimale ou la « meilleure » et pour partager les informations mises à jour avec d'autres routeurs.
Algorithmes Distance Vector. L'algorithme *Distance Vector* (DV) est un algorithme de routage décentralisé qui calcule le « meilleur » chemin en répartissant le travail. Chaque routeur calcule les coûts de ses propres liens attachés et partage les informations de la route uniquement avec ses routeurs voisins. Le routeur va petit à petit s'enquérir du chemin le moins coûteux grâce à un procédé de calcul itératif et d'échange d'informations avec ses voisins.

Le RIP (*Protocole d'Information de Routage*) est un algorithme DV bien connu qui implique l'envoi régulier de messages de mise à jour, ainsi que l'envoi des modifications de routage vers la table de routage. Le choix du chemin est basé sur sa « longueur », c'est-à-dire le nombre de routeurs intermédiaires (connu aussi sous le nom de « pas »). Après avoir mis à jour sa propre table de routage, le routeur commence immédiatement à la transmettre aux routeurs voisins pour les informer des modifications.

Algorithmes Link State. Contrairement aux algorithmes DV, les algorithmes *Link State* (LS) permettent aux routeurs de conserver des tables de routage qui reflètent la topologie du réseau entier. Chaque routeur diffuse ses liens attachés et leur coût vers tous les autres routeurs du réseau. Quand un routeur reçoit ces informations, il exécute l'algorithme LS et calcule son propre ensemble de chemins à moindre coût. Toute modification de l'état du lien sera envoyé partout sur le réseau, afin que tous les routeurs aient les mêmes informations sur la table de routage.

Open Shortest Path First. L'*Open Shortest Path First* (OSPF) est un logarithme LS largement utilisé. Un routeur compatible OSPF identifie en premier les routeurs et les sous-réseaux qui y sont directement connectés, puis diffuse ces informations vers tous les autres routeurs. Chaque routeur utilise les informations qu'il reçoit pour construire une table représentant l'intégralité du réseau. Avec une table de routage complète, chaque routeur peut identifier les sous-réseaux et les routeurs qui conduisent à n'importe quelle destination. Les routeurs qui utilisent l'OSPF diffusent uniquement les mises à jour qui informent d'une modification, et non pas l'intégralité de la table de routage.

L'OSPF dépend de plusieurs métriques pour déterminer le chemin à emprunter. Il prend aussi en compte les pas, la bande passante, le trafic et les délais. L'OSPF peut garantir un grand contrôle sur le processus de routage puisque ses paramètres peuvent être définis avec une grande précision.

Comparaison des algorithmes de routage dynamique. Puisque l'information sur l'état global du lien est envoyée partout sur le réseau, les algorithmes LS offrent un haut degré de contrôle de configuration et d'évolutivité. Les changements entraînent la diffusion vers d'autres routeurs de l'information mise à jour

uniquement, ce qui implique une convergence plus rapide et moins de risques de boucles de routage. L'OSPF peut aussi fonctionner au sein d'une hiérarchie, bien que le RIP ne soit pas familier avec l'adressage du sous-réseau. NetDefendOS utilise l'OSPF comme algorithme de routage dynamique pour les multiples avantages qu'il offre.
Métriques de routage. Les métriques de routage sont les critères qu'un algorithme de routage utilise pour calculer la « meilleure » route vers une destination. Un protocole de routage repose sur une ou plusieurs métriques pour évaluer les liens au travers d'un réseau et déterminer le chemin optimal. Les principales métriques utilisées incluent :

Path length (Longueur du chemin) La somme des coûts associés à chaque lien. Une des valeurs communément utilisées pour cette métrique est appelée « hop count » (décompte de pas). Elle représente le nombre d'appareils de routage qu'un paquet doit traverser entre sa source et sa destination.

Item Bandwidth (Bande passante de l'élément) La capacité de trafic d'un chemin, mesuré en « Mbps ».

Load (Charge) L'utilisation d'un routeur. Elle peut être évaluée en fonction de l'utilisation et du débit du processeur.

Delay (Durée) Le temps nécessaire pour transférer un paquet de sa source à sa destination. Cette durée dépend de plusieurs facteurs tels que la bande passante, la charge et la longueur du chemin.

OSPF

Présentation. L'*Open Shortest Path First* (OSPF) est un protocole de routage développé pour les réseaux IP par l'IETF (Détachement d'Ingénierie d'Internet). L'implantation de l'OSPF dans NetDefendOS se base sur la norme RFC 2328 et est compatible avec la norme RFC 1583.

L'OSPF route les paquets IP en se basant uniquement sur l'adresse IP de destination trouvée dans l'en-tête du paquet IP. Les paquets IP sont routés « en l'état », c'est-à-dire qu'ils ne sont pas encapsulés dans des en-têtes de protocole supplémentaires lors de leur transit dans l'AS (Système Autonome). L'OSPF est un protocole de routage dynamique qui détecte rapidement les modifications topologiques dans l'AS (tels que les échecs dans l'interface du routeur) et calcule les nouvelles routes dépourvues de boucles après une période de temps.

L'OSPF est un protocole de routage link-state qui requiert l'envoi d'annonces d'état de liens (LSA) vers tous les autres routeurs de la zone. Dans un protocole de routage link-state, chaque routeur entretient une base de données qui désigne la topologie de l'AS. Cette base de données est dénommée base de données link-state. Chaque routeur du même AS possède une base de données identique. Grâce aux informations de la base de données link-state, chaque routeur représente la base d'un arbre des chemins les plus courts qu'il se construit lui-même. Cet arbre des chemins les plus courts propose une route pour chaque destination dans l'AS.

L'OSPF permet de regrouper différents réseaux : c'est ce que l'on appelle une zone. La topologie d'une zone est cachée du reste de l'AS. Ce masquage des informations réduit l'importance du trafic échangé. De plus, le routage au sein même de la zone est uniquement déterminé par sa propre topologie, ce qui protège la zone des mauvaises données de routage. Une zone est la généralisation d'un sous-réseau IP.

Tous les échanges du protocole OSPF peuvent être authentifiés. Ceci implique que seuls les routeurs qui s'authentifient correctement peuvent joindre l'AS. Des schémas d'authentification différents peuvent être utilisés, tels que none, passphrase ou MD5digest. Il est possible de configurer des méthodes d'authentification différentes pour chaque AS.

Zones OSPF. L'AS est divisé en plus petites parties appelées *Zones OSPF*. Cette section définit les zones et les termes associés.

Zones Une zone regroupe des réseaux et des hôtes au sein d'un AS. Les routeurs qui ne font partie que d'une zone sont appelés routeurs internes. Toutes les interfaces des routeurs internes sont directement connectés aux réseaux de la zone. La topologie d'une zone est cachée du reste de l'AS.

ABR Les routeurs qui possèdent des interfaces dans plusieurs zone sont appelés ABR (Area Border Routers). Ceux-ci gèrent une base de données topologique différente pour chaque zone à laquelle ils appartiennent.

ASBR — Les routeurs qui échangent des informations de routage avec des routeurs appartenant à d'autres AS sont appelés ASBR (Autonomous System Boundary Router). Ils indiquent au sein de l'AS les routes qu'ils découvrent à l'extérieur de la zone.

Zones de cœur de réseau — Tous les réseaux OSPF ont besoin d'au moins une zone de cœur de réseau, dont l'ID est 0. Il s'agit de la zone à laquelle toutes les autres zones doivent être connectées. Ce cœur de réseau assure la distribution des informations de routage parmi les zones connectées. Quand une zone n'est pas directement connectée au cœur de réseau, elle a besoin d'être liée virtuellement avec lui.

Zone de stub — Les zones de stub sont des zones par lesquelles ou dans lesquelles les annonces externes de l'AS ne sont pas transmises. Quand une zone est configurée comme une zone de stub, le routeur annonce automatiquement une route par défaut afin que les routeurs de cette zone puissent atteindre des destinations extérieures.

Zones de transit — Les zones de transit sont utilisées pour transférer le trafic d'une zone qui n'est pas directement connectée à la zone de cœur de réseau.

Le routeur dédié. Chaque réseau de diffusion OSPF possède un routeur dédié et un routeur dédié de sauvegarde. Les routeurs utilisent le protocole OSPF hello pour choisir le routeur dédié (DR) et le routeur dédié de sauvegarde (BDR) d'un réseau, en se basant sur les priorités annoncées par tous les routeurs. S'il y a déjà un DR sur le réseau, le routeur l'acceptera en dépit de ses propres priorités de routeurs.

Voisins. Les routeurs qui appartiennent à la même zone deviennent voisins. Les voisins sont choisis via le protocole hello. Les paquets hello sont émis périodiquement par chaque interface qui utilise l'adresse IP à multidiffusion. Les routeurs deviennent voisins aussitôt qu'ils se voient répertoriés dans le même paquet hello. De cette manière, deux moyens de communication sont garantis.

Voici la définition des *États des voisins* :

Down — Il s'agir de l'état initial de la relation entre voisins.

Init — Lorsqu'un paquet HELLO est reçu de la part d'un voisin, mais qu'il n'inclut PAS l'ID routeur du firewall, le voisin sera mis à l'état Init. Aussitôt que le voisin en question reçoit un paquet HELLO, il connaît les ID routeur des routeurs expéditeurs. Il envoie alors un paquet HELLO qui contient ces informations. L'état des voisins change alors pour l'état *2-way*.

2-Way — Dans cet état, la communication entre le routeur et le voisin est bidirectionnelle. Pour les interfaces de point à point et de point à multipoints, l'état passe à *Full*. Sur des interfaces de diffusion, seuls les DR et les BDR prennent l'état *Full* avec leurs voisins. Tous les autres voisins restent à l'état 2-Way.

ExStart — Préparation à la construction d'une contiguïté.

Exchange — Les routeurs échangent des Descripteurs de données.

Loading — Les routeurs échangent des annonces d'état de liens.

Full — Il s'agit de l'état normal d'une contiguïté entre un routeur et le DR/BDR.

Agrégats. Pour OSPF, les agrégats sont utilisés pour combiner des groupes de routes avec une adresse commune en une seule entrée dans la table de routage. Ils sont généralement utilisés pour réduire la table de routage.

Liens virtuels. Les liens virtuels sont utilisés pour :

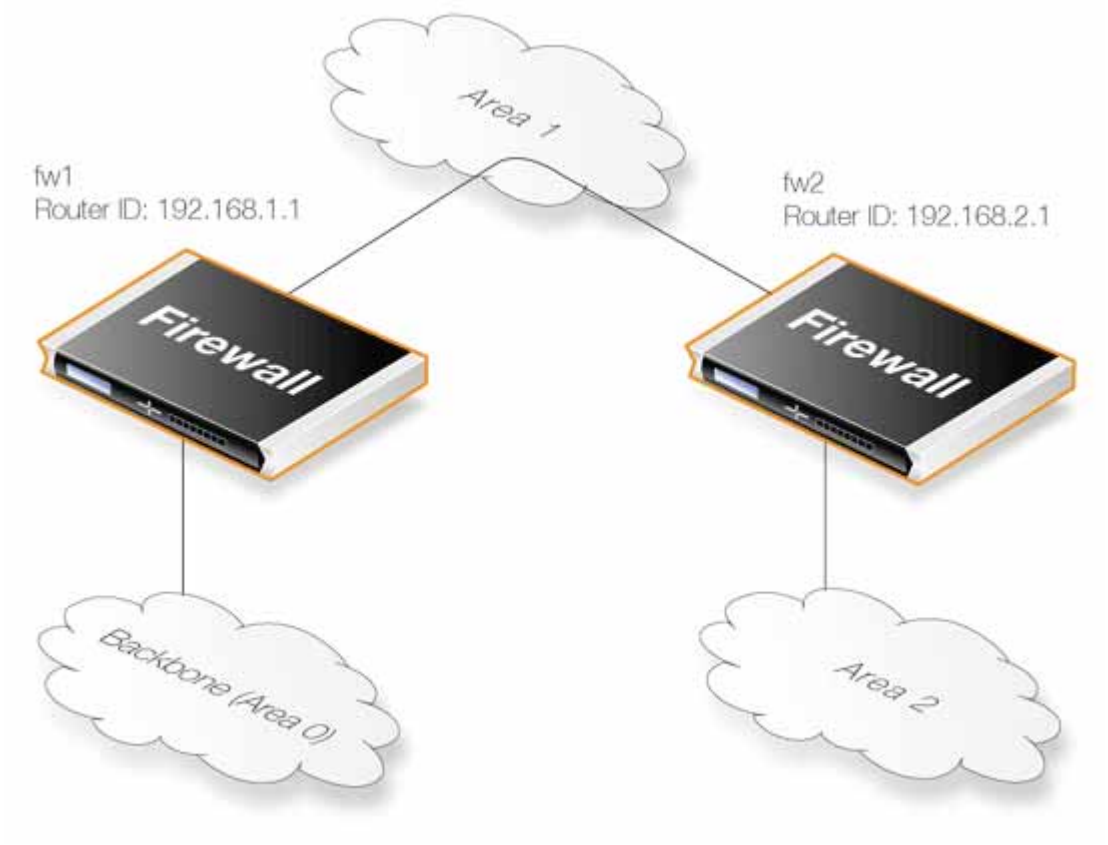
Lier une zone qui n'a pas de connexion directe au cœur de réseau.

Relier le cœur de réseau au cas où il serait partitionné.

Les zones sans connexion directe avec le cœur de réseau. Le cœur de réseau doit nécessairement être le centre de toutes les autres zones. Dans les rares cas où il est impossible de connecter physiquement une zone au cœur de réseau, on peut utiliser un lien virtuel. Le lien virtuel fournit à cette zone un chemin logique vers la zone de cœur de réseau. Ce lien virtuel est établi entre deux ABR se situant sur une zone commune, l'un des ABR étant

connectés à la zone de cœur de réseau. Dans l'exemple ci-dessous, deux routeurs sont connectés à la même zone (Zone 1) mais uniquement l'un d'entre eux (fw1) est connecté physiquement à la zone de cœur de réseau.

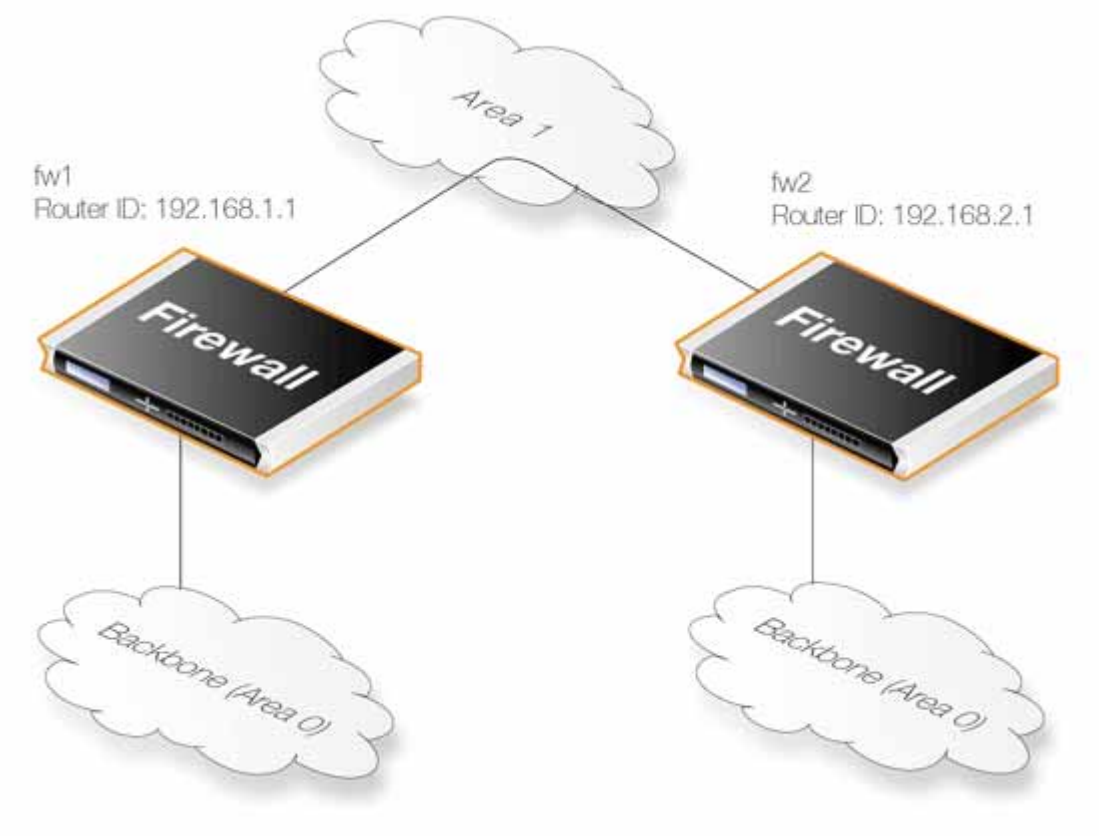
Figure 4.2. Liens virtuels exemple 1



Dans l'exemple ci-dessus, le lien virtuel est configuré entre fw1 et fw2 sur la zone 1, puisqu'elle est utilisée comme zone de transit. Dans cette solution, seul l'ID routeur doit être configurée. Le diagramme montre que fw2 a besoin d'un lien virtuel vers fw1 avec l'ID routeur 192.168.1.1 et vice-versa. Ces liens virtuels doivent être configurés dans la zone 1.

Un cœur de réseau partitionné. L'OSPF autorise les liens virtuels vers un cœur de réseau partitionné. Le lien virtuel doit être configuré entre deux différents ABR qui touchent le cœur de réseau de chaque côté et qui partagent une zone commune.

Figure 4.3. Liens virtuels exemple 2



Le lien virtuel est configuré entre fw1 et fw2 sur la zone 1, puisqu'elle est utilisée comme zone de transit. Dans cette solution, seule l'ID routeur doit être configurée. L'exemple ci-dessus montre que fw2 nécessite un lien virtuel vers fw1 avec l'ID routeur 192.168.1.1 et vice-versa. Ces liens virtuels doivent être configurés dans la zone 1.

Assistance de haute disponibilité OSPF. Notez qu'il existe des limitations dans l'assistance de haute disponibilité pour l'OSPF :

Chacune des parties actives et inactives d'un cluster de haute disponibilité exécutent des processus OSPF différents, bien que la partie inactive assure qu'elle n'est pas le choix préféré pour le routage. Le maître et l'esclave de haute disponibilité ne forment pas de contiguïté l'un avec l'autre et ne sont pas autorisés à devenir des DR ou BDR sur un réseau de diffusion. Ceci peut être accompli en forçant la priorité du routeur à 0.

Pour que l'assistance de haute disponibilité de l'OSPF fonctionne correctement, le firewall D-Link doit posséder une interface de diffusion avec au moins UN voisin pour CHAQUE zone à laquelle le firewall est attaché. Par définition, la partie inactive du cluster doit avoir un voisin pour en obtenir la base de données link state.

Notez aussi qu'il n'est pas possible de mettre un cluster de haute disponibilité sur le même serveur de diffusion sans aucun voisin (ils ne forment pas de contiguïté ensemble parce que la priorité du routeur est à 0). Cependant, il est possible selon le scénario de paramétrer un lien de point à point entre eux. Une attention particulière doit être portée lors du paramétrage d'un lien virtuel à un firewall de haute disponibilité. Le paramétrage final du lien vers le firewall de haute disponibilité doit comporter 3 liens différents : un lien vers l'ID routeur partagée, un vers l'ID routeur du maître et un vers l'ID routeur de l'esclave du firewall.

Règles de routage dynamique

Présentation. Dans un environnement de routage dynamique, il est important que les routeurs soient capables de réguler dans quelle mesure ils participent à l'échange du routage. Il ne faut pas qu'ils acceptent ou se fient à toutes les informations de routage reçues. Il peut être crucial d'éviter que certaines parties de la base de données du routage ne soient transmises à d'autres routeurs.

C'est pour cette raison que NetDefendOS fournit des *règles de routage dynamique* qui sont utilisées pour réguler le flux des informations de routage dynamique.

Une règle de routage dynamique filtre les routes aussi bien celles configurées statiquement que celles découvertes par l'OSPF, selon des paramètres tels que l'origine des routes, la destination, la métrique et autres. Les routes correspondantes peuvent être contrôlées par des actions pour être soit exportées vers des processus OSPF, soit ajoutées à une ou plusieurs tables de routage.

Les utilisations les plus courantes des règles de routage dynamique sont :

L'importation des routes OSPF d'un processus OSPF vers une table de routage.

L'exportation des routes d'une table de routage vers un processus OSPF.

L'exportation de routes d'un processus OPSF vers un autre.

Remarque

Par défaut, NetDefendOS n'importe ni n'exporte aucune route. En d'autres termes, pour que le routage dynamique soit significatif, il est obligatoire de définir au moins une règle de routage dynamique.

Exemple 4.6. Importation de routes d'un AS OSPF vers la table de routage principale

Dans cet exemple, les routes reçues qui utilisent l'OSPF sont ajoutées dans la table de routage principale. Tout d'abord, un filtre des règles de routage dynamique doit être créé. Le filtre doit être nommé. Dans cet exemple, nous utiliserons le nom *ImportOSPFRoutes* puisqu'il explique la fonction du filtre.

Le filtre doit aussi spécifier de quel AS OSPF les routes doivent être importées. Dans cet exemple, nous utiliserons un AS OSPF préconfiguré nommé *as0*.

Selon la topologie de votre routage, vous pourriez vouloir importer seulement certaines routes en utilisant les filtres *Destination Interface/Destination Network* (Interface de destination/Réseau de destination), mais dans ce scénario toutes les routes qui sont en *tout réseau* (ce qui revient à spécifier une adresse IP *0.0.0.0/0*) sont incluses.

Interface de ligne de commande

```
gw-world:/> add DynamicRoutingRule OSPFProcess=as0 Name=ImportOSPFRoutes
   DestinationNetworkExactly=all-nets
```

Interface Web

Sélectionnez Routing > Dynamic Routing Rules > Add > Dynamic routing policy rule (Routage > Règles de routage dynamique > Ajouter > Règle de routage dynamique).

Saisissez un nom convenable pour le filtre (dans notre exemple, ImportOSPFRoutes).

Dans Select OSPF Process (Sélectionnez un processus OSPF), sélectionnez as0.

Choisissez all-nets dans le menu déroulant …Exactly Matches (…correspondances exactes).

Cliquez sur OK.

L'étape suivante consiste à créer une action de routage dynamique qui se chargera de l'importation des routes vers une table de routage. Spécifiez la table de routage de destination à laquelle les routes doivent être ajoutées (dans cet exemple, *main*).

Interface de ligne de commande

```
gw-world:/> cc DynamicRoutingRule ImportOSPFRoutes

gw-world:/ImportOSPFRoutes> add DynamicRoutingRuleAddRoute
   Destination=MainRoutingTable
```

Interface Web

Sélectionnez Routing > Dynamic Routing Rules (Routage > Règles de routage dynamique).

Cliquez sur le filtre ImportOSPFRoutes récemment créé.

Sélectionnez OSPF Routing Action > Add > DynamicRoutingRuleAddRoute (Action de routage OSPF > Ajouter > Route de règle de routage dynamique).

Dans Destination, ajoutez la table de routage principale dans la liste Selected (Sélection).

Cliquez sur OK.

Exemple 4.7. Exportation des routes par défaut vers un AS OSPF

Dans cet exemple, la route par défaut de la table de routage principale est exportée vers un AS OSPF nommé as0. Ajoutez d'abord un filtre de règles de routage dynamique qui correspond à la table de routage principale et à la route par défaut :

Interface de ligne de commande

```
gw-world:/> add DynamicRoutingRule OSPFProcess=as0 name=ExportDefRoute
   RoutingTable=MainRoutingTable DestinationInterface=wan
   DestinationNetworkExactly=all-nets
```

Interface Web

Sélectionnez Routing > Dynamic Routing Rules > Add > Dynamic routing policy rule (Routage > Règles de routage dynamique > Ajouter > Règle de routage dynamique).

Spécifiez un nom convenable pour le filtre (par exemple, *ExportDefRoute*).

Dans From Routing Table (Depuis la table de routage), sélectionnez Main Routing Table (Table de routage principale).

Choisissez wan dans Destination Interface (Interface de destination).

Choisissez all-nets dans la liste …Exactly Matches (…correspondances exactes).

Cliquez sur OK.

Puis, créez une action OSPF qui exportera la route filtrée vers l'AS OSPF spécifié :

Interface de ligne de commande

```
gw-world:/> cc DynamicRoutingRule ExportDefRoute

gw-world:/ExportDefRoute/> add DynamicRoutingRuleExportOSPF ExportToProcess=as0
```

Interface Web

Sélectionnez Routing > Dynamic Routing Rules (Routage > Règles de routage dynamique).

Cliquez sur le filtre ExportDefRoute récemment créé.

Sélectionnez OSPF Action > Add > DynamicRoutingRuleExportOSPF (Action OSPF > Ajouter > OSPF d'exportation de la règle de routage dynamique).

Dans Export to process (Exporter vers le processus), choisissez as0.

Cliquez sur OK.

Routage multidiffusion

Présentation

Certains types d'interactions sur Internet (telles que les conférences en ligne et la diffusion de vidéos) impliquent qu'un seul client ou hôte envoie le même paquet à plusieurs récepteurs. Ce scénario est possible grâce à la duplication du paquet avec des adresses IP différentes par l'émetteur ou grâce à la diffusion du paquet sur Internet. Ces solutions gaspillent énormément les ressources de l'émetteur ou la bande passante du réseau. Elles ne sont

donc pas satisfaisantes. Une solution appropriée devrait aussi être capable de réguler le grand nombre de récepteurs.

Le routage multidiffusion résout ce problème grâce aux routeurs du réseau eux-mêmes, qui dupliquent et transmettent les paquets via une route optimale à tous les membres d'un groupe. Les standards IETF qui autorisent le routage multidiffusion sont :

Classe D de la plage d'adresses IP dédiée au trafic multidiffusion. Chaque adresse IP à multidiffusion représente un groupe arbitraire de récepteurs.

L'IGMP (Internet Group Membership Protocol) autorise un récepteur à annoncer au réseau qu'il est membre d'un groupe de multidiffusion particulier.

Le PIM (Protocol Independent Multicast) est un groupe de protocoles de routage qui déterminent le chemin optimal à emprunter pour les paquets de multidiffusion.

Le routage multidiffusion fonctionne selon le principe où un récepteur intéressé rejoint un groupe de multidiffusion en utilisant le protocole IGMP. Les routeurs PIM peuvent alors dupliquer et transmettre les paquets à tous les membres de ce groupe de multidiffusion, ce qui crée un *arbre de distribution* pour le flux du paquet. Plutôt que d'acquérir de nouvelles informations sur le réseau, le PIM utilise les informations de routage des protocoles déjà existants, tels que l'OSPF, pour choisir le chemin optimal.

L'un des mécanismes clé dans le processus de routage multidiffusion est le *Reverse Path Forwarding* (Transmission par chemin inverse). Pour le trafic à diffusion unique, le routeur ne s'intéresse qu'à la destination du paquet. Avec l'envoi en multidiffusion, le routeur s'intéresse aussi à la source du paquet puisqu'il transmet le paquet sur des chemins de sens descendant depuis la source. Cette approche est adoptée pour éviter les boucles dans l'arbre de distribution.

Par défaut, les paquets de multidiffusion sont routés par NetDefendOS jusqu'à l'interface du noyau. Les règles SAT Multiplex sont paramétrées dans l'ensemble de règles IP pour réaliser la transmission vers les bonnes interfaces. Une démonstration de cette situation apparaît dans les exemples qui suivent.

Remarque

Pour que l'envoi en multidiffusion fonctionne sur une interface Ethernet avec n'importe quel firewall D-Link, cette interface doit avoir le paramètre multidiffusion sur On ou Auto. Pour plus de détails, veuillez consulter la section intitulée « Ethernet ».

Transfert multidiffusion avec règle SAT Multiplex

La règle SAT Multiplex est utilisée pour effectuer la duplication et la transmission des paquets au travers de plusieurs interfaces. Cette fonctionnalité applique le transfert multidiffusion dans NetDefendOS, grâce auquel un paquet de multidiffusion est envoyé via plusieurs interfaces. Notez que si cette règle outrepasse les tables de routage normales, les paquets qui doivent être dupliqués par la règle multiplex sont nécessairement routés vers l'interface du noyau.

Par défaut, les adresses IP à multidiffusion **224.0.0.0/4** sont toujours routées vers le noyau et ne doivent pas être ajoutées manuellement aux tables de routage. Chaque interface de sortie spécifiée peut être configurée séparément avec une traduction statique de l'adresse de destination. Le champ Interface dans la boîte de dialogue Interface/Net Tuple (N-uplet réseau) peut être vide si le champ IPAddress (Adresse IP) est paramétré. Dans ce cas, l'interface de sortie est déterminée lors d'une recherche de route sur l'adresse IP spécifiée.

La règle multiplex peut fonctionner selon deux modes :

Use IGMP (Avec IGMP) Les hôtes qui utilisent l'IGMP doivent requérir le flux de trafic spécifié par la règle multiplex avant que tout paquet de multidiffusion ne soit transmis au travers des interfaces spécifiées. C'est le comportement par défaut de NetDefendOS.

Not Using IGMP (Sans IGMP) Le flux de trafic est transféré directement par les interfaces spécifiées sans aucune interférence de l'IGMP.

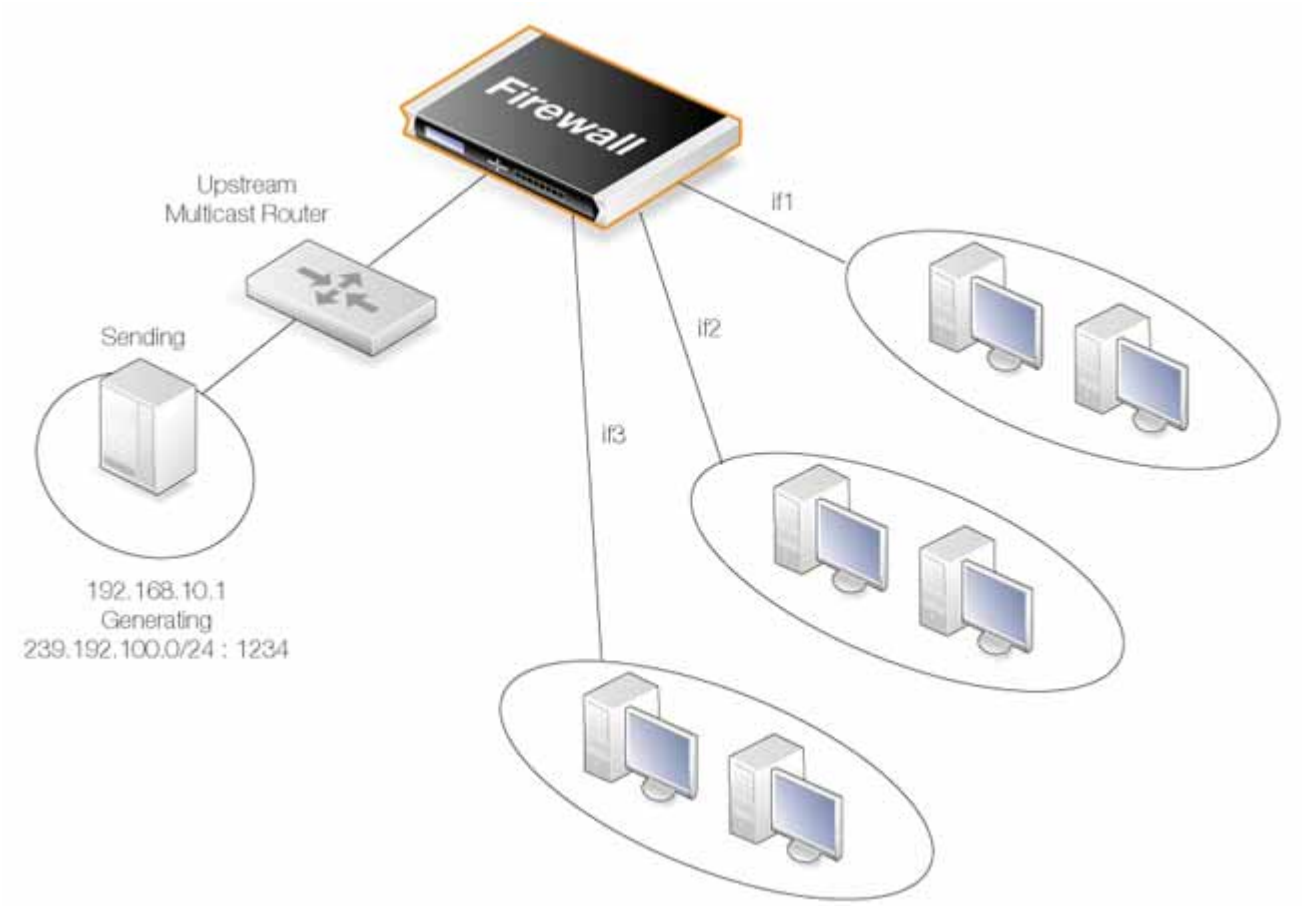
Remarque

Puisque la règle multiplex est une règle SAT, une règle Allow ou NAT doit être spécifiée avec la règle multiplex.

Transfert multidiffusion sans traduction d'adresses

Ce scénario indique comment configurer le transfert multidiffusion avec IGMP. L'émetteur de multidiffusion est **192.168.10.1** et génère un flux de multidiffusion **239.192.10.0/24 :1234**. Ces flux doivent être transférés depuis une interface wan en traversant les interfaces if1, if2 et if3. Les flux doivent être transférés uniquement si certains hôtes ont requis les flux avec le protocole IGMP. L'exemple ci-dessous ne traite que de la configuration du transfert multidiffusion. La configuration de l'IGMP est consultable dans la section intitulée « Configuration de règles IGMP sans traduction d'adresses ».

Figure 4.4. Transfert multidiffusion sans traduction d'adresses



Remarque

Pensez bien à ajouter une règle Allow qui correspond à la règle SAT multiplex.

Exemple 4.8. Transfert de trafic multidiffusion avec règle SAT multiplex

Dans cet exemple, nous allons créer une règle multiplex afin de transférer les groupes de multidiffusion **239.192.10.0/24:1234** vers les interfaces if1, if2 et if3. Tous les groupes ont le même émetteur **192.168.10.1**, situé derrière l'interface wan. Les groupes de multidiffusion doivent uniquement être transférés vers les interfaces de sortie si des clients derrière ces interfaces ont requis l'utilisation de l'IGMP. La procédure suivante doit être respectée pour configurer le transfert du trafic multidiffusion. L'IGMP doit être configuré à part.

Interface Web

A. Créez un service personnalisé pour l'envoi en multidiffusion nommé *multicast_service* :

Sélectionnez Objects > Services > Add > TCP/UDP (Objets > Services > Ajouter > TCP/UDP).

Saisissez :

Name (nom) : multicast_service

Type : UDP

Destination : 1234

B. Créez une règle IP :

Sélectionnez Rules > IP Rules > Add > IP Rule (Règles > Règles IP > Ajouter > Règle IP).

Sous General (Général), entrez :

Name (nom) : un nom pour la règle (par exemple, *Multicast_Multiplex)*

Action : Multiplex SAT

Service: multicast_service

Sous Address Filter (Filtre d'adresses), entrez :

Source Interface (Interface source) : wan

Source Network (Réseau source) : 192.168.10.1

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : 239.192.10.0/24

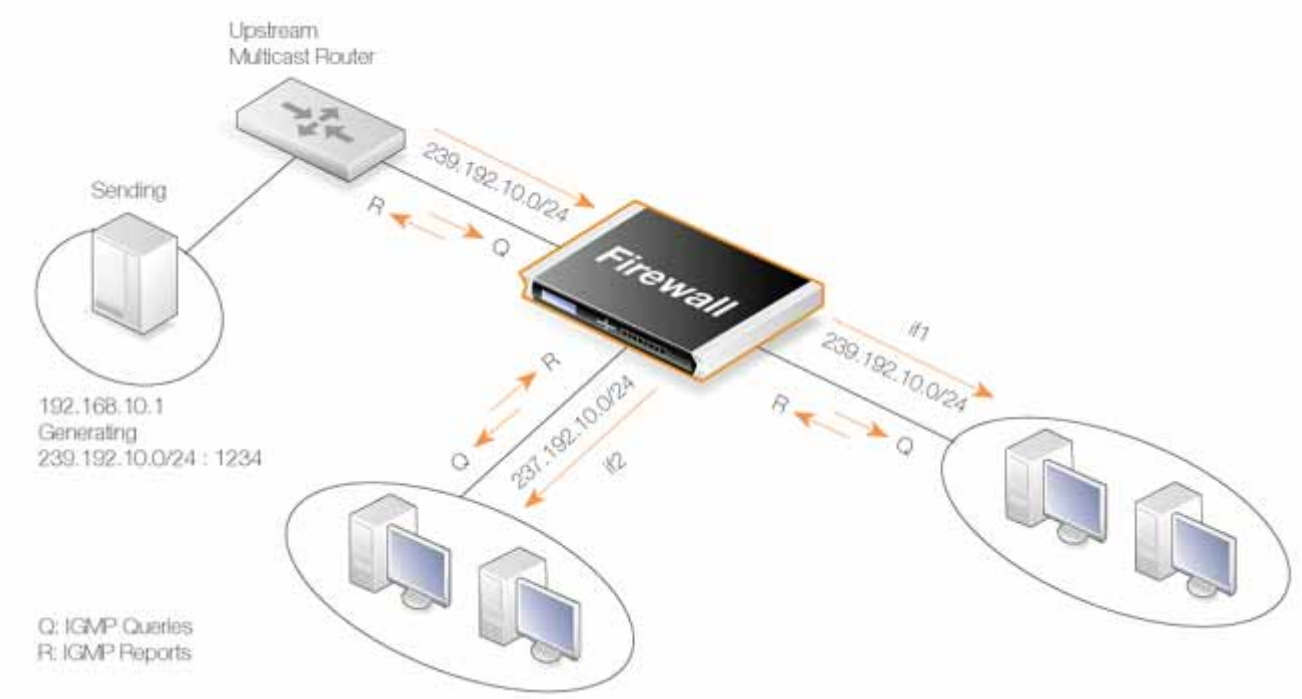
Cliquez sur l'onglet Multiplex SAT et ajoutez les interfaces de sortie if1, if2 et if3 une par une. Pour chaque interface, laissez le champ IP Address (Adresse IP) vide puisqu'aucune traduction d'adresses de destination n'est requise.

Assurez-vous d'avoir activé le transfert avec IGMP.

Cliquez sur OK.

Transfert multidiffusion avec traduction d'adresses

Figure 4.5. Transfert multidiffusion avec traduction d'adresses



Ce scénario se base sur le scénario précédent à l'exception que nous allons traduire le groupe de multidiffusion. Lorsque les flux de multidiffusion **239.192.10.0/24** sont transférés via l'interface if2, les groupes de multidiffusion doivent être traduits en **237.192.10.0/24**. Aucune traduction d'adresses ne doit être faite lors d'un transfert via l'interface if1. La configuration des règles IGMP correspondantes est consultable dans la section intitulée « Configuration de règles IGMP avec traduction d'adresses ».

Attention

Comme indiqué précédemment, pensez à ajouter une règle Allow qui correspond à la règle SAT multiplex.

Figure 4.9. Transfert multidiffusion avec traduction d'adresses

La règle SAT multiplex suivante doit être configurée pour correspondre au scénario décrit ci-dessus :

Interface Web

A. Créez un service personnalisé pour l'envoi en multidiffusion nommé *multicast_service* :

Sélectionnez Objects > Services > Add > TCP/UDP (Objets > Services > Ajouter > TCP/UDP).

Saisissez :

Name (nom) : multicast_service

Type : UDP

Destination : 1234

B. Créez une règle IP :

Sélectionnez Rules > IP Rules > Add > IP Rule (Règles > Règles IP > Ajouter > Règle IP).

Sous General (Général), entrez :

Name (nom) : un nom pour la règle, par exemple *Multicast_Multiplex*

Action : Multiplex SAT

Service: multicast_service

Sous Address Filter (Filtre d'adresses), entrez :

Source Interface (Interface source) : wan

Source Network (Réseau source) : 192.168.10.1

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : 239.192.10.0/24

Cliquez sur l'onglet Address Translation (Traduction d'adresses).

Ajoutez l'interface if1, mais laissez l'IPAddress (Adresse IP) vide.

Ajoutez l'interface if2, mais cette fois entrez 237.192.10.0 comme adresse IP.

Assurez-vous d'avoir activé le transfert avec IGMP.

Cliquez sur OK.

Remarque

Si la traduction de l'adresse source est requise, la règle Allow qui suit la règle SAT Multiplex doit être remplacée par une règle NAT.

Configuration IGMP

La signalisation IGMP entre les hôtes et les routeurs peut être divisée en deux catégories :

IGMP Reports (Rapports IGMP) Des rapports sont envoyés depuis les hôtes vers les routeurs lorsqu'un hôte veut souscrire à un nouveau groupe de multidiffusion ou modifier ses actuelles souscriptions de multidiffusion.

IGMP Queries (Requêtes IGMP) Les requêtes sont des messages IGMP émis par le routeur à destination des hôtes afin de s'assurer qu'aucun flux attendu par un hôte ne sera interrompu.

Normalement, ces deux types de règles doivent être spécifiés pour que l'IGMP fonctionne. Il existe une exception : si la source de multidiffusion est située sur un réseau directement connecté au routeur. Dans ce cas, il n'y a pas besoin d'une règle de requête.

Voici une autre exception : si un routeur voisin est configuré statiquement pour délivrer un flux de multidiffusion vers le firewall D-Link. Là encore, il est inutile de spécifier une requête IGMP.

NetDefendOS est compatible avec deux modes de fonctionnement d'IGMP : surveillance et Proxy.

Figure 4.6. Surveillance multicast

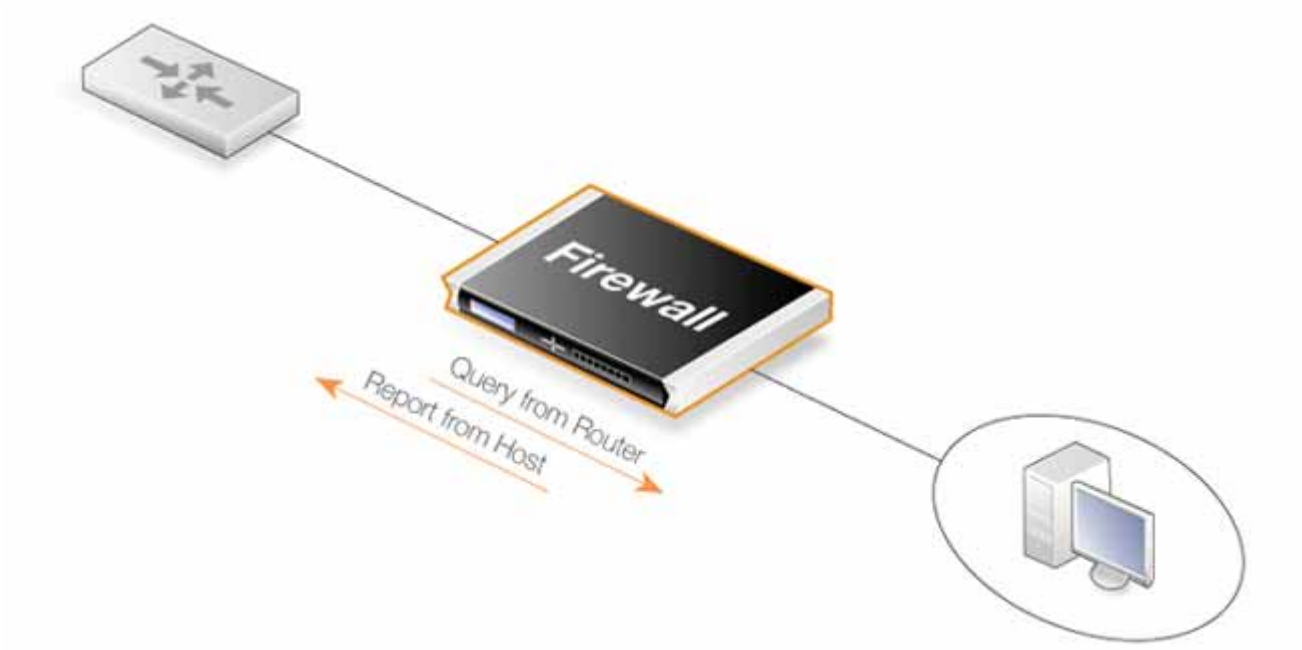
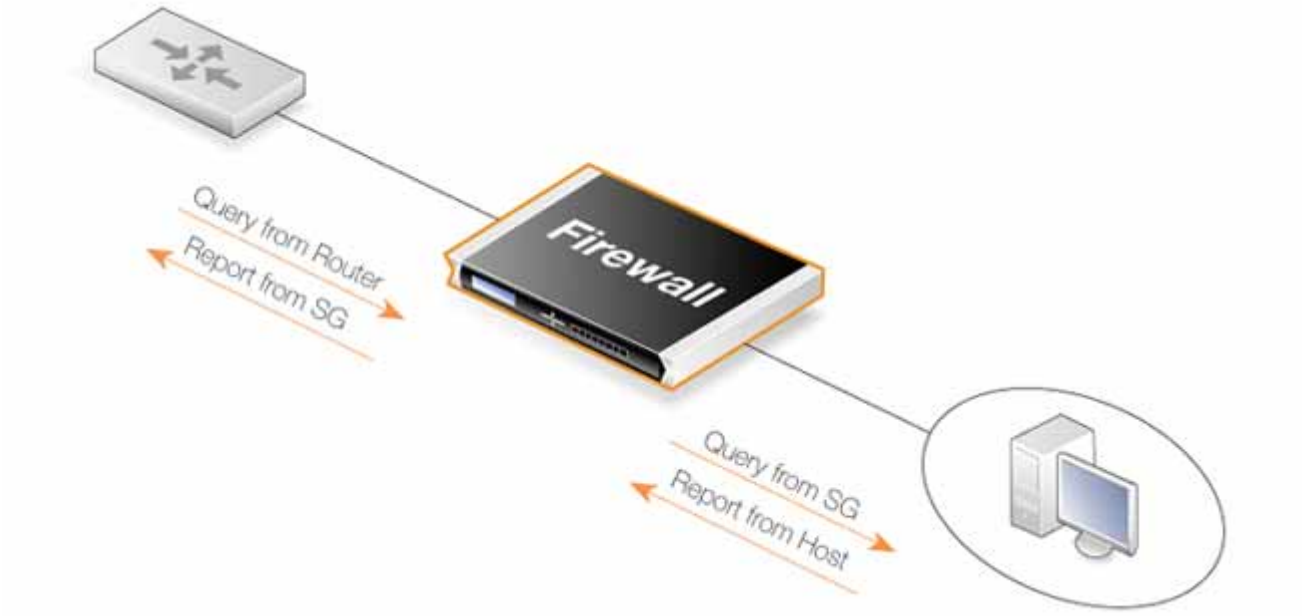


Figure 4.7. Proxy de multidiffusion



En mode surveillance, le routeur agit de manière transparente entre l'hôte et un autre routeur IGMP. Il n'envoie aucune requête IGMP. Il se contente de transférer les requêtes et les rapports entre l'autre routeur et l'hôte. En mode Proxy, le routeur agit comme un routeur IGMP envers les clients et envoie des requêtes de manière active. Envers le routeur émetteur, il agit comme un hôte normal qui souscrit à des groupes de multidiffusion à la place de ses clients.

Configuration des règles IGMP sans traduction d'adresses

Cet exemple décrit les règles IGMP nécessaires pour configurer l'IGMP selon le scénario sans traduction d'adresses décrit ci-dessus. Nous voulons que le routeur agisse comme un hôte envers le routeur émetteur. Il faut donc configurer l'IGMP pour qu'il fonctionne en mode proxy.

Exemple 4.10. IGMP sans traduction d'adresses

L’exemple suivant requiert un groupe d’interfaces configuré, IfGrpClients, qui comprend les interfaces if1, if2 et if3. L’adresse IP du routeur IGMP émetteur est connue en tant que UpstreamRouterIP.
Nous avons besoin de deux règles. La première est une règle de rapport qui permet aux clients se situant derrière les interfaces if1, if2 et if3 de souscrire au groupe de multidiffusion **239.192.10.0/24**. La deuxième est une règle de requête qui permet au routeur émetteur de nous envoyer une requête pour les groupes de multidiffusion que les clients demandent. La procédure suivante doit être respectée pour créer ces deux règles :

Interface Web

A. Créez la première règle IGMP.

Sélectionnez Routing > IGMP > IGMP Rules > Add > IGMP Rule (Routage > IGMP > Règles IGMP > Ajouter > Règle IGMP).

Sous General (Général), entrez :

Name (nom) : un nom qui convient pour la règle (par exemple, *Reports)*.

Type : Report (Rapport)

Action : Proxy

Output (Sortie) : wan *(qui est l’interface relais)*

Sous Address Filter (Filtre d’adresses), entrez :

Source Interface (Interface source) : lfGrpClients

Source Network (Réseau source) : if1net, if2net, if3net

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : auto

Multicast Source (Source de multidiffusion) : 192.168.10.1

Multicast Group (Groupe de multidiffusion) : 239.192.10.0/24

Cliquez sur OK.

B. Créez la deuxième règle IGMP :

Retournez dans Routing > IGMP > IGMP Rules > Add > IGMP Rule (Routage > Règles IGMP > Ajouter > Règle IGMP).

Sous General (Général), entrez :

Name (nom) : un nom qui convient pour la règle (par exemple, *Queries*).

Type : Query (Requête)

Action : Proxy

Output (Sortie) : IfGrpClients *(qui est l’interface de relais)*

Sous Address Filter (Filtre d’adresses), entrez :

Source Interface (Interface source) : wan

Source Network (Réseau source) : UpstreamRouterIp (IP du routeur émetteur)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : auto

Multicast Source (Source de multidiffusion) : 192.168.10.1

Multicast Group (Groupe de multidiffusion) : 239.192.10.0/24

Cliquez sur OK.

Configuration des règles IGMP avec traduction d'adresses

Les exemples suivant indiquent les règles IGMP nécessaires pour configurer l'IGMP selon le scénario de traduction d'adresses décrit dans la section intitulée « Transfert multicast avec traduction d'adresses ». Deux règles de rapport IGMP sont nécessaires, c'est-à-dire une pour chaque interface client. If1 ne fait pas de traduction d'adresses et if2 traduit le groupe de multidiffusion en **237.192.10.0/24**. Deux règles de requête sont aussi nécessaires : une pour l'interface et l'adresse traduites, l'autre pour l'envoi de l'adresse d'origine vers if1.

Vous trouverez ci-après deux exemples, un pour chaque paire de règle. Le routeur qui émet en multidiffusion utilise l'IP UpstreamRouterIP.

Exemple 4.11. Configuration de if1

La procédure suivante doit être respectée pour créer la paire de règles de rapport et de requête pour if1 qui n'utilise pas de traduction d'adresses.

Interface Web

A. Créez la première règle IGMP.

Sélectionnez Routing > IGMP > IGMP Rules > Add > IGMP Rule (Routage > IGMP > Règles IGMP > Ajouter > Règle IGMP).

Sous General (Général), entrez :

Name (nom) : un nom qui convient pour la règle (par exemple, *Reports_if1*).

Type : Report (Rapport)

Action : Proxy

Output (Sortie) : wan *(qui est l'interface relais)*

Sous Address Filter (Filtre d'adresses), entrez :

Source Interface (Interface source) : if1

Source Network (Réseau source) : if1net

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : auto

Multicast Source (Source de multidiffusion) : 192.168.10.1

Multicast Group (Groupe de multidiffusion) : 239.192.10.0/24

Cliquez sur OK.

B. Créez la deuxième règle IGMP :

Retournez dans Routing > IGMP > IGMP Rules > Add > IGMP Rule (Routage > Règles IGMP > Ajouter > Règle IGMP).

Sous General (Général), entrez :

Name (nom) : un nom qui convient pour la règle (par exemple, *Queries_if1*).

Type : Query (Requête)

Action : Proxy

Output (Sortie) : if1 *(qui est l'interface relais)*

Sous Address Filter (Filtre d'adresses), entrez :

Source Interface (Interface source) : wan

Source Network (Réseau source) : UpstreamRouterIp (IP du routeur émetteur)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : auto

Multicast Source (Source de multidiffusion) : 192.168.10.1

Multicast Group (Groupe de multidiffusion) : 239.192.10.0/24

Cliquez sur OK.

Exemple 4.12. Configuration d'if2 et traduction de groupe

La procédure suivante doit être respectée pour créer la paire de règles de rapport et de requête pour if2 qui fait la traduction du groupe de multidiffusion. Notez que le groupe traduit et que les rapports IGMP incluent donc les adresses IP traduites. Les requêtes contiennent les adresses IP d'origine.

Interface Web

A. Créez la première règle IGMP.

Sélectionnez Routing > IGMP > IGMP Rules > Add > IGMP Rule (Routage > IGMP > Règles IGMP > Ajouter > Règle IGMP).

Sous General (Général), entrez :

Name (nom) : un nom qui convient pour la règle (par exemple, *Reports_if2*).

Type : Report (Rapport)

Action : Proxy

Output (Sortie) : wan *(qui est l'interface relais)*

Sous Address Filter (Filtre d'adresses), entrez :

Source Interface (Interface source) : if2

Source Network (Réseau source) : if2net

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : auto

Multicast Source (Source de multidiffusion) : 192.168.10.1

Multicast Group (Groupe de multidiffusion) : 239.192.10.0/24

Cliquez sur OK.

B. Créez la deuxième règle IGMP :

Retournez dans Routing > IGMP > IGMP Rules > Add > IGMP Rule (Routage > Règles IGMP > Ajouter >

Règle IGMP).

Sous General (Général), entrez :

Name (nom) : un nom qui convient pour la règle, par exemple : *Queries_if1*.

Type : Query (Requête)

Action : Proxy

Output (Sortie) : if2 *(qui est l'interface relais)*

Sous Address Filter (Filtre d'adresses), entrez :

Source Interface (Interface source) : wan

Source Network (Réseau source) : UpstreamRouterIp (IP du routeur émetteur)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : auto

Multicast Source (Source de multidiffusion) : 192.168.10.1

Multicast Group (Groupe de multidiffusion) : 239.192.10.0/24

Cliquez sur OK.

Paramètres IGMP avancés

Il y a beaucoup de paramètres avancés qui englobent et s'appliquent à toutes les interfaces qui n'ont pas de paramètres IGMP explicitement spécifiés. Ces paramètres globaux sont consultables dans le *Chapitre 13, Paramètres avancés*. Les paramètres individuels sont quant à eux consultables dans la section IGMP de l'interface d'administration.

Mode transparent

Présentation du mode transparent

Le fait de déployer des firewalls D-Link qui fonctionnent en mode transparent dans une topologie de réseau préexistante peut renforcer sa sécurité. Cette solution est simple à réaliser et ne requiert aucune reconfiguration des modes préexistants. Une fois déployé, NetDefendOS peut autoriser ou refuser l'accès à différents types de services (par exemple, le HPPT) et dans des directions spécifiées. Tant que les utilisateurs du réseau accèdent à des services autorisés avec le firewall D-Link, ils ne ressentent pas sa présence. Le fait de spécifier une route de commutation à la place d'une route standard active le mode transparent.

La capacité du mode transparent à accroître la sécurité trouve l'une de ses applications en environnement d'entreprise, où il peut être nécessaire de protéger les différents services les uns des autres. Le service financier peut n'avoir besoin d'accéder qu'à un petit panel de services (HTTP par exemple) sur le serveur du service des ventes et le service des ventes n'avoir besoin d'accéder qu'à un petit panel d'applications sur le réseau du service financier. En ne déployant qu'un seul firewall D-Link entre les réseaux de ces deux départements, un accès transparent mais contrôlé peut être obtenu grâce au mode transparent.

Un autre exemple peut être celui d'une organisation qui autorise le trafic entre l'Internet externe et un ensemble d'adresses IP publiques sur un réseau interne. Le mode transparent peut contrôler le type de services qui sont autorisés pour ces adresses IP et dans quelle direction. Par exemple, les seuls services autorisés dans une telle situation seraient l'accès HTTP vers l'Internet.

Comparaison avec le mode routage

Le firewall D-Link peut fonctionner sous deux modes : le mode routage ou le mode transparent. En mode routage,

le firewall D-Link a toutes les fonctionnalités d'un routeur L3 (Layer 3). Si le firewall est installé pour la première fois sur un réseau ou si la topologie du réseau change, la configuration du routage doit donc être consciencieusement vérifiée pour s'assurer que la table de routage est compatible avec la nouvelle structure. Une reconfiguration des paramètres IP peut être requise pour les routeurs déjà présents et les serveurs protégés. Le fonctionnement de ce mode est adapté lorsqu'un contrôle complet du routage est souhaité.

En mode transparent, une route de commutation est empruntée plutôt qu'une Route. Le firewall agit donc presque à la manière d'un switch : il filtre les paquets IP et les transfère de manière transparente jusqu'à la bonne interface sans modifier les informations de source ni de destination au niveau de l'IP ou d'Ethernet. Ce mode transparent présente deux avantages :

Lorsqu'un client change d'interface sans changer d'adresse IP, il peut encore avoir accès aux mêmes services qu'avant (par exemple HTTP, FTP) sans devoir reconfigurer le routage.

Le même type d'adresse réseau peut exister sur plusieurs interfaces.

Remarque

Les firewalls D-Link ne doivent pas nécessairement fonctionner en mode transparent mais peuvent combiner le mode transparent avec le mode routage pour fonctionner en mode hybride. Ainsi, le firewall peut aussi bien être défini sur des routes de commutation que sur des routes standard. Il est aussi possible de créer une solution hybride en appliquant la traduction d'adresses sur un tout autre trafic transparent.

Mise en œuvre du mode transparent

En mode transparent, NetDefendOS autorise aux transactions ARP le passage au travers du firewall D-Link et détermine grâce à ce trafic ARP la relation entre les adresses IP, les adresses physiques et les interfaces. NetDefendOS enregistre ces adresses afin de relayer les paquets d'IP vers le bon récepteur. Lors des transactions ARP, ni la source ni le destinataire ne se rendra compte de la présence du firewall.

Au début de la communication, un hôte localise l'adresse physique de l'hôte de destination en diffusant une requête ARP. Cette requête est interceptée par NetDefendOS qui paramètre une entrée ARP Transaction State (État de transaction ARP) et diffuse la requête ARP vers toutes les autres interfaces switch-routes, à l'exception de l'interface de réception de la requête ARP. Si NetDefendOS reçoit une réponse ARP de la destination durant une période de temps configurable, il relaiera la réponse à l'émetteur de la requête en utilisant les informations précédemment stockées dans l'entrée ARP Transaction State (État de transaction ARP).

Lors de la transaction ARP, NetDefendOS intègre les adresses source des émetteurs de la requête et de la réponse. NetDefendOS utilise deux tables pour stocker ces informations : la table de mémoire à contenu adressable (CAM) et le cache L3. La table CAM suit les adresses MAC disponibles sur une interface donnée et le cache L3 mappe une adresse IP avec une adresse MAC et une interface. Puisque le cache L3 est uniquement utilisé pour le trafic IP, ses entrées sont stockées comme appartenant à un hôte unique sur la table de routage.

Pour chaque paquet d'IP qui passe par le firewall D-Link, une recherche de route vers la destination est effectuée. Si la route du paquet correspond à une route de commutation ou à une entrée du cache L3 dans la table de routage, NetDefendOS sait qu'il doit se charger de ce paquet d'une manière transparente. Si une interface de destination et une adresse MAC sont disponibles sur une route, NetDefendOS a les informations nécessaires pour transférer le paquet vers sa destination. Si la route est une route de commutation, aucune information spécifique sur la destination n'est disponible et le firewall doit découvrir la localisation de la destination sur le réseau. NetDefendOS effectue cette recherche en envoyant des requêtes ARP et ICMP (ping), comme s'il était l'émetteur du paquet IP d'origine vers la destination sur les interfaces spécifiées dans la route de commutation. Si une réponse ARP est reçue, NetDefendOS mettra à jour la table CAM et le cache L3 et transférera le paquet jusqu'à sa destination.

Si la table CAM ou le cache L3 sont saturés, les tables sont automatiquement alignées de manière partielle. Grâce au mécanisme de recherche qui consiste à envoyer des requêtes ARP et ICMP, NetDefendOS découvre les destinations qui ont pu être alignées.

Activation du mode transparent

Deux étapes sont normalement requises pour que NetDefendOS puisse fonctionner en mode transparent :

Si vous le souhaitez, créez un groupe des interfaces qui doivent être transparentes. Les interfaces d'un groupe peuvent être marquées comme équivalent sécurité/transport si les hôtes doivent pouvoir se déplacer librement entre eux.

Créez des routes de commutation et s'il est en fonction, utilisez le groupe d'interfaces créé plus tôt. En ce qui concerne le paramètre Network (Réseau), spécifiez la plage d'adresses IP qui seront considérées comme transparentes entre les interfaces. Lorsque le firewall entier fonctionne en mode transparent, cette plage est normalement *all-nets* (tout réseau).

Haute disponibilité avec mode transparent

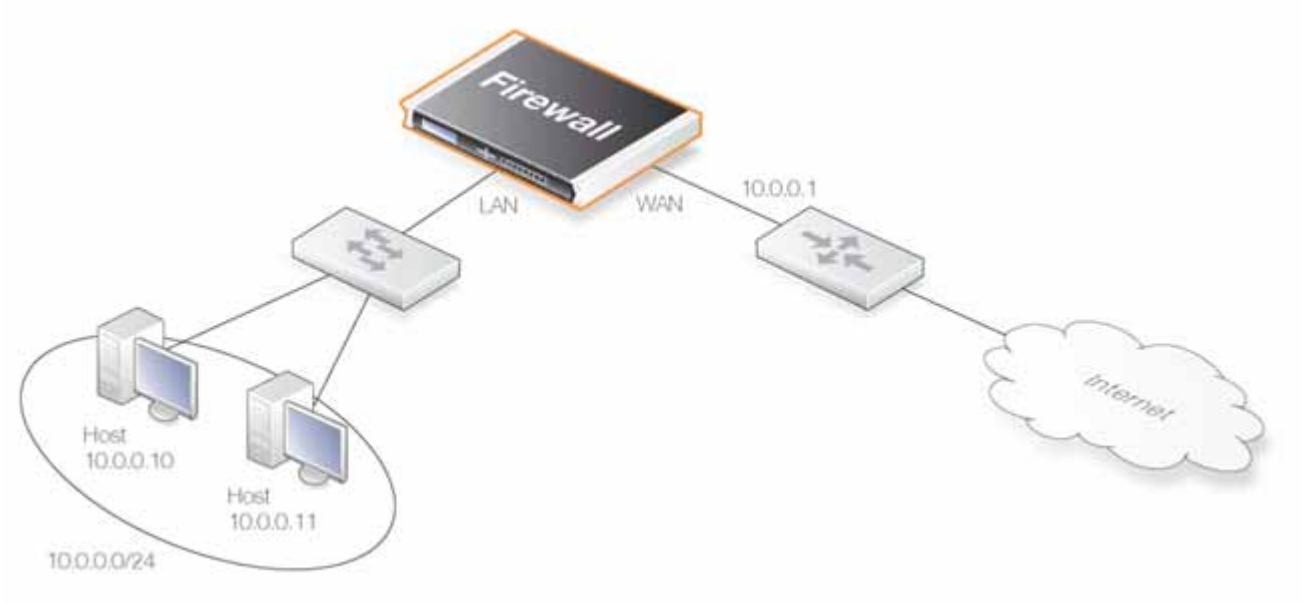
Les routes de commutation ne peuvent pas être utilisées en haute disponibilité. Un vrai mode transparent ne peut donc pas être mis en application dans un cluster de haute disponibilité de NetDefendOS.

À la place de routes de commutation, la solution pour un paramétrage de haute disponibilité consiste à utiliser un proxy ARP pour séparer deux réseaux. Cette manipulation est décrite plus en détail dans la section intitulée « Proxy ARP ». L'inconvénient clé de cette approche est que les clients ne peuvent pas voyager à travers les interfaces NetDefendOS en conservant la même adresse IP.

Scénarios de mode transparent

Scénario 1. Le firewall en mode transparent est placé entre le routeur d'accès à Internet et le réseau interne. Le routeur est utilisé pour partager la connexion Internet avec une adresse IP publique unique. Le réseau interne NAT derrière le firewall se définit sur la plage d'adresses 10.0.0.0/24. L'accès Internet est autorisé aux clients du réseau interne via le protocole HTTP.

Figure 4.8. Scénario 1 du mode transparent



Exemple 4.13. Scénario 1 : paramétrage du mode transparent

Interface Web
Configurez les interfaces :

Sélectionnez Interfaces > Ethernet > Edit (wan) (Interfaces > Ethernet > Modifier (wan)).

Saisissez :

IP Address (Adresse IP) : 10.0.0.1

Network (Réseau) : 10.0.0.0/24

Default Gateway (Passerelle par défaut) : 10.0.0.1

Transparent Mode (Mode transparent) : Enable (Activer)

Cliquez sur OK.

Sélectionnez Interfaces > Ethernet > Edit (lan) (Interfaces > Ethernet > Modifier (lan)).

Saisissez :

IP Address (Adresse IP) : 10.0.0.2

Network (Réseau) : 10.0.0.0/24

Transparent Mode (Mode transparent) : Enable(Activer)

Cliquez sur OK.

Configurez les règles :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): HTTPAllow

Action : Allow (Autoriser)

Service: http

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : any (toutes)

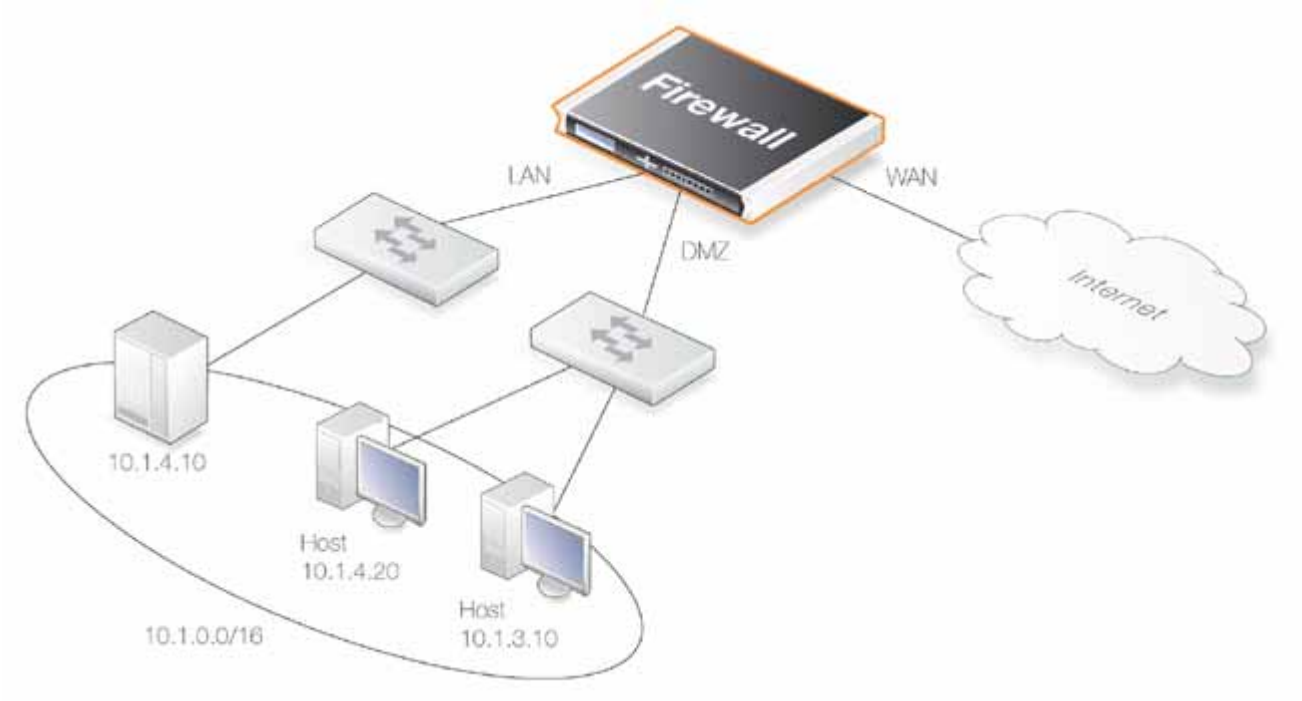
Source Network (réseau source) : 10.0.0.0/24

Destination Network (Réseau de destination) : all-nets (0.0.0.0/0)

Cliquez sur OK.

Scénario 2. Ici, le firewall D-Link en mode transparent sépare les ressources serveur d'un réseau interne en les connectant à une interface tierce avoir à utiliser des plages d'adresses différentes.

Figure 4.9. Scénario 2 du mode transparent



Tous les hôtes connectés à LAN et DMZ (les interfaces lan et dmz) partagent la plage d'adresses 10.0.0.0/24. Puisque ceci est configuré avec le mode transparent, n'importe quelle adresse IP peut être utilisée pour les serveurs et il n'est pas nécessaire que les hôtes du réseau internet sachent si une ressource se trouve sur le même réseau ou sur le DMZ. Les hôtes du réseau interne sont autorisés à communiquer avec un serveur HTTP sur le DMZ alors que ces derniers peuvent être atteints depuis Internet. Le firewall est transparent entre le DMZ et le LAN alors que le trafic est soumis à l'ensemble de règles IP.

Exemple 4.14. Scénario 2 : paramétrage du mode transparent

Configurez une route de commutation sur les interfaces LAN et DMZ pour la plage d'adresses 10.0.0.0/24 (en supposant que l'interface WAN est déjà configurée).

Configurez les interfaces :

Comme indiqué dans l'exemple précédent, vous devez d'abord spécifier les interfaces *lan* et *dmz* impliquées en utilisant les adresses IP données en exemple dans ce scénario.

Groupes d'interfaces :

Suivez les indications données dans l'exemple précédent. Configurez les interfaces *lan* et *dmz* dans le même groupe.

Switch Route (Route de commutation) :

Suivez les indications données dans l'exemple précédent. Paramétrez la route de commutation selon le nouveau groupe d'interfaces créé plus tôt.
Configurez les règles :

Sélectionnez Rules > New Rule (Règles > Nouvelle règle).

La boîte de dialogue Rule Properties (Propriétés de la règle) s'affiche.

Saisissez un nom qui convient pour la règle (par exemple, *HTTP-LAN-to-DMZ*).

Saisissez ensuite :

Action : Allow (Autoriser)

Source Interface (interface source) : lan

Destination Interface (Interface de destination) : dmz

Source Network (réseau source) : all-nets (tout réseau)

Destination Network (Réseau de destination) : 10.1.4.10

Sous l'onglet Service, choisissez *http* dans Pre-defined control (Contrôle prédéfini).

Cliquez sur OK

Sélectionnez Rules > New Rule (Règles > Nouvelle règle).

La boîte de dialogue Rule Properties (Propriétés de la règle) s'affiche.

Saisissez un nom qui convient pour la règle (par exemple, *HTTP-WAN-to-DMZ).*

Saisissez ensuite :

Action : SAT

Source Interface (interface source) : wan

Destination Interface (Interface de destination) : dmz

Source Network (réseau source) : all-nets (tout réseau)

Destination Network (Réseau de destination) : wan_ip

Sous l'onglet Service, choisissez *http* dans Pre-defined control (Contrôle prédéfini).

Sous l'onglet Address Translation (Traduction d'adresses), choisissez *Destination IP Address* (Adresse IP de destination) et entrez 10.1.4.10 dans New IP Address control (Contrôle de la nouvelle adresse IP).

Cliquez sur OK.

Sélectionnez Rules > New Rule (Règles > Nouvelle règle).

La boîte de dialogue Rule Properties (Propriétés de la règle) s'affiche.

Saisissez un nom qui convient pour la règle, par exemple *HTTP-LAN-to-DMZ.*

Saisissez ensuite :

Action : Allow (Autoriser)

Source Interface (interface source) : wan

Destination Interface (Interface de destination) : dmz

Source Network (réseau source) : all-nets (tout réseau)

Destination Network (Réseau de destination) : wan_ip

Sous l'onglet Service, choisissez *http* dans le Pre-defined control (Contrôle prédéfini).

Cliquez sur OK.

Interface Web
Configurez les interfaces :

Sélectionnez Interfaces > Ethernet > Edit (lan) (Interfaces > Ethernet > Modifier (lan)).

Saisissez :

IP Address (Adresse IP) : 10.0.0.1

Network (Réseau) : 10.0.0.0/24

Transparent Mode (Mode transparent) : Disable (Désactivé)

Add route for interface network (Ajout d’une route dans le réseau d’interface) : Disable (Désactivé)

Cliquez sur OK.

Sélectionnez Interfaces > Ethernet > Edit (dmz) (Interfaces > Ethernet > Modifier (dmz)).

Saisissez :

IP Address (Adresse IP) : 10.0.0.2

Network (Réseau) : 10.0.0.0/24

Transparent Mode (Mode transparent) : Disable (Désactivé)

Add route for interface network (Ajout d’une route dans le réseau d’interface) : Disable (Désactivé)

Cliquez sur OK.

Configurez les groupes d’interfaces :

Sélectionnez Interfaces > Interface Groups > Add > InterfaceGroup (Interfaces > Groupes d’interfaces > Ajouter > Groupe d’interfaces).

Saisissez :

Name (nom): TransparentGroup

Security/Transport Equivalent (Équivalent sécurité/transport) : Disable (Désactivé)

Interfaces : sélectionnez lan et dmz

Cliquez sur OK.

Configurez le routage :

Sélectionnez Routing > Main Routing Table > Add > SwitchRoute (Routage > Table de routage principale > Ajouter > Route de commutation).

Saisissez :

Switched Interfaces (Interfaces commutées) : TransparentGroup

Network (Réseau) : 10.0.0.0/24

Metric (Métrique) : 0

Cliquez sur OK.

Configurez les règles :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): HTTP-LAN-to-DMZ

Action : Allow (Autoriser)

Service: http

Source Interface (interface source) : lan

Destination Interface (Interface de destination) : dmz

Source Network (réseau source) : 10.0.0.0/24

Destination Network (Réseau de destination) : 10.1.4.10

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): HTTP-WAN-to-DMZ

Action : SAT

Service: http

Source Interface (interface source) : wan

Destination Interface (Interface de destination) : dmz

Source Network (réseau source) : all-nets (tout réseau)

Destination Network (Réseau de destination) : wan_ip

Translate (Traduire) : sélectionnez Destination IP (IP de destination).

New IP Address (Nouvelle adresse IP) : 10.1.4.10

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): HTTP-WAN-to-DMZ

Action : Allow (Autoriser)

Service: http

Source Interface (interface source) : wan

Destination Interface (Interface de destination) : dmz

Source Network (réseau source) : all-nets (tout réseau)

Destination Network (Réseau de destination) : wan_ip

Cliquez sur OK.

Chapitre 5. Services DHCP

Le présent chapitre décrit les services DHCP de NetDefendOS.

Présentation

DHCP (Dynamic Host Configuration Protocol) est un protocole qui autorise les administrateurs réseau à attribuer automatiquement des adresses IP aux ordinateurs d'un réseau.

Affectation des adresses IP. Un *serveur DHCP* est chargé d'attribuer des adresses IP aux clients DHCP. Ces adresses proviennent d'un groupe d'adresses IP prédéfini géré par DHCP. Lorsqu'un serveur DHCP reçoit une requête en provenance d'un client DHCP, il retourne au client les paramètres de configuration (c'est-à-dire une adresse IP, une adresse MAC, un nom de domaine et une attribution d'adresse IP) dans un message unicast.

Attributions DHCP. Contrairement aux attributions statiques, où le client est propriétaire de l'adresse, l'adressage dynamique par serveur DHCP attribue l'adresse à chaque client pour une période de temps prédéfinie. Pendant la durée de vie d'une attribution, le client est autorisé à garder l'adresse attribuée et il est protégé contre les télescopages d'adresses avec d'autres clients.

Pour pouvoir continuer à utiliser l'adresse IP attribuée, le client doit renouveler l'attribution avant son expiration à partir du serveur. Le client peut donc décider à tout moment de ne plus utiliser l'adresse IP qui lui a été attribuée ; il peut mettre un terme à l'attribution et libérer l'adresse IP.

La durée d'attribution peut être configurée sur un serveur DHCP par l'administrateur.

Serveurs DHCP

NetDefendOS peut jouer le rôle d'un ou plusieurs serveurs logiques DHCP. Le filtrage des requêtes en provenance des clients DHCP repose sur l'interface, de telle sorte que chaque interface NetDefendOS peut posséder, au plus, un seul serveur logique DHCP qui lui est associé. En d'autres termes, NetDefendOS peut approvisionner les clients DHCP en utilisant différentes plages d'adresses selon l'interface sur laquelle ils se trouvent.

Un certain nombre d'options standard peuvent être configurées pour chaque exemple de serveur DHCP :

IP Address (adresse IP)

Netmask (masque réseau) - masque réseau envoyé au client DHCP.

Subnet (sous-réseau)

Gateway Address (adresse de passerelle) - précise quelle adresse IP doit être envoyée au client pour être utilisée comme passerelle par défaut. Si l'adresse 0.0.0.0 est spécifiée, alors l'IP attribuée au client sera envoyée comme passerelle.

Domain Name (nom de domaine)

Lease Time (durée de l'attribution) - durée en secondes pendant laquelle une attribution DHCP doit être allouée à un hôte et à l'issue de laquelle le client doit renouveler cette attribution.

DNS Servers (Serveurs DNS)

WINS Servers (serveurs WINS)

Next Server (serveur suivant) - adresse IP du serveur suivant dans le processus de démarrage. Il s'agit généralement d'un serveur TFTP.

De plus, des *options personnalisées* peuvent être définies pour que les serveurs DHCP gèrent tous les types d'options prises en charges par la norme DHCP.

Les serveurs DHCP attribuent et gèrent les adresses IP récupérées dans le groupe d'adresses spécifié. Les serveurs DHCP de NetDefendOS ne se limitent pas à distribuer une seule plage d'adresses IP, mais peuvent utiliser n'importe quelle plage d'adresses IP pouvant être spécifiée par un objet d'adresse NetDefendOS.

Exemple 5.1. Configuration d'un serveur DHCP

Cet exemple montre comment configurer un serveur DHCP appelé *DHCPServer1* qui attribue et gère les adresses IP provenant d'un groupe d'adresses appelé *DHCPRange1*. Cet exemple suppose que vous avez créé une plage d'adresses IP pour le serveur DHCP.

Interface de ligne de commande

```
gw-world:/> add DHCPServer DHCPServer1 Interface=lan
  IPAddressPool=DHCPRange1 Netmask=255.255.255.0
```

Interface Web

Sélectionnez System > DHCP > DHCP Servers > Add > DHCPServer (Système > DHCP > Serveurs DHCP > Ajouter > Serveur DHCP).

Saisissez :

Name (nom): DHCPServer1

Interface Filter (filtre d'interface) : lan

IP Address Pool (groupe d'adresses IP) : DHCPRange1

Netmask (masque réseau) : 255.255.255.0

Cliquez sur OK.

Exemple 5.2. Vérification de l'état d'un serveur DHCP

Interface Web

Dans la barre de menu, Sélectionnez Status > DHCP Server (Statut > Serveur DHCP).

Interface de ligne de commande

Pour vérifier l'état de tous les serveurs :

```
gw-world:/> dhcpserver
```

Pour établir une liste de tous les serveurs configurés :

```
gw-world:/> show dhcpserver
```

Conseil

Le système garde en mémoire les attributions DHCP entre les redémarrages.

Attribution DHCP statique

Lorsque l'administrateur requiert une relation fixe entre un client et l'adresse IP attribuée, NetDefendOS permet d'attribuer une adresse IP donnée à une adresse MAC spécifique.

Exemple 5.3. Configuration du mode DHCP statique

Cet exemple montre comment attribuer l'adresse IP *192.168.1.1* à l'adresse MAC *00-90-12-13-14-15*. L'exemple suppose que le serveur DHCP, *DHCPServer1*, a déjà été défini.

Interface de ligne de commande

Paramétrez tout d'abord le contexte *DHCPServer1 :*

```
gw-world:/> cc DHCPServer DHCPServer1
```

Ajoutez ensuite l'attribution DHCP statique :

```
gw-world:/> add DHCPServerPoolStaticHost Host=192.168.1.1
  MACAddress=00-90-12-13-14-15
```

Vous pouvez établir une liste de toutes les attributions statiques, chacune étant classée selon un numéro d'index :

```
gw-world:/> show

 # Comments
 - -------
+ 1 (none)
```

Vous pouvez consulter chaque attribution statique individuelle grâce à son numéro d'index :

```
gw-world:/> show DHCPServerPoolStaticHost 1

 Property Value
---------- -----------------
  Index: 1
  Host: 192.168.1.1
MACAddress: 00-90-12-13-14-15
 Comments: (none)
```

L'attribution pourra par la suite être transformée en adresse IP *192.168.1.12* par la commande suivante :

```
gw-world:/> set DHCPServerPoolStaticHost 1 Host=192.168.1.12
  MACAddress=00-90-12-13-14-15
```

Interface Web

Sélectionnez System > DHCP > DHCP Servers > DHCPServer1 > Static Hosts > Add > Static Host Entry (Système > DHCP > Serveurs DHCP > Serveur DHCP 1 > Hôtes statiques > Ajouter > Entrée d'hôte statique).

