CO325 - Computer & Network Security
Lab 01 - Introduction to ASA and Basic network security handling

---

E/17/219
Nawarathna K.G.I.S.

1.What are the specific purposes of “access-list” and “access-group” commands?

access-list : There is a list named access control list which has some rules to give access or block the access for a network.(from other networks). These rules are used by the router and we can add new rules to the access control list using this command.

access-group : This command is used to configure an interface by applying a certain access list to the interface to a certain direction.

2.Identify the pros and cons of this approach in permitting traffic from outside to reach the internal network.

Pros :

1. Not allowing the unsecure packets to come to the network from outside unknown networks.
2. Used to separate devices with high secured sensitive data without separating the network. Only blocking access to selected hosts can be done without separating the network.
3. Managing access to outgoing/incoming traffic by managing the permissions.

Cons :

1. When there is incoming and outgoing traffic, those packets need to be processed to see whether they are allowed on the network. This will increase the procession power of the system.Due to the extra processing power power and cost may increase a bit.
2. Application level security is not provided.

3.Check the connectivity (ping) and try to create the following Browser Session for each scenario

- Check the main page on External Server from the Internal Computer
- Check the main page on Internal Server from the External Computer

	Connectivity	Inside pc to outside server	Inside pc to outside pc	Outside pc to inside server	Outside pc to inside pc
1.0	ping	No	No	No	No
	http	Yes	N/A	No	N/A
2.1	ping	Yes	Yes	Yes	Yes
	http	Yes	N/A	Yes	N/A
2.2	ping	No	Yes	Yes	Yes
	http	Yes	N/A	Yes	N/A
2.3	ping	No	No	Yes	No
	http	No	N/A	Yes	N/A
2.4	ping	No	No	No	No
	http	Yes	N/A	Yes	N/A
2.5	ping	Yes	Yes	Yes	Yes
	http	No	N/A	No	N/A
2.6	ping	No	No	No	No
	http	Yes	N/A	No	N/A
2.7	ping	No	No	No	No
	http	Yes	N/A	Yes	N/A
2.8	ping	Yes	Yes	Yes	Yes
	http	Yes	N/A	Yes	N/A
2.9	ping	Yes	Yes	Yes	Yes
	http	Yes	N/A	No	N/A

4.What has been excluded from the filtering (i.e., permitted) by the ACEs in each scenario? Be precise!

Scenario 1

- Traffic(any kind of packet) can flow from inside to outside network, for example inside network devices can establish a TCP connection with outside network but devices in the outside network can not communicate with the inside network devices via TCP

Scenario 2.1

- Each and every host in one network can send traffic with any kind of packets with each and every other host in the other network

Scenario 2.2

- External computer can send any packets to all the hosts in the inside network

Scenario 2.3

- Hosts in the outside network can send any packets to Internal server

Scenario 2.4

- TCP packets from the outside network to the inside network are allowed.(Only TCP)
- But all the packets from the inside network to the outside network are allowed.

Scenario 2.5

- All the ICMP(ping) packets from outside to inside network are allowed.(Only ICMP)

Scenario 2.6

- Only permits, the TCP packets from the external server to the hosts with inside network subnet

Scenario 2.7

- Both TCP and HTTP packets from the outside network to the internal server are permitted.

Scenario 2.8

- ICMP,TCP,HTTP packets are allowed from outside to inside network

Scenario 2.9

- All the packets from outside to inside the network are allowed but TCP or HTTP packets which are coming to the internal server from outside are blocked.

5.Identify the situation(s) that are best suited for each scenario and Access Control Entries (ACEs), if any. If not, explain why.

Scenario 1:

- Used when high level security network wants to send HTTP requests and receive HTTP responses to those requests from a low level security network

Scenario 2.1:

- This scenario is not very good. Any kind of traffic flow through the firewall is not something intended and may result in possible security threats.

Scenario 2.2:

- Used when the access of the high security level network wants to limit its' access by other low secured network devices i.e. when one/few devices in low secured network is given the access to the high secured network.

Scenario 2.3:

- GIving access for the lower level secured network to access one host in the inside network

Scenario 2.4:

- Used when low secured network and high secured network need to communicate through TCP protocol only

Scenario 2.5:

- Used when low secured network and high secured network need to communicate through ICMP protocol only. (pinging only)

Scenario 2.6:

- Used when a subnet in a highly secured network wants to communicate to a low secured host through TCP

Scenario 2.7:

- Used when a single host in a high secured network wants to communicate to low secured network devices through TCP/HTTP
  Ex: typical web server in the internet

Scenario 2.8:

- Very vulnerable situation. Since the priority is given to low level ACE, in the practice, this is not used.

Scenario 2.9:

- Used when all the traffic intended to a host in the high security level is allowed while TCP is blocked.