



Cisco Secure Firewall 7.x Advanced Lab v3.0

Last Updated: 06-JANUARY--2022

About This Demonstration

This guide for this preconfigured demonstration includes:

- [Requirements](#)
- [About This Solution](#)
- [Topology](#)
- [Get Started](#)
- [Scenario 1: File & Malware Policy](#)
- [Scenario 2: IPS Policies](#)
- [Scenario 3: High Availability Configuration](#)
- [Scenario 4: AnyConnect with RADIUS](#)
- [Scenario 5: Site-to-Site VPN](#)
- [Scenario 6: Route Based VTI Site-to-Site VPN](#)
- [Scenario 7: Site-to-Site VPN Between FMC and FDM Managed Devices](#)
- [Scenario 8: Monitoring and Troubleshooting](#)
- [Scenario 9: PxGrid 2.0 Remediation with ISE using ANC](#)
- [Scenario 10: TLS/SSL Decryption](#)
- [Scenario 11: TLS Server Identity Discovery](#)
- [Scenario 12: Network Discovery and Firepower Recommendations](#)
- [Scenario 13: Cisco Threat Intelligence Director \(CTID\)](#)
- [Appendix A: FMC Pre-configuration](#)
- [Appendix B: REST API Scripts](#)
- [Appendix C: ISE RA VPN Configuration](#)

Requirements

The table below outlines the requirements for this preconfigured demonstration.

Table 1. Requirements

Required	Optional
• Laptop	• Cisco AnyConnect®

About This Solution

IT teams have been asked to manage security using a patchwork of siloed point products, starting with legacy next-generation firewalls (NGFW), which were created with a focus on application and bolted on best effort threat protection. As such, these legacy NGFWs are unable to provide an enterprise with the contextual information, automation, and prioritization that they need to handle today's modern threats.

Cisco Firepower is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. The system is designed to help you handle network traffic in a way that complies with your organization's security policy-your guidelines for protecting your network.

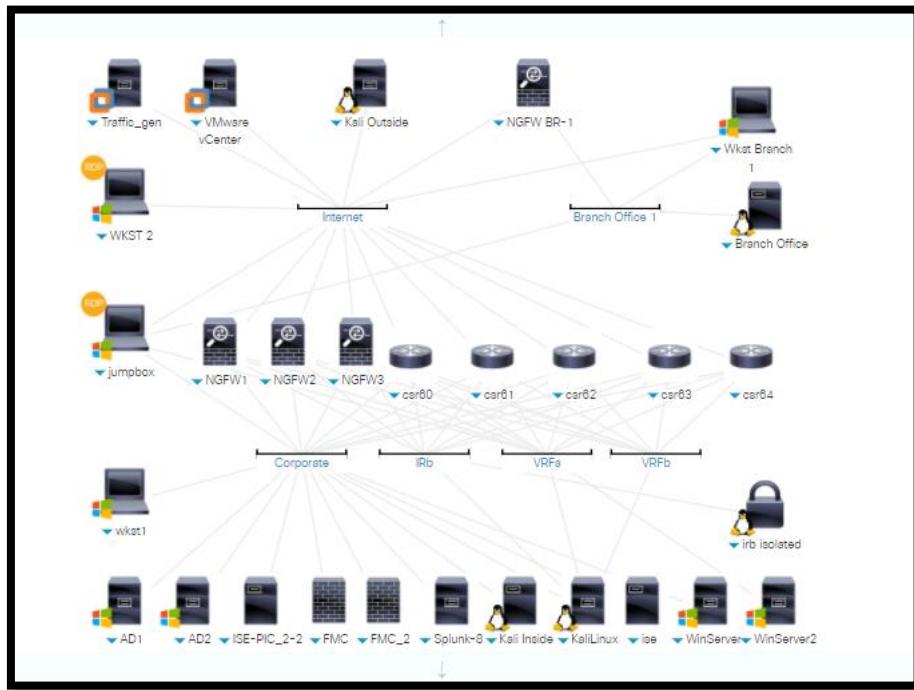
This allows the Cisco Firepower NGFW to evolve with a focus on enabling enterprises to stop, prioritize, understand, and automate responses to modern threats in real-time. Firepower NGFW is unique in its threat-focus, with a foundation of comprehensive network visibility, best-of-breed threat intelligence and highly-effective threat prevention to address both known and unknown threats. Firepower NGFW also enables retrospective security, through Advanced Malware Protection, that can "go back in time" to quickly find and remediate sophisticated attacks that may have slipped through defenses. This has led to a significant reduction in time-to-detection (TTD) for Cisco customers compared to industry averages.

In this lab you will build a multi-site network Next Generation Firewall (NGFW) solution at between a corporate and two branch sites. Using the Firepower Management Console (FMC) you will build High Availability NGFWs at the corporate site, and manage a branch. In this lab you will also configure a NGFW using the FDM (Firepower Device Manager). You will also configure remote access and site to site VPNs. You will also configure Cisco Threat Intelligence Director to accept and implement third party updates to your NGFW devices.

Topology

This content includes preconfigured users and components to illustrate the scripted scenarios and features of the solution. Most components are fully configurable with predefined administrative user accounts. You can see the IP address and user account credentials to use to access a component by clicking the component icon in the **Topology** menu of your active session and in the scenario steps that require their use.

Figure 1. dCloud Topology



Get Started

BEFORE PRESENTING

Cisco dCloud strongly recommends that you perform the tasks in this document with an active session before presenting in front of a live audience. This will allow you to become familiar with the structure of the document and content.

It may be necessary to schedule a new session after following this guide in order to reset the environment to its original configuration.

PREPARATION IS KEY TO A SUCCESSFUL PRESENTATION.

Follow the steps to schedule a session of the content and configure your presentation environment.

1. Initiate your dCloud session. [[Show Me How](#)]

NOTE: It may take up to 10 minutes for your session to become active.

2. For best performance, connect to the workstation with **Cisco AnyConnect VPN** [[Show Me How](#)] and the **local RDP client on your laptop** [[Show Me How](#)]

Jump PC: **198.18.133.50**, Username: **administrator**, Password: **C1sco12345**

NOTE: You can also connect to the workstation using the Cisco dCloud Remote Desktop client [[Show Me How](#)]. The dCloud Remote Desktop client works best for accessing an active session with minimal interaction. However, many users experience connection and performance issues with this method.

NOTE: Check the connection for Remote Desktops for Wkstbr2 make sure you get the Login prompt password C1sco12345

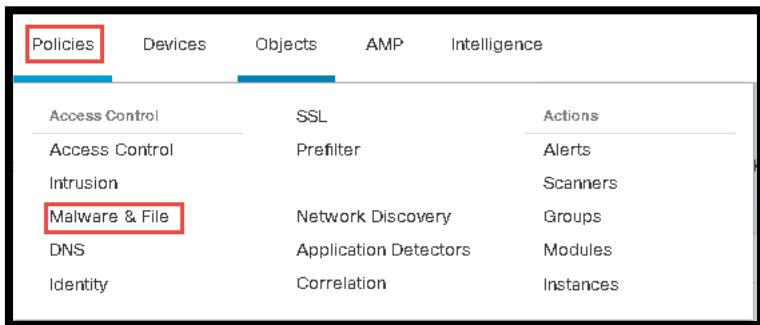
Scenario 1. File & Malware Policy

This exercise consists of the following tasks.

- Configure the Malware & File policy settings in the FMC to allow the FTD to block files that are identified as malware and block specified file types

Create Malware & File Policy

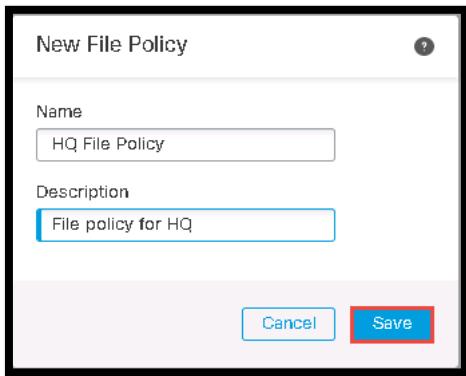
- Login to the FMC **admin/C1sco12345**
- Click **Policies** and select **Malware & File**



- Click **New File Policy**

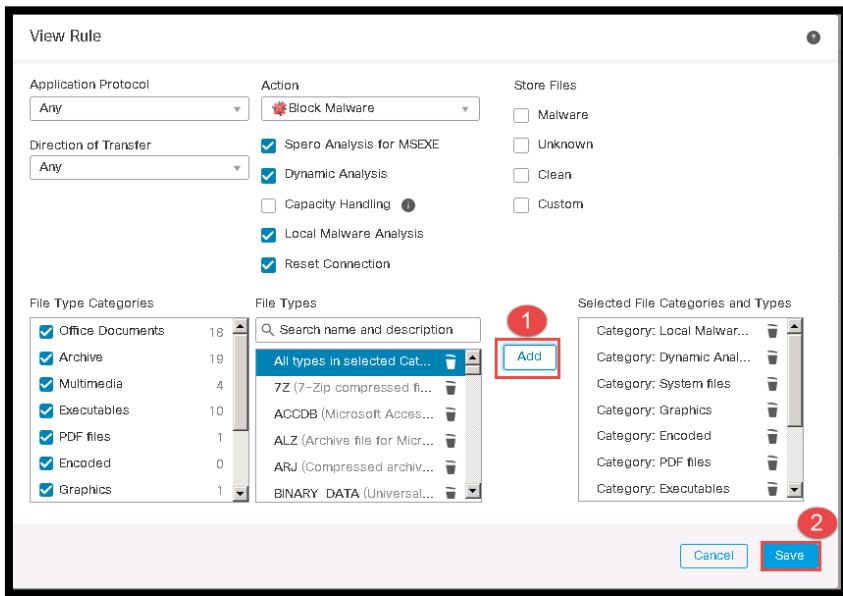


- Enter the following:
 - Name: **HQ File Policy**
 - Description: **File policy for HQ**

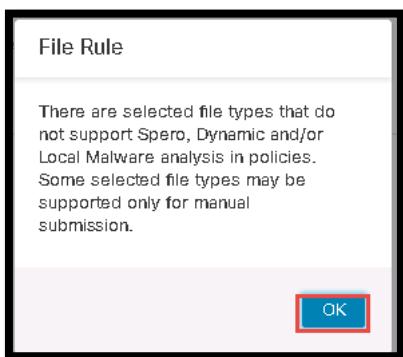


- Save**
- Click Add Rule**
- Configure the rule to apply to all possible protocols and file types with the following:
 - Application Protocol: **Any**
 - Direction of Transfer: **Any**
 - Action: **Block Malware**
 - Spero Analysis for MSEXE: **checked**
 - Dynamic Analysys: **checked**
 - Local Malware Analysis: **checked**
 - Reset Connection: **checked**

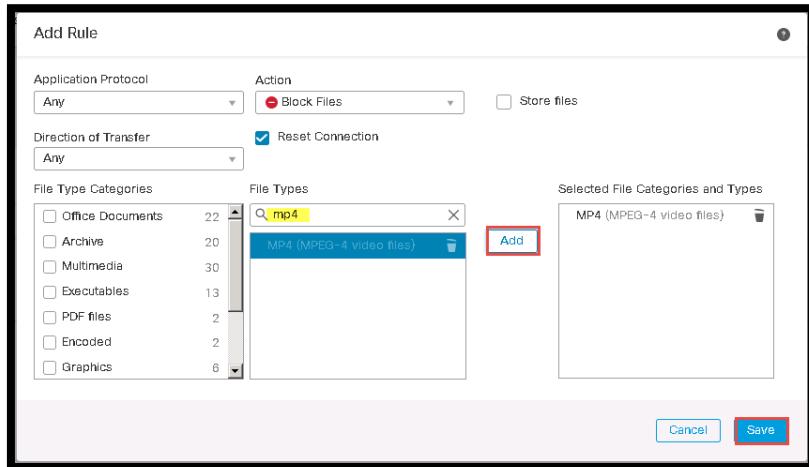
- h. File type Categories: (**place a checkmark in all categories**)
 i. File types: All types in selected Categories



8. Click **Add** and **Save**
 9. Click **OK** on **File Rule** box

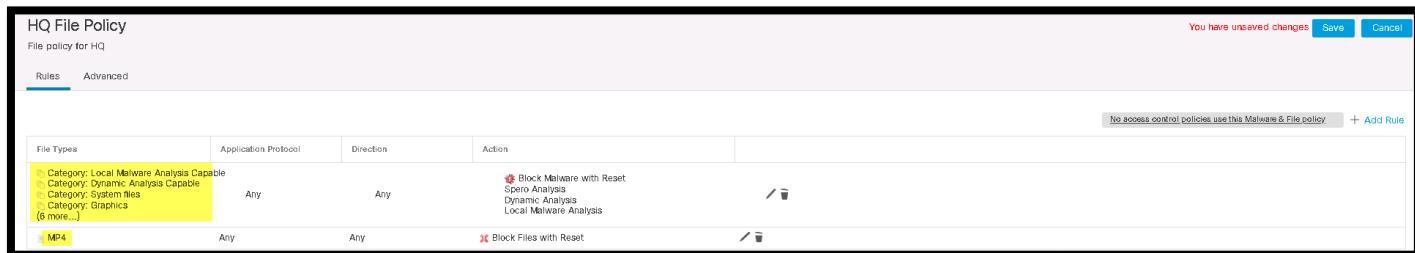


10. Click on **Add Rule** to add another rule
 11. Configure the Following:
 a. Application Protocol: **Any**
 b. Direction of Transfer: **Any**
 c. Action: **Block Files**
 d. Reset Connection: **Checked**
 e. File Types: **MP4**
 12. Click the **Add** button to add **MP4** to the Selected File Categories and Types section



13. Click Save

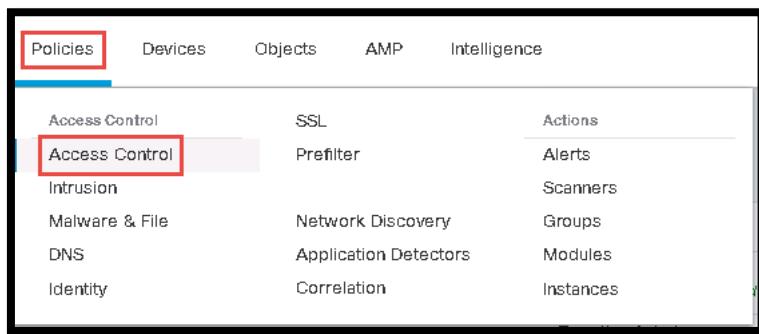
14. The HQ File Policy should look like this:



NOTE: You are blocking MP4 files as an example of a specific file type. The Firewall will block this file type regardless, if it is clean, unknown or malicious without further inspection. For customer deployments make sure you understand their requirements for file blocking.

15. Click **Save** to save the changes to the File & Malware policy

16. Click on **Policies** menu and select **Access Control**



17. Double click on **Base_Policy** to edit

18. Disable or delete the Block ICMP Over GRE rule in the Mandatory rule section

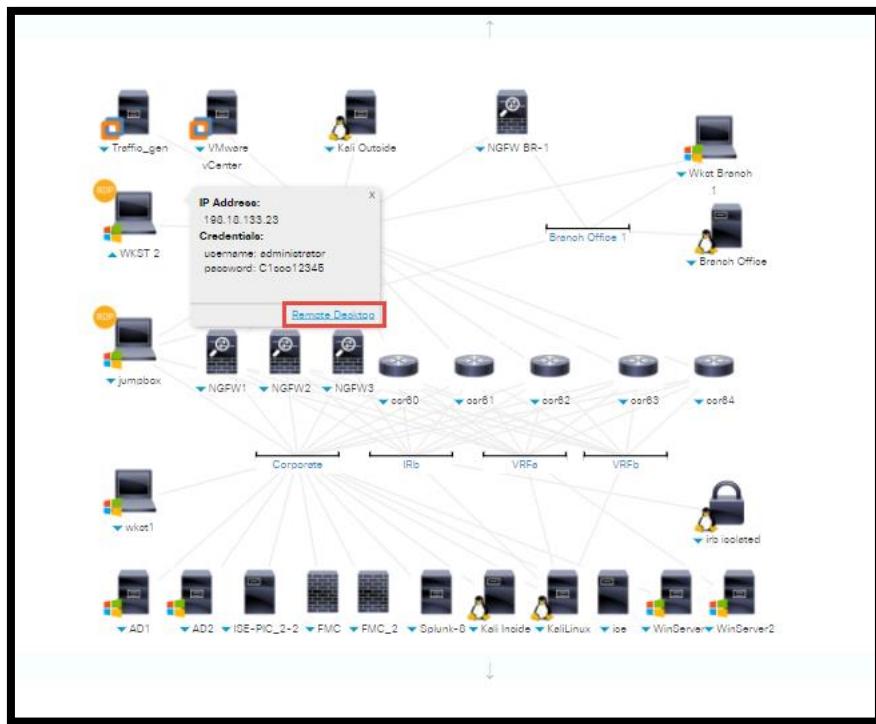
19. Disable or delete the Allow GRE Traffic in the Default rule section

20. Modify the **Allow Outbound rule Web Server Access** rule Inspection to use File Policy **HQ File Policy**

a. Make sure each rule is also logging at the end of the connection

21. Click **Save** and then **Deploy** the Changes

22. Go to wkst2 from the dCloud menu



- a. Double Click on the Firefox Icon



- b. In the URL Field type: <http://198.18.128.202>
c. Click on the **Files** link
d. Right Click on **Zombies.pdf** and select Save Link As... Save to Desktop: This should Fail (If you right click on the **Zombies.pdf** file on the desktop and look at properties you will see the file has **0 Bytes**)
e. Right Click on **test1.mp4** and select Save Link As... Save to Desktop: This should Fail (If you right click on the **test1.mp4** file on the desktop and look at properties you will see the file has **0 Bytes**)
f. Move **Zombies.pdf** and **test1.mp4** to the Recycle Bin

23. You have now Checked the HQ File Policy from OutZone to InZone1

- a. OPTIONAL
i. Type <HTTPS://198.18.128.202>
1. Try downloading **test1.mp4** it should succeed (This is because you are downloading the file over an encrypted connection so the traffic cannot be inspected. This will be fixed in a later lab).

24. Log back into the FMC **admin/C1sco12345**

- a. Go to Analysis > Connection Events and look at the logs you will see the **File Block** also go to **Malware Events** and **File Events** to show the files that were blocked.

Scenario 2. IPS Policies

In this scenario we will configure and use custom IPS policies. You will make copies of the Balanced Security and Connectivity and Security Over Connectivity policies; modify the variables used by the policies and apply those polices to the ACP.

Create IPS Policies

1. Login to the FMC from the Jumpbox
2. Click **Policies** menu and select **Intrusion**

The screenshot shows the FMC's main navigation bar with tabs for Policies, Devices, Objects, AMP, and Intelligence. The Policies tab is active. Below the navigation, there is a grid of policy categories. The 'Intrusion' category is highlighted with a red box around its name. Other categories include Access Control, SSL, Prefilter, Alerts, Malware & File, Network Discovery, Scanners, DNS, Application Detectors, Groups, Identity, Correlation, Modules, and Instances.

3. You will see that **Demo Intrusion Policy** is defined
4. Click **Create Policy** [Accept the warning if prompted]
5. Set the following values:
 - a Name: **HQ-Balanced-Policy**
 - b Description: **Policy for standard traffic at HQ**
 - c Inspection Mode: **Prevention**
 - d Base Policy: **Balanced Security and Connectivity**

The dialog box has a title 'Edit Intrusion Policy'. It contains fields for 'Name*' (set to 'HQ-Balanced-Policy'), 'Description' (set to 'Policy for standard traffic at HQ'), and 'Inspection Mode' (radio button selected for 'Prevention'). Below these, a note states: 'Intrusion rule actions are always applied. Connections that match a drop rule are blocked.' Under 'Base Policy', a dropdown menu is set to 'Balanced Security and Connectivity'. At the bottom are 'Cancel' and 'Save' buttons, with 'Save' being highlighted with a red box.

6. Click Create Policy

7. You will now create another policy. Click **Create Policy**
8. Set the following values:
 - a Name: **HQ-High-Security-Policy**
 - b Description: **Policy for traffic outside HQ**
 - c Inspection Mode: **Prevention**
 - d Base Policy: **Security Over Connectivity**

Create Intrusion Policy

Name*
HQ-Hight-Security-Policy

Description
Policy for traffic outside HQ

Inspection Mode
 Detection Prevention

Intrusion rule actions are always applied. Connections that match a drop rule are blocked.

Base Policy
Security Over Connectivity

Cancel Save

9. On the policies page click the **Snort 2 or Snort 3 Version**

Intrusion Policies		Network Analysis Policies			
Show Snort 3 Sync status	Search by Intrusion Policy, Description, or Base Policy	All IPS Rules	IPS Mapping	Compare Policies	Create Policy
Intrusion Policy	Description	Base Policy	Usage Information	Snort 2 Version	Snort 3 Version
Demo Intrusion Policy		Balanced Security and Connectivity	3 Access Control Policies 2 Devices		
HQ-Balanced-Policy	Policy for standard traffic at HQ	Balanced Security and Connectivity	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version
HQ-Hight-Security-Policy	Policy for traffic outside HQ	Security Over Connectivity	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version

10. Look at the Number of rules that are enabled for that policy
 - a Snort 3 Example shown below

Intrusion Policy

Policy Name: HQ-Balanced-Policy

Mode: Prevention | **Base Policy**: Balanced Security and Connectivity

Description: Policy for standard traffic at HQ

Disabled: 36695 | **Alert**: 467 | **Block**: 6397 | **Overridden**: 0

Rule Groups

51 items | **Search Rule Group** | Excluded | Included | Overridden

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action	Info	Rule Action	Assigned Groups	Comments
0 SID/SID		1:28498	BROWSER-IE Microsoft Internet Explorer CreateRange user after free attempt	Browser/Internet Explorer
		1:32478	BROWSER-IE Microsoft Internet Explorer CSecurityContext use after free attempt	Browser/Internet Explorer
		1:32479	BROWSER-IE Microsoft Internet Explorer CSecurityContext use after free attempt	Browser/Internet Explorer
		1:28633	BROWSER-IE Microsoft Internet Explorer Html reload loop attempt	Browser/Internet Explorer
		1:31821	BROWSER-IE Microsoft Internet Explorer Onreadystatechange use after free attempt	Browser/Internet Explorer
		1:31822	BROWSER-IE Microsoft Internet Explorer Onreadystatechange use after free attempt	Browser/Internet Explorer
		1:27788	BROWSER-PLUGINS Oracle Java Security Slider feature bypass attempt	Browser/Plugins
		1:27789	ENDPOINT-KT Blackhole/2!CnH exploit kit outbreak module available now	Malware/Exploit Kit

11. Click on < Intrusion Policy to go back to Intrusion Policies
12. Edit the **HQ-High-Security-Policy** and look at the number of rules.

Intrusion Policy

Policy Name: HQ-High-Security-Policy

Mode: Prevention | **Base Policy**: Security Over Connectivity

Description: Policy for traffic outside HQ

Disabled: 27725 | **Alert**: 637 | **Block**: 17097 | **Overridden**: 0

Rule Groups

58 items | **Search Rule Group** | Excluded | Included | Overridden

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action	Info	Rule Action	Assigned Groups	Comments
0 SID/SID		108.4	(rpc_decode) incomplete RPC segment	Protocol/Builtin
		108.3	(rpc_decode) large RPC record fragment	Protocol/Builtin
		108.5	(rpc_decode) zero-length RPC fragment	Protocol/Builtin
		1:13359	APP-DETECT failed IMAP login attempt - invalid username/password	Potentially Unwanted Applications/Application...
		1:27999	APP-DETECT Possible Dynamic Internet Technology Frontgate application PL...	Potentially Unwanted Applications/Application...
		1:38788	BROWSER-IE Microsoft Internet Explorer CreateColorSpace vulnerability atte...	Browser/Internet Explorer
		1:28677	BROWSER-IE Microsoft Internet Explorer CRootElement Object use after free...	Browser/Internet Explorer
		1:38678	BROWSER-IE Microsoft Internet Explorer CRootElement Object use after free...	Browser/Internet Explorer

13. Add an Intrusion Rule to the Policy to **Snort 2** if you want Snort 3 start after Step (i)
 - a Click on **HQ-High-Security-Policy** > **Snort 2 Version**
 - b Click on Policy Layers > My Changes click Manage Rules

The screenshot shows the 'Policy Information' section with the 'Rules' tab selected. On the left, a sidebar lists 'Policy Layers' with 'My Changes' highlighted. The main area displays the 'Layer: My Changes' configuration. It includes fields for 'Name' (My Changes), 'Description', 'Sharing' (unchecked), and a 'Rules (0)' section showing 0 rules generate events, 0 rules drop and generate events, and 0 rules disabled. A 'Manage Rules' button is highlighted with a red box. Below this is a 'Specific Threat Detection' section with 'Sensitive Data Detection' checked, and buttons for 'Enabled', 'Disabled', and 'Inherit'.

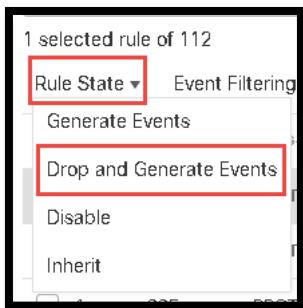
c Under Rule Configuration Rule Content Categories Scroll down until you see: **protocol-ftp** and Click

The screenshot shows the 'Rules - Layer: M' configuration interface. On the left, a sidebar lists 'Rule Configuration', 'Rule Content', and 'Category'. The 'Category' dropdown menu is open, showing a list of categories including 'os-windows', 'policy-multimedia', 'policy-other', 'policy-social', 'policy-spam', 'preprocessor', 'protocol-dns', 'protocol-finger', 'protocol-ftp' (which is highlighted with a red box), 'protocol-icmp', 'protocol-imap', 'protocol-nntp', 'protocol-other', and 'protocol-pop'. The 'Protocol-ftp' category is the target of the instruction.

d Click on the SID field to sort the Rules by number and select rule **336**

Filter:		
Category:"protocol-ftp"		
0 selected rules of 112		
Rule State ▾ Event Filtering ▾ Dynamic State ▾ Alerting ▾ Comments ▾		
GID	SID ▾	Message
1	144	PROTOCOL-FTP ADMw0rm ftp login attempt
1	334	PROTOCOL-FTP .forward
1	335	PROTOCOL-FTP .rhosts
1	336	PROTOCOL-FTP CWD ~root attempt
1	337	PROTOCOL-FTP CEL overflow attempt
1	353	PROTOCOL-FTP adm scan
1	354	PROTOCOL-FTP iss scan
1	355	PROTOCOL-FTP pass whoot

e Under Rule State choose: **Drop and Generate Events**

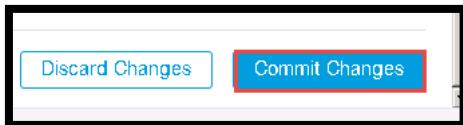


f At the Success Window click **OK**

g You will now see an Orange Triangle by **Policy Information** click on the Triangle



h Go to the bottom of the screen and click **Commit Changes**



i In the Description of Changes window type: **Add FTP Intrusion Rule** and click **OK**

14. SNORT 3

a HQ-High-Security-Policy

i Snort 3 Version

b Under rule Groups click on **Protocol** and **Select FTP** and then click the SID to sort by number and select SID **336**

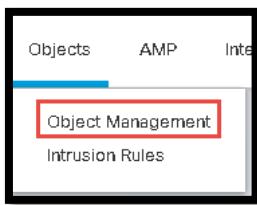
The screenshot shows the 'Intrusion Policy' interface for the 'HQ-High-Security-Policy'. The left sidebar lists 'Rule Groups' such as Malware, File, Operating Systems, and Protocol (including ICMP, SCADA, NetBIOS, and FTP). The main pane displays 'Protocol / FTP' rules. Rule 1:338 is highlighted with a red box and an arrow pointing to its 'Info' link. The rule details are as follows:

Rule Action	Description	Rule Action	Assigned Groups	Comments
<input type="checkbox"/> 1:144	PROTOCOL-FTP ADMwOrm ftp login attempt	<input type="button" value="Disable (Default)"/>	Protocol/FTP	
<input type="checkbox"/> 1:334	PROTOCOL-FTP forward	<input type="button" value="Disable (Default)"/>	Protocol/FTP	
<input type="checkbox"/> 1:335	PROTOCOL-FTP_rhosts	<input type="button" value="Disable (Default)"/>	Protocol/FTP	
<input checked="" type="checkbox"/> 1:338	PROTOCOL-FTP CWD ~root attempt	<input type="button" value="Block"/>	Protocol/FTP (Overridden)	
<input type="checkbox"/> 1:337	PROTOCOL-FTP CEL overflow attempt	<input type="button" value="Disable (Default)"/>	Protocol/FTP	
<input type="checkbox"/> 1:353	PROTOCOL-FTP adm scan	<input type="button" value="Disable (Default)"/>	Protocol/FTP	
<input type="checkbox"/> 1:354	PROTOCOL-FTP iss scan	<input type="button" value="Disable (Default)"/>	Protocol/FTP	

Customize IPS Variable Sets

You will now create Variable Sets for these policies.

1. Click **Objects** and menu and select **Object Management**



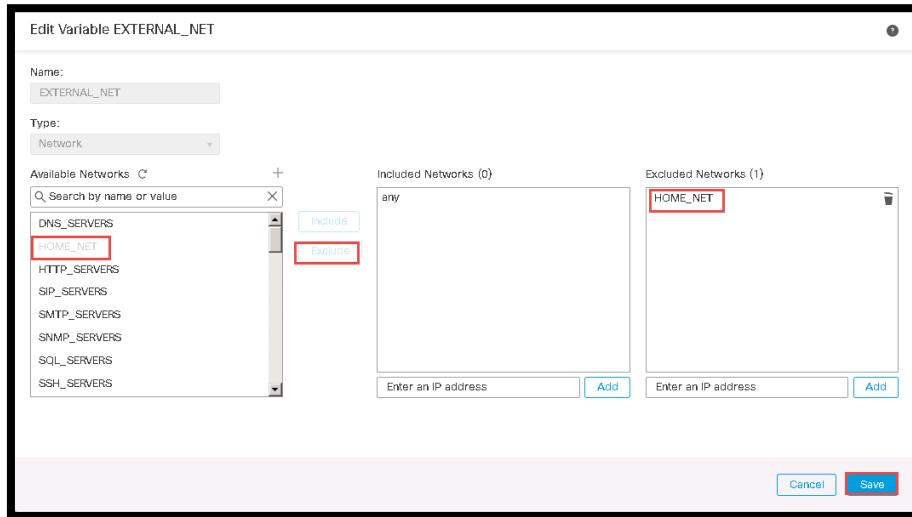
2. On the left window pane Click on **Variable Set**



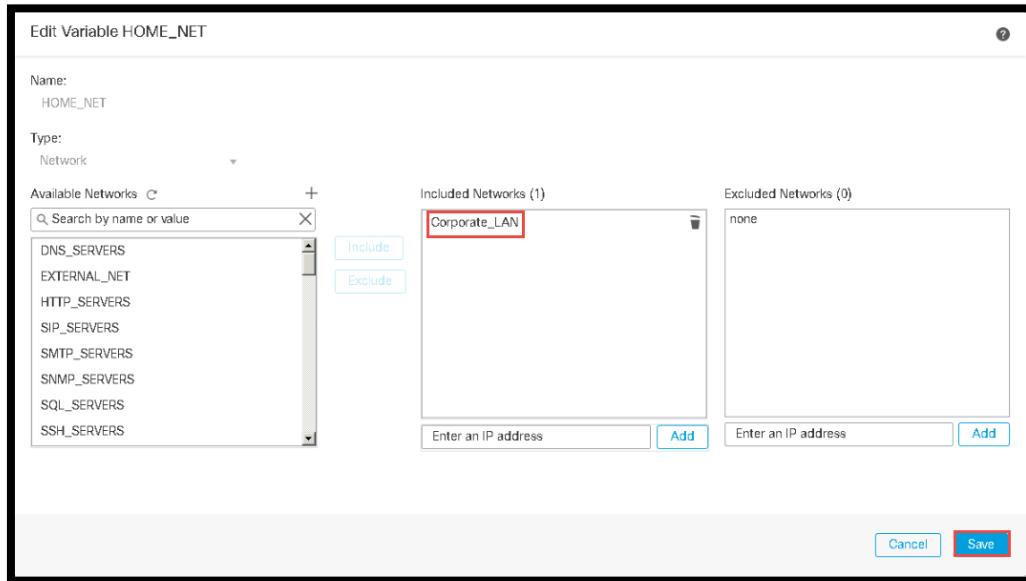
3. Click **Add Variable Set**

- a Name: **ExternalTraffic**
- b Description: **Used for rules involving an internet host. Defines External as anything not internal**

4. Click the **Edit** button for the **EXTERNAL_NET** variable
5. In the list of Available Networks select **HOME_NET** and click **Exclude** to add it to the list of Excluded Networks and **Save**



6. Click **Home_Net**
7. Select and add **Corporate_LAN** (198.19.10.0/24) if not specified and select **Include**
8. **Save**



9. Click **Save**
10. Note that the **EXTERNAL_NET** is now listed as a Customized Variable and its value is anything that is not **HOME_NET** and **HOME_NET** is also a Customized Variable

EXTERNAL_NET	Network	!HOME_NET	
HOME_NET	Network	Corporate_LAN	
Default Variables			

11. Click **Save**
12. Click **Add Variable Set**
13. Configure the following:
 - a Name **InternalTraffic**
 - b Description: **Used for traffic crossing the FTD but not Internet related. Defines External as Any**

New Variable Set

Name:	InternalTraffic		
Description:	related. Defines External as Any		
Add			
Variable Name	Type	Value	
Customized Variables			
This category is empty			
Default Variables			
DNS_SERVERS	Network	Authorized-Internal-DNS-Servers	
EXTERNAL_NET	Network	any	
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	
FTP_PORTS	Port	[21, 2100, 3535]	
GTP_PORTS	Port	[3386, 2123, 2152]	
HOME_NET	Network	[Corporate_LAN, DMZ-Web]	

Cancel **Save**

14. Click **Save**

NOTE: The InternalTraffic set is not functionally different from the DefaultSet right now. For the current configuration DefaultSet could be used in place of InternalTraffic.

Configure ACP to Use IPS Policies

You have configured some IPS policies and Variable Sets but have not attached these configurations to ACP rules

1. Click the **Policies** menu and select **Access Control**
2. Click on edit [Pencil] icon for the **Base_Policy**
3. Select the **Advanced** tab

Base_Policy

ACP for Corporate Network

SSL Policy to use for inspecting encrypted connections: None

Prefilter Policy Settings: Default Prefilter Policy

Network Analysis and Intrusion Policies: No Rule Active

Intrusion Policy used before Access Control rule is determined: Default-Set

Intrusion Policy Variable Set: Balanced Security and Connectivity

4. Click the **Edit** button for **Network Analysis and Intrusion Policies**
5. Configure the following:
 - a. Intrusion Policy used before Access Control rule is determined: **HQ-High-Security-Policy**
 - b. Intrusion Policy Variable Set: **ExternalTraffic**

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined: HQ-High-Security-Policy

Intrusion Policy Variable Set: ExternalTraffic

Network Analysis Rules: No Custom Rules | Network Analysis Policy List

Default Network Analysis Policy: Balanced Security and Connectivity

Revert to Defaults | OK

6. Click **OK**
7. Click **Rules**
8. Edit the **Web Server Access Rule**
9. Click **Inspection**
10. Change the following:
 - a. Intrusion Policy: **HQ-High-Security-Policy**
 - b. Variable Set: **ExternalTraffic**

11. Click **Save**
12. Locate the **Allow Outbound** InZone(s) to OutZone
13. Go to **Inspection** and Configure the following:
 - a Intrusion Policy: **HQ-Balanced-Policy**
 - b Variable Set: **ExternalTraffic**

14. Click **Save**
15. **Save** the ACP and **Deploy**

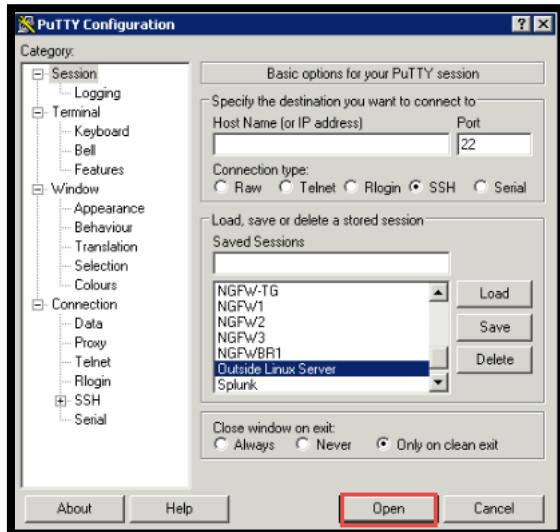
Test IPS Policies

You will now test that IPS policy using Metasploit and review events.

1. Click on **PuTTY Icon** on the Jumpbox desktop



2. Click on the **Outside Linux Server** and then click **Open**



3. Login as: **root/C1sco12345**
4. Type: **msfconsole**

```
root@KaliLinuxOutside:~# msfconsole
[-] ***Rting the Metasploit Framework console...\
[-] * WARNING: No database support: could not connect to server: Connection refused
Is the server running on host "localhost" (::1) and accepting
TCP/IP connections on port 5432?
```

5. Once the console loads type the following: **use auxiliary/scanner/http/dir_webdav_unicode_bypass**

```
msf6 > use auxiliary/scanner/http/dir_webdav_unicode_bypass
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) >
```

6. Type the following command
 - a. set RHOSTS **198.18.128.202**

7. Type **set THREADS 20**

```
msf6 > use auxiliary/scanner/http/dir_webdav_unicode_bypass
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) > set RHosts 198.18.128.202
RHosts => 198.18.128.202
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) > set THREADS 20
THREADS => 20
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) >
```

8. Type **run**

```

msf6 > use auxiliary/scanner/http/dir_webdav_unicode_bypass
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) > set RHosts 198.18.128.202
RHosts => 198.18.128.202
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) > set THREADS 20
THREADS => 20
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) > run

[*] Using code '404' as not found.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) >

```

9. Close the putty window and go back to the FMC
10. Click on **Analysis > Connections > Events**
11. Click on **Edit Search** to specify search criteria for connection events
 - a. Action: **Block**

General Information

First Packet	> 2009-07-16 13:00:31, < today at 4:30pm
Last Packet	> 2009-07-16 13:00:31, < today at 4:30pm
Action	Block
Allow, Block	

12. Scroll down to the **Networking** section
 - a. Initiator IP field type **198.18.133.200**

Networking

Geolocation	Initiator IP*	198.18.133.200	192.168.1.0/24, !192.168.1.3, block, monitor
Device	Responder IP*		192.168.1.0/24, !192.168.1.3, block, monitor
SSL	Original Client IP*		192.168.1.0/24, !192.168.1.3, 2001:db8:85a3::1370
Application			

13. Click on **Search** at the top right screen
14. Notice the Action, Reason and URL

Connection Events (select workflow)

2021-10-01 12:42:07 - 2021-10-01 19:11:17 Expanding

Table View of Connection Events																		
Jump to...		Table View of Connection Events																
		Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
		Block	Intrusion Block	198.18.133.200		198.19.10.202		Outzone	InZone1	38885 / tcp	80 (http) / tcp	HTTP	Internet Explorer	http://198.18.128.202/mx-console/			NGFW1	

15. Go to **Analysis > Intrusions > Events**

Events By Priority and Classification (switch_worldflow)

No Search Constraints (Edit Search)

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

	Message	Priority	Classification	Count
<input checked="" type="checkbox"/>	SERVER-WEBAPP JBoss JMX console access attempt [1:21516:9]	medium	Attempted Information Leak	1

16. Click on the arrow next to the messages

Events By Priority and Classification (switch_worldflow)

Search Constraints (Edit Search)

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

Time	Priority	Impact	Initial Result	Reason	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Type	SSL Status	VLAN ID	Message	Classification	Generator
2021-10-01 19:07:54	medium	6	Dropped		198.18.133.200		198.19.10.202		38885 / tcp	80 (http) / tcp	Unknown (Unknown)	0	SERVER-WEBAPP JBoss JMX console access attempt [1:21516:9]	Attempted Information Leak	Standard Test

Source User	Application Protocol	Client	Web Application	IOC	Application Risk	Business Relevance	Ingress Security Zone	Egress Security Zone	Device	Ingress Interface	Egress Interface	Ingress Virtual Router	Egress Virtual Router	Intrusion Policy	Access Control Policy	Access Control Rule	Network Analysis Policy
No Authentication Required	HTTP	Internet Explorer	Web Browsing	Medium	Medium	Outzone	InZone	NGFW1	Outside_Interface	Inside_Interface	Global	HQ-High-Security-Policy	Base_Policy	Web Server Access	Balanced Security and Connectivity		

17. Scroll to the right to see Intrusion Policy, Access Control Policy and Rule that caught the compromise.

Scenario 3. High Availability Configuration

This exercise consists of the following tasks.

- Configure and Deploy Backup NGFW
- Configure and Deploy Backup FMC
- Create High Availability Pair of Firewalls
- Configure Active/Standby with Virtual Mac Address
- Test the configuration

The objective of this exercise is to understand and configure High Availability for NGFW. You will configure the second firewall and then add it to the High Availability group.

Steps

Run the REST API script to configure NGFW3

1. Go to the Jump PC and Open the PUTTY Session Select **NGFW3** Select Load Select Open
 - a. Username: **admin** password: **C1sco12345**
 - b. Type: show managers
 - c. Output should read Managed Locally
 - d. If it says managed locally type:
 - a. configure manager delete and select **yes** then follow step [e] below
 - e. If it says No managers configured
 - i. Type the following: configure manager add fmc.dcloud.local C1sco12345 select **yes** (must type yes in full)
 - ii. When command prompt returns type: show managers make sure fmc.dcloud.local shows “status pending”

NOTE: The following information is communicated over the failover link:

The unit state (active or standby)

Hello messages (keep-alives)

Network link status

MAC address exchange

Configuration replication and synchronization

Creating or breaking a Firepower Threat Defense high availability pair immediately restarts the Snort process on the primary and secondary devices, temporarily interrupting traffic inspection on both devices. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See Snort® Restart Traffic Behavior for more information. The system warns you that continuing to create a high availability pair restarts the Snort process on the primary and secondary devices and allows you to cancel.

