Lab cấu hình cơ bản firewall asa

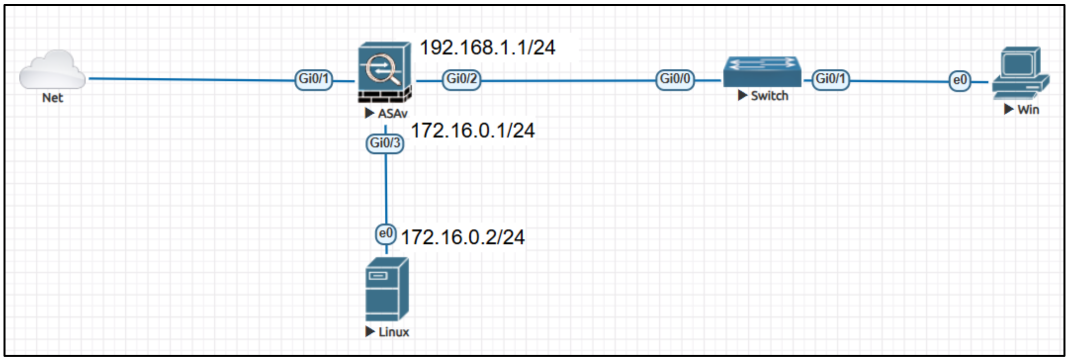
Chuẩn bị

- Một Firewall asa
- Một máy window đặt ip tĩnh 192.168.1.2
- Một máy linux đặt ip tĩnh 172.16.0.1

Mục tiêu

- Khảo sát các chế độ dòng lệnh trên Firewall ASA.
- Thực hành đặt tên(hostname) cho asa.
- Cấu hình IP trên các interface của Firewall ASA.
- Cấu hình cho phép ICMP từ vùng Inside tới vùng DMZ.
- Cấu hình cấp DHCP vùng Inside.
- Cấu hình NAT overload.
- Cấu hình NAT Overload trên Firewall ASA cho phép các PC thuộc Inside Zone truy cập được
- Lưu lại cấu hình trên Firewall ASA.

Mô hình

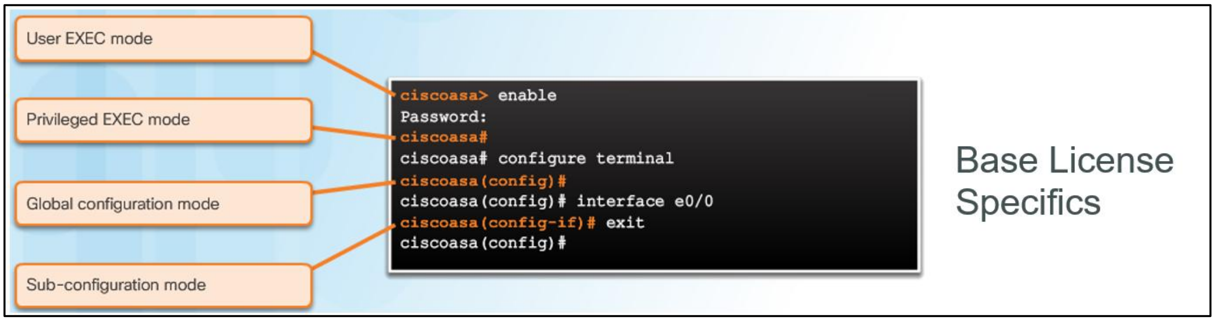


Mô tả: Mô hình gồm 1 firewall kết nối với internet qua cổng Gi0/1, vùng DMZ có subnet là 172.16.0.0/24 chứa một máy linux, Vùng client là vùng có subnet 192.168.1.0/24 gồm 1 switch và 1 máy window.

Phần thực hành

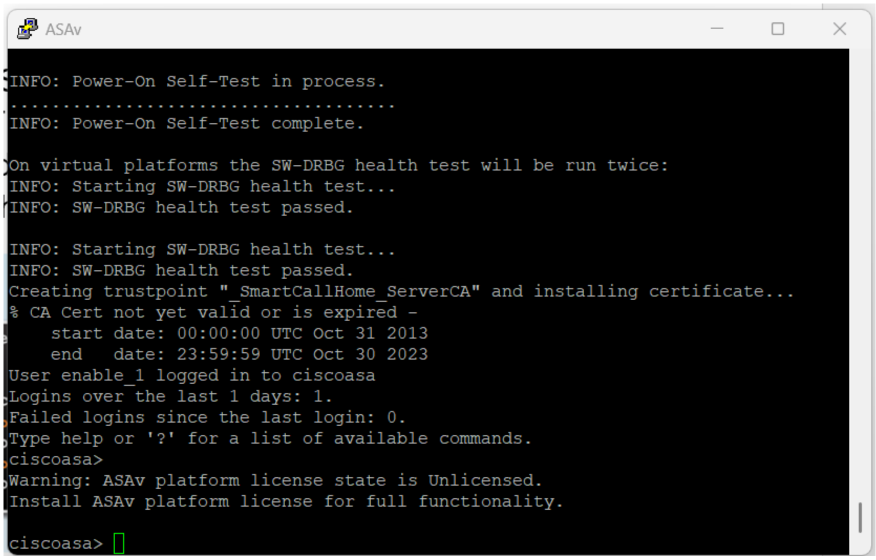
1. Thực hành khảo sát các chế độ dòng lệnh trên Firewall ASA

