Academia International College

**(Affiliated to Tribhuvan University)**

**Gwarko, Ring Road, Lalitpur -7, P.O. Box: 6246, KTM, Nepal.**

**Tel.: 00977-1-5525393, 5543037, email: mail@academiacollege.edu.np, URL: www.academiacollege.edu.np**



**Lab Sheet**

**Subject: Internet Technology**

**Title: Familiarization with Basic of Firewall: Access List**

**Practical No. : 06**

**Submitted by: Rosy Dangol**

**Roll No. : 35**

**Date: 04 October, 2020 Submitted To: Sugan Shakya**

**Introduction**

**Firewall**

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. The main purpose of a firewall system is to control access to or from a protected network (i.e., a site). The firewall acts as a packet filter.

It inspects each and every incoming and outgoing packet. Packets meeting some criterion described in rules formulated by the network administrator are forwarded normally. Those that fail the test are unceremoniously dropped. A firewall can be a hardware, software or both.

**Access List**

An access list is essentially a list of conditions that categorize packets. They can be really helpful when you need to exercise control over network traffic. An access list would be your tool of choice for decision making in these situations.

There are two main types of access lists:

**Standard access lists**

These use only the source IP address in an IP packet as the condition test. All decisions are made based on the source IP address. This means that standard access lists basically permit or deny an entire suite of protocols. They don’t distinguish between any of the many types of IP traffic such as Web, Telnet, UDP, and so on.

**Extended access lists**

Extended access lists can evaluate many of the other fields in the layer 3 and layer 4 headers of an IP packet. They can evaluate source and destination IP addresses, the Protocol field in the Network layer header, and the port number at the Transport layer header. This gives extended access lists the ability to make much more granular decisions when controlling traffic.

So, by specifying the direction of traffic, you can—and frequently you’ll need to—use different access lists for inbound and outbound traffic on a single interface:

**Inbound access lists**

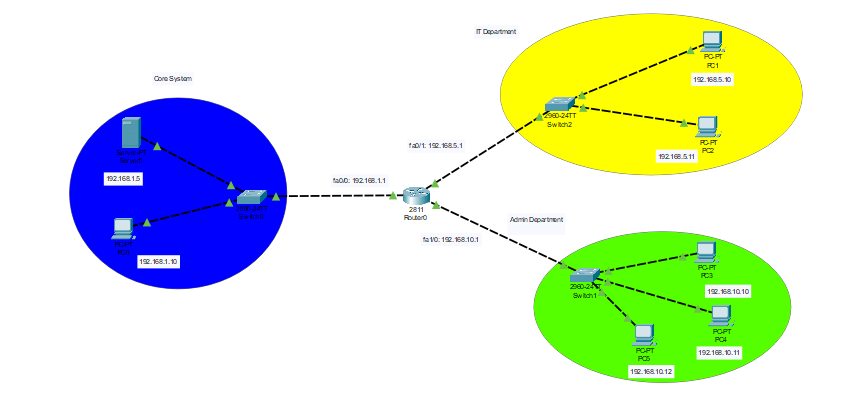
When an access list is applied to inbound packets on an interface, those packets are processed through the access list before being routed to the outbound interface. Any packets that are denied won’t be routed because they’re discarded before the routing process is invoked.

**Outbound access lists**

When an access list is applied to outbound packets on an interface, packets are routed to the outbound interface and then processed through the access list before being queued.

**Range of number for the Standard Access List:** It uses the range 1-99 and extended range 1300-1999.

**Range of number for the Extended Access List:** It uses the range 100 – 199 & extended range 2000 – 2699.



**Procedure**

**Network and Requirements**

An organization has an intranet network as shown above in the figure, which consists of a Core system network with address 192.168.1.1, IT Department Network with address 192.168.5.1 and Admin Network with address 192.168.10.1.

The **requirements** to setup the access permission to the core system is:

Any client in its own network (192.168.1.0) is allowed to access it. Further, any client in IT Department network (192.168.5.0) is allowed to access it as well.

But, it should be accessible from any other client in Admin Department (network: 192.168.10.0), except for an IT Engineer, who has a static IP of 192.168.10.10. Besides those, access is denied for all other.

**Commands to configure the required access-list**

a) Router (config)# access-list <access-list-number> deny/permit/remark A.B.C.D WildcardMask

This command is used whenever we want to deny/permit/remark all client in a network A.B.C.D WildcardMask.

b) Router(config)# access-list <access-list-number> deny/permit/remark host A.B.C.D

This command is used whenever we want to deny/permit/remark a specific host in a network A.B.C.D.

c) Router(config)# access-list <access-list-number> deny/permit/remark any

This command is used whenever we want to deny/permit/remark every other networks or host except the one which was mentioned just before this command during the configuration in the router.

d) Router(config)# int fa0/0

Router(config-if)# ip access-group <access-list-number> in/out

This command is used to activate the access-list on the interface in an either inbound or outbound direction.

**Commands to assign access list in interface fa0/0 in outbound direction**

Router> enable

Router# configure terminal

Router(config)# access-list 20 permit host 192.168.10.10

Router(config)# access-list 20 permit 192.168.5.0 0.0.0.255

Router(config)# access-list 20 deny any

Router(config)# interface fa0/0

Router(config-if)# ip access-group 20 out

The third statement will permit the access to host 192.168.10.10.

The fourth statement will permit the access to entire clients in network 192.168.5.0.

The fifth statement will deny the access to any other clients other than mentioned in third and fourth command.

The seventh statement applies the access-lists mentioned above in the interface fa0/0 in outbound direction.

**Results and Findings**

Since, the clients in the network 192.168.5.1 i.e. IT department have the access to the network 192.168.1.1 i.e. Core system, when we send an packet from both the pcs in the IT department to the Core system, it successfully reach to the destination i.e. the server in the core system.

In the network 192.168.10.1 i.e. Admin department, the access is provided only to IT engineer i.e. 192.168.10.10. When we send a packet from the client, it was successful.

The transmission from any other clients were failed which prove the requirements that were stated.

**Conclusion**

From this lab we gather the information on how on a network we can provide or deny access to communicate to particular server or the network using the access-list configurations.