

Configuration Guide



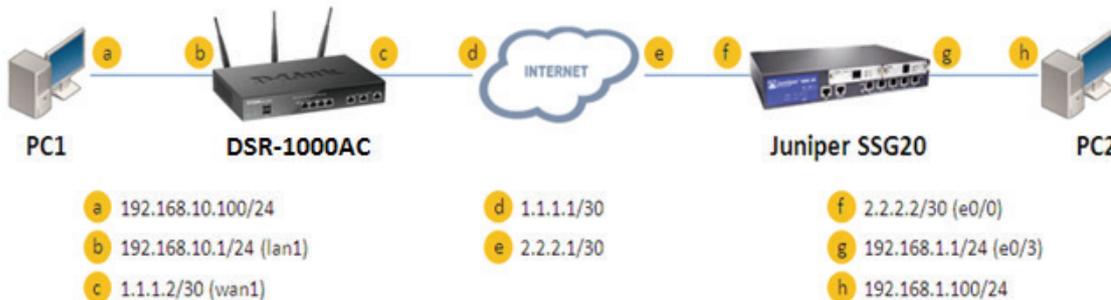
How to set up the IPsec site-to-site Tunnel between the D-Link DSR Router and the Juniper Firewall

Overview

This document describes how to implement IPsec with pre-shared secrets establishing a site-to-site VPN tunnel between the D-Link DSR-1000AC and the Juniper SSG20. The screenshots in this document are from firmware version 3.10 of the DSR-1000AC and firmware version 6.3.0r24 (Released in June 2017) of the Juniper SSG20. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see in your browser.

Situation note

Site-to-site VPNs can be implemented in an enterprise to allow access and the exchange of data between two or more geographically separated sites or offices. Once the site-to-site VPN has been set up, the clients in the groups of the different sites can communicate as if they are on the same internal network. Because companies may have other gateways that are not D-Link products, this document can be used to create IPsec VPN tunnels between the DSR router and other existing gateway appliances.



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: [Internet Settings > WAN1 Settings > WAN1 Setup](#).

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

Operation Succeeded

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.

IPv4 WAN1 Settings

WAN1 Setup

Connection Type

Enable VLAN Tag OFF

Static IP

IP Address

IP Subnet Mask

Gateway IP Address

Domain Name System (DNS) Servers

Primary DNS Server

Secondary DNS Server

MAC Address

MAC Address Source Use Default MAC Clone your PC's MAC Use this MAC

Port Setup

MTU Size Default Custom

Port Speed

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

Press the **"Add New IPsec Policy"** button to create a new policy. In the General section, fill in the relevant information. The IP address of the **Remote Endpoint** refers to the external connection of the Juniper SSG20, which is shown as the point "f" in the topology. The internal IP address range, which is indicated by the **Local Start IP Address**, is the IP range allowed access to the remote network group over the VPN, which indicated by the IP information on **Remote Start IP Address**, is the IP range reachable through the VPN tunnel with the Juniper SSG20.

Logged in as: admin (ADMIN) | Language: English [US] | Logout
Serial: 539X1G1000007 | Firmware: 3.10_VWV
Wizard | System Search...

VPN > IPsec VPN > Policies

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with "" represents a Client Policy.

IPSec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
No data available in table								

Showing 0 to 0 of 0 entries

First Previous Next Last

Add New IPsec Policy

IPsec Policy Configuration

General

Policy Name: IPSec1

Policy Type: Auto Policy

IP Protocol Version: IPv4

IKE Version: IKEv1

L2TP Mode: None

IPSec Mode: Tunnel Mode

Select Local Gateway: Dedicated WAN

Remote Endpoint: IP Address

IP Address / FQDN: 2.2.2.2

Enable Mode Config: OFF

Save

IPSec Policy Configuration

Enable Mode Config OFF

Enable NetBIOS OFF

Enable RollOver OFF

Protocol ESP

Enable DHCP OFF

Local IP Subnet

Local Start IP Address

Local Subnet Mask

Remote IP Subnet

Remote Start IP Address 192.168.1.0

Remote Subnet Mask 255.255.255.0

Enable Keepalive OFF

Save

In the Phase 1 section, fill in the relevant information. Please notice that the **Pre-shared Key** must be the same as the pre-shared key that will be entered into the Juniper SSG20 later.

IPSec Policy Configuration

Phase1(IKE SA Parameters)

Exchange Mode Main

Direction / Type Both

Nat Traversal ON

NAT Keep Alive Frequency 20 Seconds

Local Identifier Type Local Wan IP

Remote Identifier Type Remote Wan IP

Encryption Algorithm

DES OFF 3DES ON

AES-128 OFF AES-192 OFF

AES-256 OFF

BLOWFISH OFF

Save

IPSec Policy Configuration

Authentication Algorithm

MD5 OFF SHA-1 ON

SHA2-256 OFF SHA2-384 OFF

SHA2-512 OFF

Authentication Method Pre-Shared Key

Pre-Shared Key 12345678 [Length: 8 - 49]

Diffie-Hellman (DH) Group Group 2 (1024 bit)

SA-Lifetime 28800 [Range: 300 - 2147483647] Seconds

Enable Dead Peer Detection OFF

Extended Authentication None

Phase2-(Auto Policy Parameters)

SA Lifetime 3600 Seconds

Save

In the Phase 2 section, fill in relevant information.

IPSec Policy Configuration ✕

Phase 2-(Auto Policy Parameters)

SA Lifetime

Encryption Algorithm

DES <input type="checkbox"/> OFF	None <input type="checkbox"/> OFF
3DES <input checked="" type="checkbox"/> ON	AES-128 <input type="checkbox"/> OFF
AES-192 <input type="checkbox"/> OFF	AES-256 <input type="checkbox"/> OFF
TWOFISH (128) <input type="checkbox"/> OFF	TWOFISH (192) <input type="checkbox"/> OFF
TWOFISH (256) <input type="checkbox"/> OFF	
BLOWFISH <input type="checkbox"/> OFF	
CAST128 <input type="checkbox"/> OFF	

Integrity Algorithm

MD5 <input type="checkbox"/> OFF	SHA-1 <input checked="" type="checkbox"/> ON
----------------------------------	----------------------------------------------

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

VPN >> IPsec VPN >> Policies ? ↻

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with [™] represents a Client Policy.

IPsec Policies List

Show entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPsec Mode	Local	Remote	Auth	Encr
Enabled	IPSec1	None	Auto Policy	Tunnel Mode	192.168.10.0/255.255.255.0	192.168.1.0/255.255.255.0	SHA1	3DES

Showing 1 to 1 of 1 entries

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

The activity will be shown in the list as the tunnel is established with the other side.

Status » Network Information » Active VPNs » IPsec SAs

[IPsec SAs](#) [SSL VPN Connections](#) [PPTP VPN Connections](#) [Open VPN Connections](#) [L2TP VPN Connections](#) [GRE Tunnel Status](#)

This page lists current established IPsec Security Associations.

Active IPsec SAs List

Show entries [Right click on record to get more options]

Policy Name	Endpoint	tx (KB)	tx (Packets)	State
IPsec1	2.2.2.2	19.36	167	IPsec SA Established

Showing 1 to 1 of 1 entries

[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

Juniper_SSG20 Settings

1. Set up the Untrust_Zone (WAN port) and Trust_Zone (LAN port) IP addresses.

Navigate to: [Network > Interfaces > List](#).

Click **"Edit"**.

Network > Interfaces (List) ssg20

20 per page

List ALL(0) Interfaces

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Up	-	Edit
ethernet0/2				Up	-	Edit
ethernet0/3				Down	-	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	0.0.0.0/0	DMZ	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	unnumbered	Trust	Tunnel	Up	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Configure the Untrust_Zone interface with the relevant information as below. The **IP Address/ Netmask** of the Basic tab is the IP address of external network connection, which is shown as point “f” in the topology. Click the “**OK**” button to finish this configuration.

Network > Interfaces > Edit ssg20 ?

Interface: ethernet0/0 (IP/Netmask: 2.2.2.2/30) [Back To Interface List](#)

Properties: [Basic](#) [Proxy ARP](#) [Phy](#) [MIP](#) [DIP](#) [VIP](#) [IGMP](#) [Monitor](#) [802.1X](#) [IRDP](#)

Interface Name: ethernet0/0 0014.f6e6.70c0

Zone Name: Untrust

Obtain IP using DHCP Automatic update DHCP server parameters
 Obtain IP using PPPoE: None [Create new pppoe setting](#)
 Static IP

IP Address / Netmask: 2.2.2.2 / 30 Manageable
 Manage IP: 2.2.2.2 0014.f6e6.70c0

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

VRRP:

Admin Status Up:

OK

Configure Trust_Zone interface with the relevant information as below. The **IP Address/ Netmask** of the Basic tab is the IP address of the internal network connection, which is shown as point “g” in the topology. Click the “OK” button to finish this configuration.

Network > Interfaces > Edit ssg20 ?

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

Properties: [Basic](#) [Proxy ARP](#) [Bind Port](#) [MIP](#) [DIP](#) [VIP](#) [Secondary IP](#) [IGMP](#) [Monitor](#) [IRDP](#)

Interface Name: bgroup0.0014.f6e6.70c9

Zone Name: Trust_Zone

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

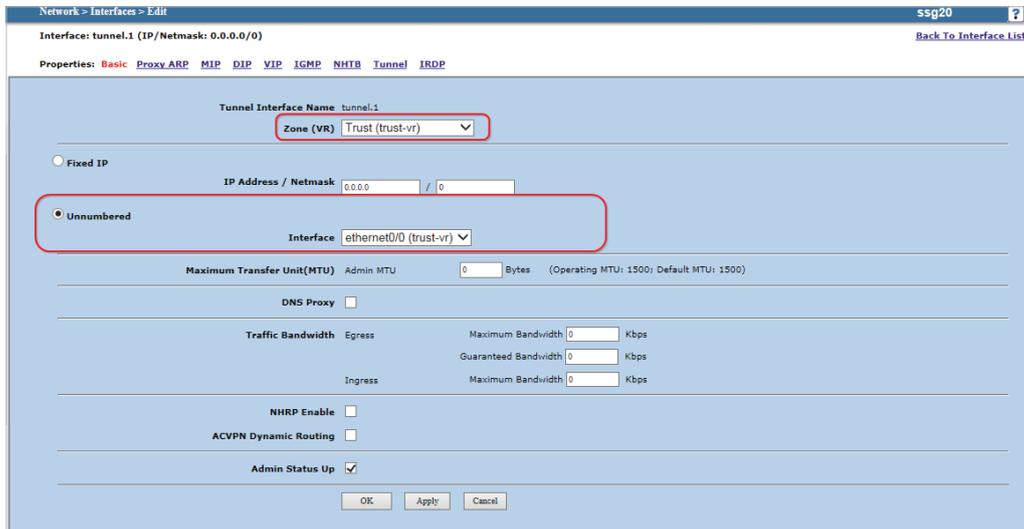
Admin Status Up:

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

Select **"TunnelIF"** from the scroll down menu. Press the **"New"** button to create a new tunnel interface.



Configure the relevant settings as below.



3. Add an IPsec Remote Gateway. Navigate to: VPNs > AutoKey Advanced > Gateway.

Press the "New" button and fill in relevant information as below.

VPNs > AutoKey Advanced > Gateway > Edit

SSG20

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: None

Dialup User Group Group: None

ACVPN-Dynamic

Local ID: [DistinguishedName]

ACVPN-Profile

OK Cancel **Advanced**

Press the "Advanced" button to configure the preshared key setting. Fill in the relevant information as below. Insert the **Pre-shared Key**, which is the same as the one previously entered in the DSR-1000AC.

IKEv2 Auth Method

Self: None

Peer: None

Preshared Key: ***** 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:

Keaplive Frequency: 0 Seconds (0~300)

Peer Status Detection

Heartbeat

Hello: 0 Seconds (1~3600, 0: disable)

Reconnect: 0 Seconds (60~9999, 0: default)

Threshold: 5 (2~9999)

DPD

Interval: 0 Seconds (3~28800, 0: disable)

Retry: 5 (1~127)

Always Send:

Reconnect Interval: 0 (60~9999) Seconds, 0 Disable

Preferred Certificate(optional)

Local Cert: None

Peer CA: None

Peer Type: X509-SIG

Use Distinguished Name for Peer ID:

CN: _____

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

The screenshot shows the Juniper SSG20 configuration interface. The left sidebar contains a navigation tree with the following items: Update, Admin, Auth, Infranet Auth, Report Settings, Network, Binding, DNS, Zones, Interfaces, List, Backup, DHCP, 802.1X, Routing, PPP, DSCP, Security, Policy, and VPNs. Under the VPNs folder, 'AutoKey IKE' is selected and highlighted with a red box. The main content area shows a table of VPN tunnels. The table has columns for Name, Gateway, Security, Monitor, and Configure. A single row is visible with the name 'ipsec_1', gateway 'DSR', security 'Custom', and monitor 'On'. The 'Configure' column contains links for 'Edit', 'Proxy ID', and 'Remove'. A 'New' button is located in the top right corner of the main area, also highlighted with a red box.

Name	Gateway	Security	Monitor	Configure
ipsec_1	DSR	Custom	On	Edit Proxy ID Remove

Fill in relevant information as below.

VPN Name: ipsec_1

Remote Gateway: Predefined DSR Create a Simple Gateway

Gateway Name: _____

Version: IKEv1 IKEv2

Type: Static IP Dynamic IP Dialup User Dialup Group

Address/Hostname: _____

Peer ID: _____

User: None

Group: None

Local ID: _____ (optional)

Preshared Key: _____ Use As Seed:

Security Level: Standard Compatible Basic

Outgoing Interface: ethernet0/0

Gateway: None Tunnel Towards Hub: None

Binding to Tunnel: None

OK Cancel **Advanced**

ACVPN-Dynamic
ACVPN-Profile

Press the **"Advanced"** button and configure the settings as below and click **"Return"**.

Security Level

Predefined: Standard Compatible Basic

User Defined: Custom

Phase 2 Proposal: nopfs-esp-3des-sha

Replay Protection:

Transport Mode:

Bind to: None Tunnel Interface Tunnel Zone

Proxy-ID Check:

DSCP Marking: Disable Enable Dscp Value: 0

VPN Group: None Weight: 0

VPN Monitor:

Source Interface: default

Destination IP: default

Optimized:

Rekey:

Return Cancel

Click **Proxy ID**.

VPNs > AutoKey IKE ssg20 ?

List per page New

Name	Gateway	Security	Monitor	Configure
ipsec_1	DSR	Custom	On	Edit Proxy ID Remove

The internal IP address range, indicated by the **Local IP/ Netmask** field, is the range of addresses allowed access to the remote network over the VPN, and the remote network range, indicated by **Remote IP/ Netmask** field, is the IP address range reachable through the VPN with the DSR-1000AC.

VPN Name ipsec_1

Local

Local IP IP:

Local Address Zone: Address:

Remote

Remote IP IP:

Remote Address Zone: Address:

Service

5. Create the Routings. Navigate to: **Network > Routing > Destination**.

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

Network - Routing - Routing Entries ssg20

List 20 per page

List route entries for All virtual routers

trust-vr New

trust-vr	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	192.168.1.0/24		bgroup0	C			Root		-
*	192.168.1.1/32		bgroup0	H			Root		-
*	2.2.2.0/30		etherme0/0	C			Root		-
*	2.2.2.2/32		etherme0/0	H			Root		-
*	1.1.1.0/30	2.2.2.1	etherme0/0	S	20	1	Root		Remove
	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 the relevant information as below.

Virtual Router Name trust-vr

IP Address/Netmask 192.168.1.0 / 24

Next Hop Virtual Router untrust-vr

Gateway

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 **New** button.

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

List 20 per page

From: Trust To: Untrust

Search: New

From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Any	Any	ANY	Permit		Edit Clone	Enable	Move

Fill in the relevant information as below.

Name (optional): To_DSR

Source Address:

- New Address: 192.168.1.0 / 24
- Address Book Entry: Any

Destination Address:

- New Address: 192.168.10.0 / 24
- Address Book Entry: Any

Service: ANY

Application: None

WEB Filtering

Action: Permit

Antivirus Profile: None

Antispam enable:

Tunnel VPN: None

Modify matching bidirectional VPN policy

L2TP: None

Logging: at Session Beginning

Position at Top:

Session-limit

Counter: 0

Alarm without drop:

OK Cancel Advanced

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

From: **Untrust** To: **Trust**

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 the relevant information as below.

Name (optional)

Source Address
 New Address /
 Address Book Entry

Destination Address
 New Address /
 Address Book Entry

Service

Application

WEB Filtering

Action

Antivirus Profile

Antispam enable

Tunnel
 Modify matching bidirectional VPN policy

L2TP

Logging at Session Beginning

Position at Top

Session-limit
Counter

Alarm without drop

7. Check VPN status. Navigate to: [VPNs > Monitor Status](#).

VPN Monitor Status

List 20 per page

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

Status logs are also viewable on the homepage.

Total alarms: 7 (Emergencies: 0; Alerts: 0; Critical: 7) [More...](#)

Date/Time	Level	Description
2013-01-06 19:04:44	critical	VPN 'ipsec_1' from 1.1.1.2 is up.
2013-01-06 19:04:34	critical	VPN 'ipsec_1' from 1.1.1.2 is down.
2013-01-06 19:02:04	critical	VPN 'ipsec_1' from 1.1.1.2 is up.
2013-01-06 18:58:24	critical	VPN 'ipsec_1' from 1.1.1.2 is down.
2013-01-06 18:56:34	critical	VPN 'ipsec_1' from 1.1.1.2 is up.

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 © 2017 D-Link Corporation. All Rights Reserved.