

Cisco cihazlarda faydalı bir ACL(erişim kontrol listeleri) yeniliği: **Named ACL Support for Noncontiguous Ports on an Access Control Entry**

Sınmaz KETENCİ – İTÜ/BİDB 2009

Cisco cihazlarda extended access-list'lerde **range** parametresi kullanılarak istenilen port aralıkları ifade edilebiliyor. Fakat range komutu ile belirtilen ilk ve son port arasındaki ardışık tüm portlar bu access-list'e match ediyor. Örnek verecek olursak sadece ftp ve telnet trafiğine izin vermek isteyen biri aşağıdaki ACL satırlarını kullanacaktır.

```
ip access-list extended ftp_telnet
permit tcp any any range 20 21
permit tcp any any eq 23
```

Senaryomuza göre 22 port yasaklı olduğundan range komutu ile tek satırda gerekli izinleri veremiyoruz. Eğer ssh bağlantısına izin veriliyorsa aşağıdaki tek satır ihtiyaçlarımızı karşılayacaktı.

```
ip access-list extended ftp_ssh_telnet
permit tcp any any range 20 23
```

12.2(25)S sürüm IOS ile birlikte gelen **Named ACL Support for Noncontiguous Ports on an Access Control Entry** özelliği sayesinde tek ACE(ACL satırı) ile ortak kaynak ve hedef için ayrı ayrı birbirini takip etmeyen 10'ar port belirtilebiliyor. Bu özellik sadece named, extended ACL'lerde kullanılabilir. Bunun en önemli getirisi kullanımı cihaz kaynaklarına bağlı kısıtlı olan ACE sayılarını minimuma indirmesi ve cihazların kontrol etmesi gereken satır sayısı azaldığından CPU ve RAM yükünün azalmasıdır.

Cihazların kısıtlı olan ACE kaynaklarındaki kazancı basit bir örnek ile daha anlaşılır kılalım. Aşağıda kullanım politikalarına bağlı olarak kullanıcıların erişimini kontrol eden bir ACL'nin bir bölümü gözükmekte. Aynı ihtiyaçların 2 farklı network yöneticisi tarafından ele alındığını düşünelim. İlk olarak 1. Network yöneticisinin en basit düzeyde erişim kontrolünde gerekli her port için bir ACE(ACL satırı) kullanarak yapacağı yapılandırmaya bakalım.

```
deny tcp any eq 20 any
deny tcp any eq 21 any
deny tcp any eq 23 any
deny tcp any eq 25 any
deny tcp any eq 53 any
deny tcp any eq 80 any
deny tcp any eq 110 any
deny tcp any eq 443 any
deny tcp any eq 411 any
deny tcp any eq 412 any
```

```

permit tcp any any eq 20
permit tcp any any eq 21
permit tcp any any eq 22
permit tcp any any eq 80
permit tcp any any eq 443

```

Oysa 2. network yöneticisi **Named ACL Support for Noncontiguous Ports on an Access Control Entry** özelliğini kullanarak yukarıdaki erişim kontrolünün tamamını aşağıdaki ACE ile sağlayabilir.

```

permit tcp any neq 20 21 23 25 53 80 110 443 411 412 any eq 20 21 22 80 443

```

Aşağıdaki iki ACL tamamen aynı işlevi yerine getirmektedir.

Extended IP access list netAdmin1

```

10 deny tcp any eq ftp-data any
20 deny tcp any eq ftp any
30 deny tcp any eq telnet any
40 deny tcp any eq smtp any
50 deny tcp any eq domain any
60 deny tcp any eq www any
70 deny tcp any eq pop3 any
80 deny tcp any eq 443 any
90 deny tcp any eq 411 any
100 deny tcp any eq 412 any
110 permit tcp any any eq ftp-data
120 permit tcp any any eq ftp
130 permit tcp any any eq 22
140 permit tcp any any eq www
150 permit tcp any any eq 443

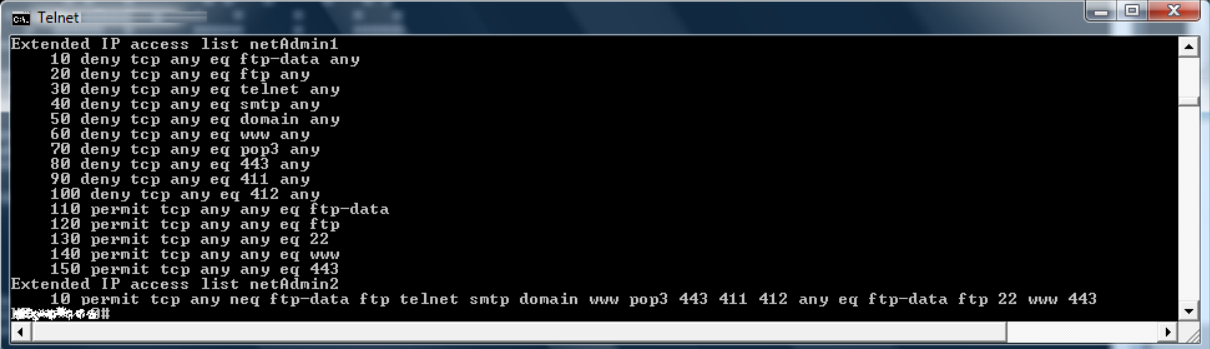
```

Extended IP access list netAdmin2

```

10 permit tcp any neq ftp-data ftp telnet smtp domain www pop3 443 411 412 any eq ftp-data ftp
22 www 443

```



```

CA Telnet
Extended IP access list netAdmin1
10 deny tcp any eq ftp-data any
20 deny tcp any eq ftp any
30 deny tcp any eq telnet any
40 deny tcp any eq smtp any
50 deny tcp any eq domain any
60 deny tcp any eq www any
70 deny tcp any eq pop3 any
80 deny tcp any eq 443 any
90 deny tcp any eq 411 any
100 deny tcp any eq 412 any
110 permit tcp any any eq ftp-data
120 permit tcp any any eq ftp
130 permit tcp any any eq 22
140 permit tcp any any eq www
150 permit tcp any any eq 443
Extended IP access list netAdmin2
10 permit tcp any neq ftp-data ftp telnet smtp domain www pop3 443 411 412 any eq ftp-data ftp
22 www 443

```

Son olarak bu özelliđin kullanılması için gereken şartları ve kısıtlamaları özetleyecek olursak;

-12.2(25)S ve üzeri IOS sürümlerinde bu destek gelmektedir.

-Sadece named, extended ACL ile kullanılabilir.

-Bir ACE(tek ACL satırı) için kaynak ve hedef için 10'ar tane port belirtilebilir.