IERG4831

Lab 2: Implementation of SOHO Networks by Cisco ASA

NAME: Doria Tang

SID: 1155126139

N1 = 63, N2 = 19

ASA:

- Internet interface G0/0. IP: 10.189.99.63/24 GW:10.189.99.254 DNS:10.189.99.254
- LAN interface G0/1. IP: 10.63.0.254/24
- DMZ interface G0/2. IP: 10.19.0.254/24

PC1, PC2, PC3:

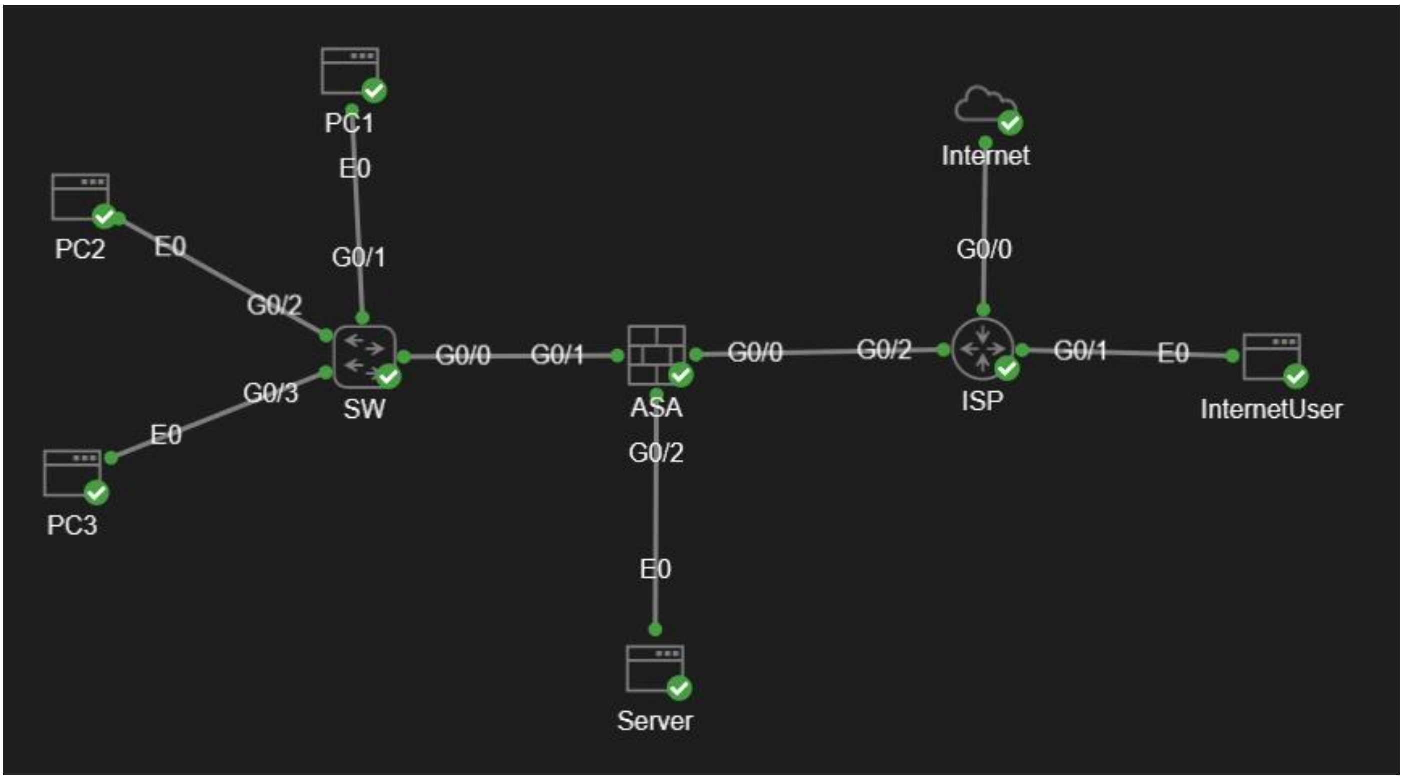
- Acquire LAN IP address, gateway address and DNS address from ASA's LAN interface (G0/2) via DHCP with subnet 10.63.0.0/24

Server:

- Connected to DMZ network with fix IP address 10.19.0.1/24

Task 1: Create a Network Topology in CML

- Record a screen dump of the network topology.



