

## DRAYTEK ROUTERLARI ARASINDA MAIN MODDA IPSEC TUNNEL

Bu makalede, VPN istemcisi, dinamik ve statik bir Public IP adresi kullandığında iki Vigor Router arasında Main Modda bir IPsec Tüneli'nin nasıl kurulacağı açıklanmaktadır. NAT'ın arkasında bulunan VPN istemcisini, lütfen Aggressive modda IPsec VPN olarak kullanın.

### DrayOS

#### VPN Server Kurulumu - VPN Client Dinamik IP Kullandığında

1. **VPN and Remote Access >>IPsec General Setup** sayfasına gidin ve General IPsec Pre-Shared Key'i girin. Burada girilen Pre-Shared Key, dinamik IP adresleri kullanan tüm IPsec Main mod VPN istemcilerinin kimliğini doğrulamak için kullanılacaktır.

#### VPN and Remote Access >> IPsec General Setup

##### VPN IKE/IPsec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

<b>IKE Authentication Method</b>	
Certificate for Dial-in	None ▼
<b>General Pre-Shared Key</b>	
Pre-Shared Key	.....
Confirm Pre-Shared Key	.....
<b>Pre-Shared Key for XAuth User</b>	
Pre-Shared Key	Max: 64 characters
Confirm Pre-Shared Key	
<b>IPsec Security Method</b>	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authenticated, but will not be encrypted.
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and authenticated.

2. Peer VPN istemcisi routeri için **VPN and Remote Access >> LAN to LAN** sayfasında LAN to LAN profil oluşturun. Profil eklemek için uygun bir indexe tıklayın.



## LAN-to-LAN Profiles:

[Set to Factory Default](#)View:  All  Trunk

Index	Enable	Name	Remote Network	Status	Index	Enable	Name	Remote Network	Status
<b>1.</b>	<input type="checkbox"/>	???		---	<b>17.</b>	<input type="checkbox"/>	???		---
<b>2.</b>	<input type="checkbox"/>	???		---	<b>18.</b>	<input type="checkbox"/>	???		---
<b>3.</b>	<input type="checkbox"/>	???		---	<b>19.</b>	<input type="checkbox"/>	???		---
<b>4.</b>	<input type="checkbox"/>	???		---	<b>20.</b>	<input type="checkbox"/>	???		---
<b>5.</b>	<input type="checkbox"/>	???		---	<b>21.</b>	<input type="checkbox"/>	???		---

3. Profil ayarlarını aşağıdaki gibi yapılandırın.

- **Enable this profile**'ı etkinleştirin.
- **Call Direction** için **Dial-In** seçin.
- VPN istemcisinin bağlanacağı **WAN Interface**'sini seçin.
- **Idle Timeout**'u 0 saniye olarak değiştirin.

## 1. Common Settings

Profile Name <input type="text" value="Dial_In"/>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	Tunnel Mode <input type="radio"/> GRE Tunnel
VPN Dial-Out Through <input type="text" value="WAN1 Only"/>	<input type="checkbox"/> Always on
<input type="text" value="1-192.168.239.29"/>	Idle Timeout <input type="text" value="0"/> second(s)
Netbios Naming Packet <input checked="" 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	PING to the IP <input type="text"/>

- Dial-In Settings'de **IPsec Tunnel**'e izin verin.

## 3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="checkbox"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text" value="Max: 11 characters"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text" value="Max: 47 characters"/>	<b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="Max: 64 characters"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First

- TCP/IP Network Settings'de **Remote Network IP and Mask**'da VPN istemcisi olarak kullanacağınız IP subnetini girin.
- VPN profilini 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	192.168.1.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.239.0
Local Network Mask	255.255.255.0 / 24
<a href="#">More</a>	

## VPN Server Kurulumu - VPN Client Statik IP Kullandığımda

1. Peer VPN istemcisi routerı için **VPN and Remote Access** >> **LAN to LAN** sayfasında LAN to LAN profil oluşturun. Profil eklemek için uygun bir indexe tıklayın.

