Standart Erişim Kontrol Listeleri (ACL) ATÖLYESİ

ATÖLYENİN HEDEFİ:

ACL kurmayı öğrenmeniz.

ATÖLYENİN AMACI:

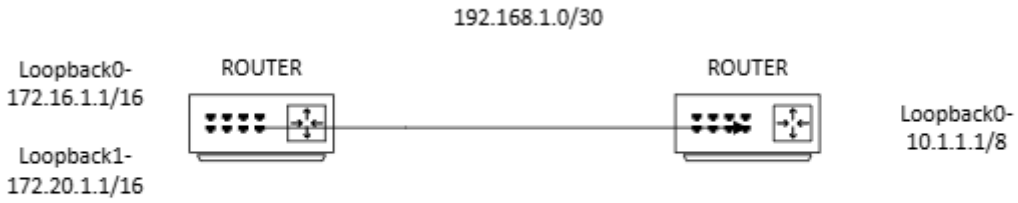
Erişim listeleri (access list), trafiğin ağa girip giremeyeceğini ya da ağdan engellenip engellenmeyeceğini belirleyen izin (permit) veya reddetme (deny) ifadelerinden oluşur. Çeşitli kurallar nedeniyle karmaşık hale gelebilirler. Şunu unutmamak gerekir: Bir trafik akışı listedeki herhangi bir kuralla eşleşirse, listedeki diğer kurallara bakılmaz; o noktada ya izin verilir ya da reddedilir. Her erişim listesinin sonunda ise örtük (implicit) bir deny ifadesi bulunur. Bu ifade yapılandırmada görünmese bile her zaman geçerlidir.

ATÖLYE ARACI:

Cisco Packet Tracer

ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için aşağıdaki topolojiyi kullanmanız tavsiye edilir.



ATÖLYE ANLATIMI:

Adım 1:

İki routeri birbirine bağlayıp arayüzlerine topolojideki adresleri verin.

```
R0(config-if)#int g0/0
R0(config-if)#ip add 192.168.1.1 255.255.255.252
R0(config-if)#no shut

R0(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R0(config-if)#int l0
R0(config-if)#ip add 172.16.1.1 255.255.0.0
R0(config-if)#int l1

R0(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R0(config-if)#ip add 172.20.1.1 255.255.0.0
R0(config-if)#end
R0#
%SYS-5-CONFIG_I: Configured from console by console


R1(config)#int g0/0
R1(config-if)#ip add 192.168.1.2 255.255.255.252
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config-if)#int l0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip add 10.1.1.1 255.0.0.0
R1(config-if)#end
```

Adım 2:

Routerler arasında bir statik yol(route) ayarlayın ve ping atarak test edin.

```
R0(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2


 R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1

R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Adım 3:

R0 üzerinde bir erişim listesi (ACL) yapılandırın. 10.1.1.1 adresinden gelen trafik engellenecek, ancak diğer tüm trafiğe izin verilecek. ACL'in sonunda varsayılan olarak tüm trafik engellendiği için, diğer her şeye izin vermemiz gerekmektedir. Ayrıca, erişim listesini bir arayüze uygulamamız gerekmektedir.

```
R0(config)#access-list 1 deny host 10.1.1.1
R0(config)#access-list 1 permit any
R0(config)#int g0/0
R0(config-if)#ip access-group 1 in
```

Adım 4:

192.168.1.2'den 172.16.1.1'e ve 10.1.1.1'den 172.16.1.1'e ping atarak ACL'yi kontrol edin.

```
R1#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
R1#ping
Protocol [ip]:
Target IP address: 172.16.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: loopback0
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
UUUUU
Success rate is 0 percent (0/5)
```

Router'den aldığımız UUUUU cevabı bize trafiğin engellenmiş olduğunu gösteriyor.

Adım 5:

Eğer isterseniz ACL kurallarını da görüntüleyebilirsiniz.

```
R0#show ip access-lists
Standard IP access list 1
    10 deny host 10.1.1.1 (5 match(es))
    20 permit any (15 match(es))
```