Introduction

Overview

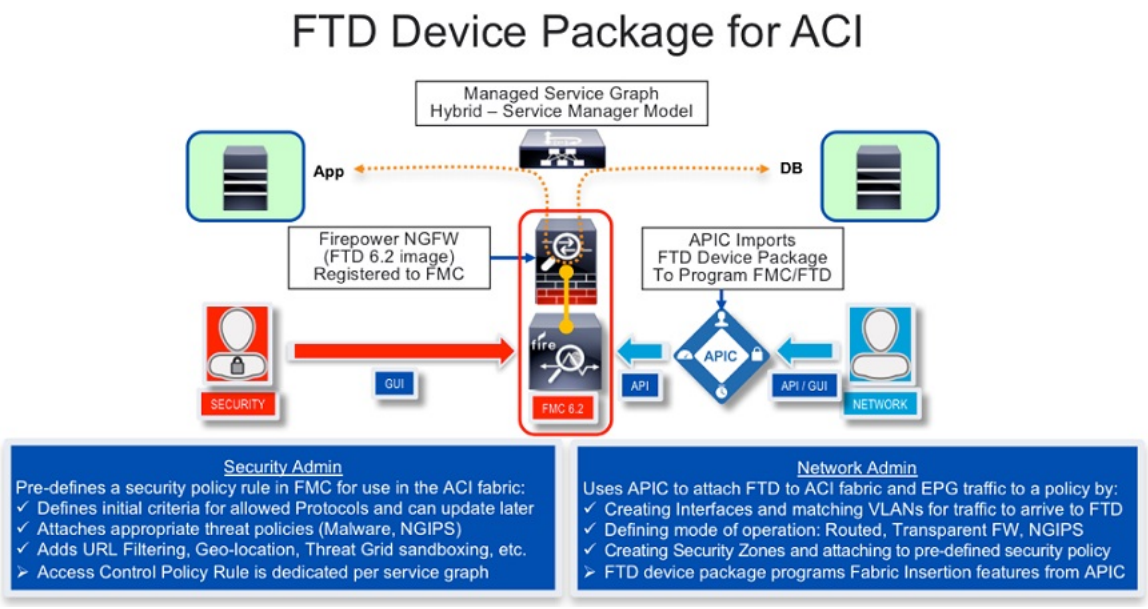
The Cisco Application Policy Infrastructure Controller (APIC) is a single point of control for centralized functions on the Cisco Application Centric Infrastructure (ACI). The APIC can automate the insertion of services such as a Cisco Firepower Threat Defense (FTD) northbound between applications, also called endpoint groups (EPGs). The APIC uses northbound Application Programming Interfaces (APIs) for configuring the network and services. You use these APIs to create, delete, and modify a configuration using managed objects.

To configure and monitor service devices, the APIC requires a device package. A device package manages a class of service device and provides the APIC with information about the device so that the APIC knows what the device can do. By using a device package, you can insert and configure network service functions on a service device such as an FTD appliance.

The FTD Fabric Insertion (FI) Device Package is based on a hybrid model (Service Manager, in ACI terminology) where the responsibility of the full-device configuration is shared between security and network administrators:

- Security administrator. Uses the FMC to pre-define a security policy for the new service graph, leaving Security Zone criteria unset. The new policy rule(s) defines appropriate access (allowed protocols) and an advanced set of protections such as NGIPS and malware policy, URL filtering, Threat Grid, and more.
- Network admininistrator. Uses the APIC to orchestrate a service graph, insert an FTD device into the ACI fabric, and attach directed traffic to this pre-defined security policy. Inside the APIC's L4-L7 Device Parameters or Function profile, the network administrator sets parameters defined in this guide, including matching a pre-defined FMC Access Control Policy and Rule(s).

When the APIC matches the name of the Access Control Policy Rule in the FMC, it simply inserts newly created security zones into the rule(s). If a rule is not found, the APIC creates a new rule by that name, attaches security zones to it, and sets the Action to Deny. This forces the security administrator to update the new Rule(s) criteria and appropriate set of protections before traffic can be allowed for a given service graph.



