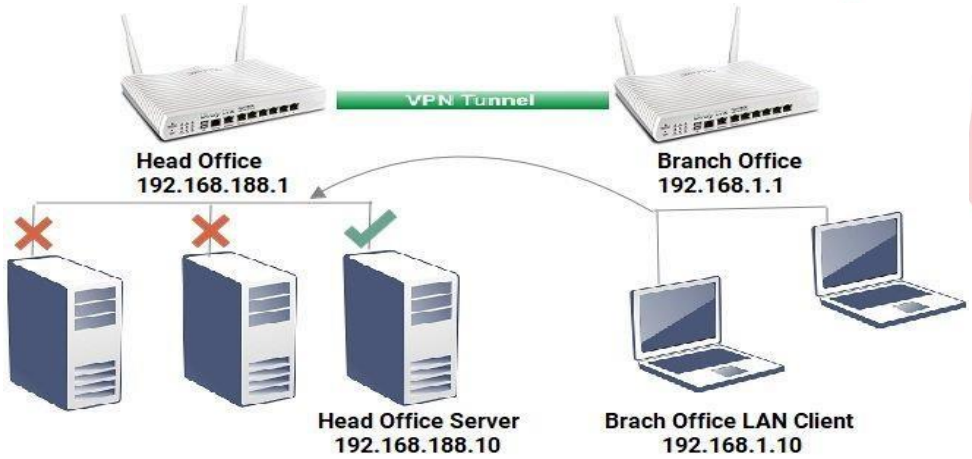
Uzak VPN Ağının Belirli IP'ye Erişimini Kısıtlama

VPN, Local network ile Remote network arasında güvenli bir bağlantı sağlar. VPN kurulduktan sonra, Remote Network Local Networkteki tüm cihazlara fiziksel olarak bağlanmış gibi erişebilir. Ancak, yalnızca belirli bir sunucuya erişmek için Remote Network için VPN'i kurarsak? Bu makale, Routerin nasıl yapılandırılacağını ve Remote VPN kullanıcılarının sadece aşağıdaki senaryo için belirli bir Local sunucu ile nasıl kısıtlanacağını gösterecektir.

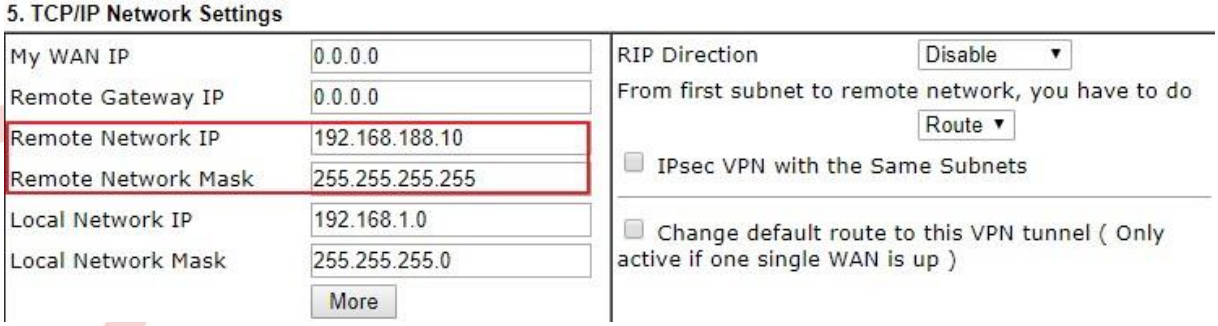


DrayOS

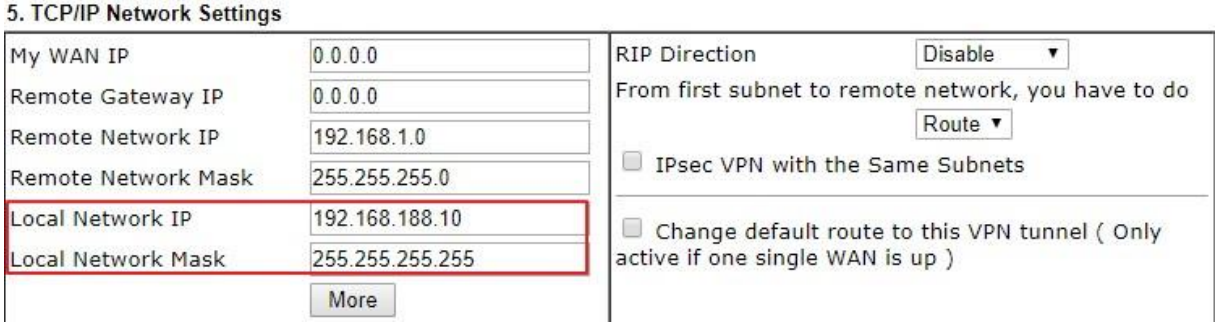
Bunu başarmanın iki yolu vardır: VPN Configuration ve Firewall Rules.

