SAFE Design Guide

Places in the Network: Secure Data Center

Cisco ACI Multi-Site Reference Design

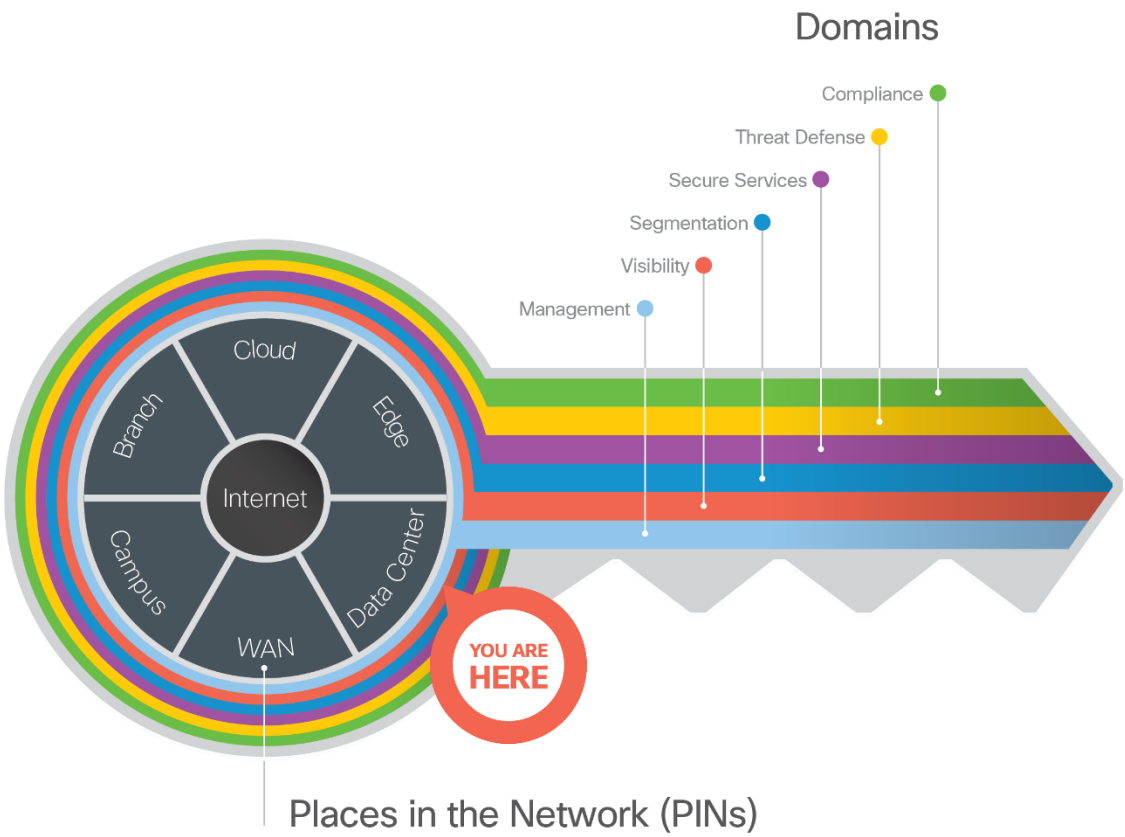
December 2020

SAFE
SIMPLIFIES SECURITY

Contents

Introduction

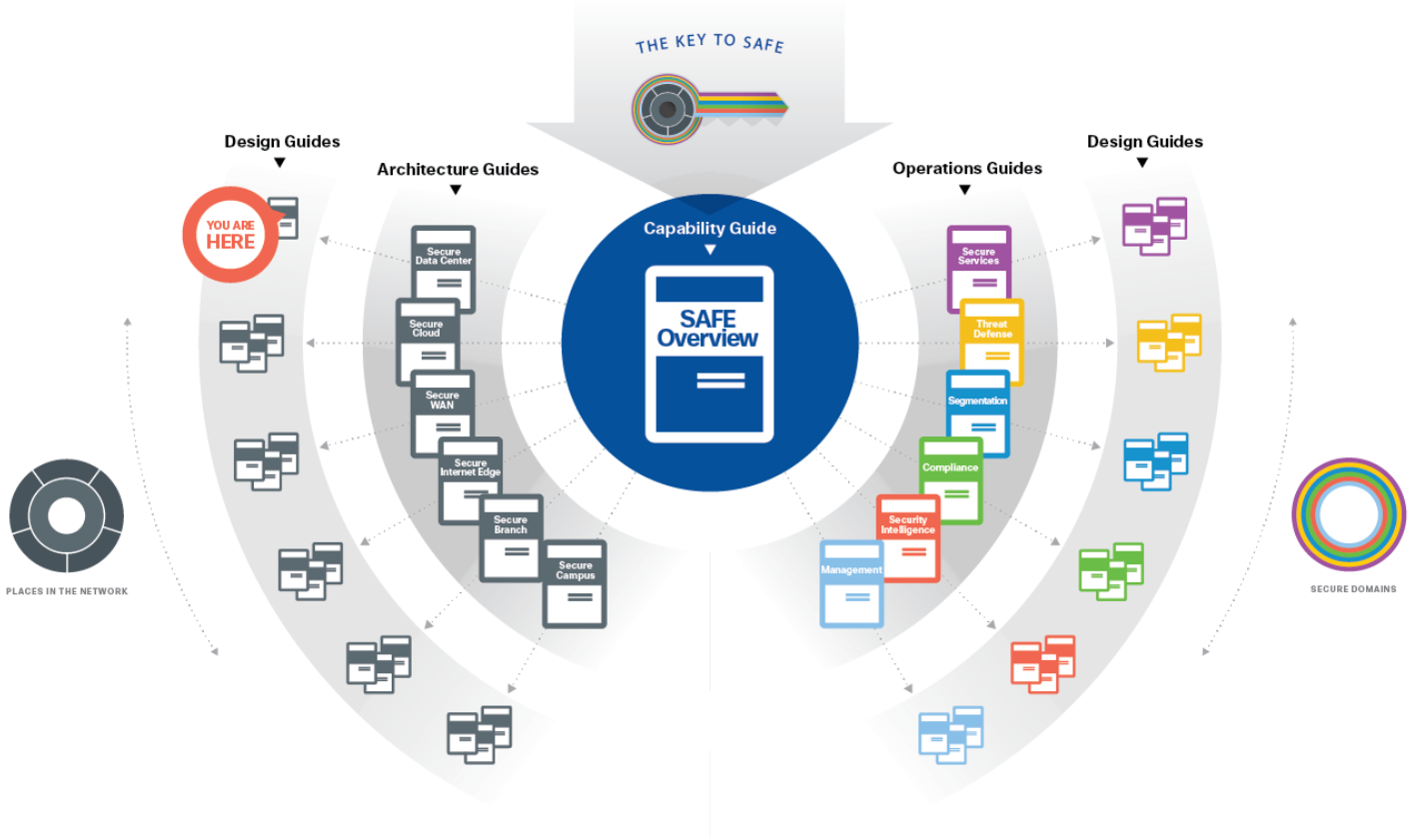
Cisco's Secure Data Center Solution includes effective and intent based security that follows the workload across physical data centers and multicloud environments to protect applications, infrastructure, data, users Cisco's solution continuously learns, adapts, and protects. As the network changes and new threats arise in the data center, Cisco Security Solutions dynamically detect and automatically adjust, mitigating threats in real-time.



The Key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domains.

Return to Contents

SAFE simplifies end-to-end security by using views of complexity depending on the audience needs. Ranging from business flows and their respective threats to the corresponding security capabilities, architectures and designs, SAFE provides guidance that is holistic and understandable.



More information about how Cisco SAFE simplifies security, along with this and other Cisco Validated Designs (CVD), can be found here: www.cisco.com/go/safe

This design guide is based on the Secure Data Center Architecture Guide, which can be found with the other PIN Architecture Guides here:

Return to Contents

6

Revision History

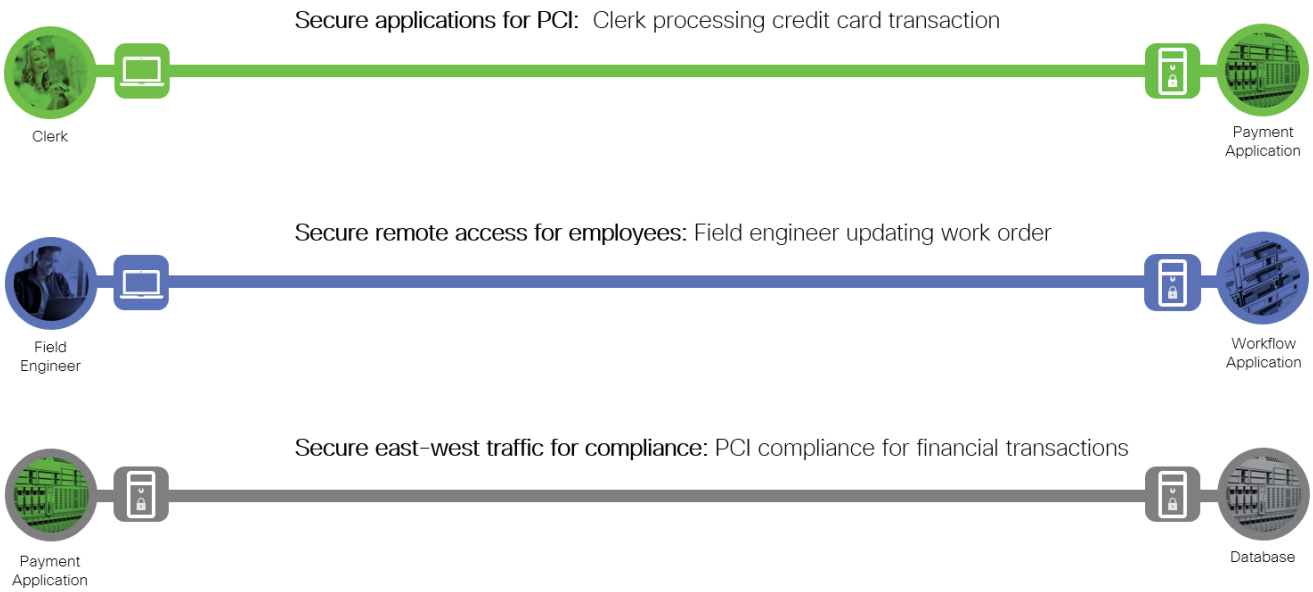
Date	Description
December 2018	Initial Input
June 2019	Updated images for Hyperflex, APIC, MSO, Nexus 9000, Fabric Interconnects, FTD, FMC and regression tested Test Case 1. Maintenance update rewrote Appendix C APIC initial configuration for better flow.
August 2019	Combined Appendix C and D and included them in Test Case 1. Added link to APIC tested config files on Github.
June 2020	Added Test case 8 – Tetration and ISE integration
December 2020	Added Test case 9 – TrustSec: ISE, APIC and FMC

Data Center Business Flows

SAFE uses the concept of business flows to simplify the identification of threats. This enables the selection of capabilities necessary to protect them.

This solution addresses the following Data Center business use cases:

- Secure applications and servers that are present on network
- Secure remote access for support
- Securing east-west traffic

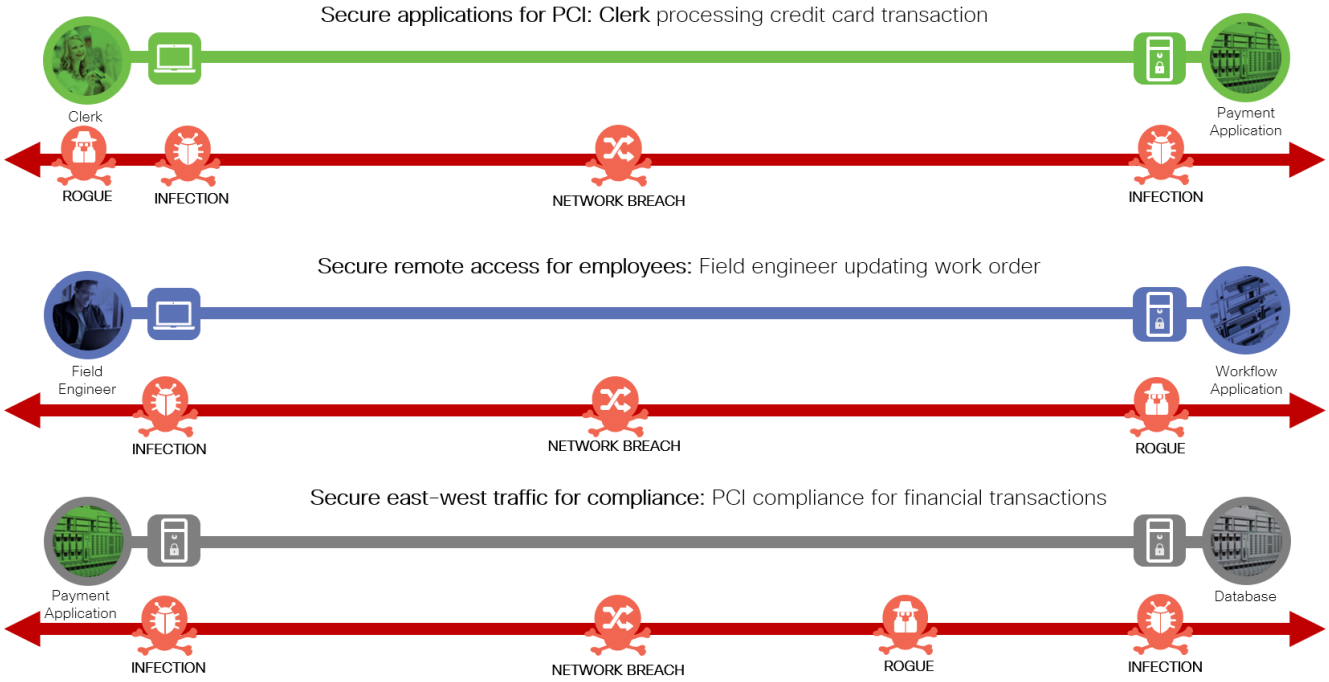


Return to Contents

Data Center Attack Surface

The Secure Data Center solution protects systems by applying security controls to the attack surface found in the data center. The attack surface in data center spans the business flows used by humans, devices, and the network.

Threats include; rogue identity, infections, and advanced persistent threats allowing hackers the ability to take control of your devices and networks. Legacy remote administration access to devices (such as modems) adds additional risk. Zero-day vulnerability attacks can bypass existing controls and infect systems.



Return to Contents

Solution Overview

Cisco's security approach for the modern data center allow companies to achieve:

- Improved resiliency to enable data center availability and secure services
- Operational efficiency from automated provisioning and flexible, integrated security
- Advanced threat protection from Cisco Talos - industry leading threat intelligence to stay up to date, informed, and secure

The integrated product workflow enables:

- Visibility - Complete visibility of users, devices, networks, applications, workloads, and processes
- Segmentation - Reduce the attack surface by preventing attackers from moving laterally, with consistent security policy enforcement, application allowed/blocked listing and micro-segmentation
- Threat Protection - Stop the breach by deploying multi-layered threat sensors strategically in the data center to quickly detect, block, and dynamically respond to threats

The top priorities for securing data centers are:

Visibility

"See Everything"

Complete visibility of users, devices, networks, applications, workloads and processes

Segmentation

"Reduce the Attack Surface"

Prevent attackers from moving laterally east-west with application allowed/blocked listing and micro-segmentation

Threat protection

"Stop the Breach"

Quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations

Return to Contents

Security Capabilities

Specific capabilities are necessary to protect the data center and build the appropriate layers of defense. These capabilities work together to create several layers of defense protecting the data center. The following sections describe the security capabilities required for each of the priorities.

Visibility

Visibility is critical in the data center. Companies need to see every user, device, network, application, workload and process.

You cannot protect what you cannot see. Visibility across the network and connected devices is achieved via several methods. Within the enterprise, each capability provides an increasing breadth of visibility and context. They provide visibility and security intelligence across an entire organization before, during, and after an attack. They continuously monitor the network and provide real-time anomaly detection and Incident response forensics.

These capabilities are required to achieve visibility in the data center.

Icon	Capability	Function
	Application Visibility Control	Provides deep packet inspection of application flows.
	Analysis and Anomaly Detection	Analyzes normal network behaviors, creating a baseline for operations and known devices connected to the network. Analyzes normal application and process behavior. Generates alerts when abnormal activities start.
	Device Trajectory	Provides historical representation of all process and file related activities on the endpoint/server. This includes visibility into binary executions with command line arguments, copy and move events, as well as network connections tied back to those executions.
	File Trajectory	Provides file-centric visibility, including file propagation across the enterprise and the data center in a single view. Used for efficient threat investigations and incident response.

Icon	Capability	Function
	Flow & Process Analytics	Monitor data center communications flows–Uses the information to better pinpoint nuisances in the network, and identifies and alerts on abnormal device traffic flows. Monitor process behavior for detecting anomalies, and sends alerts on abnormal behavior.
	Identity	Provides visibility of the users and the servers at the start and end of the data flow.

Segmentation

Segmentation reduces the attack surface by preventing hackers or unintended data from moving laterally (east-west) across the network. Once you have implemented visibility, you can enable segmentation in new and more effective ways. These capabilities provide segmentation across the data center.

Segmentation reduces the scope of an attack by limiting its ability to spread through the data center from one resource to another. For servers on delayed patch cycles, segmentation is an important tool, reducing the potential for vulnerability exploitation until adequate patch qualification and deployment into production is complete. For legacy systems, segmentation is critical to protect resources that don't receive maintenance releases or patch updates.

Segmentation plays an important role in audit and compliance scenarios. For industry requirements such as the Payment Card Industry Data Security Standard (PCI DSS), regulations like the General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA). Segmentation can be used to help reduce the number of systems that require controls, as well as the scope of an audit.

These capabilities provide segmentation across the data center.

Icon	Capability	Function
	Firewall	Firewall for North/South segmentation of flows into and out of the data center.
	Host-based Firewall	Provides micro-segmentation between all application and services.
	Tagging	Software-defined segmentation between groups East/West within the data center.

Return to Contents

11

Threat Protection

Threat Protection is a multi-layered threat sensor deployment. It is able to quickly detect, block and respond dynamically when threats arise preventing breaches from impacting the business.

All data centers have something in common: they need to protect their applications and data from an increasing number of sophisticated threats and global attacks. All organizations are under threat of attack; many have been breached but are unaware of it. Protecting the modern data center is a challenge for security teams. Workloads are constantly moving across physical data centers and multi-cloud environments. These capabilities enable threat protection in the data center.

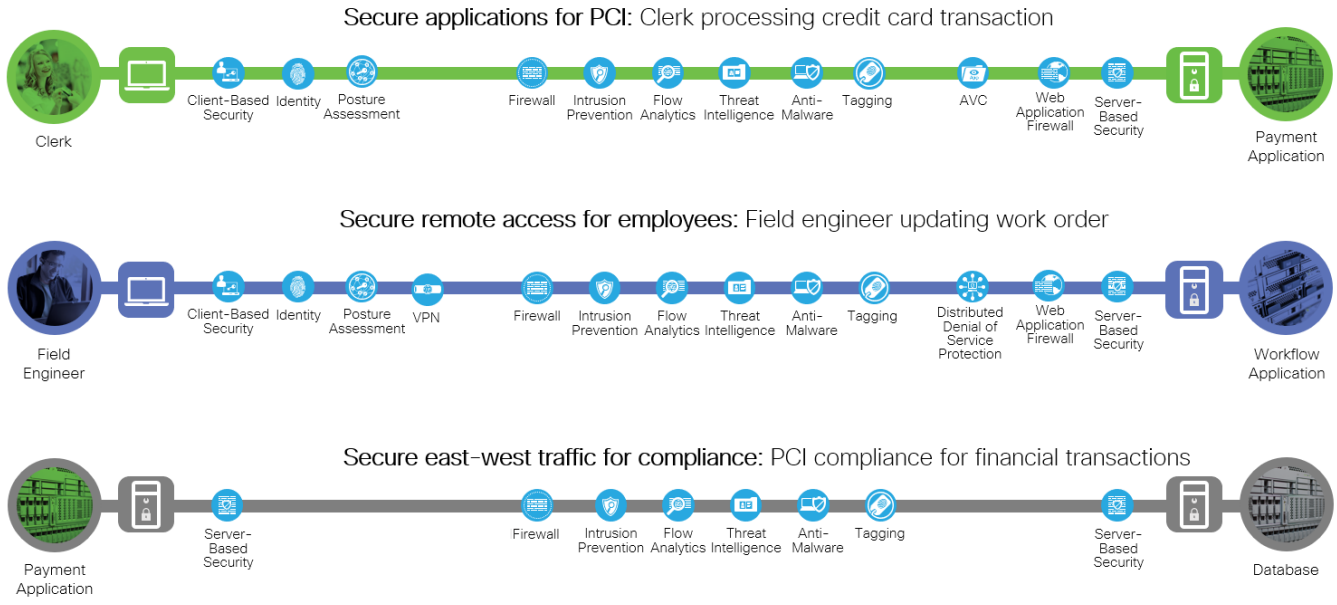
Icon	Capability	Function
	Anti-Malware	Identify, block, and analyze malicious files and transmissions.
	Anti-Virus	Identify and block known malicious files and signatures.
	File Analysis	Apply automatic static and dynamic analysis for unknown files to improve security efficacy and understand behaviors
	Firewall	Block traffic from quarantine groups.
	Flow & Process Analytics	Network traffic metadata identifying security incidents enables automatic quarantine response.
	Host-based Firewall	Automatically quarantine a host to rapidly contain a threat.
	Intrusion Prevention	Initiate quarantine request based on anomalous activity.
	Posture Assessment and Patching	Corrective action to fix vulnerabilities.
	Tagging	Software based segmentation to automatically to quarantine hosts to rapidly contain the threat and prevent further lateral movement.
	Threat Intelligence	Protect against newly identified threats via a global threat information service.

Return to Contents

Solution Architecture

Developing a defense-in-depth architecture requires identifying existing threats and applying appropriate security capabilities to thwart them.

The three business flows defined earlier are shown with the necessary security capabilities.



These capabilities are implemented through product features. The following sections briefly describe each area and the products selected that implement the needed capabilities.

Return to Contents

Visibility

Cisco provides complete insight into workloads and application behavior. The following products contain the capabilities needed to gain that visibility.

Capability		Solution Component
	Application Visibility Control	Cisco Firepower Next Generation Firewall (NGFW) or Cisco Firepower Next Generation IPS (NGIPS)
	Analysis and Anomaly Detection	Cisco Stealthwatch with Cognitive Intelligence and Cisco Tetration
	Device Trajectory	Cisco Advanced Malware Protection for Endpoints
	File Trajectory	Cisco Advanced Malware Protection for Endpoints
	Flow & Process Analytics	Cisco Stealthwatch, network switches, firewalls, and routers sending NetFlow. Cisco Tetration
	Identity	Cisco Identity Services Engine (ISE), Cisco Application Centric Infrastructure (ACI), Cisco Tetration

Return to Contents

Segmentation

Cisco provides multilayer segmentation. The following products contain the capabilities needed to achieve segmentation.

Capability		Solution Component
	Firewall	Cisco Firepower Next Generation Firewall
	Host-based Firewall	Cisco Tetration agent configuring native host firewalls.
	Tagging	Cisco ACI Endpoint Groups (EPGs), Cisco TrustSec Security Group Tags (SGTs) Traditional VLANs

Return to Contents

Threat Protection

Strategically placed sensors enable companies to quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations. The following products contain the capabilities needed to enable threat protection.

Capability		Solution Component
	Anti-Malware	Cisco Advanced Malware Protection for Endpoints and Cisco Advanced Malware Protection for Networks
	Anti-Virus	Cisco Advanced Malware Protection for Endpoints and Cisco Advanced Malware Protection for Networks
	File Analysis	Cisco Threat Grid
	Firewall	Cisco Firepower Next Generation Firewall
	Flow & Process Analytics	Cisco Stealthwatch and Cisco Tetration
	Host-based Firewall	Cisco Tetration
	Intrusion Prevention	Cisco Firepower Next Generation Intrusion Prevention System
	Posture Assessment and Patching	Cisco Tetration
	Tagging	ACI, TrustSec and VLANs
	Threat Intelligence	Cisco Talos Security Intelligence Cisco Cognitive Intelligence and Encrypted Traffic Analytics

Return to Contents

Cisco Secure Data Center Reference Architecture

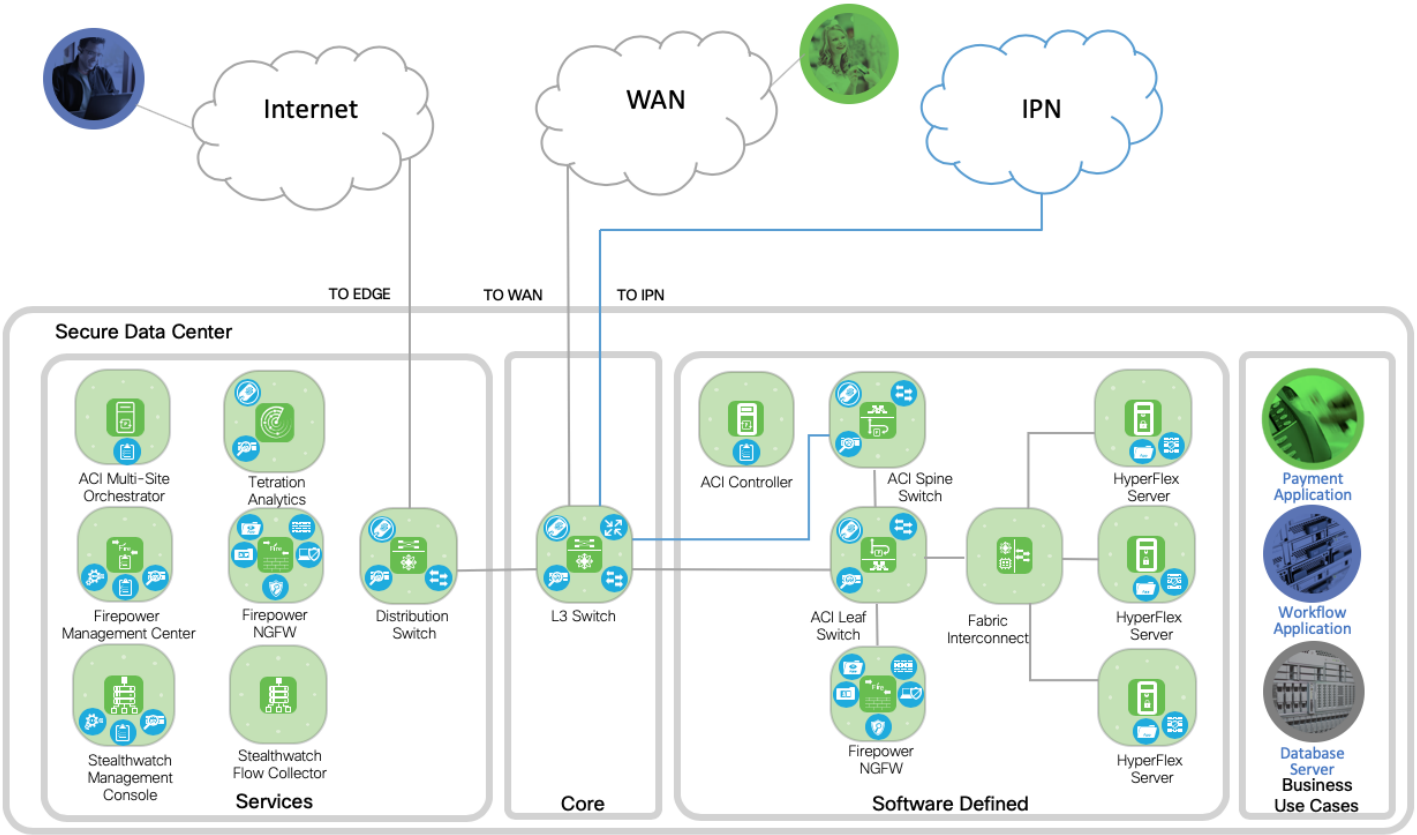
The Cisco Secure Data Center reference architecture is a solution that includes the best of Cisco's products for a modern data center.

- The data center network is based on a Multi-Site Application Centric Infrastructure (ACI).
- Firepower™ Next Generation Firewall (NGFW) is used to protect the workloads.
- Tetration and Stealthwatch are used to provide visibility and threat protection.
- Advanced Malware Protection for Endpoints (AMP4E) on the servers for endpoint threat protection.
- Cisco Hyperflex is the hyperconverged data center platform which includes compute, storage and network.

Product information details will be discussed in the Implementation section below. The capabilities that each architectural component needs to provide are included.

Hybrid cloud is included in this architecture by supporting an application in Amazon Web Services and protected with Firepower NGFW Virtual (NGFWv), AMP4E, Tetration agent, and Stealthwatch Cloud.

The Intersite Network is a network where different Application Policy Infrastructure Controller (APIC) domains are interconnected through generic Layer 3 infrastructure. Intersite Network is used for Multi-Site ACI deployment and provides data center interconnect. The Edge, WAN and Intersite Network are places in the network (PINs) that are outside of the data center. Refer to the SAFE Architecture Guides for other PINs.

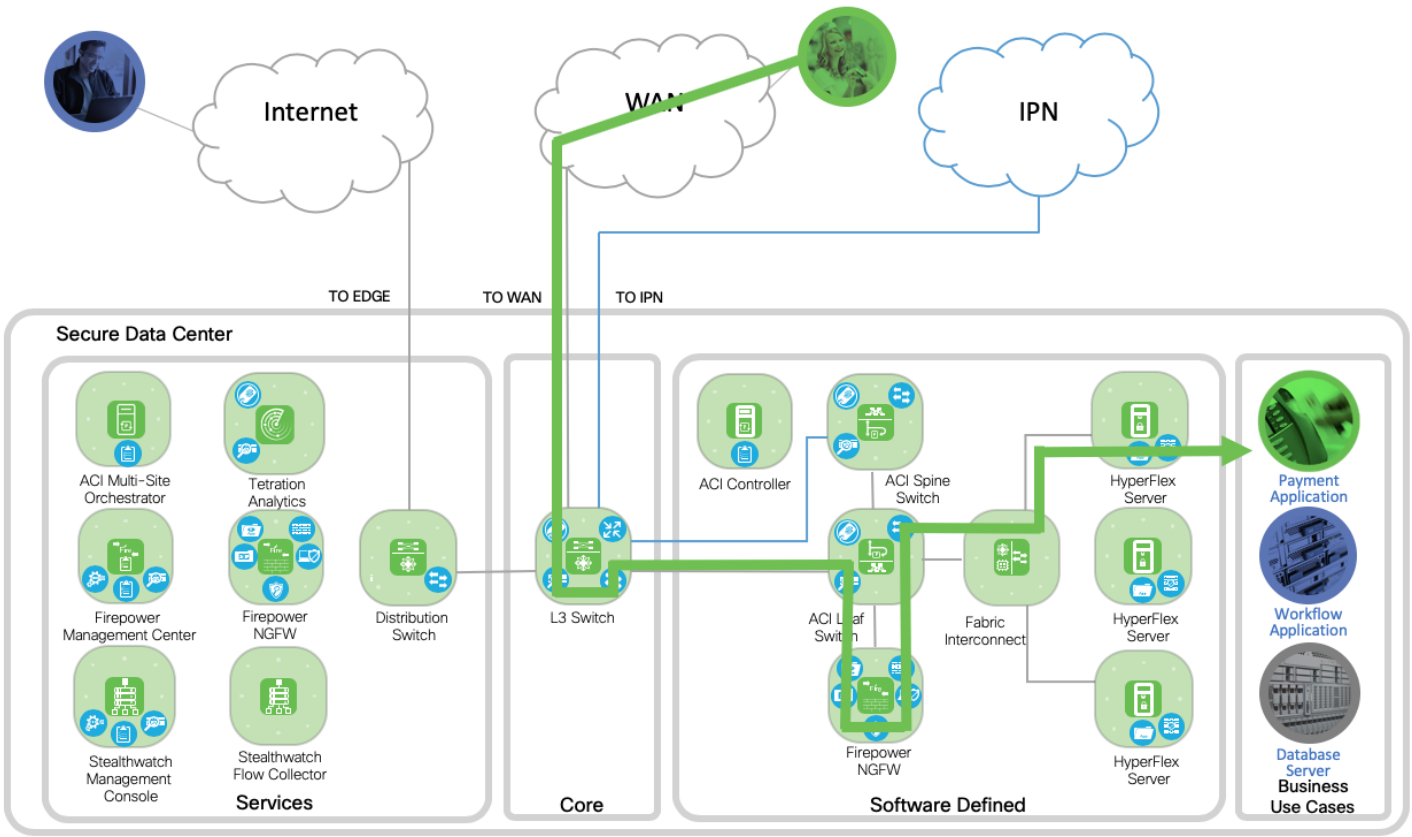


The clerk depicted by the green token could be at a branch office connected to the data center via the WAN. The field engineer depicted in blue is connected to the Internet and needs to connect to the data center securely to file a work order.

Return to Contents

17

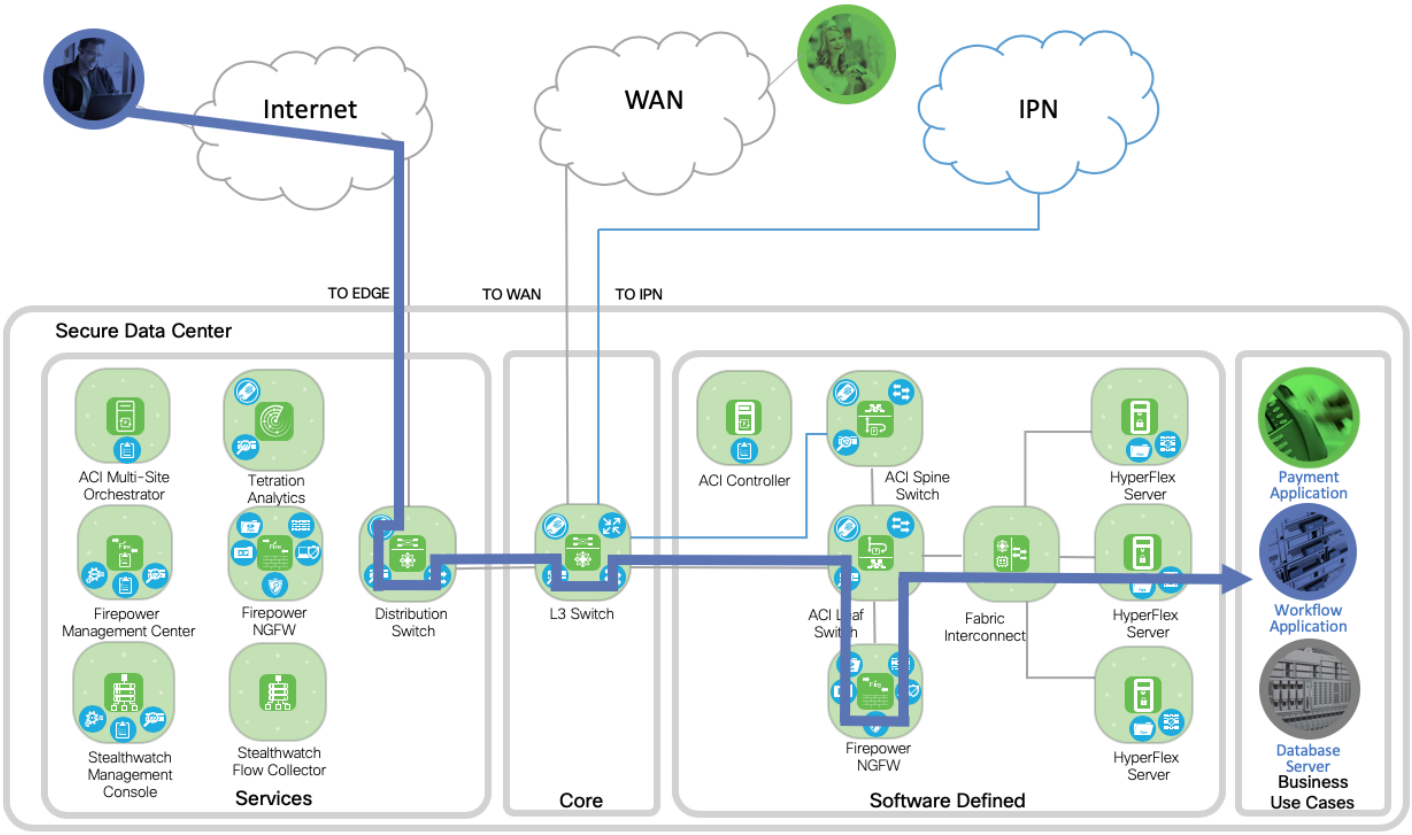
The first business flow is to secure a payment application for PCI compliance. The clerk is connected to the WAN from a branch office. She is processing a credit card transaction and accessing the payment application in the data center. The data flow enters the core zone of the data center typically on a layer 3 switch. The Software Defined zone refers to the software defined segmentation, which is delivered by ACI. The flow continues to the Software Defined zone to the ACI Leaf and redirected with a contract to the Firepower NGFW for firewall, IPS and segmentation services. The data flow then proceeds back to the ACI leaf switch, to the Fabric Interconnect and then connects to the payment application.



Return to Contents

18

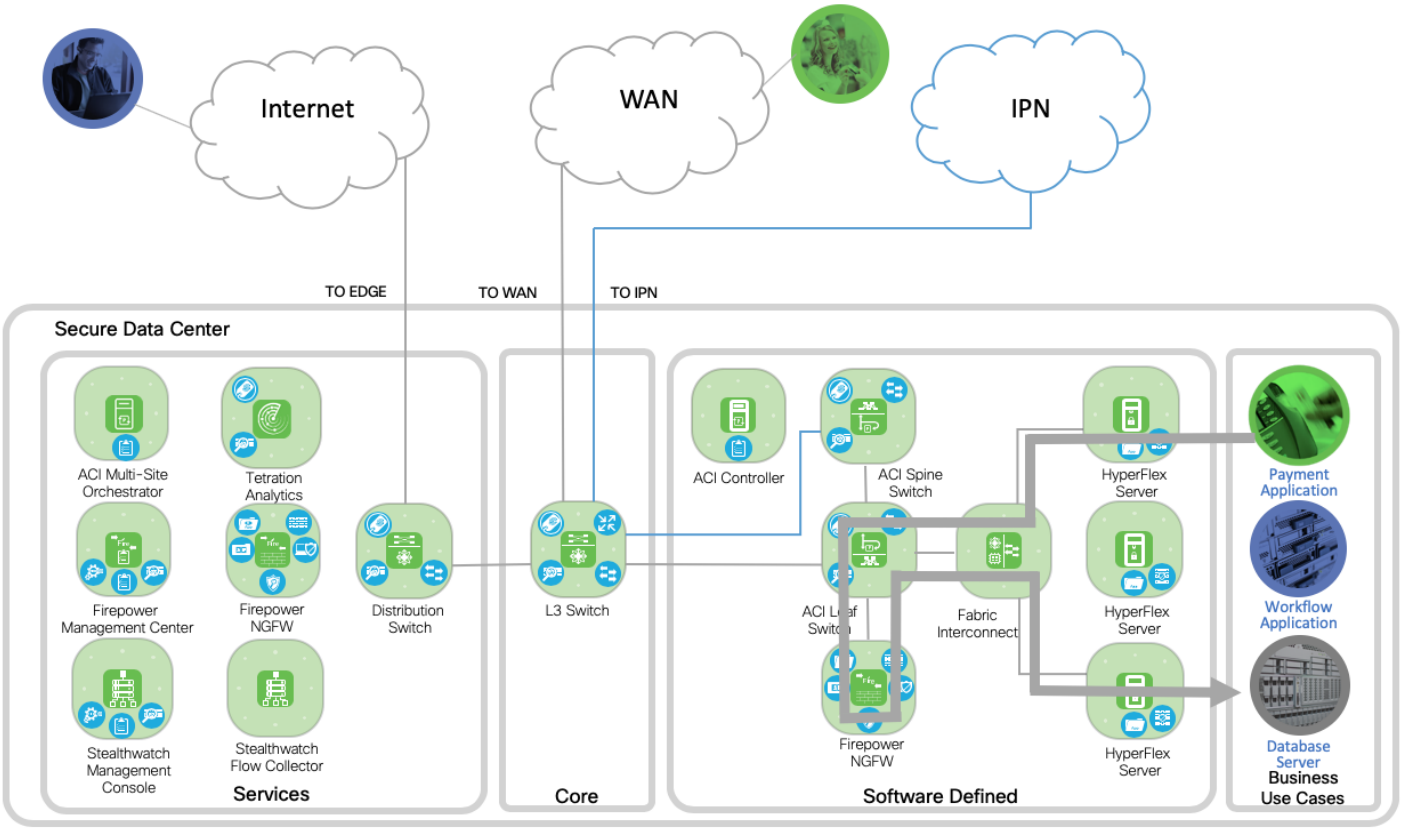
The second business flow secures remote access for employees. A field engineer is accessing the data center submitting a work order to the workflow application. The data flows from the Internet edge to a Distribution switch in the Services zone. VPN termination is handled by the Internet Edge architecture. The flow proceeds to the L3 switch in the Core zone and then to the Software Defined zone. The flow continues to the ACI Leaf and redirected with a contract to the Firepower NGFW for firewall, IPS and segmentation services. The data flow will then proceed back to the ACI leaf switch to the Fabric Interconnect and then connects to the Workflow application.



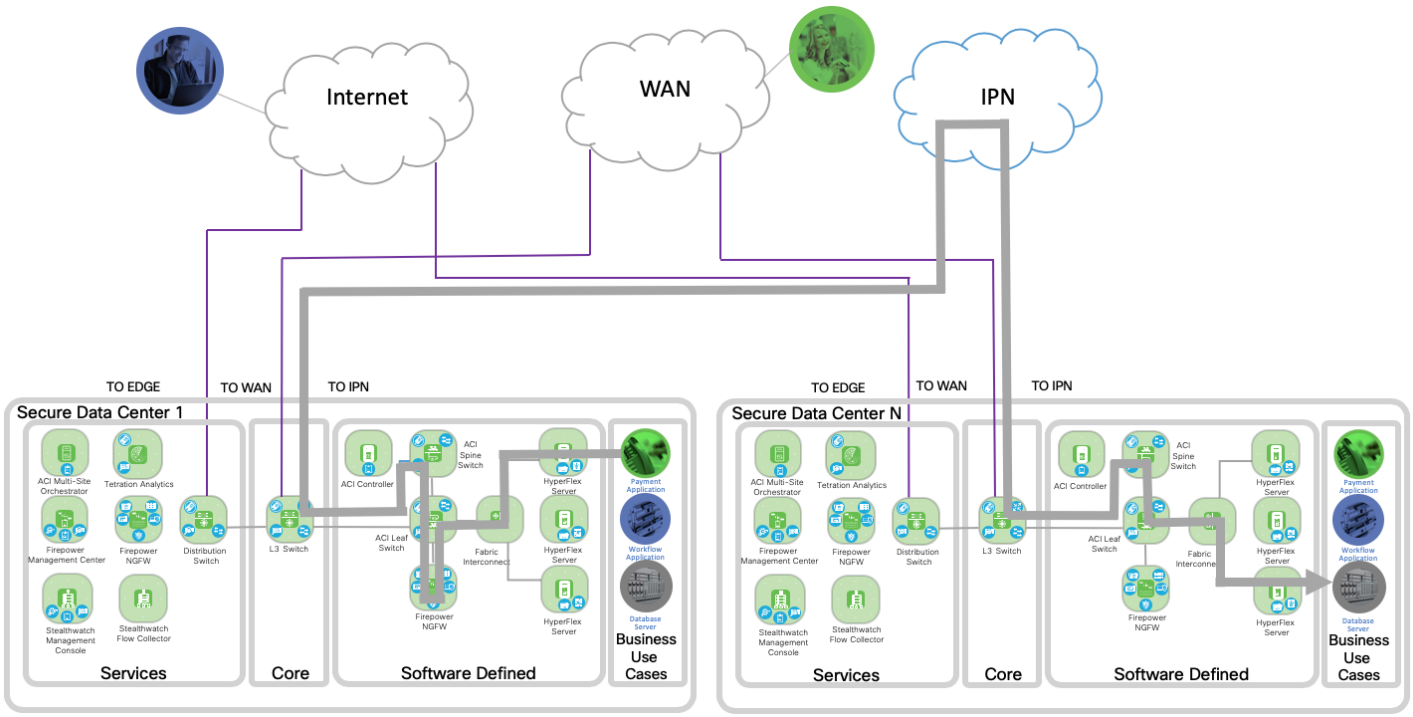
Return to Contents

19

The third business flow secures east-west traffic. In this case the database server and payment application are both communicating with each other within the data center.



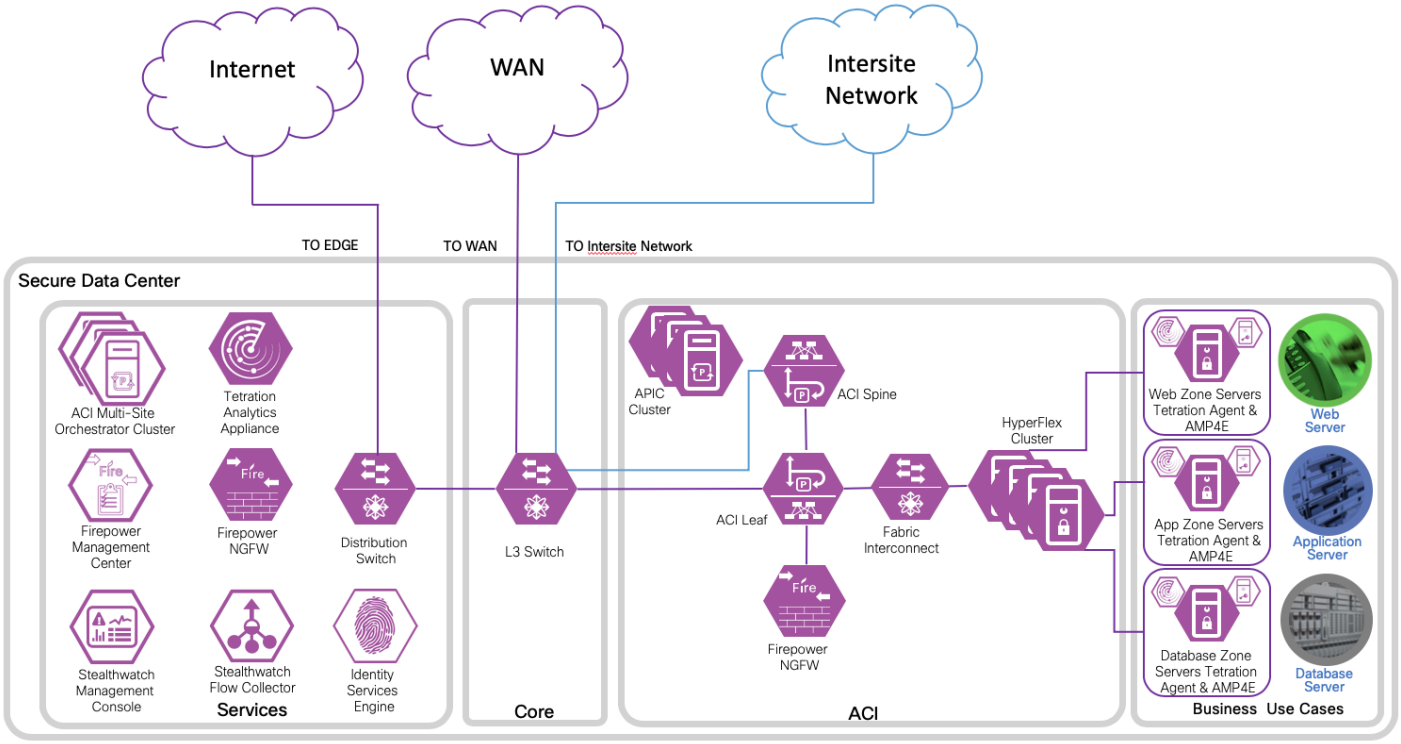
Additionally, the third business flow secures east-west traffic across data centers. In this case the database server and payment application are communicating between two data centers.



Return to Contents

Implementation

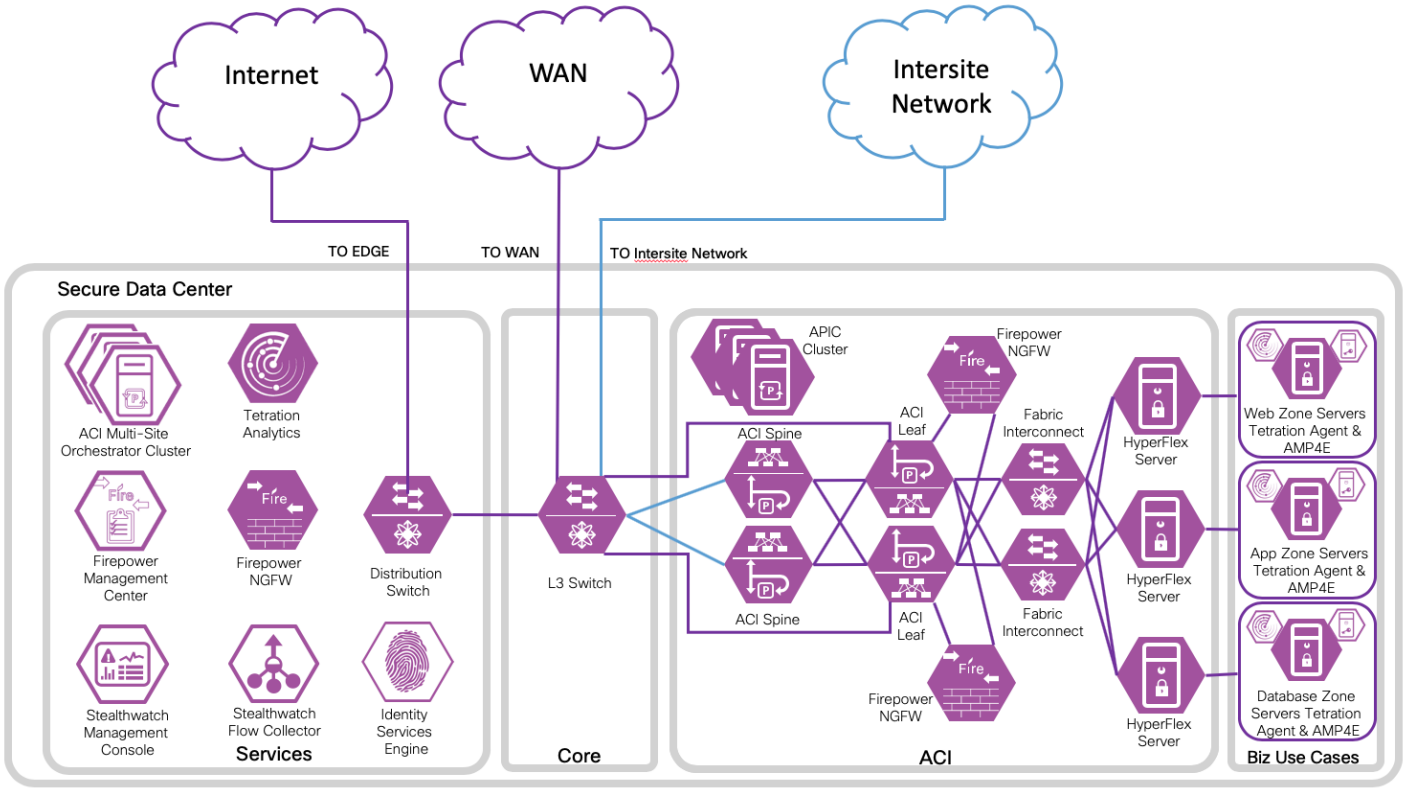
The Cisco Secure Data Center Reference Design is built based on the Secure Data Center Reference Architecture. For lab testing purposes virtual machines were used for the Multi-Site Orchestration Cluster, Firepower Management Center, Stealthwatch Management Console and Stealthwatch Flow Collector. For production environments these services (and others) should be deployed on properly sized appliances for the customer's environment and needs.



The purple design icons illustrate the product selected to provide the capabilities required. Solid purple icons refer to physical appliances, and the icons with the white background represent a virtual appliance or software.

Return to Contents

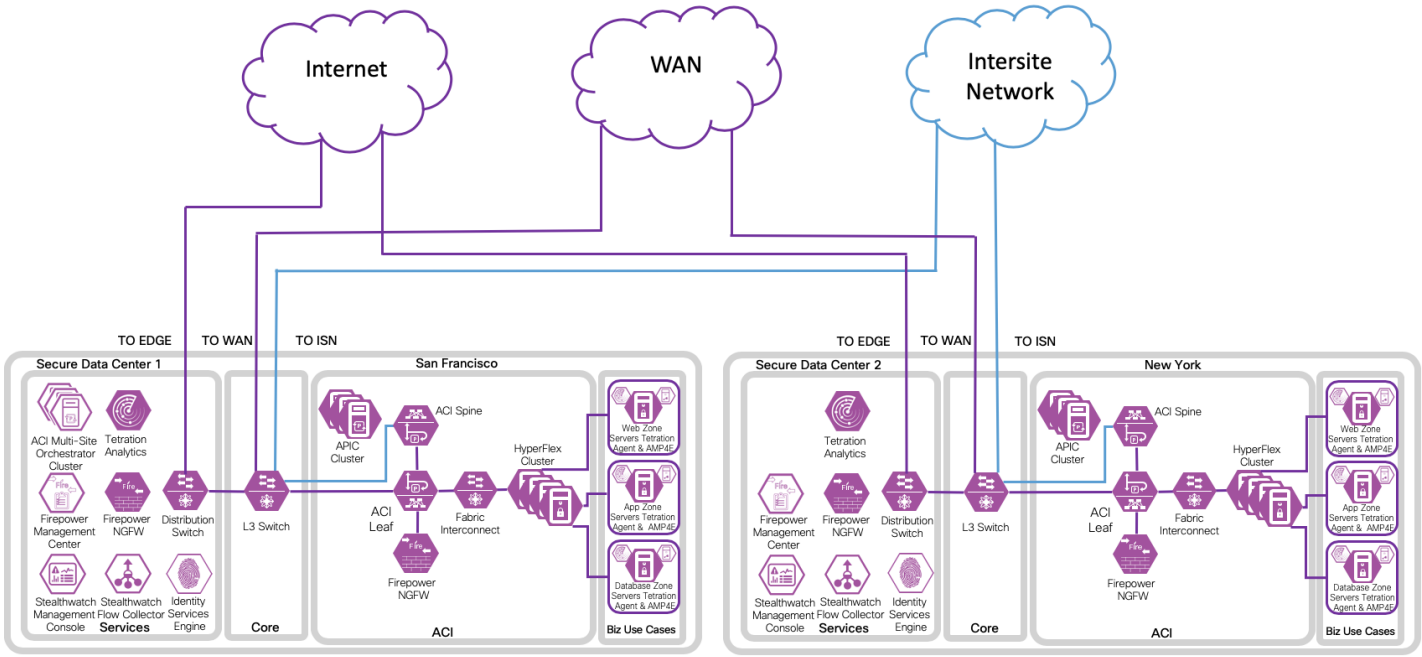
The following figure shows the redundant nodes in the ACI fabric for ACI Spine, ACI Leaf, Firepower NGFW and Fabric Interconnect. The APIC cluster is connected across the redundant leaf switches. A secure overlay management only network is implemented for out of fabric accessibility as a best practice, but is not depicted.



Return to Contents

22

The Cisco ACI Multi-Site Reference Design is a recent evolution in ACI architectures. The need for complete isolation (both network and tenant change domain levels) across separate ACI networks led to the Cisco ACI Multi-Site architecture. The Cisco Multi-Site Orchestrator (MSO) is responsible for provisioning, health monitoring, and managing the full lifecycle of Cisco ACI networking policies and stretched tenant policies across ACI sites around the world. MSO is paired with our extensive cybersecurity portfolio creating Cisco's best in class offering for the modern data center.



Return to Contents

The following sections describe the products in detail and their applicability in the data center.

A tabular listing of all products and the versions tested is available in the Appendix.

ACI

Cisco Application Centric Infrastructure (Cisco ACI™) technology enables customers to integrate virtual and physical workloads in a programmable, multi-hypervisor fabric to build a multiservice or cloud data center. The Cisco ACI fabric consists of discrete components that operate as routers and switches, but it is provisioned and monitored as a single entity. ACI is a holistic architecture with centralized automation and policy-driven application profiles. ACI delivers software flexibility with the scalability of hardware performance.

Key characteristics of ACI include:

- Simplified automation by an application-driven policy model
- Centralized visibility with real-time, application health monitoring
- Open software flexibility for DevOps teams and ecosystem partner integration
- Scalable performance and multi-tenancy in hardware

The future of networking with ACI is about providing a network that is deployed, monitored, and managed in a fashion that supports DevOps and rapid application change. ACI does this through the reduction of complexity and a common policy framework that can automate provisioning and managing of resources.

The following ACI terminology is used in this document. For a complete list, refer to ACI terminology.

Cisco ACI Term	Description
Application Policy Infrastructure Controller (APIC)	The Cisco APIC, which is implemented as a replicated synchronized clustered controller, provides a unified point of automation and management, policy programming, application deployment, and health monitoring for the Cisco ACI multitenant fabric. The minimum recommended size for a Cisco APIC cluster is three controllers.
Application Profile	An application profile defines the policies, services, and relationships between endpoint groups (EPGs).
Contract	The rules that specify what and how communication in a network is allowed. In Cisco ACI, contracts specify how communications between EPGs take place. Contract scope can be limited to the EPGs in an application profile, a tenant, a VRF, or the entire fabric.

Cisco ACI Term	Description
Endpoint Group (EPG)	A logical entity that contains a collection of physical or virtual network endpoints. In Cisco ACI, endpoints are devices connected to the network directly or indirectly. They have an address (identity), a location, attributes (e.g., version, patch level), and can be physical or virtual. Endpoint examples include servers, virtual machines, storage, or clients on the Internet.
Fabric	A fabric is the set of leaf and spines nodes under the control of the same APIC domain. Each fabric represents a separate tenant change domain, because every configuration and policy change applied in the APIC is applied across the fabric. A Cisco ACI fabric thus can be considered an availability zone.
Intersite Network (ISN)	A network where different APIC domains are interconnected through generic Layer 3 infrastructure. ISN requires plain IP routing to allow the establishment of VXLAN tunnels.
L3Out	A routed Layer 3 connection uses a set of protocols that determine the path that data follows in order to travel across multiple networks from its source to its destination. Cisco ACI routed connections perform IP forwarding according to the protocol selected, such as BGP, OSPF, or EIGRP.
Microsegmentation(uSeg) EPGs	Microsegmentation with the Cisco Application Centric Infrastructure (ACI) provides the ability to automatically assign endpoints to logical security zones called endpoint groups (EPGs) based on various attributes.
Multipod	A Multipod design consists of a single APIC domain with multiple leaf-and-spine networks (pods) interconnected. As a consequence, a Multi-Pod design is functionally a fabric (a single availability zone), but it does not represent a single network failure domain, because each pod runs a separate instance of control-plane protocols. For more details, refer to the Multipod White Paper: https://www.Cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737855.html
Multi-Site	A Multi-Site design is the architecture interconnecting multiple APIC cluster domains with their associated pods. A Multi-Site design could also be called a Multi-Fabric design, because it interconnects separate availability zones (fabrics), each deployed either as a single pod or multiple pods (a Multi-Pod design). For more details, refer to the Multi-Site White Paper: https://www.Cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html.

Cisco ACI Term	Description
Pod	A pod is a leaf-and-spine network sharing a common control plane (Intermediate System–to–Intermediate System [ISIS], Border Gateway Protocol [BGP], Council of Oracle Protocol [COOP], etc.). A pod can be considered a single network fault domain.
Policy-Based Redirect (PBR)	PBR is a primary feature of the service graph. The service graph must have a contract between two EPGs attached. Traffic redirection is based on the source EPG, destination EPG, and filter (protocol, source Layer 4 port, and destination Layer 4 port) configuration in the contract. For more details, refer to the PBR Service Graph Whitepaper, https://www.Cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739971.html
Service Graph	A service graph is a concept where Cisco ACI can insert Layer 4 through Layer 7 services into the fabric. Cisco ACI can redirect traffic between security zones to a firewall or a load balancer without the need for the firewall or the load balancer to be the default gateway for the servers.
Tunnel Endpoint (TEP) Address Pool	The TEP Address pool is used by the Cisco ACI fabric which automatically discovers the fabric switch nodes, assign the infrastructure TEP addresses to the switch nodes. It is a critical part of the configuration and should

ACI Multi-Site

The design described in this document is based on the ACI Multi-Site reference design. We tested with two sites: San FranCisco and New York, each with a single pod. The hardware components tested for each site are represented in the following table.

Hardware Component	Data Center 1 San FranCisco	Data Center 2 New York
APIC	APIC-SERVER-L1 (3), recommend moving to APIC-CLUSTER-L2 (1), Cluster of 3 Cisco APIC devices with large CPU, hard drive, and memory configurations (more than 1000 edge ports), dual attached to fabric, https://www.Cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-apic/datasheet-c78-739715.html	APIC-SERVER-M1(3), recommend moving to APIC-CLUSTER-M2 (1), Cluster of 3 Cisco APIC devices with medium CPU, hard drive, and memory configurations (more than 1000 edge ports), dual attached to fabric, https://www.Cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-apic/datasheet-c78-739715.html
Spines	Nexus 9500 Platform, N9K-C9504 (2), Each Chassis: Supervisor Module N9K-SUP-A (2), Line module N9K-X9736C-FX (1), Fabric module N9K-C9504-FM-E (3), https://www.Cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-732088.html	Cisco Nexus 9364C Switch, N9K-C9364C (2), Cisco NX-OS Fixed Spine Switch, https://www.Cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-739886.html
Leafs	Nexus 9300-FX Platform Leaf Switch (2), N9K-C93180YC-FX, 48 x 1/10/25-Gbps fiber ports and 6 x 40/100-Gbps QSFP28 ports. Note: Includes built-in Tetration hardware sensors, dual attached to spines, https://www.Cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-738259.html	Nexus 9300-FX Platform Leaf Switch (2), N9K-C93180YC-FX, 48 x 1/10/25-Gbps fiber ports and 6 x 40/100-Gbps QSFP28 ports. Note: Includes built-in Tetration hardware sensors, dual attached to the spines, https://www.Cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-738259.html

Return to Contents

Hardware Component	Data Center 1 San FranCisco	Data Center 2 New York
Compute	UCS 5108 Blade Server Chassis, UCS B-Series (1), each chassis has UCSB-B200-M4 blade servers (4), deployed with VMware ESXi hypervisor by vCenter, dual attached to fabric, https://www.Cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-5100-series-blade-server-chassis/data_sheet_c78-526830.html	HyperFlex HX240c M5 All Flash Four Node cluster, deployed with VMware ESXi hypervisor by vCenter, dual attached to fabric, https://www.Cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/datasheet-c78-736784.pdf
Fabric Interconnects	Cisco UCS 6248UP (2), 48-port fabric interconnect, UCS-FI-6248UP, https://www.Cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-6200-series-fabric-interconnects/data_sheet_c78-675245.html	Cisco UCS 6332 16UP (2), 40-port fabric interconnect, UCS-FI-6332-16UP, https://www.Cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-6300-series-fabric-interconnects/datasheet-c78-736682.html
Next Generation Firewalls	Firepower 9300 Security Appliance (2), each chassis with one SM-36 Module, deployed as an unmanaged PBR service graph with a one-arm interface for North-South and East-West traffic, clustering, dual attached to fabric, https://www.Cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html	Firepower 4110 (2), deployed as an unmanaged PBR service graph with a one-arm interface for North-South and East-West traffic, clustering, dual attached to the fabric, https://www.Cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html

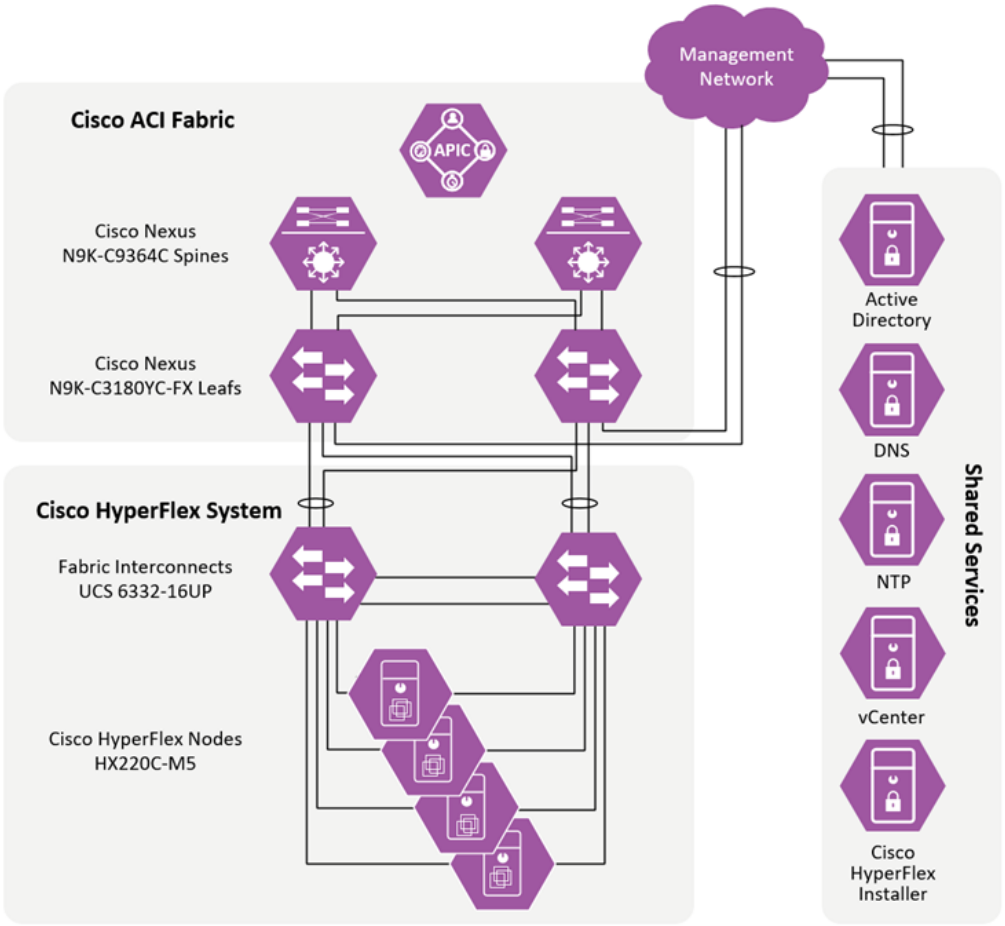
HyperFlex

Cisco HyperFlex™ systems with Intel® Xeon® Scalable processors deliver hyperconvergence with the power and simplicity for any application, on any cloud, and at any scale. Engineered on the Cisco Unified Computing System™ (Cisco UCS®), Cisco HyperFlex™ systems deliver the agility, scalability, and pay-as-you-grow economics of the cloud with the benefits of on-premises infrastructure.

Our platform includes hybrid or all-flash configurations, an integrated network fabric, and powerful data optimization features that bring the full potential of hyperconvergence to a wide range of workloads and use cases, from validated enterprise applications to edge computing. Our solution is faster to deploy, simpler to manage, and easier to scale than the current generation of systems. It is ready to provide you with a unified pool of infrastructure resources to power applications as the business needs dictate.

Cisco HyperFlex™ HX Series Datasheet, https://www.Cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/datasheet-c78-736784.pdf

This solution meets high availability design requirements and is physically redundant across the computing, network, and storage stacks. All the common infrastructure services required by this solution, such as Microsoft Active Directory, Domain Name System (DNS), Network Time Protocol (NTP), and VMware vCenter, are hosted on common management infrastructure outside the Cisco HyperFlex system.



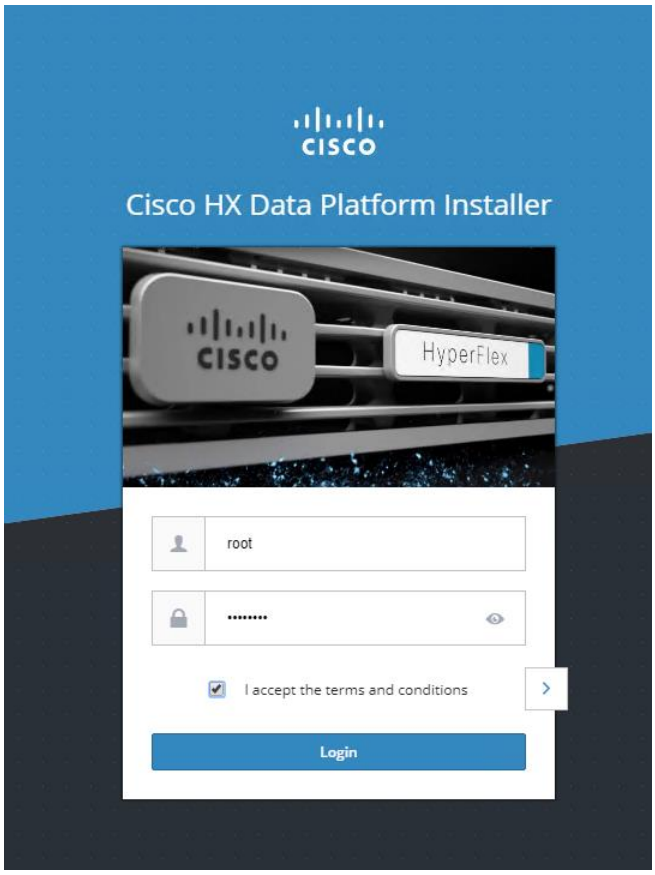
The diagram above illustrates a small deployment of the Hyperflex system. The system consists of two Cisco Fabric Interconnects and four Cisco Hyperflex nodes. It connects to the infrastructure via the leaf switches and utilizes the existing shared services.

Return to Contents

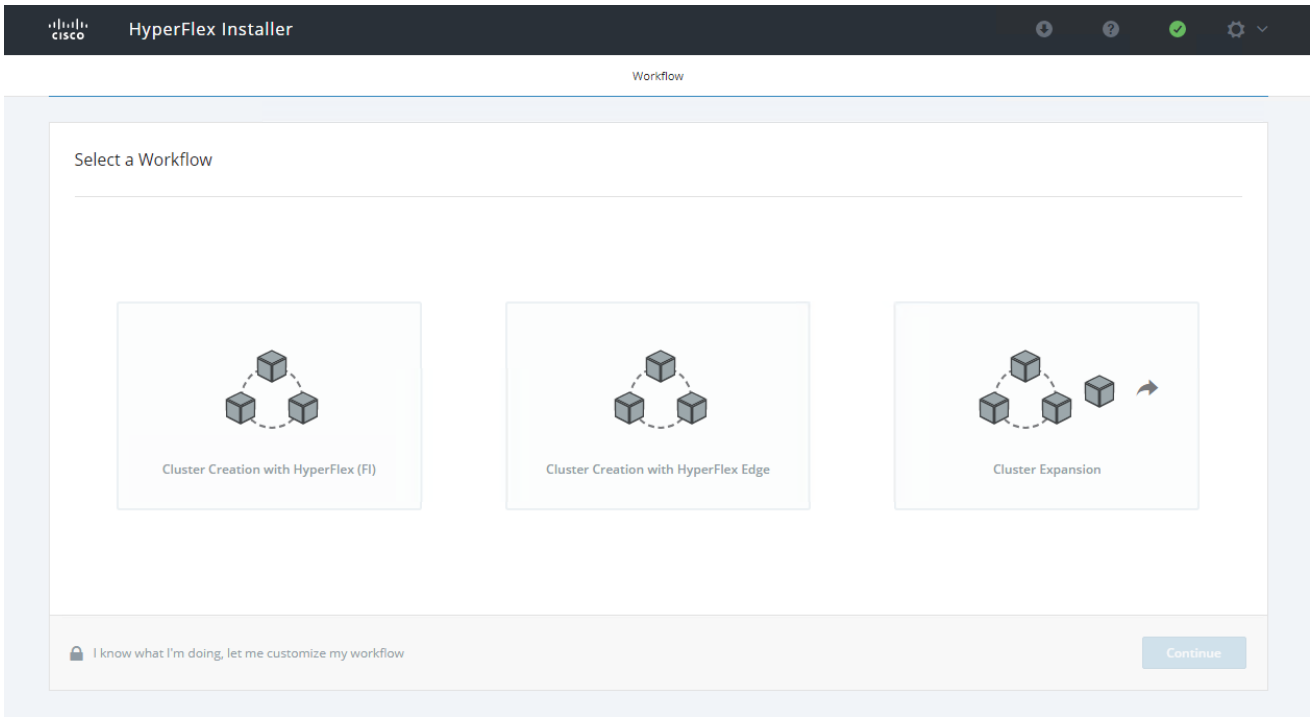
We followed this installation guide to setup a four node HyperFlex HX240c M5 All Flash cluster. Cisco HyperFlex™ Systems Installation Guide for VMware ESXi, Release 4.0(1a), https://www.Cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/Installation_VMWare_ESXi/4_0/b_HyperFlexSystems_Installation_Guide_for_VMware_ESXi_4_0.html. We setup the HyperFlex™ cluster in Data Center 2 – New York.

Additionally, we started with the Pre-Installation Checklist for VMware with Cisco HX platform, https://www.Cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HyperFlex_Preinstall_Checklist/b_HX_Data_Platform_Preinstall_Checklist.html.

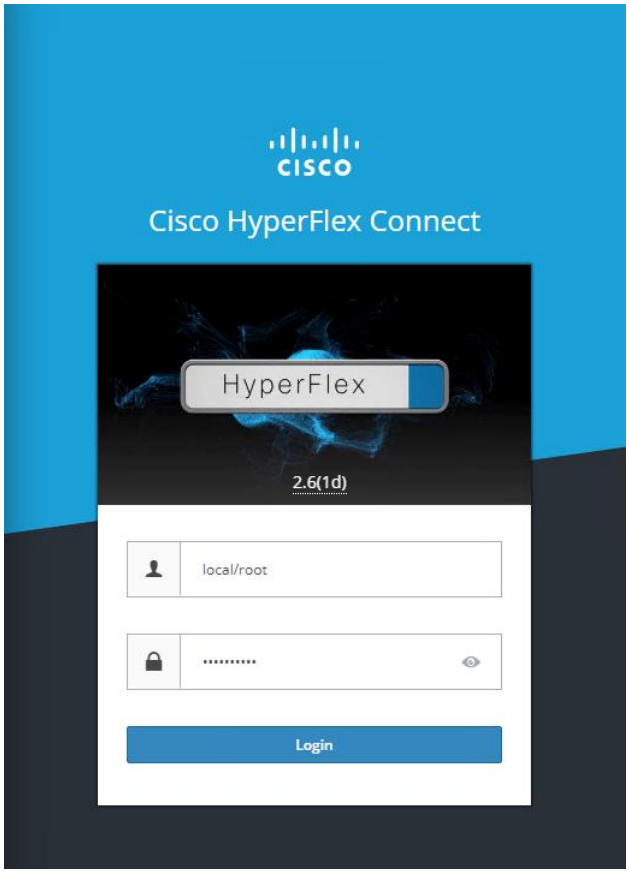
To install or expand the HyperFlex™ cluster you need to log into the Cisco HX Data Platform Installer and then select the desired workflow.



Return to Contents

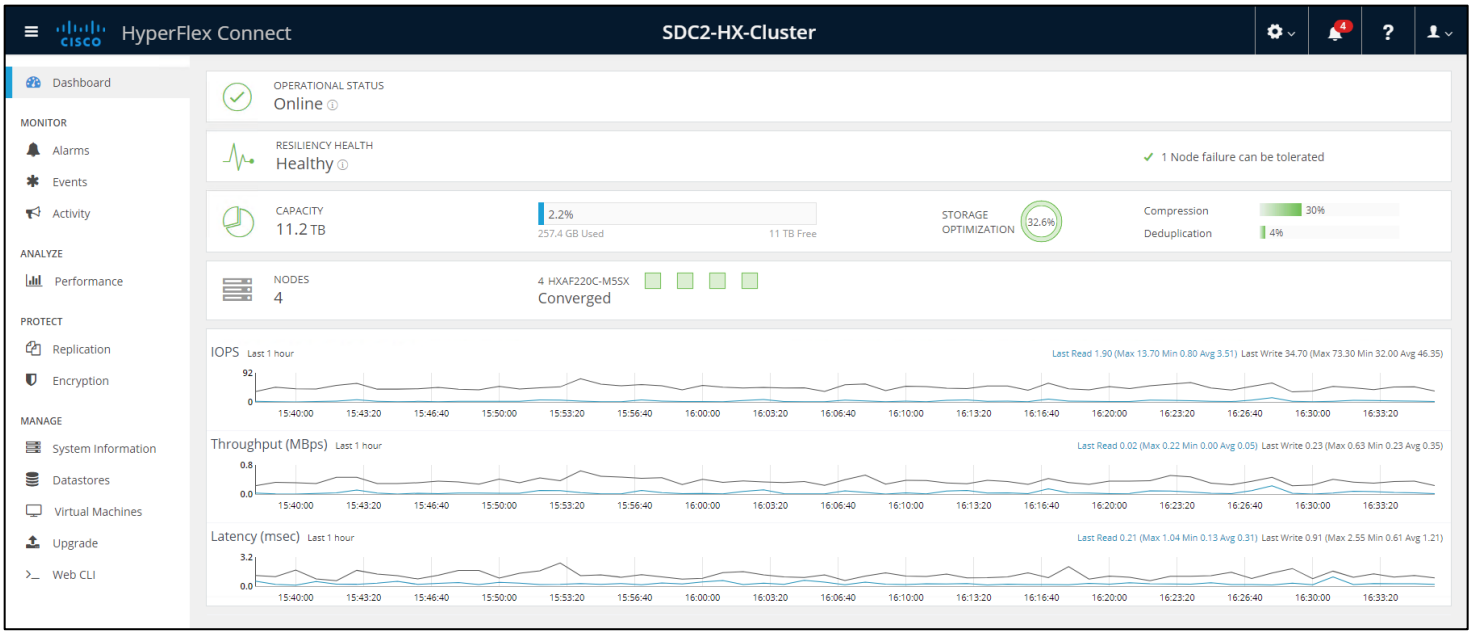


To Monitor and Manage the HyperFlex™ cluster you need to login to Hyperflex™ Connect.



Return to Contents

The figure below is the Dashboard for HyperFlex™ Connect.



The HyperFlex™ platform supports self-encrypting drives (SEDs) as well as additional security recommendations for VMware ESXi, Cisco UCS and HyperFlex™ hardening that are covered in the HyperFlex™ Hardening Guide 3.5, refer to https://www.Cisco.com/c/dam/en/us/support/docs/hyperconverged-infrastructure/hyperflex-hx-data-platform/HX-Hardening_Guide_v3_5_v12.pdf for details.

There is a Cisco Validated Design (CVD) based on the data center design used in this Secure Data Center CVD, refer to Design and Deployment Guide for Cisco HyperFlex 3.0 with VMware vSphere 6.5U2, Cisco UCS Manager 3.2, Cisco ACI 3.2, and Cisco UCS 6300 Series Fabric Interconnects, https://www.Cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/hx_30_vsi_aci_32.pdf

Firepower Next Generation Firewall

Most next-generation firewalls (NGFWs) focus heavily on enabling application control, but little on their threat defense capabilities. To compensate, some NGFW's will try to supplement their first-generation intrusion prevention with a series of non-integrated add-on products. However, this approach does little to protect your business against the risks posed by sophisticated attackers and advanced malware. Further, once you do get infected, they offer no assistance in scoping the infection, containing it, and remediating quickly. What you need is an integrated, threat-centric next-generation firewall. One that not only delivers granular application control, but also provides effective security against the threats posed by sophisticated and evasive malware attacks.

The Cisco Firepower Next-Generation Firewall (NGFW) is the industry's first fully integrated, threat-focused NGFW. It delivers comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint.

The Cisco Firepower NGFW includes the industry's most widely deployed stateful firewall and provides granular control over more than 4,000 commercial applications. Its single management interface delivers unified visibility from the network to the endpoint. Firepower NGFW enables comprehensive policy management that controls access, stops attacks, defends against malware and provides integrated tools to track, contain and recover from attacks that do get through.

Return to Contents

Firepower 4110 and Firepower 9300 have been have been tested in the Multi-Site reference design providing protection for North-South and East-West traffic between the data center servers. The FP4100/FP9000 platforms have been tested as an unmanaged device with a Policy Based Redirect (PBR) service graph implemented as a one-arm interface. Firepower Threat Defense (FTD) intra-site clustering was tested.

The management components tested for each site are represented in the following table.

Management Component	Description
ACI Multi-Site Orchestrator	Cluster of three ACI Multi-Site Orchestrator (MSO) virtual machines. MSO is responsible for provisioning, health monitoring, and managing the full lifecycle of Cisco ACI networking policies and stretched tenant policies across all ACI sites. For more information on Cisco ACI Multi-Site Architecture, refer to the whitepaper here: https://www.Cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html
Firepower Management Center	Firepower Management Center (FMC) is the administrative nerve center for select Cisco security products running on a number of different platforms. It provides complete and unified management of firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. Security administrators will use FMC to manage the security policy of Firepower Threat Defense (FTD) software that is running on the Firepower 9300 and 4110 in this reference architecture. https://www.Cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html
Firepower Chassis Manager	Firepower Chassis Manager is a web interface that makes it easy to configure Firepower 2100/4100/9300 platform settings and interfaces, provision devices, and monitor system status.
UCS Manager	Cisco UCS® Manager provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) and Cisco HyperFlex™ Systems across multiple chassis and rack servers and thousands of virtual machines. https://www.Cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/data_sheet_c78-520522.html
VMware vCenter	VMware vCenter Server® provides a centralized and extensible platform for managing VMware vSphere® environments, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vCenter/vmw-datasheetvcenter.pdf

The following cybersecurity solutions for the data center: Stealthwatch, Tetration and Advanced Malware Protection for Endpoints (AMP4E) were also tested with the ACI Multi-Site reference design. However, all of these solutions can also be used in ACI Multipod or non-ACI data center environments.

Stealthwatch

Cisco Stealthwatch™ provides continuous real-time monitoring of, and pervasive views into, all network traffic. It dramatically improves visibility across the extended network and accelerates response times for suspicious incidents. It creates a baseline of normal web and network activity for a network host, and applies context-aware analysis to automatically detect anomalous behaviors. Stealthwatch™ can identify a wide range of attacks, including malware, zero-day attacks, distributed denial-of-service (DDoS) attempts, advanced persistent threats (APTs), and insider threats.

Stealthwatch™ Enterprise dramatically improves:

- Real-time threat detection
- Incident response and forensics
- Network segmentation
- Network performance and capacity planning
- Ability to satisfy regulatory requirements

For more information on Stealthwatch refer to https://www.Cisco.com/c/en/us/products/security/stealthwatch/index.html.

We deployed Stealthwatch™ Management Console (SMC) and Stealthwatch™ Flow Collector as virtual appliances in our secure data center solution. We deployed the minimum SMC configuration for one Flow Collector with only 2 concurrent users, as well as the minimum Stealthwatch™ Flow Collector configuration.

Stealthwatch™ Management Console Virtual Edition (SMC VE)	VMware vSphere Settings Tested
Release 7.0	• ESXi 6.0 • 3 vCPUs • 16 GB of RAM • 50 GB disk

Stealthwatch™ Flow Collector Virtual Edition	VMware vSphere Settings Tested
Release 7.0	• ESXi 6.0 • 2 vCPUs • 16 GB of RAM • 50 GB disk

To deploy these two virtual machines, we followed the Stealthwatch™ Installation Guide 7.0, https://www.Cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf.

Tetration

The Cisco Tetration platform enables holistic workload protection for multicloud data centers by using:

- Allowed/Blocked list-based segmentation, allowing operators to control network communication within the data center, enabling a zero-trust model
- Behavior baselining, analysis, and identification of deviations for processes running on servers
- Detection of common vulnerabilities and exposures associated with the software packages installed on servers
- The ability to act proactively, such as quarantining server(s) when vulnerabilities are detected and blocking communication when policy violations are detected.

The Cisco Tetration platform is powered by big-data technologies to support the scale requirements of data centers. It can process comprehensive telemetry information received from servers in near-real time (up to 25,000 servers per cluster). Tetration can enforce consistent policy across thousands of applications and hundreds of millions of policy rules. And it is designed for long-term data retention to enable powerful forensics for such things as identifying incidents and operational troubleshooting.

The Tetration platform addresses important data center security challenges by providing behavior-based application insight, automating allowed/blocked policy generation, and enabling zero-trust security using application segmentation.

The Tetration enforcement layer ensures that policies move with workloads, even when application components are migrated from a bare-metal server to a virtualized environment. In addition, the platform helps ensure scalability through consistent policy implementation for thousands of applications spanning tens of thousands of workloads.

The platform is designed to normalize and automate policy enforcement within the application workload itself, track policy-compliance deviations, and keep the application segmentation policy up to date as application behavior changes. With this approach, Tetration provides stateful and consistent enforcement across virtualized and bare-metal workloads running in private, public, and on-premises data centers.

Tetration agents

Tetration agents are software sensor agents that runs within a host operation system, such as Linux or Windows. An agent's core functionality is to monitor and collect network flow information and enforce micro-segmentation policies. Agents collect other host information such as network interfaces and active processes running in the system. Information collected by agents is exported for further analytical processing to a set of collectors running within the Tetration Analytics cluster. In addition, software agents also have capability to set firewall rules on installed hosts (enforcement agents).

Tetration supports a wide range of sensors for both visibility and enforcement. For details, refer to the Tetration Platform support and compatibility information.

Follow the Deploying Cisco Tetration Software Agents Installation Guide.

We deployed the Tetration enforcement agent on all application servers, which when possible is the ideal deployment scenario for maximizing Tetration capabilities. We tested the Windows Server 2016 for Data Center and CentOS 7.4 enforcement agents.

Tetration Edge Virtual Appliance

The Tetration Edge is a control appliance that streams alerts to various notifiers and collects inventory metadata from network access controllers such as Cisco ISE. In a Tetration Edge appliance, all alert notifier connectors (such as Syslog, Email, Slack, PagerDuty and Kinesis) and ISE connector can be deployed. The function of the ISE Connector is to connect to ISE using pxGrid and provides Tetration with endpoints contextual information, such as MDM details, authentication, Security Group tags, etc as seen by ISE. The information is regularly updated and can be used in Tetration filters and policies.

Advanced Malware Protection

Advanced Malware Protection (AMP) comprises three components that were tested as part of the Secure Data Center design:

- Cisco Advanced Malware Protection for Endpoints
- Cisco Advanced Malware Protection for Networks
- Cisco Threat Grid

Cisco Advanced Malware Protection for Endpoints (AMP4E) is a cloud-managed endpoint security solution that provides the visibility, context, and control to prevent breaches, but also rapidly detect, contain, and remediate threats if they evade front-line defenses and get inside, all cost-effectively and without affecting operational efficiency.

Prevent: Strengthen defenses using the best global threat intelligence and block malware in real time.
Detect: Continuously monitor and record all file activity to quickly detect stealthy malware.
Respond: Accelerate investigations and automatically remediate malware across servers.

Host-based anti-malware is the last line of defense, and often the only defense for communications encrypted end-to-end (password protected archives, https/sftp, chat file transfers, etc.). AMP analyzes all files that reach the server's system. If the file is known to be malicious, it is quarantined immediately. We deployed AMP4E on all application servers including the application servers in AWS.

Cisco Advanced Malware Protection for Networks (AMP4N) delivers network-based advanced malware protection that goes beyond point-in-time detection to protect your organization across the entire attack continuum—before, during, and after an attack. Designed for Cisco Firepower® network threat appliances, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.

Cisco Threat Grid combines static and dynamic malware analysis with threat intelligence into one unified solution. It provides in-depth information to protection against malware of all types. It integrates real-time behavioral analysis and up-to-the-minute threat intelligence feeds with existing security technologies, protecting from both known and unknown attacks.

Identity Services Engine (ISE)

The Cisco Identity Services Engine (ISE) is a one-stop solution to streamline security policy management and reduce operating costs. ISE provides visibility to users and devices and controls access across wired, wireless, and VPN connections to the corporate network.

Cisco ISE offers a holistic approach to network access security. There are many advantages when ISE is deployed, including:

- Highly secure business and context-based access based on company policies
- Streamlined network visibility through a simple, flexible, and highly consumable interface
- Extensive policy enforcement that defines easy, flexible access rules that meet ever-changing business requirements
- Robust guest experiences that provide multiple levels of access to the network
- Self-service device onboarding for the enterprise's Bring-Your-Own-Device (BYOD) or guest policies

Platform Exchange Grid (pxGrid)

The Cisco pxGrid (Platform Exchange Grid) is an open, scalable and IETF standards-driven data-sharing and threat control platform. It allows multiple security products to work together. Security operations teams can automate to get answers faster and contain threats faster.

pxGrid primary benefits are:

Simpler integration: Use one API for open, automated data sharing and control between more than 50 security products
Instant visibility: Have all contextual and relevant data on a single screen
Fast investigations: Conduct a full analysis on one system for fast answers
Even faster responses: Stop threats instantly using the network as an enforcer

pxGrid Components:

pxGrid controller: The controller orchestrates connections between platforms. It authorizes what contextual information gets shared between those platforms. The control function is provided by ISE.

pxGrid connection agent: A connection agent is integrated into Cisco platforms as well as many partner platforms. The platform decides which information it wants to share with other platforms. In this design guide, the pxGrid connection agent tested was in the Tetration Edge Virtual appliance.

Validation Testing

Test Case	Integration	Visibility	Segmentation	Threat Protection	Orchestration and Management	Benefits
1	ACI Multi-Site Orchestrator (MSO) and Firepower Threat Defense (FTD)		✓		✓	• Enables Firepower Threat Defense (FTD) to be automated by MSO and inserted between applications in an ACI Multi-Site fabric • MSO simplifies configurations to multiple APIC domains deployed globally
2	Firepower Management Center (FMC) and APIC		✓		✓	• Enables Firepower Threat Defense (FTD) to be automated by APIC and inserted between applications in an ACI Multipod fabric
3	Tetration and VMware vCenter (VM attributes)	✓	✓			• Provides protection for east-west traffic in VMware vCenter environments • Enables richer context for analysis by Tetration Analytics Appliance • Provides Zero trust or allowed/blocked list model • Reduces the impact of policy changes
4	Stealthwatch Enterprise and Tetration	✓				• Monitors network behaviors for threat indicators and breaches • Continuous device discovery and classification • Incident response and forensics • Network performance and capacity planning
5	AMP and Firepower Threat Defense	✓		✓		• Provides a single pane of glass for visibility and analytics for Advanced Malware Protection (AMP) for NGFW, NGIPS and AMP4E
6	FTD Rapid Threat Containment and APIC			✓		• Automated Response • Prevents further lateral movement of infection by protecting other hosts in Endpoint Group (EPG)
7	FTD Rapid Threat Containment and Tetration			✓		• Automated Response • Prevents further lateral movement of infection by protecting other hosts in microsegment
8	Tetration and Identity Services Engine (ISE)	✓	✓			• Extends User Access Policy for enhanced enforcement in the Data Center • Provides Zero trust or allow/block list model
9	TrustSec, ISE, APIC and FMC	✓	✓			• Extends User Access Policy for enhanced enforcement in the Data Center • Provides Zero trust or allow/block list model

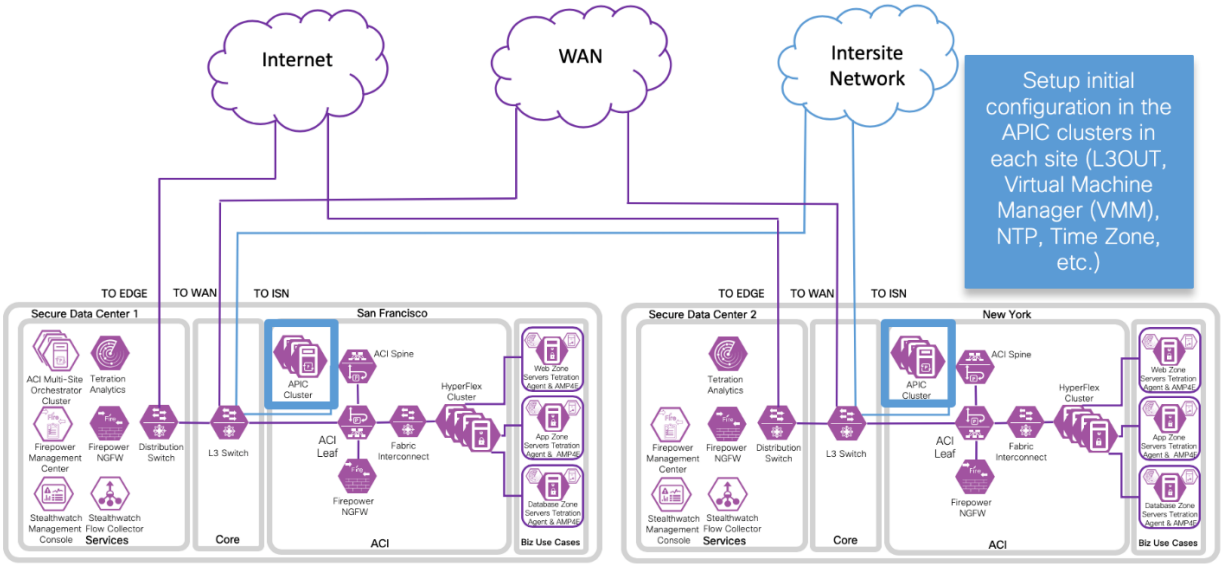
⮌ Return to Contents

Test Case 1 – ACI Multi-Site Orchestrator and Firepower Threat Defense

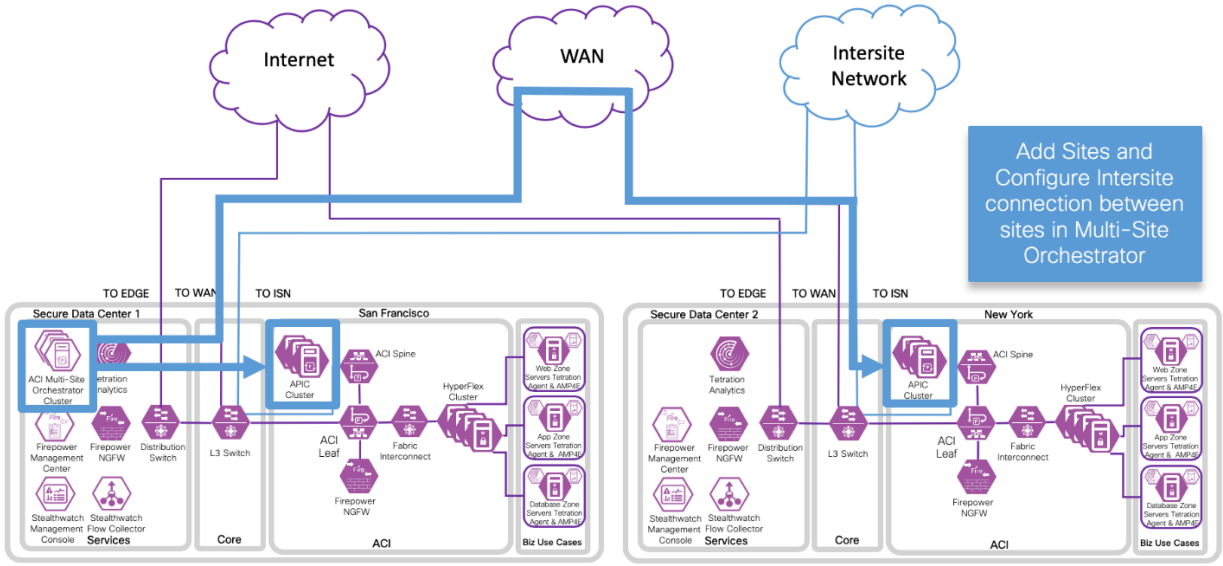
This test case involved building out the secure data center reference architecture for ACI Multi-Site. FTD is deployed as a one arm cluster in each data center. FTD is the L4-L7 service providing threat defense services for north-south and east-west traffic in the data center fabric.

Test case overview:

1. Setup initial configuration in the APIC clusters in each site (NTP, Timezone, L3OUT, Add FTD device, etc).

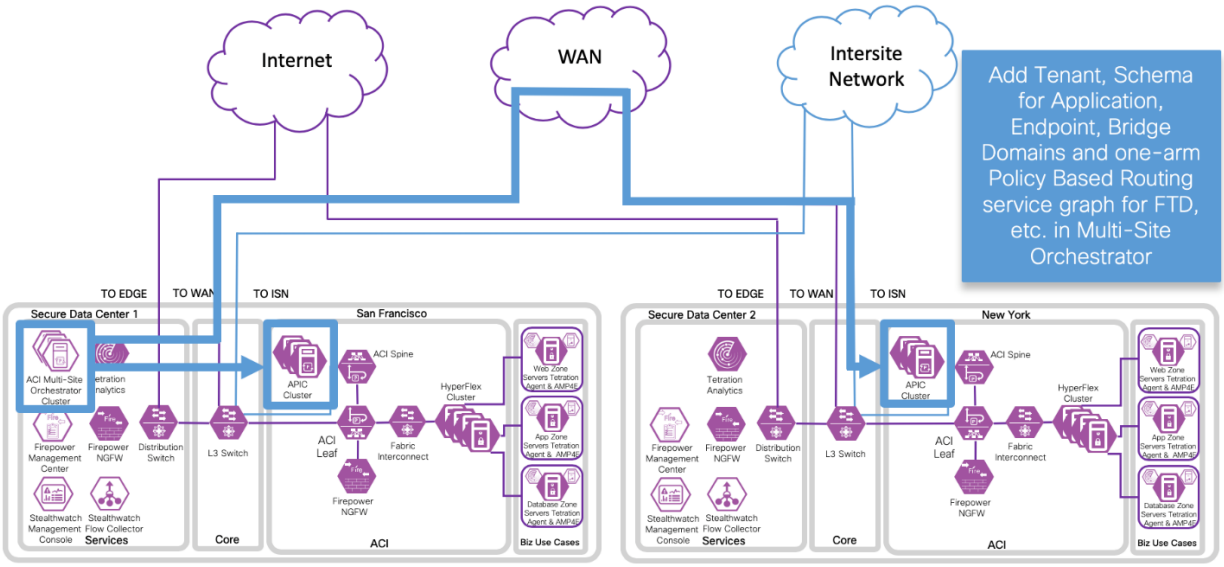


2. Add Sites and configure Intersite connection between sites in ACI Multi-Site Orchestrator.



Return to Contents

3. Add a Schema for a three tier application, EPGs, Bridge Domains and one-arm Policy Based Redirect service graph for FTD.



Return to Contents

Implementation Procedure

Step A: Determine the ACI Multi-Site deployment configuration details

Step B: Setup the ACI Fabric

- Step 1: APIC Initial Configuration
- Step 2: Out-of-Band Management
- Step 3: Pod Date and Time Policy
- Step 4: VLANs
- Step 5: Initial L3Out
- Step 6: Fabric Interconnect Interfaces
- Step 7: VMM Domain
- Step 8: FTD Cluster Control Link (CCL) and Data Interfaces
- Step 9: Overlay Tunnel Endpoint (TEP) for Intersite
- Step 10: Multi-Site Orchestrator (MSO) Admin Account

Step C: Install and Setup initial Multi-Site Orchestrator (MSO)

- Step 1: Install MSO
- Step 2: Setup Day 0 Operations in MSO GUI
- Step 3: Configure Fabric Connectivity Infrastructure (Infra) in MSO GUI
- Step 4: Validate Intersite Policy with the MSO Dashboard
- Step 5: Add Tenants using MSO GUI

Step D: Create one-arm FTD cluster, PBR and an L3Out on Tenant in APIC GUI

- Step 1: Deploy one-arm Firepower Threat Defense cluster as a L4-L7 Device in APIC GUI
- Step 2: Create Policy Based Redirect (PBR) policy in APIC GUI
- Step 3: Create initial L3Out policy in APIC GUI

Step E: Add Schema with MSO GUI

- Step 1: Create Schema
- Step 2: Add Sites
- Step 3: Create or Import VRF
- Step 4: Create Service Graph
- Step 5: Create External EPG
- Step 6: Create Filters
- Step 7: Create Bridge Domains
- Step 8: Create Contracts
- Step 9: Create Application Profile
- Step 10: Add Contracts to External EPG

Step F: Verify Schema in APIC GUI

Return to Contents

These are the steps we followed to implement the ACI Multi-Site reference design. Refer to Appendix A for the Secure Data Center Lab Diagram.

The APIC cluster configuration backup and the Tenant configuration files in XML and JSON for both data centers are available here: https://github.com/Cisco-security/Cisco-Validated-Designs/tree/master/Secure-Data-Center/APIC.

Step A: Determine the ACI Multi-Site configuration details

a. Determine configuration details for the design that you plan to deploy. The following table represents the common configuration details.

object	value
MSO node1 IP address	10.18.1.11/24
MSO node2 IP address	10.18.1.12/24
MSO node3 IP address	10.18.1.13/24
OSPF Area	0

b. Determine the site-specific configuration details.

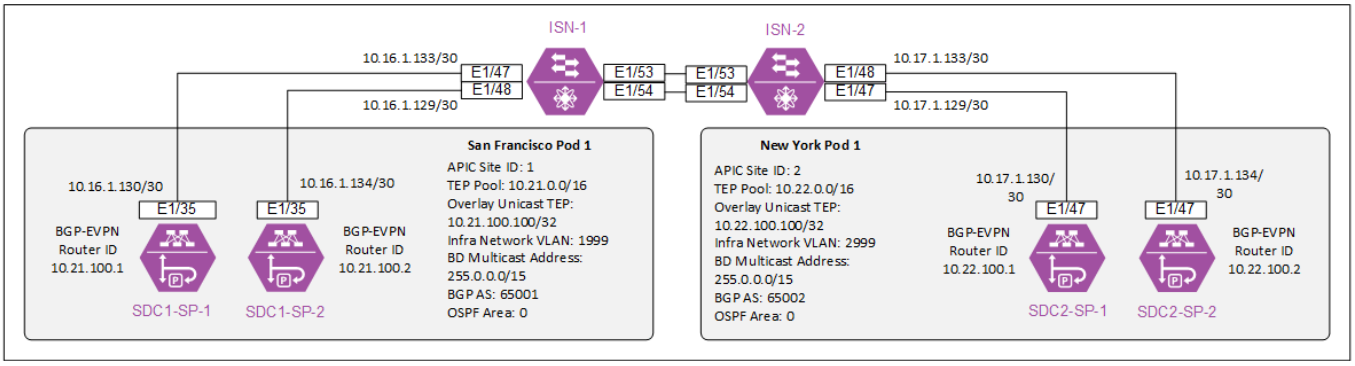
object	Data Center 1 – San FranCisco	Data Center 2 – New York
APIC – 1 IP address	10.16.1.11/24	10.17.1.11/24
APIC – 2 IP address	10.16.1.12/24	10.17.1.12/24
APIC – 3 IP address	10.16.1.13/24	10.17.1.13/24
APIC site id	1	2
BGP Route Reflector: Autonomous System Number	65001	65002
External Routed Domain	SDC1-L3OUT	SDC2-L3OUT
Leaf 1 Management IP Address	10.16.1.17/24	10.17.1.17/24

Leaf2 Management IP Address	10.16.1.18/24	10.17.1.18/24
Spine 1: Management IP address	10.16.1.19/24	10.17.1.19/24
Spine 1: Port ID	1/35	1/47
Spine 1: ISN address	10.16.1.130/30	10.17.1.134/30
Spine 1: Control Plane IP address (BGP-EVPN ROUTER-ID)	10.21.100.1	10.22.100.1
Spine 2: Management IP address	10.16.1.20/24	10.17.1.20/24
Spine 2: Port ID	1/35	1/47
Spine 2: ISN Address	10.16.1.134	10.17.1.134
Spine 2: Control Plane IP address (BGP-EVPN ROUTER-ID)	10.21.100.2	10.22.100.2

object	Data Center 1 – San FranCisco	Data Center 2 – New York
TEP Address Pool	10.21.0.0/16	10.22.0.0/16
Data Plane Unicast TEP IP address	10.21.100.100	10.22.100.100
Data Plane Multicast TEP IP address	10.21.100.200	10.22.100.200
Multipod Data Plane TEP	10.21.200.200/32	10.22.200.200/32
Address pool for BD multicast addresses (GIPO)	255.0.0.0/15	255.0.0.0/15

⮌ Return to Contents

Intersite Network overview



Step B: Setup the ACI fabric

Prepare the ACI fabric for the Multi-Site Orchestrator deployment. APIC configuration is required which includes setting up the L3Outs, Fabric Interconnects, and Firepower Threat Defense clusters.

The following ACI references were used to determine the steps we followed:

Cisco APIC Getting Started Guide, Release 4.1, Section: Initial Setup and Fabric Initialization and Switch Discovery https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/getting-started/b-Cisco-APIC-Getting-Started-Guide-411/b-Cisco-APIC-Getting-Started-Guide-411_chapter_010.html

Cisco APIC Basic Configuration Guide, Release 4.x
https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/basic-configuration/Cisco-APIC-Basic-Configuration-Guide-411.html

Cisco APIC Layer 2 Networking Configuration Guide, Section: Creating Domains, and VLANS to Deploy an EPG on a Specific Port Using the GUI,
https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/L2_config/b_Cisco_APIC_Layer_2_Configuration_Guide/b_Cisco_APIC_Layer_2_Configuration_Guide_chapter_011.html#task_A47A972D56A34061A5E0709F8AACB675

Cisco Community, Factory reset APICs and Nodes
https://community.Cisco.com/t5/application-centric/factory-reset-apic-and-nodes/td-p/3408371

Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x), Section: MP-BGP Route Reflectors https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/L3-configuration/Cisco-APIC-Layer-3-Networking-Configuration-Guide-411/Cisco-APIC-Layer-3-Networking-Configuration-Guide-411_chapter_01010.html

Cisco ACI Best Practices Guide, Section: VMM Integration with UCS-B Series
https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/ACI_Best_Practices/b_ACI_Best_Practices/b_ACI_Best_Practices_chapter_0101.html

Configure VMM Domain Integration with ACI and UCS-B Series
https://www.Cisco.com/c/en/us/support/docs/cloud-systems-management/application-policy-infrastructure-controller-apic/118965-config-vmm-aci-ucs-00.html

Cisco ACI Virtualization Guide 4.1, Chapter Cisco ACI with VMWare VDS Integration

Cisco UCS Manager Network Management Guide, Release 4.0, Section LAN Pin Groups

https://www.Cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/4-0/b_UCSM_Network_Mgmt_Guide_4_0/b_UCSM_Network_Mgmt_Guide_4_0_chapter_0101.html

The following steps will guide you through the setup of Secure Data Center 1 (SDC1) – San FranCisco. Repeat Step 1 through 8 to setup the Secure Data Center 2 (SDC2) – New York. Replace the names and IPs in these steps with appropriate values. Examples Names: SDC2-LF1 and IP:10.17.x.x.

Section Summary:

Step 1: APIC Initial Configuration

Step 2: Out-of-Band Management

Step 3: Pod Date and Time Policy

Step 4: VLANs

Step 5: Initial L3Out

Step 6: Fabric Interconnect Interfaces

Step 7: VMM Domain

Step 8: FTD Cluster Control Link (CCL) and Data Interfaces

Step 9: Overlay Tunnel Endpoint (TEP) for Intersite

Step 10: Multi-Site Orchestrator (MSO) Admin Account

Step 1: APIC Initial Configuration

a. Connect to the APICs console with a monitor and keyboard or CIMC/KVM (recommended).

b. (Optional) If you need to factory reset your APIC controllers and switches issue the following commands.

```
apic# acidiag touch clean
apic# acidiag touch setup
This command will wipe out this device. Proceed? [y/N] y
```

Simultaneously reboot all APICs.

```
apic# acidiag reboot
This command will restart this device, Proceed? [y/N] y
```

While the APICs are rebooting, connect to each switch and run **setup-clean-config.sh** and **reload**.

c. Once the APICs have booted, the Cluster Configuration will start automatically.

Complete the Cluster Configuration with the following information.

Fabric name: **SDC1 Fabric**

Number of controllers in the fabric: **3**

Controller ID: **1** *(APIC2: **2**, APIC3: **3**)*

Controller name: **SDC1-APIC1** *(APIC2: **SDC1-APIC2**, APIC3: **SDC1-APIC3**)*

Address pool for TEP addresses: **10.21.0.0/16**

VLAN ID for infra network: **1999**

Address pool for BD multicast addresses (GIPO): **255.0.0.0/15**

Management IPv4 addr: **10.16.1.11/24** *(APIC2: **10.16.1.12/24**, APIC3: **10.16.12/24**)*

Management default gateway: **10.16.1.1**

Enable strong passwords? **Y**

Enter the password for admin: **XXXXXXXX**

Reenter the password for admin: **XXXXXXXX**

Repeat this step for SDC1-APIC2 and SDC1-APIC3

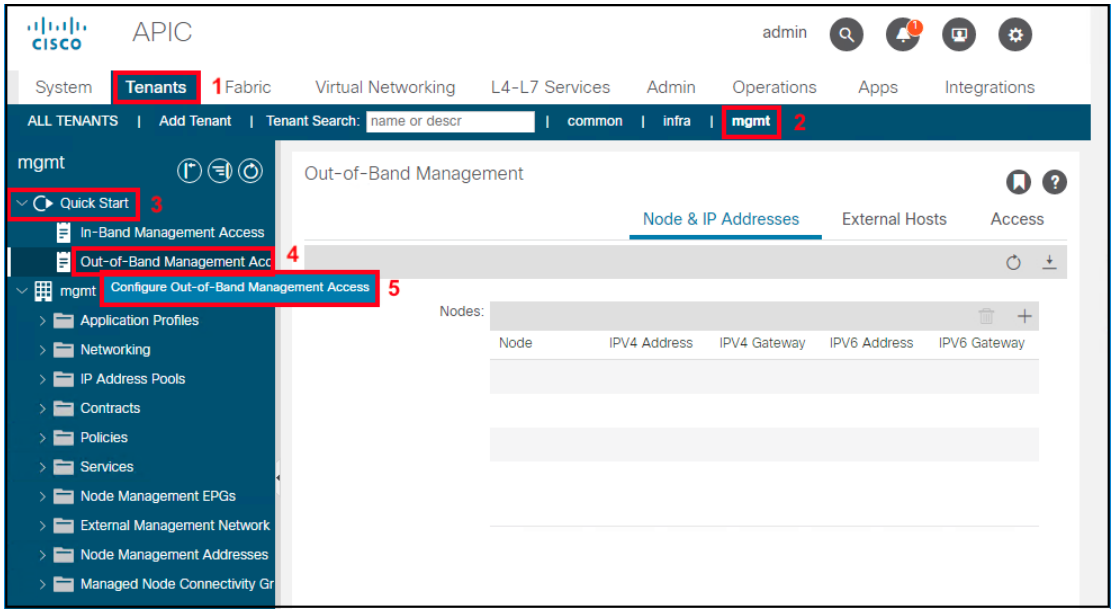
Example of a completed Cluster Configuration

```
Cluster configuration ...
  Enter the fabric name [SDC1Fabric1]:
  Enter the fabric ID (1-128) [1]:
  Enter the number of active controllers in the fabric (1-9) [3]:
  Enter the POD ID (1-12) [1]:
  Is this a standby controller? [NO]:
  Is this an APIC-X? [NO]:
  Enter the controller ID (1-3) [1]:
  Enter the controller name [SDC1-APIC1]:
  Enter address pool for TEP addresses [10.21.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (1-4094) [1999]:
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band_Mgmt Interface? [N]:
  Enter the IPv4 address [10.16.1.11/24]:
  Enter the IPv4 address of the default gateway [10.16.1.1]:
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:
```

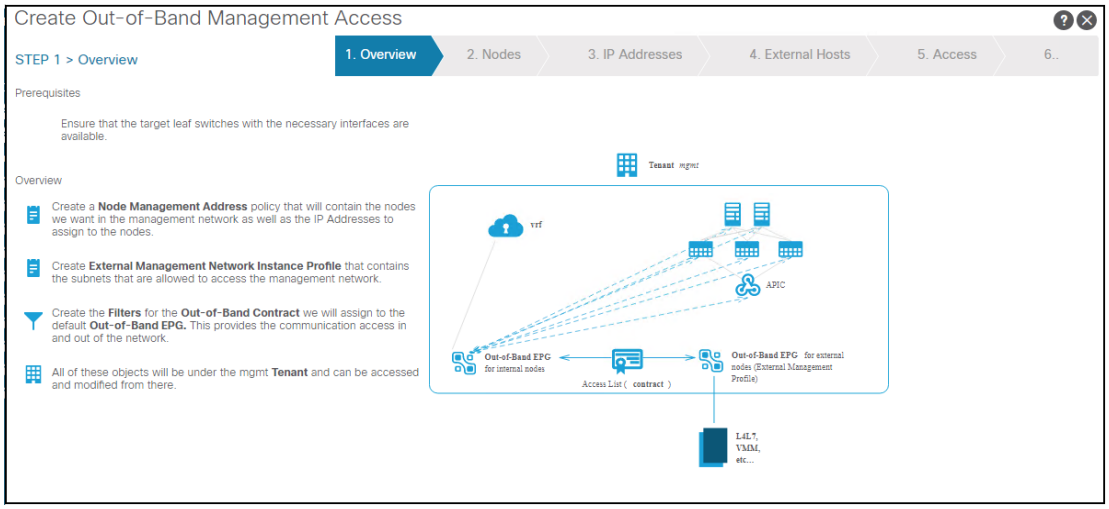
Return to Contents

Step 2: Out-of-Band Management

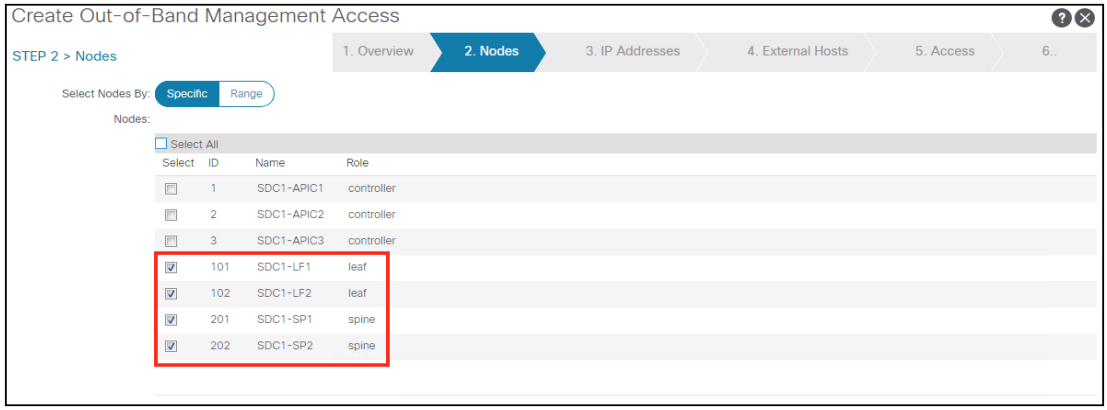
a. The simplest method to configure the Out-of-Band (OOB) Management is to use **Quick Start**. Navigate to **Tenants (1)->mgmt. (2)->Quick Start (3)**, Right click **Out-of-Band Management Access (4)** and Select **Configure Out-of-Band Management Access (5)**.



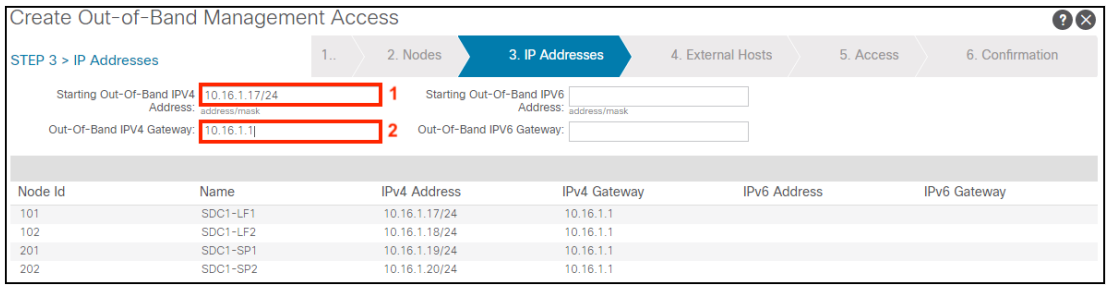
b. Follow the steps to configure the Out-of-Band Management. Click **Start** to begin.



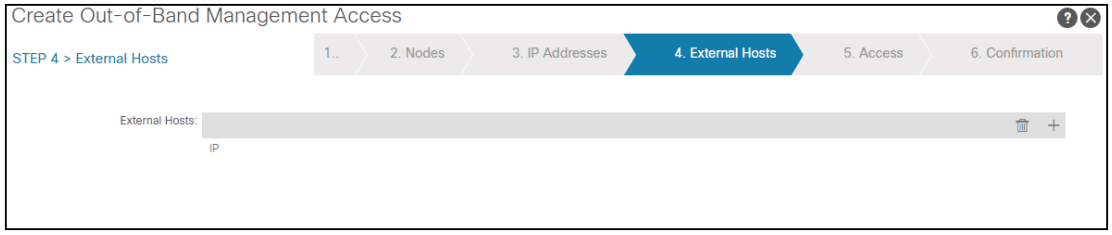
c. Select the switches to assign Management IPs and click **Next.**



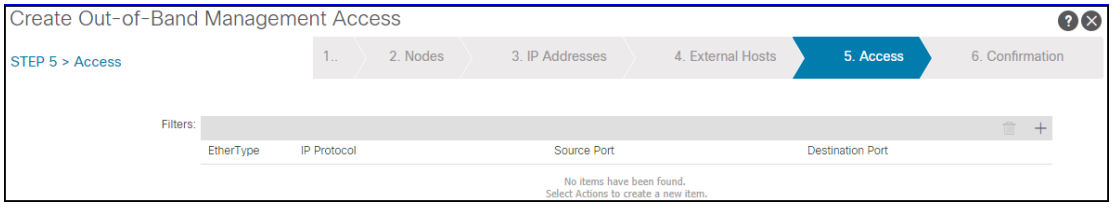
d. Enter the **Starting Out-of-Band IPV4 IP (1)** and **Gateway (2)**. Click **Next**.



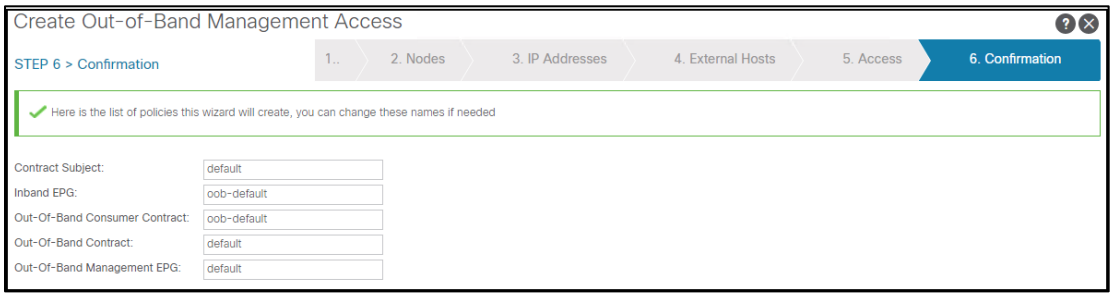
e. Specify the management hosts or subnets. Leave blank to allow all. Click **Next.**



f. Specify the management protocols and ports. Leave blank to allow all. Click **Next.**

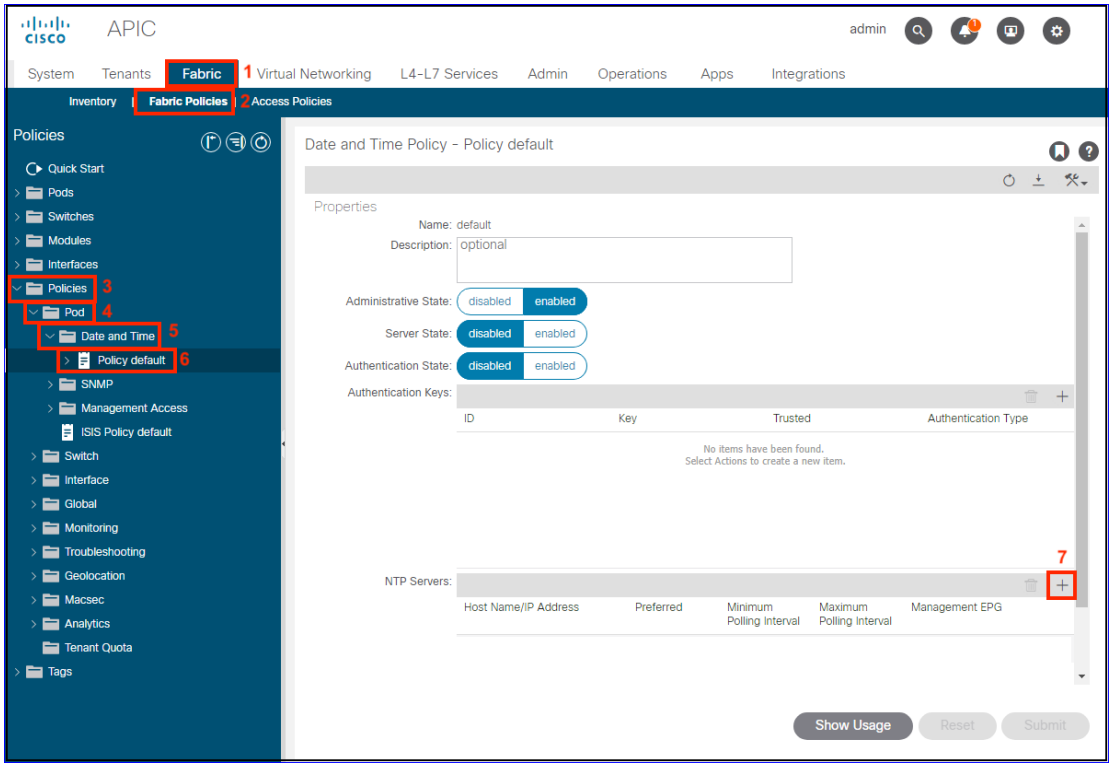


g. Review and click **Finish.**



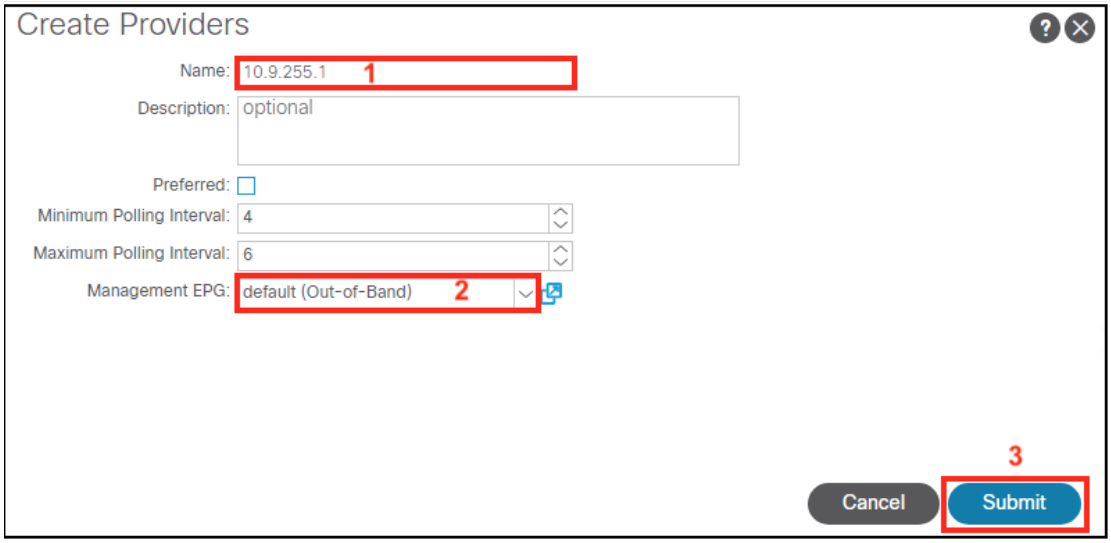
Step 3: Pod Date and Time Policy

a. Navigate to **Fabric (1)->Fabric Policies (2)->Policies (3)->Pod (4)->Date and Time (5)** and select **Policy Default (6)**. In the work pane, click the **+ sign (7)** in the NTP Servers section.

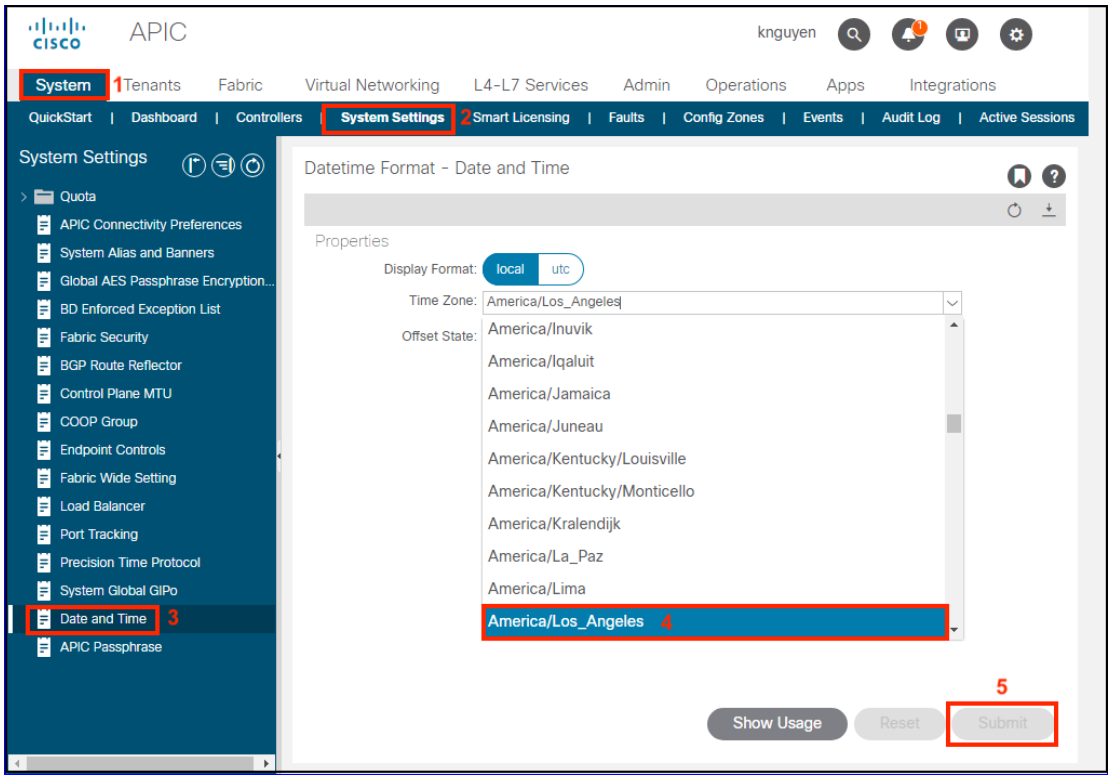


Return to Contents

b. Enter the **IP address (1)** of your NTP server, select default for the **Management EPG (2)** and click **Submit (3)**.

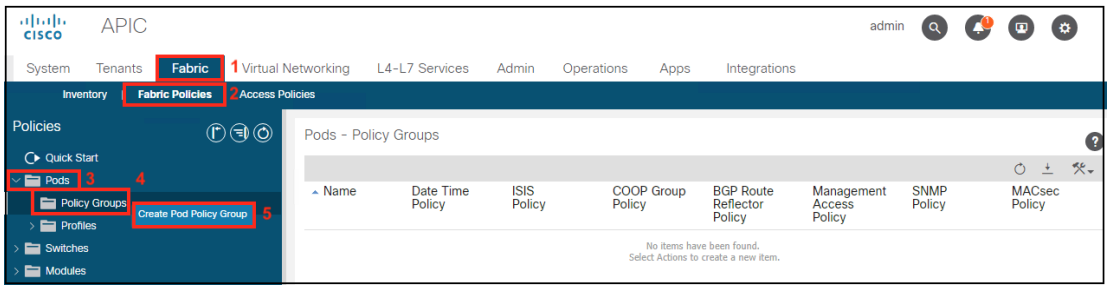


c. Navigate to **System (1)->System Settings (2) and select Date and Time (3)** in the menu pane. In the work pane, select **America/Los_Angeles (4)** as the **Time Zone** and click **Submit (5)**.

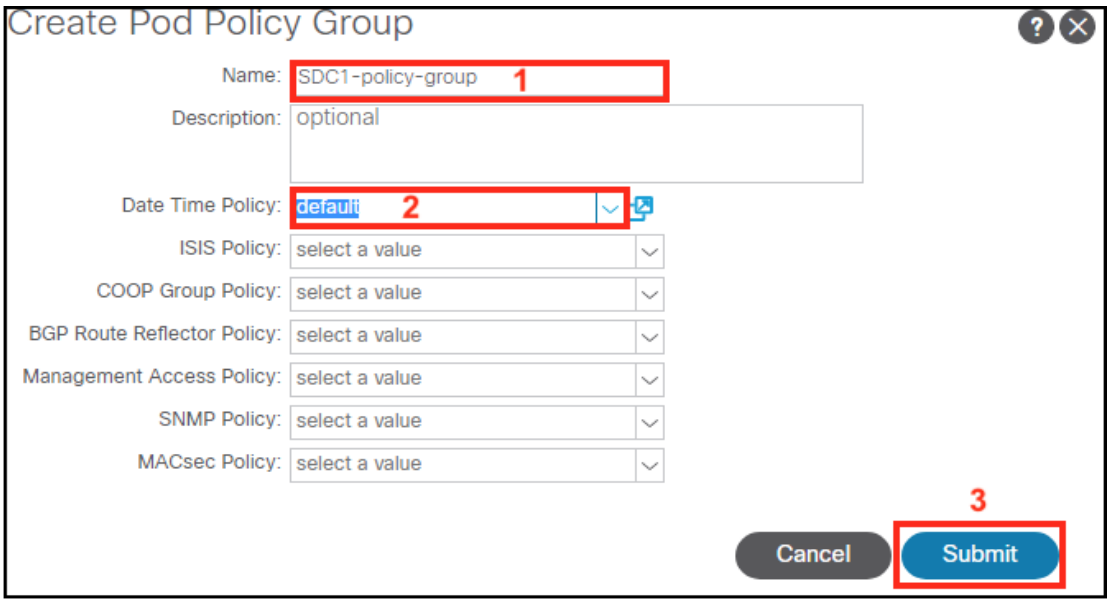


Return to Contents

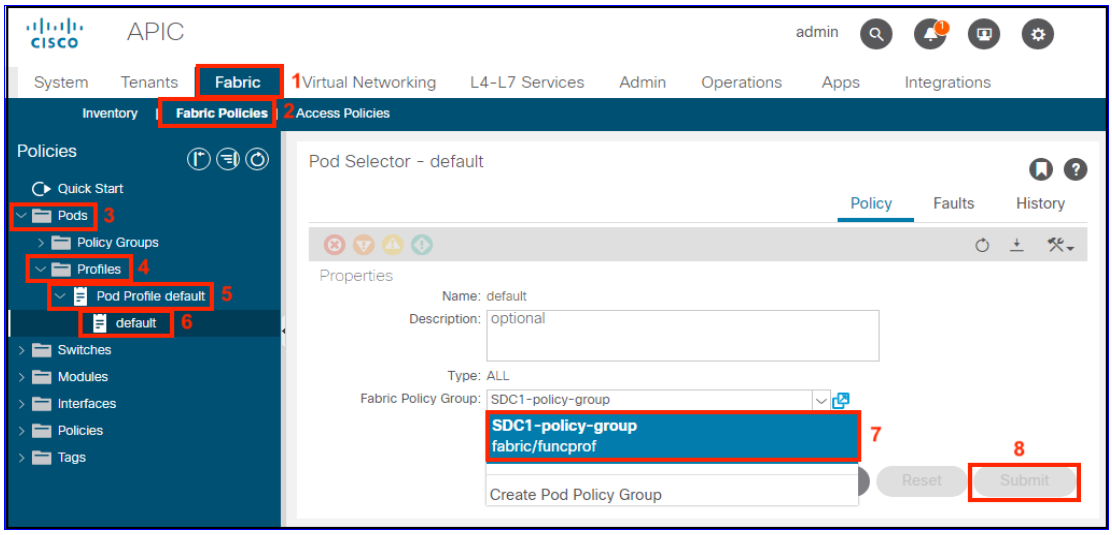
d. Create POD Policy Group. This step is required before setting up the infra tenant in MSO. Navigate to **Fabric (1)->Fabric Policies (2)->Pods (3)->Policy Group (4)**, Right-Click and select **Create Pod Policy Group (5).**



e. Setup the Pod Policy Group. Enter the **Name SDC1-Policy-Group (1)**, select the **default Date Time Policy (2)** and click **Submit (3)**.

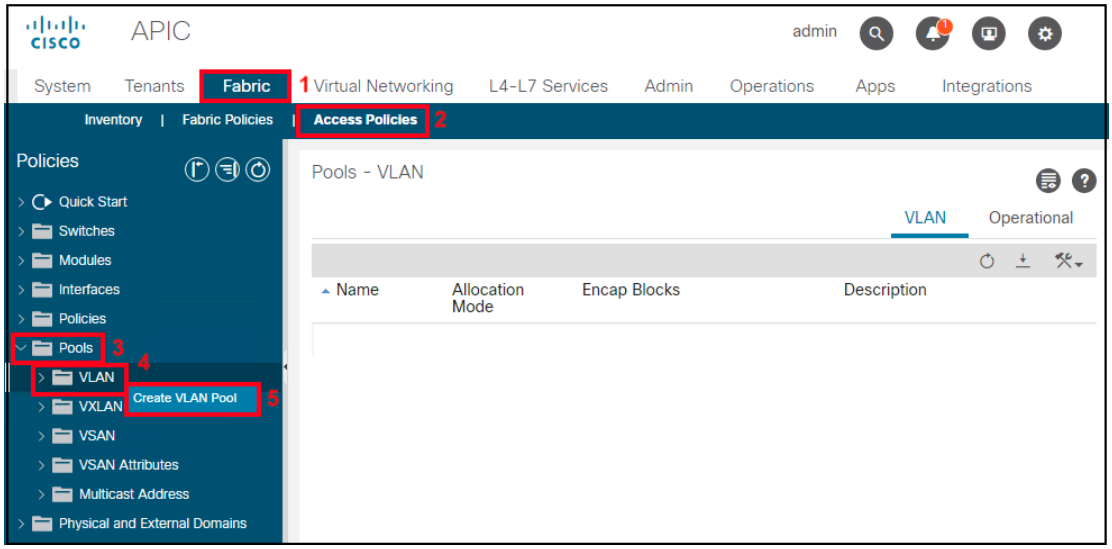


f. Setup the Fabric Policy Group in the default POD Profile Selector. Navigate to **Fabric (1)->Fabric Policies (2)->Pods (3)->Profiles (4)->Pod Profile default (5)->default (6)**. In the work pane, select the **SDC1-policy-group (7)** and click **Submit (8)**.



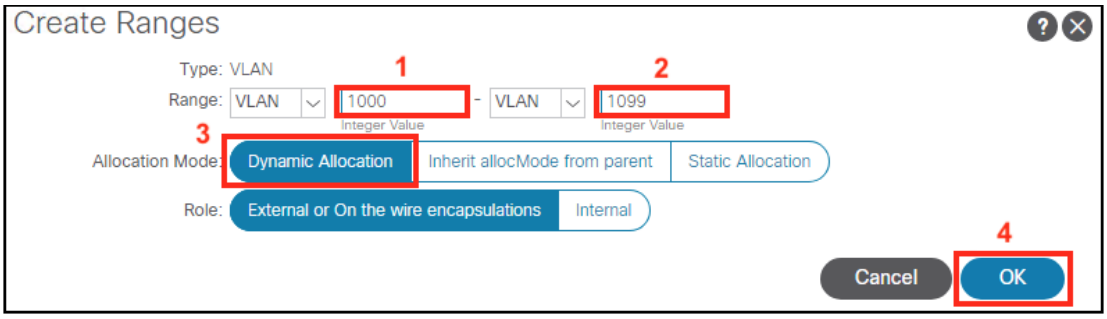
Step 4: VLANs

a. Setup the Dyanamic and Static VLAN pools. Navigate to **Fabric (1)->Access Policies (2)->Pools (3)**. Right click **VLAN (4)** and select **Create VLAN Pool (5)**.

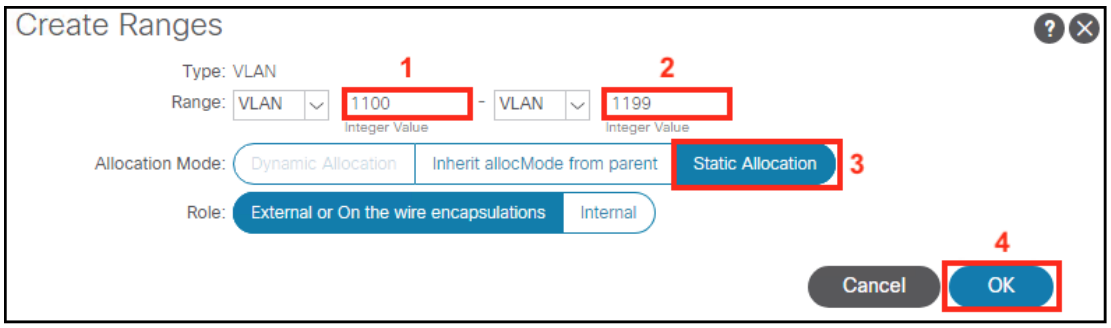


Return to Contents

b. Create the Dynamic VLAN pool. Enter the VLAN range from **1000 (1) to 1099 (2)**, select **Dynamic Allocation (3)**and click **OK (4)**.

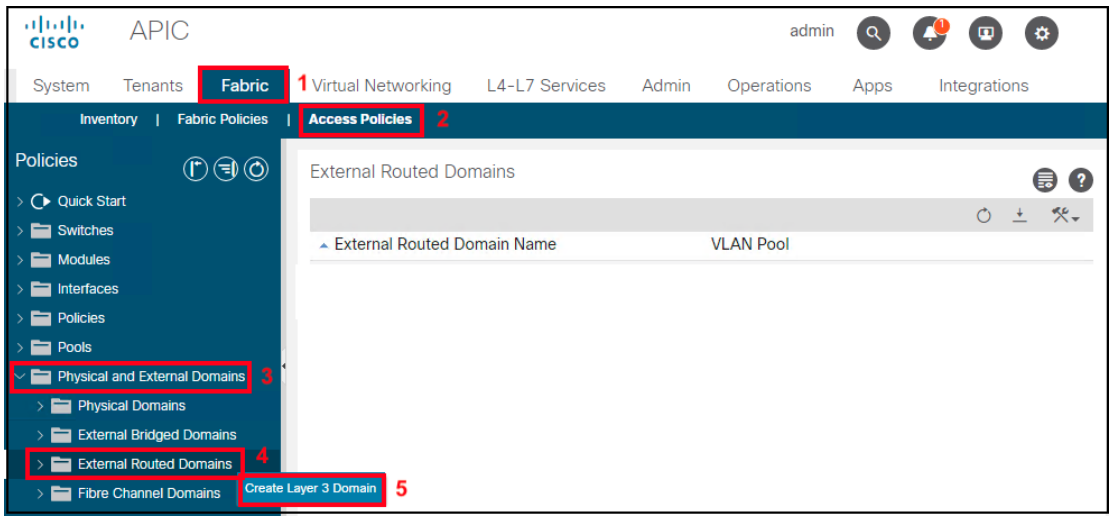


c. Create the Static VLAN pool. Repeat Step a. Enter the VLAN range from **1100 (1) to 1199 (2)**, select **Static Allocation (3)** and click **OK (4).**



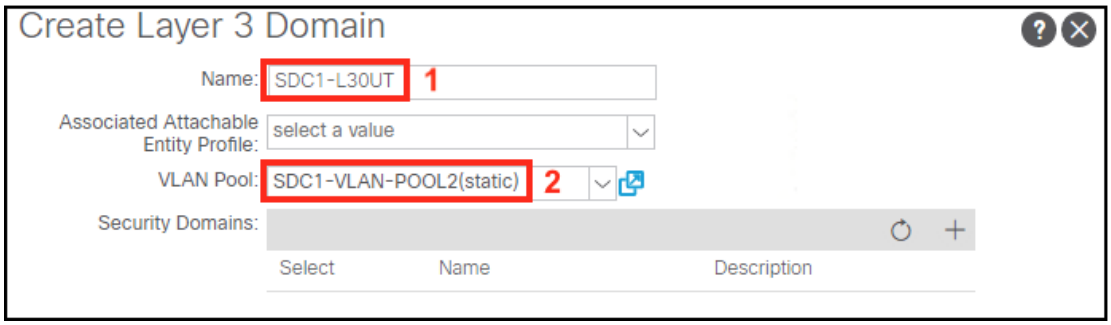
Step 5: Initial L3OUT

a. Create the L3Out External Routed Domain in each data center. Navigate to **Fabric (1)->Access Policies (2)->Physical and External Domains (3)->External Routed Domains (4)**, Right-Click and Select **Create Layer 3 Domain (5)**.

