Project 1

CS 4371 COMPUTER SYSTEMS SECURITY

Mack Scott | Blake Burns | Christian Coulter | Muhammed Rasheed | Cody Neal
GROUP 1

Section I

Introduction

i. Summary

In this project, we used network and security devices and tools to set up and configure networking systems, implement security policy as well as analyze and verify the security of these systems. We used tools such as Wireshark, Nmap, VirtualBox and the Cisco Configuration Professional tool to complete these tasks.

ii. Task Assignments

For task one, our group had to make sure that the network was set up correctly. First we had to make sure that external computer, workstation and server were all connected properly. We continued to check and make sure that both the web services and ssh services were started on the proper computers as well as checking that the firewalls in all of the computers were stopped. We also made sure that Wireshark and NMap were installed on the correct computers.

For task two we set the default Cisco firewall policy and do some exploit testing to check the default security configuration of the firewall. First we used the Cisco Configuration Professional too configure the firewall in router be where we removed all of the removable firewall policy in the firewall. We also ran NMap in our external computer to scan all computers and services running in Network B.

For task three, we had to implement a specific security policy described in the project one pdf. We used the Cisco Configuration Professional to implement the list of policies into the internal workstation and internal server. We also made an ACM (Access Control Matrix) to represent the security policy. Using the ACM that we constructed, we configured the Cisco Firewall to enforce the security policy.

For task four, we tested the implementation of the security policy that we set up during task three. We designed tests to verify that the firewall configuration could enforce our security policy. We ran NMap in our external computed to find all services and IPs of the internal network were currently exposed to the external network.

iii. Team Evaluation

Each week, our group met at our designated lab time to work on completing the project. Throughout each week, a team member was responsible for a specific task, while the rest of the team was present to help to see that each task was completed. Blake Burns was in charge of task one which was setting up the networks. All members of the team were present to make sure that the network was set up properly. Mack Scott was responsible for task two which was setting up the default Cisco Firewall policy and exploit testing. The rest of the team was present to help Mack set up the firewall and come up with experiments to check the configuration of the firewall. Christian Coulter was in charge of task three which was implementing the security policy. The rest of the team was there to make sure that the Cisco policy was implemented correctly. Muhammed Rasheed and Cody Neal were responsible for task 4, which was testing the implementation of the firewall policy. The rest of the team was there to help test the firewall.

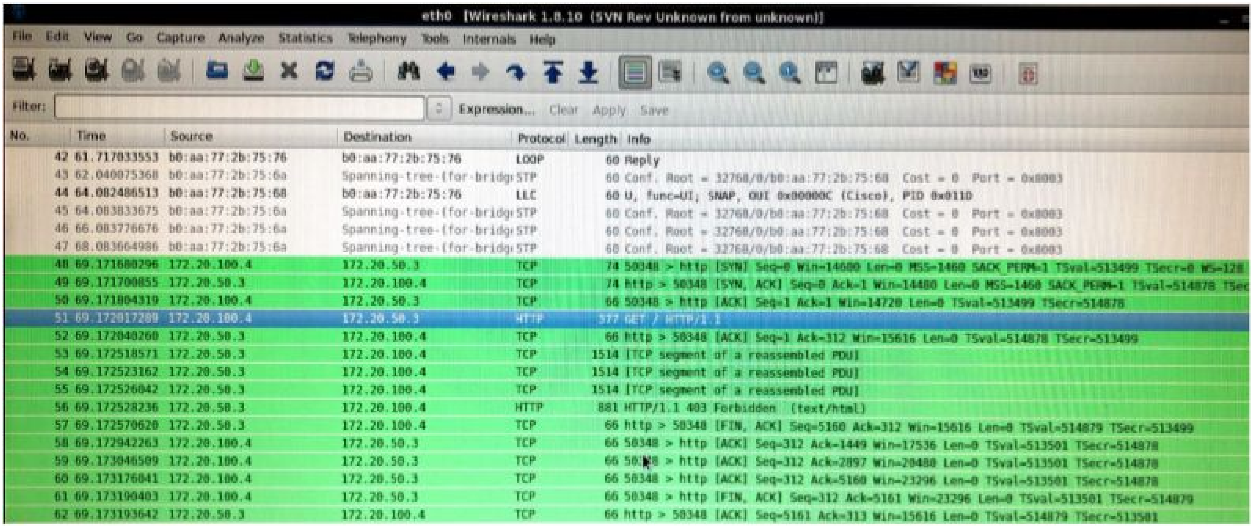
Throughout project one, our team worked great together. Our schedules worked well together and we were able to partission up the work rather well. All members of the team helped with and were able to learn from each task. The only problem we ran into while working on the project, Wireshark had been deleted off of our external computer, but luckily we were on our last task. However, we were able to work around that issue and complete the remaining task.

Who Wrote What: Blake Burns (Introduction), Mack Scott (Task Two), Christian Coulter (Task Three), Muhammed Rasheed (Task Four), Cody Neal (Task 4).

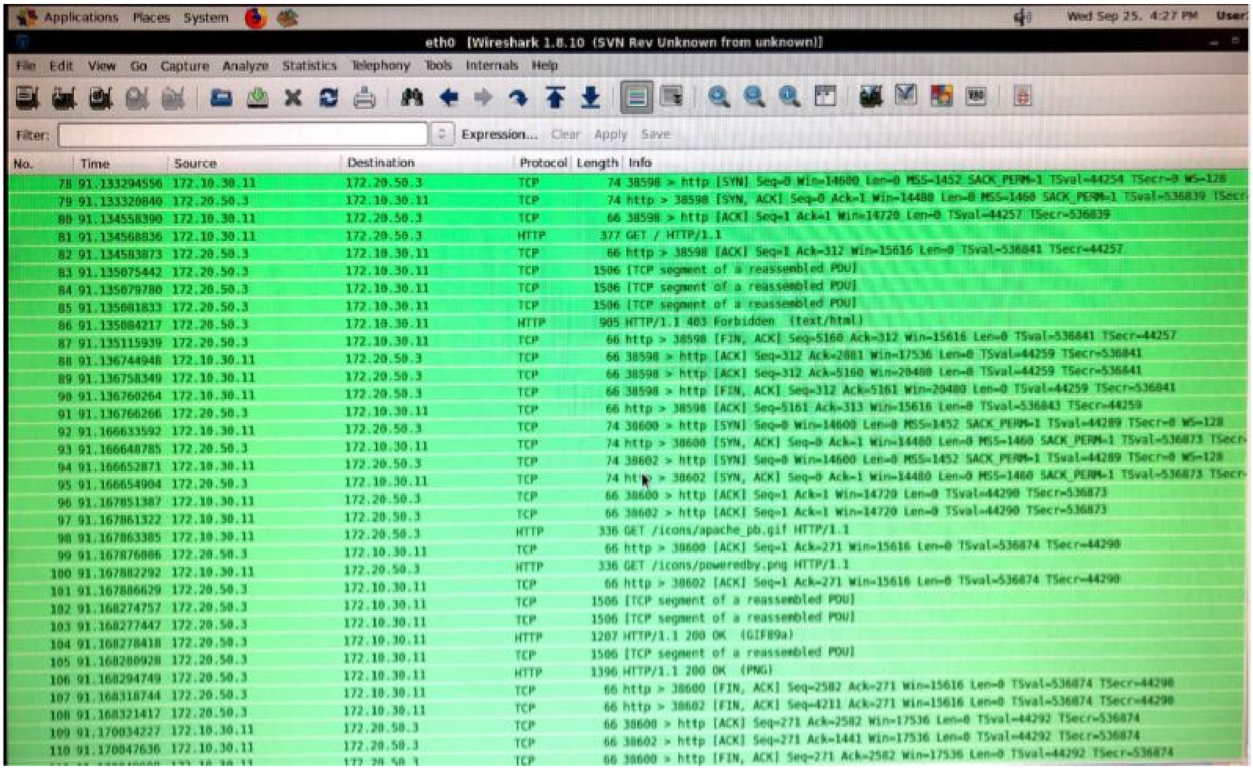
Section II

Task II

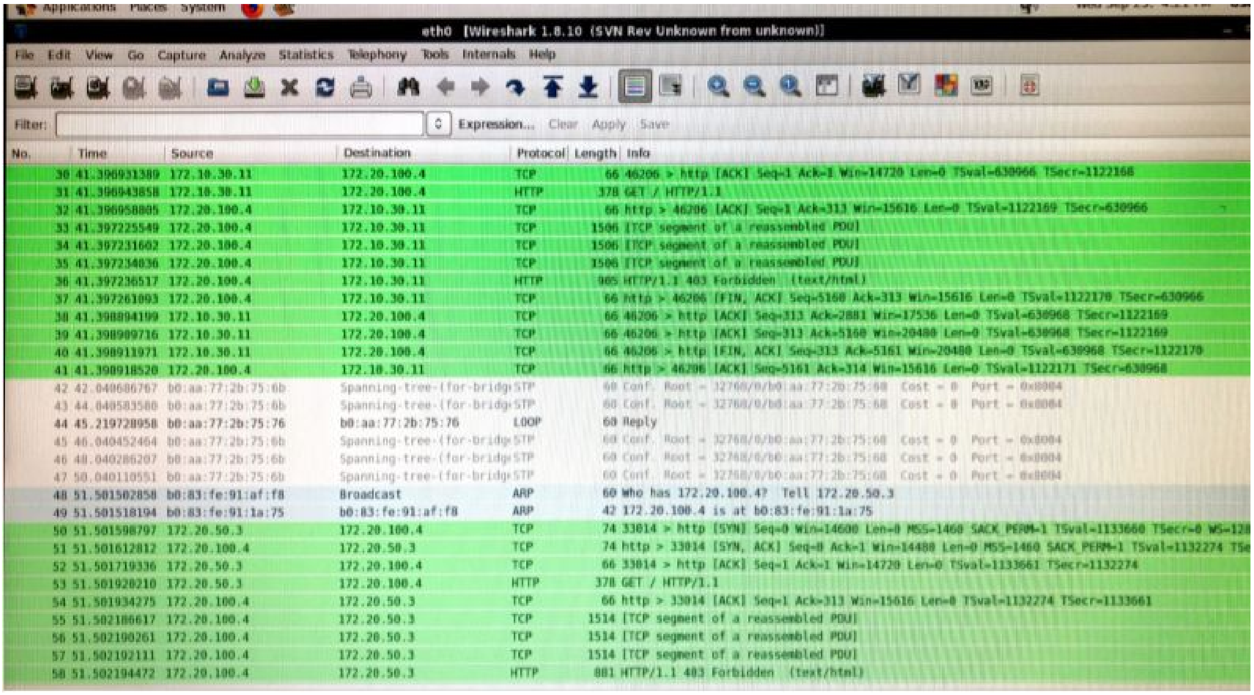
i. Show the NMap commands to scan the computers and the service ports.
   a. Nmap -T4 -A -v 170.20.0.1/16
ii. Show the Wireshark results (screen shots) of checking the web service between computers. State if web service is allowed between computers.
   a. Web services are allowed between all internal and external computers as shown in the wireshark simulation.


