Project 1: Firewall and Access Control

Due Date: 3/5/2019

Group 3 Members:
Alexander Muyshondt
Anna Crowsar
Cynthia Cordova
Dylan Olgin
Saud Altwayan

What to Deliver

Section I (Introduction):
Summarize what you have done in the project and clearly state the responsibility of each group member, e.g. who did which task, who wrote which part of the report, how your group was coordinated, etc.

Dylan Olgin: I worked on task 2 & 3 configuring the firewall. For task 2 i worked on removing the default firewall and running the tests to check if everything was able to have access to everything else. For task 3 I worked on implementing all the correct firewall settings for the given situation making sure it was able to pass all the given tasks. I inserted some of the screenshots and helped write a few of the tasks in section 3.

Alexander Muyshondt: As a group, we worked on Task 1 to ensure each computer had the appropriate services running and correct programs installed before the other tasks. For Task 2, I worked alongside the rest of my group to remove the default firewall policy and complete the experiments on the default security configuration. For Task 3, I worked alongside Dylan and Saud to design an Access Control Matrix that represented the security requirements of the company. Together we implemented the the ACM in the firewall protocol. I, along with my group, worked on Task 4 to test our security configuration and record the results. I wrote my portion of the introduction, typed the outline of the report, and helped to write the Task 3 portion of the report.

Saud Altwayan: For the tasks, I worked on task 2 where I ran NMap to scan all computers, and services in network C. I did a) to d) in task 2, with the help of my group. I also implemented task 3, by making an access control matrix and worked with Dylan and Alex in configuring the cisco firewall. Finally, I worked on the whole task IV with the group. For the report I did the matrix, as well as d) in task 3, and a) to c) in task 4. Screen shots were obtained by me and the rest of the group as well.

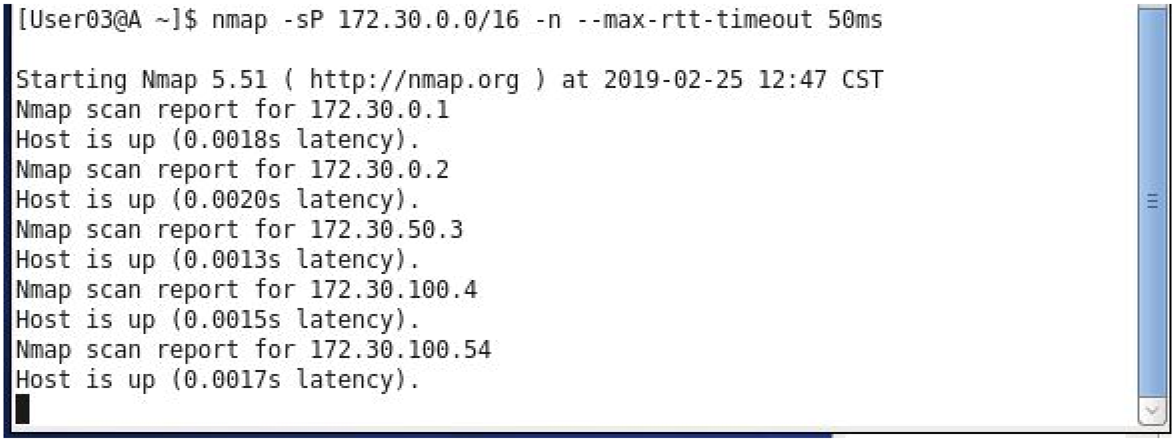
Anna Cowsar: Helped with Task 1 and getting it started. I helped with trying to figure out commands that worked by looking it up for my group members. Saud was struggling to get a command to work and I successfully helped him with that so he could get into some document to change it. Gave some advice on the iptables. I contributed to section IV part d as the second response.

Cynthia Cordova: Helped with task 1 in configuring the networks in each computer. In task 2 I helped with checking whether a computer could access another computer's web service. I also helped with some of the testing in task 4.

Section II (Task II):

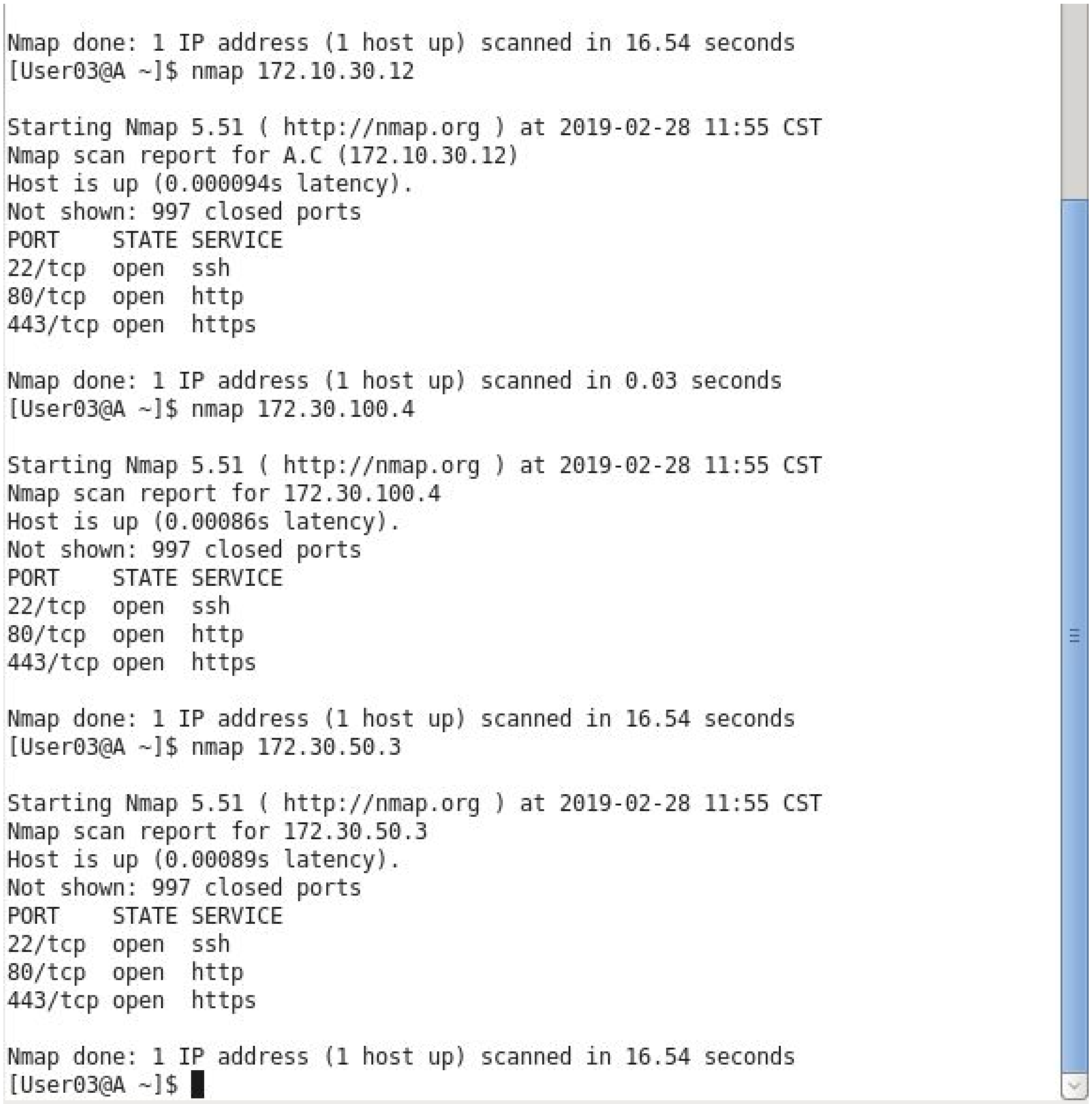
a) Show the NMap commands to scan the computers and the service ports.