Saisissez :

Host (hôte) : 19.168.1.1

MAC (adresse MAC) : 00-90-12-13-14-15

Cliquez sur OK.

Relais DHCP

Avec le protocole DHCP, les clients envoient des requêtes pour localiser le(s)serveur(s) DHCP qui utilise(nt) des messages de diffusion. Toutefois, les messages de diffusion circulent uniquement à travers le réseau local. Cela signifie que le serveur et le client DHCP doivent toujours se trouver dans le même réseau physique pour pouvoir communiquer. Dans un environnement de la taille d'Internet, cela signifie qu'un serveur différent pour chaque réseau est nécessaire. Ce problème est résolu en utilisant un relayeur DHCP.

Un relayeur DHCP remplace le serveur DHCP du réseau local pour établir le lien entre le client et le serveur DHCP distant. Il intercepte les requêtes en provenance des clients et les retransmet au serveur. Le serveur répond ensuite au relayeur, qui transfère la réponse au client. Les relayeurs DHCP adoptent la fonctionnalité BOOTP relay agent (agent de redirection BOOTP) et conservent le format de message et le protocole de communication BOOTP, raison pour laquelle ils sont souvent appelés agents de redirection BOOTP.

Exemple 5.4. Configuration d'un relayeur DHCP

Cet exemple permet aux clients des interfaces VLAN d'obtenir des adresses IP à partir d'un serveur DHCP. On suppose que le firewall est configuré avec les interfaces VLAN, « vlan1 » et « vlan2 », qui utilisent le relais DHCP, et que l'adresse IP du serveur DHCP est définie dans le carnet d'adresse comme « ip-dhcp ».

NetDefendOS installe une route pour le client lorsqu'il a terminé le processus DHCP et qu'il a obtenu une adresse IP.

Interface de ligne de commande

Ajout d'interfaces VLAN « vlan1 » et « vlan2 » qui doivent rediriger le trafic vers un groupe d'interfaces nommé « ipgrp-dhcp » :

```
gw-world:/> add Interface InterfaceGroup ipgrp-dhcp Members=vlan1,vlan2
```

Ajout d'un relais DHCP nommé « vlan-to-dhcpserver » :

```
gw-world:/> add DHCPRelay vlan-to-dhcpserver Action=Relay TargetDHCPServer=ip-dhcp
  SourceInterface=ipgrp-dhcp AddRoute=Yes ProxyARPInterfaces=ipgrp-dhcp
```

Interface Web

Ajout des interfaces VLAN « vlan1 » et « vlan2 » qui doivent rediriger le trafic vers un groupe d'interfaces nommé « ipgrp-dhcp » :

Sélectionnez Interface > Interface Groups > Add > InterfaceGroup (Interface > Groupes d'interfaces > Ajouter > Groupe d'interfaces).

Saisissez :

Name (nom) : ipgrp-dhcp

Interfaces : sélectionnez « vlan1 » et « vlan2 » dans la liste disponible et placez-les dans la liste Selected (Sélection).

Cliquez sur OK.

Ajout d'un relais DHCP nommé « vlan-to-dhcpserver » :

Sélectionnez System > DHCP > Add > DHCP Relay (Système > DHCP > Ajouter > Relais DHCP).

Saisissez :

Name (nom) : vlan-to-dhcpserver

Action : Relay (Rediriger)

Source Interface (interface source) : ipgrp-dhcp

DHCP Server to relay to (serveur DHCP vers lequel le trafic est redirigé) : ip-dhcp

Allowed IP offers from server (attributions d'IP autorisées à partir du serveur) : all-nets (tout-réseau)

Sous l'onglet Add Route (Ajouter une route), cochez Add dynamic routes for this relayed DHCP lease (ajouter routes dynamiques pour cette attribution HDCP relayée).

Cliquez sur OK.

Groupes IP

Présentation. On utilise les *groupes IP* pour permettre d'autres accès sous-systèmes à un cache d'adresses IP DHCP. Ces adresses sont rassemblées dans un groupe en maintenant une série de clients DHCP en interne (un par IP). Les serveurs DHCP utilisés par un groupe peuvent être soit des serveurs externes, soit des serveurs DHCP définis dans NetDefendOS lui-même. Les serveurs DHCP externes peuvent être définis comme des serveurs sur une interface spécifique ou par une adresse IP unique. Vous pouvez configurer plusieurs groupes IP avec des identifiants différents.

L'utilisation principale des groupes IP s'effectue avec *IKE Config Mode*, fonctionnalité qui sert à attribuer des adresses IP aux clients distants qui se connectent par des tunnels IPsec. Pour plus d'informations à ce sujet,

veuillez consulter la section intitulée « Utilisation du mode de configuration ».

Options de base des groupes IP. Voici les options de base disponibles pour un groupe IP :

DHCP Server behind interface (serveur DHCP derrière une interface) Indique que le groupe IP doit utiliser le(s) serveur(s) DHCP se trouvant sur l'interface spécifiée.

Server filter (filtre serveur) Paramètre facultatif servant à spécifier quels serveurs doivent être utilisés. S'il n'est pas spécifié, chaque serveur DHCP de l'interface sera utilisé. L'ordre des adresses ou des plages fournies (dans le cas d'adresses multiples) sera utilisé pour indiquer les serveurs préférés.

Specify DHCP Server Address (spécifier l'adresse du serveur DHCP) Sert à spécifier la ou les adresses IP du serveur DHCP à utiliser dans l'ordre croissant préféré. L'utilisation de l'adresse IP de bouclage *127.0.0.1* indique que le serveur DHCP est NetDefendOS lui-même.

Client IP filter (filtre d'IP client) Paramètre facultatif servant à spécifier quelles adresses IP proposées sont valides et peuvent être utilisées. Dans la plupart des cas, cette option est définie sur le paramètre par défaut, à savoir « all-nets » (tout-réseau). Vous pouvez également spécifier un ensemble de plages IP. Le filtre assure que seules certaines adresses IP en provenance des serveurs DHCP sont admises et on l'utilise lorsque l'on s'attend à ce qu'un serveur DHCP réponde avec une adresse IP non admise.

Options avancées des groupes IP. Voici les options avancées disponibles pour la configuration des groupes IP :

Routing table (table de routage) Règles de la table de routage qui doivent être utilisées pour les recherches lors de la résolution des interfaces de destination pour les serveurs DHCP configurés.

Receive interface (interface de réception) Interface de réception « simulée ». Cette option peut être utilisée dans les règles de routage basées sur des règles et/ou pour déclencher une règle de serveur DHCP spécifique si le groupe utilise un serveur DHCP dans NetDefendOS et si l'adresse IP de ce serveur a été spécifiée en tant qu'interface de bouclage.

MAC Range (plage MAC) Plage d'adresses MAC qui sera utilisée pour créer des « faux » clients DHCP. Cette option est utilisée lorsque le(s) serveur(s) DHCP mappe(nt) des clients en adresse MAC. L'attribution en continu par le serveur DHCP de la même adresse IP à chaque client indique la nécessité d'utiliser des plages MAC.

Prefetched leases (attributions d'adresses préchargées) Spécifie le nombre d'attributions à précharger. Le préchargement améliore les performances car il n'y aura pas de temps d'attente lorsque le système interrogera une adresse IP (lorsque des IP préchargées existent).

Maximum free (maximum libre) Nombre maximum d'adresses IP à laisser « libres ». Doit être égal ou supérieur au paramètre de préchargement. Le groupe démarre le processus de libération (en restituant les adresses IP au serveur DHCP) lorsque le nombre de clients libres est supérieur à cette valeur.

Maximum clients (clients maximums) Paramètre facultatif utilisé pour spécifier le nombre maximum de clients (adresses IP) autorisés dans le groupe.

Utilisation des attributions préchargées. Comme mentionné dans la section précédente, l'option *Prefetched Leases* (attribution d'adresses préchargées) spécifie la taille du cache des attributions dont la maintenance est assurée par NetDefendOS. Ce cache permet une affectation rapide des attributions et peut améliorer les performances globales du système. Il est important de noter toutefois que le nombre total d'attributions préchargées est requis au démarrage du système et que, si ce nombre est trop élevé, les performances initiales peuvent s'en trouver affectées.

Lorsque les attributions sont allouées dans le cache de préchargement, des requêtes sont envoyées aux serveurs DHCP, de sorte que le cache est toujours rempli. Par conséquent, l'administrateur doit définir la taille du cache de préchargement initiale de façon à ce qu'elle soit optimale.

Exemple 5.5. Création d'un groupe IP

Cet exemple montre comment créer un objet groupe IP qui utilisera le serveur DHCP à l'adresse IP *28.10.14.1* avec 10 attributions préchargées. On suppose que cette adresse IP est déjà définie dans le carnet d'adresses en tant qu'objet IP nommé *ippool_dhcp*

Interface de ligne de commande

gw-world:/> **add IPPool ip_pool_1 DHCPServerType=ServerIP ServerIP=ippool_dhcp**

Interface Web

Sélectionnez Objects > IP Pools > Add > IP Pool (Objets > Groupes IP > Ajouter > Groupe IP).

Saisissez le nom : ip_pool_1

Sélectionnez Specify DHCP Server Address (spécifier l'adresse du serveur DHCP).

Ajoutez *ippool_dhcp* à la liste sélectionnée.

Sélectionnez l'onglet Advanced (Avancé).

Définissez le nombre d'attributions préchargées sur *10*.

Cliquez sur OK.

Chapitre 6. Mécanismes de sécurité

Le présent chapitre décrit les fonctions de sécurité de NetDefendOS.

Règles d'accès

Introduction

L'une des fonctions principales de NetDefendOS est de permettre uniquement aux connexions autorisées d'accéder aux ressources de données protégées. Le contrôle d'accès est tout d'abord défini par l'ensemble de règles IP de NetDefendOS dans lequel une plage d'adresses protégées est traitée comme un hôte de confiance, le trafic provenant des sources non fiables n'étant pas autorisé à pénétrer les zones de confiance.

Avant qu'une nouvelle connexion soit confrontée à l'ensemble de règles IP, NetDefendOS confronte la source de la connexion à un ensemble de *règles d'accès*. Les règles d'accès peuvent spécifier quelle source de trafic est attendue sur une interface donnée et peuvent également rejeter automatiquement le trafic provenant de sources spécifiques. Les règles d'accès sont à même de proposer un filtrage initial efficace et ciblé des nouvelles tentatives de connexion.

La règle d'accès par défaut. Même si l'administrateur ne définit pas explicitement de règle d'accès, une règle d'accès de base est toujours en place, appelée *règle d'accès par défaut*. Cette règle par défaut vérifie systématiquement le trafic entrant en effectuant une recherche inversée dans la table de routage. Cette recherche vérifie que le trafic entrant provient d'une source signalée par les tables de routage comme étant accessible via l'interface de destination du trafic. Si cette recherche inversée échoue, la connexion est interrompue et un message « règle d'accès par défaut » est généré.

Pour la plupart des configurations, la règle d'accès par défaut suffit et l'administrateur n'a pas besoin de spécifier explicitement d'autres règles. La règle par défaut peut, par exemple, protéger contre l'usurpation d'IP, décrite dans la section suivante. Lorsque des règles d'accès sont explicitement spécifiées, la règle d'accès par défaut continue de s'appliquer si une nouvelle connexion ne correspond à aucune des règles spécifiées.

Usurpation d'IP

Le trafic qui semble provenir d'un hôte de confiance peut avoir été envoyé par un pirate pour tenter de contourner les mécanismes de sécurité d'un firewall. Une telle attaque est plus fréquemment appelée *Spoofing* (usurpation).

L'usurpation d'IP est l'une des attaques de spoofing les plus courantes. On utilise des adresses IP sécurisées pour contourner le filtrage. L'en-tête d'un paquet IP, qui indique l'adresse source du paquet, est modifié par le pirate de façon à indiquer une adresse hôte locale. Le firewall croit alors que le paquet provient d'une source sécurisée. Puisqu'on ne peut pas répondre correctement à la source du paquet, une congestion de trafic inutile risque de se créer et une situation de déni de service (DoS) peut alors survenir. Même si le firewall peut détecter une situation de déni de service, elle est par nature difficile à surveiller et à stopper.

Les VPN offrent un moyen d'éviter le spoofing mais pour les cas où ils ne constituent pas une solution appropriée, les règles d'accès peuvent offrir une fonctionnalité anti-spoofing en mettant à disposition un filtre supplémentaire pour la vérification des adresses source. Une règle d'accès peut vérifier que les paquets arrivant à une interface donnée ne possèdent pas d'adresse source associée au réseau d'une autre interface. En d'autres termes :

Tout trafic entrant avec une adresse IP source appartenant à un hôte de confiance local n'est PAS autorisé.

Tout trafic sortant avec une adresse IP source appartenant à un hôte externe non sécurisé n'est PAS autorisé.

Le premier énoncé empêche un inconnu d'utiliser l'adresse d'un hôte local en tant qu'adresse source. Le second empêche tout hôte local de lancer le processus d'usurpation.

Paramètres des règles d'accès

La configuration d'une règle d'accès ressemble à celle des autres types de règles. Ses paramètres contiennent des

champs de filtrage ainsi que l'action à entreprendre. Si une correspondance existe, la règle est activée et NetDefendOS exécute l'action spécifiée.

Champs de filtrage des règles d'accès. Les champs de filtrage des règles d'accès utilisés pour activer une règle sont les suivants :

Interface : Interface sur laquelle arrive le paquet.

Network (Réseau) : La plage IP à laquelle doit appartenir l'adresse de l'expéditeur.

Actions des règles d'accès. Les actions des règles d'accès qui peuvent être spécifiées sont les suivantes :

Drop (Ignorer) : ignore les paquets qui correspondent aux champs définis.

Accept (Accepter) : accepte les paquets qui correspondent aux champs définis pour une inspection détaillée de l'ensemble de règles.

Expect (Prévoir) : si l'adresse de l'expéditeur du paquet correspond au réseau spécifié par cette règle, l'interface réceptrice est comparée à l'interface spécifiée. Si les interfaces correspondent, le paquet est accepté de la même façon que pour l'action Accept (accepter). Si les interfaces diffèrent, le paquet est ignoré de la même façon que pour l'action Drop (Ignorer).

Remarque
Pour ces actions, la consignation peut être activée sur demande.

Désactivation des notifications de la règle d'accès par défaut. Si, pour une quelconque raison, le message « Règle d'accès par défaut » est généré en continu par telle ou telle source et doit être désactivé, vous pouvez le faire en spécifiant une règle d'accès pour cette source avec une action Ignorer.

Problèmes liés au dépannage des règles d'accès. Il est à noter que les règles d'accès constituent le filtre de trafic prioritaire par rapport aux autres modules de NetDefendOS. Pour cette raison, des problèmes peuvent parfois survenir, tels que la configuration des tunnels VPN. Il est toujours conseillé de vérifier les règles d'accès lorsque l'on résout des problèmes embarrassants au cas où une règle empêche une autre opération de fonctionner correctement, comme la mise en place d'un tunnel VPN par exemple.

Exemple 6.1. Configuration d'une règle d'accès

On définit ici une règle qui s'assure qu'aucun trafic n'est reçu par l'interface lan avec une adresse source en dehors du réseau lannet.
Interface de ligne de commande

```
gw-world:/> add Access Name=lan_Access Interface=lan Network=lannet Action=Except
```

Interface Web

Sélectionnez Rules > Access (Règles > Accès).
Sélectionnez Access Rule (Règle d'accès) dans le menu Add (Ajouter).
Saisissez :

Name (nom) : lan_Access
Action : Except (sauf)

Interface : lan

Network (Réseau) : lannet

Cliquez sur OK.

Passerelles ALG (Application Layer Gateway)

Présentation
En complément du filtrage de paquets de bas niveau, qui inspecte uniquement les en-têtes de paquets des

protocoles tels que IP, TCP, UDP et ICMP, les firewalls D-Link proposent des *passerelles ALG* qui assurent un filtrage au niveau supérieur de la couche d'*application* OSI.
Un objet ALG fonctionne comme un médiateur d'accès pour les applications Internet utilisées couramment en dehors du réseau protégé, telles que l'accès à Internet, le transfert de fichiers et le transfert de contenu multimédia. Les passerelles ALG proposent une sécurité supérieure au filtrage de paquets car elles peuvent surveiller l'ensemble du trafic pour un protocole spécifique et effectuer des vérifications aux plus hauts niveaux de la pile TCP/IP.

Voici les protocoles qui sont pris en charge par les passerelles ALG de NetDefendOS :

HTTP

FTP

TFTP

SMTP

POP3

SIP

H.323

Déploiement d'une passerelle ALG. Une fois qu'une passerelle ALG est définie par l'administrateur, elle est mise en service, tout d'abord, par son association à un objet de service, ce service étant ensuite associé à une règle IP dans l'ensemble de règles IP de NetdefendOS.

Sessions de connexion maximales. Le service associé à une ALG possède un paramètre configurable qui lui est associé, appelé *Max Sessions*, dont la valeur par défaut dépend du type d'ALG. Par exemple, la valeur par défaut pour l'ALG HTTP est *1000*. Cela signifie que 1000 connexions sont autorisées au total pour le Service HTTP sur toutes les interfaces. Voici la liste complète des valeurs par défaut minimales :

ALG HTTP - *1000* sessions.

ALG FTP - *200* sessions.

ALG TFTP - *200* sessions.

ALG SMTP - *200* sessions.

ALG POP3 - *200* sessions.

ALG H.323 - *100* sessions.

Remarque

Cette valeur par défaut peut souvent être trop basse pour le protocole HTTP si un grand nombre de clients se connectent par le firewall D-Link. Il est alors conseillé d'envisager l'utilisation d'une valeur supérieure.

Les passerelles ALG et la protection SYN-flood. Il est important de noter que les objets de service définis par l'utilisateur de manière personnalisée permettent d'activer la *protection SYN-flood*, une fonctionnalité qui cible précisément les attaques SYN-flood. Si cette option est activée pour un objet de service, alors aucune ALG associée à ce service ne sera utilisée.

HTTP

HTTP (Hyper Text Transfer Protocol) est le protocole principal utilisé pour accéder à Internet. C'est un protocole de la couche d'application, dépourvu de connexion et d'état, reposant sur une architecture requête/réponse. Un client, tel qu'un navigateur Web, envoie une requête en établissant une connexion TCP/IP vers un port connu (généralement le port 80) d'un serveur distant. Le serveur répond par une chaîne de réponses, suivie d'un message qui lui est propre. Ce message peut, par exemple, être un fichier HTML destiné à être affiché dans le navigateur Web, un composant ActiveX destiné à être exécuté sur l'ordinateur client, ou bien un message d'erreur.

Le protocole HTTP rencontre certains problèmes en raison du très grand nombre de sites Web auxquels il est possible d'accéder et de la diversité des types de fichiers pouvant être téléchargés suite à ces accès.

Le protocole ALG HTTP est un sous-système étendu de NetDefendOS qui comprend un certain nombre de modules. Ceux-ci comprennent les fonctionnalités suivantes, qui sont décrites dans les sections indiquées du manuel qui leur sont dédiées :

Static Content Filtering (filtrage de contenu statique) - Il s'agit du « *Blacklisting* » et du « *Whitelisting* » des URL spécifiques.

URL Blacklisting (« blacklisting » des URL) - Des URL spécifiques peuvent être mises sur liste noire pour qu'elles ne soient plus accessibles. Le « wildcarding » peut être utilisé au moment de spécifier ces URL.

URL Whitelisting (« whitelisting » des URL) - Inverse du « blacklisting », vérifie que certaines URL sont toujours autorisées. Vous pouvez également utiliser le « wildcarding » pour ces URL.

Il est important de noter que le fait de mettre sur liste blanche une URL implique qu'aucune vérification, telle qu'une analyse antivirus ou un filtrage de contenu, ne sera appliquée au trafic HTTP. NetDefendOS va considérer que l'on peut « faire confiance » au trafic provenant de cette URL.

Ces fonctionnalités sont décrites de façon détaillée dans la section intitulée « Filtrage de contenu statique ».

Filtrage de contenu dynamique – L'accès à des URL spécifiques peut être autorisé ou bloqué selon les règles appliquées à un certain type de contenu Web. L'accès aux sites d'actualités peut être autorisé, alors que l'accès aux sites de jeux peut être bloqué.

Ces fonctionnalités sont décrites de façon détaillée dans la section intitulée « Filtrage de contenu statique ».

Analyse antivirus - Le contenu des fichiers HTTP téléchargés peut être analysé afin de rechercher des virus.

Ces fonctionnalités sont décrites de façon détaillée dans la section intitulée « Analyse antivirus ».

Vérification de l'intégrité des fichiers - Cette partie de la passerelle ALG gère le type de fichiers téléchargés.

Vérification du type MIME - Cette fonction est utilisée pour vérifier que le type du nom de fichier utilisé pour le téléchargement s'accorde avec le contenu du fichier. Tous les types de fichiers vérifiés de cette manière par NetDefendOS figurent dans la liste de l'*Annexe C, Types de fichiers MIME vérifiés*. Ces types de fichiers figurent également dans la liste Allow/Block (Autoriser/Bloquer) décrite ci-dessous. Tout téléchargement de fichier qui échoue à la vérification est interrompu par NetDefendOS.

Autoriser/Bloquer les types sélectionnés - Cette option de liste fonctionne indépendamment de l'option de vérification MIME décrite ci-dessus. Il existe deux modes de fonctionnement de la liste :

Block Selected (Bloquer la sélection) signifie que le téléchargement des types de fichiers sélectionnés sera automatiquement bloqué. Le contenu d'un fichier sera analysé pour identifier le type de fichier correct. Par exemple, si un fichier contenant des données .exe est trouvé, mais que le type du fichier n'est pas .exe, alors il sera bloqué si les fichiers .exe sont bloqués. « Bloquer » est l'action par défaut, ce qui signifie que si rien n'est sélectionné dans la liste, aucune action n'est entreprise.

Allow Selected (Autoriser la sélection) signifie que seuls les types de fichiers sélectionnés seront autorisés au téléchargement. Le contenu des fichiers est également examiné pour déterminer le vrai type de fichier.

Les types de fichiers supplémentaires qui ne sont pas inclus par défaut peuvent être ajoutés à la liste Allow/Block (Autoriser/Bloquer). Ceux-ci ne peuvent toutefois pas être soumis à la vérification du type MIME, ce qui signifie que l'extension du fichier sera considérée comme correcte par rapport au contenu du fichier.

De plus, vous pouvez définir une taille limite pour chaque opération de téléchargement.

Déploiement d'une passerelle ALG HTTP. Comme mentionné dans l'introduction, l'objet ALG HTTP est mis en service, tout d'abord, par son association à un objet de service, ce service étant ensuite associé à une règle IP dans l'ensemble de règles IP de NetdefendOS. Un certain nombre de services HTTP prédéfinis peuvent être utilisés avec la passerelle ALG. Par exemple, vous pouvez sélectionner le service HTTP à cet effet. Tant que le

service associé est lié à une règle IP, la passerelle ALG sera appliquée au trafic ciblé par cette règle IP.

Le service HTTPS (également inclus dans le service http-all) ne peut pas être utilisé avec une passerelle ALG HTTP tant que le trafic HTTPS est chiffré.

FTP

Le File Transfer Protocol (FTP) est un protocole reposant sur le TCP/IP destiné à l'échange de fichiers entre un client et un serveur. Le client lance la connexion en se reliant au serveur FTP. Normalement, le client doit s'authentifier lui-même en fournissant un identifiant et un mot de passe prédéfinis. Après avoir autorisé l'accès, le serveur propose au client une liste de fichiers/répertoires à partir desquels il peut télécharger/charger des fichiers (selon les droits d'accès). L'ALG FTP est utilisée pour gérer les connexions FTP par le firewall D-Link.

Connexions FTP. Le FTP emploie deux canaux de communication, un pour les commandes de contrôle et un autre pour les fichiers qui sont en cours de transfert. Lorsqu'une session FTP est ouverte, le client FTP établit une connexion TCP (canal de contrôle) vers le port 21 (par défaut) sur le serveur FTP. Ce qui se passe ensuite dépend du mode de FTP utilisé.

Modes de connexion. Le FTP fonctionne selon deux modes : *active* (actif) et *passive* (passif). Ceux-ci déterminent le rôle du serveur lors de l'ouverture des canaux de données entre le client et le serveur.

En mode actif, le client FTP envoie une commande au serveur FTP, qui indique l'adresse IP et le port auxquels le serveur doit se connecter. Le serveur FTP établit le canal de données retour vers le client FTP grâce aux informations d'adresse reçues.

En mode passif, le canal de données est ouvert par le client FTP vers le serveur FTP, de la même façon que le canal de commande. Il s'agit du mode par défaut recommandé pour les clients FTP bien que certains recommandent le mode inverse.

Problèmes de sécurité du FTP. Les deux modes de fonctionnement du FTP rencontrent des problèmes liés aux firewalls. Considérez un cas de figure où un client FTP du réseau interne se connecte à travers le firewall à un serveur FTP sur Internet. La règle IP est alors configurée pour autoriser le trafic réseau du client FTP vers le port 21 du serveur FTP.

En mode actif, NetDefendOS ne sait pas que le serveur FTP est sur le point d'établir une nouvelle connexion vers le client FTP. Par conséquent, la connexion entrante pour le canal de données sera interrompue. Étant donné que le numéro de port utilisé pour le canal de données est dynamique, le seul moyen de résoudre ce problème est d'autoriser le trafic en provenance de tous les ports du serveur FTP sur tous les ports du client FTP. Ce n'est évidemment pas une bonne solution.

En mode passif, le firewall n'a pas besoin d'autoriser les connexions provenant du serveur FTP. Mais NetDefendOS ne sait toujours pas quel port le client FTP tente d'utiliser pour le canal de données. Cela signifie qu'il doit autoriser le trafic provenant de tous les ports du client FTP vers tous les ports du serveur FTP. Bien que cette opération soit plus sécurisée que celle du mode actif, elle présente toujours une menace de sécurité potentielle. De plus, tous les clients FTP ne peuvent pas utiliser le mode passif.

La solution. L'ALG FTP résout ce problème en réassemblant entièrement le flux TCP du canal de commande et en examinant son contenu. Le firewall sait donc quel port doit être ouvert pour le canal de données. De plus, l'ALG FTP propose également des fonctionnalités pour éliminer certaines commandes de contrôle grâce à son filtre, ainsi qu'une protection de base contre la saturation de la mémoire tampon.

La fonctionnalité la plus importante de l'ALG FTP est sa capacité unique à effectuer des conversions instantanées entre le mode passif et le mode actif. La conversion peut être décrite comme suit :

Vous pouvez configurer le client FTP de manière à ce qu'il utilise le mode passif, qui est le mode recommandé pour les clients.

Vous pouvez configurer le serveur FTP de manière à ce qu'il utilise le mode actif, qui est le mode plus sûr pour les serveurs.

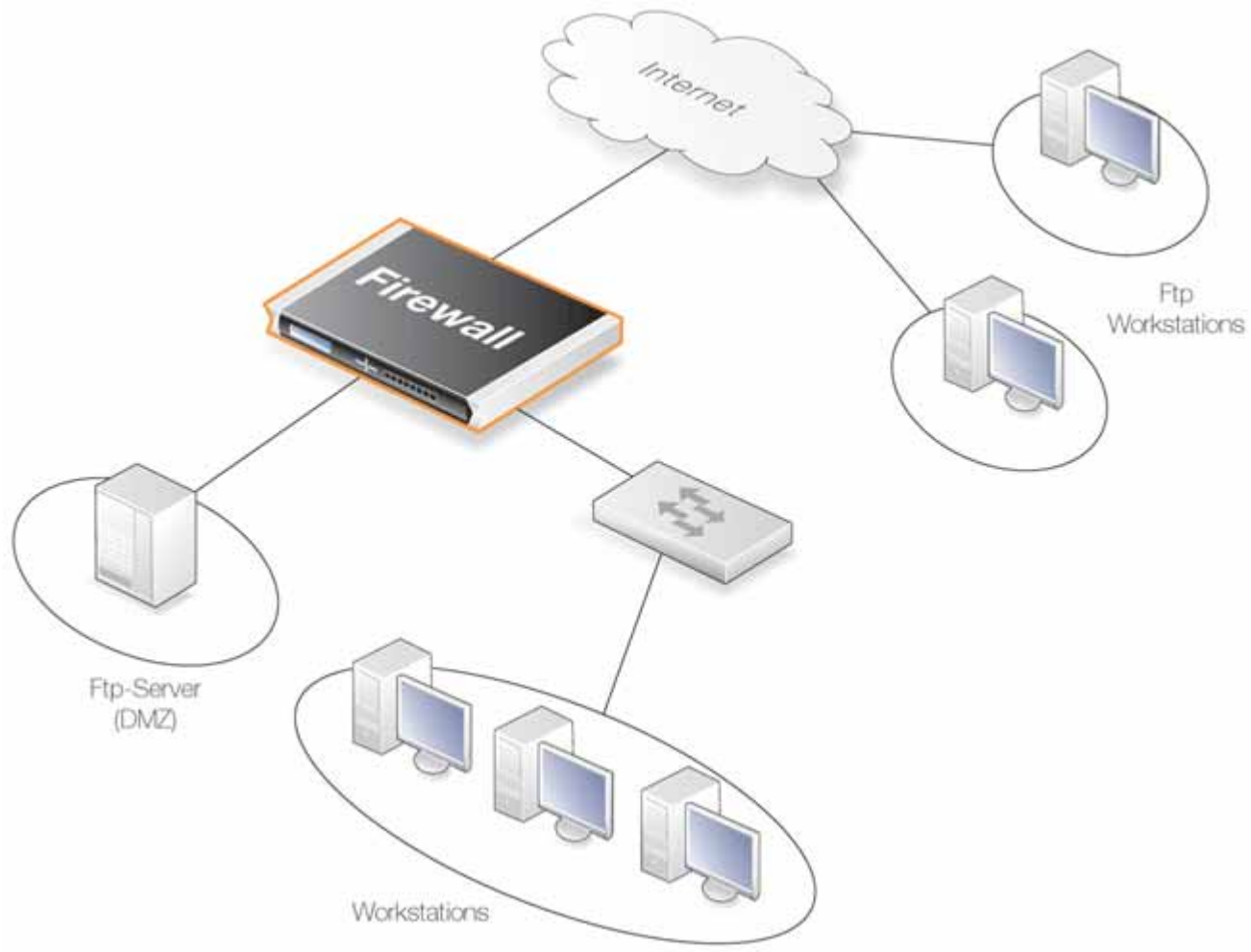
Lorsqu'une session FTP est établie, le firewall D-Link reçoit automatiquement et de manière transparente le canal des données passives du client FTP et le canal des données actives du serveur et les lie les unes avec les

autres.

Cette mise en œuvre permet à la fois au client et au serveur FTP de fonctionner dans leur mode le plus sécurisé. La conversion fonctionne également à l'inverse, c'est-à-dire que le client FTP utilise le mode actif et le serveur FTP le mode passif.

Exemple 6.2. Protection d'un serveur FTP avec une passerelle ALG

Comme illustré ci-dessous, on connecte un serveur FTP au Firewall D-Link sur un port DMZ qui possède des adresses IP privées :



Pour permettre la connexion à ce serveur à partir d'Internet via la passerelle ALG FTP, les règles et la passerelle ALG FTP doivent être configurées comme suit :

Interface Web

A. Définition de la passerelle ALG :

Sélectionnez Objects > ALG > Add > FTP ALG (Objets > ALG > Ajouter > ALG FTP).

Saisissez le nom : ftp-inbound

Cochez la case Allow client to use active mode (Autoriser le client à utiliser le mode actif).

Décochez la case Allow server to use passive mode (Autoriser le serveur à utiliser le mode passif).

Cliquez sur OK.

B. Définition du service :

Sélectionnez Objects > Services > Add > TCP/UDP Service (Objets > Services > Ajouter > Service TCP/UDP).

Saisissez les paramètres suivants :

Name (nom): ftp-inbound

Type : sélectionnez TCP dans la liste

Destination: 21 (le port sur lequel se trouve le serveur FTP).

ALG : sélectionnez « ftp-inbound » qui vient d'être créé.

Cliquez sur OK.

C. Définition d'une règle qui autorise les connexions vers les adresses IP publiques sur le port 21 et les transmet au serveur FTP interne :

Sélectionez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): SAT-ftp-inbound

Action : SAT

Service: ftp-inbound

Pour l'option Address Filter (Filtre d'adresses), saisissez :

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : all-nets (tout réseau)

Destination Network (Réseau de destination) : wan_ip (en supposant que l'interface externe a été définie ainsi)

Pour SAT, cochez la case Translate the Destination IP Address (Traduire l'adresse IP de destination).

Sélectionnez : New IP Address (Nouvelle adresse IP) : ftp-internal (en supposant que cette adresse IP interne pour le serveur FTP a été définie dans l'objet carnet d'adresse).

New Port (nouveau port) : 21

Cliquez sur OK.

D. Le trafic en provenance de l'interface interne nécessite une traduction NAT :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): NAT-ftp

Action : NAT

Service: ftp-inbound

Pour l'option Address Filter (Filtre d'adresses), saisissez :

Source Interface (Interface source) : dmz

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : dmznet

Destination Network (Réseau de destination) : wan_ip

Pour NAT, cochez la case Use Interface Address (Utiliser l'adresse de l'interface).

Cliquez sur OK.

E. Autoriser les connexions entrantes (SAT nécessite une seconde règle Allow (Autoriser)) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): Allow-ftp

Action : Autoriser

Service: ftp-inbound

Pour l'option Address Filter (Filtre d'adresses), saisissez :

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

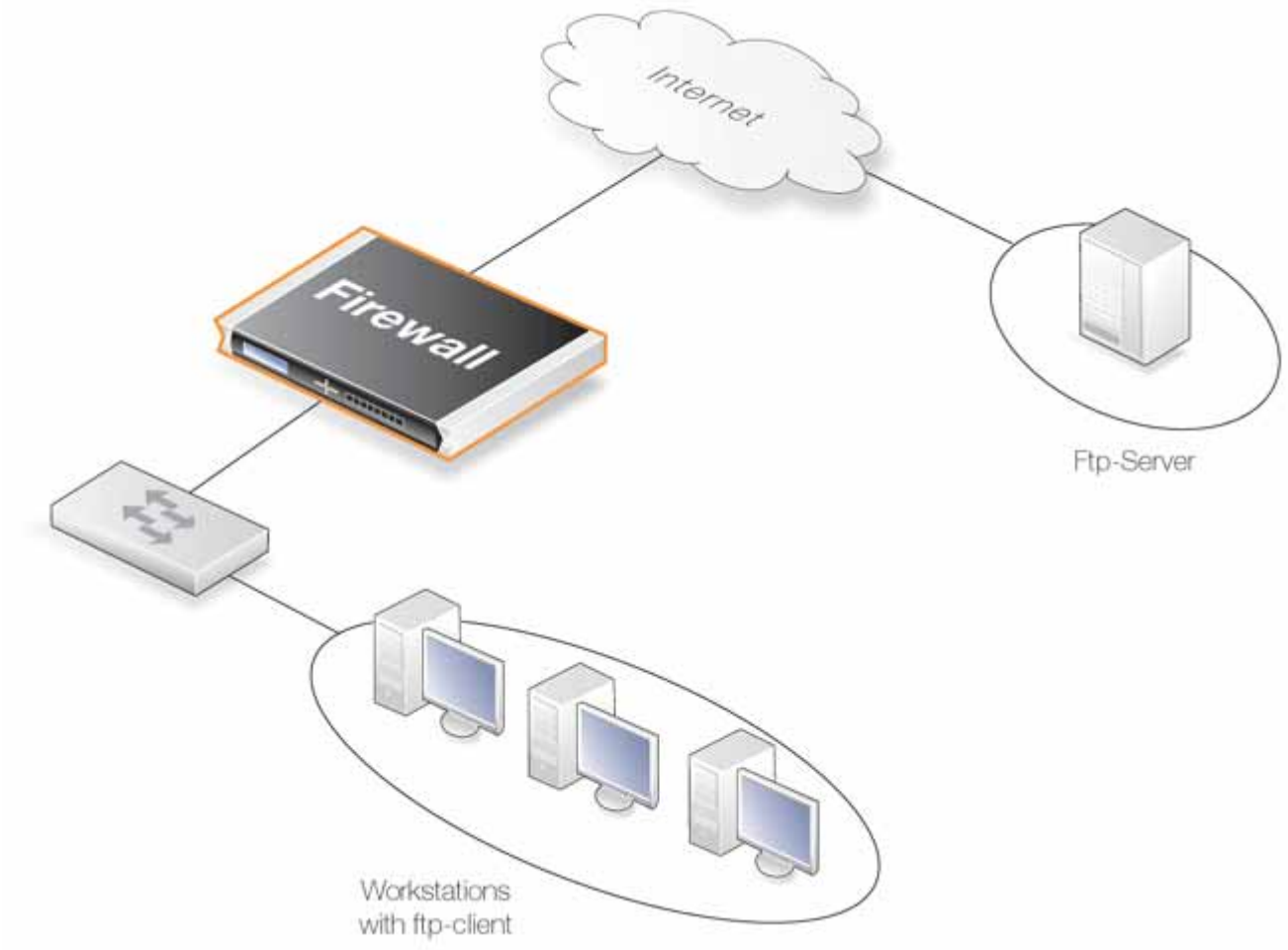
Source Network (Réseau source) : all-nets (tout réseau)

Destination Network (Réseau de destination) : wan_ip

Cliquez sur OK.

Exemple 6.3. Protection des clients FTP

Dans le cas de figure ci-dessous, le firewall D-Link protège une station de travail qui va se connecter à des serveurs FTP sur Internet.



Pour permettre la connexion à ces serveurs à partir du réseau interne via la passerelle ALG FTP, les règles et la passerelle ALG FTP doivent être configurées comme suit :

Interface Web

A. Création de la passerelle ALG FTP :

Sélectionnez Objects > ALG > Add > FTP ALG (Objets > ALG > Ajouter > ALG FTP).

Saisissez le nom : ftp-outbound

Décochez la case Allow client to use active mode (Autoriser le client à utiliser le mode actif).

Cochez la case Allow server to use passive mode (Autoriser le serveur à utiliser le mode passif).

Cliquez sur OK.

B. Création du service :

Sélectionnez Objects > Services > Add > TCP/UDP Service (Objets > Services > Ajouter > Service TCP/UDP).

Saisissez :

Name (nom): ftp-outbound

Type : sélectionnez TCP dans la liste déroulante.

Destination : 21 (le port sur lequel se trouve le serveur FTP).

ALG : sélectionnez *ftp-outbound*, qui vient d'être créé.

Cliquez sur OK.

Règles (lors de l'utilisation d'adresses IP publiques). La règle suivante doit être ajoutée aux règles IP lorsqu'on utilise des adresses IP publiques ; vérifiez qu'aucune autre règle n'interdit ou n'autorise d'ores et déjà le même type de port/de trafic. Le service employé est *ftp-outbound*, qui doit utiliser la définition ALG *ftp-outbound* comme décrit précédemment.

C. Autoriser les connexions vers les serveurs FTP externes :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): Allow-ftp-outbound

Action : Allow (Autoriser)

Service: ftp-outbound

Pour l'option Address Filter (Filtre d'adresses), saisissez :

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : wan

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : all-nets (tout réseau)

Cliquez sur OK.

D. Règles (lors de l'utilisation d'adresses IP privées). Si le firewall utilise des adresses IP privées, la nouvelle règle NAT suivante doit être ajoutée :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (nom): NAT-ftp-outbound

Action : NAT

Service: ftp-outbound

Pour l'option Address Filter (Filtre d'adresses), saisissez :

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : wan

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : all-nets (tout réseau)

Cochez la case Use Interface Address (Utiliser l'adresse de l'interface).

Cliquez sur OK.

TFTP

Trivial File Transfer Protocol (TFTP) est une version simplifiée du protocole FTP avec des fonctionnalités plus limitées. Son objectif est d'autoriser un client à charger des fichiers sur un système hôte ou de les télécharger à

partir du système hôte. Le transport de données TFTP repose sur le protocole UDP. De ce fait, il offre ses propres protocoles de transport et de contrôle de session, qui représentent des couches du protocole UDP.

TFTP est largement utilisé dans les entreprises pour la mise à jour des logiciels et la sauvegarde des configurations des périphériques réseau. Par définition, TFTP est reconnu comme étant un protocole non sécurisé et son utilisation est souvent restreinte aux réseaux internes. La passerelle ALG de NetDefendOS propose une couche de sécurité supplémentaire au TFTP car elle peut restreindre son utilisation.

Options TFTP générales.

Allow/Disallow Read (Autoriser/Refuser la lecture) La fonction GET de TFTP peut être désactivée de manière à ce que les fichiers ne puissent pas être récupérés par un client TFTP. La valeur par défaut est *Allow* (Autoriser).

Allow/Disallow Write (Autoriser/Refuser l'écriture) La fonction PUT de TFTP peut être désactivée de manière à ce qu'un client TFTP ne puisse pas écrire dans les fichiers. La valeur par défaut est *Allow* (Autoriser).

Remove Request Option (Supprimer les options de la requête) Précise si les options doivent être supprimées de la requête. La valeur par défaut est *False*, qui signifie « ne pas supprimer ».

Block Unknown Options (Bloquer les options inconnues) Cette option autorise à bloquer toutes les options d'une requête autres que la taille des blocs, la période d'expiration et la taille du transfert de fichiers. La valeur par défaut est *False*, qui signifie « ne pas bloquer ».

Options des requêtes TFTP. Tant que l'option de suppression de requête décrite ci-dessus est configurée sur *false* (les options ne sont pas supprimées), les paramètres suivants s'appliquent pour les options des requêtes :

Maximum Blocksize (Taille de bloc maximale) Vous pouvez préciser la taille de bloc maximale autorisée. Les valeurs valides sont comprises entre 0 et 65 464 octets. La valeur par défaut est 65 464 octets.

Maxiumum File Size (Taille de fichier maximale) La taille maximale d'un transfert de fichiers peut être limitée. La valeur par défaut représente le maximum absolu autorisé, c'est-à-dire 999 999 Ko.

Allow Directory Traversal (Autoriser le parcours des répertoires) Cette option peut interdire le parcours des répertoires en utilisant des noms de fichiers contenant des points consécutifs (« .. »).

Autoriser les expirations de requêtes. La passerelle ALG TFTP de NetDefendOS bloque les requêtes TFTP répétées provenant du même port et de la même adresse IP source dans une période de temps fixe. Ceci s'explique par le fait que certains clients TFTP peuvent envoyer des requêtes provenant du même port source sans allouer de période d'expiration appropriée.

SMTP

Simple Mail Transfer Protocol (SMTP) est un protocole textuel utilisé pour le transfert de messages électroniques entre les serveurs de messagerie via Internet. Généralement, le serveur SMTP local se situe sur une DMZ de telle sorte que les messages électroniques envoyés par les serveurs SMTP distants traverseront le firewall D-Link pour atteindre le serveur local (cette configuration est illustrée plus loin dans la section intitulée « Filtrage de SPAM DNSBL »). Les utilisateurs locaux utiliseront ensuite le logiciel de messagerie client pour récupérer leurs messages électroniques du serveur local SMTP.

Options ALG SMTP. Les principales fonctionnalités de la passerelle ALG SMTP sont les suivantes :

Email Rate Limiting (Limitation du débit des messages électroniques) Vous pouvez spécifier un débit maximal autorisé pour les messages électroniques.

Email Size Limiting (Limitation de la taille des messages électroniques) Vous pouvez spécifier une taille maximale autorisée pour les messages électroniques. Cette fonctionnalité

compte la somme totale d'octets envoyée pour un seul message électronique, qui correspond à la taille de l'en-tête, ajoutée à celle du corps et à celle de toutes les pièces jointes au message après son encodage. N'oubliez pas que la taille d'un message électronique comprenant, par exemple, une pièce jointe de 100 Ko, dépassera 100 Ko. La taille transférée peut être de 120 Ko ou plus, car l'encodage, qui est automatique pour les pièces jointes, peut augmenter considérablement la taille de la pièce jointe transférée. L'administrateur doit donc ajouter une marge raisonnable à la taille du message électronique prévue lorsqu'il définit cette limite.

Email address blacklisting (« blacklisting » d'adresses électroniques) Vous pouvez spécifier une liste noire d'adresses électroniques pour que les messages provenant de ces adresses soient bloqués.

Email address whitelisting (« whitelisting » d'adresses électroniques) Vous pouvez spécifier une liste blanche d'adresses électroniques pour que les messages provenant de cette adresse soient autorisés à traverser l'ALG.

Verify MIME-type (Vérification du type MIME) Les types de fichiers envoyés en pièces jointes dans les messages électroniques peuvent être vérifiés. Vous pouvez trouver une liste de tous les types de fichiers examinés dans l'*Annexe C, Types de fichiers MIME examinés.*

Anti-Virus Scanning (Analyse antivirus) Le module antivirus de NetDefendOS peut analyser les pièces jointes des messages électroniques afin de rechercher du code malveillant. Ces fonctionnalités sont décrites de façon détaillée dans la section intitulée « Analyse antivirus ».

Filtrage SPAM DNSBL

Les messages électroniques non sollicités, souvent appelés *spams*, sont devenus à la fois une grande contrariété et un problème de sécurité sur l'Internet publique. Envoyés en masse par des groupes de *spammeurs*, les courriers électroniques non sollicités peuvent gaspiller les ressources, transporter des programmes malveillants et tentent également de diriger le lecteur sur des pages Web qui peuvent exploiter certaines vulnérabilités présentes sur les navigateurs.

La passerelle ALG SMTP de NetDefendOS bénéficie d'un module SPAM intégré qui permet d'appliquer le *filtrage du spam* aux messages électroniques entrants selon leur provenance. Cela peut réduire de manière significative la charge de tels courriers électroniques dans les boîtes de messagerie des utilisateurs situés derrière un firewall D-Link. NetDefendOS propose les options suivantes :

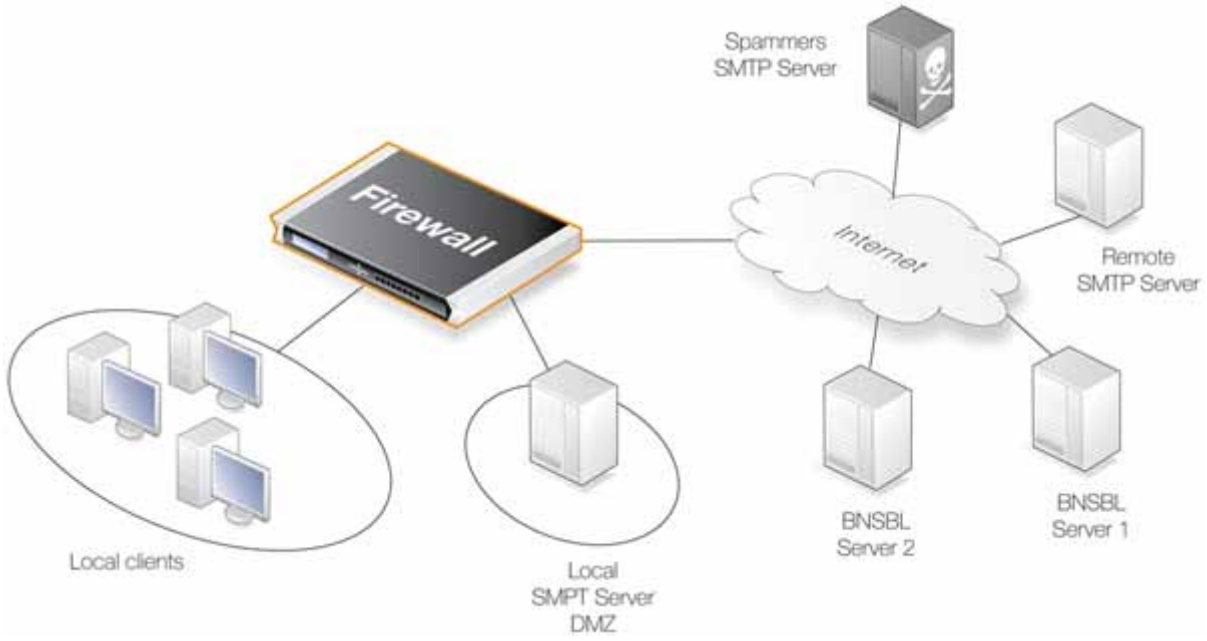
Ignorer les courriers électroniques ayant une forte probabilité d'être des spams.

Laisser passer mais marquer les courriers électroniques qui ont une probabilité modérée d'être des spams.

Mise en œuvre de NetDefendOS. SMTP fonctionne comme un protocole d'envoi de messages électroniques entre serveurs. NetDefendOS applique le filtrage du spam aux messages électroniques lorsqu'ils traversent un firewall D-Link, en provenance d'un serveur SMTP distant vers le serveur SMTP local (à partir duquel les clients locaux vont par la suite télécharger les courriers électroniques). Le serveur SMTP local est généralement configuré sur une DMZ et il y a habituellement un seul saut entre le serveur émetteur et le serveur récepteur local.

Un certain nombre d'organisations éprouvées gèrent des bases de données accessibles au plus grand nombre qui peuvent être interrogés via l'Internet publique et dans lesquelles figurent les adresses IP d'origine des serveurs de spam SMTP connus. Ces listes sont appelées bases de données *DNS Black List* (DNSBL) et leurs informations sont accessibles via une méthode de requête standardisée prise en charge par NetDefendOS. La figure ci-dessous illustre tous les éléments qui entrent en jeu :

Figure 6.1. Filtrage SPAM DNSBL



Lorsque la fonction de filtrage du spam de NetDefendOS est configurée, l'adresse IP du serveur qui émet le message électronique peut être transmise à un ou plusieurs serveurs DNSBL pour que ceux-ci nous informent si le message électronique provient ou non d'un spammeur (pour ce faire, NetDefendOS examine les en-têtes du paquet IP). La réponse envoyée par un serveur peut être une réponse *not listed* (non répertoriée) ou une réponse *listed* (répertoriée). Dans ce dernier cas, le serveur DSNBL indique que le message électronique peut être un spam et offre en général également une information appelée enregistrement *TXT*, qui constitue une explication textuelle pour la liste.

L'administrateur peut configurer l'ALG SMTP de NetDefendOS afin qu'elle consulte plusieurs serveurs DNSBL pour parvenir à un consensus quand à l'adresse d'origine d'un message électronique. Lorsqu'un nouveau message électronique arrive, on interroge les serveurs pour évaluer la probabilité que le message soit un spam, en fonction de son adresse d'origine. L'administrateur de NetDefendOS attribue un poids supérieur à 0 pour chaque serveur configuré, de telle sorte que la somme pondérée puisse ensuite être calculée en fonction de toutes les réponses. L'administrateur peut configurer l'une des actions suivantes, déterminées en fonction de la somme calculée :

Si la somme est supérieure ou égale à un *Drop threshold* (seuil de rejet) prédéfini, alors le message électronique est définitivement considéré comme un spam et il est ignoré, ou bien envoyé à une boîte de messagerie prévue à cet effet.

Si la somme est supérieure ou égale à un *SPAM threshold* (seuil de spam) prédéfini, alors le message électronique est considéré comme étant probablement un spam, mais il est acheminé vers le destinataire avec une notification.

Exemple de calcul de seuil. Supposons, par exemple, que 3 serveurs DNSBL soient configurés : *dnsbl1*, *dnsbl2* et *dnsbl3*. On leur attribue respectivement un poids de 3, 2 et 2. Le seuil de spam est alors défini sur 5.

Si *dnsbl1* et *dnsbl2* affirment qu'un message électronique est un spam mais que *dnsbl3* affirme le contraire, alors le total calculé sera 3+2+0=5. Étant donné que le total, dans ce cas 5, est égal (ou supérieur) au seuil, le message électronique sera considéré comme un spam.

Dans cet exemple, si l'on configure le *Drop threshold* (seuil de rejet) sur 7, alors les 3 serveurs DNSBL devront réagir pour que la somme calculée entraîne le rejet du message électronique (3+2+2=7).
Balisage des spams. Lorsqu'un message électronique est considéré comme un spam potentiel, c'est-à-dire lorsque la somme calculée est supérieure au SPAM threshold (seuil de spam) et inférieure au Drop threshold (seuil de rejet), alors le champ *Subject* (sujet) du message électronique est modifié par l'ajout d'un préfixe avant qu'il ne soit transmis au destinataire souhaité. Le texte du message de la balise est spécifié par l'administrateur mais peut être laissé vide (bien que cela ne soit pas recommandé).

Voici un exemple de balisage, le champ *Subject* (sujet) d'origine étant :

```
Buy this stock today! (achetez ce produit aujourd'hui !)
```

Si le texte de la balise est défini ainsi : « *** SPAM *** », alors le champ *Subject* (sujet) modifié du message électronique sera :

```
*** SPAM *** Buy this stock today!
```

C'est ce que verra le destinataire du message électronique dans le résumé du contenu de sa boîte de réception. L'utilisateur individuel peut ensuite décider de configurer ses propres filtres dans le client local pour qu'ils se chargent de ces messages électroniques balisés, en les envoyant éventuellement dans un dossier séparé.

De plus, des champs *X-SPAM* sont ajoutés au contenu du message électronique. Ceux-ci comprennent :

X-Spam-Flag (indicateur X-Spam) – Cette valeur sera toujours définie sur *Yes* (oui).

X-Spam-Checker-Version (Vérificateur de version X-Spam) – Version de NetDefendOS qui a balisé le message électronique

X-Spam-Status (état X-Spam) - Ce sera toujours *DNSBL*

X-Spam-Report (rapport X-Spam) – Liste de serveurs DNSBL qui ont marqué le message électronique comme spam

Vous pouvez faire appel à ces champs dans les règles de filtrage du serveur de messagerie configurées par l'administrateur.

Rejet des spams. Si la somme calculée est supérieure ou égale à la valeur *Drop threshold* (seuil de rejet), alors le message électronique n'est pas transmis au destinataire souhaité. Ll'administrateur peut choisir l'une ou l'autre alternative suivante pour les messages électroniques ignorés :

Une adresse de messagerie spéciale peut être configurée pour recevoir tous les mails ignorés. Une fois cette formalité accomplie, tous les messages *TXT* (mentionnés précédemment) envoyés par les serveurs DNSBL qui ont identifié le message électronique en tant que spam peuvent être, si nécessaire, ajoutés par NetDefendOS en pièce jointe au message électronique transféré.

Si aucune adresse de messagerie destinataire n'est configurée pour les messages électroniques rejetés, alors ils sont ignorés par NetDefendOS et un message d'erreur est envoyé à l'adresse de l'expéditeur avec les messages *TXT* provenant des serveurs DNSBL qui ont rejeté le message électronique.

Autorisation des serveurs d'échec DNSBL. Lorsqu'une requête vers un serveur DNSBL expire, NetDefendOS considère que la requête a échoué et le poids donné à ce serveur sera automatiquement soustrait des seuils de spam et de rejet pour le calcul du score attribué à ce message électronique.

Si un nombre suffisant de serveurs DNSBL ne répond pas, cette soustraction peut signifier que les valeurs de seuil deviennent négatives. Étant donné que le calcul du score donnera toujours la valeur 0 ou une valeur supérieure (les serveurs ne peuvent avoir de valeurs de poids négatives), tous les messages électroniques seront autorisés à passer si les seuils de spam et de rejet deviennent tous deux négatifs.

Un message de consignation est généré chaque fois qu'un serveur DNSBL configuré ne répond pas en temps voulu. Cette opération se produit une seule fois au début d'une séquence consécutive d'échecs de réponses provenant d'un serveur unique pour éviter de répéter inutilement le message.
Vérification de l'adresse électronique de l'expéditeur. Dans le cadre du module anti-spam, l'option de vérification de l'adresse électronique de l'expéditeur refuse les messages qui comportent des erreurs dans l'adresse SMTP « From » et dans l'en-tête « From ». En d'autres termes, l'adresse source de l'en-tête du protocole SMTP et l'en-tête de chargement des données SMTP doivent être les mêmes.
Le spam peut les rendre différents, c'est la raison pour laquelle cette fonctionnalité offre une vérification supplémentaire de l'intégrité du message électronique.
Consignation. Trois types de consignations sont effectués par le module de filtrage du spam.

Logging of dropped or SPAM tagged emails (Consignation des messages électroniques ignorés ou marqués comme spams) - Ces messages de consignation comportent l'adresse de messagerie et l'adresse IP sources, ainsi que le score de points pondérés et le DNSBL à l'origine du message événement.

DNSBLs not responding (Les DNSBL ne répondent pas) – Les expirations des requêtes DNSBL sont

consignées.

All defined DNBSLs stop responding (Tous les DNSBL définis cessent de répondre) – Il s'agit d'un événement de haute gravité car les messages électroniques seront autorisés à passer si cet événement se produit.

Configuration du réseau.

Résumé de la procédure de configuration. Les étapes de configuration du filtrage DNSBL du spam dans la passerelle ALG SMTP sont résumées par la liste suivante :

Spécifiez quels serveurs DNSBL seront utilisés. Ils peuvent être plusieurs et peuvent être utilisés soit pour sauvegarder des données entre eux, soit pour confirmer le statut d'un expéditeur.

Spécifiez un poids *(weight)* pour chaque serveur, qui déterminera son importance à décider si un message électronique est un spam ou non, lors du calcul de la somme pondérée.

Spécifiez le seuil pour qu'un message électronique soit marqué comme spam. Si la somme pondérée est supérieure ou égale à ce seuil, le message électronique sera considéré comme étant un spam.

Spécifiez une balise textuelle à placer en préfixe dans le champ Subject (Objet) d'un message électronique marqué comme spam.

Spécifiez le *Drop threshold* (seuil de rejet). Si la somme pondérée est supérieure ou égale à ce seuil, le message électronique sera complètement ignoré. Ce seuil doit être supérieur ou égal au seuil de spam. S'ils sont égaux, alors le seuil de rejet sera prioritaire de sorte que tous les messages électroniques seront ignorés lorsque ce seuil sera atteint.

Spécifiez, si nécessaire, une adresse de messagerie vers laquelle seront envoyés les messages électroniques ignorés (au lieu de simplement les effacer). Indiquez éventuellement si les messages *TXT* envoyés par les serveurs d'échec DNSBL doivent être ajoutés à ces messages électroniques.

Mise en cache d'adresses pour des performances accrues. Pour accélérer le traitement, NetDefendOS gère un cache contenant les adresses des expéditeurs recherchés le plus récemment dans la mémoire locale. Lorsque le cache est plein, l'entrée la plus ancienne est réécrite en premier.

L'administrateur peut modifier la valeur *Address Timeout* (expiration d'adresse) du cache. Ce paramètre détermine combien de temps une adresse, quelle qu'elle soit, sera valide une fois chargée dans le cache. Une fois ce délai expiré, une nouvelle requête d'adresse expéditeur mise en cache doit être envoyée aux serveurs DNSBL.

Le cache est vidé au démarrage ou à chaque nouvelle configuration et l'administrateur peut contrôler sa taille.

La commande *dnsbl* de l'interface de ligne de commande. La commande dnsbl de l'interface de ligne de commande offre un moyen de contrôler et de surveiller le fonctionnement du module de filtrage de spam. La commande dnsbl seule, sans option additionnelle, montre le statut global de toutes les ALG. Si le nom de la passerelle ALG SMTP sur laquelle est activé le filtrage de spam DNSBL est *my_smtp_alg*, le résultat sera le suivant :

```
gw-world:/> dnsbl

DNSBL Contexts:

Name      Status  Spam  Drop Accept
------------------------ -------- -------- -------- --------
my_smtp_alg     active  156  65 34299
alt_smtp_alg    inactive  0  0  0
```

L'option *-show* propose un résumé de l'opération de filtrage du spam d'une ALG spécifique.

```
gw-world:/> dnsbl my_smtp_alg -show

DNSBL used by ALG my_smtp_alg
Drop Threshold  : 20
Spam Threshold  : 10
Append TXT records : yes
IP Cache maximum size : 10
IP Cache current size : 5
IP Cache timeout  : 600
Configured BlackLists : 4
Disabled BlackLists : 0
```

```
Current Sessions  : 3

Statistics:
Total number of mails checked : 34520
Number of mails dropped  : 65
Number of mails spam tagged : 156
Number of mails accepted  : 34299

BlackList       Status Value Total Matches
------------------------------ -------- ------ ------- -------
server.spamcenter.org    active  25 34520  221
node1.spamlister.org    active  20 34520  65
```

Pour nettoyer le cache dnsbl de la passerelle *my_smtp_alg* et réinitialiser tous ses compteurs de statistiques, utilisez l'option de commande suivante :

```
gw-world:/> dnsbl my_smtp_alg -clean
```

Remarque

Les URL du serveur DNSBL ci-dessus sont fictives et utilisés uniquement à titre d'exemple. Vous pouvez trouver une liste de DNSBL à l'adresse suivante: http://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists.

POP3

POP3 est un protocole utilisé pour le transfert de messages électroniques qui diffère du protocole SMTP dans le sens où le transfert de messages électroniques se fait directement d'un serveur vers le logiciel client d'un utilisateur.

Options ALG POP3. Les principales fonctionnalités de la passerelle ALG POP3 sont les suivantes :

Block Clear Text Authentication (Bloquer l'authentification en texte clair) Bloque les connexions entre les clients et les serveurs qui transmettent la combinaison nom d'utilisateur/mot de passe en texte clair et donc facilement lisible (certains serveurs peuvent ne pas prendre en charge d'autres méthodes de transmission que celle-ci).

Hide User (Masquer l'utilisateur) Cette option empêche le serveur POP3 de dévoiler qu'un nom d'utilisateur n'existe pas. Cela empêche les utilisateurs d'essayer plusieurs noms d'utilisateurs jusqu'à ce qu'ils en trouvent un valide.

Allow Unknown Commands (Autoriser les commandes inconnues) Vous pouvez autoriser ou interdire les commandes POP3 non standard qui ne sont pas reconnues par la passerelle ALG.

Fail Mode (Mode échec) Lorsque l'analyse de contenu détecte une mauvaise intégrité de fichier, celui-ci peut être autorisé ou interdit.

Verify MIME-type (Vérification du type MIME) Les types de fichiers envoyés en pièces jointes dans les messages électroniques peuvent être vérifiés. Vous pouvez trouver une liste de tous les types de fichiers examinés dans l'*Annexe C, Types de fichiers MIME examinés.*

Anti-Virus Scanning (Analyse antivirus) Le module antivirus de NetDefendOS peut analyser les pièces jointes des messages électroniques à la recherche de code malveillant. Ces fonctionnalités sont décrites de façon détaillée dans la section intitulée « Analyse antivirus ». Les options disponibles sont les suivantes :

Disable (Désactiver) : désactive la surveillance.

Protect (Protéger) : interrompt les téléchargements qui peuvent contenir un virus et les consigne.

Audit (Vérification) : consigne les téléchargements pouvant contenir un virus sans les interrompre.

Options de l'antivirus. Lorsque l'analyse antivirus est activée, vous pouvez utiliser les options suivantes pour contrôler la vérification des fichiers :

Anti-Virus Compression Rate (Taux de compression antivirus) Les fichiers compressés avec un taux de compression supérieur à la valeur spécifiée vont déclencher l'une des actions suivantes :

Allow (Autoriser) : poursuit sans analyse antivirus.

Scan (Analyser) : poursuit l'analyse.

Drop (Ignorer) : ignore le fichier et interrompt le transfert.

Include/Exclude Filetypes (Inclure/Exclure les types de fichiers) Vous pouvez spécifier une liste de types de fichiers qui doivent être inclus dans l'analyse ou exclus.

SIP

Session Initiation Protocol (SIP) est un protocole de signalisation textuel ASCII (UTF-8) utilisé pour établir des sessions entre les clients d'un réseau IP. Il s'agit d'un protocole requête-réponse semblable aux protocoles HTTP et SMTP. Une session peut comprendre un appel VoIP ou représenter une conférence multimédia basée sur la collaboration. L'utilisation du protocole SIP avec les appels VoIP implique que la téléphonie peut devenir une application IP supplémentaire pouvant s'intégrer dans d'autres services.

SIP ne connaît pas les détails du contenu d'une session et se charge uniquement d'établir, de terminer et de modifier des sessions. Les sessions configurées par le protocole SIP sont généralement utilisées pour la diffusion en continu de contenus audio et vidéo sur Internet via le protocole UDP, mais elles peuvent également comporter des échanges basés sur le protocole TCP. Bien que les sessions VoIP reposant sur le protocole UDP sont courantes, les communications qui emploient d'autres protocoles tels que TCP ou TLS peuvent également être impliquées dans une session.

Le protocole SIP est défini par la norme RFC 3261, qui devient une norme de plus en plus prisée pour la VoIP. On peut le comparer au H.323, mais un objectif de conception du SIP est de le rendre plus évolutif que le H.323. (Pour plus d'informations sur la VoIP, reportez-vous également à la section intitulée « H.323 ».)

Composants SIP. Les composants suivants constituent les blocs logiques de la communication SIP :

User Agents (Agents utilisateurs) Un User Agent est une terminaison ou un « client » qui participe à une communication P2P. Il s'agit généralement d'un poste de travail ou d'un périphérique utilisé pour la téléphonie sur IP. Dans cette section, le mot *client* sera souvent utilisé dans ce contexte.

Serveurs proxy Un serveur proxy joue le rôle de routeur dans le protocole SIP. Il fonctionne à la fois comme client et serveur lorsqu'il reçoit des requêtes de client. Les serveurs proxy transfèrent les requêtes aux clients localisés, authentifient et autorisent les accès aux services. Ils mettent également en œuvre les règles de routage d'appels.

Le proxy est généralement situé du côté non protégé du firewall D-Link, c'est-à-dire à l'emplacement du proxy pris en charge par le SIP ALG de NetDefendOS.

Registrars (Agents d'enregistrement) Un serveur qui gère les requêtes SIP REGISTER est appelé « Registrar » ou « agent d'enregistrement ». Le serveur d'enregistrement se charge de localiser l'hôte à partir duquel le client associé est accessible.

Le serveur d'enregistrement et le serveur proxy sont des entités logiques et peuvent se trouver sur le même serveur physique.

Protocoles SIP orientés média. Les sessions SIP utilisent de nombreux sous-protocoles :

SDP *Session Description Protocol* (RFC4566) est utilisé pour initialiser les sessions média.

RTP *Real-time Transport Protocol* (RFC3550) est utilisé en tant que format de paquets sous-jacent pour la

diffusion de contenus audiovisuels par IP grâce au protocole UDP.

RTCP *Real-time Control Protocol* (RFC3550) est utilisé avec le RTP pour offrir une gestion du flux de contrôle hors bande.

Exemples d'utilisation du SIP. Le SIP ALG de NetDefendOS prend en charge les exemples d'utilisation suivants :

1. Internal to External (Interne à externe) La session SIP relie un client situé du côté protégé du firewall D-Link à un client situé du côté externe non protégé. Généralement, la communication a lieu via l'Internet publique.

2. Same Network (Réseau identique) Une particularité du cas de figure interne à interne est le cas où deux clients d'une session se trouvent sur le même réseau.

Dans ces trois cas de figure, le serveur proxy est supposé se trouver du côté non protégé du firewall D-Link.

Options de configuration SIP. Vous pouvez configurer les options suivantes pour un objet SIP ALG :

Maximum Sessions per ID (Nombre de sessions maximales par IP) Le nombre de sessions simultanées dans lesquelles peut être impliqué un client unique est limité par cette valeur. La valeur par défaut est 5.

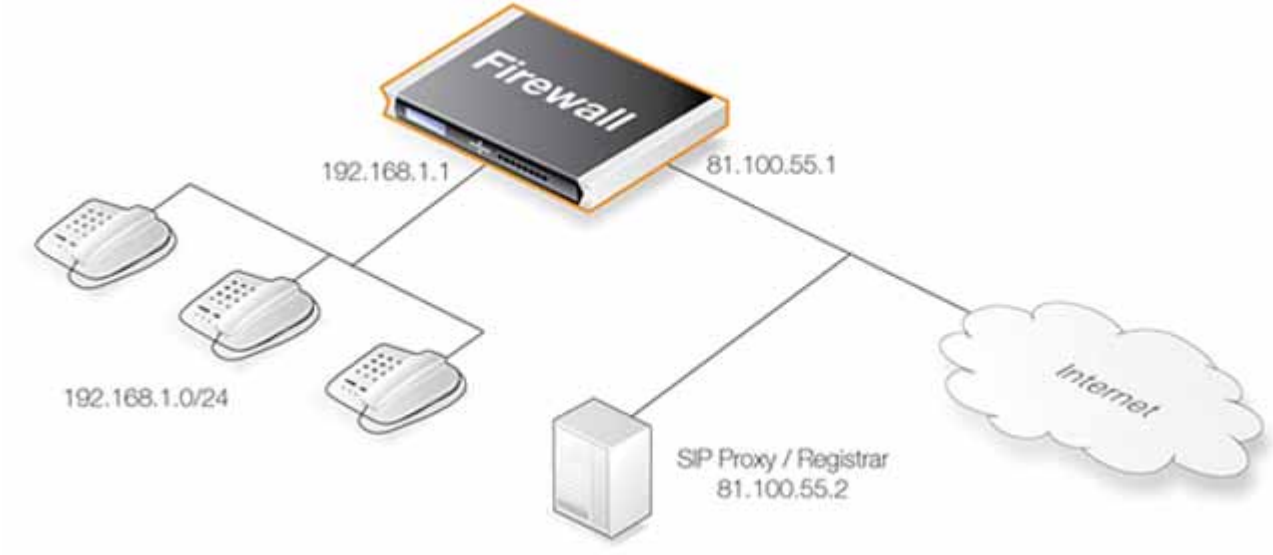
Maximum Registration Time (Durée maximale d'enregistrement) Durée maximale d'enregistrement avec un agent d'enregistrement SIP. La valeur par défaut est *3 600* secondes.

SIP Request-Response Timeout (Délai d'expiration des requêtes-réponses SIP) Durée maximale autorisée pour répondre à des requêtes SIP. Passé ce délai, une condition d'expiration est appliquée. La valeur par défaut est *180 secondes*.

SIP Signal Timeout (Délai d'expiration du signal SIP) Durée maximale autorisée pour les sessions SIP. La valeur par défaut est *43 200 secondes*.

Data Channel Timeout (Délai d'expiration du canal de données) Durée maximale autorisée pour les périodes sans trafic lors d'une session SIP. Lorsque cette valeur est dépassée, une condition d'expiration est appliquée. La valeur par défaut est *120 secondes*.

Résumé de la configuration du SIP. Pour cette configuration, nous considérons un cas de figure où les utilisateurs VoIP se trouvent dans le réseau privé interne de leur société et que la topologie de leur réseau est cachée en utilisant NAT. Ce cas de figure est illustré ci-dessous :



Le serveur proxy SIP du schéma ci-dessus peut également être localisé à distance via Internet. Le serveur proxy SIP doit être configuré avec la fonctionnalité Record-Route (Enregistrer route) activée pour assurer que

l'ensemble du trafic SIP en direction et en provenance des clients de la société sera envoyé par le serveur proxy SIP. Cette option est recommandée, car si vous n'autorisez que le trafic de signalisation SIP envoyé par ce serveur proxy à entrer sur le réseau local, la zone d'attaque est minimisée. Voici les étapes à suivre :

Remarque

Les agents utilisateurs SIP et les serveurs proxy SIP ne doivent pas être configurés pour l'emploi du *NAT Traversal* (franchissement NAT) dans une installation. La technique *Simple Traversal of UDP through NATs* (STUN), par exemple, ne doit pas être utilisée. Le SIP ALG de NetDefendOS se chargera de tous les problèmes de franchissement NAT dans une configuration SIP.

Définissez un objet *SIP ALG* avec les options décrites ci-dessus.

Un objet de *service* est utilisé pour l'ALG à laquelle est associé le SIP ALG de l'étape précédente. Le service doit avoir les paramètres suivants :

Destination Port (port de destination) configuré sur *5060*

Type configuré sur *UDP*

Définissez deux règles dans l'ensemble de règles IP :

Une règle NAT pour le trafic sortant depuis les agents utilisateurs du réseau interne vers le serveur proxy SIP localisé à l'extérieur. Le SIP ALG prendra en charge toutes les traductions d'adresses requises par la règle NAT. Cette traduction va intervenir à la fois au niveau IP et au niveau applicatif. Ni les agents utilisateurs, ni les serveurs proxy ne doivent être au courant que les utilisateurs locaux subissent le NAT.

Une règle Allow (Autoriser) pour le trafic SIP entrant, en provenance du proxy SIP vers l'IP du Firewall D-Link. Cette règle utilisera l'interface core (c'est-à-dire NetDefendOS lui-même) en tant qu'interface de destination. Cette règle est obligatoire pour pouvoir fonctionner avec la règle NAT précédemment configurée. Lorsqu'un appel entrant est reçu, NetDefendOS localise automatiquement le récepteur local, effectue la traduction d'adresse et transfère les messages SIP au récepteur. Cette opération sera réalisée selon l'état interne de la passerelle ALG.

Une règle SAT n'est pas nécessaire puisque l'ALG s'occupe du mappage des adresses IP des utilisateurs individuels, situés derrière la passerelle, en adresses Internet publiques. Lorsqu'un utilisateur situé derrière un Firewall D-Link s'enregistre avec un proxy SIP, il envoie son URI SIP (pour l'identification de manière unique) à l'adresse IP publique du firewall. Lorsqu'un utilisateur externe lance par la suite un appel, le trafic SIP parvient à l'adresse IP publique et l'ALG effectue la traduction nécessaire en adresse IP interne de l'utilisateur.

Vérifiez que les clients sont correctement configurés. Le serveur proxy SIP joue un rôle capital pour localiser l'emplacement actuel du client associé pour la session. L'adresse IP du proxy n'est pas spécifiée directement dans l'ALG. Son emplacement est saisi directement dans le logiciel client utilisé par le client, ou alors, dans certains cas, le client possède un moyen de retrouver l'adresse IP du proxy automatiquement, via DHCP par exemple.

Gestion du trafic de données. Les étapes de configuration ci-dessus traitent de la communication SIP pour établir des communications P2P. Les deux règles IP sont toujours nécessaires pour que les clients puissent accéder au serveur proxy SIP, mais aucune règle n'est nécessaire pour manipuler le trafic de données réel impliqué, par exemple, lors d'un appel VoIP. Le SIP ALG met en place automatiquement les objets NetDefendOS nécessaires pour permettre au trafic de données de traverser le Firewall D-Link, ceux-ci étant invisibles pour l'administrateur.

Conseil

Vérifiez qu'aucune règle existante de l'ensemble de règles IP n'interdit ou n'autorise d'ores et déjà le même type de trafic.

Selon l'environnement SIP, le SIP ALG NetDefendOS peut opérer dans des environnements présentant une topologie cachée avec des adresses IP privées, ainsi que dans des environnements avec des adresses IP publiques. SIP est un protocole hautement configurable et les étapes suivantes décrivent la configuration requise.

H.323

H.323 est une norme approuvée par l'ITU (International Telecommunication Union) qui garantit la compatibilité des transmissions des vidéoconférences sur les réseaux IP. Elle est utilisée pour la communication audio, vidéo et de données en temps réel sur les réseaux reposant sur les paquets comme Internet. Elle spécifie les composants, les protocoles et les procédures pour offrir ces communications multimédia, notamment la téléphonie Internet et la VoIP. (Pour plus d'informations sur la VoIP, reportez-vous également à la section intitulée « SIP ».)

Composants H.323. H.323 comprend quatre éléments principaux :

Terminals (Terminaux)	Périphériques utilisés pour la communication audio et, de manière optionnelle, la communication vidéo et de données, comme par exemple les téléphones, les appareils de conférence ou les « softphones » tels que le logiciel « NetMeeting ».
Gateways (Passerelles)	Une passerelle H.323 relie deux réseaux différents et transporte le trafic entre eux. Elle propose une connectivité entre les réseaux H.323 et les réseaux non H.323 tels que les réseaux téléphoniques publics commutés (RTPC), en traduisant les protocoles et en convertissant les média entre eux. Une passerelle n'est pas nécessaire pour la communication entre deux terminaux H.323.
Gatekeepers (Portiers)	Le portier est un composant du système H.323 utilisé pour la traduction d'adresse, la gestion des autorisations et des authentifications des terminaux et des passerelles. Il peut également prendre en charge la gestion, la comptabilité et la facturation de la bande passante. Le portier peut autoriser que des appels soient effectués directement entre deux extrémités. Il peut également assurer le routage de l'appel, en signalant par lui-même de lancer des fonctions telles que follow-me/find-me (suivez-moi, trouvez-moi), forward on busy (renvoi des appels en cas d'occupation), etc. Il est nécessaire lorsque plusieurs terminaux H.323 se trouvent derrière un périphérique NAT possédant une seule adresse IP publique.
Multipoint Control Units (Unités de contrôle multipoint)	Les MCU prennent en charge des conférences avec au moins trois terminaux H.323. Tous les terminaux H.323 qui participent à l'appel de conférence doivent établir une connexion avec les MCU. Les MCU gèrent ensuite les appels, les ressources et les codecs vidéo et audio utilisés pendant l'appel.

Protocoles H.323. Voici les différents protocoles utilisés pour mettre en œuvre H.323 :

H.225 RAS signaling and Call Control (Setup) signaling (Signalisation H.225 RAS et signalisation Call Control)	Utilisés pour signaler des appels. Permet d'établir une connexion entre deux extrémités H.323. Ce canal pour le signal d'appel est ouvert entre deux extrémités H.323 ou entre une extrémité H.323 et un portier. Pour communiquer entre deux extrémités H.323, on utilise TCP 1720. Pour se connecter à un portier, on utilise le port UDP 1719 (messages H.255 RAS).
H.245 Media Control and Transport (Contrôle multimédia et transport H.245)	Propose un contrôle des sessions multimédia établies entre deux extrémités H.323. Sa tâche principale est de négocier l'ouverture et la fermeture des canaux logiques. Un canal logique est, par exemple, un canal audio utilisé pour les communications vocales. Les canaux vidéo et T.120 sont également appelés canaux logiques pendant la négociation.
T.120	Suite de protocoles de communication et d'application Selon le type de produit H.323, le protocole T.120 peut être utilisé pour le partage d'applications, le transfert de fichiers, ainsi que pour les fonctionnalités de conférence comme les tableaux blancs.

Fonctionnalités H.323 ALG. Le H.323 ALG est une passerelle ALG flexible qui permet aux périphériques H.323 tels que les téléphones et les applications H.323 de passer et de recevoir des appels entre eux lorsqu'ils sont connectés sur des réseaux privés sécurisés par les firewalls D-Link.

La norme H.323 n'a pas été conçue pour gérer NAT, car les adresses IP et les ports sont envoyés dans la charge utile des messages H.323. Le H.323 ALG modifie et traduit les messages H.323 pour s'assurer qu'ils seront routés vers la destination correcte et autorisés à traverser le firewall D-Link.

Le H.323 ALG présente les caractéristiques suivantes :

Le H.323 ALG prend en charge la version 5 de la norme H.323. Cette norme est basée sur H.225.0 v5 et H.245 v10.

En plus de la prise en charge de la voix et des appels vidéo, le H.323 ALG permet également le partage d'applications via le protocole T.120. T.120 utilise le protocole TCP pour le transport des données, tandis que la voix et la vidéo sont transportées via le protocole UDP.

Pour prendre en charge les portiers, la passerelle ALG surveille le trafic entre les extrémités H.323 et le portier, afin de configurer correctement le firewall D-Link pour qu'il laisse passer les appels.

Les règles NAT et SAT sont prises en charge, ce qui permet aux clients et aux portiers d'utiliser des adresses IP privées sur un réseau situé derrière le firewall D-Link.

Configuration du H.323 ALG. La configuration du H.323 ALG standard peut être modifiée pour s'adapter à différents cas de figure. Voici les options paramétrables :

Allow TCP Data Channels (Autoriser les canaux de données TCP) : cette option autorise la négociation des canaux de données reposant sur le protocole TCP. Les canaux de données sont utilisés, par exemple, par le protocole T.120.

Number of TCP Data Channels (Nombre de canaux de données TCP) : précise le nombre de canaux de données TCP autorisés.

Address Translation (Traduction d'adresses) : vous pouvez spécifier le réseau pour le trafic traité par NAT, c'est-à-dire ce qui est autorisé à être traduit. L'IP externe pour le réseau, qui est l'adresse IP à traduire par NAT, est spécifiée. Si l'IP externe est configurée sur *Auto*, elle est alors trouvée automatiquement via une recherche de route.

Translate Logical Channel Addresses (Traduction des adresses des canaux logiques) : cette option est généralement toujours configurée. Si elle n'est pas activée, aucune traduction des adresses des canaux logiques ne sera effectuée et l'administrateur devra être sûr quant aux adresses IP et aux routes utilisées dans un cas de figure particulier.