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

```
No.  Time         Source             Destination             Protocol Length Info
 42 61.717033553 b0:aa:77:2b:75:76  b0:aa:77:2b:75:76       LOOP       60 Reply
 43 62.040075368 b0:aa:77:2b:75:6a  Spanning-tree-(for-bridg STP       60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
 44 64.082486513 b0:aa:77:2b:75:68  b0:aa:77:2b:75:76       LLC        60 U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x011D
 45 64.083833675 b0:aa:77:2b:75:6a  Spanning-tree-(for-bridg STP       60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
 46 66.083776676 b0:aa:77:2b:75:6a  Spanning-tree-(for-bridg STP       60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
 47 68.083664986 b0:aa:77:2b:75:6a  Spanning-tree-(for-bridg STP       60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
 48 69.171680296 172.20.100.4       172.20.50.3             TCP        74 50348 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=513499 TSecr=0 WS=128
 49 69.171700855 172.20.50.3        172.20.100.4            TCP        74 http > 50348 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=514878 TSec
 50 69.171804319 172.20.100.4       172.20.50.3             TCP        66 50348 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=513499 TSecr=514878
 51 69.172017289 172.20.100.4       172.20.50.3             HTTP      377 GET / HTTP/1.1
 52 69.172040260 172.20.50.3        172.20.100.4            TCP        66 http > 50348 [ACK] Seq=1 Ack=312 Win=15616 Len=0 TSval=514878 TSecr=513499
 53 69.172518571 172.20.50.3        172.20.100.4            TCP      1514 [TCP segment of a reassembled PDU]
 54 69.172523162 172.20.50.3        172.20.100.4            TCP      1514 [TCP segment of a reassembled PDU]
 55 69.172526042 172.20.50.3        172.20.100.4            TCP      1514 [TCP segment of a reassembled PDU]
 56 69.172528236 172.20.50.3        172.20.100.4            HTTP      881 HTTP/1.1 403 Forbidden  (text/html)
 57 69.172570620 172.20.50.3        172.20.100.4            TCP        66 http > 50348 [FIN, ACK] Seq=5160 Ack=312 Win=15616 Len=0 TSval=514879 TSecr=513499
 58 69.172942263 172.20.100.4       172.20.50.3             TCP        66 50348 > http [ACK] Seq=312 Ack=1449 Win=17536 Len=0 TSval=513501 TSecr=514878
 59 69.173046509 172.20.100.4       172.20.50.3             TCP        66 50348 > http [ACK] Seq=312 Ack=2897 Win=20480 Len=0 TSval=513501 TSecr=514878
 60 69.173176041 172.20.100.4       172.20.50.3             TCP        66 50348 > http [ACK] Seq=312 Ack=5160 Win=23296 Len=0 TSval=513501 TSecr=514878
 61 69.173190403 172.20.100.4       172.20.50.3             TCP        66 50348 > http [FIN, ACK] Seq=312 Ack=5161 Win=23296 Len=0 TSval=513501 TSecr=514879
 62 69.173193642 172.20.50.3        172.20.100.4            TCP        66 http > 50348 [ACK] Seq=5161 Ack=313 Win=15616 Len=0 TSval=514879 TSecr=513501
```


Applications Places System
Wed Sep 25, 4:27 PM
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

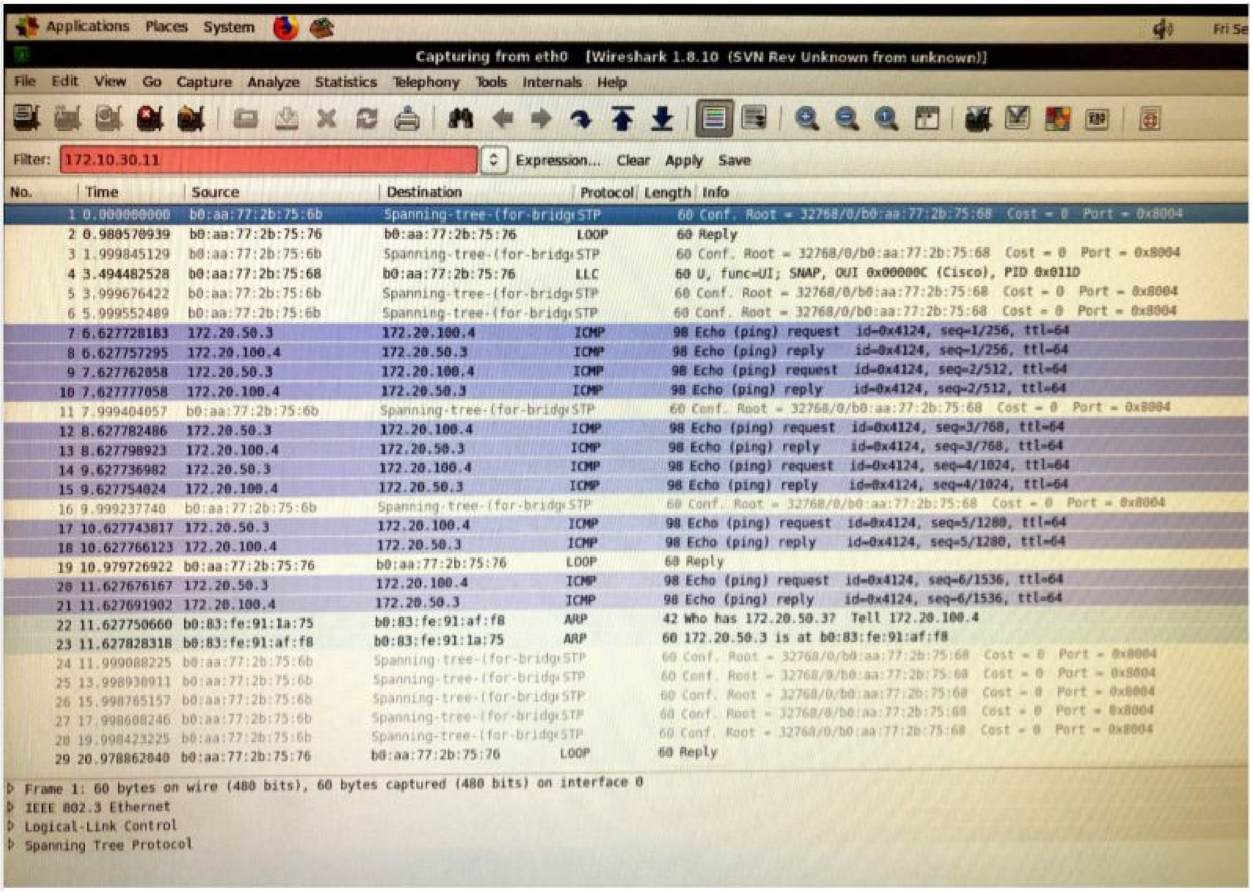
```
No.   Time         Source        Destination   Protocol Length Info
   78 91.133294556 172.10.30.11  172.20.50.3   TCP        74 38598 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1452 SACK_PERM=1 TSval=44254 TSecr=0 WS=128
   79 91.133320840 172.20.50.3   172.10.30.11  TCP        74 http > 38598 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=536839 TSecr
   80 91.134558390 172.10.30.11  172.20.50.3   TCP        66 38598 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=44257 TSecr=536839
   81 91.134568836 172.10.30.11  172.20.50.3   HTTP      377 GET / HTTP/1.1
   82 91.134583873 172.20.50.3   172.10.30.11  TCP        66 http > 38598 [ACK] Seq=1 Ack=312 Win=15616 Len=0 TSval=536841 TSecr=44257
   83 91.135075442 172.20.50.3   172.10.30.11  TCP      1506 [TCP segment of a reassembled PDU]
   84 91.135079780 172.20.50.3   172.10.30.11  TCP      1506 [TCP segment of a reassembled PDU]
   85 91.135081833 172.20.50.3   172.10.30.11  TCP      1506 [TCP segment of a reassembled PDU]
   86 91.135084217 172.20.50.3   172.10.30.11  HTTP      905 HTTP/1.1 403 Forbidden  (text/html)
   87 91.135115939 172.20.50.3   172.10.30.11  TCP        66 http > 38598 [FIN, ACK] Seq=5160 Ack=312 Win=15616 Len=0 TSval=536841 TSecr=44257
   88 91.136744948 172.10.30.11  172.20.50.3   TCP        66 38598 > http [ACK] Seq=312 Ack=2881 Win=17536 Len=0 TSval=44259 TSecr=536841
   89 91.136758349 172.10.30.11  172.20.50.3   TCP        66 38598 > http [ACK] Seq=312 Ack=5160 Win=20480 Len=0 TSval=44259 TSecr=536841
   90 91.136760264 172.10.30.11  172.20.50.3   TCP        66 38598 > http [FIN, ACK] Seq=312 Ack=5161 Win=20480 Len=0 TSval=44259 TSecr=536841
   91 91.136766266 172.20.50.3   172.10.30.11  TCP        66 http > 38598 [ACK] Seq=5161 Ack=313 Win=15616 Len=0 TSval=536843 TSecr=44259
   92 91.166633592 172.10.30.11  172.20.50.3   TCP        74 38600 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1452 SACK_PERM=1 TSval=44289 TSecr=0 WS=128
   93 91.166648785 172.20.50.3   172.10.30.11  TCP        74 http > 38600 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=536873 TSecr
   94 91.166652871 172.10.30.11  172.20.50.3   TCP        74 38602 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1452 SACK_PERM=1 TSval=44289 TSecr=0 WS=128
   95 91.166654904 172.20.50.3   172.10.30.11  TCP        74 http > 38602 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=536873 TSecr
   96 91.167851387 172.10.30.11  172.20.50.3   TCP        66 38600 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=44290 TSecr=536873
   97 91.167861322 172.10.30.11  172.20.50.3   TCP        66 38602 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=44290 TSecr=536873
   98 91.167863385 172.10.30.11  172.20.50.3   HTTP      336 GET /icons/apache_pb.gif HTTP/1.1
   99 91.167876886 172.20.50.3   172.10.30.11  TCP        66 http > 38600 [ACK] Seq=1 Ack=271 Win=15616 Len=0 TSval=536874 TSecr=44290
  100 91.167882292 172.10.30.11  172.20.50.3   HTTP      336 GET /icons/poweredby.png HTTP/1.1
  101 91.167886629 172.20.50.3   172.10.30.11  TCP        66 http > 38602 [ACK] Seq=1 Ack=271 Win=15616 Len=0 TSval=536874 TSecr=44290
  102 91.168274757 172.20.50.3   172.10.30.11  TCP      1506 [TCP segment of a reassembled PDU]
  103 91.168277447 172.20.50.3   172.10.30.11  TCP      1506 [TCP segment of a reassembled PDU]
  104 91.168278418 172.20.50.3   172.10.30.11  HTTP     1207 HTTP/1.1 200 OK  (GIF89a)
  105 91.168280928 172.20.50.3   172.10.30.11  TCP      1506 [TCP segment of a reassembled PDU]
  106 91.168294749 172.20.50.3   172.10.30.11  HTTP     1396 HTTP/1.1 200 OK  (PNG)
  107 91.168318744 172.20.50.3   172.10.30.11  TCP        66 http > 38600 [FIN, ACK] Seq=2582 Ack=271 Win=15616 Len=0 TSval=536874 TSecr=44290
  108 91.168321417 172.20.50.3   172.10.30.11  TCP        66 http > 38602 [FIN, ACK] Seq=4211 Ack=271 Win=15616 Len=0 TSval=536874 TSecr=44290
  109 91.170034227 172.10.30.11  172.20.50.3   TCP        66 38600 > http [ACK] Seq=271 Ack=2582 Win=17536 Len=0 TSval=44292 TSecr=536874
  110 91.170047636 172.10.30.11  172.20.50.3   TCP        66 38602 > http [ACK] Seq=271 Ack=1441 Win=17536 Len=0 TSval=44292 TSecr=536874
                                 172.20.50.3   TCP        66 38600 > http [FIN, ACK] Seq=271 Ack=2582 Win=17536 Len=0 TSval=44292 TSecr=536874
```


