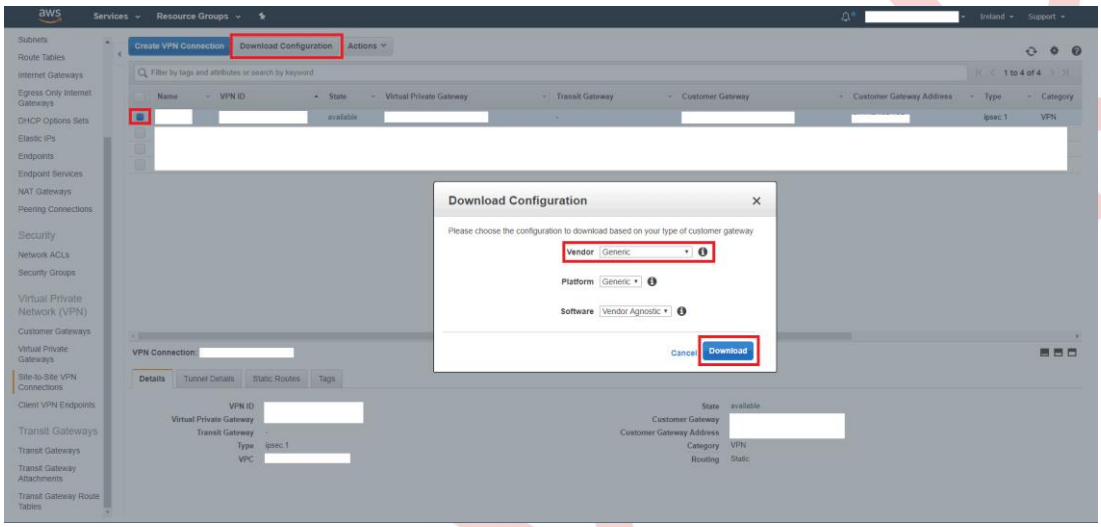
AMAZON VPC VE VIGOR ROUTER ARASINDA IPSEC VPN

Bu makale Vigor Router ve Amazon VPC arasında IPsec VPN tünelinin nasıl kurulacağını göstermektedir.

Amazon VPC Ayarları

1. **AWS >> VPC Dasboard >> Virtual Private (VPN) >> Site-to-Site VPN Connection**'a giriş yapın.
2. **VPN >> Download Configuration >> Generic** 'i seçin. IT sonraki adımlar için gerekli detayları içeren bir .txt dosyası indirecektir.



3. Metin dosyasını WordPad ile açın ve **Pre-Shared Key**'i not edin.

```
===============
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum
requirement of AES128, SHA1, and DH Group 2.
Category "VPN" connections in the GovCloud region have a minimum
requirement of AES128, SHA2, and DH Group 14.
You will need to modify these sample configuration files to take
advantage of AES256, SHA256, or other DH groups like 2, 14-18,
22, 23, and 24.
Higher parameters are only available for VPNs of category "VPN,"
and not for "VPN-Classic".
The address of the external interface for your customer gateway
must be a static address.
Your customer gateway may reside behind a device performing
network address translation (NAT).
To ensure that NAT traversal (NAT-T) can function, you must
adjust your firewall !rules to unblock UDP port 4500. If not
behind NAT, we recommend disabling NAT-T.
  - IKE version              : IKEv1
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : NCF.YJ8_C6XCREyWDHbRuj_Rd90Hugwp
  - Authentication Algorithm : sha1
  - Encryption Algorithm     : aes-128-cbc
  - Lifetime                 : 28800 seconds
  - Phase 1 Negotiation Mode : main
  - Diffie-Hellman           : Group 2
```