Gatekeeper Registration Lifetime (Durée de vie d'enregistrement des portiers) : la durée de vie d'enregistrement des portiers peut être contrôlée afin de forcer le réenregistrement des clients à partir d'un certain temps. Un laps de temps plus court exige des clients de s'enregistrer plus fréquemment auprès du portier et diminue la probabilité de rencontrer un problème si le réseau devient inaccessible et que le client pense qu'il est toujours enregistré.

Vous trouverez ci-dessous des cas de figure réseau pour lesquels le H.323 ALG peut s'appliquer. Pour chaque cas de figure, un exemple de configuration, à la fois de la passerelle ALG et des règles, est présenté. Voici les trois définitions de services utilisées dans ces cas de figure :

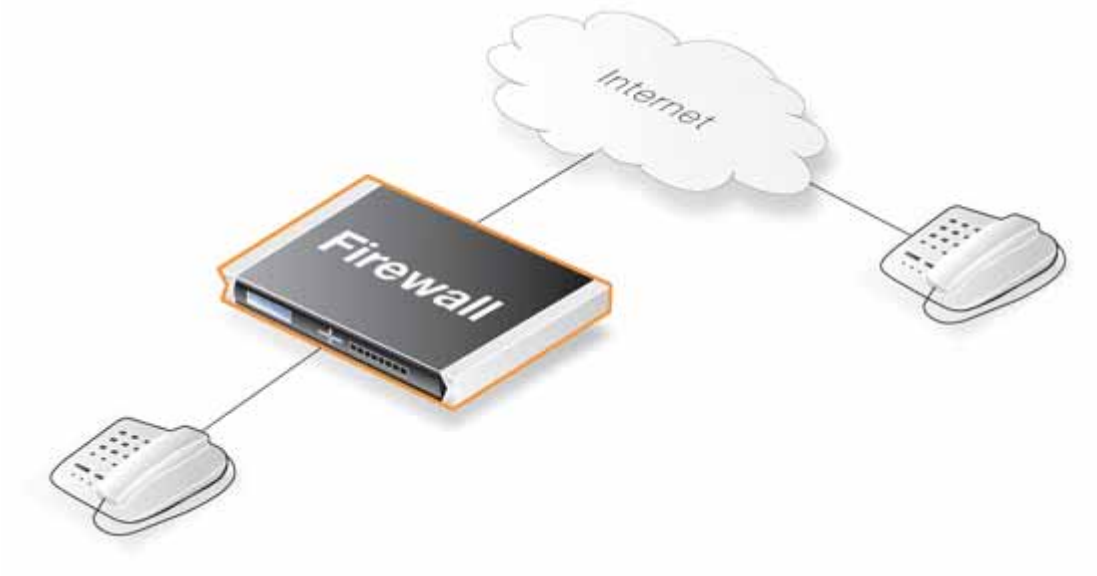
Gatekeeper (UDP ALL > 1719)

H323 (H.323 ALG, TCP ALL > 1720)

H323-Gatekeeper (H.323 ALG, UDP > 1719)

Exemple 6.4. Protection des téléphones situés derrière les firewalls D-Link

Dans le premier cas de figure, un téléphone H.323 est connecté au firewall D-Link sur un réseau (lannet) avec des adresses IP publiques. Pour permettre de passer un appel à partir de ce téléphone vers un autre téléphone H.323 sur Internet et autoriser les téléphones H.323 sur Internet à appeler ce téléphone, nous devons configurer certaines règles. Les règles suivantes doivent être ajoutées à l'ensemble de règles IP ; vérifiez qu'aucune autre règle n'interdit ou n'autorise d'ores et déjà le même type de port/de trafic.



Interface Web
Outgoing Rule (Règle de sortie) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323AllowOut

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : any (toutes)

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : 0.0.0.0/0 (all-nets)

Comment (commentaire) : Allow outgoing calls (Autoriser les appels sortants)

Cliquez sur OK.

Incoming Rule (Règle d’entrée) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323AllowIn

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : lan

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : lannet

Comment (commentaire) : Allow incoming calls (Autoriser les appels entrants)

Cliquez sur OK.

Exemple 6.5. H.323 avec adresses IP privées

Dans ce cas de figure, un téléphone H.323 est connecté au firewall D-Link sur un réseau avec des adresses IP privées. Pour permettre de passer un appel à partir de ce téléphone vers un autre téléphone H.323 sur Internet et autoriser les téléphones H.323 sur Internet à appeler ce téléphone, nous devons configurer certaines règles. Les règles suivantes doivent être ajoutées à l'ensemble de règles IP ; vérifiez qu'aucune autre règle n'interdit ou n'autorise d'ores et déjà le même type de port/de trafic. Étant donné que nous utilisons des adresses IP privées sur le téléphone, le trafic entrant doit subir une opération SAT comme illustré ci-dessous. L'objet ip-phone ci-dessous doit être l'IP interne du téléphone H.323.

Interface Web
Outgoing Rule (Règle de sortie) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323Out

Action : NAT

Service : H323

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : any (toutes)

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : 0.0.0.0/0 (all-nets)

Comment (commentaire) : Allow outgoing calls (Autoriser les appels sortants)

Cliquez sur OK.

Incoming Rule (Règle d'entrée) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323In

Action : SAT

Service : H323

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : wan_ip (IP externe du firewall)

Comment (commentaire) : Allow incoming calls to H.323 phone at ip-phone (Autoriser les appels entrants vers le téléphone H.323 par ip-phone)

Pour SAT, saisissez Translate Destination IP Address (Traduire l'adresse IP de destination) To New IP Address (En nouvelle adresse IP) : ip-phone (Adresse IP du téléphone).

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323In

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : wan_ip (IP externe du firewall)

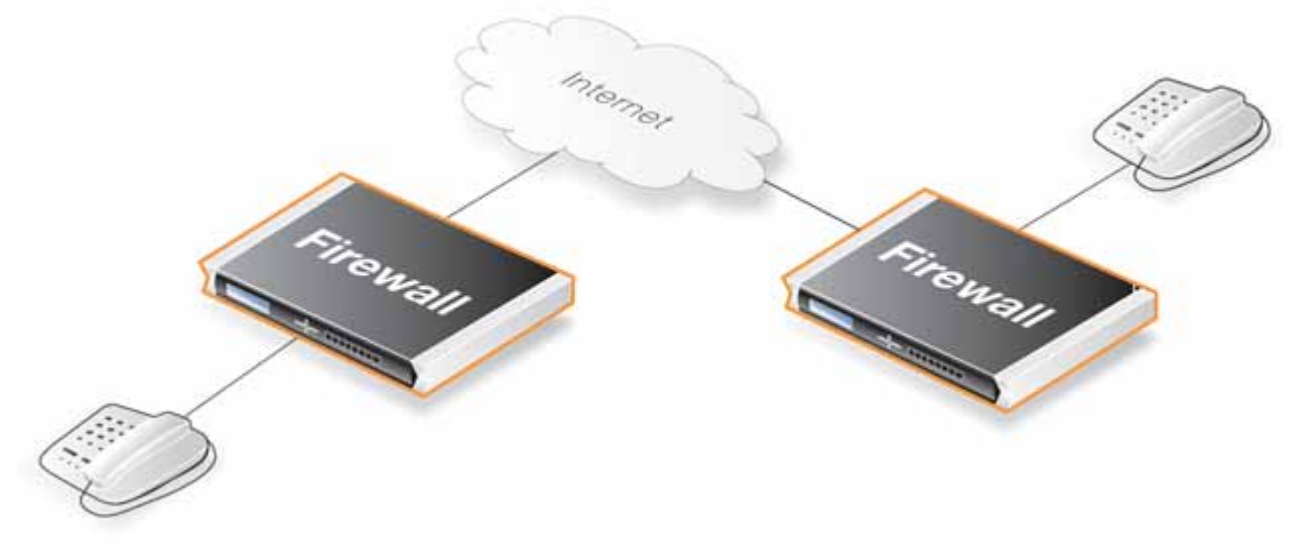
Comment (commentaire) : Allow incoming calls to H.323 phone at ip-phone (Autoriser les appels entrants vers le téléphone H.323 par ip-phone)

Cliquez sur OK.

Pour passer un appel vers le téléphone situé derrière le firewall D-Link, passez un appel vers l'adresse IP externe du firewall. Si plusieurs téléphones H.323 sont placés derrière le firewall, une règle SAT doit être configurée pour chacun d'entre eux. Cela signifie que plusieurs adresses externes doivent être utilisées. Toutefois, on préfère utiliser un portier H.323 comme dans le cas de figure « H.323 avec portier », car il ne nécessite qu'une seule adresse externe.

Exemple 6.6. Deux téléphones situés derrière des firewalls D-Link différents

Dans ce cas de figure, deux téléphones H.323 sont connectés derrière le firewall D-Link sur un réseau avec des adresses IP publiques. Pour passer des appels par Internet avec ces téléphones, les règles suivantes doivent être ajoutées dans les listes de règles des deux firewalls. Vérifiez qu'aucune autre règle n'interdit ou n'autorise d'ores et déjà le même type de port/de trafic.



Interface Web
Outgoing Rule (Règle de sortie) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323AllowOut

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : any (toutes)

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : 0.0.0.0/0 (all-nets)

Comment (commentaire) : Allow outgoing calls (Autoriser les appels sortants)

Cliquez sur OK.

Incoming Rule (Règle d'entrée) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323AllowIn

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : lan

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : lannet

Comment (commentaire) : Allow incoming calls (Autoriser les appels entrants)

Cliquez sur OK.

Exemple 6.7. Utilisation d'adresses IP privées

Dans ce cas de figure, deux téléphones H.323 sont connectés derrière le firewall D-Link sur un réseau avec des adresses IP privées. Pour passer des appels sur Internet avec ces téléphones, les règles suivantes doivent être ajoutées à l'ensemble de règles du firewall ; vérifiez qu'aucune autre règle n'interdit ou n'autorise d'ores et déjà le même type de port/de trafic. Étant donné que nous utilisons des adresses IP privées sur les téléphones, le trafic entrant doit subir une opération SAT comme illustré ci-dessous. L'objet ip-phone ci-dessous doit être l'IP interne du téléphone H.323 situé derrière chaque firewall.

Interface Web

Outgoing Rule (Règle de sortie) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323Out

Action : NAT

Service : H323

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : any (toutes)

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : 0.0.0.0/0 (all-nets)

Comment (commentaire) : Allow outgoing calls (Autoriser les appels sortants)

Cliquez sur OK.

Incoming Rules (Règles d'entrée) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323In

Action : SAT

Service : H323

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : wan_ip (IP externe du firewall)

Comment (commentaire) : Allow incoming calls to H.323 phone at ip-phone (Autoriser les appels entrants vers le téléphone H.323 par ip-phone)

Pour SAT, saisissez Translate Destination IP Address (Traduire l'adresse IP de destination) To New IP Address (En nouvelle adresse IP) : ip-phone (Adresse IP du téléphone).

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323In

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : wan_ip (IP externe du firewall)

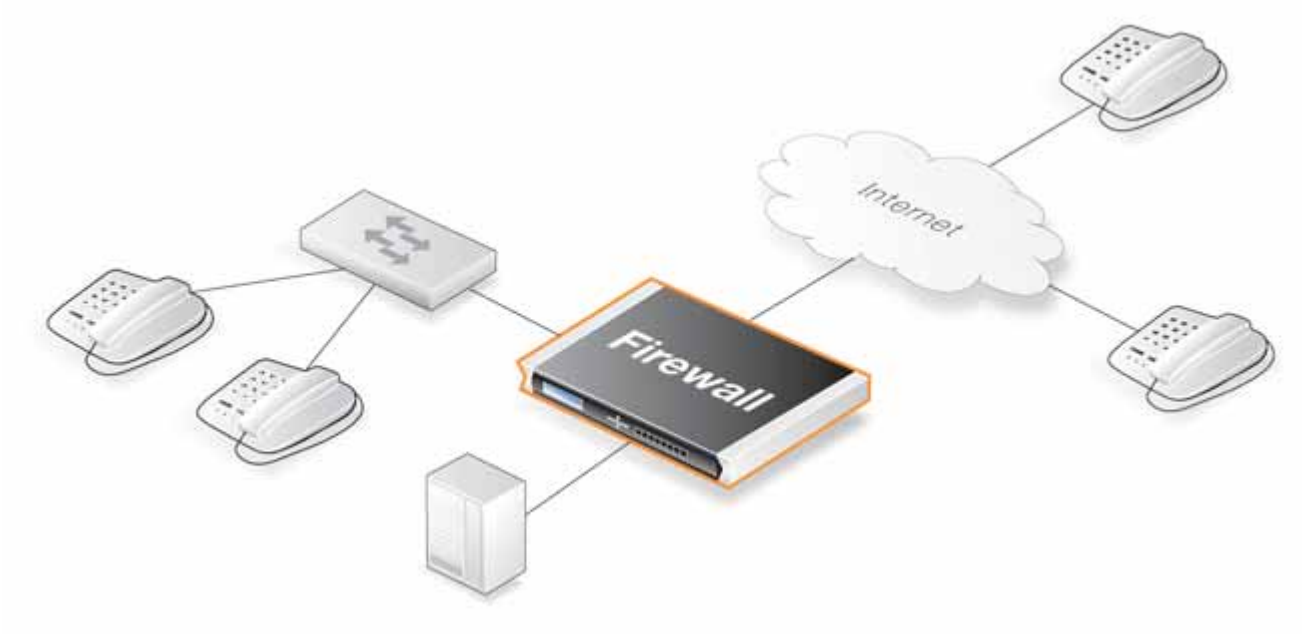
Comment (commentaire) : Allow incoming calls to H.323 phone at ip-phone (Autoriser les appels entrants vers le téléphone H.323 par ip-phone)

Cliquez sur OK.

Pour passer un appel vers le téléphone situé derrière le firewall D-Link, passez un appel vers l'adresse IP externe du firewall. Si plusieurs téléphones H.323 sont placés derrière le firewall, une règle SAT doit être configurée pour chacun d'entre eux. Cela signifie que plusieurs adresses externes doivent être utilisées. Toutefois, on préfère utiliser un portier H.323 car celui-ci ne nécessite qu'une seule adresse externe.

Exemple 6.8. H.323 avec portier

Dans ce cas de figure, un portier H.323 est placé dans la DMZ du firewall D-Link. On configure une règle pour le firewall, qui autorise le trafic entre le réseau privé où sont connectés les téléphones H.323 en interne et le portier situé sur la DMZ. Le portier situé sur la DMZ est configuré avec une adresse privée. Les règles suivantes doivent être ajoutées aux listes de règles des deux firewalls ; vérifiez qu'aucune autre règle n'interdit ou n'autorise d'ores et déjà le même type de port/de trafic.



Interface Web
Incoming Gatekeeper Rules (Règles d'entrée du portier) :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323In

Action : SAT

Service : H323-Gatekeeper

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : wan_ip (IP externe du firewall)

Comment (commentaire) : SAT rule for incoming communication with the Gatekeeper located at ip-gatekeeper (Règle SAT pour les communications entrantes avec le portier situé à l'emplacement ip-gatekeeper)

Pour SAT, saisissez Translate Destination IP Address (Traduire l'adresse IP de destination) To New IP Address (En nouvelle adresse IP) : ip-gatekeeper (Adresse IP du portier).

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323In

Action : Allow (Autoriser)

Service : H323-Gatekeeper

Source Interface (Interface source) : any (toutes)

Destination Interface (Interface de destination) : core (noyau)

Source Network (Réseau source) : 0.0.0.0/0 (all-nets)

Destination Network (Réseau de destination) : wan_ip (IP externe du firewall)

Comment (commentaire) : Allow incoming communication with the Gatekeeper (Autoriser les communications entrantes avec le portier)

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323In

Action : Allow (Autoriser)

Service : Gatekeeper

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : dmz

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : ip-gatekeeper (Adresse IP du portier).

Comment (commentaire) : Allow incoming communication with the Gatekeeper (Autoriser les communications entrantes avec le portier)

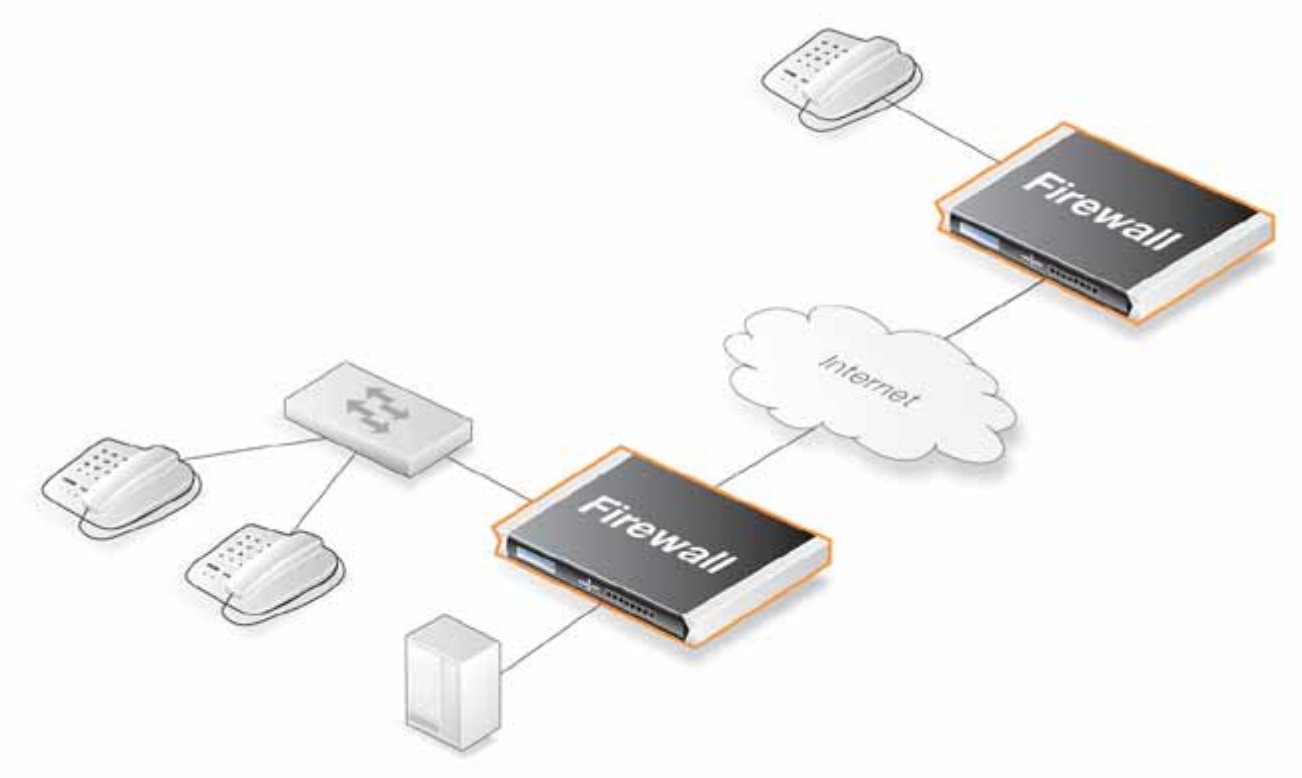
Cliquez sur OK.

Remarque

Il n’est pas nécessaire de préciser de règle spécifique pour les appels sortants. NetDefendOS surveille la communication entre les téléphones « externes » et le portier pour vérifier que les téléphones internes peuvent appeler les téléphones externes enregistrés auprès du portier.

Exemple 6.9. H.323 avec un portier et deux firewalls D-Link

Ce cas de figure est assez similaire au cas de figure n°3, à la différence que le firewall D-Link protège les téléphones « externes ». Le firewall D-Link avec le portier connecté à la DMZ doit être configuré exactement comme dans le cas de figure n°3. Les autres firewalls D-Link doivent être configurés comme suit. Ces règles doivent être ajoutées aux listes de règles ; vérifiez qu’aucune autre règle n’interdit ou n’autorise d’ores et déjà le même type de port/de trafic.



Interface Web

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : H323Out

Action : NAT

Service : H323-Gatekeeper

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : any (toutes)

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : 0.0.0.0/0 (all-nets)

Comment (commentaire) : Allow outgoing communication with a gatekeeper (Autoriser les communications sortantes avec un portier)

Cliquez sur OK.

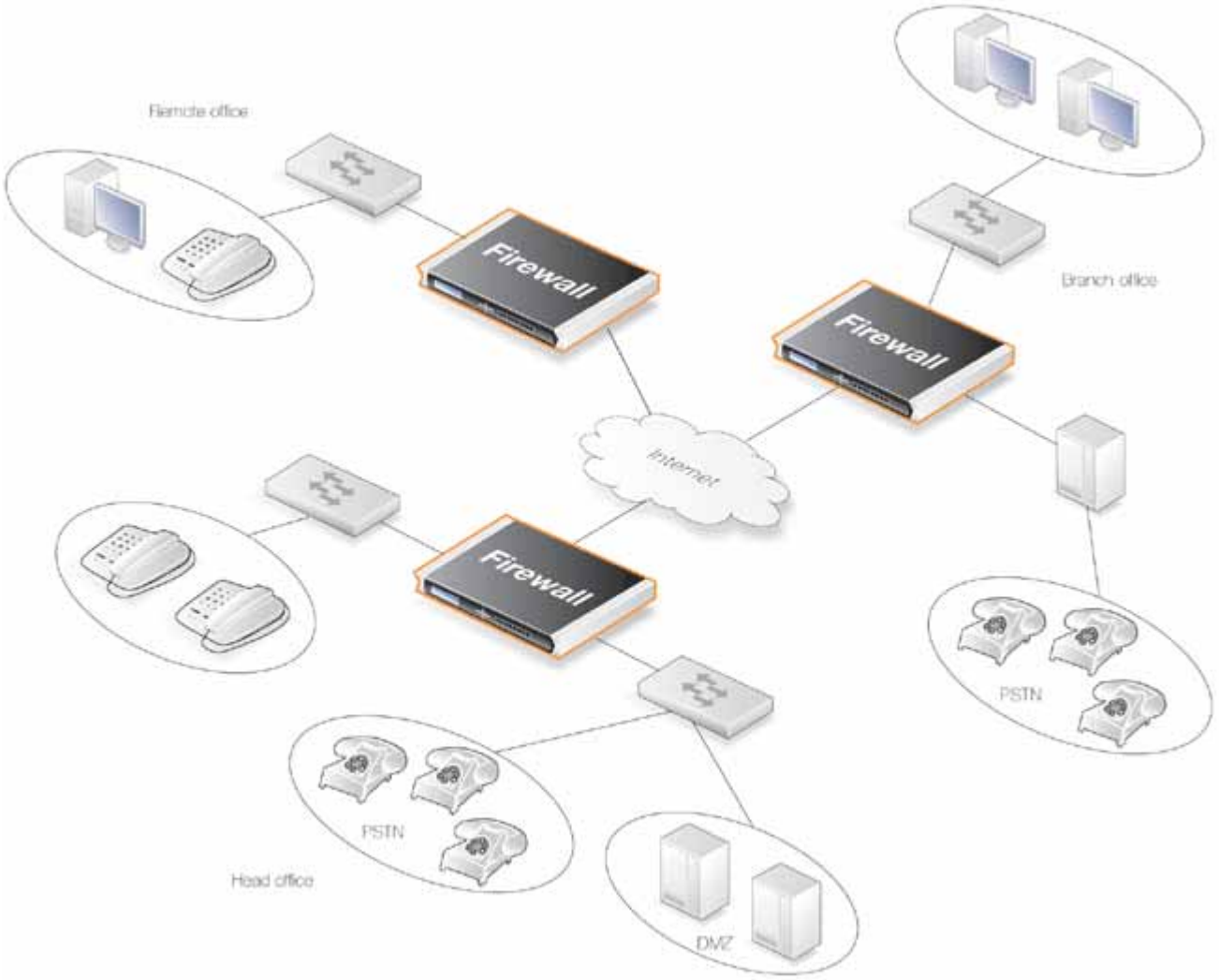
Remarque

Il n’est pas nécessaire de préciser de règle spécifique pour les appels sortants. NetDefendOS surveille la communication entre les téléphones « externes » et le portier pour vérifier que les téléphones internes peuvent appeler les téléphones externes enregistrés auprès du portier.

Exemple 6.10. Utilisation du H.323 ALG en entreprise

Ce cas de figure est un exemple de réseau plus complexe qui montre comment le H.323 ALG peut être déployé en entreprise. Un portier H.323 est placé au siège DMZ pour gérer tous les clients H.323 des sièges, des succursales et des bureaux à distance. Cela permet à l’ensemble de l’entreprise d’utiliser le réseau à la fois pour la

communication vocale et le partage d'applications. On suppose que les tunnels VPN sont correctement configurés et que tous les bureaux utilisent des plages d'adresses IP privées sur leurs réseaux locaux. Tous les appels extérieurs s'effectuent par le réseau téléphonique existant grâce à la passerelle (ip-gateway) connectée au réseau téléphonique ordinaire.



Le siège a placé un portier H.323 dans la DMZ du firewall D-Link d'entreprise. Ce firewall doit être configuré comme suit :

Interface Web

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : LanToGK

Action : Allow (Autoriser)

Service : Gatekeeper

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : dmz

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : ip-gatekeeper

Comment (commentaire) : Allow H.323 entities on lannet to connect to the Gatekeeper (Autoriser les entités H.323 sur lannet à se connecter au portier)

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : LanToGK

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : dmz

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : ip-gateway

Comment (commentaire) : Allow H.323 entities on lannet to call phones connected to the H.323 Gateway on the DMZ (Autoriser les entités H.323 sur lannet à appeler les téléphones connectés à la passerelle H.323 sur la DMZ)

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : GWToLan

Action : Allow (Autoriser)

Service : H323

Source Interface (Interface source) : dmz

Destination Interface (Interface de destination) : lan

Source Network (Réseau source) : ip-gateway

Destination Network (Réseau de destination) : lannet

Comment (commentaire) : Allow communication from the Gateway to H.323 phones on lannet (Autoriser les communications de la passerelle vers les téléphones H.323 sur lannet)

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : BranchToGW

Action : Allow (Autoriser)

Service : H323-Gatekeeper

Source Interface (Interface source) : vpn-branch

Destination Interface (Interface de destination) : dmz

Source Network (Réseau source) : branch-net

Destination Network (Réseau de destination) : ip-gatekeeper, ip-gateway

Comment (commentaire) : Allow communication with the Gatekeeper on DMZ from the Branch network (Autoriser les communications avec le portier sur la DMZ en provenance des succursales)

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : BranchToGW

Action : Allow (Autoriser)

Service : H323-Gatekeeper

Source Interface (Interface source) : vpn-remote

Destination Interface (Interface de destination) : dmz

Source Network (Réseau source) : remote-net

Destination Network (Réseau de destination) : ip-gatekeeper

Comment (commentaire) : Allow communication with the Gatekeeper on DMZ from the Remote network (Autoriser les communications avec le portier sur la DMZ en provenance des réseaux distants)

Cliquez sur OK.

Exemple 6.11. Configuration des entreprises distantes pour H.323

Si les téléphones H.323 et les applications des succursales ou des bureaux à distance doivent être configurés pour utiliser la passerelle H.323 du siège, les firewalls D-Link des succursales et des bureaux à distance doivent être configurés comme suit : (cette règle devrait se trouver à la fois dans les firewalls des succursales et dans ceux des bureaux à distance).

Interface Web

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : ToGK

Action : Allow (Autoriser)

Service : H323-Gatekeeper

Source Interface (Interface source) : lan

Destination Interface (Interface de destination) : vpn-hq

Source Network (Réseau source) : lannet

Destination Network (Réseau de destination) : hq-net

Comment (commentaire) : Allow communication with the Gatekeeper connected to the Head Office DMZ (Autoriser les communications avec le portier connecté au siège DMZ)

Cliquez sur OK.

Exemple 6.12. Autoriser la passerelle H.323 à s'enregistrer auprès du portier

Le firewall D-Link de la succursale possède une passerelle H.323 connectée à sa DMZ. Pour autoriser la passerelle à s'enregistrer auprès du portier H.323 du siège, vous devez configurer la règle suivante :

Interface Web

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : GWToGK

Action : Allow (Autoriser)

Service : H323-Gatekeeper

Source Interface (Interface source) : dmz

Destination Interface (Interface de destination) : vpn-hq

Source Network (Réseau source) : ip-branchgw

Destination Network (Réseau de destination) : hq-net

Comment (commentaire) : Allow the Gateway to communicate with the Gatekeeper connected to the Head Office (Autoriser la passerelle à communiquer avec le portier connecté au siège)

Cliquez sur OK.

Remarque

Il n'est pas nécessaire de préciser de règle spécifique pour les appels sortants. NetDefendOS surveille la communication entre les téléphones « externes » et le portier pour vérifier que les téléphones internes peuvent appeler les téléphones externes enregistrés auprès du portier.

Filtrage de contenu Web

Présentation

Le trafic Web est l'une des plus grandes sources de problèmes de sécurité et des abus d'Internet. La navigation sur des sites inappropriés peut exposer un réseau à un grand nombre de menaces de sécurité ainsi qu'à des responsabilités légales et réglementaires. La productivité et la bande passante Internet peuvent donc être affaiblies.

NetDefendOS propose trois mécanismes de filtrage du contenu Web considéré comme inapproprié pour une entreprise ou un groupe d'utilisateurs :

Le traitement du contenu actif peut être utilisé pour « nettoyer » les pages Web du contenu qui présente une menace potentielle selon l'administrateur, tel que les objets ActiveX et les applets Java.

Le filtrage de contenu statique permet de classer manuellement les sites Web comme étant « bons » ou « mauvais ». Cette fonctionnalité est également appelée *blacklisting* et *whitelisting* des URL.

Le filtrage de contenu dynamique est une fonctionnalité efficace qui permet à l'administrateur d'autoriser ou de bloquer l'accès aux sites Web selon la catégorie dans laquelle ils sont classés par un service de classement automatique. Le filtrage de contenu dynamique nécessite un effort minimum en matière de gestion et offre une très haute précision.

Toutes les fonctions du filtrage de contenu Web sont activées via la passerelle ALG HTTP (reportez-vous à la

section intitulée « HTTP »).

Traitement du contenu actif

Certains contenus Web peuvent renfermer des codes malveillants conçus pour nuire au poste de travail ou au réseau à partir desquels navigue l'utilisateur. Généralement, ces codes sont intégrés dans divers types d'objets ou de fichiers contenus dans les pages Web.

NetDefendOS prend en charge la suppression des types d'objets suivants du contenu d'une page Web :

Les objets ActiveX (y compris Flash)

Les applets Java

Les codes Javascript/VBScript

Les cookies

Les caractères UTF-8 au format invalide (un format d'URL invalide peut être utilisé pour attaquer les serveurs Web)

Vous pouvez sélectionner individuellement les types d'objets à supprimer en configurant les ALG HTTP correspondantes.

Attention

Des précautions doivent être prises avant d'activer la suppression d'objets du contenu Web.

Un grand nombre de sites Web utilisent Javascript et d'autres types de codes côté client et, dans la plupart des cas, ces codes ne sont pas malveillants. Des exemples fréquents de ces codes sont les scripts utilisés pour mettre en place des menus déroulants ou pour afficher ou masquer des éléments sur les pages Web.

La suppression de ce code légitime peut, dans le meilleur des cas, entraîner une déformation dans l'affichage du site Web et dans le pire des cas, provoquer un dysfonctionnement total dans le navigateur. Le traitement du contenu actif doit donc être uniquement utilisé lorsque l'on comprend parfaitement ses conséquences.

Exemple 6.13. Élimination des applets Java et ActiveX

Cet exemple montre comment configurer une ALG HTTP pour éliminer les applets Java et ActiveX. Cet exemple utilise l'objet ALG content_filtering et suppose que vous avez utilisé l'un des exemples précédents.

Interface de ligne de commande

```
gw-world:/> set ALG ALG_HTTP content_filtering RemoveActiveX=Yes RemoveApplets=Yes
```

Interface Web

Sélectionnez Objects > ALG (Objets > ALG).

Dans la liste, cliquez sur notre objet HTTP ALG, content_filtering.

Cochez la case Strip ActiveX objects (including flash) (Éliminer les objets ActiveX, y compris flash).

Cochez la case Strip Java applets (Éliminer les applets Java).

Cliquez sur OK.

Filtrage de contenu statique

NetDefendOS peut autoriser ou bloquer certaines pages Web en fonction de listes d'URL configurées appelées *blacklists* (listes noires) et *whitelists* (listes blanches). Ce type de filtrage est également appelé *Static Content*

Filtering (filtrage de contenu statique). Le principal avantage du filtrage de contenu statique est qu'il est excellent pour cibler des sites Web spécifiques et décider de les bloquer ou de les autoriser.

Ordre de filtrage statique et dynamique. De plus, le filtrage de contenu statique a lieu *avant* le filtrage de contenu dynamique (décrit ci-dessous), ce qui permet de faire manuellement des exceptions au processus automatique de classement dynamique. Dans un cas de figure où des produits doivent être achetés dans une boutique en ligne particulière, le filtrage de contenu dynamique peut être configuré pour empêcher l'accès aux sites d'achats en bloquant la catégorie « shopping ». Si vous placez l'URL de la boutique en ligne dans la liste blanche de la passerelle ALG HTTP, l'accès à cette URL sera toujours autorisé, ayant la priorité sur le filtrage de contenu dynamique.

Wildcarding. Les listes noires et les listes blanches d'URL prennent toutes les deux en charge la correspondance joker des URL afin d'être plus flexibles. Cette correspondance joker s'applique également au chemin qui suit le nom d'hôte de l'URL, ce qui signifie que le filtrage peut être contrôlé au niveau fichier et répertoire.

Voici quelques bons et mauvais exemples d'URL de la liste noire utilisés pour le blocage :

.example.com/	Correct. Bloque tous les hôtes du domaine *example.com* et toutes les pages Web desservies par ces hôtes.
www.example.com/*	Correct. Bloque le site Web *www.example.com* et toutes les pages Web desservies par ce site.
/.gif	Correct. Bloque tous les fichiers ayant l'extension de nom de fichier *.gif* .
www.example.com	Incorrect. Bloque uniquement la première requête au site Web. La navigation sur la page *www.example.com/index.html*, par exemple, ne sera pas bloquée.
example.com/	Incorrect. Provoque également le blocage du site *www.myexample.com* car cela bloque tous les sites se terminant par *example.com*.

Remarque

La fonctionnalité blacklisting des URL du filtrage de contenu Web est un concept qui se détache de la section intitulée « Blacklisting des hôtes et réseaux ».

Exemple 6.14. Configuration des listes blanches et noires

Cet exemple montre comment utiliser le filtrage de contenu statique qui permet à NetDefendOS d'autoriser ou de bloquer certaines pages Web en fonction des listes noires et blanches. Étant donné que c'est l'utilisation du filtrage de contenu statique qui est illustrée, le filtrage de contenu dynamique et le traitement du contenu actif ne sont pas activés dans cet exemple.

Dans ce simple cas de figure, une règle de navigation générale empêche les utilisateurs de télécharger des fichiers .exe. Toutefois, le site Web D-Link propose des programmes sûrs et indispensables que l'on doit autoriser au téléchargement.

Interface de ligne de commande
Commencez par ajouter une ALG HTTP pour le filtrage du trafic HTTP :

```
gw-world:/> add ALG ALG_HTTP content_filtering
```

Créez ensuite une URL pour l'ALG HTTP afin de configurer une liste noire :

```
gw-world:/> cc ALG ALG_HTTP content_filtering

gw-world:/content_filtering> add ALG_HTTP_URL URL=*/*.exe Action=Blacklist
```

Enfin, définissez une exception à la liste noire en créant une liste blanche spécifique :

```
gw-world:/content_filtering> add ALG_HTTP_URL URL=www.D-Link.com/*.exe
  Action=Whitelist
```

Interface Web
Commencez par ajouter une ALG HTTP pour le filtrage du trafic HTTP :

Sélectionnez Objects > ALG > Add > HTTP ALG (Objets > ALG > Ajouter > ALG HTTP).

Saisissez un nom convenable pour l'ALG, par exemple : content_filtering.

Cliquez sur OK.

Créez ensuite une URL pour l'ALG HTTP afin de configurer une liste noire :

Sélectionnez Objects > ALG (Objets > ALG).

Dans la liste, cliquez sur l'ALG HTTP récemment créée (content_filtering), puis sélectionnez Add > HTTP ALG URL (Ajouter > URL de l'ALG HTTP).

Sélectionnez Blacklist dans le menu déroulant Action.

Saisissez */*.exe* dans la boîte de texte URL

Cliquez sur OK.

Enfin, définissez une exception à la liste noire en créant une liste blanche spécifique :

Sélectionnez Objects > ALG (Objets > ALG).

Dans la liste, cliquez sur l'ALG HTTP récemment créée (*content_filtering*), puis sélectionnez Add > HTTP ALG URL (Ajouter > URL de l'ALG HTTP).

Sélectionnez Whitelist dans le menu déroulant Action.

Saisissez *www.D-Link.com/*.exe* dans la boîte de texte URL.

Cliquez sur OK.

Il vous suffit simplement de continuer à ajouter des listes noires et blanches spécifiques jusqu'à ce que le filtre réponde à vos besoins.

Filtrage de contenu Web dynamique

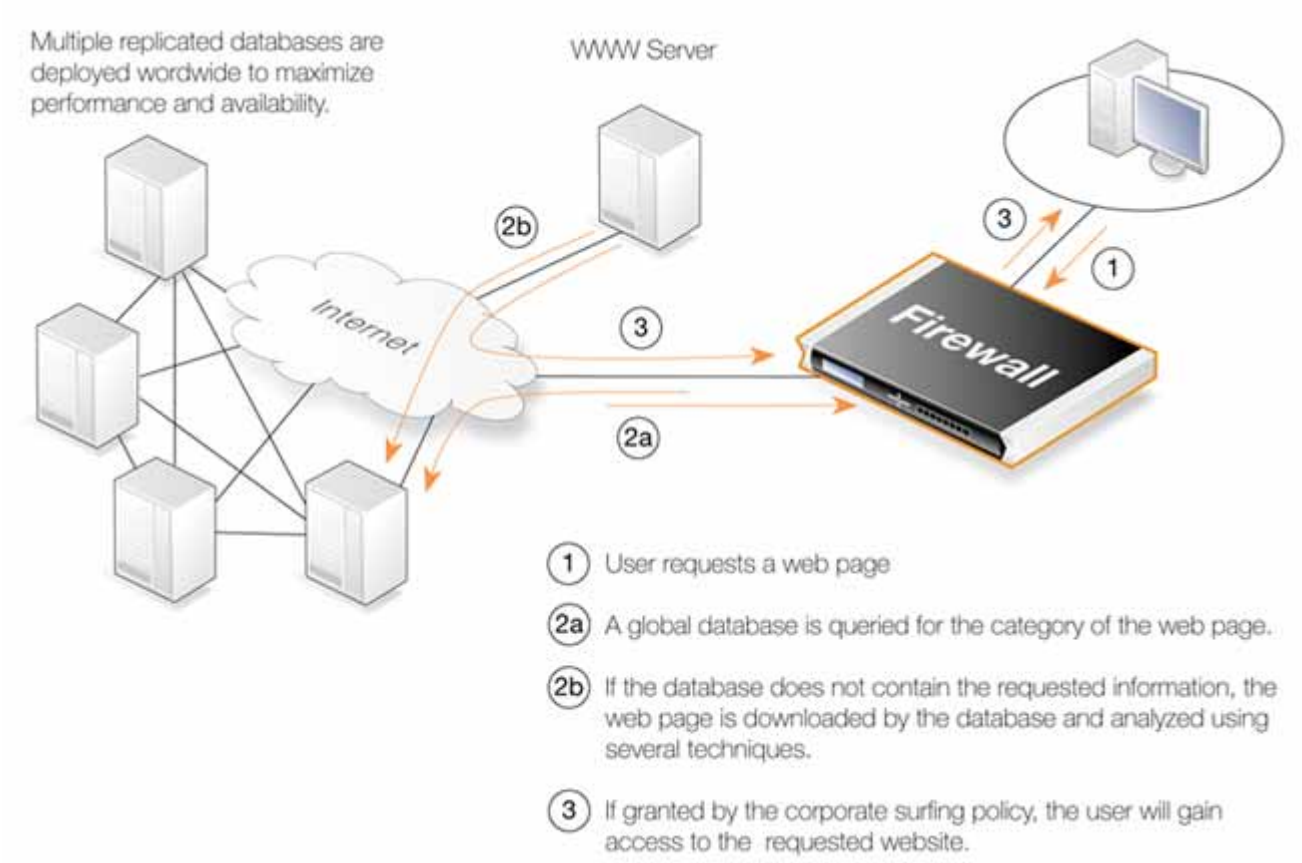
Présentation. NetDefendOS prend en charge le *Dynamic Web Content Filtering* (filtrage de contenu Web dynamique) qui permet à un administrateur d'autoriser ou de bloquer les accès aux pages Web suivant leur contenu. Cette fonctionnalité est automatisée et vous n'avez pas à spécifier manuellement les URL à autoriser ou bloquer. D-Link garantit une infrastructure internationale de bases de données contenant un très grand nombre d'adresses URL de sites Web actuels, regroupées en plusieurs catégories : shopping, actualités, sport, contenu pour adultes, etc. Ces bases de données sont mises à jour toutes les heures avec de nouvelles URL organisées en catégories, pendant que les URL antérieures incorrectes sont rejetées. Le contenu de la base de données est international et englobe des sites Web en de nombreuses langues différentes qui sont hébergés dans des pays du monde entier.

Disponibilité du filtrage de contenu Web dynamique sur les modèles D-Link

Le filtrage de contenu dynamique est disponible uniquement sur les produits DFL-260 et DFL-860 de D-Link.

Flux de traitement des URL. Lorsqu'un utilisateur demande l'accès à un site Web, NetDefendOS envoie une requête à ces bases de données pour récupérer la catégorie du site demandé. L'accès au site est ensuite autorisé ou refusé à l'utilisateur suivant les règles de filtrage en place pour cette catégorie. Si l'accès est refusé, une page Web expliquant à l'utilisateur que le site demandé a été bloqué s'affiche. Pour rendre le processus de recherche de route aussi rapide que possible, NetDefendOS conserve les URL récemment visités dans un cache local. La mise en cache peut s'avérer très efficace car une communauté d'utilisateurs donnée, comme par exemple un groupe d'étudiants d'université, navigue souvent sur un nombre de sites limité.

Figure 6.2. Flux de filtrage de contenu dynamique



Si l'URL de la page Web demandée n'existe pas dans les bases de données, alors le contenu de la page Web de cette URL sera automatiquement téléchargé dans l'entrepôt central de données D-Link et automatiquement analysé grâce à une combinaison de techniques telles que les réseaux de neurones et le filtrage par motif. Une fois organisée en catégories, l'URL est envoyée aux bases de données internationales et NetDefendOS reçoit la catégorie pour cette URL. Le filtrage de contenu dynamique nécessite, par conséquent, un effort de gestion minimum.

Remarque

Les nouvelles URL qui ne sont pas classées en catégories et envoyées sur le réseau D-Link sont considérées comme des propositions anonymes et les sources à l'origine des nouvelles propositions ne sont pas mises en mémoire.

Classement des pages et non des sites. Le filtrage dynamique de NetDefendOS classe les pages Web et non les sites. En d'autres termes, un site Web peut contenir des pages spécifiques qui doivent être bloquées, sans que le site le soit dans son intégralité. NetDefendOS permet un blocage par pages, de façon à ce que les utilisateurs puissent toujours accéder aux parties des sites non bloquées par la règle de filtrage.

Activation. Le filtrage de contenu dynamique est une fonctionnalité qui peut être activée en souscrivant un abonnement supplémentaire à ce service. C'est une fonctionnalité qui s'ajoute à la licence normale de NetDefendOS. Pour une description complète des services d'abonnement, consultez l'*Annexe A, Abonnement aux mises à jour de sécurité*.

Après avoir souscrit un abonnement, un objet ALG HTTP peut être défini avec le filtrage de contenu dynamique activé. Cet objet est ensuite associé à un objet de service, l'objet de service étant lui-même associé à une règle de l'ensemble de règles IP pour déterminer quel trafic doit être soumis au filtrage. Cela permet de configurer une règle de filtrage détaillée en fonction des paramètres de filtrage utilisés pour les règles de l'ensemble de règles IP.

Conseil

Si vous souhaitez que le contenu de votre règle de filtrage change suivant la période de la journée, utilisez un objet programme dans la règle IP correspondante. Pour plus d'informations, reportez-vous à la section

intitulée « Programmation ».

Exemple 6.15. Activation du filtrage de contenu Web dynamique

Cet exemple montre comment configurer une règle de filtrage de contenu dynamique pour le trafic HTTP de intnet vers all-nets. La règle sera configurée pour bloquer tous les moteurs de recherche et cet exemple suppose que le système utilise une seule règle NAT pour le trafic HTTP de intnet vers all-nets.

Interface de ligne de commande
(La règle NAT est appelée NATHttp pour cet exemple dans l'interface de ligne de commande)
Tout d'abord, créez un objet ALG HTTP :

```
gw-world:/> add ALG ALG_HTTP content_filtering WebContentFilteringMode=Enabled
    FilteringCategories=SEARCH_SITES
```

Puis, créez un objet de service à l'aide de la nouvelle ALG HTTP :

```
gw-world:/> add ServiceTCPUDP http_content_filtering Type=TCP DestinationPorts=80
    ALG=content_filtering
```

Enfin, modifiez la règle NAT pour utiliser le nouveau service :

```
gw-world:/> set IPRule NATHttp Service=http_content_filtering
```

Interface Web

Tout d'abord, créez un objet ALG HTTP :

Sélectionnez Objects > ALG > Add > HTTP ALG (Objets > ALG > Ajouter > ALG HTTP).

Spécifiez un nom convenable pour la passerelle ALG, par exemple *content_filtering.*

Cliquez sur l'onglet Web Content Filtering (Filtrage de contenu Web).

Sélectionnez Enabled (Activé) dans la liste Mode.

Dans la liste Blocked Categories (Catégories bloquées), sélectionnez Search Sites (Recherche de sites) et cliquez sur le bouton >>.

Cliquez sur OK.

Créez ensuite un objet de service à l'aide de la nouvelle ALG HTTP :

Sélectionnez Local Objects > Services > Add > TCP/UDP service (Objets locaux > Services > Ajouter > Service TCP/UDP).

Spécifiez un nom convenable pour le service, par exemple *http_content_filtering*.

Sélectionnez TCP dans la liste déroulante Type

Saisissez 80 dans la boîte de texte Destination Port (port de destination).

Dans la liste ALG, sélectionnez l'ALG HTTP que vous venez de créer.

Cliquez sur OK.

Enfin, modifiez la règle NAT pour utiliser le nouveau service :

Sélectionnez Rules > IP Rules (Règles > Règles IP).

Dans la commande de la liste, cliquez sur la règle NAT qui gère votre trafic HTTP.

Cliquez sur l'onglet Service.

Sélectionnez votre nouveau service (http_content_filtering) dans la liste pre-defined Service (Services prédéfinis).

Cliquez sur OK.

Le filtrage de contenu dynamique est à présent activé pour l'ensemble du trafic Web de lannet à all-nets. Pour valider la fonctionnalité, procédez comme suit :

Sur un poste de travail du réseau lannet, lancez un navigateur Web standard.

Essayez de naviguer sur un moteur de recherche, par exemple www.google.com.

Si tout est configuré correctement, votre navigateur affichera une page Web pour vous informer que le site demandé est bloqué.

Mode Audit. En *Audit Mode* (mode audit), le système classe et consigne l'ensemble de la navigation selon la règle de filtrage de contenu, mais les sites Web interdits sont toujours accessibles aux utilisateurs. Cela signifie que la fonctionnalité de filtrage de contenu de NetDefendOS peut être utilisée comme un outil d'analyse pour examiner quelles catégories de sites Web font l'objet de tentatives d'accès par une communauté d'utilisateurs ainsi que la fréquence de ces accès.

Après quelques semaines de fonctionnement en mode audit, il est plus facile d'avoir une bonne compréhension du comportement de navigation et également du gain de temps potentiel qui peut être réalisé en activant le filtrage de contenu. Il est recommandé que l'administrateur mette en place progressivement le blocage, en bloquant seulement certaines catégories à la fois. Cela permet aux utilisateurs individuels de s'habituer à l'idée que le blocage existe et d'éviter une contestation générale si toutes les catégories sont bloquées simultanément. La mise en place progressive permet également de mieux déterminer si les objectifs de blocage sont atteints.

Exemple 6.16. Activation du mode Audit

Cet exemple repose sur le même cas de figure que l'exemple précédent, mais le mode Audit est à présent activé.

Interface de ligne de commande
Tout d'abord, créez un objet ALG HTTP :

```
gw-world:/> add ALG ALG_HTTP content_filtering WebContentFilteringMode=Audit
    FilteringCategories=SEARCH_SITES
```

Interface Web

Tout d'abord, créez un objet ALG HTTP :

Sélectionnez Objects > ALG > Add > HTTP ALG (Objets > ALG > Ajouter > ALG HTTP).

Spécifiez un nom convenable pour la passerelle ALG, par exemple *content_filtering*

Cliquez sur l'onglet Web Content Filtering (Filtrage de contenu Web).

Sélectionnez Audit dans la liste Mode
Dans la liste Blocked Categories (Catégories bloquées), sélectionnez Search Sites (Recherche de sites) et cliquez sur le bouton >>.

Cliquez sur OK.

L'exemple précédent décrit la procédure à suivre pour créer ensuite un objet de service en utilisant la nouvelle ALG HTTP et modifier la règle NAT pour utiliser le nouveau service.

Autoriser l'annulation. Le filtrage de contenu actif peut parfois empêcher les utilisateurs de réaliser des tâches autorisées. Imaginez un agent de change traitant avec des éditeurs de jeux en ligne. Dans son travail quotidien, il peut avoir besoin de naviguer sur des sites de jeu de hasard pour procéder aux évaluations des entreprises. Si la règle de son entreprise bloque les sites de jeu de hasard, il ne pourra pas faire son travail.

C'est pourquoi NetDefendOS prend en charge une fonctionnalité appelée *Allow Override.* Lorsque cette fonctionnalité est activée, le filtrage de contenu affiche un avertissement à l'utilisateur, lui signalant qu'il est sur le point d'entrer sur un site interdit d'après la politique d'entreprise et que sa visite sur le site sera consignée. Cette page est appelée *restricted site notice* (notification de site restreint). L'utilisateur est ensuite libre de continuer

vers cette URL ou d'abandonner la requête pour ne pas être consigné.

En activant cette fonctionnalité, seuls les utilisateurs qui possèdent une raison valable de visiter des sites inappropriés pourront le faire. Les autres éviteront ces sites afin de ne pas dévoiler leurs habitudes de navigation.

> **Attention**
> L'activation de cette fonctionnalité peut permettre aux utilisateurs de naviguer sur des sites en rapport avec le site visité.

Reclassement des sites bloqués. Étant donné que le processus de classement des sites Web inconnus est automatisé, il existe toujours un risque minime d'attribuer une classification incorrecte à certains sites. NetDefendOS propose un mécanisme qui autorise les utilisateurs à proposer manuellement une nouvelle classification pour les sites.

Ce mécanisme peut être activé au niveau de l'ALG HTTP, ce qui signifie que vous pouvez choisir d'activer cette fonctionnalité pour les utilisateurs habituels ou uniquement pour un groupe d'utilisateurs sélectionné.

Lorsque le reclassement est activé et qu'un utilisateur demande l'accès à un site interdit, la page de blocage comportera une liste déroulante contenant toutes les catégories disponibles. Si l'utilisateur pense que le site Web demandé est classé de façon incorrecte, il peut choisir une catégorie plus appropriée dans la liste déroulante et la soumettre comme proposition.

L'URL du site Web demandé ainsi que la catégorie proposée sont alors envoyées vers l'entrepôt de données central D-Link pour y subir une inspection manuelle. Cette inspection peut entraîner le reclassement du site dans la catégorie proposée ou bien dans une catégorie que l'on estime appropriée.

Exemple 6.17. Reclassement d'un site bloqué

Cet exemple montre comment un utilisateur peut proposer le reclassement d'un site Web lorsqu'il pense que son classement est incorrect. Ce mécanisme est activé au niveau de l'ALG HTTP.

Interface de ligne de commande
Tout d'abord, créez un objet ALG HTTP :

```
gw-world:/> add ALG ALG_HTTP content_filtering WebContentFilteringMode=Enable
    FilteringCategories=SEARCH_SITES AllowReclassification=Yes
```

Poursuivez ensuite la configuration de l'objet service et la modification de la règle NAT comme nous l'avons fait dans les exemples précédents.

Interface Web

Tout d'abord, créez un objet ALG HTTP :

Sélectionnez Objects > ALG > Add > HTTP ALG (Objets > ALG > Ajouter > ALG HTTP).

Spécifiez un nom convenable pour la passerelle ALG, par exemple *content_filtering.*

Cliquez sur l'onglet Web Content Filtering (Filtrage de contenu Web).

Sélectionnez Enabled (Activé) dans la liste Mode.

Dans la liste Blocked Categories (Catégories bloquées), sélectionnez Search Sites (Recherche de sites) et cliquez sur le bouton >>.

Cochez la case Allow Reclassification (Autoriser le reclassement).

Cliquez sur OK.

Poursuivez ensuite la configuration de l'objet service et la modification de la règle NAT comme nous l'avons fait dans les exemples précédents.
Le filtrage de contenu dynamique est à présent activé pour l'ensemble du trafic Web de lannet à all-nets et l'utilisateur peut proposer un reclassement des sites bloqués. Pour valider la fonctionnalité, procédez comme suit :

Sur un poste de travail du réseau lannet, lancez un navigateur Web standard.

Essayez de naviguer sur un moteur de recherche, par exemple www.google.com.

Si tout est configuré correctement, votre navigateur Web affichera une page de blocage, contenant une liste déroulante avec toutes les catégories disponibles.

L'utilisateur peut à présent sélectionner une catégorie plus appropriée et proposer un reclassement.

Catégories de filtrage de contenu

Cette section fournit une liste de toutes les catégories utilisées avec le filtrage de contenu dynamique et décrit l'usage de chaque catégorie.

Catégorie 1 : Contenu pour adulte. Un site Web peut être classé dans la catégorie « contenu pour adulte » si son contenu comprend la description ou la représentation d'actes sexuels ou érotiques, ou des messages à caractère pornographique. Cette catégorie exclut les sites Web contenant des informations relatives à la sexualité et à la santé sexuelle, qui peuvent être classées dans la catégorie « sites de santé » (21). Voici quelques exemples :

www.naughtychix.com

www.fullonxxx.com

Catégorie 2 : Actualités. Un site Web peut être classé dans la catégorie « actualités » si son contenu comprend des articles d'actualité comprenant des événements locaux récents (par exemple une ville, un pays) ou culturels, y compris les prévisions météorologiques. Ceux-ci incluent généralement la plupart des publications d'actualité en ligne en temps réel ou les revues technologiques ou spécialisées. Cette catégorie exclut les cours financiers (reportez-vous à la catégorie « sites d'affaires » (11)) et le sport (consultez la catégorie « sports » (16)). Voici quelques exemples :

www.newsunlimited.com

www.dailyscoop.com

Catégorie 3 : Recherche d'emploi. Un site Web peut être classé dans la catégorie « recherche d'emploi » si son contenu comprend des services permettant de rechercher un emploi ou de mettre en ligne des demandes d'emploi. Cette catégorie comprend également la rédaction et la publication de CV, les entretiens d'embauche, le recrutement du personnel et les stages. Voici quelques exemples :

www.allthejobs.com

www.yourcareer.com

Catégorie 4 : Jeux de hasard. Un site Web peut être classé dans la catégorie « jeux de hasard » si son contenu comprend des publicités, des encouragements et des services incitant à participer à toutes sortes de jeux de hasard, impliquant de l'argent ou non. Cette catégorie comprend les jeux en ligne, les cotes des bookmakers et les sites Web de loterie. Elle exclut les jeux traditionnels ou les jeux vidéo ; consultez la catégorie « sites de jeux » (10). Voici quelques exemples :

www.blackjackspot.com

www.pickapony.net

Catégorie 5 : Voyages / Tourisme. Un site Web peut être classé dans la catégorie « voyages / tourisme » si son contenu comprend des informations concernant les voyages, notamment les voyages de loisir et les services de réservation. Voici quelques exemples :

www.flythere.nu

www.reallycheaptix.com.au

Catégorie 6 : Shopping. Un site peut être classé dans la catégorie « shopping » si son contenu comprend toutes sortes de publicités pour des biens ou des services payants et peut également inclure les services utilisés pour

réaliser ces transactions en ligne. Cette catégorie comprend la promotion de marchés, la vente de catalogues et les services de commercialisation. Voici quelques exemples :

www.megamall.com

www.buy-alcohol.se

Catégorie 7 : Divertissement. Un site Web peut être classé dans la catégorie « divertissement » si son contenu comprend toute forme générale de divertissement qui n'est pas précisément couverte par une autre catégorie. Ce sont, par exemple, les sites de musique, de films, de hobbies, d'intérêt particulier et les fans clubs. Cette catégorie comprend également les pages Web personnelles, notamment celles fournies par les FAI. Les catégories suivantes englobent plus précisément différents types de contenus de divertissement : pornographie / sexe (1), jeux d'argent (4), salons de discussion (8), sites de jeux (10), sport (16), clubs et sociétés (22) et téléchargement de musique (23). Voici quelques exemples :

www.celebnews.com

www.hollywoodlatest.com

Catégorie 8 : Salons de discussion. Un site Web peut être classé dans la catégorie « salons de discussion » si son contenu comporte ou se focalise sur des groupes de discussion en ligne et en temps réel. Cette catégorie comprend également les journaux internes, les serveurs télématiques, les forums en ligne, les groupes de discussion ainsi que les URL pour le téléchargement de logiciels de discussion. Voici quelques exemples :

www.thetalkroom.org

chat.yazoo.com

Catégorie 9 : Sites de rencontres. Un site Web peut être classé dans la catégorie « sites de rencontres » si son contenu comporte des services permettant de soumettre et modifier des petites annonces personnelles, d'arranger des rencontres romantiques avec d'autres personnes et s'il comporte des agences matrimoniales d'« épouses sur catalogue » et des services d'accompagnement. Voici quelques exemples :

adultmatefinder.com

www.marriagenow.com

Catégorie 10 : Les sites de jeux. Un site Web peut être classé dans la catégorie « sites de jeux » si son contenu comporte ou se focalise sur les tests de jeux vidéo ou de jeux traditionnels ou s'il intègre les services de téléchargement de logiciels de jeux vidéo ou la participation à des jeux en ligne. Voici quelques exemples :

www.gamesunlimited.com

www.gameplace.com

Catégorie 11 : Sites d'investissement. Un site Web peut être classé dans la catégorie « sites d'investissement » si son contenu comporte des informations ou des services relatifs aux investissements personnels. Les URL de cette catégorie comportent du contenu tel que les services de courtage, les solutions de portefeuille en ligne, la gestion des gains et les cours de la bourse. Cette catégorie exclut les services bancaires en ligne ; consultez la catégorie « banque en ligne » (12). Voici quelques exemples :

www.loadsofmoney.com.au

www.putsandcalls.com

Catégorie 12 : Banque en ligne. Un site Web peut être classé dans la catégorie « banque en ligne » si son contenu comprend des informations ou des services bancaires en ligne. Cette catégorie n'inclut pas le contenu relatif aux investissements ; consultez la catégorie « sites d'investissement » (11). Voici quelques exemples :

www.nateast.co.uk

www.borganfanley.com

Catégorie 13 : Crimes / Terrorisme. Un site Web peut être classé dans la catégorie « crimes / terrorisme » si son

contenu comporte la description, la promotion ou l'enseignement d'activités, de cultures ou d'idées criminelles ou terroristes. Voici quelques exemples :

www.beatthecrook.com

Catégorie 14 : Croyances / Cultes personnels. Un site Web peut être classé dans la catégorie « croyances / cultes personnels » si son contenu comporte la description, la représentation ou l'enseignement de systèmes de croyances religieuses et de leurs pratiques. Voici quelques exemples :

www.paganfed.demon.co.uk

www.cultdeadcrow.com

Catégorie 15 : Politique. Un site Web peut être classé dans la catégorie « politique » si son contenu comporte des idées ou des informations de nature politique, des informations électorales et des groupes de discussions politiques. Voici quelques exemples :

www.democrats.org.au

www.political.com

Catégorie 16 : Sport. Un site Web peut être classé dans la catégorie « sport » si son contenu comporte des informations ou des instructions liées aux sports de loisirs ou professionnels ou bien des comptes rendus et résultats d'événements sportifs. Voici quelques exemples :

www.sportstoday.com

www.soccerball.com

Catégorie 17 : Sites www de messagerie électronique. Un site peut être classé dans la catégorie « sites www de messagerie électronique » si son contenu comporte des services de messagerie en ligne basés sur le Web. Voici quelques exemples :

www.coldmail.com

mail.yazoo.com

Catégorie 18 : Violence / Choc. Un site Web peut être classé dans la catégorie « violence / choc » si son contenu est extrêmement violent ou de nature choquante. Cette catégorie comprend la promotion, la description ou la représentation d'actes violents, ainsi que les sites Web à contenu indésirable qui ne peuvent être classés dans d'autres catégories. Voici quelques exemples :

www.itstinks.com

www.ratemywaste.com

Catégorie 19 : Malveillant. Un site Web peut être classé dans la catégorie « malveillant » si son contenu peut endommager un ordinateur ou un environnement informatique ou provoquer une consommation superflue de bande passante réseau. Cette catégorie inclut également les URL de « phishing », conçues pour capter des informations personnelles d'authentification utilisateur en se faisant passer pour un organisme légitime. Voici quelques exemples :

hastalavista.baby.nu

Catégorie 20 : Moteurs de recherche. Un site Web peut être classé dans la catégorie « moteurs de recherche » si son activité principale consiste à offrir des services de recherche sur Internet. Consultez la section relative aux catégories uniques au début de ce document. Voici quelques exemples :

www.zoogle.com

www.yazoo.com

Catégorie 21 : Sites de santé. Un site Web peut être classé dans la catégorie « sites de santé » si son contenu

comporte des informations ou des services concernant la santé, y compris la sexualité et la santé sexuelle, ainsi que les groupes de soutien, les informations hospitalières et chirurgicales ainsi que les revues médicales. Voici quelques exemples :

www.thehealthzone.com

www.safedrugs.com

Catégorie 22 : Groupes et associations. Un site Web peut être classé dans la catégorie « groupes et associations » si son contenu comprend des informations et des services liés à un groupe ou une association. Cette catégorie inclut les sites Web de membres ou de colloques. Voici quelques exemples :

www.sierra.org

www.walkingclub.org

Catégorie 23 : Téléchargement de musique. Un site Web peut être classé dans la catégorie « téléchargement de musique » s'il propose des services de téléchargement, d'envoi et de partage de musique en ligne, ainsi que de la diffusion audio à large bande passante. Voici quelques exemples :

www.onlymp3s.com

www.mp3space.com

Catégorie 24 : Orienté gestion. Un site Web peut être classé dans la catégorie « orienté gestion » si son contenu fait référence aux activités quotidiennes générales ou au bon fonctionnement d'Internet, comme par exemple les mises à jour de navigateurs Web. Dans la plupart des cas, l'accès aux sites Web de cette catégorie ne sera pas considéré comme improductif ou inapproprié.

Catégorie 25 : Liste de blocage publique. Cette catégorie comporte des URL spécifiées par un organisme gouvernemental, qui sont considérées comme inappropriées pour être visionnées par le grand public du fait de leur nature extrême. Voici quelques exemples :

www.verynastystuff.com

www.unpleasantvids.com

Catégorie 26 : Éducatif. Un site Web classé dans la catégorie « éducatif » peut appartenir à d'autres catégories mais possède un contenu qui se rapporte à des services éducatifs, qui apporte une valeur pédagogique ou qui est considéré ou comme une ressource éducative par les organismes d'éducation. Cette catégorie est remplie sur demande ou sur proposition de divers organismes d'éducation. Voici quelques exemples :

highschoolessays.org

www.learn-at-home.com

Catégorie 27 : Publicité. Un site Web peut être classé dans la catégorie « publicité » si son activité principale consiste à offrir des informations ou des services qui concernent la publicité. Voici quelques exemples :

www.admessages.com

www.tripleclick.com

Catégorie 28 : Drogue/Alcool. Un site Web peut être classé dans la catégorie « drogue/alcool » si son contenu comprend des informations ou des services qui concernent la prévention de l'alcool et des drogues. Certaines URL classées dans cette catégorie peuvent donc être classées dans la catégorie « santé ». Voici quelques exemples :

www.the-cocktail-guide.com

www.stiffdrinks.com

Catégorie 29 : Informatique/IT. Un site Web peut être classé dans la catégorie « informatique/IT » si son contenu comprend des informations ou des services qui concernent l'informatique. Voici quelques exemples :

www.purplehat.com

www.gnu.org

Catégorie 30 : Maillot de bain/lingerie/mannequinat. Un site Web peut être classé dans la catégorie « maillot de bain/lingerie/mannequinat » si son contenu comprend des informations ou des images concernant les maillots de bain, la lingerie ou le mannequinat en général. Voici quelques exemples :

www.vickys-secret.com

sportspictured.cnn.com/features/2002/swimsuit

Catégorie 31 : Spam. Un site Web peut être classé dans la catégorie « spam » si on le trouve dans les messages électroniques envoyés en nombre ou dans les spams. Voici quelques exemples :

kaqsovdij.gjibhgk.info

www.pleaseupdateyourdetails.com

Catégorie 32 : Non-gérés. Les sites non classés et ceux qui ne rentrent pas dans l'une des autres catégories sont placés dans ce groupe. Il n'est pas courant de bloquer cette catégorie car cela peut occasionner le blocage de la plupart des URL inoffensives.

Analyse antivirus

Présentation

Le module antivirus de NetDefendOS protège contre les codes malveillants transportés au cours d'un téléchargement de fichier. Les fichiers peuvent être téléchargés dans le cadre d'une page Web lors d'un transfert HTTP, d'un téléchargement FTP ou bien en tant que pièce jointe dans un message électronique distribué par SMTP. Les codes malveillants de ces téléchargements peuvent avoir différents objectifs qui varient des simples désagréments causés par des programmes à des objectifs plus sérieux comme le renvoi de mots de passe, des numéros de cartes de crédit et d'autres informations sensibles. Le terme « virus » peut être utilisé comme description générique de toutes les formes de codes malveillants transportés par les fichiers.

Combinaison avec l'analyse antivirus client. Contrairement à l'IDP, orienté principalement sur les attaques contre les serveurs, l'analyse antivirus se focalise sur les téléchargements effectués par les clients. L'antivirus de NetDefendOS est conçu pour compléter l'analyse antivirus standard, normalement effectuée localement par un logiciel spécialisé installé sur les ordinateurs clients. IDP n'est pas conçu pour se substituer totalement à l'analyse locale mais est plutôt utilisé comme bouclier supplémentaire pour renforcer la protection du client. Plus important encore, il peut jouer le rôle de sauvegarde lorsque l'analyse antivirus locale du client ne fonctionne pas pour une quelconque raison.

L'antivirus de NetDefendOS est activé via la passerelle ALG HTTP (reportez-vous à la section intitulée « HTTP »).

Disponibilité de l'antivirus sur les modèles D-Link

L'analyse antivirus est disponible uniquement sur les produits DFL-260 et DFL-860 de D-Link.

Mise en œuvre :

Diffusion. Lorsqu'un transfert de fichier est diffusé à travers le firewall D-Link, NetDefendOS analyse le flux de données pour détecter la présence de virus si le module antivirus est activé. Puisque les fichiers sont diffusés et pas entièrement lus en mémoire, une quantité de mémoire minimale est nécessaire et l'effet sur le débit global est minime.

Filtrage par motif. Le processus de filtrage repose sur le *pattern matching* (filtrage par motif) qui compare les données aux schémas de virus connus stockés dans une base de données et peut déterminer si un virus est sur le point d'être téléchargé vers un utilisateur placé derrière un firewall D-Link. Lorsqu'un virus est reconnu dans le contenu d'un fichier, le téléchargement en cours peut être arrêté.

Types de fichiers analysés. Le module antivirus de NetDefendOS peut analyser les types de téléchargements de fichiers suivants :

HTTP, FTP, TFTP, SMTP et POP3

Tout type de fichier non compressé transféré par ces protocoles.

Si le fichier téléchargé a été compressé, les fichiers ZIP et GZIP peuvent être analysés.

L'administrateur peut toujours ignorer l'analyse de fichiers spécifiques ou préciser une taille limite pour les fichiers analysés. Si aucune taille limite n'est spécifiée, alors il n'existe aucune limite supérieure par défaut pour les tailles de fichiers.

Analyses simultanées. Il n'existe pas de limite fixe pour définir combien d'analyses antivirus peuvent avoir lieu simultanément dans un seul firewall D-Link. Toutefois, la mémoire libre disponible peut limiter le nombre d'analyses simultanées pouvant être exécutées. L'administrateur peut augmenter la quantité de mémoire libre disponible par défaut pour l'analyse antivirus en modifiant le paramètre avancé AVSE_MAXMEMORY. Ce paramètre précise le pourcentage de mémoire totale à utiliser pour l'analyse antivirus.

Comportement spécifique du protocole. Puisque l'analyse antivirus est mise en œuvre par une ALG, des fonctionnalités spécifiques du protocole sont mises en place dans NetDefendOS. Avec le FTP, par exemple, l'analyse considère les canaux de transfert de données et de double contrôle ouverts et peut envoyer une requête via la connexion de contrôle pour interrompre un téléchargement lorsqu'un virus est détecté.

Activation de l'analyse antivirus

Association avec une ALG. L'activation de l'analyse antivirus est réalisée par une ALG associée au protocole cible. Un objet ALG HTTP doit tout d'abord être créé, l'antivirus étant activé. L'ALG doit ensuite être associée à l'objet de service approprié pour que le protocole soit analysé. Cet objet de service est ensuite associé à une règle de l'ensemble de règles IP, qui définit l'origine et la destination du trafic auquel va s'appliquer l'ALG.

Création de règles antivirus. Puisque l'ensemble de règles IP permet de déployer la fonctionnalité antivirus, ce déploiement peut reposer sur des règles (*policy based*). Les règles IP peuvent spécifier que l'ALG et l'analyse antivirus qui lui est associée peuvent s'appliquer au trafic allant dans une certaine direction et entre des adresses IP et/ou réseaux sources et de destination spécifiques. Vous pouvez également appliquer une planification à l'analyse antivirus, de façon à ce qu'elle ait lieu uniquement à certains moments.

La base de données des signatures

Safestream. L'analyse antivirus de NetDefendOS est mise en œuvre par D-Link via la base de données de signatures de virus « SafeStream ». La base de données SafeStream est créée et gérée par Kaspersky, leader mondial en matière de détection de virus. La base de données propose une protection contre presque toutes les menaces virales connues comme les chevaux de Troie, les vers, les portes dérobées, etc. La base de données est également entièrement testée pour offrir un taux de faux positifs proche de zéro.

Mises à jour de la base de données. La base de données SafeStream est mise à jour quotidiennement avec des nouvelles signatures de virus. Les anciennes signatures sont rarement enlevées, mais plutôt remplacées par des signatures qui couvrent plusieurs virus. La copie locale NetDefendOS de la base de données SafeStream doit donc être mise à jour régulièrement et ce service de mise à jour est activé dans le cadre de l'abonnement à l'antivirus D-Link.

Souscription au service antivirus de D-Link

La fonctionnalité antivirus de D-Link est un composant additionnel à la licence de base de D-Link que vous pouvez acheter sous la forme d'un abonnement renouvelable. Un abonnement antivirus comprend des mises à jour régulières de la base de données SafeStream de Kaspersky pendant la période de souscription avec les signatures des dernières menaces virales.

Pour vous abonner au service d'antivirus, veuillez vous reporter à l'*Annexe A, « Souscription aux mises à jour de sécurité »*.

Options de l'antivirus

Lors de la configuration de l'analyse antivirus dans une ALG, vous pouvez définir les paramètres suivants :

1. Options générales.

Mode — Doit être défini sur l'une des options suivantes :
A. Enabled (Activé), qui signifie que l'antivirus est actif.
B. Audit, qui signifie qu'il est actif mais que la consignation sera la seule action entreprise.

Fail mode behaviour (Comportement en mode échec) — Si une analyse antivirus échoue pour une quelconque raison, le transfert peut être interrompu ou autorisé, l'événement étant consigné.

2. Type de fichier à bloquer/à autoriser.

Action — Lorsqu'un type de fichier particulier est téléchargé, l'administrateur peut explicitement décider si le fichier doit être autorisé ou bloqué au téléchargement.

Types de fichiers — Le type de fichier à bloquer ou à autoriser peut être ajouté à la liste. « GIF » peut, par exemple, être ajouté.

Si un type de fichier figure dans la liste autorisée, il faut noter que la correspondance MIME fonctionnera même si elle est désactivée (à condition que le type de fichier fasse partie de la liste de l'*Annexe C, « Types de fichiers MIME vérifiés* ». Ceci permet de se protéger contre une attaque qui tente d'exploiter le fait que le type de fichier figure dans la liste autorisée.

3. Option « exclure de l'analyse ». Vous pouvez, si vous le souhaitez, exclure explicitement de l'analyse antivirus certains types de fichiers. Cela peut augmenter le débit global si un type de fichier exclu est couramment rencontré dans un cas de figure particulier.

4. Limite du taux de compression. Si l'on souhaite analyser des fichiers compressés, NetDefendOS doit les décompresser pour examiner leur contenu. Certains types de données peuvent entraîner des taux de compression très élevés où le fichier compressé représente une petite fraction de sa taille d'origine lorsqu'il est décompressé. Cela peut nécessiter de décompresser une pièce jointe de petite taille en un fichier beaucoup plus important par comparaison, ce qui peut placer une charge excessive sur les ressources de NetDefendOS et ralentir sensiblement le débit.

Pour éviter cette situation, l'administrateur peut spécifier une limite pour le *Compression Ratio* (taux de compression). Si la limite du taux est réglée sur 10, cela implique que si le fichier décompressé est 10 fois plus grand que le fichier compressé, l'action spécifiée doit être entreprise. Cette action peut être l'une des suivantes :

Allow (Autoriser) : le fichier est autorisé à passer sans subir d'analyse antivirus.

Scan (Analyser) : comme d'habitude, analyse le fichier à la recherche de virus

Drop (Ignorer) : ignore le fichier

Dans les trois cas ci-dessus, l'événement est consigné.

Vérification du type MIME. Vous pouvez utiliser les options de l'ALG concernant l'intégrité des fichiers avec l'analyse antivirus pour vérifier que le contenu du fichier correspond au type MIME qu'il prétend être.

Le type MIME désigne un type de fichier. Un fichier peut, par exemple, être identifié comme étant de type *.gif* et doit, par conséquent, contenir des données d'image de ce type. Certains virus peuvent tenter de se dissimuler à l'intérieur des fichiers en utilisant un type de fichier trompeur. Un fichier peut se faire passer pour un fichier *.gif*, mais les données du fichier ne vont pas correspondre au motif de données de ce type car il est infecté par un virus.

L'activation de cette fonction est recommandée pour s'assurer que ce type d'attaque ne puisse pas permettre à un virus de passer. Les types MIME qu'il est possible de vérifier sont répertoriés dans l'*Annexe C, Types de fichiers MIME vérifiés*.

Configuration de l'heure exacte du système. Pour que la fonctionnalité de mise à jour automatique du module antivirus puisse fonctionner correctement, il est important que l'heure système de NetDefendOS soit paramétrée de façon exacte. Une heure incorrecte peut entraîner la désactivation de la mise à jour automatique.

La commande console

```
> updatecenter -status
```

affiche l'état actuel de la fonctionnalité de mise à jour automatique. Vous pouvez également le faire via l'interface utilisateur Web.

Mise à jour dans les clusters de haute disponibilité. La mise à jour des bases de données antivirus pour les deux firewalls D-Link d'un cluster de haute disponibilité est effectuée automatiquement par NetDefendOS. Dans un cluster, il y a toujours une unité *active* et une unité inactive. Seule l'unité active du cluster vérifiera régulièrement les nouvelles mises à jour de la base de données. Si une nouvelle mise à jour de la base de données est disponible, on aura cette suite d'événements :

L'unité active détermine qu'une nouvelle mise à jour est disponible et télécharge les fichiers nécessaires pour cette mise à jour.

L'unité active effectue une reconfiguration automatique pour mettre à jour sa base de données.

Cette reconfiguration provoque un basculement, de sorte que l'unité passive devient l'unité active.

Lorsque la mise à jour est terminée, la nouvelle unité active télécharge également les fichiers de mise à jour et effectue une reconfiguration.

Cette seconde reconfiguration provoque un nouveau basculement, de sorte que l'unité passive redevient l'unité active.

Ces étapes entraînent la mise à jour des bases de données des deux firewalls D-Link dans un cluster et la restauration des rôles actif/passif d'origine. Pour plus d'informations sur les clusters de haute disponibilité, consultez le *chapitre 11, Haute disponibilité*.

Exemple 6.18. Activation de l'analyse antivirus

Cet exemple montre comment configurer une règle d'analyse antivirus pour le trafic HTTP de lannet à all-nets. Nous supposons qu'une règle NAT pour gérer ce trafic est déjà définie dans l'ensemble de règles IP.

Interface de ligne de commande
Tout d'abord, créez un objet ALG HTTP en activant l'analyse antivirus :

```
gw-world:/> set ALG ALG_HTTP anti_virus Antivirus=Protect
```

Créez ensuite un objet de service à l'aide de la nouvelle ALG HTTP :

```
gw-world:/> add ServiceTCPUDP http_anti_virus Type=TCP DestinationPorts=80
   ALG=anti_virus
```

Enfin, modifiez la règle NAT pour utiliser le nouveau service :

```
gw-world:/> set IPRule NATHttp Service=http_anti_virus
```

Interface Web

A. Tout d'abord, créez un objet ALG HTTP :

Sélectionnez Objects > ALG > Add > HTTP ALG (Objets > ALG > Ajouter > ALG HTTP).

Spécifiez un nom convenable pour l'ALG, par exemple *anti_virus.*

Cliquez sur l'onglet Antivirus.

Sélectionnez Protect (Protéger) dans la liste déroulante Mode.

Cliquez sur OK.

B. Créez ensuite un objet de service à l'aide de la nouvelle ALG HTTP :

Sélectionnez Local Objects > Services > Add > TCP/UDP service (Objets locaux > Services > Ajouter > Service TCP/UDP).

Spécifiez un nom convenable pour le service, par exemple http_anti_virus.

Sélectionnez TCP dans la liste déroulante Type.

Saisissez 80 dans la boîte de texte « Destination Port » (Port de destination).

Dans la liste déroulante ALG, sélectionnez l'ALG HTTP que vous venez de créer.

Cliquez sur OK.

C. Enfin, modifiez la règle NAT (appelée dans cet exemple NATHttp) pour utiliser le nouveau service :

Sélectionnez Rules > IP Rules (Règles > Règles IP).

Dans la commande de la liste, cliquez sur la règle NAT qui gère le trafic entre lannet et all-nets.

Cliquez sur l'onglet Service.

Sélectionnez votre nouveau service, http_anti_virus, dans la liste déroulante « pre-defined Service » (Services prédéfinis).

Cliquez sur OK.

L'analyse antivirus est à présent activée pour l'ensemble du trafic Web de lannet à all-nets.

Prévention et détection des intrusions

Présentation

Définition d'une intrusion. Les ordinateurs serveurs peuvent parfois présenter des vulnérabilités qui les exposent aux attaques véhiculées par le trafic réseau. Les vers, les chevaux de Troie et les portes dérobées sont des exemples de ces attaques qui peuvent potentiellement mettre en péril ou prendre le contrôle d'un serveur. Le terme générique *intrusions* peut être utilisé pour décrire ces menaces orientées serveur.

Détection des intrusions. Les intrusions diffèrent des virus dans le sens où un virus est normalement contenu dans un seul téléchargement de fichier qui est d'habitude téléchargé par un système client. Une intrusion se manifeste comme un motif de données Internet malveillant qui vise à contourner les mécanismes de sécurité d'un serveur. Les intrusions ne sont pas rares et peuvent constamment évoluer car leur création peut être automatisée par le pirate. L'IDP de NetDefendOS propose une importante ligne de défense contre ces menaces.

La prévention et la détection des intrusions (IDP) est un module de NetDefendOS conçu pour se protéger contre ces tentatives d'intrusions. Il fonctionne en surveillant le trafic réseau lorsqu'il traverse le firewall D-Link, à la recherche de motifs qui indiquent une tentative d'intrusion. Une fois détectée, l'IDP de NetDefendOS autorise des actions qui permettent de neutraliser à la fois la tentative d'intrusion et sa source.

Questions IDP. Pour avoir un système efficace et fiable, les questions suivantes doivent être abordées :

Quelle sorte de trafic doit être analysé ?