(Nmap commands to scan for devices on network)



```
[User03@A ~]$ nmap -sP 172.30.0.0/16 -n --max-rtt-timeout 50ms

Starting Nmap 5.51 ( http://nmap.org ) at 2019-02-25 12:47 CST
Nmap scan report for 172.30.0.1
Host is up (0.0018s latency).
Nmap scan report for 172.30.0.2
Host is up (0.0020s latency).
Nmap scan report for 172.30.50.3
Host is up (0.0013s latency).
Nmap scan report for 172.30.100.4
Host is up (0.0015s latency).
Nmap scan report for 172.30.100.54
Host is up (0.0017s latency).
```

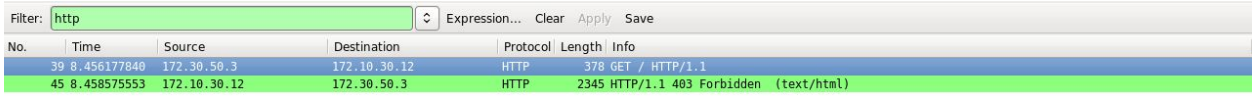
(Nmap commands to scan ports of all three computers)



```
Nmap done: 1 IP address (1 host up) scanned in 16.54 seconds
[User03@A ~]$ nmap 172.10.30.12

Starting Nmap 5.51 ( http://nmap.org ) at 2019-02-28 11:55 CST
Nmap scan report for A.C (172.10.30.12)
Host is up (0.000094s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
[User03@A ~]$ nmap 172.30.100.4

Starting Nmap 5.51 ( http://nmap.org ) at 2019-02-28 11:55 CST
Nmap scan report for 172.30.100.4
Host is up (0.00086s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 16.54 seconds
[User03@A ~]$ nmap 172.30.50.3

Starting Nmap 5.51 ( http://nmap.org ) at 2019-02-28 11:55 CST
Nmap scan report for 172.30.50.3
Host is up (0.00089s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 16.54 seconds
[User03@A ~]$ 
```

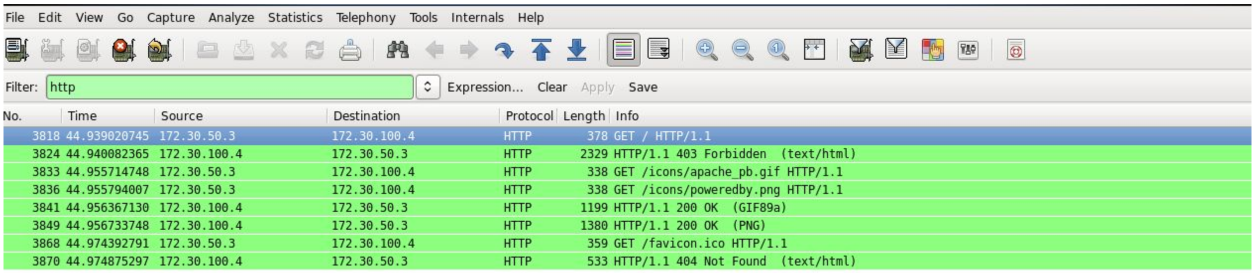
b) Show the Wireshark results (screen shots) of checking the web service between computers. State if web service is allowed between computers.

(C.1 access web service of A.C, web service is allowed)



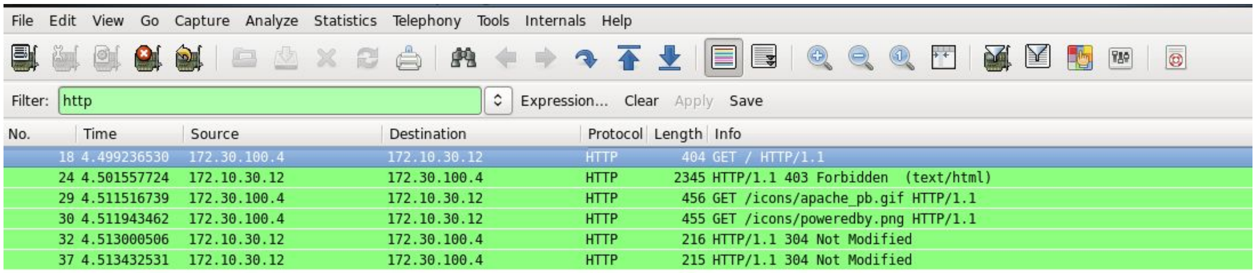
```
Filter: http

No.  Time         Source        Destination   Protocol Length Info
  39 8.456177840  172.30.50.3   172.10.30.12  HTTP      378 GET / HTTP/1.1
  45 8.458575553  172.10.30.12  172.30.50.3   HTTP     2345 HTTP/1.1 403 Forbidden  (text/html)
```

(C.1 access web service of C.2, web service is allowed)



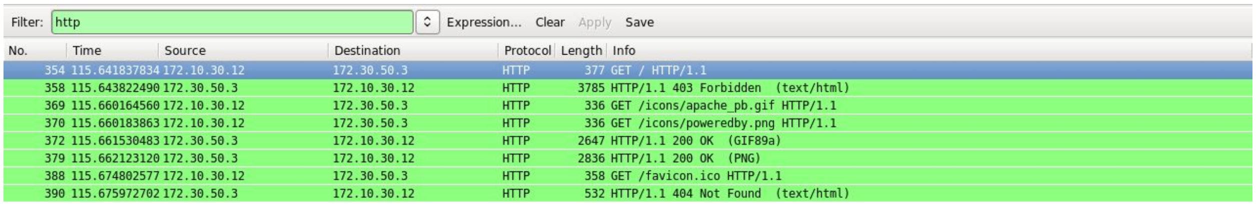
```
Filter: http

No.   Time          Source        Destination   Protocol Length Info
3818 44.939020745  172.30.50.3   172.30.100.4  HTTP      378 GET / HTTP/1.1
3824 44.940082365  172.30.100.4  172.30.50.3   HTTP     2329 HTTP/1.1 403 Forbidden  (text/html)
3833 44.955714748  172.30.50.3   172.30.100.4  HTTP      338 GET /icons/apache_pb.gif HTTP/1.1
3836 44.955794007  172.30.50.3   172.30.100.4  HTTP      338 GET /icons/poweredby.png HTTP/1.1
3841 44.956367130  172.30.100.4  172.30.50.3   HTTP     1199 HTTP/1.1 200 OK  (GIF89a)
3849 44.956733748  172.30.100.4  172.30.50.3   HTTP     1380 HTTP/1.1 200 OK  (PNG)
3868 44.974392791  172.30.50.3   172.30.100.4  HTTP      359 GET /favicon.ico HTTP/1.1
3870 44.974875297  172.30.100.4  172.30.50.3   HTTP      533 HTTP/1.1 404 Not Found  (text/html)
```

(C.2 access web of A.C, web service is allowed)