1.Yöntem 1: VPN Yapılandırması ile

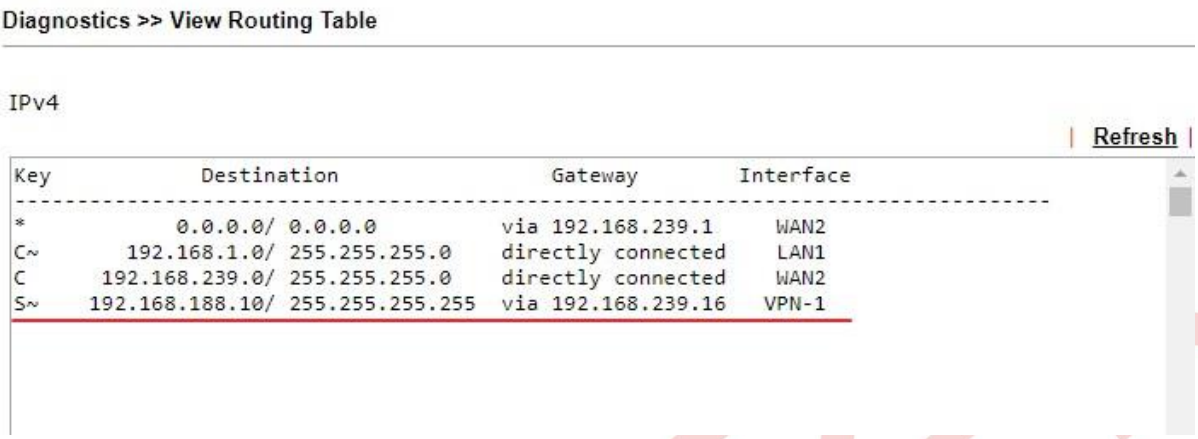
- Branch Office'de Vigor Router'ın LAN-LAN VPN profilinde, Remote Network IP'sini tüm ağdan sadece sunucunun IP'sine çevirin.



- Head Office'deki Vigor Router'ın LAN-LAN VPN profilinde, Local Network IP'sini tüm ağdan sadece sunucunun IP'sine değiştirin.

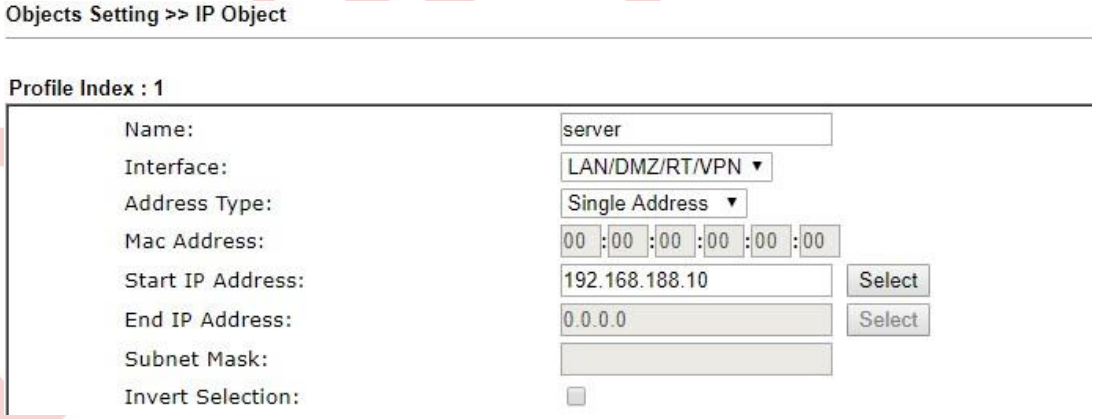


3. VPN kurulduğunda, Branch Office Router, yönlendirme bilgisine sadece sunucunun IP 192.168.188.10/32 bilgisine sahip olacak, böylece Branch Office'teki istemciler sadece sunucuya erişebilecektir.

