

AYNI IP SUBNET'İNİ KULLANAN İKİ VIGOR ROUTER ARASINDA IPSEC TUNNEL

Bu makalede, aynı yerel IP aralığını kullanan iki Vigor Router arasında LAN-to-LAN VPN'in nasıl yapılandırılacağı gösterilmektedir. VPN tünellerini aynı IP aralığını kullanan başka bir routera inşa etmenin sorunu, aynı IP subnette birbiriyle çakışan iki yol olacaktır. Hiçbiri IP subnetini değiştiremezse, çözüm yerel IP'yi VPN bağlantısı için kullanılmamış bir aralığa çevirmektir. Aşağıda Vigor Router'larda bunun nasıl yapılacağı açıklanmaktadır.

DrayOS

Router A'nın Yapılandırması (VPN Server)

1. Aşağıdaki şekilde bir VPN profili oluşturmak için **VPN and Remote Access >> LAN to LAN** sayfasına gidin. Common settings'de:

- **Enable this profile**'i etkinleştirin.
- **Call Direction** için Dial-In seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name branch1	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through WAN1 First	Idle Timeout 0 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 (for some IGMP,IP-Camera,DHCP Relay..etc.)	PING to the IP

2. DialIn settings'de:

- **Allowed Dial-in Type** için IPsec Tunnel'i seçin.
- Specify Remote VPN Gateway'i seçin ardından **Peer ID** için bazı dizeler girin.
- **IKE Pre-Shared Key**'i tıklayın sonra Pre-Shared Key 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	Username ???
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP or Peer ID branch1	Password(Max 11 char)
	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="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

3. TCP/IP Network Settings:

- **IPsec VPN with the Same Subnets**'i etkinleştirin.
- **Translated Type** için Whole Subnet'i seçin.
(Not: "Whole Subnet" routerın tüm ağ IP Adresini otomatik olarak çevireceği anlamına gelir. Örneğin, Local IP 192.169.1.10 192.168.11.10 'a, Local IP 192.168.1.11, 192.168.11.11'e vb. dönüştürülecektir. "Specific IP Address" routerın yalnızca Ağ Yöneticisinin Virtual IP Mapping tablosuna elle eklediği IP Adresini çevireceği anlamına gelir.)
- Kullanılmayan bir IP aralığı olarak **Remote Network IP** girin. (Router B'de kullanılacak olan Translated Network IP'sidir.)
- **Translated Local Network IP** için başka bir kullanılmamış IP aralığı girin.
- Kaydetmek için **OK**'atıklayın.

5. TCP/IP Network Settings

Remote Network IP	192.168.11.0 c	From Local Subnet to Remote network, you have to do
Remote Network Mask	255.255.255.0	
<input checked="" type="checkbox"/> Translated Local Network	LAN1 to	a Route ▾
	192.168.129.0 d	<input checked="" type="checkbox"/> IPsec VPN with the Same Subnets
<input type="button" value="Advanced"/>		Translated Type <input checked="" type="radio"/> Whole Subnet b
		<input type="radio"/> Specific IP Address
		<input type="button" value="Virtual IP Mapping"/>

Router B'nin Yapılandırması (VPN Client)

1. **VPN and Remote Access >> LAN to LAN** sayfasına giderek aşağıdaki gibi profil ekleyin. Common Settings'de:
 - **Enable this profile**'i etkinleştirin.
 - **Call Direction** için Dial-Out seçin.
 - **VPN Dial-Out Through** Router A'nın WAN Interface'sini seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name	toHQ	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 checked="" type="checkbox"/> Always on	
VPN Dial-Out Through	WAN1 First	Idle Timeout	-1 second(s)
	1-111.111.111.111	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive	
Netbios Naming Packet	<input checked="" type="radio"/> Pass <input type="radio"/> Block	PING to the IP	
Multicast via VPN	<input type="radio"/> Pass <input checked="" type="radio"/> Block		
(for some IGMP,IP-Camera,DHCP Relay..etc.)			

2. Dial-Out Settings'de yapılandırma:

- **Type of Server I am calling** için "IPsec Tunnel"i seçin.
- Router A'nın WAN IP'sini **Server IP**'ye girin.
- Router A'nın konfigürasyonunda girin **IKE Pre-Shared Key** değerinin aynısını girin.
- **IPsec Security Method** için High(ESP) seçin ve **Advanced**'e tıklayın.
- **"Aggressive mode"** seçin.

- Router A'daki Peer ID'yi **Local ID**'ye girin.

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 <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="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) <input type="text" value="220.132.88.33"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key <input checked="" type="radio"/> IKE Pre-Shared Key <input type="text" value="....."/> <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 type="button" value="Advanced"/>

3. TCP/IP Network Settings yapılandırma:

- **IPsec with the Same Subnets**'i etkinleştirin.
- **Translated Type** için Whole Subnet'i seçin.
- Router A'da Local IP dönüşümünü **Remote Network IP** olarak girin.
- **Translated Local Network IP**'yi girin. (Router A'da Remote Network IP'deki yapılandırmanın aynı olmalıdır.)
- Konfigurasyonu kaydetmek için **OK**'a tıklayın.

5. TCP/IP Network Settings

Remote Network IP <input type="text" value="192.168.129.0"/> c Remote Network Mask <input type="text" value="255.255.255.0"/> <input checked="" type="checkbox"/> Translated Local Network LAN1 ▼ to <input type="text" value="192.168.11.0"/> d <input type="button" value="Advanced"/>	From Local Subnet to Remote network, you have to do <input checked="" type="checkbox"/> a Route ▼ <input checked="" type="checkbox"/> IPsec VPN with the Same Subnets Translated Type <input checked="" type="radio"/> Whole Subnet b <input type="radio"/> Specific IP Address <input type="button" value="Virtual IP Mapping"/>
---	--

4. Yapılandırmalardan sonra, Ağ Yöneticisi VPN Durumunu **VPN and Remote Access >> Connection Management** sayfasından kontrol edebilir.

