Fortray - CCNA Sec

ASA Static NAT with Port Forwarding

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

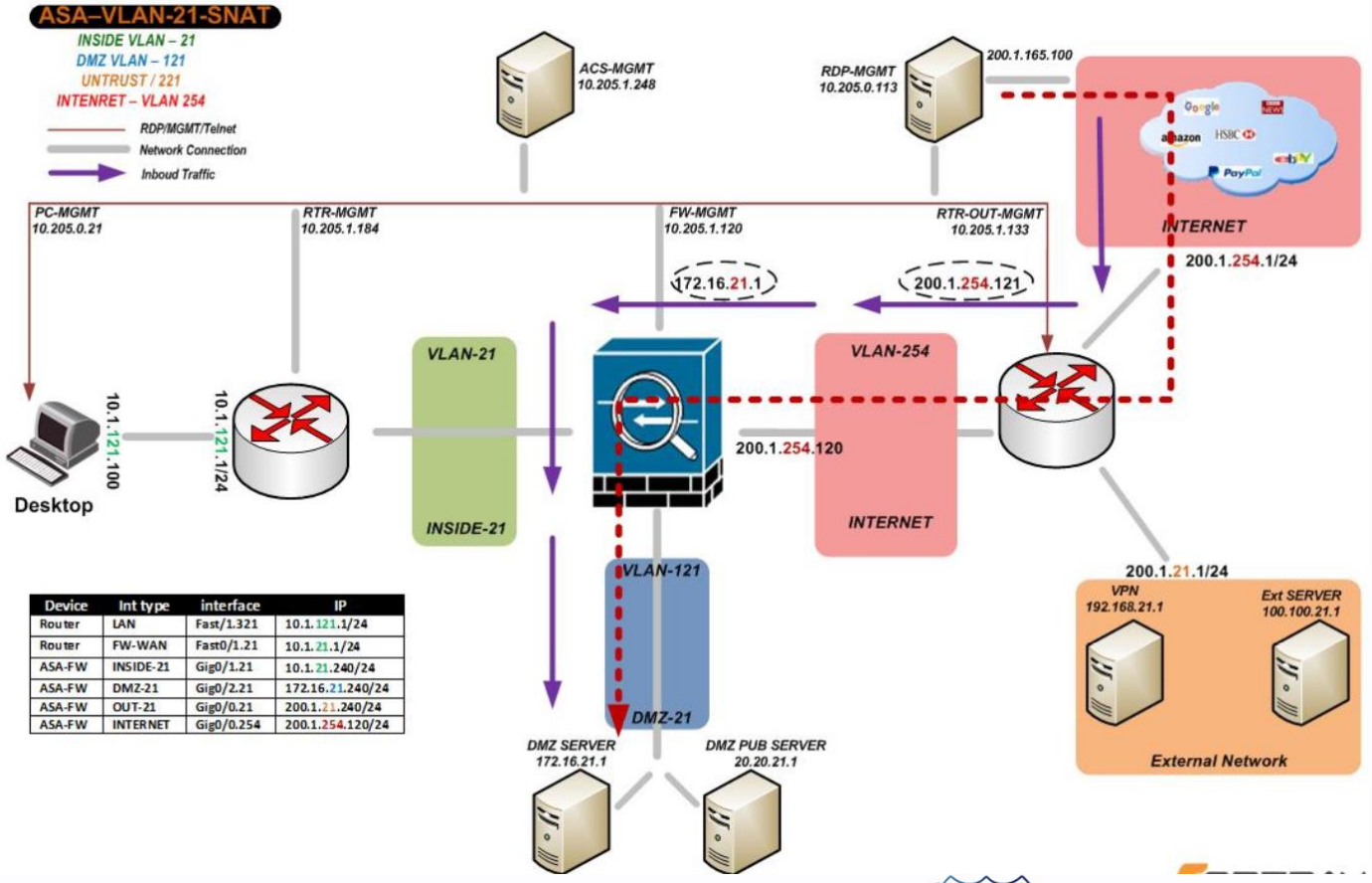
- ✓ We understand that delegate already understand L2/L3, Routing.
- ✓ The delegate already knows the "***Fortray Networks – CCNA Security"*** physical and logical connection.
- ✓ The delegate already has a basis Troubleshooting skill, such as ping and trace.
- ✓ The delegate already has access to the "***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 topology and follow this step by step guide.
- ✓ We assume that delegate already has 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 a 10MB Internet connection.
- ✓ We assume that we already have ***INTERNAL, DMZ, OUTISE*** interfaces that are already configured.

5. NOTE About Configuration Example

The configuration example is based in the "**VLAN-21**".
Please refer to the "**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
Router	LAN	Fast/1.321	10.1.121.1/24
Router	FW-WAN	Fast0/1.21	10.1.21.1/24
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 the below table and login to the router, switches and Test machine.

Each delegate has his /her 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

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

8. Fortray CCNA Security – Static NAT – Real and Global IP Information

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.

Note: Refer to the Student Spread Static NAT spreadsheet. Column L&M showing the Real DMZ IP Public-Facing IP

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Cisco AS FW - Static NAT & Test PC info																		
NO	**Student VLAN**	**ASA FW (Admin)**	**DMZ Interface**	**NAMEIF**	**DMZ - IP**	**OUTSIDE Interface**	**NAMEIF**	**OUTSIDE VLAN**	**INTERNET Interface**	**INTERNET IP**	**Static NAT GLOBAL IP**	**Static NAT PRIVATE IP**	**External Test PC**	**User name**	**Password**	**LDAP/AD User name**	**Password**	
1	21		Gig0/2.21	DMZ-21	172.16.21.240/24	Gig0/0.21	OUT-21	200.1.21.240/24	Gig0/0.254	200.1.254.120	200.1.254.121	172.16.21.1	10.205.0.113	user1	Cisco@123 (C in CAP)	user01	@123 (C in CAP)	
2	22	ASA - 1	Gig0/2.22	DMZ-22	172.16.22.240/24	Gig0/0.22	OUT-22	200.1.22.240/24	Gig0/0.254		200.1.254.122	172.16.22.1	10.205.0.113	user2	Cisco@123 (C in CAP)	user02	@123 (C in CAP)	
3	23	10.205.1.120	Gig0/2.23	DMZ-23	172.16.23.240/24	Gig0/0.23	OUT-23	200.1.23.240/24	Gig0/0.254		200.1.254.123	172.16.23.1	10.205.0.113	user3	Cisco@123 (C in CAP)	user03	@123 (C in CAP)	
4	24	(Primary)	Gig0/2.24	DMZ-24	172.16.24.240/24	Gig0/0.24	OUT-24	200.1.24.240/24	Gig0/0.254		200.1.254.124	172.16.24.1	10.205.0.113	user4	Cisco@123 (C in CAP)	user04	@123 (C in CAP)	
5	25		Gig0/2.25	DMZ-25	172.16.25.240/24	Gig0/0.25	OUT-25	200.1.25.240/24	Gig0/0.254		200.1.254.125	172.16.25.1	10.205.0.113	user5	Cisco@123 (C in CAP)	user05	@123 (C in CAP)	
6	26		Gig0/2.26	DMZ-26	172.16.26.240/24	Gig0/0.26	OUT-26	200.1.26.240/24	Gig0/0.254	AS Above	200.1.254.126	172.16.26.1	10.205.0.113	user6	Cisco@123 (C in CAP)	user06	@123 (C in CAP)	
7	27	ASA - 1	Gig0/2.27	DMZ-27	172.16.27.240/24	Gig0/0.27	OUT-27	200.1.27.240/24	Gig0/0.254		200.1.254.127	172.16.27.1	10.205.0.113	user7	Cisco@123 (C in CAP)	user07	@123 (C in CAP)	
8	28	10.205.1.121	Gig0/2.28	DMZ-28	172.16.28.240/24	Gig0/0.28	OUT-28	200.1.28.240/24	Gig0/0.254		200.1.254.128	172.16.28.1	10.205.0.113	user8	Cisco@123 (C in CAP)	user08	@123 (C in CAP)	
9	29	(Backup)	Gig0/2.29	DMZ-29	172.16.29.240/24	Gig0/0.29	OUT-29	200.1.29.240/24	Gig0/0.254		200.1.254.129	172.16.29.1	10.205.0.113	user9	Cisco@123 (C in CAP)	user09	@123 (C in CAP)	
10	30		Gig0/2.30	DMZ-30	172.16.30.240/24	Gig0/0.30	OUT-30	200.1.30.240/24	Gig0/0.254		200.1.254.130	172.16.30.1	10.205.0.113	user10	Cisco@123 (C in CAP)	user10	@123 (C in CAP)	

9. Fortray CCNA Security – Static NAT – Inbound Traffic from Test Machine to DM z

Fortray Networks head office has a DMZ server that responds to SSH/TELNET and HTTP Services. ***Fortray Information Sec*** Team is concerned about exposing the original Services and have asked **"Security Engineering team"** to design a solution where original port /services 80 is not visible to the outside world.

"Fortray Engineering Team" has requested operation team to use the port forwarding feature where 8080 will be forwarding to the port 80/HTTP.

Engineering team has provided Public Ip range 200.1.254.X. (X is in the range of 121 to 130 check your spread sheet) and source port 8080 where the original IP will be DMZ server IP 172.16.X.1 (X is VLAN)

This is a configuration example for VLAN 21, every delegate would refer to the spreadsheet + diagram and configure the port Forwarding.

This LAB assume that Static NAT is already configured.

Summary of the Configuration Steps are below:

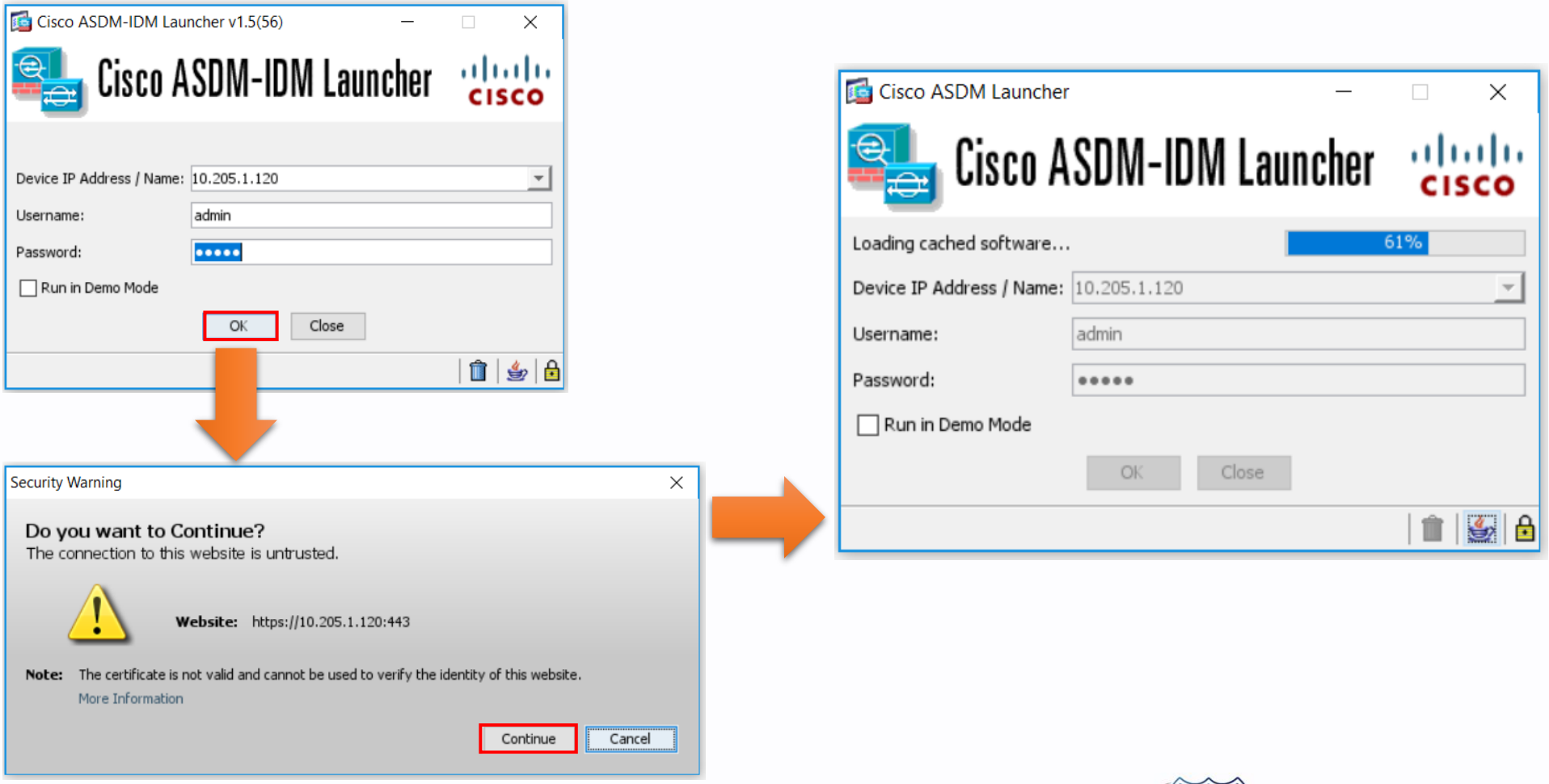
- Login to FW via ASDM or Telnet/SSH
- Modify the Static existing STATIC NAT Entry
- Login to the outside test machine 10.205.0.113 (refer to the spreadsheet for user /password) and Test the services.

10. Fortray CCNA Security Remote VPN Configuration Steps

***Note:** This is a configuration example for VLAN 21, every delegate would refer to the spreadsheet + diagram.*

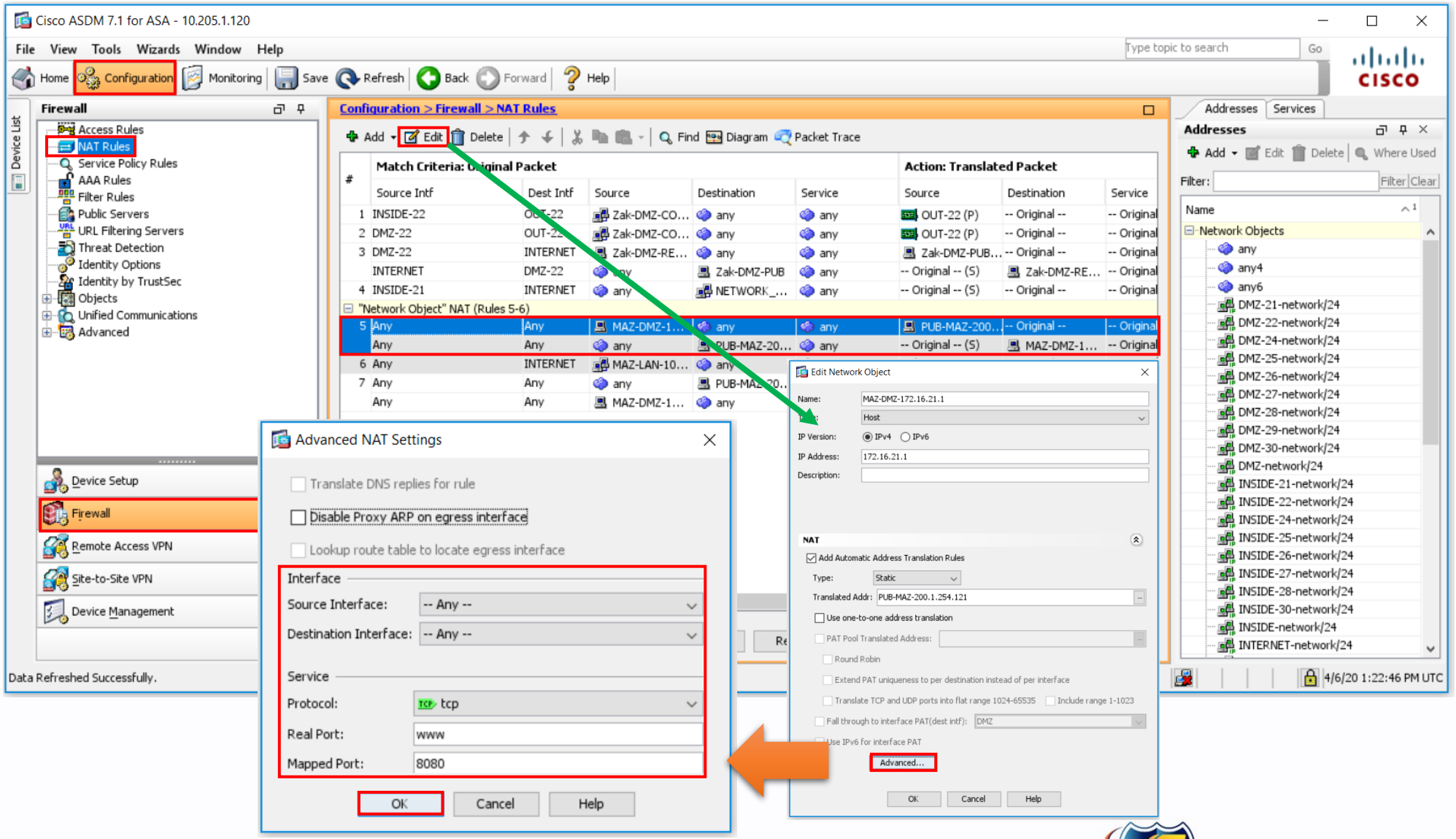
10.1. Step 1: Loin to ASA Firewall via ASDM

Login to ASA firewall using the IP Address via the ASDM with your or admin account



10.2. Modify the Static existing STATIC NAT Entry

Create a NAT entry using the Real DMZ IP address



10.3. Command Line Configuration

Blow is the command line configuration example (user your own DMZ and Public IP as per Spreadsheet)

```
!
1. Static NAT
object network MAZ-DMZ-172.16.21.1
 nat (any,any) static PUB-MAZ-200.1.254.121 service tcp www 8080!
```

11. Verification

11.1. Summary commands - Command line verification

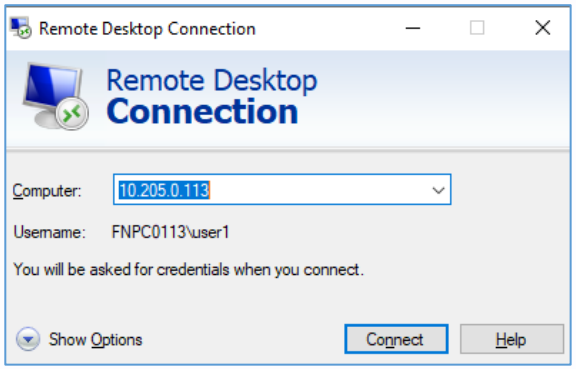
Connect Cisco ASA Firewall and use following commands:

```
Show running access-list
Show running access-group
Show access-list
ping
trace
show conn detail
show xlate
```

11.1. Step 1: RDP to the Test Machine

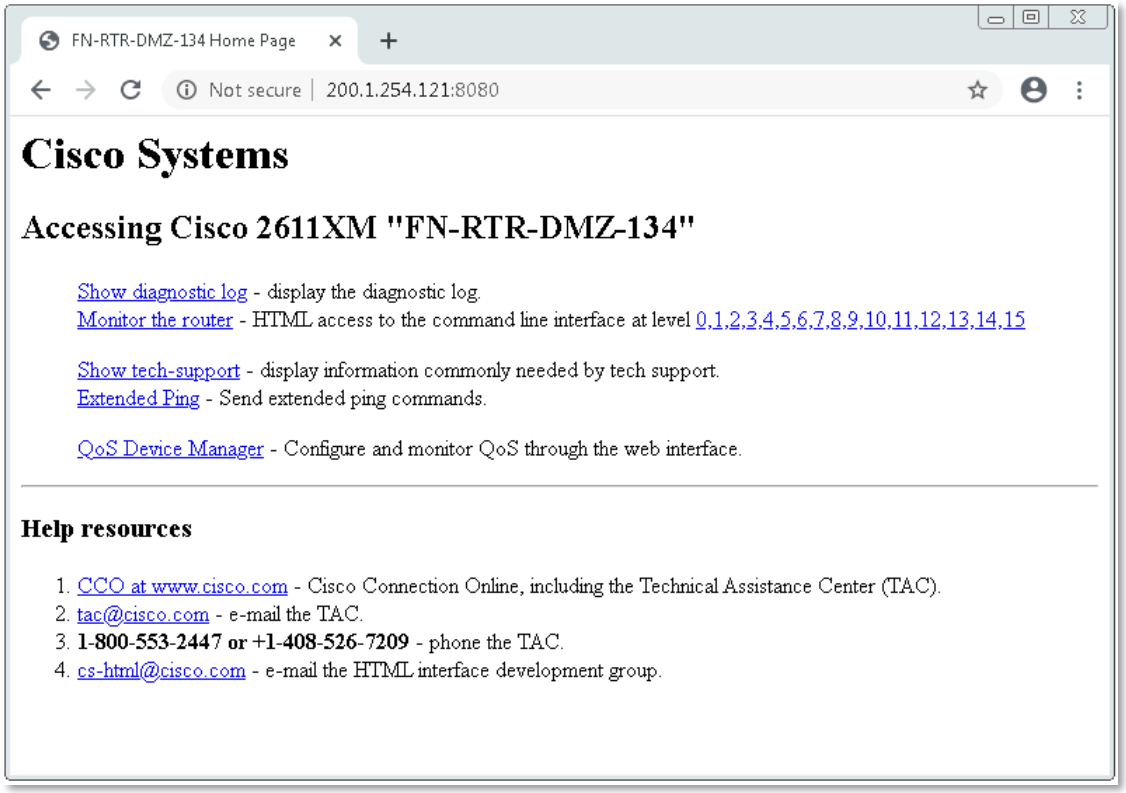
In this section, we will verify and test the configuration created in the previous section

RDP to INTERNET test machine 10.205.0.113, use the user/password as shown in the diagram



11.2. Step 2: Ping to the DMZ server using public IP

Open web browser and type http://200.1.121:8080, you can see the webpage.



Thanks, and Good Luck