

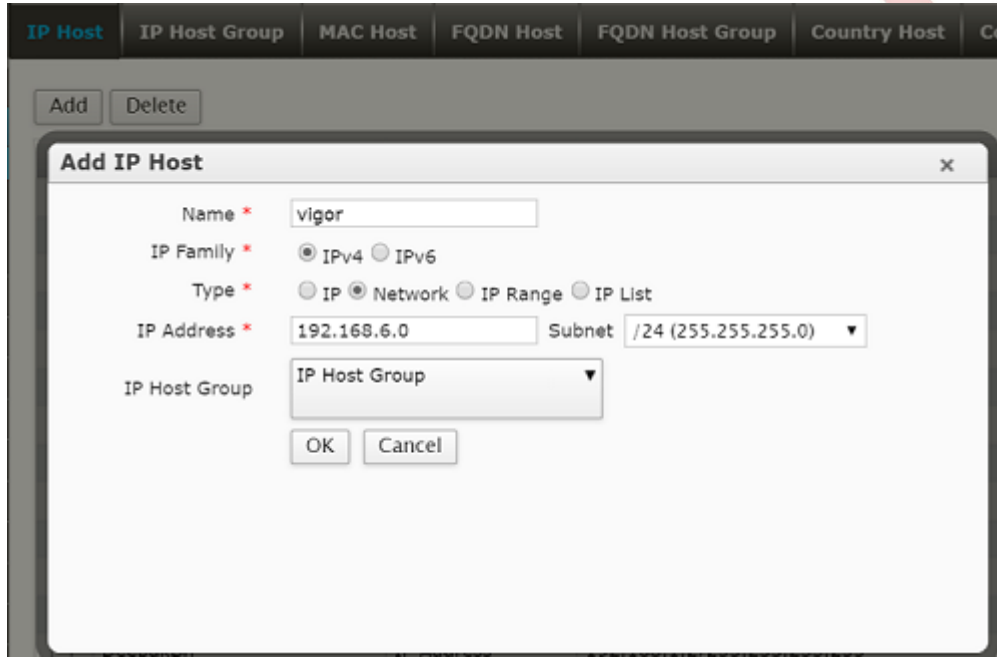
CYBEROAM VE DRAYTEK ARASINDA IPSEC TUNNEL

Bu makale, Cyberoam router ve Vigor router arasında IPsec VPN tünelinin nasıl kurulduğunu göstermektedir.

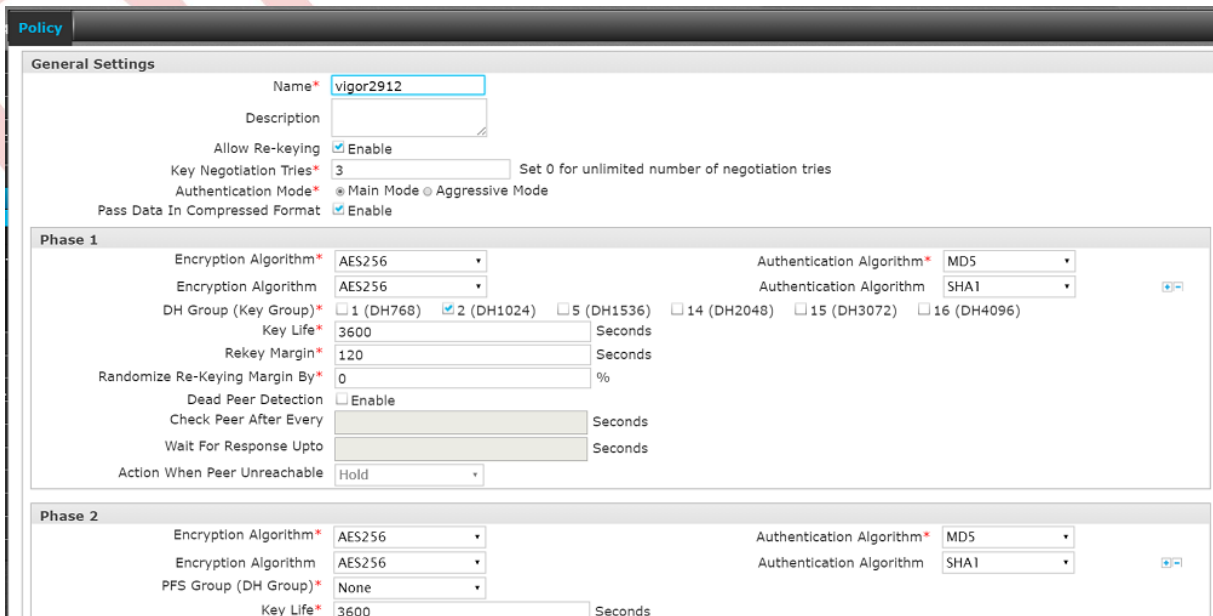
Cyberoam Ayarları

1. **OBJECTS >> Hosts >> IP Host** sekmesine gidin. Host eklemek için aşağıdaki adımları takip edin:

- **Type** için Network'ü seçin.
- **IP Address and Subnet** de Vigor Router'ın LAN IP'sini ve Subnet Mask'ını girin.
- Kaydetmek için **OK**'a tıklayın.