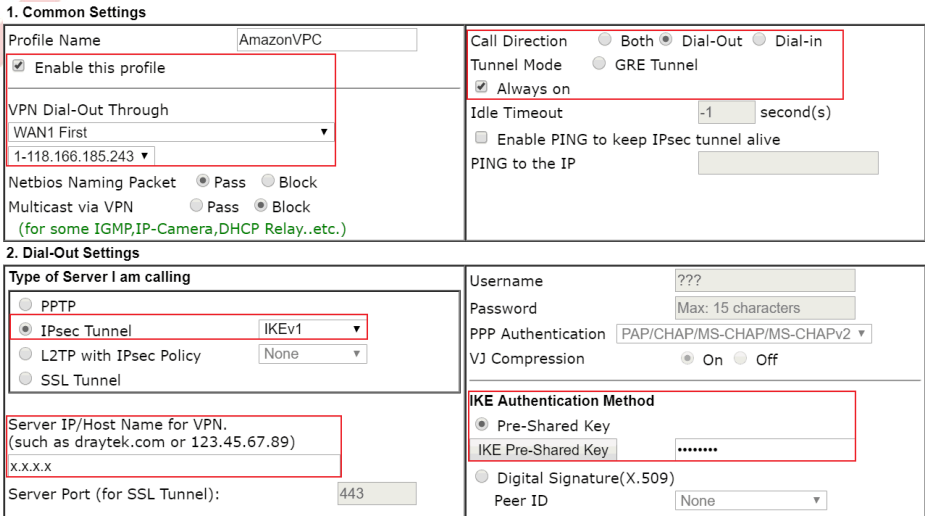
4. AWS sunucusunun WAN IP'si olan **Virtual Gateway IP** 'sini not edin.

```
#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface
that is
associated with the IPSec tunnel. All traffic transmitted to the
tunnel
interface is encrypted and transmitted to the Virtual Private
Gateway.


The Customer Gateway and Virtual Private Gateway each have two
addresses that relate
to this IPSec tunnel. Each contains an outside address, upon
which encrypted
traffic is exchanged. Each also contain an inside address
associated with
the tunnel interface.

The Customer Gateway outside IP address was provided when the
Customer Gateway
was created. Changing the IP address requires the creation of a
new
Customer Gateway.

The Customer Gateway inside IP address should be configured on
your tunnel
interface.

Outside IP Addresses:
  - Customer Gateway                :
  - Virtual Private Gateway         :        X.X.X.X

Inside IP Addresses
  - Customer Gateway                : 169.254.23.170/30
  - Virtual Private Gateway          : 169.254.23.169/30
```

