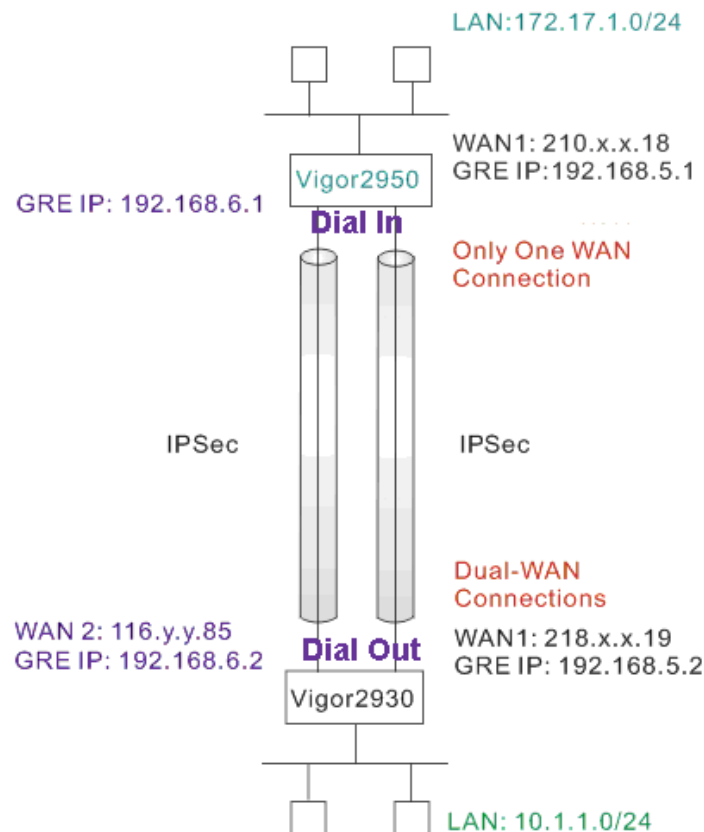


How to setup GRE over IPSec VPN for VPN Load Balance in one WAN connection (2 WAN to 1 WAN)

Suppose we have the following scenario. There is only one WAN connection for Vigor2950, while Vigor2930 has dual-WAN connection. You want to create two tunnels between Vigor2950 and Vigor2930. One tunnel is set via WAN1 connection of Vigor2930, the other is set via WAN2 connection of Vigor2930. Both are terminated to the only WAN connection on Vigor 2950 WAN1 port.



Since both Vigor2950 and Vigor2930 support VPN load balance feature, you may start the VPN from Vigor2950 to Vigor2930 or from Vigor2930 to Vigor2950. Here will introduce settings for the “Dual-WAN to One WAN” scenario (from Vigor2930 to Vigor2950).

For Vigor2930

1. Setup two IPSec LAN-to-LAN VPN profiles with Dial-Out direction.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

Index	Name	Status
<u>1.</u>	wan-1	X
<u>2.</u>	wan-2	X
<u>3.</u>	???	X
<u>4.</u>	???	X
<u>5.</u>	???	X

2. In the profile of wan-1, configure a standard IPSec connection first. Type a Pre-Shared Key. In this example, we use “test”.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: wan-1	Call Direction: <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Connection Through: WAN1 Only	Idle Timeout: 300 second(s)
Netbios Naming Packet: <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive
Multicast via VPN: <input type="radio"/> Pass <input checked="" type="radio"/> Block	PING to the IP:
(for some IGMP, IP-Camera, DHCP Relay..etc.)	