This document describes how to integrate FTD with the ACI and configure the APIC to utilize capabilities of the FTD:

- Enable the REST API in the Firepower Management Center (FMC)
- Download the FTD for ACI device package software from CCO
- Import the FTD for ACI device package into the APIC
- Register the FTD appliance
- Define a network service graph that utilizes the FTD appliance

Note The screenshots of the examples used in this document show a pre-existing tenant named **SampleTenant**. When following the steps in this guide and using provided templates, use the actual name of your tenant.

Service Function Insertion

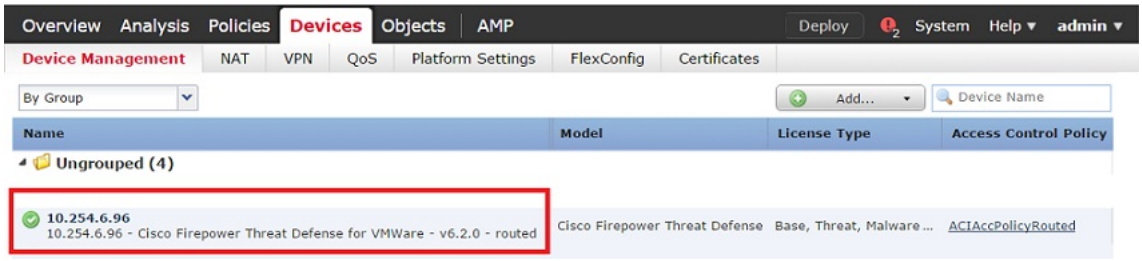
When a service function is inserted in the service graph between applications, traffic from these applications is classified by the APIC and identified using a tag in the overlay network. Service functions use the tag to apply policies to the traffic. For the FTD integration with the APIC, the service function forwards traffic using either routed, transparent, or inline firewall operation.

Available APIC Products

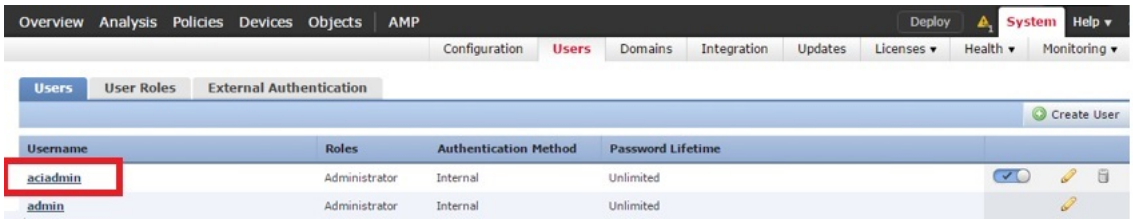
The initial software release contains the Cisco FTD Device Package Fabric Insertion software for ACI.

