Fortray - CCNA Sec

FW Interfaces Configuration

Step by Step Configuration Guide

Intellectual Property

1. Table of contents

2. Version

Version	Date	Notes	Created By	Release
1.0	15/03/2019	Student Workbook for LAB	Mazhar Minhas	Initial Release
2.1	03/04/2020	Errors Removed	Farooq Zafar	Final Release

3. Reference Document

Click for the Reference document

4. Assumption

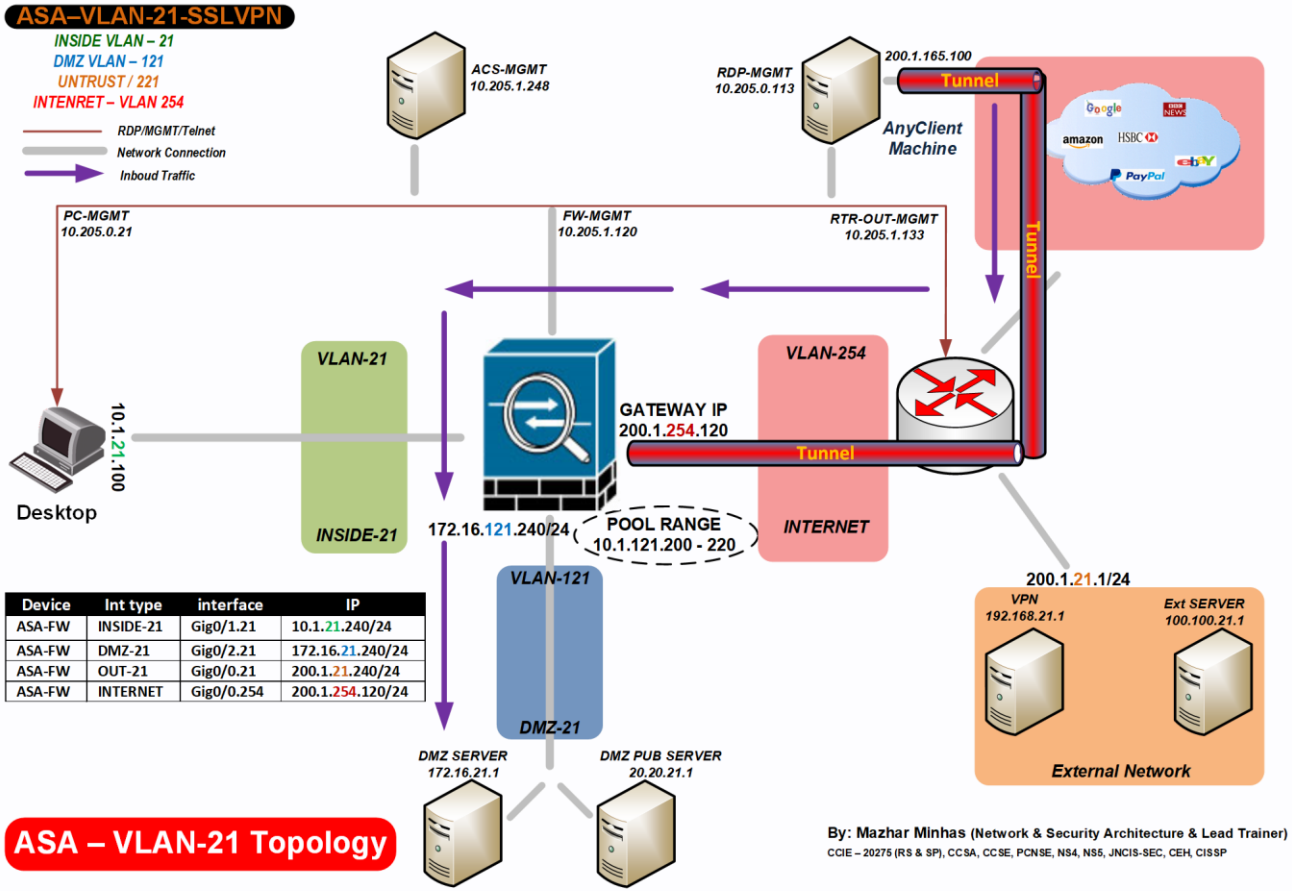
- ✓ We understand that delegate already understand L2/L3, Routing.
- ✓ The delegate already knows the "***Fortray Networks – CCNA Security"*** physical and logical connection.
- ✓ The delegate already has basis Troubleshooting skill, such as ping and trace.
- ✓ The delegate already has access to the "***Fortray Networks – CCNA Security"*** *Spreadsheet encompassing the Basic Layer, 2, 3 and allocated subnet information. For more details refer to the "****Student Folder".***
- ✓ This document is created to show an example for one topology only. The candidate needs to refer to his own topology and follow this step by step guide.
- ✓ We assume that delegate already have installed the VPN software and him/she have VPN user / Password. If any issue, contact our Technical team.
- ✓ Our VPN software is supported by PC, MAC, Android, and IOS devices.
- ✓ It's also assumed that delegate has access to PC/Laptop i5 with 4GB RAM.
- ✓ For optimal connectivity, we recommend at least 10MB Internet connection.
- ✓ We assume that we already have ***INTERNAL, DMZ, OUTISE*** interfaces are already configured.

5. NOTE About Configuration Example

The configuration example is based in the "**VLAN-21**".
Please refer to "**Student Spreadsheet**" and complete your task based on your Network Topology, & Task list assigned.

6. Fortray CCNA Security - Network Topology

The below network topology is just for information purpose only. Please refer to your student folder and your designated topology. If any doubt, please ask your instructor.



Device	Int type	interface	IP
ASA-FW	INSIDE-21	Gig0/1.21	10.1.21.240/24
ASA-FW	DMZ-21	Gig0/2.21	172.16.21.240/24
ASA-FW	OUT-21	Gig0/0.21	200.1.21.240/24
ASA-FW	INTERNET	Gig0/0.254	200.1.254.120/24

7. Fortray CCNA Security - LAB-ASA Firewall MGMT Access

Refer to below table and login to router, switches and Test machine.

Each delegate has his /her own test machine, refer to the spreadsheet provided in the student shared folder

Device Name	Type	IP	Access method	User	Password	Enable password	Comments
ASA-PRIM-1-120	ASA 5510	10.205.1.120	Telnet port 23	Admin	cisco	cisco	
ASA-BACK-1-121	ASA 5510	10.205.1.121	Telnet port 23	Admin	cisco	cisco	
FN-SEC-1-184	Router	10.205.1.184	Telnet port 23	Cisco	cisco	cisco	
FN-PC-SEC-21	Test Machine	10.205.0.21	RDP	Administrator	cisco	N/A	Refer to spreadsheet
AnyClient-PC	External PC	10.205.0.113	RDP	Refer to spreadsheet		N/A	Refer to spreadsheet
Active Directory	AD Server	10.205.0.254	LDAP	Refer to spreadsheet		N/A	Refer to spreadsheet

Warning: Please don't change the above password for any devices.

8. Fortray CCNA Security – Interface Spread Sheet

The below-spread sheet shows the value of LAN & WAN interfaces and allocation IPv4 IP range, each delegate will be referring to his/her own LAN/WAN interface and will be completing his/her LAB.

NO	Student VLAN	ASA FW (Admin)	Test PC (RDP)	PC USERS	PC Password	Inside Interface	NAMEIF	Sec Level	Inside VLAN	Inside-IP	DMZ Interface	NAMEIF	Sec Level	DMZ VLAN	DMZ - IP	OUTSIDE Interface	NAMEIF	Sec Level	OUTISDE VLAN	OUTSIDE VLAN
1	21	ASA - 1 10.205.1.120 (Primary)	10.205.0.21	administrator	cisco	Gig0/1.21	INSIDE-21	100	21	10.1.21.240/24	Gig0/2.21	DMZ-21	50	121	172.16.21.240/24	Gig0/0.21	OUT-21	0	221	200.1.21.240/24
2	22		10.205.0.22	administrator	cisco	Gig0/1.22	INSIDE-22	100	22	10.1.22.240/24	Gig0/2.22	DMZ-22	50	122	172.16.22.240/24	Gig0/0.22	OUT-22	0	222	200.1.22.240/24
3	23		10.205.0.23	administrator	cisco	Gig0/1.23	INSIDE-23	100	23	10.1.23.240/24	Gig0/2.23	DMZ-23	50	123	172.16.23.240/24	Gig0/0.23	OUT-23	0	223	200.1.23.240/24
4	24		10.205.0.24	administrator	cisco	Gig0/1.24	INSIDE-24	100	24	10.1.24.240/24	Gig0/2.24	DMZ-24	50	124	172.16.24.240/24	Gig0/0.24	OUT-24	0	224	200.1.24.240/24
5	25		10.205.0.25	administrator	cisco	Gig0/1.25	INSIDE-25	100	25	10.1.25.240/24	Gig0/2.25	DMZ-25	50	125	172.16.25.240/24	Gig0/0.25	OUT-25	0	225	200.1.25.240/24
6	26	ASA - 1 10.205.1.121 (Backup)	10.205.0.26	administrator	cisco	Gig0/1.26	INSIDE-26	100	26	10.1.26.240/24	Gig0/2.26	DMZ-26	50	126	172.16.26.240/24	Gig0/0.26	OUT-26	0	226	200.1.26.240/24
7	27		10.205.0.27	administrator	cisco	Gig0/1.27	INSIDE-27	100	27	10.1.27.240/24	Gig0/2.27	DMZ-27	50	127	172.16.27.240/24	Gig0/0.27	OUT-27	0	227	200.1.27.240/24
8	28		10.205.0.28	administrator	cisco	Gig0/1.28	INSIDE-28	100	28	10.1.28.240/24	Gig0/2.28	DMZ-28	50	128	172.16.28.240/24	Gig0/0.28	OUT-28	0	228	200.1.28.240/24
9	29		10.205.0.29 10.205.1.29	administrator	cisco	Gig0/1.29	INSIDE-29	100	29	10.1.29.240/24	Gig0/2.29	DMZ-29	50	129	172.16.29.240/24	Gig0/0.29	OUT-29	0	229	200.1.29.240/24
10	30		10.205.0.30	administrator	cisco	Gig0/1.30	INSIDE-30	100	30	10.1.30.240/24	Gig0/2.30	DMZ-30	50	130	172.16.30.240/24	Gig0/0.30	OUT-30	0	230	200.1.30.240/24

NO	Student VLAN	ASA FW (Admin)	INTERNET Interface	UNTRUST VLAN	INTERNET IP	PAT IP	Static NAT GLOBAL IP	Static NAT PRIVATE IP	External Test PC	User name	Password	LDAP User name	Password
1	21	ASA - 1 10.205.1.120 (Primary)	Gig0/0.254	254	200.1.254.120	200.1.254.120	200.1.254.121	172.16.21.1	10.205.0.113	user1	Cisco@123 (C in CAP)	user01	Cisco@123 (C in CAP)
2	22		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.122	172.16.22.1	10.205.0.113	user2	Cisco@123 (C in CAP)	user02	Cisco@123 (C in CAP)
3	23		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.123	172.16.23.1	10.205.0.113	user3	Cisco@123 (C in CAP)	user03	Cisco@123 (C in CAP)
4	24		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.124	172.16.24.1	10.205.0.113	user4	Cisco@123 (C in CAP)	user04	Cisco@123 (C in CAP)
5	25		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.125	172.16.25.1	10.205.0.113	user5	Cisco@123 (C in CAP)	user05	Cisco@123 (C in CAP)
6	26	ASA - 1 10.205.1.121 (Backup)	Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.126	172.16.26.1	10.205.0.113	user6	Cisco@123 (C in CAP)	user06	Cisco@123 (C in CAP)
7	27		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.127	172.16.27.1	10.205.0.113	user7	Cisco@123 (C in CAP)	user07	Cisco@123 (C in CAP)
8	28		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.128	172.16.28.1	10.205.0.113	user8	Cisco@123 (C in CAP)	user08	Cisco@123 (C in CAP)
9	29		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.129	172.16.29.1	10.205.0.113	user9	Cisco@123 (C in CAP)	user09	Cisco@123 (C in CAP)
10	30		Gig0/0.254	AS above	200.1.254.120	200.1.254.120	200.1.254.130	172.16.30.1	10.205.0.113	user10	Cisco@123 (C in CAP)	user10	Cisco@123 (C in CAP)

9. Fortray CCNA Security Interface Configuration Task

Fortray Networks head office ***"Network Administrator"*** would like to configure Cisco ASA Firewall's interfaces.

In this example we are configuring the Ethernet0/0.21, Ethernet0/1.21, Ethernet0/2.21, Ethernet0/0.254
Please refer to student spreadsheet to configure students assigned interfaces.

Summary steps to be done by the network administrator are mentioned below: -

Summary of the Configuration Steps

- Configure interfaces
- Verify the configuration

10. Fortray CCNA Security Interface Configuration Task

This section will be explaining how to configure sub-interfaces in the Cisco ASA Firewall

10.1. STEP 1 >> Configure the Layer 3 OUTSIDE sub-Interface

Every Delegate will be creating 3 x sub interfaces. LAN, DMZ, and OUSISDE, in addition to that, only Trainer will be doing the 1 x extra sub-interface for “INTERNET” which will be using for internet only

Following parameters are required for each interface

```
Nameif, IP address, VLAN id, Security Level
```

Make sure you are in the user privilege Mode # please refer to the spread sheet Interface “TAB” and configure your interface as per guide.

```
configure terminal
 interface Ethernet0/0.21
 vlan 221
 nameif OUT-21
 security-level 0
 ip address 200.1.21.240 255.255.255.0
```

10.2. STEP 2 >> Configure the Layer 3 “INSIDE”sub-Interface

Following parameters are required for each interface

```
Nameif, IP address, VLAN id, Security Level
```

Make sure you are in the user privilege Mode # please refer to the spread sheet Interface “TAB” and configure your interface as per guide.

```
configure terminal interface Ethernet0/1.21
 vlan 21
 nameif INSIDE-21
 security-level 100
 ip address 10.1.21.240 255.255.255.0
```

10.3. STEP 3 >> Configure the Layer 3 “DMZ”sub-Interface

Following parameters are required for each interface

```
Nameif, IP address, VLAN id, Security Level
```

Make sure you are in the user privilege Mode # please refer to the spread sheet Interface “TAB” and configure your interface as per guide.

```
configure terminal interface Ethernet0/2.21
 vlan 121
 nameif DMZ-21
 security-level 50
 ip address 172.16.21.240 255.255.255.0
```

10.4. STEP 4 >> Configure Ethernet0/0.254 interface

Following parameters are required for each interface

```
Nameif, IP address, VLAN id, Security Level
```

Make sure you are in the user privilege Mode # please refer to the spread sheet Interface “TAB” and configure your interface as per guide.

Only Trainer will configure this interface

```
configure terminal interface Ethernet0/0.254
 vlan 254
 nameif INTERNET
 security-level 0
 ip address 200.1.254.120 255.255.255.0
```

11. Verification Steps via Command line

Follow command can be used to verify your interfaces configuration

```
show interface ip brief
show nameif
ping
```

11.1. Step 1 >> Verify the IP and Interface status

```
FN-ASA-1-120/act/pri# show int ip brief | in 21
Ethernet0/0.21             200.1.21.240    YES CONFIG up                    up
Ethernet0/1.21             10.1.21.240     YES CONFIG up                    up
Ethernet0/2.21             172.16.21.240   YES CONFIG up                    up
```

11.2. Step 2 >> Verify interfaces names & security levels

```
FN-ASA-1-120/act/pri# sh nameif | in 21
Ethernet0/0.21           OUT-21                   0
Ethernet0/1.21           INSIDE-21              100
Ethernet0/2.21           DMZ-21                  50
Ethernet0/2.21           172.16.21.240   YES CONFIG up                    up
```

11.3. Step 3 >> Veify the Neighobur connectivity

After configuring the IP, VLAN and security level, all the delegate needs to test the connection with the ngibhour deivces, please refer to your network diagarma and test the connectivity. We need to ensure to test with Inside, DMZ, OUTSIDE

Ping the LAN

```
FN-ASA-1-120/act/pri# ping 10.1.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Ping the DMZ

```
N-ASA-1-120/act/pri# ping 172.16.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.16.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/20 ms
```

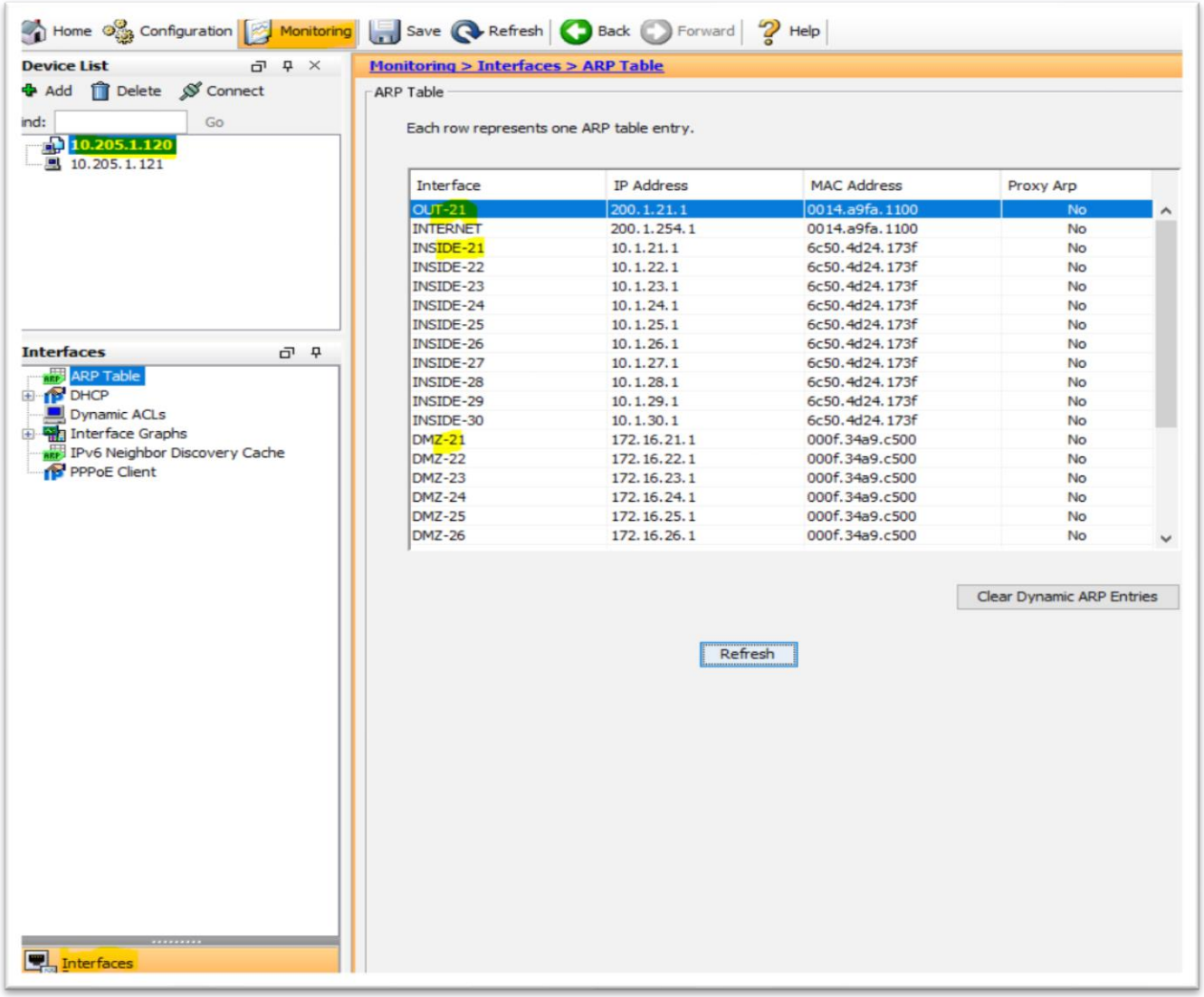
Ping the OUTSIDE

```
FN-ASA-1-120/act/pri# ping 200.1.16.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.16.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/20 ms
```

11.4. Step 4 >> Veify via the ASDM

Login to ASDM and veriy the iinteface status

- **Home > Monitor > Interface**



Thanks, and Good Luck