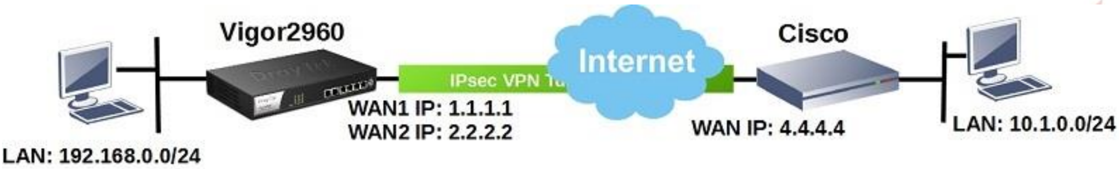
## CISCO ASA VE VIGOR3900 ARASINDA IPSEC VPN

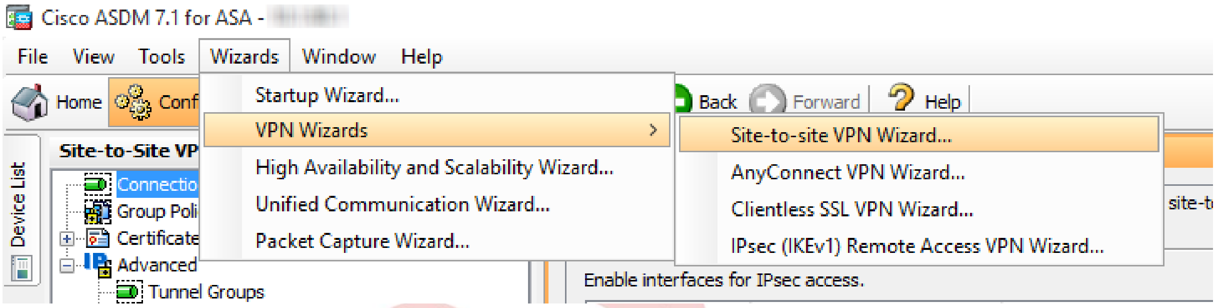
Bu belge CiscoASA ve Vigor3900 / 2960 arasında nasıl bir IPsec tüneli kurulacağını tanıtmaktadır. Senaryo, Vigor2960'ın iki WAN ara yüzüne sahip olduğu ve WAN1 kapalıyken Cisco'ya WAN2 aracılığıyla nasıl sesleneceğidir.

Bu örnekte, Vigor2960'ın WAN1'inin Public bir IP adresi 1.1.1.1, WAN2'nin 2.2.2.2'si vardır ve local subnet IP'si 192.168.0.0/2'dir. Cisco ASA 5515'in Public bir WAN IP'si 4.4.4.4'ü vardır ve local subnet IP'si 10.1.0.0/24'tür.