Task 2: Device configuration in CML

- Record the initial setup for each device

PC1:

```
# this is a shell script which will be sourced at boot
```

```
hostname PC1
# configurable user account
USERNAME=cisco
PASSWORD=cisco
# no password for tc user by default
TC_PASSWORD=
```

PC2:

```
# this is a shell script which will be sourced at boot
hostname PC2
# configurable user account
USERNAME=cisco
PASSWORD=cisco
# no password for tc user by default
TC_PASSWORD=
```

PC3:

```
# this is a shell script which will be sourced at boot
hostname PC3
# configurable user account
USERNAME=cisco
PASSWORD=cisco
# no password for tc user by default
TC_PASSWORD=
```

SW:

```
hostname SW
```

Server:

```
# this is a shell script which will be sourced at boot
hostname Server
# configurable user account
USERNAME=cisco
PASSWORD=cisco
# no password for tc user by default
TC_PASSWORD=
ifconfig eth0 10.19.0.1 netmask 255.255.255.0 broadcast 10.19.0.255 up
route add default gw 10.19.0.254
```

ISP:

```
Hostname ISP

interface GigabitEthernet0/0
 description Internet
 ip address dhcp
 ip nat outside
 no shutdown

```

```
interface GigabitEthernet0/1
 description InternetUser
 ip address 172.20.21.254 255.255.255.0
 ip nat inside
 no shutdown

interface GigabitEthernet0/2
 description SOHO_ASA
 ip address 10.189.99.254 255.255.255.0
 ip nat inside
 no shutdown

ip access-list extended IUser
 permit ip 172.20.21.0 0.0.0.255 any
ip access-list extended SOHO
 permit ip 10.189.99.0 0.0.0.255 any

ip dns server
ip nat inside source list IUser interface GigabitEthernet0/0 overload
ip nat inside source list SOHO interface GigabitEthernet0/0 overload
```

InternetUser:

```
# this is a shell script which will be sourced at boot
hostname InternetUser
# configurable user account
USERNAME=cisco
PASSWORD=cisco
# no password for tc user by default
TC_PASSWORD=
ifconfig eth0 172.20.21.22 netmask 255.255.255.0 broadcast 172.20.21.255 up
route add default gw 172.20.21.254
echo nameserver 172.20.21.254 >> /etc/resolv.conf
```

Task 3: Configuration of Internet access on ASA

- Configure the IP address on Internet connected interface, the default gateway and DNS settings. After configuration, the ASA should be able to PING www.google.com . Record the PING test.

```
ciscoasa(config)# ping www.google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 142.250.204.68, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

- Record the ASA configuration in this task.

```
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.189.99.63 255.255.255.0
!
interface GigabitEthernet0/1
```

```
 nameif inside
 security-level 100
 ip address 10.63.0.254 255.255.255.0
!
interface GigabitEthernet0/2
 nameif DMZ
 security-level 100
 ip address 10.19.0.254 255.255.255.0
!
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 8.8.8.8
 name-server 4.2.2.2
object network obj_any
 subnet 0.0.0.0 0.0.0.0
!
route outside 0.0.0.0 0.0.0.0 10.189.99.254 1
dhcpd dns 10.189.99.254
dhcpd auto_config outside
!
dhcpd address 10.63.0.10-10.63.0.200 inside
dhcpd enable inside
!
```

Task 4: Configuration of LAN on ASA

- Record the result of “ifconfig eth0” and “route” on PC1, PC2 and PC3.

PC1:

