

Cisco PIX Temel Firewall Konfigürasyonu

Mehmet Ali Karagöl / İTÜ'BİDB 2010

PIX firewall'da interface seçimi, inside ya da outside interface'in belirtilmesi, seçilen bu interface'lere göre rotaların düzenlenmesi temel olarak aşağıdaki şekilde yapılabilir. Öncelikle firewall'ın iç ve dış ayağının hangisi olacağının ve bu interface'lere güvenlik seviyelerinin atanması yapılır.

```
pixfirewall(config)# interface <interface_türü>
pixfirewall(config)# nameif <interface_adi>
pixfirewall(config)# security-level <0-100>
```

Örnek olarak aşağıdaki gibi bir konfigürasyon yapılabilir;

```
Agciyiz_Firewall(config)# interface Ethernet0
Agciyiz_Firewall(config-if)# nameif inside
Agciyiz_Firewall(config-if)# security-level 100 (Default Değeri 100'dür.)
```

```
Agciyiz_Firewall(config)# interface Ethernet1 (Default Değeri 0'dır.)
Agciyiz_Firewall(config-if)# nameif outside
Agciyiz_Firewall(config-if)# security-level 0
```

Daha sonra, belirlenen bu interface'lere ip adresleri aşağıdaki şekilde verilir.

```
Agciyiz_Firewall(config)# ip address {inside | outside} <ip adresi> <alt ağ maskesi>
```

Örnek konfigürasyona devam edecek olursak;

```
Agciyiz_Firewall(config)# ip address outside 122.16.201.3 255.255.255.224
Agciyiz_Firewall(config)# ip address inside 122.16.202.129 255.255.255.0
```

Örnekteki konfigürasyon için topolojide outside interface'e direkt olarak bağlı olan router'ın ip adresi **122.16.201.9** olsun. Bu durumda firewall tarafından yapılacak routing işlemi aşağıdaki satırla belirtilir.

```
Agciyiz_Firewall(config)# route outside 0.0.0.0 0.0.0.0 122.16.201.9
```

Eğer NAT yapılmak istenmiyorsa örnek konfigürasyon için aşağıdaki komut girilmelidir;

```
Agciyiz_Firewall(config)# nat (inside) 0 122.16.201.3 255.255.255.224
```

Buradaki "0" parametresi NAT yapılmayacağını gösteriyor.

Eğer NAT yapılmak istenirse aşağıdaki şekilde konfigürasyon yapılmalıdır.

```
Agciyiz_Firewall(config)# nat (inside) 1 0 0
```

Burada "1" parametresi NAT yapılacağını göstermesinin yanı sıra bu NAT satırı için oluşturulacak ip havuzunun da bu parametreyle konfigüre edilmesi gerektiğini belirtmektedir. 1'den sonra gelen iki tane 0 parametresi ise hangi ip uzayı için NAT yapılacağını belirtir ki, 0 0 olarak girilmesi tüm ip adreslerine izin verildiğini gösterir. Bunun yerine **122.16.200.0 255.255.255.0** olarak da belirtilebilirdi.

```
Agciyiz_Firewall(config)# global (outside) 1 122.16.201.12-122.16.201.20
```

```
Agciyiz_Firewall(config)# global (outside) 1 122.16.201.10
```

Yukarıdaki ilk satır belirli bir ip aralığının NAT ip havuzu olarak kullanılmasını sağlar. İkinci satırda da ilk satırda verilen aralığın yetersiz kaldığı durumlarda PAT yapılarak tek bir ip adresinden internete çıkılması sağlanmıştır.

Firewall'ın telnet bağlantısına açılması da IOS'ta olduğundan farklıdır.

```
pixfirewall (config)# telnet <ip adresi> <alt ağ maskesi> <interface_adi>
```

```
Agciyiz_Firewall(config)# telnet 122.16.200.5 255.255.255.255 inside
```

```
Agciyiz_Firewall(config)# telnet 122.16.10.0 255.255.255.0 inside
```

İlk satırda sadece **122.16.200.5** ip adresine telnet izni verilirken, ikinci satırda **122.16.10.0** network'ünün tamamına telnet izni verilmiştir.

Not: Bu konfigürasyon PIX firewall için geçerlidir ancak ASA ya da FWSM için de hemen hemen aynı konfigürasyon geçerlidir, çok küçük farklılıklar oluşabilir.

Firewall konfigürasyonundan farklı olarak, 6500 ya da 7600 serisi Cisco cihazlara modül olarak takılan FWSM'ye konsol bağlantısı yapılmak istenirse 6500 ya da 7600 (takılı olduğu cihaz) komut satırından aşağıdaki komut çalıştırılır.

```
Agciyiz_7600# session slot <slot_id> processor <processor_id>
```

```
Agciyiz_7600# session slot 3 processor 1
```