ACL Oluşturma ve Firewall Teknolojilerinin Uygulunması

CCNA-Security

Cisco | Networking Academy®
Mind Wide Open™

Konular

4.0 Giriş

4.1 Access Control Listler

4.2 Firewall Teknolojileri

4.3 Zone-Based Policy Firewalllar

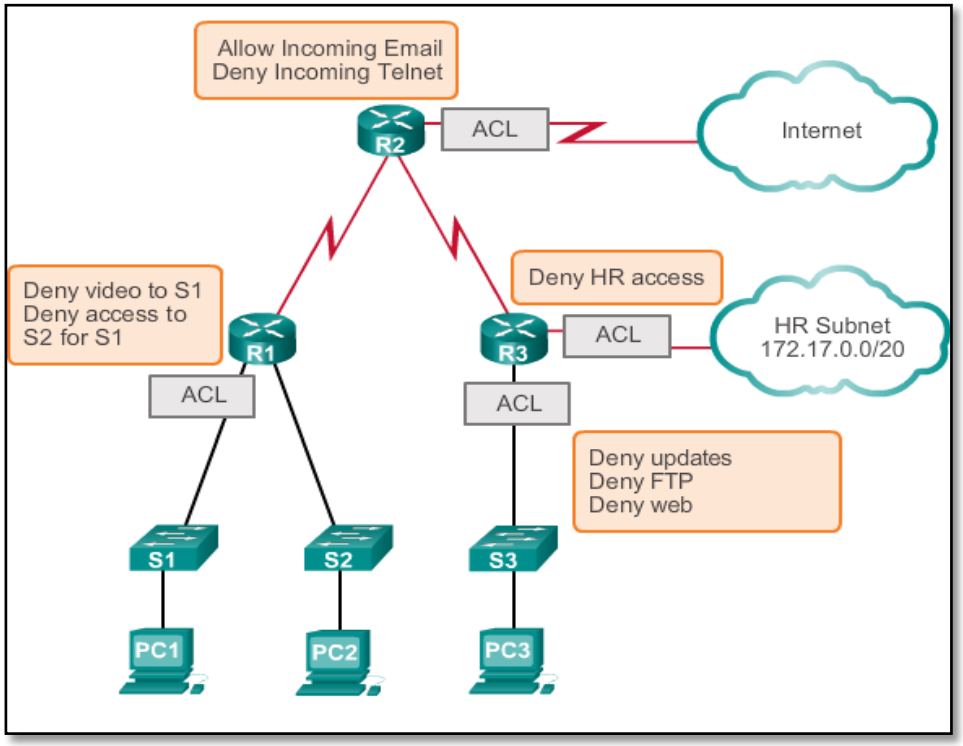
4.4 Özet

4.1 Access Control Lists (Erişim Kontrol Listeleri)

Cisco | Networking Academy®
Mind Wide Open™

Access Control List'lere Giriş

- Access Control Listler (ACLler) network ataklarını azaltmak ve trafiği kontrol etmek için yaygın olarak kullanılır
- Güvenlikle ilişkili ACLler IPv4, IPv6 adresleri ve TCP, UDP port numaraları için parametreler içerir



Standart ve Genişletilmiş IP ACL'ler

Standart Numara ile IP ACL

```
access-list {acl-#} {permit | deny | remark} source-addr
[source-wildcard] [log]
```

Parameter	Description
acl-#	This is a decimal number from 1 to 99, or 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Add a remark about entries in an IP access list to make the list easier to understand and scan.
source-addr	Number of the network or host from which the packet is being sent. There are two ways to specify the *source-addr* : • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) 32-bit wildcard mask to be applied to the source. Places ones in the bit positions you want to ignore.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the ACL number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at five-minute intervals, including the number of packets permitted or denied in the prior five-minute interval.

Standart ve Genişletilmiş IP ACL'ler

- ACL numaraları1–99 veya 1300–1999 aralığındaysa standart IPv4'dür.
- Standart ACL'ler paketlerin IP başlığındaki source IP adres alanındaki eşleşmeyi kontrol eder.
- Standard ACL'ler paketlerin Layer 3 source bilgilerini kullanarak filtrelemek için kullanılır.

Standart ve Genişletilmiş IP ACL'ler

Genişletilmiş Numaralı IP ACL'ler

```
access-list { acl-# } { permit | deny | remark } protocol
source-addr [ source-wildcard ]  destination-
addr [destination-wildcard ] [ operator operand ] [port]
[ established ][ log ]
```

Parameter	Description
	199 (for an extended IP ACL) and 2000 to 2699 (expanded IP ACLs).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Used to enter a remark or comment.
protocol	Name or number of an Internet protocol. Common keywords include **icmp**, **ip**, **tcp**, or **udp**. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword.
source-addr	Number of the network or host from which the packet is being sent.
source-wildcard	Wildcard bits to be applied to source.
destination-addr	Number of the network or host to which the packet is being sent.
destination-wildcard	Wildcard bits to be applied to the destination.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) The decimal number or name of a TCP or UDP port.
established	(Optional) For the TCP protocol only: Indicates an established connection.

Standart ve Genişletilmiş IP ACL'ler

ACL numarası 100–199 veya 2000–2699 aralığındaysa genişletilmiş ACLdir.

Genişletilmiş ACL IP paketini şu kriterlere göre filtreler:

- Source ve destination IP adresleri
- Source ve destination TCP ve UDP Portlar
- Protokol Türü

Standart ve genişletilmiş ACLler:

- IP access-group komutu kullanarak bir interface üzerine uygulanabilir.
- access-class komutu kullanarak bir VTY portuna uygulanabilir

Standart ve Genişletilmiş İsimli IP ACL'ler

`Router(config)#` **`ip access list [standard | extended]`** *`name_of_ACL`*

Standart İsimli IP ACL örneği

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Genişletilmiş İsimli IP ACL örneği:

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

ACL Eşleşmelerini Loglama

Log parameter komutu log eşleşmeleri için kullanılabilir. Şu bilgiler içerilir:

- **Action** - Permit veya deny
- **Protocol** - TCP, UDP veya ICMP
- **Source and destination** - IPv4 veya IPv6 adresleri
- **TCP and UDP** - Source ve destination port numaraları
- **ICMP** - Mesaj türü

Log mesajları ilk paket eşleşmesinde üretilir ve sonra beş dakikalık aralıklarla tekrar edilir

Erişim Kontrol Giriş (ACE) Kuralları

Bir ACL bir veya daha fazla ACE kuralı ile oluşturulur. İşlemlerin askıya alınması aşağıdaki durumlar için gözönünde bulundurulur.

