Security Project 1: Firewall and Access Control - Group 8

Eric H Ly

Matthew I Morales

Philip Arturo Cesani

Ricardo Jose Reyna

Sahara Armen

**Section I:**

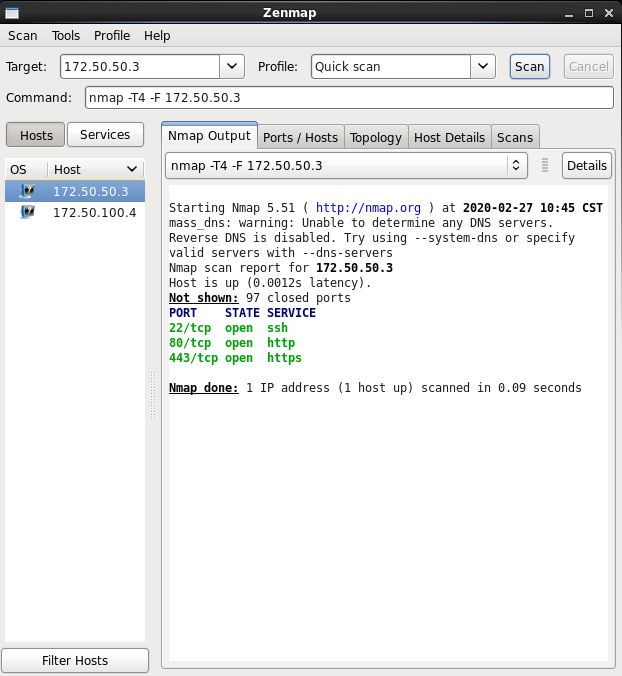
For Project 1, we tried to keep everyone caught up on how to do each task by documenting everything thoroughly through OneNote. Task 1 was completed by the whole group. Task 2 was completed by Matthew, Sahara and Eric. Task 3 was done by Matthew, Eric, and Philip. Task 4 was done by Eric, Philip and Ricardo. Section 2 was written by Sahara and Eric. Section 3 was completed by Philip, Matthew and Sahara. Section 4 was written by Ricardo. Overall we all worked together to complete all the tasks and sections.

**Section II (Task II):**

a)

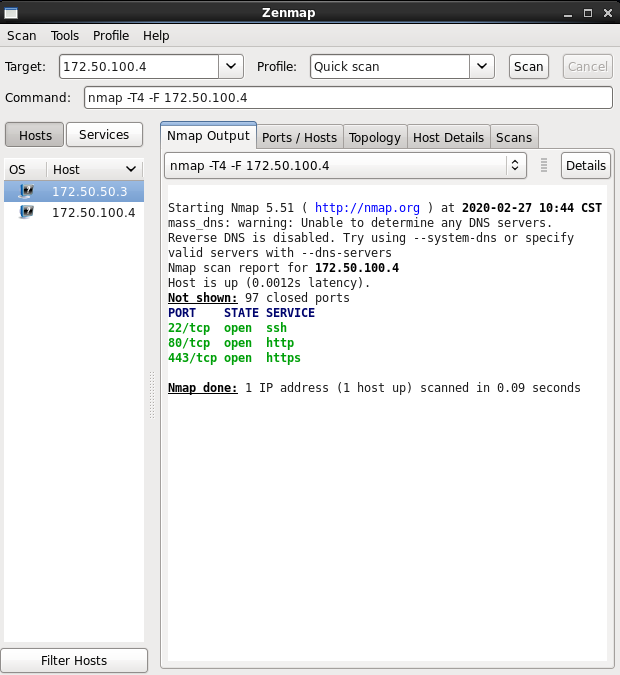
* **nmap 172.50.50.3**

This picture shows the NMap of Workstation E.1.



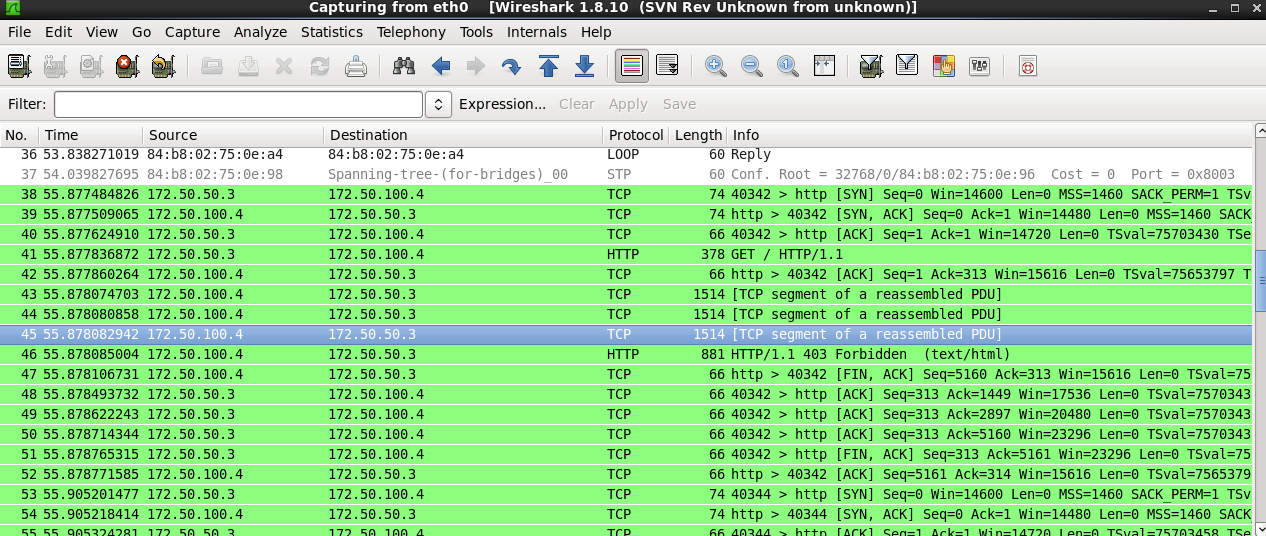
* **nmap 172.50.100.4**

This picture shows the NMap of Server E.2.