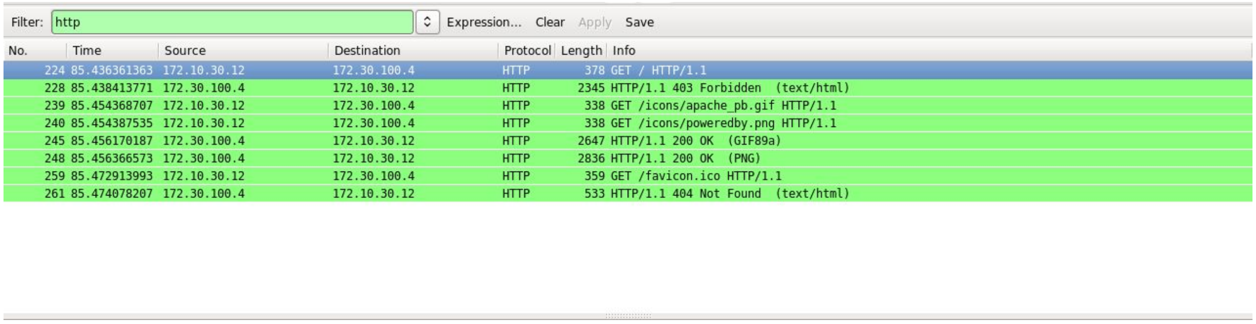
```
Filter: http

No.  Time         Source        Destination   Protocol Length Info
  18 4.499236530  172.30.100.4  172.10.30.12  HTTP      404 GET / HTTP/1.1
  24 4.501557724  172.10.30.12  172.30.100.4  HTTP     2345 HTTP/1.1 403 Forbidden  (text/html)
  29 4.511516739  172.30.100.4  172.10.30.12  HTTP      456 GET /icons/apache_pb.gif HTTP/1.1
  30 4.511943462  172.30.100.4  172.10.30.12  HTTP      455 GET /icons/poweredby.png HTTP/1.1
  32 4.513000506  172.10.30.12  172.30.100.4  HTTP      216 HTTP/1.1 304 Not Modified
  37 4.513432531  172.10.30.12  172.30.100.4  HTTP      215 HTTP/1.1 304 Not Modified
```

(A.C web access in C.1, web service is allowed)



```
Filter: http

No.  Time          Source        Destination   Protocol Length Info
 354 115.641837834 172.10.30.12  172.30.50.3   HTTP      377 GET / HTTP/1.1
 358 115.643822490 172.30.50.3   172.10.30.12  HTTP     3785 HTTP/1.1 403 Forbidden  (text/html)
 369 115.660164560 172.10.30.12  172.30.50.3   HTTP      336 GET /icons/apache_pb.gif HTTP/1.1
 370 115.660183863 172.10.30.12  172.30.50.3   HTTP      336 GET /icons/poweredby.png HTTP/1.1
 372 115.661530483 172.30.50.3   172.10.30.12  HTTP     2647 HTTP/1.1 200 OK  (GIF89a)
 379 115.662123120 172.30.50.3   172.10.30.12  HTTP     2836 HTTP/1.1 200 OK  (PNG)
 388 115.674802577 172.10.30.12  172.30.50.3   HTTP      358 GET /favicon.ico HTTP/1.1
 390 115.675972702 172.30.50.3   172.10.30.12  HTTP      532 HTTP/1.1 404 Not Found  (text/html)
```

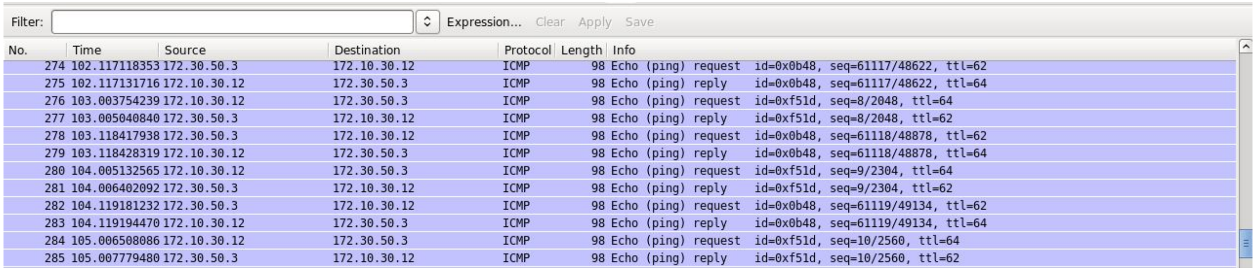
(A.C web access in C.2, web service is allowed)



```
Filter: http

No.  Time         Source        Destination   Protocol Length Info
 224 85.436361363 172.10.30.12  172.30.100.4  HTTP      378 GET / HTTP/1.1
 228 85.438413771 172.30.100.4  172.10.30.12  HTTP     2345 HTTP/1.1 403 Forbidden  (text/html)
 239 85.454368707 172.10.30.12  172.30.100.4  HTTP      338 GET /icons/apache_pb.gif HTTP/1.1
 240 85.454387535 172.10.30.12  172.30.100.4  HTTP      338 GET /icons/poweredby.png HTTP/1.1
 245 85.456170187 172.30.100.4  172.10.30.12  HTTP     2647 HTTP/1.1 200 OK  (GIF89a)
 248 85.456366573 172.30.100.4  172.10.30.12  HTTP     2836 HTTP/1.1 200 OK  (PNG)
 259 85.472913993 172.10.30.12  172.30.100.4  HTTP      359 GET /favicon.ico HTTP/1.1
 261 85.474078207 172.30.100.4  172.10.30.12  HTTP      533 HTTP/1.1 404 Not Found  (text/html)
```

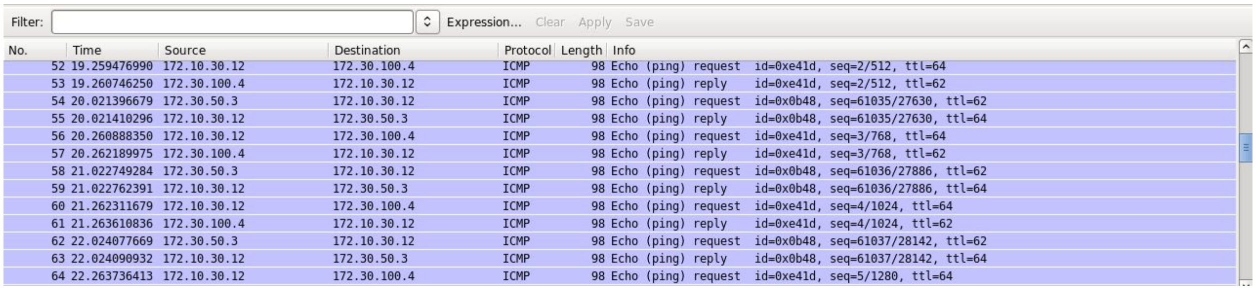
c) Show the Wireshark results (screen shots) of checking the ping between computers. State if ping is allowed between computers.