- **Implicit deny all** – Tüm ACLler bir implicit deny all cümlesi ile sona erer.
- **Standart ACL paket filtreleme**
  - Standart ACLler sadece source adresi kullanarak paket filtreleme ile sınırlıdır.
  - Genişletilmiş ACLler güvenlik politikası için diğer işleri de yapabilir.
- **Cümlelerin sıralaması**
  - ACLler ilk eşleşme için politikaya sahiptir; bir cümle ile eşleşme olursa diğer cümlelere bakılmaz.
  - Üst sıralardaki kural cümlelerinin alt sıralardaki cümleleri geçersiz kılmadığından emin olunmalıdır.
  - Spesifik kurallar üst sıralara, genel kurallar alt sıralara yerleştirilir.

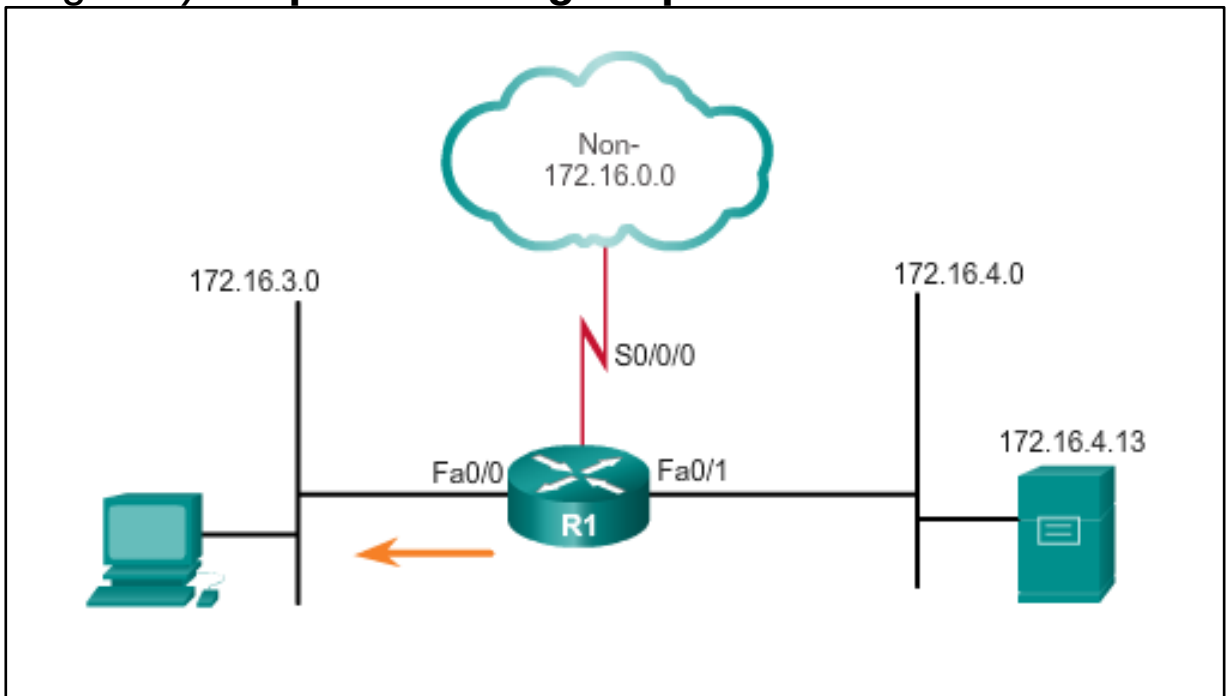
Erişim Kontrol Giriş (ACE) Kuralları

- **Doğrudan filtreleme**
  - ACLler, interface'e gelen veya interfaceden çıkan paketlere uygulanabilir.
  - ACL filtreleme yaparken verinin yönüne göre çifte kontrol yapar.
- **Özel paketler**
  - Router tarafından üretilen rota tablosu güncellemeleri gibi paketler çıkış ACL kurallarına tabi tutulmaz.
  - Eğer güvenlik ilkesi gereği bu tip paketlerin filtrelenmesi gerekiyorsa komşu routerın giriş yönünde filtrelenmelidir.
- **ACLleri Değiştirme**
  - ACL'e yeni kurallar eklenebilir, yeni eklenen her kural en alt sıraya eklenir.
  - Bir ACL'i düzenlemek için sıra numarası bilgisi kullanılabilir.
  - ACL kural cümlelerinin sıra numarasına dayalı olarak yukarıdan aşağıya yani küçük değerli olanından büyük değerli olanına doğru işlenir.

