Configuration Guide

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

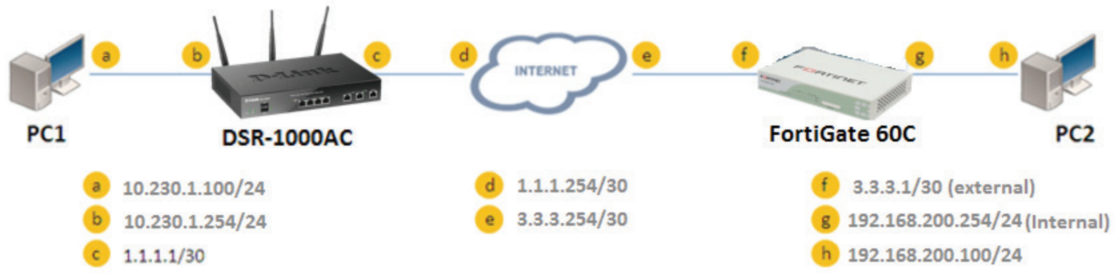
Overview

This document describes how to implement IPsec with pre-shared secrets establishing a site-to-site VPN tunnel between the D-Link DSR-1000AC and the Fortinet Fortigate 60C. The screenshots in this document are from firmware version 3.10 of the DSR-1000AC and firmware version 5.2.3 of the Fortinet Fortigate 60C. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see in your browser.

D-Link®

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: **1.1.1.1/30**
DSR LAN: **10.230.1.254/24**

FortiGate 60C WAN: **3.3.3.1/30**
ForiGate 60C LAN: **192.168.200.254/24**

IPsec Parameters:

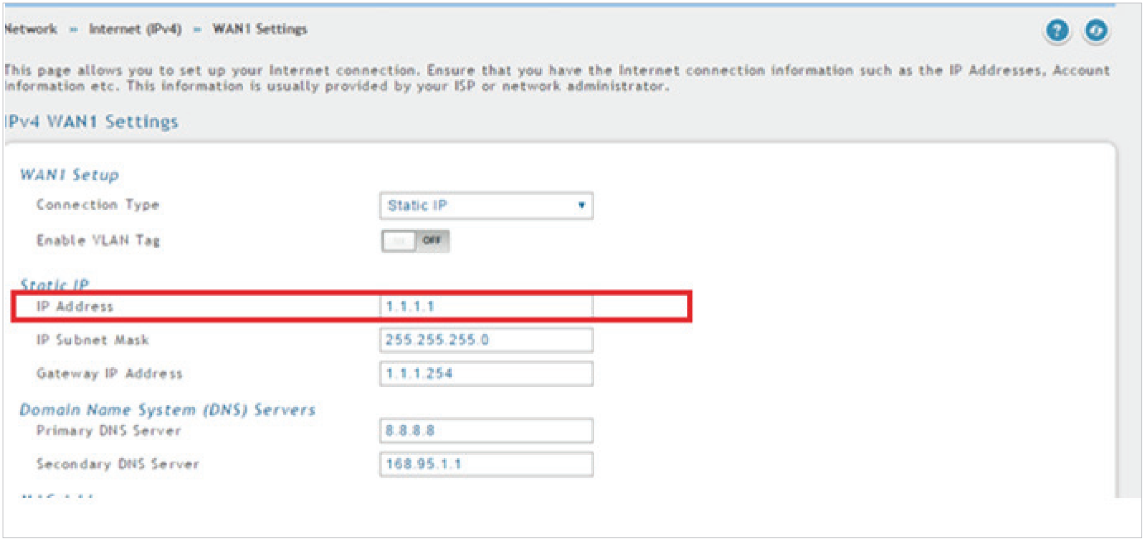
IPsec Mode: **Tunnel Mode**
IPsec Protocol: **ESP**
Phase1 Exchange Mode: **Main**
Phase1 Encryption: **3DES, AES128**
Phase1 Authentication: **SHA1**
Phase1 Authentication Method: **Pre-Shared Key**

Diffie-Hellman Group: **Group 2**
Phase1 Lifetime: **28800 sec**
Phase2 Encryption: **3DES, AES128, AES192**
Phase2 Authentication: **SHA1, MD5**
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 the point "**c**" in the topology. Click the "**Save**" button to complete the WAN IP address setting.



Network » Internet (IPv4) » WAN1 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.

