Configuration Guide

How to Configure IPSec VPN Tunnel between DSR Router and DFL Firewall

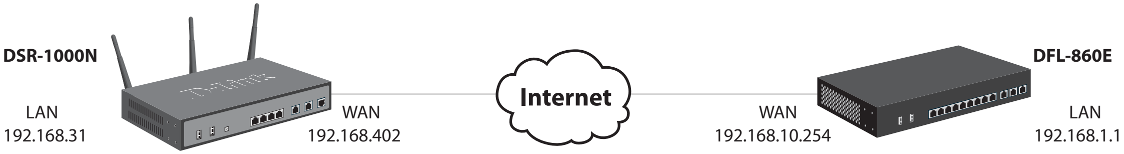
Overview

This document describes how to configure the D-Link DSR routers to implement IPSec gateway to gateway with pre-shared secrets. This use case will cover IPSec VPN tunnel configuration between D-Link DSR-1000N router and DFL-860E firewall

D-Link®

Situation note

The IPSec VPN tunnel is the most secure and popular approach to ensure end-to-end data security across Internet. This document will be very useful when you intend to create IPSec VPN tunnel.



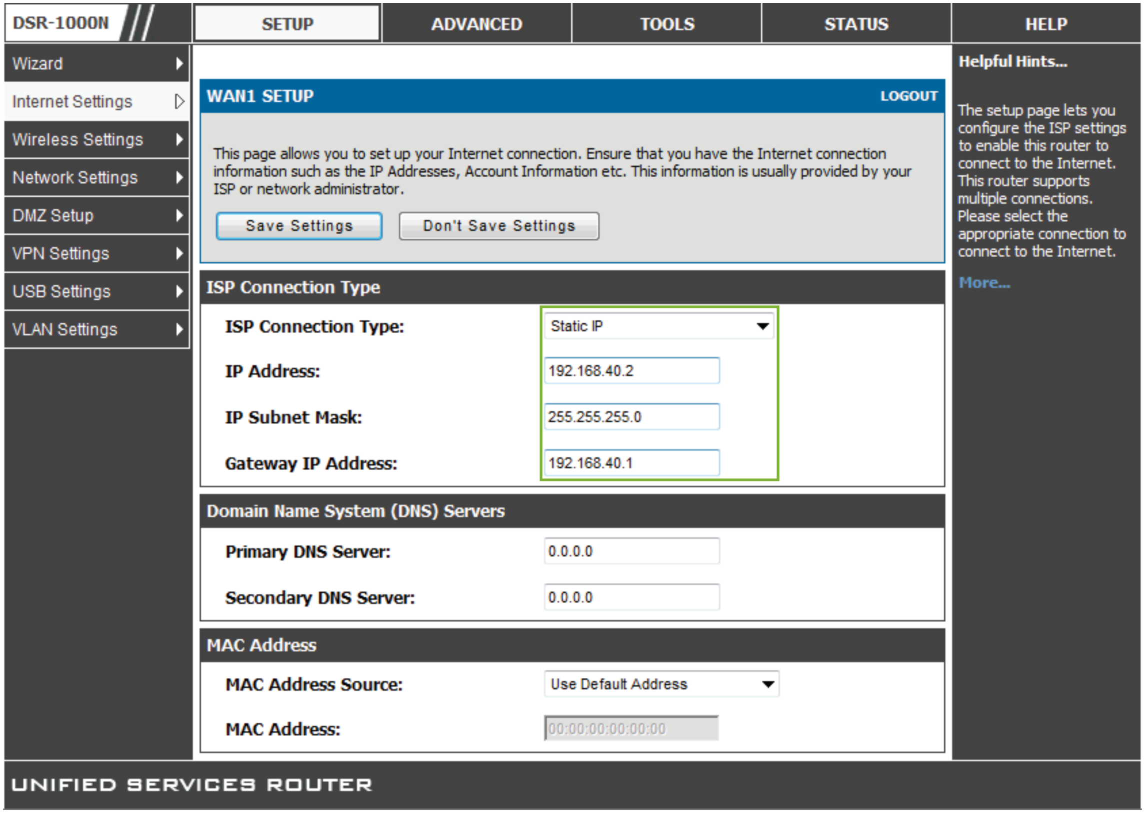
The settings of DFL-860E

```
set Interface Ethernet wan1 DHCPEnabled=No
set Interface Ethernet wan1 DefaultGateway=192.168.10.1
set Address IP4Address InterfaceAddresses/wan1_ip Address=192.168.10.254
set Address IP4Address InterfaceAddresses/wan1net Address=192.168.10.0/24
add PSK ipsec-psk Type=ASCII PSKAscii=testtest

add Interface IPsecTunnel ipsec-if AuthMethod=PSK IKEAlgorithms=Medium IPsecAlgorithms=Medium
PSK=ipsec-psk LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=192.168.3.0/24 Remote
Endpoint=192.168.40.2

add Interface InterfaceGroup ipsec-lan Members=ipsec-if,lan

add IPRule Action=Allow SourceInterface=ipsec-lan SourceNetwork=all-nets DestinationInterface=ipsec-lan
DestinationNetwork=all-nets Service=all_services Index=1 LogEnabled=Yes Name=ipsec-lan-allow
```