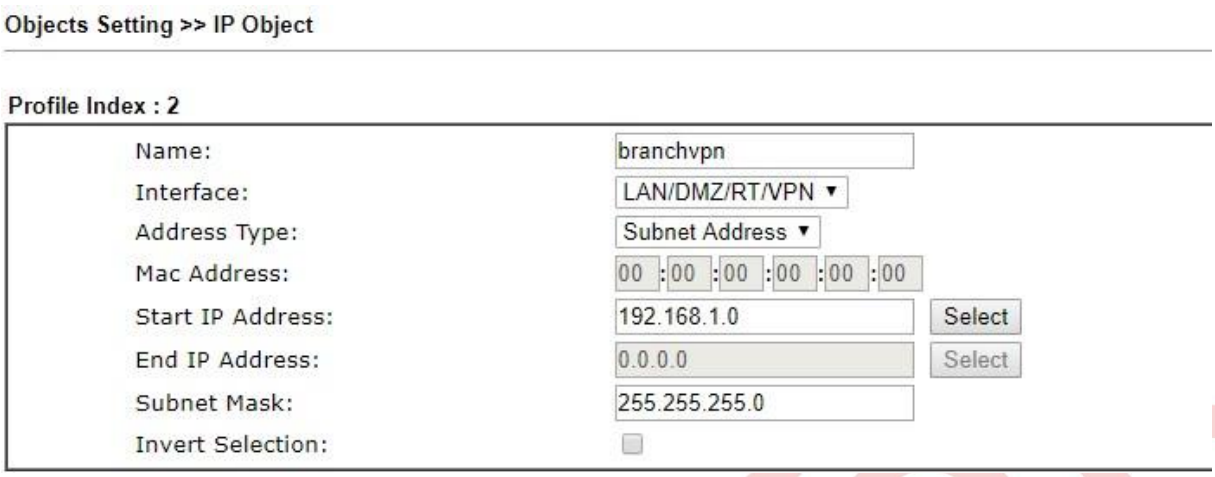


2.Yöntem 2: Firewall Kuralı'na Göre

- Branch Office'deki bağlantıyı sınırlandırmak için genel merkez Router'indeki firewall kuralını oluşturabiliriz. İlk önce **Objects Setting >> IP Object'e** gidin, serverin IP'si için bir IP Object profili oluşturmak için uygun bir indexe tıklayın:
- Nesneyi tanımlamak için Name girin
- Interface için "LAN / DMZ / RT / VPN" seçeneğini seçin
- Address Type için "Single Address" seçeneğini seçin ve ardından server IP adresini 192.168.188.10 olarak girin.
- Kaydetmek için OK'a tıklayın.

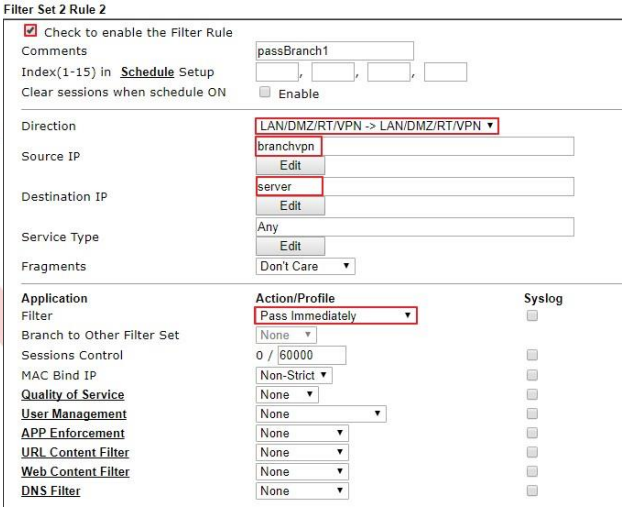


1. Şube VPN Network'ü için bir IP Object profili oluşturmak üzere başka bir uygun indexe tıklayın,
Name girin.
- Inteface için "LAN/DMZ/RT/VPN" seçin.
- Address Type için "Subnet Address" seçeneğini seçin ve ardından 192.168.1.0 IP adresini ve 255.255.255.0 Subnet Mask'ını girin.
- Kaydetmek için OK'a tıklayın.