2. On the Inside Linux server [root/C1sco12345]

- Type **runapiscript** wait for the prompt
- When asked **Which Firewall do you want to register?** Type the number **3**
- When it asked **Enter name of new Access Control Policy to be create: (Type HA) for the name)**

```
root@inside:~ [root@inside ~]# runapiscript
Specify firewall to register.
Enter 1 for NGFW1.
Enter 2 for NGFW2.
Enter 3 for NGFW3.
Which firewall do you want to register? 3
```

- Go back to Firefox and check the registration status of NGFW3 on the FMC and allow device to register
- Go to Device> Device Management> NGFW3 and enable the interfaces GigabitEthernet0/0-0/4 and remove the names from the interfaces
- Click Save

Configure High Availability Pair

1. Go to Devices > Device Management> Add > Add High Availability

Name	Model	Version	Chassis	Licenses	Access Control Policy
NGFW1 198.19.10.81 - Routed	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	Base_Policy
NGFW3 198.19.10.83 - Routed	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	HA

NOTE: The NGFW3 Management Interface (198.19.10.83) was preconfigured during initial setup. Interfaces G0/0 and G0/1 were configured by the script. They do not have security zones listed on the interface, but they will inherit the security zones and the interface IP Address' from NGFW1 when the HA process is run.

- Name: HA_Test
- Device Type: Firepower Threat Defense
- Primary Peer: NGFW1
- Secondary Peer: NGFW3
- Then Continue

Add High Availability Pair

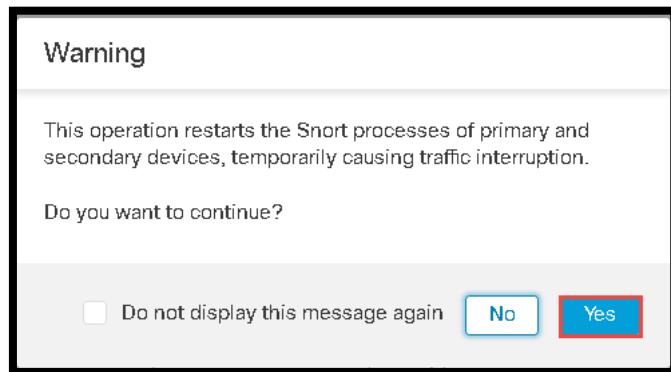
Name:^{*} 1

Device Type: 2

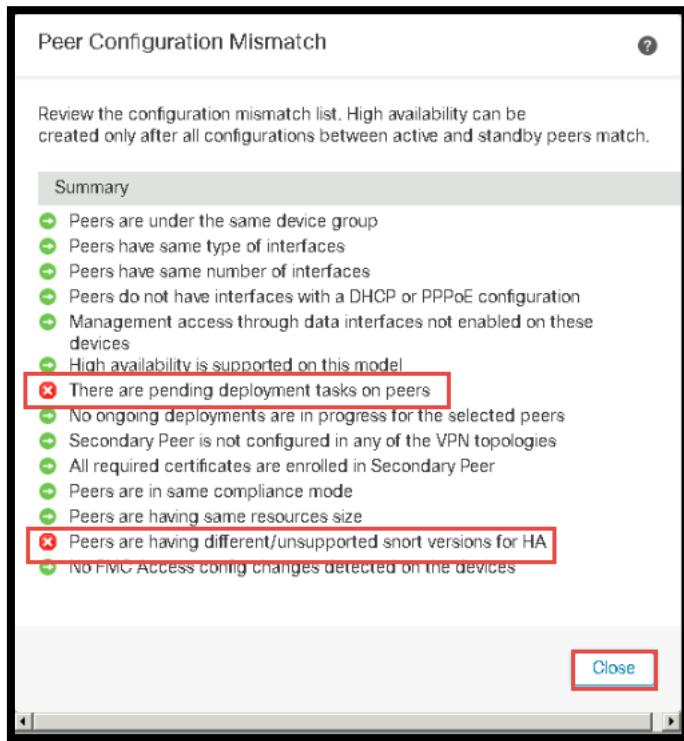
Primary Peer: 3

Secondary Peer: 4

Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers. 5



NOTE: If you have done configuration tasks on either of the HA Peers and have not deployed then you will get the following message:



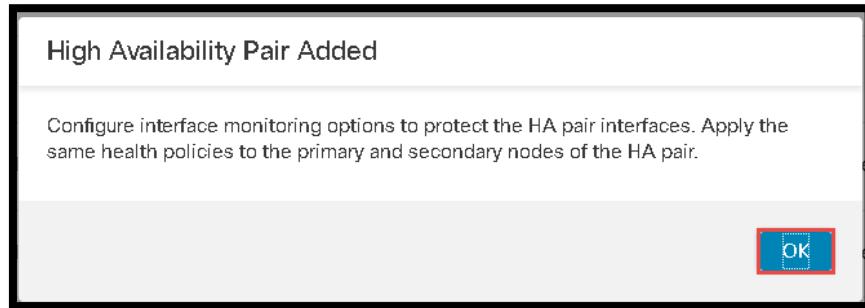
2. If needed On NGFW3 go to Device > Inspection Engine > Revert to Snort2
3. On NGFW1 go to GigabitEthernet0/3 Edit and delete the name and Security Zone of that Interface
4. Deploy the changes to NGFW1 and NGFW3
5. Go back and repeat step 1
6. Select Interface: GigabitEtherent0/3
7. Name: Failover_Link
8. Primary IP: 198.19.254.1
Secondary IP: 198.19.254.2 Subnet Mask: 255.255.255.0
9. State Link: Interface Same as LAN Failover
10. IPsec Encryption: Enabled (OPTIONAL)

NOTE: If Interfaces do not show up go back to Devices > Device Manager > Click on the Pencil Icon for each firewall click on the Interfaces to make sure they are enabled and that the interfaces do not have names.

Add High Availability Pair

High Availability Link	State Link
Interface: * <input type="text" value="GigabitEthernet0/3"/> 1	Interface: * <input type="text" value="Same as LAN Failover"/> 2
Logical Name: * <input type="text" value="Failover_Link"/> 3	Logical Name: * <input type="text" value="Failover_Link"/>
Primary IP: * <input type="text" value="198.19.254.1"/> 4	Primary IP: * <input type="text" value="198.19.254.1"/>
<input type="checkbox"/> Use IPv6 Address	<input type="checkbox"/> Use IPv6 Address
Secondary IP: * <input type="text" value="198.19.254.2"/> 5	Secondary IP: * <input type="text" value="198.19.254.2"/>
Subnet Mask: * <input type="text" value="255.255.255.0"/> 6	Subnet Mask: * <input type="text" value="255.255.255.0"/>
IPsec Encryption	
<input type="checkbox"/> Enabled Key: <input type="text" value="Auto"/> Generation:	
<small>LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.</small>	
7 <input type="button" value="Cancel"/> <input style="background-color: red; color: white; border: 2px solid red;" type="button" value="Add"/>	

11. Click on OK to add the High Availability Pair



NOTE: The configuration of the HA will take some time you will see status updates from time to time if you watch the Tasks next to the deployment button.

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
HA_Test					
NGFW1(Primary, Unknown) 198.18.10.81 - Router	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	Base_Policy
NGFW3(Secondary, Unknown) 198.18.10.83 - Router	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	HA

12. When complete you will see the following:

13. Go to Devices > Device Management Click on the pencil icon next to the HA Policy

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
HA_Test					
NGFW1(Primary, Active) 198.18.10.81 - Router	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	Base_Policy
NGFW3(Secondary, Standby) 198.18.10.83 - Router	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	Base_Policy

NOTE: MAC Addresses and IP Addresses in Failover.

When you configure your interfaces, you can specify an active IP address and a standby IP address on the same network.

Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state. You also cannot connect to the standby unit on that interface for management purposes.

When the primary unit or failover group fails over, the secondary unit assumes the IP addresses and MAC addresses of the primary unit and begins passing traffic.

The unit that is now in standby state takes over the standby IP addresses and MAC addresses.

Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

If the secondary unit boots without detecting the primary unit, the secondary unit becomes the active unit and uses its own MAC addresses, because it does not know the primary unit MAC addresses. However, when the primary unit becomes available, the secondary (active) unit changes the MAC addresses to those of the primary unit, which can cause an interruption in your network traffic. Similarly, if you swap out the primary unit with new hardware, a new MAC address is used.

Virtual MAC addresses guard against this disruption because the active MAC addresses are known to the secondary unit at startup, and remain the same in the case of new primary unit hardware. In multi-instance capability the FXOS chassis autogenerates only primary MAC addresses. You can overwrite the generated MAC address with a virtual MAC address with both the primary and secondary MAC addresses, setting the secondary MAC address does ensure that to-the-box management traffic is not interrupted in the case of new secondary unit hardware.

If you do not configure virtual MAC addresses, you might need to clear the ARP tables on connected routers to restore traffic flow. The FTD does not send gratuitous ARPs for static NAT addresses when the MAC address changes, so connected routers do not learn of the MAC address change for these addresses.

The IP address and MAC address for the state link do not change at failover; the only exception is if the state link is configured on a regular data interface.

14. Select the "+" icon next to the Interface MAC Address

Interface MAC Addresses		
Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

15. Physical Interface: GigabitEthernet0/1 Active Interface MAC Address: student choice (IP Address of interface used in example) Standby Interface Mac Address: Student Choice of input [example below] Click Ok

NOTE*: The above step is an example of how to configure an Interface Mac Address

Add Interface Mac Address ?

Physical Interface:*	GigabitEthernet0/1
Active Interface Mac Address:*	0000.1981.9101
Standby Interface Mac Address:*	0000.1981.9102
<small> ⓘ Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab</small>	
<input type="button" value="Cancel"/> <input style="border: 2px solid red;" type="button" value="OK"/>	

16. Configure Monitored Interfaces Go to the pencil icon next to Monitored Interfaces

Monitored Interfaces	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
in10	198.19.40.1					<input checked="" type="checkbox"/>
in20	198.19.20.1					<input checked="" type="checkbox"/>
in10	198.19.10.1					<input checked="" type="checkbox"/>
Outside_Interface	198.18.133.81					<input checked="" type="checkbox"/>

17. Select In10 and enter the Standby IP Address: 198.19.10.31 Repeat for the outside Interface 198.18.133.132

Edit in10

Monitor this interface for failures

IPv4 IPv6

Interface Name:
in10

Active IP Address:
198.19.10.1

Mask:
24

Standby IP Address:
198.19.10.31

Edit Outside_Interface

Monitor this interface for failures

IPv4 IPv6

Interface Name:
Outside_Interface

Active IP Address:
198.18.133.81

Mask:
18

Standby IP Address:
198.18.133.132

18. Click **OK Save** and then **Deploy** Select HA_Test and then Deploy

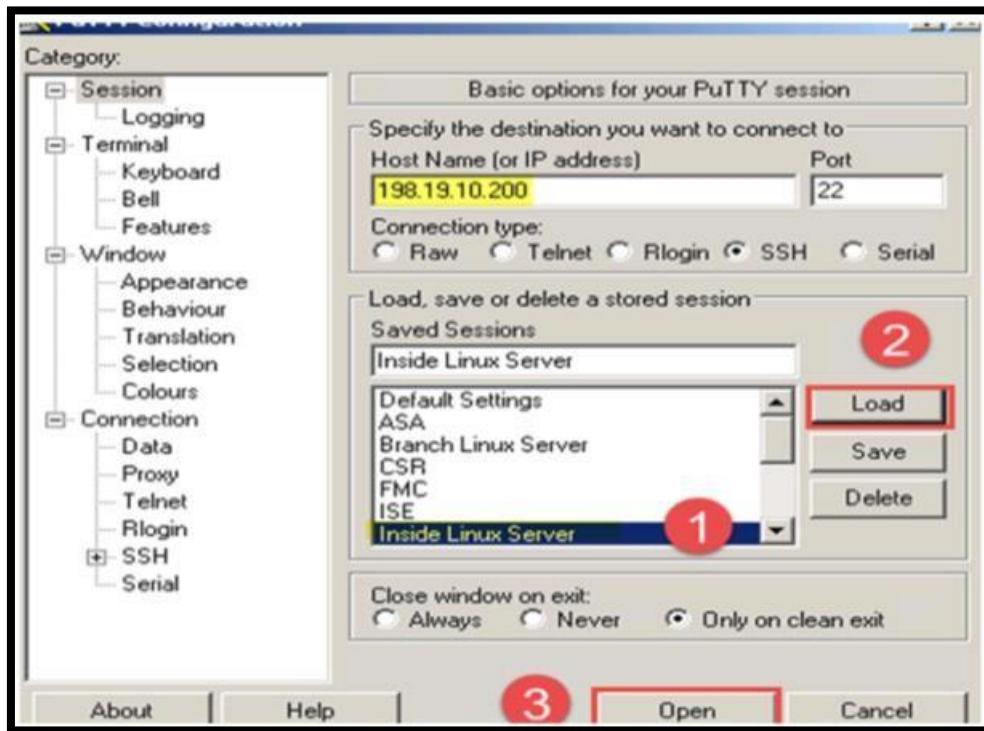
The screenshot shows the Firepower Management Center web interface. At the top, there's a navigation bar with links like Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. On the right side, there are buttons for Deploy, admin, and other settings. Below the navigation, there's a search bar and a table listing devices. One device, 'HA_Test', is selected and highlighted with a red border. The table columns include Inspect Interruption, Type, Group, Last Deploy Time, Preview, and Status. The status for 'HA_Test' is listed as 'Pending'.

Looking at the configuration of NGFW3.

1. Let's look at some of the configuration parameters that NGFW3 received during the HA setup
2. Go to the Jump PC open PUTTY and select NGFW3
3. Login into the NGFW Username: admin Password: C1sco12345 Type:
 - a show running-config interface
 - i What is the primary IP Address of each Interface?
 - ii Is there a Standby IP Address associated with the Interface?
 - b show running-config failover
 - i What is the Failover Mac Address for Interface GigabitEthernet0/1?
 - ii What is the Interface for the Failover_Link?
 - iii What is the Interface IP Address for the Failover_Link?

Testing Failover

1. On the Jump PC go to PUTTY and open up a session to the Inside Linux Server



2. Login: **root** Password: **C1sco12345** Type: "ping outside" and let the script continue to run

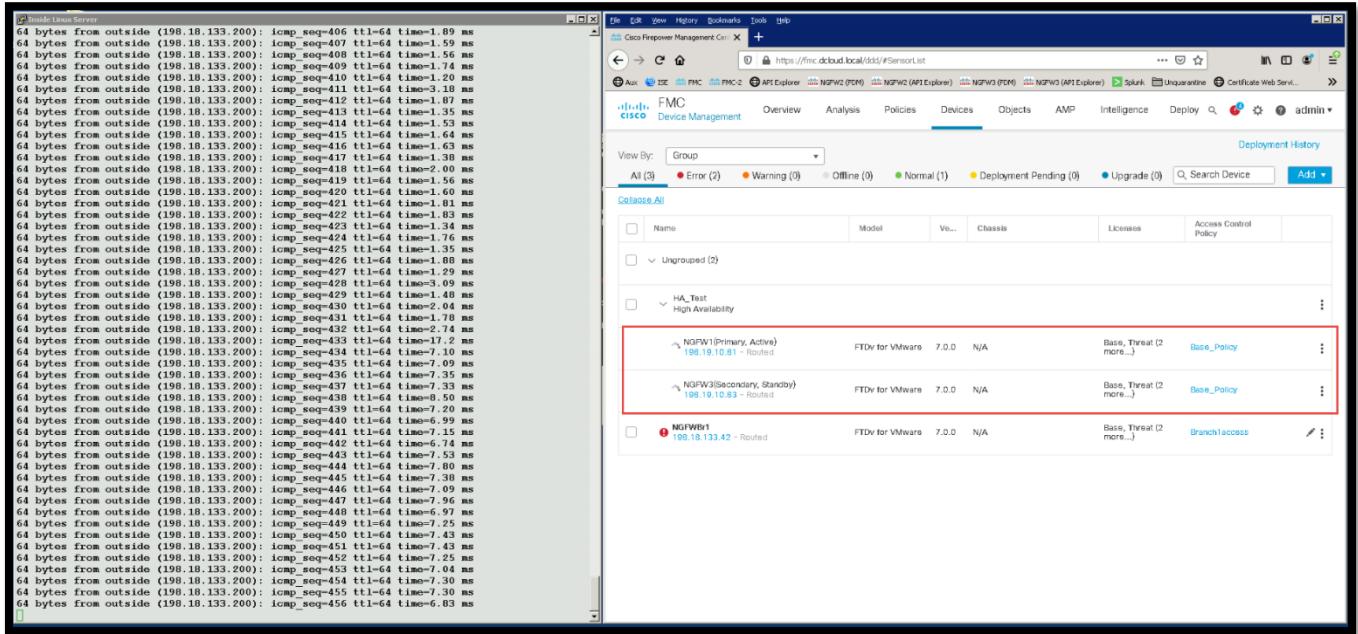
- a If the ping is unsuccessful go to the access policy "Base_Policy" and make sure the Outbound Web Server Access rule includes ICMP

```
[root@inside ~]# ping outside
PING outside (198.18.133.200) 56(84) bytes of data.
64 bytes from outside (198.18.133.200): icmp_seq=1 ttl=64 time=2.13 ms
64 bytes from outside (198.18.133.200): icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from outside (198.18.133.200): icmp_seq=3 ttl=64 time=2.17 ms
64 bytes from outside (198.18.133.200): icmp_seq=4 ttl=64 time=1.43 ms
64 bytes from outside (198.18.133.200): icmp_seq=5 ttl=64 time=1.22 ms
64 bytes from outside (198.18.133.200): icmp_seq=6 ttl=64 time=5.87 ms
64 bytes from outside (198.18.133.200): icmp_seq=7 ttl=64 time=5.15 ms
64 bytes from outside (198.18.133.200): icmp_seq=8 ttl=64 time=4.92 ms
64 bytes from outside (198.18.133.200): icmp_seq=9 ttl=64 time=5.48 ms
```

3. Go to the web interface of the FMC Devices > Device Management Click on the Switch Peers icon and click Yes



4. Resize the Firefox window so you can also see the results of the pinging from the Inside Linux Server.



Check to see if any packets are lost

5. Switch back to NGFW1 as Primary

Note: Switch back so that NGFW1 becomes Primary Again.

For the next scenarios 4, 5, 6, you will be configuring Remote Access VPN [RAVPN] with RADIUS , Multiple Factor Authentication and Enhancement using the FDM [Firepower Device Manager]. You can do all or any of the three different scenarios. Also note that the High Availability [HA] is an optional lab. The screenshots reflect a non HA environment. If you have completed the HA scenario substitute HA_Test for NGFW1.

FMC High Availability

Roles vs Status

When setting up FMC in a HA pair you configure a primary and a secondary. The primary's policies are synchronized to the secondary. After synchronization the primary FMC become active and the secondary becomes standby.

Confirm Software Prerequisites for FMC HA

The two FMC in HA must have the same major minor and maintenance software version.

They must have the same version of the intrusion rule and vulnerability database. It is also recommended that the geolocation database is the same version.

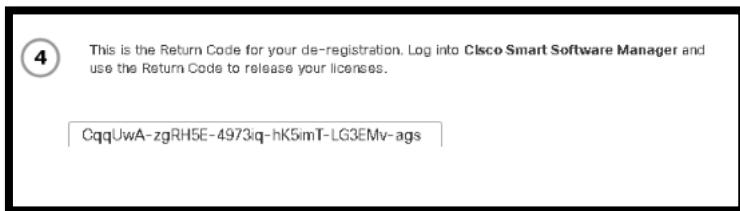
1. On the Jumphost open two browser tabs. One to the FMC and the other to FMC2 found on the bookmark ribbon
2. Click on the **?** and **About** and verify the settings for both FMC's

3. Confirm that the following three versions agree between FMC and FMC2
 - a. Same major, minor, and maintenance software version
 - b. Intrusion rule update version
 - c. Geolocation update version
 - d. Vulnerability database version
4. Both the FMC and FMC2 have permanent license reservation (PLR) You cannot form an HA pair between two FMC's with PLR enabled. HA pair can only consume one PLR license
5. FMC2 click on the gear icon in the upper right corner and select Universal Licenses

6. Click on the red circle and then yes

The screenshot shows the FMC interface with the 'Licenses' tab selected. In the 'Permanent License Reservation Status' section, there is a modal dialog box titled 'Smart License Product De-Registration'. The dialog contains text explaining the de-registration process and two buttons: 'No' and 'Yes'. A red arrow points to the 'Yes' button.

7. Click on Generate a request code



Note: If this were an actual deployment, you would save the return code. You need this code to delete the device from your smart license account. This would retrieve the PLR entitlement, which you could then apply to another device.

8. Open PuTTY on the jump box desktop. Open the FMC-2 predefined session
- Login: admin/C1sco12345
 - Type: expert
 - Type: sudo /var/sf/bin/manage_plr.pl password C1sco12345
 - Enter 3 to disable PLR

```

FMC-2
login as: admin

Using keyboard-interactive authentication.
Password:
Last login: Thu Jul  8 20:18:18 UTC 2021 from 198.19.10.50 on pts/0

Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.10.1 (build 159)
Cisco Firepower Management Center for VMware v7.0.0 (build 94)

> [expert]
admin@fmc2:~$ sudo /var/sf/bin/manage_plr.pl
Password:

***** Configuration Utility *****

1 Show PLR Status
2 Enable PLR
3 Disable PLR
0 Exit

***** Enter choice: 3 *****

```

FMC-2

```
*****
 Configuration Utility *****
1 Show PLR Status
2 Enable PLR
3 Disable PLR
0 Exit

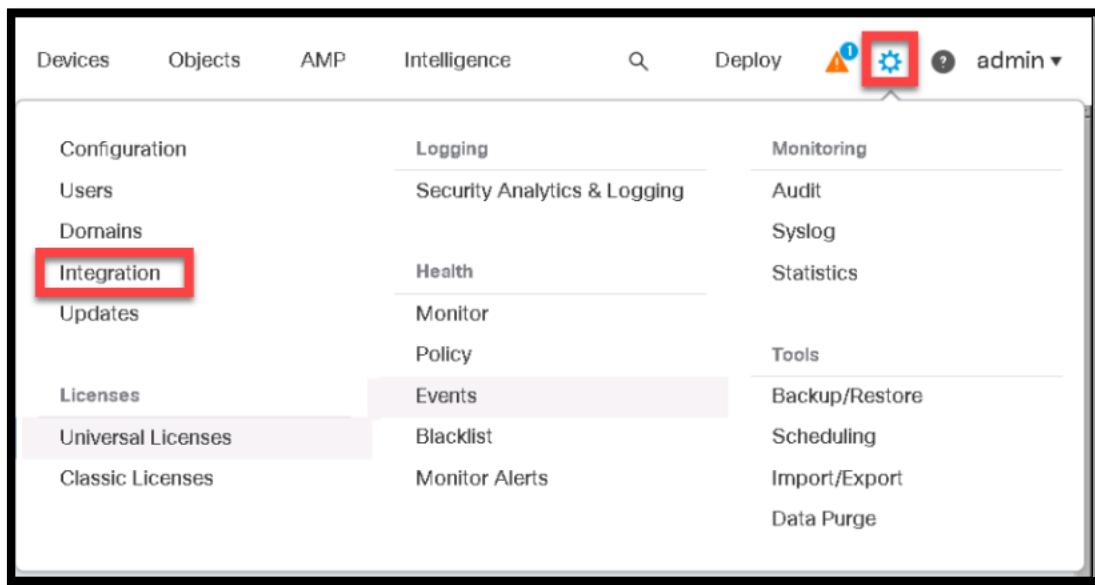
*****
Enter choice: 1
PLR is not enabled on FMC

*****
 Configuration Utility *****
1 Show PLR Status
2 Enable PLR
3 Disable PLR
0 Exit

*****
Enter choice: 0
```

iii. Enter 0

9. On FMC-2 click on the gear icon and then select Integration



10. Select the High Availability sub-tab

11. Select Secondary

- For Primary: fmc.dcloud.local
- Register Key: C1sco12345
- Register
- Select Yes and Yes

Cloud Services Realms Realm Sequences Identity Sources **High Availability** eStreamer Host Input Client Smart Software Satellite

Select a role for this Management Center and specify peer details to setup high availability.

Role For This FMC:

Standalone (No High Availability)

Primary

Secondary

Peer Details:

After Firepower Management Center high availability is configured on VMWare, each registered FTD consumes an additional Firepower MCv Device license.

Primary FMC Host:

Registration Key*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

Note: You will see that HA FMC page now says Pending Registration

Configure FMC as the Primary FMC

1. FMC click on the gear icon in the upper right corner and select Integration

Configuration	Logging	Monitoring
Users	Security Analytics & Logging	Audit
Domains		Syslog
Integration	Health	Statistics
Updates	Monitor	
Licenses	Policy	Tools
Universal Licenses	Events	Backup/Restore
Classic Licenses	Blacklist	Scheduling
	Monitor Alerts	Import/Export
		Data Purge

2. Select High Availability
 - a. Select Primary
 - b. Secondary FMC Host: fmc2.dcloud.local
 - c. Registration Key: C1sco12345
 - d. Register

Cloud Services Realms Realm Sequences Identity Sources **High Availability** eStreamer Host Input Client Smart Software Sate

Select a role for this Management Center and specify peer details to setup high availability.

Role For This FMC:

Standalone (No High Availability)

Primary

Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.
After Firepower Management Center high availability is configured on VMWare, each registered FTD consumes an additional Firepower MCv Device license.

Secondary FMC Host:

Registration Key*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

3. Check the status

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin▼

System / Integration / **High Availability** Peer Manager

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem

High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete.

Summary		System Status	
Status	⚠ Temporarily degraded - high availability operations are in progress.	Local	Remote
Synchronization	⚠ Failed	Standby - Primary (198.19.10.120)	Active - Secondary (fmc2.dcloud.local)
Active System	fmc2.dcloud.local	Operating System	7.0.0
Standby System	198.19.10.120	Software Version	7.0.0-94
		Model	Cisco Firepower Management Center for VMware

RemoteOnly And LocalOnly Device Registration

IP Address	Host Name	Last Changed	Status
> Registration Pending/Failed (Remote) (2)			

The screenshot shows the Cisco dCloud interface with the 'Tasks' tab selected. At the top, there are tabs for 'Deployments', 'Upgrades', 'Health' (with a warning icon), and 'Tasks'. Below these are status counts: 20+ total, 1 waiting, 0 running, 0 retrying, 20+ success, 0 failures. A 'Show Notifications' toggle is on, and a 'Filter' search bar is present. The main area lists tasks:

- High Availability**: Config DB Files Synchronization Transaction - Active. Status: Extracting database files. Duration: 2m 33s.
- Reset High Availability**: REGISTRATION fmc2.dcloud.local. HA post registration completed for peer fmc2.dcloud.local. Duration: 22s. This task is highlighted with a red box.
- Health Policy**: Apply Initial_Health_Policy 2020-11-20 21:02:54 to NGFW1. Status: Health Policy applied successfully. Duration: 1m 27s.
- Health Policy Apply**: Health policy apply to appliance fmc.dcloud.local. Status: Health Policy applied successfully. Duration: 1m 2s.

A 'Remove completed tasks' button is at the bottom.

Confirm the FMC HA Configuration

1. Click on the **Gear Icon > Integration**
2. Click on **High Availability**

The screenshot shows the Peer Manager interface with the 'High Availability' tab selected. Other tabs include 'Cloud Services', 'Realms', 'Identity Sources', 'eStreamer', 'Host Input Client', and 'Smart Software Manager On-Prem'. A 'Peer Manager' header is at the top right. Below the tabs are two sections: 'Summary' and 'System Status'.

Summary (highlighted with a red box):

Status	Synchronization task is in progress
Synchronization	OK
Active System	198.19.10.120 (HA synchronization time : Mon Oct 11 20:31:28 2021)
Standby System	fmc2.dcloud.local (HA synchronization time : Mon Oct 11 20:31:22 2021)

System Status:

Local	Active - Primary (198.19.10.120)	Remote	Standby - Secondary (fmc2.dcloud.local)
Operating System	7.0.0	Software Version	7.0.0-94
Model	Cisco Firepower Management Center for VMware	Model	Cisco Firepower Management Center for VMware

3. Open the PuTTY session for **NGFW1 admin/C1sco12345**
4. Type show managers

```
> show managers
Type                  : Manager
Host                 : fmc2.dcloud.local
Registration         : Completed

Type                  : Manager
Host                 : fmc.dcloud.local
Registration         : Completed

>
```

5. On FMC-2 Look at available services like Devices and AMP
6. Look at **System > Integrations**

7. On FMC High Availability Click **Switch Peer Roles** yes and OK

Summary		System Status	
Status	Healthy	Local	Active - Primary (198.19.10.120)
Synchronization	OK	Operating System	7.0.0
Active System	198.19.10.120 (HA synchronization time : Mon Oct 11 20:37:39 2021)	Software Version	7.0.0-94
Standby System	fmc2.dcloud.local (HA synchronization time : Mon Oct 11 20:37:42 2021)	Model	Cisco Firepower Management Center for VMware
			Cisco Firepower Management Center for VMware

8. Check FMC-2 to see Policies, Devices, Click on Integration and High Availability

a. Note the System Status

- i. You will see that 198.19.10.121 is Active-Secondary

Summary		System Status	
Status	Synchronization task is in progress	Local	Active - Secondary (198.19.10.121)
Synchronization	OK	Operating System	7.0.0
Active System	198.19.10.121 (HA synchronization time : Mon Oct 11 21:13:05 2021)	Software Version	7.0.0-94
Standby System	fmc2.dcloud.local (HA synchronization time : Mon Oct 11 21:12:08 2021)	Model	Cisco Firepower Management Center for VMware
			Cisco Firepower Management Center for VMware

9. On FMC-2 click **Switch Peers Roles**, YES and OK

10. Confirm settings of 198.19.10.120 as the Primary. (Needed for other Lab exercises).

11. Break HA from FMC Select Yes

a. **Select Manage registered devices from this console**

How do you want to manage devices after breaking high availability?

Manage registered devices from this console.

Manage registered devices from peer console.

Stop managing registered devices from both consoles.

All devices will be unregistered from peer console.

Cancel **OK**

b. Click **OK**

12. After the HA pair is broken Click on FMC-2 **Analysis > Connection > Events**

- a. You can see that the **Events were saved**
b. Verify that FMC-2 is not managing any devices

13. Go to FMC and verify devices are being managed

NOTE: If you are going to keep the FTD HA you can remove InZone3 from the Base_Policy rules in order to remove the warnings. You can also delete the Manual NAT rule for InZone3. If you want to delete the FTD_HA rename GigabitEthernet3/0 and add InZone3 as the Security Zone.

Scenario 4. AnyConnect with RADIUS

This exercise consists of the following tasks.

- Create a group policy
- Create an IP pool
- Modify the Access control and NAT policies
- Deploy and test the configuration

In this exercise, we will use ISE RADIUS to validate a VPN user.

The objectives of this exercise are the following:

- To configure an AnyConnect VPN client to connect to the NGFW
- To test the Intrusion prevention and Malware configuration of the NGFW

NOTE: In order to save time, ISE is pre-configured with all required configuration for all the lab exercises. This includes the selection of group policy and IP pool based on AD group membership. **Because of this, the name of the new group policy and IP pool must be exactly the names given in the instructions.** If you want to review the ISE configuration, see Appendix 3.

Steps

1. Go to System > Licenses > Universal Licenses

- a. Click on Edit Licenses
- b. Select AnyConnect Apex
 - i. IF not assigned: Select HA_Test or NGFW1 [if HA Lab was not done]
 - 1 Click Add and then Apply

Create objects needed for this scenario

NOTE: Most of these objects can be created while running the RA VPN wizard. This approach may be better for administrators that are not familiar with the components of the RA VPN configuration. However, in this scenario you will create the objects separately. This will simplify running the RA VPN wizard later.

1. In the FMC, navigate to Objects > Object Management.
2. Click Add Network > Add Object.
 - a. Create an IP range object called
 - i. VPNPoolIPs IP address range 198.19.10.57-198.19.10.62.
 - ii. This object will be used to create a NAT exemption.
 - iii. Click **Save**

Edit Network Object

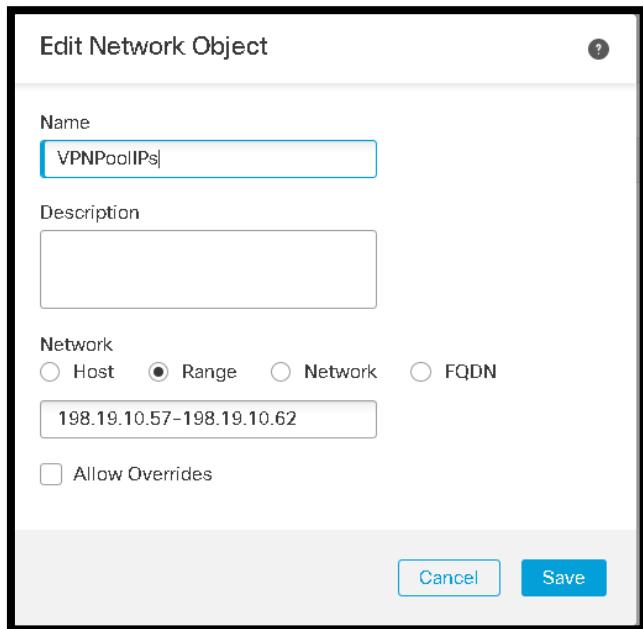
Name
VPNPoolIPs|

Description

Network
 Host Range Network FQDN
198.19.10.57-198.19.10.62

Allow Overrides

[Cancel](#) [Save](#)



3. Click Add Network > Add Object. Create a Network object called LAN_Network with IP addresses 198.19.10.0/24

Edit Network Object

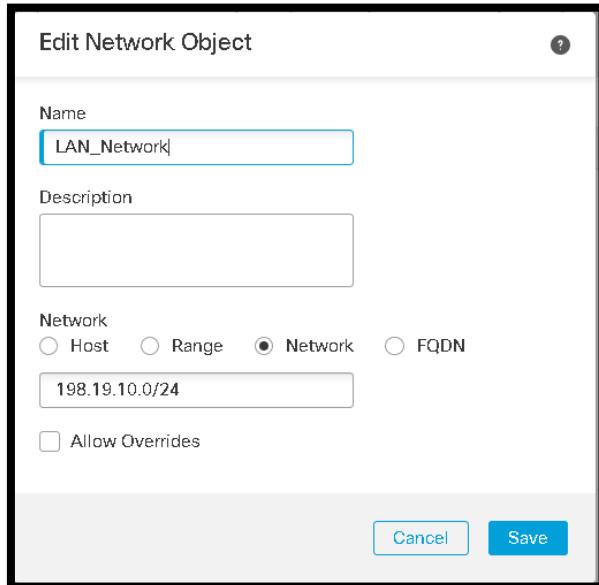
Name
LAN_Network|

Description

Network
 Host Range Network FQDN
198.19.10.0/24

Allow Overrides

[Cancel](#) [Save](#)



4. Click Add Network > Add Object. Create a host object called ISE_Server with IP address 198.19.10.130.

Edit Network Object

Name
ISE_Server

Description

Network
 Host Range Network FQDN
 198.19.10.130

Allow Overrides

Cancel **Save**

- Click Add Network > Add Object. Create a host object called DNS_Server with IP address 198.19.10.100.

Edit Network Object

Name
DNS_Server

Description

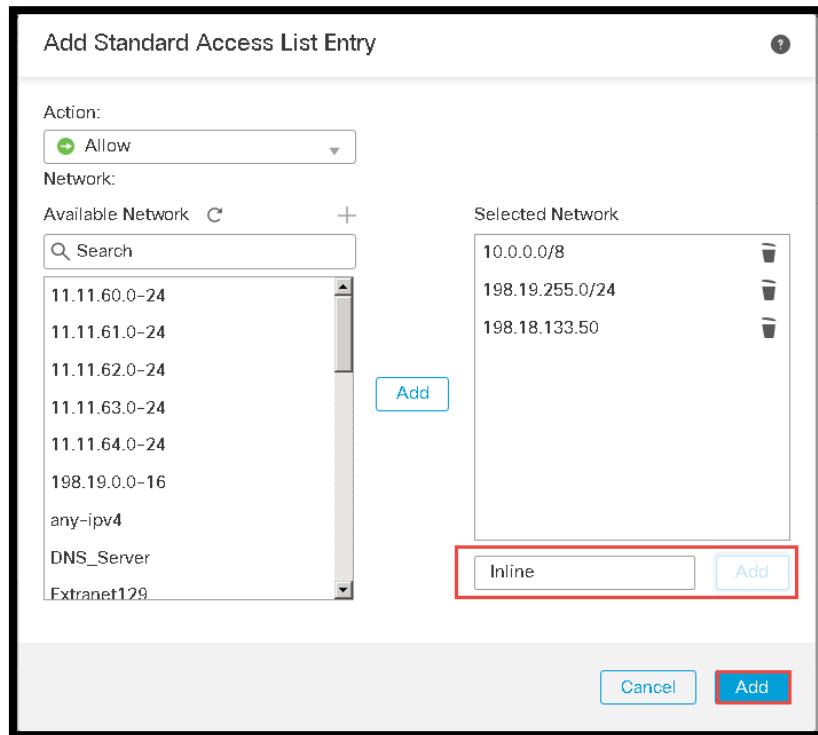
Network
 Host Range Network FQDN
 198.19.10.100

Allow Overrides

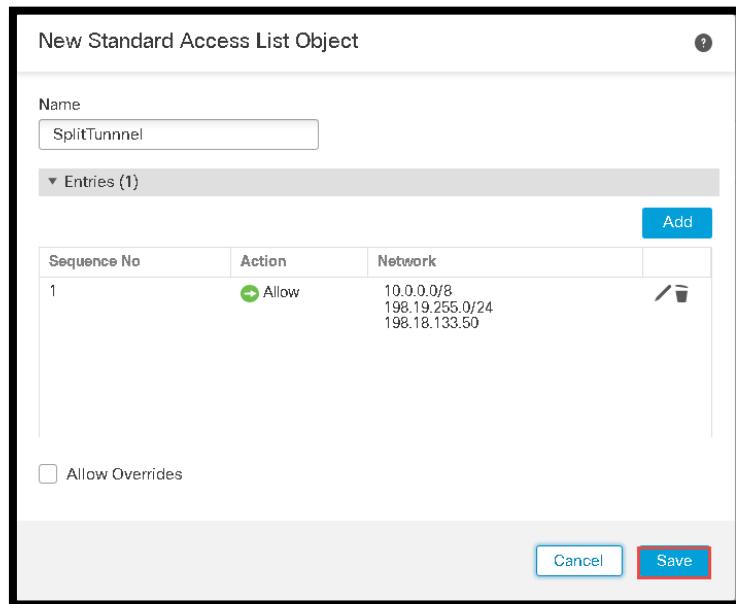
Cancel **Save**

NOTE: For best security, it is recommended that split-tunneling not be used. However, because there is no console access for the endpoint on which you will run AnyConnect, split tunneling must be used in this Scenario. Since there are different ways to access the endpoint in dCloud, you need to create a standard ACL to bypass all these potential access addresses. You will do this now.

- Select Access List > Standard from the left navigation pane. Click Add Standard Access List.
- Create a standard access list called SplitTunnel with the ACE that allows 10.0.0.0/8, 198.19.255.0/24 and 198.18.133.50. To do this, type these networks into the text box under the Selected Network box, and click Add.



- Click Save to save the access list.



- Select Access List > Extended from the left navigation pane. Click Add Extended Access List.
- Create an extended access list called **redirect** that looks like the following. This will be used to determine what traffic is to be redirected to ISE when posture assessment is taking place. The ACEs where the action is block will be exempted from redirection.

New Extended Access List Object

Name
redirect

Entries (3)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	ISE_Server	TCP (6):8443
2	Block	Any	Any	DNS_Server	DNS_over_UDP
3	Allow	Any	Any	Any	Any

Allow Overrides

Cancel Save

11. Select Address Pools > IPv4 Pools from the left navigation pane. Click Add IPv4 Pools.
 - a. For Name, enter VPNPool.
 - i. For IPv4 Address Range, enter 198.19.10.57-198.19.10.62.
 - ii. For Mask, enter 255.255.255.248.
 - iii. Click Save

Edit IPv4 Pool

Name*	VPNPool
IPv4 Address Range*	198.19.10.57-198.19.10.62
Format:	ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150
Mask	255.255.255.248
Description	
<input checked="" type="checkbox"/> Allow Overrides	
<small>Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices</small>	
Override (0)	
Cancel	Save

NOTE: Although the objects VPNPoolIPs and VPNPool represent the same IP address range, they are different object types. VPNPool will be referenced in the RA VPN object, whereas VPNPoolIPs will be used for configuring a NAT exemption.

12. Select VPN > AnyConnect Files from the left navigation pane.
13. Click Add AnyConnect File. Click Browse and select AnyConnectProfile.xml from the RA VPN folder on the Jumpbox desktop. For File Type select: AnyConnect VPN Profile.

Add AnyConnect File

Name:*

File Name:*

File Type:*

Description:

14. Click Add AnyConnect File. Click Browse and select anyconnect-win-4.7.XXXXX-webdeploy-k9.pkg from the RA VPN folder on the Jumpbox desktop. For File Type: Select AnyConnect Client Image.

Edit AnyConnect File

Name:*

File Name:*

File Type:*

Description:

15. Select PKI > Cert Enrollment from the left navigation pane. Click Add Cert Enrollment.
- For Name, enter **NGFW1_Outside**. [If you have done the High Availability Lab you can name HA if you wish]
 - Select PKCS12 File from the Enrollment Type drop-down menu.
 - Click Browse and select Certificates > Lab Certificates > Other Certificates > **ngfw-outside** on the Jumpbox desktop.

- d. For Passphrase, enter **C1sco12345**.

Add Cert Enrollment

Name*
NGFW1_Outside

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:
PKCS12 File

PKCS12 File*: ngfw-dcloud.pfx Browse PKCS12 File

Passphrase: *****

Allow Overrides

Cancel Save

Create and configure a RADIUS server group for ISE

1. Select AAA > RADIUS Server Group from the left navigation pane. Click Add RADIUS Server Group.
 - a. Call the group ISE_RADIUS.
 - b. Check the Enable dynamic authorization checkbox.
 - c. Click the plus to add a RADIUS server.
2. Enter the following information, leaving other attributes as default.
 - a. For IP Address/Hostname, enter 198.19.10.130.
 - b. For Key, and Confirm key enter C1sco12345.
 - c. Select the Specific interface radio button and select InZone1 from the drop-down menu.
 - d. For Redirect ACL, select **redirect**.

