Cisco dCloud

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

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.

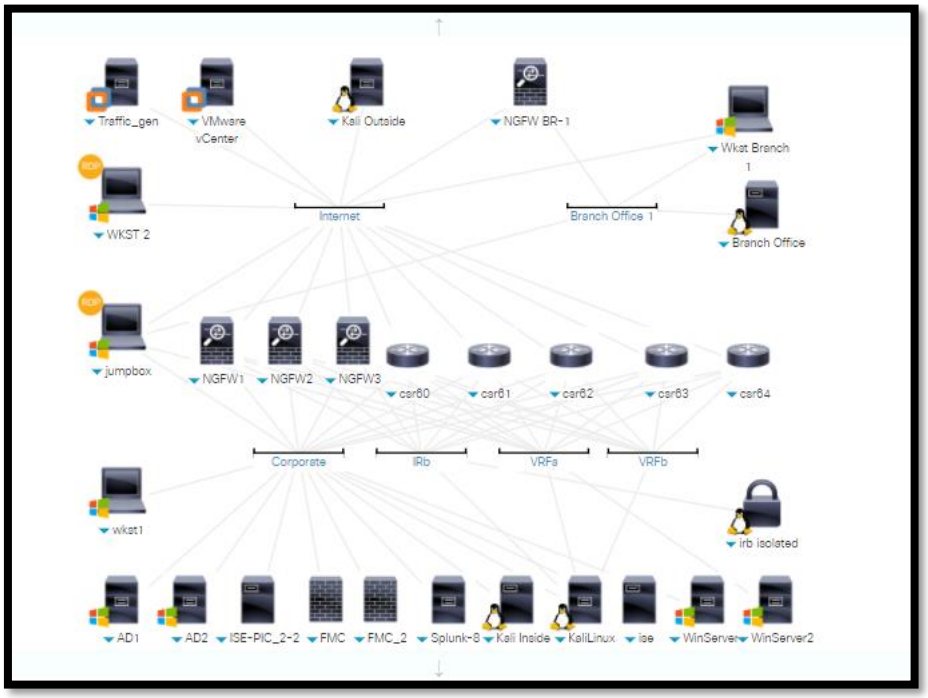
This allows the Cisco Firepower NGFW to evolve with a focus on enabling enterprises to stop, prioritize, understand, and automate responses to modern threats in real-time. Firepower NGFW is unique in its threat-focus, with a foundation of comprehensive network visibility, best-of-breed threat intelligence 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

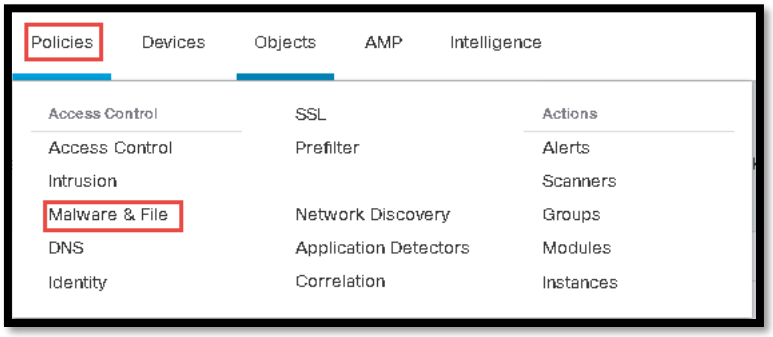
Scenario 1. File & Malware Policy

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

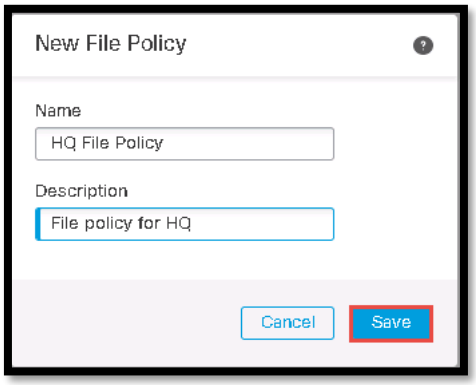
Create Malware & File Policy

1. Login to the FMC **admin/C1sco12345**
2. Click **Policies** and select **Malware & File**



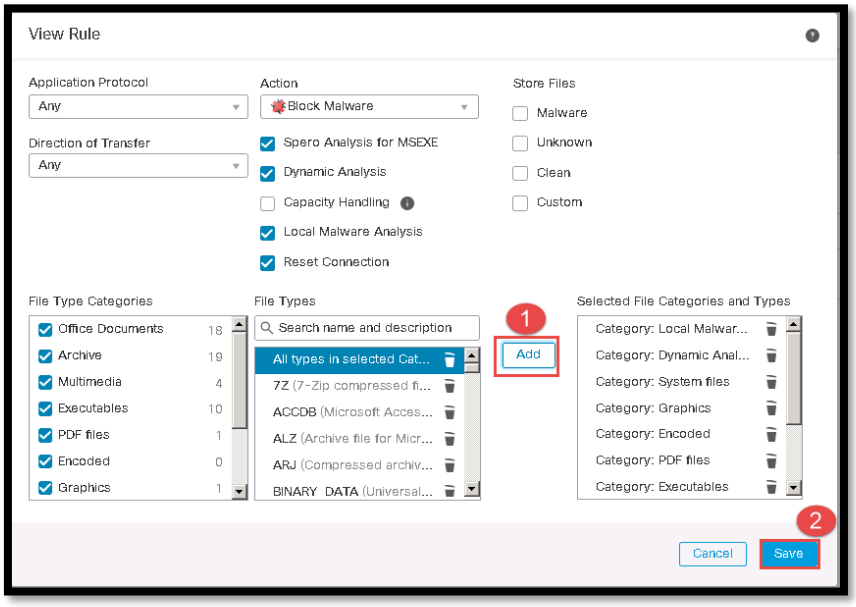
3. Click **New File Policy**

4. Enter the following:
    a. Name: **HQ File Policy**
    b. Description: **File policy for HQ**

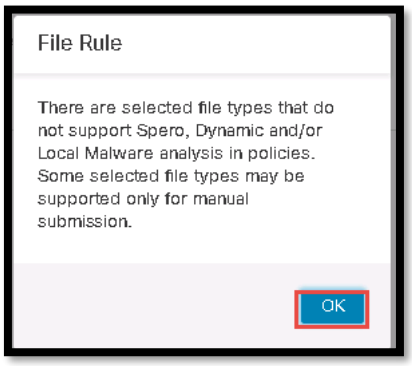


5. **Save**
6. Click **Add Rule**
7. Configure the rule to apply to all possible protocols and file types with the following:
    a. Application Protocol: **Any**
    b. Direction of Transfer: **Any**
    c. Action: **Block Malware**
    d. Spero Analysis for MSEXE: **checked**
    e. Dyanamic Analsys: **checked**
    f. Local Malware Analysis: **checked**
    g. Reset Connection: **checked**

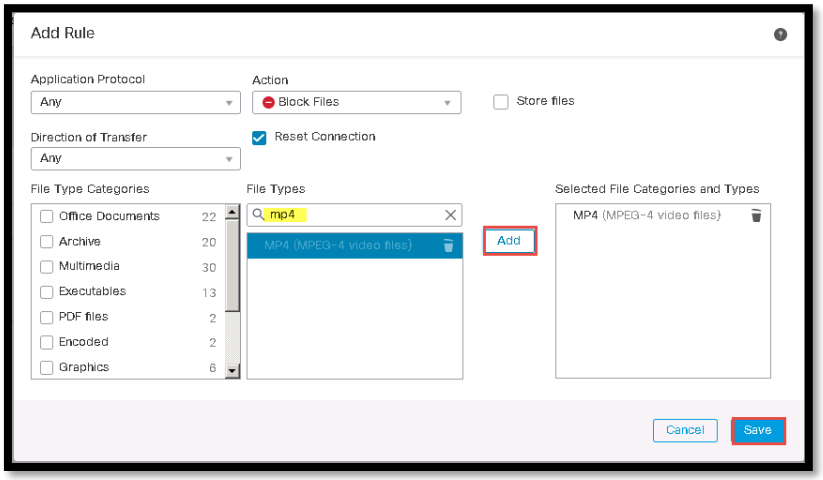
h. File type Categories: **(place a checkmark in all categories)**
i. File types: All types in selected Categories



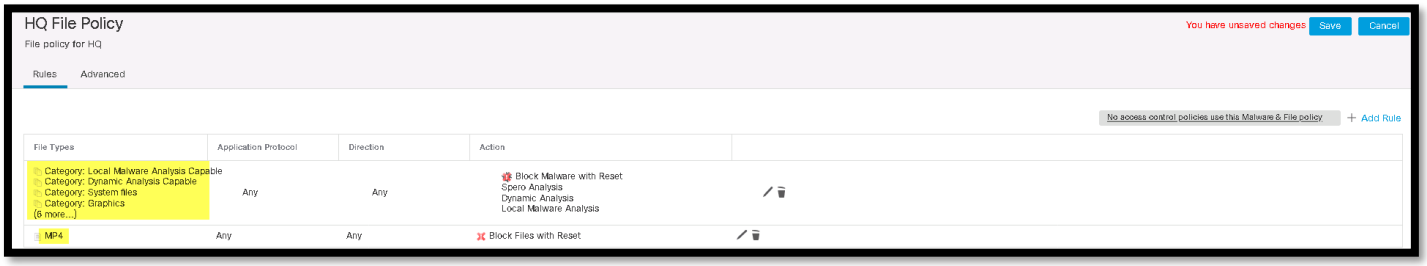
8. Click **Add** and **Save**
9. Click **OK** on **File Rule** box



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

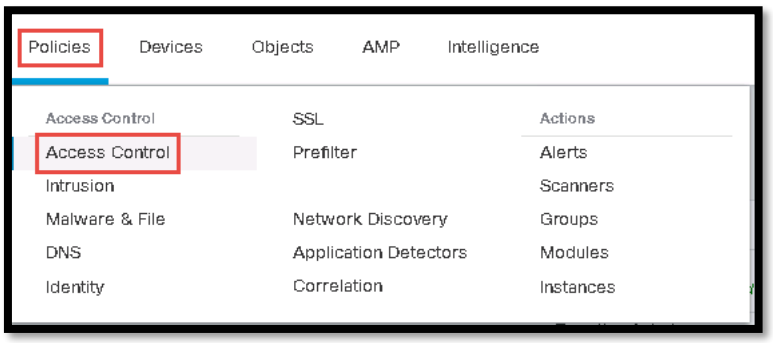


13. Click **Save**
14. The HQ File Policy should look like this:

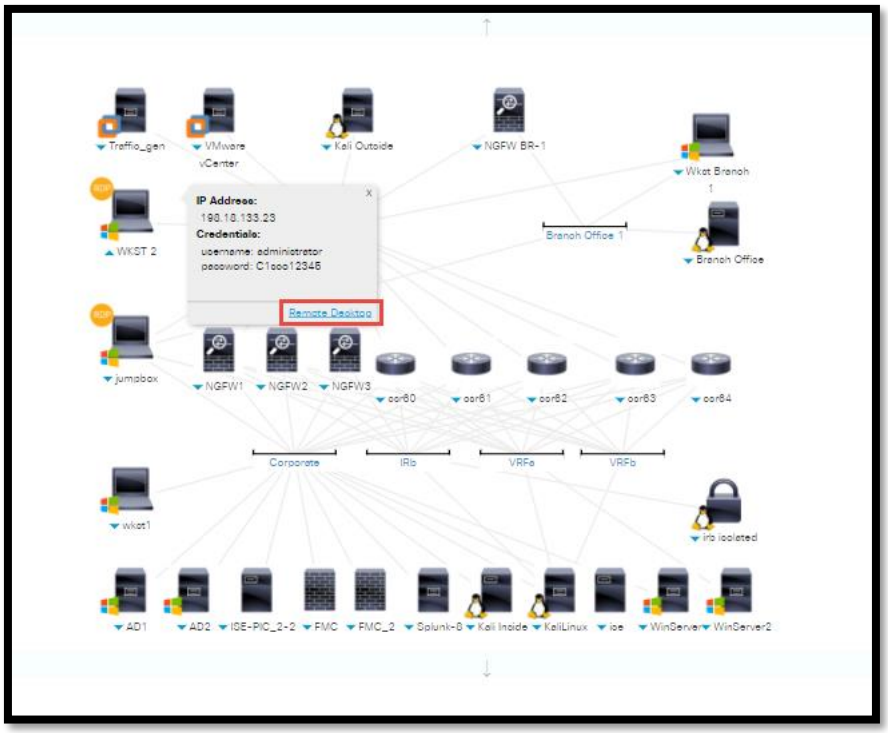


NOTE: You are blocking MP4 files as an example of a specific file type. The Firewall will block this file type regardless, if it is clean, unknown or malicious without further inspection. For customer deployments make sure you understand their requirements for file blocking.

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

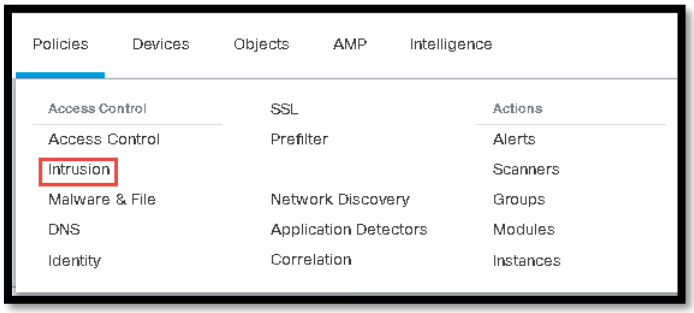
23. You have now Checked the HQ File Policy from OutZone to InZone1
    a. OPTIONAL
        i. Type **HTTPS://198.18.128.202**
            1. Try downloading **test1.mp4** it should succeed (This is because you are downloading the file over an encrypted connection so the traffic cannot be inspected. 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

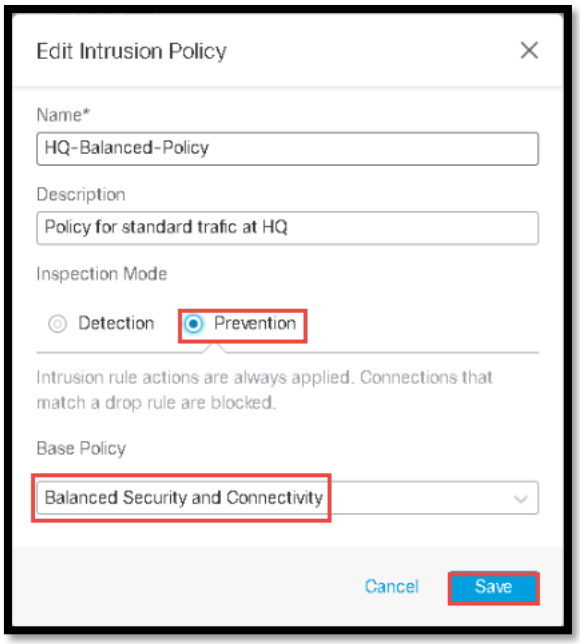
In this scenario we will configure and use custom IPS policies. You will make copies of the Balanced Security and Connectivity and Security Over Connectivity policies; modify the variables used by the policies and apply those polices to the ACP

Create IPS Policies

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

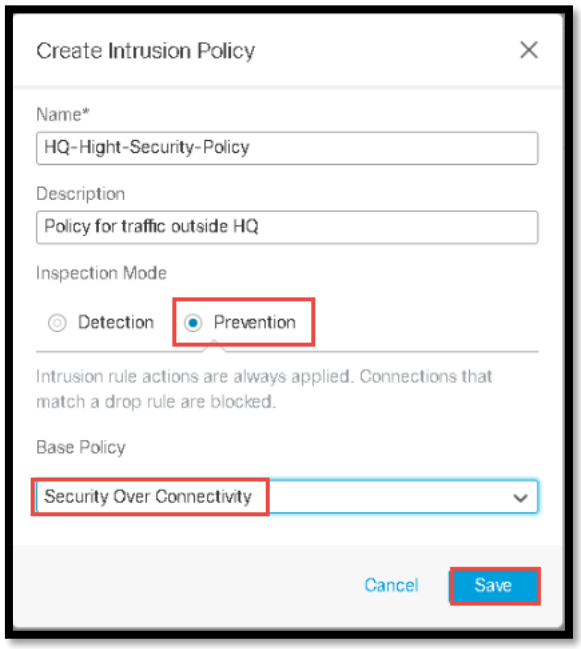


3. You will see that **Demo Intrusion Policy** is defined
4. Click **Create Policy** [Accept the warning if prompted]
5. Set the following values:
    a Name: **HQ-Balanced-Policy**
    b Description: **Policy for standard traffic at HQ**
    c Inspection Mode: **Prevention**
    d Base Policy: **Balanced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

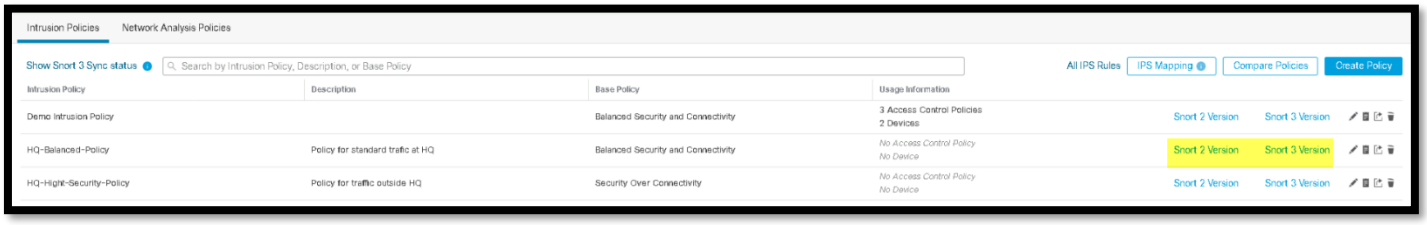


6. Click Create Policy

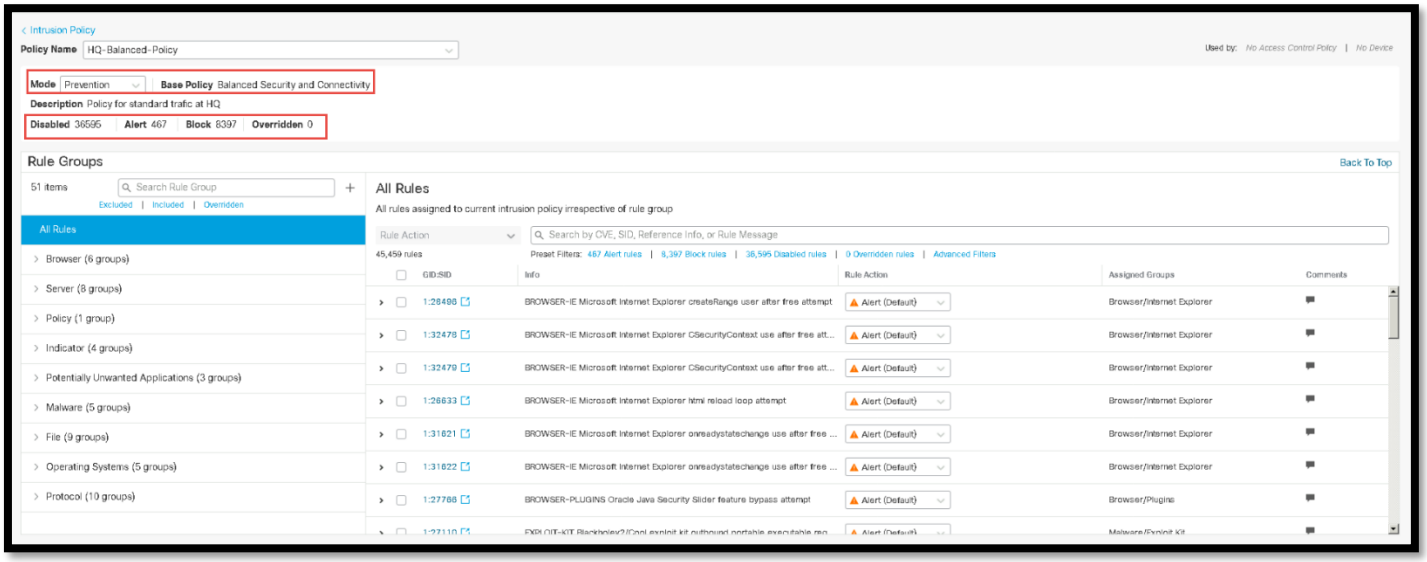
7. You will now create another policy. Click **Create Policy**
8. Set the following values:
    a Name: **HQ-High-Security-Policy**
    b Description: **Policy for traffic outside HQ**
    c Inspection Mode: **Prevention**
    d Base Policy: **Security Over Connectivity**



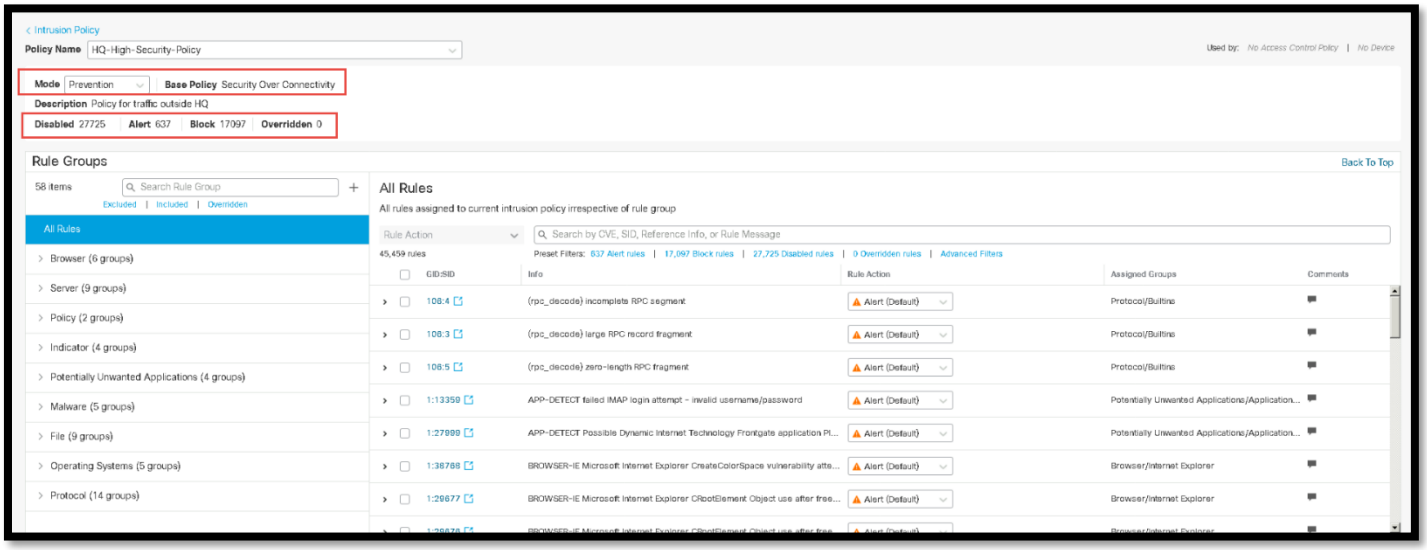
9. On the policies page click the **Snort 2 or Snort 3 Version**



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

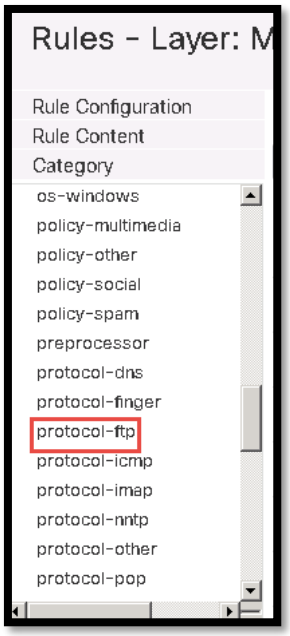


11. Click on **< Intrusion Policy** to go back to Intrusion Policies
12. Edit the **HQ-High-Security-Policy** and look at the number of rules.



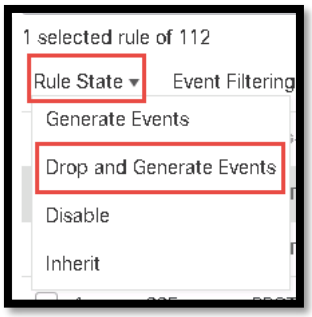
13. Add an Intrusion Rule to the Policy to **Snort 2 if you want Snort 3 start after Step (i)**
    a Click on **HQ-High-Security-Policy > Snort 2 Version**
    b Click on Policy Layers > My Changes click Manage Rules

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



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

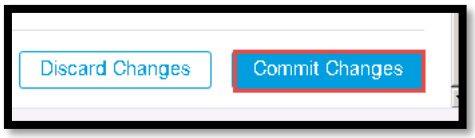
e Under Rule State choose: **Drop and Generate Events**



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**



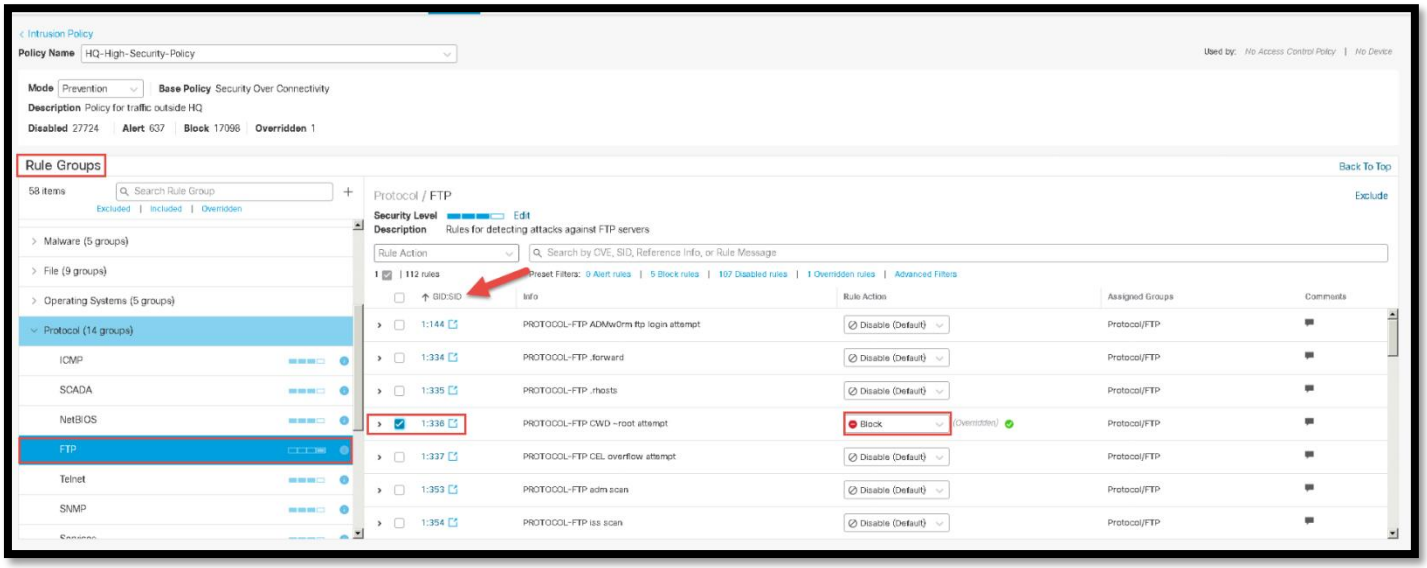
i In the Description of Changes window type: **Add FTP Intrusion Rule** and click **OK**

14. **SNORT 3**

a HQ-High-Security-Policy

i Snort 3 Version

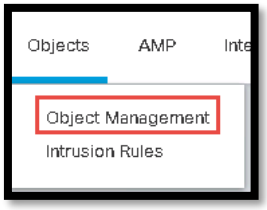
b Under tule Groups click on **Protocol and Select FTP and then click the SID to sort by number and select SID 336**



Customize IPS Variable Sets

You will now create Variable Sets for these policies.

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

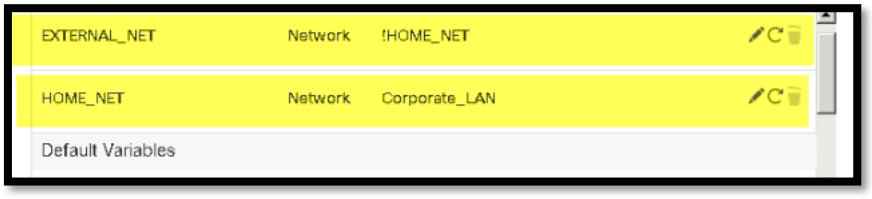


2. On the left window pane Click on **Variable Set**

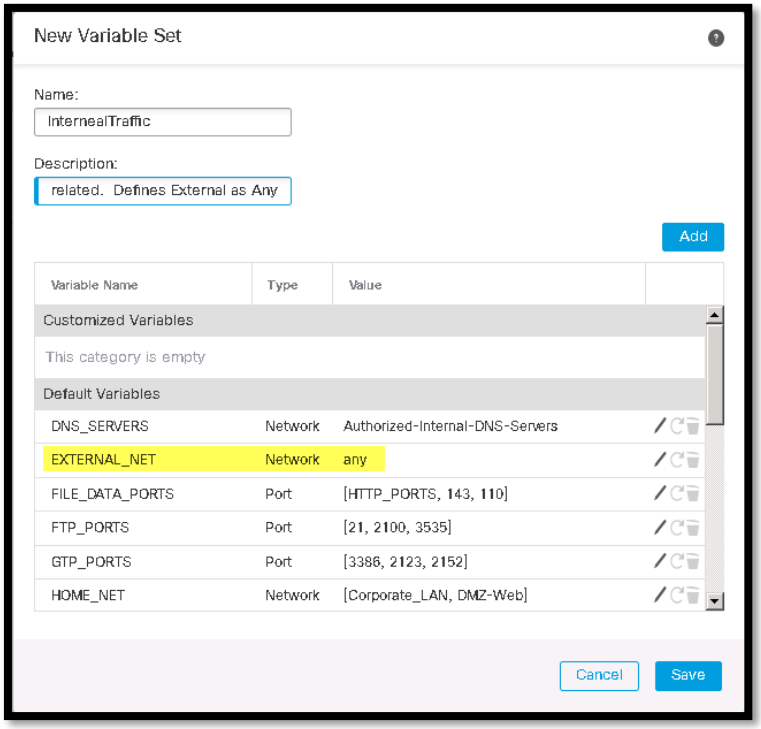
3. Click **Add Variable Set**
   a Name: **ExternalTraffic**
   b Description: **Used for rules involving an internet host. Defines External as anything not internal**
4. Click the **Edit** button for the **EXTERNAL_NET** variable
5. In the list of Available Networks select **HOME_NET** and click **Exclude** 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



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**



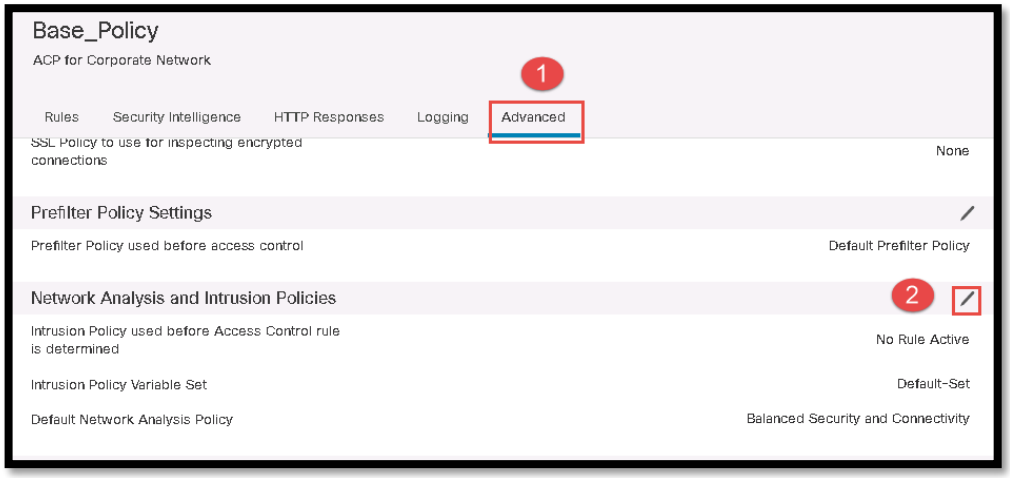
14. Click **Save**

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.

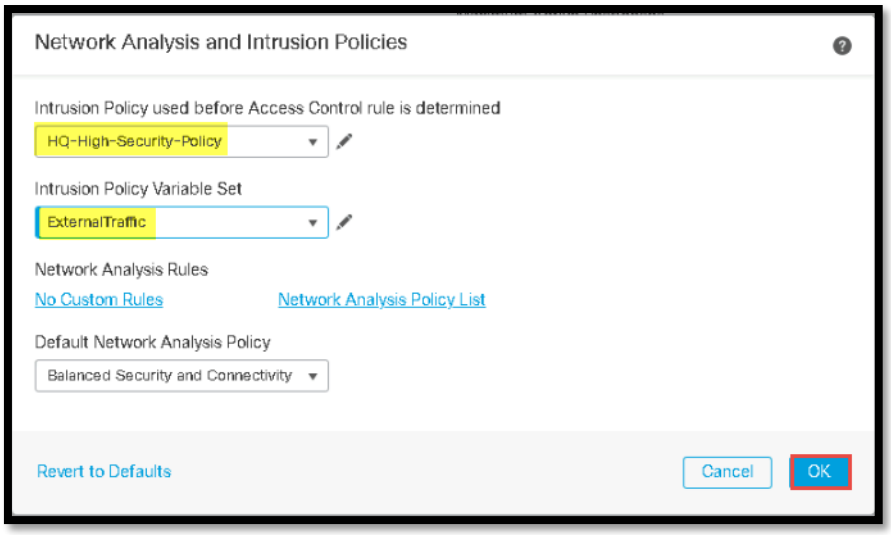
Configure ACP to Use IPS Policies

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

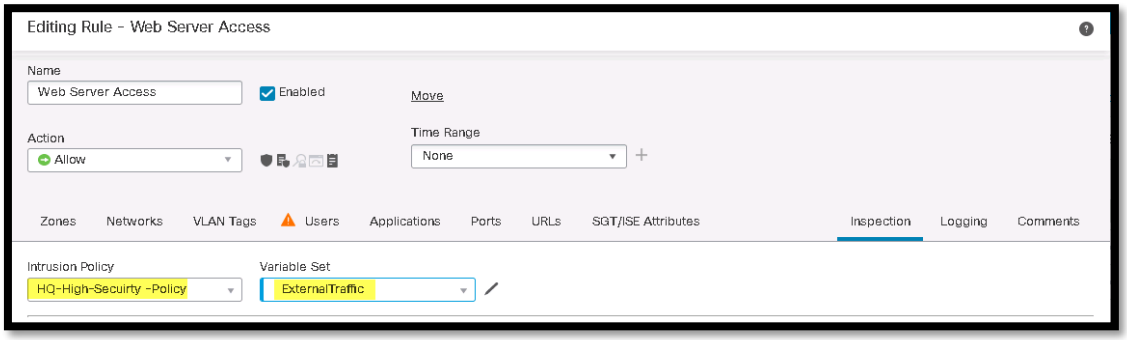
1. Click the **Policies** menu and select **Access Control**
2. Click on edit [Pencil] icon for the **Base_Policy**
3. Select the **Advanced** tab



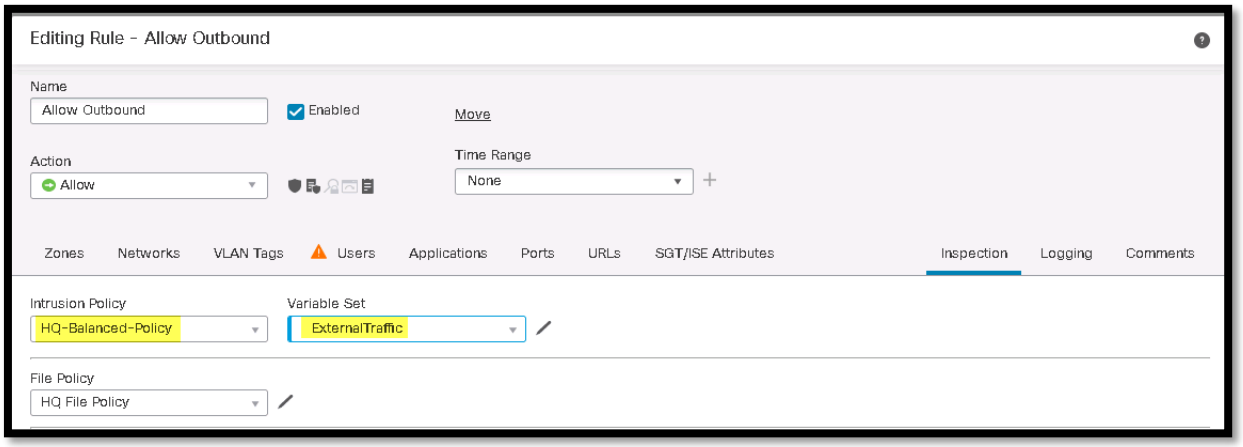
4. Click the **Edit** button for **Network Analysis and Intrusion Policies**
5. Configure the following:
    a Intrusion Policy used before Access Control rule is determined: **HQ-High-Security-Policy**
    b Intrusion Policy Variable Set: **ExternalTraffic**



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**



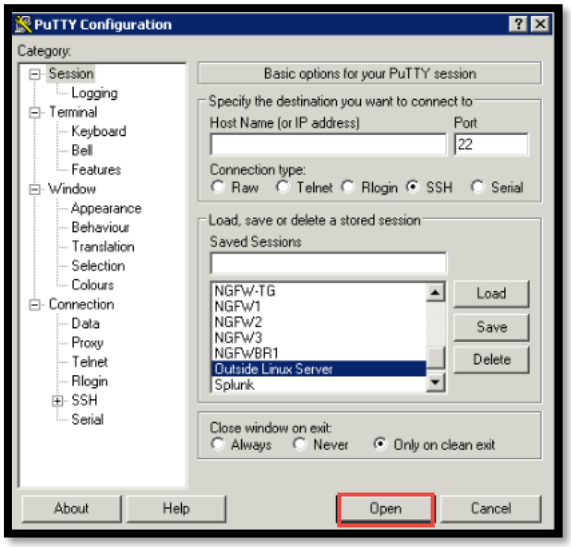
14. Click **Save**
15. **Save** the ACP and **Deploy**

