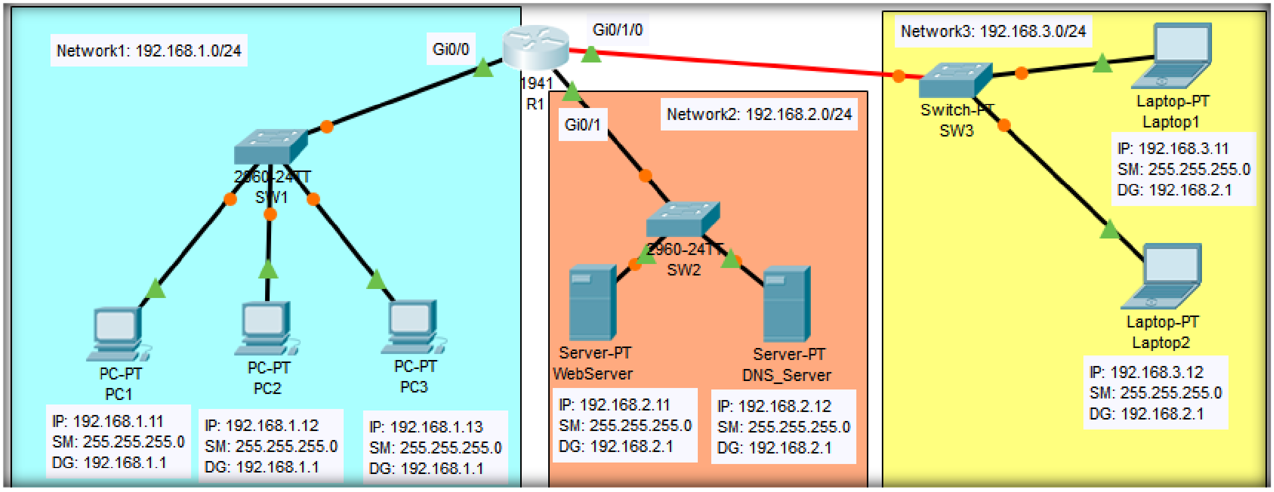
Ağ Yöneticileri Derneği
CCNA3 LAB 02 - PROJE ÇÖZÜMÜ
Standard ACL Uygulamasi



ÖN BİLGİ:

// ACLyazımında isim veya numaralı kullanılanilir.

- STANDARD ACL numaraları: 1-99, 1300-1399
- Standart ACL'ler sadece **SOURCE adrese** göre yazılır. (permit | deny | remark)
- Standard ACL'ler hedefe en yakın cihazda yazılır. (mümkün olduğu kadar hedefe yakın yazılması tercih edilir.)
- ACL’nin sonunda gizli bir <deny any> satırı bulunur. ACL ile eşleşmeyen tüm trafik çöpe atılır.

// ACL YAZMA ADIMLARI:

1) ACCESS LIST yaratılır (Standard veya Extended)
2) ACCESS LIST istenilen interface INBOUND veya OUTBOUND yönünde uygulanır.

// ACL Konfunda Sorun Çözme Komutları:

show running-config
show access-lists // ACL'ler listelenir. Kaç paketin ilgili satırla eşleştiği gözlemlenebilir
show ip interface Gi 0/0 // ACL nin interface'e uygulanıp uygulanmadığı görülebilir.

//R1 Yapılandırması	//R2 Yapılandırması

R1# **show access-lists**
 	
Standard IP access list 21
  10 deny host 192.168.1.11
  20 deny host 192.168.1.12
  30 deny host 192.168.1.13
  40 permit host 192.168.1.14
  50 permit host 192.168.1.15
  60 deny host 192.168.1.16
  70 permit host 192.168.1.17
  80 permit host 192.168.1.18
 	
Standard IP access list 45
  10 permit host 192.168.2.11
  20 permit host 192.168.2.12
  30 permit host 192.168.2.13
  40 permit host 192.168.2.15
  50 permit 192.168.2.0 0.0.0.255
 	