Standart ACL Örneği

172.16.4.0 alt ağından gelen paketlerin yasaklanması, diğer tüm trafiğin geçmesine izin verilmesi

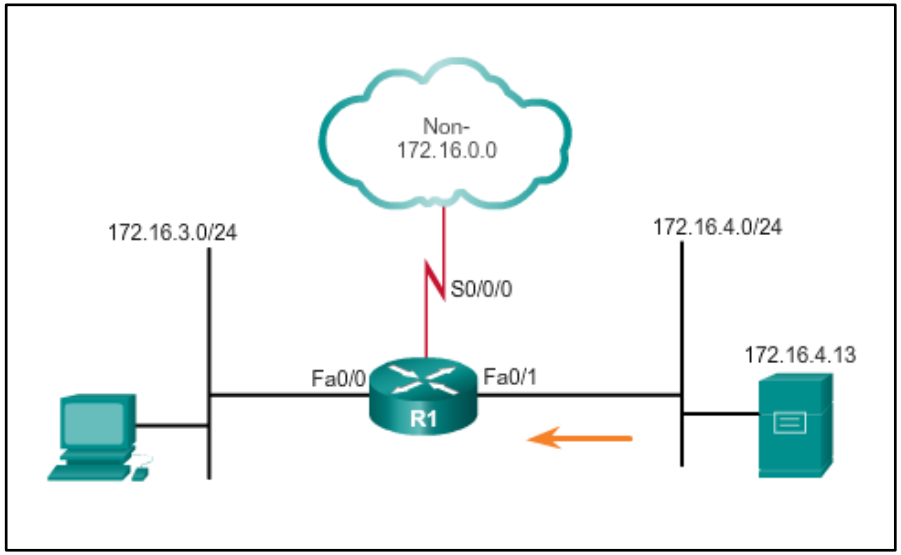
- `R1(config)# access-list 1 deny 172.16.4.0 0.0.0.255`
- `R1(config)# access-list 1 permit any`
- `R1(config)# interface FastEthernet 0/0`
- `R1(config-if)# ip access-group 1 out`



Standart ACL Örneği

Bir alt ağdaki FTP trafiğinin diğer alt ağa geçmesini yasaklama.

- `R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21`
- `R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20`
- `R1(config)# access-list 101 permit ip any any`



Genişletilmiş ACL'i Düzenleme

Üç kural içeren mevcut bir ACL:

```
Router# show access-lists
Extended IP access list 101
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
```

ACL düzenlenerek yeni bir kural ekleniyor ve 20 numaralı kural değiştiriliyor:

```
Router(config)# ip access-list extended 101
Router(config-ext-nacl)# no 20
Router(config-ext-nacl)# 5 deny tcp any any eq telnet
Router(config-ext-nacl)# 20 deny udp any any
```

Güncellenmiş ACL 4 kurala sahip hale geldi:

```
Router# show access-lists
Extended IP access list 101
     5 deny tcp any any eq telnet
    10 permit tcp any any
    20 deny udp any any
    30 permit icmp any any
```

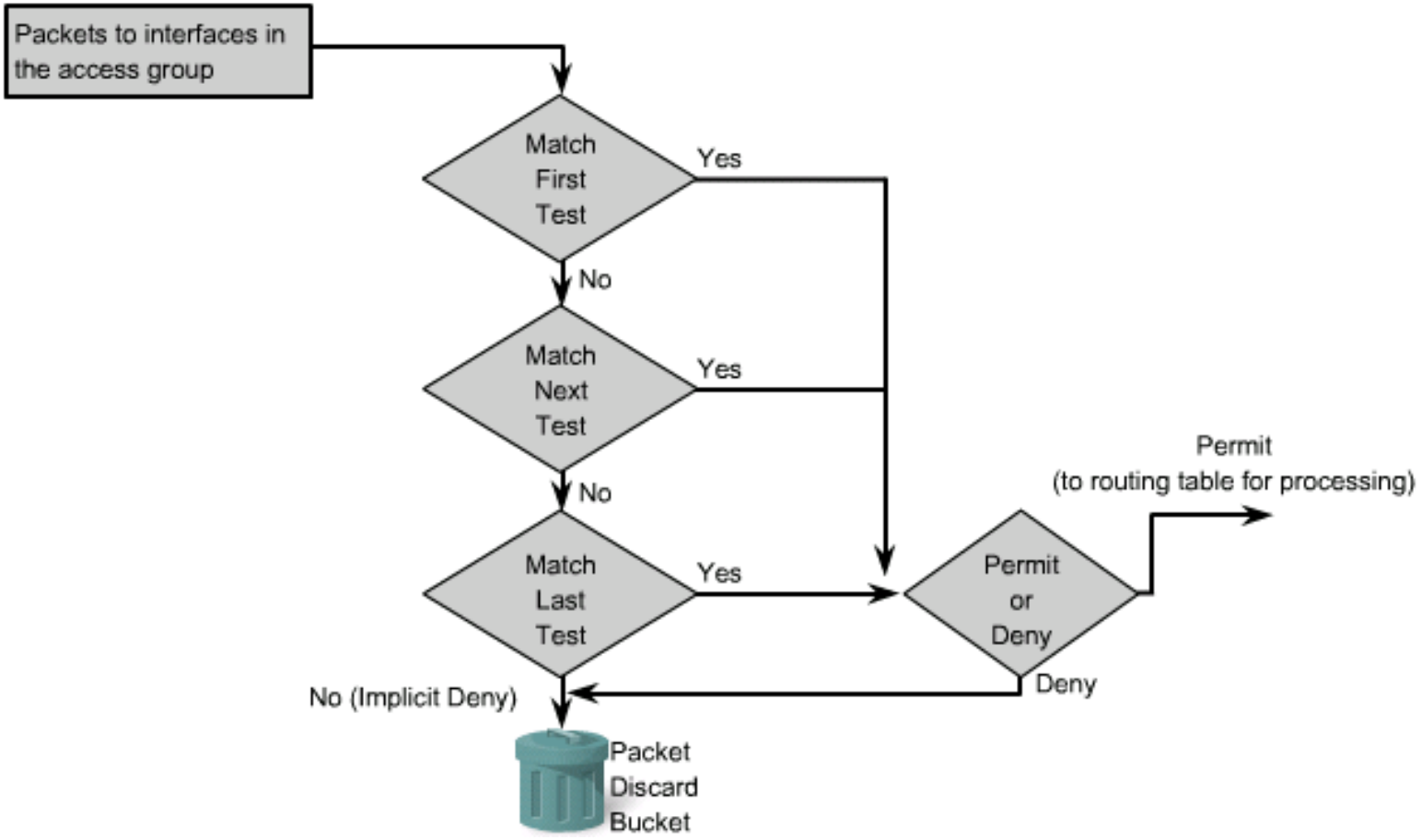
ACL için Topoloji ve Trafik Akışı

Router ACL Eşleşmelerini Nasıl Yönetir?