Bên dưới là các chế độ dòng lệnh trên asa.



```
ciscoasa> enable
Password:
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)#
ciscoasa(config)# interface e0/0
ciscoasa(config-if)# exit
ciscoasa(config)#
```

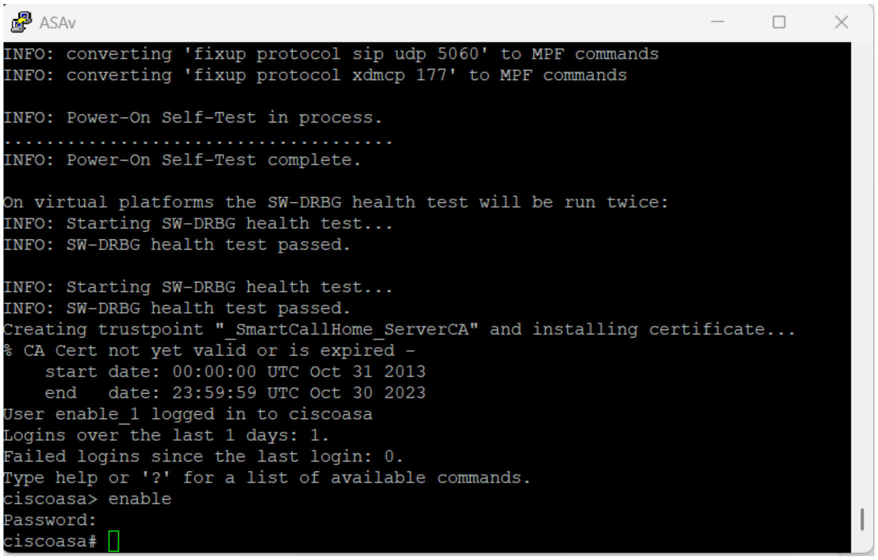
Khi khởi động lên asa sẽ ở chế độ EXEC Mode



```
INFO: Power-On Self-Test in process.
.....................................
INFO: Power-On Self-Test complete.

On virtual platforms the SW-DRBG health test will be run twice:
INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.
Creating trustpoint "_SmartCallHome_ServerCA" and installing certificate...
% CA Cert not yet valid or is expired -
    start date: 00:00:00 UTC Oct 31 2013
    end   date: 23:59:59 UTC Oct 30 2023
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa>
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.

ciscoasa>
```

Để vào chế độ Privileged EXEC Mode dùng lệnh

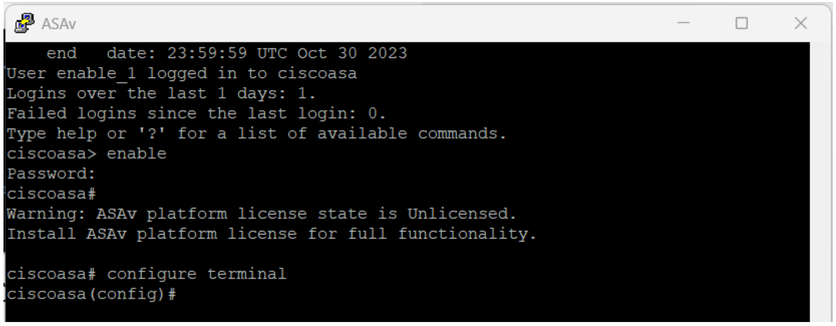
```
ciscoasa> enable
Password: # Nhấn enter khi chưa đặt mật khẩu
```



```
INFO: converting 'fixup protocol sip udp 5060' to MPF commands
INFO: converting 'fixup protocol xdmcp 177' to MPF commands

INFO: Power-On Self-Test in process.
.....................................
INFO: Power-On Self-Test complete.

On virtual platforms the SW-DRBG health test will be run twice:
INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.
Creating trustpoint "_SmartCallHome_ServerCA" and installing certificate...
% CA Cert not yet valid or is expired -
    start date: 00:00:00 UTC Oct 31 2013
    end   date: 23:59:59 UTC Oct 30 2023
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa#
```

Để vào chế độ Global Configuration Mode dùng lệnh

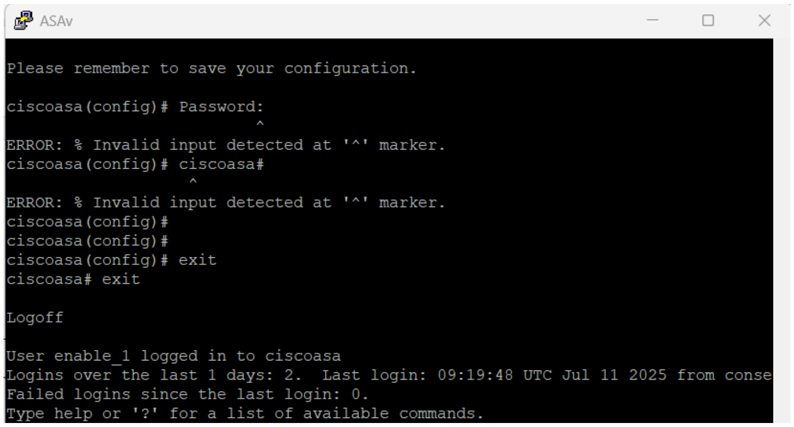
```
ciscoasa# configure terminal
```



```
    end   date: 23:59:59 UTC Oct 30 2023
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa#
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.

ciscoasa# configure terminal
ciscoasa(config)#
```