Qu'est ce qu'on doit rechercher dans ce trafic ?

Quelle action doit être entreprise lorsqu'une intrusion est détectée ?

Composants NetDefendOS IDP. L'IDP NetDefendOS traite les questions IDP ci-dessus grâce aux mécanismes suivants :

Les règles IDP sont définies par l'administrateur pour déterminer quel trafic doit être analysé.

Le filtrage par motif est appliqué par l'IDP NetDefendOS au trafic qui correspond à une règle IDP lorsqu'il traverse le firewall.

Si l'IDP NetDefendOS détecte une intrusion, l'action spécifiée pour la règle IDP déclenchante est entreprise.

Les règles IDP, le filtrage par motif et les actions de la règle IDP sont décrites dans les sections suivantes.

Disponibilité de l'IDP sur les modèles D-Link

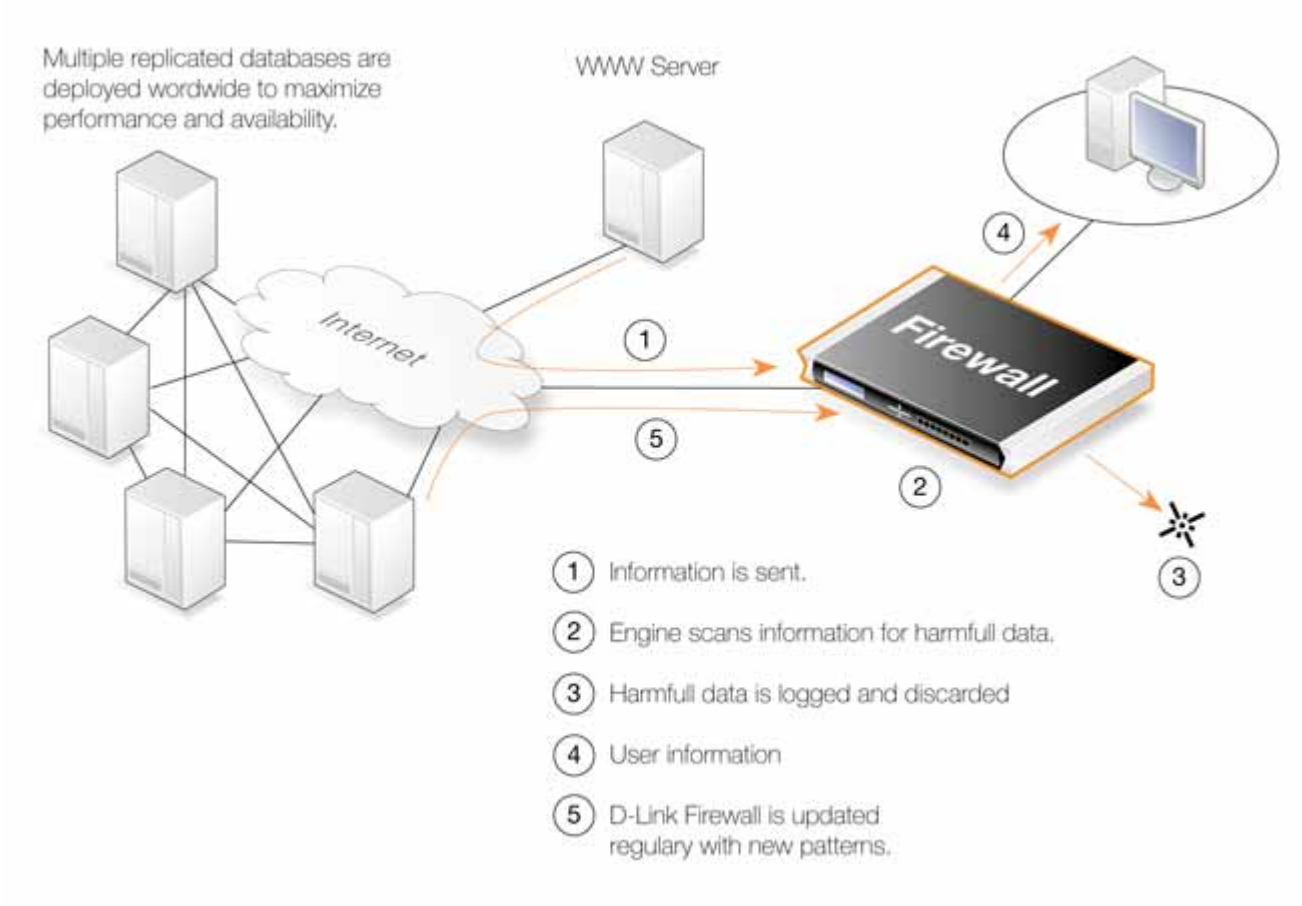
IDP maintenance et IDP avancé. D-Link propose deux types d'IDP :

L'IDP maintenance est un système IDP de base fourni en standard avec les firewalls D-Link DFL-210/800/1600/2500. Il s'agit d'un IDP simplifié qui offre une protection de base contre les attaques. Il est possible de le mettre à niveau vers la version professionnelle *Advanced IDP* (IDP avancé).

L'IDP avancé est un système d'abonnement IDP avec une plage de signatures de base de données élargie pour les installations de type professionnel/entreprises. Cette fonctionnalité est disponible sur tous les firewalls D-Link. L'IDP maintenance peut être considéré comme un sous-ensemble limité de l'IDP avancé et les sections suivantes décrivent le mode de fonctionnement du service IDP avancé.

Souscription au service IDP avancé de D-Link. Vous pouvez acheter l'IDP avancé en tant que composant additionnel à la licence de base de NetDefendOS. Il s'agit d'un service d'abonnement qui permet de télécharger la base de données des signatures IDP sur une installation NetDefendOS, cette base de données étant régulièrement mise à jour avec les dernières menaces d'intrusions. Pour des informations complètes sur l'obtention du service IDP, reportez-vous à l'*Annexe A, Abonnement aux mises à jour de sécurité*.

Figure 6.3. Mise à jour de la base de données IDP



Une nouvelle base de données de signatures, mise à jour, est téléchargée automatiquement par le système NetDefendOS à un intervalle défini. Le téléchargement s'effectue via une connexion HTTP au réseau de serveurs

D-Link qui distribue les mises à jour les plus récentes de la base de données de signatures. Si la base de données des signatures du serveur possède une version plus récente que la base de données locale actuelle, cette nouvelle base de données sera téléchargée et remplacera la version antérieure.

IDP, IPS et IDS

Dans la terminologie D-Link, on utilise indifféremment les termes prévention et détection des intrusions (IDP), système de prévention des intrusions (IPS) et système de détection des intrusions (IDS).

Configuration de l'heure exacte du système. Pour que la fonctionnalité de mises à jour automatiques du module IDP puisse fonctionner correctement, il est important que l'heure système de NetDefendOS soit paramétrée de façon exacte. Une heure incorrecte peut entraîner la désactivation des mises à jour automatiques.

La commande console

```
> updatecenter -status
```

affiche l'état actuel de la fonctionnalité de mise à jour automatique. Vous pouvez également le faire via l'interface utilisateur Web.

Mise à jour dans les clusters de haute disponibilité. La mise à jour des bases de données IDP pour les deux firewalls D-Link d'un cluster de haute disponibilité est effectuée automatiquement par NetDefendOS. Dans un cluster, il y a toujours une unité *active* et une unité inactive. Seule l'unité active du cluster vérifiera régulièrement les nouvelles mises à jour de la base de données. Si une nouvelle mise à jour de la base de données est disponible, on aura cette suite d'événements :

L'unité active détermine qu'une nouvelle mise à jour est disponible et télécharge les fichiers nécessaires pour cette mise à jour.

L'unité active effectue une reconfiguration automatique pour mettre à jour sa base de données.

Cette reconfiguration provoque un basculement, de sorte que l'unité passive devient l'unité active.

Lorsque la mise à jour est terminée, la nouvelle unité active télécharge également les fichiers de mise à jour et effectue une reconfiguration.

Cette seconde reconfiguration provoque un nouveau basculement, de sorte que l'unité passive redevient l'unité active.

Ces étapes entraînent la mise à jour des bases de données des deux firewalls D-Link dans un cluster et la restauration des rôles actif/passif d'origine. Pour plus d'informations sur les clusters de haute disponibilité, consultez le *chapitre 11, Haute disponibilité*.

Règles IDP

Composants d'une règle. Une règle IDP définit le type de trafic ou de service qui doit être analysé. Une règle IDP ressemble en apparence à une règle IP. Les règles IDP sont établies comme les autres règles de sécurité de NetDefendOS telles que les règles IP. Une règle IDP spécifie une combinaison donnée d'interfaces/adresses source/de destination et elle est également associée à un objet de service qui définit quels protocoles analyser. Un horodatage peut aussi être associé à une règle IDP. Plus important encore, une règle IDP précise l'action à entreprendre lorsqu'une intrusion est détectée dans le trafic ciblé par la règle.

Traitement initial des paquets. L'ordre initial du traitement des paquets par IDP est le suivant :

Un paquet arrive au firewall et NetDefendOS effectue une vérification habituelle. Si le paquet fait partie de la nouvelle connexion, alors il est comparé à l'ensemble de règles IP avant d'être transféré au module IDP. Si le paquet fait partie d'une connexion existante, il est transféré directement au système IDP. Si le paquet ne fait pas partie d'une connexion existante ou qu'il est rejeté par l'ensemble de règles IP, alors il est ignoré.

Les informations sur la source et la destination du paquet sont comparées à l'ensemble de règles IDP définies par l'administrateur. Si une correspondance est trouvée, on passe à l'étape suivante du traitement IDP, c'est-à-dire le filtrage par motif, décrit ci-dessous. S'il n'existe aucune correspondance avec une règle IDP, le paquet est accepté et le système IDP n'entreprend pas d'actions supplémentaires bien que celles définies dans

l’ensemble de règles IP, telles que la traduction d’adresses ou la consignation, s’appliquent.

Vérification des paquets ignorés. Cette option existe dans l’IDP NetDefendOS pour rechercher des intrusions dans l’ensemble du trafic, même dans les paquets qui sont rejetés par l’ensemble de règles IP qui vérifie les nouvelles connexions, ainsi que les paquets qui ne font pas partie d’une connexion existante. Cela permet à l’administrateur du firewall de détecter tout trafic qui apparaît comme une intrusion. Cette option permet uniquement l’action « consigner » de la règle IDP. Vous devez faire attention lorsque vous utilisez cette option car la charge de traitement peut être plus élevée lorsque tous les paquets de données sont vérifiés.

Prévention des attaques de type insertion/évasion

Présentation. Lorsqu’il définit une règle IDP, l’administrateur a la possibilité d’activer ou de désactiver l’option Protect against Insertion/Evasion attack (Protection contre les attaques de type insertion/évasion). Les attaques de type *Insertion/Evasion Attack* visent spécifiquement les systèmes IDP. Elles exploitent le fait que, dans les transferts de données TCP/IP, le flux de données doive fréquemment être reformé à partir de paquets de données plus petits. En effet, les paquets individuels sont souvent fragmentés ou arrivent dans le désordre. Les attaques de type *Insertions* ou *Evasions* visent à exploiter ce processus de réassemblage.

Attaques de type Insertion. Une attaque de type Insertion consiste à insérer des données dans un flux de telle façon que l'ordre des paquets de données soit accepté par le sous-système IDP mais refusé par l'application cible. Au final, deux flux de données différents sont créés.

Prenons l’exemple d’un flux de données composé de 4 paquets : p1, p2, p3 et p4. Le pirate peut commencer par envoyer les paquets p1 et p4 à l’application cible. Ces paquets sont mis en attente par le sous-système IDP et par l’application jusqu’à l’arrivée des paquets p2 et p3 en vue du réassemblage. Le pirate envoie ensuite délibérément deux paquets, p2' et p3', qui sont refusés par l’application mais acceptés par le système IDP. Le système IDP est désormais en mesure de réassembler les paquets puisqu’il pense disposer du flux de données complet. Le pirate envoie alors deux paquets supplémentaires, p2 et p3, qui sont acceptés par l’application. Cette dernière procède au réassemblage et obtient un flux de données différent de celui généré par le sous-système IDP.

Attaques de type Évasion. Une attaque de type Évasion procède à l’inverse d’une attaque de type Insertion mais provoque le même résultat : deux flux de données différents sont créés, celui du sous-système IDP et celui de l’application cible. Elle consiste à envoyer des paquets de données qui sont refusés par le sous-système IDP mais acceptés par l’application cible.

Action de détection. Si une attaque de type insertion/évasion est détectée alors que l’option de protection contre ce type d’attaque est activée, NetDefendOS corrige automatiquement le flux de données en supprimant les données parasites générées par l’attaque

Événements Insertion/Évasion. Le sous-système Insertion/Evasion Attack de NetDefendOS peut générer deux types de message :

Un message Attack Detected (Attaque détectée), indiquant qu’une attaque a été identifiée et évitée.

Un message Unable to Detect (Détection impossible), indiquant que NetDefendOS n’a pas pu identifier d’attaques potentielles lors du réassemblage d’un flux de données TCP/IP bien qu’une telle attaque ait pu se produire. Cette situation est provoquée par des schémas de données anormalement complexes et peu fréquents dans le flux.

Configuration recommandée. Par défaut, la protection contre les attaques de type Insertion/Evasion est activée pour toutes les règles IDP. Ce paramétrage est recommandé pour la plupart des configurations. La désactivation de cette option peut être motivée par l’une des deux raisons suivantes :

Augmentation du débit – Lorsqu’un débit optimal est requis, la désactivation de cette option peut augmenter sensiblement la vitesse de traitement.

Nombre excessif de faux positifs – Si un niveau anormalement élevé de faux positifs Insertion/Evasion est prouvé, il peut être prudent de désactiver cette option jusqu’à ce que les raisons de ce taux soient étudiées.

Filtrage par motif IDP

Signatures. Pour que le système IDP identifie correctement une attaque, il utilise un profil d'indicateurs, ou *pattern* (motif), associé à différentes types d'attaques. Ces motifs prédéfinis, également appelés *signatures*, sont stockés dans une base de données locale de NetDefendOS et sont utilisés par le système IDP pour comparer le trafic aux schémas d'attaque. Chaque signature IDP est repérée par un numéro unique.
Considérez l'exemple suivant d'une attaque simple impliquant un échange avec un serveur FTP. Un utilisateur pirate peut tenter de récupérer le fichier mot de passe « passwd » d'un serveur FTP via la commande RETR passwd. Une signature cherchant les chaînes de texte ASCII *RETR* et *passwd* trouvera alors une correspondance indiquant une attaque éventuelle. Dans cet exemple, le motif s'apparente à du texte brut mais le filtrage par motif est effectué de la même manière sur les données purement binaires.

Reconnaissance des menaces inconnues. Les pirates qui conçoivent de nouvelles intrusions réutilisent souvent d'anciens codes. Cela signifie que leurs nouvelles attaques peuvent surgir rapidement « dans la nature ». Pour les contrer, le système IDP de D-Link emploie une approche où le module inspecte ces composants réutilisables, grâce au filtrage par motif qui recherche des unités logiques plutôt que des motifs de code entiers. Vous pouvez ainsi être protégés contre les menaces « connues » ainsi que les nouvelles menaces à peine sorties et encore « inconnues », formées avec les composants logiciels réutilisés.

Avis de signatures. Un *advisory* (avis) est une description textuelle explicative d'une signature. La lecture d'un avis de signatures explique à l'administrateur ce que la signature va rechercher. Étant donné que la base de données des signatures est en perpétuel changement, les avis ne sont pas fournis avec la documentation D-Link mais sont disponibles sur le site Web de D-Link :

http://security.dlink.com.tw

Vous pouvez trouver les avis dans les options de « NetDefend IDS » du menu « NetDefend Live ».

Types de signatures IDP. Le système IDP offre trois types de signatures qui autorisent différents niveaux de sécurité selon les menaces :

Signatures de protection des intrusions (IPS) : celles-ci sont extrêmement précises, ce qui signifie qu'une correspondance indique presque automatiquement une menace. Il est recommandé d'utiliser l'action Protection. Ces signatures peuvent détecter les actions administrateur et les analyses de sécurité.

Signatures de détection des intrusions (IDS) : celles-ci peuvent détecter des événements pouvant être des intrusions. Elles sont moins précises que les IPS et peuvent donner des faux positifs. Il est donc recommandé d'utiliser l'action Audit avant d'utiliser l'action Protection.

Signatures des règles : celles-ci détectent différents types de trafic entre les applications. Elles peuvent être utilisées pour bloquer certaines applications telles que le partage de fichiers et la messagerie instantanée.

Groupes de signatures IDP

Utilisation des groupes. Il existe généralement plusieurs lignes d'attaques pour un protocole spécifique et il vaut mieux toutes les rechercher en même temps lorsque l'on analyse le trafic réseau. Pour cela, les signatures liées à un protocole particulier sont regroupées. Par exemple, les signatures qui se rapportent au protocole FTP forment un groupe. Il vaut mieux spécifier un groupe qui fait référence au trafic inspecté plutôt que d'examiner des signatures individuelles. Pour des raisons de performances, l'objectif serait que NetDefendOS examine les données en utilisant le moins de signatures possibles.

Spécification des groupes de signatures. Les groupes de signatures IDP sont organisés en une structure hiérarchique à trois niveaux. Au niveau le plus élevé de cette hiérarchie se trouve la signature *Type* ; la catégorie (*Category*) et la sous-catégorie (*Sub-Category*) représentent respectivement les deuxième et troisième niveaux. Le groupe de signatures appelé POLICY_DB_MSSQL illustre ce principe où la règle est le *Type*, la base de données la catégorie (*Category)* et MSSQL est la *Sub-Category* (sous-catégorie). Ces 3 composants de signature sont expliqués ci-dessous :

1. Type Groupe de signatures. Le type de groupe est l'une des valeurs *IDS*, *IPS* ou *Policy* (Règle). Ces types sont expliqués ci-dessous.

2. Catégorie Groupes de signatures. Ce deuxième niveau de désignation décrit le type d'application ou de protocole. Voici des exemples :

BACKUP (sauvegarde)

DB (base de données)

DNS

FTP

HTTP

3. Sous-catégorie Groupe de signatures. Le troisième niveau de désignation indique la destination du groupe et précise souvent l'application, par exemple *MSSQL*. La sous-catégorie peut ne pas être nécessaire si le *Type* et la *Category* (catégorie) suffisent à indiquer le groupe, par exemple APP_ITUNES.

Liste des groupes IDP. Une liste des groupes IDP se trouve à l'*Annexe, Groupes de signatures IDP*. La liste indique des noms de groupes composés de la *Category* (catégorie), suivie de la *Sub-Category* (sous-catégorie) car le *Type* pourrait être l'une des valeurs IDS, IPS ou POLICY (Règle).

Traitement d'opérations multiples. Pour toute règle IDP, il est possible d'indiquer plusieurs opérations et un type d'opération, comme par exemple Protect (Protéger), peut être répété. Chaque opération aura alors une ou plusieurs signatures ou groupes associés. Lorsqu'une correspondance de signature se produit, l'opération s'effectue de haut en bas, la correspondance des signatures pour la première opération indiquée étant la première effectuée.

Wildcarding des signatures IDP. Lors de la sélection de groupes de signatures IDP, il est possible d'utiliser le wildcarding pour sélectionner plusieurs groupes. Le caractère « ? » peut être utilisé comme joker pour un seul caractère dans un nom de groupe. Le caractère « * » peut également être utilisé comme joker pour tout ensemble de caractères de n'importe quelle longueur dans un nom de groupe.

Avertissement contre l'utilisation d'un nombre excessif de signatures IDP

N'utilisez pas l'ensemble de la base de données de signatures et évitez d'utiliser des signatures et des groupes de signatures inutilement. Veillez à utiliser uniquement les signatures ou groupes qui s'appliquent au type de trafic que vous tentez de protéger. Par exemple, utiliser les groupes IDS_WEB*, IPS_WEB*, IDS_HTTP* et IPS_HTTP* IDP serait approprié pour protéger un serveur HTTP.

L'analyse du trafic IDP crée une charge supplémentaire sur le matériel qui dans la plupart des cas ne devrait pas affecter les performances de façon notable. L'utilisation d'un trop grand nombre de signatures lors de l'analyse peut rendre la charge sur le matériel du firewall inutilement lourde, affectant négativement le débit.

Actions IDP

Options d'action. Une fois que la correspondance de motif reconnaît une intrusion dans l'objet du trafic vers une règle IDP, l'action associée à cette règle est entreprise. L'administrateur peut associer l'une des trois options d'action à une règle IDP :

Ignorer – Ne rien faire si une intrusion est détectée et laisser la connexion ouverte

Vérifier – Laisser la connexion ouverte mais consigner l'événement

Protéger – Cette action ignore la connexion et consigne l'événement (avec la possibilité d'ajouter à la liste noire la source de la connexion ou l'activation de ZoneDefense tel que décrit ci-dessous).

Listes noires IDP. L'option Protect (Protéger) permet d'ajouter l'hôte ou le réseau particulier qui déclenche la règle IDP à une *Blacklist* (liste noire) de sources de trafic irrégulières. Ceci signifie que tout le trafic provenant d'une source sur liste noire sera automatiquement ignoré par NetDefendOS. Pour en savoir plus sur le fonctionnement des listes noires, consultez la section « Blacklisting des hôtes et réseaux ».

ZoneDefense IDP. L'action Protect (Protéger) permet de désactiver le commutateur D-Link particulier qui déclenche la règle IDP via la fonction *ZoneDefense* de D-Link. Pour en savoir plus sur le fonctionnement de ZoneDefense, consultez le *Chapitre 12, ZoneDefense*.

Récepteur de journaux SMTP pour les événements IDP

Afin de recevoir des notifications par e-mail des événements IDP, un récepteur de journaux SMTP peut être configuré. Cet e-mail contiendra un résumé des événements IDP qui se sont produits au cours d'une période de temps configurable par l'utilisateur.

Lorsqu'un événement IDP se produit, le NetDefendOS patientera pendant les secondes de la durée de retenue (Hold Time) avant d'envoyer l'e-mail de notification. Cependant, l'e-mail sera uniquement envoyé si le nombre d'événements produits au cours de cette période est supérieur ou égal au seuil de consignation. Lorsque cet e-mail est envoyé, NetDefendOS patientera pendant les secondes de la durée de répétition minimum avant d'envoyer un nouvel e-mail.

Exemple 6.19. Configuration d'un récepteur de journaux SMTP

Dans cet exemple, une règle IDP est configurée avec un récepteur de journaux SMTP. Une fois qu'un événement IDP se produit, la règle est déclenchée. Au moins un nouvel événement se produit au cours de la période de retenue de 120 secondes, atteignant ainsi le niveau du seuil de consignation (au moins 2 événements se sont produits). Ceci entraîne l'envoi d'un e-mail contenant un résumé des événements IDP. Plusieurs événements IDP supplémentaires peuvent se produire par la suite, mais pour éviter d'encombrer le serveur de messagerie, NetDefendOS patientera pendant 600 secondes (équivalent à 10 minutes) avant d'envoyer un nouvel e-mail. Un serveur SMTP est supposé avoir été configuré dans le carnet d'adresses avec le nom du serveur smtp.

Interface de ligne de commande
Ajout d'un récepteur de journaux SMTP :

```
gw-world:/> add LogReceiver LogReceiverSMTP smt4IDP IPAddress=smtp-server
   Receiver1=youremail@yourcompany.com
```

Règles IDP :

```
gw-world:/> cc IDPRule examplerule

gw-world:/examplerule> set IDPRuleAction 1 LogEnabled=Yes
```

Interface Web
Ajout d'un récepteur de journaux SMTP :

Sélectionnez System > Log and Event Receivers > Add > SMTP Event Receiver (Système > Récepteurs de journaux et d'événements > Ajouter > Récepteur d'événements SMTP).

Saisissez :

Name (Nom) : smtp4IDP

SMTP Server (Serveur SMTP) : smtp-server

Server Port (Port de serveur) : 25

Indiquez d'autres adresses électroniques (jusqu'à 3).

Sender (Expéditeur) : hostmaster

Subject (Objet) : Événement de journal de NetDefendOS

Minimum Repeat Delay (Délai de répétition minimum) : 600

Hold Time (Durée de retenue) : 120

Log Threshold (Seuil de consignation) : 2

Cliquez sur OK.

Règles IDP :

Sélectionnez IDP > IDP Rules (IDP > Règles IDP).

Sélectionnez une règle dans la liste, cliquez sur le bouton droit de la souris et sélectionnez Edit (Modifier).

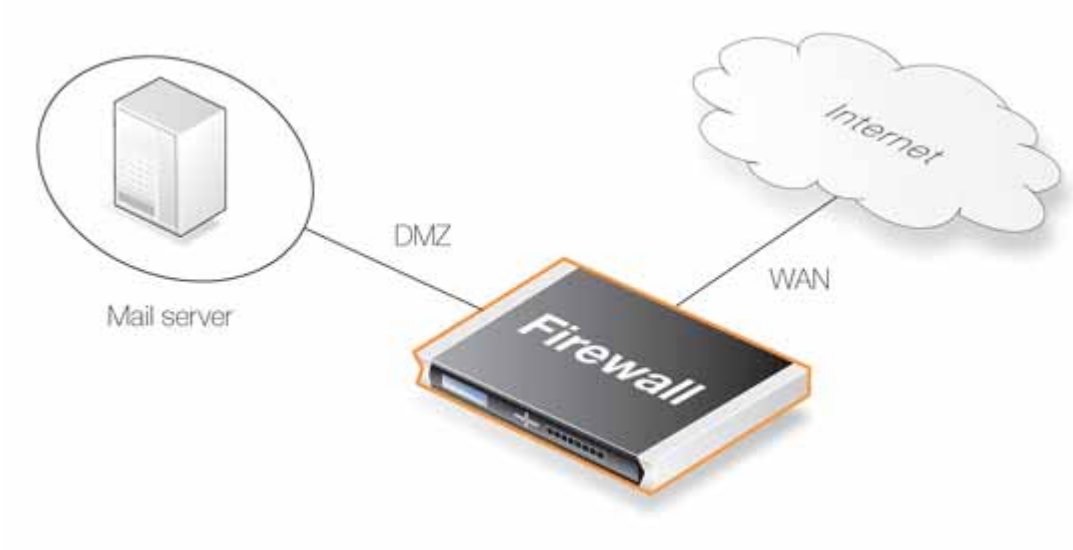
Sélectionnez l'action que vous souhaitez consigner et sélectionnez Edit (Modifier).

Cochez la case Enable logging (Activer la consignation) dans l'onglet Log Settings (Paramètres de consignation).

Cliquez sur OK.

Exemple 6.20. Configuration d'un IDP pour un serveur de messagerie

L'exemple suivant détaille les étapes nécessaires à la configuration d'un IDP pour un simple scénario dans lequel un serveur de messagerie est exposé à Internet sur le réseau DMZ avec une adresse IP publique. L'Internet public peut être atteint via le firewall sur l'interface WAN tel qu'illustré ci-dessous.



Interface de ligne de commande
Créez une règle IDP :

```
gw-world:/> add IDPRule Service=smtp SourceInterface=wan SourceNetwork=wannet
   DestinationInterface=dmz DestinationNetwork=ip_mailserver
   Name=IDPMailSrvRule
```

Créez une action IDP :

```
gw-world:/> cc IDPRule IDPMailSrvRule

gw-world:/IDPMailSrvRule> add IDPRuleAction Action=Protect
   IDPServity=All Signatures=IPS_MAIL_SMTP
```

Interface Web

Créez une règle IDP :

Cette règle IDP sera appelée IDPMailSrvRule et s'appliquera au service SMTP. L'interface source et le réseau source définissent l'origine du trafic, dans cet exemple le réseau externe. L'interface de destination et le réseau de destination définissent la destination du trafic, dans ce cas le serveur de messagerie. Le réseau de destination doit par conséquent être défini sur l'objet définissant le serveur de messagerie.

Sélectionnez Rules > IP Rules > Add > IP Rule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : IDPMailSrvRule

Service : smtp

Also inspect dropped packets (Inspecter également les paquets ignorés) : Dans le cas où l'ensemble du trafic correspondant à cette règle devrait être analysé (ceci comprend également le trafic que l'ensemble de règles principales ignorerait), la case « Also inspect dropped packets » (Inspecter également les paquets ignorés) est cochée, ce qui est le cas dans cet exemple.

Source Interface (Interface source) : wan

Source Network (Réseau source) : wannet

Destination Interface (Interface de destination) : dmz

Destination Network (Réseau de destination) : ip_mailserver

Cliquez sur OK.

Si l'on souhaite consigner des tentatives d'intrusion, ceci peut être configuré dans l'onglet Log Settings (Paramètres de consignation).

Créez une action IDP :

Lorsque cette règle IDP a été créée, une action doit également être créée, indiquant les signatures que l'IDP doit utiliser lors de l'analyse des données correspondant à la règle IDP et ce que NetDefendOS doit faire en cas de détection d'intrusion. La connexion devrait être ignorée en cas de tentatives d'intrusion, l'action est donc définie sur Protect (Protéger). La gravité est définie sur Attack (attaque), afin de correspondre à toutes les attaques SMTP. Signatures est défini sur IPS_MAIL_SMTP afin d'utiliser les signatures qui décrivent des attaques du réseau externe, concernant le protocole SMTP.

Sélectionnez Rules > IP Rules > Add > IP Rule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Action : Protect (Protéger)

Severity (Gravité) : All (Tous)

Signatures : IPS_MAIL_SMTP

Cliquez sur OK.

En bref, voici ce qui se passera : En cas de trafic entre le réseau externe et le serveur de messagerie, l'IDP sera activé. Si le trafic correspond à l'une des signatures du groupe de signatures IPS_MAIL_SMTP, la connexion sera ignorée, protégeant ainsi le serveur de messagerie.

Attaques de déni de service

Présentation

En adoptant Internet, les entreprises disposent de nouvelles opportunités commerciales et de croissance. Le réseau de l'entreprise et les applications qui y sont exécutées sont essentielles à l'activité. Non seulement une société touche un plus grand nombre de clients via Internet, mais elle peut les servir plus rapidement et de façon plus efficace. Dans le même temps, l'utilisation d'un réseau IP public permet aux entreprises de réduire les coûts liés à l'infrastructure.

Malheureusement, les mêmes avantages qu'Internet apporte à l'entreprise bénéficient également aux pirates qui utilisent la même infrastructure publique pour développer des attaques. Des outils d'attaque sont disponibles sur Internet et le travail de développement de ces outils est souvent divisé entre plusieurs groupes de pirates débutants – connus sous le nom de « script kiddies » (pirates néophytes) ou « larval hackers » (pirates débutants) - dispersés aux quatre coins du monde, permettant une évolution 24 h/24 des méthodes d'attaques automatisées. Bon nombre des nouvelles méthodes d'attaque utilisent la nature distribuée d'Internet pour lancer des attaques de déni de service contre des organisations.

Être victime d'une attaque de déni de service est probablement la dernière chose dont un administrateur réseau souhaite faire l'expérience. Les attaques peuvent apparaître sans prévenir et les conséquences peuvent être dévastatrices avec des serveurs endommagés, des connexions Internet bloquées et des systèmes essentiels à l'activité en surcharge.

Cette section aborde l'utilisation du firewall D-Link pour protéger les organisations contre les attaques de déni de service.

Mécanismes d'attaque de déni de service

Une attaque de déni de service peut être réalisée de plusieurs manières, mais il existe trois types d'attaques de base :

consommation des ressources informatiques, comme la bande passante, l'espace disque ou le temps de processeur ;

interruption des informations de configuration, comme les informations d'acheminement ;

interruption des composants réseau physiques.

L'une des méthodes les plus couramment utilisées est la consommation des ressources informatiques, ce qui signifie que l'attaque de déni de service inonde le réseau et bloque des ressources essentielles utilisées pour exécuter des applications importantes. Dans certains cas, des vulnérabilités dans les systèmes d'exploitation Unix et Windows sont exploitées pour provoquer volontairement un crash du système, alors que dans d'autres cas, un volume important de trafic apparemment valide est dirigé vers des sites jusqu'à ce que ceux-ci soient surchargés et fassent l'objet d'un crash.

Voici quelques-unes des attaques de déni de service les plus couramment utilisées :

Les attaques Ping of Death / Jolt

Les attaques de chevauchement de fragmentation : Teardrop / Bonk / Boink / Nestea

Les attaques Land et LaTierra

L'attaque WinNuke

Les attaques d'amplification : Smurf, Papasmurf, Fraggle

L'attaque d'inondation TCP SYN

L'attaque Jolt2

Les attaques *Ping of Death* et *Jolt*

L'attaque « ping of death » est l'une des attaques les plus anciennes de couche 3/4. Une des façons les plus simples de l'exécuter est d'exécuter « ping -l 65510 1.2.3.4 » sur un système Windows 95 où 1.2.3.4 est l'adresse IP de la victime ciblée. L'attaque « Jolt » est simplement un programme volontairement paramétré pour générer des paquets sur des systèmes d'exploitation dont les commandes ping refusent de générer des paquets trop volumineux.

Le facteur de déclenchement est le dernier fragment qui fait dépasser les 65 535 octets de volume de paquet, ce qui est le nombre le plus élevé qu'un entier à 16 bits peut stocker. Lorsque la valeur déborde, elle repasse à un nombre très faible. La suite dépend alors de la façon dont la pile d'IP de la victime est mise en œuvre.

NetDefendOS n'autorisera jamais la transmission de fragments qui entraîneraient un dépassement de volume total de 65 535 octets. De plus, il existe des limites configurables pour les tailles des paquets IP dans la section « Paramètres avancés ».

L'attaque Ping of death apparaîtra dans les journaux NetDefendOS comme ignorances avec le nom de règle défini sur « LogOversizedPackets ». L'adresse IP de l'expéditeur peut être usurpée.

Les attaques de chevauchement de fragmentation : *Teardrop, Bonk, Boink et Nestea*

Teardrop et les attaques dérivées sont des attaques de chevauchement de fragments. De nombreuses piles d'IP ont montré un comportement erratique (épuisement des ressources excessives ou crash) lorsqu'elles ont été exposées à des fragments en chevauchement.

NetDefendOS offre une protection totale contre les attaques de chevauchement de fragmentation. Les fragments en chevauchement ne sont jamais autorisés à transiter par le système.

L'attaque Teardrop et ses dérivées apparaîtront dans les journaux NetDefendOS comme ignorances avec le nom de règle défini sur « IllegalFrags ». L'adresse IP de l'expéditeur peut être usurpée.

Les attaques *Land* et *LaTierra*

Les attaques Land et LaTierra fonctionnent par l'envoi d'un paquet à une victime et le fait que la victime y réponde, ce qui à son tour génère une autre réponse, etc. Ceci provoquera une panne ou un crash de la machine de la victime.

L'attaque est accomplie par l'utilisation de l'adresse IP de la victime dans le champ source d'un paquet IP ainsi que dans le champ de destination.

NetDefendOS protège contre cette attaque en appliquant une protection contre l'usurpation d'IP à tous les paquets. Dans sa configuration par défaut, il comparera simplement les paquets arrivant au contenu de la table de routage ; si un paquet arrive sur une interface différente de l'interface sur laquelle le système prévoit la présence de la source, le paquet sera ignoré.

Les attaques Land et LaTierra apparaîtront dans les journaux NetDefendOS comme ignorances avec le nom de règle défini sur « AutoAccess » par défaut, ou, si vous avez écrit des règles d'accès personnalisées, le nom de la règle d'accès qui a ignoré le paquet. L'adresse IP de l'expéditeur est sans intérêt ici car c'est toujours la même que l'adresse IP de destination.

L'attaque *WinNuke*

L'attaque WinNuke fonctionne par une connexion à un service TCP qui ne dispose d'aucun gestionnaire de données « hors bande » (segments TCP avec l'ensemble de bits URG), mais qui accepte tout de même ces données. Ceci mettra en général le service dans une boucle serrée qui consommera tout le temps de processeur disponible.

Ce service était NetBIOS sur le service TCP/IP sur les machines Windows, ce qui a donné son nom à l'attaque.

NetDefendOS protège contre cette attaque de deux façons :

Avec une règle d'entrée attentive, la surface de l'attaque est considérablement réduite. Seuls les services exposés peuvent potentiellement être victimes de l'attaque et les services publics ont tendance à être mieux écrits que les services qui doivent uniquement servir le réseau local.

En éliminant le bit URG par défaut de tous les segments TCP qui traversent le système, ce qui peut être configuré via Advanced Settings > TCP > TCPUrg (Paramètres avancés > TCP > TCPUrg).

Les attaques WinNuke apparaîtront en général dans les journaux NetDefendOS comme ignorances normales avec le nom de votre règle qui a interdit la tentative de connexion. Pour les connexions autorisées via le système, les entrées de catégorie « TCP » ou « DROP » (selon le paramètre TCPUrg) apparaîtront, avec un nom de règle de « TCPUrg ». L'adresse IP de l'expéditeur n'est pas susceptible d'être usurpée ; une liaison complète à trois voies doit être effectuée avant de pouvoir envoyer des segments hors bande.

Les attaques d'amplification : *Smurf, Papasmurf, Fraggle*

Cette catégorie d'attaques utilise des « amplificateurs » : des réseaux mal configurés qui amplifient un flux de paquets et l'envoient à la cible ultime. L'objectif est la consommation excessive de bande passante - consommer toute la capacité de connexion Internet de la victime. Un pirate avec suffisamment de bande passante peut

délaisser la totalité de l'étape d'amplification et simplement diffuser suffisamment de bande passante à la victime. Cependant, ces attaques permettent aux pirates qui disposent de moins de bande passante que la victime d'amplifier leur flux de données pour submerger la victime.

Les attaques « Smurf » et « Papasmurf » envoient des paquets d'écho ICMP à l'adresse de diffusion de réseaux ouverts sur de nombreuses machines, en faisant passer l'adresse IP source pour celle de la victime. Toutes les machines présentes sur le réseau ouvert « répondent » alors à la victime.

L'attaque « Fraggle » utilise la même idée générale, mais utilise à la place l'écho UDP (port 7) pour accomplir la tâche. L'attaque Fraggle obtient en général des facteurs d'amplification plus faibles car il y a moins d'hôtes sur Internet qui ont activé le service d'écho UDP.

Les attaques Smurf apparaîtront dans les journaux NetDefendOS comme des masses de paquets ICMP Echo Reply ignorés. Les adresses IP source seront celles que les réseaux de l'amplificateur ont utilisées. Les attaques Fraggle apparaîtront dans les journaux NetDefendOS comme masses de paquets ignorés (ou autorisés, selon la règle). Les adresses IP source seront celles que les réseaux de l'amplificateur ont utilisées.

Éviter le phénomène d'amplification. Même si l'importance du flux de la bande passante est du côté de la victime, le fait d'être sélectionné comme réseau amplificateur peut également consommer d'importantes ressources. Dans sa configuration par défaut, NetDefendOS ignore explicitement les paquets envoyés à l'adresse de diffusion des réseaux connectés directement. Ceci peut être configuré via Advanced Settings > IP > DirectedBroadcasts (Paramètres avancés > IP > DirectedBroadcasts). Cependant, avec une règle d'entrée raisonnable, aucun réseau protégé ne devrait s'inquiéter de devenir amplificateur smurf.

Protection du côté de la victime. Les attaques Smurf et ses dérivées sont des attaques d'épuisement des ressources en ceci qu'elles utilisent toute la capacité de connexion à Internet. En général, le firewall se trouve du « mauvais » côté du goulot d'étranglement de la connexion Internet pour fournir une protection efficace contre ce type d'attaques. Le mal est déjà fait avant que les paquets atteignent le firewall.

Cependant, NetDefendOS peut être utile en permettant de maintenir la charge en dehors des serveurs internes, en les rendant disponibles pour le service interne, ou peut-être un service via une connexion secondaire à Internet non ciblée par l'attaque.

Les inondations Smurf et Papasmurf seront considérées comme des Réponses à l'écho ICMP du côté de la victime. À moins d'utiliser des règles « FwdFast », ces paquets ne sont jamais autorisés à lancer de nouvelles connexions, que des règles autorisent ou non le trafic.

Des paquets Fraggle peuvent arriver sur n'importe quel port de destination UDP ciblé par le pirate. Il peut être utile de renforcer l'ensemble de règles d'entrée.

La fonction de mise en forme du trafic intégrée à NetDefendOS aide également à absorber une partie de l'inondation avant qu'elle n'atteigne des serveurs protégés.

Les attaques d'inondation TCP SYN

L'attaque d'inondation TCP SYN fonctionne en envoyant de grandes quantités de paquets TCP SYN vers un port donné, puis en ne répondant pas aux SYN ACK envoyés en réponse. Ceci bloquera les ressources de piles TCP locales sur la machine de la victime jusqu'à ce qu'elle soit incapable de répondre à davantage de paquets SYN jusqu'à l'expiration des connexions à demi ouvertes existantes.

NetDefendOS protègera contre les attaques d'inondation TCP SYN s'il est activé dans un objet Service associé à la règle dans l'ensemble de règles IP qui autorise le trafic. Par défaut, c'est le cas des services prédéfinis http-in, https-in, smtp-in et ssh-in. Si un nouvel objet Service personnalisé est défini par l'administrateur, la protection Syn Flood peut alors être activée ou désactivée comme on le souhaite.

La protection « SynRelay » fonctionne en établissant une liaison à 3 voies avec le client avant d'établir une deuxième liaison avec le service cible. Les situations de surcharge ne se produisent pas aussi facilement dans NetDefendOS en raison d'une gestion des ressources bien meilleure et d'un manque de restrictions normalement placé sur un système d'exploitation complet. Alors qu'un système d'exploitation normal peut présenter des problèmes avec 5 connexions à demi ouvertes seulement, NetDefendOS peut remplir la totalité de sa table d'état (des milliers ou des millions de connexions, selon le modèle de votre produit) avant qu'un élément inhabituel apparaisse. Lorsque la table d'état se remplit, d'anciennes connexions SYN seront parmi les premières à être

ignorées pour faire de la place à de nouvelles connexions.

Les attaques d'inondation TCP SYN apparaîtront dans les journaux NetDefendOS comme des quantités excessives de nouvelles connexions (ou d'ignorances, si l'attaque vise un port fermé). L'adresse IP de l'expéditeur est presque toujours usurpée.

À noter : si la protection Syn Flood est activée sur un objet Service et qu'un ALG est associé à cet objet Service, l'ALG sera alors désactivée.

L'attaque *Jolt2*

L'attaque Jolt2 fonctionne en envoyant un flux stable de fragments identiques à la machine de la victime. Quelques centaines de paquets par seconde bloqueront complètement les machines vulnérables jusqu'à la fin du flux.

NetDefendOS offre une protection complète contre cette attaque. Le premier fragment sera mis en file d'attente en attendant l'arrivée de fragments précédents, de façon à pouvoir être transmis en ordre. Mais ceci n'arrive jamais, ce qui signifie que même le premier fragment ne passe pas. Les fragments suivants seront éliminés car ils sont identiques au premier fragment.

Si le pirate sélectionne une compensation de fragment supérieure aux limites imposées par Advanced Settings > LengthLim (Paramètres avancés > LengthLim) dans NetDefendOS, les paquets n'iront même pas jusque là ; ils seront immédiatement ignorés. Les attaques Jolt2 peuvent apparaître dans les journaux NetDefendOS ou pas. Si le pirate sélectionne une compensation de fragment trop élevée pour l'attaque, ces attaques apparaîtront comme ignorances de la part des règles définies à « LogOversizedPackets ». Si la compensation de fragment est assez faible, il n'y aura aucune consignation. L'adresse IP de l'expéditeur peut être usurpée.

Les attaques de déni de service distribué

Une forme plus sophistiquée de déni de service est l'attaque de déni de service distribué. Les attaques de déni de service distribué impliquent de diviser en centaines ou milliers des machines présentes sur Internet pour y installer le logiciel de déni de service distribué, permettant au pirate de contrôler toutes ces machines pour lancer des attaques coordonnées sur les sites victimes. Ces attaques épuisent en général la bande passante, la capacité de traitement du routeur ou les ressources de piles du réseau, en interrompant la connectivité réseau vers les victimes.

Bien que de récentes attaques de déni de service distribué aient été lancées à partir de systèmes institutionnels publics et d'entreprises privées, les pirates ont tendance à favoriser les réseaux universitaires en raison de leur nature ouverte et distribuée. Les outils utilisés pour lancer des attaques de déni de service distribué comprennent notamment : Trin00, TribeFlood Network (TFN), TFN2K et Stacheldraht.

Blacklisting des hôtes et réseaux

NetDefendOS met en place une *Blacklist* (liste noire) d'adresses IP d'hôtes ou de réseaux qui peut être utilisée pour protéger contre tout trafic provenant de sources Internet spécifiques.

Certains modules de NetDefendOS, en particulier le module Intrusion Detection and Prevention (IDP) (Détection et prévention des intrusions), ainsi que des règles de seuil, peuvent utiliser la liste noire dans certaines situations, comme par exemple lorsque le trafic déclenche une règle de limite de seuil.

L'ajout d'un hôte ou d'un réseau à la liste noire peut être activé dans IDP et dans les règles de seuil en indiquant l'action Protect (Protéger) en cas de déclenchement d'une règle. Une fois activé, il existe trois options de blacklisting :

Time to Block Host/Network in seconds (Durée de blocage d'un hôte/réseau en secondes)
: L'hôte ou le réseau qui est la source du trafic sera maintenu sur la liste noire pendant la durée indiquée, avant d'être supprimé. Si la même source déclenche une autre entrée dans la liste noire, la durée de blocage est alors ramenée à sa valeur complète d'origine (en d'autres termes, elle ne peut pas se cumuler).

Block only this Service (Bloquer uniquement ce service)
: Par défaut, le blacklisting bloque tous les services pour l'hôte de déclenchement.

Exempt already established connections from Blacklisting (Exclure du blacklisting les connexions déjà établies)
: Si des connexions établies ont la même source que cette nouvelle entrée de la liste noire, elles ne seront pas ignorées si cette option est sélectionnée.

Des adresses IP ou réseaux sont ajoutés à la liste et le trafic en provenance de ces sources est bloqué pendant un certain temps. La liste noire est maintenue, même si le firewall D-Link s'arrête ou redémarre.
Liste blanche. Pour s'assurer que de « bonnes » sources de trafic Internet ne sont en aucun cas mises sur liste noire, une *Whitelist* (liste blanche) est également tenue par NetDefendOS.

Conseil

Il est recommandé d'ajouter le firewall D-Link lui-même à la liste blanche ainsi que les adresses IP du poste de travail de gestion.

Il est important de bien comprendre que bien que la liste blanche évite la mise sur liste noire d'une source de trafic réseau, ceci n'empêche pas les mécanismes tels que les règles de seuil d'ignorer ou de refuser des connexions à partir de cette source. Tout l'intérêt de la liste blanche est d'empêcher l'ajout d'une source à une liste noire s'il s'agit de l'action qu'une règle a indiquée.

Pour plus d'informations, consultez les sections intitulées « Actions IDP », « Blacklisting de règles de seuil » et la section intitulée « Règles de seuil ».

Remarque

Le blacklisting du filtrage de contenu est un objet distinct qui utilise une liste logique distincte (consultez la section intitulée « Filtrage du contenu Web »).

Chapitre 7. Traduction d’adresses

Le présent chapitre décrit les fonctionnalités NetDefendOS de traduction d’adresses.

La capacité de NetDefendOS à modifier les adresses IP des paquets lors de leur passage dans un firewall D-Link est connue sous le nom de *traduction d'adresses*. NetDefendOS prend en charge deux types de traduction : le NAT (*Network Address Translation* ou Traduction d’adresses réseau) dynamique et le SAT (*Static Address Translation* ou Traduction d’adresses statique). Les deux types de traduction sont basées sur des règles, ce qui signifie qu’ils peuvent être appliqués à un trafic spécifique en fonction du réseau source/de destination, de l’interface source/de destination ainsi que du service. Deux types de règles IP (*règles NAT* et *règles SAT*) sont utilisée pour spécifier la traduction d’adresses au sein de l’ensemble de règles IP.

L'utilisation de la traduction d’adresses a deux principaux fondements :

Fonctionnalité. Vous utilisez peut-être des adresses IP privées sur votre réseau et vos hôtes protégés pour accéder à Internet. Dans ce cas, la traduction d’adresses dynamique peut être utilisée. Vous pouvez également utiliser des serveurs avec des adresses IP privées qui doivent être accessibles au public. Dans ce cas, la traduction d’adresses statique peut être la solution.

Sécurité. En elle-même, la traduction d’adresses ne fournit pas un niveau plus important de sécurité, mais elle rend difficile pour les intrus de comprendre la structure exacte du réseau protégé que certaines machines voudraient attaquer. Dans le pire des scénarios, l'utilisation de la traduction d'adresses impliquerait que les attaques prendraient plus de temps, ce qui les rendrait aussi plus visibles dans les fichiers de consignation de NetDefendOS. Dans le meilleur des scénarios, l’intrus renoncera simplement.

Cette section décrit le fonctionnement des traductions d’adresses dynamique et statique, leurs fonctionnalités et leurs limites. Des exemples sont également fournis pour vous aider à configurer les règles NAT et SAT.

NAT dynamique

La *NAT dynamique* propose un mécanisme de traduction des adresses IP de la source d’origine vers des adresses différentes. La NAT est plus fréquemment adoptée lorsqu’on utilise des adresses IP privées dans un réseau interne et qu'il est souhaitable que les connexions sortantes apparaissent comme provenant du firewall D-Link lui-même plutôt que des adresses internes.

La NAT est un mode de traduction plusieurs-un, ce qui signifie que chaque règle NAT traduira plusieurs adresses IP source en une seule. Pour maintenir les informations d’état de session, chaque connexion en provenance des adresses traduites de manière dynamique doit utiliser la même combinaison numéro de port/adresse IP que son émetteur. NetDefendOS traduira donc automatiquement le numéro de port source. Le port source est le prochain port libre, habituellement au-dessus de 32 768. Ceci implique l’existence d’une limitation d’environ 30 000 connexions simultanées qui utilisent la même adresse IP source traduite.

NetDefendOS prend en charge deux stratégies de traduction des adresses source :

Use Interface Address (Utiliser l’adresse de l’interface) Lorsqu’une nouvelle connexion est établie, la consultation de la table de routage permet de trouver l'interface de sortie de cette connexion. L’adresse IP de cette interface est alors utilisée en tant que nouvelle adresse IP source lors de la traduction d'adresses par NetDefendOS.

Specify Sender Address (Spécifier l’adresse de l’émetteur) Une adresse IP spécifique peut être déterminée comme nouvelle adresse IP source. L’adresse IP spécifiée doit nécessairement avoir une entrée correspondante ARP Publish configurée pour l’interface de sortie. Sans cela, le firewall D-Link ne pourra pas recevoir le trafic retour.

L’exemple suivant illustre la manière dont la NAT est appliquée sur une nouvelle connexion.

L’émetteur (par exemple 192.168.1.5) envoie un paquet depuis un port assigné en dynamique (par exemple le port 1038) vers un serveur (par exemple 195.55.66.77 port 80).

192.168.1.5:1038 => **195.55.66.77:80**

Dans cet exemple, l’option Use Interface Address (Utiliser l’adresse de l’interface) est activée. Elle utilise l’adresse d’interface 195.11.22.33. De plus, le port source est changé pour un port libre sur le firewall D-Link (il se situe habituellement au-dessus de 32 768). Dans cet exemple, nous allons utiliser le port 32 789. Le paquet est donc envoyé vers sa destination.

195.11.22.33:32789 => **195.55.66.77:80**

Le serveur destinataire traite le paquet et envoie sa réponse.

195.55.66.77:80 => **195.11.22.33:32789**

NetDefendOS reçoit le paquet et le compare à sa liste de connexions ouvertes. Une fois la connexion trouvée, il restaure l’adresse d’origine et transfère le paquet.

195.55.66.77:80 => **192.168.1.5:1038**

L'émetteur d’origine reçoit la réponse.

Exemple 7.1. Ajout d’une règle NAT

Pour ajouter une règle NAT qui fera une traduction d’adresses pour tout trafic HTTP provenant du réseau interne, suivez les étapes ci-dessous :

Interface de ligne de commande

```
gw-world:/> add IPRule Action=NAT Service=http SourceInterface=lan
   SourceNetwork=lannet DestinationInterface=any
   DestinationNetwork=all-nets Name=NAT_HTTP NATAction=UseInterfaceAddress
```

Interface Web

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Spécifiez un nom convenable pour la règle, par exemple : *NAT_HTTP*.

Saisissez :

Action : NAT

Service : http

Source Interface (Interface source) : lan

Source Network (Réseau source) : lannet

Destination Interface (Interface de destination) : any (toutes)

Destination Network (Réseau de destination) : all-nets (tout réseau)

Sous l’onglet NAT, assurez-vous que l'option Use Interface Address (Utiliser l’adresse de l'interface) est sélectionnée.

Cliquez sur OK.

Protocoles pris en charge par la NAT. La traduction d’adresses dynamique est compatible avec les protocoles TCP, UDP et ICMP et ce avec un haut niveau de fonctionnalité puisque l'algorithme sait quelles valeurs peuvent être ajustées pour devenir uniques dans ces trois protocoles. Pour d’autres protocoles de niveau IP, les connexions uniques sont identifiées par leurs adresses d’émetteur, leurs adresses de destination et leurs numéros de protocole.

En d’autres termes :

Une machine interne peut communiquer avec plusieurs serveurs externes en utilisant le même protocole IP.

Une machine interne peut communiquer avec plusieurs serveurs externes en utilisant différents protocoles IP.

Plusieurs machines internes peuvent communiquer avec des serveurs externes différents en utilisant le même protocole IP.

Plusieurs machines internes peuvent communiquer avec le même serveur externe en utilisant différents protocoles IP.

Plusieurs machines internes *ne* peuvent *pas* communiquer avec le même serveur externe en utilisant le même protocole IP.

Remarque

Ces restrictions s’appliquent uniquement aux protocoles de niveau IP autres que TCP, UDP et ICMP, c’est-à-dire les protocoles tels que OSPF, L2TP, etc. Elles ne s’appliquent pas aux « protocoles » transportés par TCP, UDP et ICMP, c’est-à-dire : telnet, FTP, HTTP, SMTP, etc. NetDefendOS peut altérer le numéro de port dans les en-têtes TCP et UDP pour rendre chaque connexion unique, même si les adresses des émetteurs de ces connexions ont été traduites par la même adresse IP.

Certains protocoles ne s’intéressent pas au mode de transport utilisé, ce qui peut causer des problèmes lors de la traduction d'adresses.

Groupes NAT

Présentation. Comme spécifié dans la section intitulée « NAT dynamique », la NAT fait en sorte que plusieurs clients et hôtes internes avec des adresses IP internes privées et uniques puissent communiquer avec des hôtes distants grâce à une seule adresse IP publique externe. Lorsque plusieurs adresses IP externes publiques sont disponibles, alors un objet *Groupe NAT* peut être utilisé pour attribuer des nouvelles connexions à ces adresses IP publiques.

Les groupes NAT sont habituellement utilisés lorsqu’un grand nombre de connexions de port uniques sont nécessaires. Le gestionnaire de ports de NetDefendOS est limité à 65 000 connexions pour la combinaison unique des adresses IP source et de destination. Lorsqu'un grand nombre de clients internes utilisent des applications telles que des logiciels de partage de fichiers, un très grand nombre de ports peuvent être requis pour chaque client. Cette situation peut être aussi difficile si un grand nombre de clients accèdent à Internet par l’intermédiaire d’un serveur proxy. Le problème de la limitation du nombre de ports est résolu en attribuant des adresses IP externes supplémentaires aux accès Internet et en utilisant des groupes NAT pour leur attribuer de nouvelles connexions.

Types de groupes NAT. Un groupe NAT peut être d’un de ces trois types, chaque type attribuant les nouvelles connexions d’une manière différente :

Stateful (Pourvu d’état)

Stateless (Dépourvu d’état)

Fixed (Fixé)

Ces trois types sont présentés ci-dessous.
Groupe NAT en Stateful (Pourvu d'état). Quand l’option *Stateful* (Pourvu d’état) est sélectionnée, NetDefendOS attribue une nouvelle connexion à l’adresse IP externe qui présente à ce moment le moins de connexions routées et qui est donc présumée être la moins chargée. NetDefendOS conserve en mémoire une trace de toutes ces connexions. Les connexions suivantes avec le même client/hôte interne utilisent alors la même adresse IP externe.

L’avantage de cette approche est qu’elle peut équilibrer les connexions entre plusieurs liens ISP externes tout en assurant la communication d'un hôte externe avec la même adresse IP. Ceci est essentiel avec des protocoles tels que le HTTP lorsqu’il y a des cookies. Les inconvénients sont la mémoire supplémentaire requise par NetDefendOS pour les enregistrements dans sa table d’état et la petite surcharge d’activité qu’implique le traitement d’une nouvelle connexion.

Pour s’assurer que la table d’état ne contient pas d’entrées caduques pour les communications qui ne sont plus actives, une durée State Keepalive (Entretien de l’état) peut être spécifiée. Cette durée représente le nombre de

secondes d'inactivité possible avant qu'un état ne soit effacé de la table d'état. Après cette période, NetDefendOS suppose que plus aucune communication ne proviendra de l’hôte interne en question. Une fois que l’état est effacé, la communication suivante du même hôte entraînera la création d'une nouvelle entrée dans la table d'état. Une adresse IP externe différente peut lui être attribuée par le groupe NAT.

La table d’état elle-même utilise de la mémoire et il est possible de limiter sa taille grâce à la valeur *Max States* dans un objet groupe NAT. La table d’état n’est pas attribuée entièrement en une fois, mais sa taille peut être augmentée à volonté. Une entrée dans la table d'état suit toutes les connexions d'un seul hôte derrière le firewall D-Link, quel que soit l’hôte externe. Si le *Max States* est atteint, alors l’état existant avec le plus long temps d'inactivité est écrasé. Si tous les états de la table sont actifs, alors la nouvelle connexion est abandonnée. En règle générale, la valeur *Max States* doit correspondre au moins au nombre d'hôtes ou de clients locaux qui vont se connecter sur Internet.

Il n’y a qu’une seule table d’état par groupe NAT. Si un seul groupe NAT est réutilisé dans des règles IP NAT multiples, elles partagent alors la même table d’état.

Pools NAT en Stateless (Dépourvu d’état). L’option *Stateless* (dépourvu d’état) signifie qu’aucune table d’état n’est créée et que l’adresse IP externe choisie pour chaque nouvelle connexion est celle qui est pourvue du plus petit nombre de connexions. Ceci signifie que deux connexions entre un hôte interne et un même hôte externe peuvent utiliser deux adresses IP externes différentes.

Un groupe NAT dépourvu d'état a l’avantage d’offrir une bonne répartition des nouvelles connexions entre les adresses IP externes, de requérir moins de mémoire puisqu'elle n'est plus allouée à une table d'état et de limiter le temps passé à paramétrer la nouvelle connexion. L'inconvénient est qu’il n’est pas adapté aux communications qui nécessitent une adresse IP externe constante.

Pools NAT en Fixed (Fixé). L’option *Fixed* (Fixé) implique qu'un algorithme de chiffrage attribue à chaque client ou hôte interne une des adresses IP externes. Bien que l’administrateur n’ait pas le contrôle sur la répartition des connexions externes, ce schéma assure la communication d’un client ou hôte interne particulier avec une adresse IP externe fixe.

L’option Fixed (Fixé) a l’avantage de ne requérir aucune mémoire pour une table d’état et d'établir très rapidement une nouvelle connexion. Bien que l’équilibrage de la charge ne soit pas assuré par cette option, la charge se répartit sur les connexions externes grâce à la nature aléatoire de l’algorithme d’attribution.

Utilisation du groupe IP. Lors de l’attribution des adresses IP externes à un groupe NAT, il n’est pas nécessaire de leur donner un état. Au lieu de quoi, un objet *IP Pool* de NetDefendOS peut être sélectionné. Les pools IP accumulent des adresses IP directement grâce au DHCP et peuvent donc automatiquement fournir des adresses IP externes à un groupe NAT. Pour plus de détails, veuillez consulter la section intitulée « Groupes IP ».

Utilisation du proxy ARP. Lorsqu’un routeur externe envoie des requêtes ARP à un firewall D-Link pour résoudre les adresses IP d’un groupe NAT, NetDefendOS devra envoyer les bonnes réponses ARP afin que la résolution d'adresse s'effectue grâce à son mécanisme de proxy ARP et que le routeur externe puisse construire correctement sa table de routage.

Par défaut, l’administrateur doit spécifier dans les paramètres du groupe NAT quelles interfaces doivent être utilisées avec ce groupe. Cependant, une option permet d’activer un proxy ARP pour un groupe NAT sur toutes les interfaces, mais ceci peut parfois causer des problèmes du fait de la possible création de routes vers des interfaces sur lesquelles des paquets ne devraient pas arriver. Il est toutefois recommandé que les interfaces à utiliser avec le mécanisme de groupe NAT avec un proxy ARP soient explicitement désignées.

Utilisation de pools NAT. Les pools NAT sont utilisés avec une règle IP NAT normale. Lors de la définition d’une règle NAT, la boîte de dialogue inclut une option qui permet de lui attribuer un groupe NAT. Cette association permet au groupe NAT de fonctionner.

Exemple 7.2. Utilisation de pools NAT

Dans cet exemple, nous allons créer un groupe NAT qui s’appliquera sur la plage d’adresses IP 10.6.13.10 à 10.16.13.15 ; puis nous allons l’utiliser dans une règle IP NAT pour le trafic HTTP sur l’interface Wan.

Interface Web

A. Créez d’abord un objet dédié à la plage d'adresses dans le carnet d'adresses.

Sélectionnez Objects > Address Book > Add > IP address (Objets > Carnet d’adresses > Ajouter > Adresse IP).

Saisissez un nom convenable pour la plage IP : *nat_pool_range*.

Entrez *10.6.13.10-10.16.13.15* dans la boîte de texte Address (Adresse).
(Ici, un réseau tel que 10.6.13.0/24 peut être utilisé, les adresses 0 et 255 seront automatiquement effacées)

Cliquez sur OK.

B. Ensuite, créez un objet groupe NAT en Stateful (pourvu d’état) nommé *stateful_natpool* :

Sélectionnez Objects > NAT Pools > Add > NAT Pool (Objets > Groupe NAT > Ajouter > Groupe NAT).

Saisissez :

Name (Nom) : stateful_natpool

Pool type (Type du groupe) : stateful

IP Range (Plage d’IP) : nat_pool_range

Sélectionnez l’onglet proxy ARP et ajoutez l’interface WAN.

Cliquez sur OK.

C. Définissez la règle NAT dans l’ensemble de règles IP.

Allez dans Rules > IP Rules > Add > IP Rule (Règles > Règles IP > Ajouter > Règle IP).

Sous General (Général), entrez :

Name (Nom) : saisissez un nom adapté

Action : NAT

Sous Address Filter (Filtre d’adresses), entrez :

Source Interface (Interface source) : int

Source Network (Réseau source) : int-net

Destination Interface (Interface de destination) : wan

Destination Network (Réseau de destination) : all-nets (tout réseau)

Service : HTTP

Sélectionnez l’onglet Address Translation (Traduction d’adresses) et entrez :

Cochez l’option Use NAT Pool (Utiliser le groupe NAT).

Sélectionnez stateful_natpool dans la liste déroulante.

Cliquez sur OK.

Traduction d’adresses statique

NetDefendOS peut traduire des plages entières d’adresses IP et/ou de ports. Ces traductions sont des transpositions, c’est-à-dire que chaque adresse est mappée sur une adresse ou un port correspondant dans la nouvelle plage, plutôt que de les traduire toutes vers la même adresse ou le même port. Cette fonctionnalité est connue sous le nom de SAT (*Static Address Translation* ou Traduction d’adresses statique).

Contrairement à la NAT, la SAT requière plus d'une règle SAT pour fonctionner. NetDefendOS n’achève pas la recherche dans l'ensemble de règles après qu'une règle SAT correspondante ait été trouvée. À la place, la recherche continue jusqu’à trouver une règle Allow, NAT ou FwdFast qui correspond. C’est seulement après avoir trouvé une de ces règles que NetDefendOS exécute la règle SAT.

Traduction d’une adresse IP unique (1:1)

La forme la plus simple de l’utilisation de la SAT est pour la traduction d'une adresse IP unique. Un des scénarios les plus communs consiste à permette aux utilisateurs externes d'accéder à un serveur protégé dont l'adresse est privée. Ce scénario est quelques fois appelé *Virtual IP* (IP virtuelle) ou *Virtual Server* (Serveur virtuel) chez d'autres fabricants.

Exemple 7.3. Autorisation du trafic vers un serveur Web protégé par une DMZ

Dans cet exemple, nous allons créer une règle SAT qui traduira et autorisera les connexions provenant d'Internet vers un serveur Web situé dans une DMZ. Le firewall D-Link est connecté à Internet en utilisant une interface wan dont l'adresse IP est l'adresse de l'objet wan_ip (défini par 195.55.66.77). L’adresse IP du serveur Web est 10.10.10.5 et peut être atteint grâce à l'interface dmz.

Interface de ligne de commande
D’abord, créez une règle SAT.

```
gw-world:/> add IPRule Action=SAT Service=http SourceInterface=any
   SourceNetwork=all-nets DestinationInterface=core
   DestinationNetwork=wan_ip SATTranslate=DestinationIP
   SATTranslateToIP=10.10.10.5 Name=SAT_HTTP_To_DMZ
```

Puis créez une règle Allow correspondante.

```
gw-world:/> add IPRule action=Allow Service=http SourceInterface=any
   SourceNetwork=all-nets DestinationInterface=core
   DestinationNetwork=wan_ip Name=Allow_HTTP_To_DMZ
```

Interface Web

D’abord, créez une règle SAT.

Sélectionnez Rules > IP Rules > Add > IPRule

Spécifiez un nom convenable pour la règle, par exemple : *SAT_HTTP_To_DMZ*.

Saisissez :

Action : SAT

Service : http

Source Interface (Interface source) : any (toutes)

Source Network (Réseau source) : all-nets (tout réseau)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : wan_ip

Sous l’onglet NAT, assurez-vous que l'option Destination IP Address (Adresse IP de destination) est sélectionnée.

Dans la boîte de texte New IP Address (Nouvelle adresse IP), saisissez 10.10.10.5.

Cliquez sur OK.

Puis créez une règle Allow correspondante.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Spécifiez un nom convenable pour la règle, par exemple : *Allow_HTTP_To_DMZ*.

Saisissez :

Action : Allow (Autoriser)

Service : http

Source Interface (Interface source) : any (toutes)

Source Network (Réseau source) : all-nets (tout réseau)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : wan_ip

Sous l’onglet Service, sélectionnez http dans la Pre-defined list (Liste prédéfinie).

Cliquez sur OK.

Cet exemple correspond aux deux règles suivantes dans l'ensemble de règles :

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST 10.10.10.5 80
2	Allow (Autoriser)	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http

Ces deux règles nous permettent d’accéder au serveur Web via l'adresse IP externe du firewall D-Link. La règle 1 énonce que la traduction d’adresses peut être effectuée si la connexion a été autorisée et la règle 2 autorise la connexion.

Bien entendu, nous avons aussi besoin d’une règle qui autorise les machines internes à avoir une traduction d’adresses dynamique pour accéder à Internet. Dans cet exemple, nous utilisons une règle qui autorise tout ce qui provient du réseau interne à accéder à l’Internet via le masque NAT.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
3	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	Tous

Quelque chose ne convient pas avec cet ensemble de règles.

En admettant que nous voulions exécuter la traduction d’adresses pour des raisons tant de sécurité que de fonctionnalité, on se rend compte que cet ensemble de règles ne cache pas nos adresses internes dans la DMZ. La connexion des machines internes au port wan_ip 80 est autorisée par la règle 2 qui gère les communications. D’un point de vue interne, toutes les machines de la DMZ doivent être considérées comme n’importe quel serveur Internet connecté. Cependant, on ne peut se fier à tous les serveurs, c’est pourquoi il faut d’abord les localiser dans la DMZ.

Deux solutions sont possibles :

Vous pouvez modifier la règle 2 pour qu'elle ne s'applique qu'au trafic externe.

Vous pouvez échanger les places des règles 2 et 3 afin que la règle NAT du trafic interne soit exécutée avant la règle Allow.

Laquelle de ces deux options est la meilleure ? Dans cette configuration, les deux solutions ne font aucune

différence. Elles fonctionnent aussi bien l’une que l’autre.

Cependant, en supposant que nous utilisions une autre interface (ext2) dans le firewall D-Link et que nous la connections à un autre réseau, par exemple celui d’une entreprise voisine, la communication serait alors bien plus rapide avec nos serveurs.

Si l'option 1 a été choisie, l’ensemble de règles doit donc être ajusté :

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST 10.10.10.5 80
2	Allow (Autoriser)	wan	all-nets (tout réseau)	core (noyau)	wan_ip	http
3	Allow (Autoriser)	ext2	ext2net	core (noyau)	wan_ip	http
4	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	Tous

Cette solution augmente le nombre de règles : une pour chaque interface autorisée à communiquer avec le serveur Web. Cependant, l’ordre des règles n’est pas important, ce qui peut éviter des erreurs.

Si l'option 2 a été choisie, l’ensemble de règles doit donc être ajusté :

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST 10.10.10.5 80
2	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	Tous
3	Allow (Autoriser)	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http

Avec cette solution, il n’est pas nécessaire d’augmenter le nombre de règles. Il n’y a pas de problèmes tant que toutes les interfaces sont suffisamment fiables pour pouvoir communiquer avec le serveur Web. Toutefois, si plus tard vous ajoutez une interface qui n'est pas suffisamment fiable pour pouvoir communiquer avec le serveur Web, des règles Drop (Ignorer) doivent être placées avant celle qui autorise l'accès au serveur Web à toutes les machines.

Il faut déterminer la meilleure méthode au cas par cas et prendre en compte toutes les circonstances.

Exemple 7.4. Autorisation du trafic vers un serveur Web sur un réseau interne

L'exemple que nous avons choisi d'utiliser est celui d'un serveur Web avec une adresse privée situé sur un réseau interne. Du point de vue de la sécurité, cette approche n'est pas bonne, car les serveurs Web sont très vulnérables face aux attaques et doivent donc se situer sur une DMZ. Cependant, nous avons retenu ce modèle dans notre exemple du fait de sa simplicité.

Afin que des utilisateurs externes puissent accéder au serveur Web, ils doivent pouvoir le contacter avec une adresse publique. Dans cet exemple, nous avons choisi de traduire le port 80 de l’adresse externe du firewall D-Link en port 80 sur le serveur Web.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST wwwsrv 80
2	Allow (Autoriser)	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http

Ces deux règles nous permettent d’accéder au serveur Web via l'adresse IP externe du firewall D-Link. La règle 1 énonce que la traduction d’adresse peut être effectuée si la connexion a été autorisée et la règle 2 autorise la connexion.

Bien entendu, nous avons aussi besoin d’une règle qui autorise les machines internes à avoir une traduction d’adresses dynamique pour accéder à Internet. Dans cet exemple, nous utilisons une règle qui autorise tout ce qui provient du réseau interne à accéder à l’Internet via le masque NAT.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
3	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	Tous

Le problème posé par cet ensemble de règles est qu'il ne fonctionnera pas du tout pour tout trafic provenant du réseau interne.

Afin d’illustrer ce qu’il se passe exactement, nous utilisons les adresses IP qui suivent :

wan_ip (195.55.66.77) : une adresse IP publique

lan_ip (10.0.0.1) : l’adresse IP interne privée du firewall D-Link

wwwsrv (10.0.0.2) : l’adresse IP privée des serveurs Web

PC1 (10.0.0.3) : une machine avec une adresse IP privée

PC1 envoie un paquet à wan_ip pour atteindre « www.notresociété.com » :
10.0.0.3:1038 => **195.55.66.77:80**

NetDefendOS traduit l’adresse en fonction de la règle 1 et transfère le paquet en fonction de la règle 2.
10.0.0.3:1038 => **10.0.0.2:80**

wwwsrv traite le paquet et répond :
10.0.0.2:80 => **10.0.0.3:1038**

Cette réponse arrive directement à PC1 sans passer par le firewall D-Link. Ceci pose des problèmes. Ce dysfonctionnement est causé par le fait que PC1 attend une réponse de la part de 195.55.66.77:80, et non pas de 10.0.0.2:80. La réponse non attendue est rejetée et PC1 continue d'attendre une réponse qui n’arrivera pas.

Le fait d'opérer un changement mineur dans l'ensemble de règles comme décrit ci-dessus résout le problème. Dans cet exemple, nous avons choisi d'utiliser l'option 2 sans aucune raison particulière :

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST wwwsrv 80
2	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	Tous
3	Allow (Autoriser)	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http

PC1 envoie un paquet à wan_ip pour atteindre « www.notresociété.com » :
10.0.0.3:1038 => **195.55.66.77:80**

NetDefendOS traduit l’adresse de manière statique en fonction de la règle 1 et de manière dynamique en fonction de la règle 2 :
10.0.0.1:32789 => **10.0.0.2:80**

wwwsrv traite le paquet et répond :
10.0.0.2:80 => **10.0.0.1:32789**

La réponse est reçue et les deux adresses sont restaurées :
195.55.66.77:80 => **10.0.0.3:1038**

De cette manière, la réponse arrive à PC1 avec la bonne adresse.

Une autre solution consiste à autoriser les clients internes à s’adresser directement à 10.0.0.2, ce qui évitera tous problèmes associés à la traduction d’adresses. Cependant, cette solution n’est pas toujours pratique.

Traduction d’adresses IP multiples (M:N)

Une règle SAT unique peut être utilisée pour traduire une plage entière d’adresses IP. Dans ce cas, le résultat réside en une transposition où la première adresse d'origine sera traduite par la première adresse de la liste de traduction, et ainsi de suite.

Par exemple, une règle SAT qui spécifie que les connexions vers le réseau 194.1.2.16/29 doivent être traduites par 192.168.0.50 entraînera des transpositions suivant le tableau ci-dessous :

Adresse d’origine	**Adresse traduite**
194.1.2.16	192.168.0.50
194.1.2.17	192.168.0.51
194.1.2.18	192.168.0.52
194.1.2.19	192.168.0.53
194.1.2.20	192.168.0.54
194.1.2.21	192.168.0.55
194.1.2.22	192.168.0.56
194.1.2.23	192.168.0.57

En d’autres termes :

Les tentatives de communication avec 194.1.2.16 entraîneront une connexion avec 192.168.0.50.

Les tentatives de communication avec 194.1.2.22 entraîneront une connexion avec 192.168.0.56.

Un exemple de l’utilité de cette solution s'illustre lorsque chaque serveur protégé par une DMZ ne doit être accessible que par une adresse IP publique unique.

Exemple 7.5. Traduction du trafic en direction de plusieurs serveurs Web protégés

Dans cet exemple, nous allons créer une règle SAT qui traduira et autorisera les connexions provenant d'Internet vers cinq serveurs Web situés dans une DMZ. Le firewall D-Link est connecté à Internet via l’interface wan et les adresses IP publiques à utiliser font partie de la plage 195.55.66.77 à 195.55.66.81. Les adresses IP des serveurs Web font partie de la plage 10.10.10.5 à 10.10.10.9 et sont accessibles via l'interface dmz.

Pour accomplir cette tâche, les étapes suivantes doivent être effectuées :

Définissez un objet adresse qui contient les adresses IP publiques.

Définissez un autre objet adresses pour la base des adresses IP des serveurs Web.

Publiez les adresses IP publiques sur l'interface wan en utilisant le mécanisme de l’ARP.

Créez une règle SAT qui opérera la traduction.

Créez une règle Allow qui autorisera les connexions HTTP entrantes.

Interface de ligne de commande
Créez un objet adresse pour les adresses IP publiques :

```
gw-world:/> add Address IP4Address wwwsrv_pub Address=195.55.66.77-195.55.66.81
```

Créez un autre objet pour la base des adresses IP des serveurs Web :

```
gw-world:/> add Address IP4Address wwwsrv_priv_base Address=10.10.10.5
```

Publiez les adresses IP publiques sur l'interface wan en utilisant l’ARP. Un élément ARP est nécessaire pour chaque adresse IP :

```
gw-world:/> add ARP Interface=wan IP=195.55.66.77 mode=Publish
```

Répétez l’opération pour les cinq adresses IP publiques. Créez une règle SAT pour la traduction :

```
gw-world:/> add IPRule Action=SAT Service=http SourceInterface=any
   SourceNetwork=all-nets DestinationInterface=core
   DestinationNetwork=wwwsrv_pub SATTranslateToIP=wwwsrv_priv_base
   SATTranslate=DestinationIP
```

Pour finir, créez une règle Allow correspondante :

```
gw-world:/> add IPRule Action=Allow Service=http SourceInterface=any
   SourceNetwork=all-nets DestinationInterface=core
   DestinationNetwork=wwwsrv_pub
```

Interface Web

Créez un objet adresse pour l’adresse IP publique :

Sélectionnez Objects > Address Book > Add > IP address (Objets > Carnet d’adresses > Ajouter > Adresse IP).

Spécifiez un nom convenable pour l’objet, par exemple *wwwsrv_pub*.

Entrez *195.55.66.77-195.55.66.77.81* comme adresse IP.

Cliquez sur OK.

Créez un autre objet adresse pour la base des adresses IP des serveurs Web :

Sélectionnez Objects > Address Book > Add > IP address (Objets > Carnet d’adresses > Ajouter > Adresse IP).

Spécifiez un nom convenable pour l’objet, par exemple *wwwsrv_priv_base*.

Entrez l’adresse IP*10.10.10.5*.

Cliquez sur OK.

Publiez les adresses publiques sur l'interface wan en utilisant l’ARP. Un élément ARP est nécessaire pour chaque adresse IP :

Sélectionnez Interfaces > ARP > Add > ARP (ARP > Ajouter > ARP).

Saisissez :

Mode : Publish (Publier)

Interface : wan

IP Address (Adresse IP) : 195.55.66.77

Cliquez sur OK et répétez l'opération pour les 5 adresses IP publiques.

Créez une règle SAT pour la traduction :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Spécifiez un nom convenable pour la règle, par exemple : *SAT_HTTP_To_DMZ*.

Saisissez :

Action : SAT

Service : http

Source Interface (Interface source) : any (toutes)

Source Network (Réseau source) : all-nets (tout réseau)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : wwwsrv_pub

Allez sur l'onglet SAT.

Assurez-vous que l'option Destination IP Address (Adresse IP de destination) est sélectionnée.

Dans la liste déroutante New IP Address (Nouvelle adresse IP), sélectionnez *wwwsrv_priv*.

Cliquez sur OK.

Pour finir, créez une règle Allow correspondante :

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Spécifiez un nom convenable pour la règle, par exemple : *Allow_HTTP_To_DMZ*.

Saisissez :

Action : Allow (Autoriser)

Service : http

Source Interface (Interface source) : any (toutes)

Source Network (Réseau source) : all-nets (tout réseau)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : wwwsrv_pub

Cliquez sur OK.

Mappages tous-un (N:1)

NetDefendOS peut être utilisé pour traduire des plages et/ou des groupes en une seule adresse IP.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	194.1.2.16-194.1.2.20, 194.1.2.30	http SETDEST all-to-one (tous-un) 192.168.0.50 80

Cette règle entraîne une traduction N:1 de toutes les adresses dans le groupe (la plage 194.1.2.16 à 194.1.2.20 et 194.1.2.30) jusqu'à l'IP 192.168.0.50.

Les tentatives de communication avec 194.1.2.16 sur le port 80 entraîneront une connexion avec 192.168.0.50.

Les tentatives de communication avec 194.1.2.30 sur le port 80 entraîneront une connexion avec 192.168.0.50.

Remarque

Quand *all-nets* (tout réseau) est la destination, un mappage tous-un est toujours effectué.

Traduction de port

La *traduction de port*, ou PAT (*Port Address Translation*, Traduction d’adresses de port), peut être utilisée pour modifier le port source ou de destination.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wwwsrv_pub	TCP 80-85 SETDEST 192.168.0.50 1080

Cette règle effectue une traduction 1:1 de tous les ports de la plage 80 à 85 vers la plage 1080 à 1085.

Les tentatives de communication avec l’adresse publique des serveurs Web sur le port 80 entraîneront une connexion avec l’adresse privée des serveurs Web sur le port 1080.

Les tentatives de communication avec l’adresse publique des serveurs Web sur le port 84 entraîneront une connexion avec l’adresse privée des serveurs Web sur le port 1084.

Remarque

Afin de créer une règle SAT qui permette la traduction de port, il faut utiliser un service personnalisé.

Protocoles gérés par la SAT

De manière générale, la traduction d’adresses statique peut gérer tous les protocoles qui permettent la traduction d’adresses. Cependant, il existe certains protocoles qui ne peuvent être traduits que dans des cas spéciaux et d’autres qui ne peuvent pas être traduits du tout.