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



## LAN-to-LAN Profiles:

[Set to Factory Default](#)
View:  All  Trunk

Index	Enable	Name	Remote Network	Status	Index	Enable	Name	Remote Network	Status
<a href="#">1.</a>	<input type="checkbox"/>	???		---	<a href="#">17.</a>	<input type="checkbox"/>	???		---
<a href="#">2.</a>	<input type="checkbox"/>	???		---	<a href="#">18.</a>	<input type="checkbox"/>	???		---
<a href="#">3.</a>	<input type="checkbox"/>	???		---	<a href="#">19.</a>	<input type="checkbox"/>	???		---
<a href="#">4.</a>	<input type="checkbox"/>	???		---	<a href="#">20.</a>	<input type="checkbox"/>	???		---
<a href="#">5.</a>	<input type="checkbox"/>	???		---	<a href="#">21.</a>	<input type="checkbox"/>	???		---

2. Profil ayarlarını aşağıdaki gibi yapılandırın.

- **Enable this profile**'ı etkinleştirin.
- **Call Direction** için **Dial-In** seçin.
- VPN istemcisinin bağlanacağı **WAN Interface**'sini seçin.
- **Idle Timeout**'u 0 saniye olarak değiştirin.

## 1. Common Settings

Profile Name	Dial_In	Call Direction	<input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile		Tunnel Mode	<input type="radio"/> GRE Tunnel
VPN Dial-Out Through	WAN1 Only	<input type="checkbox"/> Always on	
1-192.168.239.29		Idle Timeout	0 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	PING to the IP	

- Dial-In Settings'de **IPsec Tunnel**'e izin verin.
- **Specify Remote VPN Gateway** işaretleyin ve Peer VPN istemcisinin IP adresini girin.
- **IKE Pre-Shared Key**'e tıklayın ve Pre-Shared Key girin.

## 3. Dial-In Settings

<b>Allowed Dial-In Type</b> <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> L2TP with IPsec Policy <span>None</span> <input type="checkbox"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text" value="Max: 11 characters"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="192.168.1.111"/> or Peer ID <input type="text" value="Max: 47 characters"/>	<b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key <input checked="" type="checkbox"/> IKE Pre-Shared Key <input type="text" value="....."/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First

- TCP/IP Network Settings'de **Remote Network IP and Mask**'da VPN istemcisi olarak kullanacağınız IP subnetini girin.
- VPN profilini kaydetmek için **OK**'a tıklayın.

## 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"/>
Remote Network IP	<input type="text" value="192.168.1.0"/>
Remote Network Mask	<input type="text" value="255.255.255.0 / 24"/>
Local Network IP	<input type="text" value="192.168.239.0"/>
Local Network Mask	<input type="text" value="255.255.255.0 / 24"/>
<input type="button" value="More"/>	

## VPN Client Kurulumu

1. Benzer şekilde, **VPN and Remote Access >> LAN to LAN** sayfasına gidip profil oluşturun.
  - **Profil adı** girin.
  - **Enable this profile**'ı etkinleştirin.
  - Call Direction için **Dial-Out** seçin
  - **Always On**'u işaretleyin.

## 1. Common Settings

Profile Name <input type="text" value="toServer"/> <input checked="" type="checkbox"/> Enable this profile	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in Tunnel Mode <input type="radio"/> GRE Tunnel <input checked="" type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 Only"/> <input type="text" value="1-192.168.239.29"/>	Idle Timeout <input type="text" value="-1"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
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.)	

- Dial-Out Settings'de **IPsec Tunnel**'i seçin.
- **Server IP/Host Name for VPN**'de VPN sunucusunun WAN IP'sini ya da domain adını girin.

- IPsec Security Method'da **Advanced**'a tıklayın.

## 2. Dial-Out Settings

<b>Type of Server I am calling</b> <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <span style="border: 1px solid red; padding: 2px;">IKEv1</span> <input type="radio"/> L2TP with IPsec Policy <span style="border: 1px solid gray; padding: 2px;">None</span> <input type="radio"/> SSL Tunnel	Username <span style="border: 1px solid gray; padding: 2px;">???</span> Password <span style="border: 1px solid gray; padding: 2px;">Max: 15 characters</span> PPP Authentication <span style="border: 1px solid gray; padding: 2px;">PAP/CHAP/MS-CHAP/MS-CHAPv2</span> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <span style="border: 1px solid red; padding: 2px;">111.222.111.222</span>	<b>IKE Authentication Method</b> <input checked="" type="radio"/> Pre-Shared Key <span style="border: 1px solid red; padding: 2px;">IKE Pre-Shared Key</span> <span style="border: 1px solid gray; padding: 2px;">*****</span> <input type="radio"/> Digital Signature(X.509) Peer ID <span style="border: 1px solid gray; padding: 2px;">None</span> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <span style="border: 1px solid gray; padding: 2px;">None</span>
Server Port (for SSL Tunnel): <span style="border: 1px solid gray; padding: 2px;">443</span>	<b>IPsec Security Method</b> <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <span style="border: 1px solid gray; padding: 2px;">AES with Authentication</span> <span style="border: 1px solid red; padding: 2px;">Advanced</span>

## 2. IKE Advanced Settings'de

- **IKE phase 1 mode** için **Main Mode** seçin.
- Phase 1 and Phase 2 proposal'ın güvenlik yöntemlerini kullandığından emin olun.
- Kaydetmek için **OK**'a tıklayın.

