# Cisco Secure Firewall 7.x Basic 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.

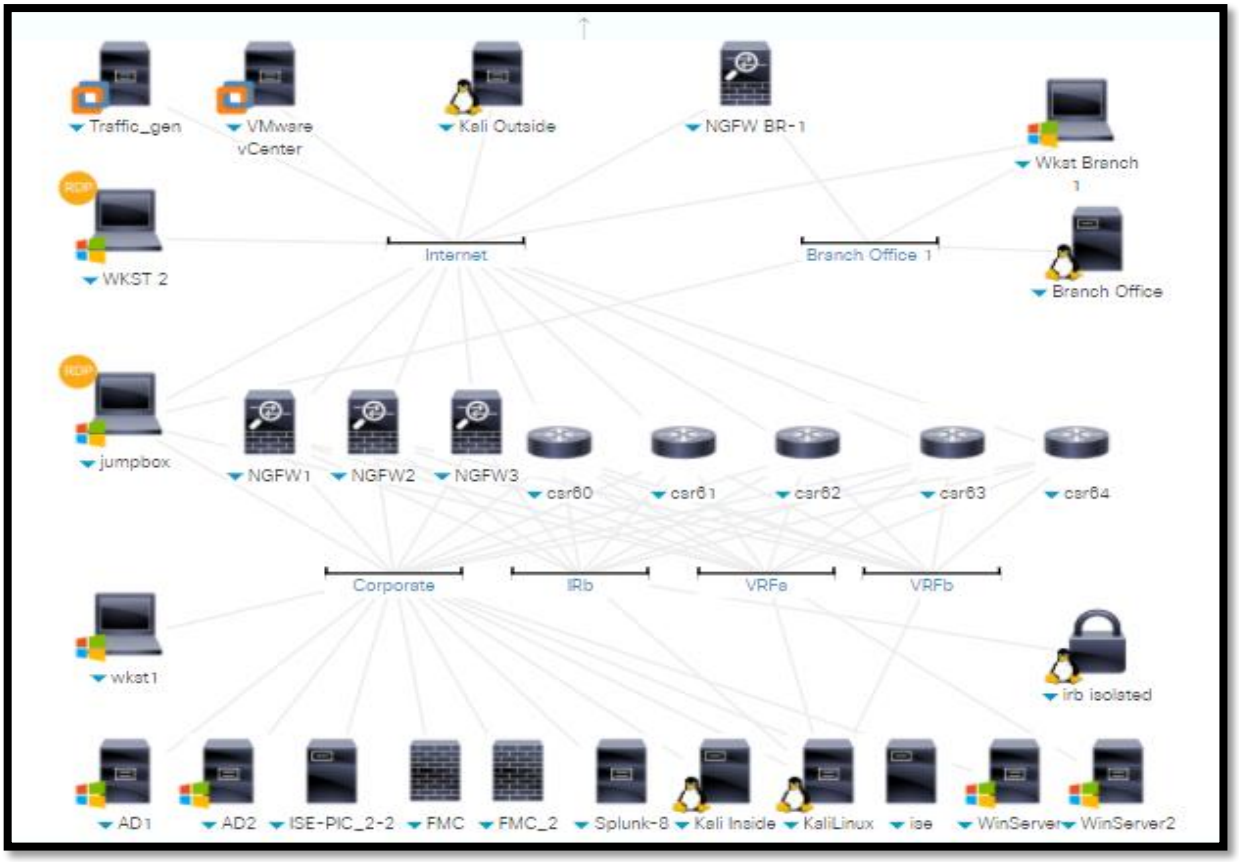
This allows the Cisco Firepower NGFW to evolve with a focus on enabling enterprises to stop, prioritize, understand, and automate responses to modern threats in real-time. Firepower NGFW is unique in its threat-focus, with a foundation of comprehensive network visibility, best-of-breed threat intelligence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

Initiate your dCloud session. [Show Me How]

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

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 1: **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.

# Scenario 1. Configure FMC

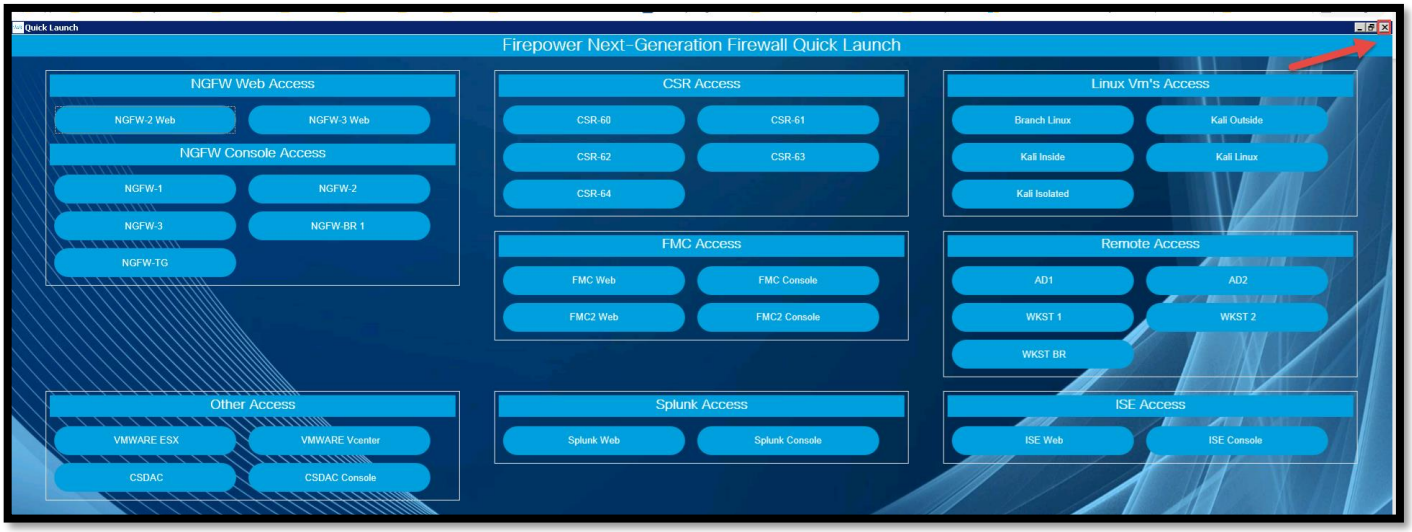
You have been assigned as the Field Engineer to implement the Firepower Management Center and Firepower Threat Defense appliances for your customer. You will now go through the configuration steps on the FMC to prepare it for managing the FTD appliance. In this scenario, your customer has performed the initial appliance load and bootstrap to get it on the network but has not completed any of the required configuration to move forward and use the appliance in production.

**NOTE:** Because the equipment you are working with in this lab is hosted in a remote virtual environment in dCloud, there are some aspects of initial device configuration that are not able to be experienced. This lab will step you through as closely as possible to a new FMC and FTD appliance being deployed as possible. The FMC virtual machine has been deployed as a VM, has had an IP address assigned to it, a certificate has been installed, and has been licensed. The FTD virtual machine, NGFW1, has been deployed as a VM and has an IP address assigned to its management IP address.

# Steps

## Quick Launch

1. This lab guide does not reference any connections using the Quick Launch.
2. If you would like to disable for the duration of the lab click on the [X] at the top right of the screen




## FMC Access

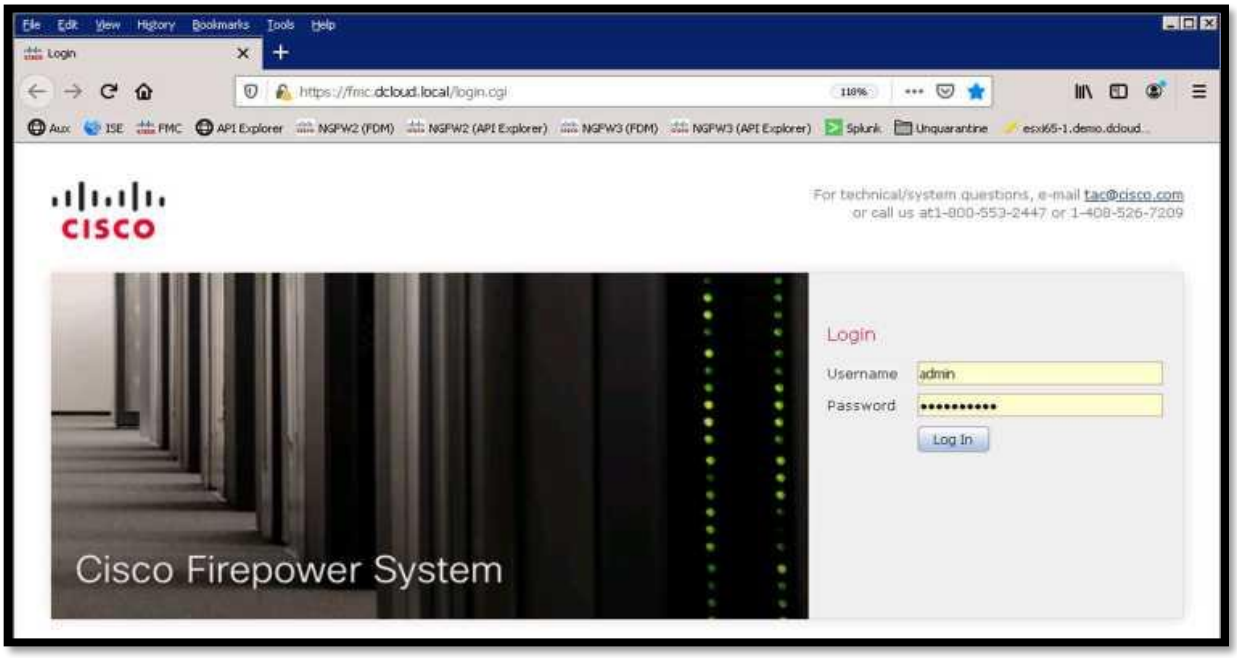
1. Open the Firefox web browser using the link located on the desktop of the Jumpbox desktop.


The browser window opens the login page for the FMC by default.

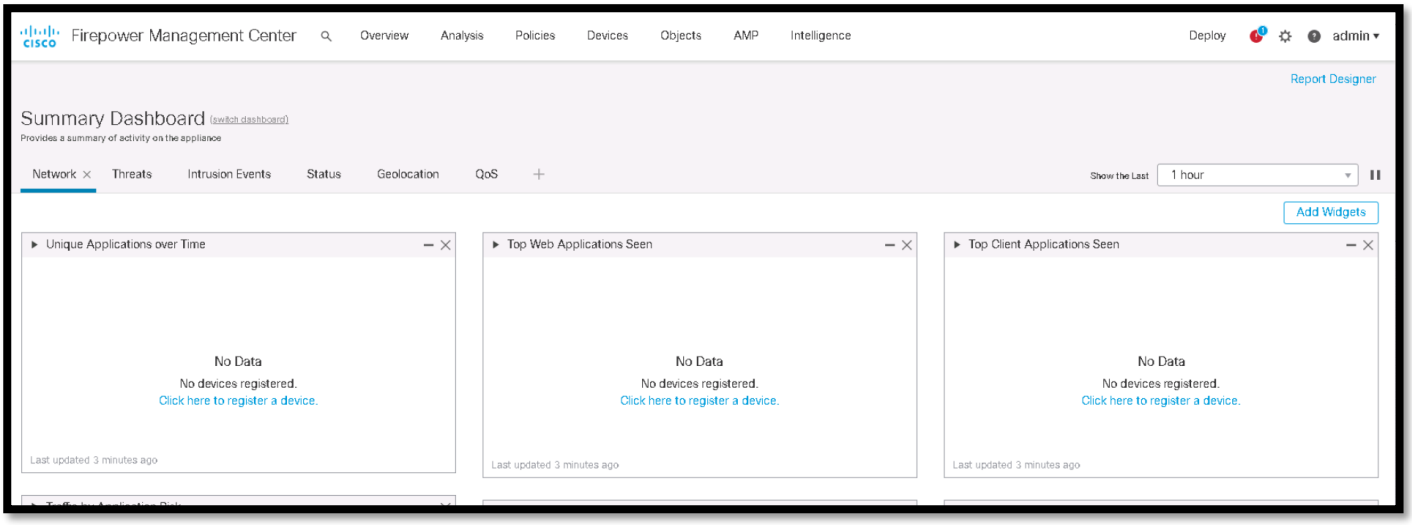
To access the FMC manually in case the browser does not open by default, navigate to **https://fmc.dcloud.local** or click the **FMC** bookmark on the bookmark's toolbar of the Firefox browser.

2. Log in to the FMC using the credentials below and clicking the **Log In** button. The password may be saved in the browser. If so, then click the **Log In** button and proceed.

- Username: **admin**
- Password: **C1sco12345**



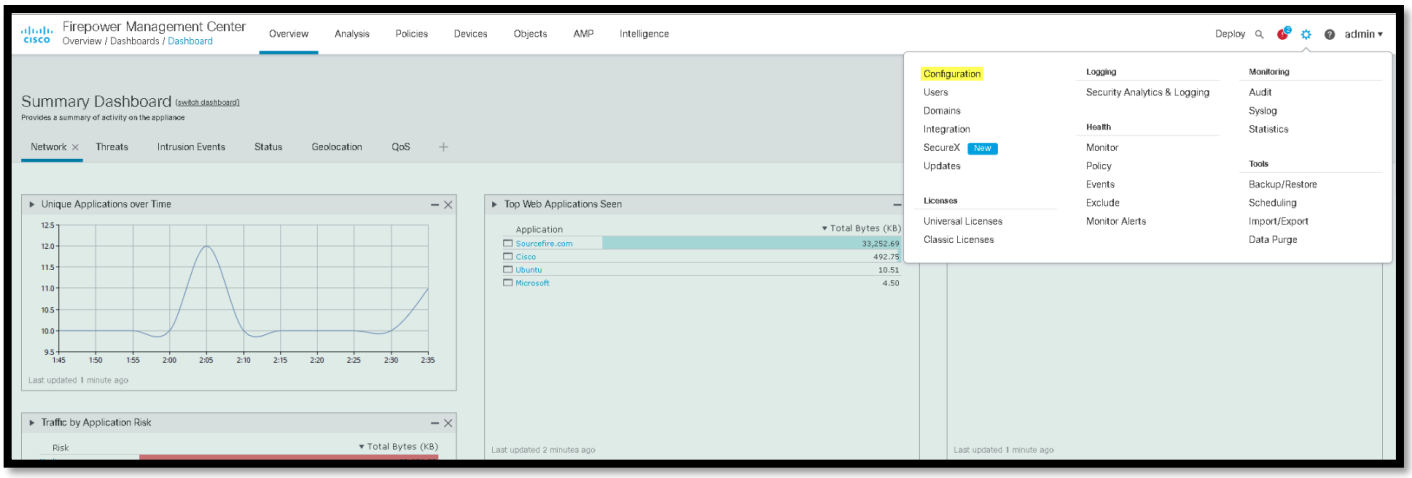

You are presented with the Summary Dashboard screen. There will not be many items with data on the screen as there are no devices added to the FMC at this point in the implementation.



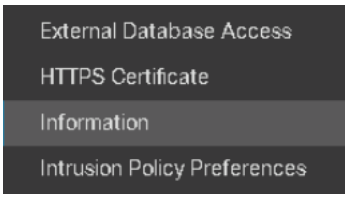

**NOTE:** The menus across the top of the screen will be used in configuring the features and settings used by the devices managed from the FMC as well as reviewing event and security data being reported by devices the FMC manages. You will now use the System menu represented by the gear icon in the top right of the screen to make configuration changes for the FMC itself.

## Configure FMC Settings

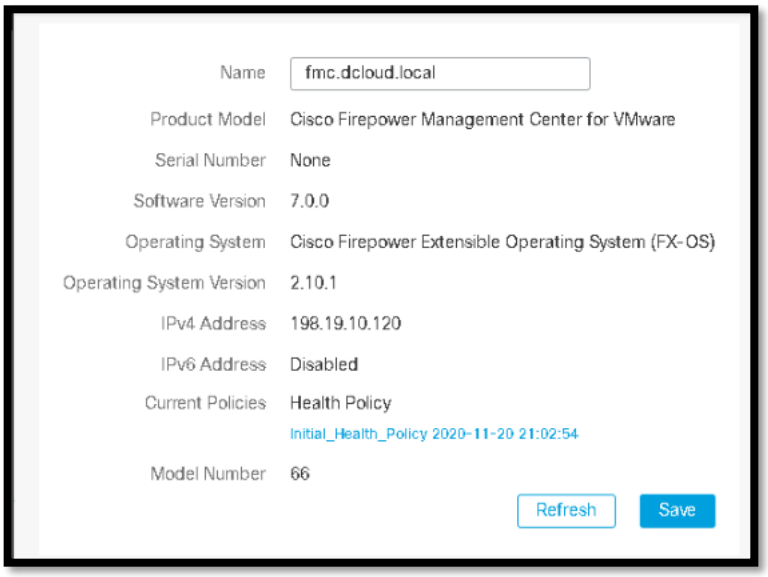
1. In the top right corner of the FMC user interface click the **System** menu represented by the gear icon and select C**onfiguration**



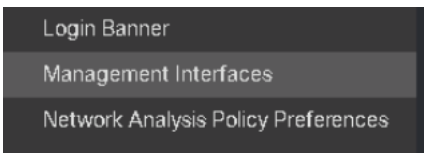

2. On the left window select **Information**



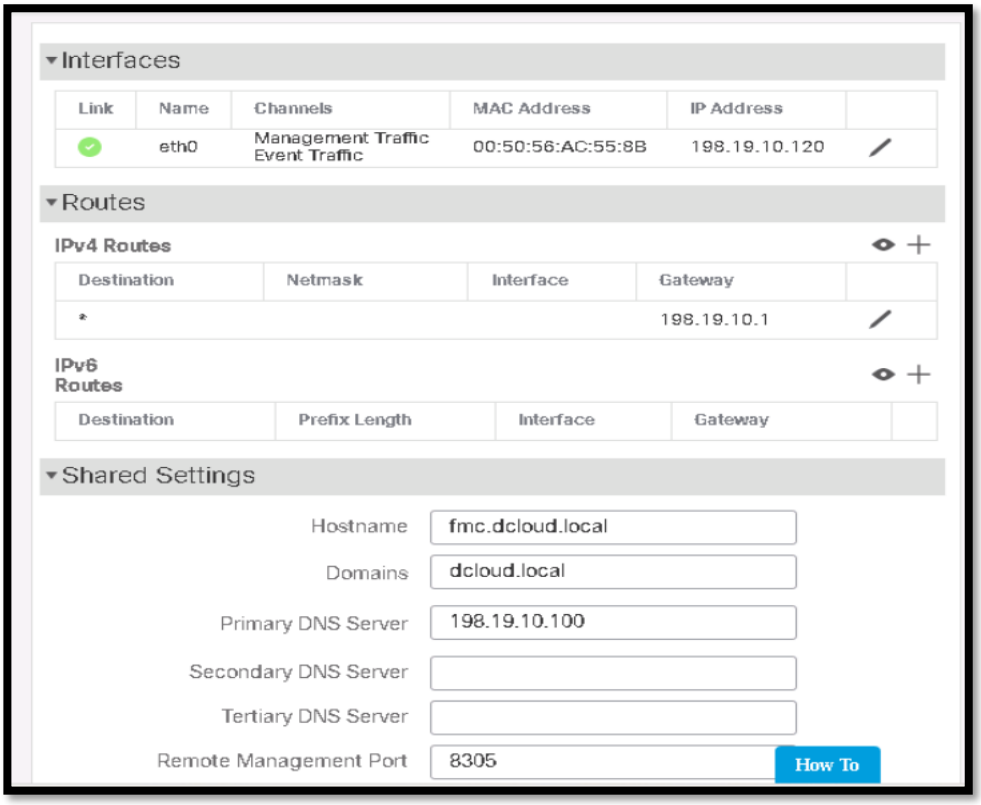

3. Information includes Model, Serial Number, Version etc., is displayed on this page.




4. Select **Management Interfaces** from the left window pane

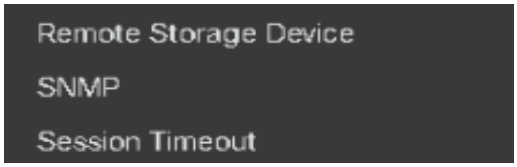


5. Review the configuration items on this page but do not make any changes. This is where items such as the management interface IP address, routes, DNS hostname, DNS domain, DNS Server settings, and Remote Management Port are configured.

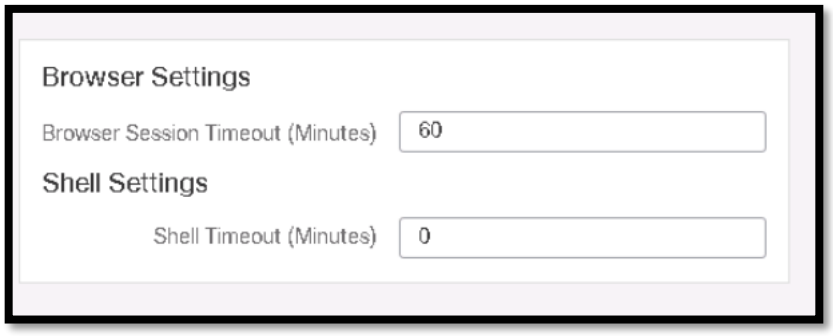



**NOTE:** In a customer deployment, you would obtain the hostname, domains, and DNS server settings from the customer and specify the values here so the FMC can resolve DNS names. The hostname is also important when dealing with certificates for the FMC as the common name of the certificate must match the hostname in order for the certificate to be recognized as valid.

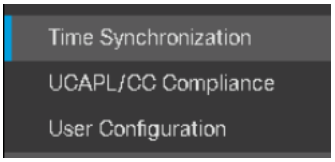
6. On the left window pane select **Session Timeout**




7. The session timeout for web browser access and SSH/console command line access to the FMC is controlled with this setting. Review the current settings that allow for 60 minutes of time to pass before logging the user out of the FMC web user interface and no timeout for the command line shell interface and then proceed with the next step of the lab.

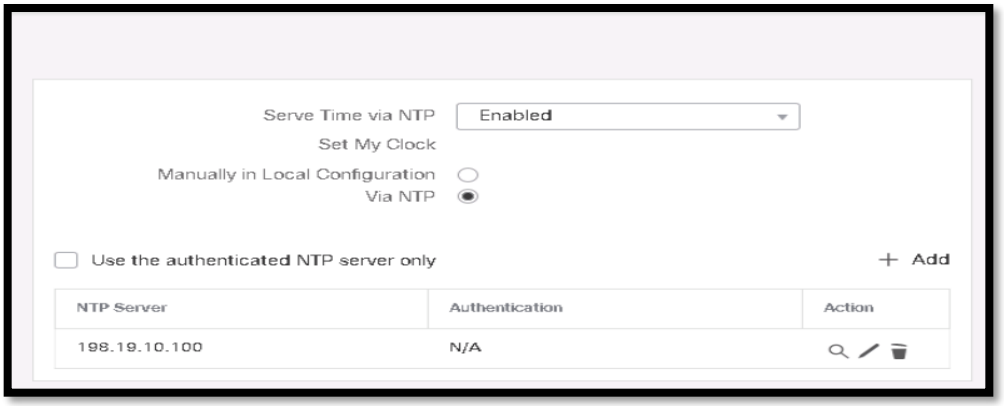


8. On the left windows pane select **Time Synchronization**

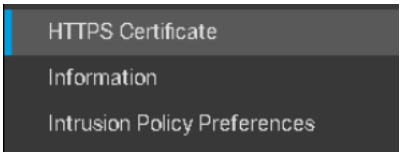



**NOTE:** The FMC can function as a time source for managed devices. In this lab environment, the time and NTP settings are preconfigured to help ensure the lab environment is functional. In a customer deployment, you would configure these settings to have a reliable trusted customer time source added to the list of NTP servers to ensure the FMC has correct time.

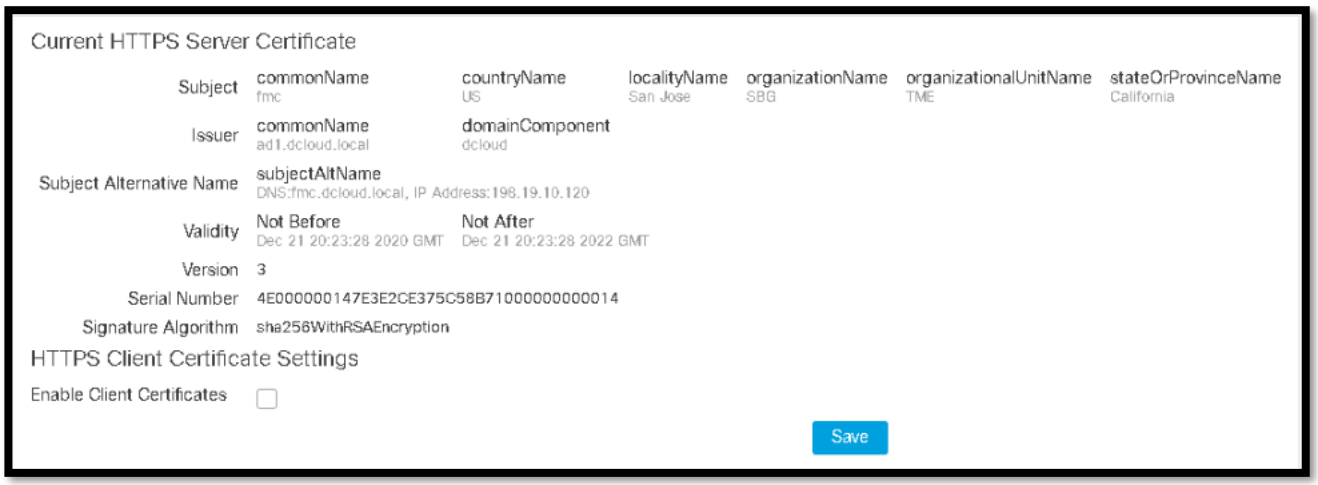
9. Review the settings on the page, do not make any changes at this time, continue with the lab.




10. Review the HTTPS certificate for the FMC. From the left window pane select **HTTPS Certificate.**

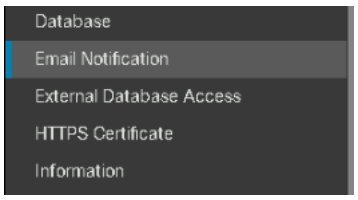



11. The current certificate being used by the FMC is shown. This is a certificate generated by the Certificate Authority in the lab and preconfigured for lab purposes. In a customer environment a best practice would be to replace the default self-signed certificate with a certificate generated by a trusted Certificate Authority. Review the settings and proceed with the lab.



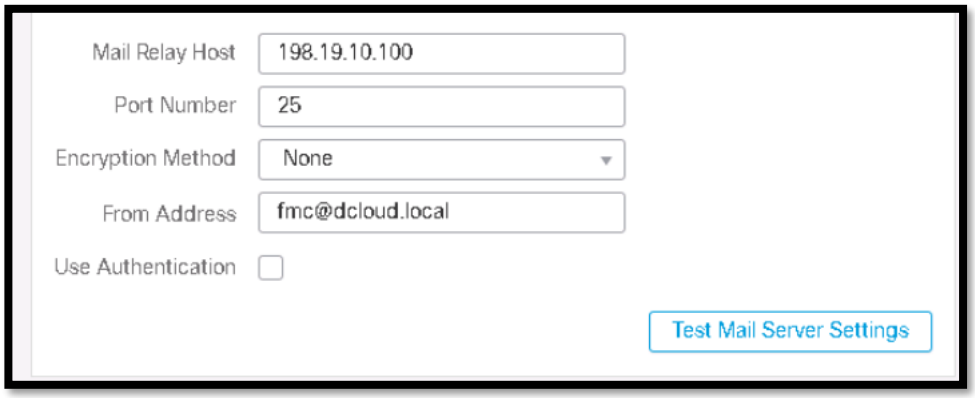
**NOTE:** The FMC can generate a Certificate Signing Request (CSR) to submit to a Certificate Authority (CA) or if a certificate was already generated for the FMC it can be imported from this screen as well.

12. From the left window pane select **Email Notification**



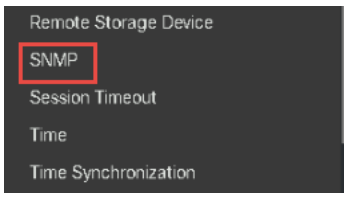

13. You will now configure the FMC to send email notifications through the customer SMTP server. Use the following settings to configure Email Notification.

    Mail Relay Host: **198.19.10.100**
    Port Number: **25**
    Encryption Method: **None**
    From Address: **fmc@dcloud.local**

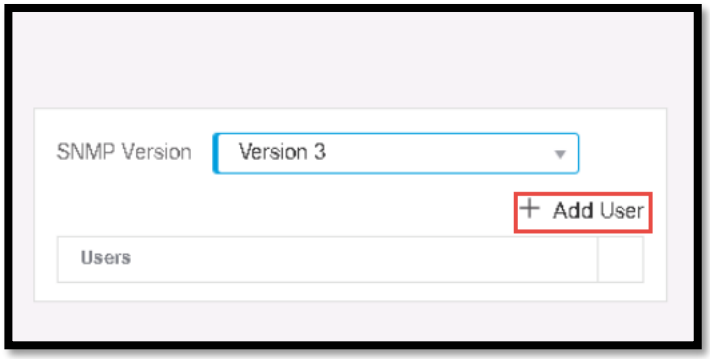



**NOTE:** In your customer environment you will need to get the correct settings from the customer for the encryption method, port number, and authentication settings to use. In dCloud there is not an SMTP server currently implemented so clicking the Test Mail Server Settings will not succeed.

15. Configure SNMP on the FMC so that it can be polled by the customer's monitoring system for status and performance. From the left window panel select **SNMP.**

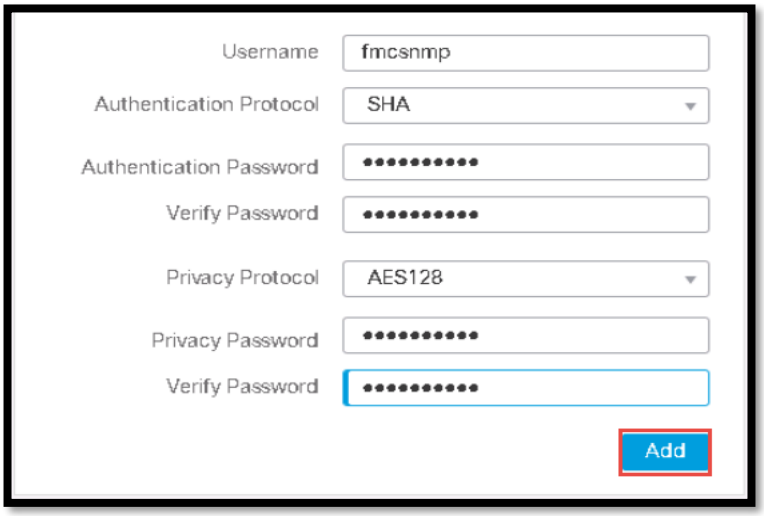



16. For the **SNMP Version** settings choose **Version 3** and click **Add User**




17. Configure the following SNMPv3 user settings

Username: **fmcsnmp**
Authentication Protocol: **SHA**
Authentication Password: **C1sco12345**
Verify Password: **C1sco12345**
Privacy Protocol: **AES128**
Privacy Password: **C1sco12345**
Verify Password: **C1sco12345**




18. Click **Add**

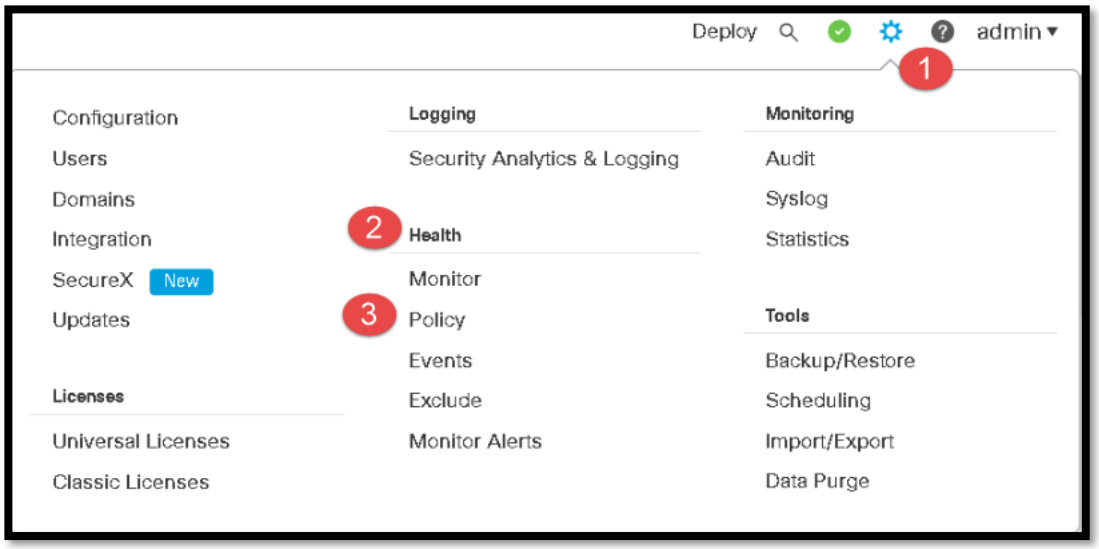
**NOTE:** In your customer environment you should use values provided to you from your customer to match their SNMP polling settings. A best practice is to use SNMPv3 with Authentication and Privacy protocols enabled and complex passwords

19. The SNMP v3 user will appear in the list. The FMC can be polled for health and performance statistics. Click **Save**

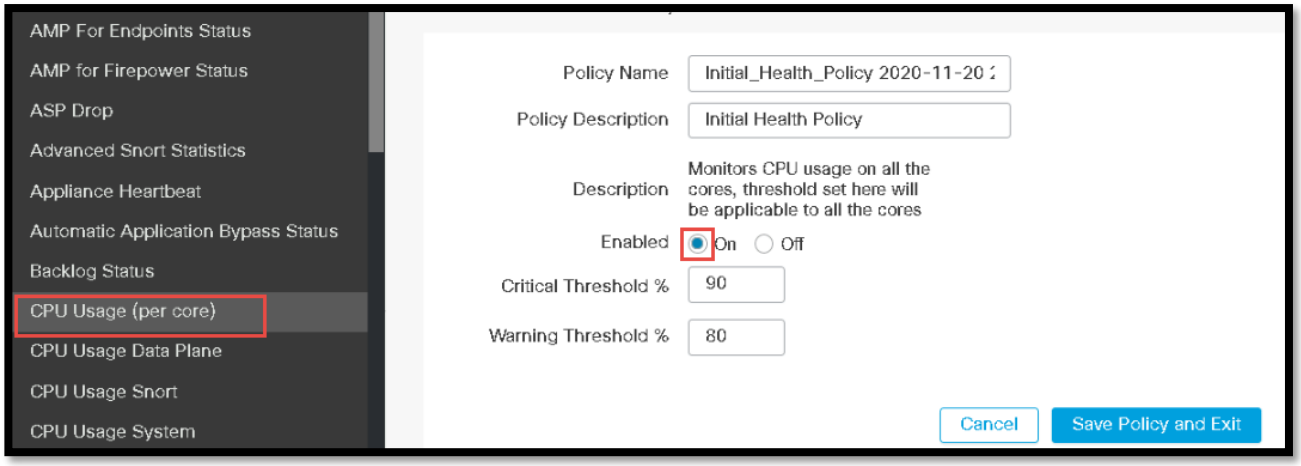

## FMC Device Health Monitoring

Here we will show you some monitoring features that were added in 6.7.

