

## DRAYTEK ROUTERLARI ARASINDA IPSEC TUNELI MAIN MODU (DINAMIK IP'LI İSTEMCİ)

Bu makale, VPN istemcisi dinamik bir public IP adresi kullandığında iki Vigor Router arasında Main Modda bir IPsec Tüneli'nin nasıl kurulacağını açıklamaktadır. NAT'ın arkasında bulunan VPN istemcisi için lütfen Aggressive modda IPsec VPN'i kullanın.

### DrayOS

#### VPN Server Kurulumu

1. **VPN and Remote Access >>IPsec General Setup** sayfasına gidin ve **General IPsec Pre-Shared Key**'i konfigüre edin. Burada yapılandırılan 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).

**IKE Authentication Method**

Certificate for Dial-in

**General Pre-Shared Key**

Pre-Shared Key

Confirm Pre-Shared Key

**Pre-Shared Key for XAuth User**

Pre-Shared Key

Confirm Pre-Shared Key

**IPsec Security Method**

Medium (AH)  
Data will be authenticated, but will not be encrypted.

High (ESP)  DES  3DES  AES  
Data will be encrypted and authenticated.

OK

Cancel

2. Eş VPN istemcisi routerı için **VPN and Remote Access >> LAN to LAN** sayfasında VPN LAN-to-LAN profili oluşturun ve yeni bir profil eklemek için kullanılabilir bir indexe tıklayın.

#### VPN and Remote Access >> 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
<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. Profili aşağıdaki gibi düzenleyin:
  - a. **Enable this profile**'ı işaretleyin.
  - b. **Call Direction** için **Dial-In** seçeneğini seçin.
  - c. VPN istemcisinin arayacağı **WAN Interface**'ini seçin.
  - d. **Idle Timeout**'u **0** saniye olarak değiştirin.
  - e. Dial-In Settings'de **IPsec Tunnel**'e izin verin.

### 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  <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <span>Max: 47 characters</span>	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  <b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value="Max: 64 characters"/> <input type="checkbox"/> Digital Signature(X.509) None Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
---	--

- f. TCP/IP Network Settings'de **Remote Network IP and Mask** için VPN istemcisinin kullandığı IP subnetini girin.
- g. 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** 'da profil oluşturun.
  - **Profile Name** girin.
  - **Enable this profile**'ı işaretleyin.
  - Call Direction için **Dial-Out** seçeneğini seçin.
  - **Always On**'u işaretleyin.

### 1. Common Settings

Profile Name <input type="text" value="toServer"/> <input checked="" type="checkbox"/> Enable this profile  VPN Dial-Out Through <input type="text" value="WAN1 Only"/> <input type="text" value="1-192.168.239.29"/> 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 Tunnel Mode <input type="radio"/> GRE Tunnel <input checked="" type="checkbox"/> Always on 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"/>
--	--

- Dial-Out Settings'de **IPsec Tunnel**'i seçin.
- **Server IP/Host Name for VPN**'de VPN sunucusunun WAN IP'sini veya domain adını girin.
- VPN Server'da yapılandırılan aynı **IKE Pre-Shared Key**'i 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="float: right;">IKEv1 ▼</span> <input type="radio"/> L2TP with IPsec Policy <span style="float: right;">None ▼</span> <input type="radio"/> SSL Tunnel	Username <input type="text" value="???"/> Password <input type="text" value="Max: 15 characters"/> PPP Authentication <span>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) <input type="text" value="111.222.111.222"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	<b>IKE Authentication Method</b> <input checked="" type="radio"/> Pre-Shared Key <input checked="" type="radio"/> IKE Pre-Shared Key <input type="text" 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>
	<b>IPsec Security Method</b> <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <span>AES with Authentication ▼</span> <input checked="" type="radio"/> Advanced

IKE Advanced Settings'de:

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

## IKE advanced settings

IKE phase 1 mode(IKEv1)	<input checked="" type="radio"/> Main mode
IKE phase 1 proposal Encryption	Auto ▼
IKE phase 1 proposal ECDH Group	G14 ▼
IKE phase 1 proposal Authentication	SHA256 ▼
IKE phase 2 proposal	AES128_[SHA1,MD5,SHA256] ▼
IKE phase 1 key lifetime	28800 (900 ~ 86400)
IKE phase 2 key lifetime	3600 (600 ~ 86400)
Perfect Forward Secret	<input checked="" type="radio"/> Disable
Local ID	<input type="text"/>

TCP/IP Network Settings'de **Remote Network IP** ve **Remote Network Mask**'da VPN Server'ın LAN Network'ünü girin. 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	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
More	

Yukarıdaki konfigürasyonlar tamamlandıktan sonra VPN İstemcisi IPsec tüneline otomatik olarak çevirir. VPN durumunu VPN and Remote Access >> Connection Management sayfasından kontrol edebiliriz.

## VPN and Remote Access &gt;&gt; Connection Management

## Dial-out Tool

Refresh

General Mode:	( toServer )	Dial
Backup Mode:		Dial
Load Balance Mode:		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

xxxxxxx : Data is encrypted.

xxxxxxx : Data isn't encrypted.

## Linux

## VPN Server Kurulumu

1. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin, **Preshared Key** girin ve VPN istemcisinin arayacağı **WAN Profilini** 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. Yeni bir profil eklemek için **Add'e** tıklayın.
  - Basic sekmesinde, **Profile** name girin ve profili etkinleştirmek için **Enable'ı** işaretleyin.
  - **Auto Dial-Out** ve **For Remote Dial-In User** ayarlarını **Disabled** olarak bırakın.
  - **Dial-Out Through** için VPN istemcisinin arayacağı **WAN Interface'ini** seçin.
  - **Local IP /Subnet Mask'da** VPN Server'ın 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'da** eş VPN routerının LAN ağını girin.
  - IKE Protocol için **IKEv1** ve IKE phase1 için **Main Mode** seçeneğini seçin.
  - Pre-Shared Key'i Empty olarak bırakın.
  - Profili kaydetmek için **Apply'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 Client Kurulumu

1. VPN and Remote Access >> VPN Profile >> IPsec'e gidin. Yeni bir profil eklemek için Add'e tıklayın.
  - Basic sekmesinde, Profile name girin ve profili etkinleştirmek için Enable'ı işaretleyin.
  - Auto Dial-Out için Enable'ı işaretleyin.
  - VPN İstemcisinin, Dial-Out Through'dan tüneli arayacağı WAN Interface'ini seçin.
  - Local IP /Subnet Mask'da VPN istemcisinin local Network IP'sini ve subnetini girin.
  - Remote Host'da VPN Server'ın WAN IP'sini veya Domain adını girin.
  - Remote IP/ Subnet Mask'da Eş VPN sunucusunun LAN ağını girin.
  - IKE Protocol için IKEv1 ve IKE phase1 için Main Mode seçeneğini seçin.

- Pre-Shared Key'i Empty olarak bırakın.
- Profili kaydetmek için **Apply**'a tıklayın.

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

IP	Subnet Mask
No items	

More Remote Subnet :

IKE Protocol :

IKE Phase 1 :  Main Mode  Aggressive Mode

Auth Type :

Preshared Key :  (If Aggressive mode is disabled)

Security Protocol :

Yukarıdaki konfigürasyonlar tamamlandıktan sonra VPN İstemcisi IPsec tüneline otomatik olarak çevirir. 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 :    Auto Refresh : 1 Minute

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)

