

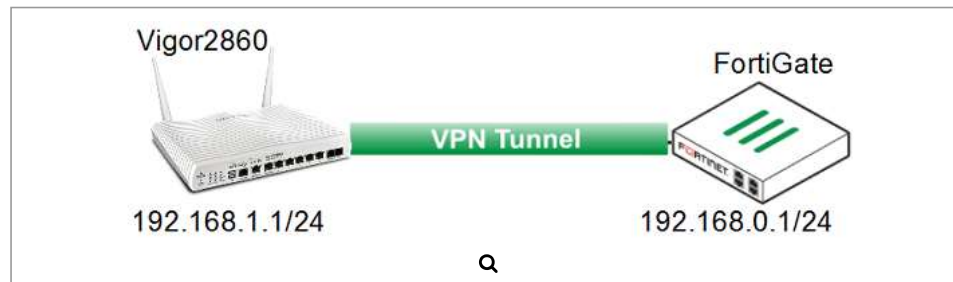
Vigor Router to FortiGate(FortiOS 5.4.0) - IPsec

Support Model :

Tags :

This note demonstrates how to establish IPsec between Vigor Router and FortiGate with FortiOS 5.4.0. We take the following network for example.

(For establishing IPsec VPN between FortiGate and Vigor3900/Vigor2960, please refer to the article [here](#))



Setting up Vigor Router

1. Go to **VPN and Remote Access >> LAN to LAN**, and click an available index. In Common settings, give a profile name and enable the profile, select "Dial-Out" as Call Direction.

The screenshot shows the configuration page for Profile Index 1. The "1. Common Settings" section is active. The "Profile Name" is set to "VPN". The "Enable this profile" checkbox is checked. The "VPN Dial-Out Through" dropdown is set to "WAN2 First". The "Netbios Naming Packet" is set to "Pass". The "Multicast via VPN" is set to "Block". The "Call Direction" is set to "Dial-Out". The "Always on" checkbox is unchecked. The "Idle Timeout" is set to 0 seconds. The "Enable PING to keep IPsec tunnel alive" checkbox is unchecked. The "PING to the IP" field is empty. A magnifying glass icon is positioned below the form.

2. In Dial-out settings,

- select "IPsec Tunnel" as Type of Server I am Calling,
- type the WAN IP of FortiGate in Server IP,
- type the Pre-shared Key,
- in IPsec Security Method, select **High(ESP) AES with Authentication** and click **Advanced**

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None	Username ??? Password(Max 15 char) PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2 VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 123.45.67.89	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key ***** <input type="radio"/> Digital Signature(X.509) Peer ID None Local ID <input type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
	IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) AES with Authentication Advanced
	Index(1-15) in Schedule Setup: / / /

Q

3. Configure Key Lifetime and Proposal of IKE phase1 and 2, and Click OK to apply

IKE advanced settings - Google Chrome

192.168.1.1/doc/I2IkeDt.htm

IKE advanced settings

IKE phase 1 mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
IKE phase 1 proposal	AES128_SHA1_G5
IKE phase 2 proposal	AES128_SHA1/AES128_MD5
IKE phase 1 key lifetime	86400 (900 ~ 86400)
IKE phase 2 key lifetime	3600 (600 ~ 86400)
Perfect Forward Secret	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Local ID	

Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote include: DES_(MD5/SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5/SHA)_G5, AES128_MD5_(G2/G5), AES256_S, AES256_SHA_G14

OK Close

Q

4. In TCP/IP Network Settings, type the LAN IP of FortiGate in Remote Network IP and Click OK to apply

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	Route
Remote Network IP	192.168.0.1	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)	
Local Network IP	192.168.1.1		
Local Network Mask	255.255.255.0		

More

OK Clear Cancel

Q

Setting up FortiGate

1. Go to VPN >> IPsec Wizard, give a name of VPN tunnel and select Custom as Template Type, then click Next >

VPN Creation Wizard

1 VPN Setup

Name

Template Type ☐ Site to Site ☐ Remote Access ☒ Custom

Q

2. In Network settings, type the WAN IP of Vigor Router in IP Address, and select the WAN interface used for VPN as Interface.

