Configuration Guide

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

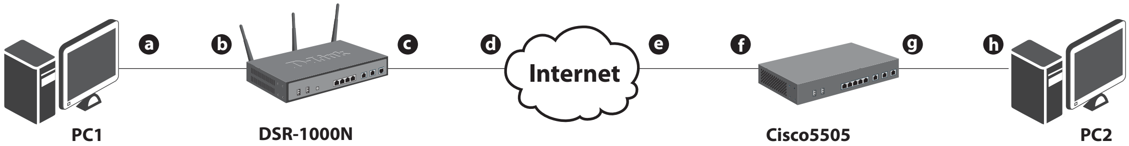
Overview

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 Cisco 5505. 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.

D-Link®

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.



a	192.168.10.100/24
b	192.168.10.1/24 (LAN 1)
c	1.1.1.2/30 (WAN1)
d	1.1.1.2/30
e	2.2.2.1/30
f	2.2.2.1/30 (external)
g	192.168.1.1/24 (internal)
h	192.168.1.100/24

IP addresses

DSR WAN: **1.1.1.2/30**
DSR LAN: **192.168.10.1/24**

FortiGate100 WAN: **2.2.2.2/30**
ForiGate100 LAN: **192.168.1.99/24**

IPSec Parameters

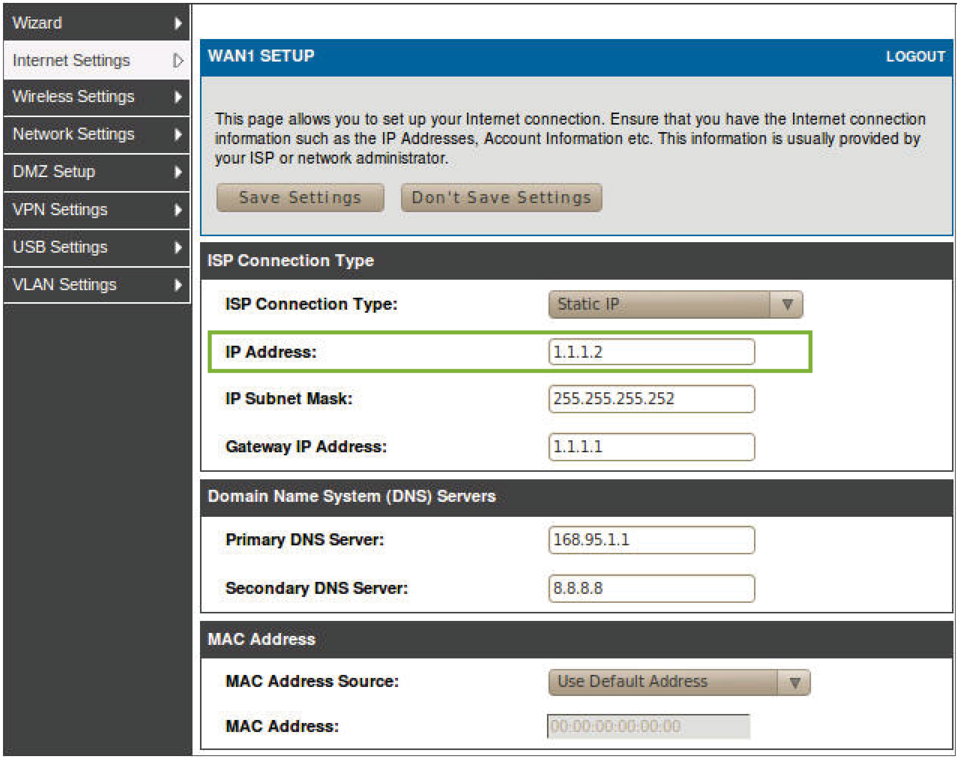
IPSec Mode: **Tunnel Mode**
IPSec Protocol: **ESP**
Phase1 Exchange Mode: **Main**
Phase1 Encryption: **3DES**
Phase1 Authentication: **SHA1**
Phase1 Authentication Method: **Pre-Shared Key**

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.



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.

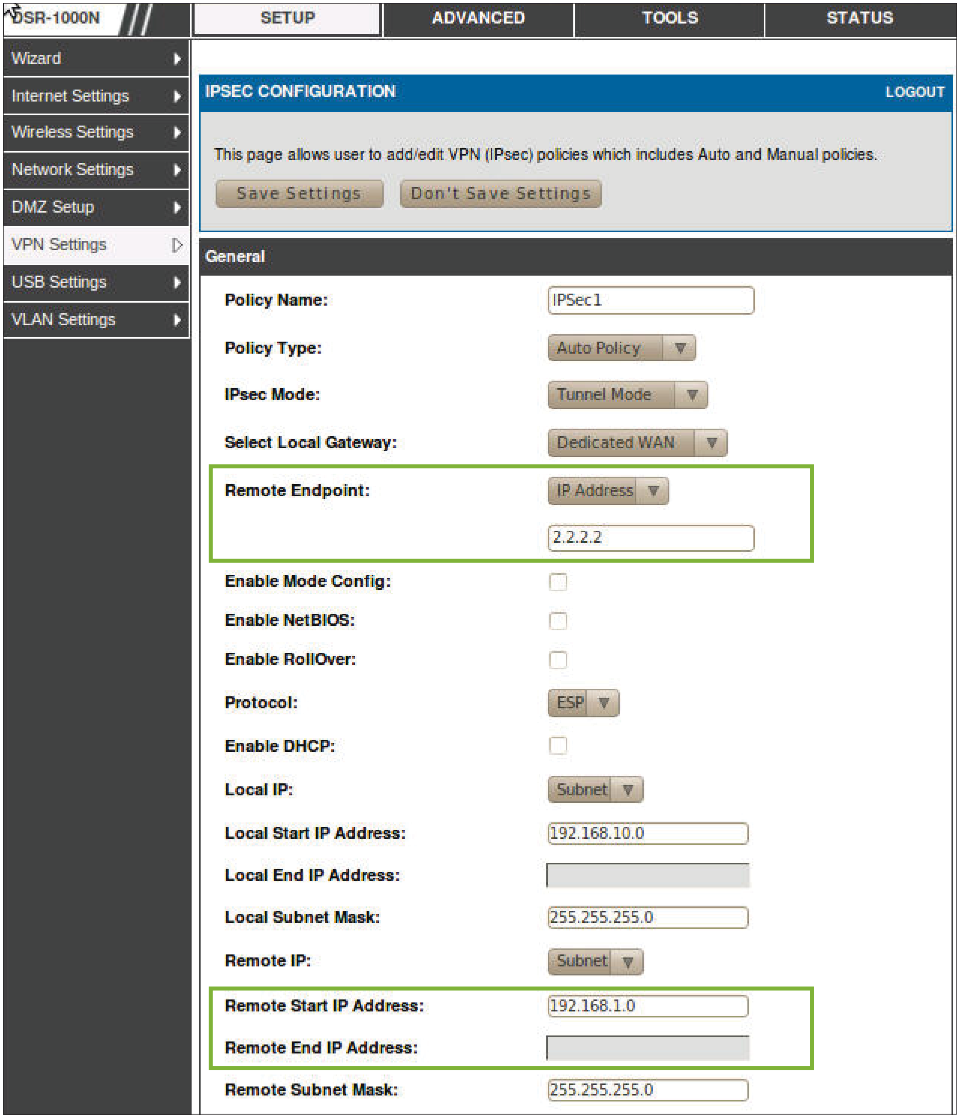
ISP Connection Type: Static IP
IP Address: 1.1.1.2
IP Subnet Mask: 255.255.255.252
Gateway IP Address: 1.1.1.1

Primary DNS Server: 168.95.1.1
Secondary DNS Server: 8.8.8.8

MAC Address Source: Use Default Address
MAC Address: 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 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.



IPSEC CONFIGURATION

This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.