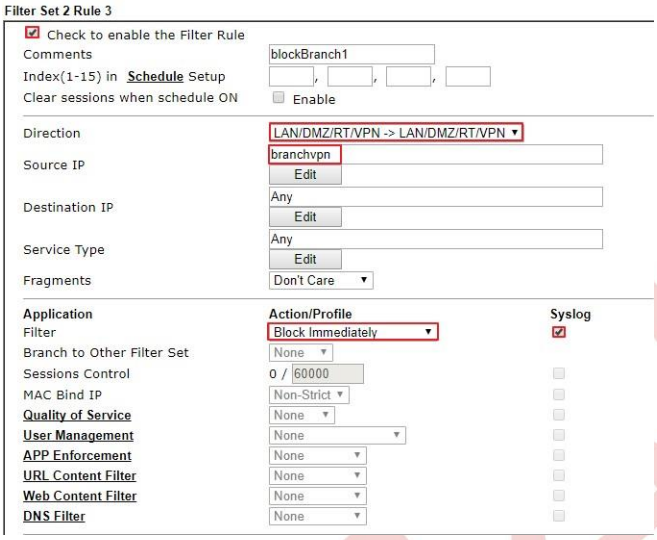
2. **Firewall >> Filter Setup >> Filter Set 2 (Default Data Filter)'e git,** paketleri Branch Office'den sunucuya geçirmek üzere Firewall kuralını düzenlemek için mevcut bir profile tıkla.

Firewall kuralını etkinleştir.
Profil Name girin.
Direction: LAN/DMZ/RT/VPN → LAN/DMZ/RT/VPN
Source IP: Branch VPN networkü için oluşturduğumuz IP nesnesini seçin.
Destination IP: Local server için oluşturduğumuz IP nesnesini seçin
(İsteğe bağlı) **Service Type**: Burada VPN networkünün sunucuya belirli bir porttan erişmesini istiyorsanız belirtin.
Filter: Pass Immediately

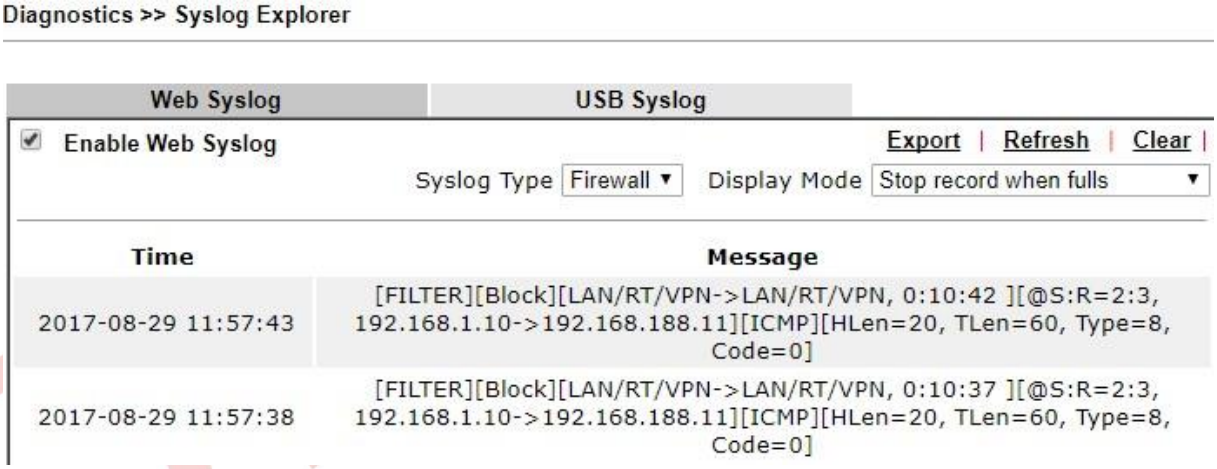


3. Paketleri şubeden diğer IP adreslerine engellemek için bir IP Filter kuralı oluşturmak için (Index number, step 3'den bir büyük olmalıdır) bir başka Index'e tıklayın.

- Bu Firewall kuralını etkinleştir.
- Profile Name gir.
- **Direction:** LAN/DMZ/RT/VPN → LAN/DMZ/RT/VPN
- **Source IP**:Şube VPN networkü için oluşturduğumuz IP nesnesini seçin.
- **Destination IP:** Any
- **Filter:** Block Immediately
  -



Ve bu gerekli yapılandırmayla. Filtrelenen trafik olup olmadığını görmek için, **Diagnostics >> Syslog Explorer** sayfasındaki Firewall loglarını kontrol edebiliriz.

