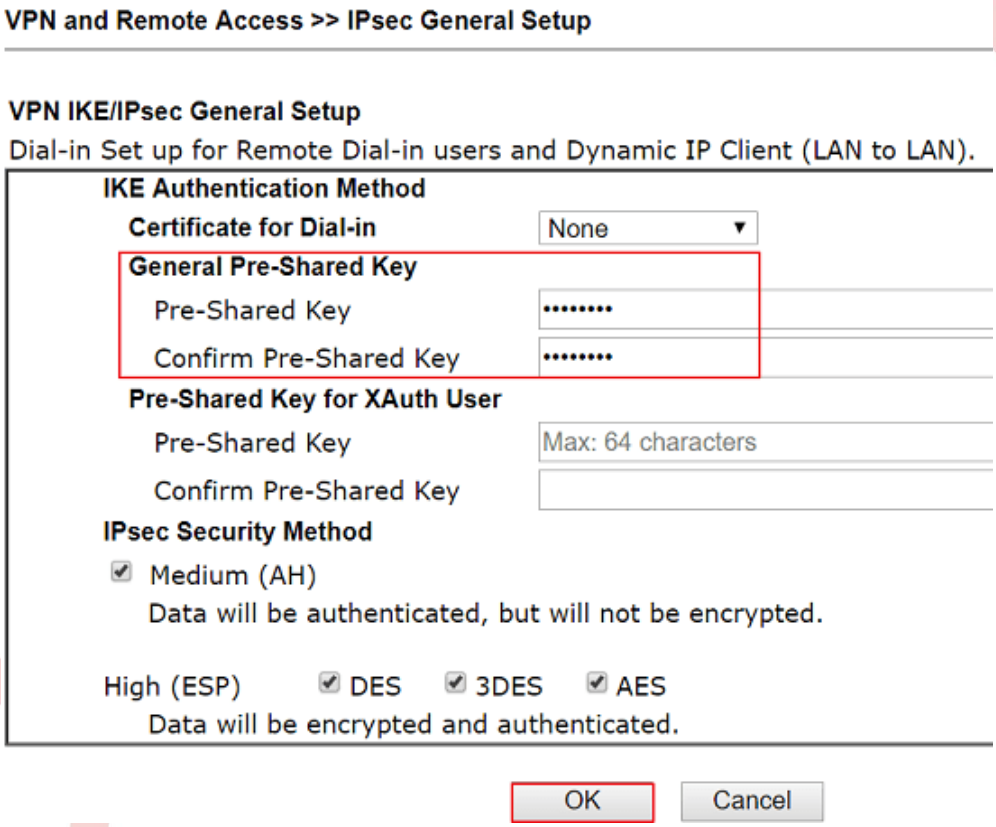
# DRAYTEK ROUTERLARI ARASINDA IPSEC TÜNELİ MAIN MODU (DİNAMİK IP'Lİ İSTEMCİ)

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 Aggresive modda IPsec VPN'i kullanın.

