

Configuration Guide



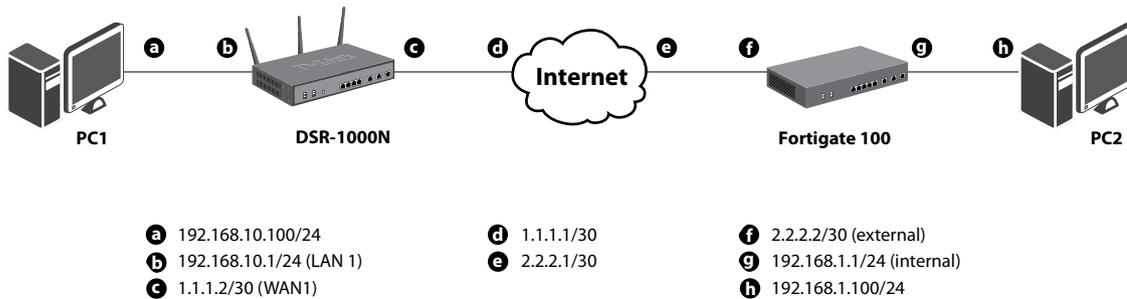
How to set up the IPSec site-to-site Tunnel between the D-Link DSR Router and the Fortinet Firewall

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 Fortigate100. The screenshots in this document is from firmware version 1.03B12 of DSR-1000N and firmware version 3.00-b0750 of Fortigate100. 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**

FortiGate100 WAN: **2.2.2.2/30**

FortiGate100 LAN: **192.168.1.99/24**

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

Wireless Settings

Network Settings

DMZ Setup

VPN Settings

USB Settings

VLAN Settings

WAN1 SETUP LOGOUT

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:

IP Address:

IP Subnet Mask:

Gateway IP Address:

Domain Name System (DNS) Servers

Primary DNS Server:

Secondary DNS Server:

MAC Address

MAC Address Source:

MAC Address:

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 Fortigate 100 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 Fortigate 100 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:	Auto Policy ▼		
USB Settings	IPsec Mode:	Tunnel Mode ▼		
VLAN Settings	Select Local Gateway:	Dedicated WAN ▼		
	Remote Endpoint:	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:	ESP ▼		
	Enable DHCP:	<input type="checkbox"/>		
	Local IP:	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:	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 Fortigate 100 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.