```
cisco@PC1:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 52:54:00:02:6C:CF
          inet addr:10.63.0.12  Bcast:10.63.0.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe02:6ccf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1727 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11988 (11.7 KiB)  TX bytes:167674 (163.7 KiB)
cisco@PC1:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.63.0.254     0.0.0.0         UG    0      0        0 eth0
10.63.0.0       *               255.255.255.0   U     0      0        0 eth0
127.0.0.1       *               255.255.255.255 UH    0      0        0 lo
```

PC2:

```
cisco@PC2:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 52:54:00:00:5D:DB
          inet addr:10.63.0.10  Bcast:10.63.0.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe00:5ddb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:1 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7694 (7.5 KiB)  TX bytes:6342 (6.1 KiB)
cisco@PC2:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.63.0.254     0.0.0.0         UG    0      0        0 eth0
10.63.0.0       *               255.255.255.0   U     0      0        0 eth0
127.0.0.1       *               255.255.255.255 UH    0      0        0 lo
```

PC3:

```
cisco@PC3:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 52:54:00:0D:47:BD
          inet addr:10.63.0.11  Bcast:10.63.0.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe0d:47bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:2 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7306 (7.1 KiB)  TX bytes:6286 (6.1 KiB)
cisco@PC3:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.63.0.254     0.0.0.0         UG    0      0        0 eth0
10.63.0.0       *               255.255.255.0   U     0      0        0 eth0
127.0.0.1       *               255.255.255.255 UH    0      0        0 lo
```

- Record the ASA configurations in this task

```
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.189.99.63 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.63.0.254 255.255.255.0
!
interface GigabitEthernet0/2
 nameif DMZ
 security-level 70
 ip address 10.19.0.254 255.255.255.0
!
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 8.8.8.8
 name-server 4.2.2.2
object network obj_any
 subnet 0.0.0.0 0.0.0.0
!
route outside 0.0.0.0 0.0.0.0 10.189.99.254 1
dhcpd dns 10.189.99.254
dhcpd auto_config outside
```

```
!
dhcpd address 10.63.0.10-10.63.0.200 inside
dhcpd enable inside
!
```

Task 5: Configuration of Internet access of hosts on LAN

- Record the result of PING test.

PC1:

```
cisco@PC1:~$ ping -c 3 www.google.com
PING www.google.com (142.250.204.100): 56 data bytes
64 bytes from 142.250.204.100: seq=0 ttl=117 time=13.394 ms
64 bytes from 142.250.204.100: seq=1 ttl=117 time=6.053 ms
64 bytes from 142.250.204.100: seq=2 ttl=117 time=5.607 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.607/8.351/13.394 ms
```

PC2:

```
cisco@PC2:~$ ping -c 3 www.google.com
PING www.google.com (142.250.204.100): 56 data bytes
64 bytes from 142.250.204.100: seq=0 ttl=117 time=8.886 ms
64 bytes from 142.250.204.100: seq=1 ttl=117 time=5.224 ms
64 bytes from 142.250.204.100: seq=2 ttl=117 time=5.565 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.224/6.558/8.886 ms
```

PC3:

```
cisco@PC3:~$ ping -c 3 www.google.com
PING www.google.com (142.250.204.100): 56 data bytes
64 bytes from 142.250.204.100: seq=0 ttl=117 time=5.788 ms
64 bytes from 142.250.204.100: seq=1 ttl=117 time=5.779 ms
64 bytes from 142.250.204.100: seq=2 ttl=117 time=5.509 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.509/5.692/5.788 ms
```

- Record the ASA configuration in this task

```
ciscoasa(config)# sh run | i inspect
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  no tcp-inspection
 class inspection_default
  inspect ip-options
  inspect netbios
  inspect rtsp
  inspect sunrpc
  inspect tftp
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect skinny
  inspect snmp
  inspect icmp
ciscoasa(config)# sh run object network
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network LAN
 subnet 10.63.0.0 255.255.255.0
ciscoasa(config)# sh run nat
!
object network LAN
 nat (inside,outside) dynamic interface
```

Task 6: Configuration of DMZ network on ASA

- Record the result of PING test. (i.e. PC1 → Server and Server → PC1)

PC1 → Server