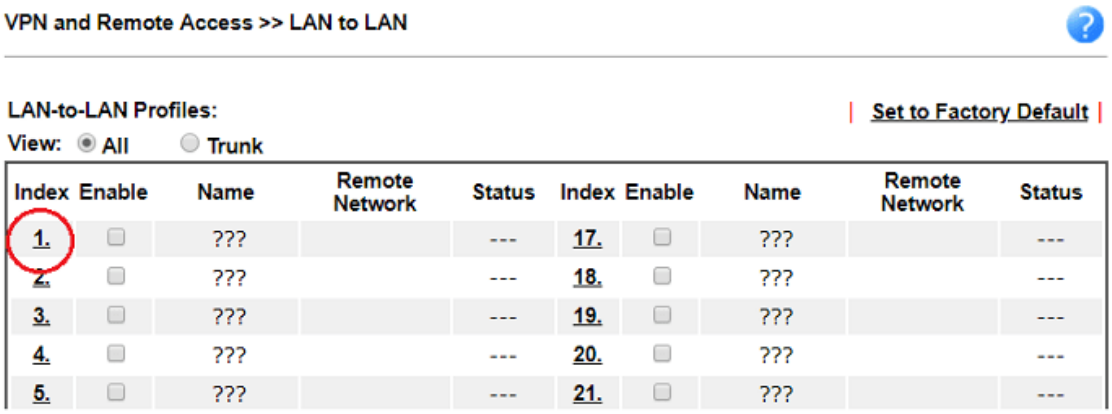
## DrayOS

### 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.

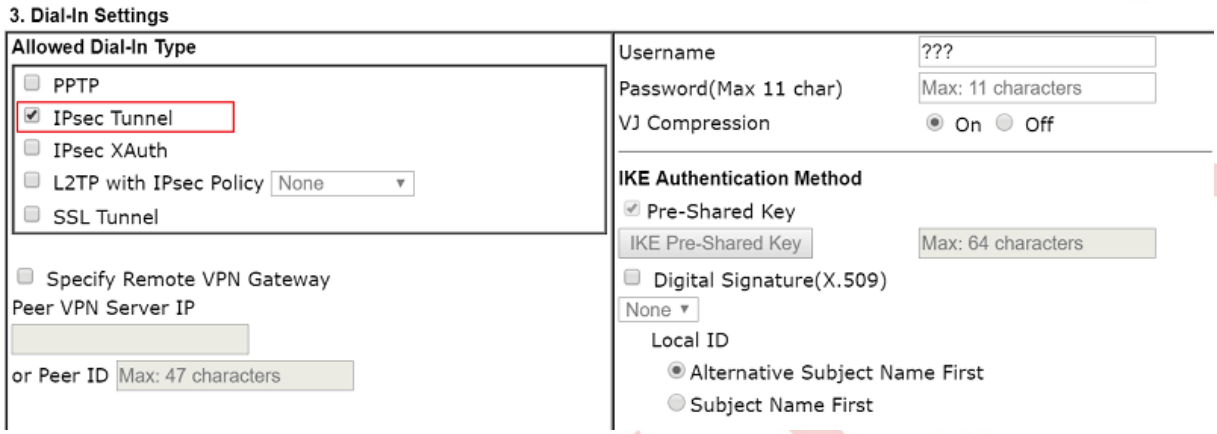



2. Eş VPN istemcisi routerı için **VPN and Remote Access >> LAN to LAN** sayfasında VPN LAN-to-LAN profili oluşturun vr yeni bir profil eklemek için kullanılabilir bir indexe tıklayın.

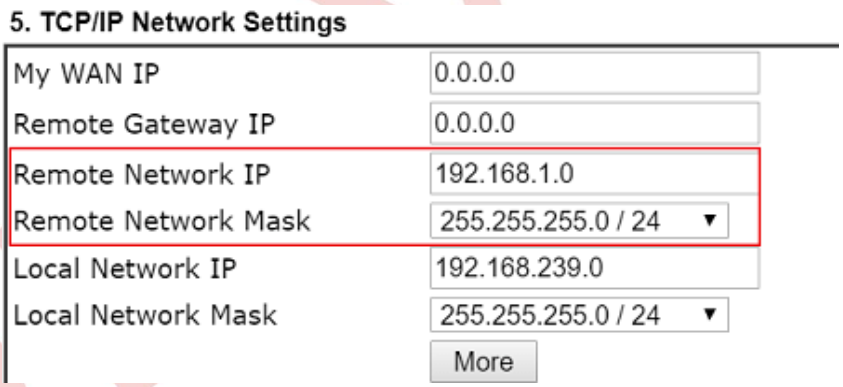



| Index | Enable | Name | Remote Network | Status | Index | Enable | Name | Remote Network | Status |
|---|---|---|---|---|---|---|---|---|---|
| 1. | ☐ | ??? | | --- | 17. | ☐ | ??? | | --- |
| 2. | ☐ | ??? | | --- | 18. | ☐ | ??? | | --- |
| 3. | ☐ | ??? | | --- | 19. | ☐ | ??? | | --- |
| 4. | ☐ | ??? | | --- | 20. | ☐ | ??? | | --- |
| 5. | ☐ | ??? | | --- | 21. | ☐ | ??? | | --- |