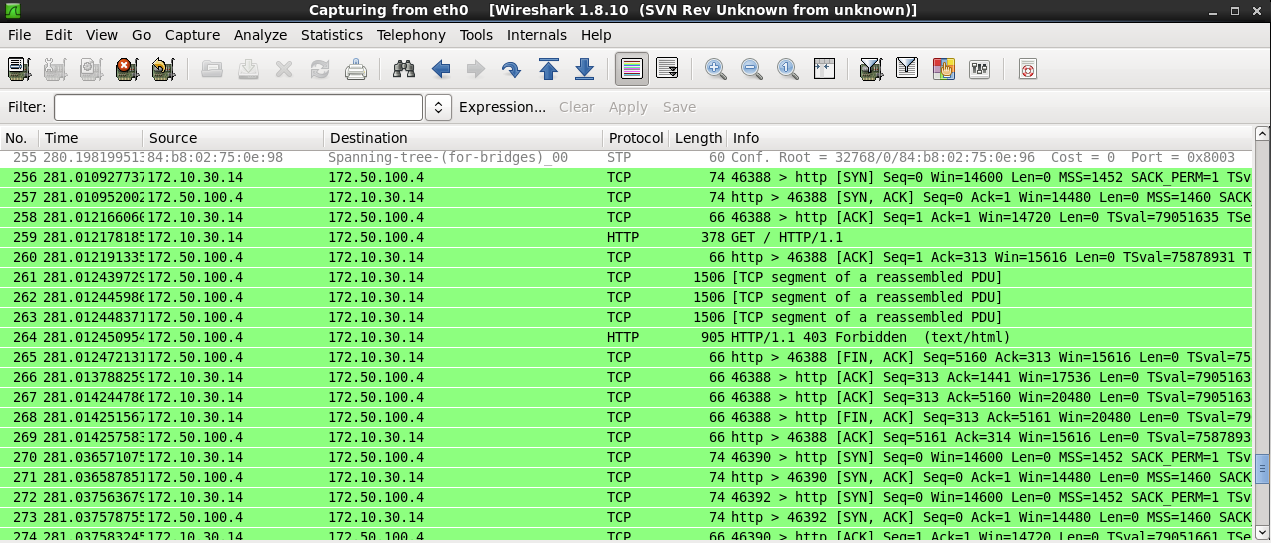


b) Web service is allowed between all the computers.

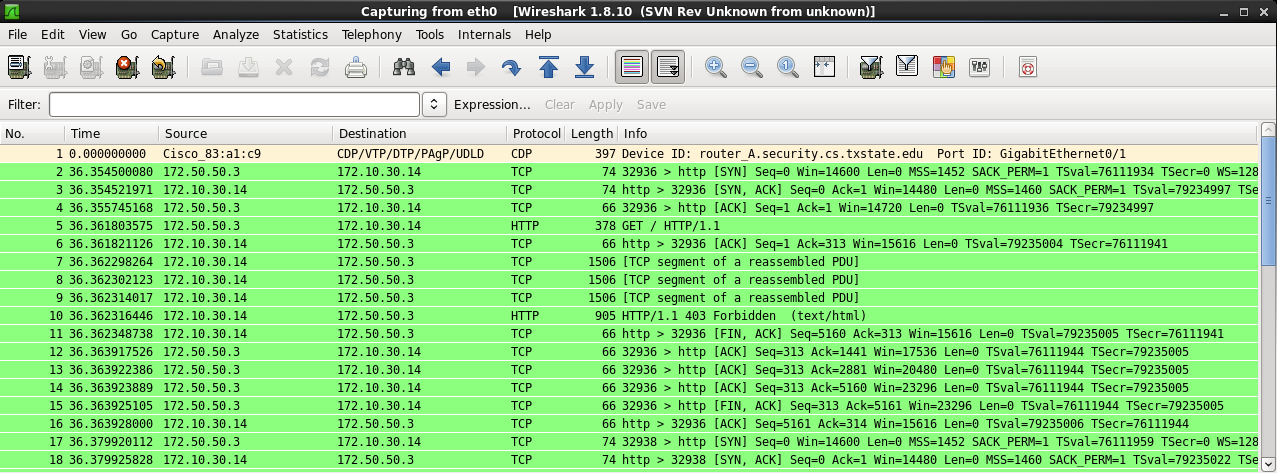
Internal workstation E.1 checking web services on Internal server E.2 web service = Allowed