IPv4 WAN1 Settings

WAN1 Setup

Connection Type	Static IP
Enable VLAN Tag	OFF

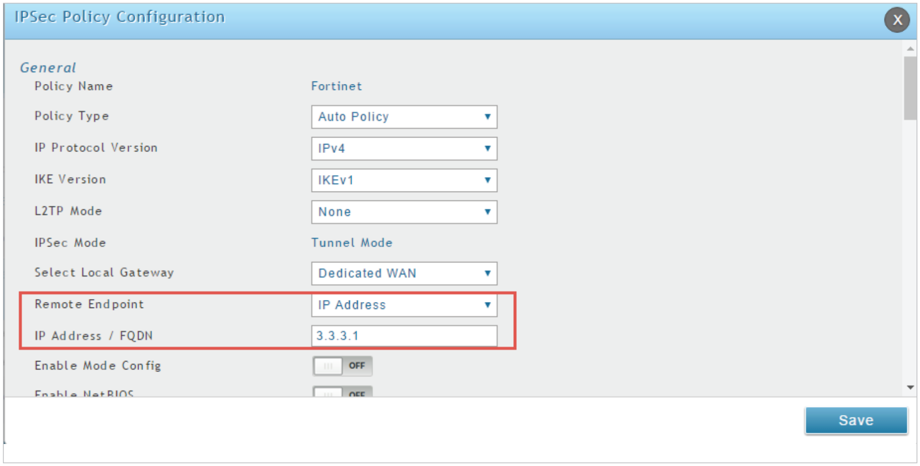
Static IP

IP Address	1.1.1.1
IP Subnet Mask	255.255.255.0
Gateway IP Address	1.1.1.254

Domain Name System (DNS) Servers

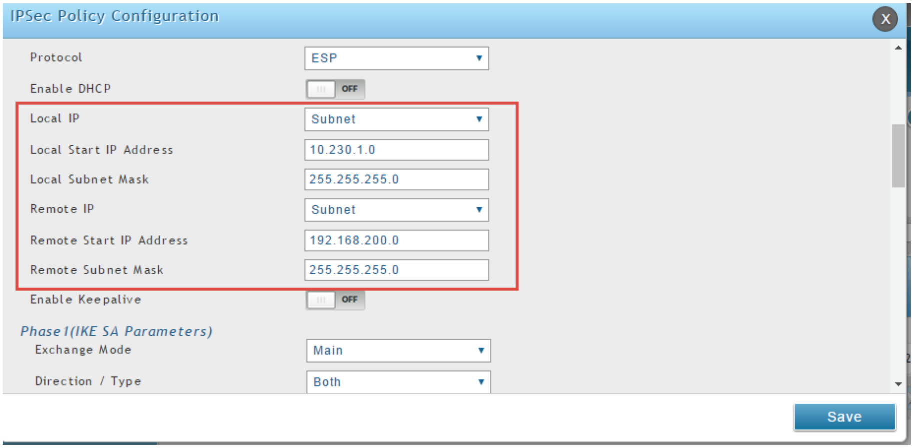
Primary DNS Server	8.8.8.8
Secondary DNS Server	168.95.1.1

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 Fortigate 60C, 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 Fortigate 60C.



General

Policy Name	Fortinet
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	3.3.3.1
Enable Mode Config	OFF
Enable NetBIOS	OFF

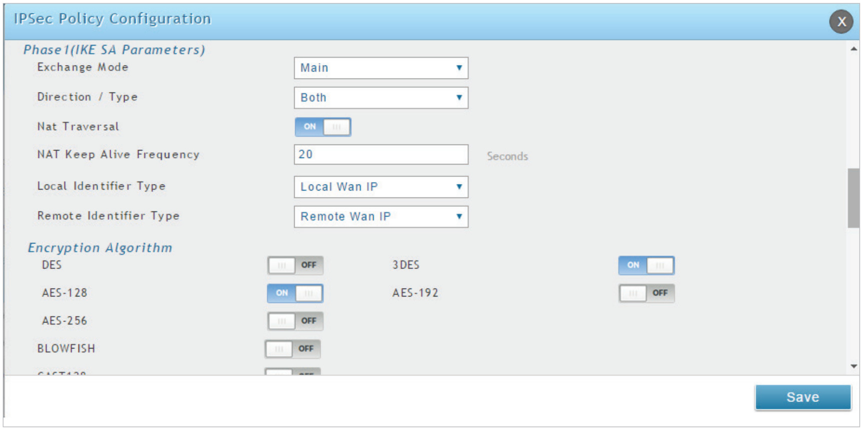


Protocol	ESP
Enable DHCP	OFF
Local IP	Subnet
Local Start IP Address	10.230.1.0
Local Subnet Mask	255.255.255.0
Remote IP	Subnet
Remote Start IP Address	192.168.200.0
Remote Subnet Mask	255.255.255.0
Enable Keepalive	OFF

Phase1(IKE SA Parameters)

Exchange Mode	Main
Direction / Type	Both

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 Fortigate 60C later.



IPSec Policy Configuration

Phase I(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

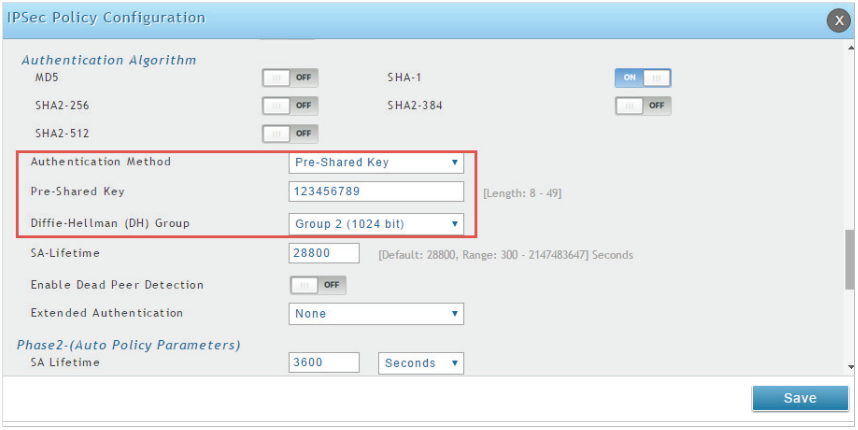
3DES: ON

AES-128: ON

AES-192: OFF

AES-256: OFF

BLOWFISH: OFF



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: 123456789 [Length: 8 - 49]