Les protocoles qui ne peuvent pas être traduits avec la SAT ne le sont vraisemblablement pas non plus avec NAT. Ceci s’explique de différentes manières :

Le protocole cryptographique nécessite que les adresses ne soient pas altérées, et ceci s’applique à beaucoup de protocoles VPN.

Le protocole intègre ses adresses IP dans les données de niveau TCP ou UDP et par la suite requiert que, d’une façon ou d’une autre, les adresses visibles au niveau de l’IP soient les mêmes que celles intégrées dans les données. Quelques exemples de ces protocoles : le FTP et les ouvertures de sessions aux domaines NT via NetBIOS.

Chaque partie essaie d’ouvrir les nouvelles connexions dynamiques aux adresses visibles par cette même partie. Dans certains cas, ce problème peut être résolu en modifiant l’application ou bien la configuration du firewall.

Il n’existe pas de liste définitive des protocoles qui peuvent ou ne peuvent pas subir de traduction d’adresses. La règle générale est que les protocoles VPN ne peuvent pas être traduits. En outre, les protocoles qui ouvrent des connexions secondaires en plus des connexions initiales peuvent être difficiles à traduire.

Certains protocoles dont l'adresse est difficile à traduire peuvent être pris en charge par des algorithmes spécialement écrits pour eux, afin de lire et/ou altérer les données d'application. On les évoque souvent en tant que passerelles ALG (*Application Layer Gateways*) ou *filtres au niveau application*. NetDefendOS prend en charge

beaucoup de ces passerelles ALG. Pour obtenir plus d'informations, veuillez consulter la section intitulée « Passerelles ALG ».

Multiples correspondances de règles SAT

NetDefendOS n’achève pas la recherche dans l'ensemble de règles après qu'une règle SAT correspondante ait été trouvée. À la place, la recherche continue jusqu’à trouver une règle Allow, NAT ou FwdFast correspondante. C’est seulement après avoir trouvé une de ces règles que le firewall opère la traduction d’adresses statique.

Malgré cela, la première règle SAT correspondante trouvée pour chaque adresse est celle qui est utilisée.

« Chaque adresse » signifie que deux règles SAT peuvent être effectives au même moment sur la même connexion, à condition que l'une traduise l'adresse de l'émetteur et l'autre l'adresse du récepteur.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wwwsrv_pub	TCP 80-85 SETDEST 192.168.0.50 1080
2	SAT	lan	lannet	all-nets (tout réseau)	Standard	SETSRC pubnet

Les deux règles ci-dessus peuvent être exécutées simultanément sur la même connexion. Dans cet exemple, les adresses de l'émetteur interne seront traduites dans le « pubnet » sur une base 1:1. De plus, si quiconque tente de se connecter à l’adresse publique du serveur Web, l’adresse de destination changera pour son adresse privée.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	lan	lannet	wwwsrv_pub	TCP 80-85	SETDEST intrasrv 1080
2	SAT	any (toutes)	all-nets (tout réseau)	wwwsrv_pub	TCP 80-85	SETDEST wwwsrv-priv 1080

Dans cet exemple, les deux règles sont paramétrées pour traduire l'adresse de destination, ce qui signifie qu’une seule d’entre elles sera exécutée. Si une tentative interne de communiquer avec l'adresse publique des serveurs Web est opérée, elle sera redirigée vers un serveur intranet. Si une quelconque autre tentative de communiquer avec l'adresse publique des serveurs Web est opérée, elle sera redirigée vers l’adresse privée du serveur Web accessible au public.

Encore une fois, notez que les règles ci-dessus ne peuvent pas fonctionner si une règle Allow ne leur est pas associée dans l'ensemble de règles.

Règles SAT et FwdFast

Il est possible d’utiliser la traduction d’adresses statique conjointement avec les règles FwdFast, bien que le trafic retour doive être explicitement autorisé et traduit.

Les règles qui suivent forment un exemple concret de la traduction d’adresses statique grâce à des règles FwdFast vers un serveur situé sur un réseau interne.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST wwwsrv 80
2	SAT	lan	wwwsrv	any (toutes)	all-nets (tout réseau)	80 -> All SETSRC wan_ip 80

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
3	FwdFast	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http
4	FwdFast	lan	wwwsrv	any (toutes)	all-nets (tout réseau)	80 -> All

Ajoutons une règle NAT pour autoriser les connexions depuis le réseau interne vers l'Internet.

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
5	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	Tous

Que se passe t'il désormais ?

Le trafic externe vers wan_ip:80 correspond aux règles 1 et 3 et est envoyé vers wwwsrv. Vrai.

Le trafic retour provenant de wwwsrv:80 correspond aux règles 2 et 4 et apparaît comme étant envoyé par wan_ip:80. Vrai.

Le trafic interne vers wan_ip:80 correspond aux règles 1 et 3 et est envoyé vers wwwsrv. Presque vrai, les paquets arrivent vers wwwsrv, mais :

le trafic retour provenant de wwwsrv:80 et en direction des machines internes est envoyé directement vers les machines elles-mêmes. Cette solution ne fonctionnera pas, puisque les paquets seront vus comme provenant de la mauvaise adresse.

Essayons maintenant de déplacer la règle NAT entre les règles SAT et FwdFast :

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST wwwsrv 80
2	SAT	lan	wwwsrv	any (toutes)	all-nets (tout réseau)	80 -> All SETSRC wan_ip 80
3	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	All (Tous)
4	FwdFast	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http
5	FwdFast	lan	wwwsrv	any (toutes)	all-nets (tout réseau)	80 -> All (Tous)

Que se passe t'il désormais ?

Le trafic externe vers wan_ip:80 correspond aux règles 1 et 4 et est envoyé vers wwwsrv. Vrai.

Le trafic retour qui provient de wwwsrv:80 correspond aux règles 2 et 3. Les réponses subissent donc une traduction d'adresses dynamique. Ceci change complètement le numéro de port source, qui ne fonctionnera plus.

Le problème peut être résolu en utilisant l'ensemble de règles qui suit :

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
1	SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	wan_ip	http SETDEST wwwsrv 80

#	Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Paramètres
2	SAT	lan	wwwsrv	any (toutes)	all-nets (tout réseau)	80 -> All SETSRC wan_ip 80
3	FwdFast	lan	wwwsrv	any (toutes)	all-nets (tout réseau)	80 -> All (Tous)
4	NAT	lan	lannet	any (toutes)	all-nets (tout réseau)	All (Tous)
5	FwdFast	lan	wwwsrv	any (toutes)	all-nets (tout réseau)	80 -> All (Tous)

Le trafic externe vers wan_ip:80 correspond aux règles 1 et 5 et est envoyé vers wwwsrv.

Le trafic retour qui provient de wwwsrv:80 correspond aux règles 2 et 3.

Le trafic interne vers wan_ip:80 correspond aux règles 1 et 4 et est envoyé vers wwwsrv. L’adresse de l’émetteur est l’adresse IP interne du firewall D-Link. Ceci garantit que le trafic retour passe par le firewall D-Link.

Le trafic retour est automatiquement pris en charge par le mécanisme d'inspection dynamique du firewall D-Link.

Chapitre 8. Authentification de l’utilisateur

Le présent chapitre indique comment NetDefendOS met en application l’authentification de l’utilisateur

Présentation

Lorsque des utilisateurs individuels se connectent à des ressources protégées via un firewall D-Link, l’administrateur demande souvent leur *authentification* avant que l’accès ne leur soit accordé. Ce chapitre traite du paramétrage de l'authentification pour NetDefendOS. Mais dans un premier temps, nous allons examiner les problèmes généraux qui y sont liés.

Confirmation d’identité. Le but de l’authentification est de faire en sorte que l’utilisateur prouve son identité afin que l’administrateur du réseau puisse autoriser ou refuser l’accès aux ressources à cet utilisateur identifié. Voici plusieurs manières de prouver son identité :

A. Ce que l'utilisateur est. Un attribut unique qui est différent pour chaque personne : par exemple les empreintes digitales.

B. Ce que l'utilisateur a : une carte d’accès, un certificat numérique X.507 ou des clés privées ou publiques.

C. Ce que l'utilisateur sait : un mot de passe.

La méthode A requiert un lecteur d’empreintes spécial. De plus, si ce dispositif est perdu, il ne peut dans la plupart des cas pas être remplacé. Les méthodes B et C sont donc les plus communes en matière de sécurisation d’un réseau. Cependant, elles présentent des inconvénients : Les clés peuvent être interceptées, les cartes d’accès volées, les mots de passe devinés ou les secrets difficiles à garder. Les méthodes B et C sont souvent combinées (cas d’une carte d’accès qui nécessite un mot de passe ou un code PIN pour fonctionner, par exemple).

Utilisation de noms d’utilisateur et de mots de passe. Ce chapitre traite spécialement de l’authentification de l’utilisateur via la validation combinée de son nom d’utilisateur et de son mot de passe lorsqu'il essaie d'accéder à des ressources. L’accès à Internet via le protocole HTTP et grâce à un firewall D-Link représente un bon exemple du cas de figure où la combinaison d'un nom d'utilisateur et d'un mot de passe est la méthode d'authentification de base.

Avec cette approche, les mots de passe sont souvent soumis à des attaques d'indésirables qui supposent le mot de passe ou bien qui font des recherches systématiques. Pour parer à cela, le mot de passe doit être choisi avec précaution. Le mot de passe idéal doit :

contenir plus de 8 caractères sans répétition ;

utiliser des caractères aléatoires qu’on ne retrouve généralement pas dans des mots ;

contenir des caractères en minuscule ET en majuscule ;

contenir des chiffres ET des caractères spéciaux.

Pour une sécurité optimale, les mots de passe doivent aussi :

n’être inscrits nulle part ;

ne jamais être confiés à un tiers ;

être modifiés de façon régulière (une fois tous les trois mois).

Configuration de l’authentification

Résumé du paramétrage

La liste suivante répertorie les étapes du paramétrage de l’authentification de l’utilisateur avec NetDefendOS.

Paramétrez une base de données des utilisateurs, chacun avec une combinaison nom d’utilisateur/mot de passe. Elle peut se trouver en local dans un objet *User DB* (BD utilisateur) de NetDefendOS, ou à distance dans un serveur RADIUS sur lequel elle est désignée comme *source de l'authentification*. L’appartenance à un *groupe d’authentification* peut être éventuellement spécifiée pour chaque utilisateur.

Définissez une *règle d’authentification de l’utilisateur* qui indique quel trafic va être authentifié et quelle *source de l’authentification* va être utilisée.

Définissez un objet IP pour les adresses IP des clients qui vont être authentifiés. Associez ces adresses à un groupe d'authentification si nécessaire.

Paramétrez des règles IP pour que l'authentification puisse s'opérer, mais également pour permettre aux clients appartenant à l'objet IP créé dans l'étape précédente d'accéder aux ressources.

Les sections suivantes décrivent en détail les composants de ces étapes.

Sources de l’authentification. Base de données qu’une règle d’authentification utilise pour vérifier la combinaison nom d'utilisateur/mot de passe. Elle peut être de l'un de ces deux types :

La base de données locale au sein de NetDefendOS.

Un serveur RADIUS qui est externe au firewall D-Link.

La base de données locale

La base de données utilisateur locale est un registre intégré à NetDefendOS qui contient les profils des utilisateurs et des groupes d'utilisateurs autorisés. Des noms d’utilisateurs et des mots de passe peuvent être entrés dans cette base de données et les utilisateurs qui bénéficient des mêmes privilèges peuvent être rassemblés en *groupes* pour une plus grande facilité de gestion.

Il existe deux groupes d’utilisateurs par défaut : le groupe des administrateurs et le groupe des auditeurs. Les utilisateurs qui sont membres du groupe des administrateurs sont autorisés à modifier la configuration de NetDefendOS, tandis que les utilisateurs qui appartiennent au groupe des auditeurs ne peuvent que voir la configuration. Cliquez sur les boutons situés sous la boîte d'édition des groupes pour ajouter un utilisateur à ces groupes.

Serveurs d’authentification externes

La nécessité des serveurs. Pour une topologie de réseau et une charge de travail administratif plus importants, il est souvent préférable d’avoir une base de données d’authentification centrale sur un serveur dédié. Lorsqu’il y a plusieurs firewalls D-Link sur le réseau et des centaines d’utilisateurs, le fait d’entretenir des bases de données d’authentification séparées sur chaque routeur devient problématique. À la place, un serveur d’authentification externe peut valider la combinaison nom d'utilisateur/mot de passe en réponse à des requêtes de NetDefendOS. Pour permettre cela, NetDefendOS prend en charge le protocole RADIUS (*Service Utilisateur Entrant d’Authentification Distante*).

RADIUS et NetDefendOS. NetDefendOS agit comme un client RADIUS et envoie les authentifiants utilisateur et les paramètres de connexion dans un message RADIUS vers un serveur RADIUS précis. Le serveur traite les requêtes et répond par un message RADIUS d’autorisation ou de refus. Un ou plusieurs serveurs externes peuvent être définis dans NetDefendOS.

Sécurité RADIUS. Pour garantir la sécurité, un *secret partagé* commun est configuré sur le client RADIUS et le serveur. Ce secret permet le chiffrage des messages envoyés depuis le client RADIUS vers le serveur. Il apparaît généralement sous la forme d'une chaîne textuelle relativement longue. Cette chaîne peut contenir jusqu'à 100 caractères et est sensible à la casse.

RADIUS utilise le PPP pour transférer les requêtes nom d'utilisateur/mot de passe entre le client et le serveur

RADIUS et utilise également les schémas d'authentification PPP tels que le PAP et le CHAP. Les messages RADIUS sont envoyés comme des messages UDP via le port UDP 1812.

Règles d’authentification

Les règles d’authentification sont paramétrées d’une manière similaire à d’autres règles de sécurité de NetDefendOS, c’est-à-dire en spécifiant quel trafic est soumis à la règle en question. Elles différent des autres règles du fait que le réseau et l'interface de destination n'ont pas d'importance, contrairement au réseau et à l’interface source. Une règle d’authentification possède les paramètres suivants :

Interface : l’interface source sur laquelle arrivent les connexions à authentifier.

Source IP (IP source) : le réseau source d’où proviennent ces connexions.

Authentification Source (Source de l’authentification) : indique si l’authentification est opérée par une base de données locale définie au sein de NetDefendOS ou par un serveur RADIUS (détaillé ci-dessous).

Agent : le type du trafic à authentifier. Il peut être :

HTTP ou HTTPS : les connexions Web à authentifier via une page Web prédéfinie ou personnalisée (pour plus d’informations sur le HTTP, veuillez consulter les explications détaillées ci-dessous).

PPP : tunnel d’authentification L2TP ou PPP.

XAUTH : authentification IKE qui fait partie de l’établissement d’un tunnel IPsec.

Délais d'expiration de la connexion. Une règle d'authentification peut spécifier les délais d’expiration relatifs à une session utilisateur suivants :

Idle Timeout (Délai d'expiration de l'inactivité) : le délai durant lequel une connexion peut être inactive avant d'être automatiquement achevée (1 800 secondes par défaut).

Session Timeout (Délai d’expiration de la session) : la durée de vie maximale d'une connexion (aucune valeur n'est spécifiée par défaut).

Si le choix est porté vers un serveur d'authentification, alors l'option Use timeouts received from the authentication server (Utiliser les délais d'expiration du serveur d'authentification) peut être activée pour utiliser les valeurs de ce serveur.

Connexions multiples. Une règle d'authentification peut indiquer comment traiter les *connexions multiple*s lorsque plusieurs utilisateurs avec des adresses IP source différentes essaient de se connecter avec le même nom d’utilisateur. Voici les options disponibles :

Autoriser les connexions multiples afin que plusieurs clients puissent utiliser la même combinaison nom d’utilisateur/mot de passe en même temps.

N’autoriser qu’une seule connexion à la fois par nom d’utilisateur.

N’autoriser qu’une seule connexion à la fois par nom d’utilisateur et déconnecter un utilisateur déjà présent avec le même nom s’il est inactif depuis une certaine période de temps lorsque la nouvelle connexion se produit.

Processus d’authentification

La liste ci-dessous décrit le processus d'authentification du nom d'utilisateur et du mot de passe par NetDefendOS.

Un utilisateur crée une nouvelle connexion vers le firewall D-Link.

NetDefendOS s’aperçoit de la nouvelle connexion utilisateur sur une interface et vérifie *l'ensemble de règles d'authentification* pour voir si une règle correspond au trafic sur cette interface, provenant de ce réseau et les données qui peuvent être des types suivants :

HTTP traffic (Trafic HTTP)

HTTPS traffic (Trafic HTTPS)

IPsec tunnel traffic (Trafic tunnel IPsec)

L2TP tunnel traffic (Trafic tunnel L2TP)

PPTP tunnel traffic (Trafic tunnel PPTP)

Si aucune règle d'authentification ne correspond et si l'ensemble de règles IP le permet, la connexion est autorisée. Plus rien ne se produit alors dans le processus d'authentification.

En fonction des paramètres de la règle d'authentification correspondante, NetDefendOS invite l'utilisateur à s'authentifier.

L'utilisateur répond en saisissant ses informations d'identification qui sont généralement une combinaison nom d'utilisateur/mot de passe.

NetDefendOS valide les informations par rapport à la *source de l'authentification* spécifiée dans la règle d'authentification. Elle peut être soit une base de données locale de NetDefendOS, soit un serveur de base de données RADIUS externe.

NetDefendOS permet alors le trafic à travers cette connexion si l'authentification réussit et tant que le service requis est autorisé par l'une des règles de l'ensemble de règles IP. L'objet réseau source de cette règle peut avoir l'option No Defined Credentials (Pas d'authentifiants définis) activée, ou bien peut être associé à un groupe dont l'utilisateur est membre.

Si un délai d'expiration est précisé dans la règle d'authentification, alors l'utilisateur authentifié sera automatiquement déconnecté après avoir été inactif pendant cette période.

Tout paquet qui provient d'une adresse IP et qui échoue son authentification est rejeté (à moins qu'il ne soit retenu par une autre règle).

Authentification HTTP

Si des utilisateurs sont en communication grâce à un navigateur Web et via le protocole HTTP, ils peuvent s'authentifier avec des pages HTML où ils saisissent leurs informations utilisateur. Ce procédé est souvent appelé *WebAuth* et sa configuration requiert des précautions particulières.

Changement du port de l'interface de gestion Web utilisateur. L'authentification HTTP est incompatible avec la fonctionnalité de gestion à distance de l'interface Web utilisateur, qui utilise aussi le port TCP 80. Pour éviter cette situation, le numéro de port de l'interface Web utilisateur doit être changé avant de configurer l'authentification. Vous pouvez effectuer ceci sur l'interface Web utilisateur en allant dans Remote Management > Advanced Settings (Gestion à distance > Paramètres avancés) et en modifiant le paramètre WebUI HTTP Port (Port HTTP de l'interface Web utilisateur). Le port numéro 81 peut être utilisé à la place.

Options agents. Pour l'authentification HTTP et HTTPS, il existe un panel d'options dans les règles d'authentification qui s'appellent options agents. Ces dernières sont :

Login Type (Type de connexion). On distingue différents types :

FORM : l'utilisateur remplit une page d'authentification HTML. Les données sont envoyées à NetDefendOS avec un POST. La page HTML est déjà prédéfinie par NetDefendOS, mais elle peut être personnalisée comme décrit ci-dessous.

BASICAUTH : cette option envoie un message 401 de requête d'authentification vers le navigateur, qui utilise alors sa propre boîte de dialogue intégrée pour demander la combinaison nom d'utilisateur/mot de passe. Une chaîne de domaine peut éventuellement être précisée. Elle apparaît dans la boîte de dialogue du navigateur.

> L'option FORM est recommandée par rapport à BASICAUTH car, dans certains cas, le navigateur peut conserver les données de connexion dans son cache.

Si l'agent est paramétré sur *HTTPS*, alors le certificat de l'hôte et le certificat racine doivent être sélectionnés

parmi une liste de certificats déjà présents dans NetDefendOS.

Paramétrage des règles IP. L'authentification HTTP n'a pas lieu tant qu'une règle d'autorisation n'est pas ajoutée dans l'ensemble de règles IP. Si nous examinons l'exemple de plusieurs clients du réseau local *lannet* qui veulent accéder à l'Internet public sur l'interface *wan*, l'ensemble de règles IP contiendrait les règles suivantes :

	Action	**Interface source**	**Réseau source**	**Interface de destination**	**Réseau de destination**	**Service**
1	Allow (Autoriser)	lan	lannet	core (noyau)	lan_ip	http-all
2	NAT	lan	trusted_users	wan	all-nets (tout réseau)	http-all
3	NAT	lan	lannet	wan	all-nets (tout réseau)	dns-all

La première règle autorise l'authentification et suppose que le client tente d'accéder à *lan_ip*, qui est l'adresse IP de l'interface du firewall D-Link sur laquelle le réseau local se connecte.

La deuxième règle autorise une navigation normale, mais on ne peut pas juste utiliser *lannet* comme réseau source puisque la règle se déclencherait pour tout client non authentifié de ce réseau. À la place, le réseau source est un objet IP défini par l'administrateur et appelé *trusted_users*. Il s'agit du même réseau que *lannet*, à l'exception du fait que son option d'authentification No Defined Credentials (Pas d'authentifiants définis) est activée, ou bien qu'il soit rattaché à un groupe d'authentification (celui dont sont membres les utilisateurs).

La troisième règle permet la surveillance DNS des URL.

Authentification forcée. Avec ce paramètre, lorsque des utilisateurs qui ne sont pas authentifiés tentent de naviguer vers n'importe quelle IP sauf *lan_ip*, les règles le bloqueront et ses paquets seront ignorés. Pour que ces utilisateurs débouchent toujours sur la page d'authentification, nous devons ajouter une règle SAT, ainsi que la règle Allow associée. L'ensemble de règles est désormais semblable à celle-là :

	Action	**Interface source**	**Réseau source**	**Interface de destination**	**Réseau de destination**	**Service**
1	Allow (Autoriser)	lan	lannet	core (noyau)	lan_ip	http-all
2	NAT	lan	trusted_users	wan	all-nets (tout réseau)	http-all
3	NAT	lan	lannet	wan	all-nets (tout réseau)	dns-all
4	SAT	lan	lannet	wan	all-nets (tout réseau) All-to-one (plusieurs-un) 127.0.0.1	http-all
5	Allow (Autoriser)	lan	lannet	wan	all-nets (tout réseau)	http-all

La règle SAT intercepte toutes les requêtes non authentifiées. Elle doit être paramétrée avec un mappage d'adresse en plusieurs-un qui les redirigera vers l'adresse *127.0.0.1*. Cette adresse est celle du noyau (NetDefendOS lui-même).

Exemple 8.1. Création d'un groupe utilisateurs d'authentification

Dans l'exemple d'un objet d'adresse d'authentification dans le carnet d'adresses, nous allons utiliser le groupe d'utilisateurs « users » pour permettre l'authentification utilisateur sur « lannet ». Cet exemple indique comment configurer un groupe d'utilisateurs dans la base de données de NetDefendOS.

Interface Web

Étape A

Sélectionnez User Authentication > Local User Databases > Add > LocalUserDatabase (Authentification utilisateur > Bases de données utilisateur locale > Ajouter > Base de données utilisateur locale).

Saisissez :

Name (Nom) : lannet_auth_users

Commentaires : dossier pour « users » : groupe utilisateurs d'authentification « lannet ».
Cliquez sur OK.

Étape B

Sélectionnez lannet_auth_users > Add > User.

Saisissez :

Username (Nom d'utilisateur) : Entrez le nom de compte de l'utilisateur, par exemple *user1*.

Password (Mot de passe) : Entrez le mot de passe de l'utilisateur.

Confirm Password (Confirmer le mot de passe) : Ressaisissez le mot de passe.

Groups (Groupes) : un utilisateur peut être membre de plusieurs groupes. Entrez le nom des groupes séparés par une virgule (*users* pour cet exemple).

Cliquez sur OK.

Répétez l'étape B pour ajouter tous les utilisateurs *lannet* qui sont membres du groupe *users* dans le dossier *lannet_auth_users*.

Exemple 8.2. Configuration de l'authentification utilisateur pour l'accès au Web

La configuration ci-dessous montre comment activer l'authentification utilisateur HTTP pour le groupe *users* sur *lannet*. Une des règles IP définit que seuls les utilisateurs membres du groupe *users* peuvent avoir accès au navigateur Web après l'authentification.

Nous supposons que *lannet*, *users*, *lan_ip*, le dossier de la base de données utilisateur locale « lannet_auth_users » et qu'un objet d'adresse *lannet_users* ont été spécifiés.

Interface Web

A. Paramétrez une règle IP pour permettre l'authentification.

Sélectionnez Rules > IP Rules > Add > IP Rule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : http2fw

Action : Allow (Autoriser)

Service : HTTP

Source Interface (Interface source) : lan

Source Network (Réseau source) : lannet

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : lan_ip

Cliquez sur OK.

B. Configurez la règle d’authentification.

Sélectionnez User Authentication > User Authentication Rules > Add > User Authentication Rule (Authentification utilisateur > Règles d’authentification utilisateur > Ajouter > Règle d’authentification utilisateur).

Saisissez :

Name (Nom) : HTTPLogin

Agent : HTTP

Authentication Source (Source de l’authentification) : local

Interface : lan

Originator IP (Générateur d’IP) : lannet

Pour Local User DB (Base de données utilisateur locale), sélectionnez *lannet_auth_users*.

Pour Login Type (Type de la connexion), sélectionnez *HTMLForm*.

Cliquez sur OK.

C. Paramétrez une règle IP pour autoriser les utilisateurs authentifiés à naviguer sur le Web.

Sélectionnez Rules > IP Rules > Add > IP Rule (Règles > Règles IP > Ajouter > Règle IP).

Saisissez :

Name (Nom) : Allow_http_auth

Action : NAT

Service : HTTP

Source Interface (Interface source) : lan

Source Network (Réseau source) : lannet_users

Destination Interface (Interface de destination) : any (toutes)

Destination Network (Réseau de destination) : all-nets (tout réseau)

Cliquez sur OK.

Exemple 8.3. Configuration d’un serveur RADIUS

Interface Web

Sélectionnez User Authentication > External User Databases > Add > External User Database (Authentification utilisateur > Bases de données utilisateur externes > Ajouter > Base de données utilisateur externe).

Saisissez :

Name (Nom) : entrez le nom du serveur.

Type : sélectionnez RADIUS.

IP Address (Adresse IP) : entrez l’adresse IP du serveur ou entrez son nom symbolique si le serveur a déjà été défini dans le Carnet d'adresses.

Port (Port) : 1812 (le service RADIUS utilise le port UDP 1812 par défaut)

Retry Timeout (Délai entre les tentatives) : 2 (NetDefendOS renvoie une requête d'authentification au serveur s'il n'a pas obtenu de réponse après le délai, qui est ici de 2 secondes. Il n’y a pas plus de trois tentatives.)

Shared Secret (Secret partagé) : entrez une chaîne textuelle pour un chiffrage basique des messages RADIUS.

Confirm Secret (Confirmer le secret) : ressaisissez la chaîne pour confirmer celle que vous venez d’entrer.

Cliquez sur OK.

Chapitre 9. VPN

Le présent chapitre décrit l'utilisation du VPN avec NetDefendOS.

Présentation

La nécessité des VPN

La plupart des réseaux sont connectés entre eux grâce à Internet. Les entreprises utilisent de plus en plus Internet puisqu'il offre des possibilités de communication efficaces et peu coûteuses. Il est cependant nécessaire de garantir le transfert des données par Internet vers le bon récepteur sans qu'un tiers puisse les lire ou les altérer. Il est également important que le récepteur puisse vérifier que personne ne falsifie les informations, c'est-à-dire qu'elle ne se fasse pas passer pour quelqu'un d'autre. Les *Réseaux Privés Virtuels* (VPN) répondent à ce besoin et offrent une méthode très rentable d'établir des liens sûrs afin que des données puissent être échangées de façon sécurisée.

Chiffrage VPN

Le chiffrage permet de créer des VPN sur Internet, sans aucun investissement de connectivité supplémentaire. Le chiffrage est une méthode globale qui comprend 3 techniques et autant d'avantages :

Confidentialité	Personne d'autre que le récepteur ne peut recevoir et comprendre la communication. La confidentialité est garantie par le chiffrage.
Authentification et intégrité	C'est la preuve pour le récepteur que la communication est effectivement envoyée par le bon expéditeur et que les données n'ont pas été modifiées durant leur cheminement. Ceci est assuré par l'authentification, qui utilise elle-même souvent la méthode de hachage chiffré.
Non rejet	C'est la preuve que l'expéditeur a effectivement envoyé les données ; ainsi, il ne peut pas nier cet envoi par la suite. Le non rejet est généralement un effet secondaire de l'authentification.

De manière générale, les VPN appliquent uniquement la confidentialité et l'authentification. Le non rejet n'est normalement pas appliqué au niveau du réseau, mais plutôt lors de transactions (document par document).

Planification VPN

En principe, un pirate qui vise une connexion VPN n'essaiera pas de violer le chiffrage VPN puisque cela nécessiterait un travail énorme. Il préférera surveiller le trafic VPN afin de déterminer s'il est utile d'attaquer l'autre extrémité de la connexion. De manière générale, les clients nomades et les succursales représentent des cibles bien plus attrayantes que les réseaux des grandes entreprises. Une fois l'intrusion accomplie, pénétrer dans les réseaux des grandes entreprises devient un jeu d'enfant.

Lors de la création de la structure d'un VPN, il faut s'intéresser à plusieurs problèmes subtils. Ceux-ci incluent :

La protection des ordinateurs portables et de bureau.

La restriction des accès par le VPN aux services désirés uniquement, puisque les ordinateurs portables sont vulnérables.

La création de DMZ pour des services qui doivent nécessairement être partagés avec d'autres entreprises, via le VPN.

L'adaptation des règles d'accès VPN pour les différents groupes d'utilisateurs.

La création de règles de distribution des clés.

On pense souvent à tort que les connexions VPN équivalent à celles du réseau interne du point de vue de la sécurité et qu'elles peuvent être directement mises en relation sans plus de précautions. Il est important de se rappeler que bien que la connexion VPN en elle-même est sûre, le niveau total de sécurité n'équivaut qu'à la sécurité pourvue à chaque extrémité du tunnel.

Les utilisateurs nomades ont de plus en plus l'habitude de se connecter directement au réseau de leur entreprise via le VPN depuis leur ordinateur portable. Cependant, l'ordinateur portable lui-même est rarement protégé. Ceci signifie qu'un intrus peut avoir accès au réseau protégé par l'intermédiaire d'un ordinateur portable non protégé qui a des connexions VPN déjà actives.

Une connexion VPN ne doit jamais être considérée comme faisant partie intégrante d'un réseau protégé. Le firewall du VPN doit se situer sur un DMZ spécial ou sur un firewall externe dédié à cette tâche. De cette manière, vous pouvez sélectionner les services auxquels il est possible d'accéder via le VPN et le modem et vous assurer ainsi que ces services sont bien protégés contre les intrus. Dans les cas où le firewall intègre une fonctionnalité VPN, il est normalement possible de préciser les types de communication autorisés. Le module VPN de NetDefendOS fournit cette fonctionnalité.

Distribution de clés

Il est conseillé d'établir les schémas de distribution des clés à l'avance. Plusieurs questions se posent :

Comment les clés sont-elles distribuées ? L'utilisation d'e-mails n'est pas une bonne méthode. La communication par téléphone est suffisamment sécurisée.

Combien de clés différentes convient-il d'utiliser ? Une clé par utilisateur ? Une par groupe d'utilisateurs ? Une par connexion LAN-LAN ? Une clé pour tous les utilisateurs et une clé pour chaque connexion LAN-LAN ? Il est probablement préférable d'utiliser plus de clés que nécessaire au moment présent, car il sera plus facile d'ajuster les accès par utilisateur et par groupe d'utilisateurs par la suite.

Les clés doivent-elles être renouvelées ? Si oui, à quelle fréquence ? Dans les cas où les clés sont partagées par plusieurs utilisateurs, vous pourriez vouloir se faire chevaucher les schémas afin que les vieilles clés fonctionnent encore pendant un petit laps de temps après que les nouvelles clés aient été définies.

Que se passe-t-il quand un employé en possession des clés quitte l'entreprise ? Si plusieurs utilisateurs utilisent la même clé, elle doit être renouvelée.

Dans le cas où la clé n'est pas directement programmée dans une unité du réseau telle qu'un firewall VPN, comment la clé doit-elle être stockée ? Sur une disquette ? Sur une phrase de passe à mémoriser ? Sur une carte à puce intelligente ? S'il s'agit d'un jeton physique, comment doit-on procéder ?

Guide de démarrage rapide VPN

Les composants du VPN seront présentés dans les prochaines sections de ce chapitre. Pour rendre les sections ultérieures plus explicites, le présent guide de démarrage rapide expose les étapes importantes du paramétrage VPN.

Il dresse un tableau étape par étape du paramétrage VPN pour les scénarios les plus communs. Ces derniers sont :

LAN-LAN IPsec avec clés pré-partagées.

Clients itinérants IPsec avec clés pré-partagées.

Clients itinérants IPsec avec certificats.

Clients itinérants L2TP avec clés pré-partagées.

Clients itinérants L2TP avec certificats.

Clients itinérants PPTP

LAN-LAN IPsec avec clés pré-partagées

Créez un objet clé pré-partagée.

Vous pouvez également créer un nouvel objet liste de proposition IKE et/ou un objet liste de proposition IPsec si les paramètres de la liste par défaut ne sont pas satisfaisants. Tout dépend des capacités de l'unité à l'autre bout du tunnel.

Les hôtes et les réseaux créent des objets IP pour :

La passerelle VPN distante qui est l'adresse IP de l'unité du réseau à l'autre bout du tunnel (nous appellerons cet objet *remote_gw*).

Le réseau distant qui se situe derrière la passerelle VPN distante (nous appellerons cet objet *remote_net*).

Le réseau local situé derrière le firewall D-Link et qui communique grâce au tunnel. Ici, nous supposons qu'il s'agit de l'adresse prédéfinie *lannet* et que ce réseau est associé à l'interface *lan* de NetDefendOS.

Créez un objet tunnel IPsec (nous appellerons cet objet *ipsec_tunnel*). Spécifiez les paramètres du tunnel suivants :

Définissez Local Network (Réseau local) sur *lannet*.

Définissez Remote Network (Réseau distant) sur *remote_net*.

Définissez Remote Gateway (Passerelle distante) sur *remote_gw*.

Définissez Encapsulation mode (Mode d'encapsulation) sur *Tunnel*.

Sélectionnez les listes de proposition IKE et IPsec.

Pour Authentication (Authentification), sélectionnez l'objet clé pré-partagée défini dans l'étape (1) ci-dessus.

L'objet tunnel IPsec peut être traité exactement comme tout autre objet *d'interface* de NetDefendOS dans les prochaines étapes.

Paramétrez deux règles IP dans l'ensemble de règles IP pour ce tunnel.

Une règle Allow pour le trafic sortant avec pour interface de destination l'objet *ipsec_tunnel* défini précédemment. Le réseau de destination de la règle est le réseau distant *remote_net*.

Une règle Allow pour le trafic entrant avec pour *interface source* l'objet *ipsec_tunnel* défini précédemment. Le réseau source est *remote_net*.

Action	**Interface source**	**Réseau source**	**Interface de destination**	**Réseau de destination**	**Service**
Allow (Autoriser)	lan	lannet	ipsec_tunnel	remote_net	All (Tous)
Allow (Autoriser)	ipsec_tunnel	remote_net	lan	lannet	All (Tous)

Le service utilisé pour ces règles est *All* (Tous), mais il peut s'agir d'un autre service prédéfini.

6. Définissez une nouvelle route NetDefendOS qui spécifie que le tunnel VPN *ipsec_tunnel* est l'interface à utiliser pour le routage des paquets en direction du réseau distant à l'autre extrémité du tunnel.

Interface	**Réseau**	**Passerelle**
ipsec_tunnel	remote_net	

Clients itinérants IPsec avec clés pré-partagées

Cette section détaille le paramétrage avec des clients itinérants qui se connectent via un tunnel IPsec avec des clés

pré-partagées. Voici deux types de clients itinérants :

A. L’adresse IP des clients est connue au préalable.

B. L’adresse IP des clients n'est pas connue au préalable et doit être repérée par NetDefendOS lors de leur connexion.

A. Adresses IP déjà attribuées. Les adresses IP peuvent être connues au préalable et pré-attribuées aux clients itinérants avant qu’ils ne se connectent. L'adresse IP des clients est intégrée manuellement dans le logiciel du client VPN.

Paramétrez l’authentification utilisateur. L’authentification utilisateur XAuth n’est pas requise avec les clients itinérants IPsec, mais elle est recommandée (cette étape peut être ignorée pour simplifier le paramétrage). La source de l’authentification peut être :

Un objet base de données utilisateur locale, qui est interne à NetDefendOS.

Un serveur d’authentification externe.

Une base de données utilisateur interne est plus facile à configurer, nous en utiliserons une pour cet exemple. Changer pour un serveur externe est plus simple à faire par la suite.

Afin de mettre en pratique l’authentification utilisateur avec une base de données interne :

Définissez un objet base de données utilisateur locale (nous appellerons cet objet *TrustedUsers*).

Ajoutez des utilisateurs à *TrustedUsers*. L’objet doit contenir au moins une combinaison nom d'utilisateur/mot de passe.

La chaîne de groupe d’un utilisateur peut être spécifiée si l’accès au groupe en question doit être restreint à certains réseaux source. Le groupe peut être spécifié (avec la même chaîne textuelle) dans la section d'authentification d'un objet IP. Si cet objet IP est utilisé comme le réseau source d’une règle dans l’ensemble de règles IP, alors cette règle s’appliquera seulement à un utilisateur si sa chaîne de groupe correspond à la chaîne de groupe de l’objet IP. (Remarque : le groupe n’a aucune signification dans les règles d’authentification).

Créez une nouvelle règle d’authentification utilisateur avec l’Authentication Source (Source de l’authentification) défini sur *TrustedUsers*. Les autres paramètres de la règle sont :

Agent	**Source de l’authentification**	**Réseau source**	**Interface**	**IP source client**
XAUTH	Local	all-nets (tout réseau)	any (toutes)	all-nets (0.0.0.0/0)

2. L’objet tunnel IP *ipsec_tunnel* doit avoir les paramètres suivants :

Définissez Local Network (Réseau local) sur *lannet*.

Définissez Remote Network (Réseau distant) sur *all-nets* (tout réseau).

Définissez Remote Gateway (Passerelle distante) sur *all-nets* (tout réseau).

Définissez Encapsulation mode (Mode d’encapsulation) sur *Tunnel*.

Sélectionnez les listes de proposition IKE et IPsec pour correspondre aux capacités des clients.

Aucune route ne peut être prédéfinie : l'option Dynamically add route to the remote network when tunnel established (Ajouter une route dynamiquement à un réseau distant lorsqu'un tunnel est établi) doit donc être activée pour l’objet tunnel.

Activez l’option Require IKE XAuth user authentication (Demander l’authentification utilisateur XAuth IKE) pour les tunnels IPsec entrants. Ceci permet de rechercher la première règle XAuth correspondante dans les règles d'authentification.

3. L'ensemble de règles IP doit contenir une seule règle :

Action	Interface source	Réseau source	Interface de destination	Réseau de destination	Service
Allow (Autoriser)	ipsec_tunnel	all-nets (tout réseau)	lan	lannet	All (Tous)

Une fois qu'une règle Allow permet le paramétrage de la connexion, le trafic bidirectionnel est autorisé. C'est pour cela qu'une seule règle est nécessaire ici. Au lieu d'utiliser *all-nets* (tout réseau) comme ci-dessus, vous pouvez utiliser un objet IP défini et plus sûr, qui spécifie la plage exacte des adresses IP pré-attribuées.

B. Adresses IP repérées par NetDefendOS. Si les adresses IP des clients ne sont pas connues, alors elles doivent être repérées par NetDefendOS. Pour cela, les paramètres ci-dessus doivent être modifiés comme suit :

Si une plage d'adresses IP spécifique doit être utilisée comme pool des adresses disponibles :

Créez un objet pool mode de configuration (un seul objet de ce genre peut être associé à une installation NetDefendOS) et spécifiez sa plage d'adresses.

Activez l'option IKE Config Mode (Mode de configuration IKE) dans l'objet tunnel IPsec *ipsec_tunnel*.

Si les adresses IP des clients doivent être repérées par un DHCP :

Créez un objet pool IP et spécifiez le serveur DHCP à utiliser. Le serveur DHCP peut être spécifié comme une simple adresse IP ou comme étant accessible sur une interface spécifique. Si un serveur DHCP interne doit être utilisé, spécifiez l'adresse de bouclage *127.0.0.1* comme adresse IP du serveur HDCP.

Créez un objet pool mode de configuration (un seul objet de ce genre peut être associé à une installation NetDefendOS) et associez-lui l'objet pool IP défini dans l'étape précédente.

Activez l'option IKE Config Mode (Mode de configuration IKE) dans l'objet tunnel IPsec *ipsec_tunnel*.

Configuration du client IPsec. Dans les cas (A) et (B), le client IPsec doit être configuré avec l'URL du firewall D-Link, ainsi qu'avec la clé pré-partagée.

Clients itinérants IPsec avec certificats

Si des certificats sont utilisés avec des clients itinérants IPsec plutôt que des clés pré-partagées, alors l'objet clé pré-partagée n'est pas nécessaire. La procédure est la même que celle décrite ci-dessus, avec les différences suivantes :

Chargez un *Gateway Certificate* (Certificat de passerelle) et un *Root Certificate* (Certificat du nœud) dans NetDefendOS.

Lors du paramétrage de l'objet tunnel IPsec, spécifiez les certificats à utiliser dans Authentication (Authentification). Pour cela, procédez comme suit :

Activez l'option X.509 Certificate (Certificat X 509).

Sélectionnez le certificat de passerelle.

Ajoutez le certificat de nœud à utiliser.

Le logiciel du client IPsec devra être configuré de manière appropriée avec les certificats et les adresses IP distantes.

L'étape du paramétrage de l'authentification utilisateur est facultative puisqu'il ne s'agit que d'une sécurité supplémentaire qui vient s'ajouter à celle des certificats.

Clients itinérants L2TP avec clés pré-partagées

À cause du client L2TP intégré dans Microsoft Windows, le choix du L2TP est privilégié dans les scénarios de clients itinérants VPN. Le L2TP est habituellement encapsulé dans l'IPsec afin que lors du chiffrage, l'IPsec s'exécute en *transport mode* (mode transport) plutôt qu'en *tunnel mode* (mode tunnel). Voici les étapes du paramétrage L2TP avec IPsec :

Créez un objet IP (nous l'appellerons *l2tp_pool*) qui définit la plage d'adresses IP disponibles pour les clients. La plage choisie peut être de deux types :

Une plage du réseau interne, sur lequel les clients vont se connecter. Si la plage du réseau interne est 192.168.0.0/24, alors la plage d'adresses à utiliser serait 192.168.0.10 - 192.168.0.20. Le danger ici est qu'une adresse IP peut être accidentellement utilisée sur le réseau interne et distribuée à un client.

Utilisez une nouvelle plage d'adresses, totalement différente de celle d'un réseau interne. Cette solution permet d'éviter qu'une adresse de la plage soit aussi utilisée dans le réseau interne.

Définissez deux autres objets IP :

ip_ext, qui est l'adresse IP publique externe par laquelle les clients se connectent (supposons qu'il s'agit de l'interface *ext*).

ip_int qui est l'adresse IP interne de l'interface à laquelle le réseau interne est connecté (appelons cette interface *int*).

Définissez une clé pré-partagée pour le tunnel IPsec.

Définissez un objet *tunnel IPsec* (nous appellerons cet objet *ipsec_tunnel*) avec les paramètres suivants :

Définissez Locat Network (Réseau local) sur *ip_ext* (ou sur *all-nets* si NetDefendOS est derrière la fonctionnalité de traduction d'adresses réseau).

Définissez Remote Network (Réseau distant) sur *all-nets* (tout réseau).

Définissez Remote Gateway (Passerelle distante) sur *none*.

Pour Authentication (Authentification), sélectionnez l'objet clé pré-partagée défini lors de la première étape.

Définissez Encapsulation Mode (Mode d'encapsulation) sur *Transport*.

Sélectionnez les listes de proposition IKE et IPsec à utiliser.

Activez l'option de routage Dynamically add route to the remote network when tunnel established (Ajouter une route dynamiquement à un réseau distant lorsqu'un tunnel est établi).

Définissez un objet serveur PPTP/L2TP (nous l'appellerons *l2tp_tunnel*) avec les paramètres suivants :

Définissez Inner IP Address (Adresse IP interne) sur *ip_int*.

Définissez Tunnel Protocol (Protocole du tunnel) sur *L2TP*.

Définissez Outer Interface Filter (Filtre de l'interface extérieure) sur *ipsec_tunnel*.

Définissez Outer Server IP (IP du serveur extérieur) sur *ip_ext*.

Sélectionnez Microsoft Point-to-Point Encryption allowed (Autorisation du chiffrage point à point Microsoft). Puisque le chiffrage IPsec est en fonction, cette option peut être définie sur *None*, car le double chiffrage pourrait affecter le débit.

Définissez IP Pool (Pool IP) sur *l2tp_pool*.

Activez le proxy ARP sur l'interface *int* à laquelle le réseau interne est connecté.

Associez l'interface à une table de routage particulière afin que les routes soient automatiquement ajoutées à cette table. Normalement, c'est la table *main* qui est sélectionnée.

Pour l’authentification utilisateur :

Définissez un objet base de données utilisateur locale (nous appellerons cet objet *TrustedUsers*).

Ajoutez des utilisateurs à *TrustedUsers*. L’objet doit contenir au moins une combinaison nom d'utilisateur/mot de passe.

La chaîne de groupe d’un utilisateur peut aussi être spécifiée. Les étapes sont les mêmes que celles décrites dans la section précédente *Clients itinérants IPsec*.

Définissez une règle d’authentification utilisateur :

Agent	**Source de l’authentification**	**Réseau source**	**Interface**	**IP source client**
PPP	Local	all-nets (tout réseau)	l2tp_tunnel	all-nets (0.0.0.0/0)

7. Pour permettre le trafic dans le tunnel L2TP, les règles suivantes doivent être définies dans l'ensemble de règles IP :

Action	**Interface source**	**Réseau source**	**Interface de destination**	**Réseau de destination**	**Service**
Allow (Autoriser)	l2tp_tunnel	l2tp_pool	any (toutes)	int_net	All (Tous)
NAT	ipsec_tunnel	l2tp_pool	ext	all-nets (tout réseau)	All (Tous)

La deuxième règle est incluse pour permettre aux clients de naviguer sur Internet via l'interface *ext* du firewall D-Link. Le client se voit attribuer une adresse IP interne privée, qui peut subir une traduction NAT si les connexions vont vers l'Internet public via le firewall D-Link.

8. Paramétrez le client. En supposant que le système d’exploitation soit Windows XP, l’option Create new connection (Créer une nouvelle connexion) dans Network Connections (Connexions réseau) doit être sélectionnée pour exécuter l'assistant Nouvelle connexion. L’information la plus importante à saisir dans cet assistant est l’URL résolvable du firewall D-Link ou bien son adresse IP *ip_ext*.

   Allez ensuite dans Network > Properties (Réseau > Propriétés). Dans la boîte de dialogue qui apparaît, choisissez le tunnel L2TP et sélectionnez Properties (Propriétés). Dans la nouvelle boîte de dialogue, sélectionnez l’onglet Networking (Réseau) et choisissez Force to L2TP (Forcer vers L2TP). Revenez aux propriétés du tunnel L2TP, sélectionnez l’onglet Security (Sécurité) et cliquez sur le bouton IPsec Settings (Paramètres IPsec). Saisissez la clé pré-partagée.

Clients itinérants L2TP avec certificats

Si des certificats sont utilisés avec les clients itinérants L2TP plutôt que des clés pré-partagées, alors la procédure est la même que celle décrite ci-dessus, avec les différences suivantes :

Chargez un *Gateway Certificate* (Certificat de passerelle) et un *Root Certificate* (Certificat de nœud) dans NetDefendOS.

Lors du paramétrage de l’objet tunnel IPsec, spécifiez les certificats à utiliser dans Authentication (Authentification). Pour cela, procédez comme suit :

Activez l’option X.509 Certificate (Certificat X 509).

Sélectionnez le certificat de passerelle.

Ajoutez le certificat de nœud à utiliser.

Si vous utilisez le client L2TP de Windows XP, les certificats appropriés doivent être importés dans Windows avant de paramétrer la connexion avec l’assistant Nouvelle connexion.

L’étape du paramétrage de l'authentification utilisateur est facultative puisqu'il ne s'agit que d'une sécurité supplémentaire qui vient s’ajouter à celle des certificats.

Clients itinérants PPTP

Le PPTP est plus simple à paramétrer que le L2TP puisqu'à la place de l'IPsec il utilise sa propre méthode de chiffrage, qui est moins puissante.

Un deuxième inconvénient majeur de cette solution est l’impossibilité de faire la traduction NAT des connexions PPTP par un tunnel. Plusieurs clients peuvent donc utiliser une seule connexion jusqu'au firewall D-Link. Si la traduction NAT est tout de même activée, seul le premier client qui tentera de se connecter y parviendra.

Voici les étapes du paramétrage PPTP :

Dans Hosts & Networks (Hôtes et réseaux), définissez les objets IP suivants :

Un objet IP *pptp_pool*, qui représente la plage des adresses IP internes attribuées par un réseau interne.

Un objet *int_net*, qui représente le réseau interne depuis lequel les adresses arrivent.

Un objet *ip_int*, qui représente l’adresse IP interne de l’interface connectée au réseau interne (supposons que cette interface est *int*).

Un objet *ip_ext*, qui représente l'adresse IP publique externe à laquelle les clients se connectent (supposons qu'il s’agit de l’interface *ext*).

Définissez un objet PPTP/L2TP (nous l’appellerons *pptp_tunnel*) avec les paramètres suivants :

Définissez Inner IP Address (Adresse IP interne) sur *ip_net*.

Définissez Tunnel Protocol (Protocole du tunnel) sur *PPTP*.

Définissez Outer Interface Filter (Filtre de l’interface extérieure) sur *ext*.

Définissez Outer Server IP (IP du serveur extérieur) sur *ip_ext*.

Pour le chiffrage point à point de Microsoft, il est recommandé de désactiver toutes les options à l’exception du chiffrage en *128 bits*.

Définissez IP Pool (Pool IP) sur *pptp_pool*.

Activez le proxy ARP sur l’interface *int*.

Comme pour le L2TP, autorisez l’insertion automatique de nouvelles routes dans la table de routage principale *main*.

Définissez une règle d’authentification utilisateur, qui est presque identique à celle du L2TP :

Agent	**Source de l’authentification**	**Réseau source**	**Interface**	**IP source client**
PPP	Local	all-nets (tout réseau)	pptp_tunnel	all-nets (0.0.0.0/0)

4. Paramétrez les règles IP dans l’ensemble de règles IP :

Action	**Interface source**	**Réseau source**	**Interface de destination**	**Réseau de destination**	**Service**
Allow (Autoriser)	pptp_tunnel	pptp_pool	any (toutes)	int_net	All (Tous)
NAT	pptp_tunnel	pptp_pool	ext	all-nets (tout réseau)	All (Tous)

Comme pour le L2TP, la règle NAT permet au client d’accéder à l’Internet public via le firewall D-Link.

5. Paramétrez le client. Pour Windows XP, la procédure à suivre est exactement la même que celle du L2TP décrite ci-dessus, à l'exception qu'il ne faut pas saisir de clé pré-partagée.

Dépannage VPN

Dépannage général

Dans tous les types de VPN, des vérifications basiques de dépannage sont effectuées.

Vérifiez que toutes les adresses IP ont été correctement spécifiées.

Vérifiez que toutes les clés pré-partagées et les noms d'utilisateur et mots de passe ont été correctement saisis.

Si vous avez opté pour des certificats, vérifiez que ceux que vous utilisez sont corrects et qu'ils n'ont pas expiré.

Utilisez le *Ping* ICMP pour vous assurer du bon fonctionnement du tunnel. Avec des clients itinérants, il vaut mieux faire un ping depuis le client jusqu'aux adresses IP de l'interface du réseau local via le firewall D-Link (dans des structures LAN-LAN, le ping peut être effectué dans n'importe quelle direction). Si NetDefendOS peut répondre à un ping, alors la règle qui suit doit figurer dans l'ensemble de règles IP :

Action	**Interface source**	**Réseau source**	**Interface de destination**	**Réseau de destination**	**Service**
Allow (Autoriser)	vpn_tunnel	all-nets (tout réseau)	core (noyau)	all-nets (tout réseau)	ICMP

Assurez-vous qu'aucune définition de tunnel IPsec n'empêchera d'atteindre la bonne définition. La liste des tunnels est passée en revue de haut en bas. Si un tunnel avec le réseau distant défini sur *all-nets* (tout réseau) et la passerelle distante définie sur *none* (aucun) est placé avant notre tunnel, il peut empêcher d'atteindre le bon tunnel. Ce problème génère souvent un message *Incorrect Pre-shared Key* (Clé pré-partagée incorrecte).

Essayez d'éviter la duplication des adresses IP entre le réseau distant accessible par un client et le réseau interne auquel un client itinérant appartient.

Si un client itinérant fait temporairement partie d'un réseau tel qu'un réseau Wi-Fi dans un aéroport, le client obtiendra une adresse IP de la part du serveur DHCP du réseau Wi-Fi. Si cette IP appartient aussi au réseau situé derrière le firewall D-Link accessible via un tunnel, alors Windows continuera de supposer que l'adresse IP est disponible sur le réseau local du client. Windows n'acheminera donc pas correctement les paquets en direction du réseau à distance via le tunnel, mais les acheminera vers le réseau local.

La solution à ce problème de duplication de l'adresse IP locale/distante est de créer une nouvelle route dans la table de routage Windows du client, qui route directement l'adresse IP vers le tunnel.

Si l'authentification des clients itinérants ne demande pas de nom d'utilisateur ni de mot de passe, assurez-vous que les paramètres avancés suivants sont activés :

IPsecBeforeRules pour les clients itinérants IPsec.

PPP_L2TPBeforeRules pour les clients itinérants L2TP.

PPP_PPTPBeforeRules pour les clients itinérants PPTP.

Ces paramètres doivent être activés par défaut puisqu'ils garantissent que le trafic d'authentification utilisateur entre NetDefendOS et le client puisse contourner l'ensemble de règles IP. Si les paramètres appropriés ne sont pas activés, une règle explicite doit être ajoutée dans l'ensemble de règles IP pour permettre au trafic d'authentification de circuler entre les clients itinérants et NetDefendOS. L'interface de destination de cette règle devra être le noyau.

Dépannage des tunnels IPsec

De nombreuses commandes peuvent être utilisées pour diagnostiquer les tunnels IPsec.

La commande console *ipsecstat*. Elle peut être utilisée pour voir si les tunnels IPsec ont été correctement établis. Voici un exemple représentatif :

```
> ipsecstat

--- IPsec SAs:

Displaying one line per SA-bundle

IPsec Tunnel Local Net   Remote Net  Remote GW
------------ ------------- ------------  -------------
L2TP_IPSec  214.237.225.43 84.13.193.179 84.13.193.179
IPsec_Tun1  192.168.0.0/24 172.16.1.0/24 82.242.91.203
```

Pour examiner la première phase de négociation IKE du paramétrage du tunnel, utilisez :

```
> ipsecstat -ike
```

Pour obtenir les détails complets du paramétrage du tunnel, utilisez :

```
> ipsecstat -u -v
```

La commande console *ikesnoop*. Un problème récurrent avec le paramétrage IPsec réside dans le fait que la liste de proposition ne soit pas acceptable pour le périphérique qui se trouve à l'autre extrémité du tunnel. La commande *ikesnoop* peut révéler les problèmes liés à la liste de proposition en détaillant les négociations qui ont eu lieu.

```
ikesnoop verbose
```

Une fois que cette commande a été saisie, un *ping* ICMP peut donc être envoyé vers le firewall D-Link depuis l'autre extrémité du tunnel. Cette manipulation obligera *ikesnoop verbose* à sortir les détails des paramètres du tunnel. Les incompatibilités dans les listes de proposition IKE et/ou IPsec peuvent souvent être sources de problèmes, qui sont donc révélés par cette sortie.

S'il y a plusieurs tunnels dans un paramétrage ou plusieurs clients dans un seul tunnel, la sortie de *ikesnoop verbose* peut être accablante. Il est donc préférable de spécifier que cette sortie provient d'un seul tunnel en indiquant l'adresse IP du client.

```
ikesnoop verbose <ip-address>
```

Échec de l'interface de gestion avec VPN

Si un tunnel VPN est paramétré et que l'interface de gestion n'est plus opérationnelle, il s'agit alors sûrement d'un problème avec le trafic de gestion qui est routé vers le tunnel VPN au lieu de l'interface qui convient.

Ce problème survient lorsqu'une route établie dans la table de routage principale route l'ensemble du trafic tout réseau via le tunnel VPN. Si le tunnel VPN n'atteint pas l'interface de gestion, alors l'administrateur doit créer une route spécifique qui route le trafic de l'interface de gestion qui sort du firewall D-Link vers le sous-réseau de gestion.

Lorsqu'un tunnel VPN est défini, une route tout réseau est automatiquement définie dans la table de routage. L'administrateur doit donc toujours paramétrer une route spécifique pour que le trafic de l'interface de gestion soit toujours routé correctement.

IPsec

Présentation

L'IPsec (*Internet Protocole Security*) est un ensemble de protocoles définis par l'IETF (Internet Egineering Task Force) pour garantir la sécurité IP au niveau des réseaux. Un VPN basé sur l'IPsec est composé de deux parties :

Le protocole d'échange de clés par Internet (IKE).

Les protocoles IPsec (AH/ESP/les deux).

La première partie, l'IKE, est la phase de négociation initiale, durant laquelle les deux extrémités du tunnel VPN

s’accordent sur les méthodes à utiliser pour assurer la sécurité du trafic IP sous-jacent. De plus, l’IKE est utilisé pour gérer les connexions : il définit un ensemble d’Associations de sécurité (SA) pour chaque connexion. Les associations de sécurité sont unidirectionnelles ; il y en a donc généralement au moins deux par connexion IPsec.

La deuxième partie est le transfert des données IP en cours, pendant lequel les méthodes de chiffrage et d'authentification convenues lors des négociations IKE sont appliquées. Ceci peut être effectué de nombreuses manières : en utilisant les protocoles IPsec ESP ou AH ou bien une combinaison des deux.

Le déroulement des événements peut être décrit brièvement comme suit :

L’IKE négocie la manière dont il doit être protégé.

L’IKE négocie la manière dont l’IPsec doit être protégé.

L’IPsec déplace les données dans le VPN.

Les sections suivantes décrivent chacune de ces étapes en détail.

Protocole d’échange de clés par Internet (IKE)

Cette section décrit l’IKE, le protocole d’échange de clés par Internet, ainsi que ses paramètres d’utilisation.

Le chiffrage et l’authentification des données sont des méthodes plutôt directes. Elles ne nécessitent que des algorithmes de chiffrage et d'authentification, ainsi que leurs clés associées. Le protocole IKE est vu comme une manière de distribuer ces « clés de session », ainsi que comme un terrain d’entente sur la protection des données entre les extrémités du tunnel VPN.

L’IKE a trois tâches principales :

Il aide chaque extrémité à s’authentifier entre elles.

Il établit des nouvelles connexions IPsec (et crée des paires SA).

Il gère les connexions existantes.

L’IKE garde une trace des connexions en attribuant un ensemble d’associations de sécurité à chacune d'elles. Une SA décrit tous les paramètres associés à une connexion particulière, tels que l’utilisation du protocole IPsec (ESP/AH/les deux), ainsi que les clés de session utilisées pour chiffrer/déchiffrer et/ou authentifier/vérifier les données transmises. Une SA est par nature unidirectionnelle, d’où la nécessité de plusieurs SA par connexion. Dans la plupart des cas où l'ESP ou l'AH est utilisé, deux SA seront créées pour chaque connexion : une qui décrit le trafic entrant et l'autre le trafic sortant. Dans les cas où l’ESP et l’AH sont utilisés conjointement, quatre SA sont créées.

Négociation IKE. La procédure de négociation des paramètres de session consiste en plusieurs phases et modes. Ceux-ci sont décrits en détail dans les sections suivantes.

Le déroulement des événements peut être résumé comme suit :

IKE Phase 1

: Négociation de la façon de protéger l’IKE.

IKE Phase 2

: Négociation de la façon de protéger l’IPsec.

  Extraction de nouvelles clés lors de l’échange de clés de la phase 1, afin de fournir les clés de session à utiliser lors du chiffrage et de l’authentification du flux de données VPN.

Durées de vie de l’IKE et de l’IPsec. Les connexions IKE et IPsec ont des durées de vie limitées, toutes deux exprimées en temps (secondes) et en données (kilo-octets). Ces durées de vie empêchent une connexion d’être utilisée trop longtemps, ce qui est préférable d’un point de vue crypto-analytique.

La durée de vie de l'IPsec doit être plus courte que celle de l'IKE. La différence entre les deux doit être d'au moins 5 minutes. Ceci permet à la connexion IPsec de ré-obtenir des clés en exécutant simplement une nouvelle négociation de la phase 2. Il est inutile d'exécuter à nouveau la négociation de la phase 1 tant que la durée de vie de l'IKE n'a pas expiré.

Propositions IKE. Une proposition IKE est une suggestion sur la manière de protéger les données. L'unité VPN émettrice qui initialise une connexion IPsec envoie une liste de propositions qui suggère différentes méthodes pour protéger la connexion.

La connexion qui est négociée peut être soit une connexion IPsec qui protège le flux de données au travers du VPN, soit une connexion IKE qui protège la négociation IKE elle-même.

Après avoir reçu la liste de propositions, l'unité VPN réceptrice déterminera la proposition la plus convenable selon ses propres règles de sécurité et répondra en spécifiant son choix.

Si aucune proposition acceptable n'est trouvée, l'unité VPN répondra qu'aucune proposition ne peut être acceptée, en indiquant si possible la raison.

Les propositions contiennent toutes les paramètres nécessaires tels que les algorithmes utilisés pour le chiffrage et l'authentification des données, ou d'autres paramètres comme décrits dans la section Paramètres IKE.

IKE Phase 1 : négociation de la sécurité IKE. Une négociation IKE est effectuée en deux étapes. La première phase authentifie les deux firewalls VPN ou clients VPN l'un par rapport à l'autre, en confirmant l'adéquation de la clé pré-partagée de l'unité distante.

Cependant puisque nous ne voulons pas que la négociation soit entièrement en texte clair, il faut d'abord protéger le reste de la négociation IKE. Pour cela, l'initiateur doit envoyer une liste de propositions au récepteur. Une fois que la liste a été envoyée et que le récepteur a accepté une des propositions, il faut procéder à l'étape d'authentification pour s'assurer de l'exacte identité des deux extrémités du tunnel VPN. La technique *d'échange de clés Diffie Hellman* est utilisée pour initialiser la création d'un secret partagé entre les deux parties lors de la négociation et l'extraction de clés pour le chiffrage.

L'authentification peut être opérée grâce à des clés pré-partagées, des certificats ou un chiffrage par clé publique. La méthode des clés pré-partagées est la plus courante de nos jours. La fonction PSK et les certificats sont pris en charge par le module VPN de NetDefendOS.

IKE Phase 2 : négociation de la sécurité IPsec. Dans la phase deux, une autre négociation est effectuée, détaillant les paramètres de la connexion IPsec.

Dans la phase 2, nous allons également extraire de nouvelles clés de l'échange de clés Diffie-Hellman de la phase 1, afin de fournir des clés de session à utiliser pour protéger le flux de données VPN.

Si le protocole PFS (Perfect Forwarding Secrecy) est utilisé, un nouvel échange Diffie-Hellman est effectué pour chaque négociation de la phase 2. Bien que cette méthode soit plus lente, elle assure qu'aucune clé ne dépende d'autres clés utilisées précédemment ; aucune clé n'est extraite des mêmes clés d'origine. Il s'agit de veiller à ce que, dans le cas improbable où une clé serait altérée, aucune clé suivante ne puisse être extraite.

Une fois la négociation de la phase 2 terminée, la connexion VPN est établie et prête à l'emploi.

Paramètres IKE. Un certain nombre de paramètres sont utilisés dans le processus de négociation.

Vous trouverez ci-dessous un résumé des paramètres de configuration nécessaires à l'établissement d'une connexion VPN. Il est vivement recommandé de comprendre l'action de ces paramètres avant toute tentative de configuration des extrémités VPN, étant donné qu'il est très important que les deux extrémités soient en mesure de s'accorder sur tous ces paramètres.

Lors de l'installation de deux firewalls D-Link en extrémités VPN, ce processus est réduit à la comparaison des champs dans deux boîtes de dialogue identiques. Cependant, cette opération n'est pas si facile lorsque l'équipement provient de fournisseurs différents.

Identification des extrémités	L'*ID local* est une donnée qui représente l'identité de la passerelle VPN. Avec les clés pré-partagées, il s'agit d'une donnée unique qui identifie uniquement l'extrémité du tunnel.

	L’authentification à l’aide des clés pré-partagées est basée sur l’algorithme Diffie-Hellman.
Réseaux/hôtes locaux et distants	Il s’agit des sous-réseaux ou des hôtes entre lesquels le trafic IP sera protégé par le VPN. Dans le cadre d’une connexion LAN-LAN, il s’agira des adresses réseau des LAN respectifs. En cas d’utilisation de clients itinérants, le réseau distant sera le plus probablement défini à *tout réseau*, ce qui signifie que le client itinérant peut se connecter de n’importe où.
Mode tunnel/transport	IPsec peut être utilisé en deux modes, tunnel ou transport. Le mode Tunnel indique que le trafic sera acheminé par un tunnel vers un périphérique distant, qui déchiffrera/authentifiera les données, les extraira de leur tunnel et les transmettra à leur destination finale. Ainsi, un indiscret verra uniquement le trafic chiffré allant d'une extrémité VPN à une autre. En mode Transport, le trafic ne sera pas acheminé par un tunnel et ne s’applique donc pas aux tunnels VPN. Il peut être utilisé pour sécuriser une connexion d'un client VPN directement au firewall D-Link, par exemple pour une configuration à distance protégée par IPsec. Ce paramètre sera en général défini sur « tunnel » dans la plupart des configurations.
Passerelle distante	La passerelle distante effectuera le déchiffrement/l’authentification et transmettra les données à leur destination finale. Ce champ peut également être défini sur « none », ce qui force le VPN D-Link à traiter l’adresse distante comme passerelle distante. Ceci est particulièrement utile en cas d'accès itinérant où les adresses IP des clients VPN distants ne sont pas connues à l’avance. Une configuration sur « none » permettra à quiconque provenant d’une adresse IP conforme à l’adresse « réseau distante » susmentionnée d’ouvrir une connexion VPN, à condition qu’il s’authentifie correctement. La passerelle distante n’est pas utilisée en mode Transport.
Mode Main/Aggressive	La négociation IKE compte deux modes de fonctionnement, le mode Main et le mode Aggressive. La différence entre les deux est la suivante : le mode Aggressive transmettra plus d’informations en paquets moins nombreux, ce qui présente l'avantage d'établir une connexion légèrement plus rapidement, à condition de transmettre les identités des firewalls de sécurité en clair. En mode Aggressive, certains paramètres de configuration, comme par exemple les groupes Diffie-Hellman et PFS, ne peuvent pas être négociés, ce qui rend d’autant plus important d'avoir des configurations « compatibles » aux deux extrémités.
Protocoles IPsec	Les protocoles IPsec décrivent la façon dont les données seront traitées. Les deux protocoles sont AH (Authentication Header) et ESP (Encapsulating Security Payload). Le protocole ESP offre le chiffrement, l’authentification ou les deux. Cependant, nous ne recommandons pas d'utiliser uniquement le chiffrement, car cela réduira considérablement la sécurité. Vous trouverez plus d'informations sur le protocole ESP dans ESP (Encapsulating Security Payload).

Le protocole AH offre uniquement l'authentification. La différence par rapport au protocole ESP (authentification uniquement) est que le protocole AH authentifie également des parties de l'en-tête IP externe, par exemple les adresses source et destination, en s'assurant que le paquet provient réellement de l'en-tête IP prétendue.

Vous trouverez plus d'informations sur le protocole AH dans AH (Authentification Header).

Remarque
Les firewalls D-Link ne prennent pas en charge le protocole AH.

Chiffrement IKE

Précise l'algorithme de chiffrement utilisé dans la négociation IKE et, en fonction de l'algorithme, la taille de la clé de chiffrement utilisée.

Les algorithmes pris en charge par l'IPsec NetDefendOS sont les suivants :

- AES
- Blowfish
- Twofish
- Cast128
- 3DES
- DES

DES est fourni uniquement pour pouvoir interagir avec d'autres développements de VPN antérieurs. L'utilisation de DES doit être évitée autant que possible, car c'est un algorithme ancien dont la sécurité n'est plus garantie.

Authentification IKE

Précise les algorithmes d'authentification utilisés dans la phase de négociation IKE.

Les algorithmes pris en charge par l'IPsec NetDefendOS sont les suivants :

- SHA1
- MD5

Groupe IKE DH (Diffie-Hellman)

Précise le groupe Diffie-Hellman à utiliser lors des échanges de clés dans IKE.

Les groupes Diffie-Hellman pris en charge par NetDefendOS sont les suivants :

- Groupe DH 1 (768 bits)
- Groupe DH 2 (1024 bits)
- Groupe DH 5 (1536 bits)

La sécurité des échanges de clés est renforcée car le bit du groupe DH prend de l'importance, tout comme le temps consacré aux échanges.

Durée de vie de l'IKE

Il s'agit de la durée de vie de la connexion IKE.

Elle est exprimée en temps (secondes) ainsi qu'en volume de données (kilooctets). À l'expiration de l'une des deux données, un nouvel échange de phase 1 sera effectué. Si aucune donnée n'a été transmise lors de la

dernière « incarnation » de la connexion IKE, aucune nouvelle connexion ne sera effectuée avant que quelqu'un souhaite utiliser à nouveau la connexion VPN. Cette valeur doit être supérieure à la durée de vie SA IPsec.

PFS

Lorsque le PFS est désactivé, des clés d'origine sont « créées » lors de l'échange de clés de la phase 1 de la négociation IKE. Dans la phase 2 de la négociation IKE, les clés de session de chiffrement et d'authentification seront extraites de ces clés d'origine. En utilisant PFS (Perfect Forwarding Secrecy), des clés totalement nouvelles seront toujours créées à la ré-obtention. Si une clé était altérée, aucune autre clé ne pourrait être extraite à l'aide de ces informations.

PFS peut être utilisé en deux modes : le premier mode est PFS sur les clés, dans lequel un nouvel échange de clés aura lieu lors de chaque négociation de phase 2. Le deuxième mode est PFS sur les identités, dans lequel les identités sont également protégées en supprimant l'association de sécurité de phase 1 à chaque fois qu'une négociation de phase 2 est terminée, en veillant à ce qu'une seule négociation de phase 2 soit chiffrée en utilisant la même clé.

PFS n'est en général pas nécessaire, car il est très improbable que des clés de chiffrement ou d'authentification soient altérées.

Groupe PFS

Précise le groupe PFS à utiliser avec PFS.

Les groupes PFS pris en charge par NetDefendOS sont les suivants :

1 modp 768 bits

2 modp 1 024 bits

5 modp 1 536 bits

La sécurité est renforcée au fur et à mesure que les bits de groupe PFS prennent de l'importance, tout comme le temps consacré aux échanges.

Groupe DH IPsec

Il s'agit d'un groupe Diffie-Hellman très similaire à celui de l'IKE. Cependant, celui-ci est utilisé uniquement pour PFS.

Chiffrement IPsec

Algorithme de chiffrement à utiliser sur le trafic protégé.

Ceci n'est pas nécessaire lorsqu'on utilise le protocole AH ou lorsque le protocole ESP est utilisé sans chiffrement.

Les algorithmes pris en charge par les VPN du firewall D-Link sont les suivants :

AES

Blowfish

Twofish

Cast128

3DES

DES

Authentification IPsec

Précise l'algorithme d'authentification utilisé sur le trafic protégé.

Cette fonction n'est pas utilisée lorsque le protocole ESP est utilisé sans

	authentification, bien qu'il ne soit pas recommandé d'utiliser le protocole ESP de cette manière. Les algorithmes pris en charge par les VPN du firewall D-Link sont les suivants : SHA1 MD5
Durée de vie de l'IPsec	Il s'agit de la durée de vie de la connexion VPN. Elle est exprimée à la fois en temps (secondes) et en volume de données (kilo-octets). Lorsque l'une de ces valeurs est dépassée, une nouvelle obtention de clé sera lancée, fournissant de nouvelles clés de session de chiffrement et d'authentification IPsec. Si la connexion VPN n'a pas été utilisée lors de la dernière période d'obtention de nouvelle clé, la connexion sera interrompue, puis réouverte depuis le début lorsqu'elle sera à nouveau nécessaire. Cette valeur doit être inférieure à la durée de vie de l'IKE.

Authentification IKE

Mode manuel. La façon « la plus simple » de configurer un VPN consiste à utiliser une méthode appelée « mode manuel ». Dans cette méthode, IKE n'est pas du tout utilisé ; les clés de chiffrement et d'authentification ainsi que certains autres paramètres sont directement configurés des deux côtés du tunnel VPN.

Remarque

Les firewalls D-Link ne prennent pas en charge le mode manuel.

Avantages du mode manuel. Étant donné qu'il est très direct, il garantit une bonne interopérabilité. La plupart des problèmes d'interopérabilité rencontrés aujourd'hui concernent l'IKE. Le mode manuel contourne totalement IKE et définit son propre ensemble d'associations de sécurité IPsec.

Inconvénients du mode manuel. C'est une méthode ancienne, qui était utilisée avant l'arrivée d'IKE. Il lui manque donc toutes les fonctionnalités d'IKE. Par conséquent, cette méthode comporte un certain nombre de limites, comme par exemple l'obligation de toujours utiliser la même clé de chiffrement/d'authentification ou l'absence de services anti-relecture et n'est pas très souple. Il n'y a aucun moyen non plus de s'assurer que l'hôte/le firewall distant est réellement celui qu'il prétend être.

Ce type de connexion est également vulnérable aux « attaques de relecture », autrement dit une entité malveillante qui a accès au trafic chiffré peut enregistrer certains paquets et les envoyer vers sa destination ultérieurement. L'extrémité VPN de destination ne pourra pas indiquer si ce paquet est une « relecture » ou pas. L'utilisation d'IKE élimine cette vulnérabilité.

PSK. L'utilisation d'une clé pré-partagée (PSK) est une méthode dans laquelle les extrémités du VPN « partagent » une clé secrète. Il s'agit d'un service fourni par IKE, avec tous les avantages qui y sont associés, ce qui le rend beaucoup plus souple que le mode manuel.

Avantages du mode PSK. Le mode à clés pré-partagées (Pre-Shared Keying) présente de nombreux avantages par rapport au mode manuel, notamment l'authentification des extrémités, qui définit réellement l'utilité des PSK. Il comprend également tous les avantages de l'utilisation d'IKE. Au lieu d'utiliser un ensemble fixe de clés de chiffrement, des clés de session seront utilisées pendant une période limitée, là où un nouvel ensemble de clés de session est utilisé.

Inconvénients du mode PSK. La distribution des clés est un élément à prendre en compte lors de l'utilisation des clés pré-partagées. Comment les clés pré-partagées sont-elles distribuées aux clients et firewalls VPN distants ? Il s'agit d'une question centrale, car la sécurité d'un système PSK est basée sur le caractère secret des PSK. Si une clé pré-partagée était altérée, la configuration devrait être modifiée pour utiliser une nouvelle clé pré-partagée.

Certificats. Chaque firewall de VPN a son propre certificat, ainsi qu'un ou plusieurs certificats de nœud agréés.

L'authentification est basée sur plusieurs éléments :

Le fait que chaque extrémité possède la clé privée correspondant à la clé publique trouvée dans son certificat et que personne d'autre n'a accès à la clé privée.

Le fait que le certificat a été signé par une personne à qui la passerelle distante fait confiance.

Avantages des certificats. Plus de souplesse. De nombreux clients VPN, par exemple, peuvent être gérés sans avoir la même clé pré-partagée configurée sur la totalité des clients, ce qui est souvent le cas lorsqu'on utilise des clés pré-partagées et des clients itinérants. Au lieu de cela, si un client était altéré, le certificat du client pourrait simplement être révoqué. Il est inutile de reconfigurer chaque client.

Inconvénients des certificats. Plus de complexité. L'authentification basée sur les certificats peut être utilisée dans le cadre d'une infrastructure de clé publique plus importante, rendant tous les clients VPN et les firewalls dépendants des tiers. En d'autres termes, il y a davantage d'éléments à configurer et donc plus de possibilités d'erreur.

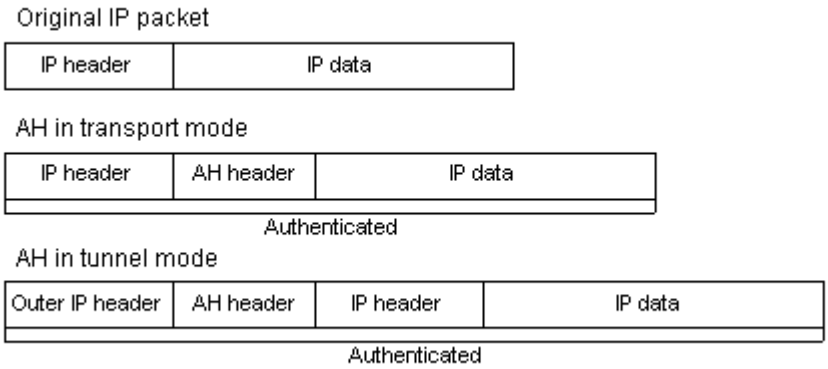
Protocoles IPsec (ESP/AH)

Les protocoles IPsec sont les protocoles utilisés pour protéger le trafic réel transmis par le VPN. Les protocoles réels utilisés et les clés utilisées avec ces protocoles sont négociés par IKE.

Deux protocoles sont associés à IPsec : AH et ESP. Ils sont abordés dans les sections ci-dessous.

AH (Authentication Header). AH est un protocole utilisé pour authentifier un flux de données.

Figure 9.1. Le protocole AH



Le protocole AH utilise une fonction de hachage chiffré pour produire une adresse MAC à partir des données du paquet IP. Cette adresse MAC est alors transmise avec le paquet, ce qui permet à la passerelle distante de vérifier l'intégrité du paquet IP d'origine en vérifiant que les données n'ont pas été falsifiées lors de leur parcours sur Internet. En plus des données du paquet IP, le protocole AH authentifie également des parties de l'en-tête IP.

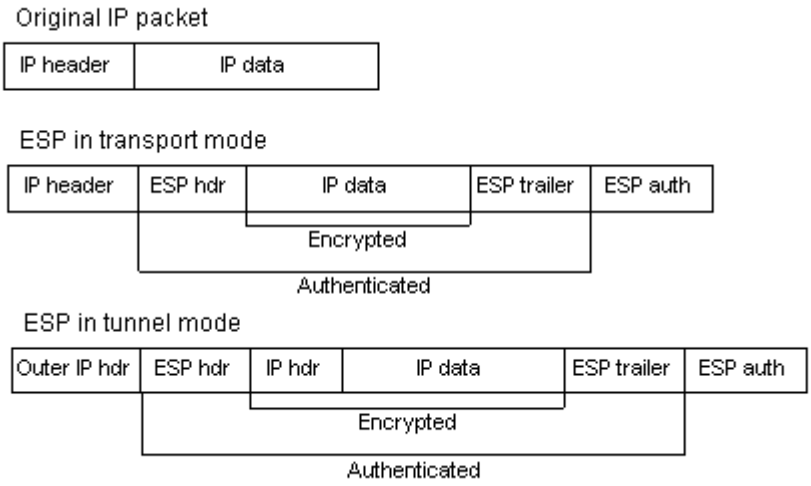
Le protocole AH insère un en-tête AH à la suite de l'en-tête IP d'origine et, en mode Tunnel, l'en-tête AH est inséré à la suite de l'en-tête externe, mais avant l'en-tête IP interne d'origine.

ESP (Encapsulating Security Payload). Le protocole ESP insère un en-tête ESP à la suite de l'en-tête IP d'origine et, en mode Tunnel, l'en-tête ESP est inséré à la suite de l'en-tête externe, mais avant l'en-tête IP interne d'origine.

Toutes les données à la suite de l'en-tête ESP sont chiffrées et/ou authentifiées. La différence par rapport au protocole AH est que le protocole ESP fournit également le chiffrement du paquet IP. La phase d'authentification diffère également par le fait que le protocole ESP authentifie uniquement les données à la suite de l'en-tête ESP ; l'en-tête IP externe n'est donc pas protégé.

Le protocole ESP est utilisé pour le chiffrement et l'authentification du paquet IP. Il peut également être utilisé pour effectuer uniquement le chiffrement ou l'authentification.