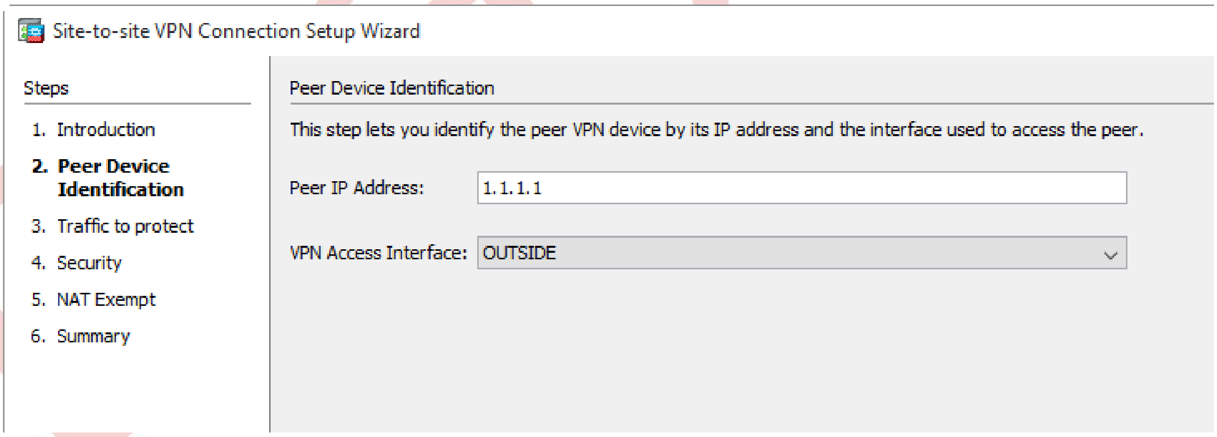


### Cisco'yu VPN Sunucusu Olarak Yapılandırma (Dial-In)

1. Vigor2960 Dial-In için Site to Site VPN profili oluşturmak için VPN Sihirbazlarını kullanın.


Cisco ASDM 7.1 for ASA - [redacted]
File View Tools Wizards Window Help
Home Conf
Back Forward Help
Site-to-Site VP
Connectio
Group Poli
Certificate
Advanced
Tunnel Groups
Device List
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
site-t
Enable interfaces for IPsec access.

2. Vigor2960'ın WAN1 IP "1.1.1.1" yi Peer IP Adresi olarak belirtin.



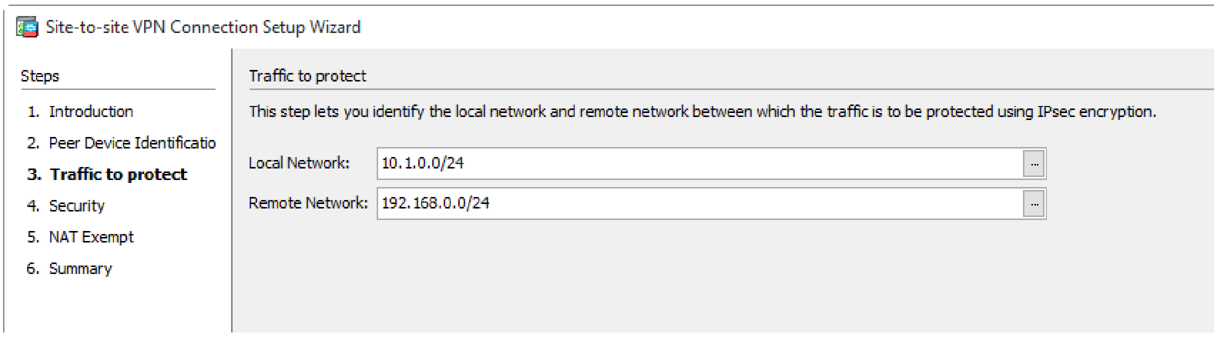
Peer Device Identification

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 1.1.1.1

VPN Access Interface: OUTSIDE

3. Local Network ve Remote Network'ü belirtin.



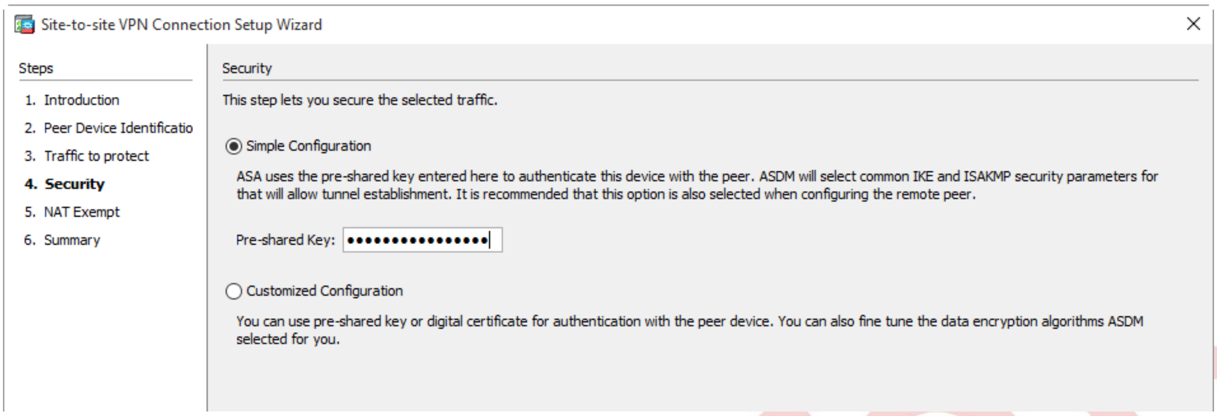
Traffic to protect

This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

Local Network: 10.1.0.0/24

Remote Network: 192.168.0.0/24

4. Pre-shared Key girin.



Security

This step lets you secure the selected traffic.