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

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

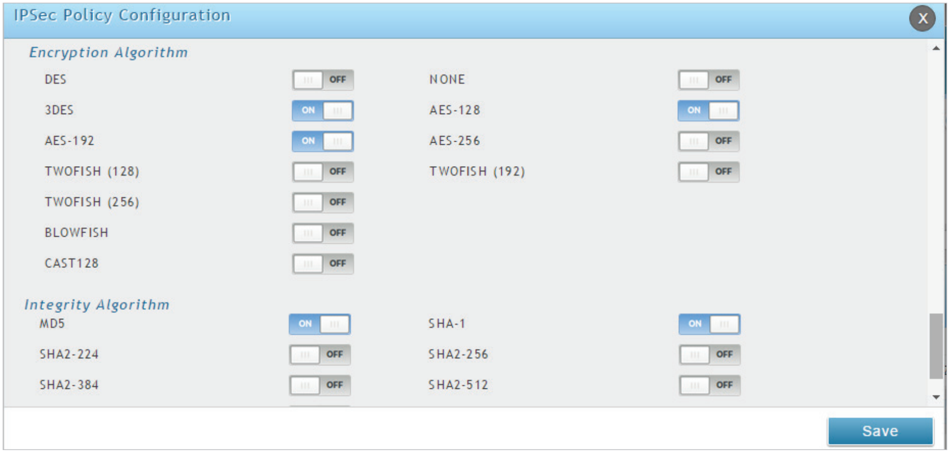
Enable Dead Peer Detection: OFF

Extended Authentication: None

Phase2-(Auto Policy Parameters)

SA Lifetime: 3600 Seconds

In the Phase 2 section, fill in relevant information.



IPSec Policy Configuration

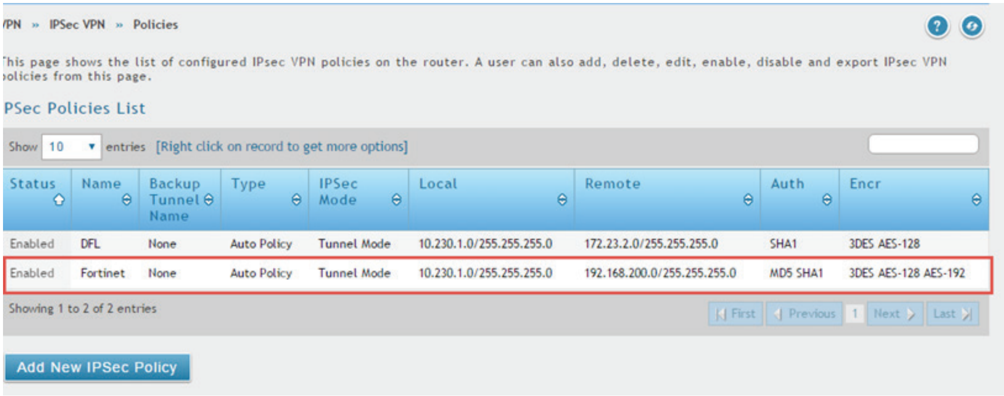
Encryption Algorithm

DES	OFF	NONE	OFF
3DES	ON	AES-128	ON
AES-192	ON	AES-256	OFF
TWOFISH (128)	OFF	TWOFISH (192)	OFF
TWOFISH (256)	OFF		
BLOWFISH	OFF		
CAST128	OFF		

Integrity Algorithm

MD5	ON	SHA-1	ON
SHA2-224	OFF	SHA2-256	OFF
SHA2-384	OFF	SHA2-512	OFF

Click the "**Save**" button to complete the IPsec Policy settings.



PN » IPSec VPN » Policies

his 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 olicies from this page.

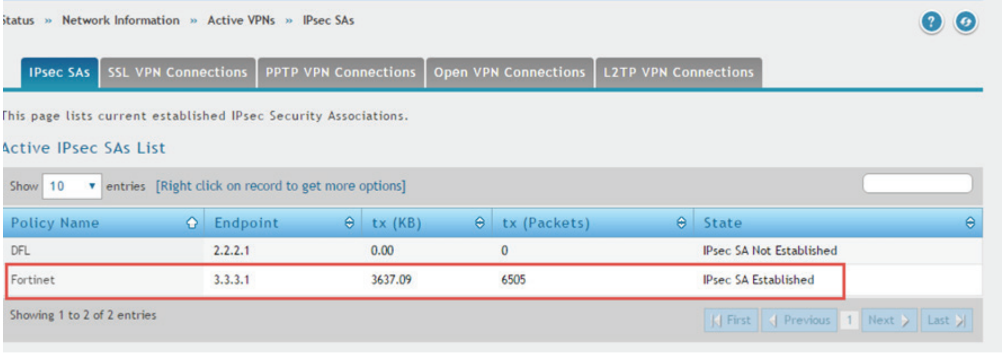
PSec Policies List

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

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
Enabled	DFL	None	Auto Policy	Tunnel Mode	10.230.1.0/255.255.255.0	172.23.2.0/255.255.255.0	SHA1	3DES AES-128
Enabled	Fortinet	None	Auto Policy	Tunnel Mode	10.230.1.0/255.255.255.0	192.168.200.0/255.255.255.0	MD5 SHA1	3DES AES-128 AES-192

Showing 1 to 2 of 2 entries

3. Check the VPN status. Navigate to: Status > Network Information > Active VPNs > IPsec SAs.
The activity will be shown in the list as the tunnel is established with the other side.