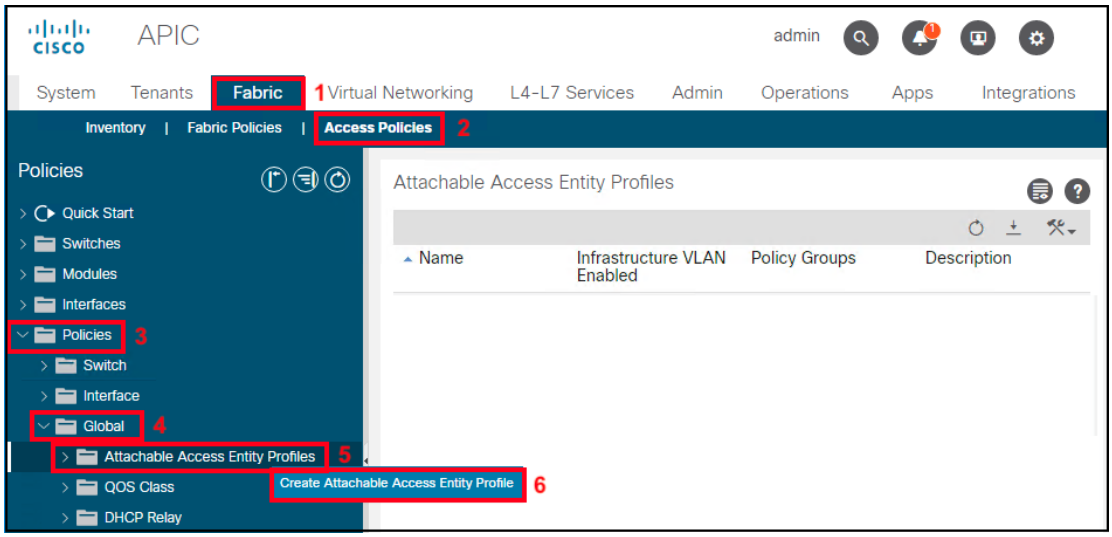


Return to Contents

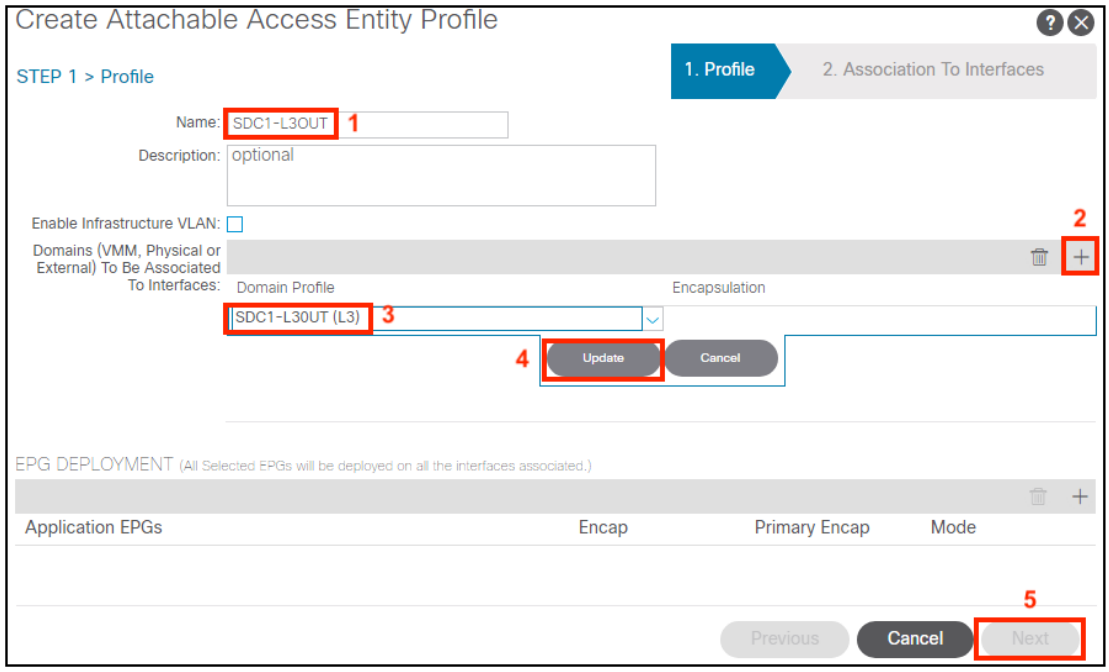
b. Enter the name **SDC1-L3OUT (1)** and select the VLAN Pool **SDC1-VLAN-POOL2(static) (2)** from the drop-down menu



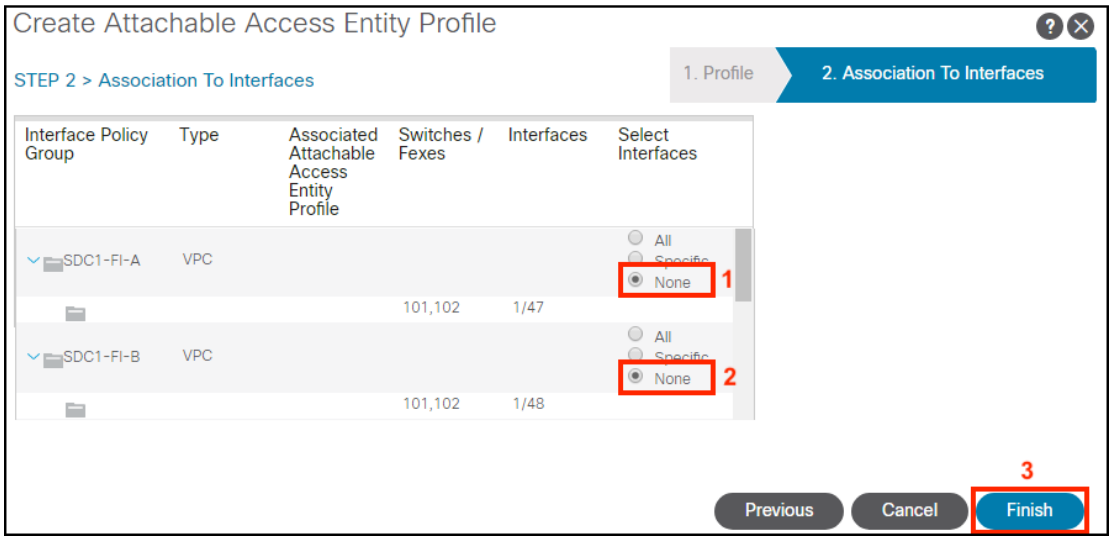
c. Create the Attached Entity Profile for the L3Out. Navigate to **Fabric (1)->Access Policies (2)->Policies (3)->Global (4)->Attachable Access Entity Profiles (5)**, Right-Click and Select **Create Attachable Access Entity Profile (6)**.



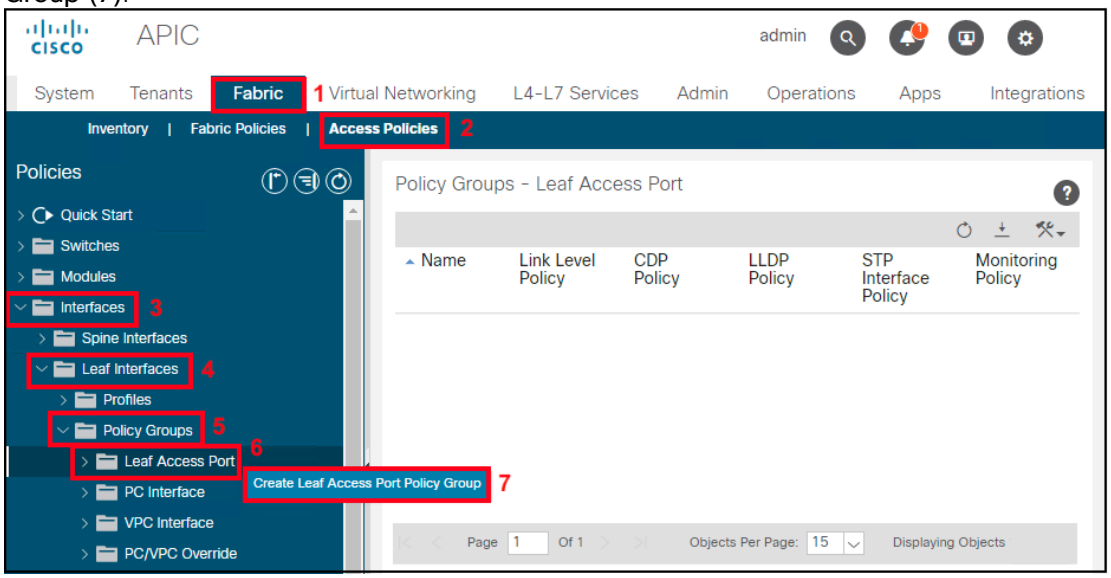
d. Enter the name **SDC1-L3OUT (1)** and click the **+ sign (2)**. Select the **SDC1-L3OUT** profile from the drop-down menu and click **Update (4)**. Select **Next (5)** to continue.



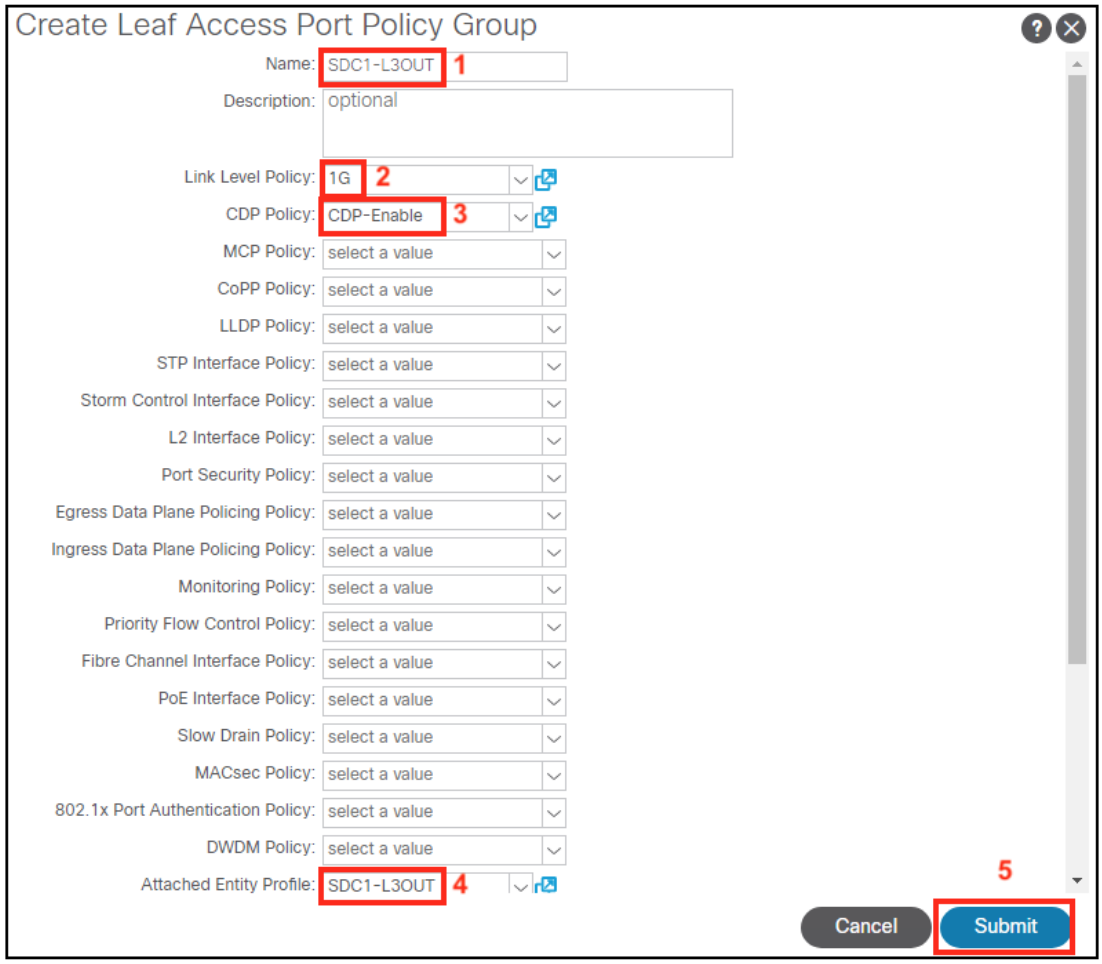
e. Leave Select Interfaces as **None (1 and 2)** and click Finish **(3)**



f. Create the L3Out interface policy group as an individual Leaf Access Port Policy Group. Navigate to **Fabric (1)->Access Policies (2)->Interfaces (3)->Leaf Interfaces (4)->Policy Groups (5)->Leaf Access Port (6)**, Right-Click and Select **Create Leaf Access Port Policy Group (7)**.

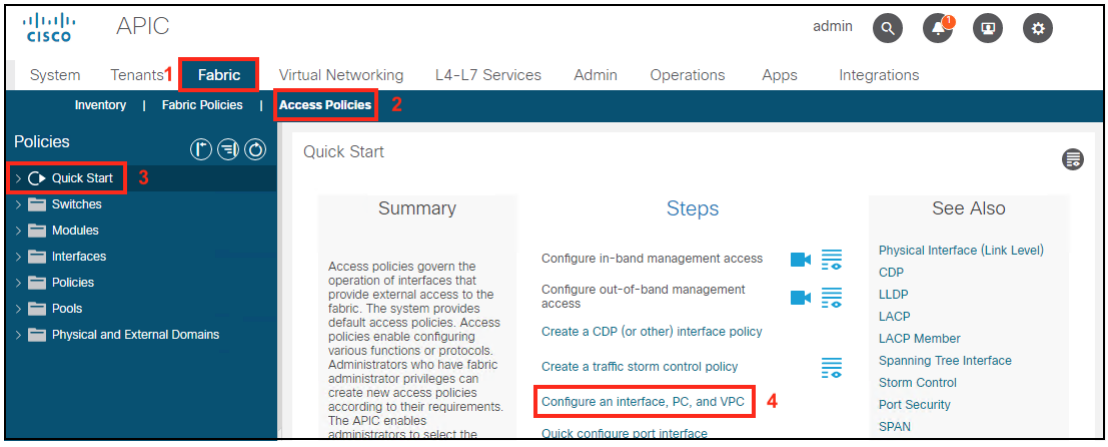


g. Enter the **Policy Group name SDC1-L3OUT (1)**, select a **Link Level Policy 1G (2)**, select the CDP Policy **CDP-Enable (3)**, the **Attached Entity Profile SDC1-L3OUT (4)** and click **Submit**.

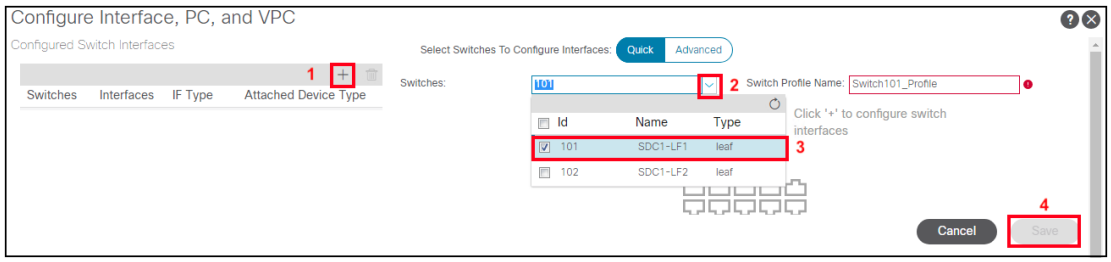


Return to Contents

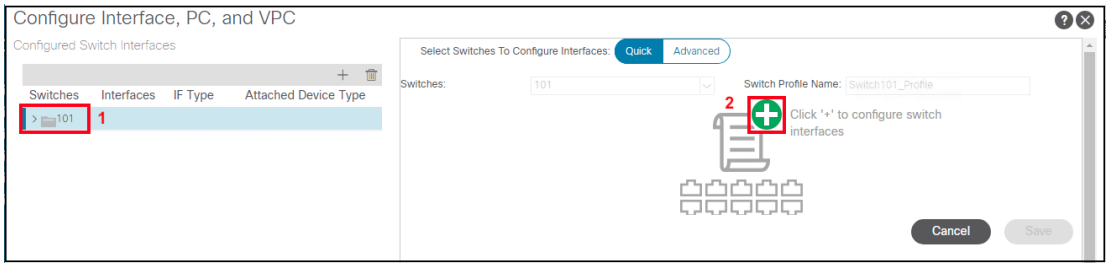
h. Setup switch interfaces for L3Out connection. In APIC, Navigate to **Fabric (1)->Access Policies (2)->Quick Start (3)**. Select **Configure an interface, PC, and VPC (4)** under Steps.



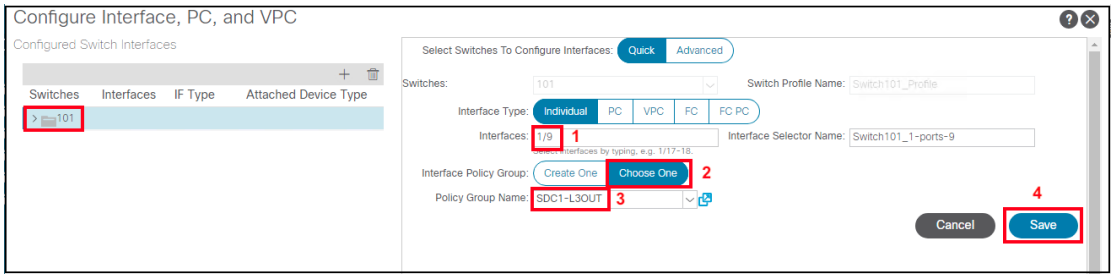
i. Create a switch profile by clicking the **+ sign (1)** under Configured Switch Interfaces. The switch profile configuration wizard will appear on the right. From the **drop-down menu (2)**, select **switch 101 (3)** and click **Save (4)**.



j. Create a port profile by selecting the **switch 101(1)** and click the **+ sign (2)** in the work pane.

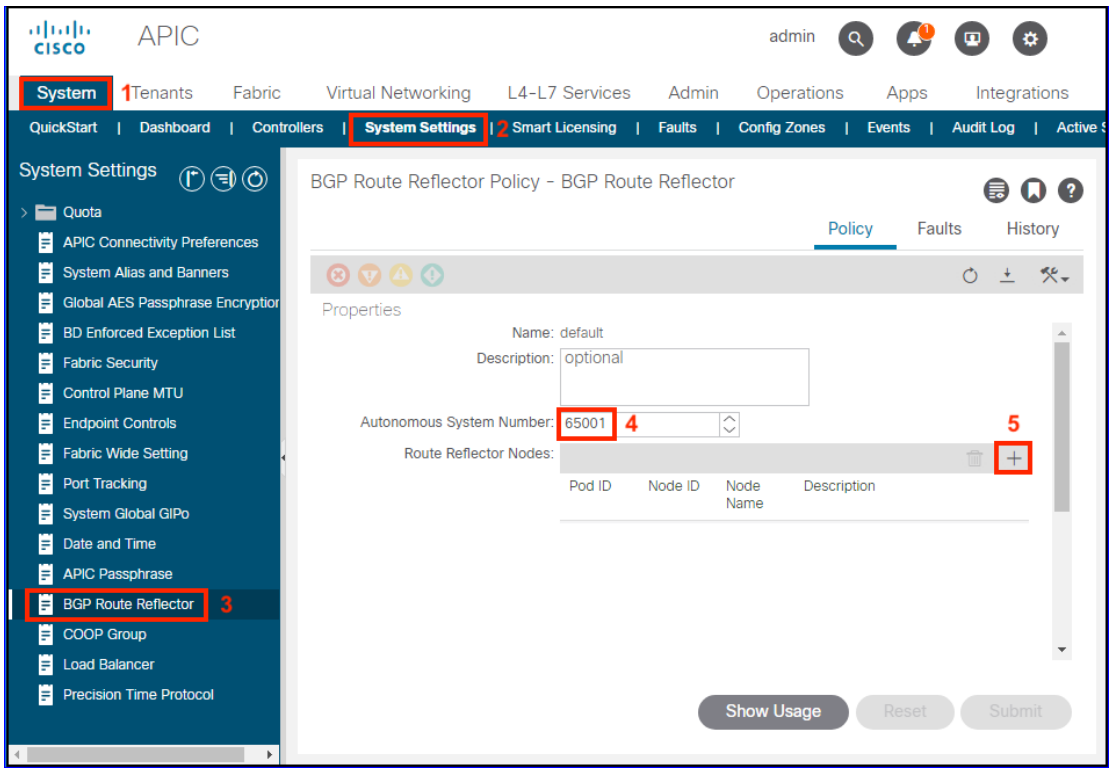


k. To setup the interface, For the Interfaces enter **1/9 (1)**. Select **Choose One (2)** for the Interface Policy Group, from the Policy Group Name drop-down menu select the **SDC1-L3OUT (3)** and click **Save (4)**.

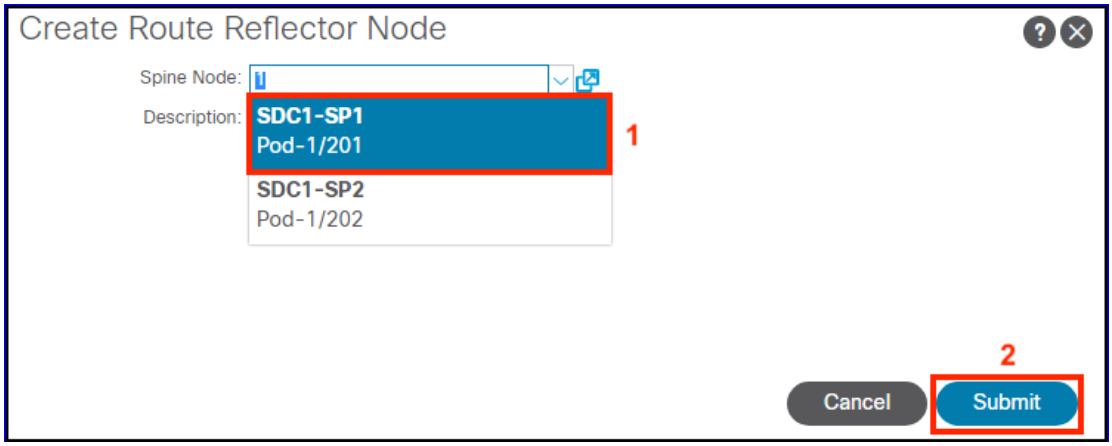


Return to Contents

l. Setup BGP Route Reflectors. Navigate to **System (1)->System Settings (2)->BGP Route Reflector (3)**. Enter the Autonomous System Number **65001 (4)** and click the **+ sign (4)** to add spine switches.

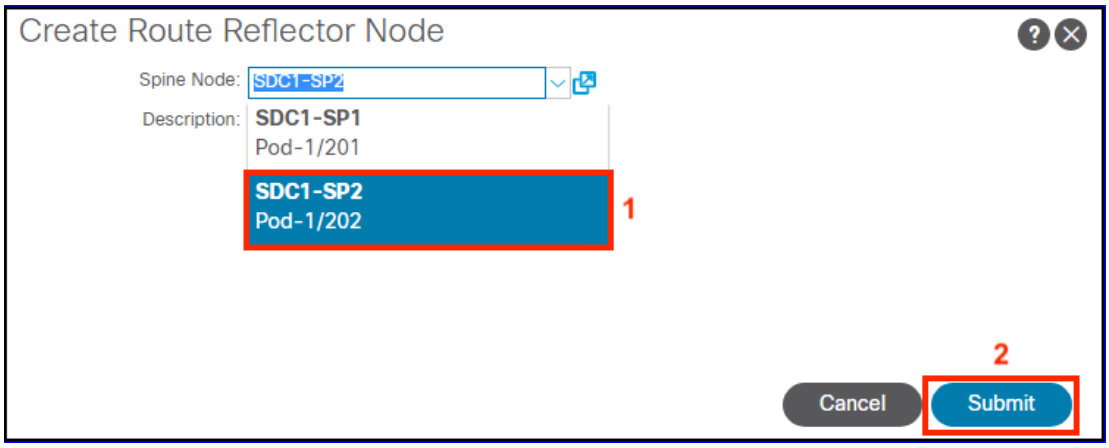


m. From the drop-down menu, select the **first spine SDC1-SP1** and click **Submit**.



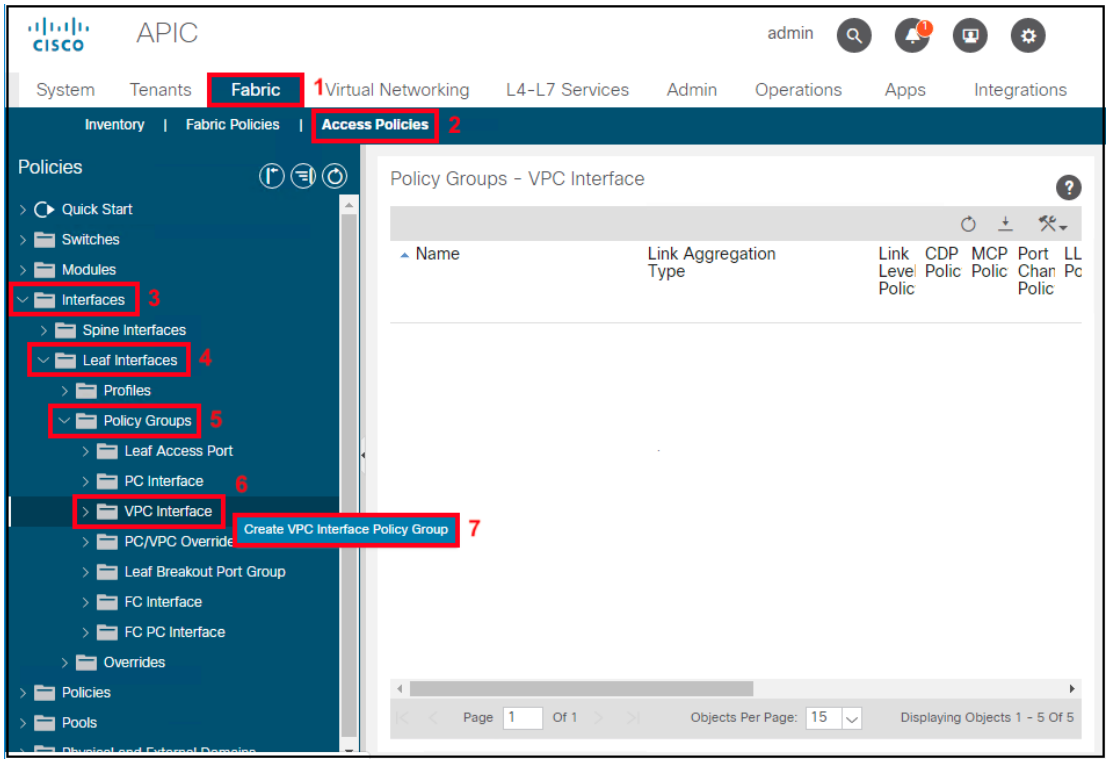
Return to Contents

n. Repeat the steps l and m to add the second spine and click **Submit**.



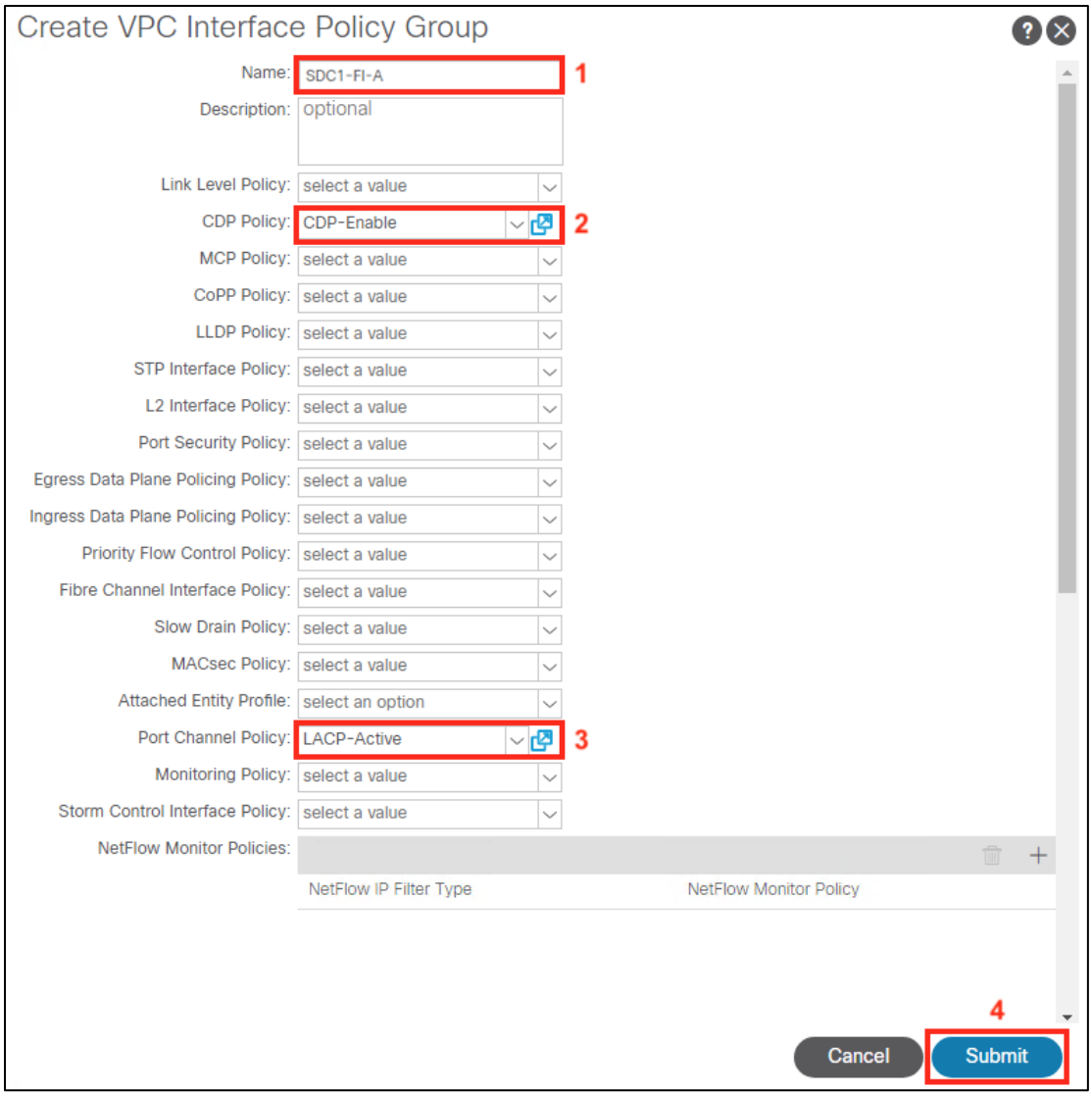
Step 6: ACI Fabric Interconnect Interfaces

a. Create the Fabric Interconnect Virtual Port Channel (VPC) Interface policy group. Navigate to **Fabric (1)->Access Policies (2)->Interfaces (3)->Leaf Interfaces (4)->Policy Groups (5)->VPC Interface (6)**, Right-Click and **Select Create VPC Policy Group (7)**.



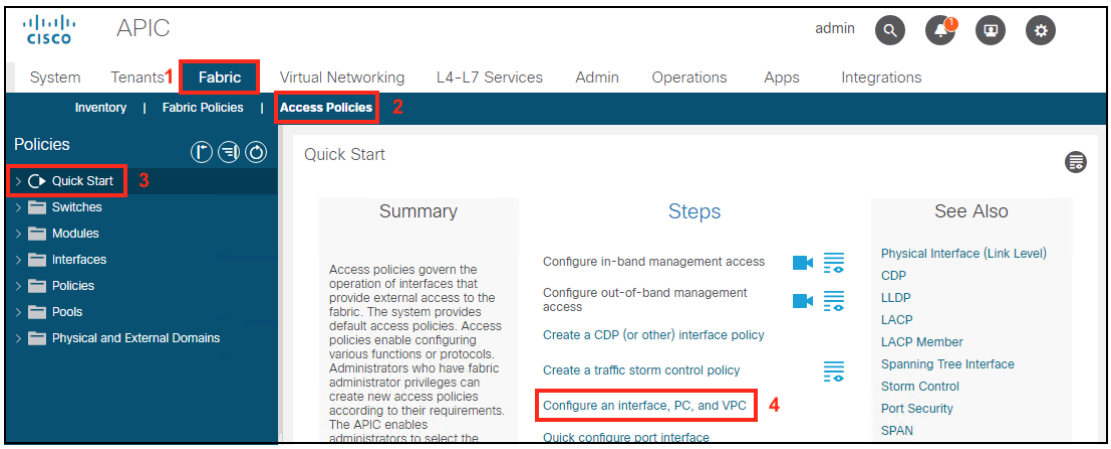
Return to Contents

b. Create the Fabric Interconnect A interface policy group. Set Name as **SDC1-FI-A(1)**, CDP Policy to **CDP-Enable(2)**, Port Channel Policy to **LACP-Active(3)** and click **Submit(4).**

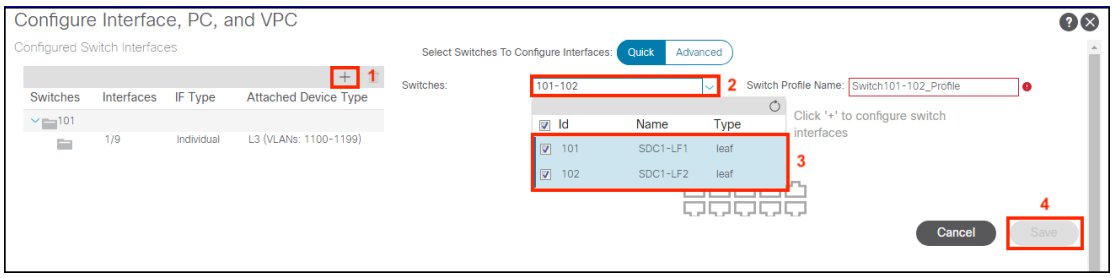


c. Repeat steps a and b to create the VPC Interface Policy Group for SDC1-FI-B.

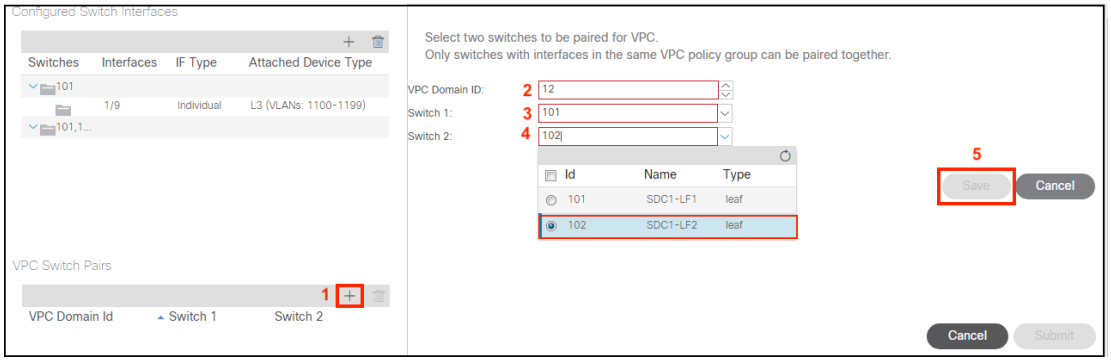
d. Setup switch interfaces for Fabric Interconnects. In APIC, navigate to **Fabric (1)->Access Policies (2)->Quick Start (3)**. In the work pane, select **Configure an Interface, PC, and VPC (4)** under Steps



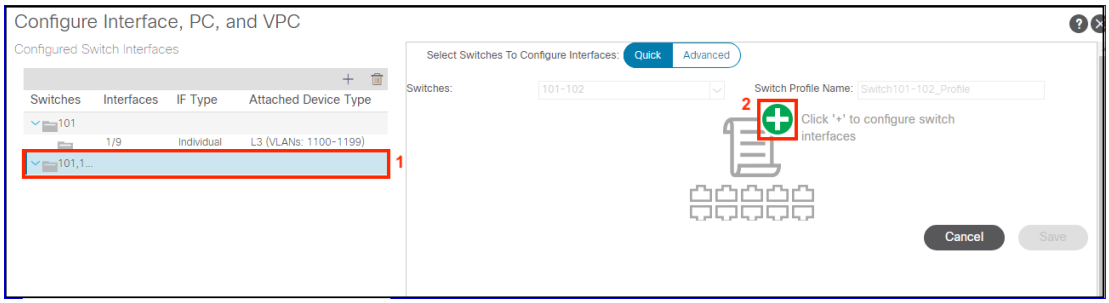
e. To configure a VPC interface to span the two leaf switch ports, create a switch profile for Leaf switches 101 and 102. Click the **+ sign (1)** on the right and in the work pane, for Switches from the **drop-down menu (2)** select **101 and 102 (3)** and click **Save (4)**.



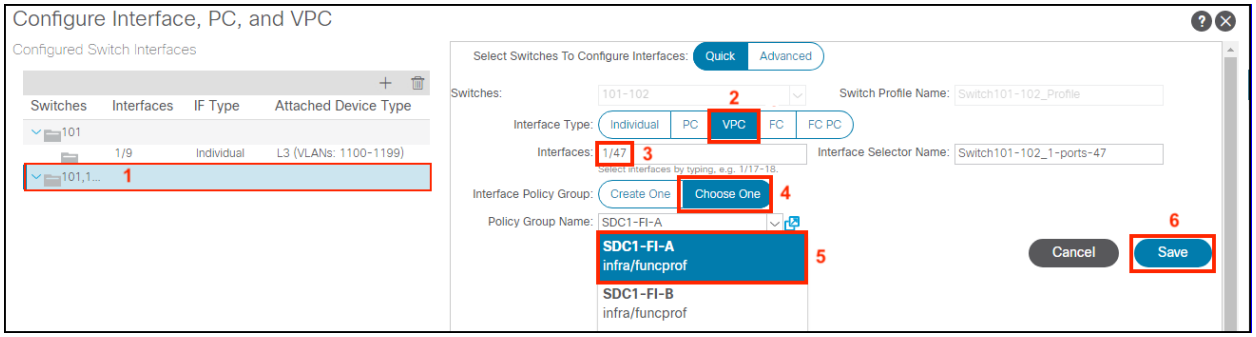
f. Next, create the VPC Domain. Click the **+ sign (1)** in the VPC Switch Pairs section. In the work pane, for the VPC Domain ID enter **12 (2)**. From the **drop-down menu (4)**, select **switch 101 for Switch 1(3)** and **102 for switch 2**, Click **Save (5)**



g. The VPC will connect both leaf switches to Fabric Interconnect A. This will enable redundancy for the fabric. To create the VPC, select the newly created **Switch Profile 101,102 (1)** and in the work pane, click the **+ sign (2)**.

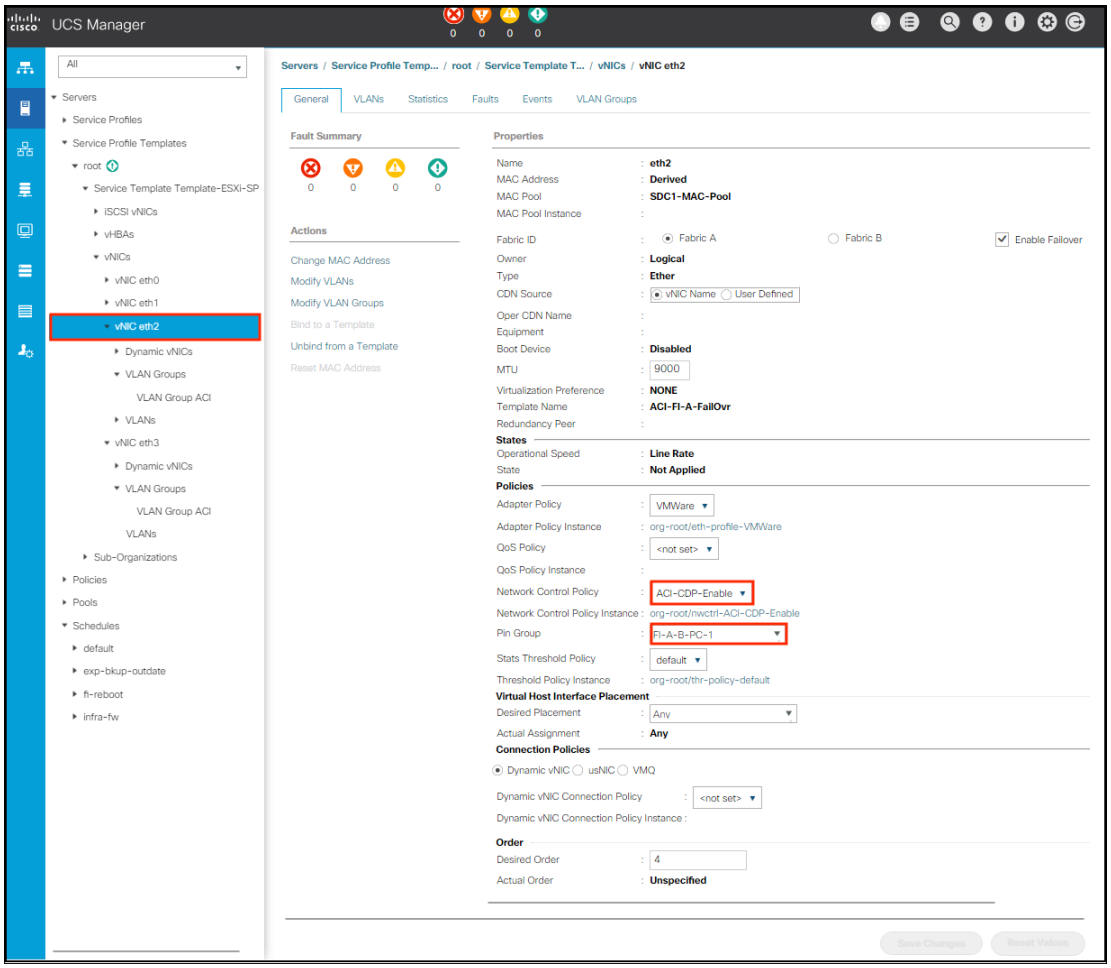


h. In the work pane, select **VPC (1)**, select **VPC (2)**, enter the port **1/47 (3)**, select **Choose One (4)** for the Interface Policy Group, select the Policy Group Name **SDC1-FI-A (5)** and click **Save (6).**



i. Repeat steps e and f to create the VPC for SDC1-FI-B Fabric Interconnect. Choose port 1/48 and Policy Group SDC1-FI-B.

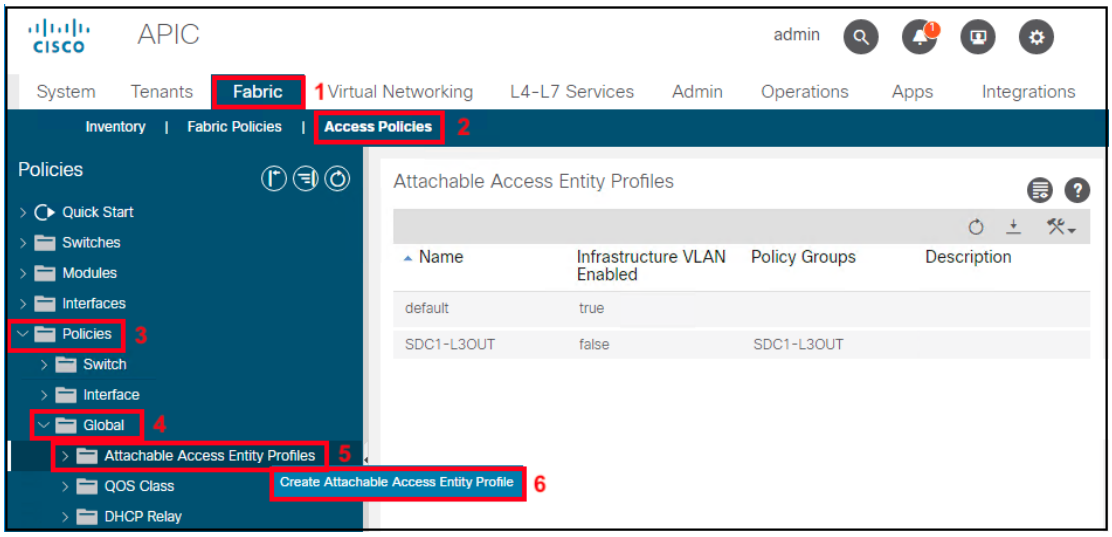
j. In UCS Manager, the Fabric Interconnects need to be configured to enable CDP and set the Pin Group in the Service Template for the vNICs. Refer to references at the beginning of Appendix C for details.



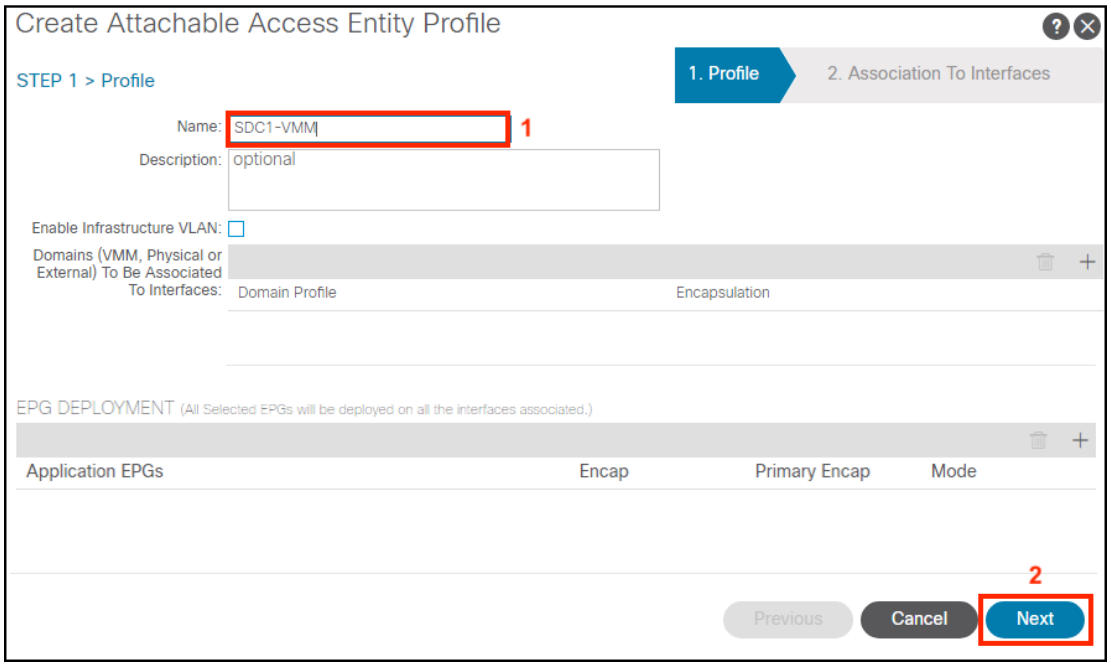
Return to Contents

Step 7: VMM Domain

a. Create the Attachable Access Entity Profile for the Fabric Interconnects in each data center. Navigate to **Fabric(1)->Access Policies (2)->Policies (3)->Global (4)-> Attachable Access Entity Profiles (5)**, Right-Click and Select **Create Attachable Access Entity Profile (6)**.

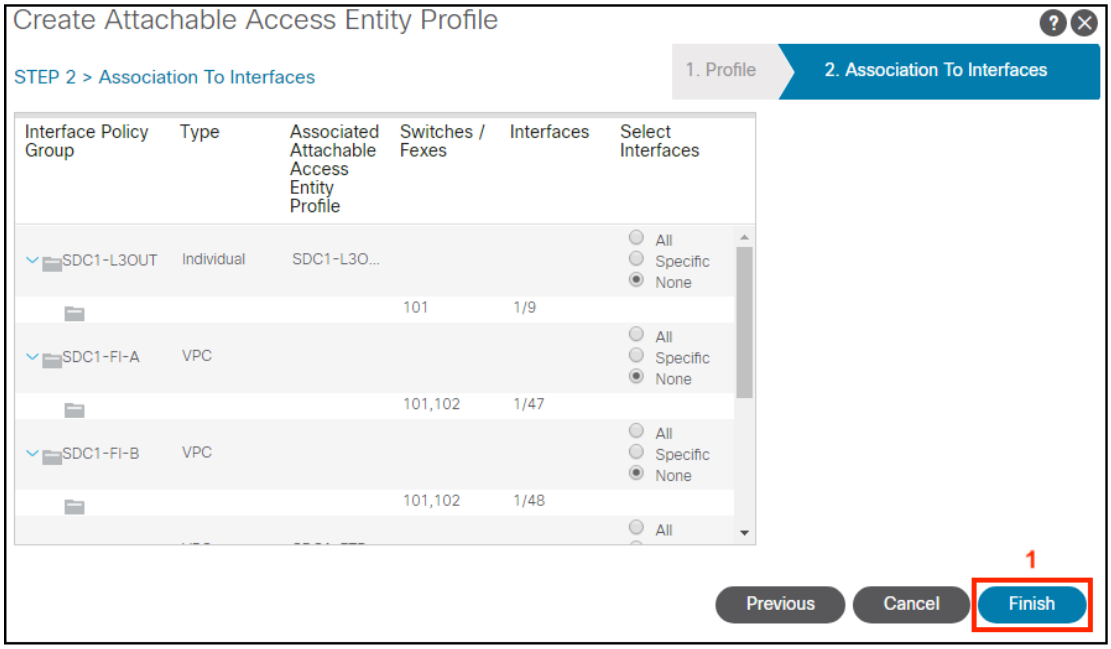


b. Enter the Name **SDC1-VMM (1)** and Click **Next (2)**.



Return to Contents

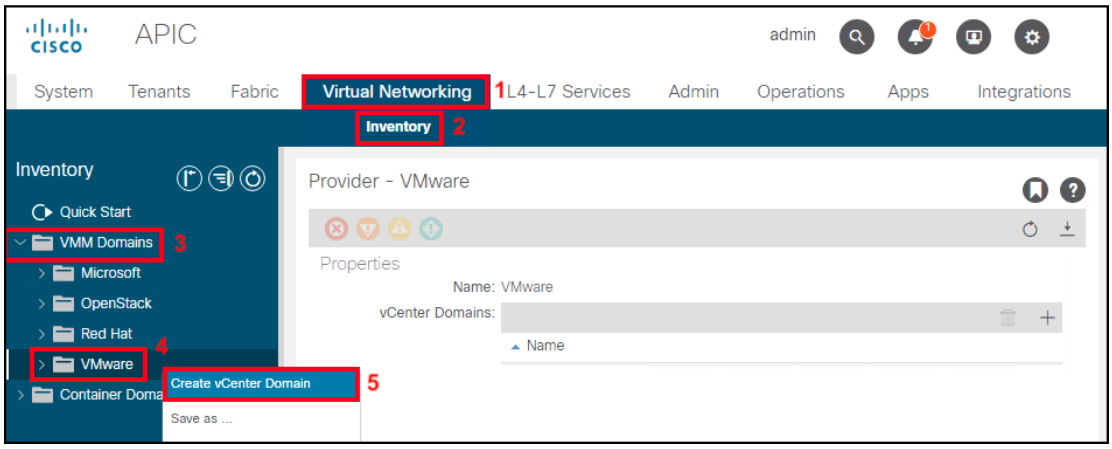
c. Leave the Selected Interfaces as None and click **Finish (1)**.



Setup VMware vSphere Distributed Switch (VDS). We are testing the VMware vCenter which is the most popular Virtual Machine Manager (VMM) currently deployed. We are using a single vCenter VM that is hosted in DC2 for managing the virtualized environment in DC1 and DC2. APIC will call the vCenter API to manage the networking settings for the VDS. We used the Cisco ACI Virtualization Guide 4.1, Chapter Cisco ACI with VMWare VDS Integration as our guide for setting up a VMM Domain with the APIC GUI.

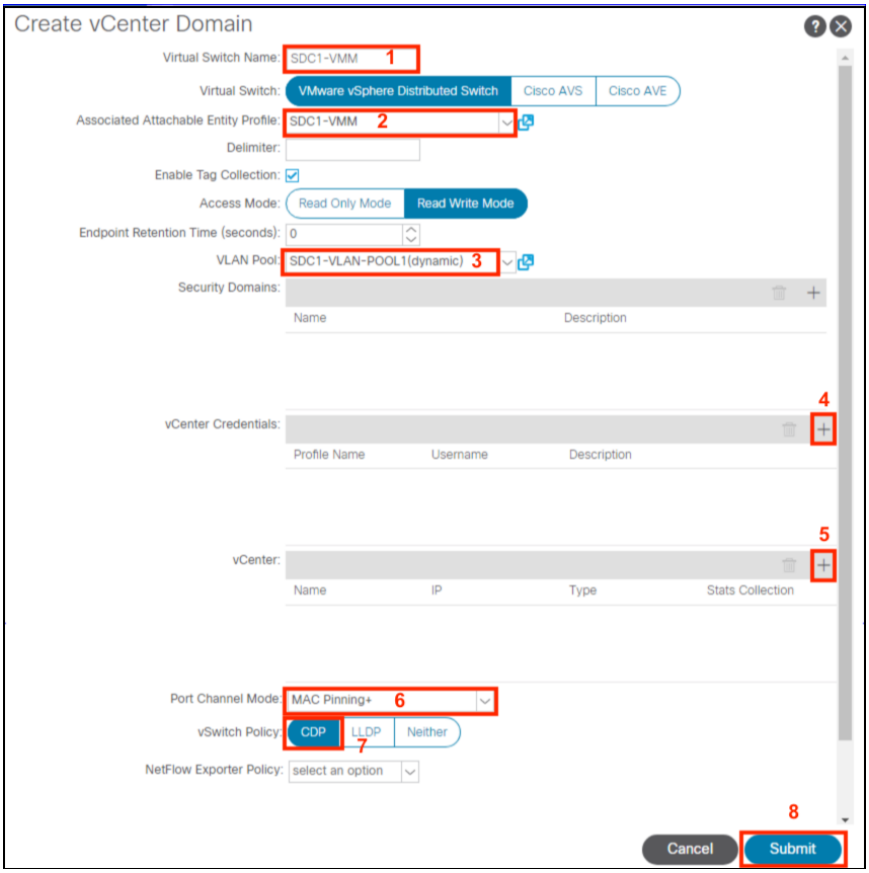
Optional: It is recommended that you create a specific account for ACI on the vCenter so that activity can be easily identified in the vCenter logs. We created an account named aciadmin1 prior to starting this step. Refer to Test Case 3, Step 2 for instructions.

d. Create vCenter Domain using the APIC GUI. Navigate to **Virtual Networking (1)-> Inventory (2)->VMM Domains (3)->VMware (4)**, Right-Click to select **Create vCenter Domain (5)**.

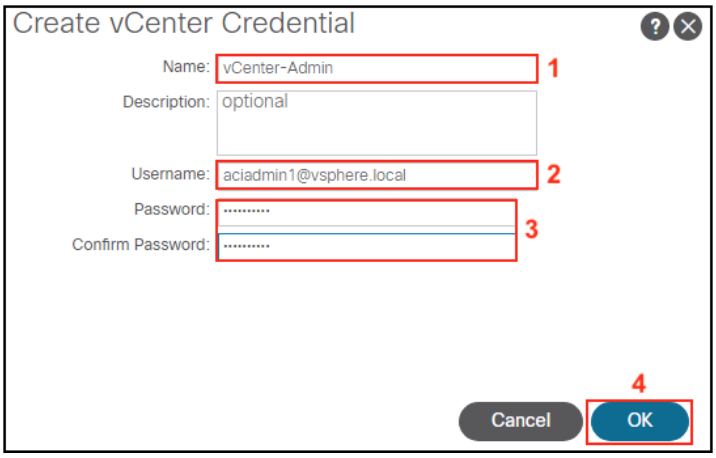


Return to Contents

e. Enter the Virtual Switch Name **SDC1-VMM (1)**, select AEP profile **SDC1-VMM (2)** from the drop-down menu, select VLAN Pool **SDC1-VLAN-Pool1(dynamic) (3)** drop-down menu. Click the **+ sign (4)** to create the vCenter Credential (see step f. for details). Click the **+ sign (5)** to create the vCenter (see step g. for details). Select Port Channel Mode **Mac-Pinning+ (6)** and vSwitch policy **CDP (7)** and click **Submit (8)**.

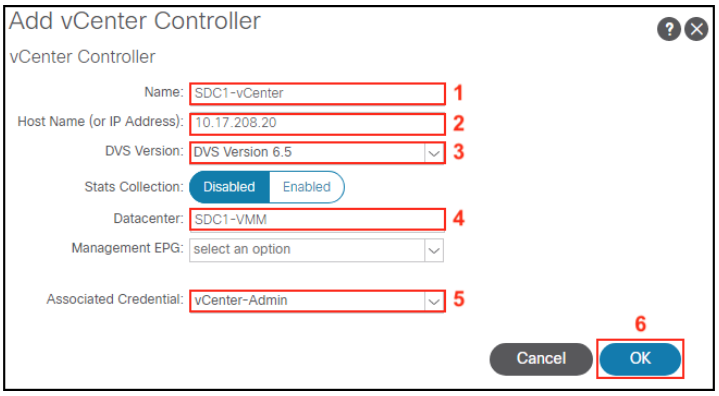


f. Enter the Name **vCenter-Admin (1)**, the username **aciadmin1@vsphere.local (2)**, enter the **password (3)** and click **OK (4)**.



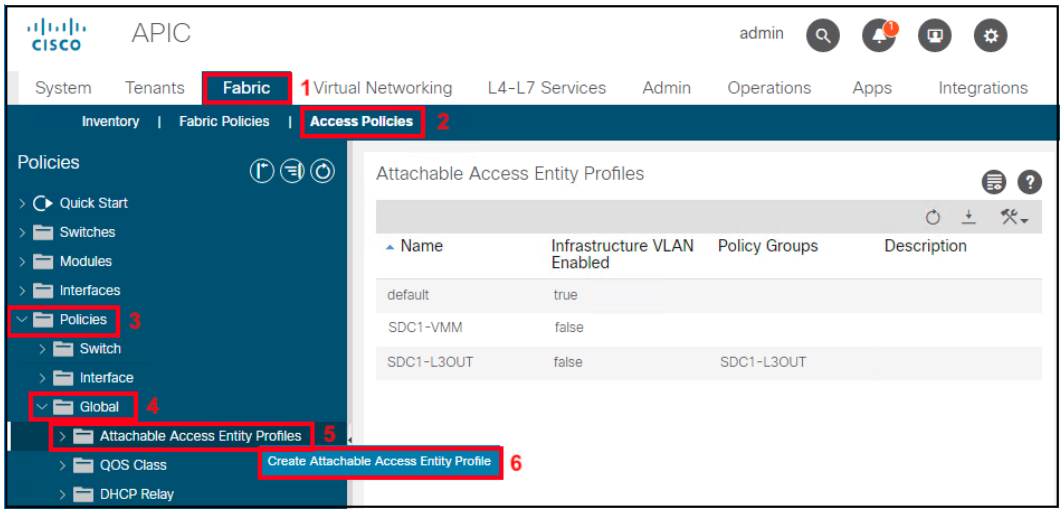
Return to Contents

g. Enter the name **SDC1-vCenter(1)** and **IP Address(2)**. Select your **DVS version(3)** from the drop-down menu. Enter the Datacenter name **SDC1-VMM(4)**, associate it with the credential **vCenter-Admin(5)** and click **OK(6).**

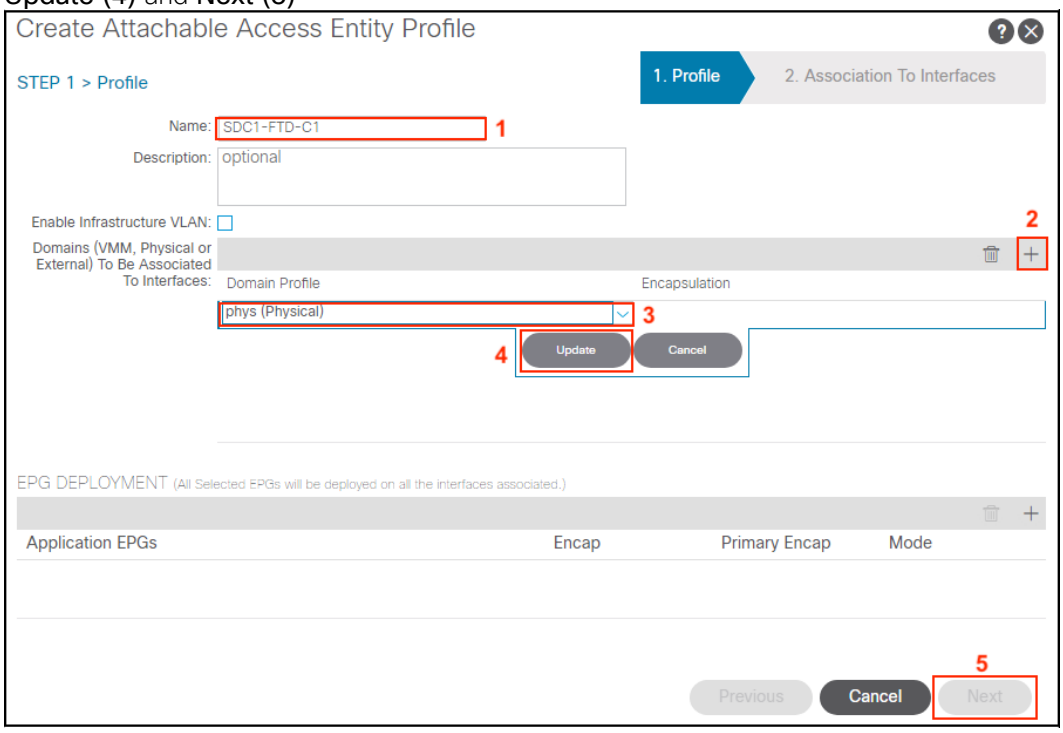


Step 8: FTD Cluster Control Link (CCL) and Data Interfaces

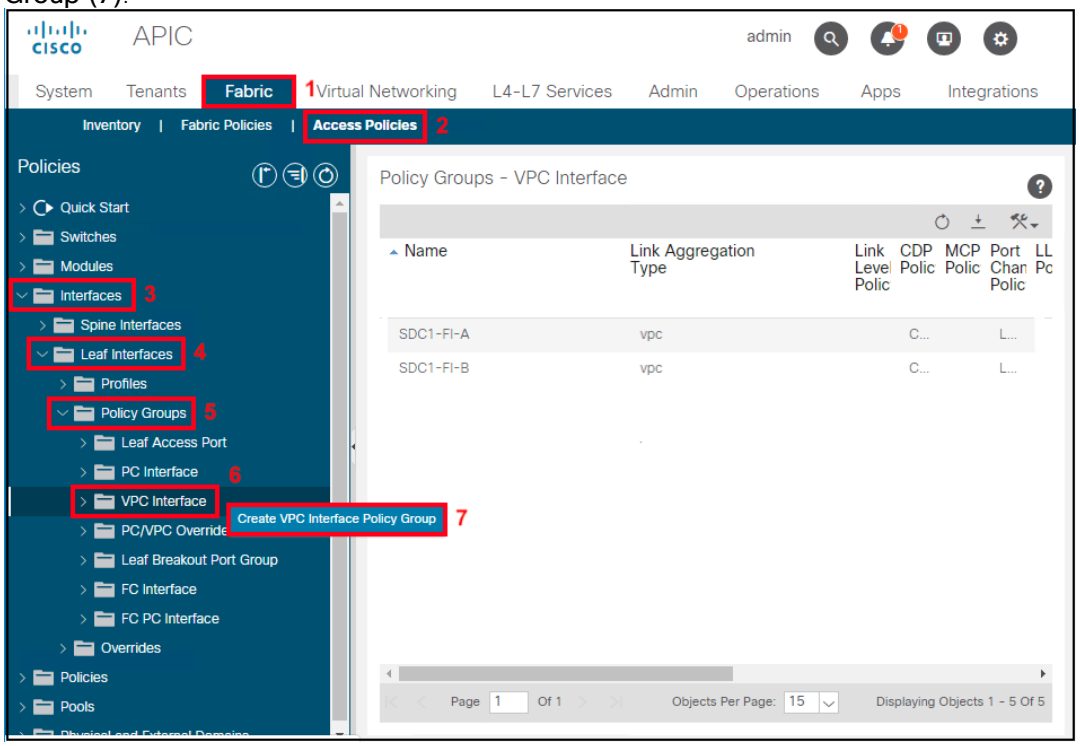
a. Create the Attachable Access Entity Profile for the FTD clusters in each data center. Navigate to **Fabric (1)->Access Policies (2)->Policies (3)->Global (4)->Attachable Access Entity Profiles (5), Right-Click and Select Create Attachable Access Entity Profile**



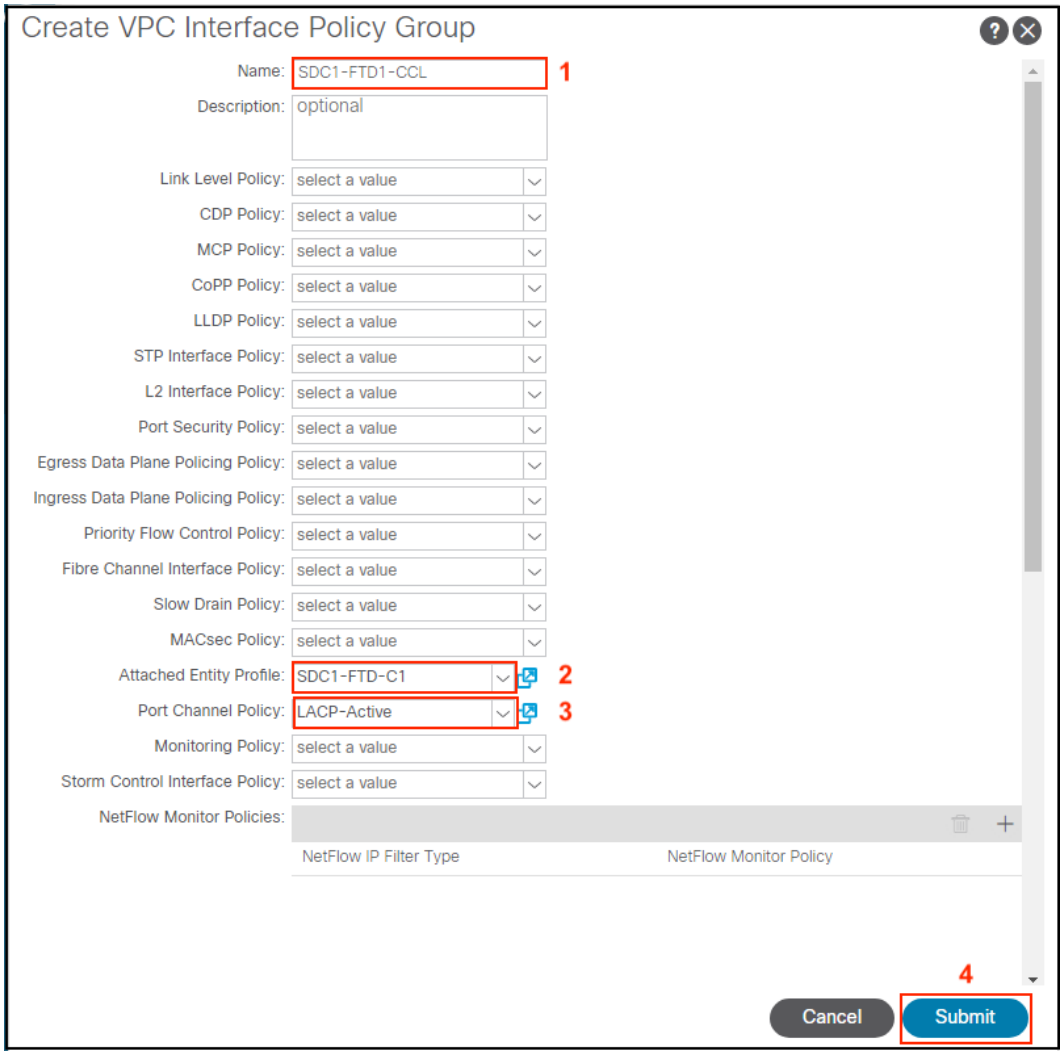
b. Enter the Name **SDC1-FTD-C1 (1)**, click the **+ sign (2)** to add the Domain **Phys (3)**. Click **Update (4)** and **Next (5)**



c. Create the FTD Cluster Control Link (CCL) interface policy group for SDC1-FTD1-CCL. Navigate to **Fabric (1)->Access Policies (2)-> Interfaces (3)->Leaf Interfaces (4)->Policy Groups (5)->VPC Interfaces (6)**, and Right-Click and Select **Create VPC Interface Policy Group (7)**.



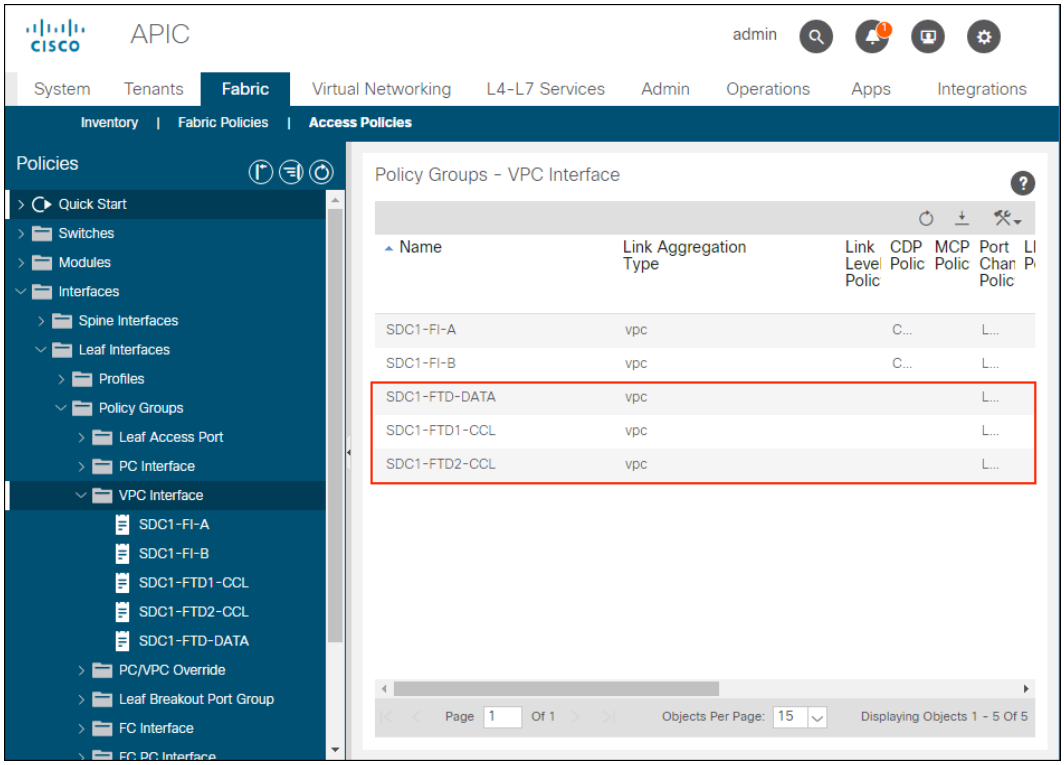
d. Enter the Name **SDC1-FTD1-CCL (1)**, select the Attached Entity Profile **SDC1-FTD-C1 (2)**, Port Channel Policy is **LACP-Active (3)** and click **Submit (4).**



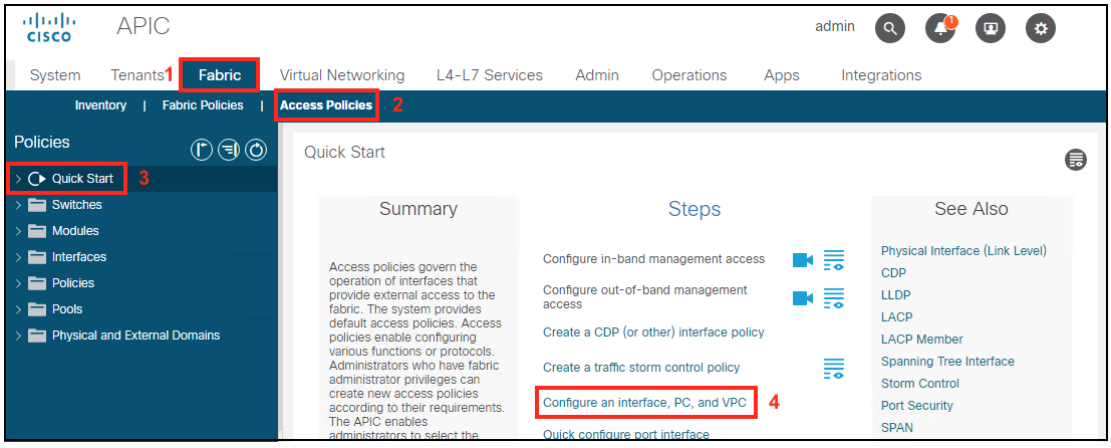
Return to Contents

e. Repeat steps c. and d. to create the VPC Interface Policy Groups for **SDC1-FTD2-CCL** and for **SDC1-FTD-DATA**. The name is unique to each policy but AEP and Port Channel Policy are the same.

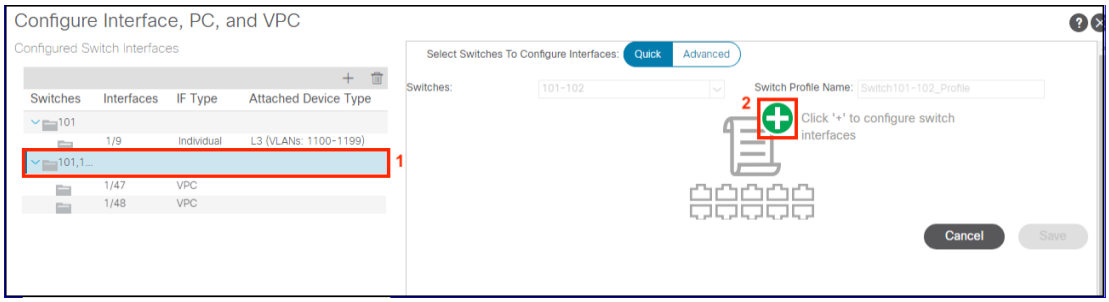
When completed, the newly configured interfaces are displayed in Policy Groups – VPC Interface summary.



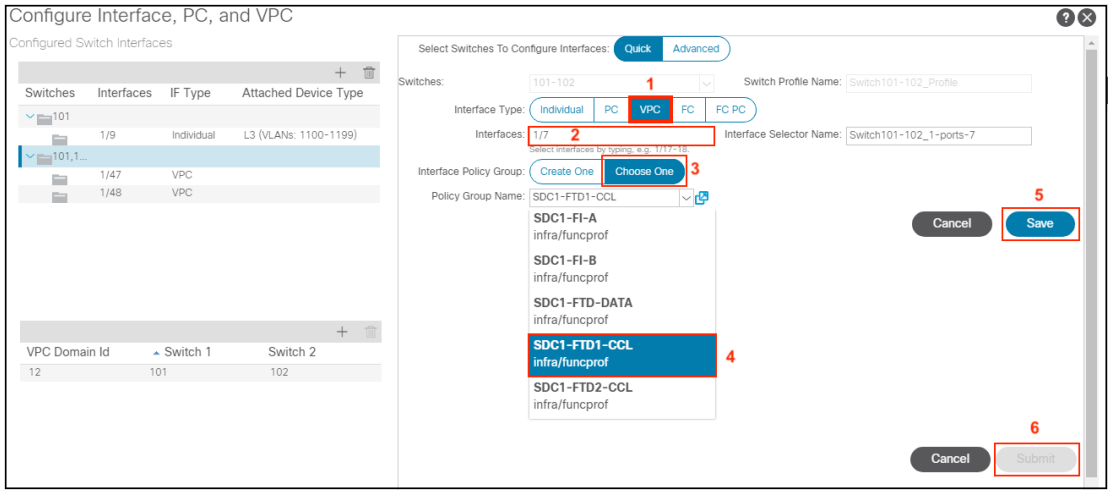
f. Setup switch interfaces for L3Out connection. In APIC, Navigate to **Fabric (1)->Access Policies (2)->Quick Start (3)**. Select **Configure an interface, PC, and VPC (4)** under Steps.



g. To create the VPC, select the newly created **Switch Profile 101,102 (1)** and in the work pane, click the **+ sign (2)**.

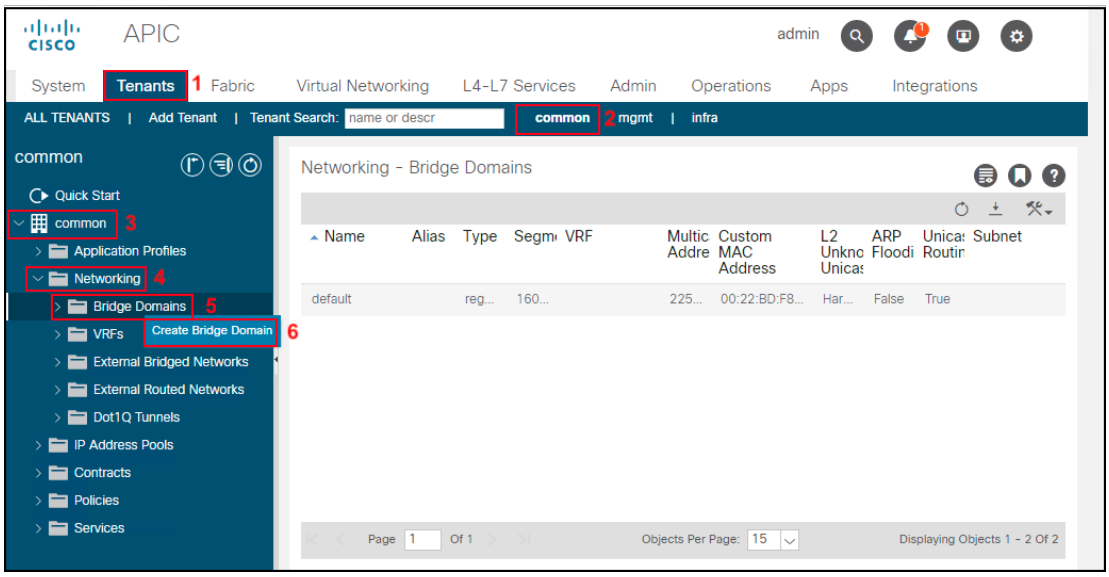


h. Select **Interface Type VPC (1)** and enter **Interface 1/7 (2)**. Click **Choose One (3)** for the Interface Policy Group and select the **Policy Group Name SDC1-FTD1-CCL (4)** from the drop-down menu. Click **Save (5)** and **Submit (6)**

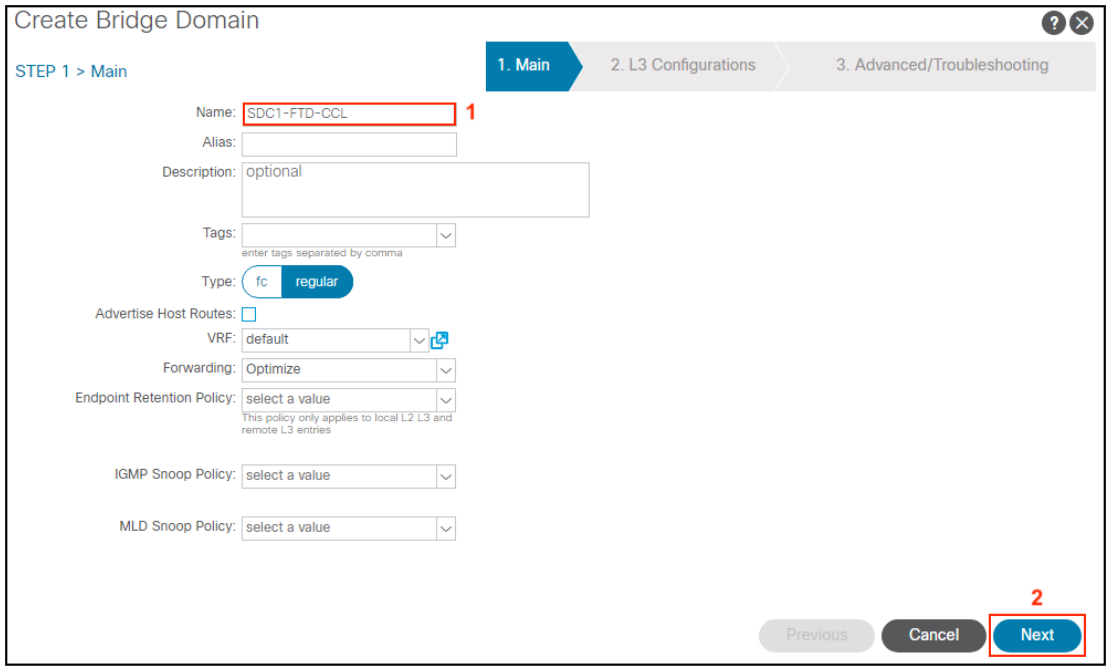


i. Repeat steps g and h to create the VPCs for **SDC1-FTD2-CCL (port 1/8)** and **SDC1-FTD-DATA (port 1/4-5)** and select the corresponding Policy Group.

j. Create a Bridge Domain to permit communication between the FTDs over the CCL interfaces. Navigate to **Tenants (1)->Common (2)->Common (3)->Networking (4)->Bridge Domains (5)**->right click and select **Create Bridge Domain (6)**.

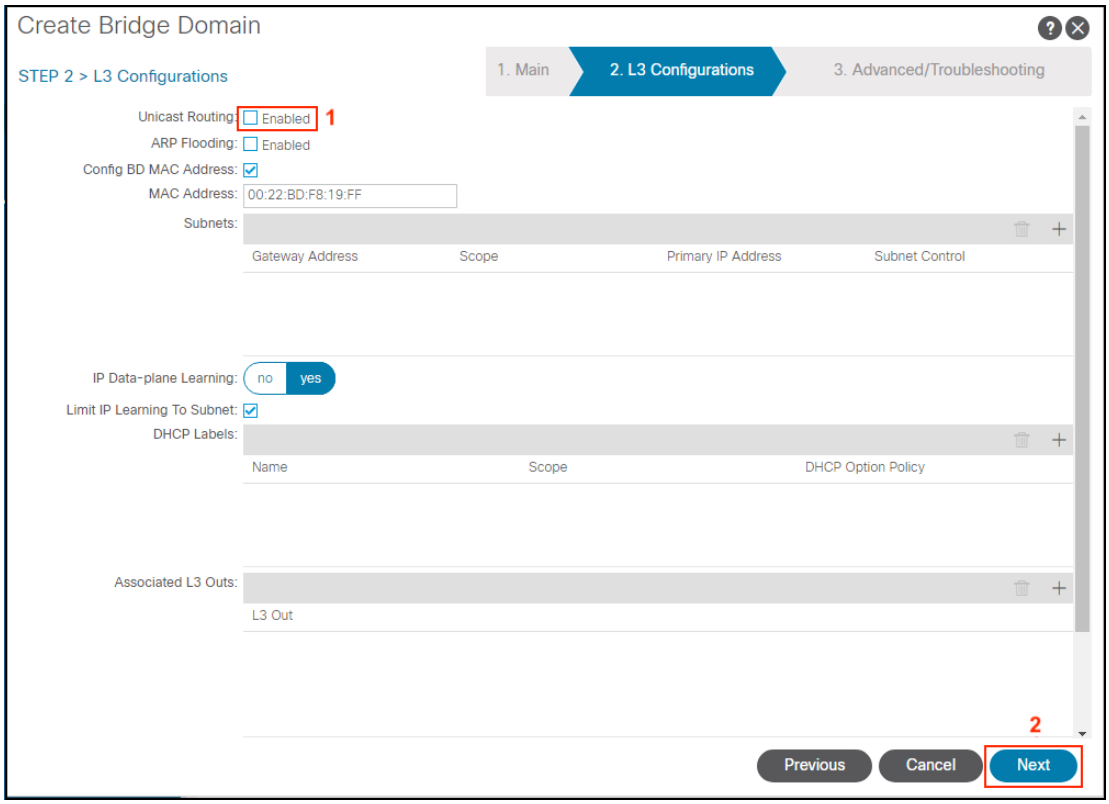


k. Enter the Bridge Domain name **SDC1-FTD-CCL (1)** and click **Next (2)**

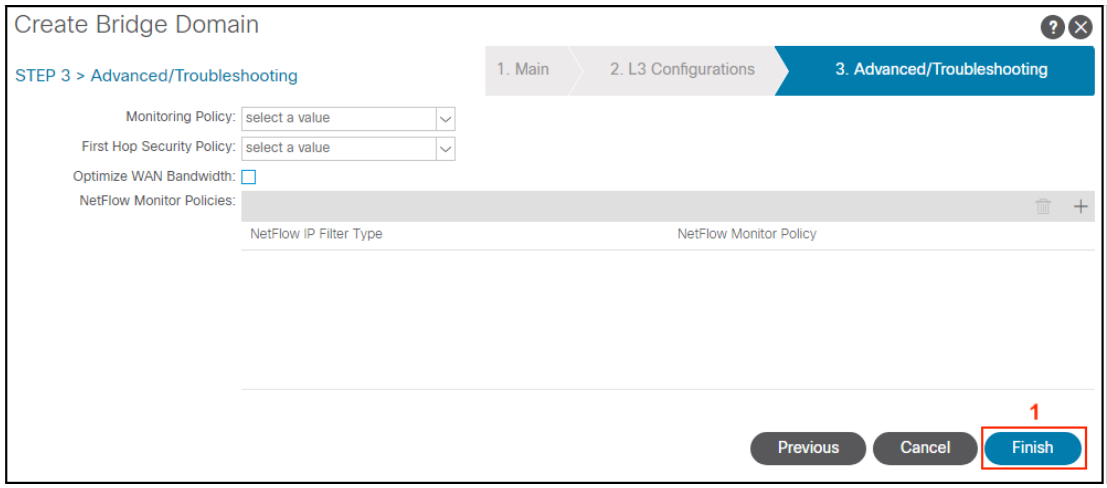


Return to Contents

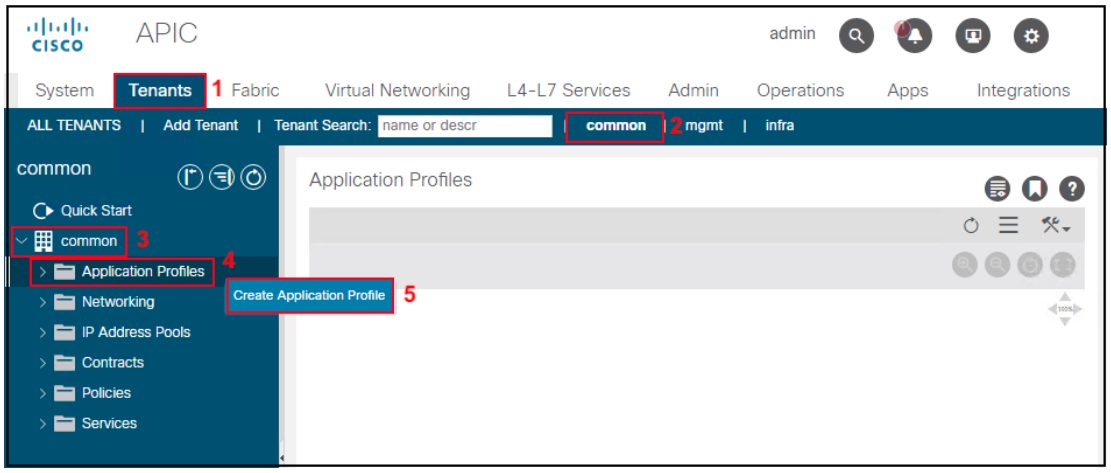
l. Uncheck **Unicast Routing (1)** and click **Next (2)**.



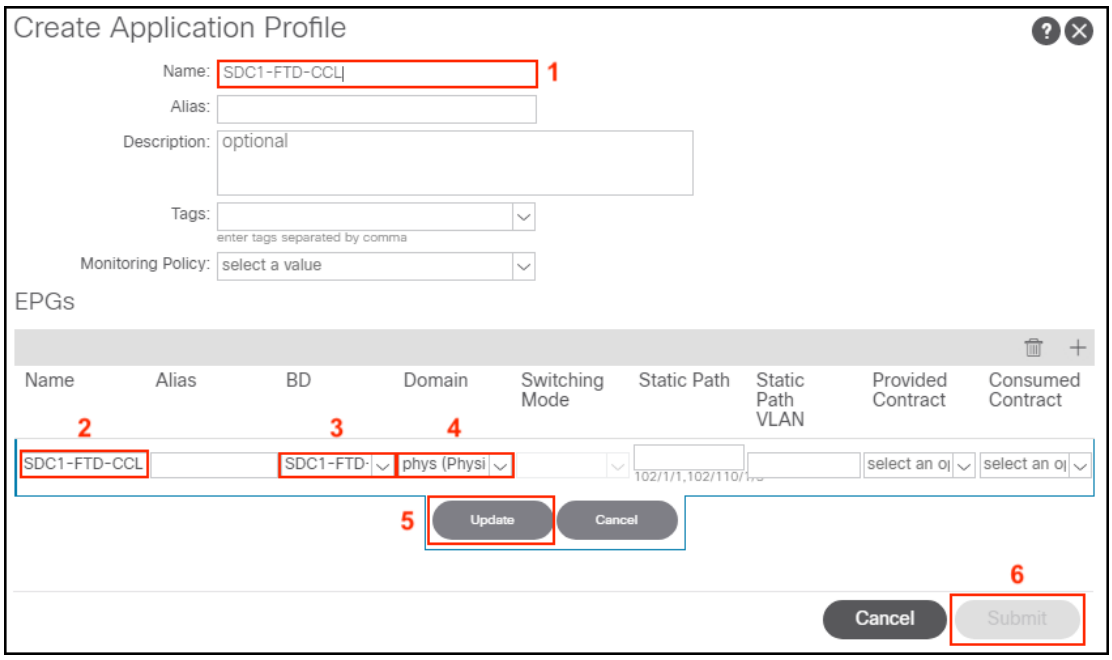
m. Click **Finish (1)**.



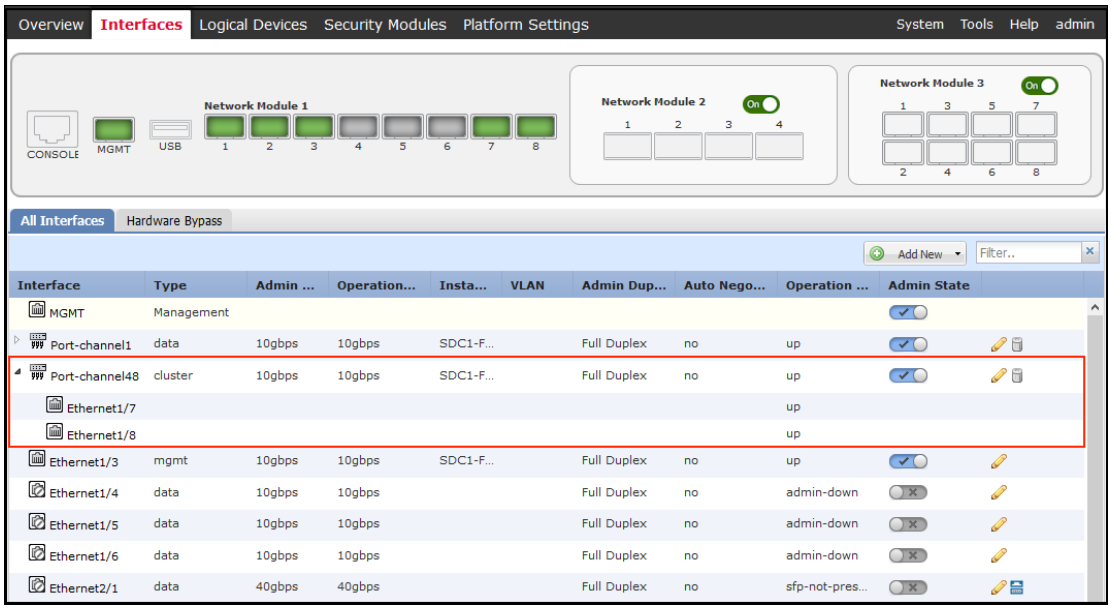
n. Create the SDC1-FTD-CCL Application Profile. Navigate to **Tenants (1)->Common (2)->Common (3)->Application Profiles (4)->**right click and select **Create Bridge Domain (5)**.



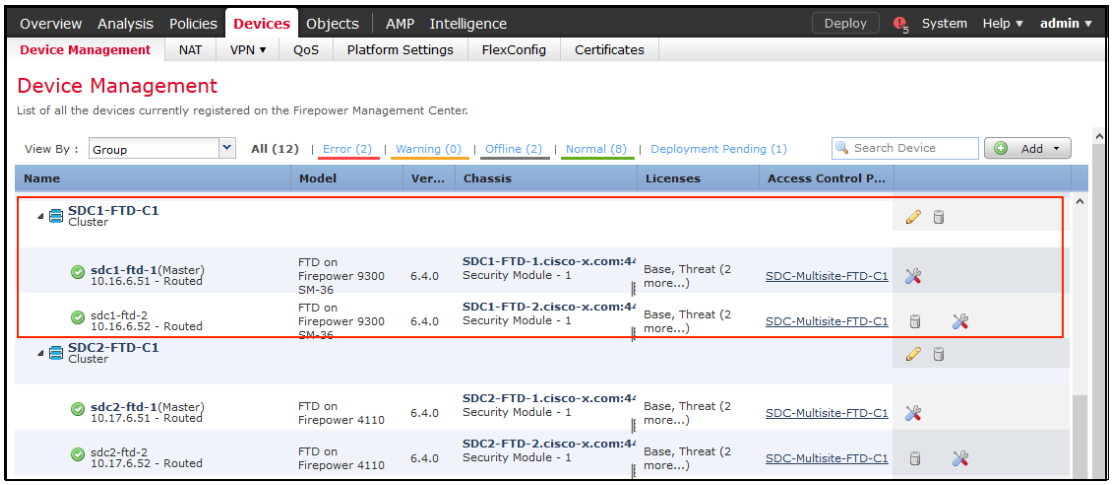
o. Enter the name **SDC1-FTD-CCL (1)** and EPG name **SDC-FTD-CCL (2)**. Select the BD **SDC1-FTD-CCL (3)** and the Domain **Phys (4)**. Click **Update (5)** and **Submit (6)**.



p. Configure the FTD CCL ports from the Firepower Chassis Manager (FCM) for each chassis. Port-channel 48 is the default port for clustering. For configuration details of the CCL port, refer the FCM configuration guide.

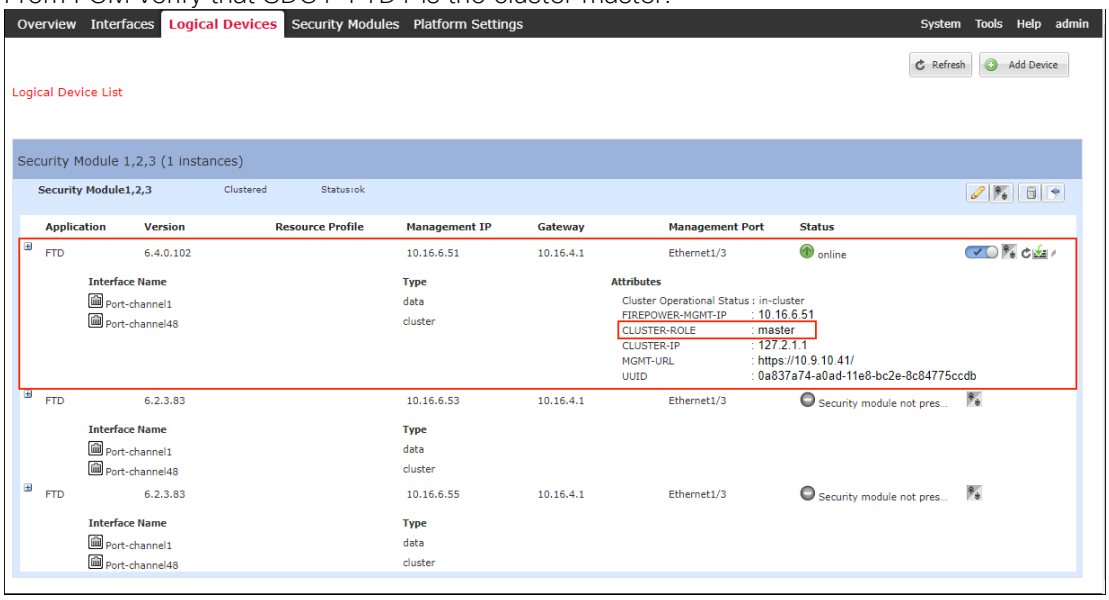


q. In Firepower Management Center (FMC), setup the FTD cluster. Refer to the FTD guides for details.

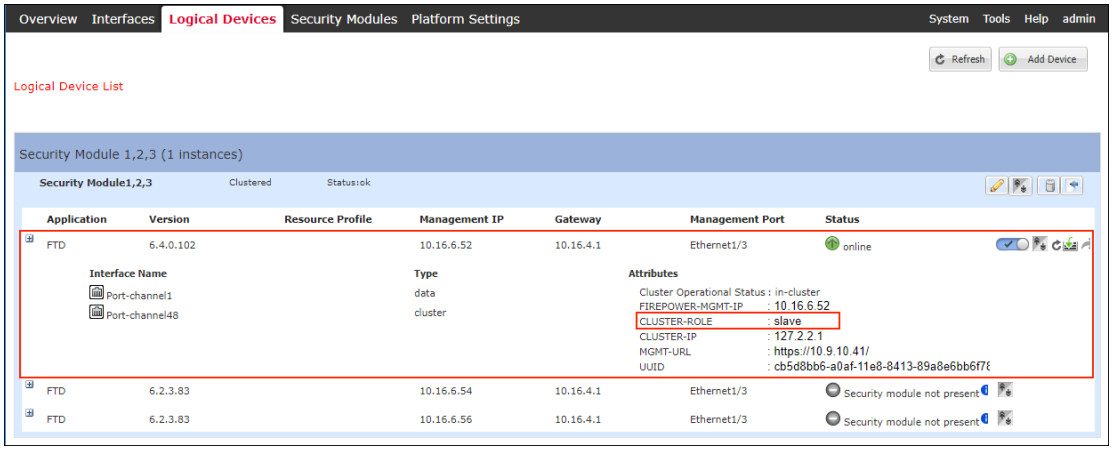


r. Once the cluster has been setup and formed on FMC, the change is reflected on FCM.

From FCM verify that SDC1-FTD1 is the cluster master.

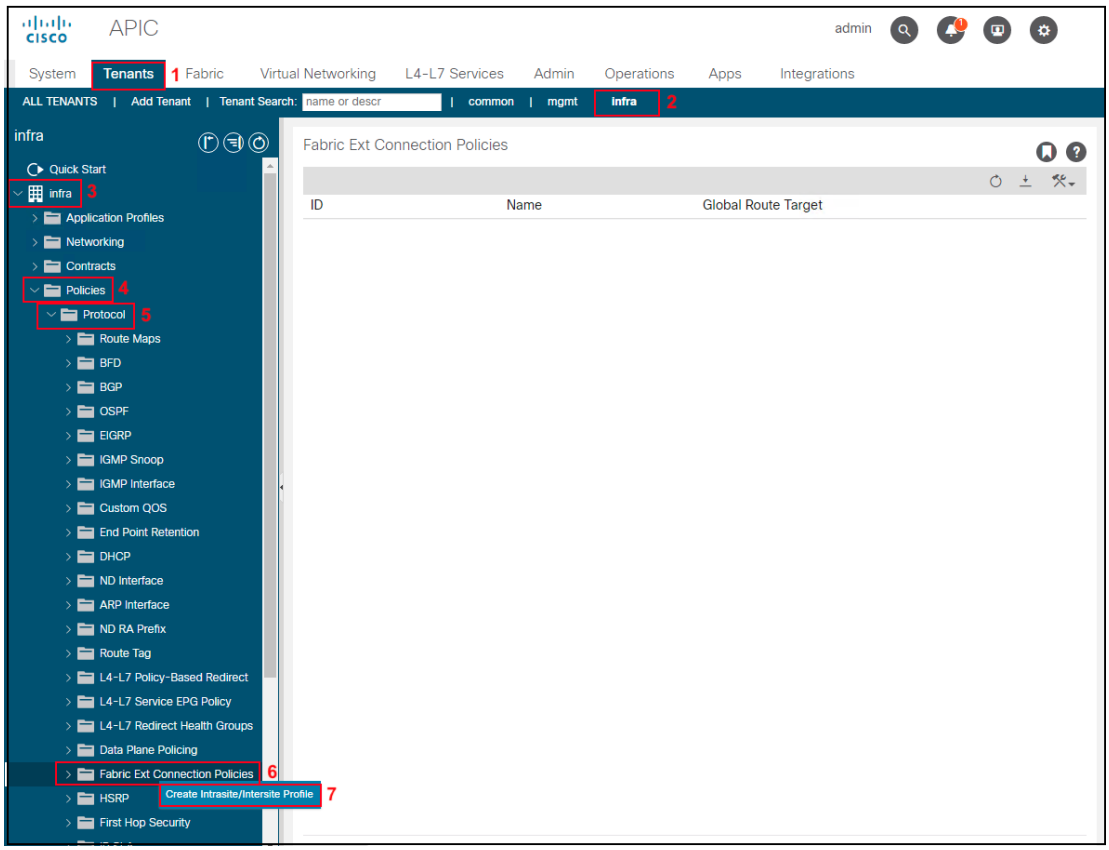


SDC1-FTD2 is the slave



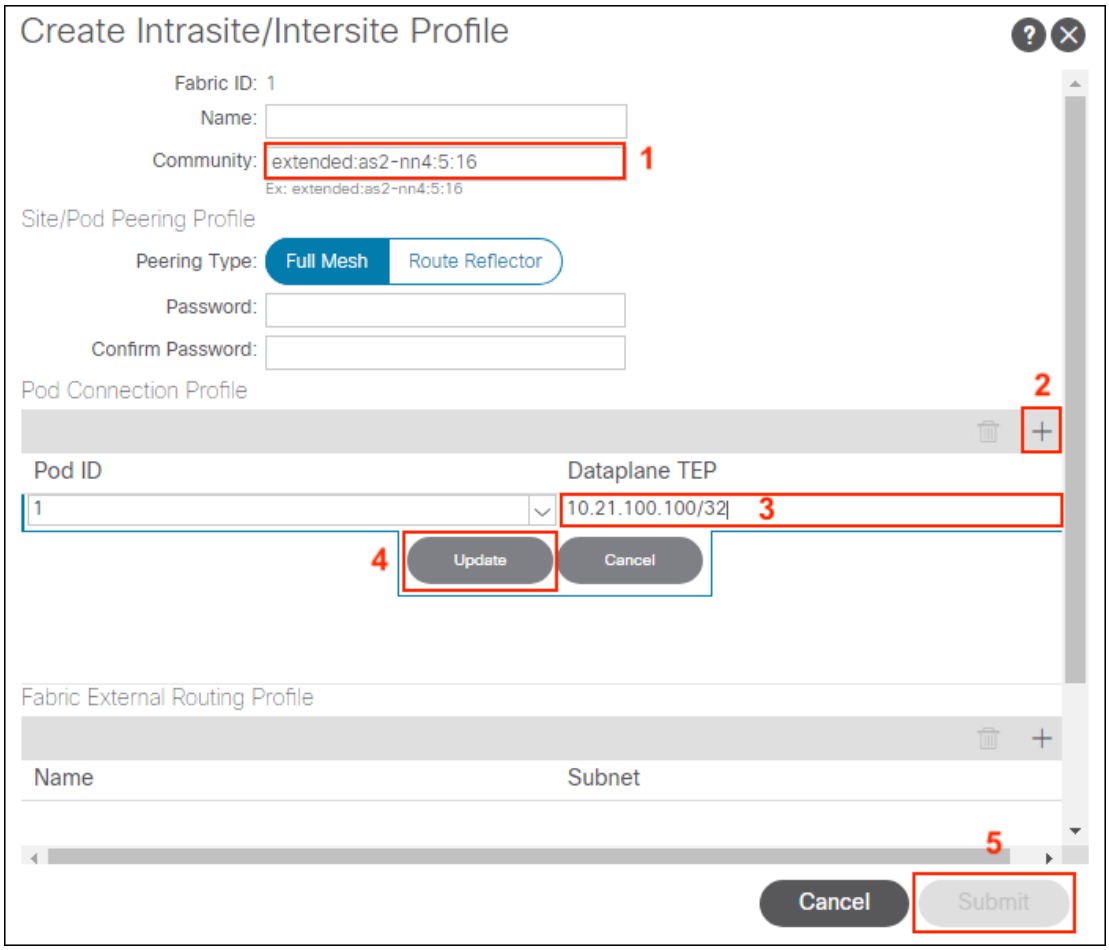
Step 9: Overlay Tunnell Endpoint (TEP) for Intersite

a. To setup the Intersite Profile, configure the Dataplane TEP IP on each end of the tunnel. Navigate to **Tenants (1)->Infra (2)->Infra (3)->Policies (4)->Protocol(5)**. Right click **Fabric Ext Connection Polices (6)** and click **Create Intrasite/Intersite Policy(7).**



Return to Contents

b. Enter the community string **extended:as2-nn4:5:16 (1) and click the + sign (2)** under Pod Connection Profile. Enter the Dataplane TEP IP **10.21.100.100/32 (3)** and click **Update (4)** and **Submit (5)**.



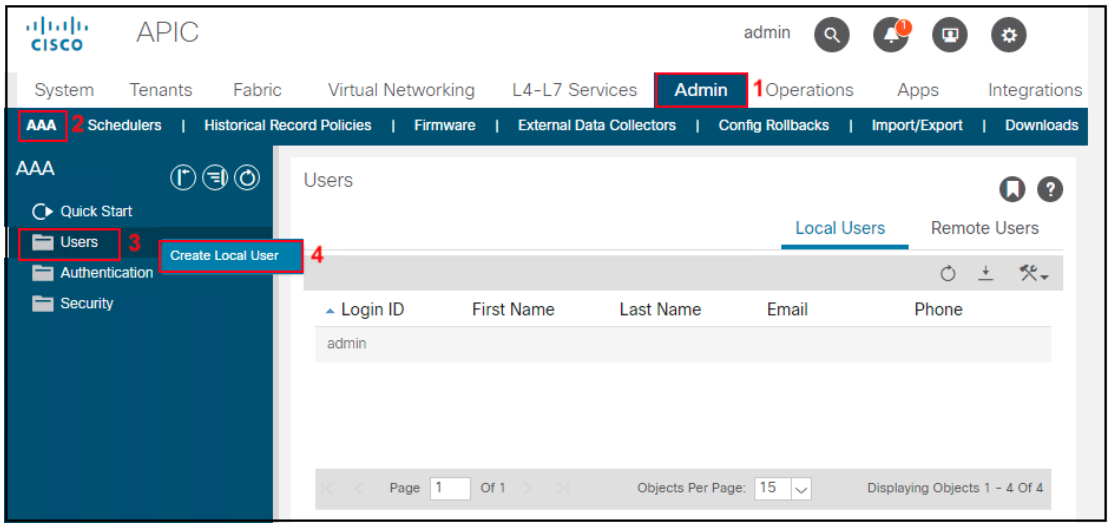
Return to Contents

Step 10: Multi-Site Orchestrator (MSO) Admin Account

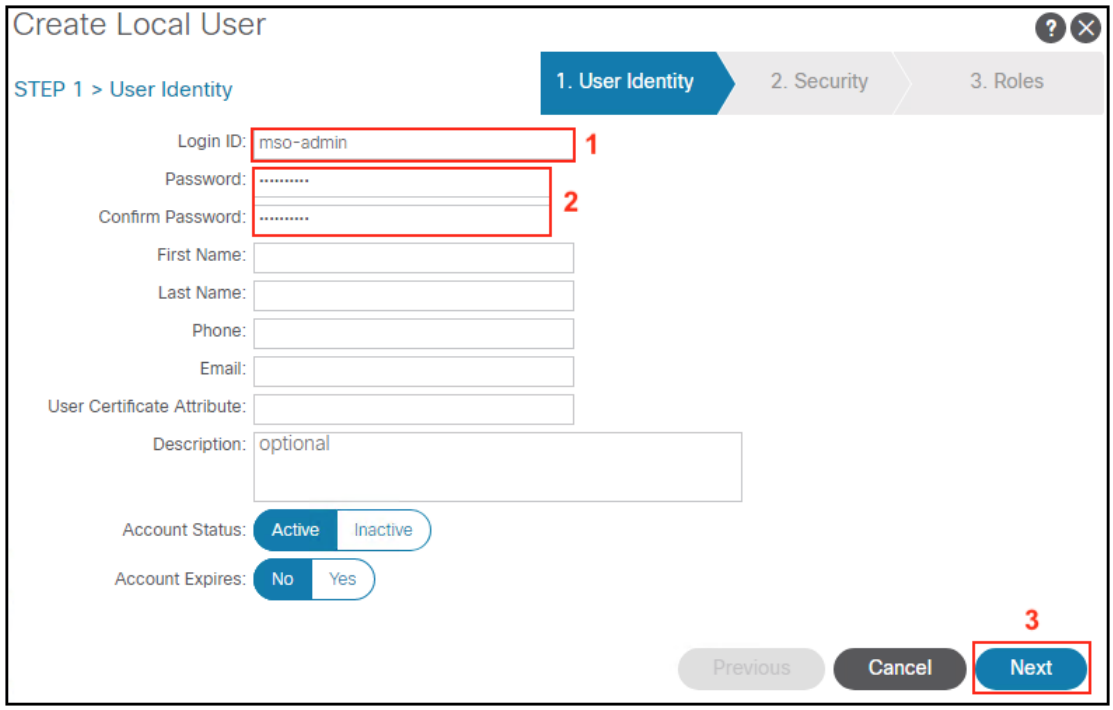
a. This step is optional. It is recommended that you create a specific account for MSO so that activity can be identified easily in APIC Audit Logs.

To setup the MSO Admin account use these instructions below for Configuring a Local User, https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/basic-config/b_ACI_Config_Guide/b_ACI_Config_Guide_chapter_011.html#concept_C29611371F5549F7AD548BA528CECE3E.

We setup an mso-admin account in each APIC cluster. Connect the APIC GUI in each site and navigate to **Admin (1)->AAA (2)->Security Management (3)->Local Users (4)**, Right-Click to select **Create Local User (4)**.

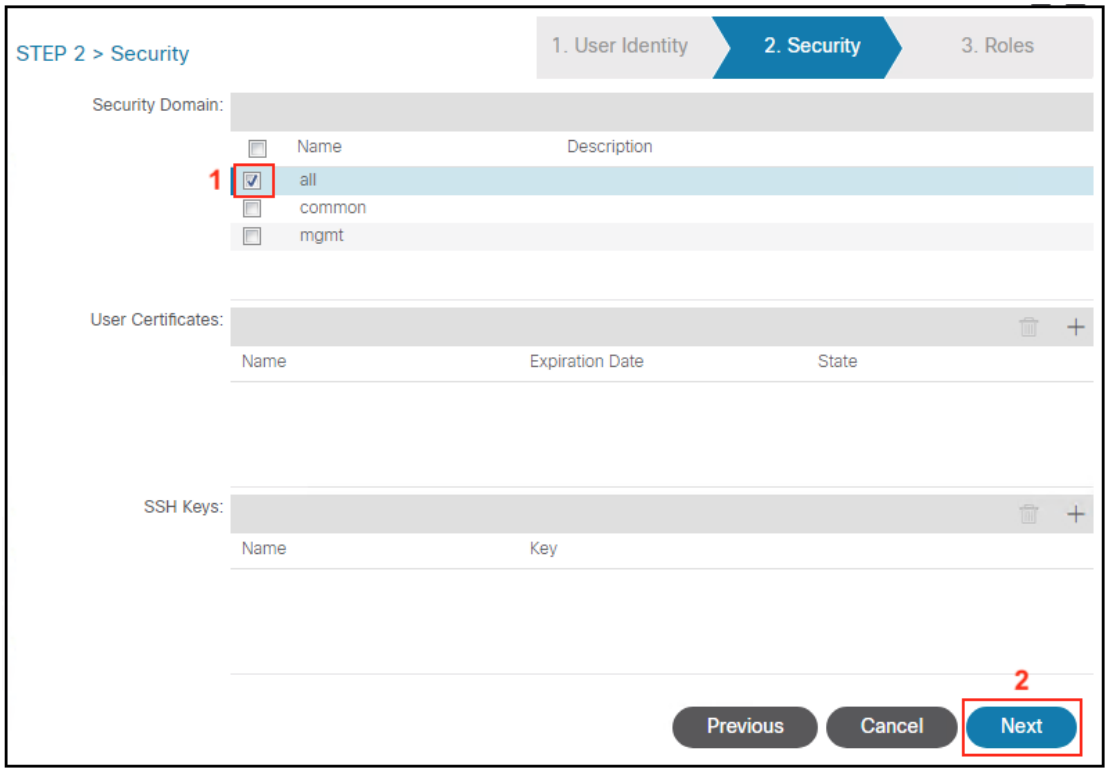


b. Fill in the **Login ID (1)** for the MSO account, **Password (2)** and Select **Next (3)**.



Return to Contents

b. Select **all Security Domains (1)** and click **Next (2)**.



c. Select the **+ sign (1)** to add a Role for the MSO Account. Select the **admin (2)** Role Name and **Write (3)** Role Privilege, click **Update (4)** and click **Finish (5)**.

Return to Contents

Step C: Install ACI Multi-Site Orchestrator and Setup Initial Configuration

Step 1: Install ACI Multi-Site Orchestrator (MSO)

Install ACI Multi-Site Orchestrator. We used the following document to setup the reference design, https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211.html

The following table represents the ACI Multi-Site – VMware vSphere Requirements. We deployed three Multi-Site Orchestrator virtual machines that defaulted to these settings.

Cisco ACI Multi-Site Orchestrator Version	VMware vSphere Requirements
Release 2.1(1i)	• ESXi 6.0 or later • 8 vCPUs • 24 GB of RAM • 64 GB disk

We followed the Deploying Cisco ACI Multi-Site Release 2.1(x) Using OVA Section, https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211_chapter_010.html#id_79611

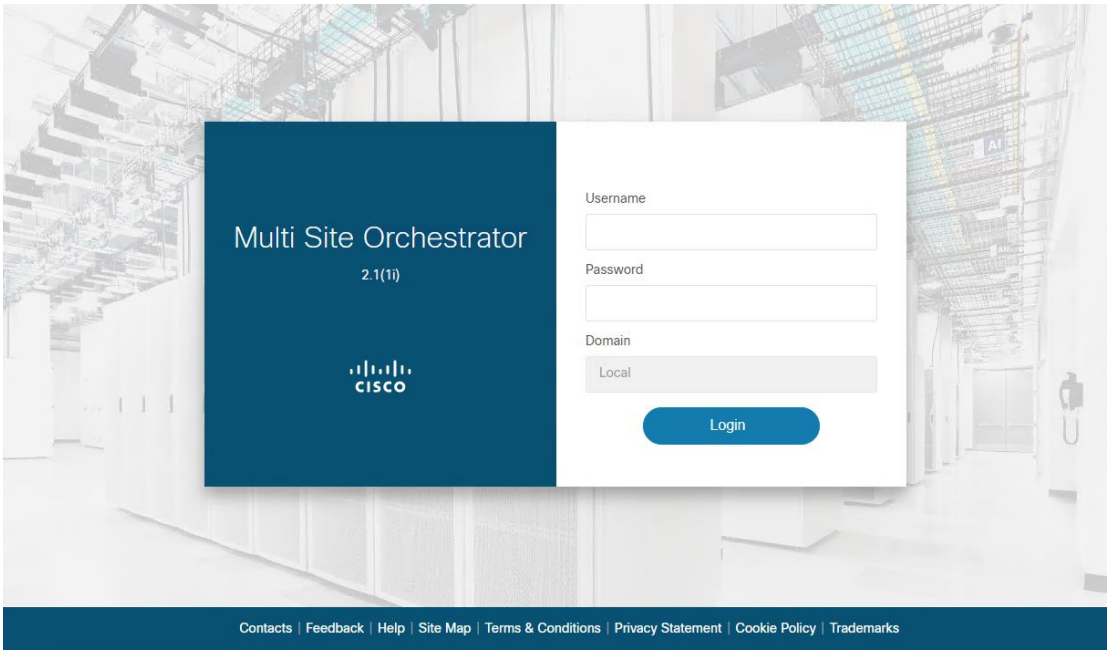
Note: In step 2 in the link above, use the root account when logging into MSO with SSH.

Step 2: Setup Day 0 Operations of ACI Multi-Site Orchestrator (MSO)

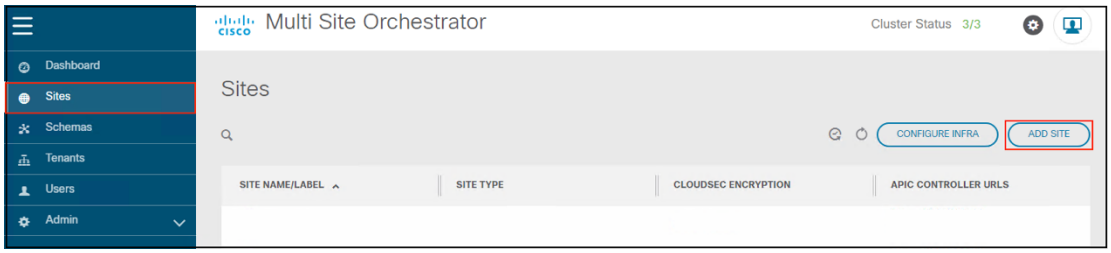
https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211_chapter_011.html

The Overlay Tunnel Endpoint (TEP) Intersite policy for Cisco APIC was setup in Step C9 above.

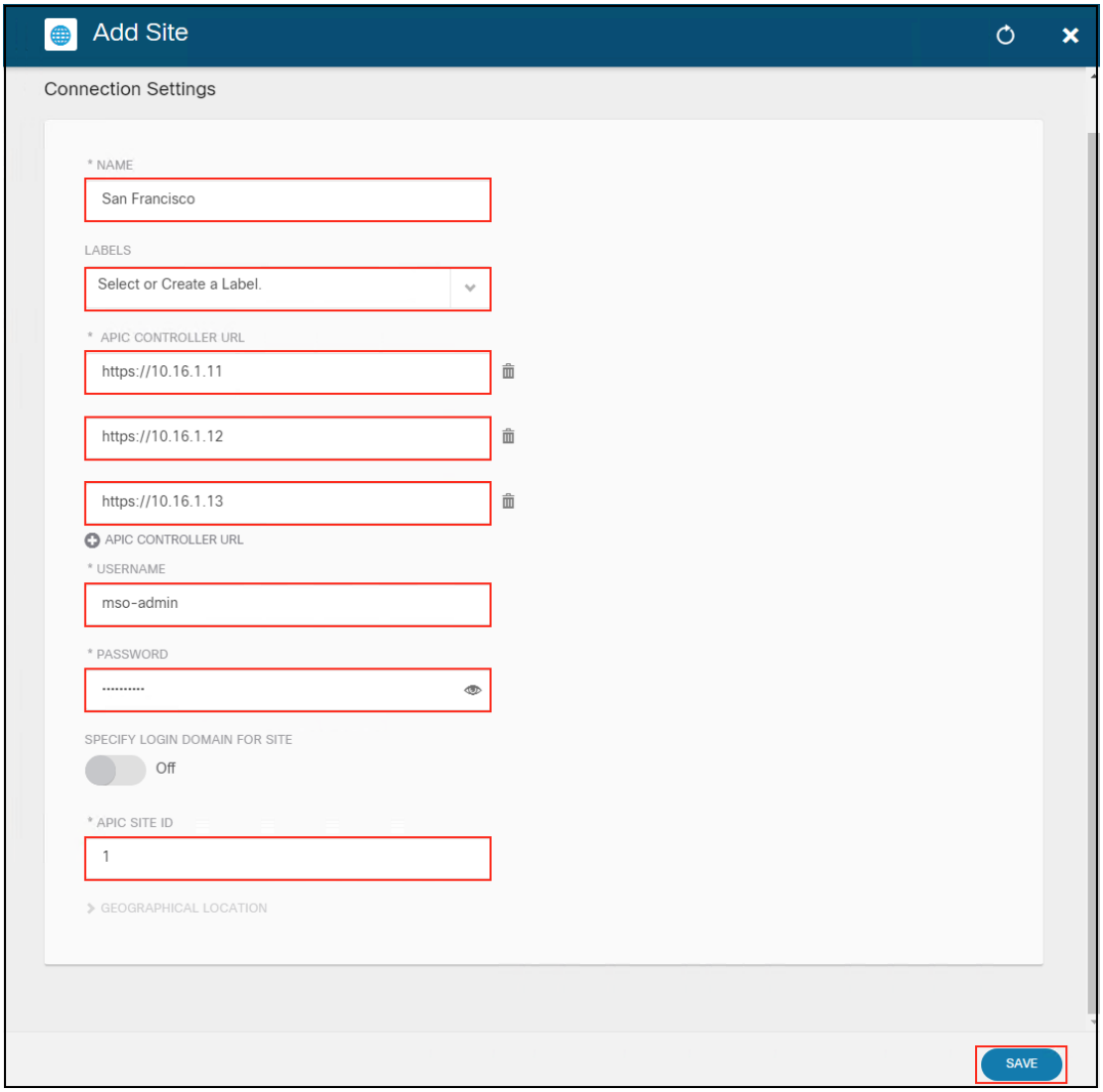
Add the Sites using the MSO GUI. Log into MSO Login Screen, **https://<your-MSO-IP address>.** You can connect to any of the nodes in the cluster. Log in using the first time login admin credentials provided in the above link, or the updated admin credentials that have previously been configured.



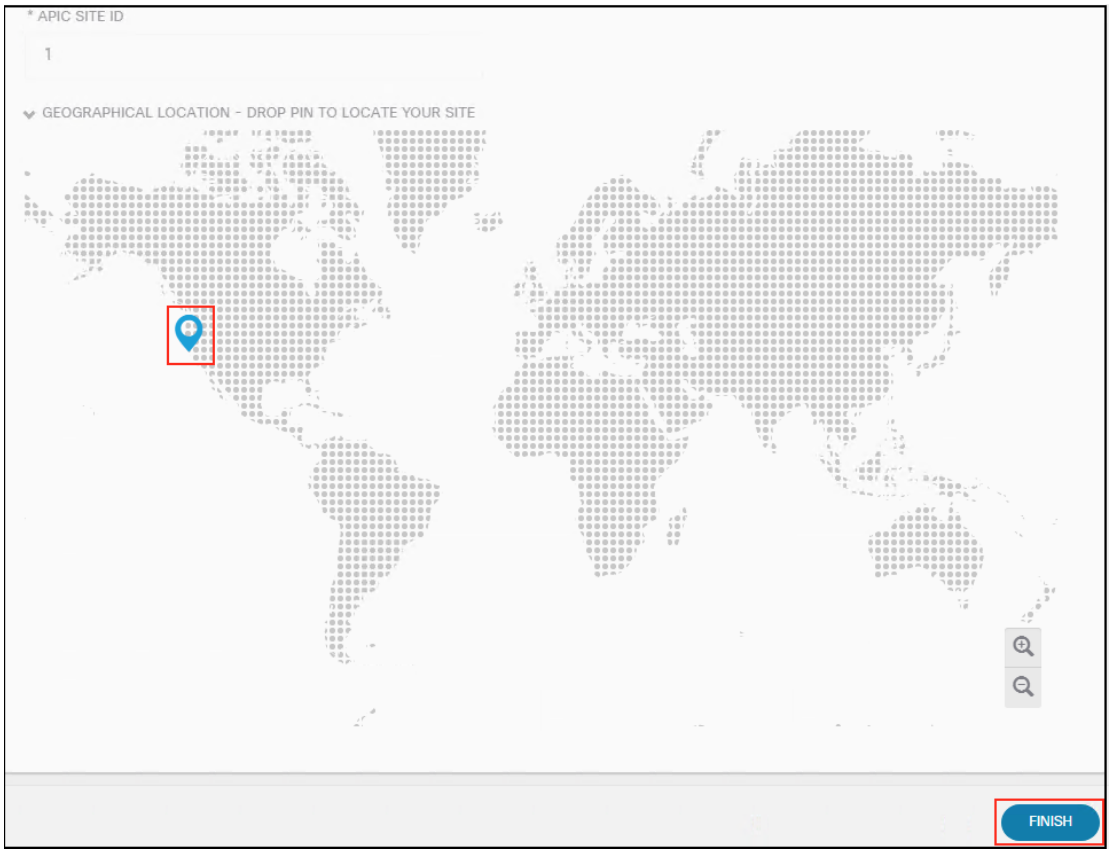
a. Navigate to Sites in the left pane and then select **ADD SITE**



b. Fill in the details for the San FranCisco Site. **Provide the Site Name, the IP addresses for each of the nodes in the APIC cluster, login credentials and APIC Site ID** and click **SAVE**.

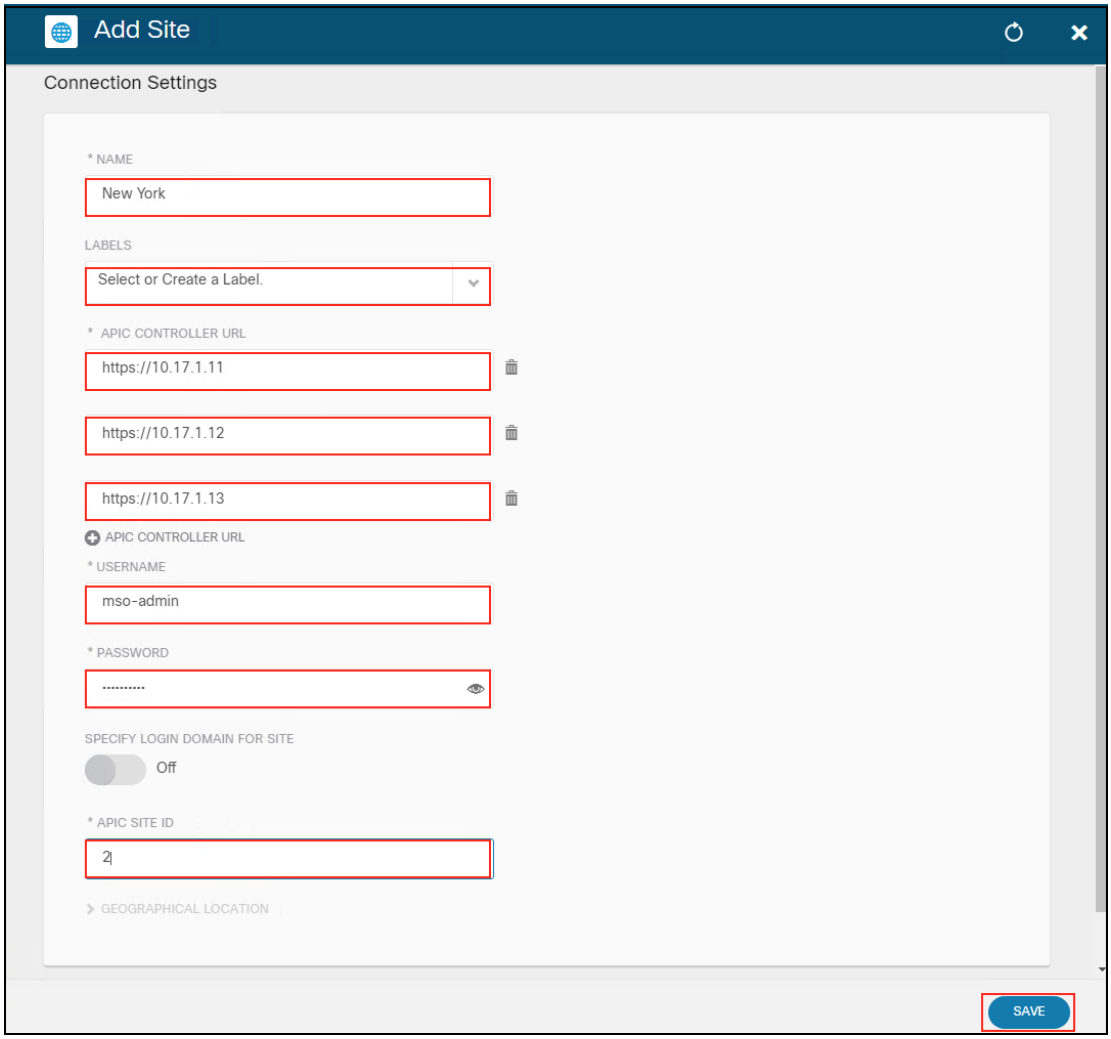


d. Drop a pin on the San FranCisco location on a map and click FINISH.

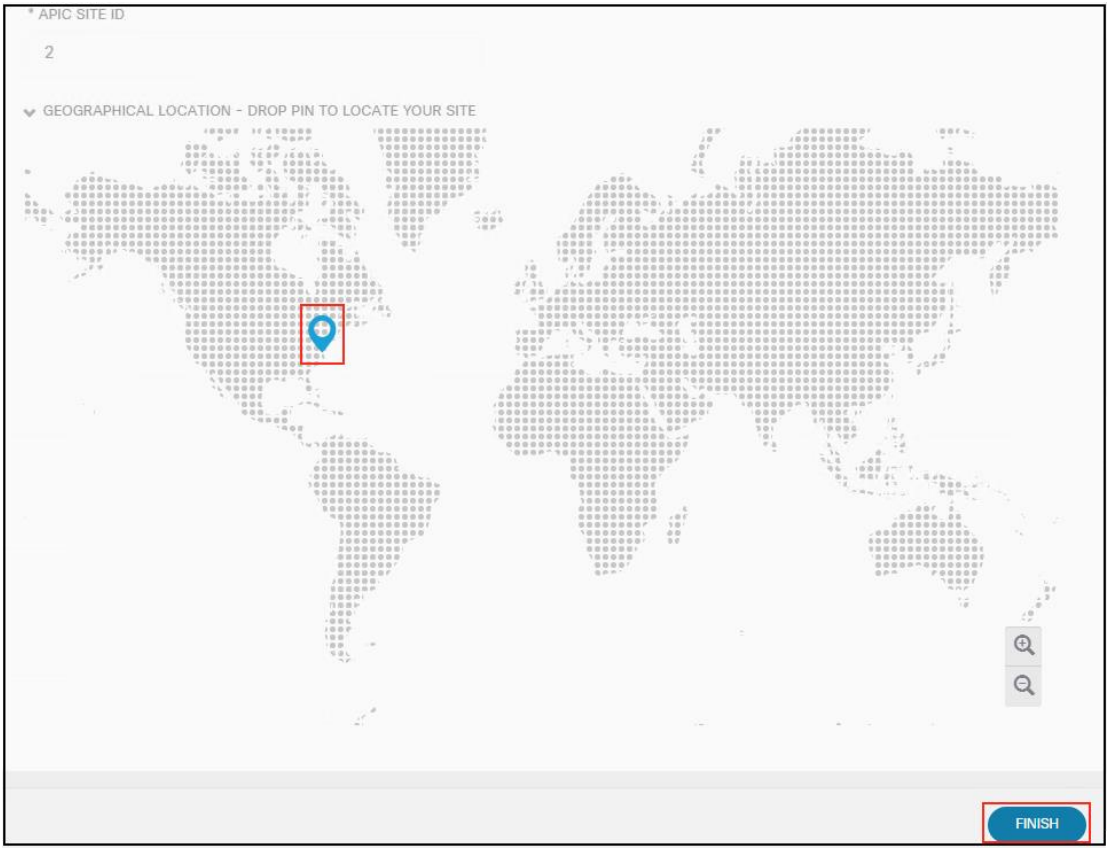


Return to Contents

e. Fill in the details for the New York Site. **Provide the Site Name, the IP addresses for each of the nodes in the APIC cluster, login credentials and APIC Site ID.**



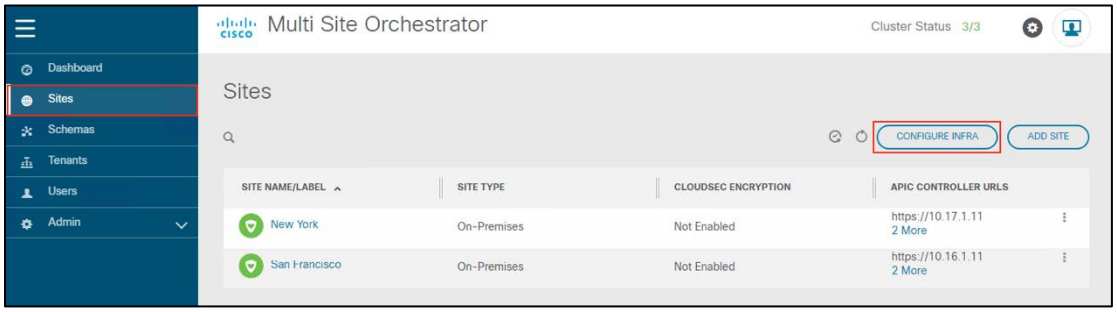
f. Drop a pin on the New York location on a map and click FINISH.



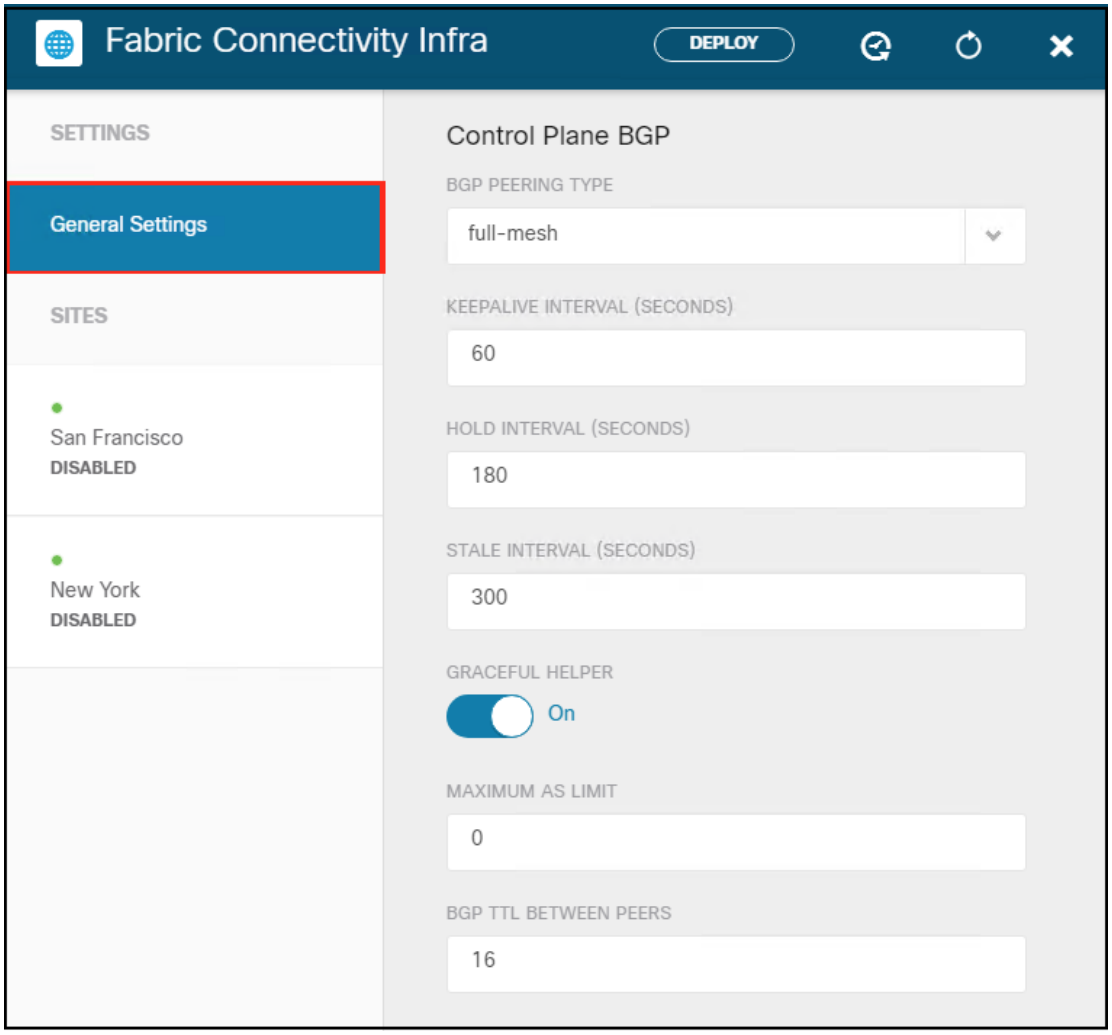
Step 3: Configure Fabric Connectivity Infrastructure (Infra) in MSO GUI

Refer to the following document for the steps we followed, https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211_chapter_011.html#id_52935 .

a. Navigate to Sites in the left pane and then select CONFIGURE INFRA.

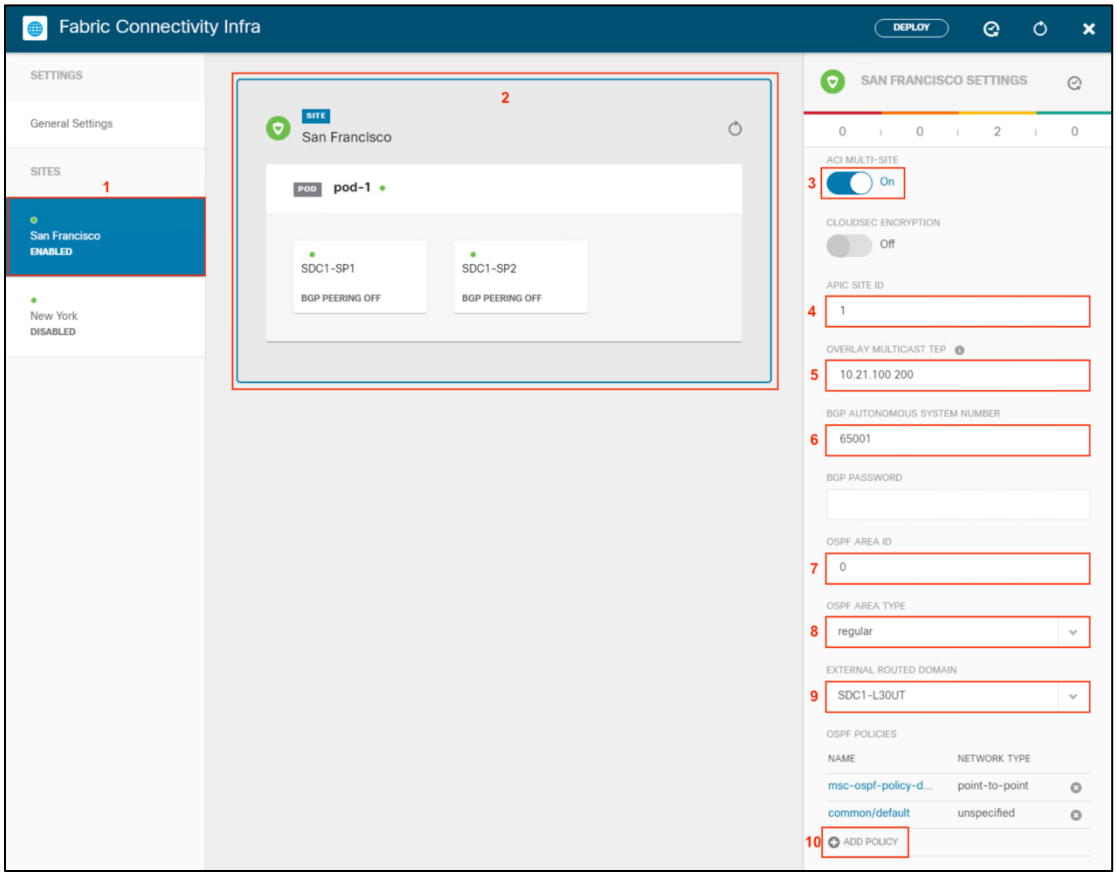


b. General Settings is the initial screen and we tested the default settings.



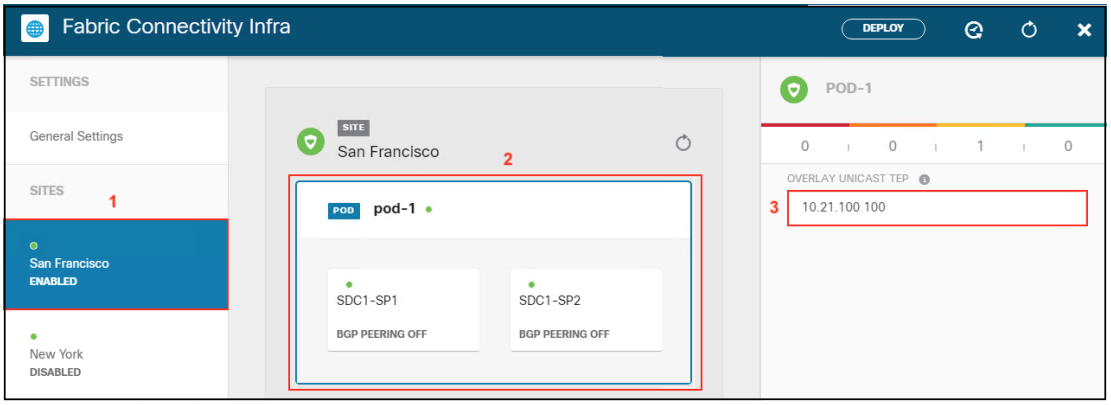
Return to Contents

c. Select Site San FranCisco and fill in the site specific settings in the right panel. Enable Multi-Site (3) and set the APIC ID (4), Data Plane Multicast TEP address (5), BGP ASN (6), OSPF area ID (7), OSPF area type (8), External Routed Domain (9). Select Add Policy (10) to create a new OSPF policy.