(A.C ping C.1, ping is allowed)



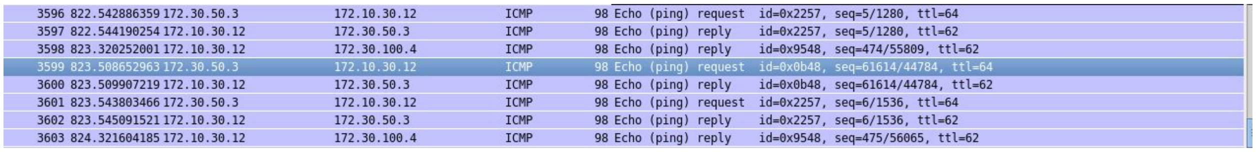
```
No.   Time           Source          Destination     Protocol Length Info
  274 102.117118353 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x0b48, seq=61117/48622, ttl=62
  275 102.117131716 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61117/48622, ttl=64
  276 103.003754239 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) request  id=0xf51d, seq=8/2048, ttl=64
  277 103.005040840 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) reply    id=0xf51d, seq=8/2048, ttl=62
  278 103.118417938 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x0b48, seq=61118/48878, ttl=62
  279 103.118428319 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61118/48878, ttl=64
  280 104.005132565 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) request  id=0xf51d, seq=9/2304, ttl=64
  281 104.006402092 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) reply    id=0xf51d, seq=9/2304, ttl=62
  282 104.119181232 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x0b48, seq=61119/49134, ttl=62
  283 104.119194470 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61119/49134, ttl=64
  284 105.006508086 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) request  id=0xf51d, seq=10/2560, ttl=64
  285 105.007779480 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) reply    id=0xf51d, seq=10/2560, ttl=62
```

(A.C ping C.2, ping is allowed)



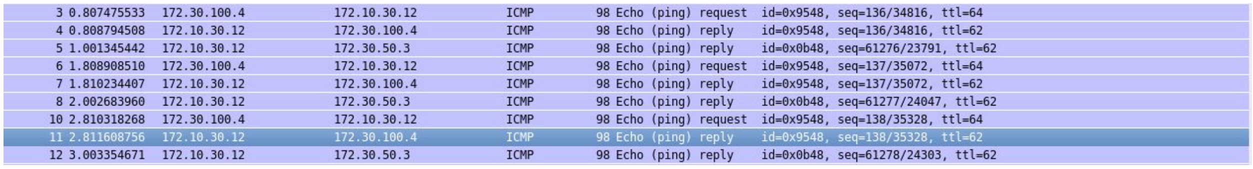
```
No.   Time           Source          Destination     Protocol Length Info
   52 19.259476990  172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) request  id=0xe41d, seq=2/512, ttl=64
   53 19.260746250  172.30.100.4    172.10.30.12    ICMP     98 Echo (ping) reply    id=0xe41d, seq=2/512, ttl=62
   54 20.021396679  172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x0b48, seq=61035/27630, ttl=62
   55 20.021410296  172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61035/27630, ttl=64
   56 20.260888350  172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) request  id=0xe41d, seq=3/768, ttl=64
   57 20.262189975  172.30.100.4    172.10.30.12    ICMP     98 Echo (ping) reply    id=0xe41d, seq=3/768, ttl=62
   58 21.022749284  172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x0b48, seq=61036/27886, ttl=62
   59 21.022762391  172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61036/27886, ttl=64
   60 21.262311679  172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) request  id=0xe41d, seq=4/1024, ttl=64
   61 21.263610836  172.30.100.4    172.10.30.12    ICMP     98 Echo (ping) reply    id=0xe41d, seq=4/1024, ttl=62
   62 22.024077669  172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x0b48, seq=61037/28142, ttl=62
   63 22.024090932  172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61037/28142, ttl=64
   64 22.263736413  172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) request  id=0xe41d, seq=5/1280, ttl=64
```

(C.1 ping A.C, ping is allowed)



```
 3596 822.542886359 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x2257, seq=5/1280, ttl=64
 3597 822.544190254 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x2257, seq=5/1280, ttl=62
 3598 823.320252001 172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) reply    id=0x9548, seq=474/55809, ttl=62
 3599 823.508652963 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x0b48, seq=61614/44784, ttl=64
 3600 823.509907219 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61614/44784, ttl=62
 3601 823.543803466 172.30.50.3     172.10.30.12    ICMP     98 Echo (ping) request  id=0x2257, seq=6/1536, ttl=64
 3602 823.545091521 172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x2257, seq=6/1536, ttl=62
 3603 824.321604185 172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) reply    id=0x9548, seq=475/56065, ttl=62
```

(C.2 ping A.C, ping is allowed)



```
    3 0.807475533   172.30.100.4    172.10.30.12    ICMP     98 Echo (ping) request  id=0x9548, seq=136/34816, ttl=64
    4 0.808794508   172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) reply    id=0x9548, seq=136/34816, ttl=62
    5 1.001345442   172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61276/23791, ttl=62
    6 1.808908510   172.30.100.4    172.10.30.12    ICMP     98 Echo (ping) request  id=0x9548, seq=137/35072, ttl=64
    7 1.810234407   172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) reply    id=0x9548, seq=137/35072, ttl=62
    8 2.002683960   172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61277/24047, ttl=62
   10 2.810318268   172.30.100.4    172.10.30.12    ICMP     98 Echo (ping) request  id=0x9548, seq=138/35328, ttl=64
   11 2.811608756   172.10.30.12    172.30.100.4    ICMP     98 Echo (ping) reply    id=0x9548, seq=138/35328, ttl=62
   12 3.003354671   172.10.30.12    172.30.50.3     ICMP     98 Echo (ping) reply    id=0x0b48, seq=61278/24303, ttl=62
```

d) Summarize the default Cisco firewall policy.

With the default Cisco firewall policy in place, the computers on the internal network (C.1 and C.2) are able to access each others web services and that of the external network (A.C). In addition, both computers on the internal network were able to ping each other and the external network computer. On the other hand, the computer on the external network is unable to ping or access web services of either of the computers on the internal network.

Section III (Task III):

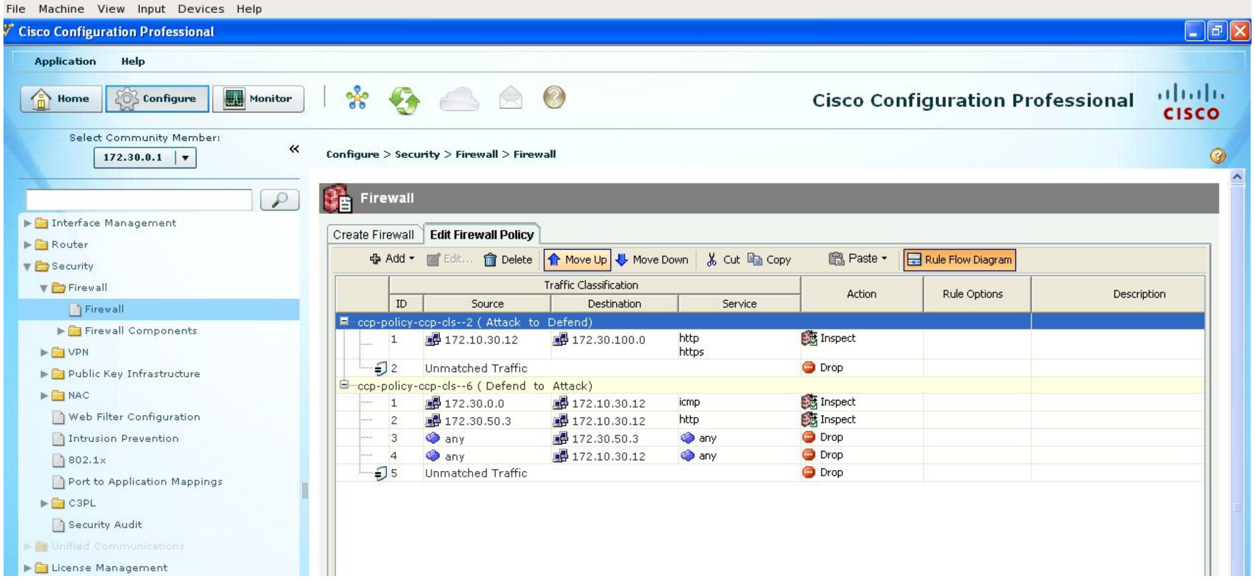
a) Copy and paste the access control matrix.