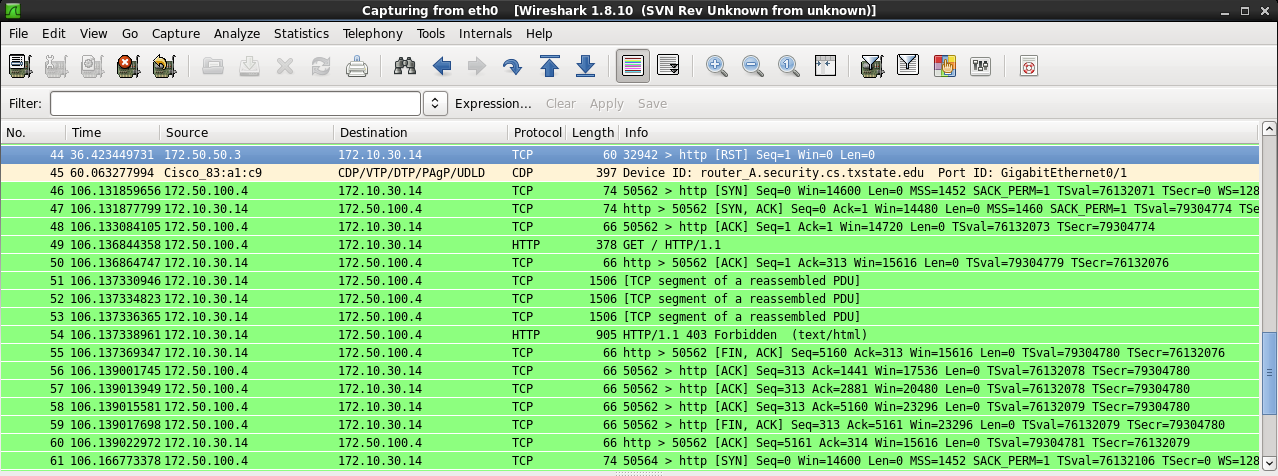
External A.E checking the web services on Internal server E.2. web service = Allowed



Internal workstation E.1 checking web services on External A.E web service = Allowed

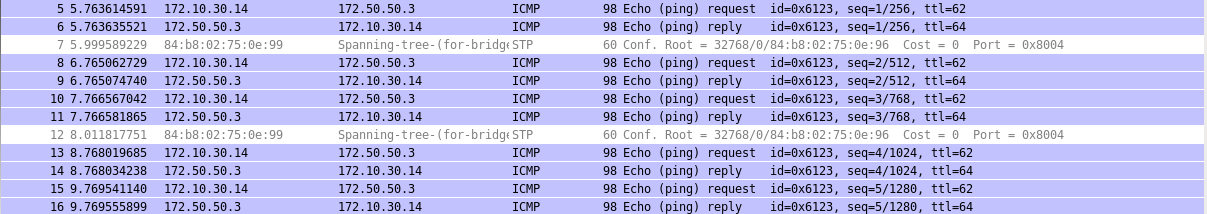


Internal server E.2 checking web services on External A.E web service = Allowed

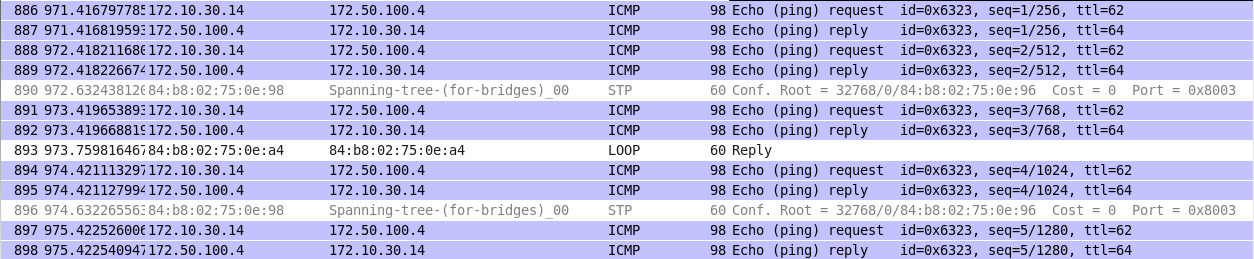


c) Pinging is allowed between all computers in both the internal and external network.

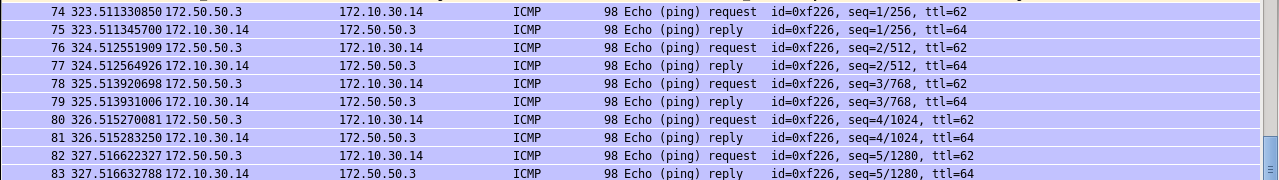
External A.E. pinging Internal workstation E.1



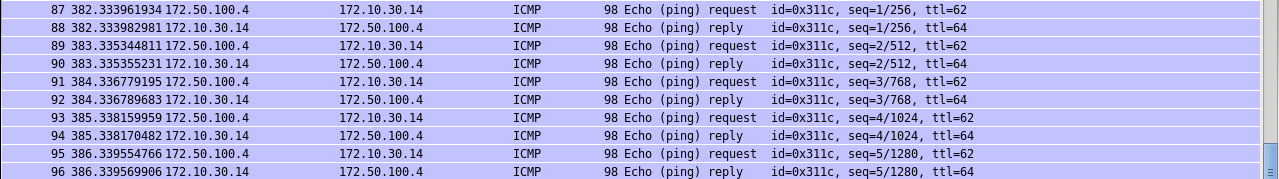
External A.E. pinging Internal server E.2



Internal workstation E.1. pinging External A.E



Internal server E.2. pinging External A.E



d) The default Cisco firewall policy allows all packets to come through from any IP network to any other IP network. There are no restrictions with the default Cisco firewall. It will remain this way until a policy is configured.

