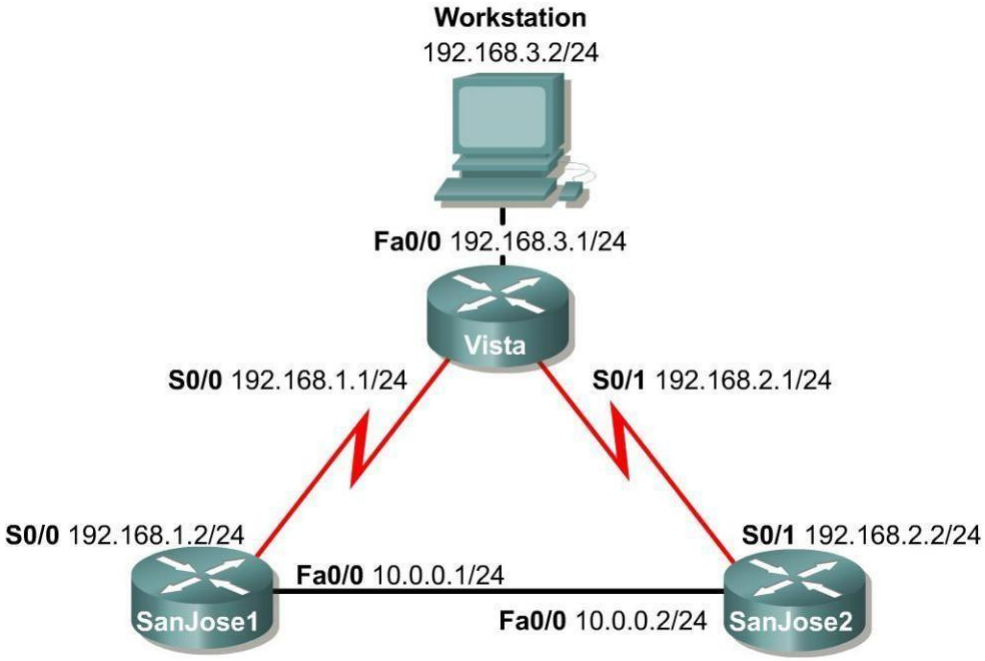
RRJETAT E KOMPJUTERAVE 1

LAB 9

Tema: Bazat e ACL (Access Control List) dhe Extended ACL



Skenari

Përdoruesit e LAN-it të lidhur me ruterin Vista janë të shqetësuar për aksesin në rrjet nga hostet në rrjetin 10.0.0.0. Duhet të përdoret një listë standarde aksesi për të bllokuar të gjithë aksesin në Vista LAN nga rrjeti 10.0.0.0 /24.
Gjithashtu, një ACL i zgjeruar duhet të përdoret për të bllokuar aksesin e hostit të rrjetit 192.168.3.0 në serverët e uebit në rrjetin 10.0.0.0 /24.

Step 1

Build and configure the network according to the diagram. Use RIPv1, and enable updates on all active interfaces with the appropriate **network** commands. The commands necessary to configure SanJose1 are shown in the following example:

SanJose1(config)#**router rip**
SanJose1(config-router)#**network 192.168.1.0**
SanJose1(config-router)#**network 10.0.0.0**

Use the **ping** command to verify the work and test connectivity between all interfaces.

Step 2
Check the routing table on Vista using the **show ip route** command. Vista should have all four networks in the routing table. Troubleshoot, if necessary

Access Control List Basics
Access Control Lists (ACLs) are simple but powerful tools. When the access list is configured, each statement in the list is processed by the router in the order in which it was created. If an individual packet meets a statement's criteria, the permit or deny is applied to that packet, and no further list entries are checked. Each packet starts at the top of the list, every time.
It is not possible to reorder an access list, skip statements, edit statements, or delete statements from a numbered access list, while in the router configuration mode. With numbered access lists, any attempt to delete a single statement results in deletion of the entire list. Named ACLs (NACLs) do allow for the deletion of individual statements. It is suggested that ACLs, of all kinds, be created in an off-line editor and pasted into the configuration.
The following concepts apply to both standard and extended access lists:

Two step process
The access list may be created with one or more **access-list** commands while in global configuration mode. Second, the access list is applied to or referenced by other commands, such as the **ip access-group** command which applies the ACL to an interface. An example would be the following:

Vista#**config terminal**
Vista(config)#**access-list 50 deny 10.0.0.0 0.0.0.255**
Vista(config)#**access-list 50 permit any**
Vista(config)#**interface fastethernet 0/0**
Vista(config-if)#**ip access-group 50 out**
Vista(config-if)#**^Z**

Syntax and Keywords
The basic syntax for creating an access list entry is as follows:
router(config)#**access-list #** *{permit | deny}ip address wildcard mask*
The **permit** command allows packets matching the specified criteria to be accepted for whatever application the access list is being used for. The **deny** command discards packets matching the criteria on that line.
Two important keywords, **any** and **host**, can be used with IP addresses and the access list. The keyword **any** matches all hosts on all networks, equivalent to

0.0.0.0 255.255.255.255. The keyword **host** can be used with an IP address to indicate a single host address. The syntax is **host** *ip address* (**host 192.168.1.10**). This is the same as entering 192.168.1.10 0.0.0.0.

