

Configuration Guide



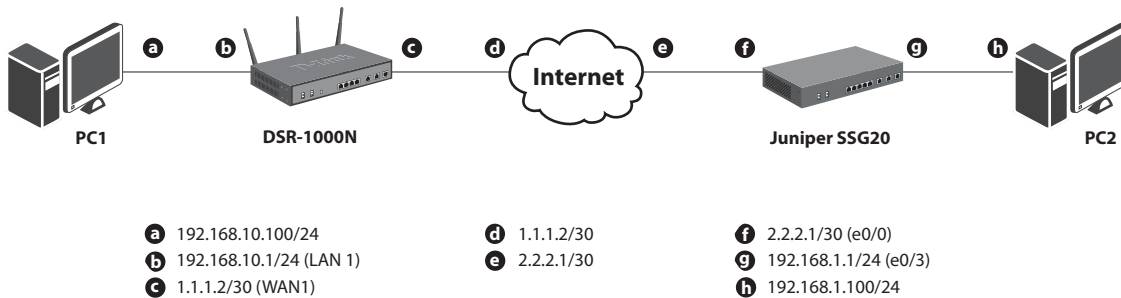
How to set up the IPSec site-to-site Tunnel between the D-Link DSR Router and the Juniper Firewall

Overview

This document describes how to implement IPSec with pre-shared secrets establishing site-to-site VPN tunnel between the D-Link DSR-1000N and the Cisco 5505. The screenshots in this document is from firmware version 1.03B12 of DSR-1000N and firmware version 6.2 Or 2.0 of Juniper SSG20. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

Situation note

Site-to-site VPN could be implemented in an enterprise allows to access and exchange data among more than two geographical sites or offices. Once the site-to-site VPN set up, the clients in the groups of the different located sites are as in the internal networks. As companies may have other gateway appliances which are not D-Link products, this document will be useful when you intend to create IPSec VPN tunnel between DSR and other existing gateway appliance.



IP addresses

DSR WAN: **1.1.1.2/30**

DSR LAN: **192.168.10.1/24**

Juniper_SSG20 Untrust_Zone(e0/0): **2.2.2.2/30**

Juniper_SSG20 Trust_Zone(e0/3): **192.168.1.1/24**

IPSec Parameters

IPSec Mode: **Tunnel Mode**

IPSec Protocol: **ESP**

Phase1 Exchange Mode: **Main**

Phase1 Encryption: **3DES**

Phase1 Authentication: **SHA1**

Phase1 Authentication Method: **Pre-Shared Key**

Diffie-Hellman Group: **G2**
Phase1 Lifetime: **28800 sec**
Phase2 Encryption: **3DES**
Phase2 Authentication: **SHA1**
Phase2 Lifetime: **3600 sec**

Configuration Step

DSR Settings

1. Set up the WAN IP address. Navigate to the [Internet Settings > WAN1 Settings > WAN1 Setup](#).

Fill in relative information based on the settings of topology. The IP Address of the field of ISP Connection Type is the IP address of external network connecting point which is shown as the point “c” on the topology. Click the button “**save settings**” to complete WAN IP address settings.

Wizard	
Internet Settings	WAN1 SETUP LOGOUT
Wireless Settings	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.
Network Settings	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>
DMZ Setup	
VPN Settings	
USB Settings	
VLAN Settings	
	ISP Connection Type
	ISP Connection Type: <input type="text" value="Static IP"/>
	IP Address: <input type="text" value="1.1.1.2"/>
	IP Subnet Mask: <input type="text" value="255.255.255.252"/>
	Gateway IP Address: <input type="text" value="1.1.1.1"/>
	Domain Name System (DNS) Servers
	Primary DNS Server: <input type="text" value="168.95.1.1"/>
	Secondary DNS Server: <input type="text" value="8.8.8.8"/>
	MAC Address
	MAC Address Source: <input type="text" value="Use Default Address"/>
	MAC Address: <input type="text" value="00:00:00:00:00:00"/>

2. Set up the IPsec policy. Navigate to the [VPN Settings > IPsec > IPsec Policies](#).

Press the button **"Add"** to increase a new policy. In General Section, fill in relative information. The IP address of [Remote Endpoint](#) refers to the external network connecting point of Juniper SSG20 which is shown as the point "f" on the topology. The internal network group, which indicates the IP information on [Local Start IP Address](#), under DSR-1000N allows access to the remote network group, which indicates the IP information on [Remote Start IP Address](#), under Juniper SSG20 through VPN tunnel.