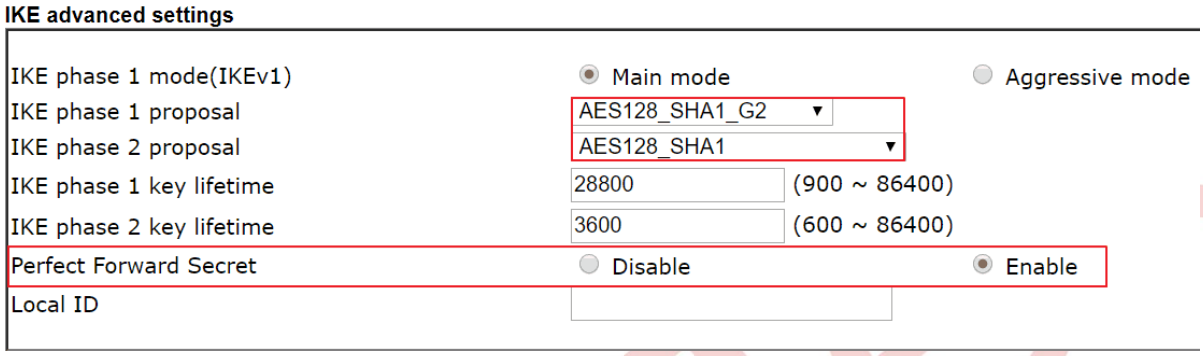
DrayOS

Vigor2926 Ayarları

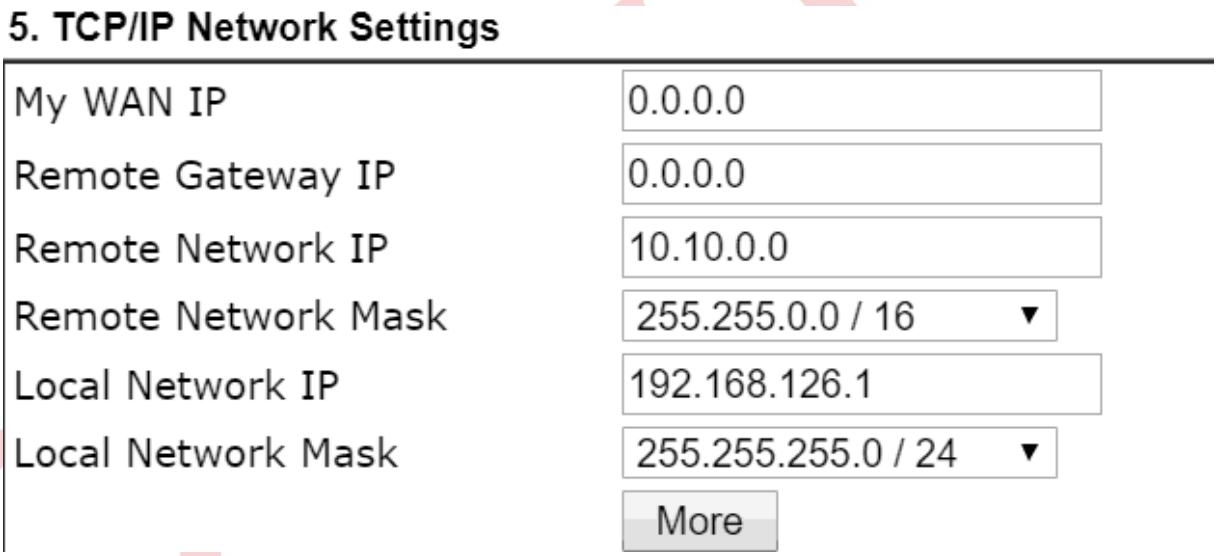
1. **VPN And Remote Access >> VPN Profile** sayfasına gidin. Profili oluşturmak için uygun bir index numarasına tıklayın.
   a. Profil adı girin ve **Enable this profile**'ı etkinleştirin.
   b. Call Direction için **Dial-Out** seçeneğini seçin.
   c. Type of Server için **IPsec Tunnel** seçeneğini seçin.
   d. Server IP'ye Amazon VPC'nin IP'sini girin.
   e. **Pre-Shared Key** girmek için IKE Pre-Shared Key butonuna tıklayın.



2. IPsec Security Method için **AES with Authentication** seçeneğini seçin. IKE gelişmiş ayarlarını açmak için **Advanced** butonuna tıklayın.
   a. IKE phase 1 proposal için **AES128_SHA1_G2** seçeneğini seçin.
   b. IKE phase 2 proposal için **AES128 SHA1** seçeneğini seçin.
   c. **Perfect Forward Secret** için "Enable" seçeneğini seçin.



3. **TCP/IP Network Settings**'de Remote Network IP ve Remote Network Mask için AWS'nin Virtual LAN network IP'sini ve Mask'ını girin. Ardından Apply'a tıklayın.

