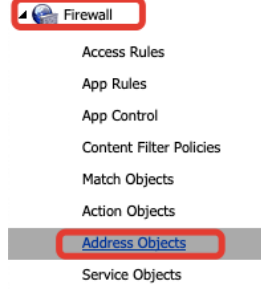


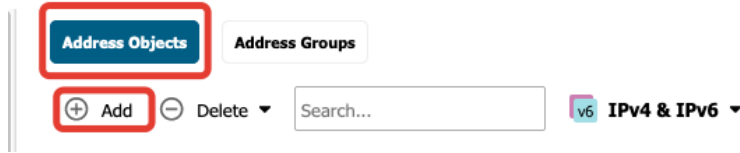
Sonicwall Site to Site VPN Ayarları

Sonicwall Site to Site VPN kurmak için öncelikli olarak **VPN** kurulacak iki lokasyona ait networkler **Address Object** olarak eklenmelidir.

Address Object eklemek için sol menüde bulunan **Firewall** ana başlığı altında **Address Object** kısmına geliyoruz.



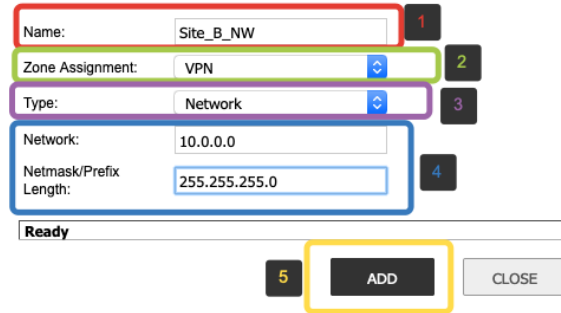
Açılan sayfada **ADD** butonuna tıklayarak Address Object ekleme işlemine başlıyoruz.



Açılan pencerede ;

1. İsim veriyoruz.
2. Zone olarak VPN seç
3. Type Network
4. Bir network belirliyoruz ve subneti giriyoruz.
5. Add diyerek kaydedip çıkıyoruz.
- 6.

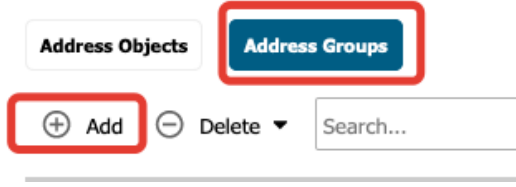
SONICWALL™ NS_a 2650



The image shows the Sonicwall Address Object configuration form. The form fields are highlighted with colored boxes and numbered 1 through 5. The fields are: Name (Site_B_NW), Zone Assignment (VPN), Type (Network), Network (10.0.0.0), and Netmask/Prefix Length (255.255.255.0). The 'ADD' button is highlighted with a yellow box and numbered 5.

Eğer birden fazla network ekliyorsak bunları kuralda daha kolay ekleyebilmek için **grup** haline getirmek daha iyi olacaktır.

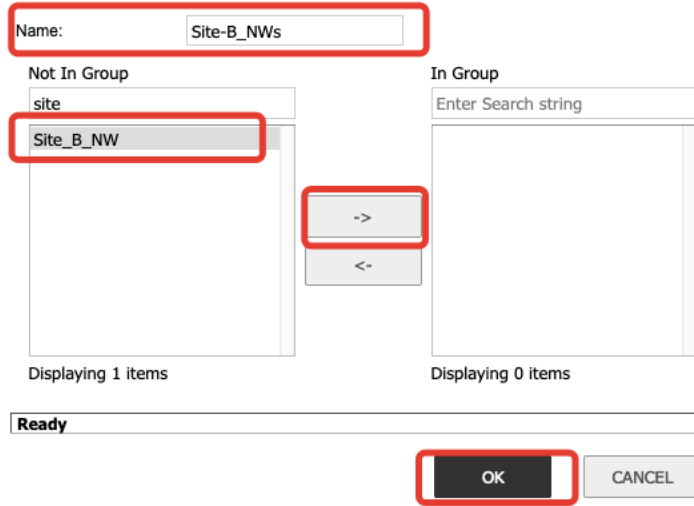
Address object eklemek için girdiğimiz sayfada üst kısımda bulunan **Address Groups** sekmesini tıklıyoruz. Grup ekleme işlemi için açılan sayfada **ADD** butonuna tıklıyoruz.