Prerequisites

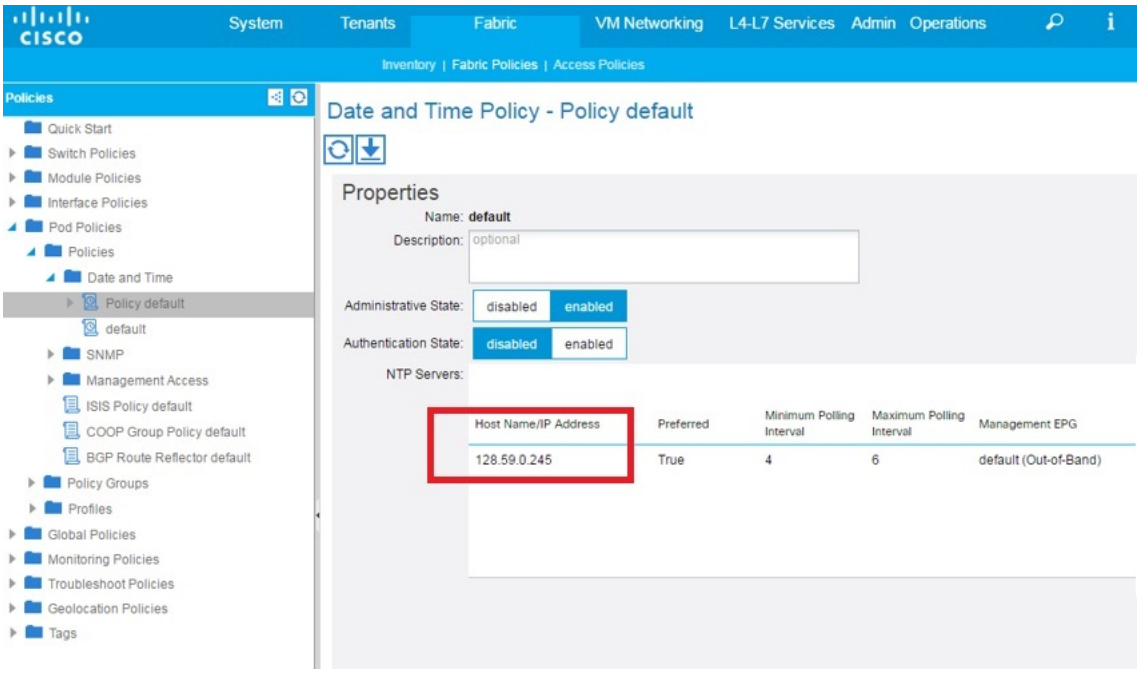
- FMC version 6.2.3; it includes REST API support for FTD.
- FTD version 6.2.3.
- APIC version 2.3(1f); its Device Manager is used to register a device. The FTD device package uses the Device Manager to allow the network portion of the FMC configuration to be instantiated by the APIC.
- Ensure that the FTD appliance you are trying to insert and configure as a network service is bootstrapped with a base configuration and registered with the FMC. For example, check the Device Management page in the FMC for the FTD:



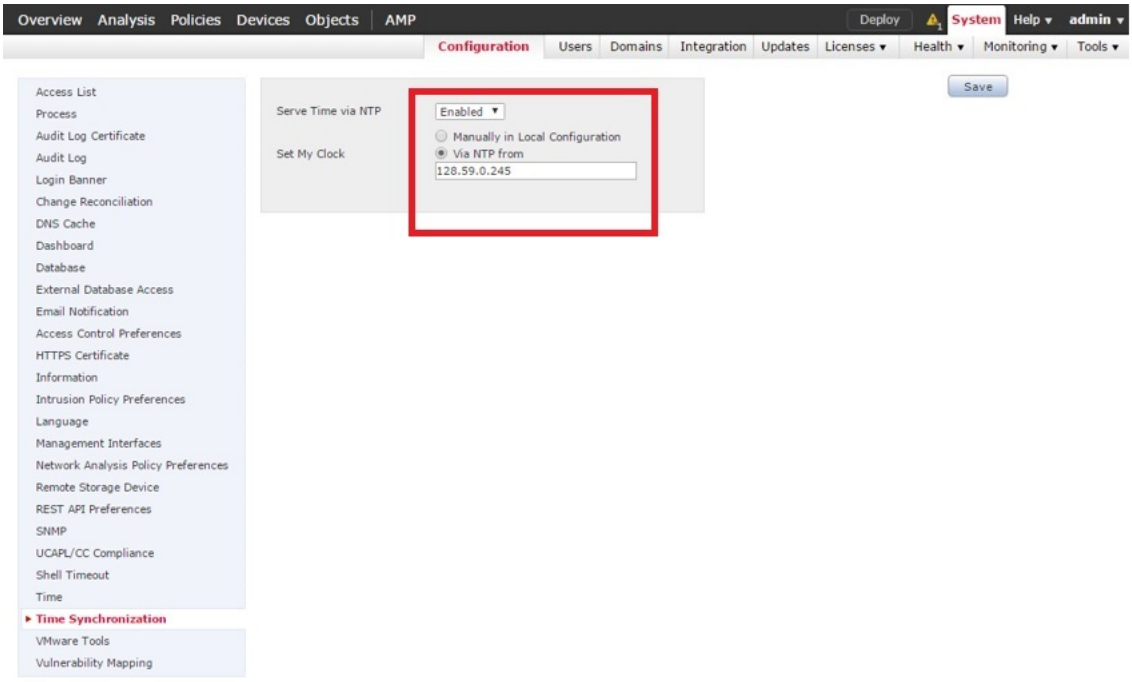
- To avoid REST API token generation race conditions, create an FMC administrator dedicated for use on the ACI. For example:



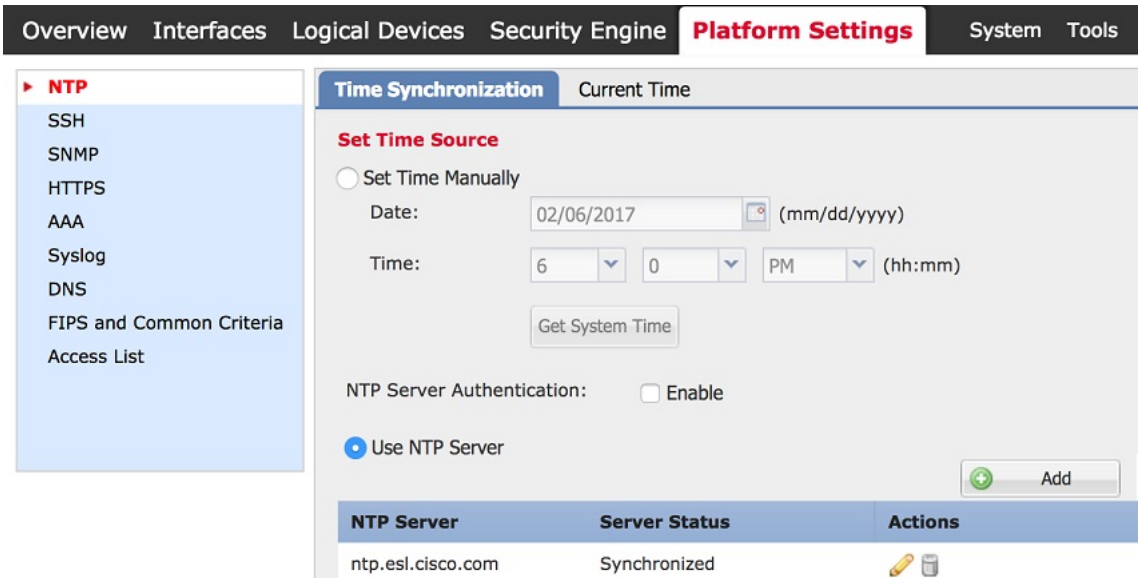
- To avoid both deployment failure and a gap in time between the servers, configure the APIC and FMC to use the same Network Time Protocol (NTP) server. With FTD on the Firepower 41xx and 93xx Series appliance, the Chassis Manager must also be configured.
  - In the APIC, navigate to **Fabric > Fabric Policies > Pod Policies > Policies > Date and Time**. Use the Create Date and Time Policy Wizard to configure the same NTP server:



- In the FMC, navigate to **System > Configuration > Time Synchronization** and configure the same NTP server:



- In the Chassis Manager of the Firepower 41xx and 93xx series appliance, navigate to **Platform Settings > NTP > Time Synchronization** and add the same NTP server:



Note If you try to create a configuration that is not supported on your current FMC or FTD version, an error similar to the following may appear on the APIC: "Major script error: Configuration error: …. ERROR: % Invalid input detected at '^' marker."

Related Documentation

- Cisco Application Centric Infrastructure Fundamentals
- Cisco APIC Layer 4 to Layer 7 Services Deployment Guide
- Cisco Firepower Threat Defense NGFW
- Cisco Firepower Management Center