Lab: Firewall features the secured network and system (II)

Objective

In this lab the student will cover the following objectives:

- Understand the firewall security settings in SMB environments.
- Understand the security appliance advanced NAT.
- Practice on packet filtering, Stateful Packet Inspection (SPI), Conduit policy, and etc.
- Test access control—traffic shaping on security appliance.

Preparation

Begin with the standard lab topology and verify the starting configuration on the Cisco ASA 5505. Test the connectivity. Access the firewall console port using the terminal emulator on the student PC.

Tools and resources:

In order to complete the lab, the following is required:

- ASA 5505
- Console cable
- HyperTerminal
- Laptops with Windows OS

Lab tasks and steps

1. Read ASA's IOS version

```
ASA# show version
```

The IOS version is Cisco Adaptive Security Appliance Software Version 9.8(3)
Base license or Security Plus license:
License mode: Smart Licensing
ASAv Platform License State: Unlicensed
(Use Security Plus license in lab)

Reset factory-defaults on the firewall.

```
ASA# config t
ASA(config)# config  factory-default
```

Note: Read the default configuration from the output of ***show run*** command.

2. Initialize your group ASA 5505 with the following settings:

Interface	**Default Name**	**Default Security level**	**Phycial Interface(s) associated**	**Default IP address /Subnet mask**	**Default NAT Policy**
VLAN 1	**inside**	**100**	**E0/1-5**	**192.168.1.1/24**	**Nat (inside) 1 0 0**
VLAN 2	**outside**	**0**	E0/0	**110.1.1.1/24**	**Global(outside) 1 interface**
VLAN 3	**DMZ1**	**40**	E0/6	**192.168.3.1/24**	**Nat(DMZ1) 1 0 0**
VLAN 4	**DMZ2**	**80**	**E0/7**	**192.168.4.1/24**	**Nat(DMZ2) 1 0 0**

Verify VLANs and ports assignment by *show switch vlan* command, note down what you have observed, and compare with the table above:

____

____

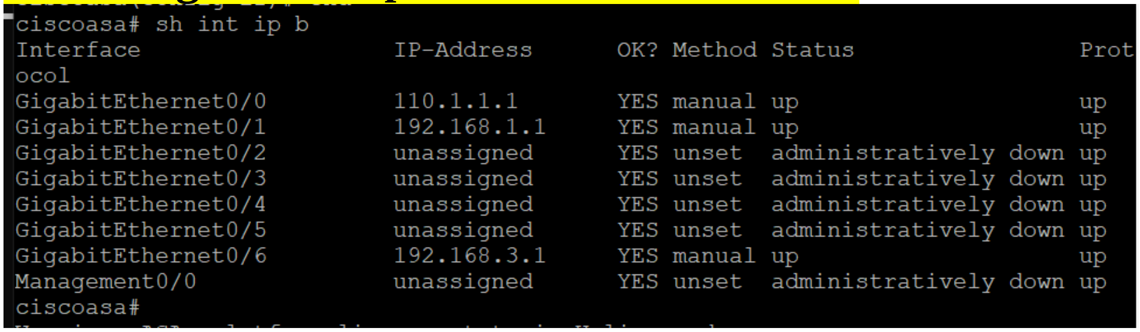
____

____.

```
int g0/1
ipaddress 192.168.1.1 255.255.255.0
no shut
nameif inside
int g0/0
ipaddress 110.1.1.1 255.255.255.0
no shut
nameif outside
```

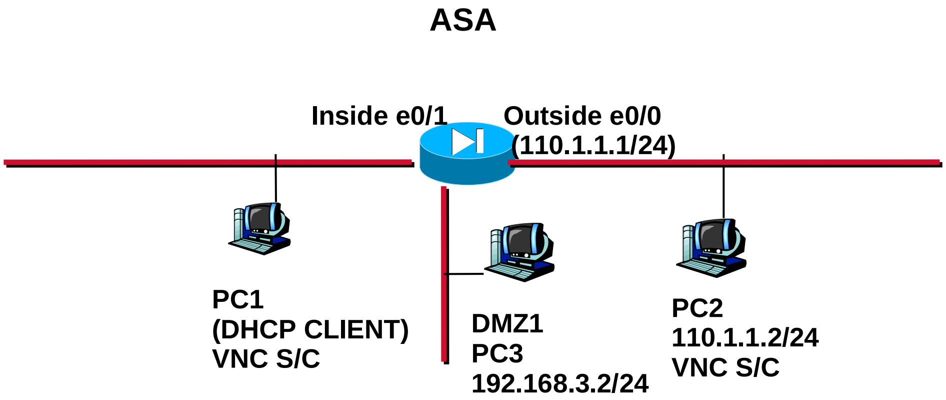
```
exit
dhcpd address 192.168.1.100-192.168.1.110 inside
dhcpd enable
```

Issue *show interface ip brief* command again, note down IP settings and compare with the table above:

