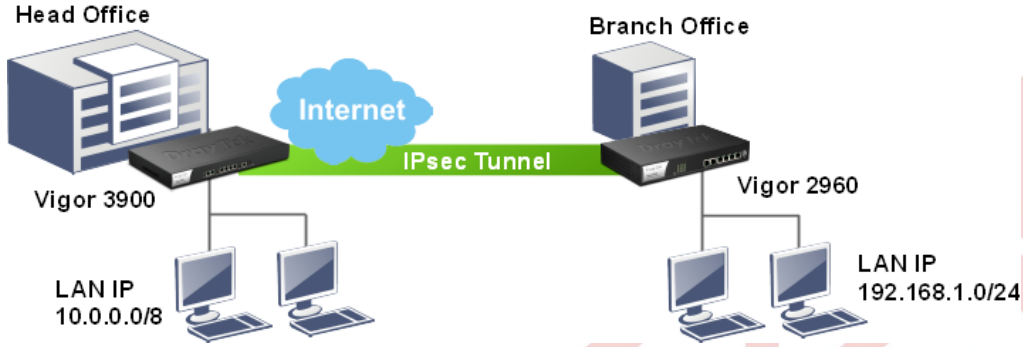


## VIGOR3900'DAKİ TÜM TRAFİK VPN TÜNELİNE NASIL GÖNDERİLİR

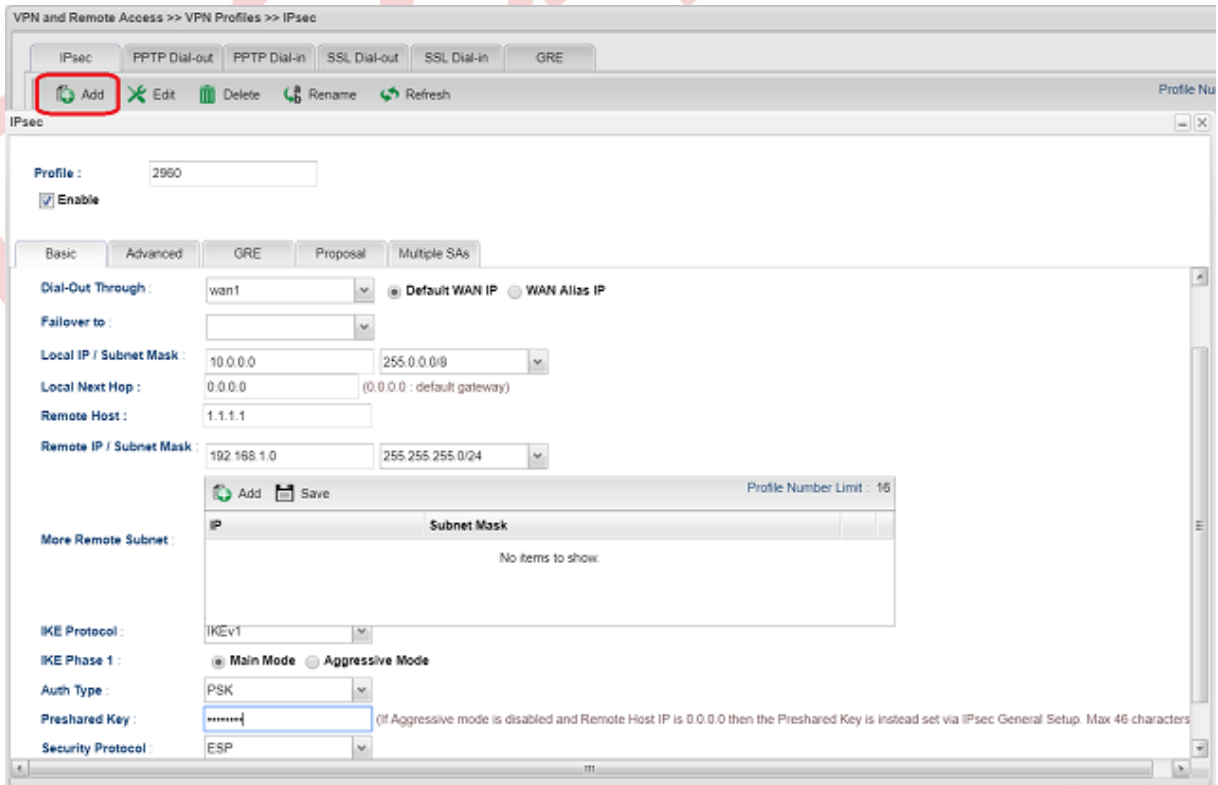
Vigor3900'ün genel merkezde ve Vigor2960'ın şube ofisinde olduğunu varsayarsak, ağ Yöneticisi iki ofis arasında bir VPN oluşturmak ve Vigor2960'ın tüm trafiğini bu VPN tüneline göndermek istiyor. Aşağıdaki örnekler size bu amacı gerçekleştirmenin iki yolunu gösterecektir.