**Section III (Task III):**

a)

|  |  |  |  |
| --- | --- | --- | --- |
| **ACM** | **Internal Servers** | **Internal Workstations** | **External Computers** |
| **Internal Servers** | N/A | Ping(ssh) | Ping(ssh) |
| **Internal Workstations** | http,httpd,ssh,ping | N/A | Web,Ping |
| **External** **Computers** | http,httpd | NONE | N/A |

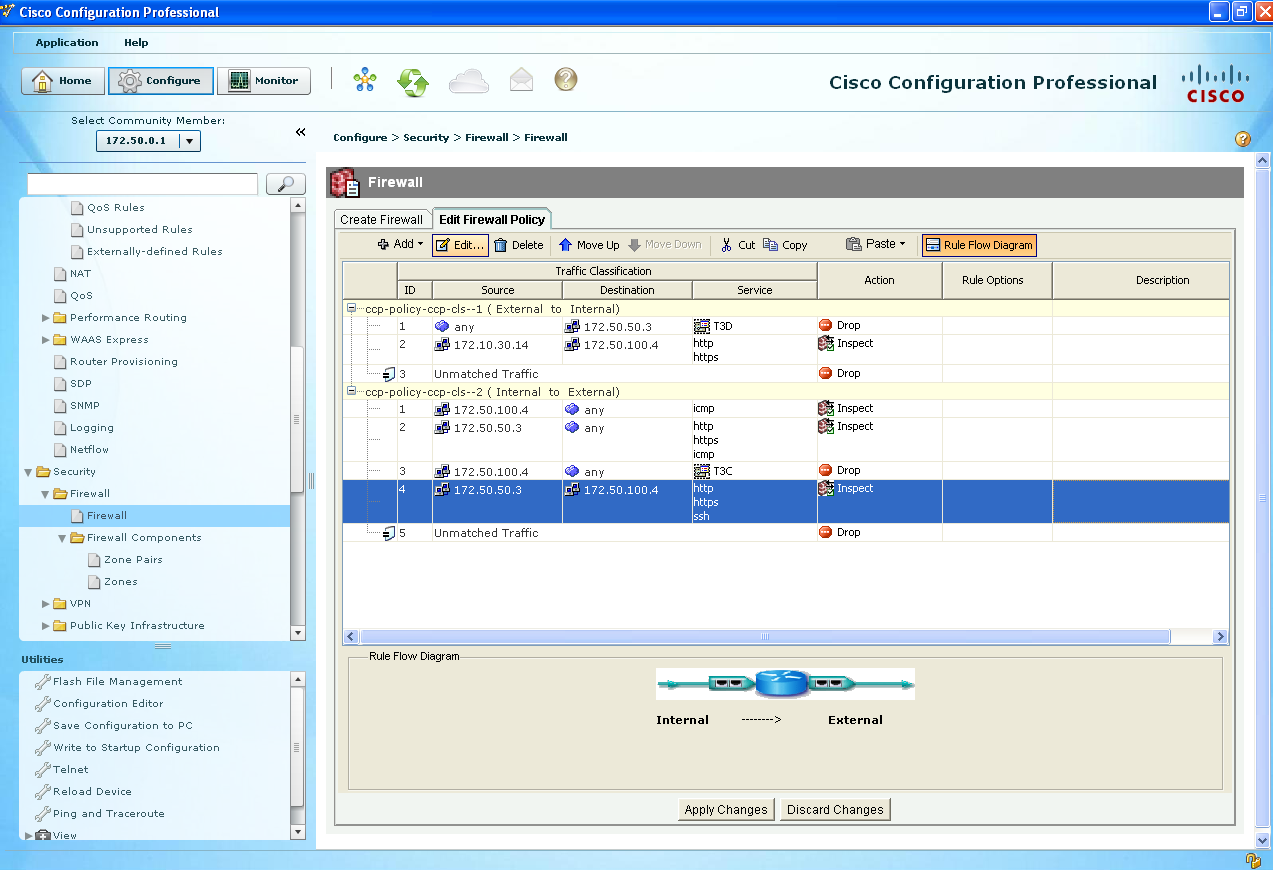
**The Internal Servers refers to the 172.50.100.4/24 computers**

**The Internal Workstations refers to the 172.50.50.3/16**

b)

Policy B cannot be enforced and policy D can only be partially enforced. This is because these policies relate to the internal workstation and internal server which are connected by ethernet and who’s traffic does not pass through the cisco firewall.

c) Cisco firewall configuration



d)

The Cisco firewall filters traffic between “zones”, the external network to the internal network, and back. Although because the internal servers and workstations are on the same network, the Cisco firewall doesn’t come in contact with that traffic or filter it. Therefore, forcing our team to utilize iptables to set the rules for packets being accepted on the server, and iptables allows us to implement those rules that we could not through Cisco. Utilizing iptables allows us to create firewall rules at the Linux kernel level, so traffic can be filtered from computers in the same zone.

e) Iptables commands in the internal server that enforce the security policy that are not

implemented in the Cisco firewall.

iptables -A INPUT -m state --state RELATED, ESTABLISHED -j ACCEPT

iptables -A INPUT -p -tcp --dport 22 -s 172.50.50.3/16 -d 172.50.100.4/24 -j ACCEPT

iptables -A INPUT -p -tcp --dport 80 -s 172.50.50.3/16 -d 172.50.100.4/24 -j ACCEPT