Standard IP access list 55
  10 permit 192.168.3.0 0.0.0.255
  20 deny any
	R1(config)# **no access-list 45**
	R1(config)# **no access-list 55**
	R1(config)# **exit**
	
	R1#**show access-lists**
	Standard IP access list 21
	  10 deny host 192.168.1.11
	  20 deny host 192.168.1.12
	  30 deny host 192.168.1.13
	  40 permit host 192.168.1.14
	  50 permit host 192.168.1.15
	  60 deny host 192.168.1.16
	  70 permit host 192.168.1.17
	  80 permit host 192.168.1.18

ADIM2:

ACL Yazılımı ve Ilgili Interface'e doğru yönde uygulanması:

```
access-list 1 deny 192.168.1.11 0.0.0.0        ---- Sadece 192.168.1.11 Source IP'sini engelleyen bir ACL yazdık
access-list 1 remark YASAKLI IP 192.168.1.11
access-list 1 permit 192.168.1.0 0.0.0.255  ---- 255.255.255.0 Subnet Maskesinin Wildcard Maskesi 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit any                       ---- İstenirse geri kalan tüm Source IP'lerine izin verilebilir.
<access-list 1 deny any>
```

Not: Bu ACL'nin R1 de ***Gi0/0 interface'inde IN*** yönünde uygulanması durumunda 192.168.1.11 IP'li cihaz hem 192.168.2.0/24 hem de 192.168.3.0/24 networküne bağlanamaz. 192.168.1.11 IP'li cihazın sadece sunucu ağına erişimini yasaklayacak Standard bir ACL yazmak istiyorsak bu ACL'yi hedefe en yakın nokta olan R1'in Gi0/1 interface'inde OUT yönünde uygulamamız gerekiyor.

```
interface Gi 0/1
 ip access-group 1 out                    ---- ACL'yi Gi0/1 arayüzüne Router'dan çıkan trafik için uyguladık
```

KONTROL KOMUTLARI:

```
R1# show access-lists 1
        Standard IP access list 1
          deny host 192.168.1.11
          permit 192.168.1.0 0.0.0.255
          permit 192.168.3.0 0.0.0.255

R1# show ip interface Gi 0/1
GigabitEthernet0/1 is up, line protocol is up
        Internet address is 192.168.2.1/24
        Broadcast address is 255.255.255.255
        Address determined by setup command
        MTU is 1500 bytes
        Helper address is not set
        Directed broadcast forwarding is disabled
        Outgoing access list is 1
        Inbound access list is not set
```

```
PC1 C:\> ping 192.168.2.11
Pinging 192.168.2.11 with 32 bytes of data:
 Reply from 192.168.1.1: Destination host unreachable.
 Reply from 192.168.1.1: Destination host unreachable.
 Reply from 192.168.1.1: Destination host unreachable.

PC2 C:\> ping 192.168.2.11
Pinging 192.168.2.11 with 32 bytes of data:
 Reply from 192.168.2.11: bytes=32 time<1ms TTL=127
 Reply from 192.168.2.11: bytes=32 time<1ms TTL=127

R1#show access-lists 1
        Standard IP access list 1
          deny host 192.168.1.11 (4 match(es))
          permit 192.168.1.0 0.0.0.255 (8 match(es))
          permit 192.168.3.0 0.0.0.255
```

ADIM4:

