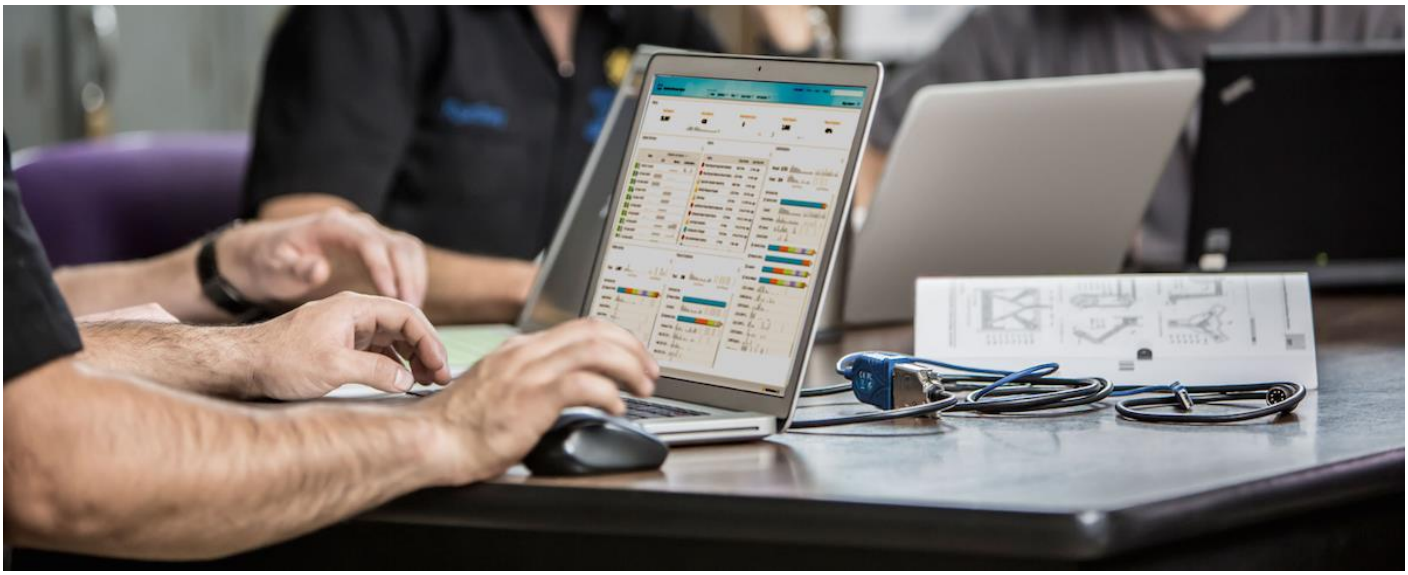


Configuring NSEL on Cisco Firepower Threat Defense (FTD)

How to configure NSEL (~NetFlow) on Cisco Firepower Threat Defense (FTD) using the FlexConfig feature introduced in Firepower Management Center (FMC) software version 6.2

Author - Anand Kanani

Technical Marketing Engineer – Stealthwatch and AMP

Version 1.0 – 06/Mar/2017

Table of Contents

About This Document

This document provides an overview of the configuration options used to configure Cisco Next-Generation Firewall (NGFW) platform running Firepower Threat Defense (FTD) to export NetFlow Secure Event Logging (NSEL) to Cisco Stealthwatch. This document also covers the benefits of enabling NSEL on FTD, how the flow information from NSEL is displayed in the Cisco Stealthwatch Management Console (SMC), and basic troubleshooting tasks.

This document has been created using:

- Virtual NGFW platform running Firepower Threat Defense (FTD) version 6.2
- Virtual Firepower Management Center (FMC) version 6.2
- Virtual components of Stealthwatch version 6.8.3

About NSEL on Firepower Threat Defense (FTD)

The NSEL feature is available on FTD software starting version 6.2 and later.

The Firepower Threat Defense (FTD) and Adaptive Security Appliance (ASA) implementations of NSEL provide a stateful, IP flow tracking method that exports specific records that indicate significant events in a flow. The important information obtained from NSEL on FTD with respect to Cisco Stealthwatch are whether the flow was permitted or denied by the pre-filter policy on FTD and the Network Address Translation (NAT) details.

In FTD version 6.2, NSEL is configured through ASA-based CLI syntax using the FlexConfigs feature available in Firepower Management Center (FMC).

For more information about Cisco Next-Generation Firewalls (NGFW) and FTD, please visit: http://www.cisco.com/go/ngfw

About FlexConfigs on Firepower Management Center (FMC)

FlexConfigs is a new feature available in Firepower Management Center starting software version 6.2.

A FlexConfig policy is a container of an ordered list of objects. Each object includes CLI-based configuration commands. It can also optionally include scripting commands and locally defined variables. The contents of each FlexConfig object is a program that generates a sequence of CLI commands that will then be deployed to the assigned devices. This command sequence then configures the related feature on the FTD.

FlexConfigs are used to configure features that are not supported directly through FMC policies and settings.

For more information on the FlexConfigs feature, please visit the configuration guide of FMC version 6.2 located here:
www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/FlexConfig_policies.html

In simple words, FlexConfig consists of two types of objects:

1- FlexConfig objects
2- Text objects

The FlexConfig objects usually contain a fixed set of commands and calls to the variables for the user-provided parameters like IP addresses or any other attributes required by those commands. There are many predefined FlexConfig objects provided for tested configurations for select features like NSEL configuration, EIGRP routing configuration, etc. The predefined FlexConfig objects are read-only and hence cannot be modified. For any change, make a copy of the existing FlexConfig object and then edit them.

FlexConfig Text objects are associated with variables used in the predefined FlexConfig objects. There are several predefined Text objects and they are all associated with one or more FlexConfig objects. In most cases, edit these Text objects to add values if the associated FlexConfig objects are used. Without providing proper values to the associated Text object, errors will occur during the deployment of a FlexConfig objects / policy. Although some of these objects contain default values, others are empty and must be explicitly defined.

FlexConfig Objects for NSEL on FMC version 6.2

In FMC software version 6.2, several pre-defined FlexConfig objects and associated text objects are provided which facilitate the configuration of NSEL on the FTD. The FlexConfig objects contain the commands, and the variable attributes are to be added only in the text objects.

There are four pre-defined FlexConfig objects available for NSEL configuration in FMC software version 6.2. Below are their definitions and the list of associated text objects. Edit and set the values of these text objects before deploying the configuration on the FTD.

Table 1. Pre-defined FlexConfig objects available in FMC for NSEL configuration on FTD

FlexConfig Object Name	Description	Associated Text Objects
Netflow_Add_Destinations	Creates and configures a NetFlow export destination	netflow_Destinations, netflow_Event_Types
Netflow_Clear_Parameters	Restores NetFlow export global default settings	-
Netflow_Delete_Destinations	Deletes a NetFlow export destination	netflow_Destinations, netflow_Event_Types
Netflow_Set_Parameters	Sets global parameters for NetFlow export	netflow_Parameters

Below is the table of the definition of the FlexConfig Text objects available for NSEL configuration in FMC software version 6.2.

Table 2. Pre-defined FlexConfig objects available in FMC for NSEL configuration on FTD

FlexConfig Text Object Name	Description	Associated FlexConfig Objects
netflow_Destinations	Defines a single NetFlow export destination's interface, destination, and UDP port number.	Netflow_Add_Destinations
netflow_Event_Types	Defines the types of events to be exported for a destination as any subset of: all, flow-create, flow-defined, flow-teardown, flow-update.	Netflow_Add_Destinations
netflow_Parameters	Provides the NetFlow export global settings: active refresh interval (number of minutes between flow update events), delay (flow create delay in seconds; default 0 = command will not appear), and template time-out rate in minutes.	Netflow_Set_Parameters

Steps to Configure NSEL on FTD

This section defines the steps to add, update, and remove NSEL configuration on FTD.

To Add the NSEL Configuration on FTD

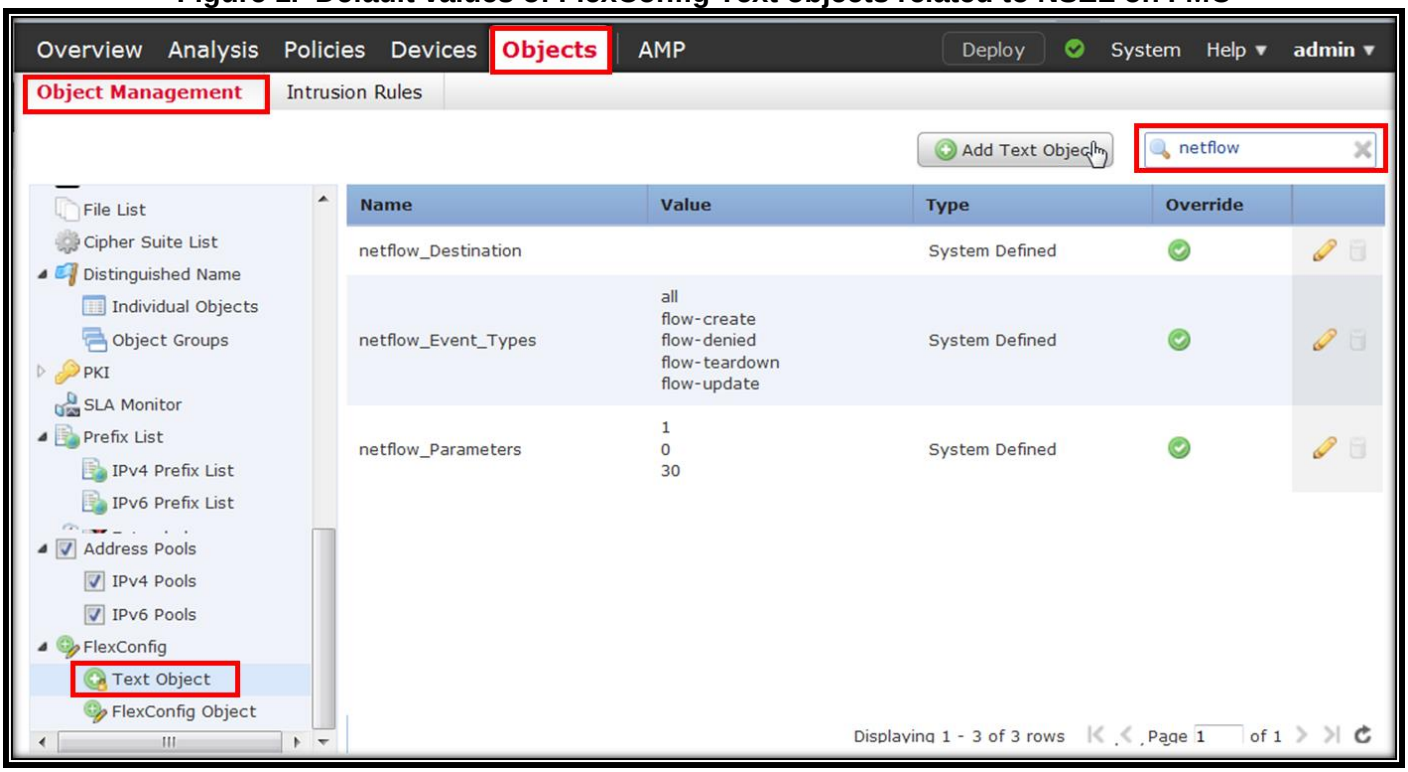
Step 1: Set the parameters of the FlexConfig Objects