Để trở về chế độ trước đó sử dụng lệnh

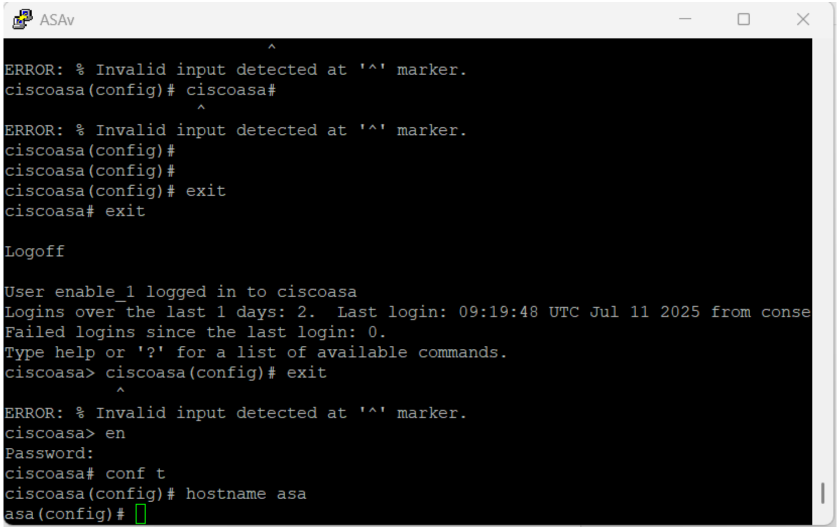
```
ciscoasa(config)# exit

ciscoasa#exit
```



```

Please remember to save your configuration.

ciscoasa(config)# Password:
                          ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa(config)# ciscoasa#
                   ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)# exit
ciscoasa# exit

Logoff

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 2.  Last login: 09:19:48 UTC Jul 11 2025 from conse
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
```

2. Thực hành đặt tên(hostname) cho asa.

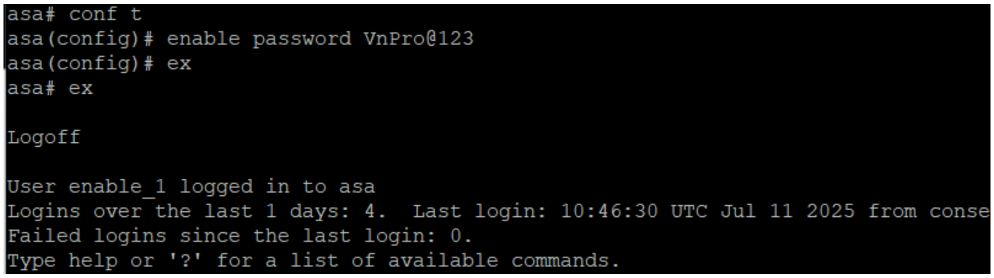
```
ciscoasa> en
Password:
ciscoasa# conf t
ciscoasa(config)# hostname asa
```



```
                          ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa(config)# ciscoasa#
                   ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)# exit
ciscoasa# exit

Logoff

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 2.  Last login: 09:19:48 UTC Jul 11 2025 from conse
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> ciscoasa(config)# exit
           ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa> en
Password:
ciscoasa# conf t
ciscoasa(config)# hostname asa
asa(config)#
```

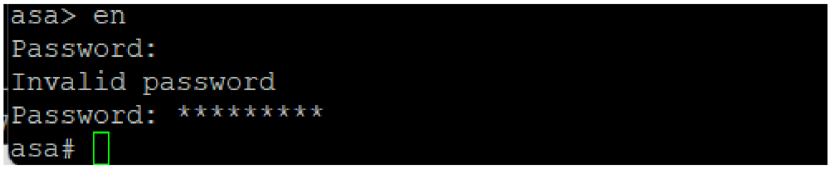
3. Cấu hình password cho ASA

```
asa# conf t
asa(config)# enable password VnPro@123
asa(config)# exit
asa# exit
```



```
asa# conf t
asa(config)# enable password VnPro@123
asa(config)# ex
asa# ex

Logoff

User enable_1 logged in to asa
Logins over the last 1 days: 4.  Last login: 10:46:30 UTC Jul 11 2025 from conse
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
```

Kiểm tra lại bằng cách exit ra Privileged EXEC Mode, sau đó vào enable, nhập mật khẩu.

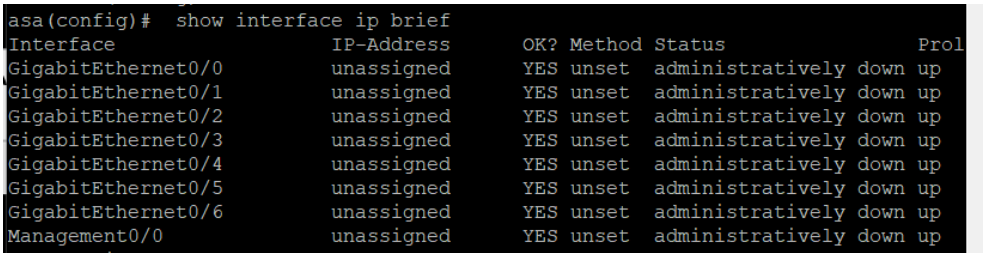


```
asa> en
Password:
Invalid password
Password: *********
asa#
```

