

# **Project 1: Firewall and Access Control**

**Date: 3/5/2019**

## **Group 2:**

**Gael Sanchez**

**Jacob Gibson**

**Johannes Schneemann**

**Rogelio Garza**

**Zachary Golla**

## **Section I Introduction:**

Group B was assigned lab time on Monday from 10:00 a.m. to 8:00 p.m. and Wednesday from 10:00 a.m. to 3:00 p.m. We agreed to meet every Monday and Wednesday from 10:00 a.m. to 12:30 p.m. to work on this project as that worked with everyone's schedules best. We also used Slack for online communication regarding any progress, questions, ideas, and Google Docs for tracking progress and collaboration in writing this report.

The objectives of this assignment are to learn how to use networking and security devices, and tools, how to setup and configure networking systems, how to implement security policies for networking systems, and how to analyze and verify the security of networking systems.

We achieved these objectives with the following four tasks and their sub tasks.

### **Task One - Setting Up Our Networks:**

Jacob setup the internal workstation

Johannes setup the internal server

Rogelio setup the external network

### **Task Two - Testing the Default Cisco Firewall Policy:**

Jacob configured the WinXP VM and removed all default Cisco firewall rules

Rogelio ran NMap on A.B to B.1 and B.2

Jacob tested if B.1 can access web services in B.2

Rogelio tested if A.B can access web services in B.2

Zac tested if B.1 can access web services in A.B

Johannes tested if B.2 can access web services in A.B

Rogelio tested if A.B can ping B.1

Rogelio tested if A.B can ping B.2

Zac tested if B.1 can ping AB

Johannes tested if B.2 can ping A.B

### **Task Three - Implementing a Security Policy:**

Zac created a firewall rule for internal servers to provide only web service to external computers.

Gael created a firewall rule for internal servers to provide only SSH and web service to internal workstations, with iptables.

Jacob created a firewall rule for internal servers to not access any service provided by any external computer.

Jacob created a firewall rule for internal workstations to not provide any service.

Rogelio created a firewall rule for internal workstations to access the services hosted by internal servers, with iptables.

Gael created a firewall rule for internal workstations to access only the web service provided by external computers.

Johannes created a firewall rule for internal computers can ping any computer.

Rogelio created a firewall rule for external computers to not be able to ping internal computers.

**Task Four - Testing Our Security Policy:**

Rogelio ran NMap on A.B to B.1 and B.2  
Johannes tested if B.1 can access web services in B.2  
Rogelio tested if A.B can access web services in B.2  
Johannes tested if B.1 can access web services in A.B  
Gael tested if B.2 can access web services in A.B  
Jacob tested if A.B can ping B.1  
Jacob tested if A.B can ping B.2  
Zac tested if B.1 can ping A.B  
Gael tested if B.2 can ping A.B

**This report has been divided into four sections for writing purposes:**

Section one of the report which is the introduction was written by Rogelio  
Section two of the report which is a summary of initial configuration and testing of the default security policy was written by Johannes  
Section three of the report which is a summary of the implementation of our security policy was written by Jacob and Gael.  
Section four of the report which a summary of testing our security policy was written by Zac.

## Section II (Task II: Default Cisco firewall policy and exploit testing):

### A. Show the NMap commands to scan the computer and the service ports

- a. Command run in terminal is: *“sudo nmap -v -PS 172.20.0.1/16”*

```
File Edit View Search Terminal Help
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
2002/tcp  open  globe
2002/tcp  open  mlchat-proxy
6002/tcp  open  X11:2
6002/tcp  open  dynamid

Nmap scan report for 172.20.0.2
Host is up (0.0049s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http

Nmap scan report for 172.20.50.3
Host is up (0.00093s latency).
All 1000 scanned ports on 172.20.50.3 are closed

Nmap scan report for 172.20.100.4
Host is up (0.00088s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 172.20.100.54
Host is up (0.0013s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
145/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

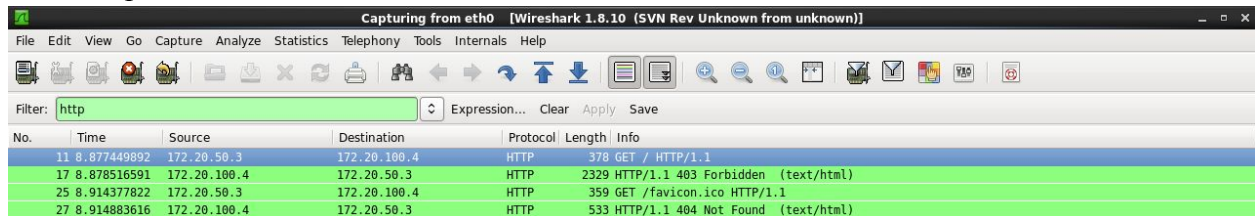
Read data files from: /usr/share/nmap
Nmap done: 65536 IP addresses (5 hosts up) scanned in 1193.51 seconds
Raw packets sent: 136271 (5.996MB) | Rcvd: 5023 (201.152KB)
User02@A ~]$
```

## B. Show the Wireshark results (screen shots) of checking the web service between computers

*Note: Though some of these screenshots show various 400 errors, every connection was allowed and displayed the Apache test page without issue. Therefore, we have concluded that each connection web service connection shown is allowed.*

This screenshot is for testing web service from B.1 to B.2 with Wireshark:

Expected Result: Web service is Allowed      Actual Result: Web service is Allowed



| No. | Time        | Source       | Destination  | Protocol | Length | Info                               |
|-----|-------------|--------------|--------------|----------|--------|------------------------------------|
| 11  | 8.877449892 | 172.20.50.3  | 172.20.100.4 | HTTP     | 378    | GET / HTTP/1.1                     |
| 17  | 8.878516591 | 172.20.100.4 | 172.20.50.3  | HTTP     | 2329   | HTTP/1.1 403 Forbidden (text/html) |
| 25  | 8.914377822 | 172.20.50.3  | 172.20.100.4 | HTTP     | 359    | GET /favicon.ico HTTP/1.1          |
| 27  | 8.914883616 | 172.20.100.4 | 172.20.50.3  | HTTP     | 533    | HTTP/1.1 404 Not Found (text/html) |

This screenshot is for testing web service from A.B to B.2 with Wireshark:

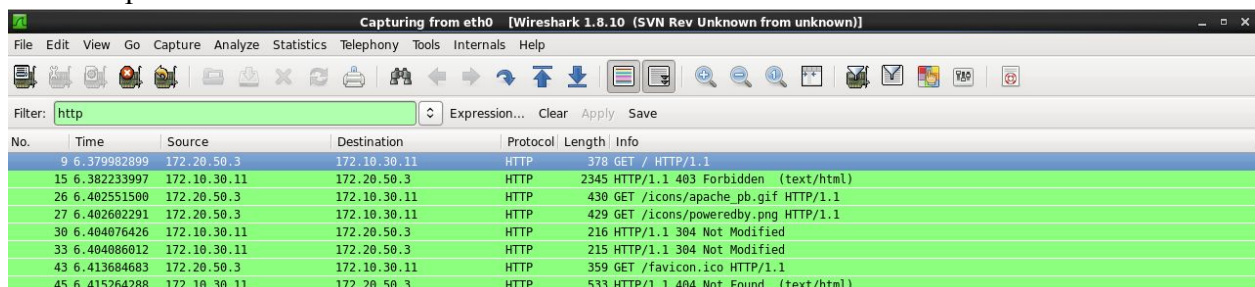
Expected Result: Web service is Allowed      Actual Result: Web service is Allowed



| No. | Time        | Source       | Destination  | Protocol | Length | Info                               |
|-----|-------------|--------------|--------------|----------|--------|------------------------------------|
| 4   | 0.001314365 | 172.10.30.11 | 172.20.100.4 | HTTP     | 378    | GET / HTTP/1.1                     |
| 8   | 0.003344718 | 172.20.100.4 | 172.10.30.11 | HTTP     | 3785   | HTTP/1.1 403 Forbidden (text/html) |

This screenshot is for testing web service from B.1 to A.B with Wireshark:

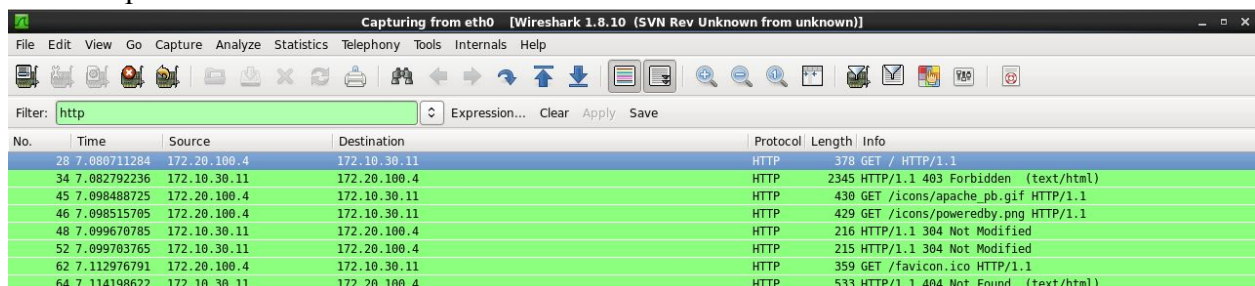
Expected Result: Web service is Allowed      Actual Result: Web service is Allowed



| No. | Time        | Source       | Destination  | Protocol | Length | Info                               |
|-----|-------------|--------------|--------------|----------|--------|------------------------------------|
| 9   | 6.379982899 | 172.10.30.11 | 172.20.50.3  | HTTP     | 378    | GET / HTTP/1.1                     |
| 15  | 6.382233997 | 172.10.30.11 | 172.20.50.3  | HTTP     | 2345   | HTTP/1.1 403 Forbidden (text/html) |
| 26  | 6.402551508 | 172.20.50.3  | 172.10.30.11 | HTTP     | 430    | GET /icons/apache_pb.gif HTTP/1.1  |
| 27  | 6.402682291 | 172.20.50.3  | 172.10.30.11 | HTTP     | 429    | GET /icons/powerby.png HTTP/1.1    |
| 30  | 6.404076426 | 172.10.30.11 | 172.20.50.3  | HTTP     | 216    | HTTP/1.1 304 Not Modified          |
| 33  | 6.404866912 | 172.10.30.11 | 172.20.50.3  | HTTP     | 215    | HTTP/1.1 304 Not Modified          |
| 43  | 6.413684683 | 172.20.50.3  | 172.10.30.11 | HTTP     | 359    | GET /favicon.ico HTTP/1.1          |
| 45  | 6.415264288 | 172.10.30.11 | 172.20.50.3  | HTTP     | 533    | HTTP/1.1 404 Not Found (text/html) |

This screenshot is for testing web service from B.2 to A.B with Wireshark:

Expected Result: Web service is Allowed      Actual Result: Web service is Allowed