Edit RADIUS Server Group

Name:*****
ISE_RADIUS

Description:

Group Accounting Mode:
Single

Retry Interval:***** (1-10) Seconds
10

Realms:

Enable authorize only

Enable interim account update

Interval:***** (1-120) hours
24

Enable dynamic authorization

Port:***** (1024-65535)
1700

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname	+
198.19.10.130	/

Save

New RADIUS Server

IP Address/Hostname:*****
198.19.10.130

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:***** (1-65535)
1812

Key:*****

Confirm Key:*****

Accounting Port: (1-65535)
1813

Timeout: (1-300) Seconds
10

Connect using:

Routing Specific Interface **1**

InZone1 +

Redirect ACL:
redirect +

Save

3. Click Save to add the RADIUS server to the RADIUS server group. Click Save.

Configure DNS Server for NGFW1

1. Navigate to Objects > Object Management > DNS Server Group. Click on Add DNS Server Group.
 - a. Enter Name as DCloud-DNS
 - b. Default Domain will be dcloud.local
 - c. Enter 198.19.10.100 as the DNS Server.
 - d. Click on Save.

The screenshot shows the 'New DNS Server Group Object' configuration dialog. It includes fields for Name (DCloud-DNS), Default Domain (dcloud.local), Timeout (2), Retries (2), and a single DNS Server entry (198.19.10.100). A note at the bottom indicates that multiple values can be specified as comma-separated entries. At the bottom right are 'Cancel' and 'Save' buttons, with 'Save' being highlighted.

New DNS Server Group Object

Name*: DCloud-DNS

Default Domain: dcloud.local

Timeout: 2

Range: 1 - 30 Seconds

Retries: 2

Range: 0 - 10

DNS Servers: 198.19.10.100

(Multiple values in IPv4 or IPv6 addresses can be specified as comma separated entries)

Cancel Save

2. Navigate to Devices > Platform Settings. Click on **New Policy** Threat Defense Settings Policy.
 - a. Name will be NGFW1_Platform_Settings.
 - b. Add NGFW1 or [HA_Test] as the Selected Device.
 - c. Click on Save.

New Policy

Name: NGFW1_Platform_Settings

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices	Selected Devices
<input type="text" value="Search by name or value"/> <ul style="list-style-type: none"> HA_Test NGFWBR1 	<input type="text" value="HA_Test"/>

Add to Policy

Cancel Save

How To

3. Navigate to DNS.
 - a. Check Enable DNS name resolution by device.
 - b. Select DCloud-DNS from the DNS Server Group dropdown.
 - c. Add InZone1 as the Interface Object.
 - d. Click on Save

DNS Resolution Settings

Specify DNS servers group and device interfaces to reach them.

Enable DNS name resolution by device

DNS Server Group*: DCLOUD-DNS +

Expiry Entry Timer: 1 Range: 1-65535 minutes

Poll Timer: 240 Range: 1-65535 minutes

Interface Objects

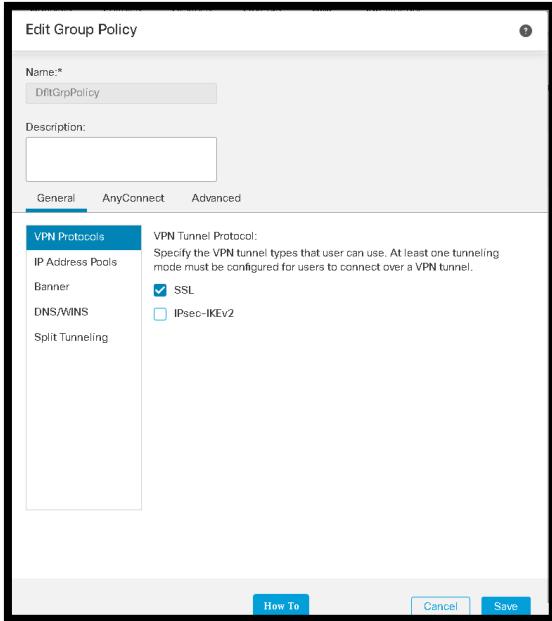
Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects	Selected Interface Objects
<input type="text" value="Search"/> <ul style="list-style-type: none"> branch1_InZone branch1_Outzone in_dummy_SZ InZone InZone1 InZone2 InZone3 InZone4 	<input type="text" value="InZone1"/>

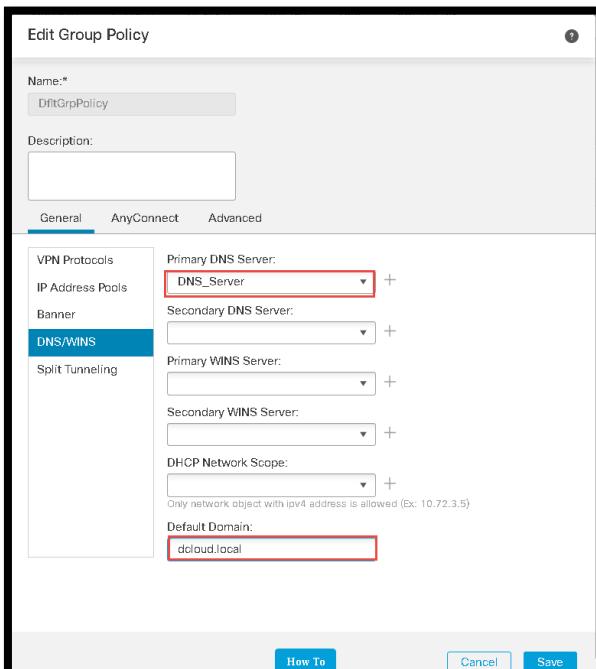
Edit the default group policy (DfltGrpPolicy)

NOTE: Typically, the VPN Group policy is edited (or a new group policy is added) while running the RA VPN wizard. This task has been separated out for clarity, and to simplify running the RA VPN wizard later.

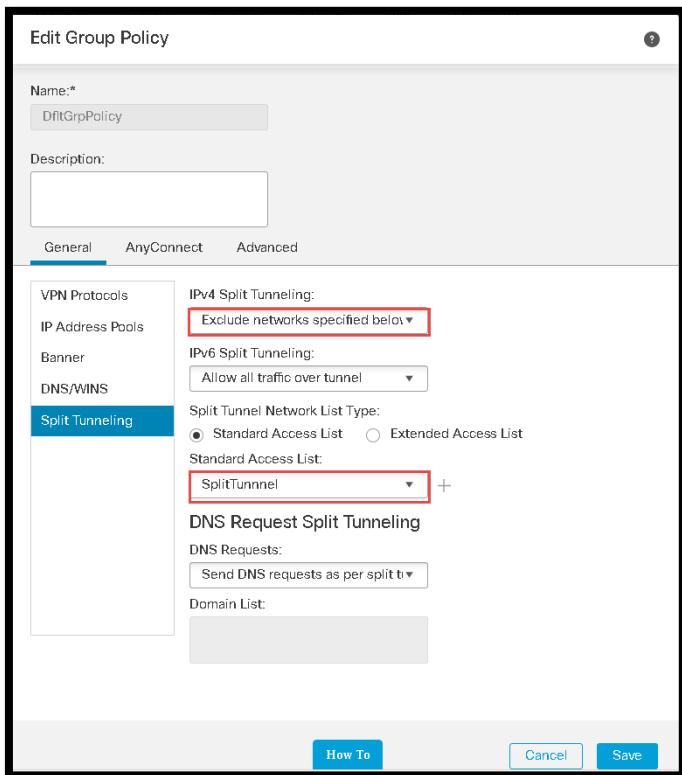
1. Navigate to Objects > Object Management > VPN > Group Policy from the left navigation pane. Click the pencil icon to edit DfltGrpPolicy
2. Under General > VPN Protocols, uncheck IPsec-IKEv2.



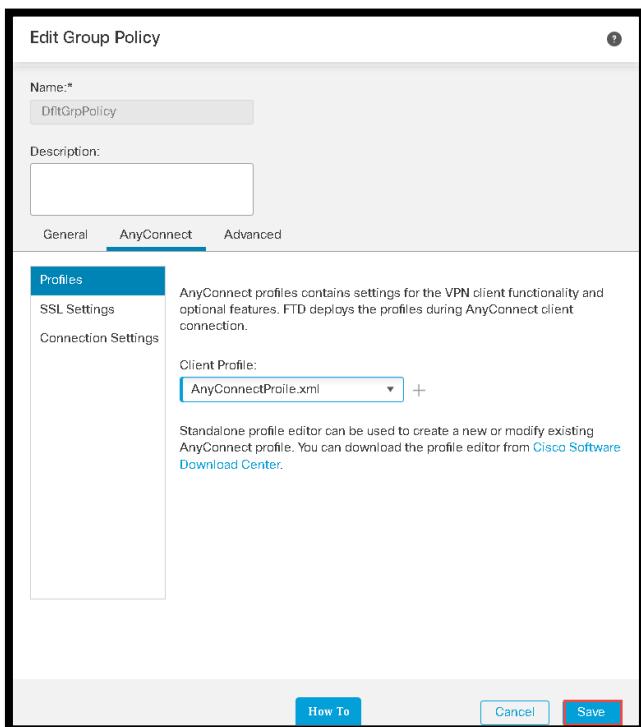
3. Under General > DNS/Wins.
 - a. Select DNS_Server from the Primary DNS Server drop-down list.
 - b. For Default Domain, check for: dccloud.local.



4. Under General > Split Tunnel.
- Select Exclude networks specified below from the IPv4 Split Tunneling drop-down list.
 - Select SplitTunnel from the Standard Access List drop-down list.



5. Under AnyConnect > Profiles. Select AnyConnectProfile.xml from the Client Profile drop-down list.



- Click Save to save the changes you made to DfltGrpPolicy.

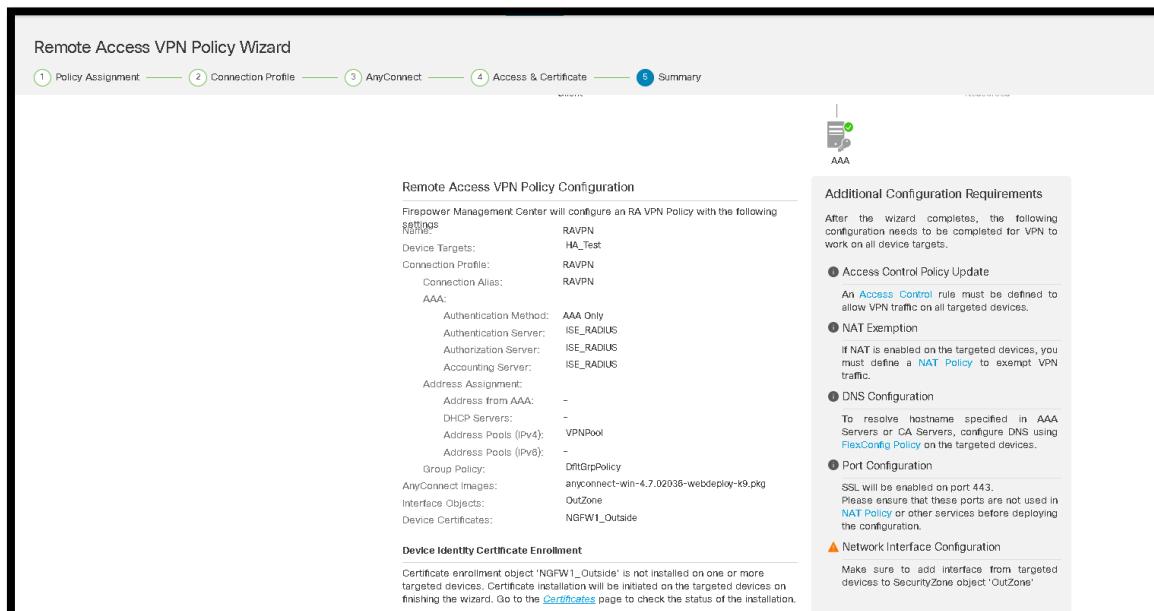
NOTE: Typically, you would also be enabling AnyConnect licensing at this point, however this has already been done. You can observe this at System > Licenses > Smart License. You will see that the FMC is using an evaluation license, but that export-controlled features are enabled. This is generally not possible, and therefore you cannot license SSL VPN with an evaluation license

Run the RA VPN wizard

- In FMC, navigate to Devices > VPN > Remote Access. Click Add. This will launch the wizard.
 - Complete the Policy Assignment page of the wizard.
 - For Name, enter RAVPN
 - From Target Devices, select HA_Test or NGFW1. Click Add.
 - Uncheck IPsec-IKEv2
 - Click Next
- Complete the Connection Profile page of the wizard.
 - For Connection Profile Name, enter RAVPN
 - Confirm that for Authentication Method, AAA Only is selected.
 - For Authentication and Authorization Server, select ISE_RADIUS
 - For Use IP Address Pools IPv4 Address Pools:
 - Select VPNPoolIPs
 - Click OK
 - Click Next
- Confirm that Group Policy is step to DfltGrpPolicy. Click Next.

Remote Access VPN Policy Wizard

- Complete the AnyConnect page of the wizard.
 - Check the file object checkboxes.
 - Click Next
- Complete the Access & Certificate page of the wizard.
 - For Interface group/Security Zone, select OutZone.
 - For Certificate Enrollment, select NGFW1_Outside.
 - Click Next
 - Review Configuration summary and click Finish



Modify the Access control and NAT policies

1. In FMC, navigate to Policies > Access Control > Access Control.
2. Select and edit the access control policy (Base_Policy). Click Add Rule.
 - a. For Name, enter AnyConnect-S4-Permit.
 - b. Select into Mandatory from the Insert drop-down list
 - c. The Zones tab should already be selected.
 - d. Select OutZone and click Add to Source.
 - e. Select InZone1, and click Add to Destination
3. Select the Networks tab.
 - a. Select VPNPoolIPs and click Add to Source.
 - b. Select LAN_Network and click Add to Destination.
4. Select the Inspection tab.
 - a. Select Demo Intrusion Policy or HQ-High-Security-Policy from the Intrusion Policy drop-down list.
 - b. Select Demo File Policy or HQ File Policy from the File Policy drop-down list.
5. Select the Logging Tab and select **Log at End of Connection**
6. Click **Add** to add the rule
7. Disable or Delete the Mandatory Rule 1 Block ICMP #1
8. Disable or Delete the Default Base_Policy Allow GRE #5
9. Click **Save** to save the changes to the access control policy changes.

Configure a NAT exemption

1. In the FMC, navigate to Devices > NAT.
2. Select and edit the existing NAT policy (Default PAT). Click Add Rule.
 - a. You will be at the Interface Objects tab.
 - b. Select InZone1 and click Add to Source.
 - c. Select OutZone, and click Add to Destination.
3. Select the Translation tab.
4. For Original Source, select LAN_Network
5. For Original Destination, select VPNPoolIPs.
6. For Translated Source, select LAN_Network
7. For Translated Destination, select VPNPoolIPs.
8. Select the Advanced tab and select Do not proxy ARP on Destination Interface.

NOTE: Enabling Do not proxy ARP on Destination Interface is critical in this lab exercise. If you miss this step, your pod may have access issues, since all devices are managed in band.

9. Click OK to save the NAT rule
10. Click **Save** to save the changes to the NAT policy.

Deploy and verify the NGFW VPN configuration

1. Deploy policy to device.
2. In FMC, click the Deploy button.
3. Select HA_Test or NGFW1 and Click Deploy.[Ignore the warning about NGFW3 if you are not in HA]
4. Wait for the deployment to complete.
5. Open a PUTTY session to the NGFW1 CLI. Run some or all of the following commands.
 - a. show running-config tunnel-group

```

NGFW1
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Sat May 22 18:45:58 UTC 2021 from jump.dcloud.local on pts/0

Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.6.4 (build 3)
Cisco Firepower Threat Defense for VMWare v6.6.4 (build 59)

> show running-config tunnel-group
tunnel-group RAVPN type remote-access
tunnel-group RAVPN general-attributes
  address-pool VPNPool
  authentication-server-group ISE_RADIUS
tunnel-group RAVPN webvpn-attributes
  group-alias RAVPN enable
>

```

b. show running-config group-policy

```

> show running-config group-policy
group-policy DfltGrpPolicy attributes
  dns-server value 198.19.10.100
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy excludespecified
  split-tunnel-network-list value SplitTunnel
  default-domain value dcloud.local
  user-authentication-idle-timeout none
  webvpn
    anyconnect keep-installer none
    anyconnect modules value dart
    anyconnect profiles value AnyConnectProfile.xml type user
    anyconnect ask none default anyconnect
    http-comp none
    activex-relay disable
    file-entry disable
    file-browsing disable
    url-entry disable
    deny-message none
>

```

c. show running-config crypto

i. Notice the crypto trustpoint is: NGFW1_Outside or HA

d. show running-config ip local pool

```

> show running-config ip local pool
ip local pool VPNPool 198.19.10.57-198.19.10.62 mask 255.255.255.248
>

```

e. show running-config nat

```
> show running-config nat
nat (inside,outside) source static LAN_Network LAN_Network destination static VPNPoolIPs VPNPoolIPs no-proxy-arp
object network FMC_Private
nat (inside,outside) static FMC_Public
object network wwwin
nat (inside,outside) static wwwout
nat (inside,outside) after-auto source dynamic any interface
>
```

6. Test AAA by running the following command on the NGFW1 CLI

```
test aaa-server authentication ISE_RADIUS host 198.19.10.130 username pc-outside password C1sco12345
```

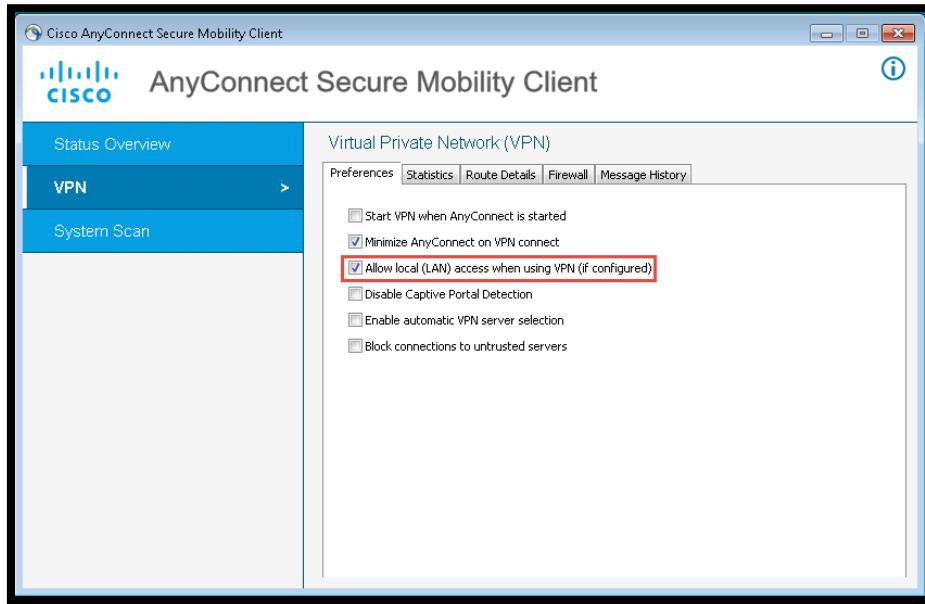
NOTE: If the test fails you will need to reset the pc-outside password. Go to the Jumpbox click on Remote Desktops and click on the ad1.Domain Controller. Click on Start Administrative Tools Active Directory Users and Computers right click on pc-outside and select Reset Password enter **C1sco12345** for the password. **Uncheck the User must change password at next logon** click OK. then retest.

NOTE: In this scenario, the definition of a compliant system is a system that has a file called compliant.txt on the desktop. In this exercise, Wkst2 will start out as non-compliant. And furthermore, the posture module is already installed on Wkst2.

1. Connect to Wkst2. You will automatically be logged in as the administrator. You can connect using one of two methods.
 - a. From the topology map, as shown in this picture. This is the recommended method.

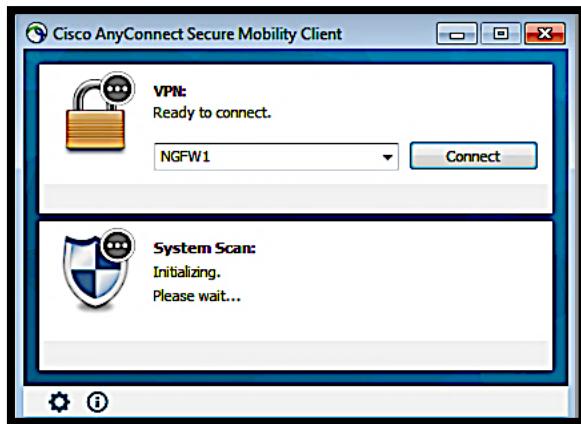


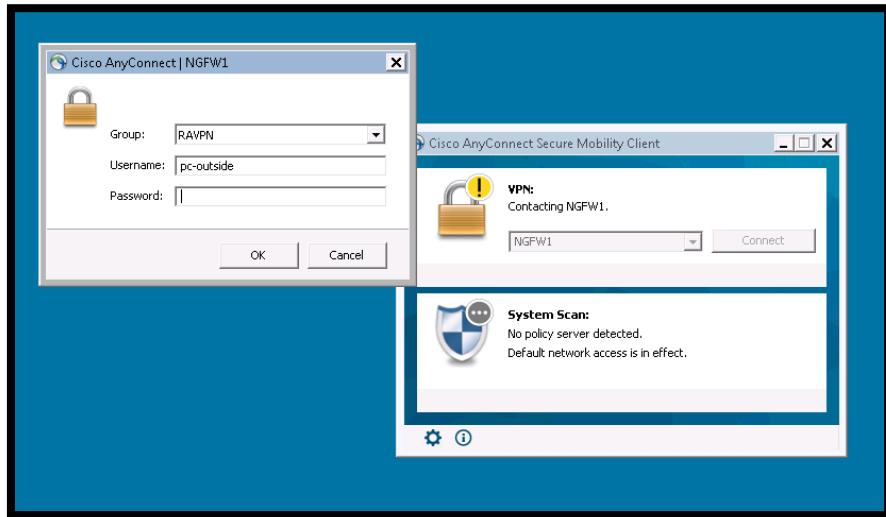
- b. By clicking the Wkst2 (Outside PC) shortcut in the Remote Desktops folder on the Jumpbox desktop. However, if you do this, you must allow local LAN access in the AnyConnect client.



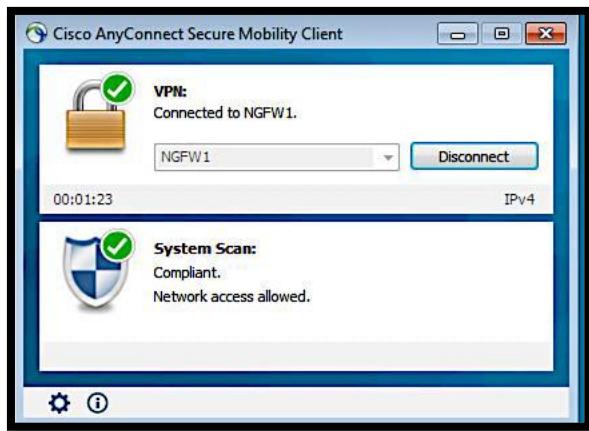
- c. If you are connected to the pod via VPN, use and RDP client on your laptop to connect to 198.18.133.23. Log in as Administrator, password C1sco12345.
2. Open AnyConnect from the Start Menu. You will see the Connect To field prepopulated with the NGFW1 FQDN. Click on Connect accept the Certificate Warnings

NOTE: If when clicking the OK the AnyConnect screen pops back up, you will need to reset the pc-outside password. Go to the Jumpbox click on Remote Desktops and click on the ad1.Domain Controller. Click on Start Administrative Tools Active Directory Users and Computers right click on pc-outside and select Reset Password enter **C1sco12345** for the password. **Uncheck the User must change password at next logon** click OK then repeat the Connection process on the Anyconnect box on WKST2.





3. For Password: **C1sco12345** and **OK**
4. On the first connect, you might see the AnyConnect Compliance module being downloaded.
5. If the system is compliant the first time we connect, you will be prompted to remediate. Click on Start.



6. Using the bookmarks in the Firefox browser on Wkst2, confirm that you can now access two internal web-sites that are bookmarked: Inside, Alt Inside, Inside Honeypot.
7. In any one of these internal servers, click on the Files link, and then click on Zombies.pdf. This is considered malware. Confirm that it is blocked. Confirm that a benign file, like ProjectX.pdf, is not blocked.

NOTE: To make sure that a cloud lookup time out (which happens occasionally in these pods) does not break the exercise, the file Zombies.pdf was added to the FMC custom detection list. If you want to perform a test that actually requires the cloud lookup, enter the URL <http://altoutside.dcloud.local/malware>, and try to download Buddy.exe.

8. Confirm that intrusions are being blocked. This can be done by opening a command prompt on Wkst2 and making an [FTP](http://198.19.10.202) 198.19.10.202. The connection should be allowed. Log in as guest, password C1sco12345. Once logged in type cd ~root. The connection should be reset. This is because Snort signature 336 has been triggered.

```

Administrator: Command Prompt - ftp inside.dcloud.local
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp inside.dcloud.local
Connected to inside.dcloud.local.
220 (vsFTPd 3.0.2)
User (inside.dcloud.local:(none)): guest
331 Please specify the password.
Password:
230 Login successful.
ftp> cd ~root
Connection closed by remote host.
ftp> -

```

9. (Optional) In the FMC, examine the malware event (Analyze > Files > Malware Events) and intrusion event (Analyze > Intrusions > Events). You can also examine RA VPN user statistics by navigating to Overview > Dashboards > Access Controlled User Statistics > VPN.

10. On NGFW1 PUTTY Session type the command: **show vpn-sessiondb detail anyconnect**

```

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1.1
Public IP : 198.18.133.23
Encryption : none
TCP Src Port : 49215
Auth Mode : userPassword
Idle Time Out: 30 Minutes
Client OS : win
Client OS Ver: 6.1.7601 Service Pack 1
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.02036
Bytes Tx : 3235874
Pkts Tx : 6
Pkts Tx Drop : 0
Bytes Rx : 605
Pkts Rx : 0
Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 1.2
Assigned IP : 198.19.10.57
Encryption : AES-GCM-256
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2
TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.02036
Bytes Tx : 8106
Pkts Tx : 6
Pkts Tx Drop : 0
Bytes Rx : 448
Pkts Rx : 6
Pkts Rx Drop : 0
Filter Name : #ACSAACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3

DTLS-Tunnel:
Tunnel ID : 1.3
Assigned IP : 198.19.10.57
Encryption : AES256
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0
UDP Dst Port : 443
Idle Time Out: 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.02036
Bytes Tx : 14895898
Pkts Tx : 10996
Pkts Tx Drop : 0
Bytes Rx : 324974
Pkts Rx : 6291
Pkts Rx Drop : 0
Filter Name : #ACSAACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3

```

Scenario 5. Site-to-Site VPN

This exercise consists of the following tasks.

- Create objects needed for this lab exercise
- Configure site-to-site VPN
- Create NAT exemption
- Modify the access control policy and deploy changes
- Deploy the changes and test the configuration

The objective of this exercise is to configure a site-to-site VPN tunnel between two FMC Controlled NGFWs

Steps

Create objects needed for this lab exercise

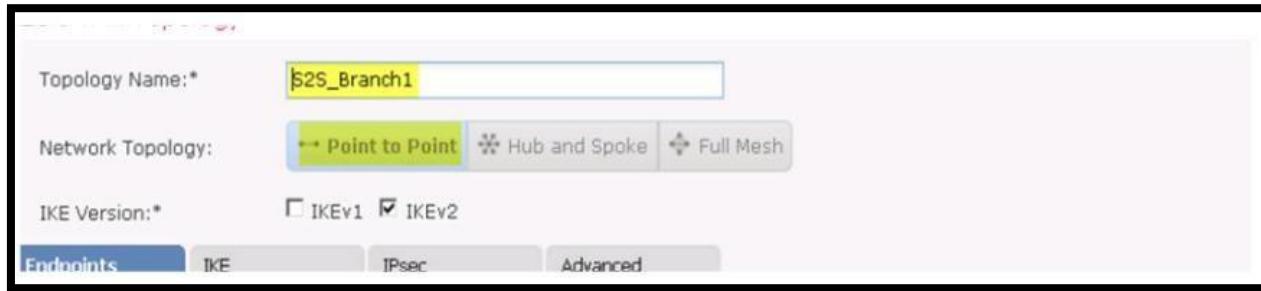
1. Navigate to **Objects > Object Management**. The **Network** object page will be selected.
 - a. Select **Add Network > Add Object**.
 - b. For Name, enter **MainOfficeNetwork**.
 - c. Select the **Network** radio button
 - d. Enter **198.19.10.0/24**.
 - e. Click **Save**.
2. Click **Add Network > Add Object**.
 - a. For Name, enter **Branch1OfficeNetwork**.
 - b. Click the Network radio button
 - c. Enter **198.19.11.0/24**.
 - d. Click **Save**.

Configure site-to-site VPN

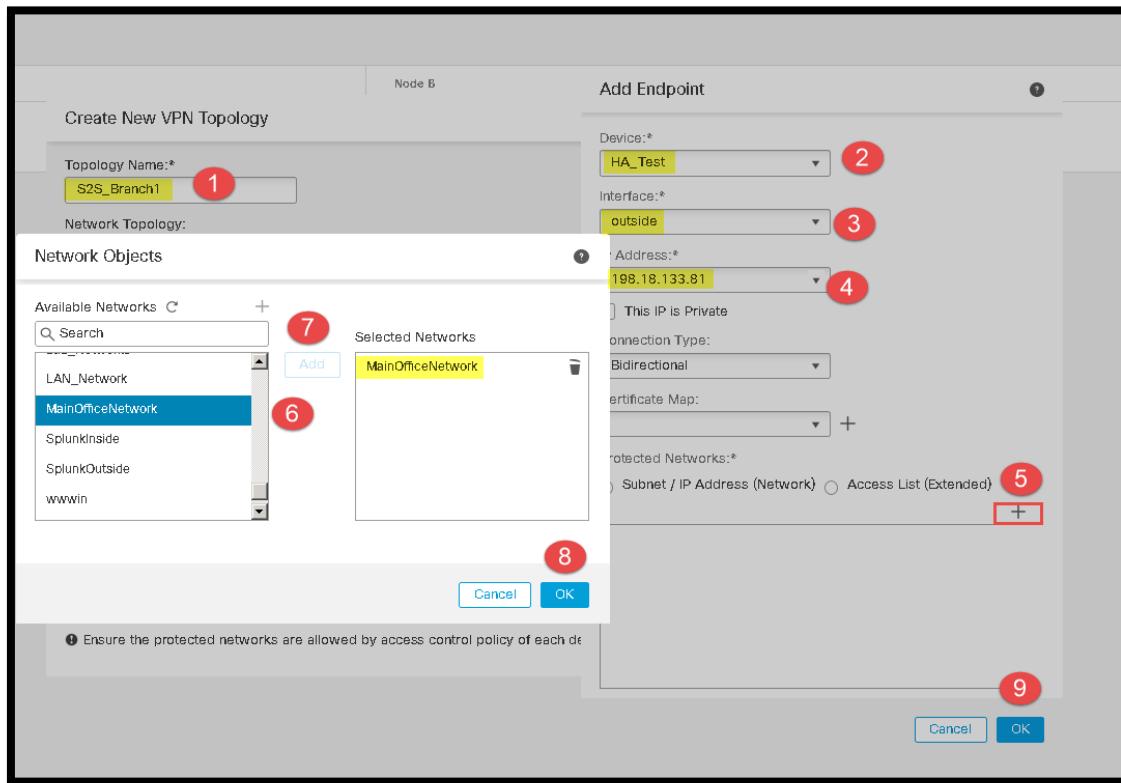
1. Navigate to **Devices > VPN > Site To Site**. Click **Add VPN > Firepower Threat Defense Device**.

NOTE: The other VPN choice, Firepower Device, is for configuring secure tunnels between Firepower devices.

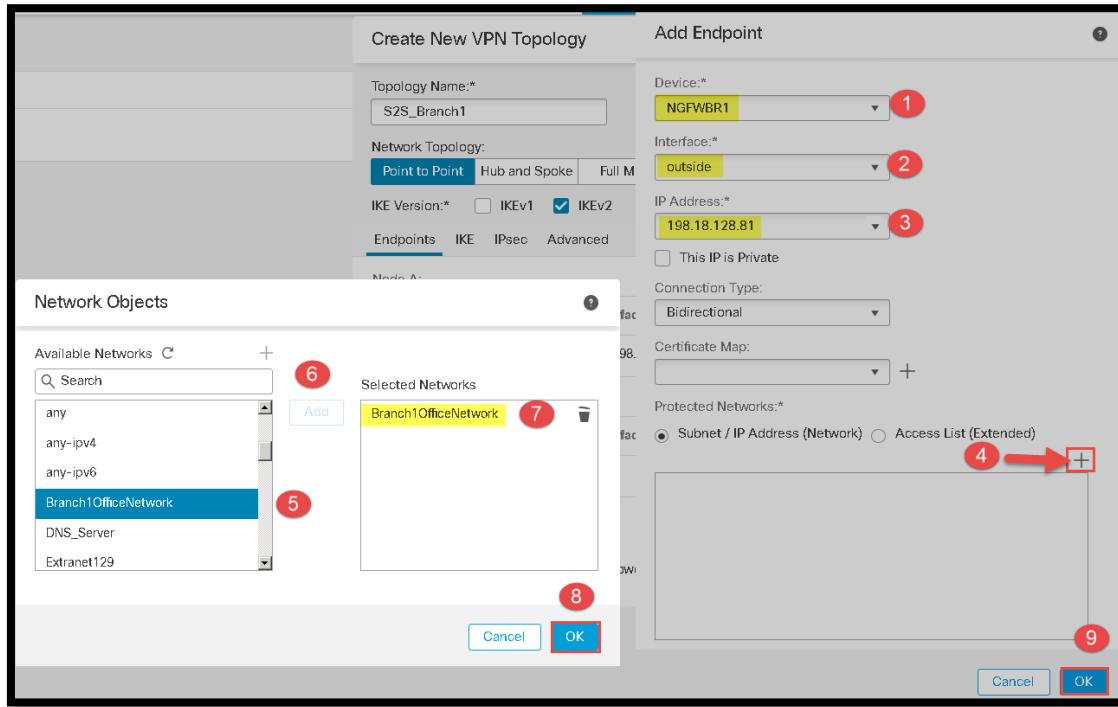
2. For Name enter **S2S_Branch1**.
 - a. Confirm that for Network Topology, Point to Point is selected. Confirm that for IKE Version, IKEv1 is not checked, and IKEv2 is checked.



- Click the plus (+) to the right of **Node A**. Fill out as in the figure below, and then click **OK**.



- Click the plus (+) icon to the right of **Node B**. Fill out the fields in the figure below, then click **OK**.



5. Select the **IKE** tab.
6. Under IKEv2 Settings, for Policy, select **AES-GCM-NULL-SHA-LATEST**.
7. Under IKEv2 Settings, for Authentication Type, select **Pre-shared Automatic Key**.

NOTE: The Automatic setting can only be used if the FMC is managing both endpoints. In this case, the FMC can generate a random shared key.

8. Select the **IPsec** tab, change the IKEv2 IPsec Proposal to Verify **AES-GCM**.
9. Click **OK** and **Save**.

Edit VPN Topology

Topology Name:*

Network Topology:

 Point to Point Hub and Spoke Full Mesh

IKE Version:*

 IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha	AES-GCM
-------------------	---------

Enable Security Association (SA) Strength Enforcement
 Enable Reverse Route Injection
 Enable Perfect Forward Secrecy

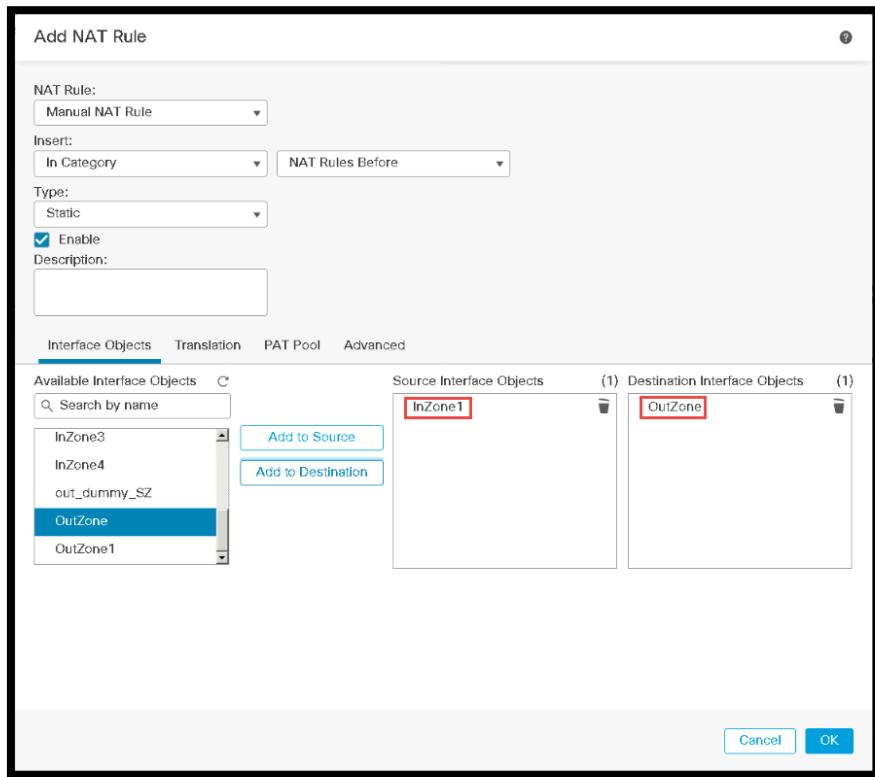
Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

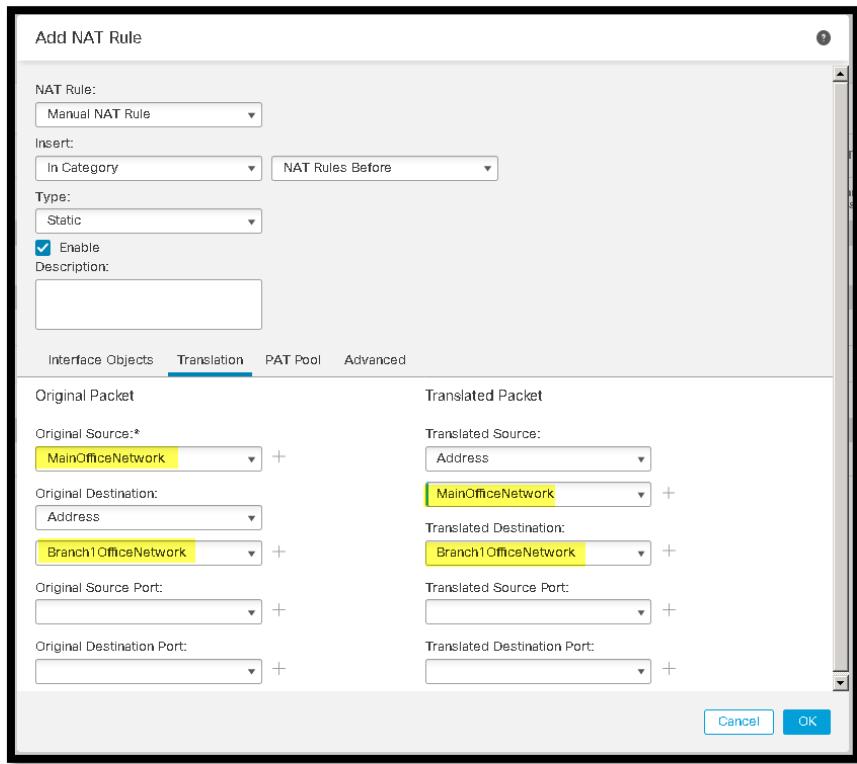
Create NAT exemption at HQ

NOTE: NAT exemption is used so that the addresses are not translated by NAT. To do this you have to have the packets translated by the NAT process back to their original addresses. This must be done before any other NAT statements so you will put the rule in the NAT Rules Before Category.

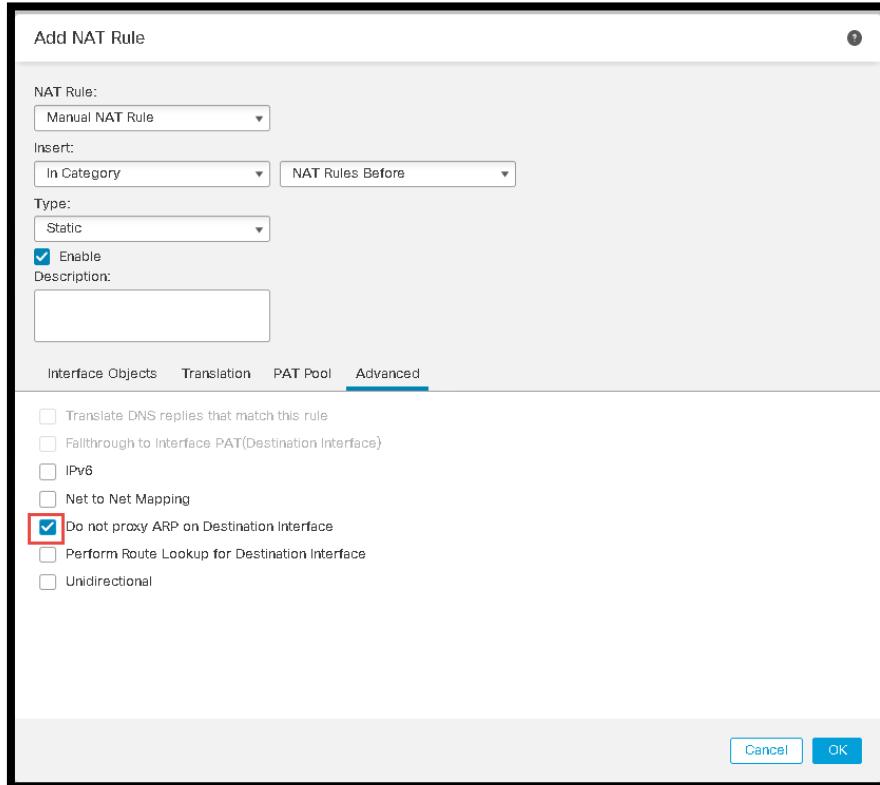
1. Navigate to **Devices > NAT**.
2. Click the pencil icon to edit the **Default PAT** policy.
3. Click **Add Rule**.
 - a. Leave **In Category** and **NAT Rules Before** from the **NAT Rule** drop-down list selected.
 - b. You will be at the **Interface Objects** tab.



- d. Select **InZone1** and click **Add to Source**
- e. Select **OutZone**, and click **Add to Destination**.
4. Select the **Translation** tab.
 - a. Select **MainOfficeNetwork** from the Original Source drop-down list.
 - b. Select **MainOfficeNetwork** from the Translated Source drop-down list.
 - c. Select **Branch1OfficeNetwork** from the Original Destination drop-down list.
 - d. Select **Branch1OfficeNetwork** from the Translated Destination drop-down list.