Configuration step of DSR-1000N

1. Go to SETUP -> Internet Settings -> WAN1 Settings -> WAN1 Setup, change the ISP connection type and its IP information as following.

ISP Connection type: **Static IP**
IP Address: **192.168.40.2**
IP Subnet Mask: **255.255.255.0**
Gateway IP Address: **192.168.40.1**



WAN1 SETUP

This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.

ISP Connection Type

ISP Connection Type:	Static IP
IP Address:	192.168.40.2
IP Subnet Mask:	255.255.255.0
Gateway IP Address:	192.168.40.1

Domain Name System (DNS) Servers

Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

MAC Address

MAC Address Source:	Use Default Address
MAC Address:	00:00:00:00:00:00

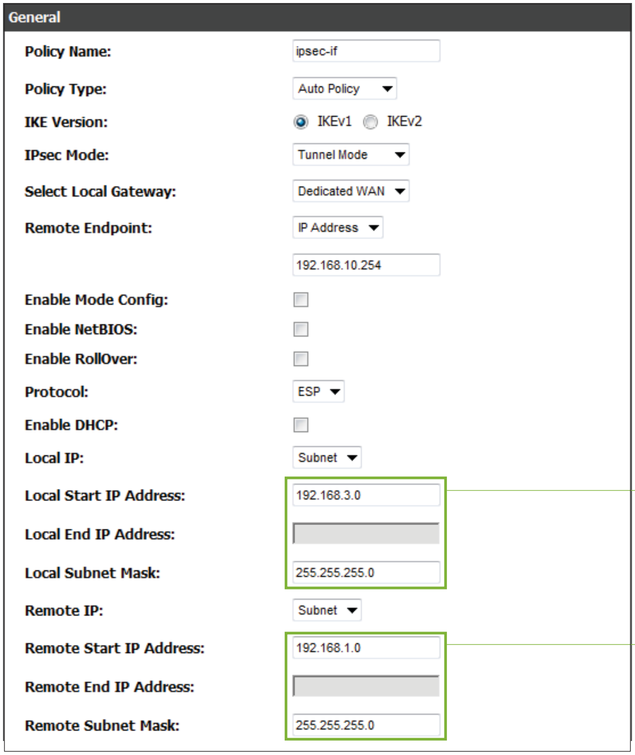
Helpful Hints...

The setup page lets you configure the ISP settings to enable this router to connect to the Internet. This router supports multiple connections. Please select the appropriate connection to connect to the Internet.

2. Go to SETUP -> VPN Settings -> IPsec -> IPsec Policies to add an IPSec policy. Follow below parameters on General section of IPsec Policies page.