2. Dial-Out Settings

Type of Server I am calling	Link Type: 64k bps
<input type="radio"/> ISDN	Username: ???
<input type="radio"/> PPTP	Password:
<input checked="" type="radio"/> IPSec Tunnel	PPP Authentication: PAP/CHAP
<input type="radio"/> L2TP with IPSec Policy: None	VJ Compression: <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Method
210.XX.XX.18	<input checked="" type="radio"/> Pre-Shared Key
	<input checked="" type="radio"/> IKE Pre-Shared Key:
	<input type="radio"/> Digital Signature(X.509)
	Peer ID: None
	Local ID:
	<input checked="" type="radio"/> Alternative Subject Name First
	<input type="radio"/> Subject Name First
	Local Certificate: None
	IPSec Security Method
	<input type="radio"/> Medium(AH)
	<input checked="" type="radio"/> High(ESP): DES without Authentication
	<input checked="" type="button"/> Advanced

3. Then configure **GRE over IPSec** as follows:

4. GRE over IPSec Settings

<input checked="" type="checkbox"/> Enable IPSec Dial-Out function GRE over IPSec
<input type="checkbox"/> Logical Traffic
My GRE IP: 192.168.5.2
Peer GRE IP: 192.168.5.1

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:
Remote Network IP: 172.17.1.0	<input checked="" type="radio"/> Route
Remote Network Mask: 255.255.255.0	
Local Network IP: 10.1.1.0	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
Local Network Mask: 255.255.255.0	
<input type="button"/> More	

- In the profile of wan- 2, configure a standard IPSec connection first. Type a Pre-Shared Key. Note that the pre-shared key must be different from the one set in “wan -1”. In this example, we use “1234”.

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="wan-2"/> <input checked="" type="checkbox"/> Enable this profile VPN Connection Through: <input type="text" value="WAN2 Only"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
--	---

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy <input type="text" value="None"/> Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="210.XX.XX.18"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input type="text"/> <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/> IPSec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advanced"/>
--	--

- Then configure GRE over IPSec as follows:

4. GRE over IPSec Settings

<input checked="" type="checkbox"/> Enable IPSec Dial-Out function GRE over IPSec <input type="checkbox"/> Logical Traffic	My GRE IP <input type="text" value="192.168.6.2"/>	Peer GRE IP <input type="text" value="192.168.6.1"/>
---	--	--

5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="172.17.1.0"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="10.1.1.0"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="Disable"/> From first subnet to remote network, you have to do <input type="text" value="Route"/> <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	---

- Open **VPN and Remote Access >> VPN TRUNK Management** page, add these two profiles into a load balance trunk.

General Setup

Status: ☒ **Enable** ☐ **Disable**

Profile Name:

Member1:

Member2:

Attribute Mode: ☐ Backup ☒ **Load Balance**

- Press the **Add** button.

Load Balance Profile List | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disable or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1(Active)Type	Member2(Active)Type
1	v	toVigor2950	1(YES) IPSec	2(YES) IPSec

- In the VPN status page, you will find the following two connections:

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds:

General Mode:

Backup Mode:

Load Balance Mode:

VPN Connection Status

Current Page: 1 Page No. >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
1 (wan1)	IPSec Tunnel DES-No Auth	218.XX.XX.18	172.17.1.0/24	3554	17620	298	516	0:0:21 <input type="button" value="Drop"/>
1 (wan2)	IPSec Tunnel AES-SHA1 Auth	218.XX.XX.18	172.17.1.0/24	0	0	0	0	0:0:0 <input type="button" value="Drop"/>

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

For Vigor 2950,

1. Setup two IPSec LAN-to-LAN VPN profiles with Dial-In direction.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

Index	Name	Status
<u>1.</u>	VPN-IN-1	X
<u>2.</u>	VPN-IN-2	X
<u>3.</u>	???	X
<u>4.</u>	???	X
<u>5.</u>	???	X

2. In the profile of VPN-IN-1, setup a standard IPSec connection first. Enable **Specify Remote VPN Gateway** and type the IP address for Vigor2950 WAN-1 connection. Type a Pre-Shared Key. In this example, we use “test”.