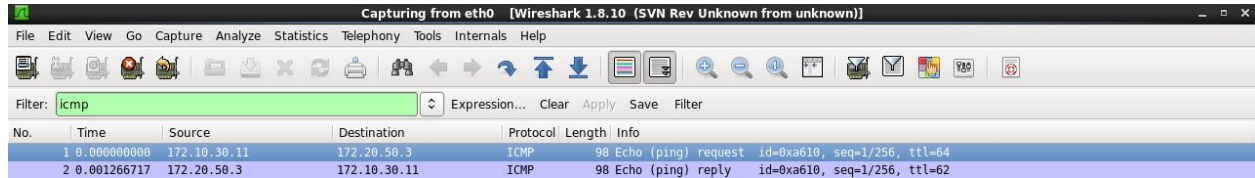


| No. | Time        | Source       | Destination  | Protocol | Length | Info                               |
|-----|-------------|--------------|--------------|----------|--------|------------------------------------|
| 28  | 7.080711284 | 172.20.100.4 | 172.10.30.11 | HTTP     | 378    | GET / HTTP/1.1                     |
| 34  | 7.082792236 | 172.10.30.11 | 172.20.100.4 | HTTP     | 2345   | HTTP/1.1 403 Forbidden (text/html) |
| 45  | 7.098488725 | 172.20.100.4 | 172.10.30.11 | HTTP     | 430    | GET /icons/apache_pb.gif HTTP/1.1  |
| 46  | 7.098515705 | 172.20.100.4 | 172.10.30.11 | HTTP     | 429    | GET /icons/powerby.png HTTP/1.1    |
| 48  | 7.099670785 | 172.10.30.11 | 172.20.100.4 | HTTP     | 216    | HTTP/1.1 304 Not Modified          |
| 52  | 7.099703765 | 172.10.30.11 | 172.20.100.4 | HTTP     | 215    | HTTP/1.1 304 Not Modified          |
| 62  | 7.112976791 | 172.20.100.4 | 172.10.30.11 | HTTP     | 359    | GET /favicon.ico HTTP/1.1          |
| 64  | 7.114198622 | 172.10.30.11 | 172.20.100.4 | HTTP     | 533    | HTTP/1.1 404 Not Found (text/html) |

**C. Show the Wireshark results (screen shots) of checking the ping between computers.  
State if ping is allowed between computers**

This screenshot is for testing ping from A.B to B.1 with Wireshark:

Expected Result: Ping is allowed      Actual Result: Ping is allowed



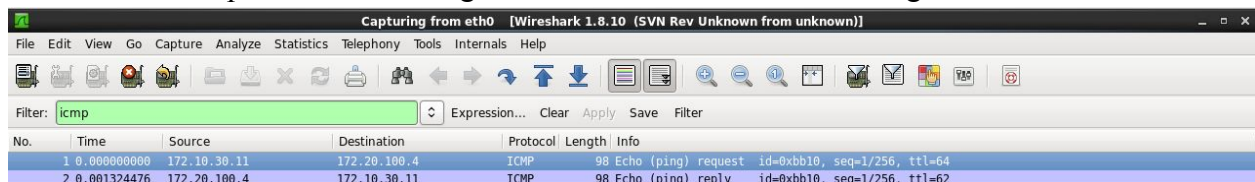
Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]

Filter: icmp

| No. | Time        | Source       | Destination  | Protocol | Length | Info   |
|-----|-------------|--------------|--------------|----------|--------|--|
| 1   | 0.000000000 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) request id=0xa610, seq=1/256, ttl=64 |
| 2   | 0.001266717 | 172.20.50.3  | 172.10.30.11 | ICMP     | 98     | Echo (ping) reply id=0xa610, seq=1/256, ttl=62   |

This screenshot is for testing ping from A.B to B.2 with Wireshark:

Expected Result: Ping is allowed      Actual Result: Ping is allowed



Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]

Filter: icmp

| No. | Time        | Source       | Destination  | Protocol | Length | Info   |
|-----|-------------|--------------|--------------|----------|--------|--|
| 1   | 0.000000000 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0xbb10, seq=1/256, ttl=64 |
| 2   | 0.001324476 | 172.20.100.4 | 172.10.30.11 | ICMP     | 98     | Echo (ping) reply id=0xbb10, seq=1/256, ttl=62   |

This screenshot is for testing ping from B.1 to A.B with Wireshark:

Expected Result: Ping is allowed      Actual Result: Ping is allowed




Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]

Filter: icmp

| No. | Time         | Source       | Destination  | Protocol | Length | Info   |
|-----|--------------|--------------|--------------|----------|--------|--|
| 619 | 12.148766332 | 172.20.50.3  | 172.10.30.11 | ICMP     | 98     | Echo (ping) request id=0xa527, seq=1/256, ttl=64 |
| 620 | 12.150190232 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0xa527, seq=1/256, ttl=62   |
| 672 | 13.150305823 | 172.20.50.3  | 172.10.30.11 | ICMP     | 98     | Echo (ping) request id=0xa527, seq=2/512, ttl=64 |
| 673 | 13.151380679 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0xa527, seq=2/512, ttl=62   |
| 724 | 14.151508820 | 172.20.50.3  | 172.10.30.11 | ICMP     | 98     | Echo (ping) request id=0xa527, seq=3/768, ttl=64 |
| 725 | 14.152881812 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0xa527, seq=3/768, ttl=62   |

This screenshot is for testing ping from B.1 to B.2 with Wireshark:

Expected Result: Ping is allowed      Actual Result: Ping is allowed



Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]

Filter: icmp

| No. | Time         | Source       | Destination  | Protocol | Length | Info   |
|-----|--------------|--------------|--------------|----------|--------|--|
| 616 | 12.232387420 | 172.20.50.3  | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x9427, seq=1/256, ttl=64 |
| 617 | 12.232556387 | 172.20.100.4 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0x9427, seq=1/256, ttl=64   |
| 669 | 13.231548794 | 172.20.50.3  | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x9427, seq=2/512, ttl=64 |
| 670 | 13.231737079 | 172.20.100.4 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0x9427, seq=2/512, ttl=64   |
| 721 | 14.231580250 | 172.20.50.3  | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x9427, seq=3/768, ttl=64 |
| 722 | 14.231748685 | 172.20.100.4 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0x9427, seq=3/768, ttl=64   |

This screenshot is for testing ping from B.2 to B.1 with Wireshark:  
Expected Result: Ping is allowed      Actual Result: Ping is allowed



This screenshot is for testing ping from B.2 to A.B with Wireshark:  
Expected Result: Ping is allowed      Actual Result: Ping is allowed



#### D. Summarize the default Cisco firewall policy

The default Cisco firewall policy has no rules in place to manage traffic control into or outside of the network. Because of this, all traffic tested was allowed to flow in and out of the router without hindrance. This allowed us to ping any computer and connect to any open web services.