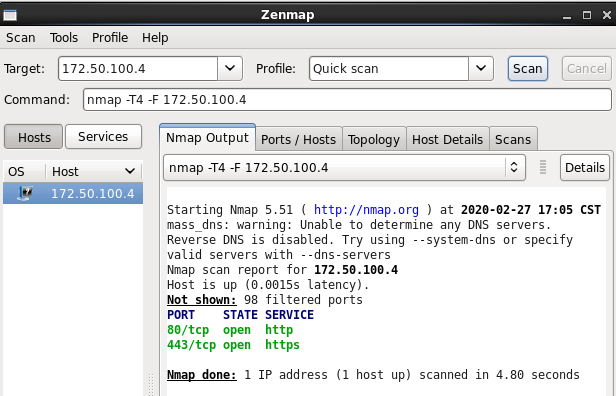
iptables -A INPUT -p -tcp --dport 80 -s 172.50.50.3/16 -d 172.50.100.4/24 -j ACCEPT

Iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT

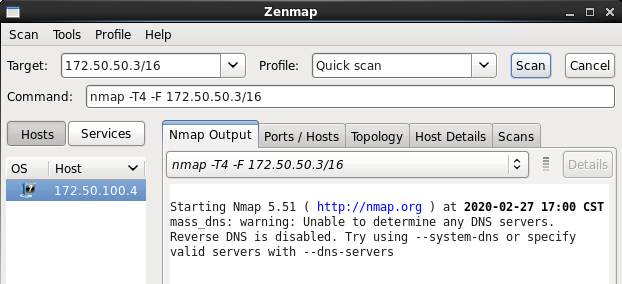
**Section IV (Task IV):**

a)

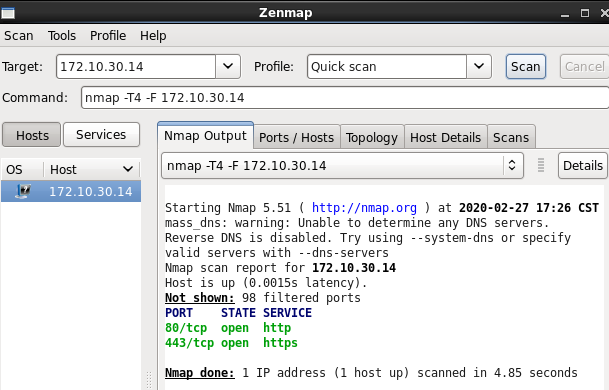
Open ports from the Internal Server E.2 checked from the External Computer A.E



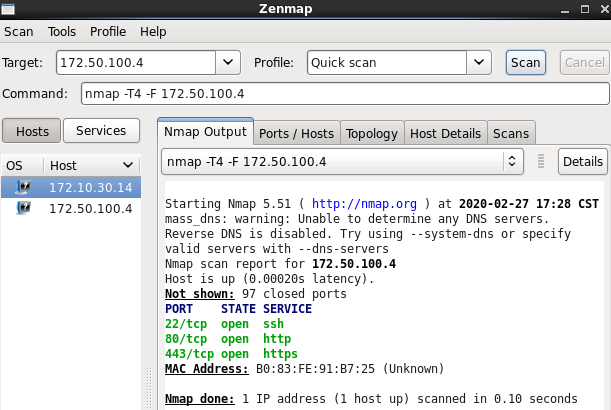
Open ports from the Internal Work Station E.1 checked from the External Computer A.E



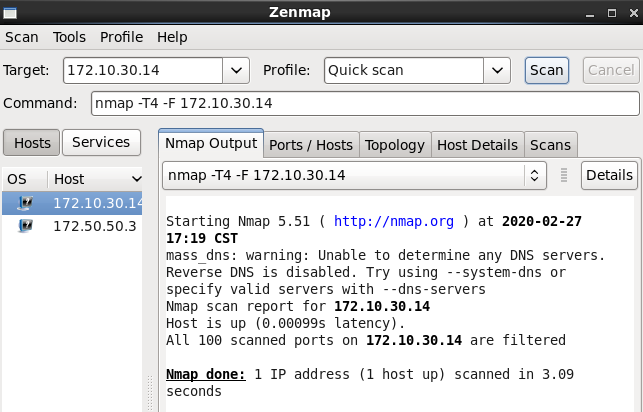
Open ports from the External Computer A.E checked from the Internal Work Station E.1



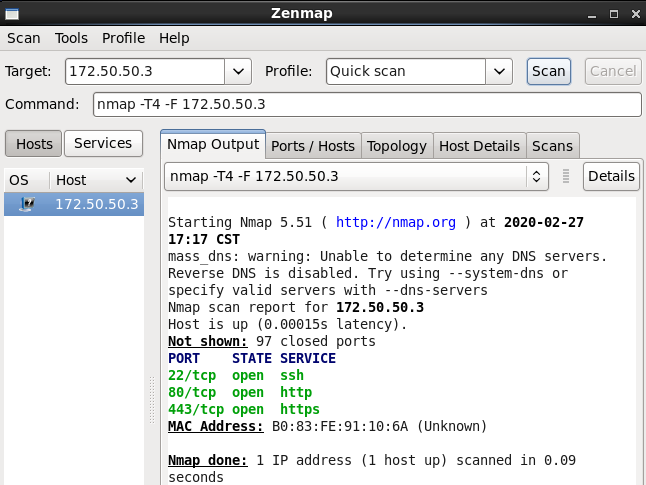
Open ports from the Internal Server E.2 checked from the Internal Work Station E.1