Applications Places System
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

```
No.   Time         Source             Destination              Protocol Length Info
   30 41.396931389 172.10.30.11       172.20.100.4             TCP        66 46206 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=630966 TSecr=1122168
   31 41.396943858 172.10.30.11       172.20.100.4             HTTP      378 GET / HTTP/1.1
   32 41.396958805 172.20.100.4       172.10.30.11             TCP        66 http > 46206 [ACK] Seq=1 Ack=313 Win=15616 Len=0 TSval=1122169 TSecr=630966
   33 41.397225549 172.20.100.4       172.10.30.11             TCP      1506 [TCP segment of a reassembled PDU]
   34 41.397231602 172.20.100.4       172.10.30.11             TCP      1506 [TCP segment of a reassembled PDU]
   35 41.397234036 172.20.100.4       172.10.30.11             TCP      1506 [TCP segment of a reassembled PDU]
   36 41.397236517 172.20.100.4       172.10.30.11             HTTP      905 HTTP/1.1 403 Forbidden  (text/html)
   37 41.397261093 172.20.100.4       172.10.30.11             TCP        66 http > 46206 [FIN, ACK] Seq=5160 Ack=313 Win=15616 Len=0 TSval=1122170 TSecr=630966
   38 41.398894199 172.10.30.11       172.20.100.4             TCP        66 46206 > http [ACK] Seq=313 Ack=2881 Win=17536 Len=0 TSval=630968 TSecr=1122169
   39 41.398909716 172.10.30.11       172.20.100.4             TCP        66 46206 > http [ACK] Seq=313 Ack=5160 Win=20480 Len=0 TSval=630968 TSecr=1122169
   40 41.398911971 172.10.30.11       172.20.100.4             TCP        66 46206 > http [FIN, ACK] Seq=313 Ack=5161 Win=20480 Len=0 TSval=630968 TSecr=1122170
   41 41.398918520 172.20.100.4       172.10.30.11             TCP        66 http > 46206 [ACK] Seq=5161 Ack=314 Win=15616 Len=0 TSval=1122171 TSecr=630968
   42 42.040686767 b0:aa:77:2b:75:6b  Spanning-tree-(for-bridg STP        60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   43 44.040583580 b0:aa:77:2b:75:6b  Spanning-tree-(for-bridg STP        60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   44 45.219720958 b0:aa:77:2b:75:76  b0:aa:77:2b:75:76        LOOP       60 Reply
   45 46.040452464 b0:aa:77:2b:75:6b  Spanning-tree-(for-bridg STP        60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   46 48.040286207 b0:aa:77:2b:75:6b  Spanning-tree-(for-bridg STP        60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   47 50.040110551 b0:aa:77:2b:75:6b  Spanning-tree-(for-bridg STP        60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   48 51.501502858 b0:83:fe:91:af:f8  Broadcast                ARP        60 Who has 172.20.100.4?  Tell 172.20.50.3
   49 51.501518194 b0:83:fe:91:1a:75  b0:83:fe:91:af:f8        ARP        42 172.20.100.4 is at b0:83:fe:91:1a:75
   50 51.501598797 172.20.50.3        172.20.100.4             TCP        74 33014 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1133660 TSecr=0 WS=128
   51 51.501612812 172.20.100.4       172.20.50.3              TCP        74 http > 33014 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1132274 TSe
   52 51.501719336 172.20.50.3        172.20.100.4             TCP        66 33014 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=1133661 TSecr=1132274
   53 51.501920210 172.20.50.3        172.20.100.4             HTTP      378 GET / HTTP/1.1
   54 51.501934275 172.20.100.4       172.20.50.3              TCP        66 http > 33014 [ACK] Seq=1 Ack=313 Win=15616 Len=0 TSval=1132274 TSecr=1133661
   55 51.502186617 172.20.100.4       172.20.50.3              TCP      1514 [TCP segment of a reassembled PDU]
   56 51.502190261 172.20.100.4       172.20.50.3              TCP      1514 [TCP segment of a reassembled PDU]
   57 51.502192111 172.20.100.4       172.20.50.3              TCP      1514 [TCP segment of a reassembled PDU]
   58 51.502194472 172.20.100.4       172.20.50.3              HTTP      881 HTTP/1.1 403 Forbidden  (text/html)
```

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

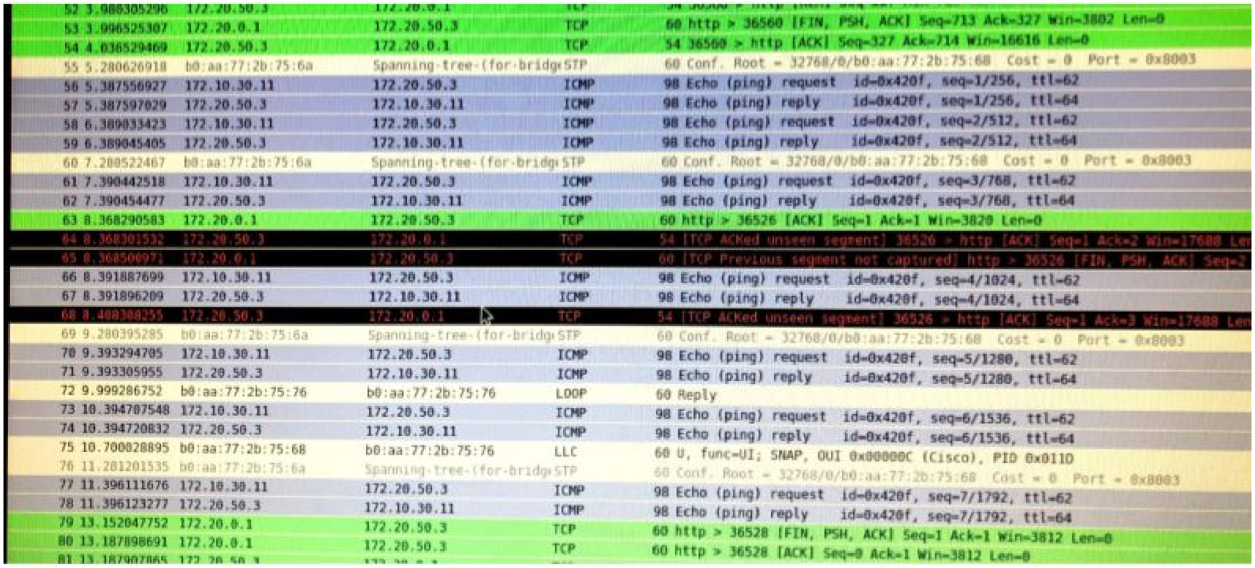
a. ICMP services are allowed between all internal and external computers as shown in the wireshark simulation.