Test IPS Polices

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**

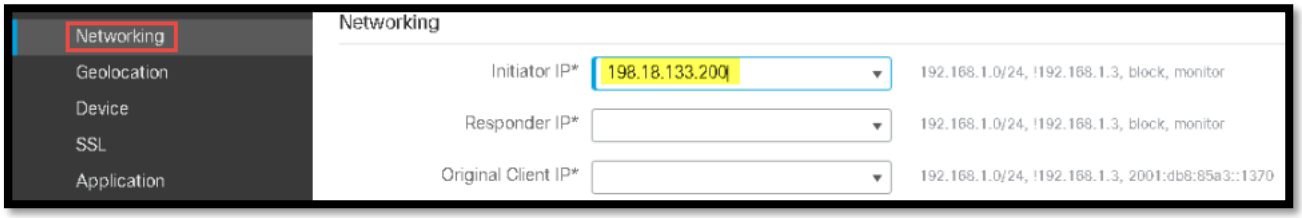
```
msf6 > use auxiliary/scanner/http/dir_webdav_unicode_bypass
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) > set RHosts 198.18.128.202
RHosts => 198.18.128.202
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass) > set THREADS 20
THREADS => 20
msf6 auxiliary(scanner/http/dir_webdav_unicode_bypass)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

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**

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



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

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

16. Click on the arrow next to the messages

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.dcoud.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

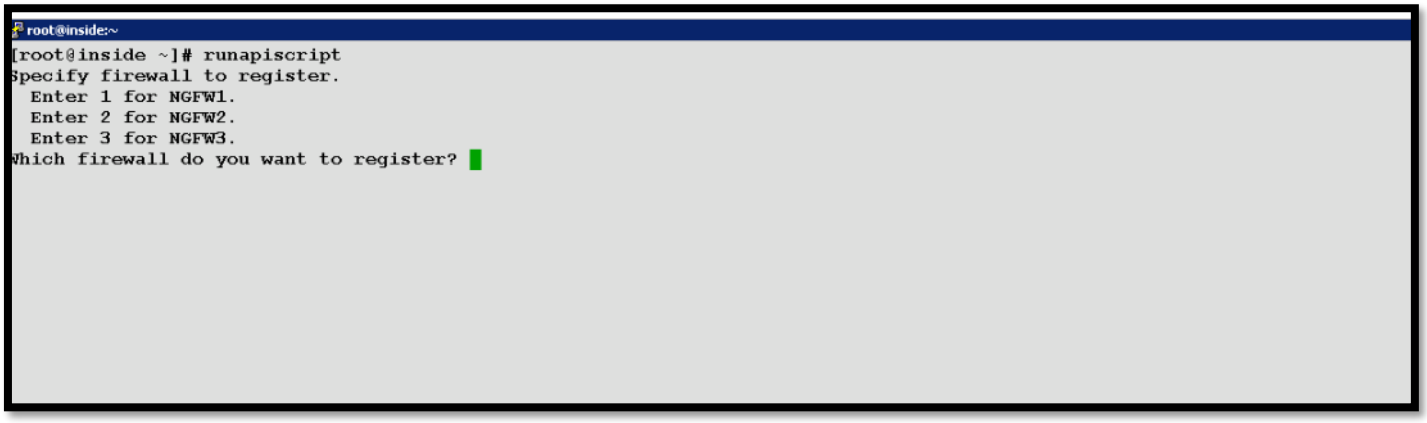
Creating or breaking a Firepower Threat Defense high availability pair immediately restarts the Snort process on the primary and secondary devices, temporarily interrupting traffic inspection on both devices. Whether traffic drops during this interruption or passes without further inspection depends 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]

a. Type **runapiscript** wait for the prompt

b. When asked **Which Firewall do you want to register?** Type the number **3**

c. When it asked **Enter name of new Access Control Policy to be create: (Type HA) for the name)**



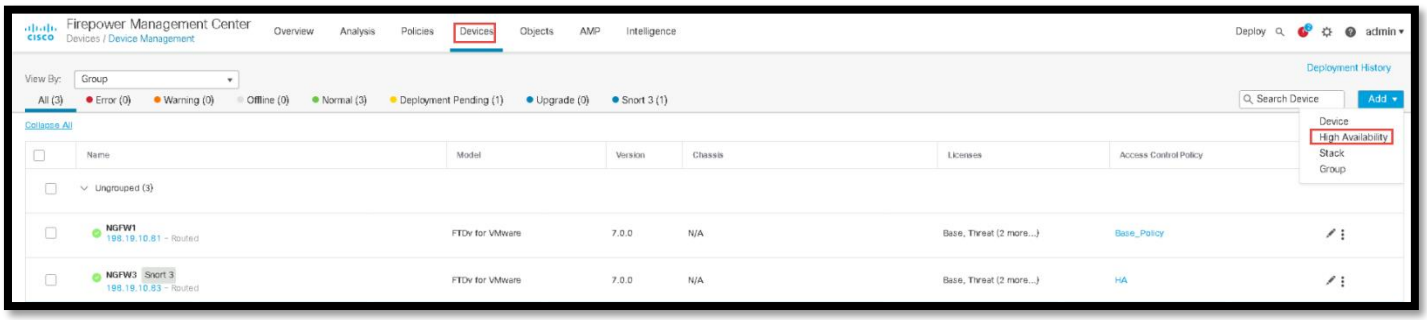
d. Go back to Firefox and check the registration status of NGFW3 on the FMC and allow device to register

e. Go to Device> Device Management> NGFW3 and enable the interfaces GigabitEthernet0/0-0/4 and remove the names from the interfaces

f. Click Save

Configure High Availability Pair

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



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.

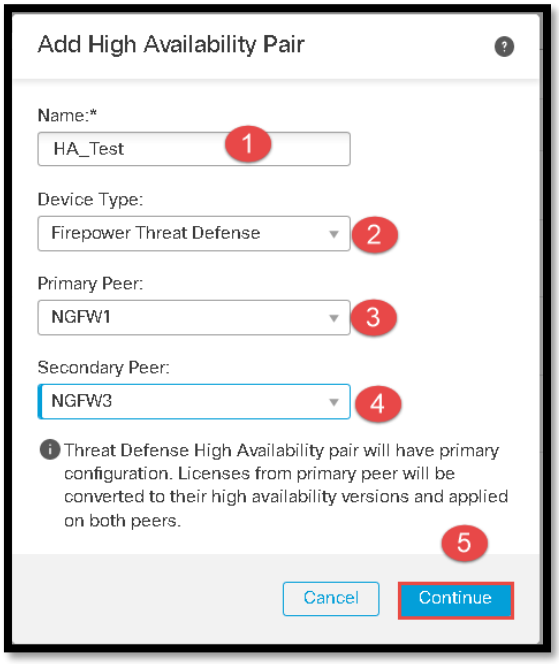
a Name: HA_Test

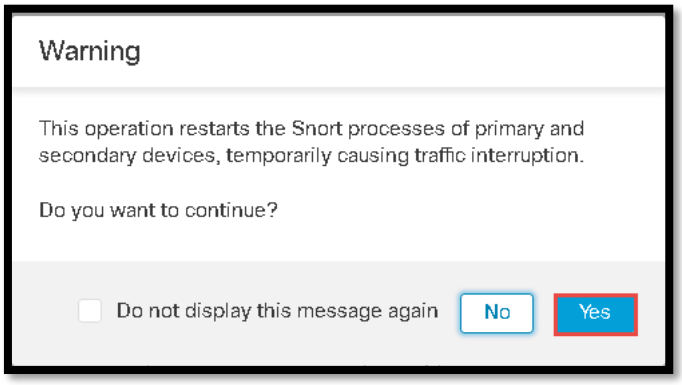
b Device Type: Firepower Threat Defense

c Primary Peer: NGFW1

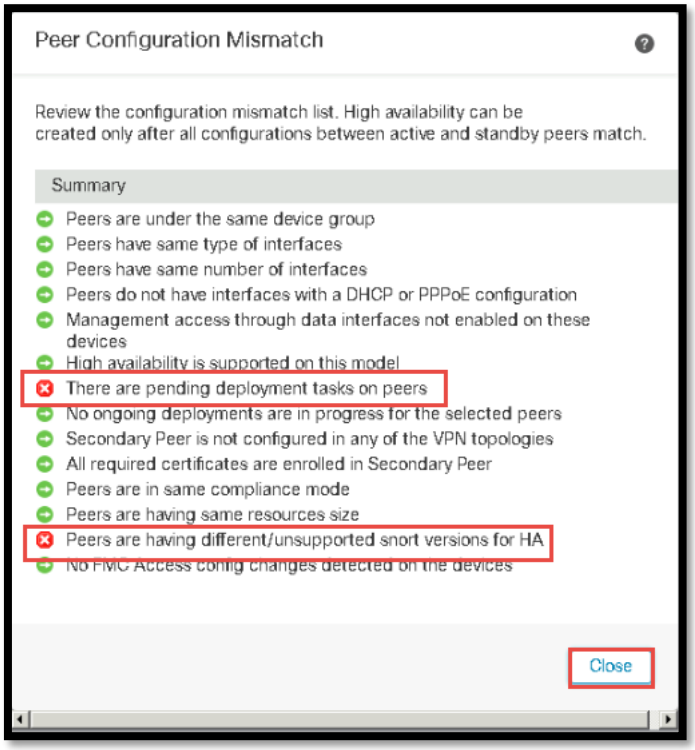
d Secondary Peer: NGFW3

e Then Continue



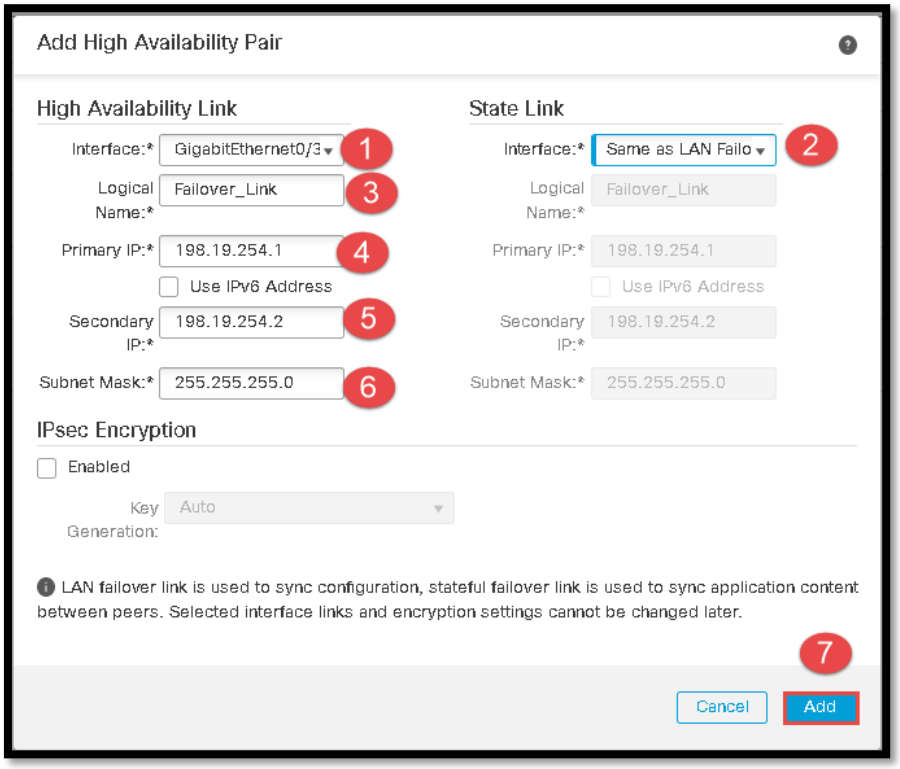


NOTE: If you have done configuration tasks on either of the HA Peers and have not deployed then you will get the following message:

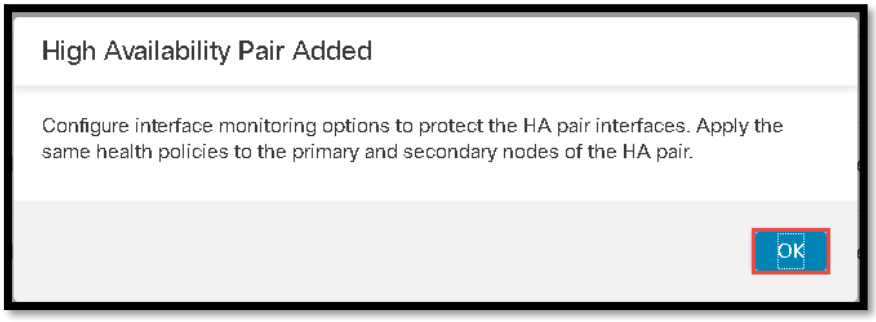


2. If needed On NGFW3 go to Device > Inspection Engine > Revert to Snort2
3. On NGFW1 go to GigabitEthernet0/3 Edit and delete the name and Security Zone of that Interface
4. Deploy the changes to NGFW1 and NGFW3
5. Go back and repeat step 1
6. Select Interface: GigabitEtherent0/3
7. Name: Failover_Link
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.



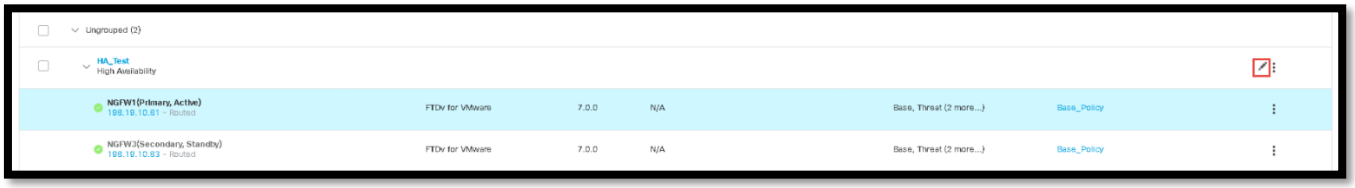
11. Click on OK to add the High Availability Pair



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.

12. When complete you will see the following:

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

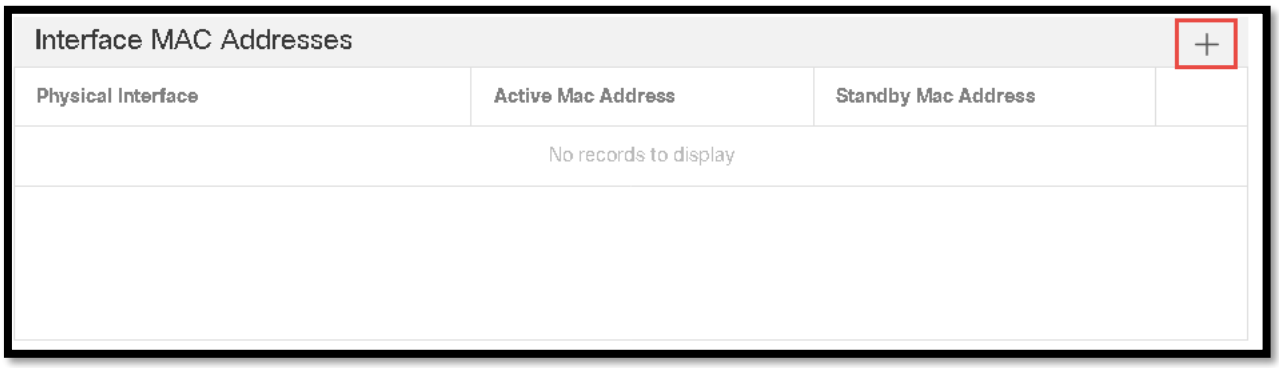
If the secondary unit boots without detecting the primary unit, the secondary unit becomes the active unit and uses its own MAC addresses, because it does not know the primary unit MAC addresses. However, when the primary unit becomes available, the secondary (active) unit changes the MAC addresses to 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.

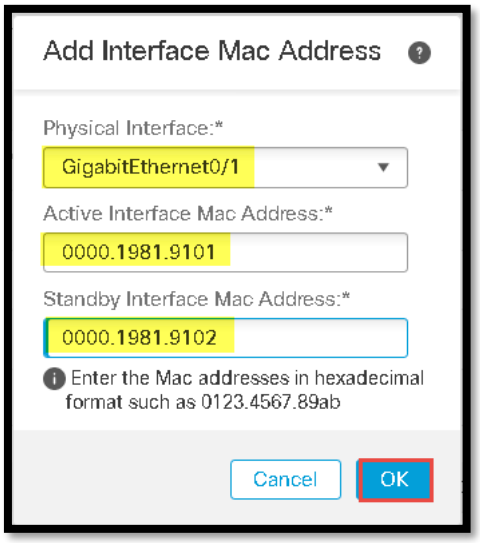
The IP address and MAC address for the state link do not change at failover; the only exception is if the state link is configured on a regular data interface.

14. Select the “+” icon next to the Interface MAC Address



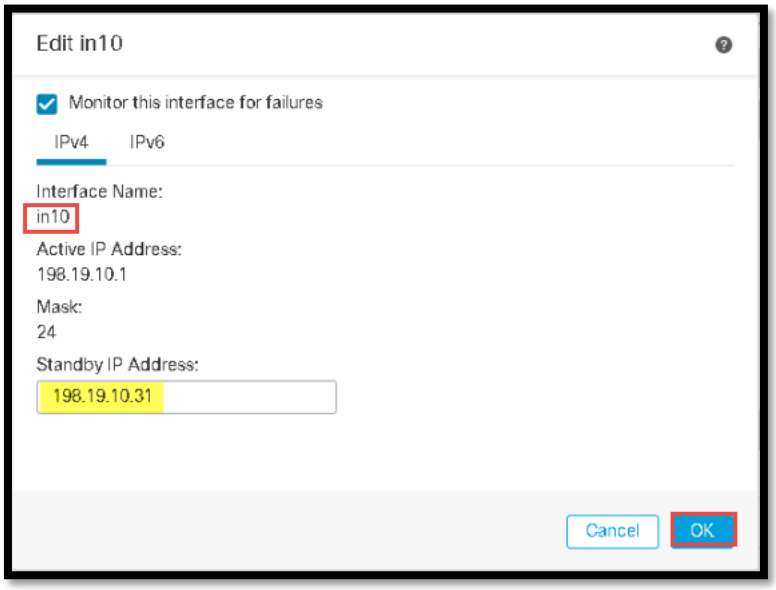
15. Physical Interface: GigabitEthernet0/1 Active Interface MAC Address: student choice (IP Address of interface used in example) Standby Interface Mac Address: Student Choice of input [example below] Click Ok

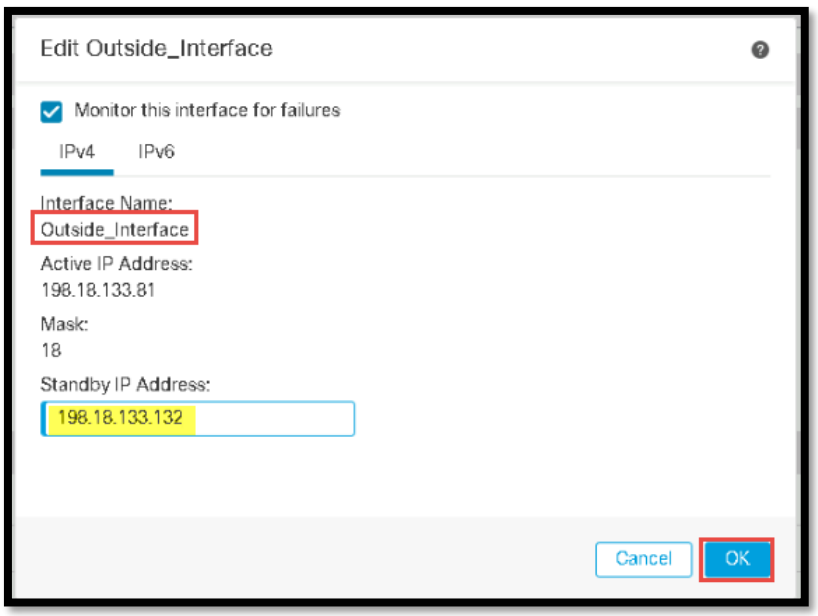
NOTE*: The above step is an example of how to configure an Interface Mac Address



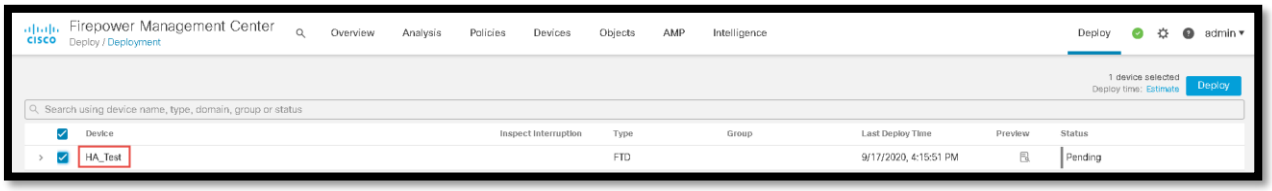
16. Configure Monitored Interfaces Go to the pencil icon next to Monitored Interfaces

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





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

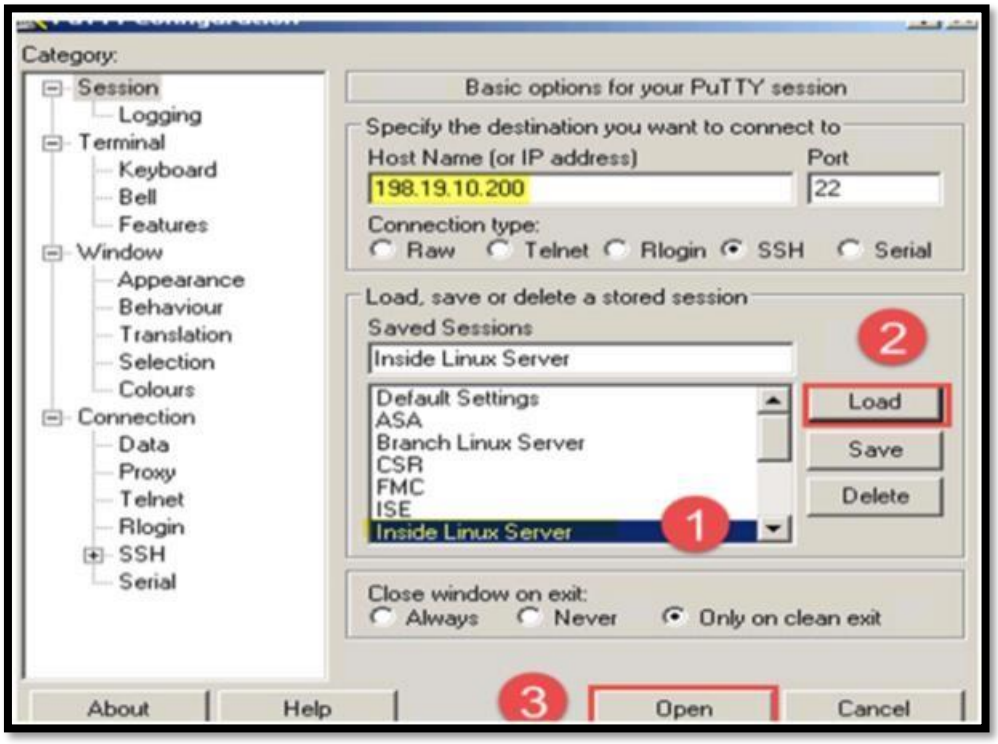


Looking at the configuration of NGFW3.

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?

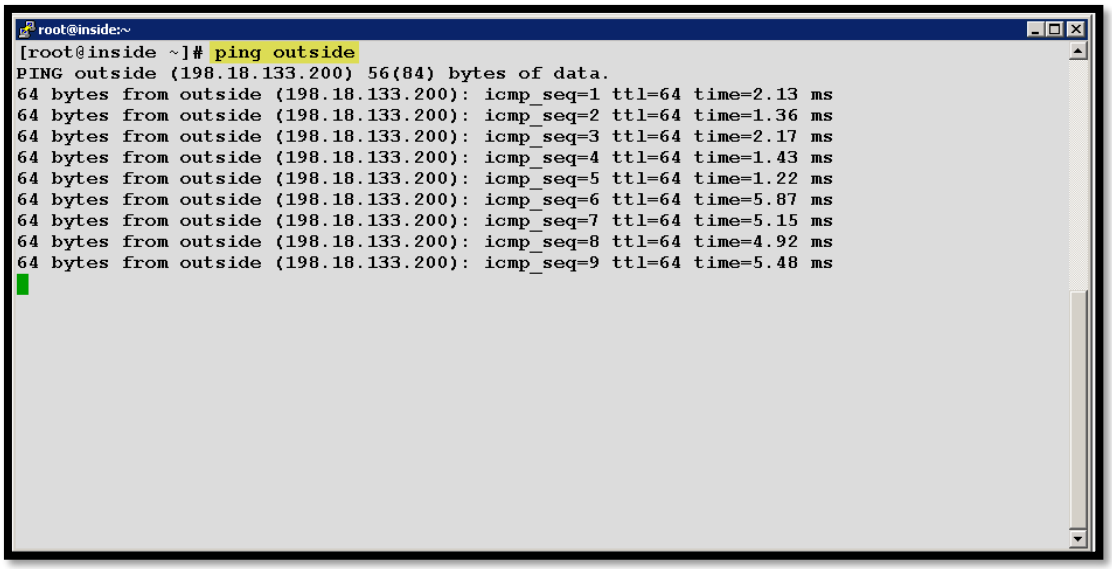
Testing Failover

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



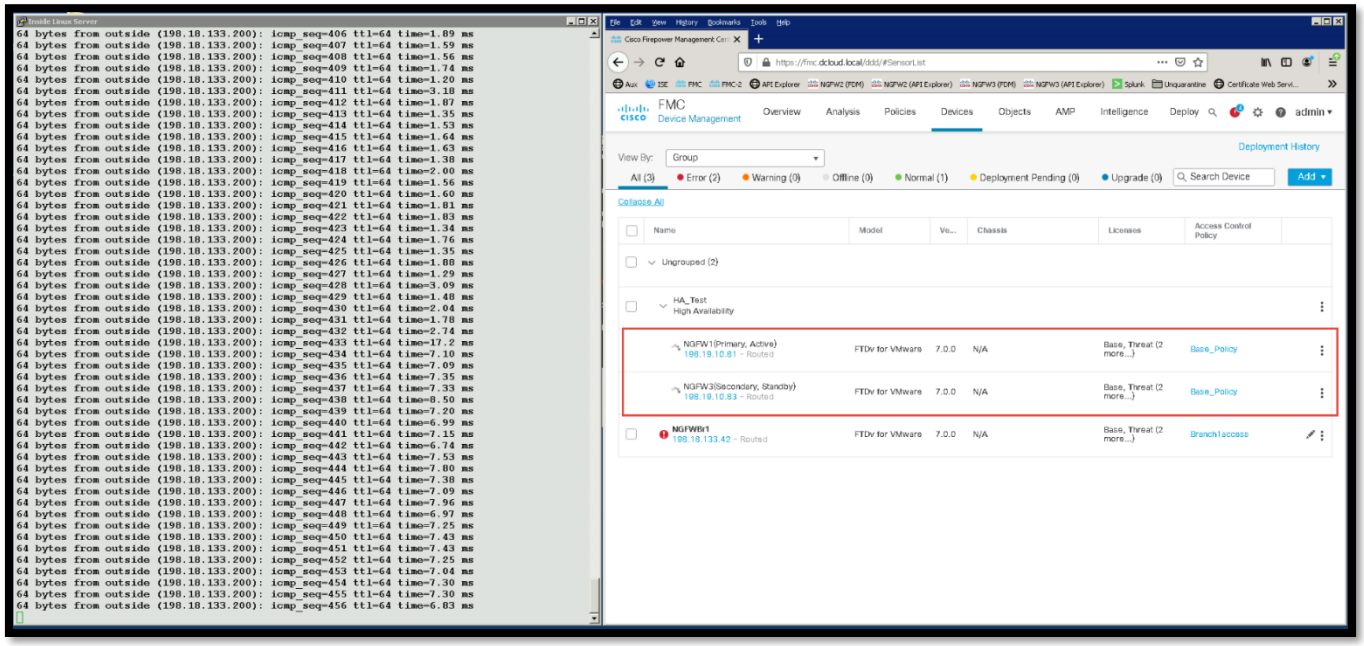
2. Login: **root** Password: **C1sco12345** Type: "ping outside" and let the script continue to run

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

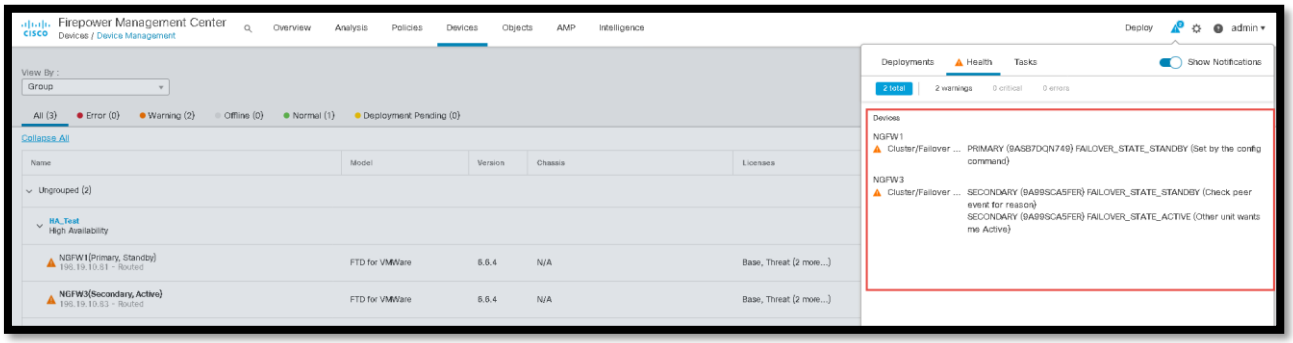


3. Go to the web interface of the FMC **Devices > Device Management** Click on the Switch Peers icon and click Yes

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

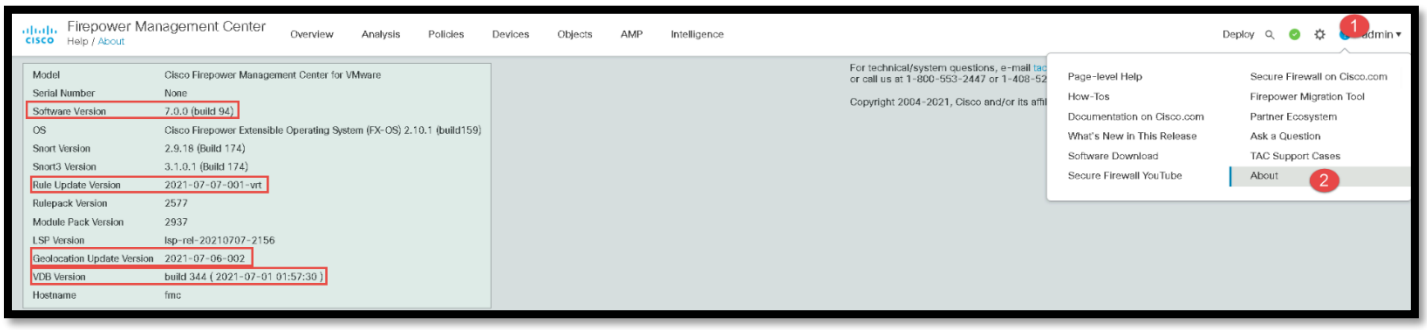
When setting up FMC in a HA pair you configure a primary and a secondary. The primary's policies are synchronized to the secondary. After synchronization the primary FMC become active and the secondary becomes standby.

Confirm Software Prerequisites for FMC HA

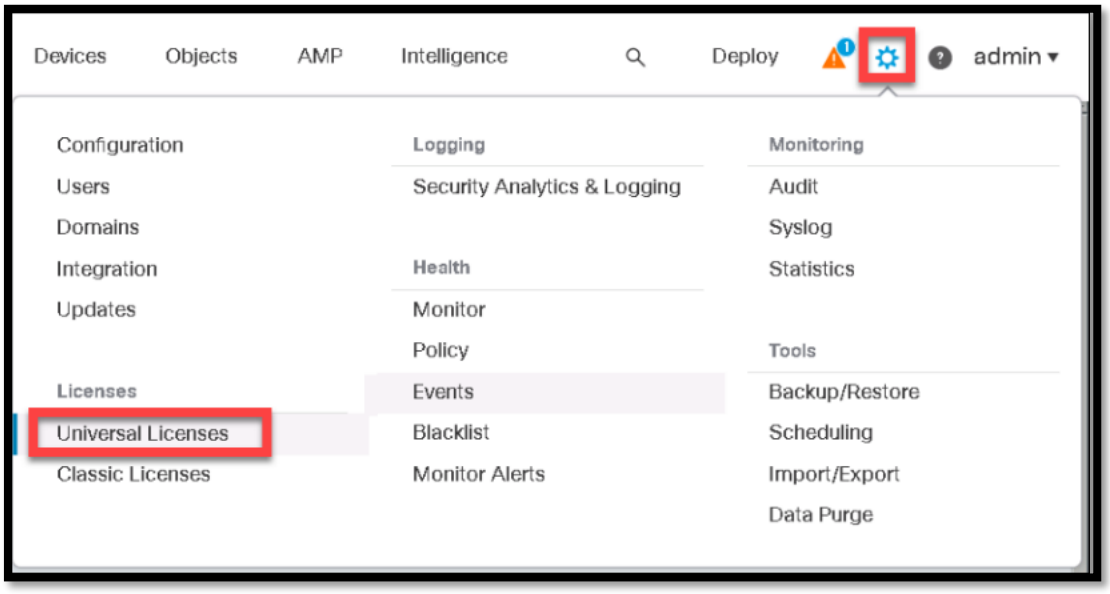
The two FMC in HA must have the same major minor and maintenance software version.

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.

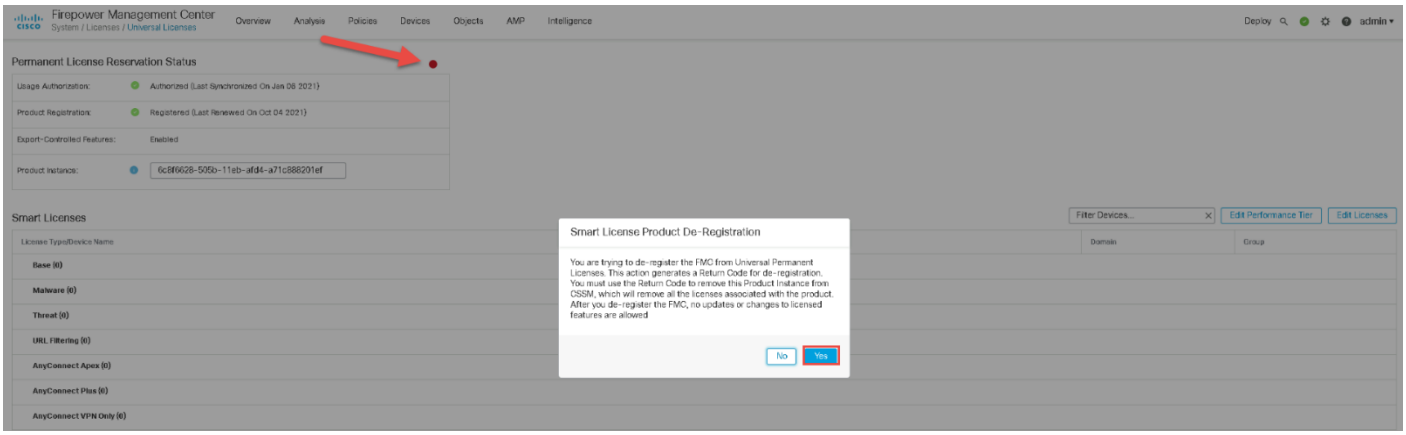
1. On the Jumphost open two browser tabs. One to the FMC and the other to FMC2 found on the bookmark ribbon
2. Click on the **? and About** and verify the settings for both FMC's



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



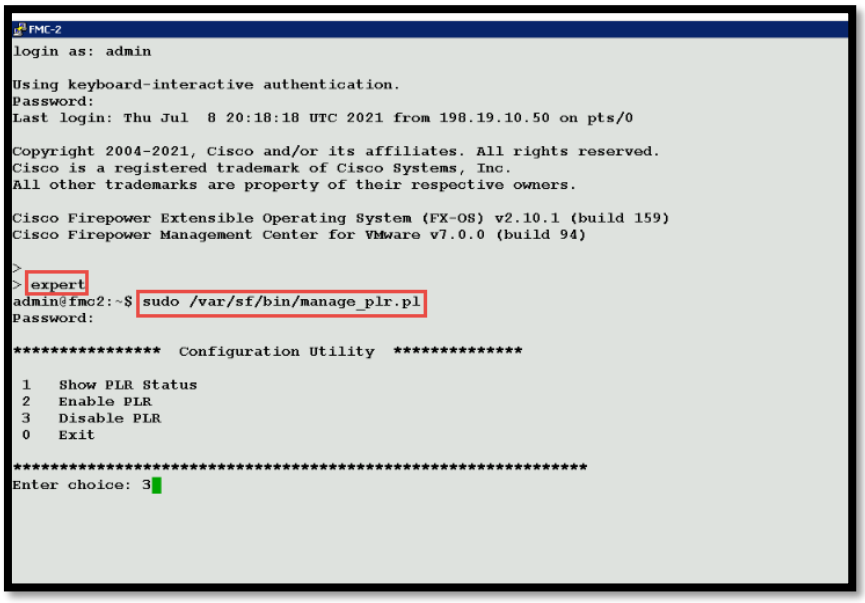
6. Click on the red circle and then yes

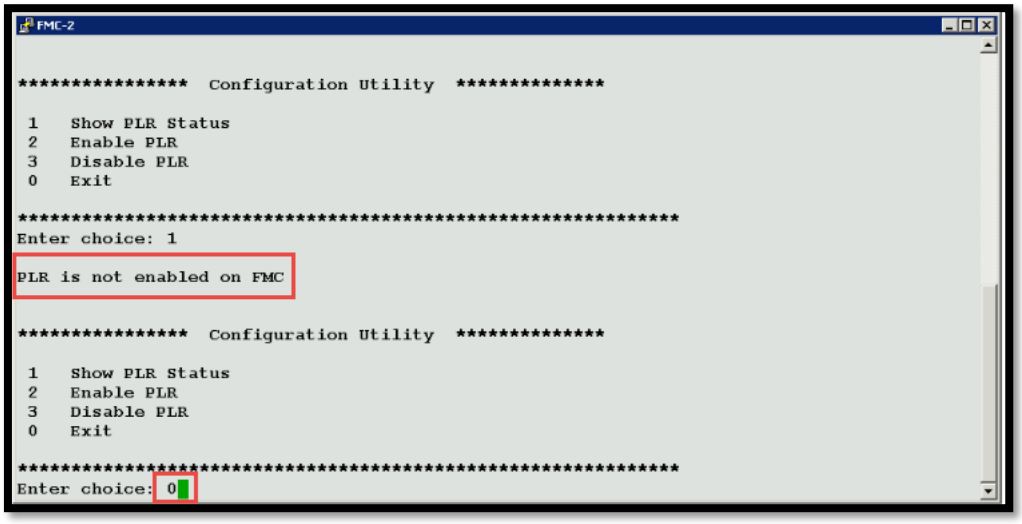


7. Click on Generate a request code

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

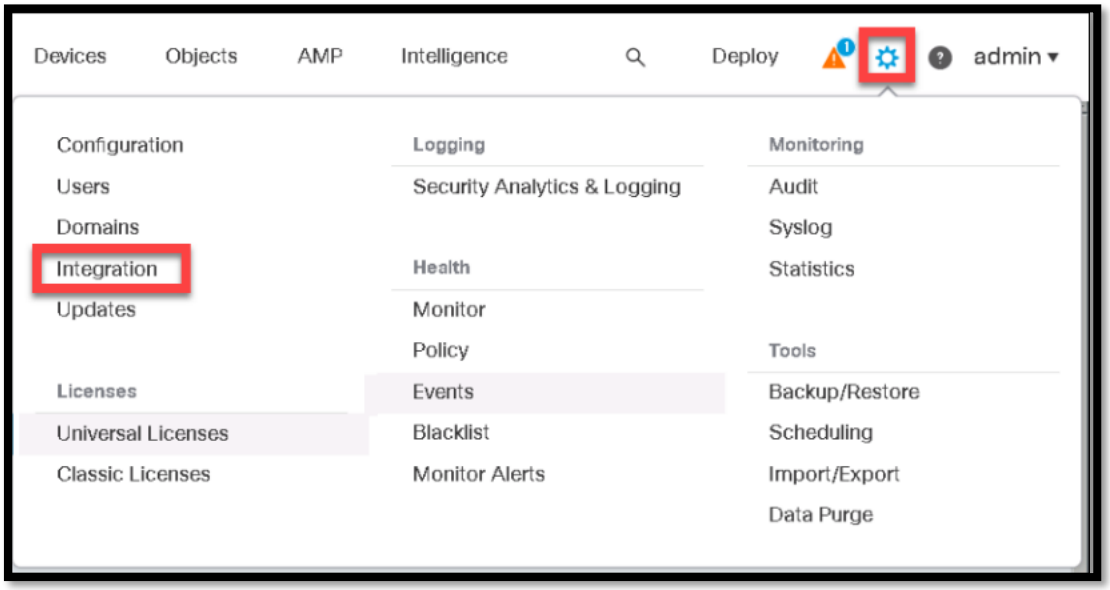
8. Open PuTTY on the jump box desktop. Open the FMC-2 predefined session
    a. Login: admin/C1sco12345
    b. Type: expert
        i. Type: sudo /var/sf/bin/manage_plr.pl password C1sco12345
        ii. Enter 3 to disable PLR



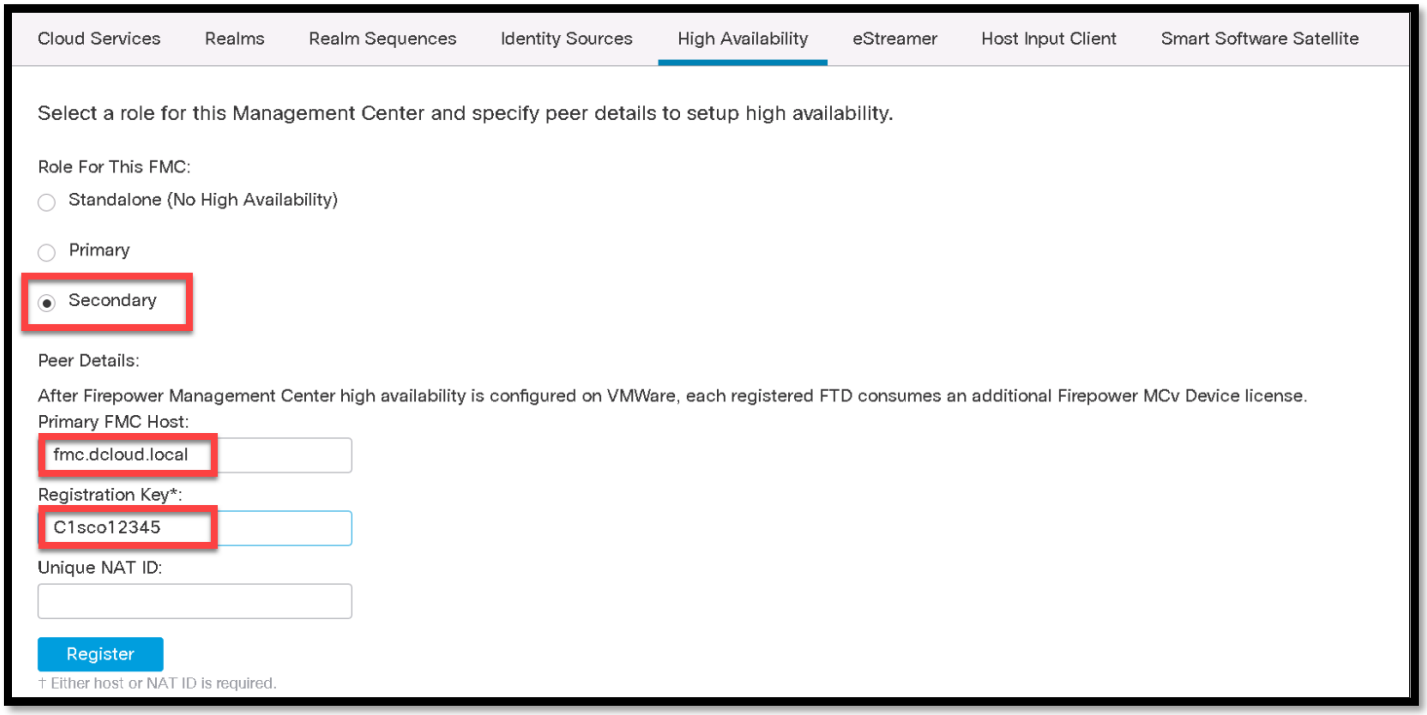


iii. Enter 0

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



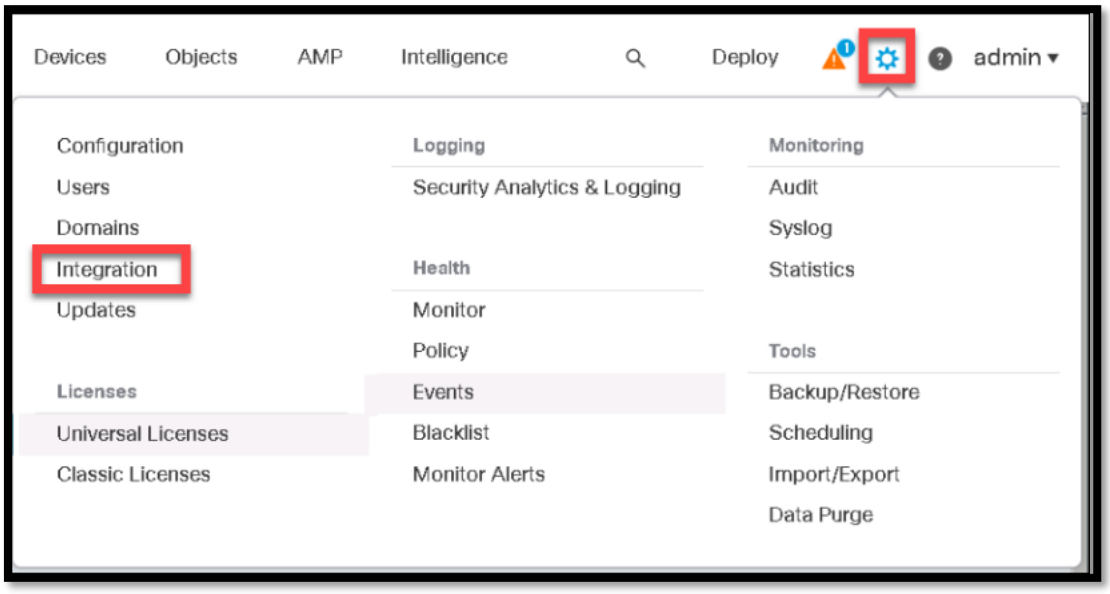
10. Select the High Availability sub-tab
11. Select Secondary
    a. For Primary: fmc.dcloud.local
    b. Register Key: C1sco12345
    c. Register
    d. Select Yes and Yes



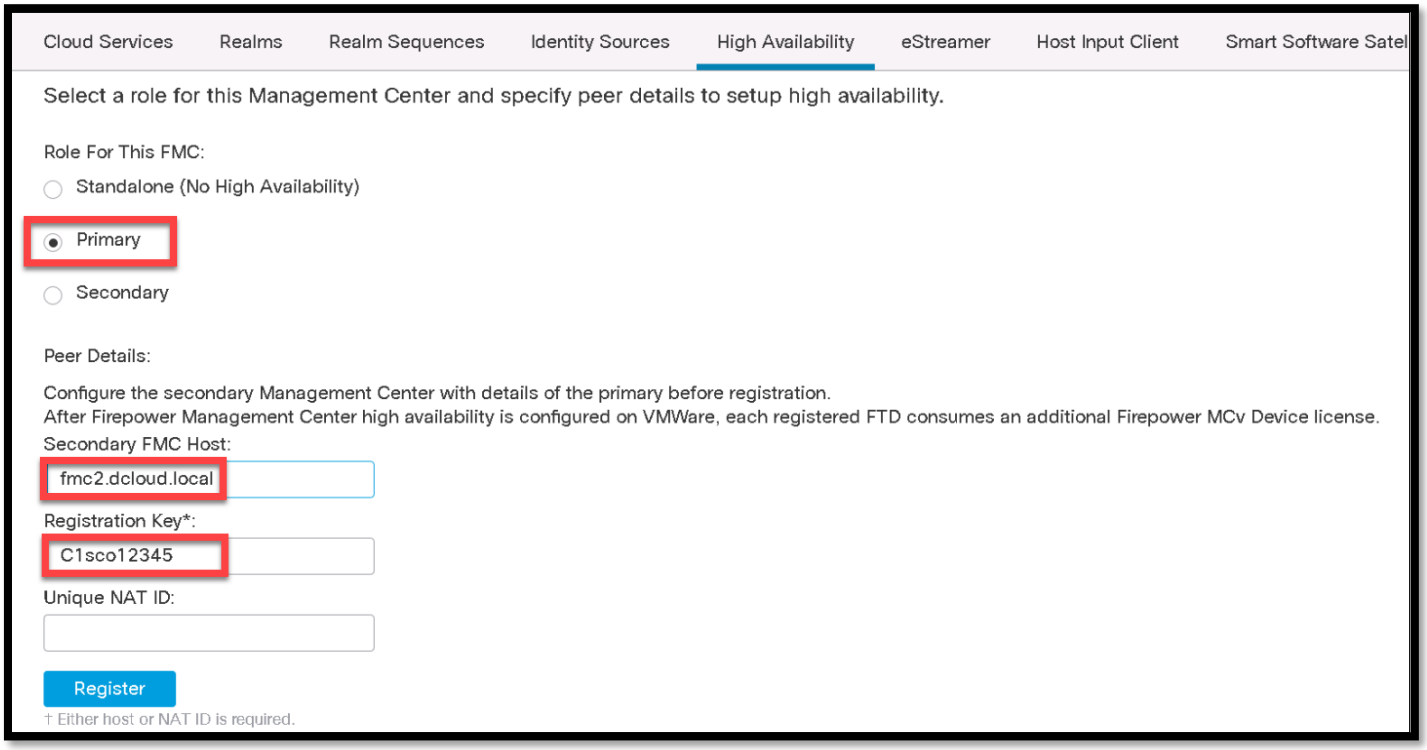
Note: You will see that HA FMC page now says Pending Registration

Configure FMC as the Primary FMC

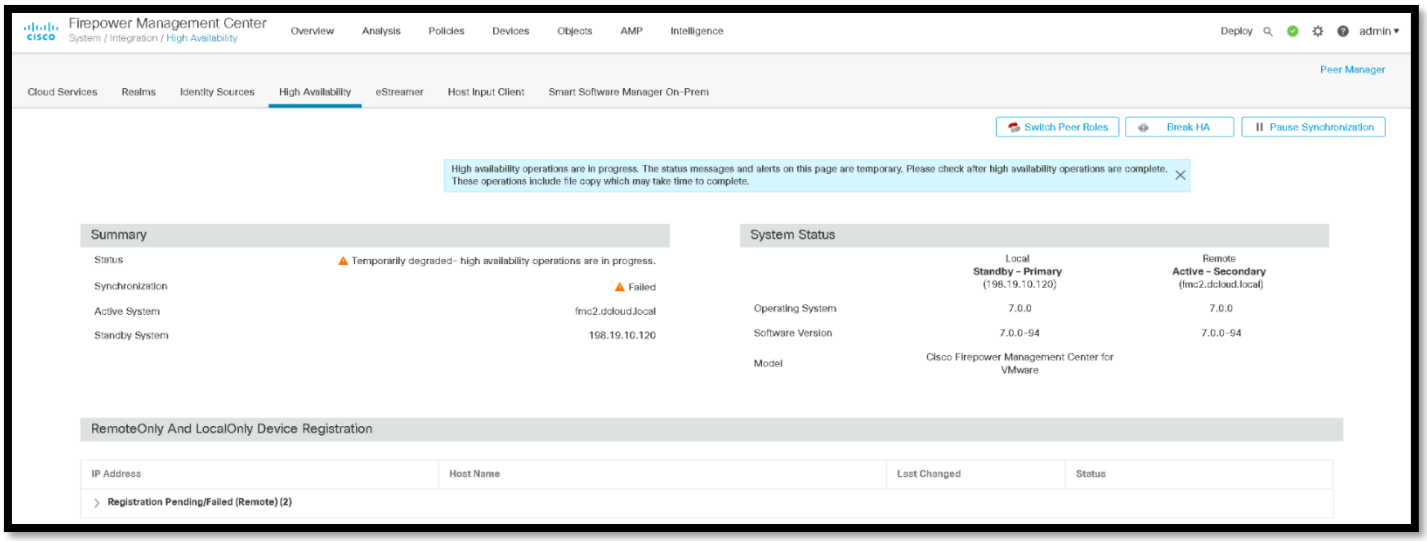
1. FMC click on the gear icon in the upper right corner and select Integration

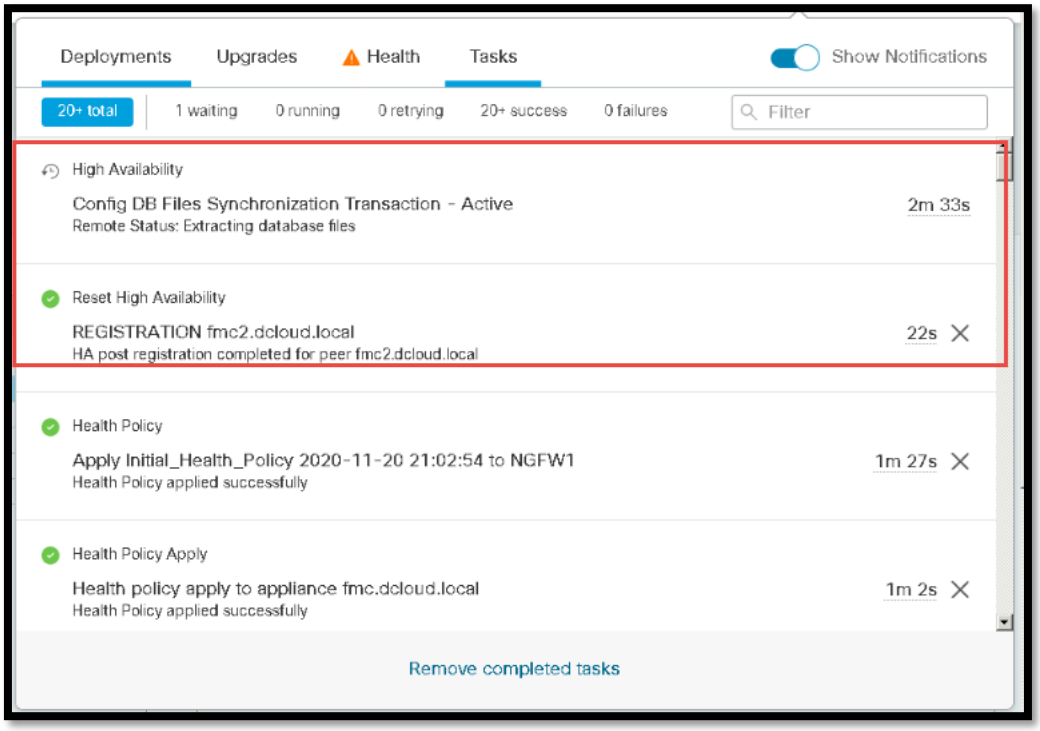


2. Select High Availability
    a. Select Primary
    b. Secondary FMC Host: fmc2.dcloud.local
    c. Registration Key: C1sco12345
    d. Register



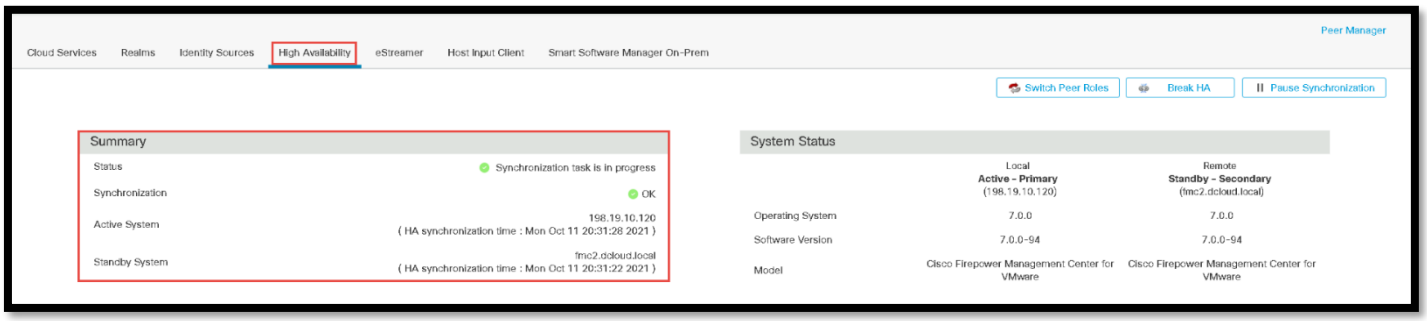
3. Check the status





Confirm the FMC HA Configuration

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

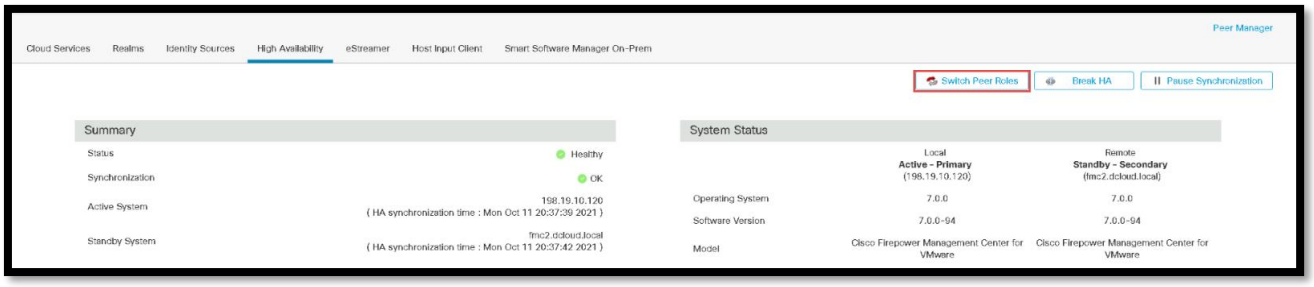


3. Open the PuTTY session for **NGFW1 admin/C1sco12345**
4. Type show managers

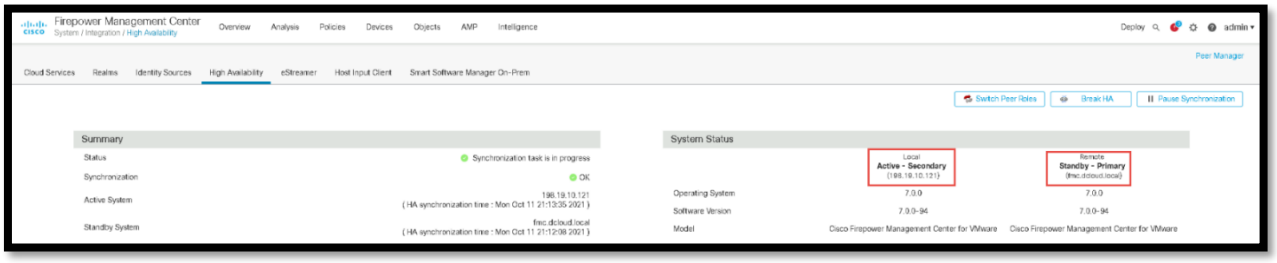
```
> show managers
Type                          : Manager
Host                          : fmc2.dcloud.local
Registration                  : Completed

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**

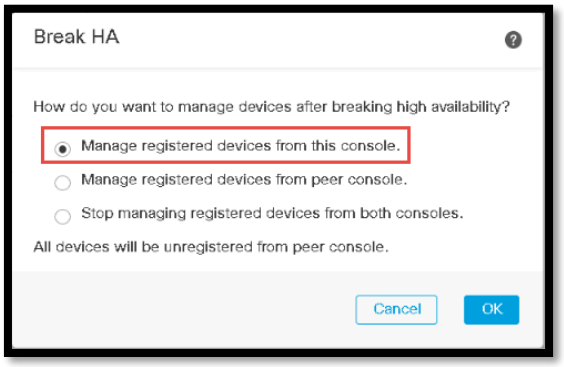
7. On FMC High Availability Click **Switch Peer Roles yes and OK**



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



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**



    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.