Navigate to *Objects -> Object Management*. From the menu on the left, scroll down towards the bottom and select ***FlexConfig -> Text Object***.

For better visibility, in the search filter on top right, search for **netflow.** This will return 3 objects by default - **netflow_Destinations, netflow_Event_Types, netflow_Parameters.**

The values of these objects needs to be set in this step.

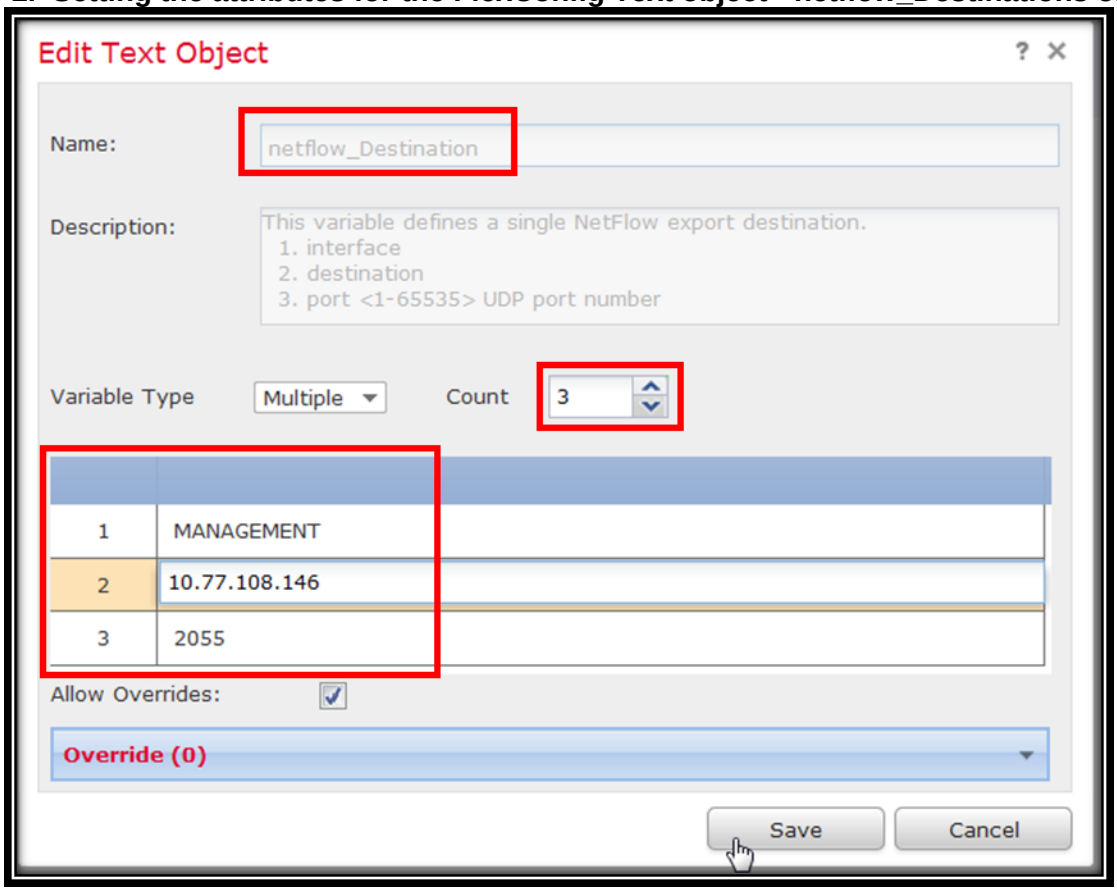
Figure 1. Default values of FlexConfig Text objects related to NSEL on FMC



For the Text object - **netflow_Destinations,** define the single NetFlow export destination's interface, destination IP (In this case, the Stealthwatch Flow Collector's IP address), and UDP port number for NetFlow (The Stealthwatch default is UDP 2055). To input these values, click on the ***edit*** icon, next to this Text object. ***Change*** the value of the Variable count to **3.** Set the value of the

3 variables to **MANAGEMENT**, **<Flow Collector's IP address>** and **2055** respectively. These values will now commonly apply to all the NGFWs running FTD to which these FlexConfig objects are defined. If the values need to be different for particular NGFWs, then use the option ***Allow override.*** In order to use any override values, ***check*** the ***checkbox*** for ***Allow Overrides.*** This will enable the values to be overridden. Select any device from the list of available NGFWs running FTD where the value needs to be overridden and add the specific values. Click ***Save*** to save the Text object.

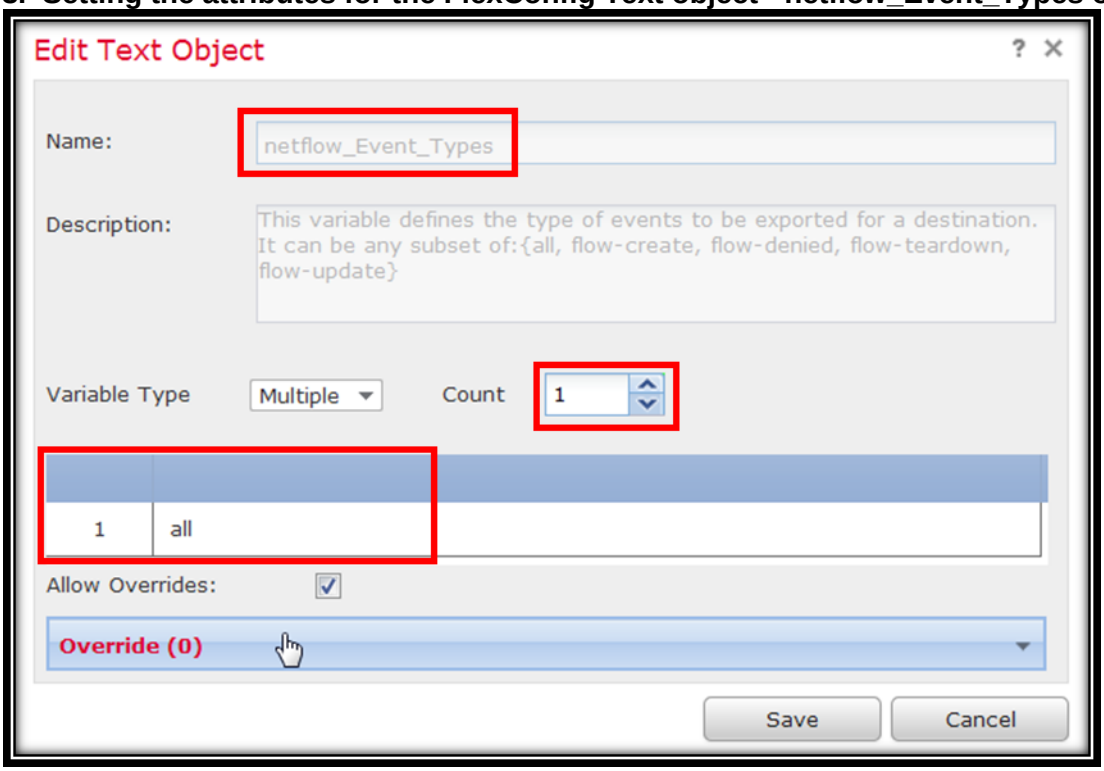
Figure 2. Setting the attributes for the FlexConfig Text object - netflow_Destinations on FMC



Similarly, for the Text object - **netflow_Event_Types,** keep **all** and remove the rest of the event types by lowering the ***count*** field.

Note: It is recommended to export ***all*** type of flow-events to Stealthwatch Flow Collector.

