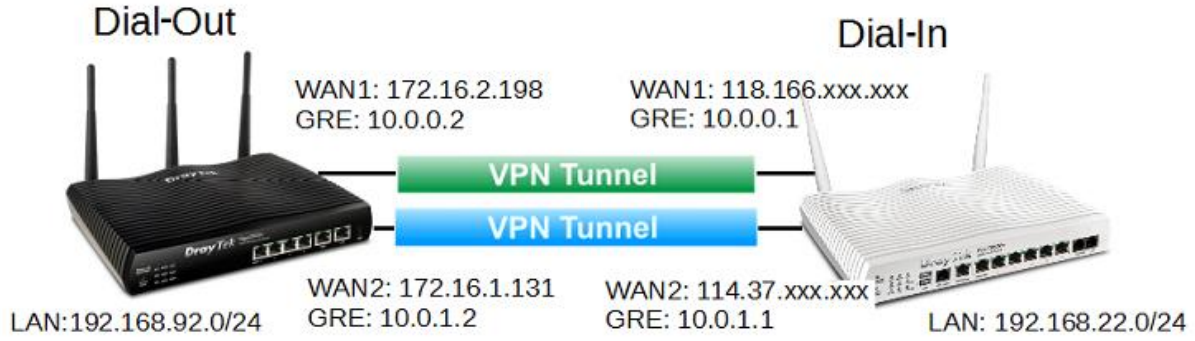


LOAD BALANCING İÇİN 2 IPSEC VPN KURULUMU

Birden çok WAN arabirimine sahip routerlar için VPN trunk, aynı remote networke yönlendirilmiş iki VPN bağlantısının ve VPN trafiğinin iki bağlantı arasında dengeli olmasını sağlar. Bu makalede, iki Vigor Router arasında iki IPsec VPN'in nasıl kurulacağı ve load balancing için VPN trunk'ın nasıl kurulacağı gösterilecektir.

DrayOS



1. VPN Server'da (Dial-In Site) bir IPsec VPN profili oluşturun. GRE Settings'de, "Enable IPsec Dial-Out function GRE over IPsec" seçeneğini etkinleştirin ve **My GRE IP** ve **Peer GRE IP** için IP adresi girin.

3. Dial-In Settings	
Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None <input type="checkbox"/> SSL Tunnel <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None <input type="text"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
4. GRE 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="10.0.0.1"/> Peer GRE IP <input type="text" value="10.0.0.2"/>	
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="192.168.92.1"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.22.1"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction Disable From first subnet to remote network, you have to do <input type="button" value="Route"/> <input type="checkbox"/> IPsec VPN with the Same Subnets <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
<input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

2. VPN Server’da **My GRE IP** ve **Peer GRE IP**’lerinin farklı olması dışında, hemen hemen aynı yapılandırmaya sahip başka bir IPsec VPN profili oluşturun .

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None <input type="checkbox"/> SSL Tunnel <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None ▼ Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
--	---

4. GRE 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="10.0.1.1"/> Peer GRE IP <input type="text" value="10.0.1.2"/>
---	---

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="192.168.92.1"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.22.1"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction Disable ▼ From first subnet to remote network, you have to do <input type="button" value="Route"/> ▼ <input type="checkbox"/> IPsec VPN with the Same Subnets <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	---

OK Clear Cancel

3. VPN Client’da (Dial-Out Site), bir IPsec VPN profili oluşturun. GRE Settings’de "Enable IPsec Dial-Out function GRE over IPsec" seçeneğini etkinleştirin ve VPN Server’ın “Peer GRE IP” sini ilk istemcisinin **MY GRE IP**’si, istemcisinin **Peer GRE IP**’sini Server’ın “My GRE IP”si olarak girin.

