A7011N Lab 3 - Group 9

Emil Berglund (50 %)
Jonathan Zulu (50 %)

November 25, 2024

1 Assignment

We are now expanding our network, both with employees connected internally and external users. The external workstations shall only be able to access the organization's web. We also need to protect our internal server from non-authorized access, so the decision is to place a web server in a DMZ. The extended network is in the file lab-topology-for-firewall.pktDownload lab-topology-for-firewall.pkt

All devices in the network can initially communicate with each other. Start with verifying that all workstations have access to both web servers using a web browser. Your task is to configure the firewalls so that external workstations only access the webserver placed in the DMZ. External workstations shall not be able to access any other service on the server in the DMZ and not any service on the internal server. Further, ping sweeps from external devices are not allowed since they might be used to identify the network topology. Hence, ping from external devices needs to be blocked.

To solve this, you need to read into access lists Links to an external site.; they are used to decide what traffic to block and let through. Place the access list on the interface right firewall interface to monitor the traffic and carry out the action based on the access list. To see what an access-list is, look at slide 7 in Lecture 3-4 slides.

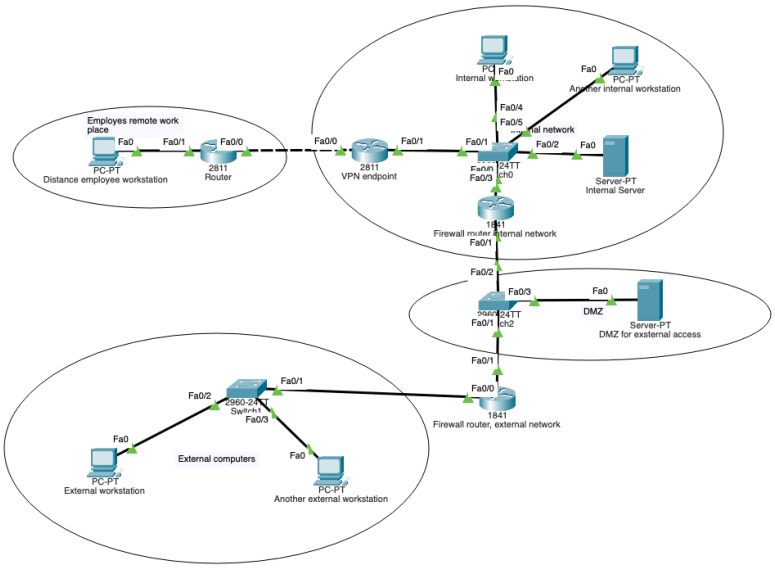

Figure 1: Network Topology

1.1 Network Zones & IPs

- External Zone:
  - External PC1: 13.1.1.2
  - External PC2: 13.1.1.3
- DMZ Zone:
  - DMZ Server: 12.1.1.3/8
- Internal Network:
  - Internal PC1: 12.1.1.4/24
  - Internal PC2: 11.1.1.5/24
  - Internal Server: 11.1.1.2/24
  - internal Router: Fa0/0 11.1.1.3/24, Fa0/1 12.1.1.1/24
  - VPN Endpoint Router: Fa0/0 10.1.1.2/24, Fa0/1 11.1.1.1/24
- Firewall Router IPs:
  - External interface (Fa0/0): 13.1.1.1/24
  - Internal interface (Fa0/1): 12.1.1.2/24
- Employees Remote Access:
  - Remote PC: 10.2.1.2/24
  - External interface (Fa0/0): 10.1.1.1/24
  - Internal interface (Fa0/1): 10.2.1.1/24

1.2 Configuration

First, we started by configuring the Firewall router and external network, then configured the internal network router and firewall:

1.2.1 External Firewall Router

- Creating ACL for External traffic control:
  - **config#** access-list 100 remark EXTERNAL-TO-DMZ-CONTROL
- Allow HTTP/HTTPS to DMZ server:
  - **config#** access-list 100 permit tcp host 13.1.1.2 host 12.1.1.3 eq www
  - **config#** access-list 100 permit tcp host 13.1.1.2 host 12.1.1.3 eq 443
  - **config#** access-list 100 permit tcp host 13.1.1.3 host 12.1.1.3 eq www
  - **config#** access-list 100 permit tcp host 13.1.1.3 host 12.1.1.3 eq 443
- Block ICMP from external sources

- **config#** access-list 100 deny icmp any any

- Block access to internal networks
  - **config#** access-list 100 deny ip any 11.1.1.0 0.0.0.255
  - **config#** access-list 100 deny ip any 12.1.1.0 0.0.0.255

- Applying ACL to the external interface
  - **config#** interface Fa0/0
  - **config-if#** ip address 13.1.1.1 255.255.255.0
  - **config-if#** ip access-group 100 in

