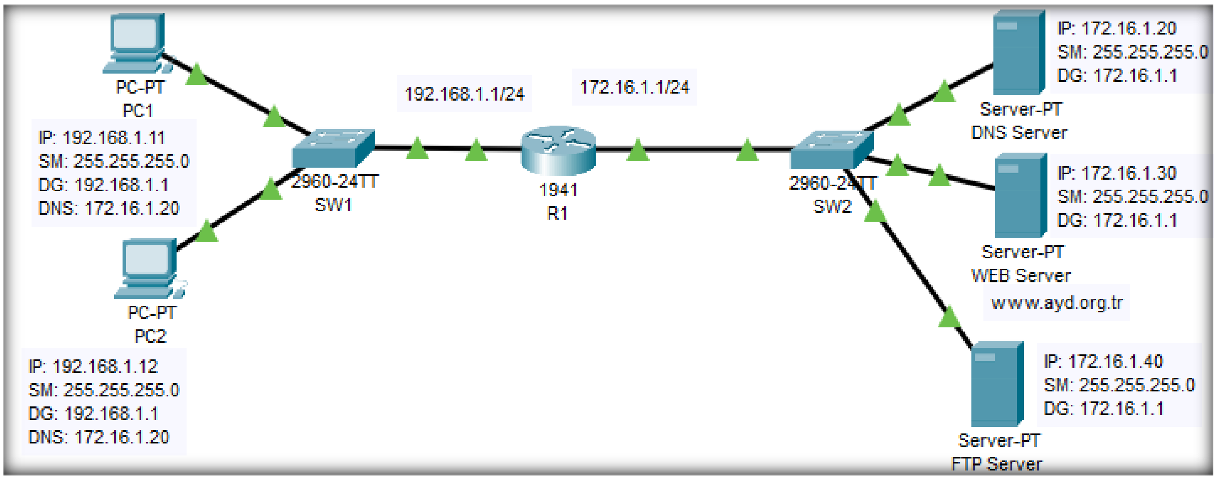
Ağ Yöneticileri Derneği
CCNA3 LAB 03 - PROJE ÇÖZÜMÜ
Extended ACL Uygulaması



LAB'IN AMACI: PC Ağından SUNUCU Ağına geçiş güvenliğinin sağlanması için Extended ACL yazılması.

ADIM1:

- R1'e ve bilgisayarlara IP adreslerini tanımlayın.
- Ping ile PC ile sunucu arasındaki baglantıları kontrol edin.

```
conf t
hostname R1

interface Gi 0/0
 ip address 192.168.1.1 255.255.255.0
 no shut

interface Gi 0/1
 ip address 172.16.1.1 255.255.255.0
 no shut
 end
wr
```

KONTROL KOMUTLARI:

PC1->	**ping 172.16.1.20** **ping 172.16.1.30** **ping 172.16.1.40**

ADIM2: SUNUCU_ERISIM isimli bir ACL yazın ve R1'in Gi0/0 interface'ine uygulayın.

PC1:

- Web Sunucusuna baglanabilsin (TCP 80 ve 443)
- DNS Sunucusuna baglanabilsin (UDP 53)
- FTP Sunucusuna baglanabilsin (TCP 20,21 ve gt 1024))
- Web Sunucusuna DNS sunucusuna ve FTP Sunucusuna ping atabilsin (icmp echo-request)

PC2:

- Web Sunucusuna baglanabilsin (TCP 80 ve 443)
- DNS Sunucusuna baglanabilsin (UDP 53)
- Hicbir sunucuya ping atamasın
- FTP sunucusuna baglanamasın.