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

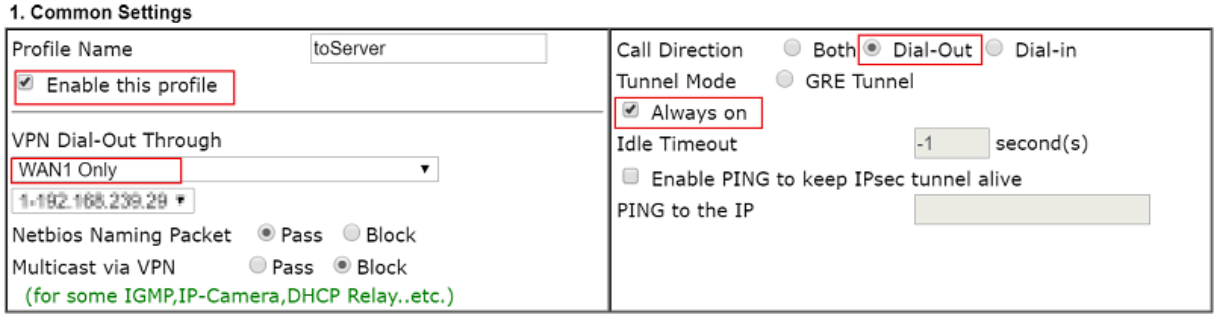



   f. TCP/IP Network Settings'de **Remote Network IP and Mask** için VPN istemcisinin kullandığı IP subnetini girin.
   g. VPN profilini kaydetmek için **OK'a** tıklayın.

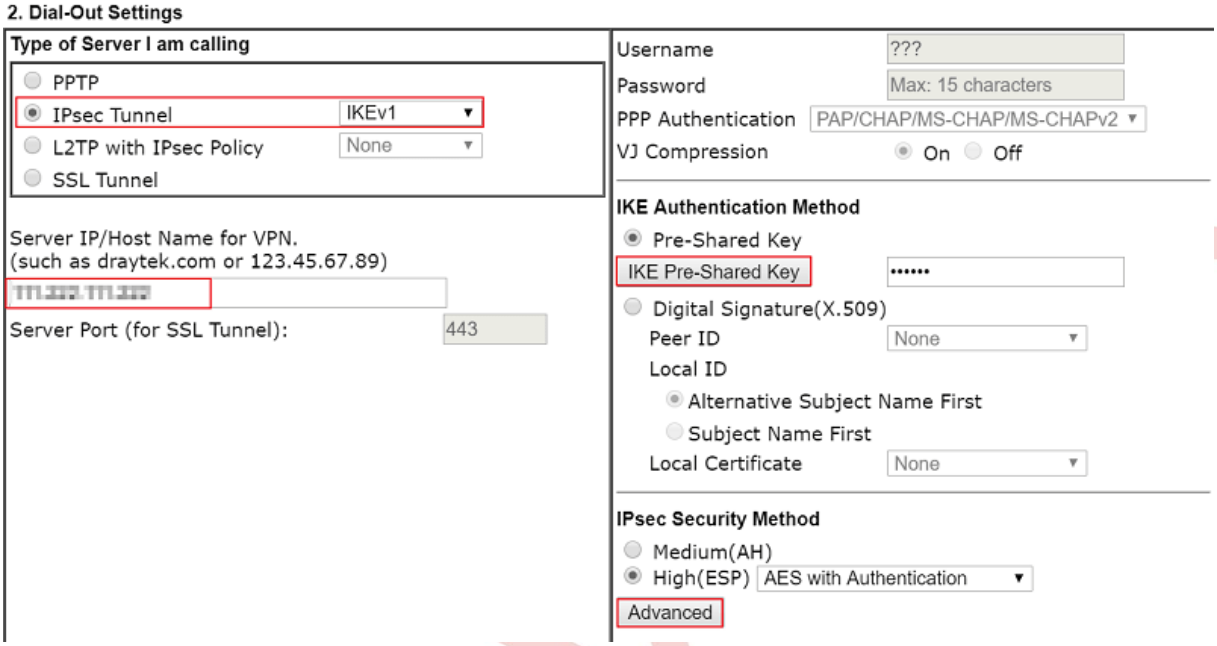



**VPN Client Kurulumu**

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.