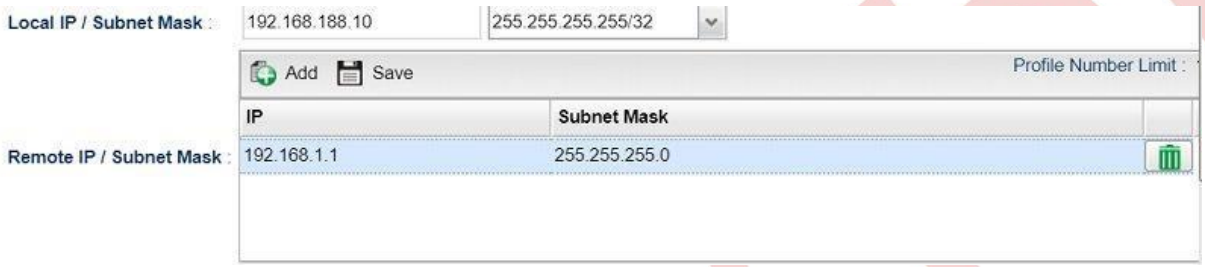


LİNUX

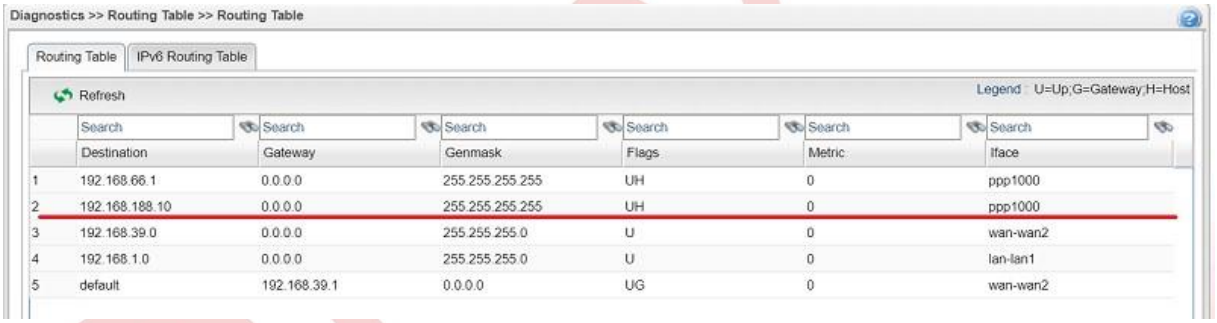
Bunu başarmanın iki yolu vardır: VPN Configuration ve Firewall kuralları.

1. **Yöntem 1: VPN Yapılandırması ile**
   - Şubedeki Vigor Router'ın LAN-LAN VPN profilinde, Remote IP / Subnet Mask'ı tüm ağdan sadece sunucunun IP'sine çevirin.

- Head Office'deki Vigor Router'ın LAN-LAN VPN profilinde, Local IP / Subnet Maskını tüm ağdan sadece sunucunun IP'sine değiştirin.