### Section III (Task III: Implement security policy)

#### A. Copy and paste the access control matrix

|  | Objects              |                            |                      |                     |
|--|----------------------|----------------------------|----------------------|---------------------|
|  |                      | Internal Server            | Internal Workstation | External Computer   |
|  | Internal Server      |                            | Ping                 | Ping                |
|  | Internal Workstation | Web Service<br>SSH<br>Ping |                      | Web Service<br>Ping |
|  | External Computer    | Web Service                |                      |                     |

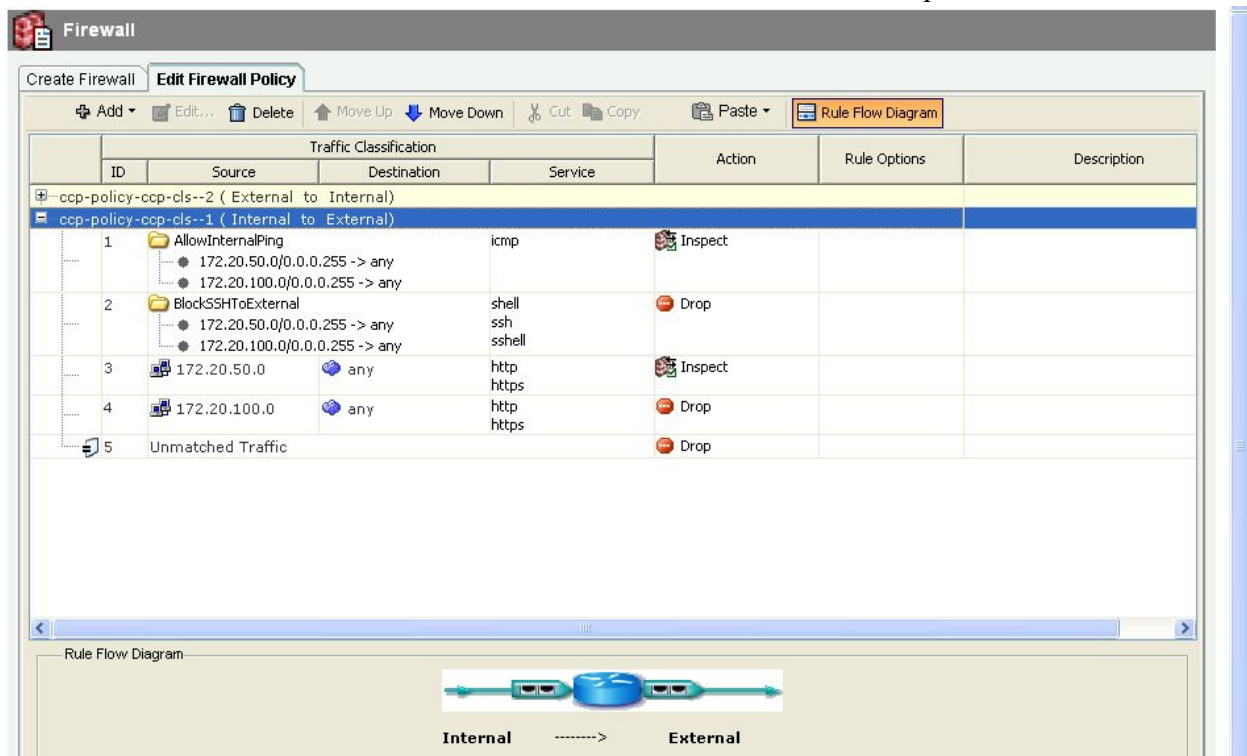


**B. Find and explain which policy cannot be enforced by the Cisco firewall and which policy can only partially be enforced by the Cisco firewall**

The firewall can't enforce rules on the internal traffic between computer B.1 and B.2. If we want to enforce policies on those individual machines, we need to utilize iptables rules on the machines. In other words, all traffic that goes through the router (internal to external and vice versa) is controlled by the firewall and the traffic within the internal network can't be enforced with the firewall. For that traffic we need to setup iptables. Specifically for our policies, this means that policy B and policy E cannot be enforced with only a firewall.