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	IPSEC CONFIGURATION LOGOUT			
Internet Settings	This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.			
Wireless Settings	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
Network Settings	General			
DMZ Setup	Policy Name: <input type="text" value="IPSec1"/>			
VPN Settings	Policy Type: <input type="button" value="Auto Policy"/> ▼			
USB Settings	IPsec Mode: <input type="button" value="Tunnel Mode"/> ▼			
VLAN Settings	Select Local Gateway: <input type="button" value="Dedicated WAN"/> ▼			
	Remote Endpoint: <input type="button" value="IP Address"/> ▼			
	<input type="text" value="2.2.2.2"/>			
	Enable Mode Config: <input type="checkbox"/>			
	Enable NetBIOS: <input type="checkbox"/>			
	Enable RollOver: <input type="checkbox"/>			
	Protocol: <input type="button" value="ESP"/> ▼			
	Enable DHCP: <input type="checkbox"/>			
	Local IP: <input type="button" value="Subnet"/> ▼			
	Local Start IP Address: <input type="text" value="192.168.10.0"/>			
	Local End IP Address: <input type="text"/>			
	Local Subnet Mask: <input type="text" value="255.255.255.0"/>			
	Remote IP: <input type="button" value="Subnet"/> ▼			
	Remote Start IP Address: <input type="text" value="192.168.1.0"/>			
	Remote End IP Address: <input type="text"/>			
	Remote Subnet Mask: <input type="text" value="255.255.255.0"/>			

In Phase 1 Section, fill in relative information. Please notice that the Pre-shared Key must be as same as the pre-shared key which will be inserted on Juniper SSG20 on the later step.

Phase1(IKE SA Parameters)	
Exchange Mode:	Main ▼
Direction / Type:	Both ▼
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
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:	1234567890
Diffie-Hellman (DH) Group:	Group 2 (1024 bit) ▼
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	<input type="checkbox"/>
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None ▼
Authentication Type:	User Database ▼
Username:	
Password:	

In Phase 2 Section, fill in relative information.

Phase2-(Manual Policy Parameters)

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key Length:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Phase2-(Auto Policy Parameters)

SA Lifetime:

Encryption Algorithm:

Key Length:

Integrity Algorithm:

PFS Key Group:

Click the button **“save settings”** to complete IPsec Policy settings.

3. Check the VPN status. Navigate to the [Status > Active VPNs](#).

The activity will be shown on the list while the tunnel is established with the other side.

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS		
Device Info	<div style="color: red; font-weight: bold;">Operation succeeded</div> <div style="color: red; font-size: small;">The page will auto-refresh in 10 seconds</div>					
Logs						
Traffic Monitor	ACTIVE VPN LOGOUT					
Active Sessions	This page displays the active VPN connections, IPSEC as well as SSL..					
Active RunTime Sessions	Active IPsec SAs					
Wireless Clients	Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action
LAN Clients	IPsec	2.2.2.2	0.00	0	IPsec SA Not Established	<input type="button" value="Connect"/>
Active VPNs	Active SSL VPN Connections					
	User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status	
	Poll Interval: <input type="text" value="10"/> (Seconds)		<input type="button" value="Start"/>	<input type="button" value="Stop"/>		

Juniper_SSG20 Settings

1. Set up the Untrust_Zone and Trust_Zone IP addresses. Navigate to the **Network > Interfaces > List**. Click **"Edit"**.

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Up	-	Edit
ethernet0/2				Down	-	Edit
ethernet0/3				Up	-	Edit
ethernet0/4				Down	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	2.2.2.2/30	Untrust	Layer3	Up	-	Edit
ethernet0/1	172.16.1.1/24	DMZ	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	unnumbered	Trust	Tunnel	Ready	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Configure **Untrust_Zone** with relative information as below. The **IP Address/ Netmask** of Basic tab is the IP address of external network connecting point which is shown as the point "f" on the topology. Click the button **"OK"** to complete this setting.

Network > Interfaces > Edit

Interface: ethernet0/0 (IP/Netmask: 2.2.2.2/30)

Properties: Basic | Phy | MIP | BIP | VIP | ICMP | Monitor | 802.1X | IRDP

Interface Name: ethernet0/0 0014.6e6.70c0

Zone Name: Untrust

Obtain IP using DHCP Automatic update DHCP server parameters
 Obtain IP using PPPoE [Create new pppoe setting](#)
 Static IP

IP Address / Netmask: 2.2.2.2 / 30 Manageable
 Manage IP #: 2.2.2.2 0014.6e6.70c0

Interface Mode: NAT Route

Block Intra-Subnet Traffic:

Service Options

Management Services: Web UI Telnet SSH

Other Services: SNMP SSL Ident-resat

Ping Path MTU(IPv4)

Maximum Transfer Unit(MTU) Admin MTU: 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy:

NTP Server:

WebAuth: IP Address: 0.0.0.0 SSL Only

G-ARP:

Traffic Bandwidth: Egress: Maximum Bandwidth: 0 kbps
 Ingress: Maximum Bandwidth: 0 kbps

VRPP:

OK Apply Cancel

Configure **Trust_Zone** with relative information as below. The **IP Address/ Netmask** of Basic tab is the IP address of internal network connecting point which is shown as the point “g” on the topology. Click the button “OK” to complete this setting.

Network > Interfaces > Edit ssg20 ?

Interface: bgroup0 (IP/Netmask: 192.168.1.1/24) Back To Interface List

Properties: Basic Bind Port MIP DDP VIP Secondary IP IGMP Monitor IRDP

Interface Name: bgroup0 0014.f6e6.70c9

Zone Name: Trust

Obtain IP using DHCP Automatic update DHCP server parameters
 Obtain IP using PPPoE

Static IP

 IP Address / Netmask: 192.168.1.1 / 24 Manageable

 Manage IP: 192.168.1.1 0014.f6e6.70c9

Interface Mode: NAT Route

Block Intra-Subnet Traffic:

Service Options

Management Services: Web UI Telnet SSH
 SNMP SSL

Other Services: Ping Path MTU (IPv4) Ident-reset

Maximum Transfer Unit (MTU) Admin MTU: 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy:

NTP Server:

WebAuth: IP Address: 0.0.0.0 SSL Only
 G-ARP

Traffic Bandwidth: Egress Maximum Bandwidth: 0 Kbps
 Ingress Maximum Bandwidth: 0 Kbps

2. Add a Tunnel Interface. Navigate to the **Network > Interfaces > List**.

Select “**Tunnel IF**” from scroll down menu. Press the button “**New**” to increase a new tunnel interface.

Network > Interfaces (List) ssg20 ?

List: 20 per page

List: ALL(9) Interfaces Tunnel IF

Name	IP / Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Up	-	Edit
ethernet0/2				Down	-	Edit
ethernet0/3				Down	-	Edit
ethernet0/4				Up	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	2.2.2.2/30	Untrust	Layer3	Down	-	Edit
ethernet0/1	172.16.1.1/24	DMZ	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	unnumbered	Trust	Tunnel	Down	-	Edit
vlan.1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Configure relative settings as below.

Network > Interfaces > Edit sbg20 ?

Interface: tunnel.1 (IPNetmask: 0.0.0.0/0)

Properties: [Basic](#) [MP](#) [DP](#) [VP](#) [KOMP](#) [NHTE](#) [Tunnel](#)

Tunnel Interface Name: tunnel.1

Zone (VR): Trust (trust-vr)

Fixed IP

IP Address / Netmask: /

Unnumbered

Interface: ethernet0/0 (trust-vr)

Maximum Transfer Unit(MTU) Admin MTU: Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy:

Traffic Bandwidth

Egress	Maximum Bandwidth	<input type="text" value="0"/> Kbps
Ingress	Guaranteed Bandwidth	<input type="text" value="0"/> Kbps
	Maximum Bandwidth	<input type="text" value="0"/> Kbps

NHRP Enable:

3. Add an IPsec Remote Gateway. Navigate to the **VPNs > AutoKey Advanced > Gateway**. Press the button **"New"** and fill in relative information as below.