Open ports from the External Computer A.E checked from the Internal Server E.2

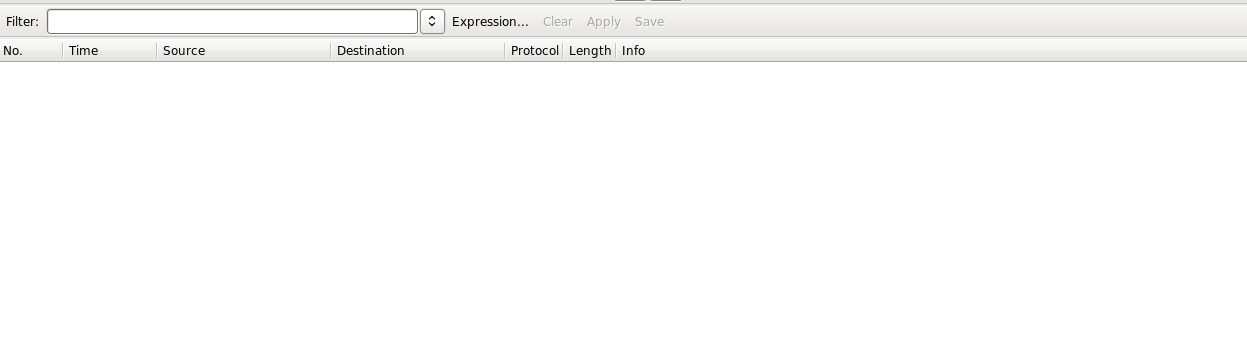


Open ports from the Internal Work Station E.1 checked from the Internal Server E.2.

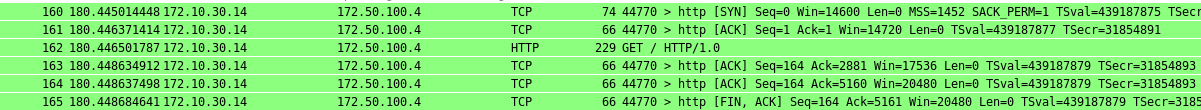


b) We used the command curl since it is a command line tool used to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE) In addition, we used Apache

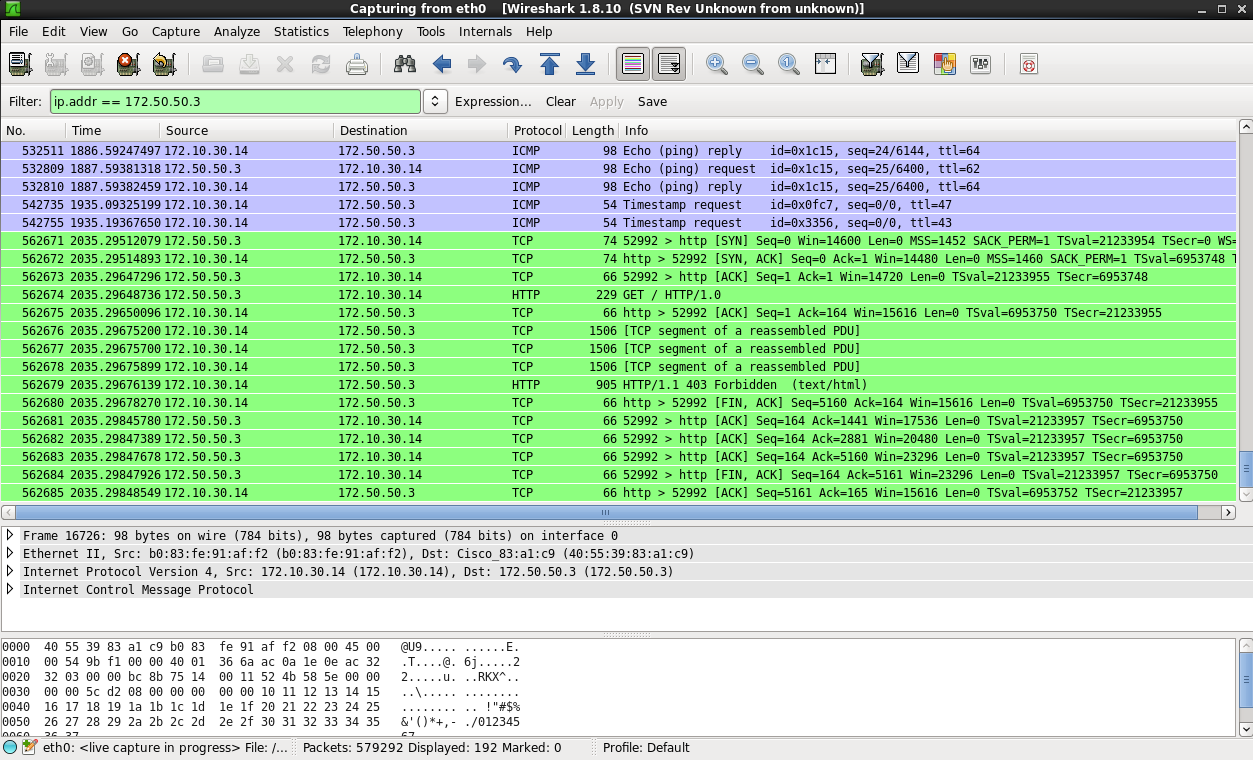
This picture shows how we could not access the Web Services of E.1 from the External Server A.E.