4. Cấu hình IP trên các interface của Firewall ASA.

Để xem thông tin interface dùng lệnh

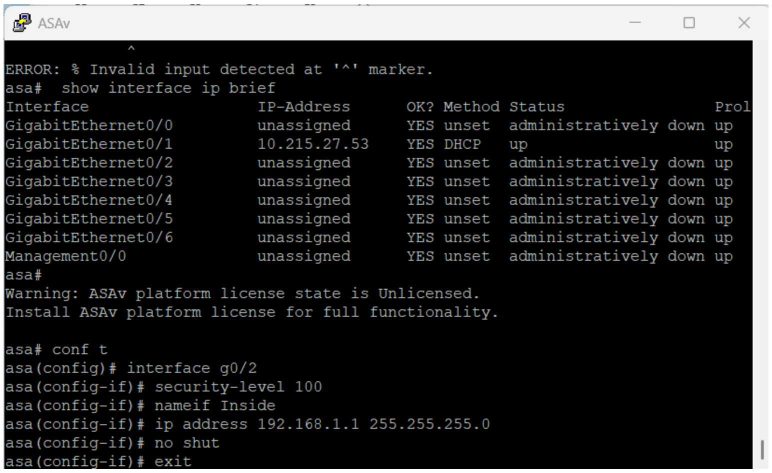
```
asa# show interface ip brief
```



```
asa(config)#  show interface ip brief
Interface                  IP-Address      OK? Method Status                Prol
GigabitEthernet0/0         unassigned      YES unset  administratively down up
GigabitEthernet0/1         unassigned      YES unset  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         unassigned      YES unset  administratively down up
GigabitEthernet0/6         unassigned      YES unset  administratively down up
Management0/0              unassigned      YES unset  administratively down up
```

Cấu hình ip trên interface gigabitEthernet0/2

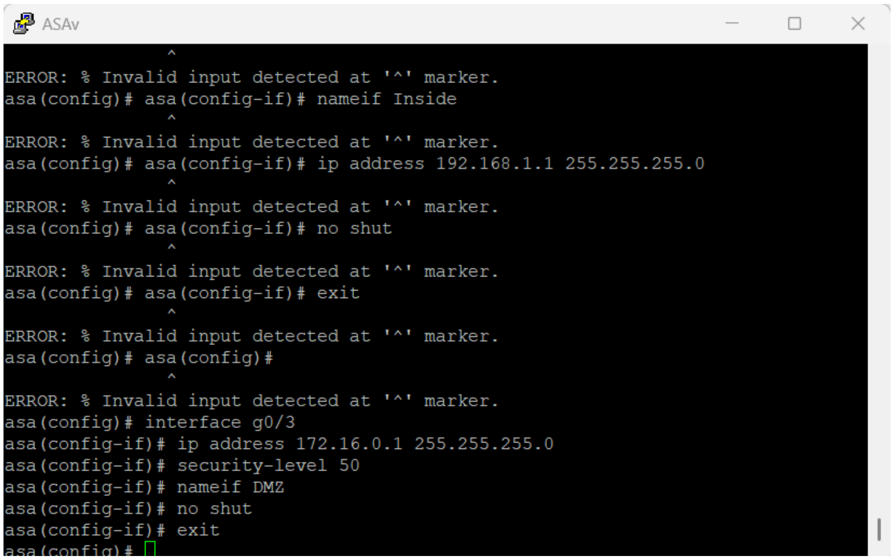
```
asa(config)# interface g0/2 # truy cập interface
asa(config-if)# security-level 100 # gán mức độ security
asa(config-if)# nameif Inside #đặt tên cho interface
asa(config-if)# ip address 192.168.1.1 255.255.255.0 #gán địa chỉ ip
asa(config-if)# no shut
asa(config-if)# exit
```



```
              ^
ERROR: % Invalid input detected at '^' marker.
asa#  show interface ip brief
Interface                  IP-Address      OK? Method Status                Prol
GigabitEthernet0/0         unassigned      YES unset  administratively down up
GigabitEthernet0/1         10.215.27.53    YES DHCP   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         unassigned      YES unset  administratively down up
Management0/0              unassigned      YES unset  administratively down up
asa#
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.

asa# conf t
asa(config)# interface g0/2
asa(config-if)# security-level 100
asa(config-if)# nameif Inside
asa(config-if)# ip address 192.168.1.1 255.255.255.0
asa(config-if)# no shut
asa(config-if)# exit
```

Làm tương tự với interface g0/3

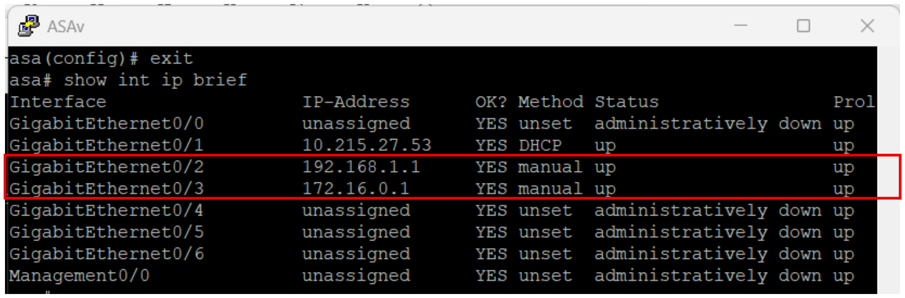
```
asa(config)# interface g0/3
asa(config-if)# ip address 172.16.0.1 255.255.255.0
asa(config-if)# security-level 50
asa(config-if)# nameif DMZ
asa(config-if)# no shut
asa(config-if)# exit
```



```
               ^
ERROR: % Invalid input detected at '^' marker.
asa(config)# asa(config-if)# nameif Inside
               ^
ERROR: % Invalid input detected at '^' marker.
asa(config)# asa(config-if)# ip address 192.168.1.1 255.255.255.0
               ^
ERROR: % Invalid input detected at '^' marker.
asa(config)# asa(config-if)# no shut
               ^
ERROR: % Invalid input detected at '^' marker.
asa(config)# asa(config-if)# exit
               ^
ERROR: % Invalid input detected at '^' marker.
asa(config)# asa(config)#
               ^
ERROR: % Invalid input detected at '^' marker.
asa(config)# interface g0/3
asa(config-if)# ip address 172.16.0.1 255.255.255.0
asa(config-if)# security-level 50
asa(config-if)# nameif DMZ
asa(config-if)# no shut
asa(config-if)# exit
asa(config)#
```