5. Go To **Advanced** and Check **Do not proxy ARP on Destination Interface** click **OK**.



6. Click **Save**.

Create NAT exemption for Branch1

1. Go to Devices > NAT > Branch NAT > click the pencil icon to edit the NAT policy

NAT Policy	Device Type	Status
Branch NAT Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices
Default NAT Policy	Threat Defense	Targeting 1 devices Out-of-date on 1 targeted devices

2. Click Add Rule.

a. Interface Objects

- i. Click **Branch1_InZone** and Add to Source.
- ii. Click **Branch1_OutZone** and Add to Destination.

Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category NAT Rules Before

Type: Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

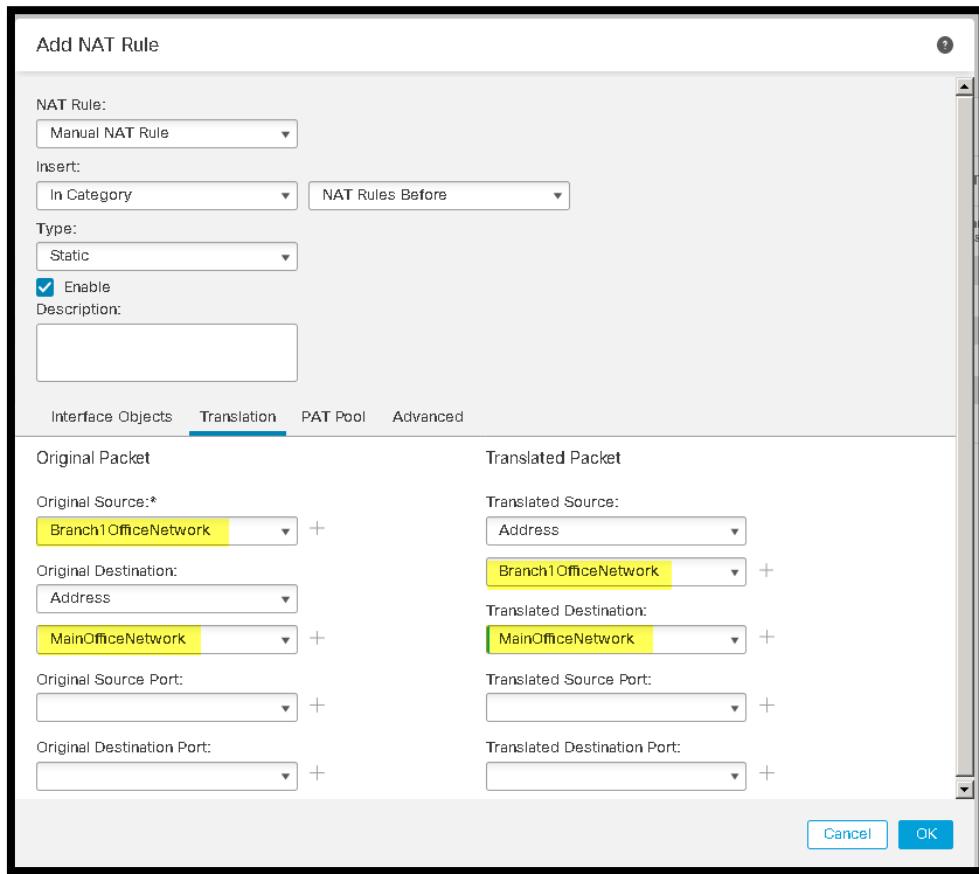
Available Interface Objects	Source Interface Objects	Destination Interface Objects
<input type="text" value="Search by name"/> Branch1_InZone Branch1_OutZone BVZone IntGroup10 InZone	(1) Branch1_InZone	(1) Branch1_OutZone

Add to Source
 Add to Destination

Cancel OK

b. Translation

- i. Original Packet
 1. Original Source Branch1OfficeNetwork
 2. Original Destination MainOfficenetwork
- ii. Translated Packet
 1. Translated Source Branch1OfficeNetwork
 2. Translated Destination MainOfficenetwork



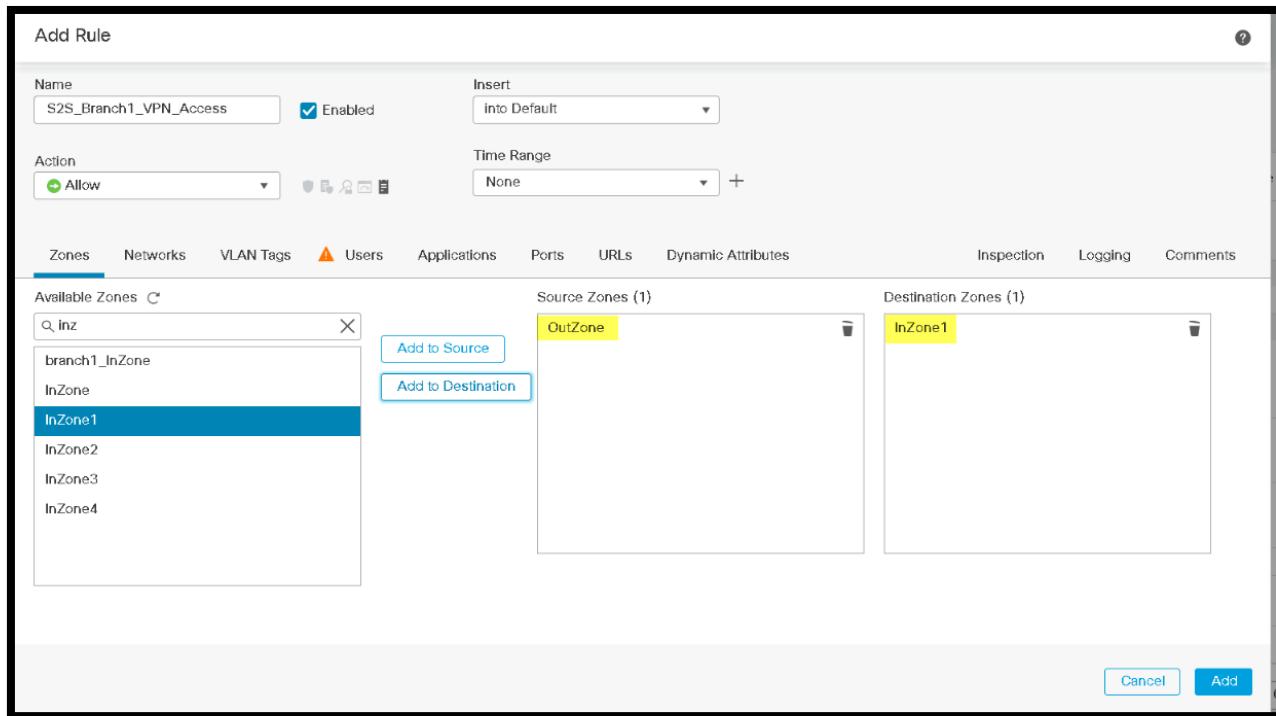
- c. Advanced
 i. On the Destination Interface, click **Do not proxy ARP on Destination Interface**

1. Click **OK**
2. Click **OK** to save NAT Rule
3. Click **Save** to save the NAT policy.

Modify the access control policy and deploy changes

You will now create a rule to allow traffic between the Branch office and Main office.

1. Navigate to **Policies > Access Control > Access Control**. Edit the **Base_Policy Access Control Policy**.
2. Click **Add Rule**.
 - a. Call the rule **S2S_Branch1_VPN_Access**.
 3. Select **into Default** from the **Insert** drop-down list. This will become the last rule in the access control policy.
 4. Keep the action at **Allow**.
 5. The **Zones** tab should already be selected.
 6. Select **OutZone**, and click **Add to Source**.
 7. Select **InZone1** and click **Add to Destination**.



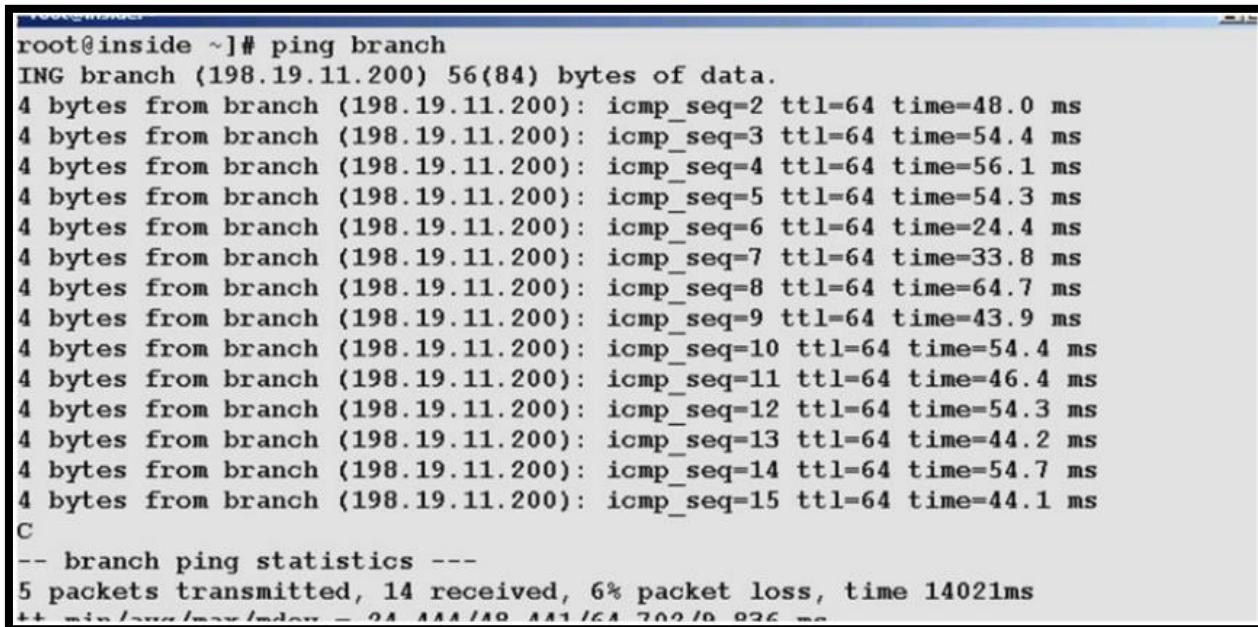
8. Select the **Networks** tab, select **Branch1OfficeNetwork**, and click **Add to Source**.
9. Select the **Networks** tab, select **MainOfficeNetwork**, and click **Add to Destination**.
10. Select the **Inspection** tab.
11. Select **HQ-Balanced-Policy** from the **Intrusion Policy** drop-down list.
12. Select **HQ File Policy** from the **File Policy** drop-down list.
13. Click **Add** to add this rule to the access control policy.
14. Modify the **Allow Outbound** rule and verify or add **ICMP** to Destination Ports
15. Click **Save** to save the access control policy.
16. **Modify the Branch1 Access Policy** to allow inbound connections

17. **Examine the Branch1_NAT Policy** to confirm the VPN NAT Exemption the first rule

Deploy the changes and test the configuration

1. **Deploy the changes on the FMC and wait for the deployment to complete.**
2. Go to the Jump PC Open PUTTY Connect to **NGFW1** and **NGFWBR1** Login: **admin** Password: **C1sco12345**
3. From the **NGFW1 CLI**, type **show crypto ipsec sa peer 198.18.128.81**. There should be no IPSec security associations.
4. Go to **NGFWBR1** and type: **show crypto ipsec sa peer 198.18.133.81** There should be no connections

5. Open a PUTTY Session to Inside Linux Server Login: **root** Password: **C1sco12345**
6. From the Inside Linux server CLI, type **ping branch**. Wait a few seconds, and the ping should succeed.

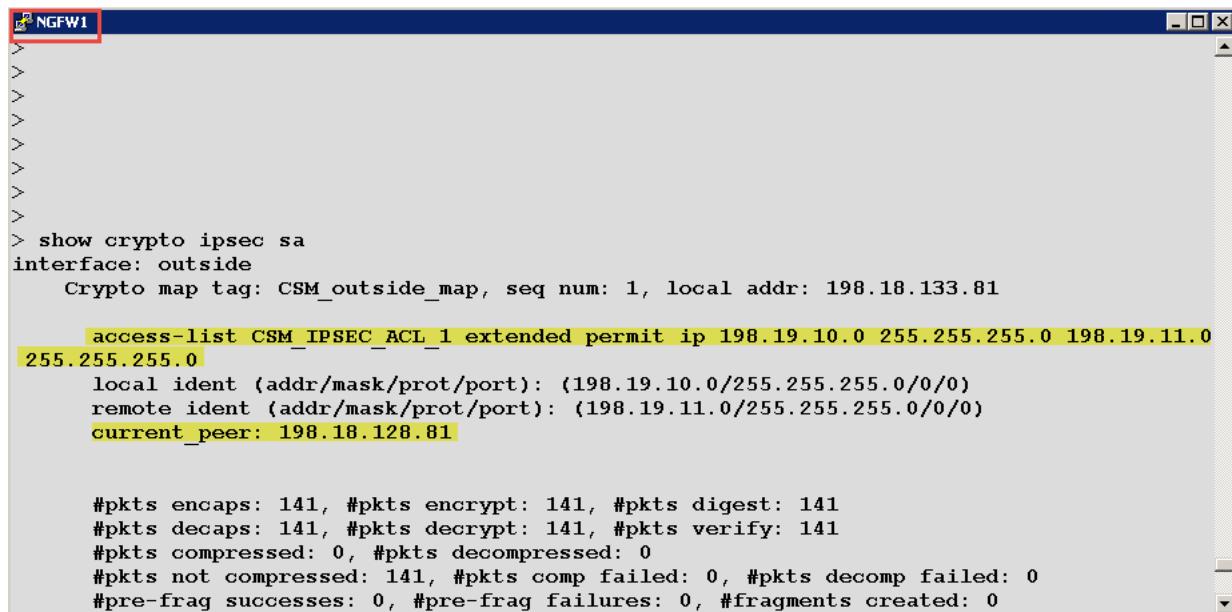


```

root@inside ~]# ping branch
PING branch (198.19.11.200) 56(84) bytes of data.
4 bytes from branch (198.19.11.200): icmp_seq=2 ttl=64 time=48.0 ms
4 bytes from branch (198.19.11.200): icmp_seq=3 ttl=64 time=54.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=4 ttl=64 time=56.1 ms
4 bytes from branch (198.19.11.200): icmp_seq=5 ttl=64 time=54.3 ms
4 bytes from branch (198.19.11.200): icmp_seq=6 ttl=64 time=24.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=7 ttl=64 time=33.8 ms
4 bytes from branch (198.19.11.200): icmp_seq=8 ttl=64 time=64.7 ms
4 bytes from branch (198.19.11.200): icmp_seq=9 ttl=64 time=43.9 ms
4 bytes from branch (198.19.11.200): icmp_seq=10 ttl=64 time=54.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=11 ttl=64 time=46.4 ms
4 bytes from branch (198.19.11.200): icmp_seq=12 ttl=64 time=54.3 ms
4 bytes from branch (198.19.11.200): icmp_seq=13 ttl=64 time=44.2 ms
4 bytes from branch (198.19.11.200): icmp_seq=14 ttl=64 time=54.7 ms
4 bytes from branch (198.19.11.200): icmp_seq=15 ttl=64 time=44.1 ms
C
-- branch ping statistics --
5 packets transmitted, 14 received, 6% packet loss, time 14021ms
+++ min/avg/max/stddev = 24.44/40.44/64.78/16.926 ms

```

7. From the NGFW1 CLI, type **show crypto ipsec sa**. There should now be an IPSec security association.



```

>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
> show crypto ipsec sa
interface: outside
  Crypto map tag: CSM_outside_map, seq num: 1, local addr: 198.18.133.81
    access-list CSM_IPSEC_ACL_1 extended permit ip 198.19.10.0 255.255.255.0 198.19.11.0
    255.255.0
      local ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (198.19.11.0/255.255.255.0/0/0)
      current_peer: 198.18.128.81
        #pkts encaps: 141, #pkts encrypt: 141, #pkts digest: 141
        #pkts decaps: 141, #pkts decrypt: 141, #pkts verify: 141
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 141, #pkts comp failed: 0, #pkts decomp failed: 0
        #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

```

8. On the Jump desktop, open the PUTTY link. Double click on the preconfigured session called **Branch Linux Server**.
9. Login as **root**, password **C1sco12345**
10. Type **curl inside**. This should succeed.

Scenario 6. Route Based VTI Site-to-Site VPN

This scenario will show the use of Virtual Tunnel Interface support for the Cisco Secure Firewall added in 6.7.

Policy based vs Route-Based VPN. Both are now available with the FTD. Route based VPN's are more flexible than Policy-Based VPN, but for some applications Policy-Based VPN's may be needed.

Clean up from Prior VPN Labs

1. FMC Devices > Default PAT
 - a. Disable the NAT Rule InZone to OutZone MainOfficeNetwork BranchOffice Network
 - b. Click **Save**
2. FMC Devices > Branch1_NAT
 - a. Disable the NAT Rule branch1_InZone branch1_Outzone Brach1OfficeNetowrk MainOfficeNetwori
 - b. Click **Save**

Create Security zone for VTI interfaces

1. On the FMC go to **Objects > Object Management**
2. Select **Interface** from the left navigation pane
3. Click **Add > Security Zones**
 - a. Name: **VTIZone**
 - b. Select: **Routed**
 - c. **Save**

The screenshot shows the 'Security Zones' configuration dialog. The 'Name:' field is filled with 'VTIZone'. The 'Interface Type:' dropdown is set to 'Routed'. Under 'Available Interfaces', 'NGFW1' is listed. An 'Add' button is positioned between the two interface lists. The 'Selected Interfaces' list is empty. At the bottom, there are 'Cancel' and 'Save' buttons, with 'Save' being highlighted.

Modify the Access Control Policies on NGFW1 and NGFWBr1

1. Go to **Policies > Access Control**
2. Edit the **Base_Policy**
 - a. Create or Edit the rule **Allow East-West**

- b. Under **Zones** make sure that All **InZones and VTIZone** are added to the Source and Destination Zones

- c. Click Add and Save

3. Go to Policies > Access Control
4. Edit **Branch1access** policy
 - a. Create or Edit the rule **Allow East-West**
 - b. Under **Zone** make sure that **branch1_InZone and VTIZone** are added to the Source and Destination Zones

c. Click Add and **Save and Save the Policy**

If you did the Remote Deployment Lab on NGFWBr1 disable the remote management and redeploy

Compare Policy-Based and Route-Based VPN configuration

1. On the FMC go to **Devices > VPN > Site to Site** delete **S2S_Branch1**
2. Click on Add VPN and Select **Firepower Threat Defense**
3. Confirm that Point to Point is selected
 - a. Click on Endpoints and then click between **Policy Based and Route Based** notice the differences
 - b. Repeat for IKE, IPSec and Advanced
4. Run the site to site VPN wizard
 - a. Topology Name: **VTIDemo**
 - b. Route Based (VTI): Select
 - c. Network Topology: Point to Point
 - d. Endpoints:
 - i. Node A: NGFW1 or HA_Test
 - ii. Virtual Tunnel Interface: Click on the [+]
 1. Name: **vti1**
 2. Security Zone: **VTIZone**
 3. Tunnel ID: **1**
 4. IPv4 Address: **10.0.1.1/30**
 5. Tunnel Source: **GigabitEthernet0/0 (Outside)**

The screenshot shows the configuration of a Virtual Tunnel Interface (VTI) in the Cisco Firepower Threat Defense interface. The fields filled in are:

- Name: vti1
- Enabled: checked
- Description: (empty)
- Security Zone: VTIZone
- Tunnel ID: 1
- IPsec Tunnel Mode: IPv4 (radio button selected)
- IPv4 Address: 10.0.1.1/30
- IPv6 Address: (empty)
- Tunnel Source: GigabitEthernet0/0 (Outside)
- Tunnel Destination IP: 198.18.128.81

6. Click **OK**
- iii. Node B: NGFWBr1
- iv. Virtual Tunnel Interface: Click on the [+]

1. Name: vti1
2. Security Zone: VTIZone
3. Tunnel ID: 1
4. IPv4 Address: 10.0.1.2/30
5. Tunnel Source: GigabitEthernet0/0 (branch1_Outside)

Name:^{*}
vti1

Enabled

Description:

Security Zone:
VTIZone

Tunnel ID:^{*}
1
Range: 0 - 10413

IPsec Tunnel Mode:^{*}
 IPv4
 IPv6

IPv4 Address:^{*}
10.0.1.2/30

IPv6 Address:

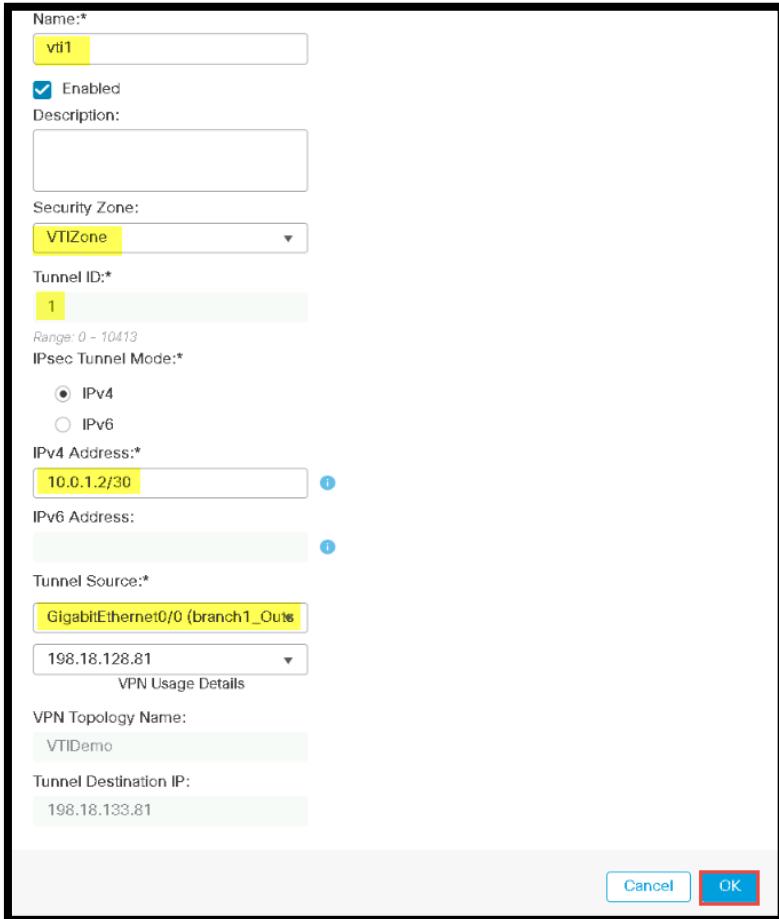
Tunnel Source:
GigabitEthernet0/0 (branch1_Outside)
198.18.128.81

VPN Usage Details

VPN Topology Name:
VTIDemo

Tunnel Destination IP:
198.18.133.81

Cancel **OK**



6. Click **OK**

Create New VPN Topology

Topology Name:

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:

Virtual Tunnel Interface: +

Tunnel Source: Outside (IP: 198.18.133.81) [Edit VTI](#)
 Tunnel Source IP is Private

+ Add Backup VTI (optional)

Connection Type:

Additional Configuration
 Route traffic to the VTI : [Routing Policy](#)
 Permit VPN traffic : [AC Policy](#)

Node B

Device:

Virtual Tunnel Interface: +

Tunnel Source: branch1_Outside (IP: 198.18.128.81) [Edit VTI](#)
 Tunnel Source IP is Private

+ Add Backup VTI (optional)

Connection Type:

Additional Configuration
 Route traffic to the VTI : [Routing Policy](#)

[Cancel](#) [Save](#)

5. Click **Save** and then **Deploy > Select NGFWBr1 and NGFW1**

Configure BGP

1. FMC Devices > Device Management
2. Edit **NGFW1** and select Routing
 - a. Under General Settings select **BGP**
 - i. Click Enable BGP if not already enabled
 - ii. AS Number: 65000
 - b. Under BGP select IPv4
 - i. Click Enable IPv4
 - ii. Select Neighbor and delete existing neighbor
 1. Click Add
 - a. IP Address: **10.0.1.2**
 - b. Remote AS: **65001**
 - c. Address Family: **Enabled**
 - d. Click **OK**
 - iii. Select Redistribution
 1. Click Add
 - a. Source Protocol: **Connected**
 - b. Metric: **0** [Needed as a placeholder]
 - c. Click **OK**
 3. Click **Save** at the top of the page

4. Edit NGFWBr1
 - a. Select Routing and BGP and Enable BGP AS Number 65001
 - b. Select IPv4 under BGP
 - i. Click Enable IPv4
 - ii. Click Neighbor
 1. Address: 10.0.1.1 Remote AS 65000, Address Family **Enabled**
 - iii. Click Redistribution
 1. Redistribute **Connected Metric 0**
 5. Click **Save** at the top of the Page
 6. **Deploy the Changes**
 7. Wait for the Deployment to complete and then an additional 30 seconds or so for the tunnel and BGP adjacency to complete
 8. Open a PuTTY session to **NGFWBr1 admin/C1sco12345**
 9. Type show crypto ipsec sa
 - a. Verify you have a connection if you do not you will need to troubleshoot your VPN configuration
 - b. Type show run router

```

> show running-config router
router rip
  network 198.19.11.0
  redistribute connected metric transparent
!
router bgp 65001
  bgp log-neighbor-changes
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.0.1.1 remote-as 65000
    neighbor 10.0.1.1 transport path-mtu-discovery disable
    neighbor 10.0.1.1 activate
    redistribute connected metric 0
  no auto-summary
  no synchronization
exit-address-family
!
>

```

- c. Type **show bgp summary**

```

> show bgp summary
BGP router identifier 198.19.11.1, local AS number 65001
BGP table version is 8, main routing table version 8
7 network entries using 1400 bytes of memory
9 path entries using 720 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2560 total bytes of memory
BGP activity 32/25 prefixes, 42/33 paths, scan interval 60 secs

Neighbor      V        AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.1.1      4       65000  116     117         8      0    0 02:04:10  6

```

- d. If you see State/Pfxcd as **Idle or Active** troubleshoot your BGP Connection
- e. If you see StatePfxcd as **0** troubleshoot your BGP redistribution
- f. Type **show route bgp** you should see multiple routes
- g. Open a PuTTY session to the **Inside Linux server**
- h. Type **Ping Branch** should succeed

Scenario 7. Site-to-Site VPN Between FMC and FDM Managed Devices

There are a few Site-to-site (S2S) VPN enhancements beginning in 6.4. While configuring the tunnel also pay attention to the other enhancement which is available – the ability to explicitly configure dynamic peering on both FMC and FDM. This allows Firepower to scale its S2S VPN capabilities to accommodate branch management.

The objectives of this scenario are:

- Create the objects required for configuration of S2S VPN on NGFW2 and NGFW Branch 1.
- Test traffic through the S2S tunnel that's established.

Steps

Lab Preparation

1. Open a PUTTY session to the Inside Linux Server Username: root Password: C1sco12345
 - a. Type route add -net 198.19.11.0 netmask 255.255.255.0 gw 198.19.10.2
 - i. This will set the path for the Inside Linux server to reach the Branch1 LAN network

Configure S2S VPN on FMC managing NGFW Branch 1

1. On the Jumpbox, open Firefox and click on FMC in the bookmarks list. Login to the FMC.
2. Navigate to Objects > Object Management > Network. Click on Add Object.
 - a. Enter NGFWBr1_LAN as the Name.
 - b. Set Network to Network and type in 198.19.11.0/24.
 - c. Click on Save.
3. Click on Add Object.
 - a. Enter NGFW2_LAN as the Name.
 - b. Set Network to Network and type in 198.19.10.0/24.
 - c. Click on Save
4. Navigate to Devices > VPN > Site to Site If you have done the previous Site to Site Lab delete current VPN and deploy
5. Click on Add VPN then click Firepower Threat Defense Device



- a. Enter Topology Name: **S2SVPN**
- b. Set IKE Version to IKEv1 only.
- c. Under Endpoints, click on + for Node A.
 - i. Select **Extranet** as Device.
 - ii. Enter **NGFW2** as Device Name.
 - iii. Set IP Address as Static and **198.18.133.82**.
 - iv. Under Protected Networks, add the **NGFW2_LAN** object.
 - v. Click on **OK**.

Add Endpoint

Device:*

Extranet

Device Name:*

NGFW2

IP Address:*

Static Dynamic

198.18.133.82

Certificate Map:

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)

NGFW2_LAN

Cancel OK

- d. Under Endpoints, click on + for Node B.
- i. Select **NGFWBR1** as Device.
 - ii. Set Interface as **branch1_outside**.
 - iii. IP Address will populate as **198.18.128.81**.
 - iv. Under Protected Networks, add the **NGFWBr1_LAN** object.
 - v. Click on **OK**.

Add Endpoint

Device:*

NGFWBR1

Interface:*

outside

IP Address:*

198.18.128.81

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)

NGFWBr1_LAN

Cancel OK

Create New VPN Topology

Topology Name:*

Network Topology:

 Point to Point Hub and Spoke Full Mesh

IKE Version:*

 IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Device Name	VPN Interface	Protected Networks	
NGFW2	198.18.133.82	NGFW2_LAN	

Device Name	VPN Interface	Protected Networks	
NGFWBR1	outside/198.18.128.81	NGFWBR1_LAN	

! Ensure the protected networks are allowed by access control policy of each device.

Cancel Save

- e. Navigate to IKE.
- i. Change IKEv1 Policy to **preshared_sha_aes256_dh14_3**
 - ii. Authentication Type: **Pre-shared Manual Key**
 - iii. Key: **C1sco12345**
 - iv. Confirm Key: **C1sco12345**

Edit VPN Topology

Topology Name:*

Network Topology:

 Point to Point Hub and Spoke Full Mesh

IKE Version:*

 IKEv1 IKEv2

Endpoints IKE IPsec Advanced

IKEv1 Settings

Policy:*

Authentication Type:

Key:*

Confirm Key:*

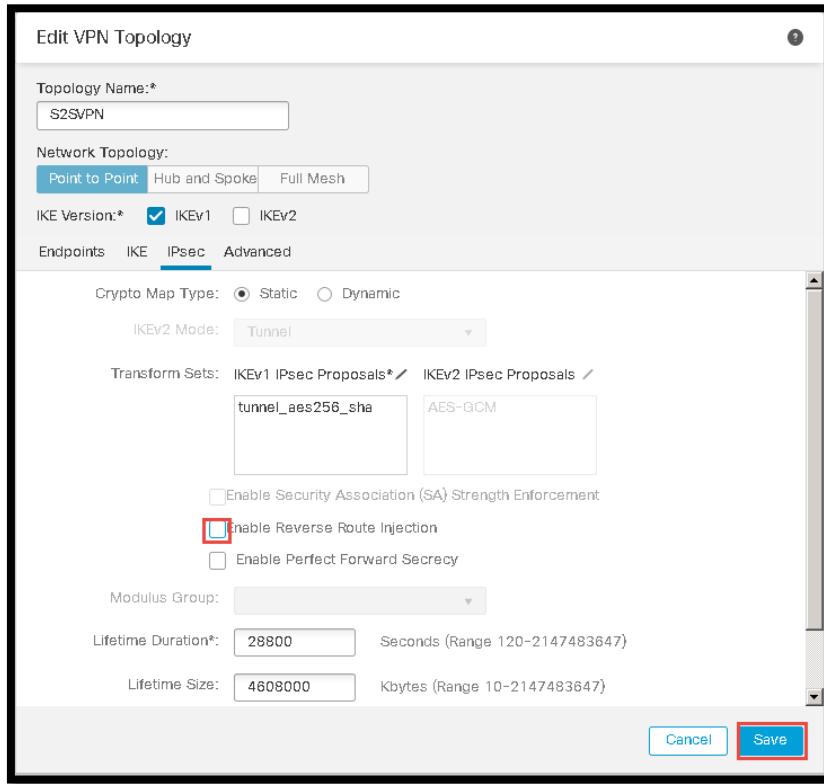
IKEv2 Settings

Policy:*

Authentication Type:

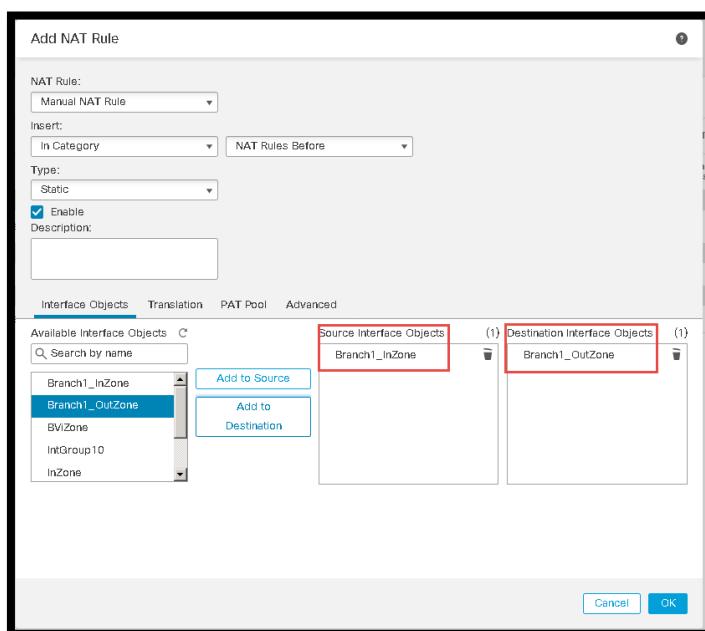
Cancel Save

f. Navigate to IPSec
 i. Uncheck Enable Reverse Route Injection

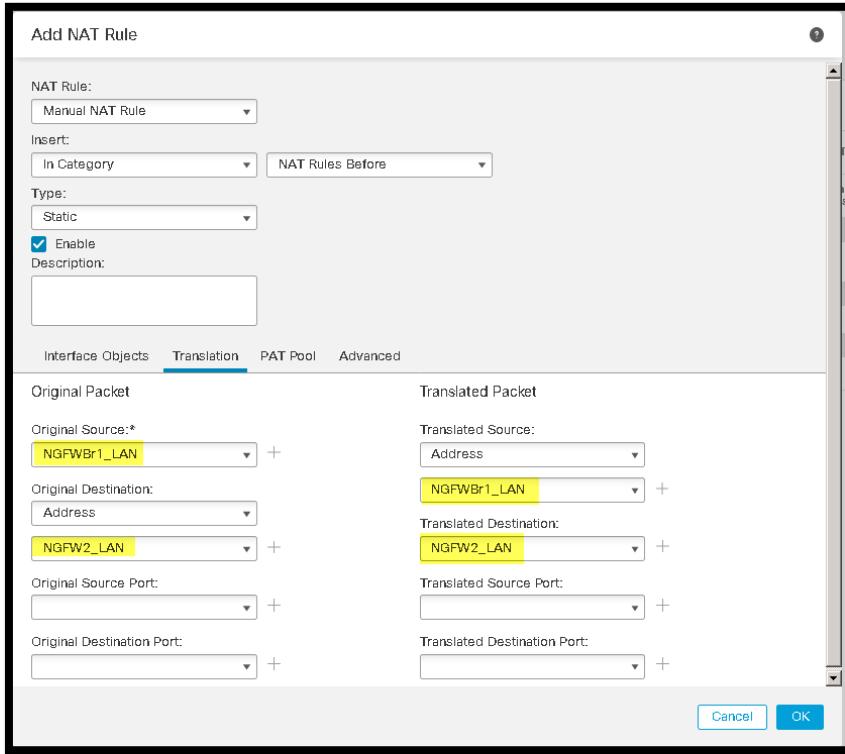


g. Click on Save.

6. Navigate to Devices > NAT and Edit Branch NAT Policy If you did the previous lab modify the NAT Exemption and enable or:
7. Click Add Rule.
 - a. Select Branch1_InZone for Source Interface Objects and Branch1_OutZone for Destination Interface Objects

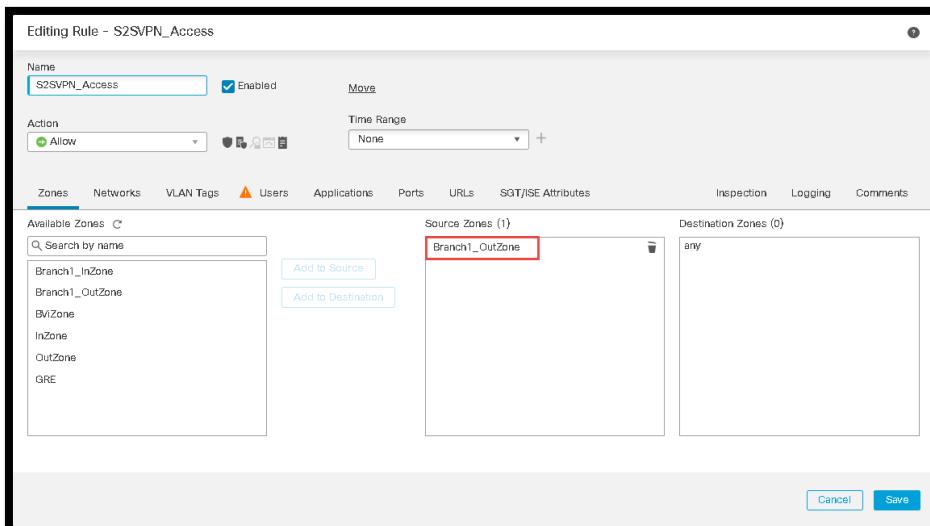


- b. Under the Translation tab, select **NGFWBr1_LAN** as Original Source and Translated Source. Select **NGFW2_LAN** as the Original Destination and Translated Destination.
- c. On the Advanced Tab select **Do not proxy ARP on Destination Interface**



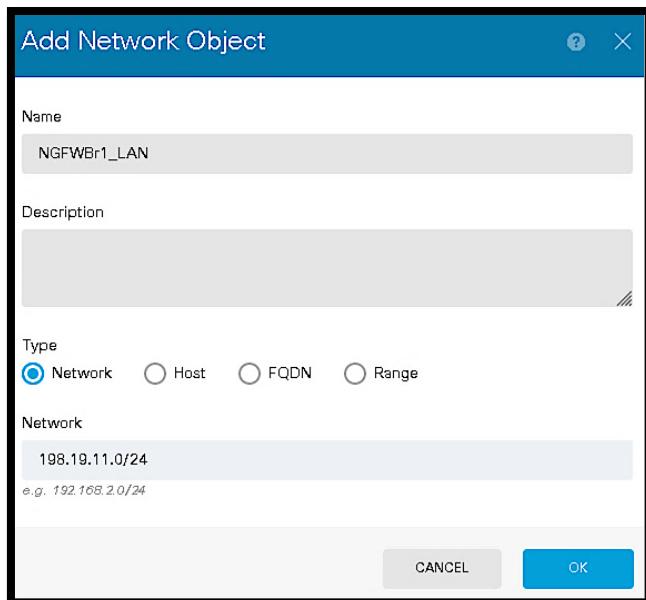
- d. Click **OK** to save the NAT rule. Click on **Save**.

8. Navigate to Policies > Access Control and edit Branch1 Access Control Policy. Click on Add Rule.
 - a. Enter Name as **S2SVPN_Access**.
 - b. Change Insert to Into Mandatory.
 - c. Add **Branch1_OutZone** to Source Zone and **NGFW2_LAN** as Source Networks.
 - d. Under Inspection, set Intrusion Policy to **HQ-High-Security-Policy** and File Policy to **HQ File Policy**.
 - e. Under Logging, check Log at End of Connection.
 - f. Click on Add. Click on Save.

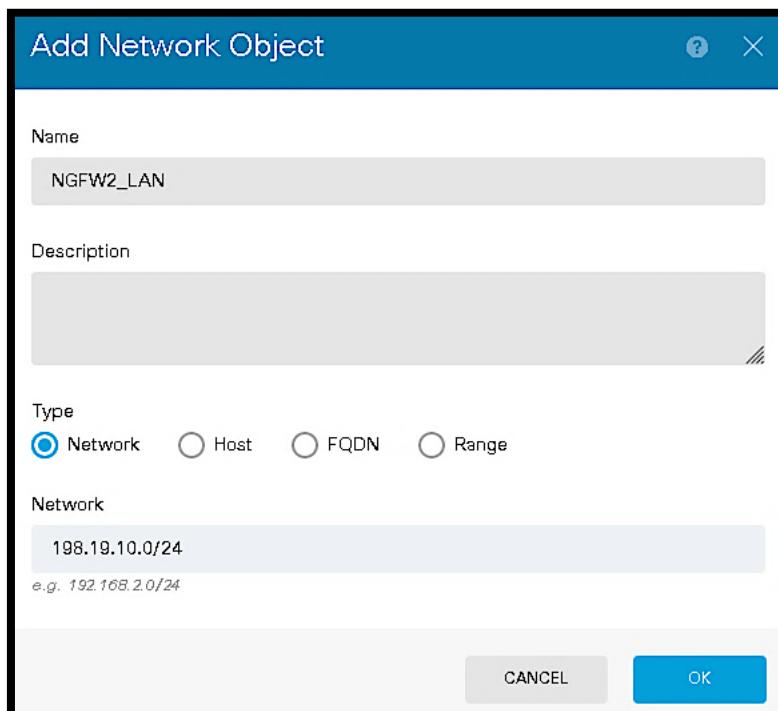


Configure S2S VPN on FDM managing NGFW2

1. On the Jumpbox, open Firefox and click on NGFW2 (FDM) in the bookmarks list. Login to the NGFW2 FDM.
2. Navigate to Objects > Networks. Click on +.
 - a. Set Name to **NGFWBr1_LAN**, Type as Network and Network as **198.19.11.0/24** and **OK**



- b. Repeat steps for: **NGFW2_LAN**, Type as Network and Network as **198.19.10.0/24**.