3. Dial-In Settings

Allowed Dial-In Type <ul style="list-style-type: none"><input checked="" type="checkbox"/> ISDN<input checked="" type="checkbox"/> PPTP<input checked="" type="checkbox"/> IPSec Tunnel<input checked="" type="checkbox"/> L2TP with IPSec Policy None<input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway <p>Peer ISDN Number or Peer VPN Server IP <input type="text" value="218.XX.XX.19"/></p> <p>or Peer ID <input type="text"/></p>	<p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p>IKE Authentication Method</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Pre-Shared Key<input type="checkbox"/> Digital Signature(X.509) <p>IKE Pre-Shared Key <input type="text" value="●●●●●●"/></p> <p>Peer ID None</p> <p>Local ID</p> <ul style="list-style-type: none"><input checked="" type="radio"/> Alternative Subject Name First<input type="radio"/> Subject Name First <p>IPSec Security Method</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Medium (AH)High (ESP)<ul style="list-style-type: none"><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
--	---

- Then configure GRE over IPSec as follows. For Dial-In VPN connection, you don't need to tick **Enable IPSec Dial-Out function GRE over IPSec**.

4. GRE over IPSec Settings

<input type="checkbox"/> Enable IPSec Dial-Out function GRE over IPSec	
<input type="checkbox"/> Logical Traffic	My GRE IP <input type="text" value="192.168.5.1"/> Peer GRE IP <input type="text" value="192.168.5.2"/>

5. TCP/IP Network Settings

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	<input type="text" value="Disable"/>
Remote Gateway IP	<input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do	
Remote Network IP	<input type="text" value="10.1.1.0"/>	<input type="text" value="Route"/>	
Remote Network Mask	<input type="text" value="255.255.255.0"/>		
<input type="button" value="More"/>		<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	

- In the profile of VPN-IN-2, also setup a standard IPSec connection first. Enable **Specify Remote VPN Gateway** and type the IP address for Vigor2950 WAN-2 connection. Type "1234" as pre-shared key.

<h3>3. Dial-In Settings</h3> <h4>Allowed Dial-In Type</h4> <div> <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input checked="" type="checkbox"/> L2TP with IPSec Policy <input type="text" value="None"/> </div> <div> <input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="116.233.153.85"/> or Peer ID <input type="text"/> </div>		<div> Username <input type="text"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off </div> <h4>IKE Authentication Method</h4> <div> <input checked="" type="checkbox"/> Pre-Shared Key <input type="button" value="IKE Pre-Shared Key"/> <input type="text" value="••••••"/> <input type="checkbox"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First </div> <h4>IPSec Security Method</h4> <div> <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES </div>
---	--	--

- Then, configure GRE over IPsec as follows. For Dial-In VPN connection, you don't need to tick **Enable IPsec Dial-Out function GRE over IPsec**.

4. GRE over IPsec Settings

☐ Enable IPsec Dial-Out function GRE over IPsec
☐ Logical Traffic

My GRE IP
 Peer GRE IP

5. TCP/IP Network Settings

My WAN IP
 Remote Gateway IP
 Remote Network IP
 Remote Network Mask

RIP Direction
 From first subnet to remote network, you have to do

☐ Change default route to this VPN tunnel (Only single WAN supports this)

- VPN Load Balance can be applied just for Dial-out VPN profiles, therefore you don't need to set the load balance policy for Dial-In site.
- In the VPN status page, you will find the following two connections:

VPN and Remote Access >> Connection Management

Dial-out Tool
Refresh Seconds :

General Mode:
 Backup Mode:
 Load Balance Mode:

VPN Connection Status
Page No. >>"/>

Current Page: 1

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime	
1 (VPN-IN-1)	IPsec Tunnel DES-No Auth	218.0.1.1	10.1.1.0/24	0	0	1	3	0:0:7	<input type="button" value="Drop"/>
2 (VPN-IN-2)	IPsec Tunnel AES-SHA1 Auth	116.2.1.1	10.1.1.0/24	195	3	91	3	45:38:56	<input type="button" value="Drop"/>