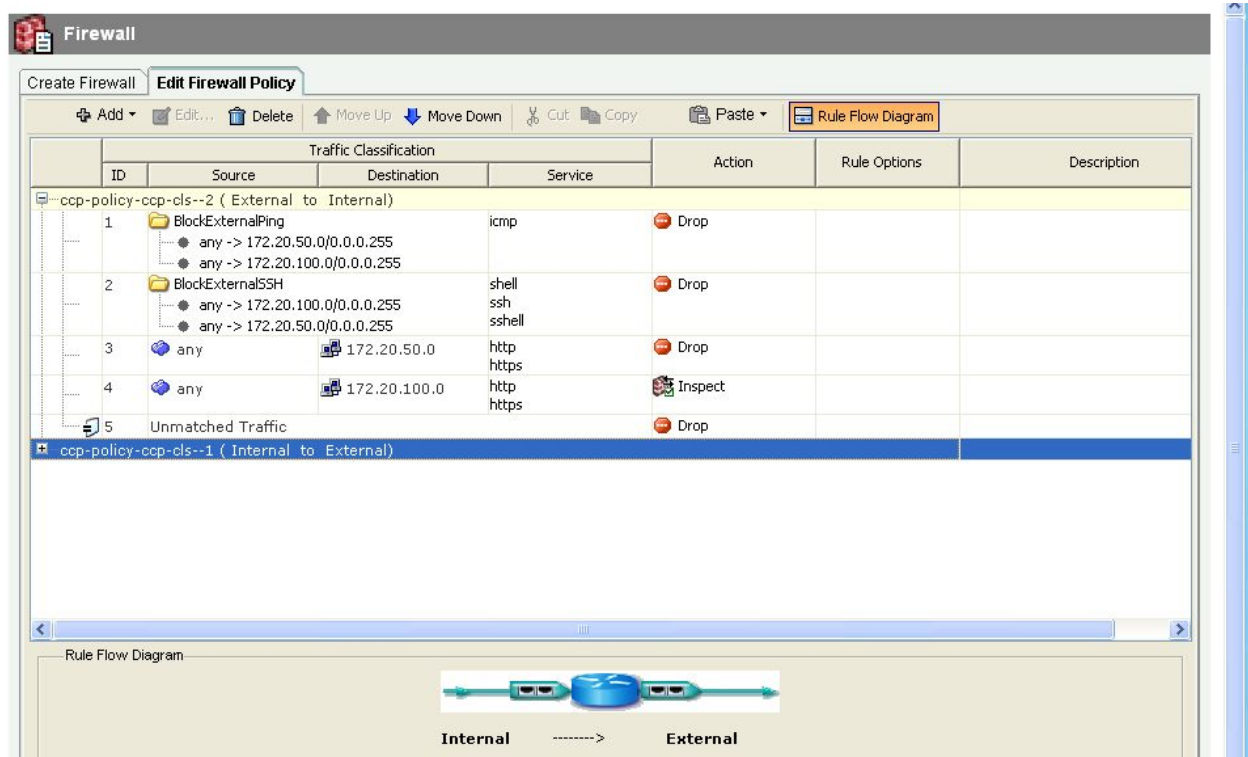
**C. Copy and paste a screenshot of your Cisco firewall configuration**

This is a screenshot of our internal zone to external zone policies:





This is a screenshot of our external zone to internal zone policies:



**D. Discuss how to use iptables to enforce the security policy that is not implemented in the Cisco firewall**

Iptables must be used to regulate internal traffic rules for policies B and E. Both of these policies refer to the fact that the servers should provide the services of web and SSH to the workstations. Therefore, iptables rules must be created to regulate this internal traffic between computers with server ip's and computers with workstation ip's

**E. Show the iptables commands in the internal server that enforce the security policy that is not implemented in the Cisco firewall**

**B) Internal servers provide only SSH and web services to internal workstations**

```
sudo iptables -A INPUT -p tcp -s 172.20.50.0/24 --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
sudo iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
sudo iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

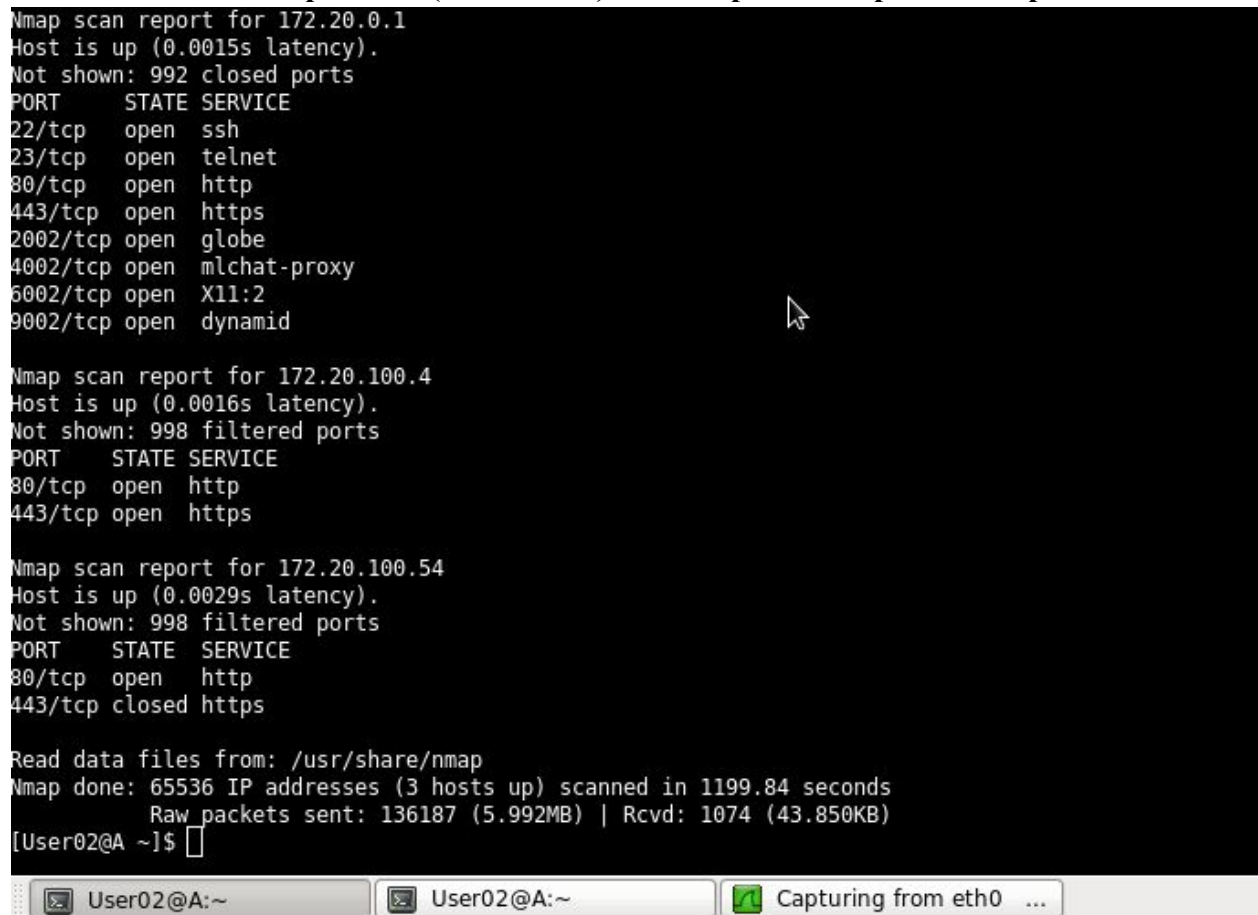
**E) Internal workstations can access the services hosted by internal servers**