● Simple Configuration

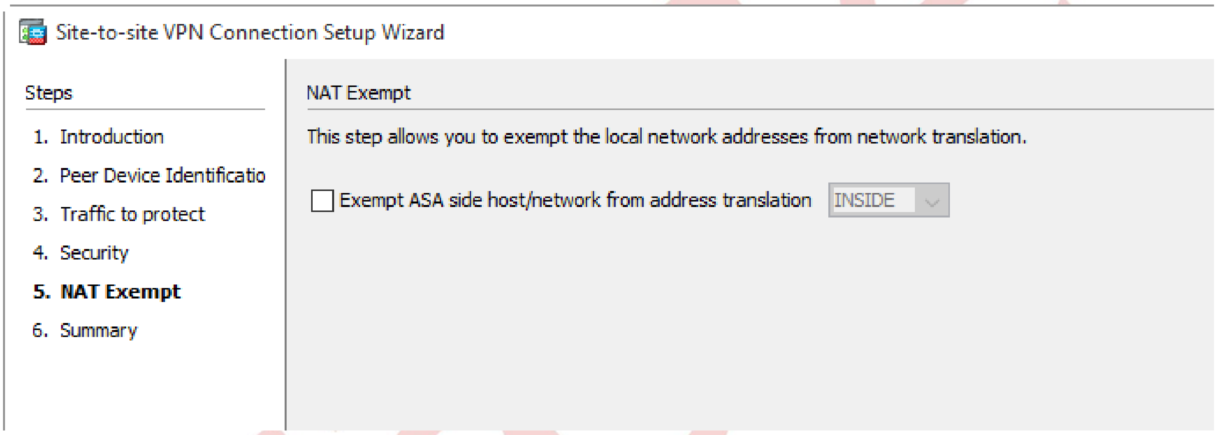
ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

Pre-shared Key: ●●●●●●●●●●●●●●●●

○ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

5. “Exempt ASA side host/network from address translation” seçeneğini seçmeyin.

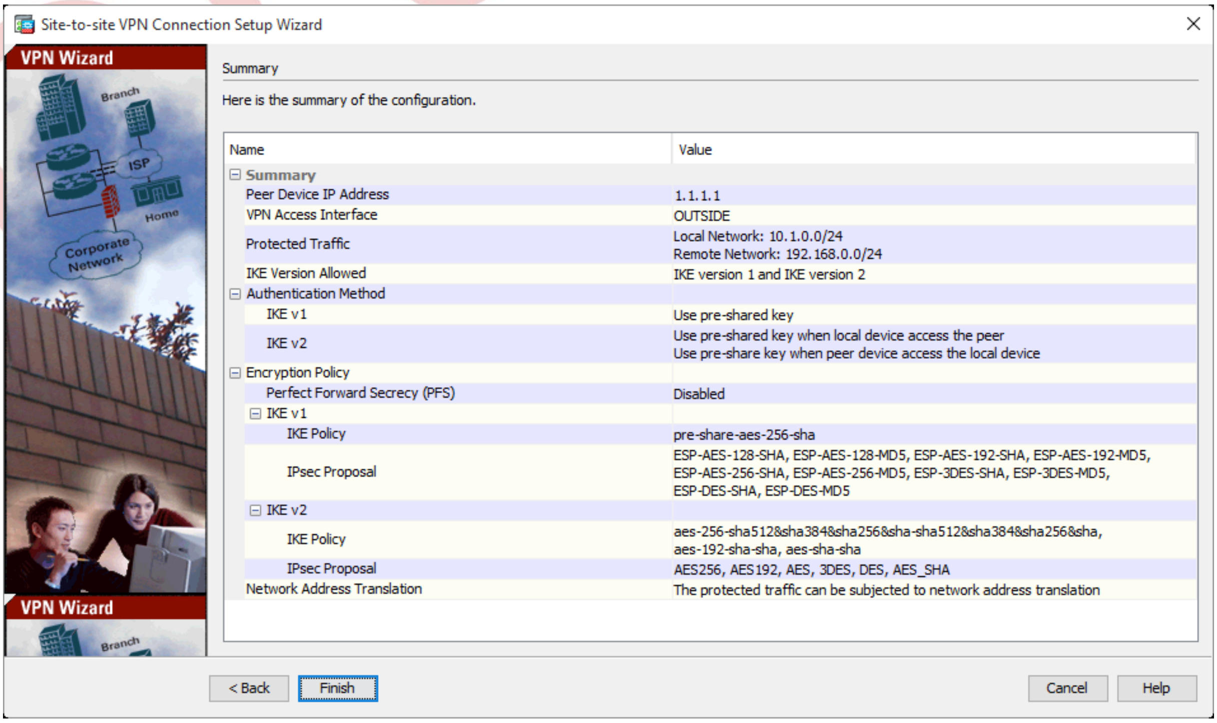


NAT Exempt

This step allows you to exempt the local network addresses from network translation.