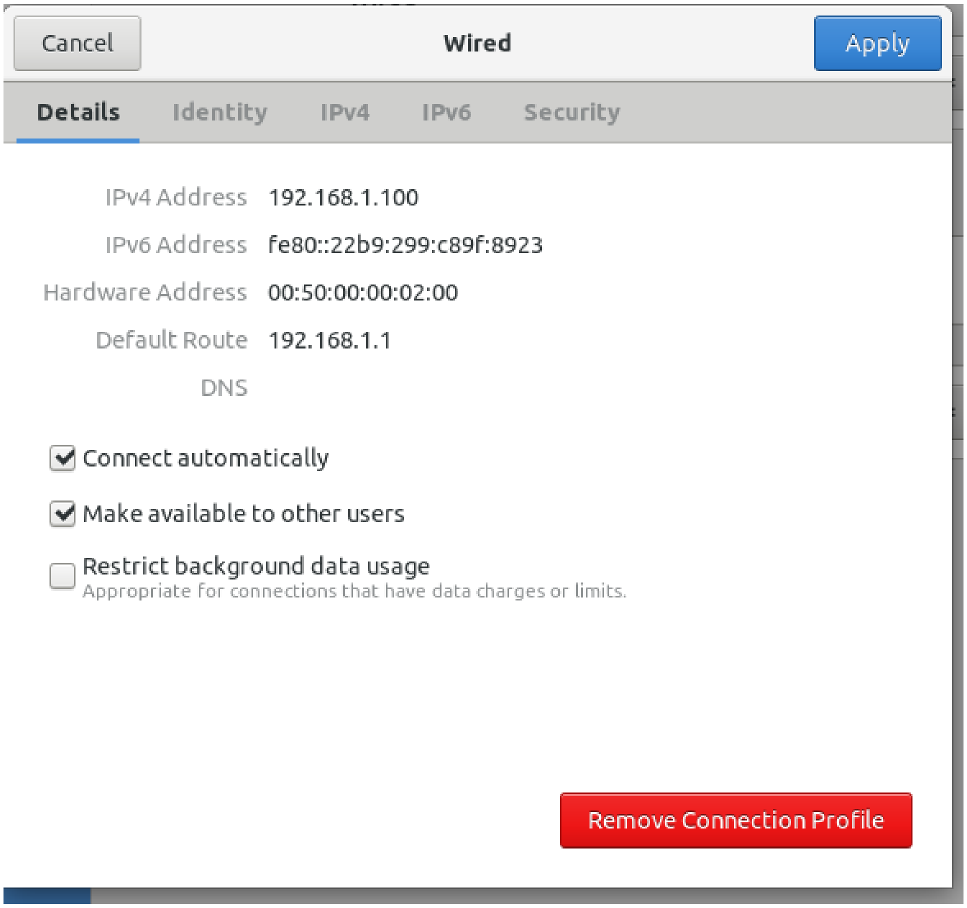


```
ciscoasa# sh int ip b
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/0         110.1.1.1       YES manual up                    up
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down up
GigabitEthernet0/3         unassigned      YES unset  administratively down up
GigabitEthernet0/4         unassigned      YES unset  administratively down up
GigabitEthernet0/5         unassigned      YES unset  administratively down up
GigabitEthernet0/6         192.168.3.1     YES manual up                    up
Management0/0              unassigned      YES unset  administratively down up
ciscoasa#
```

3. Set up the network as shown below. Review and test SPI.



a). Does PC1 retrieve a valid IP setting? YES. If so, list here



IPv4 Address 192.168.1.100

IPv6 Address fe80::22b9:299:c89f:8923

Hardware Address 00:50:00:00:02:00

Default Route 192.168.1.1

DNS

☑ Connect automatically

☑ Make available to other users

□ Restrict background data usage
Appropriate for connections that have data charges or limits.

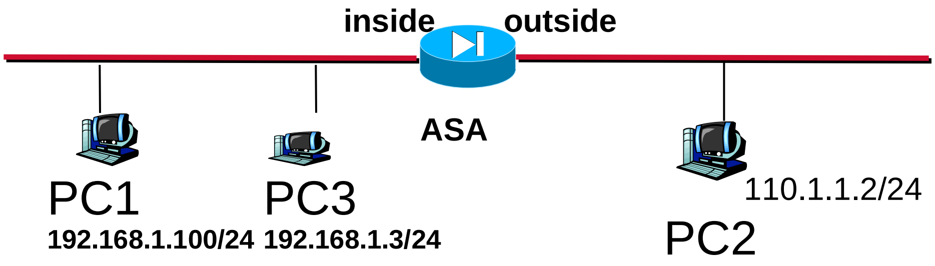
b). Test SPI, from PC1 VNC view PC2. Successful? NO

From PC3 VNC view PC2. Successful? _NO____ .