### A. IPsec + Route Policy üzerinden GRE

#### Genel Merkezdeki Vigor3900'ün Konfigürasyonları

1. Yeni bir VPN profili ekleyin: **VPN and Remote Access >> VPN Profiles** sayfasına gidin. **Add**'e tıklayın ve temel ayarları yapılandırın:
  - a. **Enable**'yi işaretleyin.
  - b. Local IP / Subnet'i 10.0.0.0/8 olarak girin.
  - c. Remote Host'u Vigor2960'ın WAN IP'si olarak girin.
  - d. Vigor2960'ın LAN IP'si olarak Remote IP/Subnet girin.
  - e. IKE Phase 1 için **Main Mode** seçin.
  - f. Preshared anahtarını girin.
  - g. Security Protocol için **ESP** seçin.



2. VPN profili için GRE ayarlarının yapılandırılması.
  - a. **GRE function** için “Enable”yi seçin.
  - b. Local GRE IP’yi girin. (Şubedeki Vigor2960’taki Remote GRE IP ile aynı olmalıdır.)
  - c. Remote GRE IP’yi girin. ( Şubedeki Vigor2960’taki Local GRE IP ile aynı olmalıdır.)
  - d. Ayarları uygulamak için **Apply**’a tıklayın.

The screenshot shows the IPsec configuration window with the following settings:

- Profile : 2960
- Enable
- Basic | **Advanced** | GRE | Proposal | Multiple SAs
- Enable GRE Function :  Enable  Disable
- Local GRE IP : 111.111.111.39
- Remote GRE IP : 111.111.111.29
- Auto Generate GRE Key :  Enable  Disable
- Note : It is necessary create Load Balance Pool/Rule in VPN Trunk Management for making GRE tunnels work.

3. Yeni VPN Load Balance havuzu oluşturun: **VPN and Remote Access >> VPN Trunk Management >> Load Balance Pool** sayfasına gidin. Ardından yeni bir profil oluşturmak için **Add**’e tıklayın.
  - a. Profil adı girin.
  - b. Oluşturduğumuz VPN profilini seçmek ve Weight vermek için **Add**’e tıklayın. (Burada sadece GRE ayarlı VPN profili listelenir.)
  - c. Kaydetmek için **Apply**’a tıklayın.

The screenshot shows the Load Balance Pool configuration window with the following settings:

- Profile : pool
- Mode : Load Balance
- Add Save Profile Number Limit : 16

Interface	Weight
Interface : 2960	1

4. VPN Load Balance Kuralı oluşturun: **VPN and Remote Access >> VPN Trunk Management >> Load Balance Rule** sayfasına gidin. Ardından yeni bir profil oluşturmak için **Add**’e tıklayın.
  - a. Profil adını girin.
  - b. Protokol için **ALL** seçeneğini seçin.
  - c. Source(kaynak) IP adresini girin.

- d. Source Mask 'ı girin.
- e. Destination(hedef) IP adresini girin.
- f. Destination Mask'ı girin.
- g. Load Balance Pool için VPN Trunk Load Balance Pool seçeneğini seçin.