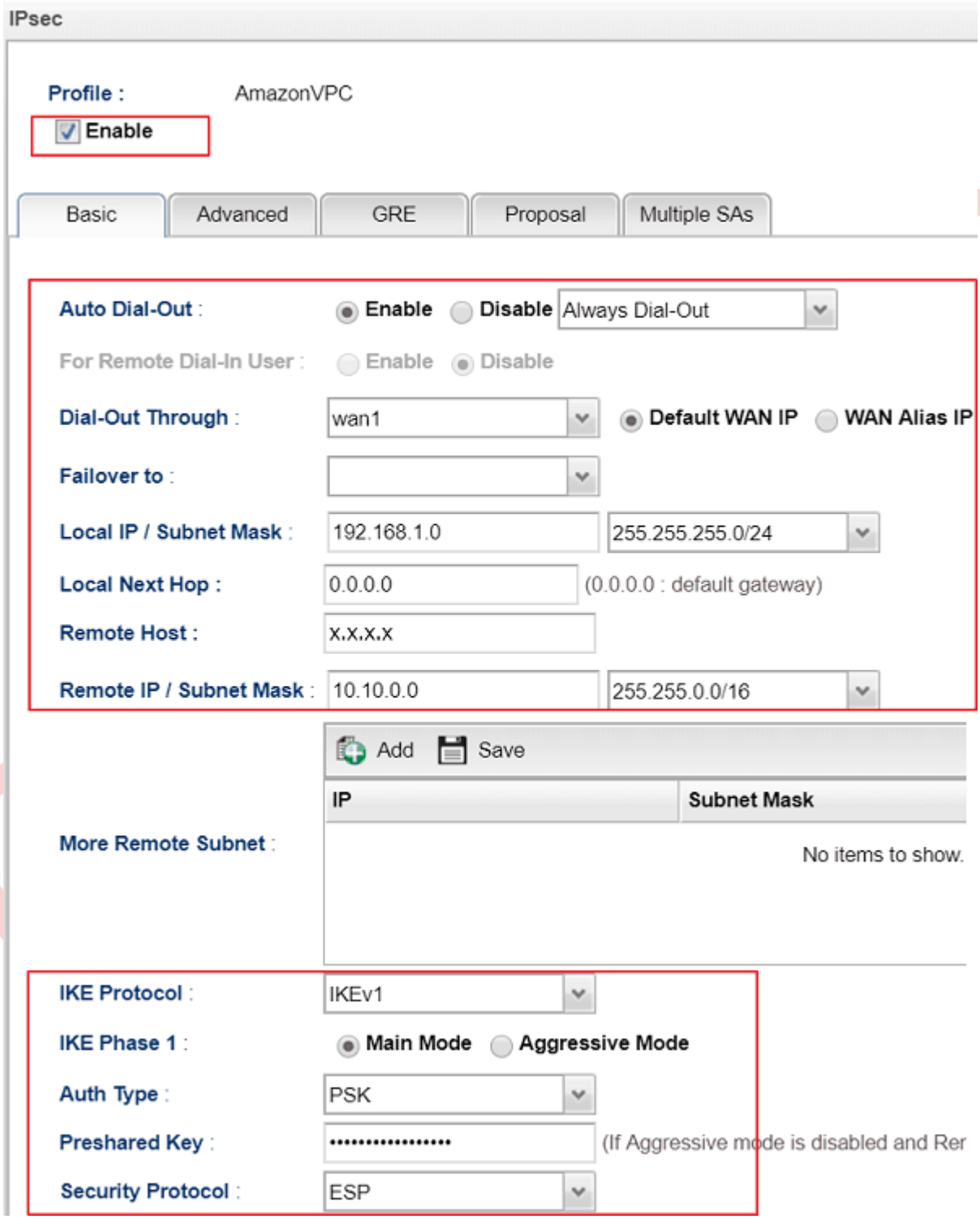


4. 30 saniye bekleyin. **VPN and Remote Access >> Connection Management** sayfasında VPN tünelinin durumunu görebilirsiniz. VPN kurulduktan sonra Vigor Router paketleri VPN tüneline yönlendirecek ancak AWS VPN paketlerini varsayılan policylerden dolayı engellediği için yanıt almayabilir. Vigor Router'ın LAN ağını içerecek şekilde AWS'nizin routera tablosunu güncellemeniz veya trafiği tünele iletmek için bir security grubu eklemeniz / güncellmeniz gerekir. Bu adım ve daha fazla yardım için lütfen AWS desteğine başvurun.