Figure 9.2. Le protocole ESP



Franchissement NAT

Les protocoles IKE et IPsec présentent tous deux un problème de fonctionnement du NAT. Les deux protocoles n'ont pas été conçus pour fonctionner via des NAT et par conséquent, une technique appelée « Franchissement NAT » a vu le jour. Le franchissement NAT est un supplément aux protocoles IKE et IPsec qui leur permet de fonctionner alors qu'ils subissent le NAT. NetDefendOS prend en charge la norme RFC3947 pour le franchissement NAT avec IKE.

Le franchissement NAT se divise en deux parties :

Les ajouts à IKE qui permettent aux pairs IPsec de s'indiquer qu'ils prennent en charge le franchissement NAT et les versions spécifiques prises en charge. NetDefendOS prend en charge la norme RFC3947 pour le franchissement NAT avec IKE.

Modifications à l'encapsulation ESP. Lorsque le franchissement NAT est utilisé, le protocole ESP est encapsulé en UDP, ce qui garantit une traduction NAT plus souple.

Voici une description plus détaillée des modifications apportées aux protocoles IKE et IPsec.

Le franchissement est utilisé uniquement si les deux extrémités le prennent en charge. Ainsi, les VPN qui ont connaissance du franchissement NAT envoient un « ID fournisseur » spécial, indiquant à l'autre extrémité qu'il comprend le franchissement NAT et indiquant les versions spécifiques qu'il prend en charge.

Détection NAT : les deux pairs IPsec envoient des hachages de leurs propres adresses IP ainsi que le port UDP source utilisé dans les négociations IKE. Ces informations sont utilisées pour voir si l'adresse IP et le port source que chaque pair utilise sont identiques à ce que l'autre pair voit. Si l'adresse et le port source n'ont pas changé, cela signifie que le trafic n'a pas été traité par NAT et que le franchissement NAT n'est pas nécessaire. Si l'adresse et/ou le port source a changé, le trafic a été traité par NAT et le franchissement NAT est utilisé.

Une fois que les pairs IPsec ont décidé que le franchissement NAT était nécessaire, la négociation IKE passe du port UDP 500 au port 4500. Ceci est nécessaire car certains périphériques NAT traitent un paquet UDP sur le port 500 différemment des autres paquets UDP afin de résoudre les problèmes de NAT avec IKE. Le problème est que cette gestion particulière des paquets IKE peut en réalité rompre les négociations IKE, c'est pourquoi le port UDP utilisé par IKE a changé.

Un autre problème résolu par le franchissement NAT est le fait que le protocole ESP est un protocole IP. Il n'y a pas d'information de port comme pour TCP et UDP, ce qui rend impossible le fait d'avoir plusieurs clients traités par NAT connectés à la même passerelle distante en même temps. Ainsi, les paquets ESP sont encapsulés dans UDP. Le trafic ESP-UDP est envoyé sur le port 4500, le même port que IKE lors de l'utilisation du franchissement NAT. Une fois le port modifié, toutes les communications IKE suivantes sont effectuées via le port 4500. Des paquets Keepalive (entretien) sont également envoyés régulièrement pour entretenir le mappage NAT.

Configuration du franchissement NAT. La plupart des fonctions du franchissement NAT sont totalement automatiques et aucune configuration particulière n'est nécessaire dans le firewall émetteur. Cependant, deux éléments doivent être notés concernant les firewalls de réponse :

Sur les firewalls de réponse, le champ Passerelle distante est utilisé comme filtre sur l'IP source des paquets IKE reçus. Celui-ci devrait être paramétré pour autoriser l'adresse IP traitée par NAT de l'émetteur.

Lors de l'utilisation de clés pré-partagées individuelles avec plusieurs tunnels se connectant à un firewall distant, puis traitées par NAT via la même adresse, il est important de veiller à ce que l'*ID local* soit propre à chaque tunnel. L'ID local peut être

Automatique – l'ID local est pris comme l'adresse IP de l'interface sortante. Il s'agit du paramètre recommandé à moins que, dans un cas improbable, les deux firewalls aient la même adresse IP externe.

IP – une adresse IP peut être saisie manuellement

DNS – une adresse DNS peut être saisie manuellement

E-mail – une adresse électronique peut être saisie manuellement

Listes de propositions

Pour s'accorder sur des paramètres de connexion VPN, un processus de négociation est lancé. Suite aux négociations, des associations de sécurité (SA) IKE et IPsec sont établies. Comme son nom l'indique, une proposition est le point de départ de la négociation. Une proposition définit les paramètres de chiffrement, par exemple l'algorithme de chiffrement, les durées de vie, etc. que le firewall du VPN prend en charge.

Il existe deux types de propositions, les propositions IKE et IPsec. Les propositions IKE sont utilisées lors de la phase 1 de l'IKE (négociation de la sécurité IKE), alors que les propositions IPsec sont utilisées lors de la phase 2 de l'IKE (négociation de la sécurité IPsec).

Une liste de propositions est utilisée pour regrouper plusieurs propositions. Lors du processus de négociation, les propositions de la liste sont offertes au firewall du VPN distant l'une après l'autre jusqu'à trouver une correspondance. Plusieurs listes de propositions peuvent être définies dans NetDefendOS pour différents scénarios de VPN. Deux listes de propositions IKE et deux listes de propositions IPsec sont définies par défaut dans NetDefendOS.

Les listes de propositions de clients itinérants IKE et ESP-TN conviennent aux tunnels VPN qui sont utilisés pour les clients VPN itinérants. Ces listes de propositions sont compatibles avec les listes de propositions par défaut du client VPN D-Link.

Comme leur nom l'indique, le LAN-LAN IKE et le LAN-LAN ESP-TN conviennent aux solutions VPN LAN-LAN. Ces listes de propositions sont adaptées à l'inclusion de propositions basées sur AES et 3DES uniquement.

Exemple 9.1. Utilisation d'une liste de propositions

Cet exemple montre comment créer et utiliser une liste de propositions IPsec à utiliser dans le tunnel VPN. Il proposera les algorithmes de chiffrement 3DES et DES. Les fonctions de hachage SHA1 et MD5 seront utilisées afin de vérifier si le paquet de données est altéré lors de sa transmission. Notez que cet exemple n'illustre pas comment ajouter l'objet de tunnel IPsec spécifique. Ceci sera également utilisé dans un exemple ultérieur.

Interface de ligne de commande
Créez d'abord une liste d'algorithmes IPsec :

```
gw-world:/> add IPsecAlgorithms esp-l2tptunnel DESEnabled=Yes DES3Enabled=Yes
   SHA1Enabled=Yes MD5Enabled=Yes
```

Puis appliquez la liste de propositions au tunnel IPsec :

```
gw-world:/> set Interface IPsecTunnel MyIPsecTunnel IPsecAlgorithms=esp-l2tptunnel
```

Interface Web

Créez d'abord une liste d'algorithmes IPsec :

Sélectionnez Objects > VPN Objects > IKE Algorithms > Add > IPsec Algorithms (Objets > Objets VPN > Algorithmes IKE > Ajouter > Algorithmes IPsec).

Nommez la liste, par ex., esp-l2tptunnel.

Vérifiez maintenant ce qui suit :

DES

3DES

SHA1

MD5

Cliquez sur OK.

Puis appliquez la liste de propositions au tunnel IPsec :

Sélectionnez Interfaces > IPsec

Dans la liste de contrôle, cliquez sur le tunnel IPsec cible.

Sélectionnez le tunnel esp-12tp récemment créé dans le contrôle des algorithmes IPsec.

Cliquez sur OK.

Clés pré-partagées

Les clés pré-partagées sont utilisées pour authentifier les tunnels VPN. Les clés sont des secrets qui sont partagés par les parties communicantes avant que la communication n'ait lieu. Pour communiquer, les deux parties doivent prouver qu'elles connaissent le secret. La sécurité d'un secret partagé dépend de la « valeur » d'une phrase de passe. Les phrases de passe qui sont des mots courants sont par exemple extrêmement vulnérables aux attaques de dictionnaire.

Les clés pré-partagées peuvent être automatiquement générées par l'interface utilisateur Web, mais également par l'interface de ligne de commande à l'aide de la commande *pskgen* (cette commande est détaillée dans le Guide de référence de l'interface de ligne de commande).

Exemple 9.2. Utilisation d'une clé pré-partagée

Cet exemple montre comment créer une clé pré-partagée et comment l'appliquer à un tunnel VPN. Étant donné que les mots et expressions ordinaires sont vulnérables aux attaques de dictionnaire, il ne faut pas les utiliser comme secrets. Ici, la clé pré-partagée est une clé hexadécimale générée de façon aléatoire. Notez que cet exemple n'illustre pas comment ajouter l'objet de tunnel IPsec spécifique.

Interface de ligne de commande
Créez d'abord une clé pré-partagée. Pour générer la clé automatiquement avec une clé 64 bits (valeur par défaut), utilisez :

```
gw-world:/> pskgen MyPSK
```

Pour obtenir une clé plus longue (donc plus sécurisée) de 512 bits, la commande serait :

```
gw-world:/> pskgen MyPSK -size=512
```

Pour ajouter la clé pré-partagée manuellement, utilisez :

```
gw-world:/> add PSK MyPSK Type=HEX PSKHex=<enter the key here>
```

Appliquez maintenant la clé pré-partagée au tunnel IPsec :

```
gw-world:/> set Interface IPsecTunnel MyIPsecTunnel PSK=MyPSK
```

Interface Web

Créez d'abord une clé pré-partagée :

Sélectionnez Objects > Authentication Objects > Add > Pre-shared key (Objets > Objets d'authentification > Ajouter > Clé pré-partagée).

Nommez la clé pré-partagée, par ex., *MyPSK*.

Sélectionnez Hexadecimal Key (Clé hexadécimale) et cliquez sur Generate Random Key (Générer une clé aléatoire) pour générer une clé dans la zone de texte de la phrase de passe.

Cliquez sur OK.

Appliquez ensuite la clé pré-partagée au tunnel IPsec :

Sélectionnez Interfaces > IPsec

Dans la commande de la liste, cliquez sur l'objet tunnel IPsec cible.

Sous l'onglet Authentication (Authentification), sélectionnez Pre-shared Key (Clé pré-partagée) et sélectionnez MyPSK.

Cliquez sur OK.

Listes d'identification

Lorsque les certificats X.509 sont utilisés comme méthode d'authentification des tunnels IPsec, le firewall D-Link accepte tous les firewalls ou clients VPN distants qui sont en mesure de présenter un certificat signé par l'une des autorités de certification autorisées. Ceci peut poser problème, en particulier lors de l'utilisation de clients itinérants.

Imaginez des employés en déplacement à qui l'on donne accès aux réseaux internes de l'entreprise et qui utilisent des clients VPN. L'organisation administre sa propre autorité de certification et les certificats ont été remis aux employés. Différents groupes d'employés sont susceptibles d'avoir accès à différentes parties des réseaux internes. Par exemple, des membres de l'équipe de vente ont besoin d'accéder à des serveurs qui exécutent le système de commande, alors que des ingénieurs techniques ont besoin d'accéder à des bases de données techniques.

Étant donné que les adresses IP des clients VPN des employés en déplacement ne peuvent pas être connues à l'avance, les connexions VPN entrantes des clients ne peuvent pas être différenciées. Ceci signifie que le firewall n'est pas en mesure de contrôler l'accès à différentes parties des réseaux internes.

Le concept de Listes d'identification représente une solution à ce problème. Une liste d'identification contient une ou plusieurs identités (ID), où chaque identité correspond au champ objet d'un certificat X.509. Les listes d'identification peuvent donc être utilisées pour réguler les certificats X.509 qui sont accordés pour accéder à des tunnels IPsec.

Exemple 9.3. Utilisation d'une liste d'identification

Cet exemple montre comment créer et utiliser une liste d'identification à utiliser dans le tunnel VPN. Cette liste d'identification contiendra une ID avec le DN de type, le nom distinctif, comme identifiant principal. Notez que cet exemple n'illustre pas comment ajouter l'objet de tunnel IPsec spécifique.

Interface de ligne de commande
Créez d'abord une liste d'identification :

```
gw-world:/> add IDList MyIDList
```

Puis créez une ID :

```
gw-world:/> cc IDList MyIDList

gw-world:/MyIDList> add ID JohnDoe Type=DistinguishedName
   CommonName="John Doe" OrganizationName=D-Link
```

```
   OrganizationalUnit=Support Country=Sweden
   EmailAddress=john.doe@D-Link.com

gw-world:/MyIDList> cc
```

Enfin, appliquez la liste d'identification au tunnel IPsec :

```
gw-world:/> set Interface IPsecTunnel MyIPsecTunnel AuthMethod=Certificate
   IDList=MyIDList RootCertificates=AdminCert GatewayCertificate=AdminCert
```

Interface Web
Créez d'abord une liste d'identification :

Sélectionnez Objects > VPN Objects > ID List > Add > ID List (Objets > Objets VPN > Liste ID > Ajouter > Liste ID).

Nommez la liste d'identification, par ex., *MyIDList*.

Cliquez sur OK.

Puis créez une ID :

Sélectionnez Objects > VPN Objects > ID List (Objets > Objets VPN > Liste ID).

Dans la liste de contrôle, cliquez sur MyIDList.

Nommez l'ID, par ex., *MonsieurX*.

Sélectionnez Distinguished name (nom distinctif) dans la commande Type.

Saisissez :

Common Name (Nom usuel) : Monsieur X

Organization Name (Nom de l'organisation) : D-Link

Organizational Unit (Unité organisationnelle) : Support

Country (Pays) : Suède

Email address (Adresse électronique) : monsieur.X@D-Link.com

Cliquez sur OK.

Enfin, appliquez la liste d'identification au tunnel IPsec :

Sélectionnez Interfaces > IPsec.

Dans la liste de contrôle, cliquez sur l'objet tunnel IPsec concerné.

Sous l'onglet Authentication, sélectionnez X.509 Certificate (Certificat X.509).

Sélectionnez le certificat approprié dans les commandes Root Certificate(s) (Certificat de nœud) et Gateway Certificate (Certificat de passerelle).

Sélectionnez MyIDList dans la liste d'identification.

Cliquez sur OK.

Tunnels IPsec

Présentation

Un tunnel IPsec définit une extrémité d'un tunnel chiffré. Chaque tunnel IPsec est interprété comme interface logique par NetDefendOS, avec les mêmes capacités de filtrage, de mise en forme du trafic et de configuration que

des interfaces ordinaires.

Lorsqu'un autre firewall D-Link ou client VPN D-Link (ou tout produit conforme à IPsec) tente d'établir un tunnel VPN IPsec vers le firewall D-Link, les tunnels IPsec configurés sont évalués. Si une définition de tunnel IPsec correspondante est trouvée, les négociations IKE et IPsec ont alors lieu, entraînant l'établissement d'un tunnel VPN IPsec.

Notez qu'un tunnel IPsec établi ne signifie *pas* automatiquement que tout le trafic de ce tunnel IPsec est autorisé. Au contraire, le trafic réseau qui a été déchiffré sera transféré vers l'ensemble de règles pour une évaluation supplémentaire. Le tunnel IPsec associé portera le nom de l'interface source du trafic réseau déchiffré. De plus, une règle d'acheminement ou d'accès, dans le cas d'un client itinérant, doit être définie pour que NetDefendOS accepte certaines adresses IP source en provenance du tunnel IPsec.

Pour le trafic réseau allant dans le sens opposé, c'est-à-dire allant dans un tunnel IPsec, un processus inverse se produit. D'abord, le trafic non chiffré est évalué par l'ensemble de règles. En cas de correspondance d'une règle et d'une route, NetDefendOS tente de trouver un tunnel IPsec établi qui répond aux critères. Dans le cas contraire, NetDefendOS tentera d'établir un tunnel vers le firewall distant indiqué par la définition du tunnel IPsec correspondante.

Remarque

Le trafic IKE et ESP/AH est envoyé vers le moteur IPsec avant la consultation de l'ensemble de règles. Le trafic chiffré vers le firewall n'a par conséquent pas besoin d'être autorisé dans l'ensemble de règles. Ce comportement peut être modifié dans la section Paramètres avancés IPsec.

Tunnels LAN-LAN avec clés pré-partagées

Un VPN peut autoriser des réseaux locaux (LAN) distribués géographiquement à communiquer de façon sécurisée sur l'Internet public. Dans le cadre d'une entreprise, ceci signifie que les LAN sur des sites géographiques distincts peuvent communiquer avec un niveau de sécurité comparable à celui qui existe dans le cadre d'un lien privé dédié.

La communication sécurisée est possible grâce à l'utilisation de la tunnelisation IPsec, le tunnel se prolongeant à partir de la passerelle VPN d'un site vers la passerelle VPN d'un autre site. Le firewall D-Link est par conséquent le vecteur de mise en place du VPN, tout en appliquant une surveillance de sécurité normale du trafic passant par le tunnel. Cette section détaille la configuration des tunnels Lan-Lan créés avec une clé pré-partagée (PSK).

Un certain nombre d'étapes sont nécessaires pour configurer les tunnels LAN-LAN avec une clé pré-partagée :

Configurez une clé pré-partagée ou un secret pour le tunnel VPN.

Configurez les propriétés du tunnel VPN.

Configurez la route.

Configurez les règles (un tunnel à 2 voies requiert 2 règles).

Clients itinérants

Un employé en déplacement qui doit accéder à un serveur d'entreprise central à partir d'un ordinateur portable depuis divers sites est un exemple typique de client itinérant. À l'exception du besoin d'accès VPN sécurisé, l'autre problème majeur des clients itinérants est que l'adresse IP de l'utilisateur mobile est souvent inconnue à l'avance. Pour gérer l'adresse IP inconnue, le NetDefendOS peut ajouter de façon dynamique des routes à la table de routage au fur et à mesure que des tunnels sont établis.

Gestion des adresses IP inconnues. Si l'adresse IP du client n'est pas connue à l'avance, le firewall D-Link doit donc créer une route dans sa table de routage de façon dynamique au fur et à mesure que les clients se connectent. C'est le cas dans l'exemple ci-dessous et le tunnel IPsec est configuré pour ajouter des routes de façon dynamique.

Si les clients doivent être autorisés à se connecter en itinérance de n'importe où, quel que soit leur adresse IP, le réseau distant doit être paramétré sur « tout réseau » (adresse IP : 0.0.0.0/0), ce qui permettra à toutes les adresses IPv4 existantes de se connecter via le tunnel.

Lors de la configuration de tunnels VPN pour les clients itinérants, il n'est généralement pas nécessaire d'ajouter ou de modifier les listes de propositions qui sont préconfigurées dans NetDefendOS.

Tunnels de clients basés sur PSK

Exemple 9.4. Configuration d’un tunnel VPN basé sur une clé pré-partagée pour les clients itinérants

Cet exemple décrit comment configurer un tunnel IPsec au niveau du firewall D-Link du siège social pour les clients itinérants qui se connectent au siège pour obtenir un accès à distance. Le réseau du siège social utilise la plage réseau 10.0.1.0/24 avec IP de firewall externe wan_ip.

Interface Web

A. Créez une clé pré-partagée pour l’authentification IPsec :

Sélectionnez Objects > Authentication Objects > Add > Pre-Shared Key (Objets > Objets d’authentification > Ajouter > Clé pré-partagée).

Saisissez :

Name (Nom) : nommez la clé pré-partagée, SecretKey par exemple.

Shared Secret (Secret partagé) : entrez une phrase de passe secrète.

Confirm Secret (Confirmer le secret) : entrez à nouveau la phrase de passe secrète.

Cliquez sur OK.

B. Configurez le tunnel IPsec :

Sélectionnez Interfaces > IPsec > Add > IPsec Tunnel (Interfaces > IPsec > Ajouter > Tunnel IPsec).

Saisissez :

Name (Nom) : RoamingIPsecTunnel

Réseau local : 10.0.1.0/24 (il s’agit du réseau local auquel les utilisateurs itinérants se connecteront)

Remote Network (réseau distant) : all-nets (tout réseau)

Extrémité distante : (aucune)

Encapsulation Mode (mode d’encapsulation) : Tunnel

Pour les algorithmes, saisissez :

Algorithmes IKE : moyen ou élevé

Algorithmes IPsec : moyen ou élevé

Pour l’authentification, saisissez :

Clé pré-partagée : Sélectionnez la clé pré-partagée créée auparavant.

Sous l’onglet Routing (routage) :

Activez l’option : Dynamically add route to the remote network when a tunnel is established. (Ajouter un routage de façon dynamique au réseau distant lorsqu'un tunnel est établi.)

Cliquez sur OK.

C. Enfin, configurez l’ensemble de règles IP pour autoriser le trafic à l’intérieur du tunnel.

Tunnels de clients basés sur un certificat autosigné

Exemple 9.5. Configuration d’un tunnel VPN basé sur un certificat autosigné pour les clients itinérants

Cet exemple décrit comment configurer un tunnel IPsec au niveau du firewall D-Link du siège social pour les clients itinérants qui se connectent au siège pour obtenir un accès à distance. Le réseau du siège social utilise la plage réseau 10.0.1.0/24 avec IP de firewall externe wan_ip.

Interface Web

A. Créez un certificat autosigné pour l’authentification IPsec :

L'étape de création réelle de certificats autosignés est réalisée en dehors de l'interface utilisateur Web à l'aide d'un logiciel adapté. Le certificat doit être au format de fichier PEM (Privacy Enhanced Mail).

B. Chargez tous les certificats autosignés de client :

Sélectionnez Objects > Authentication Objects > Add > Certificate (Objets > Objets d’authentification > Ajouter > Certificat).

Entrez un nom convenable pour l’objet Certificat.

Sélectionnez l’option Certificat X.509.

Cliquez sur OK.

C. Créez des listes d’identification :

Sélectionnez Objects > VPN Objects > ID List > Add > ID List (Objets > Objets VPN > Liste ID > Ajouter > Liste ID).

Entrez un nom convenable, par ex., *vente.*

Cliquez sur OK.

Sélectionnez Objects > VPN Objects > ID List > Sales > Add > ID List (Objets > Objets VPN > Liste ID > Ventes > Ajouter > Liste ID).

Entrez le nom du client.

Sélectionnez le type Email.

Dans le champ Adresse électronique, entrez l’adresse électronique sélectionnée lors de la création du certificat sur le client.

Créez une nouvelle ID pour chaque client à qui vous voulez accorder des droits d’accès selon les instructions ci-dessus.

D. Configurez le tunnel IPsec :

Sélectionnez Interfaces > IPsec > Add > IPsec Tunnel (Interfaces > IPsec > Ajouter > Tunnel IPsec).

Saisissez :

Name (Nom) : RoamingIPsecTunnel

Réseau local : 10.0.1.0/24 (il s’agit du réseau local auquel les utilisateurs itinérants se connecteront)

Remote Network (réseau distant) : all-nets (tout réseau)

Extrémité distante : (aucune)

Encapsulation Mode (mode d’encapsulation) : Tunnel

Pour les algorithmes, saisissez :

Algorithmes IKE : moyen ou élevé

Algorithmes IPsec : moyen ou élevé

Pour l’authentification, saisissez :

Sélectionnez Certificat X.509 comme méthode d’authentification.

Root Certificate(s) (Certificats de nœud) : sélectionnez tous vos certificats de clients et ajoutez-les à la liste Selected (Sélection).

Gateway Certificate (Certificat de passerelle) : sélectionnez votre certificat de firewall nouvellement créé.

Liste d’identification : Sélectionnez la Liste d’ID que vous voulez associer à votre tunnel VPN. Dans votre cas, il s’agira des ventes (sales).

Sous l’onglet Routing (routage) :

Activez l’option : Dynamically add route to the remote network when a tunnel is established. (Ajouter un routage de façon dynamique au réseau distant lorsqu'un tunnel est établi.)

Cliquez sur OK.

E. Enfin, configurez l’ensemble de règles IP pour autoriser le trafic à l’intérieur du tunnel.

Tunnels de clients basés sur des certificats émis par le serveur AC

La configuration des tunnels de client à l’aide d’un certificat X.509 émis par une autorité de certification est très similaire à l’utilisation de certificats autosignés, à l'exception de quelques étapes. Très important : il incombe à l'administrateur d'acquérir le certificat approprié auprès d'une autorité émettrice. Avec certains systèmes, comme par exemple Windows 2000 Server, il existe un accès intégré à un serveur AC (dans Windows 2000 Server, celui-ci se trouve dans les Services de certificat). Pour en savoir plus sur les certificats émis par un serveur AC, consultez la section intitulée « Certificats X.509 ».

Il incombe à l'administrateur d'acquérir le certificat approprié auprès d'une autorité émettrice pour les tunnels de clients. Avec certains systèmes, comme par exemple Windows 2000 Server, il existe un accès intégré à un serveur AC (dans Windows 2000 Server, celui-ci se trouve dans les Services de certificat). Pour en savoir plus sur les certificats émis par un serveur AC, consultez la section intitulée « Certificats X.509 ».

Exemple 9.6. Configuration d’un tunnel VPN basé sur un certificat émis par un serveur AC pour les clients itinérants

Cet exemple décrit comment configurer un tunnel IPsec au niveau du firewall D-Link du siège social pour les clients itinérants qui se connectent au siège pour obtenir un accès à distance. Le réseau du siège social utilise la plage réseau 10.0.1.0/24 avec IP de firewall externe wan_ip.

Interface Web

A. Chargez tous les certificats de clients :

Sélectionnez Objects > Authentication Objects > Add > Certificate (Objets > Objets d’authentification > Ajouter > Certificat).

Entrez un nom convenable pour l’objet Certificat.

Sélectionnez l’option Certificat X.509.

Cliquez sur OK.

B. Créez des listes d’identification :

Sélectionnez Objects > VPN Objects > ID List > Add > ID List (Objets > Objets VPN > Liste ID > Ajouter > Liste ID).

Entrez un nom descriptif, par ex., *ventes.*

Cliquez sur OK.

Sélectionnez Objects > VPN Objects > ID List > Sales > Add > ID List (Objets > Objets VPN > Liste ID > Vente > Ajouter > Liste ID).

Entrez le nom du client.

Sélectionnez le type Email.

Dans le champ Adresse électronique, entrez l’adresse électronique sélectionnée lors de la création du certificat sur le client.

Créez une nouvelle ID pour chaque client à qui vous voulez accorder des droits d’accès selon les instructions ci-dessus.

C. Configurez le tunnel IPsec :

Sélectionnez Interfaces > IPsec > Add > IPsec Tunnel (Interfaces IPsec > Ajouter > Tunnel IPsec).

Saisissez :

Name (Nom) : RoamingIPsecTunnel

Réseau local : 10.0.1.0/24 (il s’agit du réseau local auquel les utilisateurs itinérants se connecteront)

Remote Network (réseau distant) : all-nets (tout réseau)

Extrémité distante : (aucune)

Encapsulation Mode (mode d’encapsulation) : Tunnel

Pour les algorithmes, saisissez :

Algorithmes IKE : moyen ou élevé

Algorithmes IPsec : moyen ou élevé

Pour l’authentification, saisissez :

Sélectionnez Certificat X.509 comme méthode d’authentification.

Root Certificate(s) (Certificats de nœud) : Sélectionnez votre certificat de nœud du serveur AC importé précédemment et ajoutez-le à la liste Selected (Sélection).

Gateway Certificate (Certificat de passerelle) : Sélectionnez votre certificat de firewall nouvellement créé.

Liste d’identification : Sélectionnez la Liste d’ID que vous voulez associer à votre tunnel VPN. Dans votre cas, il s’agira des ventes (sales)

Sous l’onglet Routing (routage) :

Activez l’option : Dynamically add route to the remote network when a tunnel is established (Ajouter un routage de façon dynamique au réseau distant lorsqu'un tunnel est établi).

Cliquez sur OK.

D. Enfin, configurez l’ensemble de règles IP pour autoriser le trafic à l’intérieur du tunnel.

Utilisation du mode de configuration

IKE Configuration Mode (Mode de configuration) est une extension à IKE qui permet à NetDefendOS de fournir des informations de configuration de LAN à des clients VPN distants. Ce mode est utilisé pour configurer de façon dynamique les clients IPsec avec des adresses IP et des masques réseau correspondants et pour échanger d'autres types d'informations associés à DHCP. L'adresse IP fournie à un client peut soit être basée sur une plage d'adresses IP statiques prédéfinies définie pour le mode de configuration, soit provenir de serveurs DHCP associés à un objet *IP Pool*.

Un groupe IP est un cache d'adresses IP collectées à partir de serveurs DHCP et les attributions sur ces adresses sont renouvelées automatiquement lorsque la durée d'attribution arrive à expiration. Les groupes IP gèrent également des informations supplémentaires, comme par exemple DNS et WINS/NBNS, à la manière d'un serveur DHCP ordinaire. Pour en savoir plus sur les groupes, consultez la section intitulée « Groupes IP »).

Définition de l'objet Mode de configuration. Actuellement, un seul objet Config Mode (mode de configuration) peut être défini dans NetDefendOS et celui-ci est appelé l'objet *Config Mode Pool*. Les paramètres clés qui y sont associés sont les suivants :

Utiliser l'objet Groupe IP prédéfini	L'objet Groupe IP qui fournit les adresses IP.
Utiliser un groupe statique	Un ensemble statique d'adresses IP peut être défini comme alternative à l'utilisation d'un groupe IP.
DNS	L'adresse IP du DNS utilisé pour la résolution URL (déjà fournie par un groupe IP).
NBNS/WINS	L'adresse IP pour la résolution NBNS/WINS (déjà fournie par un groupe IP).
DHCP	Indique à l'hôte d'envoyer n'importe quelle requête DHCP interne à cette adresse.
Sous-réseaux	Une liste des sous-réseaux auxquels le client a accès.

Exemple 9.7. Configuration du mode de configuration

Dans cet exemple, l'objet Config Mode Pool (groupe de mode de configuration) est activé en l'associant à un objet Groupe IP déjà configuré appelé *ip_pool1*.

Interface Web

Sélectionnez Objects > VPN Objects > IKE Config Mode Pool (Objets > Objets VPN > Groupe de mode de configuration IKE).

La page Web des propriétés de l'objet Config Mode Pool (groupe de mode de configuration) s'affiche.

Sélectionnez Use a pre-defined IPPool object (Utiliser un objet Groupe IP prédéfini).

Sélectionnez l'objet *ip_pool1* dans la liste déroulante IP Pool (Groupe IP).

Cliquez sur OK.

Après avoir défini l'objet Config Mode (mode de configuration), il suffit d'activer le mode de configuration à utiliser avec le tunnel IPsec.

Exemple 9.8. Utilisation du mode de configuration avec des tunnels IPsec

En supposant l'existence d'un tunnel prédéfini appelé *vpn_tunnel1*, cet exemple montre comment activer le mode de configuration pour ce tunnel.

Interface Web

Sélectionnez Interfaces > IPsec.

Sélectionnez le tunnel *vpn_tunnel1* à modifier.

Sélectionnez la liste déroulante IKE Config Mode (mode de configuration IKE).

Cliquez sur OK.

Validation d'IP. NetDefendOS vérifie toujours si l'adresse IP source de chaque paquet à l'intérieur d'un tunnel IPsec est la même que l'adresse IP attribuée au client IPsec avec le mode de configuration IKE. Dans le cas d'une non-concordance, le paquet est toujours ignoré et un message de consignation est généré avec un niveau de gravité Avertissement. Ce message comprend les deux adresses IP ainsi que l'identité du client.

Il est possible de supprimer automatiquement l'association de sécurité concernée en cas d'échec de validation en activant le paramètre avancé IPsecDeleteSAOnIPValidationFailure. La valeur par défaut pour ce paramètre est *Disabled (Désactivé)*.

Recherche de CRL depuis un serveur LDAP alternatif

Un certificat de nœud X.509 comprend en général l'adresse IP ou le nom d'hôte de l'autorité de certification à contacter lorsque des certificats ou des listes de révocation de certificats doivent être téléchargées sur le firewall D-Link. Le protocole LDAP (Lightweight Directory Access Protocol) est utilisé pour ces téléchargements.

Cependant, il arrive que ces informations manquent ou que l'administrateur souhaite utiliser un autre serveur LDAP. La section de configuration du serveur LDAP peut alors être utilisée pour spécifier manuellement d'autres serveurs LDAP.

Exemple 9.9. Configuration d'un serveur LDAP

Cet exemple montre comment configurer et spécifier manuellement un serveur LDAP.

Interface de ligne de commande

```
gw-world:/> add LDAPServer Host=192.168.101.146 Username=myusername
   Password=mypassword Port=389
```

Interface Web

Sélectionnez Objects > VPN Objects > LDAP > Add > LDAP Server (Objets > Objets VPN > LDAP > Ajouter > Serveur LDAP).

Saisissez :

IP Address (Adresse IP) : 192.168.101.146

Username (Nom d'utilisateur) : monnomdutilisateur

Password (mot de passe) : monmotdepasse

Confirm Password (confirmer le mot de passe) : monmotdepasse

Port (Port) : 389

Cliquez sur OK.

PPTP/L2TP

L'accès par un client qui utilise un lien de modem sur des réseaux commutés publics bas débit, potentiellement avec une adresse IP imprévisible, vers des réseaux protégés via un VPN, pose problème. Les protocoles PPTP et L2TP fournissent deux moyens différents d'obtenir un accès VPN à partir de clients distants.

PPTP

Présentation. Le protocole tunnel point à point (PPTP) est conçu par le forum PPTP, un consortium d'entreprises comprenant Microsoft. C'est un protocole de « liaison de données » de couche 2 OSI (voir l'*Annexe D, La structure OSI*) et c'est une extension de l'ancien protocole point à point (PPP) utilisé pour l'accès à Internet en bas débit, C'était l'un des premiers protocoles conçus pour offrir un accès VPN à des serveurs distants via des réseaux commutés et il est toujours largement utilisé.

Mise en œuvre. Le protocole PPTP peut être utilisé dans le contexte VPN pour tunneliser différents protocoles sur Internet. La tunnelisation est possible grâce à l'encapsulation des paquets PPP dans des datagrammes IP à l'aide du protocole Generic Routing Encapsulation (GRE – protocole IP 47). Le client établit d'abord une connexion vers un FAI de façon normale en utilisant le protocole PPP, puis établit une connexion TCP/IP sur Internet vers le firewall D-Link, qui sert de serveur PPTP (utilisation du port TCP 1723). Le FAI n'est pas informé de l'existence du VPN car le tunnel s'étend du serveur PPTP au client. La norme PPTP ne définit pas la façon dont les données sont chiffrées. Le chiffrement est en général possible en utilisant la norme MPPE (chiffrement point à point de Microsoft).

Déploiement. Le protocole PPTP offre une solution pratique pour un accès client simple à déployer. Le protocole PPTP ne nécessite pas l'infrastructure de certificat trouvée dans L2TP mais repose sur une séquence nom d'utilisateur/mot de passe pour établir une certaine confiance entre le client et le serveur. Le niveau de sécurité fourni par une solution sans certificat est l'un des inconvénients du protocole PPTP. Le protocole PPTP présente également des problèmes d'évolutivité avec certains serveurs PPTP en limitant le nombre de clients PPTP simultanés. Étant donné que le protocole PPTP n'utilise pas IPsec, les connexions PPTP peuvent être traitées par NAT et le franchissement NAT n'est pas requis. Le protocole PPTP a été fourni par Microsoft dans ses systèmes d'exploitation depuis Windows 95 et par conséquent un grand nombre de clients sont déjà équipés du logiciel.

Dépannage du protocole PPTP. Un problème courant de configuration du protocole PPTP est qu'un routeur et/ou un commutateur sur un réseau bloque le port TCP 1723 et/ou le protocole IP 47 avant que la connexion PPTP soit établie vers le firewall D-Link. Un examen du journal peut indiquer si ce problème a eu lieu, avec un message de consignation sous la forme suivante :

```
Error PPP lcp_negotiation_stalled ppp_terminated
```

Exemple 9.10. Configuration d'un serveur PPTP

Cet exemple montre comment configurer un serveur réseau PPTP. Cet exemple suppose que vous avez déjà créé certains objets adresse dans le carnet d'adresses.

Vous devrez indiquer l'adresse IP de l'interface du serveur PPTP, une adresse IP externe (que le serveur PPTP doit écouter) et un groupe IP que le serveur PPTP utilisera pour donner des adresses IP aux clients.

Interface de ligne de commande

```
gw-world:/> add Interface L2TPServer MyPPTPServer ServerIP=lan_ip Interface=any
   IP=wan_ip IPPool=pp2p_Pool TunnelProtocol=PPTP AllowedRoutes=all-nets
```

Interface Web

Sélectionnez Interfaces > L2TP Servers > Add > L2TPServer (Interfaces > Serveurs L2TP > Ajouter > Serveur L2TP).

Nommez le serveur PPTP, par ex., MyPPTPServer.

Saisissez :

Inner IP Address (Adresse IP interne) : lan_ip

Tunnel Prococol (Protocole du tunnel) : PPTP

Outer Interface Filter (Filtre d'interface externe) : any (n'importe lequel)

Outer Server IP (IP du serveur externe) : wan_ip

Sous l'onglet PPP Parameters (Paramètres PPP), sélectionnez pptp_Pool dans la commande IP Pool (Groupe IP).

Sous l'onglet Add Route (Ajouter une route), sélectionnez all_nets (tout réseau) dans Allowed Networks (Réseaux autorisés).

Cliquez sur OK.

Use User Authentication Rules (Utiliser les règles d'authentification de l'utilisateur) est activé par défaut. Pour pouvoir authentifier les utilisateurs à l'aide du tunnel PPTP, vous devez également configurer des règles d'authentification qui ne seront pas abordées dans cet exemple.

L2TP

Le protocole de tunnelisation de couche 2 (L2TP) est une norme ouverte IETF qui permet de surmonter bien des problèmes du PPTP. Sa conception est une combinaison du protocole de transmission de niveau 2 (L2F) et du PPTP qui utilise les meilleures caractéristiques des deux. Étant donné que la norme L2TP ne met pas en œuvre le chiffrement, celui-ci est en général appliqué avec une norme IETF connue sous le nom de L2TP/IPsec, dans laquelle les paquets L2TP sont encapsulés par IPsec. Le client communique avec un concentrateur d'accès local (LAC), qui communique via Internet avec un serveur réseau L2TP (LNS). Le firewall D-Link sert de LNS. Le LAC, en effet, tunnelise les données, comme par exemple une session PPP, à l'aide d'IPsec vers le LNS via Internet. Dans la plupart des cas, le client servira lui-même de LAC.

L2TP est basé sur des certificats et par conséquent est plus simple à administrer avec un grand nombre de clients et offre une meilleure sécurité que le protocole PPTP. Contrairement à PPTP, il est possible de configurer plusieurs réseaux virtuels via un seul tunnel. Étant donné qu'il est basé sur IPsec, L2TP requiert la mise en œuvre du franchissement NAT (NAT-T) du côté LNS du tunnel.

Exemple 9.11. Configuration d'un serveur L2TP

Cet exemple montre comment configurer un serveur réseau L2TP. Cet exemple suppose que vous avez créé certains objets adresse dans le carnet d'adresses. Vous devrez indiquer l'adresse IP de l'interface du serveur L2TP, une adresse IP externe (que le serveur L2TP doit écouter) et un groupe IP que le serveur L2TP utilisera pour donner des adresses IP aux clients. L'interface sur laquelle le serveur L2TP acceptera des connexions est un tunnel IPsec virtuel, non illustré dans cet exemple.

Interface de ligne de commande

```
gw-world:/> add Interface L2TPServer MyL2TPServer ServerIP=ip_l2tp
   Interface=l2tp_ipsec IP=wan_ip IPPool=L2TP_Pool TunnelProtocol=L2TP
   AllowedRoutes=all-nets
```

Interface Web

Sélectionnez Interfaces > L2TP Servers > Add > L2TPServer (Interfaces > Serveurs L2TP > Ajouter > Serveur L2TP).

Entrez un nom convenable pour le serveur L2TP, par ex., *MyL2TPServer.*

Saisissez :

Inner IP Address (Adresse IP interne) : ip_l2tp

Tunnel Prococol (Protocole du tunnel) : L2TP

Outer Interface Filter (Filtre d'interface externe) : l2tp_ipsec

Outer Server IP (IP du serveur externe) : wan_ip

Sous l'onglet PPP Parameters (Paramètres PPP), sélectionnez L2TP_Pool dans la commande IP Pool (Groupe IP).

Sous l'onglet Add Route (Ajouter une route), sélectionnez all_nets (tout réseau) dans Allowed Networks (Réseaux autorisés).

Cliquez sur OK.

Use User Authentication Rules (Utiliser les règles d'authentification de l'utilisateur) est activé par défaut. Pour pouvoir authentifier les utilisateurs à l'aide du tunnel PPTP, vous devez également configurer des règles d'authentification qui ne sont pas abordées dans cet exemple.

Exemple 9.12. Configuration d'un tunnel L2TP

Cet exemple montre comment configurer un tunnel L2TP parfaitement fonctionnel et détaille de nombreuses parties de la configuration VPN de base. Avant de commencer, vous devez configurer certains objets adresse, par exemple le réseau qui sera attribué aux clients L2TP. Les listes de propositions et les clés pré-partagées sont également nécessaires. Nous utiliserons ici les objets créés dans les exemples précédents.

Pour pouvoir authentifier les utilisateurs en utilisant le tunnel L2TP, on utilisera une base de données utilisateur locale.

A. Commencez par préparer une nouvelle base de données utilisateur locale :

Interface de ligne de commande

```
gw-world:/> add LocalUserDatabase UserDB

gw-world:/> cc LocalUserDatabase UserDB

gw-world:/UserDB> add User testuser Password=mypassword
```

Interface Web

Sélectionnez User Authentication > Local User Databases > Add > Local User Database (Authentification utilisateur > Bases de données utilisateur locale > Ajouter > Base de données utilisateur locale).

Entrez un nom convenable de base de données utilisateur, par exemple UserDB.

Sélectionnez User Authentication > Local User Databases > UserDB > Add > User (Authentification utilisateur > Bases de données utilisateur locale > UserDB > Ajouter > Utilisateur).

Saisissez :

Username (Nom d'utilisateur) : utilisateurtest

Password (mot de passe) : monmotdepasse

Confirm Password (confirmer le mot de passe) : monmotdepasse

Cliquez sur OK.

Nous allons maintenant configurer le tunnel IPsec, qui sera ensuite utilisé dans la section L2TP. Étant donné que nous allons utiliser le protocole L2TP, le réseau local utilise la même IP à laquelle le tunnel L2TP se connectera, wan_ip. De plus, le tunnel IPsec doit être configuré pour ajouter de façon dynamique des routages vers le réseau distant lorsque le tunnel est établi.

B. Poursuivez la configuration du tunnel IPsec :

Interface de ligne de commande

```
gw-world:/> add Interface IPsecTunnel l2tp_ipsec LocalNetwork=wan_ip
   RemoteNetwork=all-nets IKEAlgorithms=ike-roamingclients
   IPsecAlgorithms=esp-l2tptunnel PSK=MyPSK EncapsulationMode=Transport
   DHCPOverIPsec=Yes AddRouteToRemoteNet=Yes IPsecLifeTimeKilobytes=250000
   IPsecLifeTimeSeconds=3600
```

Interface Web

Sélectionnez Interfaces > IPsec > Add > IPsec Tunnel (Interfaces IPsec > Ajouter > Tunnel IPsec).

Nommez le tunnel IPsec, par ex., *l2tp_ipsec*.

Saisissez :

Réseau local : wan_ip

Remote Network (réseau distant) : all-nets (tout réseau)

Extrémité distante : (aucune)

Encapsulation Mode (mode d'encapsulation) : Transport

IKE Proposal List (Liste de propositions IKE) : ike-roamingclients

IPsec Proposal List (Liste de propositions IPsec) : esp-l2tptunnel

Entrez 3 600 dans la commande en secondes IPsec Life Time (durée de vie IPsec).

Entrez 250 000 dans la commande en kilo-octets IPsec Life Time (durée de vie IPsec).

Sous l'onglet Authentication, sélectionnez Pre-shared Key (Clé pré-partagée).

Sélectionnez MyPSK dans la commande Pre-shared Key (Clé pré-partagée).

Sous l'onglet Routing (Routage), vérifiez les commandes suivantes :

Autorisez DHCP sur IPsec à partir des clients hôtes uniques.

Ajoutez une route de façon dynamique au réseau distant lorsqu'un tunnel est établi.

Cliquez sur OK.

Il est temps maintenant de configurer le serveur L2TP. L'adresse IP interne doit faire partie du réseau à partir duquel des adresses IP sont attribuées aux clients, dans ce lan_ip. Le filtre d'interface externe est l'interface sur laquelle le serveur L2TP acceptera des connexions ; il s'agira de l'interface 12tp_ipsec créée précédemment. Un proxy ARP doit également être configuré pour les IP utilisées par les clients L2TP.

C. Configurez le tunnel L2TP :

Interface de ligne de commande

```
gw-world:/> add Interface L2TPServer l2tp_tunnel IP=lan_ip Interface=l2tp_ipsec
   ServerIP=wan_ip IPPool=l2tp_pool TunnelProtocol=L2TP
   AllowedRoutes=all-nets ProxyARPInterfaces=lan
```

Interface Web

Sélectionnez Interfaces > L2TP Servers > Add > L2TPServer (Interfaces > Serveurs L2TP > Ajouter > Serveur L2TP).

Nommez le tunnel L2TP, par ex., *l2tp_tunnel.*

Saisissez :

Inner IP Address (Adresse IP interne) : lan_ip

Tunnel Prococol (Protocole du tunnel) : L2TP

Outer Interface Filter (Filtre d'interface externe) : l2tp_ipsec

Adresse IP du serveur : wan_ip

Sous l'onglet PPP Parameters (Paramètres PPP), cochez la commande Use User Authentication Rules (Utiliser les règles d'authentification utilisateur).

Sélectionnez l2tp_pool dans la commande IP Pool (Groupe IP).

Sous l'onglet Add Route (Ajouter un routage), sélectionnez all_nets (tout réseau) dans la commande Allowed Networks (Réseaux autorisés).

Dans la commande ProxyARP, sélectionnez l'interface lan.

Cliquez sur OK.

Afin d'authentifier les utilisateurs à l'aide du tunnel L2TP, une règle d'authentification d'utilisateur doit être configurée.

D. Nous allons ensuite configurer les règles d'authentification :

Interface de ligne de commande

```
gw-world:/> add UserAuthRule AuthSource=Local Interface=l2tp_tunnel
   OriginatorIP=all-nets LocalUserDB=UserDB agent=PPP TerminatorIP=wan_ip
   name=L2TP_Auth
```

Interface Web

Sélectionnez User Authentication > User Authentication Rules > Add > UserAuthRule (Authentification utilisateur > Règles d'authentification utilisateur > Ajouter > Règle d'authentification utilisateur).

Entrez un nom convenable pour la règle, par exemple *L2TP_Auth.*

Saisissez :

Agent : PPP

Authentication Source (Source de l'authentification) : Locale

Interface : l2tp_tunnel

Originator IP (Générateur d'IP) : all-nets (tout réseau)

Terminator IP (Terminateur d'IP) : wan_ip

Sous l'onglet Authentication Options (Options d'authentification), entrez *UserDB* comme base de données utilisateur locale.

Cliquez sur OK.

Lorsque les autres parties sont terminées, il ne reste que les règles. Pour permettre un trafic via le tunnel, deux règles IP doivent être ajoutées.

E. Pour finir, configurez les règles :

Interface de ligne de commande

```
gw-world:/> add IPRule action=Allow Service=all_services
   SourceInterface=l2tp_tunnel SourceNetwork=l2tp_pool
   DestinationInterface=any DestinationNetwork=all-nets name=AllowL2TP

gw-world:/> add IPRule action=NAT Service=all_services
   SourceInterface=l2tp_tunnel SourceNetwork=l2tp_pool
   DestinationInterface=any DestinationNetwork=all-nets name=NATL2TP
```

Interface Web

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Nommez la règle, par exemple *AllowL2TP*.

Saisissez :

Action : Allow (Autoriser)

Service : all_services (tous les services)

Source Interface (Interface source) : l2tp_tunnel

Source Network (Réseau source) : l2tp_pool

Destination Interface (Interface de destination) : any (n’importe lequel)

Destination Network (Réseau de destination) : all-nets (tout réseau)

Cliquez sur OK.

Sélectionnez Rules > IP Rules > Add > IPRule (Règles > Règles IP > Ajouter > Règle IP).

Nommez la règle, par exemple *NATL2TP*.

Saisissez :

Action : NAT

Service : all_services (tous les services)

Source Interface (Interface source) : l2tp_tunnel

Source Network (Réseau source) : l2tp_pool

Destination Interface (Interface de destination) : any (n’importe lequel)

Destination Network (Réseau de destination) : all-nets (tout réseau)

Cliquez sur OK.

Chapitre 10. Gestion du trafic

Le présent chapitre décrit la manière dont NetDefendOS gère le trafic réseau.

Mise en forme du trafic

Introduction

Qualité de service (QoS) avec le protocole TCP/IP. Une réelle fonction de *qualité de service* (QoS) fait défaut au protocole TCP/IP. La qualité de service consiste à garantir et à limiter la bande passante du réseau pour certains services et utilisateurs. Des solutions telles que l'architecture de *services différenciés* (Diffserv) ont été conçues afin de traiter les problèmes de qualité de service sur les réseaux à grande échelle ; elles utilisent les informations contenues dans les en-têtes des paquets pour fournir aux périphériques réseau des informations de qualité de service.

Prise en charge de Diffserv par NetDefendOS. NetDefendOS prend en charge l'architecture Diffserv de deux manières : premièrement, il transfère les 6 bits composant le point de code de services différenciés (DSCP) Diffserv, puis copie ces bits provenant du trafic de données des tunnels VPN vers les paquets encapsulés. Deuxièmement, comme indiqué plus loin dans ce chapitre, les bits DSCP peuvent être utilisés par le sous-système de mise en forme du trafic de NetDefendOS en tant que base de définition des priorités du trafic traversant un firewall D-Link.

Solution de mise en forme du trafic. Les architectures semblables à Diffserv se révèlent limitées si les applications fournissent elles-mêmes au réseau les informations de qualité de service. En règle générale, dans la plupart des réseaux, il ne convient pas que les applications et les utilisateurs du réseau décident de la priorité de leur trafic. Si les utilisateurs ne sont pas fiables, l'équipement réseau doit prendre les décisions quant aux priorités et à l'allocation de la bande passante.

NetDefendOS permet le contrôle de la qualité de service en autorisant l'administrateur à appliquer des limites et des garanties au trafic réseau traversant un firewall D-Link. Cette approche, souvent intitulée *mise en forme du trafic*, est parfaitement adaptée à la gestion de la bande passante des réseaux locaux, ainsi qu'à la gestion des goulots d'étranglement potentiels dans les réseaux étendus. Elle peut s'appliquer à n'importe quel trafic, y compris celui qui traverse des tunnels VPN.

Objectifs de la mise en forme du trafic. La mise en forme du trafic consiste à mesurer et à placer en file d'attente les paquets IP en tenant compte du nombre de paramètres configurables. Les objectifs sont les suivants :

Appliquer des limites de bande passante et placer en file d'attente les paquets qui dépassent les limites configurées, puis les envoyer une fois que les demandes de bande passante ont diminué.

Ignorer les paquets lorsque la mémoire tampon des paquets est saturée. Les paquets à ignorer doivent être sélectionnés parmi ceux responsables de « l'embouteillage ».

Définir la priorité du trafic, d'après les décisions de l'administrateur. Si le trafic de priorité élevée augmente alors qu'une ligne de transmission est saturée, le trafic de faible priorité peut être temporairement limité afin de libérer de l'espace pour le trafic de priorité supérieure.

Fournir des garanties de bande passante. En général, cette opération s'effectue en attribuant une priorité élevée à un certain volume de trafic (volume garanti). Le trafic dépassant le volume garanti présente alors la même priorité que « n'importe quel autre trafic » et se retrouve en concurrence avec le reste du trafic non prioritaire.

En général, la mise en forme du trafic ne consiste pas à placer en file d'attente d'importants volumes de données, puis à trier le trafic prioritaire à envoyer avant d'envoyer le trafic non prioritaire. En effet, le volume du trafic prioritaire est mesuré et le trafic non prioritaire est limité de manière dynamique de telle sorte qu'il n'affecte pas le débit du trafic prioritaire.

Mise en forme du trafic dans NetDefendOS

NetDefendOS offre des fonctions complètes de mise en forme du trafic pour les paquets traversant un firewall D-Link. Il est possible de créer différentes règles régissant les limites de débit et les garanties de trafic en fonction de la source, de la destination et du protocole du trafic, selon la même procédure que pour la création des ensembles de règles IP.

Dans NetDefendOS, les deux composants clés de la mise en forme du trafic sont les suivants :

Les tuyaux

Les règles des tuyaux

Tuyaux. Le tuyau est l'objet essentiel de la mise en forme du trafic. Il s'agit d'un tuyau conceptuel que les paquets de données peuvent traverser. Différentes caractéristiques définissent le mode de gestion du trafic le traversant. L'administrateur peut définir autant de tuyaux que nécessaire ; aucun n'est défini par défaut.

Les tuyaux sont sommaires dans le sens où ils ne se préoccupent pas des types de trafic qui les traversent, ni de la direction du trafic. Ils se contentent de mesurer les données qui les traversent et d'appliquer les limites configurées par l'administrateur au niveau du tuyau dans son intégralité ou alors au niveau des *Priorités* et/ou des *Groupes* (voir les explications ci-dessous).

NetDefendOS est capable de gérer simultanément des centaines de tuyaux, mais dans la plupart des cas, seul un nombre réduit est nécessaire. Toutefois, des douzaines de tuyaux peuvent être nécessaires dans des scénarios où des tuyaux spécifiques sont utilisés pour des protocoles spécifiques (ou clients, dans le cas des FAI).

Règles des tuyaux. Les règles des tuyaux constituent *l'ensemble de règles des tuyaux*. Chaque règle est définie comme les autres règles de NetDefendOS, c’est-à-dire en définissant l'interface source/destination et le réseau source/destination, ainsi que le service auquel la règle doit s'appliquer. Lorsqu'une nouvelle connexion est autorisée par l'ensemble de règles IP, les règles correspondantes de l'ensemble de règles des tuyaux sont systématiquement recherchées de la même manière, de haut en bas. Si des règles correspondantes sont trouvées, la première d'entre elles est utilisée pour la mise en forme du trafic. À l'origine, l'ensemble de règles de tuyaux est vierge.

Lorsqu'une règle de tuyau est définie, les tuyaux à utiliser avec cette dernière sont également définis, puis placés dans l'une des deux listes figurant dans la règle de tuyau. Ces listes sont les suivantes :

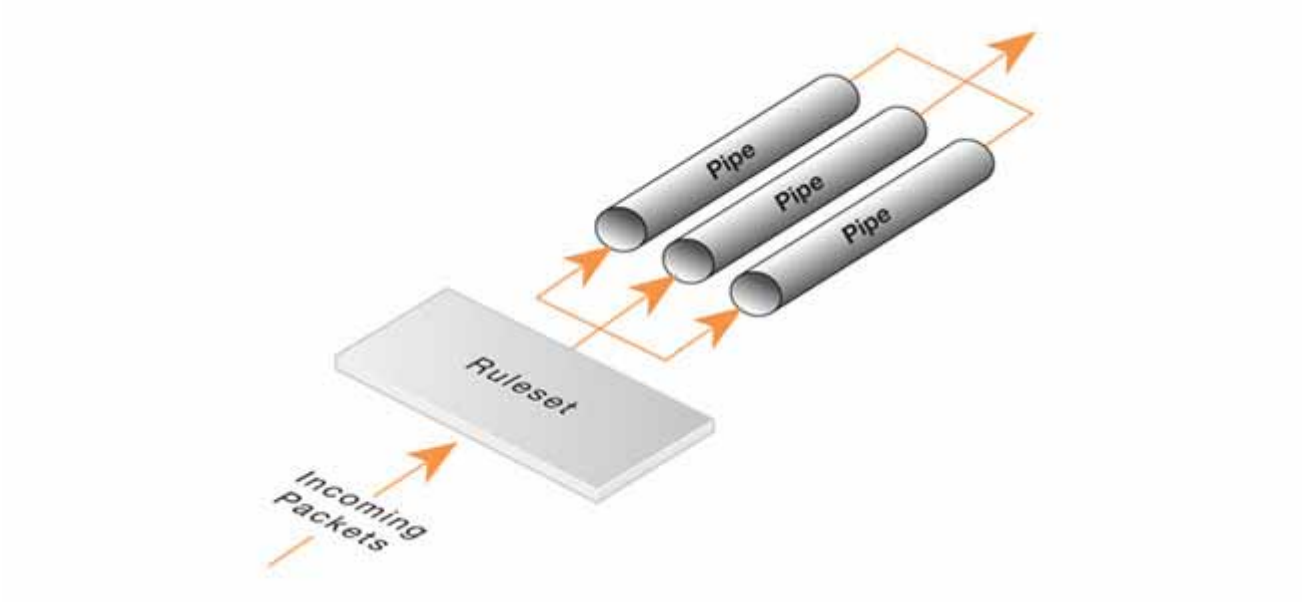
Chaînage d’envoi

Il s'agit des tuyaux qui seront utilisés pour le trafic sortant via le firewall D-Link. Il est possible d'indiquer un ou plusieurs tuyaux, ou alors aucun.

Chaînage de réception

Il s'agit des tuyaux qui seront utilisés pour le trafic entrant. Il est possible d'indiquer un ou plusieurs tuyaux, ou alors aucun.

Figure 10.1. Ensemble de règles des tuyaux appliqué au flux de paquets des tuyaux



Lorsqu'un tuyau est spécifié dans une liste, il s'agit de celui dont les caractéristiques seront appliquées au trafic. Lorsqu'un ensemble de tuyaux est spécifié, ces derniers forment une *chaîne* de tuyaux qui sera traversée par le trafic. Une chaîne peut être composée d'un maximum de 8 tuyaux.

Si aucun tuyau n'est spécifié dans une liste, le trafic correspondant à la règle ne traversera aucun tuyau. Par ailleurs, il ne sera soumis à aucune autre règle de tuyau trouvée ultérieurement dans l'ensemble de règles.

Limite simple de bande passante

La manière la plus simple d'utiliser les tuyaux est dans le cadre de la limite de la bande passante. Par ailleurs, ce scénario nécessite une planification minime. L'exemple ci-dessous applique une limite de bande passante à un trafic entrant uniquement. Il s'agit de la direction la plus à même d'entraîner des problèmes au niveau des connexions Internet.

Exemple 10.1. Application d’une limite simple de bande passante

Tout d'abord, créez un tuyau simple qui limite tout le trafic le traversant à 2 mégabits par seconde, quel que soit le trafic.

Interface de ligne de commande

```
gw-world:/> add Pipe std-in LimitKbpsTotal=2000
```

Interface Web

Sélectionnez Traffic Management > Traffic Shaping > Pipes > Add > Pipe (Gestion du trafic > Mise en forme du trafic > Tuyaux > Ajouter > Tuyau).

Indiquez un nom adapté pour le tuyau, par exemple *std-in.*

Saisissez 2000 dans la zone de texte Total.

Cliquez sur OK.

Le trafic doit traverser le tuyau ; pour ce faire, le tuyau est utilisé dans une règle de tuyau.

Nous utiliserons le tuyau ci-dessus pour limiter le trafic entrant. Cette limite s'appliquera aux paquets de données réels et non aux connexions. Dans le cadre de la mise en forme du trafic, nous nous concentrons sur la direction de circulation des données et non sur l'ordinateur qui a démarré la connexion.

Créez une règle simple autorisant tout trafic sortant. Nous ajoutons le tuyau créé au *chaînage de réception*. En d'autres termes, les paquets circulant dans le sens de réception de cette connexion (trafic entrant) doivent traverser

le tuyau *std-in*.

Interface de ligne de commande

```
gw-world:/> add PipeRule ReturnChain=std-in SourceInterface=lan
   SourceNetwork=lannet DestinationInterface=wan
   DestinationNetwork=all-nets Service=all_services name=Outbound
```

Interface Web

Sélectionnez Traffic Management > Traffic Shaping > Pipes > Add > Pipe Rule (Gestion du trafic > Mise en forme du trafic > Tuyaux > Ajouter > Règle de tuyau).

Indiquez un nom adapté pour le tuyau, par exemple *sortant*.

Saisissez :

Service : all_services (tout service)

Source Interface (Interface source) : lan

Source Network (Réseau source) : lannet

Destination Interface (Interface de destination) : wan

Destination Network (Réseau de destination) : all-nets (tout réseau)

Dans l'onglet Traffic Shaping (Mise en forme du trafic), sélectionnez std-in dans la liste Return Chain (Chaînage de réception).

Cliquez sur OK.

Ce paramétrage limite tout le trafic entrant (en provenance d'Internet) à 2 mégabits par seconde. Aucune priorité ni équilibrage dynamique n'est appliqué.

Limite de la bande passante dans les deux directions

Un tuyau unique ne tient pas compte de la provenance du trafic le traversant lorsqu'il calcule le débit total. NetDefendOS permet d'utiliser le même tuyau à la fois pour le trafic sortant et le trafic entrant ; toutefois, les limites du tuyau ne seront pas clairement partitionnées entre les deux directions. Le scénario suivant illustre ce point.

Dans l'exemple précédent, seule la bande passante entrante est limitée. Nous choisissons cette direction car dans la plupart des paramétrages, il s'agit de celle qui sature en premier. À présent, nous souhaitons limiter la bande passante sortante de la même façon.

Le simple fait d'insérer le tuyau std-in dans le chaînage d’envoi ne fonctionnera pas étant donné que vous souhaiterez probablement que la limite à 2 Mbps du trafic sortant soit distincte de la limite à 2 Mbps du trafic entrant. Si nous tentons de faire traverser 2 Mbps de trafic et 2 Mbps de trafic entrant dans le tuyau, on obtient alors 4 Mbps. Étant donné que la limite du tuyau est 2 Mbps, vous pourrez obtenir environ 1 Mbps dans chaque direction.

Le fait d'augmenter la limite totale du tuyau à 4 Mbps ne résoudra pas le problème étant donné que le tuyau unique ignorera qu'il était prévu 2 Mbps de trafic entrant et 2 Mbps de trafic sortant. En effet, le résultat obtenu peut donner un trafic sortant de 3 Mbps et un trafic entrant de 1 Mbps, ce qui revient également à 4 Mbps.

Pour contrôler la bande passante dans les deux directions, il est recommandé d'utiliser deux tuyaux distincts : l'un pour le trafic entrant et l'autre pour le trafic sortant. Dans le présent scénario, il s'agirait de limiter chaque tuyau à 2 Mbps pour atteindre le résultat escompté. L'exemple suivant présente le paramétrage correspondant.

Exemple 10.2. Limite de la bande passante dans les deux directions

Créez un deuxième tuyau pour le trafic sortant :

Interface de ligne de commande

```
gw-world:/> add Pipe std-out LimitKbpsTotal=2000
```

Interface Web

Sélectionnez Traffic Management > Traffic Shaping > Pipes > Add > Pipe (Gestion du trafic > Mise en forme du trafic > Tuyaux > Ajouter > Tuyau).

Indiquez un nom pour le tuyau, par exemple *std-out.*

Saisissez 2000 dans la zone de texte Total.

Cliquez sur OK.

Après avoir créé un tuyau pour le contrôle de la bande passante, ajoutez-le au chaînage d'envoi de la règle créée dans l'exemple précédent.

Interface de ligne de commande

```
gw-world:/> set PipeRule Outbound ForwardChain=std-out
```

Interface Web

Sélectionnez Traffic Management > Traffic Shaping > Pipe Rules (Gestion du trafic > Mise en forme du trafic > Règles des tuyaux).

Cliquez avec le bouton droit de la souris sur la règle de tuyau créée dans l'exemple précédent, puis cliquez sur Edit (Modifier).

Dans l'onglet Traffic Shaping (Mise en forme du trafic), sélectionnez *std-out* dans la liste Forward Chain (Chaînage d'envoi).

Cliquez sur OK.

Toutes les connexions sortantes sont alors limitées à 2 Mbps dans chaque direction.

Création de limites différenciées avec des chaînes

Dans les exemples précédents, une limite de trafic statique est appliquée à toutes les connexions sortantes. À présent, nous souhaitons limiter la navigation Web davantage que le reste du trafic. Il est possible dans ce cas de définir deux tuyaux de « navigation » pour le trafic entrant et le trafic sortant. Cependant, nous n'aurons vraisemblablement pas à limiter le trafic sortant. En effet, la navigation est en général composée de courtes requêtes sortantes suivies de longues réponses entrantes. Imaginons que la bande passante totale est limitée à 250 kbps, dont 125 kbps sont alloués au trafic entrant de la navigation Web. Dans ce cas, un tuyau de navigation entrante est paramétré pour le trafic entrant, avec une limite de 125 kbps.

Ensuite, une nouvelle règle de tuyau est paramétrée pour la navigation utilisant le tuyau de navigation entrante, puis est placée avant la règle régissant « tout le reste » qui traverse le tuyau std-in. De cette manière, le trafic de navigation traverse le tuyau de navigation entrante et tout le reste est géré par la règle et le tuyau créés précédemment.

Malheureusement, l'effet recherché n'est pas atteint, c'est-à-dire l'allocation d'un maximum de 125 kbps au trafic entrant de navigation compris dans le total de 250 kbps. En effet, le trafic entrant traversera l'un des deux tuyaux : celui autorisant 250 kbps ou celui autorisant 125 kbps, pour un total potentiel de 375 kbps de trafic entrant.

Pour résoudre ce problème, nous créons dans la règle de tuyau du trafic de navigation une *chaîne* composée du tuyau de navigation entrante suivi du tuyau std-in. De cette façon, le trafic entrant de navigation traversera tout d'abord le tuyau de navigation entrante et sera limité à 125 kbps maximum. Il traversera ensuite le tuyau std-in avec le reste du trafic entrant, ce qui permettra d'appliquer la limite totale de 250 kbps. Si la navigation utilise la limite de 125 kbps maximum, ces 125 kbps occuperont la moitié du tuyau std-in et ne laisseront que 125 kbps pour le reste du trafic. Si aucune navigation n'a lieu, l'intégralité des 250 kbps alloués au tuyau std-in sera disponible pour le reste du trafic.

Il ne s'agit pas d'une garantie de bande passante pour la navigation Web, mais d'une garantie de bande passante de 125 kbps pour tout ce qui ne concerne pas la navigation Web. Dans le cadre de la navigation Web, les règles standard du « premier arrivé, premier transféré » s'appliquent en cas de concurrence sur la bande passante. On peut alors obtenir 125 kbps, mais aussi une vitesse bien plus lente si la connexion est saturée.

Ce type de paramétrage des tuyaux permet uniquement de limiter les valeurs maximum de certains types de trafic et non de définir les priorités des différents types de trafic en concurrence.

Priorités

Tous les paquets qui traversent les tuyaux de mise en forme du trafic NetDefendOS sont associés à une priorité. Dans les exemples précédents, les priorités ne sont pas explicitement définies, de telle sorte que tous les paquets ont la même priorité par défaut, à savoir 0.

Il existe huit priorités, numérotées de 0 à 7, la priorité 0 étant la moins importante et la priorité 7 la plus importante. On peut considérer une priorité comme une file d'attente distincte du trafic ; le trafic de priorité 2 est transféré avant le trafic de priorité 0 et le trafic de priorité 4 avant celui de priorité 2.

La signification propre d'une priorité provient du fait qu'elle est soit supérieure, soit inférieure à une autre priorité. Par exemple, si l'on utilise deux priorités dans un scénario, le fait de sélectionner les priorités 4 et 6 au lieu des priorités 0 et 3 ne fera aucune différence.

Figure 10.2. Les huit priorités de tuyau

Affectation des priorités. Le mode d'affectation de la priorité à un paquet est déterminé par la règle de tuyau qui contrôle ce dernier et peut être effectué de trois manières :

Use the precedence of the first pipe (Utiliser la priorité du premier tuyau) : chaque tuyau est associé à une *priorité par défaut* et les paquets prennent la priorité par défaut du premier tuyau qu'ils traversent.

Use the allocated precedence (Utiliser la priorité affectée) : la règle de tuyau affecte une priorité de manière explicite.

Use the DSCP bits (Utiliser les bits DSCP) : la priorité provient des bits DSCP contenus dans le paquet. Le DSCP est un sous-ensemble de l'architecture Diffserv où les bits *ToS (type de service)* sont inclus dans l'en-tête du paquet IP.

Priorités des tuyaux. Lors de la configuration d'un tuyau, il est possible d'indiquer une *priorité par défaut*, une *priorité minimum* et une *priorité maximum*. La priorité par défaut est celle que prend un paquet si la priorité n'est pas affectée de manière explicite par une règle de tuyau (voir paragraphe précédent).

Les priorités minimum et maximum définissent la plage de priorités gérée par le tuyau. Si la priorité affectée à un paquet entrant est inférieure à la valeur minimum, elle est modifiée pour être égale à la priorité minimum. De même, si la priorité affectée à un paquet entrant est supérieure à la valeur maximum, elle est modifiée pour être égale à la priorité maximum.

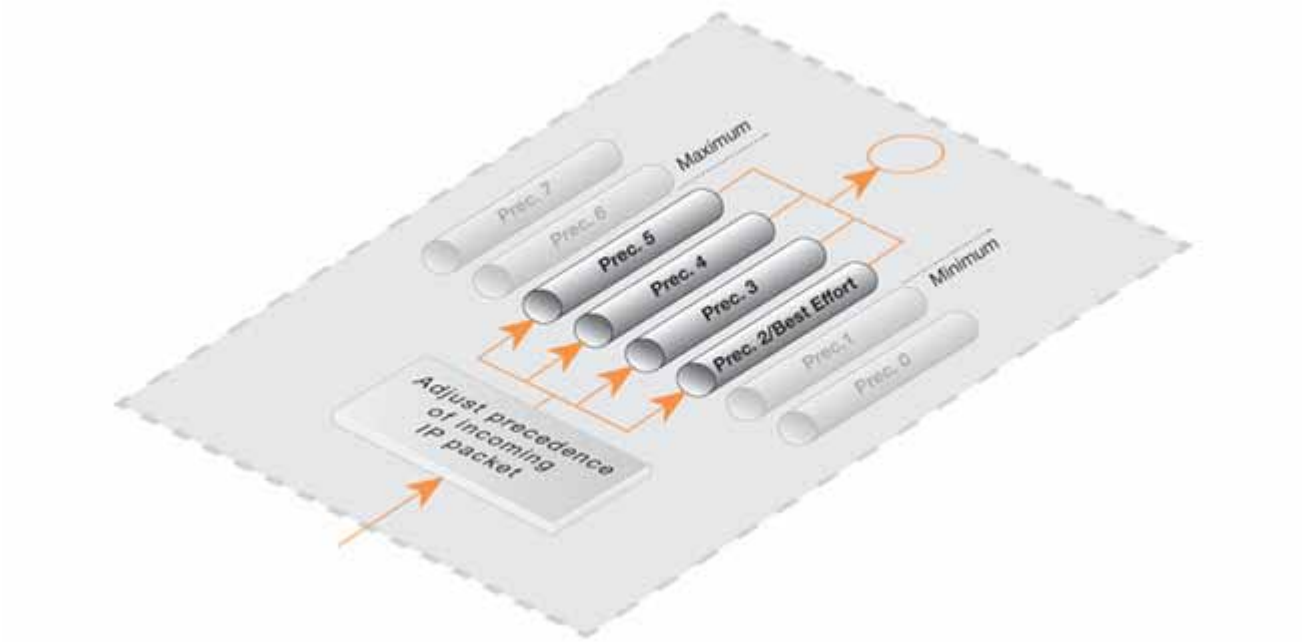
Au niveau de chaque tuyau, des limites de bande passante distinctes peuvent éventuellement être indiquées pour chaque niveau de priorité. Ces limites peuvent être spécifiées en kilobits par seconde et/ou en paquets par seconde

(si vous spécifiez les deux, la première limite atteinte sera utilisée). En cas d'utilisation des priorités, la limite totale du tuyau dans son intégralité doit être indiquée, de telle sorte que le tuyau connaisse sa capacité et, par conséquent, sache quand les priorités sont utilisées.

La priorité « *meilleur effort* ». La priorité définie en tant que priorité de tuyau minimum a un sens particulier : elle joue le rôle de *priorité « meilleur effort »*. Tous les paquets entrants à ce niveau de priorité sont toujours traités selon le principe du « premier arrivé, premier transféré » et ne peuvent pas être envoyés à un autre niveau de priorité.

Les paquets présentant une priorité supérieure et qui dépassent les limites de cette priorité sont automatiquement transférés vers la priorité « meilleur effort » et ne sont plus traités différemment des paquets présentant une priorité inférieure. Cette approche est utilisée dans la mesure où une limite de priorité traduit également une garantie de cette priorité.

Figure 10.3. Priorités de tuyau minimum et maximum



Les priorités n'ont aucun impact tant que la bande passante totale allouée à un tuyau n'est pas atteinte, c’est-à-dire tant que le tuyau n'est pas « plein ». À ce stade, le trafic est hiérarchisé par NetDefendOS et les paquets de priorité supérieure sont envoyés avant ceux de priorité inférieure. En effet, les paquets de priorité inférieure sont mis en mémoire tampon. Si l'espace de la mémoire tampon sature, ils sont supprimés.

Application des priorités. Nous ajoutons à l'exemple précédent l'exigence suivante : la priorité du trafic SSH et Telnet doit être supérieure à celle du reste du trafic. Pour ce faire, nous créons une règle de tuyau tout spécialement pour le trafic SSH et Telnet et lui affectons une priorité supérieure, soit 2. Nous y indiquons les mêmes tuyaux que ceux utilisés pour le reste du trafic.

Par conséquent, la règle SSH et Telnet affecte la priorité supérieure aux paquets associés à ces services et ces paquets sont envoyés via le même tuyau que le reste du trafic. Ensuite, le tuyau vérifie que ces paquets de priorité supérieure sont les premiers à être envoyés lorsque la limite de bande passante totale indiquée dans la configuration du tuyau est dépassée. Les paquets de priorité inférieure sont alors mis en mémoire tampon, puis envoyés lorsque le trafic de haute priorité utilise une bande passante inférieure au maximum défini pour le tuyau. Ce processus de mise en mémoire tampon est également appelé « réduction de l'encombrement » dans la mesure où il réduit le débit.

Le besoin de garanties. Si le trafic prioritaire est un flux continu (par exemple, communication audio en temps réel), un problème peut toutefois survenir et entraîner l'utilisation continue de toute la bande passante disponible et, par conséquent, provoquer des temps d'attente considérables pour les autres services tels que la navigation, DNS ou FTP. Dans ce cas, il est nécessaire de garantir que le trafic de priorité inférieure bénéficie d'une portion de la bande passante ; cela peut être réalisé grâce aux *garanties de bande passante.*

Garanties

Les garanties de bande passante assurent qu'une portion minimum de la bande passante est disponible pour une priorité donnée. Pour cela, une limite maximum est spécifiée pour la priorité d'un tuyau. Il s'agit de la portion maximum de bande passante admise par la priorité et qui sera envoyée avant les priorités inférieures. Le trafic dépassant cette limite sera envoyé au niveau de priorité « meilleur effort », c'est-à-dire la priorité la plus basse.

Pour modifier le trafic SSH et Telnet hiérarchisé de l'exemple précédent et lui appliquer une garantie de 96 kbps, vous affectez 96 kbps à la limite de priorité 2 du tuyau *std-in*.

Cela ne signifie pas que le trafic entrant SSH et Telnet est limité à 96 kbps. En effet, les limites de priorités supérieures à la priorité « meilleur effort » limitent uniquement le volume du trafic qui circule dans la priorité concernée.

Si le trafic entrant de priorité 2 est supérieur à 96 kbps, le trafic excédentaire sera affecté à la priorité « meilleur effort ». L'intégralité du trafic de priorité « meilleur effort » est ensuite transféré selon le principe du « premier arrivé, premier transféré ».

Remarque

Le fait de définir une limite maximum pour la priorité la plus basse (« meilleur effort ») ou pour toute autre priorité inférieure n'est d'aucune utilité et n'est pas pris en compte par NetDefendOS.

Garanties différenciées

Un problème se soulève lorsque vous souhaitez attribuer une garantie de bande passante de 32 kbps au trafic Telnet et de 64 kbps au trafic SHH. Il est alors possible de définir une limite de 32 kbps pour la priorité 2 et une limite de 64 kbps pour la priorité 4, puis de faire circuler les différents types de trafic dans leurs priorités respectives. Cette approche présente cependant deux problèmes évidents :

Quel trafic est le plus important ? Cette question ne pose pas de problème majeur dans ce cas, mais peut devenir stratégique à mesure que votre scénario de mise en forme du trafic devient plus complexe.

Le nombre de priorités est limité. Ce nombre peut être insuffisant dans certains cas et faire obstacle au problème précédent concernant l'importance du trafic.

Dans ce cas, la solution consiste à créer deux nouveaux tuyaux : l'un pour le trafic Telnet et l'autre pour le trafic SHH (comme le tuyau de navigation créé précédemment).

Tout d'abord, supprimez la limite de 96 kbps du tuyau std-in, puis créez deux nouveaux tuyaux : ssh-in et telnet-in. Attribuez aux deux tuyaux la priorité par défaut 2, ainsi que les limites de priorité 2 respectives, soit 32 kbps et 64 kbps.

Ensuite, divisez la règle définie précédemment pour la plage de ports 22 à 23 en deux règles couvrant respectivement le port 22 et le port 23.

Conservez la valeur std-out pour le chaînage d’envoi des deux règles. Ici aussi et dans le but de simplifier cet exemple, nous nous concentrerons uniquement sur le trafic entrant car il s'agit de la direction la plus à même de saturer dans les configurations orientées client.

Attribuez au chaînage de réception de la règle du port 22 la valeur ssh-in suivie de std-in.
Attribuez au chaînage de réception de la règle du port 23 la valeur telnet-in suivie de std-in.
Pour ces deux règles, sélectionnez Use the precedence of the first pipe (Utiliser la priorité du premier tuyau) pour l'affectation des priorités, afin que les valeurs par défaut du premier tuyau soient utilisées. La valeur par défaut des tuyaux ssh-in et telnet-in est 2.

À l'inverse du codage en dur de la priorité 2 dans l'ensemble de règles, cette approche vous permet de changer facilement la priorité de l'intégralité du trafic SSH et Telnet en modifiant la priorité par défaut des tuyaux ssh-in et telnet-in.

Notez que nous n'avons pas défini de limite totale pour les tuyaux ssh-in et telnet-in. Cela n'est pas nécessaire dans la mesure où la limite totale sera appliquée par le tuyau std-in à l'extrémité des chaînes respectives.

Les tuyaux ssh-in et telnet-in agissent en tant que « filtre de priorité » : ils garantissent que seul le total réservé, respectivement 64 kbps et 32 kbps, du trafic de priorité 2 atteindra le tuyau std-in. Le trafic SSH et Telnet dépassant la garantie atteindra le tuyau std-in avec une priorité 0, c'est-à-dire la priorité « meilleur effort » des tuyaux std-in et ssh-in.

Remarque

À ce niveau, l'ordre des tuyaux dans le chaînage de réception est important. En effet, si le tuyau std-in apparaît avant les tuyaux ssh-in et telnet-in, le trafic atteint std-in au niveau de priorité le plus bas et entre alors en concurrence avec le reste du trafic pour les 250 kbps de bande passante disponible.