☐ Exempt ASA side host/network from address translation INSIDE

6. Bu VPN profilinin özeti, aşağıdaki şekilde gösterilecektir, kabul edilen IKE Protocol’ünü, IKE Policy’i ve IPsec Proposal’ı içerir.

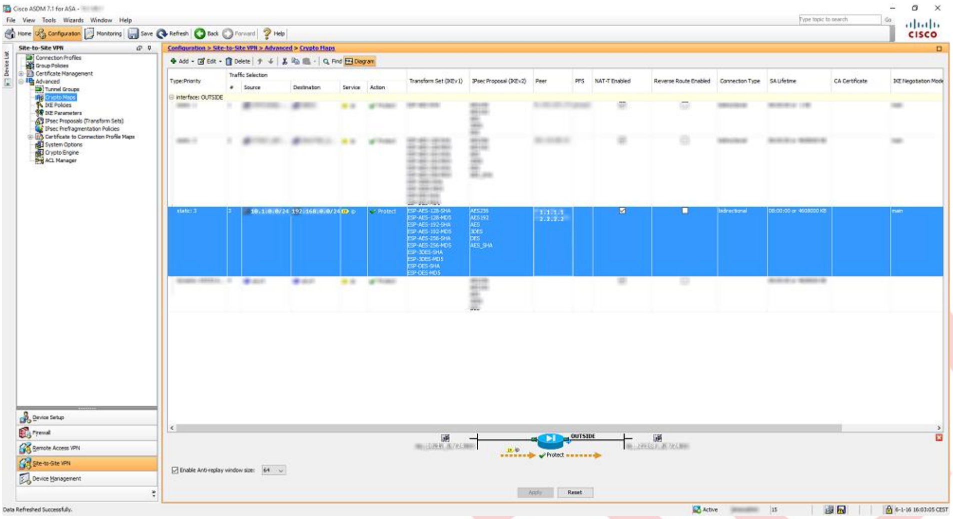


Summary

Here is the summary of the configuration.

| Name | Value |
|---|---|
| ⊟ Summary | |
| Peer Device IP Address | 1.1.1.1 |
| VPN Access Interface | OUTSIDE |
| Protected Traffic | Local Network: 10.1.0.0/24<br>Remote Network: 192.168.0.0/24 |
| IKE Version Allowed | IKE version 1 and IKE version 2 |
| ⊟ Authentication Method | |
| IKE v1 | Use pre-shared key |
| IKE v2 | Use pre-shared key when local device access the peer<br>Use pre-share key when peer device access the local device |
| ⊟ Encryption Policy | |
| Perfect Forward Secrecy (PFS) | Disabled |
| ⊟ IKE v1 | |
| IKE Policy | pre-share-aes-256-sha |
| IPsec Proposal | ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5 |
| ⊟ IKE v2 | |
| IKE Policy | aes-256-sha512&sha384&sha256&sha-sha512&sha384&sha256&sha, aes-192-sha-sha, aes-sha-sha |
| IPsec Proposal | AES256, AES192, AES, 3DES, DES, AES_SHA |
| Network Address Translation | The protected traffic can be subjected to network address translation |

7. İkinci Peer IP Adresini ekleyerek (izin vererek) belirtilen Crypto Map'lere gidin ve belirtilen Crypto Map'leri düzenleyin (Vigor2960'ın WAN2 Public IP 2.2.2.2'sidir).