```
sudo iptables -A INPUT -p tcp -s 172.20.50.0/24 -j ACCEPT  
sudo iptables -A OUTPUT -p - tcp -d 172.20.0.0/16 -j ACCEPT
```

```
sudo iptables -A INPUT -p udp -s 172.20.50.0/24 -j ACCEPT  
sudo iptables -A OUTPUT -p - udp -d 172.20.0.0/16 -j ACCEPT
```

**Section IV(Task IV: Test the implementation of the security policy)**

**A. Show the NMap results (screenshots) of the exposed computers and ports**

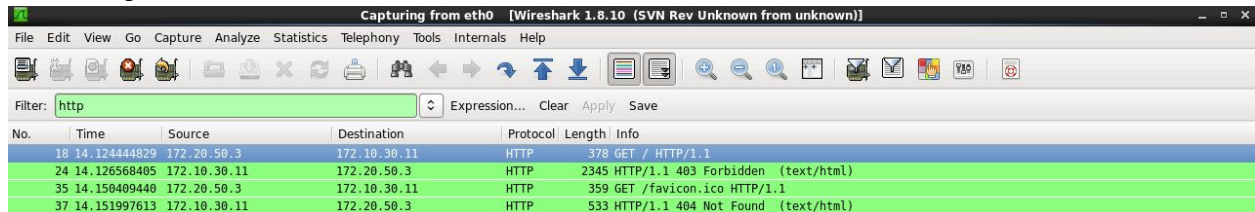


```
Nmap scan report for 172.20.0.1  
Host is up (0.0015s latency).  
Not shown: 992 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
23/tcp    open  telnet  
80/tcp    open  http  
443/tcp   open  https  
2002/tcp  open  globe  
4002/tcp  open  mlchat-proxy  
6002/tcp  open  X11:2  
9002/tcp  open  dynamid  
  
Nmap scan report for 172.20.100.4  
Host is up (0.0016s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap scan report for 172.20.100.54  
Host is up (0.0029s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   closed https  
  