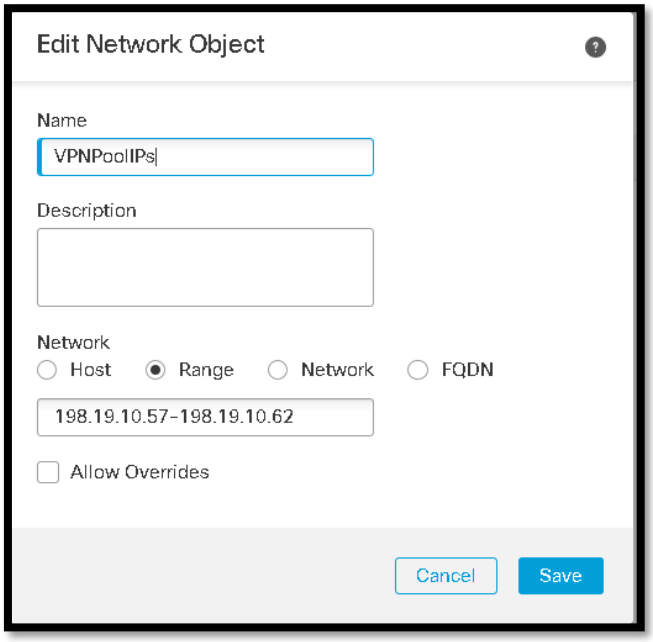
Steps

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

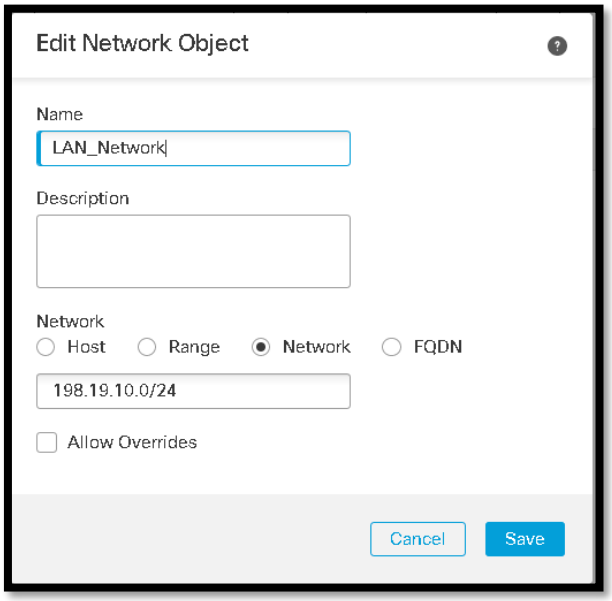
Create objects needed for this scenario

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.

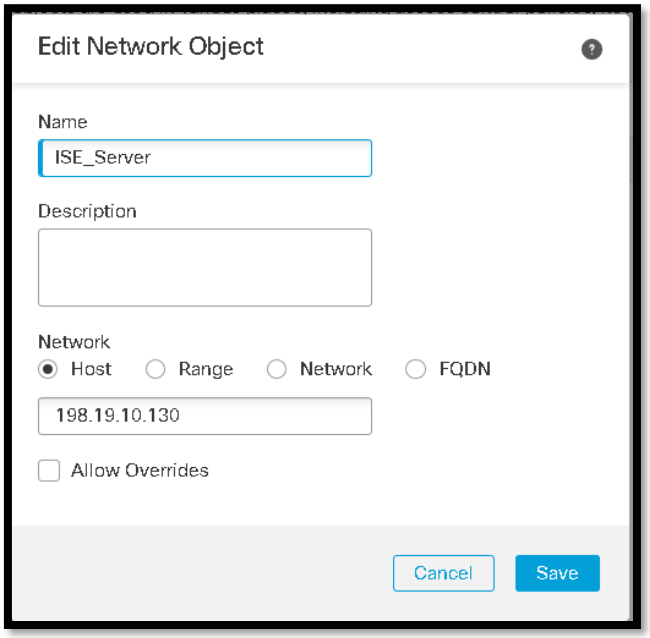
1. In the FMC, navigate to Objects > Object Management.
2. Click Add Network > Add Object.
    a. Create an IP range object called
        i. VPNPoolIPs IP address range 198.19.10.57-198.19.10.62.
        ii. This object will be used to create a NAT exemption.
        iii. Click **Save**



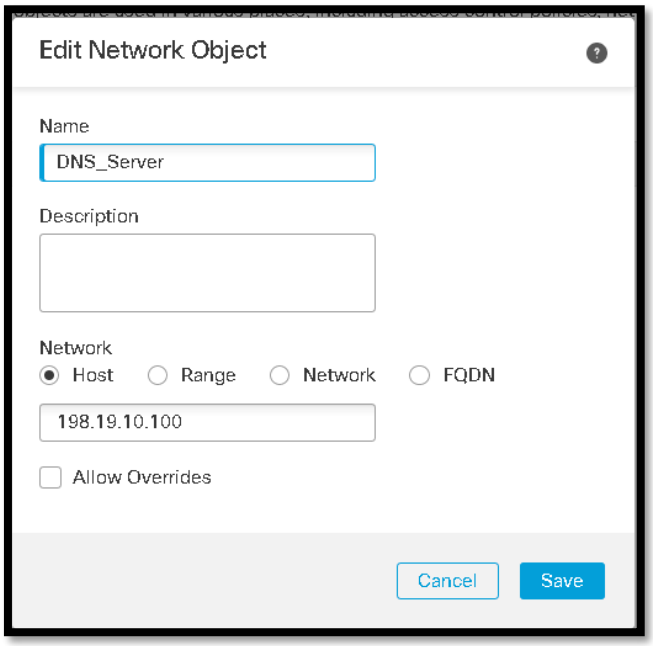
3. Click Add Network > Add Object. Create a Network object called LAN_Network with IP addresses 198.19.10.0/24



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

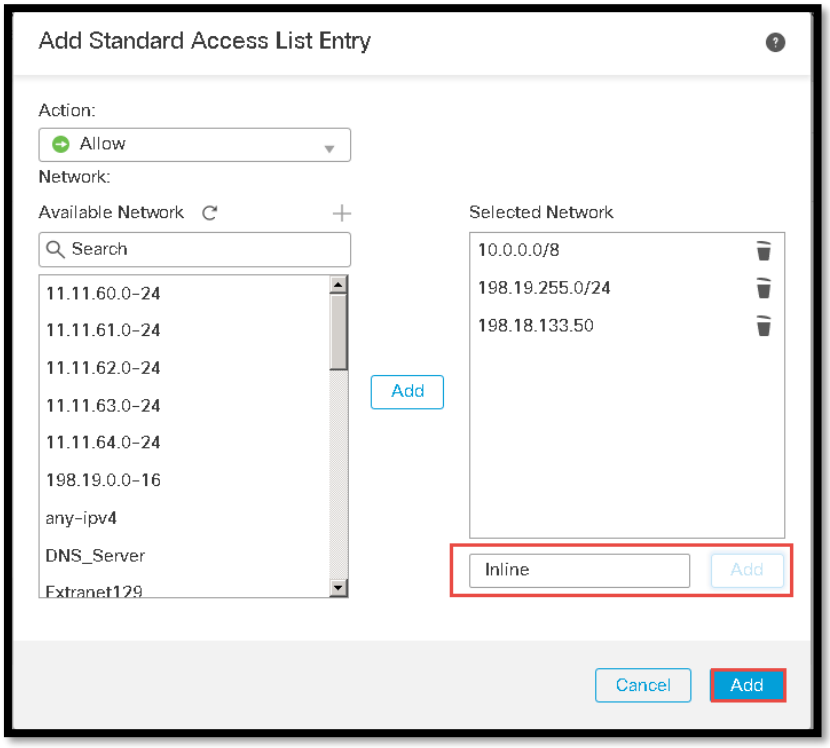


5. Click Add Network > Add Object. Create a host object called DNS_Server with IP address 198.19.10.100.

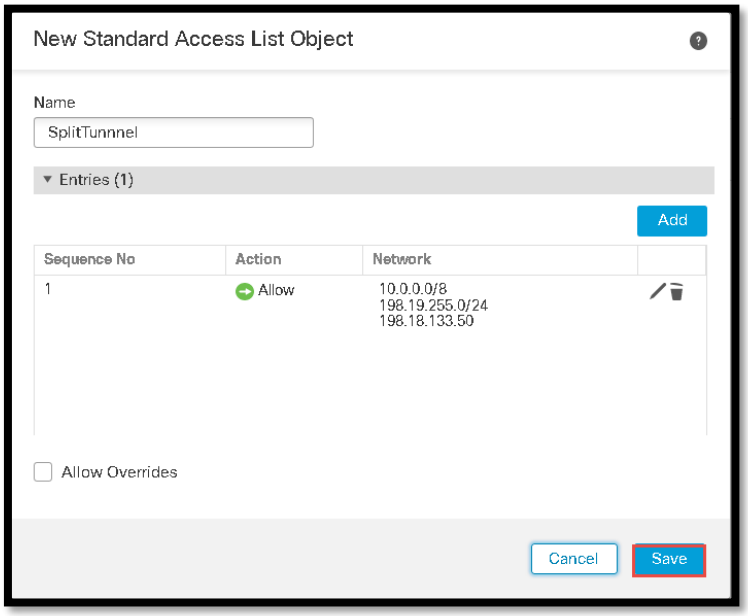


NOTE: For best security, it is recommended that split-tunneling not be used. However, because there is no console access for the endpoint on which you will run AnyConnect, split tunneling must be used in this Scenario. Since there are different ways to access the endpoint in dCloud, you need to create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

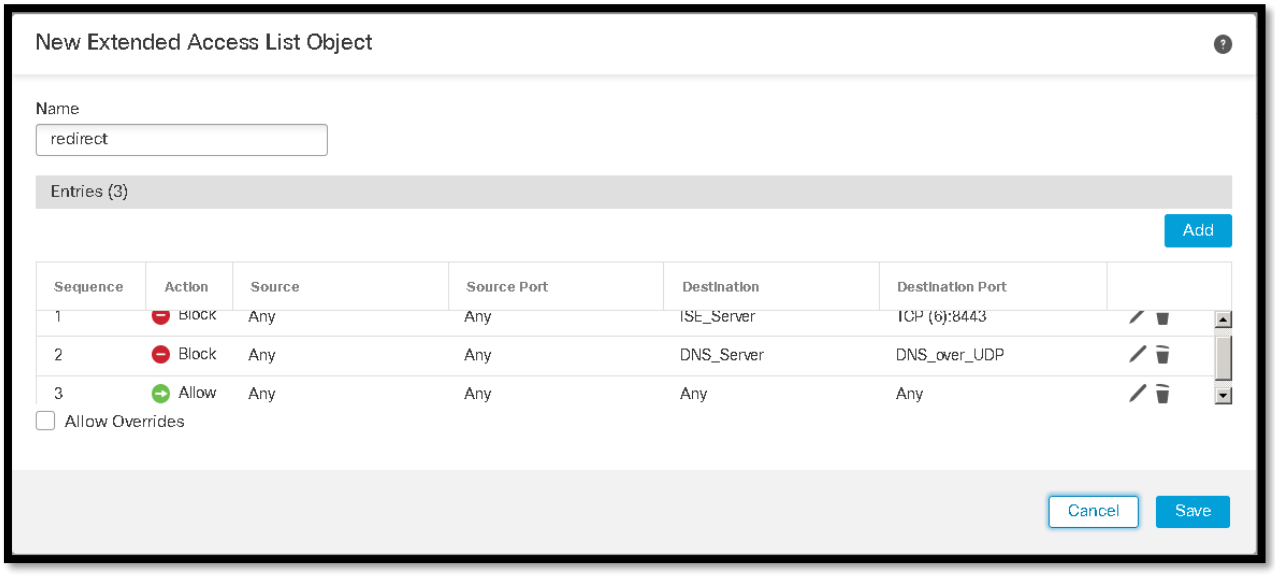
6. Select Access List > Standard from the left navigation pane. Click Add Standard Access List.
7. Create a standard access list called SplitTunnel with the ACE that allows 10.0.0.0/8, 198.19.255.0/24 and 198.18.133.50. To do this, type these networks into the text box under the Selected Network box,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



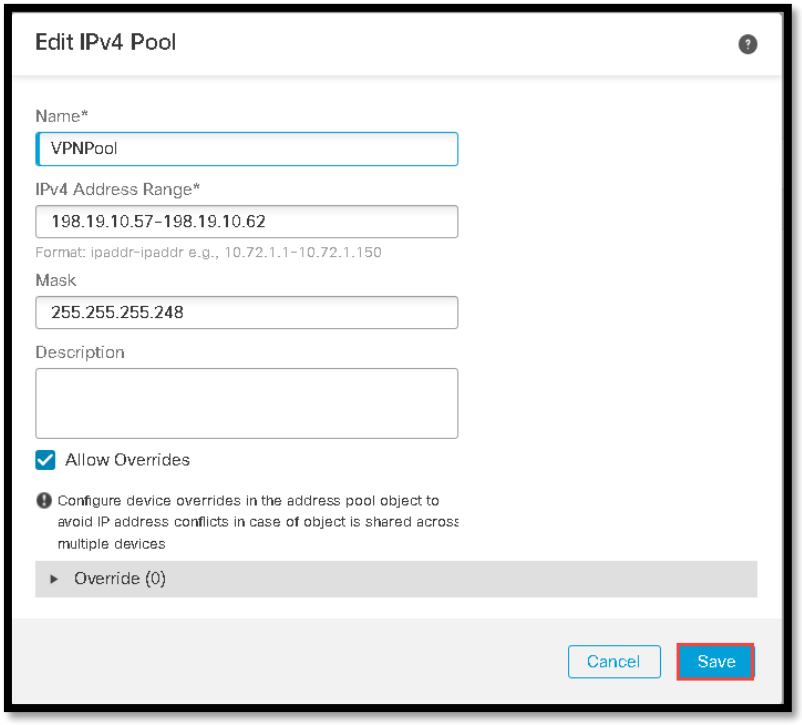
8. Click Save to save the access list.



9. Select Access List > Extended from the left navigation pane. Click Add Extended Access List.
10. 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.

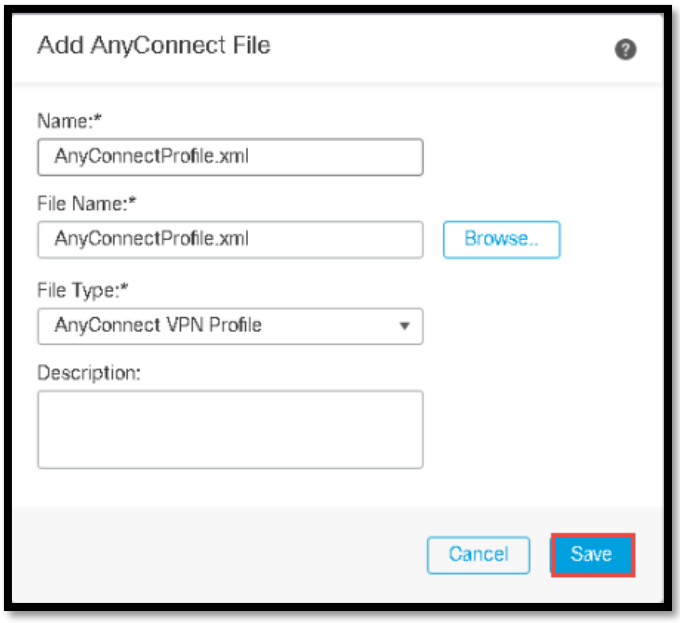


11. Select Address Pools > IPv4 Pools from the left navigation pane. Click Add IPv4 Pools.
    a. For Name, enter VPNPool.
        i. For IPv4 Address Range, enter 198.19.10.57-198.19.10.62.
        ii. For Mask, enter 255.255.255.248.
        iii. Click Save

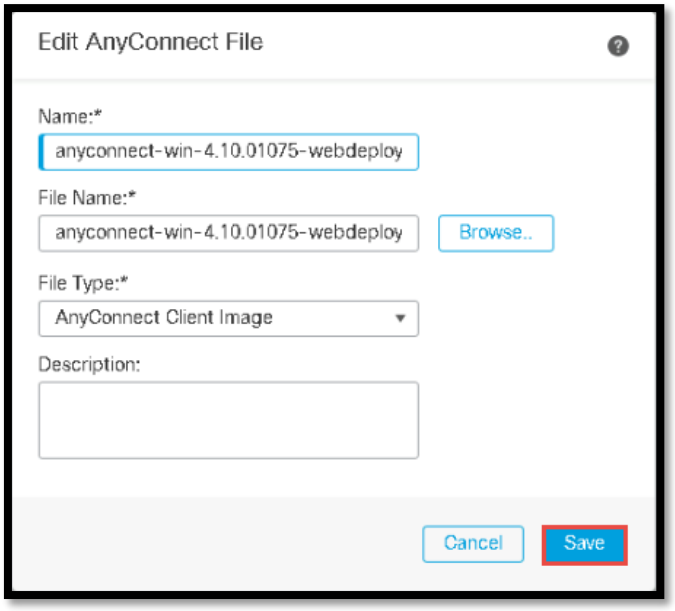


NOTE: Although the objects VPNPoolIPs and VPNPool represent the same IP address range, they are different object types. VPNPool will be referenced in the RA VPN object, whereas VPNPoolIPs will be used for configuring a NAT exemption.

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.

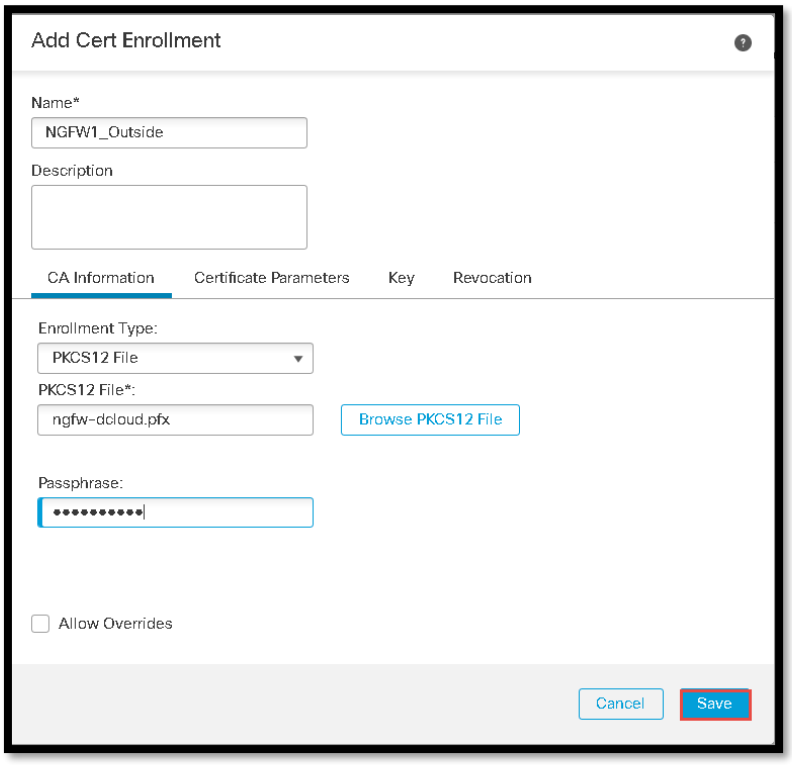


14. Click Add AnyConnect File. Click Browse and select anyconnect-win-4.7.XXXXX-webdeploy-k9.pkg from the RA VPN folder on the Jumpbox desktop. For File Type: Select AnyConnect Client Image.



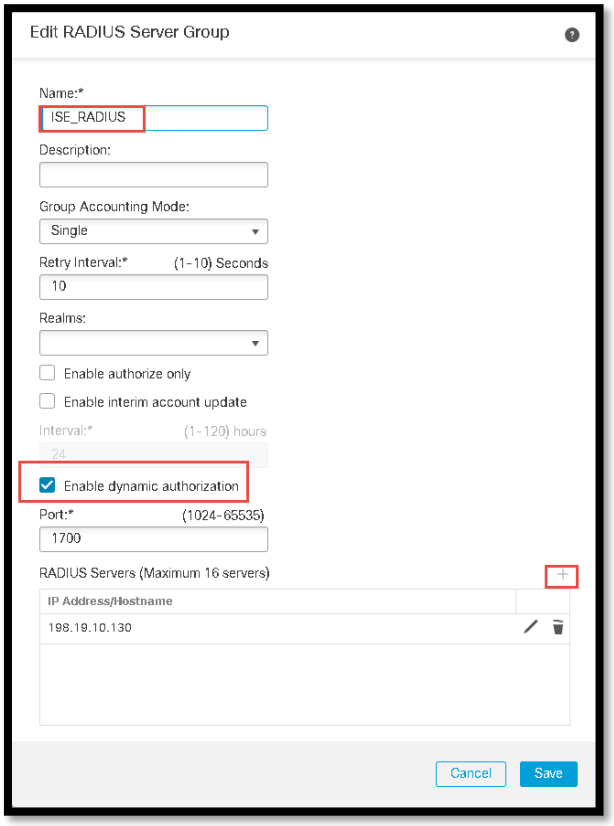
15. Select PKI > Cert Enrollment from the left navigation pane. Click Add Cert Enrollment.
    a. For Name, enter **NGFW1_Outside**. [If you have done the High Availability Lab you can name HA if you wish]
    b. Select PKCS12 File from the Enrollment Type drop-down menu.
    c. Click Browse and select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

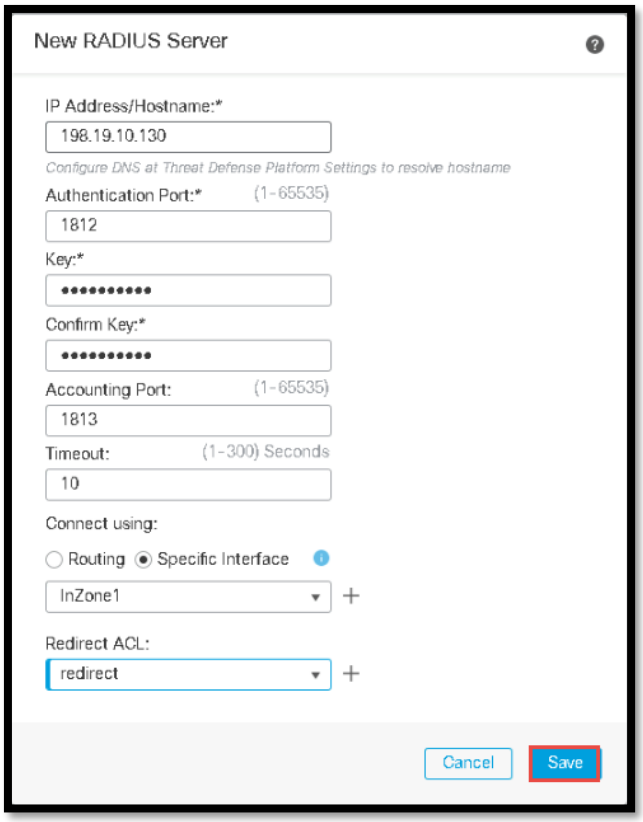
d. For Passphrase, enter **C1sco12345**.



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**.

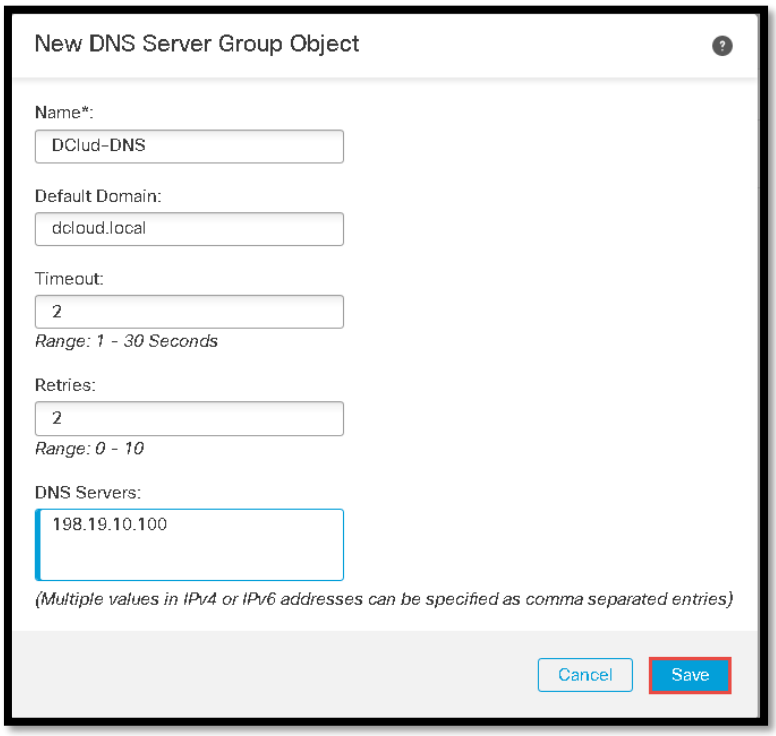




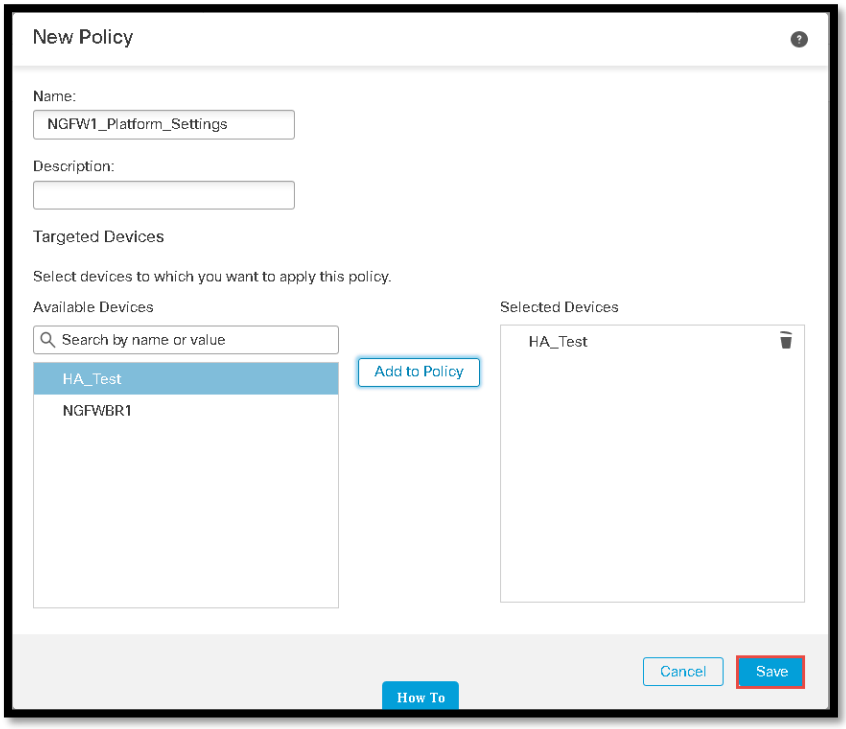
3. Click Save to add the RADIUS server to the RADIUS server group. Click Save.

Configure DNS Server for NGFW1

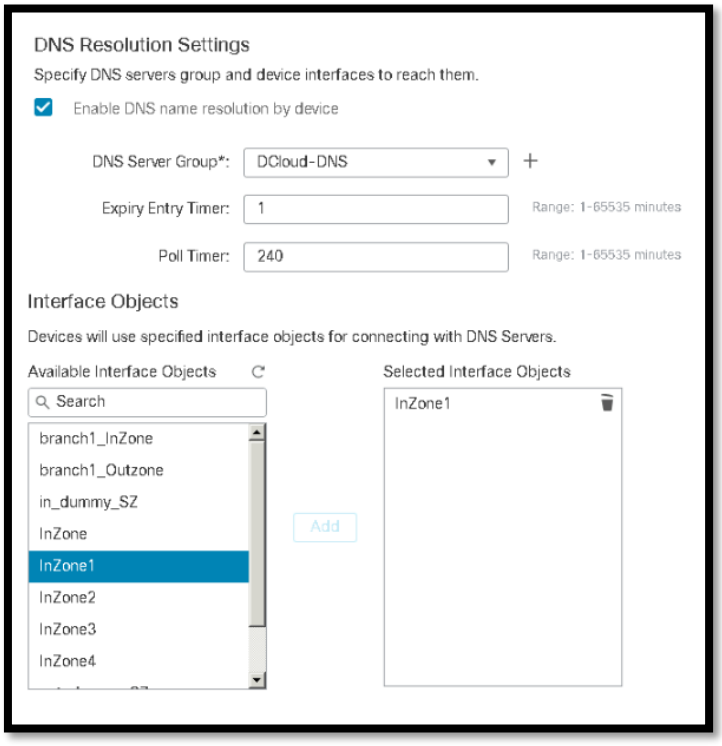
1. Navigate to Objects > Object Management > DNS Server Group. Click on Add DNS Server Group.
    a. Enter Name as DCloud-DNS
    b. Default Domain will be dcloud.local
    c. Enter 198.19.10.100 as the DNS Server.
    d. Click on Save.



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.



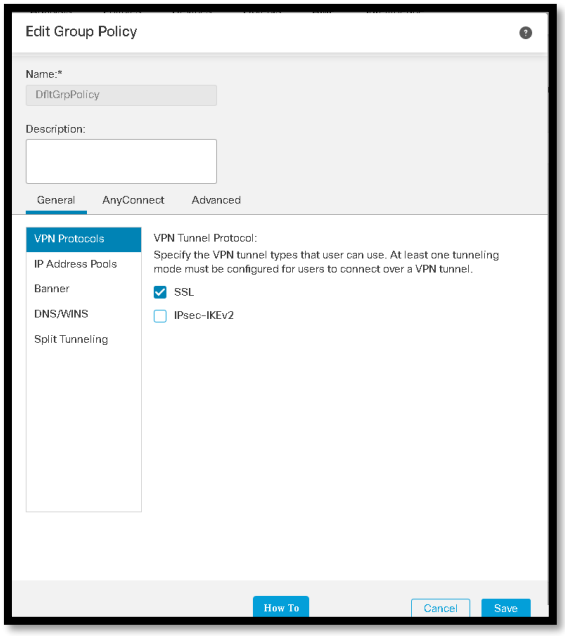
3. Navigate to DNS.
    a. Check Enable DNS name resolution by device.
    b. Select DCloud-DNS from the DNS Server Group dropdown.
    c. Add InZone1 as the Interface Object.
    d. Click on Save



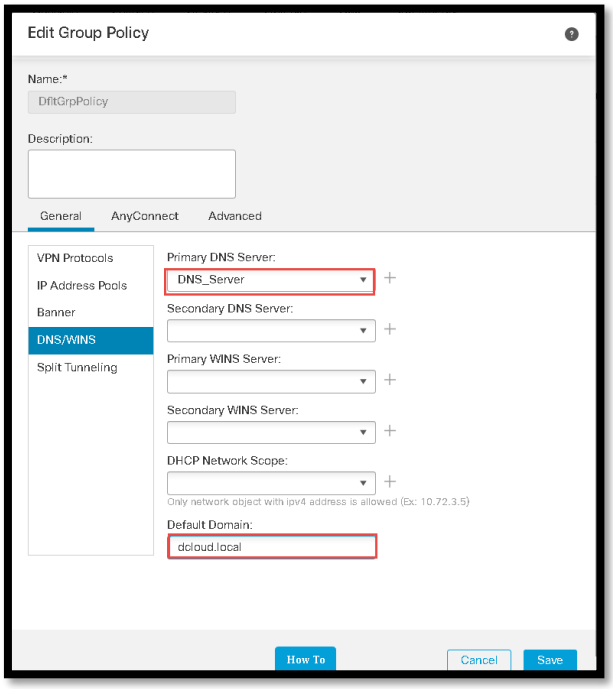
Edit the default group policy (DfltGrpPolicy)

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.

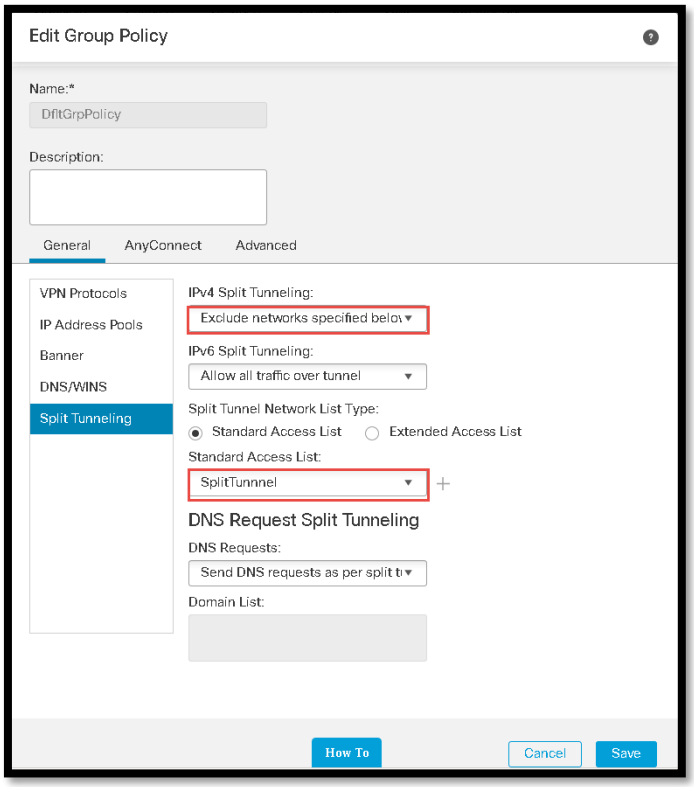
1. Navigate to Objects > Object Management > VPN > Group Policy from the left navigation pane. Click the pencil icon to edit DfltGrpPolicy
2. Under General > VPN Protocols, uncheck IPsec-IKEv2.



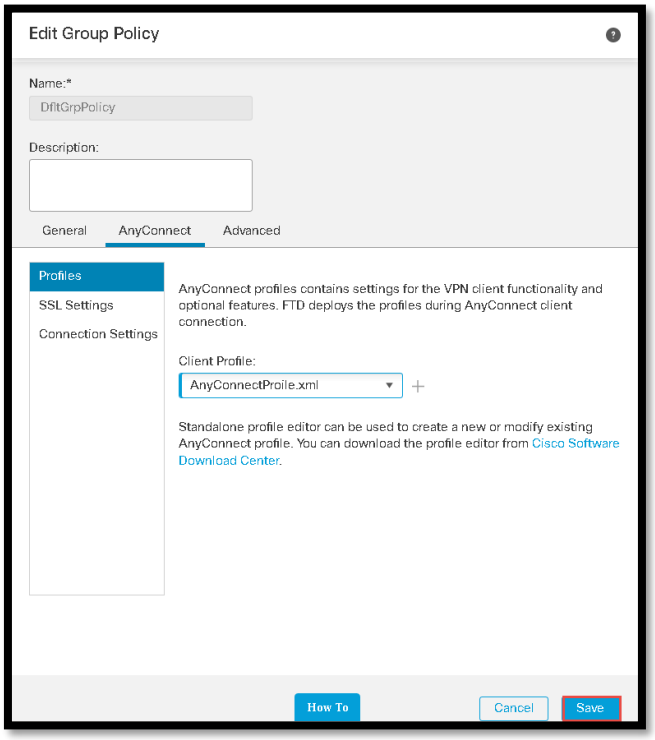
3. Under General > DNS/Wins.
    a. Select DNS_Server from the Primary DNS Server drop-down list.
    b. For Default Domain, check for: dcloud.local.



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



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



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

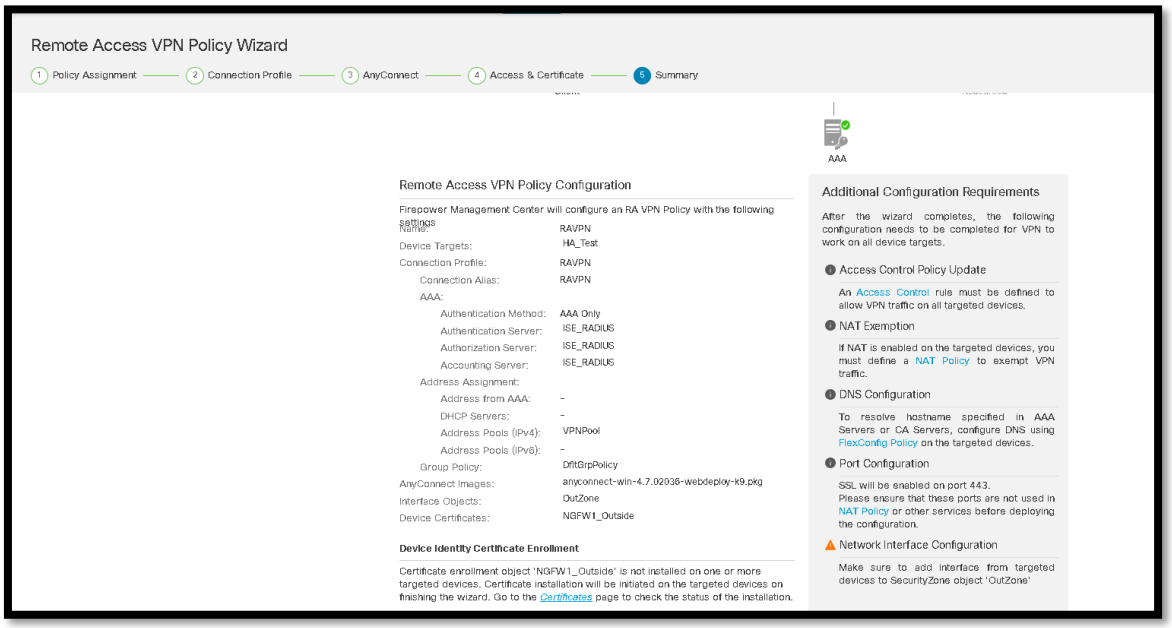
NOTE: Typically, you would also be enabling AnyConnect licensing at this point, however this has already been done. You can observe this at System > Licenses > Smart License. You will see that the FMC is using an evaluation license, but that export-controlled features are enabled. This is generally not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

Run the RA VPN wizard

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

Remote Access VPN Policy Wizard

4. Complete the AnyConnect page of the wizard.
    a. Check the file object checkboxes.
    b. Click Next
5. Complete the Access & Certificate page of the wizard.
    a. For Interface group/Security Zone, select OutZone.
    b. For Certificate Enrollment, select NGFW1_Outside.
    c. Click Next
    d. 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

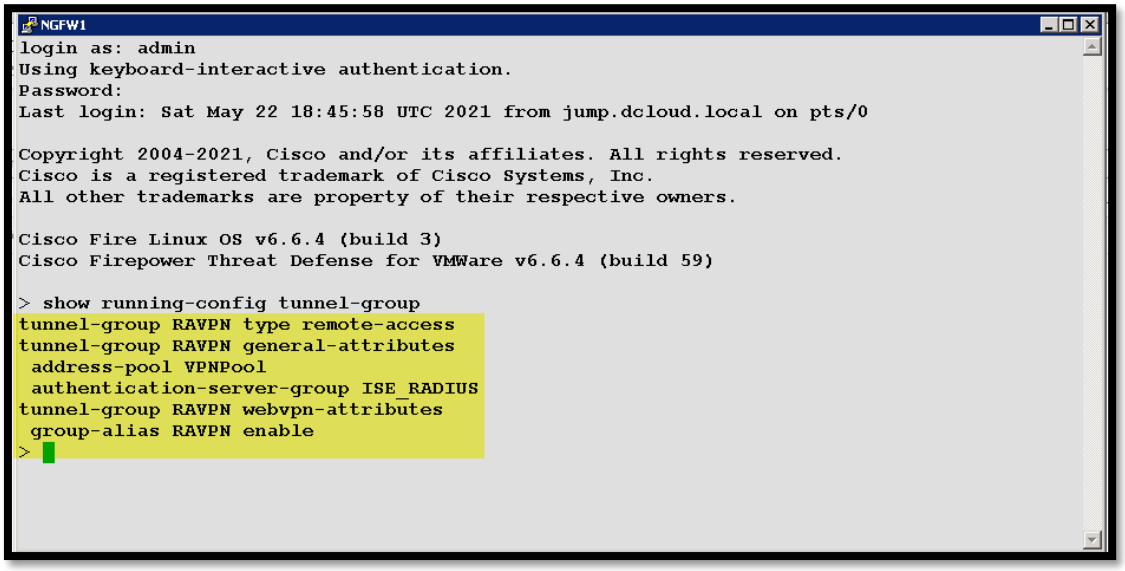
1. In the FMC, navigate to Devices > NAT.
2. Select and edit the existing NAT policy (Default PAT). Click Add Rule.
    a. You will be at the Interface Objects tab.
    b. Select InZone1 and click Add to Source.
    c. Select OutZone, and click Add to Destination.
3. Select the Translation tab.
4. For 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.

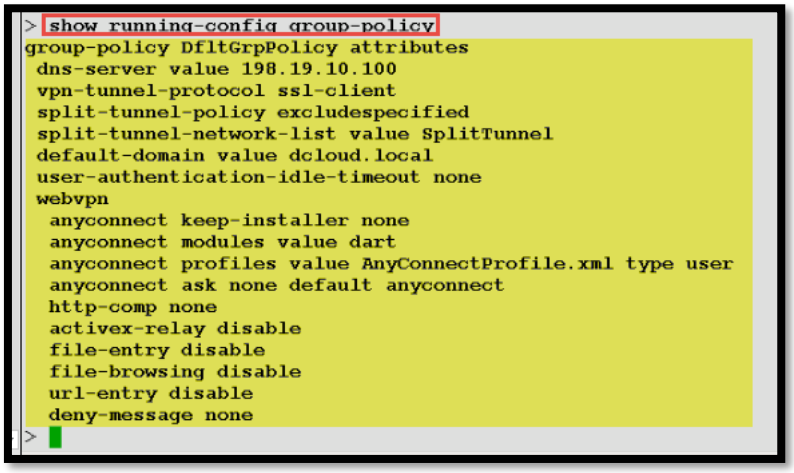
9. Click OK to save the NAT rule
10. Click **Save** to save the changes to the NAT policy.

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

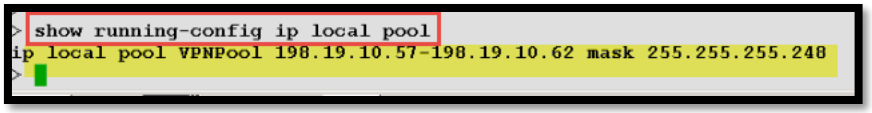


b. show running-config group-policy



c. show running-config crypto
   i. Notice the crypto trustpoint is: NGFW1_Outside or HA