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None <input type="checkbox"/> SSL Tunnel <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
--	--

4. GRE 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="10.0.0.1"/>	Peer GRE IP <input type="text" value="10.0.0.2"/>
---	---	---

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="192.168.92.1"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.22.1"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction Disable From first subnet to remote network, you have to do <input type="button" value="Route"/> <input type="checkbox"/> IPsec VPN with the Same Subnets <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	---

4. Benzer şekilde, **My GRE IP**'sinin Sunucunun ikinci profilinin "Peer GRE IP" olması ve **Peer GRE IP**'nin de aynı profildeki "My GRE IP" olması dışında, hemen hemen aynı yapılandırmaya sahip başka bir IPsec VPN profili oluşturun.

4. GRE 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="10.0.0.2"/>	Peer GRE IP <input type="text" value="10.0.0.1"/>
---	---	---

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="192.168.22.1"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.92.1"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction Disable From first subnet to remote network, you have to do <input type="button" value="Route"/> <input type="checkbox"/> IPsec VPN with the Same Subnets <input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)
---	---

5. 4 tane IPsec VPN Profili oluşturduktan sonra, VPN Client'inde **VPN and Remote Access >> VPN TRUNK Management >> General Setup** sayfasına gidin.
- Profil adı girin ve profili etkinleştirin.
 - Member 1 ve Member 2 VPN load balance için oluşturulan VPN profillerini seçin.

- Active Mode olarak Load Balance'yi seçin ve Add'e tıklayın.
- VPN istemcisinde VPN trunk ayarlarını girin.

General Setup

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Profile Name	loadbalance			
Member1	1	out1	IPsec	118.166.1.1 (192.168.22.1)
Member2	2	out2	IPsec	114.37.1.1 (192.168.22.1)
Active Mode	<input type="radio"/> Backup <input checked="" type="radio"/> Load Balance			

Add Update Delete

Şimdi VPN trunk kurulduktan sonraki VPN durumunu ve trafiği VPN and Remote Access >> Connection Management sayfasından görebilirsiniz.

VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

General Mode:		Dial
Backup Mode:		Dial
Load Balance Mode:	(loadbalance) 118.166.1.1	Dial

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	114.37.1.1	192.168.22.1/24	42	3	552	11	0:7:15
(out2)	AES-SHA1 Auth	via WAN2						
2	IPsec Tunnel	118.166.1.1	192.168.22.1/24	1603	84	371	9	0:7:13
(out1)	AES-SHA1 Auth	via WAN1						

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

VPN load balance algoritması default olarak Round Robin'dir. Detaylı load balance policy için örneğin weight, source IP, destination IP veya destination portları gibi gelişmiş ayarları VPN TRUNK Management >> Load Balance Profile List sayfasına giderek yapılandırabilirsiniz.

Load Balance Profile List

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

No.	Status	Name	Member1 (Active)Type	Member2 (Active)Type
1	x	loadbalance	15 (NO) PPTP	14 (NO) PPTP

Advanced loadbalance

VPN Load Balance Advance Settings

Profile Name: loadbalance

Load Balance Algorithm: ☒ Round Robin ☐ Weighted Round Robin ☐ Auto Weighted ☐ According to Speed Ratio (Member1:Member2): 90:10

VPN Load Balance Policy

Tunnel Bind Table Index: (1~128)