1. Go to System > Health > Policy




2. Edit the Initial_Health_Policy by clicking on the pencil icon
3. Click on CPU Usage (per core) and click Enabled On



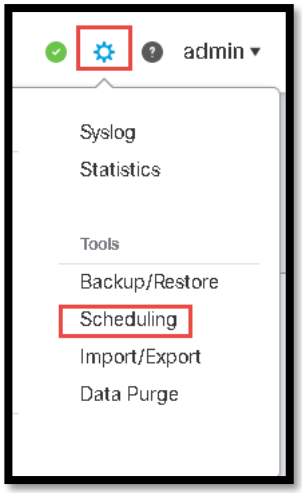

4. Look at some of the other modules and note the status
5. Click on **Save Policy and Exit**
6. Click on apply polices


7. Select all devices and **Apply**

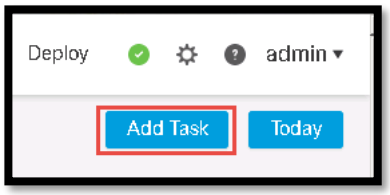

## Configure Scheduled Tasks

In this section you will configure the FMC to automate some tasks that can be run on a schedule. This will include updating the CRL (Certificate Revocation List), the VDB (Vulnerability Database), and configure a Backup

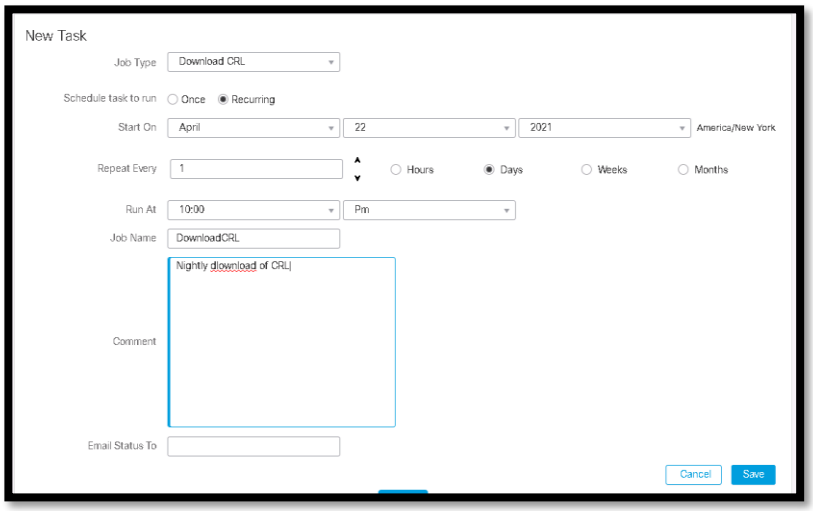
1. From the Jumphost login to the FMC admin/C1sco12345
2. Select the Gear Icon at the top right Tools > Scheduling




3. Click **Add Task**

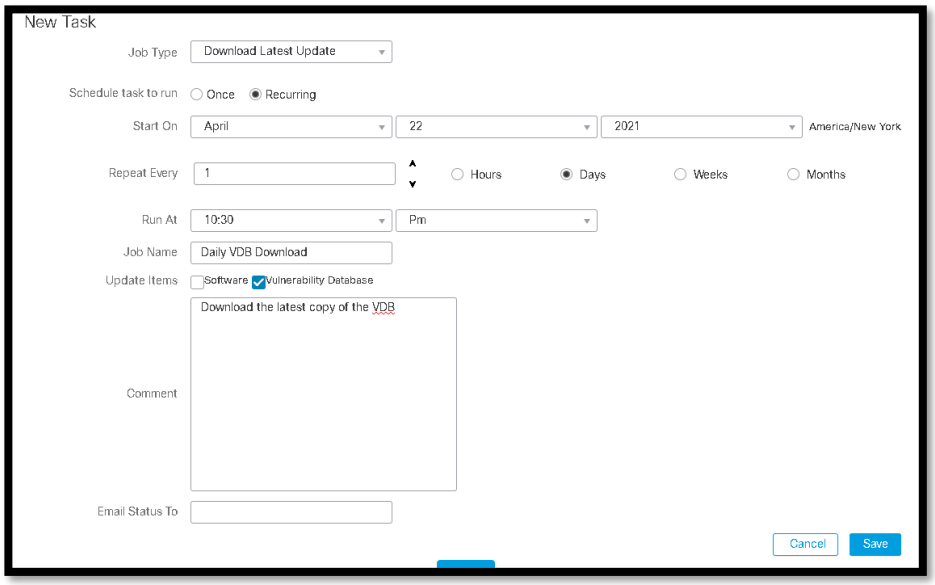



4. Fill in the following:
    a. Job Type: Download CRL
    b. Schedule task to run: Recurring
    c. Start On: (enter tomorrow's date)
    d. Repeat Every: 1 Day
    e. Run At: 10:00 pm
    f. Job Name: Download CRL
    g. Comment: Nightly download of CRL



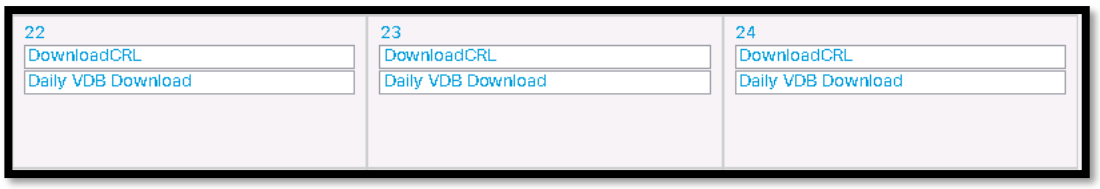

5. Click **Save**
6. You will see that the task has been added to calendar


7. Click Add Task
    a. Job Type: Download Latest Update
    b. Schedule task to run: Recurring
    c. Start On: (enter tomorrow's date)
    d. Repeat Every: 1 Days
    e. Run at 10:30 pm
    f. Job Name: Daily VDB Download
    g. Update Items: Vulnerability Database
    h. Comment: Download the latest copy of the VDB




i. Click **Save**

8. You will see the task added to your calendar




9. Click Add Task

   a. Job Type: Update URL Filtering Database (click OK to the warning regarding deploying the updates if prompted)

   b. Schedule task to run: Recurring

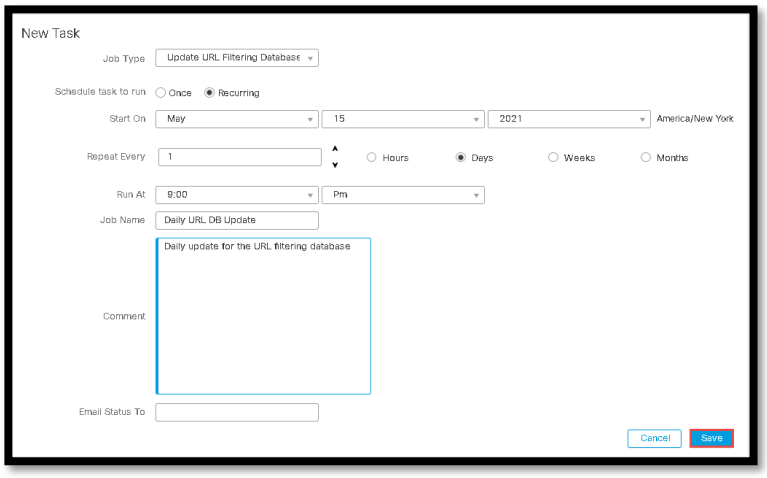
   c. Start On: (enter tomorrow's date)

   d. Repeat Every: 1 Days

   e. Run at: 9:00 pm

   f. Job Name: Daily URL DB Update

   g. Comment: Daily update for the URL filtering database




h. Click **Save**

10. Click **New Task**

a. Job Type: Deploy Policies

b. Schedule task to run: Recurring

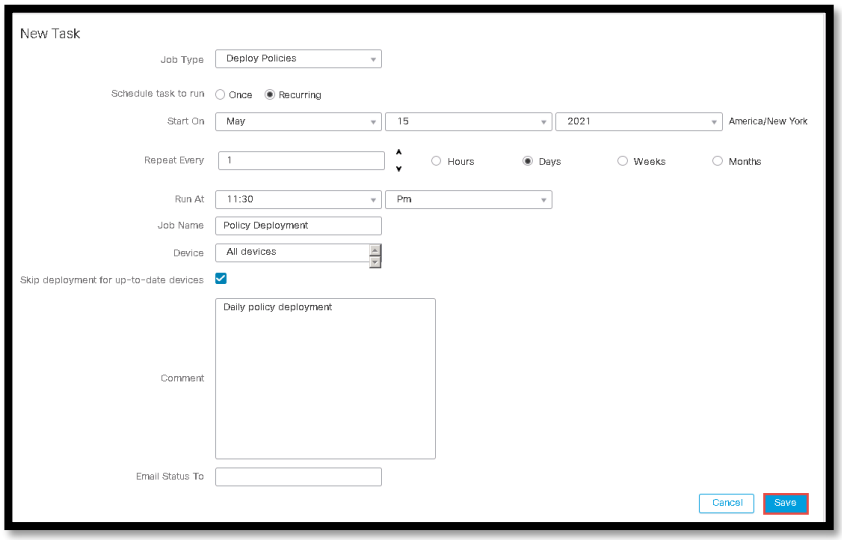
c. Start On: (next tomorrow's date)

d. Repeat Every: 1 Day

e. Run At: 11:30 Pm

f. Job Name: Policy Deployment

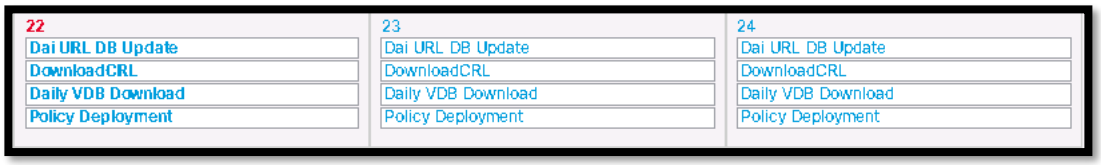
g. Devices: All devices




h. Comment: Daily policy deployment

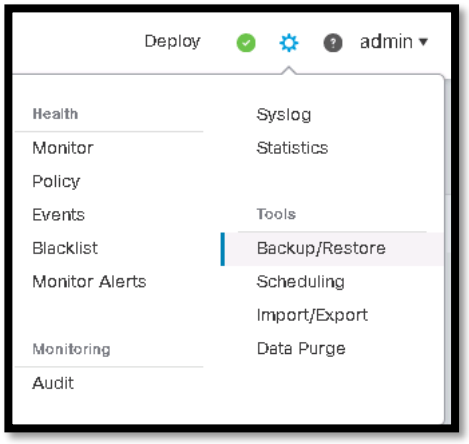
i. Click **Save** (If you receive an error stating no sensor(s) selected, click on **All devices** and try again)

11. Check the calendar

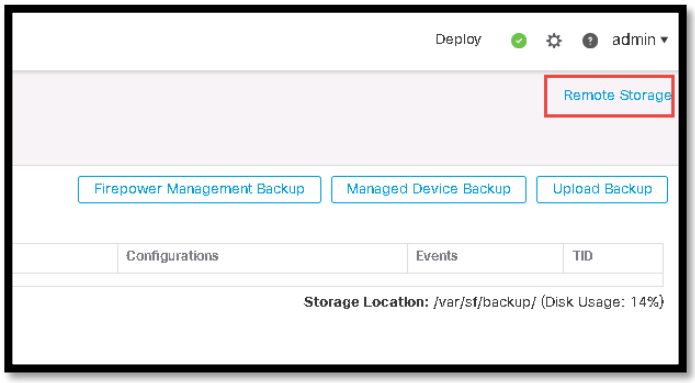



12. Configuring Backup

    a. Go to Gear Icon Backup/Restore




    b. Click Remote Storage




    i. Storage Type: SSH

    ii. Host: 198.19.10.200

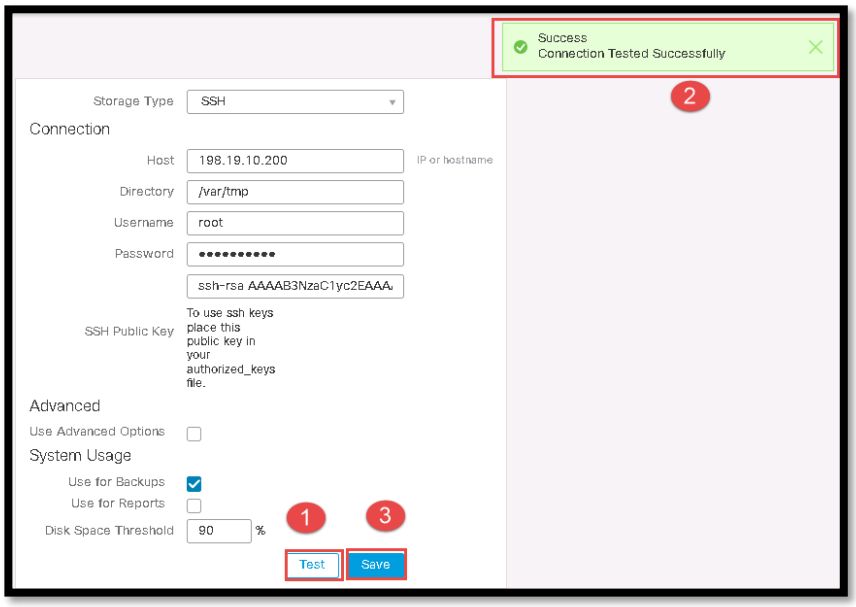
    iii. Directory: /var/tmp

    iv. Username: root

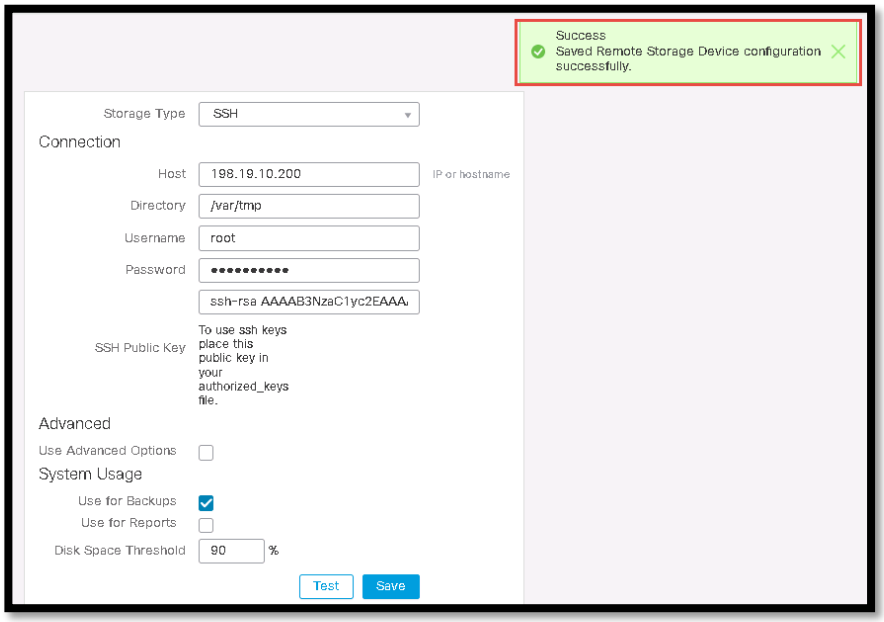
    v. Password: C1sco12345

    vi. Use for Backups: Check the box

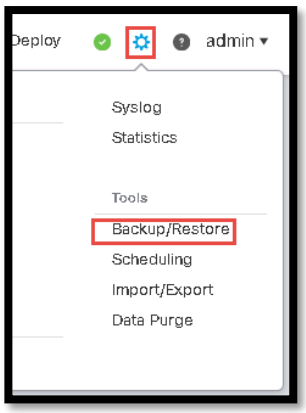
    vii. Test



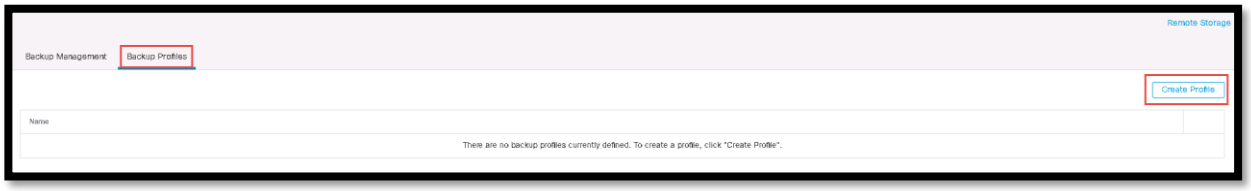

viii. Click **Save**




13. Click on the Gear Icon > Tools > Backup/Restore



14. Select Backup Profiles > Create Profile



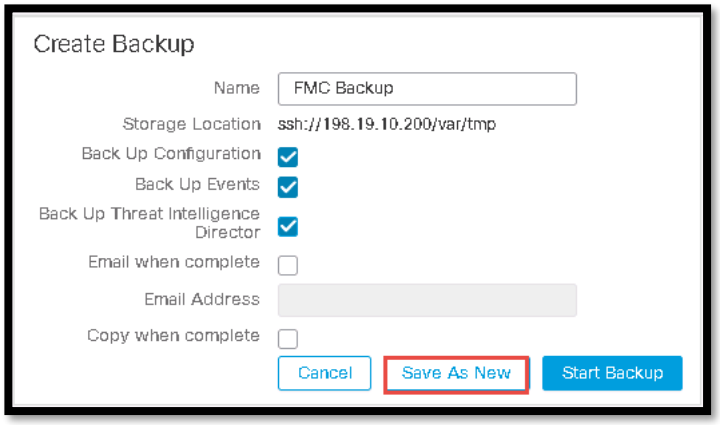

a. Name: FMC Backup

b. Back Up Configuration: Checked

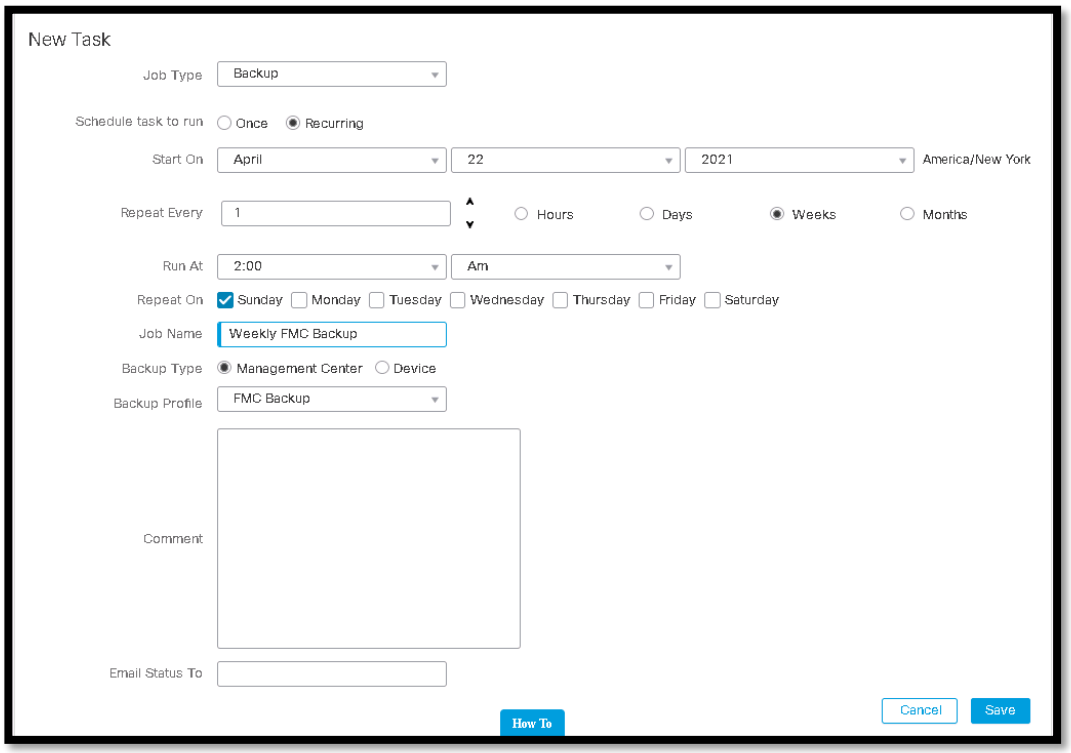
c. Back Up Events: Checked

d. Back Up Threat Intelligence Director: Checked

e. Click Save As New



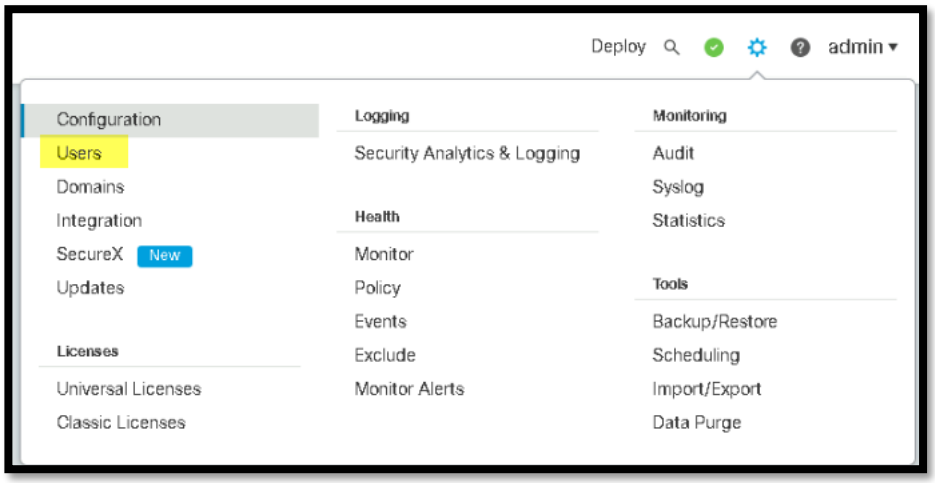

**Note:** You have created a backup profile but have not created a backup schedule. Below is a picture of a scheduled Backup.



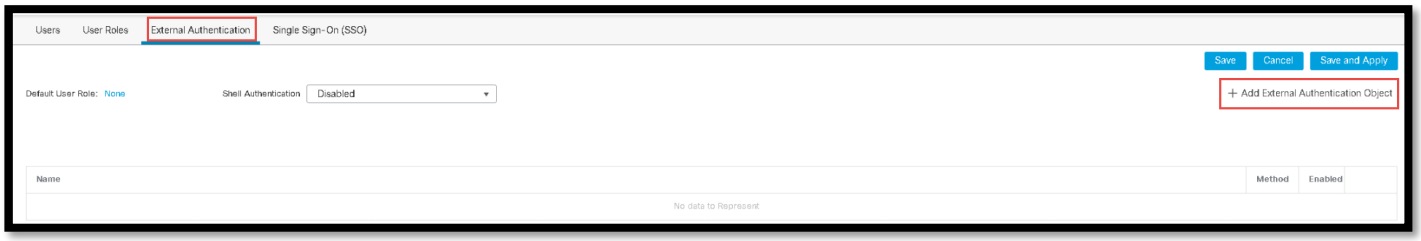
## Configure External Authentication

Your customer has requested that you configure the FMC to allow user accounts in their Active Directory instance to authenticate to the FMC. Specifically, any users in the IT group in AD should be logged int the FMC as an administrator. You will now configure the FMC to allow user accounts in the customer's Active Directory instance to authenticate to the FMC.

1. Click the **System** gear icon and select users




2. Select **External Authentication** and **Add External Authentication Object**




3. Use the following values to configure the External Authentication Object. If a value for a setting is not specified then leave the default value and do not modify it.

    a. Authentication Method: LDAP

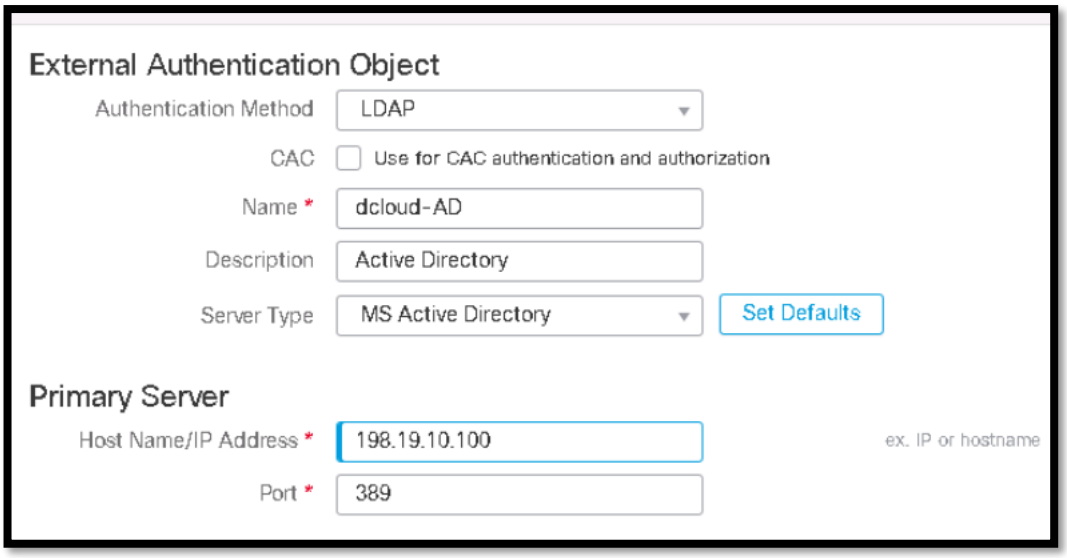
    b. Name: dcloud-AD

    c. Description: Active Directory

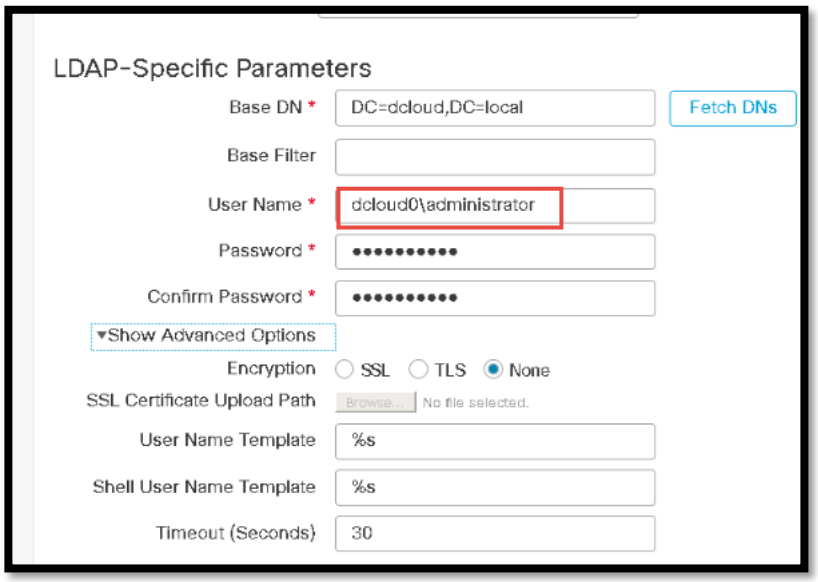
    d. Server type: MS Active Directory

    e. Primary Server: 198.19.10.100

    f. Port 389

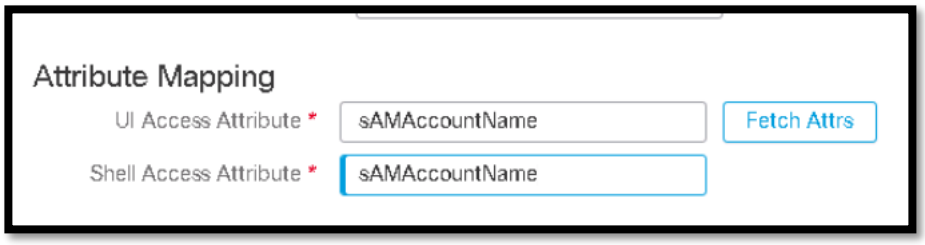



4. Click the Fetch DNs button and select DC=dcloud.DC=local as the Base DN
5. Enter the following
    a. Username: **dcloud0\administrator**
    b. Password: **C1sco12345**
    c. Confirm Password: **C1sco12345**
    d. Click **Show Advanced Options and check**

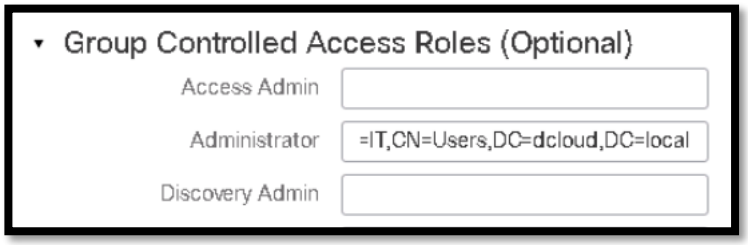



**NOTE:** In your customer environment a user account (service account) dedicated for the FMC to query Active Directory should be used instead of the actual "administrator" account. No special permissions are required in AD for the account to function correctly. Additionally, it is a best practice to use encryption (Secure LDAP runs on port 636) if the customer's domain controllers have a certificate installed so that username and passwords are not being sent clear text through the network.

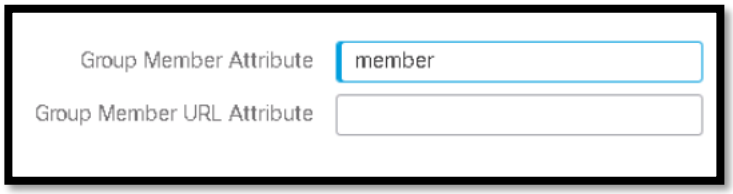
6. In the Attribute Mapping section click the **Fetch Attrs** button, and select **sAMAccountName** from the drop-down list
7. In the Shell Access Attribute field, enter **sAMAccountName** be aware of capitalization



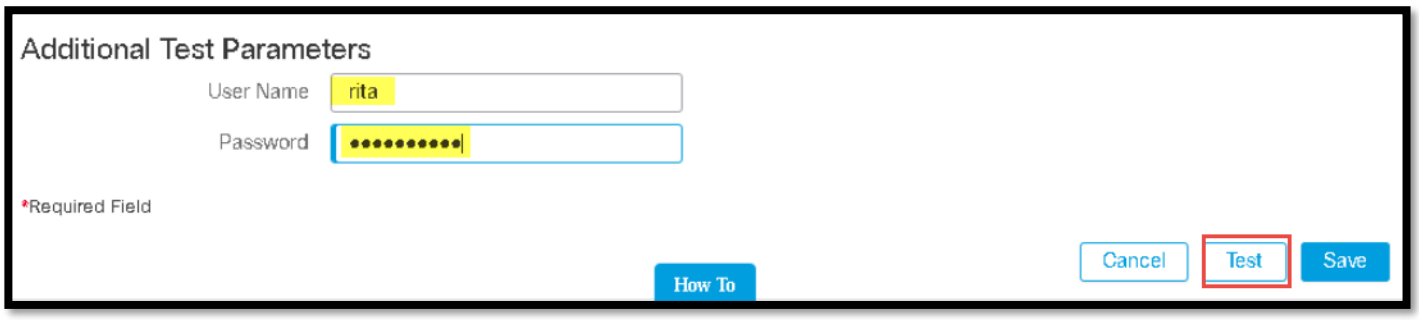

8. Expand the Group Controlled Access Roles
9. In the Administrator field enter the LDAP distinguished name of the IT group in Active Directory
    a. **CN=IT,CN=Users,DC=dcloud,DC=local**

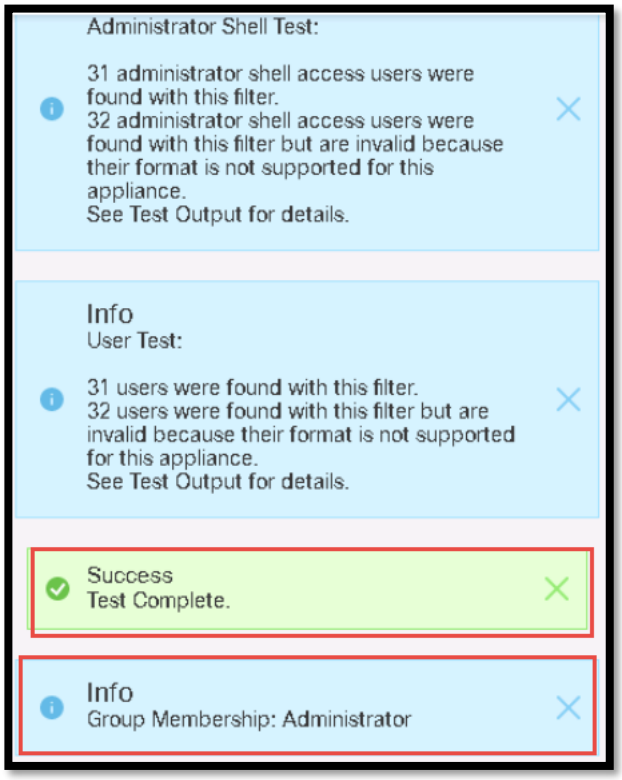



10. In **Group Member** Attribute field enter **member**




11. In **Shell Access Filter** click **Same as Base Filter**
12. In **Additional Test Parameters**
    a. Username: **rita**
    b. Password: **C1sco12345**
13. Click **Test**

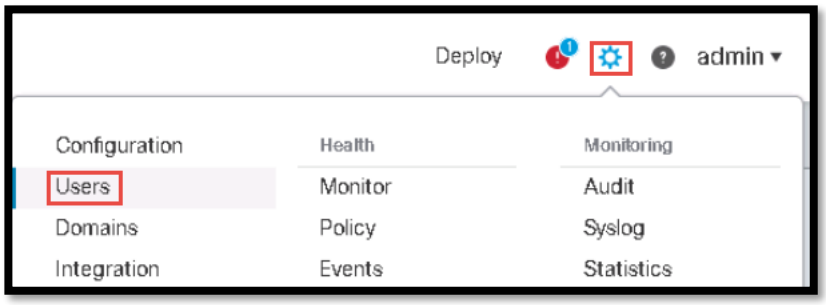





14. Click **Save**
15. Click the toggle setting under the Enabled column to change the setting from disabled (grey) to enabled (blue)

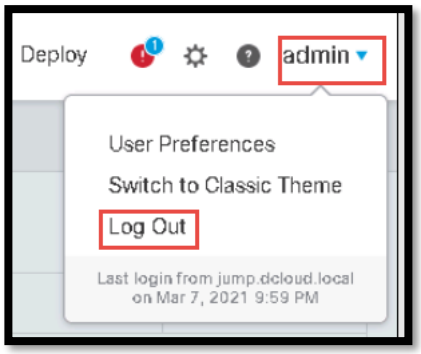

16. Click **Save and Apply**


17. For External Authentication Click **Apply Changes**
18. In the top right corner of FMC user interface click the System menu represented by the gear icon and select Users



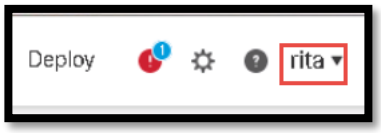

19. Look at the Users you will see admin and restapiuser


20. Click on Admin and then logout




21. Test the Active Directory Login
    a. Username: **rita**
    b. Password: **C1sco12345**


22. Check the login



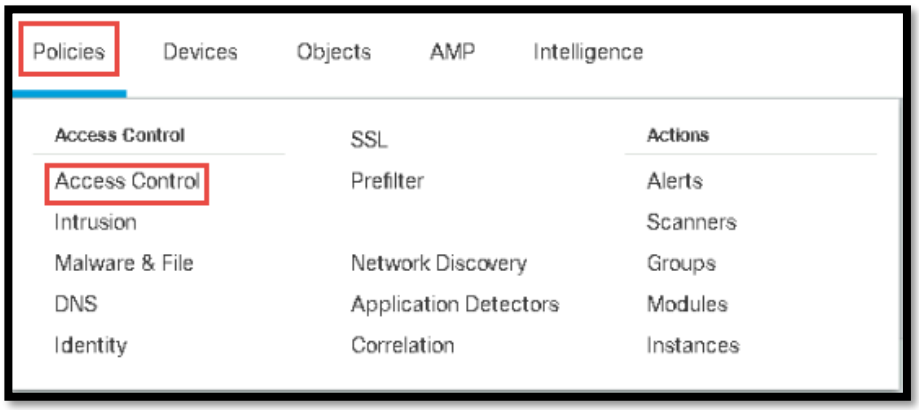

23. Click on the Gear Icon and select Users
24. Under Username you will now see **rita**


25. Log out and login as **Admin/C1sco12345**

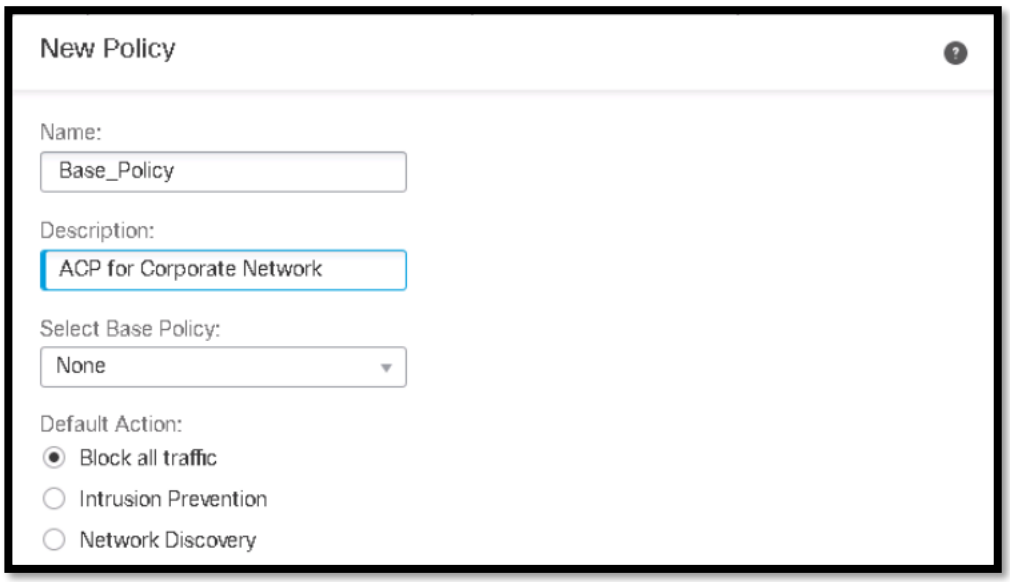
## Creating an Access Control Policy

When an FTD appliance is added to the FMC, an ACP (Access Control Policy) must be selected to be applied to the FTD. In order to prepare for the FTD appliance being added to the FMC you will now create an ACP.