VPN and Remote Access >> VPN TRUNK Management >> Load Balance Rule

Load Balance Pool Load Balance Rule

Add Edit Delete Refresh

Load Balance Rule

Profile : to29

Enable

Protocol : ALL

Source IP Address : 10.0.0.0 (Optional)

Source Mask : 255.0.0.0/8 (Optional)

Destination IP Address : 192.168.1.0 (Optional)

Destination Mask : 255.255.255.0/24 (Optional)

Load Balance Pool : pool

Apply Cancel

**Note:** VPN Load Balance Rule olan VPN Trunk tüneline ne tür bir trafik geçmesi gerektiğini tanımlamak gerekir. Aksi takdirde, trafik VPN Trunk tüneline geçemez.

#### Şubedeki Vigor2960'daki Konfigurasyonlar

1. Yeni bir VPN profili ekleyin: **VPN and Remote Access >> VPN Profiles** sayfasına gidin. **Add**'e tıklayın ve temel ayarları yapılandırın.
  - a. **Enable**'yi etkinleştirin.
  - b. Auto Dial-Out için **Enable**'yi işaretleyin ve Always Dial-Out seçeneğini seçin.
  - c. Local IP/Subnet'i 192.168.1.0/ 255.255.255.0 olarak girin.
  - d. Remote Host IP'yi Vigor3900'ün WAN IP'si olarak girin.
  - e. Remote IP/ Subnet'i 10.0.0.0/ 255.0.0.0 olarak girin.
  - f. IKE Phase 1 için **Main Mode** seçeneğini seçin.
  - g. Preshared anahtarını girin.
  - h. Security Protocol için ESP seçeneğini seçin.

VPN and Remote Access >> VPN Profiles >> IPsec

IPsec PPTP Dial-out PPTP Dial-in SSL Dial-out SSL Dial-in GRE

**Add** Edit Delete Rename Refresh

Profile : 3900

Enable

Basic Advanced GRE Proposal Multiple SAs

Dial-Out Through : wan1  Default WAN IP  WAN Alias IP

Fallover 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 : 2.2.2.2

Remote IP / Subnet Mask : 10.0.0.0 255.0.0.0/8

More Remote Subnet :

IP	Subnet Mask
No items to show.	

IKE Protocol : IKEV1

IKE Phase 1 :  Main Mode  Aggressive Mode

Auth Type : PSK

Preshared Key : \*\*\*\*\* (If Aggressive mode is disabled and Remote Host IP is 0.0.0.0 then the Preshared Key is instead set via IPsec General Setup. Max 46 characters)

Security Protocol : ESP

2. GRE ayarlarını ya da VPN profilini yapılandırın.
  - a. Enable GRE function için **Enable**'yi işaretleyin.
  - b. Local GRE IP'sini girin. (Merkezdeki Vigor3900'deki Remote GRE IP'si ile aynı olmalıdır.)
  - c. Remote GRE IP'sini girin. (Merkezdeki Vigor3900'deki Local GRE IP'si ile aynı olmalıdır.)
  - d. Ayarları kaydetmek için **Apply**'a tıklayın.

IPsec

Profile : 3900

Enable

Basic Advanced GRE Proposal Multiple SAs

Enable GRE Function :  Enable  Disable

Local GRE IP : 111.111.111.29

Remote GRE IP : 111.111.111.39

Auto Generate GRE Key :  Enable  Disable

**Note :**  
It is necessary create Load Balance Pool/Rule in VPN Trunk Management for making GRE tunnels work.

3. VPN Load Balance Havuzu oluřturun: **VPN and Remote Access >> VPN Trunk Management >> Load Balance Pool** sayfasına gidin. Ardından **Add**'e tıklayın ve yeni profil oluřturun.
  - a. Profil adını girin.
  - b. Yeni oluřturulan VPN profilini seçmek ve Weight vermek için **Add**'e tıklayın. (Burada sadece GRE ayarlı VPN Profili listelenir.)
  - c. Kaydetmek için **Apply**'a tıklayın.

