

## VPN AÇIK ANCAK REMOTE NETWORK'DEKİ HOST'A ERİŞİLEMİYOR

VPN çevrimiçi görünüyor, ancak remote ağdaki Host'a erişemiyorsanız, işte bazı sorun giderme ipuçları.

### 1. Remote PC ping işlemine izin veriyorsa?

İlk olarak, ping istekleri varsayılan olarak PC'nin Firewall'u tarafından engellenebilir ve ping yanıtlarını alamamamızın nedeni bu olabilir. Remote ağdaki diğer Hostları deneyin veya PC'nin Firewall ayarlarını değiştirin.

### 2. Yönlendirmelerin doğru oluşturulduğunu görmek için Routing Tablosunu kontrol edin.

Router'ın routing tablosunu **Diagnostics > Routing Table**'da görebilirsiniz. Routing tablosunda, VPN ara yüzü üzerinden Remote LAN ağına giden Route'a ihtiyacımız var.

#### Diagnostics >> View Routing Table

Current Running Routing Table		IPv6 Routing Table	
Key: C - connected, S - static, R - RIP, * - default, ~ - private			
*	0.0.0.0/ 0.0.0.0	via 168.95.98.254	WAN1
S~	192.168.11.0/ 255.255.255.0	via 111.251.169.163	VPN-1
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1
S	111.248.122.210/ 255.255.255.255	via 111.248.122.210	WAN1
*	168.95.98.254/ 255.255.255.255	via 168.95.98.254	WAN1

Remote ağa doğru yönlendirme yoksa, lütfen VPN profilindeki TCP / IP Network Settings'i kontrol edin.

#### 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	192.168.11.0		Route
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.0	<input type="checkbox"/> Change default route to this VPN tunnel ( Only single WAN supports this )	
Local Network Mask	255.255.255.0		
	More		

### 3. Router, bilgisayarın Default Gateway'i midir?

Bir PC'de birden fazla ağ arayüzü varsa, trafik routera bağlanmayan arabirime gönderilebilir ve bu nedenle VPN'den geçmez ve remote ağa ulaşmaz. Trafiğin doğru arabirime gönderilip gönderilmediğini doğrulamak için, ilk sekmenin router IP olup olmadığını görmek için "tracert" komutunu kullanabiliriz. Değilse, PC'de manuel olarak bir route eklemeniz gerekir.

```
C:\Users\windows user>tracert 192.168.11.10
Tracing route to 192.168.11.10 over a maximum of 30 hops
  1      2 ms      1 ms      1 ms      192.168.1.1
```

#### 4. Router'ın erişimi engelleyen Firewall Policies'i varsa?

Her iki VPN Peer Router'ının Firewall ayarlarını kontrol edin ve remote ağa veya remote ağdan gelen trafiği engelleyebilecek bir şey olup olmadığına bakın. Ayrıca, denemek için her iki routerdaki Data Filter'ini devre dışı bırakabiliriz.

Firewall >> General Setup

General Setup

General Setup
Default Rule

**Call Filter**  Enable  Disable

**Data Filter**  Enable  Disable

Start Filter Set Set#1 ▼

Start Filter Set Set#2 ▼

Accept large incoming fragmented UDP or ICMP packets ( for some games, ex. CS )

Enable Strict Security Firewall

#### 5. Router'ın, trafiği başka bir Interface'e gönderebilecek Route Policies'i varsa?

Her iki VPN Peer'inde de Route Policies'i ve Static Route'ları kontrol edin ve routerın trafiği VPN yerine başka bir ara yüze gönderip göndermediğini kontrol edin. Route Policies'i da devre dışı bırakabiliriz.

Load-Balance/Route Policy



Load-Balance/Route Policy

10 ▼ rules per page | [Set to Factory Default](#) |

Index	Enable	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input checked="" type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any		<a href="#">Down</a>
2	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	<a href="#">UP</a>	<a href="#">Down</a>
3	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	<a href="#">UP</a>	<a href="#">Down</a>

#### 6. Her iki Network'ün IP ayarları aynıysa?

Local Ağın ve Remote VPN Ağının IP'si aynıysa, bir VPN kurmadan önce onları çevirmeliyiz, aksi takdirde yönlendirme çatışmasına neden olur. (Aynı IP Subnetini Kullanan İki Vigor Router Arasında IPsec Tüneli makalesine bakabilirsiniz.)

#### 7. IPsec AH kullanıyoruz ancak router NAT'ın arkasında mı?

Lütfen AH'li IPsec'in NAT'dan geçemediğini unutmayın, bu nedenle routerlardan herhangi biri NAT'ın arkasında, ESP ile IPsec tüneli oluşturmak gerekir.

2. Dial-Out Settings

<p><b>Type of Server I am calling</b></p> <p><input type="radio"/> PPTP</p> <p><input checked="" type="radio"/> IPsec Tunnel</p> <p><input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p>Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)</p> <p><input type="text" value="tim-2920.dyndns.org"/></p>	<p>Username <input data-bbox="1123 338 1390 376" type="text" value="???"/></p> <p>Password(Max 15 char) <input data-bbox="1123 389 1390 427" type="text"/></p> <p>PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <hr/> <p><b>IKE Authentication Method</b></p> <p><input checked="" type="radio"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input type="text" value="....."/></p> <p><input type="radio"/> Digital Signature(X.509)</p> <p>Peer ID <input type="text" value="None"/></p> <p>Local ID</p> <p><input checked="" type="radio"/> Alternative Subject Name First</p> <p><input type="radio"/> Subject Name First</p> <p>Local Certificate <input type="text" value="None"/></p> <hr/> <p><b>IPsec Security Method</b></p> <p><input type="radio"/> Medium(AH)</p> <p><input checked="" type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/></p> <p>Advanced <input type="button" value=""/></p>
--	---