2. **VPN >> Policy** sekmesinde policy ekleyin. Encryption Algorithm, DH Group (Key Group) ve 1. ve 2. Phase'lerin Anahtar Key Life'ını istediğiniz gibi yapılandırın ayrıca Vigor Router'ın uyumlu bir yapılandırmaya sahip olması gerekir.



3. VPN >> IPsec >> **Connection** sekmesine gidin ve aşağıdaki bir profil ekleyin:

- General Settings’de profile bir isim girin.
- **Connection Type** için “Site-to-Site” seçeneğini seçin.
- **Policy**’e önceki adımda oluşturulan policy’i girin.
- Authentication Details’de **Authentication type**’i “Preshared Key” olarak ayarlayın ve bir Key girin.
- Endpoints Details’de **Local** için Vigor Router’daki WAN Interface’sini seçin.
- **Remote** için Vigor Router’ın WAN IP’sini ya da domain adını girin.

Connection | Failover Group

General Settings

Name* VPN2912

Description

Connection Type* Site to Site

Policy* vigor2912

Action on VPN Restart* Respond Only

Route Based Connection

Bind With An Interface ☐ Enable

Authentication Details

Authentication Type* Preshared Key

Preshared Key*

Endpoints Details

Local* PortB

Remote* vigorvpn.client.net

- Network Detail > Local’de **Add**’e tıklayın ve Vigor Router’a bağlanmak istediğiniz LAN nesnesini seçin.
- Network Detail > Remote’da **Add**’e tıklayın ve ilk adımda oluşturulan LAN nesnesini seçin.
- Kaydetmek için **OK**’a tıklayın.

Network Detail

IP Family * IPv4 IPv6

Local

Local Subnet* LAN

NATed LAN Same as Local LAN address

Local ID Select Local ID

Remote

Allow NAT Traversal ☒ Enable

Remote LAN Network* vigor

Remote ID Select Remote ID

User Authentication

Quick Mode Selectors

Advanced Settings

OK Cancel

Vigor Router Ayarları

DrayOS

1. **VPN and Remote Access >> VPN profiles >> IPsec** sayfasına gidin ve aşağıdaki gibi bir profil oluşturmak için uygun bir indexe tıklayın.

- Common settings’de profil adı girin. **Enable this profile**’ı etkinleştirin ve **Call Direction** için “Dial-Out” seçeneğini seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="cyberoam"/> <input checked="" type="checkbox"/> Enable this profile VPN Dial-Out Through <input type="text" value="WAN1 First"/> 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="0"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
--	--

- Dial-out settings’de **Type of Server I am Calling** için “IPsec Tunnel” seçin ve **Server IP**’de Cyberoam Router’ın WAN IP’sini girin.
- Cyberoam Router’da ayarlanan **Preshared Key** değerini girin.
- IPsec Security Method’da "High(ESP) AES with Authentication" seçeneğini seçin ardından **Advanced**’a tıklayın.
- Advanced Settings penceresinde Life Time, Phase1 ve Phase2 proposal ayarlarını Cyberoam Router’daki gibi ayarlayın.

Off <input type="button" value="IP6"/> Wizards Online Status WAN LAN Load-Balance/Route Policy NAT Firewall User Management Objects Setting CSM Bandwidth Management Applications VPN and Remote Access Remote Access PPP General Settings IPsec General Settings IPsec Peer ID Remote Dial-In LAN to LAN VPN TRUNK Mode Connection Mode Certificate Management Wireless LAN USB Application System Maintenance Diagnostics External Device	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] Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="cybervpn.server.net"/> IKE advanced settings - Google Chrome IKE advanced settings IKE phase 1 mode <input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode IKE phase 1 proposal <input type="text" value="AES256_SHA1_G2"/> IKE phase 2 proposal <input type="text" value="AES256_SHA1/AES256_MD5"/> IKE phase 1 key lifetime <input type="text" value="3600"/> (900 ~ 86400) IKE phase 2 key lifetime <input type="text" value="3600"/> (600 ~ 86400) Perfect Forward Secret <input checked="" type="radio"/> Disable <input type="radio"/> Enable Local ID <input type="text"/> 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_SHA1_(G2/G5), AES256_SHA_G14	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 IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key 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 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) <input type="text" value="AES with Authentication"/> Advanced Index(1-15) in Schedule Setup: <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> Username <input type="text" value="???"/> Password(Max 11 char) <input type="text"/>
---	--	--