Diger Hickimse:

- Hicbir sunucuya erisemesin

```
R1(config)# ip access-list extended SUNUCU_ERISIM
            remark PC1in WEB erisimi icin TCP 80 ve 443e izin verildi
            permit tcp host 192.168.1.11 host 172.16.1.30 eq 80
            permit tcp host 192.168.1.11 host 172.16.1.30 eq 443

            remark PC1in DNS erisimi icin UDP 53e izin verildi
            permit udp host 192.168.1.11 host 172.16.1.20 eq 53

            remark PC1in FTP erisimi icin TCP 20, 21 ve greater than 1024'e izin verildi
            permit tcp host 192.168.1.11 host 172.16.1.40 eq 20
            permit tcp host 192.168.1.11 host 172.16.1.40 eq 21
            permit tcp host 192.168.1.11 host 172.16.1.40 gt 1024

            remark PC1in ICMP erisimi icin tum sunucu uzayına izin verildi
            permit icmp host 192.168.1.11 any echo

            remark PC2nin WEB erisimi icin TCP 80 ve 443e izin verildi
            permit tcp host 192.168.1.12 host 172.16.1.30 eq 80
            permit tcp host 192.168.1.12 host 172.16.1.30 eq 443

            remark PC2nin DNS erisimi icin UDP 53e izin verildi
            permit udp host 192.168.1.12 host 172.16.1.20 eq 53
            <deny ip any any> gizli satırı

R1(config)# interface gi 0/0
R1(config-if)#ip access-group SUNUCU_ERISIM in

R1# show access-lists
Extended IP access list SUNUCU_ERISIM
           10 permit    tcp host 192.168.1.11 host 172.16.1.30 eq www
           20 permit    tcp host 192.168.1.11 host 172.16.1.30 eq 443
           30 permit   udp host 192.168.1.11 host 172.16.1.20 eq domain
           40 permit    tcp host 192.168.1.11 host 172.16.1.40 eq 20
           50 permit    tcp host 192.168.1.11 host 172.16.1.40 eq ftp
           60 permit tcp host 192.168.1.11 host 172.16.1.40 gt 1024
           70 permit icmp host 192.168.1.11 any echo
           80 permit    tcp host 192.168.1.12 host 172.16.1.30 eq www
           90 permit    tcp host 192.168.1.12 host 172.16.1.30 eq 443
          100 permit udp host 192.168.1.12 host 172.16.1.20 eq domain

R1# show ip interface gi 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.1.1/24
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 not set
Inbound access list is SUNUCU_ERISIM
….
```

KONTROL ADIMLARI:

Asagidaki islemler PC1'de Basarıyla Çalışmalı:	**Asagidaki islemler PC2'de Basarıyla Çalışmalı:**
http://172.16.1.30 **https://172.16.1.30** **http://www.ayd.org.tr** **ping 172.16.1.20** **ping 172.16.1.30** **ping 172.16.1.40** **ftp 172.16.1.40**	**http://172.16.1.30** **https://172.16.1.30** **http://www.ayd.org.tr** **Asagidaki islemler PC2'de Çalışmamalı:** **ping 172.16.1.20** **ping 172.16.1.30** **ping 172.16.1.40** **ftp 172.16.1.40**

ACL ile eşleşen paketlerin incelenmesi:

```
R1# show access-lists
        Extended IP access list SUNUCU_ERISIM
        10 permit tcp host 192.168.1.11 host 172.16.1.30 eq www (25 match(es))
        20 permit tcp host 192.168.1.11 host 172.16.1.30 eq 443 (5 match(es))
        30 permit udp host 192.168.1.11 host 172.16.1.20 eq domain (4 match(es))
        40 permit tcp host 192.168.1.11 host 172.16.1.40 eq 20
        50 permit tcp host 192.168.1.11 host 172.16.1.40 eq ftp (13 match(es))
        60 permit tcp host 192.168.1.11 host 172.16.1.40 gt 1024 (3535 match(es))
        70 permit icmp host 192.168.1.11 any echo (6 match(es))
        80 permit tcp host 192.168.1.12 host 172.16.1.30 eq www (5 match(es))
        90 permit tcp host 192.168.1.12 host 172.16.1.30 eq 443 (5 match(es))
        100 permit udp  host 192.168.1.12 host 172.16.1.30 eq domain (1 match(es))
```