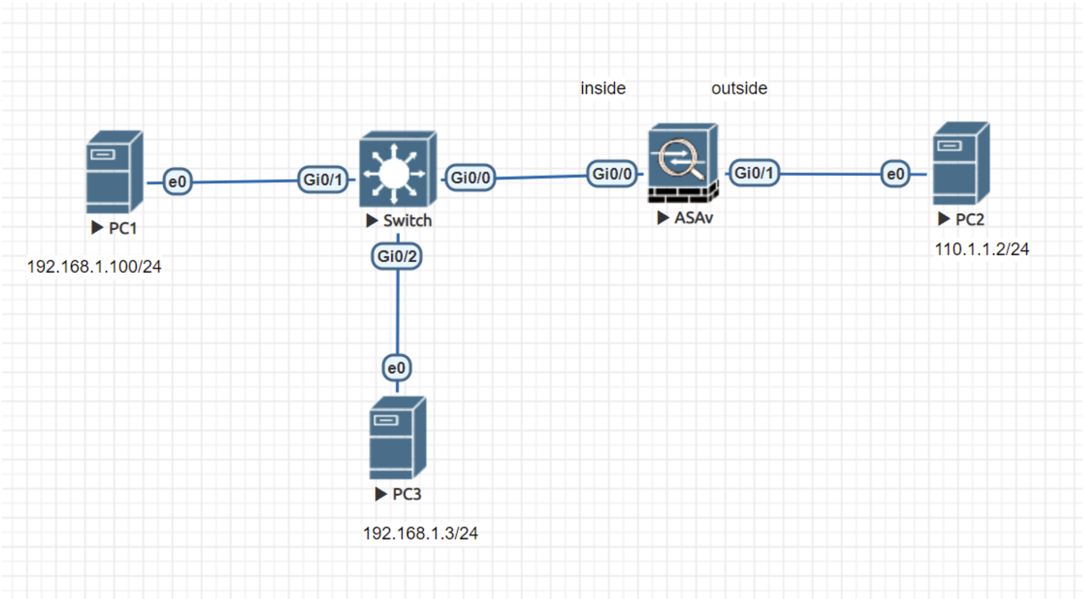
c). Verify the NAT policy by the command ***show xlate*****.**

List translation entries: 0 in staticuse, 0 most used

4. Adv. NAT policy on firewall

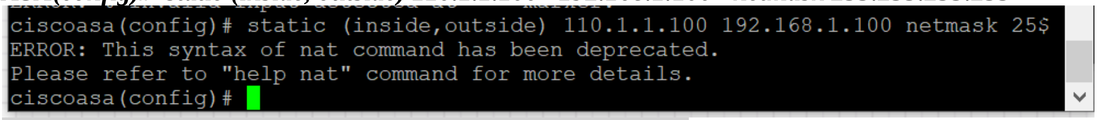


Form the above connections, and apply the right IP settings on PCs as shown in the map.



Set a static translation NAT entry on ASA5505 (only translates 192.168.1.100 to 110.1.1.100).

ASA(config)# static (inside, outside) 110.1.1.100   192.168.1.100   netmask 255.255.255.255

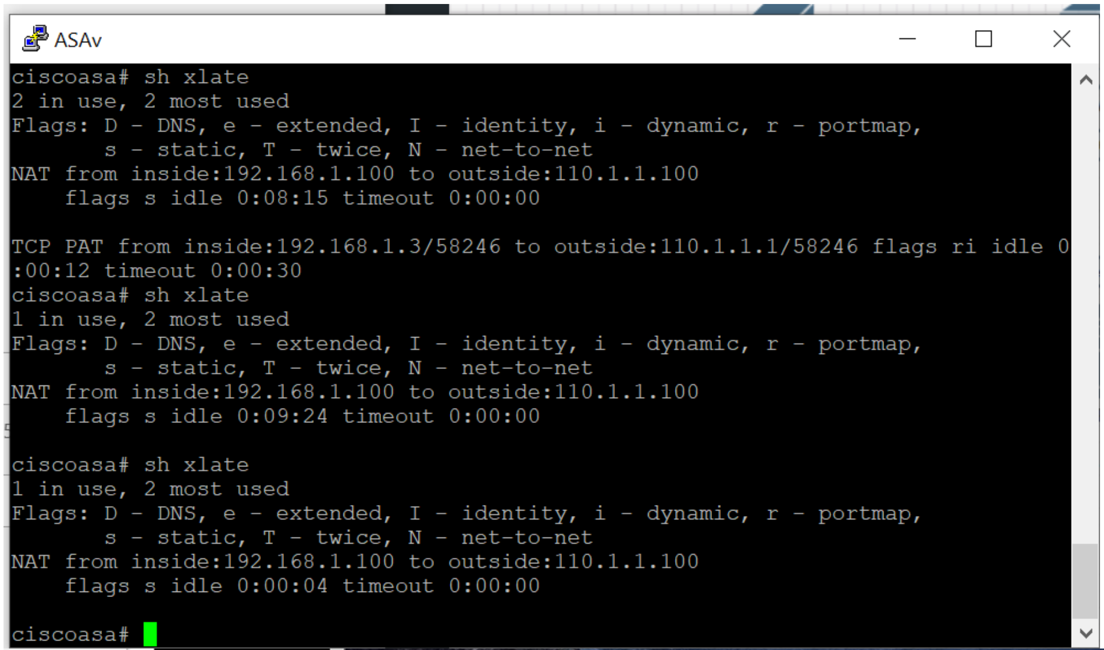


```
ciscoasa(config)# static (inside,outside) 110.1.1.100 192.168.1.100 netmask 25$
ERROR: This syntax of nat command has been deprecated.
Please refer to "help nat" command for more details.
ciscoasa(config)#
```