This page lists current established IPsec Security Associations.

Active IPsec SAs List

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

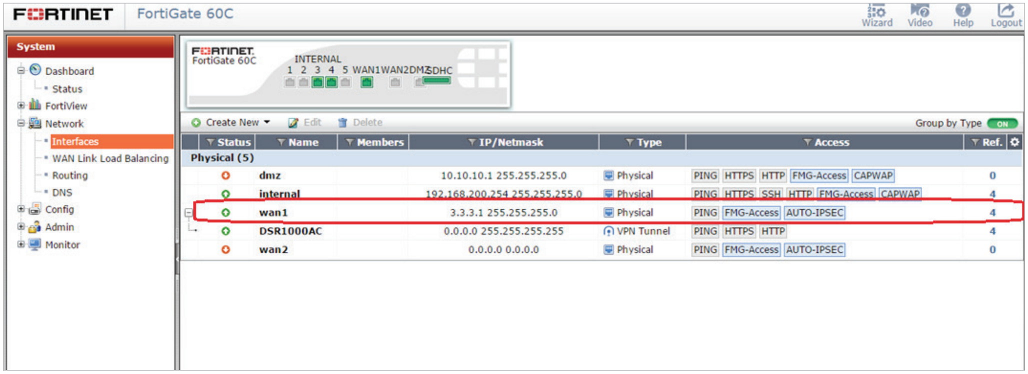
Policy Name	Endpoint	tx (KB)	tx (Packets)	State
DFL	2.2.2.1	0.00	0	IPsec SA Not Established
Fortinet	3.3.3.1	3637.09	6505	IPsec SA Established

Showing 1 to 2 of 2 entries

FortiGate Settings

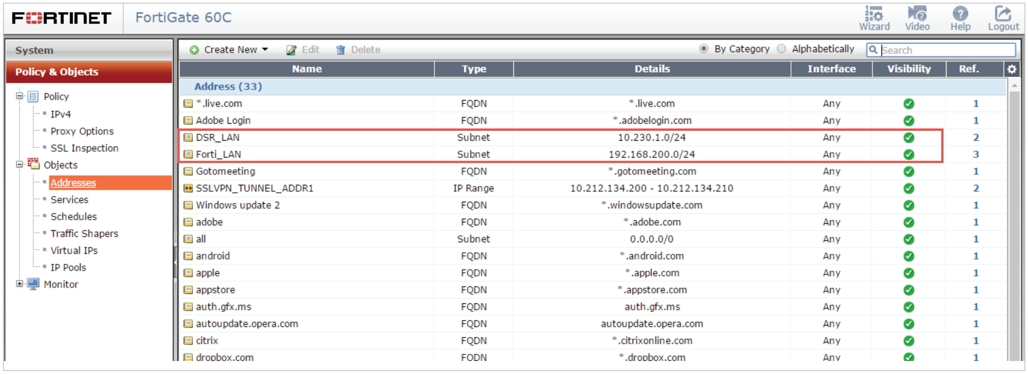
1. Set up the WAN IP address, Navigate to: System > Network

First, click the "**Edit**" button. Edit the IP Address with the following information. The **IP/Netmask** of the Interface tab is the IP address and Netmask of the external network connection, which is shown as point "**f**" in the topology.



Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (5)						
	dmz		10.10.10.1 255.255.255.0	Physical	PING HTTPS HTTP FMG-Access CAPWAP	0
	internal		192.168.200.254 255.255.255.0	Physical	PING HTTPS SSH HTTP FMG-Access CAPWAP	4
	wan1		3.3.3.1 255.255.255.0	Physical	PING FMG-Access AUTO-IPSEC	4
	DSR1000AC		0.0.0.0 255.255.255.255	VPN Tunnel	PING HTTPS HTTP	4
	wan2		0.0.0.0 0.0.0.0	Physical	PING FMG-Access AUTO-IPSEC	0

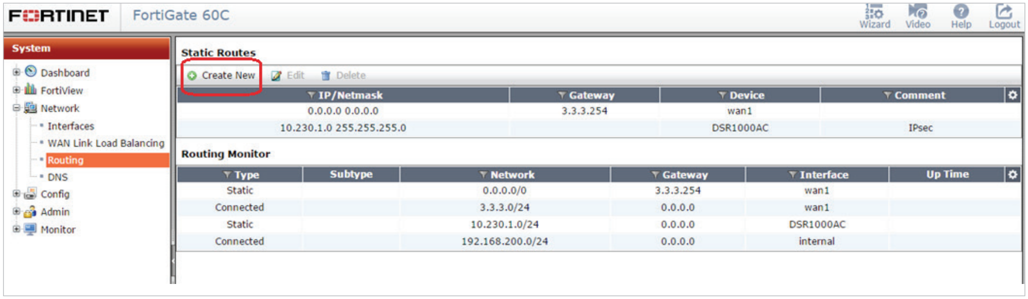
Second, navigate to **Policy & Objects > Objects > Address** to add two objects "10.230.1.0/24" and "192.168.200.0/24," which indicate the internal IP addresses of both connections.



Name	Type	Details	Interface	Visibility	Ref.
Address (33)					
*.live.com	FQDN	*.live.com	Any	✓	1
Adobe Login	FQDN	*.adobelogin.com	Any	✓	1
DSR_LAN	Subnet	10.230.1.0/24	Any	✓	2
Forti_LAN	Subnet	192.168.200.0/24	Any	✓	3
Gotomeeting	FQDN	*.gotomeeting.com	Any	✓	1
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	Any	✓	2
Windows update 2	FQDN	*.windowsupdate.com	Any	✓	1
adobe	FQDN	*.adobe.com	Any	✓	1
all	Subnet	0.0.0.0/0	Any	✓	1
android	FQDN	*.android.com	Any	✓	1
apple	FQDN	*.apple.com	Any	✓	1
appstore	FQDN	*.appstore.com	Any	✓	1
auth.gfx.ms	FQDN	auth.gfx.ms	Any	✓	1
autoupdate.opera.com	FQDN	autoupdate.opera.com	Any	✓	1
citrix	FQDN	*.citrixonline.com	Any	✓	1
dropbox.com	FQDN	*.dropbox.com	Any	✓	1

2. Set up the default gateway. Navigate to: System > Network > Routing.

Press the "**Create New**" button. Fill in the relevant information as below.

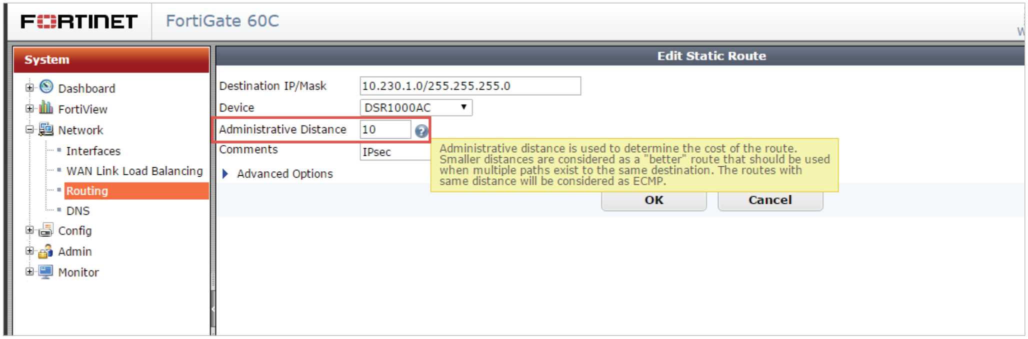


Static Routes

IP/Netmask	Gateway	Device	Comment
0.0.0.0 0.0.0.0	3.3.3.254	wan1	
10.230.1.0 255.255.255.0		DSR1000AC	IPsec

Routing Monitor

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	3.3.3.254	wan1	
Connected		3.3.3.0/24	0.0.0.0	wan1	
Static		10.230.1.0/24	0.0.0.0	DSR1000AC	
Connected		192.168.200.0/24	0.0.0.0	internal	

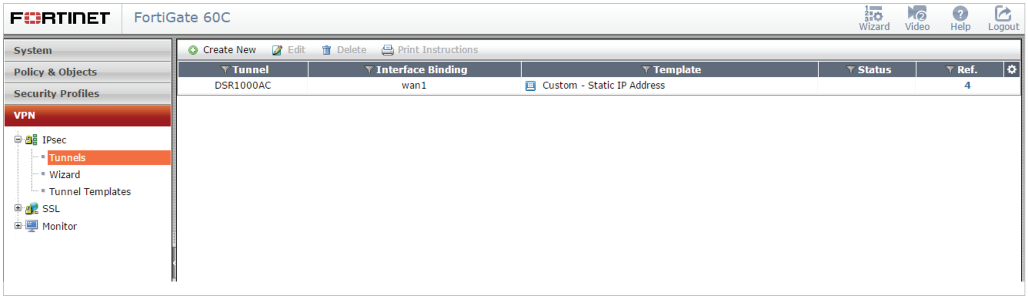


Edit Static Route

Destination IP/Mask	10.230.1.0/255.255.255.0
Device	DSR1000AC
Administrative Distance	10
Comments	IPsec