Implicit deny statement

Every access list contains a final "deny" statement that matches all packets. This is called the implicit deny. Because the implicit deny statement is not visible in **show** command output, it is often overlooked, with serious consequences. As an example, consider the following single-line access list:

Router(config)#**access-list 75 deny host 192.168.1.10**

Access- list 75 clearly denies all traffic sourced from the host, 192.168.1.10. What might not be obvious is that all other traffic will be discarded as well. This is because the implicit **deny any** is the final statement in any access list.

At least one permit statement is required

There is no requirement that an ACL contain a **deny** statement. If nothing else, the implicit **deny any** statement takes care of that. But if there are no **permit** statements, the effect will be the same as if there were only a single **deny any** statement.

Wildcard mask

In identifying IP addresses, ACLs use a wildcard mask instead of a subnet mask. Initially, the masks might look the same, but closer observation reveals that they are very different. Remember that a binary 0 in a wildcard mask instructs the router to match the corresponding bit in the IP address.

In/out

When deciding whether an ACL should be applied to inbound or outbound traffic, always view things from the perspective of the router. In other words, determine whether traffic is coming into the router, inbound, or leaving the router, outbound.

Applying ACLs

Extended ACLs should be applied as close to the source as possible, thereby conserving network resources. Standard ACLs, by necessity, must be applied as close to the destination as possible.

This is because the standard ACL can match only at the source address of a packet.

Step 3

On the Vista router, create the following standard ACL and apply it to the LAN interface:

Vista#**config terminal** Vista(config)#**access-list 50 deny 10.0.0.0 0.0.0.255**
Vista(config)#**access-list 50 permit any** Vista(config)#**interface fastethernet 0/0** Vista(config-if)#**ip access-group 50 out**
Vista(config-if)#**^Z**

Try pinging 192.168.3.2 from SanJose1.

The ping should be successful. This result might be surprising, because all traffic from the 10.0.0.0/8 network was just blocked. The ping is successful because, even though it came from SanJose1, it is not sourced from the 10.0.0.0/8 network. A ping or traceroute from a router uses the closest interface to the destination as the source address. Therefore, the ping is coming from the 192.168.1.0/24, SanJose1's Serial 0/0.

SanJose1#**ping 192.168.3.2**

Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

Step 4
In order to test the ACL from SanJose1, the extended ping command must be used to specify a source interface as follows:

On SanJose1, issue the following commands:

Note: Remember that the extended ping works only in the privileged EXEC mode.

SanJose1#**ping** Protocol
[ip]:
Target IP address: **192.168.3.2**

Repeat count [5]:

Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y Source
address or interface: **10.0.0.1** 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 192.168.3.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Step 5

Standard ACLs are numbered 1 - 99. IOS version 12.xx allows additional numbering from 1300 - 1699. Extended ACLs are numbered 100 - 199. IOS version 12.xx allows additional numbering from 2000 - 2699. Extended ACLs can be used to enforce highly specific criteria for filtering packets. In this step, configure an extended ACL to block access to a Web server. Before proceeding, issue the **no access-list 50** and **no ip access-group 50** commands on the Vista router to remove the ACL configured previously.

First, configure both SanJose1 and SanJose2 to act as Web servers, by using the **ip http server** command, as shown in the following:

SanJose1(config)#**ip http server**
SanJose2(config)#**ip http server**

From the workstation at 192.168.3.2, use a Web browser to view both Web servers on the router at 10.0.0.1 and 10.0.0.2. The Web login requires that the enable secret password for the router be entered as the password.

After verifying Web connectivity between the workstation and the routers, proceed to Step 6.

