CO3255 – Information Security

Semester-6, 2020

Laboratory-Session/Assignment

Firewalls and ACLs

Instructions:

- Use the 'Cisco Packet Tracer' simulator for this lab/assignment.
- Submit (upload) your simulation file(s).
- Marks (100%) from submission (above) + Lab-evaluation (if any).
- Advised to keep simulation/trace files with you for later examination/preparing for the evaluation.

Part-1: Institutional Network

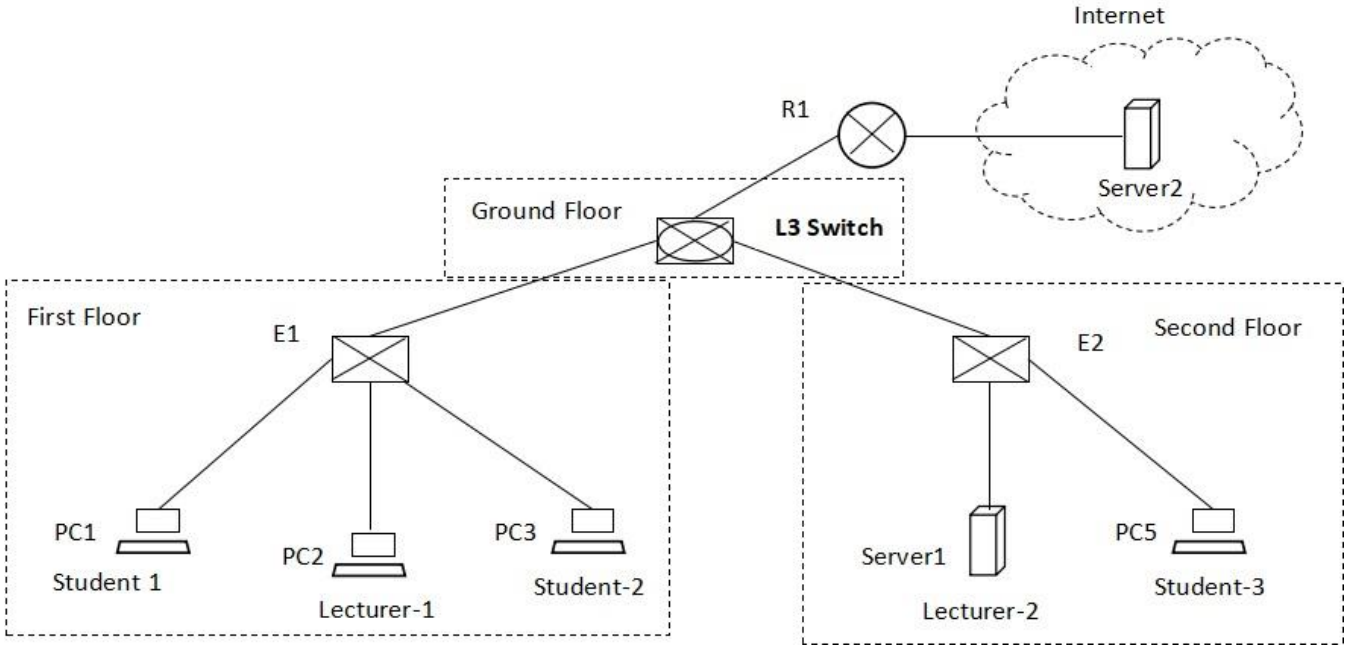

Fig. 1: Department network with no demilitarized zone (DMZ)

a. You are required to set up the above network (Fig. 1) for the Computer Engineering Department (assume a building with three floors, E-Ethernet switches, R-Routers). The network is to be used by both staff and students as shown. All types of communications such as lecturer-lecturer, lecturer-student, and student-student should be possible in the network without any restrictions based on physical locations (floors). However, when communicating, **there should be sufficient traffic isolation for the staff and students (traffic from staff should not unnecessarily reach students and vice versa)**. Use the 10.0.0.0/8 address block for the whole department and the address 142.3.2.0/24 for the external link attached to R1. Accordingly, assign (mark) appropriate IP addresses for the devices/interfaces and identify VLANs needed, and NAT. Set up and configure the network. Set up web servers on Server1 and Server2. (some Cisco L3 switch models: 3550, 3750, 3560, 4500, 6500, 7000, etc.).

b. Test & verify the network:

- Access the web server on Server2 from PC1 (Student).
- Access the web server on Server2 from PC2 (Lecturer).
- Accessing the web server on Server1 from Server2.
- Ping/traceroute from PC1 to Server2.
- Ping/traceroute from Server2 to Server1.

Part-2: Access Control with NO Demilitarized Zone (DMZ)

c. For the network that you configured above, consider policy-1: **block (only) PC5 from accessing the Internet**. Implement this policy by configuring the L3 switch. Verify.

d. Instead of configuring the L3 switch, configure R1 to implement the same policy mentioned above (policy-1). (delete relevant configurations done at the L3 switch). Verify. Note the router interface & the direction (inbound or outbound) on which you applied access control and find the order of processing for NAT and firewall: firewall first then NAT? Or NAT first then firewall?

e. For implementing policy-1, which approach is good: configure the L3switch or configure R1? Give reasons.

f. Instead of implementing policy-1 (delete relevant configurations for policy-1), you are told to implement policy-2: **block Internet access for students during an examination. However, lecturers should be able to access the Internet at all times including the examination time**. Configure R1 to implement this policy. Test all the tasks mentioned in (b) and verify.

g. Instead of implementing policy-2 (delete relevant configurations for policy-2), you are told to implement policy-3: **block all Internet traffic (inbound and outbound) except - (1) Web traffic initiated from within the organization and (2) DNS traffic.** Configure R1 to implement this policy. Test all the tasks mentioned in (b) and verify.