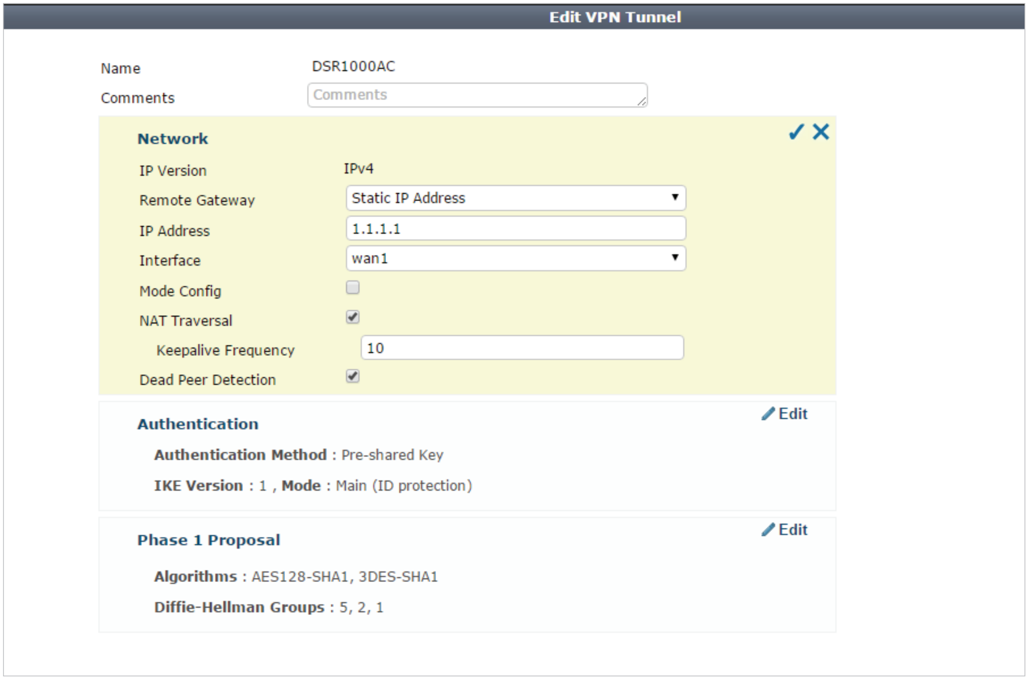
Administrative distance is used to determine the cost of the route. Smaller distances are considered as a "better" route that should be used when multiple paths exist to the same destination. The routes with same distance will be considered as ECMP.

3. Set up the IPsec Tunnel, go to: VPN > IPsec > Tunnels >.
Press the "**Create New**" button. Fill in the Name, IP Address, and Pre-shared Key.



Tunnel	Interface Binding	Template	Status	Ref.
DSR1000AC	wan1	Custom - Static IP Address		4

The **IP Address** under Remote Gateway is the IP address of the external network connection of the DSR-1000AC, which is shown as point "**c**" in the topology.



Edit VPN Tunnel

Name DSR1000AC

Comments Comments

Network ✓ ✕

IP Version	IPv4
Remote Gateway	Static IP Address ▾
IP Address	1.1.1.1
Interface	wan1 ▾
Mode Config	□
NAT Traversal	☑
Keepalive Frequency	10
Dead Peer Detection	☑

Authentication Edit

Authentication Method : Pre-shared Key

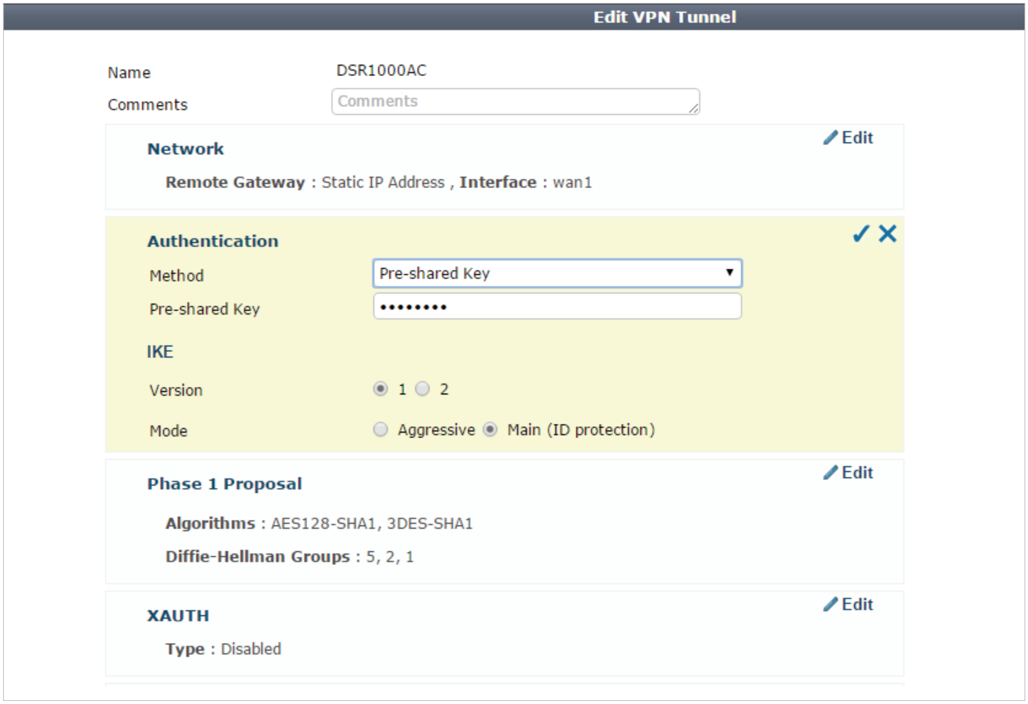
IKE Version : 1 , **Mode :** Main (ID protection)

Phase 1 Proposal Edit

Algorithms : AES128-SHA1, 3DES-SHA1

Diffie-Hellman Groups : 5, 2, 1

Press "**Edit**" in the Authentication area and insert the **Pre-shared Key**, which is the same as the one previously entered in the DSR-1000AC.