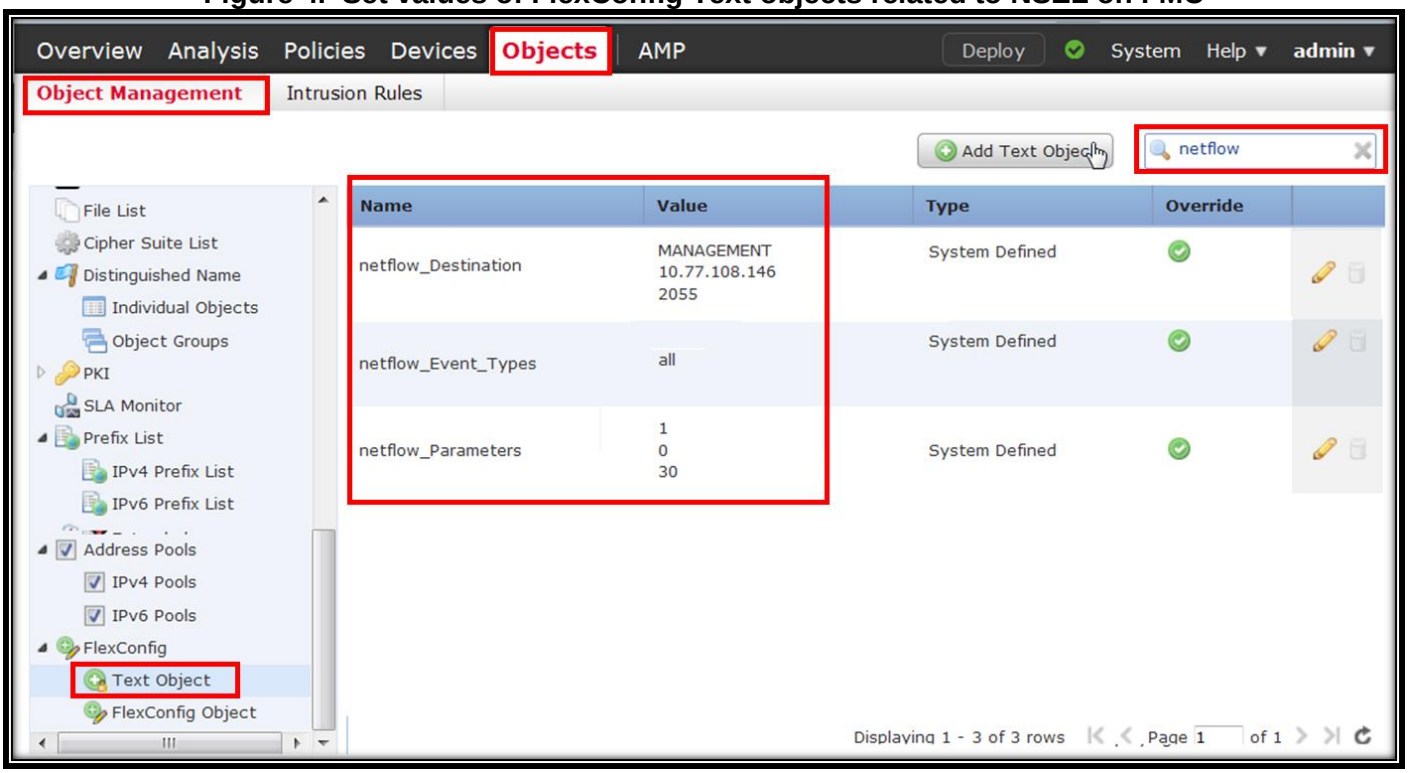
Figure 3. Setting the attributes for the FlexConfig Text object - netflow_Event_Types on FMC



For the Text object - **netflow_Parameters,** the default values should look like **1 0 30.** These values are for active refresh-interval, delay flow-create, and template timeout-rate.

Note: In most of the cases, it is recommended to keep these values as their default settings.

Figure 4. Set values of FlexConfig Text objects related to NSEL on FMC



Step 2: Configure the Diagnostic0/0 or MANAGEMENT interface on FTD

Navigate to ***Devices -> Device Management.*** From the list of NGFWs running FTD, select the NGFW to be configured. This will open the ***Interfaces tab*** for that particular NGFW.

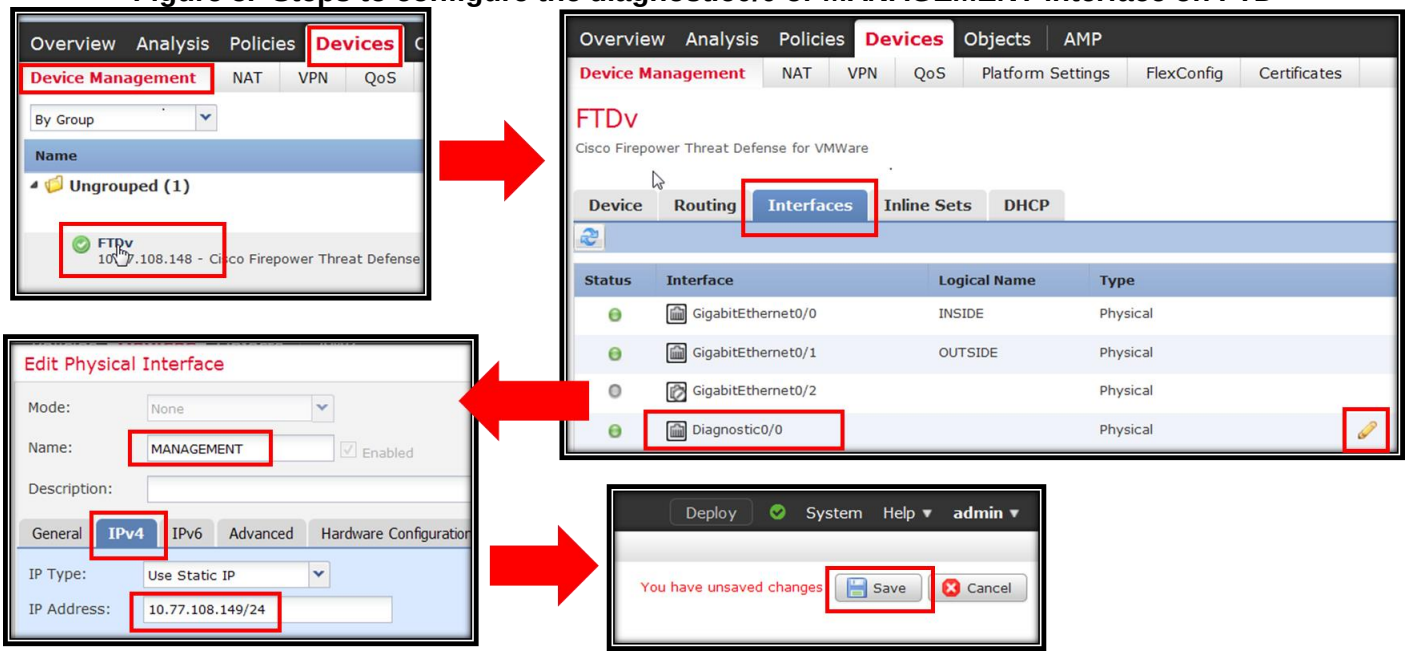
Provide an IP address to the interface that will be sending the NetFlow. Usually this should be the **management interface - Diagnostic0/0**.

Note: Alternatively, a different physical / logical interface may also be used for exporting NetFlow instead of the diagnostic0/0 interface. The process to configure the interface remains the same as given below.

Configure the ***Logical Name*** and ***IP address*** for this interface, if not already done earlier. Click on the edit (Pencil icon) for the Diagnostic0/0 interface.

Set the name as **MANAGEMENT** and click on the ***IPv4*** tab to set the IP address and prefix. **The IP address provided here must be in the same subnet as the Management interface of the FTD.** Click ***OK*** and then ***Save***.

Figure 5. Steps to configure the diagnostic0/0 or MANAGEMENT interface on FTD



Step 3: Add the FlexConfig Policy on FMC and assign it to FTD

Navigate to ***Devices -> FlexConfig***. Click on ***New Policy***.

Name it **FTD-FlexConfig** and put a description (optional).

From the list of available NGFWs running FTD, select the NGFW to apply this FlexConfig Policy and click ***Add to Policy***. Click ***Save***.

From the list of Available FlexConfig Objects, search and add **Netflow_Set_Parameters** and **Netflow_Add_Destinations** objects to the policy. The object gets added to the ***Selected Append FlexConfigs*** table.

Click ***Save***.

Optionally, verify the full FlexConfig Policy to be deployed on a particular NGFW by clicking on the ***Preview Config*** button in the top-right and selecting the particular NGFW from the drop-down list.

NOTE: Only one FlexConfig Policy can be applied per device. However, there can more than one FlexConfig objects set in a single FlexConfig Policy.