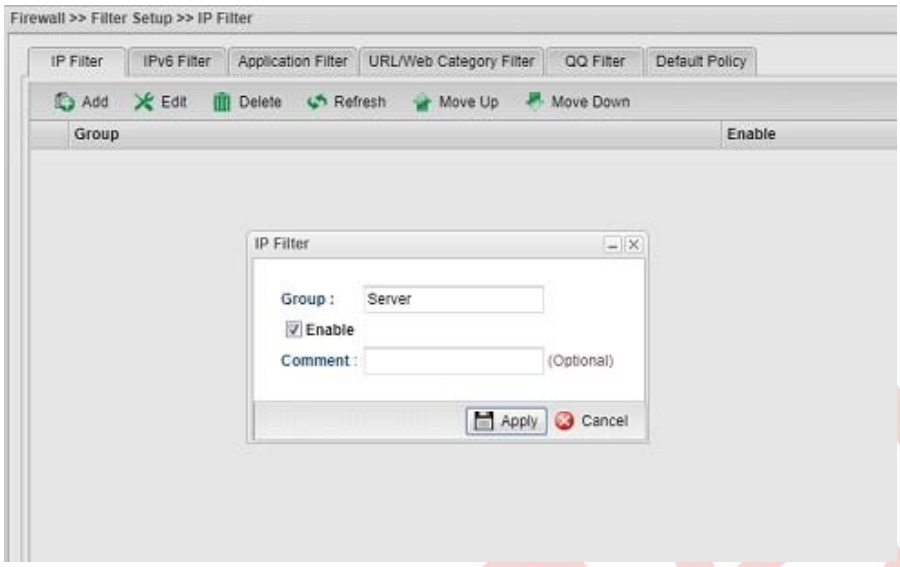


- VPN kurulduğunda, Branch Office Router, yönlendirme bilgisine sadece Server'in IP 192.168.188.10/32 bilgisine sahip olacak, böylece Branch Office'teki Client'ler sadece Server'e erişebilecektir.



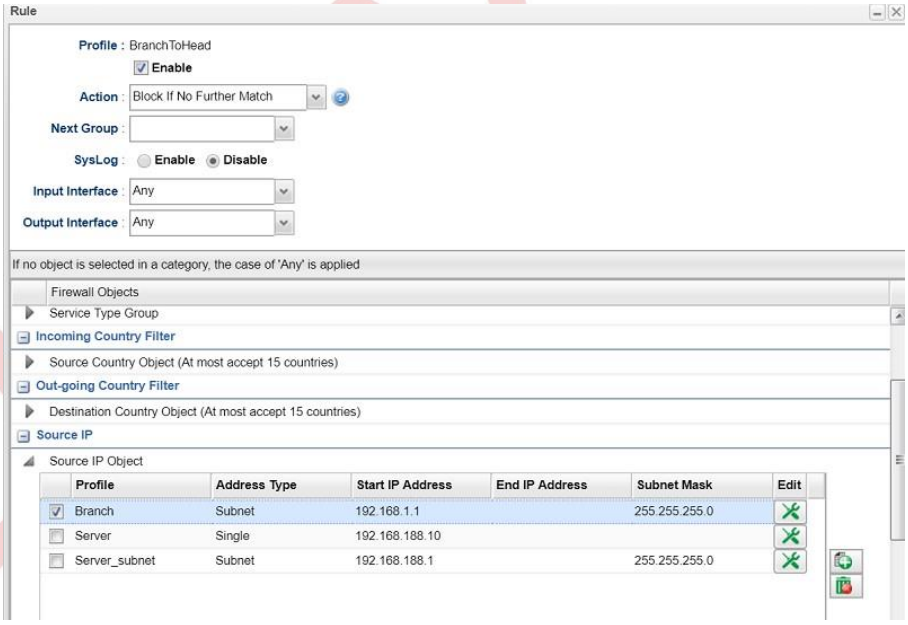
Yöntem 2 :Firewall Kuralı'na Göre

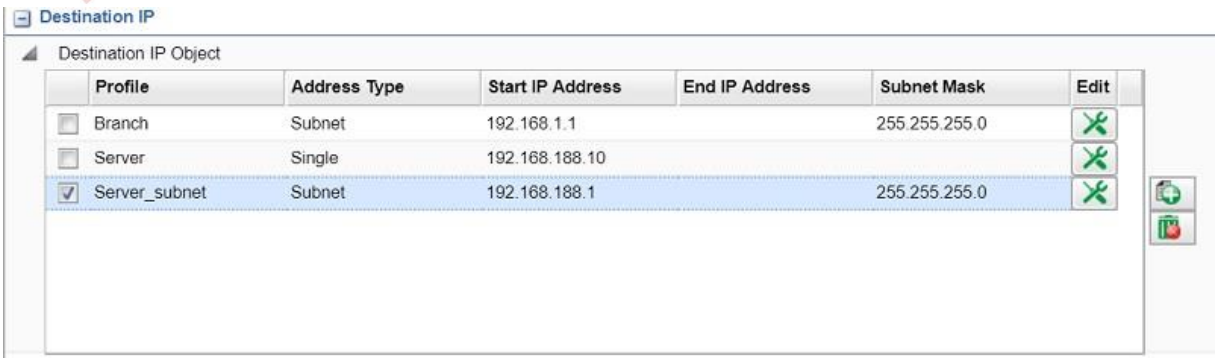
1. Brach ofisindeki bağlantıyı sınırlandırmak için merkez Router'de firewall kuralını oluşturabiliriz. Önce, Firewall >> Filter Setup >> IP Filter bölümüne gidin, yeni bir grup oluşturmak için Add'e tıklayın.