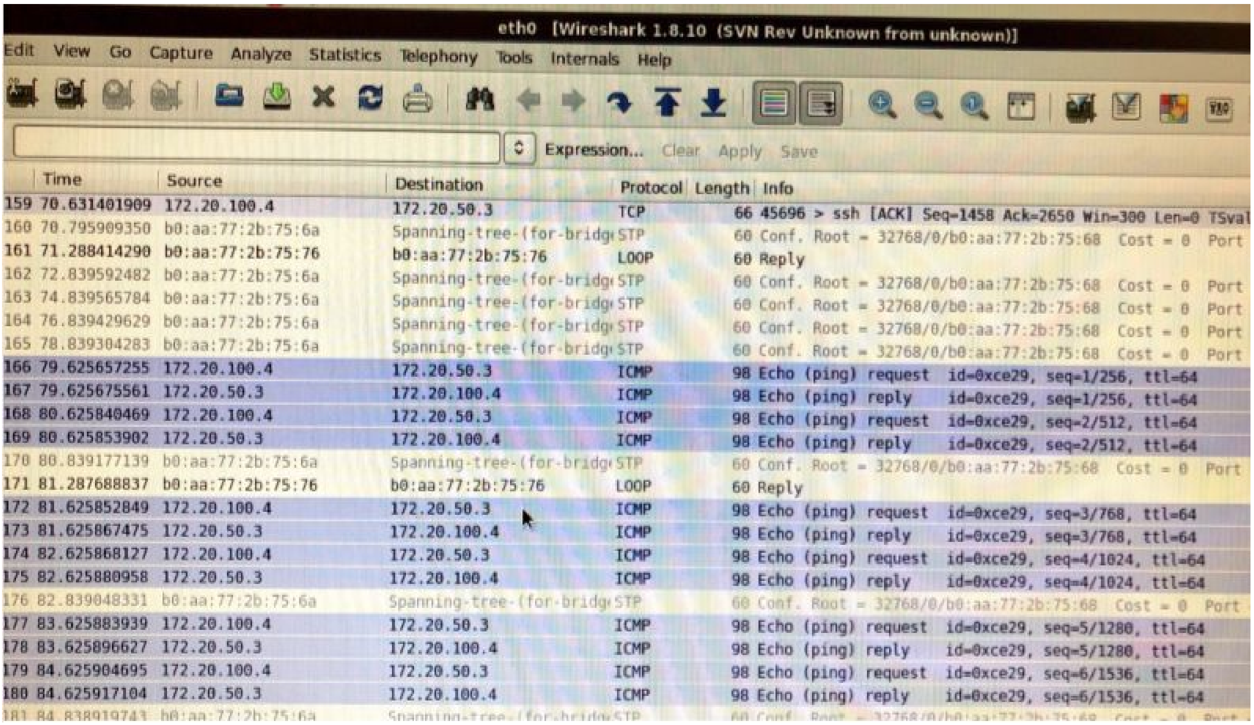
Capturing from eth0   [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]

Filter: 172.10.30.11

```
No.   Time          Source               Destination                  Protocol Length Info
    1 0.000000000   b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
    2 0.980570939   b0:aa:77:2b:75:76    b0:aa:77:2b:75:76        LOOP     60 Reply
    3 1.999845129   b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
    4 3.494482528   b0:aa:77:2b:75:68    b0:aa:77:2b:75:76        LLC      60 U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x011D
    5 3.999676422   b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
    6 5.999552489   b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
    7 6.627728183   172.20.50.3          172.20.100.4             ICMP     98 Echo (ping) request  id=0x4124, seq=1/256, ttl=64
    8 6.627757295   172.20.100.4         172.20.50.3              ICMP     98 Echo (ping) reply    id=0x4124, seq=1/256, ttl=64
    9 7.627762058   172.20.50.3          172.20.100.4             ICMP     98 Echo (ping) request  id=0x4124, seq=2/512, ttl=64
   10 7.627777058   172.20.100.4         172.20.50.3              ICMP     98 Echo (ping) reply    id=0x4124, seq=2/512, ttl=64
   11 7.999404057   b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   12 8.627782486   172.20.50.3          172.20.100.4             ICMP     98 Echo (ping) request  id=0x4124, seq=3/768, ttl=64
   13 8.627798923   172.20.100.4         172.20.50.3              ICMP     98 Echo (ping) reply    id=0x4124, seq=3/768, ttl=64
   14 9.627736982   172.20.50.3          172.20.100.4             ICMP     98 Echo (ping) request  id=0x4124, seq=4/1024, ttl=64
   15 9.627754024   172.20.100.4         172.20.50.3              ICMP     98 Echo (ping) reply    id=0x4124, seq=4/1024, ttl=64
   16 9.999237740   b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   17 10.627743817  172.20.50.3          172.20.100.4             ICMP     98 Echo (ping) request  id=0x4124, seq=5/1280, ttl=64
   18 10.627766123  172.20.100.4         172.20.50.3              ICMP     98 Echo (ping) reply    id=0x4124, seq=5/1280, ttl=64
   19 10.979726922  b0:aa:77:2b:75:76    b0:aa:77:2b:75:76        LOOP     60 Reply
   20 11.627676167  172.20.50.3          172.20.100.4             ICMP     98 Echo (ping) request  id=0x4124, seq=6/1536, ttl=64
   21 11.627691902  172.20.100.4         172.20.50.3              ICMP     98 Echo (ping) reply    id=0x4124, seq=6/1536, ttl=64
   22 11.627750660  b0:83:fe:91:1a:75    b0:83:fe:91:af:f8        ARP      42 Who has 172.20.50.3?  Tell 172.20.100.4
   23 11.627828318  b0:83:fe:91:af:f8    b0:83:fe:91:1a:75        ARP      60 172.20.50.3 is at b0:83:fe:91:af:f8
   24 11.999088225  b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   25 13.998930911  b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   26 15.998765157  b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   27 17.998608246  b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   28 19.998423225  b0:aa:77:2b:75:6b    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
   29 20.978862040  b0:aa:77:2b:75:76    b0:aa:77:2b:75:76        LOOP     60 Reply

▷ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▷ IEEE 802.3 Ethernet
▷ Logical-Link Control
▷ Spanning Tree Protocol
```



```
   52 3.988305296   172.20.50.3          172.20.0.1               TCP      54 36560 > http
   53 3.996525307   172.20.0.1           172.20.50.3              TCP      60 http > 36560 [FIN, PSH, ACK] Seq=713 Ack=327 Win=3802 Len=0
   54 4.036529469   172.20.50.3          172.20.0.1               TCP      54 36560 > http [ACK] Seq=327 Ack=714 Win=16616 Len=0
   55 5.280626918   b0:aa:77:2b:75:6a    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
   56 5.387556927   172.10.30.11         172.20.50.3              ICMP     98 Echo (ping) request  id=0x420f, seq=1/256, ttl=62
   57 5.387597029   172.20.50.3          172.10.30.11             ICMP     98 Echo (ping) reply    id=0x420f, seq=1/256, ttl=64
   58 6.389033423   172.10.30.11         172.20.50.3              ICMP     98 Echo (ping) request  id=0x420f, seq=2/512, ttl=62
   59 6.389045405   172.20.50.3          172.10.30.11             ICMP     98 Echo (ping) reply    id=0x420f, seq=2/512, ttl=64
   60 7.280522467   b0:aa:77:2b:75:6a    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
   61 7.390442518   172.10.30.11         172.20.50.3              ICMP     98 Echo (ping) request  id=0x420f, seq=3/768, ttl=62
   62 7.390454477   172.20.50.3          172.10.30.11             ICMP     98 Echo (ping) reply    id=0x420f, seq=3/768, ttl=64
   63 8.368290583   172.20.0.1           172.20.50.3              TCP      60 http > 36526 [ACK] Seq=1 Ack=1 Win=3820 Len=0
   64 8.368301532   172.20.50.3          172.20.0.1               TCP      54 [TCP ACKed unseen segment] 36526 > http [ACK] Seq=1 Ack=2 Win=17688 Len
   65 8.368500971   172.20.0.1           172.20.50.3              TCP      60 [TCP Previous segment not captured] http > 36526 [FIN, PSH, ACK] Seq=2
   66 8.391887699   172.10.30.11         172.20.50.3              ICMP     98 Echo (ping) request  id=0x420f, seq=4/1024, ttl=62
   67 8.391896209   172.20.50.3          172.10.30.11             ICMP     98 Echo (ping) reply    id=0x420f, seq=4/1024, ttl=64
   68 8.408308255   172.20.50.3          172.20.0.1               TCP      54 [TCP ACKed unseen segment] 36526 > http [ACK] Seq=1 Ack=3 Win=17688 Len
   69 9.280395285   b0:aa:77:2b:75:6a    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
   70 9.393294705   172.10.30.11         172.20.50.3              ICMP     98 Echo (ping) request  id=0x420f, seq=5/1280, ttl=62
   71 9.393305955   172.20.50.3          172.10.30.11             ICMP     98 Echo (ping) reply    id=0x420f, seq=5/1280, ttl=64
   72 9.999286752   b0:aa:77:2b:75:76    b0:aa:77:2b:75:76        LOOP     60 Reply
   73 10.394707548  172.10.30.11         172.20.50.3              ICMP     98 Echo (ping) request  id=0x420f, seq=6/1536, ttl=62
   74 10.394720832  172.20.50.3          172.10.30.11             ICMP     98 Echo (ping) reply    id=0x420f, seq=6/1536, ttl=64
   75 10.700828895  b0:aa:77:2b:75:68    b0:aa:77:2b:75:76        LLC      60 U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x011D
   76 11.281201535  b0:aa:77:2b:75:6a    Spanning-tree-(for-bridg STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8003
   77 11.396111676  172.10.30.11         172.20.50.3              ICMP     98 Echo (ping) request  id=0x420f, seq=7/1792, ttl=62
   78 11.396123277  172.20.50.3          172.10.30.11             ICMP     98 Echo (ping) reply    id=0x420f, seq=7/1792, ttl=64
   79 13.152047752  172.20.0.1           172.20.50.3              TCP      60 http > 36528 [FIN, PSH, ACK] Seq=1 Ack=1 Win=3812 Len=0
   80 13.187898691  172.20.0.1           172.20.50.3              TCP      60 http > 36528 [ACK] Seq=0 Ack=1 Win=3812 Len=0
   81 13.187907865  172.20.50.3
```


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

```
    Time         Source              Destination               Protocol Length Info
159 70.631401909 172.20.100.4        172.20.50.3               TCP      66 45696 > ssh [ACK] Seq=1458 Ack=2650 Win=300 Len=0 TSval
160 70.795909350 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
161 71.288414290 b0:aa:77:2b:75:76   b0:aa:77:2b:75:76         LOOP     60 Reply
162 72.839592482 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
163 74.839565784 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
164 76.839429629 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
165 78.839304283 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
166 79.625657255 172.20.100.4        172.20.50.3               ICMP     98 Echo (ping) request  id=0xce29, seq=1/256, ttl=64
167 79.625675561 172.20.50.3         172.20.100.4              ICMP     98 Echo (ping) reply    id=0xce29, seq=1/256, ttl=64
168 80.625840469 172.20.100.4        172.20.50.3               ICMP     98 Echo (ping) request  id=0xce29, seq=2/512, ttl=64
169 80.625853902 172.20.50.3         172.20.100.4              ICMP     98 Echo (ping) reply    id=0xce29, seq=2/512, ttl=64
170 80.839177139 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
171 81.287688837 b0:aa:77:2b:75:76   b0:aa:77:2b:75:76         LOOP     60 Reply
172 81.625852849 172.20.100.4        172.20.50.3               ICMP     98 Echo (ping) request  id=0xce29, seq=3/768, ttl=64
173 81.625867475 172.20.50.3         172.20.100.4              ICMP     98 Echo (ping) reply    id=0xce29, seq=3/768, ttl=64
174 82.625868127 172.20.100.4        172.20.50.3               ICMP     98 Echo (ping) request  id=0xce29, seq=4/1024, ttl=64
175 82.625880958 172.20.50.3         172.20.100.4              ICMP     98 Echo (ping) reply    id=0xce29, seq=4/1024, ttl=64
176 82.839048331 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
177 83.625883939 172.20.100.4        172.20.50.3               ICMP     98 Echo (ping) request  id=0xce29, seq=5/1280, ttl=64
178 83.625896627 172.20.50.3         172.20.100.4              ICMP     98 Echo (ping) reply    id=0xce29, seq=5/1280, ttl=64
179 84.625904695 172.20.100.4        172.20.50.3               ICMP     98 Echo (ping) request  id=0xce29, seq=6/1536, ttl=64
180 84.625917104 172.20.50.3         172.20.100.4              ICMP     98 Echo (ping) reply    id=0xce29, seq=6/1536, ttl=64
181 84.838919743 b0:aa:77:2b:75:6a   Spanning-tree-(for-bridg  STP      60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port
```

iv. Summarize the default Cisco firewall policy.

a. The default policy has no rules against any incoming request from internal or external computers. The default policy allows access to all open ports within the network. This policy has no restrictions and is not good practice.