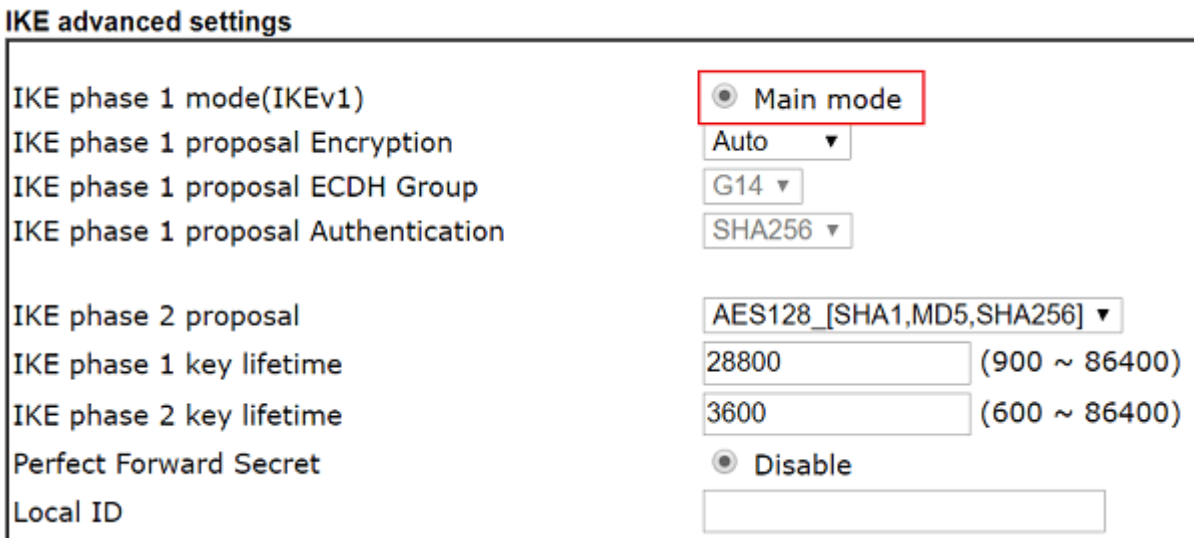


- Dial-Out Settings'de **IPsec Tunnel'i** seçin.
- **Server IP/Host Name for VPN'de** VPN sunucusunun WAN IP'sini veya domain adını girin.
- VPN Server'da yapılandırılan aynı **IKE Pre-Shared Key'i** girin.
- IPsec Security Method'da **Advanced'a tıklayın.**

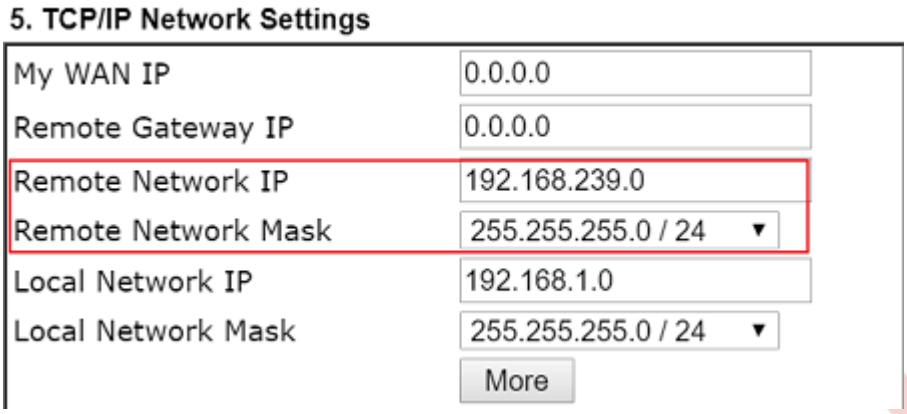



IKE Advanced Settings'de:

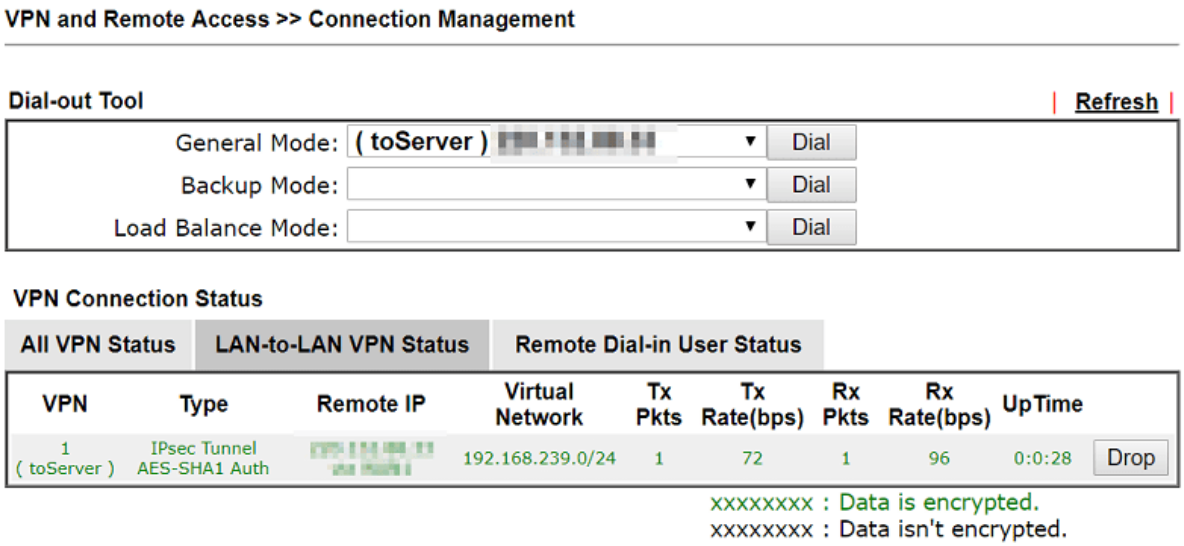
- **IKE phase 1 mode** için **Main Mode** seçin.
- Phase 1 and phase 2 proposal'ın security metodalarını kullandığından emin olun.
- Kaydetmek için **OK'a** tıklayın.




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.



