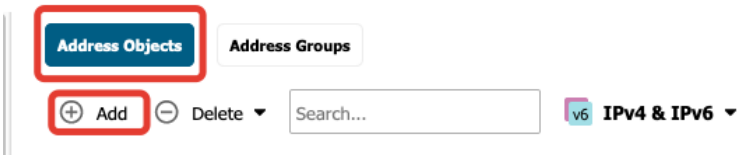
Sonicwall Site to Site VPN Ayarları

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

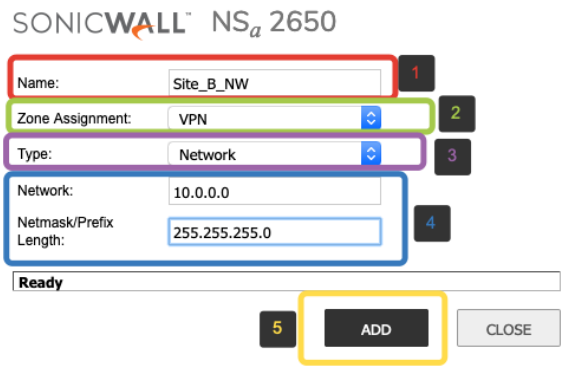
Address Object eklemek için sol menüde bulunan **Firewall** ana başlığı altında **Address Object** kısmına geliyoruz.

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

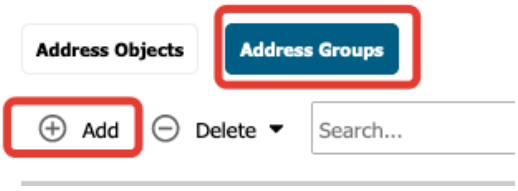


Açılan pencerede ;

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



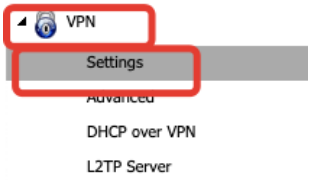
Eğer birden fazla network ekliyorsak bunları kuralda daha kolay ekleyebilmek için **grup** haline getirmek daha iyi olacaktır.
Address object eklemek için girdiğimiz sayfada üst kısımda bulunan **Address Groups** sekmesini tıklıyoruz.
Grup ekleme işlemi için açılan sayfada **ADD** butonuna tıklıyoruz.



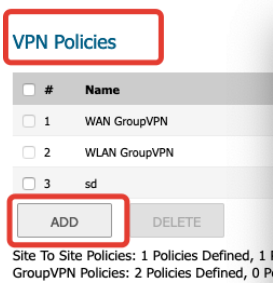
Açılan pencerede ;

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

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.



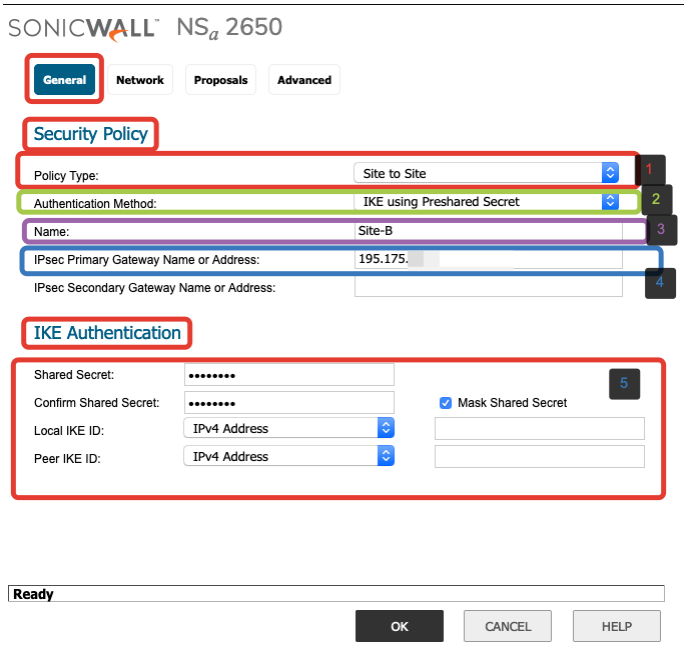
Yeni bir **Action Object** eklemek için **ADD** butonuna tıklıyoruz.