	Internal Server	Internal WorkStation	External Computer
Internal Server	ping	ping	ping
Internal WorkStation	Web, SSH, ping	ping	Web , ping
External Computer	Web	N/A	N/A

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.

Any policies that need to be implemented between the internal server and the internal workstations cannot be enforced by the Cisco firewall. Cisco requires an interface to be linked to each new zone that is created. Since the internal server and workstations are both working on the VLan, they must be placed in the same zone. The result is that any firewall policies can only be configured between the internal(VLan) and the external(FastEthernet) zones, which does not allow us to place any rules inside the internal network.

c) Copy and paste a screenshot of your Cisco firewall configuration.



Configure > Security > Firewall > Firewall

	Traffic Classification				Action	Rule Options	Description
	ID	Source	Destination	Service			
ccp-policy-ccp-cls--2 (Attack to Defend)							
	1	172.10.30.12	172.30.100.0	http https	Inspect		
	2	Unmatched Traffic			Drop		
ccp-policy-ccp-cls--6 (Defend to Attack)							
	1	172.30.0.0	172.10.30.12	icmp	Inspect		
	2	172.30.50.3	172.10.30.12	http	Inspect		
	3	any	172.30.50.3	any	Drop		
	4	any	172.10.30.12	any	Drop		
	5	Unmatched Traffic			Drop		

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

We use iptables between the internal workstation and internal servers, since any cisco firewall policy on the router cannot be enforced locally. Therefore we have to use iptables.

- With the internal workstation, other computers need to be blocked from using its web and SSH services.
- With the internal server, other internal servers need to be blocked from using its web and SSH services.

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

```
iptables -A OUTPUT -o eth0 -p tcp -s 172.30.0.0/16 --dport 22, 80 -m state --state NEW,ESTABLISHED -j DROP
```

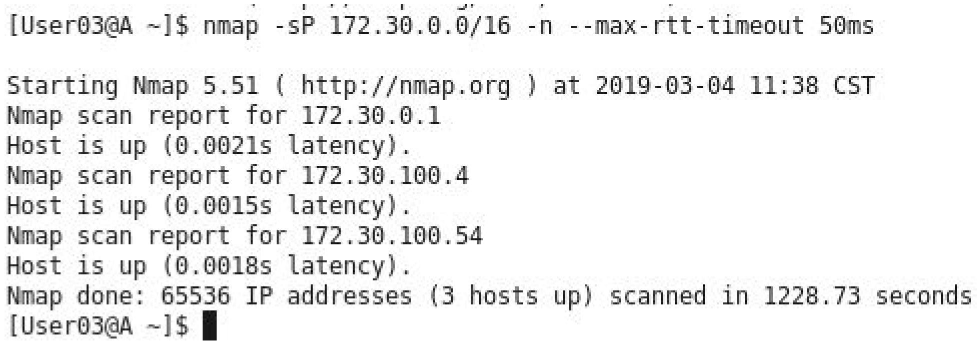
This command blocks the access of web and SSH services from the internal server to the other internal workstations (and internal servers).

Section IV (Task IV):

For the results, do not enable iptables. Only show the results with configured Cisco firewall.

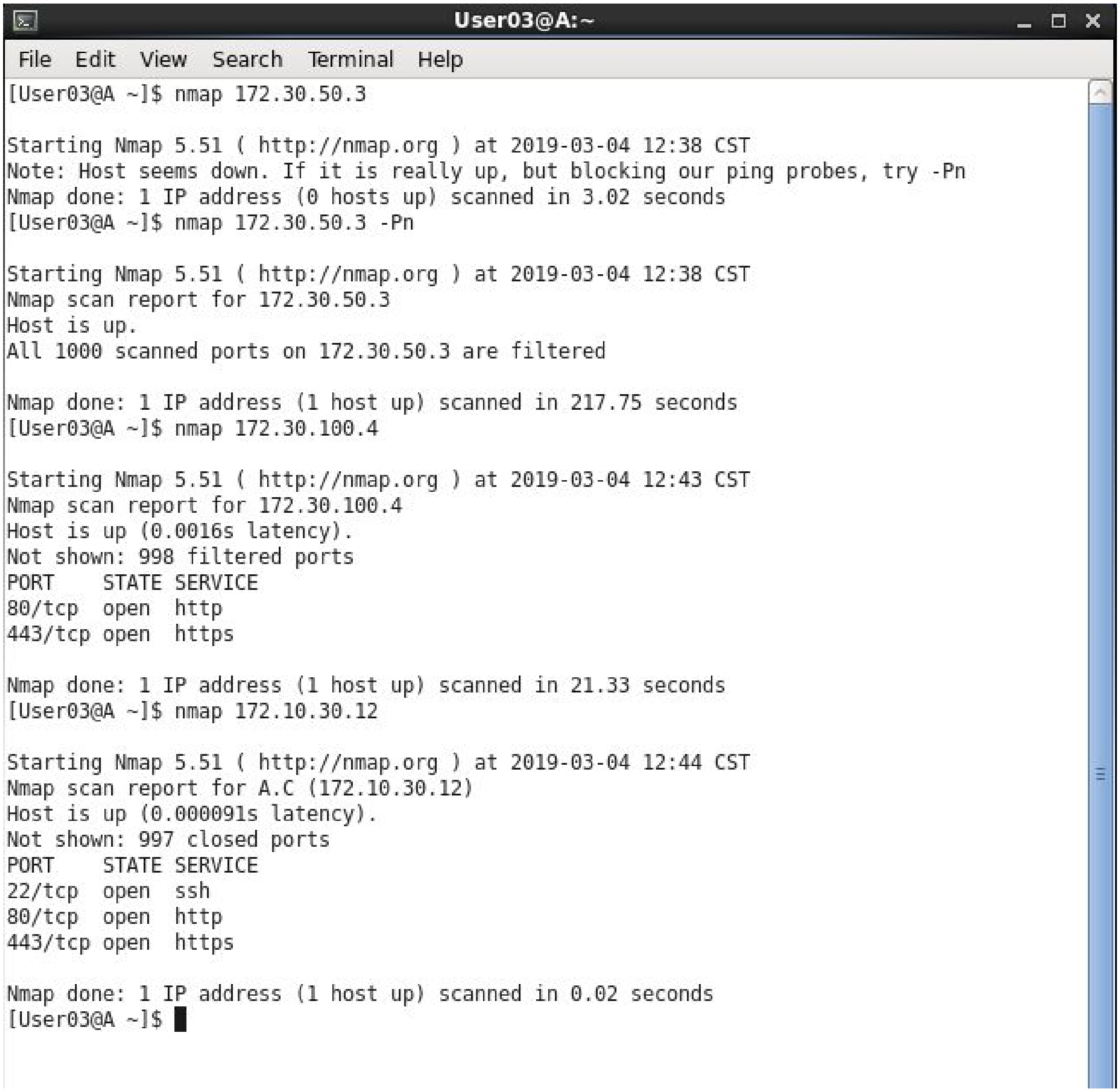
a) Show the NMap results (screen shots) of the exposed computers and ports.