Active: ☒ Edit ☐ Insert after

Binding Dial Out Profile: 15

Src IP Start: 0.0.0.0 End: 255.255.255.255

Dest IP Start: 0.0.0.0 End: 255.255.255.255

Dest Port Start: 1 End: 65535

Protocol: ANY 0

OK Close

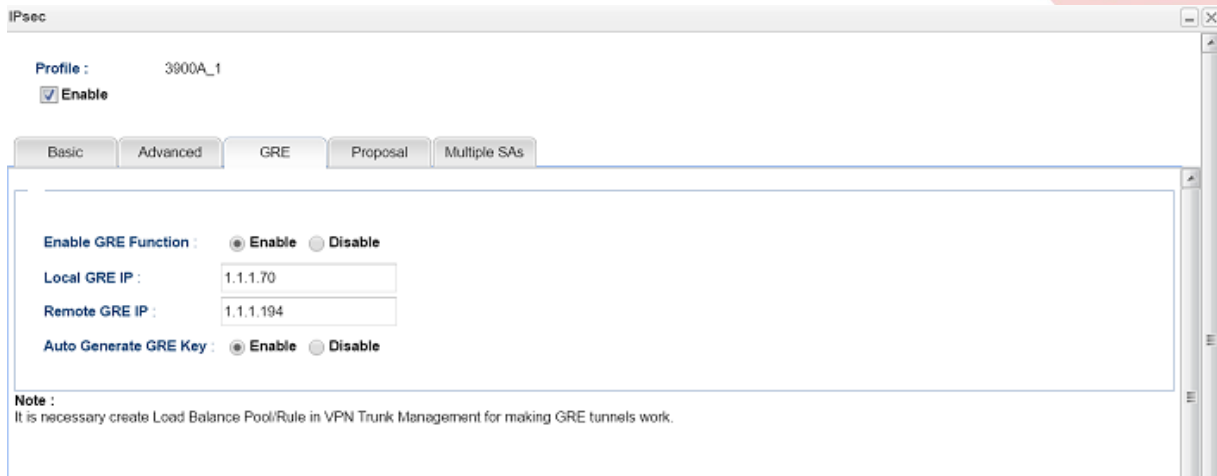
Detail Information

[VPN Load Balance Profile name: loadbalance]
[Algorithm: Round Robin]

Linux

VPN Server Konfigürasyonu (Dial-In)

1. VPN Server’da ilk IPsec VPN profilini oluřturun. Basic Sekmede:
 - a. **Enable**’yi etkinleřtirin.
 - b. **Dial-Out Through** için “WAN 1” seeneęini sein.
 - c. **Local IP/ Subnet Mask**’ı routerın LAN IP’si olarak girin.
 - d. **Remote Host IP**’de VPN istemcisinin WAN 1 IP’sini girin.
 - e.
2. GRE sekmesine gidin:
 - a. **GRE Function**’u etkinleřtirin.
 - b. **Local GRE IP**’yi örneęin 1.1.1.70 olarak ayarlayın. (Bu VPN istemcisindeki Remote GRE IP olmalıdır.)
 - c. **Remote GRE IP**’yi örneęin 1.1.1.194 olarak ayarlayın. (Bu VPN istemcisindeki Local GRE IP olmalıdır.)