Policy Name: **ipsec-if**
Policy Type: **Auto Policy**
IPSec Mode: **Tunnel Mode**
Select Local Gateway: **Dedicated WAN**
Remote Endpoint: **IP Address, 192.168.10.254**
Local IP: **Subnet**
Local Start IP Address: **192.168.3.0**
Local Subnet Mask: **255.255.255.0**
Remote IP: **Subnet**
Remote Start IP Address: **192.168.1.0**
Remote Subnet Mask: **255.255.255.0**

General section of IPSec Policy:



General

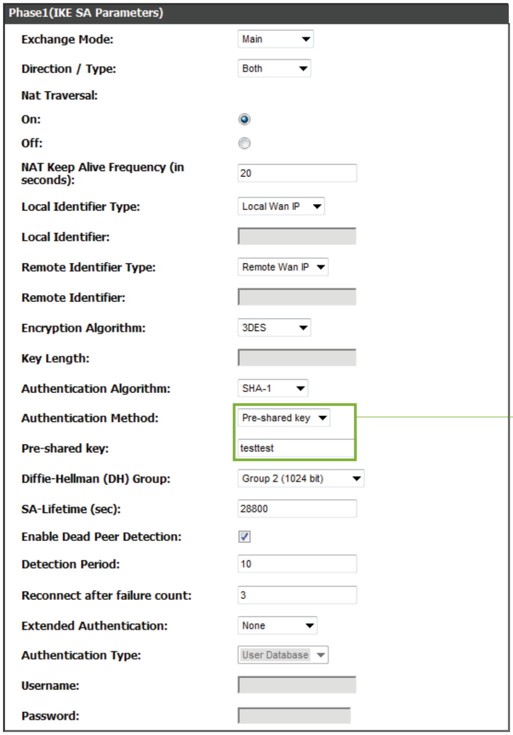
Policy Name:	ipsec-if
Policy Type:	Auto Policy
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	IP Address 192.168.10.254
Enable Mode Config:	□
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	192.168.3.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Remote IP:	Subnet
Remote Start IP Address:	192.168.1.0
Remote End IP Address:	
Remote Subnet Mask:	255.255.255.0

This part is local internal network of DSR-1000N

This part is remote internal network of DFL-860E

Follow below parameters on Phase1 (IKE SA Parameters) section.

Exchange Mode: **Main**
Direction / Type: **Both**
NAT Traversal: **ON**
NAT Keep Alive Frequency: **20**
Local Identifier Type: **Local WAN IP**
Remote Identifier Type: **Remote WAN IP**
Encryption Algorithm: **3DES**
Authentication Algorithm: **SHA-1**
Authentication Method: **Pre-shared Key**
Pre-shared Key: **testtest**
Diffie-Hellman (DH) Group: **Group 2 (1024 bit)**
SA Lifetime (sec): **28800**
Enable Dead Peer Detection: Enabled
Detection Period: 10
Reconnect after failure count: 3



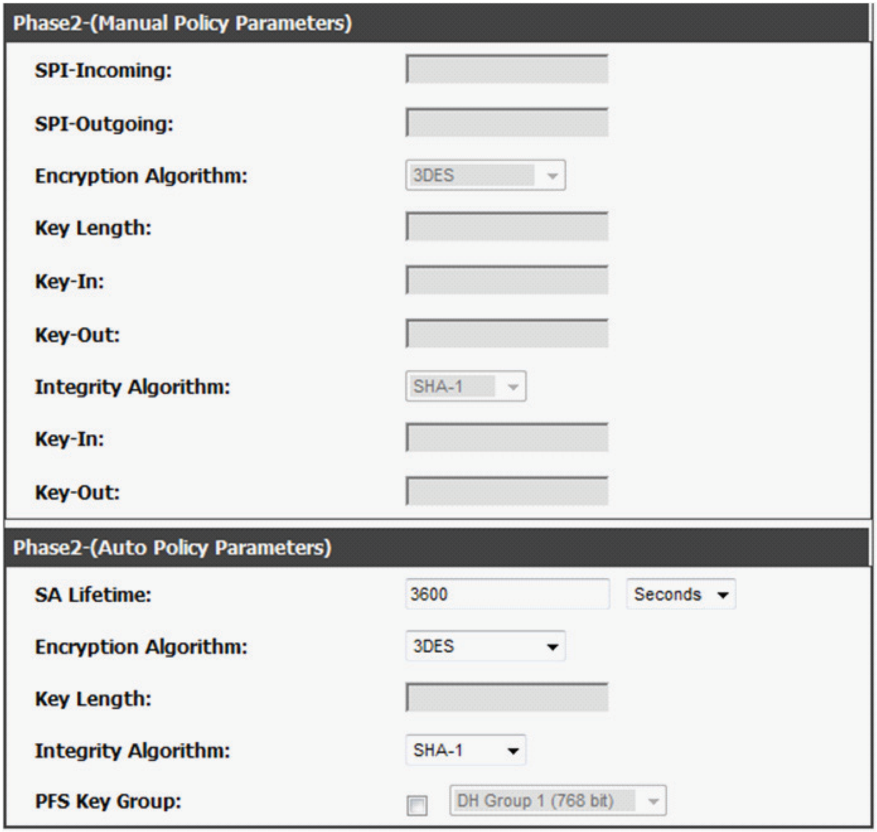
Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	3DES
Key Length:	
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	testtest
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	☑
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None
Authentication Type:	User Database
Username:	
Password:	