## IKE advanced settings

IKE phase 1 mode(IKEv1)	<input checked="" type="radio"/> <span style="border: 1px solid red; padding: 2px;">Main mode</span>
IKE phase 1 proposal Encryption	<span style="border: 1px solid gray; padding: 2px;">Auto</span>
IKE phase 1 proposal ECDH Group	<span style="border: 1px solid gray; padding: 2px;">G14</span>
IKE phase 1 proposal Authentication	<span style="border: 1px solid gray; padding: 2px;">SHA256</span>
IKE phase 2 proposal	<span style="border: 1px solid gray; padding: 2px;">AES128_[SHA1,MD5,SHA256]</span>
IKE phase 1 key lifetime	<span style="border: 1px solid gray; padding: 2px;">28800</span> (900 ~ 86400)
IKE phase 2 key lifetime	<span style="border: 1px solid gray; padding: 2px;">3600</span> (600 ~ 86400)
Perfect Forward Secret	<input checked="" type="radio"/> <span style="border: 1px solid gray; padding: 2px;">Disable</span>
Local ID	<span style="border: 1px solid gray; padding: 2px;"></span>

TCP/IP Network Settings'de, **Remote Network IP** ve **Remote Network Mask**'da VPN Sunucusunun LAN'ını girin.

## 5. TCP/IP Network Settings

My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	192.168.239.0
Remote Network Mask	255.255.255.0 / 24 ▼
Local Network IP	192.168.1.0
Local Network Mask	255.255.255.0 / 24 ▼
<a href="#">More</a>	

Yukarıdaki yapılandırmaları tamamladıktan sonra, VPN İstemcisi IPsec tüneline otomatik olarak arar. VPN durumunu VPN and Remote Access >> Connection Management sayfasından kontrol edebiliriz.

### VPN and Remote Access >> Connection Management

#### Dial-out Tool

[Refresh](#)

General Mode: ( toServer )	<input type="button" value="Dial"/>
Backup Mode:	<input type="button" value="Dial"/>
Load Balance Mode:	<input type="button" value="Dial"/>

#### VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime	
1 ( toServer )	IPsec Tunnel AES-SHA1 Auth	192.168.239.0/24	192.168.239.0/24	1	72	1	96	0:0:28	<input type="button" value="Drop"/>

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

### Linux

#### VPN Server Kurulumu - VPN Client Dinamik IP Kullandığında

1. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin, **Preshared Key** girin ve VPN istemcisinin arayacağı WAN Profili'ni seçin. Burada yapılandırılan Preshared Key, dinamik IP adresleri kullanan tüm IPsec Main mod istemcilerinin kimliğini doğrulamak için kullanılacaktır. Başka bir deyişle, birden fazla VPN istemcisi olduğunda, burada yapılandırılan VPN sunucusuyla aynı IPsec Preshared Key'i kullanmaları gerekir.



VPN and Remote Access >> IPsec General Setup

IPsec General Setup

**Preshared Key :** ..... (Max 46 characters)

**IPsec User Preshared Key :** ..... (Only for XAuth, Max 46 characters)

**WAN Profile :** wan1, wan2

**User Authentication Type :** Local (Local/Radius support IPsec XAuth/EAP)

**DHCP LAN Profile :** lan1

**IKE Port :** 500

**NAT-T Port :** 4500

**IPsec MSS :** 1300

**Security Method :**  DES  3DES  AES

2. **VPN and Remote Access >> VPN Profile >> IPsec**'e gidin ve yeni profil eklemek için **Add**'e tıklayın:

- Basic sekmesinde, Profil adı girin ve profil için **Enable**'yi işaretleyin.
- **Auto Dial-Out** ve **For Remote Dial-In User** ayarlarını **Disable** olarak seçin.
- **Dial-Out Through** için VPN istemcisini aramak için kullanılan **WAN Interface**'sini seçin.
- **Local IP /Subnet Mask** için VPN sunucusunun local network IP'sini ve subnetini girin.
- **Remote Host**'da **0.0.0.0** IP'sini kullanın. (Remote Host IP 0.0.0.0 VPN istemcisi bir dinamik IP adresi ile olduğu zaman bu VPN profili herhangi Peer IP adresini kabul eder ve uygun olduğu anlamına gelir.)
- **Remote IP/ Subnet Mask** için eş VPN routerın LAN Network'ünü girin.
- IKE Protocol için **IKEv1** seçin ve IKE phase1'i **Main Mode** olarak girin.
- **Pre-Shared Key**'i boş bırakın.
- Kaydetmek için **OK**'a 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 I

Failover to :

Local IP / Subnet Mask :

Local Next Hop :  (0.0.0.0 : default gateway)

Remote Host :

Remote IP / Subnet Mask :

IP	Subnet Mask
	No

More Remote Subnet :

IKE Protocol :

IKE Phase 1 :  Main Mode  Aggressive Mode

Auth Type :

Preshared Key :  (If Aggressive mode is dis

Security Protocol :

### VPN Server Kurulumu - VPN Client Statik IP Kullandığında

- VPN and Remote Access >> VPN Profile >> IPsec'e gidin ve yeni profil eklemek için Add'e tıklayın:
  - Basic sekmesinde, Profil adı girin ve profil için Enable'yi işaretleyin.
  - Auto Dial-Out ve For Remote Dial-In User ayarlarını Disable olarak seçin.
  - Dial-Out Through için VPN istemcisini aramak için kullanılan WAN Interface'sini seçin.

Local IP /Subnet Mask için VPN sunucusunun local network IP'sini ve



- **Remote Host** için VPN Peer'in WAN IP'sini girin.
- **Remote IP/ Subnet Mask** için eş VPN routerın LAN Network'ünü girin.
- IKE Protocol için **IKEv1** seçin ve IKE phase1'i **Main Mode** olarak girin.
- VPN istemcisinin statik IP'si için **Pre-Shared Key** girin.
- Kaydetmek için **OK**'a tıklayın.

IPsec

Profile : Server

Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out :  Enable  Disable

For Remote Dial-In User :  Enable  Disable

Dial-Out Through : wan2  Default WAN IP  WAN Alias IP

Failover to :

Local IP / Subnet Mask : 192.168.239.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 111.222.111.222

Remote IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

Add Save

IP	Subnet Mask
No items	

More Remote Subnet :

IKE Protocol : IKEv1

IKE Phase 1 :  Main Mode  Aggressive Mode

Auth Type : PSK

Preshared Key : ..... (If Aggressive mode is disabled)

Security Protocol : ESP

## VPN Client Kurulumu

1. **VPN and Remote Access >> VPN Profile >> IPsec**'e gidin ve yeni profil eklemek için **Add**'e tıklayın:
  - Basic sekmesinde, Profil adı girin ve **Enable**'yi işaretleyin.
  - **Auto Dial-Out** için **Enable**'yi seçin.
  - VPN İstemcisinin **Dial-Out Through** tüneline arayacağı **WAN Interface**'sini girin.
  - **Local IP /Subnet Mask**'da VPN istemcisinin Local Network IP'sini ve Subnet'ini girin.
  - **Remote Host**'da VPN sunucusunun WAN IP'sini veya Domain adını girin.

- **Remote IP/ Subnet Mask**'da eş VPN sunusunun LAN Network'ünü girin.
- IKE Protocol için **IKEv1** seçin ve IKE phase1'i **Main Mode** olarak girin.
- **Pre-Shared Key** girin.
- Kaydetmek için **OK**'a tıklayın.

Profile : toHQ

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 :

wan1  Default WAN IP  WAN Alias IP

Failover to :

Local IP / Subnet Mask :

192.168.1.0 255.255.255.0/24

Local Next Hop :

0.0.0.0 (0.0.0.0 : default gateway)

Remote Host :

x.x.x.x

Remote IP / Subnet Mask :

192.168.239.0 255.255.255.0/24

Add Save

More Remote Subnet :

IP	Subnet Mask
No items	

IKE Protocol :

IKEv1

IKE Phase 1 :

Main Mode  Aggressive Mode

Auth Type :

PSK

Preshared Key :

..... (If Aggressive mode is disabled)

Security Protocol :

ESP

Yukarıdaki yapılandırmaları tamamladıktan sonra, VPN İstemcisi IPsec tüneline otomatik olarak arar. VPN durumunu VPN and Remote Access >> Connection Management sayfasından kontrol edebiliriz.

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

Connection Management History

Dial-Out tool

IPsec  PPTP  SSL Profiles :  Connect Refresh Auto Refresh : 1 Minute Green : Da White : Da

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte
1	toHQ	IPsec/AES_...	wan1	192.168.239.0/24	00:01:30	0(bps)	0(bps)	1.14 (KB)	3.56 (KB)