1. Click the Policies menu and select Access Control From the Access Control section



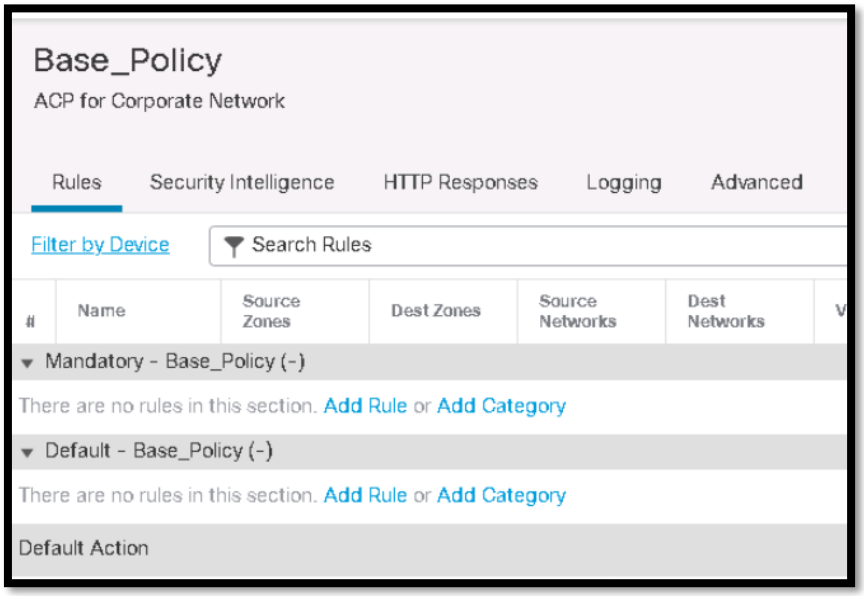

2. Click **New Policy**
3. Configure the policy
    a. Name: Base_Policy
    b. Description: ACP for Corporate Network




NOTE: The Default Action setting instructs the FTD what to do if no rule in the ACP matches the packet. The "Block all traffic" setting is a default deny rule that blocks any packet not matching a rule in the ACP and is a security best practice. The "Intrusion Prevention" setting runs the packet through the Snort IPS engine and if the packet is not blocked by the IPS engine then the packet is allowed to pass through the firewall. The "Network Discovery" setting performs network discovery on the packet and hosts involved then allows the packet through the firewall.

4. Click **Save**

The policy saves and you are taken to the screen to make changes to the ACP. You will not make any changes at this time to the ACP. You have created it to assist with adding the FTD appliance as you must choose an ACP to assign to the FTD when it is added to the FMC.



# Scenario 2. Basic Configuration

This exercise consists of the following tasks:

- Create objects needed for the exercise
- Modify the access control policy
- Create NAT policies
- Configure Branch1 FTD Using FMC
- Remote Deployment of Branch1 FTD
- Configure FTD Using FDM
- Deploy the Configuration changes
- Modify the network discovery policy
- Deploy the configuration changes

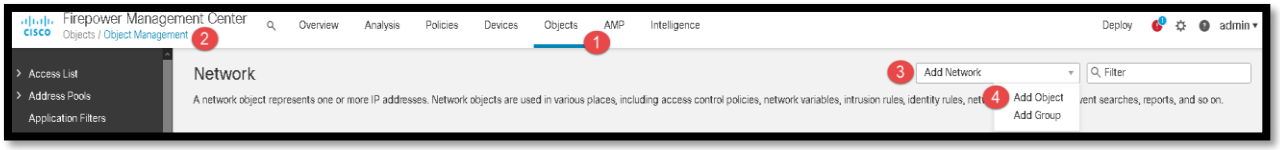
The objective of this exercise is to deploy a simple, but effective, NGFW configuration:

- Allow outbound connections, and block other connection attempts
- Perform file type and malware blocking on these outbound connections
- Provide intrusion prevention on these outbound connections

## Steps

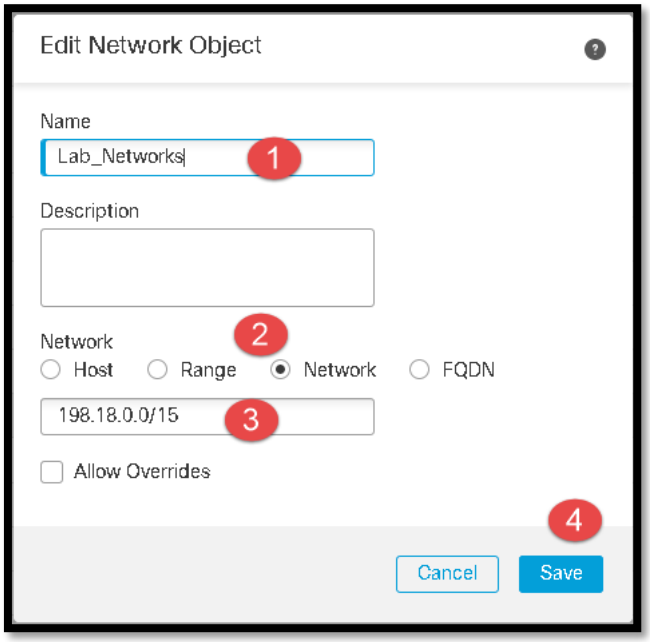
### Create objects needed for the exercise

1. On the FMC**,** select **Objects > Object Management.**
2. Click **Add Network** > **Add Object**.




a. For Name, enter Lab_Networks.

b. Enter 198.18.0.0/15. This includes all IP addresses used in the lab pod.




c. Click Network

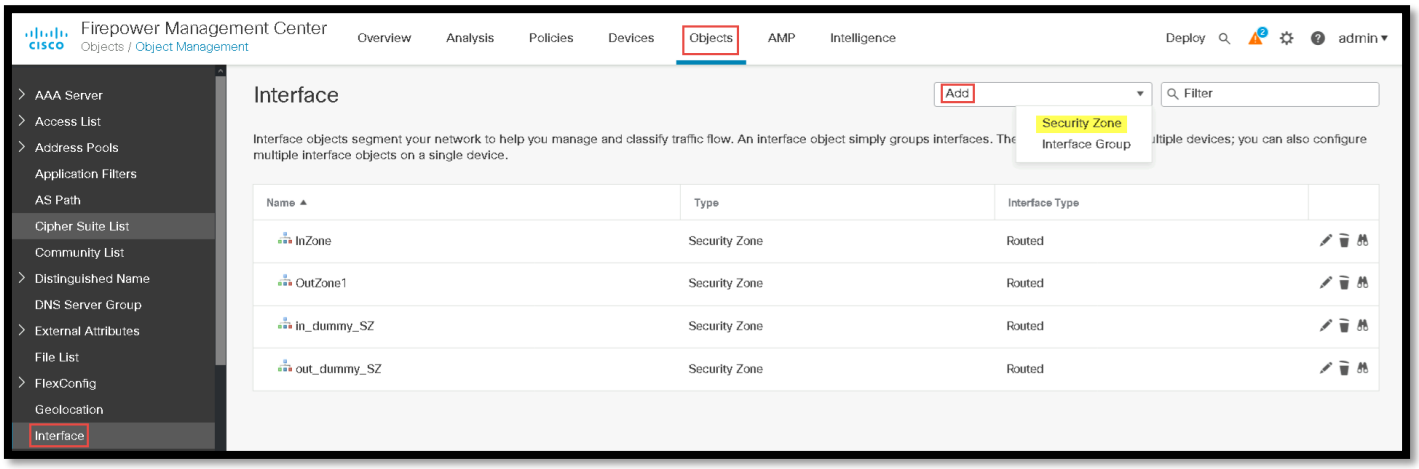
d. Click **Save**.

Select **Interface** from the left navigation panel.

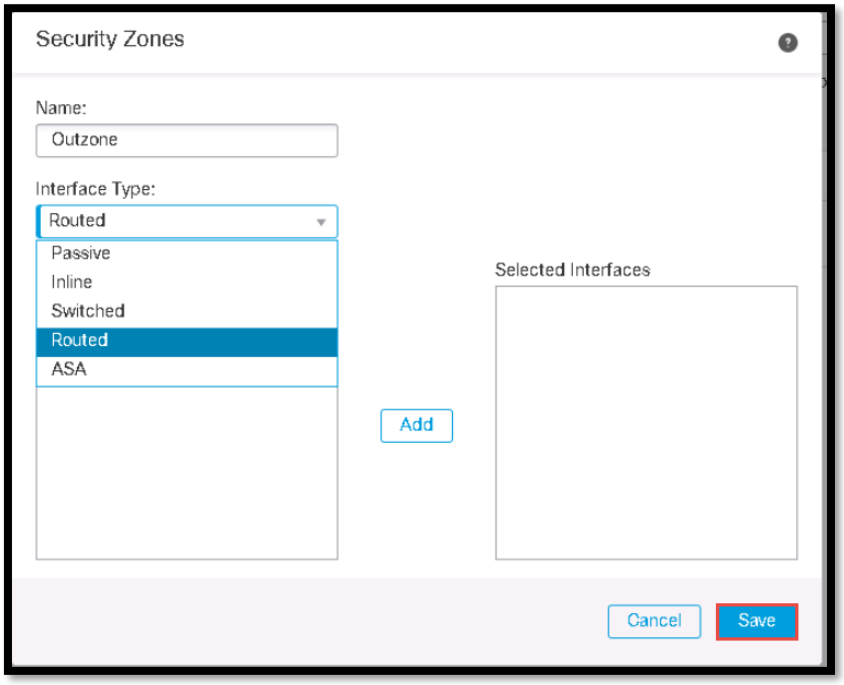
e. Click **Add > Security Zone**.

**NOTE:** There are two types of interface objects: security zones and interface groups. The key difference is that interface groups can overlap. Only security zones can be used in access control policy rules.

Create the Network Objects for the Security Zones that will be added to the interfaces.




**Name**: **OutZone** Select **Routed** from the **Interface Type** drop-down menu and click **Save**



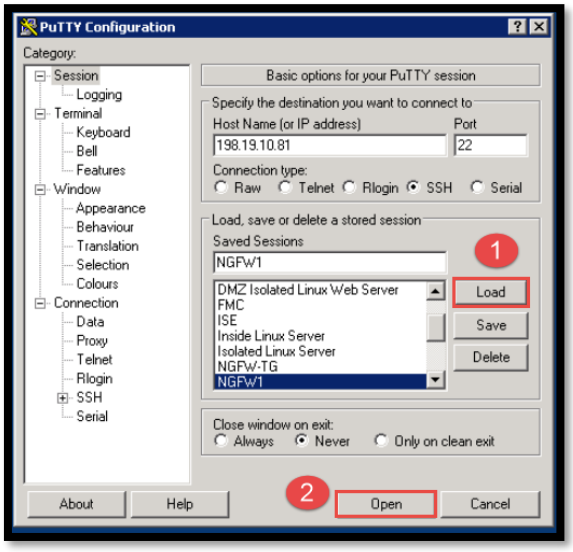

Create another Security Zone named **InZone1**.

f. Name: **InZone1** Select **Routed** from the Interface Type drop-down menu click **Save**

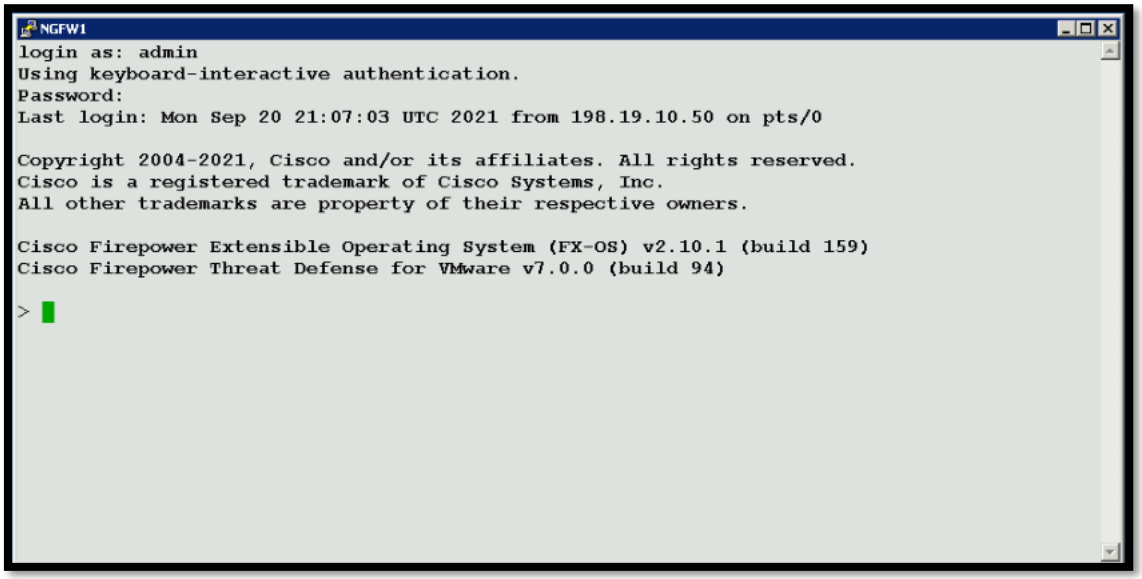
g. Create Security Zone named **InZone2, InZone3, InZone4**

## Configure the FTD

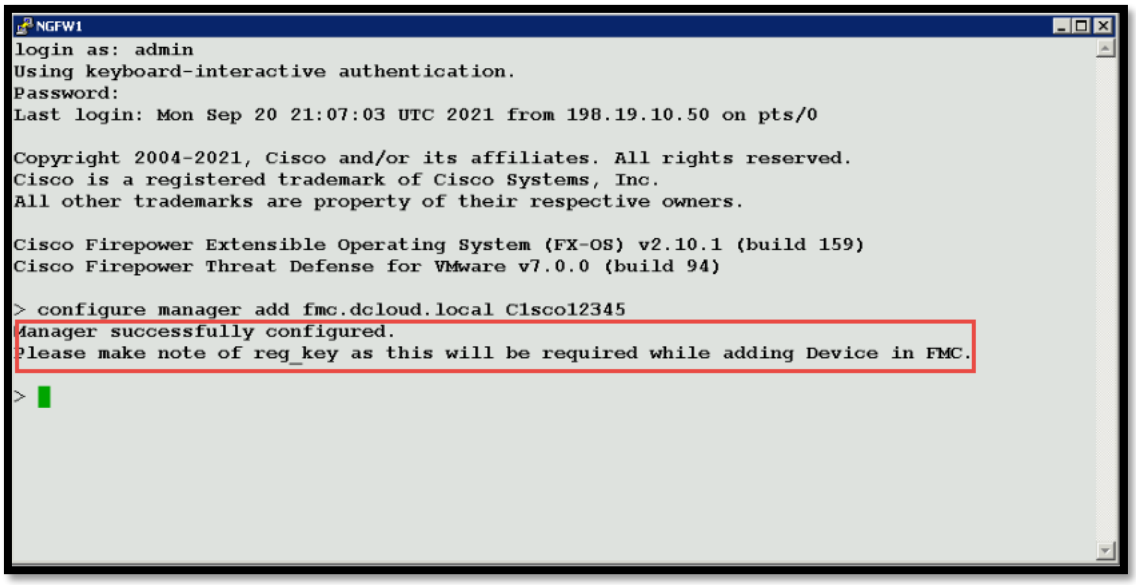
3. On the Jumpbox click on the Putty Icon and select NGFW1 click **Load** and **Open**




4. Type Login: **admin** password: **C1sco12345**

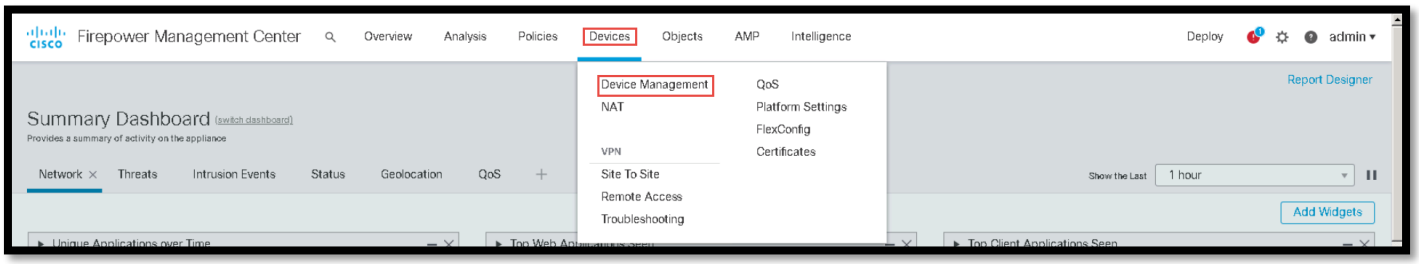



5. Type: **configure manager add fmc.dcloud.local C1sco12345 and wait for the response**

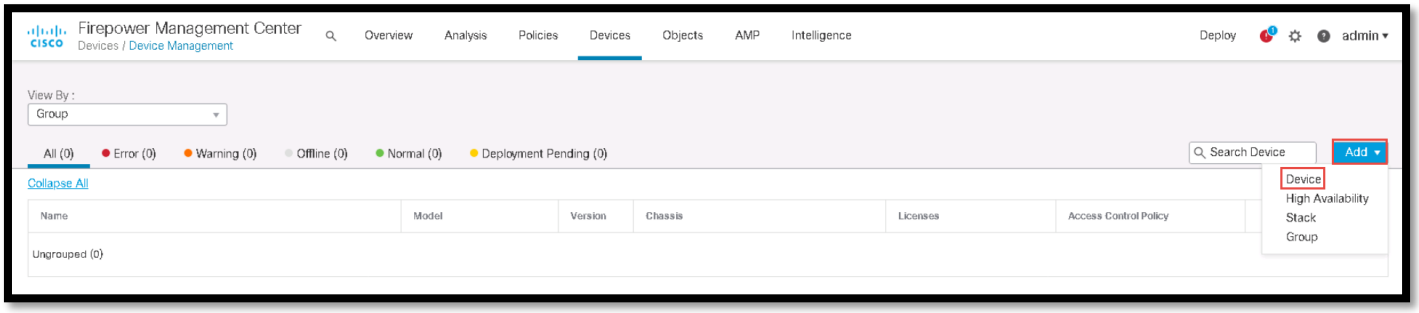



6. Login into the FMC **admin/C1sco12345**

7. Click on Devices > Device Management




8. Select Add and Device




9. Configure the following:

   a. Host: 198.19.10.81

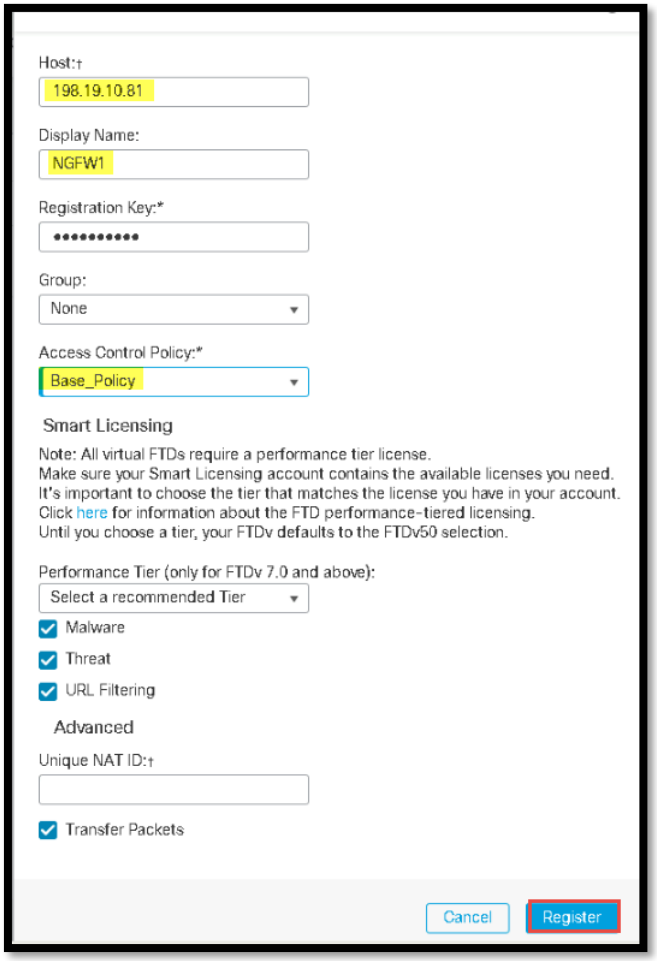
   b. Display Name: NGFW1

   c. Registration Key: C1sco12345

   d. Group: None

   e. Access Control Policy: Base_Policy

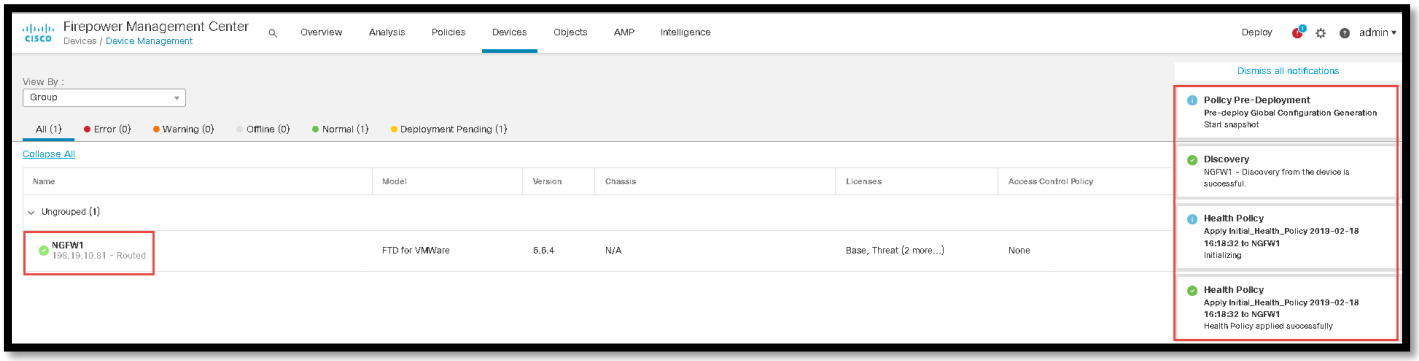
   f. Smart Licensing: Select All



**Note:** The IP Address 198.19.10.81 is the Management Interface address that terminates the SF Tunnel. It was pre-configured due to the limitations in the dCloud lab. In a customer environment you would configure the management address through the wizard.

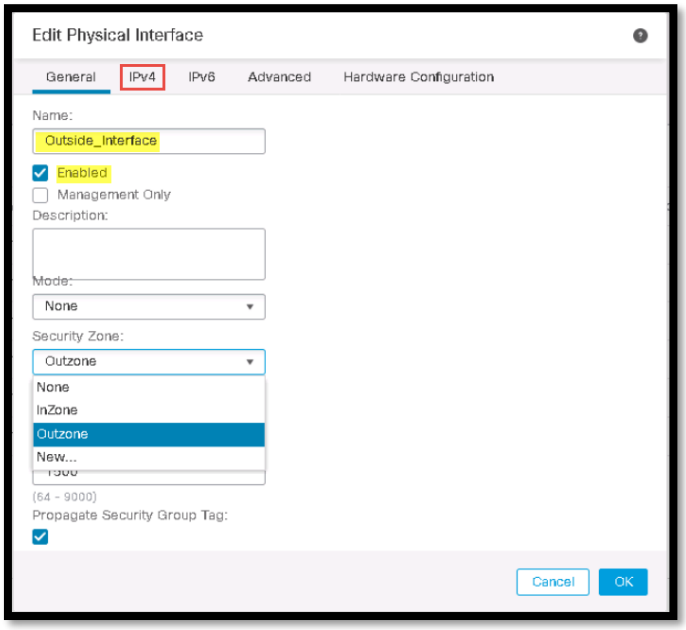
10. Click **Register**

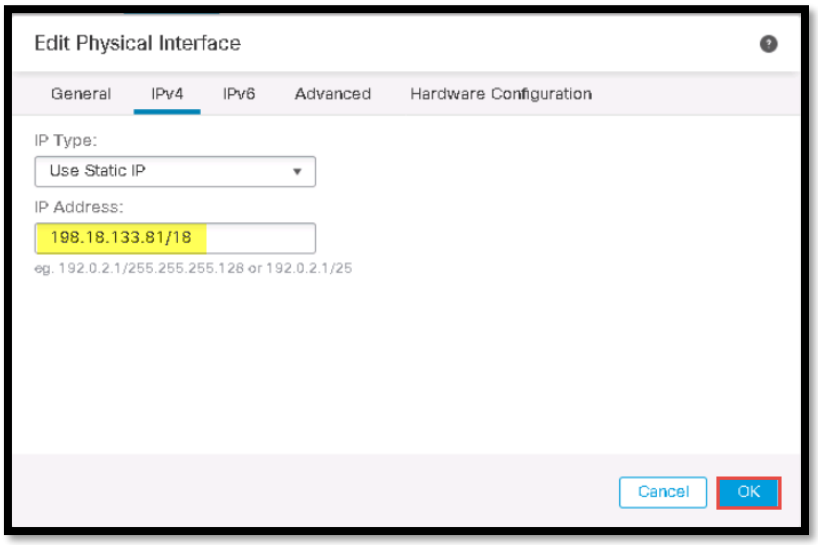
You will see the following during registration




11. Once NGFW has registered click on the Pencil icon to edit


12. Configuring the Interfaces. Click on the Pencil Icon on the **GigabitEthernet0/0** Line
    a. Name: **Outside or Outside_Interface**
    b. Enabled: **Checked**
    c. Security Zone: **OutZone**
    d. Click IPv4 Tab IP Address: **198.18.133.81 255.255.192.0** or **198.18.133.81/18**
    e. Click: **OK**




13. Configure **GigabitEthernet0/1** with the following values:
    a. Name: in10
    b. Enable: **Checked**
    c. Security Zone: **InZone1**
    d. IPv4: **198.19.10.1/24**
    e. Click **OK**
14. Configure GigabitEthernet02-04 as follows:
    a. GigabitEthernet0/2
        i. Name: in20
        ii. Security Zone: InZone2

iii. I P Address 198.19.20.1/24

b. GigabitEthernet0/3

i. Name in30

ii. Security Zone InZone3

iii. IP Address 198.19.30.1/24

c. GigabitEthernet0/4

i. Name in40

ii. Security Zone InZone4

iii. IP Address 198.19.40.1/24

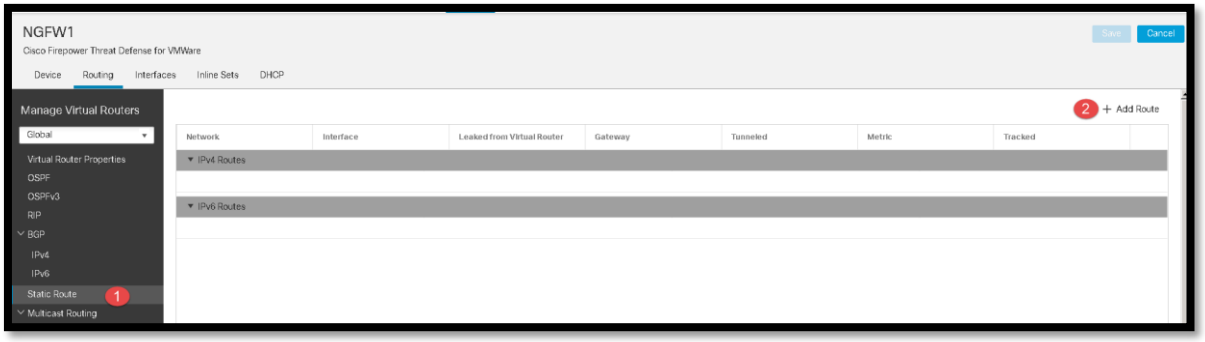
15. Click **Save**

## Configure the default route

1. If currently not on the page in the FMC, select **Devices > Device Management**. Click on the **pencil** icon to edit the NGFW1 device settings.

The Interfaces tab should be selected. Confirm that the interfaces of **NGFW1** have Security Zones configured

Select **Routing > Static Route** and click the **Add Route** button.




Select **Outside_Interface** in the Interface field.

Select **any-ipv4** from available networks (This is the equivalent of a default route).

Click **Add.**

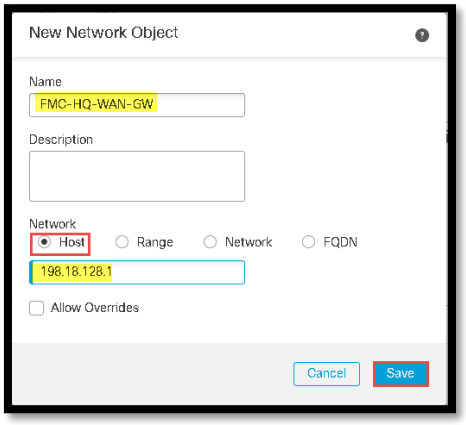
For Gateway click on the "**+**" icon to create a new object.

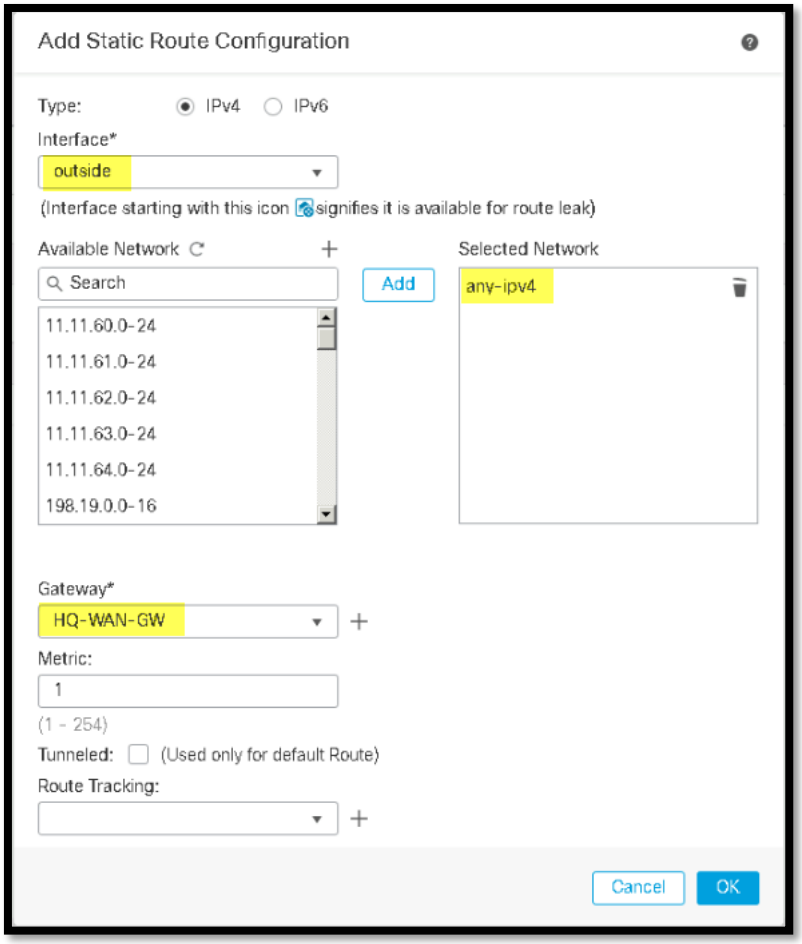
a. Select the "**+**" sign next to the Gateway* pull down menu.

b. Name the Object "**HQ-WAN-GW** (You will be able to reuse this object later).

c. Enter the Network IP Address: **198.18.128.1** (This is the outside interface of the Firewall facing the WAN).

d. Click **Save.**




Click **OK** to add the Static Route Configuration.