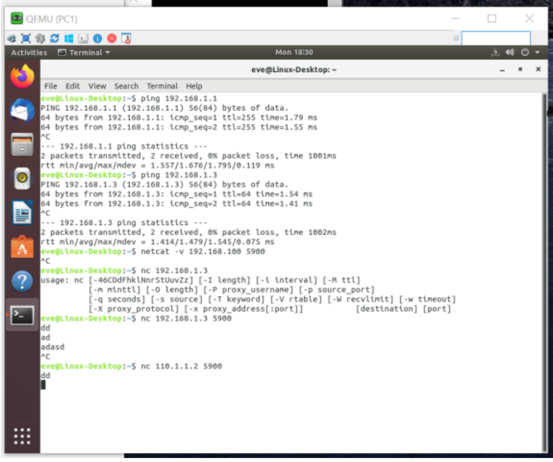
```
ciscoasa(config)# object network my-nat
ciscoasa(config-network-object)# host 192.168.1.100
ciscoasa(config-network-object)# nat (inside,outside) static
110.1.1.100
```

Again, from PC1 VNC view PC2**.** This traffic flow matches the above NAT policy—static NAT. Issue command ***show xlate.***

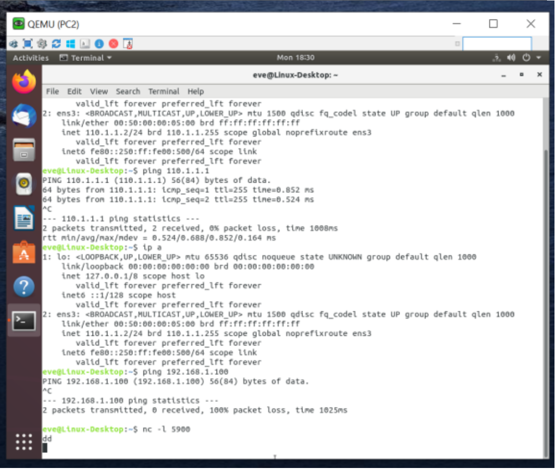
List translation entry here:



```
ciscoasa# sh xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:08:15 timeout 0:00:00

TCP PAT from inside:192.168.1.3/58246 to outside:110.1.1.1/58246 flags ri idle 0
:00:12 timeout 0:00:30
ciscoasa# sh xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:09:24 timeout 0:00:00

ciscoasa# sh xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:00:04 timeout 0:00:00

ciscoasa# 
```



```
eve@Linux-Desktop:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=1.79 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=1.55 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.557/1.676/1.795/0.119 ms
eve@Linux-Desktop:~$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=1.54 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=1.41 ms
^C
--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.414/1.479/1.545/0.075 ms
eve@Linux-Desktop:~$ netcat -v 192.168.100 5900
^C
eve@Linux-Desktop:~$ nc 192.168.1.3
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
eve@Linux-Desktop:~$ nc 192.168.1.3 5900
dd
ad
adasd
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900
dd
```

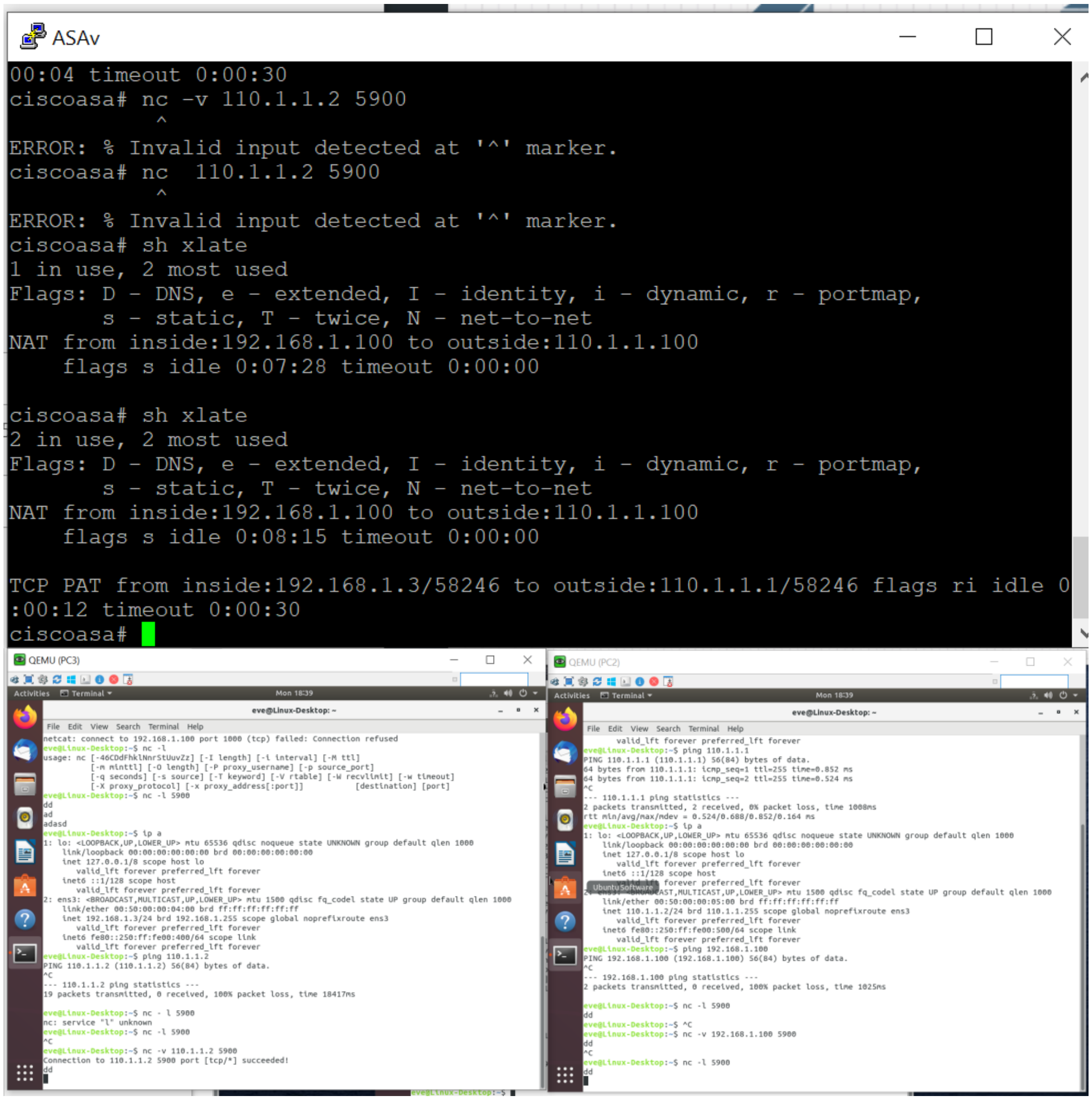


```
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:05:00 brd ff:ff:ff:ff:ff:ff
    inet 110.1.1.2/24 brd 110.1.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:500/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 110.1.1.1
PING 110.1.1.1 (110.1.1.1) 56(84) bytes of data.
64 bytes from 110.1.1.1: icmp_seq=1 ttl=255 time=0.852 ms
64 bytes from 110.1.1.1: icmp_seq=2 ttl=255 time=0.524 ms
^C
--- 110.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.524/0.688/0.852/0.164 ms
eve@Linux-Desktop:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:05:00 brd ff:ff:ff:ff:ff:ff
    inet 110.1.1.2/24 brd 110.1.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:500/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1025ms

eve@Linux-Desktop:~$ nc -l 5900
dd
```

