

DRAYTEK ROUTER'LAR ARASINDA AGGRESIVE MODE

IPSEC TUNNEL

Main moddaki IPsec VPN, IP adresini Peer authentication için Peer Identity (ID) olarak kullanır; bu nedenle, her iki VPN eşinin de statik IP adresi olmaması bir çözüm değildir. Bu gibi durumlarda, IPsec VPN'i Aggressive moda ayarlayabiliriz. Bu belge IPsec Tüneli'nin iki Vigor Router arasında Aggressive moda nasıl kurulacağını açıklar.

DrayOS

VPN Server (Dial-in Site) Kurulumu

- VPN Server'da, VPN istemcisi için bir Dial-in profili oluşturun: VPN and Remote Access >> LAN to LAN sayfasına gidin. Profili ayarlamak için boş bir indexe tıklayın. Common Settings'de,
 - Profil adı girin.
 - Enable this profile**'i etkinleştirin.
 - Call Direction** için "Dial-in" seçin.

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 300 second(s)
Netbios Naming Packet <input type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel 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 []

- Dial-In Settings'de,
 - Allowed Dial-in Type**'de IPsec Tunnel'in işaretli olduğundan emin olun.
 - Specify Remote VPN Gateway**'i etkinleştirin ve **Peer ID** girin.
 - IKE Pre-Shared Key**'ye tıklayın ve **Pre-Shared Key** girin.
 - IPsec Security Method**'da kullanılmasına izin verilen güvenlik metotlarını seçin.

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] <input type="checkbox"/> SSL Tunnel	Username Password(Max 11 char) VJ Compression	Router Web Configurator - Google Chrome 192.168.1.1/doc/pskey.htm IKE Authentication Method Pre-Shared Key Confirm: Pre-Shared Key OK
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP [] or Peer ID support@draytek.com	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None Local ID <input 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	

- TCP/IP Network Settings**'de, **Remote Network IP** ve **Remote Network Mask** için VPN istemcisinin LAN networkünü belirtin. 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	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Local Network IP	172.16.1.1	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		
	More		

VPN Client (Dial-out Site) Kurulumu

- VPN istemcisinde, VPN sunucusuna bir Dial-out profili oluşturun: **VPN and Remote Access >> LAN to LAN** sayfasına gidin, Profili eklemek için boş bir indexe tıklayın. Common Settings’de,
 - Profil adı girin.
 - Enable this profile**’ı işaretleyin.
 - Call Direction** için Dial-Out ayarlayın.

1. Common Settings

Profile Name	DrayTek HQ	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 type="checkbox"/> Always on	
VPN Dial-Out Through	WAN1 First	Idle Timeout	300 second(s)
Netbios Naming Packet	<input type="radio"/> Pass <input checked="" type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive	
Multicast via VPN	<input type="radio"/> Pass <input checked="" type="radio"/> Block	PING to the IP	
(for some IGMP,IP-Camera,DHCP Relay..etc.)			

5. Dial-out Setting’de,

- Type of **Sever I am Calling** için IPsec Tunnle’i seçin.
- Server IP/Host Name for VPN,**’de VPN sunucusunun WAN IP’sini ya da doamin adını girin.
- IKE Pre-Shared Key**’i tıklayın ve VPN sunucusunda girilen preshared key’i girin.
- IPsec Security Method’da **Advanced**’e tıklayın.

2. Dial-Out Settings

Type of Server I am calling	Username	Router Web Configurator - Google Chrome 192.168.1.1/doc/pskey.htm
<input checked="" type="radio"/> IPsec Tunnel	Password(Max 15 char)	
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	PPP Authentication	IKE Authentication Method
100.100.100.100	PAP/CHAP/MS-CHAP/MS-CHAP	Pre-Shared Key
	VJ Compression	Confirm Pre-Shared Key
	IKE Authentication Method	OK
	<input checked="" type="radio"/> Pre-Shared Key	
	<input type="radio"/> Digital Signature(X.509)	
	Peer ID	
	Local ID	
	<input type="radio"/> Alternative Subject Name First	
	<input type="radio"/> Subject Name First	
	Local Certificate	
	IPsec Security Method	
	<input type="radio"/> Medium(AH)	
	<input checked="" type="radio"/> High(ESP) DES without Authentication	
	Advanced	
	Index(1-15) in Schedule Setup:	

6. **IKE advanced settings**'de **IKE phase 1 mode** için "Aggressive Mode" seçin, VPN sunucusundaki **Peer ID**'yi **Local ID**'ye girin.

IKE advanced settings

IKE phase 1 mode Main mode Aggressive mode

IKE phase 1 proposal DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_SHA1_G1

IKE phase 2 proposal HMAC_SHA1/HMAC_MD5

IKE phase 1 key lifetime 28800 (900 ~ 86400)

IKE phase 2 key lifetime 3600 (600 ~ 86400)

Perfect Forward Secret Disable Enable

Local ID support@draytek.com

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

7. **TCP/IP Network Settings**'de, **Remote Network IP** ve **Remote Network Mask** için VPN istemcisinin LAN networkünü belirtin. Profili kaydetmek için **OK**'a tıklayın.