d. show running-config ip local pool



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
>
```

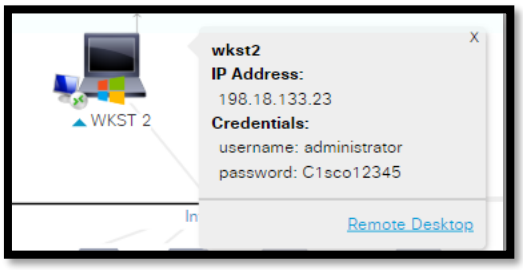
6. Test AAA by running the following command on the NGFW1 CLI

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

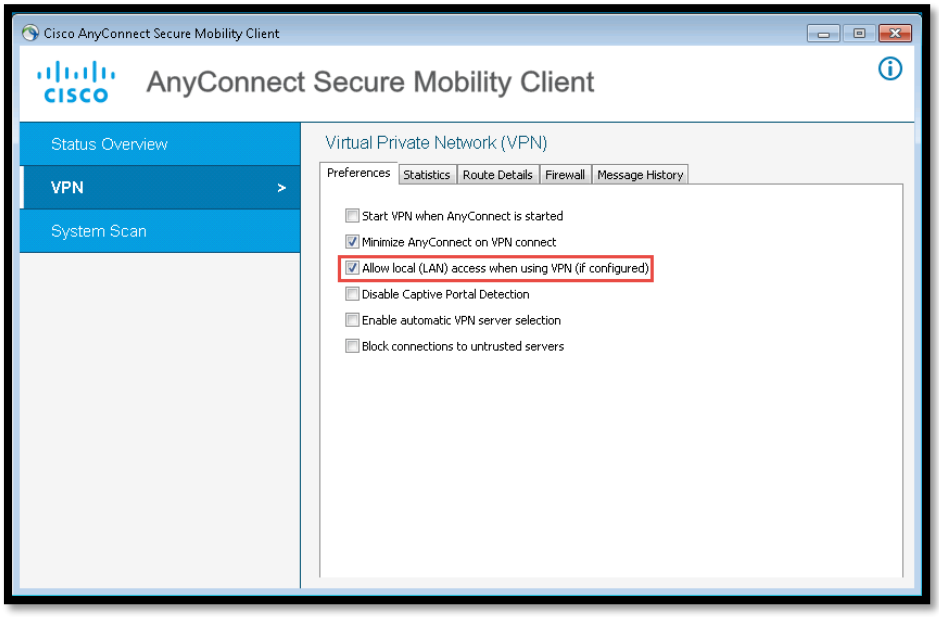
NOTE: If the test fails you will need to reset the pc-outside password. Go to the Jumpbox click on Remote Desktops and click on the ad1.Domain Controller. Click on Start Administrative Tools Active Directory Users and Computers right click on pc-outside and select Reset Password enter **C1sco12345** 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 show in this picture. This is the recommended method.



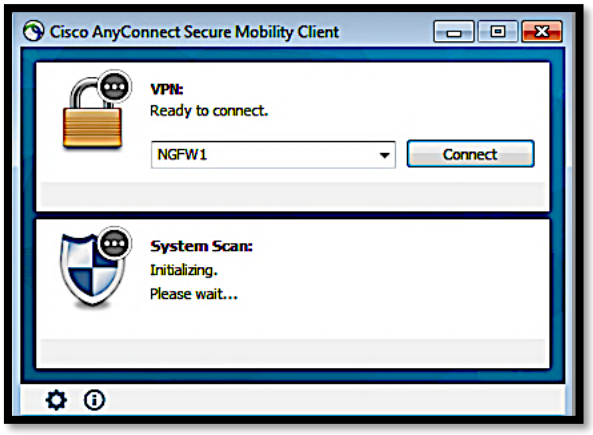
   b. By clicking the Wkst2 (Outside PC) shortcut in the Remote Desktops folder the Jumpbox desktop. However. If you do this, you must allow local LAN access in the AnyConnect client.

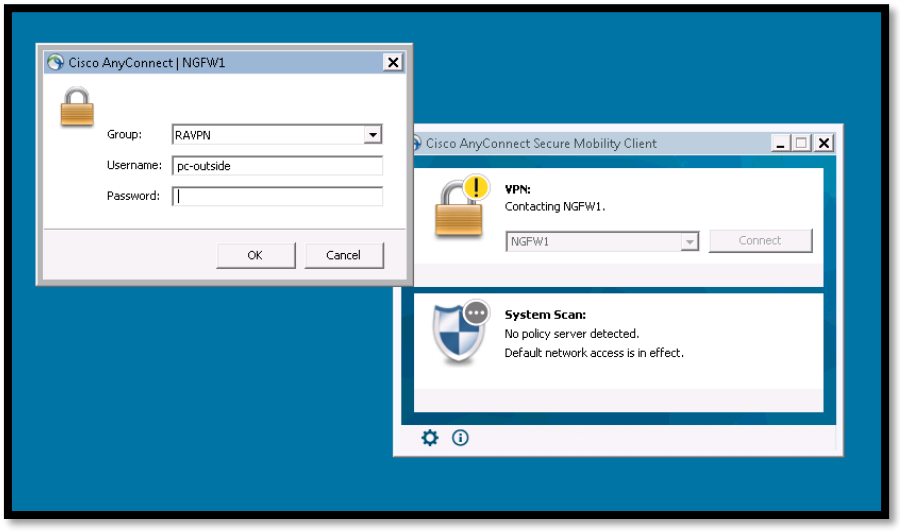


c. If you are connected to the pod via VPN, use and RDP client on your laptop to connect to 198.18.133.23. Log in as Administrator, password C1sco12345.

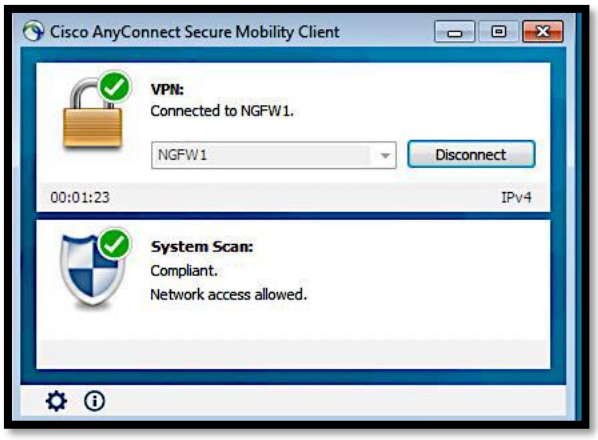
2. Open AnyConnect from the Start Menu. You will see the Connect To field prepopulated with the NGFW1 FQDN. Click on Connect accept the Certificate Warnings

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.





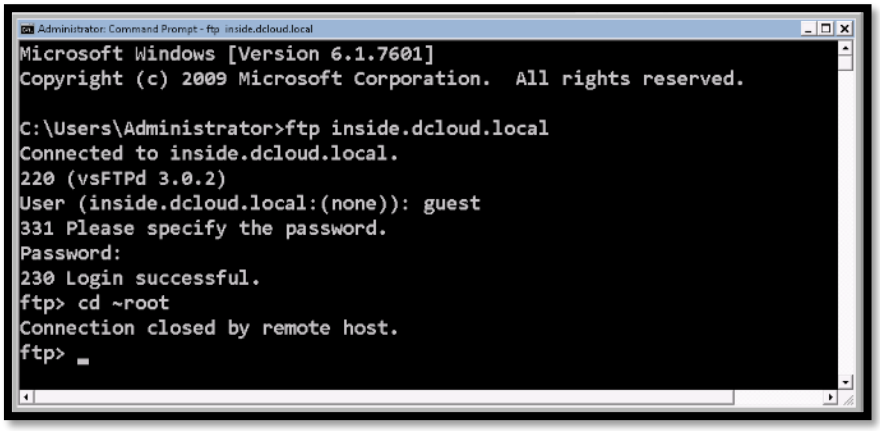
3. For Password: **C1sco12345** and **OK**
4. On the first connect, you might see the AnyConnect Compliance module being downloaded.
5. If the system is compliant the first time we connect, you will be prompted to remediate. Click on Start.



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 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.



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                    Hashing       : none
  TCP Src Port  : 49215                   TCP Dst Port  : 443
  Auth Mode     : userPassword
  Idle Time Out: 30 Minutes               Idle TO Left  : 26 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                 Bytes Rx      : 605
  Pkts Tx       : 6                       Pkts Rx       : 0
  Pkts Tx Drop  : 0                       Pkts Rx Drop  : 0

SSL-Tunnel:
  Tunnel ID     : 1.2
  Assigned IP   : 198.19.10.57            Public IP     : 198.18.133.23
  Encryption    : AES-GCM-256             Hashing       : SHA384
  Ciphersuite   : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                  TCP Src Port  : 49223
  TCP Dst Port  : 443                     Auth Mode     : userPassword
  Idle Time Out: 30 Minutes               Idle TO Left  : 26 Minutes
  Client OS     : Windows
  Client Type   : SSL VPN Client
  Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.7.02036
  Bytes Tx      : 8106                    Bytes Rx      : 448
  Pkts Tx       : 6                       Pkts Rx       : 6
  Pkts Tx Drop  : 0                       Pkts Rx Drop  : 0
  Filter Name   : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3

DTLS-Tunnel:
  Tunnel ID     : 1.3
  Assigned IP   : 198.19.10.57            Public IP     : 198.18.133.23
  Encryption    : AES256                  Hashing       : SHA1
  Ciphersuite   : DHE-RSA-AES256-SHA
  Encapsulation: DTLSv1.0                 UDP Src Port  : 49786
  UDP Dst Port  : 443                     Auth Mode     : userPassword
  Idle Time Out: 30 Minutes               Idle TO Left  : 30 Minutes
  Client OS     : Windows
  Client Type   : DTLS VPN Client
  Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.7.02036
  Bytes Tx      : 14895898                Bytes Rx      : 324974
  Pkts Tx       : 10996                   Pkts Rx       : 6291
  Pkts Tx Drop  : 0                       Pkts Rx Drop  : 0
  Filter Name   : #ACSACL#-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

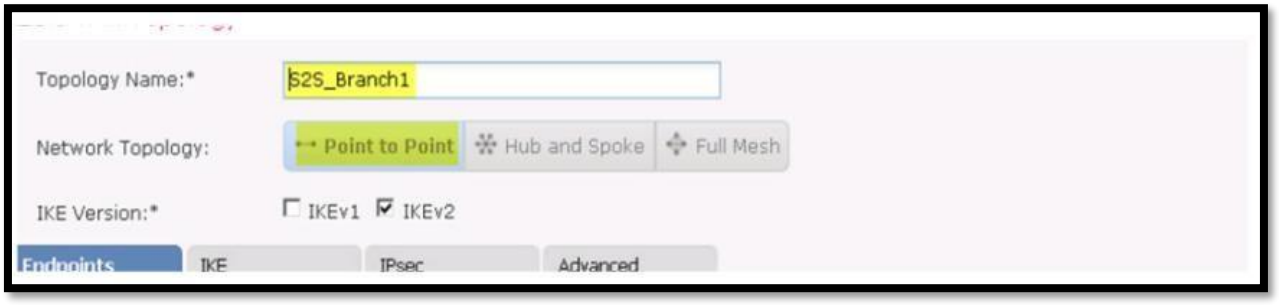
1. Navigate to **Objects > Object Management**. The **Network** object page will be selected.
    a. Select **Add Network > Add Object**.
    b. For Name, enter **MainOfficeNetwork**.
    c. Select the **Network** radio button
    d. Enter **198.19.10.0/24**.
    e. Click **Save**.
2. Click Add **Network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

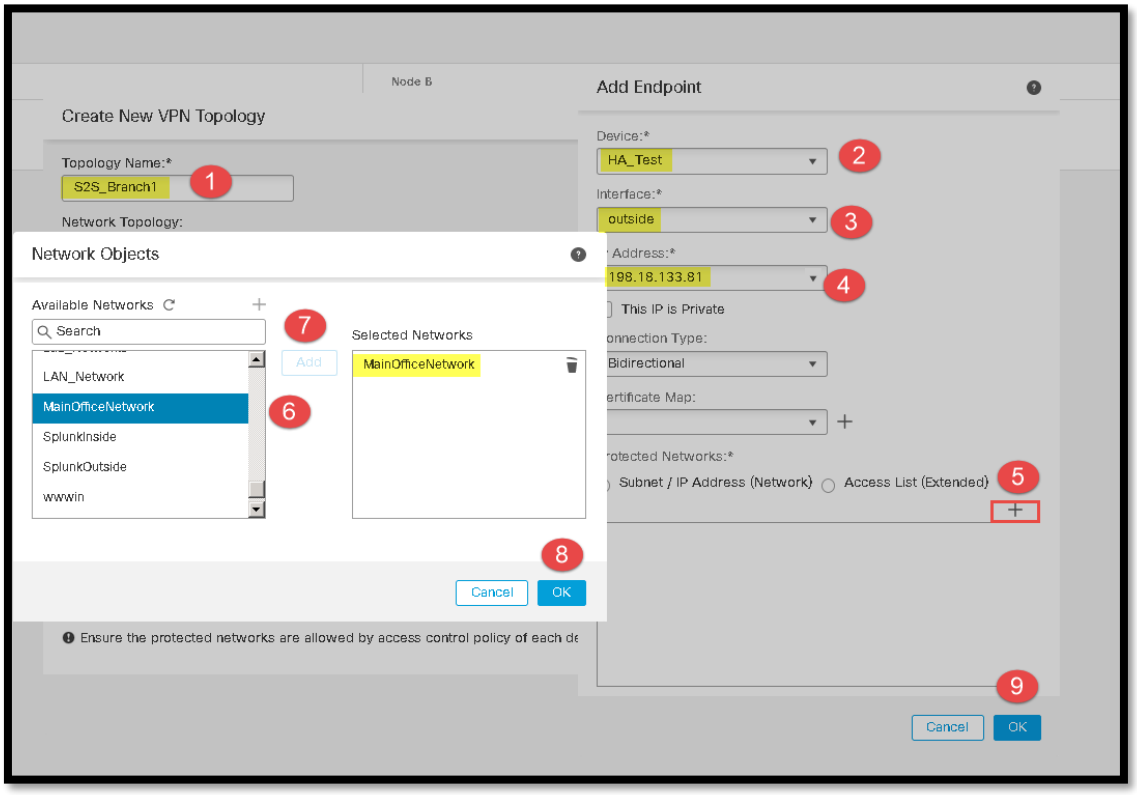
1. Navigate to **Devices > VPN > Site To Site**. Click **Add VPN > Firepower Threat Defense Device**.

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

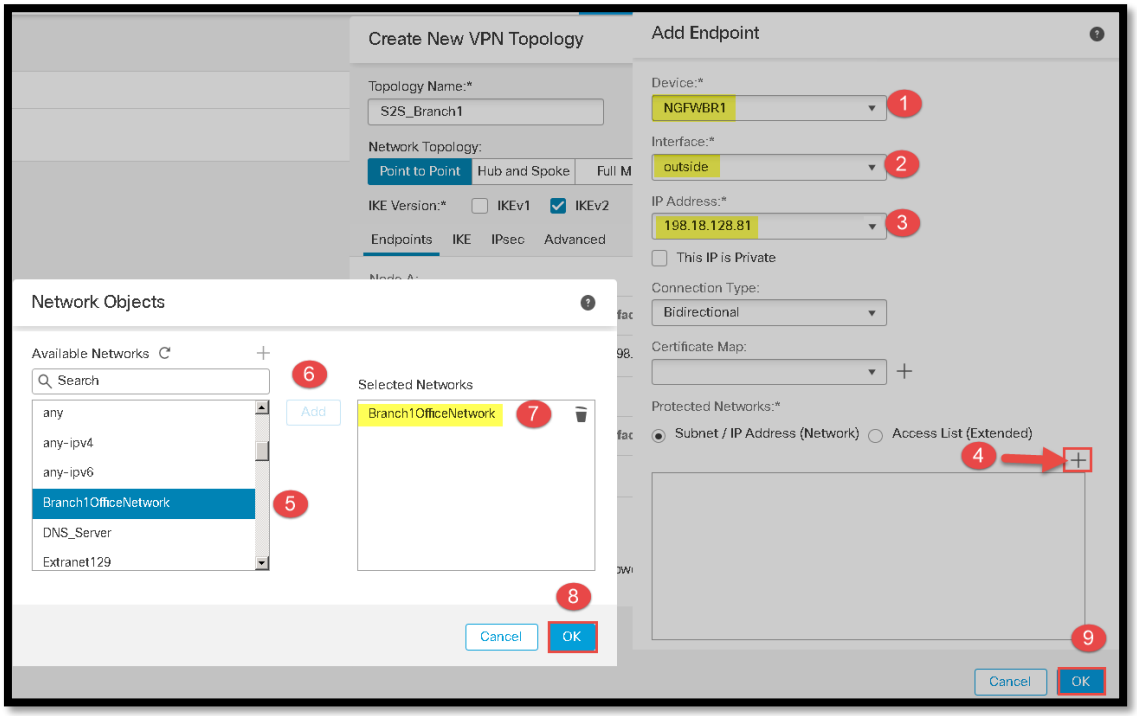
2. For Name enter **S2S_Branch1**.
    a. Confirm that for Network Topology, Point to Point is selected. Confirm that for IKE Version, IKEv1 is not checked, and IKEv2 is checked.



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



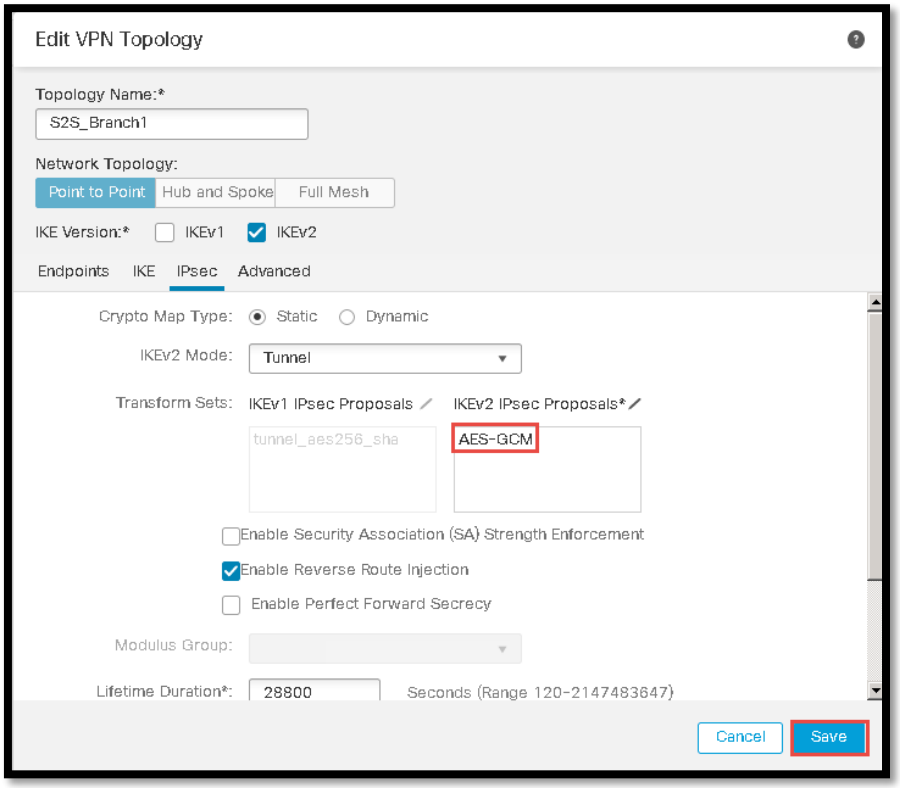
4. Click the **plus (+)** icon to the right of **Node B**. Fill out the fields in the figure below, then click **OK**.



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.

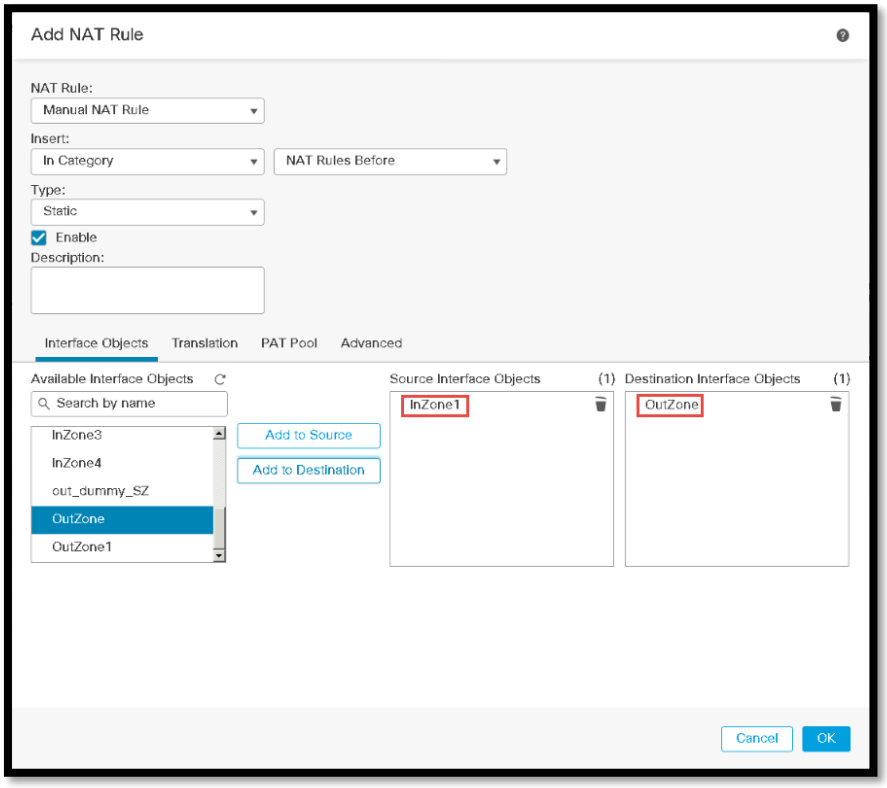
8. Select the **IPsec tab**, change the IKEv2 IPsec Proposal to Verify **AES-GCM**.
9. Click **OK** and **Save**.



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**.

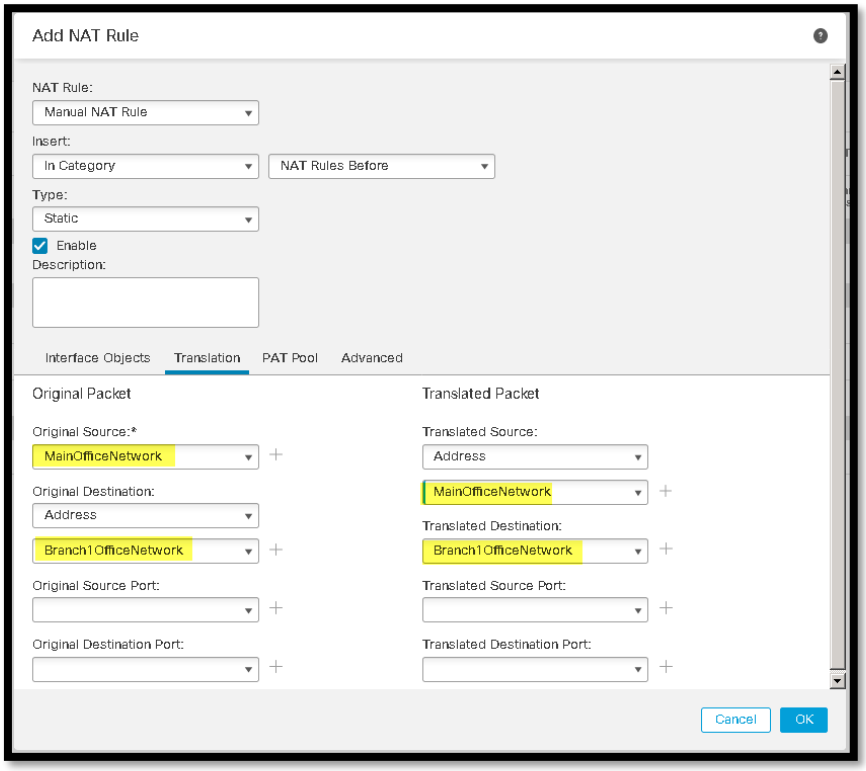
4. Select the **Translation** tab.

a. Select **MainOfficeNetwork** from the Original Source drop-down list.

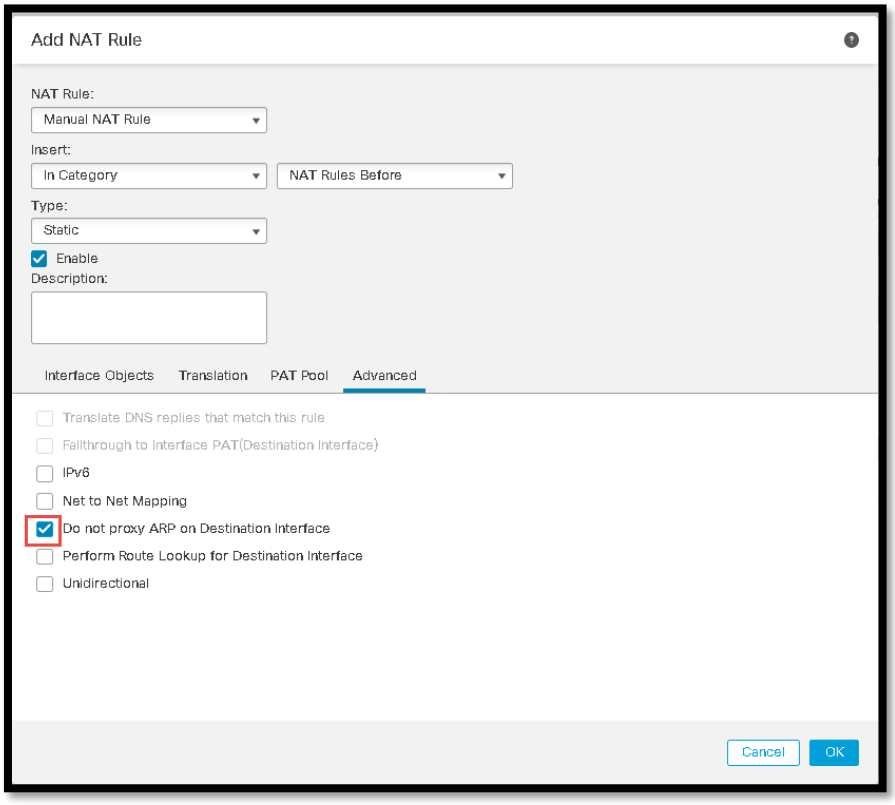
b. Select **MainOfficeNetwork** from the Translated Source drop-down list.

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

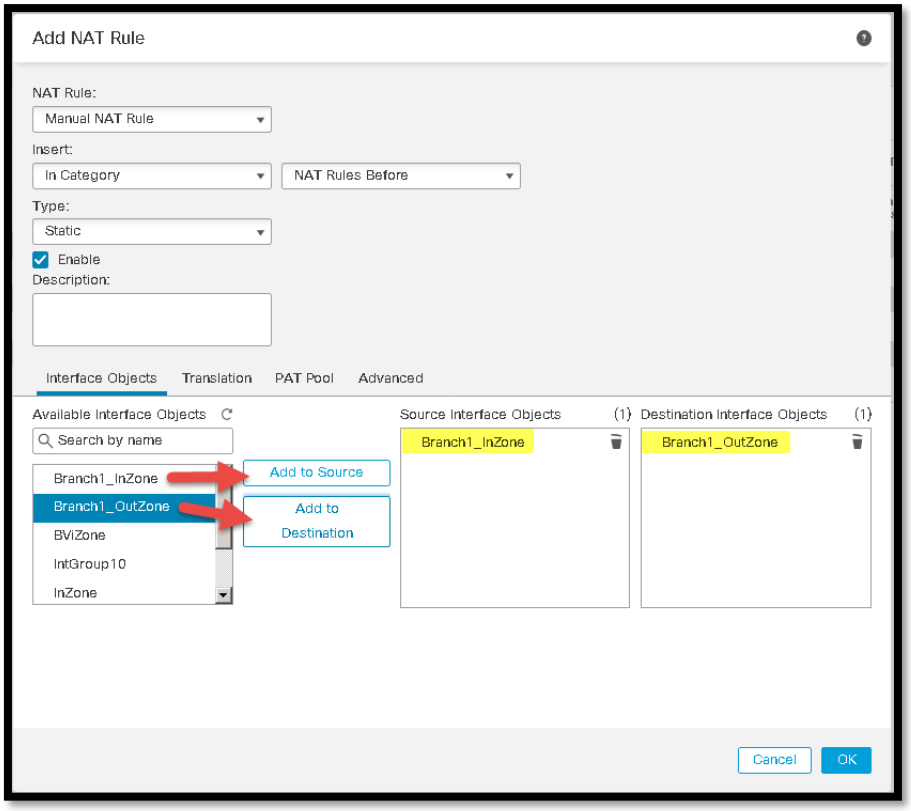
1. Go to **Devices > NAT > Branch NAT >** click the pencil icon to edit the NAT policy

2. Click **Add Rule**.

    a. Interface Objects

        i. Click **Branch1_InZone** and **Add to Source**.

        ii. Click **Branch1_OutZone** and **Add to Destination**.



    b. Translation

        i. Original Packet

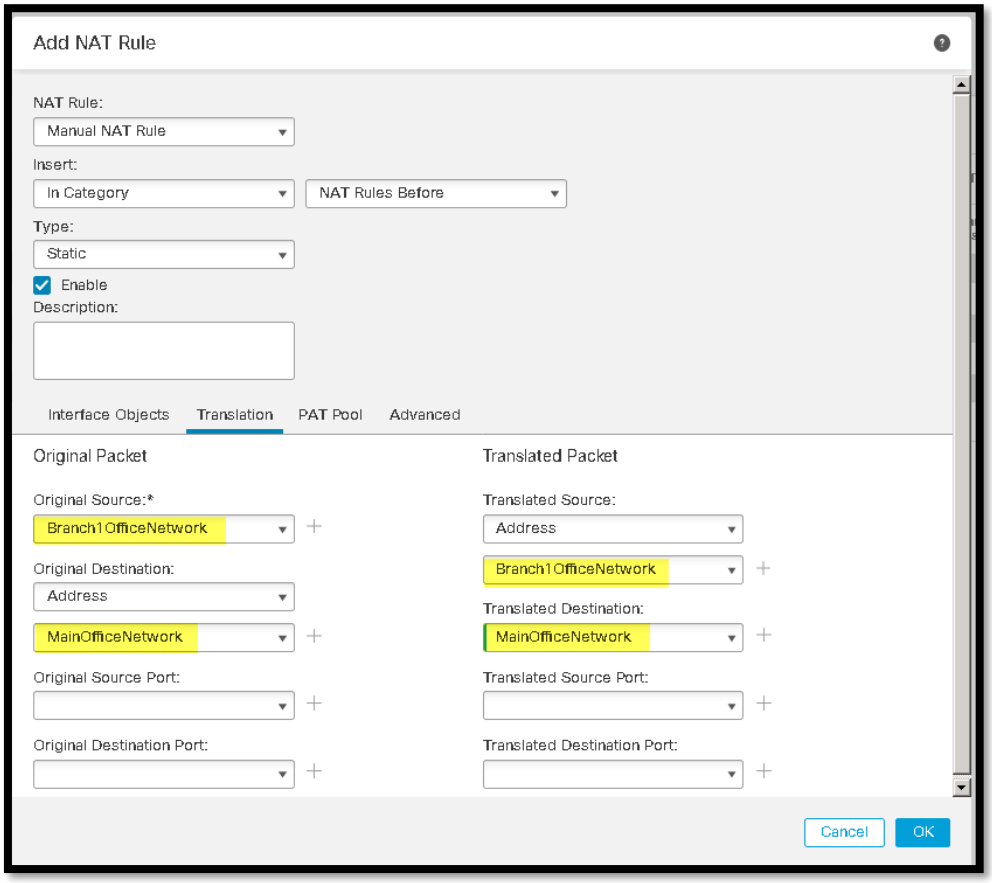
            1. Original Source Branch1OfficeNetwork

            2. Original Destination MainOfficenetwork

        ii. Translated Packet

            1. Translated Source Branch1OfficeNetwork

            2. Translated Destination MainOfficenetwork



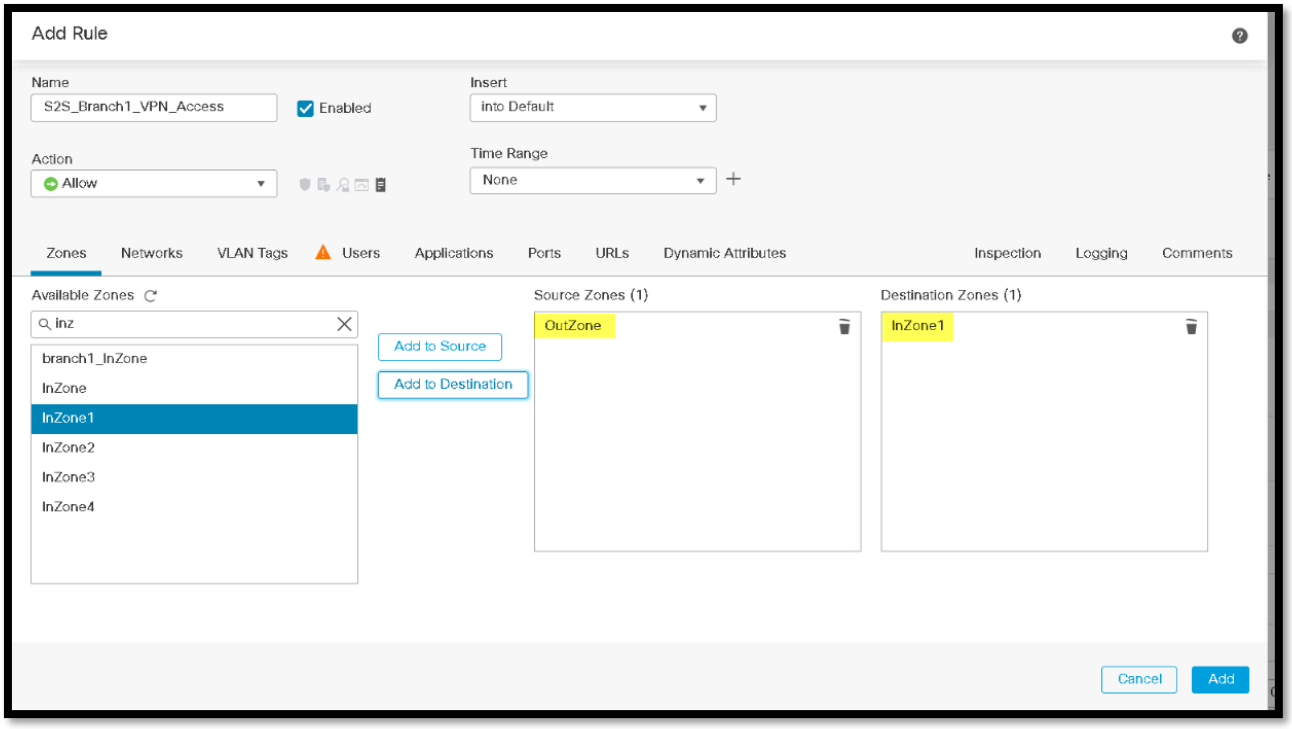
c. Advanced
   i. On the Destination Interface, click **Do not proxy ARP on Destination Interface**

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 **Branch1OfficeNetwor**k, 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

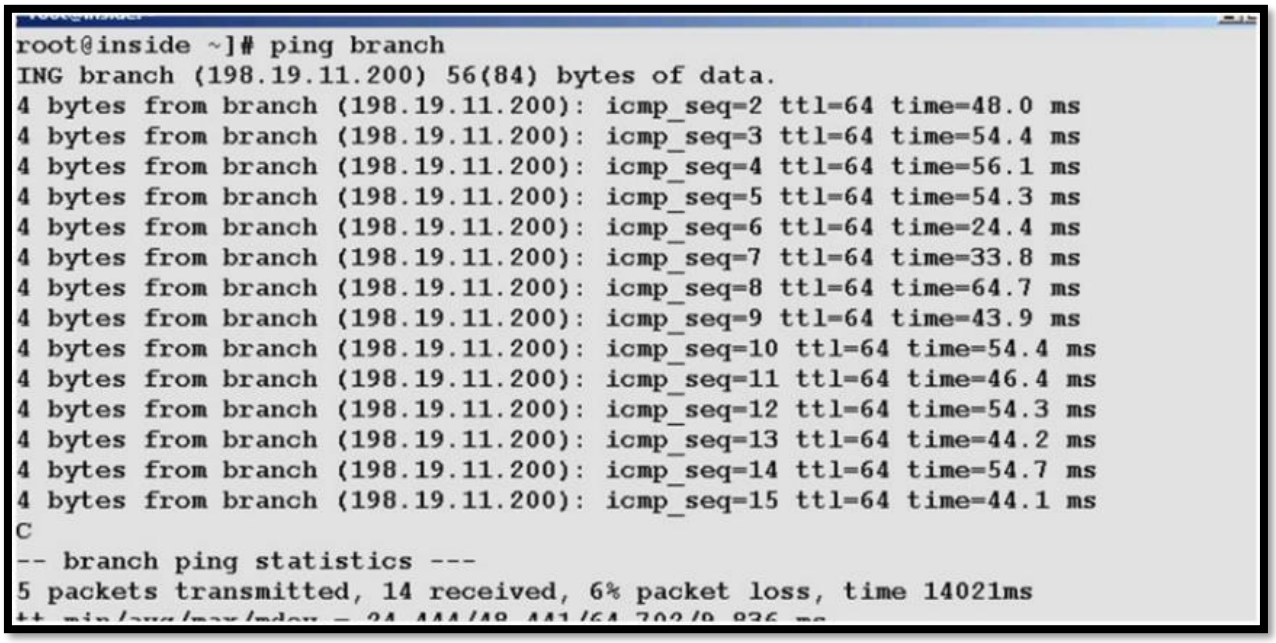
17. **Examine the Branch1_NAT Policy** to confirm the VPN NAT Exemption the first rule

Deploy the changes and test the configuration

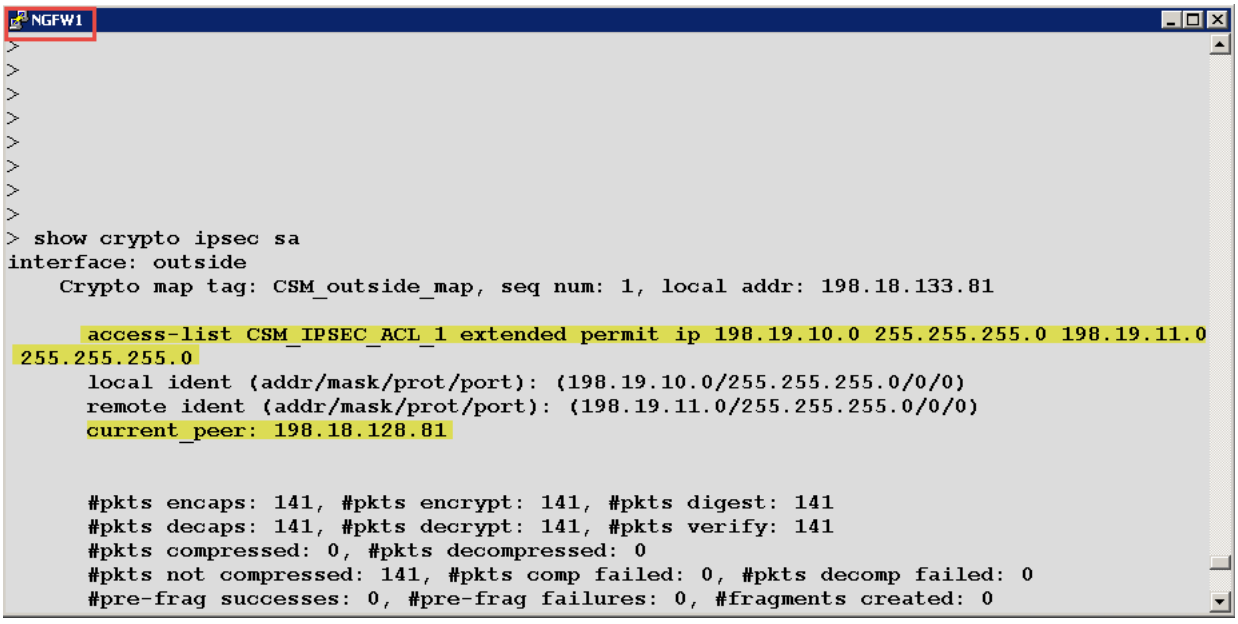
1. **Deploy the changes on the FMC and wait for the deployment to complete.**
2. Go to the Jump PC Open PUTTY Connect to **NGFW1** and **NGFWBR1** Login: **admin** Password: **C1sco12345**
3. From the **NGFW1 CLI**, type **show crypto ipsec sa peer 198.18.128.81**. There should be no IPSec security associations.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



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



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.

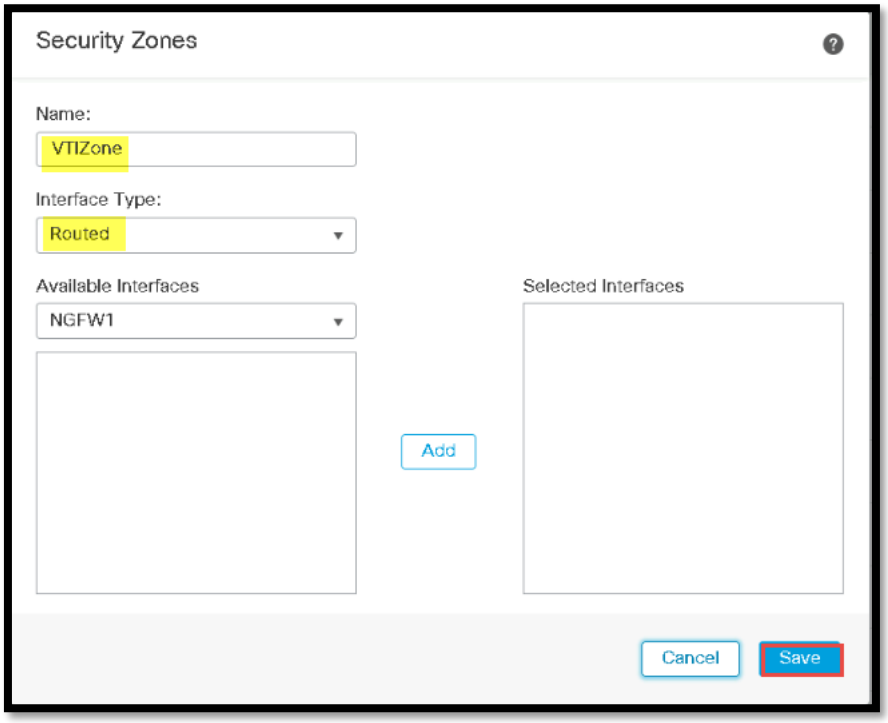
Policy based vs Route-Based VPN. Both are now available with the FTD. Route based VPN's are more flexible than Policy-Based VPN, but for some applications Policy-Based VPN's may be needed.

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

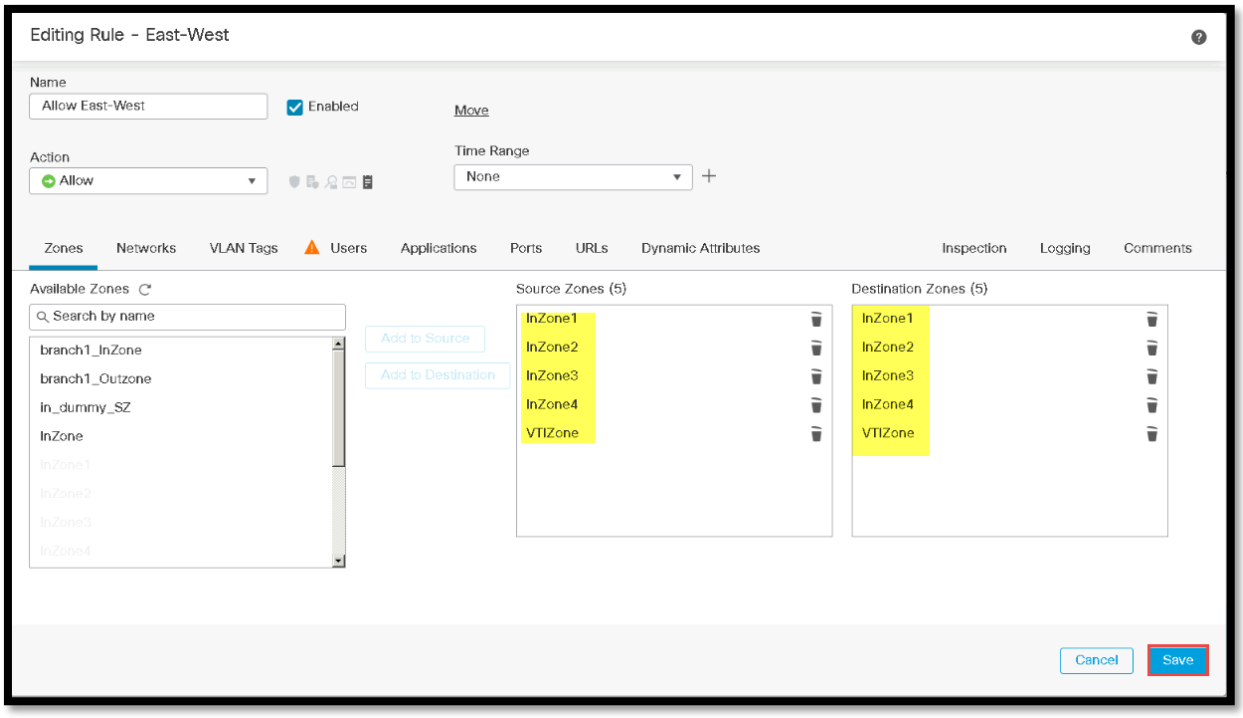
1. On the FMC go to **Objects > Object Management**
2. Select **Interface** from the left navigation pane
3. Click **Add > Security Zones**
    a. Name: VTIZone
    b. Select: **Routed**
    c. **Save**