Kiểm tra lại kết quả sau khi cấu hình:

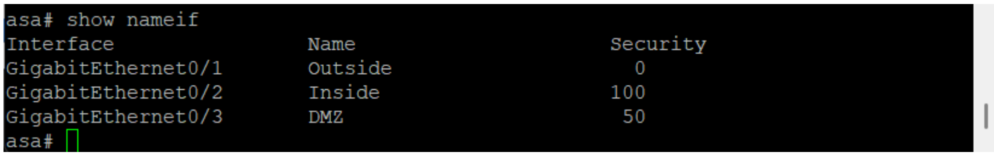
```
asa# show interface ip brief
```



```
asa(config)# exit
asa# show int ip brief
Interface                  IP-Address      OK? Method Status                Prol
GigabitEthernet0/0         unassigned      YES unset  administratively down up
GigabitEthernet0/1         10.215.27.53    YES DHCP   up                    up
GigabitEthernet0/2         192.168.1.1     YES manual up                    up
GigabitEthernet0/3         172.16.0.1      YES manual up                    up
GigabitEthernet0/4         unassigned      YES unset  administratively down up
GigabitEthernet0/5         unassigned      YES unset  administratively down up
GigabitEthernet0/6         unassigned      YES unset  administratively down up
Management0/0              unassigned      YES unset  administratively down up
```

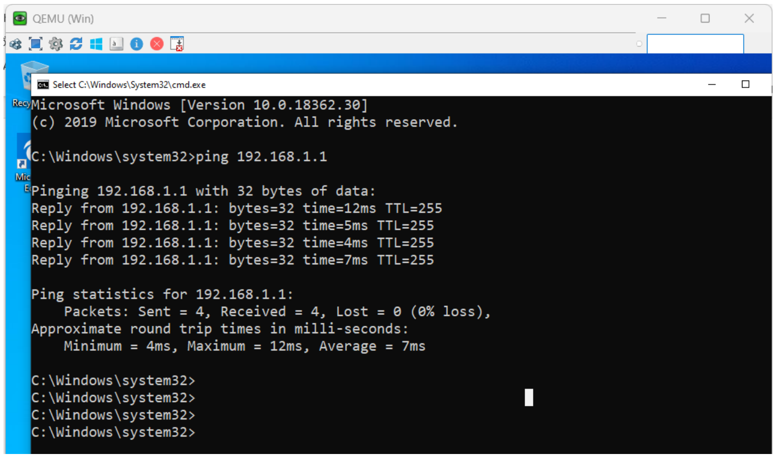
Kiểm tra nameif và security-level

```
asa# show nameif
```



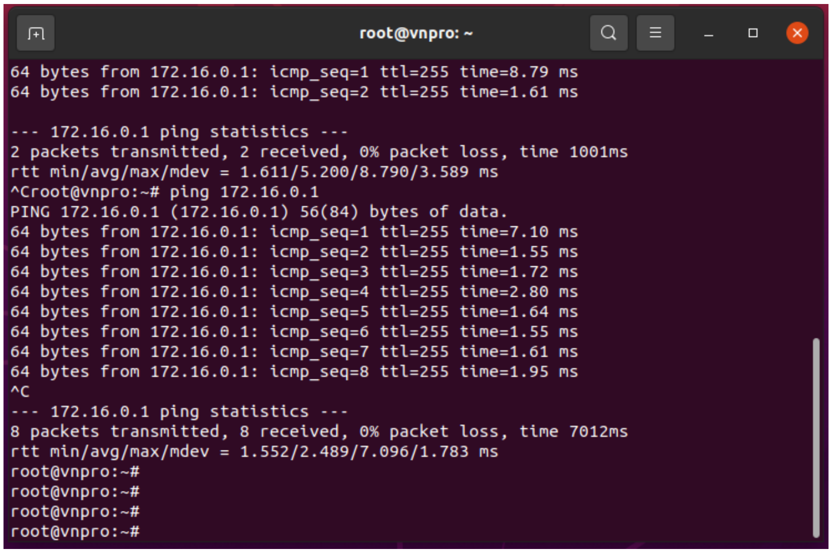
```
asa# show nameif
Interface                Name                     Security
GigabitEthernet0/1       Outside                    0
GigabitEthernet0/2       Inside                   100
GigabitEthernet0/3       DMZ                       50
asa#
```

Kiểm tra kết nối trên các thiết bị đầu cuối window



```
Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=12ms TTL=255
Reply from 192.168.1.1: bytes=32 time=5ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=7ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 12ms, Average = 7ms

C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
```