Figure 6. Steps to add the FlexConfig Policy on FMC and assign it to FTD

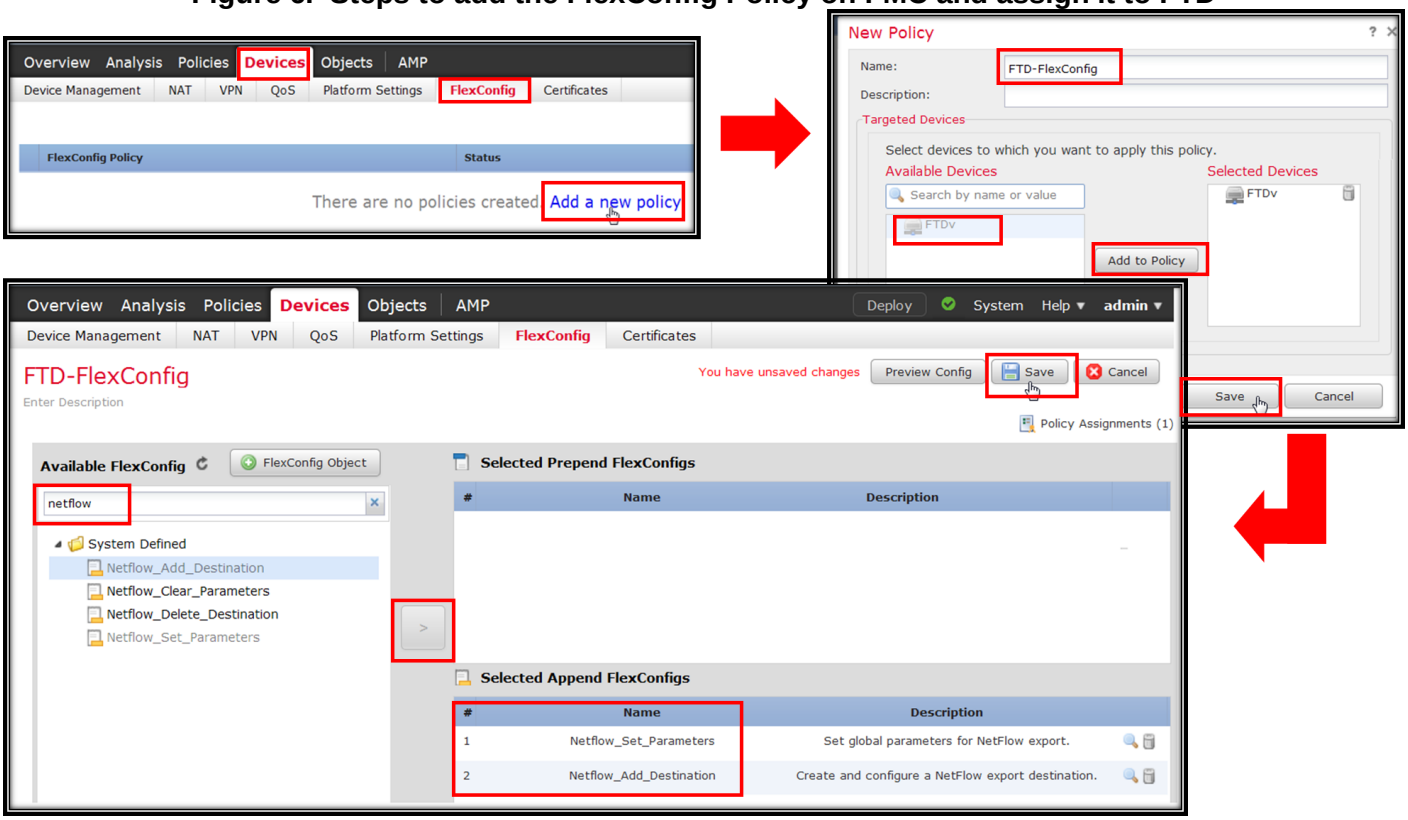


Figure 7. Preview the added FlexConfig Policy on FMC

Step 4: Add the Platform Policy on FMC for SNMP read-only configuration and assign it to FTD (optional)

This is an optional step to enable SNMP Polling from the **Stealthwatch Management Console (SMC).** This will enable the SMC to show the details like the Logical Names of the FTD's interfaces instead of names like ifIndex-x, interface utilization, etc.

Navigate to ***Devices -> Platform Settings.*** Click ***New Policy*** and select ***Threat Defense Settings.***

Name it **FTD Platform Policy** and put a description (optional).

From the list of available devices, select the NGFWs to apply this Platform Settings Policy and click ***Add*** to Policy. Click ***Save.***

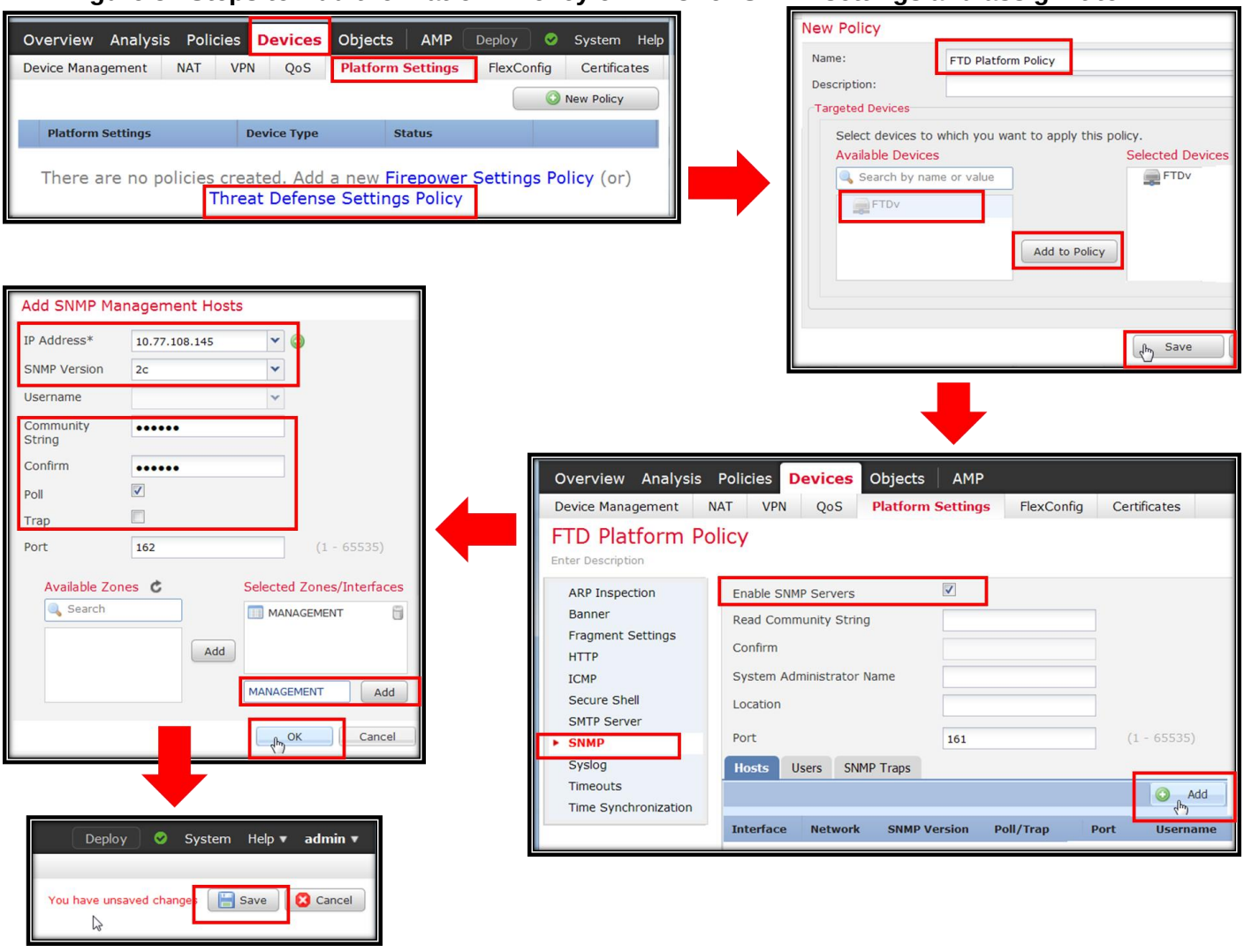
In the FTD Platform Policy, from the list of settings on the left, select ***SNMP.*** Check the box ***Enable SNMP Servers.***

In the ***Hosts tab***, click ***Add***. Put the <**IP address of SMC>**, select the ***SNMP version*** (usually **2c**), add the ***community string*** and confirm (usually this is **public**), and ***Uncheck Trap***. In the

Selected Zones/Interfaces box, ***type the Interface Name as MANAGEMENT*** (in this case) and click ***Add*** and then click ***OK***.

Click ***Save***.

Figure 8. Steps to Add the Platform Policy on FMC for SNMP settings and assign it to FTD



Step 5: Deploy the Configuration on the NGFW and verify on SMC

Click ***Deploy*** in the top-right. Select the NGFW on which the policy is supposed to be deployed. Click ***Deploy*** to finish.

Check on the deployment status. If the deployment succeeds, then the NGFW should appear in the **Stealthwatch Management Console (SMC)** in the Flow Exporters list once there is traffic

flowing through the FTD. It may take more than a minute for the NGFW to appear in the SMC, so be patient.

IMPORTANT: The NGFW appears in the SMC with the IP address of the diagnostic0/0 interface named as MANAGEMENT. Note that this is NOT the same IP address used to link NGFW to FMC.

If there is any kind of firewalling, then make sure that the traffic is allowed from the MANAGEMENT interface IP of the NGFW to the Flow Collector on UDP port 2055 for NSEL (or whatever that is configured on the NGFW). This MANAGEMENT IP address is the IP address of the diagnostic0/0 interface.

In case if the NGFW does not appear even after 4-5 minutes in the SMC, then try the steps given in Troubleshooting Common Issues section below.

Figure 9. Steps to Add the Platform Policy on FMC for SNMP settings and assign it to FTD

