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

Objective

In this lab the student will cover the following objectives:
• Understand the firewall security settings
• Understand the firewall application in different scenarios
• Practice on NAT, packet filtering, Stateful Packet Inspection (SPI), etc.
• Test connectivity

Scenario

Four scenarios will be covered in this lab to simulate the SMB security systems:

- DHCP configurations on firewall
- NAT
- Stateful Packet Inspection (SPI)

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)
Firepower Extensible Operating System Version 2.2(2.90i)
Device Manager Version 7.8(2)
Base license or Security Plus license
License mode: Smart Licensing
ASAv Platform License State: Unlicensed

Reset factory-defaults on the firewall.

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

Note down the system process.

_____
_____.

Read the default configuration from the output of ***show run*** command, and fill up the following table.

Interface	Default Name	Default Security level	Phycial Interface(s) associated	Default IP address /Subnet mask	Default NAT Policy
VLAN 1					
VLAN 2					

Create a new VLAN3 (Name: DMZ) with Security level ***50***.

ASA (conf)# int gi0/1
ASA (conf-if)# nameif DMZ
ASA (conf-if)# security-level 50
ASA (conf)# int gi0/5
ASA (conf-if)# nameif outside

Assign 172.16.1.1/24 to the VLAN interface.

ASA (conf-if)# ip address 172.16.1.1 255.255.255.0

Put interface e0/7 into the new VLAN (DMZ)

ASA (conf)# int e0/7
ASA (conf-if)#switchport access vlan 3

Put interface e0/5 into the VLAN 2 (outside)

ASA (conf)# int e0/5
ASA (conf-if)#switchport access vlan 2

Assign 110.1.1.1/24 on outside zone interface (interface vlan 2)

ASA(config)# int int g0/5
ASA(config-if)# ip address 110.1.1.1 255.255.255.0

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

_____
_____
_____
_____.

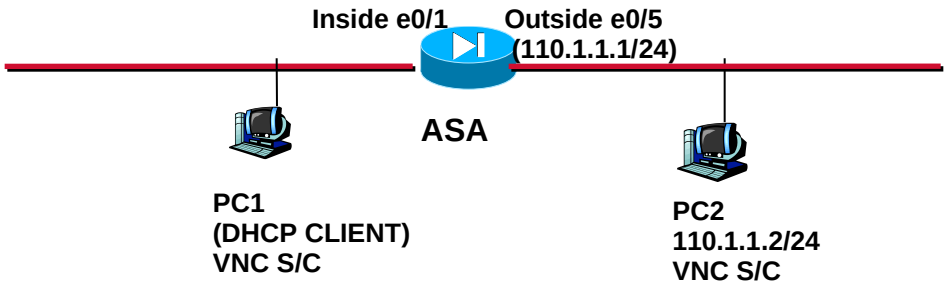
Issue *show interface ip brief* command again, note down IP settings and compare with the table above:

```
983
GigabitEthernet0/0         unassigned      YES unset  administratively down up
GigabitEthernet0/1         172.16.1.1      YES manual administratively down 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         110.1.1.1       YES manual up                    up
GigabitEthernet0/6         unassigned      YES unset  administratively down up
Management0/0              unassigned      YES unset  administratively down up
ciscoasa# conf t
ciscoasa(config)# int g0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# end
ciscoasa# sh int ip b
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/0         unassigned      YES unset  administratively down up
GigabitEthernet0/1         172.16.1.1      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         110.1.1.1       YES manual up                    up
GigabitEthernet0/6         unassigned      YES unset  administratively down up
Management0/0              unassigned      YES unset  administratively down up
ciscoasa#
```