General

Policy Name: IPSec1

Policy Type: Auto Policy

IPsec Mode: Tunnel Mode

Select Local Gateway: Dedicated WAN

Remote Endpoint: IP Address 2.2.2.2

Enable Mode Config: □

Enable NetBIOS: □

Enable RollOver: □

Protocol: ESP

Enable DHCP: □

Local IP: Subnet

Local Start IP Address: 192.168.10.0

Local End IP Address:

Local Subnet Mask: 255.255.255.0

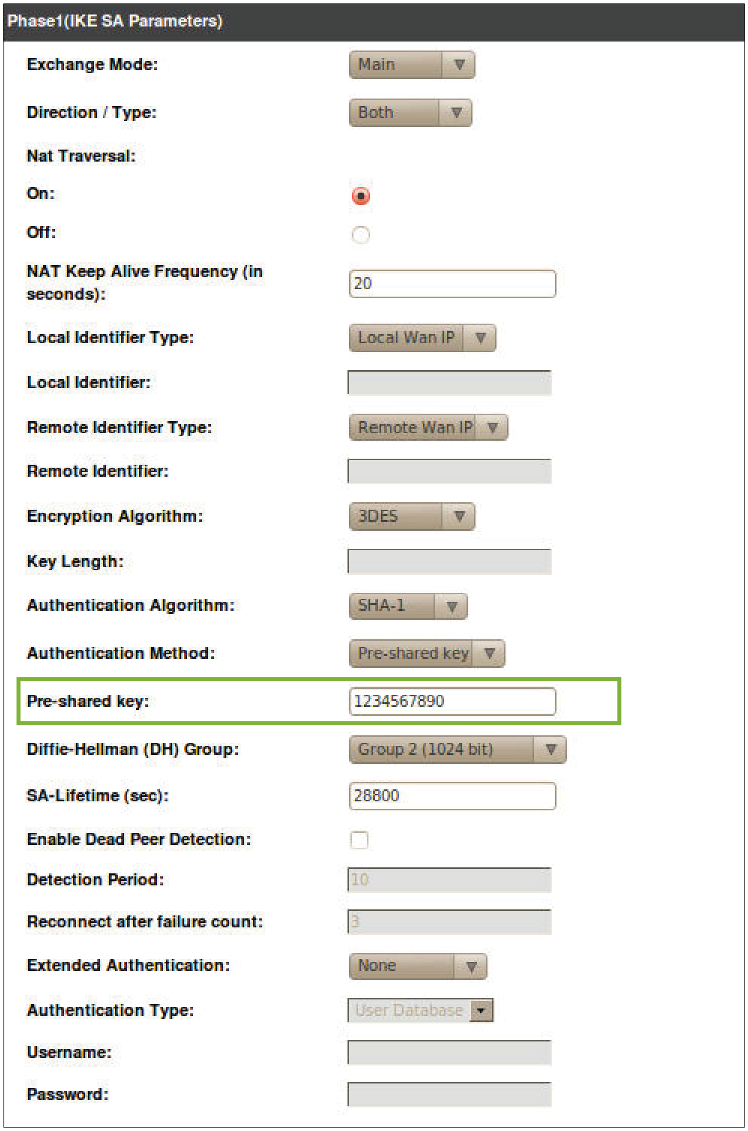
Remote IP: Subnet

Remote Start IP Address: 192.168.1.0

Remote End IP Address:

Remote Subnet Mask: 255.255.255.0

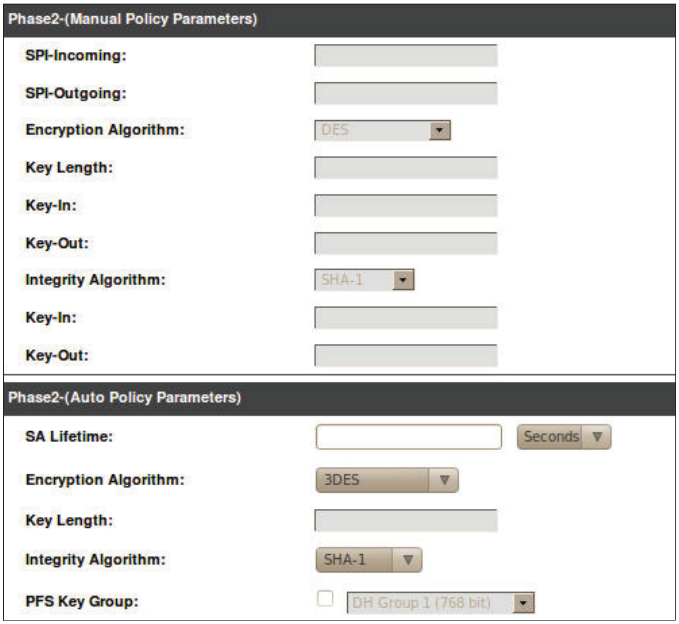
In Phase 1 Section, fill in relative information. Please notice that the **Pre-shared Key** must be as same as the pre-shared key which will be inserted on Fortigate 100 on the later step.



Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
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:	1234567890
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:	

In Phase 2 Section, fill in relative information.



Phase2-(Manual Policy Parameters)

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

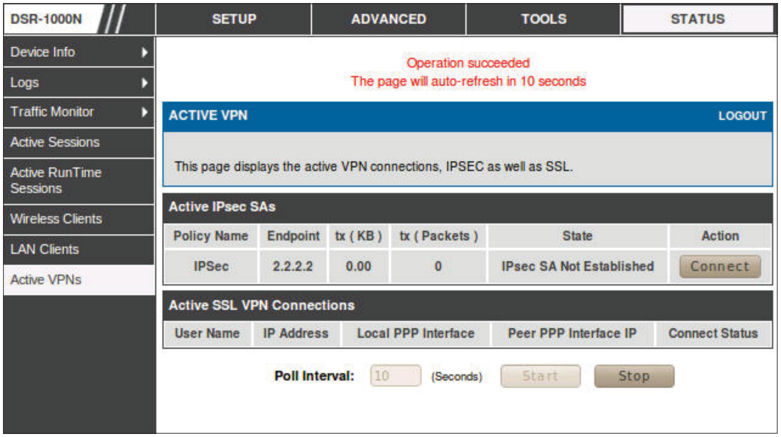
Phase2-(Auto Policy Parameters)

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

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.



Operation succeeded
The page will auto-refresh in 10 seconds

ACTIVE VPN

This page displays the active VPN connections, IPSEC as well as SSL.

Active IPsec SAs

Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action
IPSec	2.2.2.2	0.00	0	IPsec SA Not Established	Connect

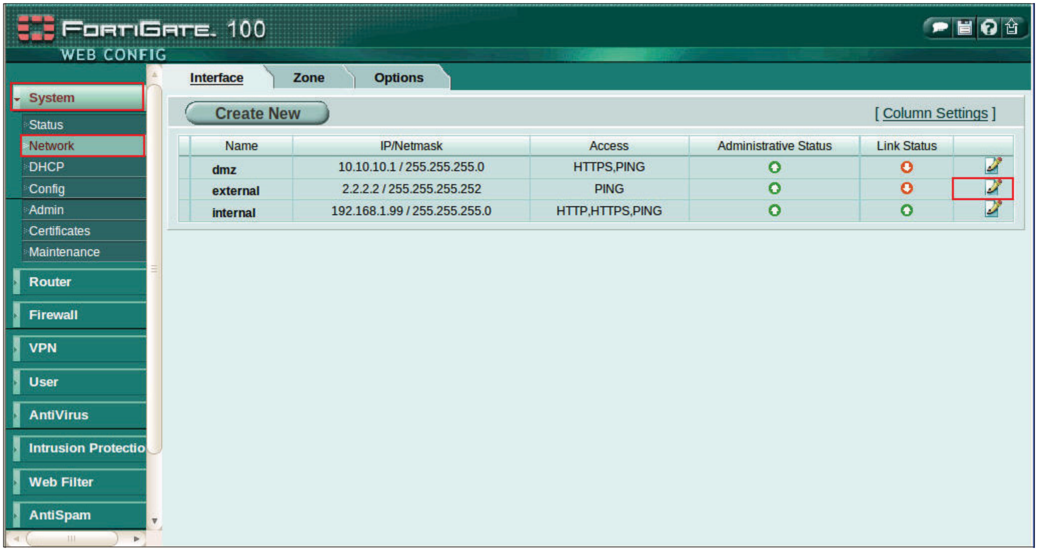
Active SSL VPN Connections

User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status

Poll Interval: 10 (Seconds) Start Stop

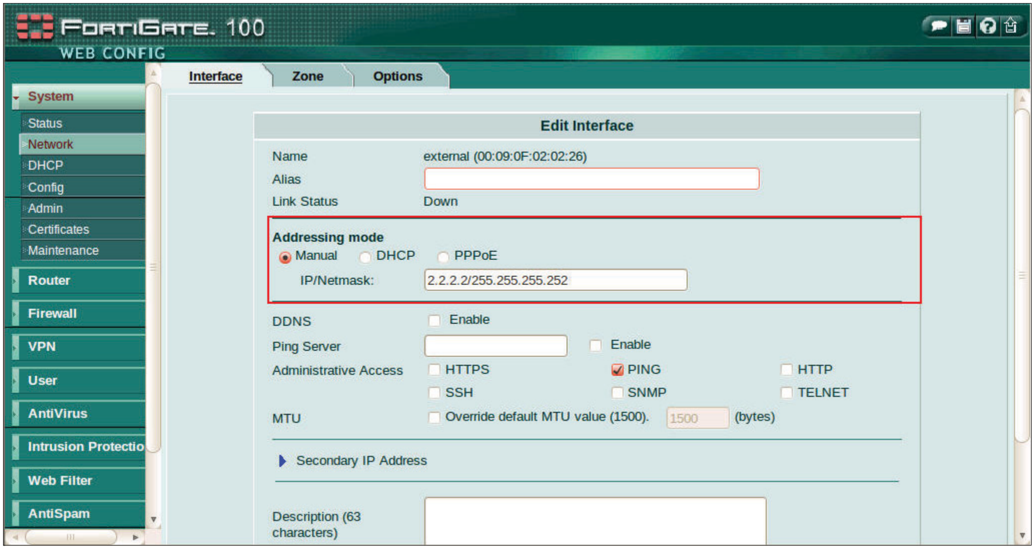
FortiGate Settings

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



Name	IP/Netmask	Access	Administrative Status	Link Status	
dmz	10.10.10.1 / 255.255.255.0	HTTPS,PING	●	●	✎
external	2.2.2.2 / 255.255.255.252	PING	●	●	✎
internal	192.168.1.99 / 255.255.255.0	HTTP,HTTPS,PING	●	●	✎

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.



Edit Interface

Name external (00:09:0F:02:02:26)

Alias

Link Status Down

Addressing mode

● Manual ○ DHCP ○ PPPoE

IP/Netmask: 2.2.2.2/255.255.255.252

DDNS □ Enable

Ping Server □ Enable

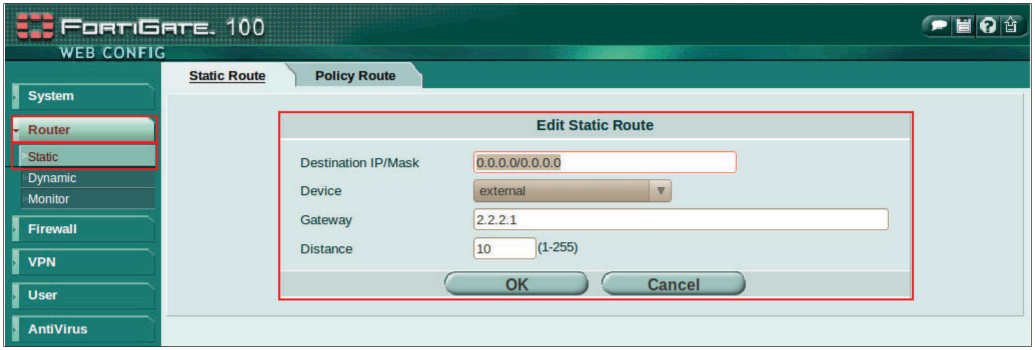
Administrative Access □ HTTPS ☑ PING □ HTTP
□ SSH □ SNMP □ TELNET

MTU □ Override default MTU value (1500). 1500 (bytes)

Secondary IP Address

Description (63 characters)

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

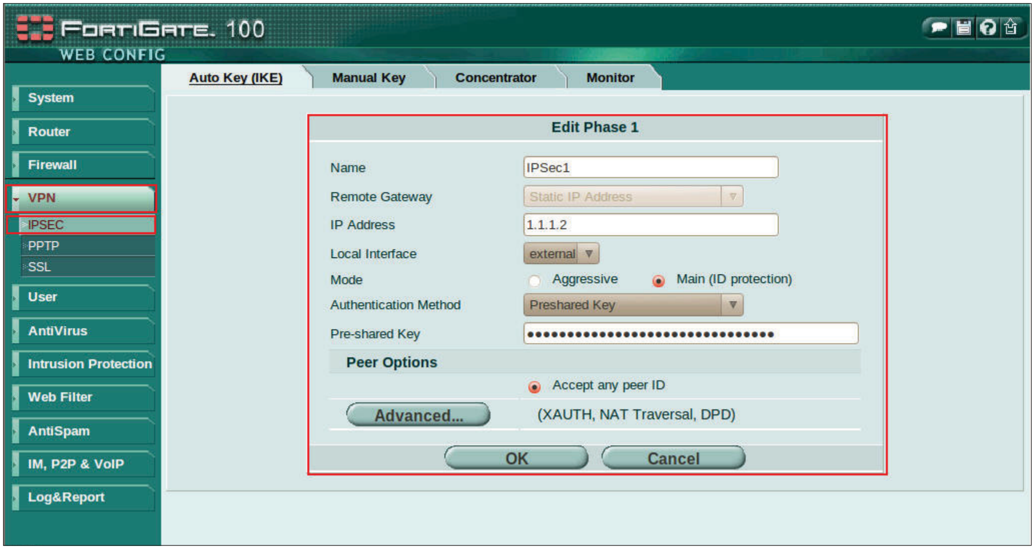


Edit Static Route

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

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

Press the button "**Create Phase1**". 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.



Edit Phase 1

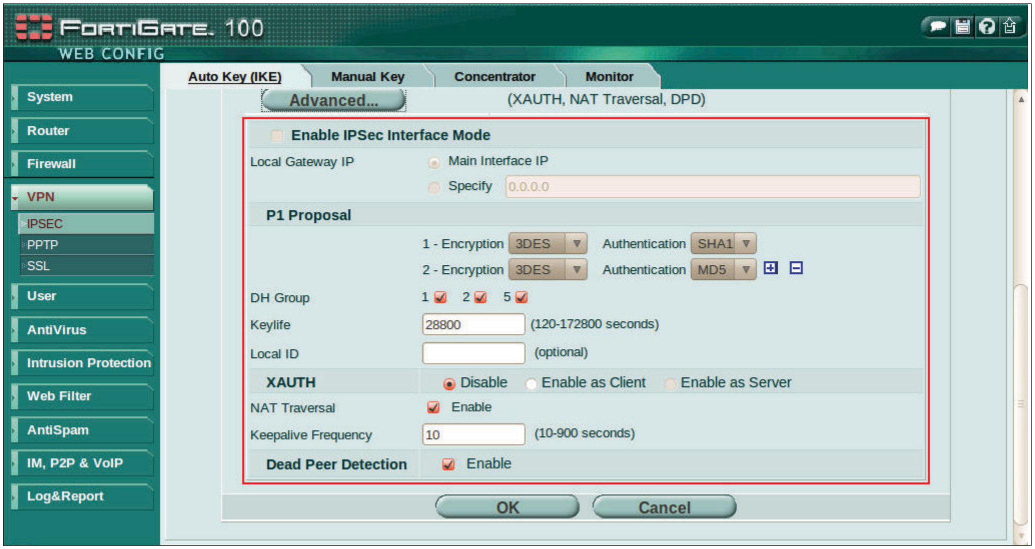
Name	IPSec1
Remote Gateway	Static IP Address
IP Address	1.1.1.2
Local Interface	external
Mode	○ Aggressive ● Main (ID protection)
Authentication Method	Preshared Key
Pre-shared Key	••••••••••••••••••••••••••••••••••

Peer Options

● Accept any peer ID

(XAUTH, NAT Traversal, DPD)

Press the button “**Advanced**”. Configure the setting as below.



(XAUTH, NAT Traversal, DPD)

□ Enable IPSec Interface Mode

Local Gateway IP ○ Main Interface IP ○ Specify 0.0.0.0

P1 Proposal

1 - Encryption 3DES Authentication SHA1

2 - Encryption 3DES Authentication MD5

DH Group 1 ☑ 2 ☑ 5 ☑

Keylife 28800 (120-172800 seconds)

Local ID (optional)

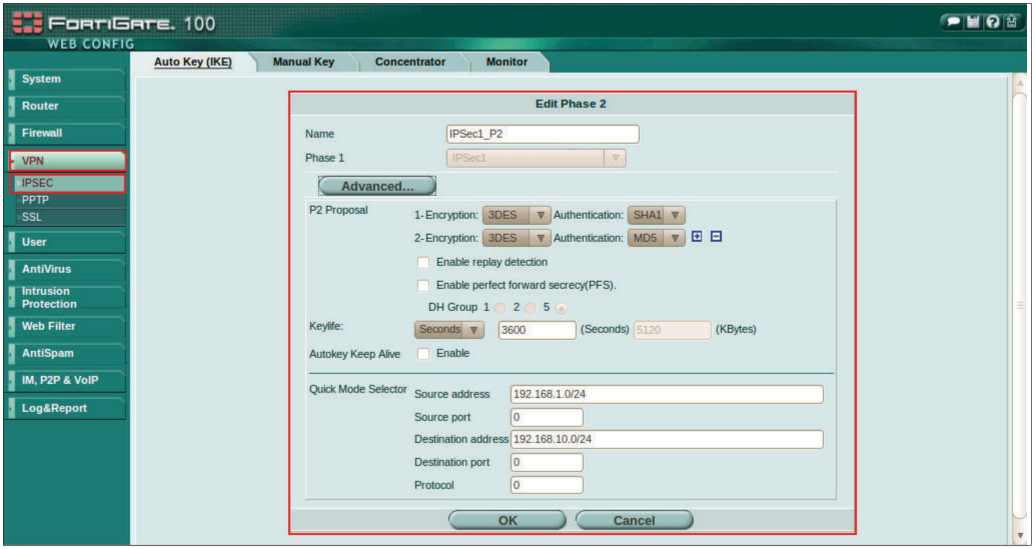
XAUTH ● Disable ○ Enable as Client ○ Enable as Server

NAT Traversal ☑ Enable

Keepalive Frequency 10 (10-900 seconds)

Dead Peer Detection ☑ Enable

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



Edit Phase 2

Name IPSec1_P2

Phase 1 IPSec1

P2 Proposal 1-Encryption: 3DES Authentication: SHA1

2-Encryption: 3DES Authentication: MD5

□ Enable replay detection

□ Enable perfect forward secrecy(PFS).

DH Group 1 ○ 2 ○ 5 ●

Keylife: Seconds 3600 (Seconds) 5120 (KBytes)

Autokey Keep Alive □ Enable

Quick Mode Selector

Source address 192.168.1.0/24

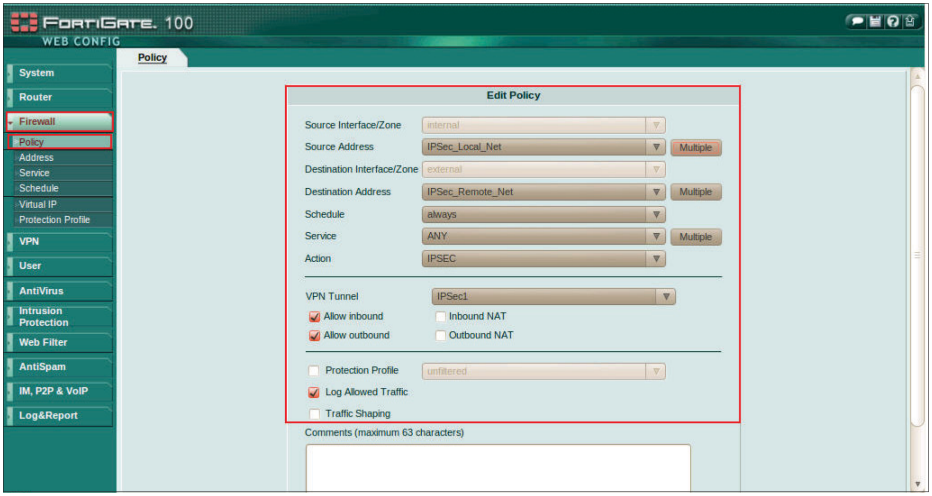
Source port 0

Destination address 192.168.10.0/24

Destination port 0

Protocol 0

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



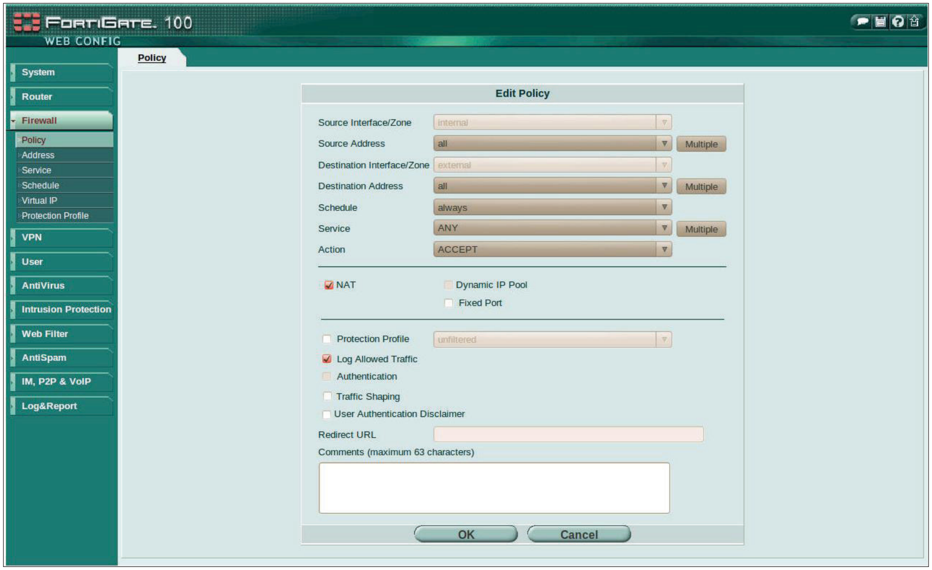
Edit Policy

Source Interface/Zone: internal
Source Address: IPSec_Local_Net
Destination Interface/Zone: external
Destination Address: IPSec_Remote_Net
Schedule: always
Service: ANY
Action: IPSEC

VPN Tunnel: IPSec1
☑ Allow inbound □ Inbound NAT
☑ Allow outbound □ Outbound NAT

□ Protection Profile: unfiltered
☑ Log Allowed Traffic
□ Traffic Shaping
Comments (maximum 63 characters)

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



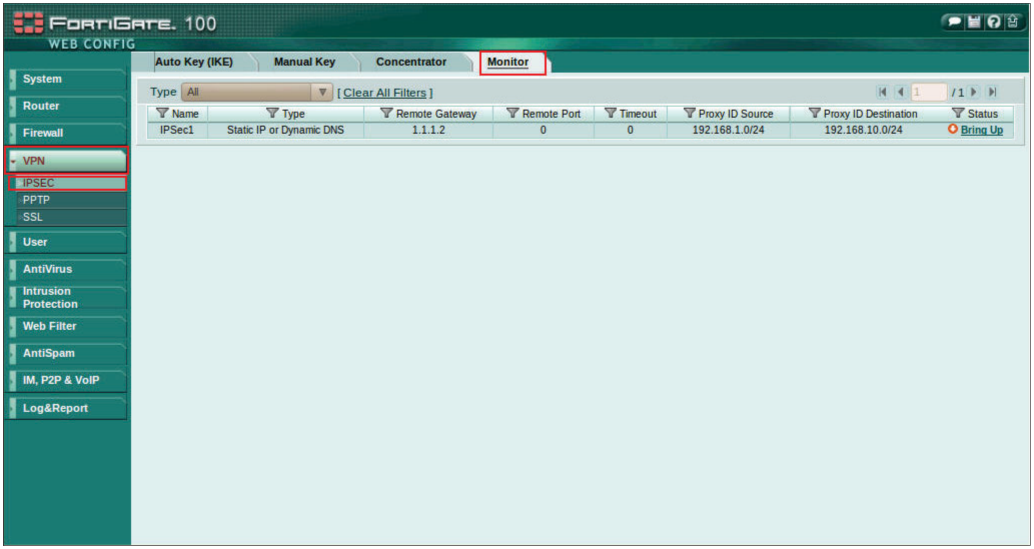
Edit Policy

Source Interface/Zone: internal
Source Address: all
Destination Interface/Zone: external
Destination Address: all
Schedule: always
Service: ANY
Action: ACCEPT

☑ NAT □ Dynamic IP Pool
□ Fixed Port

□ Protection Profile: unfiltered
☑ Log Allowed Traffic
□ Authentication
□ Traffic Shaping
□ User Authentication Disclaimer
Redirect URL:
Comments (maximum 63 characters)

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



Type: All

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