Add another static route to the **11.11.60.0 Network** with a Gateway: **198.18.133.60**

Interface:  Outside_Interface

Available Networks select

Network: 11.11.60.0/24


Click **Add**

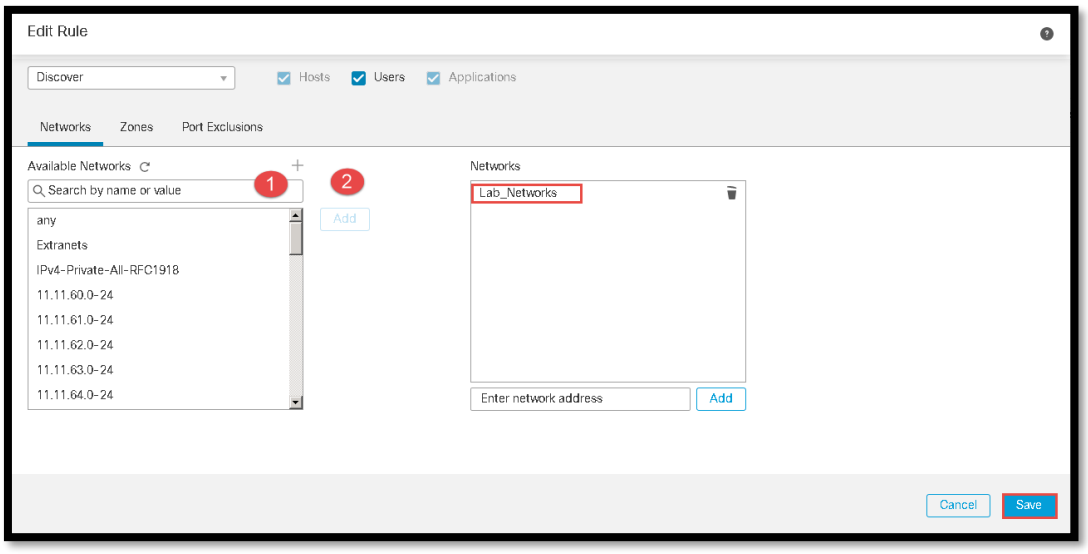
Click **Save.**

## Modify Network Discovery Policy

The default network discovery policy is configured to discover all applications, both internal and external. We will want to add host and user discovery. In a production environment, this can exceed the FMC Firepower host license. For this reason, it is best practice to modify the policy.

1. From the menu, select **Policies > Network Discovery.**
    a. Click the **pencil icon** to the right to edit the existing rule.
    b. Check the **Users** checkbox. The Hosts checkbox will auto-check.
    c. Delete both **0.0.0.0/0** and **::/0**.

Select **Lab_Networks** click **Add** and **Save**




Add and Excluded Network

    a. Click Add Rule
    b. Click **Exclude**
    c. Under the Networks Box

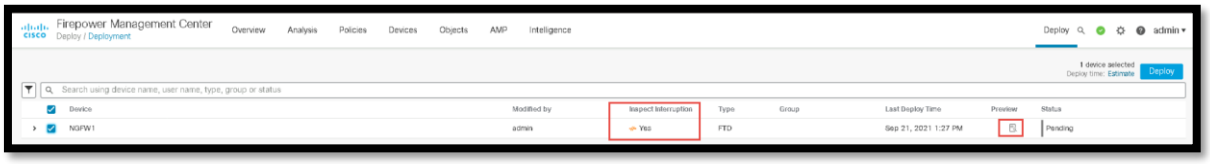
i. Type 11.11.60.0 **Add**

ii. This will add a network that is excluded from **Network Discovery**

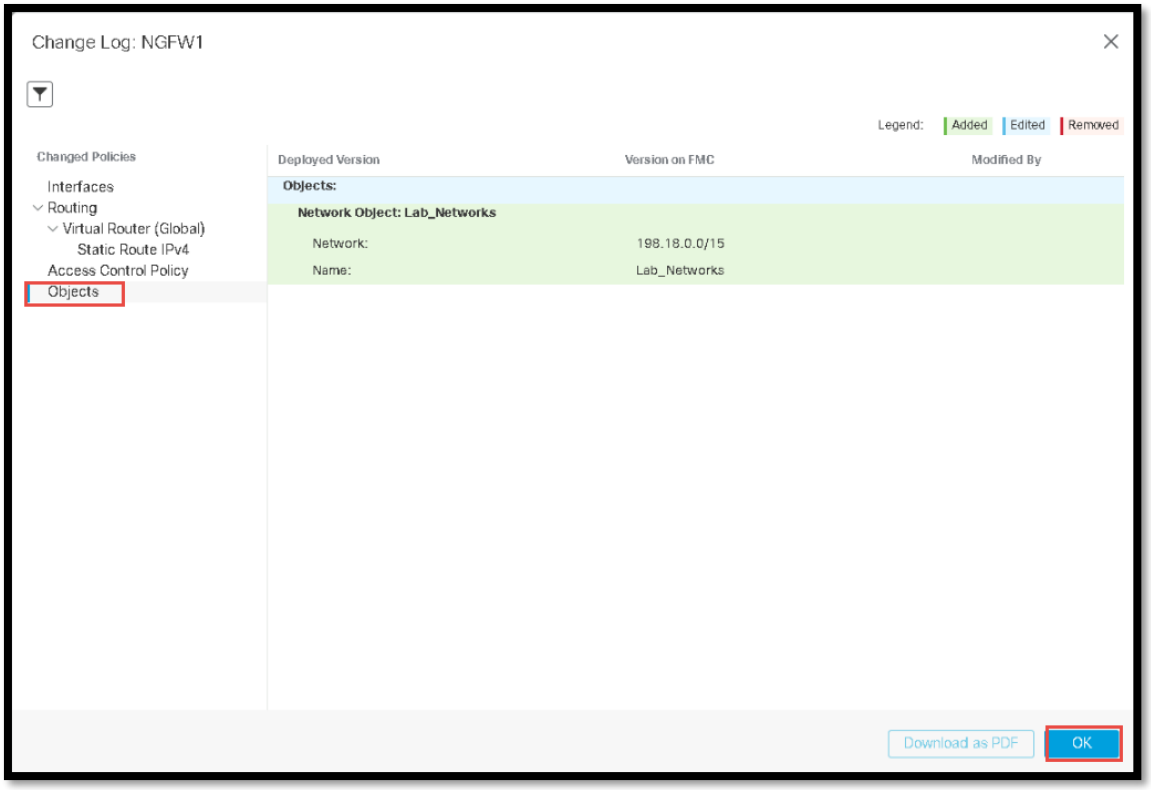
Click **Save**.

Click **Deploy** in the upper right-hand corner of the FMC.

a. Check the box for the NGFW(s) device and expand the list to see the details. The page should look similar to the following picture. As of version 6.2.3 you will be alerted if there is a SNORT interruption. In addition, you will see what will cause the interruption. If you wish to deploy later, you can click the cancel button.

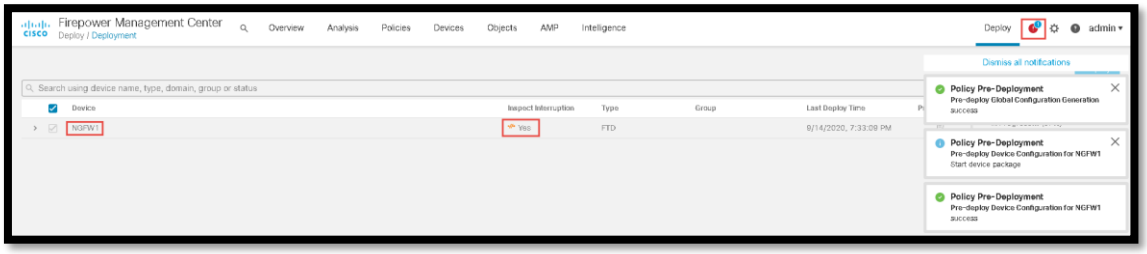


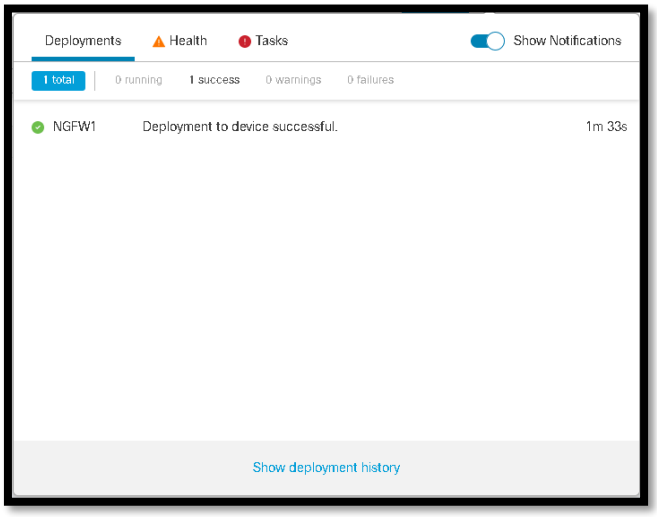

Click Preview to confirm that **NGFW settings**, interface and static route configuration will be modified.




b. Click **Deploy**.

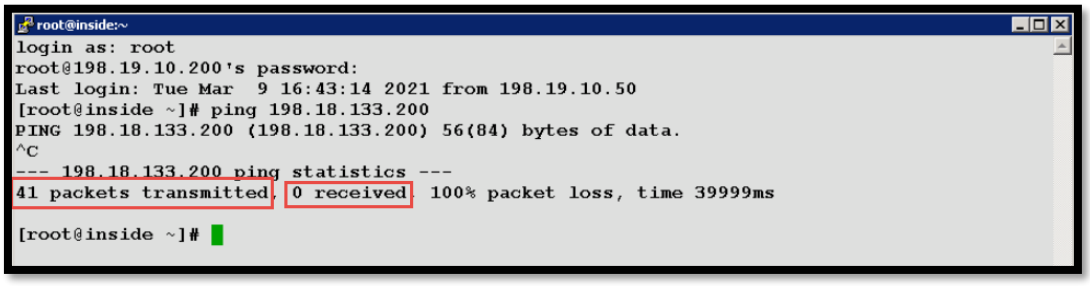
c. Click the icon to the right of the Deploy link in the upper right-hand corner of the FMC. Wait until the deployment is complete.



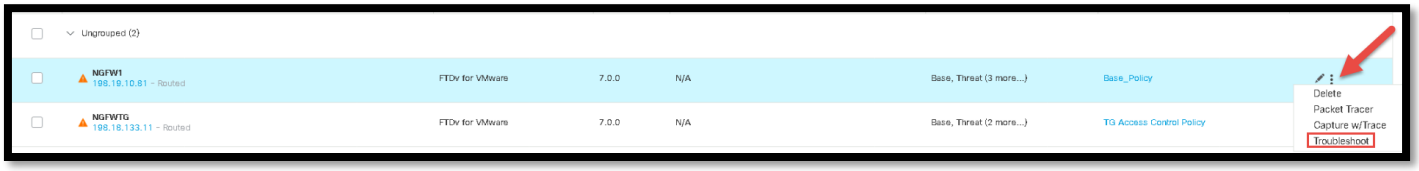

## Testing Network Connectivity

1. Open a Putty session to the **Inside Linux Server root/C1sco12345**
    a. Type **ping 198.18.133.200**
        i. You will see that Ping is not working

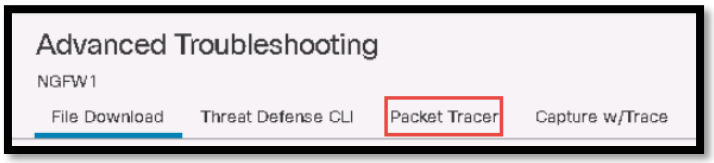



2. Troubleshooting Click on **Devices Device Management**

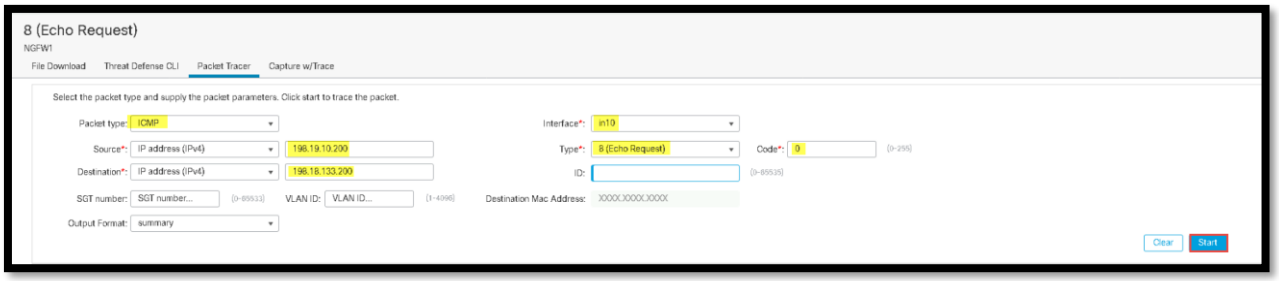

3. Click the Troubleshoot Icon for NGFW1




4. Click on the View System & Troubleshoot Details
5. Select Advanced Troubleshooting
6. Select **Packet Tracer**




7. Configure the following:
    a. Packet type: **ICMP**
    b. Source: **198.19.10.200**
    c. Destination: **198.18.133.200**
    d. Interface: in10
    e. Type: **8 (Echo Request)**
    f. Code: **0**

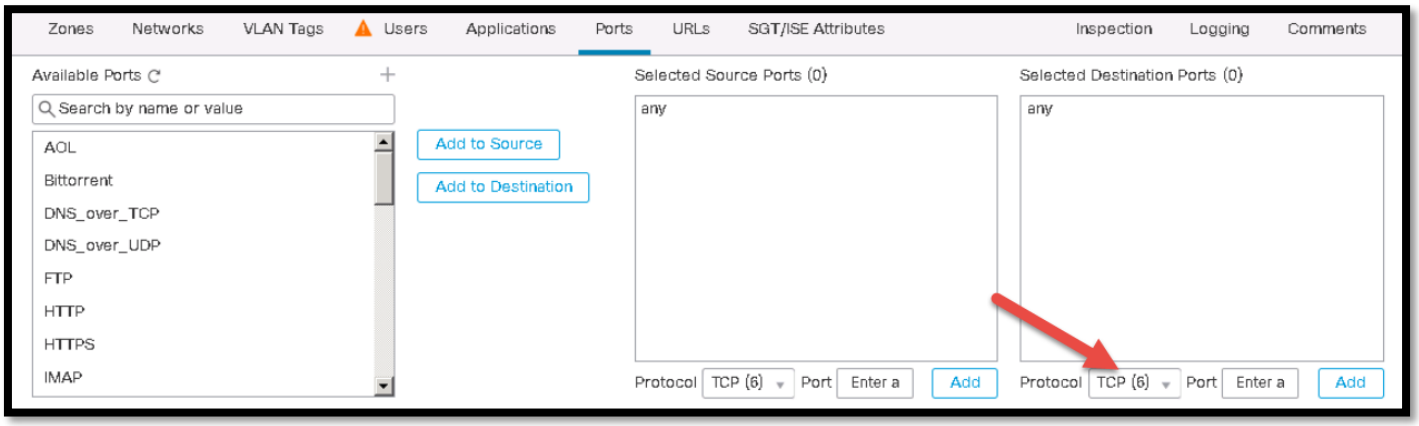



**NOTE:** For the “Type” field, you may need to place the cursor in the field and hit the down arrow key on the keyboard to populate the drop-down menu with all the choices so you can select 8. Also, the “Code” field is immediately to the right of the “Type” field but may not display clearly. Be sure to populate the Code field with a 0 as it is a required field to run a packet trace for ICMP.

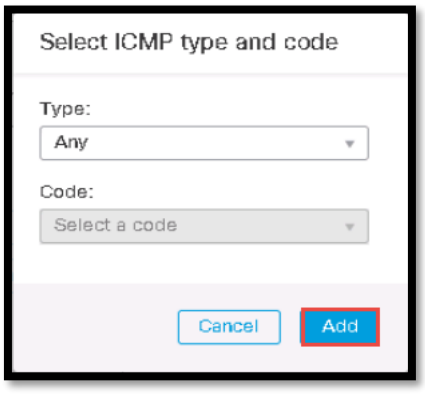
8. Click **Start**
9. Look at the **Output Phase 3 ACCEST-LIST**
    a. Result: **DROP**
        i. Packet was dropped by **DEFAULT ACTION RULE** which means it didn’t match any rules such as **ALLOW**

## Modify Access Control Policy

1. Click on **Policies > Access Control**
2. Double-click on **Base_Policy** or Click the **Pencil Icon** to edit the policy
    a. Note that the only rule configured is the **Default Action Block All Traffic**
3. Click **Add Rule**
    a. Name: **Allow ICMP**
    b. Action: **Allow**
    c. Insert: **into Default**
    d. Zones:
        i. Source: All **InZones (InZone1, InZone2, InZone3, InZone4)**
        ii. Destination: All **InZones and Outzone**
    e. Networks: **Leave any any for now**
    f. Ports under Selected Destination Ports Click on Protocol click on **ICMP**




    g. When box come up Type: **Any** and **Add**




    h. Click **Add** and **Save**

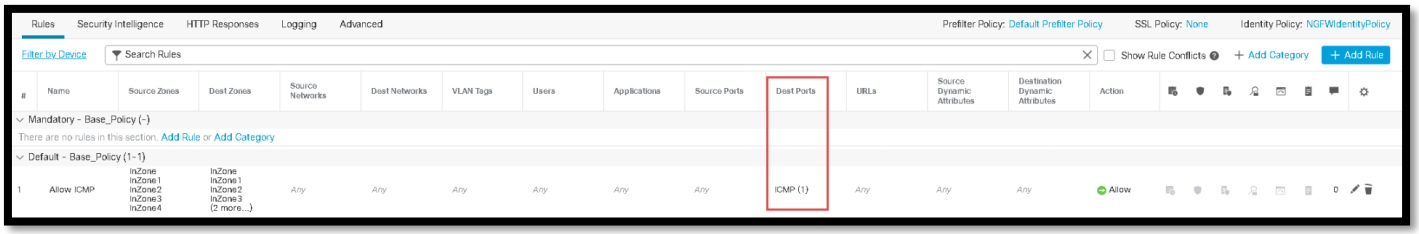
**NOTE:** Rules are divided into sets within a policy. Two sets are predefined:

**Mandatory rules**, which take precedent over rules of child policies

**Default rules**, which are evaluated after the rules of child policies.

In this exercise, you will not create a child policy, but you will use the default rule set as a convenient way of making sure this rule is evaluated last.

4. Your ACP should Look as follows:



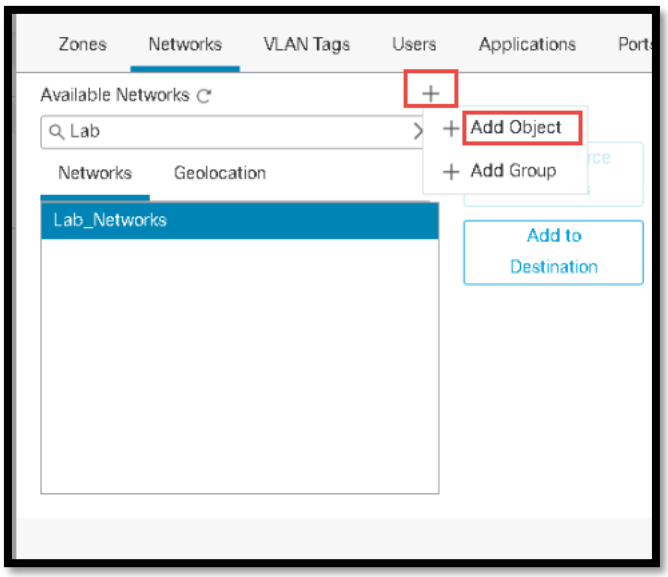

5. Create a Rule that allows for Outbound Connectivity

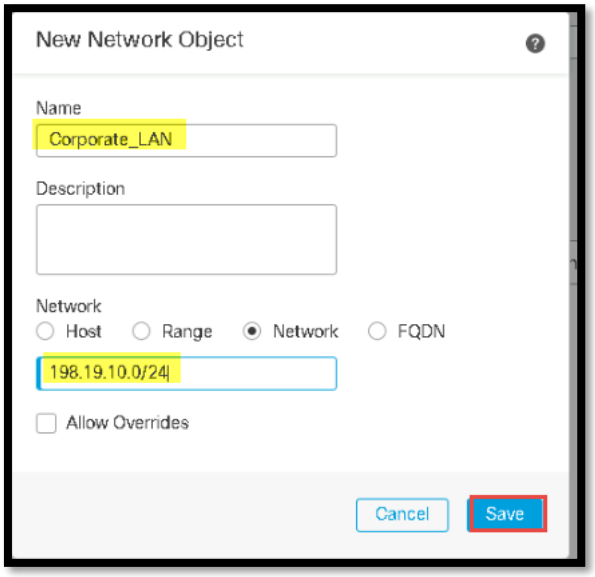
   a. Name: **Allow Outbound**

   b. Zone: **All InZones to OutZone**

   c. Source Networks: **Lab_Networks**

   d. Source Create **Corporate_LAN** (198.19.10.0/24)





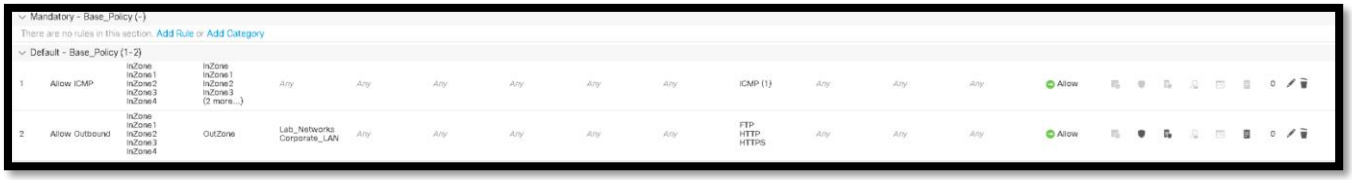

e. Ports add to Destination: **HTTP/S, & FTP**

f. Inspection: **Demo Intrusion Policy and Demo File Policy (read the note about Snort 2 and Snort 3)**

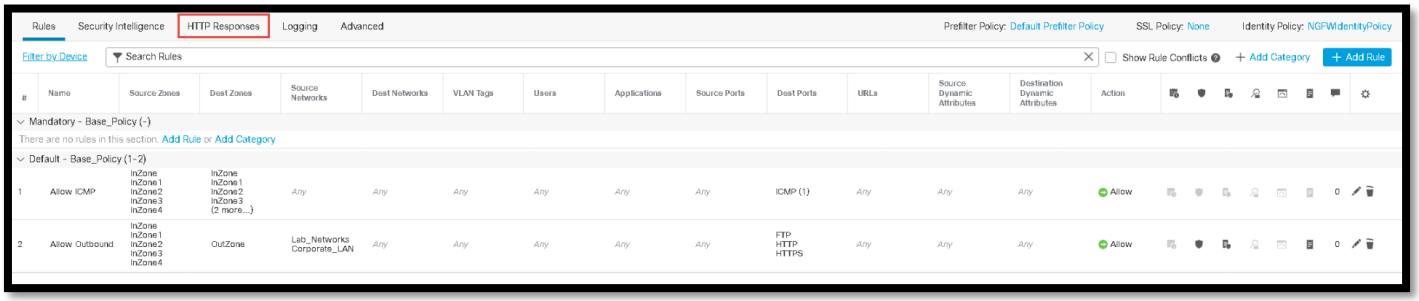
g. Logging: **End of the Connection**

h. Click **Add**

**NOTE**: The demo intrusion and file policies were pre-configured to save you time. See Appendix 1 in the Firepower Advanced Lab Guide v2.7 for instructions on how to create these.

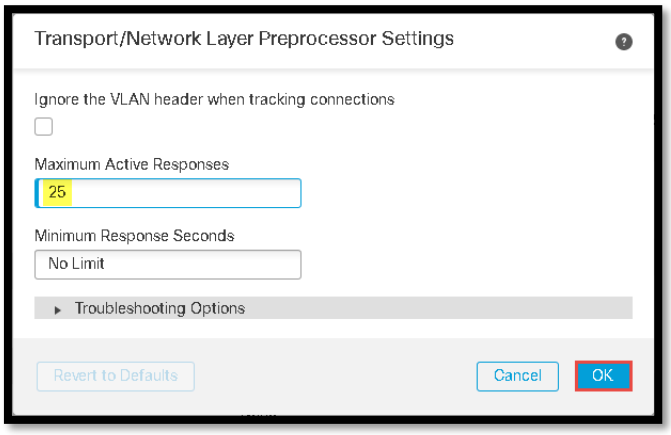


6. Select the HTTP Responses tab.




7. Select **System-provided** from the Block Response Page drop-down list.
8. Select the **Advanced** tab.

a. Click the **pencil** icon to edit the **Transport/Network Layer Preprocessor Settings**.
   i. In the Maximum Active Responses text field, enter **25**
   ii. Click **OK**.




**NOTE:** Setting Maximum Active Responses to a value greater than 0 enables the Intrusion Policy drop (IPS) rules that drop packets to send TCP resets to close the connection. Connections that do not trigger an IPS drop will be reset by the FTD if "block with reset" is applied to the rule regardless of the settings of Maximum Active Responses or if it is a LINA-only drop such as a Fastpath block. Typically, both the client and server are sent TCP resets. With the configuration above, the system can initiate up to 25 active responses (TCP Resets) if it sees additional traffic from this connection.

In a production deployment, it is probably best to leave this set to the default. Then no resets are sent, and the malicious system will not know that it has been detected. But for testing and demonstrations, it is generally better to send resets when packets match drop rules.

9. Click **Save** to save the changes to the access control policy.

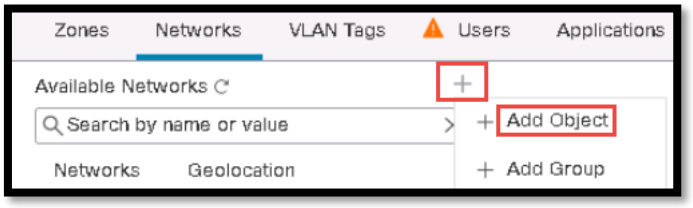
10. Create a Rule allow Outbound DNS

    a. Name: **Allow Approved DNS outbound**

    b. Zones: **All InZones to OutZone**

    c. Networks

       i. Click [+] on the Available Networks Add Object




1. Name: **host-ad1**
2. Description: **Active Directory and DNS server**
3. Network: Host: **198.19.10.100**

4. **Save**

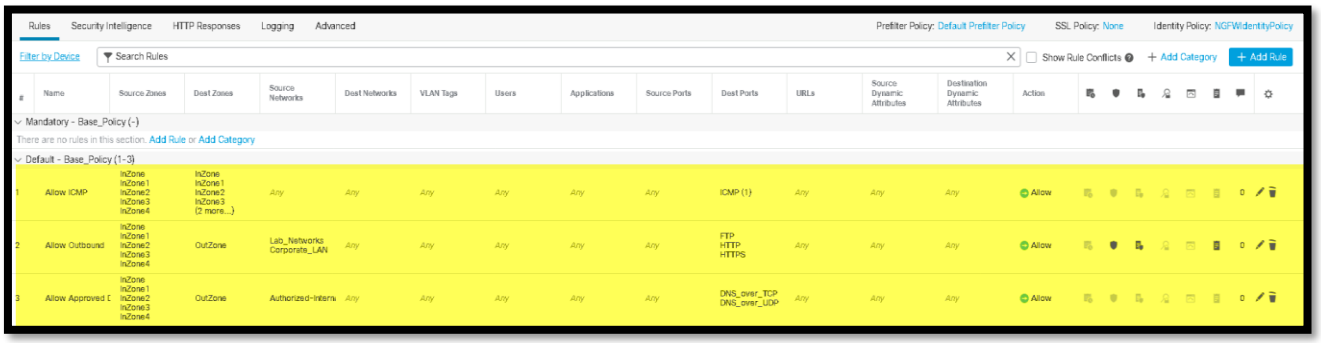
ii. Click [+] on the Available Networks Add Group

1. Name: **Authorized-Internal-DNS-Servers**
2. Description: **Internal DNS servers that are authorized to query external DNS**
3. Network Objects: **host-ad1** and **Add**
4. **Save**

iii. Available Networks select **Authorized-Internal-DNS-Servers add to Source**

iv. Click Ports tab, select **DNS_over_TCP** and **DNS_over_UDP** ports then click **Add to Destination**

v. Click **Add**

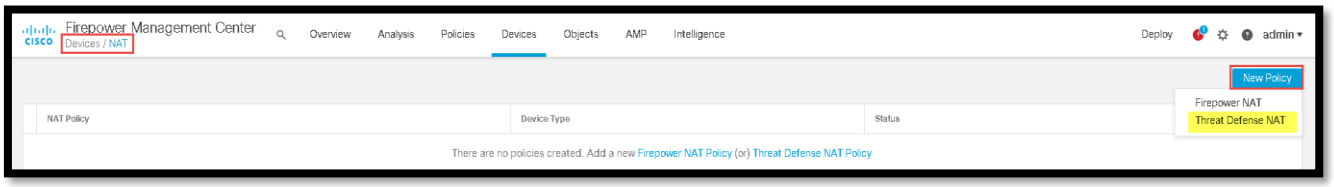



vi. Click **Save**

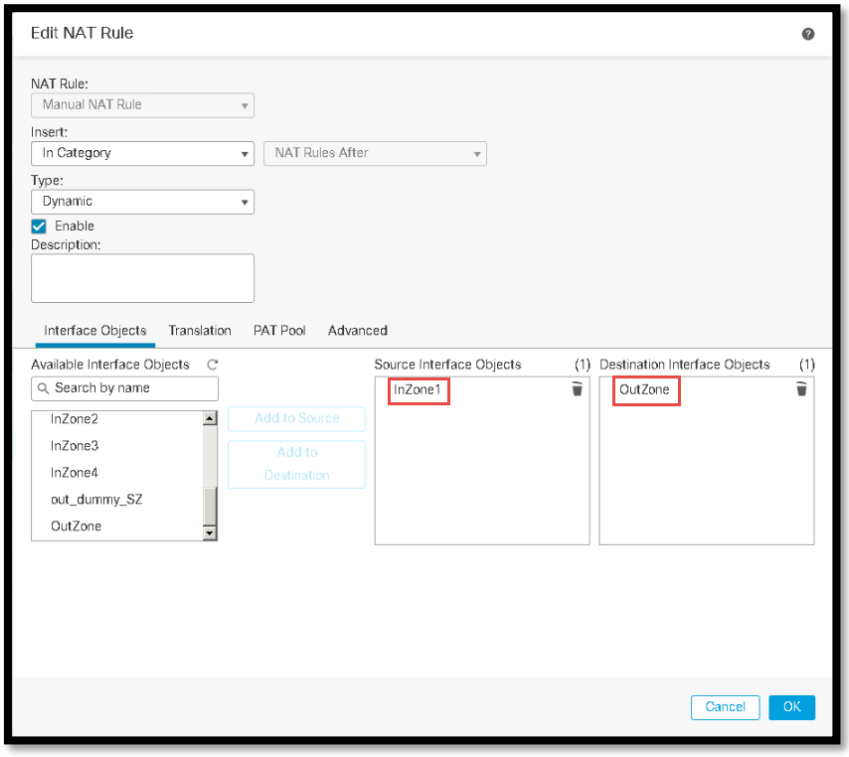
## Create NAT Policy

2. From the menu, select **Devices > NAT**.

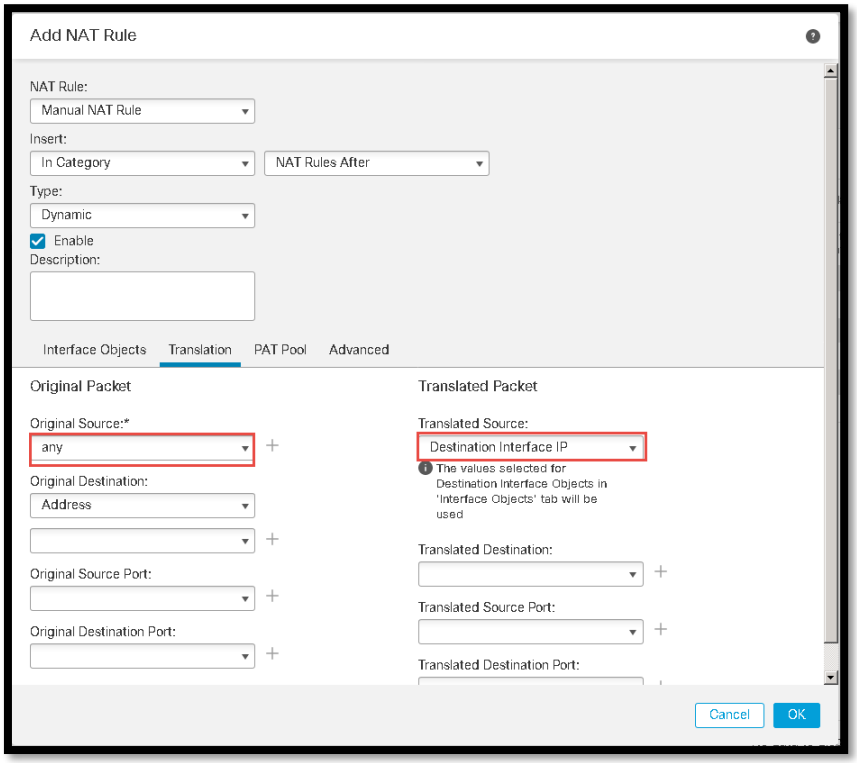
Click the New Policy button**,** and select **Threat Defense NAT.**




2. For Name, enter **Default PAT**.
3. Select the **NGFW(s)**. Click **Add to Policy** and then click **Save**.
   a. Wait for the policy to open for editing.
4. Click Add Rule.
5. Select **In Category** and **NAT Rules After** from the Insert drop-down lists.
   a. This will ensure that this rule will be evaluated after the auto-NAT (object NAT) rules.




6. Select **Dynamic** from the **Type** drop-down list.
    a. You will be at the **Interface Objects** tab.
        i. Select **InZone1** and click **Add to Source**.
        ii. Select **OutZone** and click **Add to Destination**.
7. Select the **Translation** tab.
    a. Select **Corporate_LAN** from the Original Source drop-down list**.**
    b. Select **Destination Interface IP** from the Translated Source drop-down list.
    c. Click **OK** to save the NAT rule.
8. Create NAT rules for the following:
    a. InZone2, InZone3, InZone4 as Source
    b. Outzone as the Destination
    c. Original Source **Any**
    d. Translated Source **Destination Interface IP**
9. Click **Save** to the NAT Policy.



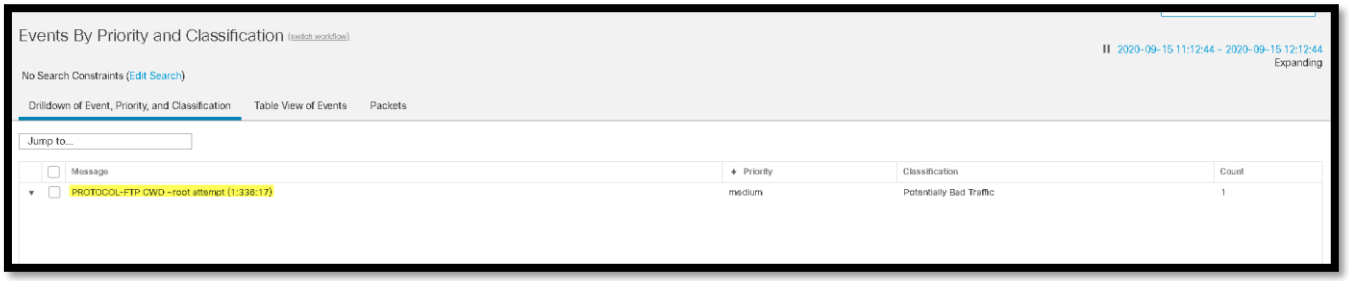

## Deploy the Changes and Test

1. Deploy the Changes to NGFW1 (Ignore the Warnings they relate to the fact that InZone is not currently defined to an Interface)
2. Test Connection from the **Inside Linux Server**
    a. If your session is not open use Putty Login **root/C1sco12345**
        i. Type **ping Outside** (198.18.133.200) **Should Succeed this confirms the ICMP**
        ii. Type **wget cisco.com Should Succeed this confirms NAT and Routing**
        iii. Type **wget outside Should Succeed**
        iv. Type **ftp outside** Login as **guest,** password **C1sco12345**
            1. Enter **cd ~root**. You should see the following message: `421 Service not available, remote server has closed connection.` This confirms that IPS is working.