Cisco ASDM 7.1 for ASA - [redacted]

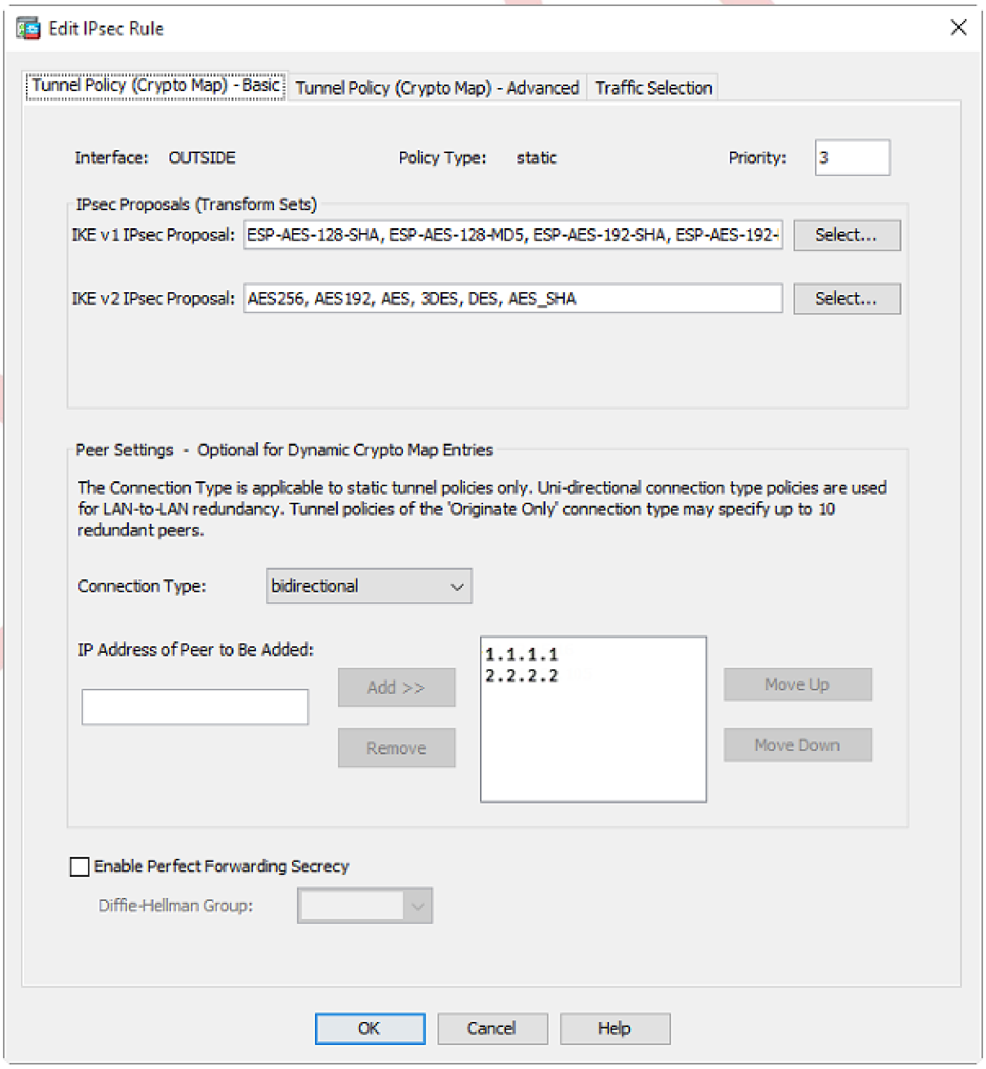
Configuration > Site-to-Site VPN > Advanced > Crypto Maps

| Type:Priority | # | Source | Destination | Service | Action | Transform Set (IKEv1) | IPsec Proposal (IKEv2) | Peer | PFS | NAT-T Enabled | Reverse Route Enabled | Connection Type | SA Lifetime | CA Certificate | IKE Negotiation Mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Interface: OUTSIDE | | | | | | | | | | | | | | | |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | | [redacted] | [redacted] | [redacted] | [redacted] | | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | | [redacted] | [redacted] | [redacted] | [redacted] | | [redacted] |
| static: 3 | 3 | 10.1.0.0/24 | 192.168.0.0/24 | IP | ✓ Protect | ESP-AES-128-SHA<br>ESP-AES-128-MD5<br>ESP-AES-192-SHA<br>ESP-AES-192-MD5<br>ESP-AES-256-SHA<br>ESP-AES-256-MD5<br>ESP-3DES-SHA<br>ESP-3DES-MD5<br>ESP-DES-SHA<br>ESP-DES-MD5 | AES256<br>AES192<br>AES<br>3DES<br>DES<br>AES_SHA | 1.1.1.1<br>2.2.2.2 | | ☑ | □ | bidirectional | 08:00:00 or 4608000 KB | | main |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | | [redacted] | | | [redacted] | [redacted] | | [redacted] | | |

☑ Enable Anti-replay window size: 64

Data Refreshed Successfully.