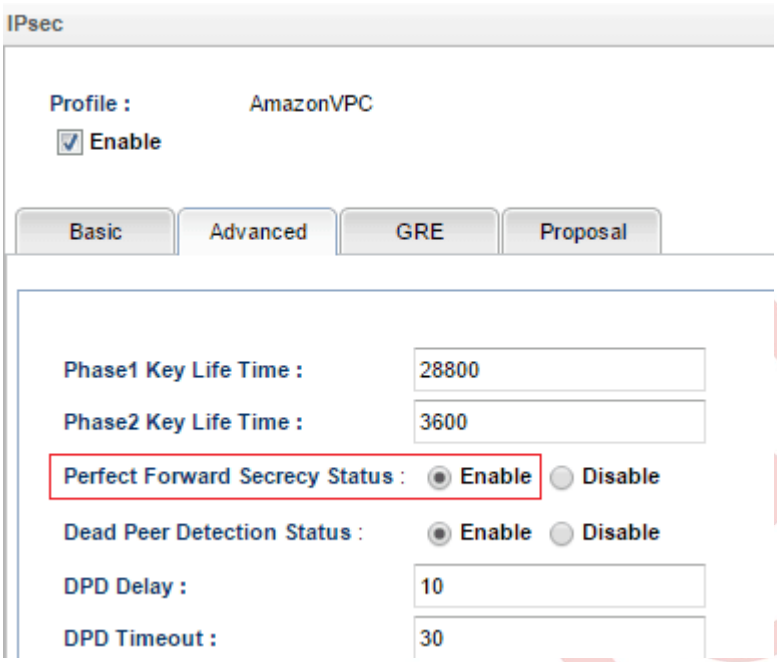
Linux

1. **VPN and Remote Access >> VPN Profile >> IPsec** sayfasına gidin ve profil oluşturmak için Add'e tıklayın. Basic sekmesinde:
   a. Profil adı girin ve "Enable this profile" ı etkinleştirin.
   b. **Auto Dial-Out** için Enable seçeneğini seçin.
   c. **Dial-Out Through** için VPN'i Amazon VPC'ye oluşturmak için **WAN** ara yüzünü seçin.
   d. **Local IP/Subnet Mask** 'da Vigor Router'ın Local network IP'sini ve Subnet'ini girin.
   e. **Remote Host**'a Amazon VPC'nin WAN IP'sini girn.

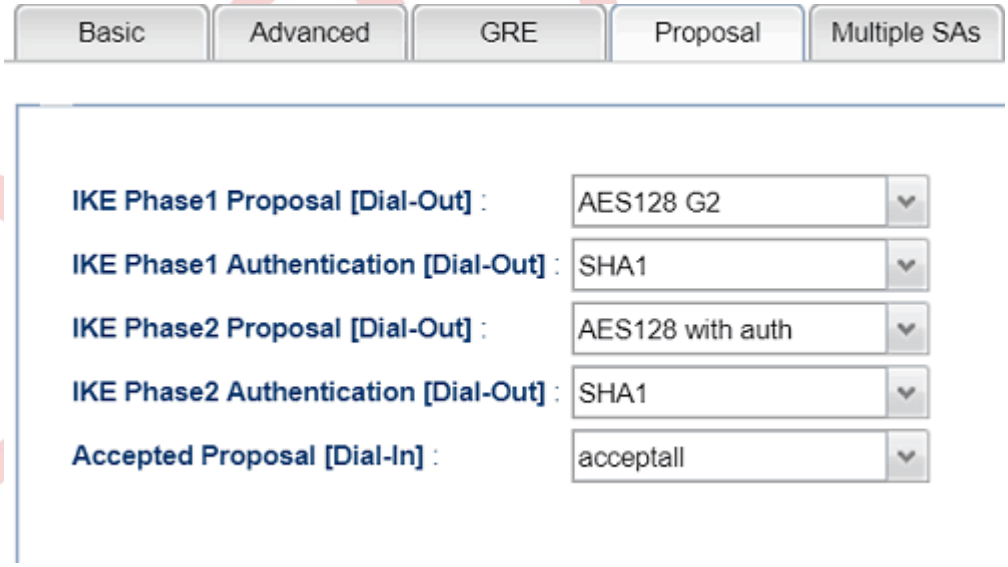
f. **Remote IP/Subnet Mask** 'a AWS'nizin Virtual LAN 'ını girin.
g. IKE Protocol için **IKEv1** ve **Main Mode** olarak IKE phase 1 seçeneğini seçin.
h. **Pre-Shared Key** girin.
i. Profili kaydetmek için **Apply**'a tılayın.



2. **Advanced** sekmesinde **Perfect Forward Secrecy Status**'u etkinleştirin.



3. **Proposal** sekmesinde:
   a. IKE Phase 1 Proposal [Dial-Out] için **AES128_G2** seçeneği seçin.
   b. IKE Phase 1 Authentication [Dial-Out] için **SHA1** seçeneği seçin.
   c. IKE Phase 2 Proposal [Dial-Out] için **AES128with auth** seçeneği seçin.
   d. IKE Phase 2 Authentication [Dial-Out] için **SHA1** seçeneği seçin.
   e. Kaydetmek için Apply'a tıklayın.



4. 30 saniye bekleyin. **VPN and Remote Access >> Connection Management** sayfasında VPN tünelinin durumunu görebilirsiniz. VPN kurulduktan sonra Vigor Router paketleri VPN tüneline yönlendirecek ancak AWS VPN paketlerini varsayılan policylerden dolayı engellediği için yanıt almayabilir. Vigor Router'ın LAN ağını içerecek şekilde AWS'nizin routera tablosunu güncellemeniz veya trafiği tünele iletmek için bir security grubu eklemeniz / güncellmeniz gerekir. Bu adım ve daha fazla yardım için lütfen AWS desteğine başvurun.