

## CISCO RV SERİLERİ VE DRAYTEK ARASINDA IPSEC VPN

Bu makale, Cisco RV Router ve DrayTek Router arasında IPsec LAN to LAN VPN'inin nasıl oluşturulacağını göstermektedir.

### Cisco RV Router Ayarları

Vigor Router için VPN >> Gateway to Gateway sayfasında bir VPN profili oluşturun.

- Interface için Vigor Router'ın olduğu **Interface**'i seçin
- **Keying Mode** için IKE with Preshared key seçeneğini seçin.
- Local Group Setup'da Vigor Router'a bağlamak istediğiniz Cisco RV Router'ın local IP Subnet'ini girin.

- Remote Group Setup'da **Remote Security Gateway Type** için "IP Only" kullanın ve **IP Address** için Vigor Router'ın WAN IP'sini girin.
- **IP Address** ve **Subnet Mask** için Vigor Router'ın LAN IP Subnet'ini girin.
- Kullanmak istediğiniz IPsec kurulumunu seçin, bu örnekte **IKE phase1** için AES256\_SHA1\_G5 ve **IKE phase2** için AES256\_SHA1, Perfect Forward Secret olmadan kullanıyoruz ve **Preshared Key** 12345678'dir.

## DrayTek Router Ayarları

## DrayOS

1. **VPN and Remote Access >> LAN to LAN** sayfasına gidin ve uygun bir indexe tıklayın.
  - o Profile Name girin.
  - o Enable the profile etkinleştirin.
  - o Call Direction için "Dial-Out" seçeneğini seçin.

## VPN and Remote Access &gt;&gt; LAN to LAN

Profile Index : 4

## 1. Common Settings

Profile Name <input type="text" value="Cisco"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	Tunnel Mode <input type="radio"/> GRE Tunnel
VPN Dial-Out Through	<input type="checkbox"/> Always on
<input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="0"/> second(s)
<input type="text" value="1-1-1-1.1.1.1"/>	<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 <input type="text"/>
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block	
(for some IGMP,IP-Camera,DHCP Relay..etc.)	

- o Dial-Out Settings'de "IPsec Tunnel" seçeneğini seçin.
- o **Server IP/Host Name** için Cisco Router'ın WAN IP'sini ya da domain adını girin.
- o Cisco Router'da yapılandırılan Preshared Key'i girin.
- o **IPsec Security Method** için High (ESP)'de AES with authentication seçeneğini seçin ve **Advanced**'de tıklayın.

## 2. Dial-Out Settings

Type of Server I am calling	Username <input <="" td="" type="text" value="???"/>
<input type="radio"/> PPTP	Password(Max 15 char) <input type="text"/>
<input checked="" type="radio"/> IPsec Tunnel	PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/>
<input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="radio"/> SSL Tunnel	
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	<b>IKE Authentication Method</b>
<input type="text" value="WAN IP of Cisco router"/>	<input checked="" type="radio"/> Pre-Shared Key
Server Port (for SSL Tunnel): <input type="text" value="443"/>	IKE Pre-Shared Key <input type="text" value="*****"/>
	<input type="radio"/> 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
	Local Certificate <input type="text" value="None"/>
	<b>IPsec Security Method</b>
	<input type="radio"/> Medium(AH)
	<input checked="" type="radio"/> High(ESP) <input type="text" value="AES with Authentication"/>
	<b>Advanced</b>
	Index(1-15) in <u>Schedule</u> Setup:
	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

- Cisco Router'daki IPsec ayarlarını eşleştirin.

**IKE advanced settings**

IKE phase 1 mode(IKEv1)	<input checked="" type="radio"/> Main mode	<input type="radio"/> Aggressive mode
IKE phase 1 proposal	Auto	
IKE phase 2 proposal	AES128_SHA1_MD5_SHA256	
IKE phase 1 key lifetime	28800	(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 site. The proposals include: DES\_(MD5/SHA)\_G1, 3DES\_MD5\_G1, 3DES\_MD5\_G2, 3DES\_(MD5/SHA)\_G5, AES128\_MD5\_(G2/G5), AES256\_SHA\_(G2/G5), AES256\_SHA\_G14

OK Close

- TCP/IP Network Settings'de **Remote IP/Mask**'da Cisco Router'ın LAN IP Subnet'ini girin.
- Kaydetmek için **OK**'a tıklayın.