Load Balance Pool

Profile : loop

Mode : Load Balance

Add Save

Interface	Weight
Interface : to3900	1

4. VPN Load Balance Kuralı oluřturun: **VPN and Remote Access >> VPN Trunk Management >> Load Balance Rule** sayfasına gidin. Ardından profil oluřturmak için **Add**'e tıklayın.
  - a. Profil adını girin.
  - b. Protocol için **ALL** seçeneğini seçin.
  - c. Source IP adresini girin.
  - d. Source Mask'ı girin.
  - e. Destination IP adresini girin.
  - f. Destination Mask'ı girin.
  - g. Load Balance Pool için VPN Trunk Load Balance Pool seçeneğini seçin.

VPN and Remote Access >> VPN TRUNK Management >> Load Balance Rule

Load Balance Pool Load Balance Rule

Add Edit Delete Refresh

Profile	Enable	Protocol	Source IP Address
Load Balance Rule			

Profile : to39

Enable

Protocol : ALL

Source IP Address : 192.168.1.0 (Optional)

Source Mask : 255.255.255.0/24 (Optional)

Destination IP Address : 10.0.0.0 (Optional)

Destination Mask : 255.0.0.0/8 (Optional)

Load Balance Pool : loop

Apply Cancel

5. Yukarıdaki konfigürasyonları tamamladıktan sonra VPN tüneli artık dialed-up olmuştur. **VPN and Remote Access >> Connection Management** sayfasından VPN durumunu kontrol edebilirsiniz. Ayrıca yerel bir bilgisayarın uzaktaki bir bilgisayardan ping yanıtı alıp almayacağını kontrol edebilirsiniz.

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

Connection Management History

Dial-Out tool

IPsec  PPTP Profiles :    Auto Refresh : 1 Minute

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Network	Up Time
1	to3900	IPsec/3DES_HMA...	wan1	220.132.88.33	111.111.111.39/32 00:43:12

命令提示字元 - ping 10.11.1.254 -t

```
C:\Users\u1>ping 10.11.1.254 -t

Pinging 10.11.1.254 with 32 bytes of data:
Reply from 10.11.1.254: bytes=32 time=33ms TTL=63
Reply from 10.11.1.254: bytes=32 time=32ms TTL=63
Reply from 10.11.1.254: bytes=32 time=32ms TTL=63
Reply from 10.11.1.254: bytes=32 time=33ms TTL=63
Reply from 10.11.1.254: bytes=32 time=33ms TTL=63
Reply from 10.11.1.254: bytes=32 time=33ms TTL=63
Reply from 10.11.1.254: bytes=32 time=39ms TTL=63
Reply from 10.11.1.254: bytes=32 time=32ms TTL=63
Reply from 10.11.1.254: bytes=32 time=32ms TTL=63
Reply from 10.11.1.254: bytes=32 time=34ms TTL=63
Reply from 10.11.1.254: bytes=32 time=33ms TTL=63
Reply from 10.11.1.254: bytes=32 time=32ms TTL=63
```

6. Tüm trafiği VPNTrunk Tünelinden geçmeye zorlamak için bir Policy Rule oluşturun: **Routing >> Policy Route** sayfasına gidin ve yeni bir kural eklemek için **Add**'e tıklayın.
- Profil adını girin.
  - Enable'yi işaretleyin.
  - Protocol için **ALL** seçeneğini seçin.
  - Source Type için **ANY** seçeneğini seçin.
  - Destination Type için **ANY** seçeneğini seçin.
  - Out-going Rule için VPN Trunk LB Pool seçeneğini seçin.
  - Load Balance Pool için VPN Load Balance Profile seçeneğini seçin.
  - Mode için NAT seçeneğini seçin.
  - Kaydetmek için **Apply**'a tıklayın.

Routing >> Policy Rule

Policy Rule

Auto Refresh : 1 Minute

Policy Rule

Profile : toANY

Enable

Priority : High

Protocol : ALL

Time

Time Objects :

Source

Source Type : Any

Destination

Destination Type : Any

Route Rule

Out-going Rule : VPN Trunk LB Pool

Load Balance Pool : loop

Mode : NAT

Failover to Next Rule :  Enable  Disable

when interface down

when target ping Fail for 3 seconds

Failback (Quick Recover) :  Enable  Disable

Apply Cancel

1. Tüm trafiğin VPN tüneline geçip geçmediğini görebilmek için traceroute komutu **tracert -d** kullanarak öğrenebilirsiniz. Aşağıdaki ekran görüntüsündeki traceroute sonucundan ikinci düğümün Vigor3900'ün LAN IP'si olduğunu görüyoruz ve bu 8.8.8.8'e giden trafiğin VPN tüneli üzerinden gönderildiği anlamına geliyor.