VPNs > AutoKey Advanced > Gateway > Edit sbg20 ?

Gateway Name: DSR

Version: IKEv1 IKEv2

Remote Gateway

Static IP Address IP Address/Hostname: 1.1.1.2

Dynamic IP Address Peer ID:

Dialup User User:

Dialup User Group Group:

ACVPN-Dynamic Local ID:

ACVPN-Profile

Press the button **“Advanced”** for preshared key setting. Fill in relative information as below. Insert the Pre-shared Key which is as same as the one put in DSR-1000N in the previous step.

VPN > AutoKey Advanced > Gateway > Edit

SSG20

Juniper NETWORKS

Home

Configuration

Network

Security

Policy

VPNs

AutoKey IKE

AutoKey Advanced

Gateway

P1 Proposal

P2 Proposal

XAuth Setting

VPN Groups

Manual Key

L2TP

Monitor Status

Objects

Reports

Wizards

Help

Logout

IKEv2 Auth Method

Self None

Peer None

Preshared Key [REDACTED] Use As Seed

Local ID [] (optional)

Outgoing Interface ethernet0/0

Security Level

Predefined Standard Compatible Basic

User Defined Custom

Phase 1 Proposal

pre-g2-3des-sha pre-g2-aes128-sha

None None

Mode (Initiator) Main (ID Protection) Aggressive

Enable NAT-Traversal

UDP Checksum

Keepalive Frequency 0 Seconds (0-300)

Peer Status Detection

Heartbeat Hello 0 Seconds (1-3600, 0: disable)

4. Create a new VPN tunnel. Navigate to **VPNs > AutoKey IKE**. Press the button **“New”**.

VPN > AutoKey Advanced > Gateway

SSG20

List 20 per page

New

Name	Peer Type	Address / ID / User Group	Local ID	Security Level	Configure
DSR	Static	1.1.1.2	-	Custom	Edit Xauth -

Juniper NETWORKS

SSG20

Date/Time

Update

Admin

Auth

Intranet Auth

Report Settings

Network

Binding

DNS

Zones

Interfaces

List

Backup

DHCP

302 IX

Routing

BPP

Security

Policy

VPNs

AutoKey IKE

AutoKey Advanced

Gateway

P1 Proposal

P2 Proposal

XAuth Settings

VPN Groups

Manual Key

L2TP

Fill in relative information as below.

The screenshot shows the Juniper SSG20 configuration interface for a VPN named 'ipsec_1'. The 'Remote Gateway' section is expanded, showing the following settings:

- VPN Name:** ipsec_1
- Remote Gateway:** Predefined, DSR
- Gateway Name:** (empty)
- Version:** IKEv1
- Type:** Static IP, Address/Hostname (empty)
- Dynamic IP:** Peer ID (empty)
- Dialup User:** User (None)
- Dialup Group:** Group (None)
- Local ID:** (empty) (optional)
- Preshared Key:** (empty) Use As Seed (unchecked)
- Security Level:** Standard
- Outgoing Interface:** ethernet0/0
- Gateway:** None
- Tunnel Towards Hub:** ipsec_1
- Binding to Tunnel:** None

Buttons at the bottom include 'OK', 'Cancel', and 'Advanced'.

Press the button "**Advanced**" and configure settings as below. The internal network group, which indicates the IP information on **Local IP/ Netmask**, under Juniper SSG20 allows access to the remote network group, which indicates the IP information on Remote **IP/ Netmask**, under DSR-1000N through VPN tunnel.

The screenshot shows the 'Security Level' configuration page for the VPN tunnel. The following settings are visible:

- Predefined:** Standard, **Compatible**, Basic
- User Defined:** Custom
- Phase 2 Proposal:**
 - Encryption: nopfs-esp-3des-sha
 - Authentication: nopfs-esp-3des-md5
 - Encryption: nopfs-esp-des-sha
 - Authentication: nopfs-esp-des-md5
- Replay Protection:** (unchecked)
- Transport Mode:** (unchecked)
- Bind to:**
 - None
 - Tunnel Interface:** tunnel.1
 - Tunnel Zone: Untrust-Tun
- Proxy-ID:** (checked)
 - Local IP / Netmask:** 192.168.1.0 / 24
 - Remote IP / Netmask:** 192.168.10.0 / 24
 - Service:** ANY
- DSCP Marking:**
 - Disable**
 - Enable (Dscp Value: 0)
- VPN Group:** None (Weight: 0)

5. Create the Routings. Navigate to **Network > Routing > Routing Entries**.

Select **"trust-vr"** from the drop down menu on the top and left corner. Press the button **"New"**.