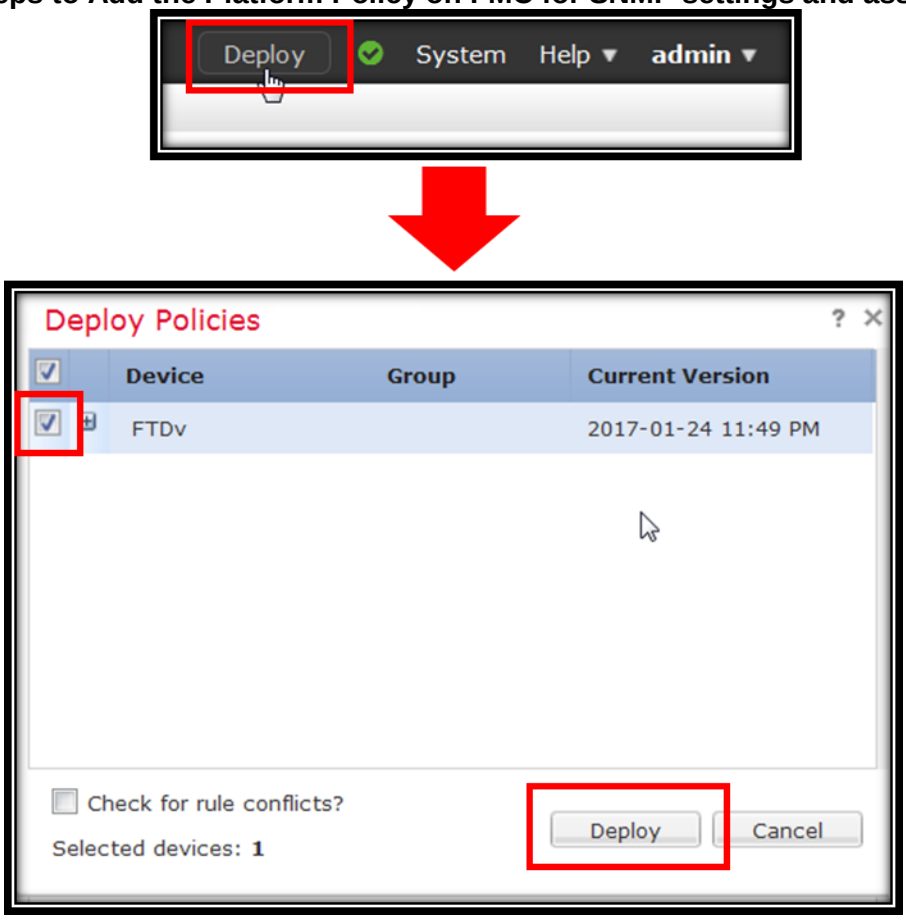
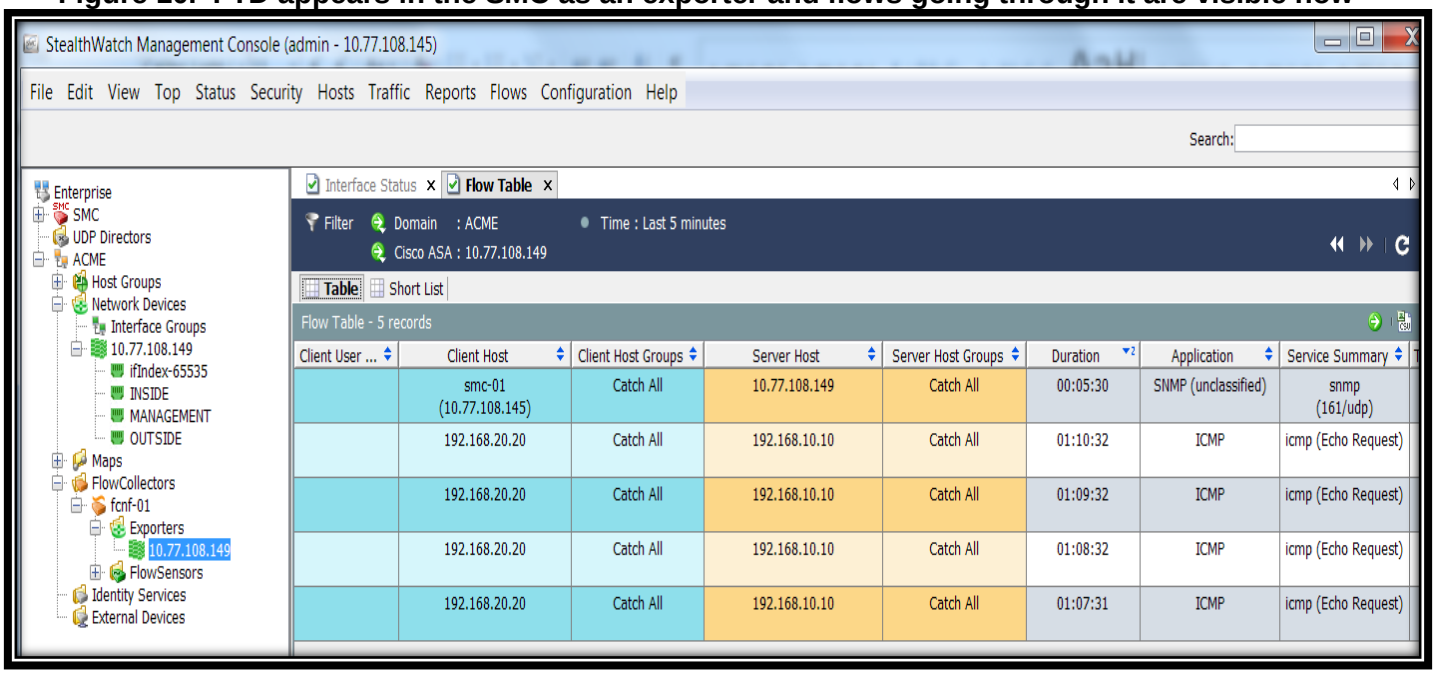
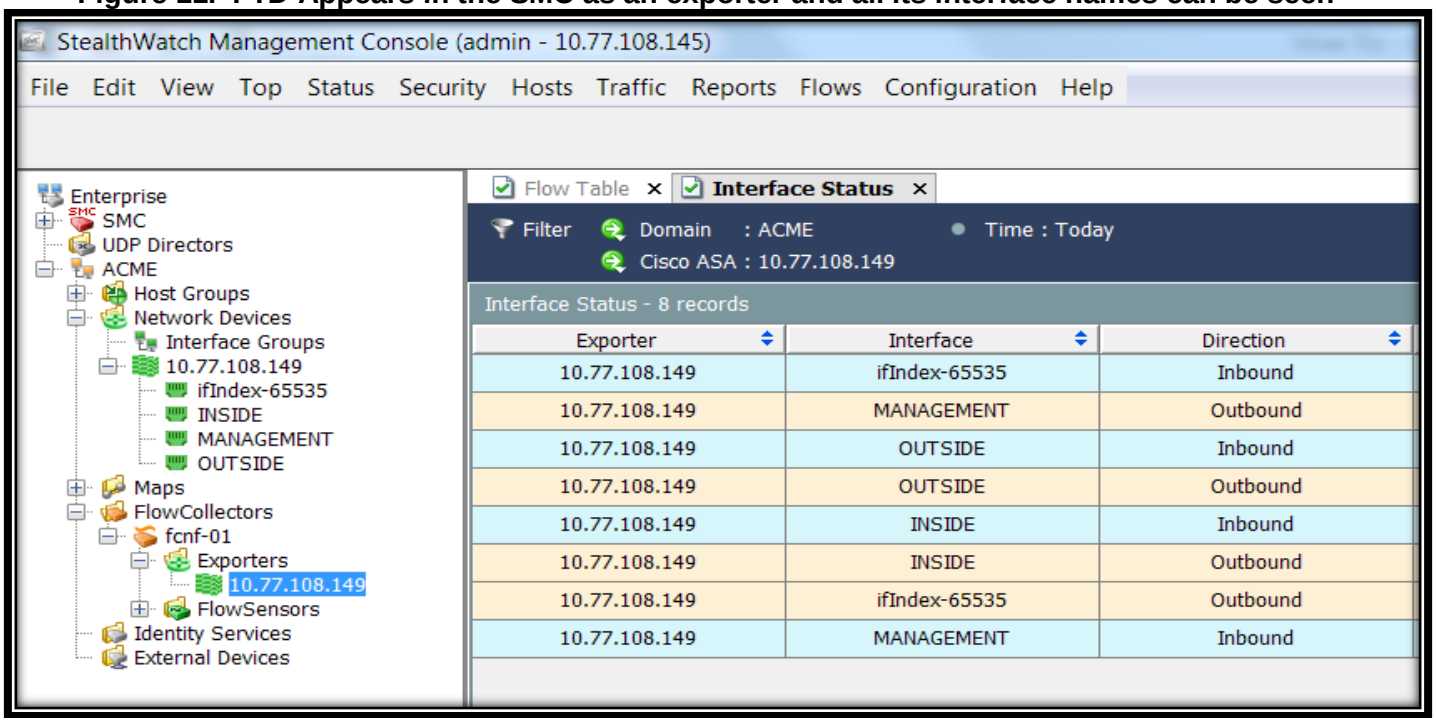


Figure 10. FTD appears in the SMC as an exporter and flows going through it are visible now



If SNMP polling from the Stealthwatch Management Console (SMC) is enabled as described in Step 4 earlier, then the actual names of the interfaces (provided they are defined) of the NGFW appear as shown below. For all the remaining interfaces whose names are not defined, they appear as ifIndex-XXX

Figure 11. FTD Appears in the SMC as an exporter and all its interface names can be seen



To Remove the NSEL Configure from FTD

Complete removal of the NSEL configuration from FTD involves two steps. First step is to remove the existing NetFlow add+set FlexConfig objects and add the NetFlow delete+clear FlexConfig objects in the FlexConfig Policy and deploying the configuration. This step involves attaching a command set with “no” commands. Second step is to remove the delete+clear FlexConfig objects from the FlexConfig Policy and redeploy the configuration. This step involves de-attaching the command set with “no” commands since they have already been deployed and executed, so they would not be effective anymore.