- Bir network cihazı için trafiğin yönü ingress (içeri akan-inbound) veya egress (dışarı akan) olarak tanımlanır.
- Inbound trafik routera gelen ve yönlendirme tablosuna ulaşan trafiğe denir.
- Outbound trafik ise router yönlendirme tablosunda karar verildikten sonra yönlendirilen trafiktir.
- Cihaz ve ACL'e bağlı olarak geri dönen trafik otomatik olarak izlenebilir.

Router ACL Eşleşmelerini Nasıl Yönetir?

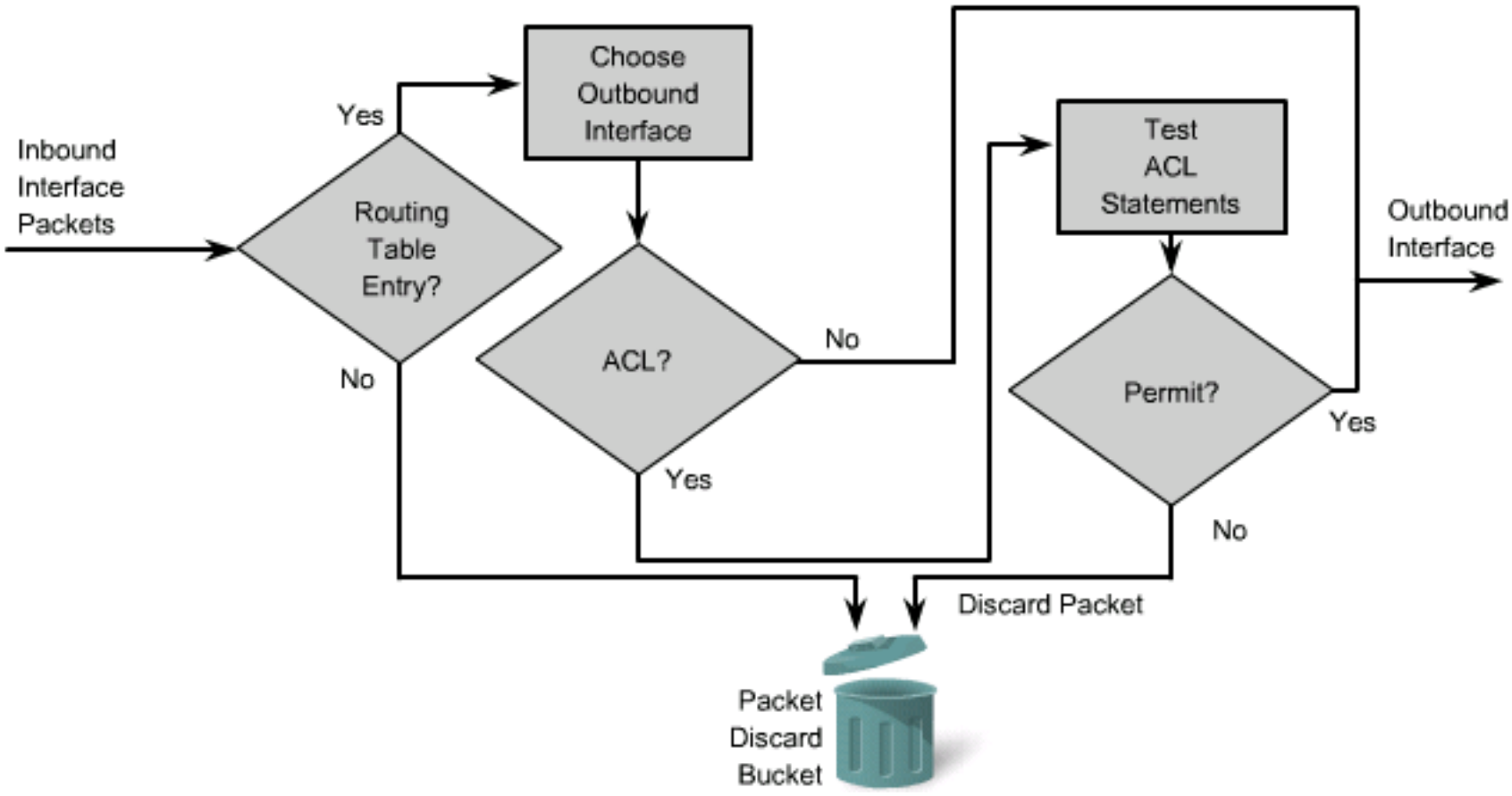
Inbound ACL İşlem Akışı



ACL için Topoloji ve Trafik Akışı

Router ACL Eşleşmelerini Nasıl Yönetir?

Outbound ACL İşlem Akışı



ACL Yerleştirme

Standart ACL Yerleştirme

- Standart ACLler hedefe mümkün olan en yakın yere yerleştirilir
- Sadece source adresine bağlı olarak filtreleme yapar.
- Standart ACL'in kaynak tarafına yakın yerleştirilmesi geçerli trafiğin bloklanmasına yol açar.

Genişletilmiş ACL Yerleştirme

- Mümkün olduğunca kaynağa en yakın routera yerleştirilir.
- Hedefe yakın yere yerleştirme network kaynaklarının verimsiz kullanımına yol açar.