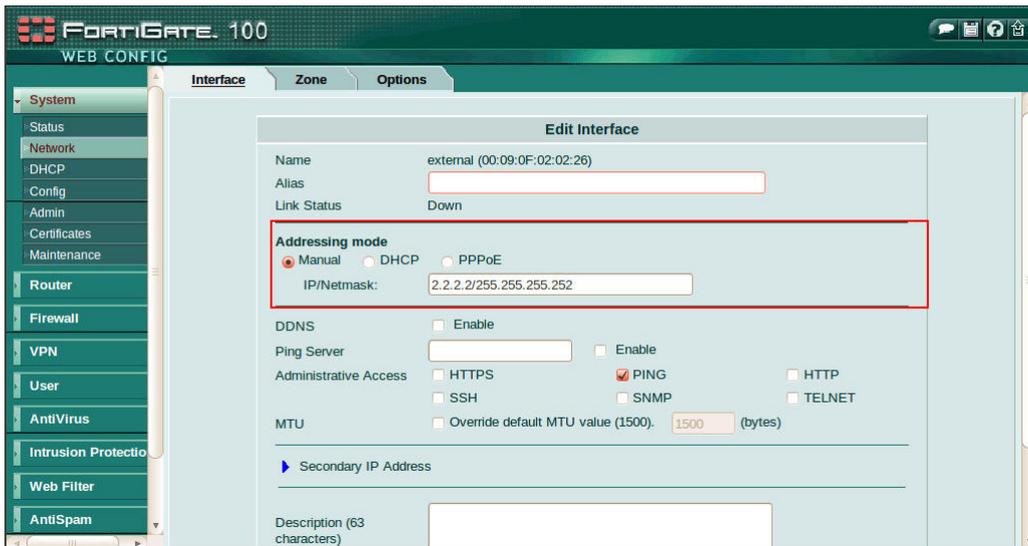
DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS												
Device Info	<p style="color: red;">Operation succeeded</p> <p style="color: red;">The page will auto-refresh in 10 seconds</p>															
Logs																
Traffic Monitor																
Active Sessions																
Active RunTime Sessions																
Wireless Clients	ACTIVE VPN LOGOUT															
LAN Clients	This page displays the active VPN connections, IPSEC as well as SSL.															
Active VPNs	<div style="background-color: #333; color: white; padding: 2px;">Active IPsec SAs</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Policy Name</th> <th>Endpoint</th> <th>tx (KB)</th> <th>tx (Packets)</th> <th>State</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>IPSec</td> <td>2.2.2.2</td> <td>0.00</td> <td>0</td> <td>IPsec SA Not Established</td> <td style="text-align: center;"><input type="button" value="Connect"/></td> </tr> </tbody> </table>				Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action	IPSec	2.2.2.2	0.00	0	IPsec SA Not Established	<input type="button" value="Connect"/>
Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action											
IPSec	2.2.2.2	0.00	0	IPsec SA Not Established	<input type="button" value="Connect"/>											
<div style="background-color: #333; color: white; padding: 2px;">Active SSL VPN Connections</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>User Name</th> <th>IP Address</th> <th>Local PPP Interface</th> <th>Peer PPP Interface IP</th> <th>Connect Status</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="text-align: center;"> Poll Interval: <input type="text" value="10"/> (Seconds) <input type="button" value="Start"/> <input type="button" value="Stop"/> </td> </tr> </tbody> </table>				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"/>							
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"/>																

FortiGate Settings

1. Set up the WAN IP address, Navigate to the **System > Network**. Click button **"edit"**.



Edit IP Address with following information. The **IP/Netmask** of Interface tab is the IP address and Netmask of external network connecting point which is shown as the point **"f"** on the topology.



2. Set up the default gateway. Navigate to **Router > Static**. Press the button "**Create New**". Fill in relative information as below.

The screenshot shows the FortiGate 100 WEB CONFIG interface. The left sidebar has 'Router' and 'Static' highlighted. The main area shows the 'Edit Static Route' dialog box with the following fields:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	external
Gateway	2.2.2.1
Distance	10 (1-255)

Buttons: OK, Cancel

3. Set up the IPSec Tunnel, go to the **VPN > IPSec > Auto Key (IKE)**.

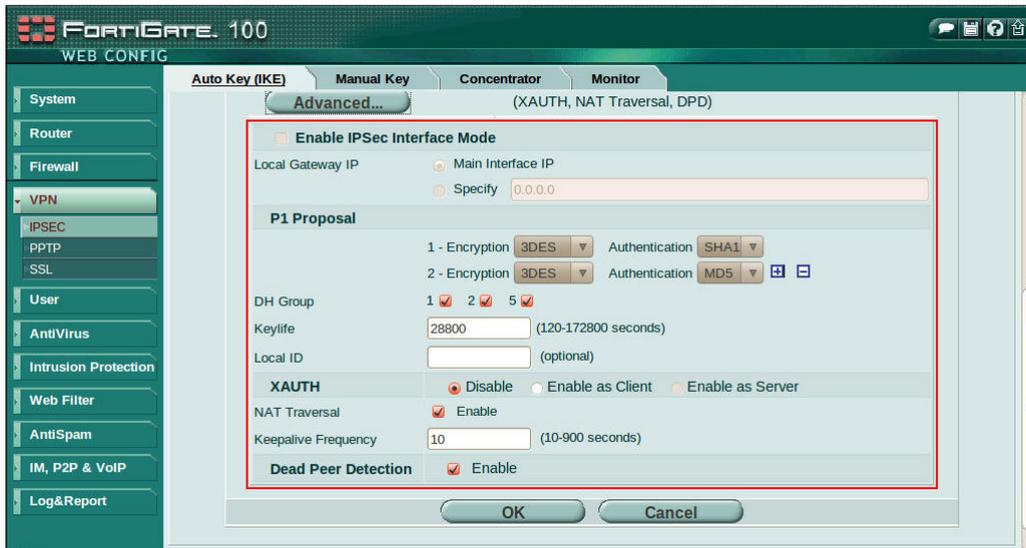
Press the button "**Create Phase 1**". Fill in Name, IP Address and Pre-share key. The **IP Address** under Remote Gateway is the IP address of external network connecting point of DSR-1000N which is shown as the point "c" on the topology. Insert the **Pre-shared Key** which is as same as the one put in DSR-1000N in the previous step.