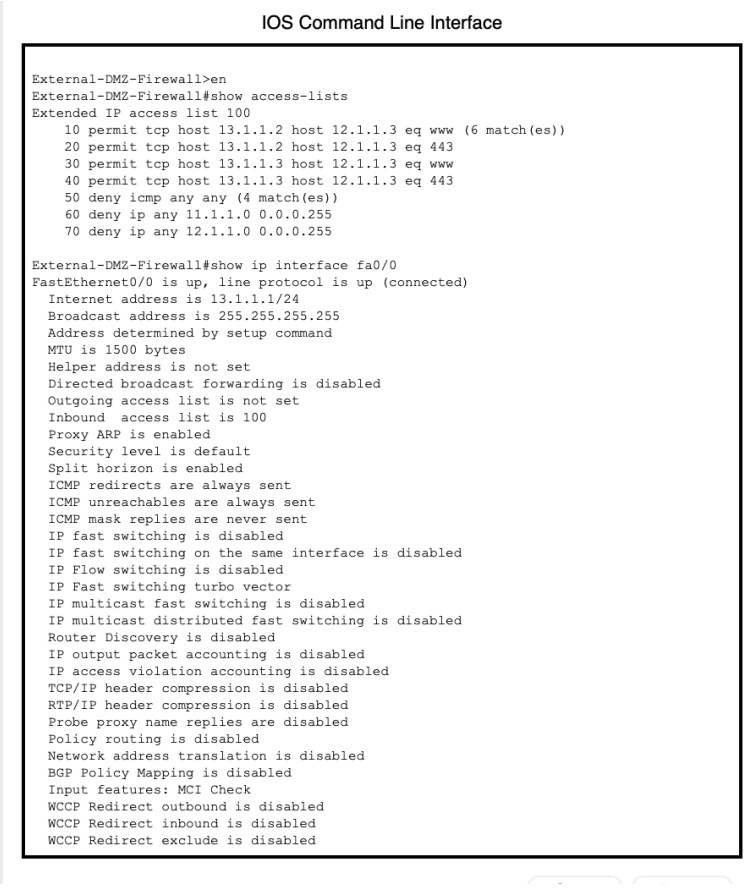

Figure 2: External Network Router - DMZ

1.2.2 Internal Firewall Router

- **ACL 110 - FROM DMZ TO INTERNAL**
  - **config#** access-list 110 remark DMZ-TO-INTERNAL-CONTROL

- Block DMZ from accessing internal network
  - **config#** access-list 110 deny ip 12.1.1.0 0.0.0.255 11.1.1.0 0.0.0.255

- Allow return traffic
  - **config#** access-list 110 permit tcp host 12.1.1.3 11.1.1.0 0.0.0.255 established
- Allow internal users full access
  - **config#** access-list 110 permit ip 11.1.1.0 0.0.0.255 any
- **ACL 120 - FROM INTERNAL TO DMZ**
  - **config#** access-list 120 remark INTERNAL-TO-DMZ-CONTROL
- Allow DMZ accessing the internal network
  - **config#** access-list 120 permit ip 11.1.1.0 0.0.0.255 any
  - **config#** access-list 120 permit ip 12.1.1.0 0.0.0.255 any
- Applying ACL to DMZ interface
  - **config#** interface Fa0/1
  - **config-if#** ip access-group 110 in
  - **config-if#** ip access-group 120 out

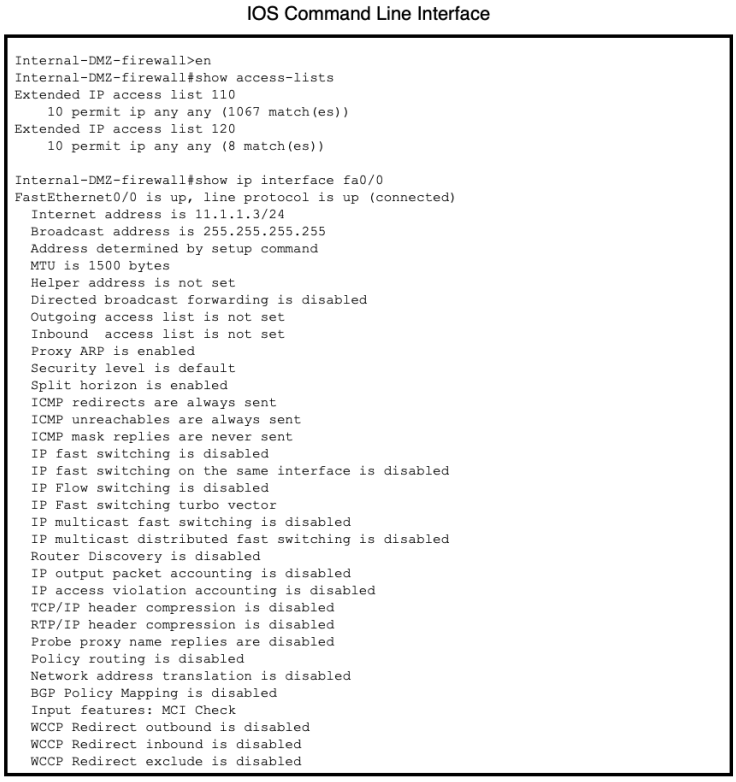

Figure 3: Internal Network Router

1.3 Tests and Summary

We were able to test the objective outcomes of this assignment, as follows:

- External PC1 (13.1.1.2) or PC2 (13.1.1.3) to DMZ Server Access:
  - ping 12.1.1.3 # Should fail (ICMP blocked)
  - telnet 12.1.1.3 80 # Should succeed (HTTP allowed)
  - telnet 12.1.1.3 443 # Should succeed (HTTPS allowed)
- Internal Network Access :
  - ping 12.1.1.3 # Should succeed from PC1 (12.1.1.4)
  - ping 11.1.1.2 # Should succeed from PC1 (12.1.1.4)
  - ping 12.1.1.3 # Should succeed from PC2 (11.1.1.5)
  - ping 11.1.1.2 # Should succeed from PC2 (11.1.1.5)
- DMZ Server Access Attempts:
  - ping 11.1.1.5 # Should fail From DMZ Server (12.1.1.3)
  - ping 12.1.1.4 # Should fail From DMZ Server (12.1.1.3)