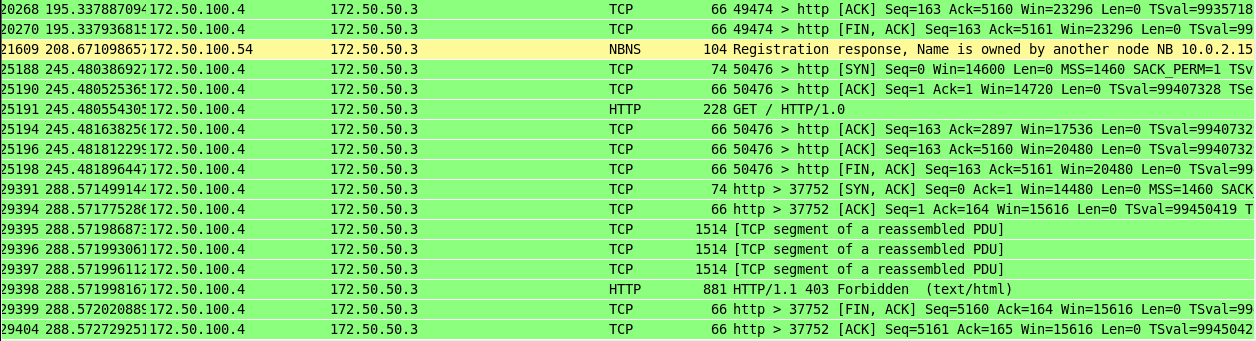
This picture shows how we could access the Web Services of Internal Server E.2 from the External Computer A.E.



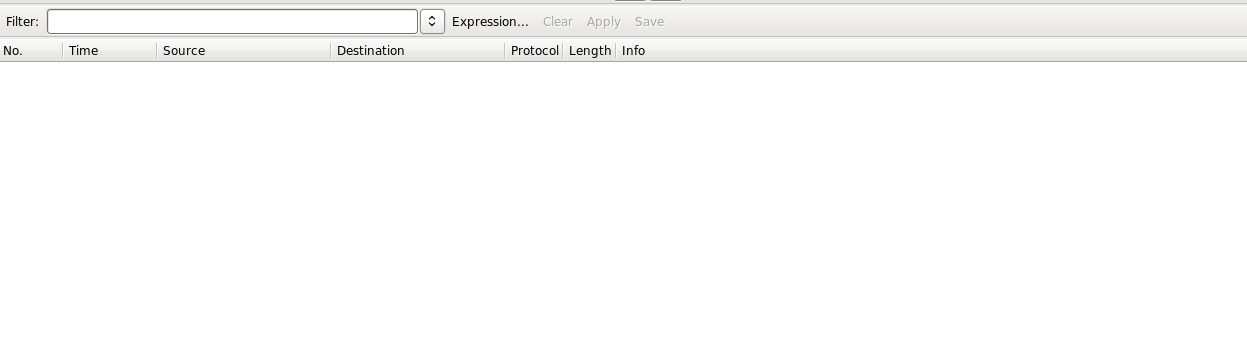
This picture shows that the Work Station E.1 was able to access the Web Services of the External Computer A.E.



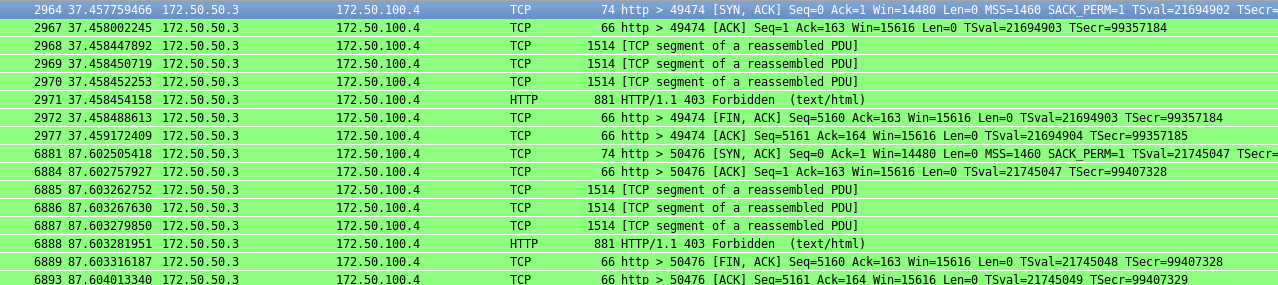
This picture shows that the Work Station E.1 was able to access the Web Services of the Internal Server E.2.



The Internal Server E.2 was not able to access the Web Services of the External Server A.E



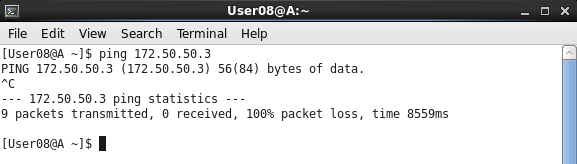
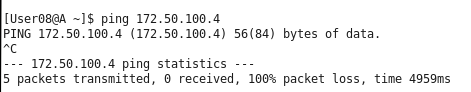
This picture shows that the Internal Server E.2 was able to access the Web Services of the Work Station E.1

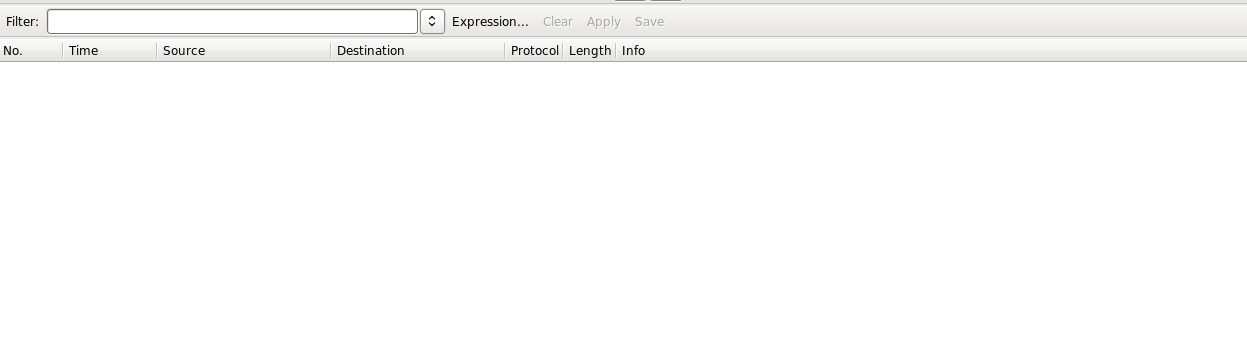


c)