Section III

Task III

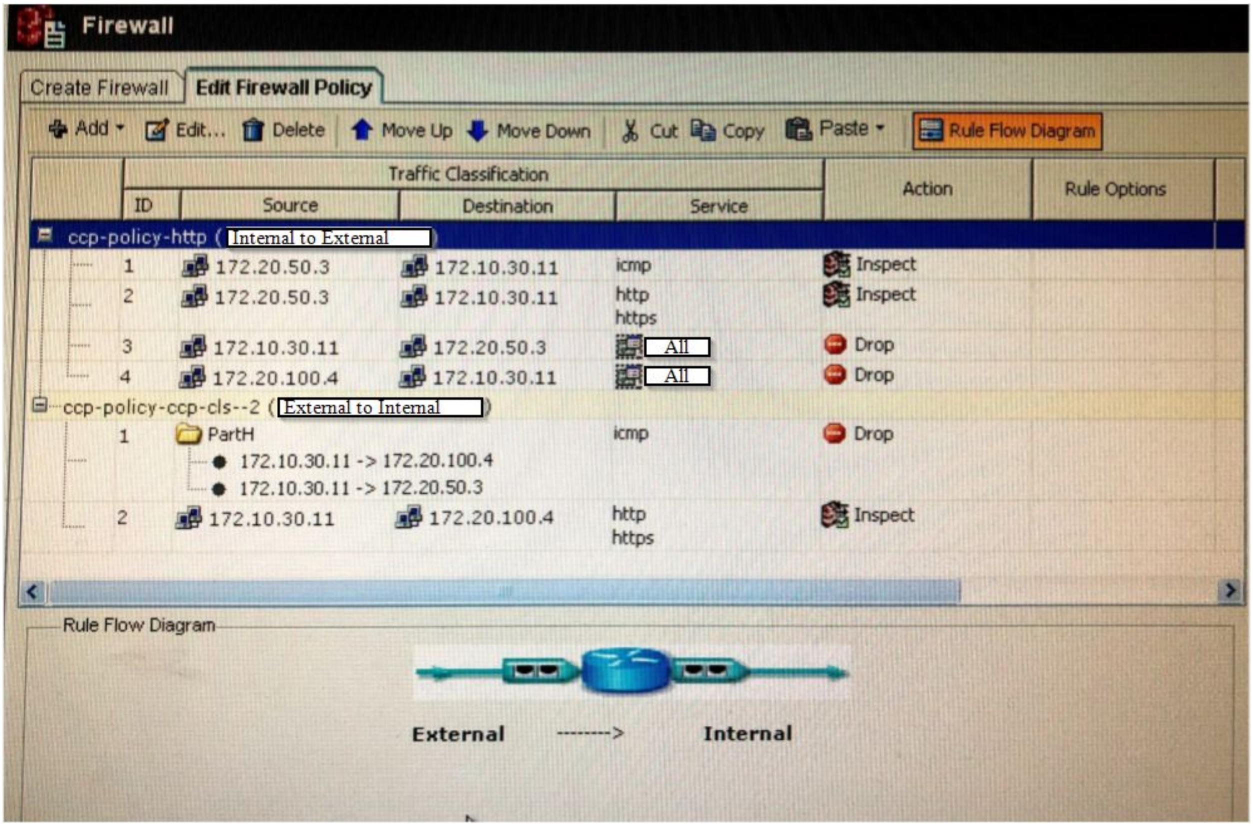
i. Copy and paste the access control matrix.

	nternal Server	ernal Workstation	ternal Computer
Internal Server	N/A	http/https/ssh	http/https
ternal Workstation	ttp/https/ssh	N/A	---
xternal Computer	---	http/https/icmp	N/A

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

a. Policies cannot be enforced to the internal server and internal workstation. Applying rules to the TCP can partially be enforced since TCP is a necessary protocol.

iii. Copy and paste a screen shot of your Cisco firewall configuration.



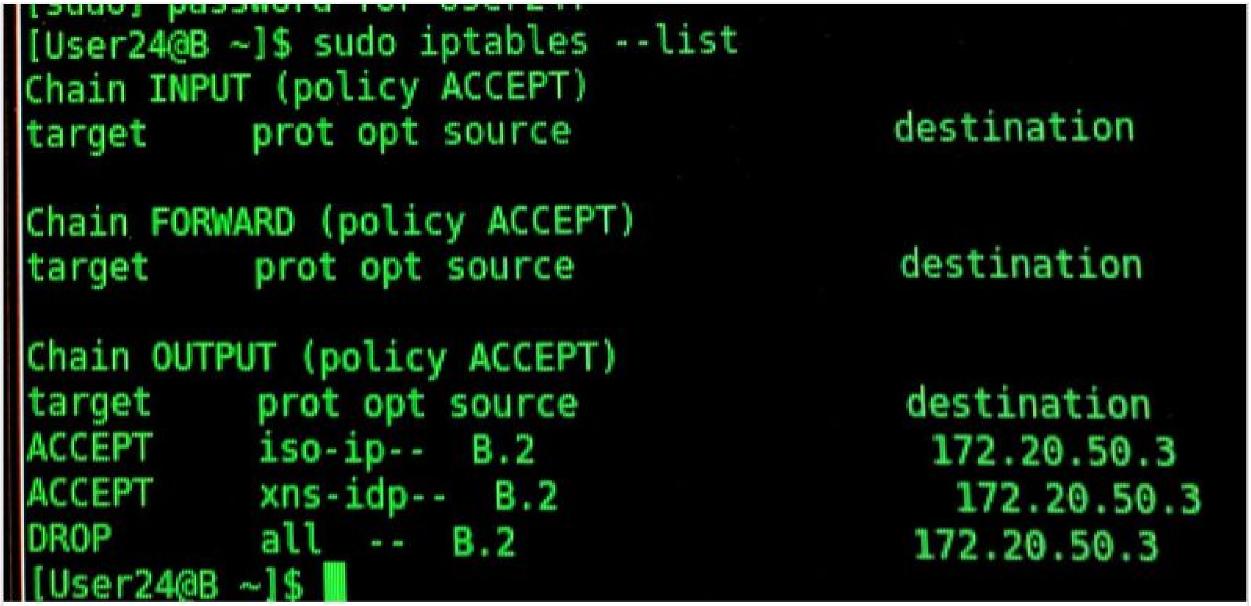
Traffic Classification				Action	Rule Options
ID	Source	Destination	Service		
ccp-policy-http (Internal to External)					
1	172.20.50.3	172.10.30.11	icmp	Inspect	
2	172.20.50.3	172.10.30.11	http https	Inspect	
3	172.10.30.11	172.20.50.3	All	Drop	
4	172.20.100.4	172.10.30.11	All	Drop	
ccp-policy-ccp-cls--2 (External to Internal)					
1	PartH ● 172.10.30.11 -> 172.20.100.4 ● 172.10.30.11 -> 172.20.50.3		icmp	Drop	
2	172.10.30.11	172.20.100.4	http https	Inspect	

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

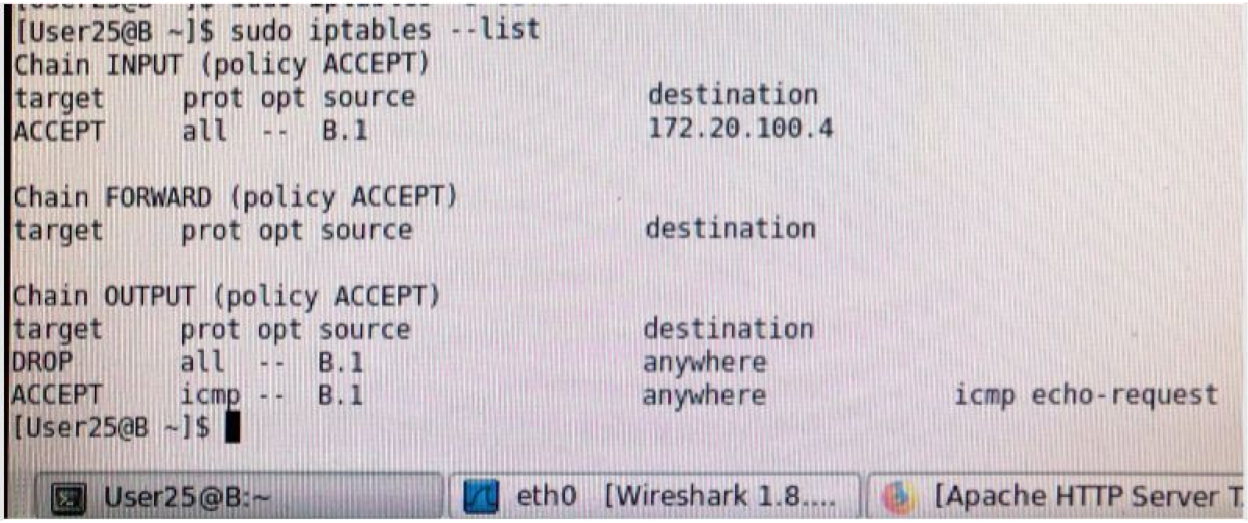
   a. Policies cannot be enforced from external to internal or vice-versa. When enforcing policies using iptables, this will apply restrictions on internal computers and servers which cannot be done by the Cisco firewall. SSH is one key protocol that Cisco firewall has limitations to which iptables do not have.