3. Navigate to Device > Site to Site VPN > View Configuration. Click on +.

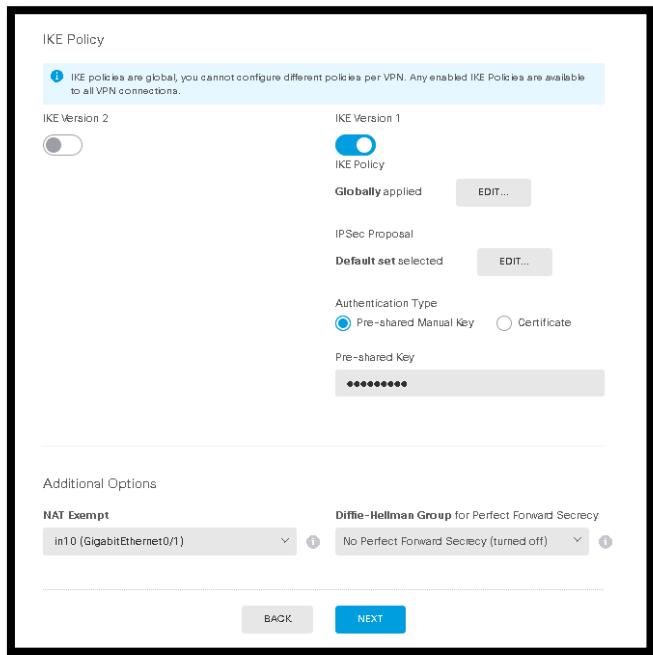
- a. Enter Connection Profile Name as **S2SVPN**
- b. Select **outside** [GigabitEthernet0/0] from Local VPN Access Interface dropdown.
- c. Add **NGFW2_LAN** as the Local Network.
- d. Enter Remote IP Address as **198.18.128.81**.
- e. Select **NGFWBr1_LAN** as the Remote Network.
- f. Click on **Next**.

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name	Type
<input type="text" value="S2SVPN"/>	<input type="radio"/> Route Based (VTI) <input checked="" type="radio"/> Policy Based
Sites Configuration	
LOCAL SITE	
Local VPN Access Interface <input type="text" value="outside (GigabitEthernet0/0)"/>	REMOTE SITE <input checked="" type="radio"/> Static <input type="radio"/> Dynamic Remote IP Address <input type="text" value="198.18.128.81"/>
REMOTE SITE	
Local Network + <input type="text" value="NGFW2_LAN"/>	Remote Network + <input type="text" value="NGFWBr1_LAN"/>
CANCEL NEXT	

- g. **Enable IKEv1 and disable IKEv2.**
- h. Edit IKE Policy and enable **SHA-AES256-GROUP14-PRE_SHARED_KEY**
- i. Edit IPSec Proposal and click on **Set Default** and **OK**.
- j. Select Authentication Type. **Pre-shared Manual Key**
- k. Pre-shared Key: **C1sco12345**
- l. Under Additional Options select **in10 (GigabitEthernet0/1)** from the NAT Exempt dropdown.



4. Click on Next

- a. Review the Summary and click on Finish.

NOTE: The FDM adds in a NAT exemption statement for VPN traffic which is only visible via CLI.

5. Navigate to Policies > Access Control. Click on +.

- a. For the new rule, set Order to 1.
- b. Name will be **S2SVPN_Access** and Action will be **Allow**.
- c. Set Source Zone to **outside_zone** and Source Networks to **NGFWBr1_LAN**.

Order	Title	Action
1	S2SVPN_Access	Allow

Source/Destination Applications URLs Users Intrusion Policy File policy Logging

SOURCE

Zones	+ <input checked="" type="checkbox"/> outside_zone	Networks	+ <input checked="" type="checkbox"/> NGFWBr1_LAN	Ports	+ <input checked="" type="checkbox"/>

DESTINATION

Zones	+ <input checked="" type="checkbox"/>	Networks	+ <input checked="" type="checkbox"/>	Ports/Protocols	+ <input checked="" type="checkbox"/>

- d. Navigate to Intrusion Policy. Enable Intrusion Policy and set the Level to **Balanced Security and Connectivity**

Add Access Rule

Order	Title	Action
1	S2SVPN_Access	Allow

Source/Destination Applications URLs Users **Intrusion Policy** File policy Logging

INTRUSION POLICY

Level of Intrusion Policy
Balanced Security and Connectivity

Balanced Security and Connectivity
This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.

PREVENTING INTRUSIONS

Use intrusion policies as a last line of defense against unwanted traffic that you are otherwise allowing. An intrusion policy examines decoded packets for intrusions, exploits, and other attacks based on patterns, and can block or alter malicious traffic. Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings.

- e. Navigate to File Policy. Select **Block Malware All**.

Add Access Rule

Order	Title	Action
1	S2SVPN_Access	Allow

Source/Destination Applications URLs Users **Intrusion Policy** **File policy** Logging

SELECT THE FILE POLICY
Block Malware All

Query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.

CONTROLLING FILES AND MALWARE

Use file policies to detect malicious software, or malware, using Advanced Malware Protection for Firepower (AMP for Firepower.) You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware

- f. Navigate to Logging. Select At End of Connection for Select Log Action. Click on OK.

Deploy and test the configuration

1. **Deploy** the configurations on both **NGFWBR1** on the FMC and the **NGFW2 FDM**.
2. On the Jumpbox, open a PUTTY session to the Inside Linux Server. **Login as root/C1sco12345**.
3. The Inside Linux Server sits in the LAN behind NGFW2. We will ping a workstation in Branch 1 with an IP address of **198.19.11.225**. The ping should be successful. (The first one might drop to initiate the tunnel)

```
[root@inside ~]# ping 198.19.11.225
PING 198.19.11.225 (198.19.11.225) 56(84) bytes of data.
64 bytes from 198.19.11.225: icmp_seq=2 ttl=128 time=2.91 ms
64 bytes from 198.19.11.225: icmp_seq=3 ttl=128 time=54.0 ms
64 bytes from 198.19.11.225: icmp_seq=4 ttl=128 time=2.85 ms
64 bytes from 198.19.11.225: icmp_seq=5 ttl=128 time=2.25 ms
64 bytes from 198.19.11.225: icmp_seq=6 ttl=128 time=2.88 ms
64 bytes from 198.19.11.225: icmp_seq=7 ttl=128 time=3.12 ms
64 bytes from 198.19.11.225: icmp_seq=8 ttl=128 time=2.10 ms
^C
--- 198.19.11.225 ping statistics ---
8 packets transmitted, 7 received, 12% packet loss, time 7008ms
rtt min/avg/max/mdev = 2.109/10.027/54.046/17.973 ms
[root@inside ~]#
```

4. You can see the tunnel status by logging into either NGFW2 or NGFWBR1 via Putty and executing show crypto ikev1 sa and show crypto ipsec sa.

```

> show crypto ikev1 sa
IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 198.18.133.82
  Type : L2L           Role : responder
  Rekey : no            State : MM_ACTIVE
>
> show crypto ipsec sa
interface: outside
Crypto map tag: CSM_outside_map, seq num: 1, local addr: 198.18.128.81
access-list CSM_IPSEC ACL 1 extended permit ip 198.19.11.0 255.255.255.0 198.19.10.0 255.255.255.0
local ident (addr/mask/prot/port): (198.19.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
current_peer: 198.18.133.82

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts frag successes: 0, #pkts frag failures: 0, #fragments created: 0
#PMUs sent: 0, #PMUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 198.18.128.81/0, remote crypto endpt.: 198.18.133.82/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
DMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current inbound spi: 5DA5050
current inbound spi : 6AB7CCC7

inbound esp sas:
spi: 0x6AB7CCC7 (1790430407)
  SA State: active
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings -(I2L, Tunnel, IKEv1, )
  slot: 0, conn_id: 1, crypto-map: CSM_outside_map
  sa timing: remaining key lifetime (kB/sec): (3914999/28613)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x000000FF
outbound esp sas:
spi: 0x5DDA5050 (1574588496)
  SA State: active
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings -(I2L, Tunnel, IKEv1, )
  slot: 0, conn_id: 1, crypto-map: CSM_outside_map
  sa timing: remaining key lifetime (kB/sec): (3914999/28613)
  IV size: 16 bytes

```

5. You can verify the tunnel authentication method that is being used by logging into either NGFW2 or NGFWBR1 via Putty and executing show vpn-sessiondb detail |2|.

```

> show vpn-sessiondb detail 121

Session Type: LAN-to-LAN Detailed

Connection : 198.18.128.81          IP Addr      : 198.18.128.81
Index       : 1                      IP Addr      : 198.18.128.81
Protocol    : IKEv1 IPsec
Encryption  : IKEv1: (1)AES256 IPsec: (1)AES256
Hashing     : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx   : 60312                 Bytes Rx    : 60312
Login Time : 10:38:14 UTC Wed May 8 2019
Duration   : 0h:12m:00s
Tunnel Zone: 0

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
Tunnel ID   : 1.1
UDP Src Port: 500                  UDP Dst Port : 500
IKE Neg Mode: Main                Auth Mode    : rsaCertificate
Encryption  : AES256               Hashing      : SHA1
Rekey Int (T): 86400 Seconds      Rekey Left(T): 85681 Seconds
D/H Group   : 5
Filter Name : 

IPsec:
Tunnel ID   : 1.2
Local Addr  : 198.19.10.0/255.255.255.0/0/0
Remote Addr : 198.19.11.0/255.255.255.0/0/0
Encryption  : AES256               Hashing      : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds       Rekey Left(T): 28081 Seconds
Rekey Int (D): 4608000 K-Bytes     Rekey Left(D): 4607942 K-Bytes
Idle Time Out: 30 Minutes         Idle To Left : 30 Minutes
Bytes Tx    : 60312               Bytes Rx    : 60312
Pkts Tx    : 718                  Pkts Rx    : 718

```

NOTE: In order to save time, ISE has been pre-configured with all required configuration for all of the lab exercises. If you want to inspect the ISE configuration, see Appendix 3. **NOTE:** Enabling **Do not proxy ARP on Destination Interface** is critical in this lab exercise. If you miss this step, your pod may have access issues, since all devices are managed in band.

Scenario 8. Monitoring and Troubleshooting

This exercise consists of the following tasks.

- Monitoring AnyConnect user activity
- Troubleshooting

You will use the FMC for Monitoring AnyConnect User activity and troubleshooting.

Steps

Monitoring AnyConnect user activity

In this section, you can monitor all active users who have logged in through AnyConnect.

1. From the Cisco dCloud Topology Map
 - a. Click on WKST 2
 - b. Login: Administrator Password: C1sco12345
 - c. Start an AnyConnect Session
 - i. Either by clicking in the bottom tray on the Windows Desktop
 - ii. or Start and type AnyConnect in the search bar
 - d. Click on the Connect Button [Should connect to ngfw1]
 - i. Username: pc-outside
 - ii. Password: C1sco12345
2. In the FMC, navigate to **Overview > Dashboards > Switch dashboard > Access Controlled User Statistics**

The screenshot shows the FMC interface with the 'Access Controlled User Statistics' dashboard selected. The navigation bar at the top has tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Status' tab is highlighted with a red box. The dashboard itself has several sections: 'Appliance Status' (green circle), 'Appliance Information' (listing name, IP address, model, and versions), 'Current Sessions' (showing one session for 'admin' from '198.19.10.50' last accessed '12:33:04'), and 'System Time' (listing system time, uptime, and boot time). There are also links for 'RSS Feed - Talos Blog' and 'Cisco Talos Intelligence Group - Comprehensive Threat'.

3. **Select the VPN tab.** Note that there are 7 widgets dedicated to VPN traffic.
4. Navigate to **Analysis > Users > Active Sessions.**
 - a. Notice that you see pc-outside VPN session.
 - b. **Check the box** to the left of pc-outside session and click **Logout**. When prompted, click **Continue**.

NOTE: You may also see other active sessions discovered with network discovery. For example, you may see guest discovered through an FTP session. For brevity, those sessions were left out of the figure above. If you want more details about users and how they were discovered, navigate to Analysis > Users > Users.

5. On Outside-PC, confirm that pc-outside has been logged out.
6. In the FMC, navigate to **Analysis > Users > User Activity**. In this window you will see details of current and past user sessions. Spend a couple minutes reviewing the information on this page.

Troubleshooting

In this section, you will modify the Syslog level for VPN events on the NGFW. You will also run some basic troubleshooting commands from the NGFW1 CLI. You will also look at the 7.x feature Unified events and look at Live Logs

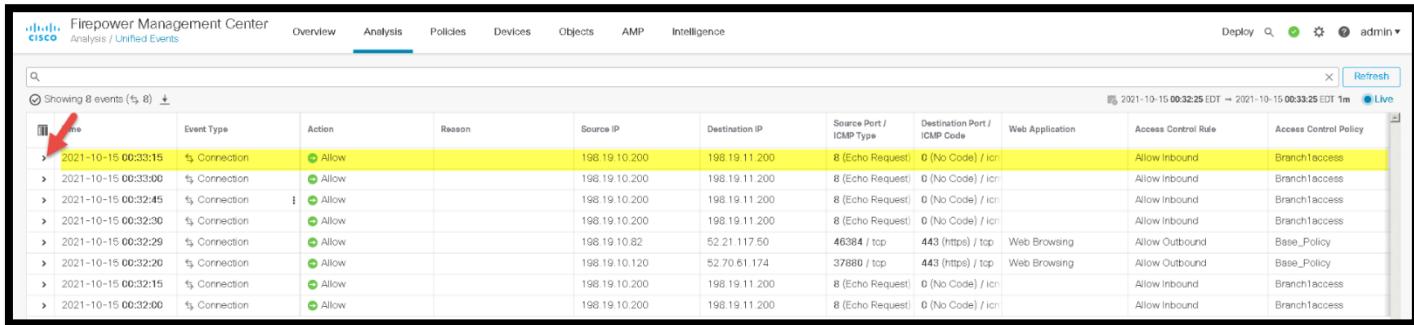
1. FMC Analysis > Unified Events

Hosts			Correlation
Network Map			Correlation Events
Hosts			Allow List Events
Indications of Compromise			Allow List Violations
Applications			Status
Application Details			
Servers		Advanced	
Host Attributes			Custom Workflows
Discovery Events			Custom Tables
Vulnerabilities			Geolocation
Third-Party Vulnerabilities			URL
Incidents			Whois
Users			Contextual Cross-launch
Active Sessions			
Users			Search
User Activity			
Indications of Compromise			

2. In the upper right corner select **Go Live**

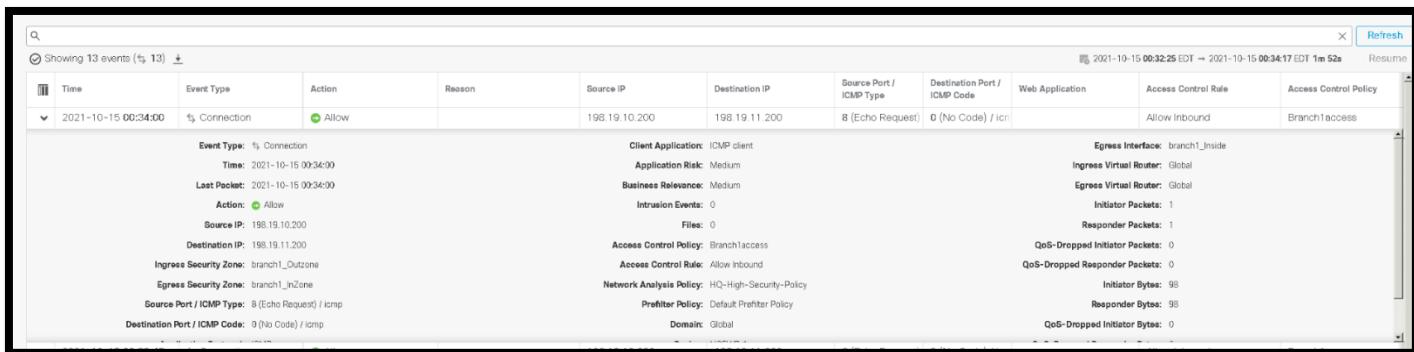
3. Wait a few seconds for the log to populate

- a. Select a Line in the Log



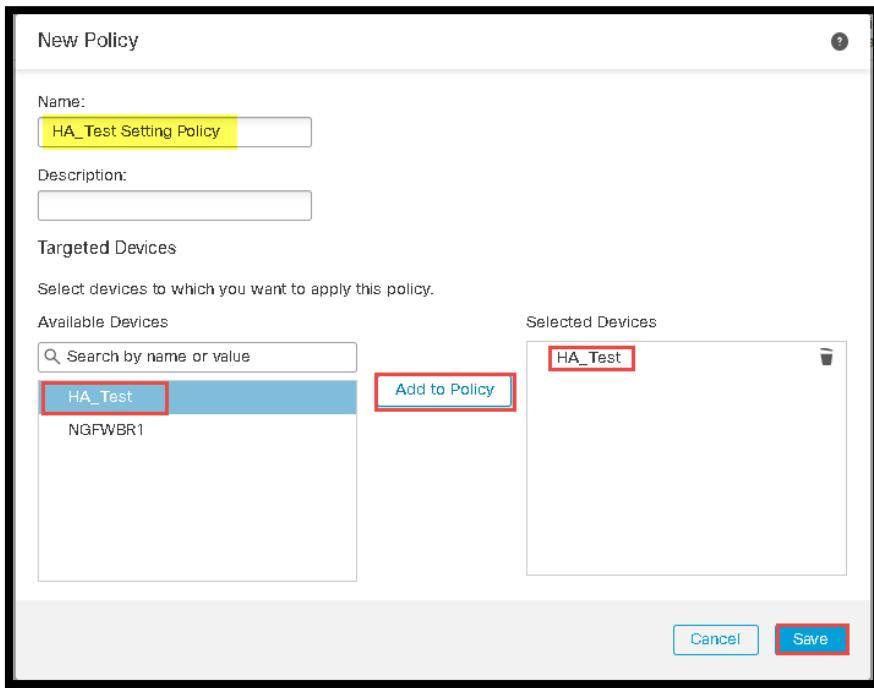
Unified Events										
Event Type		Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy
2021-10-15 00:33:15	ts Connection	Allow		198.19.10.200	198.19.11.200	8 (Echo Request)	0 (No Code) / icmp		Allow Inbound	Branch1access
2021-10-15 00:33:00	ts Connection	Allow		198.19.10.200	198.19.11.200	8 (Echo Request)	0 (No Code) / icmp		Allow Inbound	Branch1access
2021-10-15 00:32:45	ts Connection	Allow		198.19.10.200	198.19.11.200	8 (Echo Request)	0 (No Code) / icmp		Allow Inbound	Branch1access
2021-10-15 00:32:30	ts Connection	Allow		198.19.10.200	198.19.11.200	8 (Echo Request)	0 (No Code) / icmp		Allow Inbound	Branch1access
2021-10-15 00:32:29	ts Connection	Allow		198.19.10.82	52.21.117.50	46384 / tcp	443 (https) / tcp	Web Browsing	Allow Outbound	Base_Policy
2021-10-15 00:32:20	ts Connection	Allow		198.19.10.120	52.70.61.174	37880 / tcp	443 (https) / tcp	Web Browsing	Allow Outbound	Base_Policy
2021-10-15 00:32:15	ts Connection	Allow		198.19.10.200	198.19.11.200	8 (Echo Request)	0 (No Code) / icmp		Allow Inbound	Branch1access
2021-10-15 00:32:00	ts Connection	Allow		198.19.10.200	198.19.11.200	8 (Echo Request)	0 (No Code) / icmp		Allow Inbound	Branch1access

b. Note the information contained in the Log

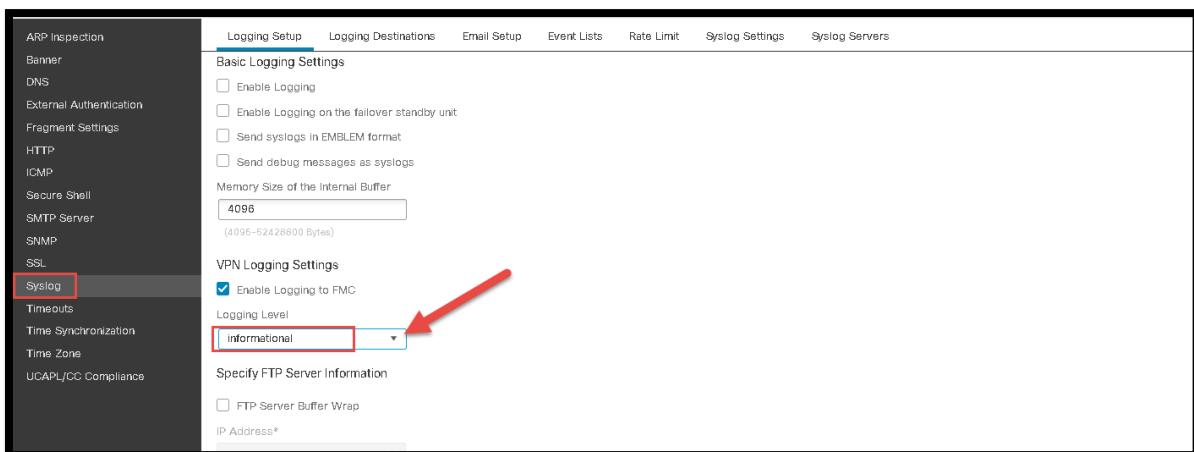


Unified Events										
Event Details										
2021-10-15 00:34:00	ts Connection	Allow		198.19.10.200	198.19.11.200	8 (Echo Request)	0 (No Code) / icmp		Allow Inbound	Branch1access
Event Type: ts Connection Time: 2021-10-15 00:34:00 Last Packet: 2021-10-15 00:34:00 Action: Allow Source IP: 198.19.10.200 Destination IP: 198.19.11.200 Ingress Security Zone: branch1_Outzone Egress Security Zone: branch1_InZone Source Port / ICMP Type: 8 (Echo Request) / icmp Destination Port / ICMP Code: 0 (No Code) / icmp										
Client Application: ICMP client Application Risk: Medium Business Relevance: Medium Intrusion Events: 0 Files: 0 Access Control Policy: Branch1access Access Control Rule: Allow inbound Network Analysis Policy: HQ-High-Security-Policy Profilter Policy: Default Profilter Policy Domain: Global										
Egress Interface: branch1_Inside Ingress Virtual Router: Global Egress Virtual Router: Global Initiator Packets: 1 Responder Packets: 1 QoS-Dropped Initiator Packets: 0 QoS-Dropped Responder Packets: 0 Initiator Bytes: 98 Responder Bytes: 98 QoS-Dropped Initiator Bytes: 0										

4. In the FMC, navigate to **Device > VPN > Troubleshooting**. Note that no records are displayed.
5. In the FMC, navigate to **Devices > Platform Settings**.
 - a. Modify Existing Platform Settings or Click New Policy **Threat Defense Settings Policy**.
 - b. Name the policy HA_Test Settings Policy.
 - c. Select the HA_Test [or NGFW1] device, and **click Add to Policy**.
 - d. **Click SAVE**



6. Click **Save**. Wait for the policy to open for editing.
7. In the left navigation pane, select **Syslog**.
 - a. Under **VPN Logging Settings** change the logging level to **informational**. Note that in a production environment, it is recommended that you set this to errors or alerts.
 - b. Click **Save**.



8. Deploy the changes to the **HA_Test**
9. On the Outside-PC, generate some VPN activity. For example, connect and disconnect a VPN session.

10. In the FMC, return to **Device > VPN > Troubleshooting**. You should see records. If you do not, try adjusting the time window on this page.
11. On the **NGFW1** CLI run some of the following commands to get a rough scope of the troubleshooting capabilities. These are useful when troubleshooting RA VPN. They are primarily included for your reference.
 - a. show vpn-sessiondb ?
 - b. test aaa-server ?
 - c. debug crypto ca ? (good for trouble-shooting certificate issues)
 - d. debug crypto ipsec ?
 - e. debug ldap ?
 - f. debug aaa ?

FDM Deployment Troubleshooting

1. Open the Firefox browser click on the FDM Tab.
2. Click **Device > Routing >View Configuration**
3. Move to **Actions Column**
4. Click on the **pencil** icon on Line #1
5. Click on the **Dropdown Arrow** by Gateway
6. Select **Create New Network Object**
 - a. Name: **tsroute**
 - b. Host: **198.18.133.82** click **OK**
7. For Gateway select the newly created gateway: **tsroute**
8. For Interface select: **outside**
9. Click **OK**
10. Click **Deploy**
11. Wait for the Deployment to finish
12. You will see a **Status** of **Failed**
13. Click the see details

The screenshot shows the Cisco dCloud interface with the title bar "Event Type = Deployment Event". Below it, a message box displays an error: "Deployment Failed: User (admin) Triggered Deployment" with the sub-error "ERROR: Invalid next hop address 198.18.133.82, it matches our IP address Config Error -- route outside 0.0.0.0 0.0.0.0 198.18.133.82 1". The main table below lists deployment details:

Event Type	Deployment Event
User	admin
Source IP	SYSTEM
Entity ID	d69bb99d-fcf8-11ea-b32c-bb4980c7078d
Entity Name	User (admin) Triggered Deployment
Entity Type	Deployment Schedule
Time Stamp	2020, 22 Sep 17:29:10
Status	FAILED

This screenshot is identical to the one above, showing the same deployment event failure message and detailed deployment information table.

14. You will see an error that references the next hop address

- Go back to the FDM and fix the issue

Troubleshooting with Packet Tracer and Packet Capture

1. When to use Packet-Tracer

- Verify if traffic to a specific port is allowed by the Lina Data path and Snort
 - Security Intelligence (IP Reputation)
 - L3/L4 IPS Intrusion Rules
- Packet Tracer **Does Not** currently work with: (Because it cannot emulate a L7 packet)
 - Identity-based rules
 - L7-related (SI DNS/URL, App ID, File Policy, L7 Intrusion Rules)

Packet-Tracer Lab

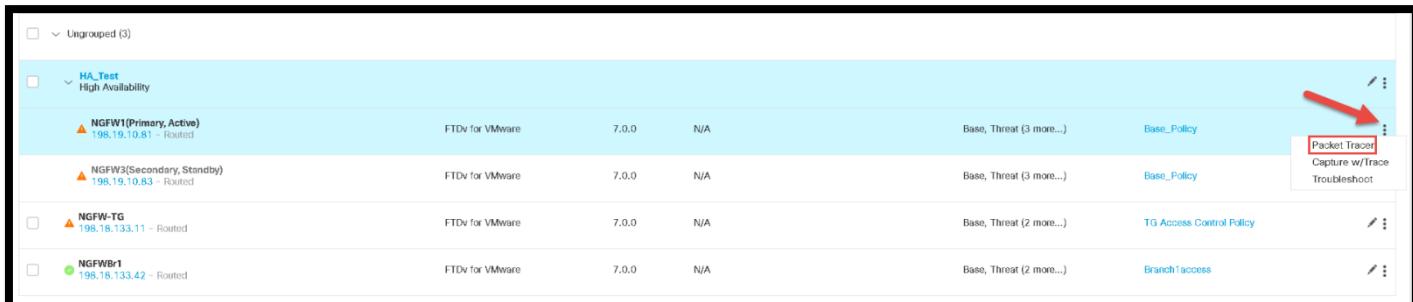
1. On the FMC go to **Policies > Access Control > Edit the Base_Policy**
2. Click Add New Rule
 - a. Name: Packet-Trace Rule
 - b. Set the Rule ABOVE rule 1
 - c. Under Action Block or Block with reset
 - d. Zones: Source Zone InZone1, Destination Zone Outzone
 - e. Networks: Source: MainOfficenetwork Destination Networks: any-ipv4
 - f. Dest Ports: ICMP, HTTPS, FTP click Add to Rule
 - g. Click Logging
 - i. Click Log at Beginning of Connections
 - i. Click **Add**
 - j. Click **Save and Deploy to HA_Test or [NGFW1]**

NOTE: We selected all the applications related to **ICMP and FTP** in a production environment you would be more specific with what particular applications you are blocking.

3. Open a PUTTY Session to **NGFW1** Username: **admin** Password **C1sco12345**
4. Type the following **packet-tracer input in10 icmp 198.19.10.200 8 0 198.18.133.200**
 - a. Look at Phases you will notice that the packet has been handed off to SNORT for further processing
 - b. You will see that SNORT used block w/reset a rule id to order a drop of the packet.
5. Repeat **packet-tracer** with HTTPS and FTP

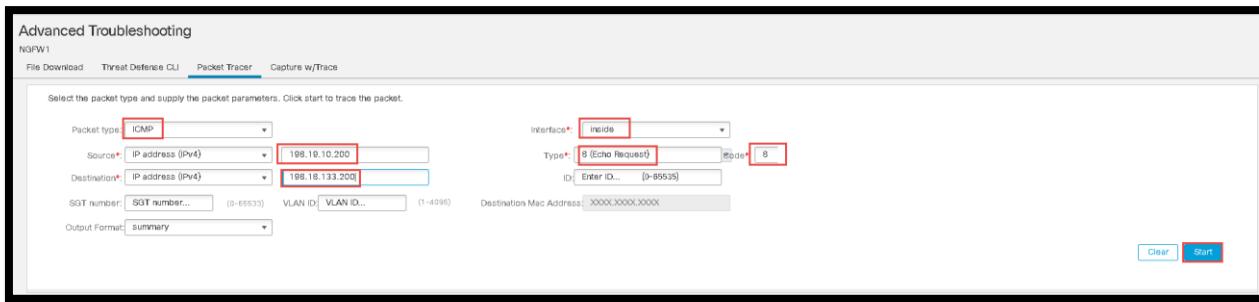
Now look at the Packet-Trace command in the FMC

6. Go to **Devices > Device Management.> NGFW1** click on the **Three Dots**



Device Management					
Device	Type	Version	Threat Level	Policy	Action
HA_Test	High Availability				
NGFW1(Primary, Active) 198.19.10.81 - Routed	FTDv for VMware	7.0.0	N/A	Base, Threat (3 more...)	Base_Policy
NGFW3(Secondary, Standby) 198.19.10.83 - Routed	FTDv for VMware	7.0.0	N/A	Base, Threat (3 more...)	Base_Policy
NGFW-TG 198.18.133.11 - Routed	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	TG Access Control Policy
NGFWB1 198.18.133.42 - Routed	FTDv for VMware	7.0.0	N/A	Base, Threat (2 more...)	BranchAccess

7. Click Packet Tracer



- a. Packet Type: **ICMP**
- b. Interface: **in10**
- c. Source: **198.19.10.200**
- d. Type: **8 (Echo Request) Code 0**
- e. Destination: **198.18.133.200**
- f. Click **Start**

NOTE: You will get the same results that you saw in the Command Line of the **NGFW1** it is just shown in the window.

8. Set up the Packet Tracer for **FTP**

- a. Packet Type: **TCP**
- b. Source: **198.19.10.200**
- c. Source Port: **1111**
- d. Destination **198.18.133.200 (Outside Linux Server)**
- e. Destination Port: **FTP**
- f. Click **Clear**
- g. Click **Start**

9. Use Packet Tracer to test HTTP traffic from 198.19.10.200 to 198.18.133.200 Interface in10, Source port 1111 Destination Port 80

- a. What Rule is matched?
- b. What is the Verdict?

Capture w/Trace Lab

NOTE: There are two types of Traffic Captures the **Lina based** and the **Snort based**.

1. Line Level **capture**
2. SNORT Level **capture-traffic**

Edit Capture: Capturewtrace

Name:	Capturewtrace	Interface:	inside
Match Criteria:			
Protocol:	ICMP	Source Host:	198.19.10.200
		Source Network:	255.255.255.255
Destination Host:	any	Destination Network:	
<input type="checkbox"/> SGT number: 0 <small>(0-65535)</small>			
Buffer:			
Packet Size:	1518	14-1522 bytes	
Buffer Size:	33554432	1534-33554432 bytes	
<input type="radio"/> Continuous Capture <input checked="" type="radio"/> Stop when full <input checked="" type="checkbox"/> Trace Trace Count: 100			
<input type="button" value="Cancel"/> <input type="button" value="Save"/>			

3. Go to **Devices > Device Management** > click on the Three dots for **NGFW1**
4. Click on **Capture w/Trace**
5. Click **Add Capture**
 - a. Name: Capturewtrace
 - b. Interface: in10
 - c. Protocol: ICMP
 - d. Source Host: 198.19.10.200 (Inside Linux Server)
 - e. Destination Host: any
 - f. Buffer Size: 33554432 (32 MB)
 - g. Trace Count 100
 - h. Save

NOTE: We have not removed the access policy denying ICMP so the pings will fail, but you will be able to see the packet shown. Also you will export the file in PCAP format to **Wireshark** in this lab.

6. Go to the Jump PC and on the Inside Linux Server type **ping outside**.
7. If you don't see information in the Packets Shown Window in about 10 seconds hit the refresh.
8. **Once you see packets stop the ping.**
9. Click on the Save icon for the packet capture you created.
 - a. Save the file as PCAP.
10. When Prompted **Save File** and click **OK**.
11. Go to the downloads arrow of Firefox and select the file just downloaded.



12. Minimize the Browser and you will see the file opened in **Wireshark**.
13. Notice that the messages have been **administratively filtered**.
14. Remove the Packet Tracer rule from the Base_Policy
15. Save and Deploy

Scenario 9. PxGrid 2.0 Remediation with ISE using ANC

Introduction

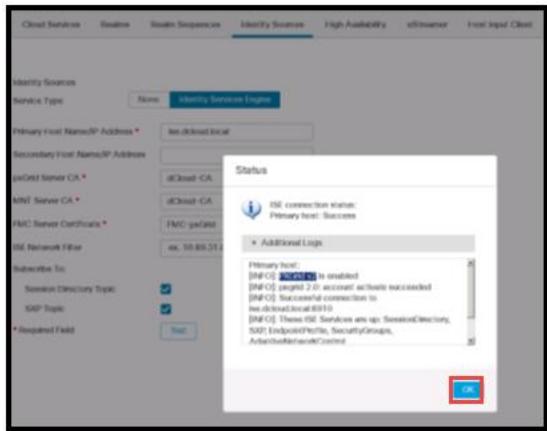
Cisco Secure Firewall Management Center uses PxGrid 1.0 protocol for integration with ISE. FMC obtains identity information from ISE, such as User-IP mappings, User-SGT/IP-SGT mappings, SXP mappings and endpoint profiles using the communication protocol. Starting with release 6.7 the communication protocol for integration from PxGrid 1.0 to 2.0. PxGrid 2.0 offers additional scale benefits for ISE, and enhances High-Availability connectivity to ISE. PxGrid 2.0 supports Adaptive Network Control (ANC) remediation. ANC now replaces Endpoint Protection Services (EPS), which is used for controlling and monitoring network access of endpoints.

Objectives

- Validate that PxGrid 1.0 protocol is updated to PxGrid 2.0
- Reconfigure EPS remediation to ANC
- Quarantine endpoint through FMC and ISE integration using ANC and PxGrid 2.0.

Integration of FMC and ISE using PxGrid 2.0 Protocol

1. Login into FMC admin/C1sco12345
2. Go to System > Integration > Identity Sources > Identity Services Engine and select **Test** button to validate connectivity to the ISE System
3. Expand **Additional Logs** to see details of FMC and ISE connectivity and the Click **OK**



4. Open a new tab on the Firefox browser and click **ISE** bookmark from the ribbon **admin/C1sco12345**
5. Navigate to **Administration > PxGrid Services > All Clients** notice that the FMC Client is in Offline status.

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

Enable Disable Approve Group Decline Delete Refresh Total Pending Approval(0)

Client Name	Description	Capabilities	Status
ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)
ise-mnt-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)
ise-admin-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)
ise-fanout-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)
ise-bridge-ise		Capabilities(0 Pub, 5 Sub)	Online (XMPP)
ia-fmc.dcloud.local-2ca6fc78		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)
fmc-c108ad6c339411e9aebaa0...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)
st-fmc.dcloud.local-2ca6fc78		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)
fdm-f9adff63e5611e9934fc1c8...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)
t-fmc-c108ad6c339411e9aebaa...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)

Note: PxGrid 2.0 is using REST and WebSocket protocols. Connections from PxGrid 2.0 appear under **Administration > PxGrid Services > Web Clients**

Client Name Connect To Session Id Certificate Subscriptions Publications IP Address Status

ise-fanout-ise	ise	ise:0	CN=ise.dcloud.l...	/topic/wildcard	127.0.0.1	ON
ise-admin-ise	ise	ise:2	CN=ise.dcloud.l...		198.19.10.130	ON
ise-mnt-ise	ise	ise:3	CN=ise.dcloud.l...	/topic/com.cisco.ise.s... /topic/com.cisco.ise.s...	198.19.10.130	ON
fmc-c108ad6c339411e9aebaa0...	ise	ise:4	CN=fmc.dcloud.l...	/topic/com.cisco.ise.s...	198.19.10.120	ON
ise-bridge-ise	ise	ise:5	CN=ise.dcloud.l...	/topic/com.cisco.ise.co...	127.0.0.1	ON
ise-fanout-ise	ise	ise:6	CN=ise.dcloud.l...	/topic/distributed	198.19.10.130	ON
fdm-f9adff63e5611e9934fc1c8...	ise	ise:8	CN=ngfw.dcloud...	/topic/com.cisco.ise.s...	198.19.10.82	ON

6. On ISE create an Adaptive Network Control (ANC) policy for assignment to an endpoint
 - a. **Operations > Adaptive Network Control > Policy List**
 - b. Click **Add**
 - c. Name: **quarantine_anc_policy**
 - d. Action: **QUARANTINE**
 - e. Click **Submit**

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations (highlighted with a red box), Policy, Administration, RADIUS, Threat-Centric NAC Live Logs, TACACS, Troubleshoot, Adaptive Network Control (highlighted with a red box), and Reports. Below the navigation is a sub-menu with Policy List (highlighted with a red box) and Endpoint Assignment. The main content area displays a 'List > New' screen for creating a policy. It requires input fields: Name * (containing 'quarantine_anc_policy') and Action * (containing 'x QUARANTINE'). The 'Submit' button is highlighted with a red box. A note at the top states: 'Input fields marked with an asterisk (*) are required.'

Configure ANC instance and assign to Correlation Policy on FMC

- FMC Policies > Actions > Instances review the existing configuration with an EPS instance configured

Note: The module name “pxgrid-mitigation” which is using PxGrid 1.0. We will add a PxGrid 2.0 module and then delete the “pxgrid-mitigation” module. You will not see this error right now because the Class image has the ISE Connector disabled in the Health policy. You will enable it in a later step.

The screenshot shows the Firepower Management Center (FMC) interface. The top navigation bar includes links for Overview, Analysis, Policies (highlighted with a blue underline), Devices, Objects, AMP, and Intelligence. Below the navigation is a sub-menu with Policies / Actions / Instances. The main content area displays a table titled 'Configured Instances' with one entry: Instance Name 'pxgrid-mitigation', Module Name 'pxGrid Mitigation', and Version '1.0'. Below the table is a section for 'Add a New Instance' with a dropdown menu 'Select a module type' set to 'Cisco IOS Null Route(v1.0)' and a 'Create' button.

- Add a New Instance **Select a module “pxGrid Adaptive Network Control (ANC) Policy Assignment(v1.0)”**
 - Click **Add**
 - Instance Name: quarantine_source_anc
 - Click **Create**
 - Configured Remediations add a new remediation of type: **ANC Policy for Source** click **Add**
 - Remediation Name: quarantine_source_anc
 - ANC Policy: quarantine_anc_policy (this was configured in ISE)
 - Click **Create and Save and Done**

Success
Created new remediation
quarantine_source_anc

Edit Remediation

Remediation Name: quarantine_source_anc
Remediation Type: ANC Policy for Source

Description: [Empty input field]

ANC Policy: quarantine_anc_policy ▾

Allow List (an optional list of networks): [Empty input field]

Done Cancel Save

3. FMC Policies > Correlation > Policy Management
4. Edit CorrelationPolicy – Malware Detection
 - a. Policy Rules select the **Responses** button

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information

Policy Name: CorrelationPolicy
Policy Description: [Empty input field]
Default Priority: None ▾

Cancel Save

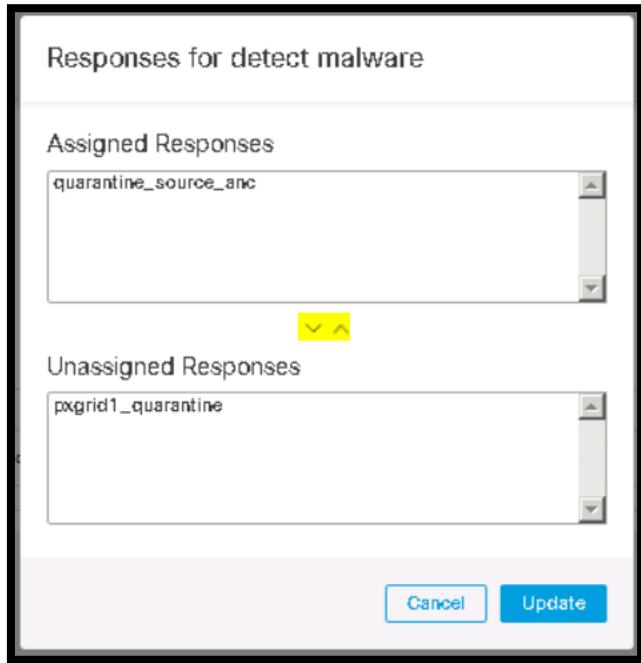
Policy Rules

Rule	Responses	Priority
DetectMalware	quarantine_source_anc (Remediation)	Default ▾

Add Rules

"Responses" button

- b. Changed Assigned responses from pxgrid1_quarantine to quarantine_source_anc using the arrows and **Update**



c. Save

5. FMC System > Health > Policy >
- Edit the Initial_Health_Policy
 - On the left panel select ISE Connection Status Monitor
 - Click Enabled: On
 - Click Save Policy and Exit

Note: The default setting is on but was disabled as part of the Class Image.

iii. Click on Apply

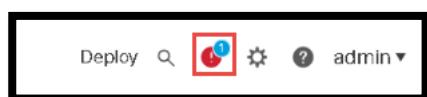
Policy Name	Domain	Applied To	Last Modified
Initial_Health_Policy 2020-11-20 21:02:54 Initial Health Policy	Global	3 appliances 3 out-of-date	2021-10-11 02:53:00 Modified by 'admin'

iv. Select All and Apply

Note: you have reconfigured the EPS module to ANC but you will now have the Health Monitoring Alerts. The below error messages should show up in 5 minutes.

FMC ISE Connection Status Health Monitor

1. FMC click the **Notification Button** to see the health warning about an EPS configuration that need to be replaced by ANC



The screenshot shows the FMC dashboard with the following details:

- Deployments**: 3 total
- Health**: 1 critical (ISE Connection Status)
- Tasks**: 0 errors
- Show Notifications** toggle switch is on.
- Filter** search bar.
- Firepower Management Center** section: fmc.dcloud.local
- ISE Connection Status**: EPS Remediations currently in use will not work with the current pxGrid connection to ISE. Please change your correlation policy to use ANC Remediations.

6. FMC go to **Policies > Instances**
 - a. Delete the pxgrid-mitigation module
7. Health Monitoring errors should resolve.