(NMap scan of computer A.C)



```
[User03@A ~]$ nmap -sP 172.30.0.0/16 -n --max-rtt-timeout 50ms

Starting Nmap 5.51 ( http://nmap.org ) at 2019-03-04 11:38 CST
Nmap scan report for 172.30.0.1
Host is up (0.0021s latency).
Nmap scan report for 172.30.100.4
Host is up (0.0015s latency).
Nmap scan report for 172.30.100.54
Host is up (0.0018s latency).
Nmap done: 65536 IP addresses (3 hosts up) scanned in 1228.73 seconds
[User03@A ~]$ 
```

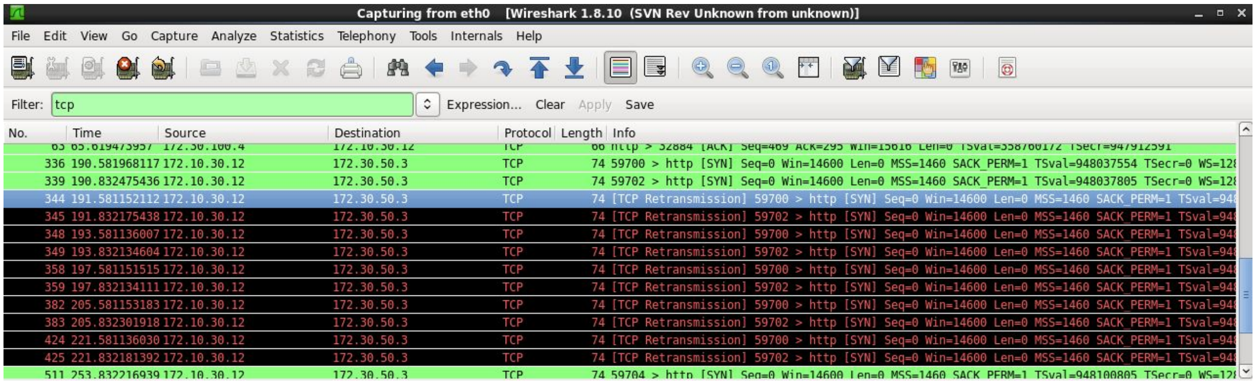
(NMap scan of the exposed ports)



```
[User03@A ~]$ nmap 172.30.50.3

Starting Nmap 5.51 ( http://nmap.org ) at 2019-03-04 12:38 CST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
[User03@A ~]$ nmap 172.30.50.3 -Pn

Starting Nmap 5.51 ( http://nmap.org ) at 2019-03-04 12:38 CST
Nmap scan report for 172.30.50.3
Host is up.
All 1000 scanned ports on 172.30.50.3 are filtered

Nmap done: 1 IP address (1 host up) scanned in 217.75 seconds
[User03@A ~]$ nmap 172.30.100.4

Starting Nmap 5.51 ( http://nmap.org ) at 2019-03-04 12:43 CST
Nmap scan report for 172.30.100.4
Host is up (0.0016s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 21.33 seconds
[User03@A ~]$ nmap 172.10.30.12

Starting Nmap 5.51 ( http://nmap.org ) at 2019-03-04 12:44 CST
Nmap scan report for A.C (172.10.30.12)
Host is up (0.000091s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
[User03@A ~]$
```

b) Show the Wireshark results (screen shots) of checking the web service between computers. State if web service is allowed between computers.

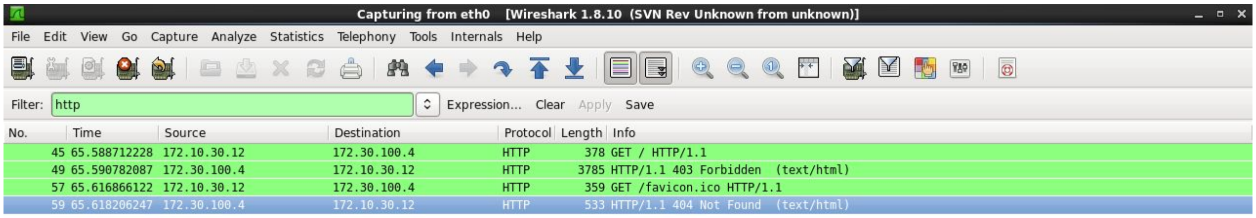
(A.C cannot access web services of C.1)


Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp

```
No.   Time          Source         Destination    Protocol Length Info
   63 65.619473957  172.30.100.4   172.10.30.12   TCP      66 http > 32884 [ACK] Seq=469 Ack=295 Win=15616 Len=0 TSval=358760172 TSecr=947912591
  336 190.581968117 172.10.30.12   172.30.50.3    TCP      74 59700 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948037554 TSecr=0 WS=128
  339 190.832475436 172.10.30.12   172.30.50.3    TCP      74 59702 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948037805 TSecr=0 WS=128
  344 191.581152112 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59700 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  345 191.832175438 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59702 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  348 193.581136007 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59700 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  349 193.832134604 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59702 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  358 197.581151515 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59700 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  359 197.832134111 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59702 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  382 205.581153183 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59700 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  383 205.832301918 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59702 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  424 221.581136030 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59700 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  425 221.832181392 172.10.30.12   172.30.50.3    TCP      74 [TCP Retransmission] 59702 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948
  511 253.832216939 172.10.30.12   172.30.50.3    TCP      74 59704 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=948100805 TSecr=0 WS=128
```

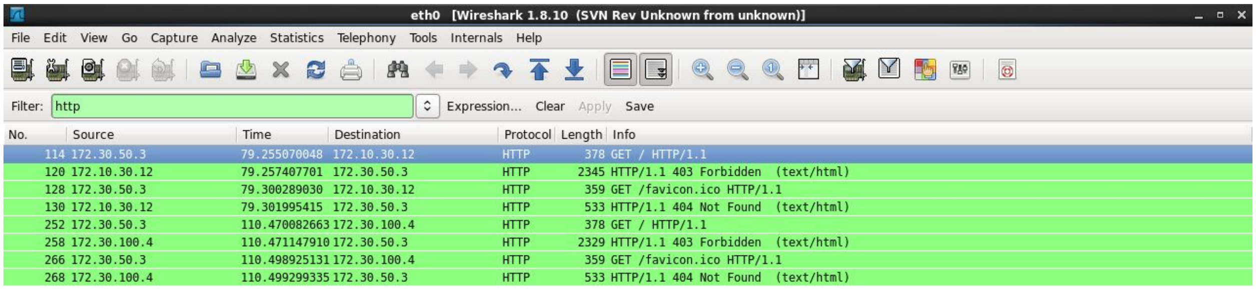
(A.C can access web services of C.2)


Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http

```
No.   Time          Source         Destination    Protocol Length Info
   45 65.588712228  172.10.30.12   172.30.100.4   HTTP      378 GET / HTTP/1.1
   49 65.590782087  172.30.100.4   172.10.30.12   HTTP     3785 HTTP/1.1 403 Forbidden  (text/html)
   57 65.616866122  172.10.30.12   172.30.100.4   HTTP      359 GET /favicon.ico HTTP/1.1
   59 65.618206247  172.30.100.4   172.10.30.12   HTTP      533 HTTP/1.1 404 Not Found  (text/html)
```

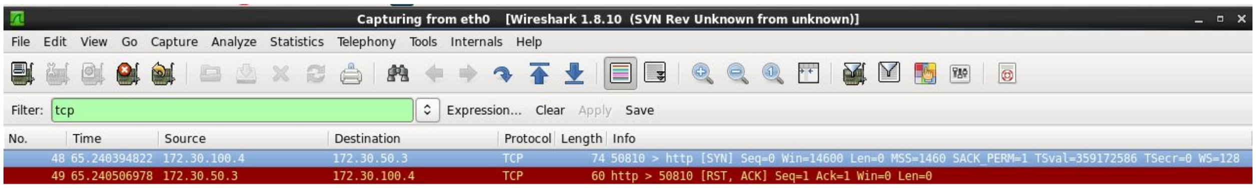
(C.1 can access web services of A.C and C.2)


eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http

```
No.   Source         Time          Destination    Protocol Length Info
  114 172.30.50.3    79.255070048  172.10.30.12   HTTP      378 GET / HTTP/1.1
  120 172.10.30.12   79.257407701  172.30.50.3    HTTP     2345 HTTP/1.1 403 Forbidden  (text/html)
  128 172.30.50.3    79.300289030  172.10.30.12   HTTP      359 GET /favicon.ico HTTP/1.1
  130 172.10.30.12   79.301995415  172.30.50.3    HTTP      533 HTTP/1.1 404 Not Found  (text/html)
  252 172.30.50.3    110.470082663 172.30.100.4   HTTP      378 GET / HTTP/1.1
  258 172.30.100.4   110.471147910 172.30.50.3    HTTP     2329 HTTP/1.1 403 Forbidden  (text/html)
  266 172.30.50.3    110.498925131 172.30.100.4   HTTP      359 GET /favicon.ico HTTP/1.1
  268 172.30.100.4   110.499299335 172.30.50.3    HTTP      533 HTTP/1.1 404 Not Found  (text/html)
```

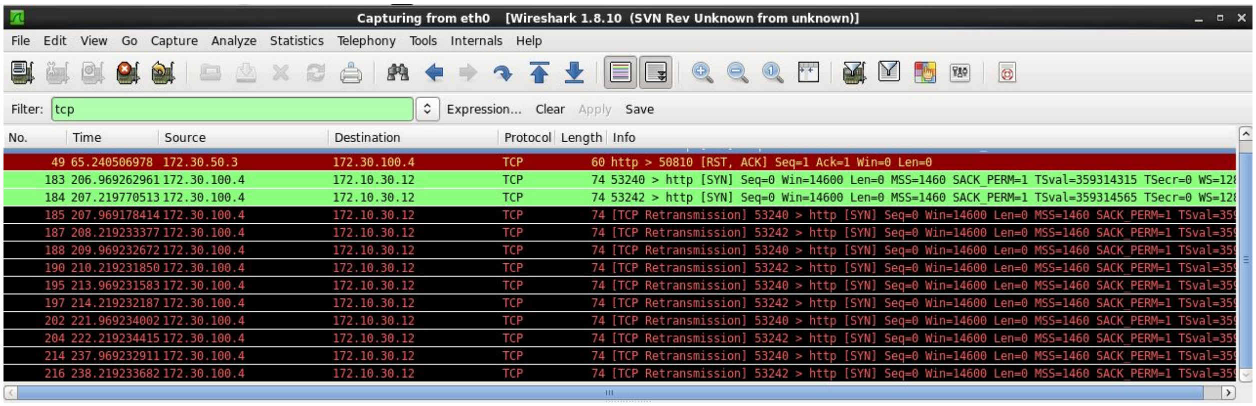
(C.2 cannot access web services of C.1)


Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp

```
No.   Time          Source         Destination    Protocol Length Info
   48 65.240394822  172.30.100.4   172.30.50.3    TCP      74 50810 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=359172586 TSecr=0 WS=128
   49 65.240506978  172.30.50.3    172.30.100.4   TCP      60 http > 50810 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

(C.2 cannot access web services of A.C)

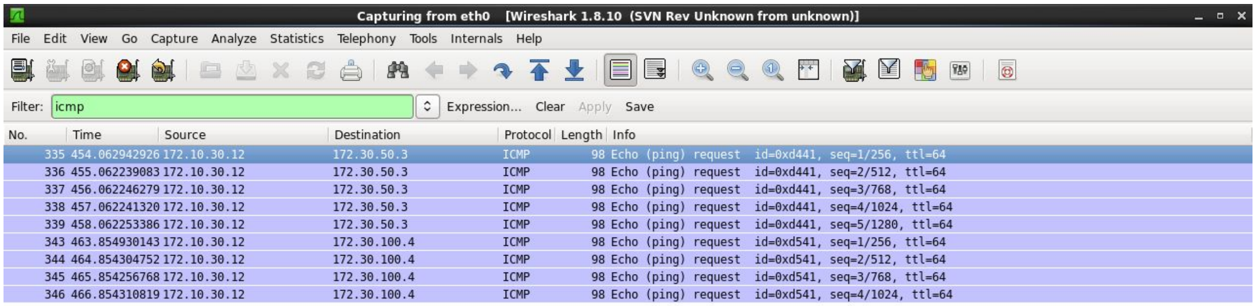

Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp

```
No.   Time          Source          Destination      Protocol Length Info
   49 65.240506978  172.30.50.3     172.30.100.4     TCP      60 http > 50810 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  183 206.969262961 172.30.100.4    172.10.30.12     TCP      74 53240 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=359314315 TSecr=0 WS=128
  184 207.219770513 172.30.100.4    172.10.30.12     TCP      74 53242 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=359314565 TSecr=0 WS=128
  185 207.969178414 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53240 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  187 208.219233377 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53242 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  188 209.969232672 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53240 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  190 210.219231850 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53242 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  195 213.969231583 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53240 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  197 214.219232187 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53242 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  202 221.969234002 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53240 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  204 222.219234415 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53242 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  214 237.969232911 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53240 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
  216 238.219233682 172.30.100.4    172.10.30.12     TCP      74 [TCP Retransmission] 53242 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=35
```

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

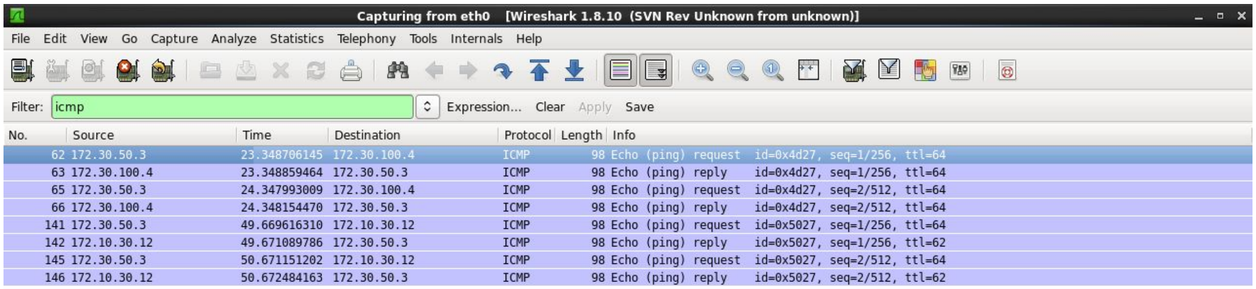
(A.C cannot ping C.1 or C.2)


Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