Network > Routing > Routing Entries ssg20

List 20 per page

List route entries for All virtual routers trust-vr New

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	2.2.2.0/30		ethernet0/0	C			Root		-
*	2.2.2.2/32		ethernet0/0	H			Root		-
*	0.0.0.0/0	2.2.2.1	ethernet0/0	C		1	Root		-
	172.16.1.0/24		ethernet0/1	C			Root		-
	172.16.1.1/32		ethernet0/1	H			Root		-
*	192.168.1.0/24		bgrousp0	C			Root		-
*	192.168.1.1/32		bgrousp0	H			Root		-
*	192.168.10.0/24		tunnel.1	S	20	1	Root		Remove

* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2
 D Dynamic N NHRP

Fill in relative information as below.

Network > Routing > Routing Entries > Configuration ssg20

Virtual Router Name trust-vr

IP Address/Netmask 192.168.10.0 / 24

Next Hop Virtual Router Gateway

Virtual Router untrust-vr

Interface tunnel.1

Gateway IP Address 0.0.0.0

Permanent

Tag 0

Metric 1

Preference 20

Description

OK Cancel

6. Set up the Policies. Navigate to **Policy > Policies**. Create the first rule. Select **“Trust”** and **“Untrust”** in the **“From”** and **“To”** drop down menus respectively. Press the button **“New”**.

Policy > Policies (From All zones To All zones) ssg20

List 20 per page

From Trust To Untrust Go New

From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Any	Any	ANY	Permit		Edit Clone Remove	<input checked="" type="checkbox"/>	Move

Fill in relative information as below.

Name (optional) To_DSR

Source Address New Address 192.168.1.0 / 24 Address Book Entry Any Multiple

Destination Address New Address 192.168.10.0 / 24 Address Book Entry Any Multiple

Service ANY Multiple

Application None

WEB Filtering

Action Permit Deep Inspection

Antivirus Profile None

Antispam enable

Tunnel VPN None

Modify matching bidirectional VPN policy

L2TP None

Create the second rule. Select **"Untrust"** and **"Trust"** in the **"From"** and **"To"** drop down menus respectively. Press the button **"New"**.

List **20** per page

From **Untrust** To **Trust** Go **New**

From Trust To Untrust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Any	Any	ANY	✓		Edit Clone Remove	<input checked="" type="checkbox"/>	↕ ⋮
2	192.168.1.0/24	192.168.10.0/24	ANY	✓		Edit Clone Remove	<input checked="" type="checkbox"/>	↕ ⋮

Fill in relative information as below.

Name (optional) from_DSR

Source Address
 New Address 192.168.10.0 / 24
 Address Book Entry 192.168.10.0/24 Multiple

Destination Address
 New Address 192.168.1.0 / 24
 Address Book Entry 192.168.1.0/24 Multiple

Service ANY Multiple

Application None

WEB Filtering

Action Permit Deep Inspection

Antivirus Profile None

Antispam enable

Tunnel VPN None

Modify matching bidirectional VPN policy

L2TP None

7. Check VPN status. Navigate to **VPNs > Monitor Status**.

The screenshot displays the Juniper Networks SSG20 VPN Monitor Status page. The page title is "VPNs > Monitor Status" and the user is logged in as "sbg20". The left sidebar shows the navigation menu with "VPNs" and "Monitor Status" highlighted. The main content area shows a table with one entry for "ipsec_1".

VPN Name	SA ID	Policy ID	Peer Gateway IP	Type	SA Status	Link
ipsec_1	00000001	-1/-1	1.1.1.2	AutoIKE	Active	Off

D-Link[®]

Visit our website for more information
www.dlink.com

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries.
All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2011 D-Link Corporation. All Rights Reserved.