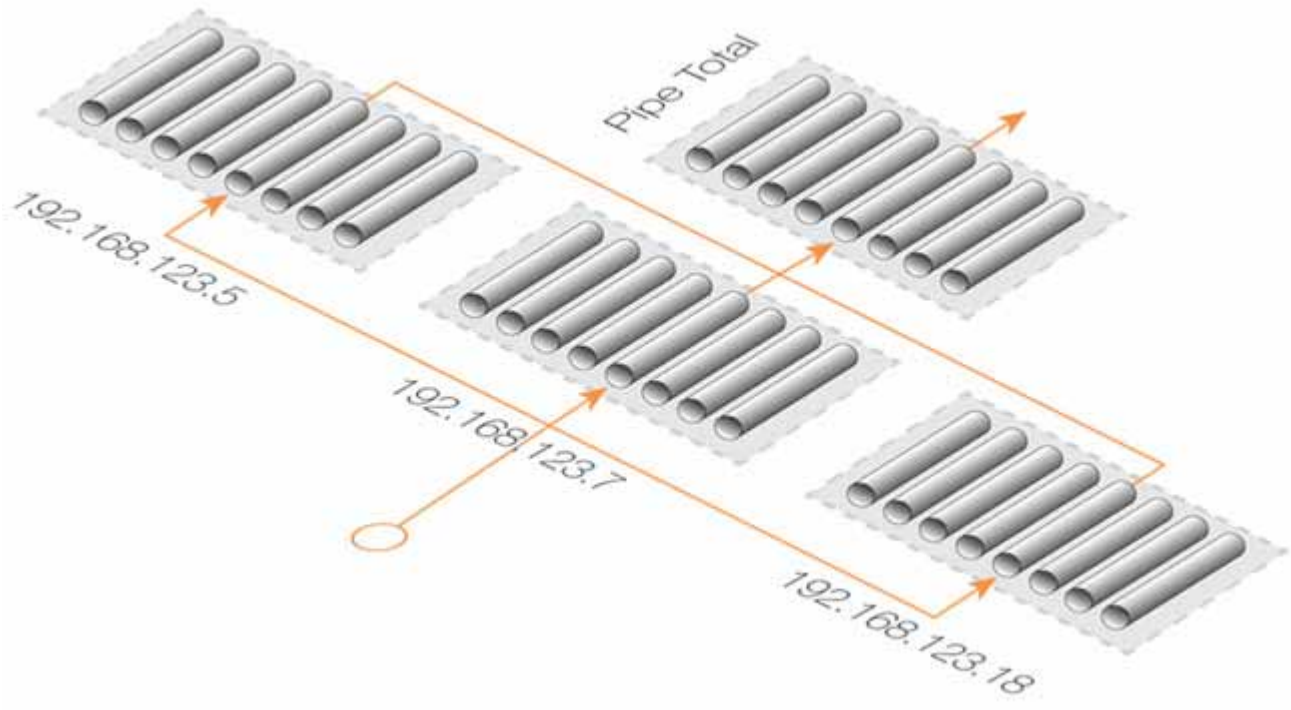
Groupes

NetDefendOS fournit une précision accrue du contrôle au sein des tuyaux. En effet, il permet de diviser la bande passante des tuyaux en fonction du réseau source/destination du paquet, de l'adresse IP, du port ou de l'interface. Cette opération est synonyme de création de *groupes*, où les membres d'un groupe, parfois appelés *utilisateurs*, peuvent être soumis à des limites et à des garanties. En règle générale, on utilise cette division du trafic en vue de créer des groupes par adresse IP ou par interface.

En cas de création de groupes par port, l'adresse IP est implicitement incluse de telle sorte que le port 1024 de l'ordinateur A est différent du port 1024 de l'ordinateur B et les connexions spécifiques sont identifiables. Si vous choisissez de créer des groupes par réseau, vous devez également indiquer la taille du réseau (même signification que le masque réseau).

Scénario de groupes simple. Si la limite de bande passante totale d'un tuyau est de 400 bps et que vous souhaitez allouer cette bande passante à plusieurs adresses IP de destination de sorte qu'aucune adresse IP ne puisse bénéficier de plus de 100 bps de la bande passante, sélectionnez le groupement « Per DestIP » (Par IP de destination) et saisissez une limite totale correspondante de 100 bps. La bande passante est alors allouée selon le principe du « premier arrivé, premier transféré » et aucune adresse IP de destination ne peut recevoir plus de 100 bps. Quel que soit le nombre de connexions impliquées, la bande passante totale combinée ne peut toujours pas dépasser la limite de 400 bps définie pour le tuyau.

Figure 10.4. Trafic groupé par adresses IP



Au lieu d'indiquer une limite totale de groupe, vous pouvez également activer l'option *Dynamic Balancing* (Équilibrage dynamique). Cette option permet de garantir que la bande passante disponible est divisée de manière égale entre toutes les adresses quel qu'en soit le nombre et ce, jusqu'à la limite du tuyau. Si une limite totale de

100 bps est également indiquée pour les groupes, comme ci-dessus, alors aucun utilisateur ne pourra obtenir une capacité supérieure à celle de la bande passante.

Limites et garanties des groupes. Outre l'indication d'une limite totale pour les utilisateurs des groupes, il est possible de spécifier des limites pour chaque préférence. Si l'on indique pour les utilisateurs des groupes une limite de 30 bps pour la priorité 2, cela signifie que les utilisateurs associés à une priorité 2 par une règle de tuyau bénéficieront d'une garantie de 30 bps, quel que soit le nombre d'utilisateurs sur le tuyau. De la même manière qu'avec les priorités de tuyau standard, le trafic des utilisateurs de priorité 2 dépassant les 30 bps est affecté à la priorité « meilleur effort ».

En nous basant sur l'exemple précédent, il est possible de limiter la quantité de bande passante garantie obtenue par chaque utilisateur interne pour le trafic entrant SSH. Cela permet d'empêcher qu'un utilisateur utilise l'intégralité de la bande passante disponible de priorité élevée.

Tout d'abord, nous groupons les utilisateurs du tuyau ssh-in de sorte que des limites s'appliquent à chaque utilisateur du réseau interne. Les paquets étant entrants, nous sélectionnons le groupement « Per DestIP » (Par IP de destination) pour le tuyau ssh-in.

Nous indiquons ensuite les limites par utilisateur, en affectant 16 kbps à la limite de priorité 2 pour chacun. En d'autres termes, chaque utilisateur pourra obtenir une garantie de 16 kbps maximum pour le trafic SSH. Si vous le souhaitez, il est également possible de limiter la bande passante totale du groupe pour chaque utilisateur, par exemple à 40 kbps.

Un problème survient lorsque plus de 5 utilisateurs utilisent le SSH simultanément : 16 kbps multiplié par 5 donne un résultat supérieur à 64 kbps. La limite totale du tuyau sera toujours active et chaque utilisateur sera en concurrence pour la bande passante disponible de priorité 2, ainsi que pour la bande passante de basse priorité. Certains utilisateurs continueront à obtenir les 16 kbps, d'autres non.

Il est possible d'activer l'équilibrage dynamique pour améliorer cette situation et garantir que les 5 utilisateurs obtiennent la même quantité de bande passante limitée. Lorsque le cinquième utilisateur commence à générer du trafic SSH, l'équilibrage abaisse la limite par utilisateur à environ 13 kbps (64 kbps divisé par 5 utilisateurs).

L'équilibrage dynamique intervient séparément dans chaque priorité d'un tuyau. En d'autres termes, si les utilisateurs se voient attribuer une petite portion de trafic de priorité élevée et une plus grande quantité de trafic de priorité « meilleur effort », tous obtiendront leur part du trafic de priorité élevée ainsi qu'une part équitable du trafic de priorité « meilleur effort ».

Recommandations

Importance de paramétrer une limite de tuyau. La mise en forme du trafic n'est effective que lorsqu'un tuyau NetDefendOS est *plein*, c'est-à-dire lorsque le trafic qui le traverse a atteint la limite totale autorisée. Si un tuyau de 500 kbps transporte 400 kbps de trafic de faible priorité et 90 kbps de trafic de priorité élevée, il reste alors 10 kbps de bande passante. Il n'y a donc pas lieu de procéder à une réduction de l'encombrement. Il est toutefois important de préciser une limite totale pour un tuyau, de sorte que ce dernier connaisse sa capacité, dont le mécanisme des priorités dépend totalement.

Limites de tuyau pour VPN. La mise en forme du trafic permet de mesurer le trafic circulant dans les tunnels VPN. Il s'agit des données brutes non chiffrées, sans aucun protocole ; ainsi, leur volume est inférieur au trafic VPN réel. Les protocoles VPN tels qu'IPsec (Internet Protocol Security) peuvent ajouter une surcharge considérable aux données. Pour cette raison, il est recommandé que les limites définies dans les tuyaux de mise en forme du trafic soient d'environ 20 % inférieures à la bande passante réelle disponible.

Utilisation de la limite de groupe. Lorsqu'une limite totale de tuyau n'est pas spécifiée, une limite de groupe peut alors être utilisée. La limite de bande passante est ensuite appliquée, par exemple, à chaque utilisateur d'un réseau dont les utilisateurs doivent partager une ressource de bande passante fixe. Un FAI peut utiliser cette approche en vue de limiter la bande passante des utilisateurs individuels, en sélectionnant le groupement « Per DestIP » (Par IP de destination). Il n'est pas important de savoir quand le tuyau est « plein » car la seule limite s'applique à chaque utilisateur. En cas d'utilisation des priorités, le maximum du tuyau doit être utilisé.

Les limites ne doivent pas dépasser la bande passante disponible. Si les limites de tuyau ont une valeur supérieure à la bande passante définie, le tuyau ne pourra pas déterminer quand la connexion physique a atteint sa capacité maximum. Si la connexion atteint 500 kbps et que la limite totale de tuyau est définie à 600 kbps, le tuyau

estimera qu'il n'est pas plein et par conséquent ne réduira pas l'encombrement des priorités inférieures.

Les limites doivent être légèrement inférieures à la bande passante disponible. La valeur définie pour les limites de tuyau doit être légèrement inférieure à la bande passante du réseau. Il est recommandé d'attribuer à la limite de tuyau 95 % de la limite physique. La nécessité de cet écart s'atténue à mesure que la bande passante disponible augmente ; en effet, 5 % représente alors une portion encore plus importante du total.

Une limite inférieure de tuyau est utile dans le cadre du traitement du trafic par NetDefendOS. Pour les connexions sortantes, où les paquets quittent le firewall D-Link, il existe toujours la possibilité que NetDefendOS surcharge légèrement la connexion en raison des retards logiciels entraînés par la décision d'envoyer les paquets et les paquets réellement expédiés des mémoires tampons.

Pour les connexions entrantes, le contrôle est moindre quant au trafic entrant et devant être traité par le sous-système de mise en forme du trafic ; par conséquent, il est plus important de définir des limites de tuyau légèrement inférieures à la limite de connexion réelle de façon à prendre en compte le temps nécessaire à NetDefendOS pour s'adapter à l'évolution des conditions.

Attaques visant la bande passante. La mise en forme du trafic ne peut pas contrer les attaques en force des ressources entrantes, telles que les attaques par déni de service ou les attaques par inondation. NetDefendOS empêche ces paquets parasites d'atteindre les hôtes situés derrière le firewall D-Link, mais ne peut pas protéger la connexion en surcharge visée par une attaque par inondation.

Surveillance des fuites. Lorsque vous effectuez les paramétrages visant à protéger et à mettre en forme un goulot d'étranglement du réseau, assurez-vous que l'intégralité du trafic traversant ce goulot d'étranglement traverse également les tuyaux NetDefendOS définis.

Si du trafic non détecté par les tuyaux passe par votre connexion Internet, ces derniers ne peuvent pas savoir quand la connexion Internet est saturée.

Les problèmes causés par les fuites sont exactement identiques à ceux rencontrés dans les scénarios décrits ci-dessus. Lorsque du trafic « s'échappe » sans avoir été mesuré par les tuyaux, il se produit les mêmes conséquences que lorsque la bande passante est absorbée par des tiers non contrôlés par l'administrateur mais qui partagent la même connexion.

Dépannage. Pour mieux comprendre ce qui se passe dans une configuration active, vous pouvez utiliser la commande console suivante :

```
pipe -u <pipename>
```

Cette commande vous permet d'afficher la liste des utilisateurs actuellement actifs dans chaque tuyau.

Récapitulatif de la mise en forme du trafic

La mise en forme du trafic NetDefendOS fournit un ensemble sophistiqué de mécanismes pour le contrôle et la hiérarchisation des paquets réseau. Les points suivants récapitulent son utilisation :

Sélection du trafic à gérer via les *règles des tuyaux*.

Les règles des tuyaux envoient le trafic via les *tuyaux*.

Une limite peut être définie pour un tuyau et correspondre à la quantité de trafic maximum autorisée.

Un tuyau peut déterminer qu'il est *plein* uniquement si une limite est spécifiée.

Un seul tuyau doit gérer le trafic dans une seule direction (même si les tuyaux bidirectionnels sont autorisés).

Les tuyaux peuvent être mis en chaîne de sorte que le trafic d'un tuyau alimente un autre tuyau.

Certains types de trafic peuvent être associés à une *priorité* dans un tuyau.

Les priorités peuvent se voir attribuer une limite maximum, qui correspond à une garantie. Le trafic qui dépasse cette limite est envoyé au niveau de priorité minimum, ou priorité *« meilleur effort »*.

Tous les paquets de priorité « meilleur effort » sont traités selon le principe du « premier arrivé, premier transféré ».

Dans un tuyau, le trafic peut être divisé par *groupes*, par adresse IP source, par exemple. Chaque utilisateur d'un groupe (par exemple, chaque adresse IP source) peut se voir attribuer une limite maximum. Les priorités d'un groupe peuvent être associées à une limite/garantie.

Il est inutile de spécifier une limite de tuyau si les membres du groupe sont associés à une limite maximum.

L'*équilibrage dynamique* peut être utilisé pour indiquer que tous les utilisateurs d'un groupe obtiennent une quantité équitable de bande passante.

Règles aux seuils

Présentation

L'objectif d'une *règle au seuil* est de fournir un moyen de détection des activités anormales liées aux connexions et d'y répondre. Par exemple, une activité anormale peut survenir lorsqu'un hôte interne est infecté par un virus qui se connecte de manière répétée à des adresses IP externes, ou lorsqu'une source externe tente d'ouvrir un nombre excessif de connexions. (Dans ce contexte, une « connexion » correspond à tous les types de connexion tels que TCP, UDP ou ICMP, suivis par le moteur d'état NetDefendOS.)

Une règle au seuil est similaire à une règle standard. Il est possible de spécifier une combinaison interface source/destination et réseau source/destination pour une règle et d'y associer un type de service, par exemple HTTP. Chaque règle peut être associée à une ou plusieurs actions, qui indiquent comment gérer les différentes conditions de seuil.

Un seuil présente les paramètres suivants :

Action : réponse au dépassement de la limite : Audit ou Protect (Protéger)

Group By (Grouper par) : Host Based (Basé sur l'hôte) ou Network Based (Basé sur le réseau)

Threshold (Seuil) : limite numérique qui doit être dépassée pour le déclenchement d'une réponse

Threshold Type (Type de seuil) : limite les connexions par seconde ou limite le nombre total de connexions simultanées

Tous ces paramètres sont décrits ci-dessous.

Limite du taux de connexion / du nombre total de connexions

La fonction Connection Rate Limiting (Limite du taux de connexion) permet à l'administrateur d'appliquer une limite au nombre de nouvelles connexions ouvertes par seconde dans le firewall D-Link.

La fonction Total Connection Limiting (Limite du nombre total de connexions) permet à l'administrateur d'appliquer une limite au nombre total de connexions ouvertes dans le firewall D-Link. Cette fonction est très utile lorsque des groupes NAT sont requis en raison du nombre important de connexions générées par des utilisateurs P2P.

Groupement

Les deux groupements suivants sont possibles :

Host Based (Basé sur l'hôte) : le seuil est appliqué séparément aux connexions dont les adresses IP diffèrent.

Network Based (Basé sur le réseau) : le seuil est appliqué à toutes les connexions qui correspondent aux règles.

Actions des règles

Lorsqu'une règle au seuil est déclenchée, l'une des deux réponses suivantes est possible :

Audit : laisser la connexion telle quelle mais consigner l'événement.

Protect (Protéger) : interrompt la connexion déclenchante.

La consignation est préférable si la valeur de déclenchement appropriée ne peut être déterminée au préalable. On peut appliquer des actions multiples pour une règle donnée ; par exemple l'action peut être Audit pour un seuil donné et devenir Protect (Protéger) pour un seuil supérieur.

Actions multiples

Lorsqu'une règle est déclenchée, NetDefendOS effectue les actions associées qui correspondent à la condition survenue. Si plusieurs actions correspondent à la condition, elles sont alors appliquées dans leur ordre d'apparition sur l'interface utilisateur.

Si plusieurs actions associées à la même combinaison de type et de groupement (voir ci-dessus pour la définition de ces termes) sont déclenchées au même moment, seule l'action présentant la valeur de seuil la plus élevée sera consignée.

Connexions dispensées

Certains paramètres avancés intitulés *BeforeRules* (Avant les règles) peuvent empêcher certains types de connexion de gestion à distance d'être examinés par l'ensemble de règles NetDefendOS. Ces paramètres dispensent également les connexions des règles aux seuils.

Règles aux seuils et ZoneDefense

Les règles aux seuils sont utilisées dans la fonction ZoneDefense de D-Link afin de bloquer les tentatives de connexions excessives provenant des hôtes internes. Pour plus d'informations à ce sujet, reportez-vous au chapitre 12, *ZoneDefense*.

Fonction de « blacklisting » des règles aux seuils

Si l'option Protect (Protéger) est sélectionnée, les règles aux seuils peuvent être configurées de telle sorte que la source qui a déclenché la règle soit automatiquement ajoutée à une *blacklist* (liste noire) d'adresses IP ou de réseaux. Si plusieurs actions Protect (Protéger) pour lesquelles la fonction de « blacklisting » est activée sont déclenchées au même moment, seule la première sera exécutée par NetDefendOS.

Lorsque la fonction de « blacklisting » est activée pour une action basée sur l'hôte, cette dernière ajoute à la blacklist un seul hôte lorsqu'elle est déclenchée. Lorsque la fonction de « blacklisting » est activée pour une action basée sur le réseau, cette dernière ajoute à la blacklist le réseau source associé à la règle. Si la règle au seuil est associée à un service, il est possible de bloquer ce service uniquement.

Lorsque la fonction de « blacklisting » est activée, l'administrateur peut décider que les connexions existantes provenant de la source déclenchante peuvent être laissées telles quelles ou interrompues.

Il est également possible de paramétrer la durée, en secondes, pendant laquelle la source est mise sur liste noire.

Cette option est décrite en détail dans la section intitulée « Blacklisting des hôtes et réseaux ».

Équilibrage du volume de trafic du serveur

Présentation

La fonction d'*équilibrage du volume de trafic du serveur* (SLB) de NetDefendOS est un outil puissant qui permet d'améliorer les aspects suivants des applications réseau :

Performances

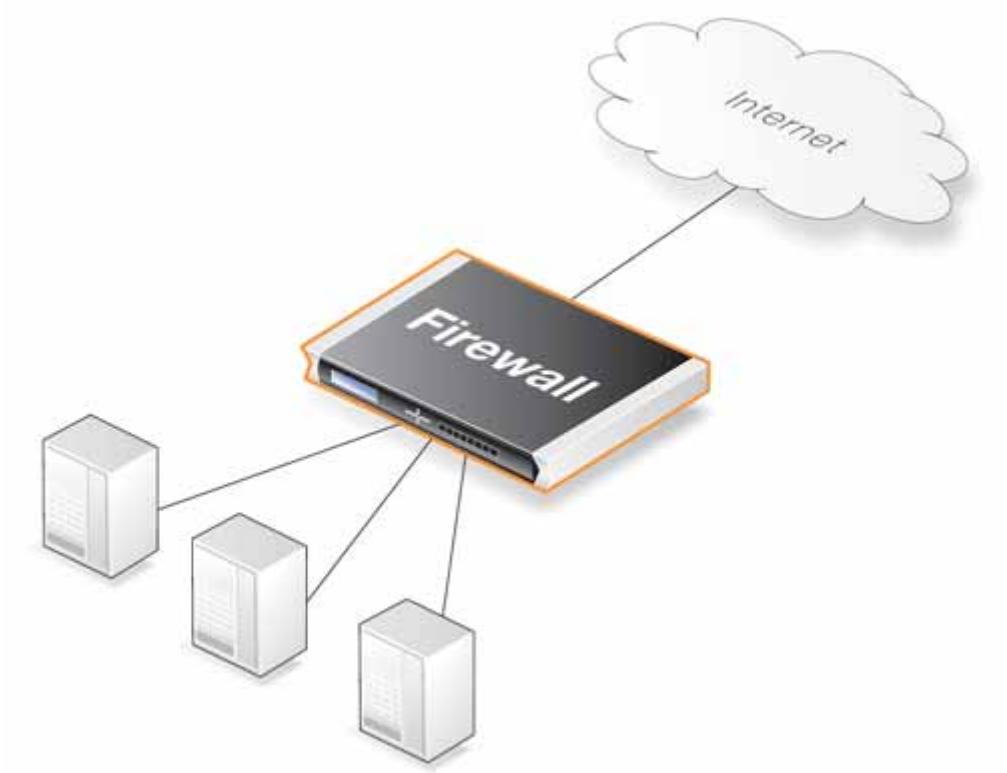
Évolutivité

Fiabilité

Facilité d'administration

La fonction SLB permet de partager entre plusieurs serveurs les demandes de service réseau. Elle permet d'améliorer à la fois les performances et l'évolutivité des applications en permettant à un cluster de serveurs (ou « ferme de serveurs ») de gérer un nombre de requêtes bien plus important qu'un seul serveur. La figure ci-dessous illustre un scénario SLB habituel, où l'accès Internet aux applications est contrôlé par un firewall D-Link.

Figure 10.5. Exemple de configuration de l'équilibrage du volume de trafic du serveur



Outre l'amélioration des performances, la fonction SLB permet d'augmenter la fiabilité des applications réseau en surveillant activement les serveurs qui partagent la charge. La fonction SLB peut détecter la défaillance ou la congestion d'un serveur et cesse d'acheminer les requêtes vers ce serveur jusqu'à sa reprise ou jusqu'à la réduction de la charge.

La fonction SLB permet également aux administrateurs réseau d'effectuer des tâches de maintenance sur les serveurs ou les applications et ce, sans avoir à interrompre les services. Chaque serveur peut être redémarré, mis à niveau, supprimé ou remplacé et de nouveaux serveurs et nouvelles applications peuvent être ajoutés ou déplacés sans affecter le reste de la grappe de serveurs ni manipuler les applications.

Par ailleurs, la combinaison de la surveillance du réseau et de la répartition de la charge offre un niveau supplémentaire de protection contre les attaques par déni de service.

La fonction SLB de NetDefendOS est mise en œuvre via l'utilisation des règles *SLB_SAT* dans l'ensemble de règles IP. Ces règles proposent aux administrateurs plusieurs algorithmes visant à répartir la charge. Cela permet d'adapter au mieux la fonction SLB aux besoins du réseau.

Lorsque vous utilisez la fonction SLB, pensez aux quatre éléments suivants :

les serveurs cible sur lesquels la charge doit être équilibrée ;

le mode de répartition de la charge ;

l'algorithme SLB utilisé ;

le mode de surveillance.

Tous ces points sont décrits dans les sections suivantes.

Identification des serveurs

La première étape consiste à identifier les serveurs sur lesquels la charge doit être équilibrée. Il peut s'agir d'une *grappe de serveurs*, c'est-à-dire un cluster de serveurs paramétrés pour fonctionner comme un seul « serveur virtuel ». Vous devez indiquer les serveurs devant être traités par la fonction SLB comme un seul serveur virtuel.

Mode de répartition de la charge

Aucune méthode de répartition du volume de trafic du serveur n'est idéale pour tous les services. Chaque type de service présente des besoins différents. L'administrateur peut configurer des règles pour chaque service dans l'ensemble de règles IP. La fonction SLB filtre ensuite le flux de paquets en fonction de ces règles.

La fonction SLB de NetDefendOS prend en charge les modes de répartition suivants :

Per-state Distribution (Répartition par état) La fonction SLB enregistre l'état de toutes les connexions. L'intégralité de la session est ensuite répartie sur un même serveur. Ce mode garantit une transmission fiable des données pour cette session.

IP Address Stickiness (Persistance de l'adresse IP) Toutes les connexions d'un client spécifique sont envoyées à un même serveur. Ce mode est particulièrement important pour les services SSL tels que HTTPS, qui exigent une connexion constante à un même hôte.

Network Stickiness (Persistance du réseau) Ce mode est identique au précédent hormis le fait que l'utilisation d'un masque de sous-réseau permet d'indiquer une plage d'hôtes de sous-réseau.

Algorithme de répartition

Il existe plusieurs façons de déterminer comment une charge est partagée sur une grappe de serveurs. La fonction SLB de NetDefendOS prend en charge les algorithmes suivants :

Round Robin (RR) L'algorithme répartit les nouvelles connexions entrantes vers une liste de serveurs à tour de rôle. Pour la première connexion, l'algorithme choisit un serveur au hasard et lui affecte la connexion. Pour les connexions suivantes, l'algorithme se répète dans la liste de serveurs et redirige la charge vers les serveurs, dans l'ordre. Quels que soient la capacité des serveurs ainsi que d'autres aspects les concernant (le nombre de connexions existantes sur un serveur et son temps de réponse, par exemple), tous les serveurs disponibles reçoivent à tour de rôle la connexion suivante.

Cet algorithme garantit que chaque serveur reçoit le même nombre de requêtes ; par conséquent, il est particulièrement adapté aux grappes de serveurs présentant des capacités identiques et dont les charges de traitement des requêtes sont potentiellement similaires.

Connection Rate (Taux de connexion) Cette algorithme prend en compte le nombre de requêtes reçu par chaque serveur sur un intervalle donné. La fonction SLB envoie la requête suivante au serveur ayant reçu le moins de connexions durant cet intervalle. L'administrateur peut indiquer l'intervalle à utiliser avec cet algorithme.

Si l'algorithme Connection Rate (Taux de connexion) est utilisé sans persistance, il se comporte de la même manière que l'algorithme Round Robin, qui affecte les nouvelles connexions aux serveurs selon un ordre précis. Il se comporte également comme l'algorithme Round Robin sides clients avec une nouvelle adresse IP effectuent en permanence une connexion.

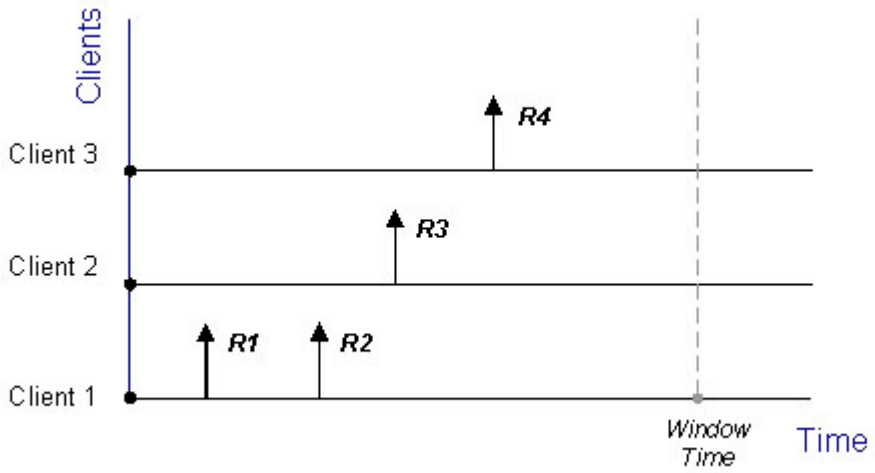
L'utilisation de cet algorithme est réellement avantageuse avec les modes de répartition « persistance » lorsque les clients effectuent plusieurs connexions. L'algorithme Connection Rate (Taux de connexion) garantit une répartition des nouvelles connexions entre les serveurs aussi équitable que possible. Avant que l'intervalle

n'atteigne le délai d'expiration de persistance défini, les nouvelles connexions entrantes provenant d'une même adresse IP qu'une connexion précédente sont affectées au même serveur. Les connexions associées à une nouvelle adresse sont redirigées vers le serveur présentant le taux de connexion le plus bas. Cet algorithme a pour objectif de réduire la charge des nouvelles connexions pour un serveur ; néanmoins, la répartition peut s'avérer inégale si le client d'une adresse IP envoie un grand nombre de nouvelles connexions sur une courte période et que les autres serveurs reçoivent un nombre de connexions inférieur.

Dans l'interface de gestion, la fenêtre de temps est variable pour le décompte inversé des secondes qui récapitule le nombre de nouvelles connexions pour l'algorithme Connection Rate (Taux de connexion). Par défaut, la valeur 10 est utilisée, de sorte que le nombre de nouvelles connexions effectuées sur chaque serveur au cours des 10 dernières secondes est enregistré.

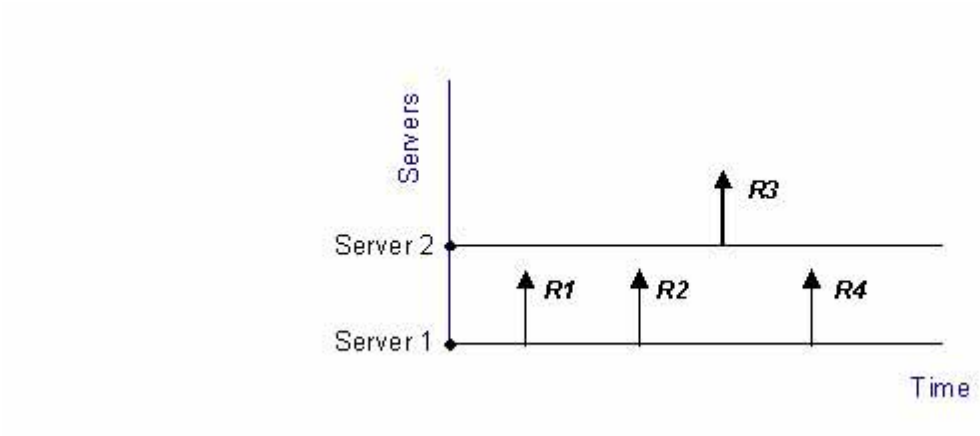
Un exemple est illustré dans la figure ci-dessous. Dans cet exemple, le firewall D-Link est chargé d'équilibrer sur 2 serveurs les connexions de 3 clients associés à des adresses différentes. Un mode de répartition « persistance » est activé.

Figure 10.6. Connexions provenant de trois clients



Lorsque l'algorithme Round Robin est utilisé, les premières requêtes entrantes R1 et R2 du Client 1 sont affectées à un serveur, disons le Serveur 1, conformément au mode « persistance ». La requête suivante, R3, du Client 2 est ensuite acheminée vers le Serveur 2. Lorsque la requête R4 du Client 3 arrive, le Serveur 1 reprend son tour et se voit affecter R4.

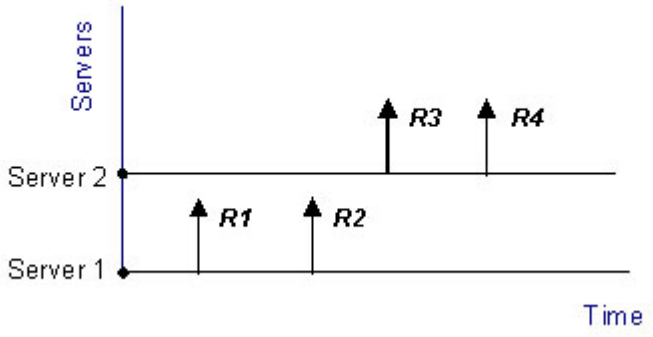
Figure 10.7. Mode « persistance » et algorithme Round-Robin



Si l'on choisit d'utiliser l'algorithme Connection Rate (Taux de connexion), les requêtes R1 et R2 sont envoyées vers le même serveur en raison du mode « persistance ». Cependant, les requêtes suivantes, R3 et R4, sont acheminées vers un autre serveur étant donné que le nombre de nouvelles connexions sur chaque serveur défini

dans la fenêtre de temps est comptabilisé pour la répartition.

Figure 10.8. Mode « persistance » et algorithme Connection Rate (Taux de connexion)



Quel que soit l'algorithme choisi, le trafic est redirigé vers d'autres serveurs en cas de défaillance du serveur. À la reprise du serveur, ce dernier peut être automatiquement réintégré à la grappe de serveurs et recevoir à nouveau les requêtes.

Surveillance de l'état des serveurs

La fonction SLB utilise la *surveillance de l'état des serveurs* pour vérifier en permanence la condition des serveurs dans une configuration SLB. La fonction SLB surveille différentes couches OSI afin de contrôler le taux de connexion de chaque serveur, ainsi que son état actuel. En cas de défaillance du serveur et quel que soit l'algorithme utilisé, la fonction SLB n'envoie plus de requêtes vers ce serveur jusqu'à sa reprise totale.

La fonction SLB utilise la table de routage par défaut, sauf si l'administrateur définit un emplacement de table de routage spécifique.

La fonction SLB de D-Link fournit les modes de surveillance suivant :

ICMP Ping (Ping ICMP) Fonctionne au niveau de la couche OSI 3. La fonction SLB exécute la commande ping sur l'adresse IP de chaque serveur de la ferme. Cela permet de détecter les serveurs défaillants.

TCP Connection (Connexion TCP) Fonctionne au niveau de la couche OSI 4. La fonction SLB tente de connecter à chaque serveur un port spécifique. Par exemple, s'il est indiqué qu'un serveur exécute les services Web sur le port 80, la fonction SLB envoie une requête TCP SYN à ce port. Si la fonction SLB ne reçoit pas de paquet TCP SYN/ACK en réponse, elle marque le port 80 de ce serveur comme défaillant. La fonction SLB identifie les conditions *pas de réponse*, *réponse normale* ou *réponse port fermé* provenant des serveurs.

Règles SLB_SAT

La définition de la règle *SLB_SAT* dans l'ensemble de règles IP constitue le composant clé de la configuration de la fonction SLB. Voici les étapes à suivre :

Définir un objet pour chaque serveur devant être soumis à la fonction SLB.

Définir un groupe qui contient tous ces objets.

Définir une règle SLB_SAT dans l'ensemble de règles IP qui se rapporte au groupe défini et dans lequel tous les autres paramètres SLB sont définis.

Définir une règle supplémentaire qui copie l'interface source/destination et le réseau source/destination de la règle SLB_SAT autorisant le trafic. Il peut exister une ou plusieurs combinaisons des éléments suivants :

ForwardFast

Allow (Autoriser)

NAT

Le tableau ci-dessous présente les règles qui seraient définies dans le cadre d'un scénario typique où l'on équilibre le volume du trafic d'un ensemble de serveurs Web situés derrière un firewall D-Link. La règle ALLOW permet aux clients externes d'accéder aux serveurs Web.

Nom de la règle	Type de règle	Interface source	Réseau source	Interface de destination	Réseau de destination
WEB_SLB	SLB_SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	ip_ext
WEB_SLB_ALW	ALLOW	any (toutes)	all-nets (tout réseau)	core (noyau)	ip_ext

Si des clients se trouvent sur le même réseau que les serveurs Web et qu'ils doivent aussi accéder à ces derniers, une règle NAT est également utilisée :

Nom de la règle	Type de règle	Interface source	Réseau source	Interface de destination	Réseau de destination
WEB_SLB	SLB_SAT	any (toutes)	all-nets (tout réseau)	core (noyau)	ip_ext
WEB_SLB_NAT	NAT	lan	lannet	core (noyau)	ip_ext
WEB_SLB_ALW	ALLOW	any (toutes)	all-nets (tout réseau)	core (noyau)	ip_ext

Notez que l'interface de destination est indiquée en tant que « core », ce qui signifie que NetDefendOS s'en charge lui-même. L'avantage clé d'une règle distincte ALLOW est que les serveurs Web peuvent consigner l'adresse IP exacte qui génère les requêtes. Si l'on utilise uniquement une règle NAT, ce qui est possible, les serveurs Web peuvent uniquement voir l'adresse IP du firewall D-Link.

Exemple 10.3. Configuration de la fonction SLB

Dans cet exemple, l'équilibrage du volume du trafic de serveur doit s'effectuer entre 2 serveurs Web HTTP situés derrière un firewall D-Link. Ces deux serveurs Web sont respectivement associés aux adresses IP privées *192.168.1.10* et *192.168.1.11*. Les valeurs SLB par défaut sont utilisées pour la surveillance, le mode de répartition et la « persistance ».

Une règle NAT est utilisée avec la règle SLB_SAT, de telle sorte que les clients situés derrière le firewall puissent accéder aux serveurs Web. Une règle ALLOW est utilisée pour autoriser l'accès aux clients externes.

Interface Web

A. Créez un objet pour chaque serveur Web :

Sélectionnez Objects > Address Book > Add > IP Address (Objets > Carnet d'adresses > Ajouter > Adresse IP).

Saisissez un nom adapté, par exemple *server1*.

Saisissez l'adresse IP *192.168.1.10*.

Cliquez sur OK.

Répétez l'opération ci-dessus de façon à créer un objet intitulé *server2* pour l'adresse IP *192.168.1.11*.

B. Créez un groupe contenant les deux objets de serveur Web :

Sélectionnez Objects > Address Book > Add > IP4 Group (Objets > Carnet d'adresses > Ajouter > Groupe IP4).

Saisissez un nom adapté, par exemple *server_group*.

Ajoutez au groupe les objets *server1* et *server2*.

Cliquez sur OK.

C. Spécifiez la règle IP SLB_SAT :

Sélectionnez Rules > IP Rule Sets > main > Add > IP Rule (Règles > Ensembles de règles IP > principal > Ajouter > Règle IP).

Saisissez les éléments suivants :

Name (Nom) : Web_SLB

Action : SLB_SAT

Service : HTTP

Source Interface (Interface source) : any (toutes)

Source Network (Réseau source) : all-nets (tout réseau)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : ip_ext

Sélectionnez l'onglet SAT SLB.

Sous Server Addresses (Adresses des serveurs), ajoutez *server_group* à la valeur Selected (Sélection).

Cliquez sur OK.

D. Spécifiez une règle IP NAT correspondante pour les clients internes :

Sélectionnez Rules > IP Rule Sets > main > Add > IP Rule (Règles > Ensembles de règles IP > principal > Ajouter > Règle IP).

Saisissez les éléments suivants :

Name (Nom) : Web_SLB_NAT

Action : NAT

Service : HTTP

Source Interface (Interface source) : lan

Source Network (Réseau source) : lannet

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : ip_ext

Cliquez sur OK.

E. Spécifiez une règle IP ALLOW pour les clients externes :

Sélectionnez Rules > IP Rule Sets > main > Add > IP Rule (Règles > Ensembles de règles IP > principal > Ajouter > Règle IP).

Saisissez les éléments suivants :

Name (Nom) : Web_SLB_ALW

Action : ALLOW

Service : HTTP

Source Interface (Interface source) : any (toutes)

Source Network (Réseau source) : all-nets (tout réseau)

Destination Interface (Interface de destination) : core (noyau)

Destination Network (Réseau de destination) : ip_ext

Cliquez sur OK.

Chapitre 11. Haute disponibilité

Le présent chapitre présente la fonction de tolérance aux pannes de haute disponibilité des firewalls D-Link.

Présentation

High Availability (HA) est une fonction de tolérance aux pannes disponibles sur certains modèles de firewalls D-Link. Actuellement, les firewalls offrant cette fonction sont les modèles DFL-1600 et DFL-2500. Les licences préinstallées pour ces modèles incluent la prise en charge de la fonction HA.

Clusters HA. La fonction *High Availability* (HA) de D-Link consiste à ajouter un firewall D-Link de sauvegarde *esclave* à un firewall *maître* existant. Le maître et l'esclave sont connectés l'un à l'autre et composent un *cluster HA* logique. L'une des unités d'un cluster est *active* tandis que l'autre est *inactive* et en mode veille. Au départ, l'esclave est inactif et surveille le maître. S'il détecte une absence de réponse du maître, un *failover* (basculement) a lieu et l'esclave devient actif. Par la suite, si le maître retrouve ses pleines fonctionnalités, l'esclave reste actif et le maître surveille à son tour l'esclave. Un nouveau failover (basculement) a lieu uniquement en cas de défaillance de l'esclave. Ce processus est également appelé mise en œuvre HA *active-passive*.

Unité *maître* et unité *active*. N'oubliez pas que l'unité *maître* d'un cluster n'est pas toujours l'unité *active*. L'unité *active* correspond au firewall D-Link qui traite l'intégralité du trafic à un moment donné. Elle peut également être l'unité *esclave* si un failover (basculement) a eu lieu en raison de la défaillance du *maître*.

Interconnexion. Dans un cluster, l'unité maître et l'unité esclave doivent être directement connectées l'une à l'autre via une connexion de synchronisation, que NetDefendOS considère comme l'interface de synchronisation. L'une des interfaces normales du maître et de l'esclave est dédiée à l'interconnexion et ces derniers sont connectés l'un à l'autre par le biais d'un câble croisé.

Gestion du cluster. Un cluster HA composé de deux firewalls D-Link est géré comme une unité unique, avec un nom de cluster unique, qui apparaît dans l'interface de gestion comme un seul firewall D-Link logique. Les opérations d'administration, par exemple le changement des règles dans l'ensemble de règles IP, sont effectuées normalement ; les modifications sont automatiquement apportées aux configurations du maître et de l'esclave.

Partage de la charge. Les clusters HA D-Link ne proposent pas le partage de charge. En effet, une seule unité est active tandis que l'autre est inactive et il ne peut exister que deux firewalls D-Link, le maître et l'esclave, dans un même cluster. La seule fonction de traitement effectuée par l'unité inactive consiste à répliquer l'état de l'unité active et de prendre à sa charge le traitement de l'intégralité du trafic si elle détecte une absence de réponse de l'unité active.

Duplication du matériel. La fonction HA de D-Link fonctionne uniquement entre deux firewalls D-Link. Le fonctionnement interne des différents logiciels de passerelle de sécurité étant complètement dissemblable, aucune méthode commune n'est disponible pour communiquer des informations d'état à un périphérique différent.

Par ailleurs, il est fortement recommandé que les firewalls D-Link utilisés dans le cluster présentent la même configuration. Il doivent également disposer des mêmes licences qui permettent des fonctions identiques, y compris la capacité d'opérer dans un cluster HA.

Redondance étendue. La mise en œuvre d'un cluster HA permet de supprimer un point de défaillance dans un réseau. Toutefois, les routeurs, les switches et les connexions Internet peuvent représenter des points de défaillance potentiels. Ils doivent par conséquent être examinés.

Les sections suivantes décrivent en détail la fonction High Availability (HA).

Mécanismes HA

La fonction HA de D-Link fournit une configuration matérielle redondante avec synchronisation des états. L'état de l'unité active, par exemple la table de connexion et d'autres informations cruciales, est en permanence copié vers l'unité inactive via l'interface de synchronisation. En cas de failover (basculement) du cluster, l'unité inactive est informée des connexions actives et le trafic peut se poursuivre.

Le système inactif repère que le système actif n'est plus opérationnel lorsqu'il ne détecte plus suffisamment de *pulsations du cluster*. Les pulsations sont envoyées vers l'interface de synchronisation, ainsi que vers les autres interfaces. NetDefendOS envoie 5 pulsations par seconde depuis le système actif ; lorsque 3 pulsations sont manquantes (c'est-à-dire après 0,6 secondes), un failover (basculement) est mis en place. En envoyant les pulsations vers toutes les interfaces, l'unité inactive dispose d'une vue générale de l'état de l'unité active. Même lorsque la synchronisation est délibérément déconnectée, le failover (basculement) peut ne pas survenir si l'unité inactive reçoit suffisamment de pulsations des autres interfaces via un switch partagé. Toutefois, l'interface de synchronisation envoie deux fois plus de pulsations que les interfaces normales. L'administrateur peut désactiver l'envoi de pulsations au niveau de n'importe quelle interface.

Les pulsations ne sont pas envoyées plus fréquemment car des retards peuvent survenir au cours d'opérations normales. Par exemple, l'ouverture d'un fichier peut entraîner des retards suffisamment importants pour que le système inactif devienne actif, même si l'autre système est resté actif.

Les pulsations de cluster présentent les caractéristiques suivantes :

L'adresse IP source est l'adresse de l'interface du firewall source.

L'adresse IP de destination est l'adresse IP partagée.

La durée de vie (TTL) a toujours pour valeur 255. Si NetDefendOS reçoit une pulsation de cluster avec une durée de vie différente, on considère que le paquet a traversé un routeur et qu'il n'est par conséquent pas fiable.

Il s'agit d'un paquet UDP, envoyé du port 999 au port 999.

L'adresse MAC de destination est l'adresse Ethernet à multidiffusion correspondant à l'adresse matérielle partagée. En d'autres termes, *11-00-00-C1-4A-nn*. Pour plus de sécurité, on utilise des multidiffusions de niveau lien à la place des paquets normaux unicast ; en effet, avec l'utilisation de paquets unicast, il est possible qu'un pirate local leurre les switches pour détourner les pulsations, de sorte que le système inactif ne les reçoive jamais.

En général, le failover (basculement) prend environ une seconde ; par conséquent, les clients peuvent rencontrer une légère perte de paquets en rafale. Dans le cas du protocole TCP, la durée nécessaire au failover (basculement) ne dépasse pas le délai d'attente normal de retransmission ; les paquets perdus sont alors retransmis très rapidement et la communication se poursuit. Peu fiable par nature, le protocole UDP ne permet pas la retransmission.

Le maître et l'esclave connaissent les adresses IP partagées. Le système actif répond aux requêtes ARP concernant l'adresse IP partagée ou toute autre adresse IP publiée via la section de configuration ARP ou le proxy ARP. L'adresse matérielle de l'adresse IP partagée et des autres adresses publiées n'est pas associée aux adresses matérielles des interfaces. Au lieu de cela, l'adresse MAC est créée par NetDefendOS à partir de l'ID cluster au format suivant : 10-00-00-C1-4A-nn. La valeur nn provient de la combinaison de l'ID cluster configuré dans la section des paramètres avancés et du bus/emplacement/port matériel de l'interface. L'ID cluster doit être unique pour chaque cluster d'un réseau.

Étant donné que l'adresse matérielle de l'adresse IP partagée est toujours la même, aucun temps de latence n'est constaté au moment du failover (basculement) lorsque les caches ARP des unités associées au même LAN que le cluster sont mis à jour.

Lorsqu'un membre d'un cluster découvre qu'un autre membre n'est pas opérationnel, il diffuse des requêtes ARP gratuites sur toutes les interfaces, en utilisant l'adresse matérielle partagée en tant qu'adresse d'expéditeur. Cela permet aux switches de réassimiler en quelques millisecondes où envoyer les paquets destinés à l'adresse partagée. Par conséquent, le seul retard de failover (basculement) est causé par la détection de l'unité active défaillante.

Les requêtes ARP sont également diffusées à intervalles réguliers afin de garantir que les switches n'oublient pas où envoyer les paquets destinés à l'adresse matérielle partagée.

Configuration de la fonction HA

Cette section présente les étapes à suivre pour configurer un cluster HA.

Configuration matérielle

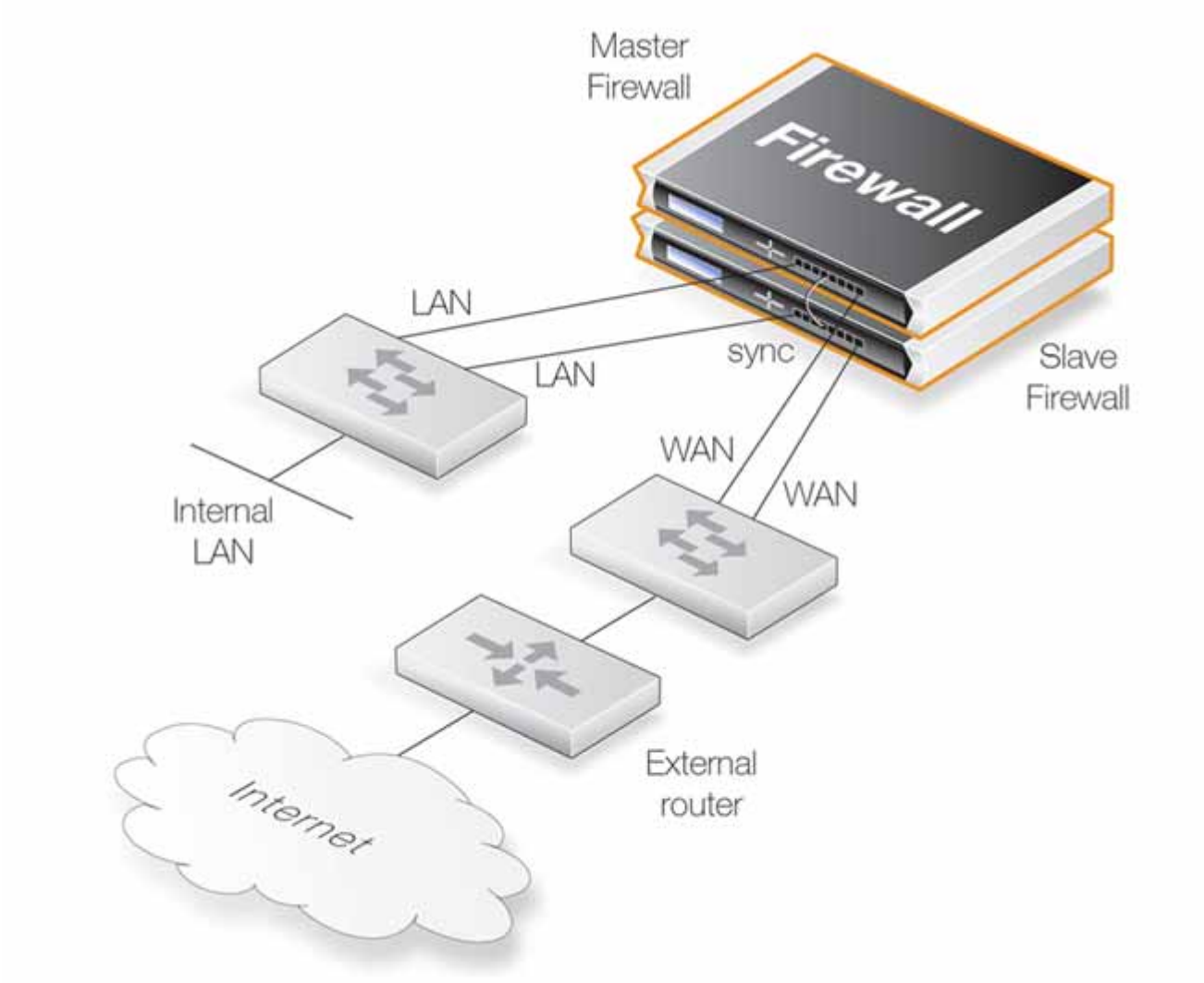
Commencez par vous procurer deux firewalls D-Link physiquement identiques. Ils peuvent tous deux être neufs ou l'un d'eux peut avoir été acheté en vue de servir d'unité de sauvegarde (en d'autres termes, d'unité esclave).

Effectuez les connexions physiques :

Connectez les interfaces correspondantes du maître et de l'esclave via un switch commun.

Sélectionnez une interface sur le maître et sur l'esclave, que les unités utiliseront afin de se surveiller mutuellement. Ensuite, connectez-les ensemble à l'aide d'un câble croisé Ethernet. Il s'agit de l'interface de synchronisation de NetDefendOS. Il est recommandé d'utiliser la même interface pour le maître et l'esclave si l'on considère qu'il s'agit de systèmes similaires.

Figure 11.1. Configuration HA



L'illustration ci-dessus présente les connexions typiques de cluster HA. Toutes les interfaces du maître doivent normalement être présentes sur l'esclave et être connectées aux mêmes réseaux. Pour cela, vous devez connecter via un switch les mêmes interfaces du maître et de l'esclave aux autres parties du réseau. L'interface LAN du maître et celle de l'esclave doivent être connectées au même switch, qui se connecte à son tour à un réseau interne. De la même façon, l'interface WAN du maître et celle de l'esclave doivent se connecter à un switch, qui se connecte à son tour à l'Internet externe.

Choisissez une adresse IP partagée pour chaque interface du cluster. Certaines interfaces ne peuvent partager

des adresses qu'avec celles qui présentent également des adresses individuelles uniques. Les adresses partagées et les adresses uniques sont utilisées comme suit :

Les adresses uniques non partagées servent à communiquer avec les firewalls D-Link pour des fonctions telles que le contrôle à distance et la surveillance. Elles peuvent également faire l'objet d'une commande ping. Elles ne doivent pas être associées au trafic qui traverse le cluster. Si l'une des unités est inopérante, l'adresse IP associée sera inaccessible. Le firewall propriétaire de l'adresse IP répond aux requêtes ARP des adresses respectives à l'aide de l'adresse matérielle normale, selon la même procédure que pour les unités IP normales.

L'adresse IP partagée qui est utilisée pour le routage est également l'adresse utilisée par la traduction d'adresses dynamiques, sauf si la configuration indique explicitement une autre adresse.

Remarque

L'adresse IP partagée ne doit pas être utilisée pour la gestion à distance ou à des fins de surveillance. Par exemple, lorsque vous utilisez SSH pour la gestion à distance des firewalls D-Link dans un cluster HA, vous devez utiliser les adresses IP individuelles des firewalls.

Configuration de NetDefendOS

Les étapes suivantes concernent la configuration du logiciel NetDefendOS via l'interface utilisateur Web :

Connectez-vous à l'unité maître via l'interface utilisateur Web.

Sélectionnez System > High Availability (Système > Haute disponibilité).

Cochez la case Enable High Availability (Activer Haute disponibilité).

Définissez l'ID cluster. Il doit être unique pour chaque cluster.

Choisissez l'interface de synchronisation.

Sélectionnez le type de nœud *Master* (Maître).

Sélectionnez Objects > Address book (Objets > Carnet d'adresses) et créez un objet d'adresse HA IP4 pour chaque interface. Chaque objet doit contenir l'adresse IP du maître et de l'esclave.

Sélectionnez Interfaces > Ethernet, accédez à chaque interface de la liste et saisissez l'adresse IP partagée de chacune dans le champ IP Address (Adresse IP).

Ensuite, sélectionnez l'onglet Advanced (Avancé) pour chaque interface et indiquez dans le champ High Availability Private IP Address (Adresse IP privée haute disponibilité) le nom de l'objet HA IP4 défini pour l'interface au cours de l'étape précédente (NetDefendOS sélectionne automatiquement l'adresse appropriée à partir des adresses IP maître et esclave définies pour l'objet).

Répétez les étapes ci-dessus pour le deuxième Firewall D-Link, mais en sélectionnant le type de nœud *Slave* (Esclave).

La configuration doit être identique pour les deux firewalls D-Link. La configuration est automatiquement synchronisée entre les unités. Pour modifier la configuration, connectez-vous au maître ou à l'esclave, apportez les modifications souhaitées et procédez au déploiement. Les changements sont automatiquement répercutés sur les deux unités.

Vérification du fonctionnement du cluster

Pour vérifier le bon fonctionnement du cluster, utilisez tout d'abord une commande ha sur chaque unité. Le résultat obtenu se présentera comme suit pour le maître :

```
> ha

This device is an HA MASTER
This device is currently ACTIVE (will forward traffic)
HA cluster peer is ALIVE
```

Utilisez ensuite la commande stat pour vérifier que le maître et l'esclave présentent tous deux à peu près le même nombre de connexions. Le résultat obtenu doit inclure une ligne comme suit :

```
Connections 2726 out of 128000
```

où le plus petit nombre correspond au nombre de connexions et le nombre le plus élevé représente la limite de connexions de la licence.

Vous devez également tenir compte des points suivants pour la configuration du cluster :

S'il ne s'agit pas du premier cluster d'un réseau, le paramètre avancé ClusterID (ID cluster) doit être modifié de façon à présenter une valeur unique (la valeur par défaut est 0). Cela permet de garantir que l'adresse MAC du cluster est unique.

Il est également recommandé d'activer le paramètre HAUseUniqueSharedMacAddressPerInterface (HA, Utiliser une adresse MAC partagée unique par interface), de sorte que chaque interface possède sa propre adresse MAC. Lorsque ce paramètre n'est pas activé, les interfaces partagent la même adresse MAC, ce qui peut désorienter certains switches.

Assurez-vous que le paramètre avancé HighBuffers (Mémoire tampon importante) est défini sur *automatique* sur toutes les unités d'un cluster. Ce paramètre alloue de la mémoire pour la gestion des connexions.

Lorsqu'un cluster présente des dizaines de milliers de connexions simultanées, il peut être nécessaire de définir une valeur supérieure à la valeur automatique. Cependant, des valeurs bien plus importantes peuvent augmenter les temps de latence du débit.

Problèmes liés à la fonction HA

Lors de la gestion et de la configuration d'un cluster HA, gardez à l'esprit les points suivants :

SNMP. Les statistiques SNMP ne sont pas partagées entre le maître et l'esclave. Les gestionnaires SNMP ne disposent pas de fonctions de failover (basculement). Par conséquent, les deux firewalls d'un cluster doivent être interrogés séparément.

Utilisation d'adresses IP individuelles. Les adresses IP individuelles du maître et de l'esclave peuvent être utilisées sans risque uniquement pour la gestion. Si vous les utilisez pour autre chose (par exemple, pour les adresses IP source dans des connexions NAT dynamiques ou pour les services de publication de ces adresses), vous rencontrerez inévitablement des problèmes. En effet, les adresses IP uniques disparaîtront en même temps que le firewall correspondant.

Interfaces défaillantes. Les interfaces défaillantes ne sont pas détectées tant que leur état n'affecte pas le fonctionnement de NetDefendOS. Par conséquent, aucun failover (basculement) n'a lieu si l'unité active peut continuer à envoyer des pulsations à l'unité inactive via l'une de leurs interfaces et ce, même si une ou plusieurs interfaces est inopérante.

Modification de l'ID cluster. Il est recommandé de ne pas changer l'ID cluster dans un environnement de production pour deux raisons. Premièrement, cela modifierait l'adresse matérielle des adresses IP partagées et provoquerait des problèmes pour toutes les unités associées au LAN ; en effet, ces dernières conserveraient l'ancienne adresse matérielle dans leurs caches ARP jusqu'à son expiration. Il faudrait alors nettoyer les caches ARP de ces unités.

Deuxièmement, cela interromprait la connexion entre les firewalls du cluster aussi longtemps qu'ils utilisent des configurations différentes. Les deux firewalls seraient alors actifs en même temps.

Totaux de contrôle non valides dans les paquets de pulsations. Les paquets de pulsations sont délibérément créés avec des totaux de contrôle non valides, de sorte qu'ils ne soient pas acheminés. Certains routeurs peuvent signaler ces totaux de contrôle non valides dans leurs messages consignés.

Chapitre 12. ZoneDefense

Le présent chapitre décrit la fonction ZoneDefense de D-Link.

Présentation

Grâce à la fonction ZoneDefense, un firewall D-Link peut contrôler des switches connectés en local. Vous pouvez utiliser cette fonction comme parade pour empêcher qu'un ordinateur appartenant à un réseau local et infecté par un virus n'infecte à son tour les autres ordinateurs de ce réseau.

Lorsque des hôtes ou des clients d'un réseau se retrouvent infectés par des virus ou par toute autre forme de code malveillant, ils présentent souvent des comportements anormaux qui laissent présager une telle infection (le plus fréquemment, il s'agit de l'ouverture d'un grand nombre de nouvelles connexions pour des hôtes extérieurs).

Grâce à la configuration des *règles avec seuil* et à la fonction ZoneDefense, vous pouvez bloquer de manière dynamique les hôtes ou les réseaux qui dépassent la valeur de seuil définie pour le nombre de connexions. Les seuils sont basés soit sur le nombre de nouvelles connexions établies par seconde, soit sur le nombre total de connexions ouvertes. Ces connexions peuvent être établies par un seul hôte ou par tous les hôtes inclus dans une plage d'adresses réseau CIDR (Classless Inter Domain Routing – routage inter-domaine sans classe) spécifiée. Les adresses IP incluses dans cette plage sont la combinaison d'une adresse IP et de son masque réseau associé.

Lorsque NetDefendOS détecte qu'un hôte ou qu'un réseau a atteint la limite définie, il télécharge via une liaison ascendante les règles ACL (Access Control List - liste de contrôle d'accès) vers les switches appropriés : tout trafic destiné à l'hôte ou au réseau qui présente un comportement inhabituel est alors bloqué. Cet hôte et ce réseau restent ainsi bloqués jusqu'à ce que l'administrateur système les débloque manuellement à l'aide de l'interface Web ou de l'interface de ligne de commande.

Remarque

La fonction ZoneDefense est proposée avec les modèles D-Link DFL-800/860/1600/2500.

Switches ZoneDefense

Vous devez préciser manuellement les informations de switch relatives à chacun des switches qui sera contrôlé par le firewall lors de la configuration de ce dernier. Les informations requises pour contrôler un switch sont les suivantes :

- L'adresse IP de l'interface de gestion du switch
- Le type de modèle du switch
- La chaîne de communauté SNMP (accès en écriture)

La fonction ZoneDefense prend actuellement en charge les switches suivants :

- D-Link DES 3226S (version minimale du firmware : R4.02-B14)
- D-Link DES 3250TG (version minimale du firmware : R3.00-B09)
- D-Link DES 3326S (version minimale du firmware : R4.01-B39)
- D-Link DES 3350SR (version minimale du firmware : R1.02.035)
- D-Link DES 3526 (version minimale du firmware : R3.01-B23)
- D-Link DES 3550 (version minimale du firmware : R3.01-B23)
- D-Link DGS 3324SR (version minimale du firmware : R4.10-B15)

Remarque

Avant d'activer la fonction ZoneDefense, vérifiez que les switches sont dotés des versions minimales requises pour le firmware.

Fonctionnement de ZoneDefense

SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole de la couche d'application conçu pour les cas complexes de gestion réseau. Le protocole SNMP permet aux gestionnaires et aux unités gérées d'un réseau de communiquer entre eux.

Gestionnaires SNMP. Un périphérique de gestion type, tel qu'un firewall D-Link, se sert du protocole SNMP pour surveiller et contrôler les périphériques réseau au sein de l'environnement géré. Le gestionnaire peut se servir de la *chaîne de communauté SNMP* pour interroger les statistiques enregistrées relatives aux périphériques contrôlés. Cette chaîne est comparable à un ID utilisateur ou à un mot de passe ; elle permet d'accéder aux informations sur l'état du périphérique. Si la chaîne de communauté est de type *write (accès en écriture)*, le gestionnaire sera autorisé à modifier l'état du périphérique.

Périphériques gérés. Ces périphériques doivent être compatibles avec le protocole SNMP. C'est le cas des switches D-Link. Ils enregistrent les données relatives aux états dans des bases de données appelées bases d'informations pour la gestion du réseau (MIB - Management Information Base), puis ils transmettent ces données au gestionnaire en réponse aux requêtes SNMP de ce dernier.

Règles avec seuil

Une règle avec seuil va déclencher la fonction ZoneDefense pour qu'elle bloque un hôte spécifique ou tout un réseau si le nombre de connexions dépasse la valeur limite définie dans la règle. Cette limite peut être de deux types :

Limite basée sur le taux de connexion : déclenchement de la fonction si le nombre par seconde de nouvelles connexions au firewall dépasse le seuil défini.

Limite basée sur le nombre total de connexions : déclenchement de la fonction si le nombre total de nouvelles connexions au firewall dépasse le seuil défini.

Les règles avec seuil sont dotées de paramètres comparables à ceux des règles IP. Ces paramètres définissent le type de trafic auquel s'applique la règle avec seuil.

Une règle avec seuil spécifique est dotée des paramètres suivants :

Interface source et réseau source

Interface de destination et réseau de destination

Service

Type de seuil : basé sur l'hôte et/ou le réseau

Si un trafic répond aux critères précédents et qu'il est la cause du dépassement du seuil défini pour un hôte/réseau, la fonction ZoneDefense va être déclenchée. Cette fonction va empêcher cet hôte/ce réseau d'accéder aux switches. Tout blocage en réponse à une violation de seuil sera basé sur l'adresse IP de l'hôte ou du réseau sur les switches. Lorsqu'un seuil basé sur un réseau est dépassé, c'est tout le réseau source qui se retrouve bloqué (et pas uniquement l'hôte fautif).

Pour obtenir une description générale de la définition et du fonctionnement des règles avec seuil, reportez-vous à la section intitulée « Règles avec seuil ».

Blocage manuel et listes d'exclusions

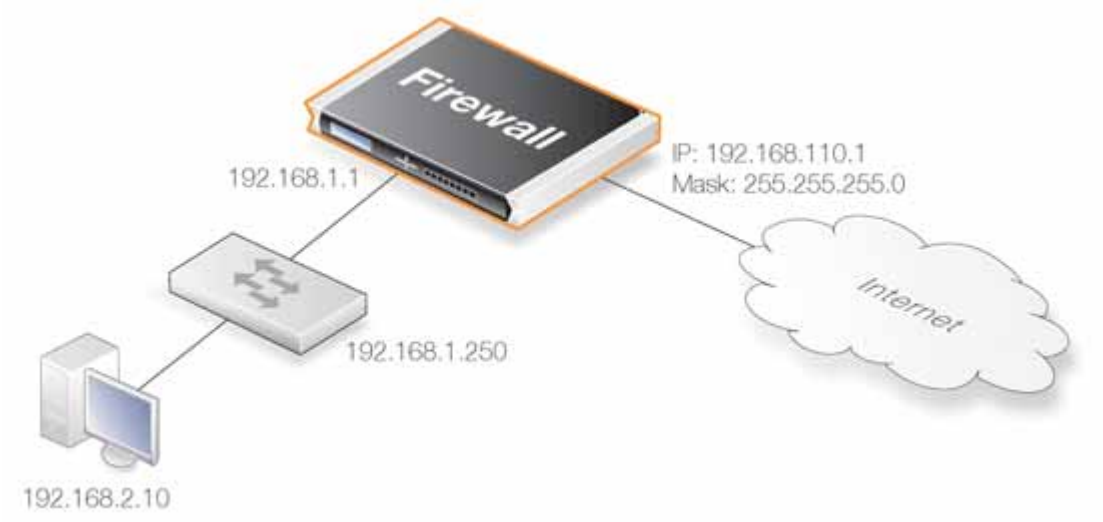
En complément des règles avec seuil, vous pouvez également définir manuellement des hôtes et des réseaux qui seront bloqués ou exclus de manière statique. Lorsque vous bloquez manuellement des hôtes et des réseaux, ce blocage peut être effectué par défaut ou en fonction d'une programmation. Vous pouvez également préciser les protocoles et les numéros de port de protocole qui doivent être bloqués.

Vous pouvez créer et utiliser des *listes d'exclusions* en vue de désigner les hôtes qui ne devront pas être bloqués lorsqu'une limite d'une règle avec seuil est atteinte. Nous vous recommandons d'ajouter dans cette liste l'adresse IP ou MAC de l'interface du firewall qui se connecte au switch ZoneDefense. Cette précaution évite le blocage accidentel du firewall.

Exemple 12.1. Un scénario ZoneDefense simple

L'exemple simple suivant illustre les étapes nécessaires pour configurer la fonction ZoneDefense. On suppose que toutes les interfaces du firewall ont déjà été configurées.

Un seuil HTTP de dix (10) connexions par seconde est appliqué. Si le taux de connexion dépasse cette limite, le firewall bloquera l'hôte spécifique (inclus dans la plage des adresses réseau 192.168.2.0/24, par exemple) qui ne pourra plus du tout accéder au switch.



C'est le modèle de switch D-Link DES-3226S qui est utilisé dans cet exemple, avec l'adresse 192.168.1.250 pour l'interface de gestion qui se connecte à l'adresse d'interface 192.168.1.1 du firewall. Cette interface de firewall est ajoutée à la liste des exclusions pour éviter que le firewall ne puisse plus accéder au switch pour cause de verrouillage.

Interface Web

Ajoutez un nouveau switch dans la section ZoneDefense :

Sélectionnez ZoneDefense > Switches > Add > ZoneDefense switch (ZoneDefense > Switches > Ajouter > Switch ZoneDefense).

Saisissez les données suivantes :

Name (Nom) : switch1

Switch model (Modèle du switch) : DES-3226S

IP Address (Adresse IP) : 192.168.1.250

Dans le champ SNMP Community (Communauté SNMP), saisissez la *chaîne de communauté avec accès en écriture* configurée pour le switch.

Cliquez sur Check Switch (Vérifier le switch) pour vérifier que le firewall peut communiquer avec le switch et que la chaîne de communauté est correcte.

Cliquez sur OK.

Ajoutez l'interface de gestion du firewall à la liste d'exclusions :

Sélectionnez ZoneDefense > Exclude list (ZoneDefense > Liste d'exclusions).

Dans la zone Addresses (Adresses), sélectionnez le nom d'objet de l'adresse d'interface 192.168.1.1 du firewall dans la liste des éléments disponibles (Available) et placez-le dans la liste des éléments sélectionnés (Selected).

Cliquez sur OK.

Configurez un seuil HTTP égal à dix (10) connexions par seconde :

Sélectionnez Traffic Management > Threshold Rules > Add > Threshold Rule (Gestion du trafic > Règles avec seuil > Ajouter > Règle avec seuil).

Pour le paramètre Threshold Rule (Règle avec seuil), saisissez les valeurs suivantes :

Name (Nom) : HTTP-Threshold (Seuil HTTP)

Service : http

Pour l'option Address Filter (filtre d'adresse), saisissez les données suivantes :

Source Interface (Interface source) : l'interface de gestion du firewall

Destination Interface (Interface de destination) : any (n'importe lequel)

Source Network (Réseau source) : 192.168.2.0/24 (ou le nom de l'objet)

Destination Network (Réseau de destination) : all-nets (tout réseau)

Cliquez sur OK.

Précisez le seuil, le type de seuil et l'action à exécuter en cas de dépassement de ce seuil :

Sélectionnez Add > Threshold Action (Ajouter > Action en cas de dépassement du seuil).

Configurez l'action en cas de dépassement du seuil comme suit :

Action : Protect (Protéger)

Group By (Regroupement) : Host-based (Basé sur l'hôte)

Threshold (Seuil) : 10

Sélectionnez l'unité de valeur Connections/Second (Connexions par seconde) pour le seuil.

Cochez la case Use ZoneDefense (Utiliser ZoneDefense).

Cliquez sur OK.

Limites

La fonction ZoneDefense ne fonctionne pas toujours tout à fait de la même manière selon le modèle de switch utilisé. La première différence se situe au niveau du temps de latence entre le déclenchement d'une règle de blocage et le moment où les switches commencent réellement à bloquer le trafic détecté par la règle. Tous les modèles de switch ne requièrent qu'un court temps de latence afin de mettre en œuvre le blocage une fois que la règle est déclenchée. Mais certains modèles peuvent activer le blocage du trafic en moins d'une seconde, tandis que d'autres peuvent nécessiter une minute, voire plus.

Une seconde différence réside au niveau du nombre maximal de règles prises en charge par les différents switches. Certains switches prennent en charge au maximum 50 règles, alors que d'autres peuvent en gérer jusqu'à 800

(généralement, pour bloquer un hôte ou un réseau, il faut une règle par port de switch). Lorsque cette limite est atteinte, aucun autre hôte ou réseau ne sera bloqué.

Important

La fonction ZoneDefense utilise une plage de la règle ACL (Access Control List - liste de contrôle d'accès) définie sur le switch. Pour éviter tout conflit potentiel au niveau des règles et pour garantir le contrôle d'accès du firewall, il est fortement recommandé que l'administrateur efface la totalité de la règle ACL définie sur le switch avant de configurer la fonction ZoneDefense.

Chapitre 13. Paramètres avancés

Le présent chapitre décrit les paramètres avancés que vous pouvez configurer dans NetDefendOS. Ces paramètres sont classés par catégories, comme suit :

> **Remarque**
> Lorsque vous modifiez un paramètre avancé, vous devez reconfigurer le firewall D-Link afin de charger sur ce dernier la nouvelle configuration NetDefendOS et de mettre en œuvre les valeurs nouvellement définies.

Paramètres IP

LogChecksumErrors

Consigne les occurrences des paquets IP qui contiennent des totaux de contrôle erronés. Normalement, ce type d'erreur survient à cause de l'endommagement des paquets au cours de leur transfert sur le réseau. Toutes les unités réseau (routeurs et postes de travail compris) ignorent ces paquets IP qui contiennent des erreurs de total de contrôle. Mais il est toutefois fort peu probable qu'une attaque soit basée sur des totaux de contrôle illégaux.

Valeur par défaut : *Enabled (Activé)*

LogNonIP4

Consigne les occurrences des paquets IP dont la version est différente de la version 4. NetDefendOS n'accepte que les paquets IP version 4. Il ignore tous les autres.

Valeur par défaut : *256*

LogReceivedTTL0

Consigne les occurrences des paquets IP reçus avec la valeur 0 (zéro) affectée au paramètre de durée de vie (paramètre TTL - Time To Live). Une unité réseau, quelle qu'elle soit, ne doit en aucun cas envoyer de paquets avec la valeur 0 associée au paramètre de durée de vie.

Valeur par défaut : *Enabled (Activé)*

Block0000Src

Bloque l'adresse source 0.0.0.0.

Valeur par défaut : *Drop (Ignorer)*

Block0Net

Bloque les adresses source de type 0.*.

Valeur par défaut : *DropLog (Ignorer et consigner)*

Block127Net

Bloque les adresses source de type 127.*.

Valeur par défaut : *DropLog (Ignorer et consigner)*

BlockMulticastSrc

Bloque les deux adresses source 224.0.0.0 et 255.255.255.255 à multidiffusion.

Valeur par défaut : *DropLog (Ignorer et consigner)*

TTLMin

Indique la durée de vie (valeur TTL - Time To Live) minimale acceptée pour les paquets reçus.

Valeur par défaut : *3*

TTLOnLow

Détermine l'action à exécuter pour les paquets dont la durée de vie (valeur TTL - Time To Live) est inférieure à la valeur TTLMin précisée.

Valeur par défaut : *DropLog (Ignorer et consigner)*

DefaultTTL

Indique la durée de vie (valeur TTL - Time To Live) que NetDefendOS doit appliquer lorsqu'il est la source émettrice d'un paquet envoyé. Il s'agit en règle générale d'une valeur comprise entre 64 et 255.

Valeur par défaut : *255*

LayerSizeConsistency

Vérifie que les informations relatives à la taille incluses dans une « couche » spécifique (Ethernet, IP, TCP, UDP et ICMP) sont cohérentes avec celles des autres couches.

Valeur par défaut : *ValidateLogBad (Valider et consigner en cas de non-correspondance)*

IPOptionSizes

Vérifie la taille des « options IP ». Ces options sont de petits blocs d'informations qui peuvent être ajoutés à la fin de chaque en-tête IP. Cette fonction vérifie la taille des types d'option les plus connus et garantit qu'aucune de ces options ne dépasse la taille limite précisée dans l'en-tête IP lui-même.

Valeur par défaut : *ValidateLogBad (valider et consigner en cas de non-correspondance)*

IPOPT_SR

Indique si les options de routage source sont autorisées. Ces options permettent à l'expéditeur de contrôler le mode d'acheminement du paquet via chaque routeur et firewall. Elles constituent un risque considérable pour la sécurité. NetDefendOS n'obéit jamais aux routes source définies par ces options, quelle que soit la valeur affectée au paramètre IPOPT_SR.

Valeur par défaut : *DropLog (Ignorer et consigner)*

IPOPT_TS

Grâce aux options d'horodatage, vous pouvez configurer chacun des routeurs et firewalls présents sur la route du paquet de sorte qu'ils indiquent l'heure à laquelle ils ont transféré ce paquet vers sa destination suivante. Ces options ne sont pas appliquées dans le cadre d'un trafic normal. Les options d'horodatage peuvent également servir à « enregistrer » la route empruntée par un paquet, depuis son expéditeur jusqu'à sa destination finale. NetDefendOS n'entre jamais d'informations dans ces options, quelle que soit la valeur affectée au paramètre IPOPT_TS.

Valeur par défaut : *DropLog (Ignorer et consigner)*

IPOPT_OTHER

Toute option différente de celles précisées ci-avant.

Valeur par défaut : *DropLog (Ignorer et consigner)*

DirectedBroadcasts

Indique si NetDefendOS transfère les paquets qui ont pour cible l'adresse de diffusion de ses réseaux connectés directement. Vous pourriez tout à fait obtenir la même fonctionnalité en ajoutant des lignes dans la section Rules (Règles). Mais une option à part entière a également été incluse ici pour plus de simplicité. Ce type de validation spécialisé est plus rapide (il vous évite de saisir des données dans la section Rules).

Valeur par défaut : *DropLog (Ignorer et consigner)*

IPRF

Indique ce que NetDefendOS doit faire s'il existe des données dans les champs « réservés » des en-têtes IP. Normalement, la valeur 0 (zéro) doit être affectée à ces champs. Les techniques de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting) exploitent ces champs.

Valeur par défaut : *DropLog (Ignorer et consigner)*

StripDFOnSmall

Élimine l'indicateur DF (Don't Fragment – ne pas fragmenter) pour les paquets dont la taille est inférieure ou égale à celle précisée par ce paramètre.

Valeur par défaut : *65535 bytes (65 535 octets)*

Paramètres TCP

TCPOptionSizes

Vérifie la taille des options TCP. Le fonctionnement de ce paramètre est comparable à celui de la fonction IPOptionSizes décrite précédemment.

Valeur par défaut : *ValidateLogBad (Valider et consigner en cas de non-correspondance)*

TCPMSSMin

Détermine la valeur minimale acceptable pour la taille maximale des segments TCP (valeur MSS – Maximum Segment Size). Les paquets contenant des segments dont la taille maximale est inférieure à cette limite sont gérés conformément au paramètre ci-après.

Valeur par défaut : *100 bytes (100 octets)*

TCPMSSOnLow

Détermine l'action à exécuter pour les paquets dont la valeur de la taille maximale des segments TCP est inférieure à la valeur affectée au paramètre TCPMSSMin. Des valeurs trop faibles pourraient engendrer des problèmes au niveau des piles TCP mal rédigées.

Valeur par défaut : *DropLog (Ignorer et consigner)*

TCPMSSMax

Détermine la valeur maximale acceptable pour la taille maximale des segments TCP (valeur MSS – Maximum Segment Size). Les paquets contenant des segments dont la taille maximale est supérieure à cette limite sont gérés conformément au paramètre ci-après.

Valeur par défaut : *1460 bytes (1 460 octets)*

TCPMSSVPNMax

Comme pour le paramètre TCPMSSMax, il s'agit de la valeur maximale autorisée pour la taille maximale des segments (valeur MSS – Maximum Segment Size). Toutefois, ce paramètre ne contrôle que la taille maximale des segments dans le cas de connexions VPN (Virtual Private Network). Ainsi, NetDefendOS peut réduire la taille réelle des segments utilisée par le protocole TCP dans toutes les connexions VPN. Cela réduit la fragmentation TCP sur la connexion VPN, même si les hôtes ne savent pas comment déterminer la taille maximale des segments pouvant être transmis (valeur MTU - Maximum Transmission Unit).

Valeur par défaut : *1400 bytes (1 400 octets)*

TCPMSSOnHigh

Détermine l'action à exécuter pour les paquets dont la valeur de la taille maximale des segments TCP (valeur MSS – Maximum Segment Size) est supérieure à la valeur affectée au paramètre TCPMSSMax. Des valeurs trop élevées pourraient engendrer des problèmes au niveau des piles TCP mal rédigées ou générer une grande quantité de paquets fragmentés, ce qui nuira aux performances.

Valeur par défaut : *Adjust (Ajuster)*

TCPMSSAutoClamping

Fixe automatiquement la taille maximale des segments TCP (valeur MSS – Maximum Segment Size) en fonction de la taille maximale des segments pouvant être transmis (valeur MTU - Maximum Transmission Unit) définie pour les interfaces impliquées, en plus du paramètre TCPMSSMax.

Valeur par défaut : *Enabled (Activé)*

TCPMSSLogLevel

Détermine quand consigner les paquets dont la taille maximale des segments TCP est trop élevée (valeur MSS – Maximum Segment Size), s'ils ne sont pas déjà consignés en fonction du paramètre TCPMSSOnHigh.

Valeur par défaut : *7000 bytes (7 000 octets)*

TCPZeroUnusedACK

Détermine si NetDefendOS doit affecter la valeur 0 au champ du numéro de séquence ACK des paquets TCP, si ce champ n'est pas utilisé. Certains systèmes d'exploitation dévoilent ainsi des informations sur les numéros de séquence. Cette caractéristique pourrait être exploitée par des intrus qui voudraient détourner des connexions établies.

Valeur par défaut : *Enabled (Activé)*

TCPZeroUnusedURG

Élimine les pointeurs de données urgentes (URG) de tous les paquets.

Valeur par défaut : *Enabled (Activé)*

TCPOPT_WSOPT

Détermine la manière dont NetDefendOS traite les options d'ajustement dynamique des fenêtres (WSOPT – Window-Scaling Options). Ces options servent à augmenter la taille des fenêtres utilisées par le protocole TCP, c'est-à-dire à accroître la quantité d'informations pouvant être transférées sans transmission d'accusé de réception à l'expéditeur. Mais elles sont également exploitées par les techniques de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting). Ces options d'ajustement dynamique des fenêtres sont couramment rencontrées dans les réseaux modernes.

Valeur par défaut : *ValidateLogBad (Valider et consigner en cas de non-correspondance)*

TCPOPT_SACK

Détermine la manière dont NetDefendOS traite les options d'accusé de réception sélectif (SACK – Selective Acknowledgement). Ces options servent à accuser réception de paquets spécifiques et non de séries entières de paquets, ce qui peut accroître les performances pour les connexions pour lesquelles le taux de perte de paquets est important. Mais elles sont également exploitées par les techniques de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting). Les options d'accusé de réception sélectif sont couramment rencontrées dans les réseaux modernes.

Valeur par défaut : *ValidateLogBad (Valider et consigner en cas de non-correspondance)*

TCPOPT_TSOPT

Détermine la manière dont NetDefendOS traite les options d'horodatage (TSOPT - Time Stamp Options). Comme le stipule la méthode de protection contre les numéros de séquence encapsulés (méthode PAWS - Protect Against Wrapped Sequence numbers), les options d'horodatage servent à empêcher que les numéros de séquence (nombre codé sur 32 bits) ne « dépassent » leur limite supérieure sans que le destinataire n'en soit averti. Cela ne constitue normalement pas un problème. Grâce au paramètre TSOPT, certaines piles TCP optimisent leur connexion en mesurant le temps qui s'écoule pour qu'un paquet soit transmis vers et depuis sa destination. Cette information peut ensuite être utilisée pour accélérer le rythme des renvois par rapport aux précédents. Mais elle est également exploitée par les techniques de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting). Les options d'horodatage sont couramment rencontrées dans les réseaux modernes.