8. Şimdi VPN sihirbazı üzerinden ikinci VPN Bağlantısını ekleyin. Peer Public IP hariç, aynı ayarları kullanın. Şimdi 1.1.1.1 yerine 2.2.2.2 kullanın.



Edit IPsec Rule

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Interface: OUTSIDE    Policy Type: static    Priority: 3

IPsec Proposals (Transform Sets)

IKE v1 IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-

IKE v2 IPsec Proposal: AES256, AES192, AES, 3DES, DES, AES_SHA

Peer Settings - Optional for Dynamic Crypto Map Entries

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

Connection Type: bidirectional

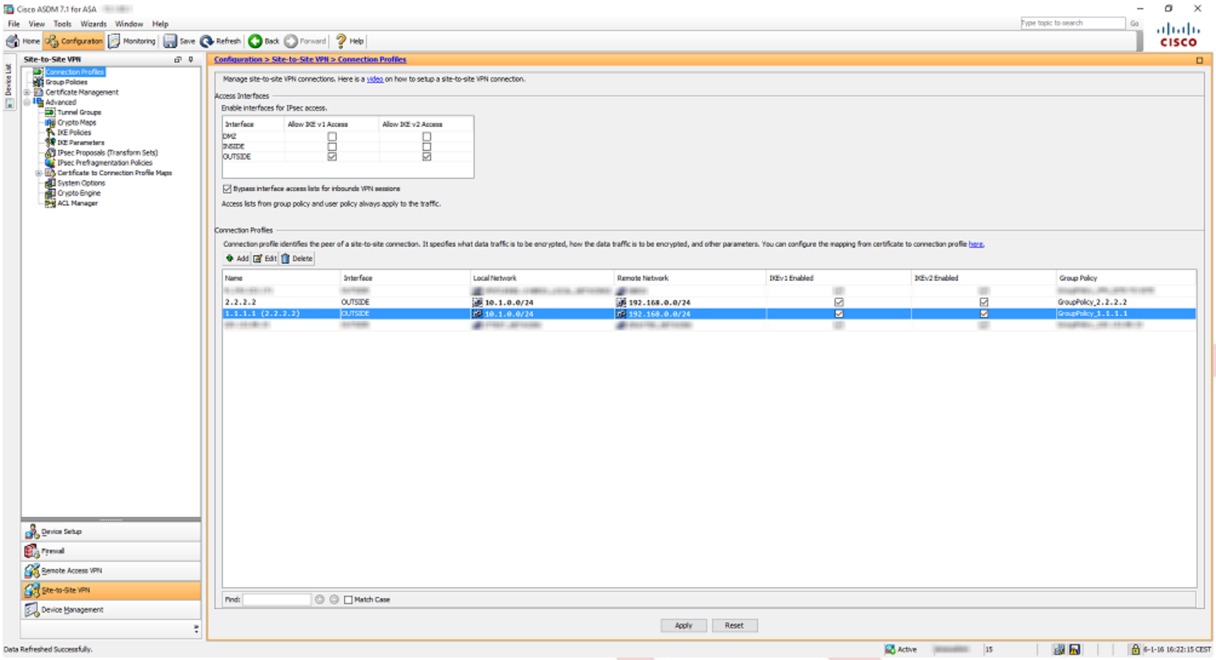
IP Address of Peer to Be Added:

1.1.1.1
2.2.2.2

□ Enable Perfect Forwarding Secrecy

Diffie-Hellman Group:

9. Bundan sonra, yapılandırma aşağıdakine benzer görünmelidir.



Configuration > Site-to-Site VPN > Connection Profiles

Manage site-to-site VPN connections. Here is a video on how to setup a site-to-site VPN connection.