IPsec

Profile : 3900A_1

☒ Enable

Basic Advanced GRE Proposal Multiple SAs

Enable GRE Function : ☒ Enable ☐ Disable

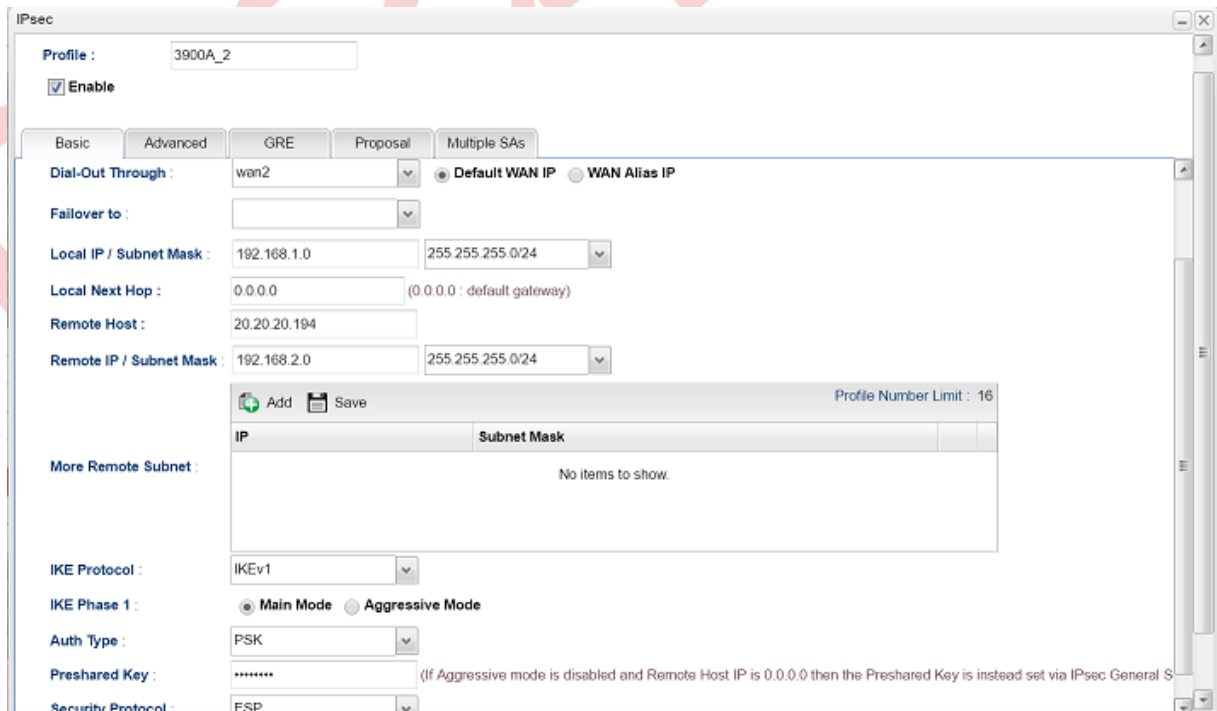
Local GRE IP : 1.1.1.70

Remote GRE IP : 1.1.1.194

Auto Generate GRE Key : ☒ Enable ☐ Disable

Note :
It is necessary create Load Balance Pool/Rule in VPN Trunk Management for making GRE tunnels work.

3. Benzer řekilde, bařka bir IPsec profili oluřturun, ancak **Dial-Out Through** için “WAN 2” yi sein. **Remote Host IP**’ye VPN istemcisinin WAN 2 IP’sini girin.



IPsec

Profile : 3900A_2

☒ Enable

Basic Advanced GRE Proposal Multiple SAs

Dial-Out Through : wan2 ☒ Default WAN IP ☐ WAN Alias IP

Failover to :

Local IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 20.20.20.194

Remote IP / Subnet Mask : 192.168.2.0 255.255.255.0/24

Add Save Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

More Remote Subnet :

IKE Protocol : IKEv1

IKE Phase 1 : ☒ Main Mode ☐ Aggressive Mode

Auth Type : PSK

Preshared Key : ***** (If Aggressive mode is disabled and Remote Host IP is 0.0.0.0 then the Preshared Key is instead set via IPsec General S

Security Protocol : ESP

4. GRE sekmesine gidin. GRE Function'ı etkinleştirin. Farklı bir **Local GRE IP**'si girin, örneğin 2.2.2.70 ve farklı bir **Remote GRE IP**'si, örneğin 2.2.2.194. GRE IP'yi aklınızda bulundurun, çünkü VPN istemcisinin eşleşme ayarlarına sahip olması gerekecektir.

IPsec

Profile : 3900A_2

☒ Enable

Basic Advanced GRE Proposal Multiple SAs

Enable GRE Function : ☒ Enable ☐ Disable

Local GRE IP : 2.2.2.70

Remote GRE IP : 2.2.2.194

Auto Generate GRE Key : ☒ Enable ☐ Disable

Note :
It is necessary create Load Balance Pool/Rule in VPN Trunk Management for making GRE tunnels work.