**NOTE:** If the FTP session hangs, you probably forgot to enable active responses in the access control policy. You need not fix this, as long as you remember to expect this behavior.

            2. Type **quit** to exit FTP.
2. In the FMC, select **Analysis > Intrusions > Events.**

**NOTE:** Observe that **Snort rule 336 was triggered**. In the Demo Intrusion Policy, the rule state for this rule is set to Drop and Generate Events. This rule is disabled in the system-defined intrusion policies such as Balanced Security and Connectivity.




**NOTE:** In a production environment, if you run into a situation where events are not appearing, the first thing you should check is the time synchronization between the NGFW and FMC. However, in this lab, it is more likely to be an issue with the eventing processes. If this happens, try restarting these processes as follows.

On the NGFW CLI run the following command.

pmtool restartbytype EventProcessor

From the Jumper desktop, connect to the **FMC** using the pre-defined PuTTY session. Login as **admin/C1sco12345** and run the following commands.

```
sudo pmtool restartbyid SFDataCorrelator
```

```
sudo pmtool restartbyid sftunnel
```

**NOTE:** The sudo password is **C1sco12345**

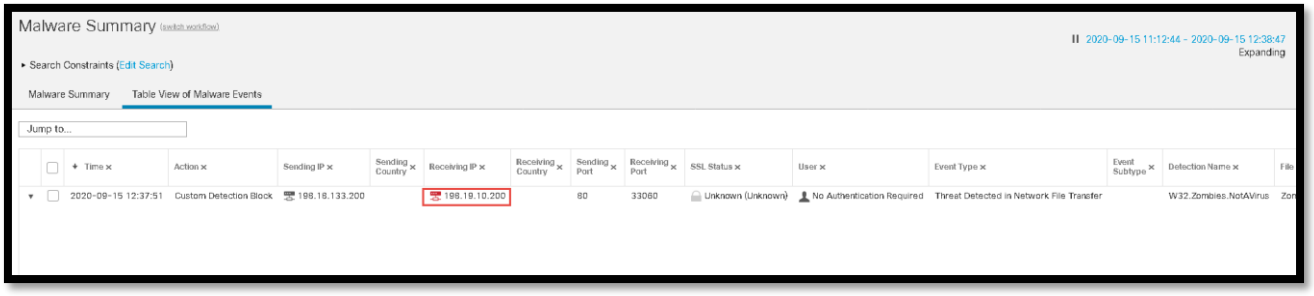
3. **Click the arrow** on the left to drill down to the table view of the events. Observe that details of the event are presented.
    a. **Click the arrow** on the left of the event to drill down further. Note that you are presented with extensive information, including the details of the Snort rule.
    b. **Expand the Actions** and note that you could disable the rule from here - but do not!
4. Test the file and malware blocking capabilities. These Wget commands can be cut and pasted from the file on the Jump desktop called Strings in order to cut and paste the text.
5. From the **Inside Linux Server** Login root/C1sco12345
    a. As a control test, use WGET to download a file that is not blocked. **wget -t 1 outside/files/ProjectX.pdf. This should succeed**.
    b. Next use WGET to attempt to download the file blocked by type: **wget -t 1 outside/files/test3.avi.**

**NOTE**: Very little of the file is downloaded. This is because the NGFW can detect the file type when it sees the first block of data. The Demo File Policy is configured to block AVI files.

    c. Finally use WGET to attempt to download malware. **wget -t 1 outside/files/Zombies.pdf.**

**NOTE**: About 99% of the file is downloaded. This is because the NGFW needs the entire file to calculate the SHA. The NGFW holds onto the last block of data until the hash is calculated and looked up. The Demo File Policy is configured to block malware detected in PDF files.

6. In the FMC, select **Analysis > Files > Malware Events**.
    a. Observe that one file, **Zombies.pdf**, was blocked.
    b. Click the arrow on the left to drill down to the table view of the events. Note that the host **198.19.10.200** is represented by a red icon. This is the Inside Linux Server. The red icon means the host has been assigned an indication of compromise.




**NOTE:** The action is reported as Custom Detection Block, instead of Malware Block. This is because we added Zombies.pdf to the custom detection list, just in case the lab has issues connecting to the cloud. See Appendix 1 for details.

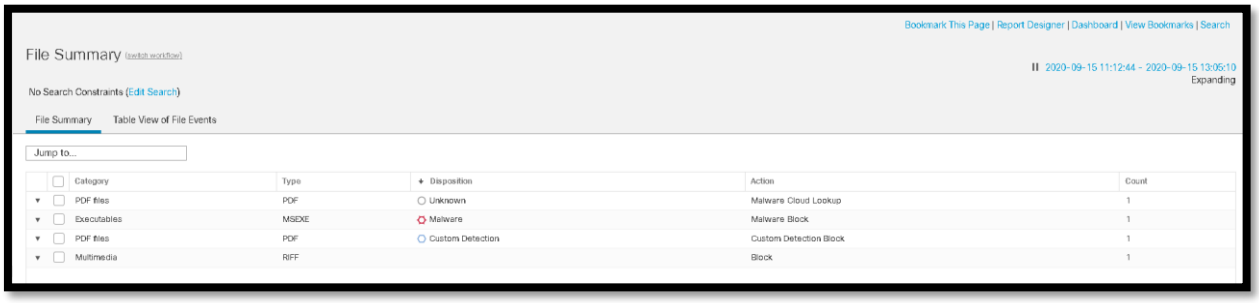
As an alternative, you can try the following from the inside Linux server:

```
wget -t 1 outside/malware/Buddy.exe
```

This should be reported as a *Malware Block.* However, in this particular lab environment, the cloud lookup may fail. Therefore, the file may not be blocked.

**Click on the red computer icon**. This will open the host profile page. Look over this page and then close it.

From the menu, select **Analysis > Files > File Events.** You should see information about all 3 file events.




**NOTE**: You can drill down if you wish.

## Static NAT Policy for FMC

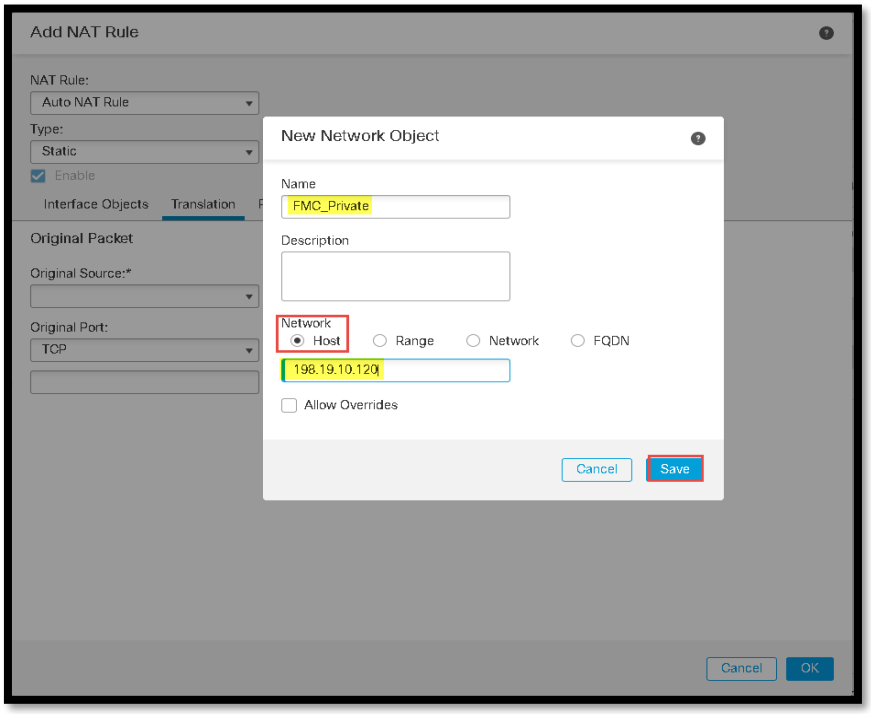
**NOTE:** We are performing this task now, but this NAT Policy will not be used until Branch 1 is brought online in a later section.

The FMC is behind the **NGFW1**, which is acting as a NAT device. We need to build a static NAT Policy so that the Branch FTD will be able to communicate with the HQ-FMC.

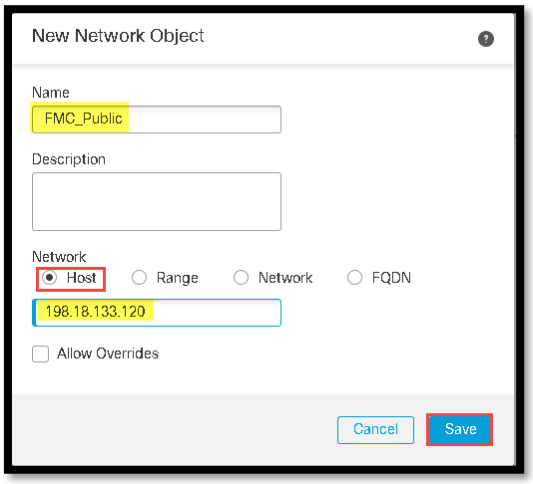
1. Go to Device > NAT > **Default PAT >** Click on **Add Rule**.

    a. NAT Rule: Select **Auto NAT Rule.**
    b. Under Interface Objects, select **InZone1** and **Add to Source**.

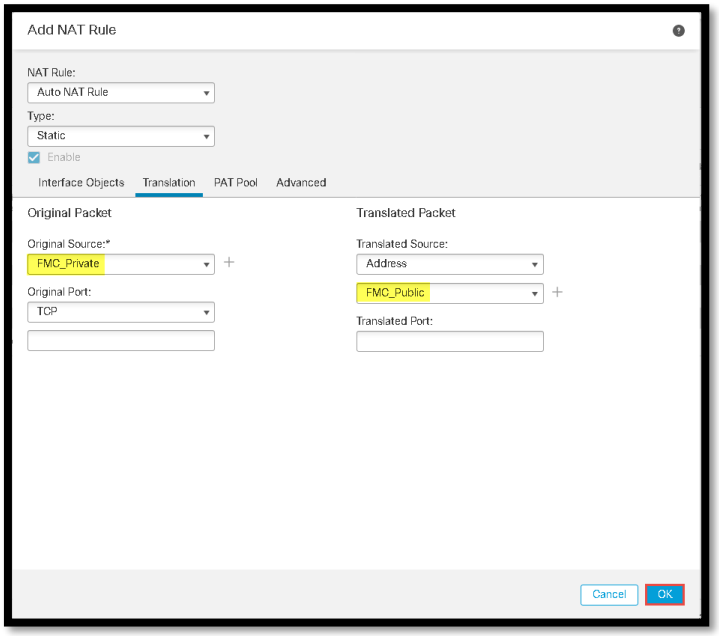
c. Select **OutZone** and **Add to Destination**.
d. Under Translation click the **(+) sign** and add the name **FMC_Private.**
   i. For Host enter **198.19.10.120** (This is the address of the HQ-FMC).
e. Click **Save.**

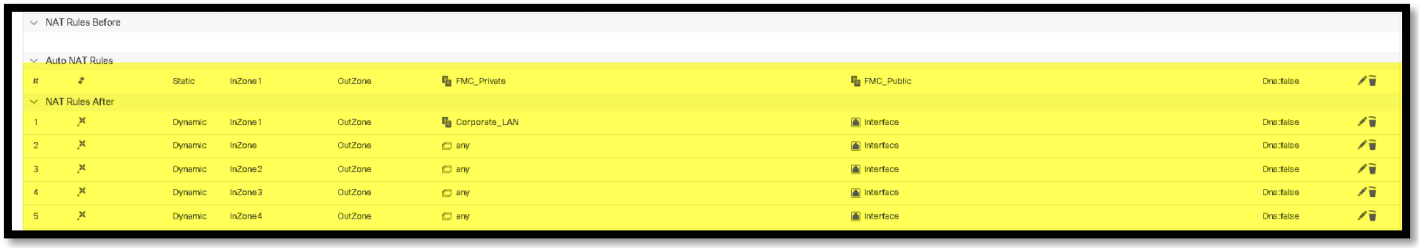



2. Click on the **(+) sign** again and add the name **FMC_Public**.
   a. For Network enter **198.18.133.120** (An Address on the WAN network).




3. For Original Source Select **FMC_Private**
4. For Translated Source Select **FMC_Public**
5. Click **OK**




**NOTE* The screenshot above shows the Auto NAT and NAT Rules After. Your screen may vary**

6. Click **Save** at the top of the web page.
7. Create an Inbound Access List for the Private FMC modifying the Access Control Policy **Base_Policy.**
    a. Select **Policies > Access Control Policies.**
    b. Click on the **pencil** icon by **Base_Policy.**
    c. Add rule called FMC_Static_NAT.
    d. Action **Allow.**
    e. Source Zone: **Outzone** Destination: **InZone1.**
    f. Destination networks **FMC_Private.**
    g. Inspection Tab.
        i. **Intrusion Policy Demo: Intrusion Policy**.
        ii. **File Policy: Demo File Policy**.
8. Click **Add** and **Save**.
9. Click **Deploy (Ignore the Warnings)**
10. Open a Putty Connection to the **Outside Linux Server**.
    a. Login as **root/C1sco12345**
    b. Ping **198.18.133.120** (Outside NAT Address of the FMC).
    c. Use **Ctrl + C** to stop the pinging.

d. Minimize the Putty session.

11. Open a Putty Connection to **Inside Linux Server root/C1sco12345**
    a. Ping **11.11.60.1**
    b. This verifies the second static route that you configured.
12. Optional**********
    a. Telnet 11.11.60.1 **admin/C1sco12345**
        i. This should Fail What would be the reason? Use Packet Tracer to find the issue

We have now deployed a FTD at the Corporate site and tested the Access Control, NAT and Intrusion policy

## Adding FTD Branch 1 to FMC

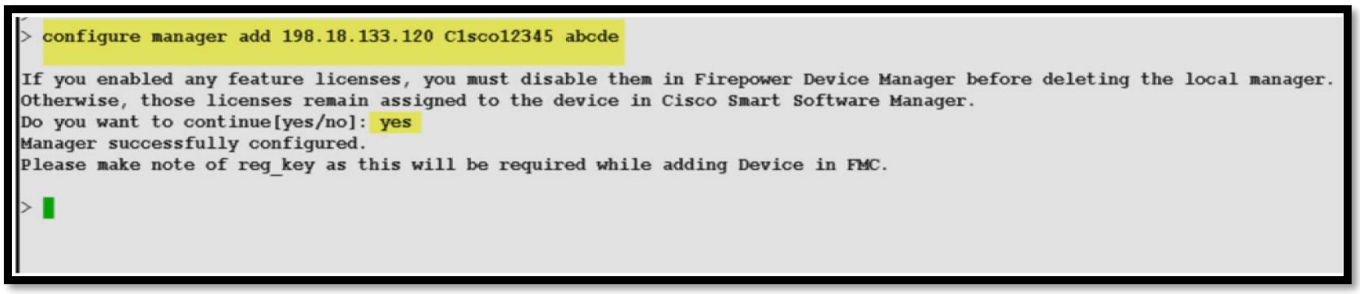
1. Earlier we created a Static NAT entry for the FMC: **198.18.133.120.**
    a. Now we will configure NGFW Branch 1 so it will also be managed by the FMC.
2. On the Jump PC Open the Putty Connection to **NGFWBR1** (198.18.133.42 : 22) Login **admin** Password **C1sco12345**

Type **show managers**

a. If the response is No mangers configured or Managed Locally we need to configure for FMC management

Type the following command configure manager add 198.18.133.120 C1sco12345 abcde

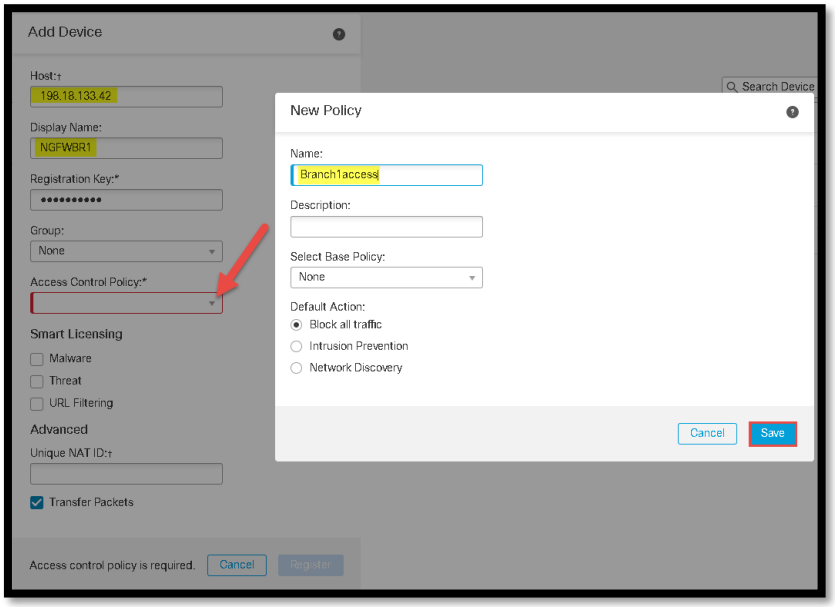
b. **If** there is a question type **yes**.




**NOTE:** You need to add the FMC's NAT Address and also a specific NAT ID (in this case abcde). The NAT ID will need to match with the NAT ID on the FMC when you go through the NGFW registration process.

Go back to the FMC webpage and go to Devices > Device Management > Add > Add Device.

a. Configure the following
b. Host: **198.18.133.42**
c. Display Name: **NGFWBr1**
d. Registration Key: **C1sco12345**
e. Group: **None**
f. Access Control Policy Click Create new policy
    i. **Branch1access**




Under Access Control Policy, select the down arrow and choose **Create New Policy.**

g. Name: **Branch1access** Select Base Policy: **None** Default Action: **Block all traffic.** Click **Save.**

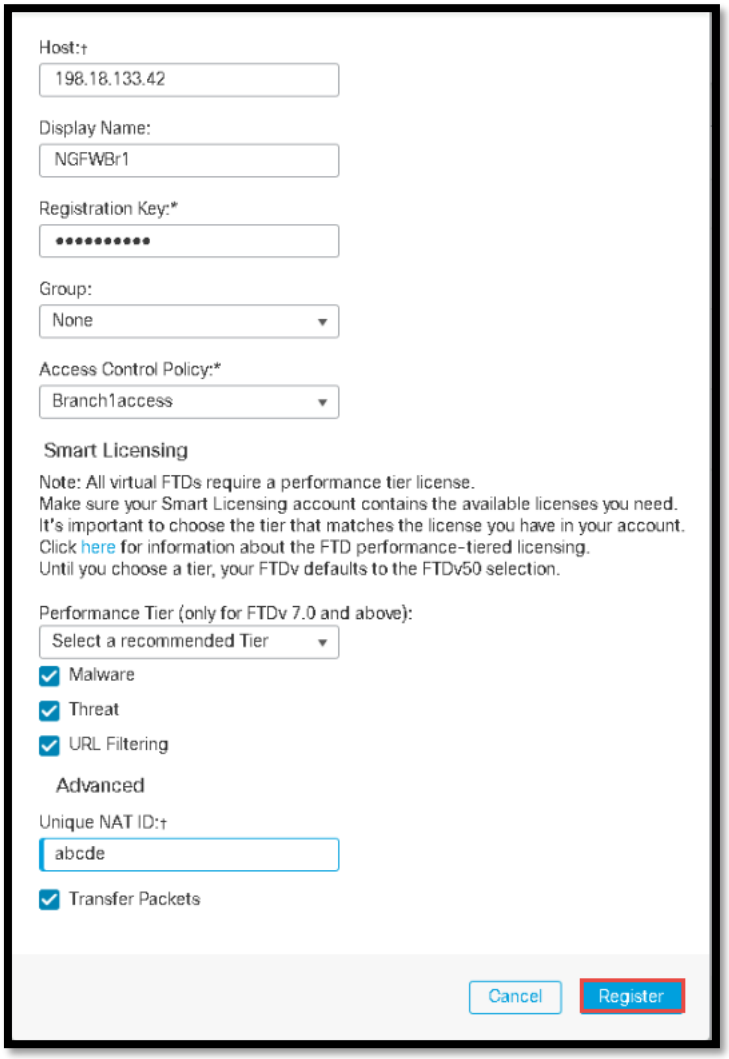
h. Smart Licensing: **Select All Licenses**

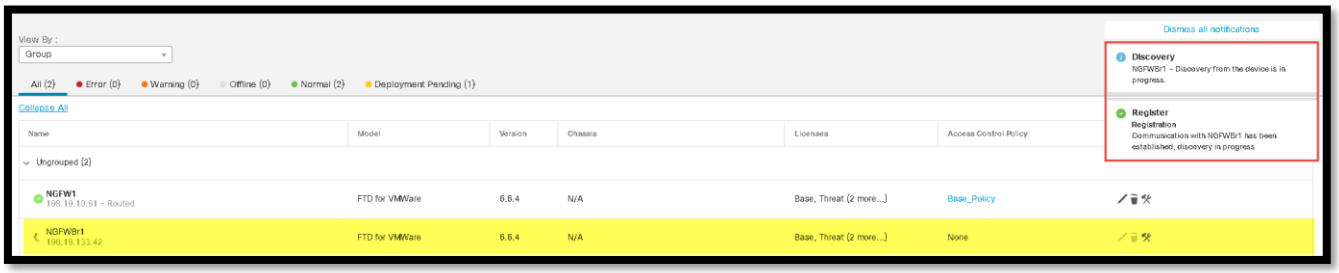
a. Unique NAT ID: **abcde**

ii. This ID is used as check to make sure the FTD is the one being configured. It is used as a one-time check and must match the same ID used in the **configure manager add 198.18.133.120 C1sco12345 abcde**

3. Select **Branch1Access** Smart Licensing: **Check all boxes** Under Advanced Type the NAT code from the FTD: **abcde.**

4. Click **Register.**



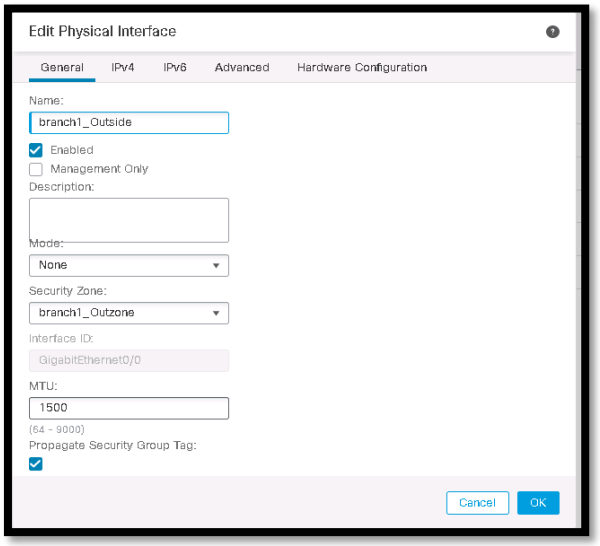




5. Wait until the **NGFWBr1** has registered.

**NOTE**: Now that the ngfwbr1 has been added we need to add interfaces, build the default route, create a NAT policy and update the Access Policy

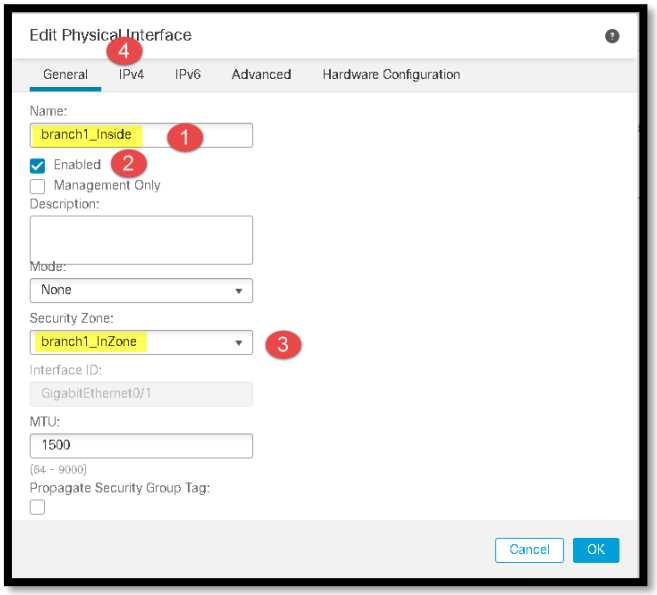
6. Go to **Devices > Device Management**. Click on the **pencil** icon next to the **NGFWBr1**.

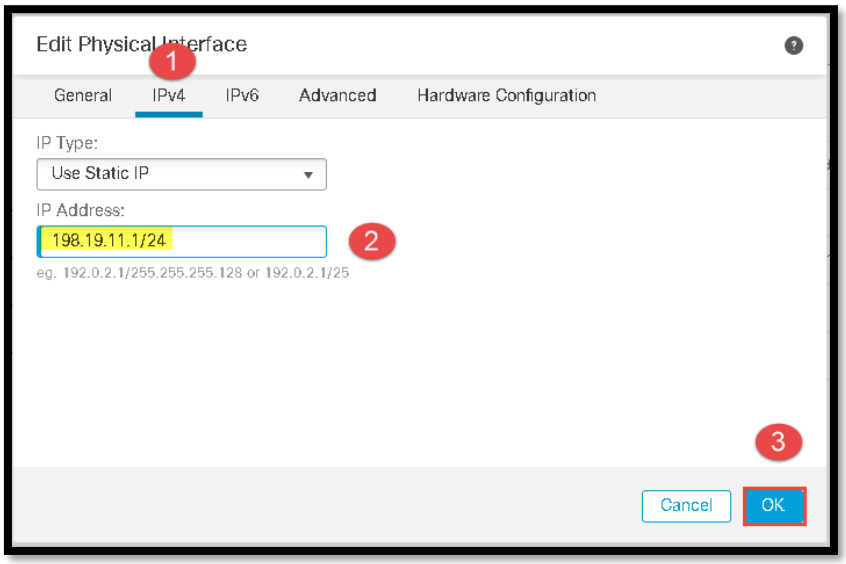
7. Click on the **pencil** icon on the **Gigabit Ethernet0/0** line.
8. Set up the **Zones** and **IP address.**
    a. Name: branch1_Outside
    b. Click: Enabled
    c. Security Zone: Click **New** Enter a name: **branch1_Outzone.**
9. Select the **IPv4 address** tab.
    a. IP Address:
        i. 198.18.128.81/255.255.192.0. This is the address of the Outside WAN (ISP).
        ii. Click OK




**NOTE:** In this scenario, we used 198.18.133.42/18 for the **Management IP Address** of the Firewall. You can see this address by entering the **show network** command from the command line or by going to **expert mode** on the FTD and run the ifconfig command and look at the **br1 interface**. The Management IP Address is accessibly only to the Operating System. We therefore have to build a WAN interface as an outside interface. The Outside Interface can also be configured by DHCP from the ISP, we did not want to add an additional server to this lab scenario.

10. Repeat for **GigabitEthernet0/1** line.
    a. Name: Branch1_inside
    b. Enabled
    c. Security Zone: branch1_InZone
    d. IPv4: 198.19.11.1/24




11. Click **Save** at the top of the Web page.
12. Go to **Routing >Static Route > Add Route >** to build a Static route to the Internet.
    a. Select Interface **branch1_Outside.**
13. For Available Network, select **any-ipv4**
    a. For Gateway. Click the (+) button and configure the New Network Object:
    b. Name: Branch1_WAN_GW
    c. Host: **198.18.128.1.**

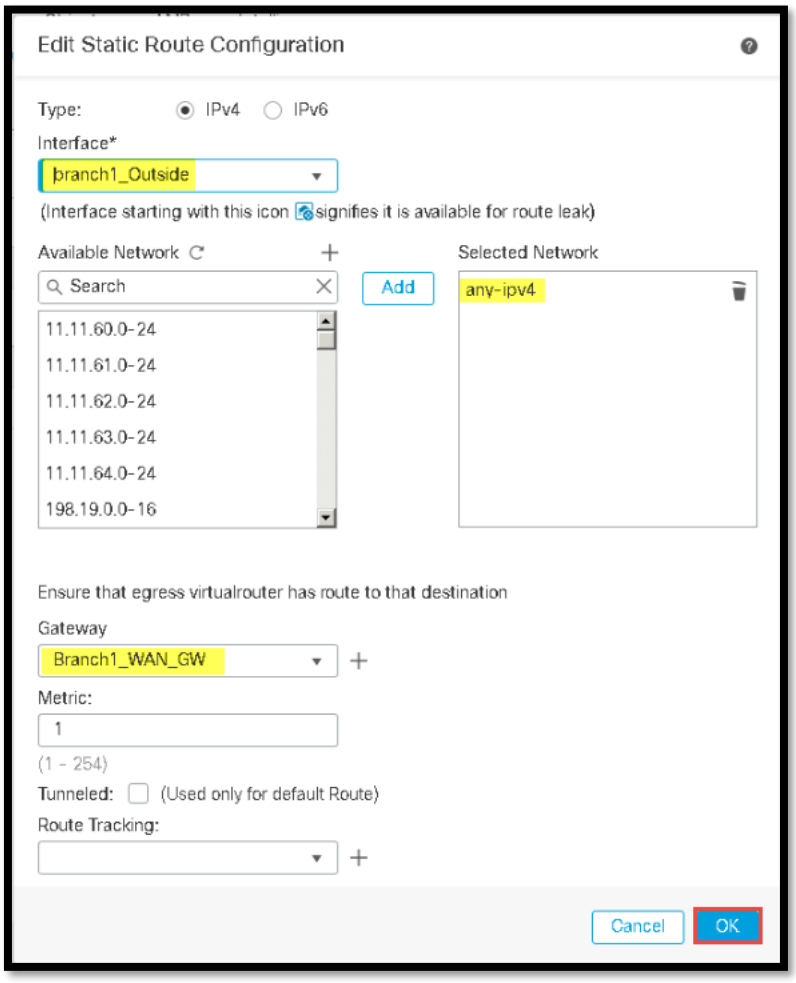
**NOTE:** This is the same address of the FMC-HQ-WAN-GW object that was created earlier. This is the gateway for the dCloud pod. You can reuse the FMC-HQ-WAN-GW for this section if you want.

14. Click **Save.**

15. **Click OK**

**NOTE:** If the Interface **outside** does not show up in the pull-down box, click on the save button on the top right of the screen.

16. When done, click **Save** at the top of the web page.



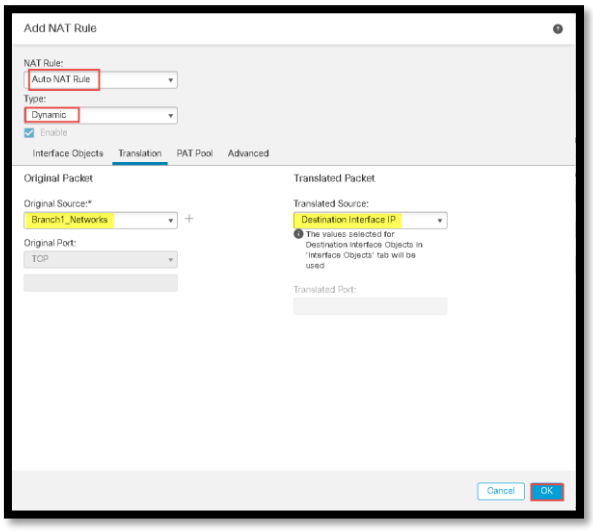

1. Go to Devices NAT > New Policy > Threat Defense NAT.
2. Name the Policy **Branch1_NAT** and under available devices select **NGFWBr1**.
3. Click Add to Policy.
4. Click **Save**.
5. Click to **Add Rule.**
6. Select Auto NAT Rule
    a. Type: **Dynamic**.
    b. Under Interface Objects, select **branch1_InZone.** Click **Add to Source**.
    c. Select **branch1_Outzone** and **Add to Destination**.

d. On the Translation Tab under Original Packet Select the (+) and configure New Network Object Name: **Branch1_Networks** Network: **198.19.11.0/24** (You could also use/create an Object in the Objects Page that would encompass an entire **lab network group** such as **198.18.0.0/15**).

7. Click **Save.**

8. On Translated Packet, select **Destination Interface IP**.

9. Select **OK** and then **Save** at the top of the web page.




10. To modify the Access Control Policy, go to **Policies > Access Control > Access Control**

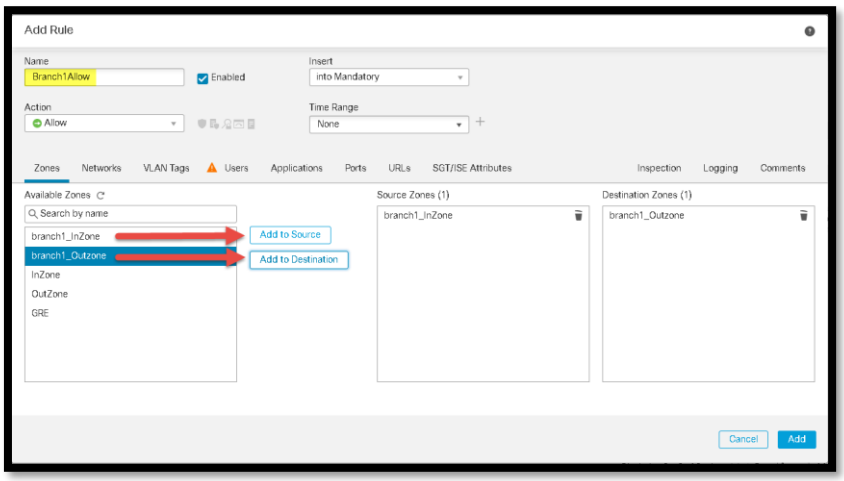
11. Click on the pencil icon to edit the Branch1access Policy

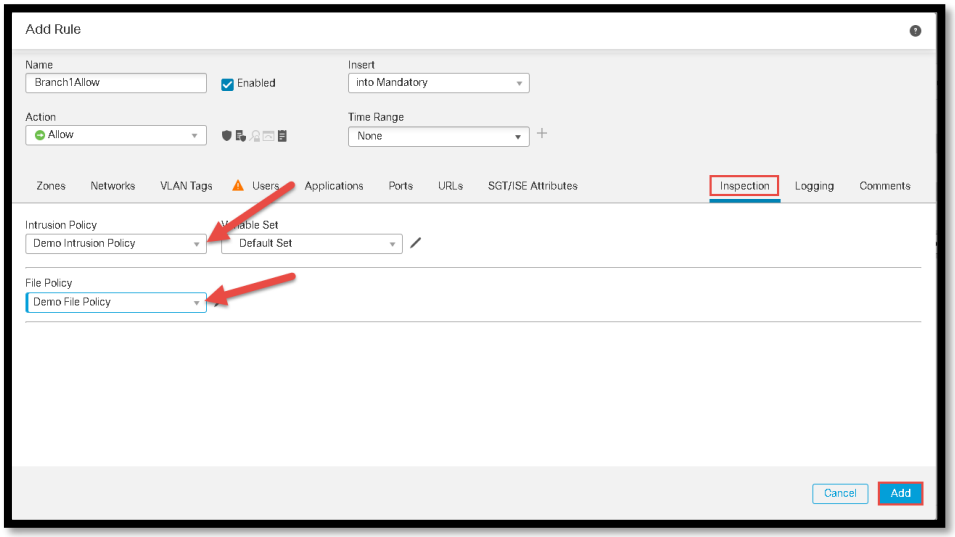
12. Click on **Add Rule**.

a. Name the rule **Branch1Allow**.