New VPN Tunnel

Name

Comments 0/255

Network

IP Version ☒ IPv4 ☐ IPv6

Remote Gateway

IP Address

Interface

Mode Config ☐

NAT Traversal ☒ Enable ☐ Disable ☐ Forced

Keepalive Frequency

Dead Peer Detection ☒ Disable ☐ On Idle ☐ On Demand

Q

3. For Authenticaion settings, type Pre-shared Key and set Key Lifetime to match the configuration on Vigor Router.

Authentication

Method

Pre-shared Key

IKE

Version ☒ 1 ☐ 2

Mode ☐ Aggressive ☒ Main (ID protection)

Phase 1 Proposal

Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="trash"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="trash"/>
Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="trash"/>
Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="trash"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="trash"/>
Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="trash"/>

Diffie-Hellman Groups ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☒ 14 ☒ 5 ☒ 2 ☐ 1

Key Lifetime (seconds)

Q

4. In Phase 2 settings, type the LAN IP of FortiGate in Local Address and the LAN IP of Vigor Router in Remote Address.

Phase 2 Selectors

Name	Local Address	Remote Address
VPN	192.168.0.0/24	192.168.1.0/24

New Phase 2

Name:

Comments:

Local Address:

Remote Address:

5. In Phase 2 Proposal setting, disable **Relay Detection** and **Perfect Forward Secrecy (PFS)**, and set Key Lifetime to match the configuration on Vigor Router. Click **OK** to finish the settings.

Advanced...

Phase 2 Proposal

Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="X"/>

Enable Replay Detection ☐

Enable Perfect Forward Secrecy (PFS) ☐

Local Port: ☒

Remote Port: ☒

Protocol: ☒

Auto-negotiate: ☐

Autokey Keep Alive: ☐

Key Lifetime:

Seconds:

6. Create an address profile for policy setting: Go to Policy & Objects >> Addresses >> Create New >> Address, give a name, type the LAN IP of Vigor Router at Subnet/ IP Range, select IPsec Tunnel we just created as Interface and click OK to apply.

New Address

Name:

Type:

Subnet / IP Range:

Interface:

Show in Address List: ☒

Static Route Configuration: ☐

Comments:

7. Create Firewall rules for VPN, Go to Policy & Objects >> IPv4 Policy >> Create New, we need to create two firewall rules in the policy: one is from Internal network segment to Remote network, another is from Remote network to Internal network. Please keep priority of the rule order in mind, because you may need to manual adjust the rule order. Usually, IPSec Traffic will be put on the top of other rules except management rule.

New Policy

Name

FortiGate to Vigor

Incoming Interface

↑

internal

Outgoing Interface

↑

VPN

Source

LAN

Destination Address

Vigor

Schedule

always

Service

ALL

Action

ACCEPT

DENY

New Policy

Name

Vigor to FortiGate

Incoming Interface

↑

VPN

Outgoing Interface

↑

internal

Source

Vigor

Destination Address

LAN

Schedule

always

Service

ALL

Action

ACCEPT

DENY

8. Create a Static Route for VPN, Go to Network >> Static Routes >> Create New, type the LAN IP of Vigor Router in Destination and Select IPsec Tunnel as Device.

New Static Route

Destination

Subnet

Named Address

Internet Service

192.168.1.0/24

Device

VPN

Administrative Distance

10

Comments

Advanced Options

OK

Cancel

Establishing the VPN

Finally, go to VPN and Remote Access >> Connection Management on Vigor Router, and select the profile we created, then click Dial.

VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

General Mode: (VPN) 31.188.214.232 Dial

Backup Mode: Dial

Q

After VPN establish successfully, we can see the status in VPN and Remote Access >> Connection Management >> VPN Connection Status of Vigor Router.

VPN Connection Status

Current Page: 1

Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1	IPsec Tunnel	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	192.168.0.1/24	3	16	3	19	0:0:30
(VPN) AES-SHA1 Auth		via WAN2						

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

Drop

Q

Was this article helpful ?

YesNo