From PC3 VNC view PC2, this traffic flow matches the default NAT policy—dynamic PAT.

```
ciscoasa(config)# object network my-pat ciscoasa(config-network-object)# host 192.168.1.3ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

List the output of ***show xlate***.



```
00:04 timeout 0:00:30
ciscoasa# nc -v 110.1.1.2 5900
                  ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa# nc  110.1.1.2 5900
                  ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa# sh xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:07:28 timeout 0:00:00

ciscoasa# sh xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:08:15 timeout 0:00:00

TCP PAT from inside:192.168.1.3/58246 to outside:110.1.1.1/58246 flags ri idle 0
:00:12 timeout 0:00:30
ciscoasa#
```

```
netcat: connect to 192.168.1.100 port 1000 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc -l
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
eve@Linux-Desktop:~$ nc -l 5900
dd
ad
adasd
eve@Linux-Desktop:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:04:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:400/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 110.1.1.2
PING 110.1.1.2 (110.1.1.2) 56(84) bytes of data.
^C
--- 110.1.1.2 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18417ms

eve@Linux-Desktop:~$ nc - l 5900
nc: service "l" unknown
eve@Linux-Desktop:~$ nc -l 5900
^C
eve@Linux-Desktop:~$ nc -v 110.1.1.2 5900
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
dd
```

```
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 110.1.1.1
PING 110.1.1.1 (110.1.1.1) 56(84) bytes of data.
64 bytes from 110.1.1.1: icmp_seq=1 ttl=255 time=0.852 ms
64 bytes from 110.1.1.1: icmp_seq=2 ttl=255 time=0.524 ms
^C
--- 110.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.524/0.688/0.852/0.164 ms
eve@Linux-Desktop:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:05:00 brd ff:ff:ff:ff:ff:ff
    inet 110.1.1.2/24 brd 110.1.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:500/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1025ms

eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -v 192.168.1.100 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
dd
```

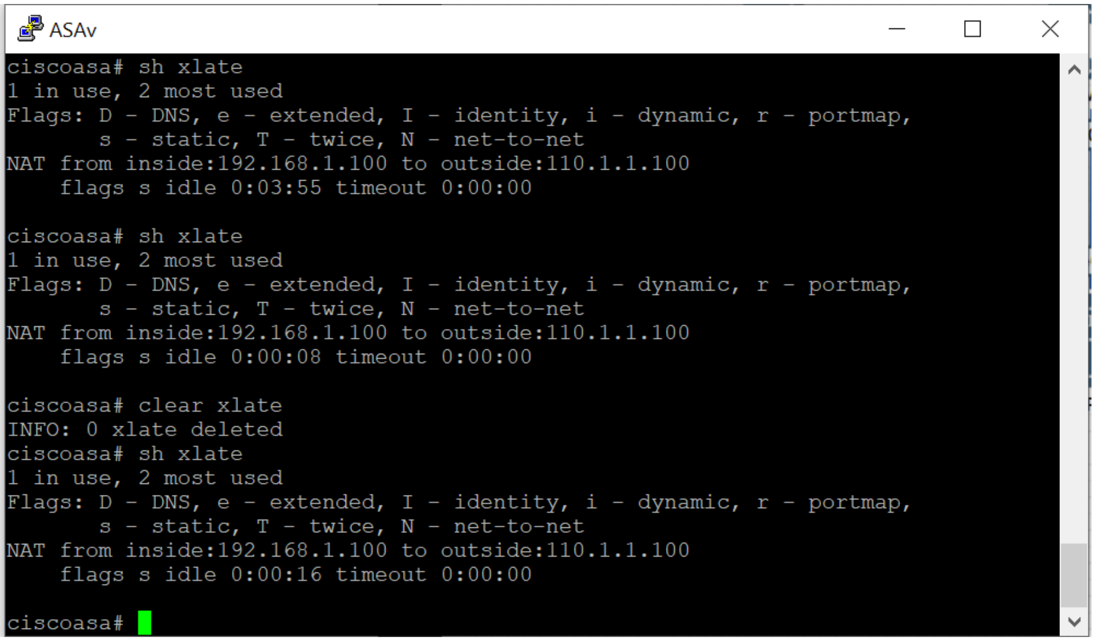
From the above two translation outputs, try to figure out the difference between static NAT and dynamic PAT.

PAT translate single port as a target port.

NAT translates all the ports into new target IP

Issue command ***clear xlate*** to clear all the translations as follows.

ASA# clear xlate



```
ciscoasa# sh xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:03:55 timeout 0:00:00

ciscoasa# sh xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:00:08 timeout 0:00:00

ciscoasa# clear xlate
INFO: 0 xlate deleted
ciscoasa# sh xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.100 to outside:110.1.1.100
    flags s idle 0:00:16 timeout 0:00:00

ciscoasa# 
```

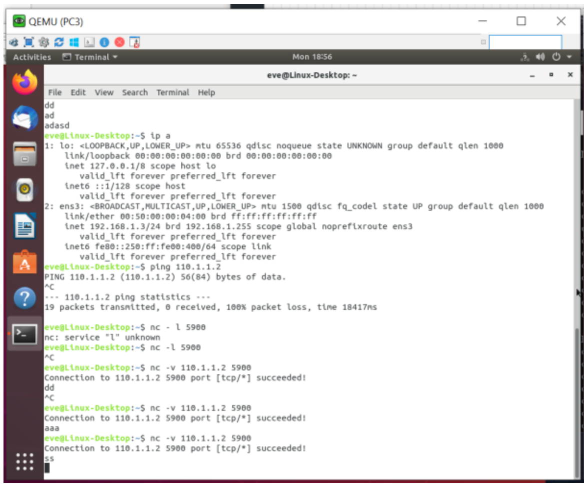
From PC1 and PC3, ping PC2 (note: it is not pingable since the firewall blocks the ICMP reply messages, but you will see the ICMP request messages still can go through the firewall and trigger NAT entry in NAT table), then repeat the last command (***ASA# show xlate)*** . Again, verify the difference between static NAT and dynamic PAT. Notes: My NAT is static, after clearing it is still there. My PAT is dynamic, it will be distorted after the connection is closed.

5. Packet Filtering by Access Control list

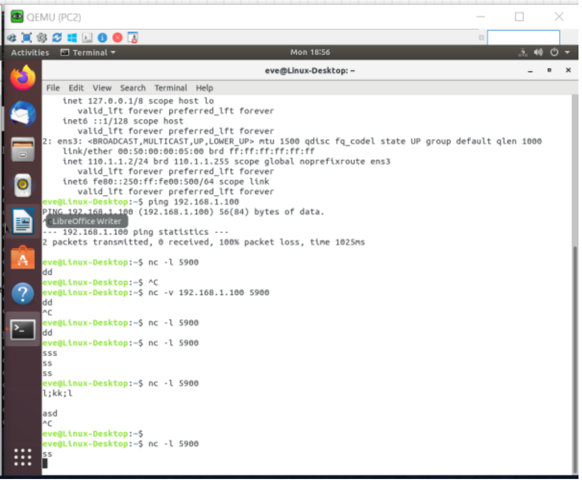
Set and test filtering policy: allow PC3 to access PC2, but deny PC1 to access PC2. Command options:

access-list 150 deny ip host 192.168.1.100 host 110.1.1.2
access-list 150 permit ip any any
access-group 150 in interface inside

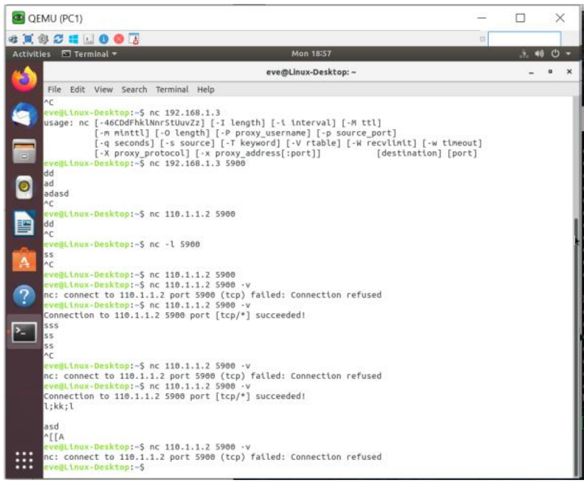
Test by PC1/PC3's VNC Viewer application and note down results:



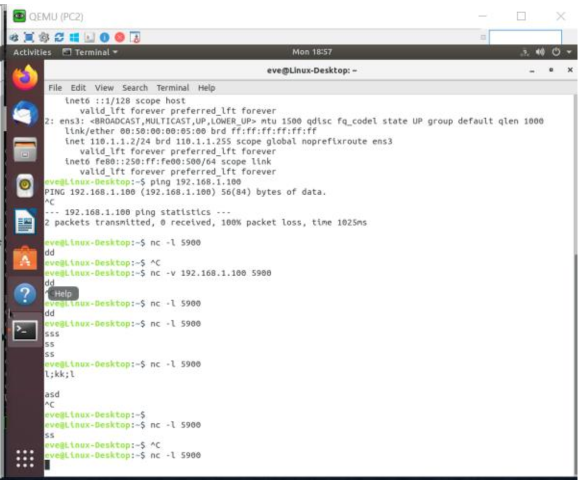
```
dd
ad
adasd
eve@Linux-Desktop:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:04:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:400/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 110.1.1.2
PING 110.1.1.2 (110.1.1.2) 56(84) bytes of data.
^C
--- 110.1.1.2 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18417ms