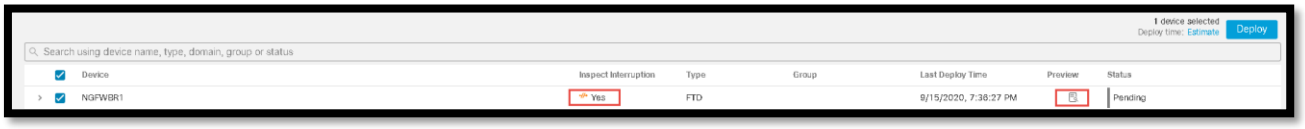
b. Select **branch1_InZone** for Source and **branch1_OutZone** for destination

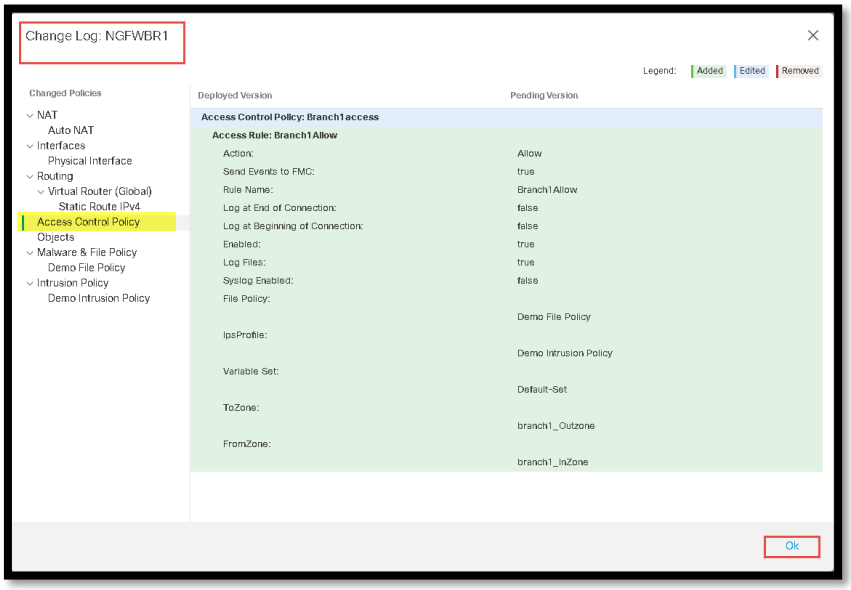
c. On Inspection Policy Select Demo Intrusion Policy and Demo File Policy.






13. Click on **Add** Click on **Save** at the top of the web page Click **Deploy** and Select **ngfwbr1.**




14. After Deployment is Complete Open Putty session to **Branch Linux Server root/C1sco12345**

    a. Type: **wget -t 1 outside/files/ProjectX.pdf** Should succeed this will verify outbound connectivity from Branch 1

## Configuring Remote Deployment NGFWBR1

You will now be configuring NGFWBR1 for remote deployments.

1. Open a PuTTY session for NGFWBR1 admin/C1sco12345
2. Type **show network**

a. Notice that br1 IPv4 address is 198.18.133.42 (NGFWBr1 Management Interface)

3. Type **show running-config sftunnel**

   a. No results will be shown, this is because the default sftunnel configuration is being used.

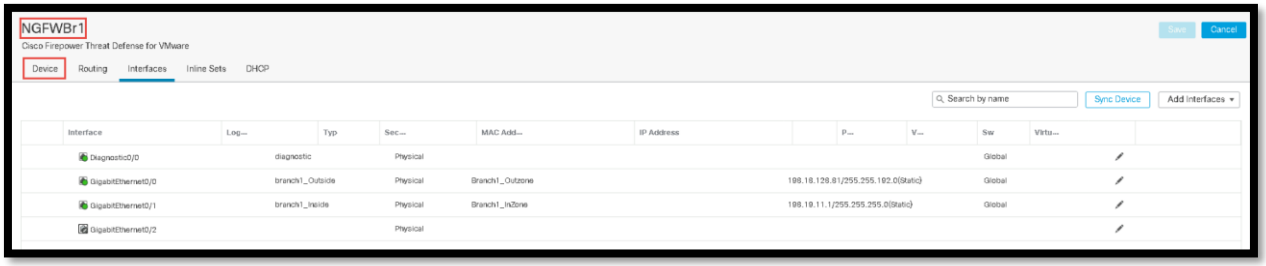
4. Type **show nat**

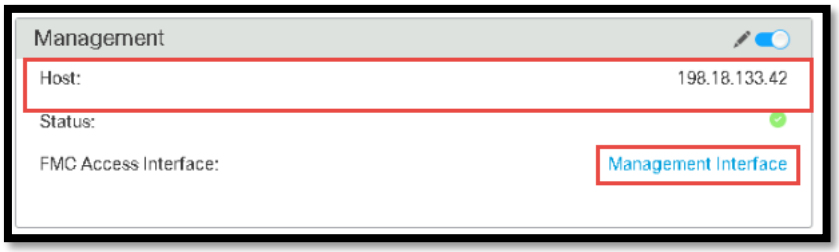
   a. There should be 1 NAT translation

5. Go back to the FMC

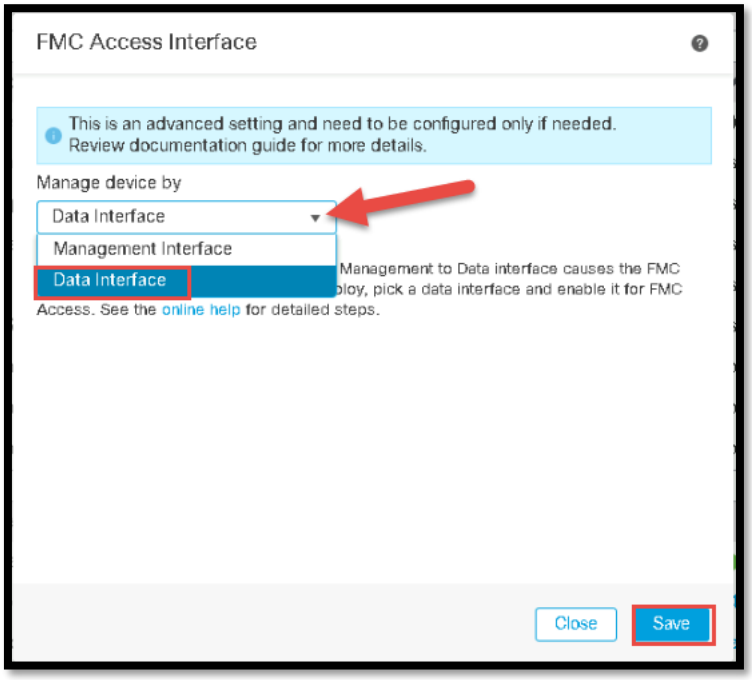
   a. Devices > Device Management > NGFWBr1

   b. Go to Device sub-tab then management section and Management interface link




   c. Select **Data Interface**



d. Click **OK** on the message and then **Close**

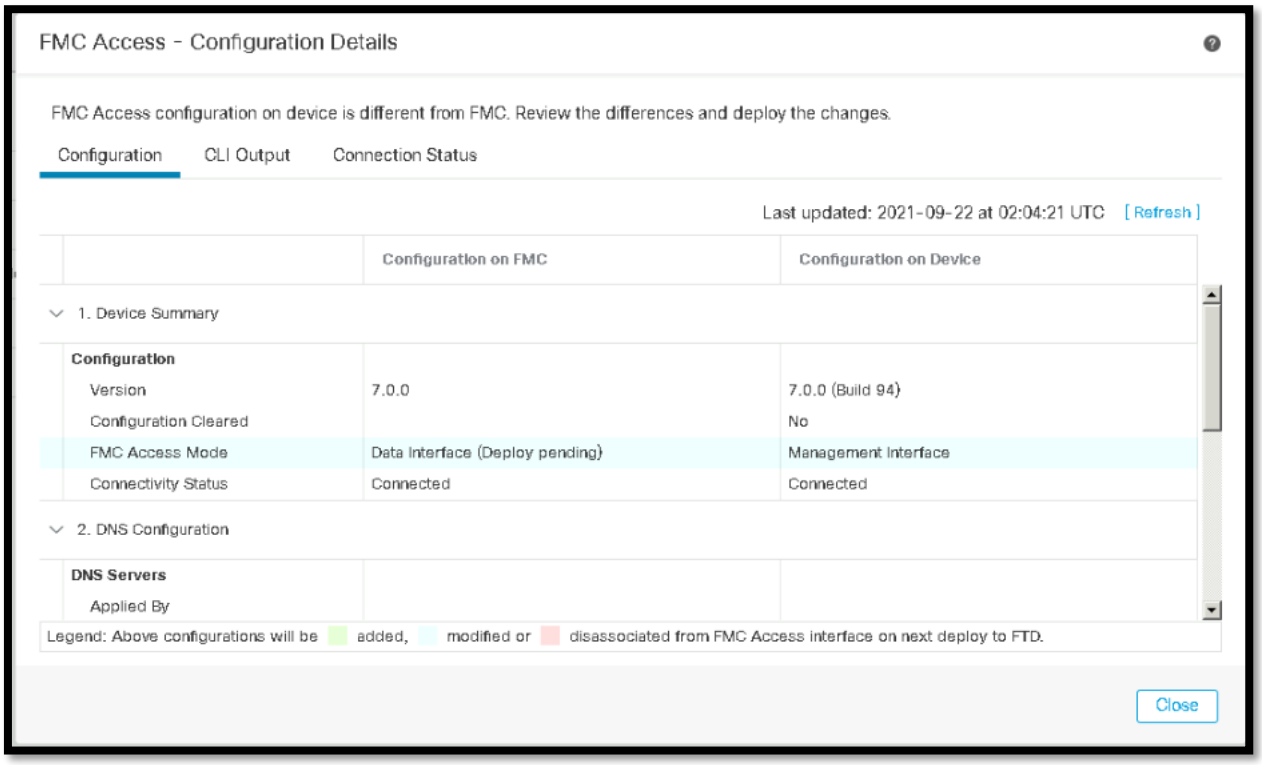
e. Select the Interfaces sub-tab and Edit GigabitEthernet0/0

f. Go to FMC Access

i. Click on Enable management on this interface for the Firepower Management Center

ii. Under Available Networks select FMC_Public and click **Add and OK** Click **Yes** under **Please Confirm**

Note in the upper right-hand corner you will see FMC Access via Data Interface (Deploy pending). You can click on View details



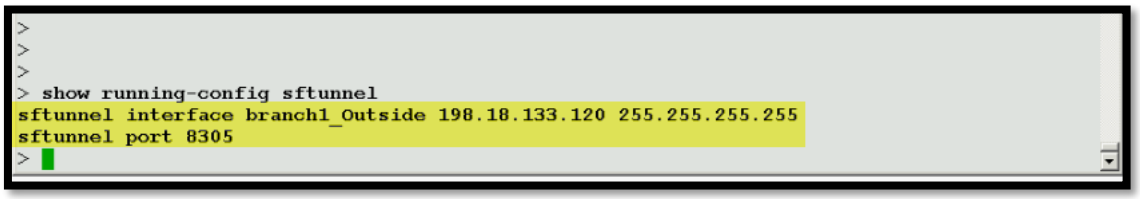

g. Click on **Save** and then **Deploy** when Deploying read the warning and click **Deploy**

h. Wait for deployment to complete and then open the PuTTY session to NGFWBr1

6. Type **show network**

a. You will now see GigbitEthernet0/0 and see the IP Address **198.18.128.81** this shows that the **Data Interface** can now be used for management to the **FMC**

7. Type **show running-config sftunnel**




8. Type **show nat**

a. You will now see 3 additional NAT rules

```
>
> show nat
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (branch1_Outside) source static nlp_server_0_sftunnel_intf2 interface
service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (branch1_Outside) source dynamic nlp_client_0_intf2 interface
    translate_hits = 0, untranslate_hits = 0
2 (branch1_Inside) to (branch1_Outside) source dynamic Branch1_Networks interface
    translate_hits = 2694, untranslate_hits = 0
3 (nlp_int_tap) to (branch1_Outside) source dynamic nlp_client_0_ipv6_intf2 interface ipv6

    translate_hits = 0, untranslate_hits = 0
>
```

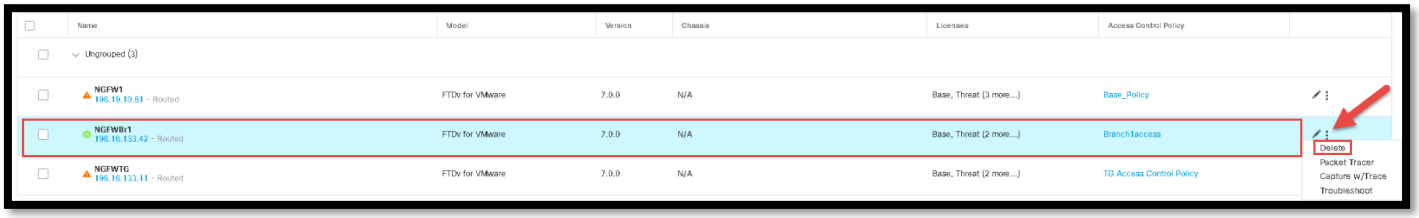
9. Type **show network**

a. You will see that the Gateway for the original Management Interface is now the data interface and the Gateway for GigabitEthernet 0/0 is the WAN Gateway

```
> show network
===============[ System Information ]===============
Hostname                  : ngfwbr1.dcloud.cisco.com
Domains                   : dcloud.cisco.com
DNS Servers               : 198.19.10.100
DNS from router           : disabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

=====================[ br1 ]=====================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:50:56:97:A2:2D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 198.18.133.42
Netmask                   : 255.255.192.0
Gateway                   : 198.18.128.81
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet0/0

===============[ GigabitEthernet0/0 ]===============
State                     : Enabled
Link                      : Up
Name                      : branch1_Outside
MTU                       : 1500
MAC Address               : 00:50:56:97:F6:1A
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 198.18.128.81
Netmask                   : 255.255.192.0
Gateway                   : 198.18.128.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

>
```

## Restoring NGFWBR1 to an unconfigured state

1. Here is a fast way to put a NGFW into a clear unrestored state.
2. On the FMC go to Devices > Device Management and click on the three dots and select Delete




