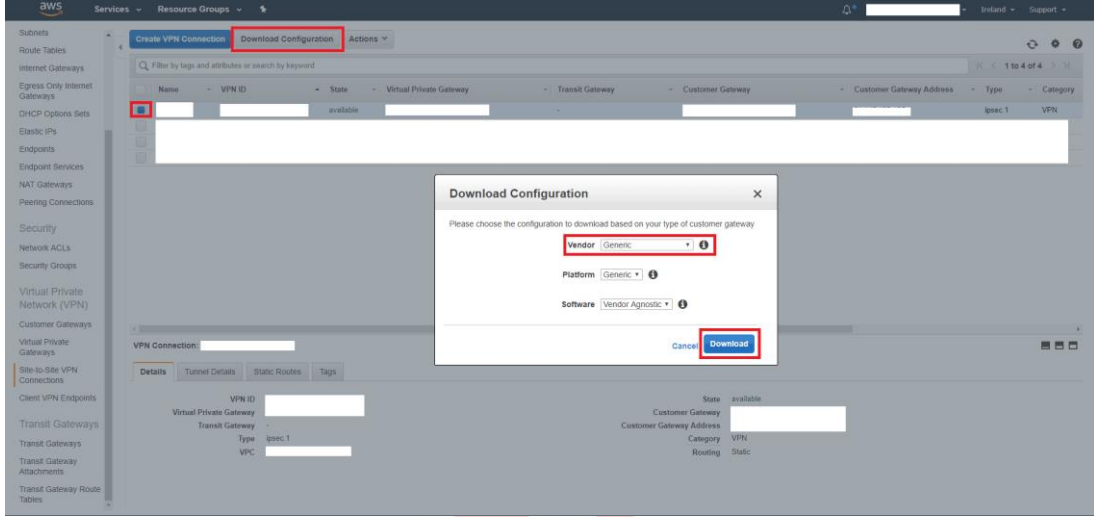


AMAZON VPC VE VIGOR ROUTER ARASINDA IPSEC VPN

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

Amazon VPC Ayarları

1. AWS >> VPC Dashboard >> 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.

1. Common Settings Profile Name: AmazonVPC <input checked="" type="checkbox"/> Enable this profile VPN Dial-Out Through: WAN1 First 1-118.168.185.243 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: -1 second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP:
2. Dial-Out Settings Type of Server I am calling: <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel IKEv1 <input type="radio"/> L2TP with IPsec Policy None <input type="radio"/> SSL Tunnel		Username: ??? Password: Max: 15 characters PPP Authentication: PAP/CHAP/MS-CHAP/MS-CHAPv2 VJ Compression: <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key: ***** <input type="radio"/> Digital Signature(X.509) Peer ID: None
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) x.x.x.x Server Port (for SSL Tunnel): 443		

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.

IKE advanced settings

IKE phase 1 mode(IKEv1)	<input checked="" type="radio"/> Main mode	<input type="radio"/> Aggressive mode
IKE phase 1 proposal	AES128_SHA1_G2 ▼	
IKE phase 2 proposal	AES128_SHA1 ▼	
IKE phase 1 key lifetime	28800	(900 ~ 86400)
IKE phase 2 key lifetime	3600	(600 ~ 86400)
Perfect Forward Secret	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Local ID		

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.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	10.10.0.0
Remote Network Mask	255.255.0.0 / 16 ▼
Local Network IP	192.168.126.1
Local Network Mask	255.255.255.0 / 24 ▼
	<input type="button" value="More"/>

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 / güncelleniz 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 girin.

- 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 tıklayın.

IPsec

Profile : AmazonVPC

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 : 10.10.0.0 255.255.0.0/16

Add Save

IP	Subnet Mask
No items to show.	

More Remote Subnet :

IKE Protocol : IKEv1

IKE Phase 1 : Main Mode Aggressive Mode

Auth Type : PSK

Preshared Key : (If Aggressive mode is disabled and Rer

Security Protocol : ESP

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

IPsec

Profile : AmazonVPC

Enable

Basic Advanced GRE Proposal

Phase1 Key Life Time : 28800

Phase2 Key Life Time : 3600

Perfect Forward Secrecy Status : Enable Disable

Dead Peer Detection Status : Enable Disable

DPD Delay : 10

DPD Timeout : 30

3. **Proposal** sekmesinde:

- IKE Phase 1 Proposal [Dial-Out] için **AES128_G2** seçeneği seçin.
- IKE Phase 1 Authentication [Dial-Out] için **SHA1** seçeneği seçin.
- IKE Phase 2 Proposal [Dial-Out] için **AES128with auth** seçeneği seçin.
- IKE Phase 2 Authentication [Dial-Out] için **SHA1** seçeneği seçin.
- Kaydetmek için Apply'a tıklayın.

Basic Advanced GRE Proposal Multiple SAs

IKE Phase1 Proposal [Dial-Out] : AES128 G2

IKE Phase1 Authentication [Dial-Out] : SHA1

IKE Phase2 Proposal [Dial-Out] : AES128 with auth

IKE Phase2 Authentication [Dial-Out] : SHA1

Accepted Proposal [Dial-In] : acceptall

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 / güncellenmeniz gerekir. Bu adım ve daha fazla yardım için lütfen AWS desteğine başvurun.