5. TCP/IP Network Settings

My WAN IP 0.0.0.0

Remote Gateway IP 0.0.0.0

Remote Network IP 172.16.1.1

Remote Network Mask 255.255.255.0

Local Network IP 192.168.1.1

Local Network Mask 255.255.255.0

More

RIP Direction Disable

From first subnet to remote network, you have to do

Route

IPsec VPN with the Same Subnets

Change default route to this VPN tunnel (Only single WAN supports this)

VPN Tunnel Kurulumu

VPN istemcisine VPN bağlantısı başlatmak gitmek için **VPN and Remote Access >> Connection Management** sayfasına gidin, VPN Server profili seçin ve **Dial**'e tıklayın.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: (DrayTek HQ) 100.100.100.100 Dial

Backup Mode: Dial

Load Balance Mode: Dial

Tüm ayarlar eşleşirse, VPN kurulacaktır ve istatistikler **VPN and Remote Access >> Connection Management** sayfasında görünecektir.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: (DrayTek HQ) 100.100.100.100 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
1 (DrayTek HQ)	IPsec Tunnel DES-No Auth	100.100.100.100 via WAN2	172.16.1.1/24	9	40	9	40	0:0:44

xxxxxxx : Data is encrypted.

xxxxxxx : Data isn't encrypted.

Linux

VPN Client (Dial-Out) Kurulumu

1. **VPN and Remote Access >> VPN Profile >> IPsec**'e gidin profil eklemek için **Add**'e tıklayın.
 - Basic sekmesinde, profil adı girin.
 - **Enable**'yi işaretleyin.
 - **Auto Dial-Out** için "Enable" yi seçin ve "Always Dial-Out" u seçin.
 - **Local IP / Subnet Mask**'a remote networke bağlanmak istediğiniz router'ın LAN networkünü girin.
 - **Remote Host**'da VPN Peer'ın WAN IP'sini girin.
 - **Remote IP/ Subnet Mask**'da VPN Peer'ın LAN IP'sini girin.
 - **Aggressive Mode** seçin.
 - **Local ID** girin
 - **Remote ID** girin.
 - **Pre-Shared Key**'i girin. (VPN Peer'daki pre-shared key ile aynı olmalıdır.)
 - Profili kaydetmek için **Apply**'i tıklayın.

IPsec

Profile :

Enable

Basic | Advanced | GRE | Proposal | Multiple SAs

Auto Dial-Out : Enable Disable Always Dial-Out

For Remote Dial-In User : Enable Disable

Dial-Out Through : Default WAN IP WAN Alias IP

Failover to :

Local IP / Subnet Mask :

Local Next Hop : (0.0.0.0 : default gateway)

Remote Host :

Remote IP / Subnet Mask :

Add Save Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

IKE Protocol :

2. Benzer şekilde, VPN Peer'da, yeni bir profil eklemek için **VPN and Remote Access >> VPN Profile >> IPsec**'e gidin.
 - Basic sekmesinde, profil adı girin.
 - **Enable**'yi işaretleyin.
 - **Auto Dial-Out** ve **For Remote Dial-In User** için **Disable**'yi işaretleyin.
 - **Local IP /Subnet Mask**'a routerın LAN networkünü girin.
 - **Remote Host**'da VPN Peer'ın WAN IP'sini girin.
 - **Remote IP/ Subnet Mask**'da VPN Peer'ın LAN IP'sini girin.
 - **Aggressive Mode** seçin.

- **Local ID** girin. (VPN Peer'daki Remote ID olmalıdır.)
- **Remote ID** girin. (VPN Peer'daki Local ID olmalıdır.)
- VPN Peer'daki aynı **Pre-Shared Key**'i girin.
- Profili kaydetmek için **Apply**'i tıklayın.

IPsec

Profile :

Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out : Enable Disable

For Remote Dial-In User : Enable Disable

Dial-Out Through : Default WAN IP WAN Alias IP

Failover to :

Local IP / Subnet Mask :

Local Next Hop : (0.0.0.0 : default gateway)

Remote Host :

Remote IP / Subnet Mask :

Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

More Remote Subnet :

IKE Protocol :

VPN Kurulumu

Tüm ayarlar eşleşirse, VPN bağlantısı otomatik olarak oluşturulur. Connection Status'de IPsec tünelinin devrede olduğunu görebiliriz.

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

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles : Auto Refresh : 1 Minute Green :Data is encry
White :Data isn't enc

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	Operation	
1	branch2	IPsec/3DES...	wan1	200.200.200	192.168.21.0/24	00:00:31	176(bps)	336(bps)	240(Byte)	448(Byte)	<input type="button" value="X"/> <input type="button" value="Refresh"/>