5. Yeni bir havuz eklemek için **VPN and Remote Access >> VPN TRUNK Management >> Load Balance Pool**'a gidin.
- Profile name** girin.
 - Mode** için "Load Balance" seçeneğini seçin.
 - Interface**'de iki tane VPN profili ekleyin. (Not: Yalnızca GRE işlevinin etkin olduğu IPsec profilleri burada listelenir.)

VPN and Remote Access >> VPN TRUNK Management >> Load Balance Pool

Load Balance Pool Load Balance Rule

Add Edit Delete Refresh

Load Balance Pool

Profile : To3900B

Mode : Load Balance

Add Save Profile Number Limit : 16

Interface	Weight
3900A_1	1
3900A_2	1

Interface :

Note :
1. Only the VPN profiles with GRE function enabled will be listed and selected as Interface setting.
2. If there is nothing displayed, please go to VPN and Remote Access >> VPN Profiles to create a new VPN profile with GRE function enabled first.

6. Yeni kural eklemek için **VPN and Remote Access >> VPN TRUNK Management >> Load Balance Rule**'a gidin.
- Enable**'yi işaretleyin.
 - Protocol** için "ALL" seçeneğini seçin.

- c. **Source IP Address** ve **Subnet Mask**'ı routerın LAN ağı olarak ayarlayın.
- d. **Destination IP Address** ve **Subnet Mask**'ı VPN istemcisinin LAN ağı olarak ayarlayın.
- e. **Load Balance Pool** için önceki adımda oluşturulan profili seçin.

The screenshot shows the 'Load Balance Rule' configuration window. The 'Profile' is set to 'AtoB'. The 'Enable' checkbox is checked. The 'Protocol' is set to 'ALL'. The 'Source IP Address' is '192.168.1.0' (Optional). The 'Source Mask' is '255.255.255.0/24' (Optional). The 'Destination IP Address' is '192.168.2.0' (Optional). The 'Destination Mask' is '255.255.255.0/24' (Optional). The 'Load Balance Pool' is set to 'To3900B'. The 'Apply' button is highlighted.

VPN Client Konfigürasyonu (Dial-Out)

1. VPN Client'da ilk IPsec VPN profilini oluşturun. Basic Sekmede:
 - a. Enable'yi işaretleyin.
 - b. **Dial-Out Through** için "WAN 1" seçeneğini seçin.
 - c. **Local IP/ Subnet Mask**'ı routerın LAN IP'si olarak ayarlayın.
 - d. **Remote Host IP**'de VPN sunucusunun WAN 1 IP'sini girin.
 - e. **Remote IP/ Subnet Mask**'ı VPN sunucusunun LAN IP'si olarak ayarlayın.
 - f. **Auth Type** için PSK seçeneğini seçin ve VPN sunucusunun ilk IPsec profilinde ayarlanan **Preshared Key**'i girin.

The screenshot shows the 'IPsec' configuration window, Basic tab. The 'Profile' is '3900B_1'. The 'Enable' checkbox is checked. The 'Auto Dial-Out' is set to 'Enable'. The 'Dial-Out Through' is set to 'wan1'. The 'Local IP / Subnet Mask' is '192.168.2.0 / 255.255.255.0/24'. The 'Local Next Hop' is '0.0.0.0'. The 'Remote Host' is '10.10.10.70'. The 'Remote IP / Subnet Mask' is '192.168.1.0 / 255.255.255.0/24'. The 'Auth Type' is 'PSK'. The 'Preshared Key' is '*****'. The 'Security Protocol' is 'ESP'. The 'Profile Number Limit' is 16.

2. GRE sekmesine gidin.
 - a. GRE Function'u etkinleştirin.
 - b. **Local GRE IP**'yi 1.1.1.194 olarak ayarlayın.
 - c. **Remote GRE IP**'yi 1.1.1.70 olarak ayarlayın.