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 (toHQ)	IPsec Tunnel DES-No Auth	220.132.88.33 via WAN1	192.168.129.0/24	4	3	7	3	0:4:35 <input type="button" value="Drop"/>

5. Router A'nın arkasındaki bir ana bilgisayara ulaşmak için Router B'nin arkasındaki bir Host IP adresini 192.168.129.0/255.255.255.0 subnette kullanabilir.

```
Pinging 192.168.129.10 with 32 bytes of data:
Reply from 192.168.129.10: bytes=32 time=31ms TTL=126
Reply from 192.168.129.10: bytes=32 time=78ms TTL=126
Reply from 192.168.129.10: bytes=32 time=30ms TTL=126
Reply from 192.168.129.10: bytes=32 time=31ms TTL=126
```

Linux

1. **VPN and Remote Access >> VPN Profile >> IPsec**'e gidin aşağıdaki gibi bir profil oluşturun.
- Basic sekmesinde **profil adı** girin ve **Enable**'yi etkinleştirin.
 - Router A'nın LAN Network'ünü **Local IP /Subnet Mask**'a girin.
 - **Remote Host**'da Router B'nin WAN IP'sini girin.
 - **Remote IP/ Subnet Mask**'da Router B'nin translated LAN IP'sini girin.
 - **Pre-Shared Key** girin.

2. Advanced sekmesinde, **Apply NAT Policy** için Enable seçin ve **Translated Local Network** için kullanılmayan bir IP aralığı girin. Ardından profili kaydetmek için **Apply**'a tıklayın.

IPsec

Profile : branch2

Enable

Basic Advanced GRE Proposal

Phase1 Key Life Time : 28800

Phase2 Key Life Time : 3600

Perfect Forward Secrecy Status : Enable Disable

Dead Peer Detection Status : Enable Disable

DPD Delay : 30

DPD Timeout : 120

Ping to Keep Alive : Enable Disable

Route / NAT Mode : Route

Source IP : auto_detect_srcip

Apply NAT Policy : Enable Disable

Translated Local Network : 192.168.11.0 255.255.255.0/24

Netbios Naming Packet : Enable Disable

Multicast via VPN : Enable Disable

Router B'nin Yapılandırması (VPN Client)

3. Benzer şekilde, **VPN and Remote Access >> VPN Profile >> IPsec**'e gidin ve aşağıdaki gibi bir profil ekleyin:
- Basic sekmesinde, **Profil adı** girin ve **Enable**'yi etkinleştirin.
 - Router B'nin LAN Network'ünü **Local IP /Subnet Mask**'a girin.
 - **Remote Host**'da Router A'nın WAN IP'sini girin.
 - **Remote IP/ Subnet Mask**'da Router A'nın translated LAN IP'sini girin.
 - Router A'nın VPN profilinde girilen **Pre-Shared Key** değerini girin.

IPsec

Profile : branch1

Enable

Basic Advanced GRE Proposal

Local IP / Subnet : 192.168.1.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 100.100.100.100

Remote IP / Subnet : 192.168.11.0 255.255.255.0/24

Add Save

IP	Subnet Mask
No items to show.	

More Remote Subnet :

IKE Phase 1 : Main Mode Aggressive Mode

Auth Type : PSK

Preshared Key :

Security Protocol : ESP

4. Advanced sekmesinde, **Apply NAT Policy** için Enable seçin ve Router A'ninkinden farklı bir Translated Local Network verin. Ardından, profili kaydetmek için **Apply**'a tıklayın.

IPsec

Profile : branch1

Enable

Basic Advanced GRE Proposal

Phase1 Key Life Time : 28800

Phase2 Key Life Time : 3600

Perfect Forward Secrecy Status : Enable Disable

Dead Peer Detection Status : Enable Disable

DPD Delay : 30

DPD Timeout : 120

Ping to Keep Alive : Enable Disable

Route / NAT Mode : Route

Source IP : auto_detect_srcip

Apply NAT Policy : Enable Disable

Translated Local Network : 192.168.21.0 255.255.255.0/24

Netbios Naming Packet : Enable Disable

Multicast via VPN : Enable Disable

5. VPN'i başlatmak için **VPN and Remote Access >> Connection Management**'a gidin, oluşturulan Profili seçin ve **Connect**'e tıklayın.

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

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles : branch2

Refresh Auto Refresh : 1 Minute

6. Tüm ayarlar eşleşirse, VPN bağlantısı kurulur. Bağlantı durumunda, Virtual ağın translated IP adresi olduğunu göreceğiz.

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

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles :

Refresh Auto Refresh : 1 Minute

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX	
1	branch2	IPsec/3DES...	wan1	200.200.200	192.168.21.0/24	00:00:31	176(bps)	336(bps)	240(Byte)	44

7. Artık uzaktaki ağı translated IP adresinden erişebiliyoruz.

```
Diagnosics >> Ping/Trace Route

Ping/Trace Route

PING 192.168.21.1 (192.168.21.1) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.21.1: icmp_seq=0 ttl=64 time=29.4 ms
64 bytes from 192.168.21.1: icmp_seq=1 ttl=64 time=28.6 ms
64 bytes from 192.168.21.1: icmp_seq=3 ttl=64 time=28.8 ms
64 bytes from 192.168.21.1: icmp_seq=4 ttl=64 time=28.7 ms

--- 192.168.21.1 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 28.6/28.8/29.4 ms
Send ICMP_ECHO_REQUEST packets done.
```