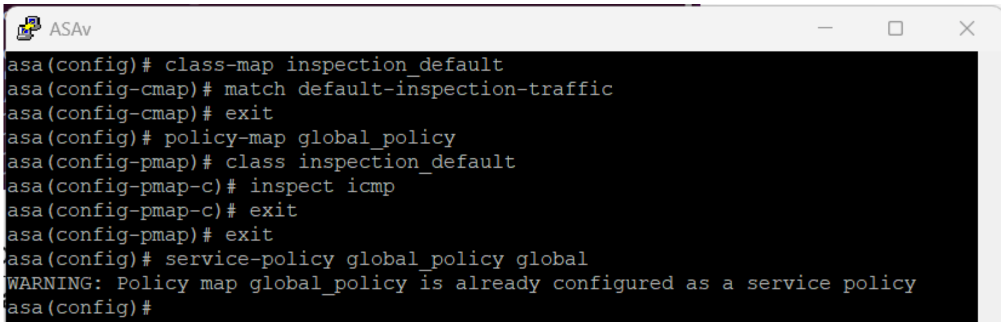
Kiểm tra trên thiết bị đầu cuối ubuntu



```
64 bytes from 172.16.0.1: icmp_seq=1 ttl=255 time=8.79 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=255 time=1.61 ms

--- 172.16.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.611/5.200/8.790/3.589 ms
^Croot@vnpro:~# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=255 time=7.10 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=255 time=1.55 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=255 time=1.72 ms
64 bytes from 172.16.0.1: icmp_seq=4 ttl=255 time=2.80 ms
64 bytes from 172.16.0.1: icmp_seq=5 ttl=255 time=1.64 ms
64 bytes from 172.16.0.1: icmp_seq=6 ttl=255 time=1.55 ms
64 bytes from 172.16.0.1: icmp_seq=7 ttl=255 time=1.61 ms
64 bytes from 172.16.0.1: icmp_seq=8 ttl=255 time=1.95 ms
^C
--- 172.16.0.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 1.552/2.489/7.096/1.783 ms
root@vnpro:~#
root@vnpro:~#
root@vnpro:~#
root@vnpro:~#
```

5. Cấu hình cho phép ICMP từ vùng Inside tới vùng DMZ.

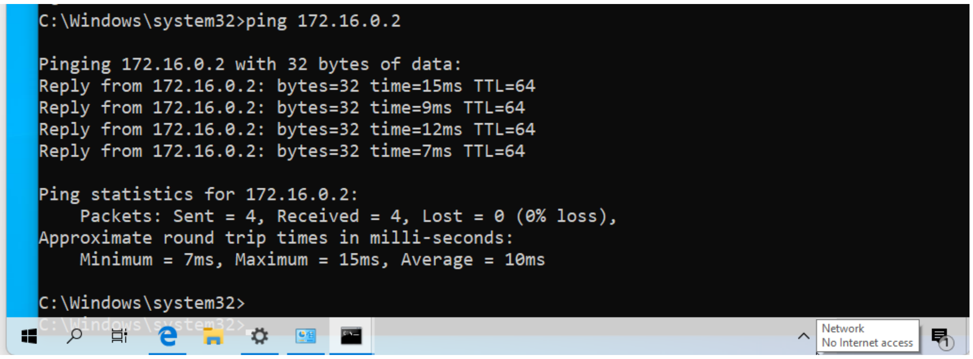
```
asa(config)# class-map inspection_default
asa(config-cmap)# match default-inspection-traffic
asa(config-cmap)# exit
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# inspect icmp
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)# service-policy global_policy global
```



```
asa(config)# class-map inspection_default
asa(config-cmap)# match default-inspection-traffic
asa(config-cmap)# exit
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# inspect icmp
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)# service-policy global_policy global
WARNING: Policy map global_policy is already configured as a service policy
asa(config)#
```

Kiểm tra kết quả:

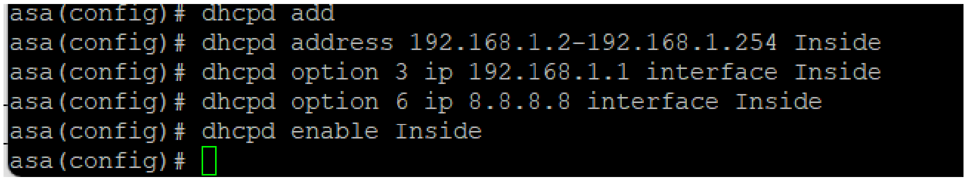
Trên máy window ping được vùng DMZ



```
C:\Windows\system32>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:
Reply from 172.16.0.2: bytes=32 time=15ms TTL=64
Reply from 172.16.0.2: bytes=32 time=9ms TTL=64
Reply from 172.16.0.2: bytes=32 time=12ms TTL=64
Reply from 172.16.0.2: bytes=32 time=7ms TTL=64

Ping statistics for 172.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 15ms, Average = 10ms

C:\Windows\system32>
```