Modify the Access Control Policies on NGFW1 and NGFWBr1

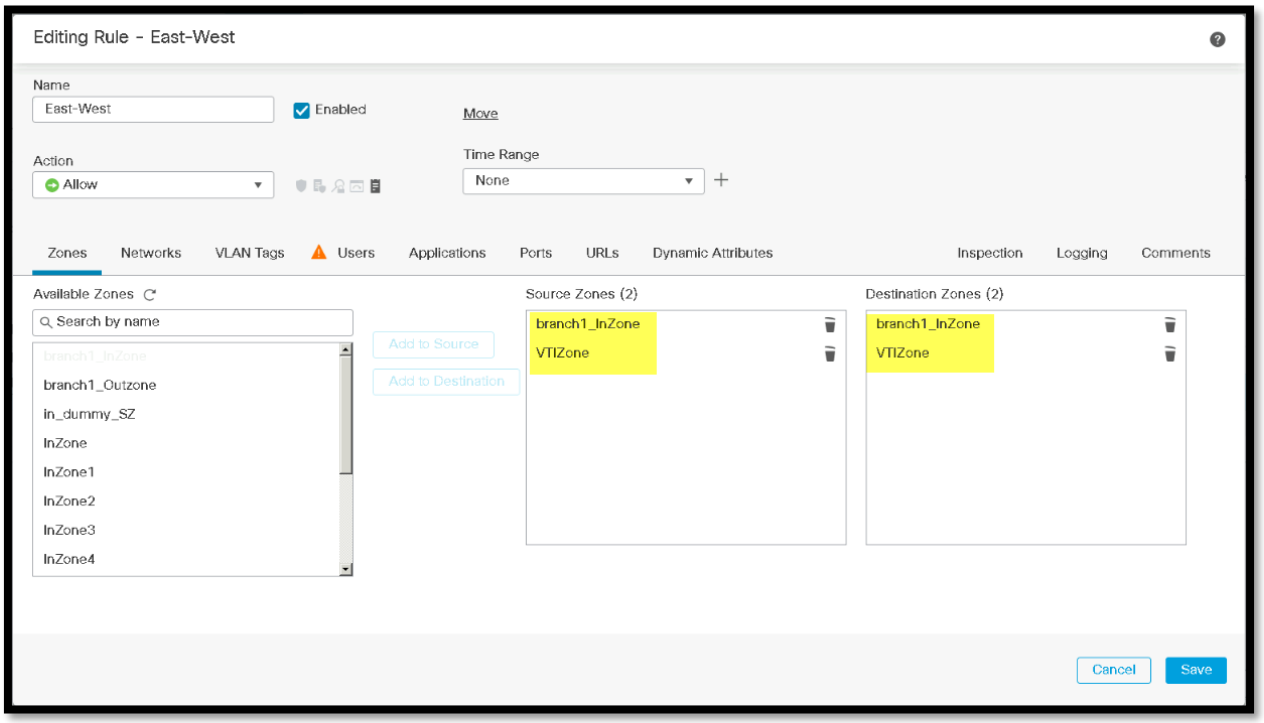
1. Go to **Policies > Access Control**
2. Edit the **Base_Policy**
    a. Create or Edit the rule **Allow East-West**

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

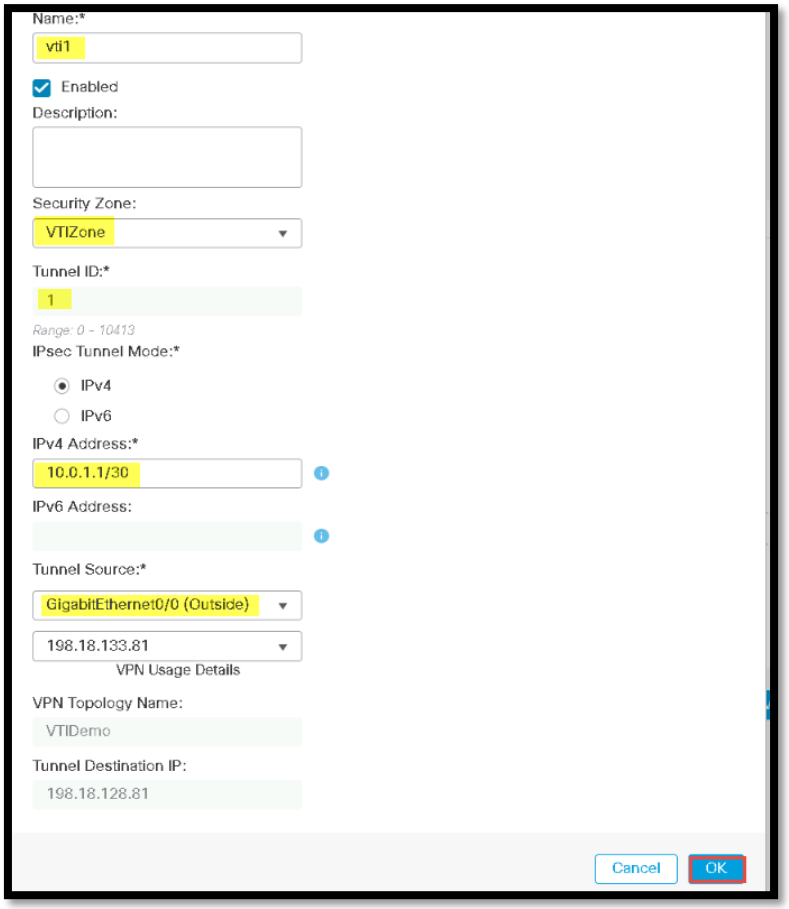


c. Click Add and **Save and Save the Policy**

If you did the Remote Deployment Lab on NGFRBr1 disable the remote management and redeploy

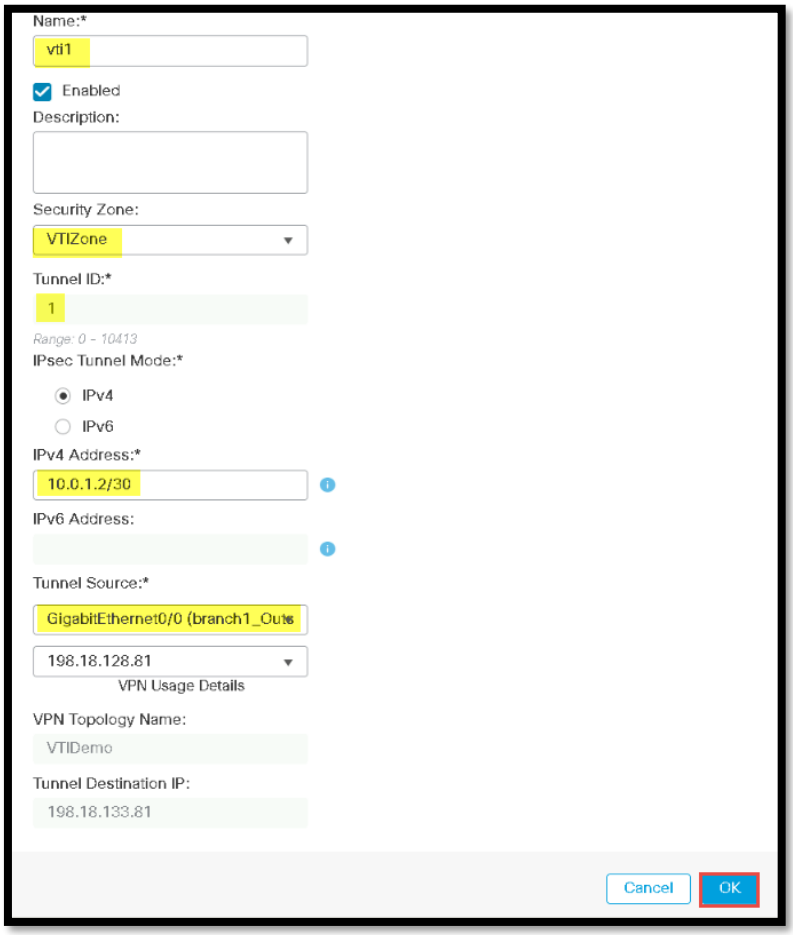
Compare Policy-Based and Route-Based VPN configuration

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)

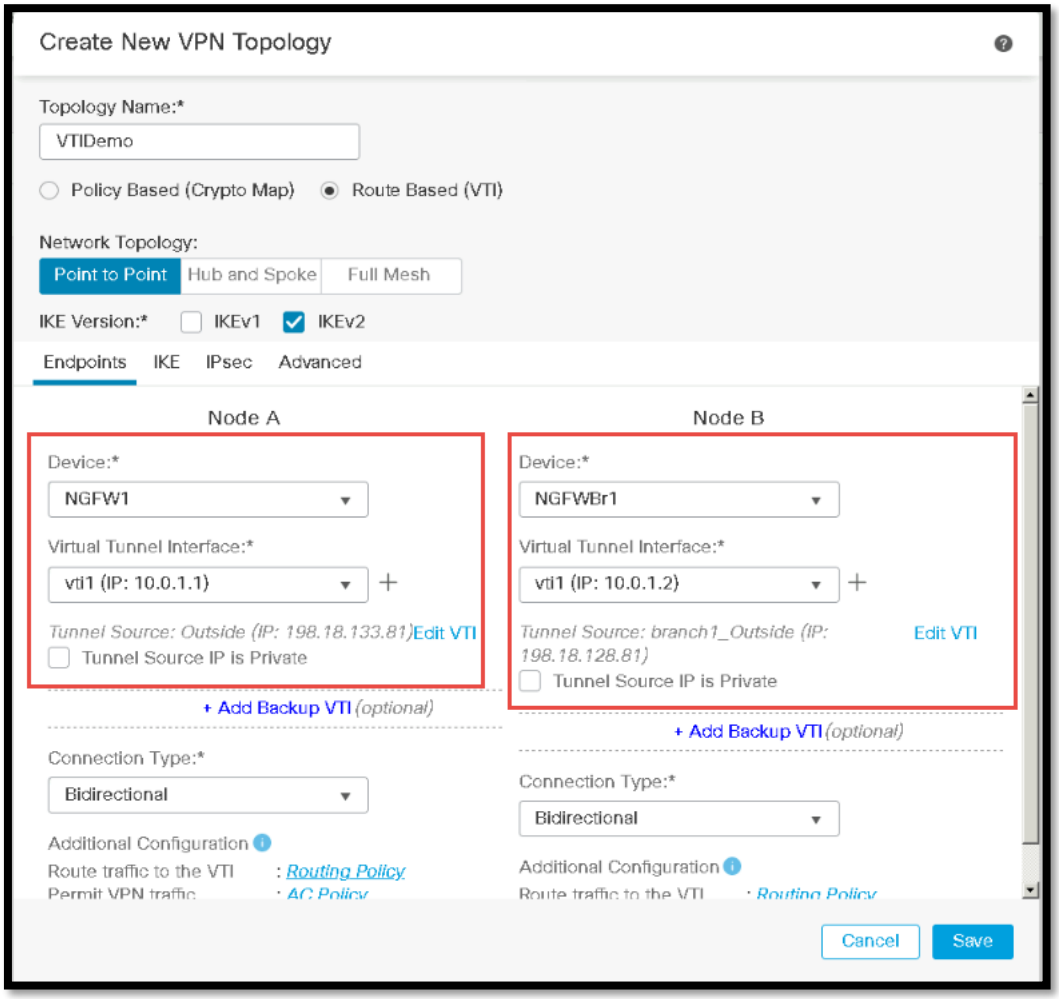


            6. Click **OK**
        iii. Node B: NGFWBr1
        iv. Virtual Tunnel Interface: Click on the [+]

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)



6. Click **OK**

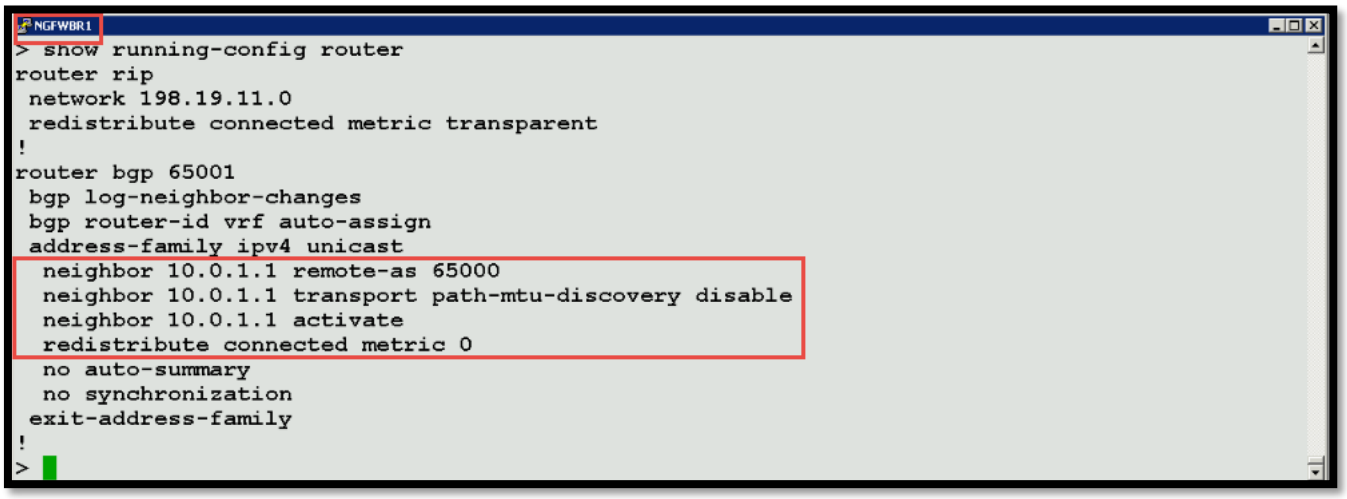


5. Click **Save** and then **Deploy > Select NGFWBr1 and NGFW1**

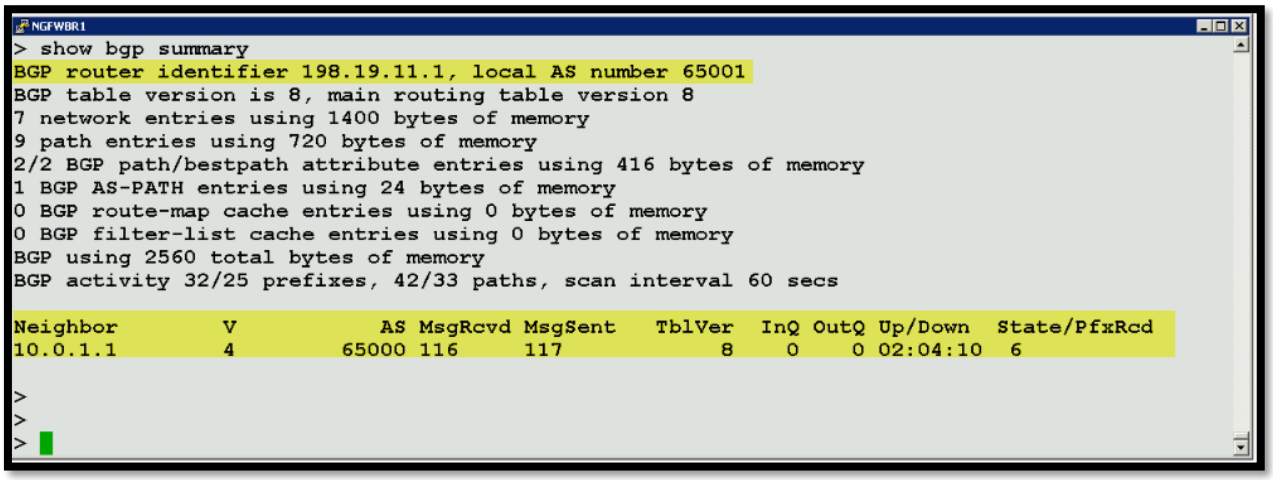
Configure BGP

1. FMC **Devices > Device Management**
2. Edit **NGFW1 and select Routing**
    a. Under General Settings select **BGP**
        i. Click Enable BGP if not already enables
        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



    c. Type **show bgp summary**



    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.

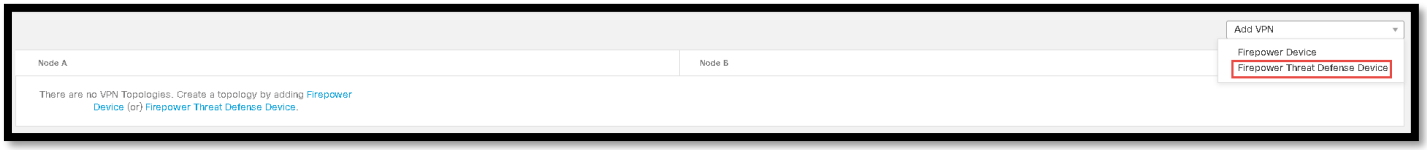
Steps

Lab Preparation

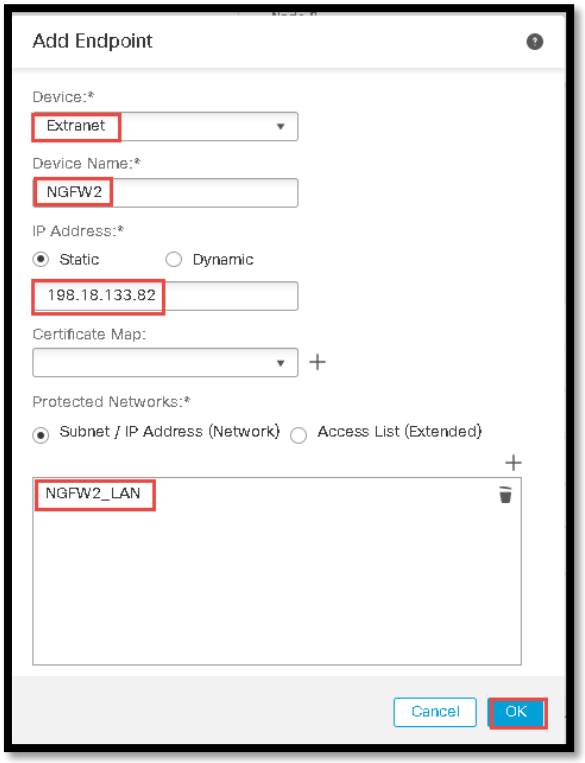
1. Open a PUTTY session to the Inside Linux Server Username: root Password: C1sco12345
    a. Type route add –net 198.19.11.0 netmask 255.255.255.0 gw 198.19.10.2
        i. This will set the path for the Inside Linux server to reach the Branch1 LAN network

Configure S2S VPN on FMC managing NGFW Branch 1

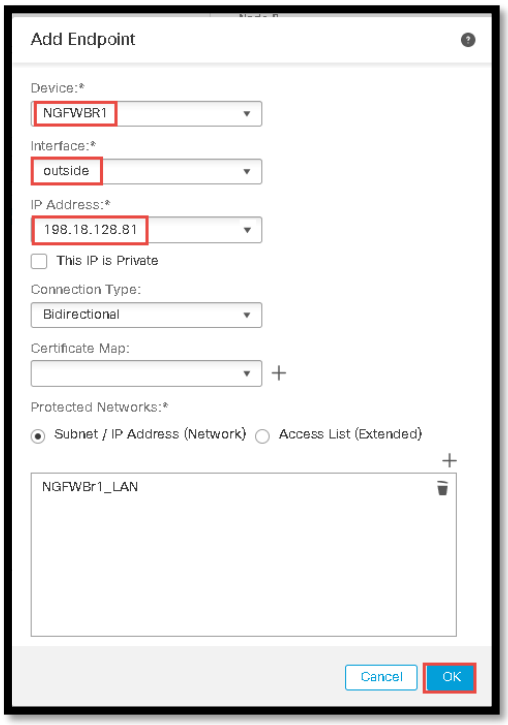
1. On the Jumpbox, open Firefox and click on FMC in the bookmarks list. Login to the FMC.
2. Navigate to Objects > Object Management > Network. Click on Add Object.
    a. Enter NGFWBr1_LAN as the Name.
    b. Set Network to Network and type in 198.19.11.0/24.
    c. Click on Save.
3. Click on Add Object.
    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

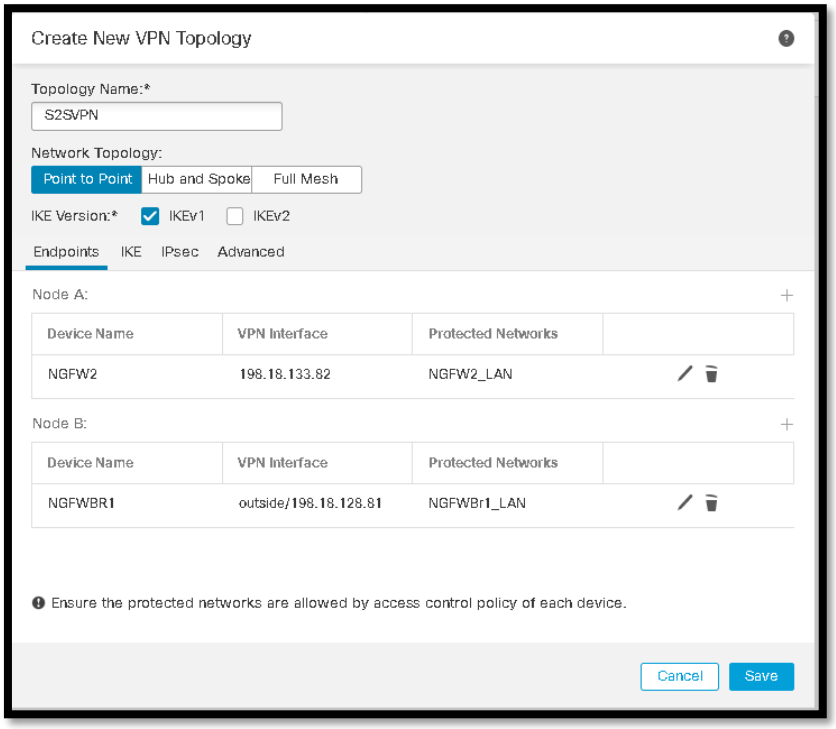


    a. Enter Topology Name: **S2SVPN**
    b. b. Set IKE Version to IKEv1 only.
    c. c. Under Endpoints, click on + for Node A.
        i. Select **Extranet** as Device.
        ii. Enter **NGFW2** as Device Name.
        iii. Set IP Address as Static and **198.18.133.82**.
        iv. Under Protected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

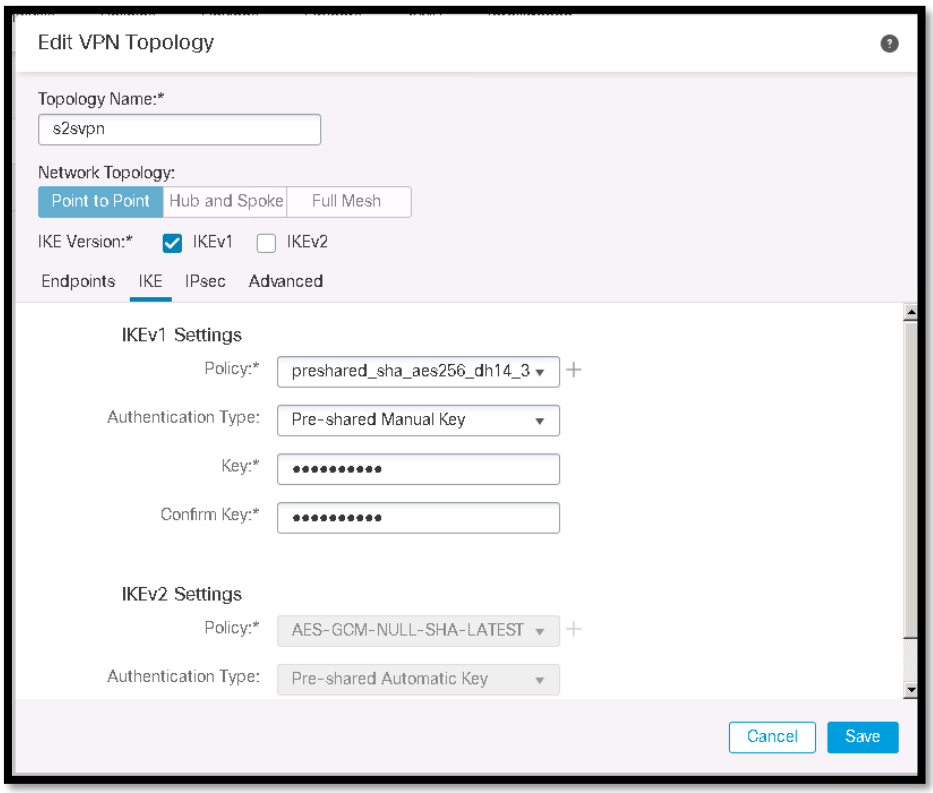


d. Under Endpoints, click on + for Node B.
   i. Select **NGFWBR1** as Device.
   ii. Set Interface as **branch1_outside**.
   iii. IP Address will populate as **198.18.128.81**.
   iv. Under Protected Networks, add the **NGFWBr1_LAN** object.
   v. Click on **OK**.

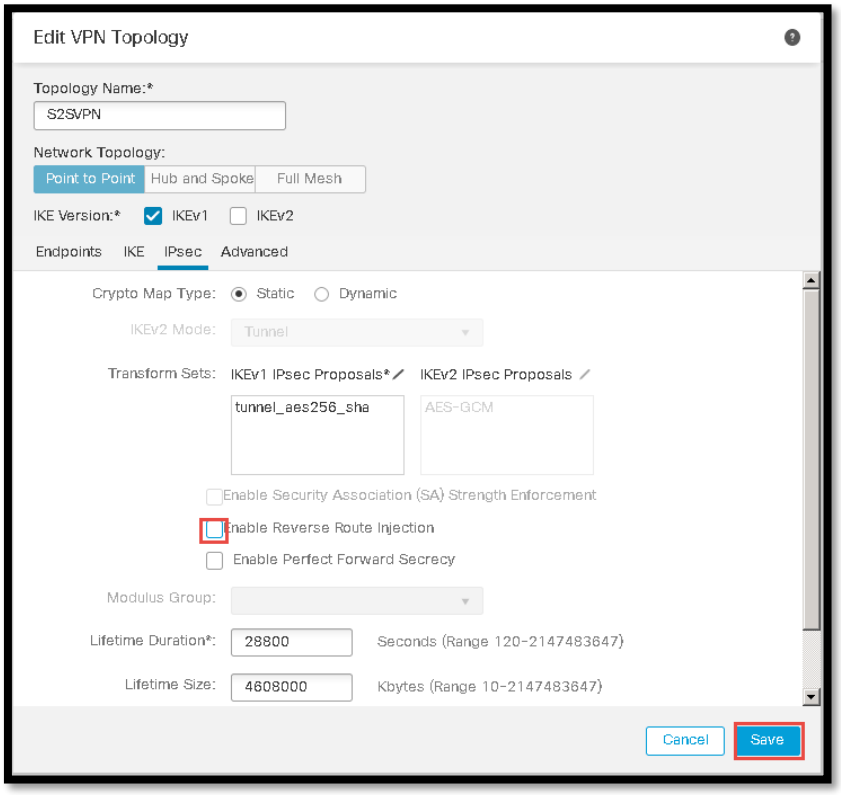




e. Navigate to IKE.
   i. Change IKEv1 Policy to **preshared_sha_aes256_dh14_3**
   ii. Authentication Type: **Pre-shared Manual Key**
   iii. Key: **C1sco12345**
   iv. Confirm Key: **C1sco12345**

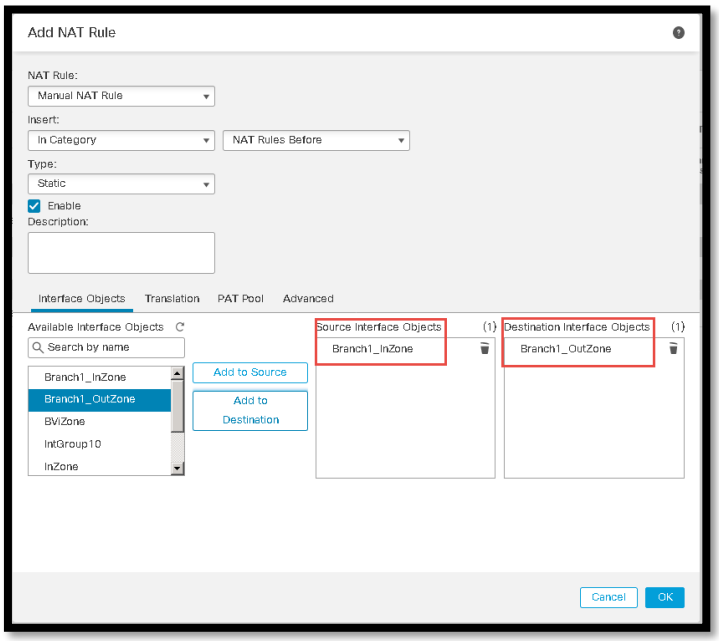


f. Navigate to IPSec
   i. **Uncheck Enable Reverse Route Injection**

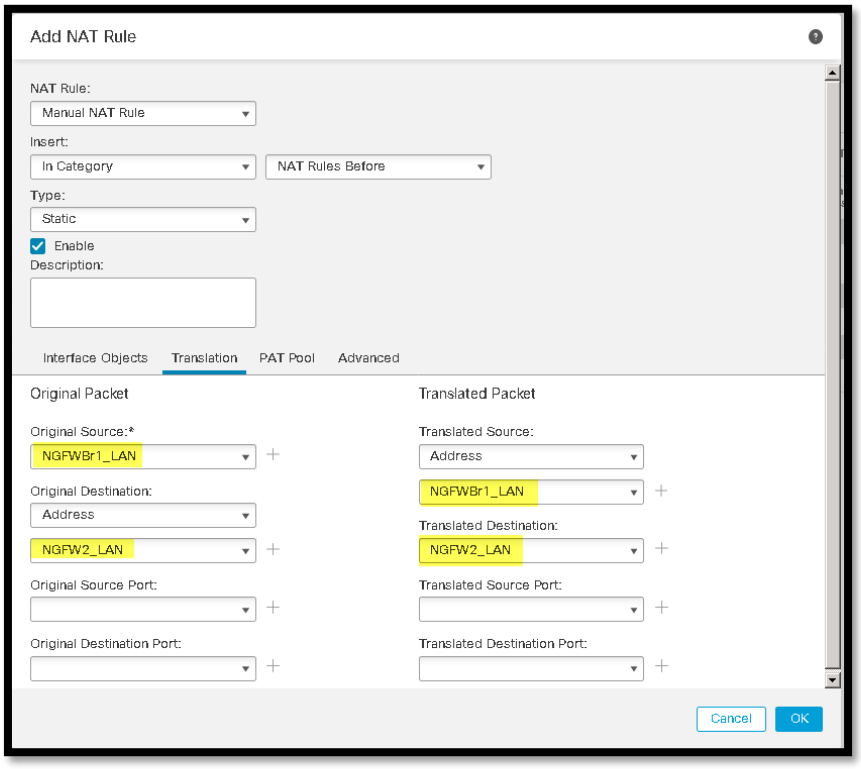


g. Click on Save.

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

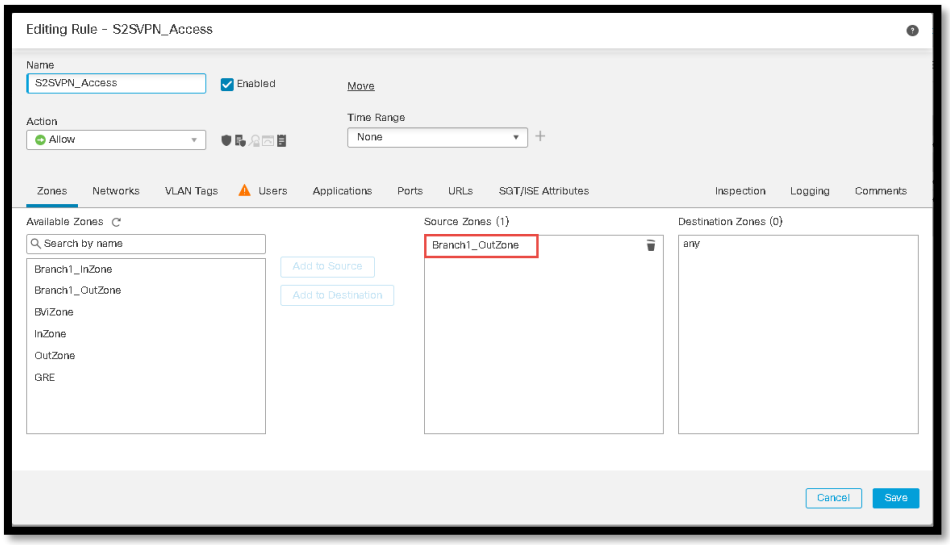


b. Under the Translation tab, select **NGFWBr1_LAN** as Original Source and Translated Source. Select **NGFW2_LAN** as the Original Destination and Translated Destination.
c. On the Advanced Tab select **Do not proxy ARP on Destination Interface**



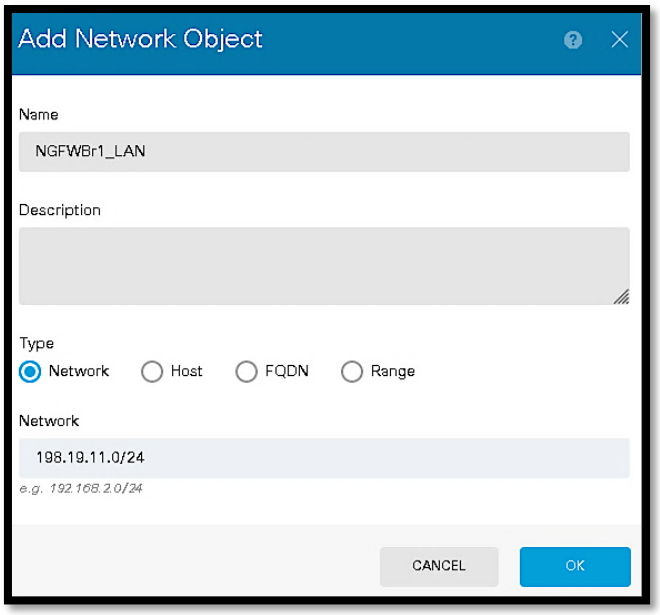
d. Click **OK** to save the NAT rule. Click on **Save.**

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.

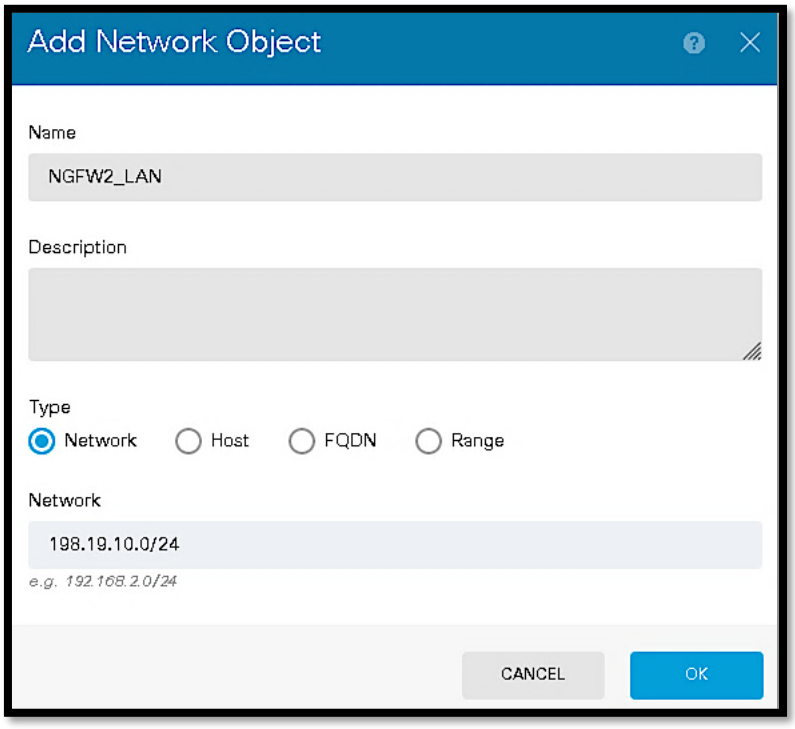


Configure S2S VPN on FDM managing NGFW2

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**

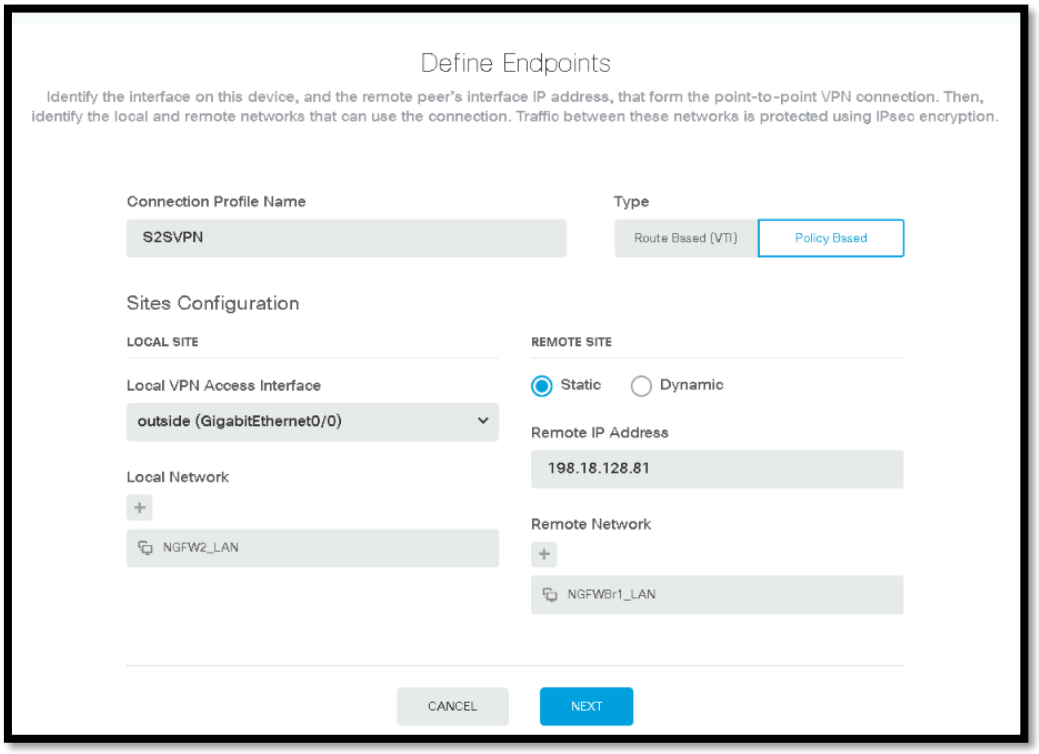


    b. Repeat steps for: **NGFW2_LAN**, Type as Network and Network as **198.19.10.0/24**.

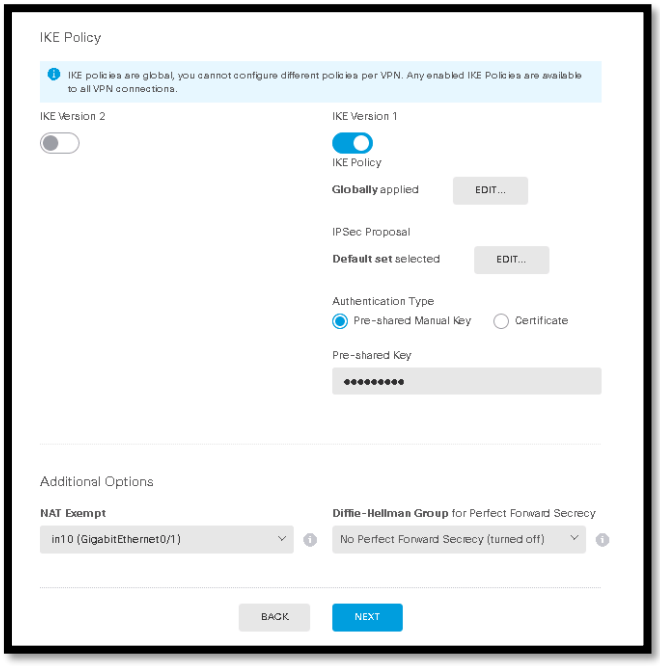


3. Navigate to Device > Site to Site VPN > View Configuration. Click on +.

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**.



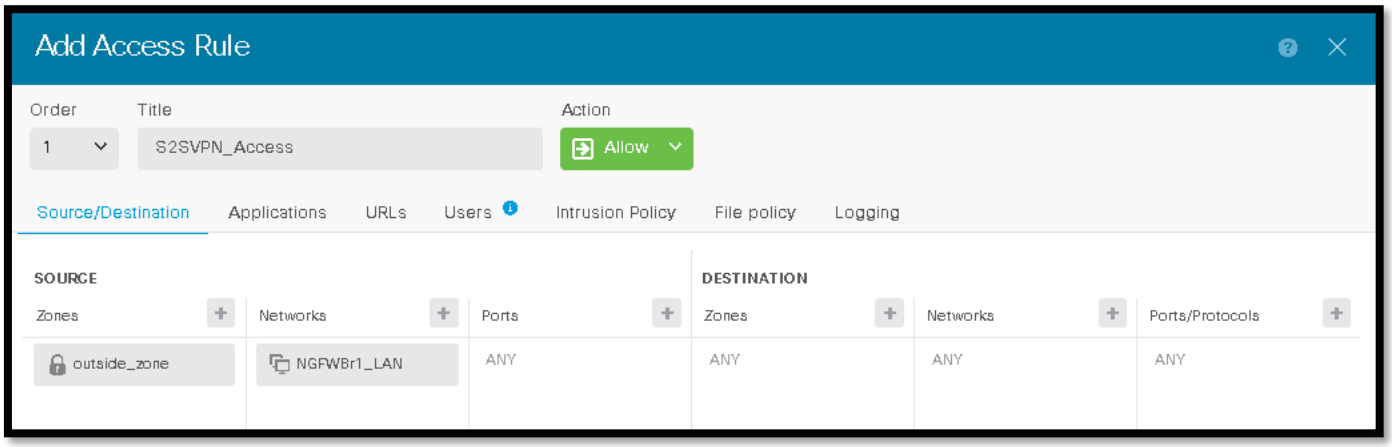
g. **Enable IKEv1** and **disable IKEv2**.
h. Edit IKE Policy and enable **SHA-AES256-GROUP14-PRE_SHARED_KEY**
i. Edit IPSec Proposal and click on **Set Default** and **OK**.
j. Select Authentication Type. **Pre-shared Manual Key**
k. Pre-shared Key: **C1sco12345**
l. Under Additional Options select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



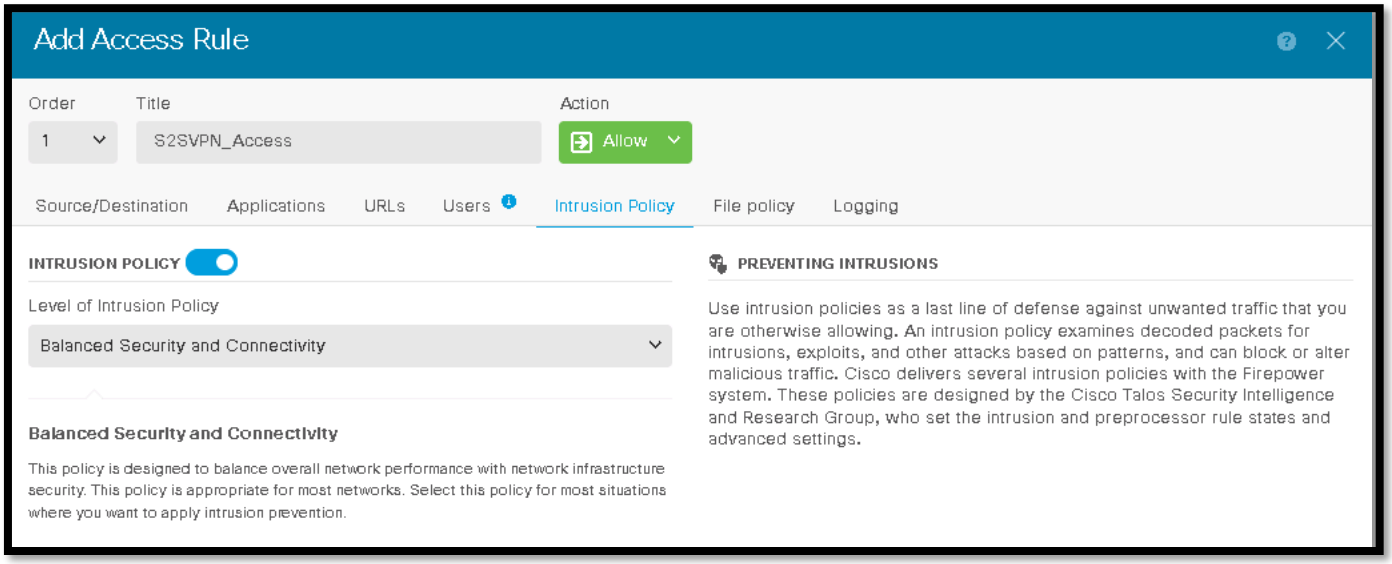
4. Click on Next
    a. Review the Summary and click on Finish.

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

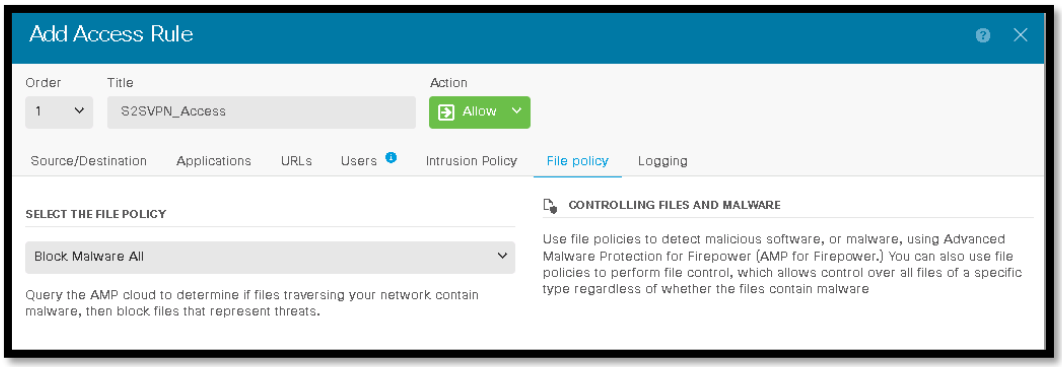
5. Navigate to Policies > Access Control. Click on +.
    a. For the new rule, set Order to 1.
    b. Name will be **S2SVPN_Access** and Action will be **Allow**.
    c. Set Source Zone to **outside_zone** and Source Networks to **NGFWBr1_LAN**.



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



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



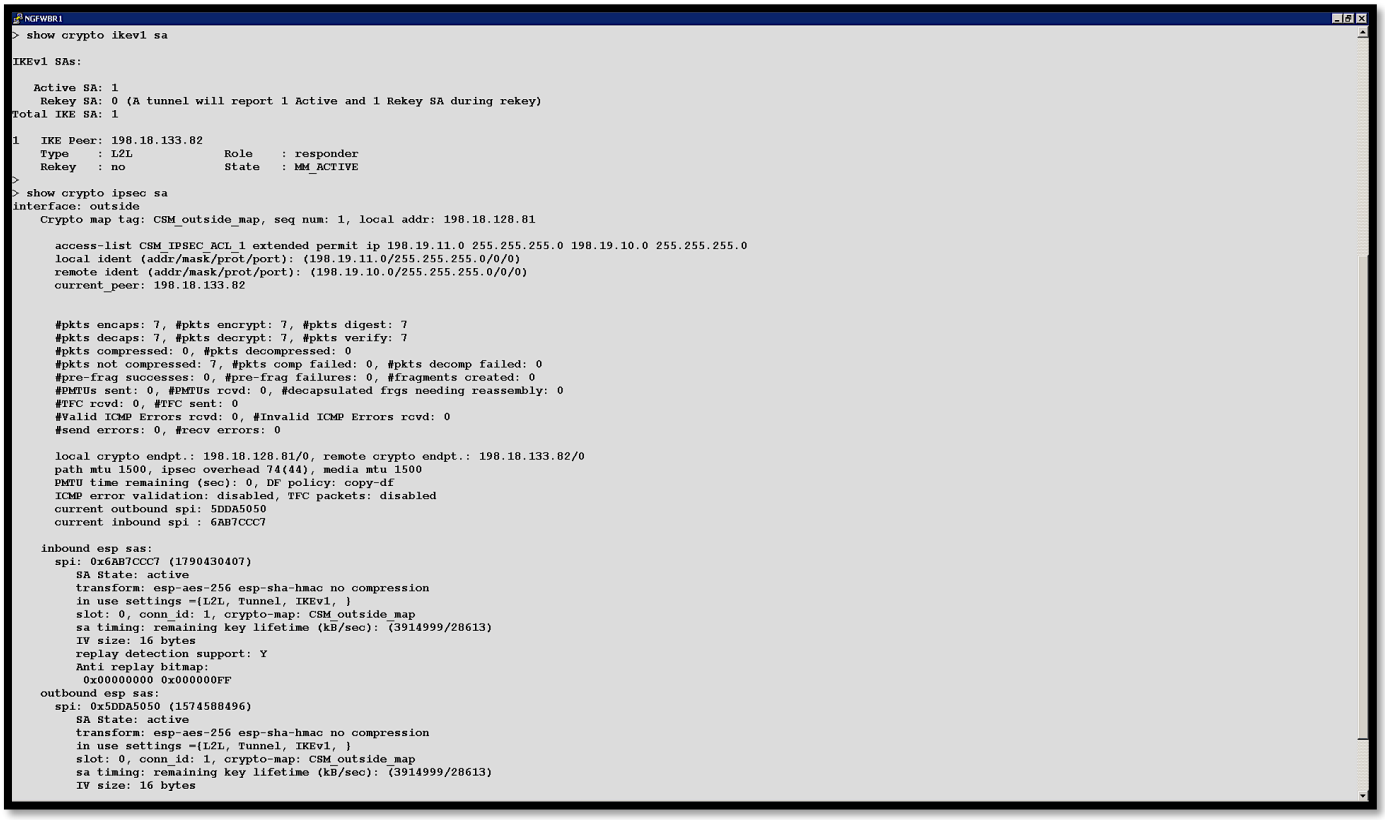
f. Navigate to Logging. Select At End of Connection for Select Log Action. Click on OK.

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.



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 l2l.

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

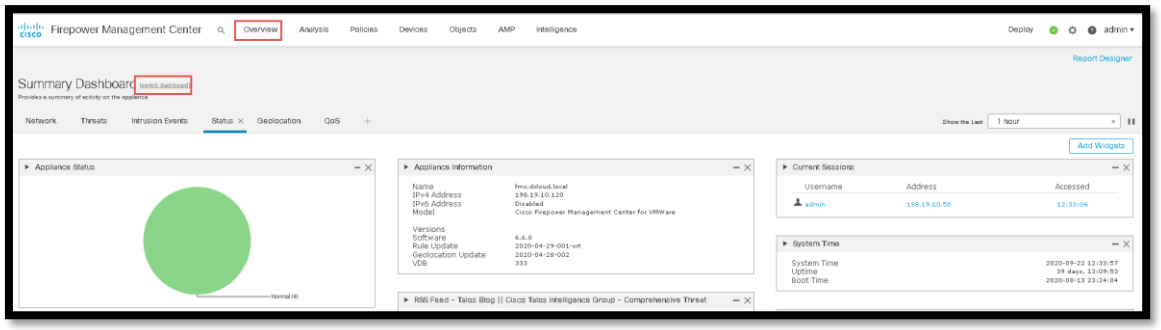
You will use the FMC for Monitoring AnyConnect User activity and troubleshooting.

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**



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**.

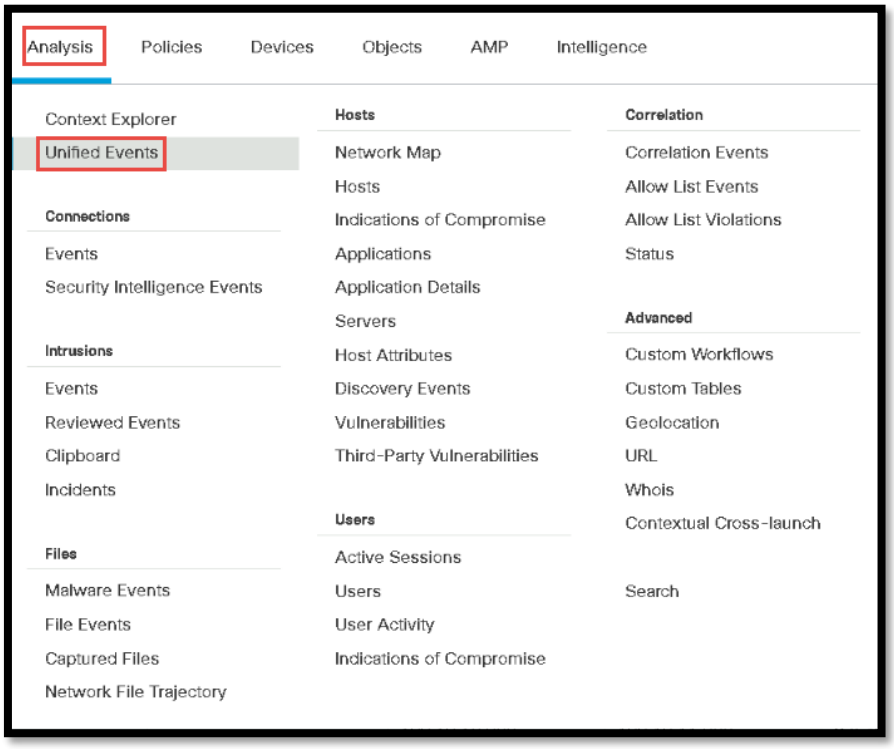
NOTE: You may also see other active sessions discovered with network discovery. For example, you may see guest discovered through an FTP session. For brevity, those sessions were left out of the figure above. If you want more details about users and how they were discovered, navigate to Analysis > Users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

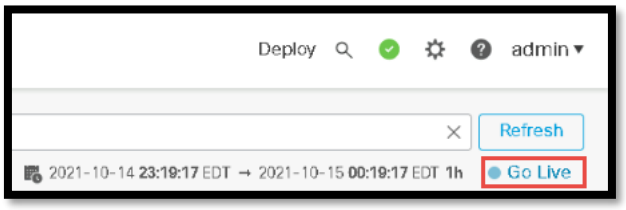
Troubleshooting

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

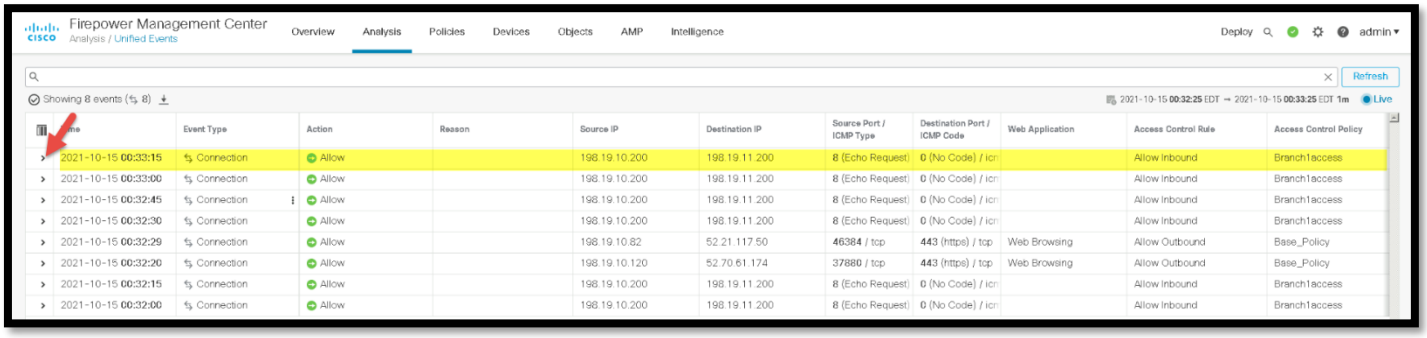
1. FMC **Analysis > Unified Events**



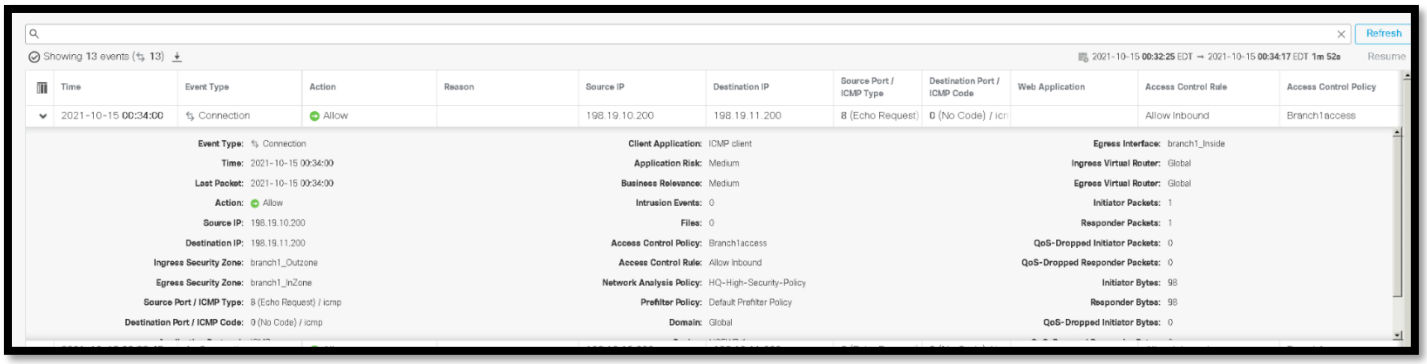
2. In the upper right corner select **Go Live**



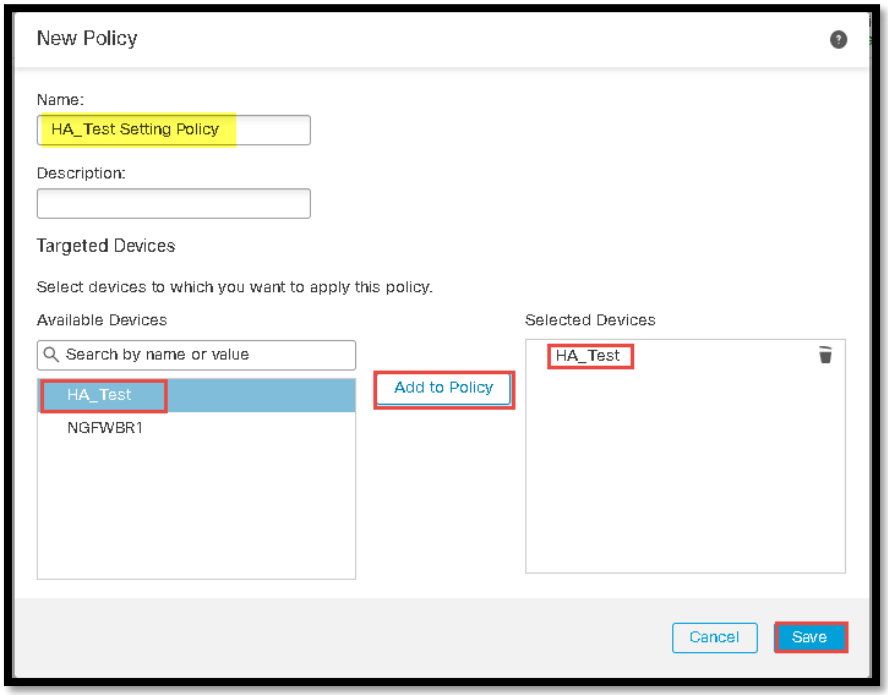
3. Wait a few seconds for the log to populate
    a. Select a Line in the Log



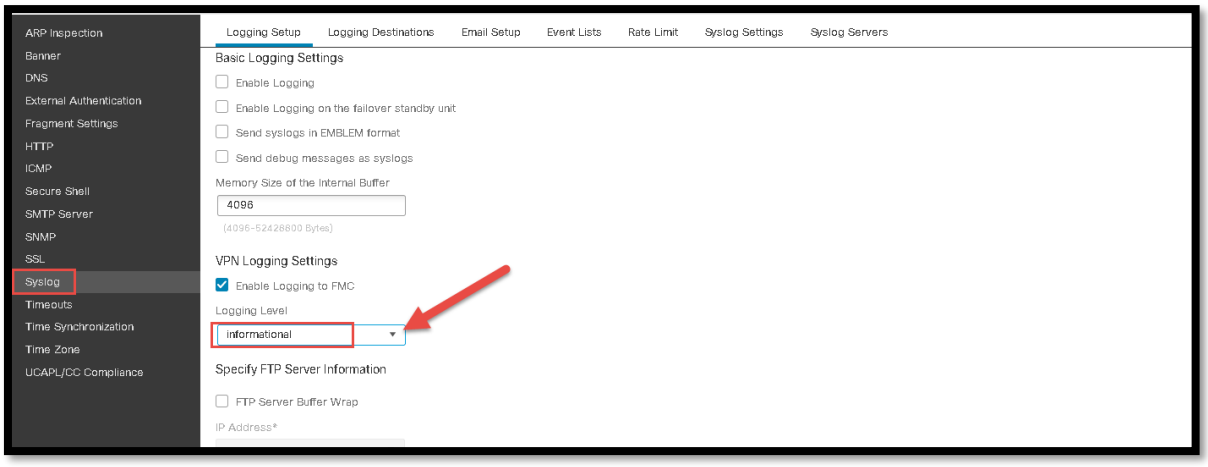
b. Note the information contained in the Log



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**.

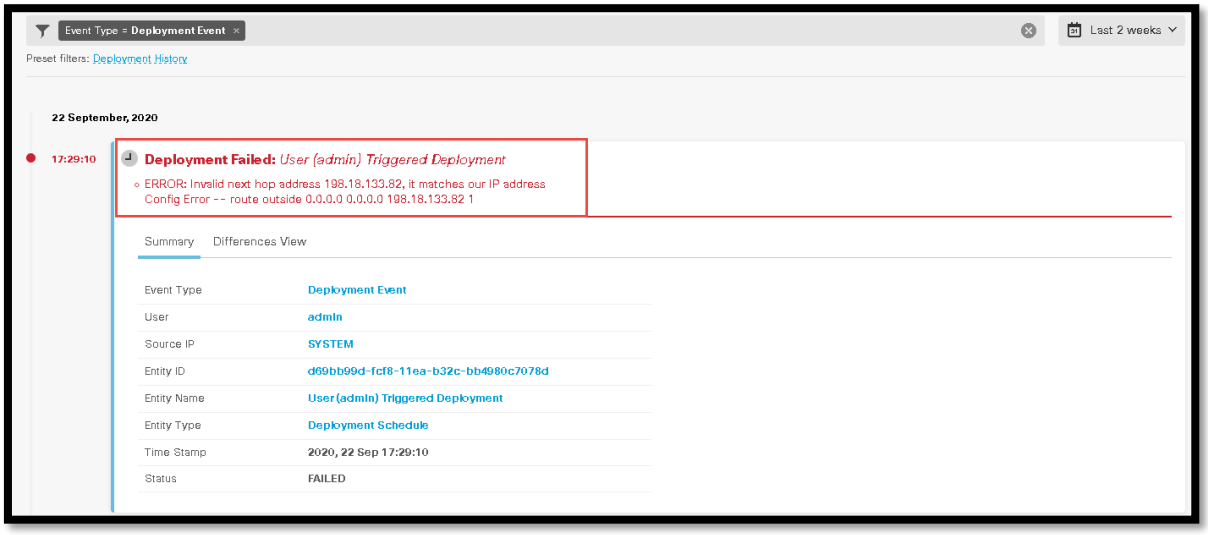


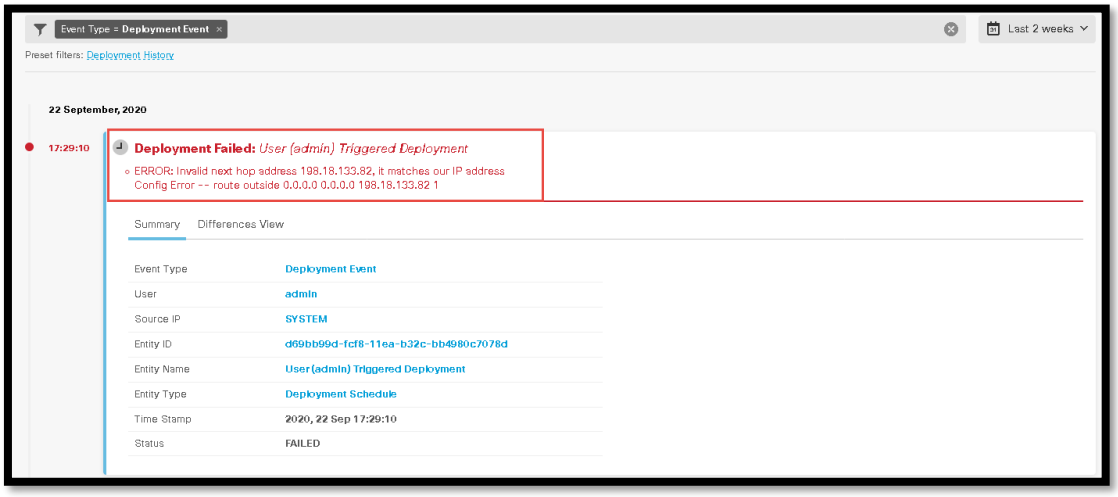
8. Deploy the changes to the **HA_Test**
9. On the Outside-PC, generate some VPN activity. For example, connect and disconnect a VPN session.

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





14. You will see an error that references the next hop address
    a. Go back to the FDM and fix the issue

Troubleshooting with Packet Tracer and Packet Capture

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

Packet-Tracer Lab

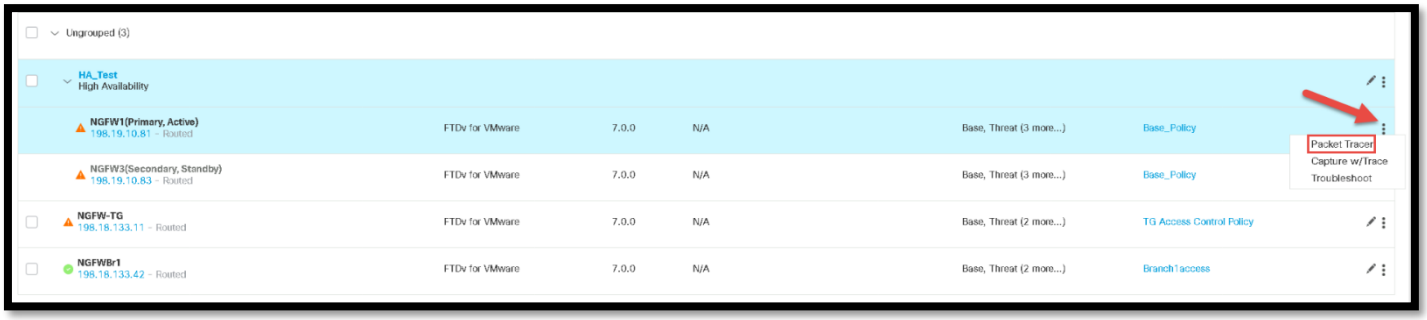
1. On the FMC go to **Policies > Access Control >** Edit the Base_Policy
2. Click Add New Rule
    a. Name: Packet-Trace Rule
    b. Set the Rule ABOVE rule 1
    c. Under Action Block or Block with reset
    d. Zones: Source Zone InZone1, Destination Zone Outzone
    e. Networks: Source: MainOfficenetwork 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.

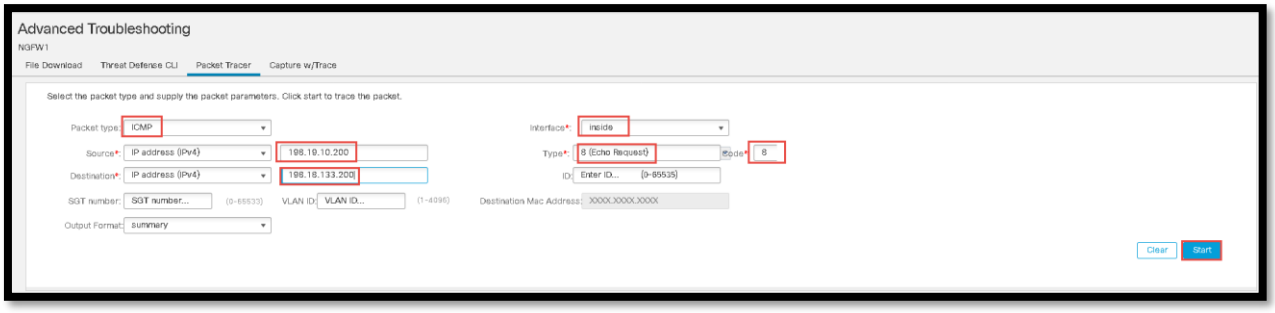