Açılan pencerede ;

General Sekmesinde

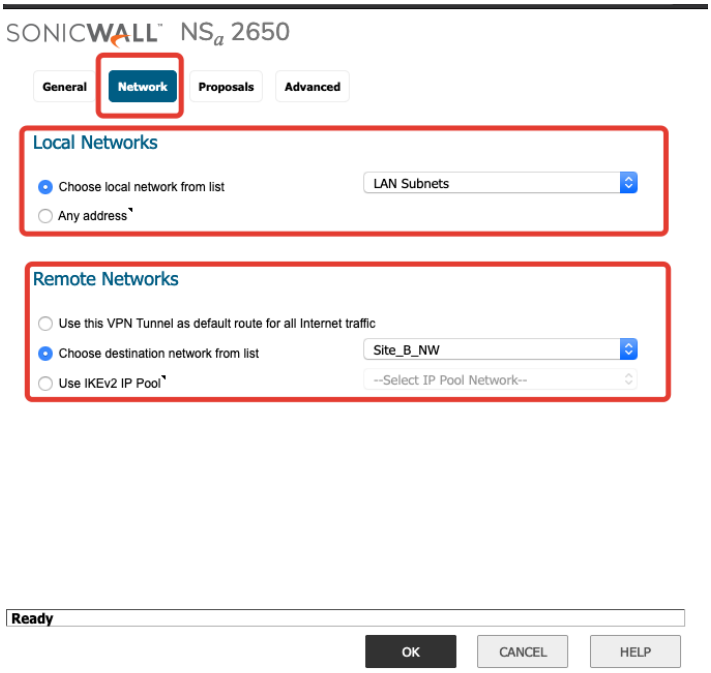
1. Policy Type : Site to Site
2. Authentication Method : IKE Using Preshared Secret
3. Name : İsim veriyoruz
4. IPsec Primary Gateway Name or Address :Bağlantı kurulacak yerin dış ip adresini giriyoruz.
5. IKE Authentication altında

Shared Secret : Burada bir key oluşturuyoruz.
Local IKE ID ve Peer IKE ID : Pıv4 Address seçilecek
Mask Shared Secret seçili olacak.



Network Sekmesinde

Local Network başlığında daha önce oluşturduğumuz local network grubunu seçiyoruz.
Remote Network başlığında bağlanacağımız lokasyondaki networkler için oluşturduğumuz grubu seçiyoruz.



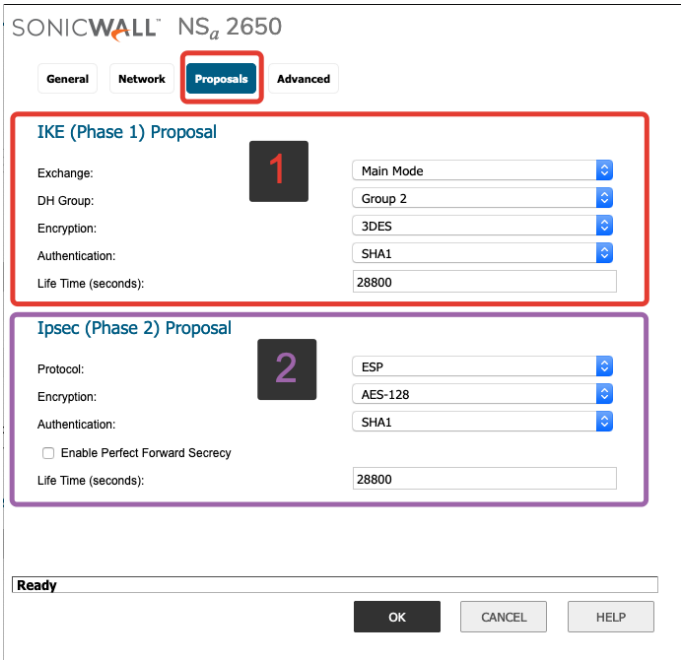
Proposals Sekmesinde

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



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.

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