3. ASA DHCP server/client testing

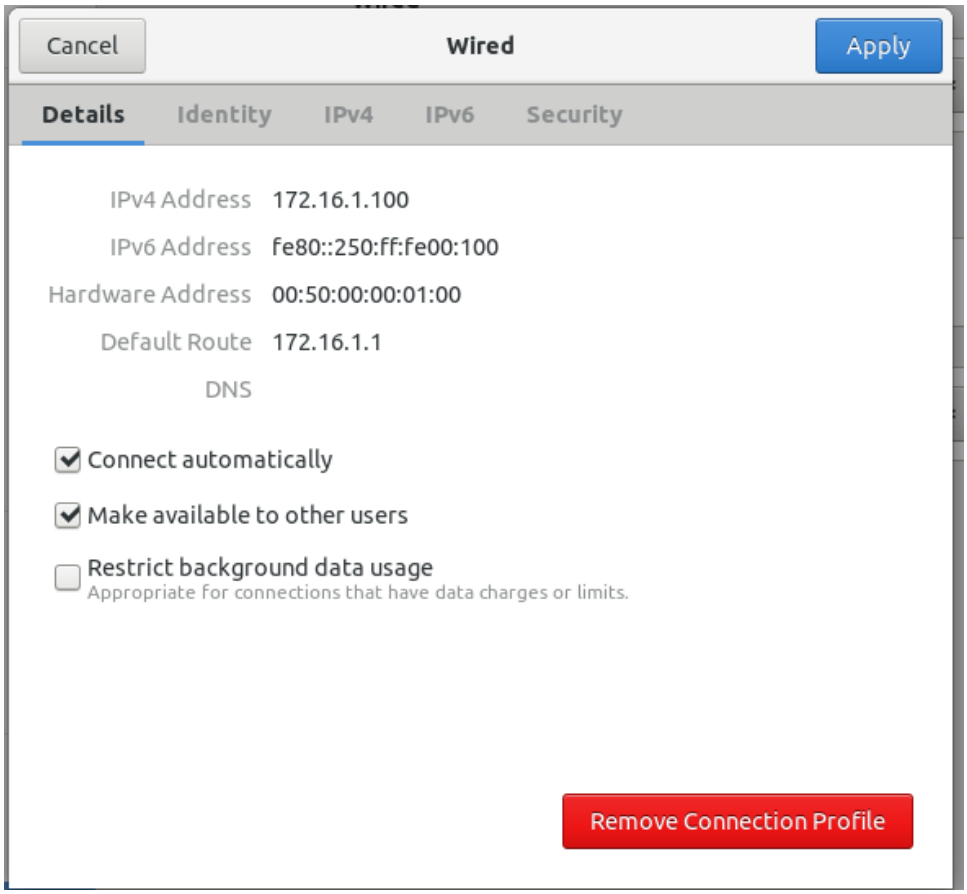
By default ASA is configured as both DHCP server and client. Outside interface obtains IP address from outside zone DHCP se16rver (if available) while inside zone hosts get IP settings from ASA5505 inside interface.

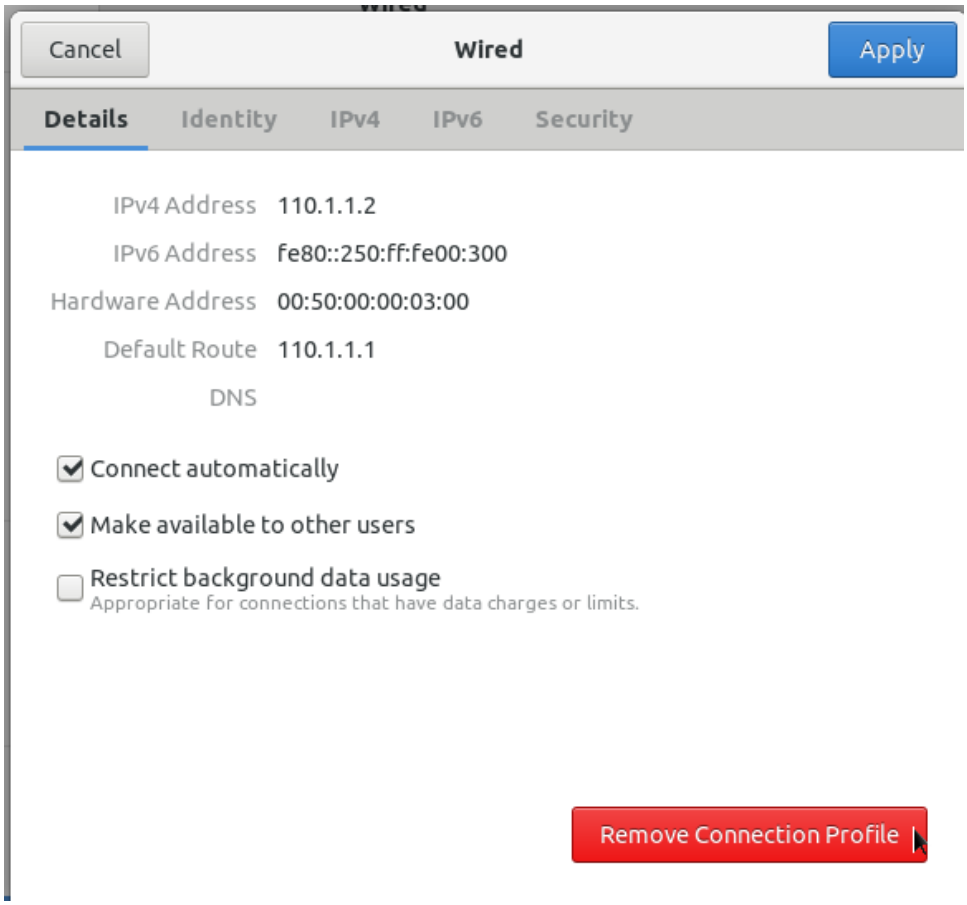
Ciscoasa(config)#dhcpd address 172.16.1.100-172.16.1.110 DMZ
Ciscoasa(config)#dhcpd enable DMZ
Ciscoasa(config)#dhcpd address 110.1.1.2-110.1.1.10 outside
Ciscoasa(config)#dhcpd enable outside



Set the above Scenario.