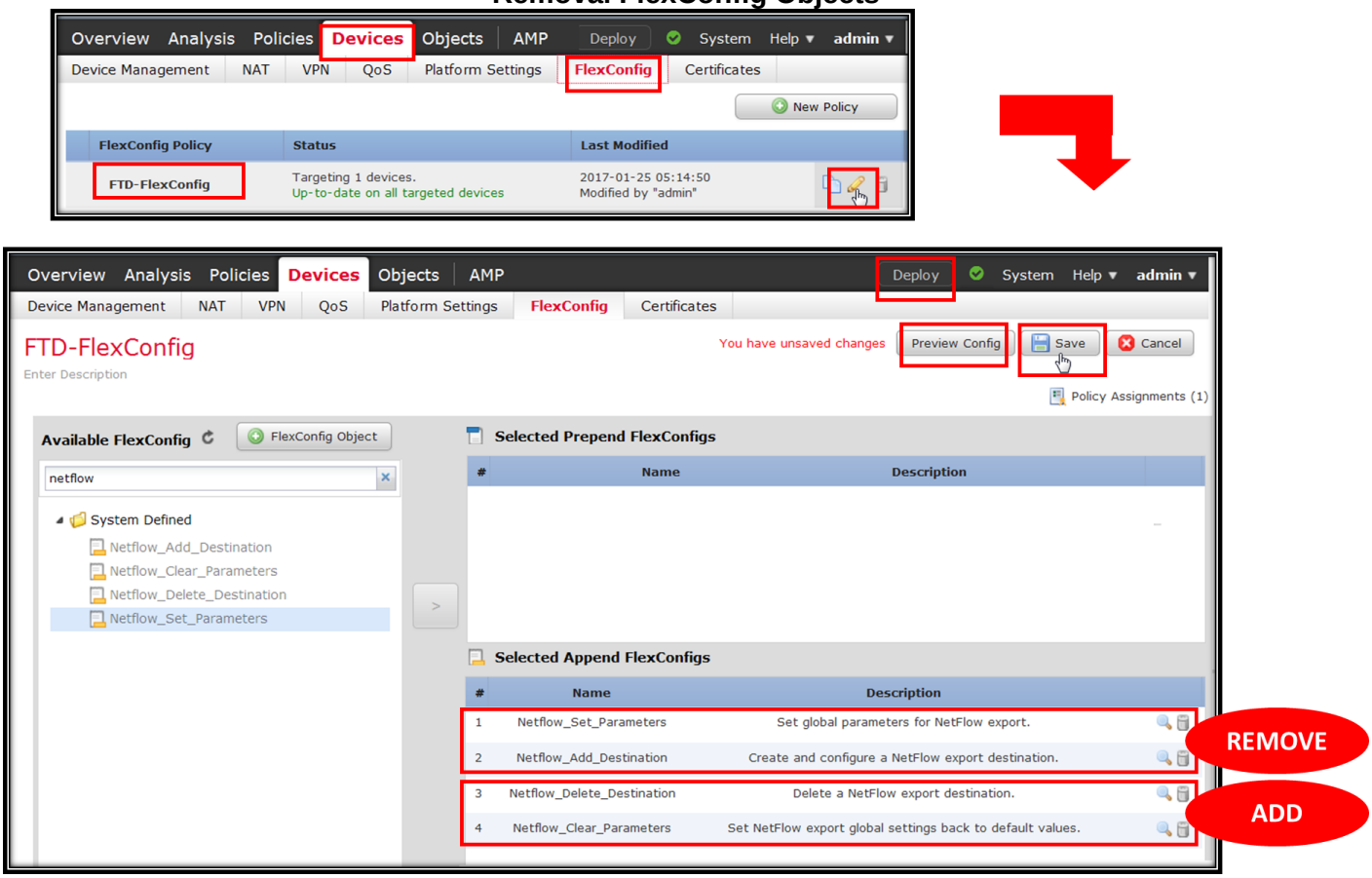
Step 1: Remove the existing FlexConfig Commands for NSEL from FTD by adding NSEL Removal FlexConfig Objects

Navigate to ***Devices -> FlexConfig***. Edit the existing **FTD-FlexConfig** policy by clicking on the ***Edit*** icon.

From the list of Available FlexConfig Objects, search and add **Netflow_Delete_Destinations** and **Netflow_Clear_Parameters** objects to the policy. The object gets added to the ***Selected Append FlexConfigs*** table. Remove the FlexConfig Objects - **Netflow_Add_Destinations** and **Netflow_Set_Parameters** from the existing list of objects currently present in the policy. Click ***Save***.

Optionally verify the full FlexConfig Policy to be deployed on a particular NGFW by clicking on the ***Preview Config*** button in the top-right and selecting the particular NGFW from the drop-down list. The preview will contain only ***"no"*** commands with respect to NSEL*(flow-export)*. Deploy the configuration changes to the NGFW.

Figure 12. Remove the existing FlexConfig Commands for NSEL from FTD by adding NSEL Removal FlexConfig Objects



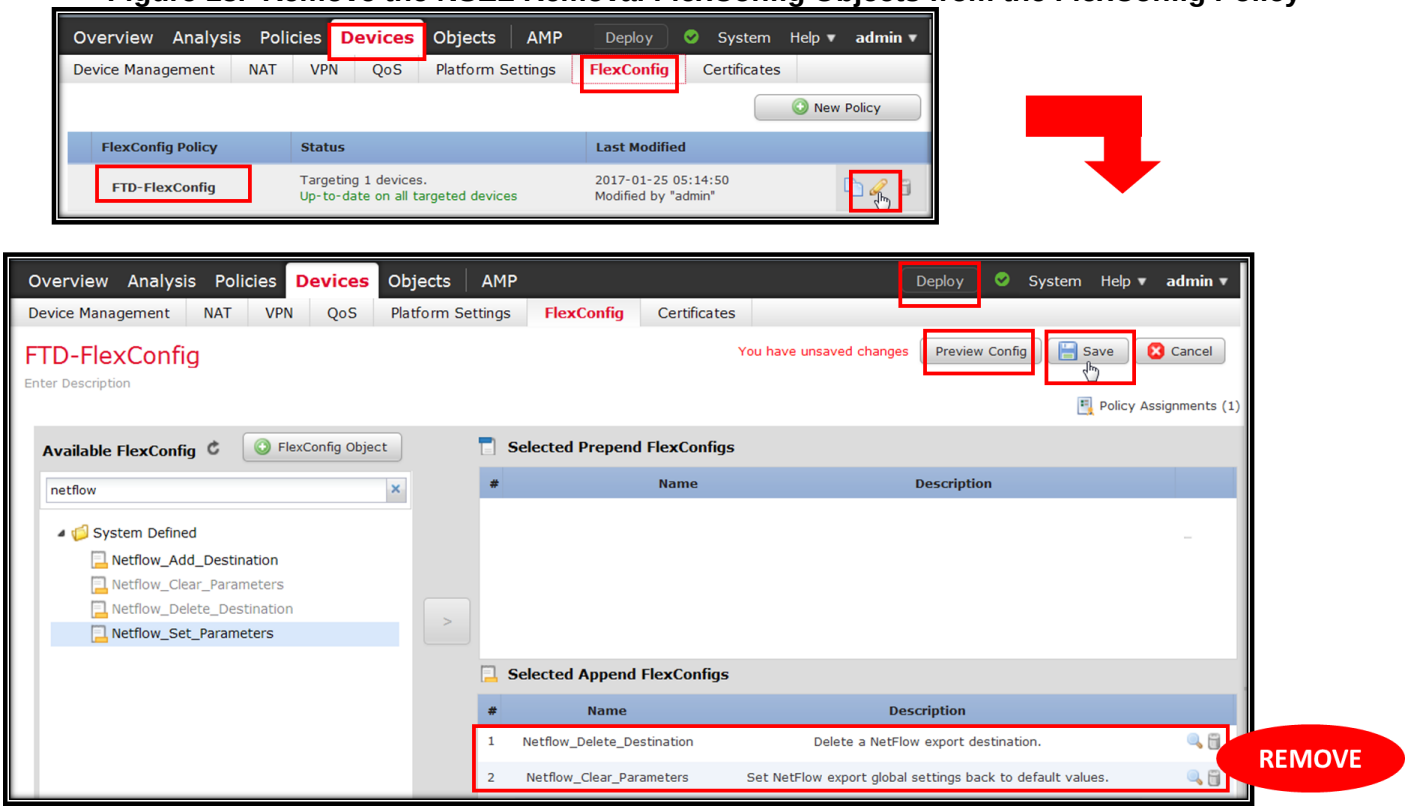
Step 2: Remove the NSEL Removal FlexConfig Objects from the FlexConfig Policy

Navigate to ***Devices -> FlexConfig***. Edit the existing **FTD-FlexConfig** policy by clicking on the ***Edit*** icon.

Remove the FlexConfig Objects - **Netflow_Delete_Destinations** and **Netflow_Clear_Parameters** from the existing list of objects currently present in the policy. Click on ***Save*** button to save.

Optionally verify the full FlexConfig Policy to be deployed on a particular NGFW by clicking on the ***Preview Config*** button in the top-right and selecting the particular NGFW from the drop-down list. The preview will not contain any commands associated with NSEL *(flow-export)*. Deploy the configuration changes to the NGFW.

Figure 13. Remove the NSEL Removal FlexConfig Objects from the FlexConfig Policy



To Modify the NSEL Configure on FTD

Any changes in the NSEL configuration on FTD involves three steps. The first two steps are the same as removing the NSEL configuration completely. The third step is to update the FlexConfig Text objects and again add the FlexConfig objects in the FlexConfig Policy and redeploy the configuration. This step is the same as adding a completely new NSEL configuration.

Here is an example where the IP of the Flow Collector is supposed to be changed for all the devices.