Read data files from: /usr/share/nmap  
Nmap done: 65536 IP addresses (3 hosts up) scanned in 1199.84 seconds  
Raw packets sent: 136187 (5.992MB) | Rcvd: 1074 (43.850KB)  
[User02@A ~]$
```

**B. Show the Wireshark results (screenshots) of checking the web service between computers. State if web service is allowed between computers**

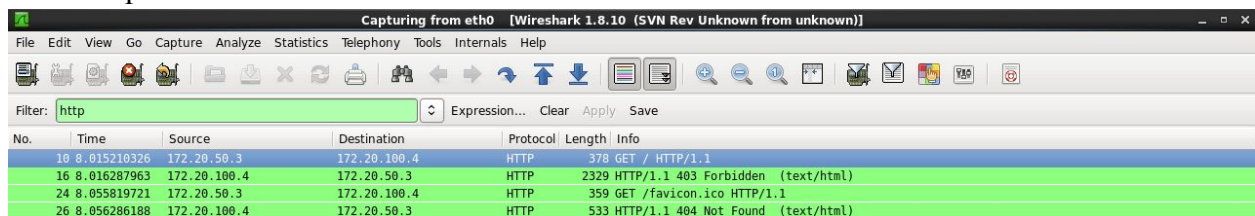
*Note: Similarly as above, some web connections show various 400 errors even when they are allowed to go through and load the Apache test page. However, it is ONLY when nothing is displayed that the web service was totally blocked.*

This screenshot is testing web services from B.1 to A.B with Wireshark:  
Expected Result: Web service is Allowed      Actual Result: Web service is Allowed



| No. | Time         | Source       | Destination  | Protocol | Length | Info                               |
|-----|--------------|--------------|--------------|----------|--------|------------------------------------|
| 18  | 14.124444829 | 172.20.50.3  | 172.10.30.11 | HTTP     | 378    | GET / HTTP/1.1                     |
| 24  | 14.126568405 | 172.10.30.11 | 172.20.50.3  | HTTP     | 2345   | HTTP/1.1 403 Forbidden (text/html) |
| 35  | 14.150409440 | 172.20.50.3  | 172.10.30.11 | HTTP     | 359    | GET /favicon.ico HTTP/1.1          |
| 37  | 14.151997613 | 172.10.30.11 | 172.20.50.3  | HTTP     | 533    | HTTP/1.1 404 Not Found (text/html) |

This screenshot is for testing web services from B.1 to B.2 with Wireshark:  
Expected Result: Web service is Allowed      Actual Result: Web service is Allowed



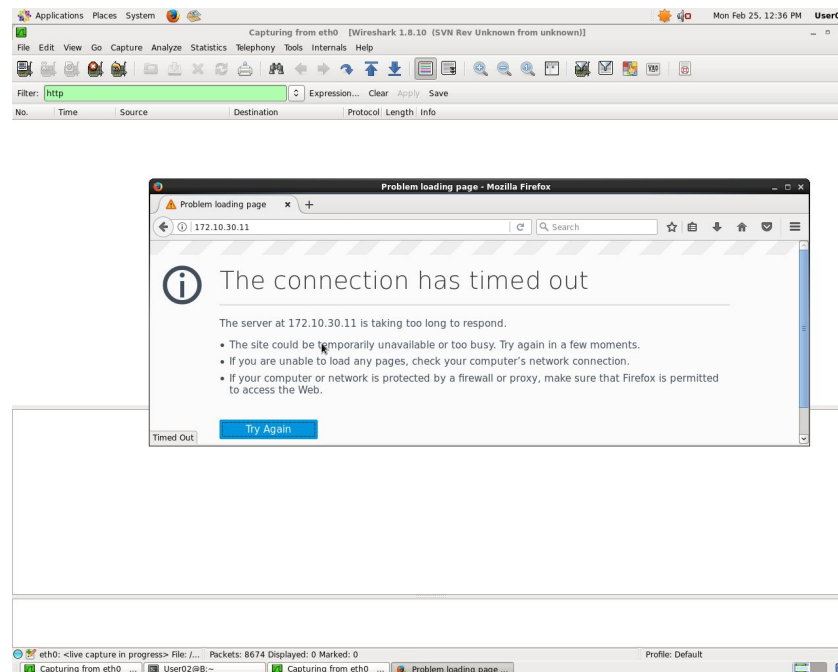
| No. | Time        | Source       | Destination  | Protocol | Length | Info                               |
|-----|-------------|--------------|--------------|----------|--------|------------------------------------|
| 10  | 8.015210326 | 172.20.50.3  | 172.20.100.4 | HTTP     | 378    | GET / HTTP/1.1                     |
| 16  | 8.016287963 | 172.20.100.4 | 172.20.50.3  | HTTP     | 2329   | HTTP/1.1 403 Forbidden (text/html) |
| 24  | 8.055819721 | 172.20.50.3  | 172.20.100.4 | HTTP     | 359    | GET /favicon.ico HTTP/1.1          |
| 26  | 8.056286188 | 172.20.100.4 | 172.20.50.3  | HTTP     | 533    | HTTP/1.1 404 Not Found (text/html) |

This screenshot is for testing web services from A.B to B.2 with Wireshark:  
Expected Result: Web service is Allowed      Actual Result: Web service is Allowed



| No. | Time        | Source       | Destination  | Protocol | Length | Info                               |
|-----|-------------|--------------|--------------|----------|--------|------------------------------------|
| 4   | 0.001565244 | 172.10.30.11 | 172.20.100.4 | HTTP     | 378    | GET / HTTP/1.1                     |
| 10  | 0.003733045 | 172.20.100.4 | 172.10.30.11 | HTTP     | 2345   | HTTP/1.1 403 Forbidden (text/html) |

This screenshot is for testing web services from B.2 to A.B with Wireshark:  
 Expected Result: Web service is Not Allowed      Actual Result: Web service is Not Allowed  
*Note: No transfer occurred, so no HTTP packets were seen in Wireshark*



**C. Show the Wireshark results (screenshots of checking the ping between computers. State if ping is allowed between computers.**

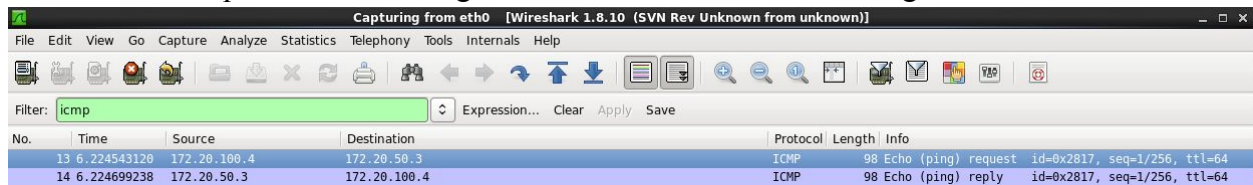
This screenshot is for testing ping from B.1 to B.2 with Wireshark:  
 Expected Result: Ping is Allowed      Actual Result: Ping is Allowed

| No. | Time         | Source       | Destination  | Protocol | Length | Info   |
|-----|--------------|--------------|--------------|----------|--------|--|
| 616 | 12.232387420 | 172.20.50.3  | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x9427, seq=1/256, ttl=64 |
| 617 | 12.232556387 | 172.20.100.4 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0x9427, seq=1/256, ttl=64   |
| 669 | 13.231548794 | 172.20.50.3  | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x9427, seq=2/512, ttl=64 |
| 670 | 13.231737079 | 172.20.100.4 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0x9427, seq=2/512, ttl=64   |
| 721 | 14.231580250 | 172.20.50.3  | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x9427, seq=3/768, ttl=64 |
| 722 | 14.231748685 | 172.20.100.4 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0x9427, seq=3/768, ttl=64   |

This screenshot is for testing ping from B.1 to A.B with Wireshark:  
 Expected Result: Ping is Allowed      Actual Result: Ping is Allowed

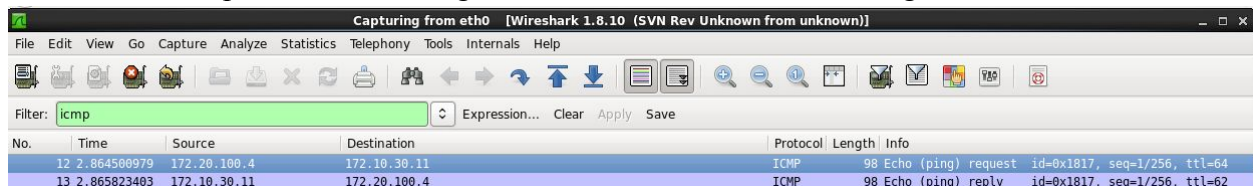