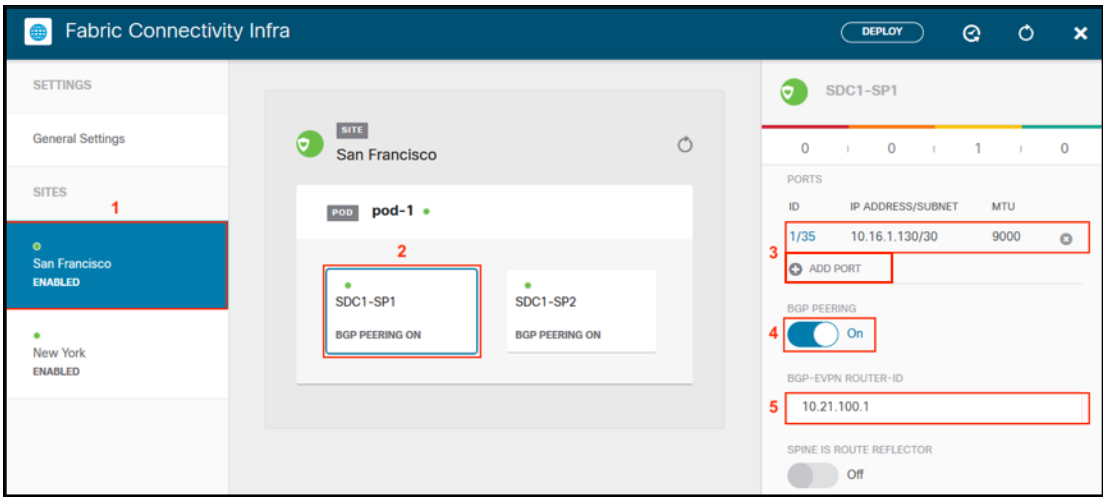


Return to Contents

d. Fill in the Pod specific settings for San FranCisco. Select San FranCisco in the left panel (1), select POD (2) and enter the Data Plane Unicast TEP IP address (3).

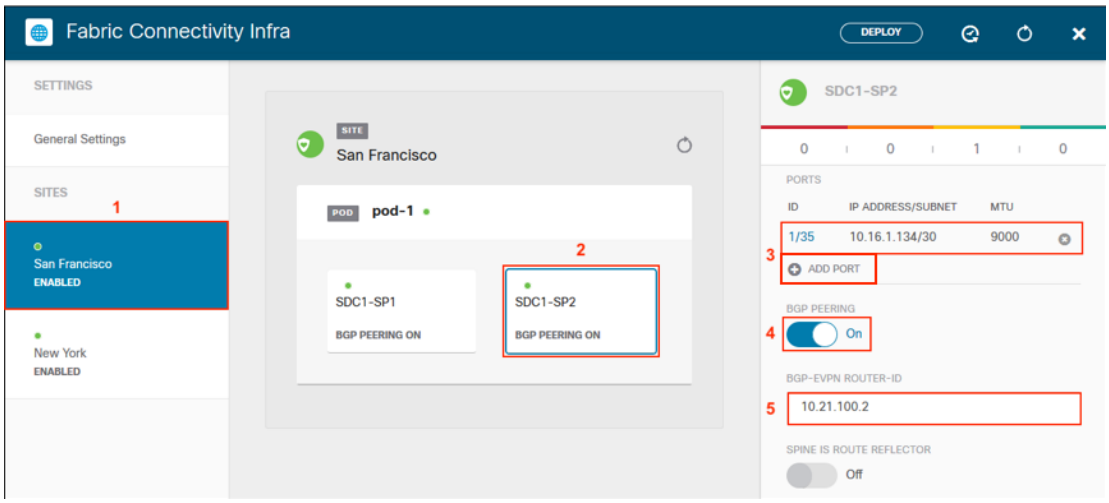


e. Fill in San FranCisco Spine 1 specific settings. Select San FranCisco in the left panel (1), select Spine 1 in POD (2). Click ADD PORT, enter the port, IP address, subnet and MTU for the intersite connection in Spine 1 (3). Enable BGP peering (4). Set the Control Plane TEP IP address(5).

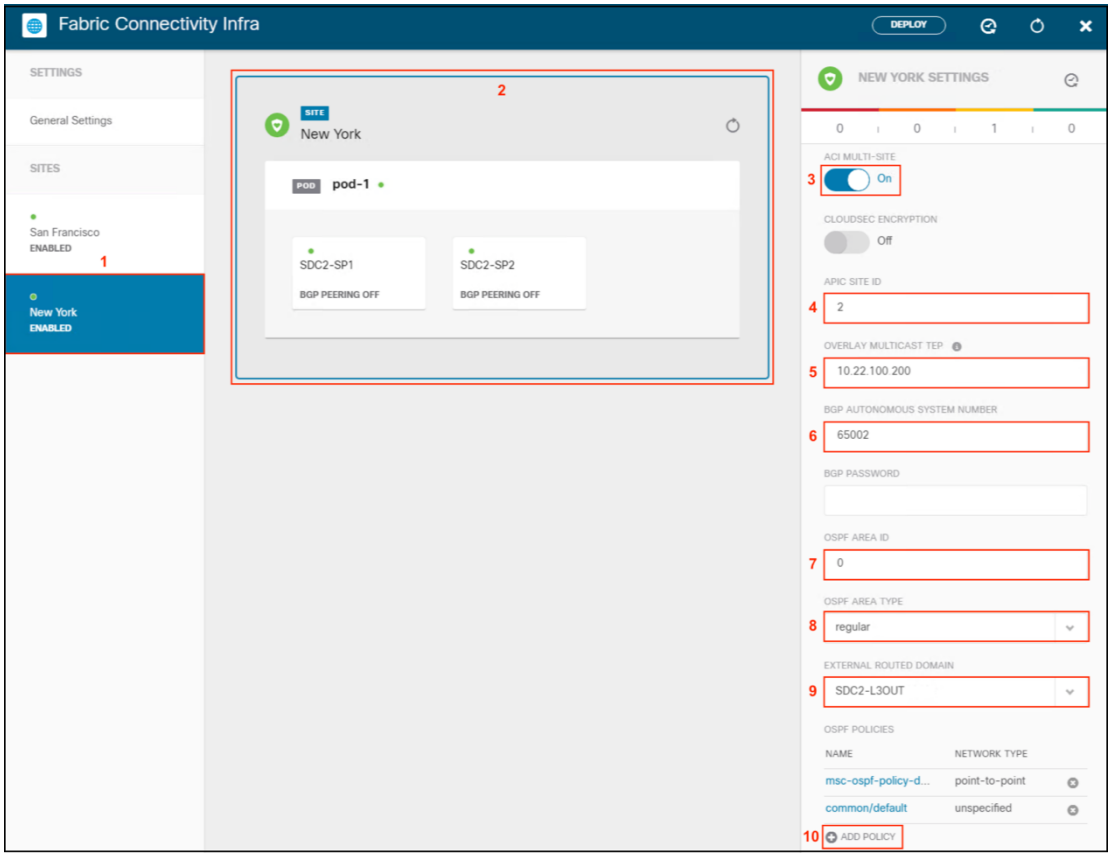


Return to Contents

f. Fill in San FranCisco Spine 2 specific settings. Select San FranCisco in the left panel (1), select Spine 2 in POD (2). Click ADD PORT, enter the port, IP address, subnet and MTU for the intersite connection in Spine 2 (3). Enable BGP peering (4). Set the Control Plane TEP address(5).

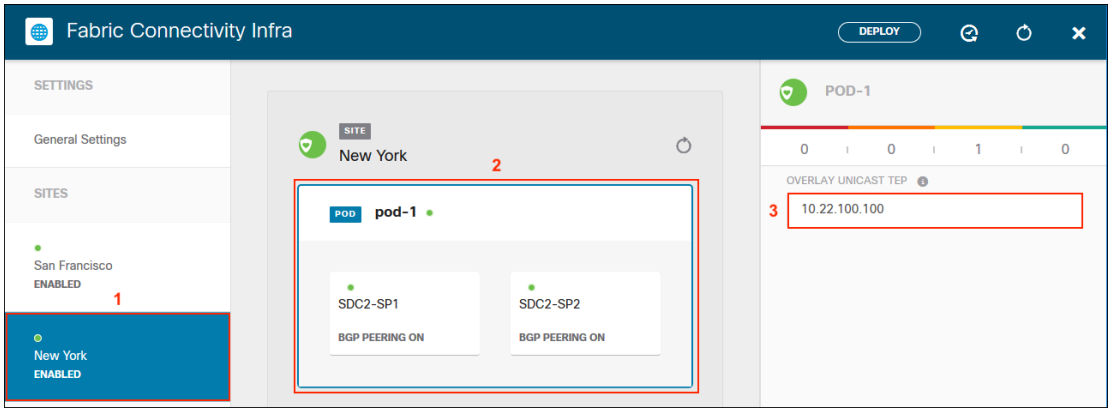


g. Select Site New York and fill in the site specific settings in the right panel. Enable ACI Multi-Site (3) and set the APIC ID (4), Data Plane Multicast TEP address (5), BGP ASN (6), OSPF area ID (7), OSPF area type (8) and External Routed Domain (9). Select Add Policy (10) to create a new OSPF policy msc-ospf-policy-default (d) above in this step, if not already available.

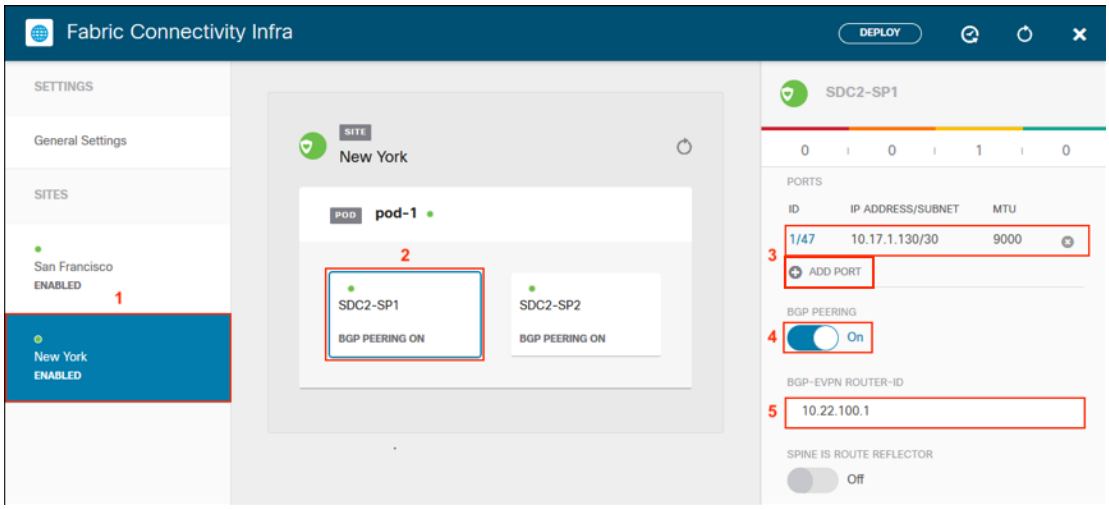


Return to Contents

h. Fill in the Pod specific settings for New York. Select New York in the left panel (1), select POD (2) and enter the Data Plane Unicast TEP IP address (3)

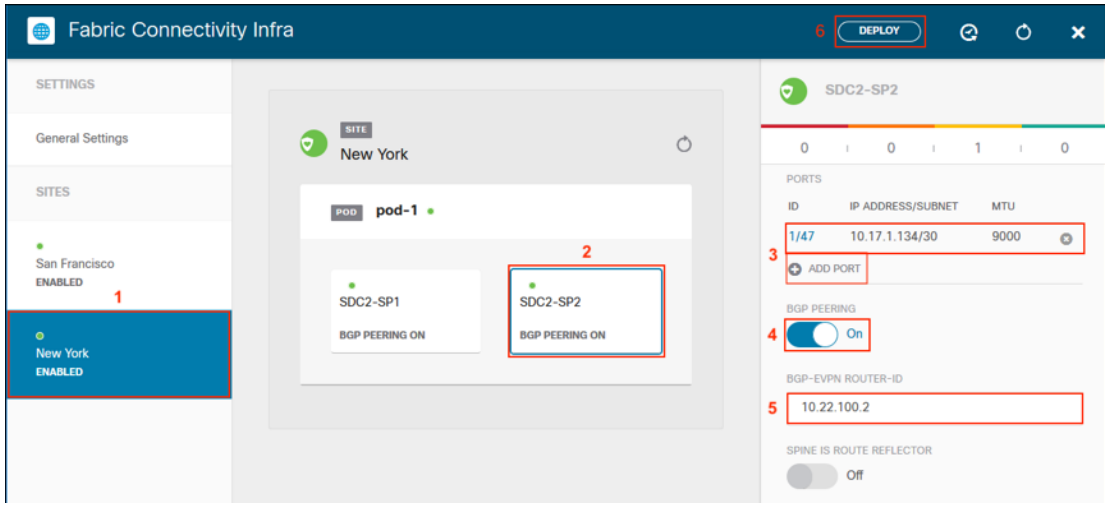


i. Fill in New York Spine 1 specific settings. Select New York in the left panel (1), select Spine 1 in POD (2). Click ADD PORT, enter the port, IP address, subnet and MTU for the intersite connection in Spine 1 (3). Enable BGP peering (4). Set the Control Plane TEP IP address(5).



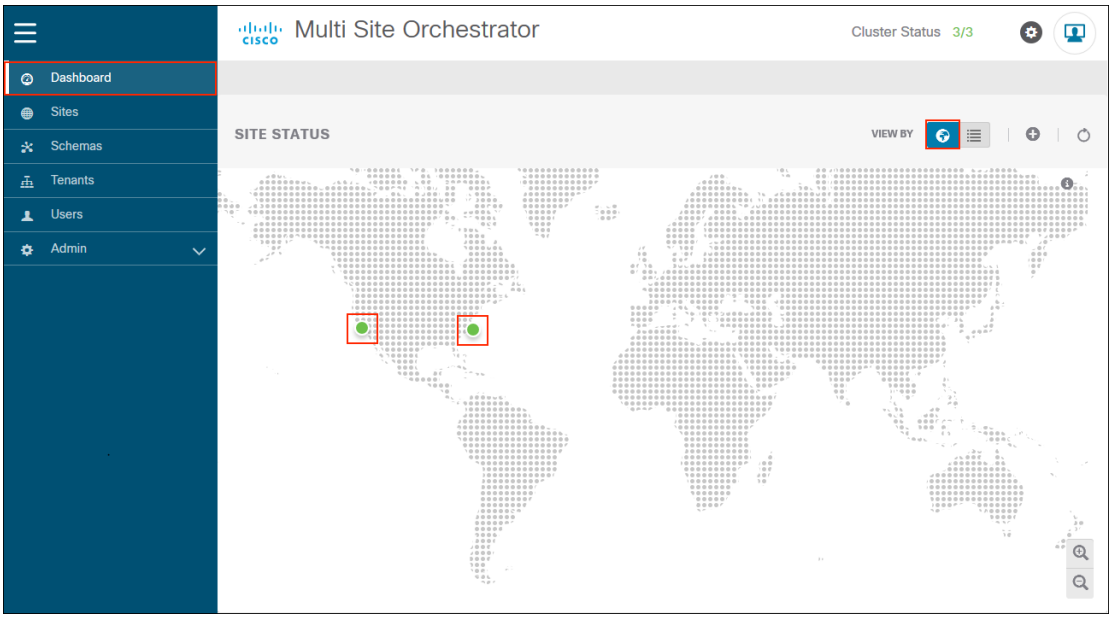
Return to Contents

j. Fill in New York Spine 2 specific settings. Select New York in the left panel (1), select Spine 2 in POD (2). Click ADD PORT, enter the port, IP address, subnet and MTU for the intersite connection in Spine 2 (3). Enable BGP peering (4). Set the Control Plane TEP IP address(5). The Infra is now configured, select Deploy (6) to push the configuration down to the APIC clusters in each site.



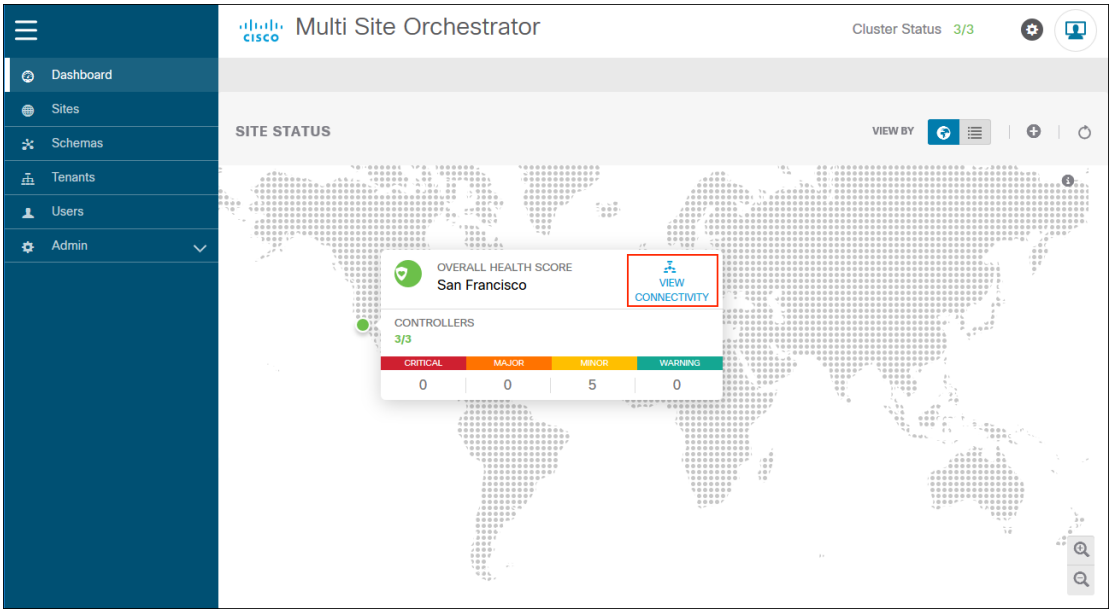
Step 4: Validate Intersite Policy with the MSO Dashboard

a. Confirm that the Intersite policy is deployed properly, go to the MSO Dashboard by selecting Dashboard in the left pane. The Dashboard has two view options: global and table. The default view is the global view. The green dots represent San FranCisco and New York.



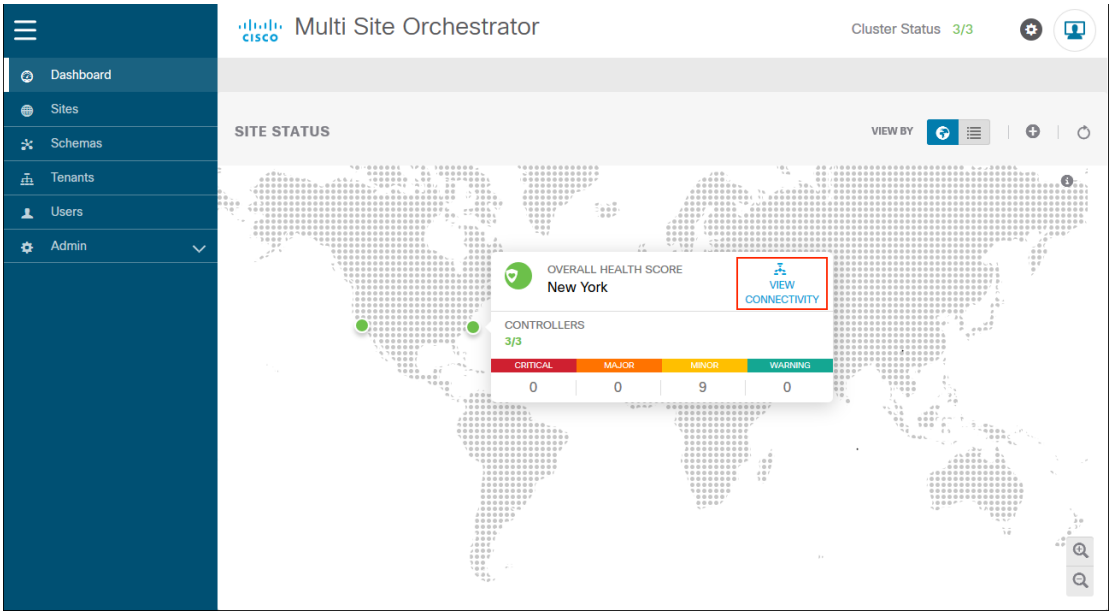
Return to Contents

b. Hover over the San FranCisco Site to view the health score. Select View Connectivity to confirm the status of the intersite connection.



c. The result of View Connectivity should be green and the white dot should be moving back and forth between the two sites.

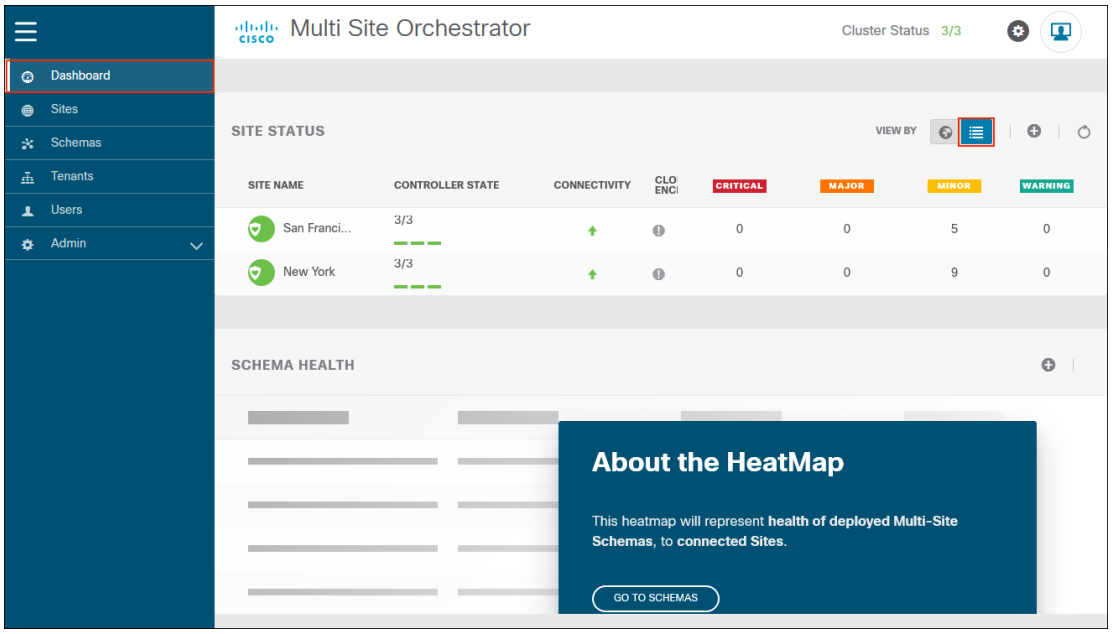
d. Hover over New York Site to view the health score. **Select View Connectivity** to confirm the status of the **intersite** connection.



e. The result of View Connectivity should be green and the white dot should be moving back and forth between the two sites.

Return to Contents

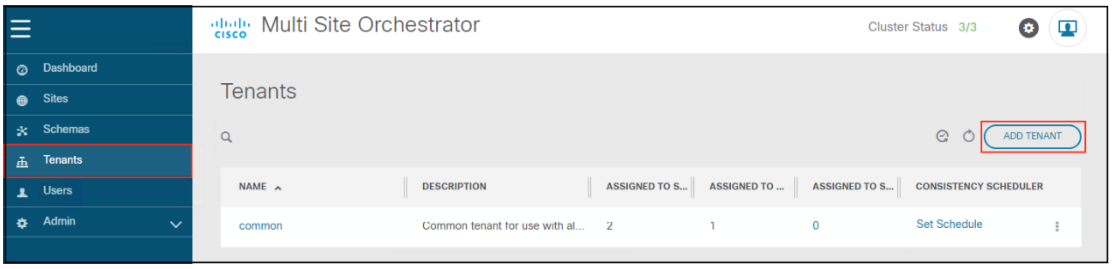
f. View the Dashboard Table view. The Site Health Score is represented as a green circle to the left of the site name. APIC controller status, connectivity status and number of faults by category are provided. Additional information is also provided for Schema Health, which will be populated after the schema is created.



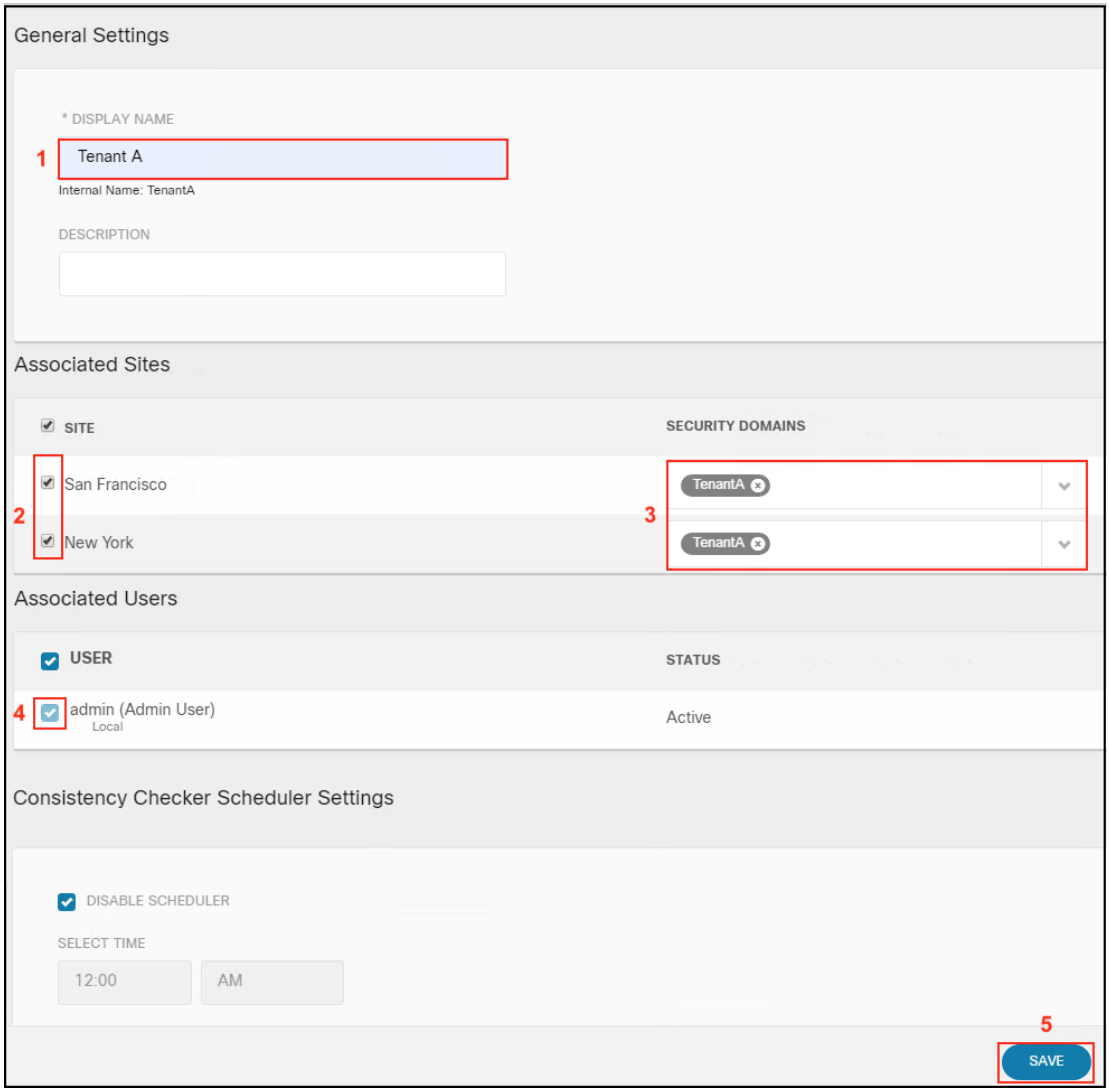
Step 5: Add Tenants using MSO GUI

a. Once intersite is up, you can proceed with adding tenants. In the MSO GUI, select **Tenants** in the left pane. From the Tenants page, Select **ADD TENANT**.

https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211_chapter_011.html#id_52937



b. **To add a Tenant , set the name (1).** Normally you would use the company name or line of business as the tenant name. We chose a tenant name that matched the schema we tested. The tenant name is Tenant A. Next you would **select the sites that are associated with this tenant (2)**. For each site that is associated, you need to **select the Security Domain name for each site (3)**. You need to also **associate the users to the tenant (4)**. Once complete, select **SAVE (5)**.



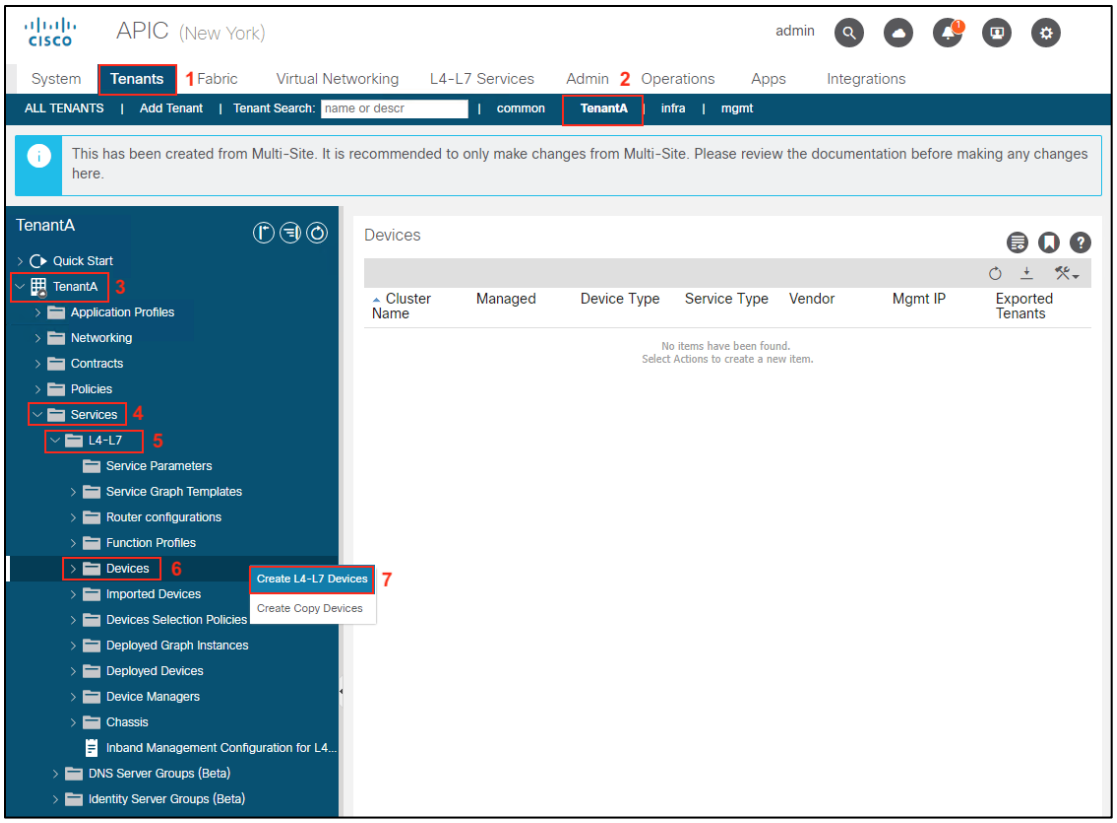
Return to Contents

Step D: Deploy one-arm FTD cluster, PBR and L3Out policy on Tenant in APIC GUI

Step 1: Deploy one-arm Firepower Threat Defense cluster as a L4-L7 Device in APIC GUI

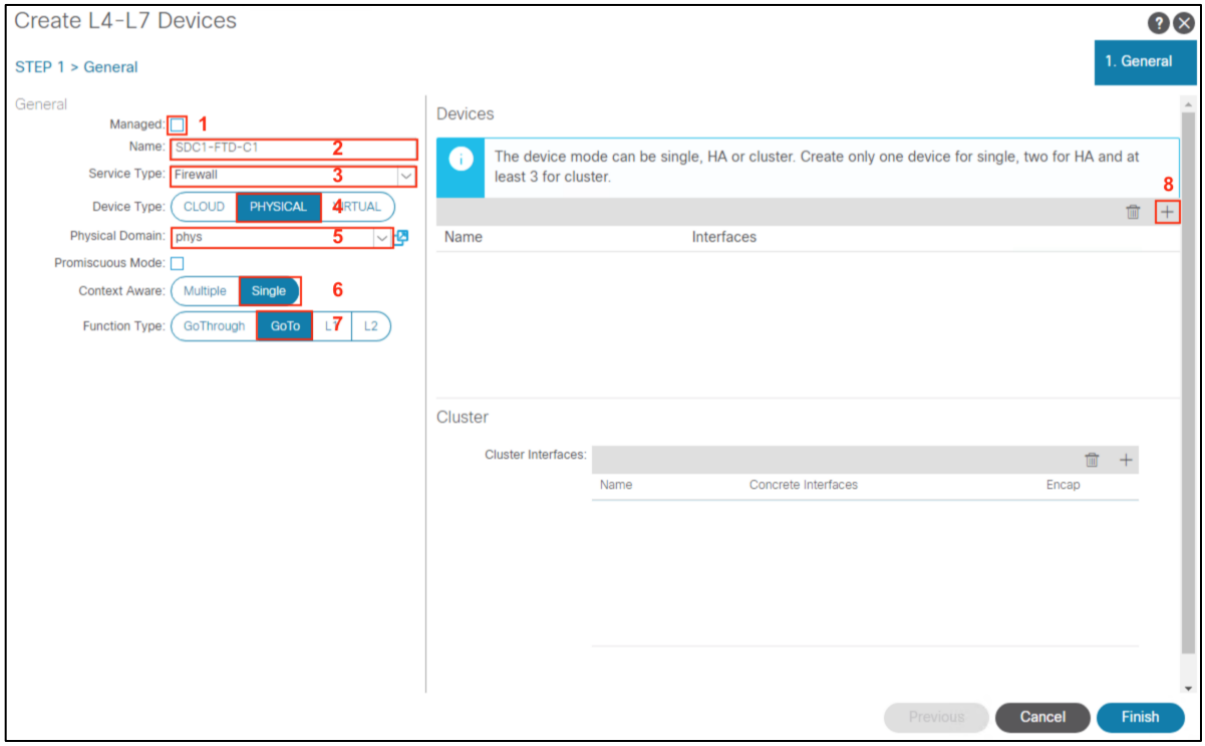
a. Creating L4-L7 Devices, https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/L4-L7-services/Cisco-APIC-Layer-4-to-Layer-7-Services-Deployment-Guide-401/Cisco-APIC-Layer-4-to-Layer-7-Services-Deployment-Guide-401_chapter_011.html

Once the Tenant is deployed, you need to go into the APIC GUI in each site and create the L4-L7 device. Navigate to **Tenant (1)->TenantA (2)-> TenantA (3)->Services (4)->L4-L7(5)->Devices (6)**, Right-Click and select **Create L4-L7 Devices (7)**.

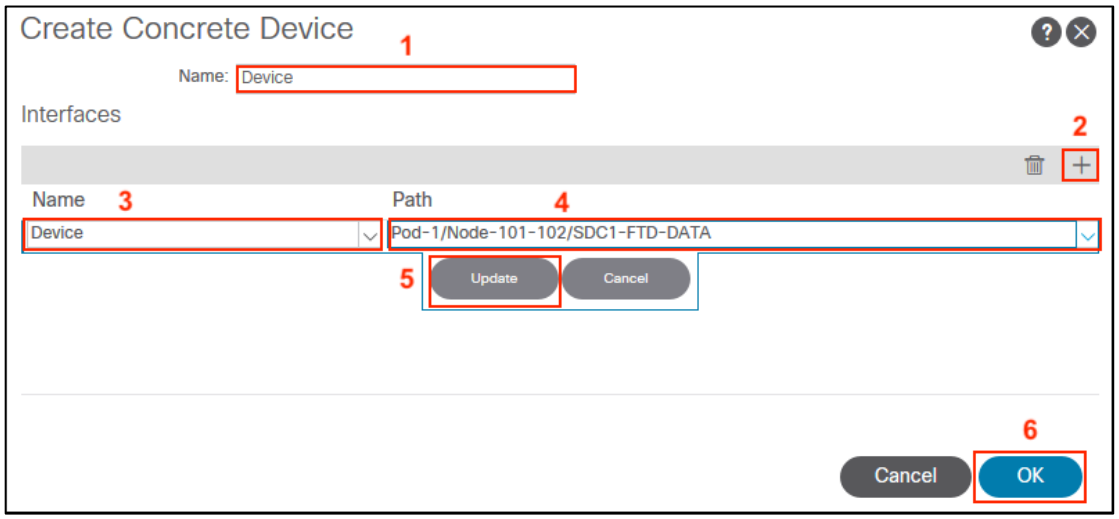


Return to Contents

b. Deploy a pair of clustered Firepower 9300 in Data Center 1 -San FranCisco. Uncheck the Managed box(1), fill in the device name (2), service type (3), device type (4) and physical domain (5). Select Context Aware Single (6) and Function Type GoTO (7). In the work pane, click the + sign (8) to create a Concrete Device.

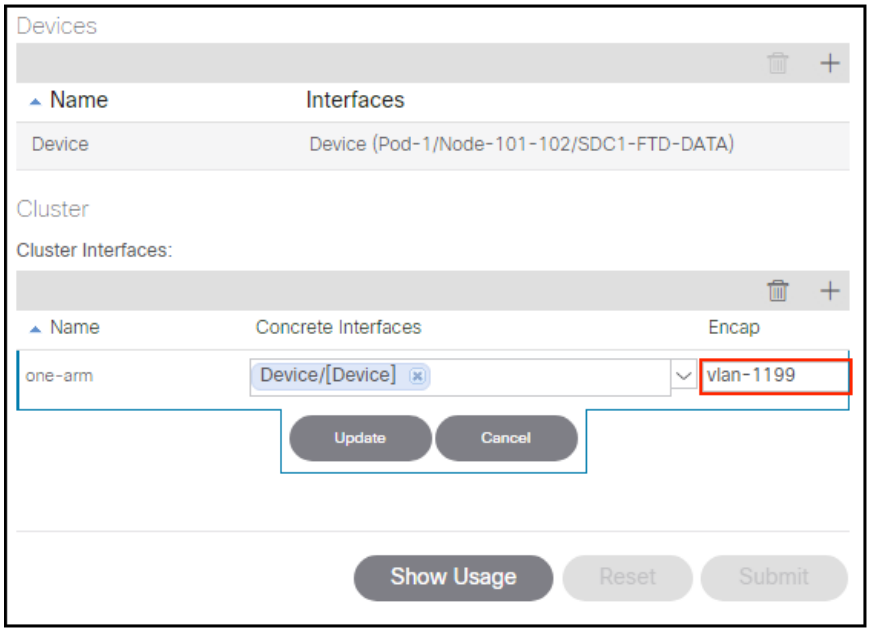


c. Deploy the Firepower cluster as a one-arm deployment, which is recommended since it simplifies the configuration. To create the concrete device, Enter the Name (2) and click the + sign (2). Enter the Name (3) and select the Path(4) from the drop-down menu, click Update (5) and OK (6).



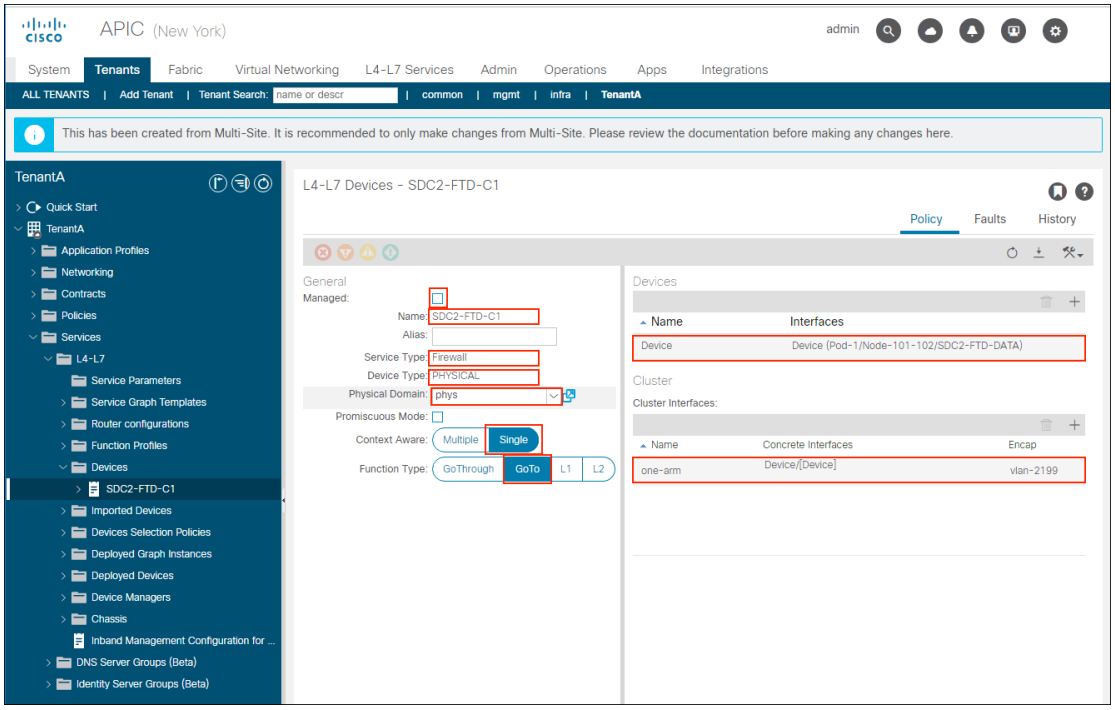
Return to Contents

d. We created a single clustered Interface named one-arm, used the device created in step c and added vlan-1199 as the Encap for the interface one-arm. In Appendix C, Step 8 there are details on how the virtual port channel SDC1-FTD-DATA was configured.



e. Repeat step a. through d. to configure the FTD Cluster one-arm interface in SDC2. Replace the names and paths to reflect the SDC2 environment.

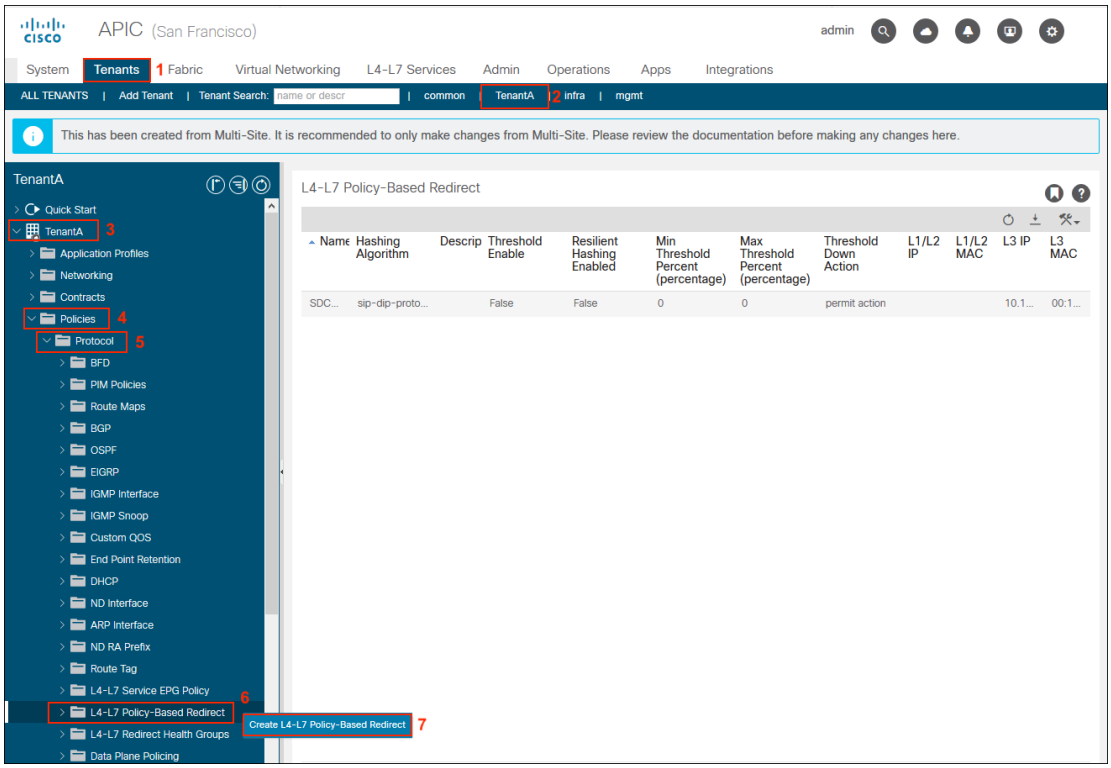
SDC2 FTD Cluster One-Arm configuration



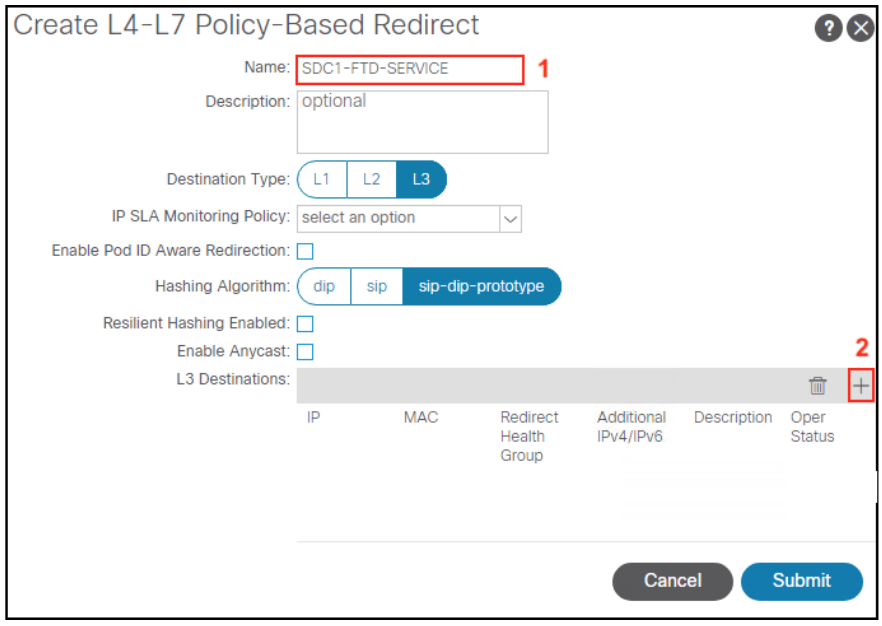
Return to Contents

Step 2: Create L4-L7 Policy Based Redirect policy

a. Create L4-L7 Policy Based Redirect (PBR) policy in the Tenant in each site. We implemented a single **FTD** bridge domain that we stretched across both sites, since it simplifies configuration. It could also be implemented in dedicated service bridge domain in each site. Navigate to **Tenant(1)->TenantA(2)-> TenantA(3)->Policies(4)->Protocol(5)->L4-L7 Policy-Based Redirect(6)**, Right-Click and select **Create L4-L7 Policy-Based Redirect(7)**.



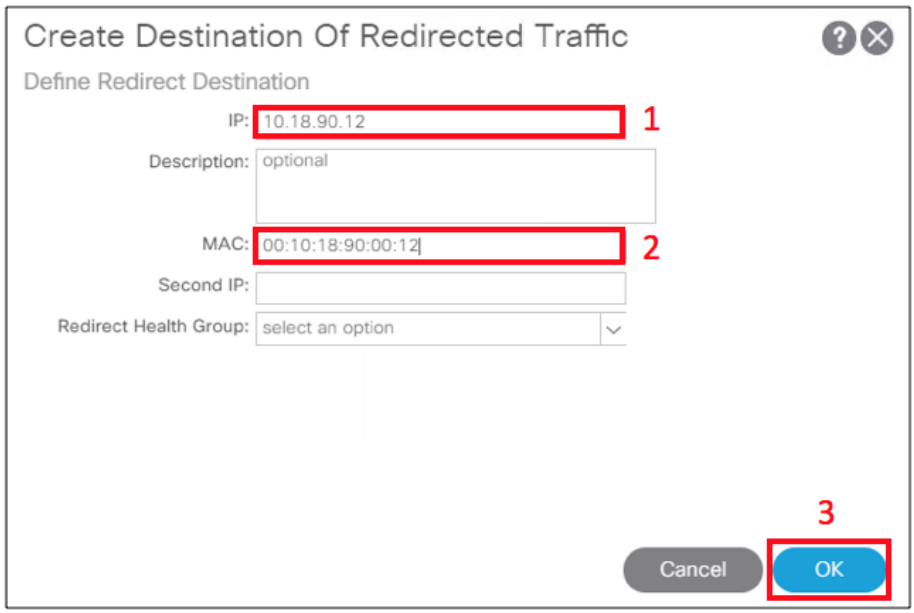
b. Create L4-L7 Policy Based Redirect policy called **SDC1-FTD-Service** (1) and add **Destination policy** (2).



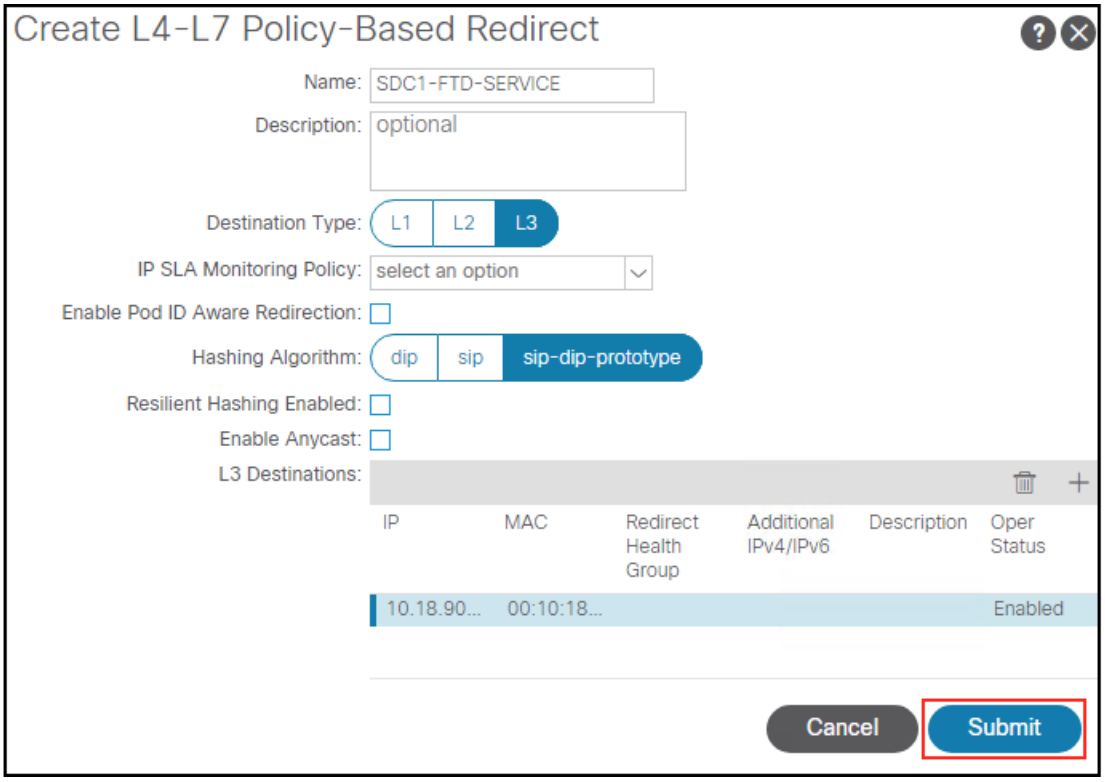
Return to Contents

c. Create Destination policy for San FranCisco. **Set the IP address of the Firepower 9300 cluster (1), enter the MAC address (2) and select OK (3).** The MAC address is a translation from IP address to MAC. Note the corresponding MAC address in Firepower Management Center for this cluster interface must be the same. Refer to Appendix C, Step 5w for the FMC cluster interface policy.

d. Create Designation policy for New York**. Set the IP address of the Firepower 4110 cluster (1), enter the MAC address (2) and select OK (3).** Note the corresponding MAC address in Firepower Management Center for this cluster interface must be the same. Refer to Appendix C, Step 5x for the FMC cluster interface policy.



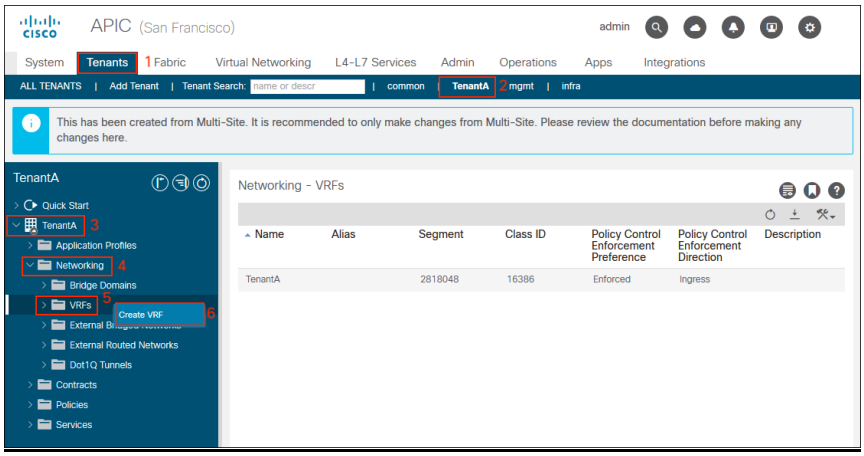
e.
Submit L4-L7 Policy Based Redirect policy **SDC1-FTD-SERVICE**.



Step 3: Create initial L3Out policy in APIC GUI

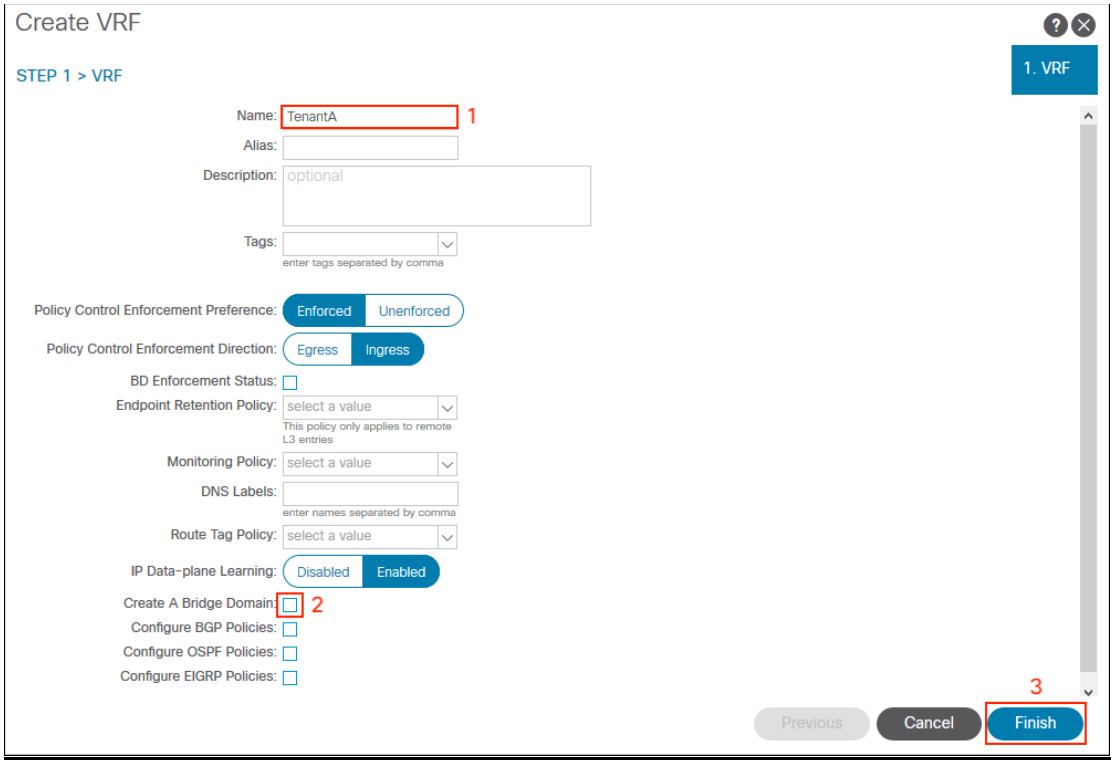
a. Create the initial L3Out policy in the Tenant in each site. MSO will complete the policy by adding the external EPG details under the Networks folder of the Tenant L3Out policy. Cisco APIC Layer 3 Networking Configuration Guide: Configuring a Layer 3 Outside for Tenant Networks Using the GUI, https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/L3_config/b_Cisco_APIC_Layer_3_Configuration_Guide/b_Cisco_APIC_Layer_3_Configuration_Guide_chapter_011.html#task_CA462A15DDFE4A85A1382D5F6589CB59. We created the VRF under the tenant and followed Step 4 in the guide.

To create the VRF, navigate to **Tenant (1)->><tenant-name> (2)->><tenant-name> (3)->Networking (4)->VRF (5),** right-click and select **Create VRF (6).**

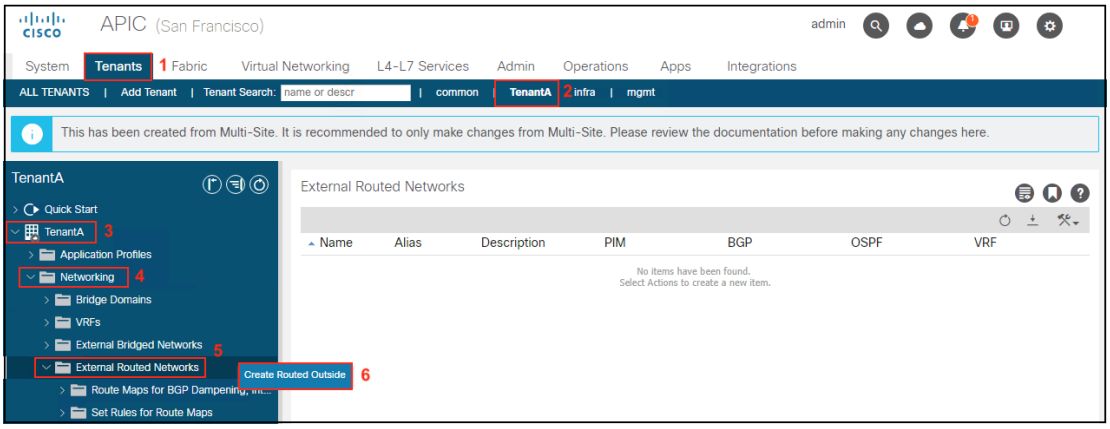


Return to Contents

b. Enter the **Name TenantA(1)**, uncheck the **Create a Bridge Domain(2)** and click **FINISH(3).**

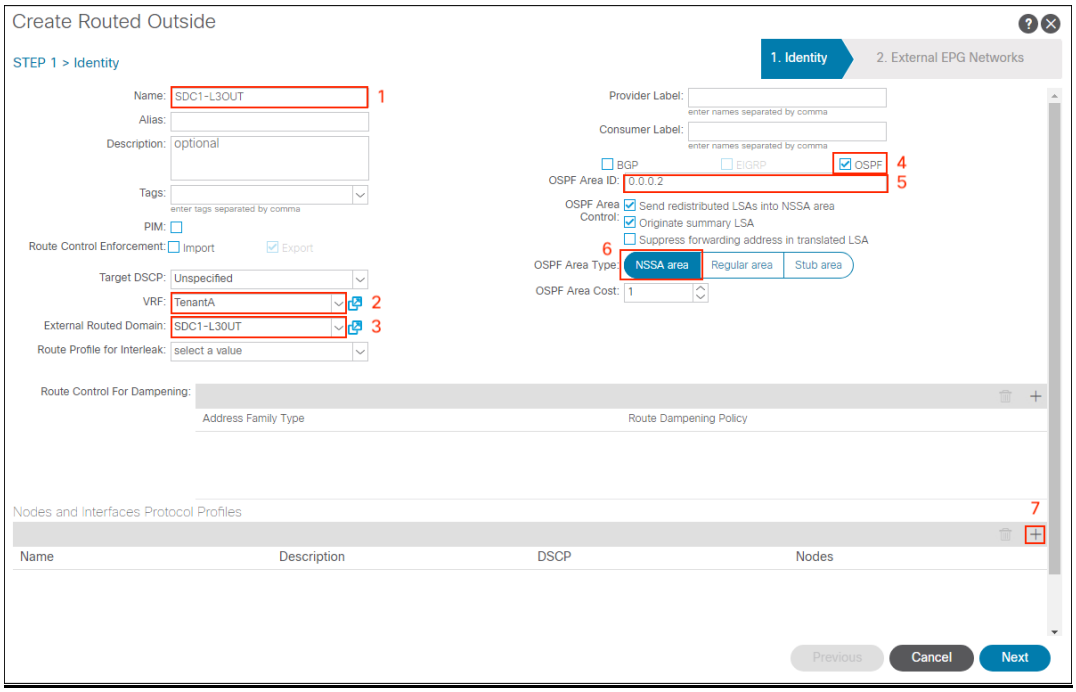


c. Next, create the L3Out. Navigate to **Tenant (1)->TenantA (2)->TenantA (3)->Networking (4)->External Routed Networks (5),** right-click and select **Create Routed Outside (6).**

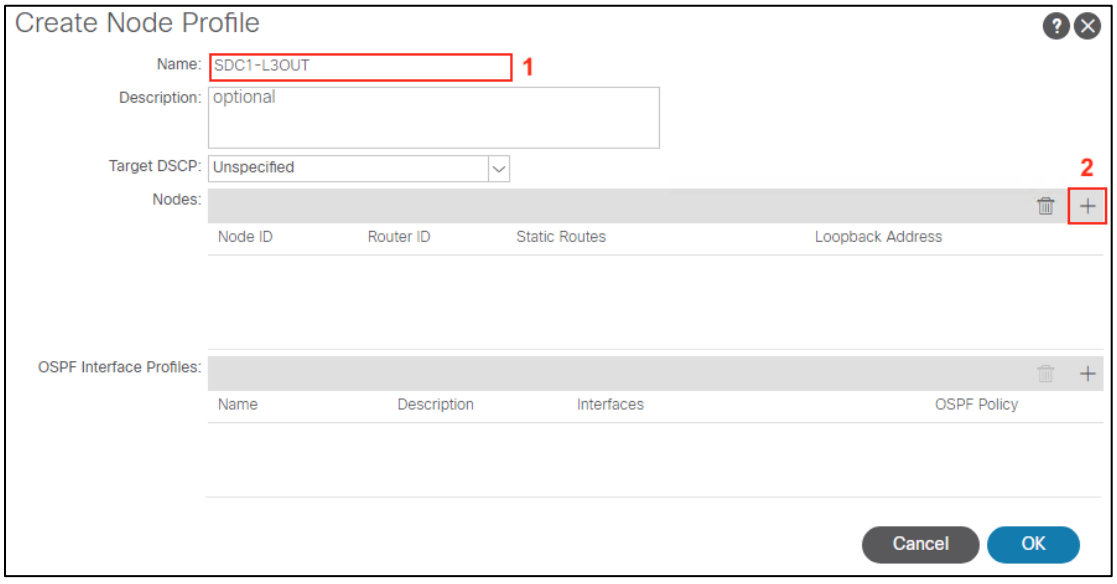


Return to Contents

d. Enter the **Name (1)**, select VRF Default from the drop-down menu, select External Routed Domain SDC1-L3OUT (3), check the **OSPF box (4), enter the OSPF area 0.0.0.2 (5)** and select OSPF Area Type NSSA area (6). Click the + Sign to configure the Nodes and Interfaces Protocol Profiles (7).

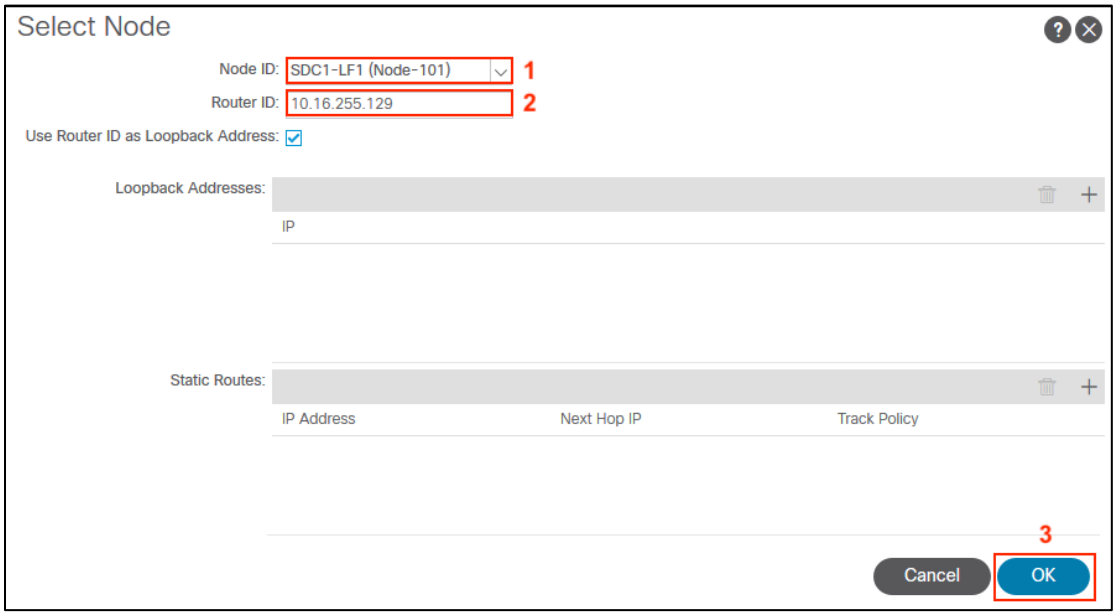


e. Create Node Profile policy for the L3Out in Data Center 1. Enter the **Name (1)** and click the **+ sign (2)**.

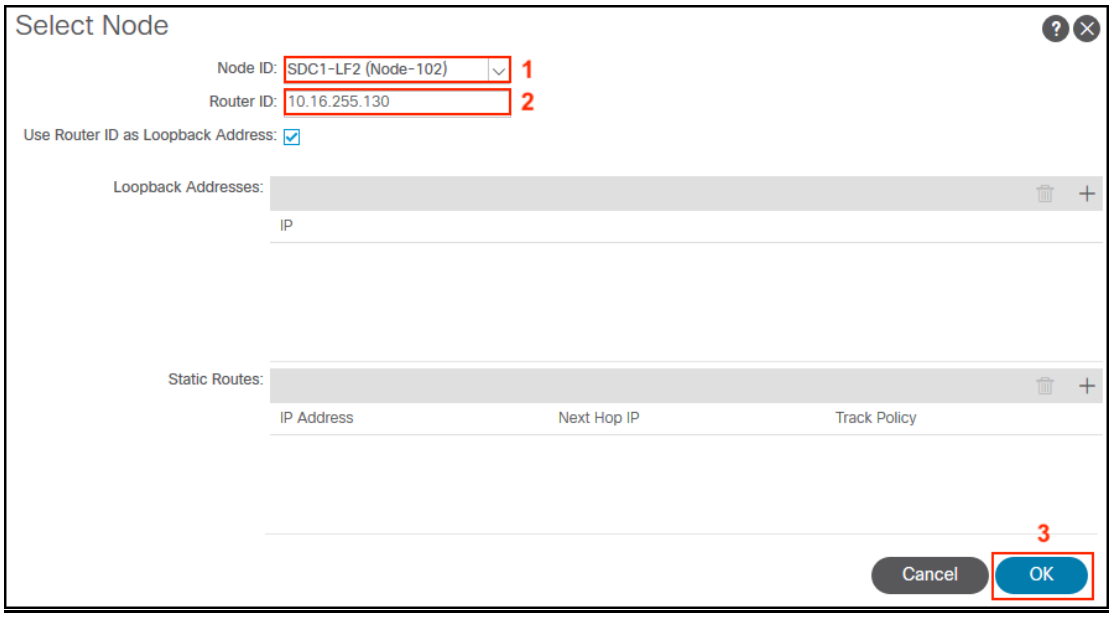


Return to Contents

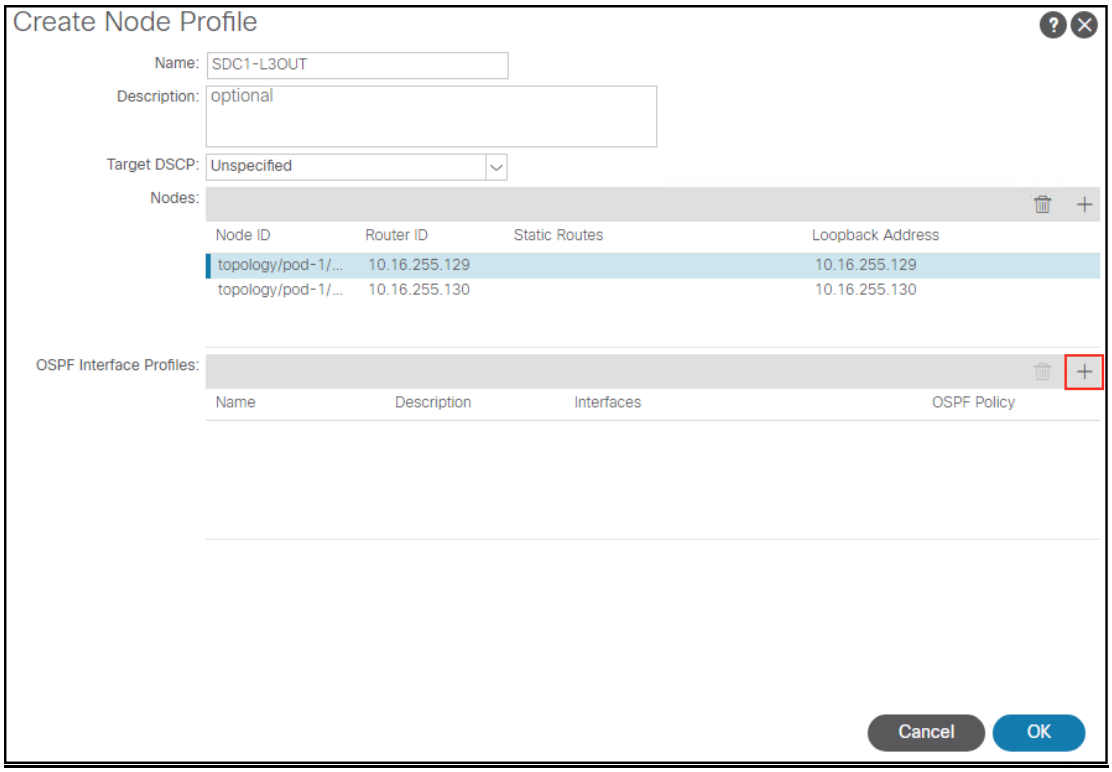
f. Select the **Node ID SDC1-LF1(1)** and enter the **Router ID 10.16.255.129 (2)** and click **OK (3).**



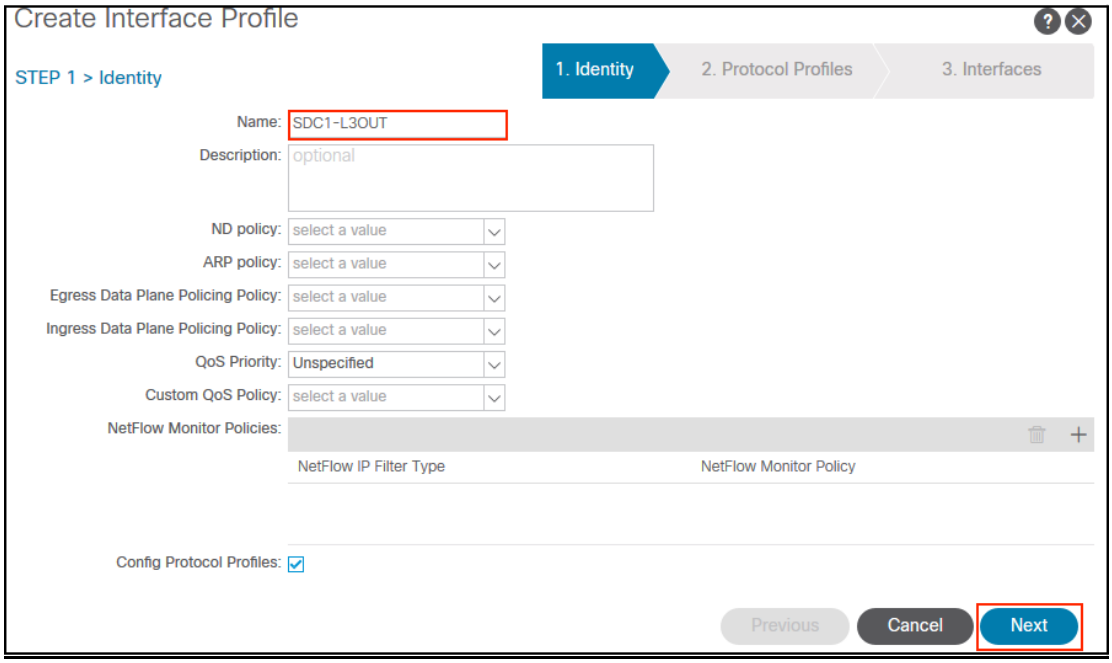
g. Repeat step d. to create the second node.



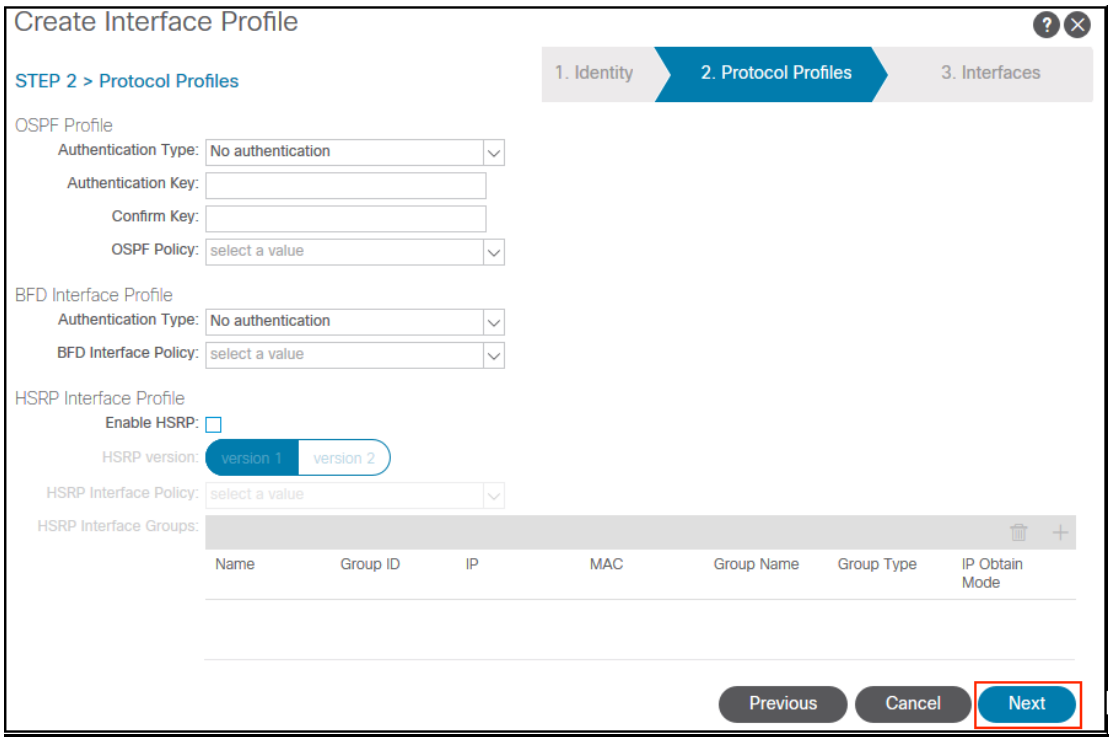
h. Back in the Node Profile, click the **+ sign** in the OSPF Interface Profiles section.



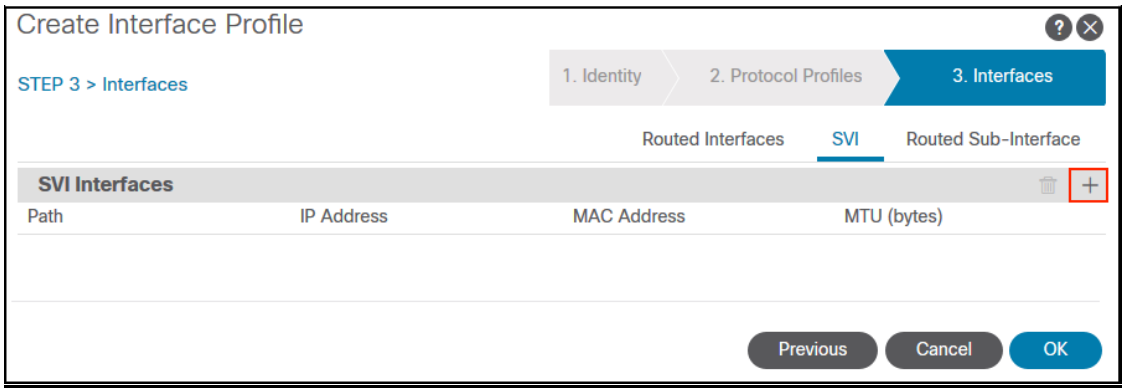
i. In Step 1 Enter the **Name** and click **Next.**



j. In Step 2, click **Next.**

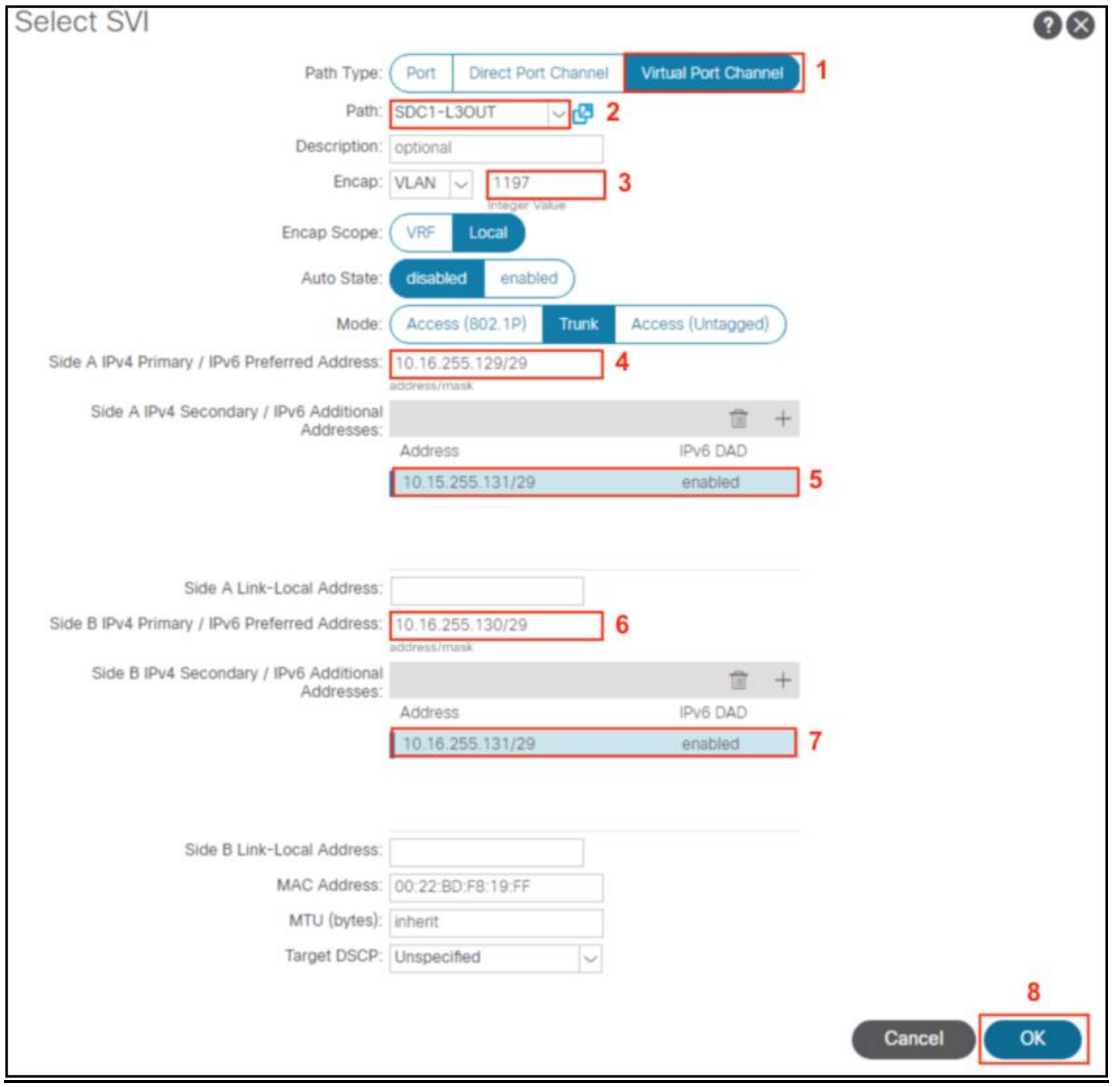


k. In Step 3, select **SVI** and click the **+ sign**.



108

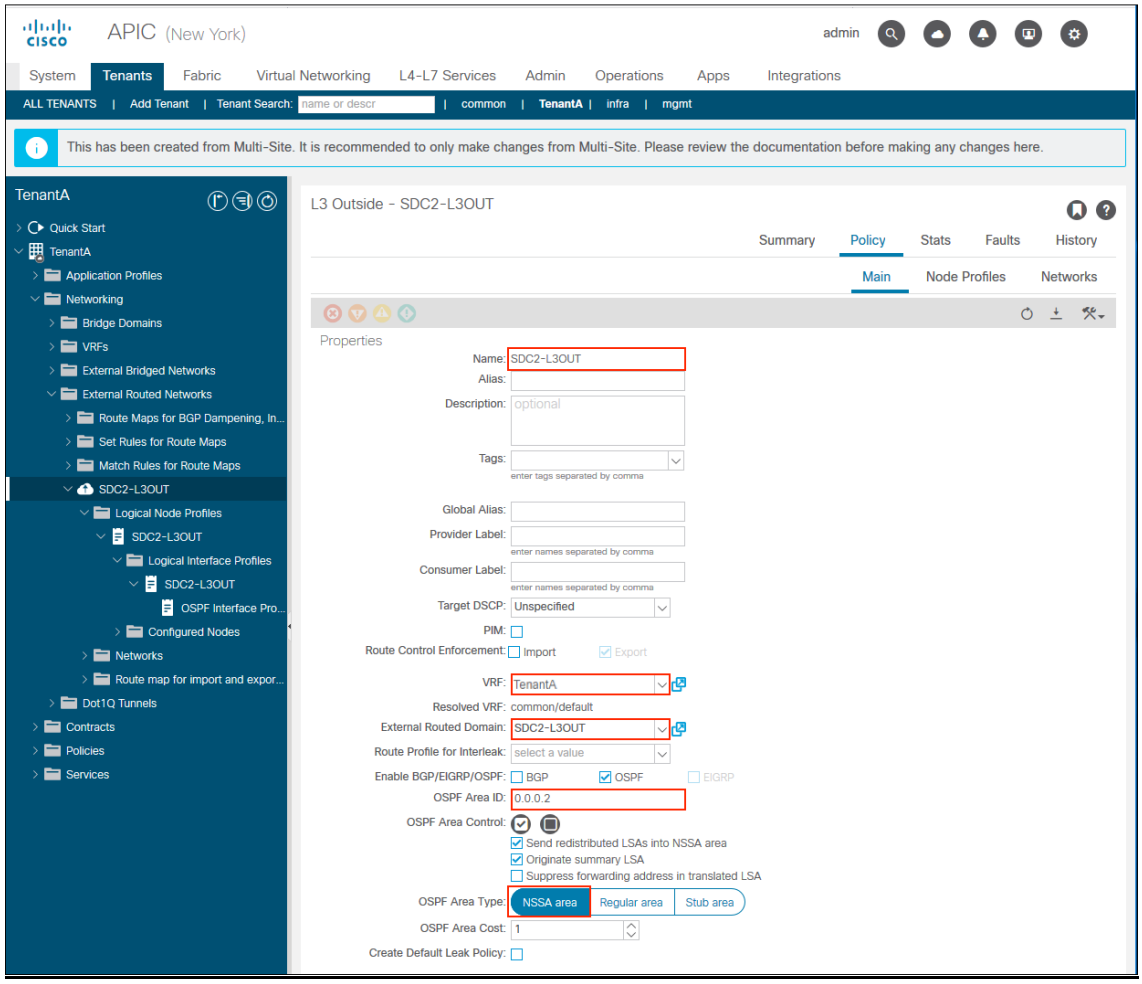
l. Select Virtual Port Channel (1), select SDC1-L3OUT (2), enter 1197 (3) for the VLAN encap. The side A Primary IP is 10.16.255.129/29 (4) and the secondary is 10.16.255.131/29 (5). The side B Primary IP is 10.16.255.130/29 (6) and shares the secondary of 10.16.255.131/29 (7) with side A. Click OK (8).



Return to Contents

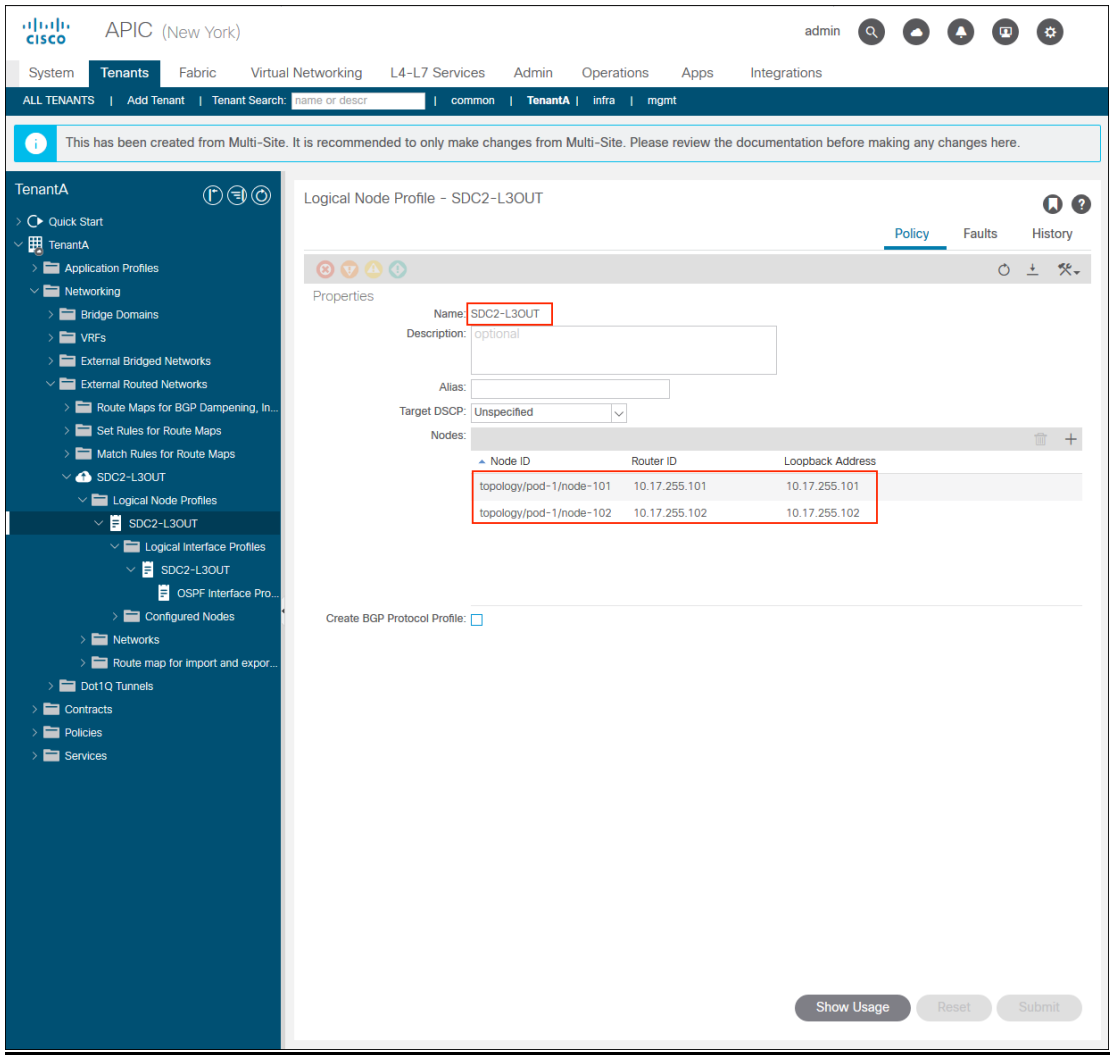
m. Repeat steps a through l to configure the SDC2-L3OUT. Refer to screenshots below details.

SDC2-L3OUT configuration



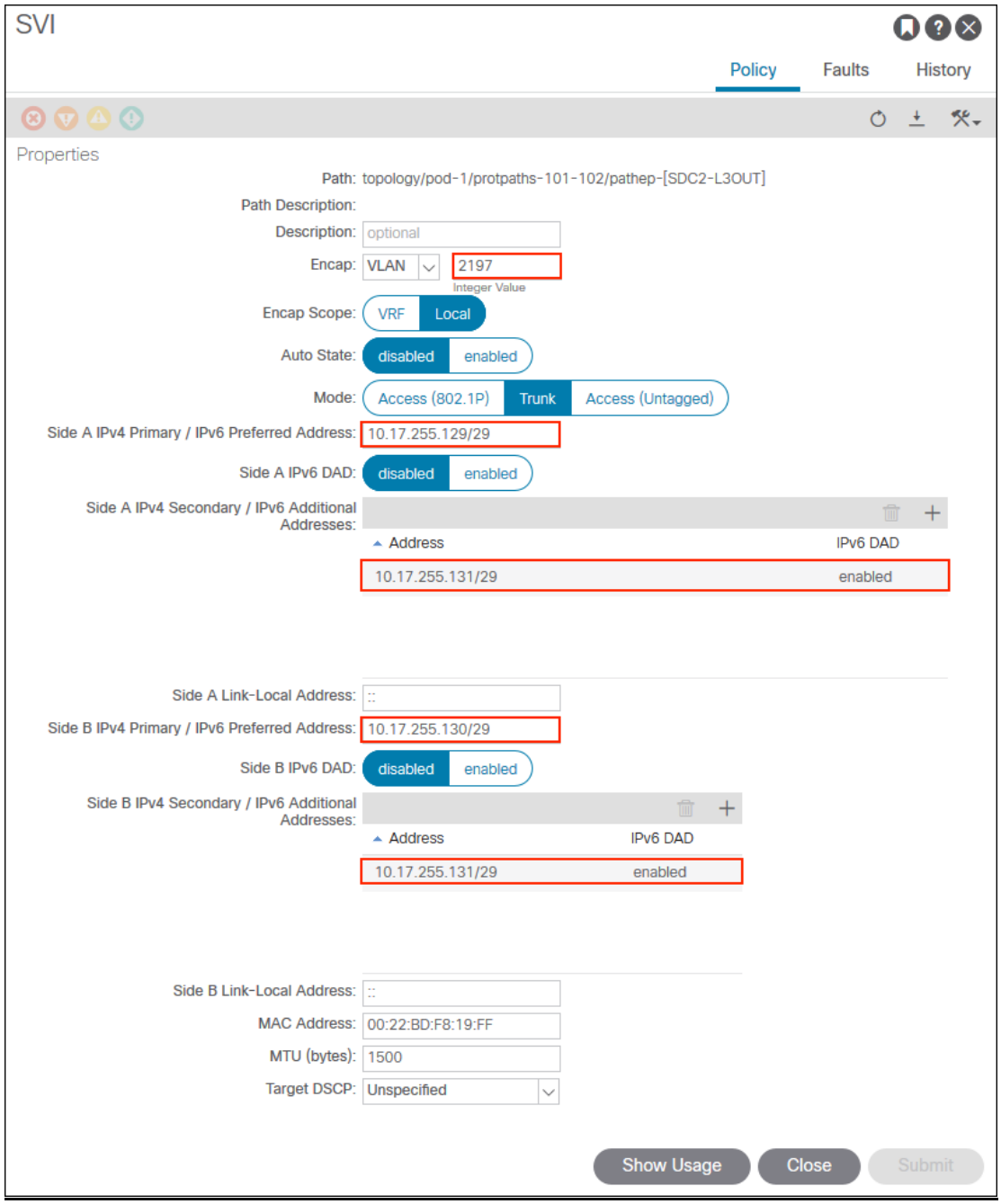
Return to Contents

SDC2-L3OUT Node Profile



Return to Contents

SDC2-L3OUT SVI configuration

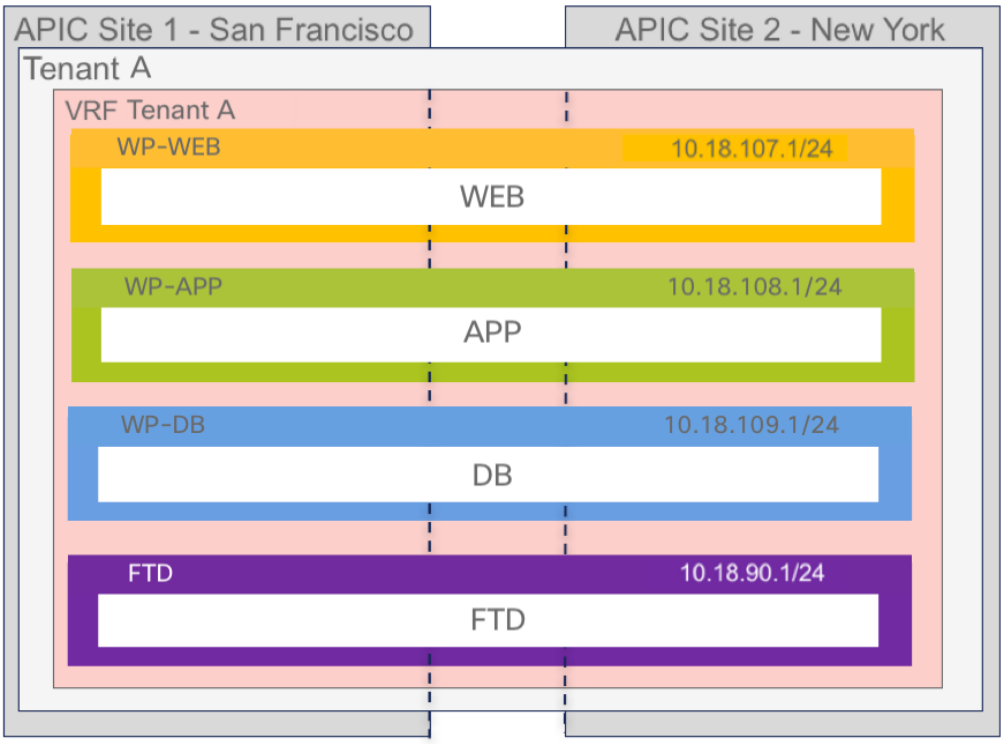


Return to Contents

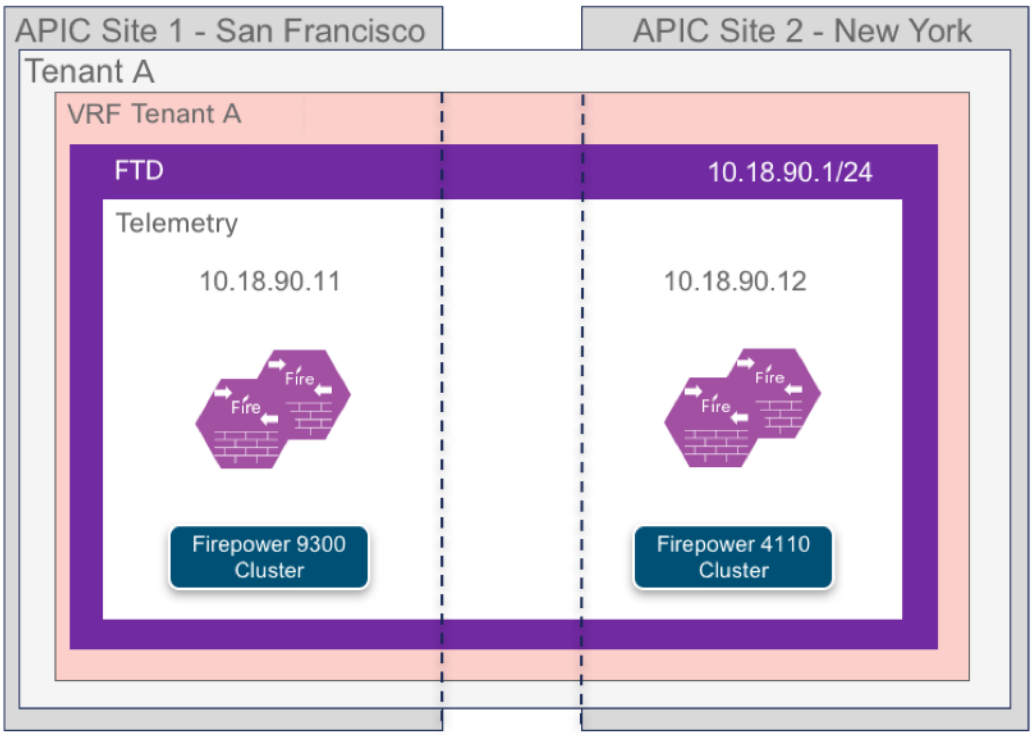
Step D: Add Schema with Multi-Site Orchestrator GUI

Once the Tenant is deployed the next step is to deploy the schema. There are many schema options, but we are focused on the most popular or likely deployment scenario. A common schema is a to stretch a bridge domain across sites for high availability. We used the Firepower cluster in each data center in a One-Arm Policy Based Redirect Design with multiple Inter-Site Contracts for a 3-tier application deployment of Wordpress. There is a single tenant named “Tenant A” which is stretched across both sites. The VRF SDC-VRF is stretched across both sites within the tenant “Tenant A”. The first three bridge domains and corresponding EPGs are a network centric view of how we have the servers are deployed. The last bridge domain FTD and FTD EPG are specific to the FTD cluster deployment in each data center. We chose a single bridge domain for FTD because it made the MSO configuration simpler. It could be implemented as an FTD bridge domain in each site. The policy based redirect policy in each site will redirect to the local FTD cluster for threat defense services.

Multi-Site Schema for Stretched Bridge Domain across multiple sites

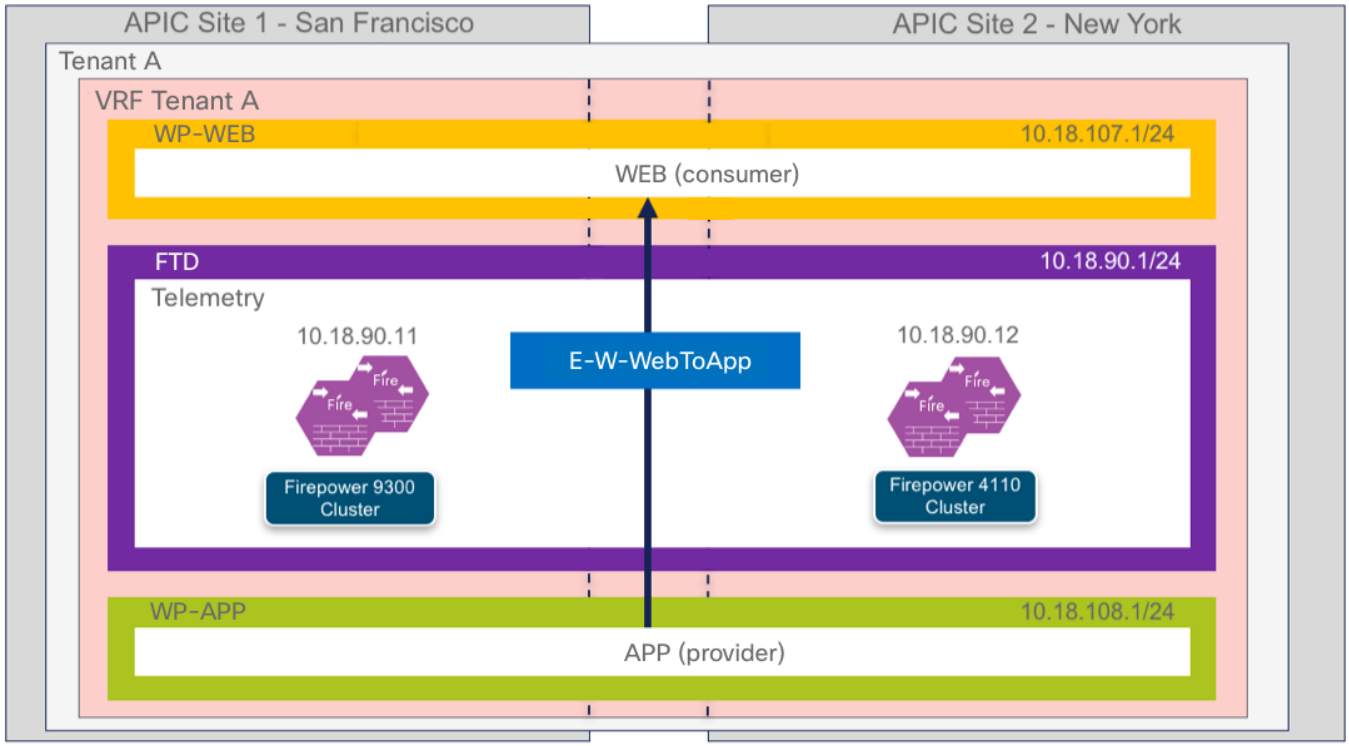


FTD L4-L7 Service Insertion in Stretched Bridge Domain deployment



The contract determines where traffic is allowed to go and if there is an L4-L7 service graph attached to it. In the figure below it shows an example inter-site contract called E-W-WebToApp, which specifies that the one-arm service graph for FTD will be attached to it.

Stretched Bridge Domain with Inter-Site Contract Example



Return to Contents

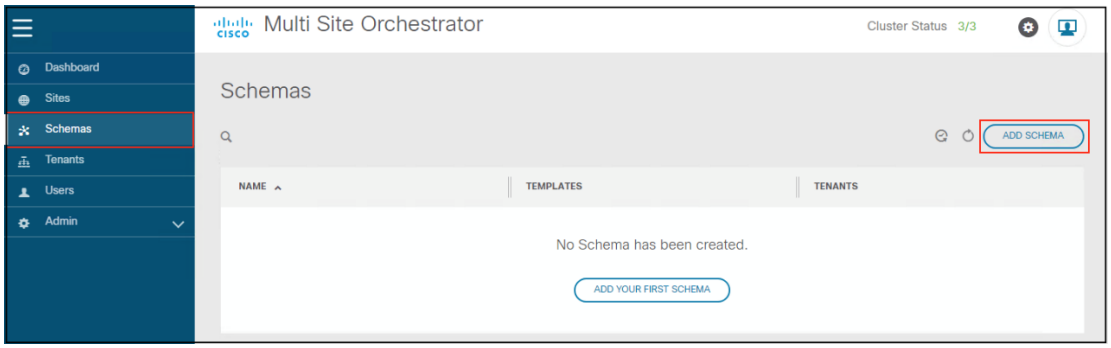
Section Summary:

The intent in selecting these steps was to minimize the number GUI clicks in deploying a service graph for a one-arm Firepower Threat Defense cluster.

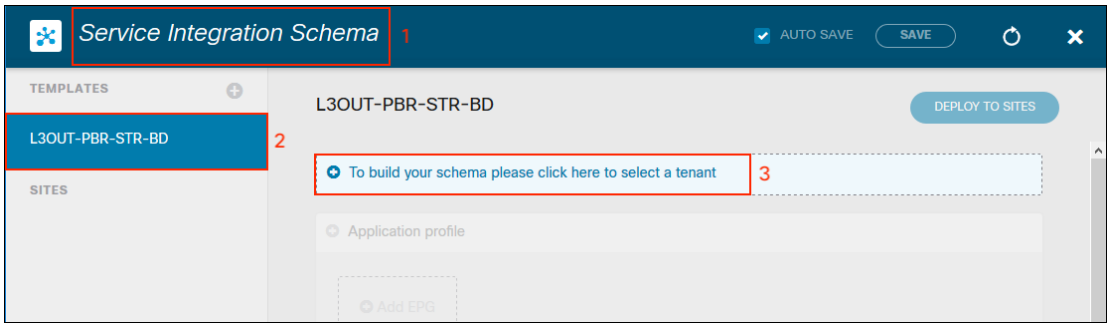
Step 1: Create schema
Step 2: Add Sites
Step 3: Import VRF
Step 4: Create Service Graph
Step 5: Create External EPG
Step 6: Create Filters
Step 7: Create Bridge Domains
Step 8: Create Contracts
Step 9: Create Application Profile
Step 10: Add contracts to External EPG

Step 1: Create Schema

a. To create a schema, in the MSO home screen, navigate to **Schemas** in left pane, and then select **ADD Schema** on the right.

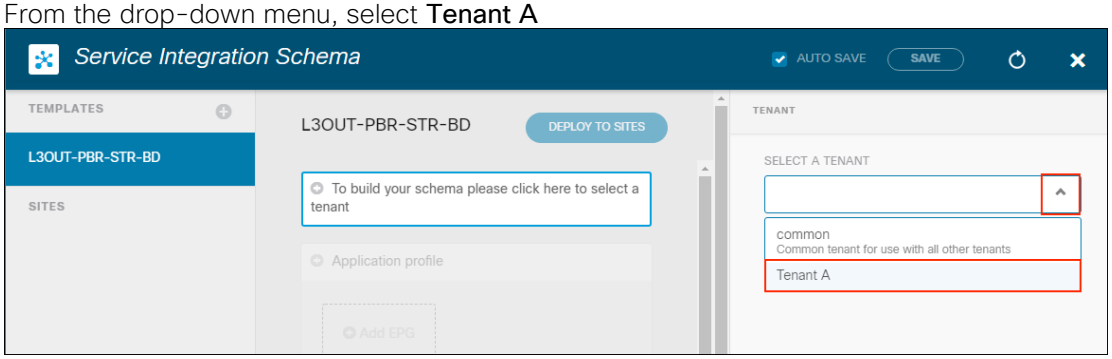


b. Change the schema name to **Service Integration Schema(1)**, change the template name to **L3OUT-PBR-STR-BD(2)** and click **To build your schema please click here to select a tenant**.



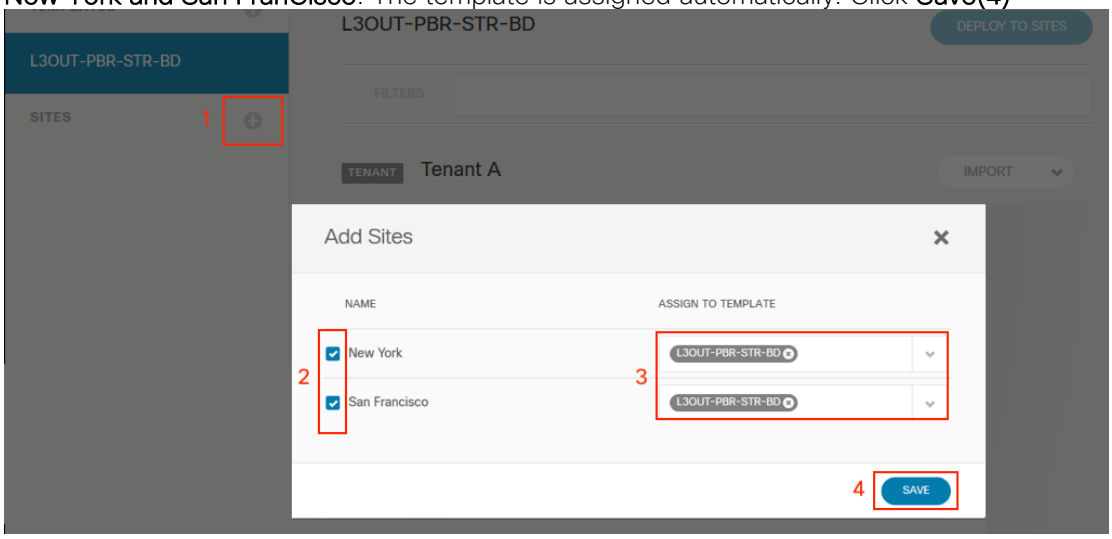
Return to Contents

c. From the drop-down menu, select **Tenant A**



Step 2: Add Sites

a. Add sites to the schema. Click the **+ sign(1) next to SITES** and click the **check boxes(2) for New York and San FranCisco**. The template is assigned automatically. Click **Save(4)**



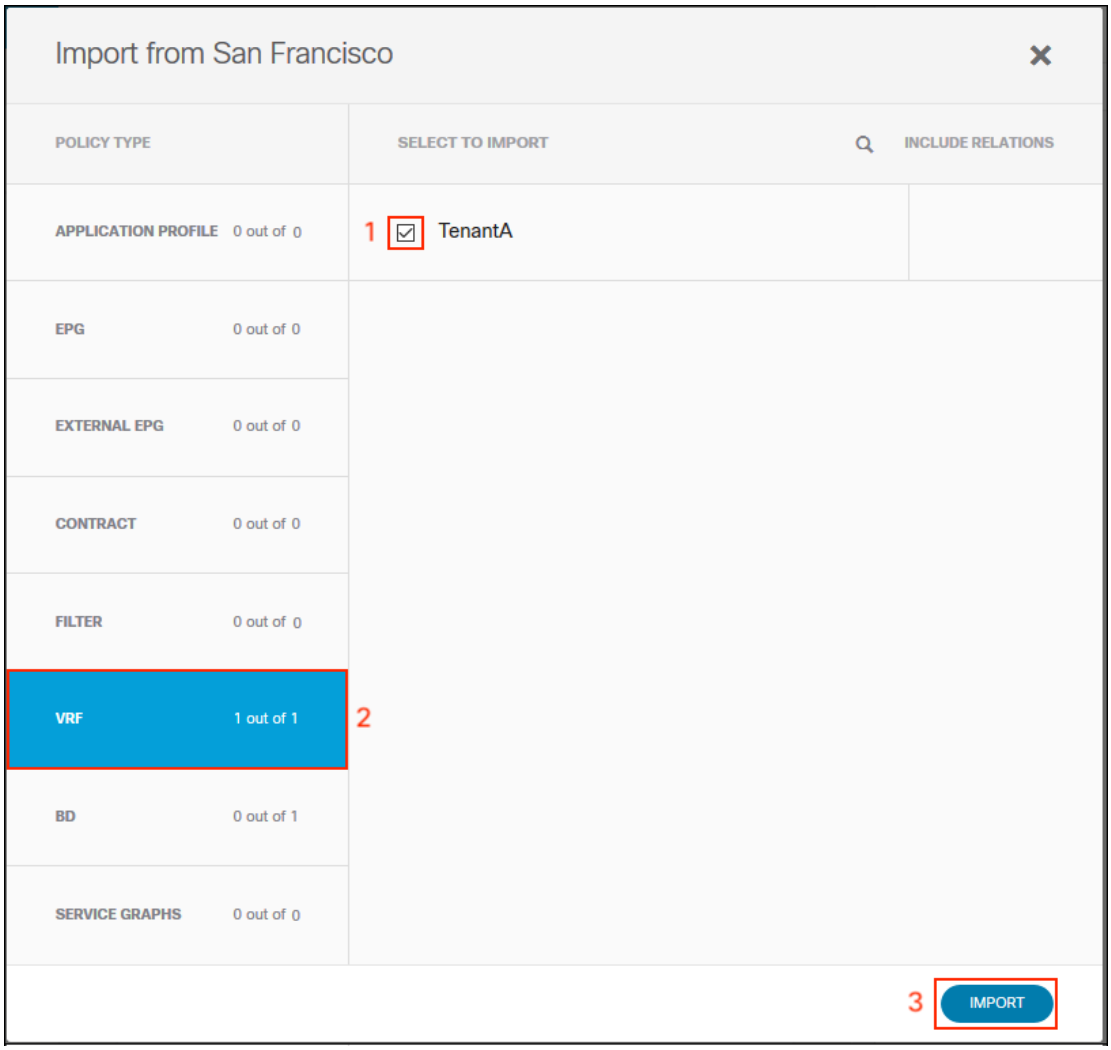
Step 3: Import VRF

In this step, a brown field deployment is assumed. We created the VRF in APIC previously. It is possible in a green field deployment to create the VRF in Multi-Site Orchestrator (MSO). Also shown in this step is that other policy (i.e. Application Profile, EPG, Contract, etc.) can also be imported from APIC into MSO.

a. To import the VRF, click **IMPORT (1)** and select **San FranCisco (2)**. The VRF is identical in both datacenters, so importing from New York is not required.

Return to Contents

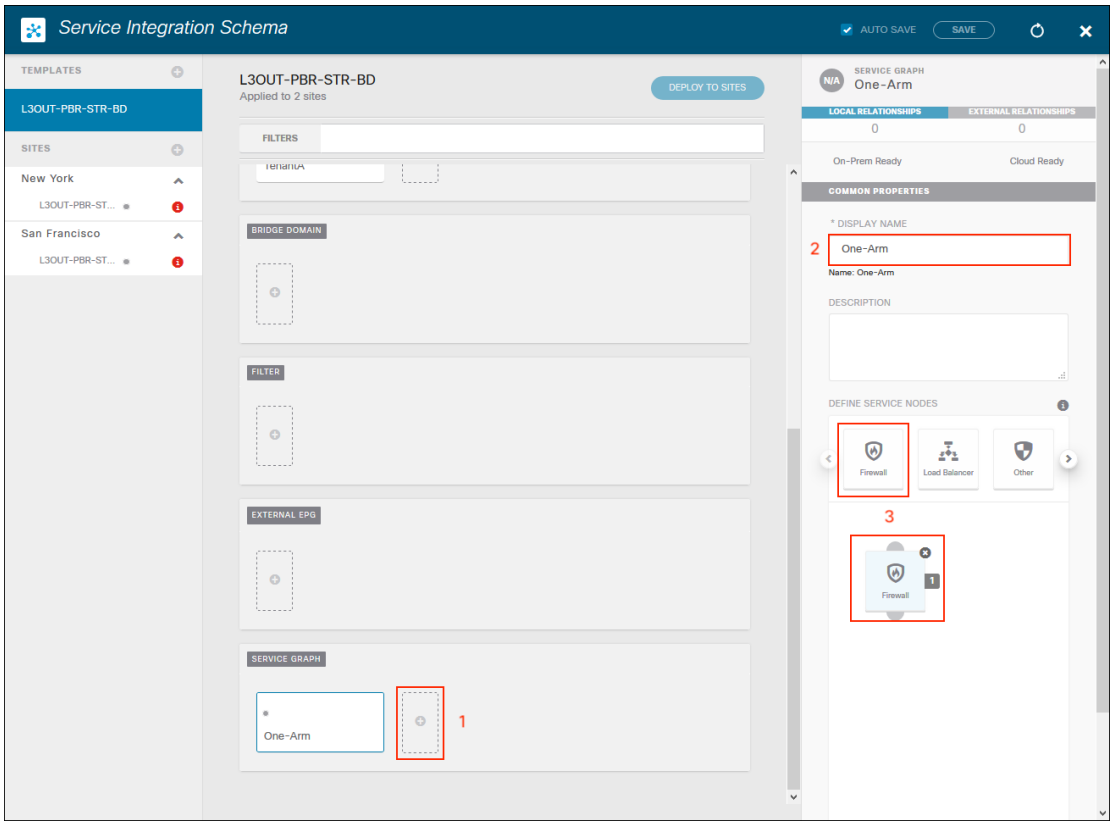
b. Select TenantA (1), select VRF (2) and click IMPORT (3).



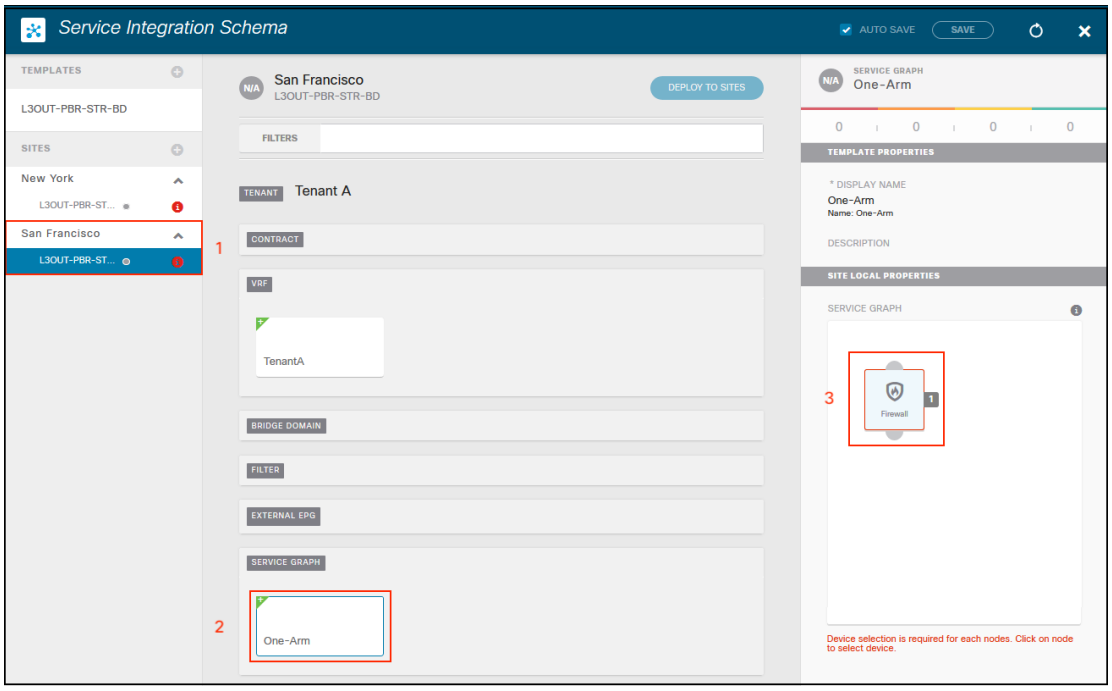
Return to Contents

Step 4: Create Service Graph

a. To Create the Service Graph, click the **+ sign (1)** in the SERVICE GRAPH section. Enter the **DISPLAY NAME One-Arm (2)** and **drag-and-drop the firewall (3)** into the window below.

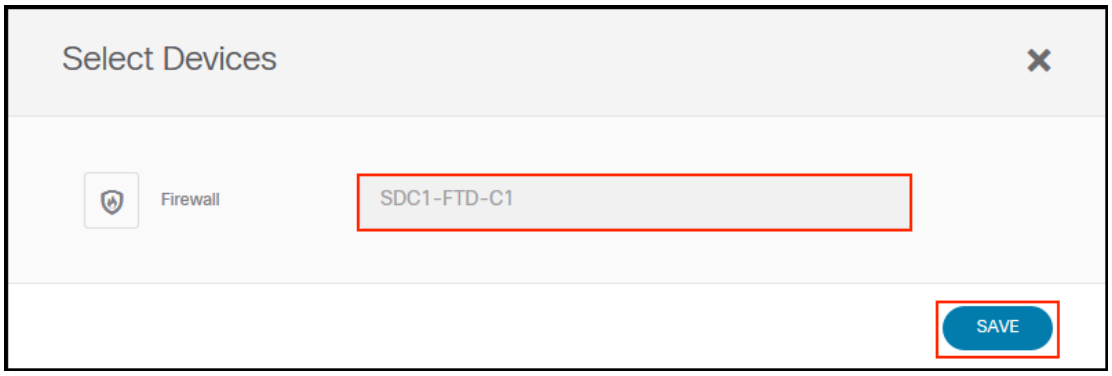


b. To associate the template node to the site device, select **San FranCisco (1),** click on the **One-Arm (2)** and click on the **firewall (3)**.



Return to Contents

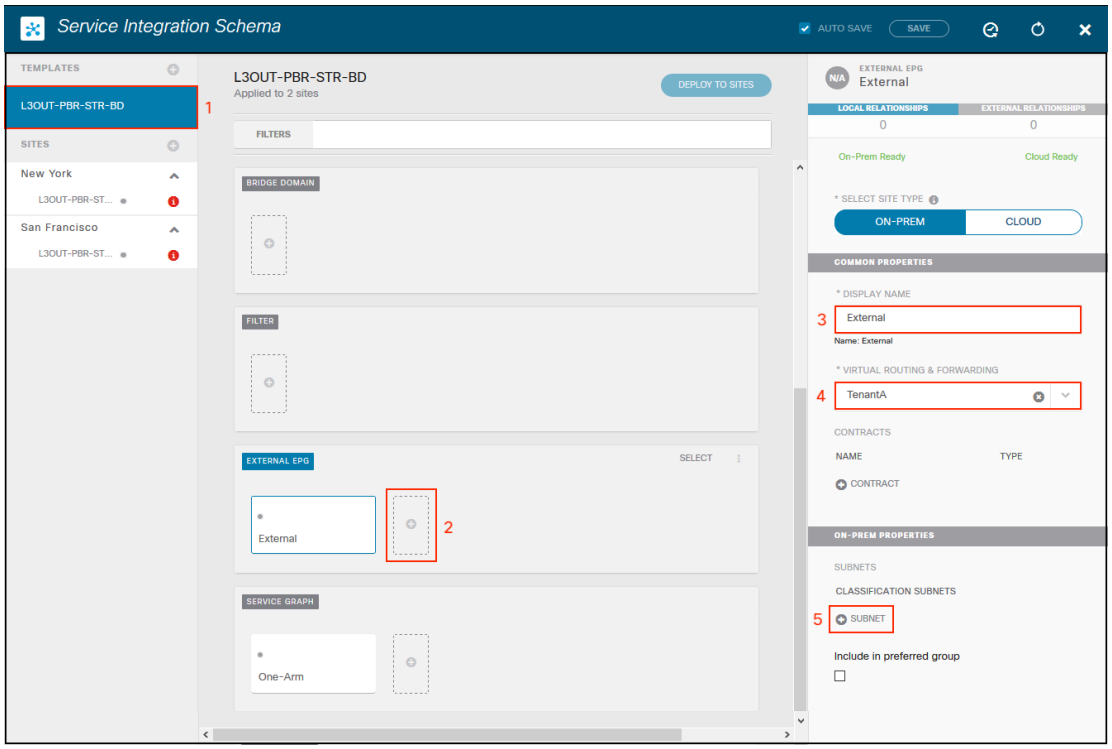
c. From the drop-down menu, select the SDC1-FTD-C1 firewall and click SAVE



d. Repeat steps b. and c. for the New York site.

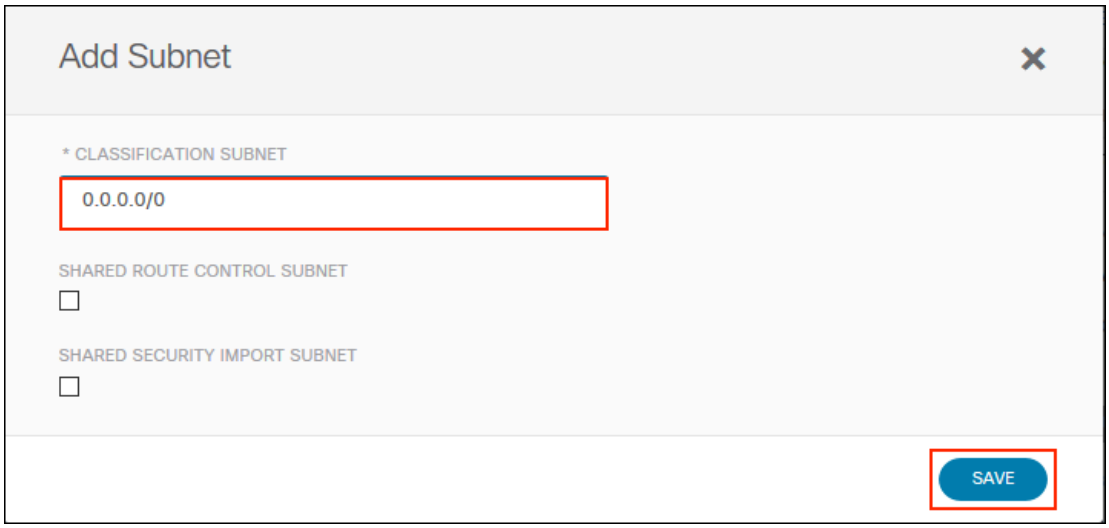
Step 5: Create External EPG

a. To create the External EPG, select the template L3OUT-PBR-STR-BD (1) and click the + sign (2) in the EXTERNAL EPG section. On the right, enter the Display Name External (3), select TenantA (4) under Virtual Routing and Forwarding. Click the + sign (5) to add a subnet.

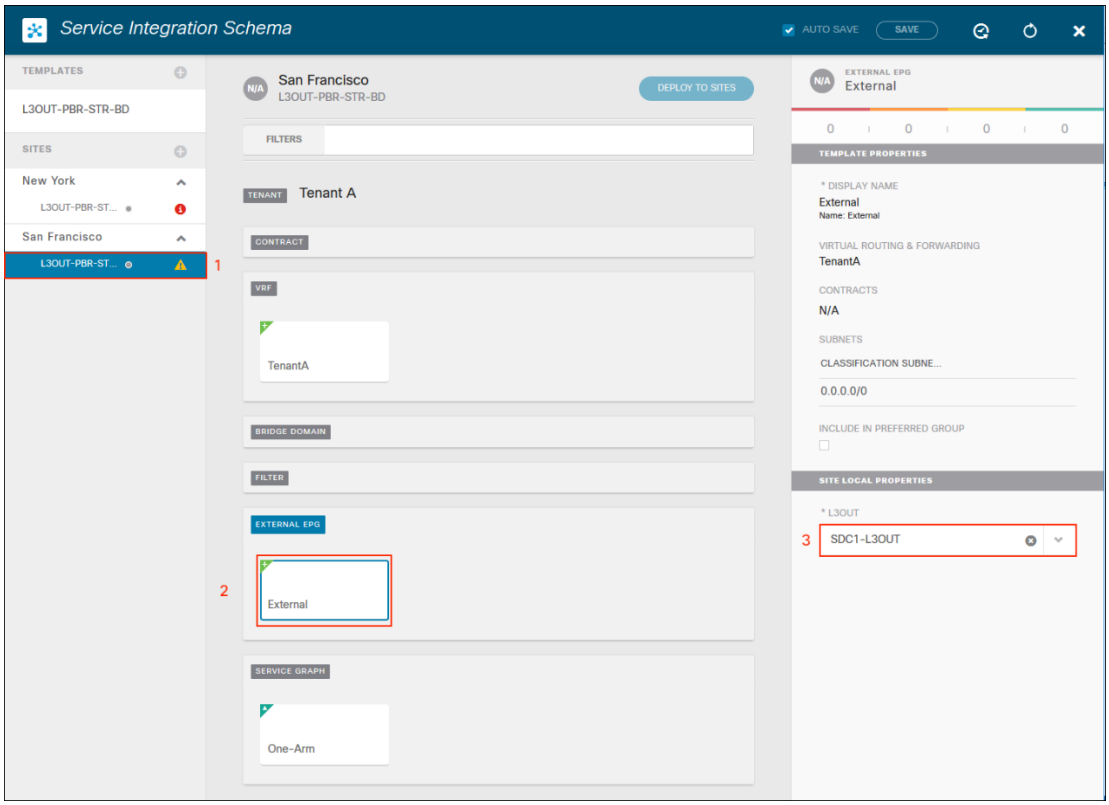


Return to Contents

b. Add the subnet **0.0.0.0/0** and click **SAVE**.



c. Associate the site L3OUT to the External EPG. Select **San FranCisco (1)** and click the **External EPG**. On the right, select the **SDC1-L3OUT (3)** from the drop down-menu.

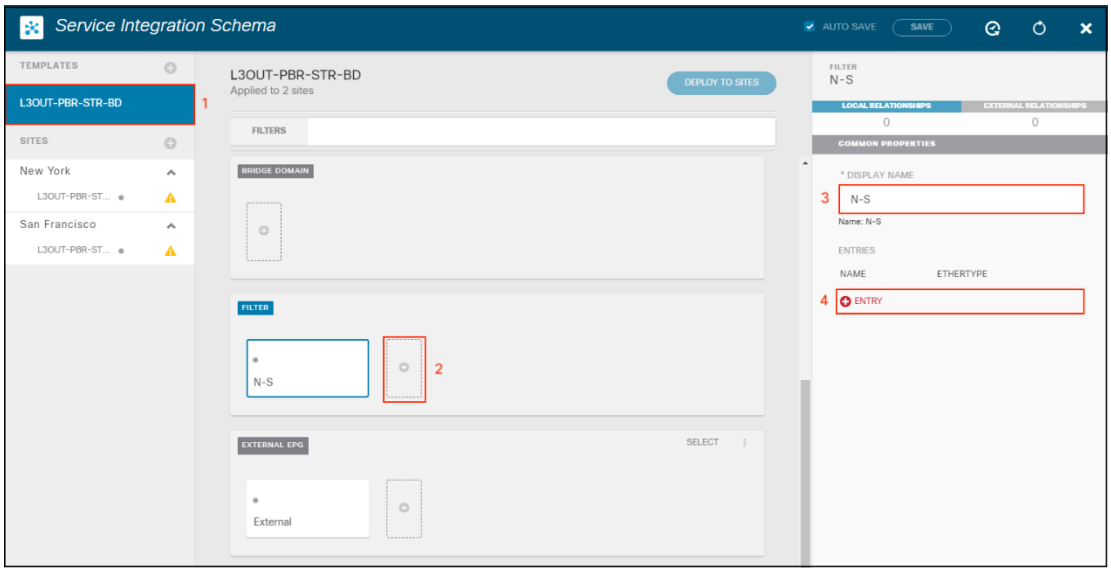


d. Repeat step c. for the New York site

Return to Contents

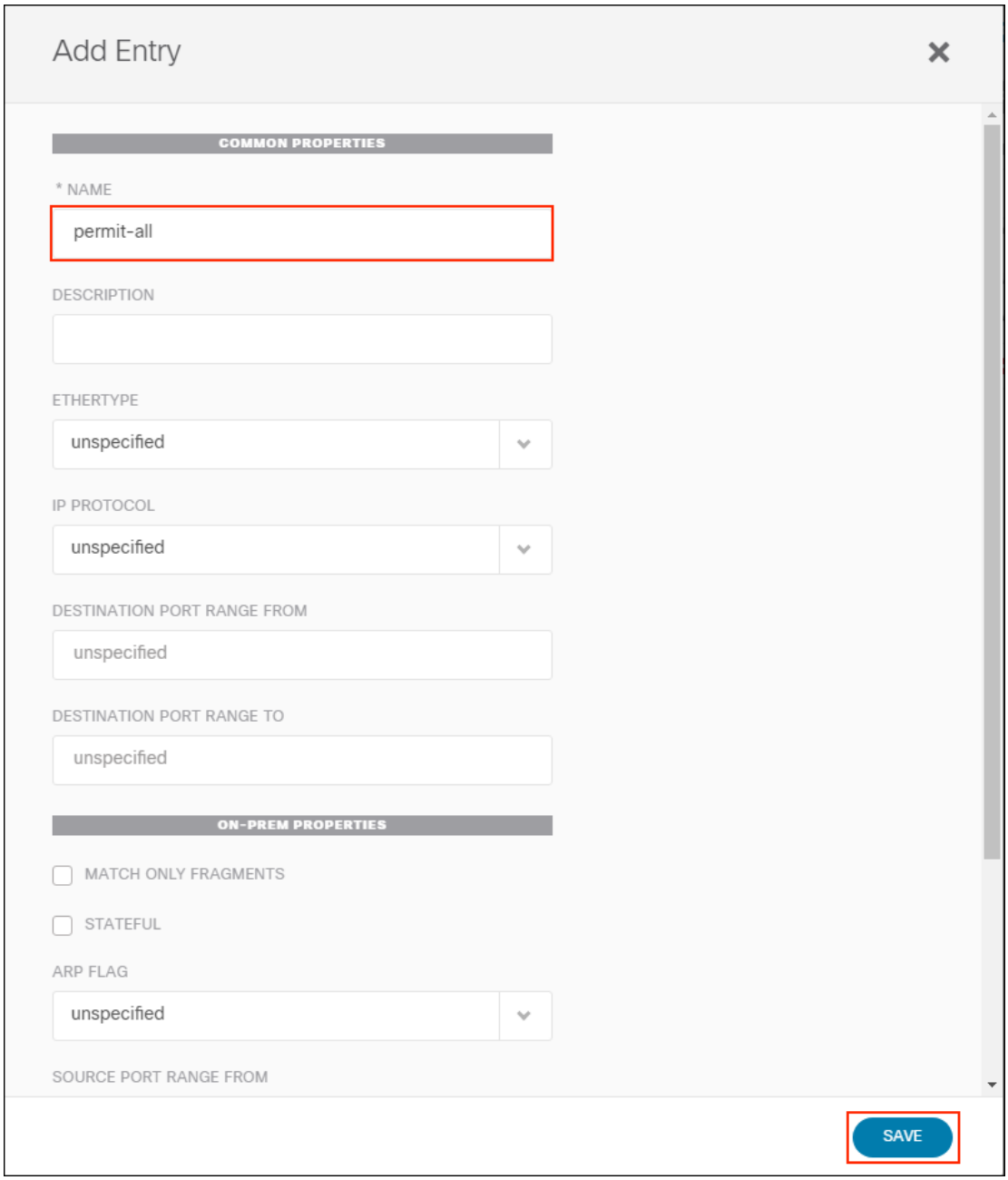
Step 6: Create Filters

a. Select the **L3OUT-PBR-STR-BD (1)** template and click the **+ sign (2). Enter N-S** for the **Display Name (3)** and click the **+ sign (4)** next to **ENTRY.**



Return to Contents

b. Enter **permit-all** in the name field and click **SAVE**.

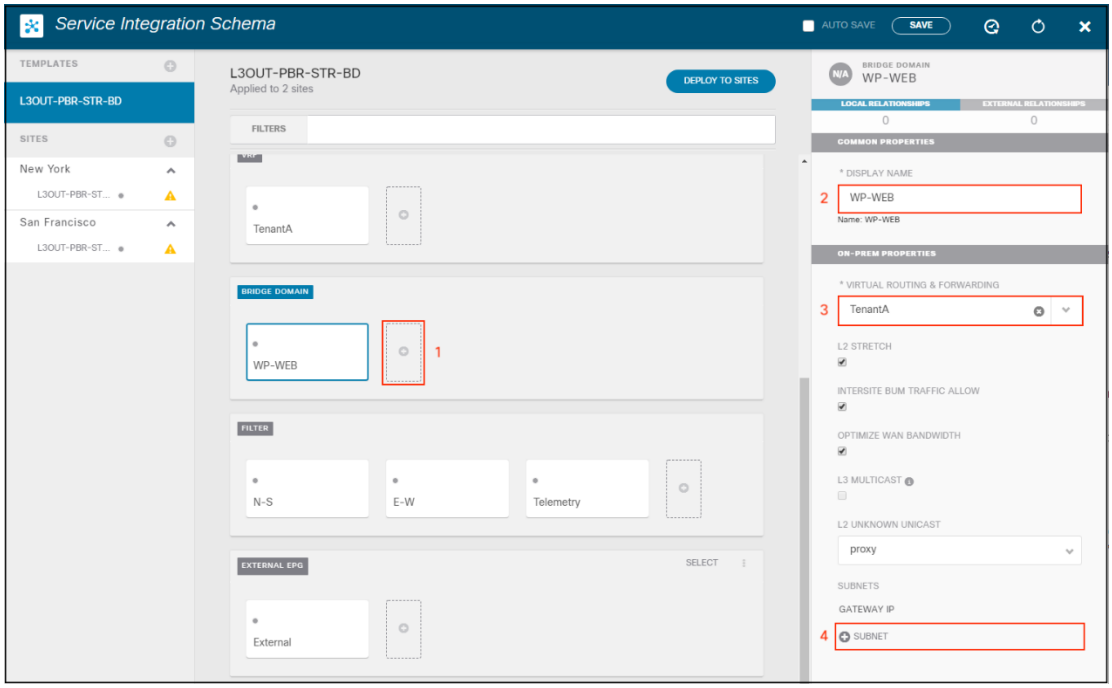


c. Repeat steps a. and b. to create the filters **E-W** and **Telemetry.**

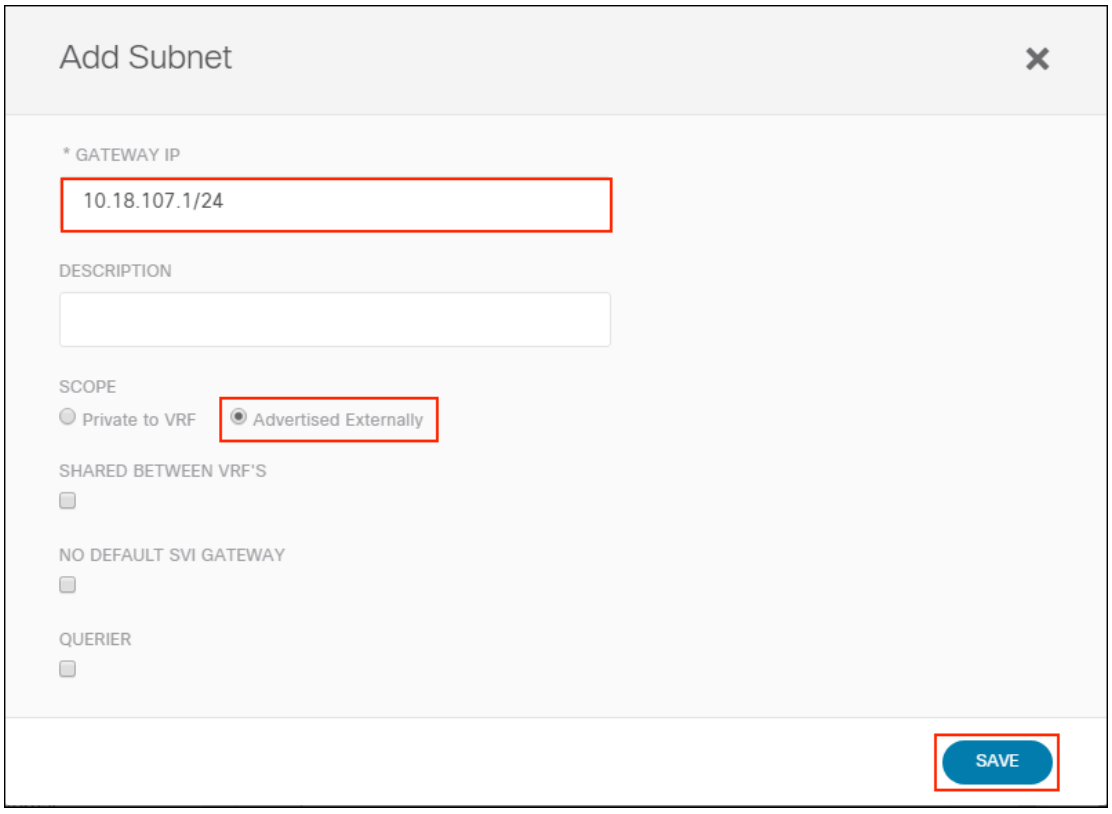
Return to Contents

Step 7: Create Bridge Domains

a. Click the **+ sign (1)** in the BRIDGE DOMAIN section, enter **WP-WEB in the DISPLAY NAME (2)** box, select **TenantA in the VIRTUAL ROUTING & FORWARDING (3)** section and click the **+ sigh under GATEWAY IP (4)**.

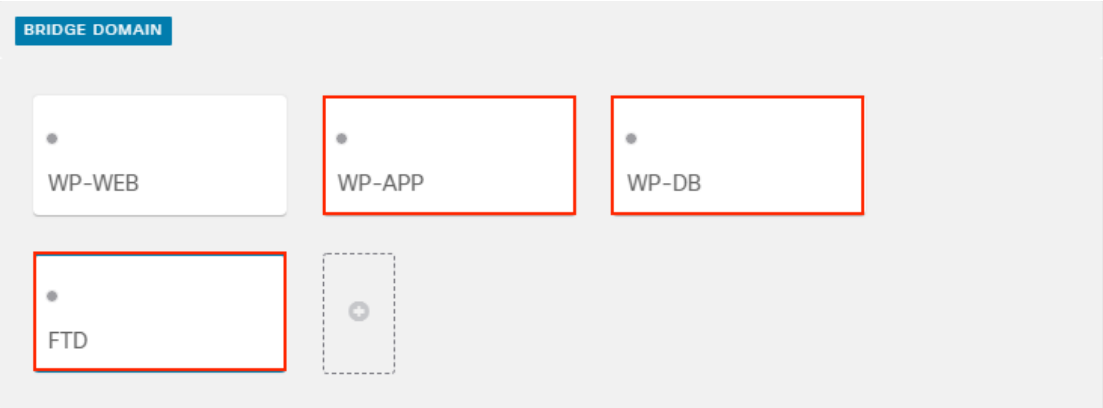


b. Enter the IP **10.18.107.1/24 for the GATEWAY IP**, select **Advertised Externally** and click **SAVE.**



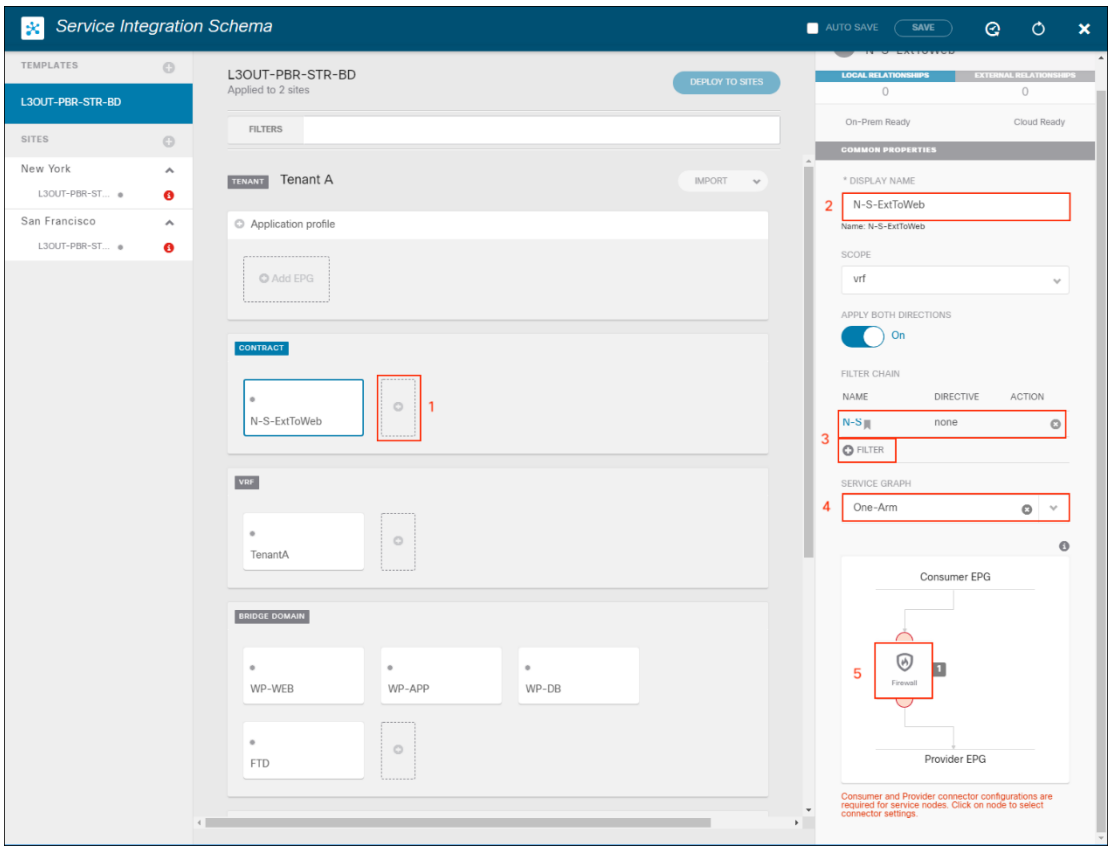
Return to Contents

c. Repeat steps a. and b. to create the bridge domains WP-APP (GW 10.18.108.1/24), WP-DB (GW 10.18.109.1/24) and FTP (GW 10.18.90.1/24).



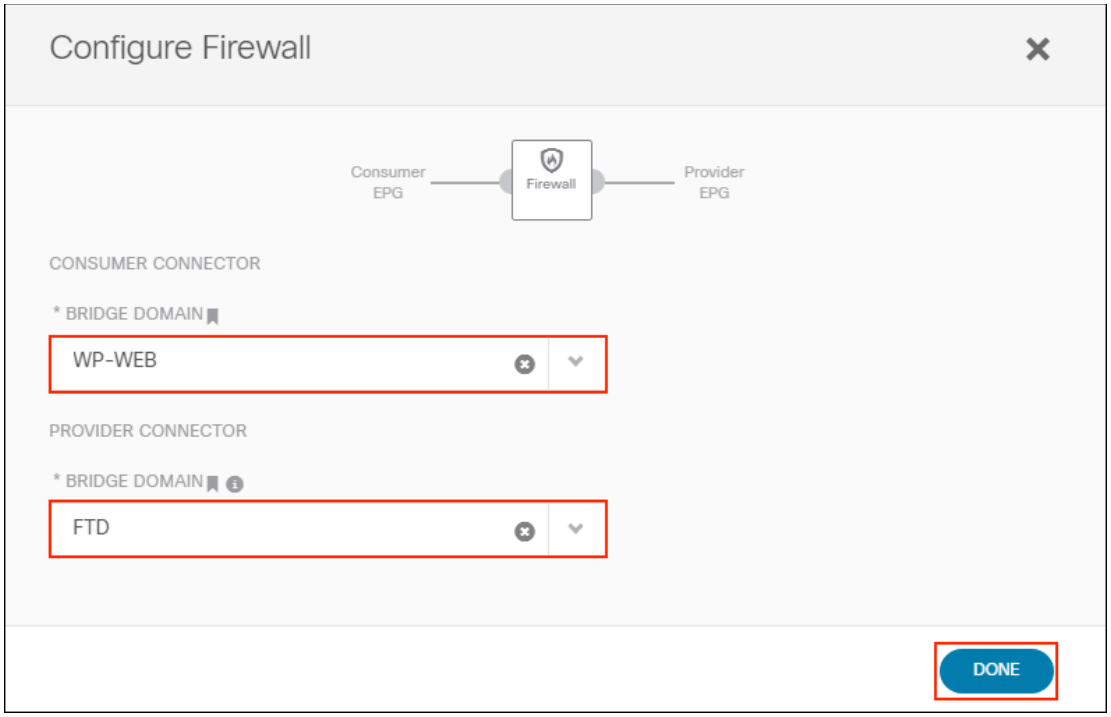
Step 8: Create Contracts

a. Click the **+ sign (1)** in the CONTRACT section and the **N-S-ExtToWeb (2)** for the DISPLAY NAME. Click the **+ sign (3) next to FILTER** and select the **N-S** filter. Select **One-Arm (4)** for the SERVICE GRAPH and click the **Firewall (5)**.

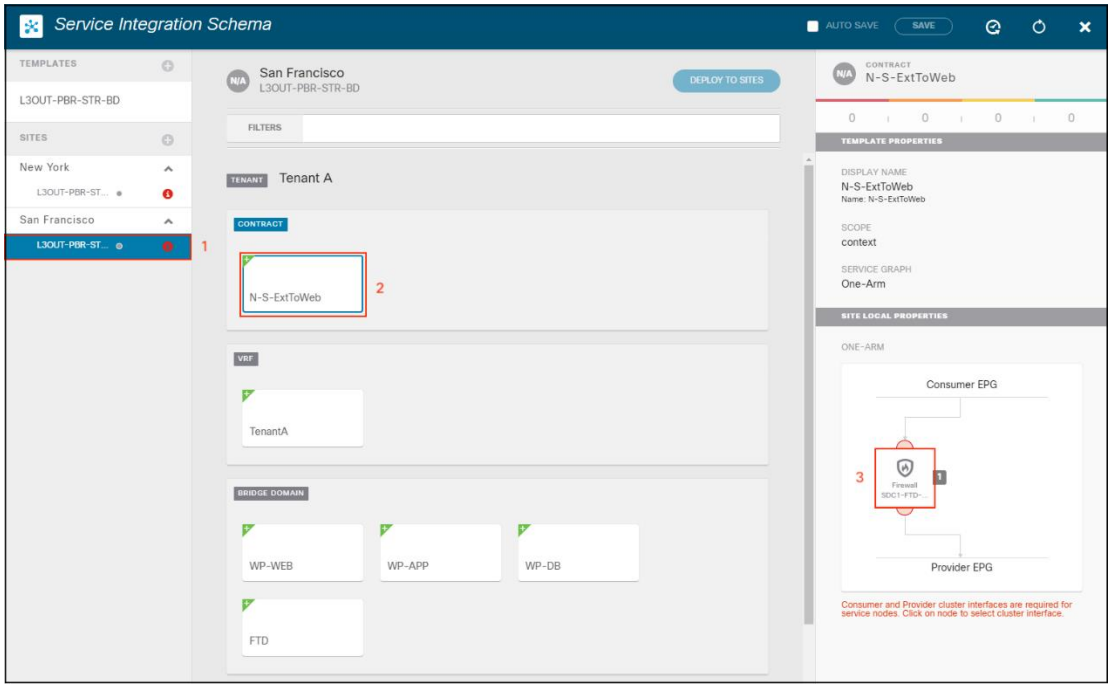


Return to Contents

b. Select **WP-WEB** for the CONSUMER CONNECTOR and **FTD** for the PROVIDER CONNECTOR. Click **DONE**

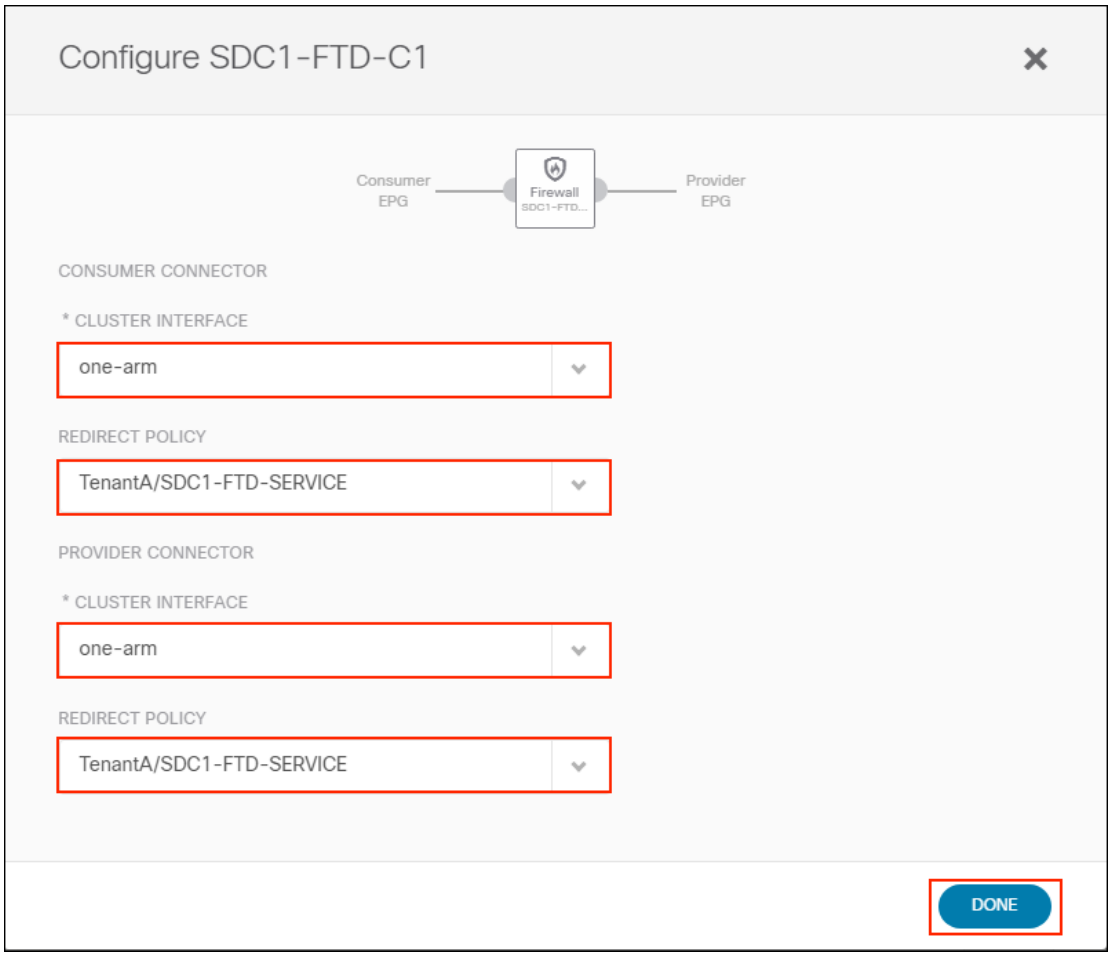


c. To associate the site specific firewall to the contract, select the **San FranCisco (1)** site, click the **N-S ExtToWeb (2)** contract and click the **Firewall icon (3)**.



Return to Contents

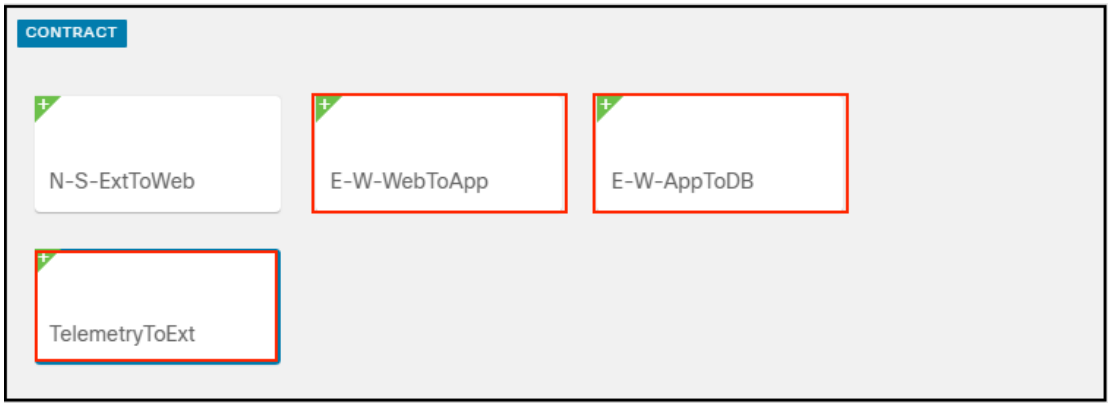
d. In the pop-up window, select **one-arm** for CLUSTER INTERFACE and **TenantA/SDC1-FTD-SERVICE** for REDIRECT POLICY for the CONSUMER and PROVIDER CONNECTORS. Click **DONE**



e. Repeat steps c. and d. for the New York site.

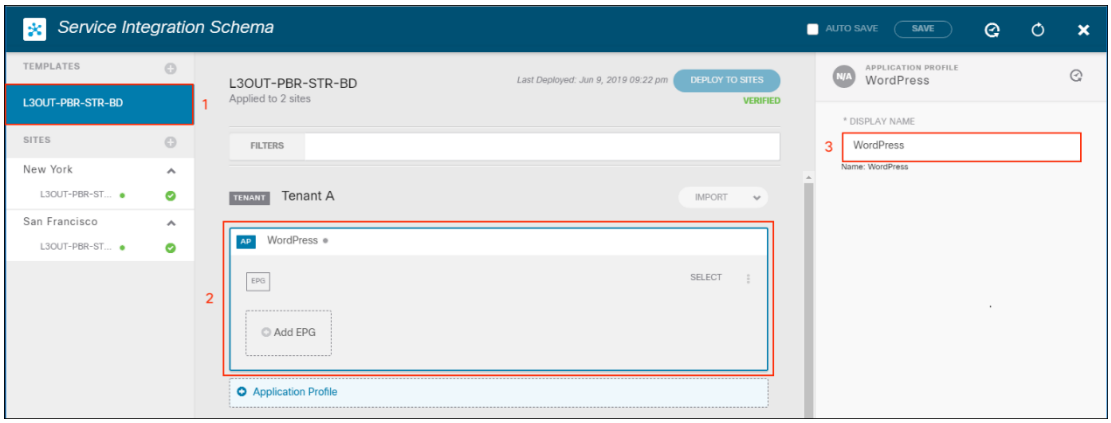
Return to Contents

f. Repeat step a. through e. to create the E-W-WebToApp, E-W-AppToDB and TelemetryToExt contracts.

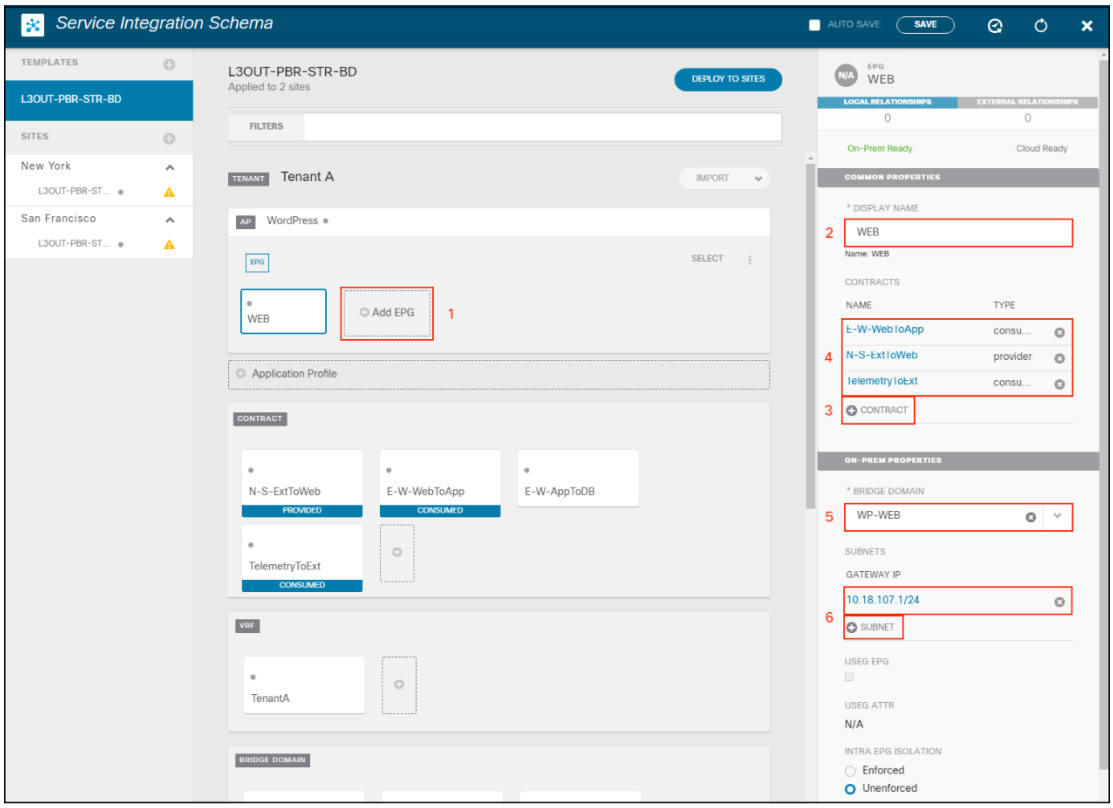


Step 9: Create Application Profile

a. To name Application Profile, click the **L3OUT-PBR-STR-BD (1)** template and click the **Application Profile (2)** section and enter **WordPress (3) in the DISPLAY NAME** box.

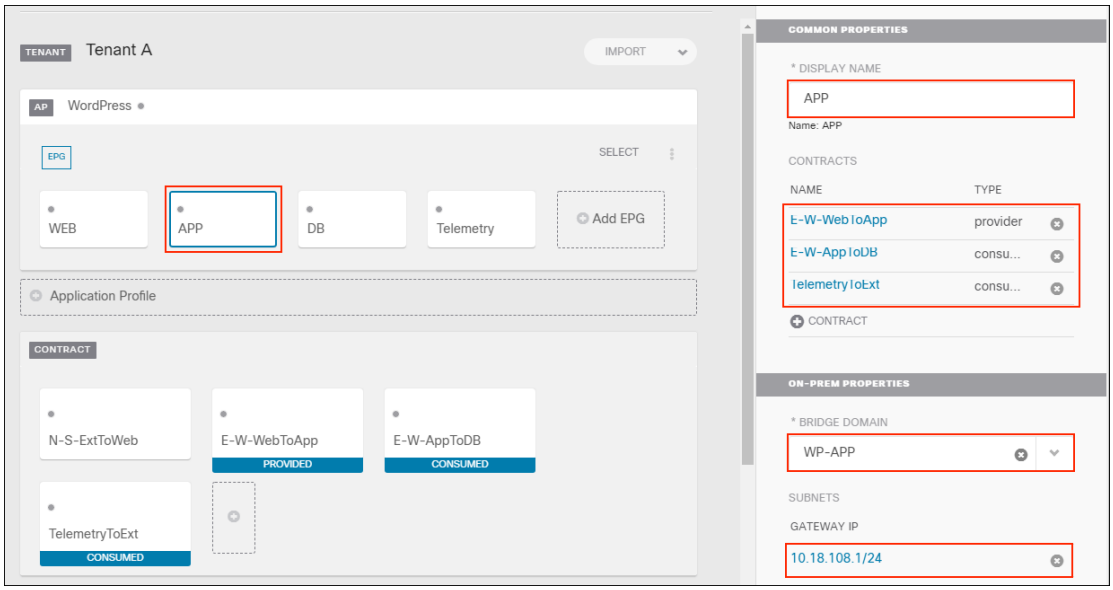


b. To add an EPG, click **Add EPG (1)**, Enter **WEB in the DISPLAY NAME (2)** box and click the **+ sign (3) next to CONTRACT** and add the required contracts. **Note the contracts names and types (4)**. Select the **WP-WEB BRIDGE DOMAIN (5)** and click the **+ sign next to subnet and enter 10.18.107.1/24 (6)** for the IP GATEWAY.



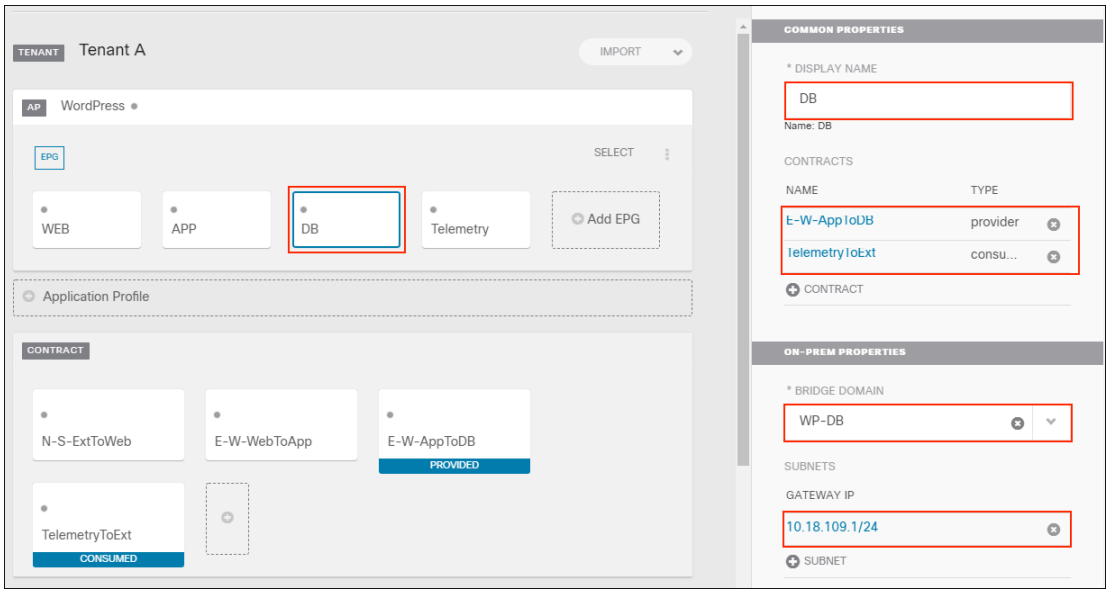
c. Repeat steps b. to create the APP, DB and Telemetry EPGs.

APP EPG

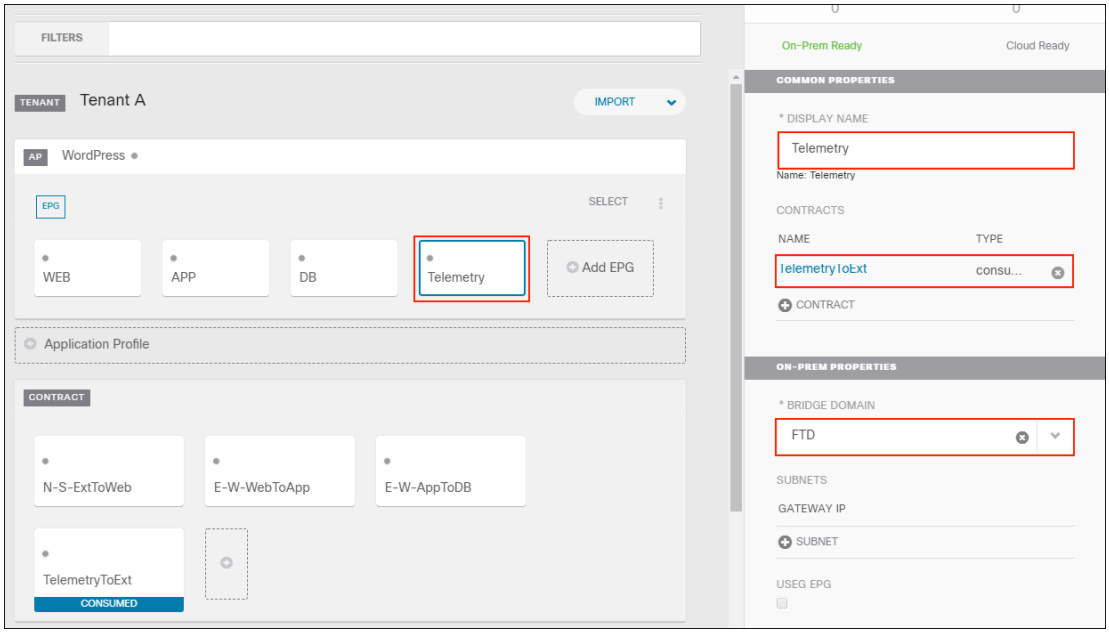


Return to Contents

DB EPG



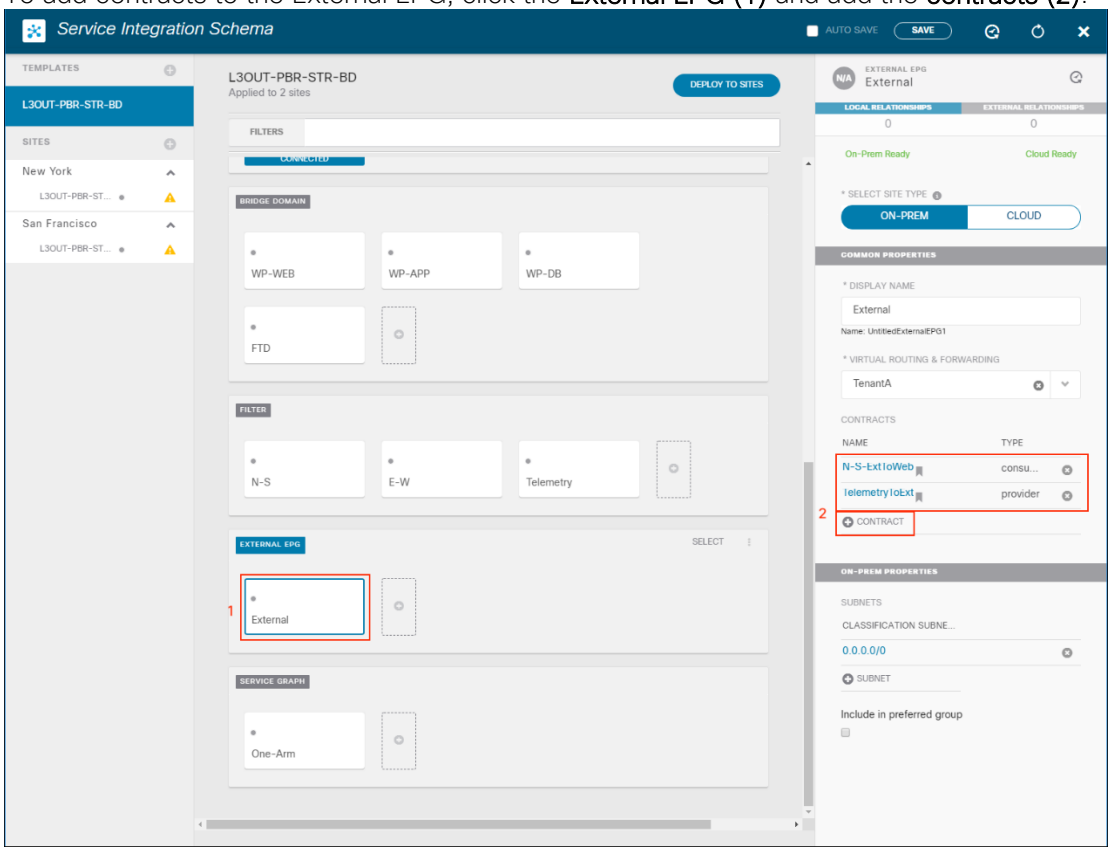
Telemetry EPG



Return to Contents

Step 10: Add contracts to External EPG

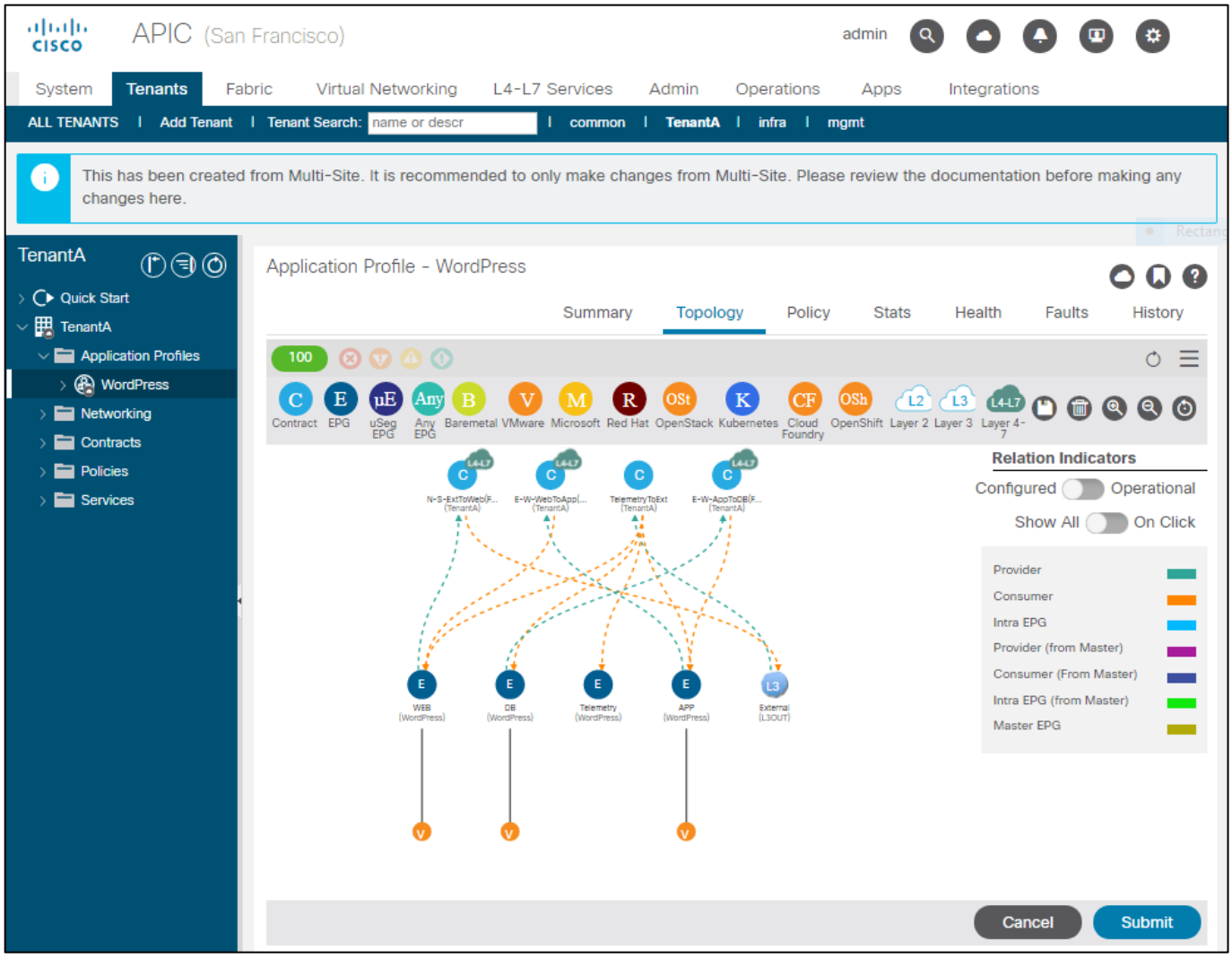
a. To add contracts to the External EPG, click the **External EPG (1)** and add the **contracts (2)**.



Return to Contents

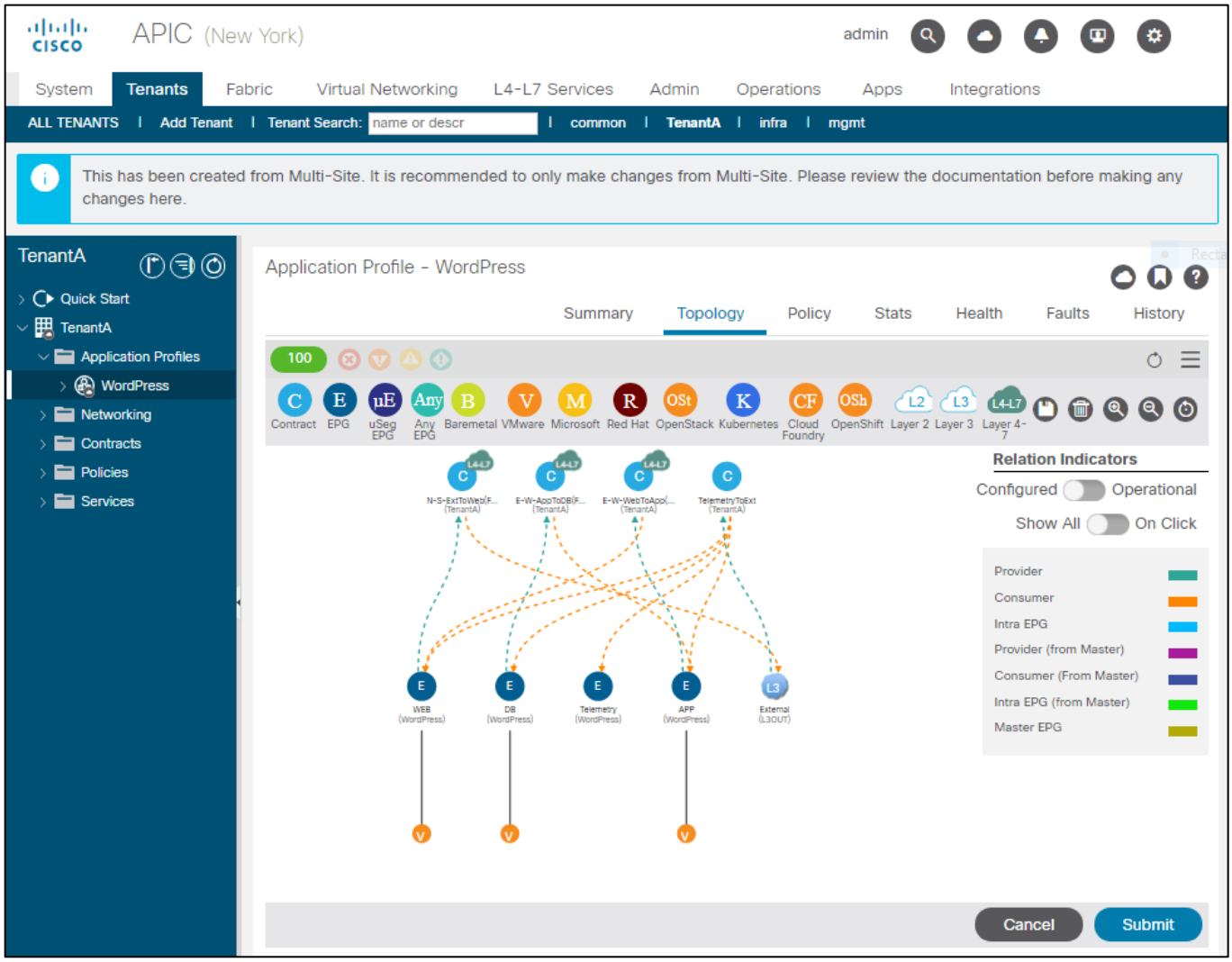
Step F: Verify Schema in APIC GUI

a. Review the APIC topology matches the Schemo deployed with MSO. This is the DC1 – San FranCisco APIC cluster.



Return to Contents

b. Review the APIC topology matches the Schema deployed with MSO. This is the DC2 – New York APIC cluster.



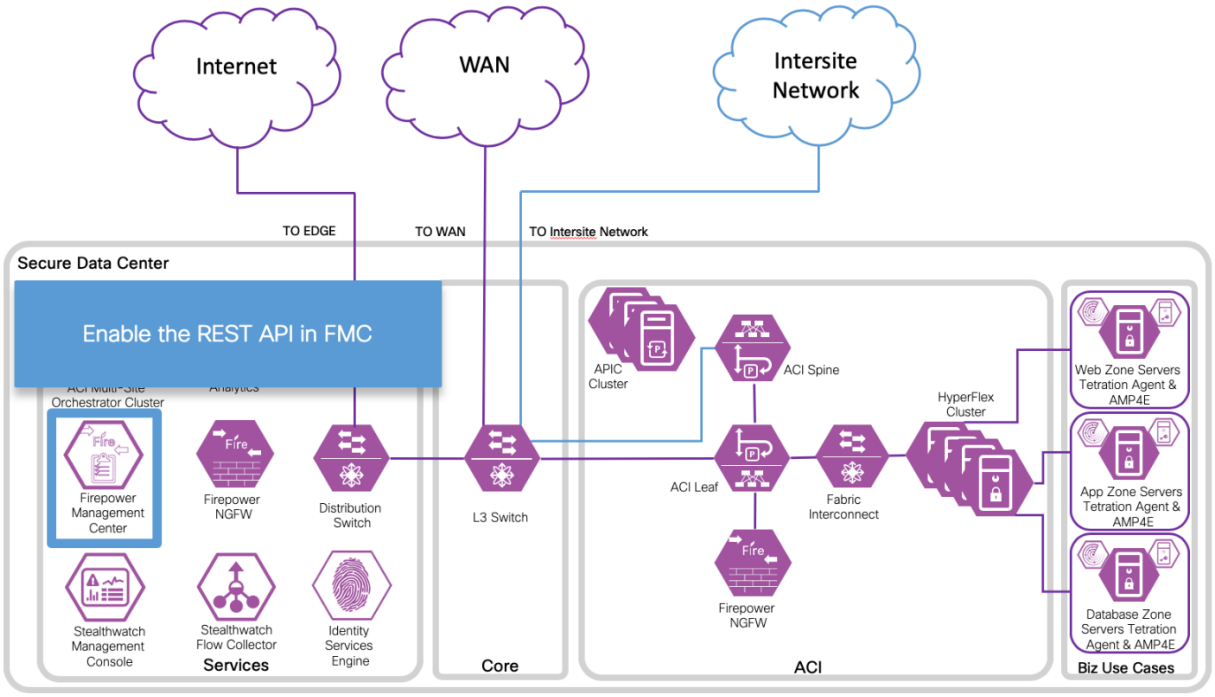
Return to Contents

Test Case 2 – Firepower Management Center and APIC

This integration involves building out a Multipod design with a single pod. The purpose of this test case is to confirm that the Firepower Threat Defense (FTD) device package works as expected with ACI. We selected a one-arm policy based redirect design similar to test case 1, but we tested with FTDv HA pair. FTD is the L4-L7 service providing threat defense services for north-south and east-west traffic in the data center fabric.

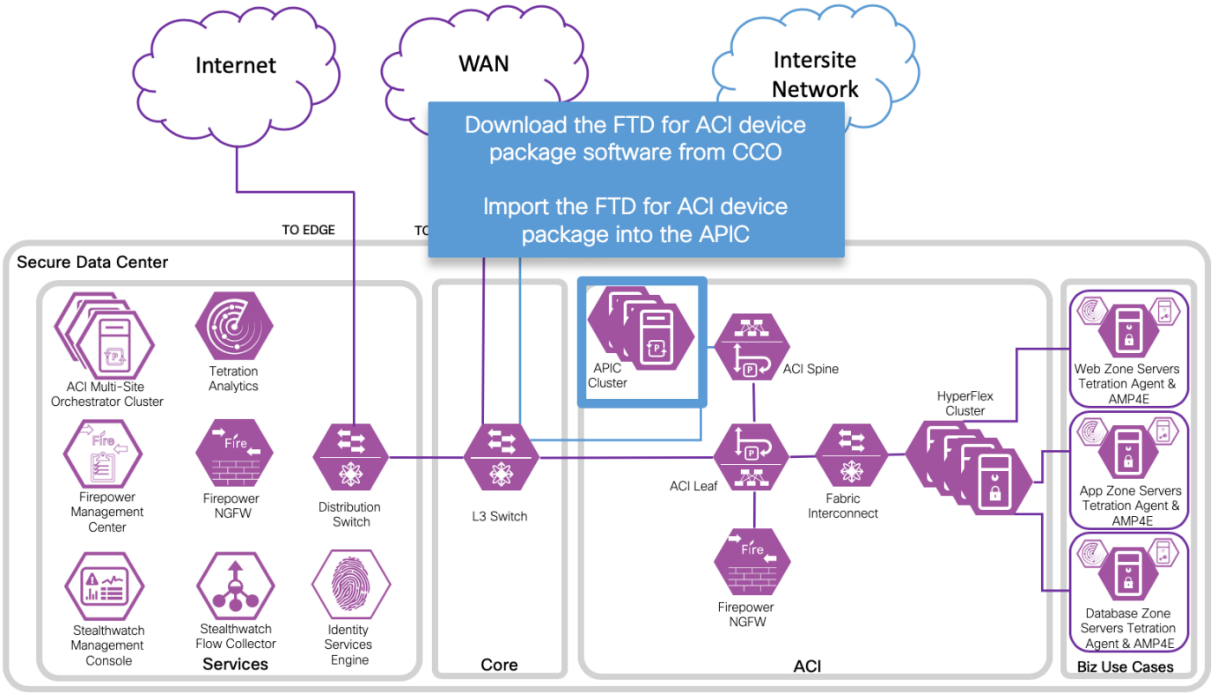
Test Description:

1. Enable the REST API in FMC.

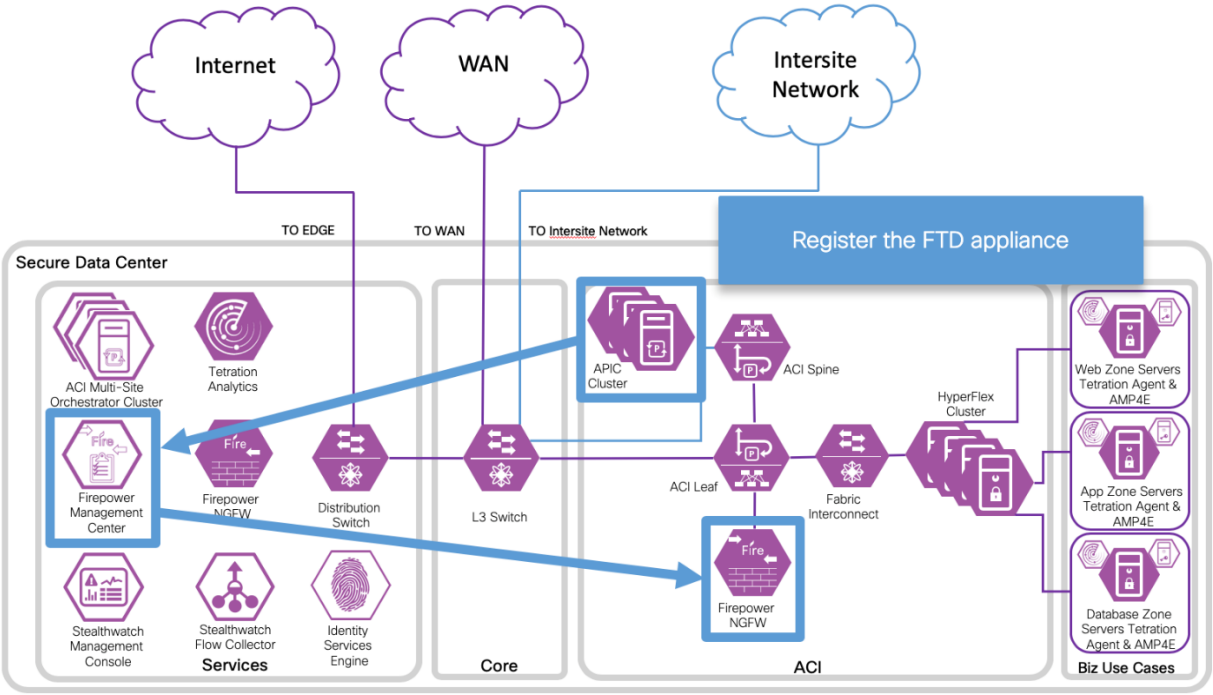


Return to Contents

2. Download the FTD for ACI device package software from CCO and Import into APIC.

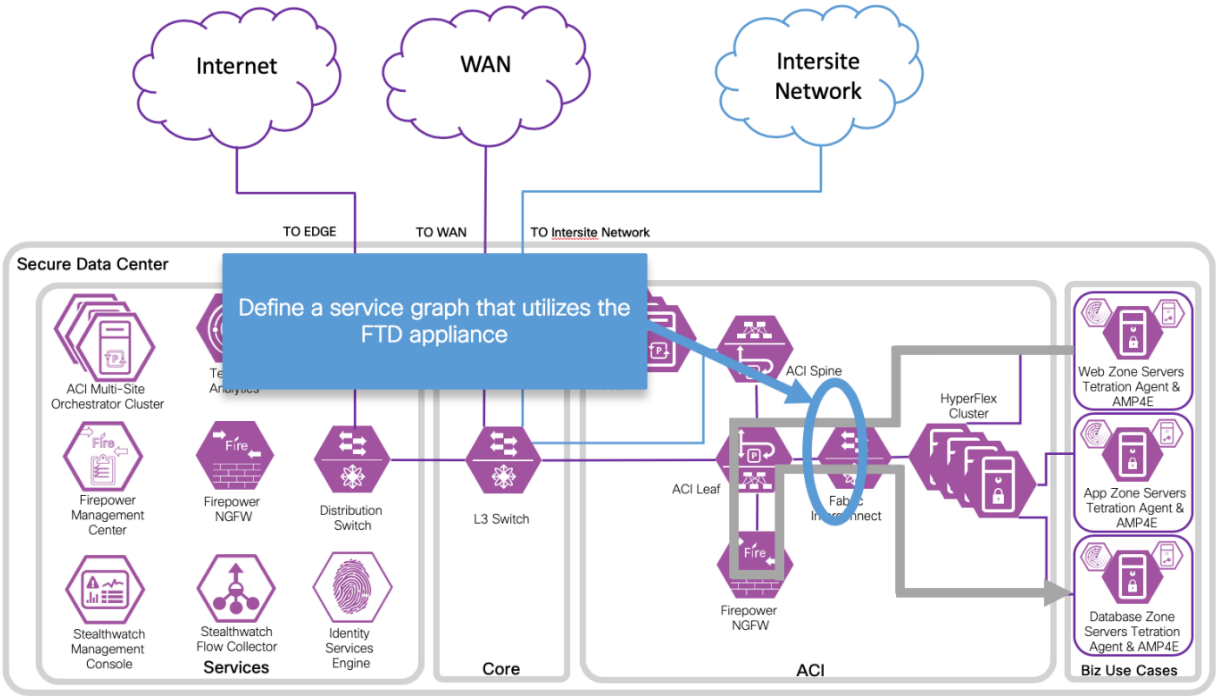


3. Register the FTD appliance.



Return to Contents

4. Define a service graph that utilizes the FTD appliance.



We tested the Cisco Firepower Threat Defense Quick Start Guide for APIC Integration, 1.0.3 https://www.Cisco.com/c/en/us/td/docs/security/firepower/APIC/quick-start/guide/ftd-apic-qsg-103.html .

This integration worked as documented in the Quick Start guide above. When the device package is applied to a device then it is considered a managed device. Multi-Site Orchestrator only supports unmanaged devices, so we didn't use this device package for our ACI Multi-Site reference design testing. The device package can help with orchestrating ACI Multipod deployments. It can enable joint management of the access control policy by a network administrator using APIC, and security administrator using FMC.

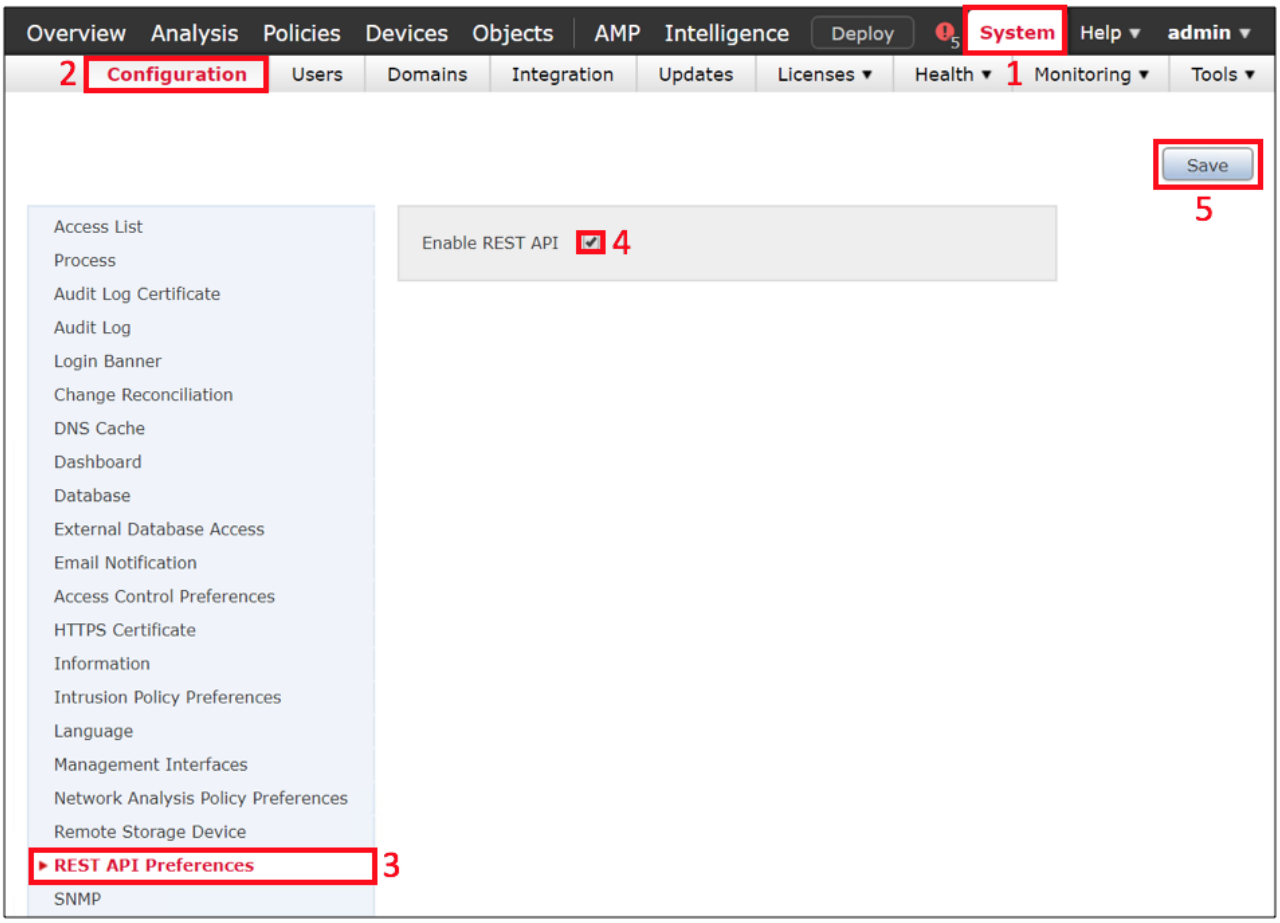
We implemented a 3-tier application in our Data Center 1 design for OpenCart. We utilized the Firepower Threat Defense Virtual (FTDv) in an HA pair as a one-arm policy based redirect deployment with multiple contracts. We implemented the one-arm interface on a physical port, but it could also be implemented as a Trunk.

The APIC required configuration steps in Test Case 1 are assumed to have already been implemented.

Implementation Procedure

Step 1

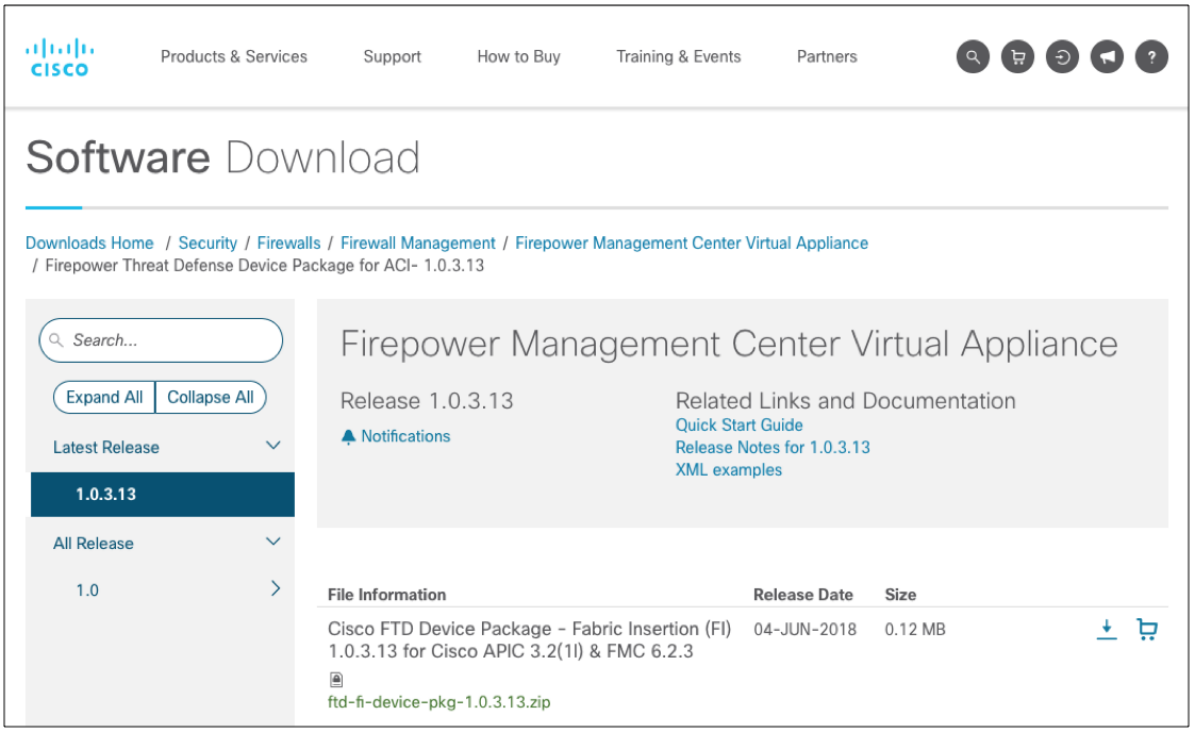
a. Enable REST API in Firepower Management Center. Navigate to System (1)->Configuration (2)->REST API Preferences (3), select the checkbox (4) to Enable REST API, and select Save (5).



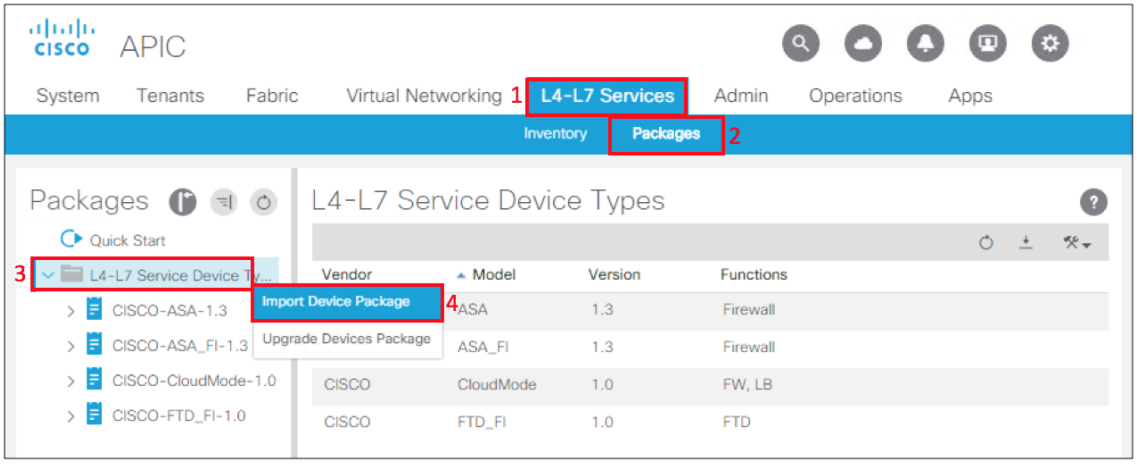
Return to Contents

Step 2

a. Download Firepower Threat Defense Device package from Cisco.com, https://software.Cisco.com/download/home/286259687/type/286320228/release/1.0.3.13

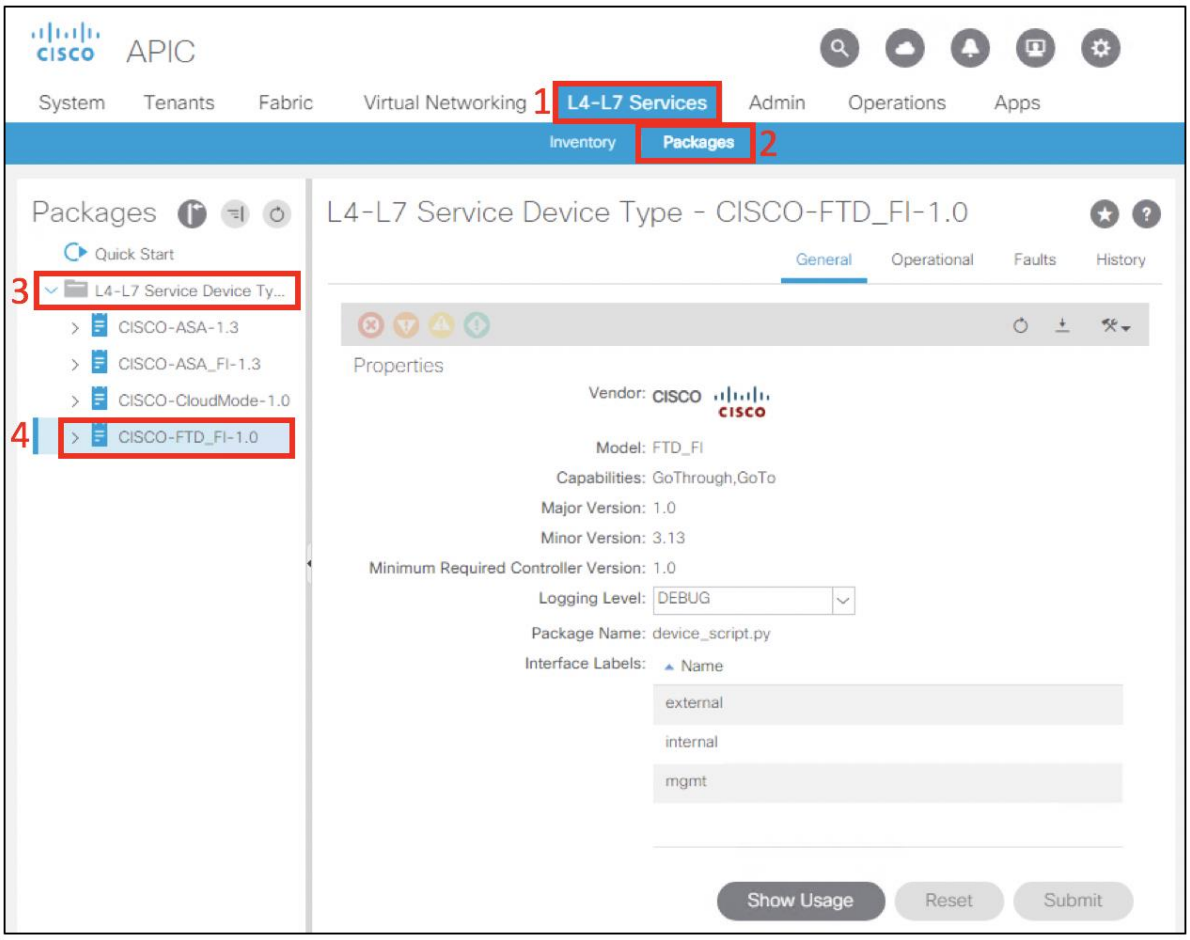


b. Import FTD device package into APIC. Navigate to L4-L7 Services (1)->Packages (2)->L4-L7 Service Device Types (3), and select Import Device Package (4).



Return to Contents

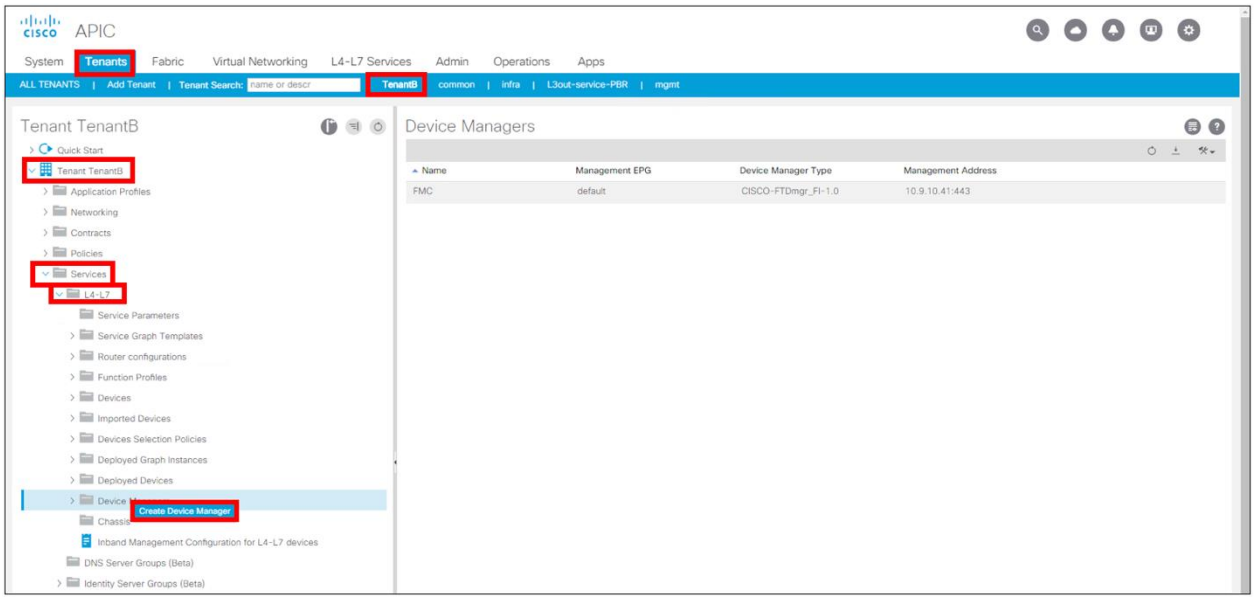
c. View FTD device package. Navigate to **L4-L7 Services (1)->Packages (2)->L4-L7 Service Device Types (3)** and select **Cisco-FTD-FI-1.0 (4)**.



Return to Contents

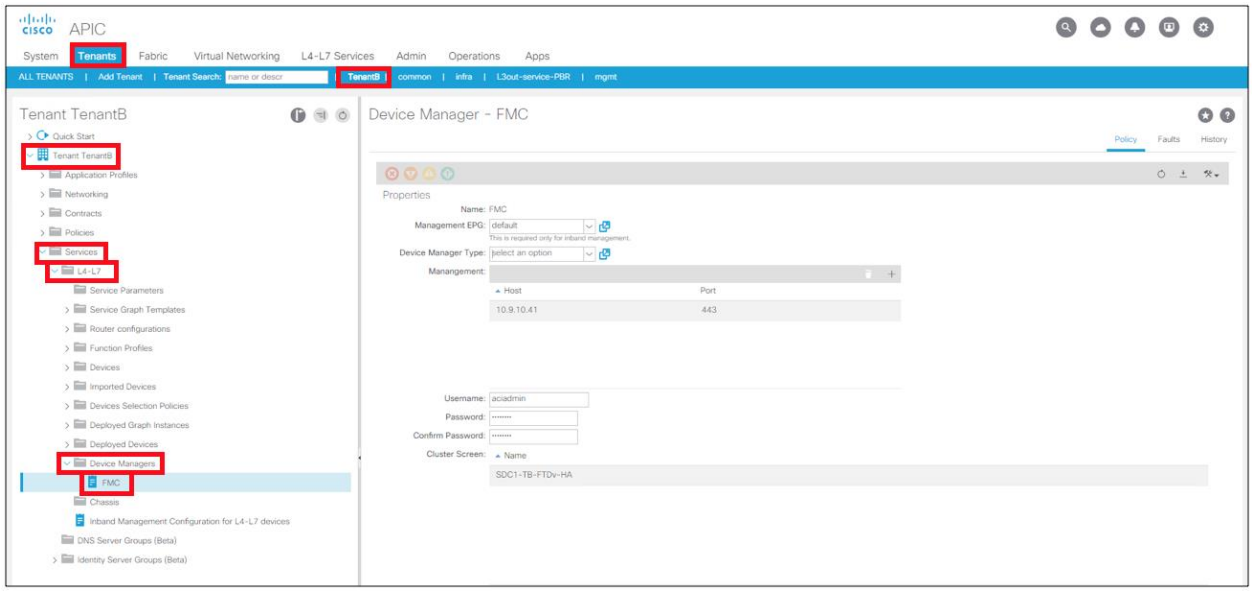
Step 3

a. Create L4-L7 Device Manager for Firepower Management Center (FMC) in APIC GUI. Navigate to Tenant-><tenant-name>->Services->L4-L7->Device Managers Right-Click and Select Create Device Manager.



b. Create Device Manager for FMC in APIC GUI. Navigate to Tenant-><tenant-name>->Services->L4-L7->Device Managers->FMC. Set the Management EPG to default. In the Management section select the plus sign and add the FMC GUI IP address and port. Add the login credentials for APIC to login into FMC and orchestrate the access policy.

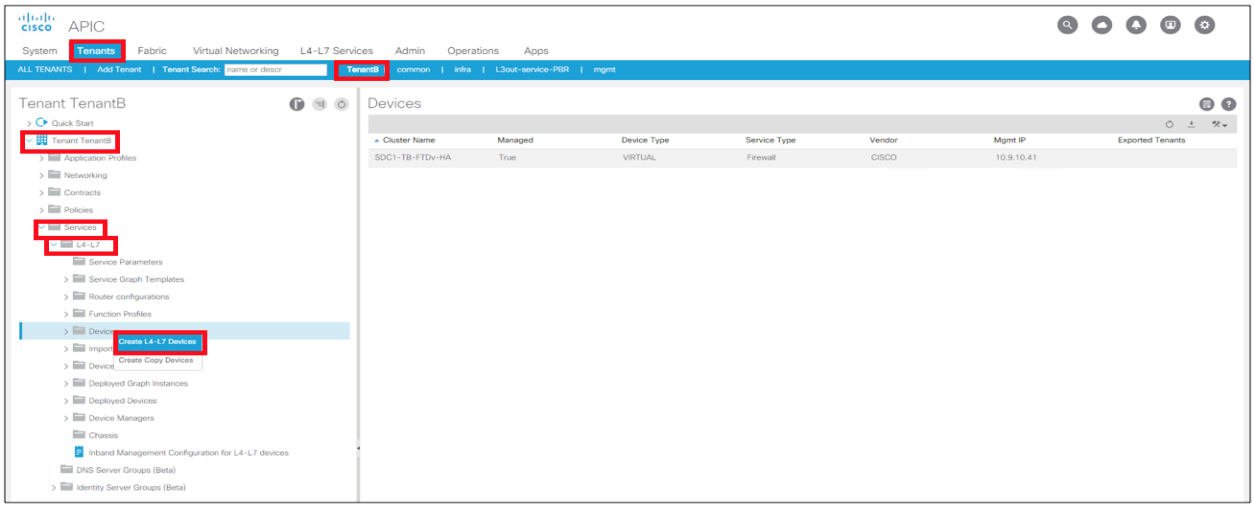
Note: It is recommended to setup unique credentials in FMC for APIC so that it can be identified easily in the FMC audit logs.



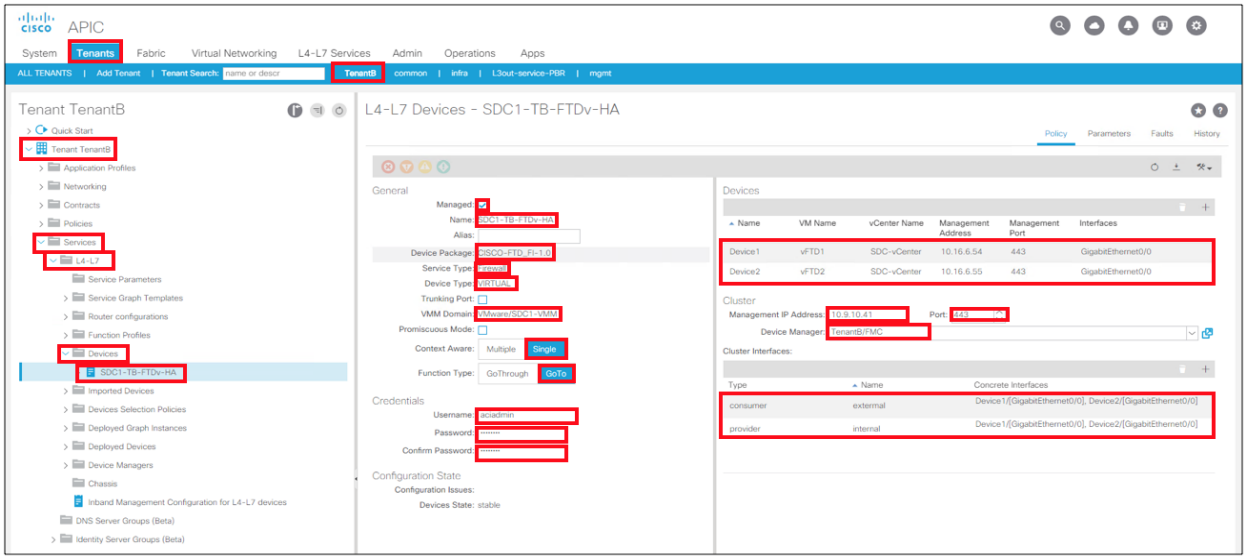
Return to Contents

Step 4

a. Create L4-L7 Device for the one-arm FTDv HA pair. Navigate to **Tenant-><tenant-name>->Services->L4-L7->Devices,** Right-Click and Select Create L4-L7 Devices.



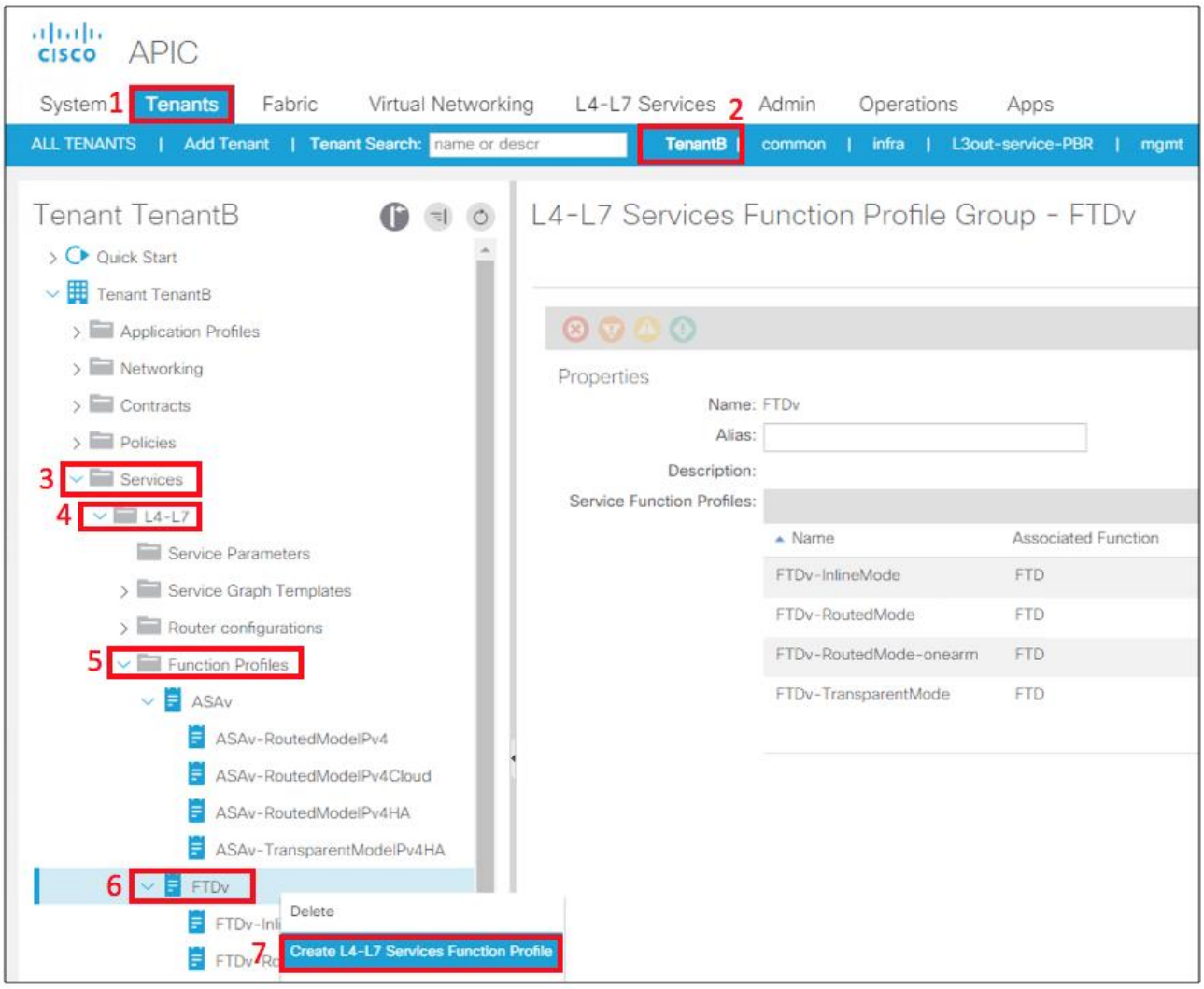
b. Create L4-L7 Device for the one-arm FTDv HA pair. Navigate to **Tenant-><tenant-name>->Services->L4-L7.** Right-click **Devices** and select **Create L4-7 Devices.** In the **Create L4-L7 Devices** dialog box, check the **Managed Checkbox**, enter a ***<Name>***, select **Service Type: Firewall,** select **Device Type: Virtual,** select the **<VMM Domain>,** select **View:Single Node,** select **Device Package: CISCO-FTD-FI-1.0,** select **Model: Virtual,** select **Context Aware: Single,** select **APIC to Device Management Connectivity: Out-of-Band,** select **Function Type: GoTo,** and enter the **credentials** ACI will use to orchestrate this device**.** Enter the device information for each of the FTDv VMs. Device1 will be for FTDv1 and Device2 is for FTDv2. For each device, enter the vCenter name, Management Address, Management Port and Interfaces. Under the Cluster section enter the Management IP address and port for FMC and select the Device Manager. Under the Cluster Interfaces sections, select the plus sign and enter consumer and provider interfaces. Although we are testing a one-arm interface, we must define both here and note that the Concrete Interfaces for both are the same. When we deploy this device package we will only use the external cluster interface which is how we currently deploy one-arm with the current device package. Confirmation that the devices created correctly is shown when Devices State is stable.



Return to Contents

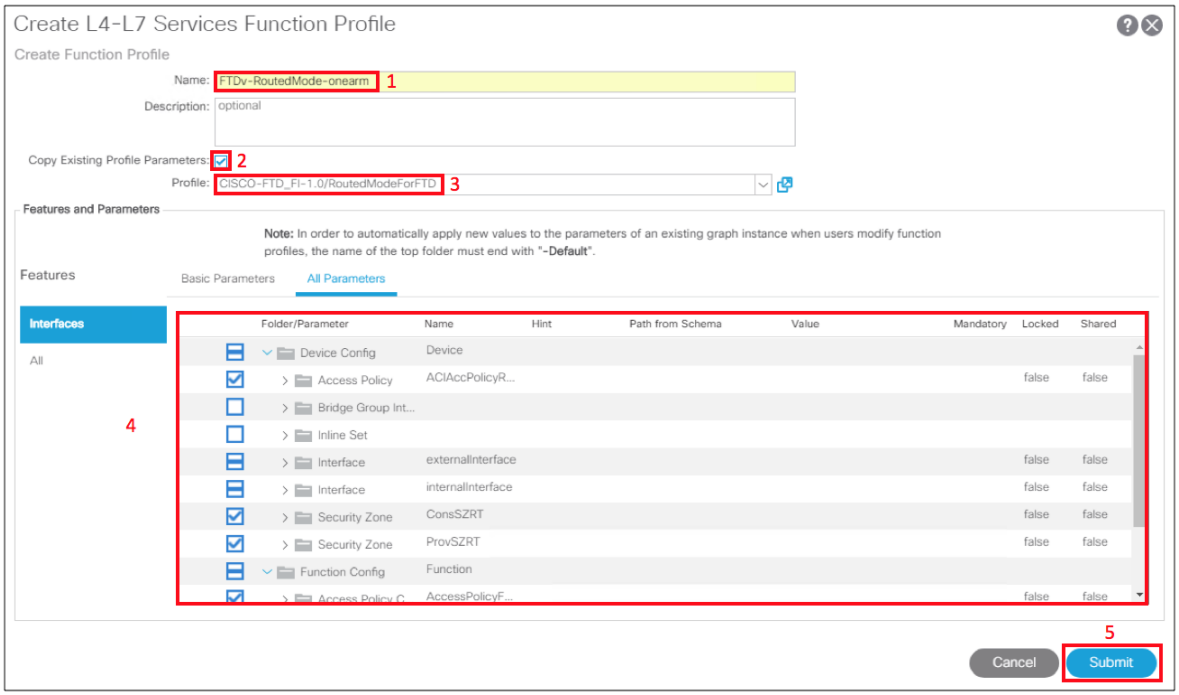
Step 5

a. Create One Arm Function Profile. Navigate to Tenant (1)-><tenant-name> (2)->Services (3)->L4-L7 (4)->Function Profiles (5)->FTDv (6). Right-Click and select Create L4-L7 Services Function Profile (7).



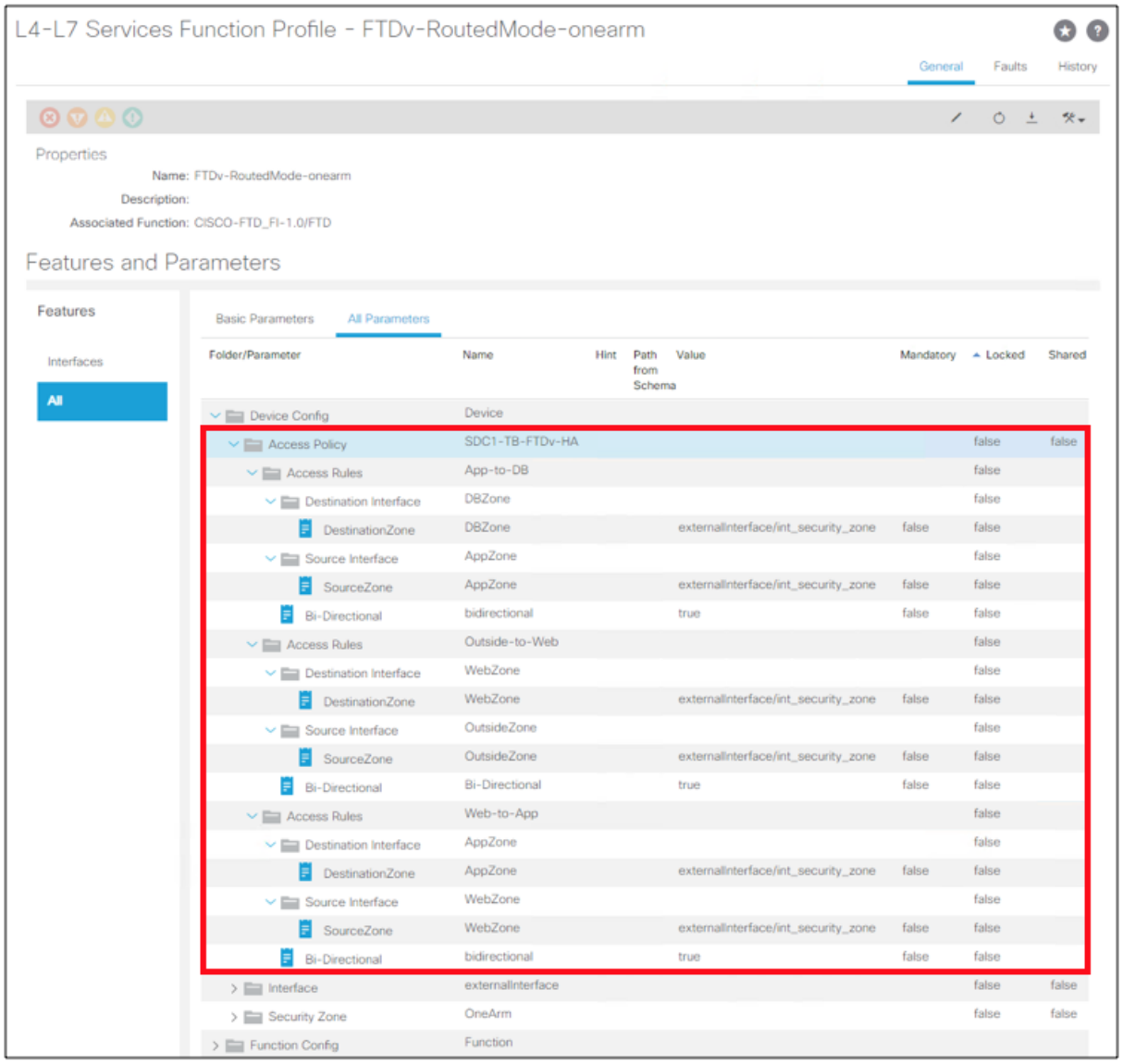
Return to Contents

b. Fill in the Function Profile Name as FTDv-RouteMode-onearm (1). Select Copy Existing Profile Parameters (2). Select the Profile to clone (3). We selected CISCO-FTD-FI-1.0/RoutedModeForFTD. The All Parameters section (4) is the initial value. Use the desired profile in c. and d. as reference and modify this existing profile to match. Select Submit (5) when complete.



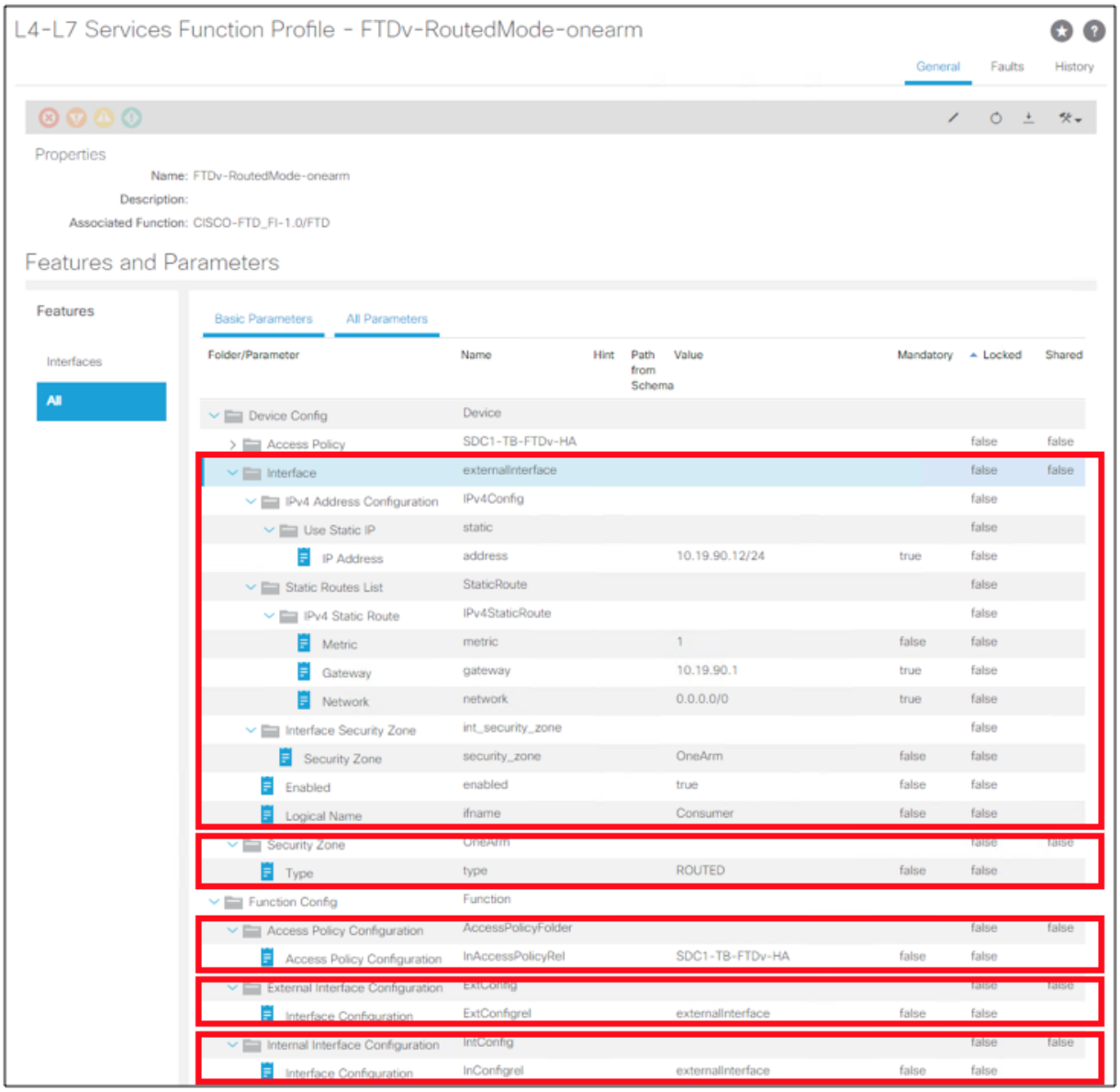
Return to Contents

c. Create One Arm Function Profile - Device Access Policy. The Access Policy section highlighted in Red below should be created. Access Rules for App-to-DB, Outside-to-Web and Web-to-App are created along with the corresponding Source and Destination Zones. Notice that only the externalinterface is used in creating the policy, which implements the one-arm deployment.



Return to Contents

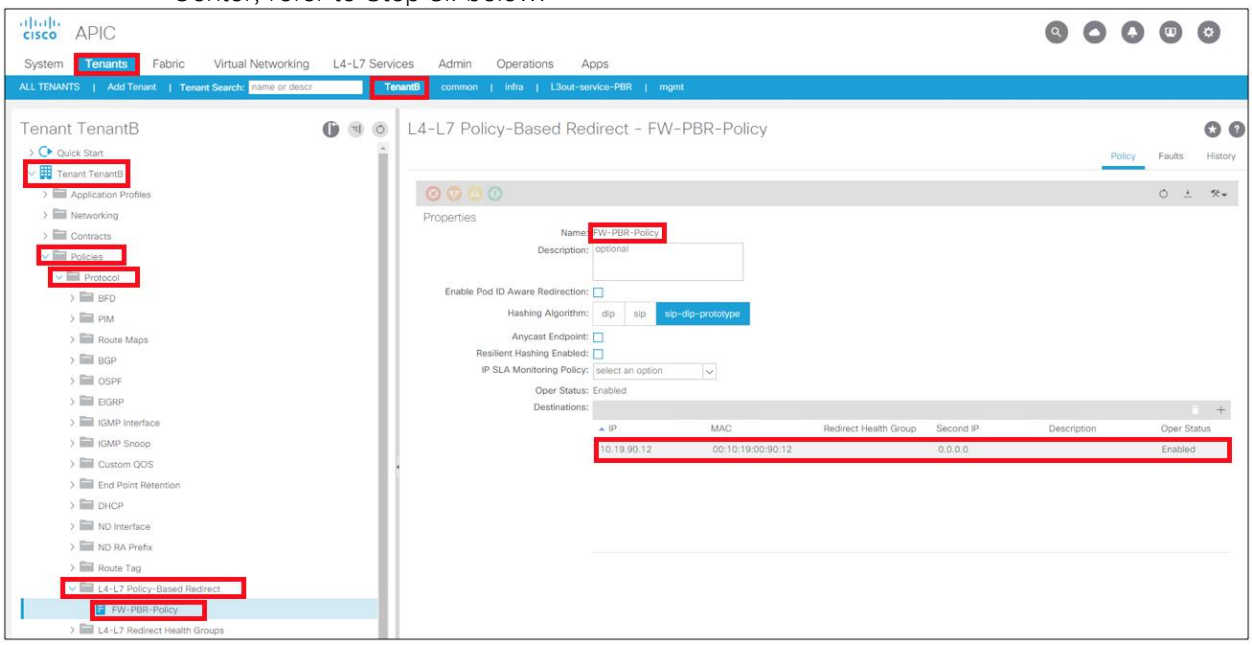
d. Create One Arm Function Profile – Interface, Security Zone, Access Policy Configuration, External and Internal Interface Configuration. The Interface policy for the externalinterface should be implemented as shown below. The IP address for the FTDv HA pair is 10.19.90.12/24 and a static route to 10.19.90.1 is setup. The Interface Security Zone is OneArm and is defined in the Security Zone parameter. The Access Policy Configuration is set to SDC1-TB-FTDv-HA. Both the External and Internal Interface Configuration are set to the externalinterface.



Return to Contents

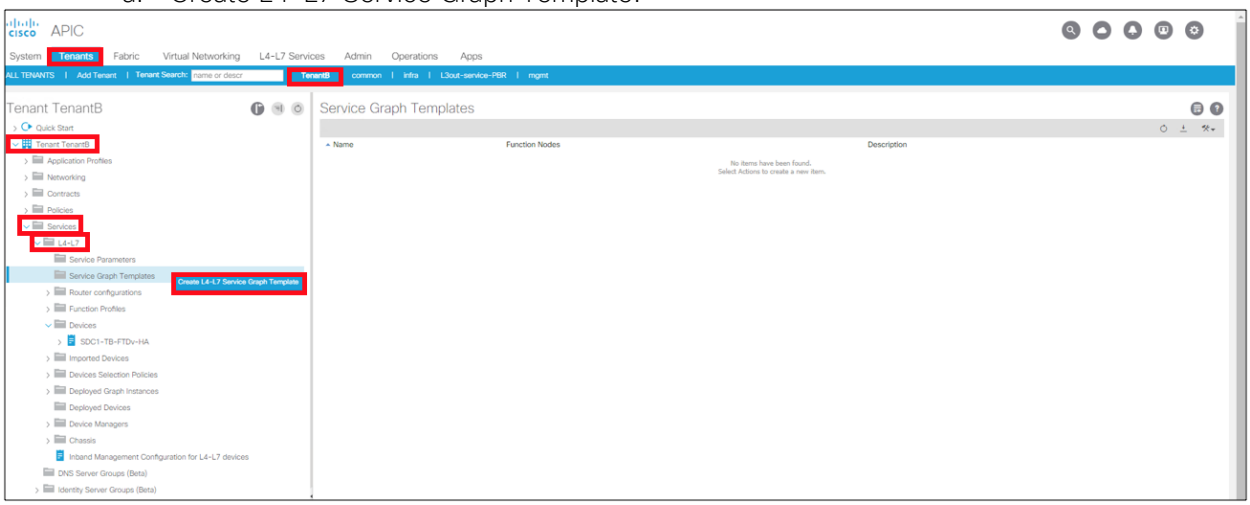
Step 6

a. Create L4-L7 Policy Based Redirect. Note that the MAC address in the PBR policy in APIC must match the MAC address on the FTD HA Pair interface in Firepower Management Center, refer to Step 8i. below.



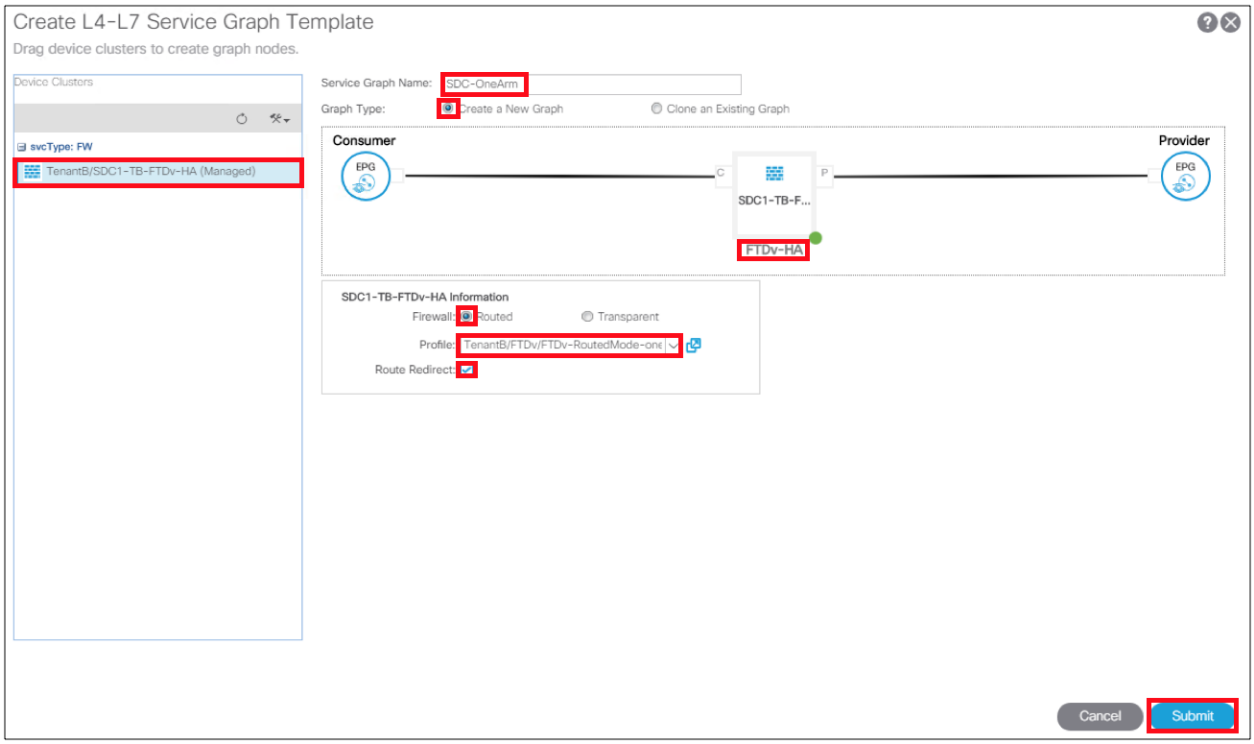
Step 7

a. Create L4-L7 Service Graph Template.



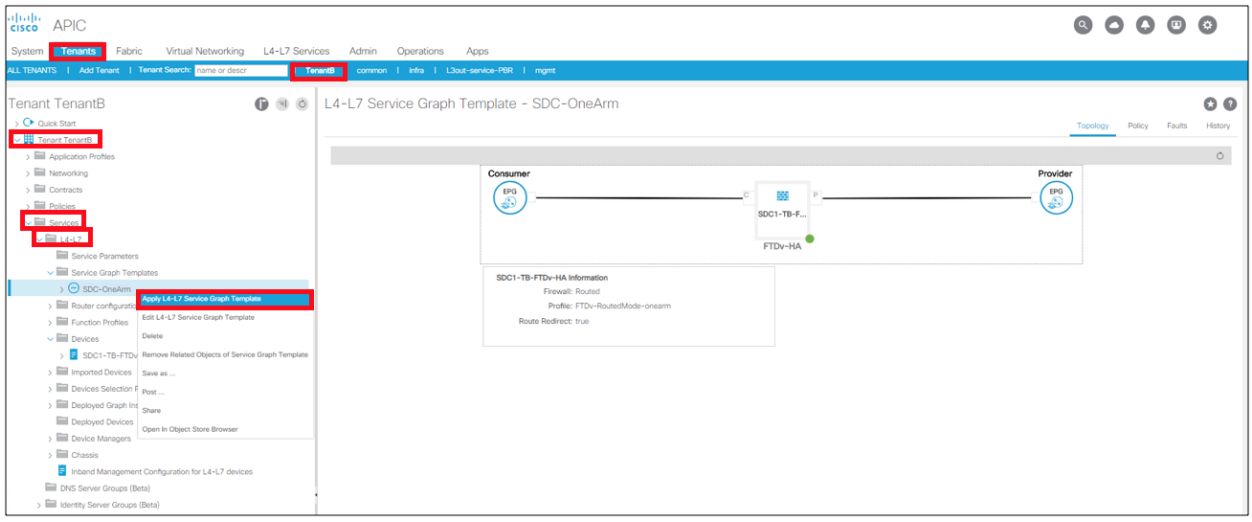
Return to Contents

b. Create One Arm PBR Service Graph with FTDv HA



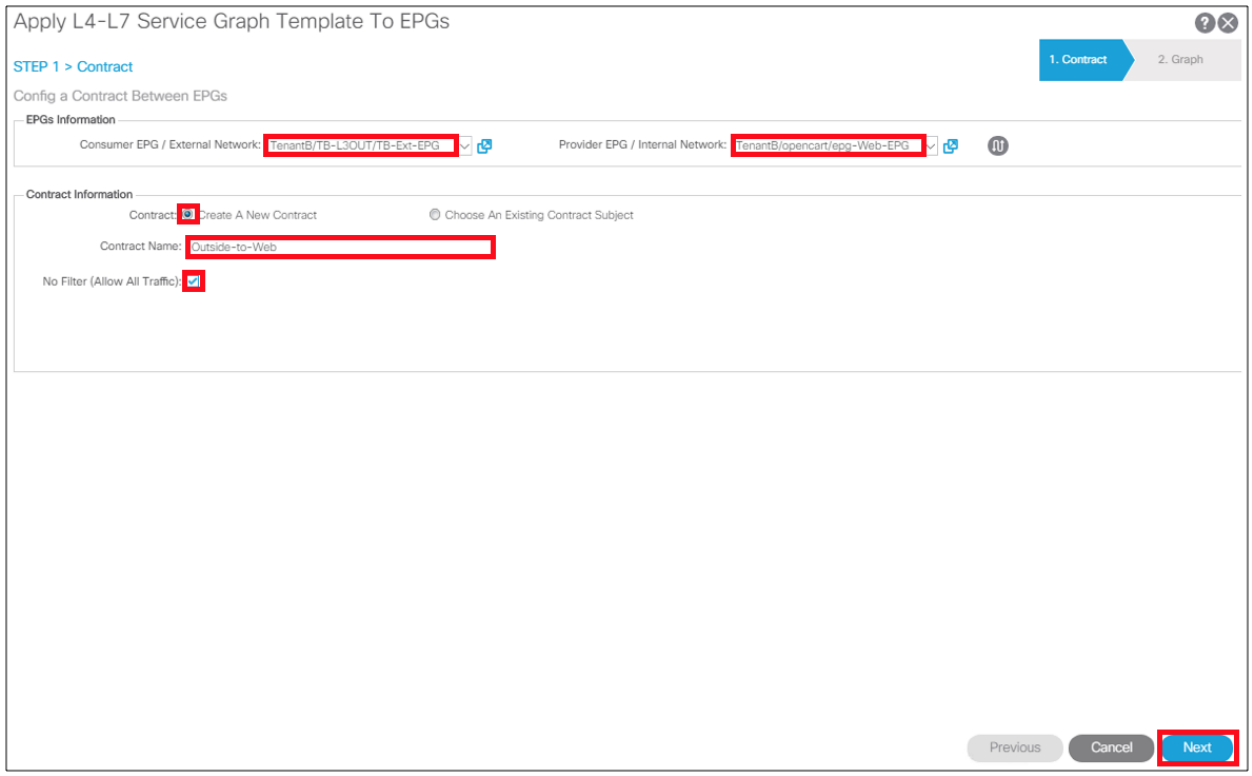
Step 8

a. Apply L4-L7 Service Graph

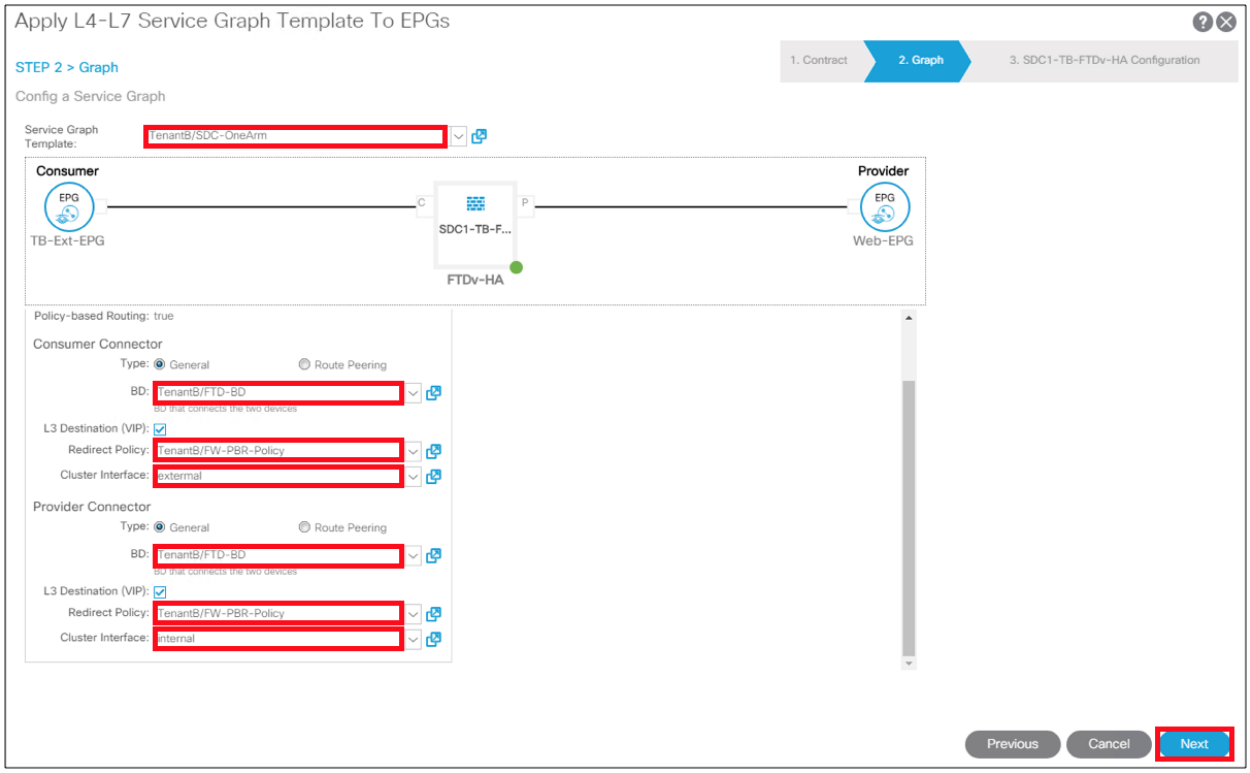


Return to Contents

b. Create Outside-to-Web Contract

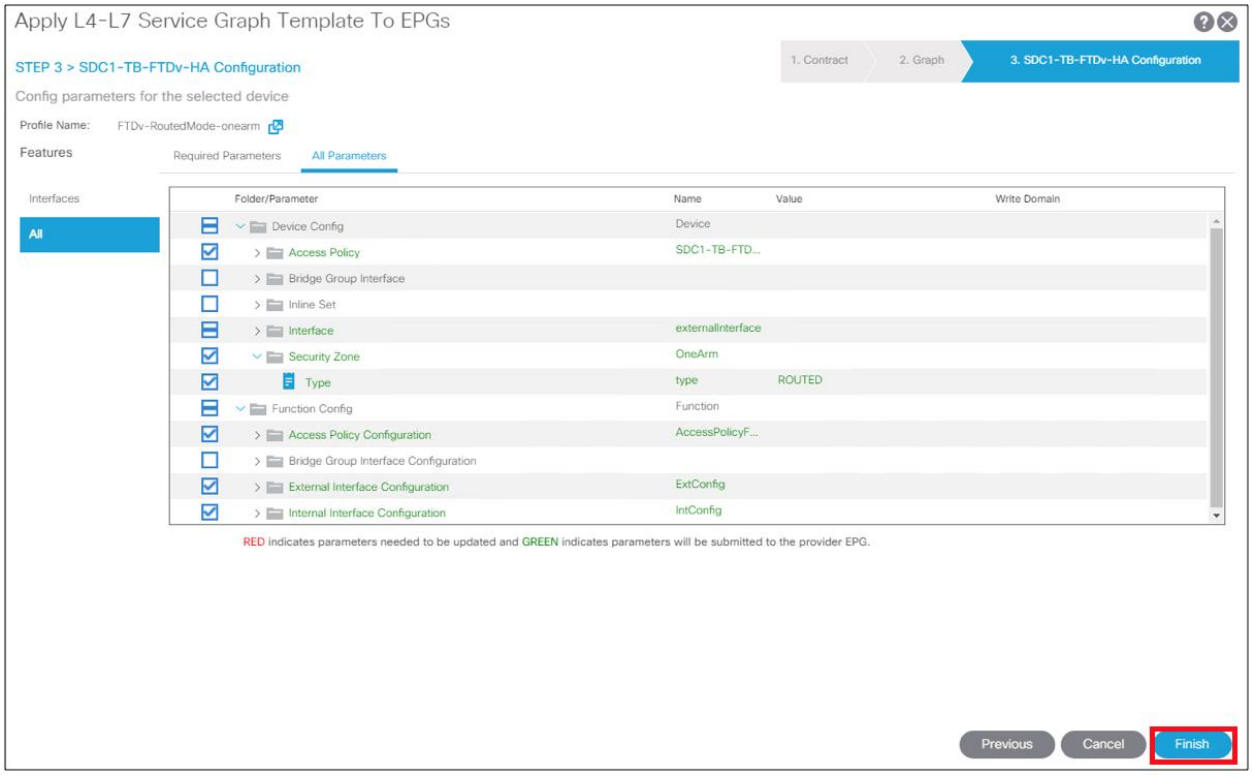


c. Apply One Arm PBR Service Graph to Outside-to-Web Contract

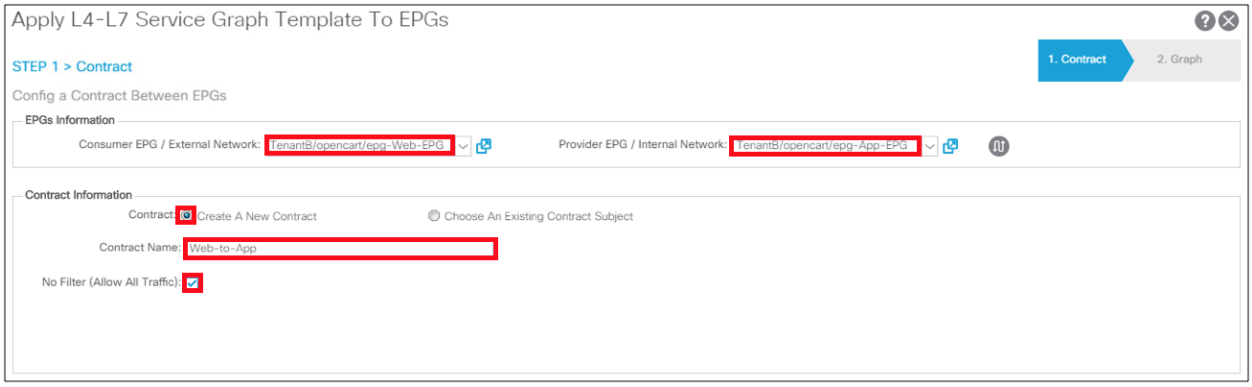


Return to Contents

d. Apply One Arm Function Profile to Outside-to-Web Contract

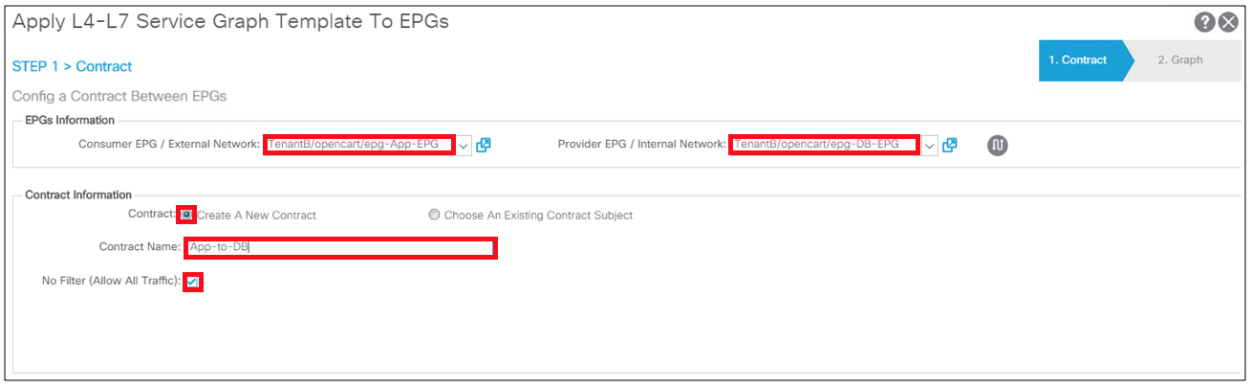


e. Create Web-to-App Contract

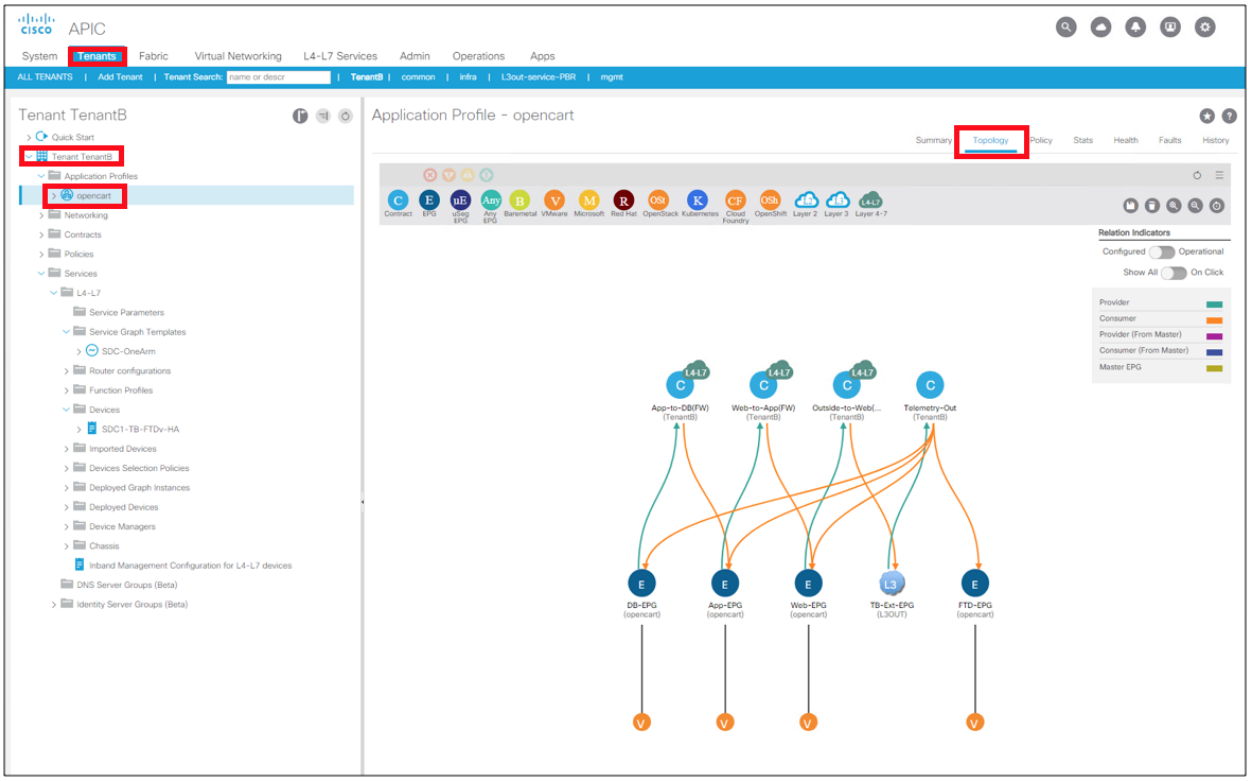


Return to Contents

f. Create App-to-DB Contract

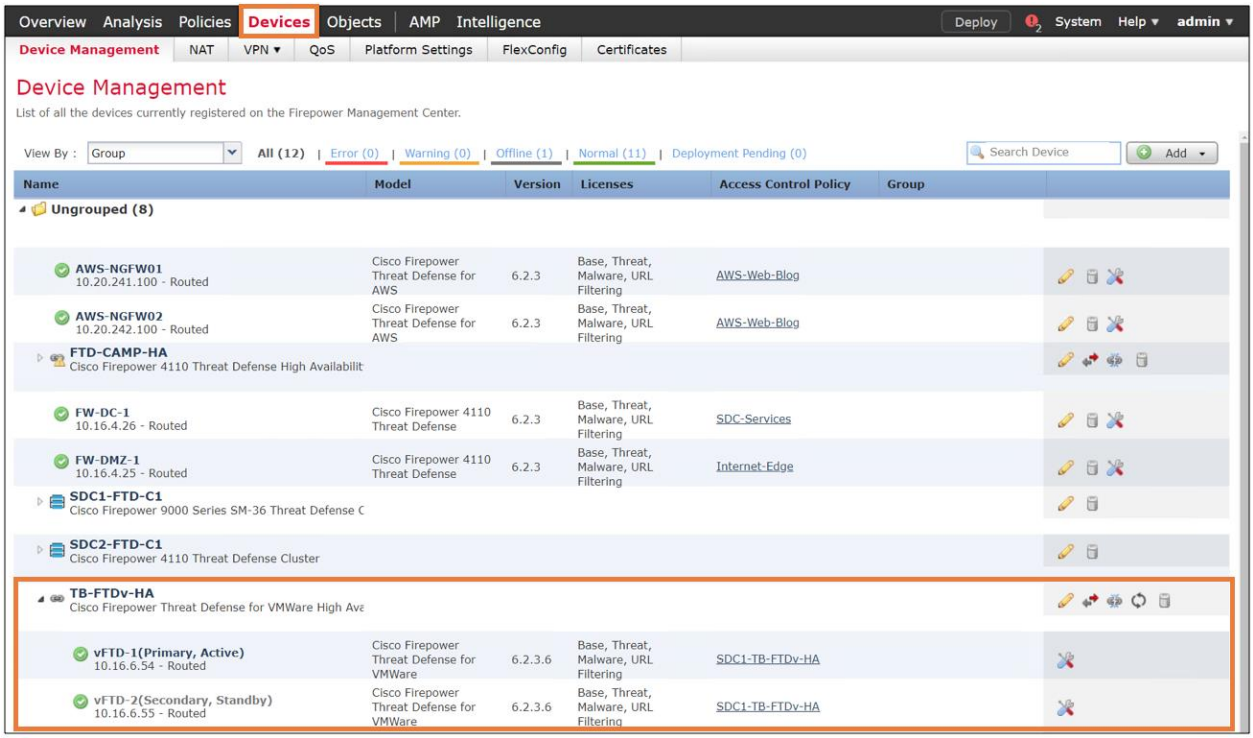


g. Application Profile Topology for OpenCart

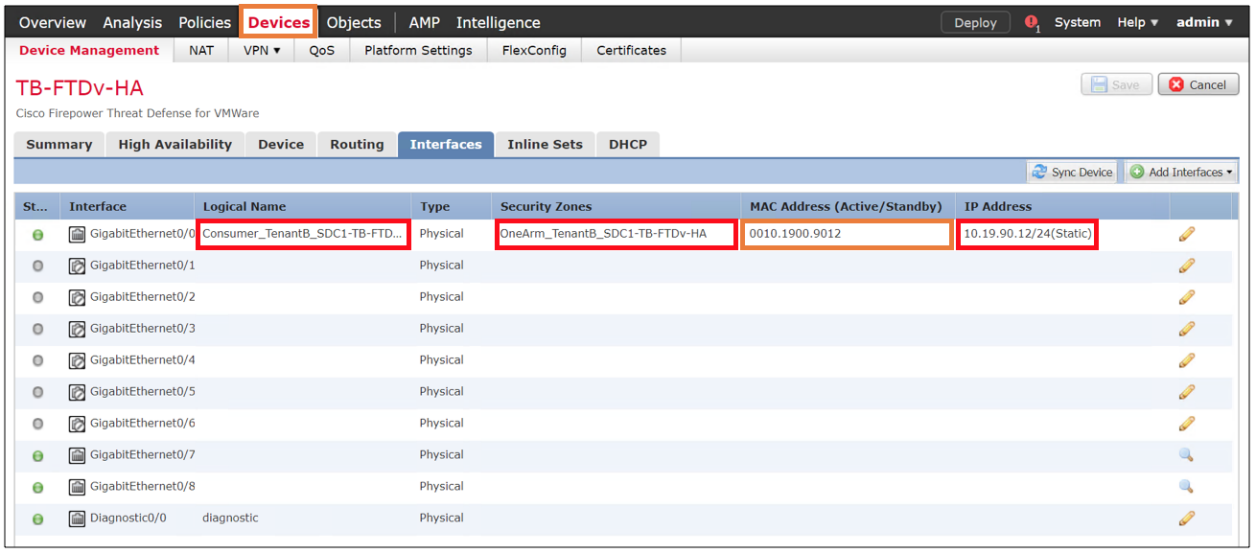


Return to Contents

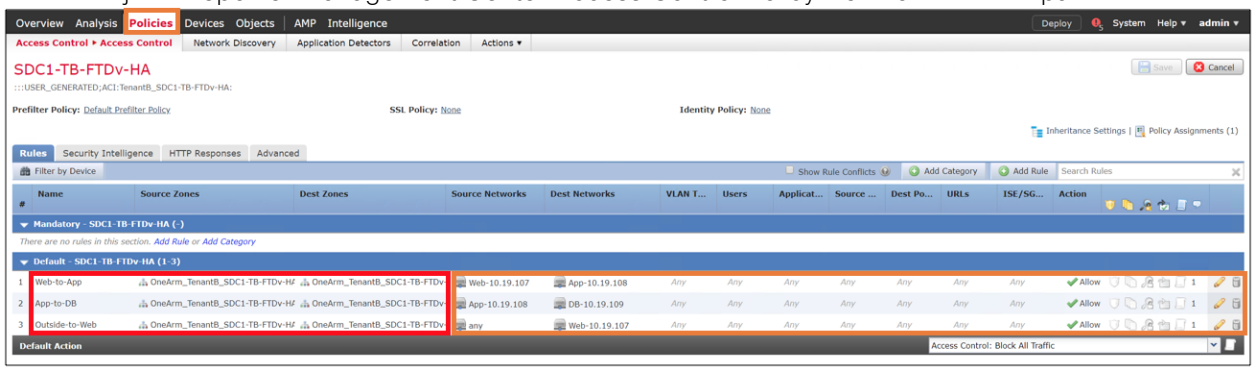
h. Firepower Management Center Devices view of FTDv HA pair.



i. Firepower Management Center (FMC) Interfaces view of FTDv HA pair. Note that the MAC address in FMC for the interface must match the MAC address in the PBR policy in APIC, refer to Step 6a above.



j. Firepower Management Center Access Control Policy view for FTDv HA pair



Return to Contents

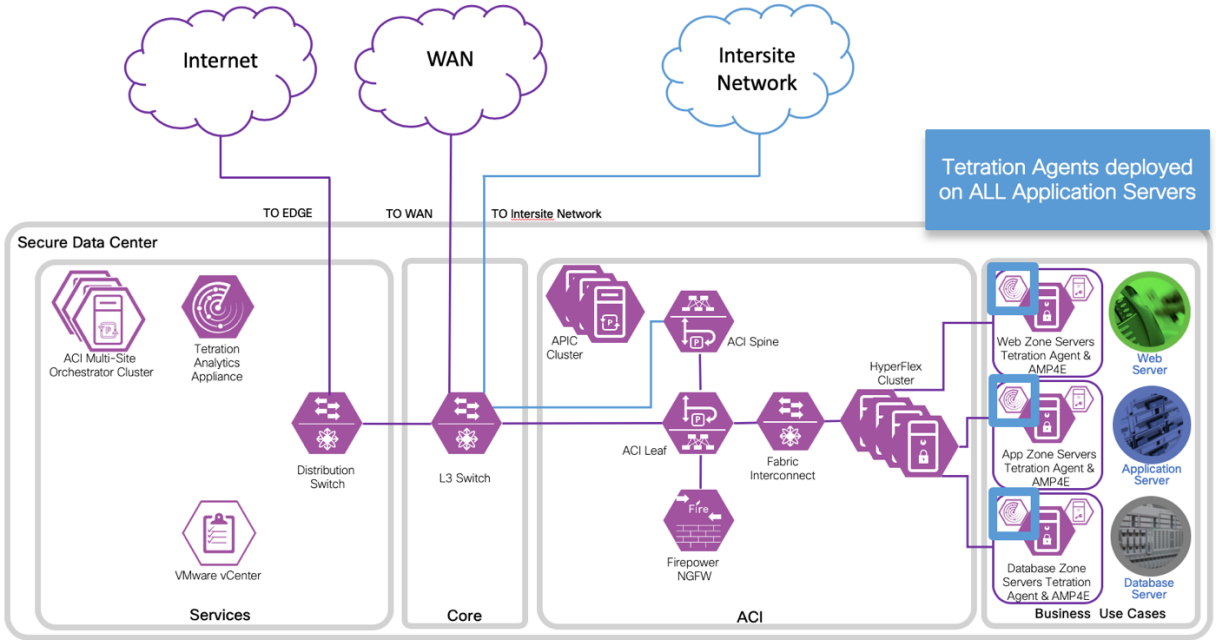
Test Case 3 – Tetration and VMware vCenter

There are three distinct parts to this integration:

- Attributes in VMware vCenter are the integrations that were tested. Tetration is using the vCenter API to learn VM attributes (name, customer tags). This will enable richer context for analysis in Tetration for vCenter. We will configure Tetration to pull in all these attributes from vCenter. The attributes are then used to construct an enforcement policy that will be pushed down to the Tetration agents running on the application servers. VMware vCenter 6.5 or later is required, we tested with 6.5.
- Encapsulated Remote Switched Port Analyzer (ERSPAN) is the ability for Tetration Analytics to receive SPAN data from vCenter. This is only needed if the Tetration agent is not supported by the server operating system and can't be deployed. We deployed Tetration agent on all our servers. Refer to https://<your-tetration-analytics-appliance-ip-address>/documentation/ui/appliances/erspan_vm.html for more details.
- NetFlow can also be enabled in the VMware vSphere Distributed Switch (VDS) to send to Tetration Analytics Appliance (TAA). Since we deployed Tetration agents on all application servers, we enabled NetFlow in VDS to provide visibility for Stealthwatch. You will need to setup a Cisco Tetration NetFlow Virtural Appliance to collect the NetFlow records for TAA. Refer to https://<your-tetration-analytics-appliance-ip-address>/documentation/ui/appliances/netflow_vm.html for more details. We have guidance in test cast 4 for how to enable NetFlow in VDS for ACI and in non-ACI environments that can be used to send to Cisco Tetration NetFlow Virtural Appliance. Refer to VMware vSphere Distributed Switch (VDS) and NetFlow section in Test Case 4.

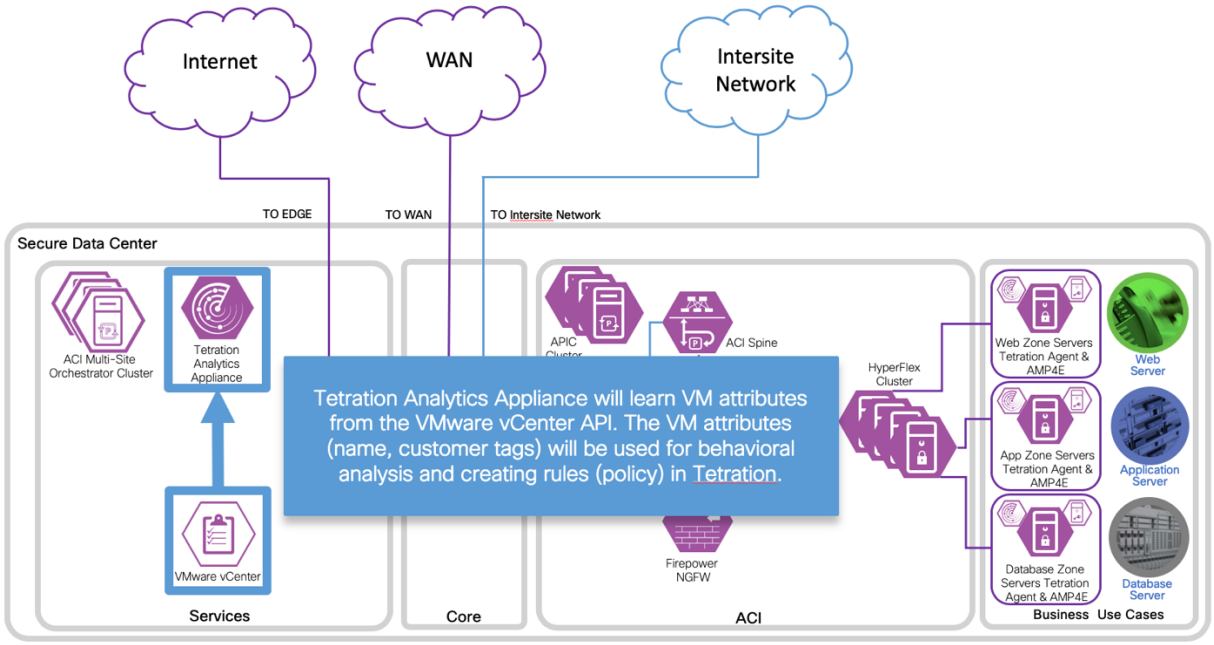
Test Description:

1. Tetration Agents will be deployed on all the application servers.

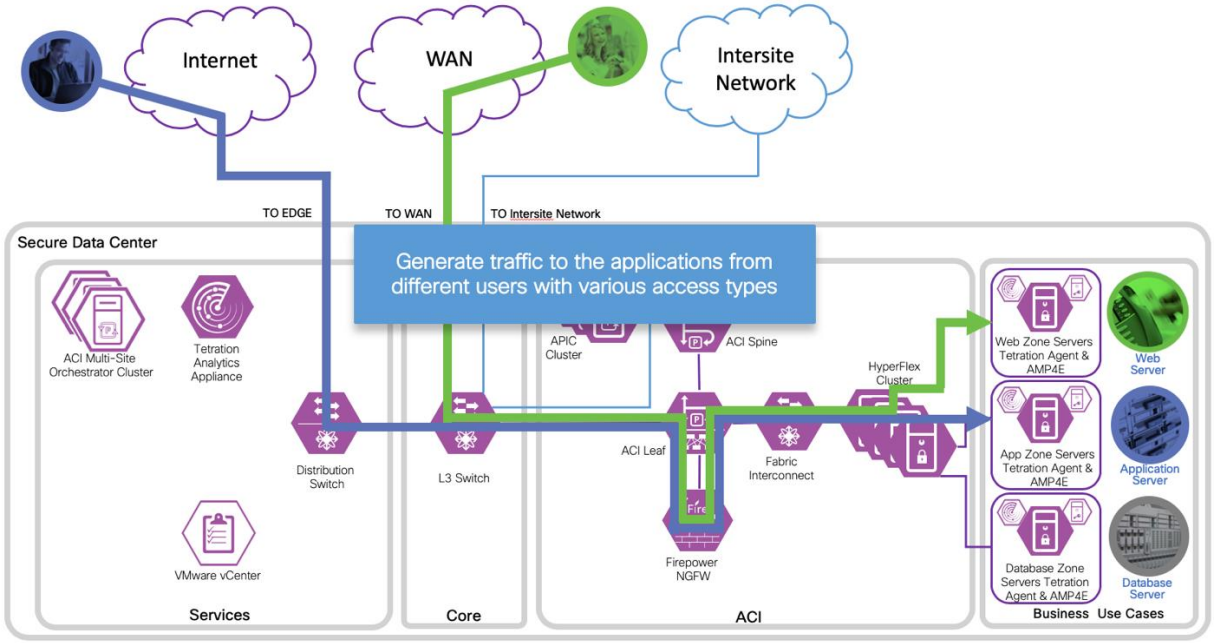


Return to Contents

2. Tetration Analytics Appliance will learn VM attributes from the VMware vCenter API. The VM attributes (name, customer tags) will be used for behavioral analysis and creating rules (policy).

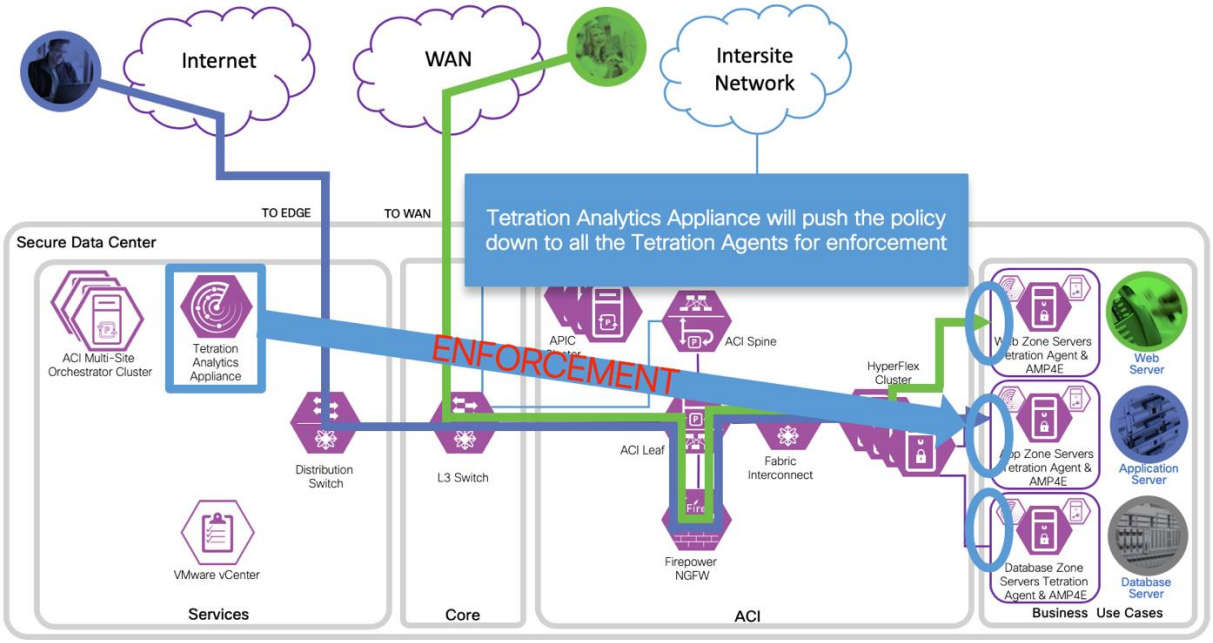


3. Generate traffic to the applications from different users with various access types (i.e. campus, branch, Internet). View the results of the behavior analysis on Tetration Analytics Appliance. Perform policy simulation before applying changes.



Return to Contents

4. Tetration Analytics Appliance will push the policy down to all the Tetration Agents for enforcement.



Implementation procedure

Step 1

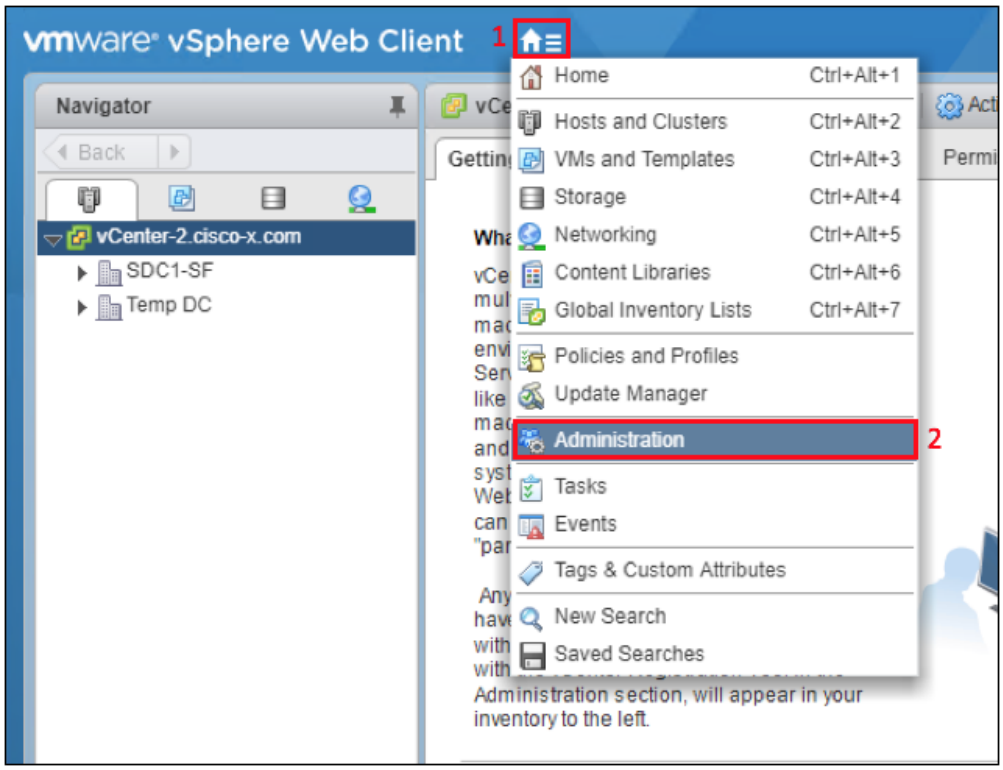
a. Deploy Tetration Agents on all application servers. We deployed multiple 3 tier applications in both sites. We deployed the Windows Sever 2016 and CentOS Linux 7.4 enforcement agents in all those 3 tier applications. We followed the documentation that is in the Tetration Analytics Appliance.

Deploying a Deep Visibility/Enforcement Linux Agent, https://<your-tetration-analytics-appliance-ip-address>/documentation/ui/software_agents/deployment.html#deploying-a-deep-visibility-enforcement-linux-agent.

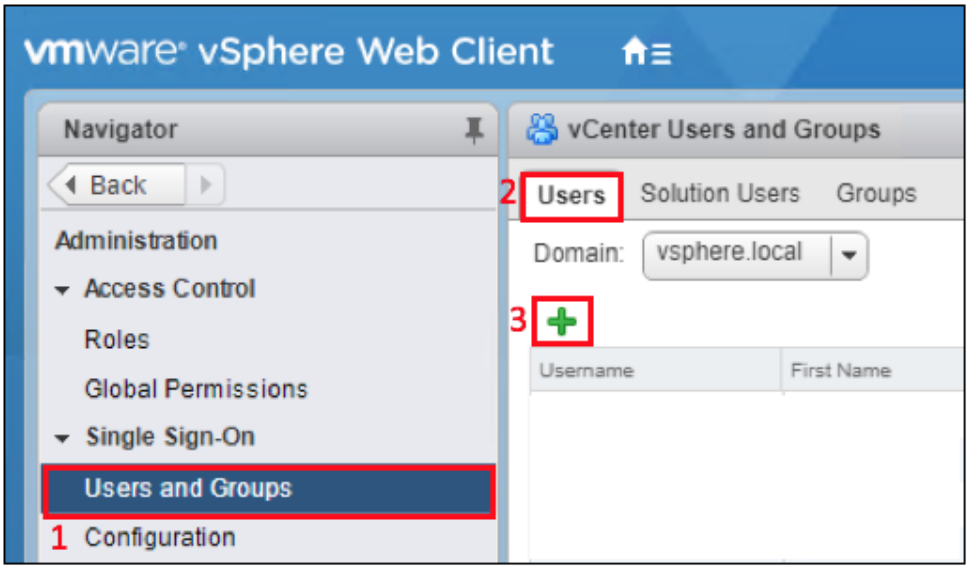
Deploying a Deep Visibility/Enforcement Windows Agent, https://<your-tetration-analytics-appliance-ip-address>/documentation/ui/software_agents/deployment.html#deploying-a-deep-visibility-enforcement-windows-agent.

Step 2

a. Setup Tetration Analytics Appliance and vCenter integration. In vCenter, create login credentials specifically for Tetration Analytics Appliance. In vCenter, navigate to Home (1)->Administration (2).

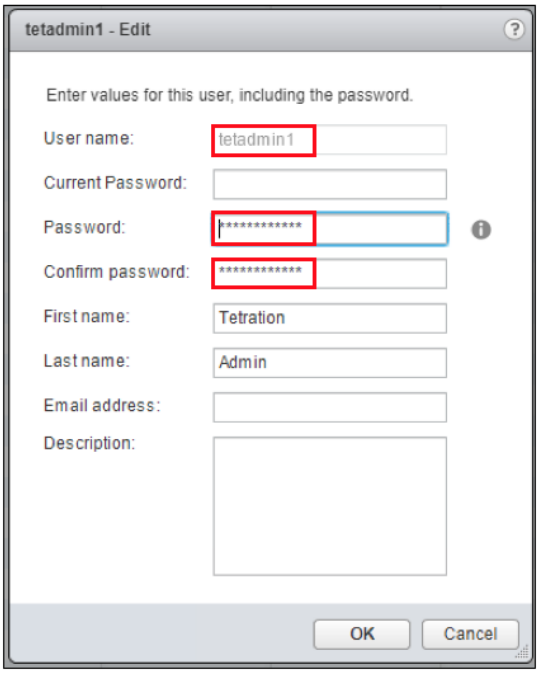


b. Add a User in vCenter. Navigate to Users and Groups (1)->Users (2) and select the plus sign (3) to add a new user.

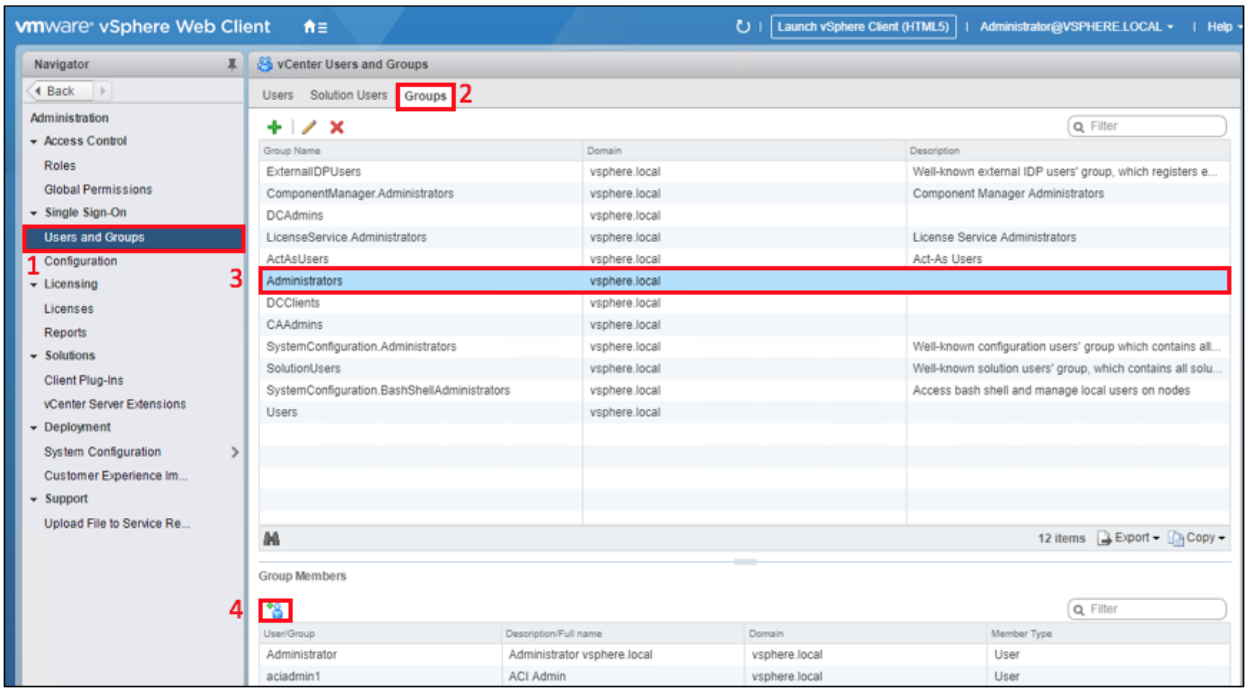


Return to Contents

c. Add a Tetration Analytics Appliance admin account. **Fill in Username, Password and Confirm password.**

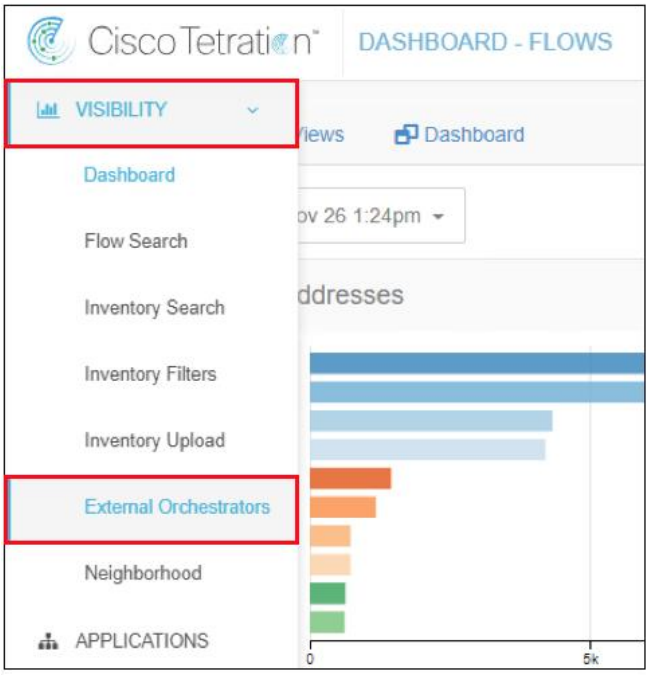


d. Add Tetration Analytics Appliance admin account tetadmin1 to the Administrators Group. Navigate to **Users and Groups (1)-> Groups (2)->Administrators (3) and select Add Group Member (4).**

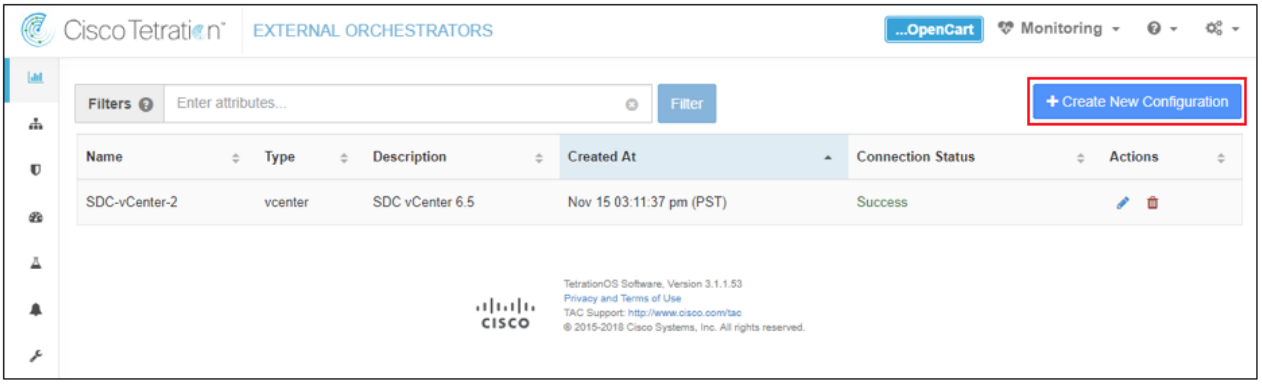


Return to Contents

e. Add External Orchestrator for vCenter in Tetration Analytics Appliance. Navigate to VISIBILITY->External Orchestrators.

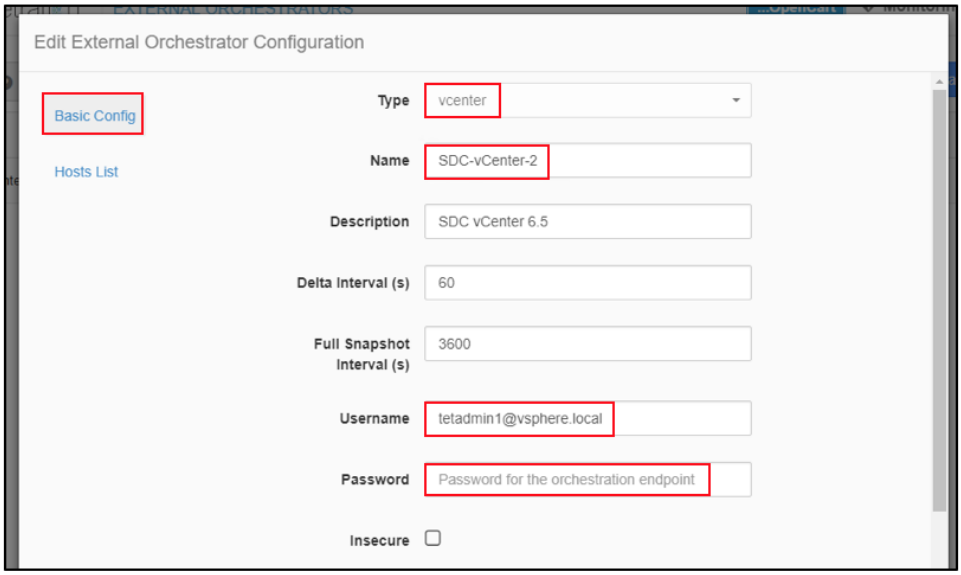


f. Select Create New Configuration



Return to Contents

g. In the Basic Config, **Select Type vcenter, Fill in the Name, Username and Password for vCenter**.

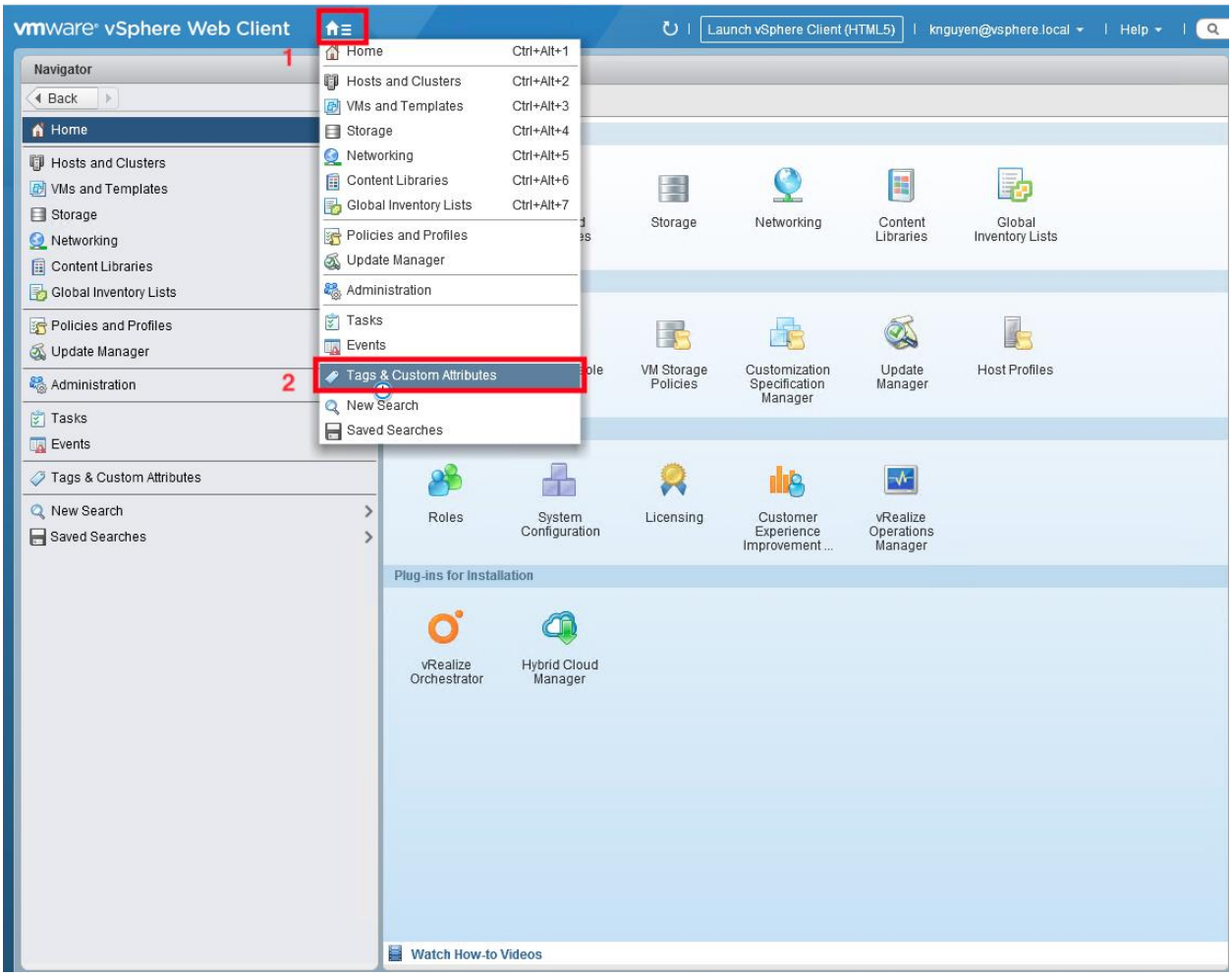


h. In the Hosts Lists, **Select the plus sign and enter the hostname (or IP address) and port**.

Return to Contents

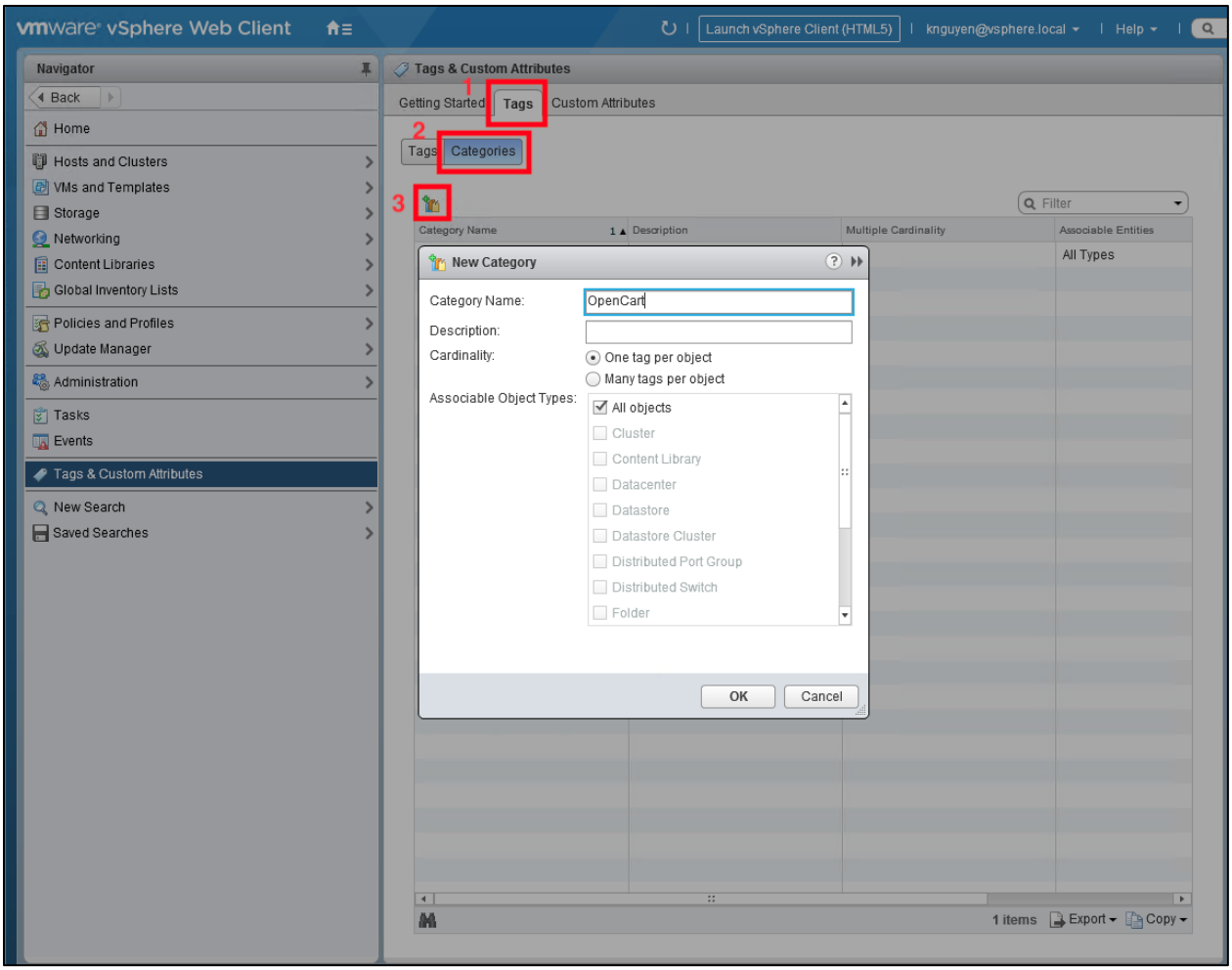
Step 3

a. Add Tags to application server VMs in vCenter. The Tags may already exist in a mature vCenter deployment, and you could use them in Step 4 to create the Scope. Connect to the vCenter portal. Navigate to Home (1) and Select Tags & Custom Attributes (2).



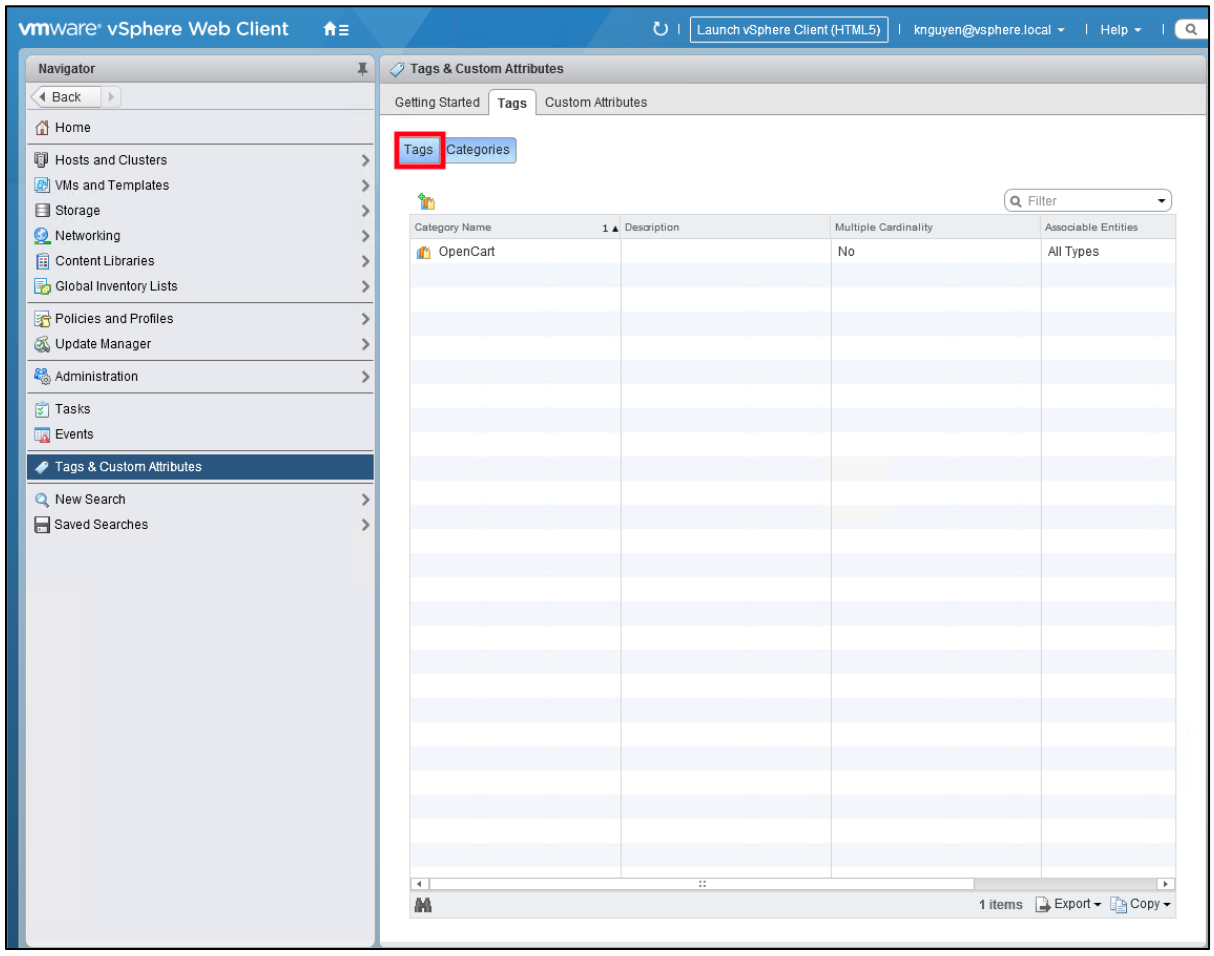
Return to Contents

b. Create Tags. Select **TAGS tab (1)**, select **Categories tab (2)**, select **New Category icon (3)** and complete the dialog box to complete the **OpenCart** Category.



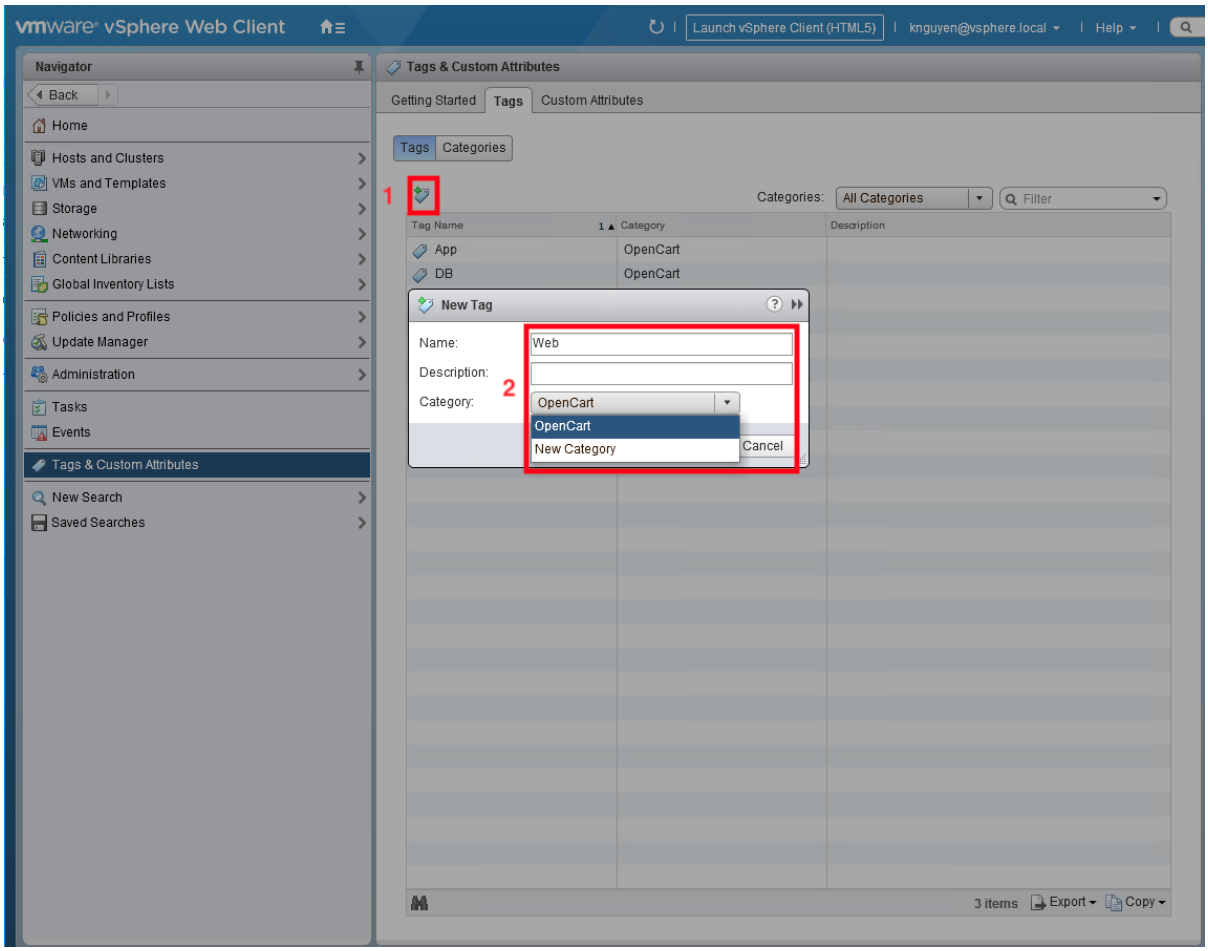
Return to Contents

c. Select **Tags tab**.



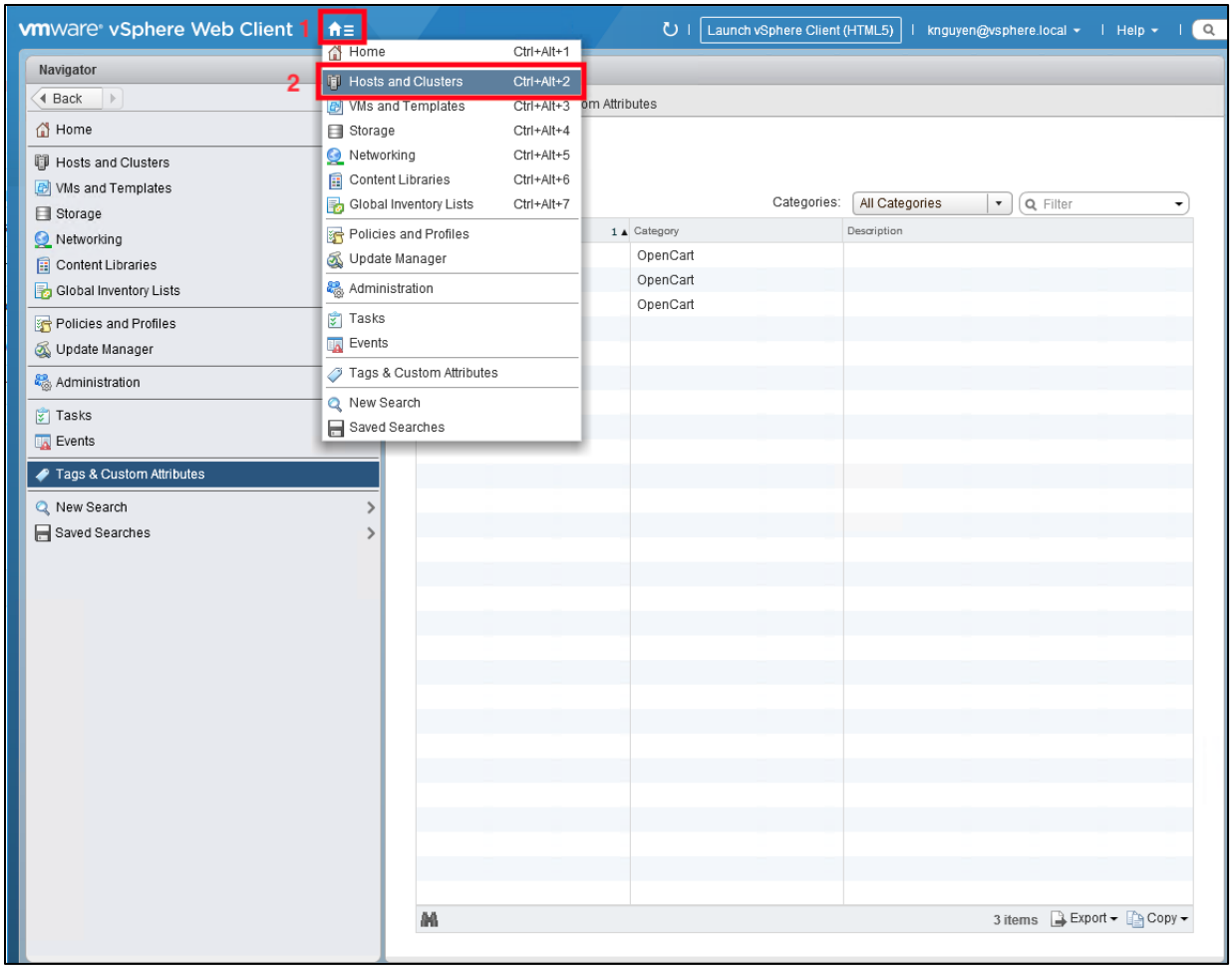
Return to Contents

d. Select **New Tag Icon (1)**. In the **New Tag dialog box (2)**, fill in the **Tag name** and select the **Category** previously created. We created Tags for Web, App and DB.



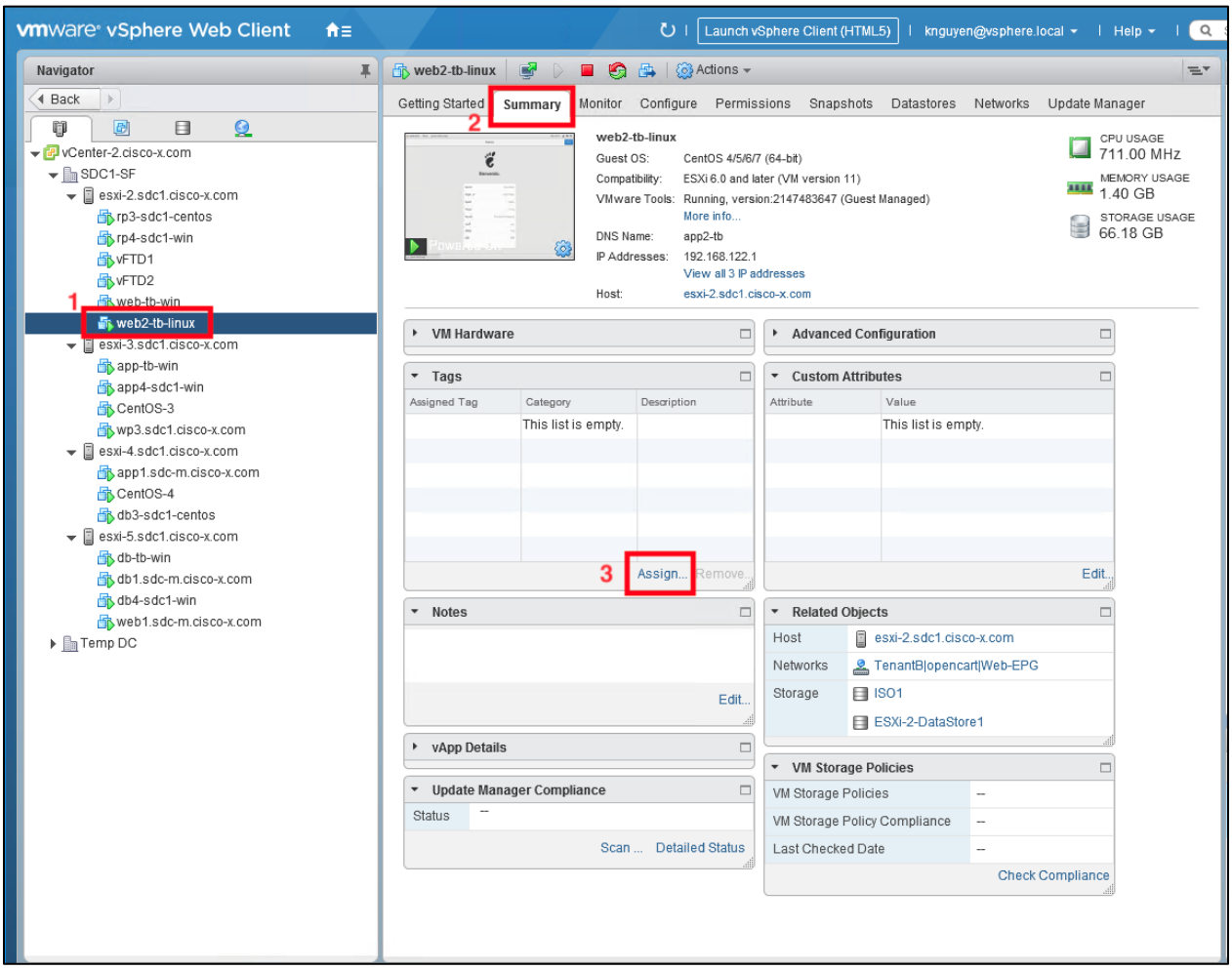
Return to Contents

e. Apply the Tags to the Hosts. Select **Home (1)** and **Hosts and Clusters (2)**.



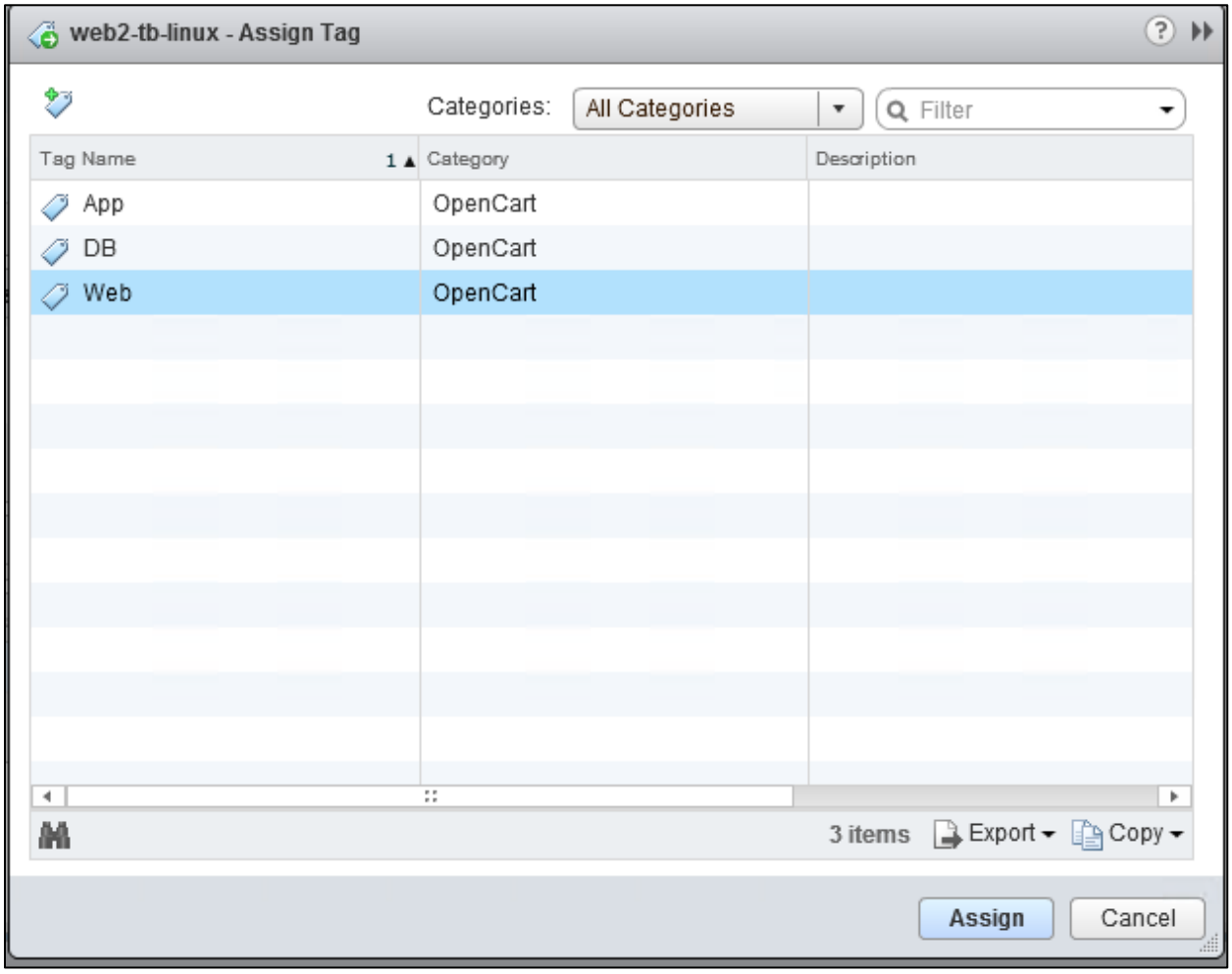
Return to Contents

f. Select the **host to tag in the left pane (1)** and then select the **Summary tab (2)**. In the Tags pane, select **Assign… (3)**.



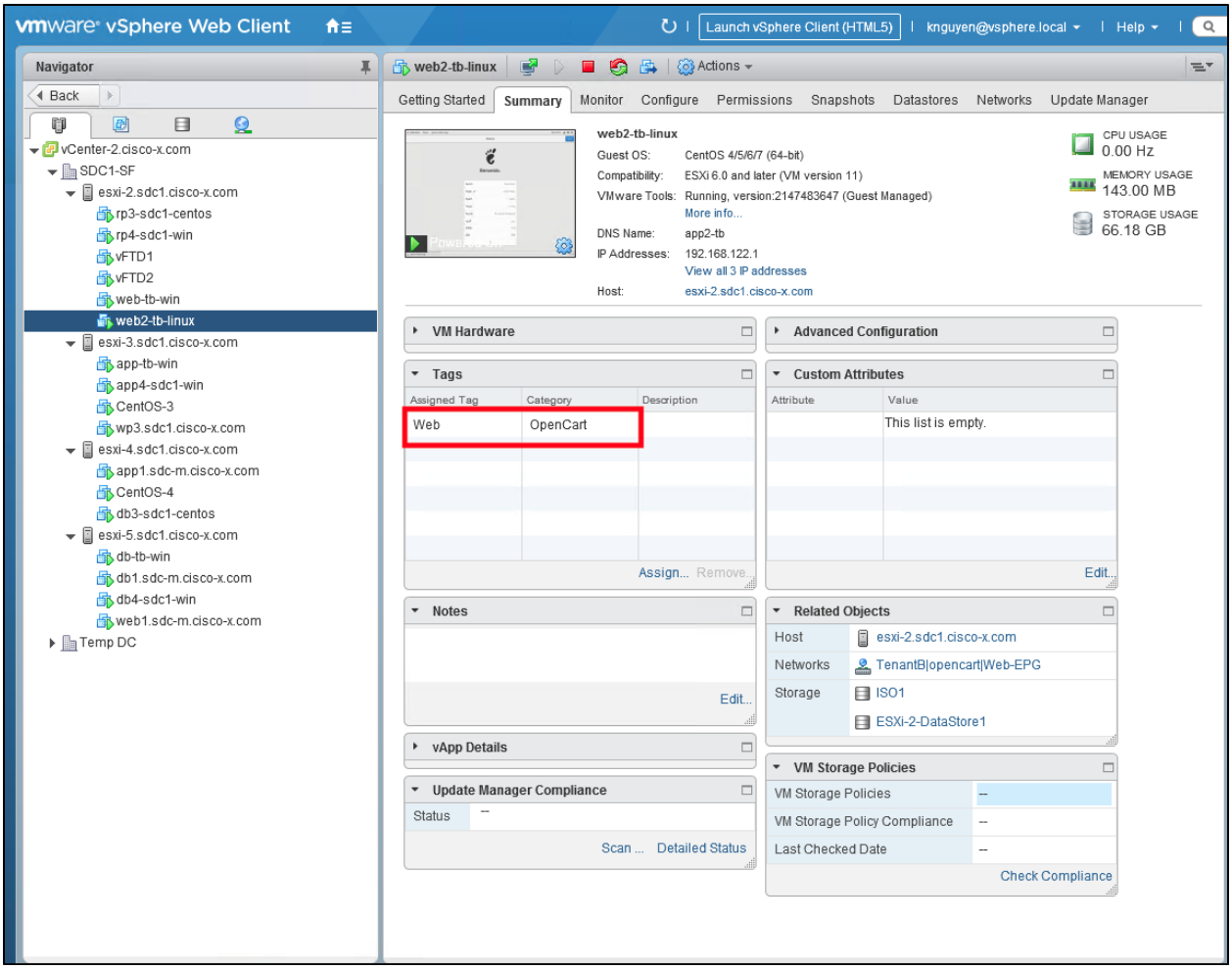
Return to Contents

g. In the Assign Tag dialog box, select the **tag to assign** and then select **Assign**. In this case we assigned the Web tag to the web2-tb-linux host.

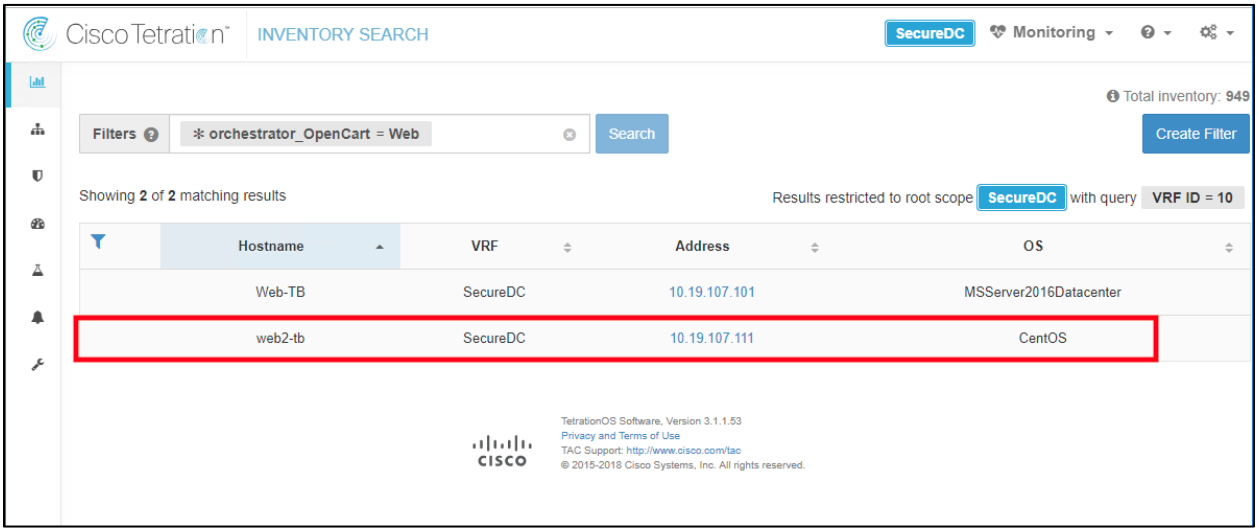


Return to Contents

h. Below is the result of assigning a Tag to the host.



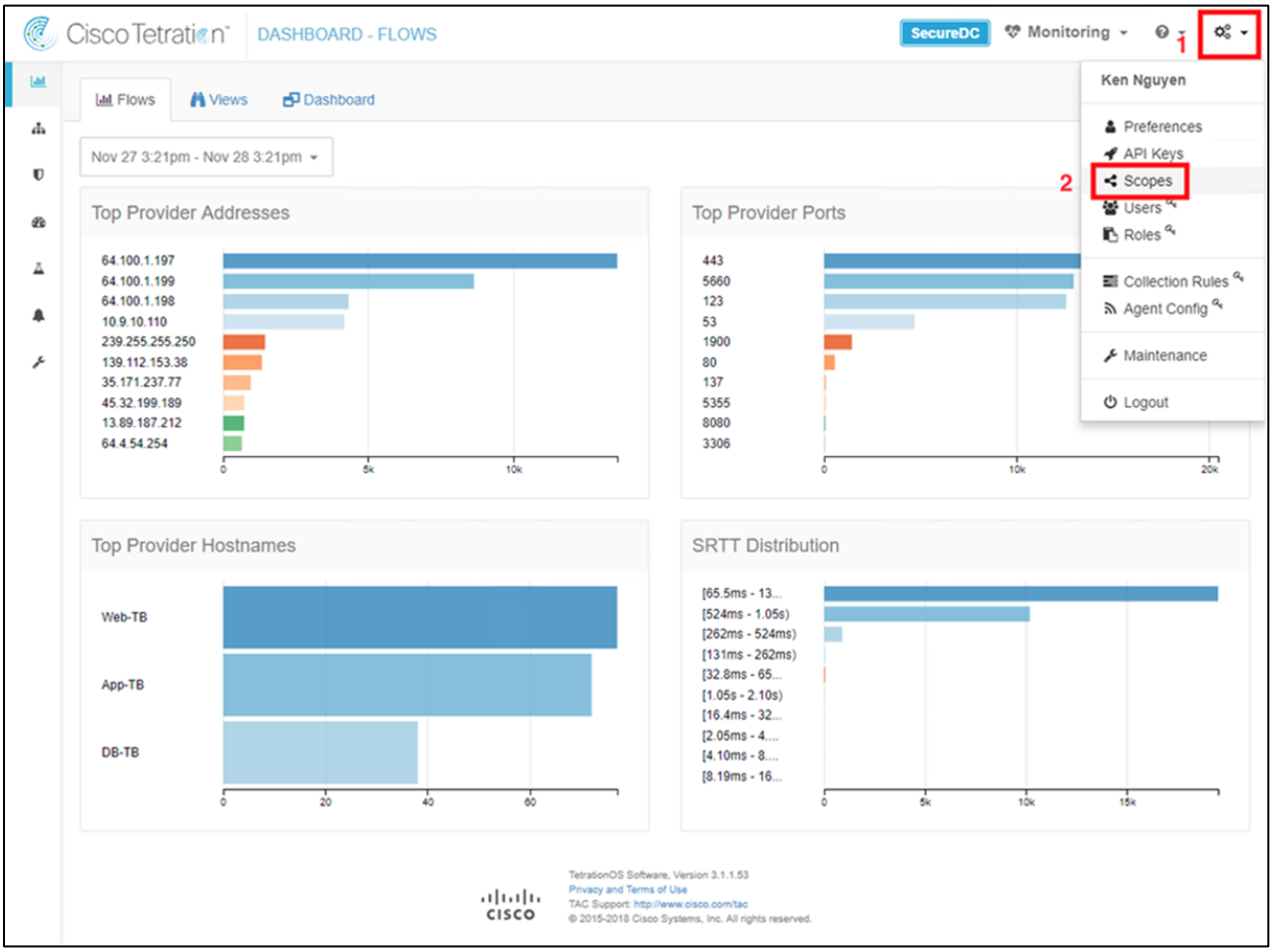
i. The tag will appear in Tetration in a few minutes. Below is a simple inventory search using the VM tag.



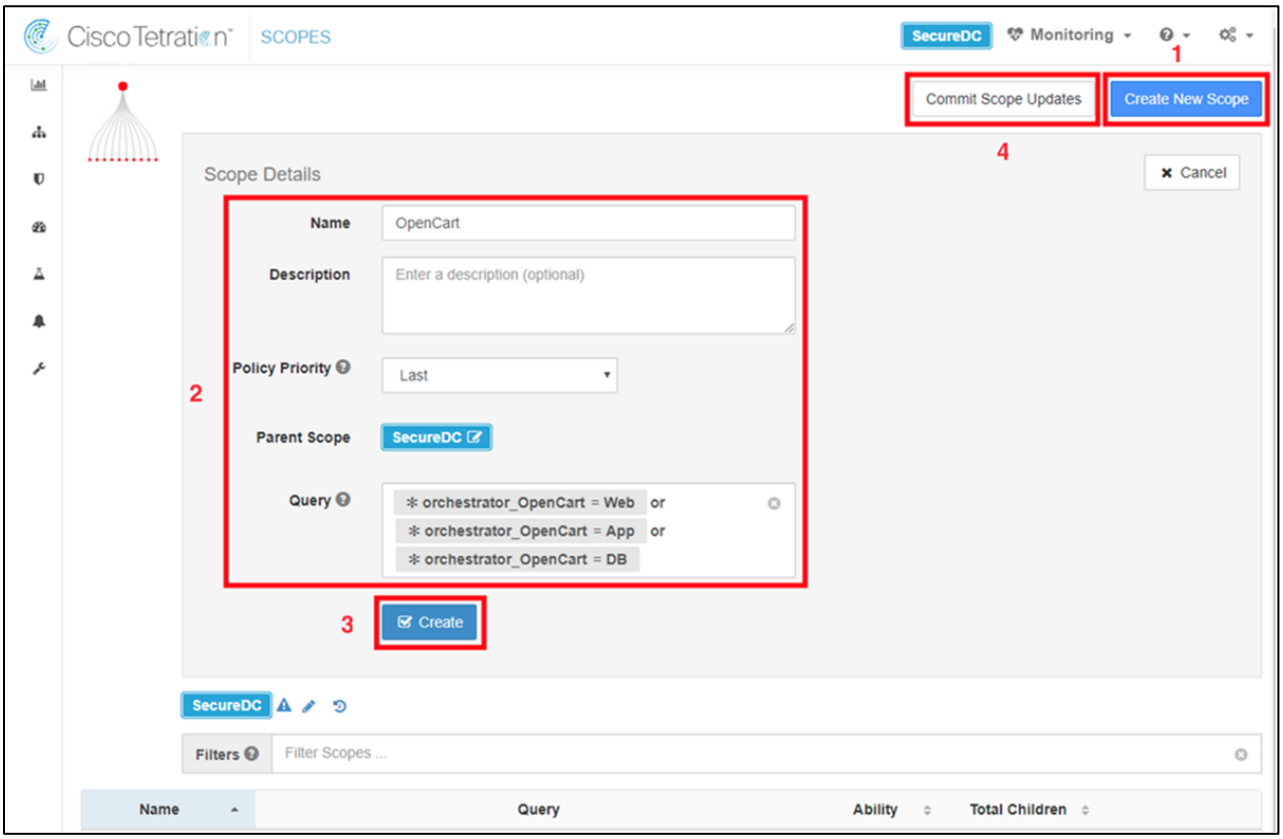
Return to Contents

Step 4

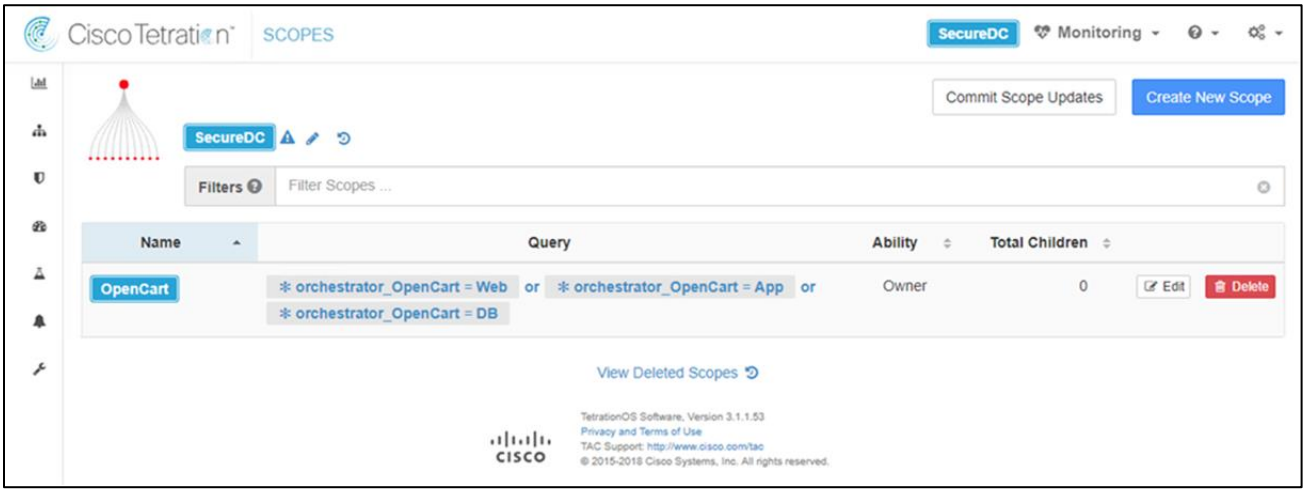
a. Create a new Scope. Select the **Gears icon in the upper right corner (1)** and select **Scopes (2)**.



b. Select **Create New Scope (1)** and the Scope Details dialog box will appear. Fill in the **Scope Details (2) with the Name, Policy Priority, and Query and select Create**. The query is selecting all vCenter VMs that are tagged with the Web, App or DB attribute. Select **Commit Scope Updates (4)**.

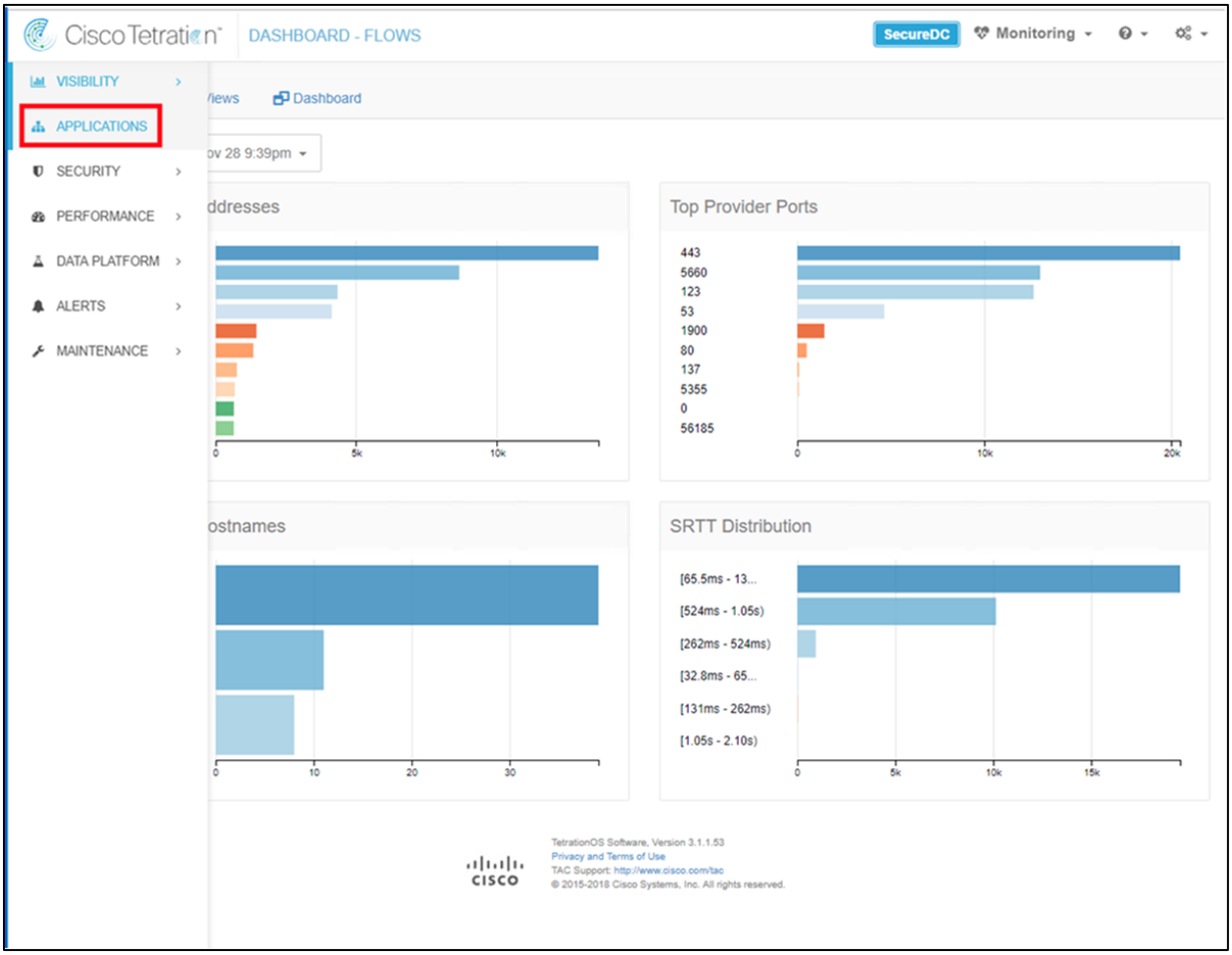


c. View the Scope created called **OpenCart**.

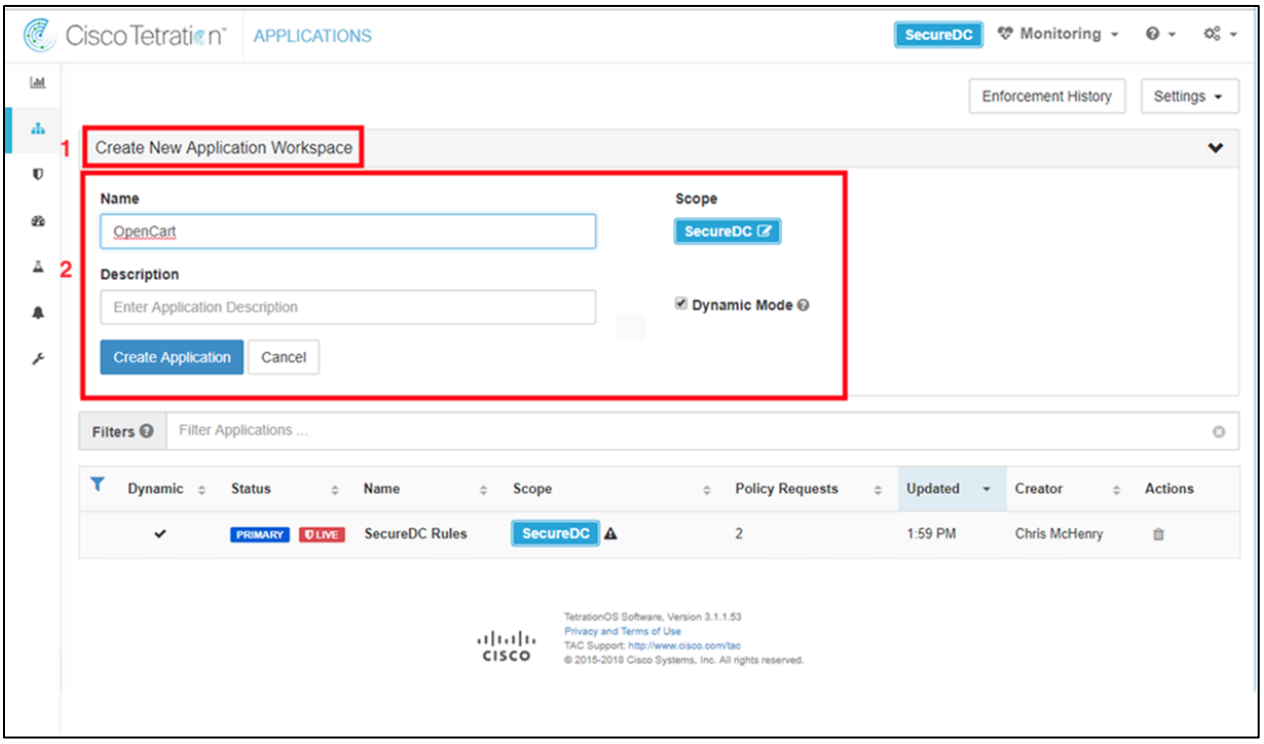


Step 5

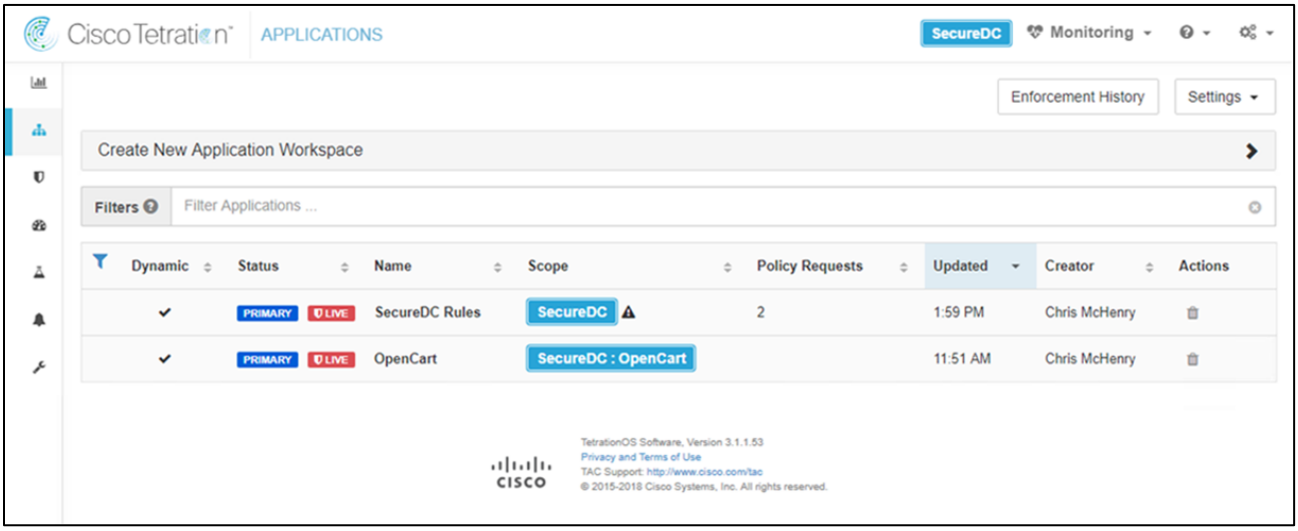
a. Create a new Application Workspace. Navigate to **Applications**.



b. Click the **Create New Application Workspace (1)** and the dialog box will appear. Fill in the Application Name and select **Create Application. (2)**.



c. View the Application Workspace created called **OpenCart**.

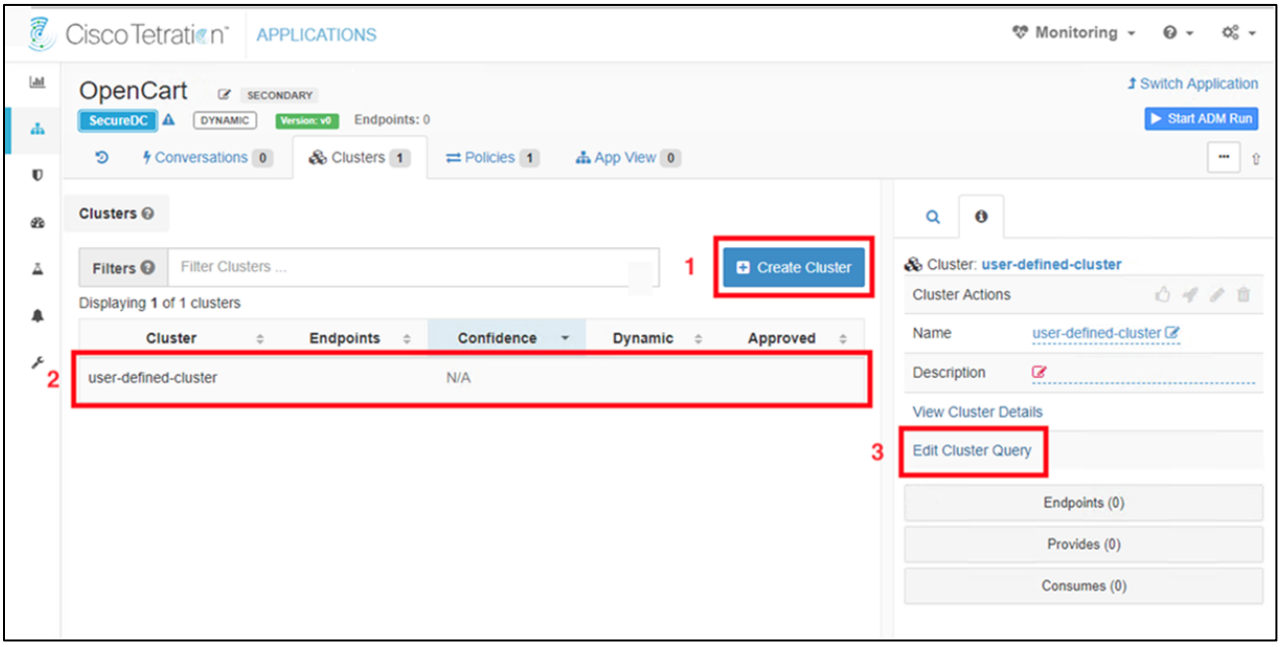


Return to Contents

Step 6

a. Create a new Cluster. From the Applications screen, double click on Application OpenCart.

b. Select Create Cluster (1). A cluster **user-defined-cluster** (2) is created. Click **Edit Cluster Query (3)** to define a query.

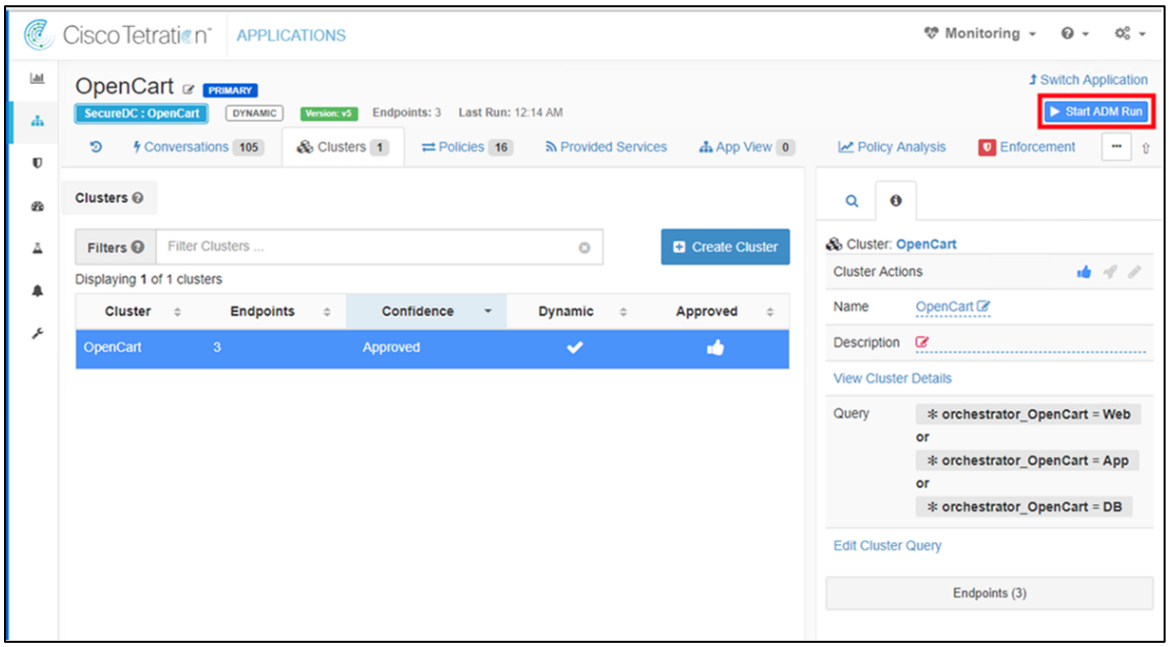


a. The query dialog box will appear, provide the name and query parameters. **TIP:** Click the ? next to Query for available options. Select **Save** when done. **Note:** The query must specify the VM tag since wildcarding the VM tag for example **orchestrator_opencart=*** is not supported.

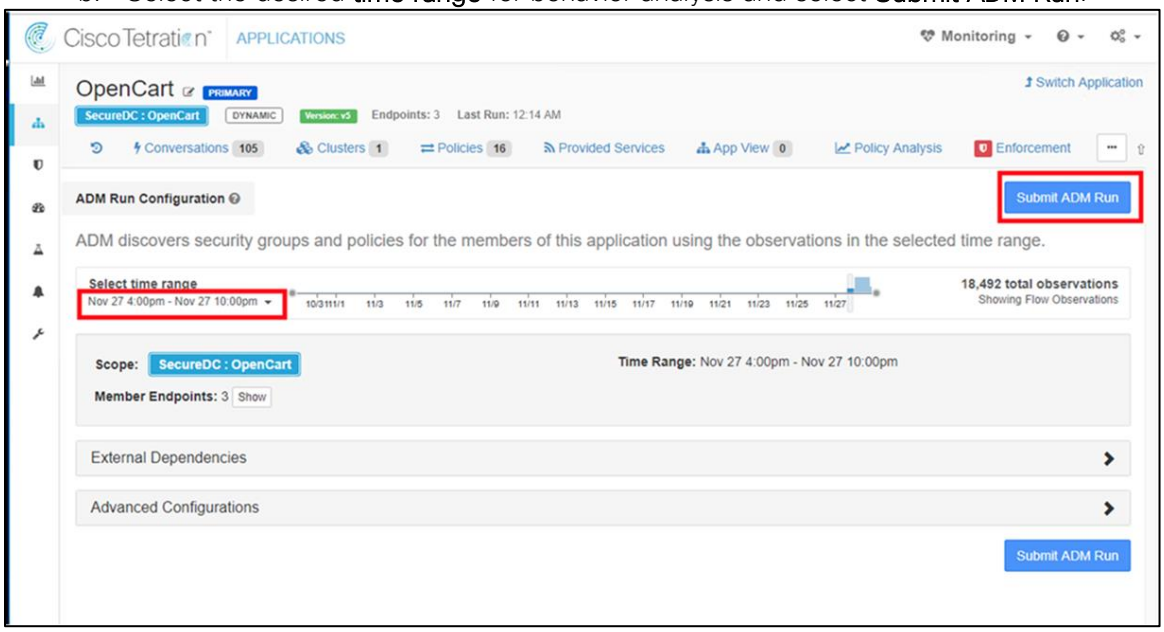
Return to Contents

Step 7

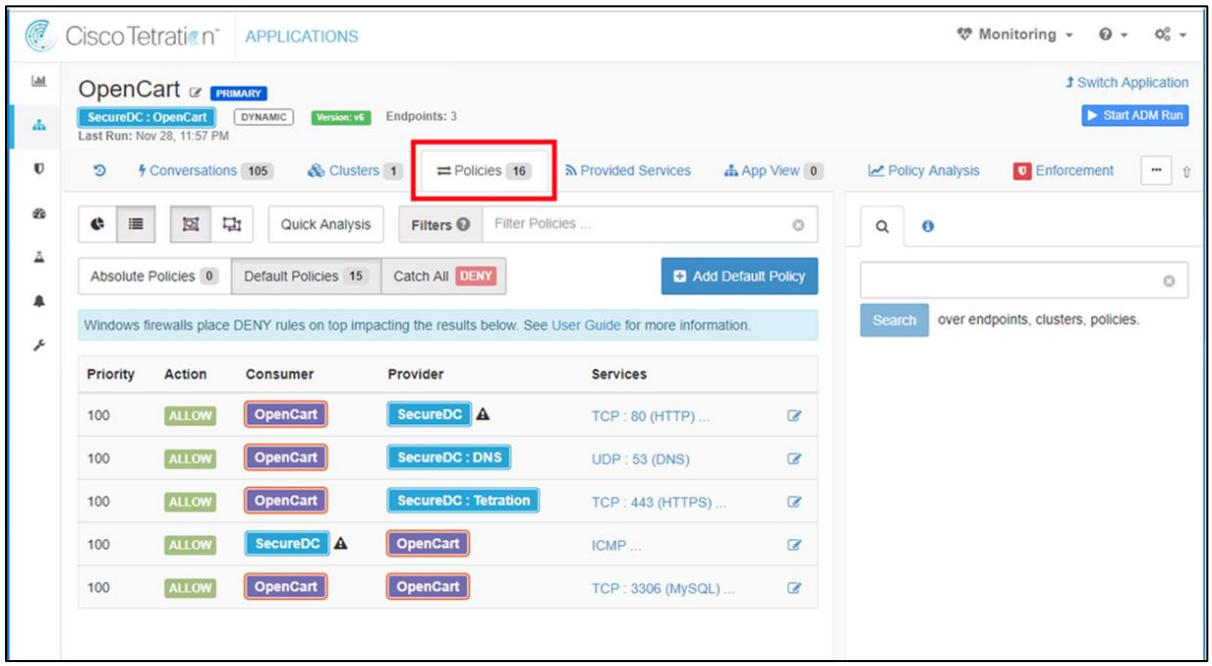
a. Start Application Dependency Mapping (ADM) Run. ADM is the behavior analysis process to analyze the traffic recorded by Tetration Analytics Appliance. In a test environment, it is important that you generate typical traffic for the hosts being analyzed prior to running ADM. Rules will be created based on observed traffic.



b. Select the desired time range for behavior analysis and select Submit ADM Run.

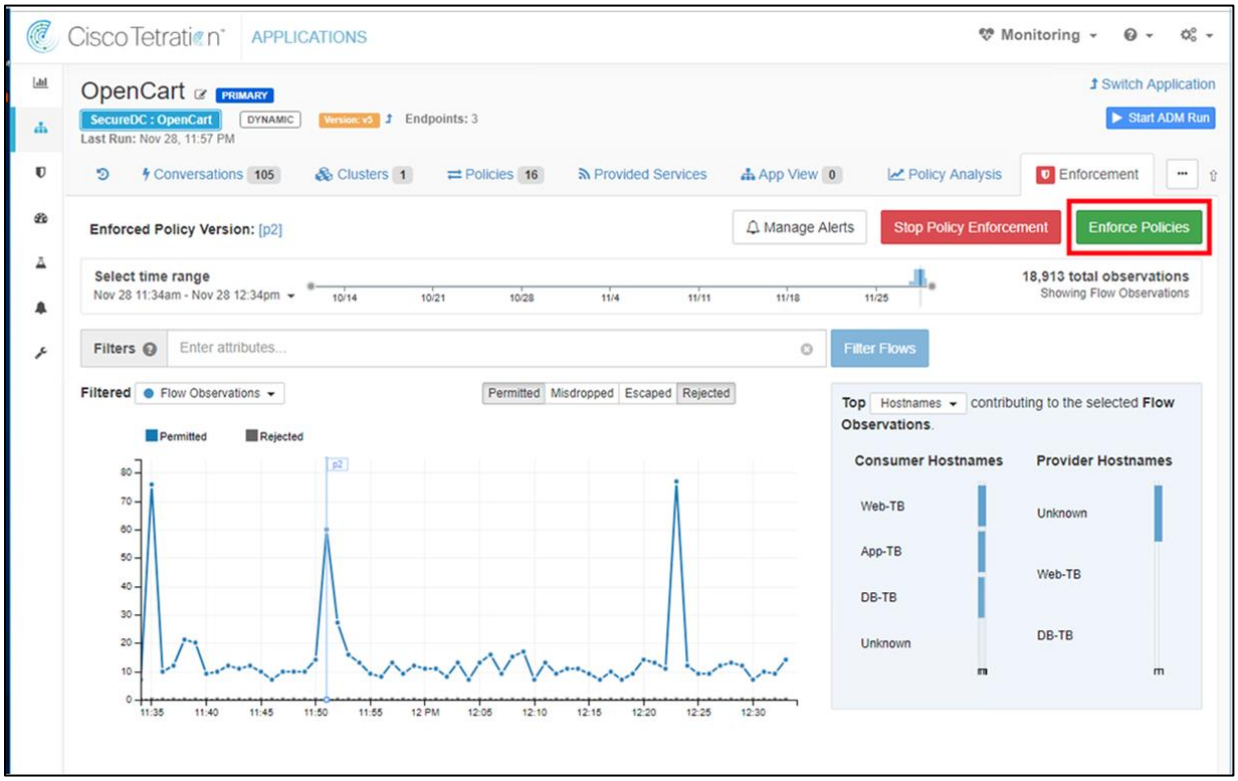


c. After the Run is complete, view the policies by selecting the **Policies** tab.



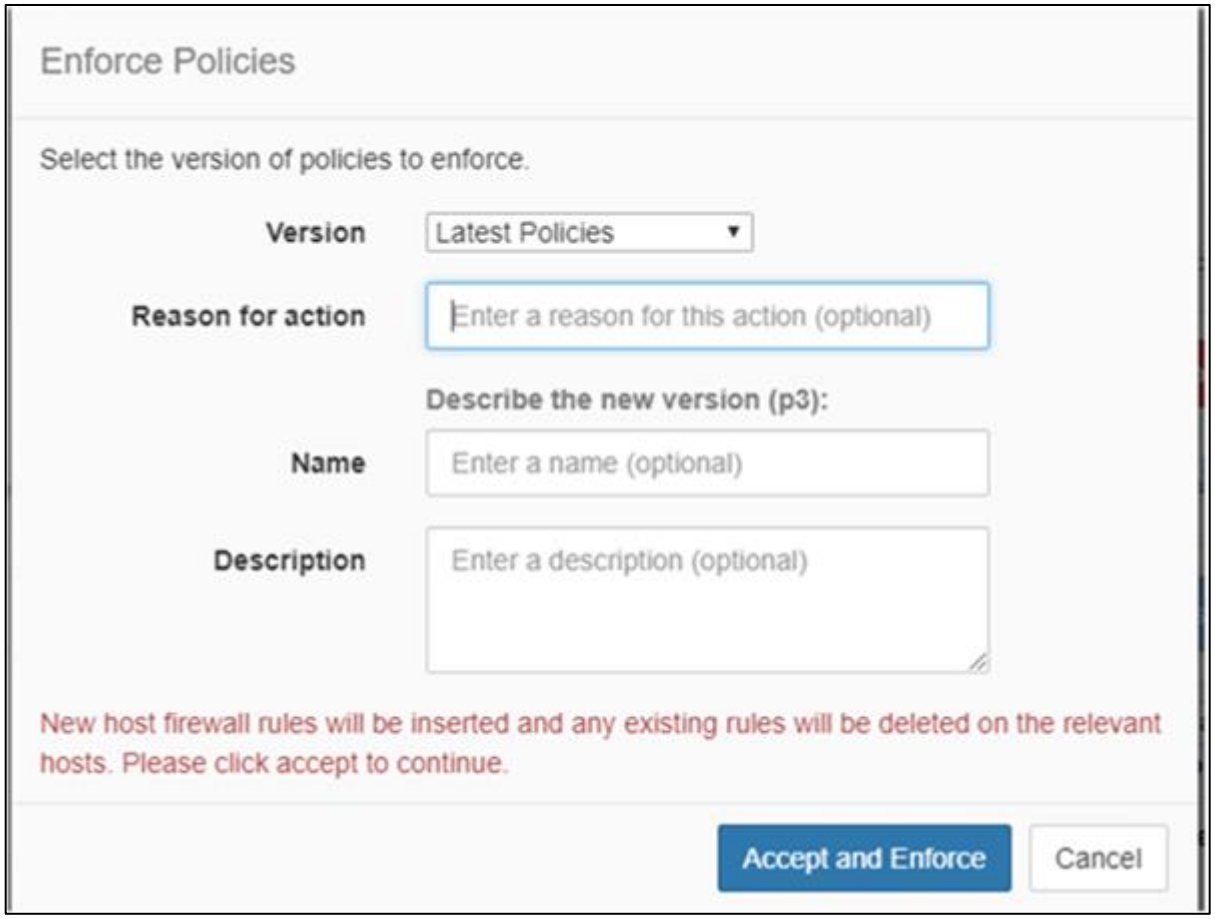
Step 8

a. Once you review the Default Policies created by ADM and determine that is the desired enforcement policy, Select **Enforcement tab** and then **Enforce Policies**.



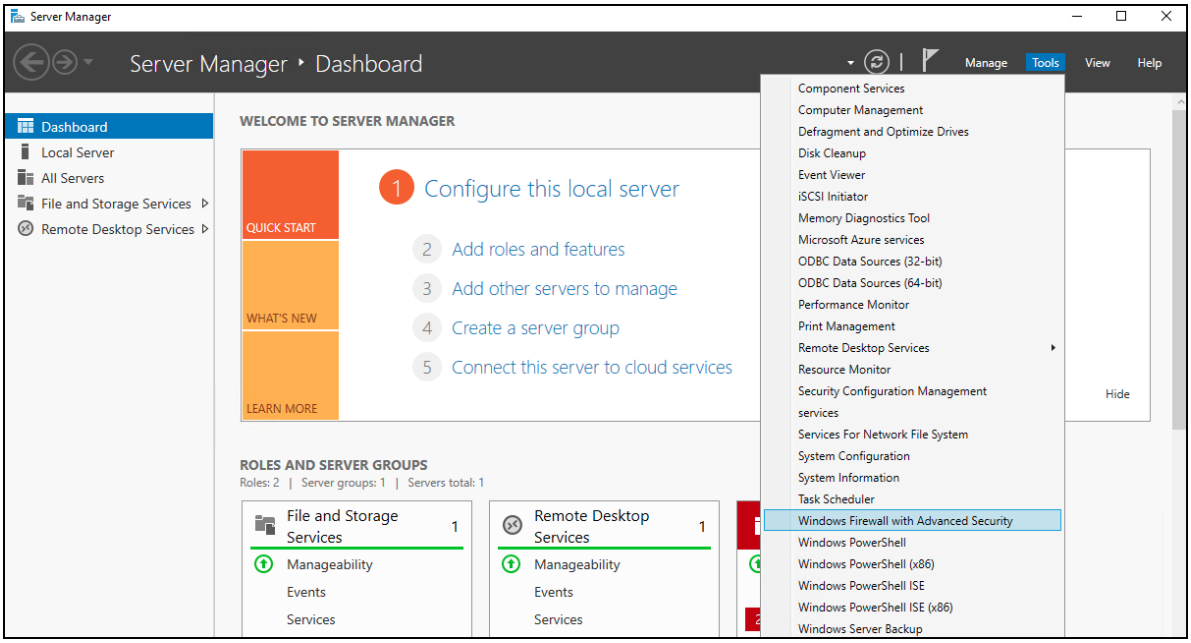
Return to Contents

b. Completed the dialog box and select Accept and Enforce.



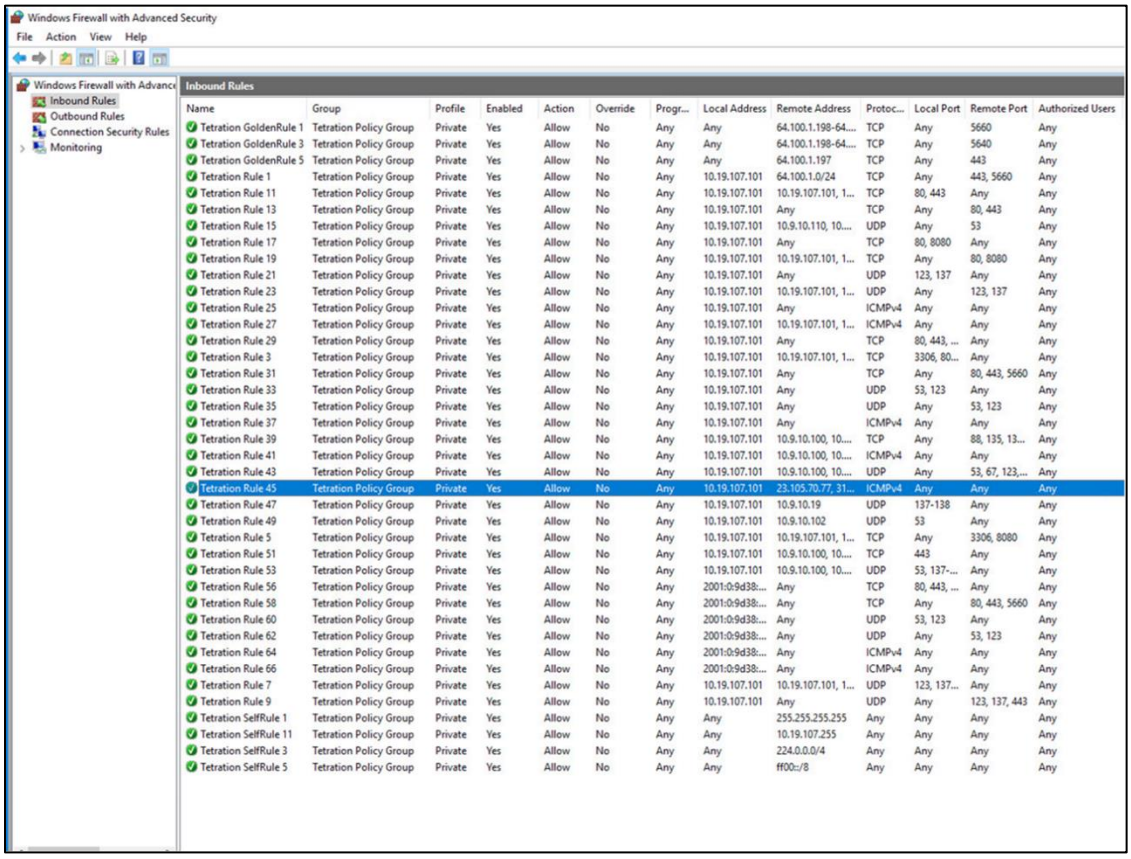
Step 9

a. For Windows Server hosts, verify that the Windows firewall is enforcing the policies. On Server Manager Dashboard, select **Tools** and **Windows Firewall with Advanced Security**.



Return to Contents

b. View the enforcement rules Tetration pushed down in the Inbound and Outbound Rules. All the rules will be prefixed with “Tetration”



Name	Group	Profile	Enabled	Action	Override	Progr...	Local Address	Remote Address	Protoc...	Local Port	Remote Port	Authorized Users
Tetration GoldenRule 1	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	64.100.1.198-64....	TCP	Any	5660	Any
Tetration GoldenRule 3	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	64.100.1.198-64....	TCP	Any	5640	Any
Tetration GoldenRule 5	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	64.100.1.197	TCP	Any	443	Any
Tetration Rule 1	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	64.100.1.0/24	TCP	Any	443, 5660	Any
Tetration Rule 11	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.19.107.101, 1...	TCP	80, 443	Any	Any
Tetration Rule 13	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	TCP	Any	80, 443	Any
Tetration Rule 15	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.110, 10....	UDP	Any	53	Any
Tetration Rule 17	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	TCP	80, 8080	Any	Any
Tetration Rule 19	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.19.107.101, 1...	TCP	Any	80, 8080	Any
Tetration Rule 21	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	UDP	123, 137	Any	Any
Tetration Rule 23	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.19.107.101, 1...	UDP	Any	123, 137	Any
Tetration Rule 25	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	ICMPv4	Any	Any	Any
Tetration Rule 27	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.19.107.101, 1...	ICMPv4	Any	Any	Any
Tetration Rule 29	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	TCP	80, 443, ...	Any	Any
Tetration Rule 3	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.19.107.101, 1...	TCP	3306, 80...	Any	Any
Tetration Rule 31	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	TCP	Any	80, 443, 5660	Any
Tetration Rule 33	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	UDP	53, 123	Any	Any
Tetration Rule 35	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	UDP	Any	53, 123	Any
Tetration Rule 37	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	ICMPv4	Any	Any	Any
Tetration Rule 39	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.100, 10....	TCP	Any	88, 135, 13...	Any
Tetration Rule 41	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.100, 10....	ICMPv4	Any	Any	Any
Tetration Rule 43	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.100, 10....	UDP	Any	53, 67, 123,...	Any
Tetration Rule 45	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	23.105.70.77, 31...	ICMPv4	Any	Any	Any
Tetration Rule 47	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.19	UDP	137-138	Any	Any
Tetration Rule 49	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.102	UDP	53	Any	Any
Tetration Rule 5	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.19.107.101, 1...	TCP	Any	3306, 8080	Any
Tetration Rule 51	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.100, 10....	TCP	443	Any	Any
Tetration Rule 53	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.9.10.100, 10....	UDP	53, 137-...	Any	Any
Tetration Rule 56	Tetration Policy Group	Private	Yes	Allow	No	Any	2001:0:9d38:...	Any	TCP	80, 443, ...	Any	Any
Tetration Rule 58	Tetration Policy Group	Private	Yes	Allow	No	Any	2001:0:9d38:...	Any	TCP	Any	80, 443, 5660	Any
Tetration Rule 60	Tetration Policy Group	Private	Yes	Allow	No	Any	2001:0:9d38:...	Any	UDP	53, 123	Any	Any
Tetration Rule 62	Tetration Policy Group	Private	Yes	Allow	No	Any	2001:0:9d38:...	Any	UDP	Any	53, 123	Any
Tetration Rule 64	Tetration Policy Group	Private	Yes	Allow	No	Any	2001:0:9d38:...	Any	ICMPv4	Any	Any	Any
Tetration Rule 66	Tetration Policy Group	Private	Yes	Allow	No	Any	2001:0:9d38:...	Any	ICMPv4	Any	Any	Any
Tetration Rule 7	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	10.19.107.101, 1...	UDP	123, 137...	Any	Any
Tetration Rule 9	Tetration Policy Group	Private	Yes	Allow	No	Any	10.19.107.101	Any	UDP	Any	123, 137, 443	Any
Tetration SelfRule 1	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	255.255.255.255	Any	Any	Any	Any
Tetration SelfRule 11	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	10.19.107.255	Any	Any	Any	Any
Tetration SelfRule 3	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	224.0.0.0/4	Any	Any	Any	Any
Tetration SelfRule 5	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	ff00::/8	Any	Any	Any	Any

Step 10

a. For Cent-OS Linux hosts, verify Cent-OS firewall is enforcing the policies as expected. Issue the “iptables -S” command to see the policy pushed by Tetration Analytics Appliance. All rules will be prefixed “TA_” prefix.

```
[root@web2-tb ~]# iptables -S
-P INPUT DROP
-P FORWARD ACCEPT
-P OUTPUT DROP
-N TA_CAST
-N TA_DROP
-N TA_GOLDEN_INPUT
-N TA_GOLDEN_OUTPUT
-N TA_INPUT
-N TA_OUTPUT
-A INPUT -j TA_GOLDEN_INPUT
-A INPUT -j TA_INPUT
-A INPUT -j TA_CAST
-A INPUT -j NFLOG --nflog-group 50880
-A OUTPUT -j TA_GOLDEN_OUTPUT
-A OUTPUT -j TA_OUTPUT
-A OUTPUT -j TA_CAST
-A OUTPUT -j NFLOG --nflog-group 50880
-A TA_CAST -m addrtype --dst-type BROADCAST -j ACCEPT
-A TA_CAST -m addrtype --dst-type MULTICAST -j ACCEPT
-A TA_CAST -j RETURN
-A TA_DROP -j NFLOG --nflog-group 50660
-A TA_DROP -j DROP
-A TA_GOLDEN_INPUT -i lo -j ACCEPT
-A TA_GOLDEN_INPUT -p tcp -m set --match-set ta_b11a75d589e301459a6fb909ff60 src -m multiport --sports 5660 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A TA_GOLDEN_INPUT -p tcp -m set --match-set ta_f5a83dd0cb816615ab0dd908e43e src -m multiport --sports 5640 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A TA_GOLDEN_INPUT -p tcp -m set --match-set ta_61ce598c76a8d629f3a8288b461d src -m multiport --sports 443 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A TA_GOLDEN_INPUT -j RETURN
-A TA_GOLDEN_OUTPUT -o lo -j ACCEPT
-A TA_GOLDEN_OUTPUT -p tcp -m set --match-set ta_b11a75d589e301459a6fb909ff60 dst -m multiport --dports 5660 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A TA_GOLDEN_OUTPUT -p tcp -m set --match-set ta_f5a83dd0cb816615ab0dd908e43e dst -m multiport --dports 5640 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A TA_GOLDEN_OUTPUT -p tcp -m set --match-set ta_61ce598c76a8d629f3a8288b461d dst -m multiport --dports 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A TA_GOLDEN_OUTPUT -j RETURN
-A TA_INPUT -p tcp -m set --match-set ta_4327ad3e3a2174b2acd49d6266c2 src -m set --match-set ta_d39506a842bc089e9657d81b9a5f dst -m multiport --sports 443,5660 -m conntrack --ctstate ESTABLISHED -m comment --comment "PolicyId=5bfef1a9497d4f422fdef82d" -j ACCEPT
-A TA_INPUT -p tcp -m set --match-set ta_a8312b0bf8e54ca326c9291073b2 src -m set --match-set ta_d39506a842bc089e9657d81b9a5f dst -m multiport --dports 3306,8080 -m conntrack --ctstate NEW,ESTABLISHED -m comment --comment "PolicyId=5bfef1a9497d4f422fdef82b" -j ACCEPT
```

↩ Return to Contents

Test Case 4 – Stealthwatch and Tetration

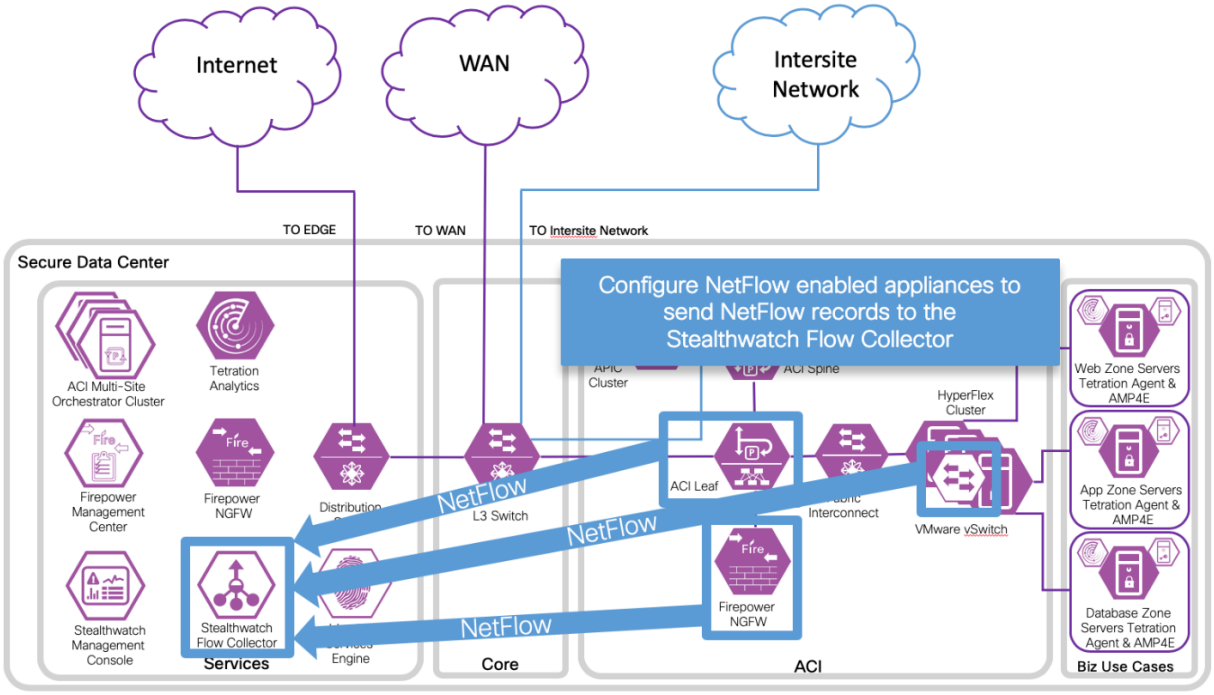
The “pivot” or “cross launch” from Stealthwatch to Tetration was tested and the details of the implementation are provided. This integration also involved enabling the sending of NetFlow records on data center appliances to Stealthwatch Flow Collector. NetFlow was enabled on the VMware vSphere Distributed Switch (VDS), Nexus 9300 switches and Firepower Threat Defense in the secure data center design.

About NetFlow

The NetFlow technology provides the metering base for a key set of applications, including network traffic accounting, usage-based network billing, network planning, as well as denial of services monitoring, network monitoring, outbound marketing, and data mining for both service providers and enterprise customers. Cisco provides a set of NetFlow applications to collect NetFlow export data, perform data volume reduction, perform post-processing, and provide end-user applications with easy access to NetFlow data.

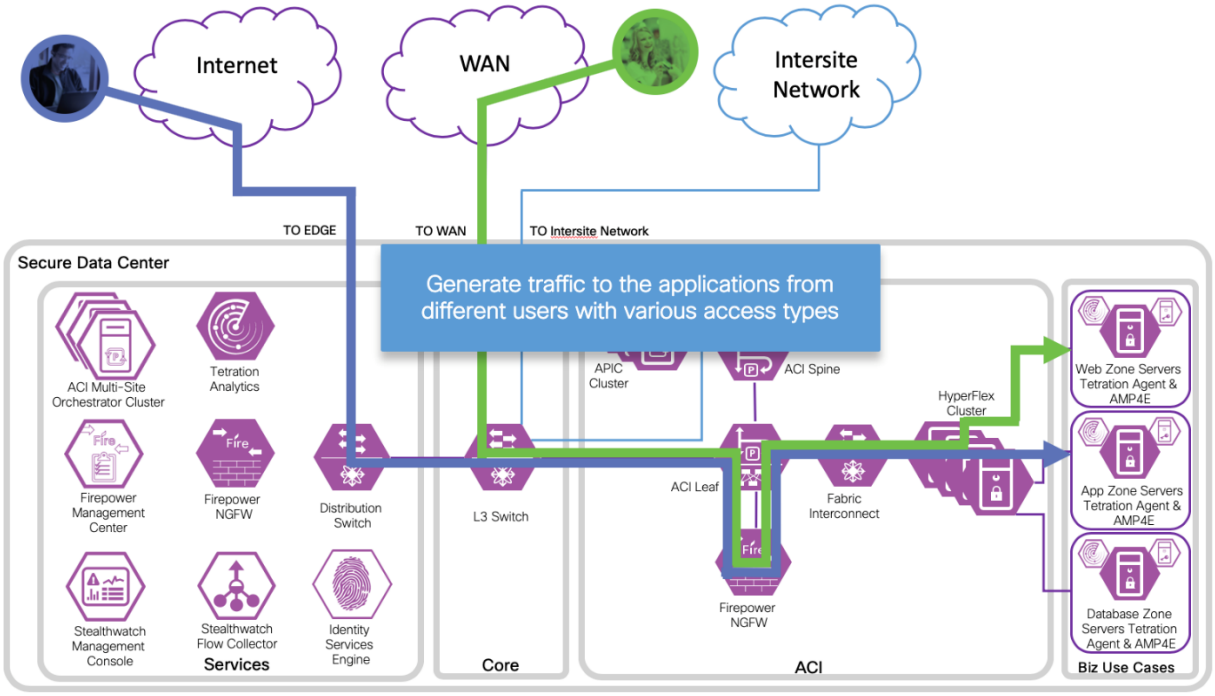
Test Description:

1. On the NetFlow enabled appliances (VMware VDS, Nexus 9300 and Firepower NGFW) enable NetFlow and deliver the NetFlow records to Stealthwatch Flow Collector

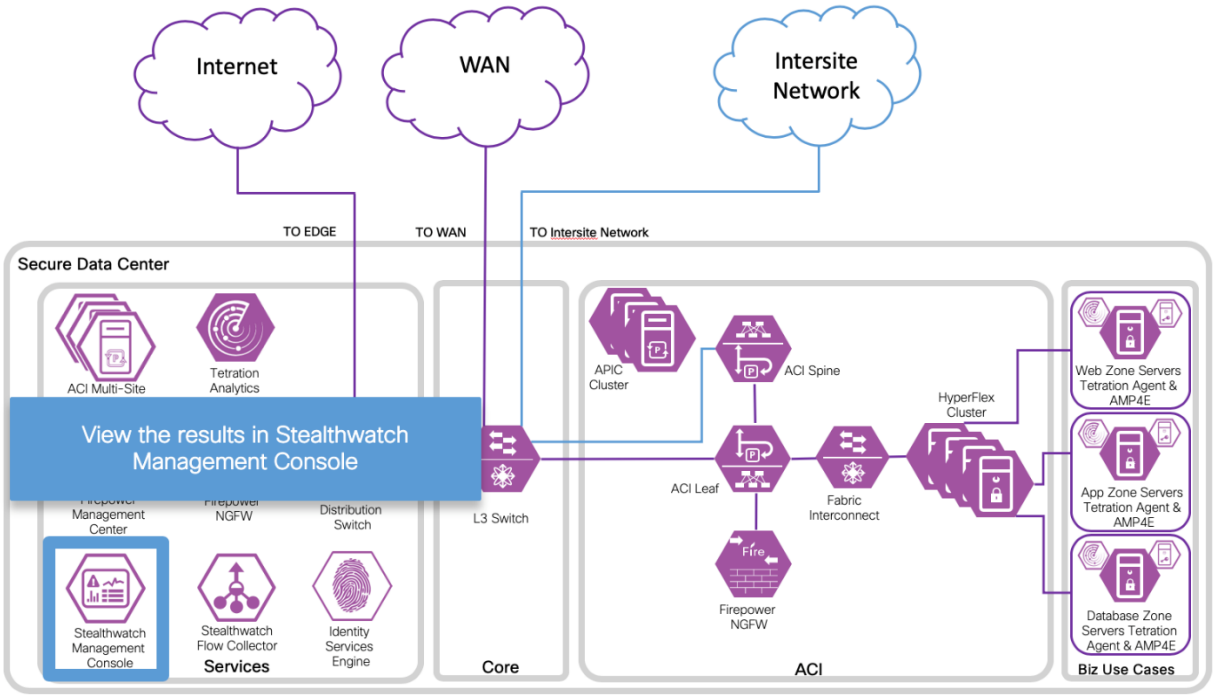


Return to Contents

2. Generate traffic to the applications from different users with various access types (i.e. campus, branch, Internet)



3. View the results in Stealthwatch Management Console



Stealthwatch and Tetration Integration

The Stealthwatch and Tetration integration involves using the Stealthwatch External Lookup feature. This feature allows you to pivot or cross launch from Stealthwatch to Tetration to view

additional information about an IP address. External lookups to Tetration: Source IP and Target IP are available. You can launch Tetration directly from the Stealthwatch Management Console (SMC) Desktop Client or the SMC Web App. For more information refer to: https://www.Cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/external_lookup/SW_7_0_External_Lookup_DV_1_0.pdf.

Procedure

Step 1	Create the following two text files: Tetration (Source IP).config and Tetration (Target IP)
Step 2	Access the External Lookup configuration on SMC
Step 3	Add Tetration (Source IP) External Lookup
Step 4	Add Tetration (Target IP) External Lookup
Step 5	Use Tetration (Source and Target IP) External Lookup

Step 1

a. Create Tetration (Source IP).config text file. This file is required for the configuration of this feature. Create this text file Tetration (Source IP) v4.txt. Make sure the file is accessible by the Stealthwatch Management console.

```
def String query = " " ;

// base https://<TetrationAnalyticsIPaddress/#/host/profile/10/<ip_address>
// parameter- IP

// attribute- source IP address

vendorValues.each { valueOperand ->

        //query += " /" ;

        def String convertedStr = " " ;

        if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue()
 instanceof Integer) {

                convertedStr = valueOperand.getFromValue().toString();
        }

        String.valueOf('java.lang.Integer');

        query += URLEncoder.encode(convertedStr," UTF-8" );
};
query = baseUrl + query + " " ;

return query;
```

(here is the full contents of Tetration (Target IP) v4.txt):

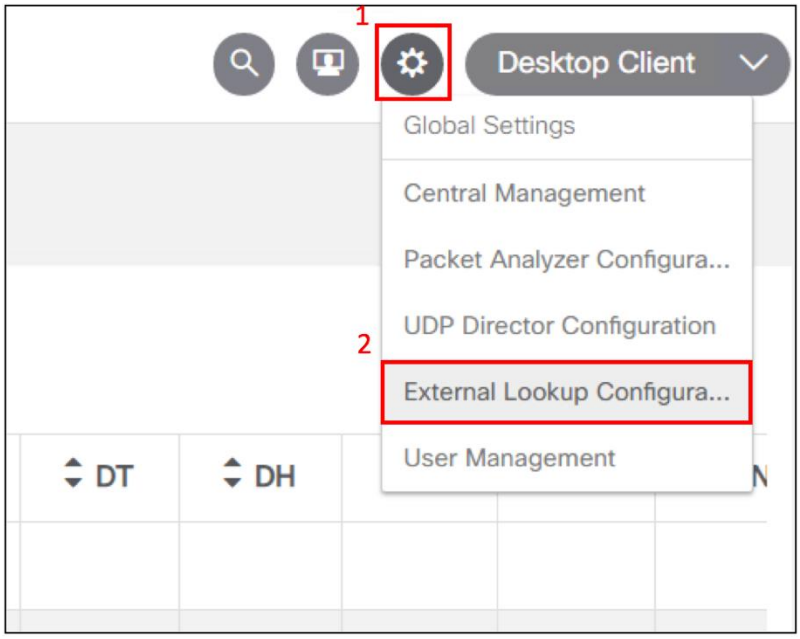
```
def String query = " " ;
```

b. Create Tetration (Target IP).config text file. This file is required for the configuration of this feature. Create this text file Tetration (Target IP) v4.txt

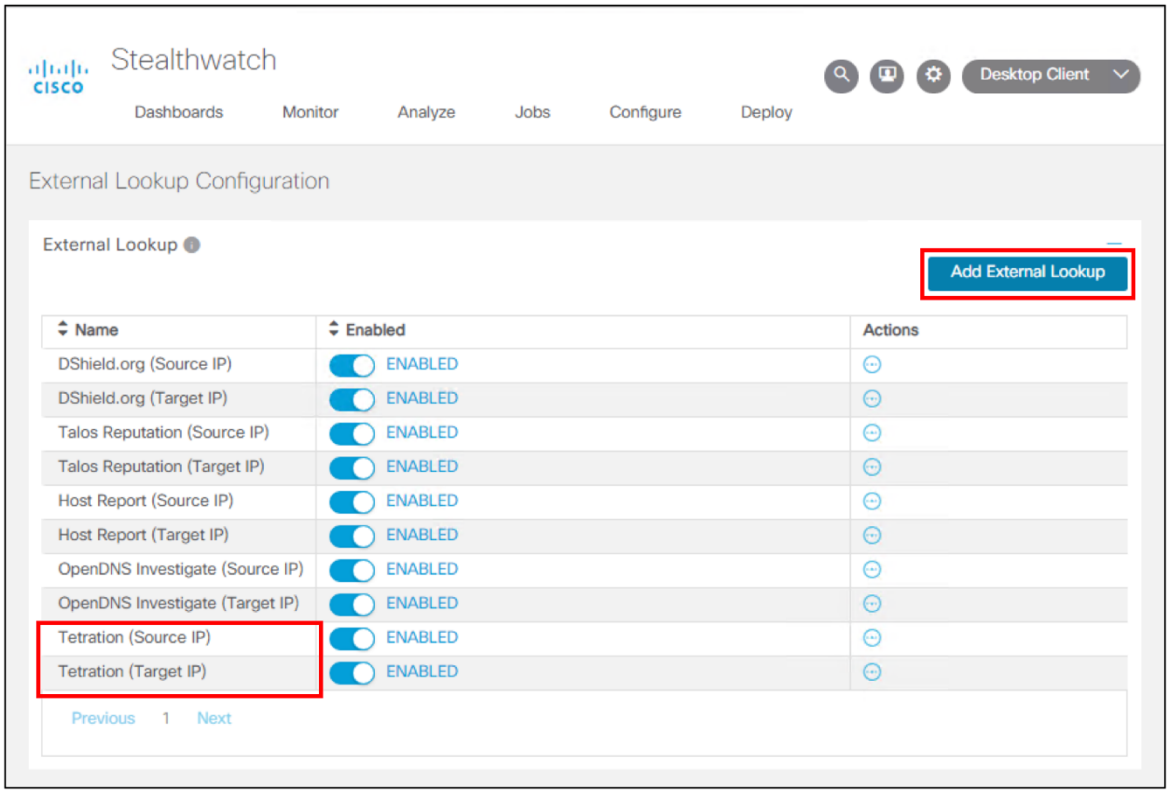
```
// base https:// TetrationAnalyticsIPaddress/#/host/profile/10/<ip_address >
// parameter- IP

// attribute- target IP address

vendorValues.each { valueOperand ->

        //query += " /" ;

        def String convertedStr = " " ;

        if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue()
 instanceof Integer) {

                convertedStr = valueOperand.getFromValue().toString();
        }

        String.valueOf('java.lang.Integer');

        query += URLEncoder.encode(convertedStr," UTF-8" );

};

query = baseUrl + query + " " ;

return query;
```

Step 2

a. Access the External Lookup Configuration on SMC. Connect to SMC with administrator rights and navigate to the **wheel** on the upper right corner (1) and select **External Lookup Configuration** (2).

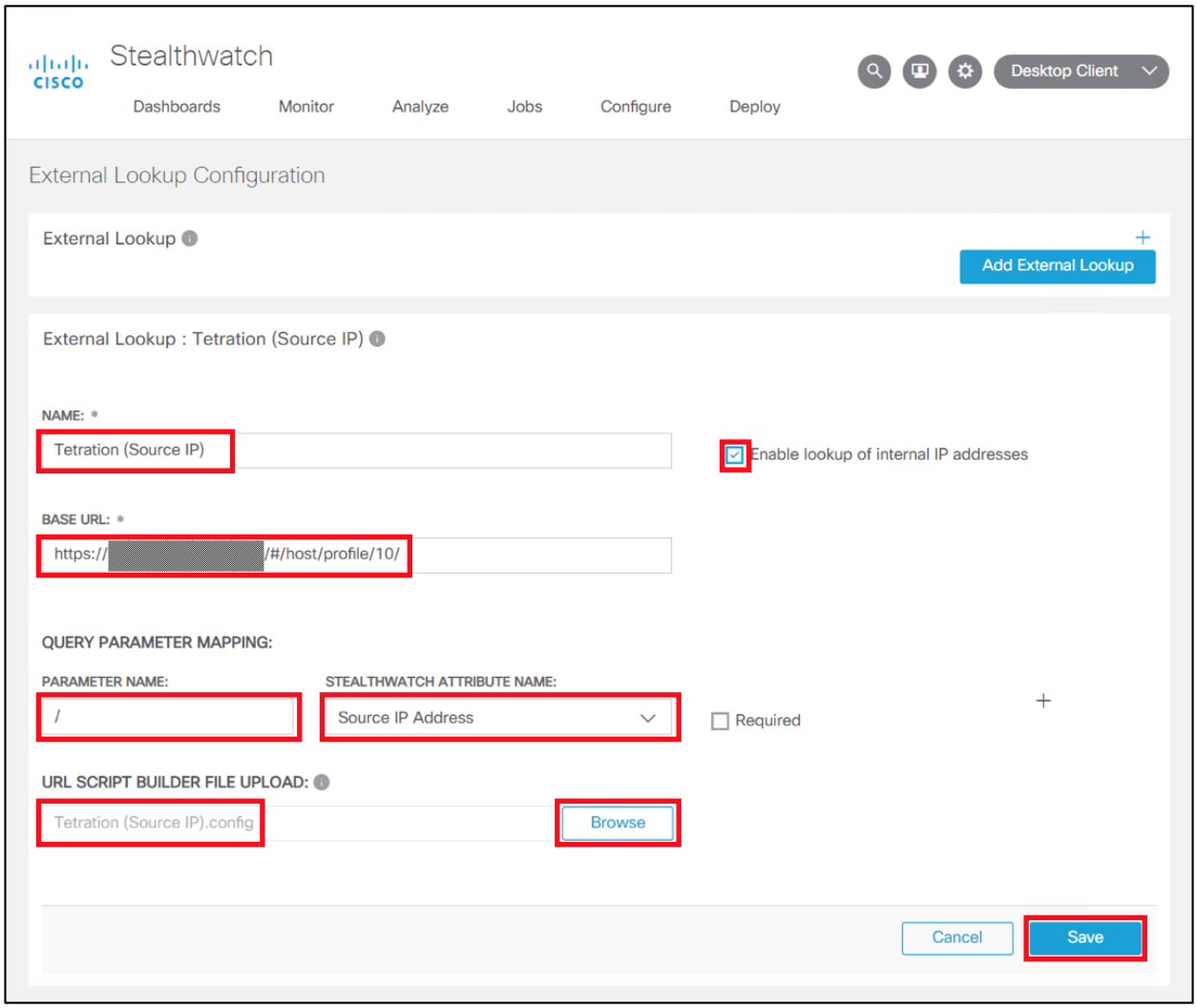


b. Select **Add External Lookup** back on the next screen.



Step 3

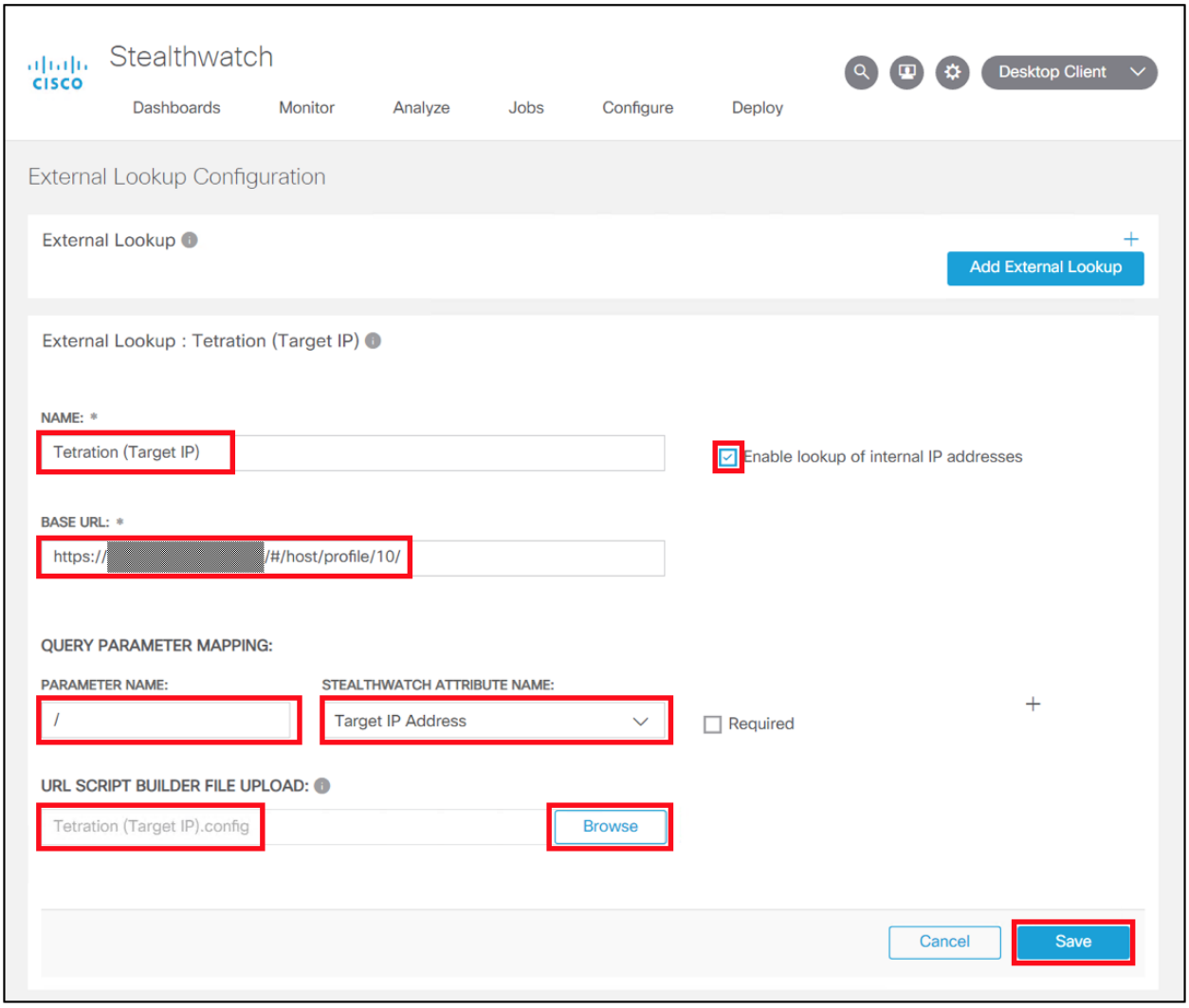
a. Add Tetration (Source IP) External Lookup. Set the **Name** to **Tetration (Source IP)**, set the **URL** for your Tetration Analytics Appliance. Setup the Query Parameter Mapping section. Set the **Parameter Name** to **"/"**, set the **Stealthwatch Attribute Name** to **Source IP Address.** **Browse** to find the **Tetration (Source IP).config** file and select **Save.**



Return to Contents

Step 4

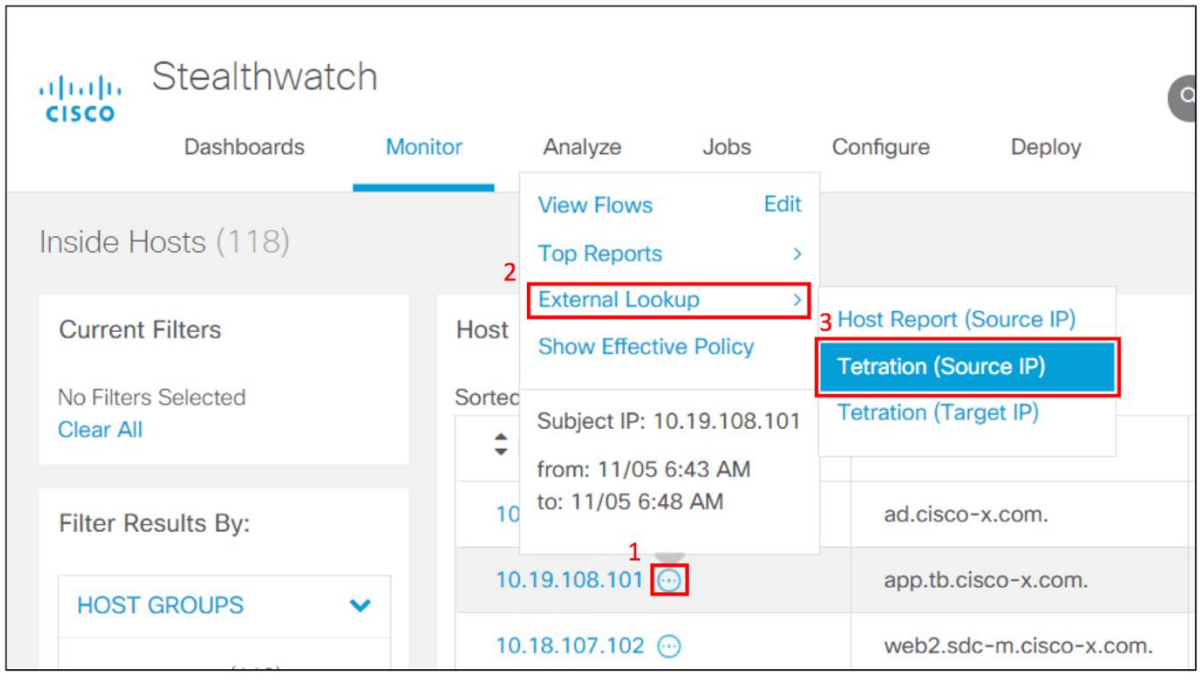
a. Add Tetration (Target IP) External Lookup. Set the **Name** to **Tetration (Target IP)**, set the **URL** for your Tetration Analytics Appliance. Setup the Query Parameter Mapping section. Set the **Parameter Name** to **"/"**, set the **Stealthwatch Attribute Name** to **Target IP Address.** **Browse** to find the **Tetration (Target IP).config** file and select **Save.**



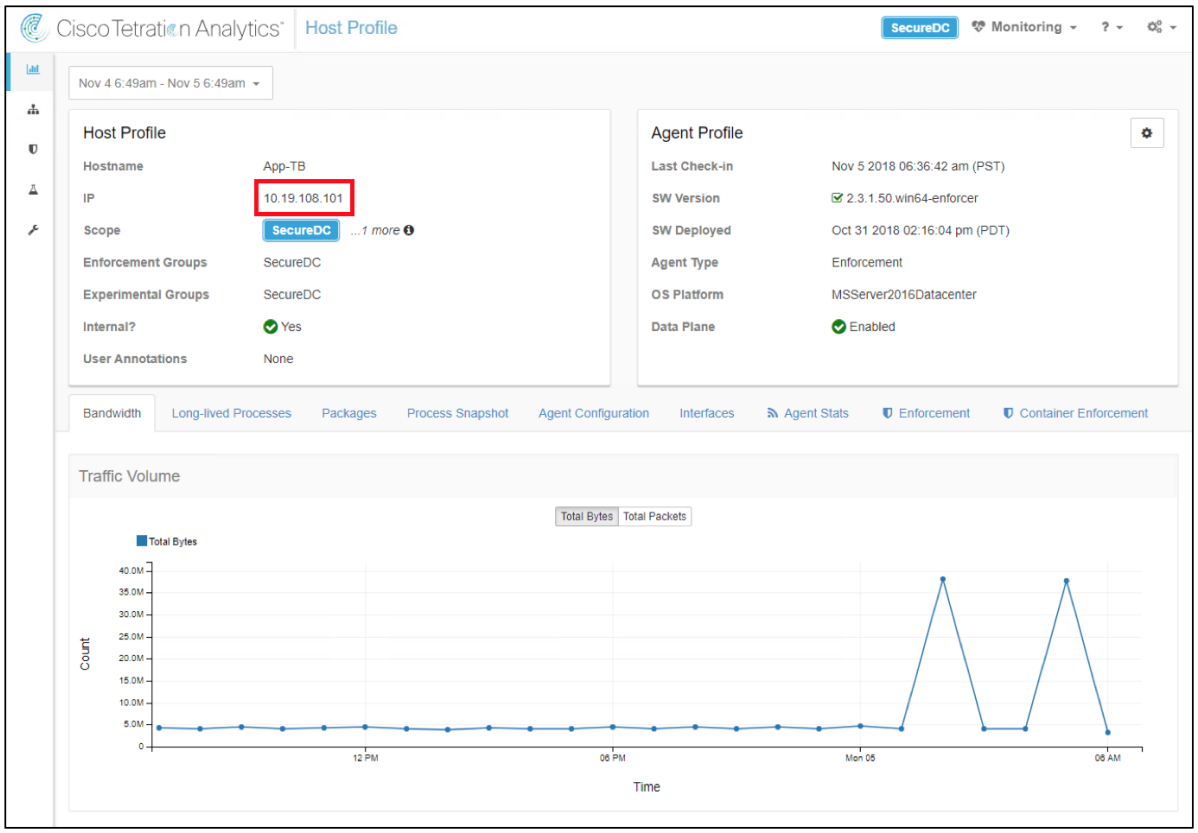
Return to Contents

Step 5

a. Use Tetration (Source IP) External Lookup. Select the **sphere** next to the Source IP address that you want to investigate further in Tetration **(1)->External Lookup(2)->Tetration (Source IP)(3).**

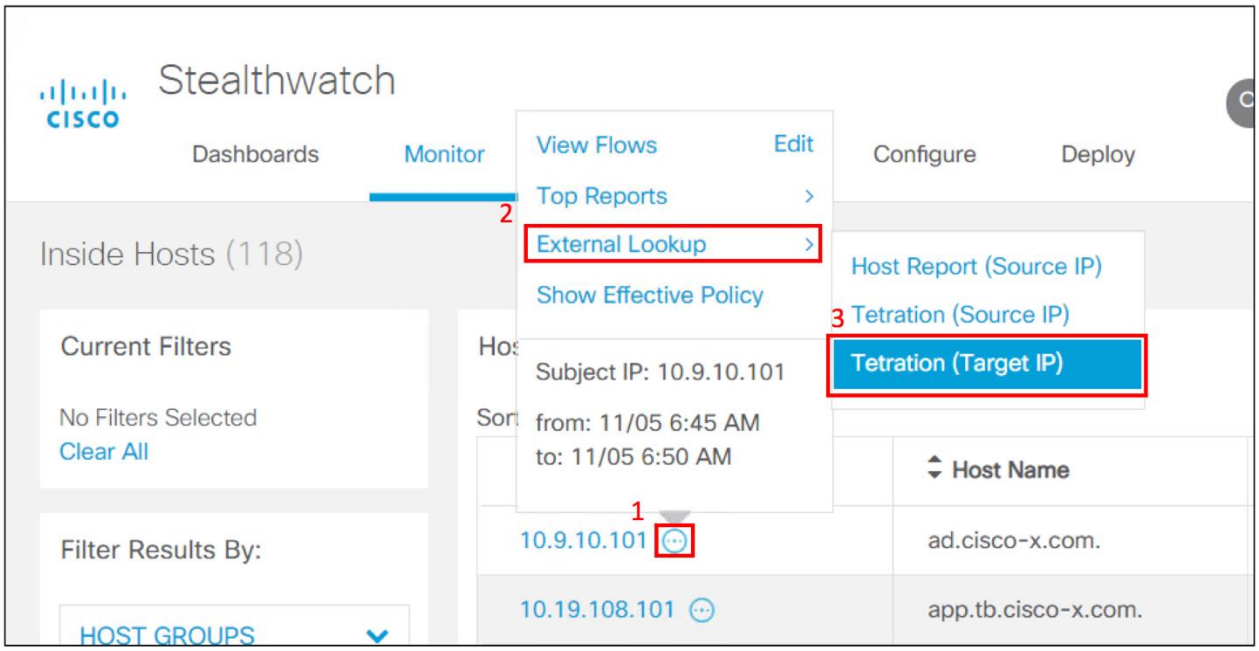


b. Tetration Analytics should open in a new browser tab. If currently not logged in, you will need to log in. The **Host Profile** for the **Source IP address** is shown.



Return to Contents

c. Use Tetration (Target IP) External Lookup. Select the **sphere** next to the Target IP address that you want to investigate further in Tetration **(1)->External Lookup(2)->Tetration (Target IP)(3).** This will show the **Host Profile** for the **Target IP address** in Tetration.



NetFlow was enabled on the following appliances to provide visibility for Stealthwatch in the data center:

- irepower Threat Defense 4100/9300
- CI - Nexus 9300
- Mware vSphere Distributed Switch (VDS)

The guidance we used for enabling NetFlow on those products is provided below.

Firepower Threat Defense and NetFlow

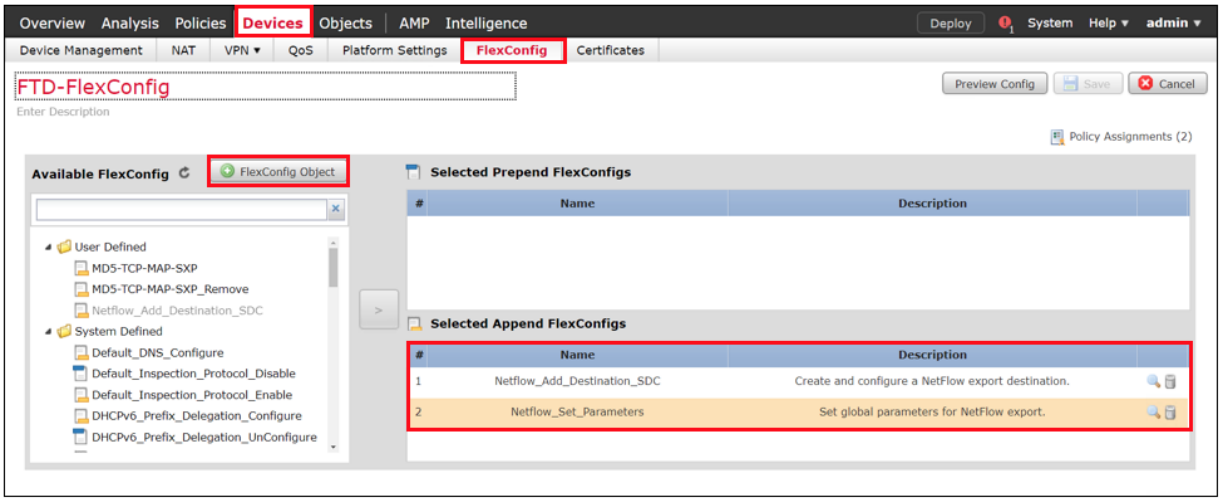
To configure NetFlow on Firepower Threat Defense, you need to use Firepower Management Center and configure NetFlow using FlexConfig. The first link is the process we followed. The second link is a recommended link on FlexConfig in general.

Configuring NetFlow Secure Event Logging (NSEL) on Cisco Firepower Threat Defense
https://community.Cisco.com/t5/security-documents/configuring-nsel-netflow-on-Cisco-firepower-threat-defense-ftd/ta-p/3646300

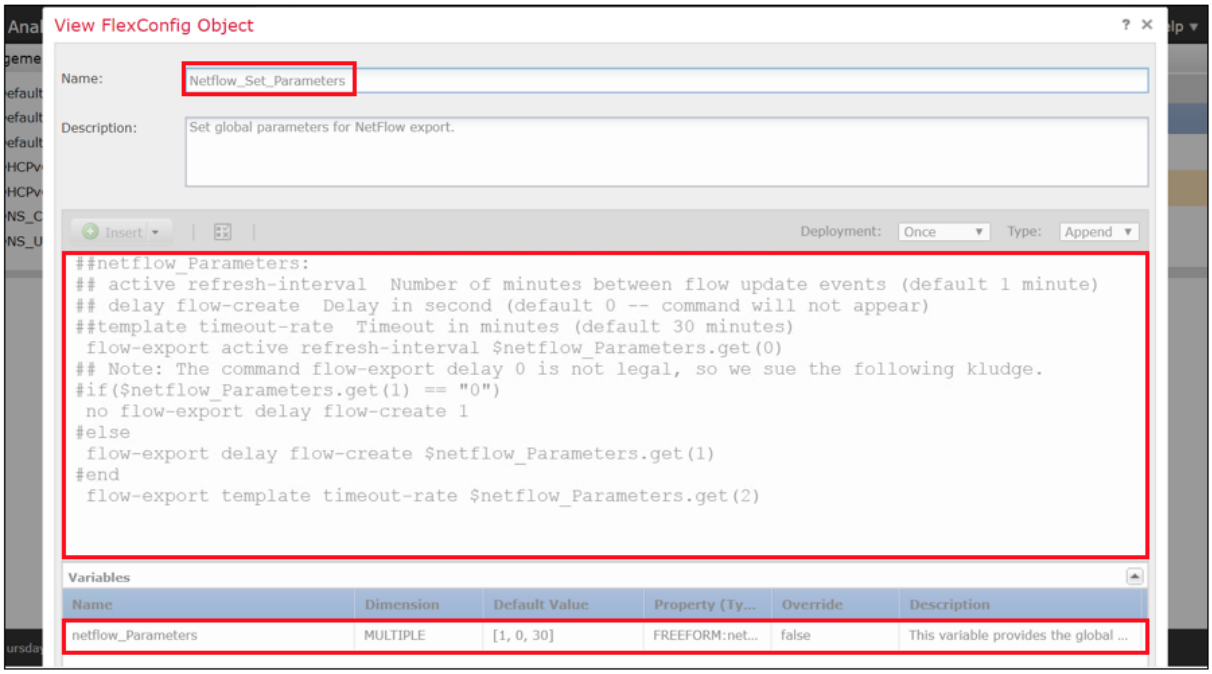
Firepower Management Center FlexConfig Overview:
https://www.Cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html

Step 1

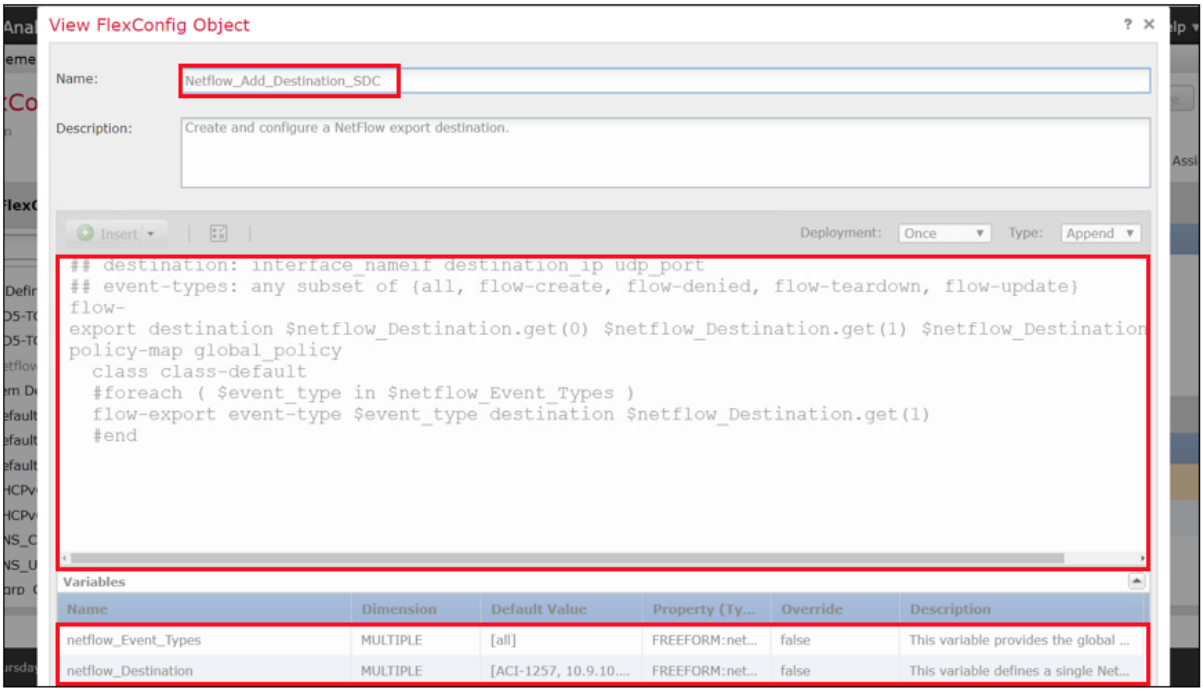
a. Create **two FlexConfig Objects** that will be used to enable NetFlow on Firepower Threat Defense, **Netflow_Add_Destination_SDC** and **Netflow_Set_Parameters**. To create a FlexConfig Object in Firepower Management Center, navigate to **Devices-> FlexConfig** and select **plus sign** to **create FlexConfig Object**.



b. Create FlexConfig Object **Netfow_Set_Parameters FlexConfig**.



c. Create FlexConfig Object **Netfow_Add_Destination_SDC FlexConfig**.



ACI and NetFlow

This guidance in this section is based on the reference **Cisco APIC and NetFlow**, https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Cisco_APIC_and_NetFlow.html.

Overview:
Step 1 – Configure NetFlow or Tetration Analytics Priority
Step 2 – Configuring a Tenant NetFlow Exporter Policy
Step 3 – Configuring a Tenant NetFlow Record Policy
Step 4 – Configuring a Tenant NetFlow Monitor Policy
Step 5 – Deploy NetFlow Monitor Policy

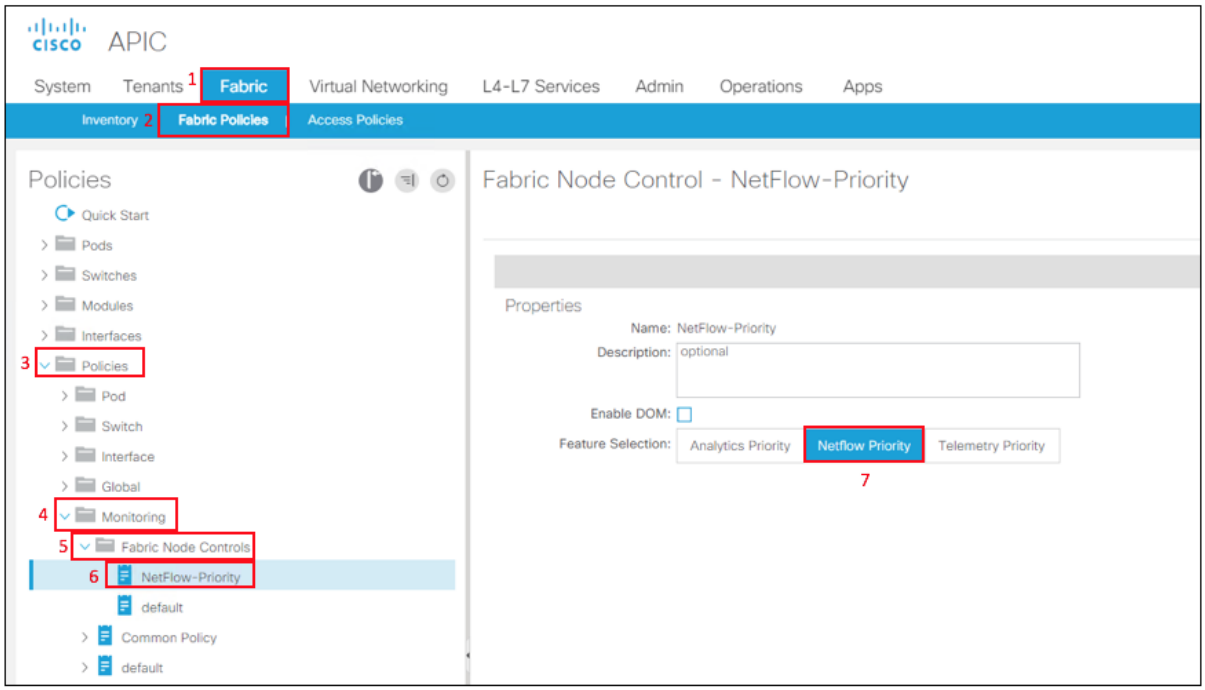
Step 1
Configure NetFlow or Tetration Analytics Priority

About NetFlow and Cisco Tetration Analytics Priority
As far the Cisco Application Centric Infrastructure (Cisco ACI) hardware is concerned, NetFlow and Cisco Tetration Analytics use the same ASIC building blocks to collect data. You cannot enable both features at the same time. NetFlow or Tetration Analytics must be explicitly enabled before configuring and deploying the related policies. **The default is Tetration Analytics**.
If the Cisco APIC pushes both Cisco Tetration Analytics and NetFlow configurations to a particular node, the chosen priority flag alerts the switch as to which feature should be given priority. The other feature's configuration is ignored. We tested NetFlow on the Nexus 9300 Leaf switches for use by Stealthwatch. Tetration enforcement agents are deployed on all the workloads in the data center.

Procedure

Step 1	On the menu bar, select Fabric > Fabric Policies.
Step 2	In the Navigation pane, select Policies > Monitoring > Fabric Node Controls.
Step 3	In the Work pane, select Right-Click > Create Fabric Node Control
Step 4	In the **Create Fabric Node Control** dialog box, enter the name, and select **NetFlow Priority** in the **Feature Selection** section. The default value is Analytics Priority which is Cisco Tetration Analytics.
Step 5	Click Submit.
Step 6	Associate the fabric node control policy to the appropriate fabric policy group and profile.

The figure below shows how you confirm that the Fabric Node Control is set to NetFlow-Priority.



Return to Contents

Step 2
Configuring a Tenant NetFlow Exporter Policy Using the GUI

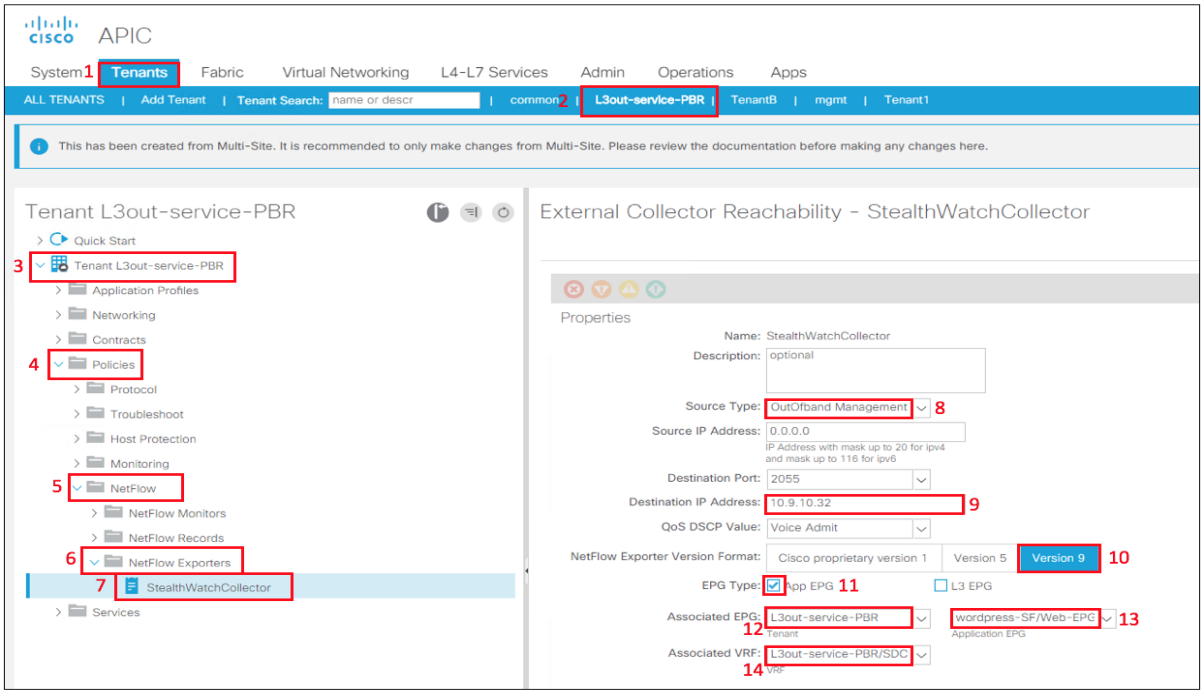
About NetFlow Exporter Policies

An exporter policy (netflowExporterPol) specifies where the data collected for a flow must be sent. A NetFlow collector is an external entity that supports the standard NetFlow protocol and accepts packets marked with valid NetFlow headers.

Procedure

Step 1	On the menu bar, select **Tenants > All Tenants**.
Step 2	In the Work pane, double-click the **tenant's name**.
Step 3	In the Navigation pane, select **Tenant *Tenant_Name* > Policies > NetFlow**.
Step 4	Right-Click **NetFlow Exporters** and select **Create External Collector Reachability**.
Step 5	In the **Create External Collector Reachability** dialog box, fill in the fields as required, except as specified below: a. For the **NetFlow Exporter Version** Format buttons, **Version 9** is the only supported choice. b. For the **EPG Type** check boxes, you can leave the boxes unchecked, or you can put a check in one box. You cannot put a check in multiple boxes.

The figure below shows the configuration of a NetFlow Exporter named **StealthWatchCollector**. The **Source Type** is **OutOfband Management (8)**, the **IP address** of the **StealthWatch Flow Collector** is **10.9.10.32(9)**, select **NetFlow Version 9(10)**, select the **Associated EPG** for the **Tenant** with **<tenant-name>(12)**, select the **Associated EPG** for the **Application EPG** with **Web-EPG(13)** and select the **Associated VRF** with **<VRF-name>(14)**.



Return to Contents

Step 3

Configuring a Tenant NetFlow Record Policy

About NetFlow Record Policies

A record policy (netflowRecordPol) lets you define a flow and what statistics to collect for each flow. This is achieved by defining the keys that NetFlow uses to identify packets in the flow as well as other fields of interest that NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. A flow record also defines the types of counters gathered per flow, and you can configure 32-bit or 64-bit packet or byte counters.

Procedure

Step 1 On the menu bar, select **Tenants > All Tenants**.

Step 2 In the Work pane, double-click the **tenant's name**.

Step 3 In the Navigation pane, select Tenant T*enant_Name* > Policies > NetFlow.

Step 4 Right-Click **NetFlow Records** and select **Create Flow Record**.

Step 5 In the **Create NetFlow Record** dialog box, fill in the fields as required, except as specified below:

For the **Collect Parameters** drop-down list, you can select multiple parameters.

For the **Match Parameters** drop-down list, you can select multiple parameters.

If you select multiple parameters, your choices must be one of the following combinations or a subset of one of the combinations:

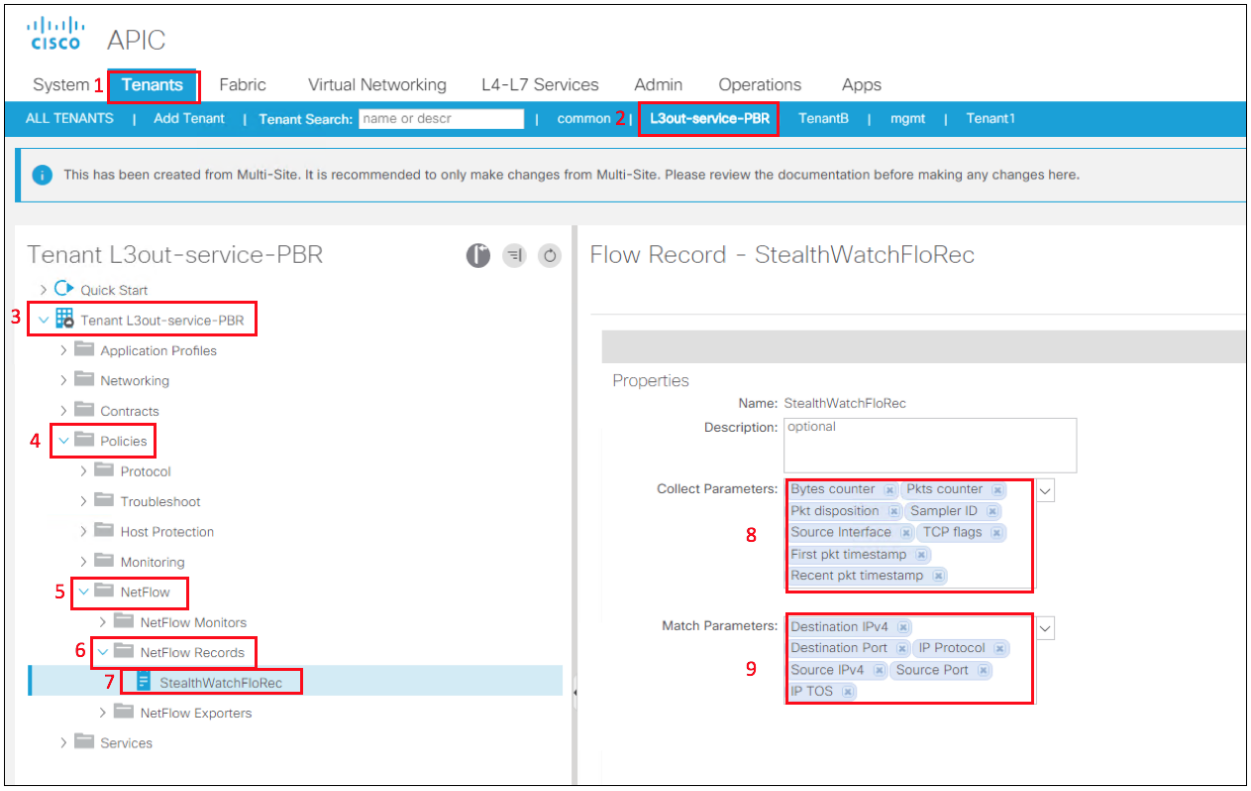
Source IPv4, Destination IPv4, Source Port, Destination Port, IP Protocol, VLAN, IP TOS

Source IPv6, Destination IPv6, Source Port, Destination Port, IP Protocol, VLAN, IP TOS

Ethertype, Source MAC, Destination MAC, VLAN

Source IP, Destination IP, Source Port, Destination Port, IP Protocol, VLAN, IP TOS, where Source IP/Destination IP qualifies both IPv4 and IPv6.

The figure below shows the NetFlow Record that we used StealthWatchFloRec. The Collect Parameters (8) and Match Parameters (9) are shown below.



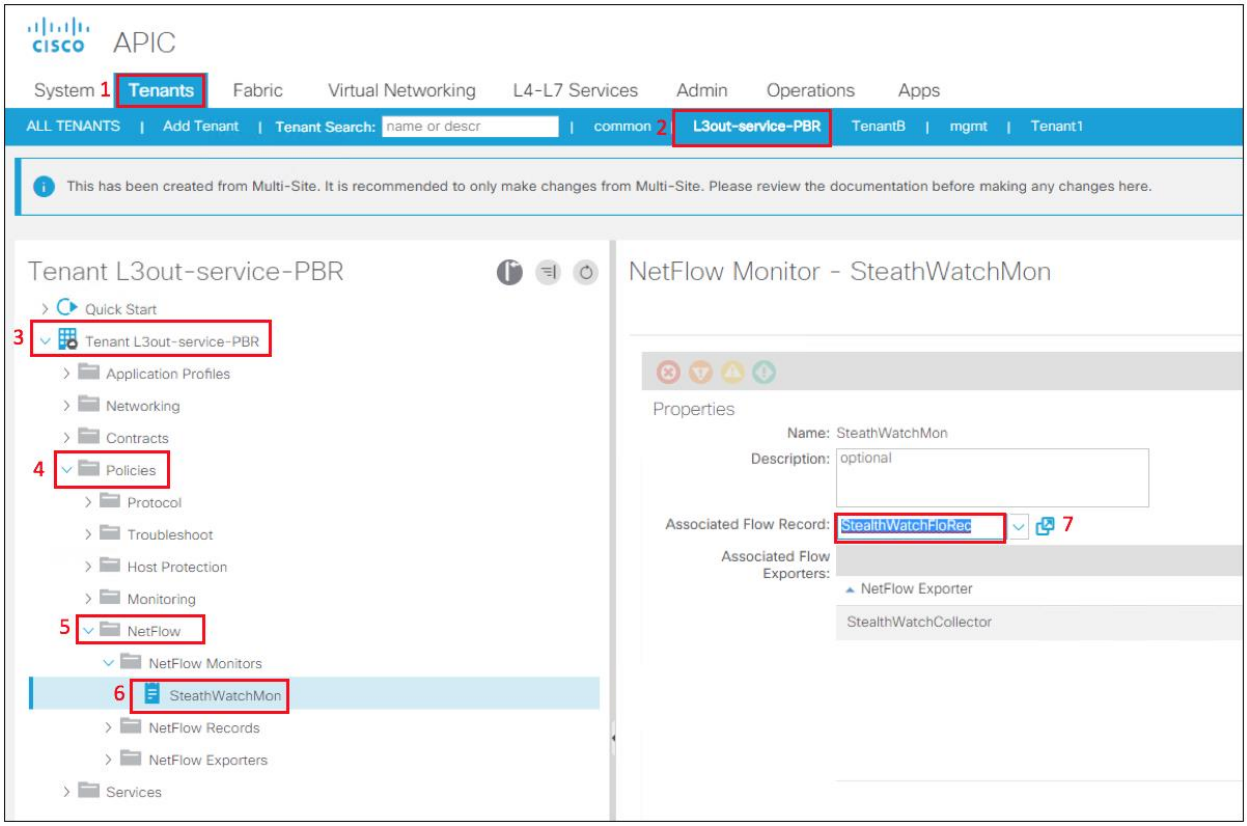
Step 4
Configuring a Tenant NetFlow Monitor Policy

The following procedure configures a tenant NetFlow monitor policy using the advanced GUI mode.

Procedure

Step 1	On the menu bar, select Tenants > All Tenants.
Step 2	In the Work pane, double-click the **tenant's name**.
Step 3	In the Navigation pane, select **Tenant Tenant_Name > Policies > NetFlow**.
Step 4	Right-Click **NetFlow Monitors** and select **Create Flow Monitor**.
Step 5	In the **Create NetFlow Monitor** dialog box, fill in the fields as required. You can associate a maximum of two flow exporters with the monitor policy.

The figure below shows the NetFlow Monitor policy called StealthWatchMon that we tested. It is associated to the flow record called StealthWatchFloRec(7).



Step 5

Deploy NetFlow Monitor Policy

Procedure

Step 1 On the menu bar, select Tenants > *Tenant_Name*

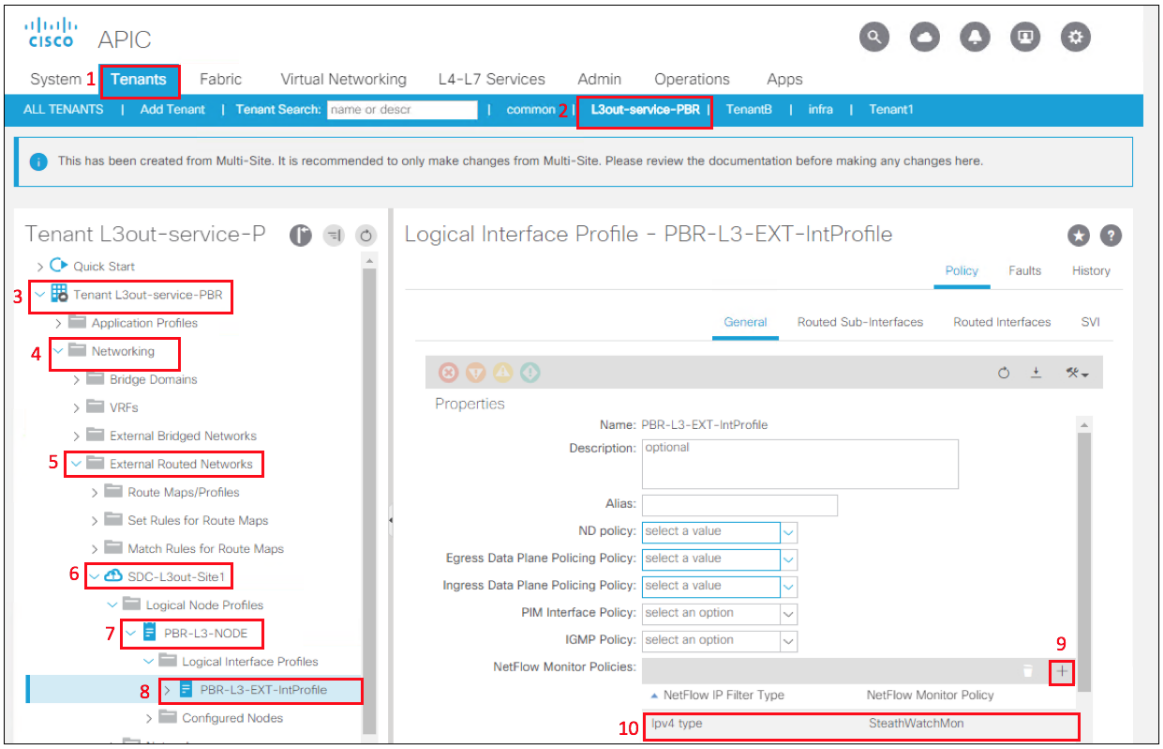
Step 2 In the Navigation pane, select Tenant *Tenant_Name* > Networking > External Routed Networks > *Network_name* > Logical Node Profiles > *Interface_Profile_Name*.

Step 3 In the Work pane, click Policy and General.

Step 4 Click the + on the NetFlow Monitor Policies.

Step 5 Select the appropriate NetFlow IP Filter Type and select the NetFlow Monitor Policy created previously.

The figure below shows how the NetFlow Monitor Policy is deployed on the L3Out(10).



Return to Contents

VMware vSphere Distributed Switch (VDS) and NetFlow

There are two possibilities when you are enabling NetFlow on VMware VDS:

- Deploy NetFlow with ACI on VMware VDS
- Deploy NetFlow without ACI on VMware VDS

Deploy NetFlow with ACI on VMware VDS

In this case you would configure NetFlow in APIC as it has a connection to VMware vCenter as a Virtual Machine Manager (VMM). The following guidance was based on the guidance in ACI Virtualization Guide 3.2(2), https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/virtualization/b_ACI_Virtualization_Guide_3_2_2/b_ACI_Virtualization_Guide_3_2_2_chapter_010.html.

Steps:
Configuring a NetFlow Exporter Policy for VM Networking Using the GUI
Consuming a NetFlow Exporter Policy Under a VMM Domain Using the GUI
Enabling NetFlow on an Endpoint Group to VMM Domain Association Using the GUI

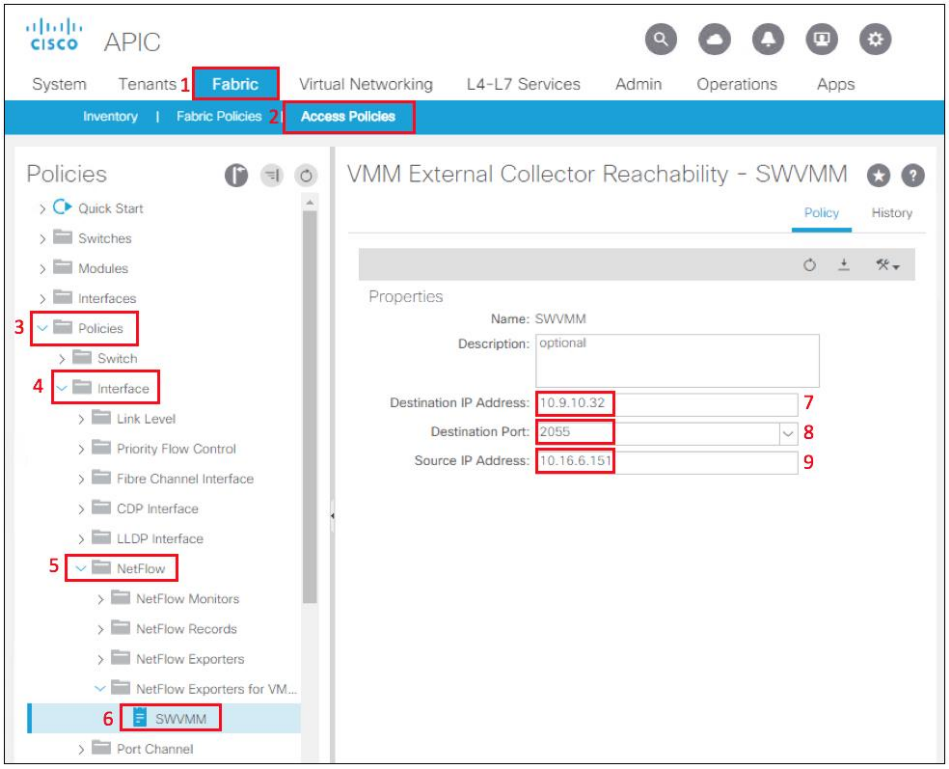
Configuring a NetFlow Exporter Policy for VM Networking Using GUI

The following procedure configures a NetFlow exporter policy for VM networking.

Procedure

Step 1	On the menu bar, select **Fabric > Access Policies**.
Step 2	In the navigation pane, expand **Policies > Interface > NetFlow**.
Step 3	Right-Click NetFlow Exporters for VM Networking and select **Create NetFlow Exporter for VM Networking**.
Step 4	In the Create **NetFlow Exporter for VM Networking** dialog box, fill in the fields as required.
Step 5	Click **Submit**.

The figure below shows the **VMM External Collector Reachability** policy **SWVMM**. The **Destination IP Address** is to the **Stealthwatch Flow Collector 10.9.10.32(7)**, **Destination Port(8)**, and **Source IP address** of the NetFlow traffic **10.16.6.151(9)**.



Consuming a NetFlow Exporter Policy Under a VMM Domain Using the GUI

The following procedure consumes a NetFlow exporter policy under a VMM domain using the GUI.

Procedure

Step 1 On the menu bar, select **Virtual Networking > Inventory**.

Step 2 In the Navigation pane, expand the **VMM Domains folder**, Right-Click **VMware**, and select **Create vCenter Domain**.

Step 3 In the **Create vCenter Domain** dialog box, fill in the fields as required, except as specified:

a. In the **NetFlow Exporter Policy** drop-down list, select the desired exporter policy or create a new one.

b. In the **Active Flow Timeout** field, enter the desired **active flow timeout, in seconds**. The Active Flow Timeout parameter specifies the delay that NetFlow waits after the active flow is initiated, after which NetFlow sends the collected data. The range is from 60 to 3600. The default value is 60.

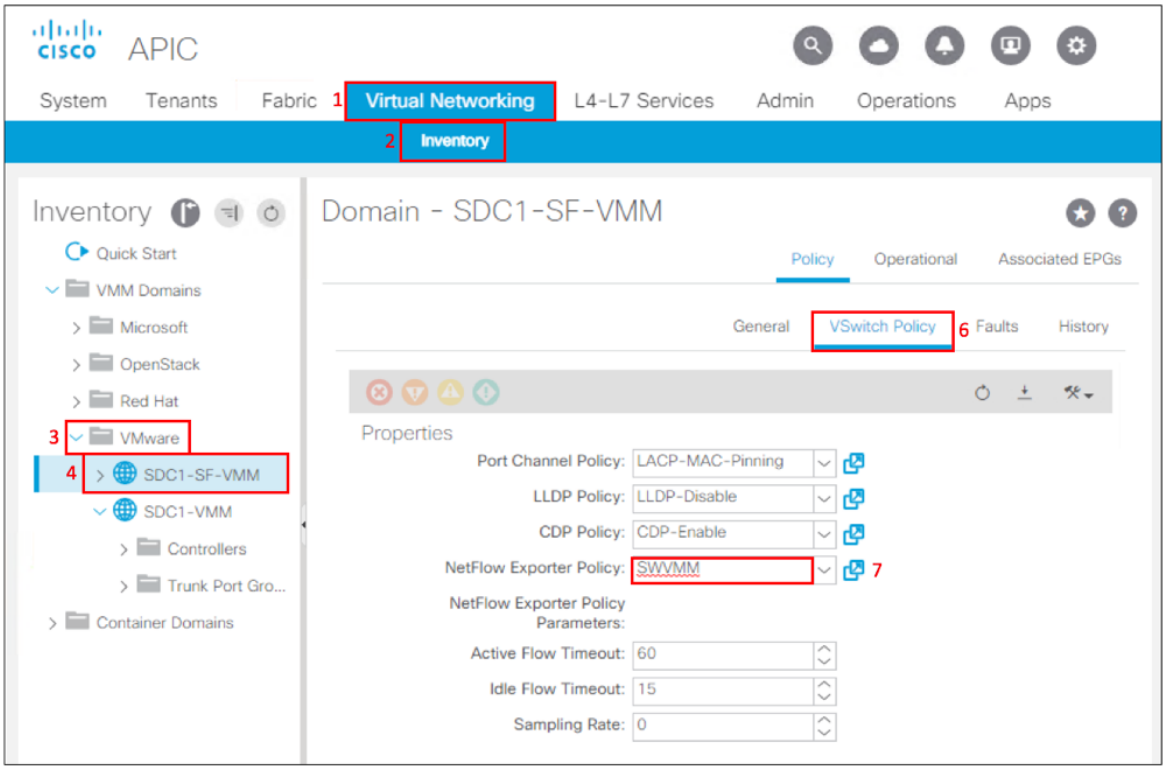
Return to Contents

c. In the **Idle Flow Timeout** field, enter the desired **idle flow timeout, in seconds**. The Idle Flow Timeout parameter specifies the delay that NetFlow waits after the idle flow is initiated, after which NetFlow sends the collected data. The range is from 10 to 300. The default value is 15.

d. (VDS only) In the **Sampling Rate** field, enter the desired **sampling rate**. The Sampling Rate parameter specifies how many packets that NetFlow will drop after every collected packet. If you specify a value of 0, then NetFlow does not drop any packets. The range is from 0 to 1000. The default value is 0.

Step 4 Click **Submit**.

The figure below shows the **NetFlow Exporter Policy SWVMM(7)** is set for the **VMM Domain SDC1-SF-VMM**.



Enabling NetFlow on an Endpoint Group to VMM Domain Association Using the GUI

The following procedure enables NetFlow on an endpoint group to VMM domain association. We tested with MSO which created the Endpoint Groups. We went into APIC after MSO created them to enable NetFlow since it is not currently supported in MSO.

Before you begin

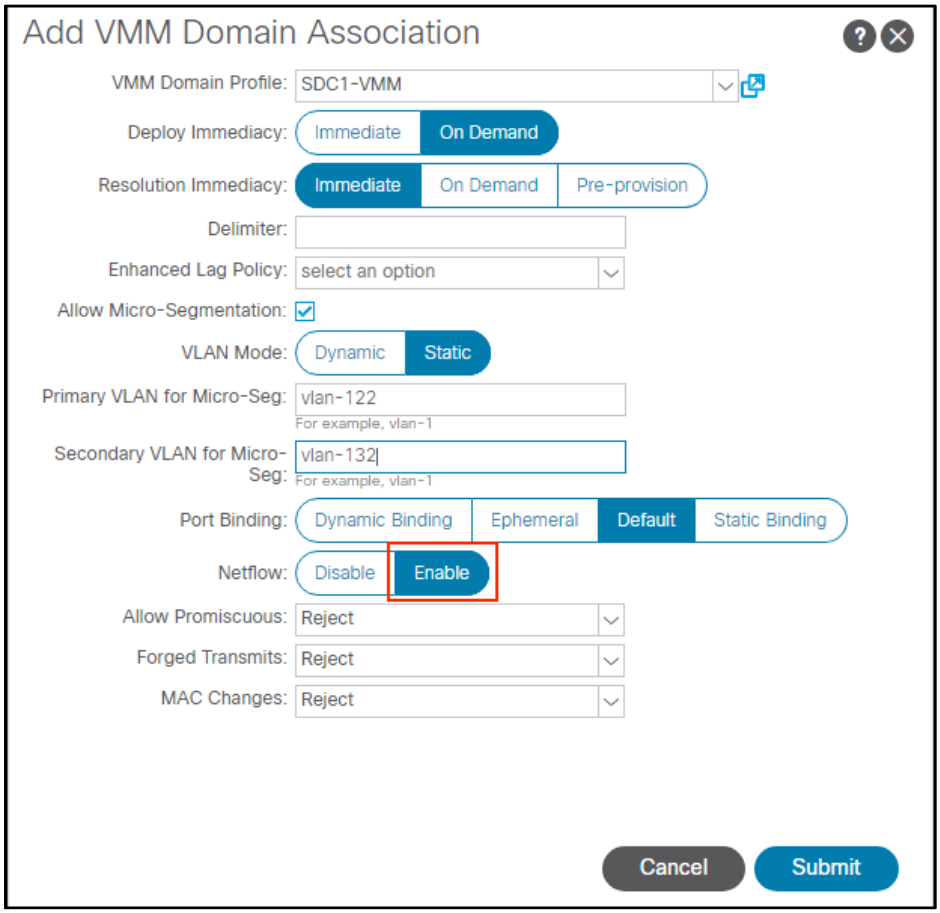
You must have configured the following:

- An application profile
- An application endpoint group

Procedure

Step 1	On the menu bar, select **Tenants > tenant's name**.
Step 2	In the left navigation pane, expand **tenant_name > Application Profiles > application_profile_name > Application EPGs > application_EPG_name**
Step 3	Right-Click **Domains (VMs and Bare-Metals)** and select **Add VMM Domain Association**.
Step 4	In the **Add VMM Domain Association** dialog box, fill in the fields as required and enable Netflow.
Step 5	Click **Submit**.

The figure below shows **NetFlow** is **Enabled** during VMM Domain Association.



Return to Contents

Deploy NetFlow without ACI on VMware VDS

We tested with ACI, but have provided the steps below to enable NetFlow on VMware VDS.

Configure the NetFlow Settings of a vSphere Distributed Switch, https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.networking.doc/GUID-55FCEC92-74B9-4E5F-ACC0-4EA1C36F397A.html

Enable or Disable NetFlow Monitoring on a Distributed Port Group or Distributed Port, https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.networking.doc/GUID-3CF9AEEB-08B0-47F5-A3B6-ADD8A919DFA0.html#GUID-3CF9AEEB-08B0-47F5-A3B6-ADD8A919DFA0

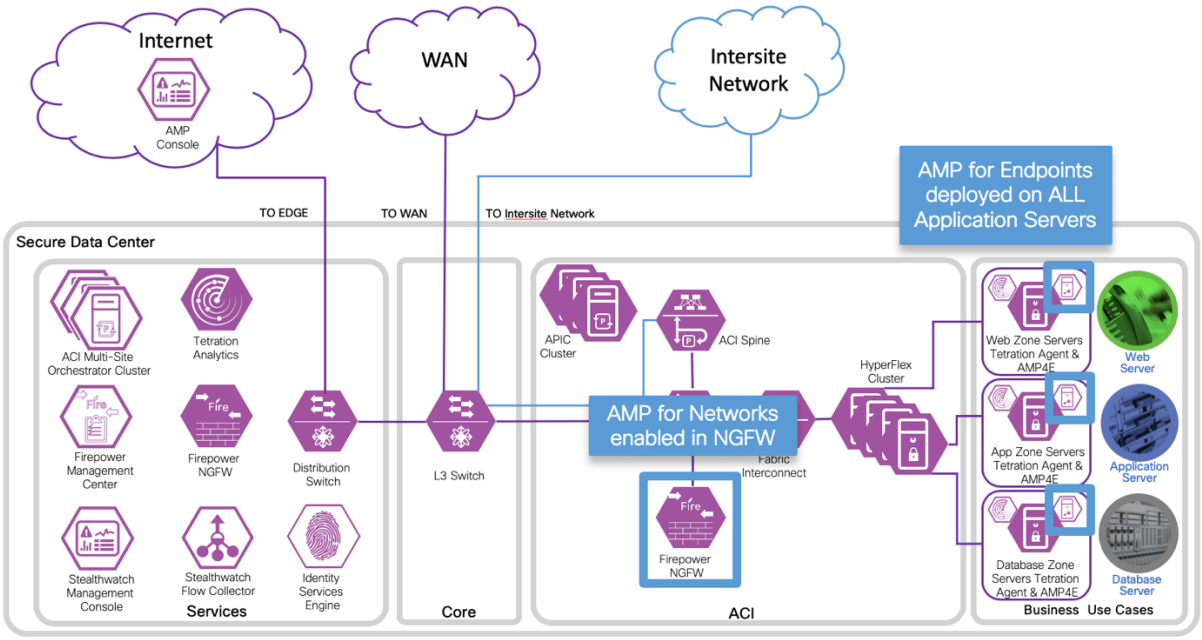
Test Case 5 – AMP and Firepower Threat Defense

The Firepower Management Center has a network file trajectory feature which maps host transferred files, including malware files, across your network. The trajectory chart includes the file transfer data, the disposition of the file, if a file transfer was blocked or if the file was quarantined. You can determine which hosts may have transferred malware, which hosts are at risk, and observe file transfer trends. This provides a single pane of glass for visibility for NGFW, NGIPS and AMP4E.

We tested with AMP Public Cloud, so we viewed the results in the AMP4E portal.

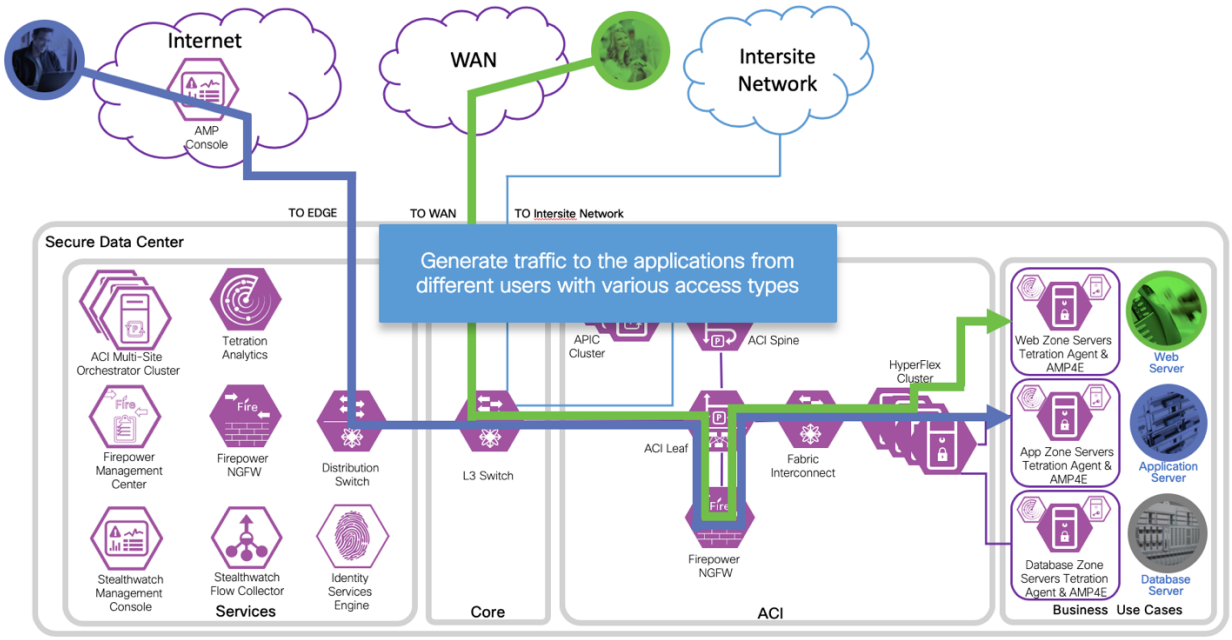
Test Description:

1. AMP4E will be deployed on all the application servers, and AMP4N will be enabled in NGFW.

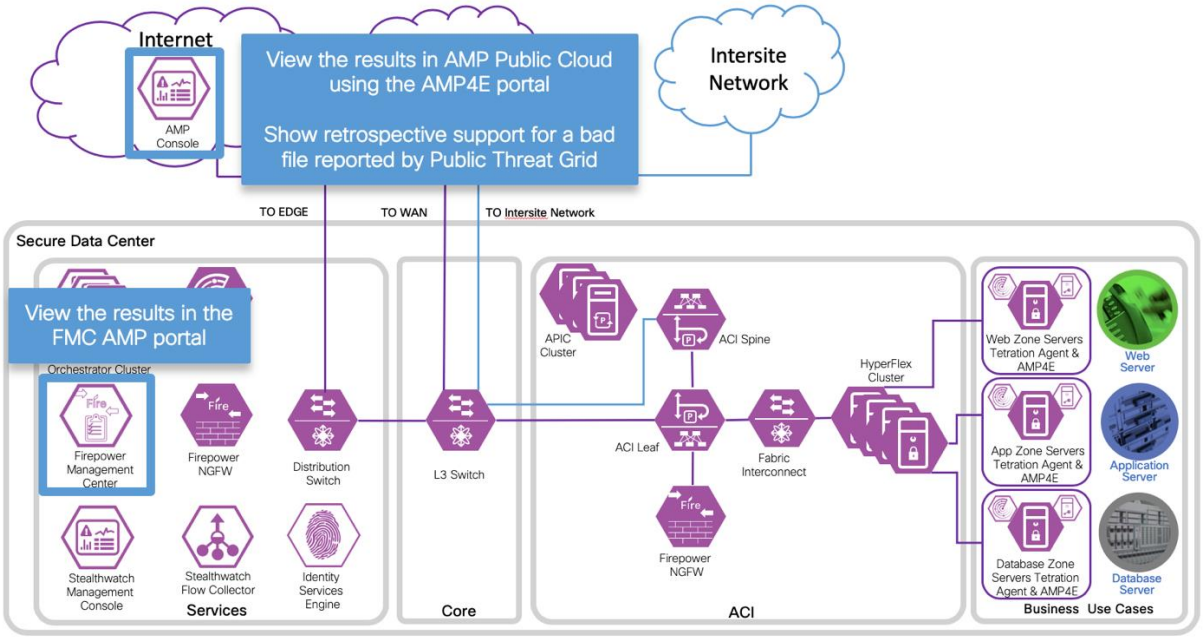


Return to Contents

2. Generate file-based traffic to the applications from different users with various access types (i.e. campus, branch, Internet). Both AMP4E and AMP4N should be active.



3. View the results in the FMC AMP portal, view the results in AMP Public Cloud using the AMP4E portal, and show retrospective support for a bad file reported by Public Threat Grid.



Return to Contents

Procedure

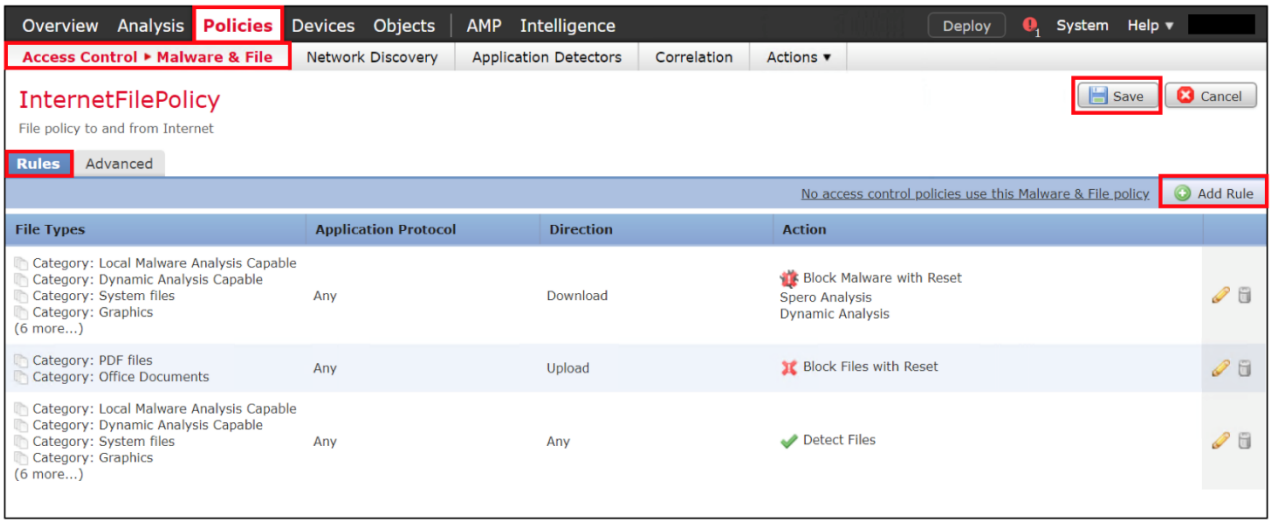
Step 1

a. Deploy AMP for Endpoints (AMP4E) on all application servers in both data centers. Refer to AMP for Endpoints User Guide, https://docs.amp.Cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf.

- Download the AMP Connector, Chapter 6
- AMP for Endpoints Windows Connector, Chapter 7
- AMP for Endpoints Linux Connector, Chapter 9

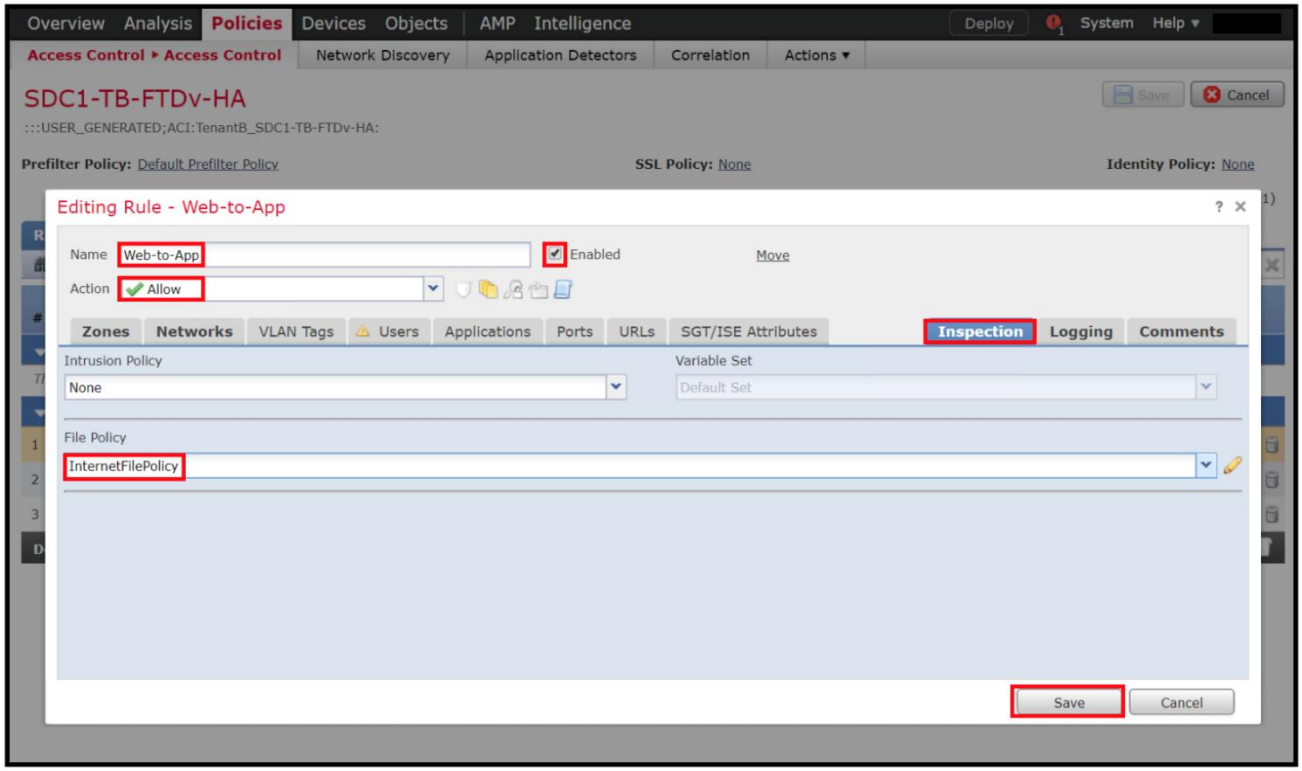
Step 2

a. Deploy AMP for Networks (AMP4N) on the Firepower Threat Defense Clusters in both data centers. In Firepower Management Center (FMC), create a File policy called **InternetFilePolicy**. **Add Rules** to define the actions for **file types, application protocols and direction**. **Save** the file policy.



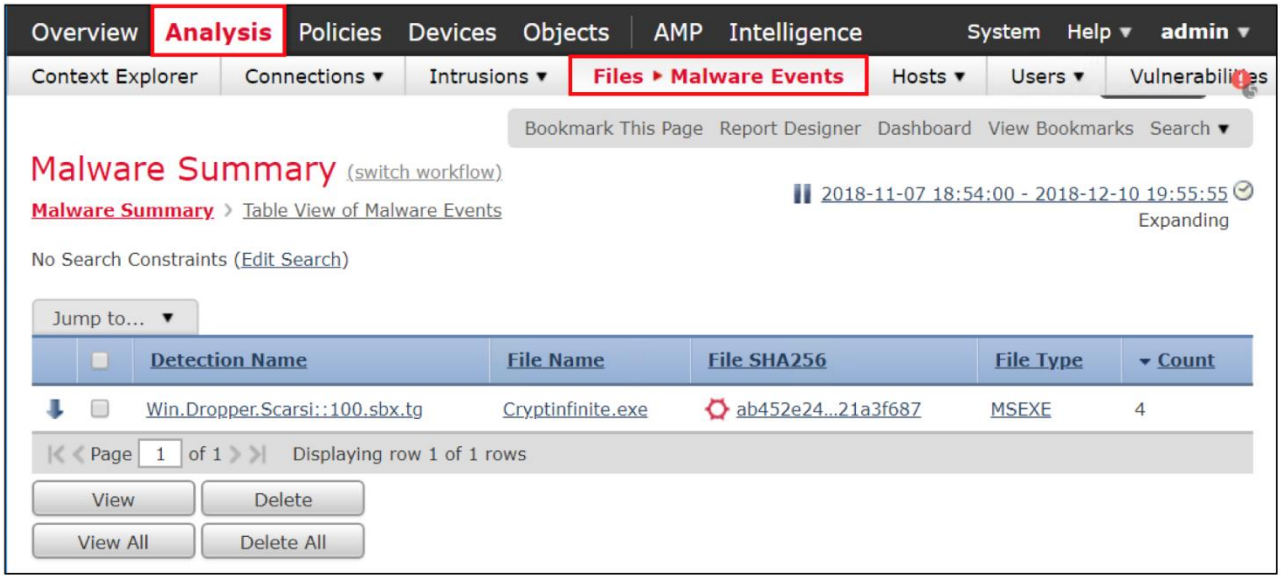
Return to Contents

b. Apply File Inspection policy to an Access Policy Rule in FMC. We had an existing Rule Web-to-App and we edited the rule an added Inspection using the file policy InternetFilePolicy and selected Save.



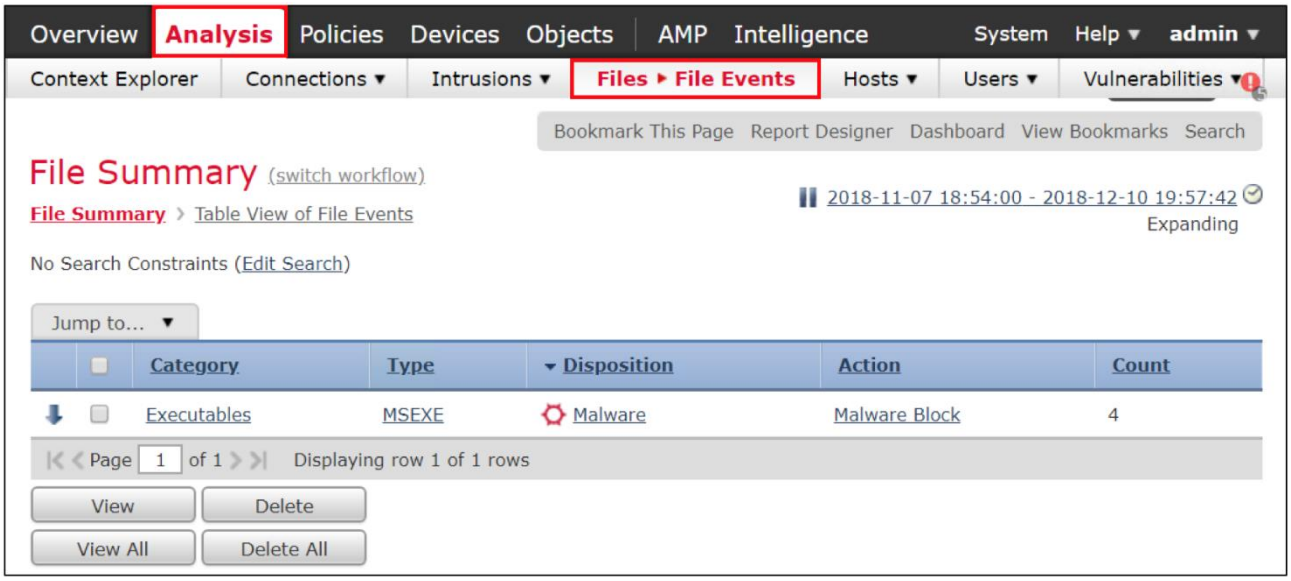
Step 3

a. View Firepower Management Center AMP portal. View Malware Events, navigate to Analysis->Files->Malware Events.

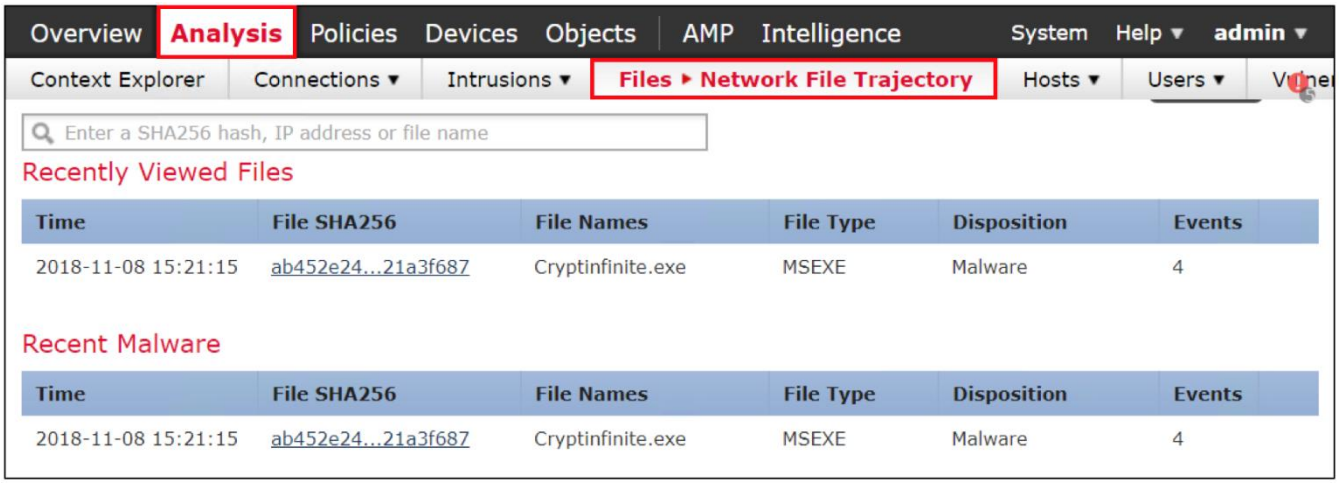


Return to Contents

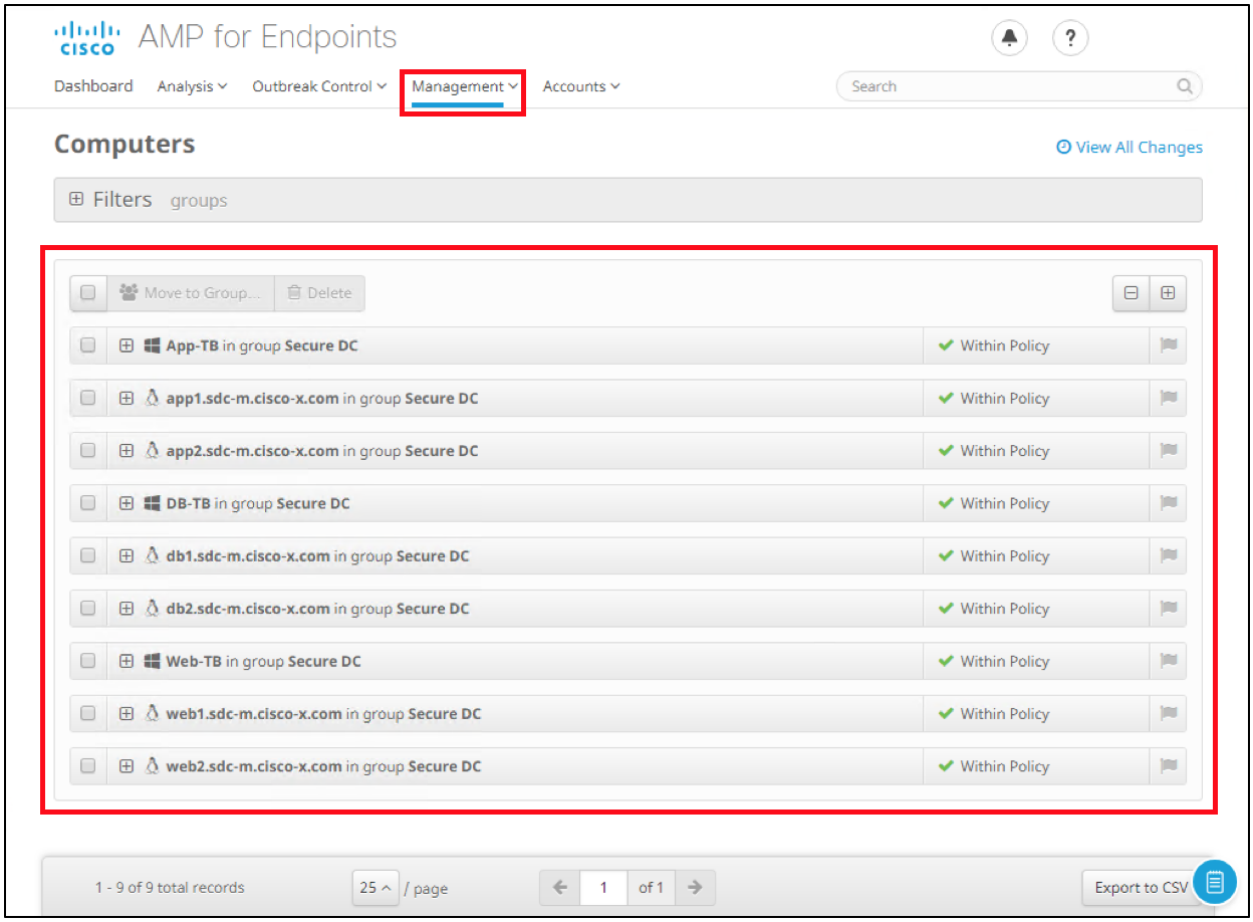
b. View Malware Events, navigate to Analysis->Files->File Events.



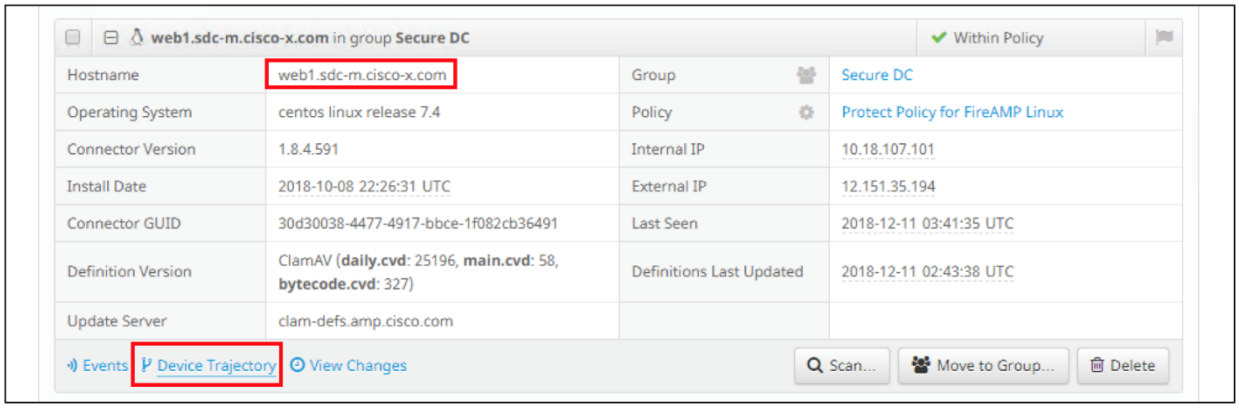
c. View Malware Events, navigate to Analysis->Files->Network File Trajectory.



d. View AMP for Endpoint portal. View all the hosts in the **Secure DC** group.

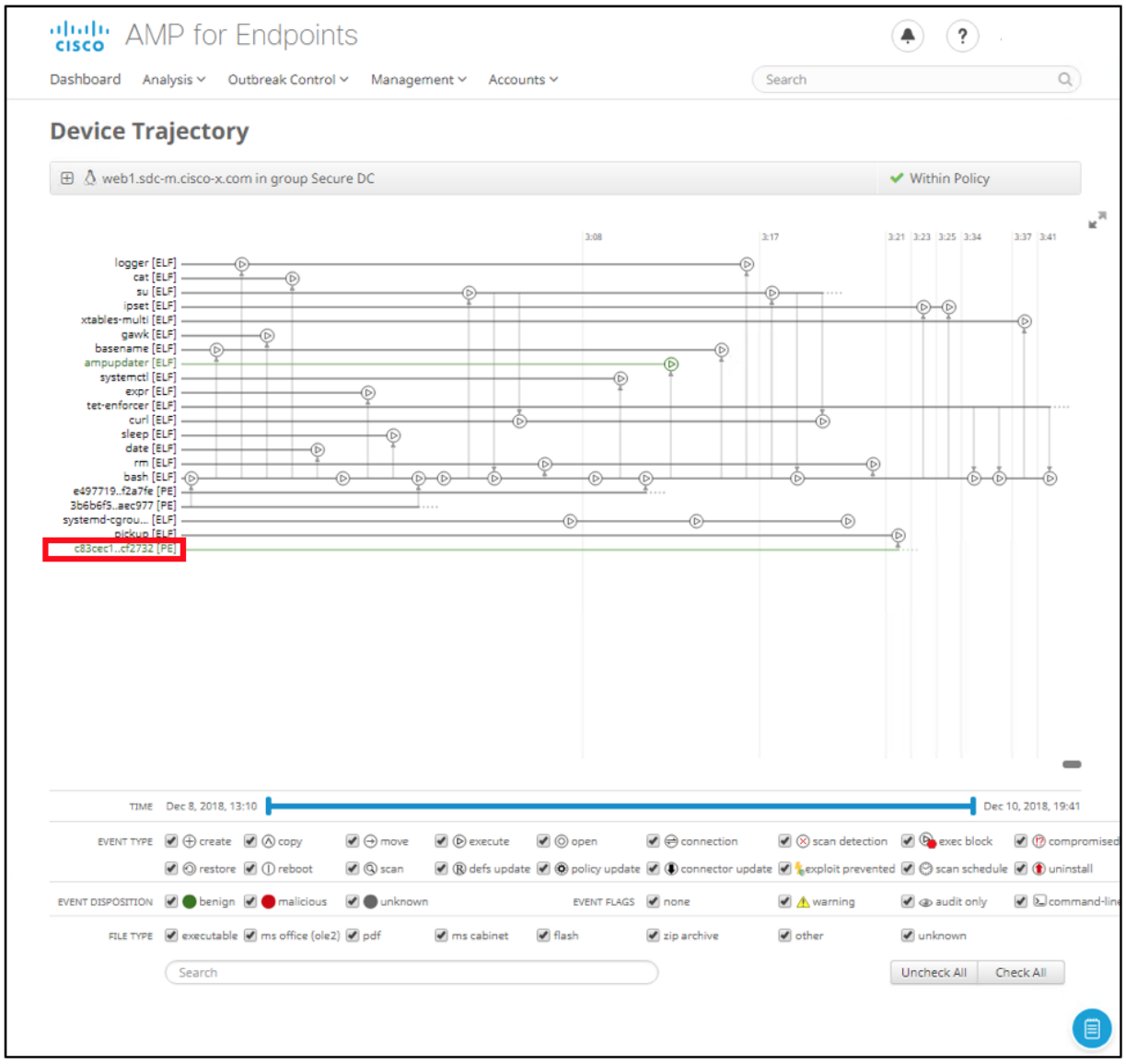


e. View AMP connector information for host **web1.sdc-m.Cisco-x.com**. Select **Device Trajectory** to see a historical representation of all process and file related activities on the host.



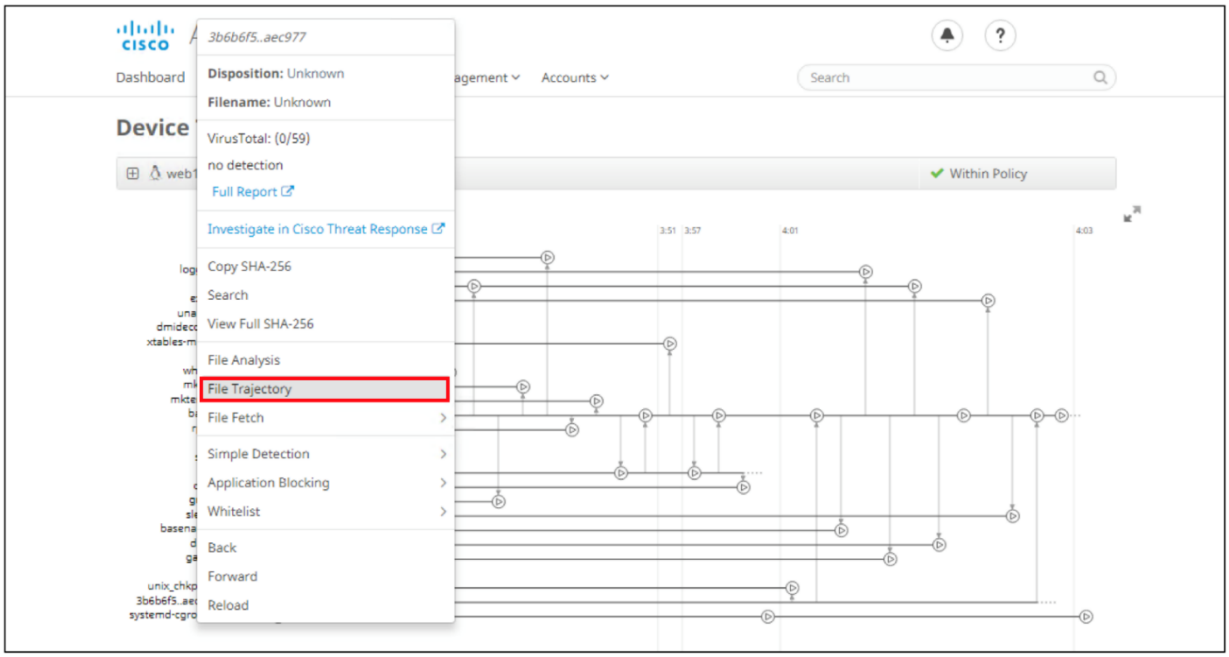
Return to Contents

f. View Device Trajectory. To view File Trajectory, select a **file** to investigate.

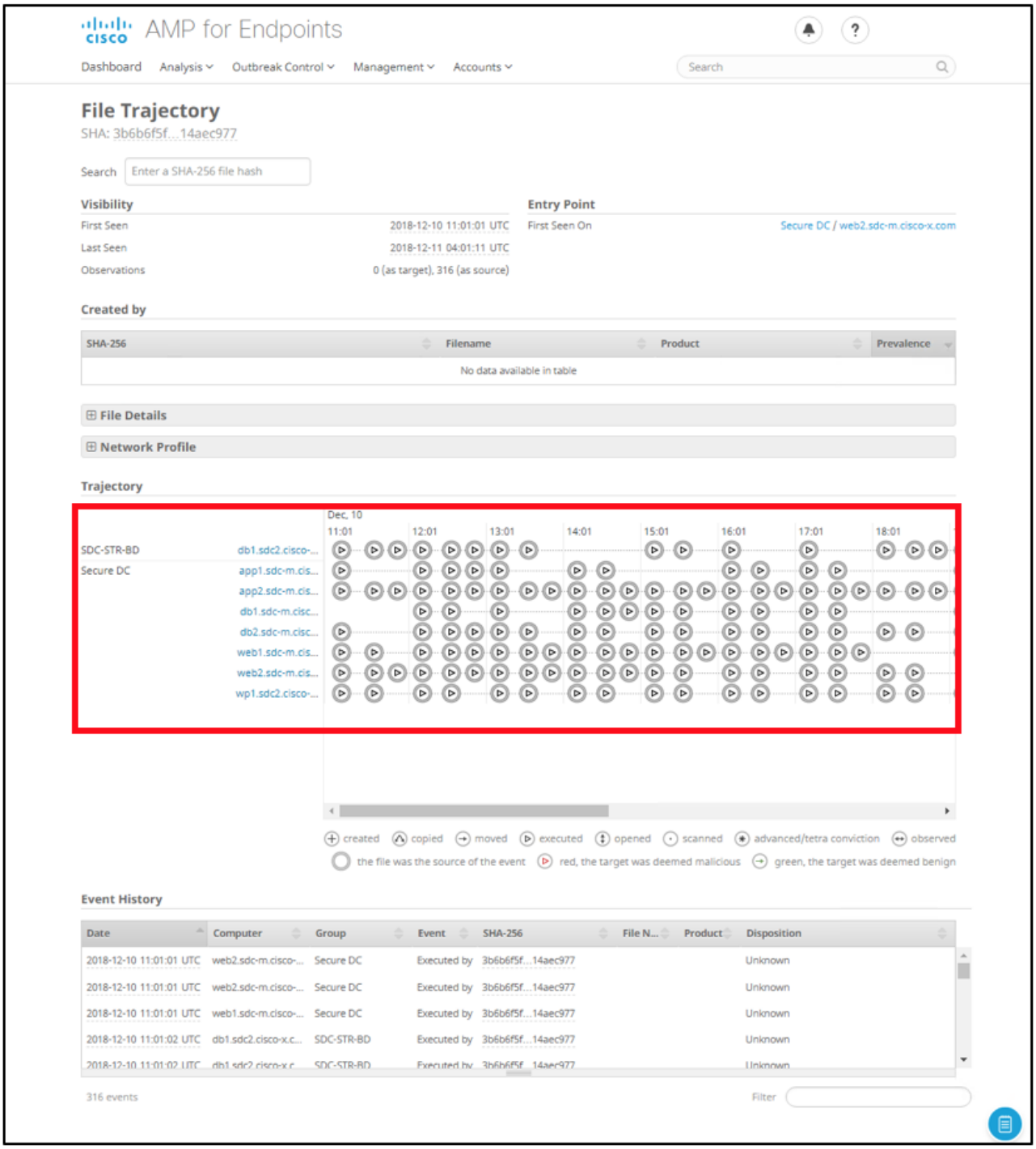


Return to Contents

g. Select **File Trajectory**.



h. View File Trajectory which provides file propagation across the enterprise and the data center in a single view.



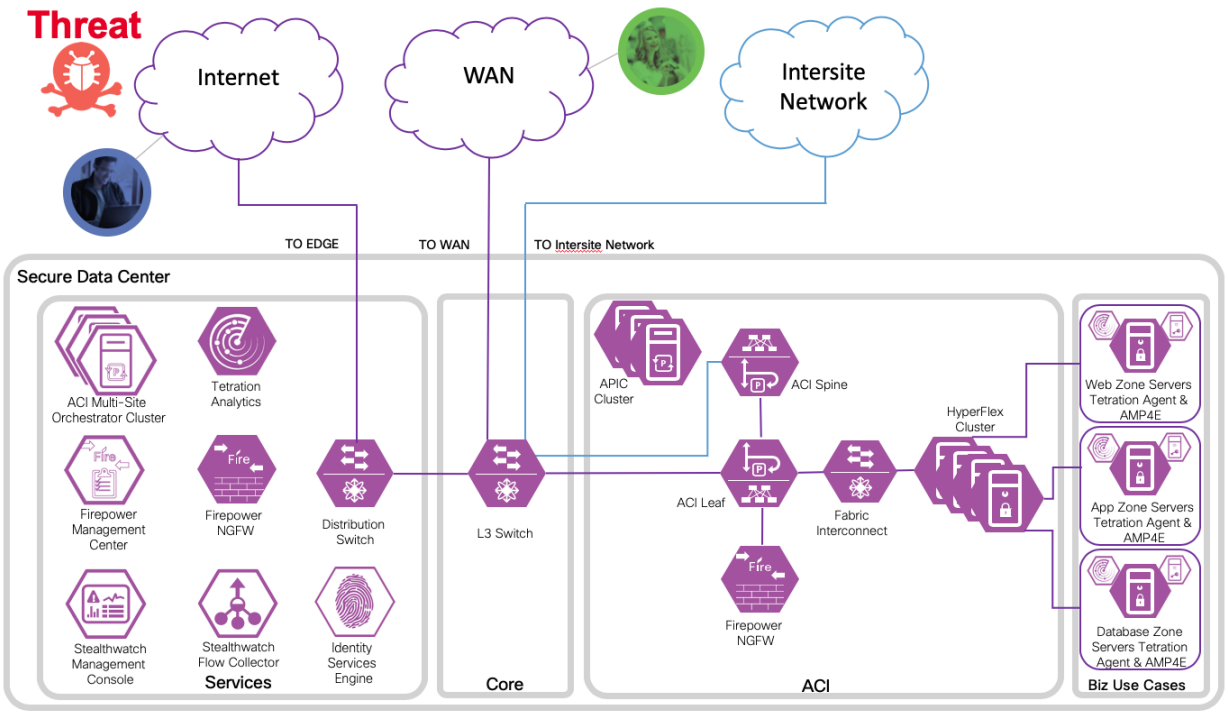
Return to Contents

Test Case 6 – FTD Rapid Threat Containment and APIC

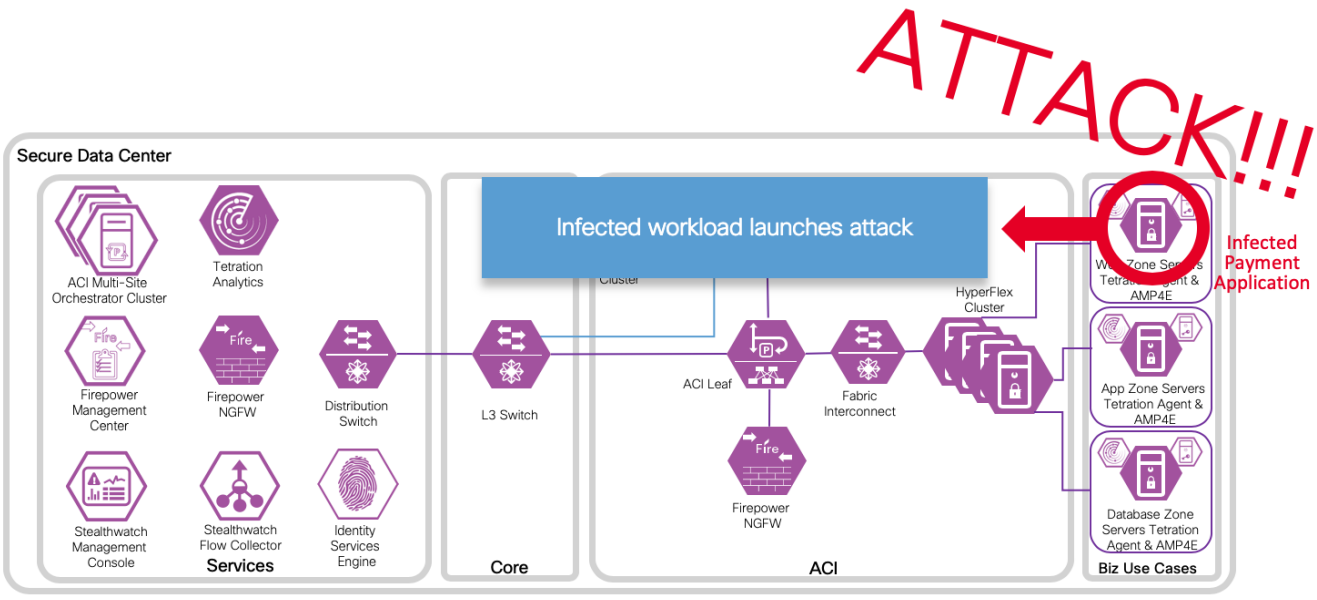
This integration involves identifying an attacker in FMC based on AMP4E, AMP4N, NGIPS and extract the IP address of the attacker. FMC will use this information in the APIC Remediation module to push out policy to quarantine this host.

Test Description:

1. Threat is coming from Internet, on FMC, setup the APIC/Firepower Remediation Module.

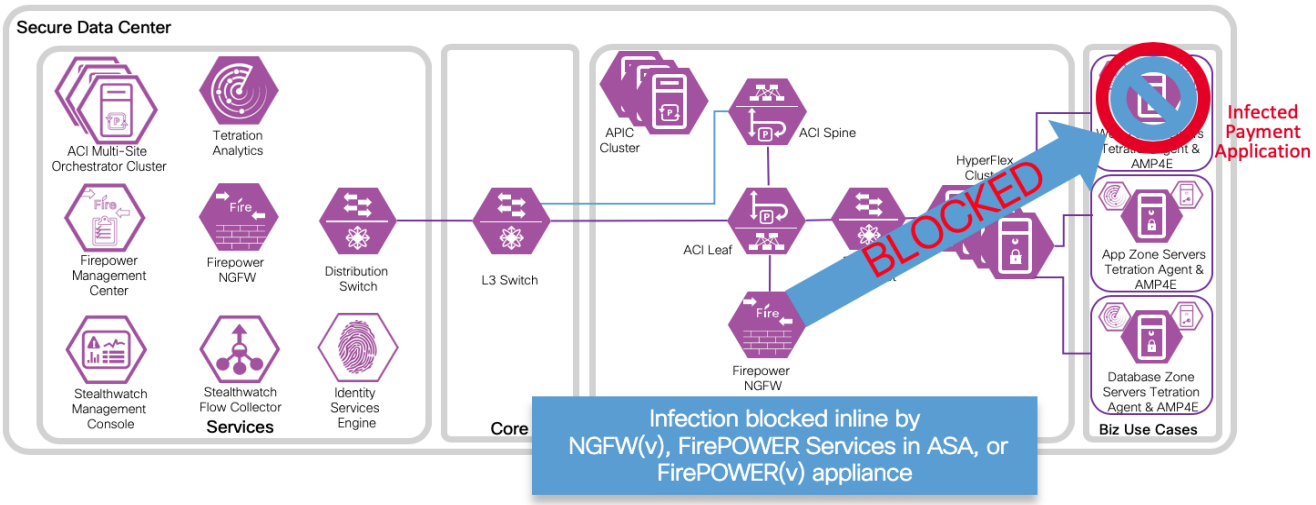


2. An endpoint with an infected application in an EPG launches an attack.

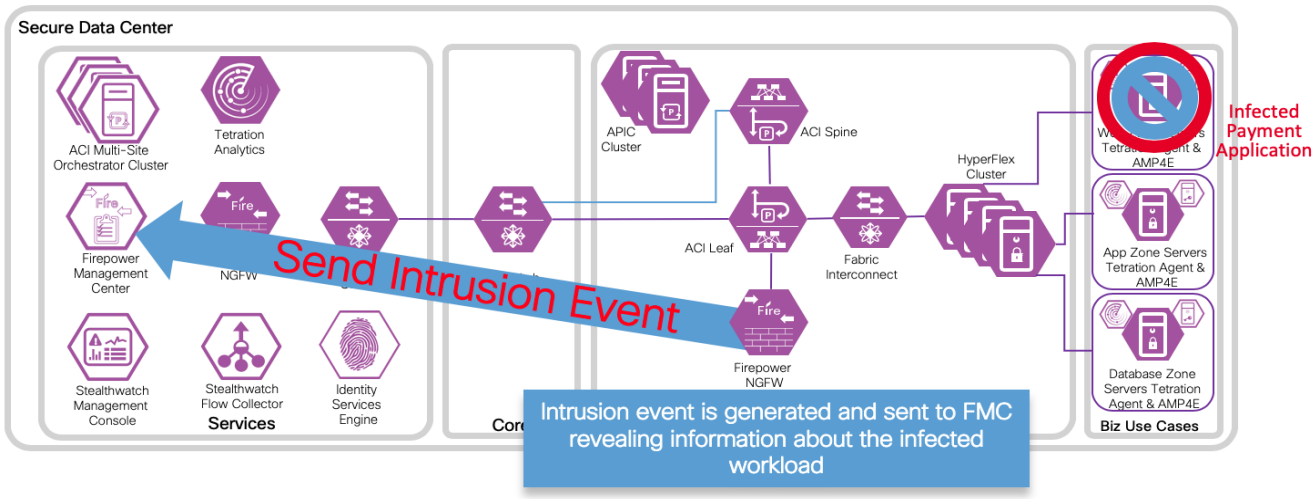


Return to Contents

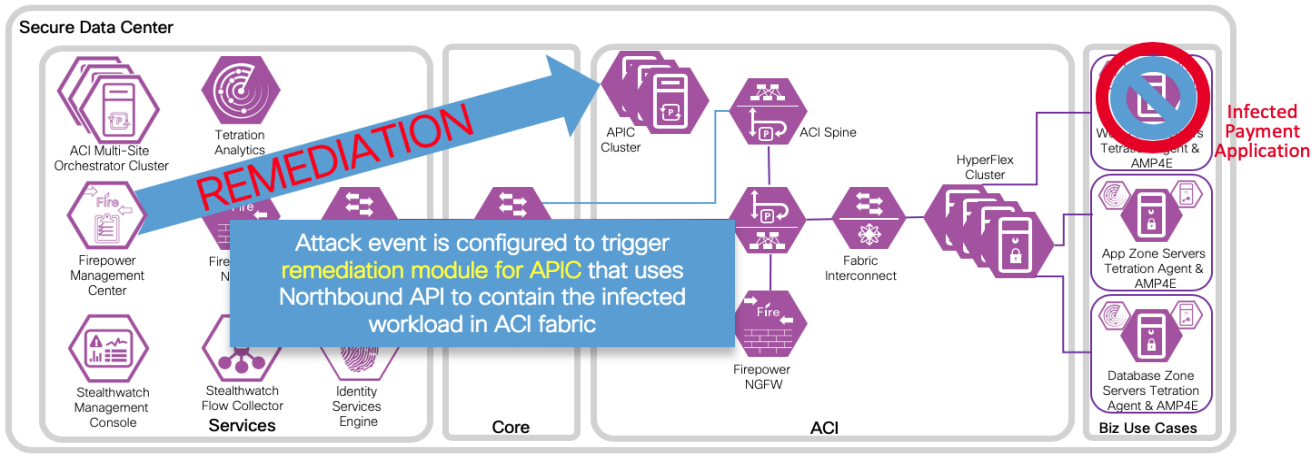
3. The attack is blocked inline by Cisco Firepower Threat Defense.



4. An attack event is generated and sent to the FMC. The attack event includes information about the infected endpoint.

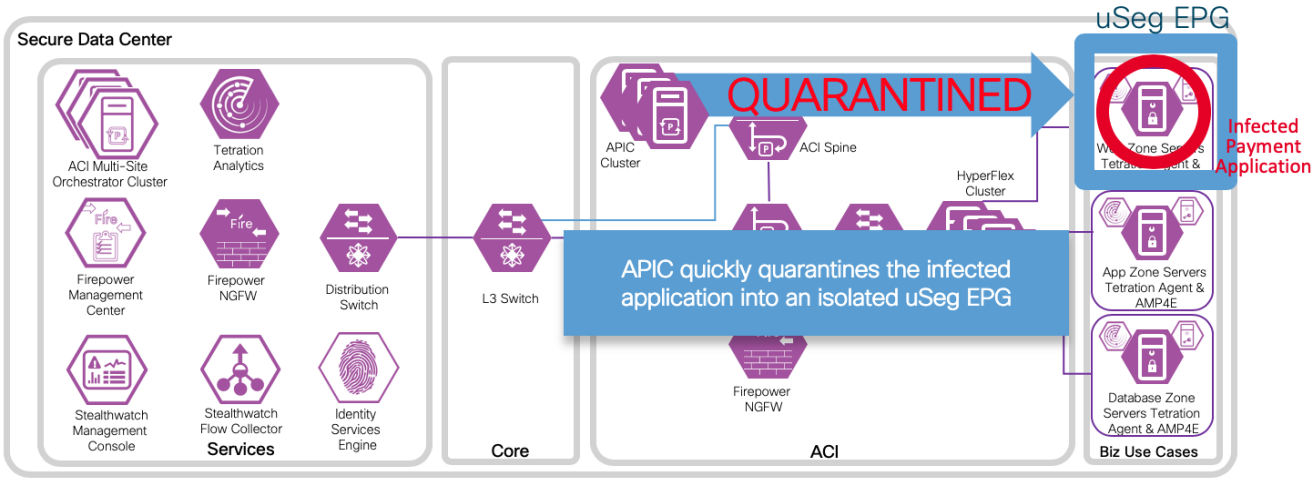


5. The attack event is configured to trigger the remediation module for APIC, which used the APIC northbound API to contain the infected endpoint in the ACI fabric.



Return to Contents

6. The APIC quickly quarantines the infected application workload into an isolated microsegment (uSeg) EPG.



Implementation Procedure

Within the ACI APIC's create a new user/password for the remediation module (or in the AAA provider). Install the APIC remediation module in Firepower Management Center. Configure new instances to enable communication between Cisco Firepower Management Center and each of the APIC clusters. Develop policies to trigger a remediation event and verify with a test.

APIC add user

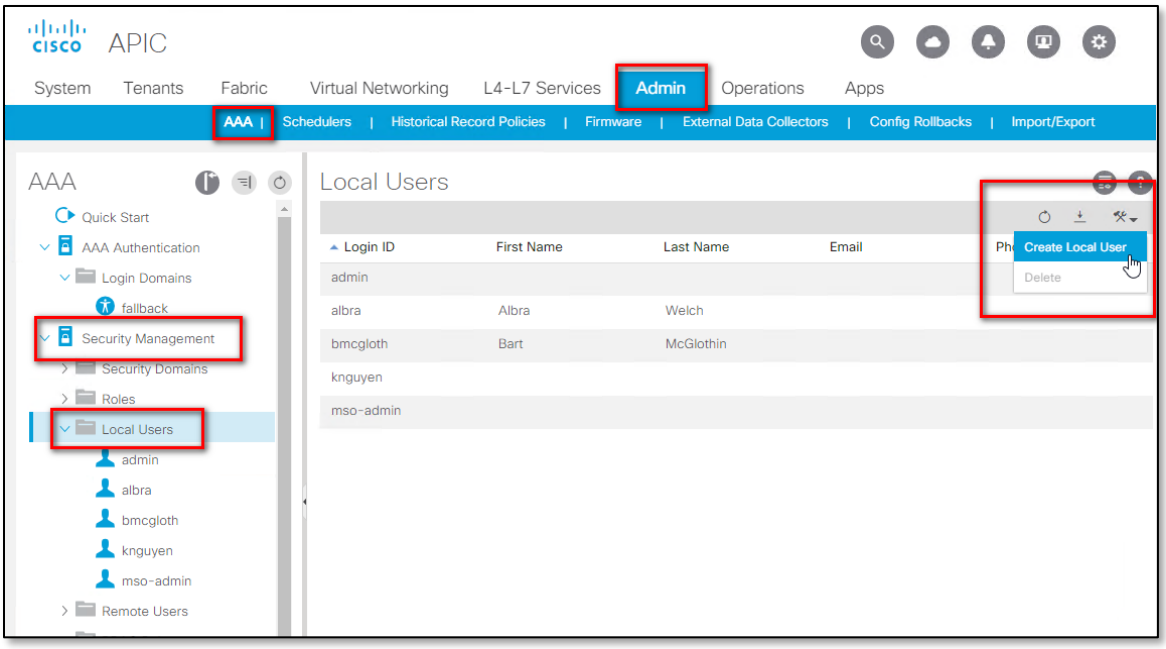
The remediation module uses credentials to authenticate and implement the uSeg request from the Firepower Management Center. These credentials can be created in the AAA provider, or as a local user as outlined in the steps below.

Step 1

a. Log in to the APIC cluster

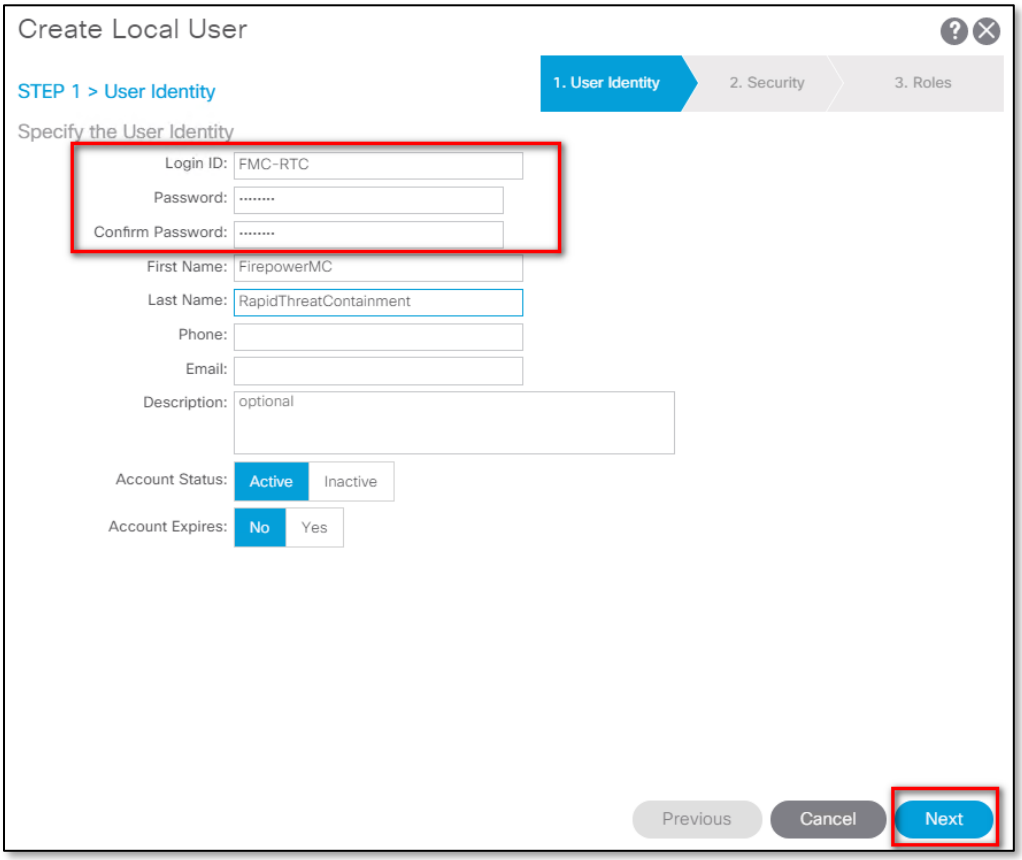
```
https://<your-APIC-server-IP-address>/
```

b. Navigate to **Admin > AAA > Security Management > Local Users** and select **Create Local User** from the menu.



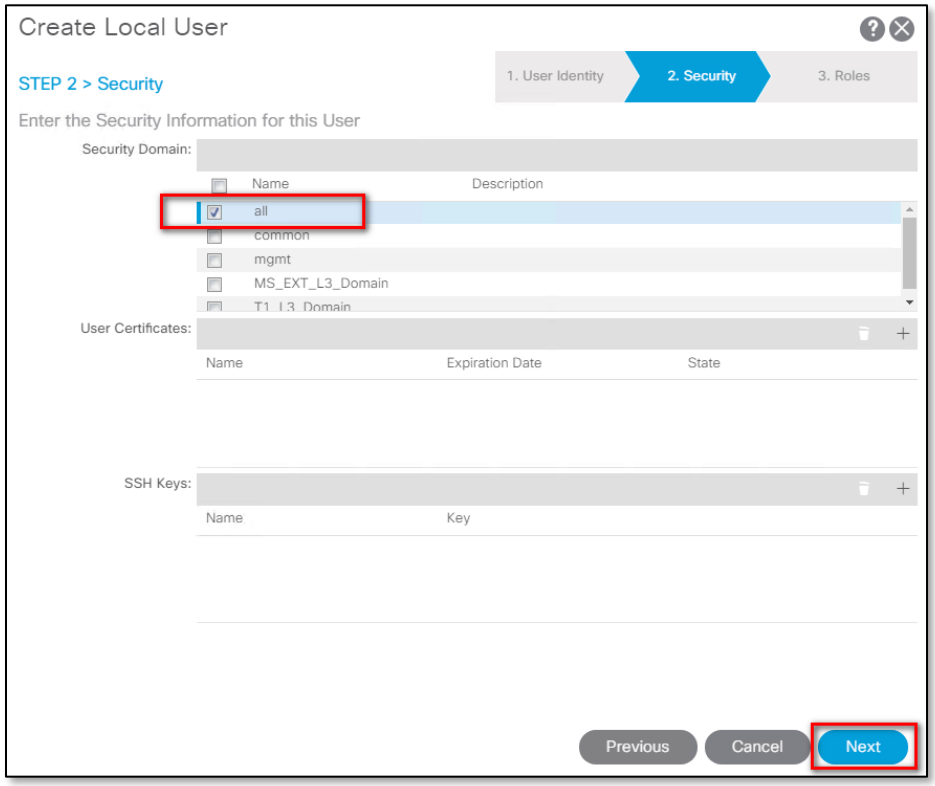
Step 2

a. Enter a descriptive **Login ID**, and a long complex secure **password**, then click **Next**.

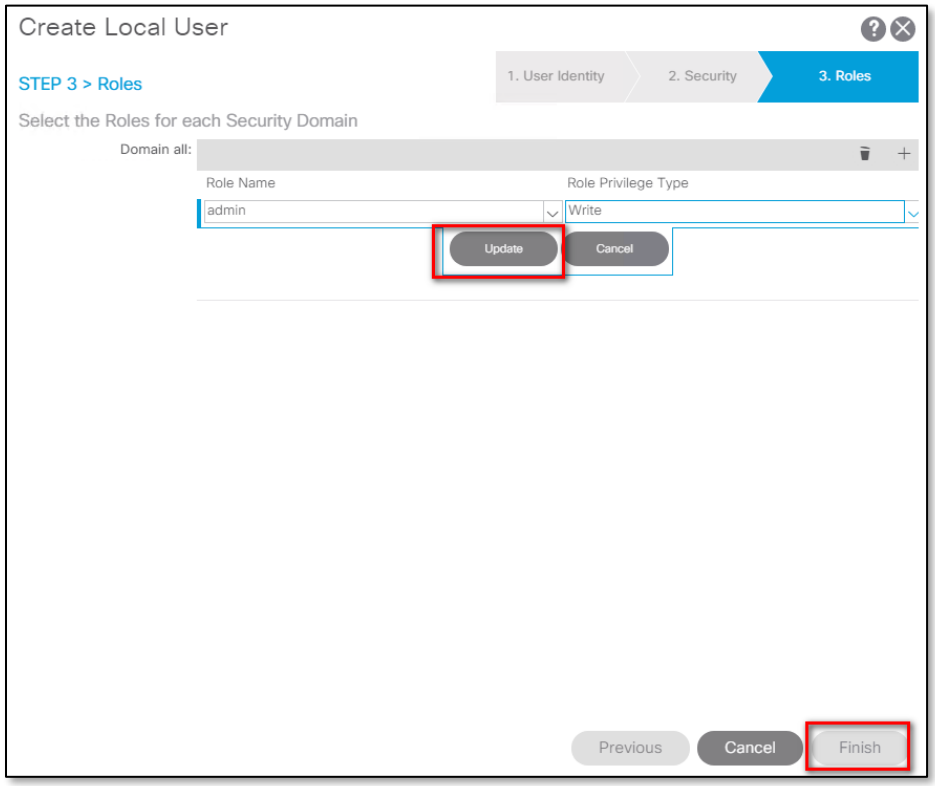


Return to Contents

b. Assign the appropriate security domains to the new user as appropriate for your environment and click **Next**.



c. Assign the appropriate security role and write privilege for your domain click **Update** and **Finish**



d. Repeat for each site.

Return to Contents

Installation

To download and install the Cisco Firepower Management Center Remediation Module for APIC, complete the following procedure:

Step 1 Use a web browser to download the remediation module:

https://software.Cisco.com/download/home/286259687/type/286311510/release/ACI

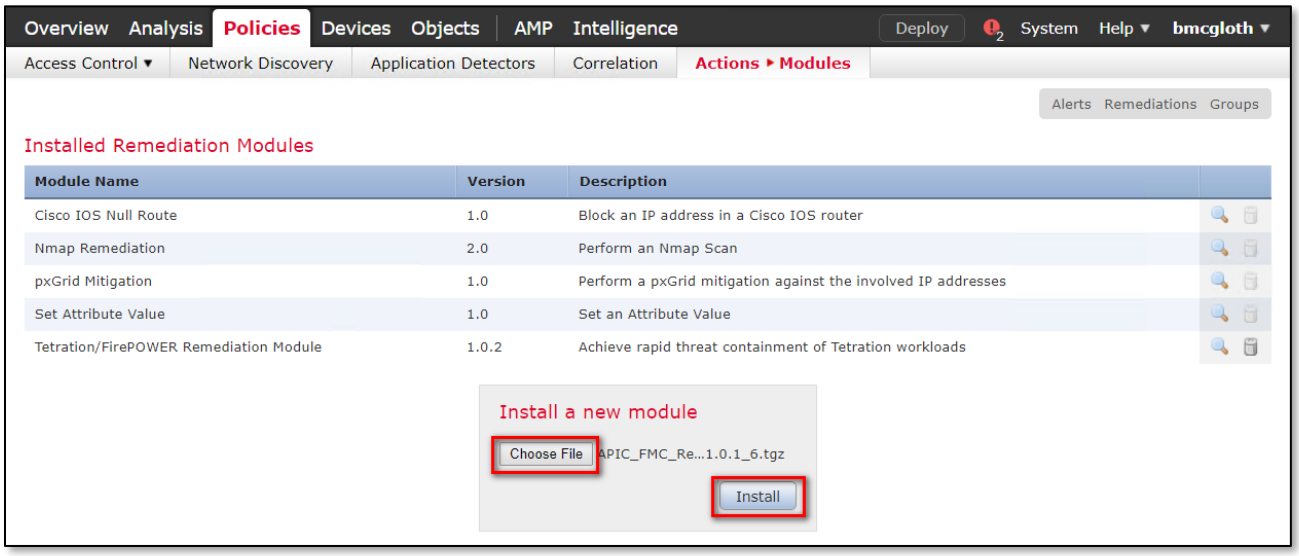
Step 2 Install the remediation module onto the FMC:

a. In the FMC GUI, navigate to **Policies > Actions > Modules.**

b. In the **Install a new module** dialog box, click **Choose File** as shown below.

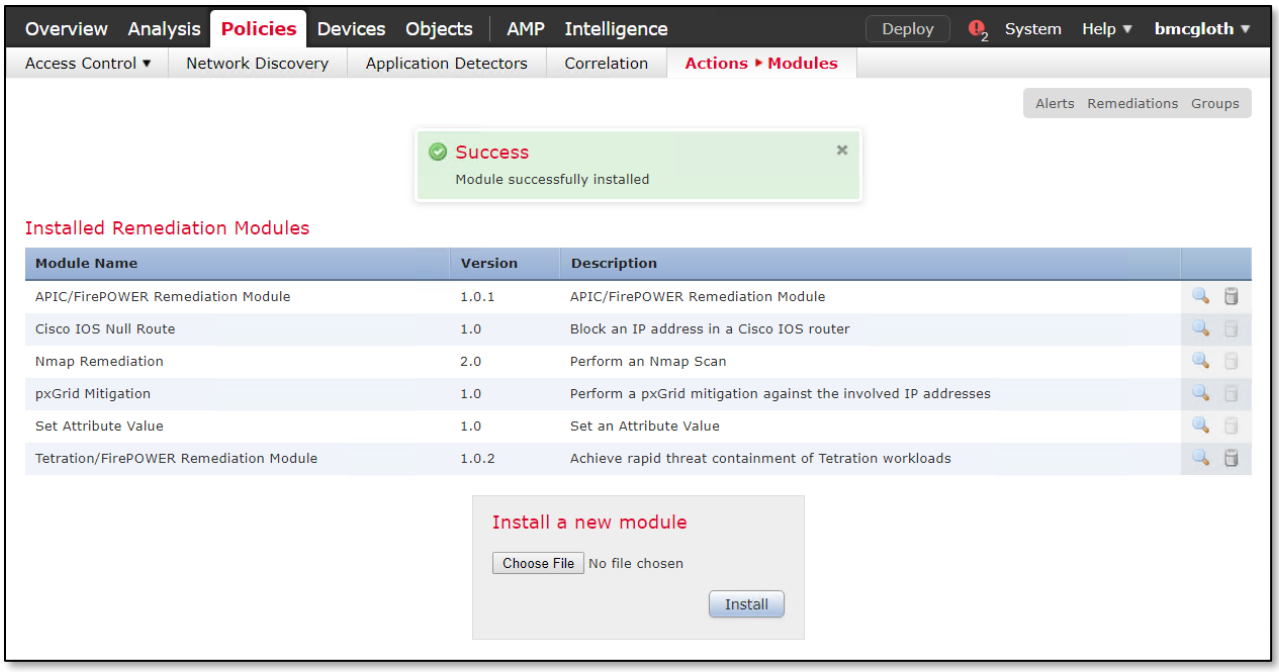
c. Select the file for the remediation module that was downloaded in Step 1.

d. Click **Install**.



NOTE:

If you receive an access error message, clear the error message and repeat Step 2.



When successfully installed, the Cisco Firepower Management Center Remediation Module for APIC is displayed in the list of installed remediation modules.

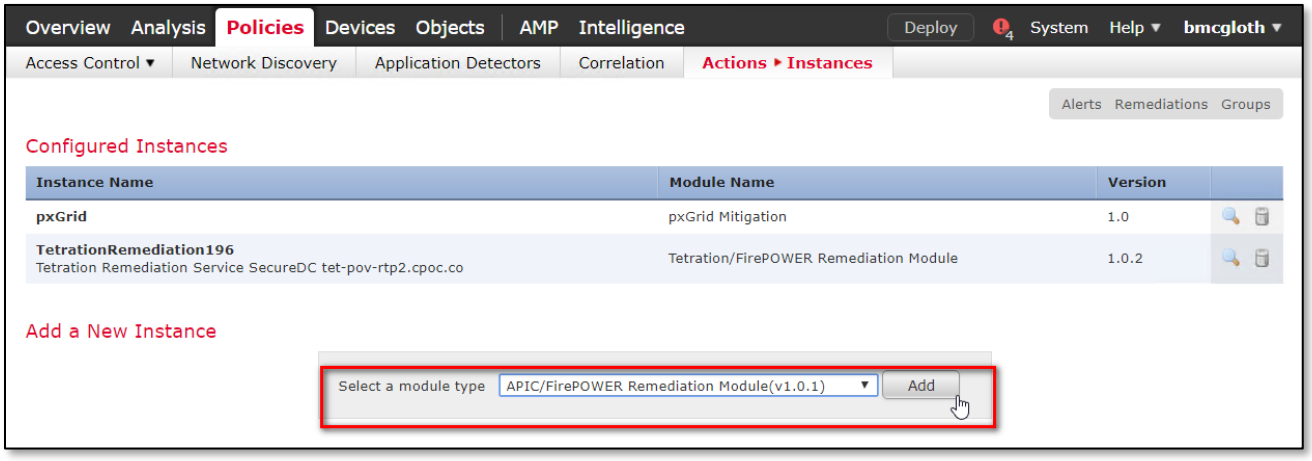
Configuration

To configure the remediation module installed on the FMC, complete the following procedure in the FMC GUI:

Step 1 Create an instance of the remediation module for each APIC Cluster in your network:

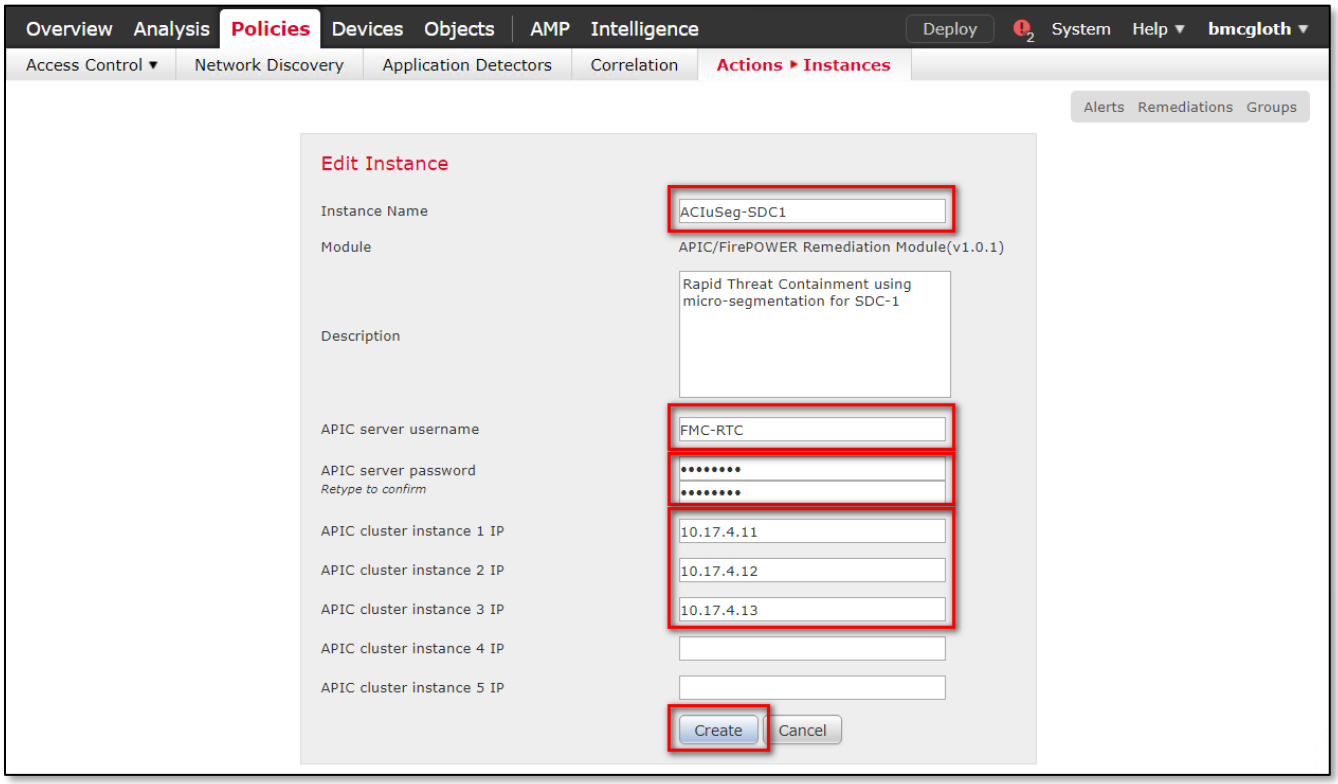
a. Navigate to **Policies > Actions > Instances**.

b. Select the remediation module in the drop-down list, and click **Add**.

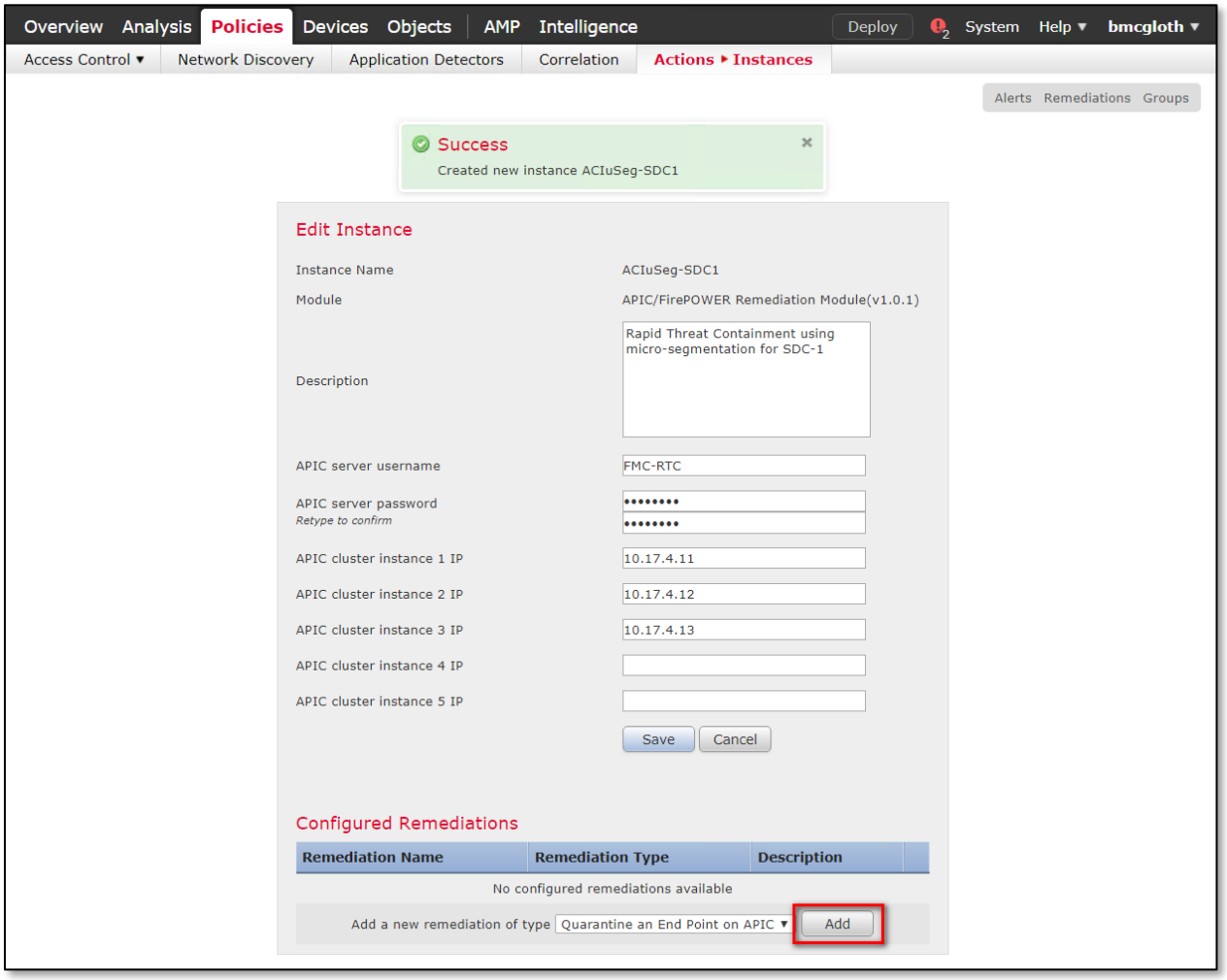


c. Enter an **Instance Name** (in this example, `ACIuSeg-SDC1`) and **description** (optional).

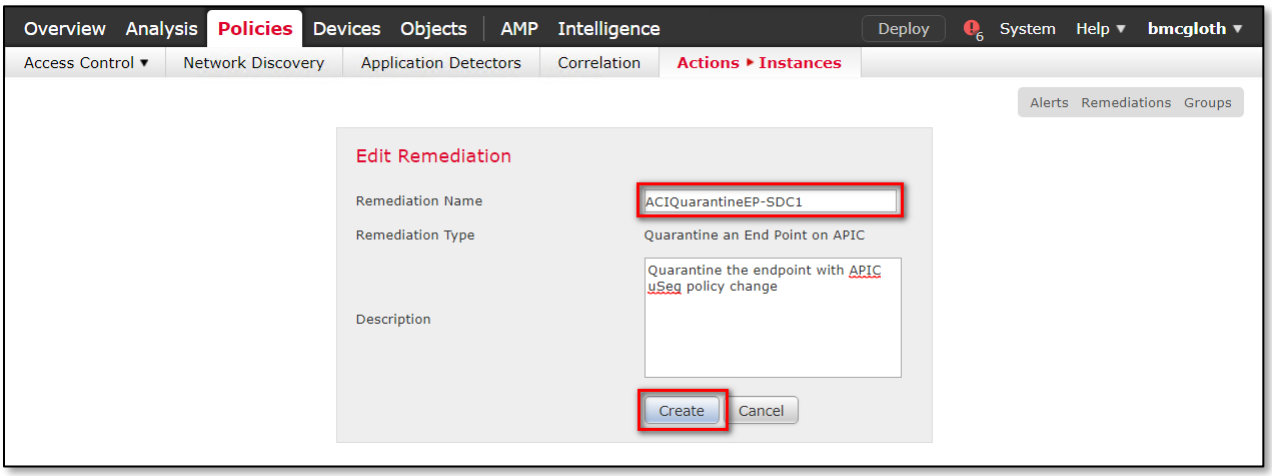
d. Enter the APIC Cluster's **Username**, **Password** and **IP addresses**. Click **Create**.



e. Under **Configured Remediations**, select a type of remediation (in this example, quarantine an End Point on APIC), and click **Add** to add a new remediation.

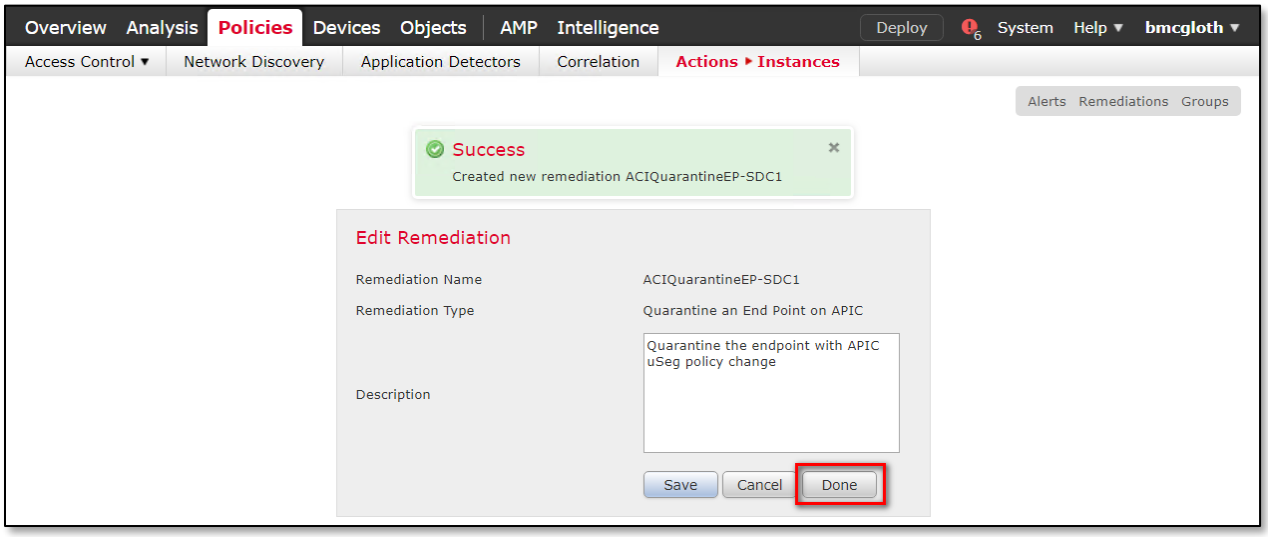


f. Enter a **Remediation Name** (in this example, `ACIQuarantineEP-SDC1`), and click **Create**.



Return to Contents

g. Return to the Instance configuration by clicking **Done**.



h. The remediation you just configured then shows up in the table. Click **Save**.

Step 2 Repeat the configurations a-h outlined in Step 1 for each APIC cluster in a Multi-Site deployment.

Step 3 Configure the policy to log connections to be tested for intrusion, in this example we identify CnC traffic.

Configure an access control policy (in this example, `SDC-Multisite-FTD-C1`):

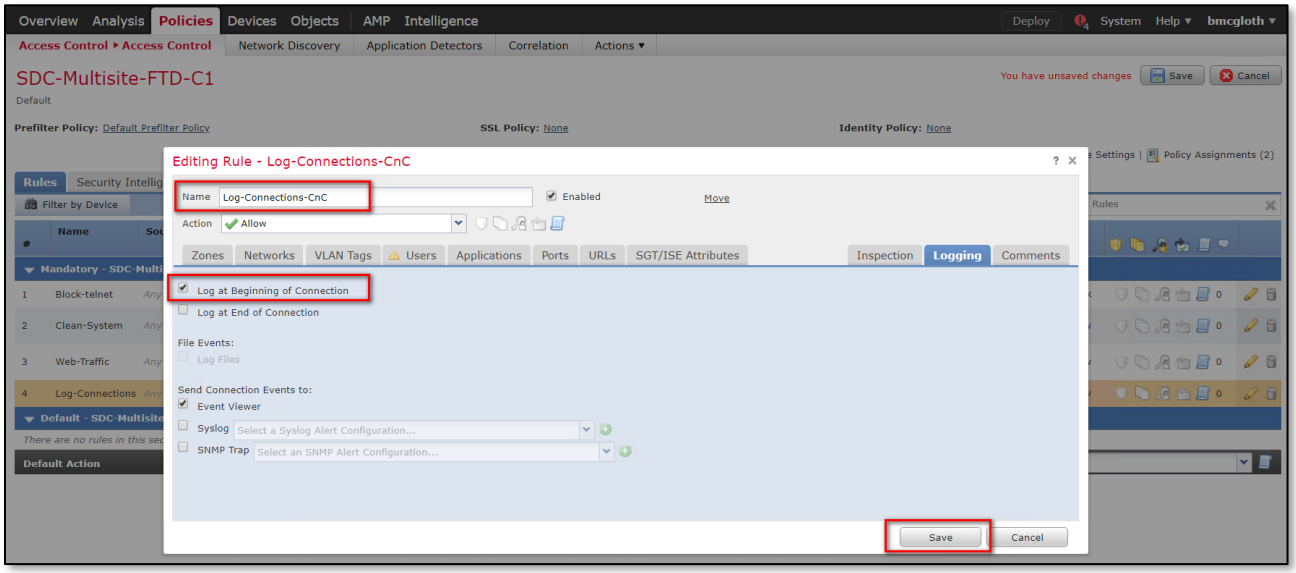
a. Navigate to **Policies > Access Control** then **Edit** the policy.

b. Click **Edit Rule** (for example, `Log-Connections-CnC or Web Traffic`).

c. On the Logging tab, select **Log at Beginning of Connection**.

Important

Ensure that logging is enabled each of the access rules, so that the FMC receives event notifications.



d. Click **Save**.

Return to Contents

e. Then **Save** and **Deploy** the policy.

Step 4 Configure a correlation rule:

a. Navigate to **Policies > Correlation > Rule Management**.

b. Click the **Create Rule** button.

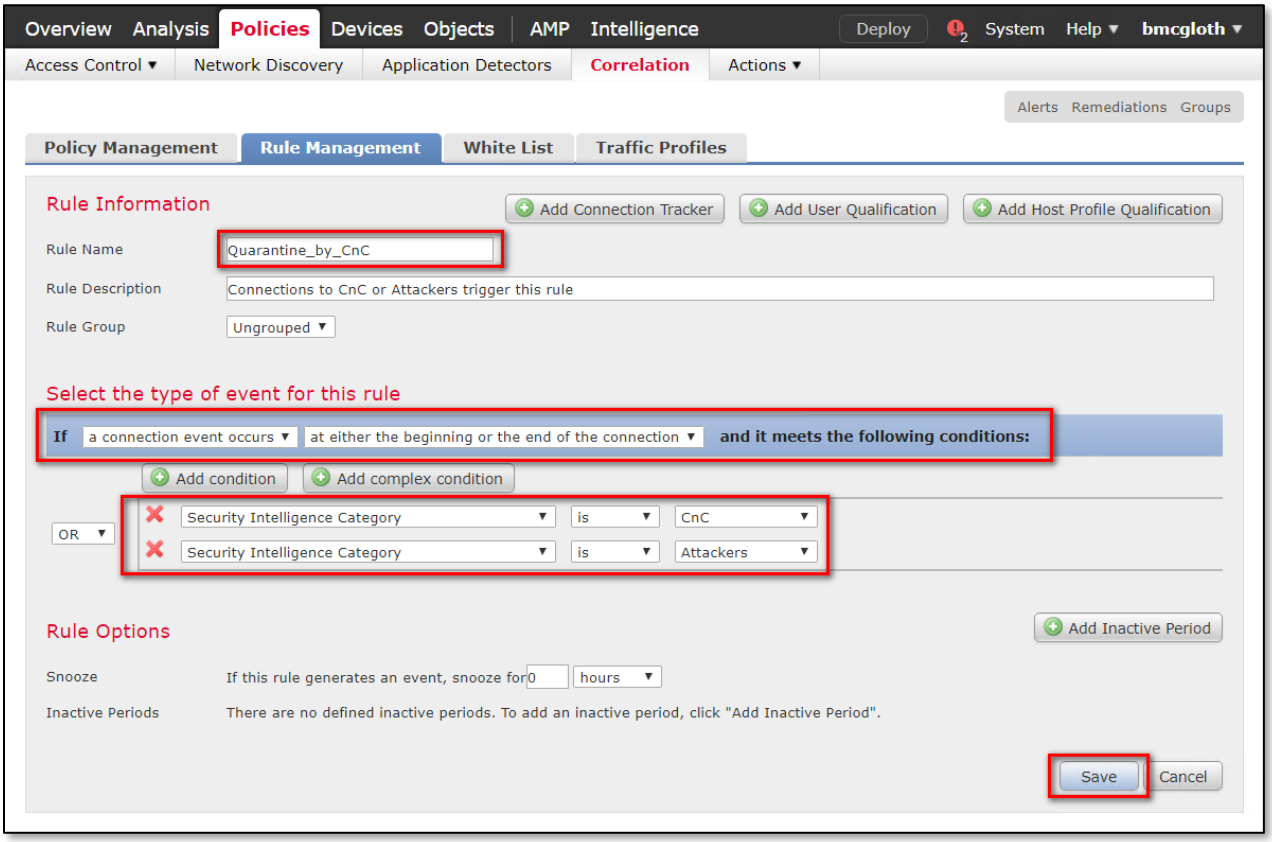
c. Enter a **Rule Name** (in this example, `Quarantine_by_CnC`) and **description** (optional).

d. In the **Select the type of event for this rule** section, select **a connection event occurs** and **at either the beginning or the end of the connection**.

e. In the drop-down list, select **Security Intelligence Category**, operator set to **is**, and category set to **CnC**.

f. Click **Add condition**, and check the operator is set to **OR** instead of **AND**.

g. In the drop-down list, select **Security Intelligence Category**, operator set to **is**, and category set to **Attackers**.



h. Click **Save**.

NOTE:

There are several other categories that may also be desirable to add; Bogon, Bots, Dga, Exploitkit, Malware, OpenProxy, OpenRelay, Phishing, Response, Spam, Suspicious, and TorExitNode.

For more information, please visit:
https://www.Cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/security_intelligence_blacklisting.html

Step 5 Associate the instance of the remediation module as a response with a correlation rule:

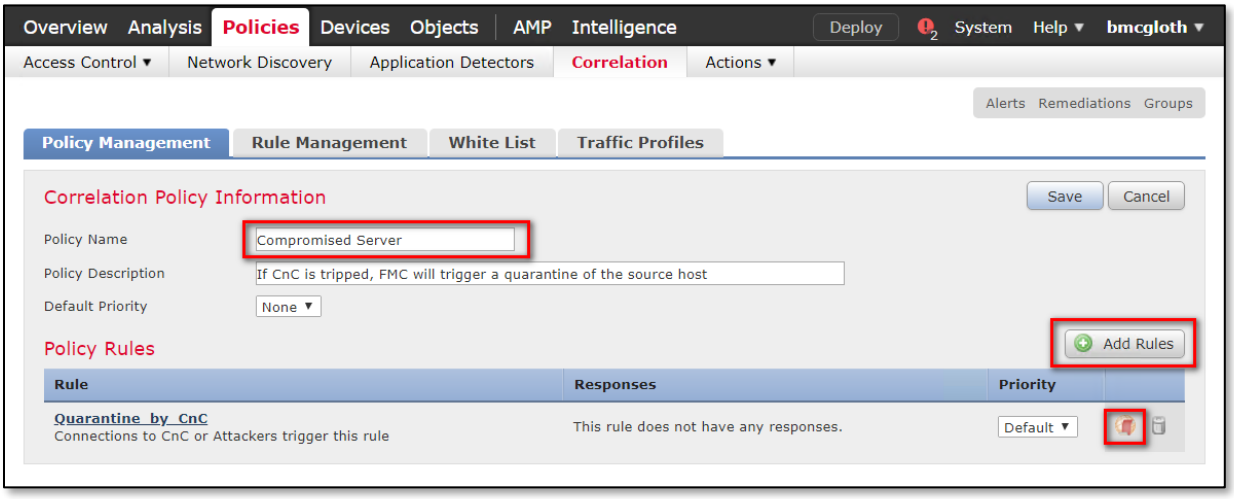
a. Navigate to **Policies > Correlation > Policy Management**.

b. Click Create Policy.

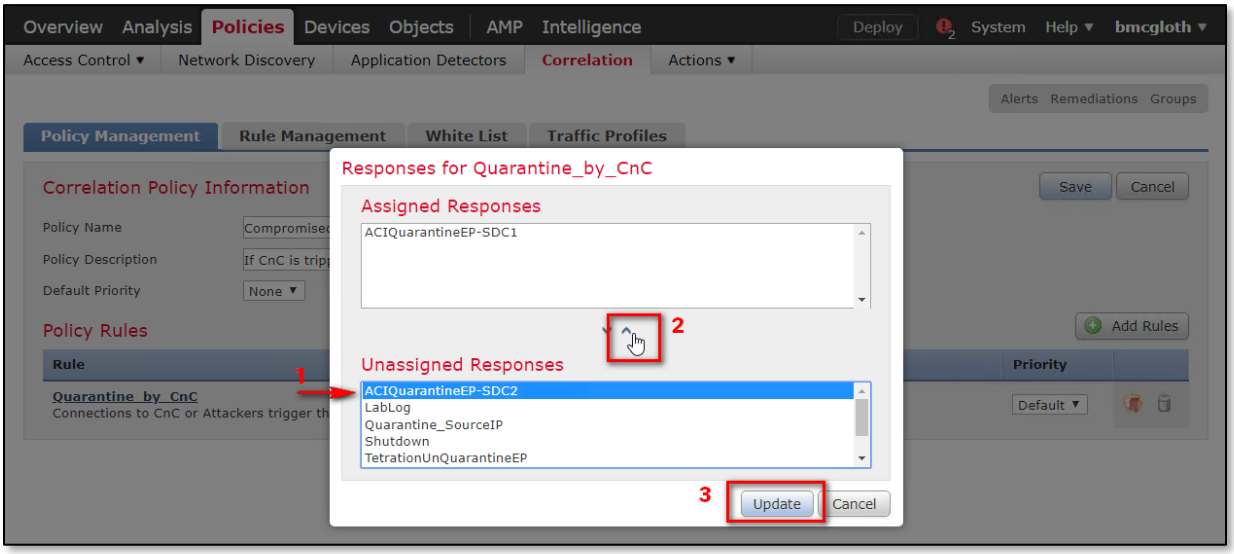
c. Enter a **Policy Name** (in this example, `Compromised Server`) and **description** (optional).

d. From the **Default Priority** drop-down list, select a priority for the policy. Select **None** to use rule priorities only.

e. Click **Add Rules**, select the correlation rule you previously configured in Step 3 (in this example, `Quarantine_by_CnC`), and click **Add**.

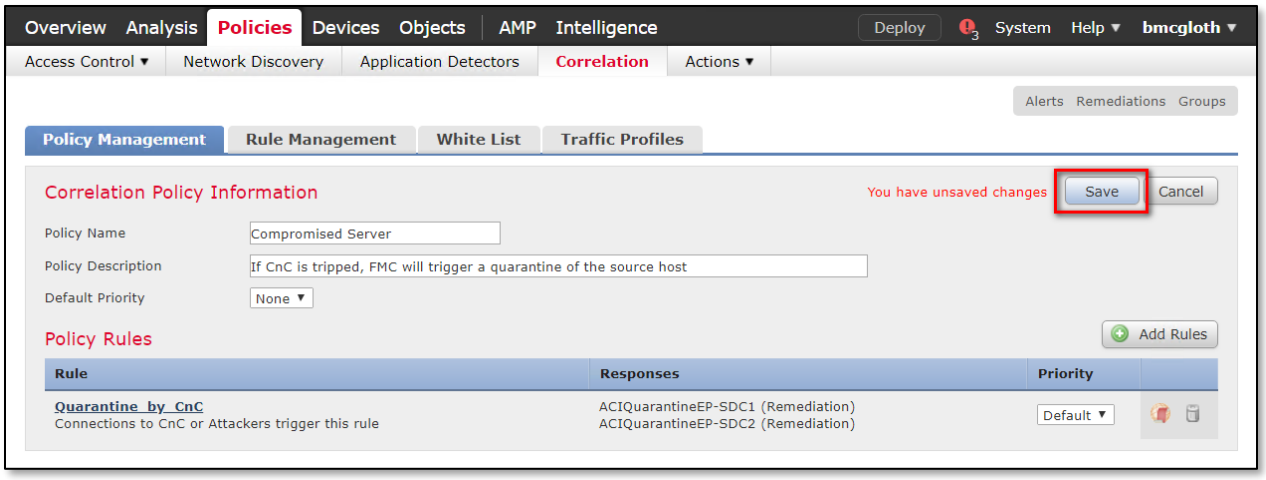


f. Click the **Responses** icon next to the rule and assign a response (in this example, `ACIQuarantineEP for both SDC's`) to the rule.



g. Click **Update**.

Return to Contents



h. Click **Save**.

Verify

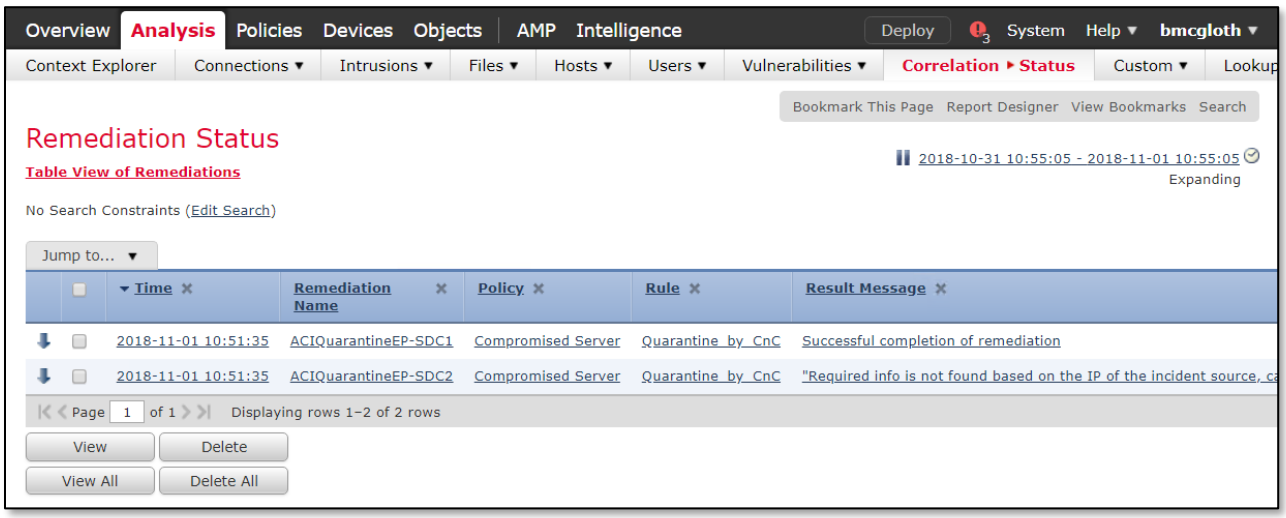
Because remediations can fail for various reasons, perform the following steps to verify that a remediation is successful:

Step1 Once the remediation module is triggered by an associated correlation rule, check the status of the remediation execution in the FMC GUI (ping a known CnC server on the internet after first creating a black hole for this IP via a null route or loop interface to prevent real leakage to the internet).

Within seconds the policy should take effect and be visible in FMC as well as the APIC interface after a screen refresh.

Step 2 Navigate to **Analysis > Correlation > Status**.

Step 3 In the Remediation Status table, find the row for your policy and view the result message. The event is sent to both clusters, and the site hosting the compromised server should show successful completion of remediation, while the other sites will respond with IP not found results.



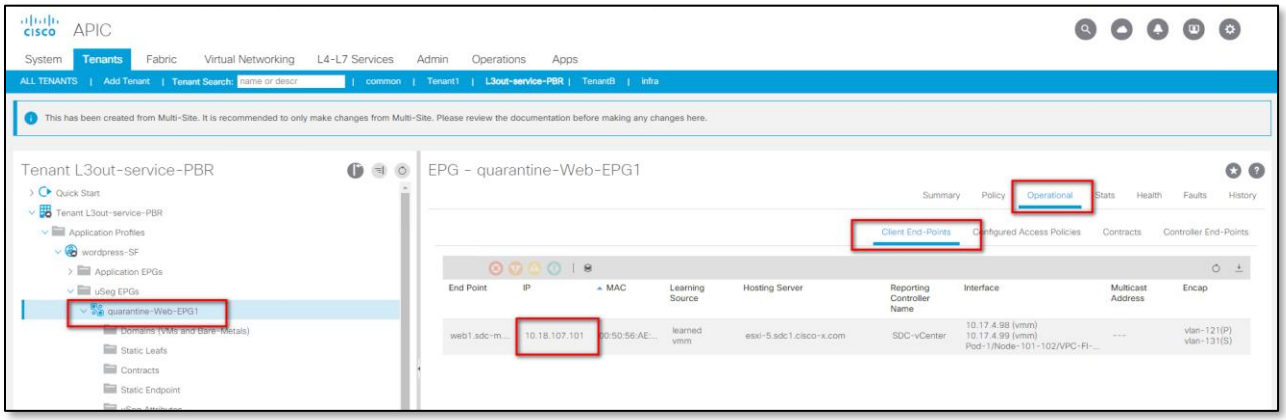
Step 4 Go to the APIC GUI:

a. Navigate to **Tenant > Application Profiles > uSeg EPGs**.

b. Select the newly created quarantine EPG (in this example, `quarantine-Web-EPG1`).

Return to Contents

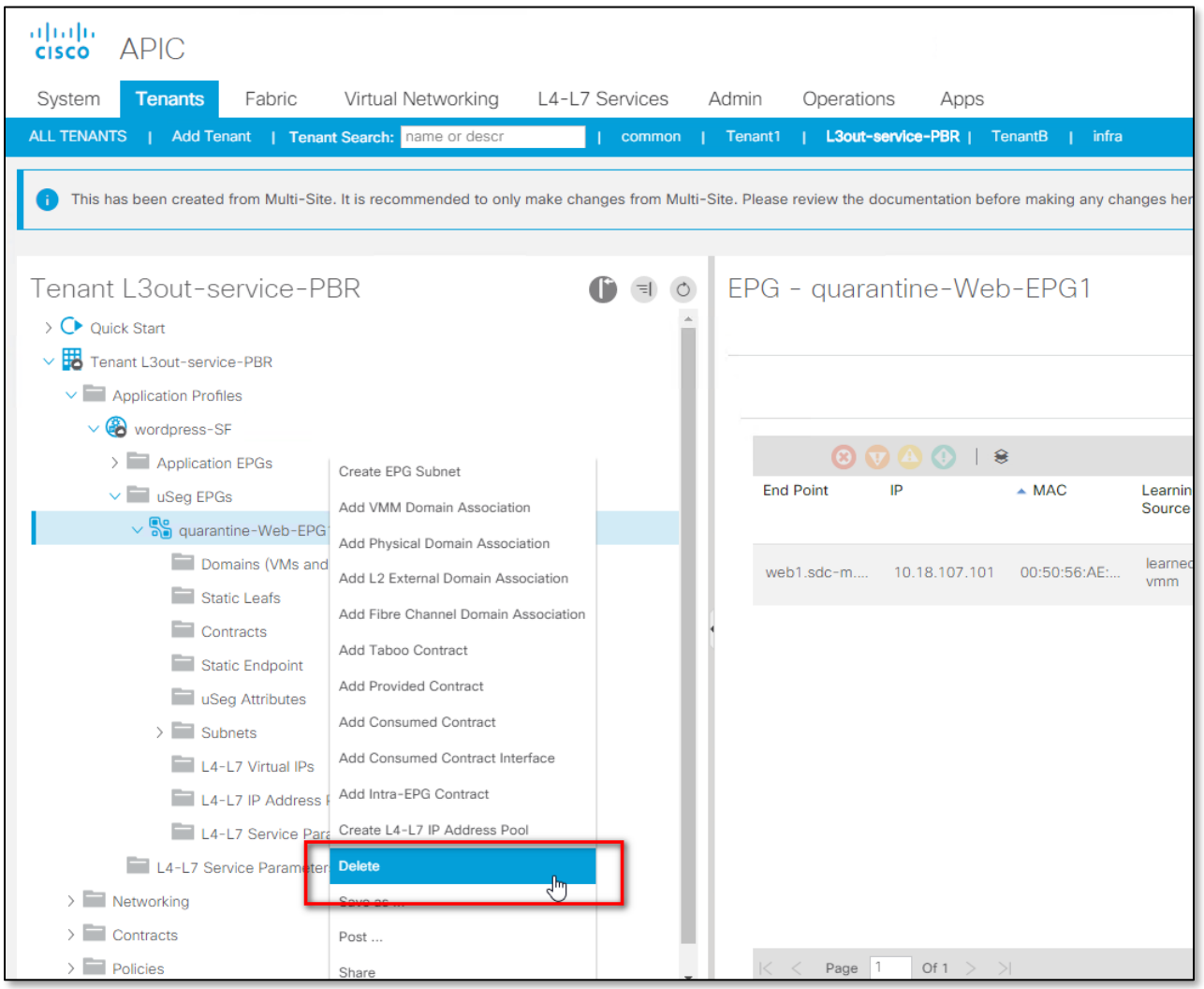
c. Select **Operational > Client End-Points** and verify the correct server IP quarantined.



Step 5 What to do next

Once you clean the quarantined host and it is no longer infected, you can remove the micro-segmentation by deleting the uSeg EPG manually.

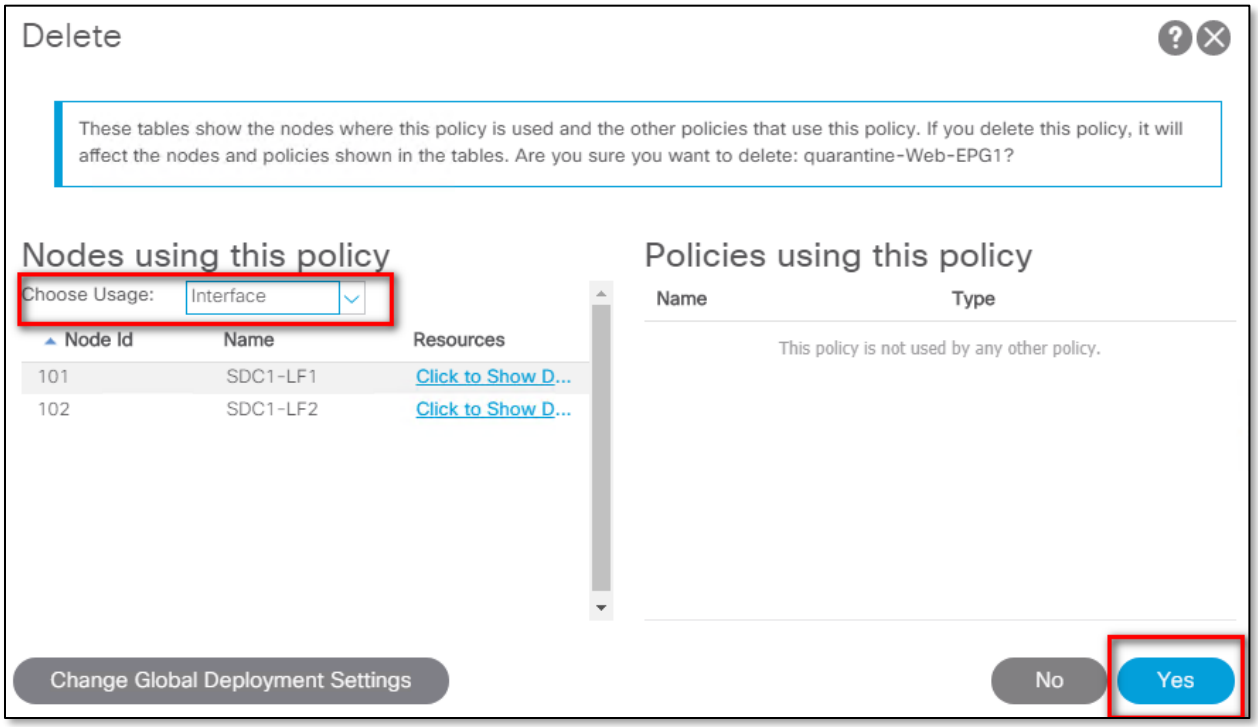
Navigate to **Tenants > {your Tenant} > Application Profiles > uSeg EPGs**. Alternate click on the uSeg and select **Delete** from the option menu.



Return to Contents

221

Verify the affected interfaces and confirm the deletion by clicking **Yes**.



Normal connectivity for the system is restored as the host returns to its original EPG.

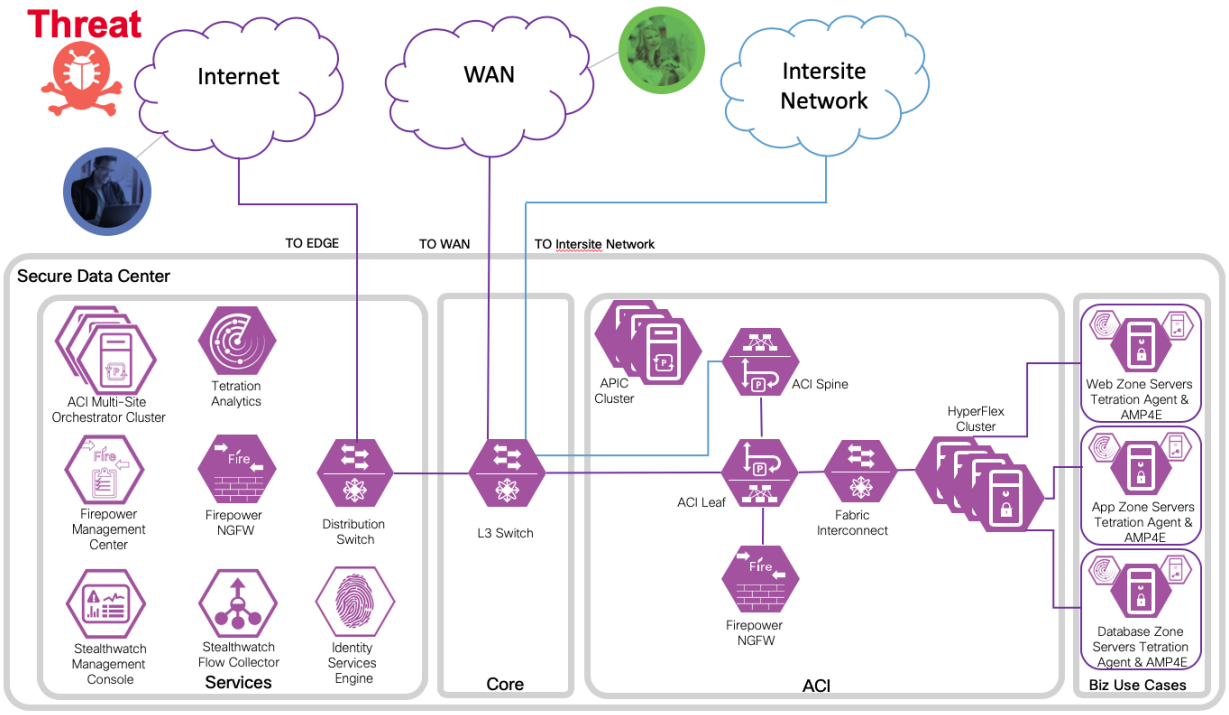
Return to Contents

Test Case 7 – FTD Rapid Threat Containment with Tetration

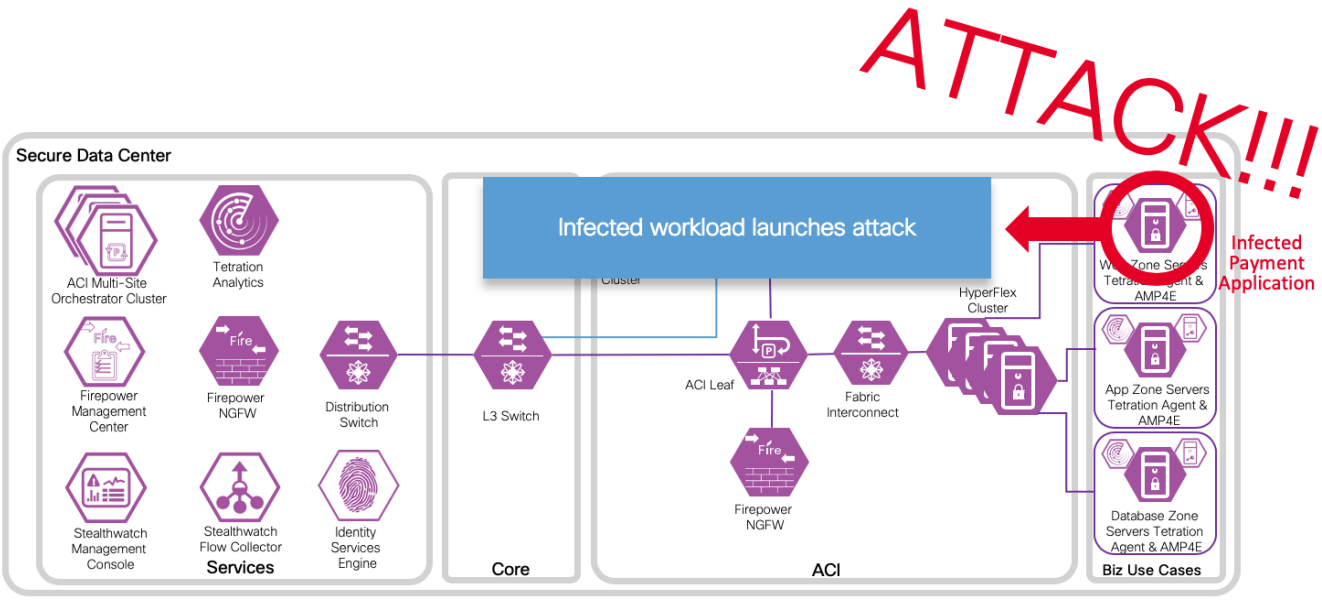
This integration involves identifying an attacker in FMC based on AMP4E, AMP4N, NGIPS and extract the IP address of the attacker. FMC will use this information in the Tetration Remediation module to push out policy to quarantine this host.

Test Description:

1. Threat is coming from Internet, on FMC, setup the Tetration/Firepower Remediation Module and Tetration agent installed on all application servers.

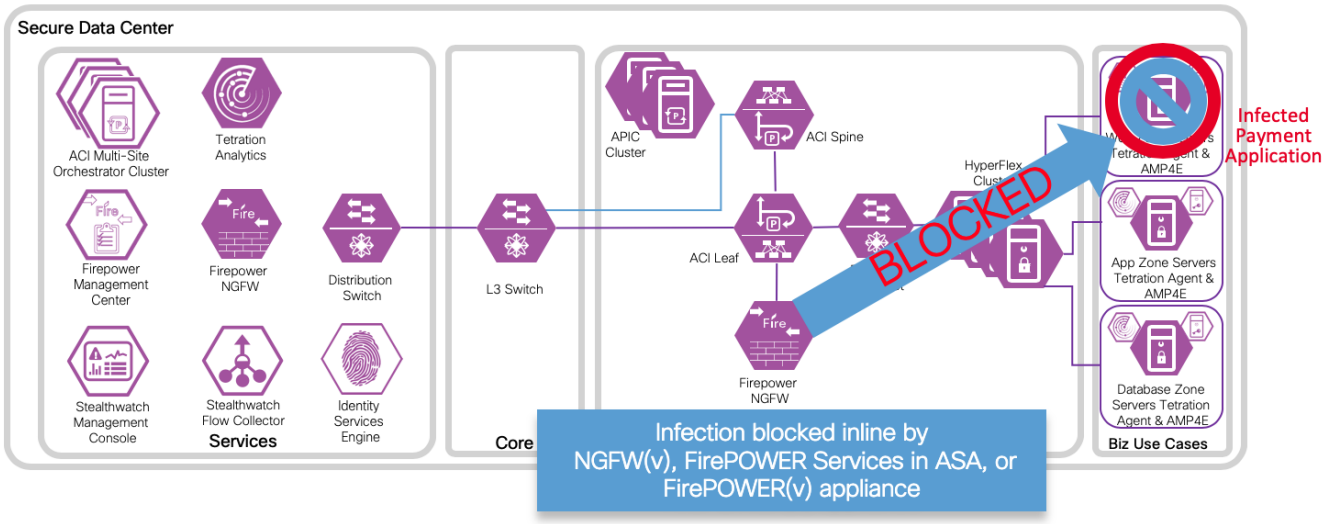


2. An endpoint with an infected application launches an attack.

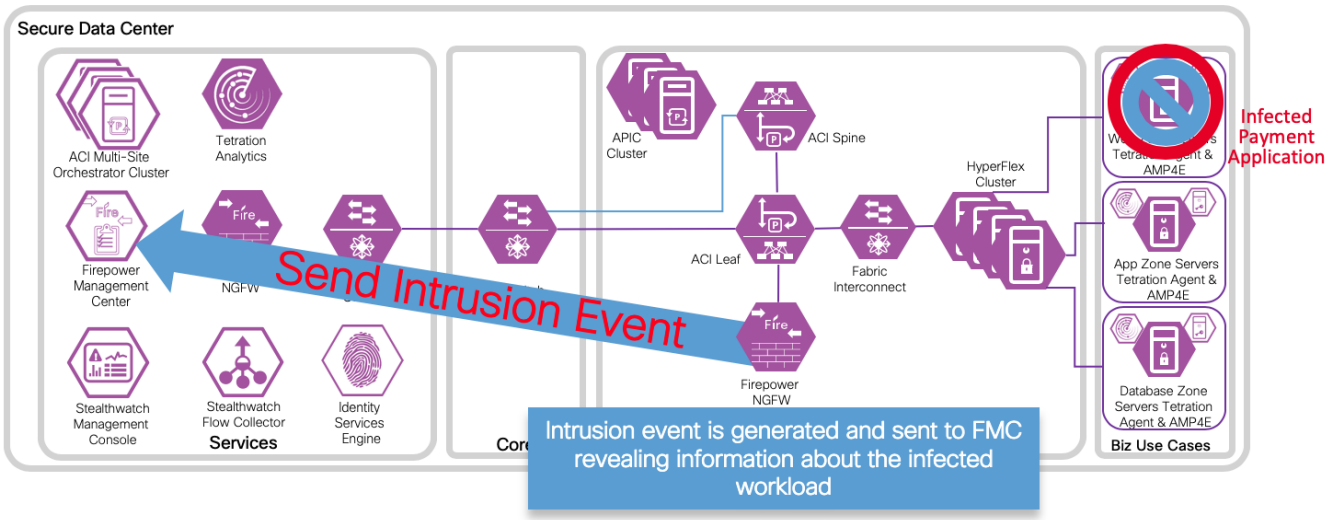


Return to Contents

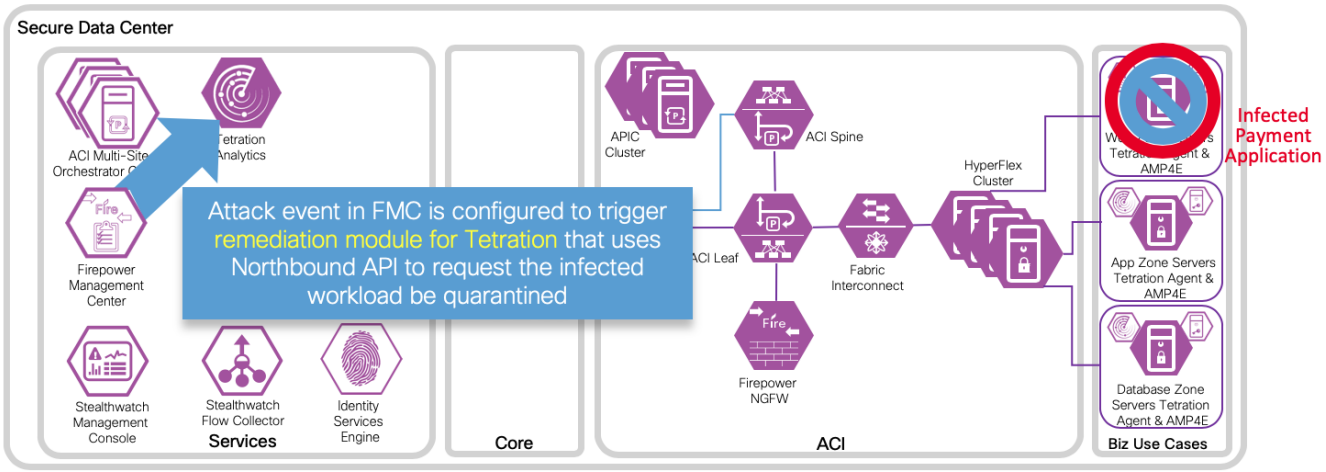
3. The attack is blocked inline by Cisco Firepower Threat Defense.



4. An attack event is generated and sent to the FMC. The attack event includes information about the infected endpoint.

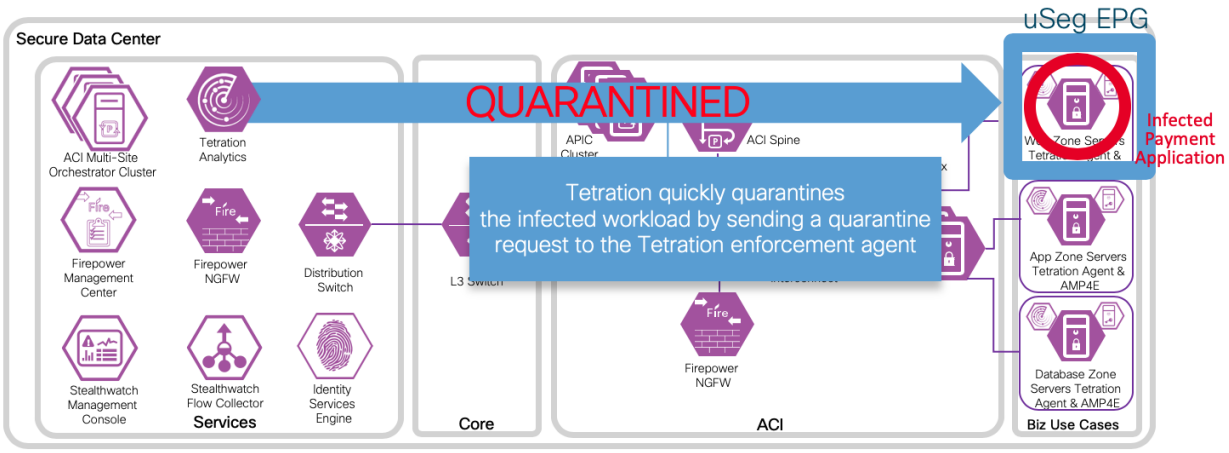


5. The attack event is configured to trigger the remediation module for Tetration, which uses the Tetration northbound API to contain the infected endpoint.



Return to Contents

6. Tetration Analytics Appliance quickly quarantines the infected application workload into an isolated microsegment.



Implementation Procedure

Within Tetration, create an API key and application rules. Install the Tetration Module in Firepower Management Center. Configure a new instance to use this key for authenticating communication between Cisco Firepower Management Center and Tetration. Develop policies to trigger a remediation event and verify with a test.

Additional information can be found at: https://www.Cisco.com/c/en/us/td/docs/security/firepower/tetration/quick-start/guide/fmc-rm-tetration-qsg-101/fmc-rm-tetration-qsg-101_chapter_01.html

Tetration API and Rules

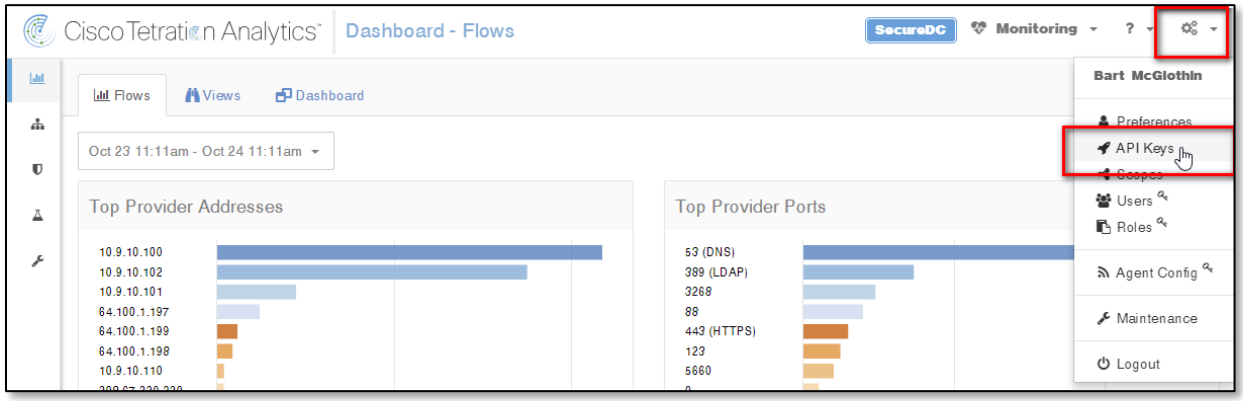
The API key and secret must first be created in TA by a site admin, customer support, or a root scope owner role. Copy that information for use in configuration steps to follow.

Step 1

a. Log in to Tetration

```
https://<your-Tetration-server-IP-address>/
```

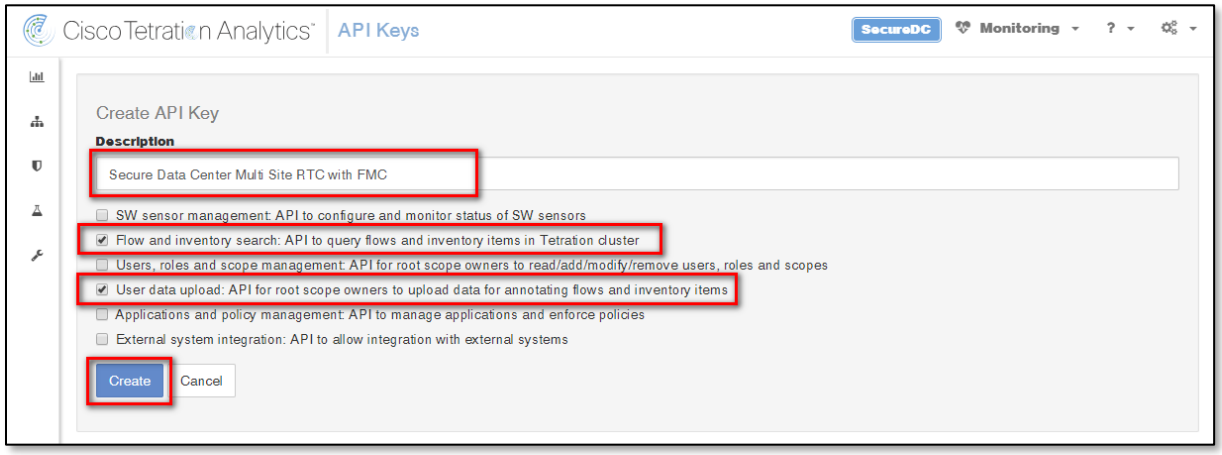
b. Navigate to API Keys in the top right settings menu



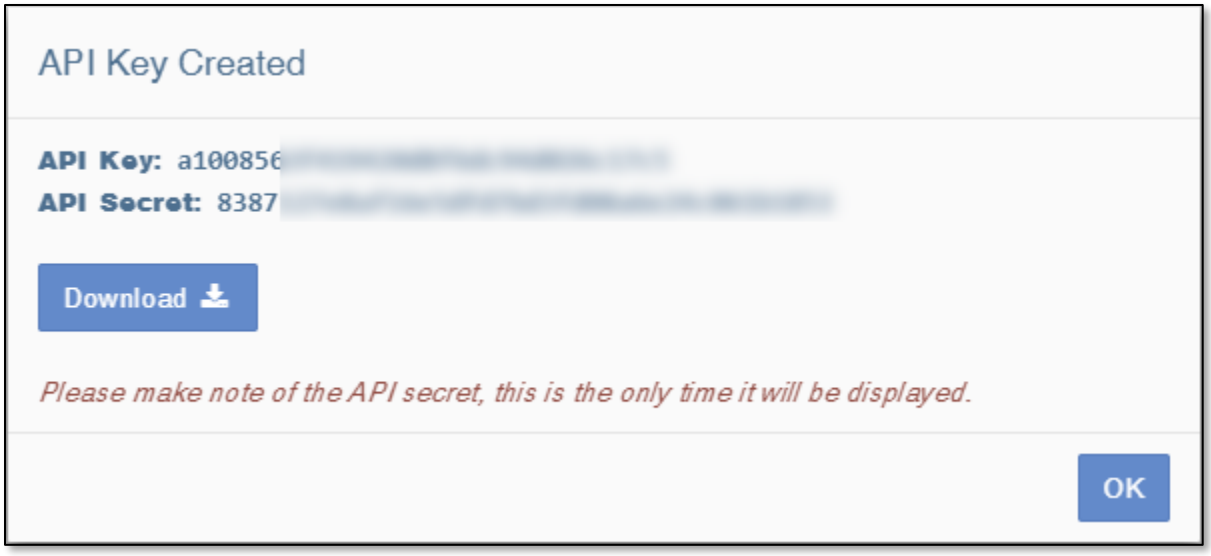
Step 2

a. Select the Create API Key option button in the top right.

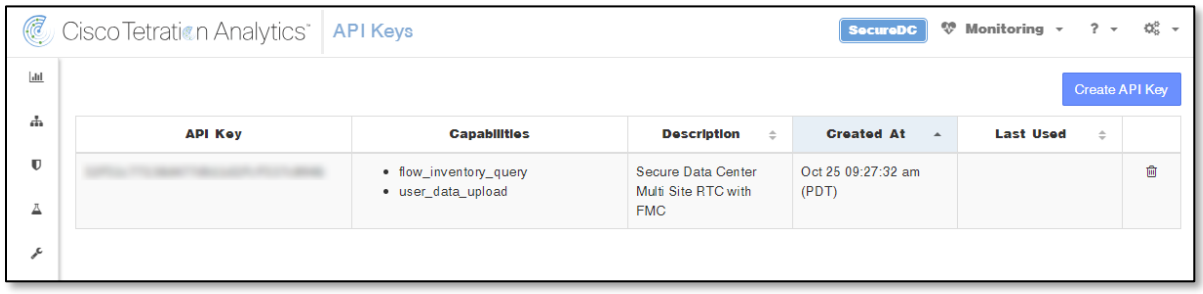
b. Enter an appropriate description and select the option: **User data upload** then click the **Create** button.



c. Save the credentials for use in the configuration steps to follow. Click **OK**



d. Continue on to Module installation, note the scope of Tetration configuration (e.g., SecureDC).



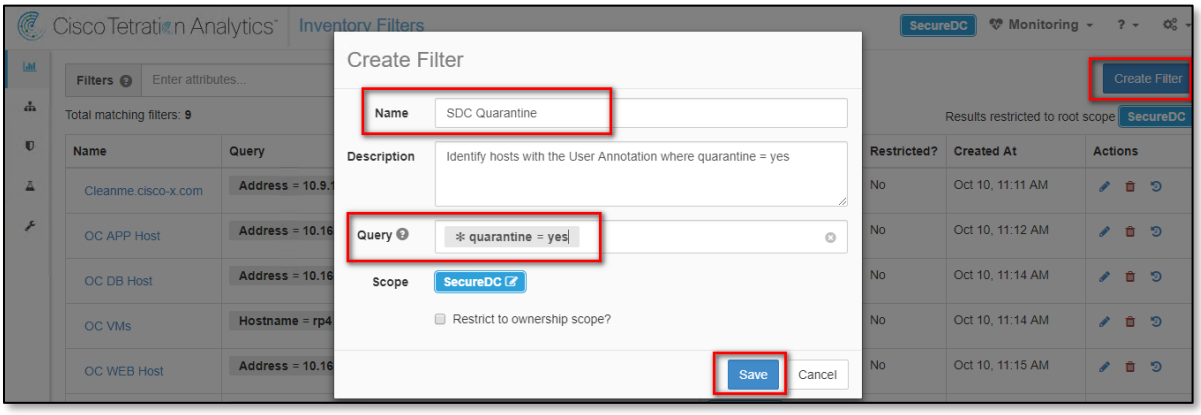
Step 3 Configure a quarantine policy and rule to segment the quarantined endpoints, but allow connectivity to a cleanup server:

a. Navigate to **Visibility > Inventory Filters**

b. Click **Create Filter** to create an inventory filter to identify quarantined hosts. Create additional filters and scopas needed to identify the cleanup server, DNS servers etc.

c. Enter a descriptive **name**, **description** and appropriate **query** (e.g. quarantine = yes).

d. Click **Save.**

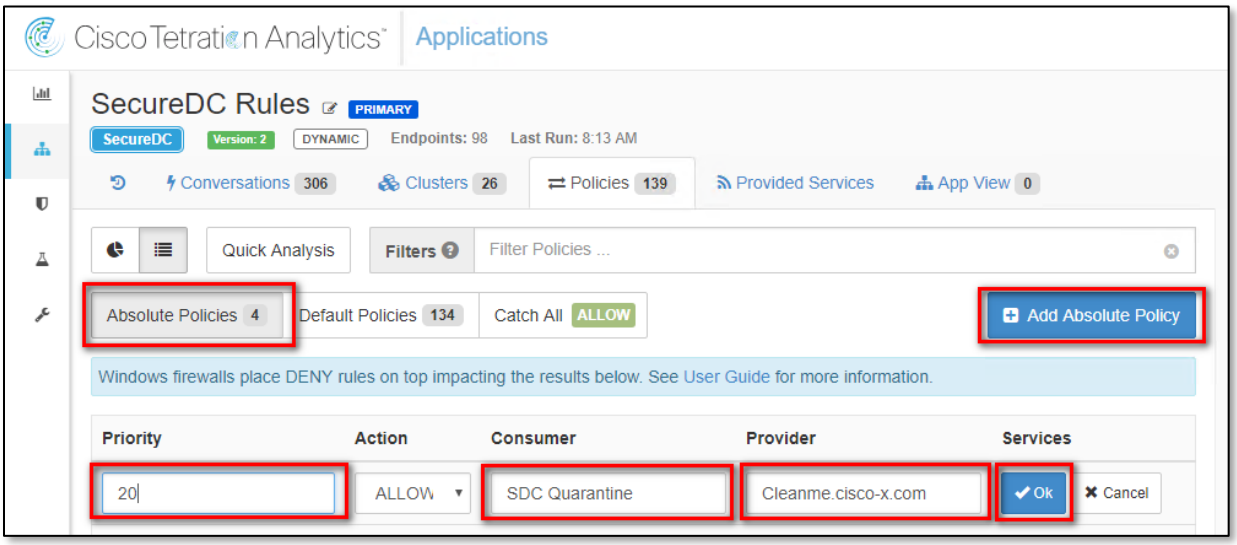


NOTE:

If you are not able to create the query as above, the quarantine User Annotation attribute may not exist yet. To create the User Annotation attribute, navigate to **Visibility > Inventory Upload** and upload a CSV file with the annotation defined as in Step 5 of the Verify section below.

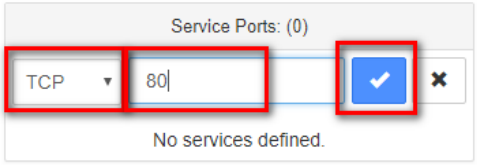
e. Navigate to **Applications > [Workspace] > Policies > Absolute Policies** and click the **Add Absolute Policy** button.

f. Set a priority, specify the consumer as the **SDC Quarantine filter** we created earlier, specify the provider as the **<your-remediation-server> filter**.



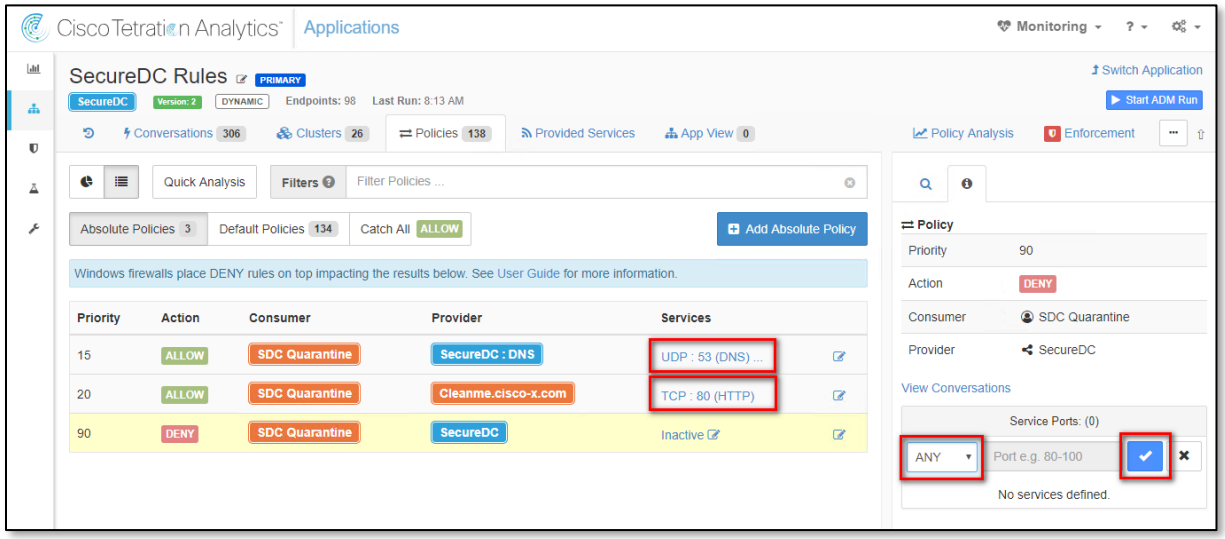
g. Click **OK**

h. Specify the services ports for the Provider by clicking the inactive icon and then the add button on the right under service ports. Select **TCP** from the selection box, enter **80** for the port, click the **checkmark**.



i. Add additional rules allowing for connectivity to the remediation server or other services as needed. Then add a **deny any** rule at the end.

j. Click the **checkmark** to complete the rule.



NOTE:

Elements are color coded; orange represent Filters, blue represent Scopes.

Installation

To download and install the Cisco Firepower Management Center Remediation Module for Tetration, complete the following procedure:

Step 1 Use a web browser to download the remediation module:

https://software.Cisco.com/download/home/286259687/type

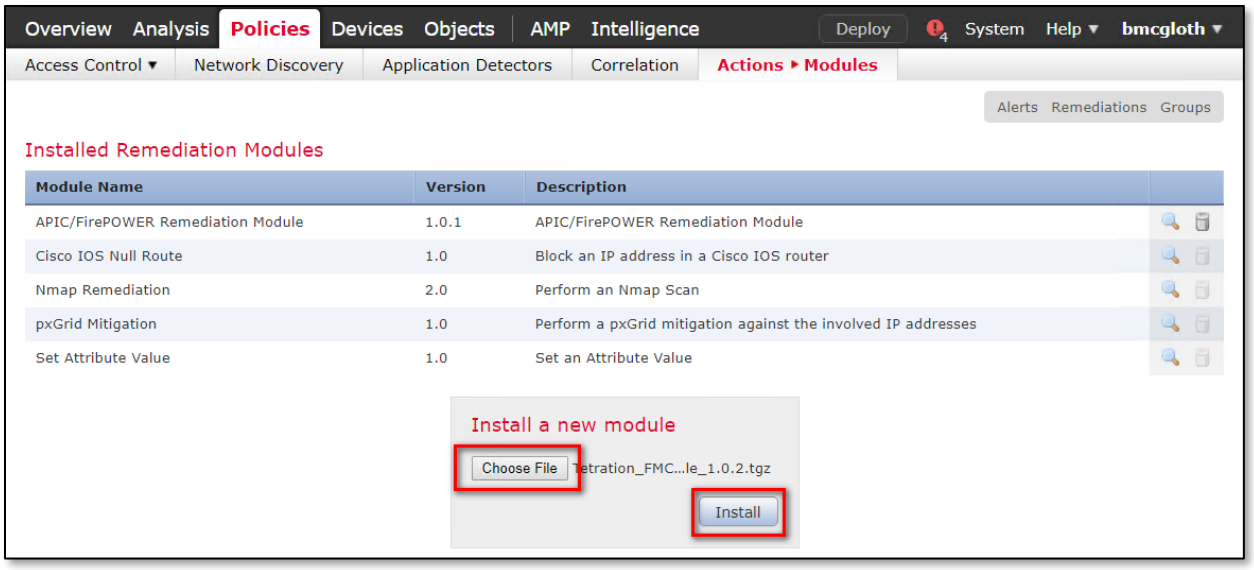
Step 2 Install the remediation module onto the FMC:

a. In the FMC GUI, navigate to **Policies > Actions > Modules.**

b. In the **Install a new module** dialog box, click **Choose File** as shown below.

c. Select the file for the remediation module that was downloaded in Step 1.

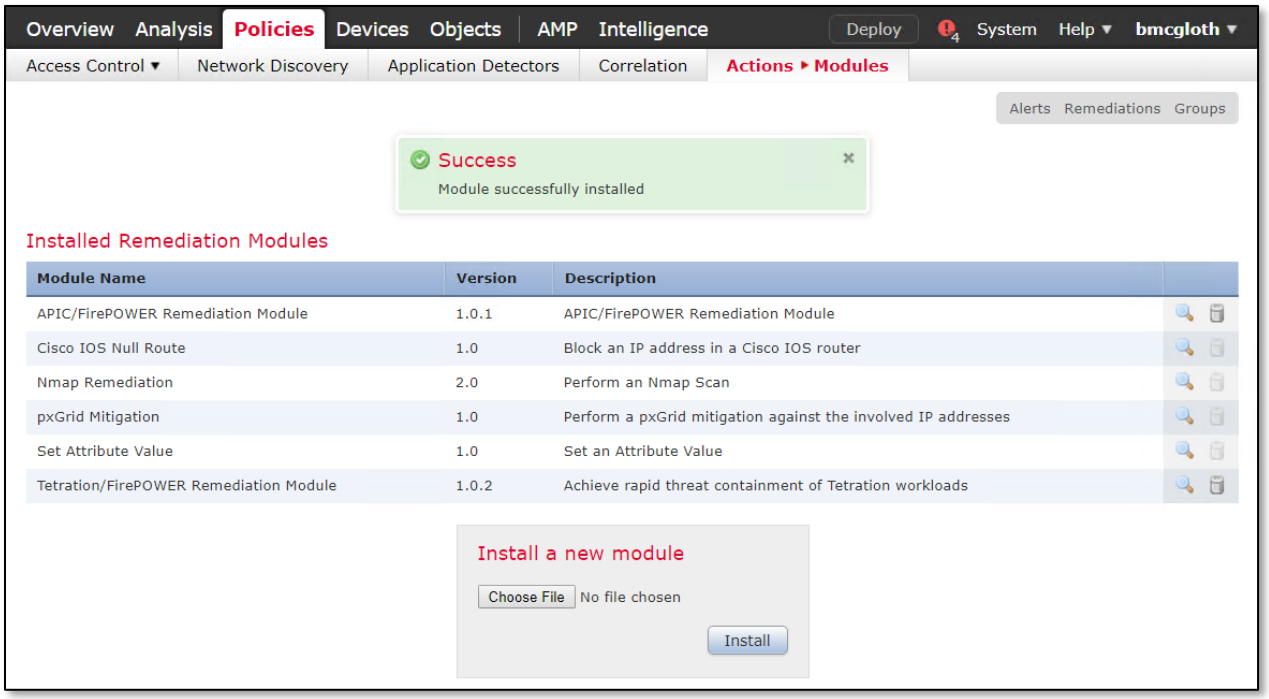
d. Click **Install**.



NOTE:

If you receive an access error message, clear the error message and repeat Step 2.

When successfully installed, the Cisco Firepower Management Center Remediation Module for Tetration is displayed in the list of installed remediation modules.



Configuration

To configure the remediation module installed on the FMC, complete the following procedure in the FMC GUI:

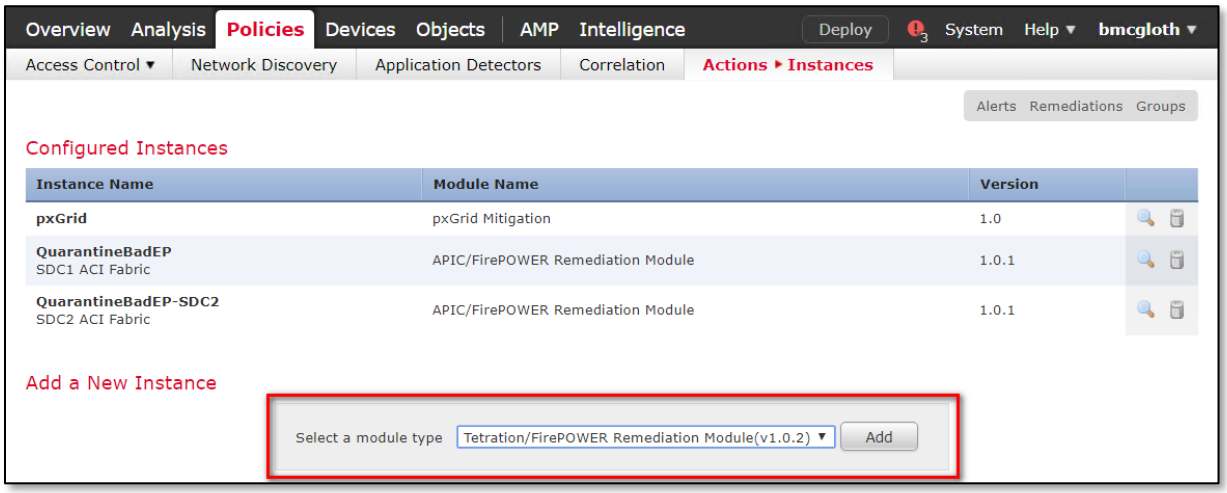
Step 1

Cr

eate an instance of the remediation module for each Tetration Analytics (TA) server in your network:

a. Navigate to **Policies > Actions > Instances**.

b. Select the remediation module in the drop-down list, and click **Add**.



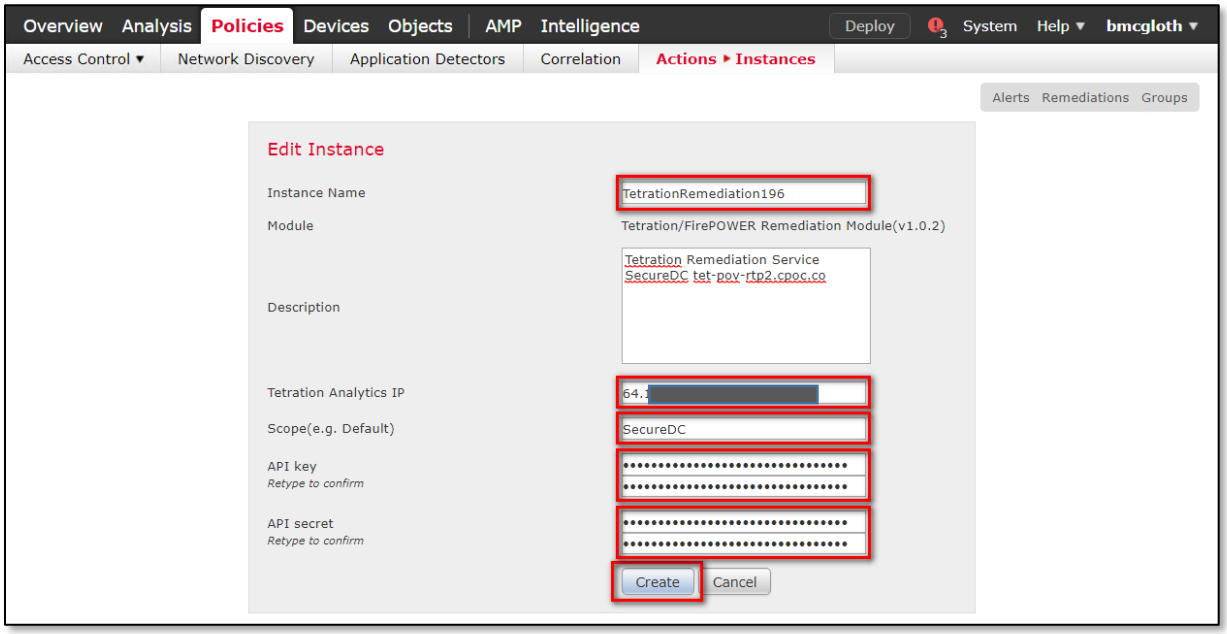
c. Enter an **Instance Name** (in this example, `TetrationRemediation196`) and **description**.

Return to Contents

d. Enter the TA server's **IP address**, **API key**, **API secret**, and **scope** containing the potentially offending host. Click **Create**.

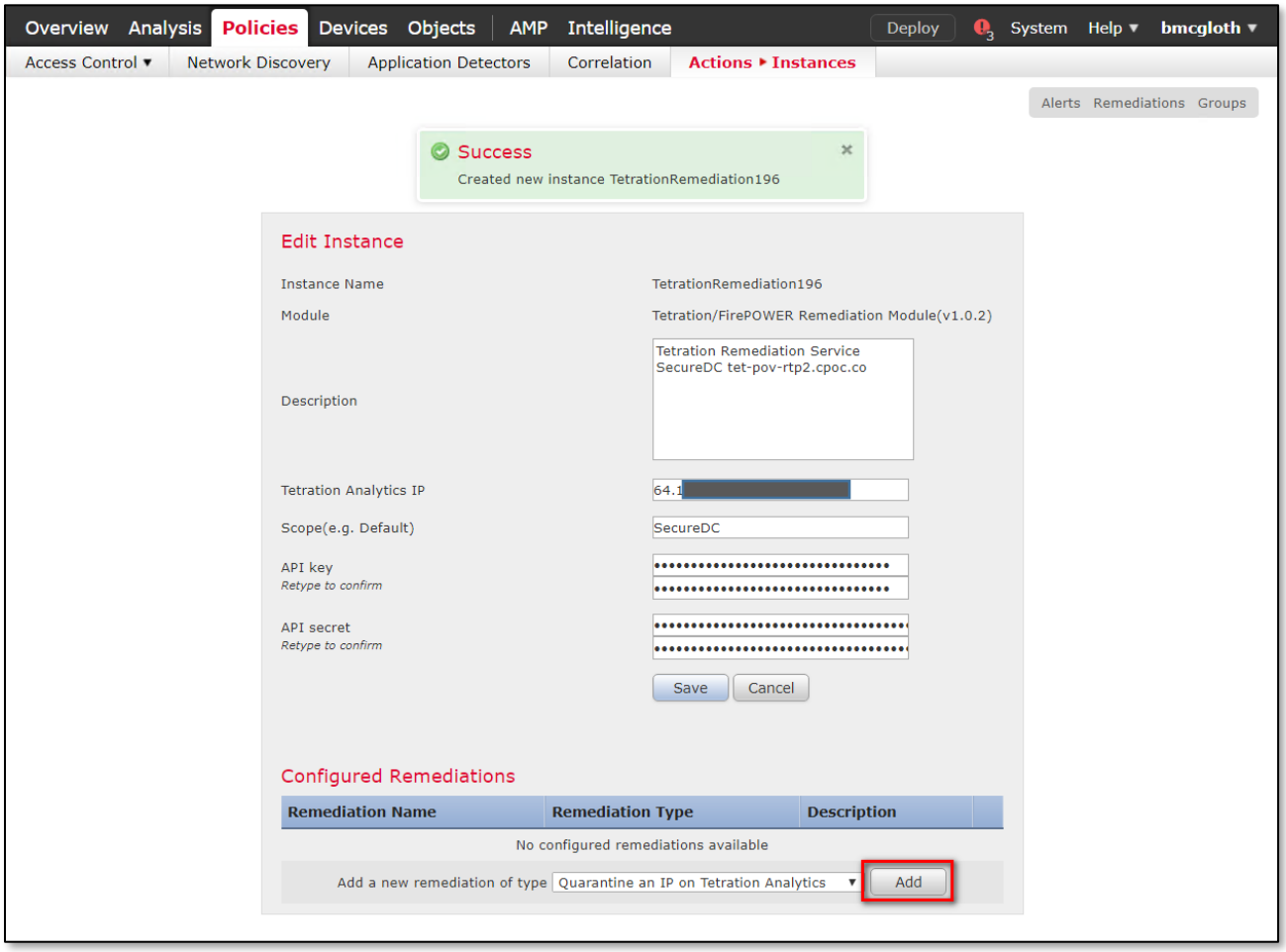
NOTE:

The API key and secret are not validated against the TA server at this point. The API key and secret must first have been created in TA by a site admin, customer support, or a root scope owner role.

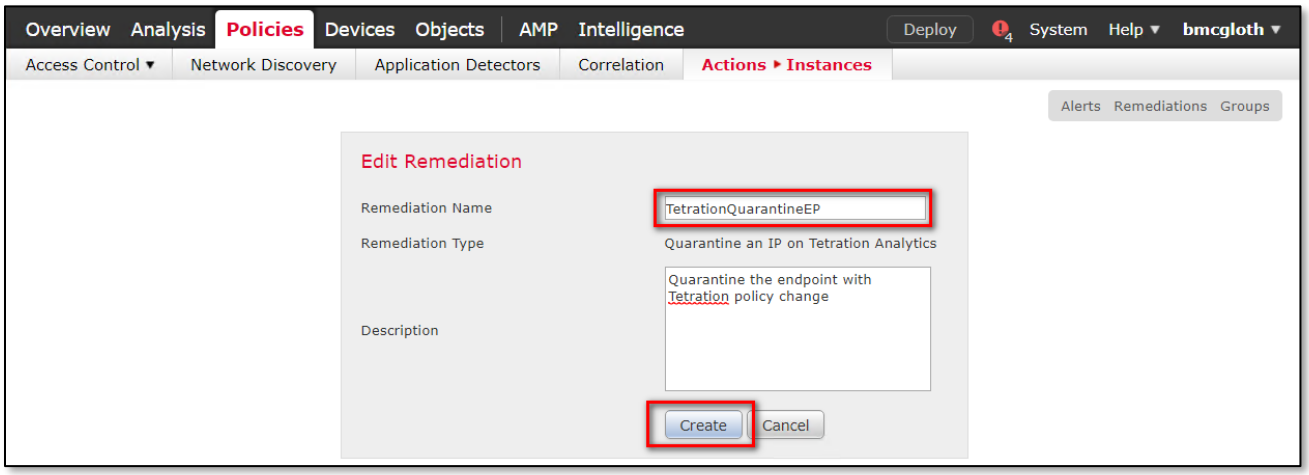


Return to Contents

e. Under **Configured Remediations**, select a type of remediation (in this example, quarantine an IP on Tetration Analytics), and click **Add** to add a new remediation.

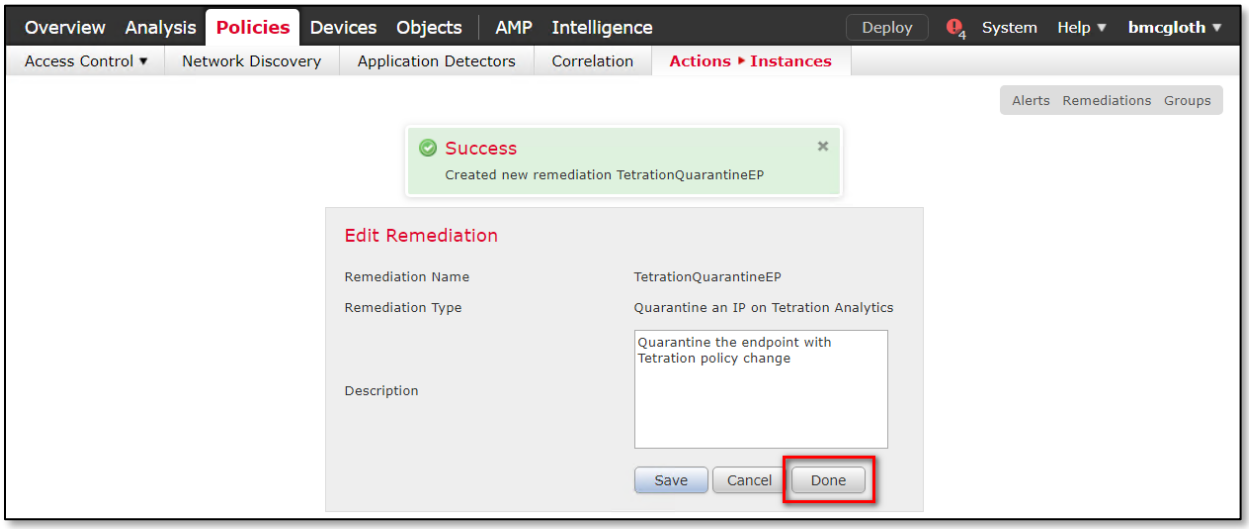


f. Enter a **Remediation Name** (in this example, `TetrationQuarantineEP`), and click **Create**.



Return to Contents

g. Return to the Instance configuration by clicking **Done**.



h. The remediation you just configured then shows up in the table. Click **Save**.

NOTE:

You can also create an un-quarantine remediation action, but it's not recommended for production environments.

Step 2 Configure the policy to log connections to be tested for CnC traffic.

Configure an access control policy (in this example, `SDC-Multisite-FTD-C1`):

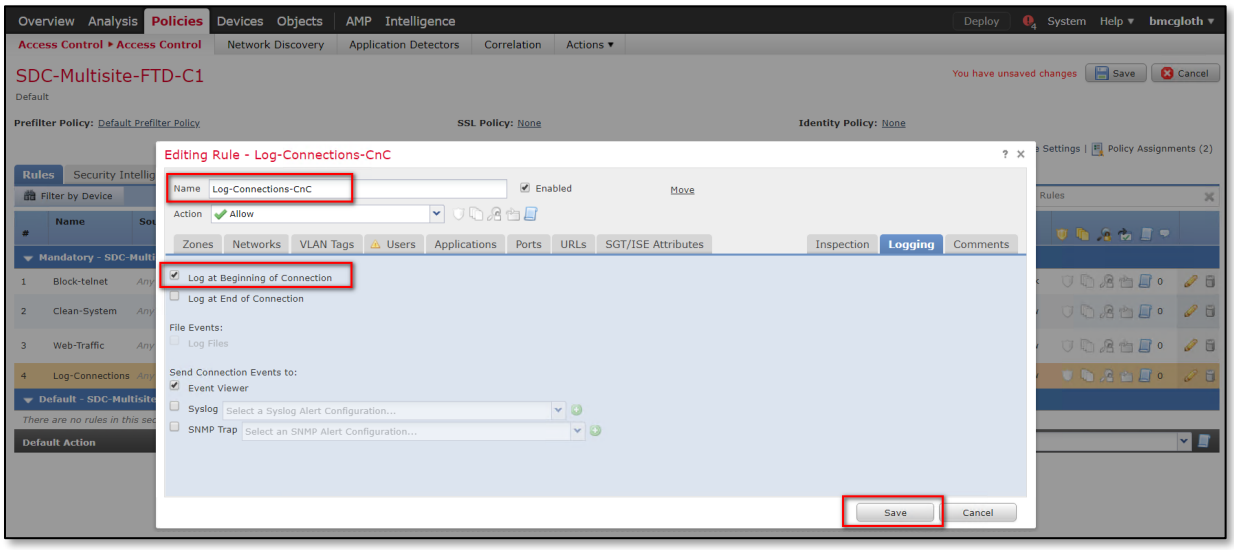
a. Navigate to **Policies > Access Control** then **Edit** the policy.

b. Click Edit Rule (for example, `Log-Connections-CnC or Web Traffic`).

c. On the Logging tab, select **Log at Beginning of Connection**.

Important

Ensure that logging is enabled each of the access rules, so that the FMC receives event notifications.



Return to Contents

d. Click **Save**.

e. Then **Save** and **Deploy** the policy.

Step 3 Configure a correlation rule:

a. Navigate to **Policies > Correlation > Rule Management**.

b. Click the **Create Rule** button.

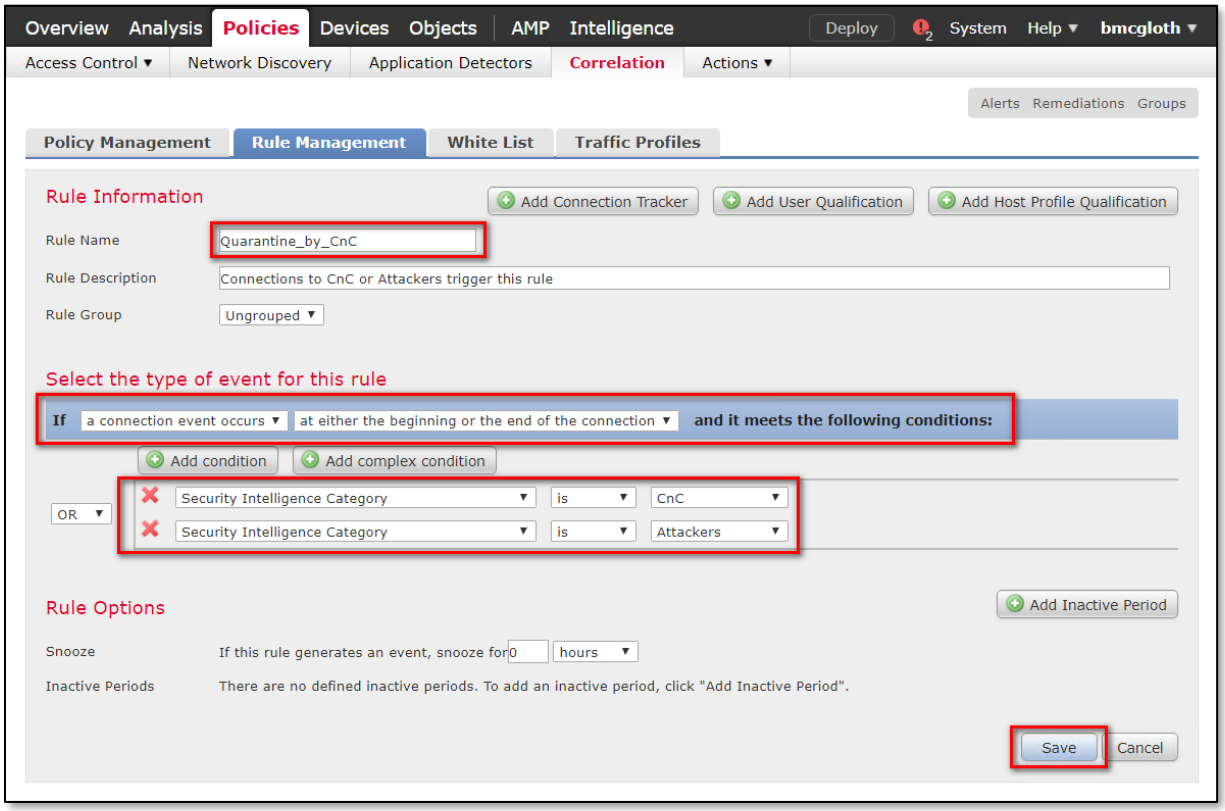
c. Enter a **Rule Name** (in this example, `Quarantine_by_CnC`) and **description** (optional).

d. In the **Select the type of event for this rule** section, select **a connection event occurs** and **at either the beginning or the end of the connection**.

e. In the drop-down list, select **Security Intelligence Category**, operator set to **is**, and category set to **CnC**.

f. Click **Add condition**, and check the operator is set to **OR** instead of **AND**.

g. In the drop-down list, select **Security Intelligence Category**, operator set to **is**, and category set to **Attackers**.



h. Click **Save**.

NOTE:

There are several other categories that may also be desirable to add; Bogon, Bots, Dga, Exploitkit, Malware, OpenProxy, OpenRelay, Phishing, Response, Spam, Suspicious, and TorExitNode.

For more information, please visit:
https://www.Cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/security_intelligence_blacklisting.html

Step 4 Associate the instance of the remediation module as a response with a correlation rule:

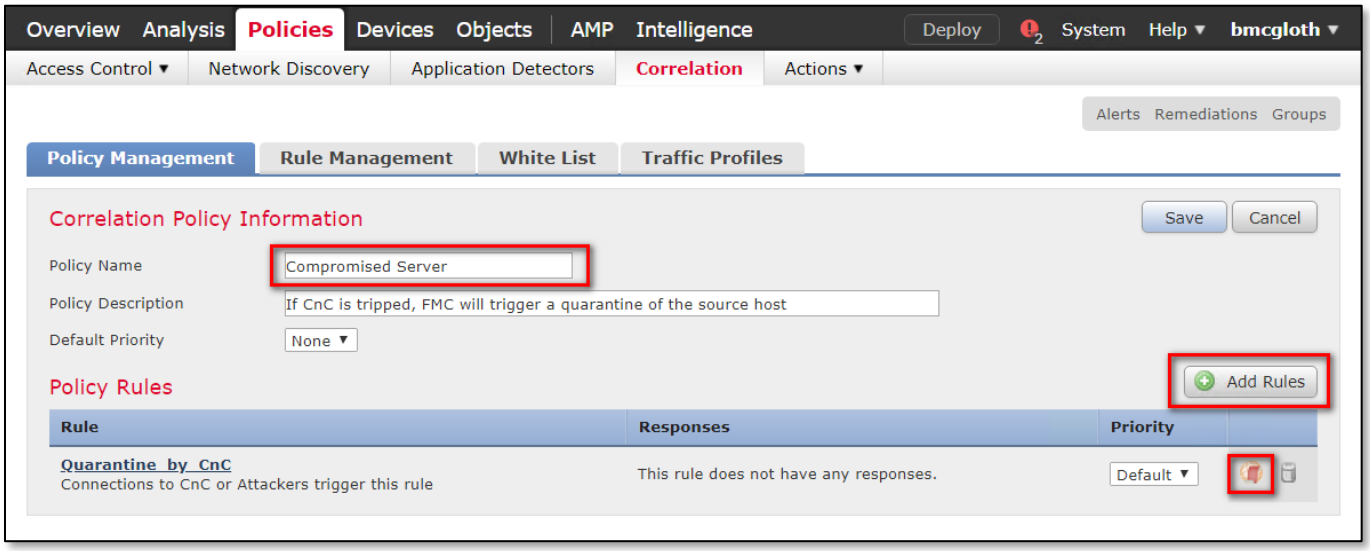
a. Navigate to **Policies > Correlation > Policy Management**.

b. Click Create Policy.

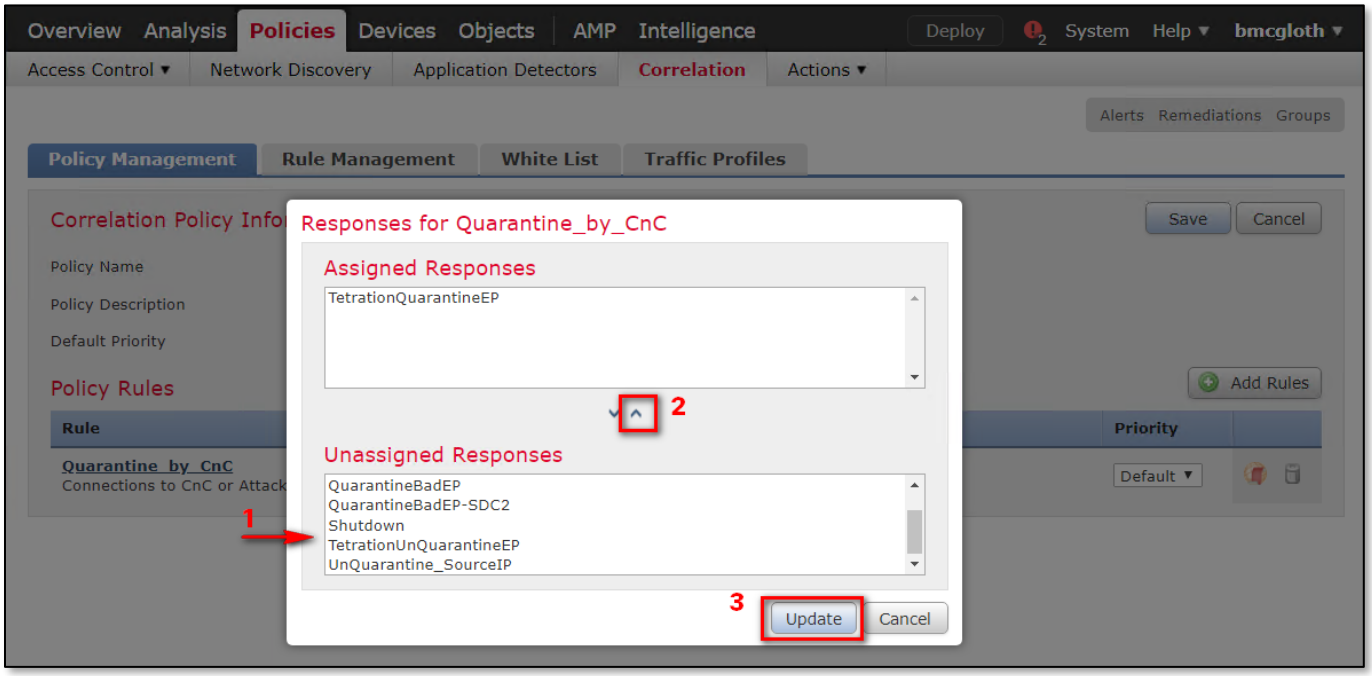
c. Enter a **Policy Name** (in this example, `Compromised Server`) and **description** (optional).

d. From the **Default Priority** drop-down list, select a priority for the policy. Select **None** to use rule priorities only.

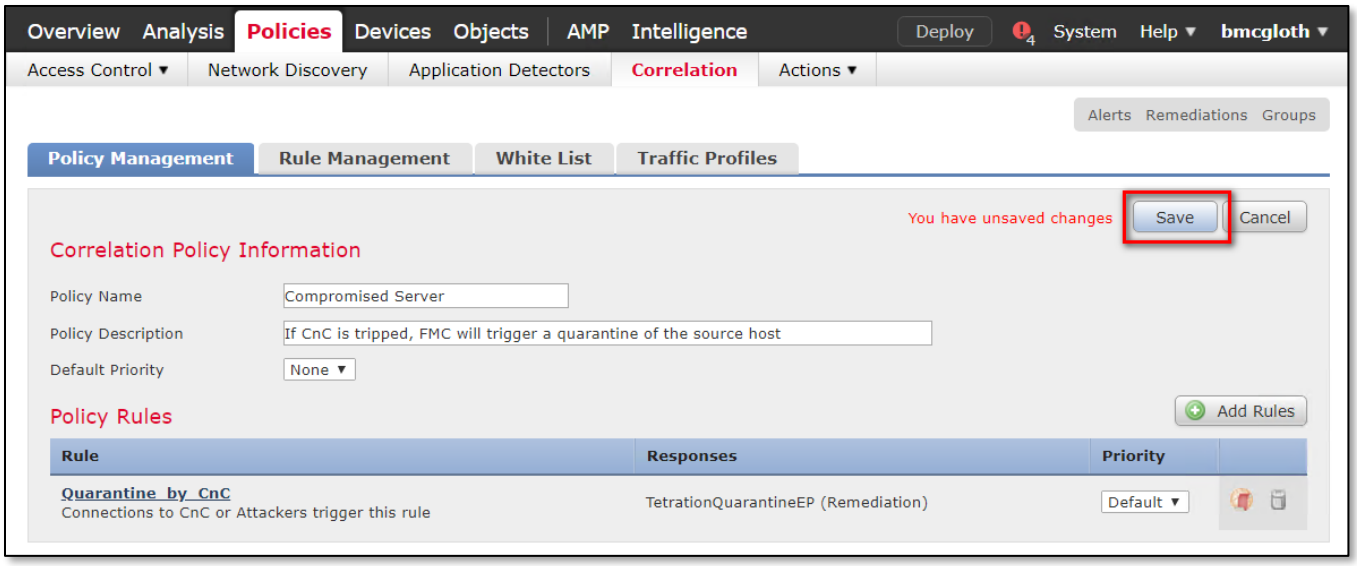
e. Click **Add Rules**, select the correlation rule you previously configured in Step 3 (in this example, `Quarantine_by_CnC`), and click **Add**.



f. Click the **Responses** icon next to the rule and assign a response (in this example, `TetrationQuarantineEP`) to the rule.



g. Click **Update**.



h. Click **Save**.

Verify

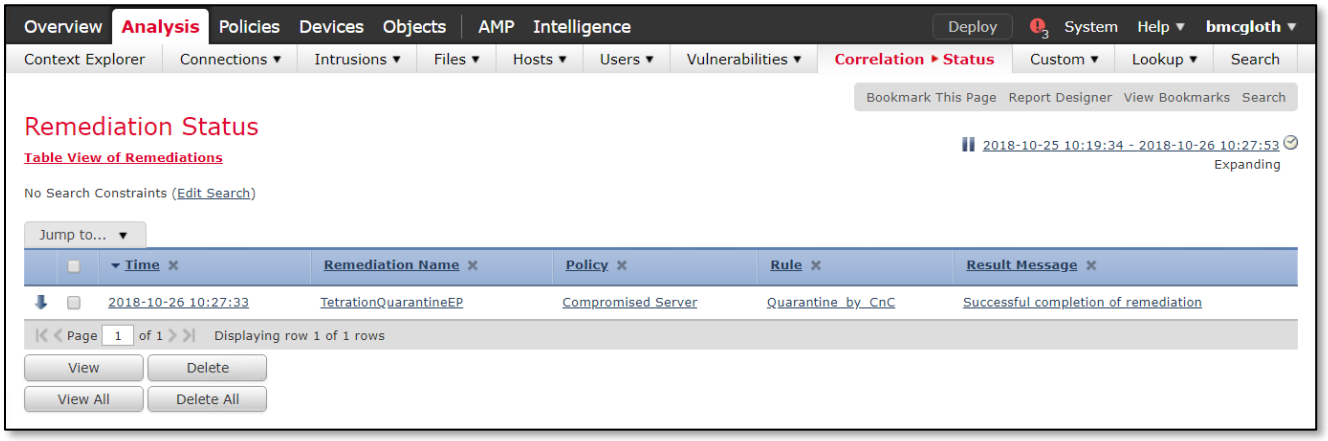
Because remediations can fail for various reasons, perform the following steps to verify that a remediation is successful:

Step 1 Once the remediation module is triggered by an associated correlation rule, check the status of the remediation execution in the FMC GUI (ping a known CnC server on the internet).

Within about 20 seconds the policy should take effect, within 2 minutes the annotation shows up in the Tetration database after a screen refresh.

Step 2 Navigate to **Analysis > Correlation > Status**.

Step 3 In the Remediation Status table, find the row for your policy and view the result message. Result may show “Remediation pending” as the module continues to check the status of the Tetration data base.

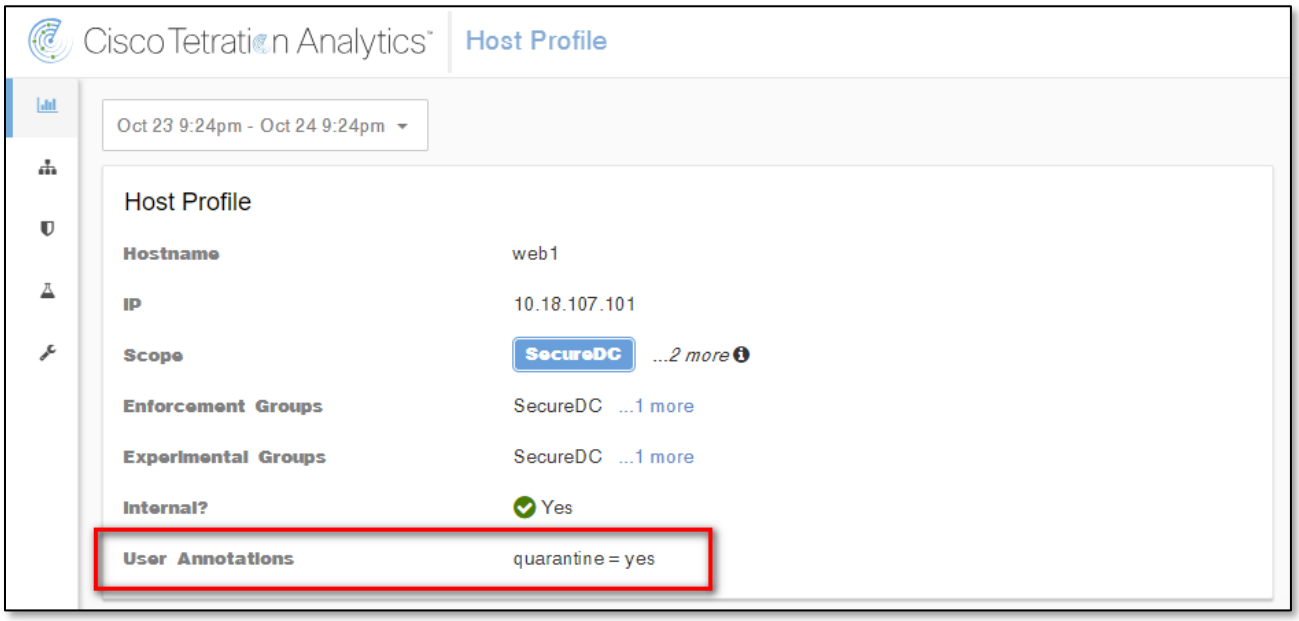


Step 4 Once the remediation is complete, go to the TA GUI:

a. Navigate to **Visibility > Inventory Search**.

b. Enter the IP address of the infected host, and click **Search**.

c. In User Annotations, you should see **quarantine = yes** annotated to the IP address of the infected host.



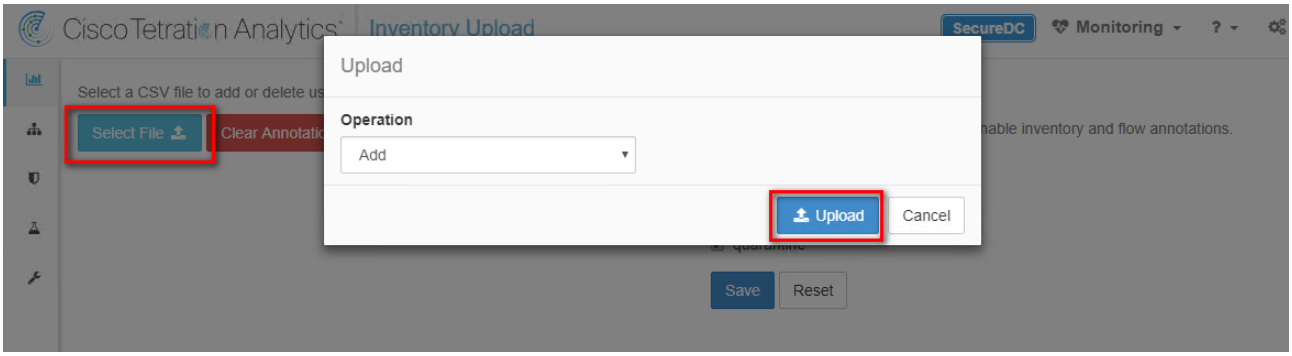
Step 5 What to do next

Once you clean the quarantined host and it is no longer infected, you can use Tetration (recommended) to change the quarantine = yes annotation back to quarantine = no as follows:

For example, if the quarantined host that is no longer infected is 10.18.107.101, create a CSV file such as:

```
IP,quarantine
10.18.107.101,no
```

Navigate to **Applications > Inventory Upload**. and upload your CSV file to Tetration using the **Add** operation.



For more info, see the online help user guide on your Tetration server:

https://<your-Tetration-server-IP-address>/documentation/ui/inventory/user_annotations.html

An alternative method is to use the FMC remediation module to remove the quarantine with an un-quarantine rule and associated policy but this is not recommended in production networks due to security concerns.

Return to Contents

Test Case 8 – Tetration and Identity Services Engine

Tetration as a Service and Identity Service Engine (ISE) integration provides Tetration with endpoint and user metadata, such as Mobile Device Manager (MDM) details (i.e. authentication, Security Group Tags (SGTs), etc). The metadata is used in Tetration inventory filters, policies, etc. The integration requires the deployment of a Tetration Virtual Edge Appliance and the Cisco Platform Exchange Grid (pxGrid) service.

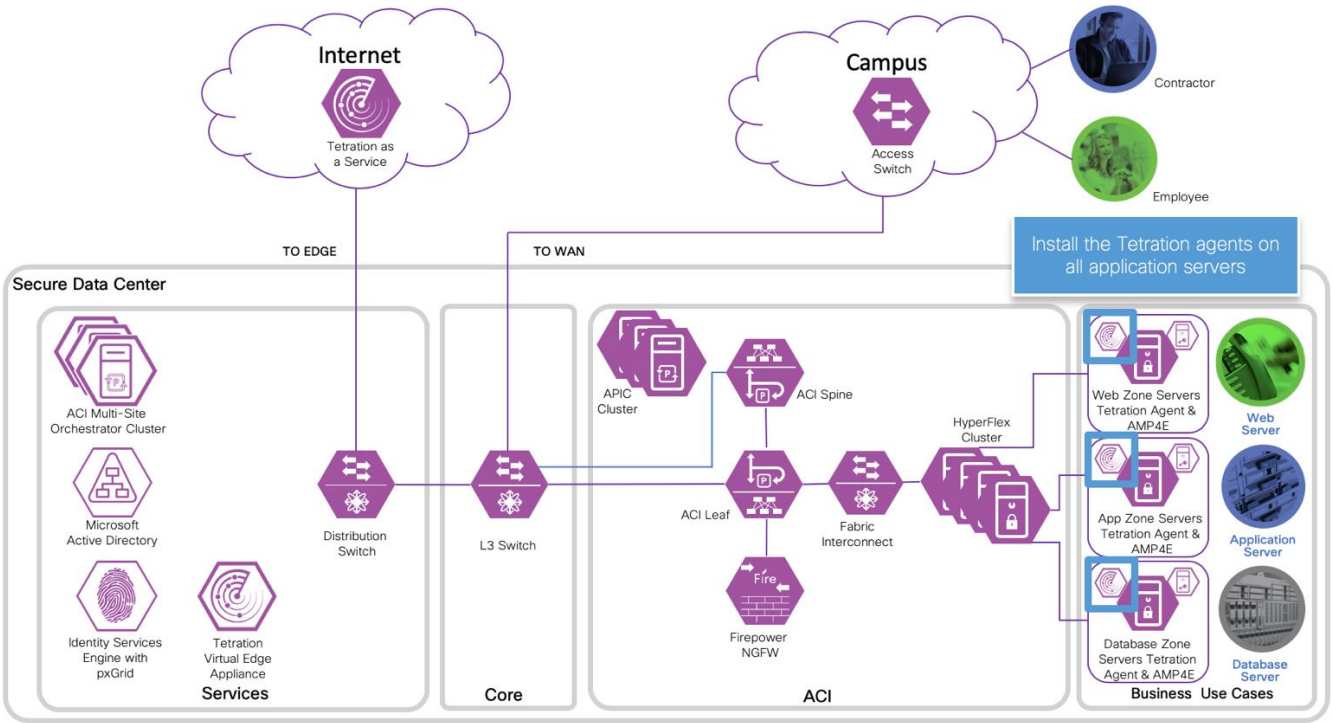
Test Description:

In this test case, Tetration is used to protect the application servers in the data center. The objective is to allow users in the AD group Employees to access the application servers while denying all others.

To accomplish this, the Tetration Enforcement Agent is installed on all servers. A Tetration policy is created to allow the group Employees to access the application servers. The policy is pushed to all the Tetration Enforcement Agents. The agents then update the server firewall rules, granting access to the group Employees.

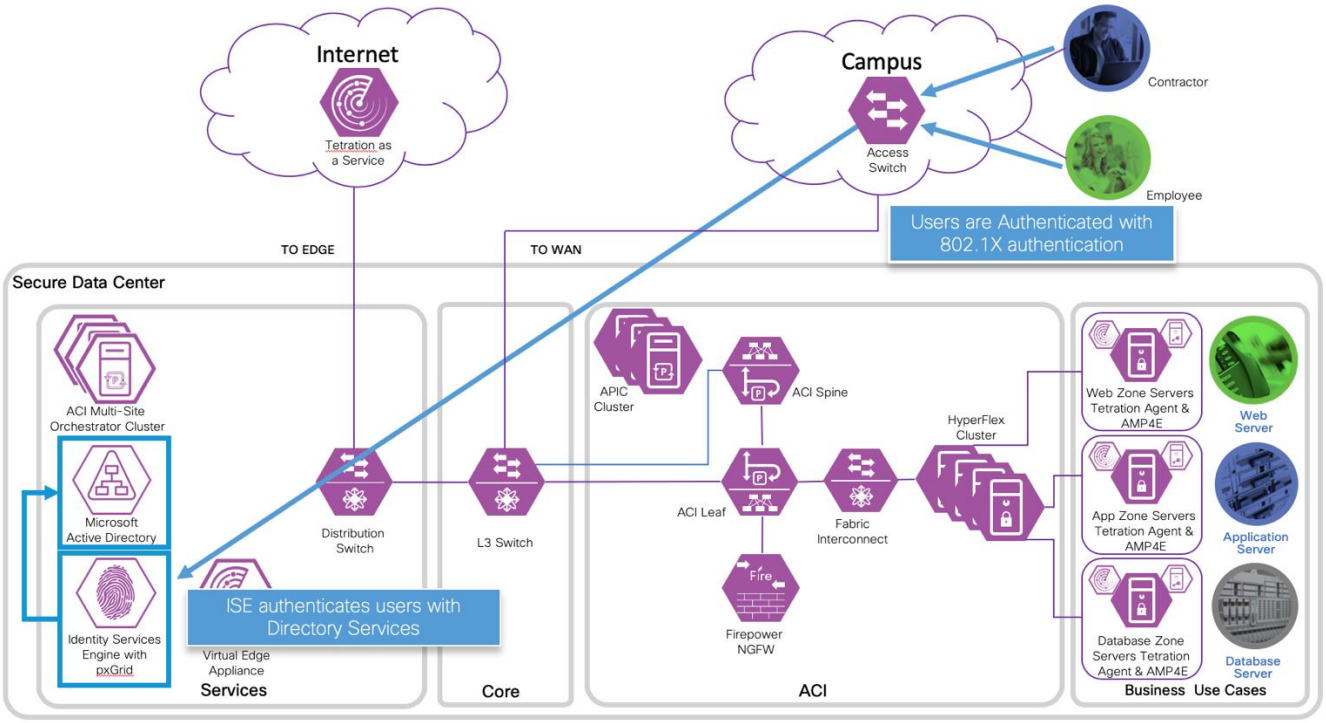
The important thing to note is the group Employees used in the policy is a Tetration filter. The filter is updated in near real time with changes in endpoint states, as users log on and off the network. These updates are provided by ISE through pxGrid and the Tetration Virtual Edge Appliance. This enables Tetration to update the server firewall rules to reflect the endpoints current state.

1. The Tetration Enforcement Agent is installed on all application servers. The agent provides Tetration with host information and traffic flows.

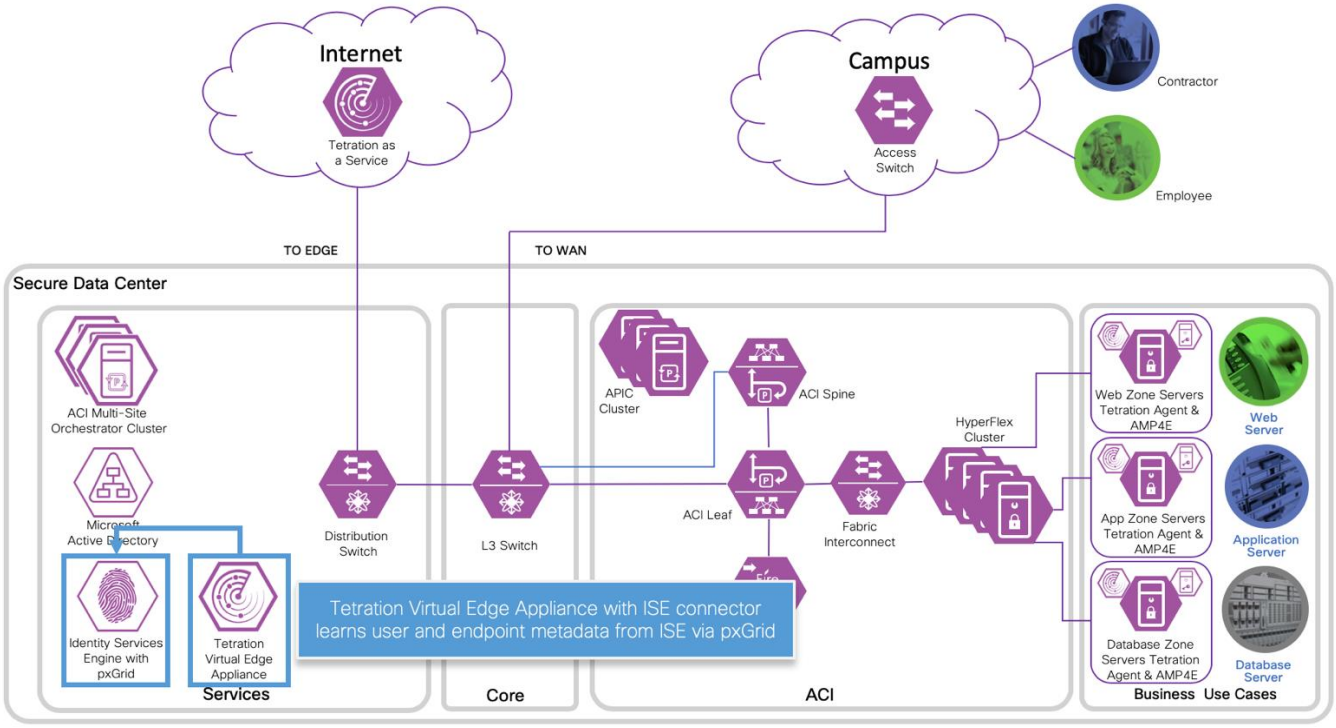


Return to Contents

2. Endpoints are authenticated using the 802.1X protocol at the access switch or access point. ISE provides the RADIUS service for the authentication. ISE uses Directory Services to authenticate and learn endpoint and user metadata.

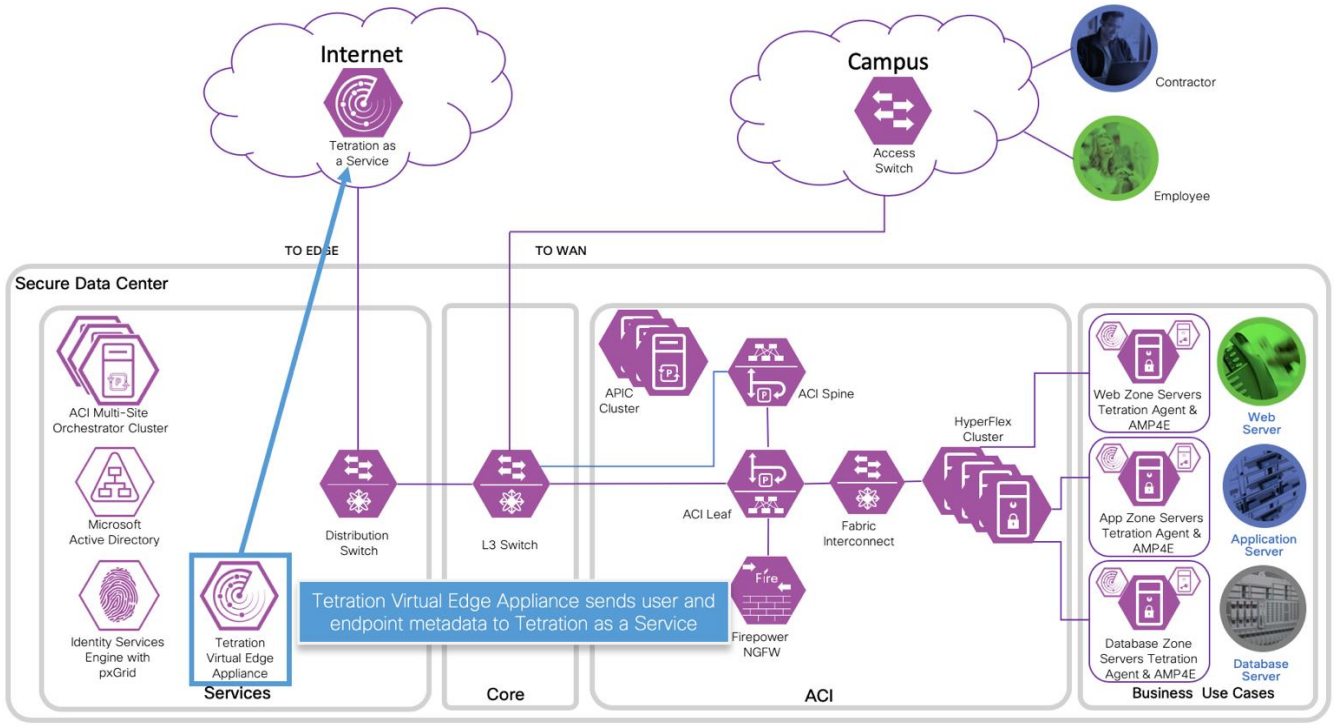


3. The Tetration Virtual Edge Appliance learns endpoint and user metadata from ISE over pxGrid.

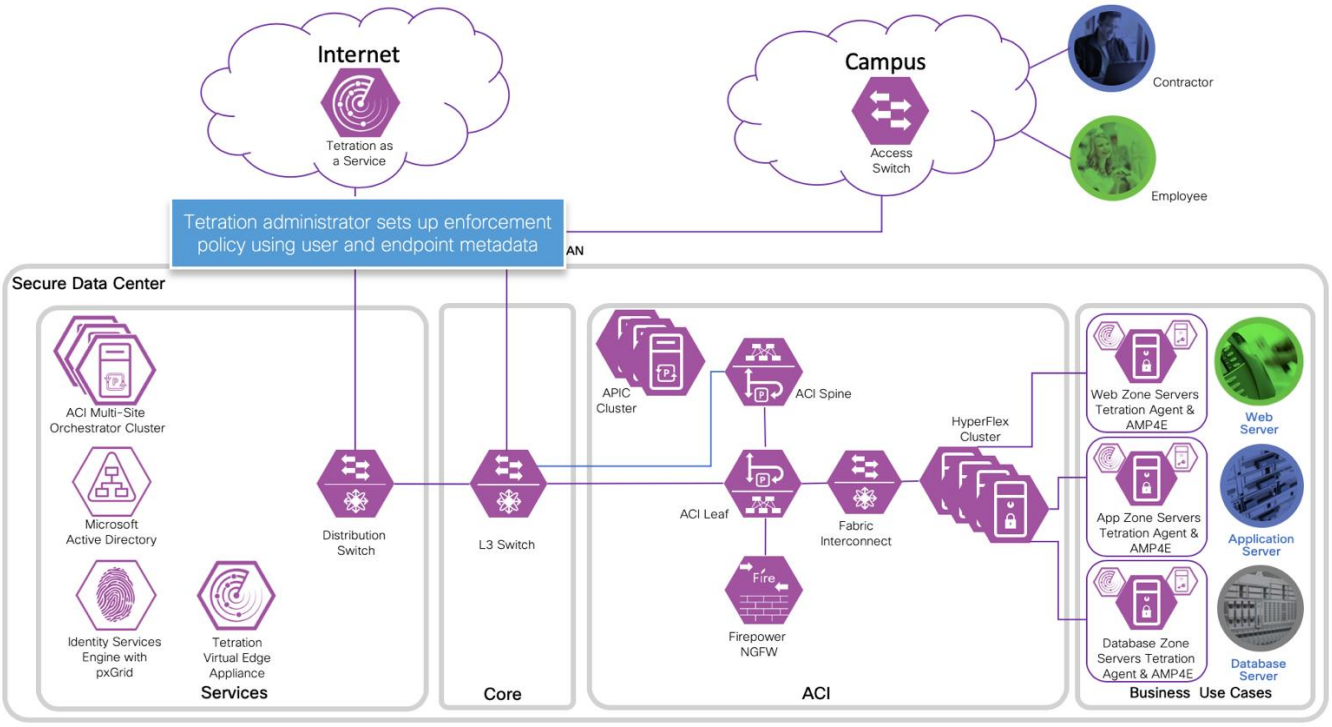


Return to Contents

4. Tetration Virtual Edge Appliance streams the endpoint and user metadata to Tetration. The data is updated in near real time to reflect the endpoints current state.

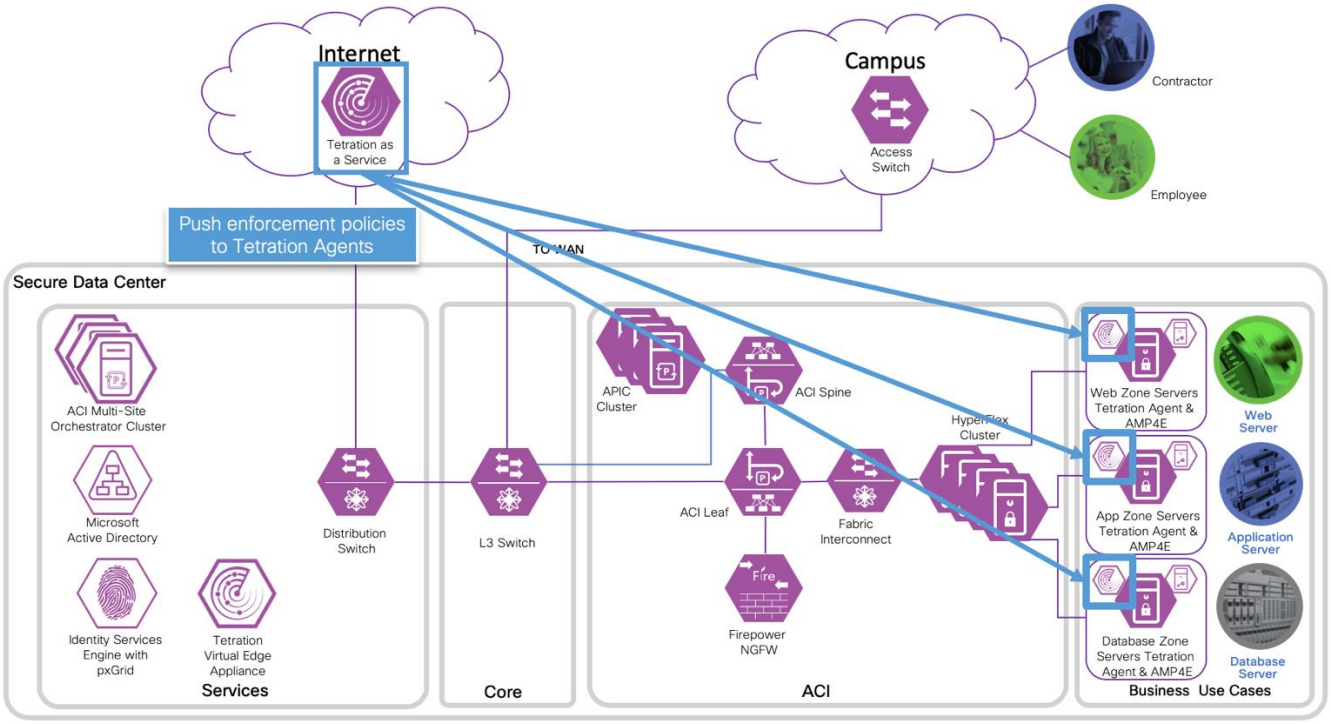


5. The Tetration administrator creates policies using Application Dependency Mapping (ADM) tool or manually. The metadata from ISE can be used as filters in Tetration policies.

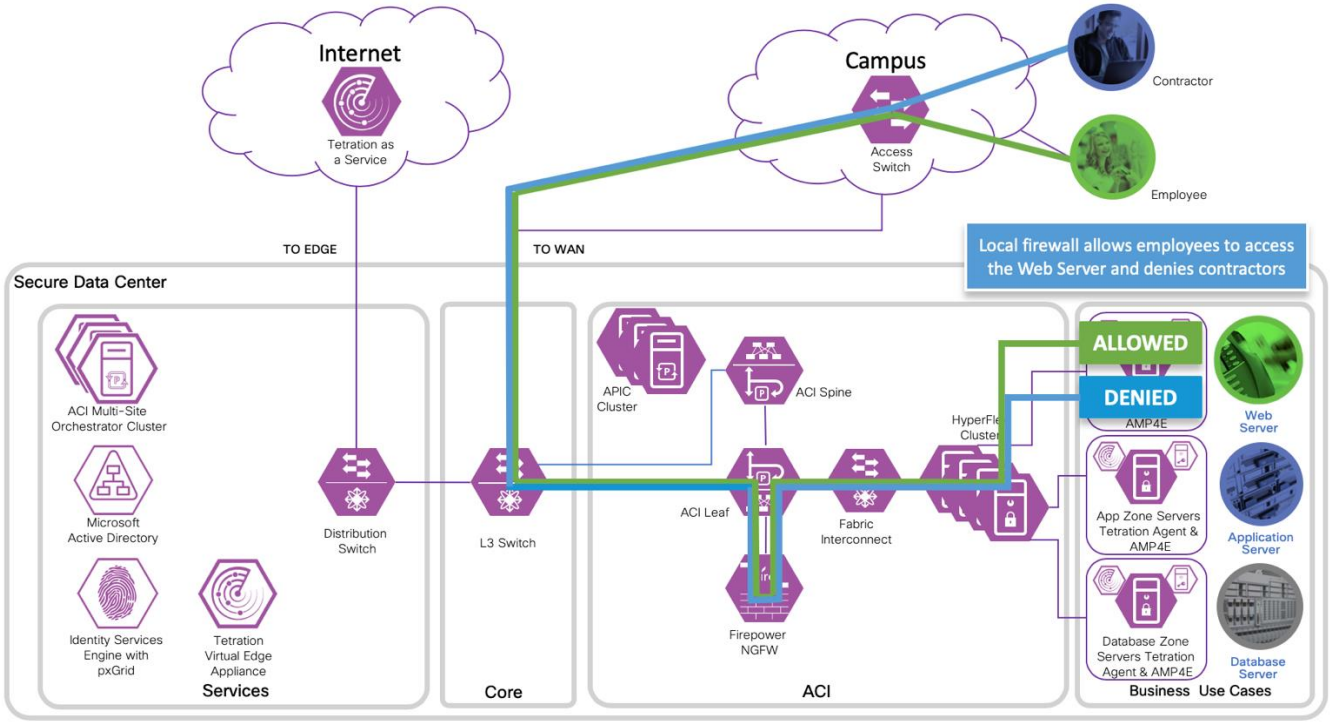


Return to Contents

6. Tetration pushes policies to the agents, then the agents update the local firewall rules.



7. With the updated firewall rules, employees are allow to access the web server and contractors are deny.



Return to Contents

Procedure

Step 1 Enable ISE pxGrid

Step 2 Generate a pxGrid Certificate

Step 3 Create the Tetration Virtual Edge Appliance Configuration Bundle

Step 4 Deploy the Tetration Virtual Edge Appliance

Step 5 Configure the ISE Connector

Step 6 LDAP Configuration

Step 7 Annotation Inventory Upload

Step 8 Create Scope

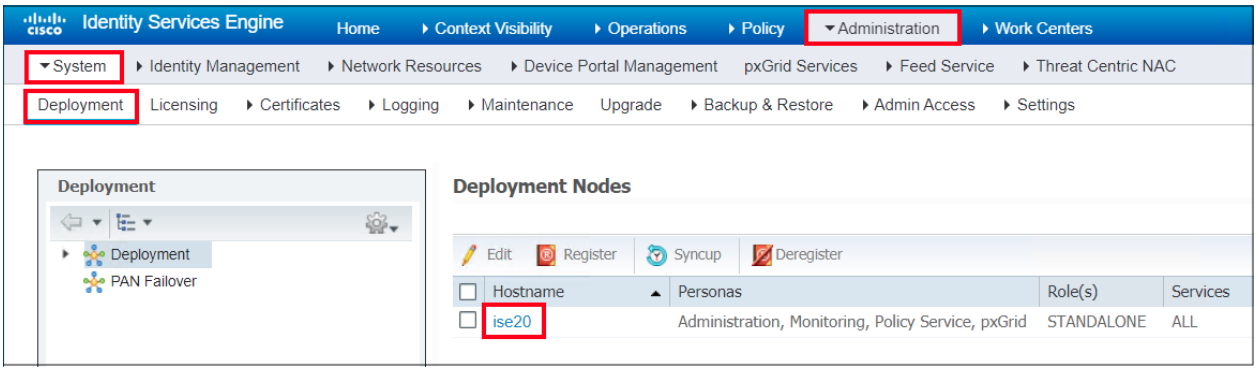
Step 9 Create Inventory Filters

Step 10 Create Workspace

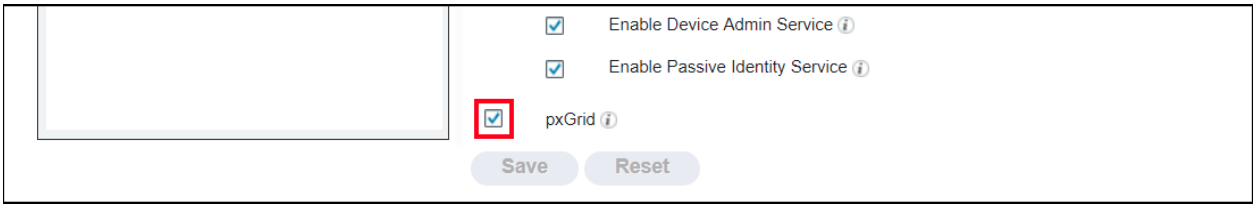
Step 11 Testing

Step 1 Enable the ISE pxGrid.

a. To edit the ISE node configuration, log into the ISE management portal. Navigate to **Administration > System > Deployment** and click on the deployed node *<Hostname>*.

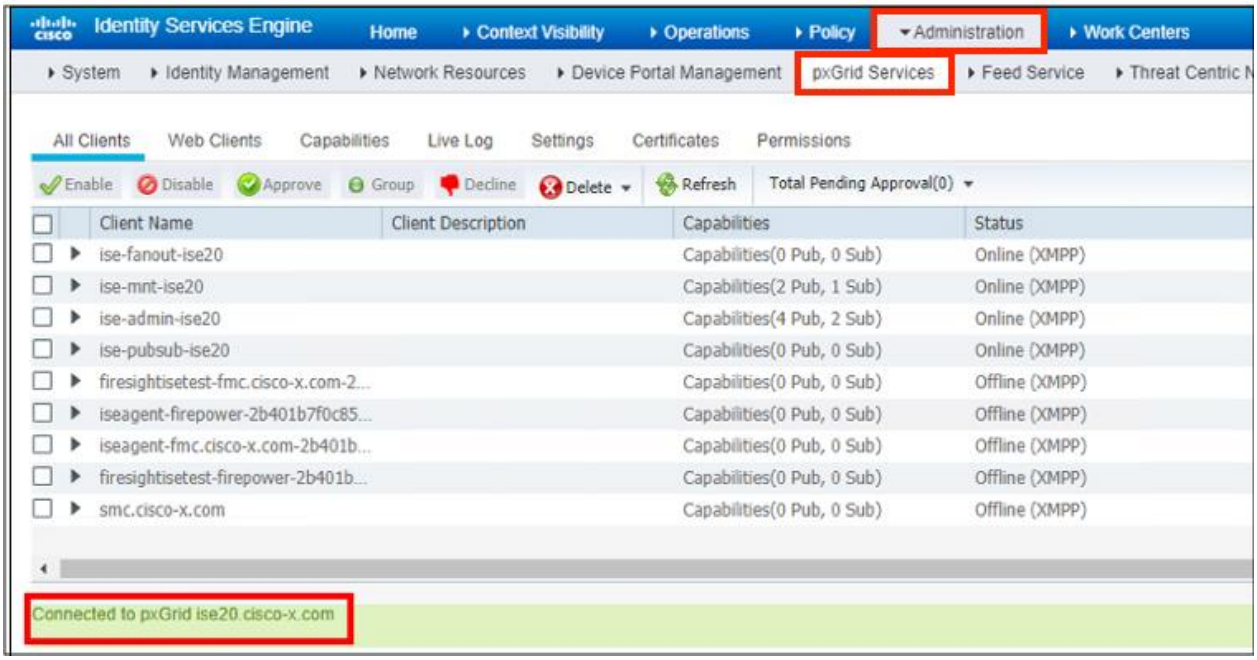


b. At the end of the **Edit Node** page, check the box to enable **pxGrid**.



Return to Contents

c. Navigate to **Administration > pxGrid Services**. The message "*Connected to pxGrid <server name>*" indicates a normal operating state.

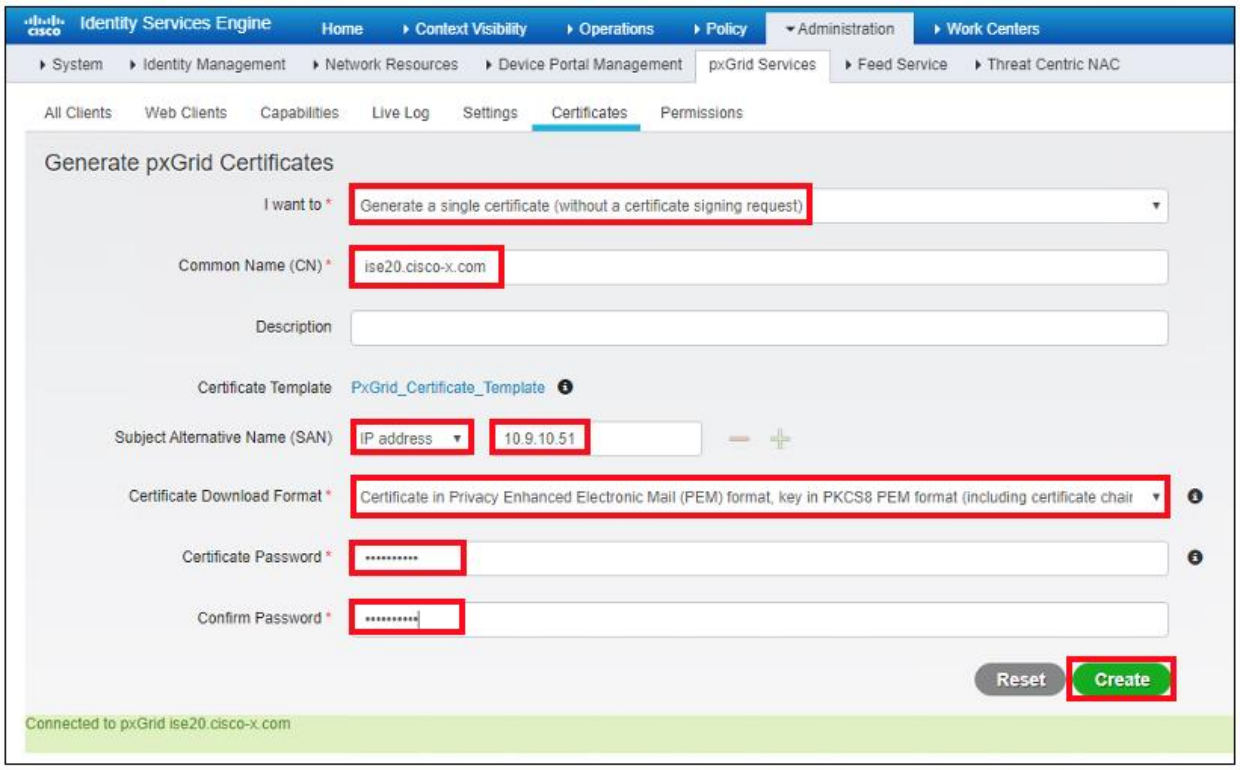


Step 2 Generate a pxGrid Certificate

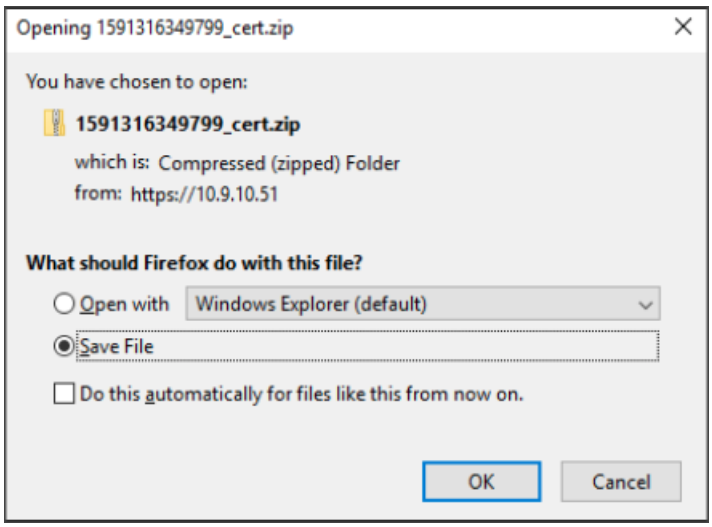
a. Navigate to the Certificates tab

b. Complete the form to generate the pxGrid Certificate.

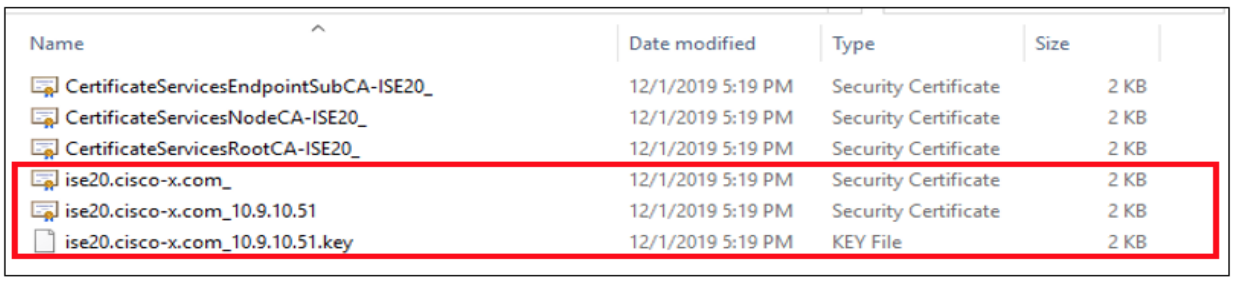
1. Use the dropdown menu in the **I want to** field and select **Generate a single certificate (without a certicate signing request)**
2. In the **Common Name (CN)** field: Type the *<FQDN>*
3. In the **Subject Alternative Name (SAN):**
   a. select **IP address**
   b. Type *< ISE server IP address>*
4. Using the **Certificate Download Format** menu, select **Certificate in Privacy Enhanced Electronic Mail (PEM), key in PKCS8**….
5. In the **Certificate Password**, field, Type *<certificate password>*
6. In the **Confirm Password field**, Type *<certificate password>*
7. Click **Create**



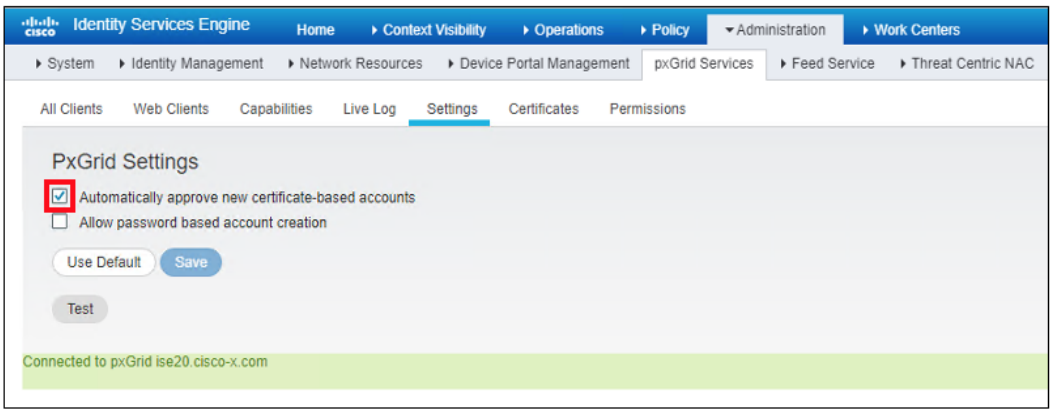
c. Once the certificates are created, the user is automatically prompted to save the zip file locally.



d. Extract the zip file and save the certificates and key for later use.

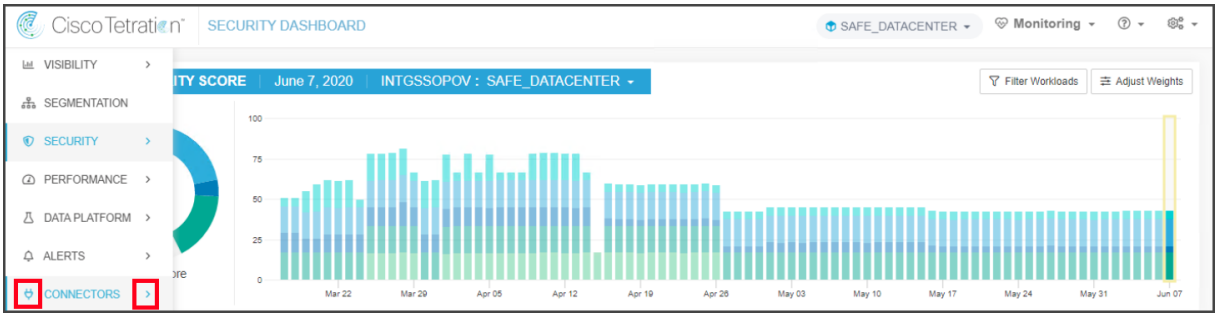


e. To automatically approve the certificates, navigate to **Administration > pxGrid > Settings** and enable **Automatically approve new certicate-based accounts.**

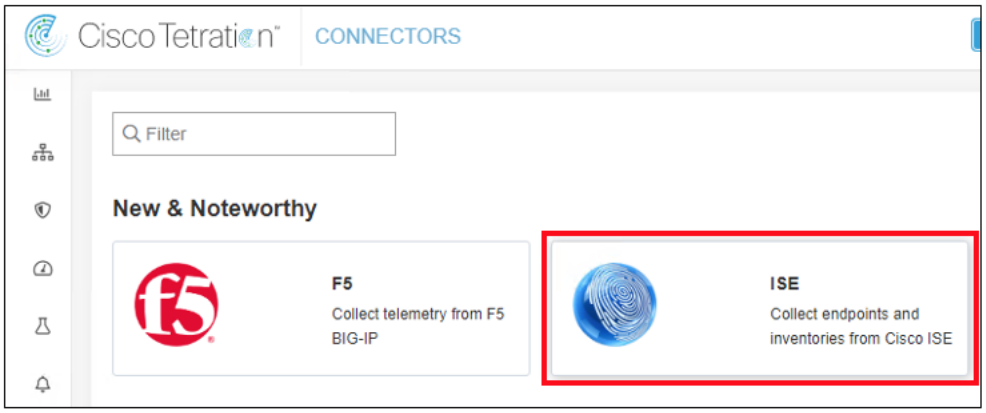


Step 3 Create the Tetration Virtual Edge Appliance Configuration Bundle

a. From the Tetration Management portal, hover over the **Connectors** Icon to expand the menu. Select **Connectors.**

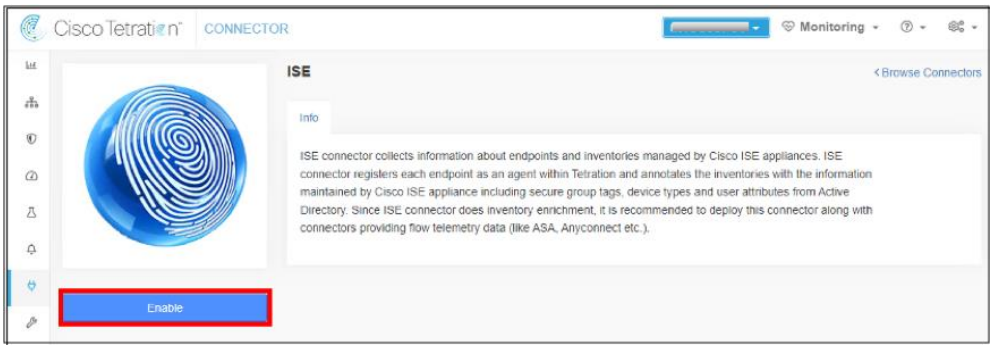


b. Select the **ISE** connector from the CONNECTORS page.

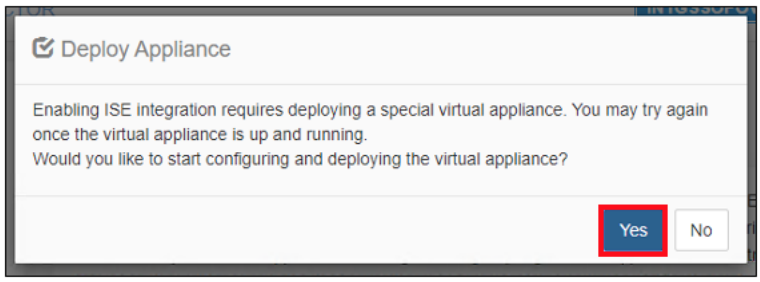


Return to Contents

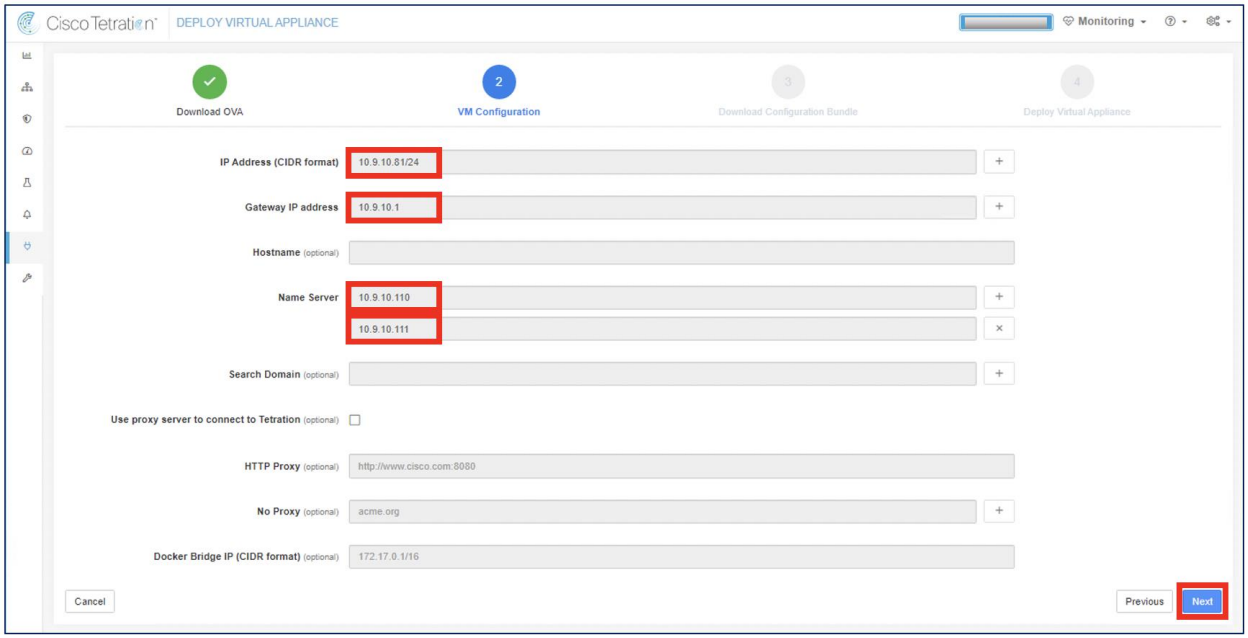
c. Click **Enable**.



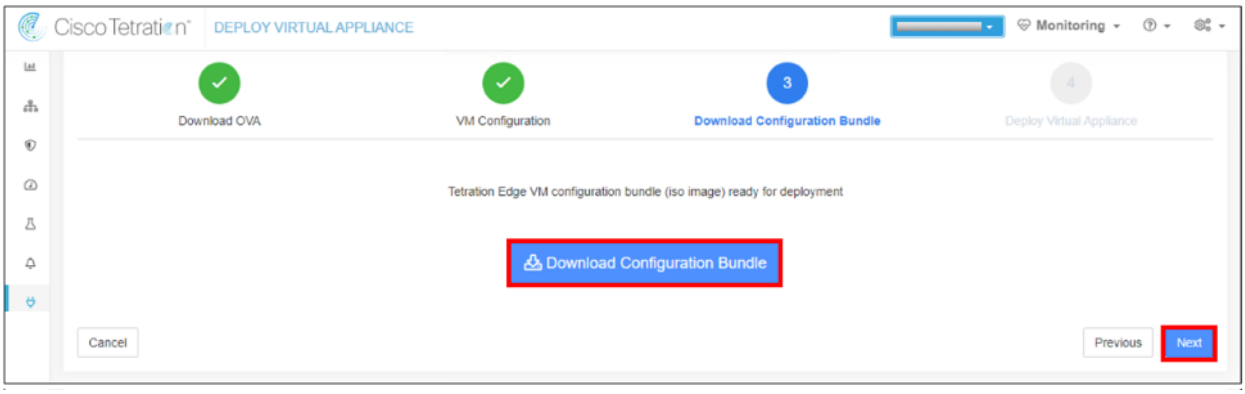
d. Click **Yes** to start the Configuration Bundle setup.



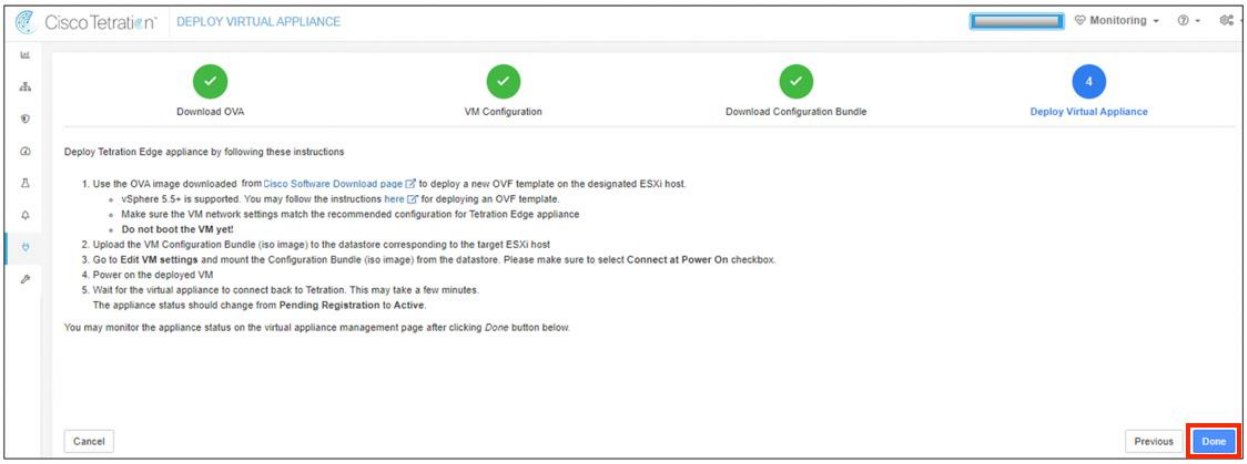
e. Enter the appliance IP information and click **Next**.



f. Click **Download Configuration Bundle**, save the ISO image and click **Next**.

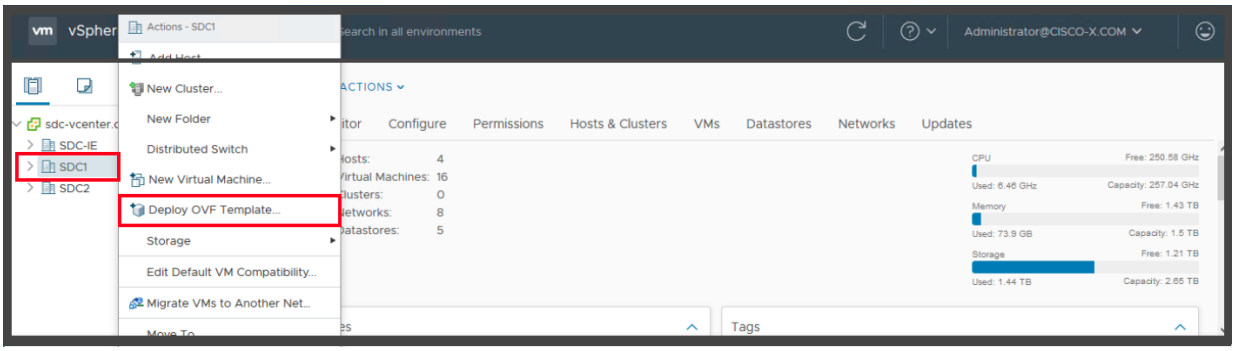


g. This page provides an overview of the deployment steps. Review and click **Done**.

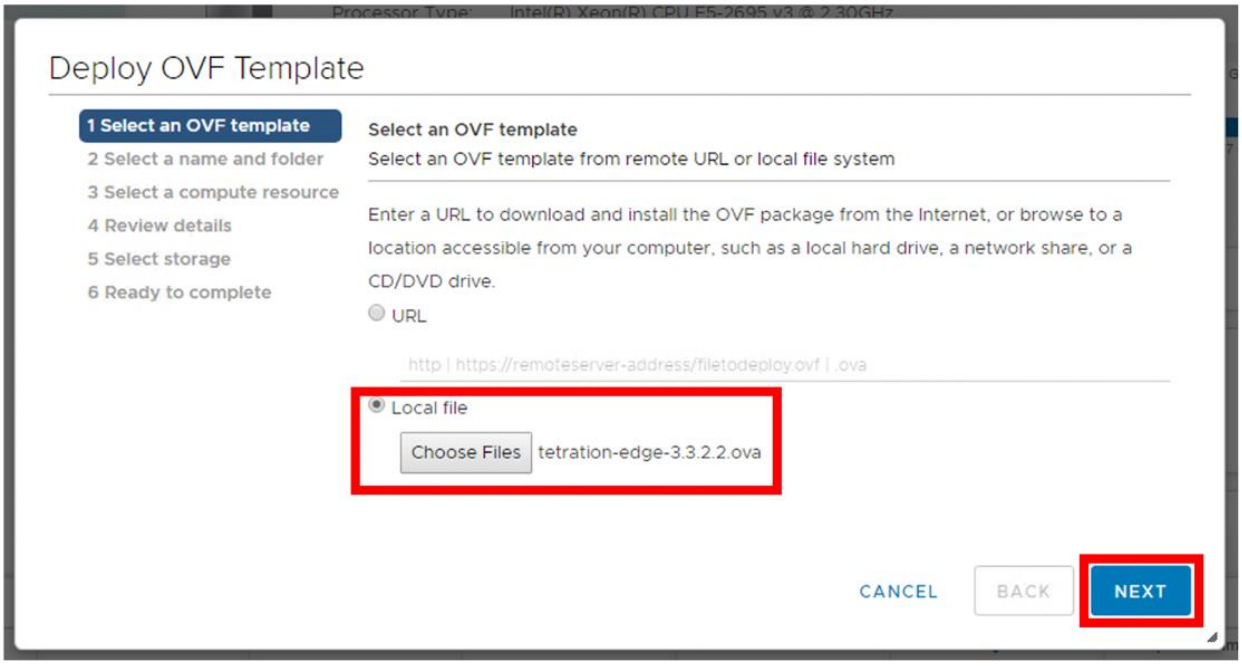


Step 4 Deploy the Tetration Virtual Edge Appliance

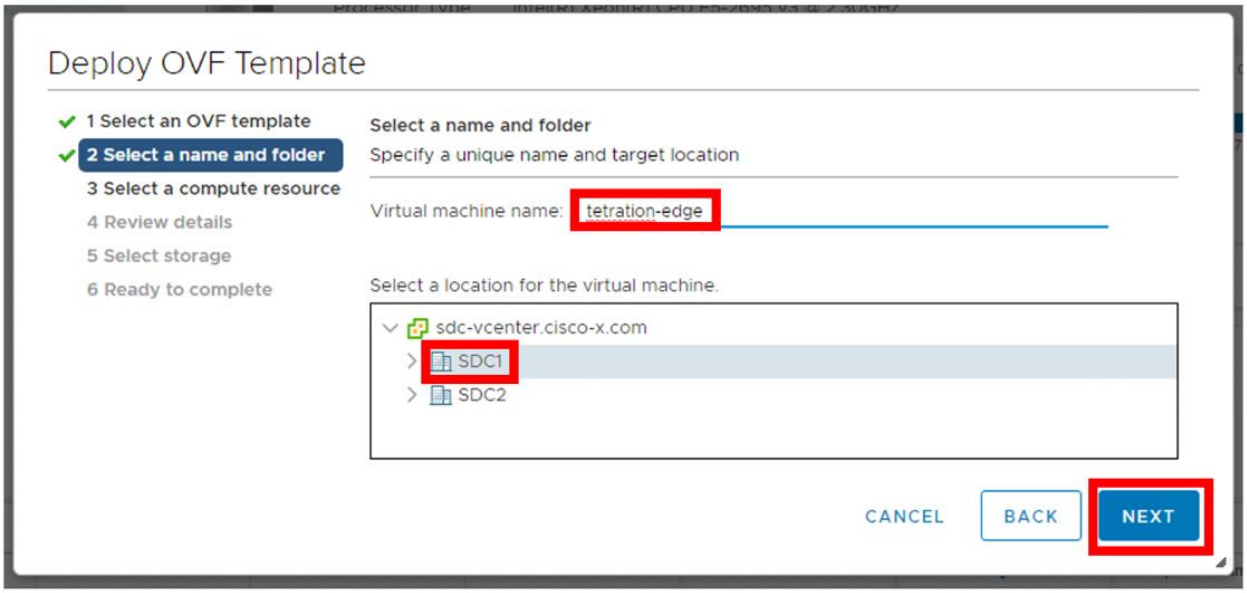
a. Log in to the vCenter. Right click the *<data center>* to host the VM and select **Deploy OVF Template**.



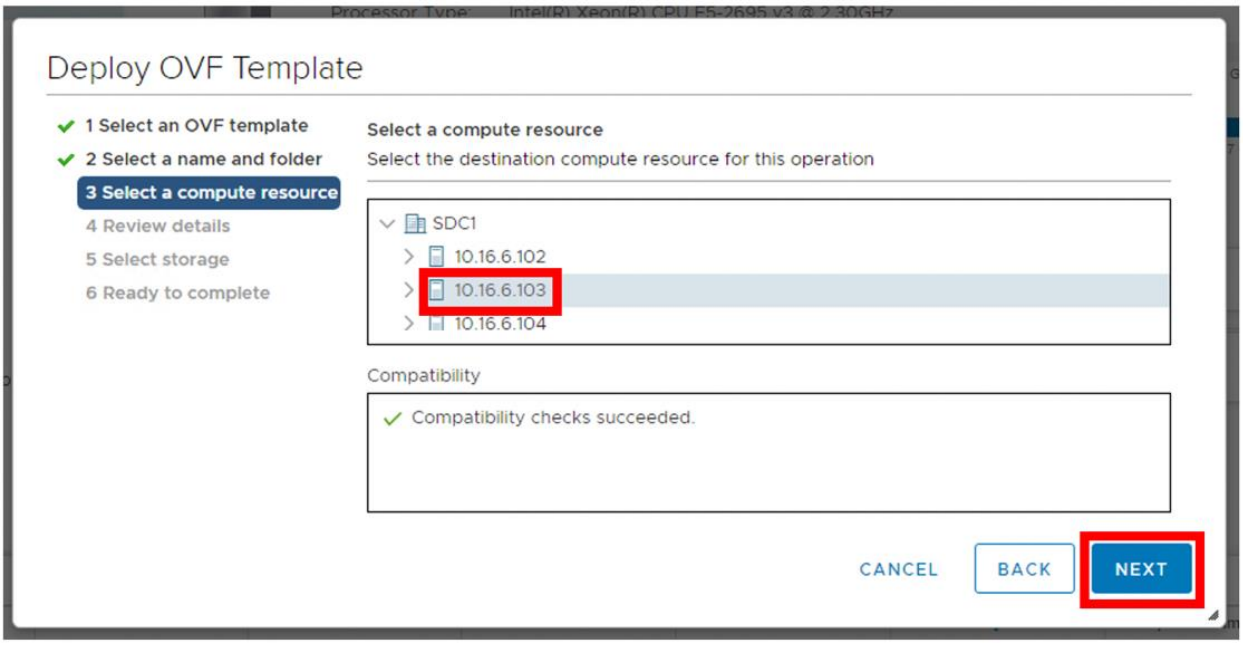
b. Select the **tetatration-edge-<version>.ova** downloaded from Cisco Software Download and click **Next**.



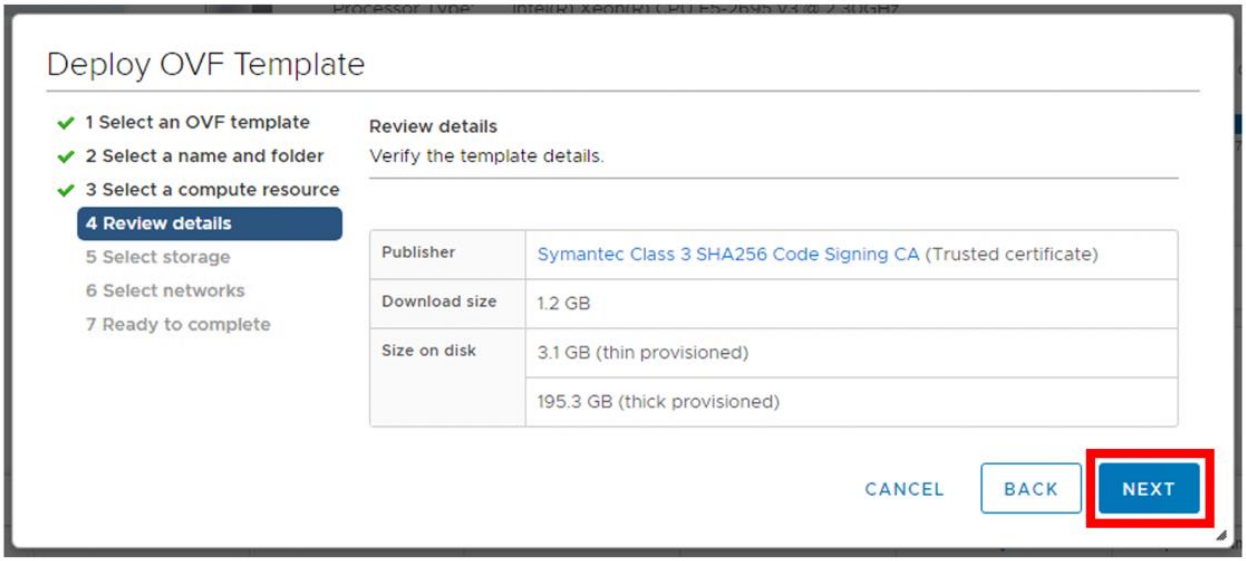
c. In the Virtual Machine Name, type *<VM Name>*. In the Select Location… window, select the <*data center*> to deploy the VM. Click **Next**.



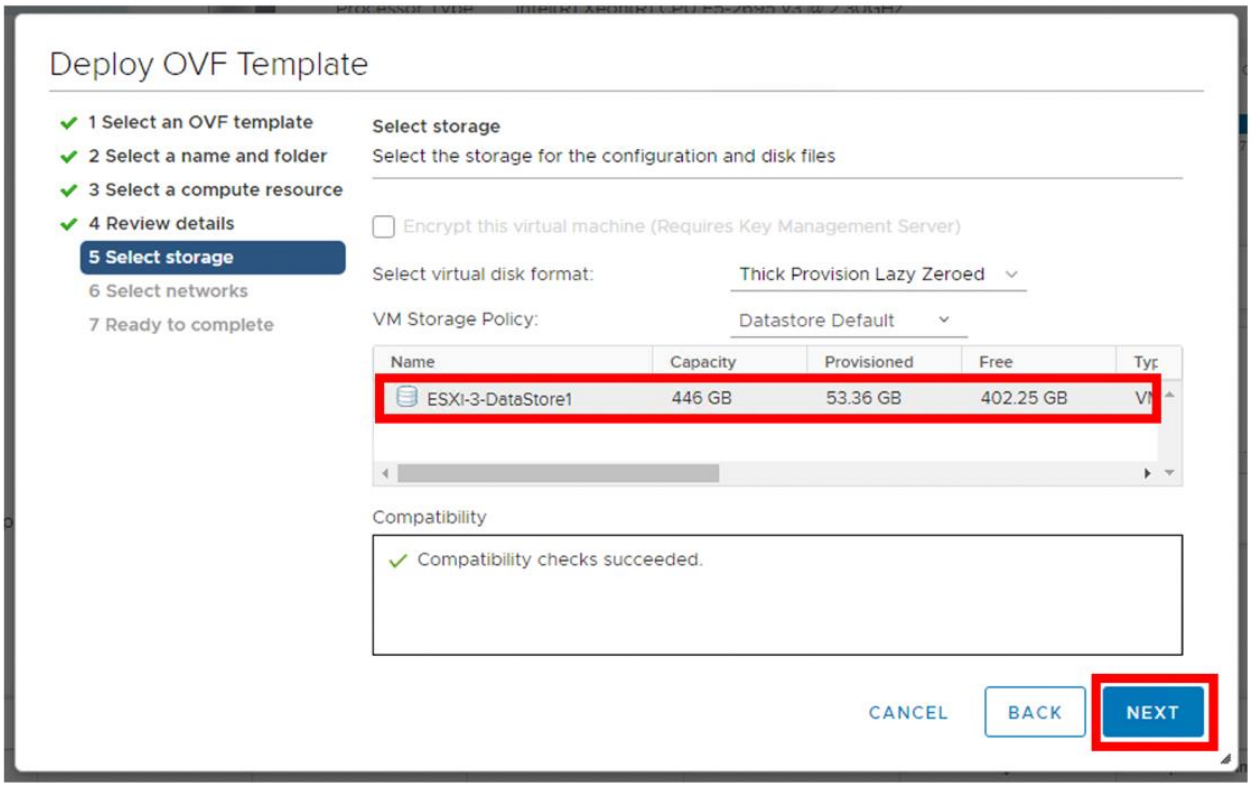
d. In the Select a Compute Resource Window, select the *<host>* and click **Next**.



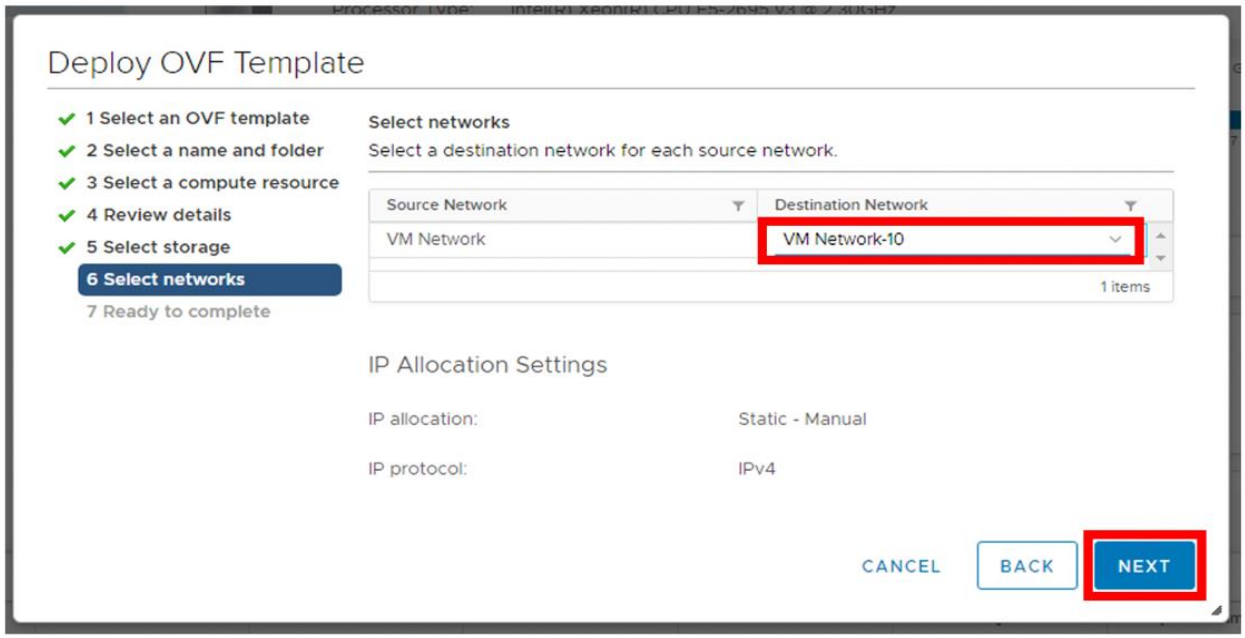
e. Review the VM settings and take note of the required storage. Click **Next**.



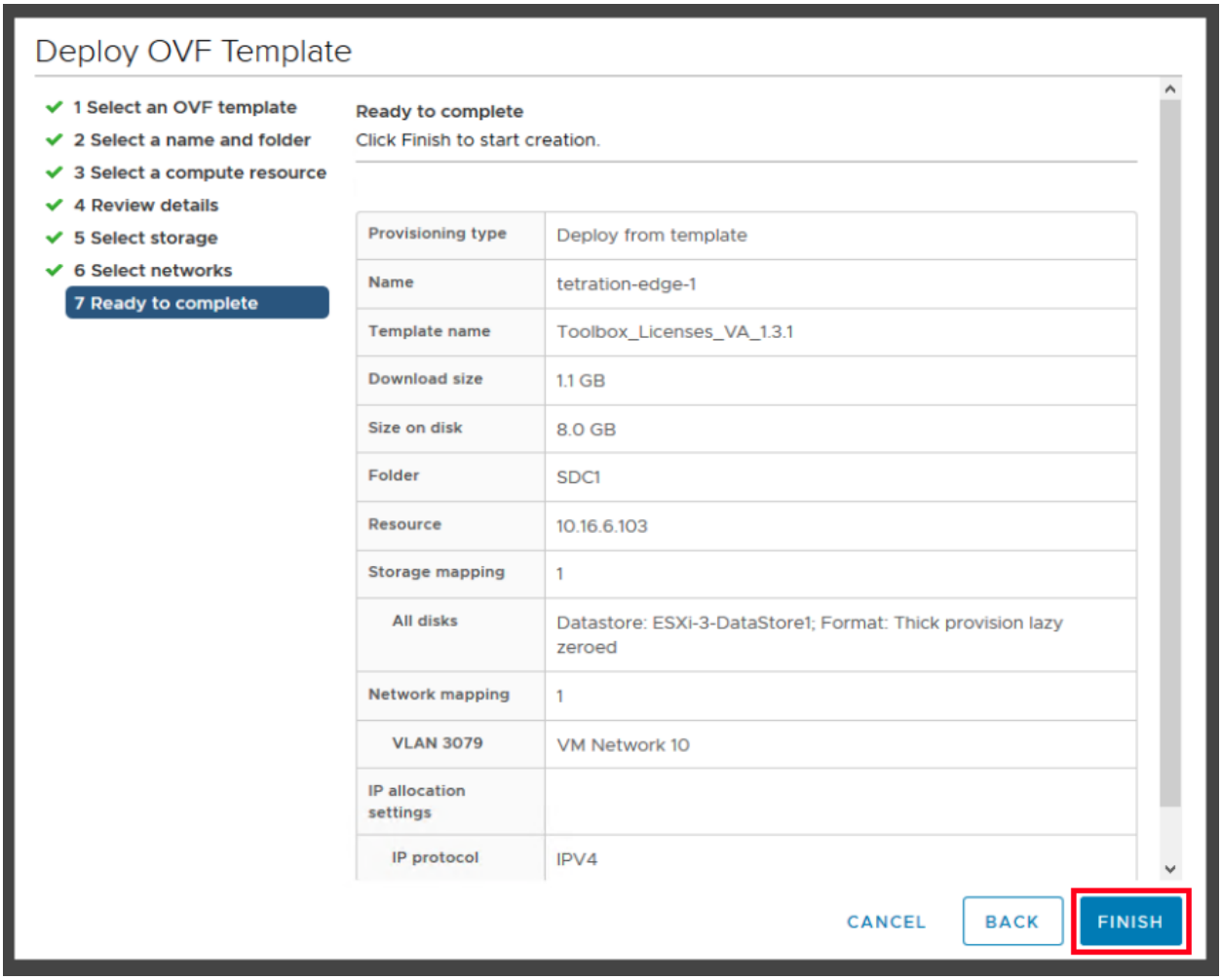
f. Select the *<datastore>* with capacity which meets the required diskspace and click NEXT.



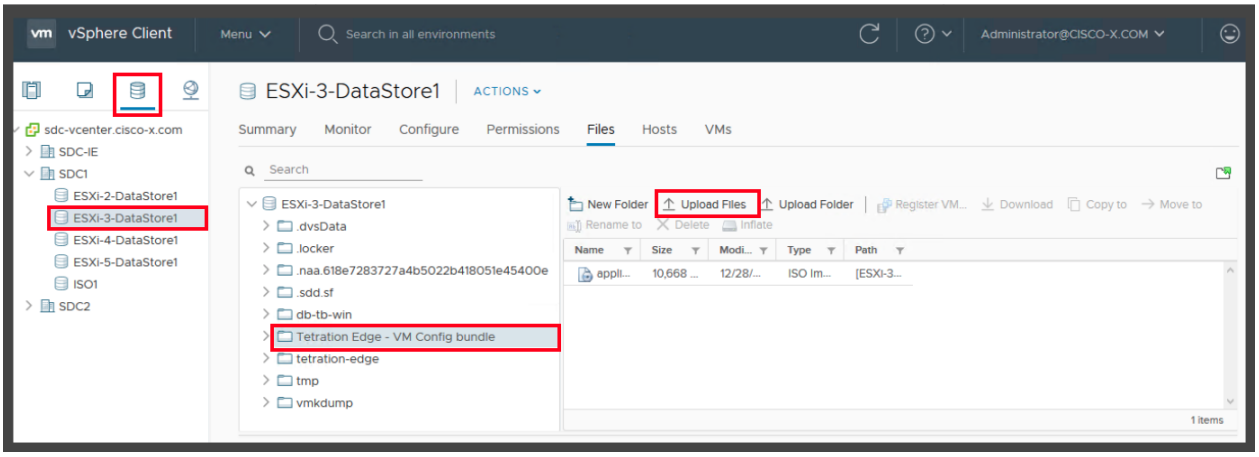
g. From the VM Network field, select the VM network which includes the appliance configured IP and click NEXT.



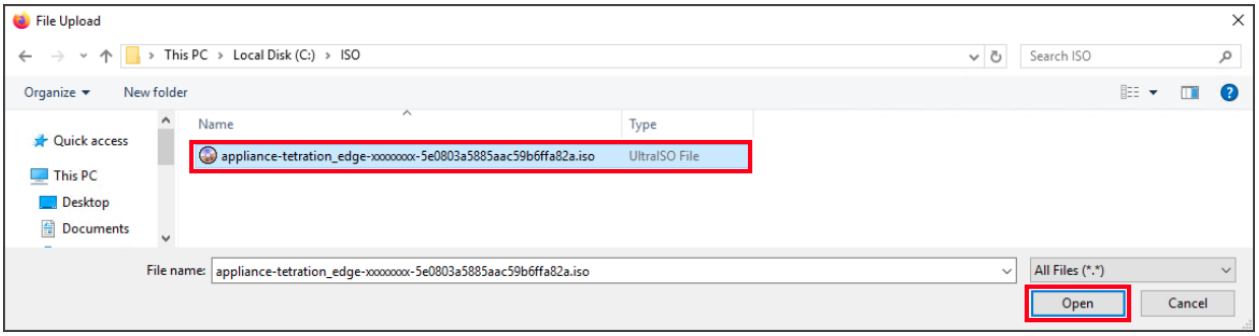
h. Review the VM configuration and click **Finish**.



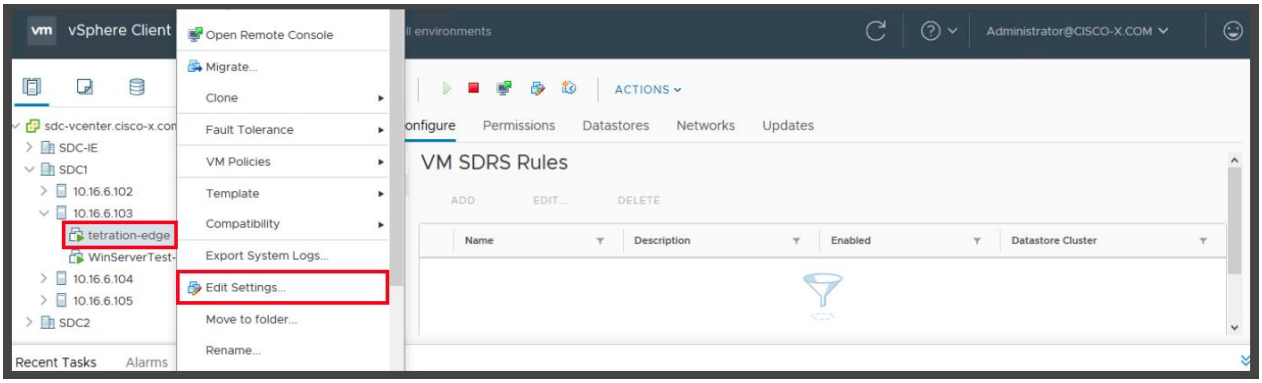
i. To upload the Configuration Bundle ISO to a datastore, Click Storage and right click on the <datastore>. Create a new folder or select an existing fold and click **Upload Files**.



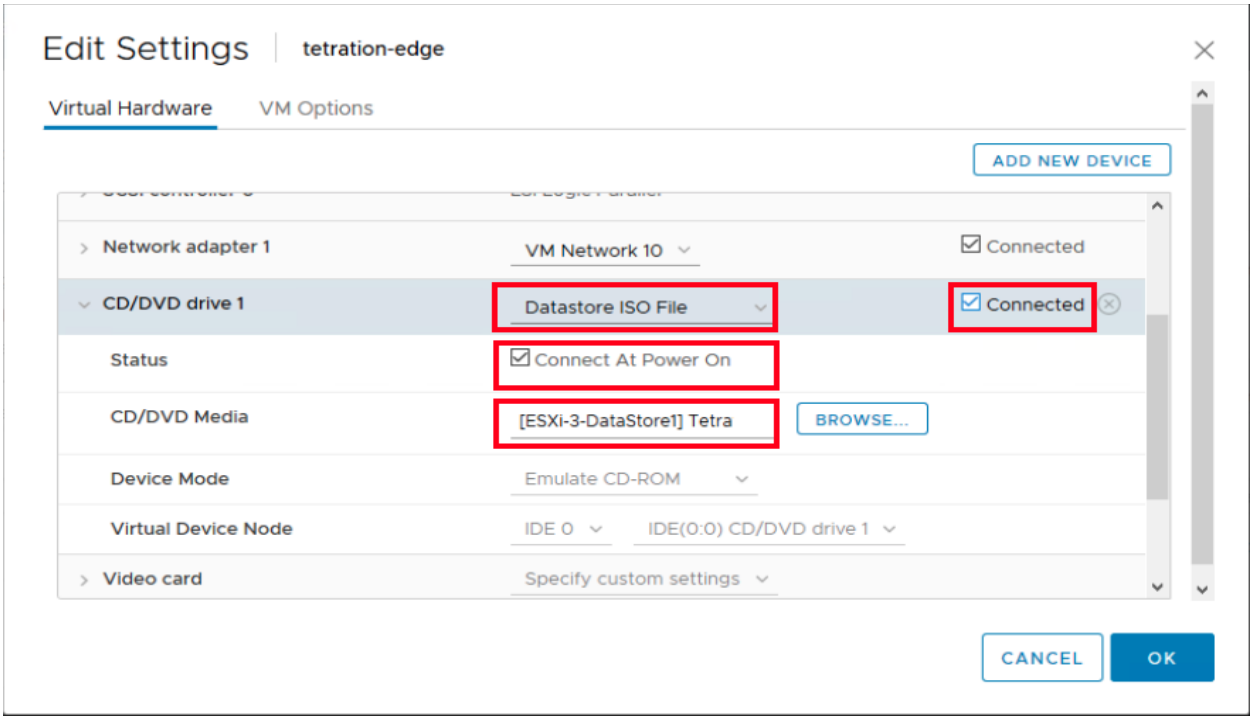
j. In the pop-up windows, select the Configuration Bundle ISO file and click **Open**.



k. Edit the Tetration Edge VM to mount the Configuration Bundle ISO. Navigate to the ESXi hosting the Tetration Edge VM, then right click the *<vm-name>* and select **Edit Settings**.



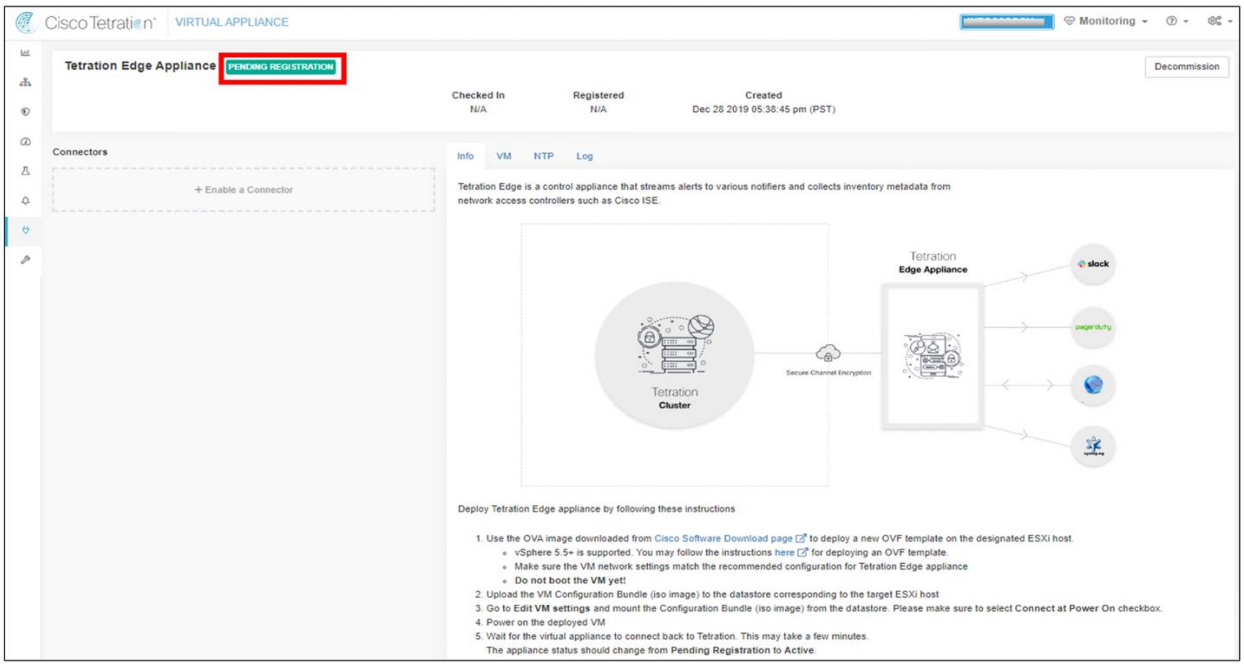
l. Use the dropdown menu in the CD/DVD drive 1 field, select the **Datastore ISO File** and check **Connected** box**.** In the Status field, check the **Connected At Power On** box. In the CD/DVD field, click **BROWSE** and select the Configuration Bundle ISO (**appliance-tetration_edge-<unique string>.iso**) previously uploaded. When completed, click **OK**.



Return to Contents

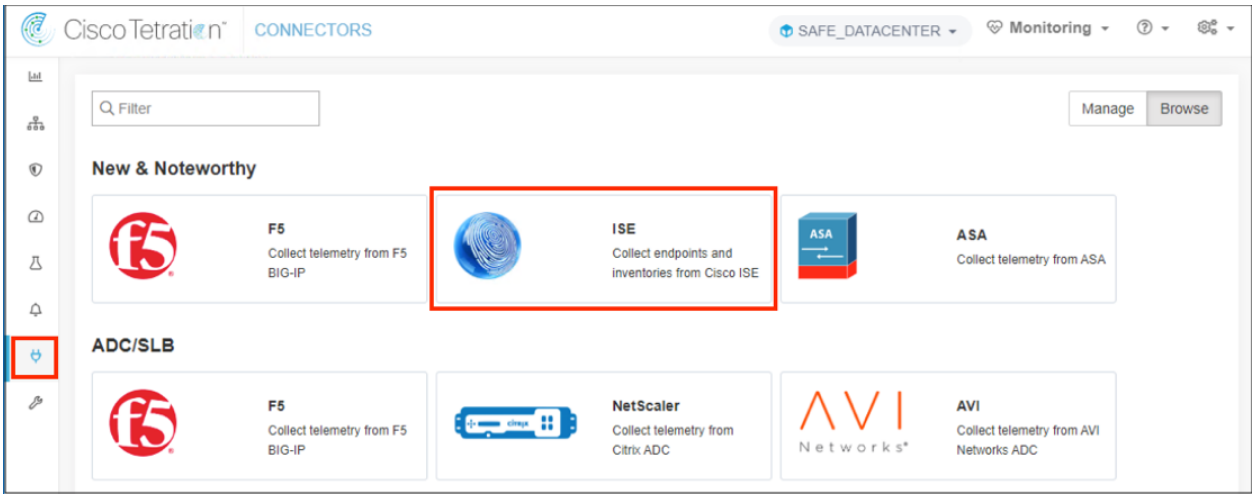
m. In the vCenter, power on the virtual machine.

Note: The Tetration Virtual Edge appliance will self-configured and self-registered using the Configuration Bundle image. In the Tetration management portal, the appliance status will change from PENDING REGISTRATION to ACTIVE when it has fully initialized and registered.

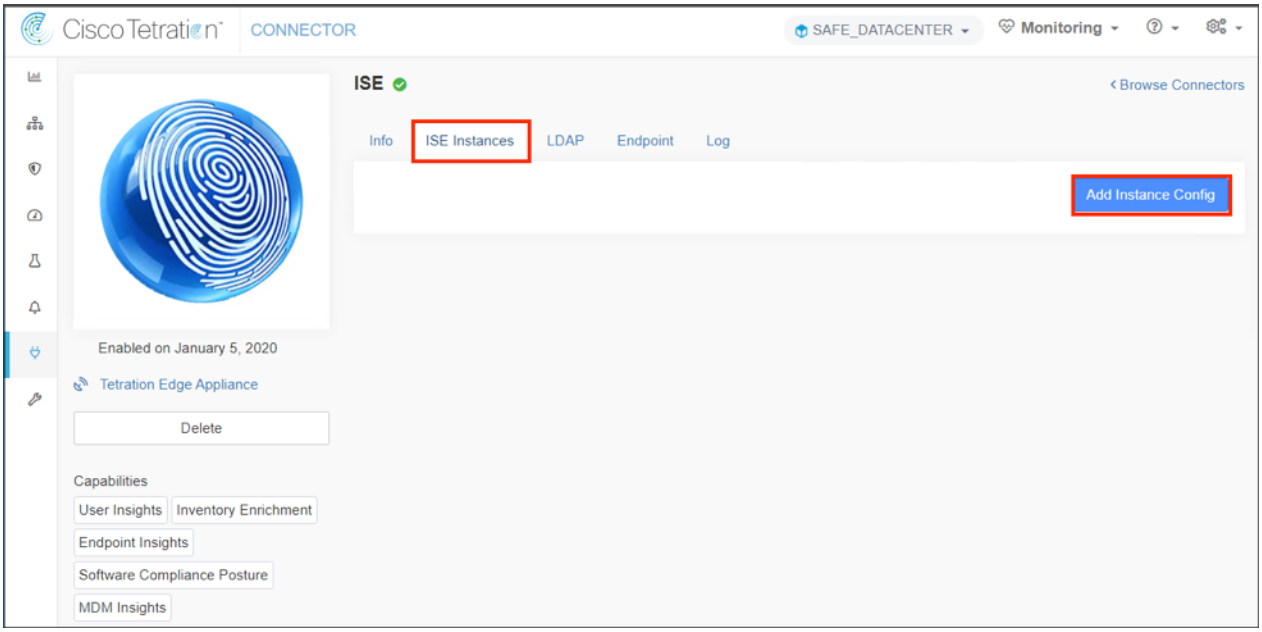


Step 5 Configure the ISE Connector

a. Click Connectors and in the workspace, select ISE.

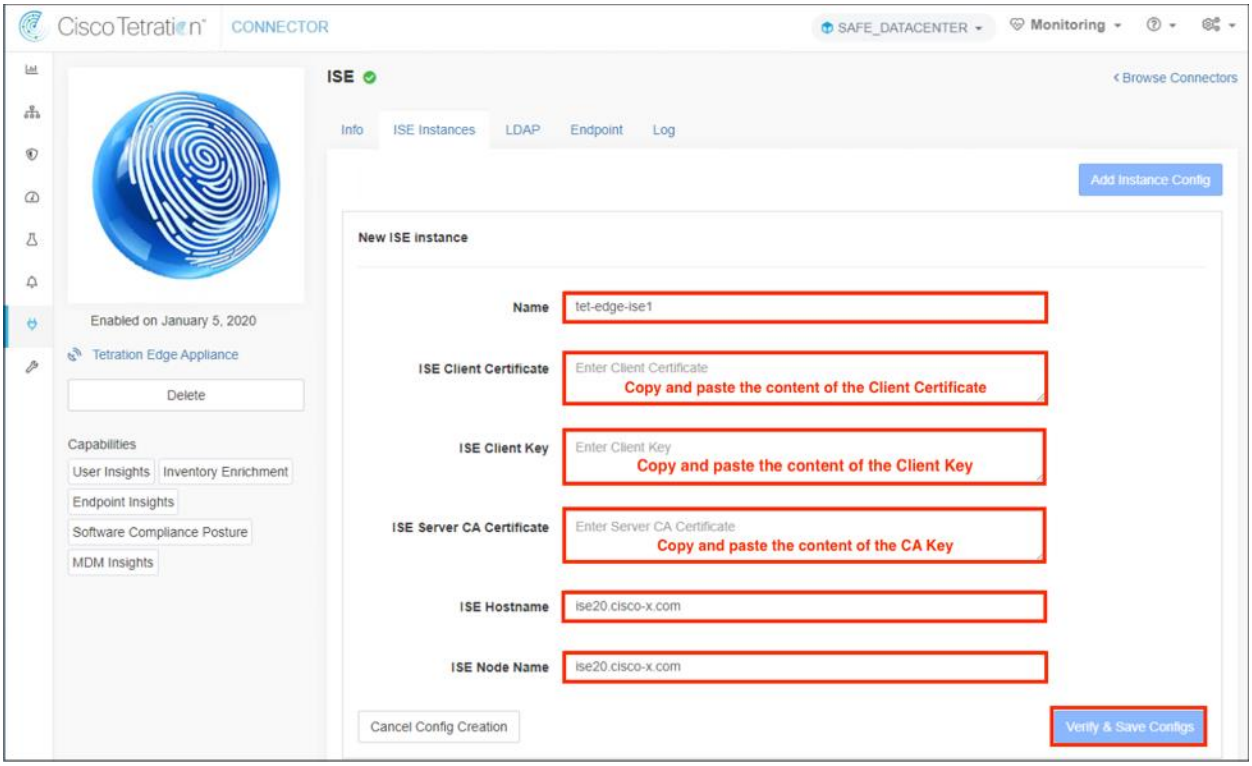


b. Select the ISE Instances tab and click Add Instance Config.



c. Complete the ISE Connector configuration.
   1. In the Name field, type *<ISE-Connector-Name>*
   2. In the ISE Client Certificate field, copy and paste the content of the ISE Client Certificate download previously.
   3. In the ISE Client key field, copy and paste the content of the ISE Client Key download previously.
   4. In the ISE Server CA Certificate field, copy and paste the content of the ISE Server CA Certificate download previously.
   5. In the ISE Hostname field, type *<ISE Server FQDN>.*
   6. In the ISE Node Name field, type *<ISE Noder FQDN>.*
   7. Click Verify &Save Configs.

Note: In this test environment, the ISE server and node are the same.

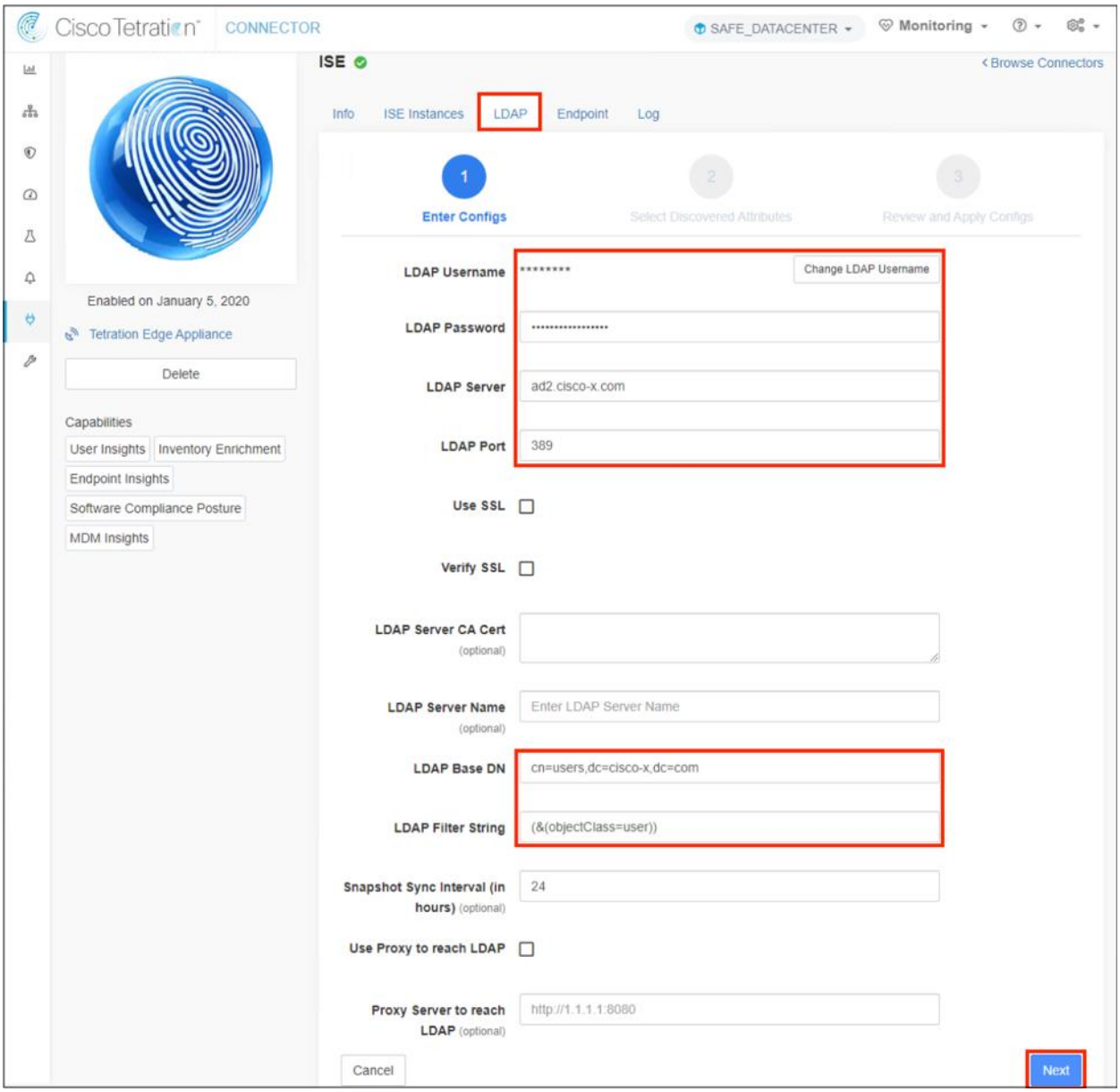


Return to Contents

Step 6 LDAP Configuration

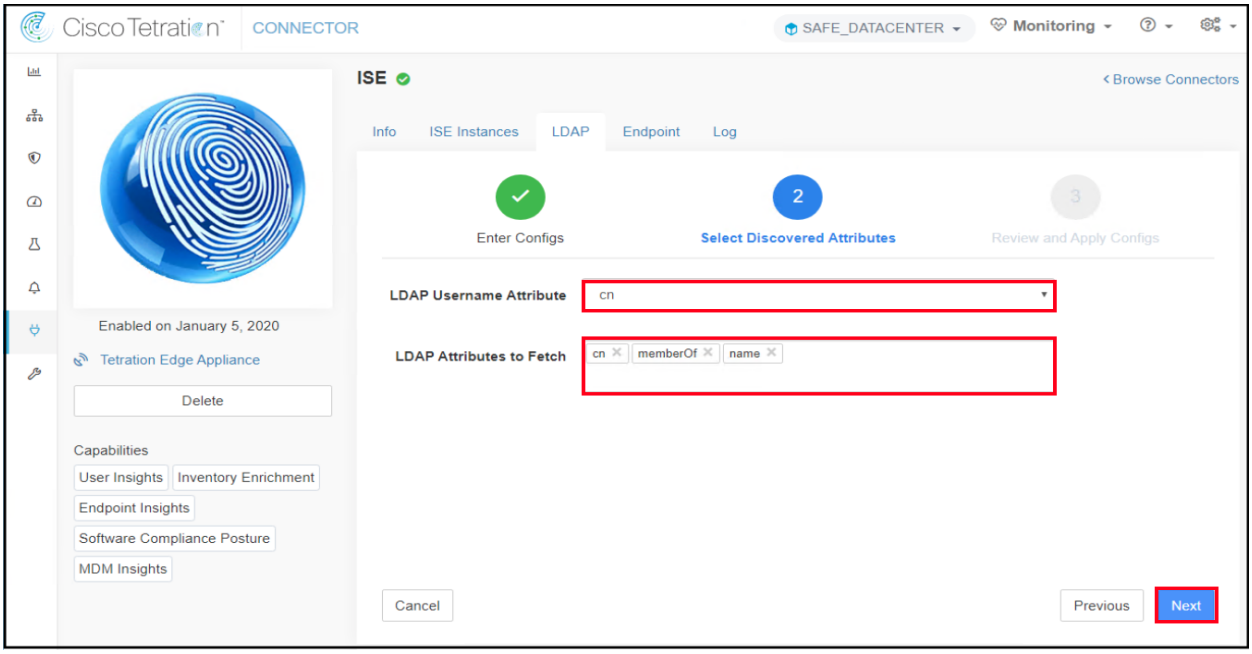
In this use case, we did not implement Tetration policy with LDAP attributes but have included the LDAP configuration to illustrate the feature. This is a minimum configuration to query LDAP and **should not be used in an production environemnt**.

a. Complete the LDAP configuration to connect ISE Connector to Microsoft Active Directory.
   1. In the LDAP User Name field, Type *<DC Service Account>*
   2. In the LDAP Password field, Type *< DC Services Account Password>*
   3. In the LDAP Server field, Type *<LDAP FQDN or IP Address>*
   4. In the LDAP Port Field, Type *<LDAP port number>*
   5. In the LDAP Base DN field, Type *<servers LDAP distinguished name>*
   6. In the LDAP Filter String field, Type *<LDAP filter String>*
   7. Click **Next**

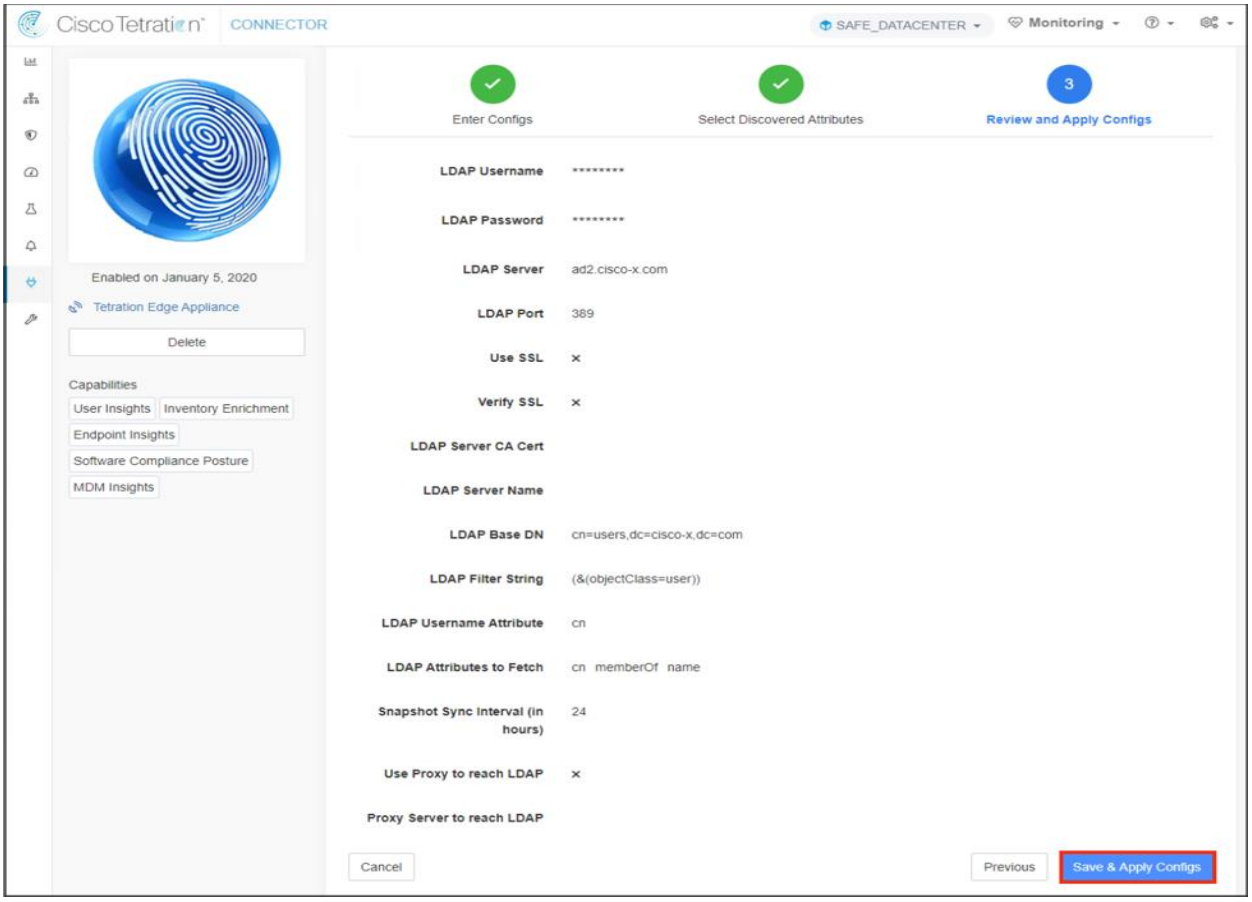


Return to Contents

b. From the Username Attribute dropdown menu, select **cn** and click **Next**.



c. Review and click **Save & Apply Configs**.



Note: The Endpoint and Log tabs were left as default.

Step 7 Annotation Inventory Upload

Tetration provides an option to add annotations (tags) to an IP or a subnet. Users can assign the annotations individually or in bulk with a CSV file. Both are options are available on the Inventory Upload page. Below are examples of the CSV file fields. An IP column is it is required, the remaining columns are user defined.

a. Create an annotation inventory file in CVS format. Use a spreadsheet application or a text editor.

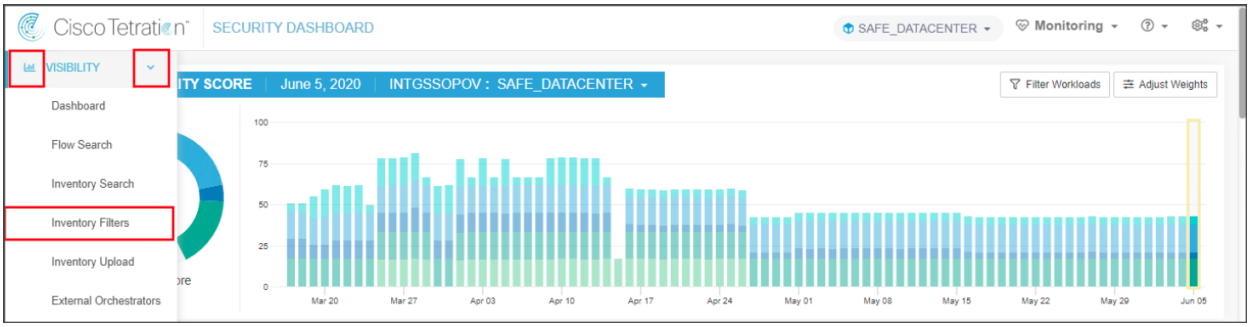
Spreadsheet Application

IP	Application	Location	Region	Tier	Type
10.18.107.0/24	WordPress			Web	DataCenter
10.18.108.0/24	WordPress			Application	DataCenter
10.18.109.0/24	WordPress			Database	DataCenter
10.9.110.0/24				Users	Campus

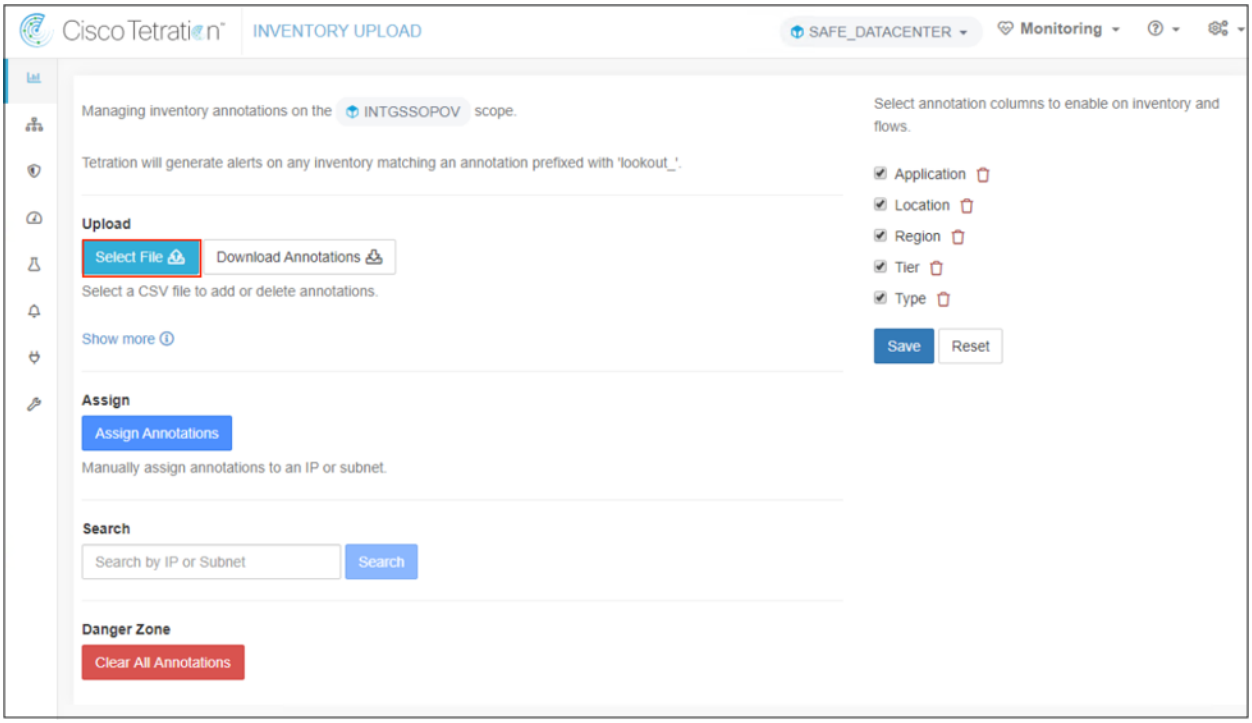
Text Editor

```
IP,Application,Location,Region,Tier,Type
10.18.107.0/24,WordPress,,,Web,DataCenter
10.18.108.0/24,WordPress,,,Application,DataCenter
10.18.109.0/24,WordPress,,,Database,DataCenter
10.9.110.0/24,,,,Users,Campus
```

b. From the Tetration Management portal, hover over the VISIBILITY Icon to expand the menu. Click the greater sign (>) to expand the VISIBILITY menu and select Inventory Upload.



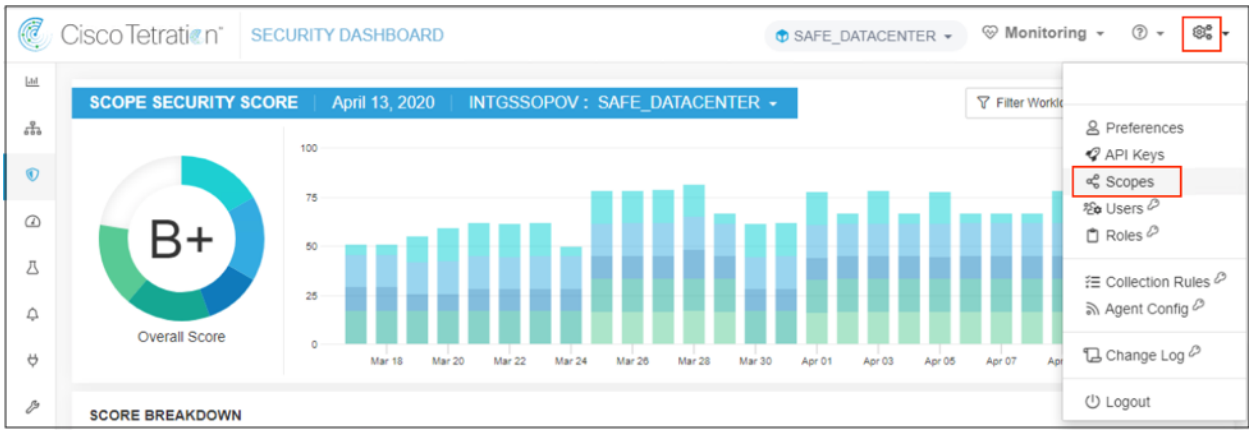
c. In the Upload section, click **Select File** and select the CSV file created in previous steps.



Note: To manually assign annotations, click the **Assign Annotations** under the Assign section

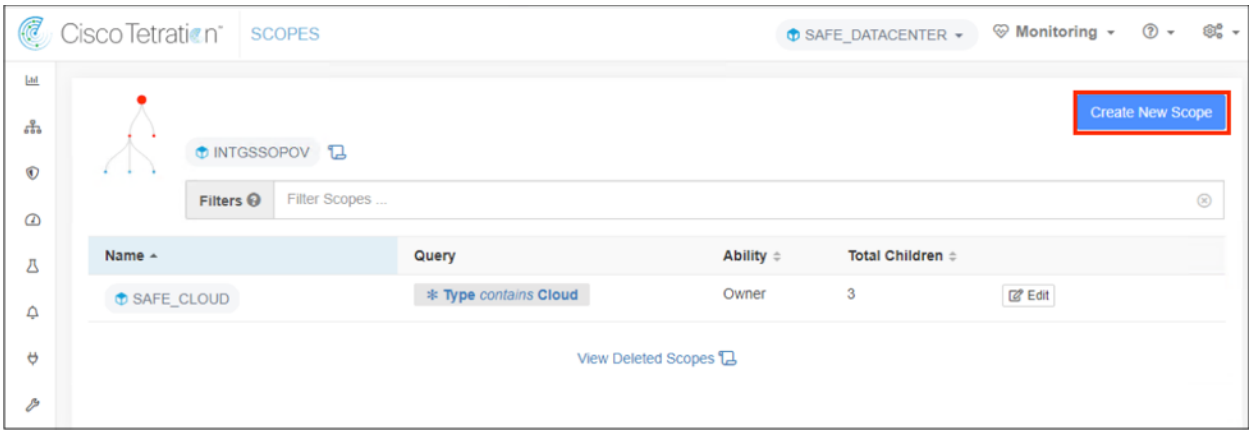
Step 8 Create Scope

a. From the Tetration management portal. Click the **Settings** icon and select **Scopes**.

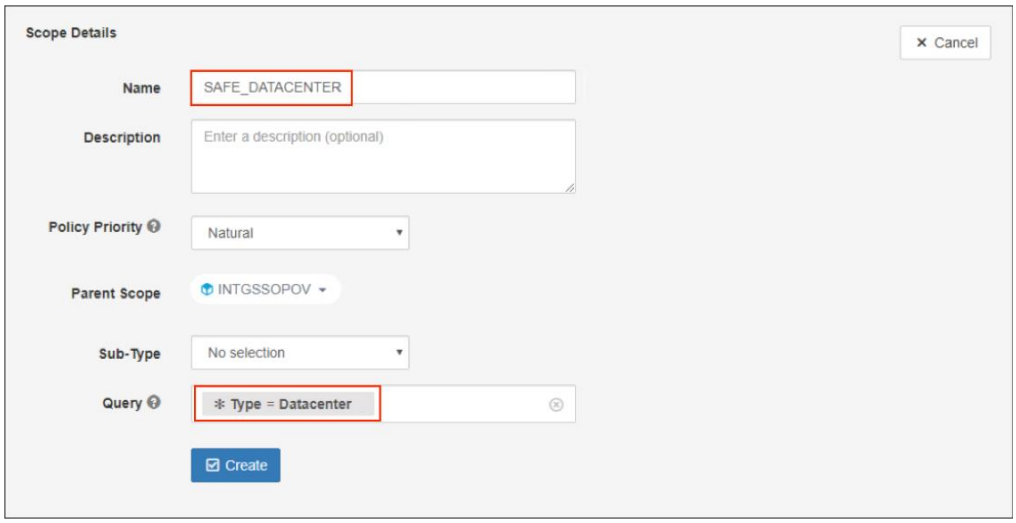


Return to Contents

b. From the scopes window, click **Create New Scope**.



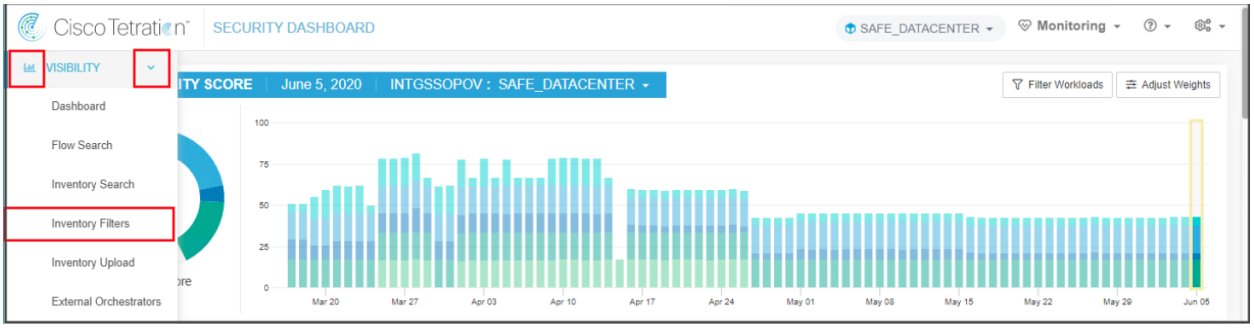
c. Complete the Scope Details form
   1. In the Name field, Type *<Scope Name>*
   2. In the Query field, Type *<Query Type>*
      Note: The Type (eg. Datacenter) was defined in the Annotation CSV file previously uploaded.
   3. When complete, click **Create**



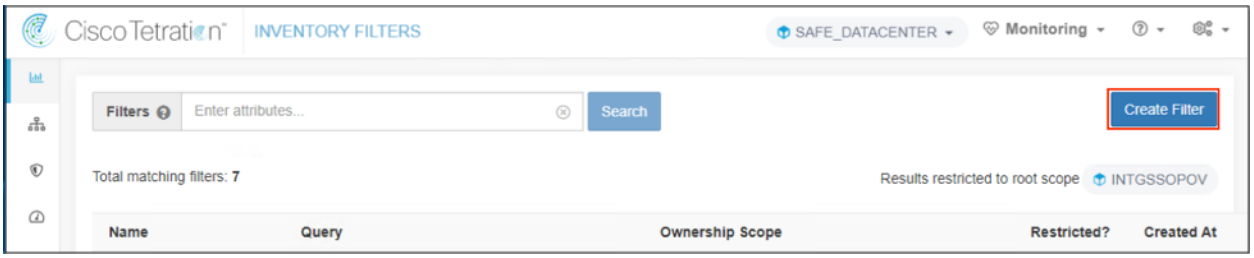
Note: For ease of management, it is recommended to limit the scope to a depth of 10 layers.

Step 9 Create Inventory Filters

a. From the Tetration Management portal, hover over the **VISIBILITY** Icon to expand the menu. Click the **greater** sign (>) to expand the VISIBILITY menu and select **Inventories Filters**.

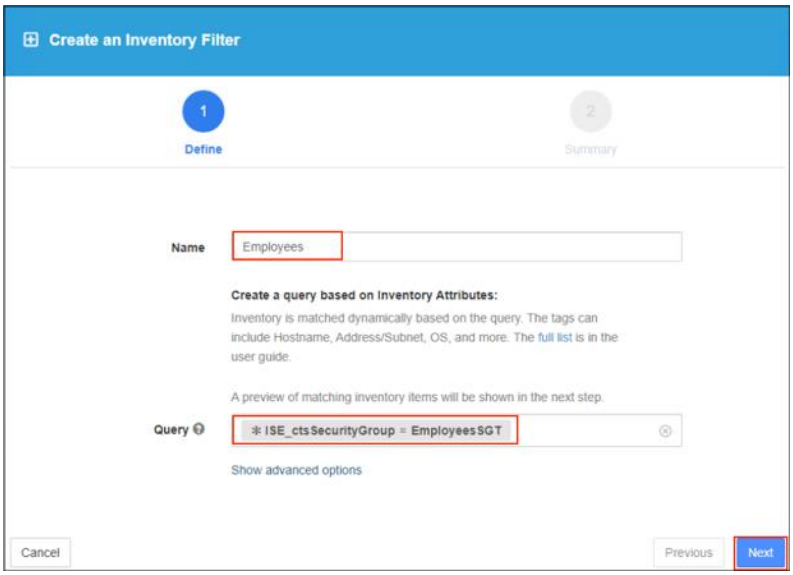


b. Click **Create Filter**.

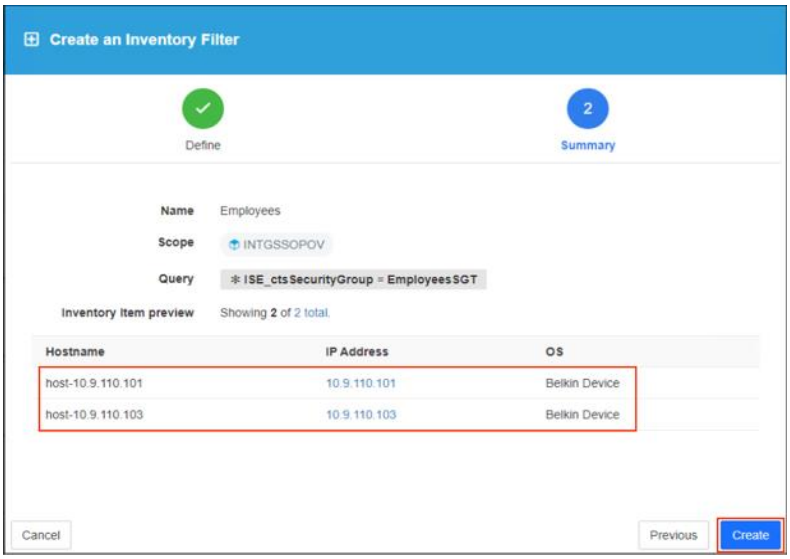


c. Complete the Create an Inventory Filter configuration.
   1. In the Name field, type *<filter-name>*
   2. In the Query field, type *<query>*
   3. When complete, click **Next**

Note: To see all available ISE queries, type ISE in the text box.

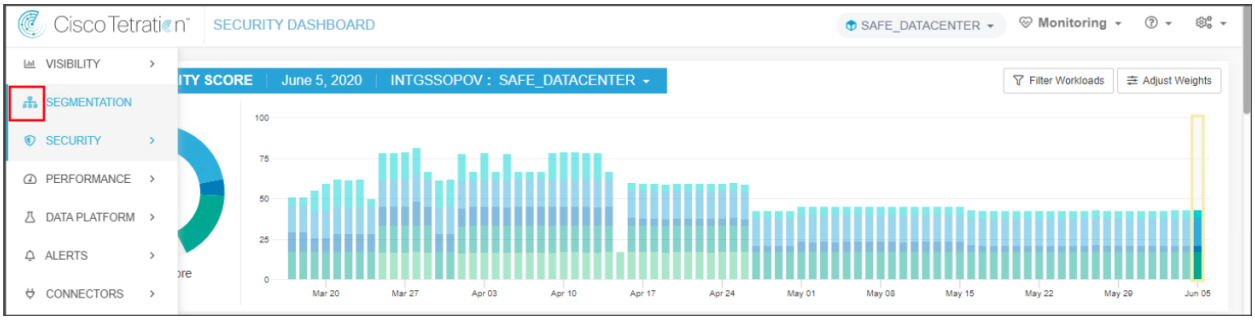


d. The query result is display. Review the result and click **Create**.

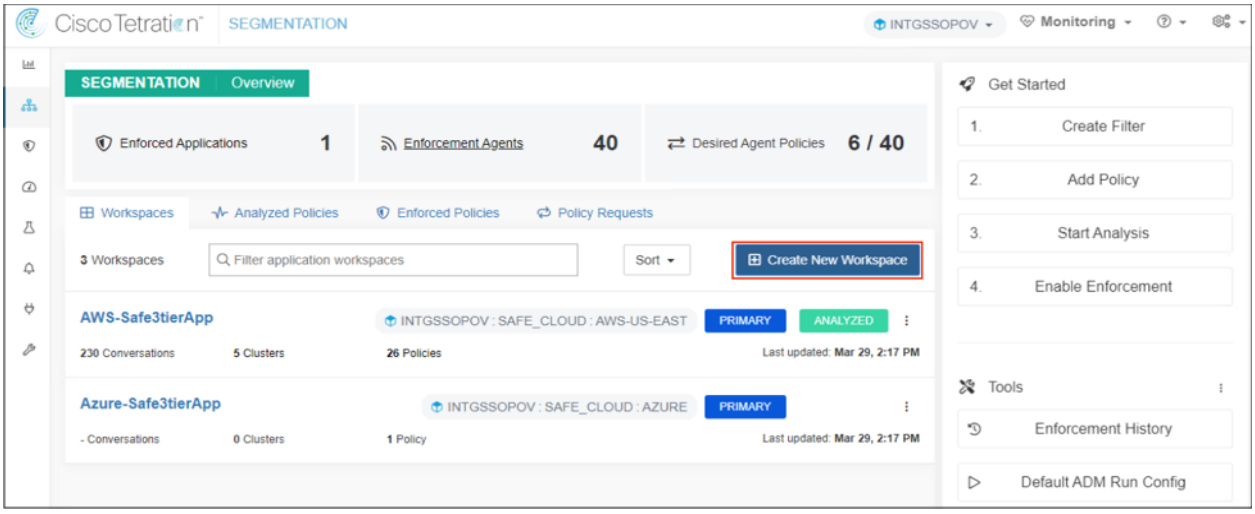


Step 10 Workspace Creation

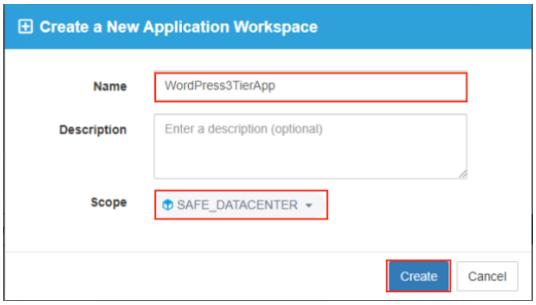
a. From the Tetration Management portal, hover over the **Segmentation Icon** to expand the menu. Select **SEGMENTATION** from the menu.



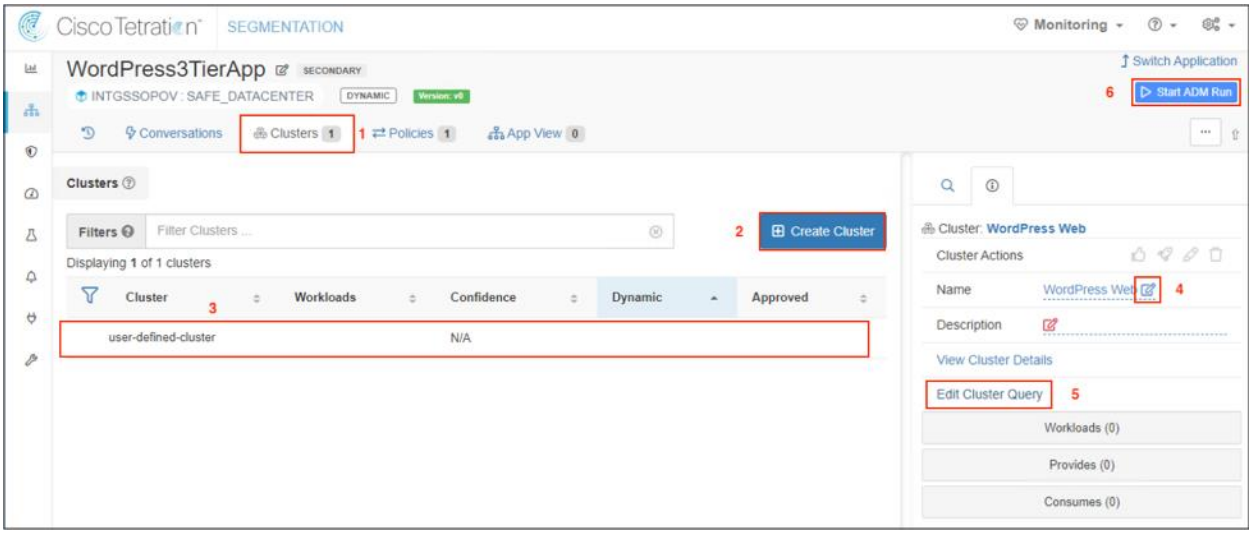
b. Click the **Create New Workspace**.



c. Enter a name for the workspace, select the previously created scope and click **Create**.



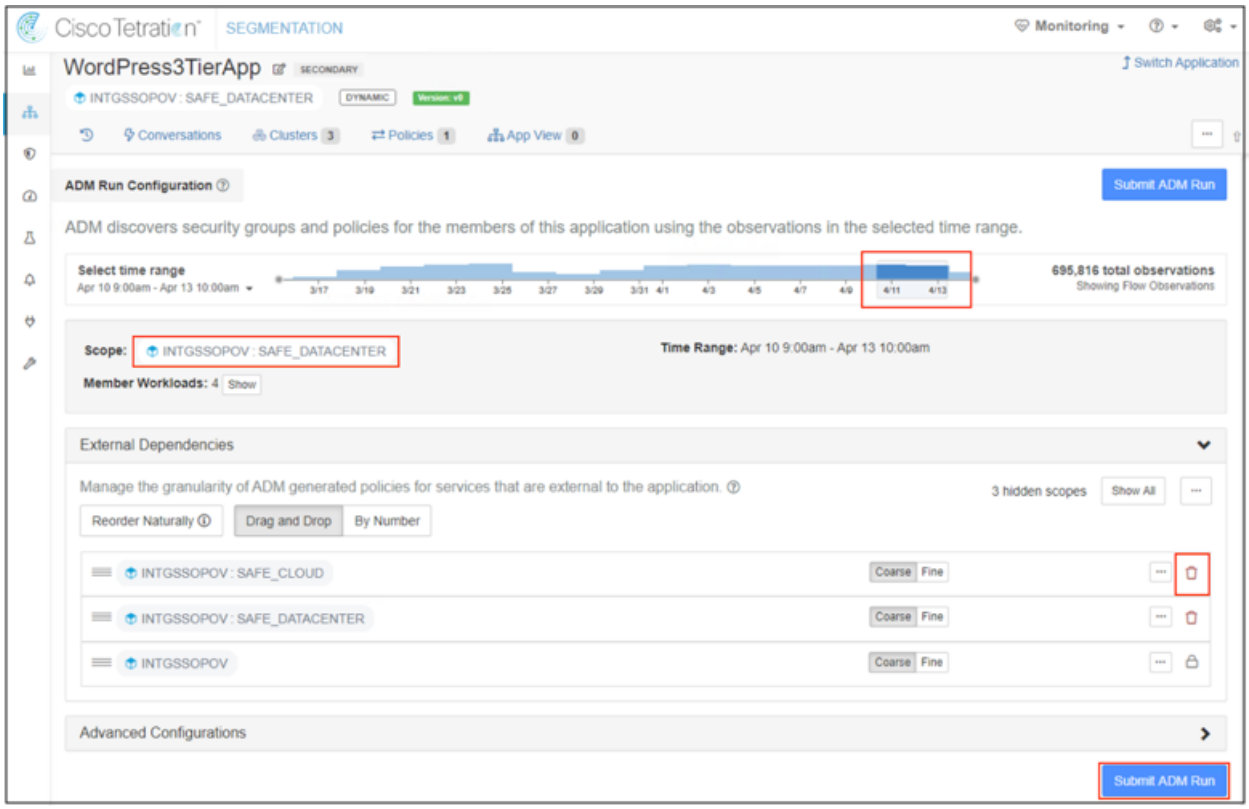
d. From the New Application Workspace, select **Clusters** (1) and click **Create Cluster** (2). Highlight *<new cluster>* (3) and click the edit icon (4) in the right panel to modify the name. Click **Edit Cluster Query** (5) to define the cluster.



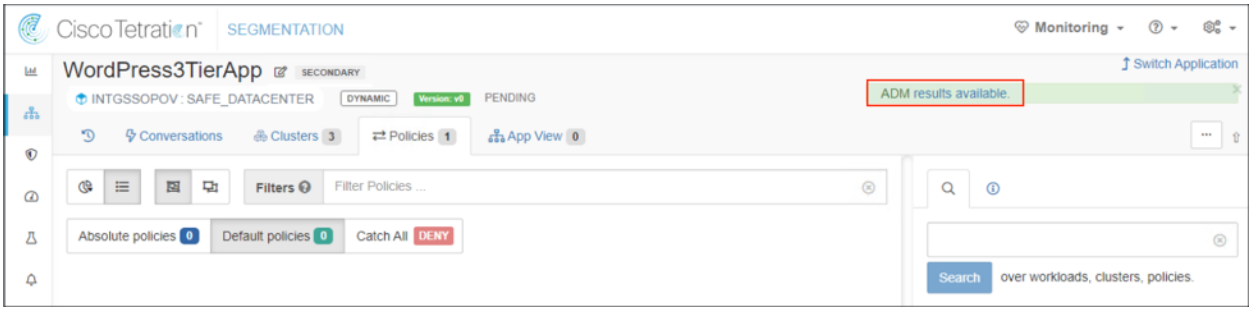
e. Enter **Type=Web** in the query box and click **Save**.

f. Repeat these steps to create the additional clusters, Application and DB. When all clusters have been defined, click **Start ADM Run** (6).

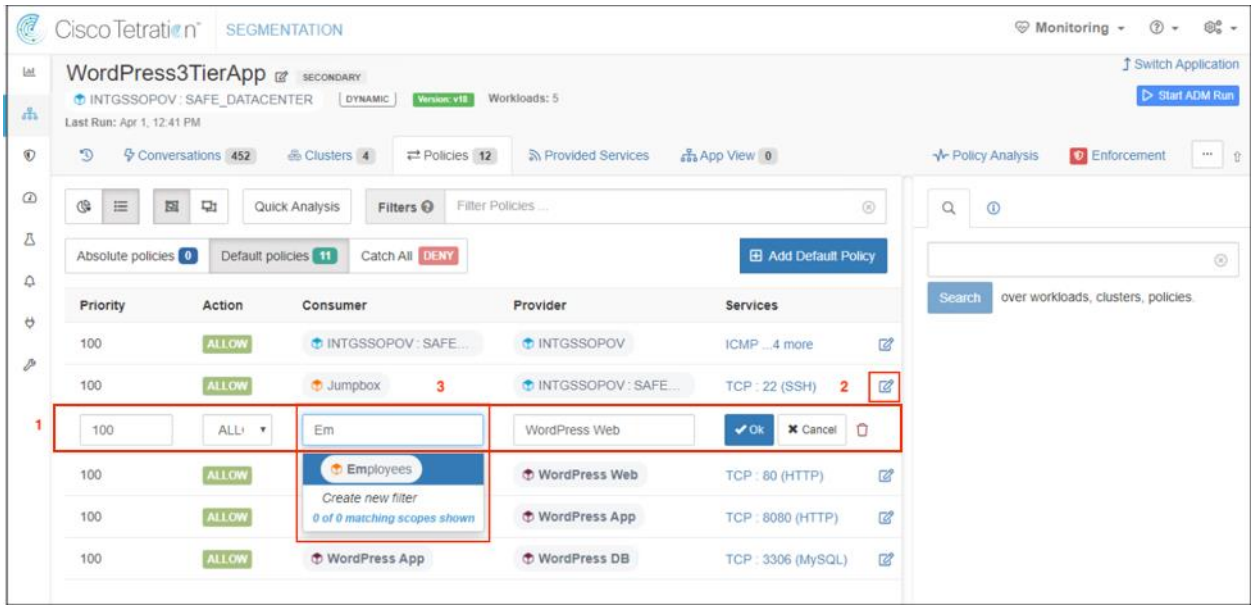
g. From the ADM Run Configuration screen, select the time range for the ADM Run to analyze. Verify the Scope is correct. Exclude unnecessary scopes by clicking the trash bin. Click on Submit ADM Run. The duration of the ADM Run can vary greatly depending on the amount of data to analyze.



h. When the ADM Run completes, the message ADM RESULTS AVAILABLE is display. Click it to view the policies created by ADM.

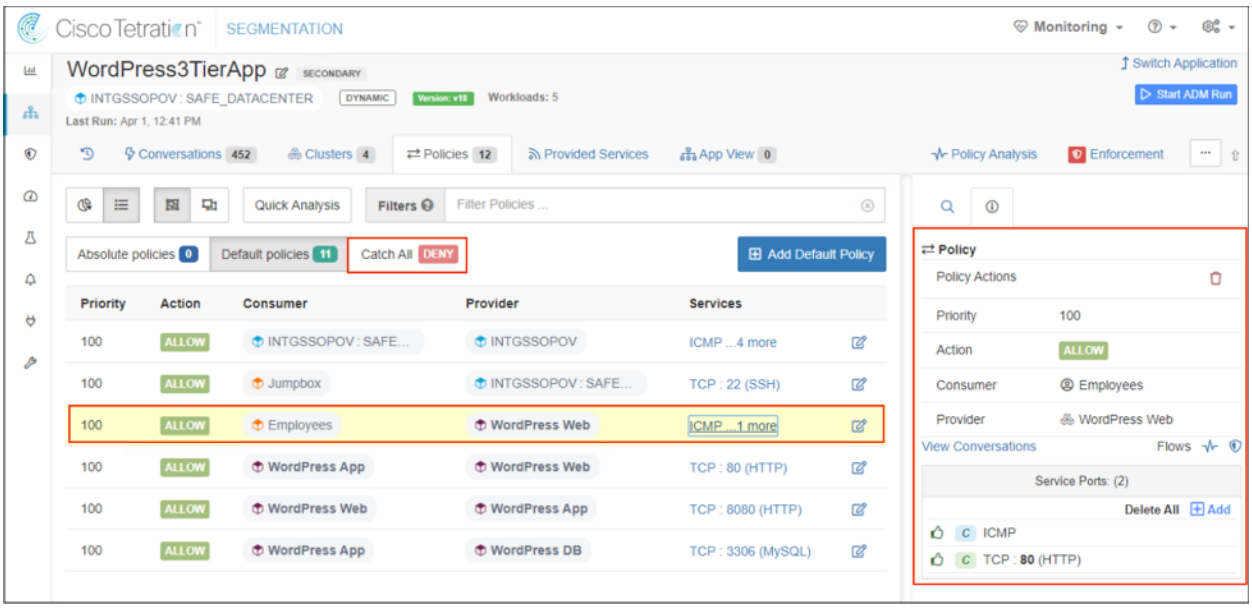


i. The Policies tab shows the policies created by the ADM Run. Locate the policy that allow network users to access the web application (1) and click the edit (2). In the Consumer field, type <filter-name> (3). The filter was created in Step 9.



j. The revised policy only allows endpoints matching the filter to access the web application.

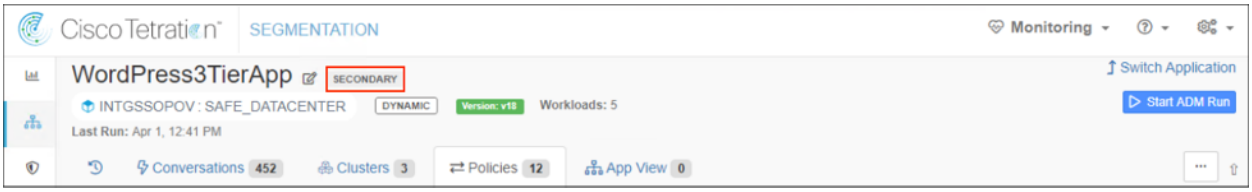
In this test case, users in the Employees group are ALLOW to access the web server and users in the Contractors group are DENY by the Catch All DENY policy.



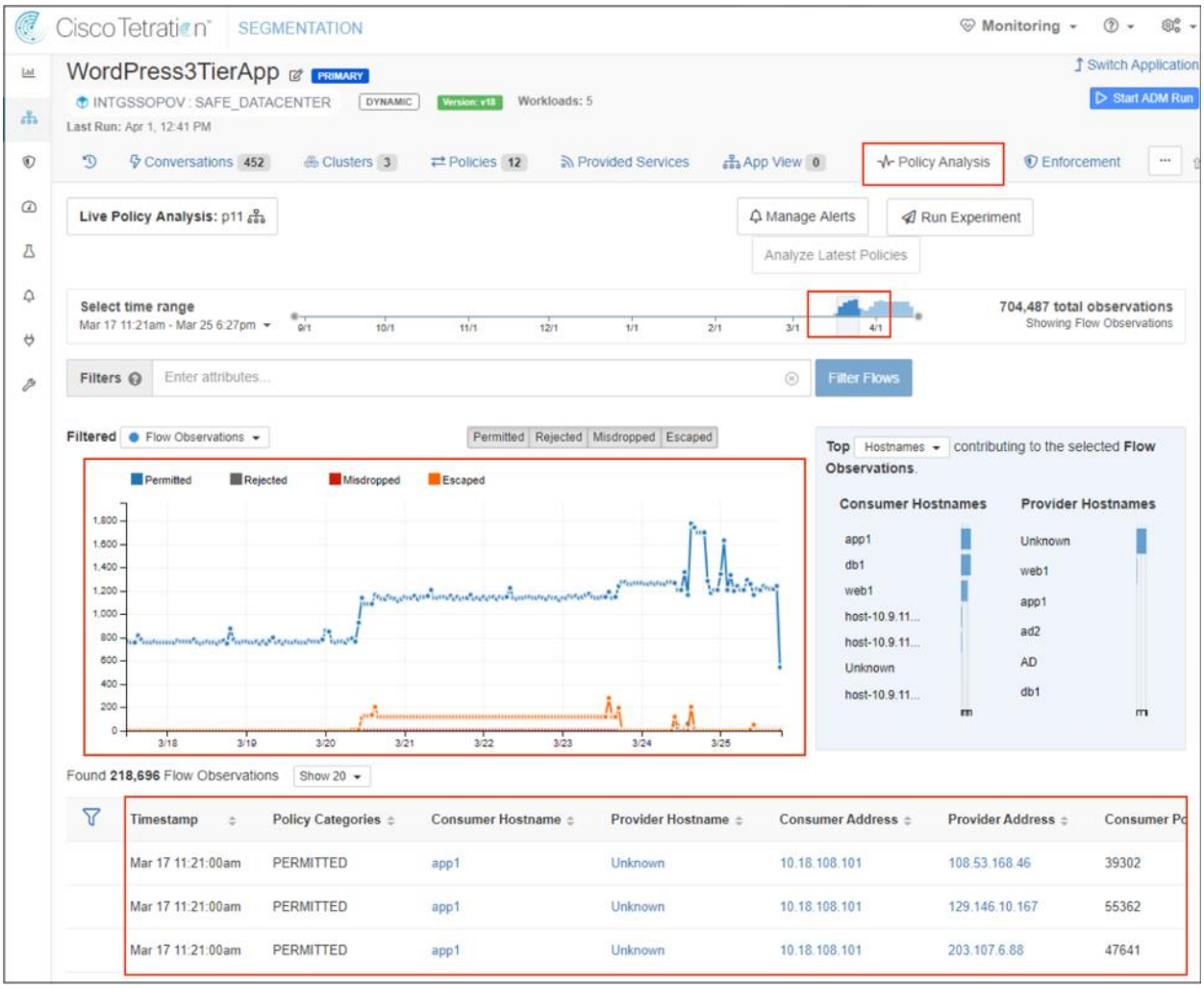
Step 11 Testing

a. Before deploying the policies to the clusters, run the Policy Analysis. The analysis applies the new policies to new and incoming flows and provide the results. The user may also choose to run an experiment against historical data. Based on the analysis results, the user can modify the polices as needed prior to deployment.

b. Make the workspace Primary by clicking on SECONDARY.

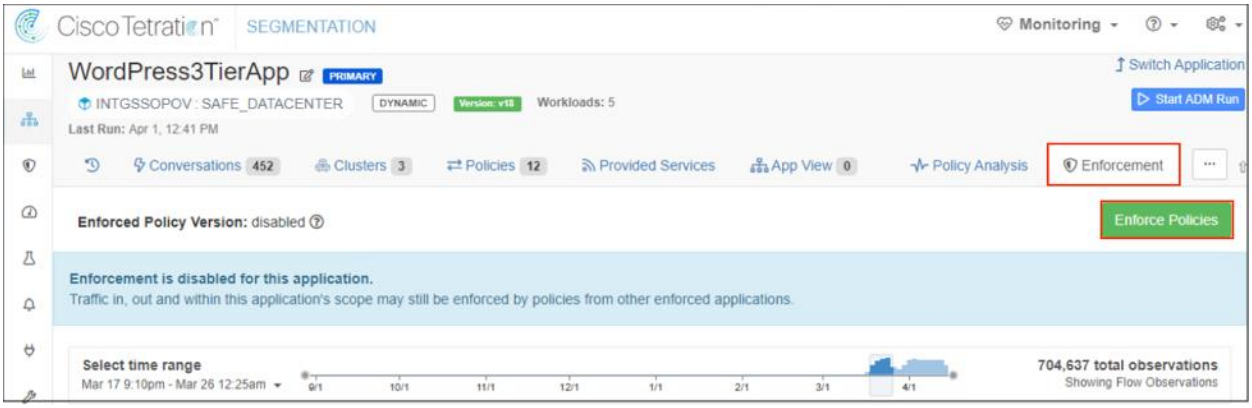


c. Click Policy Analysis tab and select a Time Range to apply the policies. The results are displayed below.

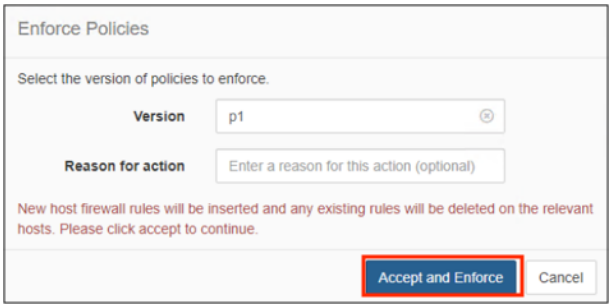


Return to Contents

d. The policies are ready for deployment. Select the **Enforcement** tab and click **Enforce Policies**.



e. Select the policy version and click **Accept and Enforce**.



The policy push completes in 1 or 2 minutes, then the new rules appear on the endpoints firewall.

Test Case 9 – Cisco TrustSec, ISE, APIC and FMC

Cisco TrustSec uses tags to represent logical group privilege. This tag is a Security Group Tag (SGT) and is used in access policies referred to as Security Group Access Control Lists (SGACL). The SGT is used to enforce traffic by Cisco switches, routers and firewalls. Cisco TrustSec is defined in three phases, classification, propagation and enforcement. When users and devices connect to your network, the network assigns a specific source SGT for their traffic. This process is called classification. Classification can be based on the results of authentication or by associating the SGT with an IP, VLAN, or port-profile. Once user traffic is classified, the SGT is propagated from where classification took place, to where enforcement action is invoked. This process is called propagation.

Cisco TrustSec has two methods of SGT propagation, inline tagging or Security Group Exchange Protocol (SXP). With inline tagging, the SGT is embedded into the ethernet frame. The ability to embed the SGT within an ethernet frame does require specific hardware support. Therefore, network devices that do not have the hardware support can use the SXP protocol. SXP is used to share the SGT to IP address mapping on the path to the destination. This allows the SGT propagation to continue to the next device in the path.

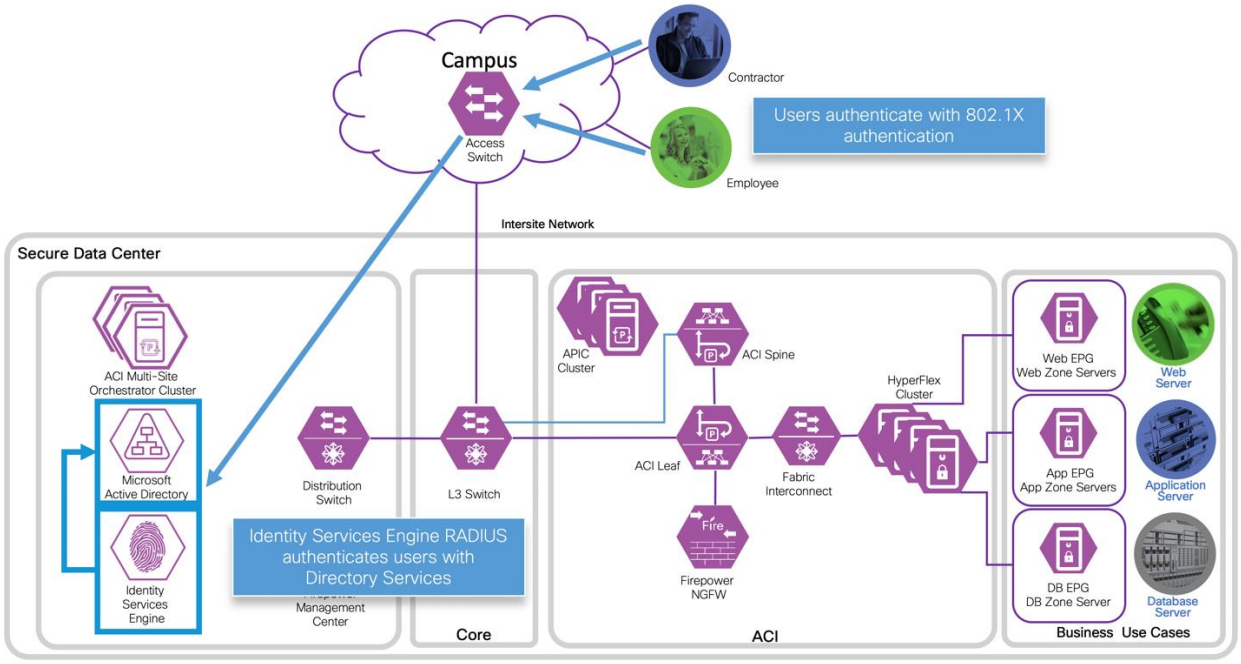
Finally, an enforcement device controls traffic based on the tag information. A TrustSec enforcement point can be a Cisco firewall, router or switch. The enforcement device takes the source SGT and looks it up against the destination SGT to determine if the traffic should be allowed or denied. The Cisco TrustSec policy manager is the Identity Services Engine (ISE).

Devices not capable of Cisco TrustSec can subscribe to Cisco Platform Exchange (pxGrid) to propagate SGTs. pxGrid is an open and scalable Security Product Integration Framework (SPIF) that enables ecosystem partners to exchange contextual information unidirectionally or bidirectionally. Cisco pxGrid uses a secure and customizable publisher/subscriber model, enabling partners to publish and/or subscribe securely only to topics relevant to their platform. Cisco pxGrid is a component of the Identity Services Engine (ISE).

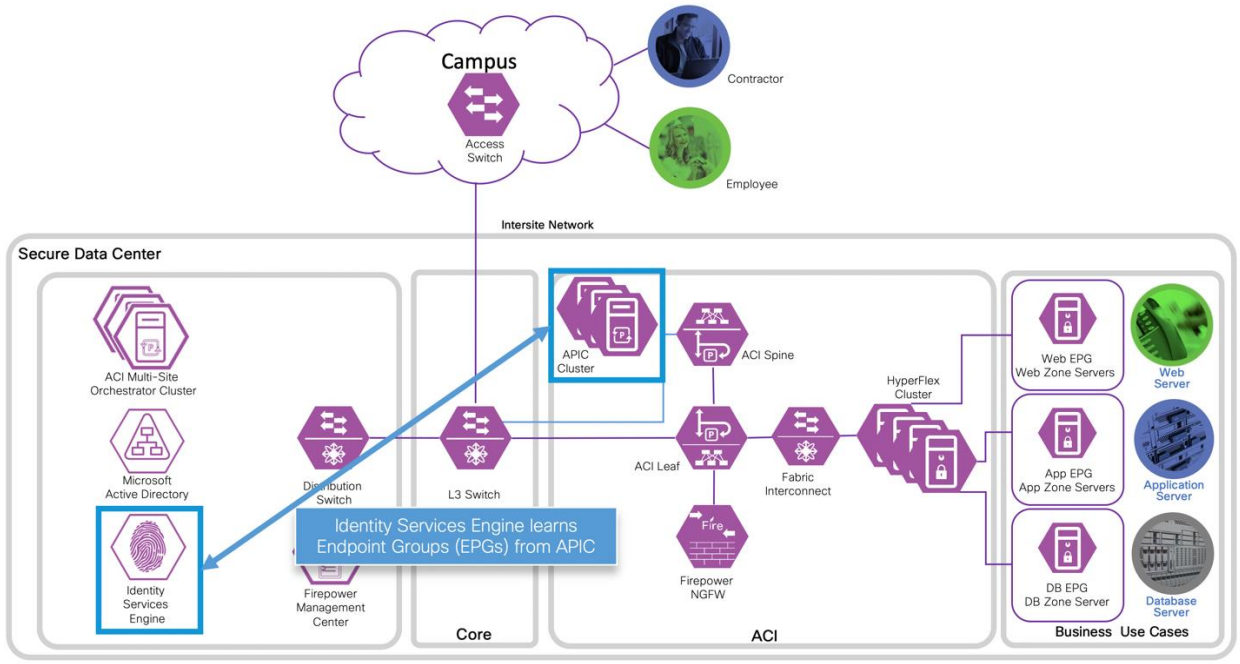
In this test case, Firepower Management Center (FMC) and the Firepower Thread Defense (FTD) is the access policy enforcement point for the workloads in the ACI Data Center. By enabling the ISE and ACI integration, ISE learns the ACI Endpoint Groups (EPGs) and creates the corresponding SGTs. FMC subscribes to pxGrid and learns the SGTs. The SGTs are used as source and destination in access policies and deployed to the FTD cluster.

Test Description:

1. ISE is integrated with Directory Services and provides network access control via RADIUS. Endpoints are authenticated using the 802.1X protocol at the point of access. ISE updates pxGrid subscribers with the login information.

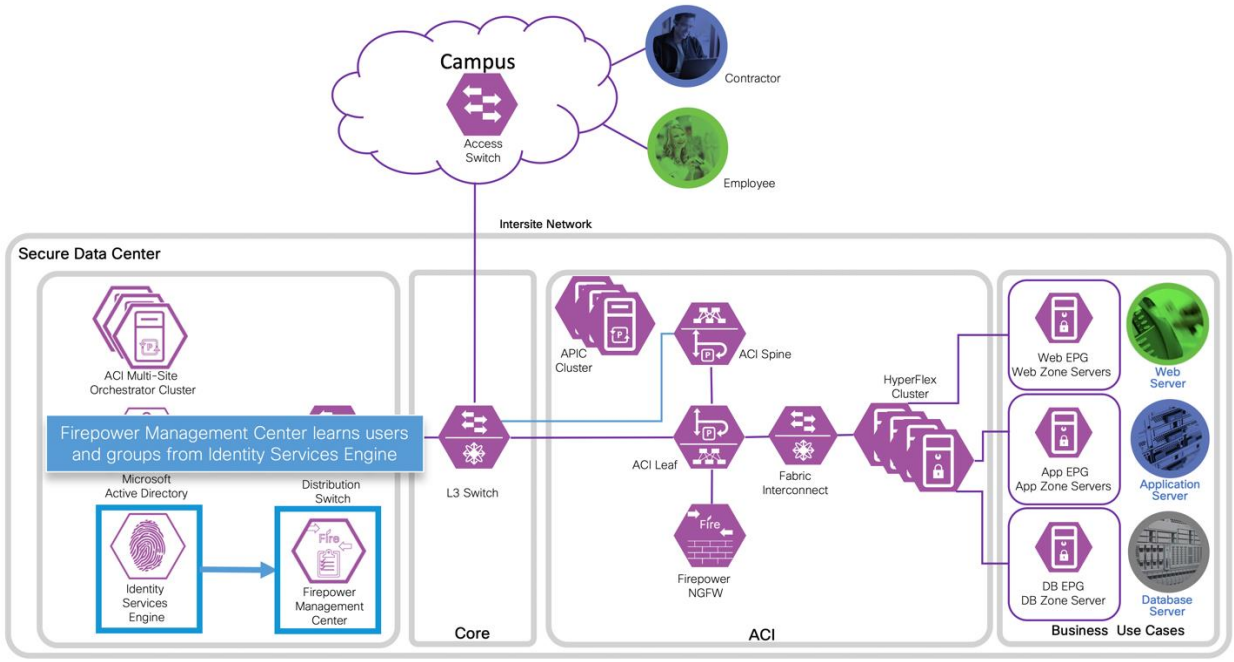


2. ISE and ACI are integrated and exchange SGTs and EPGs. ISE creates a corresponding SGT for each EPG. ACI also creates a corresponding EPG for each SGT.

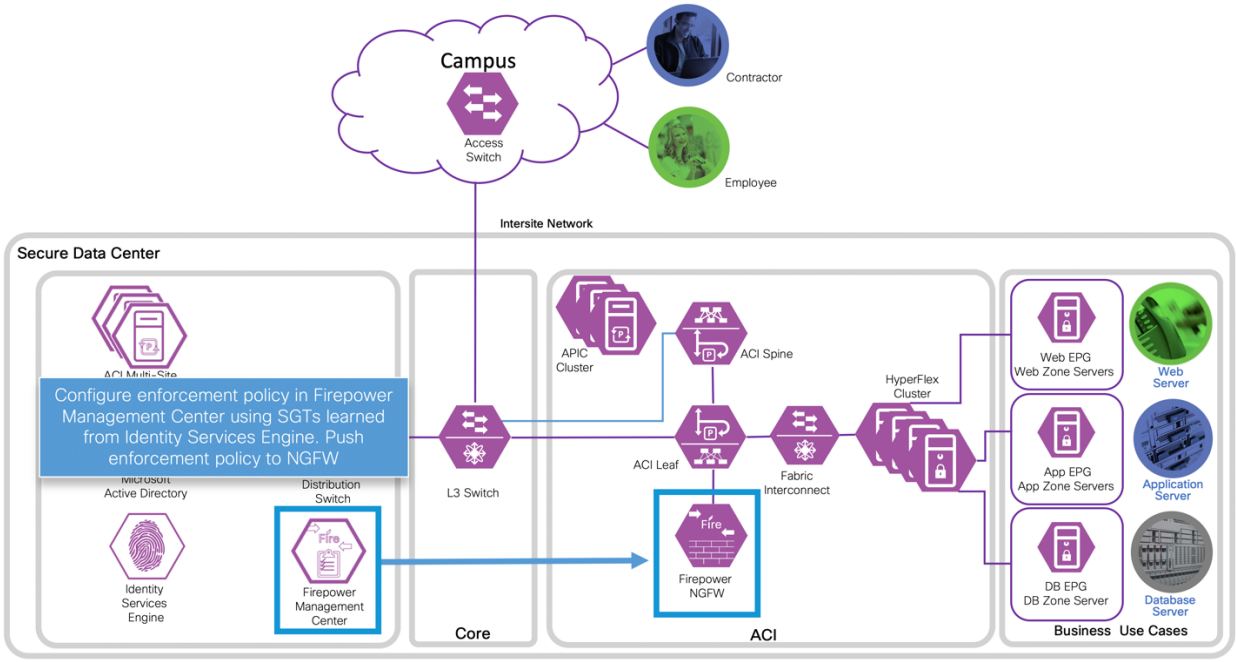


Return to Contents

3. FMC integrates with ISE through pxGrid. FMC subscribes to pxGrid topics and receive ISE SGT updates.

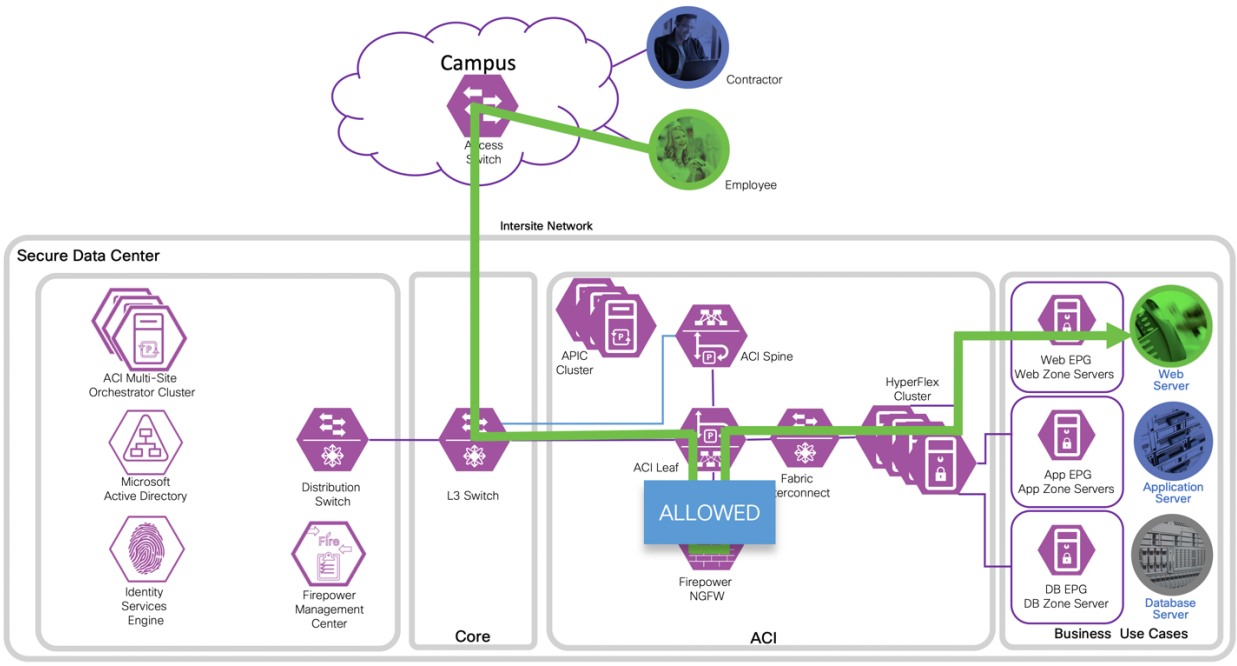


4. The SGTs are used in FMC access policy rules and are deployed to the FTD. When endpoints move within the network, FMC is updated by pxGrid with the endpoint latest metadata (e.g. IP address). FMC updates Firepower NGFW with no manual change to the access policy is required.

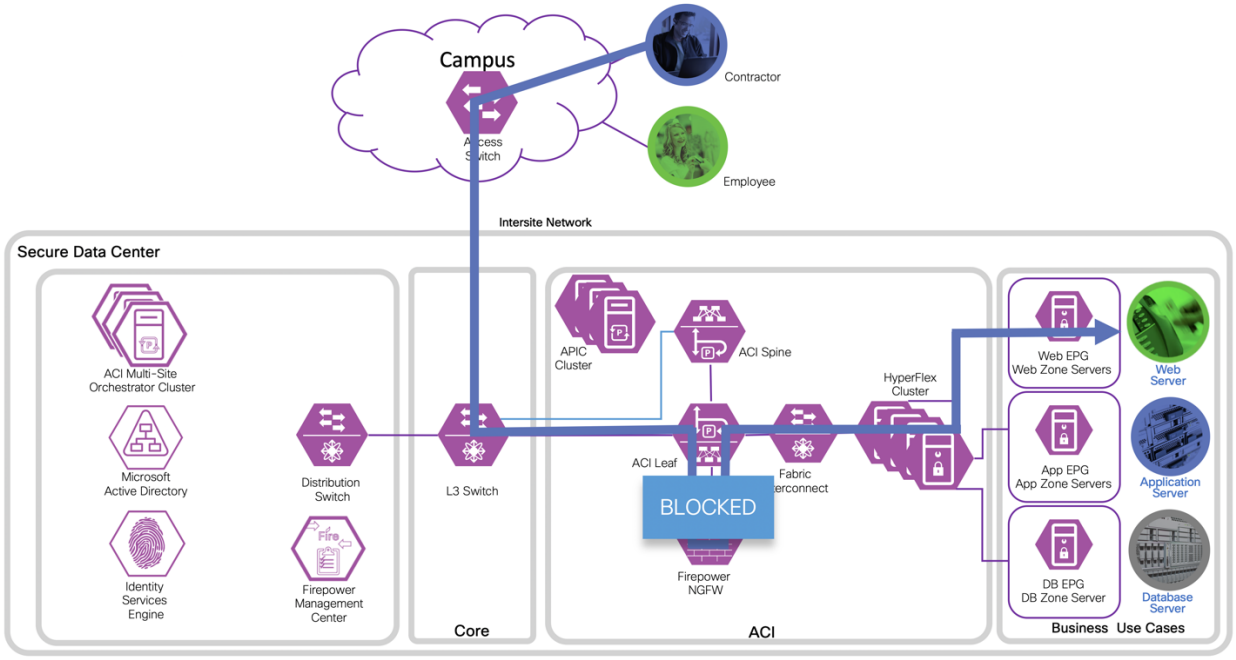


Return to Contents

5. An access control policy rule permits endpoints with the Employee SGT access to the web server.



6. Another rule denies endpoints with the Contractor SGT access to the web server.



Return to Contents

Implementation Procedure

Prerequisites

1. Access switch is configured for 802.1X authentication and ISE as the RADIUS server
2. Microsoft Active Directory (AD) is configured as an ISE External Identity Source
3. The Microsoft Active Directory Services (AD CS) is the Certificate Authority for the environment

Procedure

Step 1 Configure FMC and ISE Integration
Step 2 Configure ACI for ISE Integration
Step 3 Configure ISE for ACI Integration
Step 4 Create an FMC Access Control Policy
Step 5 Test Results

Step 1 Configure FMC and ISE Integration

For the FMC and ISE integration, we followed the guide **How to Integrate Firepower Management Center 6.0 with ISE and Trustsec through pxGrid**. The guide was based on FMC 6.0 and ISE 2.0 but the steps covered are applicable to FMC 6.6 and ISE 2.7.

The guide can be found at:
https://community.cisco.com/t5/security-documents/how-to-integrate-firepower-management-center-fmc-6-0-with-ise/ta-p/3627024?attachment-id=157865

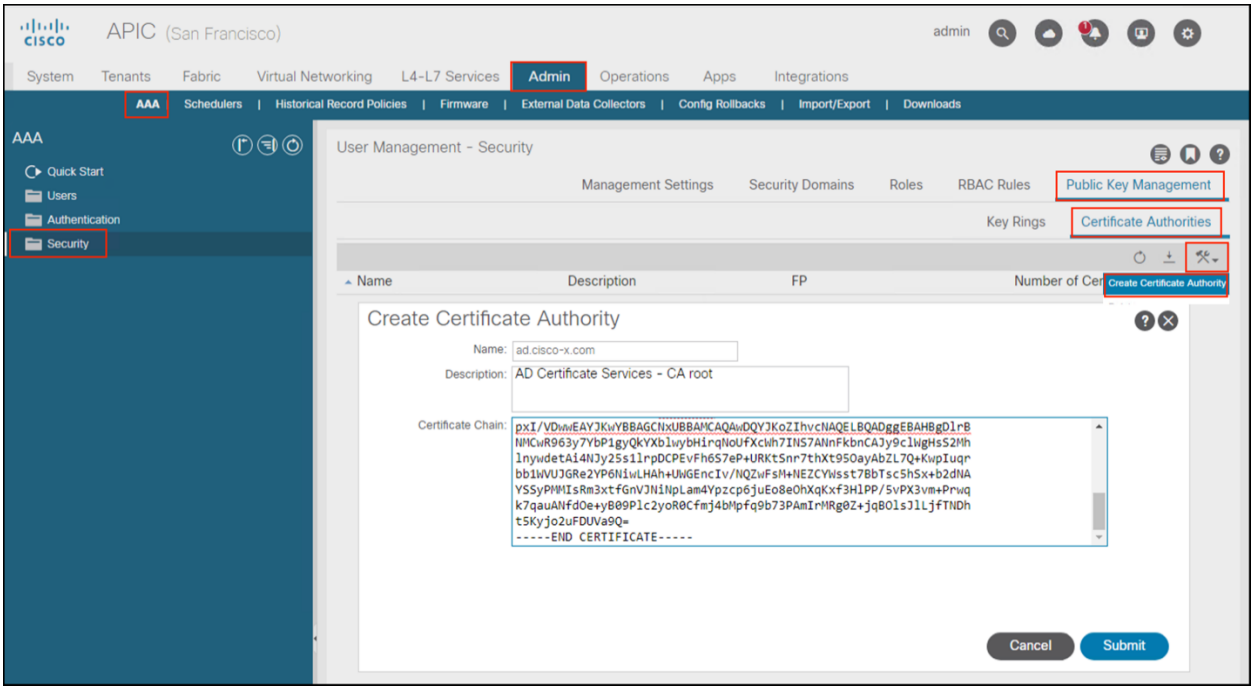
Summary of the steps we followed.

a. Create pxGrid template for CA-signed operations on the MS CS – page 22 steps 7-16
b. Create ISE security groups EmployeesSGT (SGT 4) and ContractorsSGT (SGT 5) and configure Authorization policies – page 9 steps 1 and 2
c. Export AD CS root certificate and import into ISE – page 27 steps 3-5
d. Generate ISE pxGrid certificate – page 27 steps 1, 2 and 6
e. Generate ISE Admin certificate – page 29 steps 7-15 and 20-25
f. Enable ISE pxGrid services - page 33 steps 26-30
g. Configure FMC ISE Realm – page 34 steps 1-13
h. Generate FMC certificates page 36 steps 1-10
i. Configure FMC Identity Sources page 39 steps 1-4
j. Enable FMC Network Discovery page 42 steps 1-3
k. FMC Identity Policy page 42 steps 1-6
l. FMC Default Access Control Policy page 43 steps 1-3
m. FMC Transport/Network Layer Preprocessor Settings page 44 steps 1-3

Step 2 Configure ACI and ISE

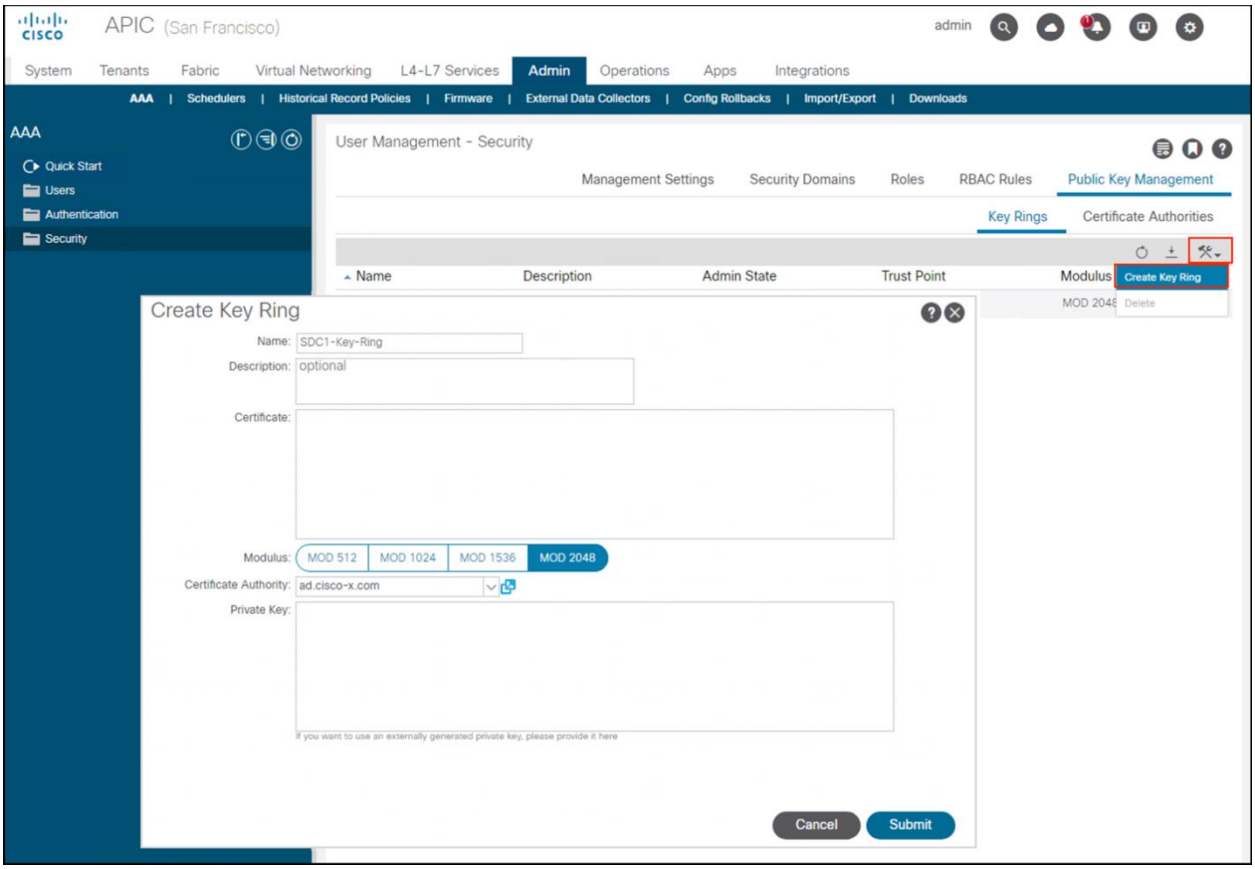
a. Import the AD CS root CA certificate into APIC.

1. From the APIC management portal Choose **Admin > AAA > Security > Public Key Management Certificate Authorities > Action > Create Certificate Authority**
2. Complete the **Create Certificate Authority** configuration and click **Submit**
   Required fields:
   - Name:
   - Certificate Chain: Open the root CA certificate from step 1c. and copy the content into the text box



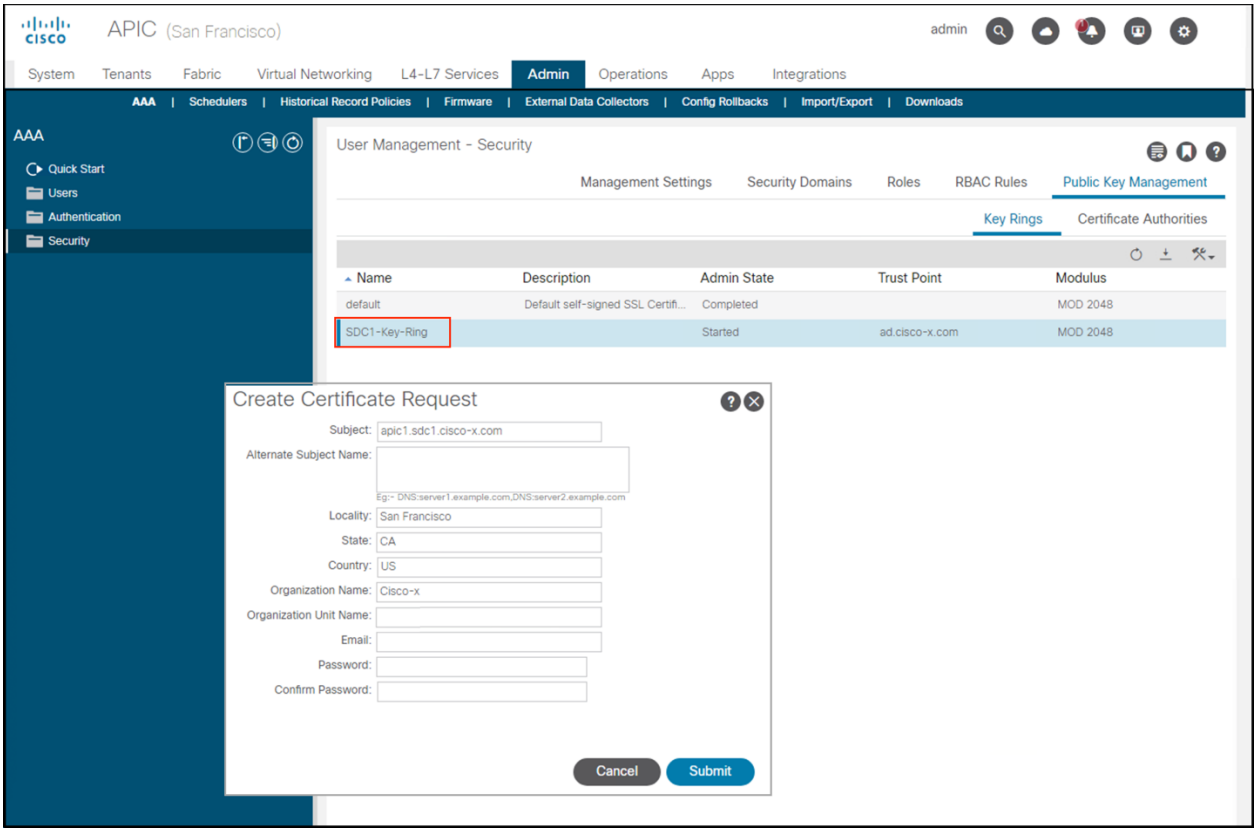
Return to Contents

b. Create a Key Ring
   1. Click in **Action > Create Key Ring**
   2. Complete the Create Key Ring configuration and click **Submit**
      Required fields:
      - Name:
      - Modulus:
      - Certificate Authority: Choose the CA created in step *a*.



Return to Contents

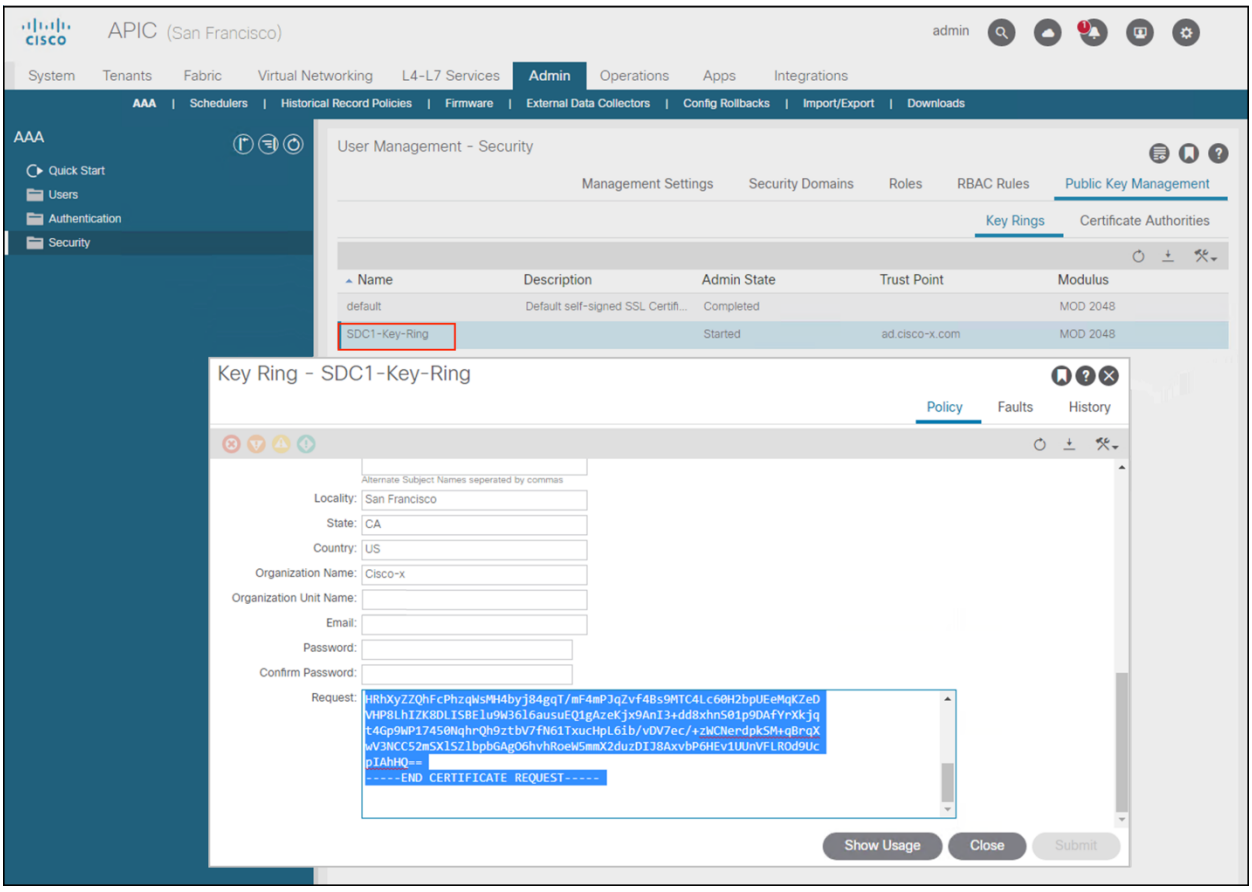
c. Generate a Certificate Signing Request (CSR)
   1. Double click the created key ring
   2. Complete the CSR configuration and click **Submit**
      Required fields:
      - Subject: enter the *<APIC FQDN>*
      - Locality:
      - State:
      - Country:
      - Organization Name:



Return to Contents

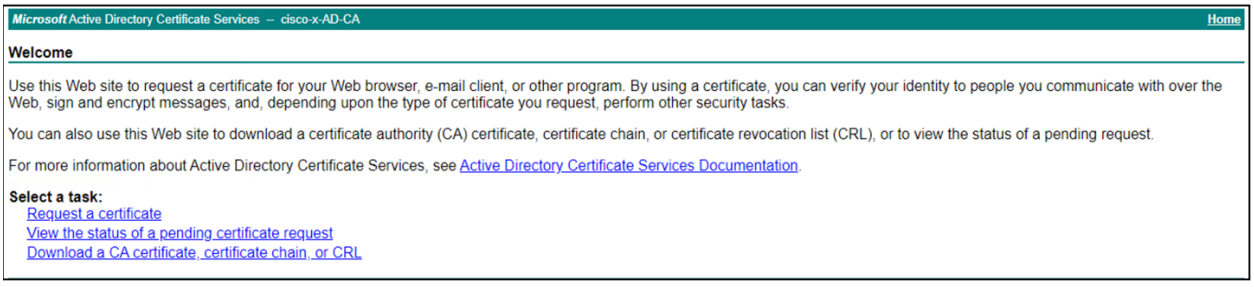
3. Double click the created key ring. This time, the Request box is populated with the certificate request.

4. Select and copy the certificate request

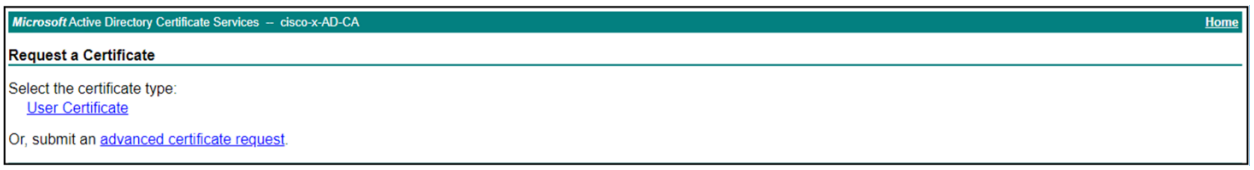


d. Sign the CSR

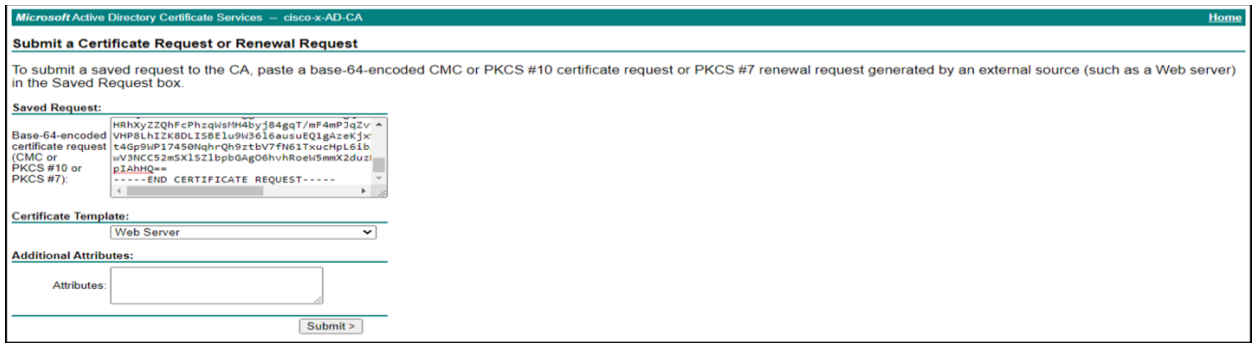
1. Navigate to the Certificate Authority server and choose **Request a Certificate**



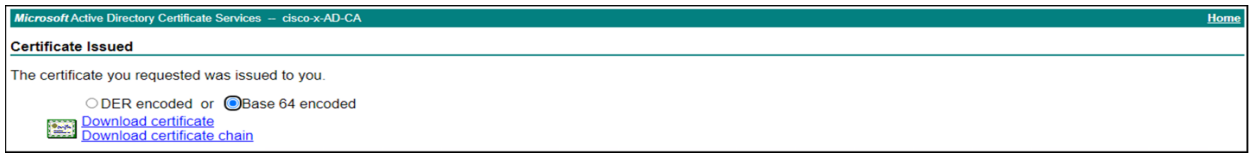
2. Choose the **Advanced Certificate Request**



3. Paste the certificate request into the **Saved Request** box. From the **Certificate Template** drop-down menu, choose **Web Server** and click **Submit**.

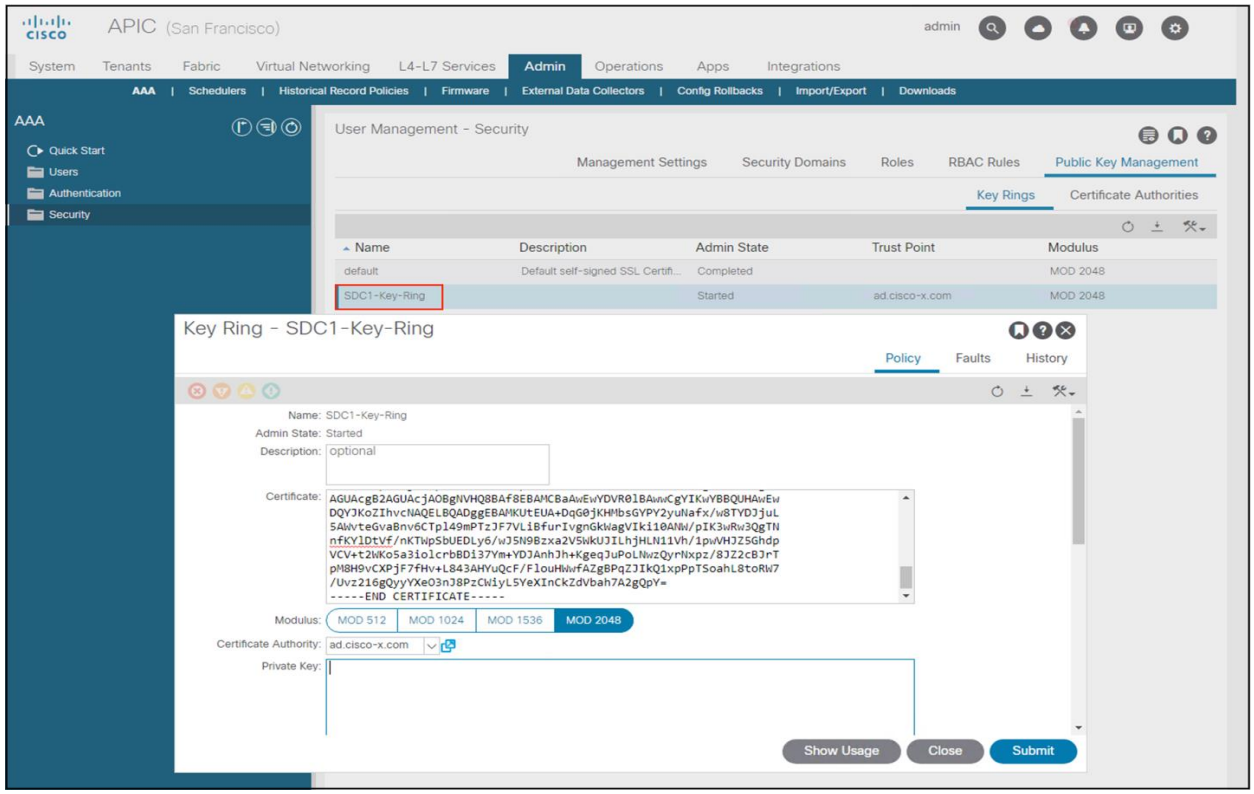


4. Choose **Base 64 encode** and **Download Certificate**



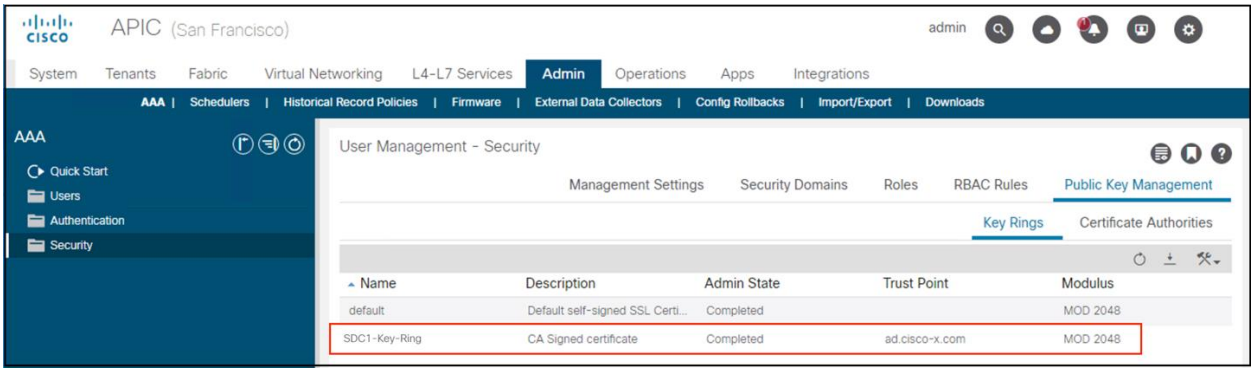
5. Save the certificate to your local machine

e. Bind the signed certificate to the CSR
   1. Open the certificate in a text editor and copy the content
   2. On the APIC, double click the key ring
   3. Paste the content into the certificate box
   4. Choose the Certificate Authority previously created and click **Submit**

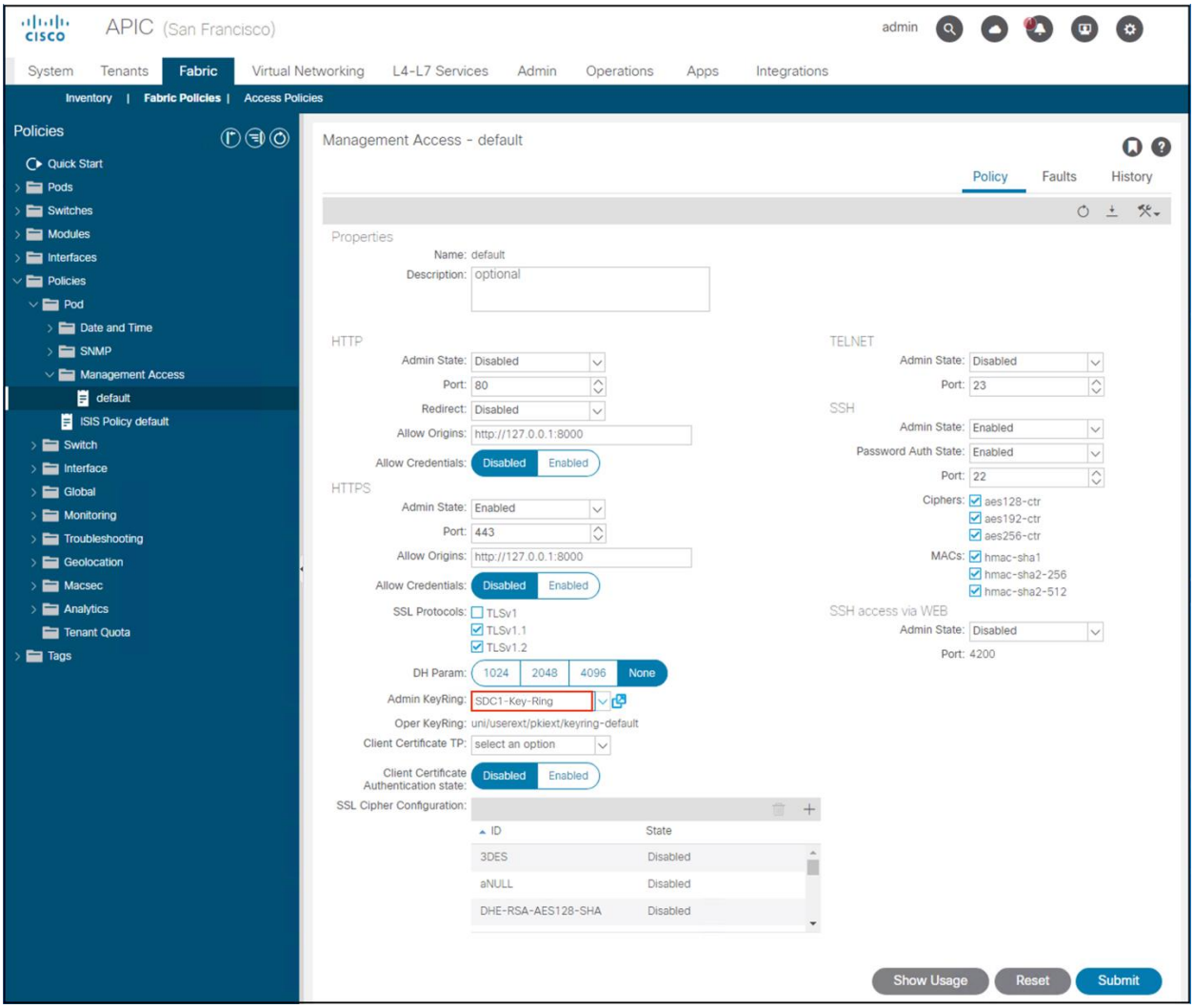


Return to Contents

5. Verify the key ring has changed state from **Started** to **Complete**



f. Apply the key ring to HTTP policy
   1. Navigate to **Fabric > Fabric Policies > Policies > Pod > Management Access > Default**
   2. Change the Admin KeyRing to the one created and click **Submit**



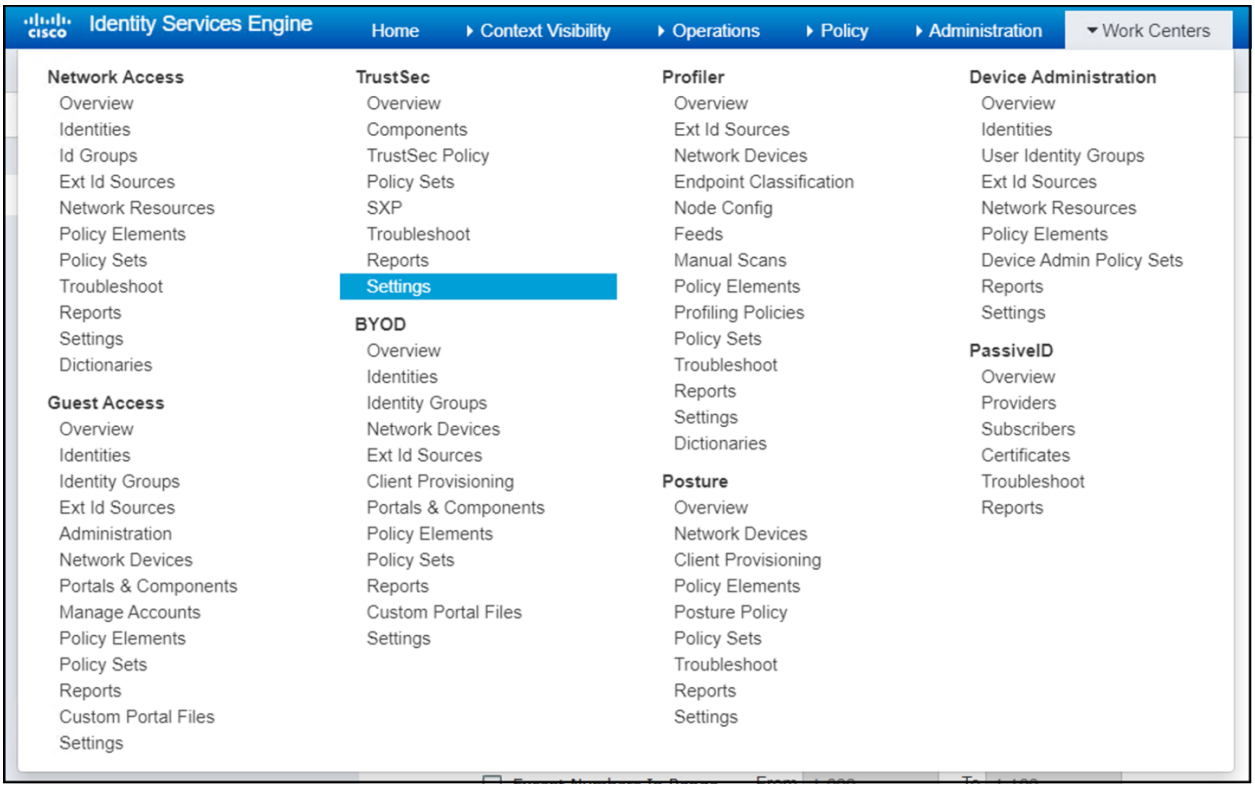
Return to Contents

278

Step 3 Configure ISE for ACI Integration

a. Enable ACI Integration

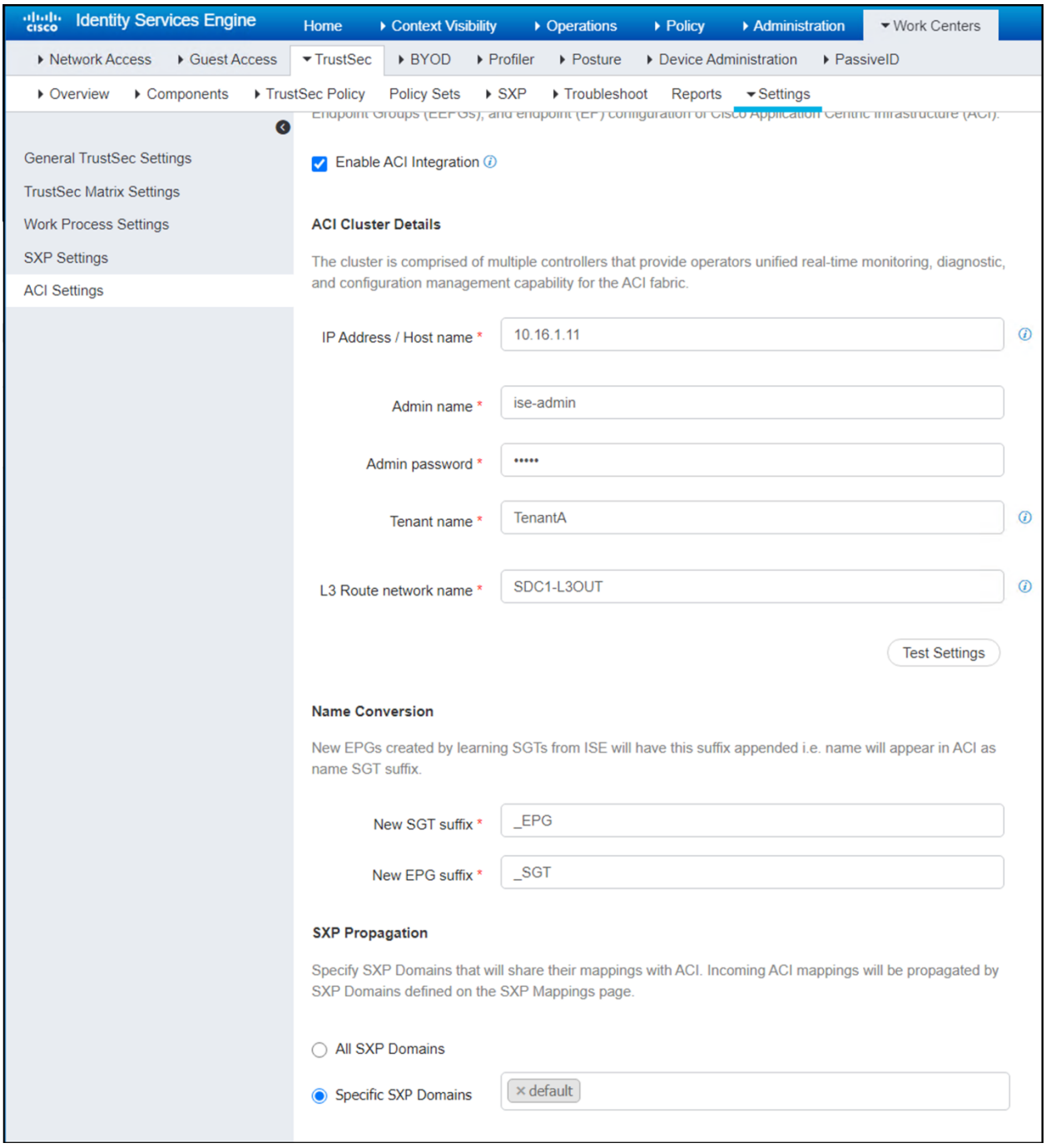
1. From the ISE management portal, navigate to **Work Centers > TrustSec > Settings**



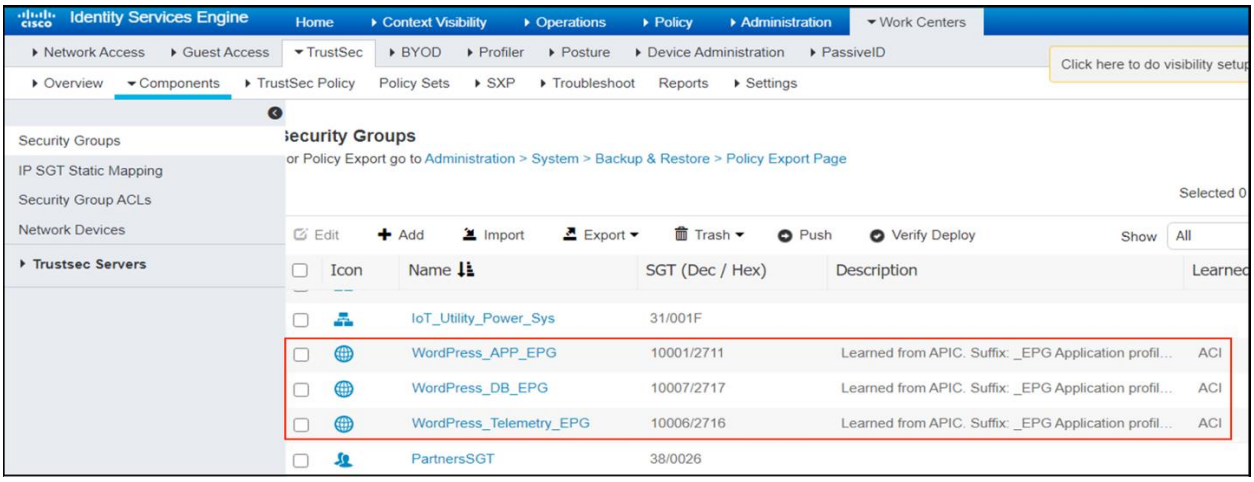
Return to Contents

2. In the Navigation Pane, choose **ACI Settings**
   a. Complete the **ACI Cluster Details** configuration
   b. Click **Test Settings** to verify the connection to ACI

   Under the Name Conversion section, note the SGT and EPG suffixes

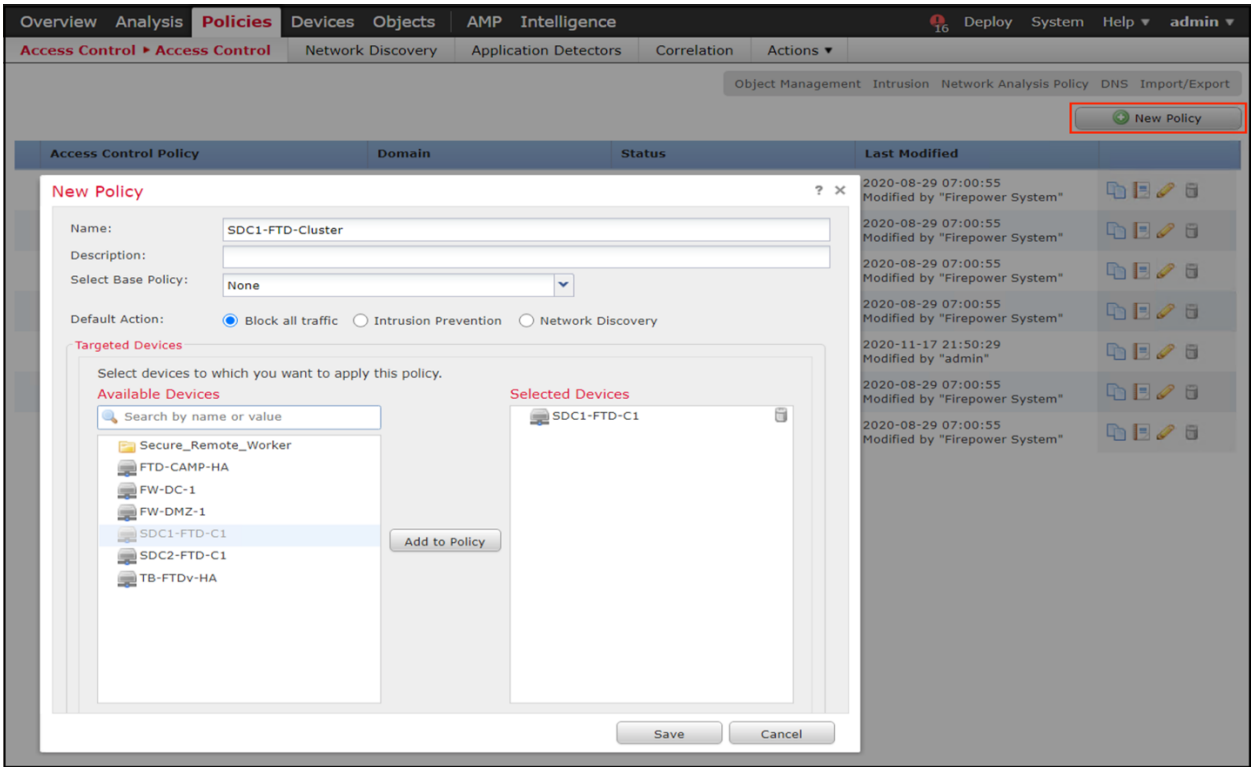


c. Verify ISE has received the EPG data. The security groups created from the ACI EPGs are appended with the suffix in the previous step.

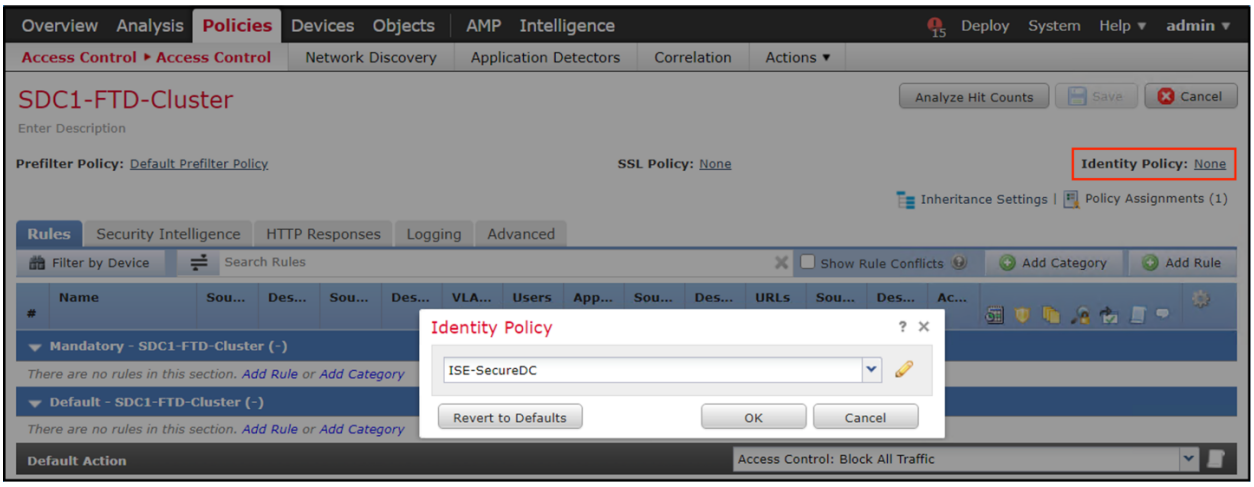


Step 4 Create an FMC Access Control Policy

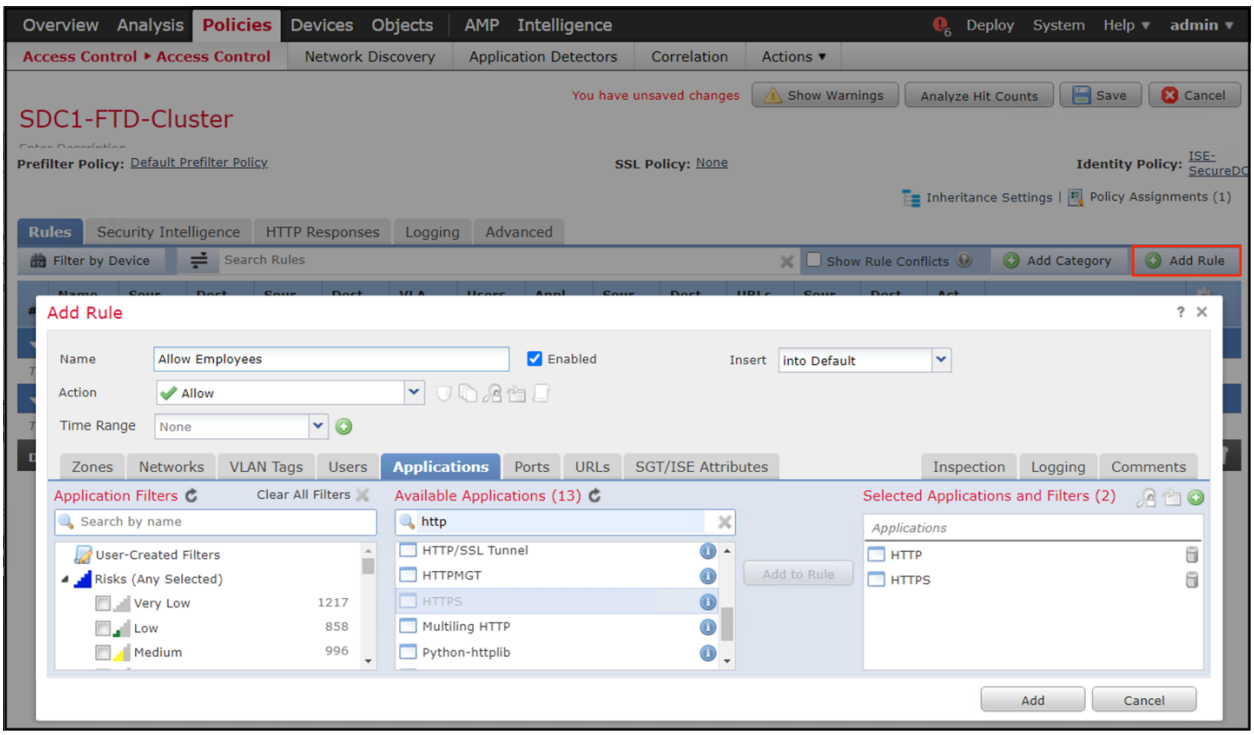
a. Create an Access Control Policy
   1. Click **Policies > Access Control >Access Control** and click **+New Policy**
   2. Complete the New Policy configuration and click **Save**
      Required fields:
      Name:
      Choose Base Policy: **None**
      Default Action: **Block all traffic**
      Target Devices: *<FTD Appliance>*
   3. click **Save**



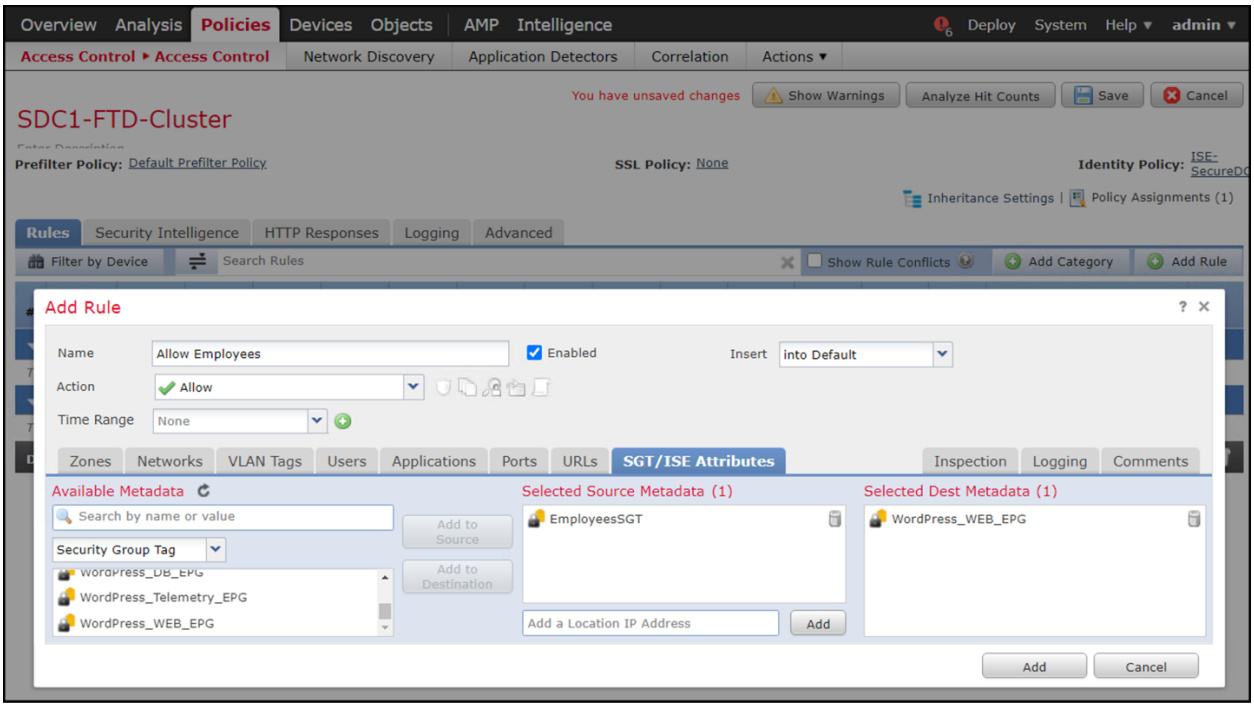
b. Assign an Identity Policy
   1. Click on the **Identity Policy: None**
   2. In the pop-up window, choose the Identity Policy previously created from the drop-down menu



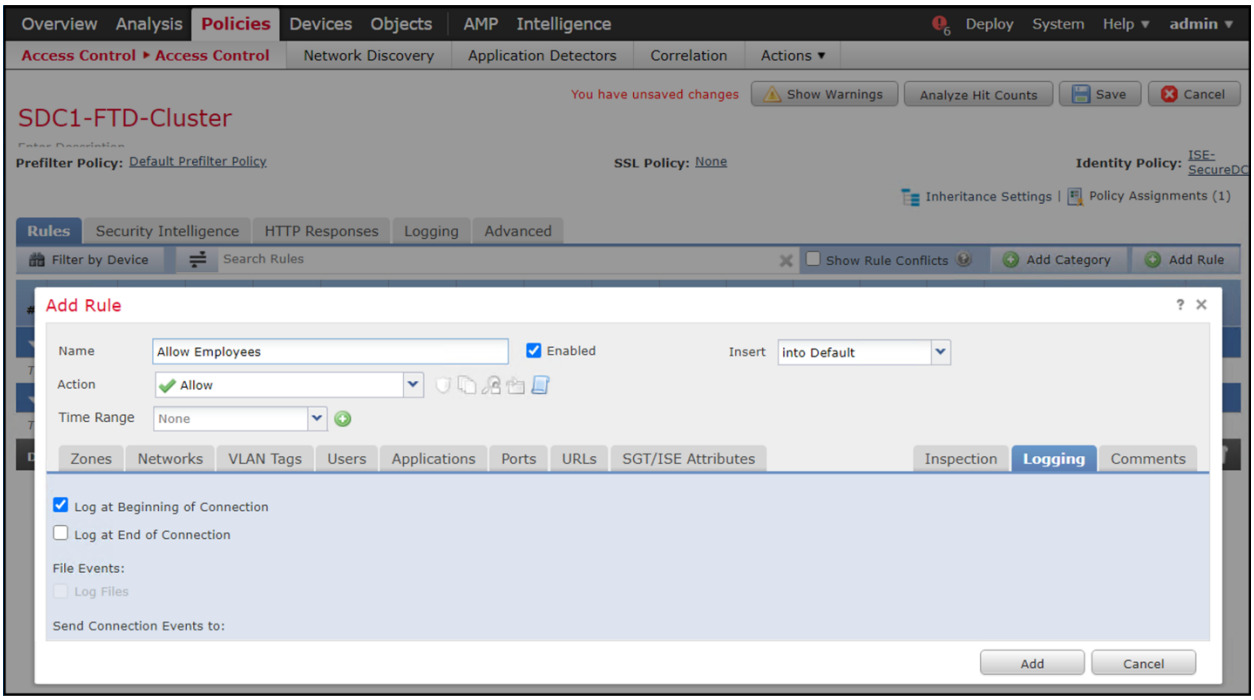
c. Add a rule
   1. Click **+Add Rule**
   2. In the pop-up window, enter the configuration for the new rule
      Name: < Name>
      Action: Allow
      Time Range: None
   3. Choose the **Applications** tab, Choose **HTTP** and **HTTPS** under **Available Applications** and click **Add to Rule**



4. Choose the **SGT/ISE Attributes** tab. Under **Available Metadata**, choose **Security Group Tag** in the drop-down menu. Choose the source and click **Add to Source**. Repeat the step to add the destination.

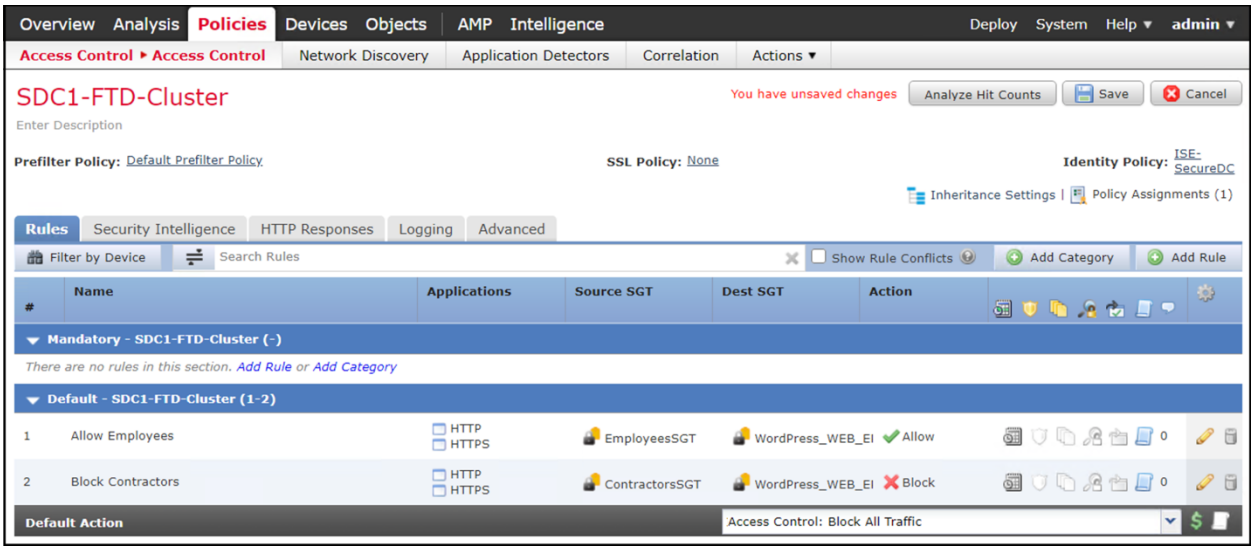


5. Choose the Logging tab and check the box **Log at Beginning of Connection** and click **Add**



Return to Contents

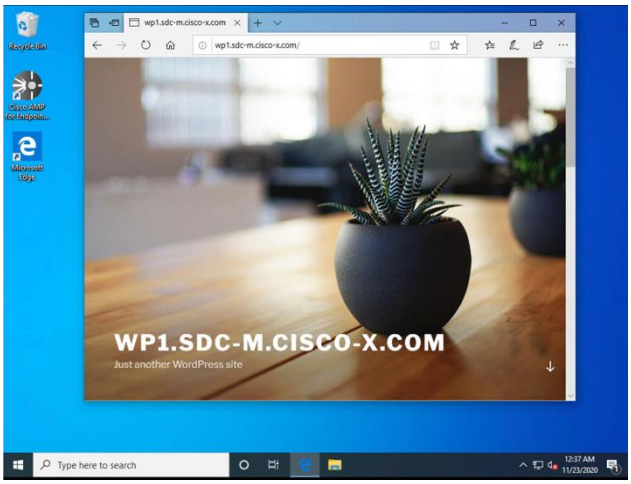
6. Repeat the steps to create a block rule for Contractors

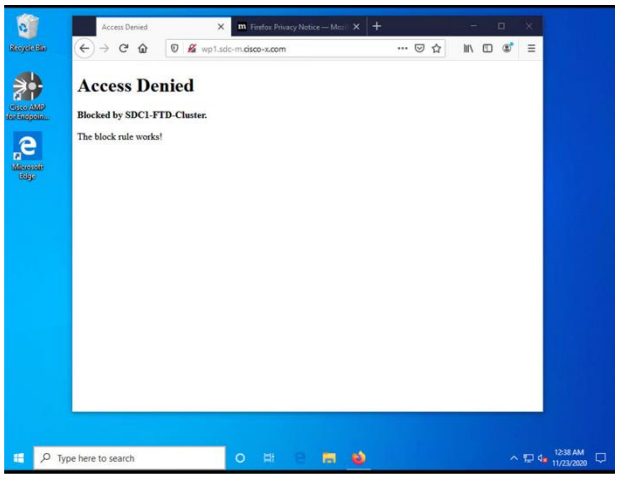


7. Click **Save** and **Deploy**

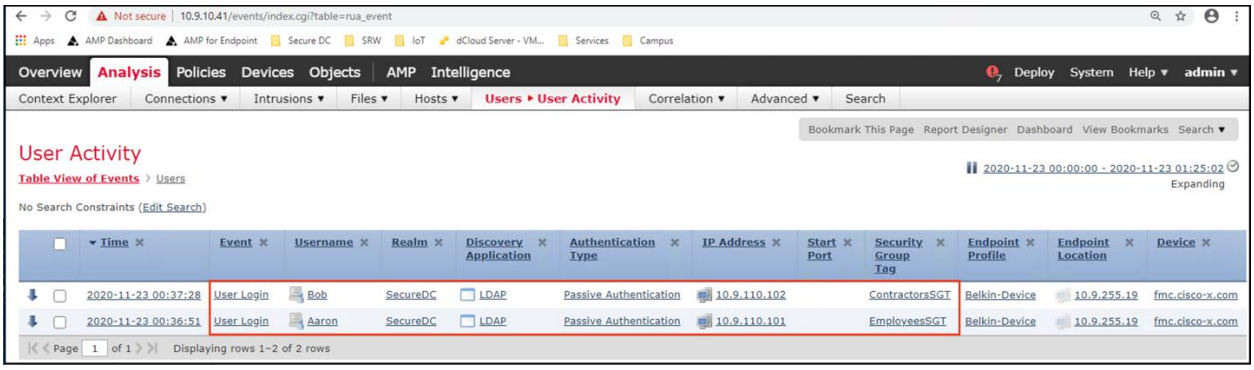
Step 5 Test Results

Two workstations log on the network. One user is in the employee group and the other in the contractor group. From a browser, each navigates to the web server. The employee (left) is permitted access and the contractor (right) is denied.

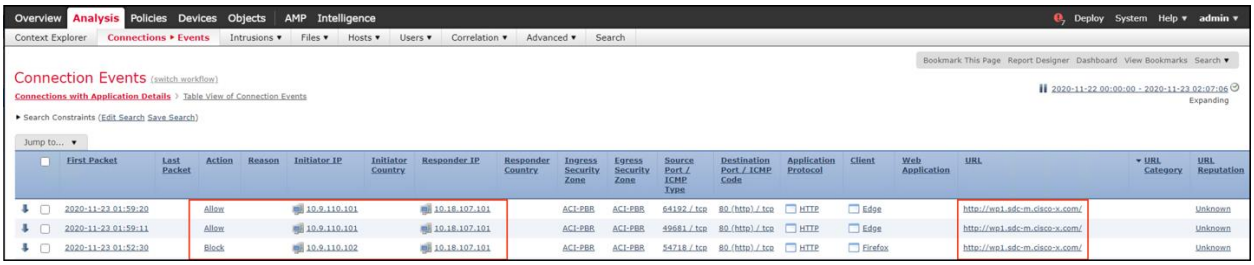




To view the users on FMC, click **Analysis > Users > User Activity**. Notice the SGT assigned to each user.



To view traffic, click **Analysis > Connections > Events**. The result is the user tagged as Employees are permitted access to the web server and the users tagged as Contractors are Denied.



Summary

Cisco helps data center teams consistently protect the workload everywhere through complete visibility and comprehensive multilayered segmentation. Our solutions provide integrated threat protection capabilities that keep your business more secure and your data center team more productive.

Return to Contents

References

Cisco SAFE Simplifies Security:

www.Cisco.com/go/safe

Cisco HyperFlex HX240c M5 Node and HX240c M5 All Flash Node

https://www.Cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/datasheet-c78-736784.pdf

Cisco Multi-Site ACI Architecture Whitepaper

https://www.Cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html

Cisco Application Centric Infrastructure Data Sheet

https://www.Cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-apic/datasheet-c78-732414.html

Cisco Application Centric Infrastructure Design Guide Whitepaper

https://www.Cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737909.html?cachemode=refresh

Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure Data Sheet

https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-729404.html

Cisco Nexus 9300-EX and 9300-FX Platform Leaf Switches for Cisco Application Centric Infrastructure Data Sheet

https://www.Cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-738259.html

Cisco Validated Design: Design and Deployment Guide for Cisco HyperFlex 3.0 with VMware vSphere 6.5U2, Cisco UCS Manager 3.2, Cisco ACI 3.2, and Cisco UCS 6300 Series Fabric Interconnects:

https://www.Cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/hx_30_vsi_aci_32.pdf

Cisco Stealthwatch:

http://www.Cisco.com/c/en/us/products/security/stealthwatch/index.html

Cisco Tetration Analytics

https://www.Cisco.com/c/en/us/products/data-center-analytics/tetration-analytics/index.html

Cisco Tetration Agent:

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Software_Agents.html

Cisco Advanced Malware Protection for Endpoints:

http://www.Cisco.com/c/en/us/products/security/fireamp-endpoints/index.html

Cisco Advanced Malware Protection:

http://www.Cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

Return to Contents

Cisco Talos - Comprehensive Threat Intelligence:

http://www.Cisco.com/c/en/us/products/security/talos.html

Cisco ThreatGrid:

http://www.Cisco.com/c/en/us/solutions/enterprise-networks/amp-threat-grid/index.html

Cisco Firepower Management Center:

http://www.Cisco.com/c/en/us/products/security/firesight-management-center/index.html

Cisco Firepower Next Generation Firewall:

https://www.Cisco.com/c/en/us/products/security/firewalls/index.html

Cisco Rapid Threat Containment Solution:

http://www.Cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html

Cisco Identity Services Engine:

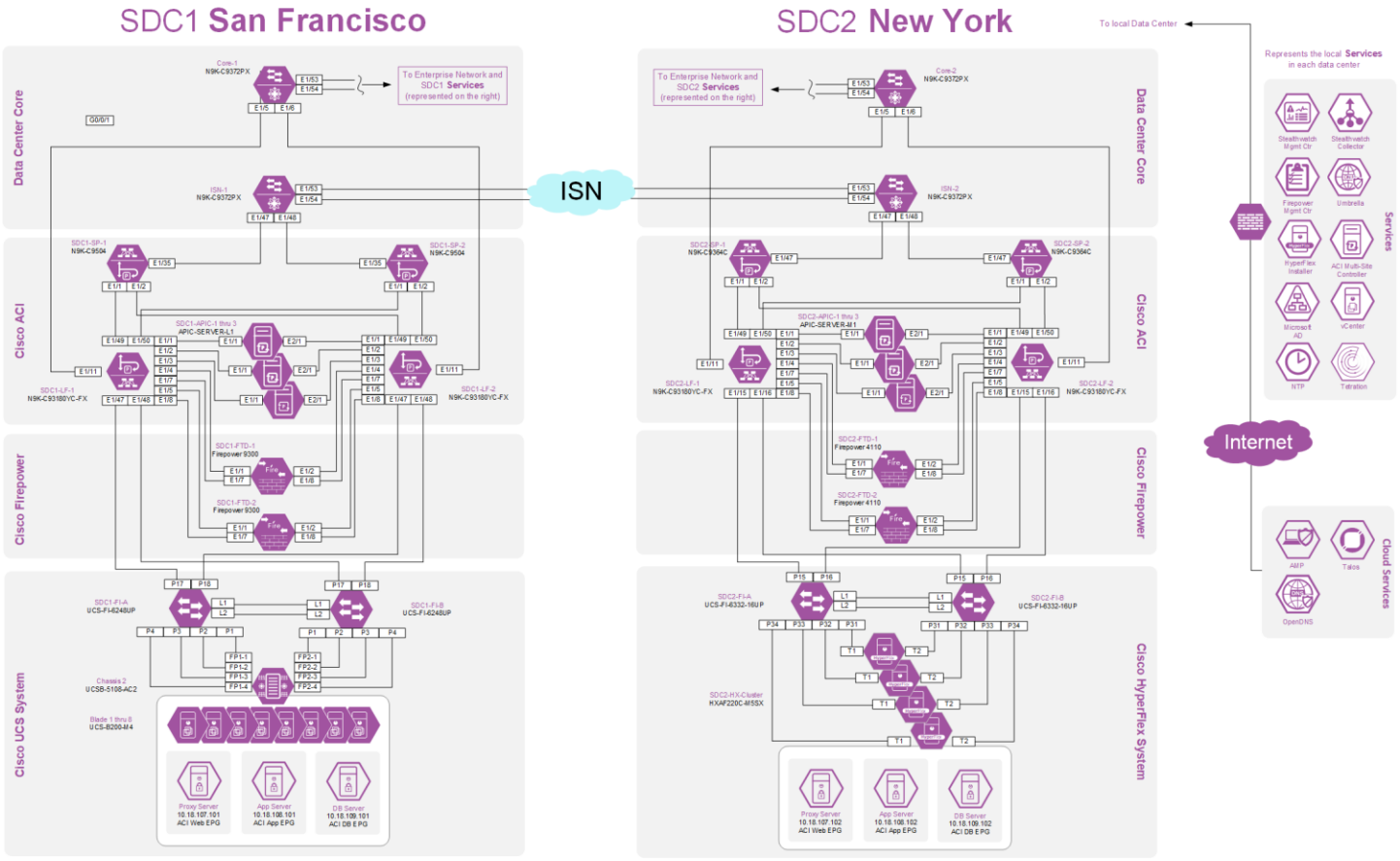
https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

Cisco TrustSec:

https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

Appendix A

Secure Data Center Lab Diagram



Return to Contents

Appendix B

Solution Products

The following products and versions were tested as part of the Secure Data Center solution.

Product	Description	Platform	Version
ACI Multi-Site Orchestrator	The Cisco ACI Multi-Site Orchestrator is responsible for provisioning, health monitoring, and managing the full lifecycle of Cisco ACI networking policies and stretched tenant policies across Cisco ACI sites around the world.	Set of 3 Virtual Machines	2.1(1i)
ACI Spines	N9K-9364C – Spine Standalone N9k-C9504-FM – ACU 2RU Chassis N9K-X9736C-FX: 100 Gigabit Ethernet Line Card	Appliance	14.1.(1j)
ACI Leafs	N9K-C93180YC-FX	Appliance	14.1(1j)
APIC	APIC is the unifying point of automation and management for the Application Centric Infrastructure (ACI) fabric	Set of 3 appliances	4.1(1j)
ACI Device Package for Firepower Threat Defense	APIC can orchestrate a device provisioning if a device package exists. We tested the device package in a Multipod scenario.	Software	V1.0.3
AMP for Endpoints (AMP4E)	AMP4E will be used on the application servers to provide Anti-Malware and Anti-Virus support	Software Agent	Windows Server 2016 Connector 6.1.7.10741
			Centos Linux 7.4 Connector 1.8.4.591
Firepower Management Center	Manages Firepower NGFW and NGIPS appliances.	Virtual or Appliance	V6.4.0

Return to Contents

Product	Description	Platform	Version
FMC – APIC Remediation Module for Rapid Threat Containment	The is a software package that must be downloaded from Cisco.com. It is imported into FMC and triggered when FTD detects an attack. A notification to quarantine the infected server is sent to APIC.	Software	V1.0.3.13
FMC – Tetration Remediation Module for Rapid Threat Containment	This is a software package that must be downloaded from Cisco.com. It is imported into FMC and triggered when FTD detects an attack. A message to quarantine the infected server is sent to the Tetration agent running on the server.	Software	V1.0.2
Firepower Next Generation Firewall	Firepower NGFW provides unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint. Physical and virtual appliances are available.	Virtual, FP4110, FP9300	V6.4.0
Hyperflex	Cisco HyperFlex HX240c M5 All Flash Node - HXAF240C-M5SX – with Self Encrypting Drives.	Appliance	V4.0(1a)
Identity Services Engine	ISE is a holistic approach to network access security. It provides network visibility and uses multiple mechanism to enforce policy, including Cisco TrustSec software-defined segmentation.	Virtual	V2.7.0.356
Stealthwatch Management Console	The Stealthwatch Management Console aggregates, organizes, and presents analysis from up to 25 Flow Collectors, the Cisco Identity Services Engine, and other sources. It uses graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis.	Virtual	V7.0
Stealthwatch Flow Collector	The Flow Collector leverages enterprise telemetry such as NetFlow, IPFIX and other types of flow data from existing infrastructure such as routers, switches,	Virtual	V7.0

⮌ Return to Contents

Product	Description	Platform	Version
	firewalls, endpoints and other network infrastructure devices.		
Tetration Analytics Appliance	Cisco Tetration offers holistic workload protection for multicloud data centers by enabling a zero-trust model using segmentation.	Appliance	3.3.2.2-PATCH-3.3.2.16 (TaaS)
Tetration Agent	Server based agent for sending analytics and for host based enforcement.	Software Agent	Window Server 2016 Agent: 3.3.2.16.win64-enforcer
			CentOS Linux 7.4 Agent: 3.3.2.16-enforcer
Tetration Edge Virtual Appliance	Tetration Edge is a control appliance that streams alerts to various notifiers and collects inventory metadata from network access controllers such as Cisco ISE. In a Tetration Edge appliance, all alert notifier connectors (such as Syslog, Email, Slack, PagerDuty and Kinesis) and ISE connector can be deployed.	Virtual	3.3.2.2
VMware vCenter	VMware vCenter is a virtual machine manager for VMware vSphere environments	Virtual	v6.7

Return to Contents

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Return to Contents