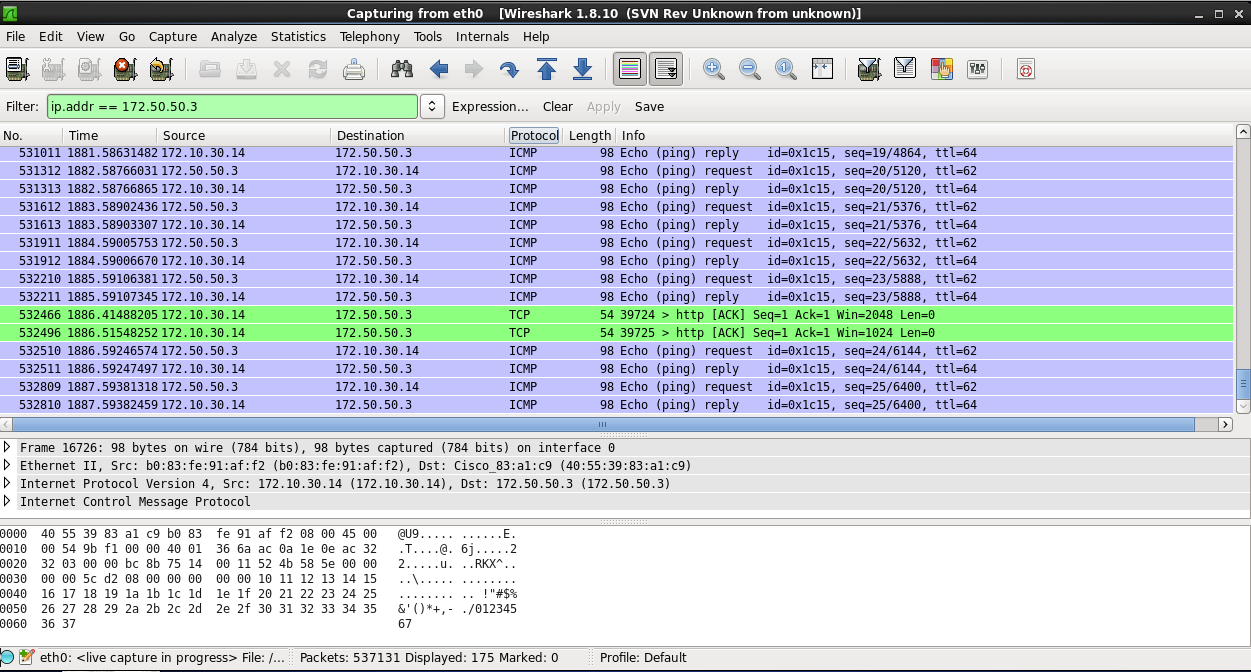
These three pictures show that you can not ping from the

* External computer A.E to the Internal Work Station E.1
* External computer A.E to the Internal Server E.2.

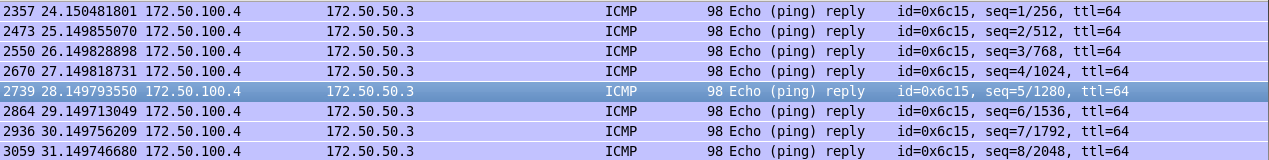




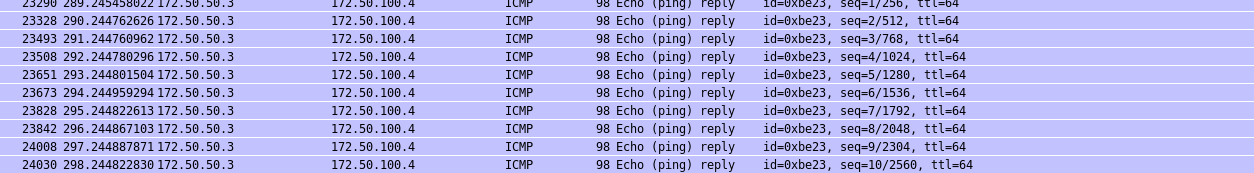
This picture shows that you can ping from the Work Station E.1 to the External Computer A.E.



Shows that you can ping from the Internal Server E.2 to the Internal Work Station E.1



Shows that you can ping from Internal Work Station E.1 the to the Internal Server E.2



d)

The security policy can ensure that classified data will not be disclosed to external computers through most attacks with the exception of any attack that uses ping. Since the internal workstation can ping external computers it is vulnerable to something like a ping tunneling attack which can fake traffic that gets through the Cisco firewall policy and could allow the hacker to get classified data.