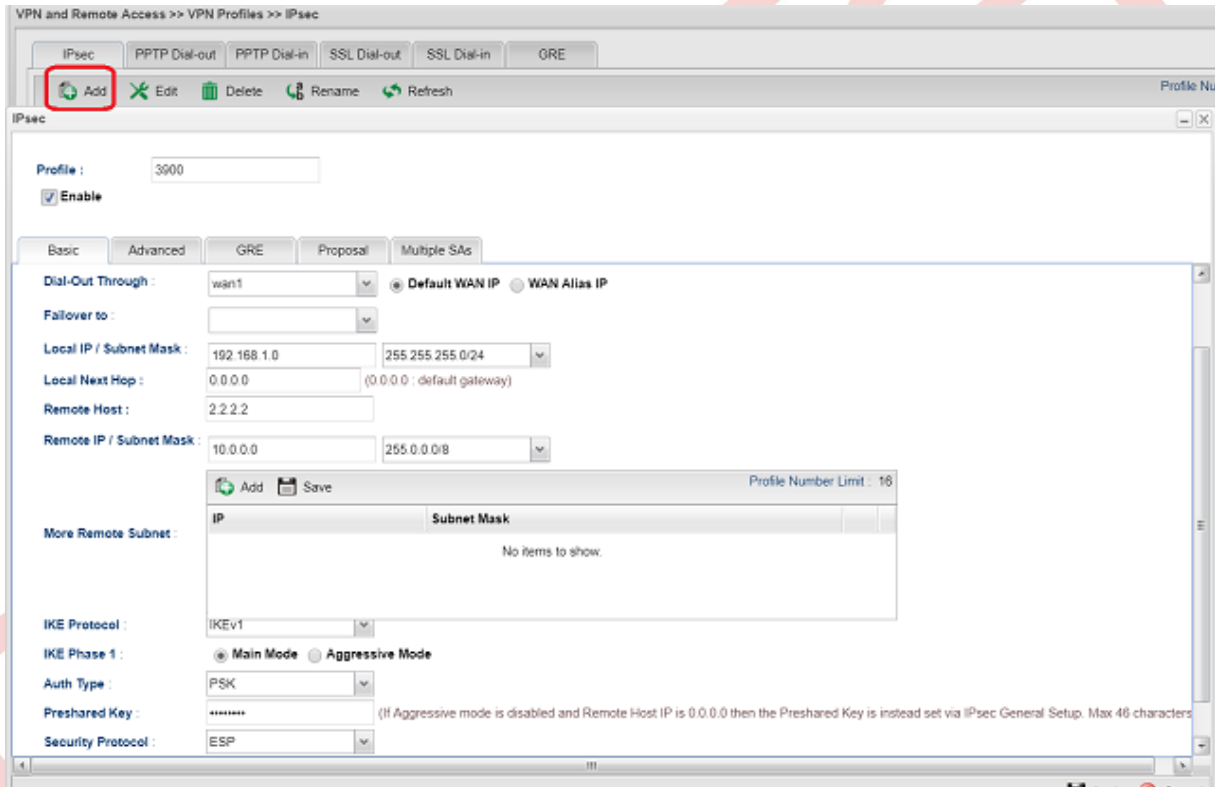
```

CAL 命令提示字元 - tracert -d 8.8.8.8
Reply from 172.16.2.8: bytes=32 time=32ms TTL=62
Ping statistics for 172.16.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 34ms, Average = 33ms
C:\Users\u1>tracert -d 8.8.8.8
Tracing route to 8.8.8.8 over a maximum of 30 hops
  0  1 ms  <1 ms  <1 ms  192.168.1.1
  1  34 ms  33 ms  33 ms  10.11.1.254
  2  39 ms  55 ms  38 ms  168.95.98.254
  3  *      39 ms  38 ms  168.95.25.210
  4  47 ms  41 ms  38 ms  220.128.7.46
  5  43 ms  42 ms  43 ms  220.128.2.30
  6  43 ms  54 ms  43 ms  220.128.9.81
  7  41 ms  41 ms  41 ms  220.128.9.225
  8  42 ms  41 ms  41 ms  72.14.196.3
  9  51 ms  51 ms  51 ms  72.14.233.20
 10  51 ms  50 ms  51 ms  209.85.252.213
 11  54 ms  53 ms  53 ms  72.14.237.177
 12  *      *
 13
  
