

## SYSLOG İLE VPN SORUNLARINI GİDERME

VPN bağlanmadığında ve sebeplerini Syslog'da görebileceğiniz bazı mesajlar.

### DrayOS

Only **Vigor-xxx ==>** but no **Vigor-xxx <==**

Bu, VPN Peer'inin VPN isteğini hiç alamadığı anlamına gelir. İki VPN routeri arasındaki erişilebilirliği önce birbirlerine gönderebileceklerini test ederek kontrol etmelisiniz. Ardından, **Remote Access >> Remote Access Control Setup** sayfasındaki hizmeti etkinleştirerek routerdan VPN isteğini dinlediğinden emin olun.

#### VPN and Remote Access >> Remote Access Control Setup

##### Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPsec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

### Incoming Call Failed : No Such Entry for xxx

PPTP VPN istemcisi, xxx kullanıcı adına sahip bir VPN tüneli oluşturmaya çalışıyor, ancak router, xxx kullanıcı adına sahip PPTP VPN Profiline sahip değil anlamına gelir.

#### 3. Dial-In Settings

<b>Allowed Dial-In Type</b> <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> L2TP with IPsec Policy <span>None</span> <input type="checkbox"/> SSL Tunnel	<b>Username</b> <input type="text" value="user"/> <b>Password(Max 11 char)</b> <input type="password" value="....."/> <b>VJ Compression</b> <input checked="" type="radio"/> On <input type="radio"/> Off <b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <span>Max: 64 characters</span>
--	--

### -CHAP Login Failed ()

PPTP VPN istemcisi VPN'i yanlış şifre ile çeviriyor. Ayrıca VPN sunucusunun, yinelenen kullanıcı adıyla birden fazla VPN profili olup olmadığını kontrol edin, eğer varsa, bunlardan birini silin.

#### 2. Dial-Out Settings

<b>Type of Server I am calling</b> <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <span>IKEv1</span> <input type="radio"/> IKEv2 EAP <input type="radio"/> IPsec XAuth <input type="radio"/> L2TP with IPsec Policy <span>None</span> <input type="radio"/> SSL Tunnel	<b>Username</b> <input type="text" value="user"/> <b>Password</b> <input type="password" value="...."/> <b>PPP Authentication</b> <span>PAP/CHAP/MS-CHAP/MS-CHAPv2</span> <b>VJ Compression</b> <input checked="" type="radio"/> On <input type="radio"/> Off <b>IKE Authentication Method</b> <input type="radio"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <span>.....</span>
--	--

### Only ISAKMP\_NEXT\_KE but no ISAKMP\_NEXT\_ID

IPsec VPN istemcisi, VPN'i uygun olmayan bir Pre-Shared Key ile çeviriyor. VPN profilinin belirli bir Remote VPN IP'si veya Peer Kimliği varsa, **Pre-Shared Key**, bu VPN profilindeki **IKE Pre-Shared Key** değeridir. Değilse, **VPN and Remote Access >> IPsec General Setup** sayfasında ayarlanan Public Pre-shared Key kullanıyordur.

## 2. Dial-Out Settings

<b>Type of Server I am calling</b> <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <span style="float: right;">IKEv1 ▾</span> <input type="radio"/> IKEv2 EAP <input type="radio"/> IPsec XAuth <input type="radio"/> L2TP with IPsec Policy <span style="float: right;">None ▾</span> <input type="radio"/> SSL Tunnel	Username <input type="text" value="user"/> Password <input type="password" value="...."/> PPP Authentication <span>PAP/CHAP/MS-CHAP/MS-CHAPv2 ▾</span> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <b>IKE Authentication Method</b> <input checked="" type="radio"/> Pre-Shared Key <input type="radio"/> IKE Pre-Shared Key <input type="password" value="....."/> <input type="radio"/> Digital Signature(X.509) Peer ID <span>None ▾</span> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <span>None ▾</span>
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="123.45.67.89"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	

Client subnet xxxxxxxx/ffffff00 match failed

Local IP ve Mask istemci TCP/IP Network Settings'de yapılandırılan Remote IP ve Mask ile eşleşmiyor.

## 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"/> <input checked="" type="radio"/> Remote Network IP <input type="text" value="172.16.1.1"/> <input type="radio"/> Remote Network Mask <span>255.255.255.0 / 24 ▾</span> <input type="radio"/> Local Network IP <input type="text" value="192.168.1.1"/> <input type="radio"/> Local Network Mask <span>255.255.255.0 / 24 ▾</span> <input type="button" value="More"/>	RIP Direction <span>Disable ▾</span> From first subnet to remote network, you have to do <span>Route ▾</span> <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 )
---	--

## Destek

Yukarıdakilerin hiçbiri VPN bağlantısı sorununuzu çözmezse, [Netfast Destek](#) ile iletişime geçmekten çekinmeyin. Lütfen daha fazla araştırma için destek ekibine aşağıdaki bilgileri sağlayın: 1. Her iki routera [İnternet Erişimi](#), 2. Her iki routerdan toplanan Syslog.