Access Interfaces

Enable interfaces for IPsec access.

| Interface | Allow IKE v1 Access | Allow IKE v2 Access |
|---|---|---|
| DMZ | ☐ | ☐ |
| INSIDE | ☐ | ☐ |
| OUTSIDE | ☑ | ☑ |

☑ Bypass interface access lists for inbounds VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Connection Profiles

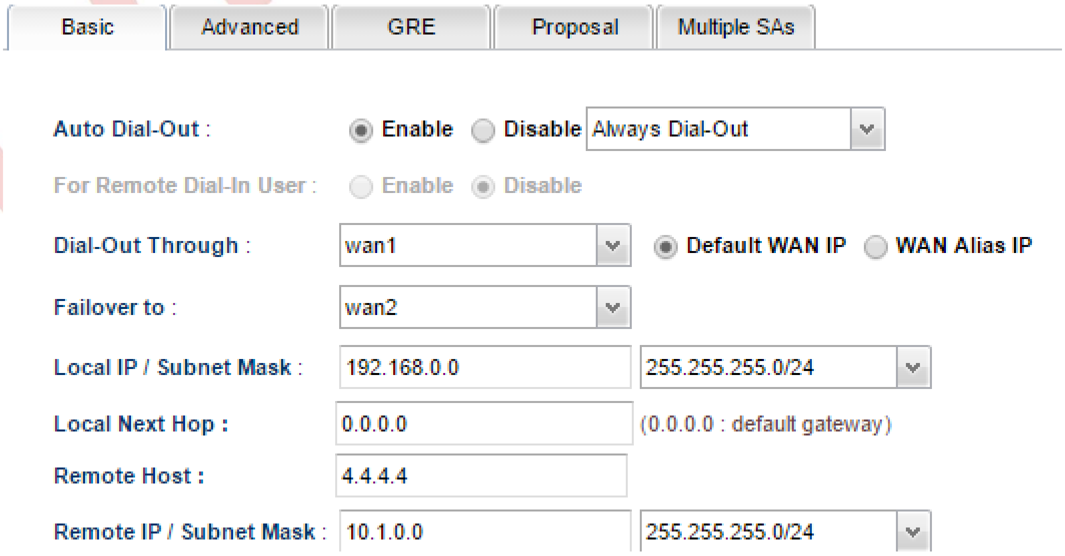
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile here.

| Name | Interface | Local Network | Remote Network | IKEv1 Enabled | IKEv2 Enabled | Group Policy |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| 2.2.2.2 | OUTSIDE | 10.1.0.0/24 | 192.168.0.0/24 | ☑ | ☑ | GroupPolicy_2.2.2.2 |
| 1.1.1.1 (2.2.2.2) | OUTSIDE | 10.1.0.0/24 | 192.168.0.0/24 | ☑ | ☑ | GroupPolicy_1.1.1.1 |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

Find: ☐ Match Case

## Vigor2960'ı VPN Client Olarak Yapılandırma (Dial-Out)

10. Teni bir profil oluşturmak için **VPN and Remote Access** >> **VPN Profile** >> **IPse**c sayfasına gidin.
    - Basic sekmesinde profil adı girin ve profil için "Enable" yi etkinleştirin.
    - **Auto Dial-Ou**t için Always Dial-Out 'u seçin.
    - **Dial-Out VPN Through** için wan1'i seçin.
    - **Failover** için wan2'yi seçin.
    - **Local IP /Subnet Mas**k'a Vigor Router'ın LAN ağını girin.
    - **Remote Host**'da Cisco'nun WAN IP'sini girin.
    - **Remote IP/ Subnet Mask**'a Cisco'nun local ağını girin.
    - **IKEv1** seçeneğini seçin.
    - **Pre-Shared Key** girin.