Test the Configuration

1. On the Jump PC go to **Desktop > RADIUS Simulator** and run the following two scripts:
 - a. RadiusListener
 - b. StartSessions
2. Jumphost open the **Remote Desktops** folder and launch Wkst1 (IP address: 198.19.12.21 admin/C1sco12345)
 - a. From Wkst1 Desktop open User folder and choose **NGFW1 is your gateway** folder and run the script **Dilbert (Engineering)** This will simulate logging into the Network
 - b. Wkst1 open a Firefox browser, it should launch the outside web server (198.18.133.200) automatically
 - i. Go to **Files** hyperlink and try to download the **Zombies.pdf** file. The connection should reset and trigger a malware event that the FTD will catch.
 - c. FMC Analysis > Files > Malware Events

Malware Summary						Table View of Malware Events	
Jump to...							
	<input type="checkbox"/> Detection Name	File Name	File SHA256	File Type	Count		
▼	<input type="checkbox"/> W32.Zombies.NotAVirus	Zombies.pdf	00b32c34...989bb002	PDF	1		

Note: This should also trigger a correlation event and quarantine the host

- d. FMC Analysis > Correlation > Status

Table View of Remediations					
Jump to...					
	<input type="checkbox"/> Time ×	Remediation Name ×	Policy ×	Rule ×	Result Message ×
▼	<input type="checkbox"/> 2020-10-20 17:39:47	quarantine_source_anc	CorrelationPolicy	DetectMalware	Successful completion of remediation

- e. From ISE
 - i. Operations > Adaptive Network Control > Endpoint Assignment

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy (which is selected), Administration, and Work Centers. Below the navigation is a secondary menu with links for RADIUS, Threat-Centric NAC Live Logs, TACACS, Troubleshoot, Adaptive Network Control, and Reports. The main content area is titled "List" and displays a table of endpoint assignments. The table has columns for MAC address, Policy Name, and Policy Actions. One entry is visible: a MAC address of 08:FD:0E:FE:3C:48 is assigned to a policy named "quarantine_anc_policy" with an action of "[QUARANTINE]".

MAC address	Policy Name	Policy Actions
08:FD:0E:FE:3C:48	quarantine_anc_policy	[QUARANTINE]

3. If you would like to test another click on **Default** and then **Harry** recheck **ISE**

Scenario 10. TLS/SSL Decryption

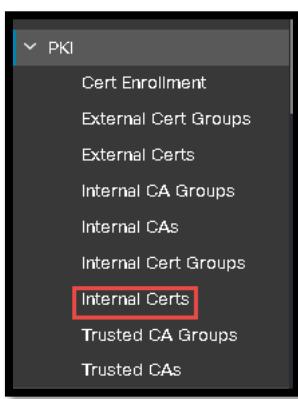
In this scenario you will be configuring SSL Decryption with a Known Key, Decryption with a Resign of the key and SSL Decryption with Additional Rules.

Steps

Import Certificates for Known Key

You will configure the FMC to decrypt traffic to and from the DMZ web server. You will need the certificate and private key of the web server to create an object in the FMC to use for an SSL rule. Once you create the object you will also create the SSL policy , rules, and configure the ACP

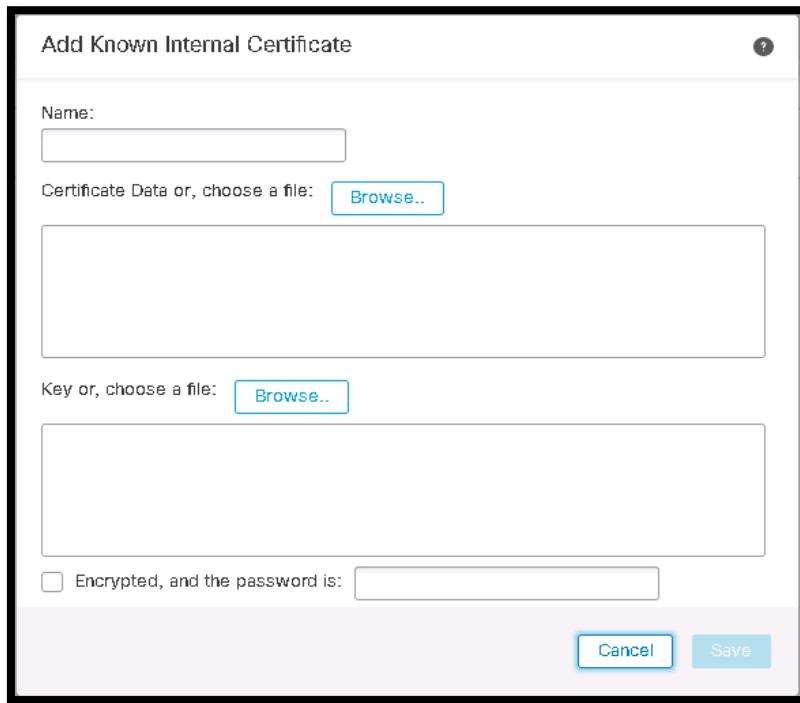
1. Login to the FMC
 - a. **Devices > NAT > Default PAT**
 - i. Add a NAT Rule
 1. NAT rules Before
 2. Interface Objects:
 - a. Source: InZone1
 - b. Destination: OutZone
 - c. Translation Create Original Source: wwwinssl (198.19.10.220)
 - d. Translation Create Original Destination: wwwoutssl (198.18.134.220)
 - e. Click **OK**
 - f. Click **Save**
 2. **Policies > Access Control > Base_Policy**
 - a. **Add or Modify a rule to allow outside connectivity from Outzone to Inzone1**
 - i. Destination network wwwinssl
 - ii. Make sure to add Demo Intrusion and File Policy
 - iii. Logging at the End of the Connection
 3. Go to **Object** menu and select **Object Management**
 4. Expand **PKI** and Select **Internal Certs** under the PKI object on the left



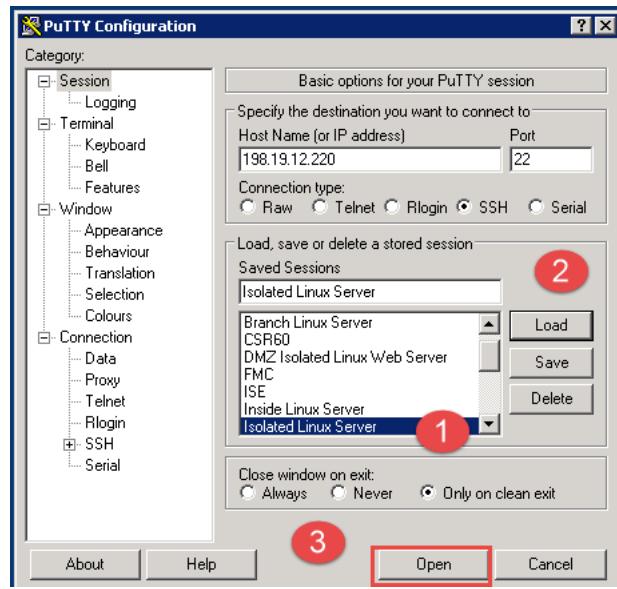
5. Click the **Add Internal Cert** button



6. The Add Known Internal Certificate window appears prompting for the certificate and private key data

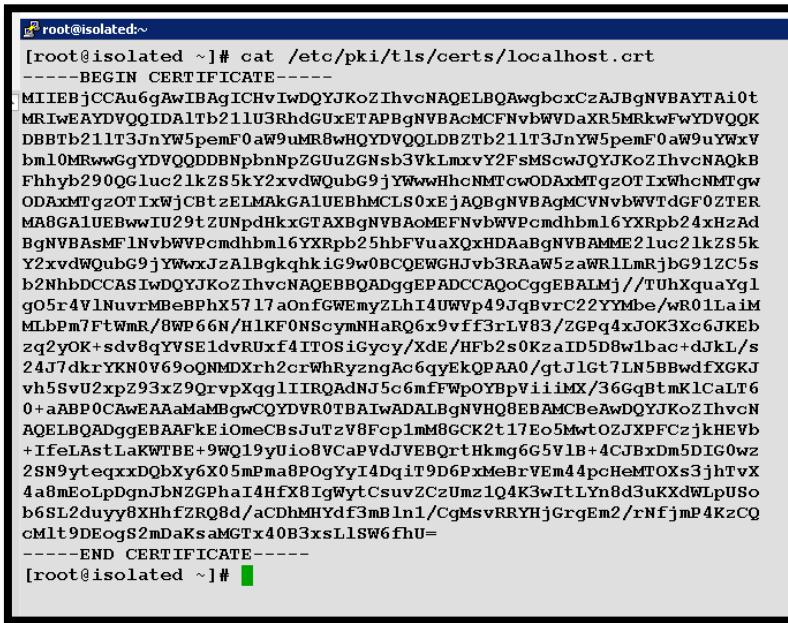


7. Configure the following:
 - a. Name: wwwinssl
8. Leave the window open and proceed back to the Jumpbox.
9. Open a Putty Session to the **Isolated Linux Server**



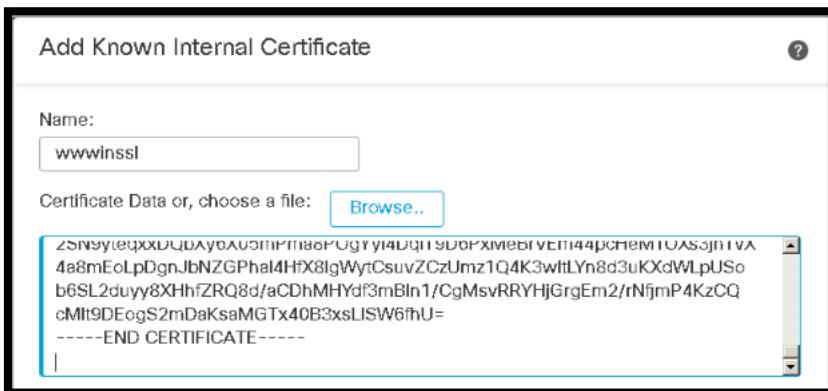
10. Login **root/C1sco12345**
11. Run the following command to display the contents of the certificate used by the DMZ webserver
 - a. cat /etc/pki/tls/certs/localhost.crt

12. Copy the output of the command by highlighting the text displayed beginning with “----BEGIN CERTIFICATE----” and ending with “----END CERTIFICATE----”



```
[root@isolated ~]# cat /etc/pki/tls/certs/localhost.crt
-----BEGIN CERTIFICATE-----
MIIEbjCCAU6gAwIBAgICHyIwDQYJKoZIhvcNAQELBQAwbcbxszAJBgNVBAYTAi0t
MRIwEAYDVQQIDA1tb21lU3RhdGUxEzAPBgNVBAcMCFNvBWWDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8whQYDVQQLDBZtb21lT3JnYW5pemF0aW9uYwXv
bml0MRwwGgYDVQDDBNpbNpZGUuZGNsh3VklmxvY2FsmScwJQYJKoZIhvcNAQkB
Fhyb290QGluc21kZS5kY2xvdWQubG9jYWwwHhcNMTCwODAxMTg2OTIxWhcNMTgw
ODAxMTg2OTIxWjC8t2eLMakGA1UEBhMCLS0xEjAQBgNVBAgMCVNVbWVfcdhbml6YXRpb24xHzAd
MA8GA1UEBwwIU29tZUNpdHkxGTAXBgNVBAoMEFNvbWVpcmdhbml6YXRpb24xHzAd
BgNVAasMF1NvbWVPcmdhbm16YXRpb25hbFFVuaxQxHDAaBgNVBAMME2luc21kZS5k
Y2xvdWQubG9jYWwxJzA1Bqkqhkig9w0BCQEWGHJvb3RAaw5zaWR1LmRjbG91ZC5s
b2NhbdCCASIwDQYJKoZIhvcNAQEBQADggEPADCCAQocCgEBAlMj//TUhXquaYg1
g05r4V1Nu vrMBeBPhX5717aOnfGWEmyZlhI4UVVp49JqBvrC22YYMbe/wR01LaiM
MLBpM7FtWmR/8WP6N/H1KF0NscymNHaRQ6x9vff3rLV83/ZGBq4xJOK3Xc6JKEb
zq2yOK+sdv8qYVSE1dvRu xf4ITOSiGycy/Xde/HFB2sOK2aID5D8w1bac+dJKL/s
24J7dkrYKN0V69oQNMDXrh2crWhRyzngAc6qyEkQPAA0/gtJlgt7LN5BBwdfxGKJ
vh5svu2xpZ93xZ9QrvpXqg1IIRQAdNj5c6mfFWpOYBpVi.iMX/36Gqb1mk1CaLT6
0+aABP0CAwEEAAmaMBgwCQYDVR0TBAIwADALBqNVHQ8EBAMCBerawDQYJKoZIhvcN
AQELBQAQdgEBAAFKeiOmeCbsJuTzv8Fcp1mM8GCK2t17Eo5MwtOZJXPFCzjkHEvb
+IfeLAstLaKWTBE+9WQ19yUi08VCaPVdJVEBQrtHkmqG6G5V1B+4CJBxDm5DIG0wz
2SN9yteeqxxDqbXY6X05mpma8POqYyI4DqiT9D6PxMeBrVEm44pcHeMTOxs3jhfvX
4a8mEoIpDgnJbNZGPhaI4Hfx8IgWytCsuvZCzUmz1Q4K3wltLyN8d3uKXdWLpUSo
b6SL2duyy8XHhfZRQ8d/aCd hMHYdf3mBln1/CgMsvRRYHjGrgEm2/rNfjmP4KzCQ
cMlt9DEogS2mDaKsaMGTx40B3xsL1SW6fhU=
-----END CERTIFICATE-----
[root@isolated ~]#
```

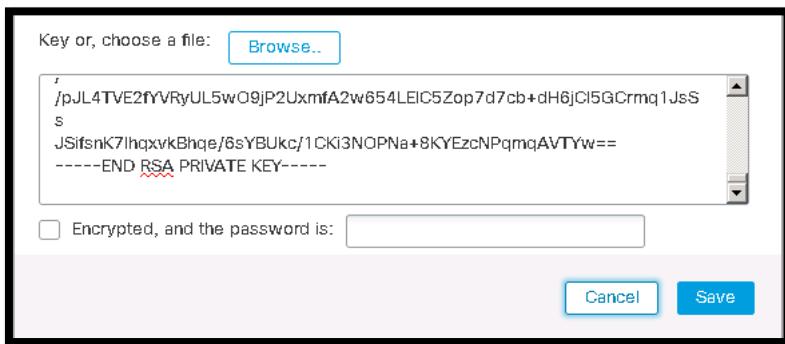
13. Return to the FMC
 14. Paste the contents of the certificate file into the **Certificate Data** field



15. Go back to the Putty session
 16. Run the following command
 a. cat /etc/pki/tls/private/localhost.key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAsyP/9NSFeq5piCWA7mvhWU26+swF4E+FfnuXto6d8ZYSbJku
EjhRZWnj0moG+sLbZhgx7/BHTUtqIwwts+bsW1aZH/xY/ro38eUoXQ1JzKY0dpF
DrH299/*estXzf9kY+rjEk4rrdzokoRvOrbI4r6x2/yphVITV29FTF/ghM5K1bJzL
9d0T8cVvazQrNogPkPzDVtpz50mQv+zbgnt2Stgo3RXr2hA0wNeuHZytafHLoeAB
zqrISRA8ADT+C0mua3ss3kEHB19cYom+H1K9TbG1n3fFn1Cu+leqCUghFAB00nlz
qZ8Vak5gG1WKKIx/faoaG2YqUJotPrT5oAE/QIDAQABAoIBAQCAgmTN19+hYJko
J+9UGmPwkoh9/fqBLcrQL41oUusPMd9jtKGORIRvwgTDH3ieT0bg+j5B+PdqIon8
jYUsv8YrBA2CZx4d4RNJ5XzETf8LfYqPkItVvwkz7I9vr3gc0PrQcdfjGA1DyJwa
Tz528JE1xQ0gg6CK5zgb1xCk81+uBE8jPlyCfu0QM63Fq6ath6d5V85nPnZQ/fq
UqydyHTYVjw5iu5ShnQvoHwQILwxVu1je1AVf5G6vW59RtAKF9PAZabbG73Qg56x
OnhoICHoZXZOQWOB74atnylayaQ/BM1uJWAipD1+tTkywPVHU1S3/
D6U31hcBAoGBANyM5B46bh2CC42Vwc7H202tLtp33ziFvCq1Pwvo1kdGy573OHBF
S1UEqr77U0xhP7Q5nRqFIBZhoIjpXZhdY5hI+Zde8IB9SRbD4ujImWmRzbBI8gZ6
DPaiaPyDnJKAhHL62M9jFNFViX1W/G5Ar61E1UryMibIxH2+ZTImpx1hAoGBAM/v
MwiIC3tCnhXChp2i4+Yk0fueF7wojZld0Ba2OgTa2E7fmYF6Xtam7LyvtY9VxehK
PcP+GyYoN4JqkgSxgPmu6Hr0DlyLc41j7K1CHQs+eWg3f86jCDczUGfjzqsX1Nq0
ikUtPjP804K3kSlnYf8+s/92+iVRcPwspcvb1EdAoGBALUjuk/haYMuxdJZhZ4Q
Alw+utaP0XQY0ry487kSWLdt+st3Nr17q35sUr+HCIFNHS/RPr9D6eSM01/cXGs
chonBwd/gEPnolnINME/0FBWgfshTj2nk7IVHekXj0dj6mSNBfj+xaWnKi8ZfGYJ
Fr0NKRj05sXX6xnjgDW6bVLBAoGAC0ULnwraLI2nw8YhoqmRcIfOWVqoLqqEAivz
e0e1HV4/GwdDaqEXQssJSbC8XPRpJY3gix7amdbUK11bTKXSN7YjI4bWwG1OdftU
eFF8+v8H1X4syyaG63b8hKT0LpG8F55xYA5zSj2bHBqW44eW6B6d4tqv9BXV6bgR
H1MkZIEcgYBzzBvJbCH77V8XvNjYIs7lqszkQo9wuLnZ7PcYQPR4GKgDCuKeBF4/
/pJL4TVE2fYVRYuL5w09jp2Uxmfa2w654LE1C5Zop7d7cb+dH6jC15GCrmq1JsSs
JSifsnK7lhqxvkBhqe/6sYBUkc/1CKi3NOPNa+8KEYEzcNPqmqAVTYw==
-----END RSA PRIVATE KEY-----
```

17. Copy the output of the command by highlighting the text displayed beginning with “-----BEGIN RSA PRIVATE KEY-----” and ending with “-----END RSA PRIVATE KEY-----”
18. Return to the FMC
19. Paste the contents of the key file into the **key** field



20. Ensure the password field is blank
21. Click the **Save** button. You will now create the SSL Policy

Create SSL Policy

1. Click the **Policies** menu and select **SSL**
2. Select **New Policy**
3. Configure the following:
 - a. Name **Corp HQ-SSL-Policy**
 - b. Description: **SSL Policy for Corp HQ**
 - c. Default Action: **Do not decrypt**
 - d. Click **Save**

New SSL Policy

Name: CorpHQ-SSL-Policy

Description: SSL Policy for Corp HQ

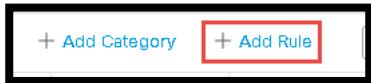
Default Action:

- Do not decrypt
- Block
- Block with reset

Cancel Save

NOTE: The Default Action is what the SSL policy will do if no rules match

4. You will now create a rule to decrypt traffic targeted at the DMZ web server. Click **Add Rule**



5. Configure the following:
 - a. Name: **Decrypt wwwinssl**
 - b. Action: **Decrypt – Known Key**
 - c. Insert: **into Category: Standard Rules**

Add Rule

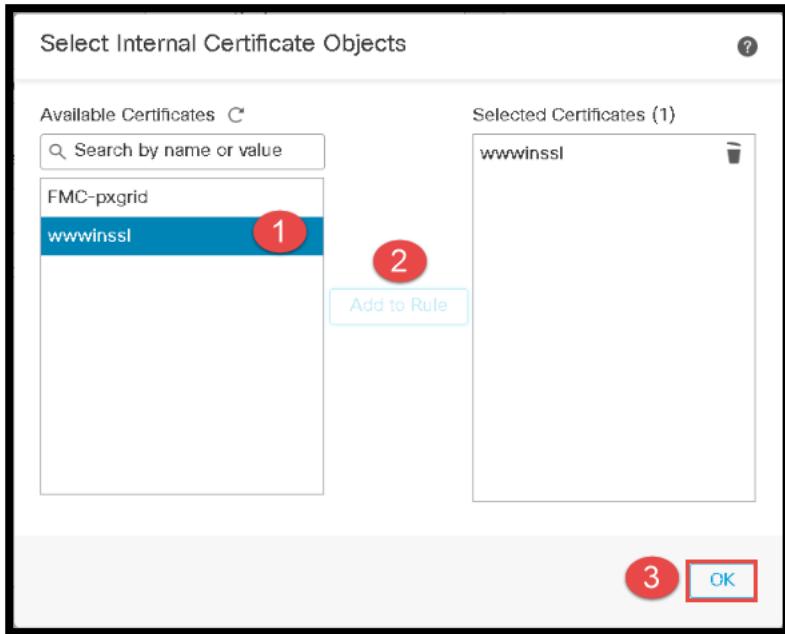
Name: Decrypt wwwinssl

Enabled

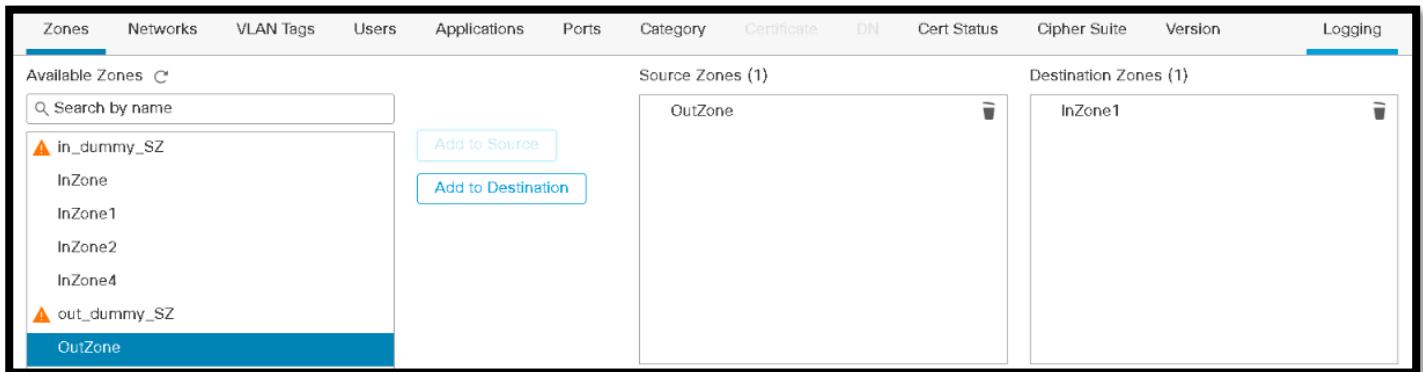
Insert: Standard Rules

Action: Decrypt - Known Key

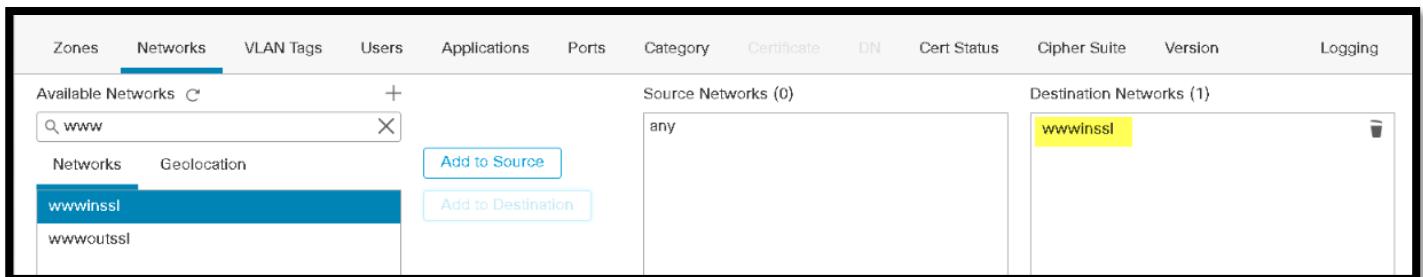
6. Next to the Action field, click in the field labeled **Click to select decryption certs**
7. Select Internal Certificate Objects window appears. Select the wwwinssl certificate object that you created earlier, click the **Add to Rule** button, and click **OK**



8. On the Zones tab select **InZone1**ne and click **Add to Destination**. Select **OutZone** objects and click **Add to Source**



9. Click the **Networks** tab select the **wwwinssl** object, and click **Add to Destination**



10. Click the **Ports** tab, and select **HTTPS**, and click the **Add to Destination** button
 11. Click the **Cert Status** tab and review the options but do not make any changes. Notice that there are many criteria to control the behavior of encrypted traffic through the FTD

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status
Revoked:	Yes	No	Any		Self Signed:	Yes	No	Any	
Valid:	Yes	No	Any		Invalid Signature:	Yes	No	Any	
Invalid Issuer:	Yes	No	Any		Expired:	Yes	No	Any	
Not Yet Valid:	Yes	No	Any		Invalid Certificate:	Yes	No	Any	
Invalid CRL:	Yes	No	Any		Server Mismatch:	Yes	No	Any	

12. Click **Logging** tab and select **Log at End of Connection**

13. Click **Add**

14. Click the **Save** button to save changes to the policy

Configure ACP

The SSL Policy has been configured but has yet to be attached to an ACP.

1. Click **Policies > Access Control> Base_Policy**
2. Click **Advanced > SSL Policy Settings and the Pencil Icon to Edit**

SSL Policy Settings

SSL Policy to use for inspecting encrypted connections

None

3. Choose the **CorpHQ-SSL-Policy** object and click **OK**

SSL Policy to use for inspecting encrypted connections

CorpHQ-SSL-Policy

Revert to Defaults Cancel OK

4. Click **Rules**

5. Locate the rule that you used for the Inbound SSL Connectivity and edit the rule

6. Configure the Following:

- Intrusion Policy: **HQ-High-Security-Policy**
- Variable Set: **ExternalTraffic**
- File Policy: **HQ File Policy**
- Click **Save**

Intrusion Policy

HQ-High-Security-Policy

Variable Set

External_Traffic

File Policy

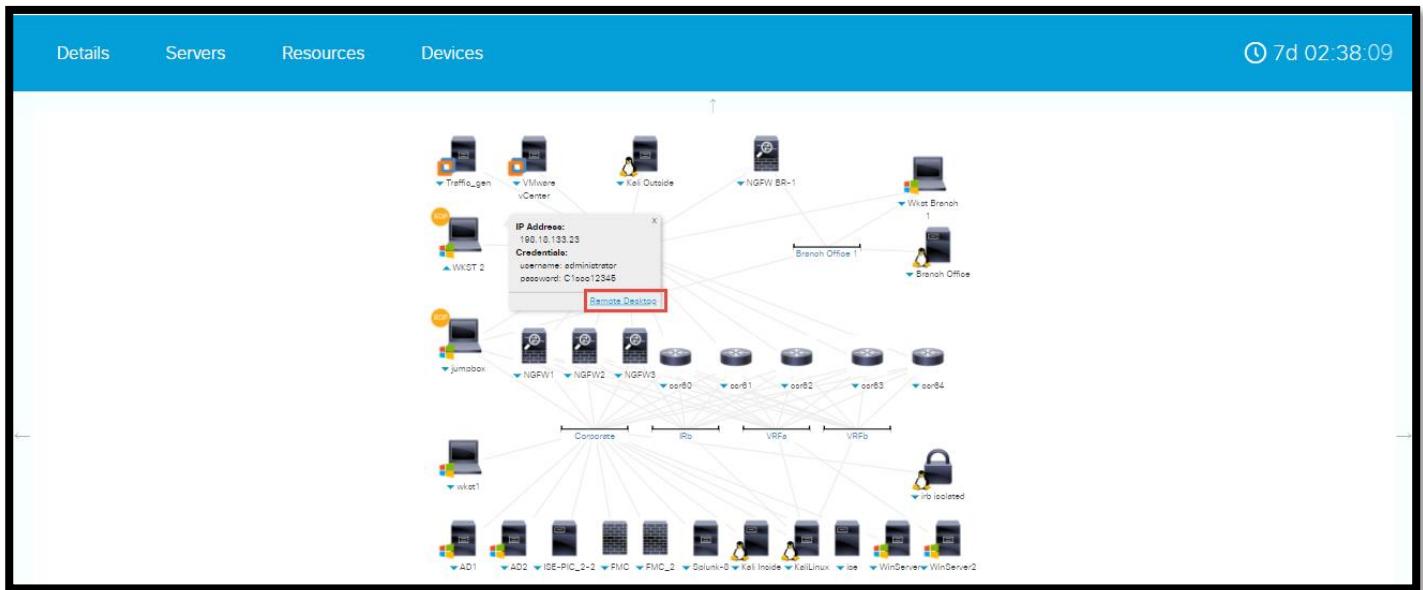
HQ File Policy

7. Click **Save** for the **Base_Policy** and Deploy

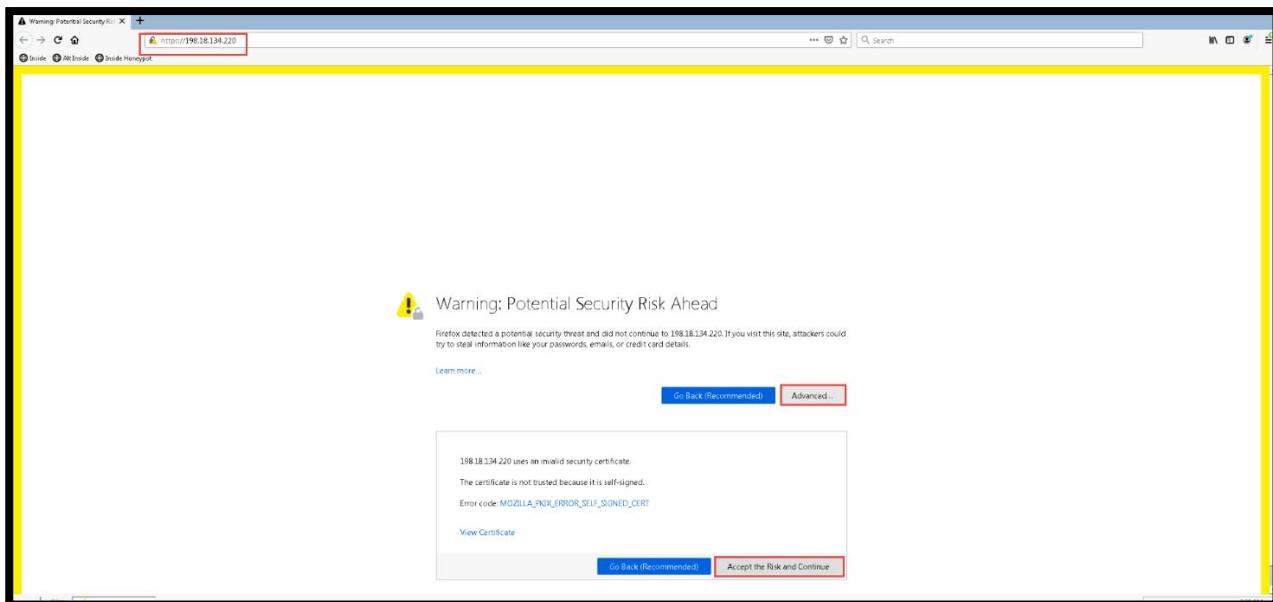
Test SSL Policy

You will now test the SSL policy from WKST2 to see if the policy is working.

1. Go to the dCloud session page in the computer's web browser, and find the **WKST2** machine arrow and then select **Remote Desktop**



2. Open the **Firefox** web browser by double-clicking on the shortcut on the desktop
3. Click on the [HTTPS://198.18.134.220](https://198.18.134.220)
4. Click on **Advanced**
5. Click on Accept the Risk and Continue



6. Click on the **Files** link
7. You will now test the SSL Policy
8. Right click on the test2.mov and select **Save Link As**
9. Select Desktop and **Save**
 - a. The file should be downloaded
10. Right Click on test1.mp4 and select **Save Link As**
 - a. Download will fail

The screenshot shows a web browser window with the URL <https://198.18.134.220/files/>. The page title is "Index of /files". The file list includes various files such as ACTTools.exe, NetCorp_logo.gif, ProjectX.doc, ProjectX.pdf, STIX.xml, URL_List.txt, Zombies.pdf, bad.zip, bandtest.wmv, eicar.txt, evil.png, good.mp, malware.exe, pq.html, py.html, pz.html, test.mp, test1.mp4, test2.mov, and test3.avi. A "Download Error" dialog box is overlaid on the page, displaying the message: "The download cannot be saved because an unknown error occurred. Please try again." with an "OK" button.

11. The file is not being allowed to transfer even though it is a HTTPS connection. You will now review the log files that show the information for the SSL policy
12. Return to the FMC
13. Go to **Analysis > Connection > Events**
14. Click **Edit Search**
 - a. Action: Block
 - b. Networking
 - i. Initiator IP: **198.18.133.23**
 - c. Click Search

The screenshot shows the "Connection Events" table in the FMC interface. The table has columns for Jump to..., First Packet, Last Packet, Action, Reason, Initiator IP, Initiator Country, Responder IP, Responder Country, Ingress Security Zone, Egress Security Zone, Source Port / ICMP Type, Destination Port / ICMP Code, Application Protocol, Client, Web Application, and URL. Two rows of data are visible, both showing a "Block" action for initiator IP 198.18.133.23. The first row is for file block and the second for file block with custom detection. The table header includes "Connections with Application Details" and "Table View of Connection Events". The time range at the top right is 2021-10-15 21:42:22 - 2021-10-15 22:42:55, and there is a note "Expanding".

15. You can see the files that were blocked. Note that the URL reveals HTTPS

16. Click **Table View of Connection Events**

17. Click the X next to one of the columns in the current view

<input type="checkbox"/>	First Packet x	Last Packet x	Action x	Reason x	Initiator IP x
▼ <input type="checkbox"/>	2021-05-10 11:59:01	2021-05-10 11:59:01	Block	File Block, Intrusion Block	198.18.133.23
▼ <input type="checkbox"/>	2021-05-10 11:52:50	2021-05-10 11:52:50	Block	File Block	198.18.133.23
▼ <input type="checkbox"/>	2021-05-10 11:52:36	2021-05-10 11:52:36	Block	File Block	198.18.133.23
▼ <input type="checkbox"/>	2021-05-10 11:32:37	2021-05-10 11:32:38	Block	File Block	198.18.133.23
▼ <input type="checkbox"/>	2021-05-10 11:22:45	2021-05-10 11:22:46	Block	File Block, File Custom Detection	198.18.133.23
▼ <input type="checkbox"/>	2021-05-10 11:22:32	2021-05-10 11:22:32	Block	Intrusion Block	198.18.133.23
▼ <input type="checkbox"/>	2021-05-10 11:22:19	2021-05-10 11:22:19	Block	File Block	198.18.133.23

18. When the column settings appear scroll down and check all columns that begin with **SSL**

All Columns

- SSL Cipher Suite
- SSL Expected Action
- SSL Flow Error
- SSL Flow Flags
- SSL Flow Messages
- SSL Policy
- SSL Rule
- SSL Session ID
- SSL Ticket ID
- SSL Version

Apply Cancel

19. Click **Apply**

20. Review all the **SSL** fields available in relation to the traffic shown on the screen

Connection Events (2 entries)

Search Constraints (Edit Search Save Search)

Connections with Application Details Table View of Connection Events

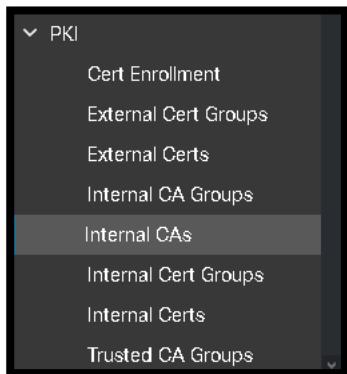
Jump to... ▾

First Packet X	Last Packet X	Action X	Reason X	Initiator IP X	Initiator User X	Responder IP X	Responder Country X	Ingress Security Zone X	Egress Security Zone X	Source Port / ICMP Type X	Destination Port / ICMP Code X	SSL Status X	SSL Flow Error X	SSL Actual Action X	SSL Expected Action X
2021-10-15 22:41:05	2021-10-15 22:41:05	Block	File Block	198.18.133.23		198.19.10.220		OutZone	InZone1	49573 / tcp	443 (https) / tcp	Decrypt (Known Key)	Success	Decrypt (Known Key)	Decrypt (Known Key)
2021-10-15 22:00:56	2021-10-15 22:01:01	Block	File Block, File Custom Detection	198.18.133.23		198.19.10.220		OutZone	InZone1	49427 / tcp	80 (http) / tcp				

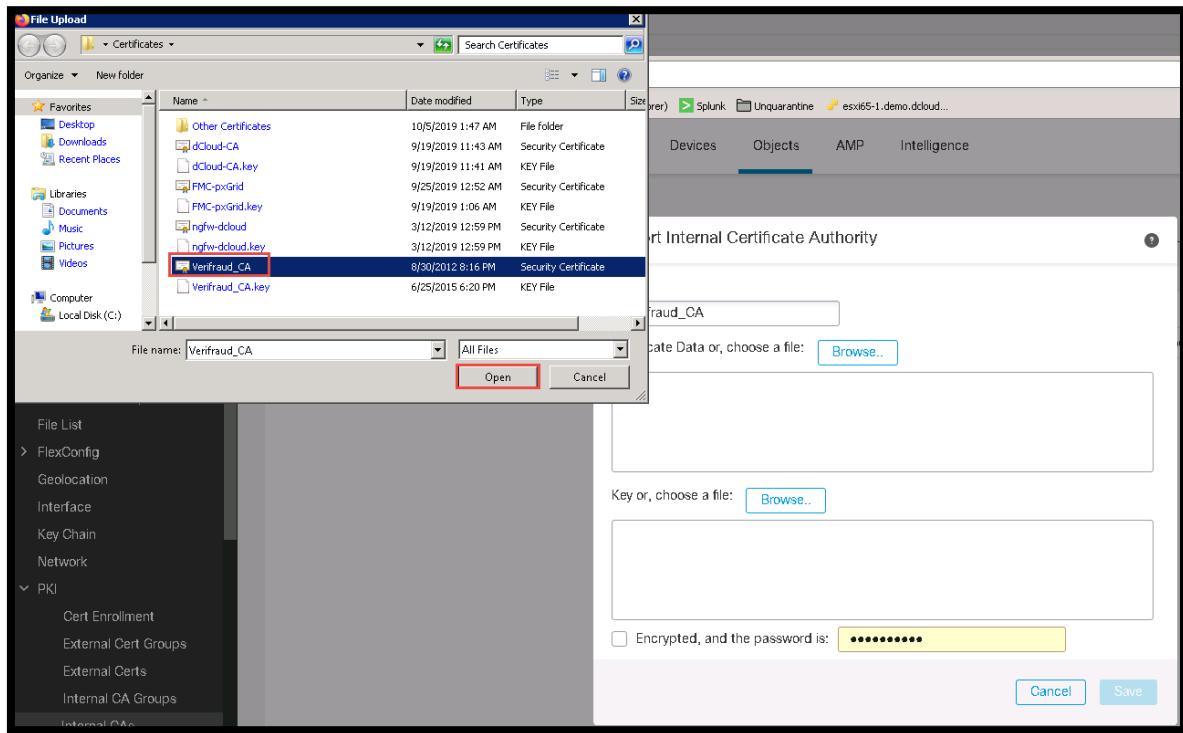
SSL Decryption – Resign

You will now decrypt outbound HTTPS traffic. You will import a CA certificate from the customer environment that will be used to decrypt the traffic and configure the SSL rule to apply to traffic from a workstation to test from in the customer environment.

1. Login to the FMC
2. Go to **Objects > Object Management > PKI > Internal CAs**

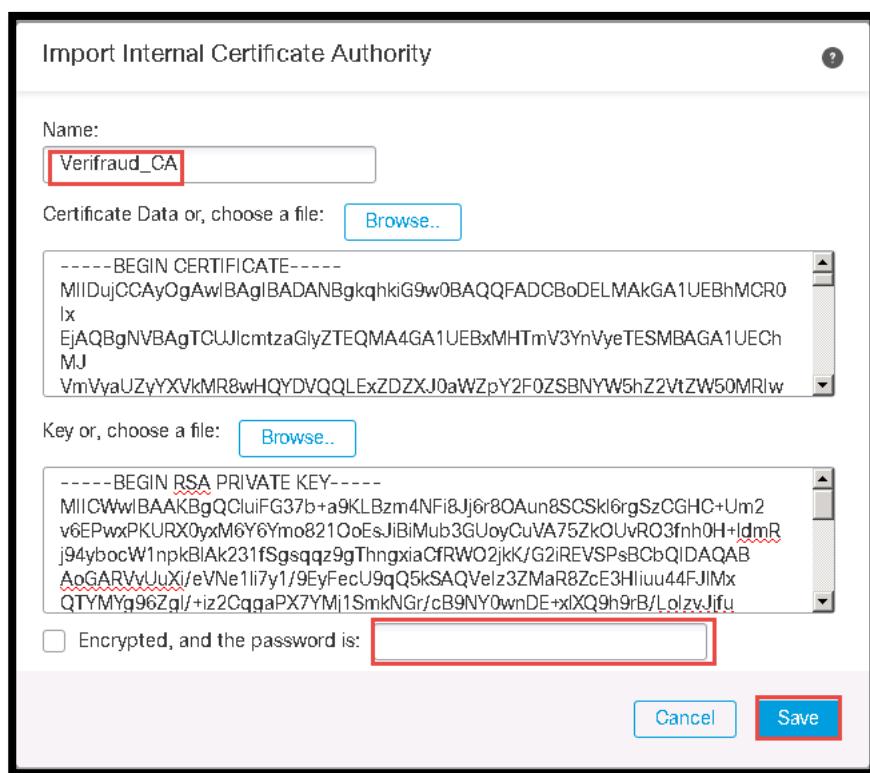


3. Verify Verifraud is there if not Click **Import CA**
4. Name Verifraud_CA
5. Certificate Data Click the Browse button
 - a. Open the **Certificates** folder located on the **Desktop** and select **Verifraud_CA** click **Open**



- b. In the **Key** section click **Browse**
- c. In the **Certificates** folder on the **Desktop** select **Verifraud_CA.key** and **Open**

6. Make sure the password field is left blank



7. Click **Save**

8. Click on **Policies** and select **SSL**
9. Edit the **Corp HQ-SSL-Policy**
10. Click **Add Rule**
11. Configure the following:
 - a. Name: **Decrypt WKST1 Outbound SSL**
 - b. Insert: **below rule 1**
 - c. Action: **Decrypt – Resign** and select the **Verifraud_CA** object from the dropdown box right of the Action field

Name: Decrypt WKST1 Outbound SSL
Enabled:
Insert: below rule 1

Action: Decrypt - Resign with Verifraud_CA
 Replace Key Only

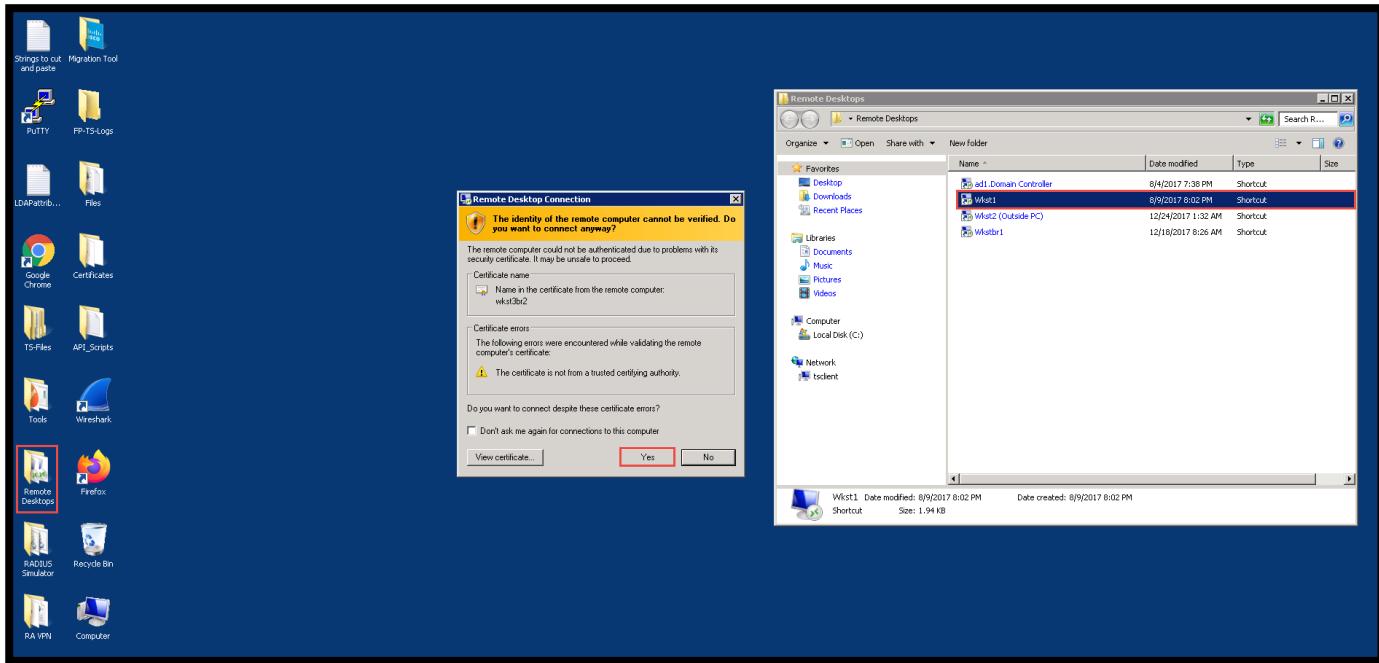
12. In the **Zones** tab add **InZone1** to the **Source Zones** and add **OutZone** to the **Destination Zones**

Add Rule

Source Zones (1)	Destination Zones (1)
InZone1	OutZone

Cancel Add

13. In the **Networks** tab select **Corporate_LAN** and add to **Source**
14. Click the **Ports** tab and select **HTTPS** and click **Add to Destination**
15. Click the **Logging** tab and select **Log at End of Connection**
16. Click **Add** and **Save** and **Deploy** the changes
17. On the **Desktop** of the **Jumpbox** click on **Remote Desktops** and open **Wkst1** select **Yes** for the **Connection**

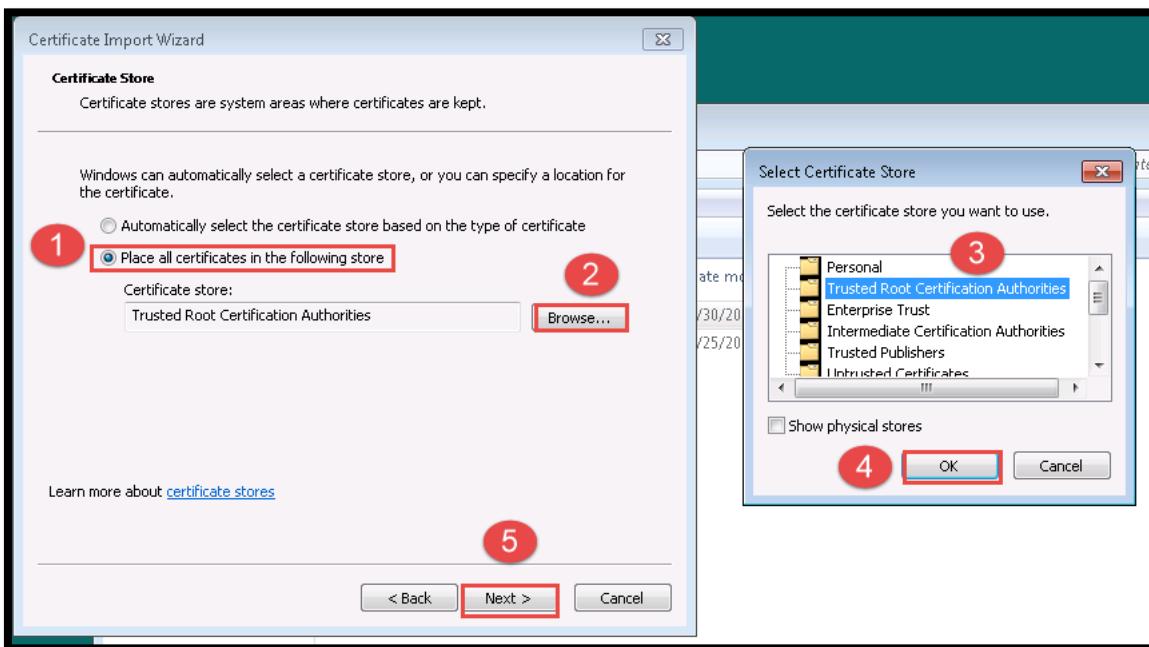


18. Open the Certificates Folder on WKST1 Desktop and Right Click on Verifraud_CA.cer and select Install Certificate

19. Click Next

20. Select Place all Certificates in the following store and click Browse

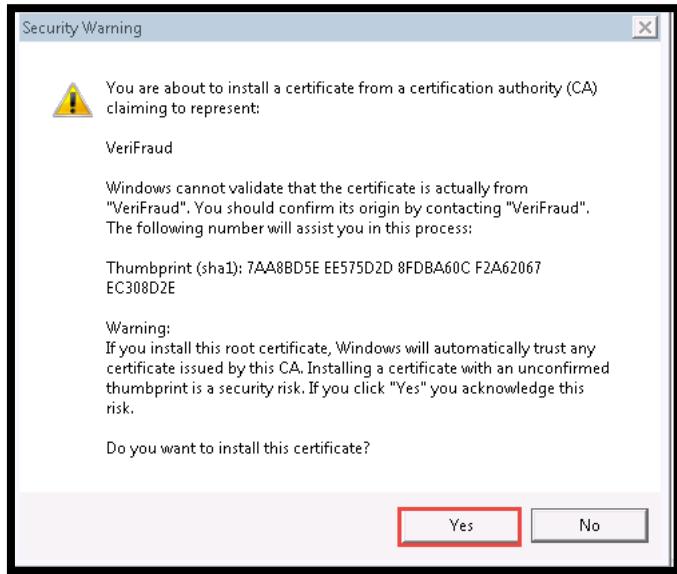
a. Certificate Store: Trusted Root Certification Authorities



b. Click **Next**

c. Click **Finish**

d. If you see the Security Warning, click **Yes**



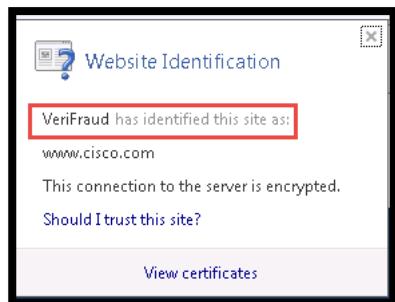
- You should get confirmation that the import was successful

Testing the SSL Policy

- Policies > Access Control > Base_Policy**
 - Review or Modify the **Allow Outbound Rule** to include the following:
 - Source Zone: **InZone1 [add to InZone]**
 - Ports: add to Destination
 - DNS_over_TCP
 - DNS_over_UDP
 - ICMP (all)
 - Click **Save and Deploy**
 - Go back to the **WKST1** remote Desktop session
 - Click on the Start Menu and open up **Internet Explorer**
 - In the URL Bar type: <https://www.cisco.com>
 - Click on the Security Report

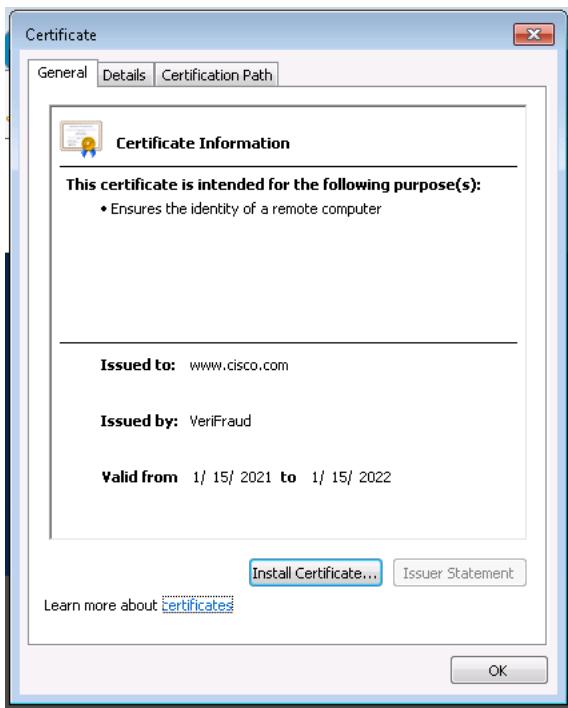


- Look at the Website Identification

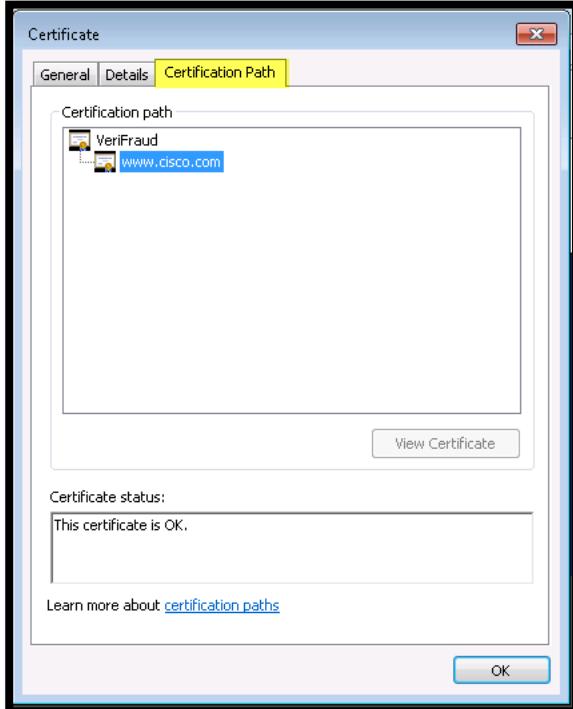


- Notice that **VeriFraud** has Identified the site as www.cisco.com

8. Select **View certificates**



9. Click on **Certification Path**



10. Note that the Certification path for www.cisco.com came from VeriFraud
11. Close the Remote Desktop for WKST1
12. Go the FMC window on the Jumpbox
13. Open the Connection Event Logs by clicking the **Analysis > Events**
14. Filter the results on the initiator IP: **198.19.10.21**

15. Change to the **Table View of Connection Events**
16. Click the [x] next to one of the columns
17. Select all SSL columns and **Apply**
18. Review the SSL events for WKST1
19. Look at the SSL Status

Connection Events (event: workflow)														II 2021-10-15 21:42:22 - 2021-10-15 23:24:22	
Connections with Application Details Table View of Connection Events														Expending	
Jump to...															
First Packet	Last Packet	Action	Initiator IP	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	SSL Flow Error	SSL Actual Action	SSL Expected Action	SSL Certificate Status	SSL Version	SSL Cipher Suite
2021-10-15 23:20:18	2021-10-15 23:20:24	Allow	198.19.10.21	72.21.81.200	InZone1	OutZone	49884 / tcp	443 (https) / tcp	Decrypt (Resign)	Success	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM
2021-10-15 23:20:18	2021-10-15 23:20:24	Allow	198.19.10.21	72.21.81.200	InZone1	OutZone	49883 / tcp	443 (https) / tcp	Decrypt (Resign)	Success	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM
2021-10-15 23:19:56	2021-10-15 23:20:24	Allow	198.19.10.21	104.16.148.64	InZone1	OutZone	49876 / tcp	443 (https) / tcp	Decrypt (Resign)	Success	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM
2021-10-15 23:19:56	2021-10-15 23:20:24	Allow	198.19.10.21	44.239.67.145	InZone1	OutZone	49881 / tcp	443 (https) / tcp	Decrypt (Resign)	Success	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM
2021-10-15 23:19:56	2021-10-15 23:19:56	Allow	198.19.10.21	72.163.15.144	InZone1	OutZone	49875 / tcp	443 (https) / tcp	Decrypt (Resign)	Success	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2	TLS_DHE_RSA_WITH_AES_128_GCM

20. You will see the Decrypt (Resign)
21. Remove the SSL Policy from Access Control Base_Policy **Save and Deploy**

Scenario 11. TLS Server Identity Discovery

Objectives

- Enable application detection and URL filtering for TLS 1.3 flows
- Access Control Policy with TLS Server Identity Discovery Enables
- Detection of SNI (Server Name Indication) Mismatch without SSL Policy

TLS server certificates are not encrypted in TLS 1.2. Firewalls were able to see the certificate information and implement policies based on clear text information. TLS 1.3 encrypts the certificates which would allow for an intruder to possibly evade AppId or URL filtering contained within a TLS 1.3 connection. TLS Server Identity Discovery helps the firewall learn TLS certificate details from servers that support TLS 1.3 and earlier version of TLS.

Application detection and URL filtering matching TLS 1.3

Firewall features such as URL filtering by (categorization and reputation) and Application Detection (AppID) rely on the information in the TLS certificates to enforce the (ACP/SSL) such as:

1. Server Name Indication (SNI)
2. Common Name (CN)
3. Subject Alternative Names (SANs)
4. Organizational Unit (OU)

Most of the useful information needed to enforce firewall rules effectively is encrypted, and information such as SNI that is in cleartext can be spoofed. The following will demonstrate how an intruder can use the SNI to bypass firewall policy and what configuration you can apply to validate the SNI further.

Investigate Default Behavior with Access Control Policy Only Enabled

1. FMC go to Policies > Prefilter > New Policy Name: **Demo Prefilter Policy**

- a. Click on **Add Prefilter Rule**
 - i. Name: CSDAC
 - ii. Enabled
 - iii. Action: Fastpath
 - iv. Interface Objects: Any
 - v. Destination Networks: 198.19.10.100, 101, 120, 121
 - vi. Ports: ICMP, TCP(6):443, TCP(6):53, UDP(17):53
 - vii. **Save**
- b. Click on **Add Prefilter Rule**
 - i. Name: Fastpath DNS traffic
 - ii. Enabled
 - iii. Action: Fastpath
 - iv. Interface Objects: Any
 - v. Networks: Any
 - vi. Ports: TCP(6):53, UDP(17):53
 - vii. Logging: Log at the end of Connection
 - viii. **Save**

2. **Save**

3. FMC Policies > Access Control > New Policy > Name TLS Policy Demo and Add HA_Test or NGFW1

- i. Click on **Add Rule**
 1. Name Allow FB APP

2. Zones: any
3. Applications: facebook
4. Logging: At the End of Connection

Name: All FB App
Enabled:

Action: Allow

Time Range: None

Applications Tab:

- Available Applications (18): Search bar shows "facebook".
- All apps matching the filter: Facebook, Facebook Applications Other, Facebook Apps, Facebook Comment, Facebook event, Facebook Games, Facebook Like.
- Add to Rule button (highlighted).

Selected Applications and Filters (1): Filter: facebook.

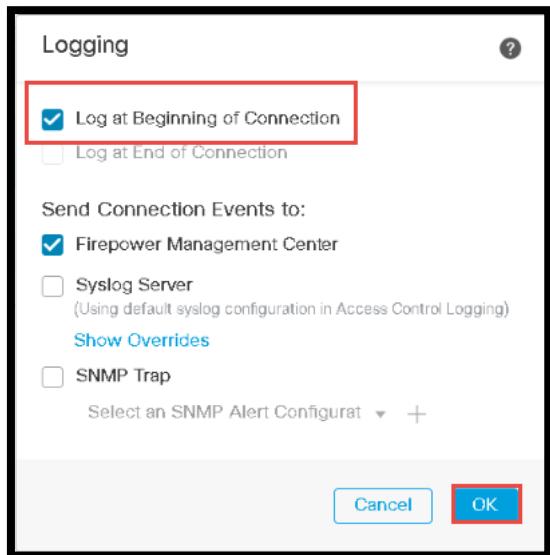
Buttons: Cancel, Save (highlighted).

5. Click Add

4. At the Bottom of the Access Control Policy where Access Control: Block all traffic
 - a. Click on Logging

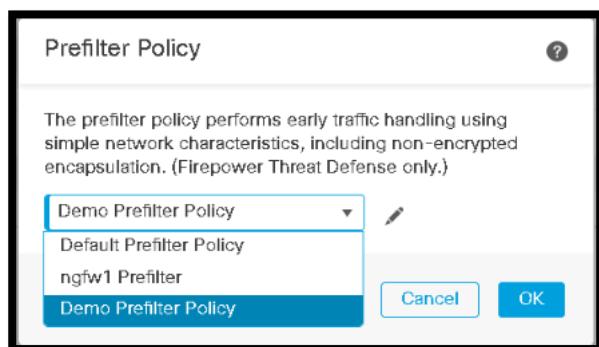
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action
1	Allow FB APP	InZone1	Any	Any	Any	Any	Any	Filter: facebook	Any	Any	Any	Any	Any	Allow

- b. Click on Log at Beginning of Connection



c. Click **OK**

5. Click on the **Default Prefilter Policy** from drop-down menu



6. Click **Save** at the top of the page
7. Click **Deploy**

TLS Server Identity Discovery Disabled and SNI not present

1. On the Jumpbox open the **Inside Linux Server** root/C1sco12345
2. On the Linux Server type the following:
 - a. `OpenSSL s_client -connect Walmart.com:443 -tls1_3`
 - i. This will generate traffic to <https://walmart.com> using TLS1.3 this command will take a few seconds to complete