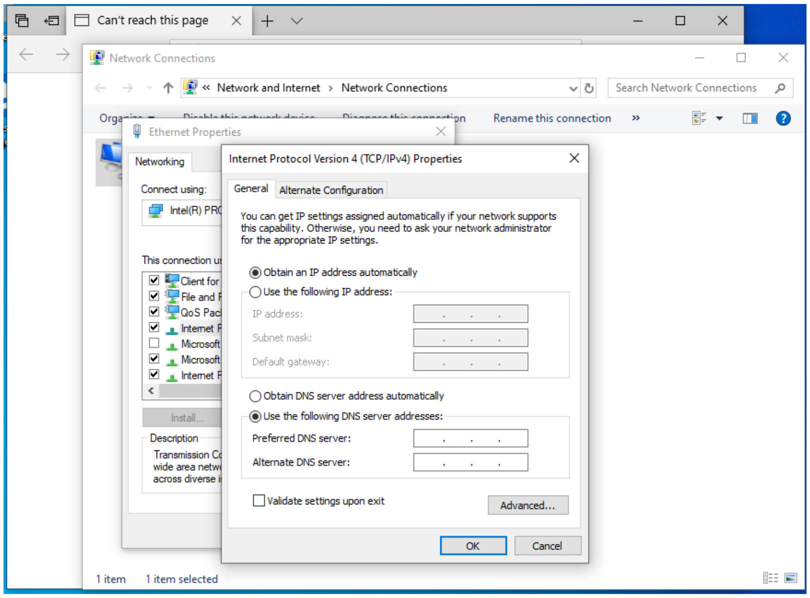
6. Cấu hình cấp DHCP vùng Inside.

```
asa(config)# dhcpd address 192.168.1.2-192.168.1.254 Inside
asa(config)# dhcpd option 3 ip 192.168.1.1 interface Inside
asa(config)# dhcpd option 6 ip 8.8.8.8 interface Inside
asa(config)# dhcpd enable Inside
```



```
asa(config)# dhcpd add
asa(config)# dhcpd address 192.168.1.2-192.168.1.254 Inside
asa(config)# dhcpd option 3 ip 192.168.1.1 interface Inside
asa(config)# dhcpd option 6 ip 8.8.8.8 interface Inside
asa(config)# dhcpd enable Inside
asa(config)#
```

Kiểm tra kết quả, trên máy Window đổi thành ip DHCP.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

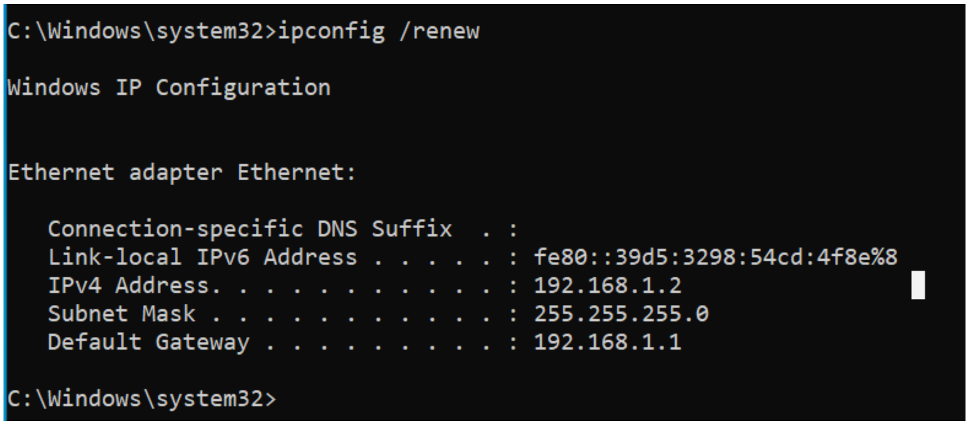
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

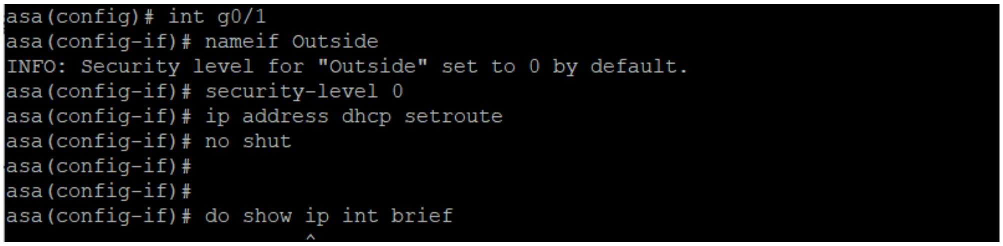
Sau đó dùng lệnh ipconfig /renew



```
C:\Windows\system32>ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::39d5:3298:54cd:4f8e%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Windows\system32>
```

7. Nhận DHCP từ vùng Outside.

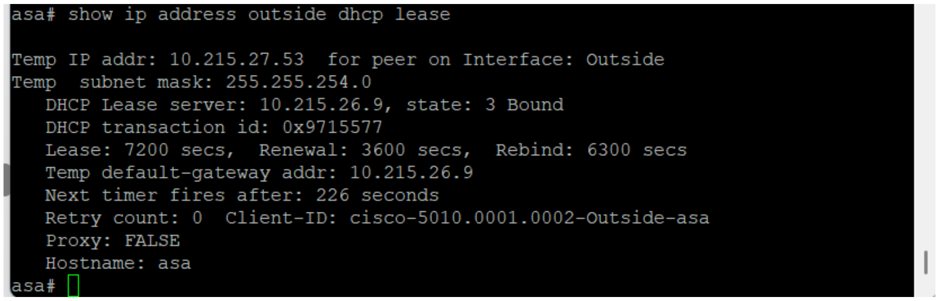
```
asa(config)# int g0/1
asa(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
asa(config-if)# security-level 0
asa(config-if)# ip address dhcp setroute
asa(config-if)# no shut
```



```
asa(config)# int g0/1
asa(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
asa(config-if)# security-level 0
asa(config-if)# ip address dhcp setroute
asa(config-if)# no shut
asa(config-if)#
asa(config-if)#
asa(config-if)# do show ip int brief
                         ^
```