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

   a. sudo iptables -A OUTPUT -s 172.20.100.4 -d 172.20.50.3 -p 22 80 443 -j ACCEPT
   b. sudo iptables -A OUTPUT -s 172.20.100.4 -d 172.20.50.3 -j DROP
   c. sudo iptables -A INPUT -s 172.20.50.3 -d 172.20.100.4 -j ACCEPT
   d. sudo iptables -A OUTPUT -s 172.20.50.3 -j DROP
   e. sudo iptables -A OUTPUT -s 172.20.50.3 -p icmp –icmp-type echo-request -j ACCEPT



```
[sudo] password for User24:
[User24@B ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     iso-ip--  B.2                  172.20.50.3
ACCEPT     xns-idp--  B.2                 172.20.50.3
DROP       all  --  B.2                  172.20.50.3
[User24@B ~]$
```

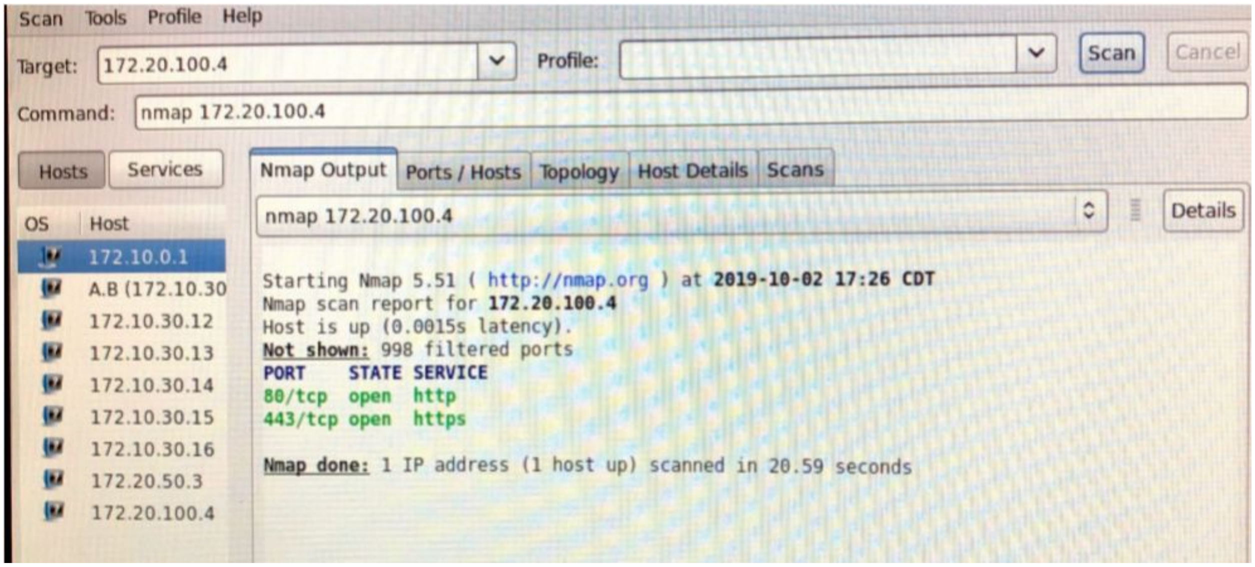


```
[User25@B ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  B.1                  172.20.100.4

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  B.1                  anywhere
ACCEPT     icmp --  B.1                  anywhere            icmp echo-request
[User25@B ~]$
```

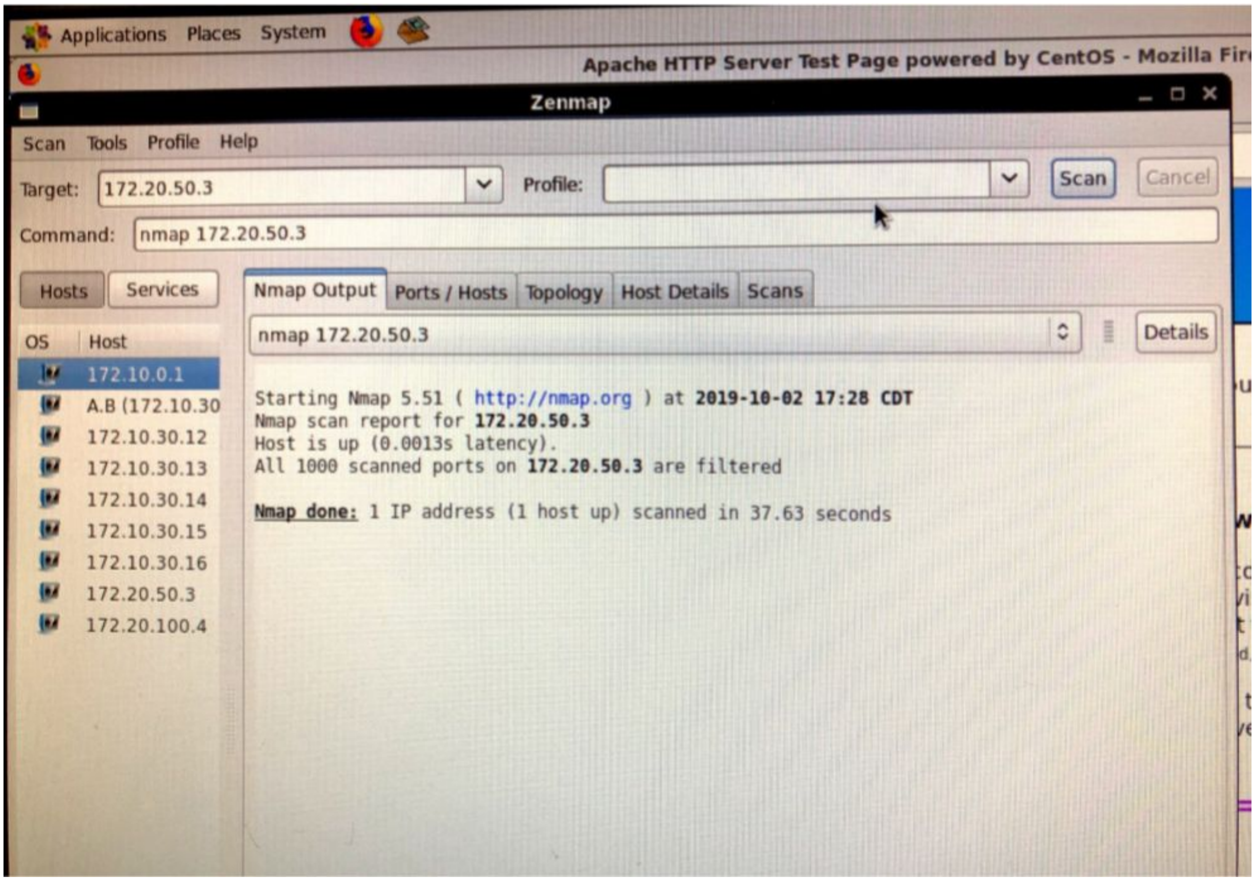
Section IV

Task IV

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



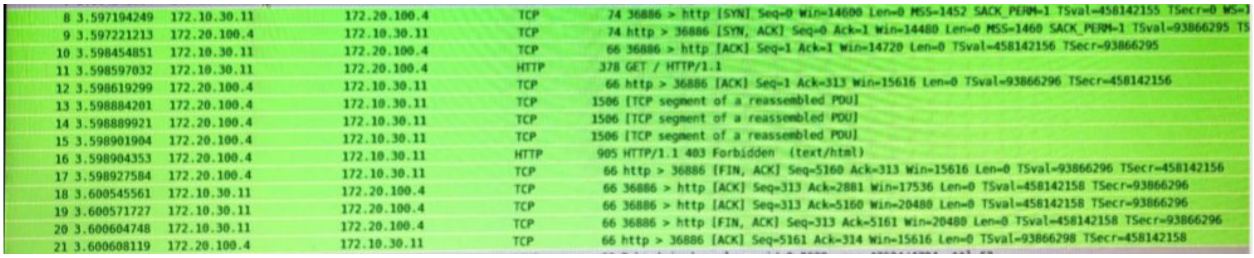
```
Starting Nmap 5.51 ( http://nmap.org ) at 2019-10-02 17:26 CDT
Nmap scan report for 172.20.100.4
Host is up (0.0015s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 20.59 seconds
```



```
Starting Nmap 5.51 ( http://nmap.org ) at 2019-10-02 17:28 CDT
Nmap scan report for 172.20.50.3
Host is up (0.0013s latency).
All 1000 scanned ports on 172.20.50.3 are filtered

Nmap done: 1 IP address (1 host up) scanned in 37.63 seconds
```

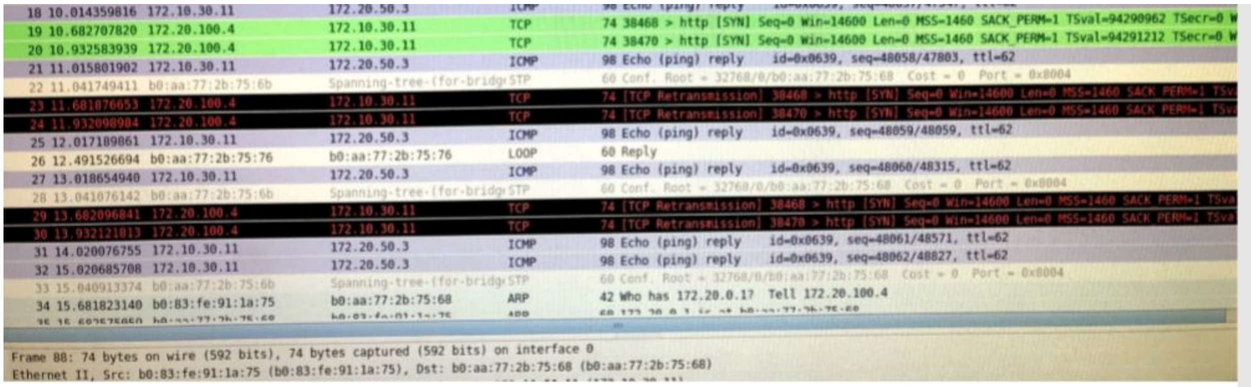
ii. Show the Wireshark results (screen shots) of checking the web service between computers. State if web service is allowed between computers.