- TCP/IP Network Settings’de **Remote Network IP**’de Cyberoam Router’ın LAN IP’sini girin.
- Profili 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	
Remote Network IP	192.168.1.1		Route
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.6.1		
Local Network Mask	255.255.255.0		
More		<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)	

OK Clear Cancel

2. Profili kaydettikten sonra, Vigor Router, profil etkin olduğu sürece VPN'i kurmaya çalışacaktır. Bununla birlikte, profili seçip **Dial**'i tıklayarak VPN'i **VPN and Remote Access >> Connection Management** sayfasından manuel olarak arayabilirsiniz.
- 3.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: (cyberoam) cybervpn.server.ne Dial

Backup Mode: Dial

4. VPN başarıyla bağlandığında VPN durumunu göreceğiz.

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 (cyber) AES-SHA1 Auth	192.168.1.1 via WAN1	192.168.1.1/24	13	3	13	3	0:1:8

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

Linux

1. **VPN and Remote Access >> LAN to LAN** sayfasına gidin ve aşağıdaki gibi bir profil oluşturmak için uygun bir **Add**'e tıklayın.
 - Basic sekmesinde, bir profil adı girin ve **Enable**'yi işaretleyin.
 - **Local IP** için Cyberoam Router'da bağlanmak istediğiniz Local networkün IP'sini ve Mask'ını girin.
 - **Remote Host**'da Cyberoam Router'ın WAN IP'sini ya da Domain adını girin.
 - **Remote IP** için Cyberoam Router'ın IP'sini ve Msk'ını girin.
 - Cyberoam Router'da yapılandırılan **Preshared Key** değerini girin.

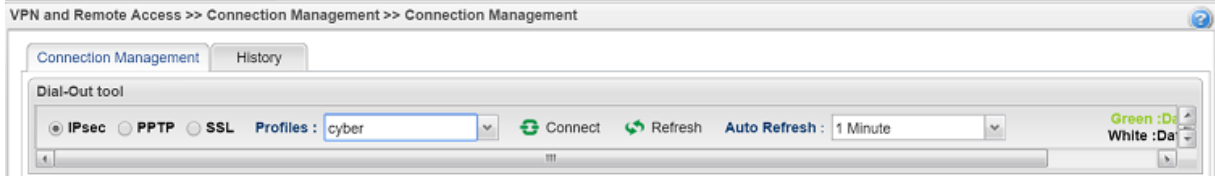
IPsec configuration window showing the Basic tab. The Profile is set to 'cyber' and is enabled. The Auto Dial-Out and For Remote Dial-In User options are both set to 'Disable'. The Dial-Out Through is set to 'wan2' with 'Default WAN IP' selected. The Local IP / Subnet Mask is 192.168.32.1 / 255.255.255.0/24. The Local Next Hop is 0.0.0.0. The Remote Host is cybervpn.server.net. The Remote IP / Subnet Mask is 192.168.1.1 / 255.255.255.0/24. The IKE Phase 1 is set to 'Main Mode' with 'Auth Type' as 'PSK' and 'Security Protocol' as 'ESP'. The Preshared Key is masked with dots. The window also shows a table for 'More Remote Subnet' which is currently empty.

IP	Subnet Mask
No items to show.	

1. Proposal sekmesinde Cyberoam router yapılandırmasındaki gibi ayarları uygulayın.

IPsec configuration window showing the Proposal tab. The Profile is set to 'cyber' and is enabled. The IKE Phase1 Proposal [Dial-Out] is set to 'AES256 G2'. The IKE Phase1 Authentication [Dial-Out] is set to 'ALL'. The IKE Phase2 Proposal [Dial-Out] is set to 'AES256 with auth'. The IKE Phase2 Authentication [Dial-Out] is set to 'ALL'. The Accepted Proposal [Dial-In] is set to 'acceptall'.

2. VPN'i kurmak için **VPN and Remote Access >> Connection Management** sayfasına gidin. Oluşturulan VPN profilinde **Dial**'e tıklayın.



1. VPN başarıyla bağlandığında VPN durumunu görebiliriz.