ACL Tasarımı

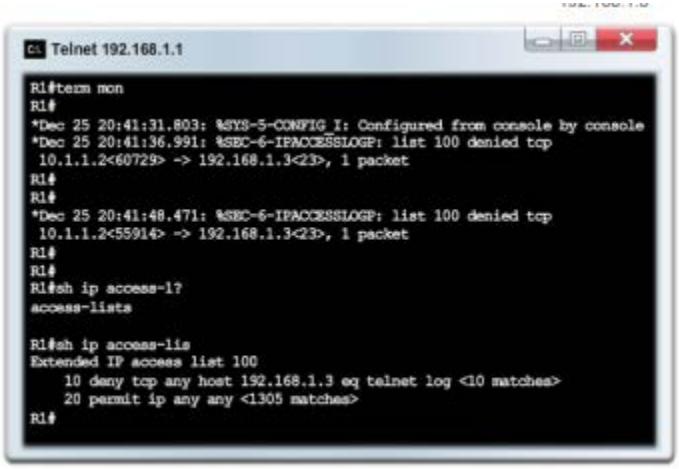
- ACLler bazı trafik türlerini engellemek için kullanılır.
- ACLler güvenli trafik türlerinin geçişine izin vermek için kullanılır. HTTPS (TCP port 443) gibi.
- Verimli ACL kullanımı için hangi portların bloklanıp hangi portların geçişine izin verileceği açıkça belirlenmelidir.
- Bir cihazda hangi portların açık olduğu Nmap programıyla belirlenebilir.

ACL Fonksiyonlarını Doğrulama

show running-config komutu

```
R1# show running-config | begin interface Serial0/0/0
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group 100 in
 clock rate 128000
!
<output omitted>
!
!
!
access-list 100 deny tcp any host 192.168.1.3
eq telnet log
access-list 100 permit ip any any log
!
<output omitted>
```

show ip access-lists komutu



Time-Based ACL

- Time-based ACL, zamana bağlı olarak erişim izinleri tanımlar.
- Timed-based ACL ile günün saati, haftanın günü, ayın günü şeklinde trafik geçişlerini yapılandırabilir.

Time-Based ACL Yapılandırma

Step 1

```
R1(config)# time-range EVERYOTHERDAY
R1(config-time-range)# periodic Monday Wednesday Friday 8:00 to
17:00
```

Step 2

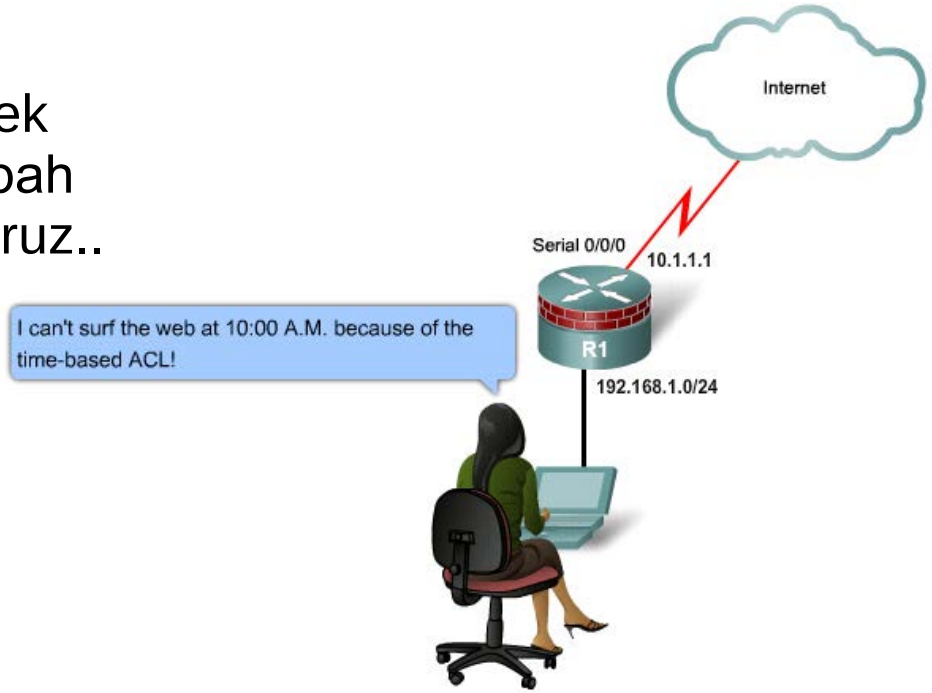
```
R1(config)# access-list 101 permit tcp 192.168.10.0 0.0.0.255
any eq telnet time-range EVERYOTHERDAY
```

Step 3

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 101 out
```

Time-Based ACL Senaryosu

Kullanıcıların iş saatlerinde internete girmelerine izin vermek istemiyoruz. Akşam beşten sabah yediye kadar izin vermek istiyoruz..



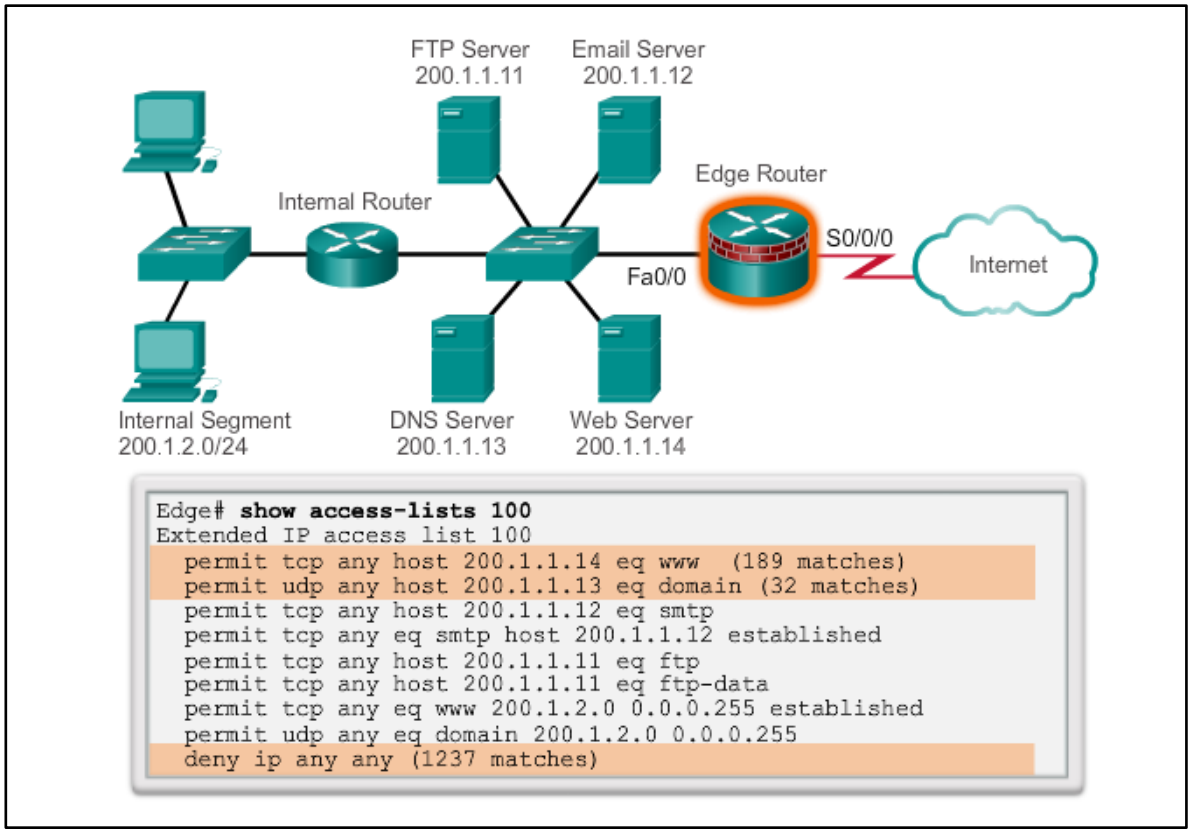