Part-3: Access Control with Demilitarized Zone (DMZ)

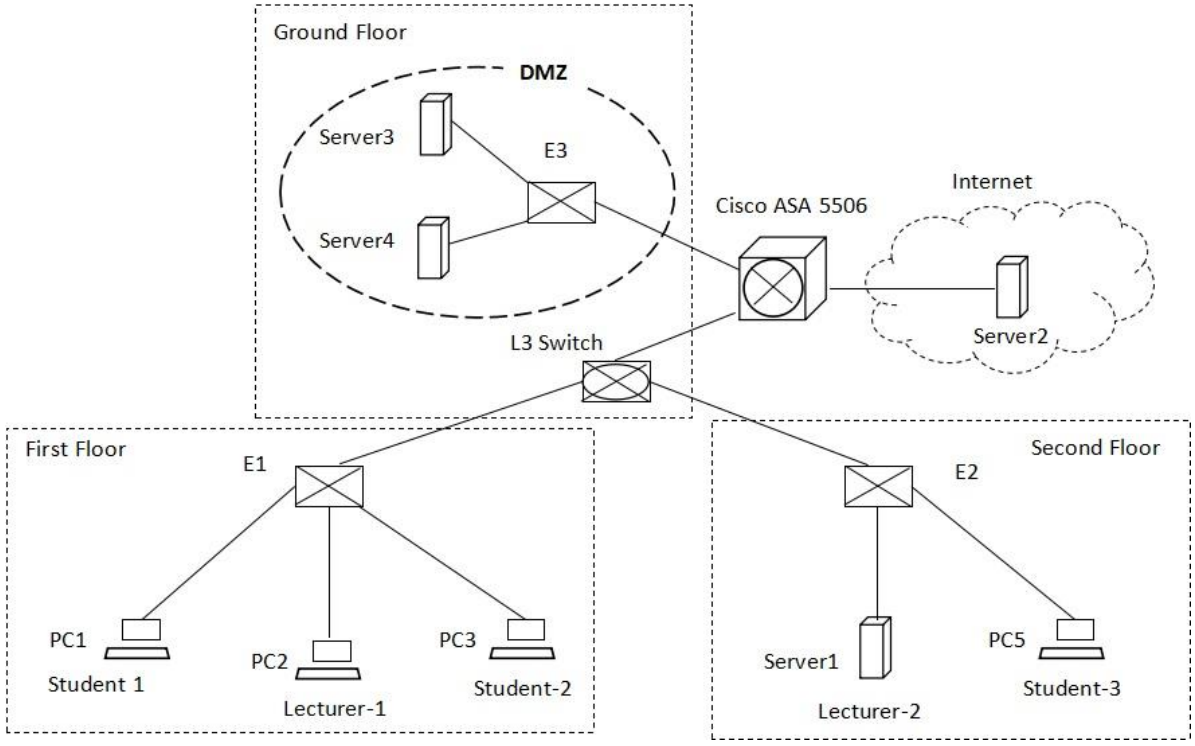

Fig. 2: Department network with demilitarized zone (DMZ)

h. Consider the network shown in Fig. 2 with a Demilitarized Zone (DMZ). The department places 2 publicly accessible web servers (Server3 and Server4) in the DMZ. A Unified Threat Management (UTM) device, Cisco ASA 5506, is used as shown (instead of R1). Assign (mark) appropriate IP addresses in the 10.0.0.0/8 address block for the DMZ (other addresses - same as assigned/mentioned in (a) including 142.3.2.0/24 addresses). The 2 publicly accessible web servers (Server3 and Server4) in the DMZ should be accessed with the public IP addresses 142.3.2.100 and 142.3.2.101 from the Internet. Set up and configure the network. Particularly,

- Configure NAT to allow users on the first and second floors to access the Internet.
- Configure NAT to allow DMZ servers to access the Internet.
- Configure inbound NAT rule(s) to allow access to the DMZ web servers from the Internet with 142.3.2.100 and 142.3.2.101 public IP addresses.
- Configure the required access-lists on the internet facing interface to implement policy-4: **(1) allow accessing the DMZ web servers from the Internet and (2) Policy-3 (mentioned in part (g)) for all the devices on the first and second floors.**
- Test & verify:
  - ✓ Test HTTP connectivity from Server2 (public) to a DMZ web server (http://142.3.2.100).
  - ✓ Test HTTP connectivity from Server2 (public) to Server1 (internal).
  - ✓ Access the web server on Server2 from PC1 (Student).
  - ✓ Access the web server on Server2 from PC2 (Lecturer).
  - ✓ Ping/traceroute from PC1 to Server2.

i. Configure 'stateful' packet filtering on Cisco ASA 5506 so that policy-4 (above) now includes the following checking: when HTTP packets with destinations on first and second floors are received, it should check whether they belong to existing/active TCP connections initiated and already established from the inside. Otherwise, it should block those packets.