```

Inside Linux Server
root@inside:~# openssl s_client -connect walmart.com:443 -tls1 3
CONNECTED(00000003)
write:errno=104
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 235 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
root@inside:~#

```

3. Click on **Analysis > Connection > Events**
 - a. Edit Search
 - b. Networking
 - i. Initiator IP*: 198.19.10.200
 - ii. Search
 - c. Click on Table view of Connection Events
4. Click on the **x** by one of the Columns
 - a. Select SSL Flow Flags
 - b. Select SSL Flow Messages

Connection Events (walmart.netflix)

Search Constraints (Edit Search Save Search)

Connections with Application Details Table View of Connection Events

Jump to... ▾

First Packet	Last Packet	Initiator IP*	Responder IP	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Type	SSL Status	Application Protocol	Client	Client Version	Web Application	Application Risk
2021-10-08 17:58:29	2021-10-08 17:58:29	161.170.232.170	161.170.232.170	USA	InZone1	OutZone	17020 / tcp	443 (https) / tcp	<input checked="" type="checkbox"/> Block With Reset	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client	<input type="checkbox"/> Walmart	Medium	
2021-10-08 17:58:29	2021-10-08 17:58:29	161.170.232.170	161.170.232.170	USA	InZone1	OutZone	55524 / tcp	443 (https) / tcp	<input checked="" type="checkbox"/> Do Not Decrypt	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client	<input type="checkbox"/> Walmart	Medium	
2021-10-08 17:59:55	2021-10-08 17:59:55	161.170.230.170	161.170.230.170	USA	InZone1	OutZone	44044 / tcp	443 (https) / tcp	<input type="checkbox"/> Block With Reset	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client	<input type="checkbox"/> Walmart	Medium	

Page 1 of 1 | Displayed 1 items

View **View All**

SSL Flow Flags
SSL Flow Messages

Apply Cancel

- c. Click **Apply**

Connection Events															2021-10-08 16:23:51 - 2021-10-08 16:31:21		Expanding			
Connections with Application Details															Table View of Connection Events					
Jump to...																				
Action X	Reason X	Initiator IP X	Initiator Country X	Initiator User X	Responder IP X	Responder Country X	Security Intelligence X Category	Ingress Security X Zone	Egress Security X Zone	Source Port / ICMP Type X	Destination Port / ICMP Code X	SSL Status X	SSL Flow Flags X							
Allow	TLS Probe	198.19.10.200			161.170.232.170	USA	InZone1	OutZone	13631 / tcp	443 (https) / tcp	Block With Reset							TLS Policy Demo		
Allow	TLS Probe	198.19.10.200			161.170.230.170	USA	InZone1	OutZone	13138 / tcp	443 (https) / tcp	Block With Reset							TLS Policy Demo		
Allow		198.19.10.200			161.170.232.170	USA	InZone1	OutZone	55518 / tcp	443 (https) / tcp								TLS Policy Demo All FB App		

SSL Flow Messages X	Application Protocol X	Client X	Client Version X	Web Application X	Application Risk X	Business Relevance X	URL X	URL Category X	URL Reputation X	DNS Query X	VLAN ID X	IOC X	Intrusion Events X	Files X	Access Control Policy X	Access Control Rule X	Network Analysis Policy X
CLIENT_HELLO	HTTPS	SSL client		Walmart	Medium	Very Low	https://walmart.com	Shopping	Trusted						TLS Policy Demo	Default Action	Balanced Security and Com
CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE							https://walmart.com										
CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE							https://walmart.com								TLS Policy Demo	Balanced Security and Com	

TLS Server Identity Discovery Disabled and with SNI Present

1. Go back to the **Inside Linux Server** and type the following
2. openssl s_client -connect Walmart.com:443 -tls1_3 -servername facebook.com

In this task, the client is trying to access Walmart.com over HTTPS protocol. The website/Application will typically be detected on the firewall based on the TLS handshake, and it will make the decision based on CN (Common Name) that is part of the Server Certificate.

```
Inside Linux Server
root@inside:~# openssl s_client -connect walmart.com:443 -tls1_3 -servername facebook.com
CONNECTED (00000003)
write:errno=104
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 236 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
root@inside:~#
```

This will set the SNI of the connection to facebook.com. When SNI is used, the hostname of the server is included in the TLS handshake. SNI provides a solution for a shared IP address that hosts multiple web server/domains that allows unique certificates to be used for each domain. In TLS 1.3 flows, SNI helps intermediate devices determine where the client is going by providing this information in clear text.

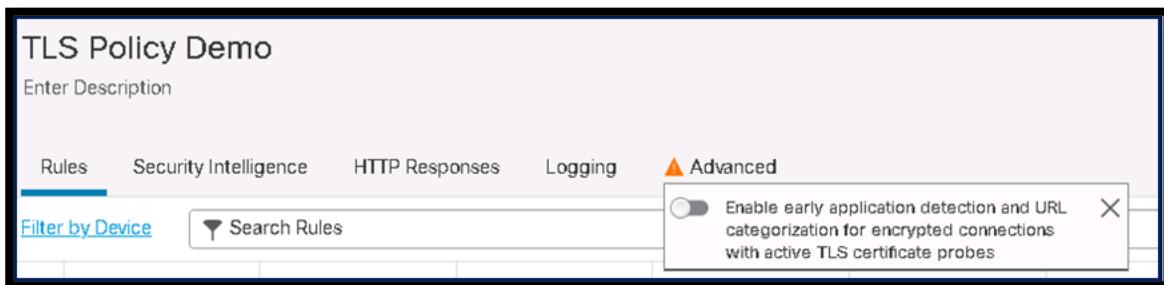
Action X	Reason X	Initiator IP X	Initiator Country X	Initiator User X	Responder IP X	Responder Country X	Security Intelligence X Category	Ingress Security X Zone	Egress Security X Zone	Source Port / ICMP Type X	Destination Port / ICMP Code X	SSL Status X	Application Protocol X	Client X	Web Application X	URL X	IOC X	Intrusion Events X	Files X	Access Control Policy X	Access Control Rule X
Allow	TLS Probe	198.19.10.200			161.170.232.170	USA	InZone1	OutZone	13631 / tcp	443 (https) / tcp	Block With Reset									TLS Policy Demo	
Allow	TLS Probe	198.19.10.200			161.170.230.170	USA	InZone1	OutZone	13138 / tcp	443 (https) / tcp	Block With Reset									TLS Policy Demo	
Allow		198.19.10.200			161.170.232.170	USA	InZone1	OutZone	55518 / tcp	443 (https) / tcp										TLS Policy Demo All FB App	

The firewall can trust a session based on the SNI information before the certificate is learned. Learning the certificate ahead of time is important to ensure the SNI is verified before the firewall makes its decision.

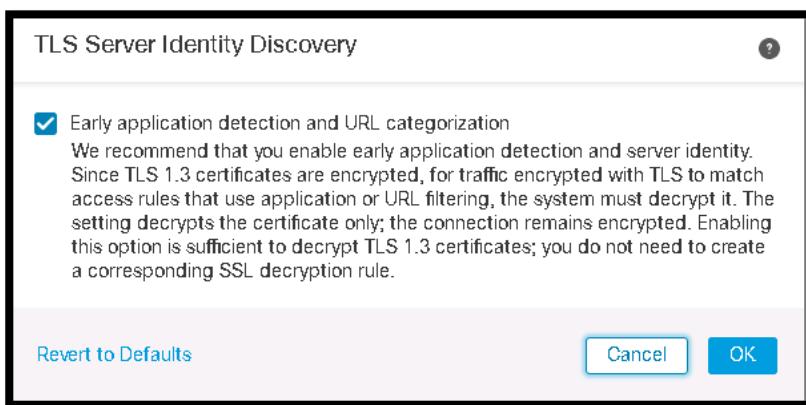
The next exercise will look at how Cisco Secure Firewall threat Defense using the **TLS Server Identity Discovery** feature makes a decision against TLS 1.3 flows based on other information, since SNI can be easily spoofed. When processing TLS 1.3 traffic flows, the FTD with TLS Server Identity Discovery feature provides CN as the higher precedence over SNI.

[Enable TLS Server Identity Discovery feature on FMC](#)

3. **FMC Policies > Access Control > TLS Policy Demo**
4. Go to the Advanced Tab



5. Click on the Toggle button to **Enable early application detection and URL categorization for encrypted connections with active TLS certificates probes** or Click on the Advanced tab in the ACP select the pencil next to “TLS Server Identity Discovery” to edit the configuration



6. **Save the ACP and Deploy**

[TLS Server Identity Discovery Enabled and with SNI Mismatch Detection](#)

1. On the Inside Linux Server type:
 - a. `openssl s_client -connect Walmart.com:443 -tls1_3 -servername facebook.com`

```

Inside Linux Server
root@inside:~# openssl s_client -connect walmart.com:443 -tls1_3 -servername facebook.com
CONNECTED(00000003)
write:errno=104
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 236 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
root@inside:~#

```

2. Go to the FMC and refresh the connection event and view Table View of Connection Events

Action X	Initiator IP X	Responder IP X	Responder Country X	Ingress Security X Zone	Egress Security X Zone	Source Port / ICMP Type X	Destination Port / ICMP Code X	SSL Status X	SSL Flow Flags X	SSL Flow Message X	Application Protocol X	Client x	Web Application X
Block	198.19.10.200	161.170.232.170	USA	InZone1	OutZone	55536 / tcp	443 (https) / tcp	<input checked="" type="checkbox"/> Do Not Decrypt	VALID, SSL_DETECTED, CH_Processed, CERTIFICATE_CACHE_HIT, SERVER_NAME_MISMATCH	CLIENT_HELLO	HTTPS	<input checked="" type="checkbox"/> SSL client	<input checked="" type="checkbox"/> Walmart

As was shown and stated before SNI is cleartext and can be spoofed or not present. The purpose of the last exercise was to show that with TLS Server Identity Discovery you can verify SNI with other information and detect a SNI mismatch without implementing an SSL policy inspection which is important because not all deployments use the SSL Policy.

TLS Server Identity Discovery Probe – Certificate not found in local cache

TLS probe helps TLS Server Identity Discovery feature learn about server certificates from TLS 1.3 sessions. This exercise aims to demonstrate that the TLS Server Identity Discovery probe can discover a server certificate, cache it, and use it to assist with the TLS 1.3 connections.

1. FMC Policies > Access Control edit the **TLS Policy Demo**
2. Click Add Rule
 - a. Name: Allow Finance
 - b. Action: Allow
 - c. URLs tab: Finance and Online Trading
 - d. Logging: Log at End of Connection
 - e. Click **Add**
 - f. Validate that TLS Server Identity Discovery is enabled in the **Advanced** tab
 - g. Click **Save**

Name: Allow Finance Enabled: Move

Action: Allow Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Categories and URLs: +

Reputations:

- Any
- 5 - Trusted
- 4 - Favorable
- 3 - Neutral
- 2 - Questionable
- 1 - Untrusted

Apply to unknown reputation

Selected URLs (2):

- Finance (Any reputation)
- Online Trading (Any reputation)

Enter URL Add

Cancel Save

h. Deploy

3. After deployment completes open a PuTTY session to NGFW1 admin/C1sco12345
4. Type system support ssl-probe-logging-enabled true

```
> system support ssl-probe-logging-enabled true
Parameter and value successfully added to configuration file.

Configuration file contents (defaults added automatically):
max_tcp_tracked=50000
max_ssl_sessions=32000
SFTLS_max_tcp_tracked=50000
probe_connection_logging=true
>
```

5. Clear the certificate cache
 - a. Type: system support ssl-cache-clear all

```
> system support ssl-cache-clear all
Clearing cache... Complete.
>
```

6. Check for a specific certificate in NGFW1 using its domain name /SNI or IP address information
 - a. Type: system support ssl-cache-certificate-search
 - i. Type 1
 - ii. Enter name: americanexpress.com

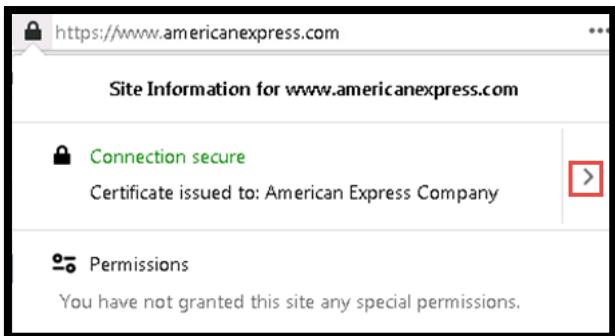
```
> system support ssl-cache-certificate-search

Please select a search option:
  1 - Search by domain name
  2 - Search by SNI
  3 - Search by IP address

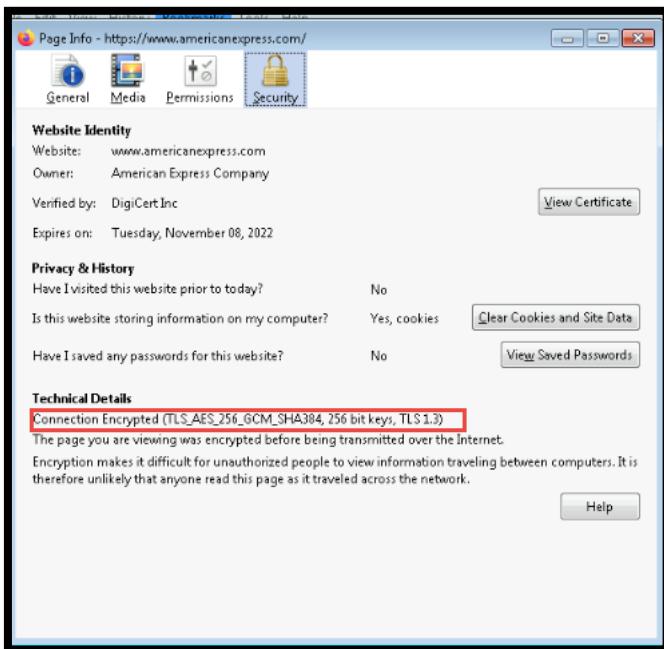
Search option (1/2/3): 1
Please enter the domain name to search: americanexpress.com

----- Output from the Cache -----
Certificate not present in cache.
> [redacted]
```

7. From Jumpbox open the folder **Remote Desktops** and click on **Wkst1**
8. On **Wkst1** open any Financial TLS 1.3 capable website <https://americanexpress.com> (might take a while for the page to load)
9. Click on the locker  button
 - a. Click [>] to expand details about Certificates issued for the website



- b. Click on **More Information**



10. FMC Analysis > Connections > Events

- a. Edit Search
- b. Under Networking add 198.19.10.21 click Search
- c. Select Table View of Connection Events for americanexpress.com

Allow	TLS Probe	198.19.10.35	52.33.45.66	21970 / tcp	443 [https] / tcp	<input checked="" type="checkbox"/> Block With Reset	VALID, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, SERVER_SESSION_ID_SEEN, CLIENT_HELLO_SESSKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, CH_CURVES_MODIFIED, ..., CERTIFICATE_CACHE_MISS, CERTIFICATE_CACHE_HIT	CLIENT_HELLO, SERVER_HELLO, SERVER_CERT
Block		198.19.10.35	99.84.191.117	638952 / tcp	443 [https] / tcp	<input checked="" type="checkbox"/> Do Not Decrypt	VALID, SSL_DETECTED, CH_PROCESSED, CERTIFICATE_CACHE_HIT	CLIENT_HELLO
Block		198.19.10.35	52.33.45.66	639533 / tcp	443 [https] / tcp	<input checked="" type="checkbox"/> Do Not Decrypt	VALID, SSL_DETECTED, CH_PROCESSED, CERTIFICATE_CACHE_MISS, CERTIFICATE_CACHE_HIT	CLIENT_HELLO

- d. SSL Flow Flags = CERTIFICAT_CACHE_MISS and CERTIFICATE_CACHE_HIT
- e. SSL Flag Message = CLIENT_HELLO

SSL Flow Flags field displays CERTIFICATE_CACHE_MISS on the first visit to the website because the certificate information is not present in the local device cache. In latter visits it displays CERTIFICATE_CACHE_HIT, since the system triggered a TLS probe that has obtained certificate details and stored it into the cache. The system uses the certificate found in cache to make policy enforcement decisions.

11. On Wkst1 close and reopen Firefox browser to <https://americanexpress.com>

12. On the FMC Analysis > Connections > Events

- a. Edit Search
- b. Enter Initiator IP: 198.19.10.21
- c. Enter URL: *americanexpress.com

▼	<input type="checkbox"/> Allow	198.19.10.21	23.78.159.52	USA	InZone1	OutZone	53431 / tcp	443 (https) / tcp	VALID, SSL_DETECTED, CH_PROCESSED, CERTIFICATE_CACHE_HIT
▼	<input type="checkbox"/> Allow	198.19.10.21	23.78.159.52	USA	InZone1	OutZone	53508 / tcp	443 (https) / tcp	VALID, SSL_DETECTED, CH_PROCESSED, CERTIFICATE_CACHE_HIT

Note that this time SSL Flow Flag reports only CERTIFICATE_CACHE_HIT and there is no TLS Server Identity Discovery probe session event displayed. This is because the TLS probe was not needed to be engaged as the TLS certificate for the sites were cached locally. The system was able to leverage the necessary certificates on future requests

13. Go bay to NGFW1 PuTTy connection and type

- a. System support ssl-cache-certificate-search
- b. Choose 1
- c. Type americanexpress.com

```

PuTTY
Certificate present in cache.
Detailed Certificate Output:

Cert SHA1 Fingerprint: 4e9a91f32a3c1d19ba15f9474a81f16a27b8fa6
Original Certificate Cache Timestamp (UTC): Sat Oct 9 18:52:09 2021
Issuer:
  C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
  Issuer Key Type: RSA
  Validity:
    Not Before (UTC): Fri Oct 8 00:00:00 2021
    Not After (UTC): Tue Nov 8 23:59:59 2022
Subject:
  C=US, O=American Express Company, CN=www.americanexpress.com
  Subject Alternative Names:
    DNS:www.americanexpress.com, DNS:americanexpress.com, DNS:amexmobile.com, DNS:amexsavings.com, DNS:personalsavings.com, DNS:www.personalsavings.americanexpress.com, DNS:www.personalsavings.com

Cert SHA1 Fingerprint: 7a0dee2ae660104f4adfc1170493cc6d9c2282
Original Certificate Cache Timestamp (UTC): Sat Oct 9 18:52:10 2021
Issuer:
  C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
  Issuer Key Type: RSA
  Validity:
    Not Before (UTC): Tue Jun 8 00:00:00 2021
    Not After (UTC): Sat Jul 9 23:59:59 2022
Subject:
  C=US, O=American Express Company, CN=www.americanexpress.com
  Subject Alternative Names:
    DNS:n.americanexpress.com, DNS:navigation.americanexpress.com, DNS:secure.cmax.americanexpress.com, DNS:m.aexp-static.com, DNS:www.aexp-static.com, DNS:maps-content.americanexpress.com, DNS:secure.americanexpress.com, DNS:cms.americanexpress.com, DNS:network.americanexpress.com, DNS:developer.americanexpress.com, DNS:icm.aexp-static.com, DNS:web.aexp-static.com