```
R1(config)# time-range EMPLOYEE-TIME
R1(config-time-range)# periodic weekdays 12:00 to 13:00
R1(config-time-range)# periodic weekdays 17:00 to 19:00
R1(config-time-range)# exit
R1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 any time-range EMPLOYEE-TIME
R1(config)# access-list 100 deny ip any any
R1(config)# interface FastEthernet 0/1
R1(config-if)# ip access-group 100 in
R1(config-if)# exit
```

Karmaşık ACL Uygulamalarında Hata Bulma

ACL Doğrulama ve Hata Bulma

Şu iki komut hata bulma için kullanışlıdır:

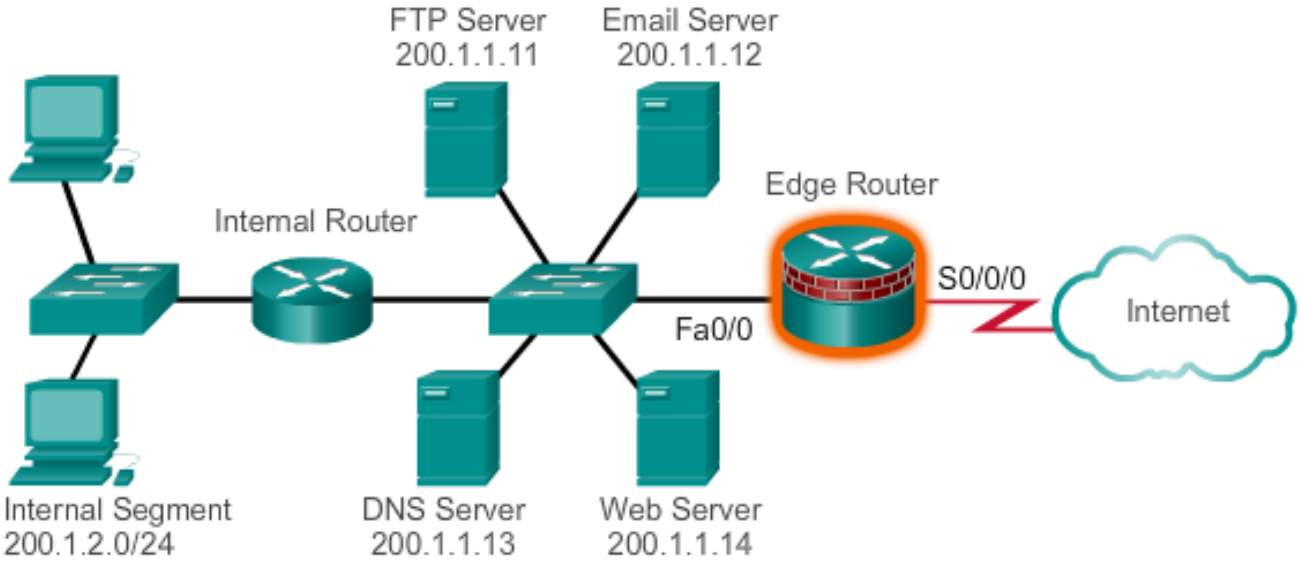
- **`show access-lists`**
- **`debug ip packet (detaylar için)`**




```
Edge# show access-lists 100
Extended IP access list 100
    permit tcp any host 200.1.1.14 eq www  (189 matches)
    permit udp any host 200.1.1.13 eq domain (32 matches)
    permit tcp any host 200.1.1.12 eq smtp
    permit tcp any eq smtp host 200.1.1.12 established
    permit tcp any host 200.1.1.11 eq ftp
    permit tcp any host 200.1.1.11 eq ftp-data
    permit tcp any eq www 200.1.2.0 0.0.0.255 established
    permit udp any eq domain 200.1.2.0 0.0.0.255
    deny ip any any (1237 matches)
```

Karmaşık ACL Uygulamalarında Hata Bulma

ACL Debug