eve@Linux-Desktop:~$ nc - l 5900
nc: service "l" unknown
eve@Linux-Desktop:~$ nc -l 5900
^C
eve@Linux-Desktop:~$ nc -v 110.1.1.2 5900
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
dd
^C
eve@Linux-Desktop:~$ nc -v 110.1.1.2 5900
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
aaa
eve@Linux-Desktop:~$ nc -v 110.1.1.2 5900
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
ss
```



```
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:05:00 brd ff:ff:ff:ff:ff:ff
    inet 110.1.1.2/24 brd 110.1.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:500/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1025ms

eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -v 192.168.1.100 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ nc -l 5900
sss
ss
ss
eve@Linux-Desktop:~$ nc -l 5900
l;kk;l

asd
^C
eve@Linux-Desktop:~$
eve@Linux-Desktop:~$ nc -l 5900
ss
```



```
^C
eve@Linux-Desktop:~$ nc 192.168.1.3
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
eve@Linux-Desktop:~$ nc 192.168.1.3 5900
dd
ad
adasd
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
ss
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
sss
ss
ss
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
l;kk;l

asd
^[[A
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$
```



```
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:05:00 brd ff:ff:ff:ff:ff:ff
    inet 110.1.1.2/24 brd 110.1.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:500/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1025ms

eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -v 192.168.1.100 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ nc -l 5900
sss
ss
ss
eve@Linux-Desktop:~$ nc -l 5900
l;kk;l

asd
^C
eve@Linux-Desktop:~$
eve@Linux-Desktop:~$ nc -l 5900
ss
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -l 5900
```

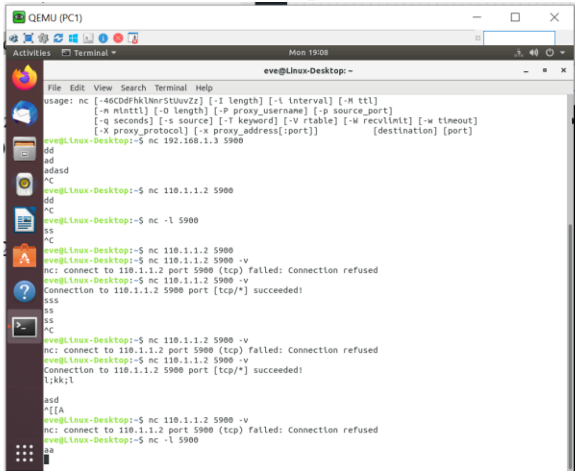
6. Set and test conduit policies

a). Policy 1: enable general IP access from PC2 to PC1

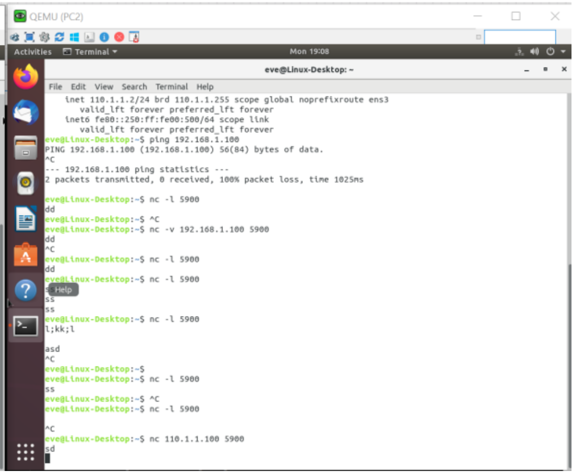
ASA(config)# access-list 120 permit ip host <u>110.1.1.2</u> host <u>110.1.1.100</u>
ASA(config)# access-group 120 in interface <u>outside</u>

Note: the destination IP address has to be **the translated address (110.1.1.100)**, instead of **the real addres**s assigned on PC1 (192.168.1.100). Why?
From outside, 110.1.100 and 110.1.1.1 are in the same conflict domain. To PC2, only 110.1.1.100 is visible.

Now test the VNC service from PC2 (VNC viewer in lower security level zone) to PC1 (VNC server in higher zone) by using the **translated address (10.1.1.100)** as destination address. Successful? nope

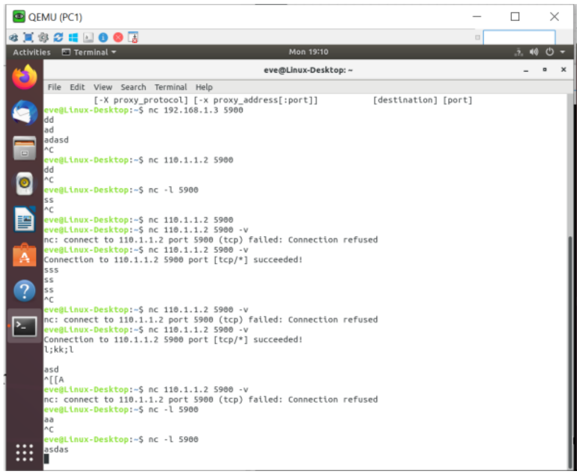


```
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
eve@Linux-Desktop:~$ nc 192.168.1.3 5900
dd
ad
adasd
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
ss
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
sss
ss
ss
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
l;kk;l

asd
^[[A
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc -l 5900
aa
```

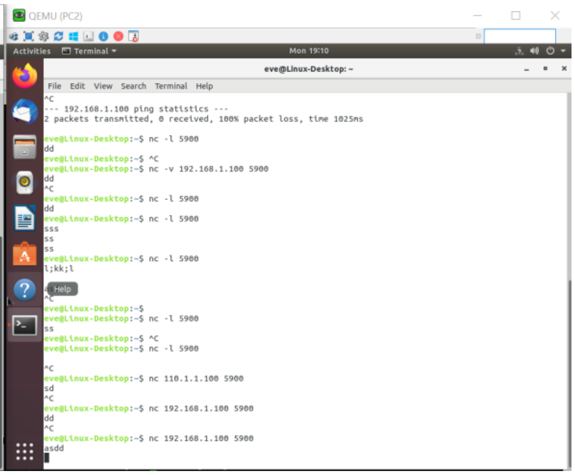


```
    inet 110.1.1.2/24 brd 110.1.1.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::250:ff:fe00:500/64 scope link
       valid_lft forever preferred_lft forever
eve@Linux-Desktop:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1025ms

eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -v 192.168.1.100 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ nc -l 5900
ss
ss
ss
eve@Linux-Desktop:~$ nc -l 5900
l;kk;l

asd
^C
eve@Linux-Desktop:~$
eve@Linux-Desktop:~$ nc -l 5900
ss
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -l 5900

^C
eve@Linux-Desktop:~$ nc 110.1.1.100 5900
sd
```

What happens if you use PC1’s **the real addres** (192.168.1.100) from PC2’s viewer window? Still not working .



```
           [-X proxy_protocol] [-x proxy_address[:port]]          [destination] [port]
eve@Linux-Desktop:~$ nc 192.168.1.3 5900
dd
ad
adasd
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
ss
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
sss
ss
ss
^C
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
Connection to 110.1.1.2 5900 port [tcp/*] succeeded!
l;kk;l

asd
^[[A
eve@Linux-Desktop:~$ nc 110.1.1.2 5900 -v
nc: connect to 110.1.1.2 port 5900 (tcp) failed: Connection refused
eve@Linux-Desktop:~$ nc -l 5900
aa
^C
eve@Linux-Desktop:~$ nc -l 5900
asdas
```



```
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1025ms

eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -v 192.168.1.100 5900
dd
^C
eve@Linux-Desktop:~$ nc -l 5900
dd
eve@Linux-Desktop:~$ nc -l 5900
sss
ss
ss
eve@Linux-Desktop:~$ nc -l 5900
l;kk;l

as
^C
eve@Linux-Desktop:~$
eve@Linux-Desktop:~$ nc -l 5900
ss
eve@Linux-Desktop:~$ ^C
eve@Linux-Desktop:~$ nc -l 5900

^C
eve@Linux-Desktop:~$ nc 110.1.1.100 5900
sd
^C
eve@Linux-Desktop:~$ nc 192.168.1.100 5900
dd
^C
eve@Linux-Desktop:~$ nc 192.168.1.100 5900
asdd
```

b). Policy 2: enable ICMP in conduit policy so that PC1 to ***PING*** PC2.

ASA(config)# access-list 140 permit icmp host 110.1.1.2 host 110.1.1.100
ASA(config)# access-group 140 in interface outside

Test ICMP, from PC1 ***PING*** PC2.   Successful? Nope.
Can PC3 ping PC2? _Nope___ .
Can PC2 ping PC1 (by 110.1.1.100)? _Nope .
Can PC2 ping PC3 (by 110.1.1.1)? .Yes

7. Free practice/testing:

a). Traffic shaping between DMZ1 and outside zone pair, test by VNC service.
Notes:

b). Create a static NAT policy for one DMZ2 host with its own translated IP address (for example, 110.1.1.80). Implement and test this NAT policy.
Notes:

c). Set a conduit policy to allow PC2 in outside zone to VNC view a VNC server in DMZ2 zone.

Notes: