

Fortray - CCNA Sec MGMT Configuration

Step by Step Configuration Guide



2020



Intellectual Property

The Copyright in this work is vested in **Fortray Networks Limited** and the document is issued in confidence for the express purpose for which it is supplied. It must not be reproduced, in whole or in part, or be used for any other purpose without prior written consent being obtained from **Fortray Networks Limited**, and then only on <u>the</u> condition that this notice be included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party without the prior written consent of **Fortray Networks Limited**.

info@fortray.com

© Copyright Fortray Networks Limited 2011-2020



2

🜐 <u>www.fortray.com</u> 💋 0207-993-4928 🖂



1. Table of contents

1.	Table of contents 3
2.	Version
3.	Reference Document
4.	Assumption4
5.	NOTE About Configuration Example
6.	Fortray CCNA Security - Network Topology
7.	Fortray CCNA Security - LAB-ASA Firewall MGMT Access
8.	Fortray CCNA Security – Interface Spread Sheet
9.	Fortray CCNA Security Interface Configuration Task
10.	Fortray CCNA Security Interface Configuration Task9
	10.1. STEP 1 >> Configure the Layer 3 Interface Parameters
	10.2. STEP 2 >> Configure Telnet Access for MGMT interface
	10.3. STEP 3 >> Configure SSH Access for MGMT interface & create your own username and password
	10.4. STEP 4 >> Configure http Access for MGMT interface
11.	Verification Steps
	11.1. Step 1 >> Verify Management interface with telnet
	11.2. Step 2 >> Verify SSH Configuration
	11.3. Step 3> Verify http configuration



🛛 💋 0207-993-4928 🛛 🖂 <u>ir</u>

8 🔽 info@fortray.com



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.

info@fortray.com

- ✓ 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.



2020

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.







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	Туре	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 spre	adsheet	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.

	Student	ASA																		
NO	Student	FW	Test PC	PC	PC	Inside		Sec	Inside	Inside-	DMZ		Sec	DMZ	DMZ -	OUTSIDE		Sec	OUTISDE	OUTSIDE
	VLAIN	(Admin)	(RDP)	USERS	Password	Interface	NAMEIF	Level	VLAN	IP	Interface	NAMEIF	Level	VLAN	IP	Interface	NAMEIF	Level	VLAN	VLAN
1	21		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	ASA - 1	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	10.205.1.120	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	(Primary)	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		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	ASA - 1	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
_	20	10.205.1.121 (Deckup)	10.205.0.29																	
9	29	(васкир)	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		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	ASA - 1	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	10.205.1.120	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	(Primary)	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		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	ACA 1	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	ASA - 1 10 205 1 121	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	(Backup)	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 the Cisco ASA Firewall's Management interface for remote access purposes.



In this example we are configuring the mgmt interface

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

Summary of the Configuration Steps

- Configure OOB interface for management
- 🖊 The management interface should only handle management traffic
- 4 Use security level 99
- Allow telnet access
- Allow SSH access
- Allow HTTP access
- Configure Banners





10. Fortray CCNA Security Interface Configuration Task

In this example we are configuring the mgmt interface.

10.1. STEP 1 >> Configure the Layer 3 Interface Parameters

configure terminal interface Management0/0 description Management management-only nameif mgmt security-level 99 password cisco enable password cisco ip address 10.205.1.120 255.255.254.0 standby 10.205.1.121

10.2. STEP 2 >> Configure Telnet Access for MGMT interface

configure terminal
telnet 0.0.0.0 0.0.0.0 mgmt
telnet timeout 60



2020

10.3. STEP 3 >> Configure SSH Access for MGMT interface & create your own username and password

configure terminal
ssh 0.0.0.0 0.0.0 mgmt
ssh timeout 60
ssh version 2
Create a username with a password. (create your own user and password)
username fortray password cisco
Configure this local username to authenticate with SSH.
aaa authentication ssh console LOCAL
Create a RSA key pair.
crypto key generate rsa modulus 1024

10.4. STEP 4 >> Configure http Access for MGMT interface

configure terminal http server enable http server session-timeout 120 http 0.0.0.0 0.0.0 mgmt



11. Verification Steps

Follow the below commands to verify your configuration.

11.1. Step 1 >> Verify Management interface with telnet







11.2. Step 2 >> Verify SSH Configuration

😰 PuTTY Configuration		? ×]						
Category:									
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy 	Basic options for your PuTTY s Specify the destination you want to comm Host Name (or IP address) 10.205.1.120 Connection type: O Raw O Telnet O Riogin O SS Load, save or delete a stored session Saved Sessions Default Settings	eession Port 22							
- Telnet Rlogin SSH Serial	Close window on exit: Always Never Only on	clean exit	10.205.1.120 - PuTTY user-alert cancel FN-ASA-1-120/act/pr FN-ASA-1-120/act/pr FN-ASA-1-120/act/pr FN-ASA-1-120/act/pr	ci# ci# ci# ci#				- 0	×
About Help	Open	Cancel	FN-ASA-1-120/act/pp FN-ASA-1-120/act/pp FN-ASA-1-120/act/pp FN-ASA-1-120/act/pp FN-ASA-1-120/act/pp FN-ASA-1-120/act/pp FN-ASA-1-120/act/pp	-1# -::# -::# -::# -::# -::#					
			FN-ASA-1-120/act/pi FN-ASA-1-120/act/pi FN-ASA-1-120/act/pi FN-ASA-1-120/act/pi FN-ASA-1-120/act/pi FN-ASA-1-120/act/pi	::# ::# ::# ::# ::# ::# show :	aah sess				
			SID Client IP 1 10.205.0.221 FN-ASA-1-120/act/pr	Version 2.0	Mode Encryption H IN aes256-cbc s OUT aes256-cbc s	mac St hal Se hal Se	ate ssionStarted ssionStarted	Username admin admin	~



2020



11.3. Step 3> Verify http configuration

ß	← ← Cisco ASDM 7.1(1) × + ∨		-										
\leftarrow	\rightarrow \circlearrowright \pitchfork https://10.205.1.120/admin/public, \circlearrowright \bigstar	∽≒	h	r									
	Cisco ASDM 7.1(1) provides an intuitive graphical user interface that makes it configure and manage your Cisco security appliances.	L easy to											
	Cisco ASDM can run as a local application or as a Java Web Start application.												
	Run Cisco ASDM as a local application When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages: • You can invoke ASDM from a desktop shortcut. No browser is required. • One desktop shortcut allows you to connect to multiple security appliances.												
	Install A SDM Launcher												
	Run Cisco ASDM as a Java Web Start application												
	Java Web Start is required to run ASDM, but it is not installed on this o	computer.											
	Install Java Web Start												
	Copyright © 2006-2012 Cisco Systems, Inc. All rights reserved	d.											
L													



Thanks, and Good Luck