```

## B. NAT Policy

### Şubedeki Vigor2960'ın Konfigürasyonları

1. Yeni bir VPN profili ekleyin: **VPN and Remote Access >> VPN Profiles** sayfasına gidin. **Add**'e tıklayın ve temel ayarları yapılandırın.
  - a. **Enable**'yi etkinleştirin.
  - b. Auto Dial-Out için **Enable**'yi işaretleyin ve Always Dial-Out seçeneğini seçin.
  - c. Local IP/Subnet'i 192.168.1.0/ 255.255.255.0 olarak girin.
  - d. Remote Host IP'yi Vigor3900'ün WAN IP'si olarak girin.
  - e. Remote IP/ Subnet'i 10.0.0.0/ 255.0.0.0 olarak girin.
  - f. IKE Phase 1 için **Main Mode** seçeneğini seçin.
  - g. Preshared anahtarını girin.
  - h. Security Protocol için ESP seçeneğini seçin.



2. Advanced sekmesinde Enable NAT Policy için "Enable" seçeneğini seçin.
  - a. Ara yüzün tüm trafiği göndermesi için Vigor2960'ların LAN'ını çevirecek bir ağ girin.

Set VPN as Default Gateway için "Enable"



IPsec

Profile : 3900

Enable

Basic Advanced GRE Proposal Multiple SAs

Phase1 Key Life Time : 28800 seconds

Phase2 Key Life Time : 3600 seconds

Perfect Forward Secrecy Status :  Enable  Disable

Dead Peer Detection Status :  Enable  Disable

DPD Delay : 30 seconds

DPD Timeout : 120 seconds

Ping to Keep Alive :  Enable  Disable

Route / NAT Mode : Route

Source IP : auto\_detect\_srcip

**Apply NAT Policy :  Enable  Disable**

**Translated Local Network : 192.168.2.0 255.255.255.0/24**

**Set VPN as Default Gateway :  Enable  Disable**

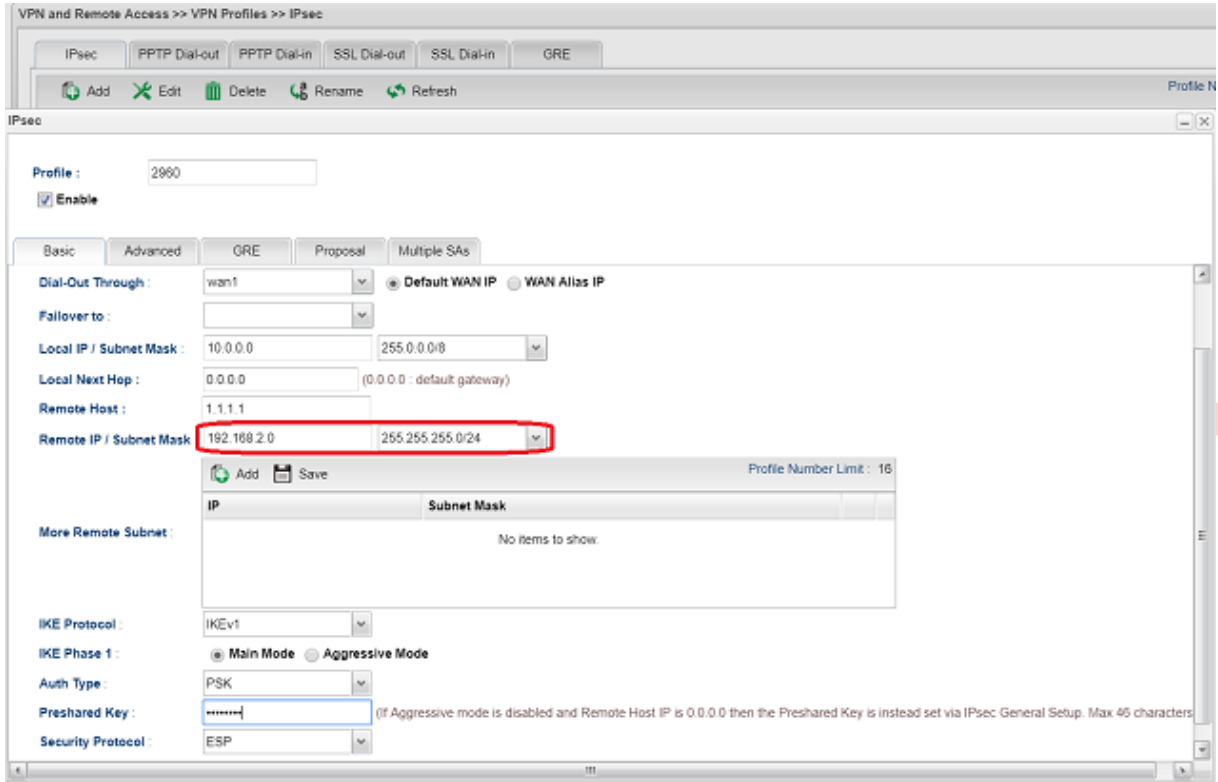
Netbios Naming Packet :  Enable  Disable

Multicast via VPN :  Enable  Disable

RIP via VPN :  Enable  Disable