3. Open a PUTTY Session to **NGFW1** Username: **admin** Password **C1sco12345**
4. Type the following **packet-tracer input in10 icmp 198.19.10.200 8 0 198.18.133.200**
    a. Look at Phases you will notice that the packet has been handed off to SNORT for further processing
    b. You will see that 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**



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

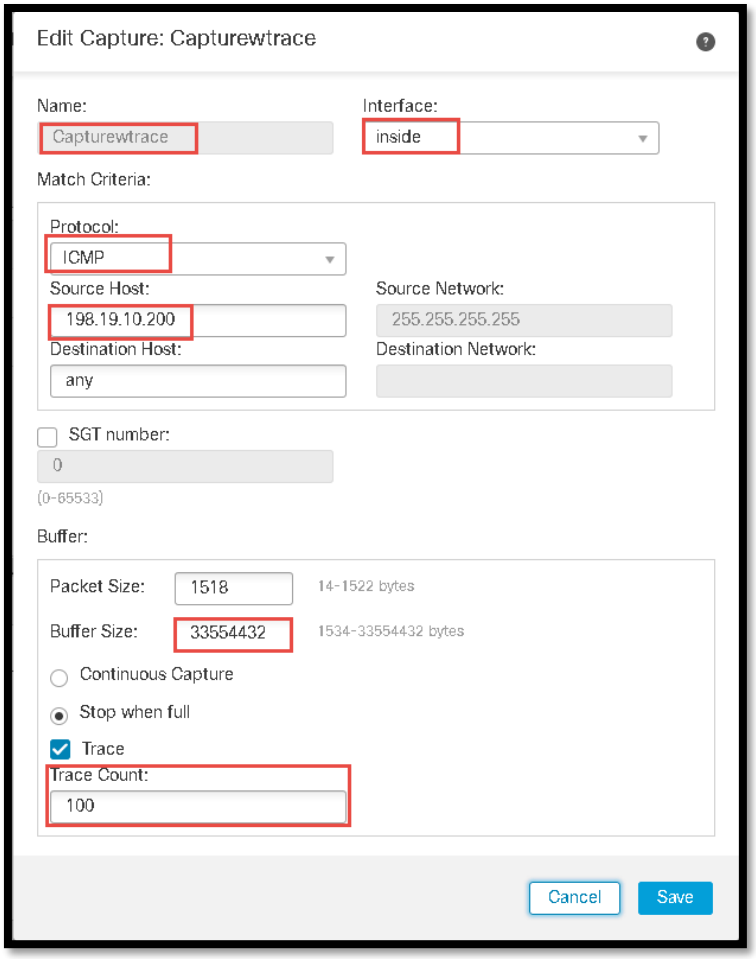
   a. What Rule is matched?

   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. Lina Level **capture**
2. SNORT Level **capture-traffic**



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

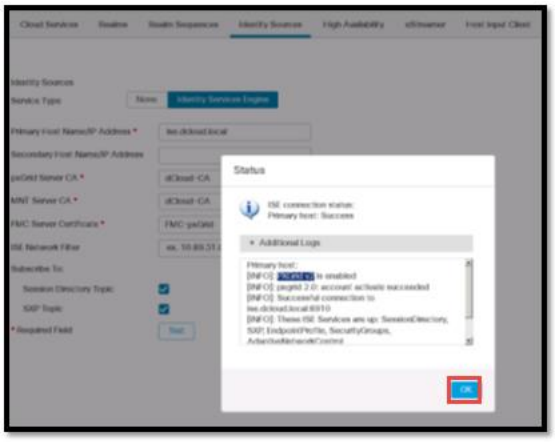
Cisco Secure Firewall Management Center uses PxGrid 1.0 protocol for integration with ISE. FMC obtains identeity information form ISE, such as User-IP mappings, User-SGT/IP-SGT mappings, SXP mappings and endpoint profiles using the communication protocol. Starting with release 6.7 the communication protocol for integrasion from PxGrid 1.0 to 2.0. PxGrid 2.0 offes 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

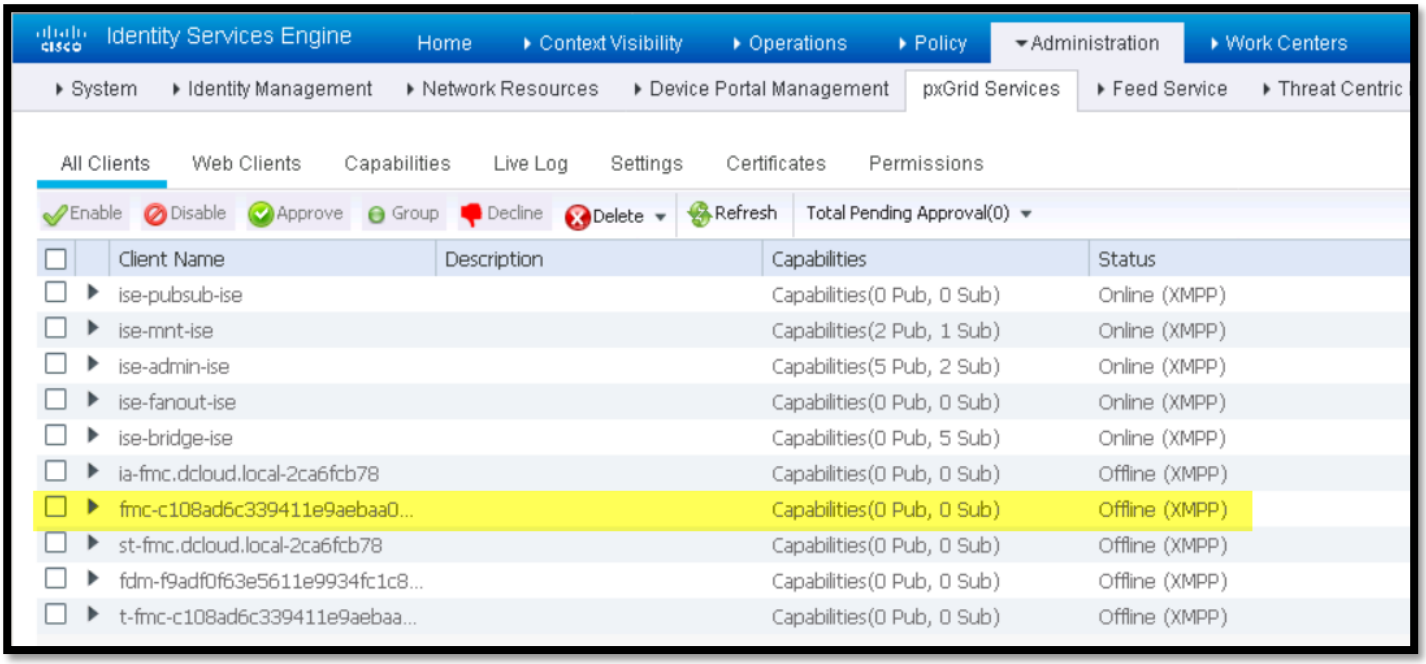
- Validate that PxGrid 1.0 protocol is updated to PxGrid 2.0
- Reconfigure EPS remediation to ANC
- Quarantine endpoint through FMC and ISE integration using ANC and PxGrid 20.

Integration of FMC and ISE using PxGrid 2.0 Protocol

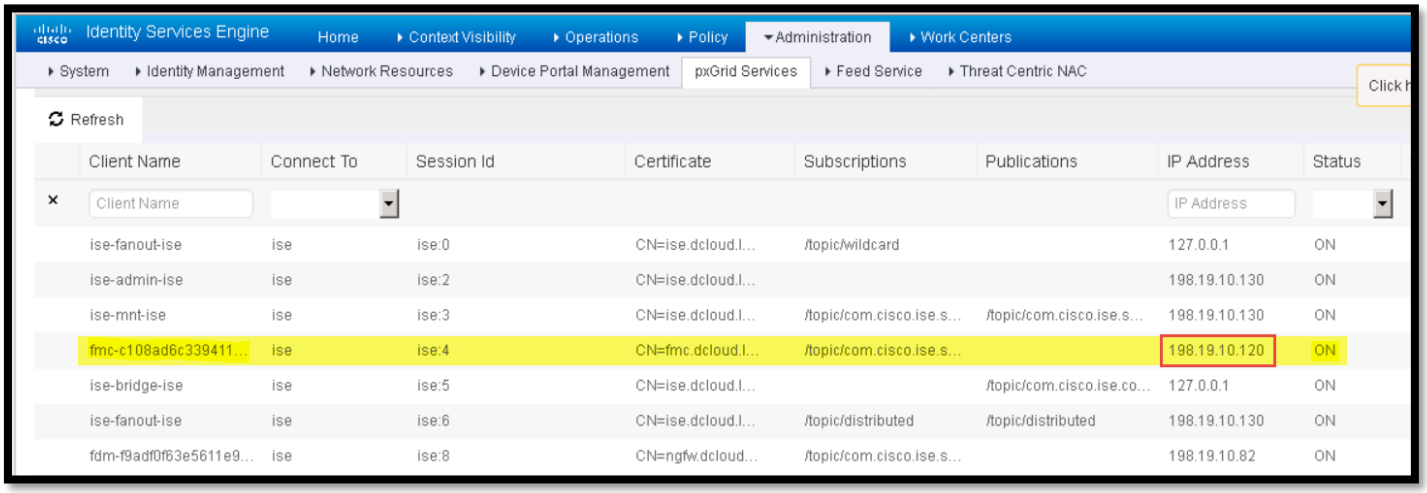
1. Login into FMC admin/C1sco12345
2. Go to System > Integration > Identity Sources > Identity Services Engine and select **Test** button to validate connectivity to the ISE System
3. Expand **Additional Logs** to see details of FMC and ISE connectivity and the Click **OK**



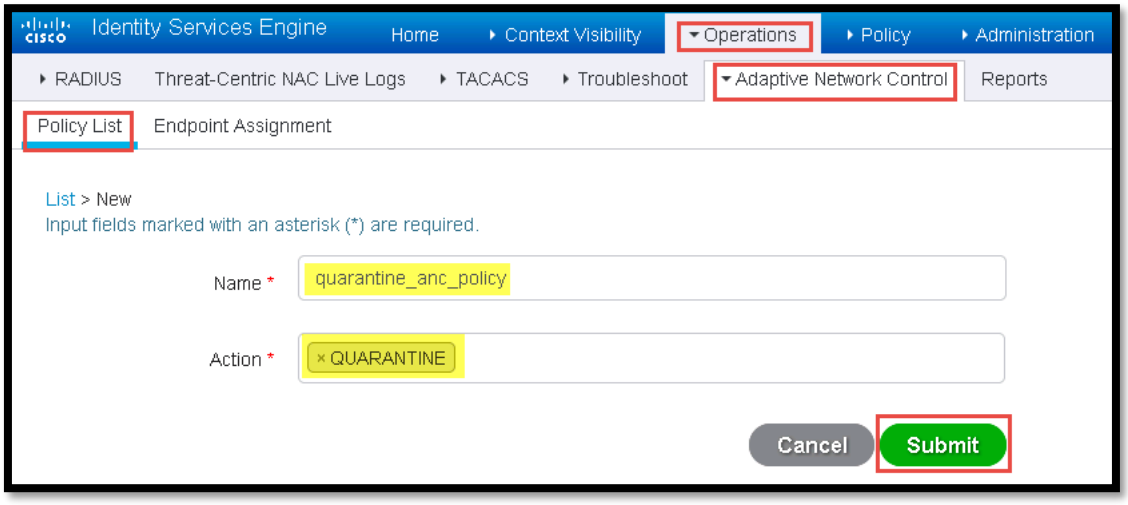
4. Open a new tab on the Firefox browser and click **ISE** bookmark from the ribbon **admin/C1sco12345**
5. Navigate to **Administration > PxGrid Services > All Clients** notice that the FMC Client is in Offline status.



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



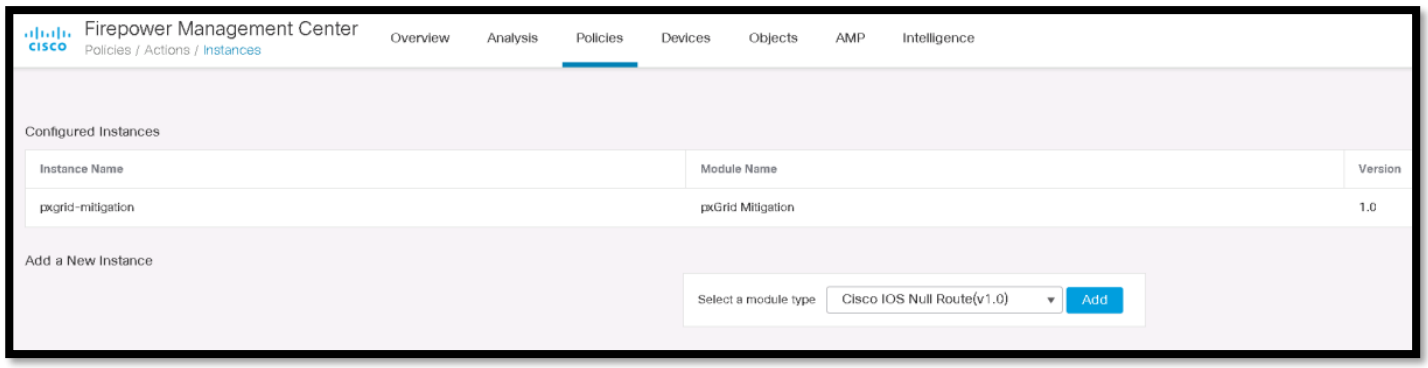
6. On ISE create an Adaptive Network Control (ANC) policy for assignment to an endpoint
    a. **Operations > Adaptive Network Control > Policy List**
    b. Click **Add**
    c. Name: **quarantine_anc_policy**
    d. Action: **QUARANTINE**
    e. Click **Submit**



Configure ANC instance and assign to Correlation Policy on FMC

1. FMC **Policies > Actions > Instances** review the existing configuration with an EPS instance configured

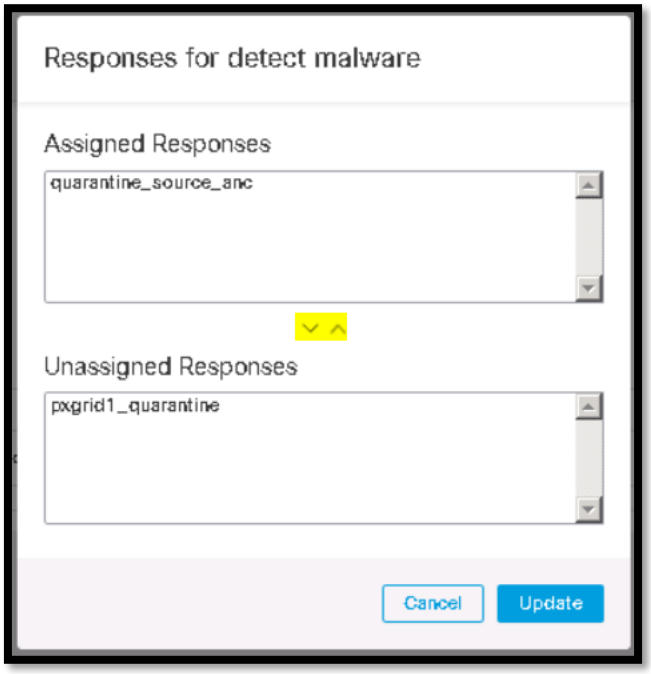
Note: The module name “pxgrid-mitigation” which is using PxGrid 1.0. We will add a PxGrid 2.0 module and then delete the “pxgrid-mitigation” module. You will not see this error right now because the Class image has the ISE Connector disabled in the Health policy. You will enable it in a later step.



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

3. FMC **Policies > Corrrelation > Policy Management**
4. Edit CorrelationPolicy – Malware Detection
    a. Policy Rules select the **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 >**
   a. **Edit the Initial_Health_Policy**
   b. On the left panel select **ISE Connection Status Monitor**
      i. Click Enabled: **On**
      ii. Click **Save Policy and Exit**

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

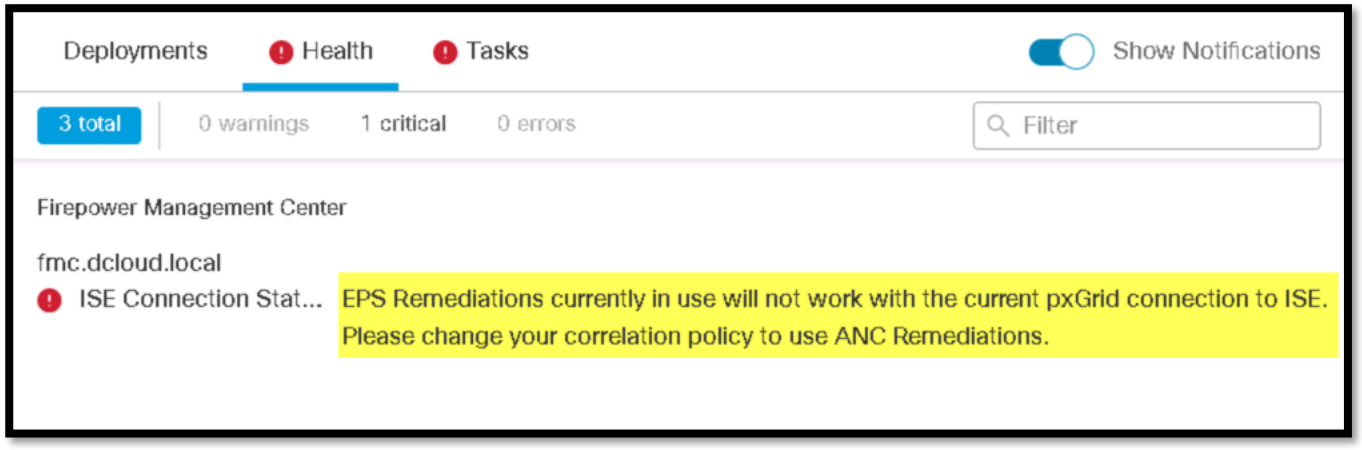
iii. Click on **Apply**

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

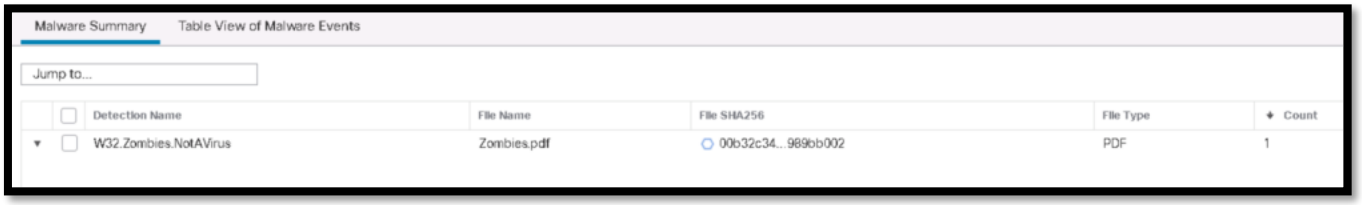
1. FMC click the **Notification Button** to see the health warning about an EPS configuration that need to be replaced by ANC



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

Test the Configuration

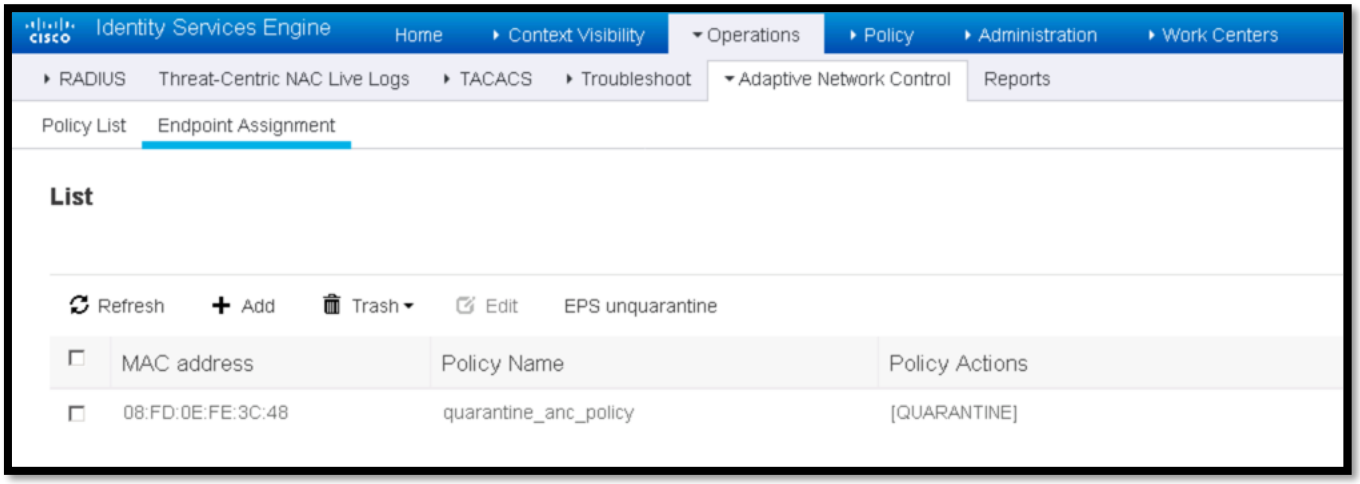
1. On the Jump PC go to **Desktop > RADIUS Simulator and run the following two scripts:**
    a. RadiusListener
    b. StartSessions
2. Jumphost open the **Remote Desktops** folder and launch **Wkst1 (IP address: 198.19.12.21 admin/C1sco12345)**
    a. From Wkst1 Desktop open User folder and choose **NGFW1 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**



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

    d. FMC **Analysis > Correlation > Status**

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



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.

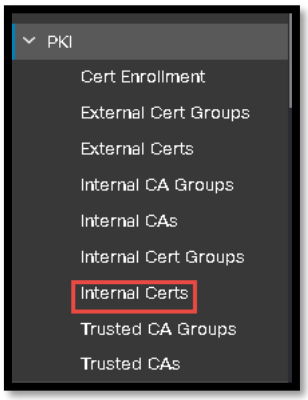
Steps

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**

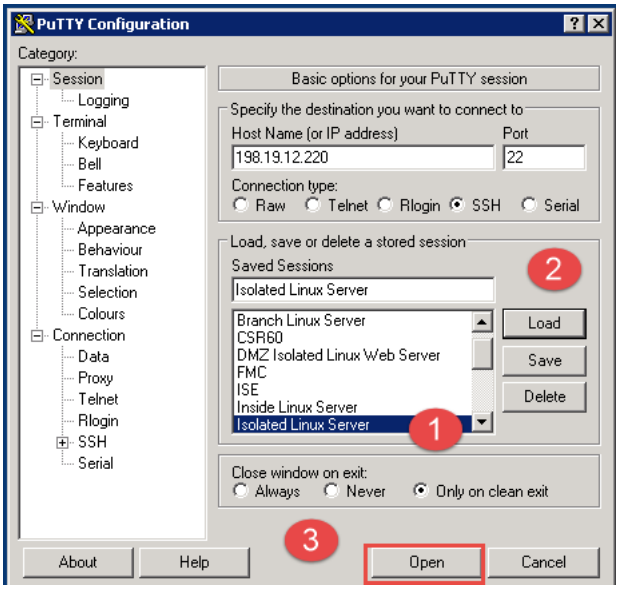
3. Go to **Object** menu and select **Object Management**
4. Expand **PKI** and Select **Internal Certs** under the PKI object on the left



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

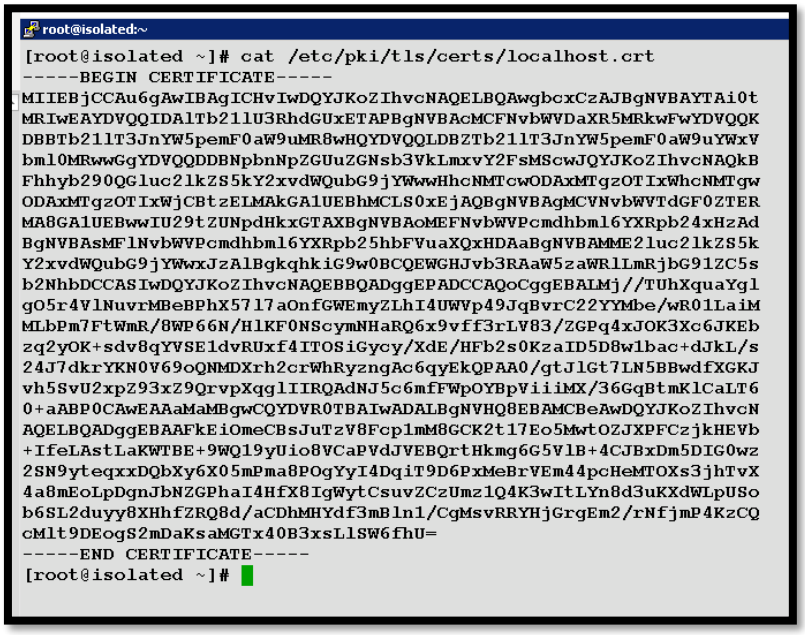
6. The Add Known Internal Certificate window appears prompting for the certificate and private key data

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**

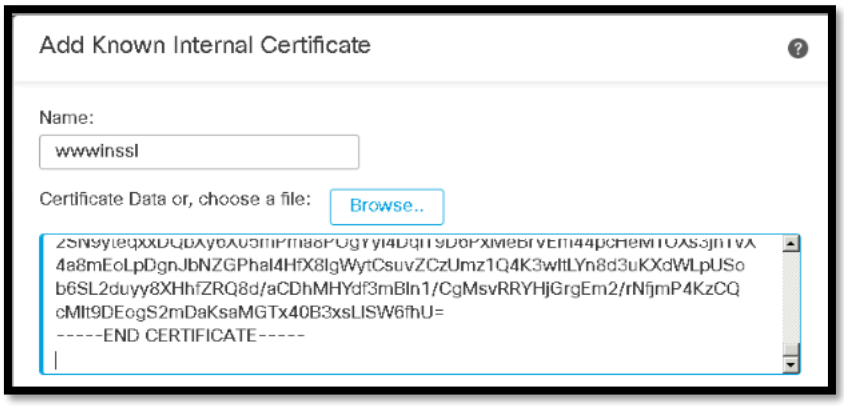


10. Login **root/C1sco12345**
11. Run the following command to display the contents of the certificate used by the DMZ webserver
    a. cat /etc/pki/tls/certs/localhost.crt

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



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



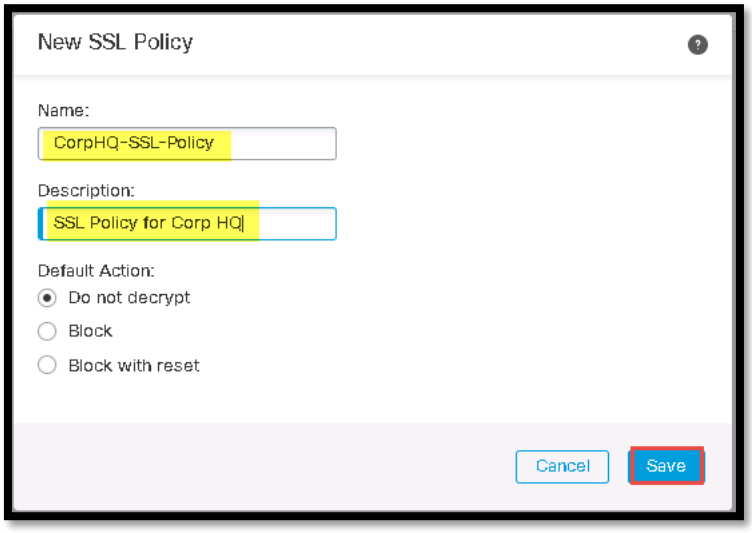
15. Go back to the Putty session
16. Run the following command
    a. cat /etc/pki/tls/private/localhost.key

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

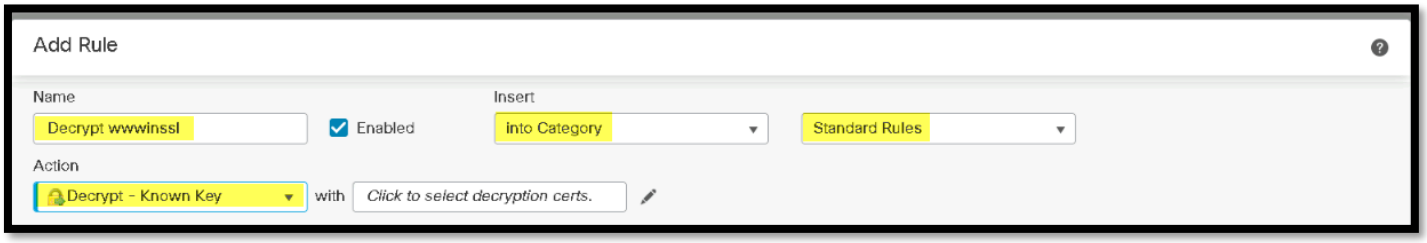
1. Click the **Policies** menu and select **SSL**
2. Select N**ew Policy**
3. Configure the following:
    a. Name **Corp HQ-SSL-Policy**
    b. Description: **SSL Policy for Corp HQ**
    c. Default Action: **Do not decrypt**
    d. Click **Save**



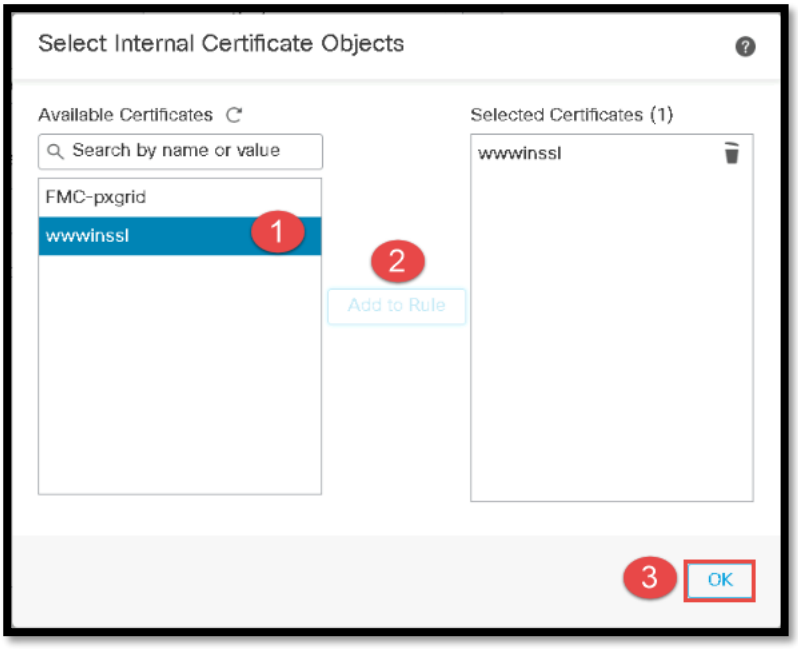
NOTE: The Default Action is what the SSL policy will do if no rules match

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

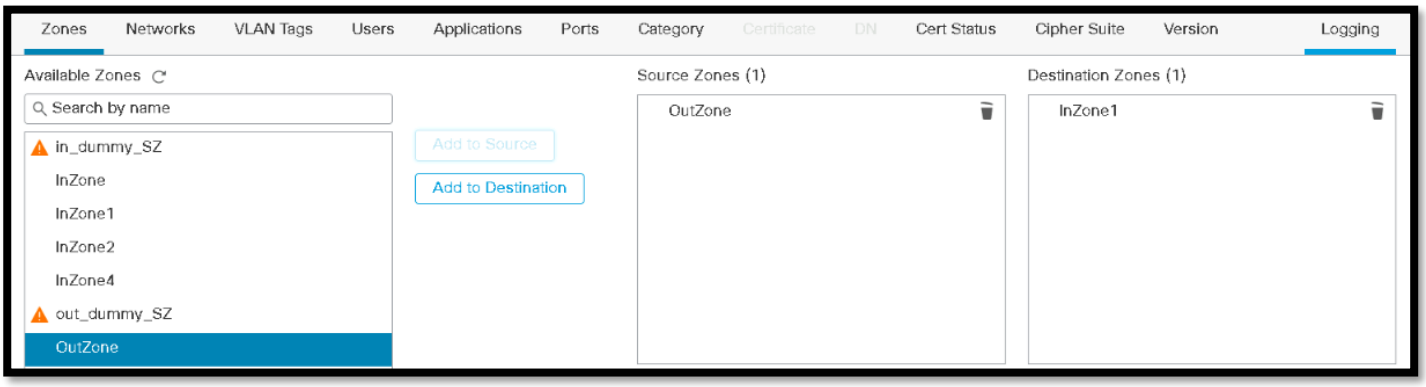
5. Configure the following:
   a. Name: **Decrypt wwwinssl**
   b. Action: **Decrypt – Known Key**
   c. Insert: **into Category: Standard Rules**



6. Next to the Action field, click in the field labeled **Click to select decryptions 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**

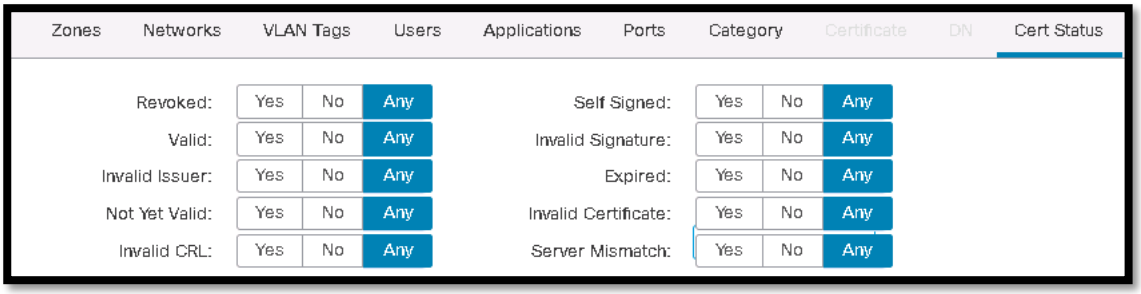


8. On the Zones tab select **InZone1**ne and click **Add to Destination.** Select **OutZone** objects and click **Add to Source**



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



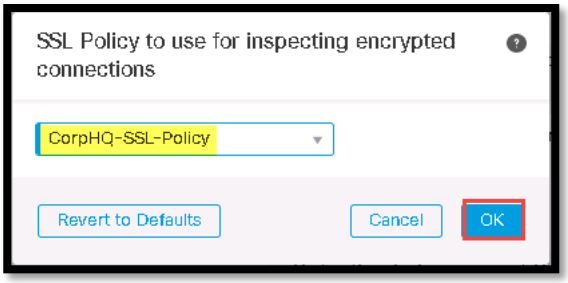
12. Click **Logging** tab and select **Log at End of Connection**
13. Click **Add**
14. Click the **Save** button to save changes to the policy

Configure ACP

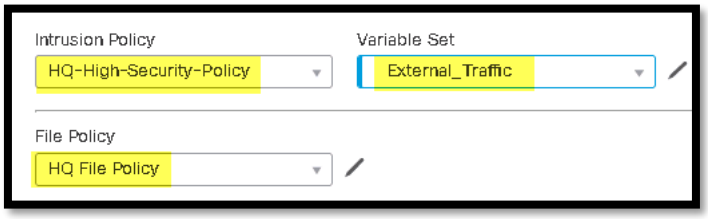
The SSL Policy has been configured but has yet to be attached to an ACP.

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

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



4. Click **Rules**
5. Locate the rule that you used for the Inbound SSL Connectivity and edit the rule
6. Configure the Following:
    a. Intrusion Policy: **HQ-High-Security-Policy**
    b. Variable Set: **ExternalTraffic**
    c. File Policy: **HQ File Policy**
    d. Click **Save**

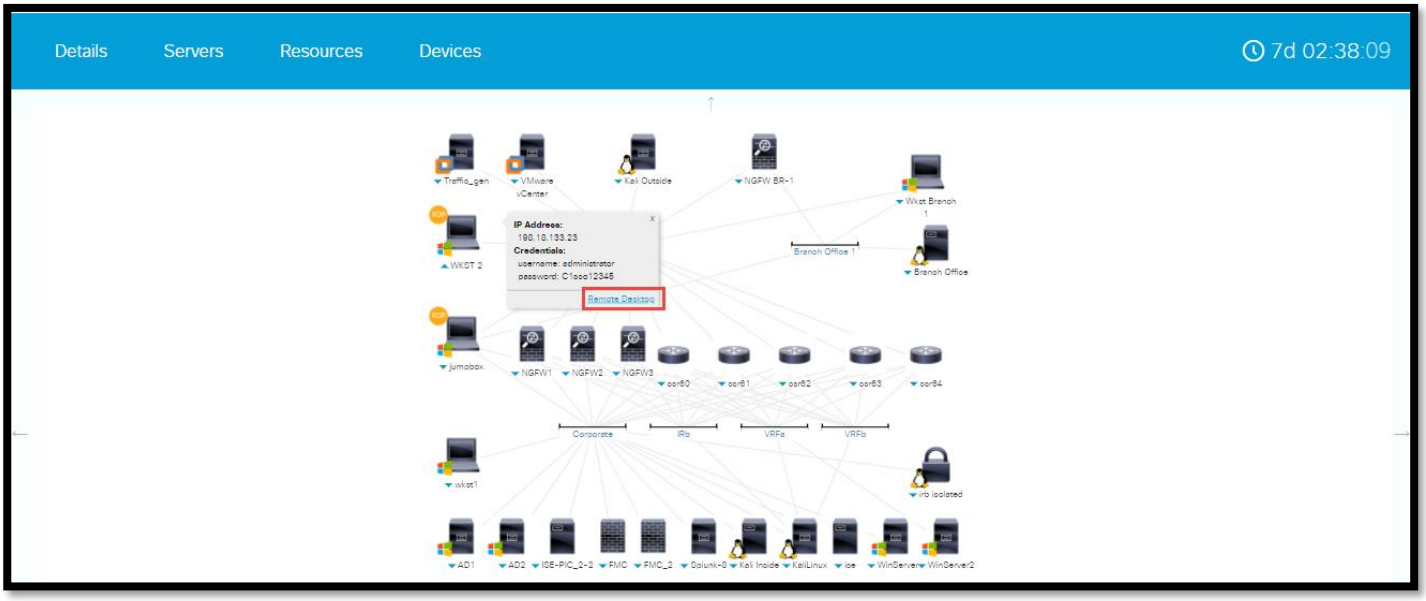


7. Click **Save** for the **Base_Policy** and **Deploy**

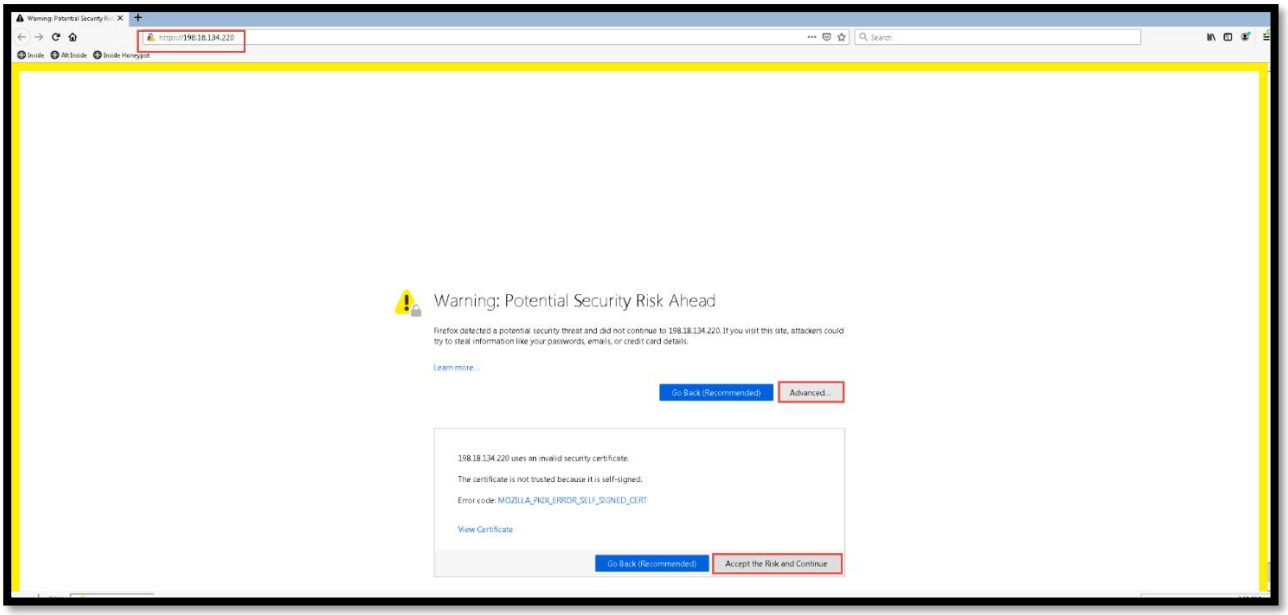
Test SSL Policy

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

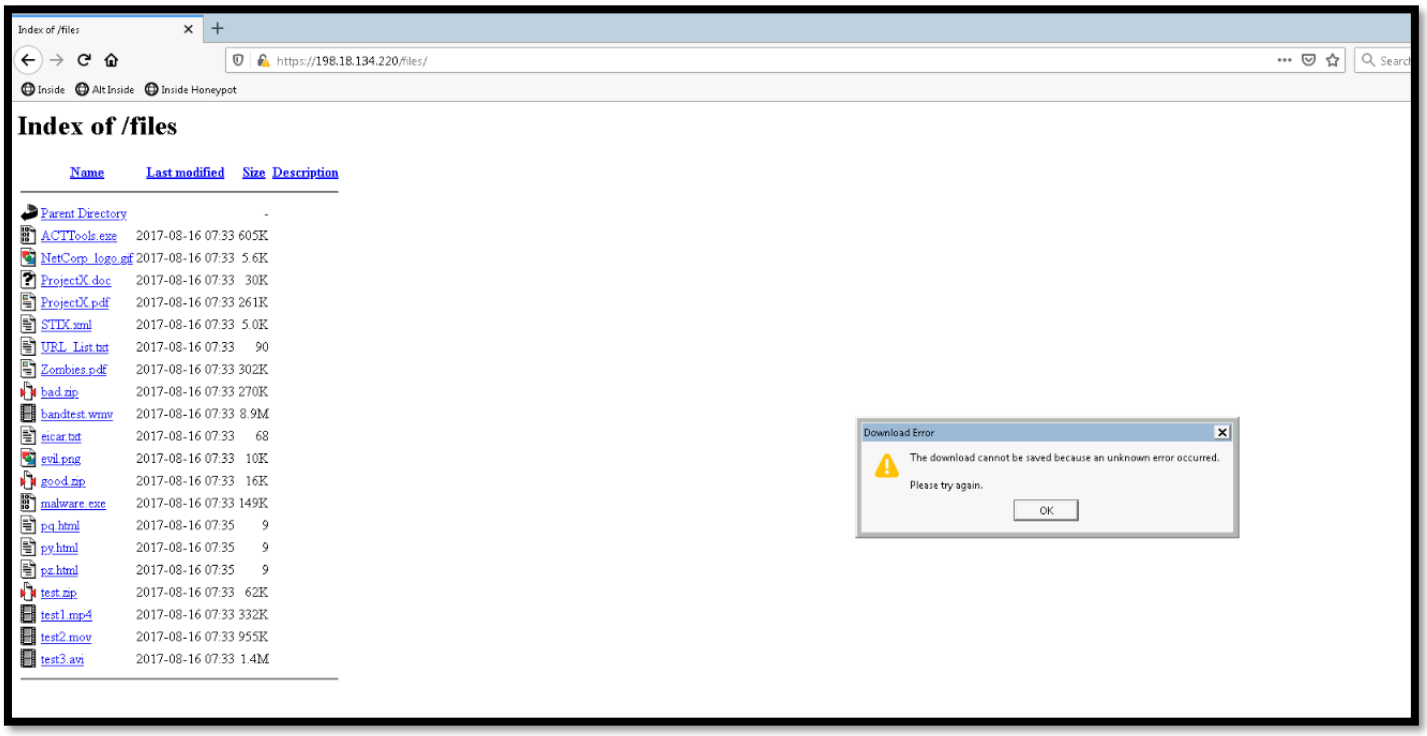
1. Go to the dCloud session page in the computer's web browser, and find the **WKST2** machine arrow and then select **Remote Desktop**



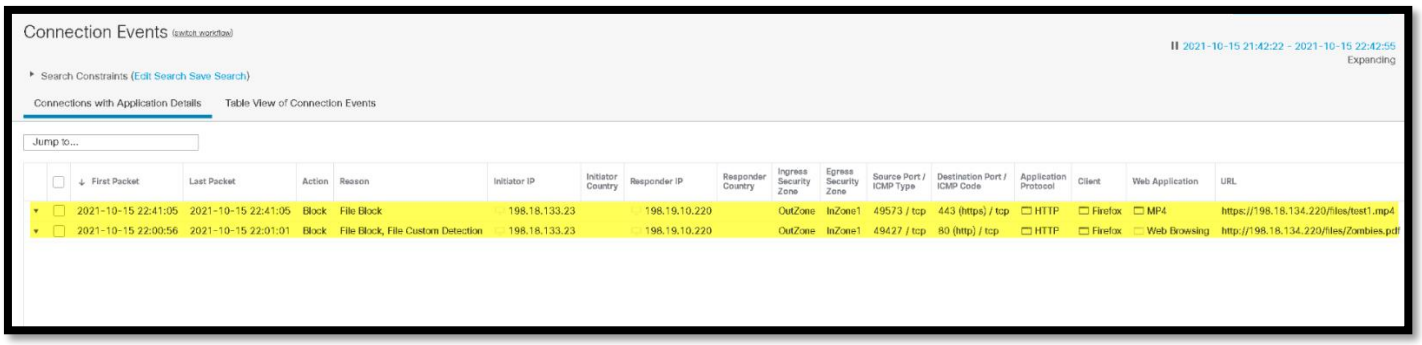