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 : wan2

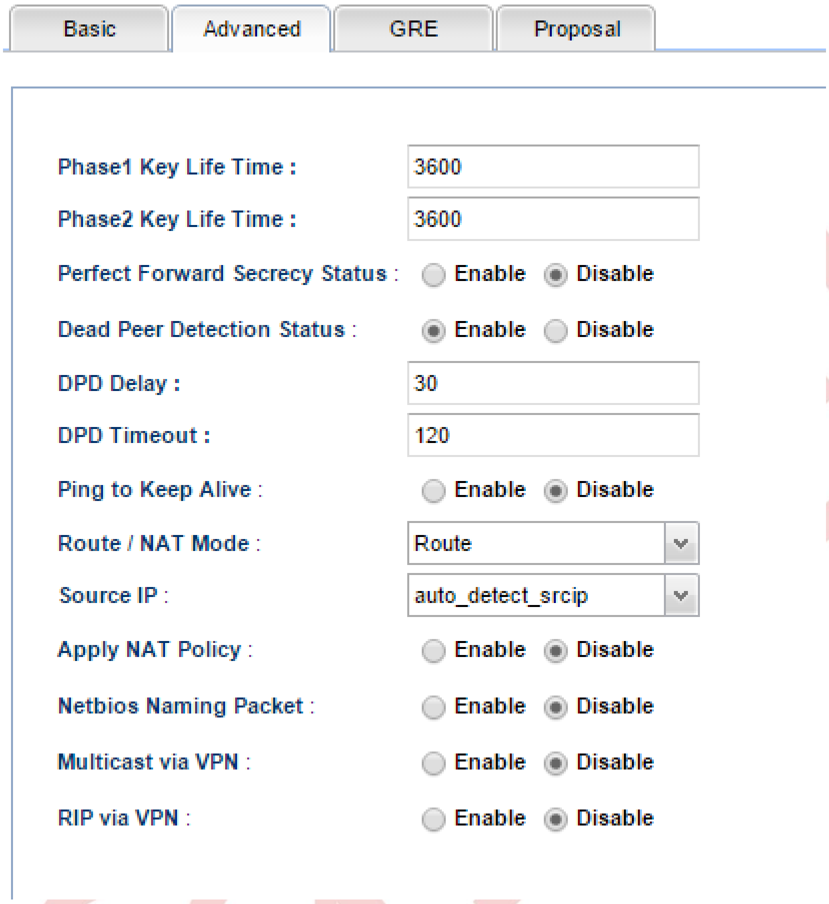
Local IP / Subnet Mask : 192.168.0.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 4.4.4.4

Remote IP / Subnet Mask : 10.1.0.0 255.255.255.0/24

11. Advanced sekmesinde **Phase1 Key Lifetime** 28800’den 3600’e çevirin. (Çünkü Cisco VPN yapılandırması phase1 key lifetime 3600 saniyedir.)



Phase1 Key Life Time : 3600

Phase2 Key Life Time : 3600

Perfect Forward Secrecy Status : ○ Enable ● Disable

Dead Peer Detection Status : ● Enable ○ Disable

DPD Delay : 30

DPD Timeout : 120

Ping to Keep Alive : ○ Enable ● Disable

Route / NAT Mode : Route

Source IP : auto_detect_srcip

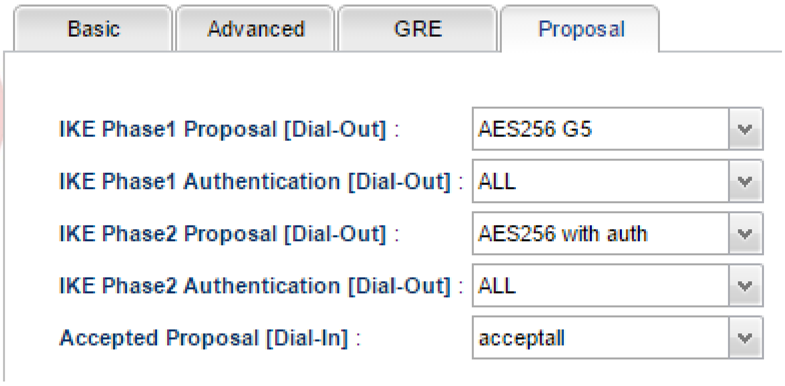
Apply NAT Policy : ○ Enable ● Disable

Netbios Naming Packet : ○ Enable ● Disable

Multicast via VPN : ○ Enable ● Disable

RIP via VPN : ○ Enable ● Disable

12. Proposal sekmesinde Cisco’daki proposal ayarlarında girilenlerin aynısını girin. Profili kaydetmek için **Apply'a** tıklayın.



IKE Phase1 Proposal [Dial-Out] : AES256 G5

IKE Phase1 Authentication [Dial-Out] : ALL

IKE Phase2 Proposal [Dial-Out] : AES256 with auth

IKE Phase2 Authentication [Dial-Out] : ALL

Accepted Proposal [Dial-In] : acceptall

Yukarıdaki konfigürasyonları tamamladıktan sonra Vigor2960, IPsec tünelini WAN1 üzerinden otomatik olarak Cisco'ya çevirecek ve WAN1 kapalıyken Failover olarak WAN2 üzerinden Cisco'ya çevirecektir.