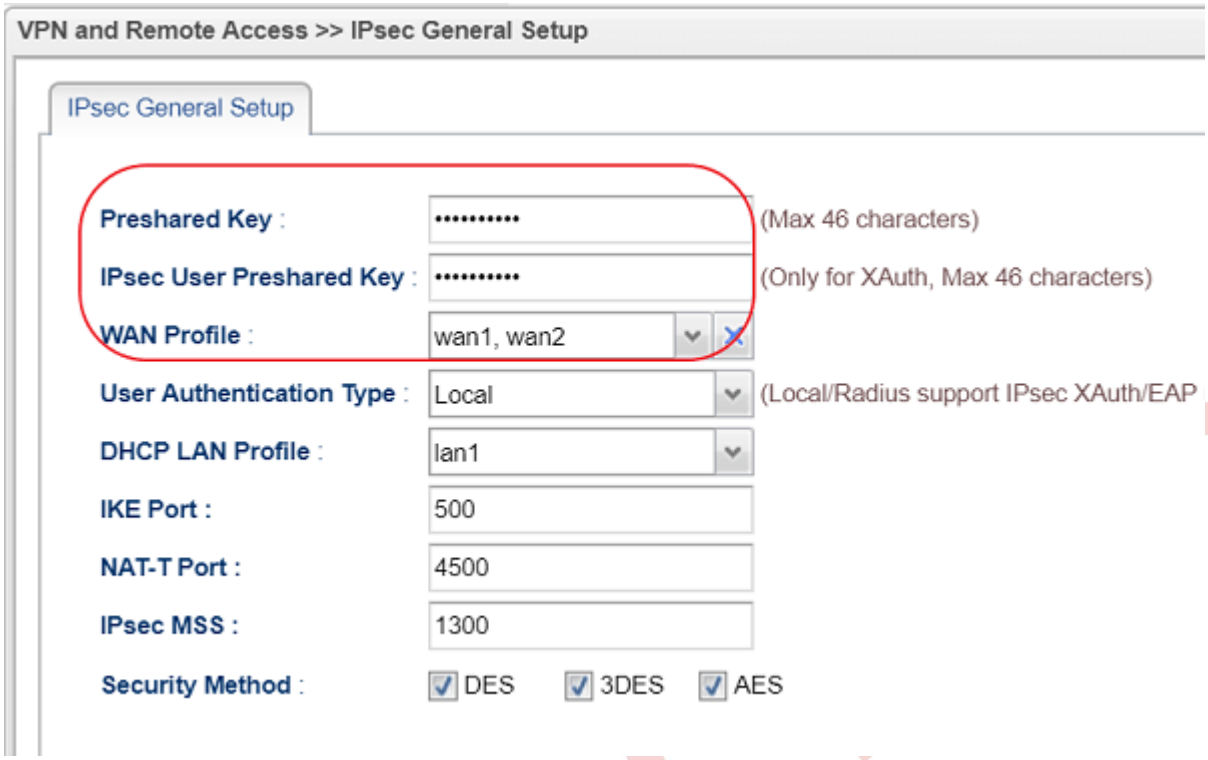

Yukarıdaki konfigürasyonlar tamamlandıktan sonra VPN İstemcisi IPsec tünelini otomatik olarak çevirir. VPN durumunu VPN and Remote Access >> Connection Management sayfasından kontrol edebiliriz.