2. Open the **Firefox** web browser by double-clicking on the shortcut on the desktop
3. Click on the **HTTPS://198.18.134.220**
4. Click on **Advanced**
5. Click on Accept the Risk and Continue



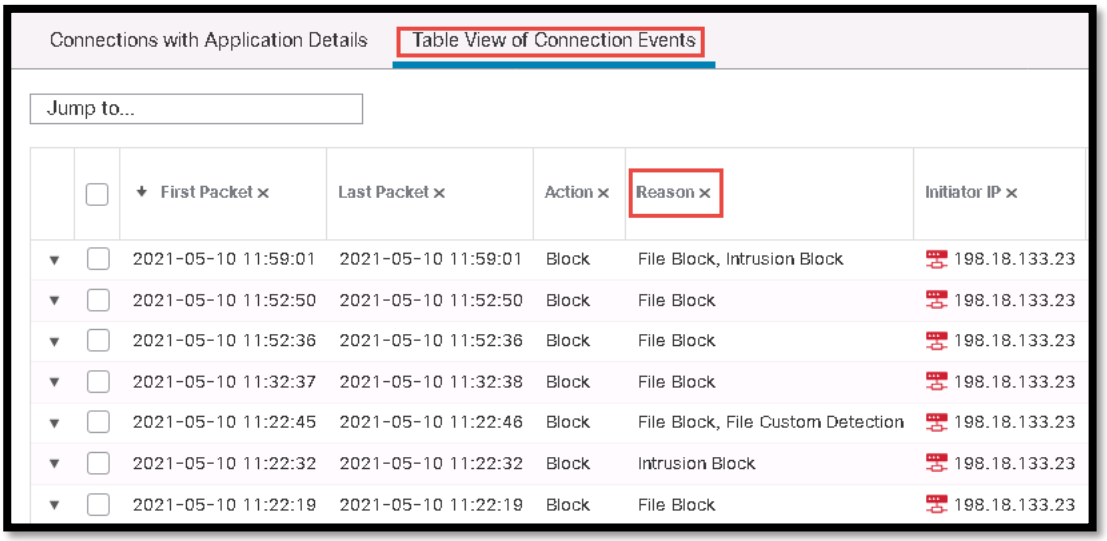
6. Click on the **Files** link
7. You will now test the SSL Policy
8. Right click on the test2.mov and select **Save Link As**
9. Select Desktop and **Save**
    a. The file should be downloaded
10. Right Click on test1.mp4 and select **Save Link As**
    a. Download will fail



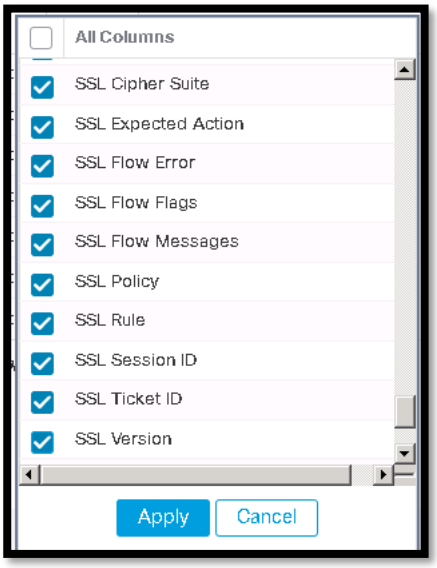
11. The file is not being allowed to transfer even though it is a HTTPS connection. You will now review the log files that show the information for the SSL policy
12. Return to the FMC
13. Go to **Analysis > Connection > Events**
14. Click **Edit Search**
    a. Action: Block
    b. Networking
     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



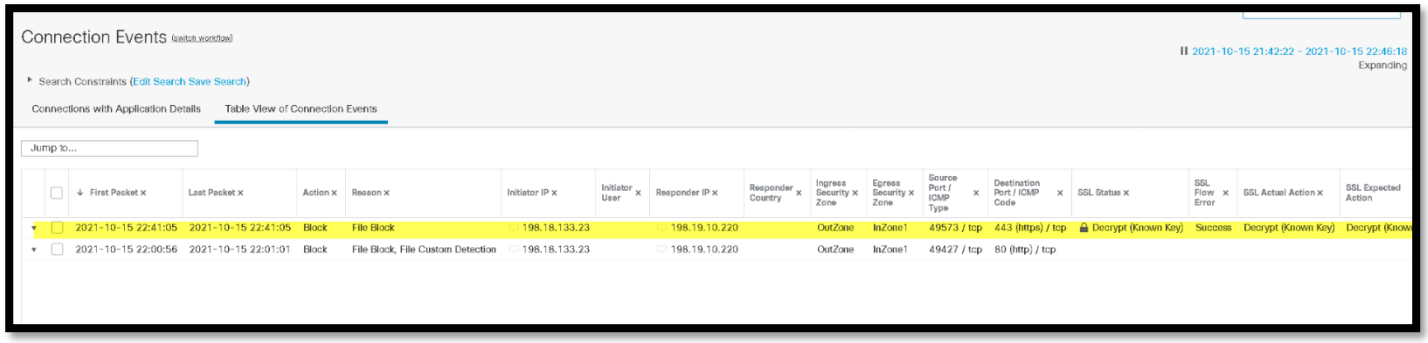
15. You can see the files that were blocked. Note that the URL reveals HTTPS
16. Click **Table view of Connection Events**
17. Click the **X** next to one of the columns in the current view



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



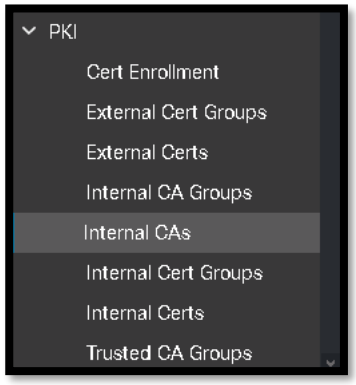
19. Click **Apply**
20. Review all the **SSL** fields available in relation to the traffic shown on the screen



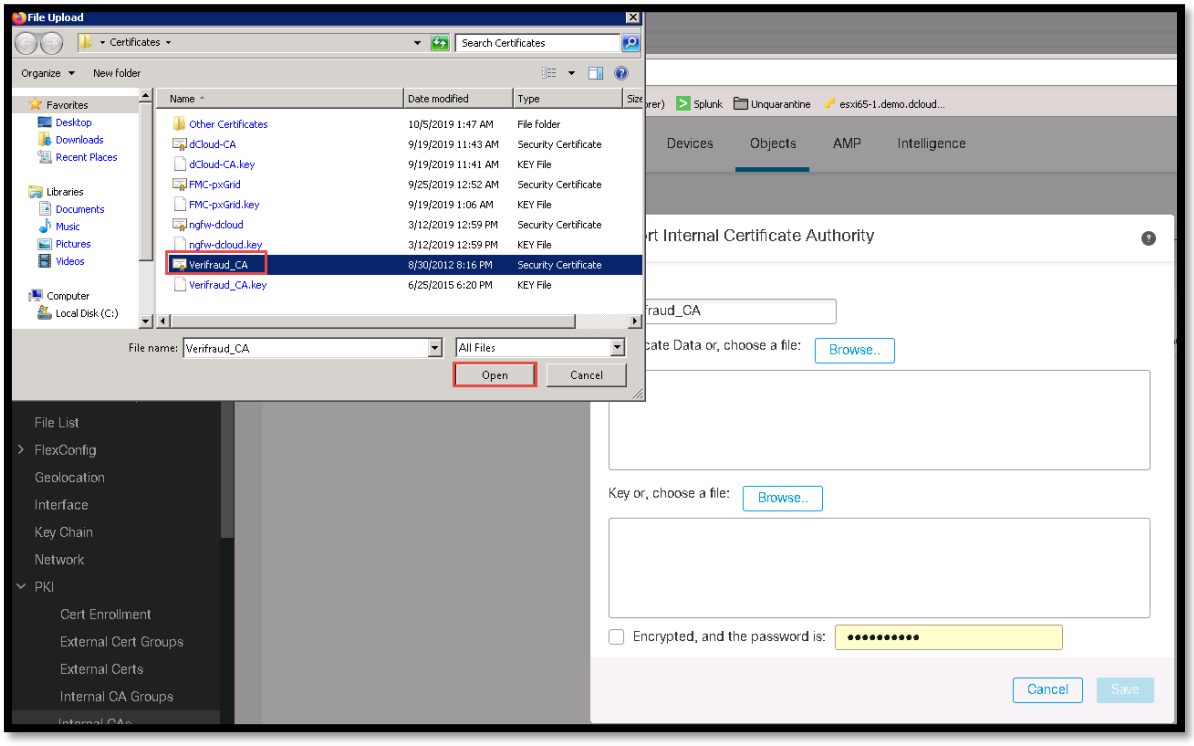
SSL Decryption – Resign

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**



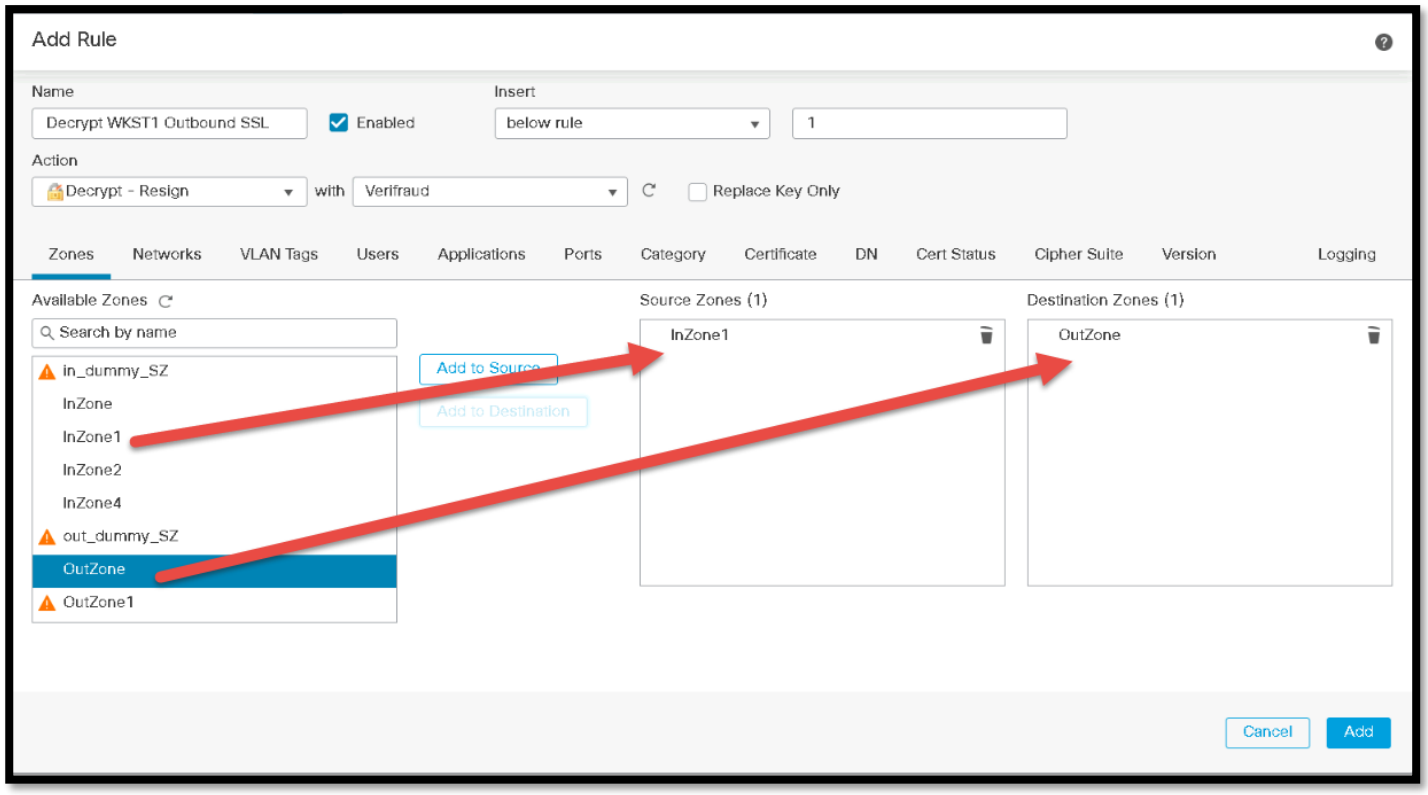
b. In the **Key** section click **Browse**
c. In the **Certificates** folder on the **Desktop** select **Verifraud_CA.key** and **Open**

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

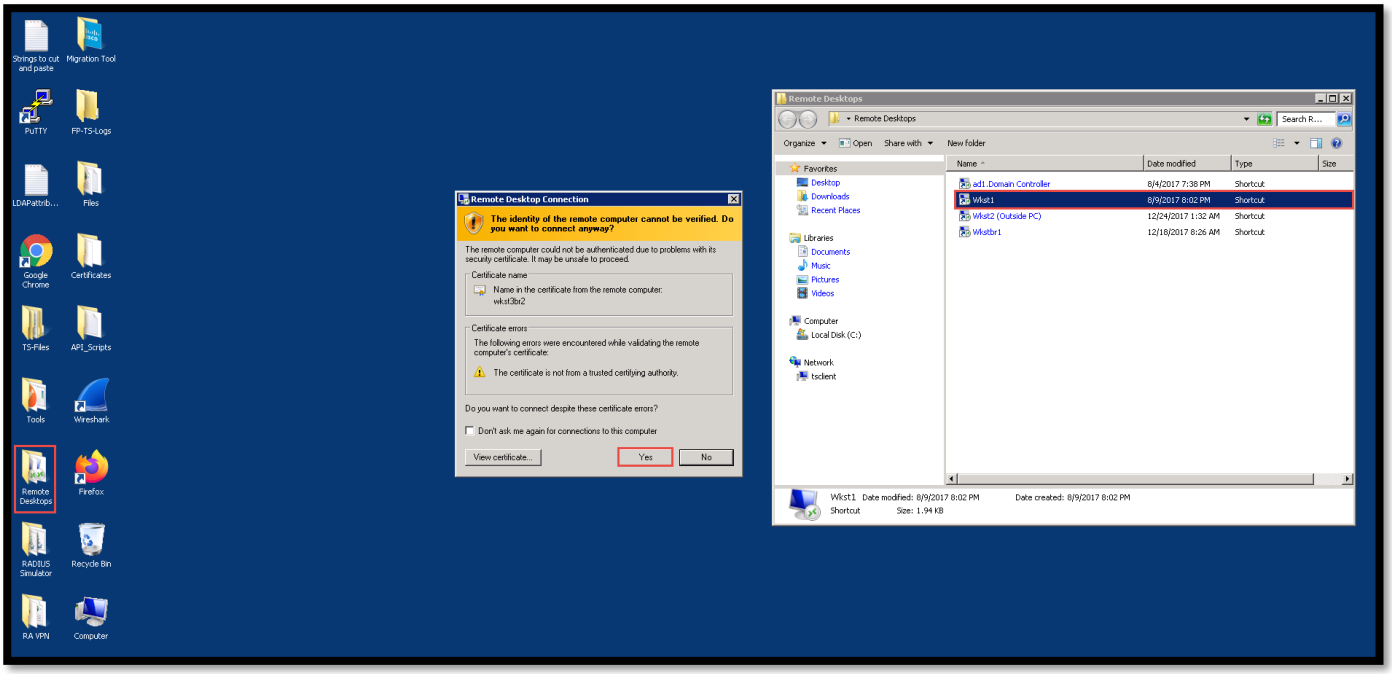
12. In the Zones tab add **InZone1** to the **Source Zones** and add **OutZone** to the **Destination Zones**



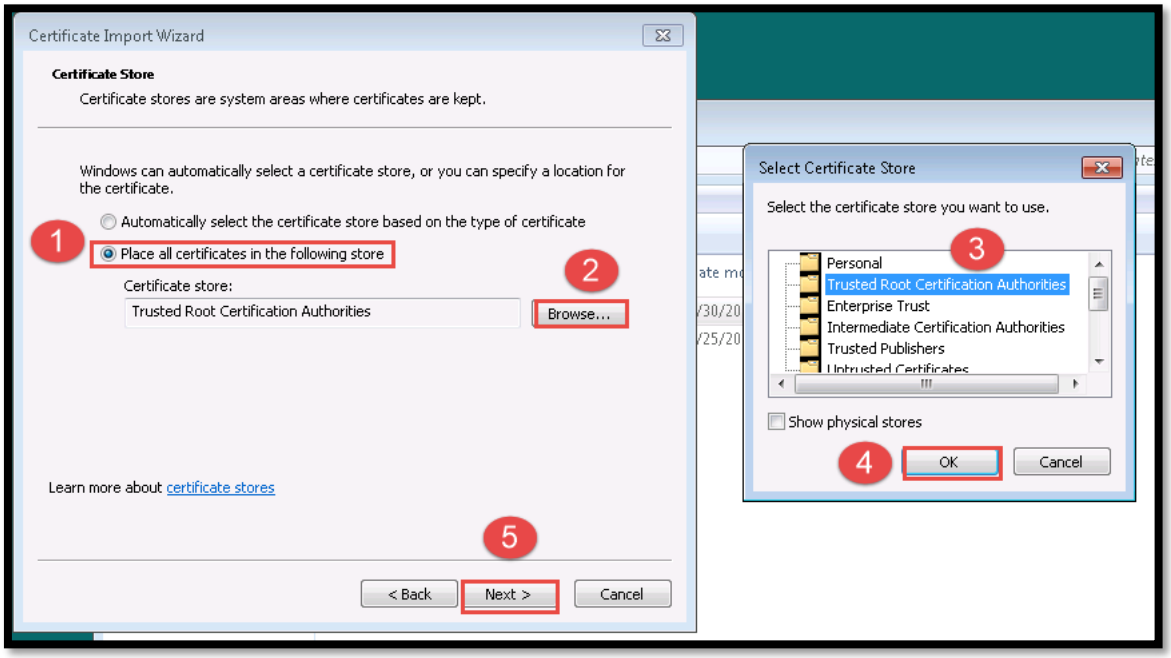
13. In the **Networks** tab select Corporate_LAN and add to **Source**

14. Click the **Ports** tab and select **HTTPS** and click **Add to Destination**

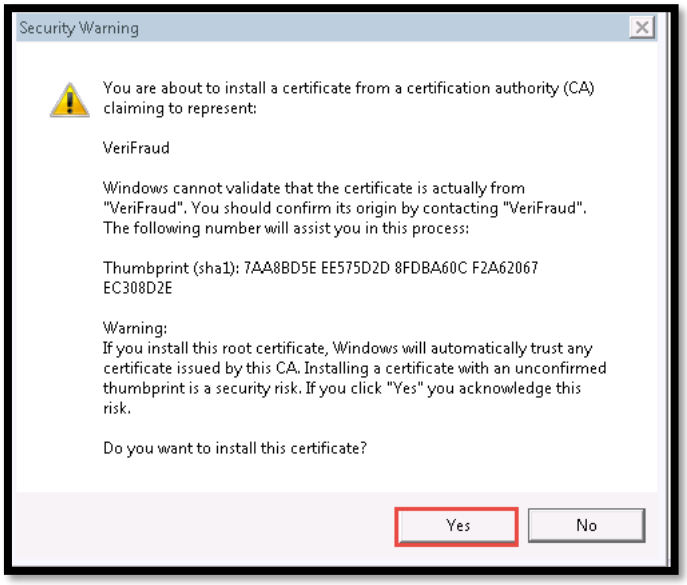
15. Click the **Logging** tab and select **Log at End of Connection**
16. Click **Add** and **Save** and **Deploy** the changes
17. On the **Desktop of the Jumpbox click on Remote Desktops and open Wkst1 select Yes for the Connection**



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**

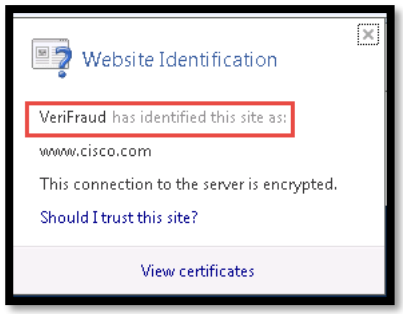


e. You should get confirmation that the import was successful

Testing the SSL Policy

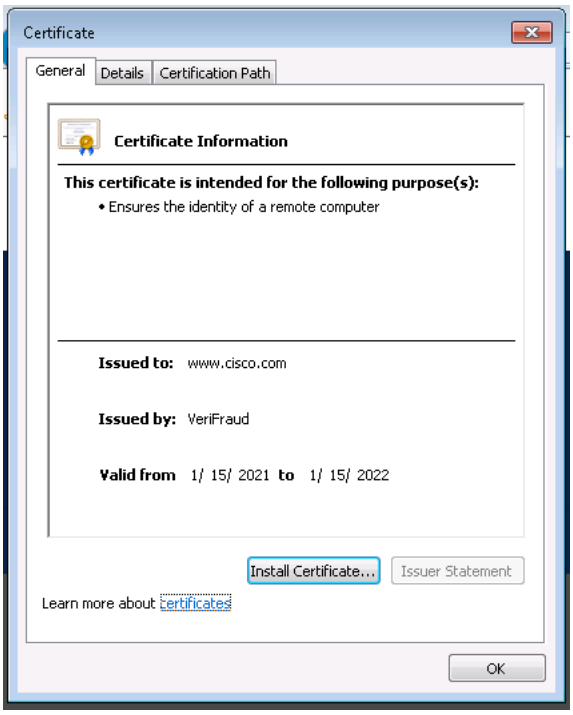
1. **Policies > Access Control > Base_Policy**
    i. Review or Modify the **Allow Outbound Rule** to include the following:
        1. Source Zone: **InZone1 [add to InZone]**
        2. Ports: add to Destination
            a. DNS_over_TCP
            b. DNS_over_UDP
            c. ICMP (all)
    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

6. Look at the Website Identification

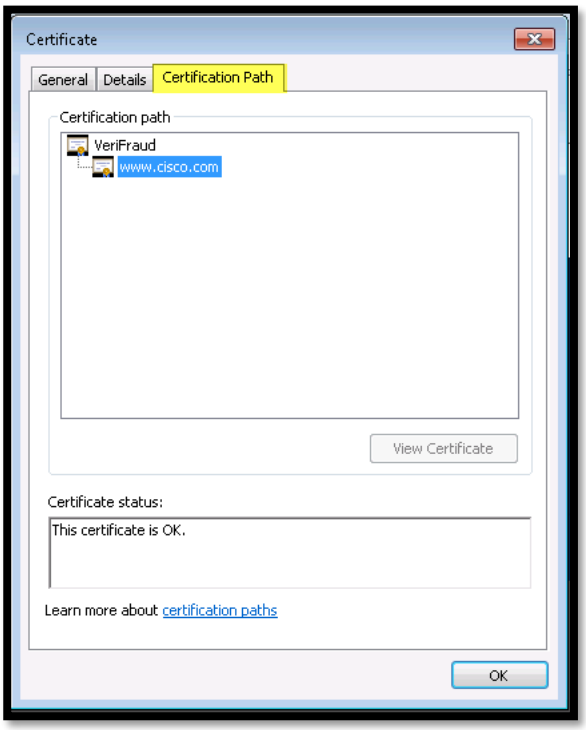


7. Notice that **VeriFraud** has Identified the site as www.cisco.com

8. Select **View certificates**

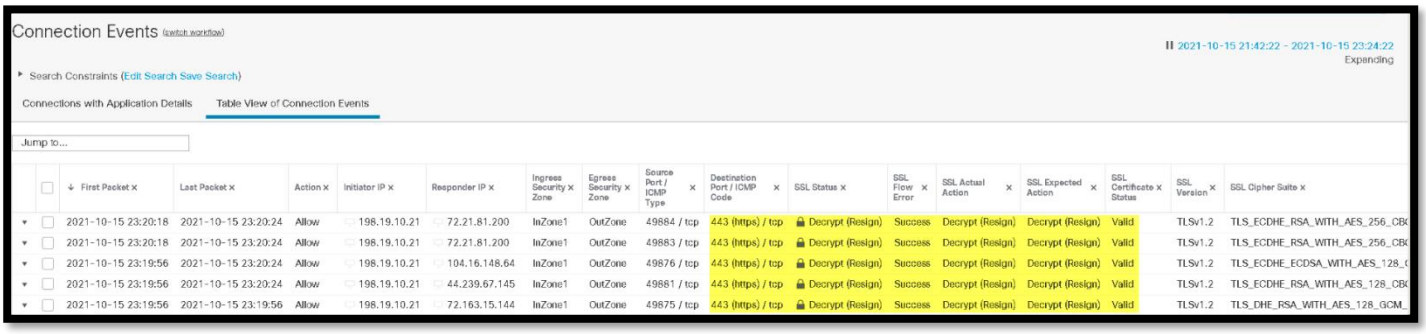


9. Click on **Certification Path**



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



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)

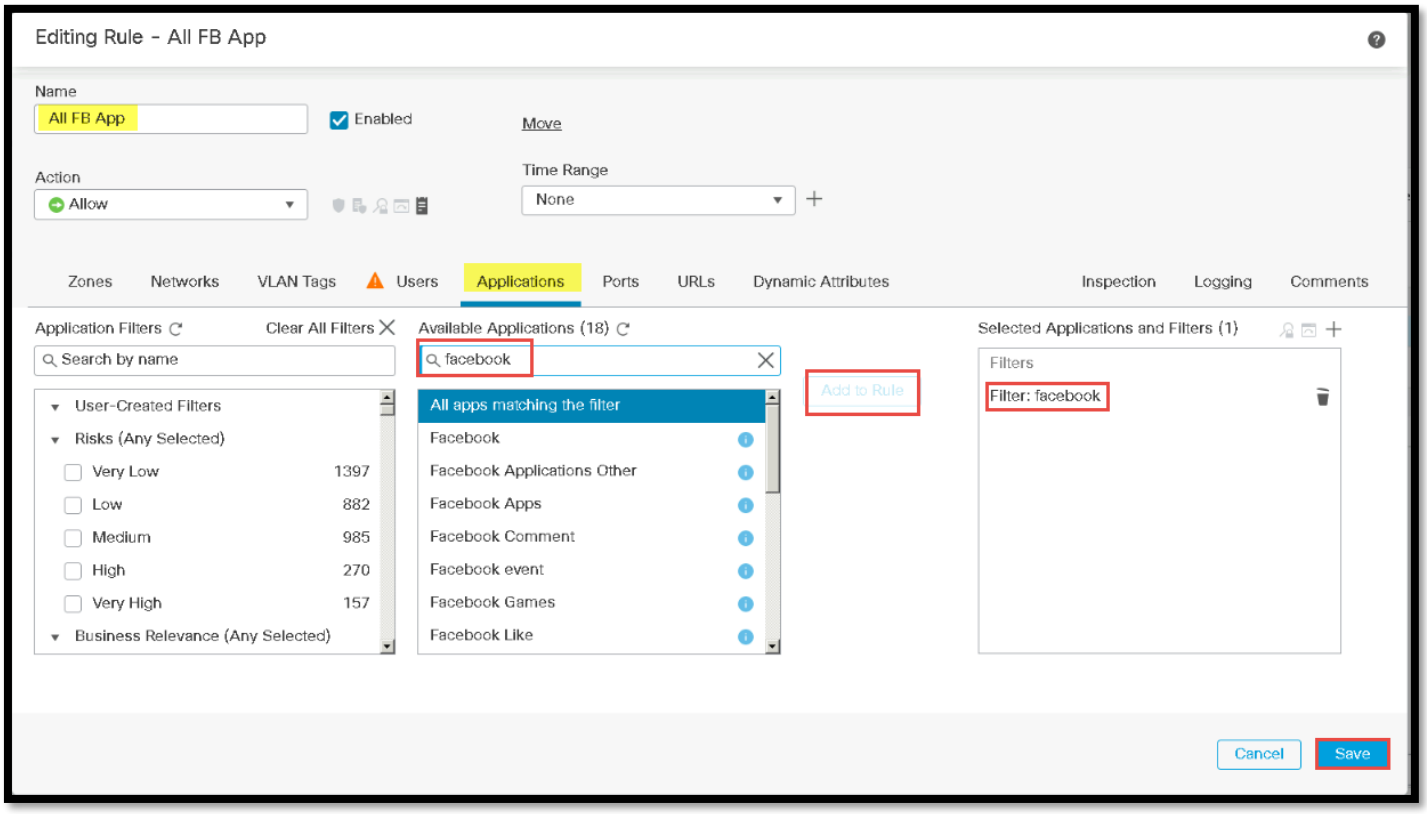
Most of the useful information needed to enforce firewall rules effectively is encrypted, and information such as SNI that is in cleartext can be spoofed. The following will demonstrate how an intruder can use the SNI to bypass firewall policy and what configuration you can apply to validate the SNI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

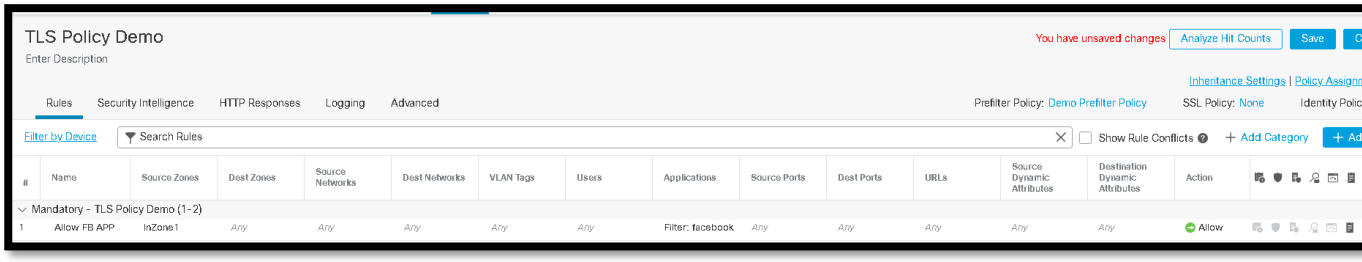
3. FMC Policies > Access Control > New Policy > Name TLS Policy Demo and Add HA_Test or NGFW1
        i. Click on **Add Rule**
            1. Name Allow FB APP

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

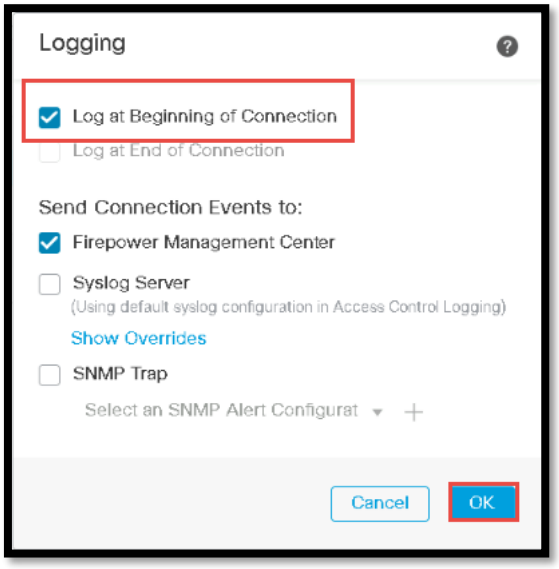


5. Click **Add**

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

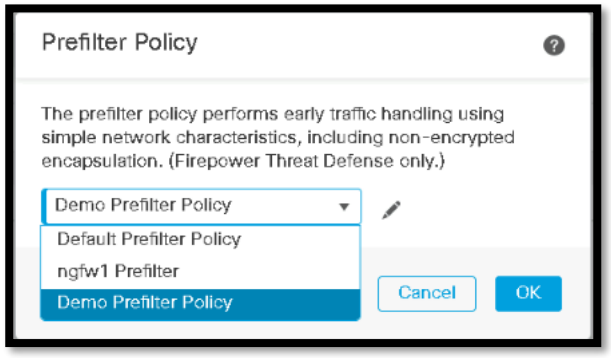


   b. Click on Log at Beginning of Connection



c. Click **OK**

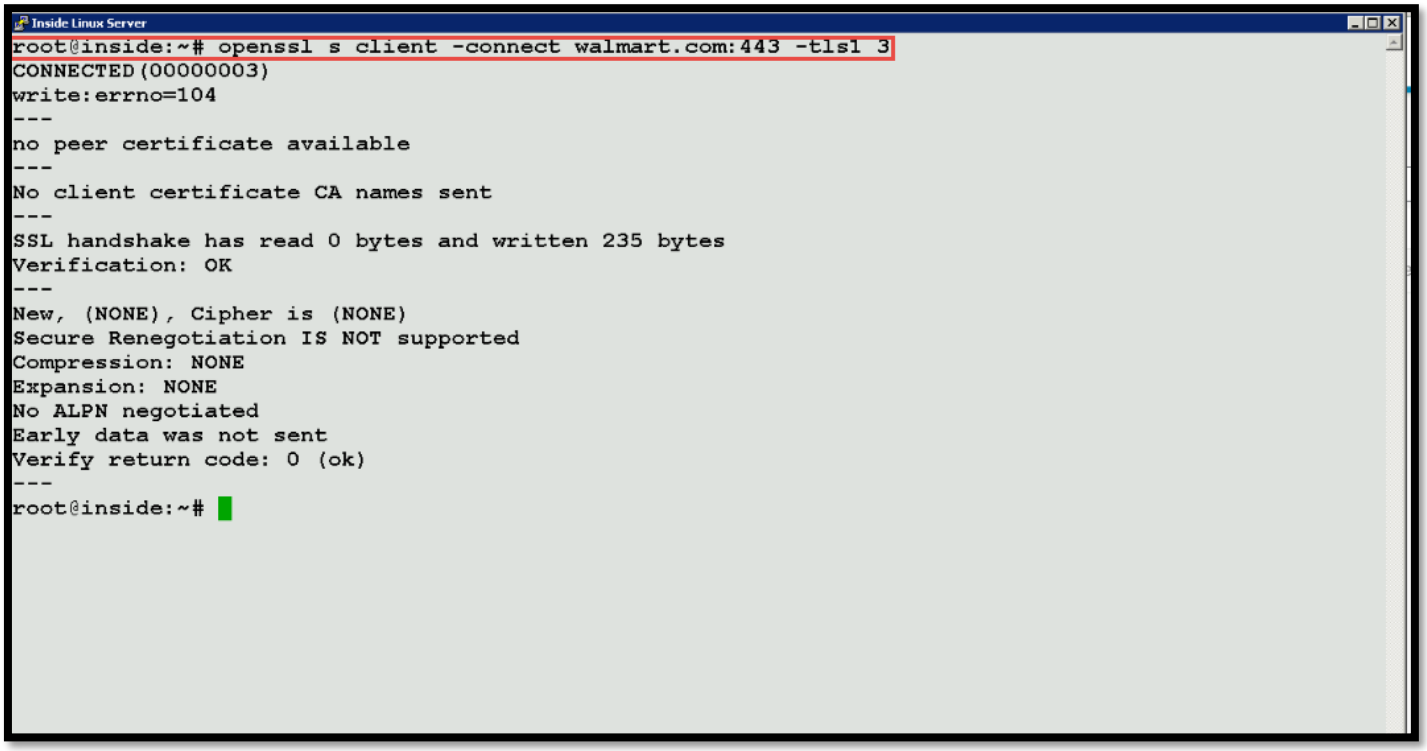
5. Click on the **Default Prefilter Policy** from drop-down menu



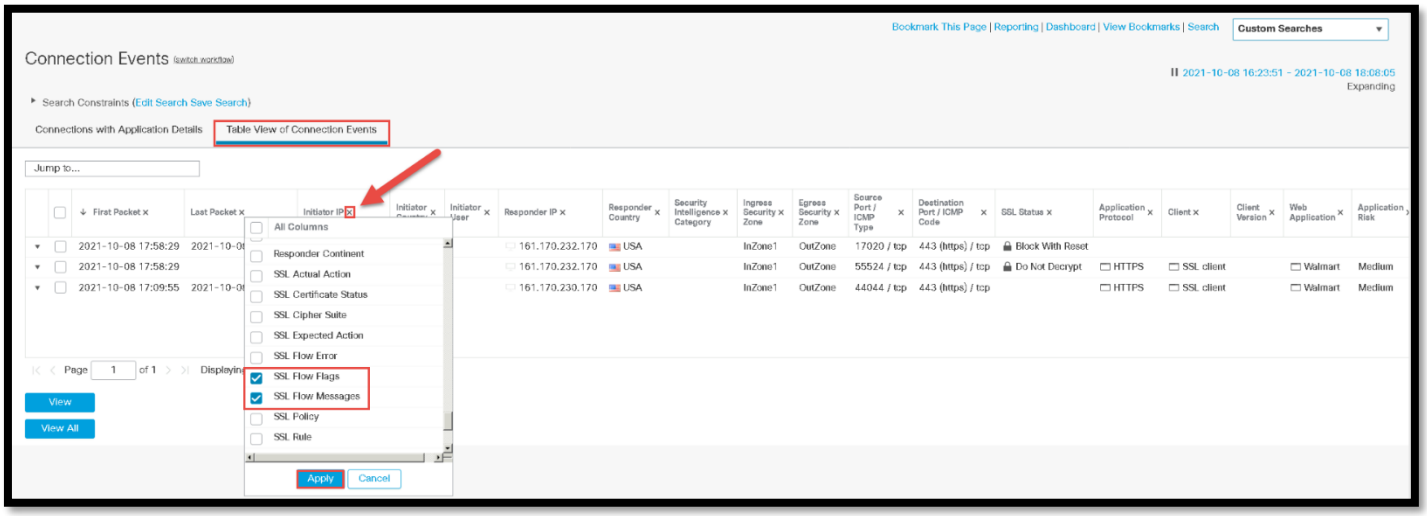
6. Click **Save** at the top of the page
7. Click **Deploy**

TLS Server Identity Discovery Disabled and SNI not present

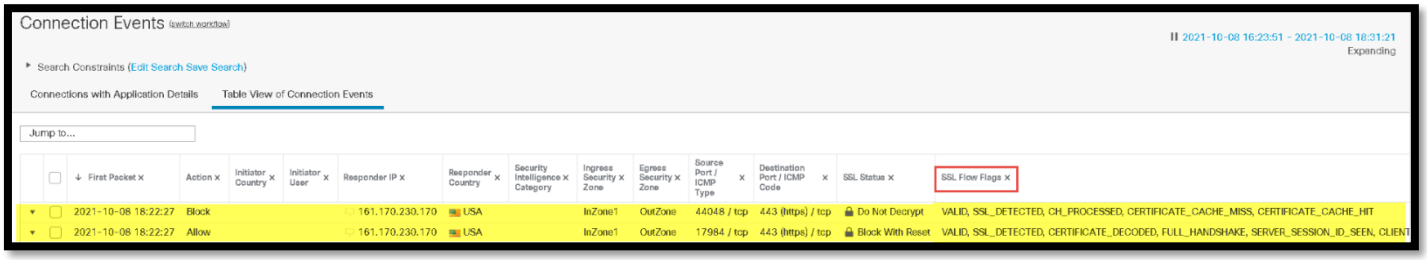
1. On the Jumpbox open the **Inside Linux Server** root/C1sco12345
2. On the Linux Server type the following:
    a. Openssl s_client -connect Walmart.com:443 -tls1_3
        i. This will generate traffic to https://wlamart.com using TLS1.3 this command will take a few seconds to complete

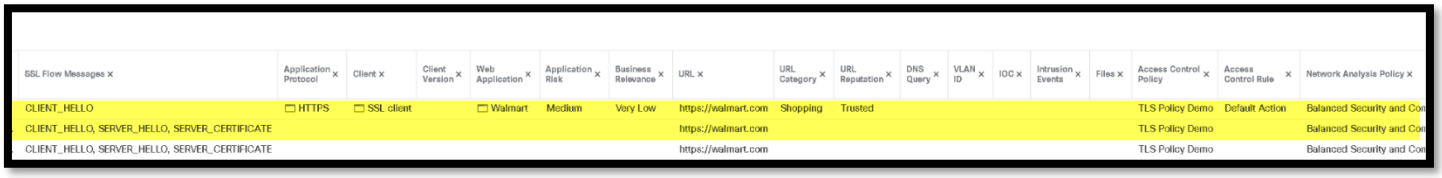


3. Click on **Analysis > Connection > Events**
    a. Edit Search
    b. Networking
        i. Initiator IP*: 198.19.10.200
        ii. Search
    c. Click on Table view of Connection Events
4. Click on the **x** by one of the Columns
    a. Select SSL Flow Flags
    b. Select SSL Flow Messages



    c. Click **Apply**

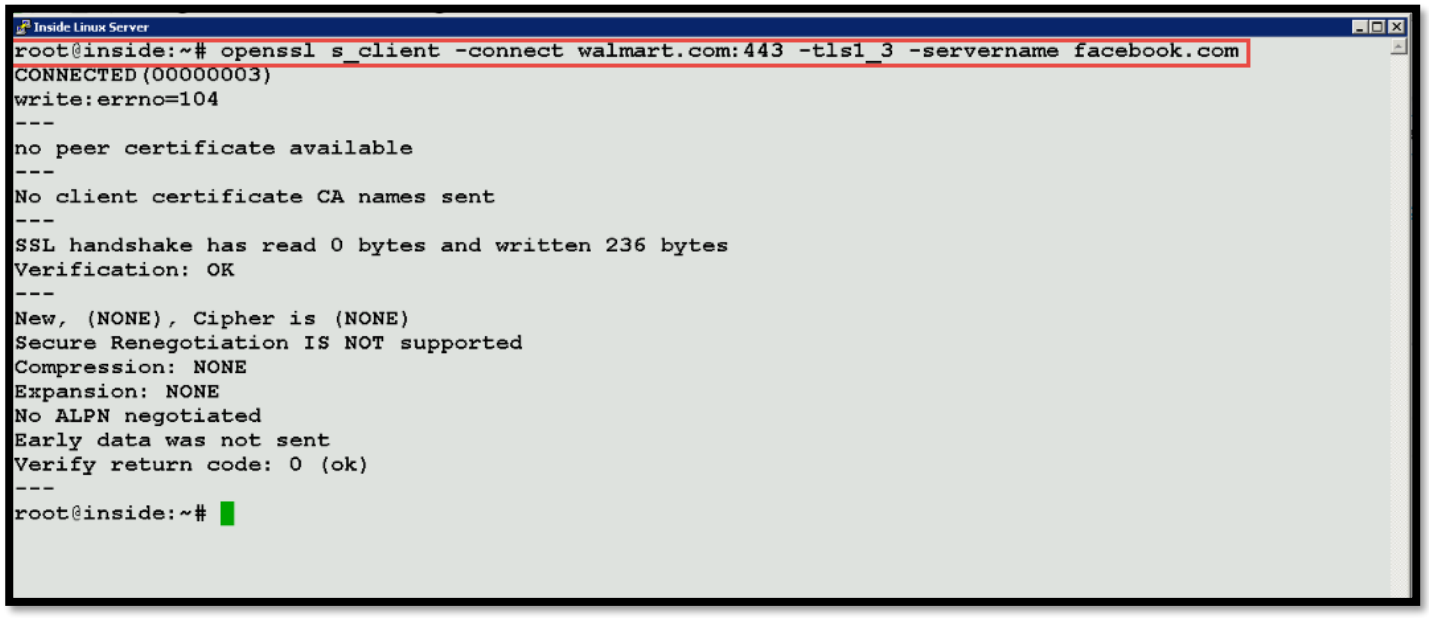




TLS Server Identity Discovery Disabled and with SNI Present

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 webside/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.



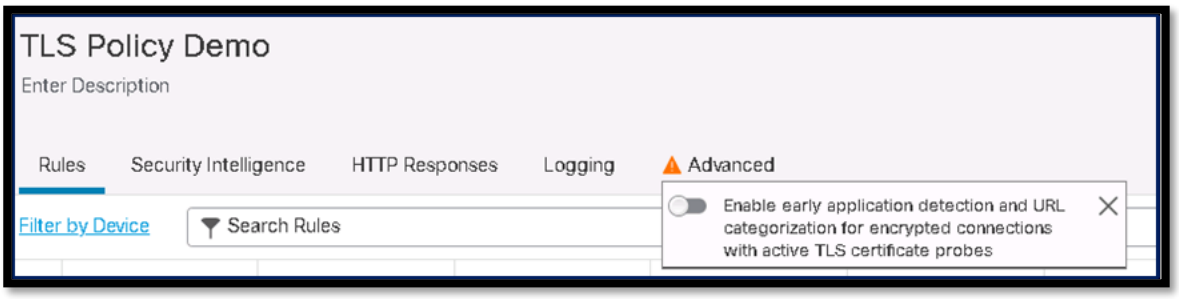
This will set the SNI of the connection to facebook.com. When SNI is used, the hostname of the server is included in the TLS handshake. SNI provides a solution for a shared IP address that hosts multiple web server/domains that allows unique certificates to be used for each domain. In TLS 1.3 flows,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

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.

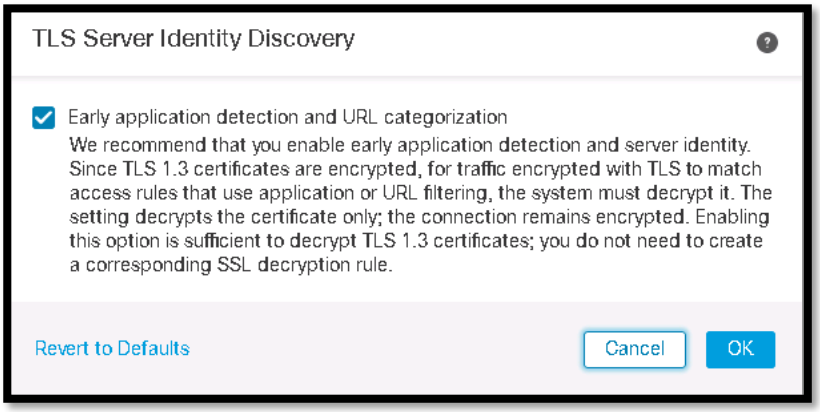
The next exercise will look at how Cisco Secure Firewall threat Defense using the **TLS Server Identity Discovery** feature makes a decision against TLS 1.3 flows based on other information, since SNI can be easily spoofed. When procession TLS 1.3 traffic flows, the FTD with TLS Server Identity Discovery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



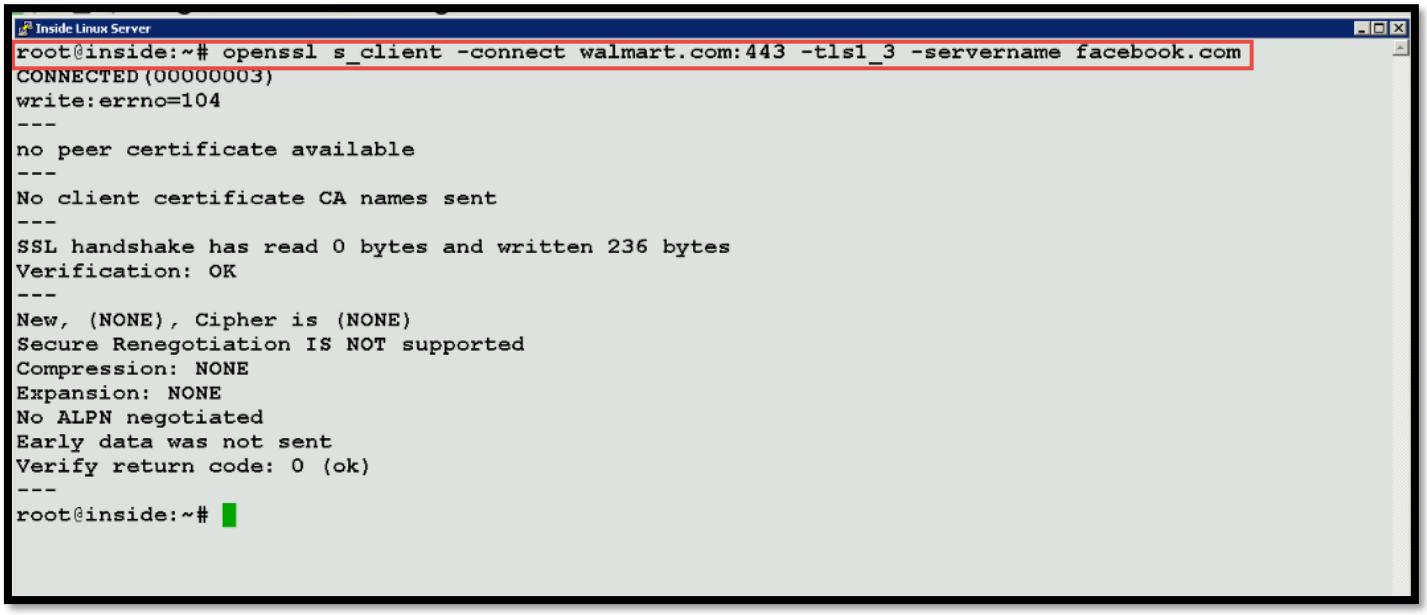
5. Click on the Toggle button to **Enable early application detection and URL categorization for encrypted connections with active TLS certificates probes or Click on the Advanced tab in the ACP select the pencil next to "TLS Server Identity Discovery"** to edit the configuration



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



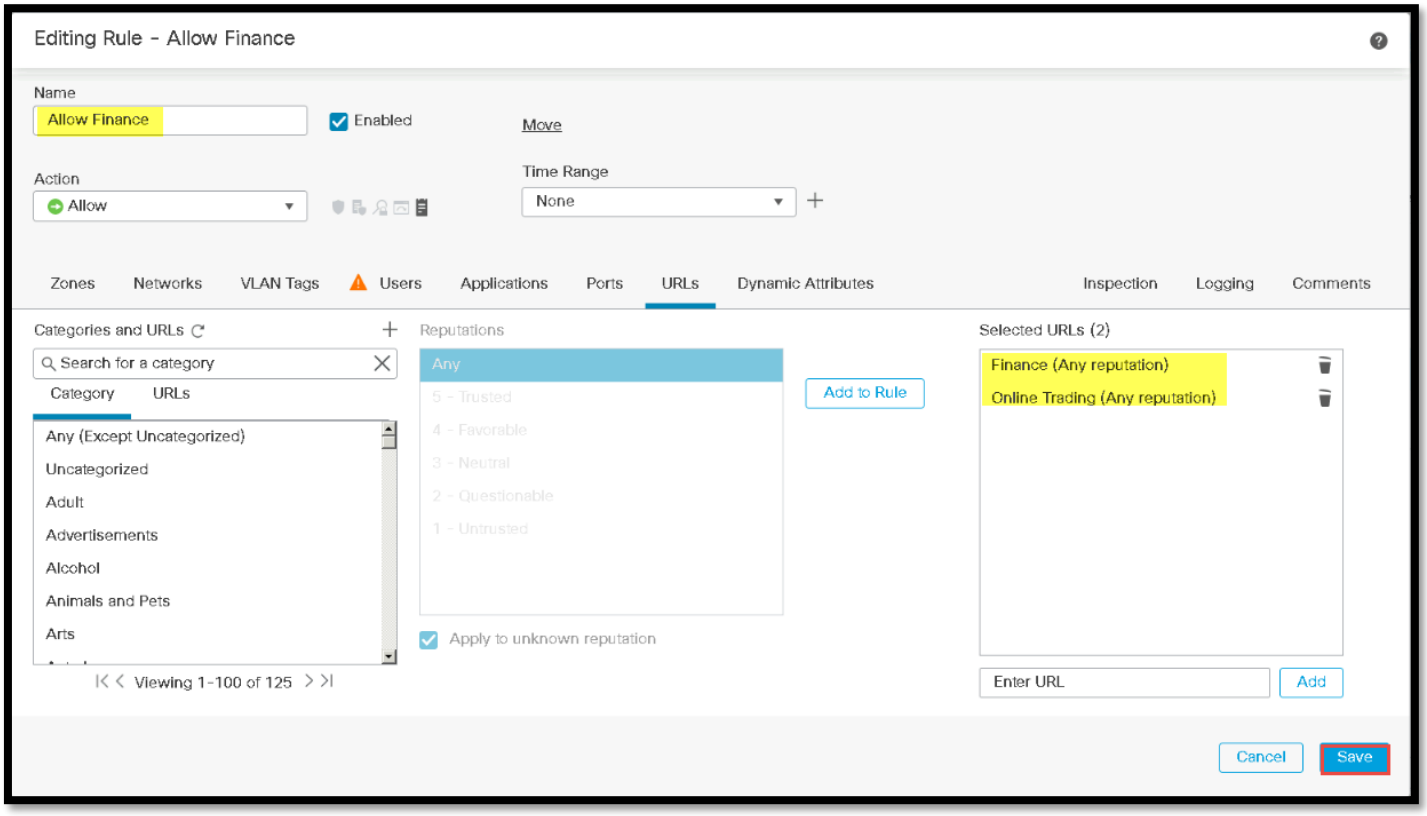
2. Go to the FMC and refresh the connection event and view Table View of Connection Events

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

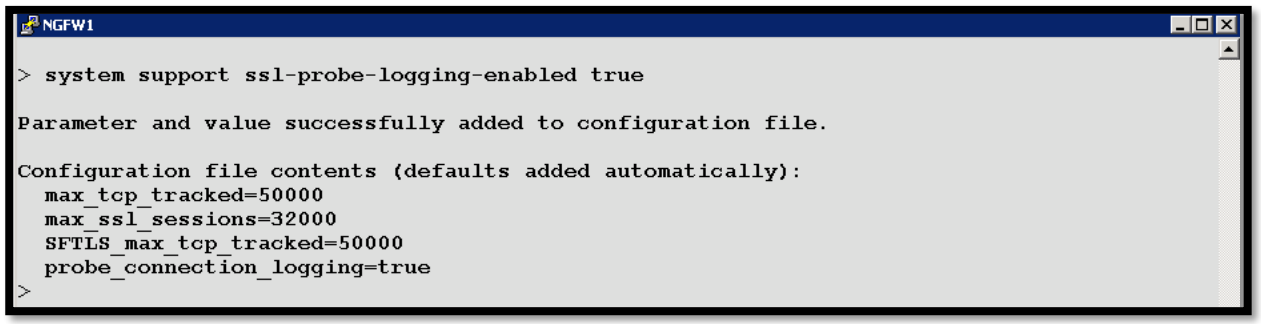
TLS probe helps TLS Server Identity Discovery feature learn about server certificates from TLS 1.3 sessions. This exercise aims to demonstrate that the TLS Server Identity Discovery probe can discover a server certificate, cache it, and use it to assist with the TLS 1.3 connections.

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**

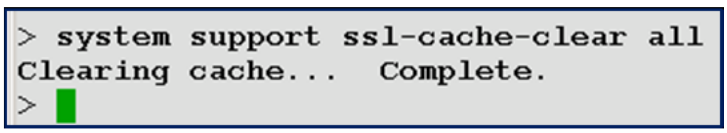


h. **Deploy**

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



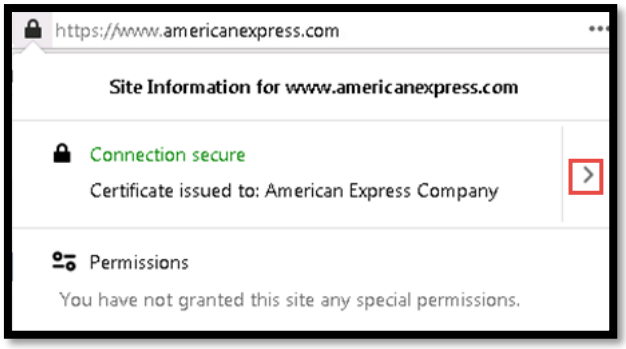
5. Clear the certificate cache
    a. Type: system support ssl-cache-clear all



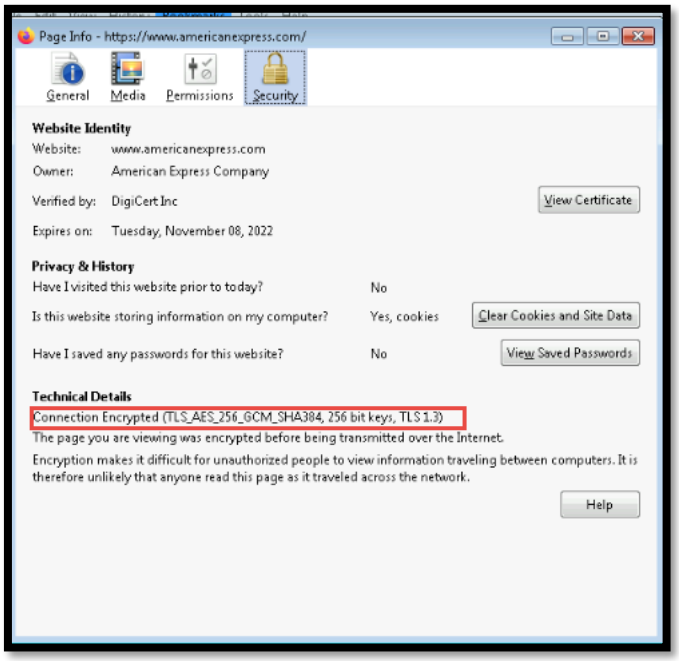
6. Check for a specific certificate in NGFW1 using its domain name /SNI or IP address information
    a. Type: system support ssl-cache-certificate-search
        i. Type 1
        ii. Enter name: americanexpress.com