3. On the PuTTY session for NGFWBr1 Type:

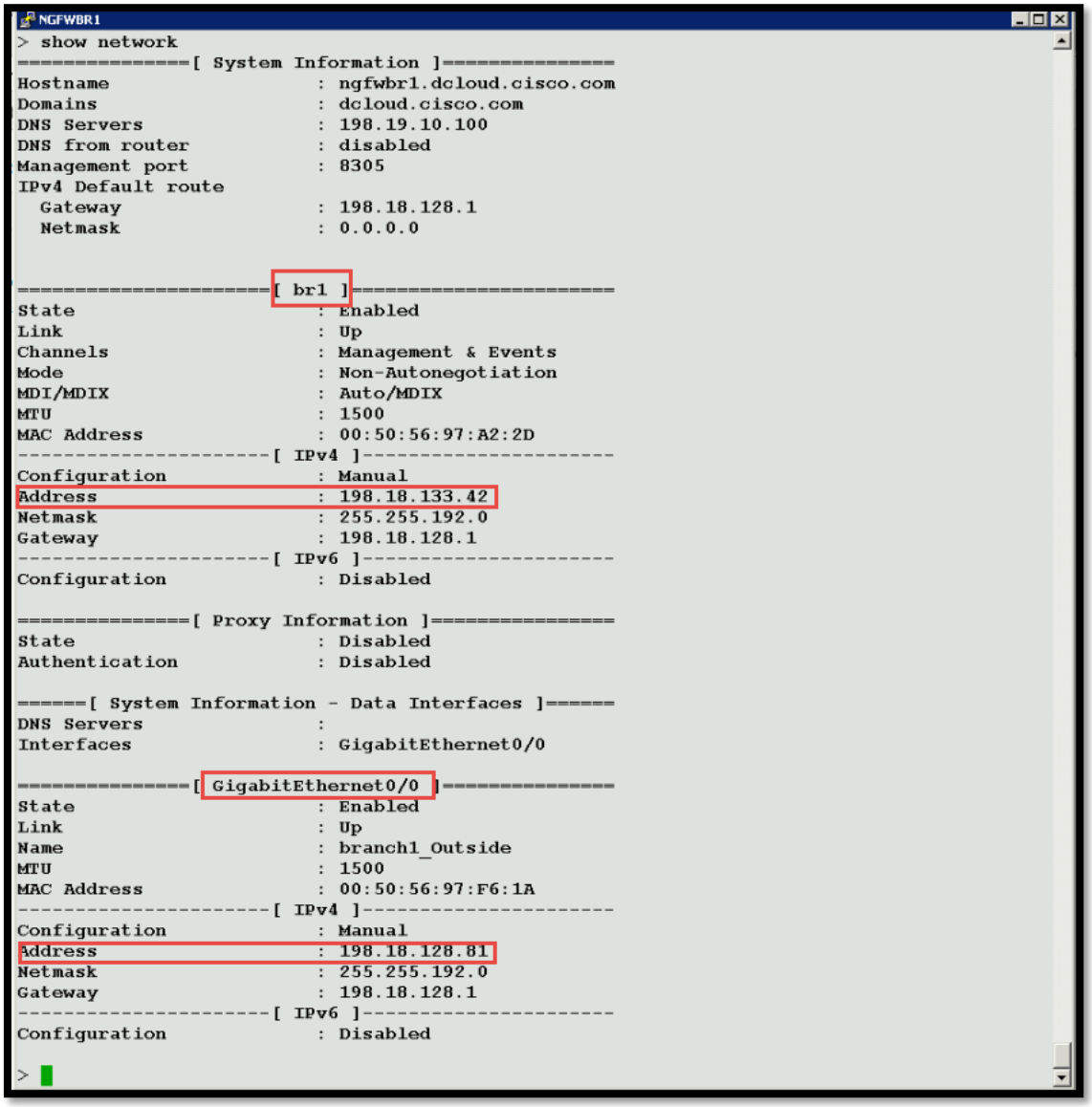
    a. **show interface ip brief**

        i. You will see interface addresses are retained

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         198.18.128.81   YES CONFIG up                    up
GigabitEthernet0/1         198.19.11.1     YES CONFIG up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down up
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Control0/1        unassigned      YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  down                  up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           169.254.1.1     YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              unassigned      YES unset  up                    up
>
```

    b. **show network**

        i. You will see the br1 management interface (198.18.133.42) and the GigabitEthernet0/0 (198.18.128.81) that is configured as the Management via the Data Interface




c. Type: **configure firewall transparent and select [y]**

d. Type: **configure firewall routed and select [y]**

e. Type: **show interface ip brief and show network and note the results**

## Configuring NGFWBr1 to boot using Data Interface for Management

1. On the NGFWBr1 PuTTY terminal type:

   a. configure network management-data-interface

      i. Data Interface to use for management: GigabitEthernet0/0

      ii. Specify a name for the interface [outside]: branch1_Outside **[indicates default value]**

      iii. IP address {manual /dhcp) [dhcp]: manual

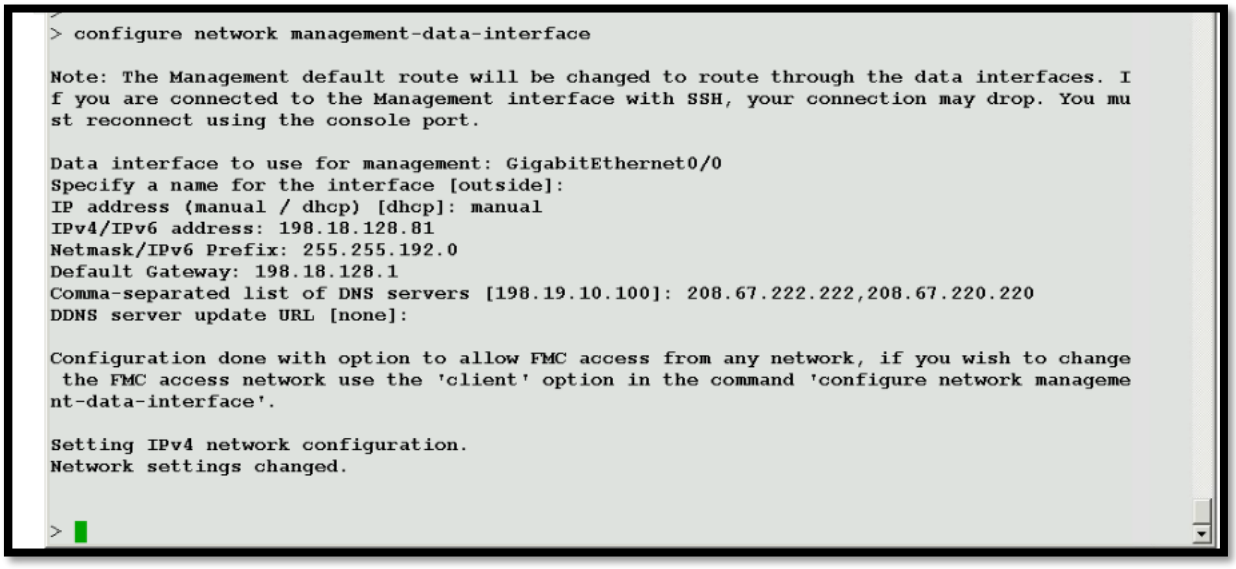
      iv. IPv4/IPv6 address: 198.18.128.81

v. Netmask/IPv6 Prefix: 255.255.192.0

vi. Default Gateway: 198.18.128.1

vii. Comma-separated list of DNS servers [198.19.10.100]: 208.67.222.222,208.67.220.220

viii. DDNS server update URL [none]:




b. Confirm settings by typing the following commands:

i. show network (confirm that GigabitEthernet0/0 is referenced)

1. Notice that the Gateway for Interface br1 is 198.18.128.81 (data-interface)

ii. show running-config sftunnel (confirm that the sftunnel is using the outside interface)

iii. show nat (confirm that there are nat rules no found in the running configuration. Verify by typing show running-config )

2. Register NGFWBr1 with the FMC

a. On the PuTTY session for NGFWBr1 type:

i. configure manager add 198.18.133.120 C1sco12345 abcde

b. On the FMC go to Devices > Device Management > Add > Device

i. Host: 198.18.128.81

ii. Display Name: NGFWBr1

iii. Group: None

iv. Access Control Policy: Branch1access

v. Smart Licensing: Click all Three

vi. Unique NAT ID: abcde

c. Click Register

## Configuring NGFW-TG

In this section we will be configuring NGFW-TG. This device will be used as a traffic generator for adding data to the FMC connection events. Since you have already configured 2 NGFW's the configuration criteria will be given but no screenshots.

1. Open a PuTTY Session to NGFW-TG admin/C1sco12345
2. Verify the Management IP Address
3. Configure NGFW-TG to connect with the FMC (198.18.133.120) use C1sco12345 as the password. Remember this is a remote device
4. Register NGFW-TG with the FMC Name: NGFW-TG use TG Access Control Policy all licenses
5. Go to NGFW-TG and make sure Interface Gigetherernet0/0 and0/1 are enabled and have IP Addresses
6. Security Zone for GigEthernet0/0- OutZone1
7. Security Zone for GigEthernet0/1 – InZone
8. Deploy the changes

## Configuring **NGFW3** Management Using Firewall Device Manager (FDM ON BOX)

**NOTE:** In order to configure the FTD using the on-box manager the default FTD address is **192.168.45.45/32** with a default gateway of **192.168.45.1 has been changed.** NGFW3 has been preconfigured with the Management IP Address and the Username/Password used below.

1. Open up a putty session to **NGFW3** Username: **admin** Password: **C1sco12345**
2. Type **configure manager delete if** prompted type **yes** not [y]
3. Type **configure manager local**

**NOTE: The previous commands cleared the manager database and reset the licensing server. This will allow you to configure the FDM. In a production environment, you should never need to do this. The configure manager delete will fail if the device is currently registered to the FMC. You will need to remove the device from the FMC; this will remove the FTD from the FMC UI and will remove the FMC from the FTD. It might take between 10 to 15 minutes to restart the services on the FTD. You will get a Service Unavailable when trying to access NGFW3 until all services are restarted.**

3. From the Jump PC, open a browser to **https://198.19.10.83** (This is a preconfigured management interface for NGFW3). You can also click on the **NGFW3 (FDM)** from the browser status bar

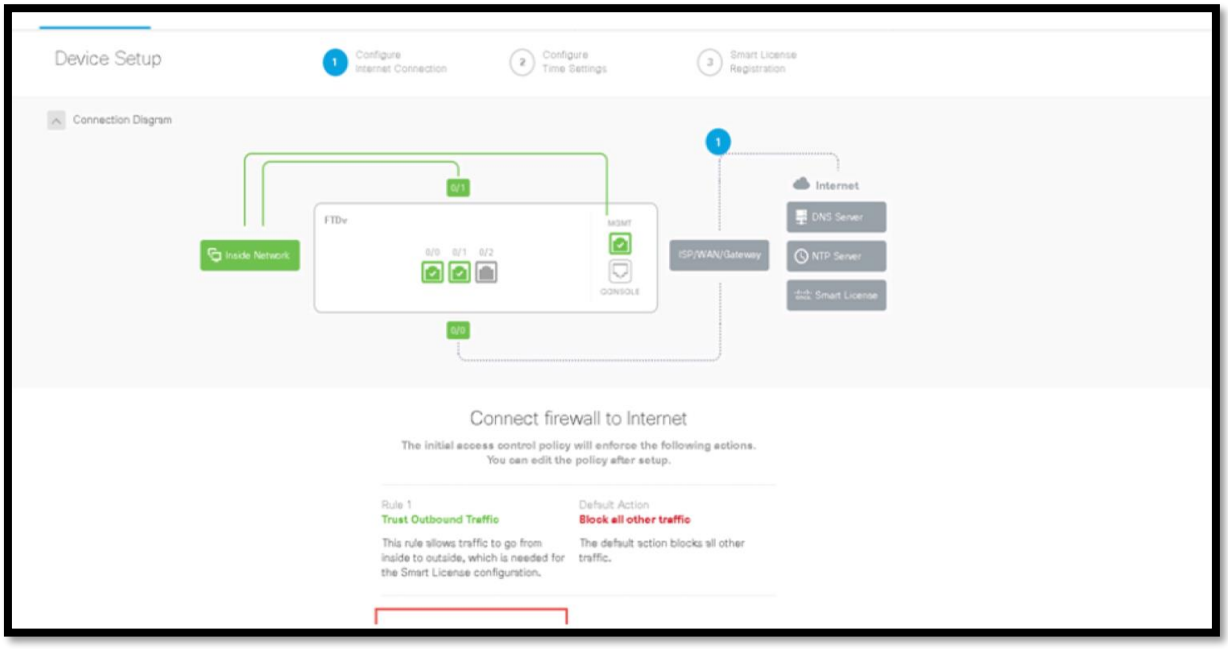
If you are prompted with a security warning accept the risks

**It might take between 10 to 15 minutes to restart the services on the FTD. You will get a Service Unavailable when trying to access NGFW3 until all services are restarted**

The Firepower Device Manager screen should prepopulate. If not, the credentials are Username: Admin Password: **C1sco12345**

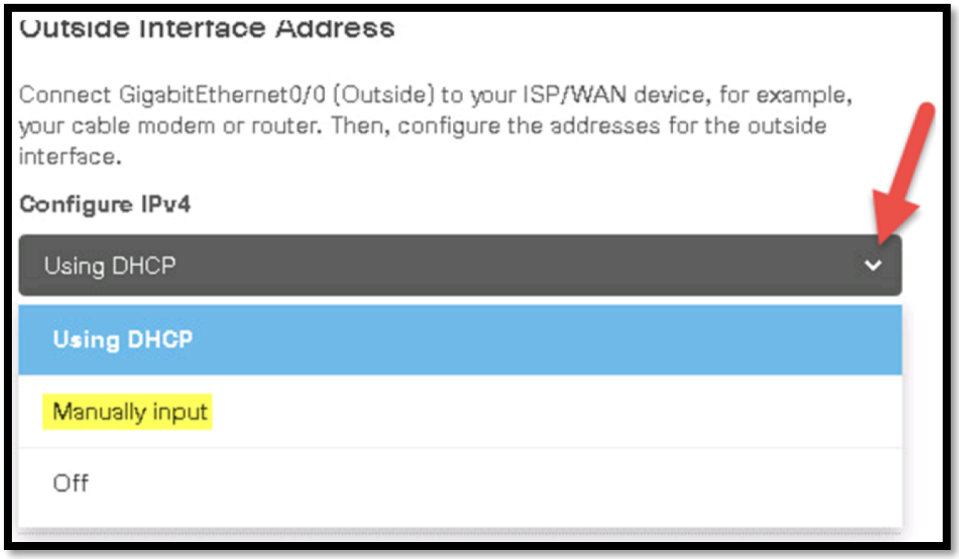
Click Login

You will come to the following screen, which displays the FTD connections. Scroll down to the **Outside Interface Address**

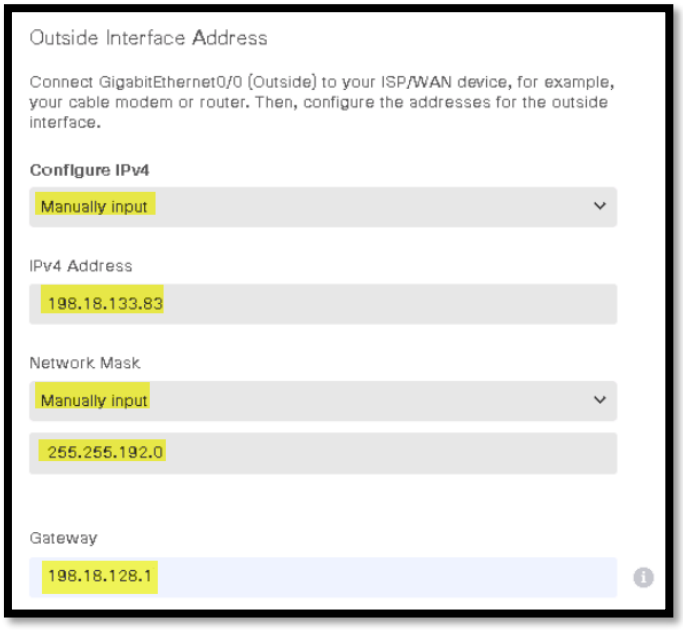



Select the arrow next to **Using DHCP.**

Click on **Manual Input**.

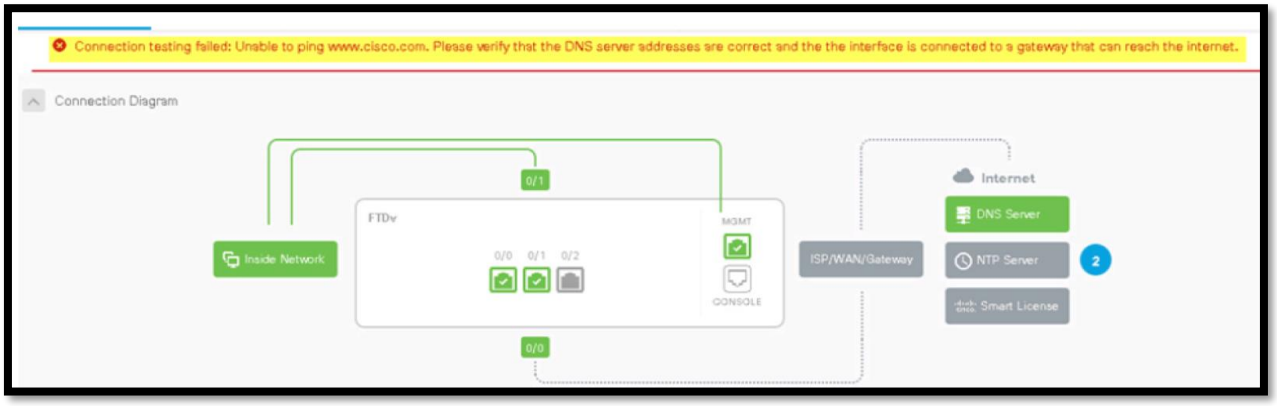



4. Configure the Outside Interface Address.
    a. IP Address: **198.18.133.83**
    b. Network Mask: **255.255.192.0**
    c. Gateway: **198.18.128.1**




5. Click **Next**

   a. If you get a message that, the connection to www.cisco.com has failed. That is ok move on to the setting of the NTP services.




Manually Set the NTP Server.

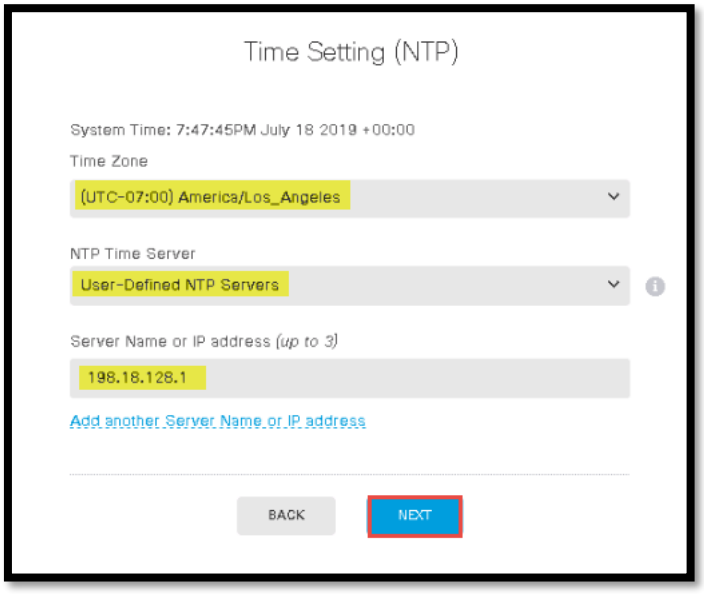
   a. Select **Time Zone.**

      iii. **Select America/Los_Angeles**

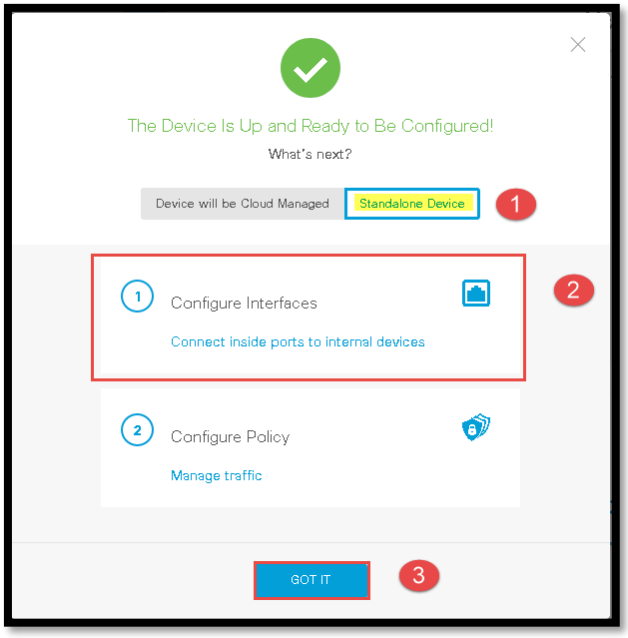
   b. NTP Time Server User-Defined

      iv. Address: **198.18.128.1.**

   c. Click **Next.**

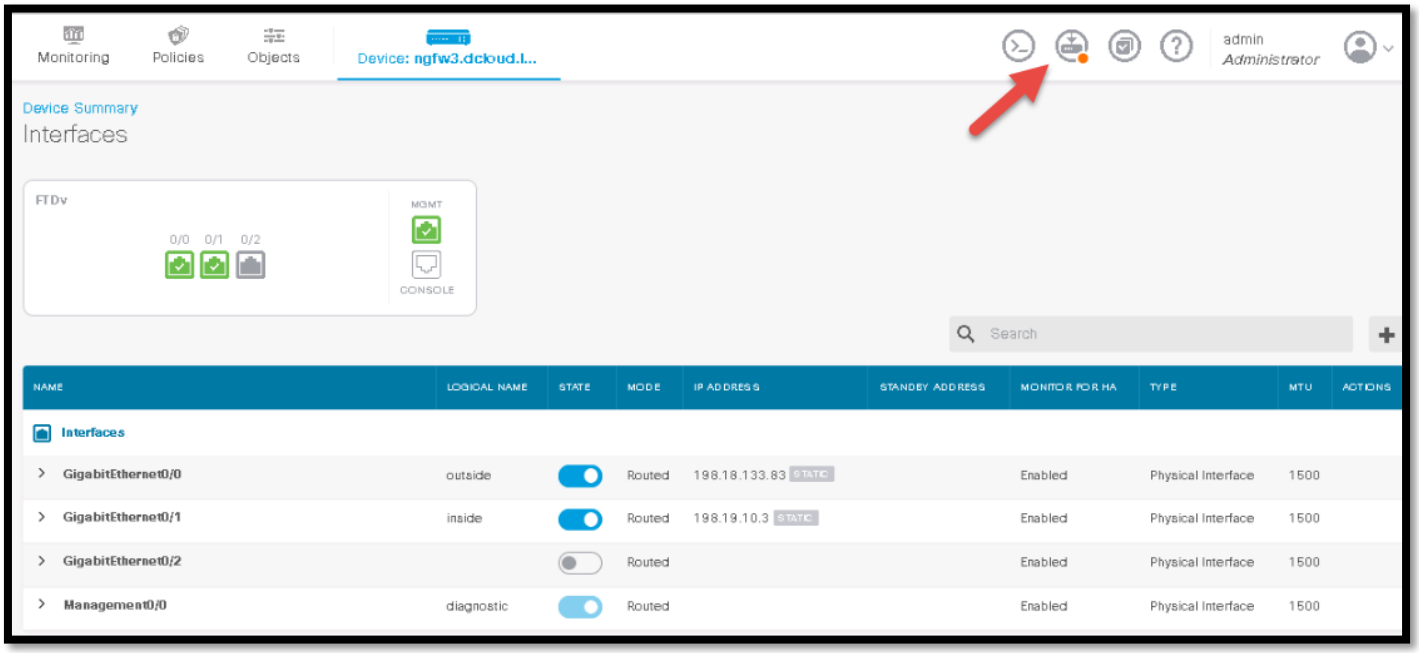



6. This will bring you to Smart License **select Start 90-day evaluation period without registration.**
7. Performance Tier: FTDv5 - Tiered
8. Click **Finish**
9. The next screen select Standalone Device to configure **Interfaces** or **Policy**.
10. Select **Interfaces**.




**NOTE:** As you can see Interface GigabitEthernet 0/1 is 192.168.45.1. Also, the Outside Interface GigabitEthernet 0/0 has the outside interface that we manually configured. If you wish to change the address of GigabitEthernet 0/1, choose the GigabitEthernet 0/1 line and go to actions. A pencil Icon will appear. Click on the icon. Delete the DHCP pool. Change the IP Address to: 198.19.10.3/255.255.255.0 and click OK

11. Click on the deployment icon and note the configuration changes that will be deployed to the FTD

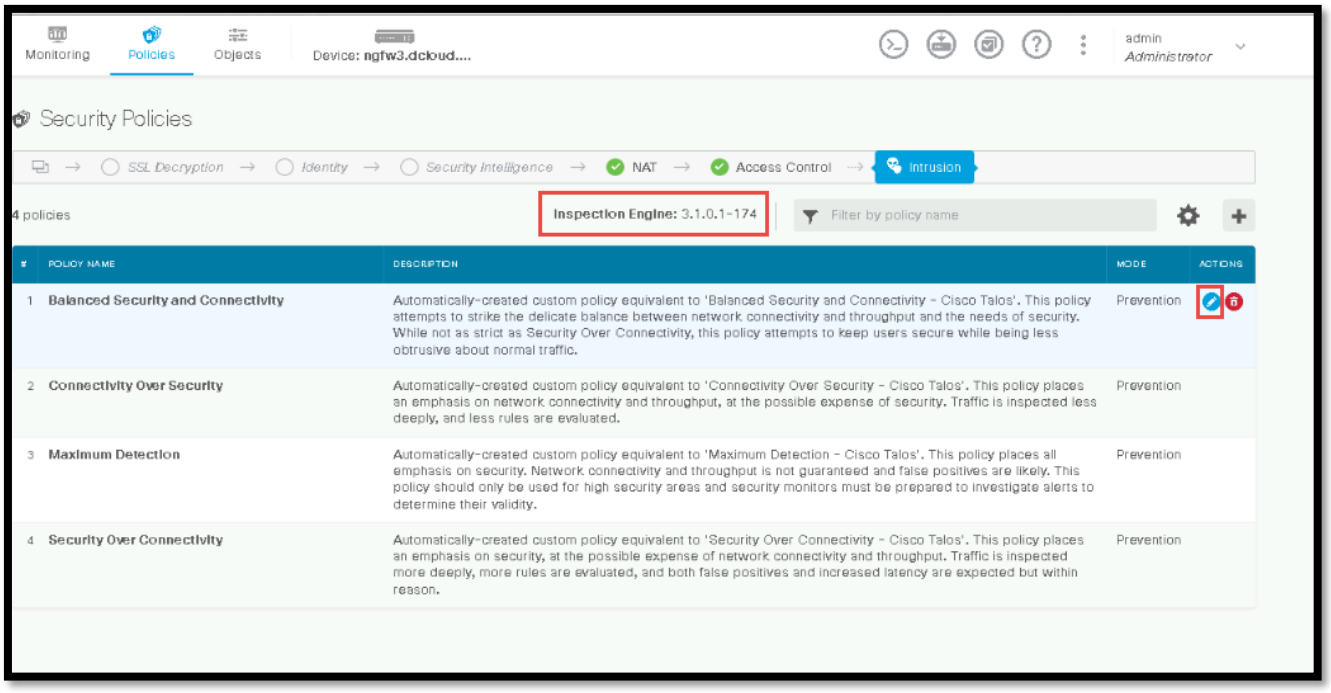



12. Deploy the configuration

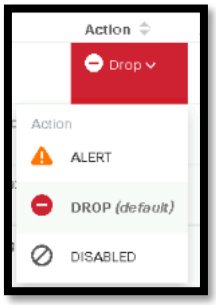
## FDM Snort 3 Intrusion Policy

Snort 3 was introduced on the FDM in code version 6.7. In the next steps we will be looking at Snort 3 rules on the FDM

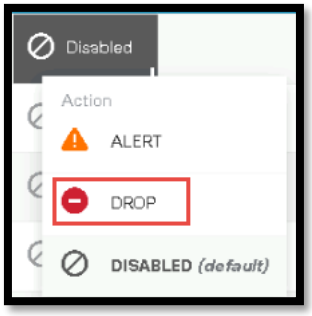
1. From the FDM go to Policies > Intrusion



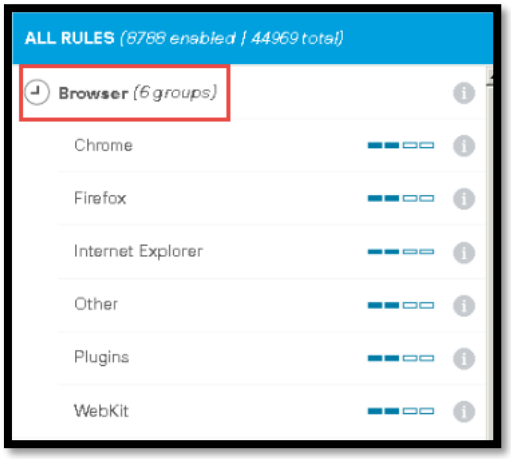
2. Click on **Balanced Security and Connectivity**
3. Note that the Snort rules are sorted by SID
4. Click on the **Action** cell for one of the rules. Note that the rule states can be set to override. (**ALERT, DROP, DISABLED)**



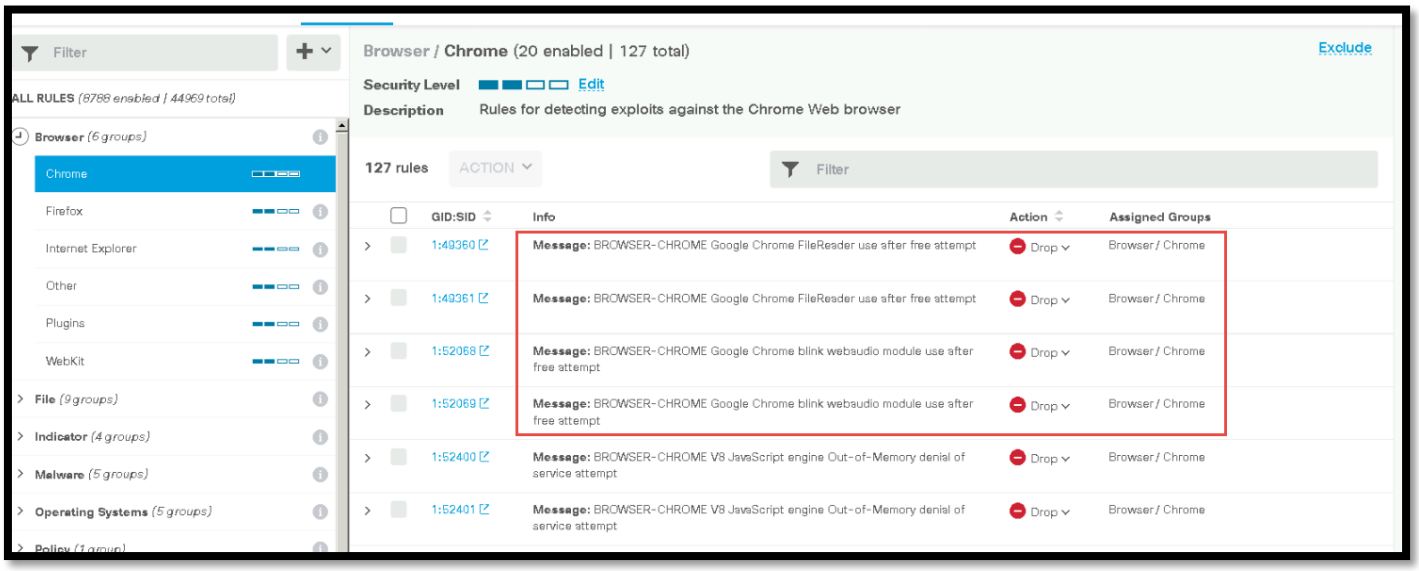

5. Click on the Search field and you will see the GID (Generator ID 1 for standard text rules, shared object rules 3), SID (Snort ID, Talos rules under 1,000,000 local rules over 1,000,000), and Action Field. Then click **Cancel**
6. Locate the 1:105 Rule (first rule), with the **MALWARE-BACKDOOR-Daggger_1.4.0**
    a. Click on the **Action Field and set to Drop**



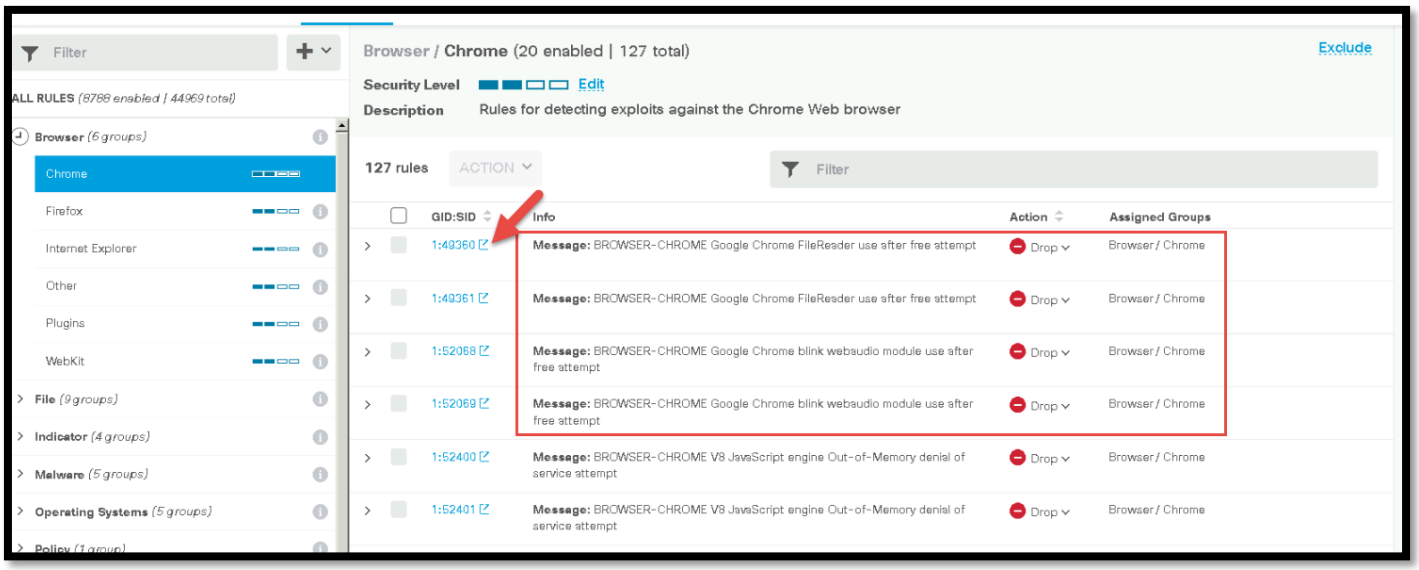

7. Deploy your policy using the deploy button  button and **Deploy Now**
8. Note the rule groups on the left
9. Click on the Browser group to show the child groups




10. Select **Chrome** child group this will show the **BROWSER-CHROME** rules




11. Click on one of the Links under the GID:SID



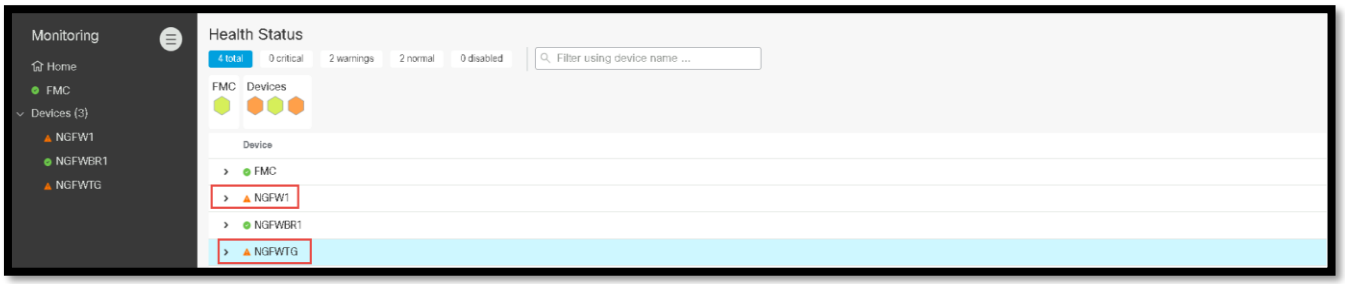
12. Note the Documentation


13. Look at the current Security Level

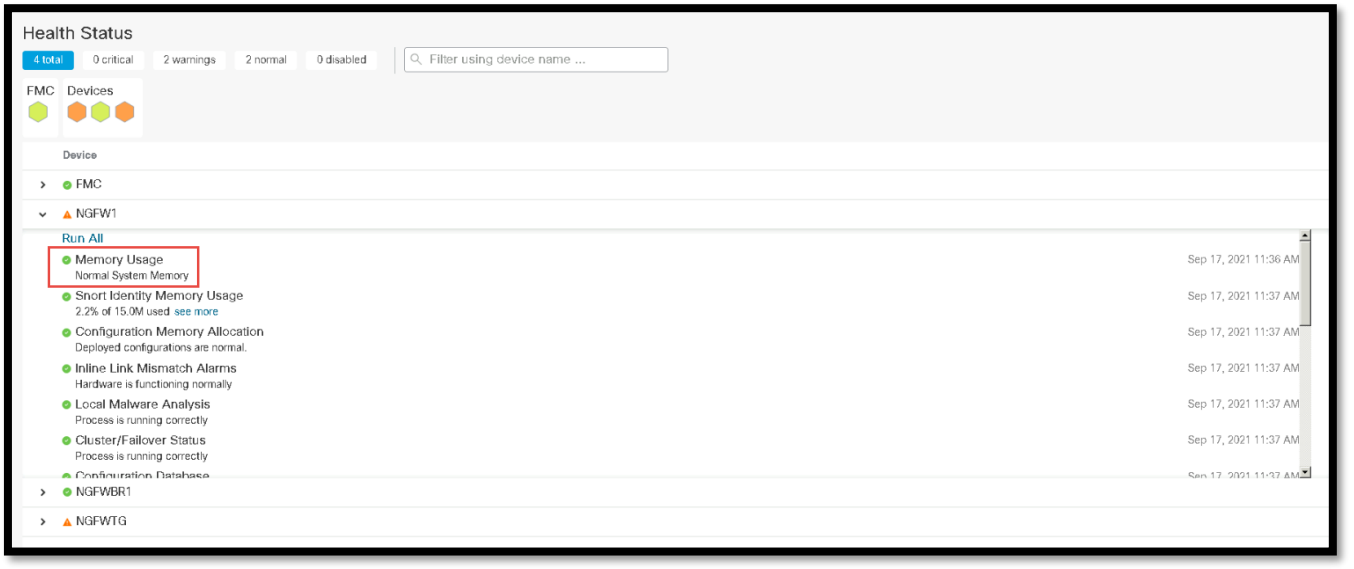

14. Click on the **Edit** link to check or change the Security Level up to **Level 3**
15. You will see more rules enabled and total rules
16. Examine some of the new rules in this Level 3

## Health Policy Adjustments on the FMC

1. On the FMC Go to System > Health > Monitor

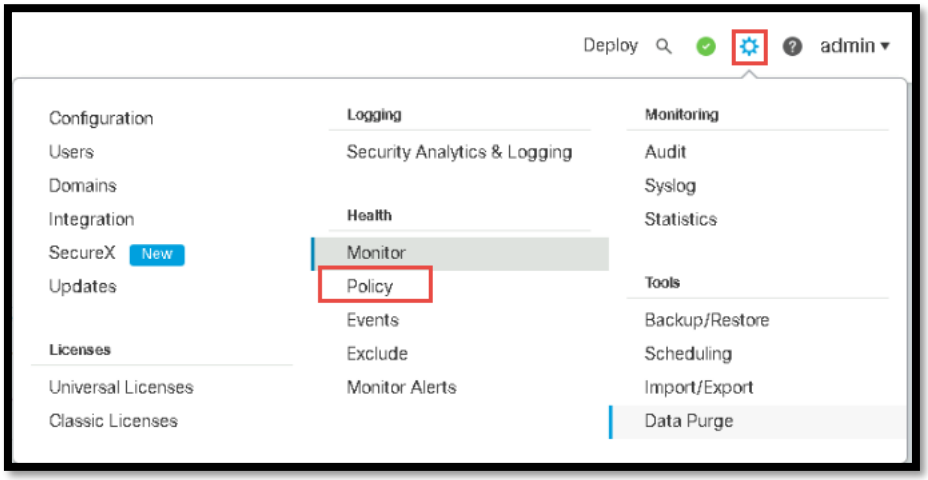



2. If you see one of the devices with the Triangle, click on it to see the warnings and then click Run All

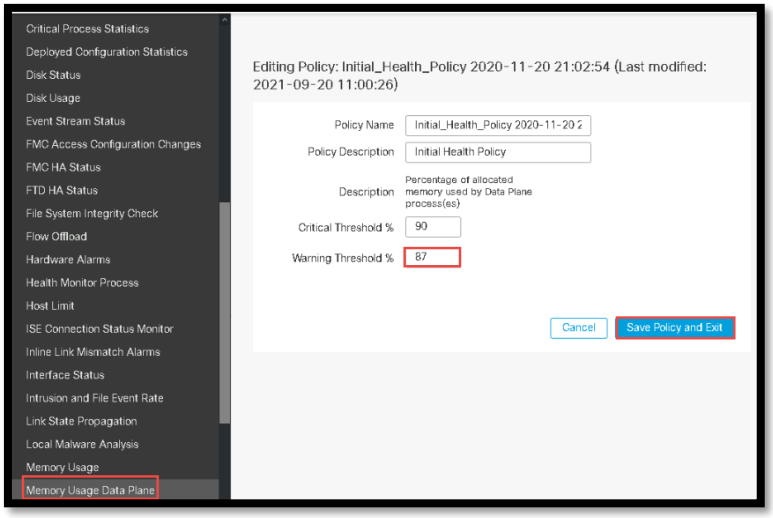




3. The memory warnings are for Lina memory usage. We will adjust the settings to fix this issue (Note, we are running low memory due to Lab resource issues, the policy change we are making is not optimal)

4. Click on System > Policy

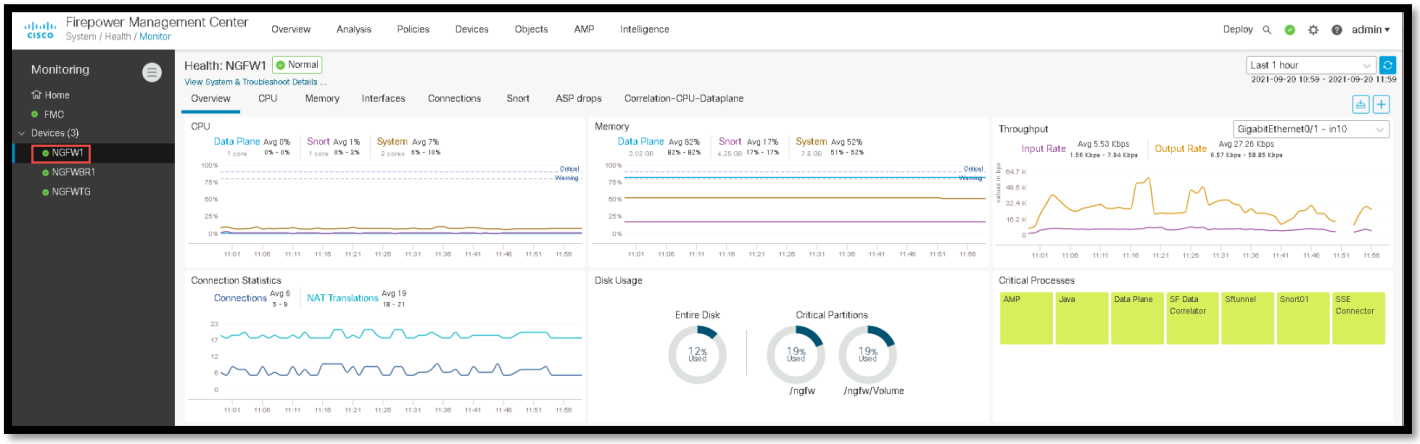



5. Click on the pencil icon on the Health Policy Line
6. On the left-hand side click **Memory Usage Data Plane** and set the Warning Threshold % to **87 Save Policy and Exit**

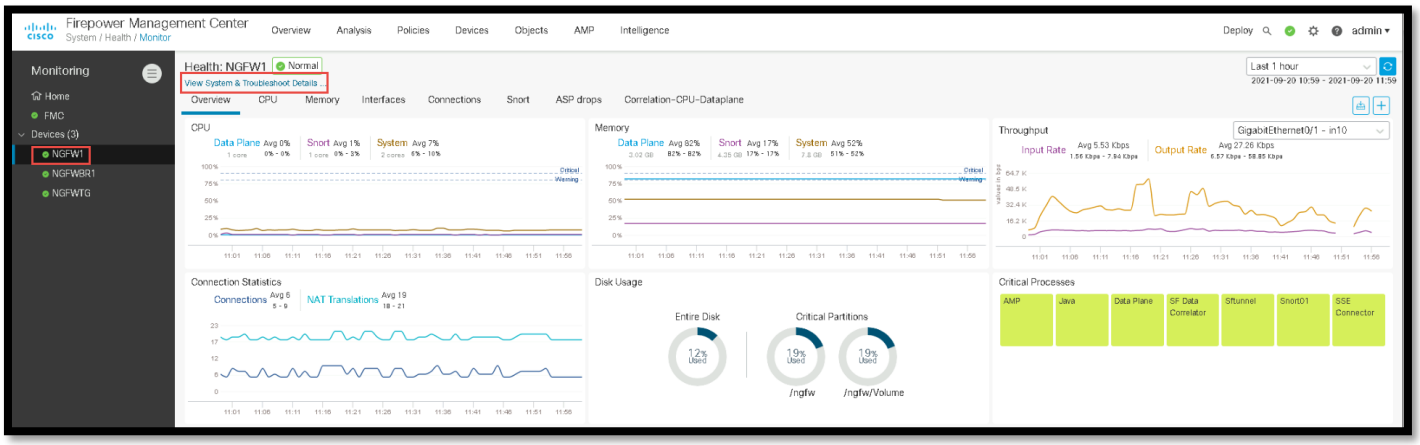



7. Click on Apply Policy


8. Go back to System > Monitor
9. Click on one of the devices (e.g., FMC, NGFW1, etc) and look at the dashboard




10. Review Click on View System & Troubleshooting Details




11. You will see under the System Details

    a. Look at the VDB build

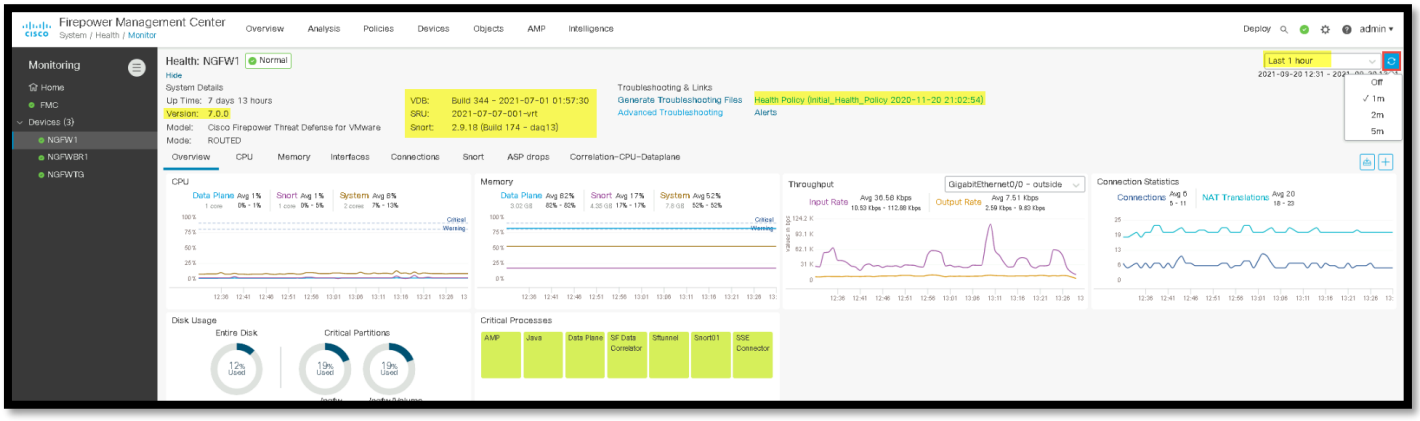
    b. Look at the SRU

    c. Notice the Snort version (2.9.x)

    d. Under Troubleshooting & Links you will notice the Health Policy that is currently assigned

    e. Notice the Link for Advanced Troubleshooting

    f. On the far right you will see where you can set the time frame for this page currently at 1 hour. Click the refresh icon and show the different intervals




12. Click on CPU, Memory, Interfaces, Connections, Snort tabs and review the results (If no results with NGFW1, try NGFWTG)

# Scenario 3. FlexConfig

This exercise consists of the following tasks.

Create a user defined FlexConfig object

Modify a Text Object used in a system defined FlexConfig object

Create and configure a FlexConfig policy

Deploy the changes and test the configuration

FlexConfig is a feature that allows the deployment of configuration directly to the Lina (ASA) configuration in the FTD. This can be used to deploy features that are not yet available in the FTD. There are two objectives for this lab exercise:

Configure EIGRP using a user defined FlexConfig object.

Use a system defined FlexConfig objects to disable SIP inspection.

**NOTE:** There are separate system defined FlexConfig objects for configuring EIGRP. For configurations that may change over time, it is better to use these objects. But to demonstrate the simplicity and power of FlexConfig, a user defined FlexConfig object will be used. System defined FlexConfig Objects will be used to configure the FTD as a source of NetFlow data.

# Steps

## Create user defined FlexConfig object

1. In the FMC UI, select **Objects > Object Management**.
2. On the left navigation panel, under **FlexConfig**, select **FlexConfig Object**.
3. Click **Add FlexConfig Object**.
   a. For Name, enter **myEIGRP**.
   b. In the main text area, enter the following commands.
      v. router eigrp 10
      vi. network 198.18.128.0 255.255.192.0
   c. Click **Save**.

## Modify a Text Object for a system defined FlexConfig object

You should still be on the **Object Management** page in the FMC UI.

1. Click on the magnifying glass icon to the right of the Flex Object called **Default_Inspection_Protocol_Disable**. You cannot edit this object, but you could copy it if you wanted to.

**NOTE:** The FlexConfig objects are written in the Apache Velocity language. This language supports loops and if statements. These begin with a #. This is not a comment. It indicates that the line is not literal text to be included in the output. Comments begin with ##.

**NOTE:** That this FlexConfig object loops over a text object called **disableInspectProtocolList**. You will now edit this text object.

Click **Close**.

**Object Management** page, under **FlexConfig**, select **Text Object.**

Edit the text object called **disableInspectProtocolList**.

a. This variable takes multiple values. Leave the value set to **1**.

b. Enter the value **sip**.

Click **Save**.

## Create and configure a FlexConfig policy

2. From the menu, select **Devices > FlexConfig. Click New Policy**.

   a. For Name, enter **NGFW1_Test Flex Policy**.

   b. Select the device **NGFW1**. Click **Add to Policy**.

   c. Click **Save**.

Wait a few seconds for the policy to open for editing.

a. In the left column, under **User Defined**, select **myEIGRP**. Click to add the FlexConfig object to the policy.

b. In the left column, under **System Defined,** select **Default_Inspection_Protocol_Disable.** Click to add the FlexConfig object to the policy.

3. Click **Save**.
4. Click **Preview Config**.
5. Select **NGFW1** from the **Select Device** drop-down list.
   a. Wait a few seconds and the configuration changes will appear. Confirm that the commands look correct.
6. Click **Close**.

## Deploy the changes and test the configuration

1. From the **NGFW1 CLI** run show running-config policy-map type inspect sip global_policy. Confirm that SIP inspection is enabled.
2. From the Inside Linux Server session, type **ping 204.44.14.1**. This should fail.

Deploy the changes you made. Wait until the deployment is complete.


From the NGFW1 CLI run show running-config policy-map type inspect sip global_policy. Confirm that SIP inspection is now disabled.

From the **NGFW1** CLI run **show eigrp neighbors**. Confirm that an adjacency has been formed between the FTD and CSR router.

From the **NGFW1** CLI run **show eigrp topology**. Confirm that the EIGRP routes have been received.

a. Look for network **203.14.10.0/24**

b. Ping **204.44.14.1** this should succeed.

**NOTE:** You will also see some routes that have no successors. These routes will be used in the next section BGP

Run show route eigrp. Confirm that the **NGFW1** now has EIGRP learned routes in its routing table.

# Scenario 4. NAT and Routing

This exercise consists of the following tasks.

Create objects needed for this lab exercise

Configure static NAT

Modify access control policy to allow outside access to wwwin

Configure BGP

Deploy the changes and test the configuration There are two objectives for this lab exercise:

Create a public web server

Create a DMZ web server

Configure BGP

The first objective will involve creating network objects, creating access control lists. Also, static NAT and dynamic routing will be configured.

**NOTE:** The public server will be deployed in the inside network. It would be more realistic to deploy this in a DMZ, but that would take more work. However, the lab pod has this capability. See Appendix 4 for information about creating a DMZ in the lab pod.

# Steps

## Create objects needed for this lab exercise

1. From the menu, select **Objects > Object Management**. The **Network** object page will be selected.
    a. Click **Add Network > Add Object**.
        i. For Name, enter **wwwin**.
            1. Click the Host Radio Button
            2. For Network, enter **198.19.10.202**.
            3. Click **Save**.
    b. Click **Add Network > Add Object**.
        i. For Name, enter **wwwout**.
            1. Click on the Host Radio Button
            2. For Network, enter **198.18.128.202**.
            3. Click **Save**.
2. Click **Add Network > Add Object**.
    a. For Name, enter **203.14.10.0**.
    b. Click on Network
    c. Enter **203.14.10.0/24**.
3. Click **Save**.

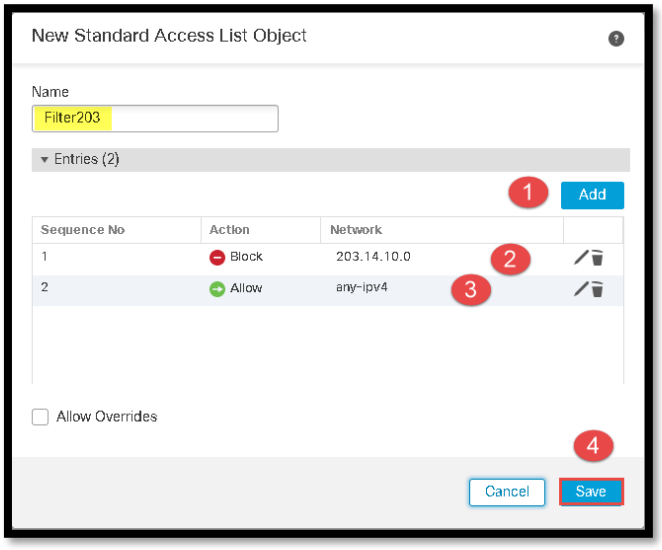
Select **Access List > Standard** from the left navigation pane.

a. Click **Add Standard Access List**.

b. For Name, enter **Filter203**.

c. Add the 2 access control entries shown below. The second entry is critical, because of an implicit deny all at the end of the list.

d. Click **Save**.



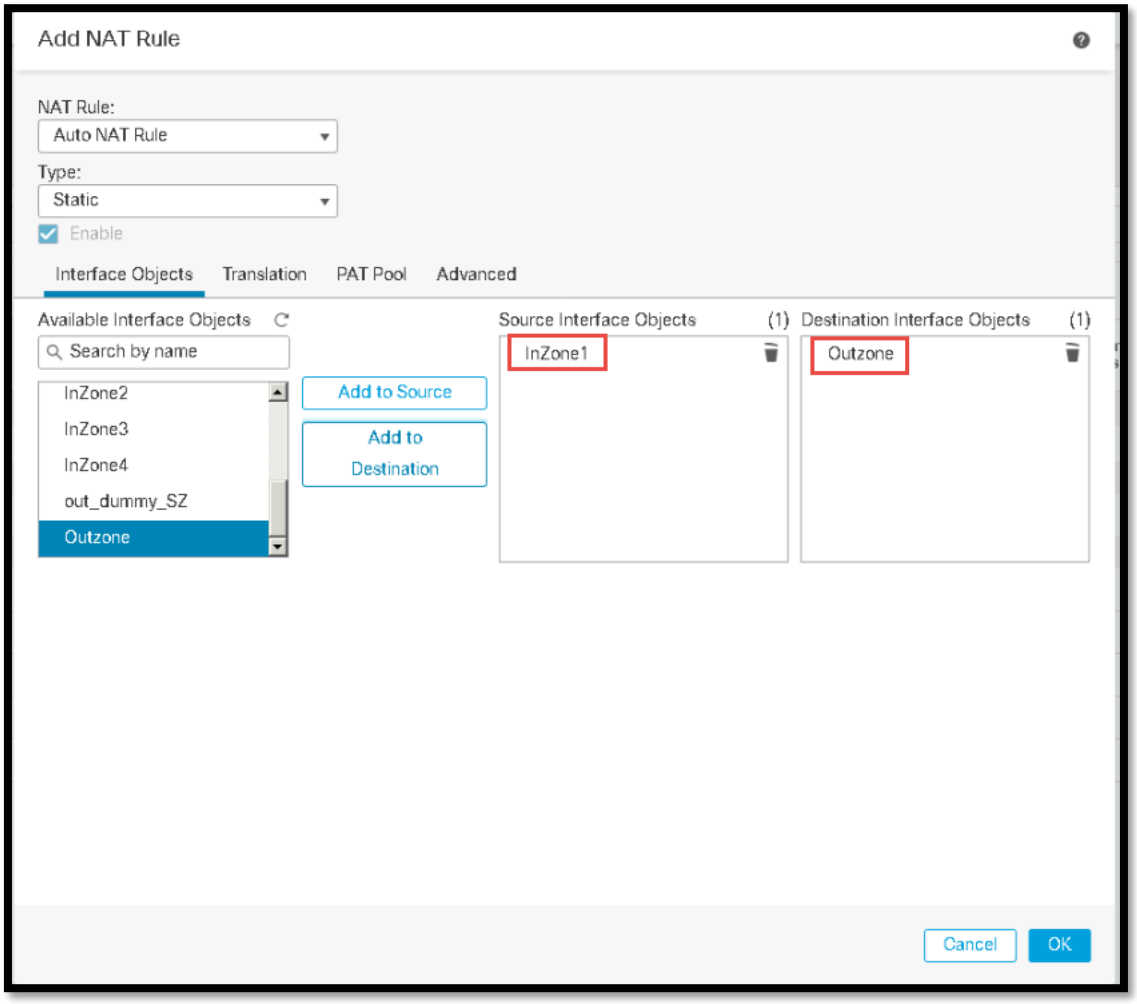

## Configure Static NAT

1. From the menu, select **Devices > NAT**.
2. Click the pencil icon to edit the **Default PAT** policy.
3. Click **Add Rule**.

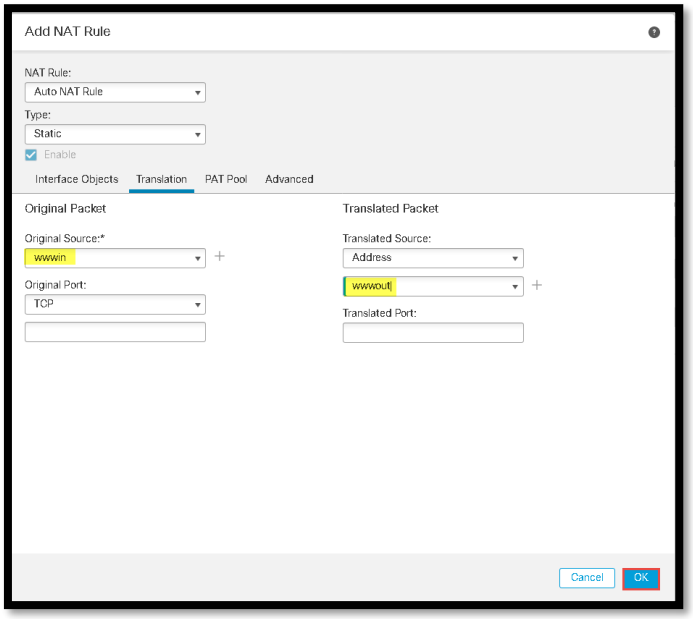
   a. Select **Auto NAT Rule** from the **Type** drop-down list.

   b. You will be at the Interface Objects tab. Select **InZone1** and click **Add to Source**.

   c. Select **OutZone** and click **Add to Destination**.



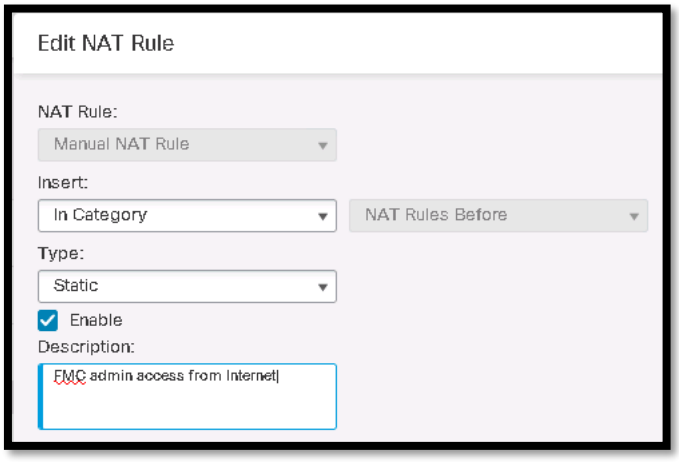

4. Select the **Translation** tab.
   a. Select **wwwin** from the **Original Source** drop-down list.
   b. Select **Address** and **wwwout** from the **Translated Source** drop-down list.



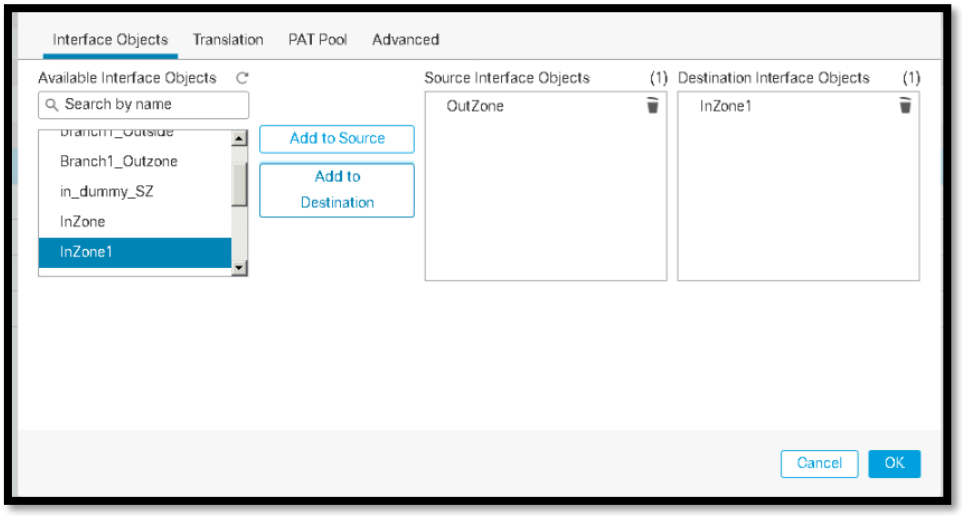

Click **OK** to save the NAT rule.

## NAT Existing IP Over Different Port

1. Edit the Default PAT policy
2. Click Add Rule
    a. NAT Rule: Manual NAT Rule
    b. Insert In Category: NAT Rules Before
    c. Type: Static
    d. Description: FMC admin access from Internet



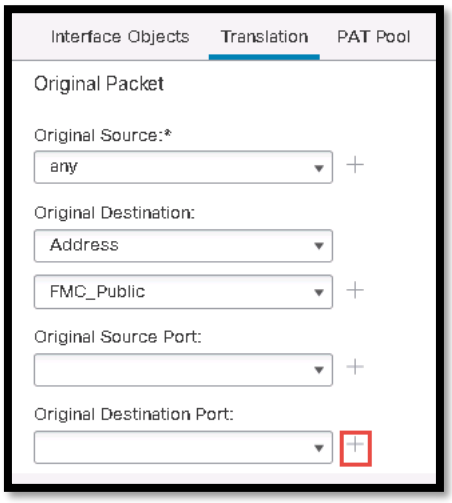

3. Interface Objects tab select **Outzone** for Source Interface Objects and **InZone1** to Destination Interface Objects




4. Select the Translation Tab

   a. Original Source: any

   b. Original Destination field: FMC_Public

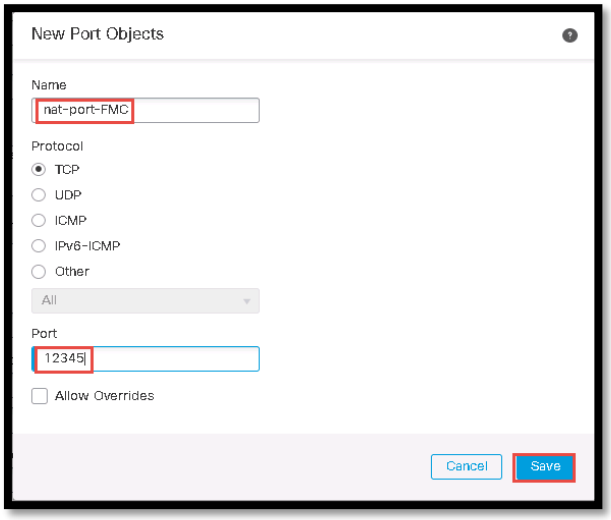



   c. Click on the [+] for Original Destination Port to add a new port object for the TCP port on the Outside interface

      i. Name: nat-port-FMC

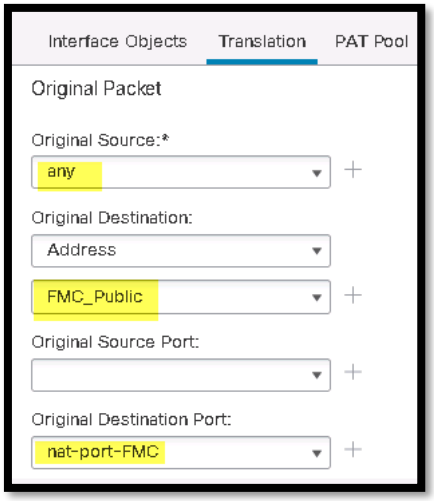
      ii. Protocol: TCP

      iii. Port: 12345




d. Click **Save**

e. Choose the nat-port-FMC object in the Original Destination Port field

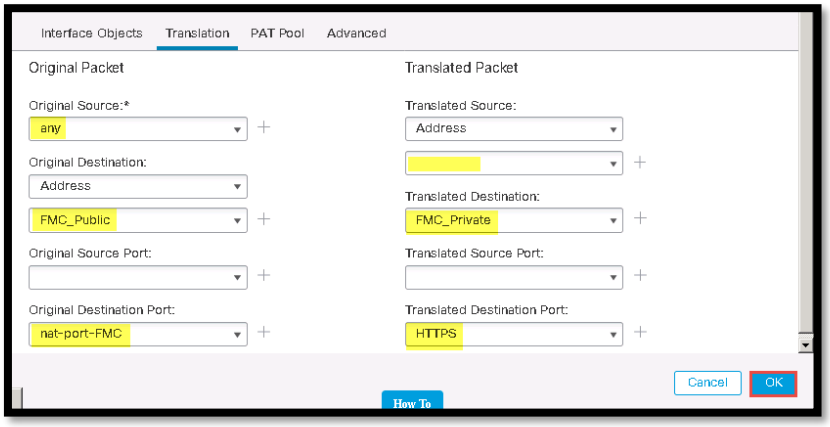



f. Translated Packet

i. Translated Source: Leave blank (will default to any)

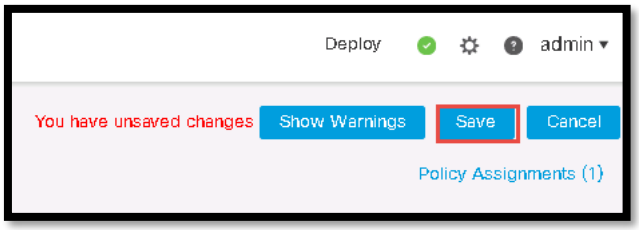
ii. Translated Destination: FMC_Private

iii. Translation Destination Port: HTTPS




iv. Click OK

5. Click **Save** at the top of the page




## Modify access control policy to allow outside access to wwwin

1. From the menu, select **Policies > Access Control > Access Control**.
2. Edit the NGFW Access Control Policy for example Base_Policy.
   a. Click **Add Rule**.
   b. For Name, enter **Web Server Access**.
   c. Select into **Default** from the Insert drop-down list.
   d. The Zones tab should already be selected. Select **InZone1** and click **Add to Destination**.
   e. Select **OutZone** and click **Add to Source**.
   f. Select the **Networks** tab.
   g. Select **wwwin** and click **Add to Destination**.
   h. Select **Ports**. Under Available Ports type **HTTP** and select **HTTP** and **HTTPS** and add to destination.
   i. Under Selected Destination Ports type in the Protocol box **ICMP select**. Click **Add**.

**NOTE**: We use the true IP of the webserver, instead of the NAT'ed address that the client will connect to.

   j. Select the **Inspection** tab.
   k. Select **Demo Intrusion Policy** from the **Intrusion Policy** drop-down list.

l. Select **Demo File Policy** from the **File Policy** drop-down list.

m. Select Logging: **Log at End of Connection**

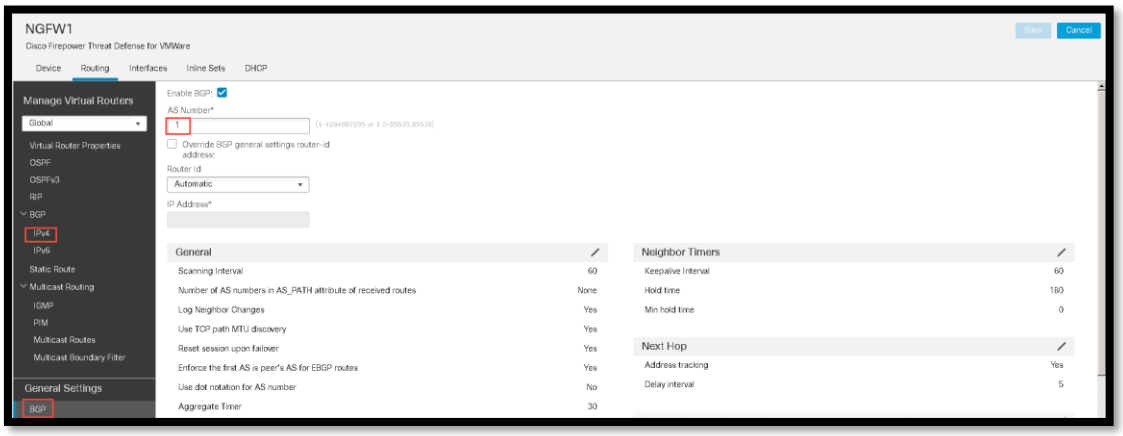
n. Click **Add**

## Modify access control policy to allow outside access to FMC via different port

1. Click on Policies > Access Control > Base_Policy to edit
2. Click Add Rule
   a. Name: **Allow External FMC Access**
   b. Action: **Allow**
   c. Enabled: **Checked**
   d. Insert: **into Mandatory**
3. Zones
   a. Source Zone: **OutZone**
   b. Destination Zone: **InZone1**
4. Networks
   a. Source: **any**
   b. Destination: **FMC_Private**
5. Ports
   a. Source: **any**
   b. Destination: **HTTPS**
6. Logging: **Log at End of Connection**
7. Click **Add**
8. Click **Save** to save the access control policy changes.

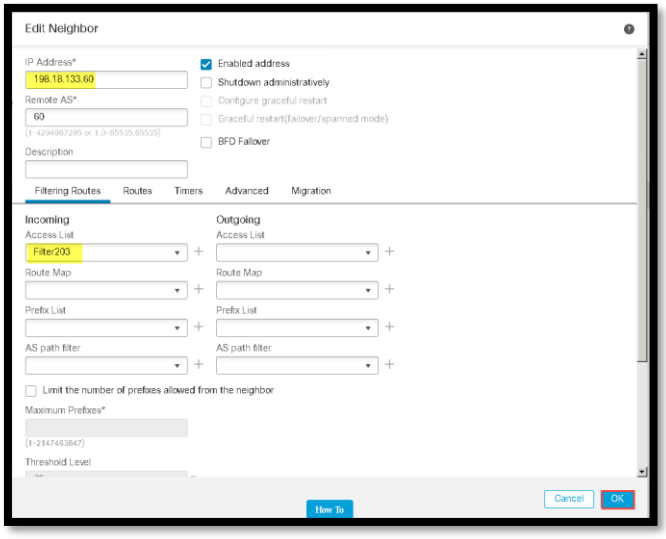
## Configure BGP

1. From the menu, select **Devices > Device Management**.
2. Click on the pencil icon to edit the device settings for the device **NGFW1**.
   a. Select the **Routing** tab.
   b. Go to General Setting Select **BGP and** check the **Enable BGP** checkbox.




c. Set the **AS Number** to **1**.

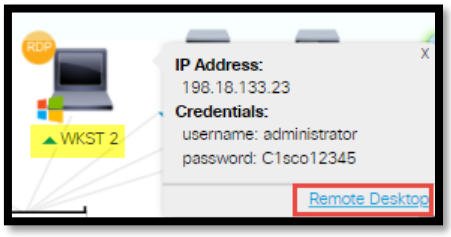
d. Expand **BGP** in the left navigation pane and select **IPv4**.
e. Check the **Enable IPv4** checkbox.
f. Click on the **Neighbor** tab and click on **Add**.
g. For **IP Address**, enter **198.18.133.60**.
h. For **Remote AS**, enter **60**.
i. Check the **Enable address** checkbox.
j. Select **Filter203** from the Incoming Access List drop-down list.
k. Click **OK** to add the neighbor.




3. Click **Save** to save the BGP configuration.

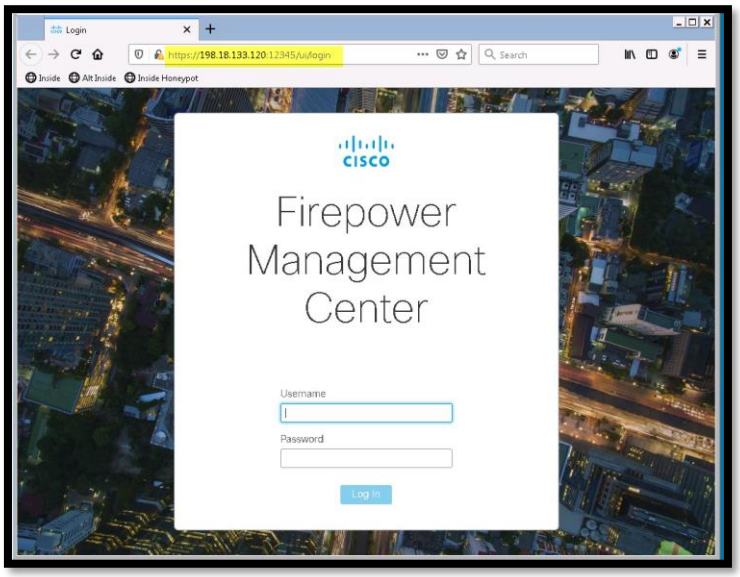
## Deploy the changes and test the configuration

1. Deploy the changes and wait until the deployment is complete.
2. On the Jump desktop, open the PuTTY link. Double click on the preconfigured session called **Outside Linux Server**. Login as **root**, password **C1sco12345**
   a. Type **curl wwwout**. This should succeed.
   b. Type **ssh wwwout**. This should fail.
3. Return to the dCloud session page in your computer's we browser that shows the diagram of the lab environment. Find the **WSKT2** machine, click the arrow icon and then select **Remote Desktop** link to connect to the **WKST2** machine

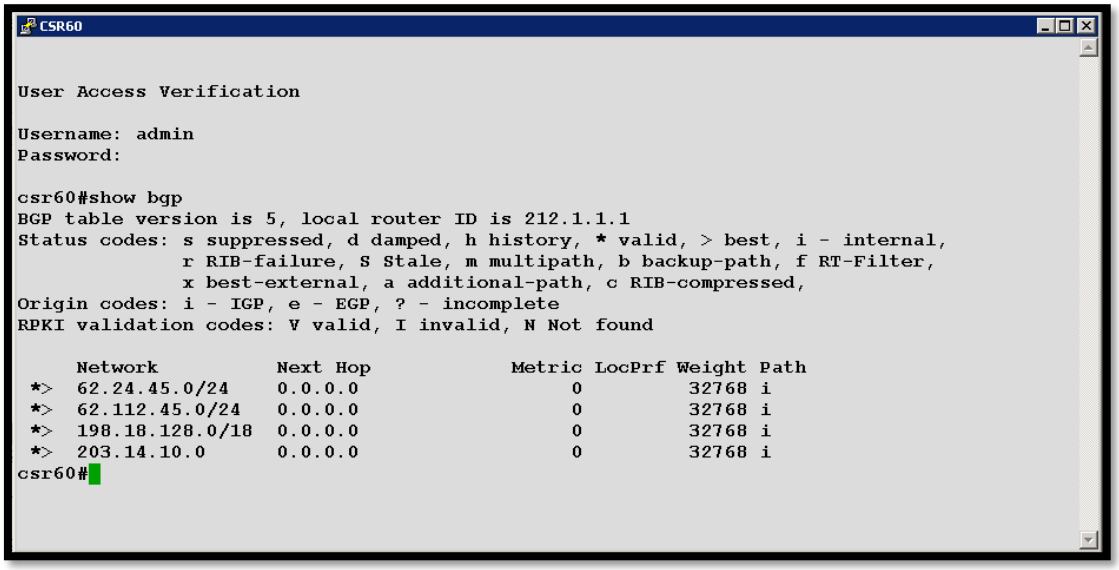



4. Open the **Firefox** web browser by double-clicking


5. Enter the address below in the address bar of the browser and press enter
   a. **https://198.18.133.120:12345**
   b. If prompted accept the risks. You should get the following:




6. Go back to the Jump desktop, open the PuTTY link. Double click on the preconfigured session called **CSR60**. Login as **admin**, password **C1sco12345**
   a. On the CSR CLI, run the command **show bgp**, and confirm that 4 routes appear.




4. From the **NGFW1** CLI:
5. Run **show route** or **show route bgp**. Confirm that the only routes learned from BGP were **62.24.45.0/24** and **62.112.24.0/24**.

a. Note that **203.14.10.0/24** was successfully filtered out of BGP. However, if you performed the FlexConfig scenario, you will see this route as an external EIGRP route.

6. Run **show bgp** and **show bgp rib-failure**. This shows that the 198.18.128.0/18 route was not inserted in the routing table because there was a better route (connected).

**NOTE:** You can also run the following commands from the FMC.

7. From the menu, select **Device > Device Management**.
8. Edit the **NGFW1** device and select the **Devices** tab.
9. Click on the Wrench and Hammer Icon
10. Click **Advanced Troubleshooting**.
    a. Select the **Threat Defense CLI** tab. From this tab, you can run several NGFW CLI commands.
        i. Command Show:
            1. Route and the Execute button
            2. BGP and the Execute button
            3. eigrp neighbors and the Execute button
11. From the Inside Linux server session, type **ping 62.24.45.1**. This should succeed.

# Scenario 5. Prefilter Policies

This exercise consists of the following tasks.

Investigate NGFW default behavior for tunneled traffic

Create a tunnel zone

Create a prefilter policy

Modify the access control policy

Deploy the changes and test the configuration

If there is a clear-text tunnel, the NGFW access control policies apply to the **tunneled** traffic. Prefilter policies give control over the **tunneling** protocol. The following tunneling protocols are supported.

GRE

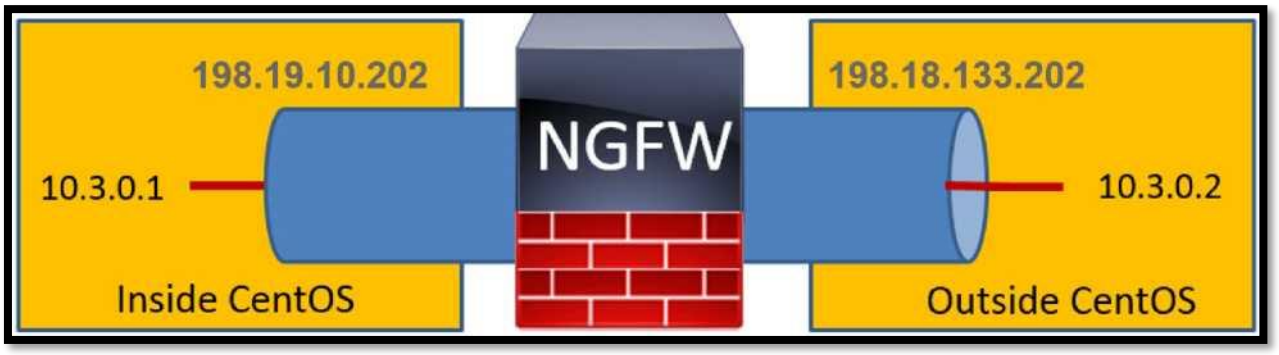
IP-in-IP

IPv6-in-IP

Teredo

Prefilter policies communicate with access control policies via tunnel tags. The prefilter policy assigns tunnel tags to specified tunnels. The access control policy can then include rules that only apply to traffic tunneled through those specified tunnel.

In this exercise, you will create a GRE tunnel between the inside and outside CentOS servers.




You will then configure the NGFW to block ICMP through this GRE tunnel.

**NOTE:** This exercise has Scenario 4 as a prerequisite. This is because the exercise assumes the static NAT rule, which translates 198.19.10.202 to 198.18.128.202. To understand the configuration of the tunnel interface, you can inspect **/etc/sysconfig/network-scripts/ifcfg-tunO** on the inside and outside servers.

# Steps

## Investigate NGFW default behavior for tunneled traffic

In this task, you will confirm that the access control policy rules apply the tunneled traffic.

1. You should still have the SSH session open to the Inside Linux server.

2. If you do not have an SSH session to the Outside Linux Server, from the Jump desktop, launch PuTTY and double-click on the pre-definite **Outside Linux Server** session. Login as **root**, password **C1sco12345**
3. Create a GRE tunnel between the Inside Linux server and Outside Linux server.
    a. On the Outside Linux Server CLI, type **ifup tun0**.
    b. On the Inside Linux Server CLI, type **ifup tun0**.
    c. On the Inside Linux Server, confirm that you can ping through the tunnel with the following command. **ping 10.3.0.2**

## Test the IPS capabilities.

1. Modify the Base_Policy ICMP Permit Access rule to allow for HTTP, HTTPS, FTP and make sure Demo File and Intrusion Policy are enabled
2. Run the following command from the Inside Linux Server CLI. ftp 10.3.0.2
    a. Login as **guest**, password **C1sco12345**
    b. Type **cd ~root**. You should see the following message:
    c. 421 Service not available, remote server has closed connection.
    d. Type **quit** to exit FTP.
3. In the FMC, from the menu, select **Analysis > Intrusions > Events**.
    a. Click the arrow on the left to drill down to the table view of the events.
    b. Observe that the source and destination IPs are 10.3.0.1 and 10.3.0.2, respectively.
4. Test the file and malware blocking capabilities by running the following commands on the **Inside Linux server CLI**.

**NOTE:** These Wget commands can be cut and pasted from the file on the Jump desktop called Strings to cut and paste.txt.

    a. As a control test, use WGET to download a file that is not blocked. **wget -t 1 10.3.0.2/files/ProjectX.pdf.**
    b. This should succeed.
    c. Next use WGET to download the file blocked by type: **wget -t 1 10.3.0.2/files/test3.avi.**

**NOTE:** Very little of the file is downloaded. This is because the NGFW can detect the file type when it sees the first block of data.

    d. Finally use WGET to download malware.
    e. **wget -t 1 10.3.0.2/files/Zombies.pdf**

**NOTE:** About 99% of the file is downloaded. This is because the NGFW needs the entire file to calculate the SHA. The NGFW holds onto the last block of data until the hash is calculated and looked up.

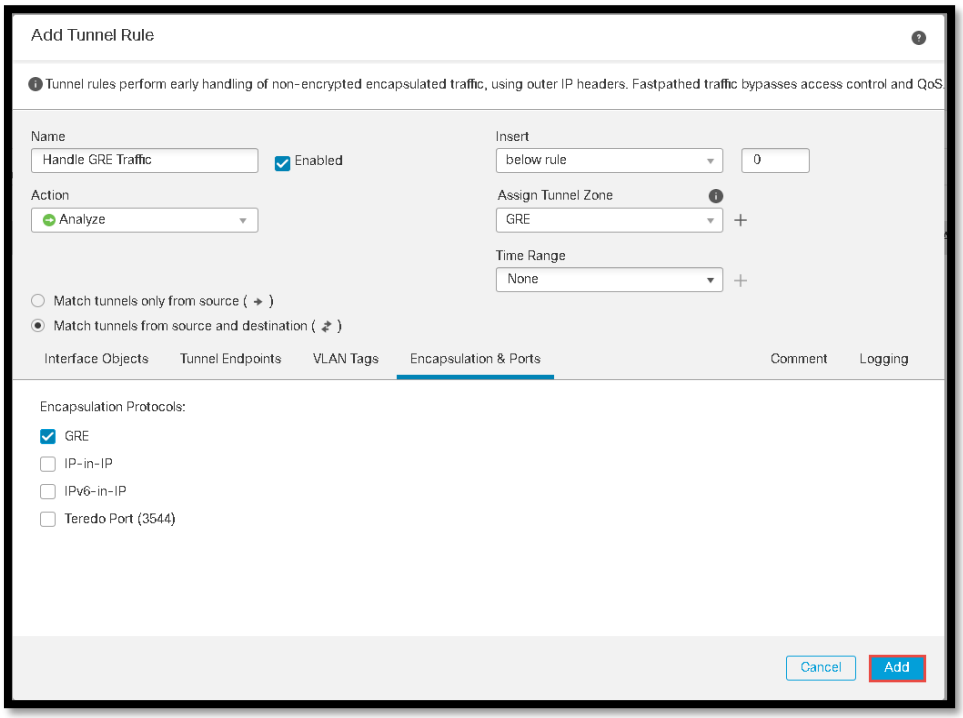
5. In the FMC, from the menu, select **Analysis > Files > File Events**.
    a. Click **Table View of File Events**.
    b. Observe that the sending and receiving IPs are 10.3.0.2 and 10.3.0.1, respectively.

## Create a tunnel zone

1. From the menu, select **Objects > Object Management**.
    a. Select **Tunnel Zone** from the left navigation pane.
    b. Click **Add Tunnel Zone**.
    c. For **Name**, enter **GRE**.
    d. Click **Save**.

## Create a prefilter policy

1. From the menu, select **Policies > Access Control > Prefilter**.
    a. Click **New Policy**. Enter a name such as **ngfw1 Prefilter** Policy. Click **Save**.
    b. Wait a few seconds for the policy to open up for editing.
2. Click **Add Tunnel Rule**.
    a. For Name, enter **Handle GRE Traffic**.
    b. Select **GRE** from the **Assign Tunnel Zone** drop-down list.
    c. Select the **Encapsulation & Ports** tab and check the **GRE** checkbox.



**NOTE:** There are 3 actions.

Analyze - traffic will be passed to Snort, and access policy rules will apply.

Block - traffic is blocked.

Fastpath - traffic is allowed, and bypasses any further inspection.

**NOTE**: You can also create prefilter rules for this policy. This gives you the ability to analyze, block or fast path traffic based on layer 2 through 4 information.

3. Click **Add** to add the rule.
4. Click **Save** to save the prefilter policy.

## Modify the access control policy

1. From the menu, select **Policies > Access Control > Access Control** to edit the NGFW Base_Policy Access Control Policy.

Click on the link **Default Prefilter Policy** to the right of the string **Prefilter Policy** above the policy rules.

Select **NGFW Prefilter Policy**.

Click **OK**.

a. Modify the Allow Outbound ICMP **Rule**.

b. Rename the rule **Block ICMP Over GRE**.

c. Select Move **into Mandatory** from the **Insert** drop-down list.

d. Set the action to **Block with reset**.

e. In the **Available Zones** column, **Delete All Zones and** select **GRE** and click **Add to Source.**

f. In the **Available Applications** column, make sure that **Only ICMP** is selected.

g. Select the **Logging** tab. Check the **Log at Beginning of Connection** checkbox.

   a. If prompted Send Connection Events to **Firepower Management Center**

h. Make sure Inspection and File Policies are removed

i. Click **Save** to add the rule to the policy.

Click **Add Rule**.

a. Call the rule **Allow GRE Traffic**.

b. Select into **Default** from the Insert drop-down list. This will become the last rule in the access control policy.

c. In the **Available Zones** column, select **GRE** and click **Add to Source**.

d. Select the **Inspection** tab.

e. Select Demo Intrusion Policy from the **Intrusion Policy** drop-down list.

f. Select Demo File Policy from the **File Policy** drop-down list.

g. Click **Add** to add the rule to the policy.

h. Click **Save** to save the access control policy.

## Deploy the changes and test the configuration

1. Deploy the changes, as you have been. Wait for the deployment to complete.

On the Outside Linux Server, run **tcpdump -n -i tun0** to monitor tunnel traffic**.**

   a. Run the following commands on the Inside Linux Server CLI.

   b. **wget 10.3.0.2** This should succeed.

   c. **ping 10.3.0.2**

2. You should see the following output, indicating that the ping is being blocked.