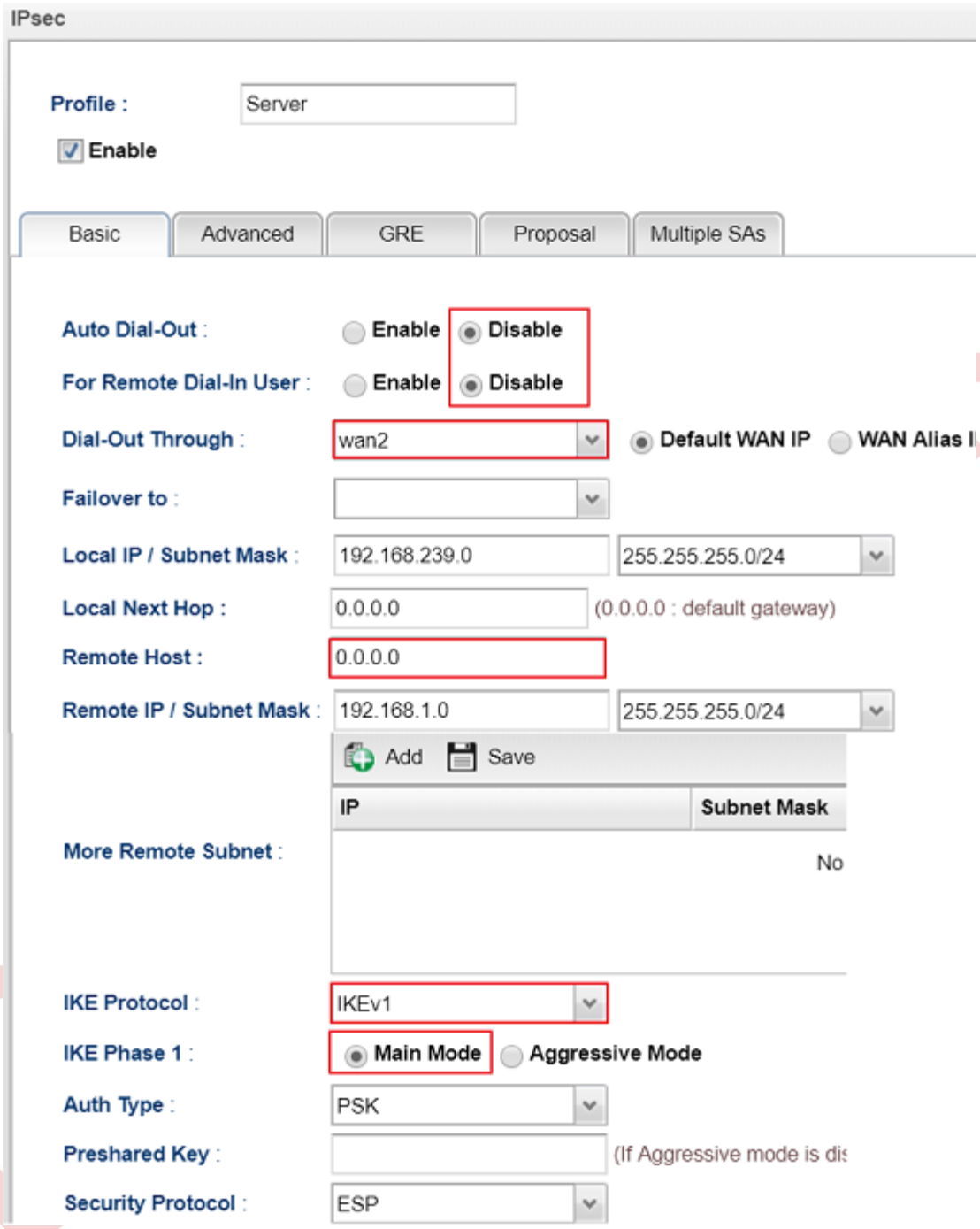

**Linux**

**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.



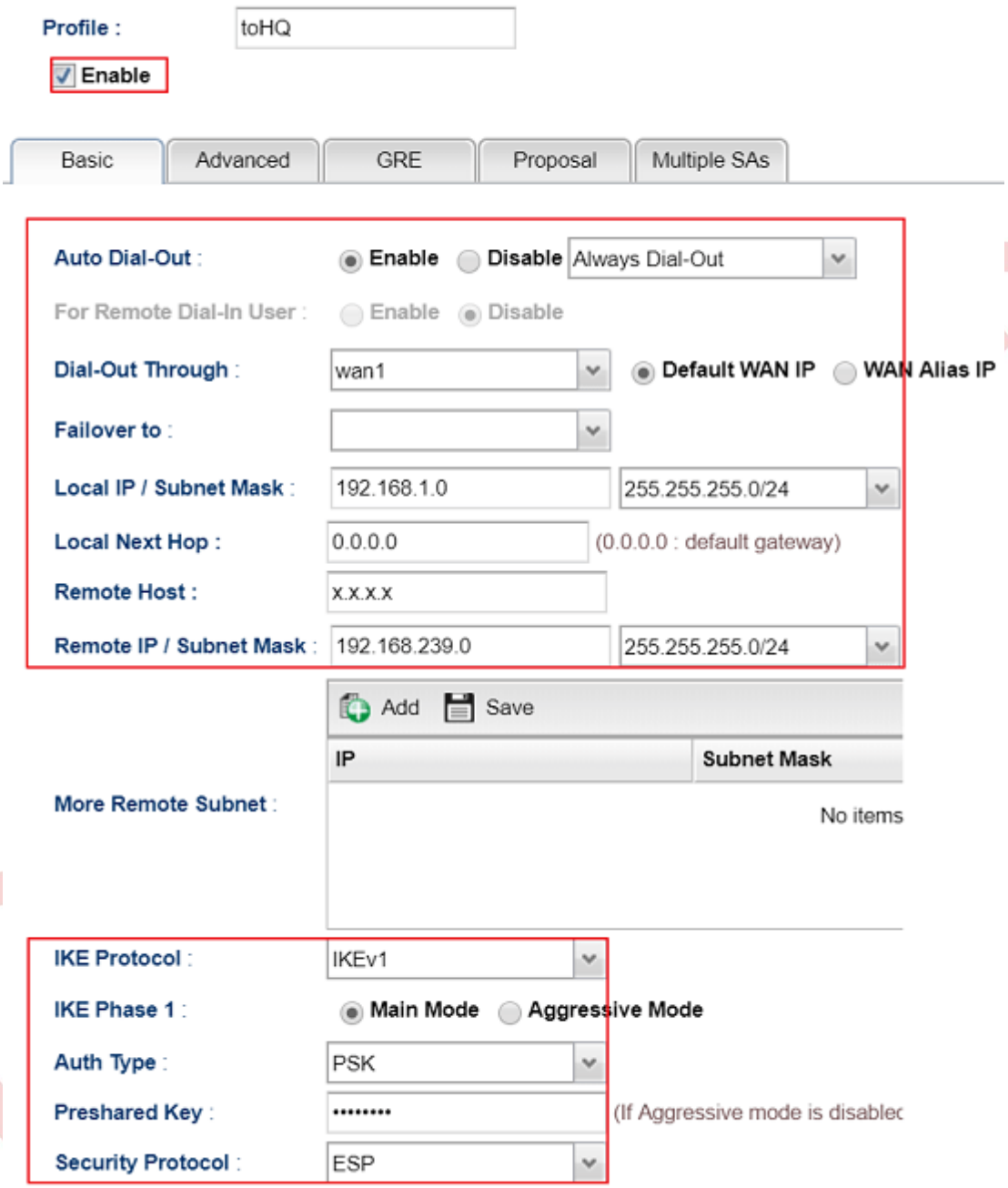

2. **VPN and Remote Access >> VPN Profile >> IPsec'e** gidin. Yeni bir profil eklemek için **Add'e** tıklayın.
   - Basic sekmesinde, **Profile** name girin ve profili etkinleştirmek için **Enable'ı** işaretleyin.
   - **Auto Dial-Out** ve **For Remote Dial-In User** ayarlarını **Disabled** olarak bırakın.