### Merkezdeki Vigor3900'ün Konfigürasyonları

1. Yeni bir VPN profili ekleyin: **VPN and Remote Access >> VPN Profiles** sayfasına gidin. **Add**'e tıklayın ve temel ayarları yapılandırın.
  - a. **Enable**'yi etkinleştirin.
  - b. Local IP/Subnet'i 10.0.0.0 olarak girin.
  - c. Remote Host IP'yi Vigor2960'ın WAN IP'si olarak girin.
  - d. Remote IP/ Subnet'i Vigor2960'ın dönüştürülmüş network IP'si olarak girin.
  - e. IKE Phase 1 için **Main Mode** seçeneğini seçin.
  - f. Preshared anahtarını girin.
  - g. Security Protocol için ESP seçeneğini seçin.



2. Tüm trafiğin VPN tüneline geçip geçmediğini görebilmek için traceroute komutu **tracert -d** kullanılarak öğrenilebilir. Aşağıdaki ekran görüntüsündeki traceroute sonucundan ikinci düğümün Vigor3900'ün LAN IP'si olduğunu görüyoruz ve bu 8.8.8.8'e giden trafiğin VPN tüneli üzerinden gönderildiği anlamına geliyor.

```

命令提示字元 - tracert -d 8.8.8.8
Reply from 172.16.2.8: bytes=32 time=32ms TTL=62
Ping statistics for 172.16.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 34ms, Average = 33ms
C:\Users\ul>tracert -d 8.8.8.8
Tracing route to 8.8.8.8 over a maximum of 30 hops
  0  1 ms    <1 ms   <1 ms   192.168.1.1
  1  34 ms   33 ms   33 ms   10.11.1.254
  2  39 ms   55 ms   38 ms   168.95.98.254
  3  *       39 ms   38 ms   168.95.25.210
  4  47 ms   41 ms   38 ms   220.128.7.46
  5  43 ms   42 ms   43 ms   220.128.2.30
  6  43 ms   54 ms   43 ms   220.128.9.81
  7  41 ms   41 ms   41 ms   220.128.9.225
  8  42 ms   41 ms   41 ms   72.14.196.3
  9  51 ms   51 ms   51 ms   72.14.233.20
 10 51 ms   50 ms   51 ms   209.85.252.213
 11 54 ms   53 ms   53 ms   72.14.237.177
 12 *       *
 13

```