```
No.   Time          Source          Destination      Protocol Length Info
  335 454.062942926 172.10.30.12    172.30.50.3      ICMP     98 Echo (ping) request  id=0xd441, seq=1/256, ttl=64
  336 455.062239083 172.10.30.12    172.30.50.3      ICMP     98 Echo (ping) request  id=0xd441, seq=2/512, ttl=64
  337 456.062246279 172.10.30.12    172.30.50.3      ICMP     98 Echo (ping) request  id=0xd441, seq=3/768, ttl=64
  338 457.062241320 172.10.30.12    172.30.50.3      ICMP     98 Echo (ping) request  id=0xd441, seq=4/1024, ttl=64
  339 458.062253386 172.10.30.12    172.30.50.3      ICMP     98 Echo (ping) request  id=0xd441, seq=5/1280, ttl=64
  343 463.854930143 172.10.30.12    172.30.100.4     ICMP     98 Echo (ping) request  id=0xd541, seq=1/256, ttl=64
  344 464.854304752 172.10.30.12    172.30.100.4     ICMP     98 Echo (ping) request  id=0xd541, seq=2/512, ttl=64
  345 465.854256768 172.10.30.12    172.30.100.4     ICMP     98 Echo (ping) request  id=0xd541, seq=3/768, ttl=64
  346 466.854310819 172.10.30.12    172.30.100.4     ICMP     98 Echo (ping) request  id=0xd541, seq=4/1024, ttl=64
```

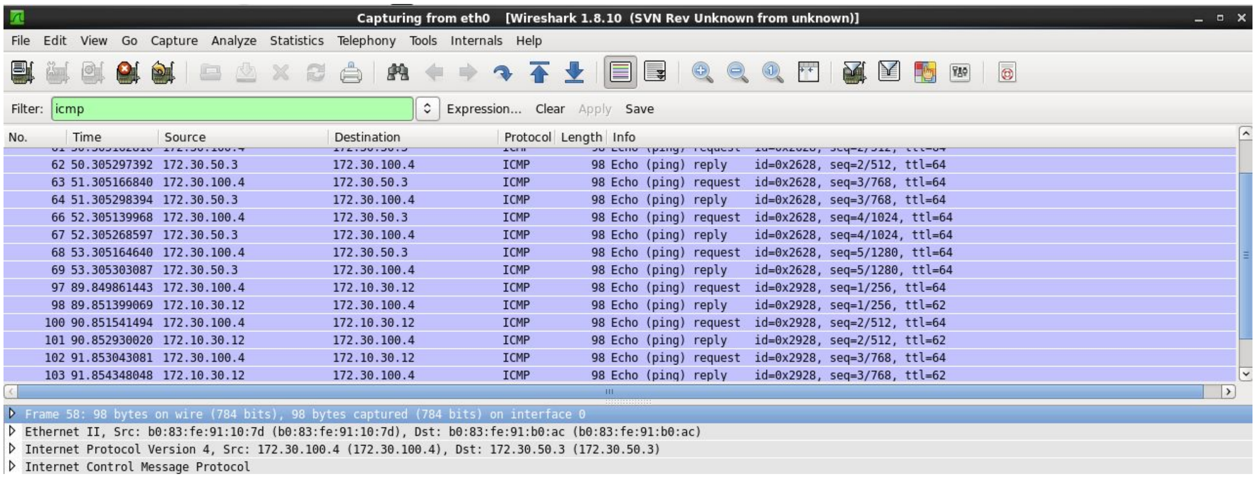
(C.1 can ping C.2 and A.C)


Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

```
No.   Source         Time          Destination      Protocol Length Info
   62 172.30.50.3    23.348706145  172.30.100.4     ICMP     98 Echo (ping) request  id=0x4d27, seq=1/256, ttl=64
   63 172.30.100.4   23.348859464  172.30.50.3      ICMP     98 Echo (ping) reply    id=0x4d27, seq=1/256, ttl=64
   65 172.30.50.3    24.347993009  172.30.100.4     ICMP     98 Echo (ping) request  id=0x4d27, seq=2/512, ttl=64
   66 172.30.100.4   24.348154470  172.30.50.3      ICMP     98 Echo (ping) reply    id=0x4d27, seq=2/512, ttl=64
  141 172.30.50.3    49.669616310  172.10.30.12     ICMP     98 Echo (ping) request  id=0x5027, seq=1/256, ttl=64
  142 172.10.30.12   49.671089786  172.30.50.3      ICMP     98 Echo (ping) reply    id=0x5027, seq=1/256, ttl=62
  145 172.30.50.3    50.671151202  172.10.30.12     ICMP     98 Echo (ping) request  id=0x5027, seq=2/512, ttl=64
  146 172.10.30.12   50.672484163  172.30.50.3      ICMP     98 Echo (ping) reply    id=0x5027, seq=2/512, ttl=62
```

(C.2 can ping C.1 and A.C)


Capturing from eth0 [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: icmp

```
No.   Time          Source          Destination     Protocol Length Info
   62 50.305297392 172.30.50.3     172.30.100.4     ICMP       98 Echo (ping) reply    id=0x2628, seq=2/512, ttl=64
   63 51.305166840 172.30.100.4    172.30.50.3      ICMP       98 Echo (ping) request  id=0x2628, seq=3/768, ttl=64
   64 51.305298394 172.30.50.3     172.30.100.4     ICMP       98 Echo (ping) reply    id=0x2628, seq=3/768, ttl=64
   66 52.305139968 172.30.100.4    172.30.50.3      ICMP       98 Echo (ping) request  id=0x2628, seq=4/1024, ttl=64
   67 52.305268597 172.30.50.3     172.30.100.4     ICMP       98 Echo (ping) reply    id=0x2628, seq=4/1024, ttl=64
   68 53.305164640 172.30.100.4    172.30.50.3      ICMP       98 Echo (ping) request  id=0x2628, seq=5/1280, ttl=64
   69 53.305303087 172.30.50.3     172.30.100.4     ICMP       98 Echo (ping) reply    id=0x2628, seq=5/1280, ttl=64
   97 89.849861443 172.30.100.4    172.10.30.12     ICMP       98 Echo (ping) request  id=0x2928, seq=1/256, ttl=64
   98 89.851399069 172.10.30.12    172.30.100.4     ICMP       98 Echo (ping) reply    id=0x2928, seq=1/256, ttl=62
  100 90.851541494 172.30.100.4    172.10.30.12     ICMP       98 Echo (ping) request  id=0x2928, seq=2/512, ttl=64
  101 90.852930020 172.10.30.12    172.30.100.4     ICMP       98 Echo (ping) reply    id=0x2928, seq=2/512, ttl=62
  102 91.853043081 172.30.100.4    172.10.30.12     ICMP       98 Echo (ping) request  id=0x2928, seq=3/768, ttl=64
  103 91.854348048 172.10.30.12    172.30.100.4     ICMP       98 Echo (ping) reply    id=0x2928, seq=3/768, ttl=62

▷ Frame 58: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▷ Ethernet II, Src: b0:83:fe:91:10:7d (b0:83:fe:91:10:7d), Dst: b0:83:fe:91:b0:ac (b0:83:fe:91:b0:ac)
▷ Internet Protocol Version 4, Src: 172.30.100.4 (172.30.100.4), Dst: 172.30.50.3 (172.30.50.3)
▷ Internet Control Message Protocol
```

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.

The outlined security policy cannot ensure that the classified business data will not be available to the external computers through the network. The fact that the internal server provides web services to the external computers, creates a vulnerability in the internal network. The current policy is only concerned with the transport layer. To better protect the data, the policy should also look at the packets in the application layer.

It is a flawed policy because if that is the only one, that is assuming that the data is secured by that computer and the ones that may have allowed access. Someone can find something in the system and exploit that to extract information or for example plant a virus for someone on Computer B to open and then become vulnerable to having access to secret information.