The screenshot shows the FortiGate 100 WEB CONFIG interface. The left sidebar has 'VPN' and 'IPSEC' highlighted. The main area shows the 'Edit Phase 1' dialog box with the following fields:

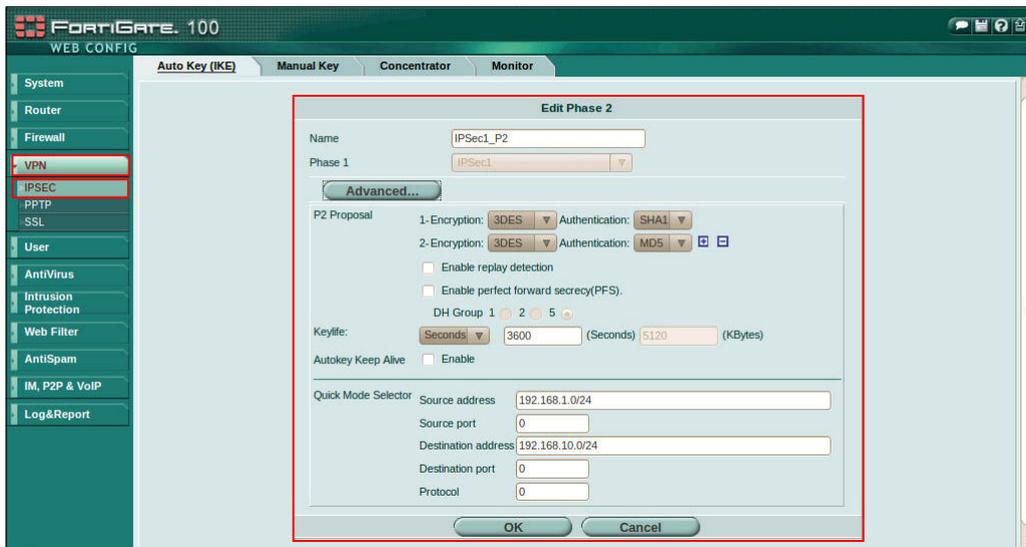
Name	IPSec1
Remote Gateway	Static IP Address
IP Address	1.1.1.2
Local Interface	external
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)
Authentication Method	Preshared Key
Pre-shared Key
Peer Options	<input checked="" type="radio"/> Accept any peer ID (XAUTH, NAT Traversal, DPD)

Buttons: Advanced..., OK, Cancel

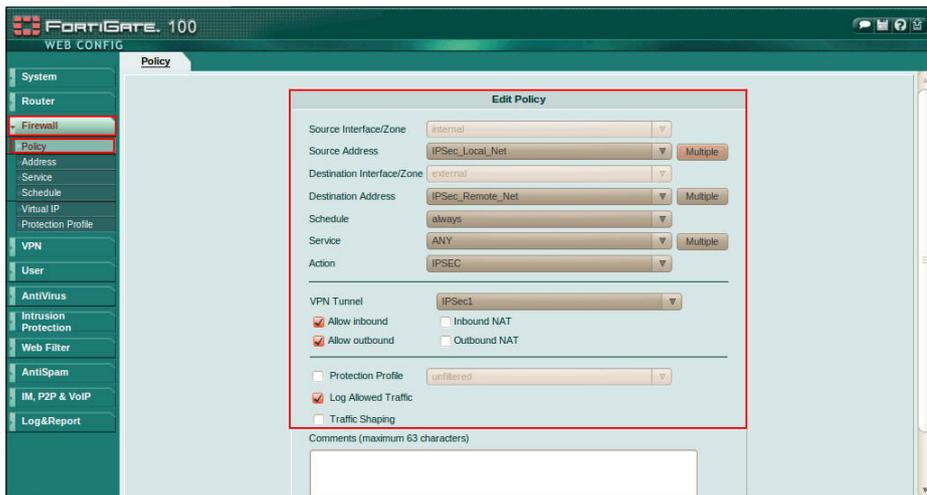
Press the button "**Advanced**". Configure the setting as below.