```
Edge# debug ip packet
IP packet debugging is on

IP:s=200.1.2.2 (FastEthernet0/0),d=172.69.2.42 (Serial0/0/0),
g=172.69.16.2,forward
IP:s=200.1.2.2 (FastEthernet0/0),d=172.16.2.42 (Serial0/0/0),
g=172.69.16.2,forward
IP:s=200.1.2.2 (FastEthernet0/0),d=172.69.43.126 (Serial0/0/0),
g=172.69.16.2,forward
IP:s=200.1.2.2 (FastEthernet0/0),d=172.16.2.42 (Serial0/0/0),
g=172.69.16.2,access denied
```

Spoofing ve DoS Ataklarını Azaltma

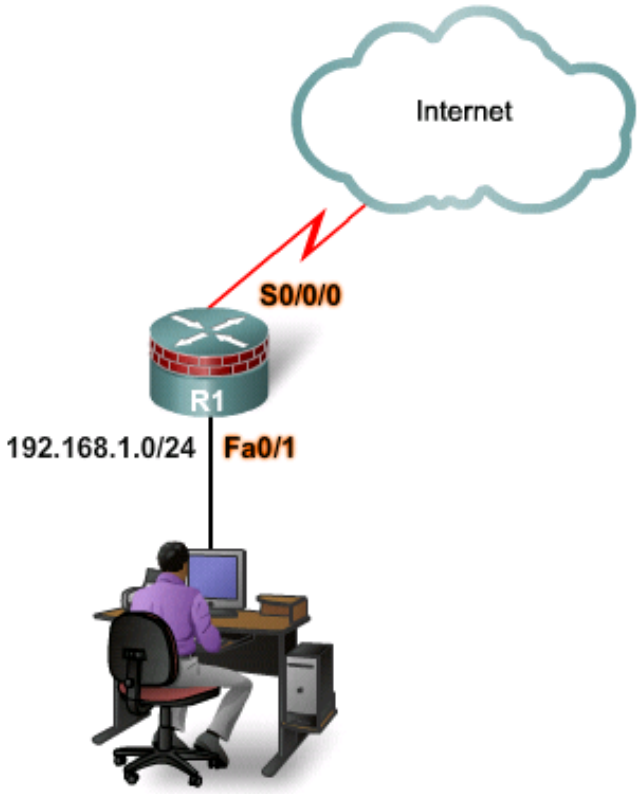
- ACLler bir çok network tehdidini azaltmak için kullanılabilir
  - IP adres spoofing, inbound ve outbound trafikte
  - DoS TCP SYN saldırıları
  - DoS smurf saldırıları
- ACLler şu trafikleri filtreleyebilir
  - ICMP mesajları (inbound ve outbound)
  - traceroute

ACL ile Saldırı Azaltma

ACL ile AntiSpoofing

Source alanında aşağıdaki IP adresleri bulunan tüm paketleri yasakla:

- Tüm local host adresleri (127.0.0.0/8)
- Tüm rezerve private adresler (RFC 1918)
- Tüm IP multicast adres aralığı (224.0.0.0/4)




```
R1(config)# access-list 150 deny ip 0.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 10.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any
R1(config)# access-list 150 deny ip 192.168.0.0 0.0.255.255 any
R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any
R1(config)# access-list 150 deny ip host 255.255.255.255 any
```

ACL ile Saldırı Azaltma

Gerekli Trafiğe İzin Verme

DNS, SMTP ve FTP gibi yaygın kullanılan servislere firewall'dan geçiş izni verilmelidir

```
R1(config)# access-list 180 permit udp any host 192.168.20.2 eq
domain
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1
eq telnet
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1
eq 22
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1
eq syslog
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1
eq snmptrap
```

ICMP Abuse (Suistimal) Saldırıları Azaltma

- Hackerlar ping demetleri ve DoS flood ataklarını ICMP paketlerini kullanarak yaparlar ve host rota tablosunu silmek için ICMP redirect mesajlarını kullanırlar.
- ICMP echo ve redirect mesajları routera girişte bloklanmalıdır.

Inbound on S0/0/0

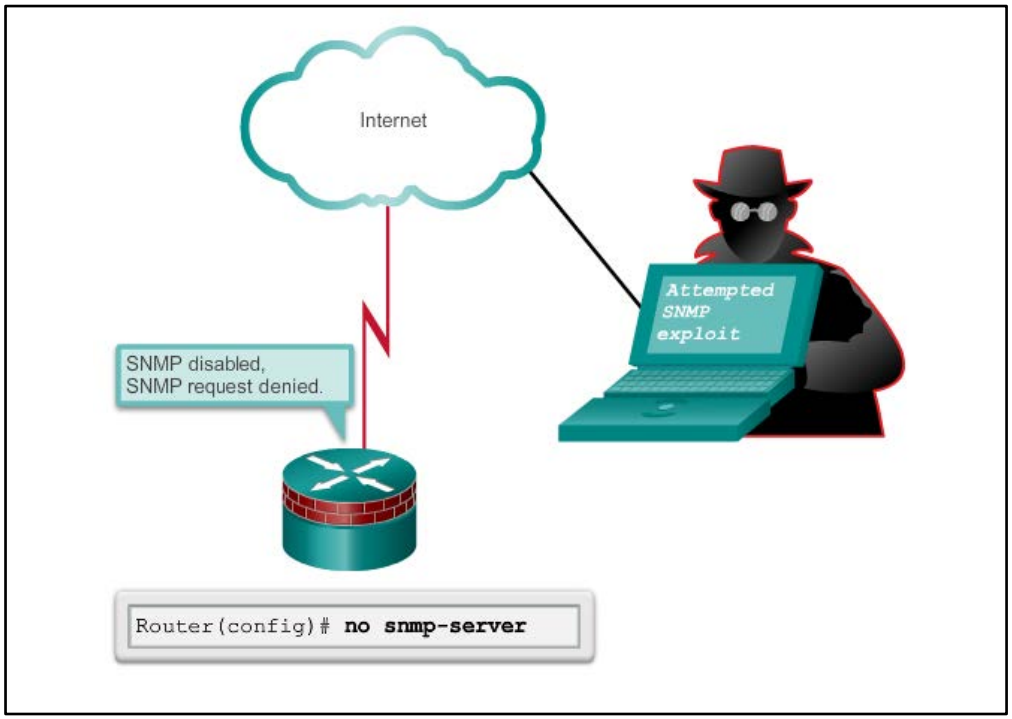
```
R1(config)# access-list 112 permit icmp any any echo-reply
R1(config)# access-list 112 permit icmp any any source-quench
R1(config)# access-list 112 permit icmp any any unreachable
R1(config)# access-list 112 deny icmp any any
R1(config)# access-list 112 permit ip any any
```

Inbound on Fa0/0