2. Filtre grubunda, aşağıdaki gibi yeni bir kural ekleyin: Profile Name girin.

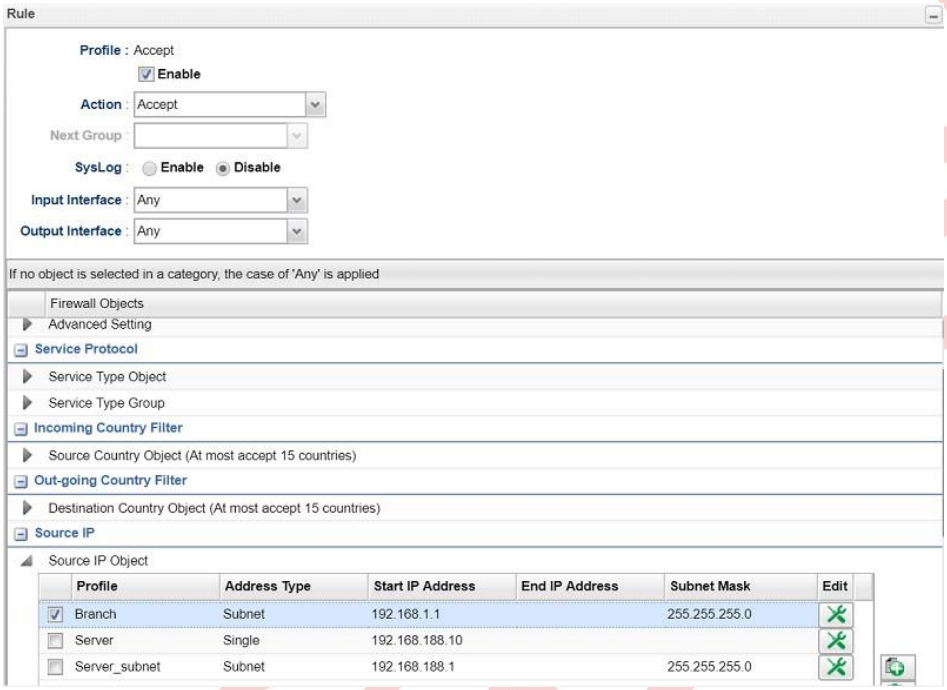
- Etkinleştirmeyi denetleyin.
- Action için "Block if No Further Match"i seçin.
- Source IP'de Branch Office networkü için bir nesne ekleyin ve onu seçin
- Destination IP'de, Head Office networkü için bir nesne ekleyin ve onu seçin.

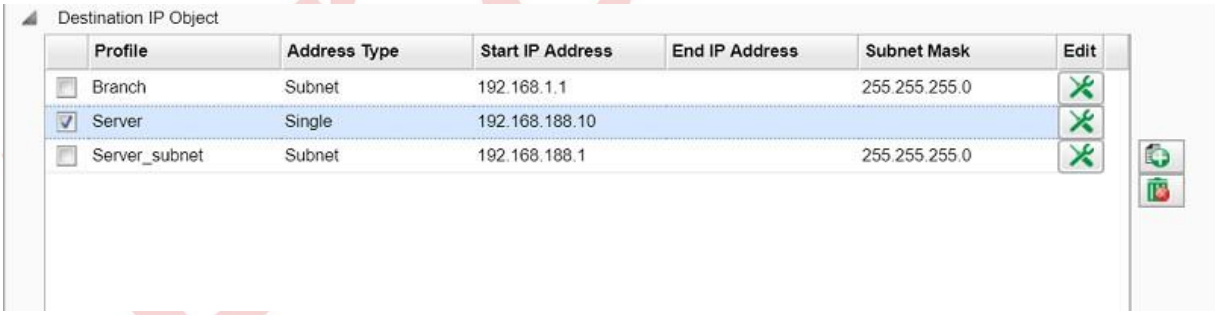




2. İkinci kuralı aşağıdaki gibi ekleyin
   Profile Name girin.

- Etkinleştirmeyi denetleyin.
- Action olarak “Accept”i seçin.
- Source IP’de Branch Office Network’ü için bir nesne ekleyin ve onu seçin Destination IP’de, Server’in IP’si için bir nesne ekleyin ve onu seçin.





Gerekli yapılandırma bu şekildedir.