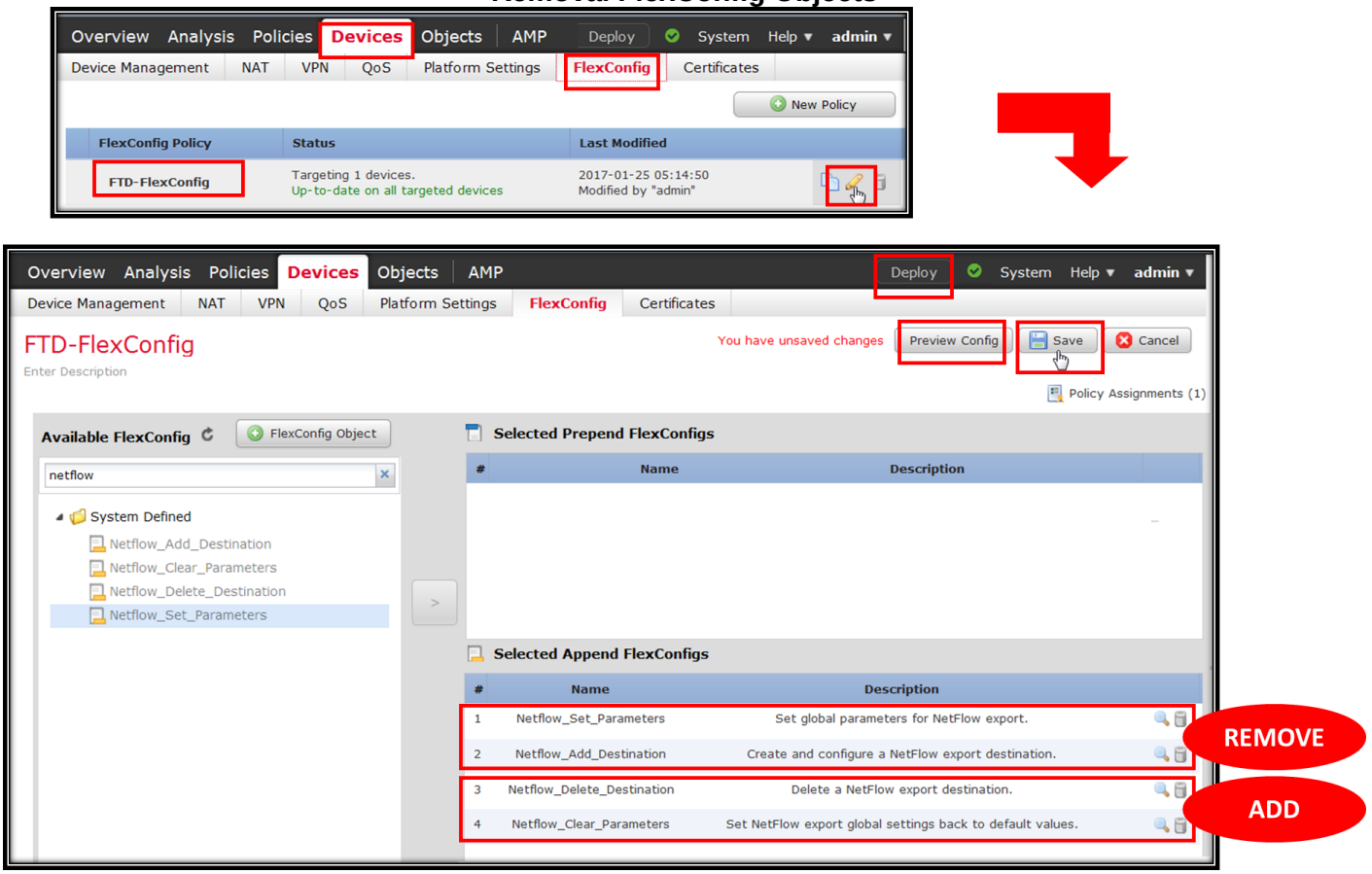
Step 1: Remove the existing FlexConfig Commands for NSEL from FTD by adding NSEL Removal FlexConfig Objects

Navigate to ***Devices -> FlexConfig***. Edit the existing **FTD-FlexConfig** policy by clicking on the ***Edit*** icon.

From the list of available FlexConfig Objects, search and add **Netflow_Delete_Destinations** and **Netflow_Clear_Parameters** objects to the policy. The object gets added to the ***Selected Append FlexConfigs*** table. Remove the FlexConfig Objects - **Netflow_Add_Destinations** and **Netflow_Set_Parameters** from the existing list of objects currently present in the policy. Click ***Save***.

Optionally verify the full FlexConfig Policy to be deployed on a particular NGFW by clicking on the ***Preview Config*** button in the top-right and selecting the particular NGFW from the drop-down list. The preview will contain only ***"no"*** commands with respect to NSEL*(flow-export)*. Deploy the configuration changes to the NGFW.

Figure 14. Remove the existing FlexConfig Commands for NSEL from FTD by adding NSEL Removal FlexConfig Objects



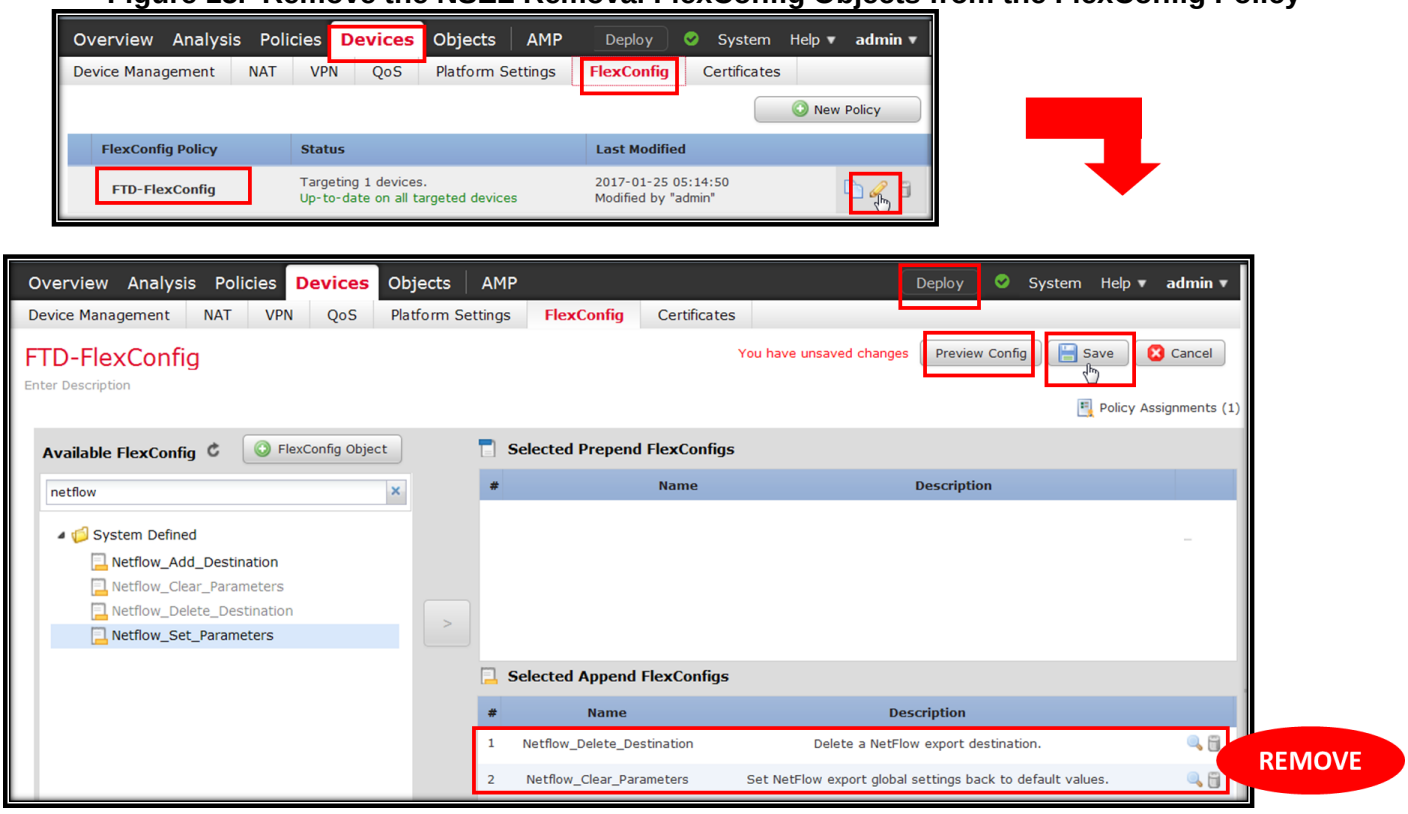
Step 2: Remove the NSEL Removal FlexConfig Objects from the FlexConfig Policy

Navigate to ***Devices -> FlexConfig***. Edit the existing **FTD-FlexConfig** policy by clicking on the ***Edit*** icon.

Remove the FlexConfig Objects - **Netflow_Delete_Destinations** and **Netflow_Clear_Parameters** from the existing list of objects currently present in the policy. Click on ***Save*** button to save.

Optionally verify the full FlexConfig Policy to be deployed on a particular NGFW by clicking on the ***Preview Config*** button in the top-right and selecting the particular NGFW from the drop-down list. The preview will not contain any commands associated to NSEL *(flow-export)*. Deploy the configuration changes to the NGFW.

Figure 15. Remove the NSEL Removal FlexConfig Objects from the FlexConfig Policy



Step 3: Modify and re-add the FlexConfig Text Object as needed and redeploy the configuration

Navigate to ***Objects -> Object Management***. From the menu on the left, scroll down towards the bottom and select ***FlexConfig -> Text Object***.

For better visibility, in the search filter on top right, search for **netflow.** This will provide 3 objects by default - **netflow_Destinations, netflow_Event_Types, netflow_Parameters.**

In this case, for example, we want to update the IP address of the Stealthwatch Flow Collector. So we select and edit the FlexConfig Text object - **netflow_Destinations.** Modify the IP address of the Flow Collector and click ***Save***.

Navigate to ***Devices -> FlexConfig***. Edit the existing **FTD-FlexConfig** policy by clicking on the ***Edit*** icon. From the list of Available FlexConfig Objects, search and add **Netflow_Set_Parameters** and **Netflow_Add_Destinations** objects to the policy. The object gets added to the ***Selected Append FlexConfigs*** table. Click ***Save***.

The full FlexConfig Policy can optionally be deployed on a particular NGFW by clicking on the ***Preview Config*** button in the top-right and selecting the particular NGFW from the drop-down list.