External Computer to Internal Server



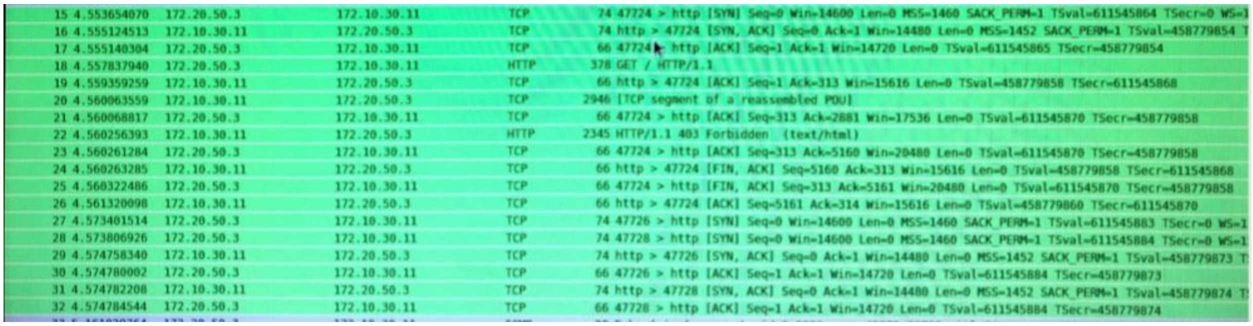
```
 8 3.597194249  172.10.30.11   172.20.100.4   TCP   74 36886 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1452 SACK_PERM=1 TSval=458142155 TSecr=0 WS=1
 9 3.597221213  172.20.100.4   172.10.30.11   TCP   74 http > 36886 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=93866295 TS
10 3.598454851  172.10.30.11   172.20.100.4   TCP   66 36886 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=458142156 TSecr=93866295
11 3.598597032  172.10.30.11   172.20.100.4   HTTP 378 GET / HTTP/1.1
12 3.598619299  172.20.100.4   172.10.30.11   TCP   66 http > 36886 [ACK] Seq=1 Ack=313 Win=15616 Len=0 TSval=93866296 TSecr=458142156
13 3.598884201  172.20.100.4   172.10.30.11   TCP 1506 [TCP segment of a reassembled PDU]
14 3.598889921  172.20.100.4   172.10.30.11   TCP 1506 [TCP segment of a reassembled PDU]
15 3.598901904  172.20.100.4   172.10.30.11   TCP 1506 [TCP segment of a reassembled PDU]
16 3.598904353  172.20.100.4   172.10.30.11   HTTP 905 HTTP/1.1 403 Forbidden  (text/html)
17 3.598927584  172.20.100.4   172.10.30.11   TCP   66 http > 36886 [FIN, ACK] Seq=5160 Ack=313 Win=15616 Len=0 TSval=93866296 TSecr=458142156
18 3.600545561  172.10.30.11   172.20.100.4   TCP   66 36886 > http [ACK] Seq=313 Ack=2881 Win=17536 Len=0 TSval=458142158 TSecr=93866296
19 3.600571727  172.10.30.11   172.20.100.4   TCP   66 36886 > http [ACK] Seq=313 Ack=5160 Win=20480 Len=0 TSval=458142158 TSecr=93866296
20 3.600604748  172.10.30.11   172.20.100.4   TCP   66 36886 > http [FIN, ACK] Seq=313 Ack=5161 Win=20480 Len=0 TSval=458142158 TSecr=93866296
21 3.600608119  172.20.100.4   172.10.30.11   TCP   66 http > 36886 [ACK] Seq=5161 Ack=314 Win=15616 Len=0 TSval=93866298 TSecr=458142158
```

Internal Server to External Computer



```
18 10.014359816 172.10.30.11      172.20.50.3                ICMP  98 Echo (ping) reply
19 10.682707820 172.20.100.4      172.10.30.11               TCP   74 38468 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=94290962 TSecr=0 W
20 10.932583939 172.20.100.4      172.10.30.11               TCP   74 38470 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=94291212 TSecr=0 W
21 11.015801902 172.10.30.11      172.20.50.3                ICMP  98 Echo (ping) reply    id=0x0639, seq=48058/47803, ttl=62
22 11.041749411 b0:aa:77:2b:75:6b Spanning-tree-(for-bridg STP   60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
23 11.681876653 172.20.100.4      172.10.30.11               TCP   74 [TCP Retransmission] 38468 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSv
24 11.932098984 172.20.100.4      172.10.30.11               TCP   74 [TCP Retransmission] 38470 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSv
25 12.017189861 172.10.30.11      172.20.50.3                ICMP  98 Echo (ping) reply    id=0x0639, seq=48059/48059, ttl=62
26 12.491526694 b0:aa:77:2b:75:76 b0:aa:77:2b:75:76          LOOP  60 Reply
27 13.018654940 172.10.30.11      172.20.50.3                ICMP  98 Echo (ping) reply    id=0x0639, seq=48060/48315, ttl=62
28 13.041076142 b0:aa:77:2b:75:6b Spanning-tree-(for-bridg STP   60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
29 13.682096841 172.20.100.4      172.10.30.11               TCP   74 [TCP Retransmission] 38468 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSva
30 13.932121813 172.20.100.4      172.10.30.11               TCP   74 [TCP Retransmission] 38470 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSva
31 14.020076755 172.10.30.11      172.20.50.3                ICMP  98 Echo (ping) reply    id=0x0639, seq=48061/48571, ttl=62
32 15.020685708 172.10.30.11      172.20.50.3                ICMP  98 Echo (ping) reply    id=0x0639, seq=48062/48827, ttl=62
33 15.040913374 b0:aa:77:2b:75:6b Spanning-tree-(for-bridg STP   60 Conf. Root = 32768/0/b0:aa:77:2b:75:68  Cost = 0  Port = 0x8004
34 15.681823140 b0:83:fe:91:1a:75 b0:aa:77:2b:75:68          ARP   42 Who has 172.20.0.1?  Tell 172.20.100.4

Frame 88: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: b0:83:fe:91:1a:75 (b0:83:fe:91:1a:75), Dst: b0:aa:77:2b:75:68 (b0:aa:77:2b:75:68)
```

Internal Workstation to External Computer

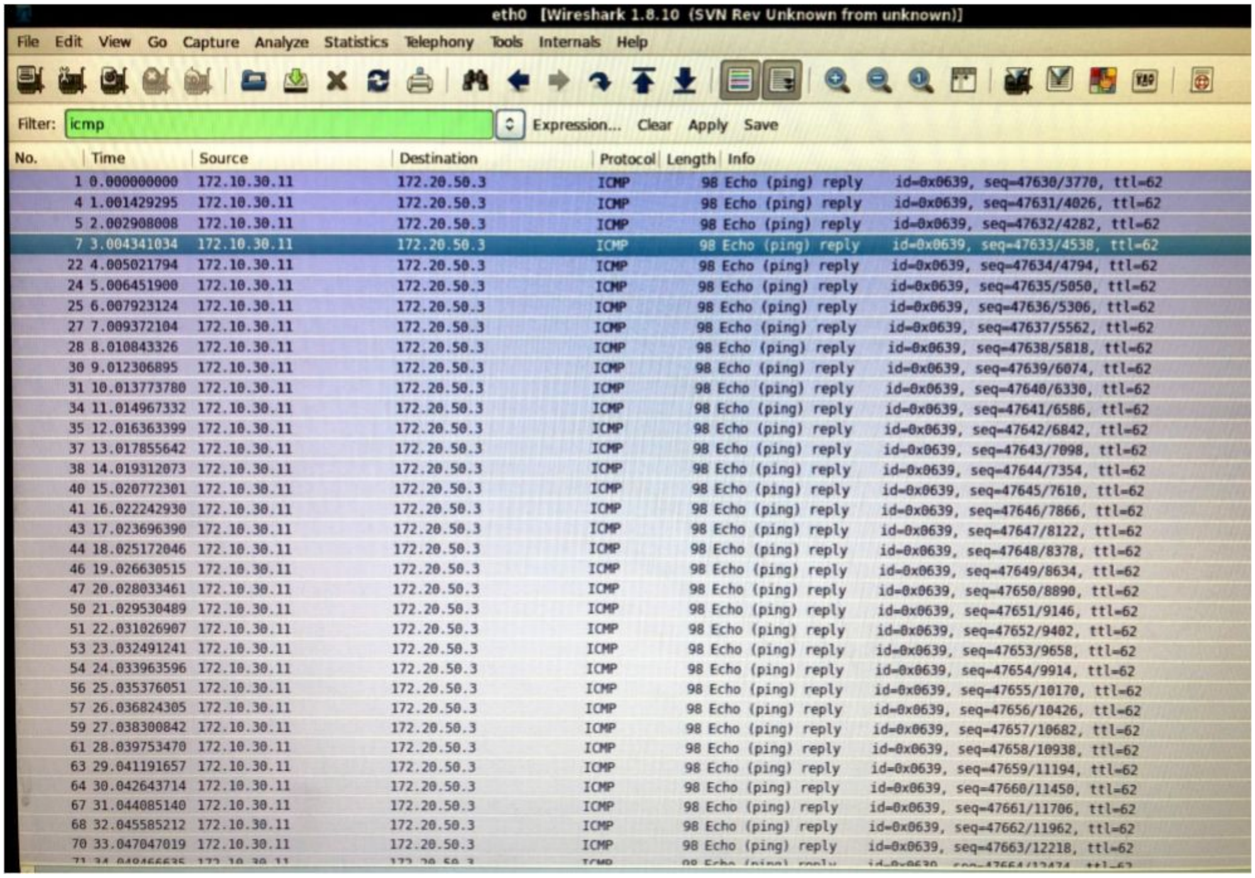


```
15 4.553654070  172.20.50.3    172.10.30.11   TCP   74 47724 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=611545864 TSecr=0 WS=1
16 4.555124513  172.10.30.11   172.20.50.3    TCP   74 http > 47724 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK_PERM=1 TSval=458779854 T
17 4.555140304  172.20.50.3    172.10.30.11   TCP   66 47724 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=611545865 TSecr=458779854
18 4.557837940  172.20.50.3    172.10.30.11   HTTP 378 GET / HTTP/1.1
19 4.559359259  172.10.30.11   172.20.50.3    TCP   66 http > 47724 [ACK] Seq=1 Ack=313 Win=15616 Len=0 TSval=458779858 TSecr=611545868
20 4.560063559  172.10.30.11   172.20.50.3    TCP 2946 [TCP segment of a reassembled PDU]
21 4.560068817  172.20.50.3    172.10.30.11   TCP   66 47724 > http [ACK] Seq=313 Ack=2881 Win=17536 Len=0 TSval=611545870 TSecr=458779858
22 4.560256393  172.10.30.11   172.20.50.3    HTTP 2345 HTTP/1.1 403 Forbidden  (text/html)
23 4.560261284  172.20.50.3    172.10.30.11   TCP   66 47724 > http [ACK] Seq=313 Ack=5160 Win=20480 Len=0 TSval=611545870 TSecr=458779858
24 4.560263285  172.10.30.11   172.20.50.3    TCP   66 http > 47724 [FIN, ACK] Seq=5160 Ack=313 Win=15616 Len=0 TSval=458779858 TSecr=611545868
25 4.560322486  172.20.50.3    172.10.30.11   TCP   66 47724 > http [FIN, ACK] Seq=313 Ack=5161 Win=20480 Len=0 TSval=611545870 TSecr=458779858
26 4.561320098  172.10.30.11   172.20.50.3    TCP   66 http > 47724 [ACK] Seq=5161 Ack=314 Win=15616 Len=0 TSval=458779860 TSecr=611545870
27 4.573401514  172.20.50.3    172.10.30.11   TCP   74 47726 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=611545883 TSecr=0 WS=1
28 4.573806926  172.20.50.3    172.10.30.11   TCP   74 47728 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=611545884 TSecr=0 WS=1
29 4.574758340  172.10.30.11   172.20.50.3    TCP   74 http > 47726 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK_PERM=1 TSval=458779873 T
30 4.574780002  172.20.50.3    172.10.30.11   TCP   66 47726 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=611545884 TSecr=458779873
31 4.574782208  172.10.30.11   172.20.50.3    TCP   74 http > 47728 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK_PERM=1 TSval=458779874 T
32 4.574784544  172.20.50.3    172.10.30.11   TCP   66 47728 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=611545884 TSecr=458779874
```