```
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255
any echo
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255
any parameter-problem
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255
any packet-too-big
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255
any source-quench
R1(config)# access-list 114 deny icmp any any
R1(config)# access-list 114 permit ip any any
```

SNMP İstismarlarını Azaltma

- SNMP gibi yönetim protokolleri network cihazlarını uzaktan görüntüleme ve yönetme amaçlarıyla kullanılırken istismara maruz kalabilirler.
- ACL interface'e uygulanarak yetkisiz sistemlerden gelen SNMP paketleri bloklanır.



IPv6 ACL'leri

- IPv6 ACLleri de IPv4 ACLlerine benzer. Kaynak ve hedef adreslere göre, kaynak ve hedef port numaralarına göre ve protokol türlerine göre filtreleme yapmaya imkan sağlar
- **`ipv6 access-list`** komutu kullanılır.

```
Router(config)# ipv6 access-list access-list-name
Router(config-ipv6-acl)# {permit | deny} protocol [source-ipv6-
prefix/prefix-length] [operator operand] [destination-ipv6-prefix/prefix-
length] [operator operand]
```

- IPv6 ACL'İ bir interface'e uygulanırken **`ipv6 traffic-filter`** *`access-list-name`* **`{in | out}`** komutu kullanılır.

IPv6 ACL'leri

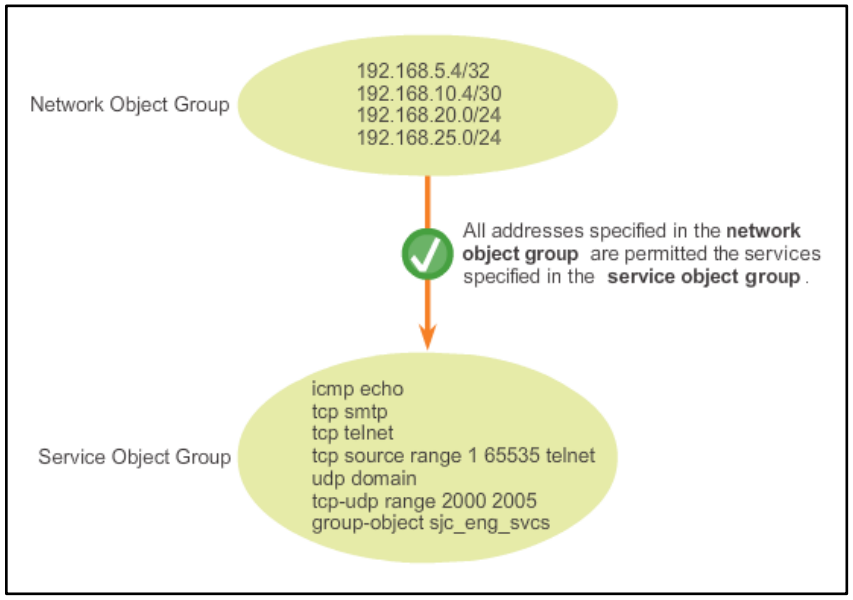
- Tüm IPv6 ACLleri iki permit cümlesiyle komşu keşif paketlerinin gönderilmesini ve alınmasını sağlar.
  - **permit icmp any any nd-na**
  - **permit icmp any any nd-ns**
- Nd-na: Neighbour discovery-neighbour advertisement
  nd-ns: Neighbour discovery-neighbour solicitation.
- IPv4 ACLleri gibi, tüm IPv6 ACLleri son cümle olarak bir deny ifadesine sahiptir:

  deny ipv6 any any
- Bu cümleler konfigürasyon çıktısında görünmeyecektir. En iyi yol yukarıdaki üç komutu elle girmektir.
- Deny cümlesinin elle girilmesi aynı zamanda deny edilen paketlerin loglanmasını da sağlar.

Nesne Grupları

- Nesne grupları kullanıcıları, cihazları veya protokolleri gruplamak için kullanılır.
- Bu gruplar erişim kontrol politikaları oluşturulurken grup halinde tanımlama yapmak için kolaylık sağlar.
- Bu özellik yöneticiye tek tek IP adreslerini, portları, cihazları yazmak yerine toplu yazma imkanı tanır.
- IPv4 ve IPv6 ACLlerinde kullanılabilir.

Network ve Servis Nesne Grupları



- Nesne grupları tekil isimlere sahip olmalıdır.
- Mevcut gruba yeni nesne eklenebilir.
- Host, port veya servis gibi nesneler gruplanabilir.
- Eğer bir ACE içinde kullanılıyorlarsa nesne grupları silinemez.

ACE içinde Nesne Grupları (Object Groups) Kullanımı

Network ve Servis Nesne Grupları Yapılandırma

```
Router> enable
Router# configure terminal
Router(config)# object-group service eng_srv_group
Router(config-service-group)# icmp echo
Router(config-service-group)# tcp smtp
Router(config-service-group)# tcp telnet
Router(config-service-group)# tcp source range 1 65535 telnet
Router(config-service-group)# udp domain
Router(config-service-group)# tcp-udp range 2000 2005
Router(config-service-group)# group-object sjc_eng_svcs
```

- **Bir nesne grubunu diğeri içine almak mümkündür. Bu örnekte önceden yazılmış sjc_eng_svcs, yeni oluşturulan eng_srv_group içine alınabilir**

ACE içinde Nesne Grupları (Object Groups) Kullanımı

Nesne Grubu Temelli ACL

- Bu ACL'de **eng_network_group** ile belirtilmiş tüm adresler ve servisler, **eng_srv_group** ile belirtilen servislere izinli hale getiriliyor.
- Örnekte protokol argümanı tcp, udp ve icmp gerekli değildir. Çünkü protokol nesne grubunda oluşturulmuştu.

```
Router# configure terminal
Router(config)# ip access-list extended acl_policy
Router(config-ext-nacl)# permit object-group eng_srv_group
object-group eng_network_group any
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
```