Valeur par défaut : *ValidateLogBad (Valider et consigner en cas de non-correspondance)*

TCPOPT_ALTCHKREQ

Détermine la manière dont NetDefendOS traite les options de demande de totaux de contrôle de remplacement (ALTCHKREQ - Alternate Checksum Request). À la base, ces options ont été conçues pour la négociation afin d'utiliser des totaux de contrôle optimum dans les en-têtes TCP. Toutefois, ces options ne sont pas comprises par tous les systèmes standard actuels. Comme NetDefendOS ne peut pas comprendre les algorithmes de total de contrôle différents de l'algorithme standard, il ne peut jamais accepter ces options. L'option ALTCHKREQ n'est normalement jamais rencontrée dans les réseaux modernes.

Valeur par défaut : *StripLog (Éliminer et consigner)*

TCPOPT_ALTCHKDATA

Détermine la manière dont NetDefendOS traite les options de données de totaux de contrôle de remplacement (ALTCHKDATA - Alternate Checksum Data). Ces options sont utilisées pour le transport des totaux de contrôle de remplacement, lorsque l'option ALTCHKREQ l'autorise. Vous ne devriez normalement jamais rencontrer ces options sur des réseaux modernes.

Valeur par défaut : *StripLog (Éliminer et consigner)*

TCPOPT_CC

Détermine la manière dont NetDefendOS traite les options de décompte de connexions.

Valeur par défaut : *StripLogBad (Éliminer et consigner en cas de non-correspondance)*

TCPOPT_OTHER

Définit la manière dont NetDefendOS traite les autres options TCP, non traitées dans les paramètres ci-dessus. Vous ne devriez normalement jamais rencontrer ces options dans les réseaux modernes.

Valeur par défaut : *StripLog (Éliminer et consigner)*

TCPSynUrg

Définit la manière dont NetDefendOS traite les paquets TCP pour lesquels les indicateurs de synchronisation (SYN) et de données urgentes (URG) sont activés simultanément. La présence d'un indicateur SYN indique qu'une nouvelle connexion est en train d'être établie et l'indicateur URG signifie que le paquet contient des données qui requièrent une attention particulière de toute urgence. Ces deux indicateurs ne doivent pas être activés pour un même paquet, car ils ne sont utilisés que pour nuire aux ordinateurs dont les piles TCP ne bénéficient pas d'une mise en œuvre satisfaisante.

Valeur par défaut : *DropLog (Ignorer et consigner)*

TCPSynPsh

Définit la manière dont NetDefendOS traite les paquets TCP pour lesquels les indicateurs de synchronisation (SYN) et de transmission immédiate (PSH - Push) sont activés simultanément. L'indicateur PSH signifie que la pile du destinataire doit immédiatement transmettre les informations incluses dans le paquet à l'application de destination présente sur l'ordinateur. Ces deux indicateurs ne doivent pas être activés en même temps, car cela pourrait présenter un risque potentiel de panne pour les piles TCP qui ne bénéficient pas d'une mise en œuvre satisfaisante. Toutefois, de nombreux ordinateurs Macintosh ne mettent pas en œuvre l'en-tête TCP correctement. En d'autres termes, ils envoient systématiquement des paquets SYN avec l'indicateur PSH activé. Aussi, c'est pour cette raison que NetDefendOS supprime normalement l'indicateur PSH et qu'il autorise le transfert du paquet, alors qu'il devrait logiquement l'ignorer.

Valeur par défaut : *StripSilent (Éliminer en silence)*

TCPFinUrg

Définit comment NetDefendOS traite les paquets TCP pour lesquels les indicateurs de fin de connexion (FIN - Finish) et de données urgentes (URG) sont activés simultanément. Cela ne devrait normalement jamais se produire. En effet, logiquement, vous ne tentez pas de mettre fin à une connexion qui doit en même temps transmettre des données « importantes ». Cette association d'indicateurs pourrait servir pour générer une panne lorsque la mise en œuvre des piles TCP n'est pas satisfaisante. Elle est également exploitée par les techniques de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting).

Valeur par défaut : *DropLog (Ignorer et consigner)*

TCPUrg

Définit la manière dont NetDefendOS traite les paquets TCP pour lesquels l'indicateur de données urgentes (URG) est activé, indépendamment de tout autre indicateur. De nombreuses piles TCP et applications ne traitent pas les indicateurs URG de manière adéquate et risquent, dans le pire des cas, de ne plus fonctionner. Notez toutefois que certains programmes (FTP et MS SQL Server, par exemple) se servent presque systématiquement de cet indicateur URG.

Valeur par défaut : *StripLog (Éliminer et consigner)*

TCPECN

Définit la manière dont NetDefendOS traite les paquets TCP pour lesquels l'indicateur Xmas ou l'indicateur Ymas est activé. À l'heure actuelle, ces indicateurs sont la plupart du temps exploités par les techniques de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting).

Remarque : la toute prochaine norme de *notification explicite de congestion* (norme ECN - Explicit Congestion Notification) utilise également ces indicateurs TCP. Mais tant que le nombre de systèmes d'exploitation qui peuvent prendre en charge cette norme restera faible, ces indicateurs devront être supprimés.

Valeur par défaut : *StripLog (Éliminer et consigner)*

TCPRF

Définit la manière dont NetDefendOS traite les informations présentes dans le « champ réservé » de l'en-tête TCP (il doit normalement s'agir de la valeur 0). Ce champ est différent des indicateurs Xmas et Ymas. Les techniques

de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting) exploitent ces champs.

Valeur par défaut : *DropLog (Ignorer et consigner)*

TCPNULL

Définit la manière dont NetDefendOS traite les paquets TCP pour lesquels aucun des indicateurs SYN, ACK, FIN ou RST n'est activé. Conformément à la norme TCP, ces paquets sont illégaux et sont utilisés aussi bien par les techniques de prise d'empreinte des systèmes d'exploitation (OS Fingerprinting) que par les techniques de balayage furtif des ports, étant donné que certains firewalls sont incapables de les détecter.

Valeur par défaut : *DropLog (Ignorer et consigner)*

TCPSequenceNumbers

Ce paramètre détermine si, avant de transférer le segment, il convient de comparer la plage des numéros de séquence occupée par un segment TCP et la fenêtre de réception annoncée par l'hôte de réception. Si la valeur *ValidateLogBad* ou *ValidateSilent* est affectée à ce paramètre, les segments qui ne correspondent pas à la fenêtre de réception annoncée par l'hôte de réception sont ignorés. Si la valeur *ValidateLogBad* est affectée à ce paramètre, ces abandons seront également consignés.

La validation du numéro de séquence TCP n'est possible que pour les connexions dont le suivi est assuré par le moteur d'état (pas pour les paquets transmis à l'aide d'une règle FwdFast).

Valeur par défaut : *ValidateLogBad (Valider et consigner en cas de non-correspondance)*

Paramètres ICMP

ICMPSendPerSecLimit

Définit le nombre maximal de messages ICMP (Internet Control Message Protocol) que NetDefendOS peut générer par seconde. Ces messages comprennent les réponses ping, les messages de type « Destination Unreachable » (Destination injoignable), ainsi que les paquets de réinitialisation RST (Reset) TCP. En d'autres termes, ce paramètre limite le nombre de rejets par seconde que les règles Reject (Rejeter) de la section Rules (Règles) peuvent générer.

Valeur par défaut : *20 par seconde*

SilentlyDropStateICMPErrors

Définit si NetDefendOS doit ignorer en silence les erreurs ICMP qui appartiennent à des connexions ouvertes et dont le suivi est assuré de manière dynamique. Si ces erreurs ne sont pas ignorées par ce paramètre, elles sont transmises à la règle définie en vue de leur évaluation, comme tout autre paquet.

Valeur par défaut : *Enabled (Activé)*

Paramètres ARP

ARPMatchEnetSender

Détermine si NetDefendOS requiert que l'adresse de l'expéditeur au niveau Ethernet soit conforme à l'adresse du matériel signalée dans les données ARP (Address Resolution Protocol).

Valeur par défaut : *DropLog (Ignorer et consigner)*

ARPQueryNoSenderIP

Détermine ce qu'il faut faire des requêtes ARP (Address Resolution Protocol) dont l'expéditeur a l'adresse IP 0.0.0.0. De telles adresses IP d'expéditeur ne sont jamais valides dans les réponses. Mais les unités

réseau qui ne connaissent pas encore leur adresse IP émettent parfois des interrogations ARP avec une adresse IP d'expéditeur « non spécifiée ».

Valeur par défaut : *DropLog (Ignorer et consigner)*

ARPSenderIP

Détermine si l'adresse IP de l'expéditeur doit être conforme aux règles définies dans la section Access (Accès).

Valeur par défaut : *Validate (Valider)*

UnsolicitedARPReplies

Détermine la manière dont NetDefendOS traite les réponses ARP (Address Resolution Protocol) qui ne sont associées à aucune interrogation. Conformément à la spécification ARP, le destinataire doit les accepter. Toutefois, étant donné que cette obligation peut favoriser le détournement des connexions locales, cette acceptation n'est généralement pas autorisée.

Valeur par défaut : *DropLog (Ignorer et consigner)*

ARPRequests

Détermine si NetDefendOS ajoute automatiquement les données des requêtes ARP (Address Resolution Protocol) dans sa table ARP. Selon la spécification ARP, il convient de procéder ainsi. Mais comme cette procédure risque de favoriser le détournement des connexions locales, cet ajout n'est généralement pas autorisé. Même lorsque la valeur « Drop » (Ignorer) est affectée au paramètre ARPRequests (c'est-à-dire que le paquet est ignoré sans être enregistré), NetDefendOS répond quand même au paquet (à condition que les autres règles définies acceptent cette demande).

Valeur par défaut : *Drop (Ignorer)*

ARPChanges

Détermine la manière dont NetDefendOS traite les cas où une réponse ou une demande ARP (Address Resolution Protocol) reçues entraîneraient la modification d'un élément existant de la table ARP. Le fait d'autoriser cette opération risque de favoriser le détournement des connexions locales. Toutefois, si on ne l'autorise pas, cela peut générer des problèmes si, par exemple, un adaptateur réseau est remplacé, car NetDefendOS n'acceptera pas la nouvelle adresse tant que l'entrée de la table ARP précédente n'est pas arrivée à expiration.

Valeur par défaut : *AcceptLog (Accepter et consigner)*

StaticARPChanges

Détermine la manière dont NetDefendOS traite les cas où une réponse ou une demande ARP (Address Resolution Protocol) reçues entraîneraient la modification d'un élément statique de la table ARP. Cela n'est, bien sûr, jamais autorisé. Par contre, grâce à ce paramètre, vous pouvez préciser si ces cas doivent ou non être consignés.

Valeur par défaut : *DropLog (Ignorer et consigner)*

ARPExpire

Définit la durée de conservation d'un élément dynamique normal de la table ARP (Address Resolution Protocol) avant d'être supprimé de la table.

Valeur par défaut : *900 secondes (15 minutes)*

ARPExpireUnknown

Précise la durée pendant laquelle NetDefendOS va conserver en mémoire les adresses injoignables. Cela permet de s'assurer que NetDefendOS ne sollicite pas indéfiniment de telles adresses.

Valeur par défaut : *3 secondes*

ARPMulticast

Détermine la manière dont NetDefendOS traite les demandes et les réponses ARP (Address Resolution Protocol) qui déclarent que leurs adresses sont des adresses à multidiffusion. Ces déclarations ne sont jamais correctes (c'est le cas de certains périphériques d'équilibrage de la charge et de redondance qui utilisent des adresses à multidiffusion de la couche matérielle).

Valeur par défaut : *DropLog (Ignorer et consigner)*

ARPBroadcast

Détermine la manière dont NetDefendOS traite les demandes et les réponses ARP (Address Resolution Protocol) qui déclarent que leurs adresses sont des adresses de diffusion. Ces déclarations ne sont jamais correctes.

Valeur par défaut : *DropLog (Ignorer et consigner)*

ARPCacheSize

Définit le nombre total d'entrées ARP (Address Resolution Protocol) que la mémoire cache peut contenir.

Valeur par défaut : *4096*

ARPHashSize

Les tables dites « de hachage » permettent de localiser rapidement des entrées dans une table. Pour une efficacité maximale, un hachage doit être deux fois plus grand que la table qu'il indexe. Donc, si le réseau local à connexion directe le plus volumineux contient 500 adresses IP, la table de hachage ARP doit comporter au moins 1 000 entrées.

Valeur par défaut : *512*

ARPHashSizeVLAN

Les tables dites « de hachage » permettent de localiser rapidement des entrées dans une table. Pour une efficacité maximale, un hachage doit être deux fois plus grand que la table qu'il indexe. Donc, si le réseau local à connexion directe le plus volumineux contient 500 adresses IP, la table de hachage ARP doit comporter au moins 1 000 entrées.

Valeur par défaut : *64*

ARPIPCollision

Détermine le comportement lors de la réception d'une demande ARP (Address Resolution Protocol) dont l'expéditeur a une adresse IP qui entre en conflit avec une autre adresse déjà utilisée dans l'interface de réception. Actions possibles : Drop (Ignorer) ou Notify (Notifier).

Valeur par défaut : *Drop (Ignorer)*

Paramètres de l'inspection dynamique

LogConnectionUsage

Ce paramètre génère un message de consignation pour chaque paquet transmis via une connexion configurée dans le moteur d'état de NetDefendOS. Le trafic dont la destination est le firewall D-Link lui-même (par exemple, le trafic de gestion de NetDefendOS) n'est pas soumis à ce paramètre.

Le message de consignation inclut le port, le service, l'adresse IP de la source/destination et l'interface. Ce paramètre ne doit être activé qu'à des fins de diagnostic et de test, car il génère des volumes de messages de consignation difficilement gérables et peut également détériorer considérablement les performances en matière de débit.

Valeur par défaut : *Disabled (Désactivé)*

ConnReplace

Permet de remplacer les connexions les plus anciennes dans la liste des connexions de NetDefendOS par de nouvelles, lorsqu'il n'y a plus suffisamment d'espace libre disponible.

Valeur par défaut : *ReplaceLog (Remplacer et consigner)*

LogOpenFails

Dans certains cas où la section Rules (Règles) détermine qu'un paquet doit être autorisé à passer, le mécanisme d'inspection dynamique peut après coup aller à l'encontre de cette configuration et ne pas autoriser ce paquet à ouvrir une nouvelle connexion. C'est ce qui se produit, par exemple, lorsqu'un paquet TCP qui, bien qu'autorisé par la section Rules (Règles) et bien que ne faisant pas partie d'une connexion déjà établie, a son indicateur de synchronisation (SYN) désactivé. Ces paquets ne peuvent en aucun cas ouvrir de nouvelles connexions. En outre, les nouvelles connexions ne peuvent jamais être ouvertes par d'autres messages ICMP qu'un message ECHO ICMP (ping). Ce paramètre détermine si NetDefendOS doit consigner l'arrivée de tels paquets.

Valeur par défaut : *Enabled (Activé)*

LogReverseOpens

Détermine si NetDefendOS consigne les paquets qui tentent de rouvrir une nouvelle connexion via une connexion déjà ouverte. Ce paramètre ne s'applique qu'aux paquets TCP dont l'indicateur de synchronisation (SYN) est activé, ainsi qu'aux paquets ECHO ICMP. Pour les autres protocoles (comme le protocole UDP, par exemple), il n'y a aucun moyen de déterminer si l'hôte distant est en train de tenter d'ouvrir une nouvelle connexion.

Valeur par défaut : *Enabled (Activé)*

LogStateViolations

Détermine si NetDefendOS consigne les paquets qui violent le diagramme de changement d'état attendu pour une connexion (par exemple, avec l'obtention de paquets de fin de connexion FIN TCP en réponse à des paquets de synchronisation SYN TCP).

Valeur par défaut : *Enabled (Activé)*

MaxConnections

Définit le nombre de connexions que NetDefendOS peut maintenir ouvertes simultanément à tout instant. Chaque connexion consomme environ 150 octets de mémoire RAM. Lorsque la valeur « dynamic » (dynamique) est affectée à ce paramètre, NetDefendOS tente d'utiliser autant de connexions que l'autorise chaque produit.

Valeur par défaut : *<dynamic> (<dynamique>)*

LogConnections

Définit la manière dont NetDefendOS consigne les connexions :

NoLog (ne pas consigner) – Il ne consigne aucune connexion. Par conséquent, peu importe si la consignation est activée pour les règles Allow (Autoriser) ou NAT (Network Address Translation) dans la section Rules (Règles), il n'y aura pas de consignation pour ces connexions. Toutefois, les règles FwdFast (Transmettre immédiatement), Drop (Ignorer) et Reject (Rejeter) seront consignées, en fonction des paramètres de la section

Rules (Règles).

Log (Consigner) – Les connexions sont consignées selon une formule abrégée. Ce paramètre donne une brève description de la connexion, indique la règle qui a autorisé son ouverture, ainsi que toute règle SAT (Static Address Translation) qui s'applique. Les connexions sont également consignées lorsqu'elles sont refermées.

LogOC (Consigner le paquet d'ouverture et de clôture) – Comparable à l'option Log, mais cette option inclut en plus les deux paquets qui provoquent l'ouverture et la clôture de la connexion. Si une connexion est refermée à la suite de l'arrivée à expiration d'un délai, aucun paquet de clôture n'est consigné.

LogOCAll (Consigner tous les paquets d'ouverture et de clôture) – Consigne tous les paquets impliqués dans l'ouverture et la clôture de la connexion. Dans le cas du protocole TCP, cela inclut tous les paquets pour lesquels les indicateurs de synchronisation (SYN), de fin de connexion (FIN) ou de réinitialisation (RST) sont activés.

LogAll (Tout consigner) – Consigne tous les paquets inclus dans la connexion.

Valeur par défaut : *Log (Consigner)*

Expiration des délais de connexion

Les paramètres inclus dans cette section définissent la durée pendant laquelle une connexion peut rester inactive (c'est-à-dire, la durée pendant laquelle aucune donnée n'est transmise via cette connexion) avant d'être refermée automatiquement. Notez que chaque connexion comprend deux valeurs de délai d'expiration : une pour chaque direction. Une connexion est refermée si l'une ou l'autre de ces deux valeurs est égale à 0.

ConnLife_TCP_SYN

Indique la durée pendant laquelle une connexion TCP en cours d'établissement peut rester inactive avant d'être refermée.

Valeur par défaut : *60 secondes*

ConnLife_TCP

Indique la durée pendant laquelle une connexion TCP totalement établie peut rester inactive avant d'être refermée. Une connexion est réputée être « totalement établie » à partir du moment où des paquets dont l'indicateur de synchronisation (SYN) est désactivé ont été transmis dans les deux directions.

Valeur par défaut : *262 144 secondes*

ConnLife_TCP_FIN

Indique la durée pendant laquelle une connexion TCP sur le point d'être refermée peut rester inactive avant d'être réellement refermée. Les connexions atteignent cet état lorsqu'un paquet dont l'indicateur de fin de connexion (FIN) est activé a été transmis dans l'une des deux directions.

Valeur par défaut : *80 secondes*

ConnLife_UDP

Indique la durée pendant laquelle les connexions UDP (User Datagram Protocol) peuvent rester inactives avant d'être refermées. Cette valeur de délai d'expiration est en règle générale faible, car le protocole UDP n'a aucun moyen de signaler lorsqu'une connexion est sur le point d'être refermée.

Valeur par défaut : *130 secondes*

ConnLife_Ping

Indique la durée pendant laquelle une connexion ping (ECHO ICMP) peut rester inactive avant d'être refermée.

Valeur par défaut : *8 secondes*

ConnLife_Other

Indique la durée pendant laquelle les connexions qui utilisent un protocole inconnu peuvent rester inactives avant d'être refermées.

Valeur par défaut : *130 secondes*

ConnLife_IGMP

Durée de vie des connexions IGMP (Internet Group Management Protocol).

Valeur par défaut : *12 secondes*

AllowBothSidesToKeepConnAlive_UDP

Ce paramètre de connexion permanente bidirectionnelle UDP (User Datagram Protocol) permet de maintenir une connexion UDP active de part et d'autre. La valeur définie par défaut permet à NetDefendOS de marquer une connexion comme active (par opposition à « inactive ») chaque fois que le côté qui a établi la connexion transmet des données. Les connexions qui ne reçoivent aucune donnée à partir du côté ayant ouvert la connexion avant l'arrivée à expiration du délai imparti pour la connexion UDP seront pas conséquent refermées, même si l'autre côté continue à transmettre des données.

Valeur par défaut : *False (Faux)*

Limites de taille par protocole

Cette section contient des informations sur les limites de taille imposées aux protocoles dépendant directement du niveau IP (TCP, UDP, ICMP, etc.).

Les valeurs définies dans cette section concernent les données IP incluses dans les paquets. Dans le cas d'Ethernet, un même paquet peut contenir jusqu'à 1 480 octets de données IP non fragmentées. De plus, 20 octets supplémentaires sont réservés pour l'en-tête IP et 14 octets pour l'en-tête Ethernet. Cela fait donc un maximum de 1 514 octets pour chaque unité de transmission (valeur MTU - Maximum Transmission Unit) sur les réseaux Ethernet.

MaxTCPLen

Définit la taille maximale d'un paquet TCP, l'en-tête compris. Cette valeur a généralement un rapport avec la quantité de données IP qui peuvent tenir dans un paquet non fragmenté. En effet, le protocole TCP adapte en règle générale la taille des segments qu'il transmet de sorte à ce qu'elle corresponde à la taille maximale des paquets. Toutefois, cette valeur peut nécessiter d'être augmentée de 20 à 50 octets sur certains systèmes VPN (Virtual Private Network) les moins courants.

Valeur par défaut : *1480*

MaxUDPLen

Définit la taille maximale d'un paquet UDP, l'en-tête compris. Cette valeur devra sans doute être assez élevée, car de nombreuses applications en temps réel utilisent des paquets UDP fragmentés volumineux. Si aucun de ces protocoles n'est utilisé, vous pouvez sans doute rabaisser cette taille limite imposée aux paquets UDP à 1 480 octets.

Valeur par défaut : *60000 bytes (60 000 octets)*

MaxICMPLen

Définit la taille maximale d'un paquet ICMP. Les messages d'erreur ICMP ne doivent jamais dépasser 600 octets

(les paquets ping peuvent toutefois être plus volumineux en cas de besoin). Vous pouvez rabaisser cette valeur à 1 000 octets si vous ne souhaitez pas utiliser de paquets ping volumineux.

Valeur par défaut : *10000 bytes (10 000 octets)*

MaxGRELen

Définit la taille maximale d'un paquet GRE. Entre autres applications, le protocole GRE (Generic Routing Encapsulation) sert notamment au transport des données PPTP (Point to Point Tunneling Protocol). Cette valeur définie doit être égale à la taille du paquet le plus volumineux autorisé à transiter via les connexions VPN, indépendamment de son protocole d'origine, à laquelle vous rajoutez environ 50 octets.

Valeur par défaut : *2000 bytes (2 000 octets)*

MaxESPLen

Définit la taille maximale d'un paquet ESP. Le protocole ESP (Encapsulation Security Payload) est utilisé par les connexions IPsec en cas de cryptage des données. Cette valeur définie doit être égale à la taille du paquet le plus volumineux autorisé à transiter via les connexions VPN, indépendamment de son protocole d'origine, à laquelle vous rajoutez environ 50 octets.

Valeur par défaut : *2000 bytes (2 000 octets)*

MaxAHLen

Définit la taille maximale d'un paquet AH. Le protocole AH (Authentication Header) est utilisé par les connexions IPsec où seule l'authentification est appliquée. Cette valeur définie doit être égale à la taille du paquet le plus volumineux autorisé à transiter via les connexions VPN, indépendamment de son protocole d'origine, à laquelle vous rajoutez environ 50 octets.

Valeur par défaut : *2000 bytes (2 000 octets)*

MaxSKIPLen

Définit la taille maximale d'un paquet SKIP (Simple Key management for Internet Protocol).

Valeur par défaut : *2000 bytes (2 000 octets)*

MaxOSPFLen

Définit la taille maximale d'un paquet OSPF. Le protocole OSPF (Open Shortest Path First) est un protocole de routage principalement utilisé dans les réseaux locaux de grande envergure.

Valeur par défaut : *1480*

MaxIPIPLen

Définit la taille maximale d'un paquet IP dans IP. Le protocole d'encapsulation IP dans IP est utilisé par les connexions Firewall-1/VPN-1 de Check Point lorsque le protocole IPsec n'est pas utilisé. Cette valeur définie doit être égale à la taille du paquet le plus volumineux autorisé à transiter via les connexions VPN, indépendamment de son protocole d'origine, à laquelle vous rajoutez environ 50 octets.

Valeur par défaut : *2000 bytes (2 000 octets)*

MaxIPCompLen

Définit la taille maximale d'un paquet IPComp (IP Payload Compression).

Valeur par défaut : *2000 bytes (2 000 octets)*

MaxL2TPLen

Définit la taille maximale d'un paquet L2TP (Layer 2 Tunneling Protocol).

Valeur par défaut : *2000 bytes (2 000 octets)*

MaxOtherSubIPLen

Définit la taille maximale des paquets dont les protocoles n'ont pas été cités ci-dessus.

Valeur par défaut : *1480 bytes (1 480 octets)*

LogOversizedPackets

Définit si NetDefendOS consigne les paquets surdimensionnés.

Valeur par défaut : *Enabled (Activé)*

Paramètres de fragmentation

Le protocole IP est capable de transporter jusqu'à 65 536 octets de données. Toutefois, la plupart des supports (Ethernet, par exemple) ne peuvent pas transporter des paquets aussi volumineux. Pour pallier ce manque, la pile IP fragmente les données à envoyer en plusieurs paquets, attribuant à chacun son propre en-tête IP et ses propres informations IP qui aideront le destinataire à reconstituer le paquet d'origine correctement.

Toutefois, de nombreuses piles IP ne sont pas capables de gérer les paquets mal fragmentés : cette caractéristique risque d'être exploitée par des intrus pour nuire aux systèmes concernés. NetDefendOS fournit différents moyens de protection contre ces attaques par fragmentation.

PseudoReass_MaxConcurrent

Nombre maximal de réassemblages de fragments concomitants. Pour ignorer tous les paquets fragmentés, affectez la valeur 0 (zéro) au paramètre PseudoReass_MaxConcurrent.

Valeur par défaut : *1024*

IllegalFrags

Détermine la manière dont NetDefendOS traite les fragments mal conçus. L'expression « mal conçus » fait référence aux fragments qui se chevauchent ou dont la taille est incorrecte, aux doublons de fragments qui contiennent des données différentes, etc. Les valeurs possibles sont les suivantes :

Drop (Ignorer) – Ignore le fragment illégal sans le consigner. Conserve également en mémoire que le paquet qui est en cours de réassemblage est « suspect », ce qui peut servir pour consigner ultérieurement d'autres informations complémentaires.

DropLog (Ignorer et consigner) – Ignore et consigne le fragment illégal. Conserve également en mémoire que le paquet qui est en cours de réassemblage est « suspect », ce qui peut servir pour consigner ultérieurement d'autres informations complémentaires.

DropPacket (Ignorer le paquet) – Ignore le fragment illégal et tous les fragments précédemment stockés. N'autorise aucun autre fragment de ce paquet à passer pendant la période définie (en secondes) par le paramètre ReassIllegalLinger.

DropLogPacket (Ignorer et consigner le paquet) – Comparable à la valeur DropPacket, mais consigne en plus l'événement.

DropLogAll (Ignorer et tout consigner) – Comparable à la valeur DropLogPacket, mais consigne également tous les autres fragments appartenant à ce paquet qui arrivent pendant la période définie (en secondes) par le paramètre ReassIllegalLinger.

Le choix d'ignorer des fragments spécifiques ou de ne pas autoriser la totalité du paquet est régi par les deux facteurs suivants :

Il est plus sûr d'ignorer la totalité du paquet.

Si, après la réception d'un fragment illégal, vous choisissez d'ignorer la totalité du paquet, les pirates pourront interrompre les communications en envoyant des fragments illégaux au cours d'un réassemblage et ainsi bloquer presque toutes les communications.

Valeur par défaut : *DropLog (Ignorer et consigner) – Des fragments spécifiques sont ignorés et la tentative de réassemblage « suspecte » correspondante est conservée en mémoire.*

DuplicateFragData

Si le même fragment arrive plusieurs fois, cela peut signifier soit qu'il a été dupliqué à un instant donné au cours de son transfert vers son destinataire, soit qu'un pirate est en train d'essayer de perturber le réassemblage du paquet. Afin de déterminer laquelle de ces deux hypothèses est la plus vraisemblable, NetDefendOS compare les composants de données du fragment. La comparaison peut être effectuée sur 2 à 512 emplacements aléatoires dans le fragment (quatre octets sont prélevés à chaque emplacement). Plus la comparaison porte sur un nombre important d'extraits, plus il y a de chances de découvrir des éléments dupliqués non conformes. Toutefois, plus le nombre de comparaisons est important, plus la charge au niveau de l'UC est élevée.

Valeur par défaut : *Check8 (Vérifier 8) – Comparaison de 8 emplacements aléatoires, soit un total de 32 octets.*

FragReassemblyFail

Les réassemblages peuvent échouer pour l'une des raisons suivantes :

Certains fragments ne sont pas arrivés dans le délai imparti défini par les paramètres ReassTimeout ou ReassTimeLimit. Cela peut signifier qu'un ou plusieurs de ces fragments se sont perdus au cours du transfert via Internet, ce qui est assez fréquent.

NetDefendOS a été forcé d'interrompre la procédure de réassemblage à cause de l'arrivée de nouveaux paquets fragmentés et le système est temporairement à cours de ressources. Les anciennes tentatives de réassemblage sont alors soit ignorées, soit marquées comme « failed » (échec).

Un pirate a tenté d'envoyer un paquet mal fragmenté.

Normalement, vous ne souhaitez pas forcément consigner les échecs, car ils sont fréquents. Toutefois, il peut s'avérer utile de consigner les échecs qui impliquent des fragments « suspects ». Ces échecs peuvent se produire si, par exemple, la valeur Drop (Ignorer) a été affectée au paramètre IllegalFrags au lieu de la valeur DropPacket (Ignorer le paquet).

Les valeurs disponibles pour le paramètre FragReassemblyFail sont les suivantes :

NoLog (Ne pas consigner) – Aucune consignation n'est effectuée en cas d'échec d'une tentative de réassemblage.

LogSuspect (Consigner les suspects) – Les échecs de tentative de réassemblage ne sont consignés que si des fragments « suspects » sont impliqués.

LogSuspectSubseq (Consigner les suspects ultérieurs) – Comparable à la valeur LogSuspect, mais les fragments ultérieurs du paquet sont consignés lorsqu'ils arrivent (données temporelles incluses).

LogAll (Tout consigner) – Tous les échecs de tentative de réassemblage sont consignés.

LogAllSubseq (Consigner tous les fragments ultérieurs) – Comparable à la valeur LogAll, mais les fragments ultérieurs du paquet sont également consignés lorsqu'ils arrivent (données temporelles incluses).

Valeur par défaut : *LogSuspectSubseq (Consigner les suspects ultérieurs)*

DroppedFrags

Si l'entrée du système est refusée à un paquet en raison des paramètres de la section Rules (Règles), cela peut également valoir la peine de consigner des fragments spécifiques de ce paquet. Le paramètre DroppedFrags définit comment NetDefendOS va réagir. Les valeurs possibles pour cette règle sont les suivantes :

NoLog (Ne pas consigner) – Aucune consignation n'est effectuée en dehors de celle stipulée dans la règle définie.

LogSuspect (Consigner les suspects) – Consigne les fragments spécifiques ignorés associés aux tentatives de réassemblage affectées par des fragments « suspects ».

LogAll (Tout consigner) – Consigne systématiquement tous les fragments ignorés.

Valeur par défaut : *LogSuspect (Consigner les suspects)*

DuplicateFrags

Si le même fragment arrive plusieurs fois, cela peut signifier soit qu'il a été dupliqué à un instant donné au cours de son transfert vers son destinataire, soit qu'un pirate est en train d'essayer de perturber le réassemblage du paquet. Le paramètre DuplicateFrags détermine si ce type de fragment doit être consigné. Notez que le paramètre DuplicateFragData peut également provoquer la consignation de ces fragments si les données qu'ils contiennent ne sont pas conformes. Les valeurs possibles pour ce paramètre sont les suivantes :

NoLog (Ne pas consigner) – Normalement, aucune consignation n'est effectuée.

LogSuspect (Consigner les suspects) – Les fragments dupliqués sont consignés si la procédure de réassemblage est affectée par des fragments « suspects ».

LogAll (Tout consigner) – Tous les fragments dupliqués sont systématiquement consignés.

Valeur par défaut : *LogSuspect (Consigner les suspects)*

FragmentedICMP

Sauf en ce qui concerne les paquets ECHO ICMP (ping), les messages ICMP ne doivent normalement pas être fragmentés, car ils contiennent trop peu de données pour justifier une fragmentation. Le paramètre FragmentedICMP détermine l'action à exécuter lorsque NetDefendOS reçoit des messages ICMP fragmentés qui ne sont ni des messages ECHO ICMP, ni des messages ECHOREPLY.

Valeur par défaut : *DropLog (Ignorer et consigner)*

MinimumFragLength

Le paramètre MinimumFragLength détermine la valeur minimale pour tous les fragments, à l'exception du fragment final, d'un paquet. Bien que l'arrivée d'un trop grand nombre de fragments trop petits peut générer des problèmes pour les piles IP, il n'est généralement pas possible de définir une valeur trop élevée pour cette limite. Il est rare que les expéditeurs créent de très petits fragments. Un expéditeur peut envoyer des fragments de 1 480 octets. Un routeur ou un tunnel VPN placés sur leur route en direction du destinataire peuvent toutefois réduire après coup à 1 440 octets la valeur réelle de la taille maximale des segments pouvant être transmis (MTU - Maximum Transmission Unit). Par conséquent, cela créerait un certain nombre de fragments de 1 440 octets et un nombre identique de fragments de 40 octets. À cause des problèmes potentiels que cela pourrait engendrer, les paramètres par défaut de NetDefendOS ont été conçus pour permettre le transfert des plus petits fragments possibles (soit des fragments de 8 octets). Pour une utilisation interne, où toutes les tailles des supports utilisés sont connues, vous pouvez augmenter cette valeur à 200 octets ou plus.

Valeur par défaut : *8 bytes (8 octets)*

ReassTimeout

Une tentative de réassemblage sera interrompue si aucun autre fragment n'arrive dans le délai imparti défini (en secondes) par le paramètre ReassTimeout, après réception du précédent fragment.

Valeur par défaut : *65 secondes*

ReassTimeLimit

Une tentative de réassemblage sera systématiquement interrompue à l'arrivée à expiration du délai ReassTimeLimit imparti défini (en secondes), après la réception du premier fragment.

Valeur par défaut : *90 secondes*

ReassDoneLinger

Une fois qu'un paquet a été réassemblé, NetDefendOS est capable de le conserver en mémoire pendant une brève période afin d'empêcher l'arrivée d'autres fragments (par exemple, des anciens fragments dupliqués) de ce paquet.

Valeur par défaut : *20 secondes*

ReassIllegalLinger

Une fois qu'un paquet a été globalement marqué en tant que paquet illégal, NetDefendOS peut conserver cette information en mémoire afin d'empêcher l'arrivée d'autres fragments de ce paquet.

Valeur par défaut : *60 secondes*

Paramètres de réassemblage des fragments locaux

LocalReass_MaxConcurrent

Nombre maximal de réassemblages locaux concomitants.

Valeur par défaut : *256*

LocalReass_MaxSize

Taille maximale d'un paquet réassemblé en local.

Valeur par défaut : *10000*

LocalReass_NumLarge

Nombre de tampons (de la taille définie ci-avant) pour le réassemblage en local de paquets volumineux (au-delà de 2 Ko).

Valeur par défaut : *32*

Paramètres DHCP

DHCP_MinimumLeaseTime

Durée d'attribution minimale (en secondes) acceptée sur le serveur DHCP.

Valeur par défaut : *60*

DHCP_ValidateBcast

Requiert que l'adresse de diffusion attribuée soit l'adresse la plus grande possible au sein du réseau attribué.

Valeur par défaut : *Enabled (Activé)*

DHCP_AllowGlobalBcast

Permet au serveur DHCP d'attribuer l'adresse 255.255.255.255 en tant qu'adresse de diffusion. (Non standard.)

Valeur par défaut : *Disabled (Désactivé)*

DHCP_UseLinkLocalIP

Si ce paramètre est activé, NetDefendOS utilise l'adresse IP locale de la couche de liaison (169.254.*.*) au lieu de l'adresse 0.0.0.0 en attendant une attribution.

Valeur par défaut : *Disabled (Désactivé)*

DHCP_DisableArpOnOffer

Désactive la vérification ARP (Address Resolution Protocol) effectuée par NetDefendOS portant sur l'adresse IP proposée. La vérification émet une demande ARP afin de vérifier si cette adresse IP est déjà utilisée.

Valeur par défaut : *Disabled (Désactivé)*

Paramètres des relais DHCP (DHCPRelay)

DHCPRelay_MaxTransactions

Nombre maximal de transactions simultanées.

Valeur par défaut : *32*

DHCPRelay_TransactionTimeout

Durée possible d'une transaction DHCP.

Valeur par défaut : *10 secondes*

DHCPRelay_MaxPPMPerIface

En une minute, le nombre de paquets DHCP qu'un client peut envoyer via NetDefendOS vers le serveur DHCP.

Valeur par défaut : *500 packets (500 paquets)*

DHCPRelay_MaxHops

Le nombre de « pas » que la demande DHCP peut effectuer entre le client et le serveur DHCP.

Valeur par défaut : *5*

DHCPRelay_MaxLeaseTime

La durée d'attribution maximale autorisée via NetDefendOS. Si le serveur DHCP est doté de valeurs supérieures pour les attributions, ces valeurs seront rabaissées en fonction de la valeur DHCPRelay_MaxLeaseTime.

Valeur par défaut : *10 000 secondes*

DHCPRelay_MaxAutoRoutes

Le nombre de relais qui peuvent être actifs simultanément.

Valeur par défaut : *256*

DHCPServer_SaveRelayPolicy

La règle qui doit être utilisée pour enregistrer la liste des relais sur le disque. Les paramètres possibles sont Disabled, ReconfShut ou ReconfShutTimer.

Valeur par défaut : *ReconfShut*

DHCPRelay_AutoSaveRelayInterval

La fréquence à laquelle la liste des relais doit être enregistrée sur le disque, si la valeur ReconfShutTimer est attribuée au paramètre DHCPServer_SaveRelayPolicy.

Valeur par défaut : *86400*

Paramètres du serveur DHCP (DHCPServer)

DHCPServer_SaveLeasePolicy

La règle qui doit être utilisée pour enregistrer la base de données des attributions sur le disque. Les paramètres possibles sont Disabled, ReconfShut ou ReconfShutTimer.

Valeur par défaut : *ReconfShut*

DHCPServer_AutoSaveLeaseInterval

La fréquence à laquelle la base de données des attributions doit être enregistrée sur le disque, si la valeur ReconfShutTimer est attribuée au paramètre DHCPServer_SaveLeasePolicy.

Valeur par défaut : *86400*

Paramètres IPsec

IKESendInitialContact

Détermine si la technologie IKE doit ou non envoyer le message de notification « Initial Contact » (contact initial). Ce message est envoyé à chaque passerelle distante lorsqu'une connexion est ouverte vers cette passerelle et qu'il n'y a pas d'association de sécurité IPsec antérieure qui utilise cette passerelle.

Valeur par défaut : *Enabled (Activé)*

IKESendCRLs

Précise si les listes de révocation des certificats (CRL - Certificate Revocation Lists) doivent être envoyées ou non en tant que partie intégrante de l'échange IKE. Ce paramètre doit normalement être activé, sauf lorsque l'hôte distant ne comprend pas les données utiles des listes de révocation des certificats.

Valeur par défaut : *Enabled (Activé)*

IKECRLValidityTime

Une liste de révocation des certificats contient un champ dédié à la « prochaine mise à jour » : il précise la date et l'heure à laquelle une nouvelle liste pourra être téléchargée à partir de l'autorité de certification. Le délai entre les mises à jour des listes de révocation des certificats peut aller de quelques heures à beaucoup plus, en fonction de la configuration de l'autorité de certification. La plupart des logiciels pour les autorités de certification permettent à l'administrateur de l'autorité de certification de publier de nouvelles listes de révocation des certificats à tout moment. Donc, même si le champ de la « prochaine mise à jour » indique qu'une nouvelle liste sera disponible dans 12 heures, il se peut qu’une soit déjà proposée pour le téléchargement.

Ce paramètre limite la durée de validité d'une liste de révocation des certificats. Une nouvelle liste de révocation des certificats est téléchargée lorsque le paramètre IKECRLValidityTime arrive à expiration ou lorsque le délai imparti selon le champ de la « prochaine mise à jour » est écoulé. L'événement déclencheur est celui qui se produit

en premier.

Valeur par défaut : *90000*

IKEMaxCAPath

Pour vérifier la signature d'un certificat utilisateur, NetDefendOS examine le champ « issuer name » (nom de l'émetteur) inclus dans ce certificat afin d'identifier le certificat d'autorité de certification en fonction duquel ce certificat a été signé. Ce certificat d'autorité de certification peut à son tour avoir été signé par une autre autorité de certification, qui peut aussi être signée par une autre autorité de certification, et ainsi de suite. Chaque certificat sera vérifié jusqu'à ce que l'un d'entre eux soit marqué comme fiable ou jusqu'à ce qu'il soit reconnu qu'aucun d'entre eux n'est fiable.

Si le nombre de certificats inclus dans ce chemin est supérieur à celui défini par ce paramètre, le certificat utilisateur est considéré comme non valide.

Valeur par défaut : *15*

IPsecCertCacheMaxCerts

Détermine le nombre maximal de certificats/listes de révocation de certificats qui peuvent être conservés dans la mémoire cache interne des certificats. Lorsque la mémoire cache des certificats arrive à saturation, les entrées sont supprimées en fonction d'un algorithme LRU (Least Recently Used), c'est-à-dire que les entrées qui n'ont pas été utilisées depuis le plus longtemps sont supprimées.

Valeur par défaut : *1024*

IPsecBeforeRules

Permet de transférer directement vers le moteur IPsec le trafic IKE et IPsec (ESP/AH) envoyé vers NetDefendOS, sans consultation de la règle définie.

Valeur par défaut : *Enabled (Activé)*

IPsecDeleteSAOnIPValidationFailure

Contrôle ce qui se passe pour les associations de sécurité si la validation IP en mode de configuration échoue. Si ce paramètre est activé, les associations de sécurité sont supprimées en cas d'échec.

Valeur par défaut : *Disabled (Désactivé)*

Paramètres de consignation

LogSendPerSecLimit

Ce paramètre limite le nombre de paquets de consignation que NetDefendOS peut envoyer par seconde. Vous ne devez jamais affecter une valeur trop faible à ce paramètre, car un nombre trop important d'événements risqueraient de ne pas être consignés. Mais vous ne devez pas non plus choisir une valeur trop élevée. Un cas dans lequel une valeur trop élevée pourrait générer des problèmes, c'est lorsque NetDefendOS envoie un message de consignation à un serveur dont le récepteur de consignation n'est pas actif. Ce serveur renverra en retour un message ICMP UNREACHABLE (injoignable), ce qui risque d'amener NetDefendOS à renvoyer un autre message de consignation. Le serveur générera encore une fois à son tour un autre message ICMP UNREACHABLE, et ainsi de suite. En limitant le nombre de messages de consignation que NetDefendOS envoie chaque seconde, vous éviterez ces scénarios catastrophiques, avec une forte consommation de bande passante.

Valeur par défaut : *3 600 secondes (soit une fois par heure)*

Paramètres de synchronisation temporelle

TimeSync_SyncInterval

Le nombre de secondes écoulées entre chaque nouvelle synchronisation.

Valeur par défaut : *86400*

TimeSync_MaxAdjust

Le décalage temporel maximal qu'un serveur est autorisé à ajuster.

Valeur par défaut : *3600*

TimeSync_ServerType

Le type de serveur pour la synchronisation temporelle, à savoir UDPTime ou SNTP (Simple Network Time Protocol).

Valeur par défaut : *SNTP*

TimeSync_GroupIntervalSize

Fréquence à laquelle les réponses serveur sont regroupées.

Valeur par défaut : *10*

TimeSync_TimeServerIP1

Nom de l'hôte DNS ou adresse IP du serveur horaire Timeserver 1.

Valeur par défaut : *none (aucun)*

TimeSync_TimeServerIP2

Nom de l'hôte DNS ou adresse IP du serveur horaire Timeserver 2.

Valeur par défaut : *none (aucun)*

TimeSync_TimeServerIP3

Nom de l'hôte DNS ou adresse IP du serveur horaire Timeserver 3.

Valeur par défaut : *none (aucun)*

TimeSync_TimeZoneOffs

Décalage en minutes entre les fuseaux horaires.

Valeur par défaut : *0*

TimeSync_DSTEnabled

Règle l'heure d'été en fonction des valeurs DSTOffs/DSTStartDate/DSTEndDate.

Valeur par défaut : *OFF (Désactivé)*

TimeSync_DSTOffs

Décalage en minutes avec l'heure d'été.

Valeur par défaut : *0*

TimeSync_DSTStartDate

Le mois et le jour de l'application de l'heure d'été, au format MM-JJ.

Valeur par défaut : *none (aucun)*

TimeSync_DSTEndDate

Le mois et le jour de fin de l'heure d'été, au format MM-JJ.

Valeur par défaut : *none (aucun)*

Paramètres PPP

PPP_L2TPBeforeRules

Transmet directement au serveur L2TP le trafic L2TP (Layer 2 Tunneling Protocol) envoyé au firewall D-Link, sans consultation de la règle définie.

Valeur par défaut : *Enabled (Activé)*

PPP_PPTPBeforeRules

Transmet directement au serveur PPTP le trafic PPTP (Point to Point Tunneling Protocol) envoyé au firewall D-Link, sans consultation de la règle définie.

Valeur par défaut : *Enabled (Activé)*

Paramètre du moniteur matériel

HWM_PollInterval

Fréquence d'interrogation du moniteur matériel, soit le délai en millisecondes entre les lectures des valeurs du moniteur matériel. Minimum : 100 ; maximum : 10 000.

Valeur par défaut : *500 millisecondes*

HWMMem_Interval

Fréquence d'interrogation de la mémoire, soit le délai en minutes entre les lectures des valeurs en mémoire. Minimum : 1 ; maximum : 200.

Valeur par défaut : *15 minutes*

HWMMem_LogRepetition

Indique s'il faut envoyer un message de consignation après chaque interrogation qui renvoie un niveau Alert (Alerte), Critical (Critique) ou Warning (Avertissement), ou s'il ne faut n'en envoyer un que lorsqu'il y a un changement de niveau. Si ce paramètre est défini sur True (Vrai), un message est envoyé chaque fois que le paramètre HWMMem_Interval est déclenché. S'il est défini sur False (Faux), un message est envoyé lorsqu'une valeur change de niveau.

Valeur par défaut : *False (Faux)*

HWMMem_UsePercent

Valeur True (Vrai) si l'unité utilisée pour la surveillance de la mémoire est le pourcentage ; valeur False (Faux) si l'unité est le méga-octet. S'applique aux valeurs HWMMem_AlertLevel, HWMMem_CriticalLevel et

HWMMem_WarningLevel.

Valeur par défaut : *True (vrai)*

HWMMem_AlertLevel

Génère un message de consignation de niveau Alert (alerte) si la mémoire disponible est inférieure à cette valeur. Vous pouvez désactiver ce paramètre en lui affectant la valeur 0. La valeur maximale est 10 000.

Valeur par défaut : *0*

HWMMem_CriticalLevel

Génère un message de consignation de niveau Critical (Critique) si la mémoire disponible est inférieure à cette valeur. Vous pouvez désactiver ce paramètre en lui affectant la valeur 0. La valeur maximale est 10 000.

Valeur par défaut : *0*

HWMMem_WarningLevel

Génère un message de consignation de niveau Warning (avertissement) si la mémoire disponible est inférieure à cette valeur. Vous pouvez désactiver ce paramètre en lui affectant la valeur 0. La valeur maximale est 10 000.

Valeur par défaut : *0*

Paramètres de réassemblage des paquets

Le réassemblage d'un paquet collecte les fragments IP afin de former des datagrammes IP complets. Pour le protocole TCP, l'opération de réassemblage réorganise ces segments de sorte à ce qu'ils soient traités dans l'ordre adéquat. Cela permet également d'assurer le suivi de chevauchements potentiels entre les segments et d'informer les autres sous-systèmes de ces chevauchements. Les paramètres associés limitent la quantité de mémoire utilisée par le sous-système de réassemblage.

Reassembly_MaxConnections

Ce paramètre définit le nombre de connexions que le système de réassemblage peut utiliser simultanément. Il est exprimé en pourcentage du nombre total de connexions autorisées. Minimum : 1 ; maximum : 100.

Valeur par défaut : *80*

Reassembly_MaxProcessingMem

Ce paramètre précise la quantité de mémoire que le système de réassemblage peut allouer pour traiter les paquets. Il est exprimé en pourcentage de la quantité de mémoire totale disponible. Minimum : 1 ; maximum : 100.

Valeur par défaut : *3*

Autres paramètres

BufFloodRebootTime

Comme solution ultime, NetDefendOS redémarre automatiquement si ses mémoires tampons sont en surcharge depuis une longue durée. Ce paramètre précise cette durée.

Valeur par défaut : *3600*

MaxPipeUsers

Le nombre maximal d'utilisateurs de tuyaux qu'il est possible d'allouer. Étant donné que le suivi des utilisateurs de

tuyaux n'est assuré que pendant un 20^{e} de seconde, vous n'avez en règle générale pas besoin de rapprocher ce nombre du nombre réel d'utilisateurs, ni du nombre de connexions surveillées de manière dynamique. Si aucun tuyau n'est configuré, aucun utilisateur de tuyau ne sera alloué, quelle que soit la valeur de ce paramètre. Pour plus d'informations sur les tuyaux et les utilisateurs de tuyaux, reportez-vous au chapitre 10, intitulé « Gestion du trafic ».

Valeur par défaut : *512*

Annexe A. Abonnement aux mises à jour de sécurité

Introduction

Les modules antivirus (AV), de détection et de prévention des intrusions (IDP) et de filtrage de contenu Web dynamique de NetDefendOS utilisent tous des bases de données D-Link externes, qui contiennent des informations sur les derniers virus, les menaces de sécurité et la catégorisation d'URL. Ces bases de données sont en permanence mises à jour. Pour avoir accès aux dernières mises à jour, vous devez vous abonner aux mises à jour de sécurité D-Link. Pour cela, procédez comme suit :

Achetez un abonnement auprès de votre revendeur local D-Link.

Vous recevrez alors un code d'activation unique pour vous identifier en tant qu'utilisateur du service.

Sur l'interface Web de votre firewall D-Link, sélectionnez Maintenance > License (Maintenance > Licence), puis saisissez ce code d'activation. NetDefendOS indique que le code est accepté et active le service de mise à jour. (Assurez-vous que vous avez accès à l'Internet public lors de cette opération.)

Remarque

Un « guide d'inscription » détaillé expliquant les procédures d'inscription et de service de mise à jour peut être téléchargé sur le site Web de D-Link.

Renouvellement de l'abonnement

Sur l'interface Web, sélectionnez Maintenance > License (Maintenance > Licence) et vérifiez les services de mise à jour qui sont activés ainsi que leur date d'expiration.

Attention

Pensez à renouveler votre abonnement avant la fin de l'abonnement en cours !

Contrôle des mises à jour des bases de données

Sur l'interface Web, sélectionnez Maintenance > Update (Maintenance > Mise à jour) pour configurer la mise à jour automatique des bases de données. Vous pouvez également vérifier la date de la dernière mise à jour ainsi que son état.

Par ailleurs, cette section de l'interface Web vous permet aussi de lancer manuellement la mise à jour en sélectionnant Update now (Mettre à jour maintenant), afin de télécharger les dernières signatures dans la base de données.

Commandes console des bases de données

Les bases de données IDP et antivirus (AV) peuvent être contrôlées directement via plusieurs commandes console.

Anticiper les mises à jour des bases de données. Il est possible d'appliquer la mise à jour d'une base de données

IDP à tout moment à l'aide de la commande suivante :

```
gw-world:/> updatecenter -update IDP
```

De la même façon, une mise à jour de la base de données antivirus peut être lancée à l'aide de la commande suivante :

```
gw-world:/> updatecenter -update Antivirus
```

Obtenir l'état des mises à jour. Pour obtenir l'état des mises à jour IDP, utilisez la commande suivante :

```
gw-world:/> updatecenter -status IDP
```

Pour obtenir l'état des mises à jour AV :

```
gw-world:/> updatecenter -status Antivirus
```

Obtenir l'état des serveurs. Pour obtenir l'état des serveurs de réseau D-Link, utilisez la commande suivante :

```
gw-world:/> updatecenter -servers
```

Supprimer les bases de données locales. Certains problèmes techniques touchant le fonctionnement des modules IDP ou antivirus peuvent se résoudre par la suppression de la base de données, suivie d'un redémarrage. Pour la base de données IDP, utilisez la commande suivante :

```
gw-world:/> removedb IDP
```

Pour supprimer la base de données antivirus, utilisez la commande suivante :

```
gw-world:/> removedb Antivirus
```

Une fois les bases de données supprimées, vous devez redémarrer le système et lancer une mise à jour des bases de données. Il est également recommandé de supprimer la base de données si la base IDP ou antivirus n'est pas utilisée pendant de longues périodes.

Remarque

L'optimisation des mises à jour de la base de données antivirus exige quelques secondes après le téléchargement d'une mise à jour. Par conséquent, le fonctionnement du firewall est momentanément interrompu. Il peut alors être préférable de planifier les mises à jour au moment où le trafic est réduit, comme par exemple tôt le matin. La suppression d'une base de données peut également entraîner une interruption du fonctionnement.

Annexe B. Groupes de signatures IDP

Pour l'analyse IDP, les groupes de signatures ci-dessous peuvent être sélectionnés. Ces groupes sont disponibles uniquement pour le service IDP avancé de D-Link. Une version de chaque groupe se trouve sous les trois *types* IDS, IPS et Policy (Règle). Pour plus d'informations, reportez-vous à la section intitulée « Prévention et détection des intrusions ».

Nom de groupe	**Type d'intrusion**
APP_AMANDA	Amanda, logiciel de sauvegarde répandu
APP_ETHEREAL	Ethereal
APP_ITUNES	Lecteur Apple iTunes
APP_REALPLAYER	Lecteur multimédia de RealNetworks
APP_REALSERVER	Lecteur RealServer RealNetworks
APP_WINAMP	WinAMP
APP_WMP	Lecteur multimédia MS Windows
AUTHENTICATION_GENERAL	Authentification
AUTHENTICATION_KERBEROS	Kerberos
AUTHENTICATION_XTACACS	XTACACS
BACKUP_ARKEIA	Solution de sauvegarde réseau
BACKUP_BRIGHTSTOR	Solutions de sauvegarde de CA
BACKUP_GENERAL	Solutions générales de sauvegarde
BACKUP_NETVAULT	Solution de sauvegarde NetVault
BACKUP_VERITAS	Solutions de sauvegarde
BOT_GENERAL	Activités liées aux robots, y compris ceux contrôlés par canaux IRC
BROWSER_FIREFOX	Mozilla Firefox
BROWSER_GENERAL	Attaques générales visant les clients/navigateurs Web
BROWSER_IE	Microsoft IE
BROWSER_MOZILLA	Mozilla Browser
COMPONENT_ENCODER	Encodeurs intégrés à une attaque
COMPONENT_INFECTION	Infection intégrée à une attaque
COMPONENT_SHELLCODE	Code shell intégré aux attaques
DB_GENERAL	Systèmes de base de données
DB_MSSQL	MS SQL Server
DB_MYSQL	MySQL DBMS
DB_ORACLE	Oracle DBMS
DB_SYBASE	Serveur Sybase
DCOM_GENERAL	MS DCOM
DHCP_CLIENT	Activités liées au client DHCP

279

Nom de groupe	Type d'intrusion
DHCP_GENERAL	Protocole DHCP
DHCP_SERVER	Activités liées au serveur DHCP
DNS_EXPLOIT	Attaques DNS
DNS_GENERAL	Systèmes de noms de domaine
DNS_OVERFLOW	Attaque par débordement DNS
DNS_QUERY	Attaques liées aux requêtes
ECHO_GENERAL	Protocole/mises en œuvre Echo
ECHO_OVERFLOW	Débordement de la mémoire tampon Echo
FINGER_BACKDOOR	Finger backdoor
FINGER_GENERAL	Protocole/mise en œuvre Finger
FINGER_OVERFLOW	Débordement de protocole/mise en œuvre Finger
FS_AFS	Andrew File System
FTP_DIRNAME	Attaque des noms de répertoire
FTP_FORMATSTRING	Attaque des chaînes de format
FTP_GENERAL	Protocole/mise en œuvre FTP
FTP_LOGIN	Attaques de connexion
FTP_OVERFLOW	Saturation de la mémoire tampon FTP
GAME_BOMBERCLONE	Jeu Bomberclone
GAME_GENERAL	Serveurs/clients de jeux génériques
GAME_UNREAL	Serveur UnReal Game
HTTP_APACHE	Apache httpd
HTTP_BADBLUE	Serveur Web Badblue
HTTP_CGI	HTTP CGI
HTTP_CISCO	Serveur Web intégré Cisco
HTTP_GENERAL	Activités générales HTTP
HTTP_MICROSOFTIIS	Attaques HTTP propres au serveur Web MS IIS
HTTP_OVERFLOWS	Saturation de la mémoire tampon des serveurs HTTP
HTTP_TOMCAT	Tomcat JSP
ICMP_GENERAL	Protocole/mise en œuvre ICMP
IGMP_GENERAL	IGMP
IMAP_GENERAL	Protocole/mise en œuvre IMAP
IM_AOL	AOL IM
IM_GENERAL	Mises en œuvre d'Instant Messenger
IM_MSN	MSN Messenger
IM_YAHOO	Yahoo Messenger
IP_GENERAL	Protocole/mise en œuvre IP
IP_OVERFLOW	Débordement de protocole/mise en œuvre IP
IRC_GENERAL	Internet Relay Chat
LDAP_GENERAL	Clients/serveurs LDAP généraux
LDAP_OPENLDAP	LDAP ouvert
LICENSE_CA-LICENSE	Gestion des licences des logiciels CA
LICENSE_GENERAL	Gestionnaire global des licences
MALWARE_GENERAL	Attaque de programme malveillant
METASPLOIT_FRAME	Attaque de structure Metasploit

Groupes de signature IDP

Nom de groupe	Type d'intrusion
METASPLOIT_GENERAL	Attaque générale de Metasploit
MISC_GENERAL	Attaque générale
MSDTC_GENERAL	MS DTC
MSHELP_GENERAL	Microsoft Windows Help
NETWARE_GENERAL	NetWare Core Protocol
NFS_FORMAT	Format
NFS_GENERAL	Protocole/mise en œuvre NFS
NNTP_GENERAL	Protocole/mise en œuvre NNTP
OS_SPECIFIC-AIX	AIX
OS_SPECIFIC-GENERAL	Système d'exploitation général
OS_SPECIFIC-HPUX	HP-UX
OS_SPECIFIC-LINUX	Linux
OS_SPECIFIC-SCO	SCO
OS_SPECIFIC-SOLARIS	Solaris
OS_SPECIFIC-WINDOWS	Windows
P2P_EMULE	Outil P2P eMule
P2P_GENERAL	Outils P2P généraux
P2P_GNUTELLA	Outil P2P Gnutella
PACKINGTOOLS_GENERAL	Attaques générales d'outils de compression
PBX_GENERAL	PBX
POP3_DOS	Déni de service (Dos) pour POP
POP3_GENERAL	Protocole POP3
POP3_LOGIN-ATTACKS	Recherche de mot de passe et attaque de connexion associée
POP3_OVERFLOW	Débordement du serveur POP3
POP3_REQUEST-ERRORS	Erreur de requête
PORTMAPPER_GENERAL	PortMapper
PRINT_GENERAL	Serveur d'impression LP : LPR LPD
PRINT_OVERFLOW	Débordement de protocole/mise en œuvre LPR/LPD
REMOTEACCESS_GOTOMYPC	GotoMYPC
REMOTEACCESS_PCANYWHERE	PcAnywhere
REMOTEACCESS_RADMIN	Remote Administrator (radmin)
REMOTEACCESS_VNC-CLIENT	Attaques visant les clients VNC
REMOTEACCESS_VNC-SERVER	Attaque visant les serveurs VNC
REMOTEACCESS_WIN-TERMINAL	Terminal Windows/Remote Desktop
RLOGIN_GENERAL	Protocole/mise en œuvre RLogin
RLOGIN_LOGIN-ATTACK	Attaques de connexion
ROUTER_CISCO	Attaque de routeur Cisco

281

Nom de groupe	Type d'intrusion
ROUTER_GENERAL	Attaque générale de routeur
ROUTING_BGP	Protocole de routeur BGP
RPC_GENERAL	Protocole/mise en œuvre RFC
RPC_JAVA-RMI	RMI Java
RSYNC_GENERAL	Rsync
SCANNER_GENERAL	Scanners génériques
SCANNER_NESSUS	Scanner Nessus
SECURITY_GENERAL	Solutions antivirus
SECURITY_ISS	Logiciel Internet Security Systems
SECURITY_MCAFEE	McAfee
SECURITY_NAV	Solution antivirus Symantec
SMB_ERROR	Erreur SMB
SMB_EXPLOIT	SMB Exploit
SMB_GENERAL	Attaques SMB
SMB_NETBIOS	Attaques NetBIOS
SMB_WORMS	Vers SMB
SMTP_COMMAND-ATTACK	Attaque de commande SMTP
SMTP_DOS	Déni de service (Dos) pour SMTP
SMTP_GENERAL	Protocole/mise en œuvre SMTP
SMTP_OVERFLOW	Débordement SMTP
SMTP_SPAM	SPAM
SNMP_ENCODING	Encodage SNMP
SNMP_GENERAL	Protocole/mise en œuvre SNMP
SOCKS_GENERAL	Protocole/mise en œuvre SOCKS
SSH_GENERAL	Protocole/mise en œuvre SSH
SSH_LOGIN-ATTACK	Recherche de mot de passe et attaques de connexion associée
SSH_OPENSSH	Serveur OpenSSH
SSL_GENERAL	Protocole/mise en œuvre SSL
TCP_GENERAL	Protocole/mise en œuvre TCP
TCP_PPTP	Protocole PPTP
TELNET_GENERAL	Protocole/mise en œuvre Telnet
TELNET_OVERFLOW	Attaque par débordement Telnet
TFTP_DIR_NAME	Attaque des noms de répertoire
TFTP_GENERAL	Protocole/mise en œuvre TFTP
TFTP_OPERATION	Attaque de l'exploitation
TFTP_OVERFLOW	Attaque par débordement TFTP
TFTP_REPLY	Attaque de réponse TFTP
TFTP_REQUEST	Attaque de requête TFTP
TROJAN_GENERAL	Chevaux de Troie
UDP_GENERAL	UDP général
UDP_POPUP	Fenêtre contextuelle pour MS Windows
UPNP_GENERAL	UPNP
VERSION_CVS	CVS
VERSION_SVN	Subversion

Groupes de signature IDP

Nom de groupe	Type d'intrusion
VIRUS_GENERAL	Virus
VOIP_GENERAL	Protocole/mise en œuvre VoIP
VOIP_SIP	Protocole/mise en œuvre SIP
WEB_CF-FILE-INCLUSION	Inclusion de fichiers en coldfusion
WEB_FILE-INCLUSION	Inclusion de fichiers
WEB_GENERAL	Attaques d'applications Web
WEB_JSP-FILE-INCLUSION	Inclusion de fichiers JSP
WEB_PACKAGES	Packages d'applications Web répandues
WEB_PHP-XML-RPC	PHP XML RPC
WEB_SQL-INJECTION	SQL Injection
WEB_XSS	Cross-Site-Scripting
WINS_GENERAL	MS WINS Service
WORM_GENERAL	Vers
X_GENERAL	Applications X génériques

283

Annexe C. Types de fichiers MIME vérifiés

La passerelle ALG (Application Layer Gateway) HTTP peut vérifier que le contenu des fichiers téléchargés via le protocole HTTP correspond au type de fichier indiqué par leur nom.

Cette annexe répertorie les types de fichiers MIME qui peuvent être vérifiés par NetDefendOS afin de garantir que le contenu correspond bien au type de fichier d'un téléchargement. La vérification est effectuée si l'option *Check MIME Type* (Vérifier type MIME) est activée comme indiqué dans la section intitulée « HTTP ». Par ailleurs, la vérification est toujours effectuée si le type de fichier est sélectionné dans la liste *Allow Selected* (Autorisé les types sélectionnés) pour une passerelle ALG HTTP.

Extension de type de fichier	Application
3ds	Fichiers 3d Studio
3gp	Fichiers multimédia 3GPP
aac	Fichiers MPEG-2 Advanced Audio Coding
ab	Applix Builder
ace	Archive ACE
ad3	Fichiers son compressés pour systèmes Dec
ag	Fichiers Applix Graphic
aiff, aif	Fichiers Audio Interchange
am	Applix SHELF Macro
arc	Fichiers d'archive
alz	Fichiers compressés ALZip
avi	Fichiers Audio Video Interleave
arj	Archive compressée
ark	Archive de fichiers compressés QuArk
arq	Archive compressée
as	Fichiers Applix Spreadsheet
asf	Fichiers Advanced Streaming Format
avr	Son Audio Visual Research
aw	Fichiers Applix Word
bh	Fichiers de format d'archive Blackhole
bmp	Graphiques Windows Bitmap
box	Fichiers de messages vocaux VBOX
bsa	Archive compressée BSARC
bz, bz2	Fichiers compressés Bzip UNIX
cab	Fichiers Microsoft Cabinet
cdr	Fichiers Corel Vector Graphic Drawing

284

Types de fichiers MIME vérifiés

Extension de type de fichier	Application
cgm	Computer Graphics Metafile
chz	Archive de fichiers compressés ChArc
class	Pseudo-code Java
cmf	Creative Music file
core/coredump	Unix core dump
cpl	Fichiers Windows Control Panel Extension
dbm	Fichiers de base de données
dcx	Fichiers Bitmap Multipage PCX
deb	Fichiers Debian Linux Package
djvu	Fichiers DjVu
dll	Fichiers de bibliothèque de liens dynamiques Windows
dpa	Données d'archive DPA
dvi	Document TeX Device Independent
eet	Archive EET
egg	Fichier de données Allegro
elc	Code source compilé eMacs Lisp Byte
emd	Fichier ABT EMD Module/Song Format
esp	Données d'archive ESP
exe	Exécutable Windows
fgf	Fichiers Free Graphics Format
flac	Fichiers Free Lossless Audio Codec
flc	FLIC Animated Picture
fli	FLIC Animation
flv	Macromedia Flash Video
gdbm	Fichiers de base de données
gif	Fichiers Graphic Interchange Format
gzip, gz, tgz	Archive compressée Gzip
hap	Données d'archive HAP
hpk	Archive de fichiers compressés HPack
hqx	Archive compressée Macintosh BinHex 4
icc	Kodak Color Management System, profil ICC
icm	Fichiers Microsoft ICM Color Profile
ico	Fichiers Windows Icon
imf	Données sonores Imago Orpheus
Inf	Fichiers d'informations Sidplay
it	Impulse Tracker Music Module
java	Code source Java

285

Extension de type de fichier	Application
jar	Archive Java JAR
jng	Format vidéo JNG
jpg, jpeg, jpe, jff, jfif, jif	Fichiers JPEG
jrc	Archive compressée Jrchive
jsw	Just System Word Processor Ichitaro
kdelnk	Fichier lien KDE
lha	Archive de fichiers compressés LHA
lim	Archive compressée Limit
lisp	Données d'archive LIM
lzh	Archive de fichiers compressés LZH
md	Archive de fichiers compressés MDCD
mdb	Microsoft Access Database
mid,midi	Musical Instrument Digital Interface MIDI-sequention Sound
mmf	Yamaha SMAF Synthetic Music Mobile Application Format
mng	Multi-image Network Graphic Animation
mod	Données sonores Ultratracker
mp3	MPEG Audio Stream, Layer III
mp4	Fichiers vidéo MPEG-4
mpg,mpeg	Fichiers vidéo MPEG 1 System Stream
mpv	Fichiers vidéo MPEG-1
Fichiers Microsoft	Fichiers Miscrosoft Office et autres fichiers Microsoft
msa	Données d'archive Atari MSA
niff, nif	Navy Interchange file Format Bitmap
noa	Nancy Video CODEC
nsf	Fichiers son NES
obj, o	Fichiers objet Windows, fichiers objet Linux
ocx	Object Linking and Embedding (OLE) Control Extension
ogg	Fichiers WAV compressés Ogg Vorbis Codec
out	Exécutable Linux
pac	Données d'archive CrossePAC
pbf	Image Portable Bitmap Format
pbm	Portable Bitmap Graphic
pdf	Acrobat Portable Document Format
pe	Fichiers Portable Executable
pfb	PostScript Type 1 Font
pgm	Portable Graymap Graphic
pkg	SysV R4 PKG Datastreams
pll	Données d'archive PAKLeo
pma	Données d'archive PMarc
png	Portable (Public) Network Graphic
ppm	PBM Portable Pixelmap Graphic
ps	Fichiers PostScript
psa	Données d'archive PSA
psd	Fichiers Photoshop Format

Types de fichiers MIME vérifiés

Extension de type de fichier	Application
qt, mov, moov	Fichiers QuickTime Movie
qxd	Document QuarkXpress
ra, ram	RealMedia Streaming Media
rar	Archive compressée WinRAR
rbs	Fichiers ReBirth Song
riff, rif	Fichiers Microsoft Audio
rm	RealMedia Streaming Media
rpm	RedHat Package Manager
rtf, wri	Fichiers Rich Text Format
sar	Archive compressée Streamline
sbi	Fichiers SoundBlaster Instrument
sc	Tableur SC
sgi	Fichiers Silicon Graphics IRIS
sid	Fichiers de musique Commodore64 (C64) (fichiers SID)
sit	Archives StuffIt
sky	Archive compressée SKY
snd, au	Fichiers audio Sun/NeXT
so	Fichiers de librairie partagée UNIX
sof	Archive ReSOF
sqw	Données d'archive SQWEZ
sqz	Données d'archive Squeeze It
stm	Scream Tracker v2 Module
svg	Fichiers Scalable Vector Graphics
svr4	SysV R4 PKG Datastreams
swf	Fichiers Macromedia Flash Format
tar	Fichiers Tape Archive
tfm	Données TeX font metric
tiff, tif	Fichiers Tagged Image Format
tnef	Transport Neutral Encapsulation Format
torrent	Fichiers BitTorrent Metainfo
ttf	TrueType Font
txw	Fichiers audio Yamaha TX Wave
ufa	Données d'archive UFA
vcf	Fichiers Vcard
viv	Fichiers vidéo en streaming VivoActive Player
wav	Waveform Audio
wk	Documents Lotus 1-2-3

287

Extension de type de fichier	Application
wmv	Windows Media file
wrl, vrml	Fichiers Plain Text VRML
xcf	Fichiers d'image GIMP
xm	Fichiers audio Fast Tracker 2 Extended Module
xml	Fichiers XML
xmcd	Fichiers de base de données xmcd pour kscd
xpm	BMC Software Patrol UNIX Icon file
yc	Archive compressée YAC
zif	Image ZIF
zip	Archive de fichiers compressés Zip
zoo	Archive de fichiers compressés ZOO
zpk	Données d'archive ZPack
z	Fichiers compressés Unix

Annexe D. La structure OSI

Le modèle OSI (Open Systems Interconnection) définit une structure pour les communications entre ordinateurs. Il classe les différents protocoles d'un grand nombre d'applications réseau en sept couches plus petites et par conséquent, plus simples à gérer. Ce modèle décrit comment transférer, via un support réseau, les données d'une application d'un ordinateur vers une application d'un autre ordinateur.

Le contrôle du trafic de données passe d'une couche à la suivante ; il commence au niveau de la couche « application » d'un ordinateur, soit la couche du bas, puis est transféré via le support vers un autre ordinateur pour atteindre finalement le haut de la hiérarchie. Chaque couche gère un ensemble de protocoles, de sorte que les tâches visant à atteindre une application peuvent être réparties sur différentes couches et être mises en œuvre séparément.

Figure D.1. Les 7 couches du modèle OSI

Numéro de couche	Objet de la couche
Couche 7	Application
Couche 6	Présentation
Couche 5	Session
Couche 4	Transport
Couche 3	Réseau
Couche 2	Liaison de données
Couche 1	Physique

Chaque couche a une fonction propre :

Couche « application » Définit l'interface utilisateur qui prend directement en charge les applications. Protocoles : HTTP, FTP, DNS, SMTP, Telnet, SNMP, etc.

Couche « présentation » Convertit les différentes applications de façon à uniformiser les formats réseau identifiables par les autres couches.

Couche « session » Établit, gère et ferme les sessions sur le réseau. Protocoles : NetBIOS, RPC, etc.

Couche « transport » Contrôle le flux des données et permet le traitement des erreurs. Protocoles : TCP, UDP, etc.

Couche « réseau » Effectue l'adressage et le routage. Protocoles : IP, OSPF, ICMP, IGMP, etc.

Couche « liaison de données » Crée une structure de données pour la transmission sur la couche « physique » et permet la vérification/correction des erreurs. Protocoles : Ethernet, PPP, etc.

Couche « physique » Définit les connexions matérielles physiques.

289

Annexe E. Bureaux internationaux de D-Link

Vous trouverez ci-dessous la liste complète des bureaux de ventes internationaux de D-Link. Pour plus de détails sur la prise en charge des produits D-Link ainsi que sur les coordonnées du support local, consultez le site Web associé à votre pays.

Australie	1 Giffnock Avenue, North Ryde, NSW 2113, Australia. TEL. : 61-2-8899-1800, FAX : 61-2-8899-1868. Site Web : www.dlink.com.au
Belgique	Rue des Colonies 11, B-1000 Brussels, Belgium. TEL. : +32(0)2 517 7111, Fax : +32(0)2 517 6500. Site Web : www.dlink.be
Brésil	Av das Nacoes Unidas, 11857 – 14- andar - cj 141/142, Brooklin Novo, Sao Paulo - SP - Brazil. CEP 04578-000 (code postal) TEL. : (55 11) 21859300, FAX : (55 11) 21859322. Site Web : www.dlinkbrasil.com.br
Canada	2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada. TEL. : 1-905-8295033, FAX : 1-905-8295223. Site Web : www.dlink.ca
Chine	No.202,C1 Building, Huitong Office Park, No. 71, Jianguo Road, Chaoyang District, Beijing, 100025, China. TEL. : +86-10-58635800, FAX : +86-10-58635799. Site Web : www.dlink.com.cn
République tchèque	Vaclavske namesti 36, Praha 1, Czech Republic. TEL. : +420 (603) 276 589 Site Web : www.dlink.cz
Danemark	Naverland 2, DK-2600 Glostrup, Copenhagen Denmark. TEL. : 45-43-969040, FAX : 45-43-424347. Site Web : www.dlink.dk
Égypte	47, El Merghany street, Heliopolis, Cairo-Egypt. TEL. : +202-2919035, +202-2919047, FAX : +202-2919051. Site Web : www.dlink-me.com
Europe (R.U.)	4th Floor, Merit House, Edgware Road, Colindale, London NW9 5AB, UK. TEL. : 44-20-8731-5555, FAX : 44-20-8731-5511. Site Web : www.dlink.co.uk
Finlande	Latokartanontie 7A, FIN-00700 HELSINKI, Finland. TEL. : +358-10 3098840, FAX : +358-10 309 8841. Site Web : www.dlink.fi
France	2, Allée de la Fresnerie, 78330 Fontenay le Fleury, France. TEL. : 33-1-30238688, FAX : 33-1-30238689. Site Web : www.dlink.fr
Allemagne	Schwalbacher Strasse 74, D-65760 Eschborn, Germany. TEL. : 49-6196-77990, FAX : 49-6196-7799300. Site Web : www.dlink.de
Grèce	101, Panagoulis Str. 163-43, Helioupolis Athens, Greece. TEL. : +30 2109914512, FAX : +30 210 9916902. Site Web : www.dlink.gr
Hongrie	R-k-czi-t 70-72, HU-1074, Budapest, Hungary. TEL. : +36 (0) 1 461 30 00, FAX : +36 (0) 1 461 30 09. Site Web : www.dlink.hu
Inde	D-Link House, Kurla Bandra Complex Road, Off CST Road, Santacruz (East), Mumbai - 400098, India. TEL. : 91-022-26526696/56902210, FAX : 91-022-26528914. Site Web : www.dlink.co.in
Israël	11 Hamanofim Street, Ackerstein Towers, Regus Business Center, P.O.B 2148, Hertzelia-Pituach 46120, Israel. TEL. : +972-9-9715700, FAX : +972-9-9715601. Site Web : www.dlink.co.il

Italie	Via Nino Bonnet n. 6/b, 20154 – Milano, Italy. TEL. : 39-02-2900-0676, FAX : 39-02-2900-1723. Site Web : www.dlink.it
Amérique latine	Isidora Goyeechea 2934, Ofcina 702, Las Condes, Santiago – Chile. TEL. : 56-2-232-3185, FAX : 56-2-232-0923. Site Web : www.dlink.cl
Luxembourg	Rue des Colonies 11, B-1000 Brussels, Belgium TEL : +32 (0)2 517 7111, FAX : +32 (0)2 517 6500. Site Web : www.dlink.be
Moyen-Orient (Dubaï)	P.O.Box : 500376, Office : 103, Building : 3, Dubai Internet City, Dubai, United Arab Emirates. TEL. : +971-4-3916480, Fax : +971-4-3908881. Site Web : www.dlink-me.com
Pays-Bas	Weena 290, 3012 NJ, Rotterdam, Netherlands. TEL. : +31-10-282-1445, FAX : +31-10-282-1331. Site Web : www.dlink.nl
Norvège	Karihaugveien 89 N-1086 Oslo, Norway. TEL. : +47 99 300 100, FAX : +47 22 30 95 80. Site Web : www.dlink.no
Pologne	Budynek Aurum ul. Walic-w 11, PL-00-851, Warszawa, Poland. TEL. : +48 (0) 22 583 92 75, FAX : +48 (0) 22 583 92 76. Site Web : www.dlink.pl
Portugal	Rua Fernando Pahla, 50 Edificio Simol, 1900 Lisbon, Portugal. TEL. : +351 21 8688493. Site Web : www.dlink.es
Russie	Grafsky per., 14, floor 6, Moscow, 129626 Russia. TEL. : 7-495-744-0099, FAX : 7-495-744-0099 #350. Site Web : www.dlink.ru
Singapour	1 International Business Park, #03-12 The Synergy, Singapore 609917. TEL : 65-6774-6233, FAX : 65-6774-6322. Site Web : www.dlink-intl.com
Afrique du Sud	Einstein Park II, Block B, 102-106 Witch-Hazel Avenue, Highveld Technopark, Centurion, Gauteng, Republic of South Africa. TEL. : 27-12-665-2165, FAX : 27-12-665-2186. Site Web : www.d-link.co.za
Espagne	Avenida Diagonal, 593-95, 9th floor, 08014 Barcelona, Spain. TEL. : 34 93 4090770, FAX : 34 93 4910795. Site Web : www.dlink.es
Suède	P.O. Box 15036, S-167 15 Bromma, Sweden. TEL. : 46-(0)8564-61900, FAX : 46-(0)8564-61901. Site Web : www.dlink.se
Suisse	Glatt Tower, 2.OG CH-8301, Glattzentrum Postfach 2.OG, Switzerland. TEL. : +41 (0) 1 832 11 00, FAX : +41 (0) 1 832 11 01. Site Web : www.dlink.ch
Taïwan	No. 289 , Sinhu 3rd Rd., Neihu District, Taipei City 114, Taiwan. TEL. : 886-2-6600-0123, FAX : 886-2-6600-1188. Site Web : www.dlinktw.com.tw
Turquie	Cetin Emec Bulvari, 74.sokak, ABC Plaza No:9/3, Ovecler/Ankara- TURKEY. TEL. : 0090 312 473 40 55, FAX : 0090 312 473 40 58. Site Web : www.dlink.com.tr
États-Unis	17595 Mt. Herrmann Street, Fountain Valley, CA 92708. TEL. : 1-800-326-1688. Site Web : www.dlink.com

Alphabetical Index

A

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z