```
From 10.3.0.2 icmp_seq=1 Packet filtered
```

   a. **If no success go to step 4 below to reset the tunnels**

3. Inspect the output of the **tcpdump** command on the Outside Linux Server to confirm that the ping is not making it to 10.3.0.2.
   a. If you are not getting the results above
      i. Tear down tunnel:
         1. On the Outside Linux Server CLI, type Ctrl C then **ifdown tun0**.
         2. On the Inside Linux Server CLI, type **ifdown tun0**.
      ii. Re-establish the tunnel:
         1. Retest
         2. If you still do not see results from above
      iii. On the FMC **Analysis > Connections > Events**
         1. Look for traffic from 10.3.0.1 to 10.3.0.2
         2. You should see Block with reset for ICMP traffic

4. Create a GRE tunnel between the Inside Linux server and Outside Linux server.
   a. On the Outside Linux Server CLI, type **ifup tun0**.
   b. On the Inside Linux Server CLI, type **ifup tun0**.
   c. On the Inside Linux Server, confirm that you can ping through the tunnel with the following command. **ping 10.3.0.2**

5. Tear down the tunnel:
   a. On the Outside Linux Server CLI, type Ctrl C then **ifdown tun0**.
   b. On the Inside Linux Server CLI, type **ifdown tun0**.