```
> 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.
>
```

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**

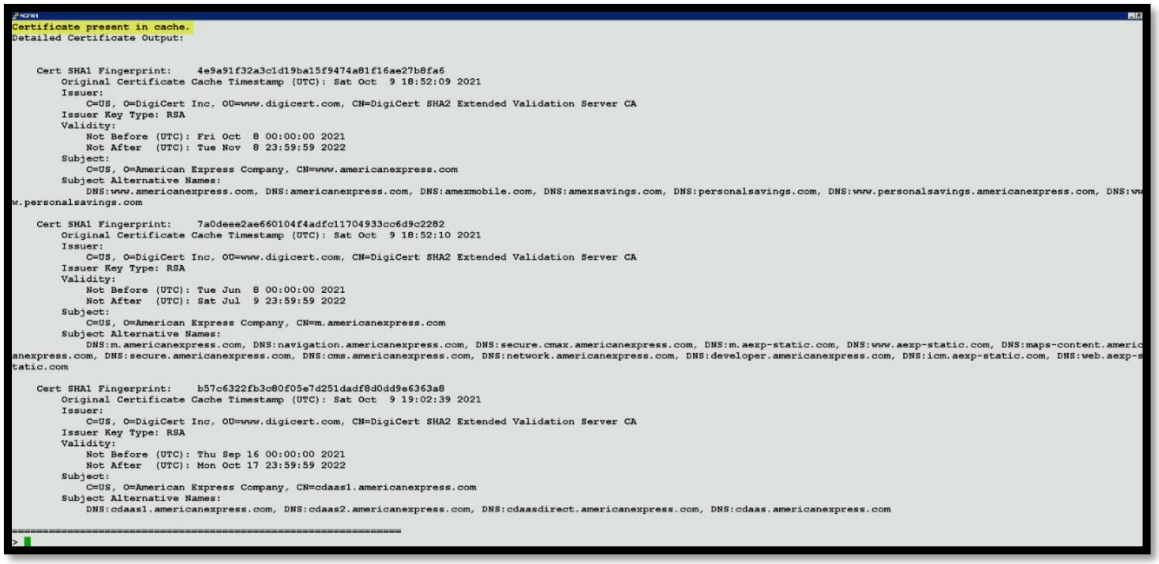
    d. SSL Flow Flags = CERTIFICAT_CACHE_MISS and CERTIFICATE_CACHE_HIT
    e. SSL Flag Message = CLIENT_HELLO

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

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



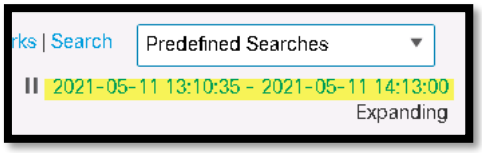
14. On NGFW1 change the ACP back to Base_Policy **Save and Deploy**

Scenario 12. Network Discovery and Firepower Recommendations

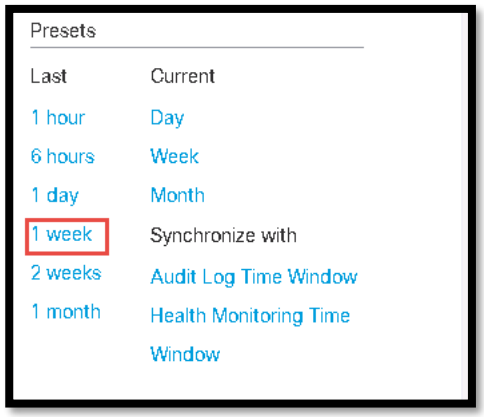
Review Discovery Data

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

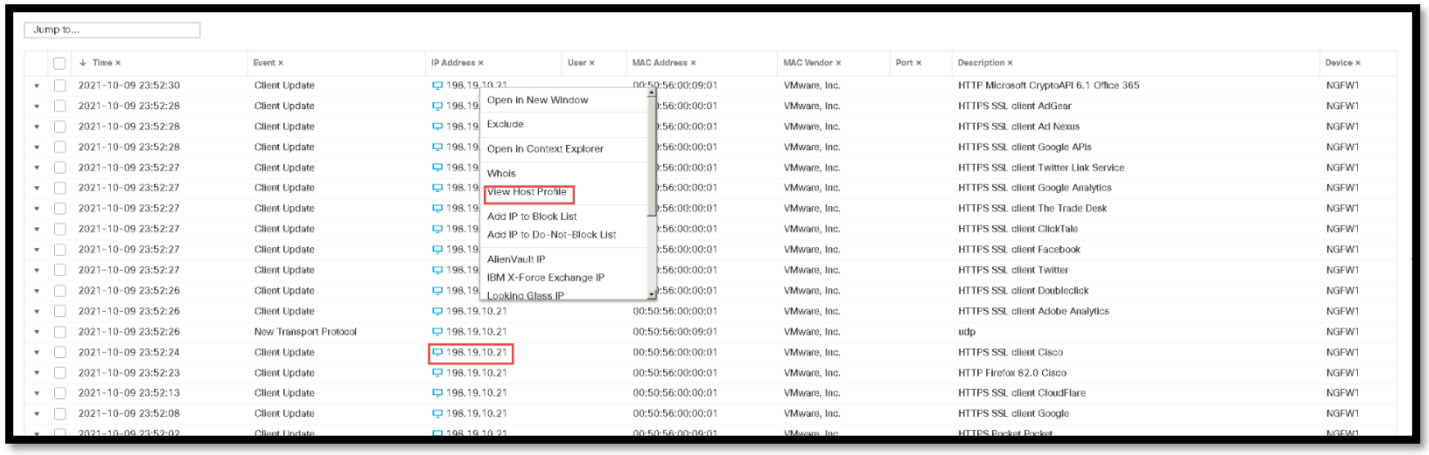
1. Click **Analysis > Hosts > Discovery Events**
2. Click the link in the upper right of the screen that shows the time period the data is from



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**



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

8. Look at the **Operating System**

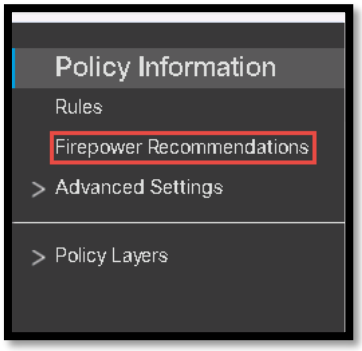
9. Scroll Down and look at **Vulnerabilities**
10. Click on **Content Explorer**
    a. Scroll down and look at the information
11. Go back to the Host Profile and Click on the **Malware Events**
    a. Note the events

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**

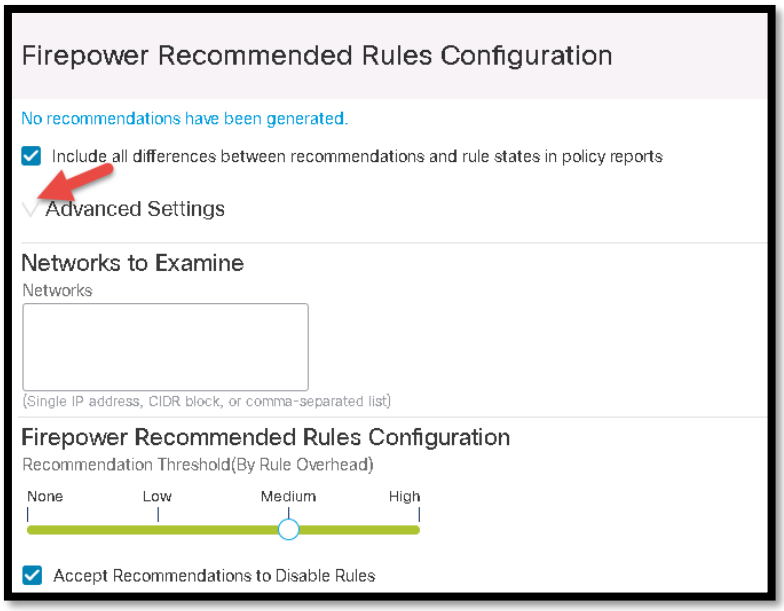
Firepower Recommendations

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**



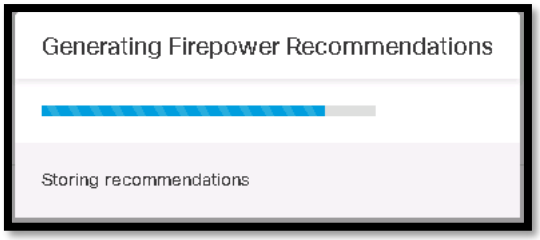
3. Place a checkmark in the **Include all differences…** box and **Click Advanced Settings**



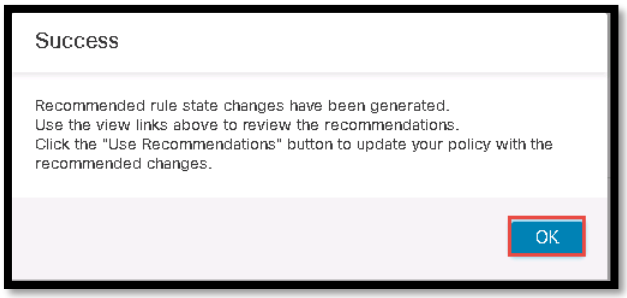
4. Leave the **Accept Recommendations to Disable Rules**

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.

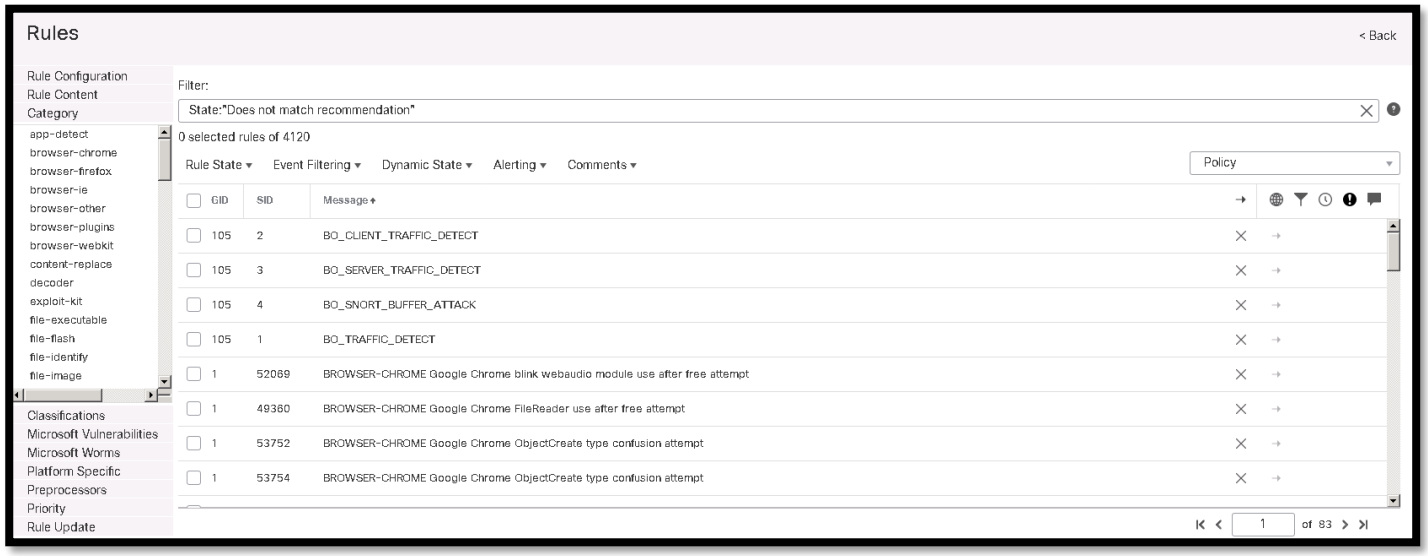
5. Click **Generate Recommendations**



6. Click **OK** on the **Success Box**



7. Click on **View Recommend Changes**



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.

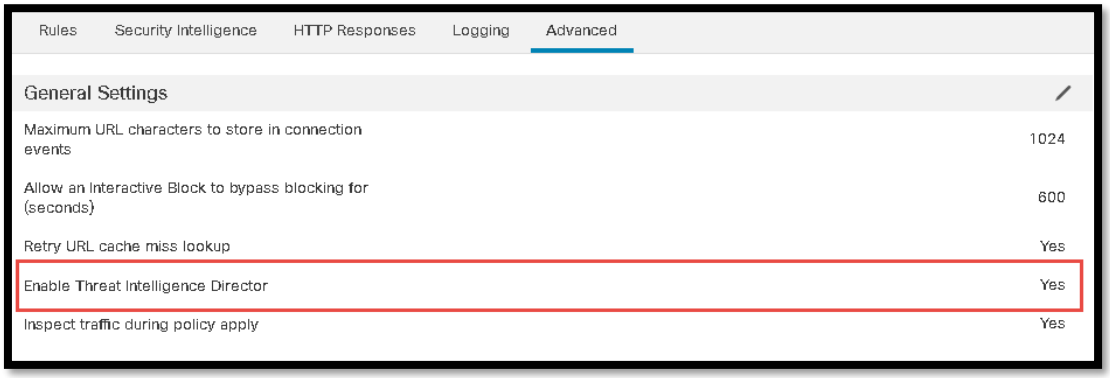
- Upload a list of URLs to CTID that will trigger an Incident
- Subscribe CTID to a TAXII feed
- Generate CTID incidents

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 indictors 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:

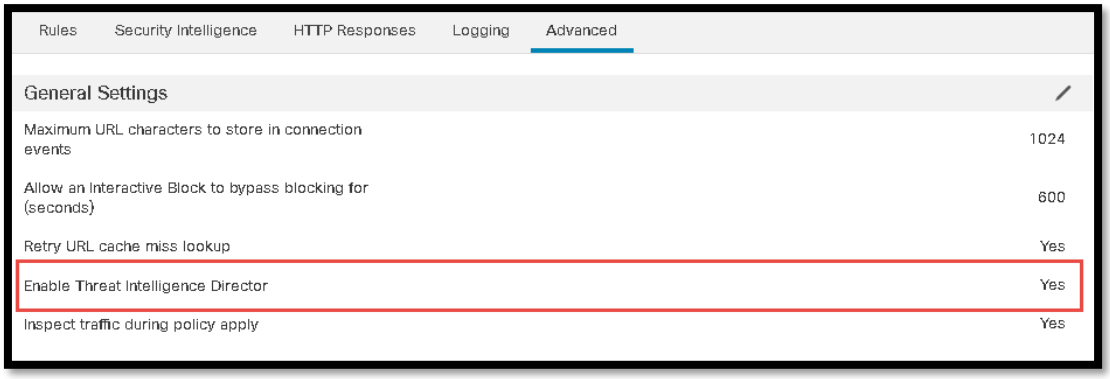
- Uploaded from the computer where the FMC UI is running.
- Retrieved from a URL on a remote web server.
- Received from a TAXII feed (STIX files only).

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

Steps

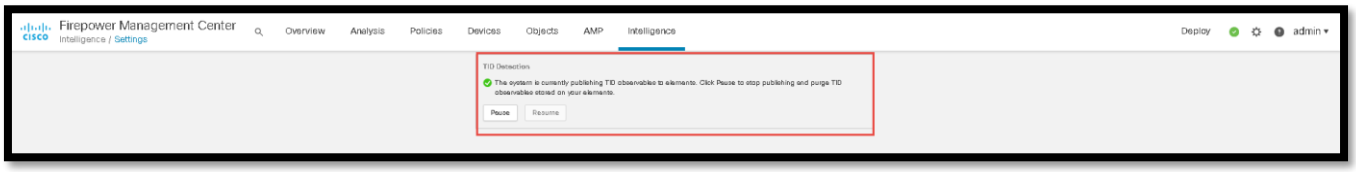
Confirm that CTID will publish observables to the NGFW

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.



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.



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

   a. Navigate to **Intelligence > Sources > Sources**. Click the plus sign (**+**) on the right to add an intelligence source.

   b. For **DELIVERY**, select **Upload**.

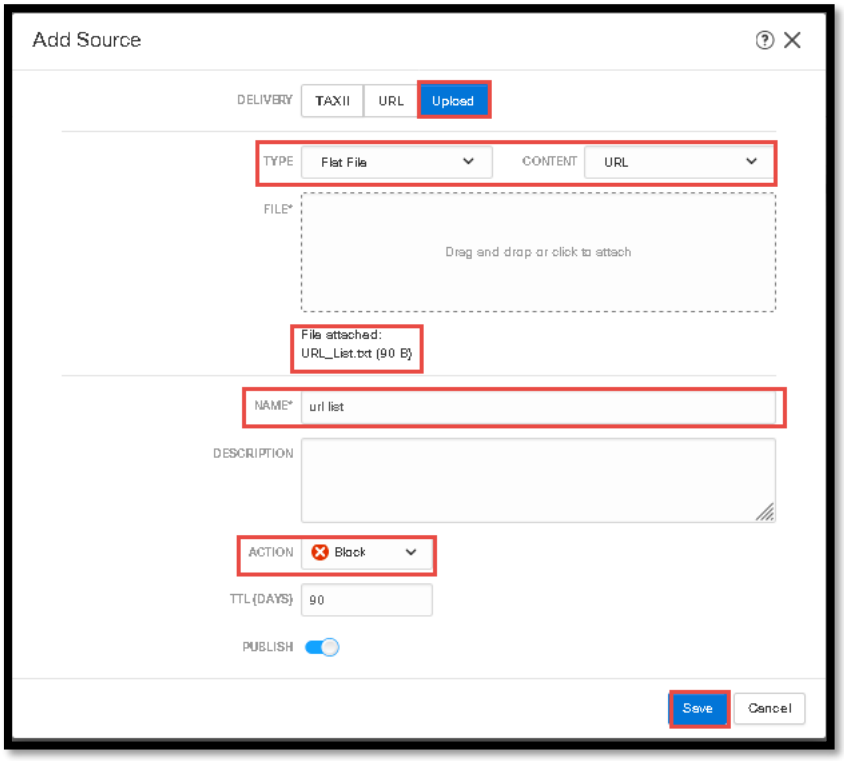
   c. For **TYPE**, select **Flat File**. The **CONTENT** drop-down list will appear.

   d. For **CONTENT**, select **URL**.

   e. Click in the **FILE** area, and select **URL_LIST.txt** from the **Files** folder on the Jump desktop.

   f. For **NAME**, enter url list.

   g. For **ACTION**, select **Block**.



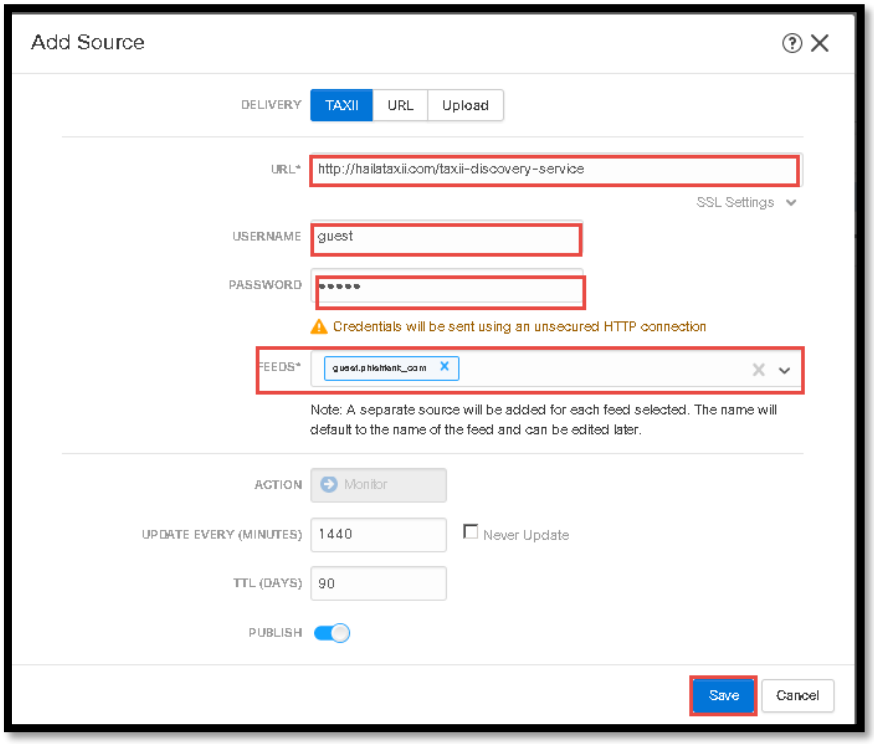
8. Click **Save**.
9. Navigate to **Intelligence > Sources > Observables**. Confirm that two type URL observables have been added.

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.



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/iprep_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 (iprep_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/iprep_download/731625d4-9512-11e7-915c-7252ae92ac.blf:198.18.133.200

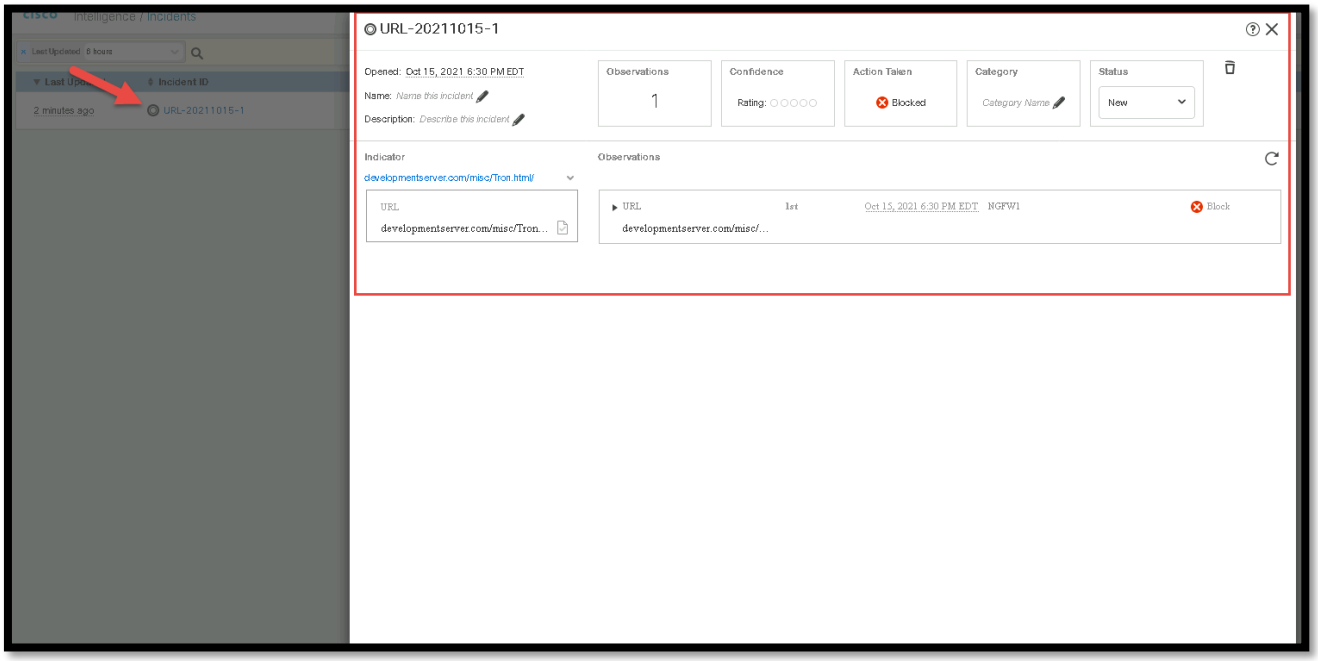
NOTE: If you do not, wait a minute and try again. You must wait for this to be published before you go on.

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 s 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

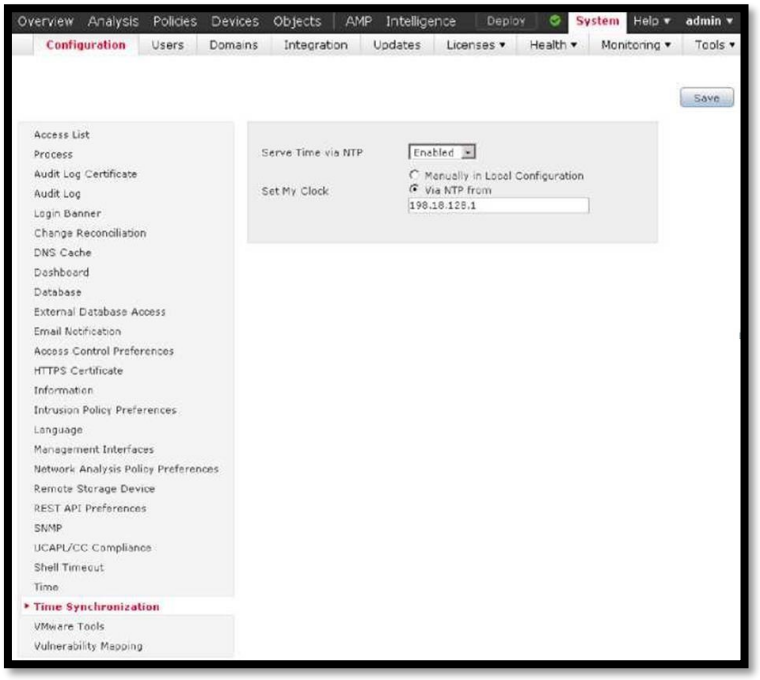
After the initial installation, several configuration steps were performed on the FMC to expedite the lab exercises. These configuration steps are detailed in this appendix.

- 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

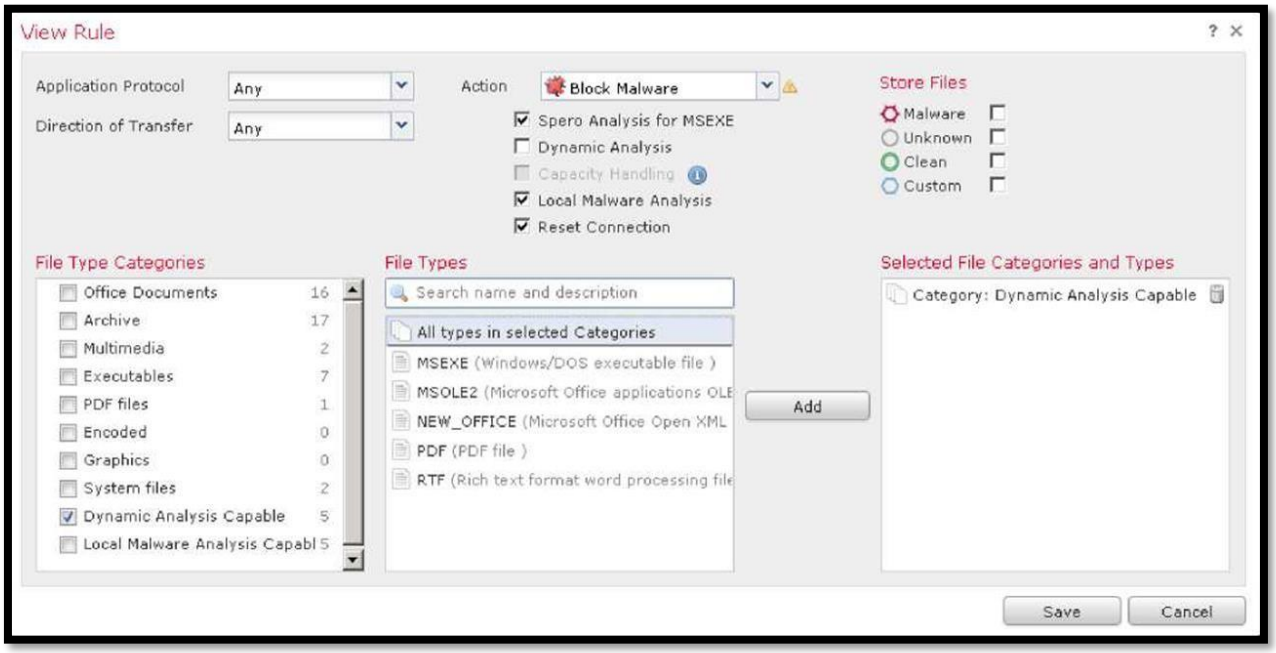
Configuration A1,1: NTP settings

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

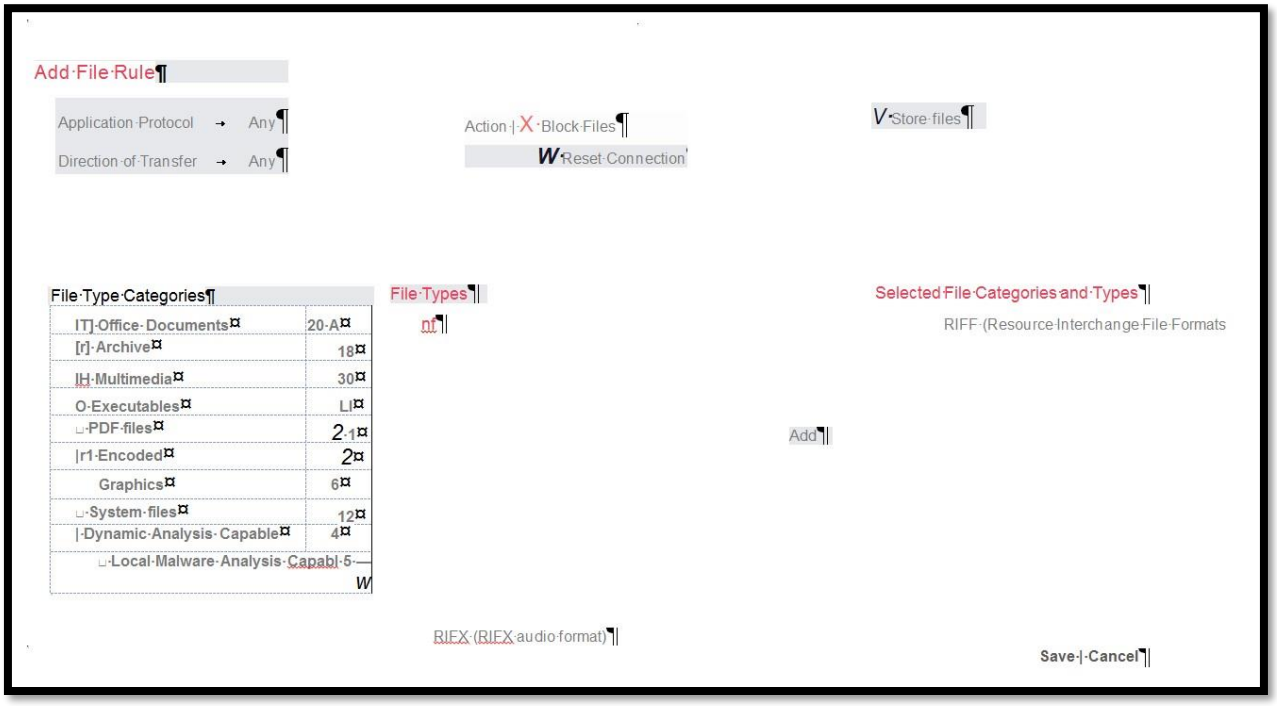


Configuration A1,2: Demo file policy

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 Categorie**s, 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**.



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.

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 > Networ**k.**
    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 Filter**s, search for **Sear**. You will see **Search Engin**e under **Categories**. Check this checkbox, and click **Add to Rule**.
    e. Select the **Logging** tab, and check the **Log at End of Connectio**n 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 use 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\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

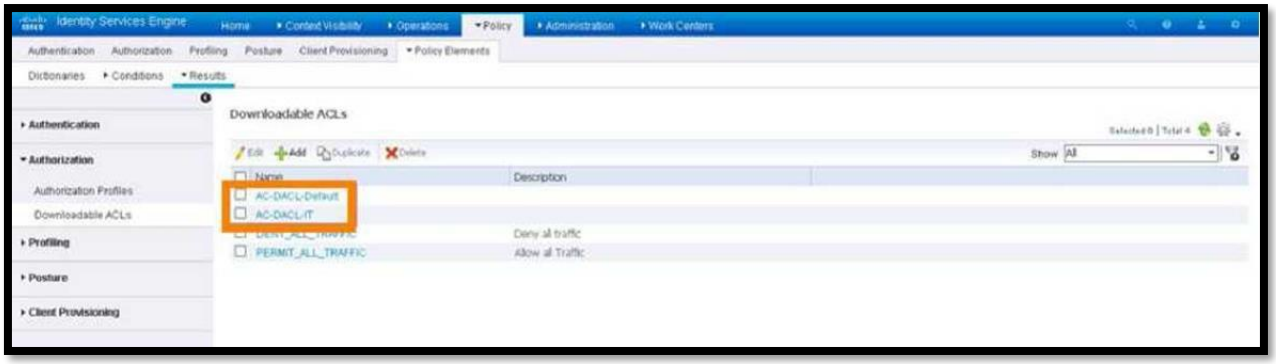
1. Navigate to **Policy > Authorization**. The first two policies were created for this lab: **AC-IT-Policy** and **AC-Default-Policy**. These policies reference two authorization profiles: AC-Auth-IT and AC-Auth-Default.

Authorization profiles

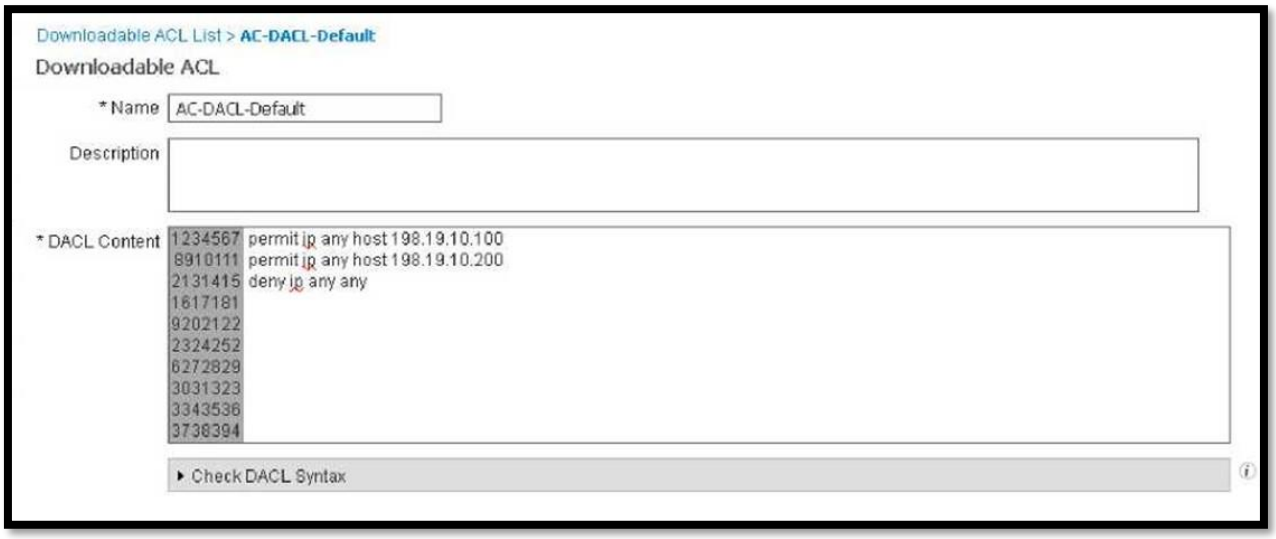
1. **Navigate to** Policy > Policy Elements > Results > Authorization > Authorization Profiles**. The first two profiles were created for this lab:** AC-Auth-Default **and** AC-Auth-IT**.**
2. If you drill down into **AC-Auth-Default**, you will see that it references the **DACL AC-DACL-Default**, described 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.

Downloadable ACLs

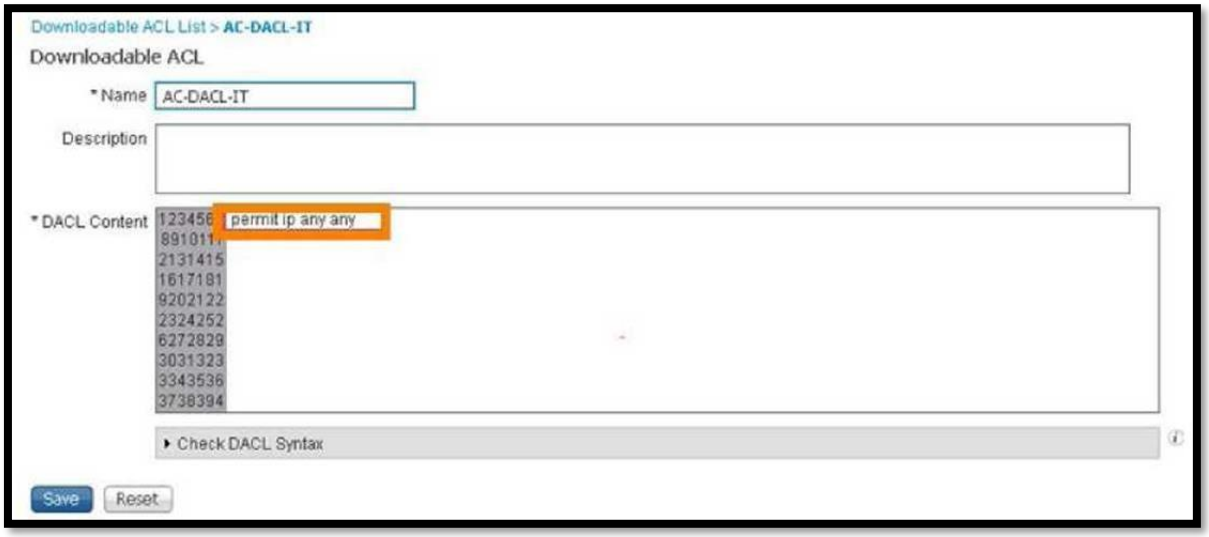
1. Navigate to **Policy > Policy Elements > Authorization > Downloadable ACLs**. The first two DACLs were created for this lab: **AC-DACL-Default** and AC-DACL-IT.



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.



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



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.**