Step 6

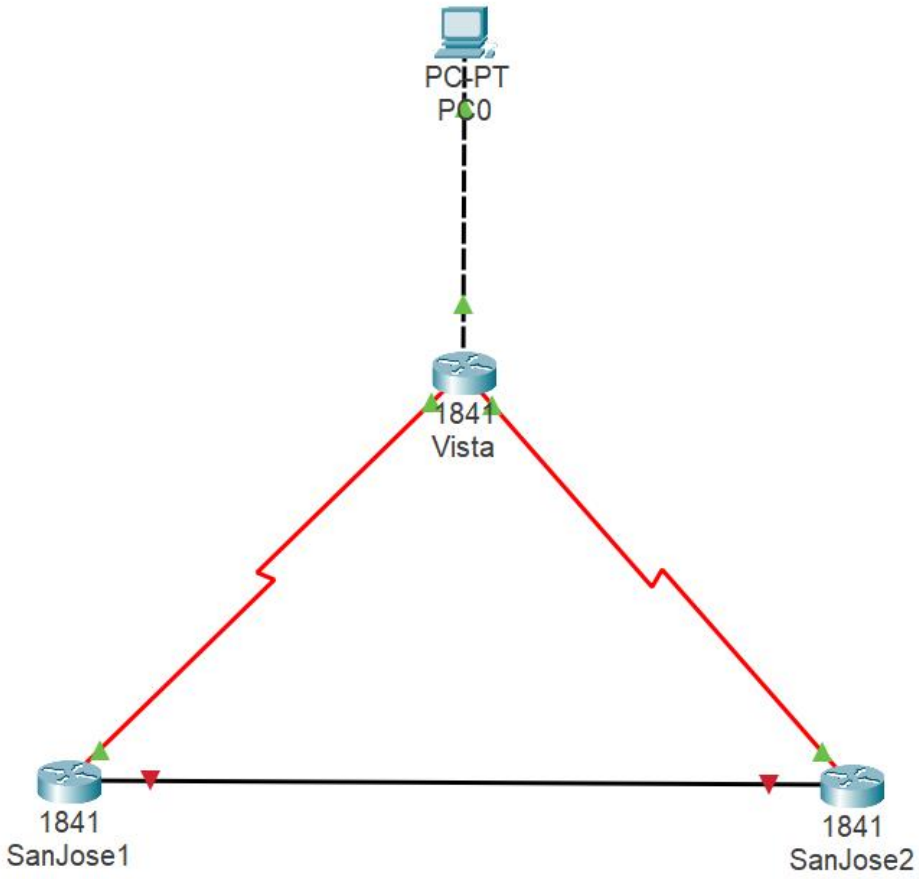
On the Vista router, enter the following commands:

Vista(config)#**access-list 101 deny tcp 192.168.3.0 0.0.0.255 10.0.0.0 0.0.0.255 eq www** Vista(config)#**access-list 101 deny tcp 192.168.3.0 0.0.0.255 any eq ftp** Vista(config)#**access-list 101 permit ip any any** Vista(config)#**interface fastethernet 0/0** Vista(config-if)#**ip access-group 101 in**

From the workstation at 192.168.3.2, again attempt to view the Web servers at 10.0.0.1 and
10.0.0.2. Both attempts should fail.

Next, browse SanJose1 at 192.168.1.2. Why is this not blocked?

_____



Step 1:
Konfigurojme sipas skemes

```
SanJose1(config)#
SanJose1(config)#router rip
SanJose1(config-router)#network 192.168.1.0
SanJose1(config-router)#network 10.0.0.0
SanJose1(config-router)#
```

Provojme ping prej SanJose1

```
SanJose1#ping 192.168.1.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.0, timeout is 2 seconds:

Reply to request 0 from 192.168.1.1, 11 ms
Reply to request 1 from 192.168.1.1, 4 ms
Reply to request 2 from 192.168.1.1, 3 ms
Reply to request 3 from 192.168.1.1, 5 ms
Reply to request 4 from 192.168.1.1, 5 ms

SanJose1#ping 10.0.0.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.0, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SanJose1#
```

Step 2:
Pasi konfigurojmë Router Vista përdorim komandën show ip route per te pare IP

```
VISTA#
VISTA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VISTA(config)#router rip
VISTA(config-router)#network 192.168.1.0
VISTA(config-router)#network 192.168.2.0
VISTA(config-router)#network 192.168.3.0
VISTA(config-router)#end
Vista#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Serial0/1/0
C    192.168.2.0/24 is directly connected, Serial0/1/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0

Vista#
```

Perdorim ping nga Vista per te pare qe lidhjet punojnë

```
Vista#ping 192.168.1.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.0, timeout is 2 seconds:

Reply to request 0 from 192.168.1.2, 9 ms
Reply to request 1 from 192.168.1.2, 5 ms
Reply to request 2 from 192.168.1.2, 3 ms
Reply to request 3 from 192.168.1.2, 2 ms
Reply to request 4 from 192.168.1.2, 5 ms

Vista#ping 192.168.2.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.0, timeout is 2 seconds:

Reply to request 0 from 192.168.2.2, 6 ms
Reply to request 1 from 192.168.2.2, 3 ms
Reply to request 2 from 192.168.2.2, 2 ms
Reply to request 3 from 192.168.2.2, 2 ms
Reply to request 4 from 192.168.2.2, 2 ms

Vista#ping 192.168.3.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.0, timeout is 2 seconds:

Reply to request 0 from 192.168.3.2, 0 ms
Reply to request 1 from 192.168.3.2, 0 ms
Reply to request 2 from 192.168.3.2, 0 ms
Reply to request 3 from 192.168.3.2, 0 ms
Reply to request 4 from 192.168.3.2, 2 ms

Vista#
```

Lidhjet janë ne rregull.