Cert SHA1 Fingerprint: b57c6322fb3c80f05e7d251dadfd8d0dd9e6363a8
Original Certificate Cache Timestamp (UTC): Sat Oct 9 19:02:39 2021
Issuer:
  C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
  Issuer Key Type: RSA
  Validity:
    Not Before (UTC): Thu Sep 16 00:00:00 2021
    Not After (UTC): Mon Oct 17 23:59:59 2022
Subject:
  C=US, O=American Express Company, CN=cdaas1.americanexpress.com
  Subject Alternative Names:
    DNS:cdaas1.americanexpress.com, DNS:cdaas2.americanexpress.com, DNS:cdaasd1.americanexpress.com, DNS:cdaasd2.americanexpress.com, DNS:cdaas.americanexpress.com

```

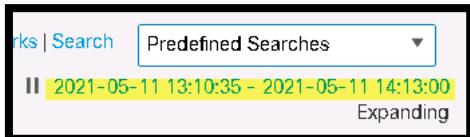
14. On NGFW1 change the ACP back to Base_Policy **Save and Deploy**

Scenario 12. Network Discovery and Firepower Recommendations

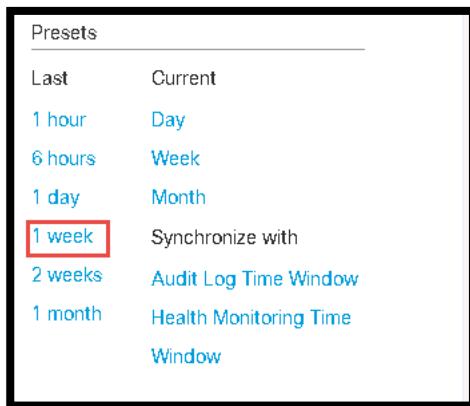
Review Discovery Data

You will now review the discovery data contained in the FMC that has been generated by the FTD.

1. Click Analysis > Hosts > Discovery Events
2. Click the link in the upper right of the screen that shows the time period the data is from



3. Select from the 1 week before and click **Apply**



4. A list of the Discovery Events for the last week is shown. The events correspond to a host initiating network traffic through the firewall that triggered a Discovery event where the firewall obtained detailed information about the host.
5. Find an entry or Edit Search for host **198.19.10.21** right click the host's IP address and select **View Host Profile**

Event x	IP Address x	User x	MAC Address x	MAC Vendor x	Port x	Description x	Device x
Client Update	198.19.10.21		00:56:00:09:01	VMware, Inc.		HTTP Microsoft CryptoAPI 6.1 Office 365	NGFW1
Client Update	198.19.	Open In New Window	00:56:00:00:01	VMware, Inc.		HTTPS SSL client AdGear	NGFW1
Client Update	198.19.	Exclude	00:56:00:00:01	VMware, Inc.		HTTPS SSL client Ad Nexus	NGFW1
Client Update	198.19.	Open In Context Explorer	00:56:00:00:01	VMware, Inc.		HTTPS SSL client Google APIs	NGFW1
Client Update	198.19.	Whois	00:56:00:00:01	VMware, Inc.		HTTPS SSL client Twitter Link Service	NGFW1
Client Update	198.19.		00:56:00:00:01	VMware, Inc.		HTTPS SSL client Google Analytics	NGFW1
Client Update	198.19.	Add IP to Block List	00:56:00:00:01	VMware, Inc.		HTTPS SSL client The Trade Desk	NGFW1
Client Update	198.19.	Add IP to Do-Not-Block List	00:56:00:00:01	VMware, Inc.		HTTPS SSL client ClickTale	NGFW1
Client Update	198.19.	AlienVault IP	00:56:00:00:01	VMware, Inc.		HTTPS SSL client Facebook	NGFW1
Client Update	198.19.	IBM X-Force Exchange IP	00:56:00:00:01	VMware, Inc.		HTTPS SSL client Twitter	NGFW1
Client Update	198.19.	Locking Glass IP	00:56:00:00:01	VMware, Inc.		HTTPS SSL client Doubleclick	NGFW1
Client Update	198.19.10.21		00:56:00:00:01	VMware, Inc.		HTTPS SSL client Adobe Analytics	NGFW1
New Transport Protocol	198.19.10.21		00:56:00:00:01	VMware, Inc.	tcp		NGFW1
Client Update	198.19.10.21		00:56:00:00:01	VMware, Inc.		HTTPS SSL client Cisco	NGFW1
Client Update	198.19.10.21		00:56:00:00:01	VMware, Inc.		HTTP Firefox 82.0 Cisco	NGFW1
Client Update	198.19.10.21		00:56:00:00:01	VMware, Inc.		HTTPS SSL client CloudFlare	NGFW1
Client Update	198.19.10.21		00:56:00:00:01	VMware, Inc.		HTTPS SSL client Google	NGFW1
Client Update	198.19.10.21		00:56:00:00:01	VMware, Inc.		HTTPS SSL client Pocket	NGFW1

6. From the Host Profile page, you have the ability to access data related to that host such as:
 - a. Content Explorer

- b. Connection Events
 - c. Intrusion Events
 - d. File Events
 - e. Malware Events
7. Look at the **Indication of Compromise**
- a. If you don't see any, go back to Wkst1 open Firefox and download Zombies.pdf and recheck

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2021-05-11 19:40:06	2021-05-11 19:40:06

8. Look at the Operating System

Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008, 8.1	Firepower

9. Scroll Down and look at **Vulnerabilities**
10. Click on **Content Explorer**
- a. Scroll down and look at the information
11. Go back to the Host Profile and Click on the **Malware Events**
- a. Note the events

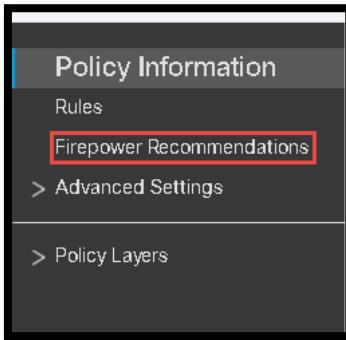
Detection Name	File Name	File SHA256	File Type	Count
Zombies.pdf	Zombies.pdf	00b32c34...989bb002	PDF	1

12. Go to **Analysis > Hosts > Network Map**
13. Expand the **198** until you get to the **198.18.133.200** and **Click on it**
- a. Look to see if you have the following:
 - i. **Operating Systems**
 - ii. **Attributes**
 - iii. **Host Protocols**
 - iv. **Vulnerabilities**
14. Expand the **198.19** until you get to the **198.19.10.100** and **Click on it**
- a. Look at the following:
 - i. **Indications of Compromise**
 - ii. **Operating Systems**
 - iii. **Attributes**
 - iv. **Host Protocols**
 - v. **Most Recent Malware Detection**
 - vi. **Vulnerabilities**

Firepower Recommendations

You will now see how to tune the IPS policy based on Firepower recommendations.

1. Click **Policies > Intrusion**
2. Click the **HQ-Balanced-Policy Snort 2 Version** and click **Firepower Recommendations**



3. Place a checkmark in the **Include all differences...** box and **Click Advanced Settings**

Firepower Recommended Rules Configuration

No recommendations have been generated.

Include all differences between recommendations and rule states in policy reports

Advanced Settings

Networks to Examine

Networks
(Single IP address, CIDR block, or comma-separated list)

Firepower Recommended Rules Configuration

Recommendation Threshold(By Rule Overhead)

None Low Medium High

Accept Recommendations to Disable Rules

4. Leave the **Accept Recommendations to Disable Rules**

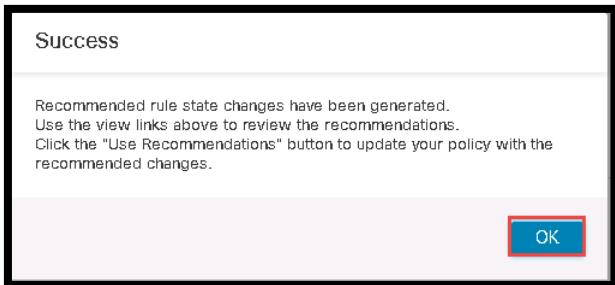
NOTE: Enabling this option can reduce the number of IPS rules active in a policy. You will leave this enabled to view the effect of the option. In a customer environment that has no performance issues, it may be undesirable to reduce the about of rules active in the policy.

5. Click **Generate Recommendations**

Generating Firepower Recommendations

Storing recommendations

6. Click OK on the Success Box



Firepower Recommended Rules Configuration

Firepower recommends 24277 rule state settings for 20 hosts

- Set 281 rules to generate events
- ∅ Set 7751 rules to drop and generate events
- + Set 16245 rules to disabled

Policy is not using the recommendations. [Click to change recommendations](#)

Last generated: 2021 May 12 01:03:59

Include all differences between recommendations and rule states in policy reports

[View Recommended Changes](#)

7. Click on View Recommend Changes

Rules

Rule Configuration Rule Content Category

app-detect browser-chrome browser-firefox browser-ie browser-other browser-plugins browser-webkit content-replace decoder exploit-kit file-executable file-flash file-identify file-image

Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific Preprocessors Priority Rule Update

Filter: State:"Does not match recommendation"

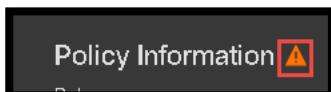
0 selected rules of 4120

Rule State ▾ Event Filtering ▾ Dynamic State ▾ Alerting ▾ Comments ▾ Policy

GID	SID	Message	Action
105	2	BO_CLIENT_TRAFFIC_DETECT	X →
105	3	BO_SERVER_TRAFFIC_DETECT	X →
105	4	BO_SNORT_BUFFER_ATTACK	X →
105	1	BO_TRAFFIC_DETECT	X →
1	52069	BROWSER-CHROME Google Chrome blink webaudio module use after free attempt	X →
1	49380	BROWSER-CHROME Google Chrome FileReader use after free attempt	X →
1	53752	BROWSER-CHROME Google Chrome ObjectCreate type confusion attempt	X →
1	53754	BROWSER-CHROME Google Chrome ObjectCreate type confusion attempt	X →

8. You can look at the output of the pages

9. Click on **Use Recommendations** and Click **OK** on the Success message
10. Click the **Orange Caution symbol** next to the Policy Information



11. Click **Commit Changes**
12. Type **Generate policy recommendations** in the Description of Changes window and click **OK**
13. **Deploy the changes**

Scenario 13. Cisco Threat Intelligence Director (CTID)

This exercise consists of the following tasks.

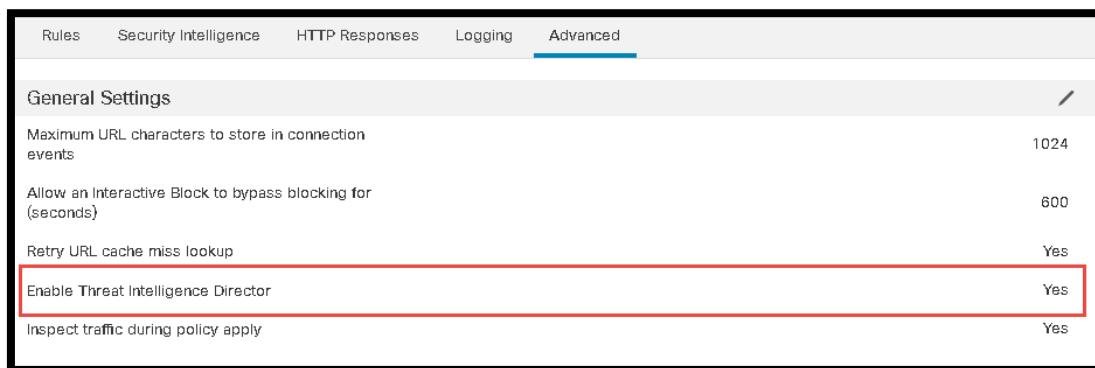
- Upload a list of URLs to CTID that will trigger an Incident
- Subscribe CTID to a TAXII feed
- Generate CTID incidents

The CTID is a component of the FMC that can consume third party cyber threat intelligence indicators; CTID parses these indicators to produce observables that can be detected by the NGFW. The NGFW reports detection of the observables to CTID. Then CTID determines whether the observations constitute an incident.

Steps

Two file formats are supported.

- Flat files - Lists of simple indicators such as IP addresses, URLs or SHA256 hashes.
- Threat Intelligence Director is enabled by default You can find it under **Policies > Access Control > Then the policy (Base_Policy in our case) under Advanced.**



STIX files - XML files that can describe simple or complex indicators There are 3 ways these files can be retrieved:

- Uploaded from the computer where the FMC UI is running.
- Retrieved from a URL on a remote web server.
- Received from a TAXII feed (STIX files only).

The objective of this exercise is to configure and test CTID.

Steps

Confirm that CTID will publish observables to the NGFW

1. Navigate to **Policies > Access Control > Access Control**.
2. Edit the access control policy (Base_Policy) by clicking the pencil icon to the right of the policy.
3. Select the Advanced tab. Using this advanced setting, CTID can be enabled or disabled at the access policy level.

Rules Security Intelligence HTTP Responses Logging Advanced

General Settings

Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
Retry URL cache miss lookup	Yes
Enable Threat Intelligence Director	Yes
Inspect traffic during policy apply	Yes

4. Navigate to **Intelligence > Elements**.

5. Confirm that the NGFW1 is an element. This means that CTID can publish observables to the NGFW1 retrieved from a STIX file from a web server.

Name	Element Type	Registered On	Access Control Policy
NGFW1	Cisco Firepower Threat Defense for vSphere	Mar.11, 2019 1:29 AM EDT	None_Policy
NGFWIR1	Cisco Firepower Threat Defense for vSphere	Mar.11, 2019 2:25 AM EDT	Branch Access Control Policy
NGFW2	Cisco Firepower Threat Defense for vSphere	Sep.17, 2020 11:49 AM EDT	None_Policy

TID Detection
The system is currently publishing TID observables to elements. Click Pause to stop publishing and purge TID observables stored on your elements.
 Pause Resume

NOTE: The CTID can be enabled or disabled globally. Clicking Pause will stop the CTID publishing to all elements.

6. Navigate to **Intelligence > Sources > Sources**.

7. Upload a list of URLs to CTID that will trigger an Incident

- Navigate to **Intelligence > Sources > Sources**. Click the plus sign (+) on the right to add an intelligence source.
- For **DELIVERY**, select **Upload**.
- For **TYPE**, select **Flat File**. The **CONTENT** drop-down list will appear.
- For **CONTENT**, select **URL**.
- Click in the **FILE** area, and select **URL_LIST.txt** from the **Files** folder on the Jump desktop.
- For **NAME**, enter **url list**.
- For **ACTION**, select **Block**.

The screenshot shows the 'Add Source' dialog box with the following fields and settings:

- DELIVERY:** TAXII (selected)
- TYPE:** Flat File (selected)
- CONTENT:** URL
- FILE***: A dashed box for file attachment, with a placeholder 'Drag and drop or click to attach'.
- NAME***: url list
- DESCRIPTION**: An empty text area.
- ACTION**: Black (selected)
- TTL(DAYS)**: 90
- PUBLISH**: Enabled (blue switch)

8. Click **Save**.
9. Navigate to **Intelligence > Sources > Observables**. Confirm that two type URL observables have been added.

Subscribe CTID to a TAXII feed

1. Navigate to **Intelligence > Sources > Sources**. Click the plus sign (+) on the right to add an intelligence source.
2. For **DELIVERY**, select **TAXII**.
3. For **URL**, enter <http://hailataxii.com/taxii-discovery-service>.
4. For **USERNAME**, enter **guest**.
5. For **PASSWORD**, enter **guest**.
6. For **FEEDS**, select **guest_phishtank_com**.

NOTE: It may take several seconds for the FEEDS drop-down list to populate.

7. Confirm that the screen looks like the following figure.

The screenshot shows the 'Add Source' dialog box for TAXII delivery. Key fields highlighted with red boxes include the URL, FEEDS*, and the 'Save' button at the bottom right.

8. Click **Save**.
9. Wait until the Status column for this source changes to **Parsing**. Do not wait for the parsing to complete - this would take too long.
10. Navigate to **Intelligence > Sources > Indicators**. Confirm that several URL indicators have been added.
11. Navigate to **Intelligence > Sources > Observables**. Confirm that several URL observables have been added.

Generate CTID incidents

1. It can take several minutes for the observables to be published to the sensor. In this step, you will see how to confirm the publication of a particular observable. In the **NGFW1 CLI**, perform the following:
2. Type **expert** to get into expert mode.
3. Type **ls -d /var/sf/*download**.

NOTE: There are several directories listed. admin@ngfw:~\$ ls -d /var/sf/*download

```
ls -d /var/sf/clamupd_download
ls -d /var/sf/irep_download
ls -d /var/sf/sifile_download
ls -d /var/sf/cloud_download
ls -d /var/sf/sidns_download
ls -d /var/sf/siurl_download
```

Four of these (irep_download, sidns_download, sifile_download and siurl_download) are used by security intelligence and CTID.

4. Type **grep developmentserver /var/sf/*download/*lf**.

5. You should see a type URL CTID observable.

/var/sf/siurl_download/731625d4-9512-11e7-915c-7e7252ae92ac.lf:developmentserver.com/misc/Tron.html/

NOTE: If you do not, wait a minute and try again. You must wait for this to be published before you go on.

6. Type grep 198.18.133.200 /var/sf/*download/*lf.

You should see a type URL CTID observable.

/var/sf/irep_prep_download/731625d4-9512-11e7-915c-7252ae92ac.blf:198.18.133.200

NOTE: If you do not, wait a minute and try again. You must wait for this to be published before you go on.

7. Type exit to exit expert mode.

On the Inside Linux server CLI:

1. Run wget -t 1 outside/files/ProjectX.pdf. This should succeed.
2. Run wget -t 1 developmentserver.com/misc/Tron.html. This should be blocked.
3. On the FMC, navigate to **Intelligence > Incidents**. Confirm that there is an incident.
 - a You might have to refresh a few times.

4. Drill down into the incident and observe the details for this incident.
5. Confirm that there is an incident for a URL indicator. Drill down into the incident and observe the details for this incident

Appendix A. FMC Pre-configuration

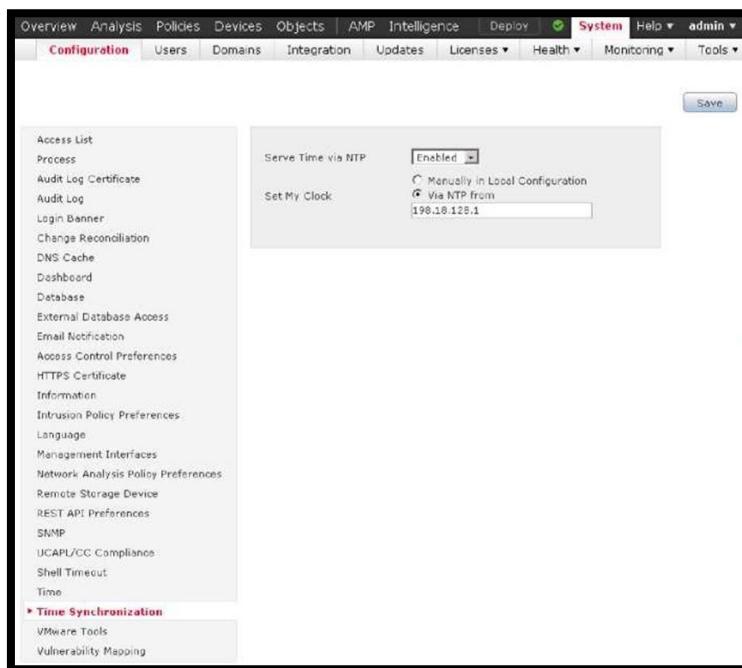
After the initial installation, several configuration steps were performed on the FMC to expedite the lab exercises. These configuration steps are detailed in this appendix.

- Configuration A1,1: NTP settings
- Configuration A1,2: Demo file policy
- Configuration A1,3: Demo intrusion policy
- Configuration A1,4: Demo SSL policy
- Configuration A1,5: Custom detection list
- Configuration A1,6: Add restapiuser.
- Configuration A1,7: Install server certificate

Steps

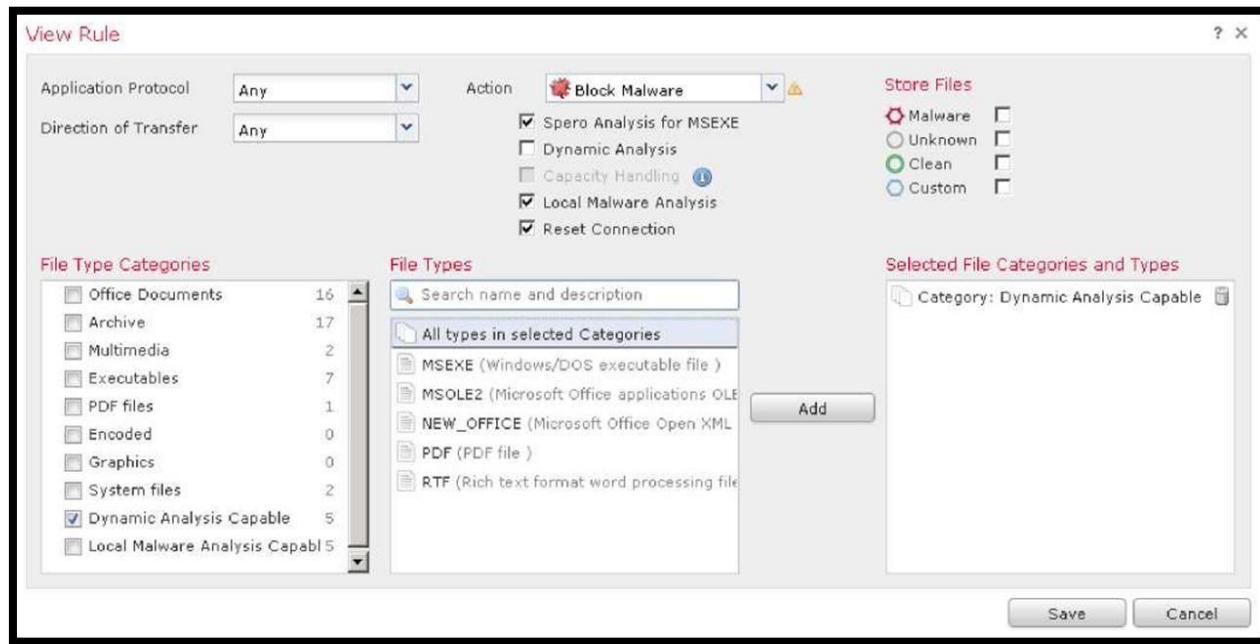
Configuration A1,1: NTP settings

1. Configure NTP settings on the FMC.
 - a. In the FMC, navigate to **System > Configuration**.
 - b. Select **Time Synchronization** from the left-side navigation pane.
 - c. Replace the default NTP server with 198.18.128.1.
 - d. Click Save.



Configuration A1,2: Demo file policy

1. **Navigate to Policies > Access Control > Malware & File.**
2. **Click New File Policy.** Enter a name **Demo File Policy**. **Click Save.**
3. Click **Add File Rule**. This rule will block malware found in files MSEXE, MSOLE2, NEW_OFFICE and PDFs.
4. **For Action select Block Malware.**
5. Check the Spero and **Local Malware Analysis** checkboxes.
6. Under **File Type Categories**, check *Dynamic Analysis Capable*. **Note** that several file types belong to this category. Click **Add**.
7. Your screen should look like the figure below.



8. Click **Save**. Ignore the warning and click **OK**, when prompted.
9. Click **Add File Rule**. This rule will block RIFF files. You will use an AVI file to test this rule, since an AVI file is a type of RIFF file. But **Note** that AVI is not listed separately as a file type.
10. **For Action select Block Files.**
11. Under **File Types**, type **rif** into the search box. Select **RIFF** from the list. Click **Add**.
12. Use default values for other settings. Your screen should look like the figure below.
13. Click **Save**.

Add File Rule

Application Protocol → Any	Action: <input checked="" type="checkbox"/> Block Files	<input checked="" type="checkbox"/> Store files																				
Direction of Transfer → Any	<input type="button" value="W Reset Connection"/>																					
File Type Categories <table border="1"> <tr><td>[I]-Office-Documents</td><td>20-A</td></tr> <tr><td>[R]-Archive</td><td>18</td></tr> <tr><td>[H]-Multimedia</td><td>30</td></tr> <tr><td>O-Executables</td><td>1</td></tr> <tr><td> └-PDF-files</td><td>2</td></tr> <tr><td> └-Encoded</td><td>2</td></tr> <tr><td> └-Graphics</td><td>6</td></tr> <tr><td> └-System-files</td><td>12</td></tr> <tr><td> └-Dynamic-Analysis-Capable</td><td>4</td></tr> <tr><td> └-Local-Malware-Analysis-Capable</td><td>5</td></tr> </table>			[I]-Office-Documents	20-A	[R]-Archive	18	[H]-Multimedia	30	O-Executables	1	└-PDF-files	2	└-Encoded	2	└-Graphics	6	└-System-files	12	└-Dynamic-Analysis-Capable	4	└-Local-Malware-Analysis-Capable	5
[I]-Office-Documents	20-A																					
[R]-Archive	18																					
[H]-Multimedia	30																					
O-Executables	1																					
└-PDF-files	2																					
└-Encoded	2																					
└-Graphics	6																					
└-System-files	12																					
└-Dynamic-Analysis-Capable	4																					
└-Local-Malware-Analysis-Capable	5																					
File Types <table border="1"> <tr><td>RIFF-(Resource-Interchange File Formats)</td></tr> </table>			RIFF-(Resource-Interchange File Formats)																			
RIFF-(Resource-Interchange File Formats)																						
Selected File Categories and Types <table border="1"> <tr><td>RIFF-(Resource-Interchange File Formats)</td></tr> </table>			RIFF-(Resource-Interchange File Formats)																			
RIFF-(Resource-Interchange File Formats)																						
<input type="button" value="Add"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>																						

RIFEX-(RIFF audio format)

NOTE: You cannot change the order of the rules you create. The order of the rules does not matter. The action of the rule determines its precedence. The precedence of actions is as follows.

- 1 - Block Files
 - 2 - Block Malware
 - 3 - Malware Cloud Lookup
 - 4 - Detect Files
- 5 - Select the **Advanced** tab. Confirm that **Enable Custom Detection List** is selected.
 6 - Check the **Inspect Archives** checkbox.

General		<input type="button" value="Revert to Defaults"/>
First Time File Analysis	0	
Enable Custom Detection List	0	
Enable Clean List	0	
Mark files as malware based on dynamic analysis threat score	Very High	
Archive File Inspection	0	
Inspect Archives	0	
Block Encrypted Archives	1	
Block Uninspectable Archives	0	
Max Archive Depth	2 → Enter a value between 1 and 3	

NOTE: Archives unable to be inspected are corrupt archive, or archives with a depth that exceeds the Max Archive Depth.

14. Click the **Save** button in the upper-right to save the file policy.

NOTE: Archives unable to be inspected are corrupt archive, or archives with a depth that exceeds the Max Archive Depth.

15. Click the **Save** button in the upper-right to save the file policy.

Configuration A1.3: Demo intrusion policy

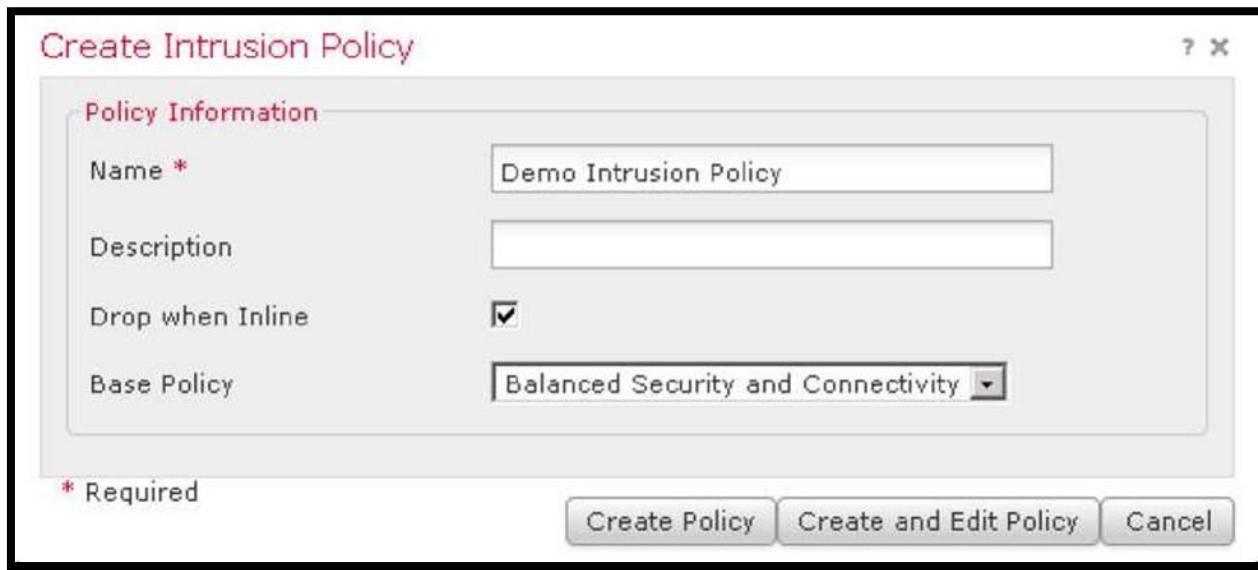
1. **Navigate to Objects > Intrusion Rules.** **Click Import Rules.**
 - a. **Select the Rule update or text rule file to upload and install radio button.**
 - b. **Click Browse,** and open the **Snort_Rules.txt** file in the **Files** folder of the Jump desktop.

NOTE: This file contains 2 simple Snort rules that are useful for testing IPS. They do not resemble published snort rules.

```
alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR"; sid: 1001001; rev:1;) alert tcp any any -> any any (msg:"ProjectZ detected"; content:"ProjectZ"; sid: 1001002; rev:1;)
```

The first rule replaces the string ProjectQ with ProjectR. The second detects the string ProjectZ. Since the rules do not specify where the string is in the flow, they could cause issues in a production deployment.

- c. **Click Import.** The import process will take a minute or two. When it completes you will see the **Rule Update Import Log page.** Confirm that 2 rules were successfully imported.
2. **Navigate to Policies > Access Control > Intrusion.**
3. **Click Create Policy.**
 - a. **Set Name to Demo Intrusion Policy.**
 - b. Make sure that **Drop when Inline** is checked.
 - c. Select **Balanced Security and Connectivity** as **Base Policy.**



- d. **Click Create and Edit Policy.**
4. You will now modify the rules states for this new policy.
 - a. **Click Rules** under Policy Information menu on the left-hand side of the **Edit Policy** page.
 - b. Select **local** from the Category section of the rules. You should see the 2 uploaded rules. The light green arrows on the right of each rule indicate that the rules are disabled for this policy.

- c. Check the checkbox next to the first rule. Select Generate Events from the Rule State drop-down menu. Click OK. Uncheck the checkbox next to the first rule.
- d. Check the checkbox next to the second rule. Select Drop and Generate Events from the Rule State drop-down menu. Click OK.
- e. Clear the filter by clicking on the X on the right side of the Filter text field.
- f. Select **SID** from the **Rule Content** section of the rules. Enter 336 into the **Enter the SID** filter popup. Click **OK**.
- g. Check the checkbox next to the rule. Select **Drop and Generate Events** from the **Rule State** drop-down menu. Click OK.

NOTE: This rule looks for a change to the root home directory in FTP traffic established on port 21. It only looks for traffic coming from the external network, but in our lab we use the default value of \$EXTERNAL_NET, which is any, so the rule can be triggered in both directions.

An interesting exercise would be to modify this rule to search in FTP traffic in any direction, and to use the appid attribute to detect FTP traffic on any port.

Click **Policy Information** in the menu on the upper-left.

Click **Commit Changes**.

Click **OK**.

Configuration A1,4: Demo SSL policy

1. **Navigate to** Objects > Object Management > PKI > Internal CAs.
 - a. Click **Import CA**.
 - b. For **Name**, enter Verifraud.
 - c. Click the **Browse** button to the right of the text **Certificate Data or, choose a file**.
 - d. Browse to the **Certificates** folder on the Jump desktop.
 - e. **Upload** Verifraud_CA.cer.
 - f. Click the **Browse** button to the right of the text **Key or, choose a file**.
 - g. **Upload** Verifraud_CA.key.
 - h. Click **Save**.
2. You will exempt from decryption infrastructure devices, such as the FMC and AMP Private Cloud. To do this, create a network object that includes these devices.
 - a. **Navigate to** Objects > Object Management > Network.
 - b. **Click** Add Network > Add Object.
 - c. For **Name**, enter Infrastructure.
 - d. For Network, enter 198.19.10.80-198.19.10.130.

- e. Click **Save** to save the network object.
3. Navigate to **Policies > Access Control > SSL**.
3. Click the text **Add a new policy** or click the **New Policy** button.
 - a. For **Name**, enter Demo ssl Policy.
 - b. Leave the default action to **Do not decrypt**.
 - c. Click **Save**. Wait a few seconds, and the policy will open for editing.
4. Click **Add Rule**.
 - a. For **Name**, enter Exempt Infrastructure.
 - b. Leave Action **set to** Do Not decrypt.
 - c. In the Networks tab, under Networks, select Infrastructure, and click Add to Source.
 - d. Click **Add** to add this rule to the SSL policy.
5. Click **Add Rule**.
 - a. For **Name**, enter Decrypt Search Engines.
 - b. Set Action **to** Decrypt - Resign.
 - c. Select Verifraud from the drop-down list to the right of the word **with**.
 - d. In the Applications tab, under Application Filters, search for **Sear**. You will see **Search Engine** under Categories. Check this checkbox, and click **Add to Rule**.
 - e. Select the **Logging** tab, and check the **Log at End of Connection** checkbox.
 - f. Click **Add** to add this rule to the SSL policy.
6. Click **Add Rule**.
 - a. For Name, enter **Decrypt Other**.
 - b. Set Action **to** Decrypt - Resign.
 - c. Select Verifraud from the drop-down list to the right of the word **with**.
 - d. Select the **Logging** tab, and check the **Log at End of Connection** checkbox.
 - e. Click **Add** to add this rule to the SSL policy.
7. Click **Save** to save the SSL policy.

NOTE: The Replace Key checkbox deserves explanation. Whenever the action is set to Decrypt - Resign, Firepower will replace the public key. The Replace Key checkbox determines how the decrypt action is applied to self-signed server certificates.

If Replace Key is deselected, self-signed certificates are treated like any other server certificates. Firepower replaces the key, and resigns the certificate. Generally the endpoint is configured to trust Firepower, and therefore will trust this resigned certificate.

If Replace Key is selected, self-signed certificates are treated differently. Firepower replaces the key, and generates a new self-signed cert. The browser on the endpoint will generate a certificate warning.

In other words, checking the Replace Key checkbox makes the resign action preserve lack-of-trust for self-signed certificates.

Configuration A1,5: Custom detection list

There is a harmless file called Zombies.pdf that will trigger a malware event, assuming the cloud lookup succeeds. Sometimes labs have issues with cloud connectivity. Therefore, this is added to the custom detection list to ensure it will trigger a malware event.

1. **Navigate to** Objects > Object Management > File List.
2. Click the pencil icon to edit the **Custom-Detection-List**.
 - a. Select **Calculate SHA** from the **Add by** drop-down list.
 - b. Click **Browse**.
 - c. Browse to the Files folder on the Jump desktop.
 - d. Select **Zombies.pdf**, and click **OK**.
 - e. Click **Calculate and Add SHAs**.
 - f. Click **Save**.

Configuration A1,6: Add restapiuser

It is convenient to have a separate user to use the API Explorer. This allows use of both the FMC and API Explorer at the same time.

1. **Navigate to** System > Users. Click **Create User**.
 - a. For **User Name**, enter restapiuser.
 - b. For **Password**, enter **C1sco12345** Confirm the password.
 - c. Set Maximum Number of Failed Logins to 0.
 - d. Check the **Administrator** checkbox.

Configuration A1,7: Install server certificate

By default the FMC UI uses a self-signed certificate. This is replaced by a certificate signed by the pod AD server, which the Jump browsers trust.

1. **Navigate to** Objects > Object Management > PKI > Trusted CAs.
 - a. Click **Add Trusted CA**.
 - b. For **Name**, enter **dCloud**.
 - c. Click the **Browse** button to the right of the text **Certificate Data or, choose a file**.
 - d. Browse to the **Certificates** folder on the Jump desktop.
 - e. Upload **AD-ROOT-CA-CERT.cer**.
 - f. Click **Save**.

2. Connect to the FMC CLI via SSH. Become root by typing **sudo -i**. The Sudo password is **C1sco12345**

- a. **Type** cd /etc/ssl **and then type** cp server* /root.
- b. **Type** cat > /etc/ssl/server.crt
- c. From the **Certificates** folder on the Jump desktop edit the file **fmc.cer** with Notepad++.
- d. Select all, and then copy and paste into the FMC CLI
- e. Type **Ctrl+D**.
- f. **Type** cat > /etc/ssl/server.key
- g. From the **Certificates** folder on the Jump desktop edit the file **fmc.key** with Notepad++.
- h. Select all, and then copy and paste into the FMC CLI
- i. Type **Ctrl+D**.
- j. **Type** pmtool restartbyid httpsd.

Appendix B. REST API Scripts

Here are the two Python scripts that were used in the first lab exercise. You only run the first script **register_config.py**. It will call the second script **connect.py**, which will create the compiled file **connect.pyc**.

Python script register_config.py

```
#!/usr/bin/python import json import connect import sys host = "fmc.example.com"
username = "restapiuser" password = "C1sco12345" name="NGFW"
#connect to the FMC API headers,uuid,server = connect.connect (host, username, password) user_input
= str(raw_input("Would you like to register the managed device? [y/n]")) if user_input == "y":
policy_name = str(raw_input("Enter name of new Access Control Policy to be create:")) access_policy = {
"type": "AccessPolicy",
"name": policy_name,
"defaultAction": { "action": "BLOCK" }
} post_response = connect.accesspolicyPOST(headers,uuid,server,access_policy)
policy_id = post_response["id"] print "\n\nAccess Control Policy\n" + policy_name +
"\ncreated\n" device_post = { "name": name,
"hostName": "ngfw.example.com",
"regKey": "C1sco12345",
"type": "Device",
"license_caps": [
"BASE",
"MALWARE",
"URLFilter",
"THREAT"
],
"accessPolicy": {
"id": policy_id,
"type": "AccessPolicy"
} } post_data = json.dumps(device_post) output = connect.devicePOST (headers, uuid, server,
post_data) print "\n\nPost request is: \n" + json.dumps(output,indent=4) + "\n\n" GET ALL THE
DEVICES AND THEIR corresponding interfaces user_input = str(raw_input("In the FMC UI, confirm that
the device discovery has completed and then press 'y' to continue or 'n' to exit. [y/n]"))
headers,uuid,server = connect.connect (host, username, password) if
user_input == "n": quit()
devices = connect.deviceGET(headers,uuid,server) for device in devices["items"]:
if device["name"] == name: print "DEVICE FOUND, setting ID" device_id = device["id"] NOW THAT WE HAVE THE DEVICE ID WE
NEED TO GET ALL THE INTERFACES interfaces = connect.interfaceGET(headers,uuid,server,device id)
Interfaces i want to change interface_1 = "GigabitEthernet0/0" interface_2 =
"GigabitEthernet0/1" for interface in interfaces["items"]:
if interface["name"] == interface_1:
interface_1_id = interface["id"] print "interface 1 found" if interface["name"] == interface_2:
interface_2_id = interface["id"] print "interface 2 found" user_input = str(raw_input("Would you
like to configure device interfaces? [y/n]")) if user_input == "y": interface_put = {
"type": "PhysicalInterface",
"hardware": {
```

```

"duplex": "AUTO",
"speed": "AUTO"
},
"enabled": True,
"MTU": 1500,
"managementOnly": False,
"ifname": "outside",
"enableAntiSpoofing": False,
"name": "GigabitEthernet0/0",
"id": interface_1_id,
"ipv4" : {
"static": {
"address": "198.18.133.2",
"netmask": "18"
}
} } put_data = json.dumps(interface_put) connect.interfacePUT (headers, uuid, server,
put_data, device_id, interface_1_id) interface_put = {
"type": "PhysicalInterface",
"hardware": {
"duplex": "AUTO",
"speed": "AUTO"
},
"enabled": True,
"MTU": 1500,
"managementOnly": False,
"ifname": "inside", "enableAntiSpoofing": False,
"name": "GigabitEthernet0/1",
"id": interface_2_id,
"ipv4" : {
"static": {
"address": "198.19.10.1",
"netmask": "24"
}
} } put_data = json.dumps(interface_put) connect.interfacePUT (headers, uuid,
server, put_data, device_id, interface_2_id)

```

Python script connect.py

```

#!/usr/bin/python import json import sys import requests #Surpress
HTTPS insecure errors for cleaner output from
requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
#define fuction to connect to the FMC API and generate authentication token def connect (host, username,
password): headers = {'Content-Type': 'application/json'} path =
"/api/fmc_platform/v1/auth/generatetoken" server = "https://" + host url = server + path try:
r = requests.post(url, headers=headers, auth=requests.auth.HTTPBasicAuth(username,password),
verify=False) auth_headers = r.headers token = auth_headers.get('X-auth-access-token',
default=None) uuid = auth_headers.get('DOMAIN UUID', default=None) if token == None:
print("No Token found, I'll be back terminating....") sys.exit()
except Exception as err:
print ("Error in generating token --> " + str(err)) sys.exit() headers['X-auth-access-token'] =
token return headers,uuid,server

```

```
def devicePOST (headers, uuid, server, post_data): api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords url = server+api_path try:  
r = requests.post(url, data=post_data, headers=headers, verify=False) status_code = r.status_code resp = r.text json_response = json.loads(resp) print("status code is: " + str(status_code)) if status_code == 201 or status_code == 202: print("Post was sucessfull...") else:  
r.raise_for_status() print("error occured  
in POST -->" + resp) except  
requests.exceptions.HTTPError as err: print  
("Error in connection --> " + str(err))  
finally:  
if r: r.close() return json_response def deviceGET (headers, uuid, server): api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords" url = server+api_path try: r = requests.get(url, headers=headers, verify=False) status_code = r.status_code resp = r.text json_response = json.loads(resp) print("status code is: " + str(status_code)) if status_code == 200: print("GET was sucessfull...") else:  
r.raise_for_status() print("error occured  
in POST -->" + resp) except  
requests.exceptions.HTTPError as err: print  
("Error in connection --> " + str(err))  
finally:  
if r: r.close() return json_response def interfaceGET (headers, uuid, server, device_id):  
api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords/" + device_id + "/physicalinterfaces" url = server+api_path try:  
r = requests.get(url, headers=headers, verify=False) status_code = r.status_code resp = r.text json_response = json.loads(resp) print("status code is: " + str(status_code)) if status_code == 200: print("GET was sucessfull...") else:  
r.raise_for_status() print("error occured  
in POST -->" + resp) except  
requests.exceptions.HTTPError as err: print  
("Error in connection --> " + str(err))  
finally:  
if r: r.close() return json_response def interfacePUT (headers, uuid, server, put_data, device_id, interface_id):  
api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords/" + device_id + "/physicalinterfaces/" + interface_id url = server+api_path try:  
r = requests.put(url, data=put_data, headers=headers, verify=False) status_code = r.status_code resp = r.text json_response = json.loads(resp) print("status code is: " + str(status_code)) if status_code == 200 : print("Put was sucessfull...") else:  
r.raise_for_status()  
print("error occured in POST -->" + resp) except  
requests.exceptions.HTTPError as err: print  
("Error in connection --> " + str(err)) finally:  
if r: r.close() return json_response def accesspolicyPOST (headers, uuid, server, post_data):  
api_path= "/api/fmc_config/v1/domain/" + uuid + "/policy/accesspolicies" url = server+api_path try:
```

```
r = requests.post(url, data=json.dumps(post_data), headers=headers, verify=False) status_code =
r.status_code resp = r.text json_response = json.loads(resp) print("status code is: "+
str(status_code)) if status_code == 201 or status_code == 202: print("Post was sucessfull...") else:
r.raise_for_status() print("error occured in POST -->" +resp) except
requests.exceptions.HTTPError as err: print ("Error in connection --> " +str(err))
finally:
if r: r.close() return json_response
```

Appendix C. ISE RA VPN Configuration

ISE was configured to support all the lab exercises. In this appendix, this configuration is summarized. Note that there is an ISE link on the Firefox bookmarks toolbar. The credentials should prepopulate. They are username **admin**, password **C1sco12345**

NOTE: This appendix is not a tutorial on ISE. It does not go into details about how ISE is configured. It only covers the details required to configure RA VPN components for the lab exercises in this guide. The configurations are described in a top-down manor. To create this configuration, you would probably prefer to build these objects from the bottom-up.

Authorization policies

1. Navigate to **Policy > Authorization**. The first two policies were created for this lab: **AC-IT-Policy** and **AC-Default-Policy**. These policies reference two authorization profiles: AC-Auth-IT and AC-Auth-Default.

Authorization profiles

1. **Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles.** **The first two profiles were created for this lab:** AC-Auth-Default **and** AC-Auth-IT.
2. If you drill down into **AC-Auth-Default**, you will see that it references the **DACL AC-DACL-Default**, described below.
3. If you drill down into **AC-Auth-IT**, you will see that it references the **DACL AC-DACL-IT**, described below. It also has two advanced attributes: one for the address pool, and one for the group policy.

The screenshot displays the configuration interface for an Authorization Profile in Cisco ISE. It is divided into three main sections:

- Common Tasks:** Contains a dropdown menu for "DACL Name" set to "AC-DACL-IT". Other options like "ACL (Filter-ID)", "VLAN", and "Voice Domain Permission" are shown but not selected.
- Advanced Attributes Settings:** Shows two entries under "Cisco-VPN3000": "Cisco-VPN3000:CVPN3000/ASA/f = AC-IP-Pool-IT" and "Cisco-VPN3000:CVPN3000/ASA/f = ITGP".
- Attributes Details:** Displays the following configuration details:
 - Access Type = ACCESS_ACCEPT
 - DACL = AC-DACL-IT
 - CVPN3000/ASA/PIX7x-Address-Pools = AC-IP-Pool-IT
 - CVPN3000/ASA/PIX7x-IPSec-Group-Policy = ITGP

Downloadable ACLs

1. Navigate to **Policy > Policy Elements > Authorization > Downloadable ACLs**. The first two DACLs were created for this lab: **AC-DACL-Default** and **AC-DACL-IT**.

Name	Description
AC-DACL-Default	Deny all traffic
AC-DACL-IT	Allow all traffic

2. If you drill down into **AC-DACL-Default**, you will see that it restricts access to 198.19.10.100 and 198.19.10.200.

* Name	AC-DACL-Default
Description	
* ACL Content	1234567 permit ip any host 198.19.10.100 8910111 permit ip any host 198.19.10.200 2131415 deny ip any any 1617181 9202122 2324252 6272829 3031323 3343536 3738394

Check ACL Syntax

3. If you drill down into **AC-DACL-IT**, you will see that there are no restrictions.

Downloadable ACL List > AC-DACL-IT

Downloadable ACL

* Name

Description

* DACL Content
891011
2131415
1617181
9202122
2324252
6272829
3031323
3343536
3738394



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)