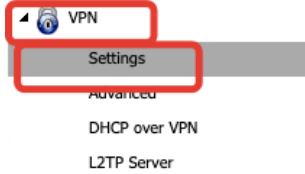
Açılan pencerede ;

1. İsim ver
2. Eklencek Address objectleri seç
3. Ok diyerek kaydedip çıkıyoruz.

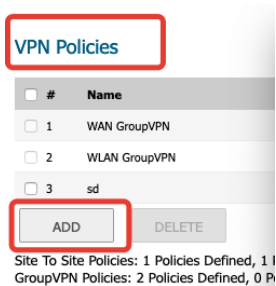
SONICWALL™ NS_a 2650



Site to Site VPN kuralını yazmak için sol menüde bulunan **VPN** ana başlığı altında **Settings** kısmına gidiyoruz.



Açılan sayfada **VPN Policies** altında **ADD** butonuna tıklıyoruz.



Yeni bir **Action Object** eklemek için **ADD** butonuna tıklıyoruz.

+ Add **-** Delete View **All Types**

#	Name
1	Advanced BWM High

Açılan pencerede ;

General Sekmesinde

1. Policy Type : Site to Site
2. Authentication Method : IKE Using Preshared Secret
3. Name : İsim veriyoruz
4. IPsec Primary Gateway Name or Address :Bağlantı kurulacak yerin dış ip adresini giriyoruz.
5. IKE Authentication altında

Shared Secret : Burada bir key oluşturuyoruz.

Local IKE ID ve Peer IKE ID : Piv4 Address seçilecek

Mask Shared Secret seçili olacak.

SONICWALL® NS₄ 2650

General Network Proposals Advanced

Security Policy

Policy Type: Site to Site **1**

Authentication Method: IKE using Preshared Secret **2**

Name: Site-B **3**

IPsec Primary Gateway Name or Address: 195.175. **4**

IPsec Secondary Gateway Name or Address:

IKE Authentication

Shared Secret: **5**

Confirm Shared Secret:

Mask Shared Secret

Local IKE ID: IPv4 Address

Peer IKE ID: IPv4 Address

Ready

Network Sekmesinde

Local Network başlığında daha önce oluşturduğumuz local network grubunu seçiyoruz.

Remote Network başlığında bağlanacağımız lokasyondaki networkler için oluşturduğumuz grubu seçiyoruz.

Local Networks

Choose local network from list Any address^{*}

LAN Subnets

Remote Networks

Use this VPN Tunnel as default route for all Internet traffic

Choose destination network from list Use IKEv2 IP Pool^{*}

Site_B_NW

--Select IP Pool Network--

Ready

OK

CANCEL

HELP

Proposals Sekmesinde

1. IKE (Phase 1) Proposal başlığında

Exchange: Main mod olarak seçilir.

DH Group: Group 2

Encryption: AES-128

Authentication:SHA1

Life Time (seconds): 28800

2. Ipsec (Phase 2) Proposal başlığında

Protocol: ESP

Encryption: AES-128

Authentication: SHA1

Enable Perfect Forward Secrecy

Life Time (seconds):28800

SONICWALL NS_a 2650

General Network **Proposals** Advanced

IKE (Phase 1) Proposal

Exchange: **1** Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipssec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-128

Authentication: SHA1

Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Ready

OK CANCEL HELP

Advanced Sekmesinde

Enable Keep Alive seçiyoruz.

Eğer VPN üzerinden bağlantı yapanların Firewall a erişmesini istiyorsak

Management via this SA ve **User login via this SA** satırlarında bulunan HTTPS kısımları seçilmelidir.

OK diyerek kaydedip çıkıyoruz.

SONICWALL NS_a 2650

General Network Proposals **Advanced**

Advanced Settings

Enable Keep Alive

Suppress automatic Access Rules creation for VPN Policy

Disable IPsec Anti-Replay

Require authentication of VPN clients by XAUTH

Enable Windows Networking (NetBIOS) Broadcast

Enable Multicast

WXA Group: None

Display Suite B Compliant Algorithms Only

Apply NAT Policies

Allow SonicPointN Layer 3 Management

Management via this SA: HTTPS SSH SNMP

User login via this SA: HTTP HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

Ready

OK CANCEL HELP

Aynı işlemleri bağlanacağımız diğer lokasyonda da yapıyoruz . Ayarlar tamamlandıktan sonra **VPN Policies** başlığı altında bağlantımızın yanında **yeşil** bir ışık yanacaktır. Buda bağlantının tamamlandığını gösterir