//R1'de LAPTOP_KORUMA isimli ACL yazılması

```
R1(config)# ip access-list standard LAPTOP_KORUMA
R1(config-std-nacl)#  deny 192.168.1.0 0.0.0.255
R1(config-std-nacl)#  permit 192.168.2.0 0.0.0.255
R1(config-std-nacl)#  permit 192.168.4.0 0.0.0.255
R1(config-std-nacl)#  permit 192.168.5.0 0.0.0.255
R1(config-std-nacl)#  permit any

R1(config)# interface Gi 0/1/0
R1(config-if)# ip access-group LAPTOP_KORUMA out

R1# show access-lists
……
 Standard IP access list LAPTOP_KORUMA
   10 deny 192.168.1.0 0.0.0.255
   20 permit 192.168.2.0 0.0.0.255
   30 permit 192.168.4.0 0.0.0.255
   40 permit 192.168.5.0 0.0.0.255
   50 permit any
```

```
R1(config)#ip access-list standard LAPTOP_KORUMA
R1(config-std-nacl)# no 30
R1(config-std-nacl)# 5 permit host 192.168.1.11

R1# show access-lists
Standard IP access list LAPTOP_KORUMA
  5   permit host 192.168.1.11
  10 deny 192.168.1.0 0.0.0.255
  20 permit 192.168.2.0 0.0.0.255
  40 permit 192.168.5.0 0.0.0.255
  50 permit any

PC1 C:\> ping 192.168.3.11
Reply from 192.168.3.11: bytes=32 time<1ms
Reply from 192.168.3.11: bytes=32 time<1ms

PC2 C:\> ping 192.168.3.11
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

```
R1# show access-lists
Standard IP access list LAPTOP_KORUMA
   5 permit host 192.168.1.11 (4 match(es))
 10 deny 192.168.1.0 0.0.0.255 (4 match(es))
 20 permit 192.168.2.0 0.0.0.255
 40 permit 192.168.5.0 0.0.0.255
 50 permit any
```

ADIM6:   //21 No’Lu ACL’yi Düzenleme

```
R1#show access-lists
  Standard IP access list 21
   10 deny host 192.168.1.11
   20 deny host 192.168.1.12
   30 deny host 192.168.1.13
   40 permit host 192.168.1.14
   50 permit host 192.168.1.15
   60 deny host 192.168.1.16
   70 permit host 192.168.1.17
   80 permit host 192.168.1.18
```

```
R1(config)# ip access-list standard 21
R1(config-std-nacl)# no 10
R1(config-std-nacl)# no 20
R1(config-std-nacl)# no 30
R1(config-std-nacl)# no 60
R1(config-std-nacl)# end
R1#wr
Building configuration...
[OK]

R1#show access-lists
  Standard IP access list 21
   40 permit host 192.168.1.14
   50 permit host 192.168.1.15
   70 permit host 192.168.1.17
   80 permit host 192.168.1.18
```

Adım 7: // SW1 ve SW2’nin Temel Konfigurasyonu, SADECE 192.168.1.12’ye telnet izni verilmesi.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname SW1
SW1(config)# enable secret cisco
!
SW1(config)# line vty 0 15
SW1(config-line)# password cisco
SW1(config-line)# login
SW1(config-line)# exit
!
SW1(config)# interface vlan 1
SW1(config-if)#ip address 192.168.1.101 255.255.255.0
SW1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
SW1(config-if)# exit
SW1(config)# ip default-gateway 192.168.1.1
!
SW1(config)# ip access-list standard VTY_ERISIM
SW1(config-std-nacl)# permit host 192.168.1.12
SW1(config-std-nacl)# deny any
SW1(config-std-nacl)# exit
!
SW1(config)# line vty 0 15
SW1(config-line)# access-class VTY_ERISIM in
```

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname SW2
SW2(config)# enable secret cisco
!
SW2(config)# line vty 0 15
SW2(config-line)# password cisco
SW2(config-line)# login
SW2(config-line)# exit
!
SW2(config)# interface vlan 1
SW2(config-if)#ip address 192.168.2.101 255.255.255.0
SW2(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
SW2(config-if)# exit
SW2(config)# ip default-gateway 192.168.2.1
!
SW2(config)# ip access-list standard VTY_ERISIM
SW2(config-std-nacl)# permit host 192.168.1.12
SW2(config-std-nacl)# deny any
SW2(config-std-nacl)# exit
!
SW2(config)# line vty 0 15
SW2(config-line)# access-class VTY_ERISIM in
```

```
PC2 C:\> telnet 192.168.1.101

Trying 192.168.1.101 ...Open
User Access Verification
Password:
SW1>en
```

```
PC3 C:\> telnet 192.168.1.101

Trying 192.168.1.101 ...
% Connection refused by remote host
```