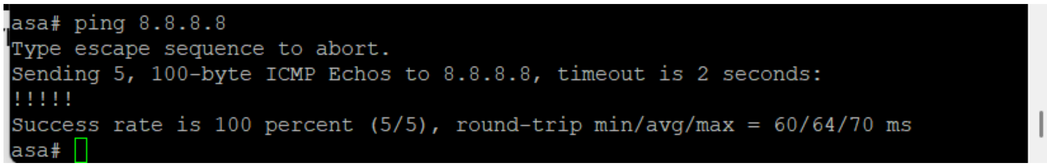
Kiểm tra lại bằng lệnh

```
show ip address outside dhcp lease
```



```
asa# show ip address outside dhcp lease

Temp IP addr: 10.215.27.53  for peer on Interface: Outside
Temp  subnet mask: 255.255.254.0
   DHCP Lease server: 10.215.26.9, state: 3 Bound
   DHCP transaction id: 0x9715577
   Lease: 7200 secs,  Renewal: 3600 secs,  Rebind: 6300 secs
   Temp default-gateway addr: 10.215.26.9
   Next timer fires after: 226 seconds
   Retry count: 0  Client-ID: cisco-5010.0001.0002-Outside-asa
   Proxy: FALSE
   Hostname: asa
asa#
```

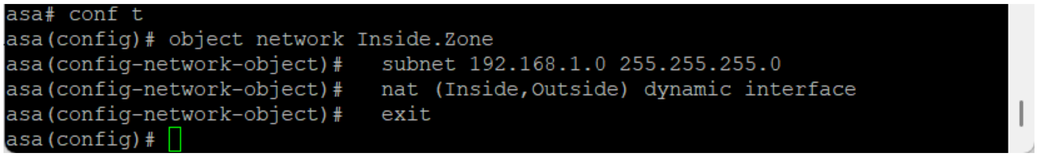
Lúc này firewall đã có thể ping được ra internet



```
asa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/70 ms
asa#
```

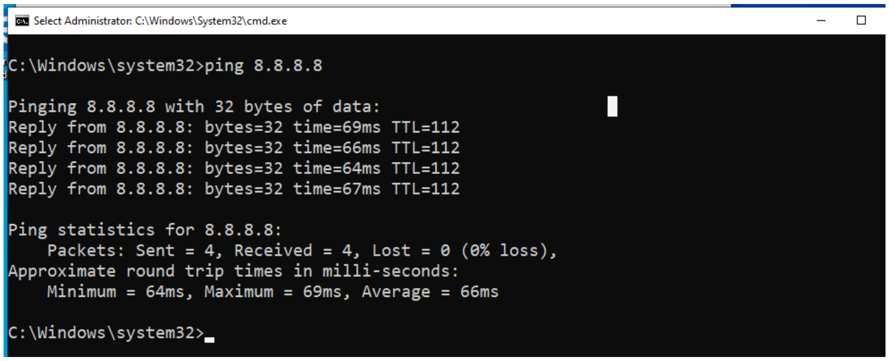
8. Cấu hình NAT overload.

```
asa(config)# object network Inside.Zone
asa(config-network-object)#   subnet 192.168.1.0 255.255.255.0
asa(config-network-object)#   nat (Inside,Outside) dynamic interface
asa(config-network-object)#   exit
```



```
asa# conf t
asa(config)# object network Inside.Zone
asa(config-network-object)#   subnet 192.168.1.0 255.255.255.0
asa(config-network-object)#   nat (Inside,Outside) dynamic interface
asa(config-network-object)#   exit
asa(config)#
```

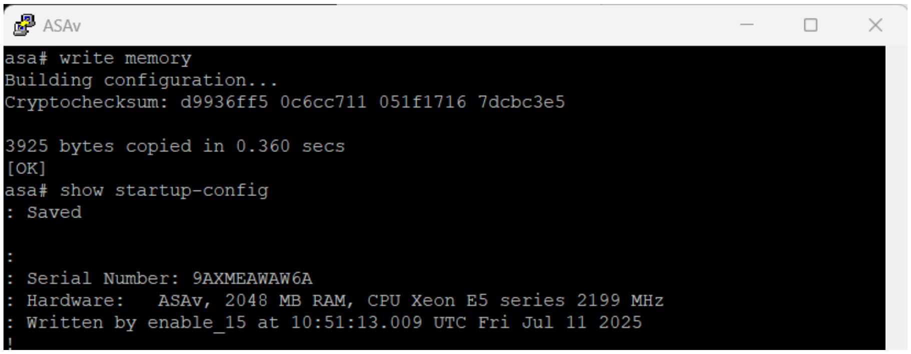
Kiểm tra lại bằng cách ping đến 8.8.8.8 trên máy window.



```
C:\Windows\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=69ms TTL=112
Reply from 8.8.8.8: bytes=32 time=66ms TTL=112
Reply from 8.8.8.8: bytes=32 time=64ms TTL=112
Reply from 8.8.8.8: bytes=32 time=67ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 64ms, Maximum = 69ms, Average = 66ms

C:\Windows\system32>
```

9. Lưu lại cấu hình

```
asa# write memory
```



```
asa# write memory
Building configuration...
Cryptochecksum: d9936ff5 0c6cc711 051f1716 7dcbc3e5

3925 bytes copied in 0.360 secs
[OK]
asa# show startup-config
: Saved

:
: Serial Number: 9AXMEAWAW6A
: Hardware:   ASAv, 2048 MB RAM, CPU Xeon E5 series 2199 MHz
: Written by enable_15 at 10:51:13.009 UTC Fri Jul 11 2025
!
```

Như vậy toàn bộ cấu hình sẽ được lưu, trong trường hợp shutdown hay reload đều giữ nguyên cấu hình.