Edit VPN Tunnel

Name DSR1000AC

Comments Comments

Network ✎Edit

Remote Gateway : Static IP Address , **Interface** : wan1

Authentication ✓ ✕

Method Pre-shared Key ▾

Pre-shared Key ••••••••

IKE

Version ● 1 ○ 2

Mode ○ Aggressive ● Main (ID protection)

Phase 1 Proposal ✎Edit

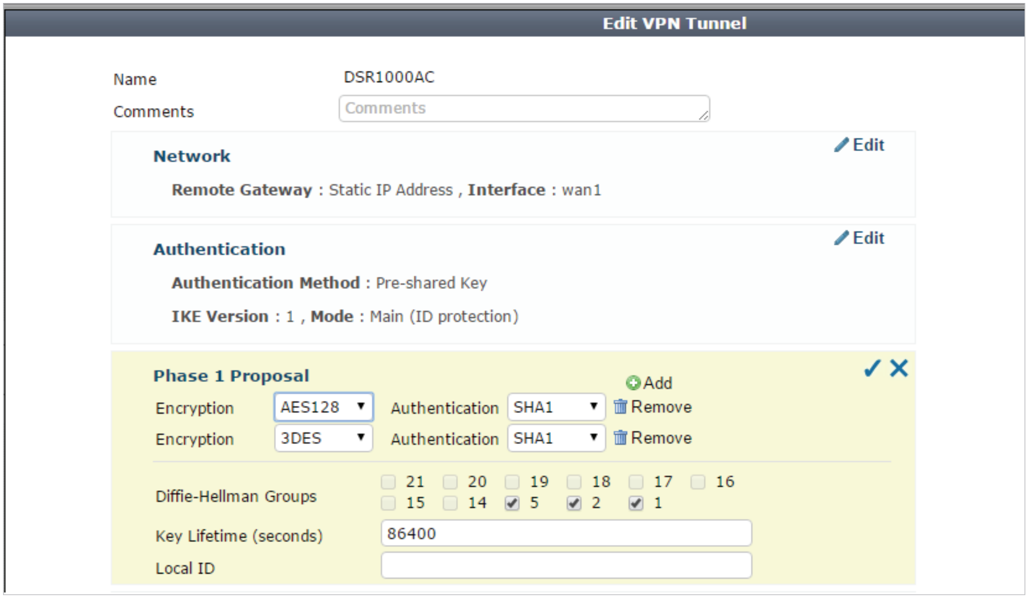
Algorithms : AES128-SHA1, 3DES-SHA1

Diffie-Hellman Groups : 5, 2, 1

XAUTH ✎Edit

Type : Disabled

Press "**Edit**" in the Phase 1 Proposal area and configure the relevant information below.



Edit VPN Tunnel

Name DSR1000AC

Comments

Network

Remote Gateway : Static IP Address , **Interface** : wan1

Authentication

Authentication Method : Pre-shared Key

IKE Version : 1 , **Mode** : Main (ID protection)

Phase 1 Proposal

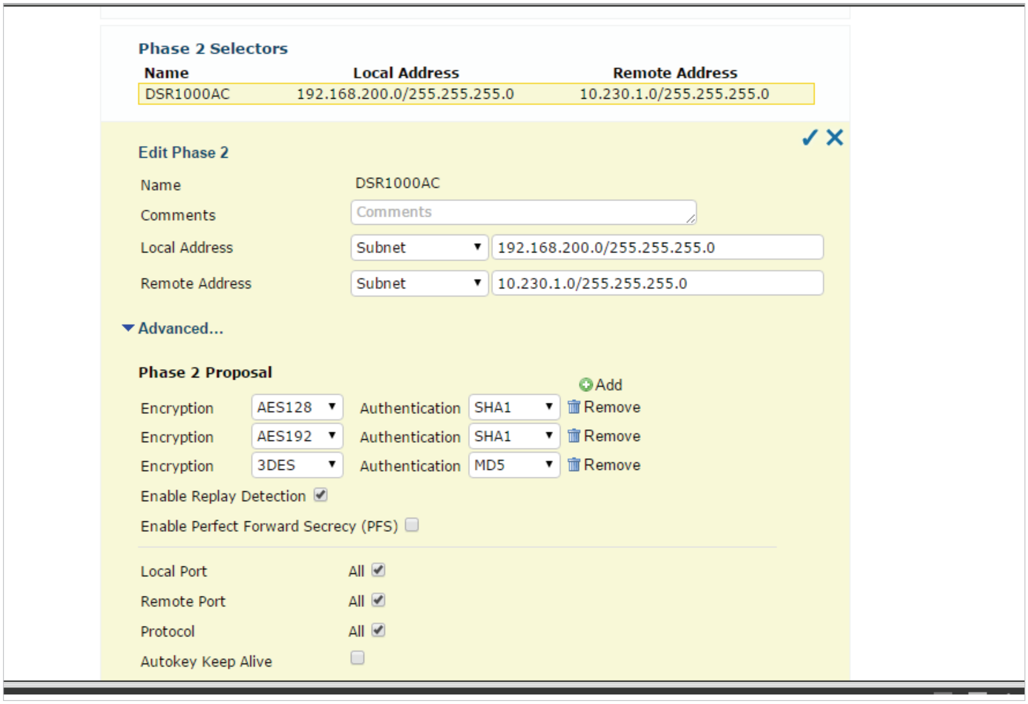
Encryption	AES128 ▾	Authentication	SHA1 ▾	Remove
Encryption	3DES ▾	Authentication	SHA1 ▾	Remove