| No. | Time         | Source       | Destination  | Protocol | Length | Info   |
|-----|--------------|--------------|--------------|----------|--------|--|
| 619 | 12.148766332 | 172.20.50.3  | 172.10.30.11 | ICMP     | 98     | Echo (ping) request id=0xa527, seq=1/256, ttl=64 |
| 620 | 12.150190232 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0xa527, seq=1/256, ttl=62   |
| 672 | 13.150305823 | 172.20.50.3  | 172.10.30.11 | ICMP     | 98     | Echo (ping) request id=0xa527, seq=2/512, ttl=64 |
| 673 | 13.151380679 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0xa527, seq=2/512, ttl=62   |
| 724 | 14.151508820 | 172.20.50.3  | 172.10.30.11 | ICMP     | 98     | Echo (ping) request id=0xa527, seq=3/768, ttl=64 |
| 725 | 14.152881812 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) reply id=0xa527, seq=3/768, ttl=62   |

This screenshot is for testing ping from B.2 to B.1 with Wireshark:  
Expected Result: Ping is Allowed      Actual Result: Ping is Allowed



| No. | Time        | Source       | Destination  | Protocol | Length | Info   |
|-----|-------------|--------------|--------------|----------|--------|--|
| 13  | 6.224543128 | 172.20.100.4 | 172.20.50.3  | ICMP     | 98     | Echo (ping) request id=0x2817, seq=1/256, ttl=64 |
| 14  | 6.224699238 | 172.20.50.3  | 172.20.100.4 | ICMP     | 98     | Echo (ping) reply id=0x2817, seq=1/256, ttl=64   |

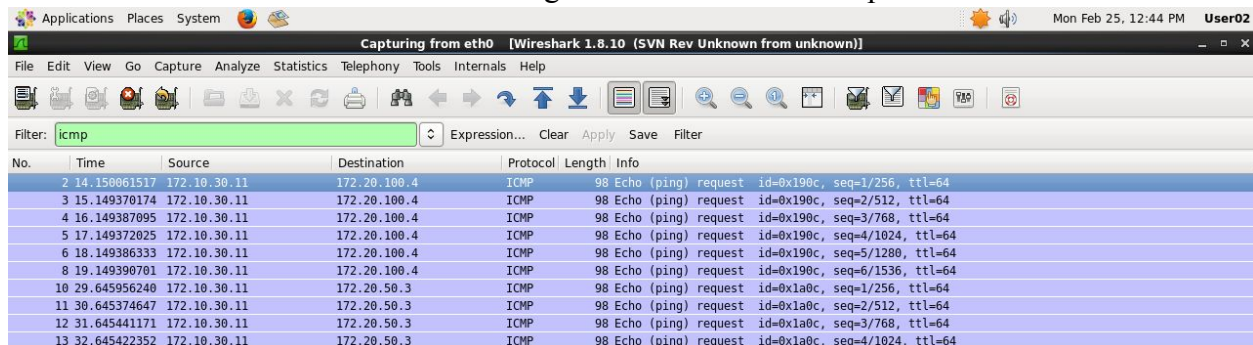
This screenshot is for testing ping from B.2 to A.B with Wireshark:  
Expected Result: Ping is Allowed      Actual Result: Ping is Allowed



| No. | Time        | Source       | Destination  | Protocol | Length | Info   |
|-----|-------------|--------------|--------------|----------|--------|--|
| 12  | 2.864508979 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x1817, seq=1/256, ttl=64 |
| 13  | 2.865923403 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) reply id=0x1817, seq=1/256, ttl=62   |

This screenshot is for testing ping from A.B to B.1 and B.2 (both captured in one screenshot) with Wireshark:

Expected Result: Ping is Not Allowed - no response  
Actual Result: Ping is Not Allowed - no response



| No. | Time         | Source       | Destination  | Protocol | Length | Info  |
|-----|--------------|--------------|--------------|----------|--------|---|
| 2   | 14.150061517 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x190c, seq=1/256, ttl=64  |
| 3   | 15.149370174 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x190c, seq=2/512, ttl=64  |
| 4   | 16.149387095 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x190c, seq=3/768, ttl=64  |
| 5   | 17.149372025 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x190c, seq=4/1024, ttl=64 |
| 6   | 18.149386333 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x190c, seq=5/1280, ttl=64 |
| 8   | 19.149390701 | 172.10.30.11 | 172.20.100.4 | ICMP     | 98     | Echo (ping) request id=0x190c, seq=6/1536, ttl=64 |
| 10  | 29.645956240 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) request id=0x1a0c, seq=1/256, ttl=64  |
| 11  | 30.645374647 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) request id=0x1a0c, seq=2/512, ttl=64  |
| 12  | 31.645441171 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) request id=0x1a0c, seq=3/768, ttl=64  |
| 13  | 32.645422352 | 172.10.30.11 | 172.20.50.3  | ICMP     | 98     | Echo (ping) request id=0x1a0c, seq=4/1024, ttl=64 |

- D. Assume the company only stores classified business data in Computer B.1 and does not allow anyone to carry a device to transfer data. Discuss whether or not the security policy can ensure that the classified data will not be disclosed to external computers through network. Be as specific as possible in your discussion. For example, if you do not think the security policy is secure, you shall show which item of the policy has problem or what policy is missing.**

According to our ACM, internal Workstation (B.1) shall have access to external computers through the internet. Therefore, the classified business data stored on workstation B.1 is not secure. Even though no data can be transferred to a carrying device within the company, and no service is provided by the Workstation, the data can be uploaded and transferred to external computers through the internet. In other words, any user of the workstation could write their classified data to the web, thereby disclosing it and breaking the company's data confidentiality.