**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	192.168.1.1	<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	192.168.66.1		
Local Network Mask	255.255.255.0		
	More		

OK Clear Cancel

2. Profil etkinleştirildiğinde, Vigor Router VPN'i otomatik olarak başlatmaya çalışır. Ancak, el ile VPN aramak için, **VPN and Remote Access >> Connect Management** sayfasında IPsec profili seçin ve **Dial**'e tıklayın.

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

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode:	( Cisco ) 192.168.1.1	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

3. VPN başarıyla bağlandıktan sonra, aşağıdaki bağlantı durumunu görebiliriz.

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

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode:	( Cisco ) 192.168.1.1	Dial
Backup Mode:		Dial
Load Balance Mode:		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	Drop
1 ( Cisco )	IPsec Tunnel AES-SHA1 Auth	192.168.1.1 via WAN1	192.168.1.1/24	77	109	43	63	0:1:10	Drop

## Linux

1. **VPN and Remote Access >> VPN Profiles** 'a gidin ve yeni bir profil oluşturmak için IPsec sekmesindeki **Add**'e tıklayın.
  - o **Profile**'ı etkinleştirin.
  - o **Dial-Out Through** için Cisco Router'ın bulunduğu WAN Interface'sini seçin.
  - o **Local IP/Subnet Mask**'da Vigor Router'ın Local IP'sini veya Subnet'ini girin.
  - o **Remote Host** için Cisco Router'ın WAN IP adresini veya Domainini girin.
  - o **Remote IP/Subnet Mask**'da Cisco Router'ın Network IP'sini ya da Subnet'ini girin.
  - o Cisco Router'da girilen **Preshared Key**'i girin.

VPN and Remote Access >> VPN Profiles >> IPsec

IPsec PPTP Dial-out PPTP Dial-in SSL Dial-out SSL Dial-in GRE

**Add** Edit Delete Rename Refresh

IPsec

Profile : Cisco

Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out :  Enable  Disable

For Remote Dial-In User :  Enable  Disable

Dial-Out Through : wan1  Default WAN IP  WAN Alias IP

Fallover to : [ ]

Local IP / Subnet Mask : 192.168.101.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : Cisco WAN IP

Remote IP / Subnet Mask : 192.168.201.1 255.255.255.0/24

More Remote Subnet : 

IP	Subnet Mask
No items to show.	

IKE Protocol : IKEv1

IKE Phase 1 :  Main Mode  Aggressive Mode

Auth Type : PSK

Preshared Key : [redacted] (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.)

Security Protocol : ESP

2. Proposal sekmesinde Cisco Router'daki IPsec ayarlarıyla eşleşmesi için IKE Proposal seçin ardından kaydetmek için **Apply**'a tıklayın.

IPsec

Profile : Cisco

Enable

Basic Advanced GRE Proposal Multiple SAs

IKE Phase1 Proposal [Dial-Out] : AES256 G5

IKE Phase1 Authentication [Dial-Out] : SHA1

IKE Phase2 Proposal [Dial-Out] : AES256 with auth

IKE Phase2 Authentication [Dial-Out] : SHA1

Accepted Proposal [Dial-In] : acceptall

3. Profil etkinleştirildiğinde, Vigor Router VPN'i otomatik olarak başlatmaya çalışır. Ancak, VPN'yi manuel olarak aramak için, **VPN and Remote Access >> Connect Management** sayfasında IPsec profili seçin ve **Connect**'e tıklayın.



4. VPN başarıyla bağlandıktan sonra, aşağıdaki bağlantı durumunu görebiliriz.