Step 3:

```
Vista#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Vista(config)#
Vista(config)#access-list 50 deny 10.0.0.0 0.0.0.255
Vista(config)#access-list 50 permit any
Vista(config)#interface fastEthernet 0/0
Vista(config-if)#ip access-group 50 out
Vista(config-if)#^Z
```

Provojmë ping ne 192.168.3.2

```
SanJose1>enable
SanJose1#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/8 ms

SanJose1#
```

Step 4:

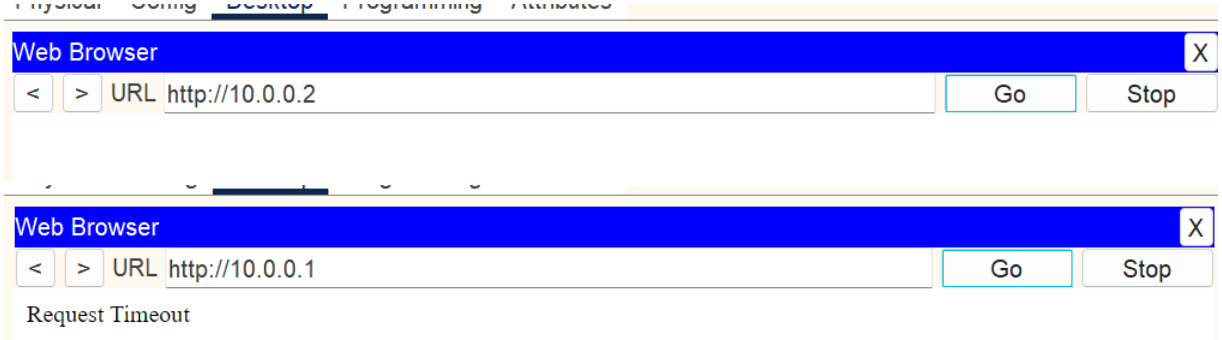
```
SanJose1#ping
Protocol [ip]:
Target IP address: 192.168.3.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.0.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
.....
Success rate is 0 percent (0/5)

SanJose1#
```

Step 5:

```
Vista(config)#no access-list 50
Vista(config)#no ip access-group 50
SanJose2(config)#ip http server
SanJose1(config)#ip http server
```

Step 6:

```
Vista>enable
Vista#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Vista(config)#access-list 101 deny tcp 192.168.3.0 0.0.0.255 10.0.0.0 0.0.0.255
Vista(config)#access-list 101 deny tcp 192.168.3.0 0.0.0.255 10.0.0.0 0.0.0.255 eq www
Vista(config)#access-list 101 deny tcp 192.168.3.0 0.0.0.255 any eq ftp
Vista(config)#access-list 101 permit ip any any
Vista(config)#interface fastethernet 0/0
Vista(config-if)#interface fastethernet 0/0
Vista(config-if)#end
Vista#
```



Pse SanJose1 (192.168.1.2) nuk është bllokuar?
Kur provoni të shfletoni **SanJose1** (në IP **192.168.1.2**), ai nuk është bllokuar sepse:

- **ACL** është konfiguruar për të bllokuar trafikun vetëm midis **192.168.3.0/24** dhe **10.0.0.0/24**, veçanërisht për **HTTP** (port 80) dhe **FTP** (port 21).
- **IP e destinacionit të SanJose1 (192.168.1.2)** nuk bie brenda rrjetit **10.0.0.0/24**. **ACL** bllokon vetëm trafikun për në **10.0.0.0/24** (si për shembull, serverët web si **10.0.0.1** dhe **10.0.0.2**).
- **ACL** nuk bllokon trafikun për në rrjete të tjera, si për shembull **192.168.1.0/24**, ku ndodhet **SanJose1**.
- Asnjë rregull i veçantë "deny" (bllokimi) nuk aplikohet për rrjetin **192.168.1.0/24**, kështu që **ACL** e lejon këtë trafik për shkak të rregullit të fundit **permit ip any any**, i cili lejon çdo trafik që nuk është bllokuar nga një rregull tjetër.

Ky është arsyeja pse mund të shfletoni **SanJose1** dhe nuk bllokohet, ndërsa serverët e tjerë web (**10.0.0.1** dhe **10.0.0.2**) janë bllokuar.