   - **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.



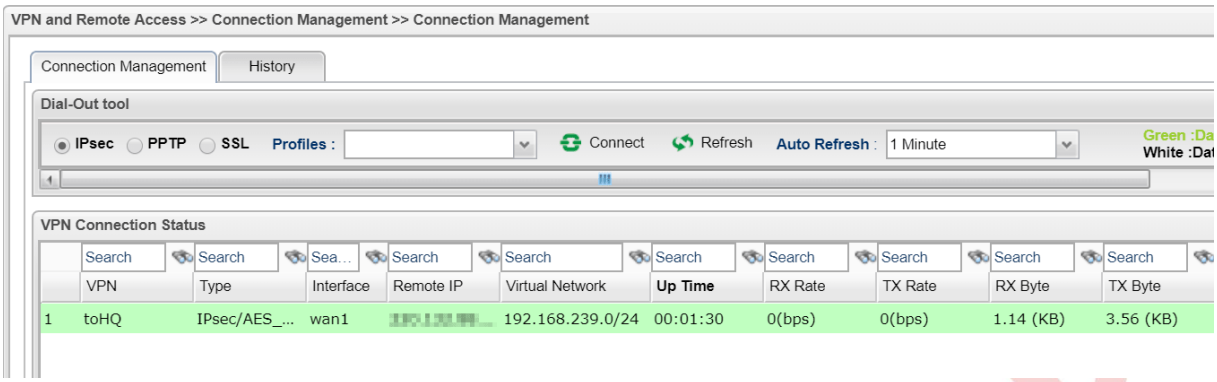

**VPN Client Kurulumu**

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 İnterface'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.




Yukarıdaki konfigürasyonlar tamamlandıktan sonra VPN İstemcisi IPsec tünelini 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 :
Connect
Refresh
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)