Figure 16. Modify the FlexConfig Text Object as needed

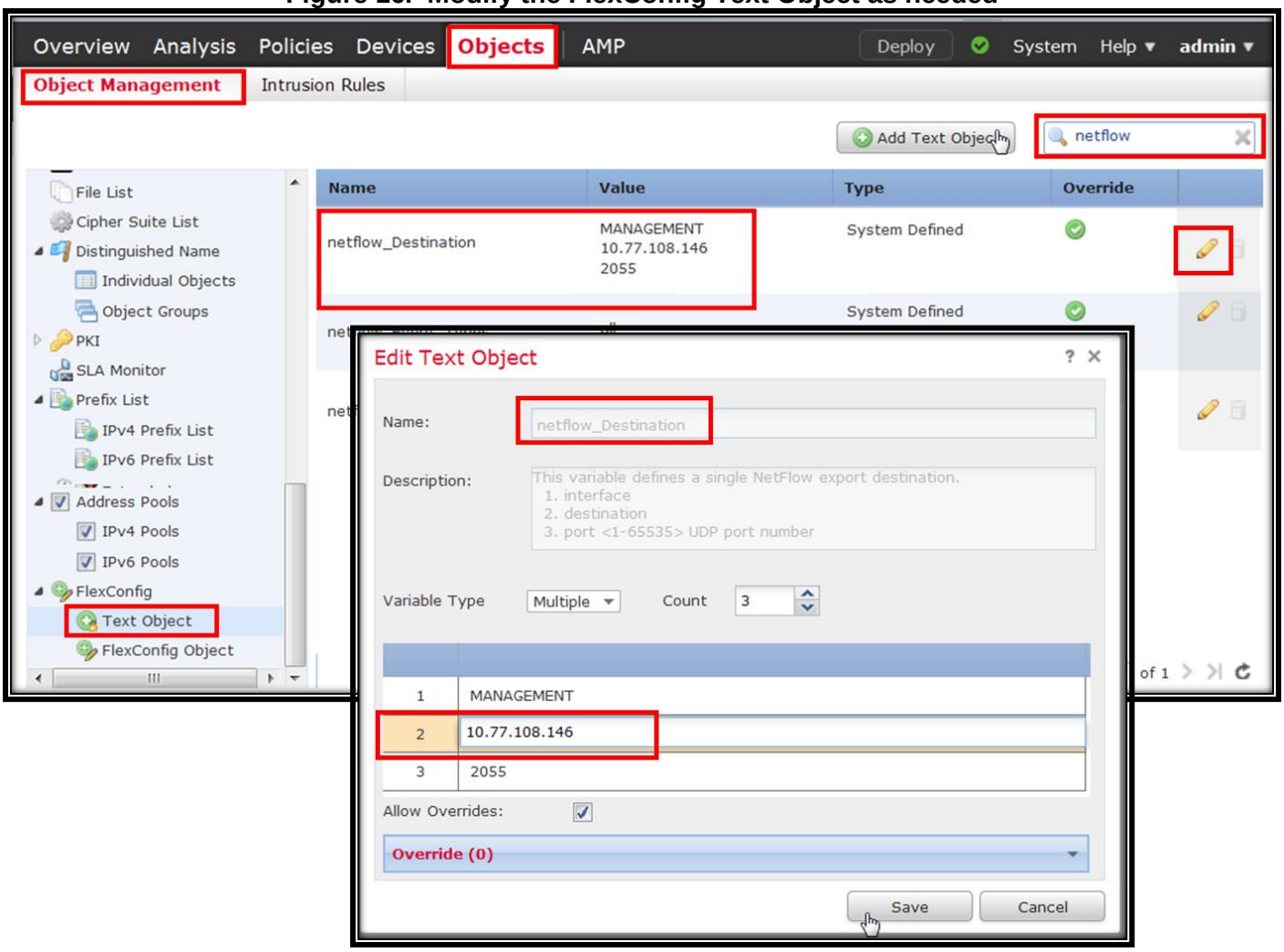
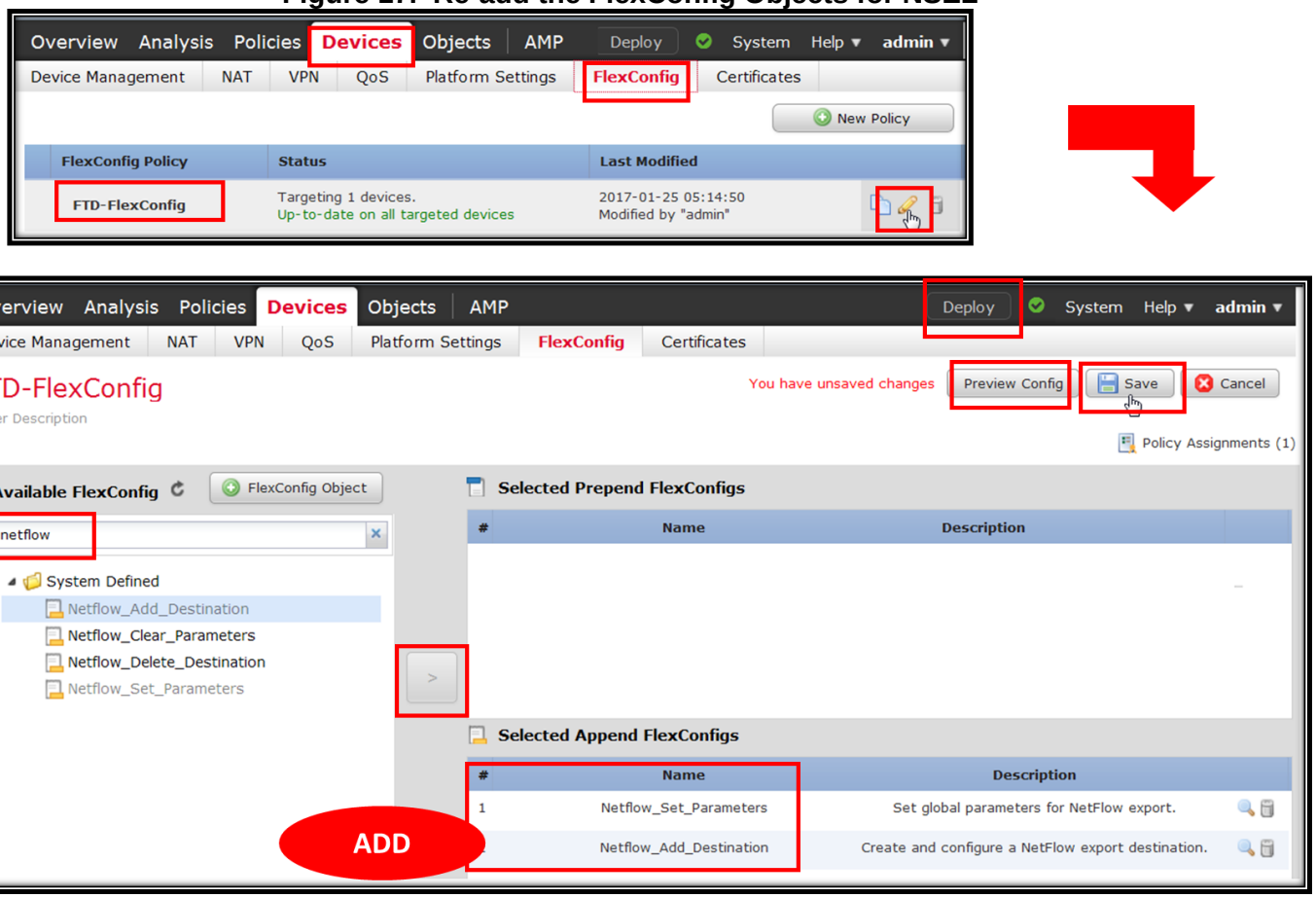


Figure 17. Re-add the FlexConfig Objects for NSEL



Troubleshooting Common Issues

The Configuration deployment fails while deploying NSEL configuration via FlexConfigs for the first time

In the event the deployment fails while deploying NSEL configuration via FlexConfigs for the first time, then look for the error details in the task details. Usually the deployment fails either because the Interface Name added in the FlexConfig Object does not exist on the NGFW or is not spelled correctly or the IP address of the Flow Collector is not in the correct IPv4 format.

The deployment succeeds and still the NGFW does not appear in the list of exporters

If the deployment succeeds and still the NGFW does not appear in the list of exporters, then the flows from the NGFW are not reaching the Flow Collector. This can be either because there are no flows being generated by the NFGW or because the Flow Collector's IP is not reachable from the interface of the FTD that is generating flows. Try the following commands on the FTD CLI.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# show run flow-export
flow-export destination MANAGEMENT x.x.x.x 2055
flow-export delay flow-create 1
firepower# ping x.x.x.x
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to x.x.x.x, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
firepower#
firepower# show flow-export counters
destination: MANAGEMENT x.x.x.x 2055
  Statistics:
    packets sent  17367
```

If the pings to the Flow Collector fail, then the management interface settings needs to be checked. Either the IP address is not assigned, the interface is down, or there is no route for the Flow Collector. These settings can be fixed in the Interface settings of the NGFW.

If the pings to the Flow Collector succeed and if there is a firewall in between the NGFW and the Flow Collector, make sure that the traffic is allowed from the MANAGEMENT interface IP of the

NGFW to the Flow Collector on UDP port 2055 for NSEL (or whichever port the NGFW is configured for). **This MANAGEMENT IP address is the IP address of the diagnostic0/0 interface and NOT the IP address used to link the NGFW to FMC.**

The Configuration deployment fails while deploying NSEL configuration with certain CLI-based error messages shown in the error message log

In case the configuration deployment fails while deploying NSEL configuration with certain CLI-based error messages shown in the error message log, then create a temporary FlexConfig object with certain ***"no"*** commands to be deployed only once to counter the commands causing the issue.

For example, adding a new Flow Collector IP to the FTD fails with an error message that a flow destination already exists; whereas nothing is present in the records of FMC. In order to fix this issue, create and attach a temporary FlexConfig object with the specific ***"no"*** commands and deploy the config. The exact ***"no"*** commands that needs to be added can be found by using the ***"system support diagnostic-cli"*** and ***"show run flow-export".*** Then disassociate and remove the temporary FlexConfig object.

More Information

For more information on Cisco Stealthwatch, please visit:

http://cisco.com/go/stealthwatch

For more information about Cisco Next Generation Firewalls (NGFW) and Firepower Threat Defense, please visit:

http://www.cisco.com/go/ngfw

Cisco Security Communities Page for Stealthwatch:

https://communities.cisco.com/community/technology/security/stealthwatch