Authentication Method and Pre-Shared Key setting must be identical with remote Pre-Shared Key setting of DFL-860E

Follow below parameters on Phase2 (Manual Policy and Auto Policy Parameters) section.

SA Lifetime: **3600 Seconds**
Encryption Algorithm: **3DES**
Integrity Algorithm: **SHA-1**



Phase2-(Manual Policy Parameters)

SPI-Incoming:	
SPI-Outgoing:	
Encryption Algorithm:	3DES
Key Length:	
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1
Key-In:	
Key-Out:	

Phase2-(Auto Policy Parameters)

SA Lifetime:	3600 Seconds
Encryption Algorithm:	3DES
Key Length:	
Integrity Algorithm:	SHA-1
PFS Key Group:	□ DH Group 1 (768 bit)

Verification:

1. Check the IPSEC SAs database, both IKE and IPSEC SAs are established without problem.
2. To initial the ICMP traffic from DFL-860E, DFL-860E is able to reach the LAN1 IP of DSR-1000N

```
 vpnstats -ike -ipsec -verbose
 --- Active IKE SAs:
 1  Remote peer: 192.168.40.2:500
 Identities:
 local: 192.168.10.254
 remote: 192.168.40.2
 # Negotiations in progress: 1
 Bytes sent: 796
 Created: 2010-09-16 07:12:08
 Last used: 2010-09-16 07:12:18
 Expires: 2010-09-16 15:12:08
 Encryption alg: 3des-cbc
 Hash alg: sha1
 PRF alg: hmac-sha1
--- Active IPsec SAs:
2  IPsec Tunnel: ipsec-if
 Endpoints: 192.168.1.0/24 <--> 192.168.3.0/24
 Local IP: 192.168.1.1
 Remote gateway: 192.168.40.2
 Protocol: ESP: 3des-cbc hmac-sha1-96
 SPI (in): 0x539d72e0
 SPI (out): 0x2084729
 NAT information:
 Local end behind NAT : No
 Remote end behind NAT: No
 Authentication information:
 Auth method: Pre-shared key
 Local ID: 192.168.1.0/24
 Remote ID: 192.168.3.0/24
 DFL-860E:/> ping 192.168.3.1 -count=5
 Sending 5 4-byte ICMP pings to 192.168.3.1 from 192.168.1.1
 ICMP Reply from 192.168.3.1  seq=0  time=<10 ms  TTL=64
 ICMP Reply from 192.168.3.1  seq=1  time=<10 ms  TTL=64
 ICMP Reply from 192.168.3.1  seq=2  time=<10 ms  TTL=64
 ICMP Reply from 192.168.3.1  seq=3  time=<10 ms  TTL=64
 ICMP Reply from 192.168.3.1  seq=4  time=<10 ms  TTL=64
```

D-Link®

Visit our website for more information
www.dlink.com