External Computer to Internal Workstation

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

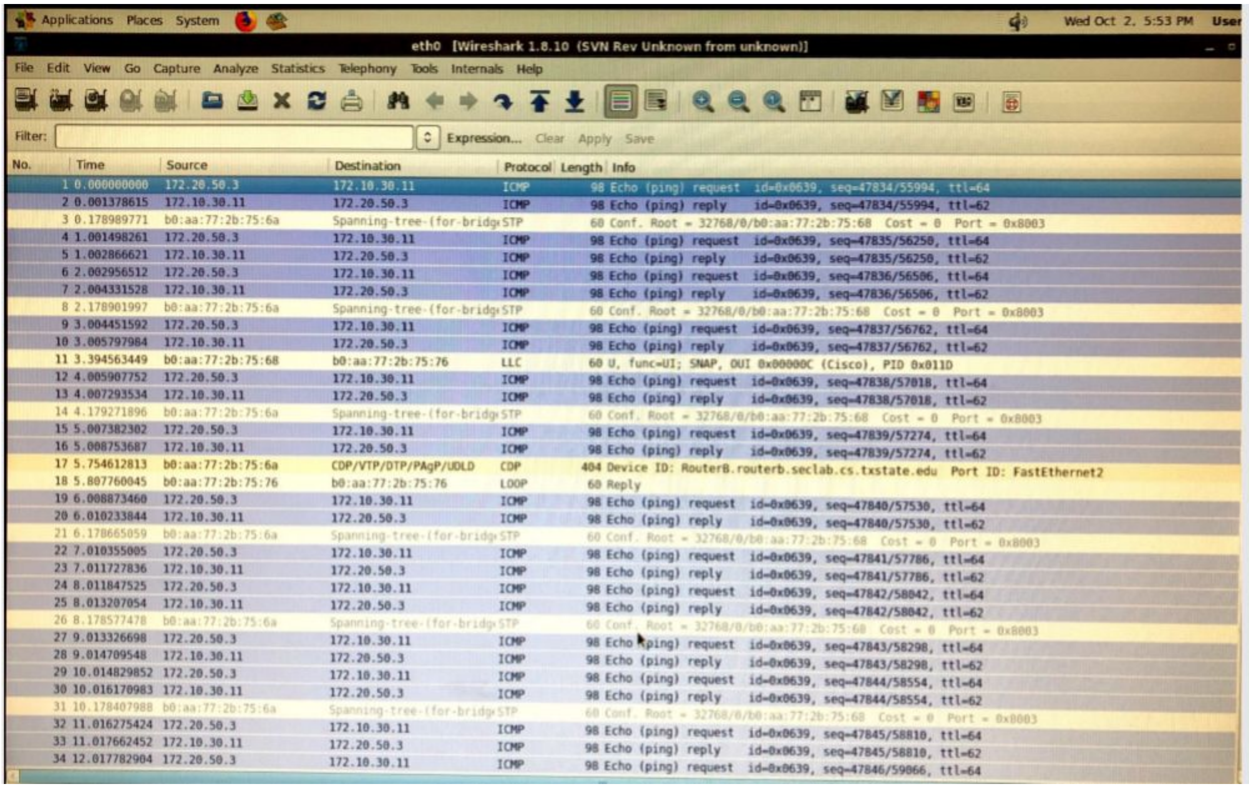
External Computer to Internal Workstation


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
   1 0.000000000   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47630/3770, ttl=62
   4 1.001429295   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47631/4026, ttl=62
   5 2.002908008   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47632/4282, ttl=62
   7 3.004341034   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47633/4538, ttl=62
  22 4.005021794   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47634/4794, ttl=62
  24 5.006451900   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47635/5050, ttl=62
  25 6.007923124   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47636/5306, ttl=62
  27 7.009372104   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47637/5562, ttl=62
  28 8.010843326   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47638/5818, ttl=62
  30 9.012306895   172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47639/6074, ttl=62
  31 10.013773780  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47640/6330, ttl=62
  34 11.014967332  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47641/6586, ttl=62
  35 12.016363399  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47642/6842, ttl=62
  37 13.017855642  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47643/7098, ttl=62
  38 14.019312073  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47644/7354, ttl=62
  40 15.020772301  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47645/7610, ttl=62
  41 16.022242930  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47646/7866, ttl=62
  43 17.023696390  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47647/8122, ttl=62
  44 18.025172046  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47648/8378, ttl=62
  46 19.026630515  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47649/8634, ttl=62
  47 20.028033461  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47650/8890, ttl=62
  50 21.029530489  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47651/9146, ttl=62
  51 22.031026907  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47652/9402, ttl=62
  53 23.032491241  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47653/9658, ttl=62
  54 24.033963596  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47654/9914, ttl=62
  56 25.035376051  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47655/10170, ttl=62
  57 26.036824305  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47656/10426, ttl=62
  59 27.038300842  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47657/10682, ttl=62
  61 28.039753470  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47658/10938, ttl=62
  63 29.041191657  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47659/11194, ttl=62
  64 30.042643714  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47660/11450, ttl=62
  67 31.044085140  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47661/11706, ttl=62
  68 32.045585212  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47662/11962, ttl=62
  70 33.047047019  172.10.30.11   172.20.50.3    ICMP     98 Echo (ping) reply   id=0x0639, seq=47663/12218, ttl=62
```

Internal Workstation to External Computer


Applications Places System
Wed Oct 2, 5:53 PM User
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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47834/55994, ttl=64
2	0.001378615	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47834/55994, ttl=62
3	0.178989771	b0:aa:77:2b:75:6a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:68 Cost = 0 Port = 0x8003
4	1.001498261	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47835/56250, ttl=64
5	1.002866621	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47835/56250, ttl=62
6	2.002956512	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47836/56506, ttl=64
7	2.004331528	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47836/56506, ttl=62
8	2.178901997	b0:aa:77:2b:75:6a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:68 Cost = 0 Port = 0x8003
9	3.004451592	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47837/56762, ttl=64
10	3.005797984	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47837/56762, ttl=62
11	3.394563449	b0:aa:77:2b:75:68	b0:aa:77:2b:75:76	LLC	60	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x011D
12	4.005907752	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47838/57018, ttl=64
13	4.007293534	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47838/57018, ttl=62
14	4.179271896	b0:aa:77:2b:75:6a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:68 Cost = 0 Port = 0x8003
15	5.007382302	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47839/57274, ttl=64
16	5.008753687	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47839/57274, ttl=62
17	5.754612813	b0:aa:77:2b:75:6a	CDP/VTP/DTP/PAgP/UDLD	CDP	404	Device ID: RouterB.routerb.seclab.cs.txstate.edu Port ID: FastEthernet2
18	5.807760045	b0:aa:77:2b:75:76	b0:aa:77:2b:75:76	LOOP	60	Reply
19	6.008873460	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47840/57530, ttl=64
20	6.010233844	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47840/57530, ttl=62
21	6.178665059	b0:aa:77:2b:75:6a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:68 Cost = 0 Port = 0x8003
22	7.010355005	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47841/57786, ttl=64
23	7.011727836	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47841/57786, ttl=62
24	8.011847525	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47842/58042, ttl=64
25	8.013207054	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47842/58042, ttl=62
26	8.178577478	b0:aa:77:2b:75:6a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:68 Cost = 0 Port = 0x8003
27	9.013326698	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47843/58298, ttl=64
28	9.014709548	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47843/58298, ttl=62
29	10.014829852	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47844/58554, ttl=64
30	10.016170983	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47844/58554, ttl=62
31	10.178407988	b0:aa:77:2b:75:6a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:68 Cost = 0 Port = 0x8003
32	11.016275424	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47845/58810, ttl=64
33	11.017662452	172.10.30.11	172.20.50.3	ICMP	98	Echo (ping) reply id=0x0639, seq=47845/58810, ttl=62
34	12.017782904	172.20.50.3	172.10.30.11	ICMP	98	Echo (ping) request id=0x0639, seq=47846/59066, ttl=64

iv. 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.

I think that this policy is not secure. The internal workstations are not allowed to provide any services to the external computers. However, the internal servers can be accessed by the external computers through its web service. The problem arises due to the internal workstation being able to access the internal server through ssh and http. If the internal workstation is providing services to the internal server, it creates a vulnerability for the external computer to retrieve information through accessing the internal server's web service.