IPsec

Profile : 3900B_1

☒ Enable

Basic Advanced GRE Proposal Multiple SAs

Enable GRE Function : ☒ Enable ☐ Disable

Local GRE IP : 1.1.1.194

Remote GRE IP : 1.1.1.70

Auto Generate GRE Key : ☒ Enable ☐ Disable

Note :
It is necessary create Load Balance Pool/Rule in VPN Trunk Management for making GRE tunnels work.

3. VPN sunucusunun aynı ağında başka bir IPsec VPN profili oluşturun, ancak **Dial-Out Through** için WAN 2'yi seçin ve **Remote Host**'da VPN Server'ın WAN 2 IP'sini girin. **Preshared Key** VPN sunucusunun ikinci IPsec profilinde ayarlarına uygun olmalıdır.

IPsec

Profile : 3900B_2

☒ Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out : ☒ Enable ☐ Disable Always Dial-Out

For Remote Dial-In User : ☐ Enable ☒ Disable

Dial-Out Through : wan2 ☐ Default WAN IP ☐ WAN Alias IP

Fallover to :

Local IP / Subnet Mask : 192.168.2.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 20.20.20.70

Remote IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

More Remote Subnet :
No items to show.

IKE Protocol : IKEv1

IKE Phase 1 : ☒ Main Mode ☐ Aggressive Mode

Auth Type : PSK

Preshared Key : (If Aggressive mode is disabled and Remote Host IP is 0.0.0.0 then the Preshared Key is instead set via IPsec General Setup. Max 40 characters.)

Security Protocol : ESP

4. GRE sekmesine gidin. GRE function'u etkinleştirin. **Local GRE IP** için 2.2.2.194 ve **Remote GRE IP** için 2.2.2.70 girin.

IPsec

Profile : 3900B_2

☒ Enable

Basic Advanced GRE Proposal Multiple SAs

Enable GRE Function : ☒ Enable ☐ Disable

Local GRE IP : 2.2.2.194

Remote GRE IP : 2.2.2.70

Auto Generate GRE Key : ☒ Enable ☐ Disable

Note :
It is necessary create Load Balance Pool/Rule in VPN Trunk Management for making GRE tunnels work.

5. Benzer şekilde, 2 IPsec VPN profili için yeni bir havuz eklemek için **VPN and Remote Access >> VPN TRUNK Management >> Load Balance Pool**'a gidin.

Load Balance Pool

Profile : To3900A

Mode : Load Balance

Add Save Profile Number Limit : 16

Interface	Weight
3900B_1	1
3900B_2	1

Interface :

Note :
 1. Only the VPN profiles with GRE function enabled will be listed and selected as Interface setting.
 2. If there is nothing displayed, please go to VPN and Remote Access >> VPN Profiles to create a new VPN profile with GRE function enabled first.

Apply Cancel

6. Benzer şekilde, **Load Balance Rule**'agidin ve oluşturulan Load Balance Pool için bir kural oluşturun.

Load Balance Rule

Profile : BtoA

☒ Enable

Protocol : ALL

Source IP Address : 192.168.2.0 (Optional)

Source Mask : 255.255.255.0/24 (Optional)

Destination IP Address : 192.168.1.0 (Optional)

Destination Mask : 255.255.255.0/24 (Optional)

Load Balance Pool : To3900A

Apply Cancel

7. Ayarları tamamladıktan sonra, iki IPsec VPN tüneli aynı anda çevrimiçi olmalıdır. **Connection Management** sayfasından 2 VPN'in durumunu da görebilirsiniz.

VPN and Remote Access >> Connection Management >> Connection Management

Connection Management History

Dial-Out tool

☒ IPsec ☐ PPTP Profiles : Connect Refresh

Green :Data is encrypted.
White :Data isn't encrypted.

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Netw...	Up Time	RX(Packets)	TX(Packets)	Operation
1 3900A_2	IPsec/3DES...	wan2	20.20.20.194	2.2.2.194/32	00:02:41	15	15	
2 3900A_1	IPsec/3DES...	wan1	10.10.10.194	1.1.1.194/32	00:03:06	4	4	