Diffie-Hellman Groups □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 ☑ 2 ☑ 1

Key Lifetime (seconds) 86400

Local ID

Edit Phase 2 and configure the relevant information below.



Phase 2 Selectors

Name	Local Address	Remote Address
DSR1000AC	192.168.200.0/255.255.255.0	10.230.1.0/255.255.255.0

Edit Phase 2

Name	DSR1000AC
Comments	Comments
Local Address	Subnet 192.168.200.0/255.255.255.0
Remote Address	Subnet 10.230.1.0/255.255.255.0

Advanced...

Phase 2 Proposal

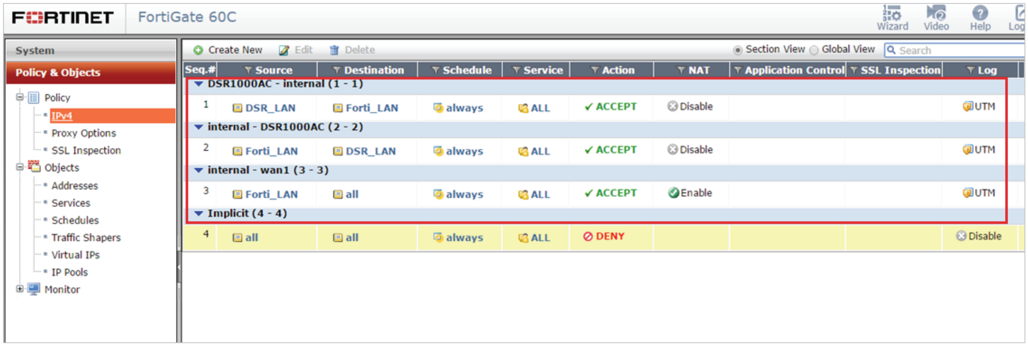
Encryption	AES128	Authentication	SHA1	Remove
Encryption	AES192	Authentication	SHA1	Remove
Encryption	3DES	Authentication	MD5	Remove

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) □

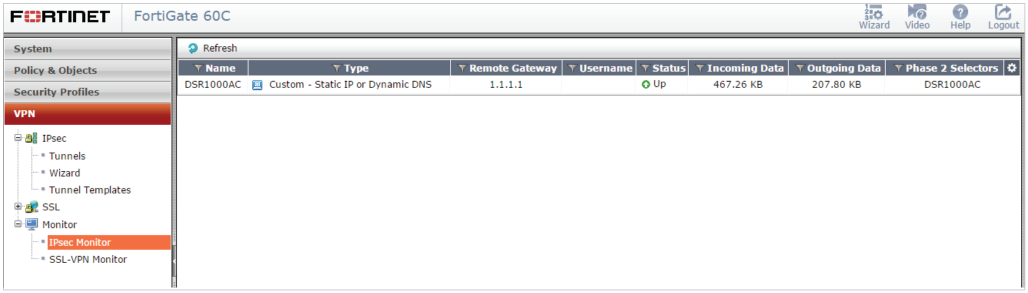
Local Port	All ☑
Remote Port	All ☑
Protocol	All ☑
Autokey Keep Alive	□

4. Set up the Firewall Policy. Navigate to: Policy & Objects > Policy > IPv4.
Press "**Create New**" button and configure the settings as below.



Seq.#	Source	Destination	Schedule	Service	Action	NAT	Application Control	SSL Inspection	Log
DSR1000AC - internal (1 - 1)									
1	DSR_LAN	Forti_LAN	always	ALL	✓ ACCEPT	Disable			UTM
internal - DSR1000AC (2 - 2)									
2	Forti_LAN	DSR_LAN	always	ALL	✓ ACCEPT	Disable			UTM
internal - wan1 (3 - 3)									
3	Forti_LAN	all	always	ALL	✓ ACCEPT	Enable			UTM
Implicit (4 - 4)									
4	all	all	always	ALL	DENY				Disable

5. Check the IPsec status. Navigate to: VPN > Monitor > IPsec Monitor.



Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2 Selectors
DSR1000AC	Custom - Static IP or Dynamic DNS	1.1.1.1		Up	467.26 KB	207.80 KB	DSR1000AC

D-Link®

Visit our website for more information
www.dlink.com