Navigate to **VPN > IPSec > Auto Key (IKE)**. Press the button "**Create Phase2**" and configure below relative information.



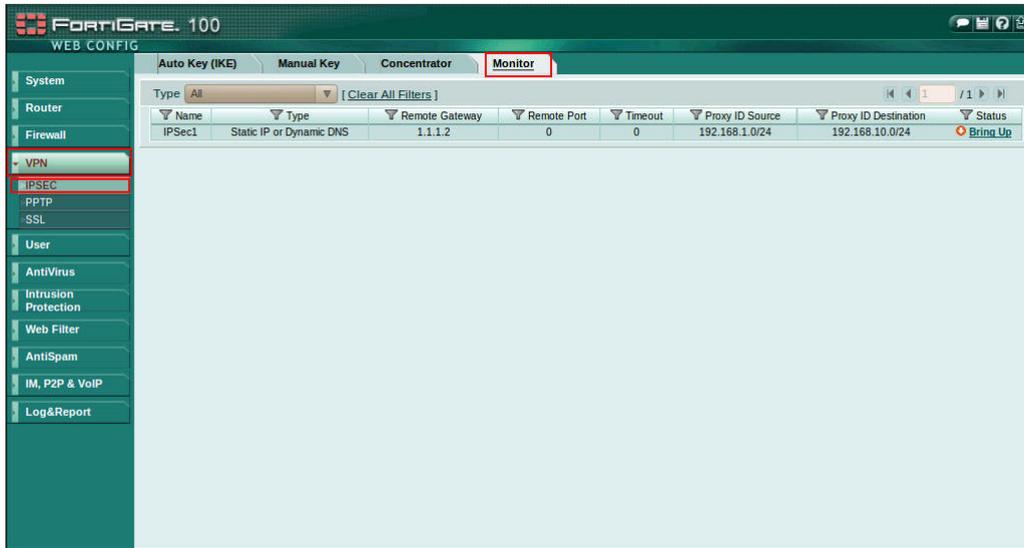
4. Set up Firewall Policy. Navigate to **Firewall > Policy**. Press button **“Create New”** and configure the settings as below.



5. Set up the Firewall Policy. Navigate to the **Firewall > Policy**. Press the button **“Create New”** and configure settings as below.



6. Check the IPSec status. Navigate to the **VPN > IPSec > Monitor**.



The screenshot displays the FortiGate 100 Web Config interface. The left sidebar shows the navigation menu with 'VPN' and 'IPSEC' highlighted. The main content area is titled 'Monitor' and shows a table of IPSec configurations. The table has the following columns: Name, Type, Remote Gateway, Remote Port, Timeout, Proxy ID Source, Proxy ID Destination, and Status. One configuration is listed: 'IPSec1' with Type 'Static IP or Dynamic DNS', Remote Gateway '1.1.1.2', Remote Port '0', Timeout '0', Proxy ID Source '192.168.1.0/24', Proxy ID Destination '192.168.10.0/24', and Status 'Bring Up'.

Name	Type	Remote Gateway	Remote Port	Timeout	Proxy ID Source	Proxy ID Destination	Status
IPSec1	Static IP or Dynamic DNS	1.1.1.2	0	0	192.168.1.0/24	192.168.10.0/24	Bring 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 © 2011 D-Link Corporation. All Rights Reserved.