```
cisco@PC1:~$ ping -c 3 10.19.0.1
PING 10.19.0.1 (10.19.0.1): 56 data bytes
64 bytes from 10.19.0.1: seq=0 ttl=64 time=3.747 ms
64 bytes from 10.19.0.1: seq=1 ttl=64 time=3.439 ms
64 bytes from 10.19.0.1: seq=2 ttl=64 time=2.769 ms

--- 10.19.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.769/3.318/3.747 ms
```

PC2 → Server

```
cisco@PC2:~$ ping -c 3 10.19.0.1
PING 10.19.0.1 (10.19.0.1): 56 data bytes
64 bytes from 10.19.0.1: seq=0 ttl=64 time=3.154 ms
64 bytes from 10.19.0.1: seq=1 ttl=64 time=2.752 ms
64 bytes from 10.19.0.1: seq=2 ttl=64 time=2.737 ms

--- 10.19.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.737/2.881/3.154 ms
```

PC3 → Server

```
cisco@PC3:~$ ping -c 3 10.19.0.1
PING 10.19.0.1 (10.19.0.1): 56 data bytes
64 bytes from 10.19.0.1: seq=0 ttl=64 time=2.800 ms
64 bytes from 10.19.0.1: seq=1 ttl=64 time=2.584 ms
64 bytes from 10.19.0.1: seq=2 ttl=64 time=3.023 ms

--- 10.19.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.584/2.802/3.023 ms
```

Server → PC1 (10.63.0.12)

```
cisco@Server:~$ ping -c 3 10.63.0.12
PING 10.63.0.12 (10.63.0.12): 56 data bytes

--- 10.63.0.12 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

Server → PC2 (10.63.0.10)

```
cisco@Server:~$ ping -c 3 10.63.0.10
PING 10.63.0.10 (10.63.0.10): 56 data bytes

--- 10.63.0.10 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

Server → PC3 (10.63.0.11)

```
cisco@Server:~$ ping -c 3 10.63.0.11
PING 10.63.0.11 (10.63.0.11): 56 data bytes

--- 10.63.0.11 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

- Record the ASA configuration in this task

```
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.189.99.63 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.63.0.254 255.255.255.0
!
interface GigabitEthernet0/2
 nameif dmz
 security-level 70
 ip address 10.19.0.254 255.255.255.0
!
```

Task 7: Configuration of Server to access the Internet

- Record the result of PING test

```
cisco@Server:~$ ping -c 3 www.google.com
PING www.google.com (142.250.204.68): 56 data bytes
64 bytes from 142.250.204.68: seq=0 ttl=117 time=4.389 ms
64 bytes from 142.250.204.68: seq=1 ttl=117 time=4.773 ms
64 bytes from 142.250.204.68: seq=2 ttl=117 time=4.104 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 4.104/4.422/4.773 ms
```

- Record the ASA configuration in this task

```
object network dmz-subnet
 subnet 10.19.0.0 255.255.255.0
object network Google-DNS
 host 8.8.8.8
!
object network dmz-subnet
 nat (dmz,outside) dynamic interface
object network Google-DNS
 nat (outside,dmz) static interface service udp domain domain
```

Task 8: Configuration of access of Server by the host from Internet (via InternetUser)

- To verify the configuration, start a SSH access from InternetUser to the IP address of ASA:G0/0 by the command "ssh 10.189.99.N1 –p 2222". Record the result.

```
cisco@InternetUser:~$ ssh 10.189.99.63 -p 2222
The authenticity of host '[10.189.99.63]:2222 ([10.189.99.63]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:WspmkR3Qty78HyHC6dyfLo9arDuO4E8JR4h5iFNXYXM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[10.189.99.63]:2222' (ECDSA) to the list of known hosts.
cisco@10.189.99.63's password:
Permission denied, please try again.
cisco@10.189.99.63's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

cisco@Server:~$
```

- Record the ASA configuration in this task.

```
object network dmz_server
 host 10.19.0.1
access-list inbound extended permit tcp any object dmz_server eq ssh
object network dmz_server
 nat (dmz,outside) static interface service tcp ssh 2222
access-group inbound in interface outside
```