Does PC1 retrieve a valid IP setting? YES . If so, list here 172.16.1.100/24





4. NAT policy on firewall

a). Read the two commands (from ***show run)*** that set ASA default NAT policy--means that all inside zone hosts' IP addresses will be translated into outside zone interface's IP address.
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0

Issue command ***show xlate*** to get the translation table as follows.
ASA# show xlate

Are there any translation entries? If available, list here:

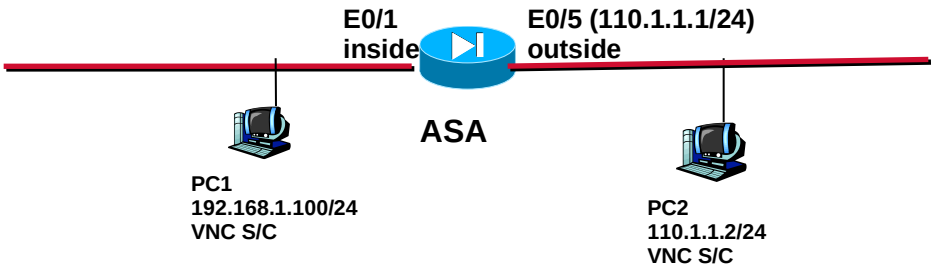
```
ciscoasa(config)# sh xlate
0 in use, 0 most used

ciscoasa(config)#
```

From PC1, 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)*** . Are there any translation entries? If available, list here:
_____.

5. SPI testing



Based on the same scenario.

a). Set PC2 as VNC server, from PC1 (VNC viewer) initiate a VNC session. Successful? If yes, issue command ***show xlate*** to get the translation table as follows.
Are there any translation entries? If available, list here:

object network obj-172.16.1.0
subnet 172.16.1.0 255.255.255.0
object network obj-natted
range 110.1.1.11 110.1.1.19
object network obj-172.16.1.0
nat (DMZ,outside) dynamic obj-natted

Logging enable
Logging buffered 6

Sh log

```
ciscoasa# sh log
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: level debugging, 69 messages logged
    Monitor logging: level debugging, 73 messages logged
    Buffer logging: level debugging, 67 messages logged
    Trap logging: level debugging, facility 20, 54 messages logged
    Global TCP syslog stats::
        NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
        CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
        PARTIAL_REWRITE_CNT: 0
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
%ASA-5-111008: User 'enable_15' executed the 'clear logging buffer' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'clear logging buffer'
%ASA-7-111009: User 'enable_15' executed cmd: show logging
%ASA-7-111009: User 'enable_15' executed cmd: show logging
%ASA-7-111009: User 'enable_15' executed cmd: show logging
<--- More --->
```

Sh xlate

Sh nat

```
ciscoasa# sh xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

NAT from DMZ:172.16.1.100 to outside:110.1.1.13 flags i idle 0:00:06 timeout 3:00:00
ciscoasa# sh nat

Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source dynamic obj-172.16.1.0 obj-natted
    translate_hits = 2, untranslate_hits = 8
ciscoasa#
```

If not, test IP connectivity.

b). Set PC1 as VNC server, from PC2 (VNC viewer) initiate a VNC session (note: view the PC1's translated IP address 110.1.1.1). Successful? Why?

```
eve@Linux-Desktop:~$ netcat -v 110.1.1.13 500
^C
eve@Linux-Desktop:~$
```

```
%ASA-2-106001: Inbound TCP connection denied from 110.1.1.2/51924 to 172.16.1.100/500 flags SYN  on interface ou
tside
```

The packet is denied by ASA due to the source security level 0(outside) is lower than the destination level 50(DMZ).

6. Free practice/testing:

a). Utilizing DMZ zone, test Remote Desktop Connection/VNC service in between inside zone and DMZ zone.

Notes:

b). Create a new security level zone (for example DMZ-Partner), assign a new set of interface settings (security-level, name, IP address/mask, physical interface, etc.)

Notes: