



SAFE Design Guide

Places in the Network: Secure Data Center
Cisco ACI Multi-Site Reference Design

December 2020



Contents

4	Introduction
	Revision History 6
	Data Center Business Flows 6
	Data Center Attack Surface 7
8	Solution Overview
	Security Capabilities 9
12	Solution Architecture
	Visibility 13
	Segmentation 14
	Threat Protection 15
	Cisco Secure Data Center Reference Architecture 16
20	Implementation
	ACI 23
	ACI Multi-Site 26
	HyperFlex 28
	Firepower Next Generation Firewall 31
	Stealthwatch 33
	Tetration 34
	Advanced Malware Protection 36
	Identity Services Engine (ISE) 37
	Platform Exchange Grid (pxGrid) 37
38	Validation Testing
	Test Case 1 – ACI Multi-Site Orchestrator and Firepower Threat Defense 39
	Test Case 2 – Firepower Management Center and APIC 132
	Test Case 3 – Tetration and VMware vCenter 151
	Test Case 4 – Stealthwatch and Tetration 176
	Test Case 5 – AMP and Firepower Threat Defense 198
	Test Case 6 – FTD Rapid Threat Containment and APIC 207
	Test Case 7 – FTD Rapid Threat Containment with Tetration 222
	Test Case 8 – Tetration and Identity Services Engine 237

3

Test Case 9 - Cisco TrustSec, ISE, APIC and FMC 267

285 Summary

286 References

288 Appendix A

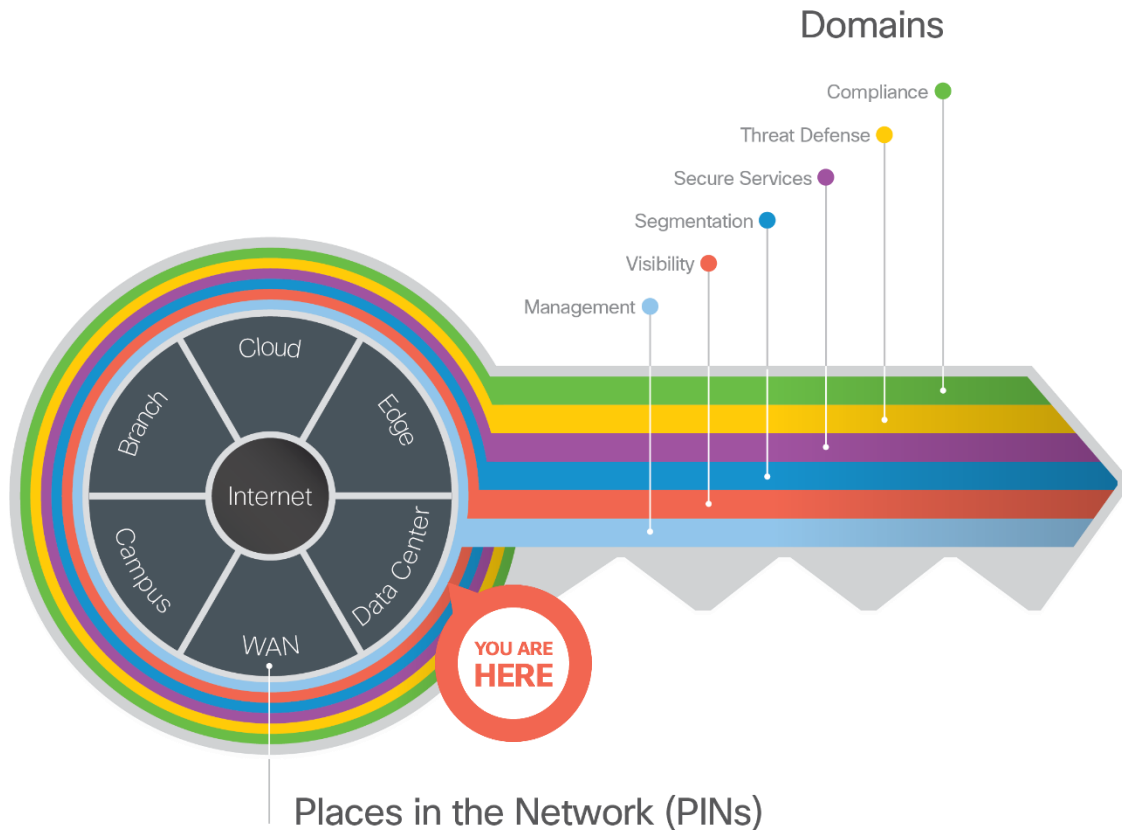
Secure Data Center Lab Diagram 288

289 Appendix B

Solution Products 289

Introduction

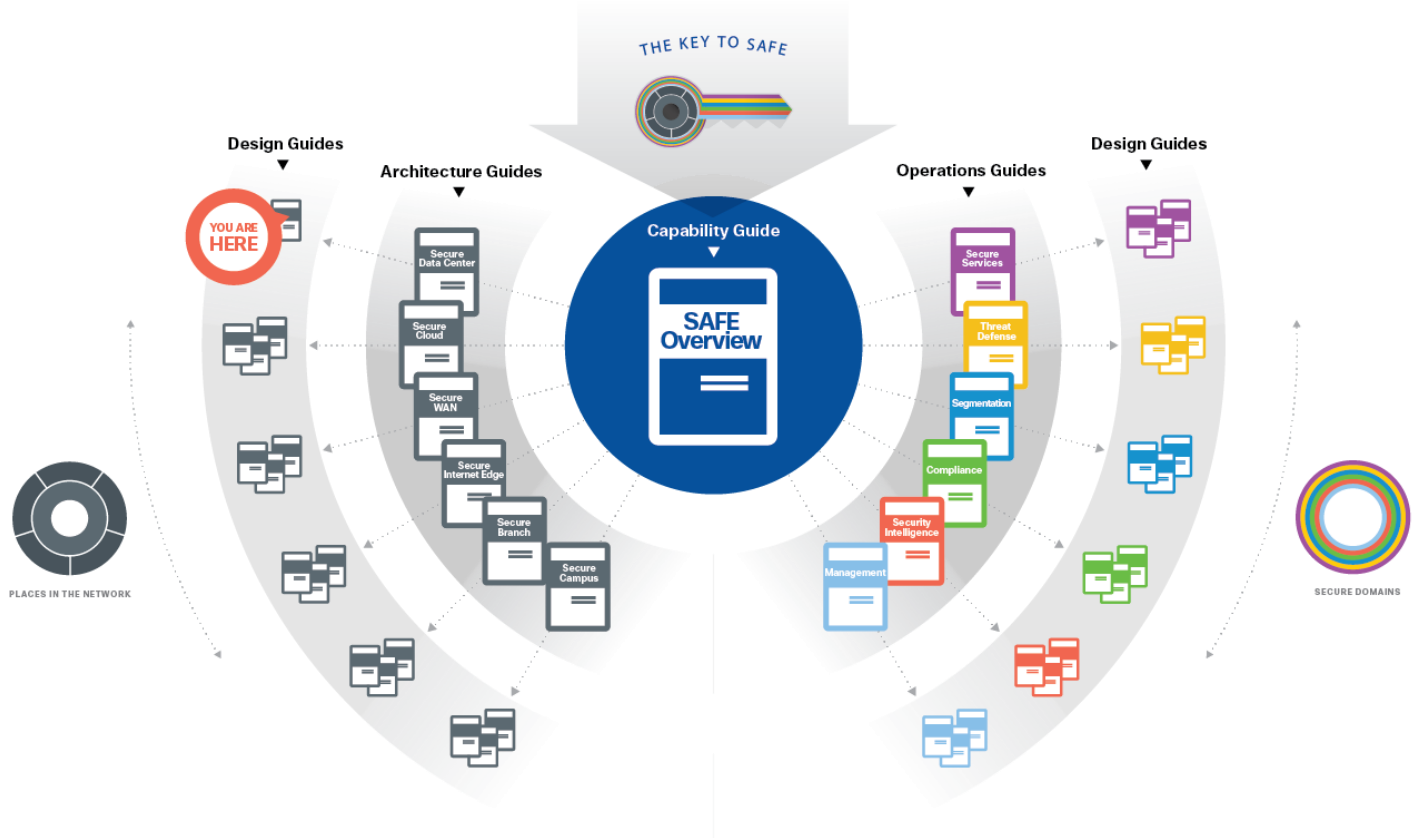
Cisco's Secure Data Center Solution includes effective and intent based security that follows the workload across physical data centers and multicloud environments to protect applications, infrastructure, data, users. Cisco's solution continuously learns, adapts, and protects. As the network changes 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.

5

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:

6

Revision History

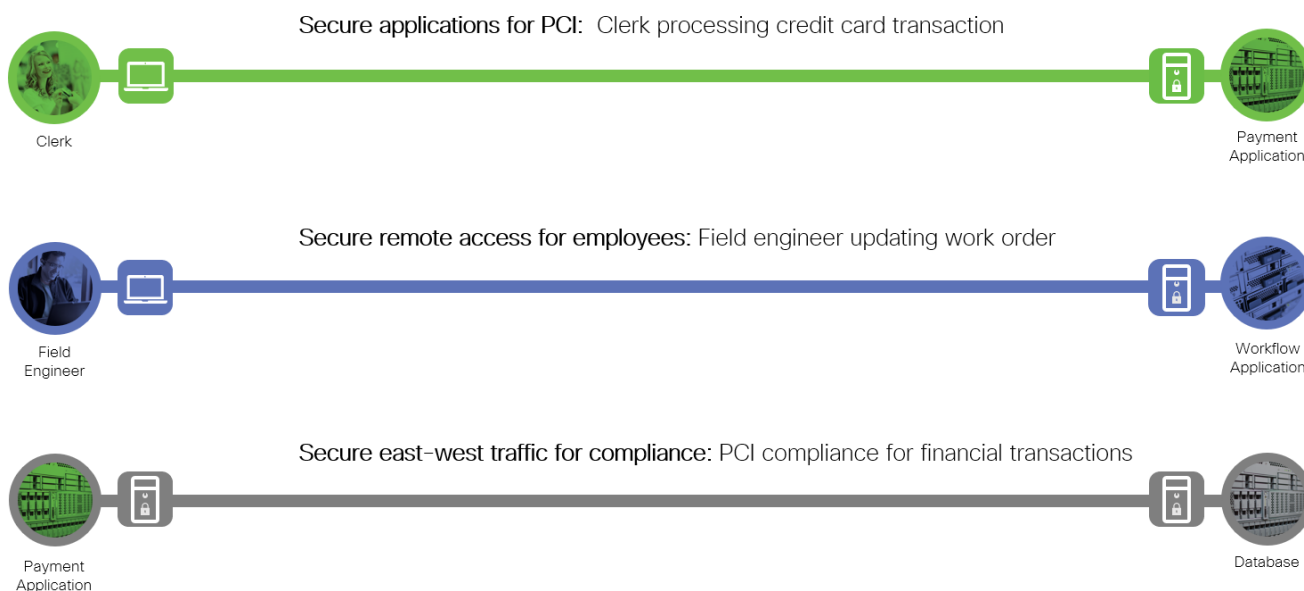
Date	Description
December 2018	Initial Input
June 2019	Updated images for Hyperflex, APIC, MSO, Nexus 9000, Fabric Interconnects, FTD, FMC and regression tested Test Case 1. Maintenance update rewrote Appendix C APIC initial configuration for better flow.
August 2019	Combined Appendix C and D and included 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:

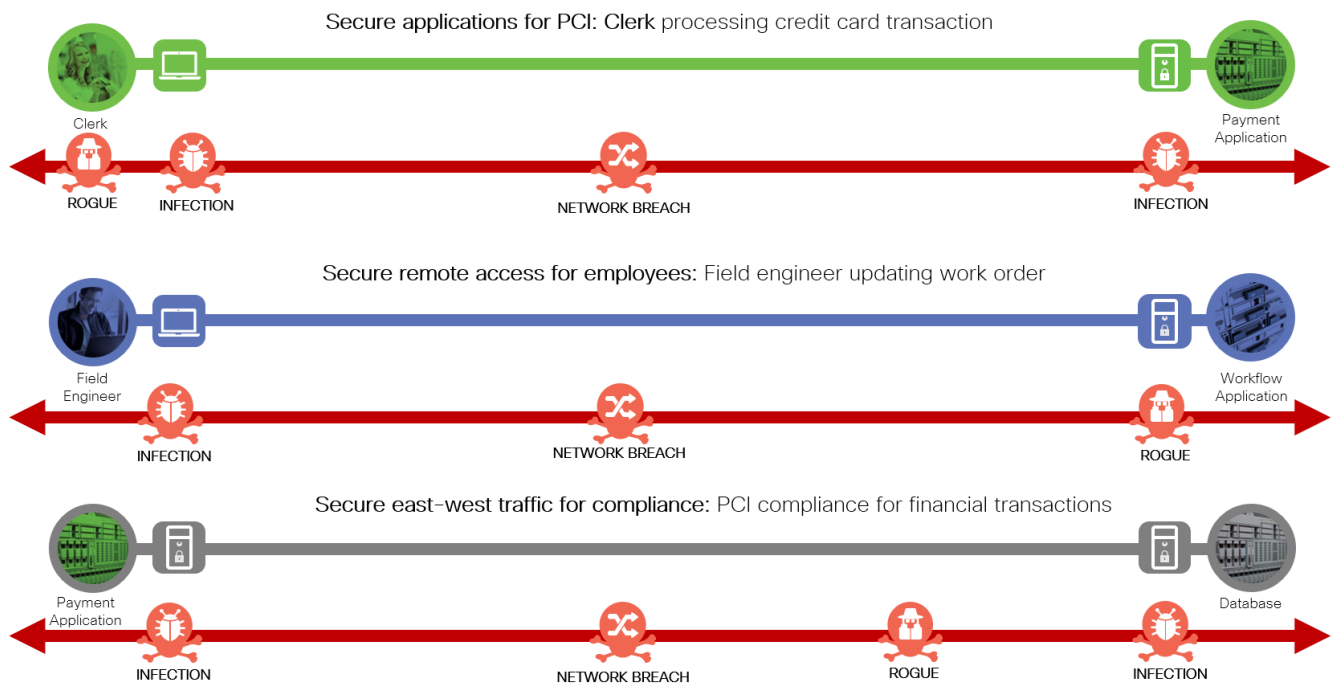
- Secure applications and servers that are present on network
- Secure remote access for support
- Securing east-west traffic



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.



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

9

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.

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.



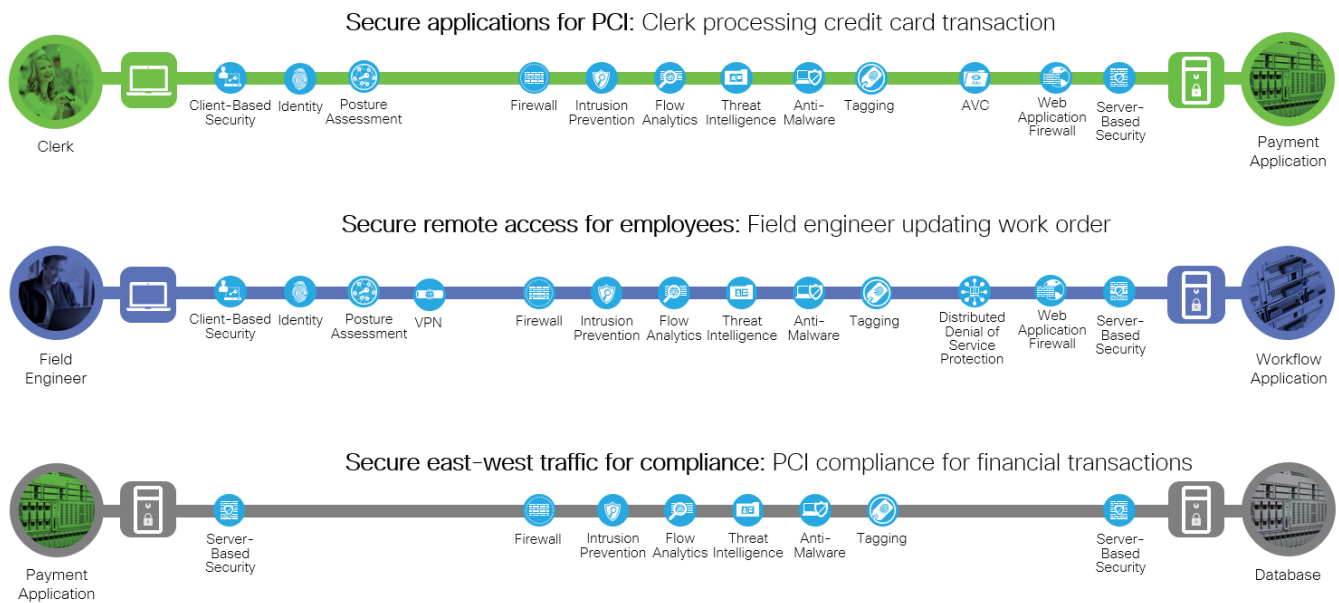
All data centers have something in common: they need to protect their applications and data from an increasing number of sophisticated threats and global attacks. All organizations are under threat of attack; many have been breached but are unaware of it. Protecting the modern data center is a challenge 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.

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.

13

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

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

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

Cisco Secure Data Center Reference Architecture

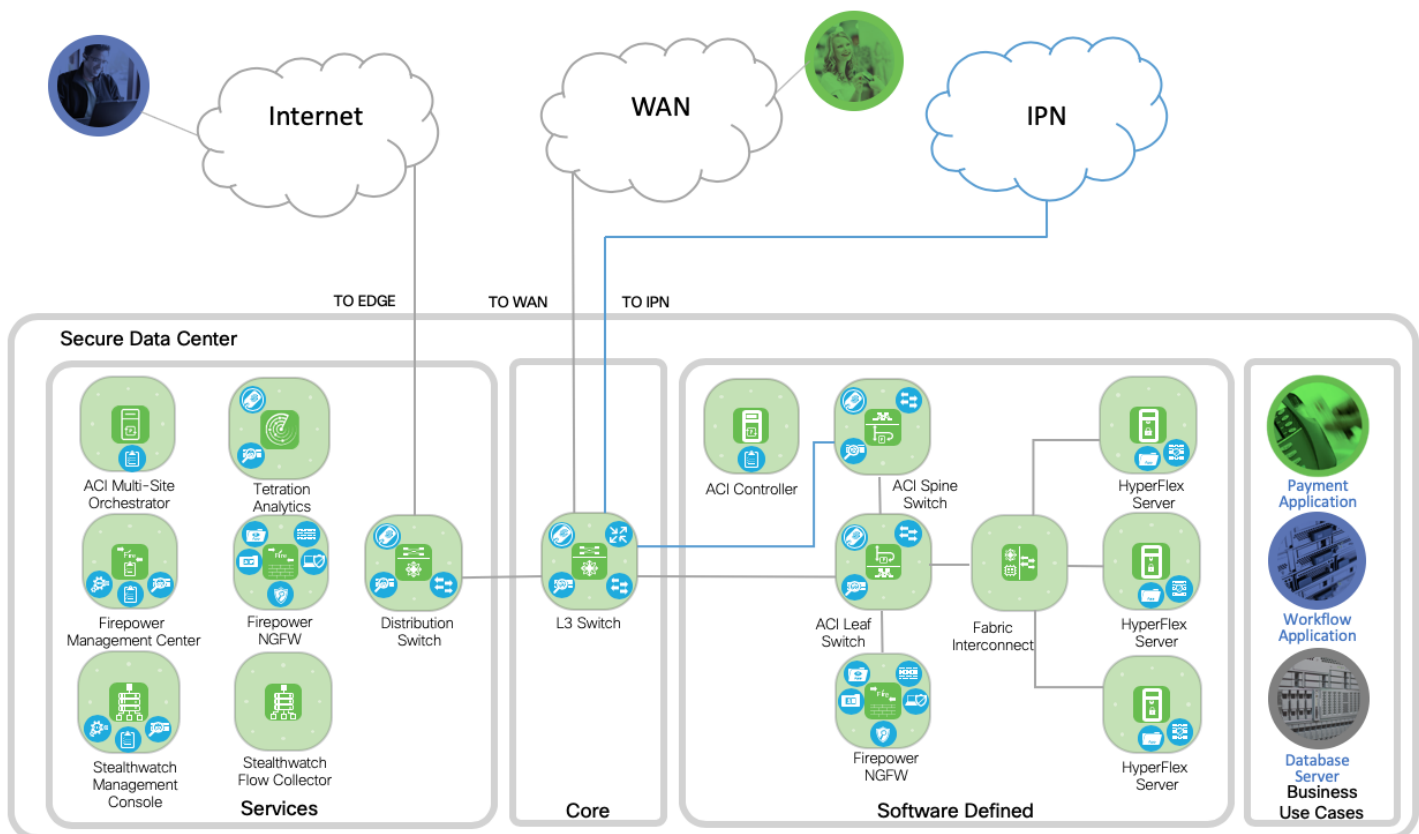
The Cisco Secure Data Center reference architecture is a solution that includes the best of Cisco's products for a modern data center.

- 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.

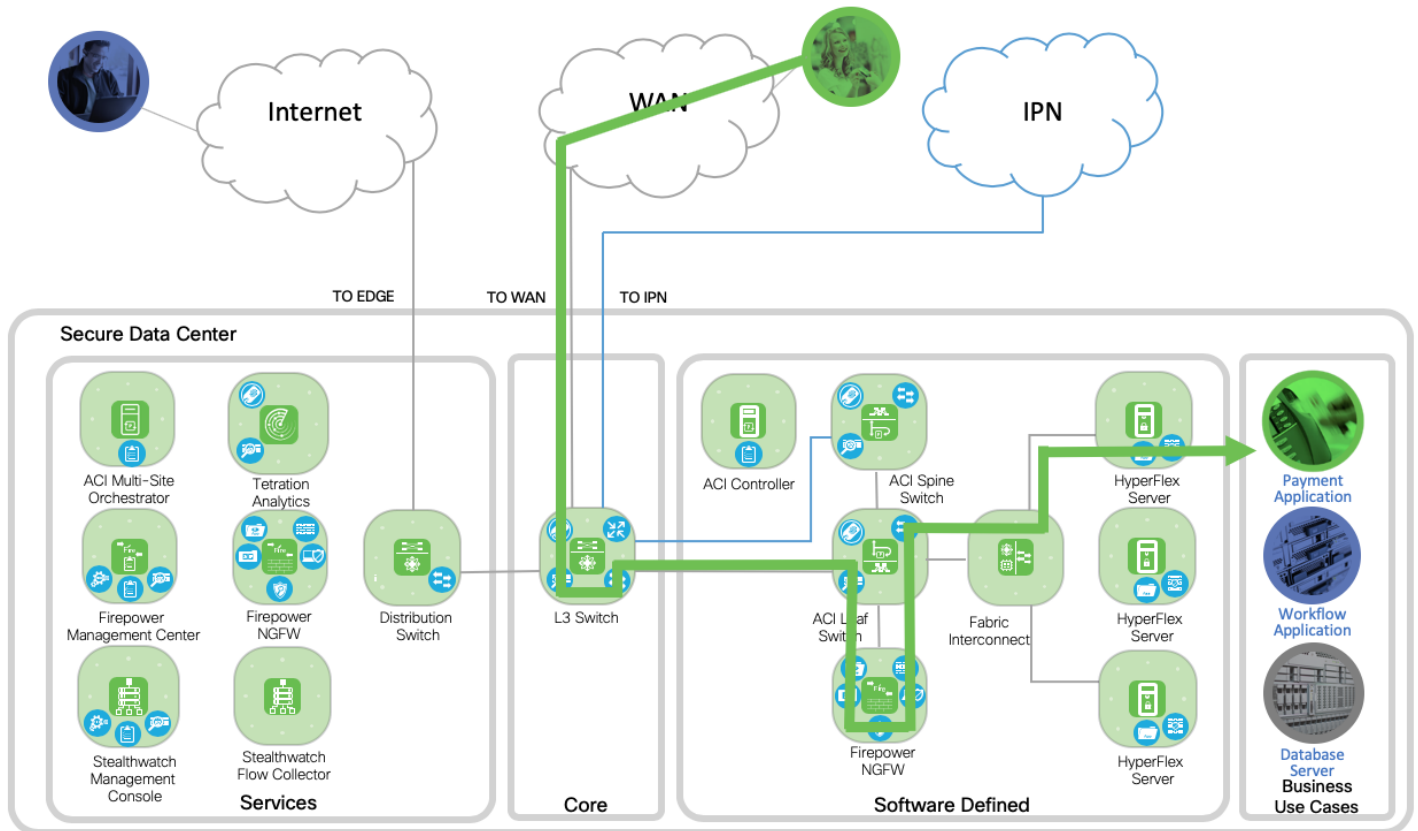
The Intersite Network is a network where different Application Policy Infrastructure Controller (APIC) domains are interconnected through generic Layer 3 infrastructure. Intersite Network is used for Multi-Site ACI deployment and provides data center interconnect. The Edge, WAN and Intersite Network 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.

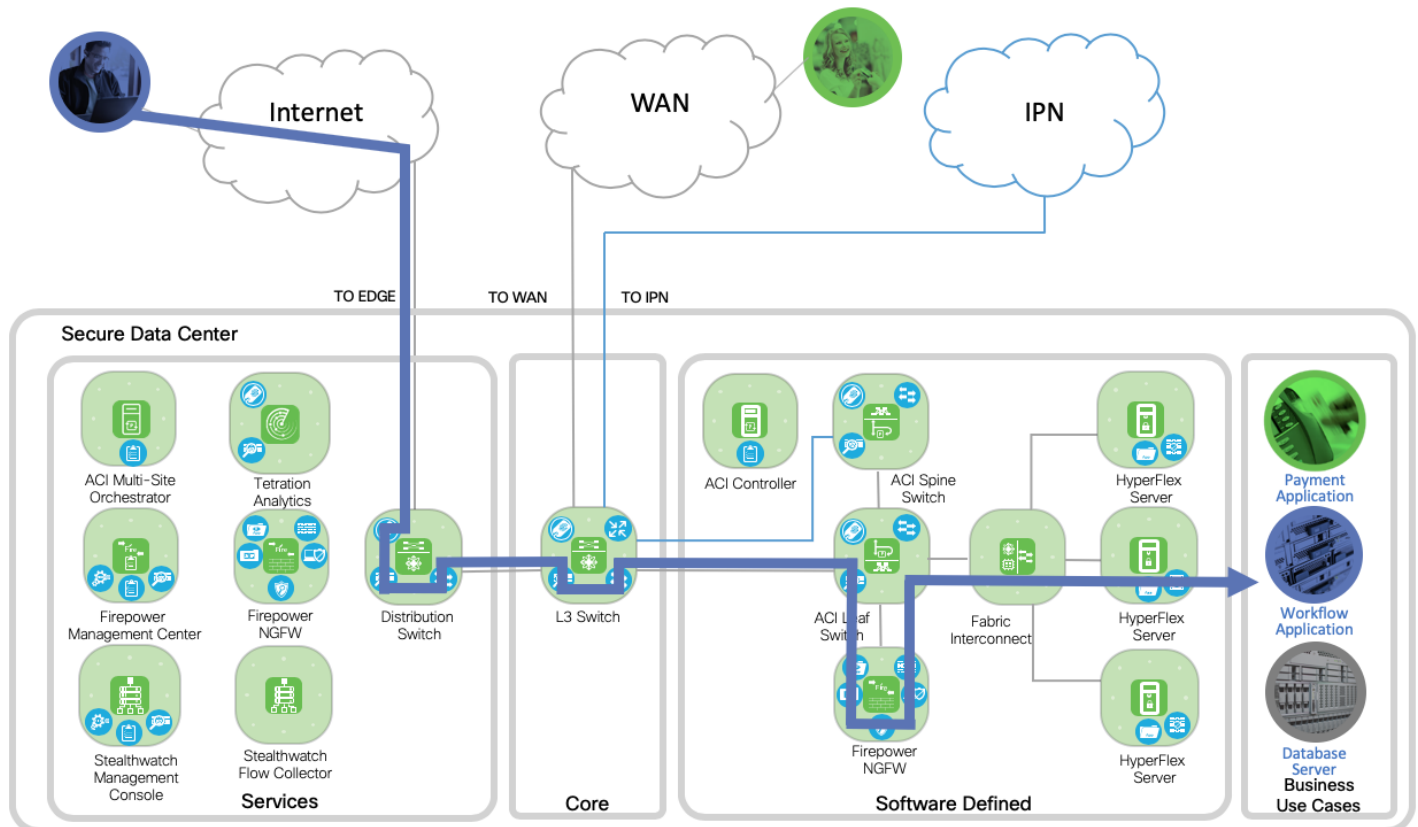
17

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.

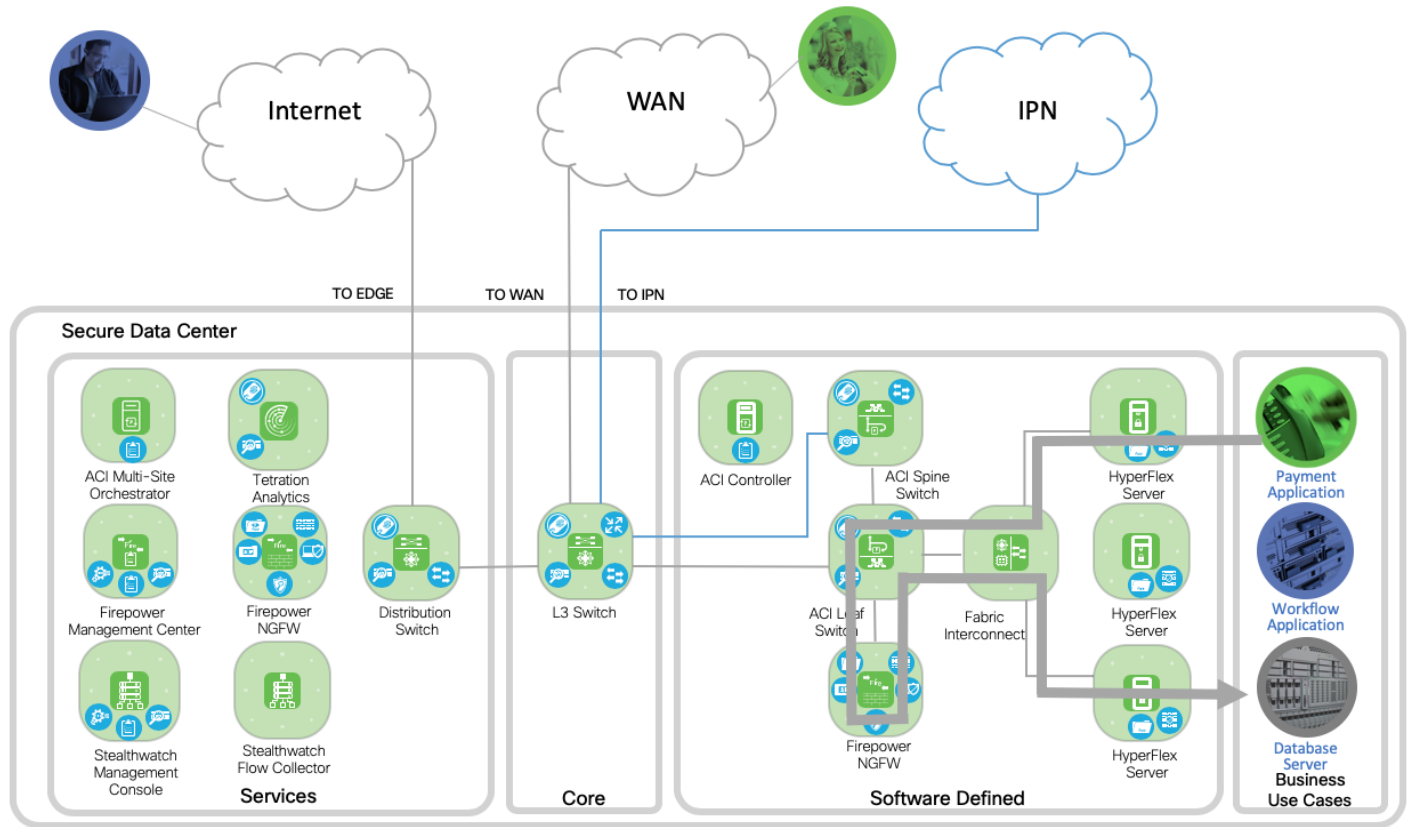


18

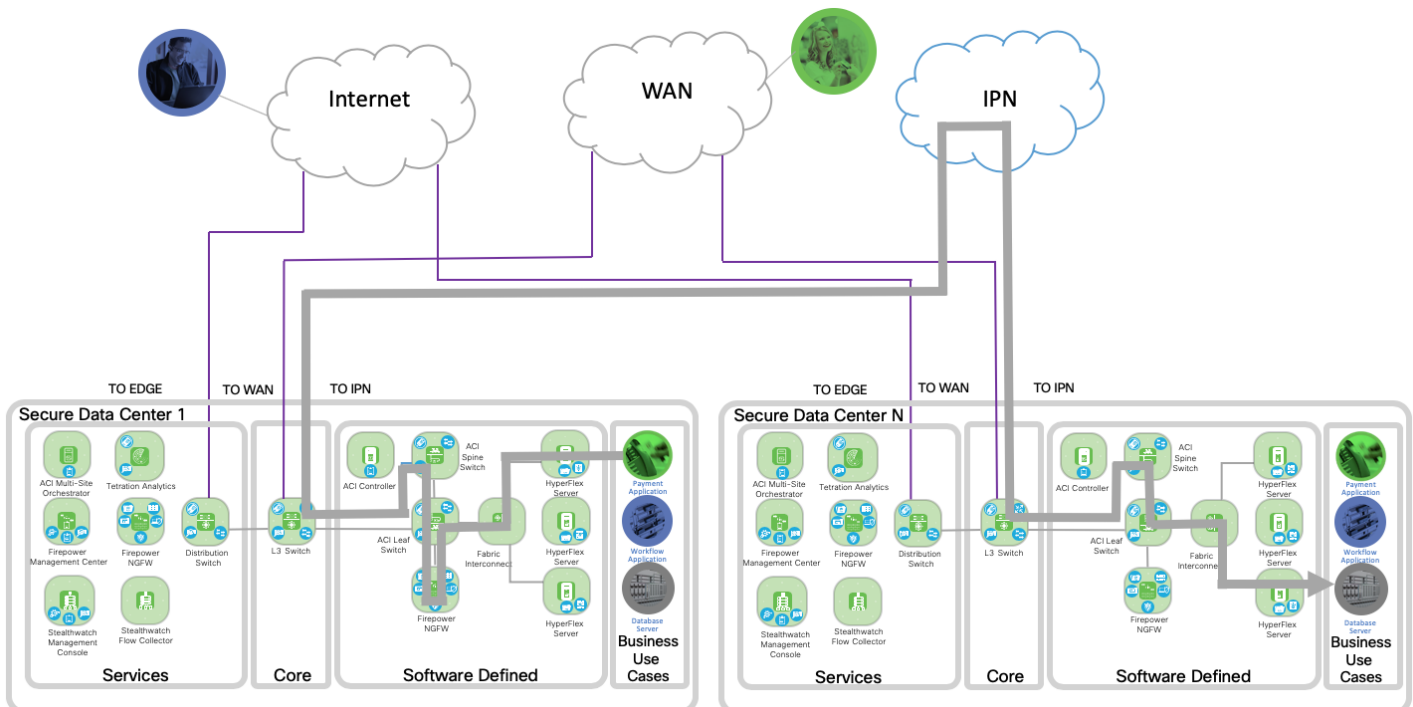
The second business flow secures remote access for employees. A field engineer is accessing the data center submitting a work order to the workflow application. The data flows from the Internet edge to a Distribution switch in the Services zone. VPN termination is handled by the Internet Edge architecture. 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.



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.

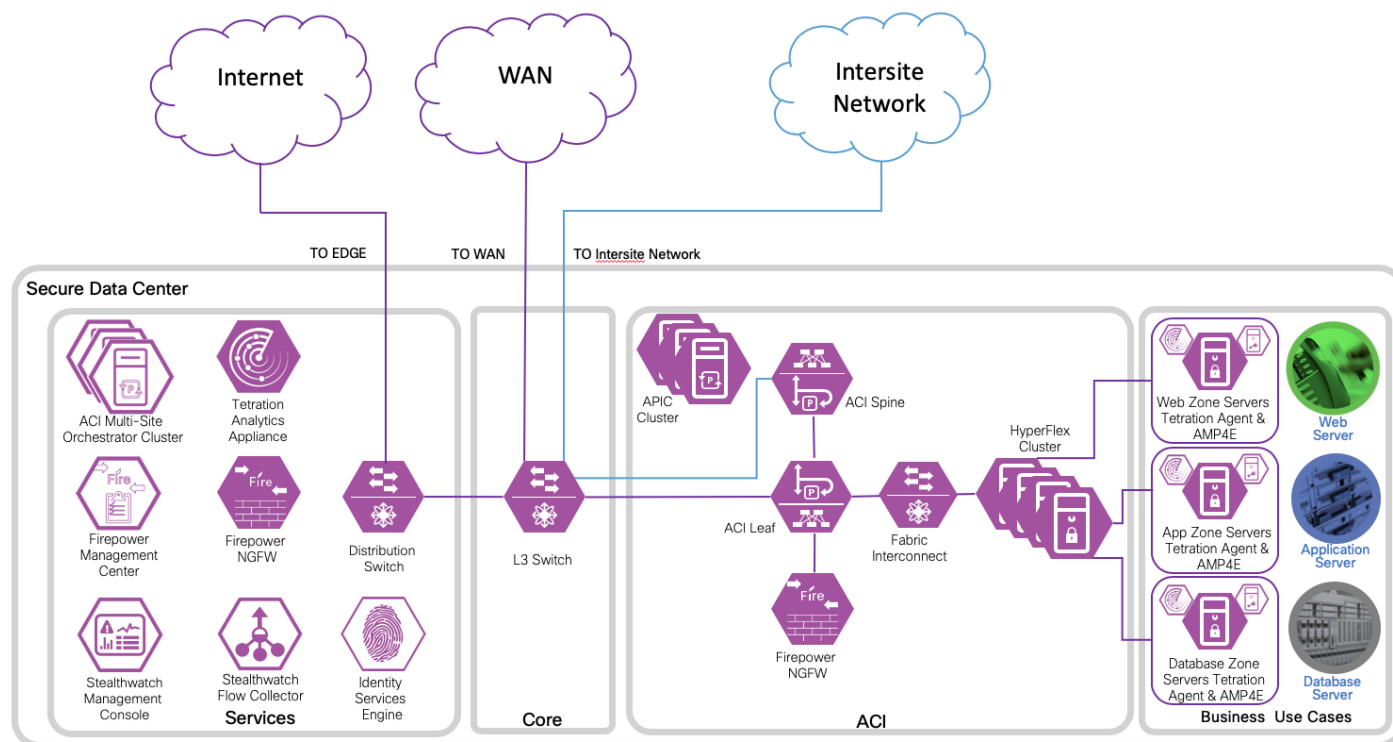


Additionally, the third business flow secures east-west traffic across data centers. In this case the database server and payment application are communicating between two data centers.



Implementation

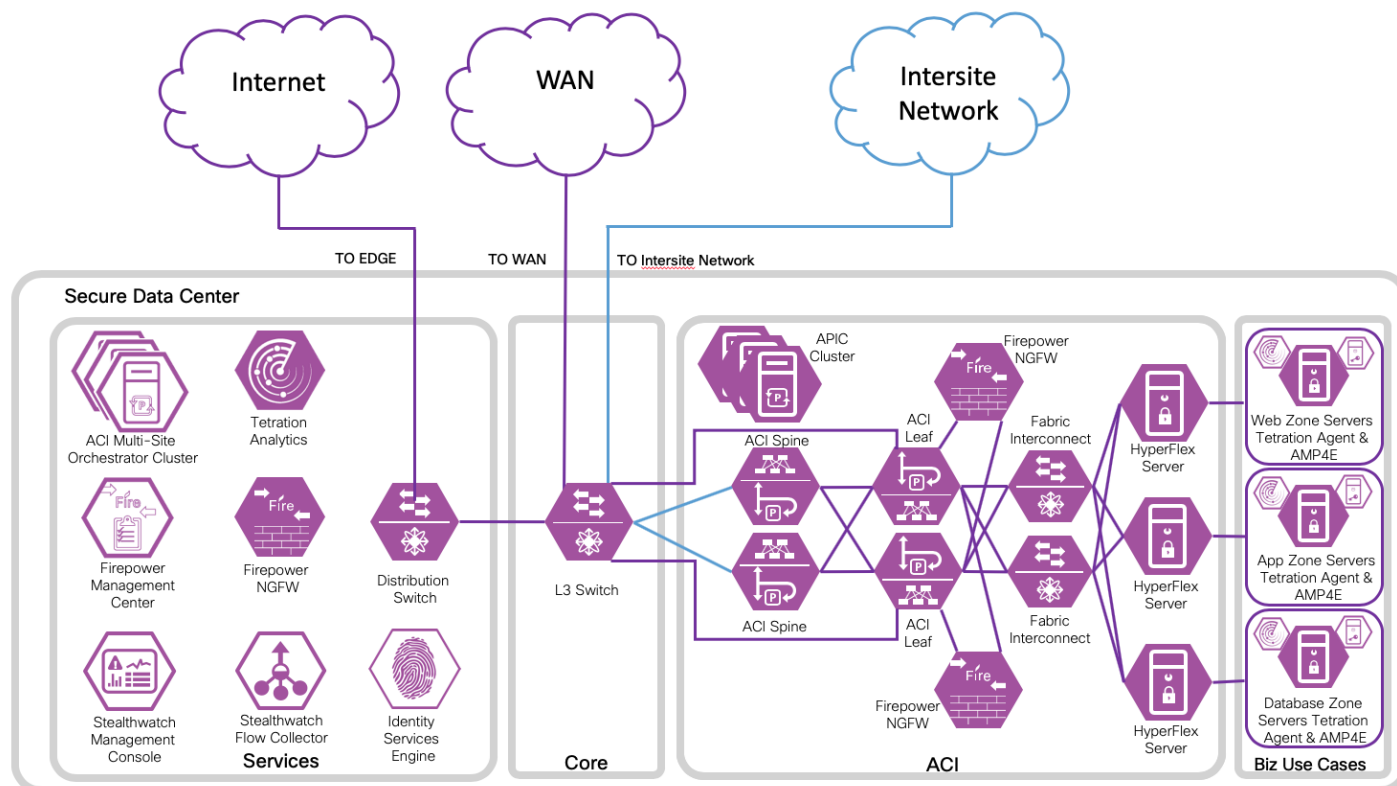
The Cisco Secure Data Center Reference Design is built based on the Secure Data Center Reference Architecture. For lab testing purposes virtual machines were used for the Multi-Site Orchestration Cluster, Firepower Management Center, Stealthwatch Management Console and Stealthwatch Flow Collector. For 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.

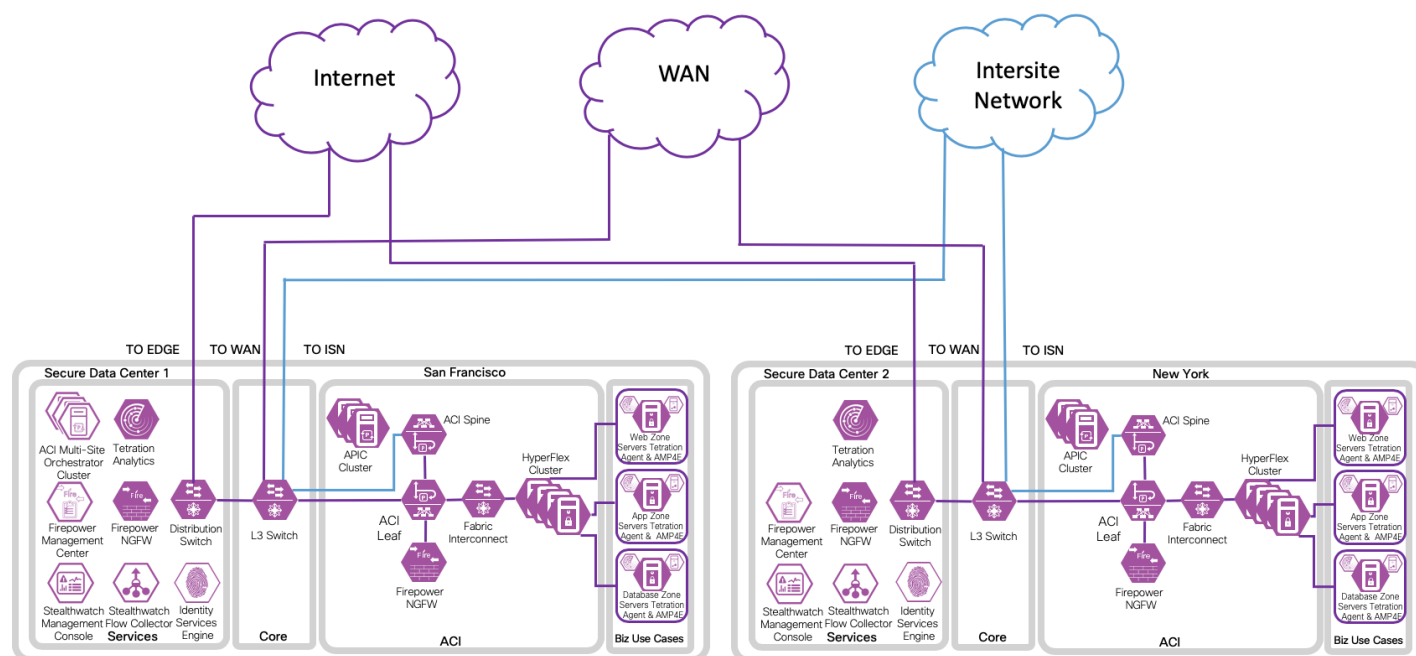
21

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.



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.



23

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

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

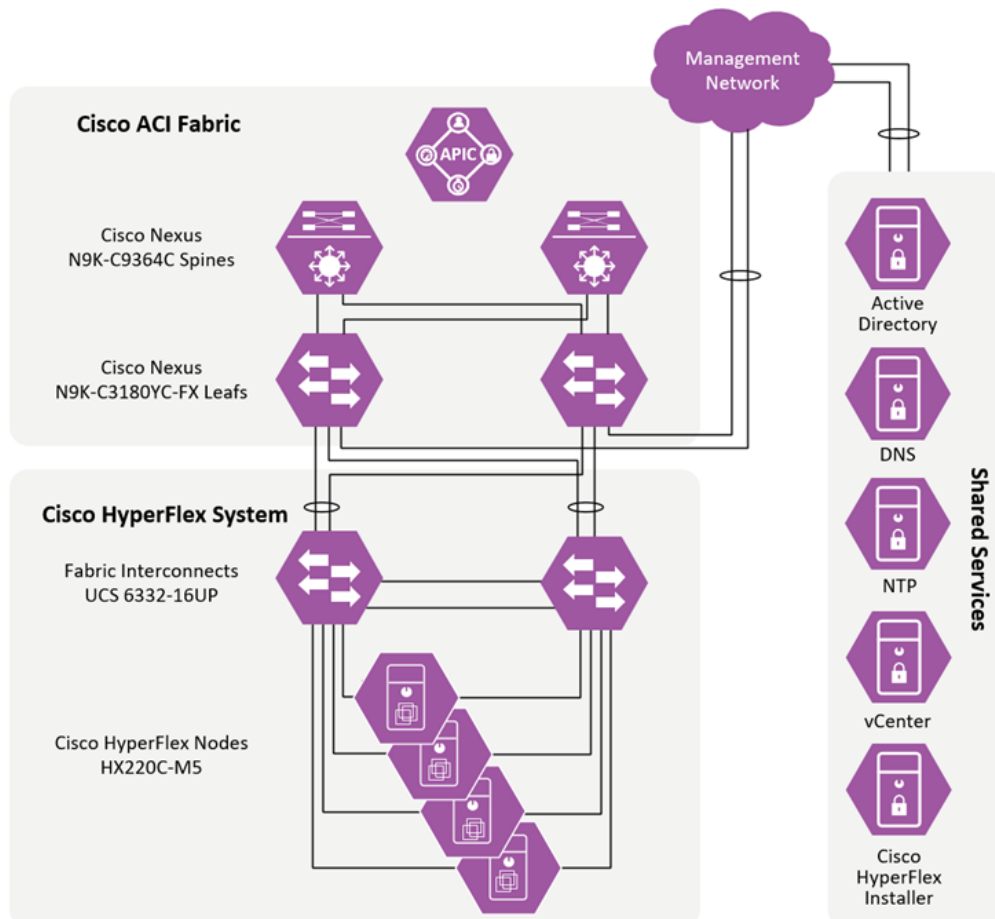
Cisco HyperFlex™ systems with Intel® Xeon® Scalable processors deliver hyperconvergence with the power and simplicity for any application, on any cloud, and at any scale. Engineered on the Cisco Unified Computing System™ (Cisco UCS®), Cisco HyperFlex™ systems deliver the agility, scalability, and pay-as-you-grow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

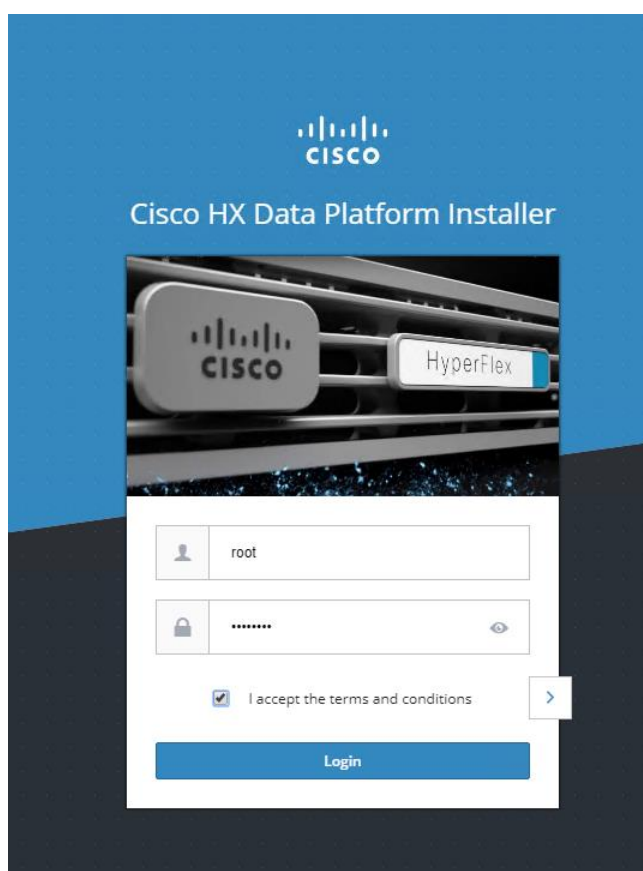


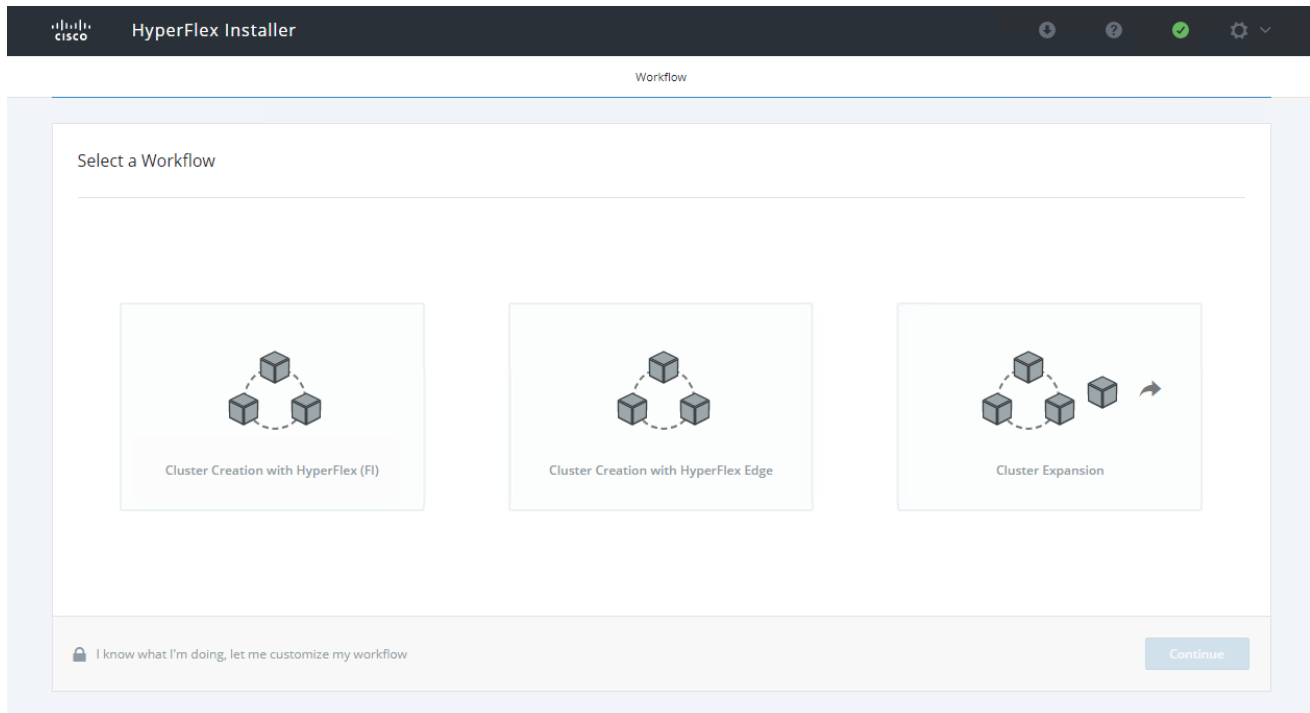
The diagram above illustrates a small deployment of the Hyperflex system. The system consists of two Cisco Fabric Interconnects and four Cisco Hyperflex nodes. It connects to the infrastructure via the leaf switches and utilizes the existing shared services.

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.

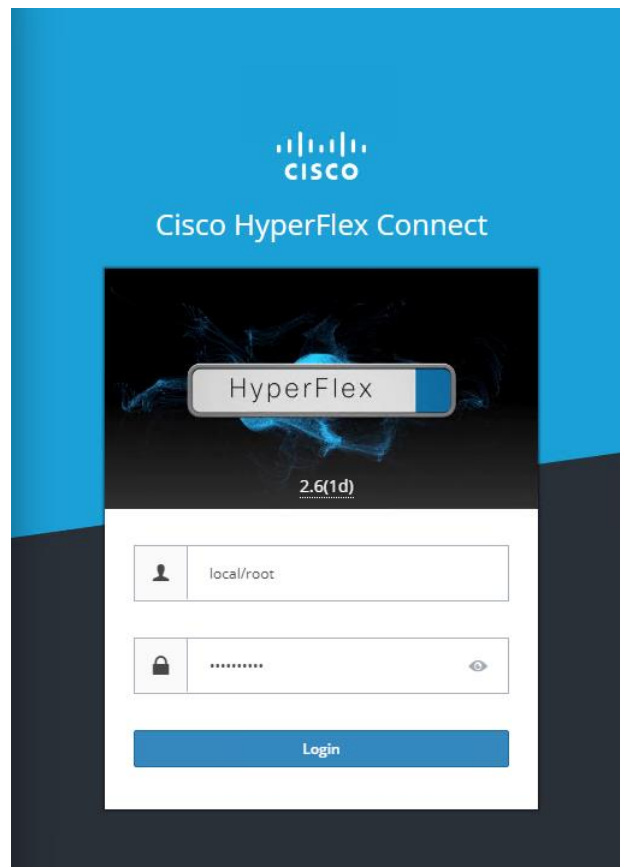
Additionally, we started with the Pre-Installation Checklist for VMware with Cisco HX platform, https://www.Cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HyperFlex_Preinstall_Checklist/b_HX_Data_Platform_Preinstall_Checklist.html.

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





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



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.

32

Firepower 4110 and Firepower 9300 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	<ul style="list-style-type: none">• ESXi 6.0• 3 vCPUs• 16 GB of RAM• 50 GB disk

Stealthwatch™ Flow Collector Virtual Edition	VMware vSphere Settings Tested
Release 7.0	<ul style="list-style-type: none"> • 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

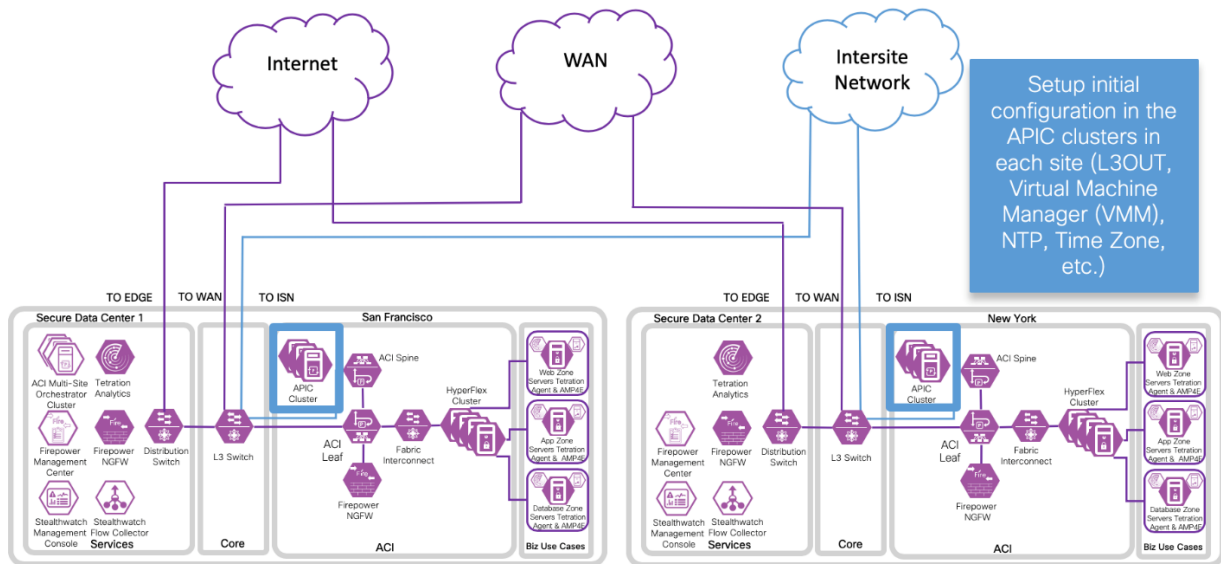
Test Case	Integration	Visibility	Segmentation	Threat Protection	Orchestration and Management	Benefits
1	ACI Multi-Site Orchestrator (MSO) and Firepower Threat Defense (FTD)		✓		✓	<ul style="list-style-type: none"> Enables Firepower Threat Defense (FTD) to be automated by MSO and inserted between applications in an ACI Multi-Site fabric MSO simplifies configurations to multiple APIC domains deployed globally
2	Firepower Management Center (FMC) and APIC		✓		✓	<ul style="list-style-type: none"> 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)	✓	✓			<ul style="list-style-type: none"> 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	✓				<ul style="list-style-type: none"> 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	✓		✓		<ul style="list-style-type: none"> 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			✓		<ul style="list-style-type: none"> Automated Response Prevents further lateral movement of infection by protecting other hosts in Endpoint Group (EPG)
7	FTD Rapid Threat Containment and Tetration			✓		<ul style="list-style-type: none"> Automated Response Prevents further lateral movement of infection by protecting other hosts in microsegment
8	Tetration and Identity Services Engine (ISE)	✓	✓			<ul style="list-style-type: none"> 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	✓	✓			<ul style="list-style-type: none"> Extends User Access Policy for enhanced enforcement in the Data Center Provides Zero trust or allow/block list model

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

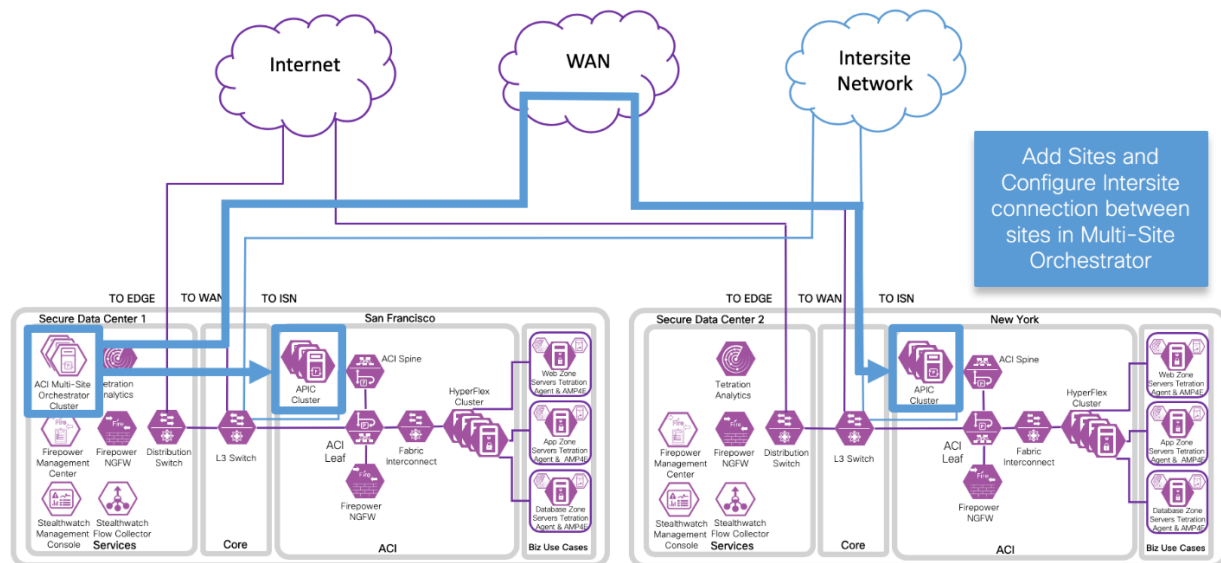
This test case involved building out the secure data center reference architecture for ACI Multi-Site. FTD is deployed as a one arm cluster in each data center. FTD is the L4-L7 service providing threat defense services for north-south and east-west traffic in the data center fabric.

Test case overview:

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

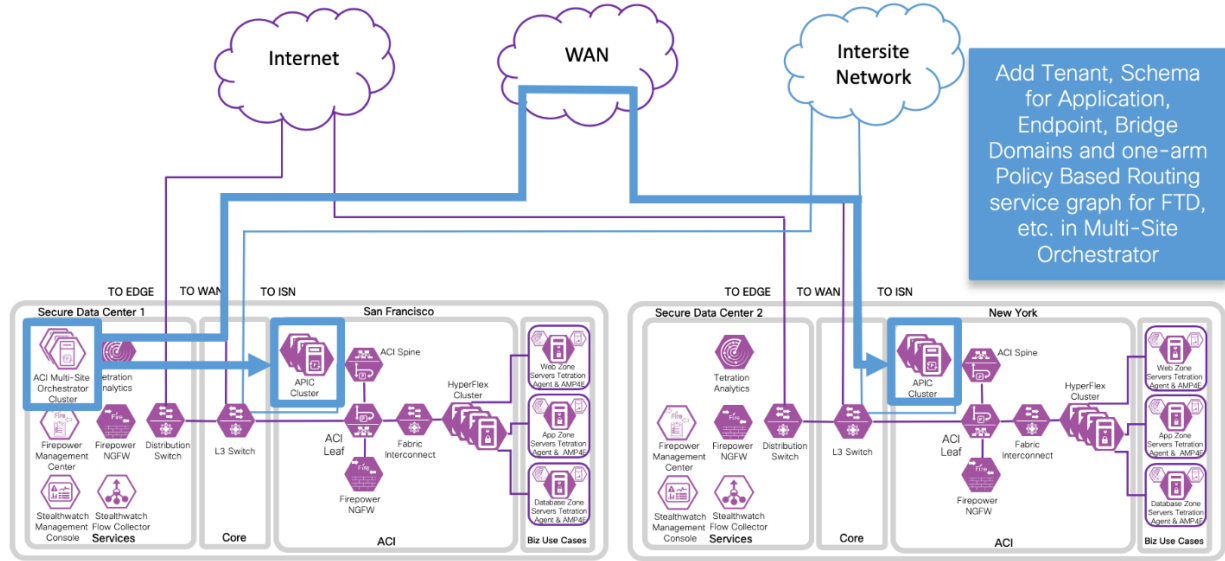


2. Add Sites and configure Intersite connection between sites in ACI Multi-Site Orchestrator.



40

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



41

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

42

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

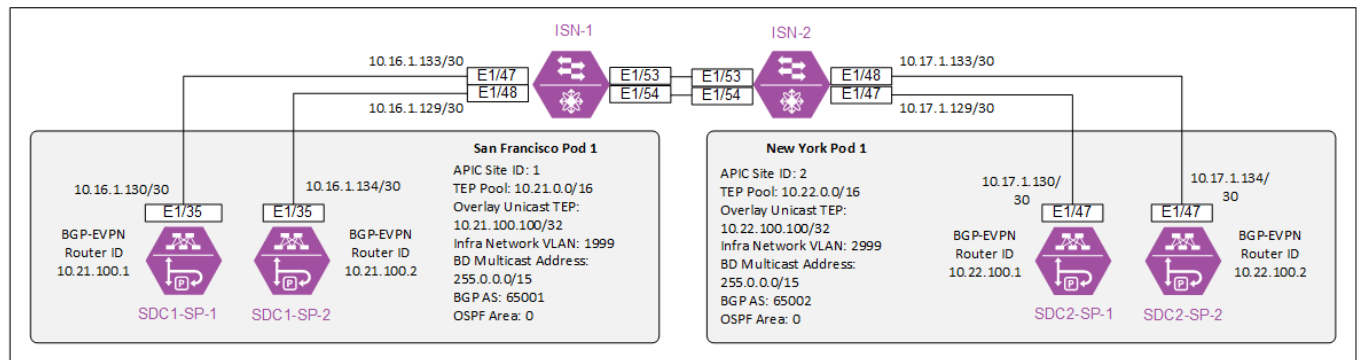
43

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

44

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-411/Cisco-APIC-Layer-2-Configuration-Guide-411_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**

46

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

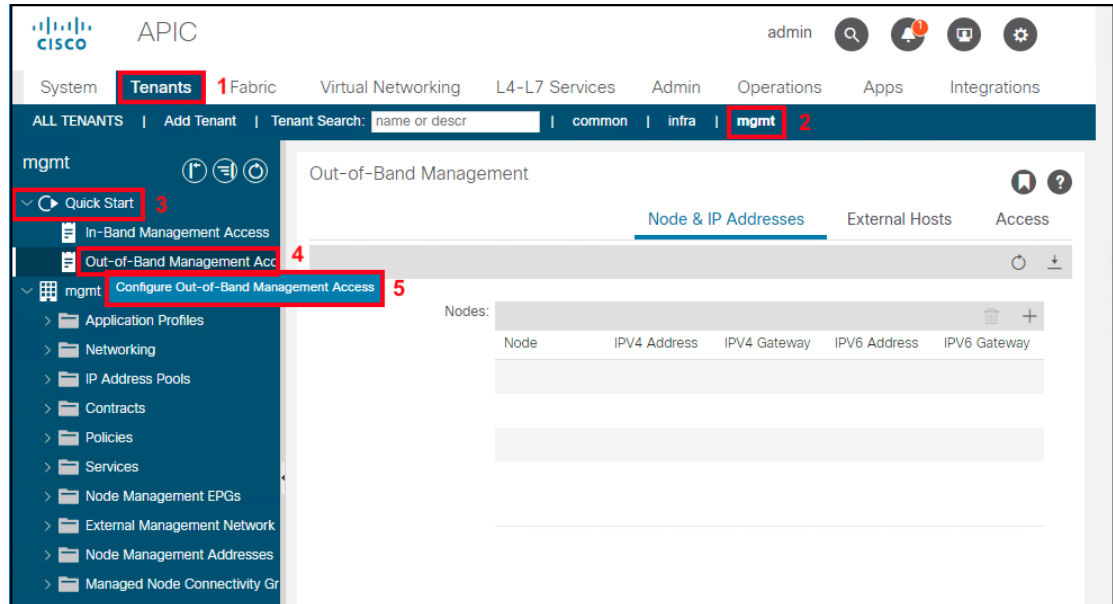
```
Cluster configuration ...
  Enter the fabric name [SDC1Fabric1]:
  Enter the fabric ID (1-128) [1]:
  Enter the number of active controllers in the fabric (1-9) [3]:
  Enter the POD ID (1-12) [1]:
  Is this a standby controller? [NO]:
  Is this an APIC-X? [NO]:
  Enter the controller ID (1-3) [1]:
  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]:

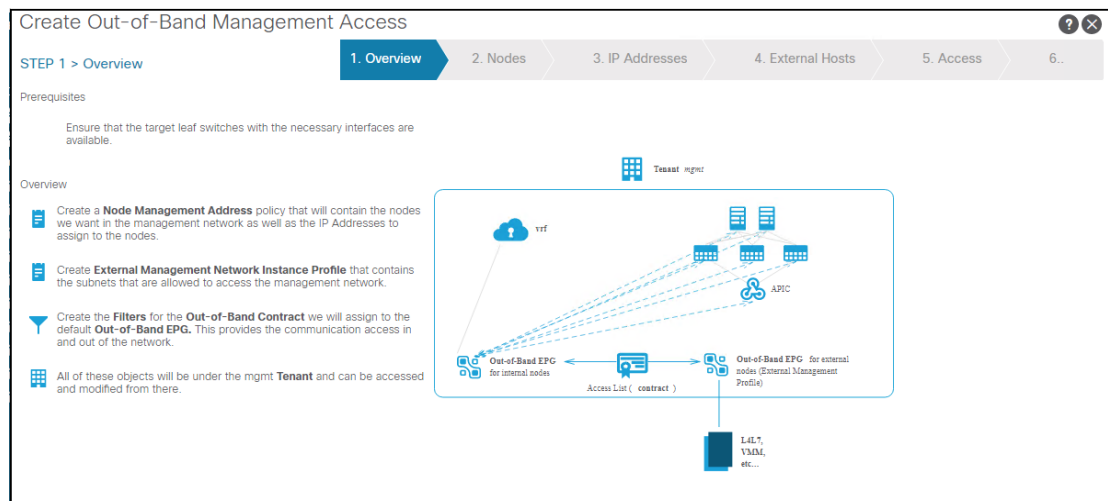
admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:
```

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.



48

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

Create Out-of-Band Management Access

STEP 2 > Nodes

1. Overview 2. Nodes 3. IP Addresses 4. External Hosts 5. Access 6. Confirmation

Select Nodes By: **Specific** Range

Nodes:

☐ Select All

Select	ID	Name	Role
<input type="checkbox"/>	1	SDC1-APIC1	controller
<input type="checkbox"/>	2	SDC1-APIC2	controller
<input type="checkbox"/>	3	SDC1-APIC3	controller
<input checked="" type="checkbox"/>	101	SDC1-LF1	leaf
<input checked="" type="checkbox"/>	102	SDC1-LF2	leaf
<input checked="" type="checkbox"/>	201	SDC1-SP1	spine
<input checked="" type="checkbox"/>	202	SDC1-SP2	spine

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

Create Out-of-Band Management Access

STEP 3 > IP Addresses

1. Overview 2. Nodes 3. IP Addresses 4. External Hosts 5. Access 6. Confirmation

Starting Out-of-Band IPV4 Address: **10.16.1.17/24** 1

Starting Out-of-Band IPV6 Address:

Out-Of-Band IPV4 Gateway: **10.16.1.1** 2

Out-Of-Band IPV6 Gateway:

Node Id	Name	IPv4 Address	IPv4 Gateway	IPv6 Address	IPv6 Gateway
101	SDC1-LF1	10.16.1.17/24	10.16.1.1		
102	SDC1-LF2	10.16.1.18/24	10.16.1.1		
201	SDC1-SP1	10.16.1.19/24	10.16.1.1		
202	SDC1-SP2	10.16.1.20/24	10.16.1.1		

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

Create Out-of-Band Management Access

STEP 4 > External Hosts

1. Overview 2. Nodes 3. IP Addresses 4. External Hosts 5. Access 6. Confirmation

External Hosts:

IP

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

Create Out-of-Band Management Access

STEP 5 > Access

1. Overview 2. Nodes 3. IP Addresses 4. External Hosts 5. Access 6. Confirmation

Filters:

EtherType	IP Protocol	Source Port	Destination Port

No items have been found.
Select Actions to create a new item.

49

- g. Review and click **Finish**.

Create Out-of-Band Management Access

STEP 6 > Confirmation

1.. 2. Nodes 3. IP Addresses 4. External Hosts 5. Access 6. Confirmation

✓ Here is the list of policies this wizard will create, you can change these names if needed

Contract Subject:	default
Inband EPG:	oob-default
Out-Of-Band Consumer Contract:	oob-default
Out-Of-Band Contract:	default
Out-Of-Band Management EPG:	default

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.

CISCO APIC

admin

System Tenants **Fabric** 1 Virtual Networking L4-L7 Services Admin Operations Apps Integrations

Inventory **Fabric Policies** 2 Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies** 3
 - Pod** 4
 - Date and Time** 5
 - Policy default** 6
 - SNMP
 - Management Access
 - ISIS Policy default
 - Switch
 - Interface
 - Global
 - Monitoring
 - Troubleshooting
 - Geolocation
 - Macsec
 - Analytics
 - Tenant Quota
 - Tags

Date and Time Policy - Policy default

Properties

Name: default
Description: optional

Administrative State: disabled enabled
Server State: disabled enabled
Authentication State: disabled enabled

Authentication Keys:

ID	Key	Trusted	Authentication Type
No items have been found. Select Actions to create a new item.			

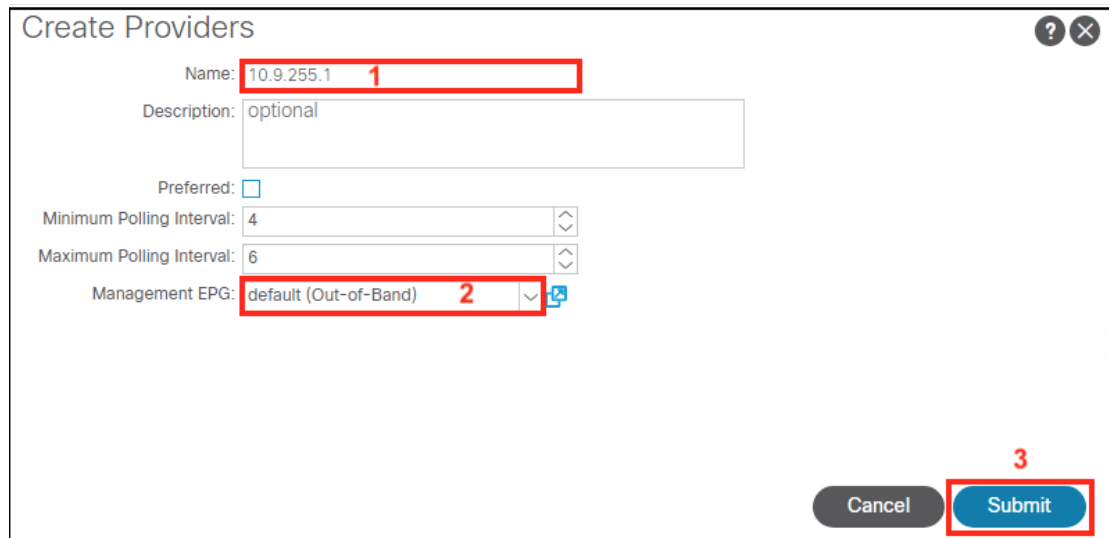
NTP Servers:

Host Name/IP Address	Preferred	Minimum Polling Interval	Maximum Polling Interval	Management EPG
+				

Show Usage Reset Submit

50

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



Create Providers

Name: 10.9.255.1 **1**

Description: optional

Preferred: ☐

Minimum Polling Interval: 4

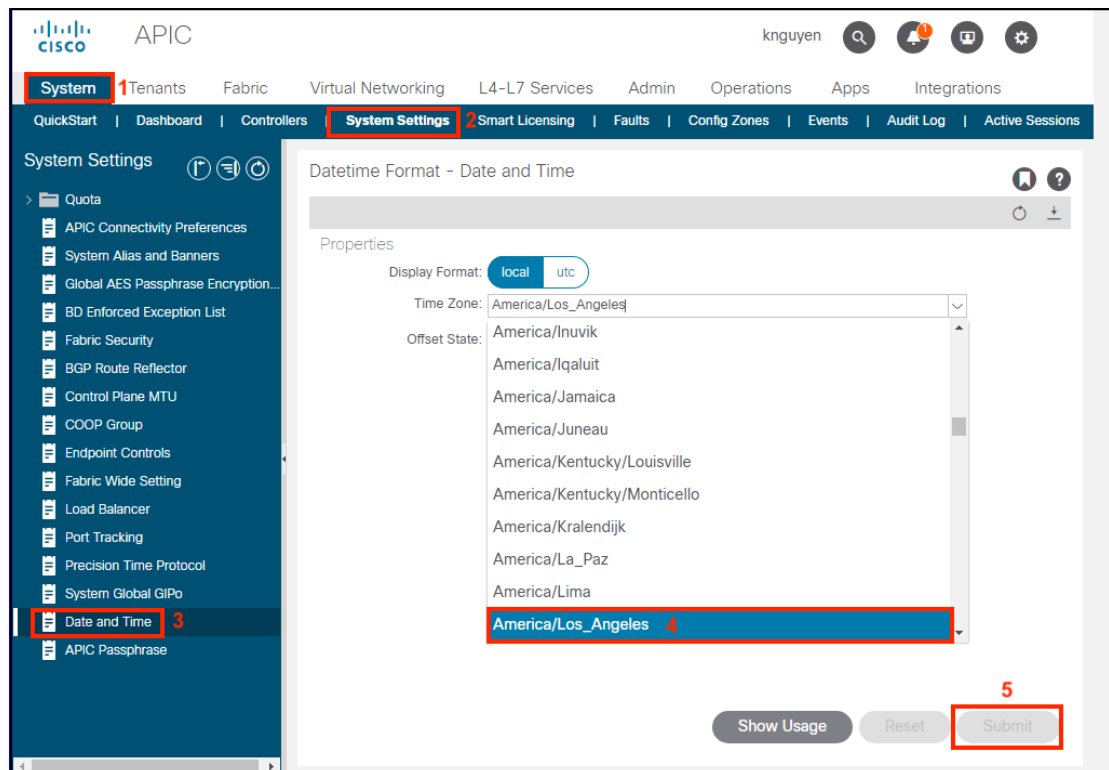
Maximum Polling Interval: 6

Management EPG: default (Out-of-Band) **2**

3

Cancel Submit

- 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)**.



APIC knguyen

System **1** Tenants Fabric Virtual Networking L4-L7 Services Admin Operations Apps Integrations

QuickStart | Dashboard | Controllers **System Settings** **2** Smart Licensing | Faults | Config Zones | Events | Audit Log | Active Sessions

System Settings

- Quota
- APIC Connectivity Preferences
- System Alias and Banners
- Global AES Passphrase Encryption...
- BD Enforced Exception List
- Fabric Security
- BGP Route Reflector
- Control Plane MTU
- COOP Group
- Endpoint Controls
- Fabric Wide Setting
- Load Balancer
- Port Tracking
- Precision Time Protocol
- System Global GIPo
- Date and Time** **3**
- APIC Passphrase

Datetime Format - Date and Time

Properties

Display Format: local utc

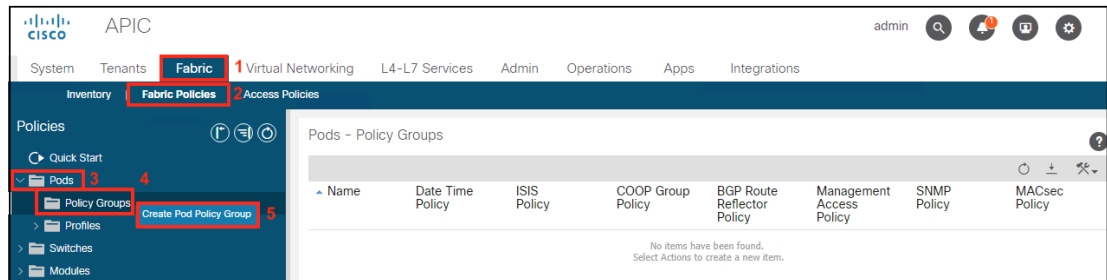
Time Zone: America/Los_Angeles

Offset State: America/Inuvik
America/Iqaluit
America/Jamaica
America/Juneau
America/Kentucky/Louisville
America/Kentucky/Monticello
America/Kralendijk
America/La_Paz
America/Lima
America/Los_Angeles **4**

Show Usage Reset **Submit** **5**

51

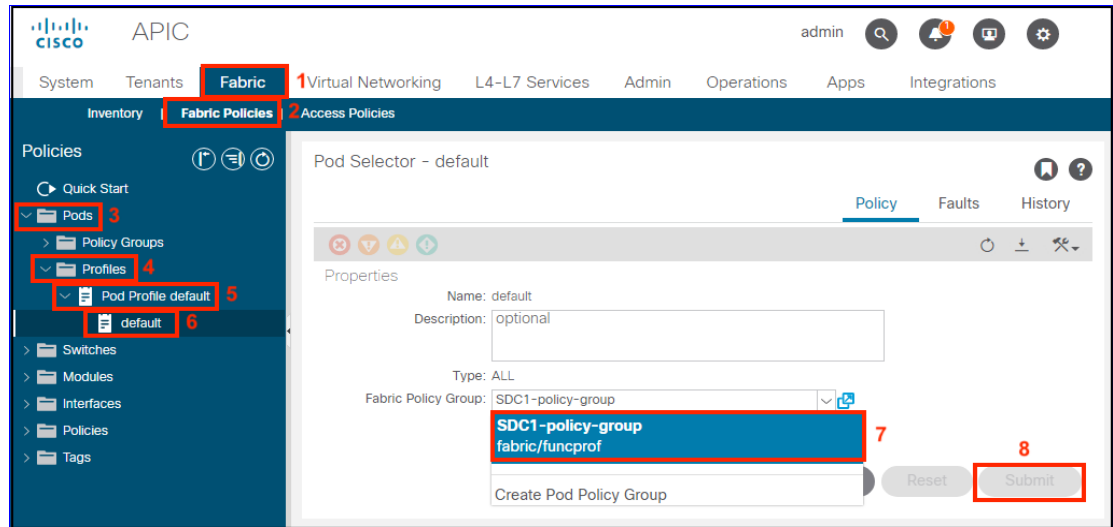
- d. Create POD Policy Group. This step is required before setting up the infra tenant in MSO. Navigate to **Fabric (1)**->**Fabric Policies (2)**->**Pods (3)**->**Policy Group (4)**, Right-Click and select **Create Pod Policy Group (5)**.



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

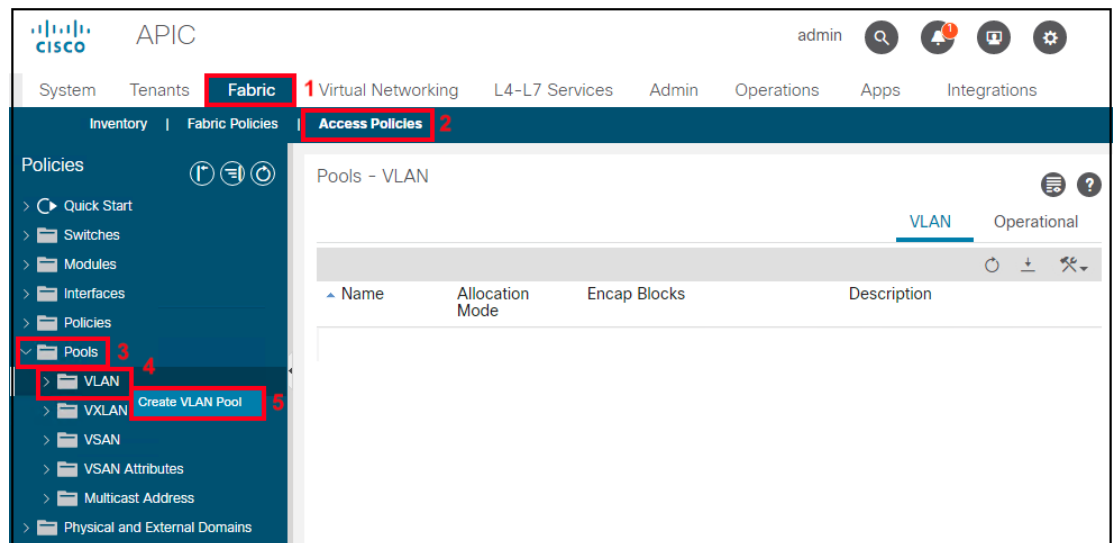
The screenshot shows the 'Create Pod Policy Group' form. The 'Name' field is filled with 'SDC1-policy-group' (labeled 1). The 'Description' field contains 'optional'. The 'Date Time Policy' dropdown is set to 'default' (labeled 2). Below this are several other policy dropdowns: 'ISIS Policy', 'COOP Group Policy', 'BGP Route Reflector Policy', 'Management Access Policy', 'SNMP Policy', and 'MACsec Policy', all currently set to 'select a value'. At the bottom right, the 'Submit' button is highlighted with a red box and labeled 3, next to a 'Cancel' button.

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



53

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

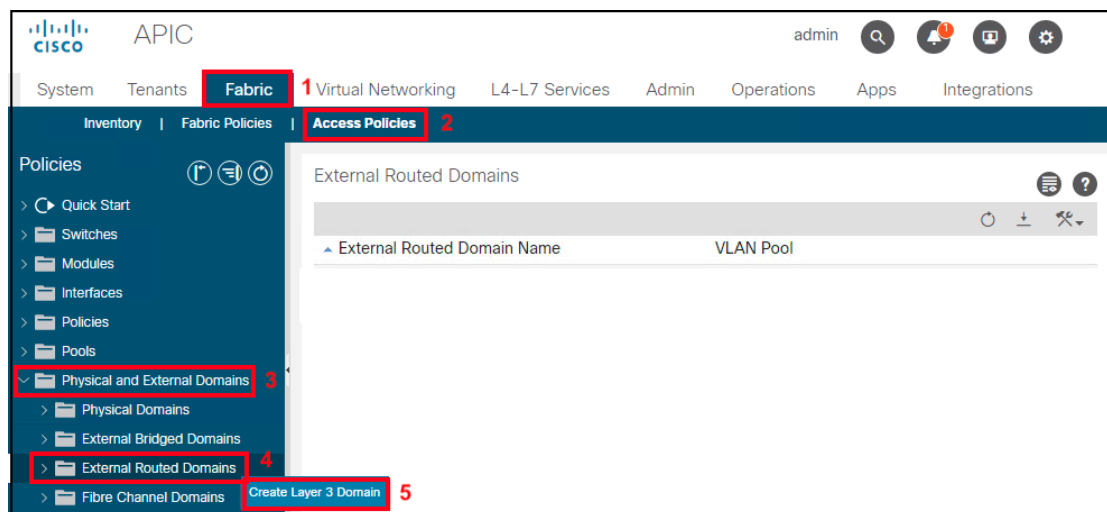
The 'Create Ranges' dialog box shows the configuration for a Dynamic VLAN pool. The 'Type' is set to 'VLAN'. The 'Range' is 'VLAN' with values '1000' (1) and '1099' (2). The 'Allocation Mode' is 'Dynamic Allocation' (3). The 'Role' is 'External or On the wire encapsulations'. The 'OK' button is highlighted (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)**.

The 'Create Ranges' dialog box shows the configuration for a Static VLAN pool. The 'Type' is set to 'VLAN'. The 'Range' is 'VLAN' with values '1100' (1) and '1199' (2). The 'Allocation Mode' is 'Static Allocation' (3). The 'Role' is 'External or On the wire encapsulations'. The 'OK' button is highlighted (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)**.



54

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

Create Layer 3 Domain

Name: **SDC1-L3OUT** **1**

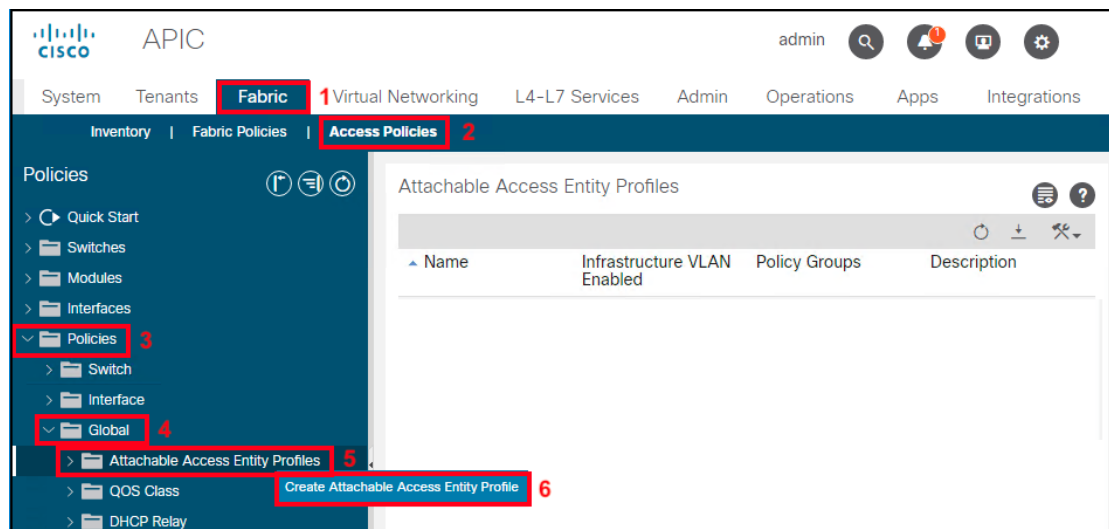
Associated Attachable Entity Profile: select a value

VLAN Pool: **SDC1-VLAN-POOL2(static)** **2**

Security Domains:

Select	Name	Description
--------	------	-------------

- 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.

Create Attachable Access Entity Profile

1. Profile

2. Association To Interfaces

STEP 1 > Profile

Name: SDC1-L3OUT 1

Description: optional

Enable Infrastructure VLAN: ☐

Domains (VMM, Physical or External) To Be Associated To Interfaces:

+ 2

Domain Profile: SDC1-L3OUT (L3) 3

Encapsulation:

4 Update Cancel

EPG DEPLOYMENT (All Selected EPGs will be deployed on all the interfaces associated.)

Application EPGs	Encap	Primary Encap	Mode

Previous

Cancel

Next 5

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

Create Attachable Access Entity Profile

1. Profile

2. Association To Interfaces

STEP 2 > Association To Interfaces

Interface Policy Group	Type	Associated Attachable Access Entity Profile	Switches / Fexes	Interfaces	Select Interfaces
SDC1-FI-A	VPC		101,102	1/47	<div><div>All</div><div>Specific</div><div>None 1</div></div>
SDC1-FI-B	VPC		101,102	1/48	<div><div>All</div><div>Specific</div><div>None 2</div></div>

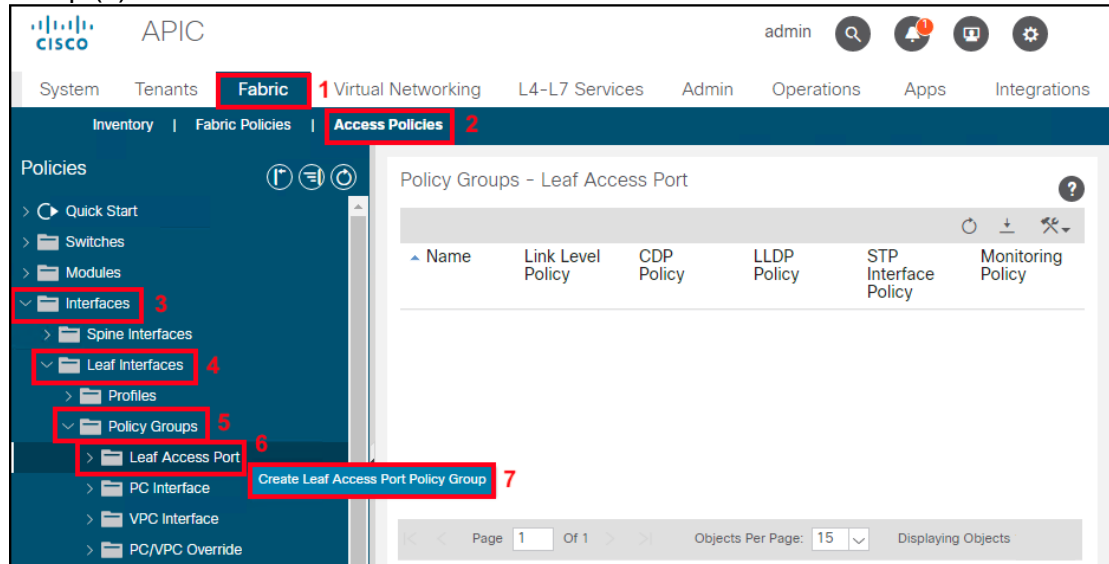
Previous

Cancel

Finish 3

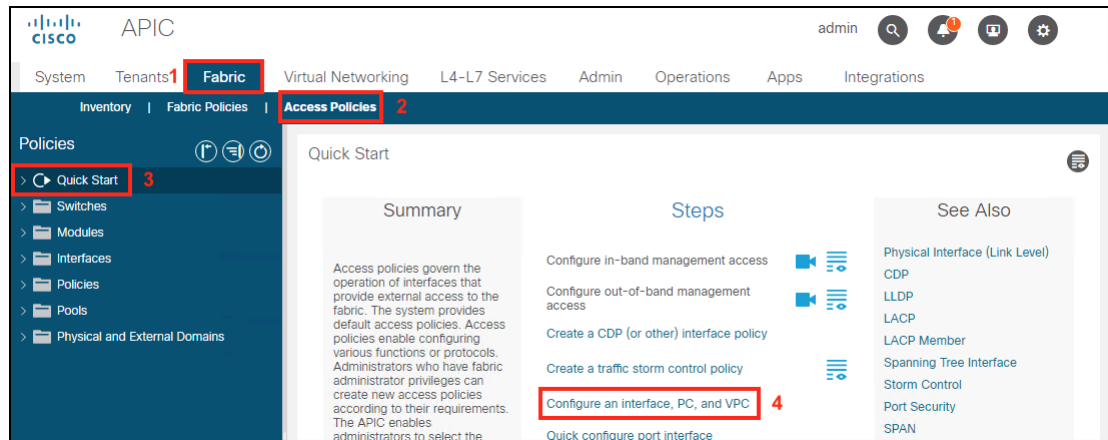
56

- 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)**.

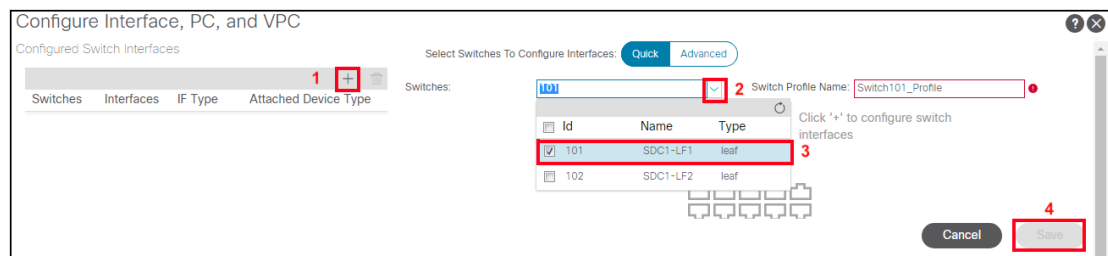


- g. Enter the **Policy Group name SDC1-L3OUT (1)**, select a **Link Level Policy 1G (2)**, select the **CDP Policy CDP-Enable (3)**, the **Attached Entity Profile SDC1-L3OUT (4)** and click **Submit**.

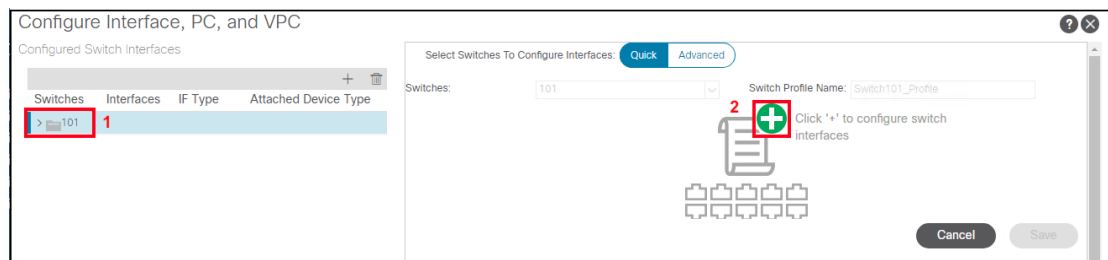
- h. Setup switch interfaces for L3Out connection. In APIC, Navigate to **Fabric (1)**->**Access Policies (2)**->**Quick Start (3)**. Select **Configure an interface, PC, and VPC (4)** under Steps.



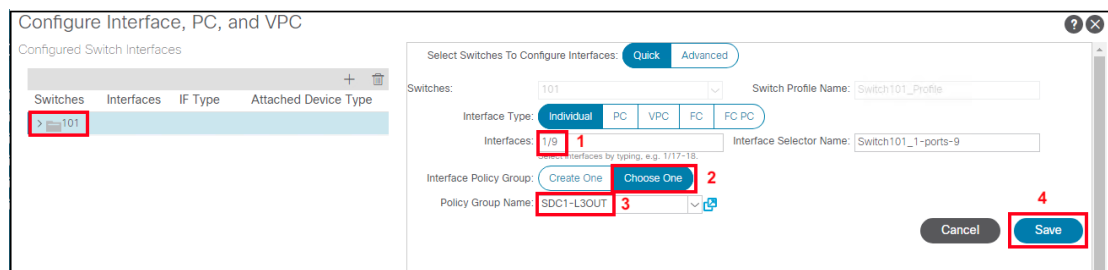
- i. Create a switch profile by clicking the **+ sign (1)** under Configured Switch Interfaces. The switch profile configuration wizard will appear on the right. From the **drop-down menu (2)**, select **switch 101 (3)** and click **Save (4)**.



- 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)**.



- 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.

The screenshot shows the APIC web interface. The top navigation bar includes 'System' (1), 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'System Settings' (2) tab is selected. On the left sidebar, 'BGP Route Reflector' (3) is highlighted. The main content area is titled 'BGP Route Reflector Policy - BGP Route Reflector'. It has tabs for 'Policy', 'Faults', and 'History'. The 'Policy' tab is active, showing a 'Properties' section with a 'Name' field set to 'default' and a 'Description' field set to 'optional'. The 'Autonomous System Number' is set to '65001' (4). Below this, there is a table for 'Route Reflector Nodes' with columns 'Pod ID', 'Node ID', 'Node Name', and 'Description'. A red box with a '+' sign (5) is next to the table header, indicating where to click to add a new node. At the bottom right, there are buttons for 'Show Usage', 'Reset', and 'Submit'.

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

The screenshot shows the 'Create Route Reflector Node' dialog box. It has a 'Spine Node' dropdown menu and a 'Description' field. The 'Description' field is open, showing a list of options: 'SDC1-SP1 Pod-1/201' (1), 'SDC1-SP2 Pod-1/202', and 'SDC1-SP3 Pod-1/203'. The first option, 'SDC1-SP1 Pod-1/201', is highlighted. At the bottom right, there are buttons for 'Cancel' and 'Submit' (2).

59

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

Create Route Reflector Node

Spine Node: SDC1-SP2

Description: SDC1-SP1 Pod-1/201

SDC1-SP2 Pod-1/202

Cancel 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)**.

APIC

admin

System Tenants **Fabric** 1 Virtual Networking L4-L7 Services Admin Operations Apps Integrations

Inventory | Fabric Policies | **Access Policies** 2

Policies

- Quick Start
- Switches
- Modules
- Interfaces** 3
 - Spine Interfaces
 - Leaf Interfaces** 4
 - Profiles
 - Policy Groups** 5
 - Leaf Access Port
 - PC Interface 6
 - VPC Interface**
 - Create VPC Interface Policy Group** 7
 - PC/VPC Override
 - Leaf Breakout Port Group
 - FC Interface
 - FC PC Interface
 - Overrides
 - Policies
 - Pools

Policy Groups - VPC Interface

Name	Link Aggregation Type	Link Level Polic	CDP Polic	MCP Polic	Port Chan	LL Pc Polic
------	-----------------------	------------------	-----------	-----------	-----------	-------------

Page 1 Of 1 Objects Per Page: 15 Displaying Objects 1 - 5 Of 5

60

- 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)**.

Create VPC Interface Policy Group

Name: **SDC1-FI-A** 1

Description: optional

Link Level Policy: select a value

CDP Policy: **CDP-Enable** 2

MCP Policy: select a value

CoPP Policy: select a value

LLDP Policy: select a value

STP Interface Policy: select a value

L2 Interface Policy: select a value

Port Security Policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Priority Flow Control Policy: select a value

Fibre Channel Interface Policy: select a value

Slow Drain Policy: select a value

MACsec Policy: select a value

Attached Entity Profile: select an option

Port Channel Policy: **LACP-Active** 3

Monitoring Policy: select a value

Storm Control Interface Policy: select a value

NetFlow Monitor Policies:

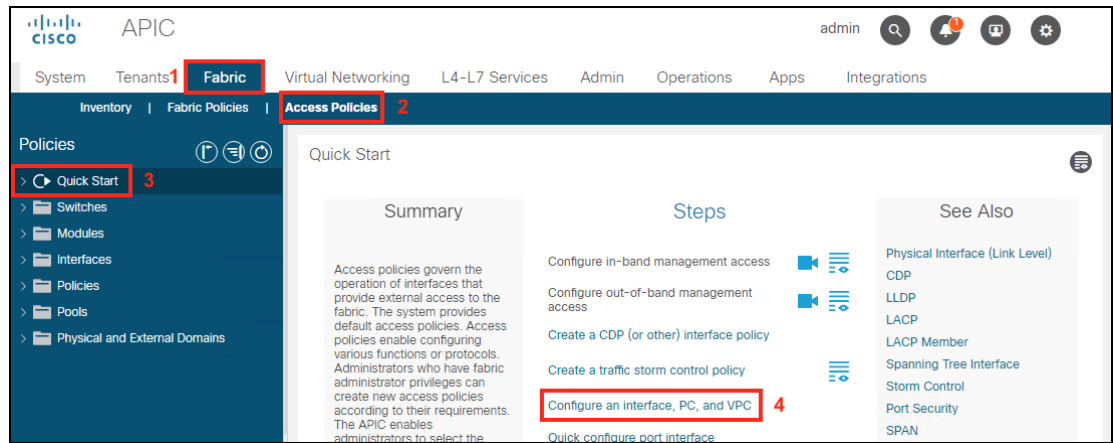
NetFlow IP Filter Type	NetFlow Monitor Policy
------------------------	------------------------

Cancel Submit 4

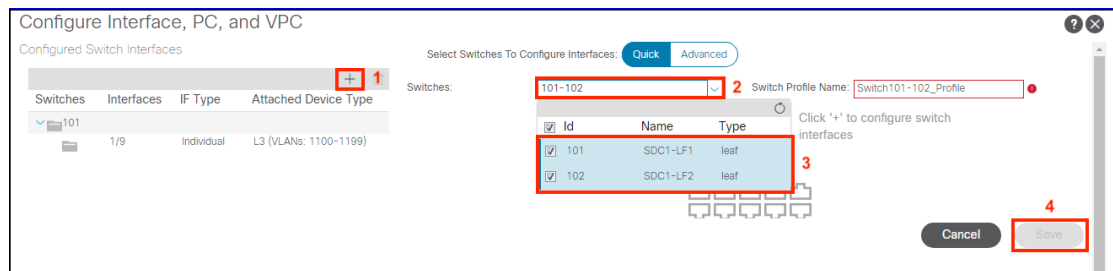
- c. Repeat steps a and b to create the VPC Interface Policy Group for SDC1-FI-B.

61

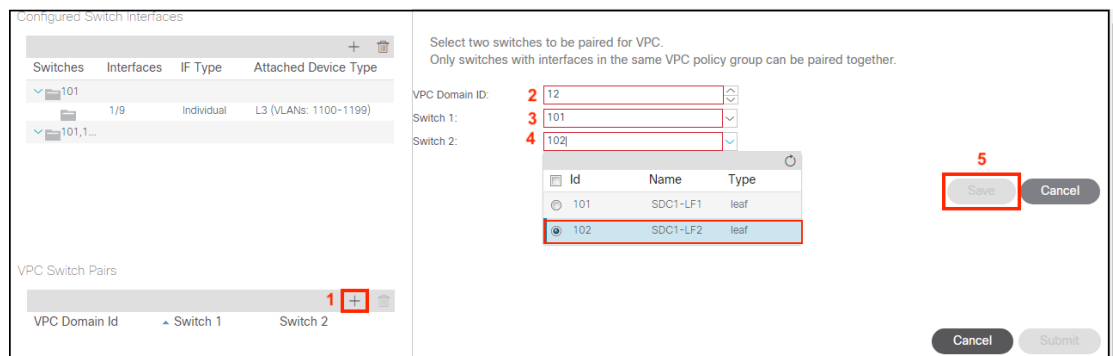
- d. Setup switch interfaces for Fabric Interconnects. In APIC, navigate to **Fabric (1)**→**Access Policies (2)**→**Quick Start (3)**. In the work pane, select **Configure an Interface, PC, and VPC (4)** under Steps



- 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)**.

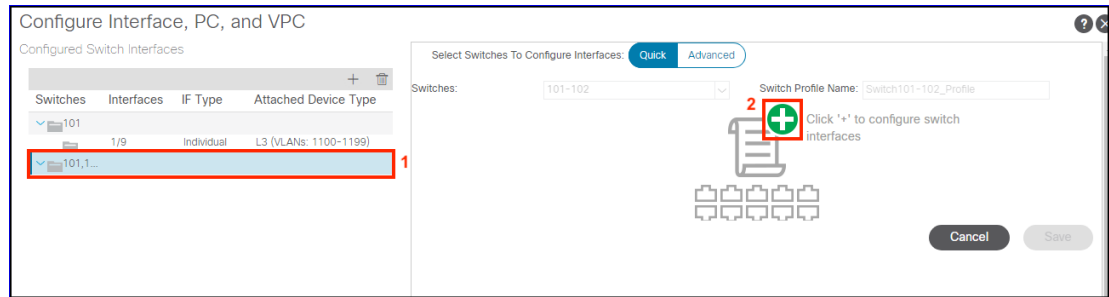


- f. Next, create the VPC Domain. Click the **+ sign (1)** in the VPC Switch Pairs section. In the work pane, for the VPC Domain ID enter **12 (2)**. From the **drop-down menu (4)**, select **switch 101 for Switch 1 (3)** and **102 for switch 2**, Click **Save (5)**

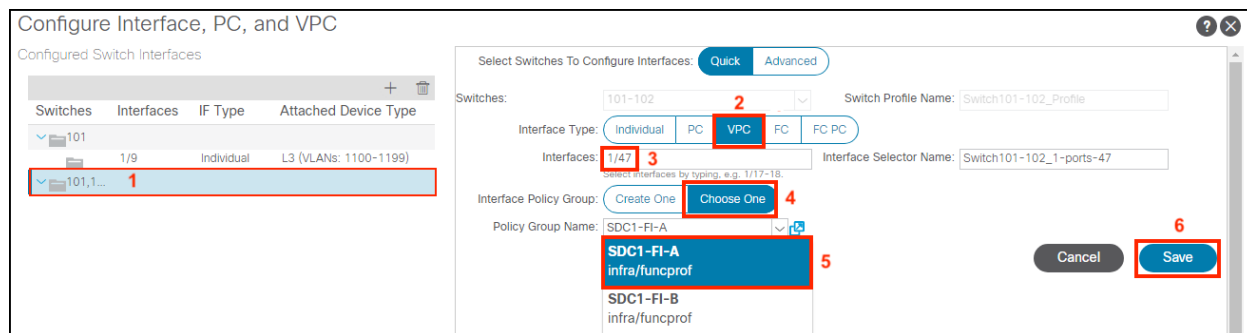


62

- 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).

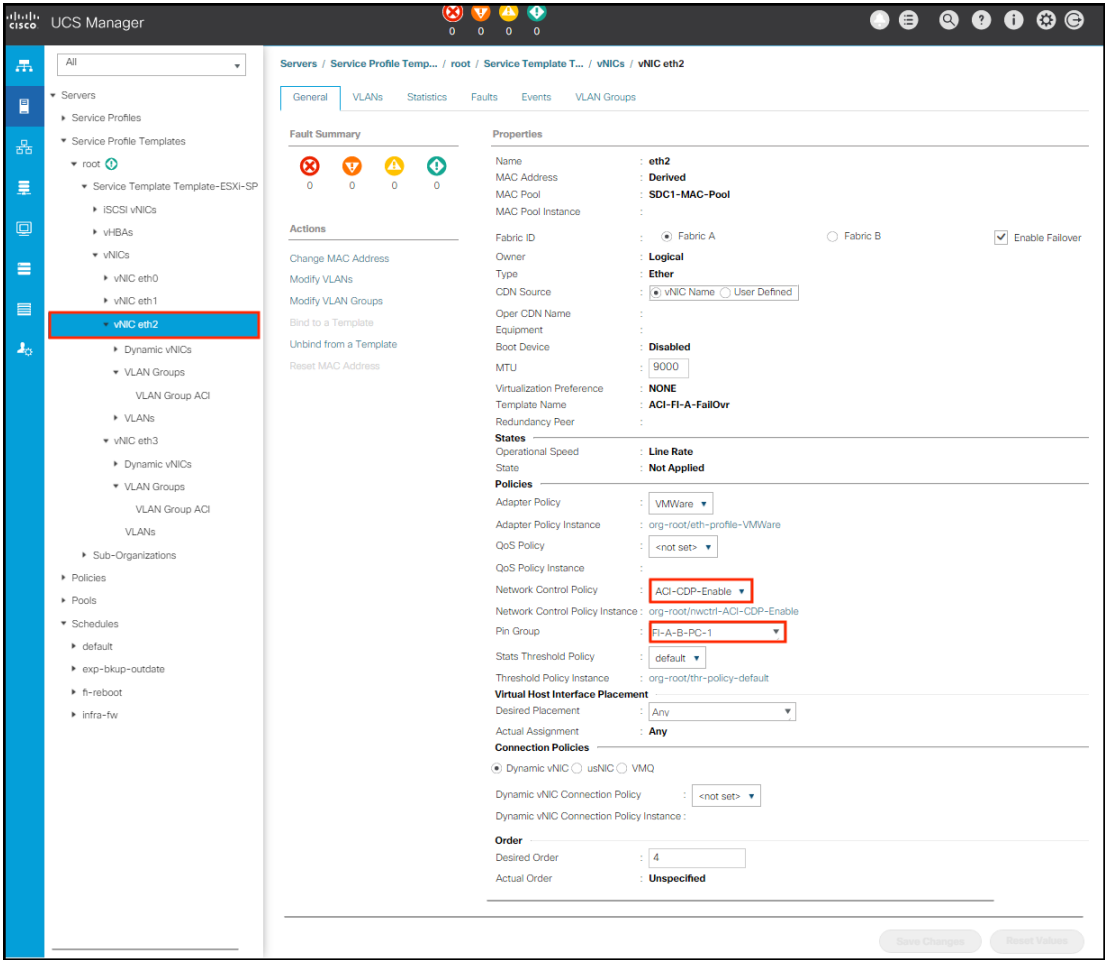


- h. In the work pane, select **VPC (1)**, select **VPC (2)**, enter the port **1/47 (3)**, select **Choose One (4)** for the Interface Policy Group, select the Policy Group Name **SDC1-FI-A (5)** and click **Save (6)**.



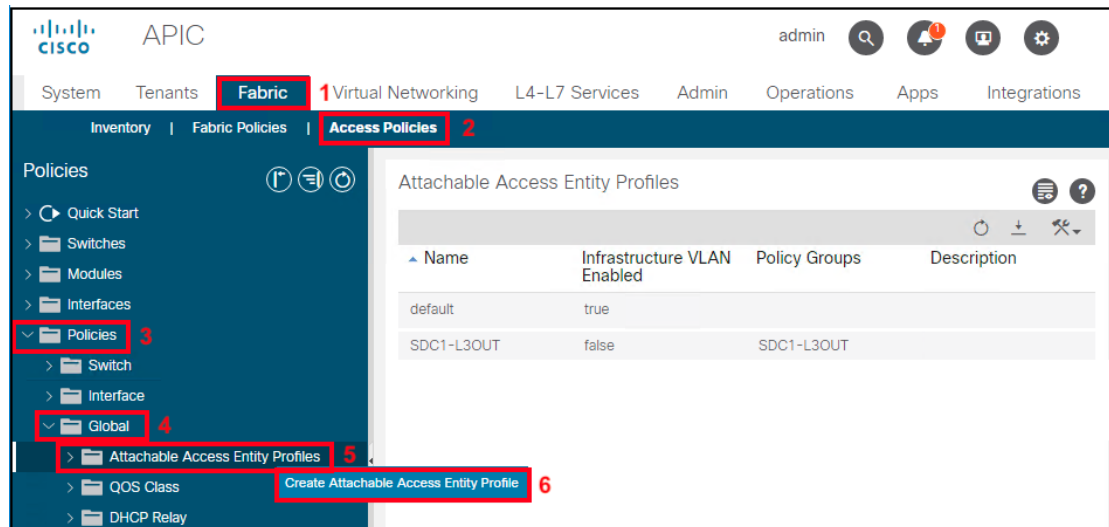
- i. Repeat steps e and f to create the VPC for SDC1-FI-B Fabric Interconnect. Choose port 1/48 and Policy Group SDC1-FI-B.

- 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.

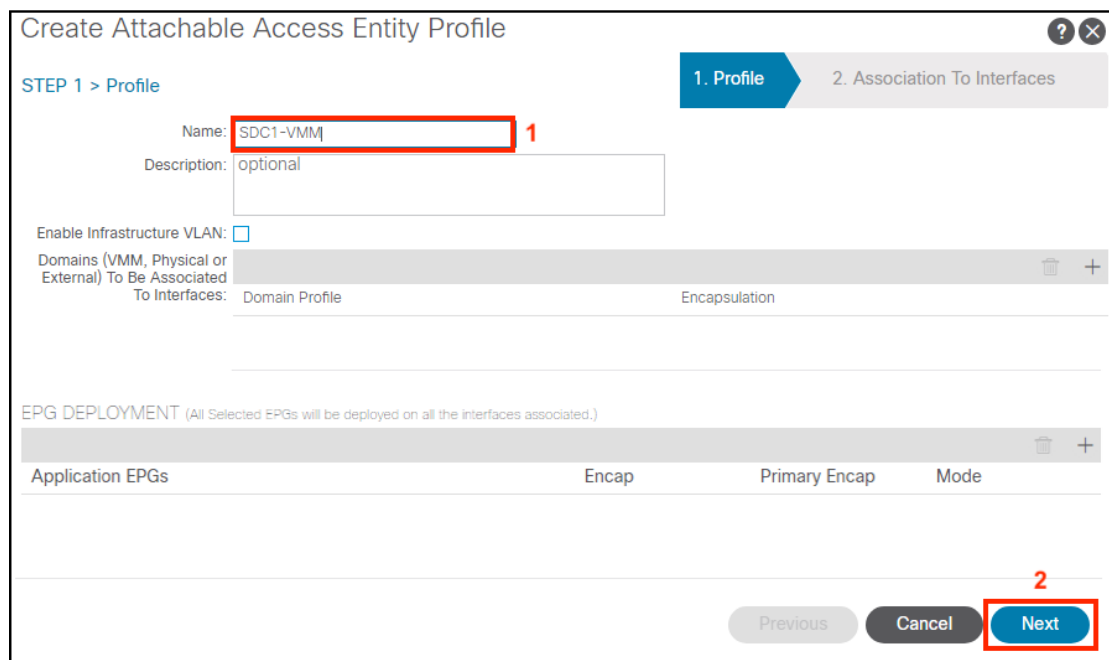


Step 7: VMM Domain

- 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)**.

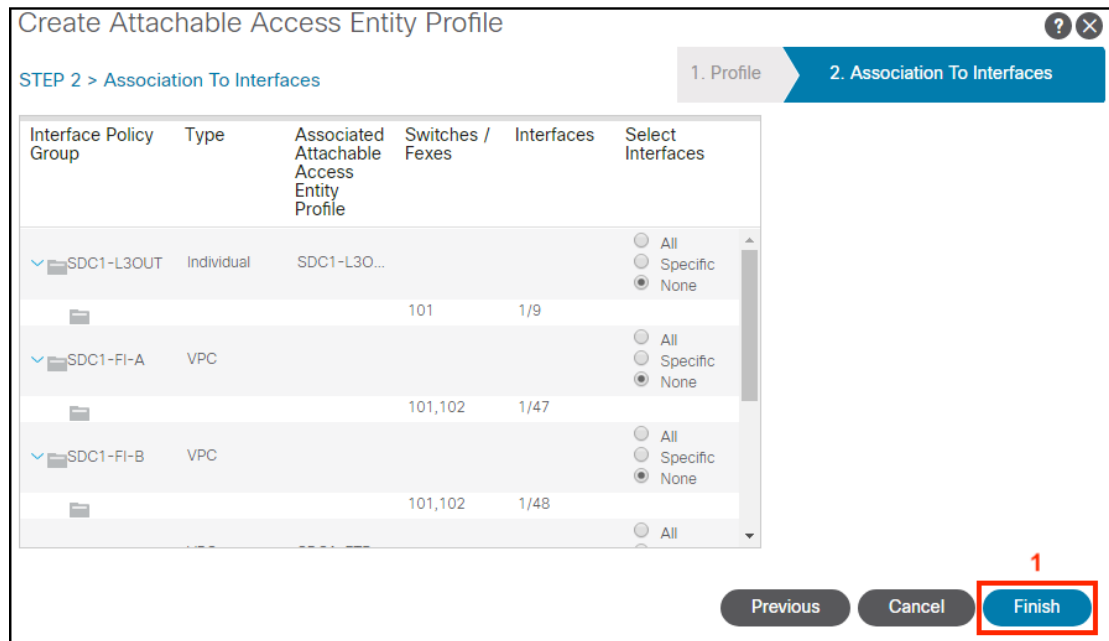


- b. Enter the Name **SDC1-VMM (1)** and Click **Next (2)**.



65

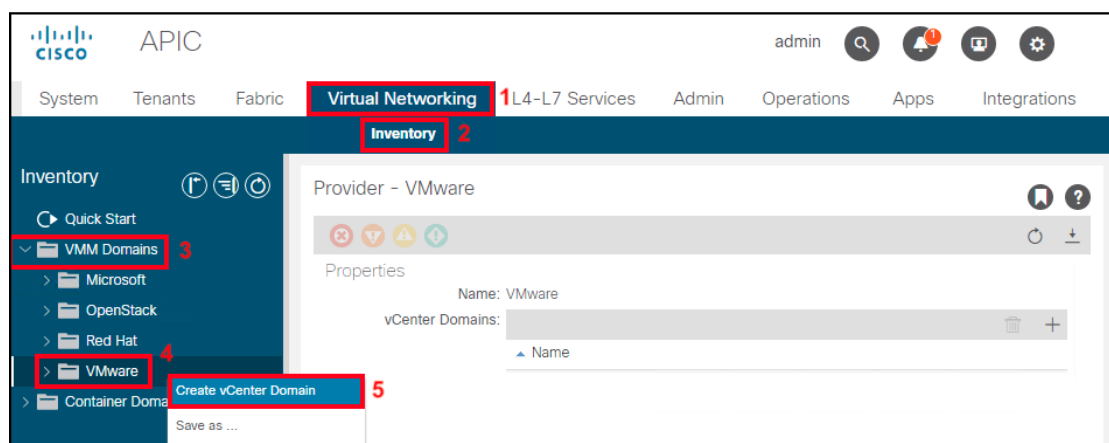
- c. Leave the Selected Interfaces as None and click **Finish (1)**.



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)**.



66

- 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)**.

Create vCenter Domain

Virtual Switch Name: SDC1-VMM 1

Virtual Switch: VMware vSphere Distributed Switch Cisco AVS Cisco AVE

Associated Attachable Entity Profile: SDC1-VMM 2

Delimiter:

Enable Tag Collection: ☒

Access Mode: Read Only Mode Read Write Mode

Endpoint Retention Time (seconds): 0

VLAN Pool: SDC1-VLAN-POOL1(dynamic) 3

Security Domains:

Name	Description
------	-------------

vCenter Credentials:

Profile Name	Username	Description
--------------	----------	-------------

vCenter:

Name	IP	Type	Stats Collection
------	----	------	------------------

Port Channel Mode: MAC Pinning+ 6

vSwitch Policy: CDP 7 LLDP Neither

NetFlow Exporter Policy: select an option

Cancel Submit 8

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

Create vCenter Credential

Name: vCenter-Admin 1

Description: optional

Username: aciadmin1@vsphere.local 2

Password: 3

Confirm Password:

Cancel OK 4

67

- 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)**.

Add vCenter Controller

vCenter Controller

Name: 1

Host Name (or IP Address): 2

DVS Version: 3

Stats Collection: ☐ Disabled ☐ Enabled

Datacenter: 4

Management EPG:

Associated Credential: 5

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 (6)**

APIC

admin

System Tenants **Fabric** 1 Virtual Networking L4-L7 Services Admin Operations Apps Integrations

Inventory | Fabric Policies | **Access Policies** 2

Policies

- Quick Start
- Switches
- Modules
- Interfaces
- Policies** 3
 - Switch
 - Interface
 - Global** 4
 - Attachable Access Entity Profiles** 5
 - Create Attachable Access Entity Profile 6
 - QOS Class
 - DHCP Relay

Attachable Access Entity Profiles

Name	Infrastructure VLAN Enabled	Policy Groups	Description
default	true		
SDC1-VMM	false		
SDC1-L3OUT	false	SDC1-L3OUT	

68

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

Create Attachable Access Entity Profile

STEP 1 > Profile

1. Profile 2. Association To Interfaces

Name: SDC1-FTD-C1 (1)

Description: optional

Enable Infrastructure VLAN: ☐

Domains (VMM, Physical or External) To Be Associated To Interfaces:

Domain Profile	Encapsulation
phys (Physical) (3)	

Update (4) Cancel

EPG DEPLOYMENT (All Selected EPGs will be deployed on all the interfaces associated.)

Application EPGs	Encap	Primary Encap	Mode

Previous Cancel 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).

APIC

admin

System Tenants **Fabric** (1) Virtual Networking L4-L7 Services Admin Operations Apps Integrations

Inventory | Fabric Policies | **Access Policies** (2)

Policies

- Quick Start
- Switches
- Modules
- Interfaces** (3)
 - Spine Interfaces
 - Leaf Interfaces** (4)
 - Profiles
 - Policy Groups** (5)
 - Leaf Access Port
 - PC Interface (6)
 - VPC Interface**
 - Create VPC Interface Policy Group (7)
 - PC/VPC Override
 - Leaf Breakout Port Group
 - FC Interface
 - FC PC Interface
 - Overrides
 - Policies
 - Pools

Policy Groups - VPC Interface

Name	Link Aggregation Type	Link Level Polic	CDP Polic	MCP Polic	Port Chan Polic	LL Chan Polic
SDC1-FI-A	vpc	C...			L...	
SDC1-FI-B	vpc	C...			L...	

Page 1 Of 1 Objects Per Page: 15 Displaying Objects 1 - 5 Of 5

- 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).

Create VPC Interface Policy Group

Name: SDC1-FTD1-CCL

Description: optional

Link Level Policy: select a value

CDP Policy: select a value

MCP Policy: select a value

CoPP Policy: select a value

LLDP Policy: select a value

STP Interface Policy: select a value

L2 Interface Policy: select a value

Port Security Policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Priority Flow Control Policy: select a value

Fibre Channel Interface Policy: select a value

Slow Drain Policy: select a value

MACsec Policy: select a value

Attached Entity Profile: SDC1-FTD-C1

Port Channel Policy: LACP-Active

Monitoring Policy: select a value

Storm Control Interface Policy: select a value

NetFlow Monitor Policies:

NetFlow IP Filter Type

NetFlow Monitor Policy

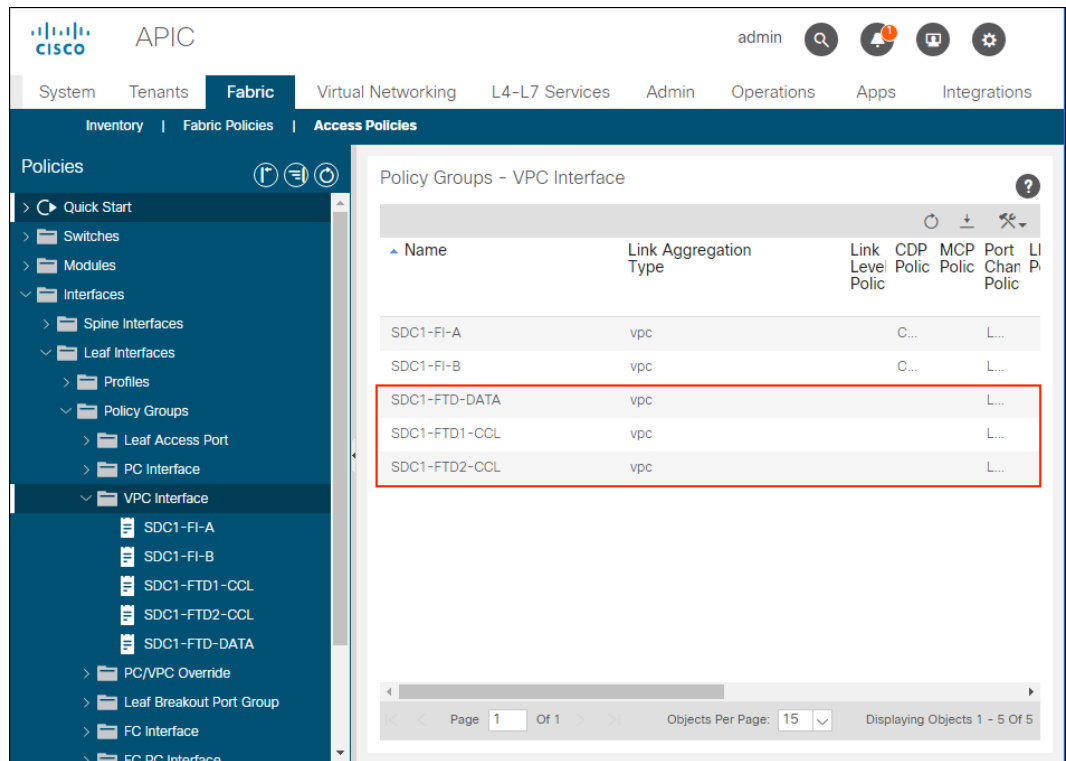
Cancel

Submit

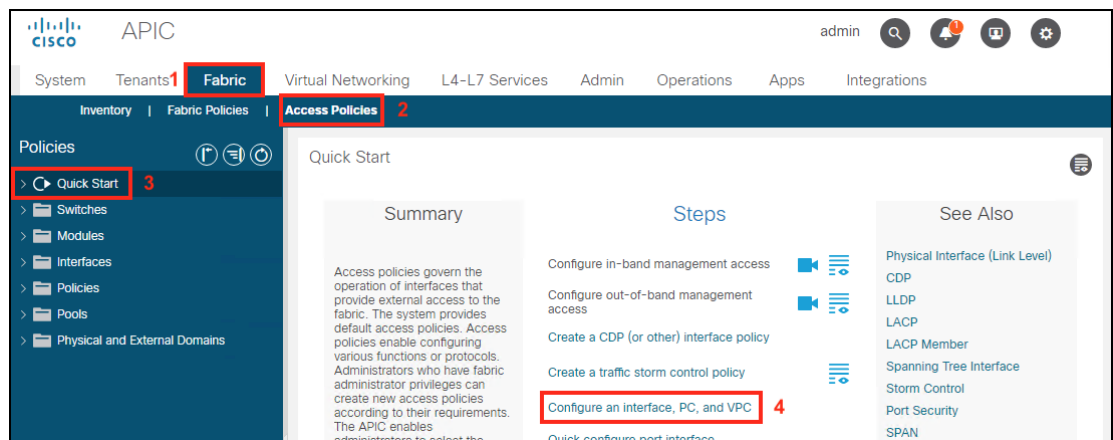
70

- 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.

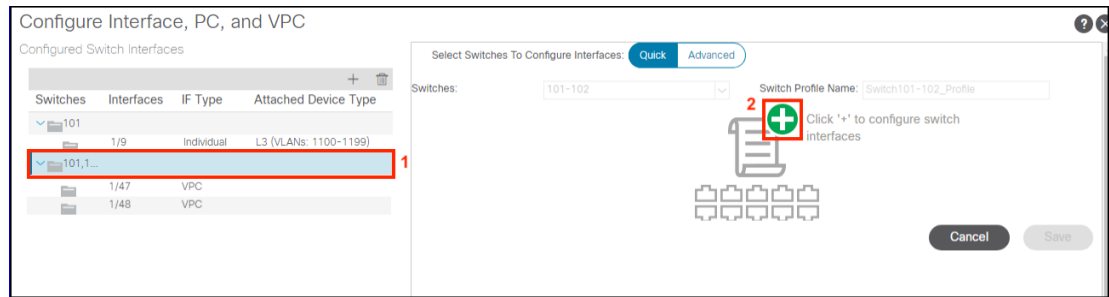


- f. Setup switch interfaces for L3Out connection. In APIC, Navigate to **Fabric (1)**->**Access Policies (2)**->**Quick Start (3)**. Select **Configure an interface, PC, and VPC (4)** under Steps.

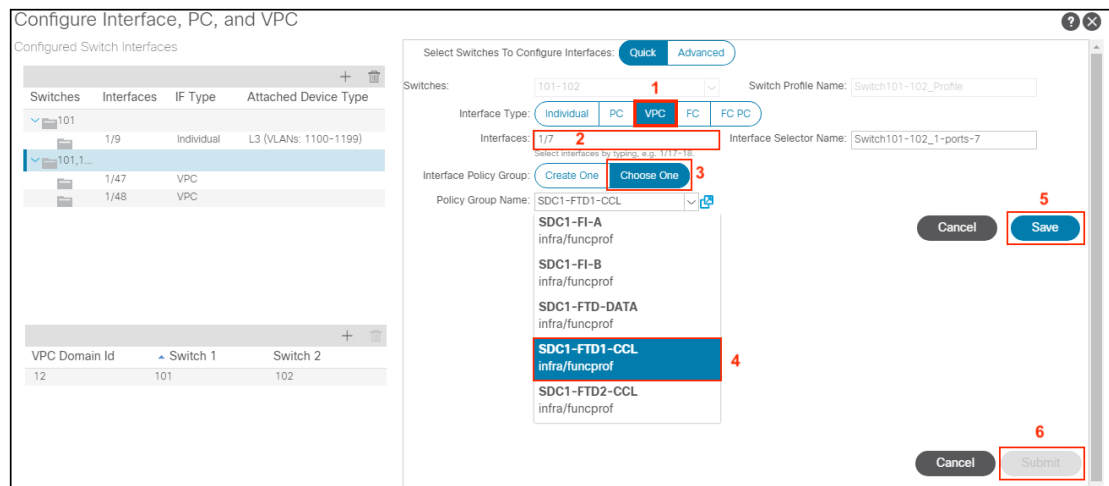


71

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



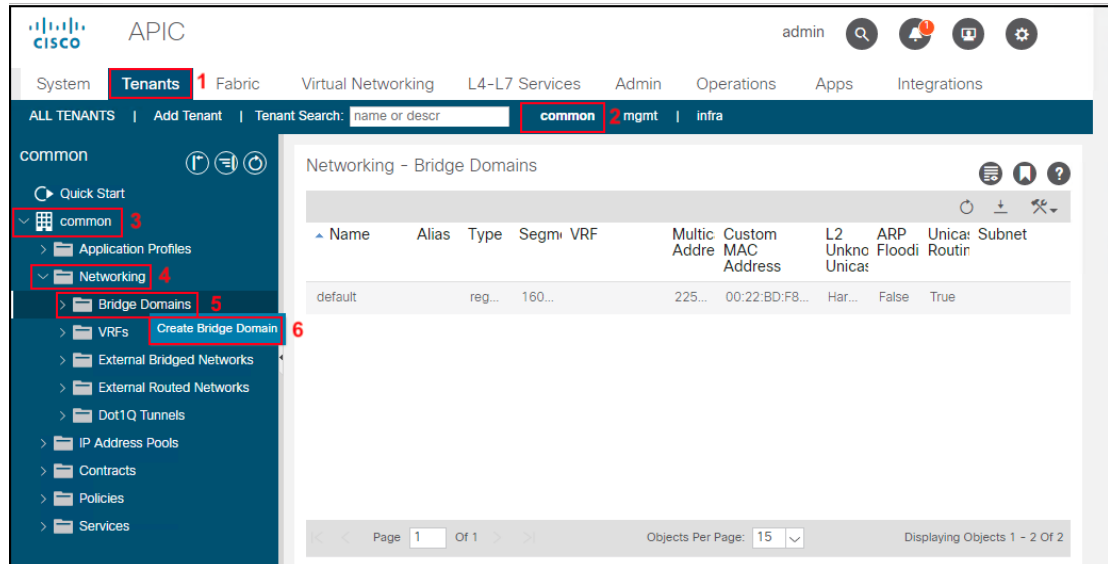
- h. Select **Interface Type VPC (1)** and enter **Interface 1/7 (2)**. Click **Choose One (3)** for the Interface Policy Group and select the **Policy Group Name SDC1-FTD1-CCL (4)** from the drop-down menu. Click **Save (5)** and **Submit (6)**



- 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.

72

- 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)**

The screenshot shows the 'Create Bridge Domain' configuration page. The page has three tabs: '1. Main' (active), '2. L3 Configurations', and '3. Advanced/Troubleshooting'. Under the 'Main' tab, the 'Name' field is populated with 'SDC1-FTD-CCL' (labeled 1). Other fields include 'Alias', 'Description' (optional), 'Tags' (with a dropdown), 'Type' (radio buttons for 'fc' and 'regular'), 'Advertise Host Routes' (checkbox), 'VRF' (dropdown), 'Forwarding' (dropdown), 'Endpoint Retention Policy' (dropdown), 'IGMP Snoop Policy' (dropdown), and 'MLD Snoop Policy' (dropdown). At the bottom right, there are three buttons: 'Previous', 'Cancel', and 'Next' (labeled 2 and highlighted with a red box).

73

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

Create Bridge Domain

STEP 2 > L3 Configurations

1. Main 2. L3 Configurations 3. Advanced/Troubleshooting

Unicast Routing: ☒ Enabled **1**

ARP Flooding: ☐ Enabled

Config BD MAC Address: ☒

MAC Address: 00:22:BD:F8:19:FF

Subnets:

Gateway Address	Scope	Primary IP Address	Subnet Control
-----------------	-------	--------------------	----------------

IP Data-plane Learning: ☐ no ☒ yes

Limit IP Learning To Subnet: ☒

DHCP Labels:

Name	Scope	DHCP Option Policy
------	-------	--------------------

Associated L3 Outs:

L3 Out

Previous Cancel **Next** **2**

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

Create Bridge Domain

STEP 3 > Advanced/Troubleshooting

1. Main 2. L3 Configurations 3. Advanced/Troubleshooting

Monitoring Policy: select a value

First Hop Security Policy: select a value

Optimize WAN Bandwidth: ☐

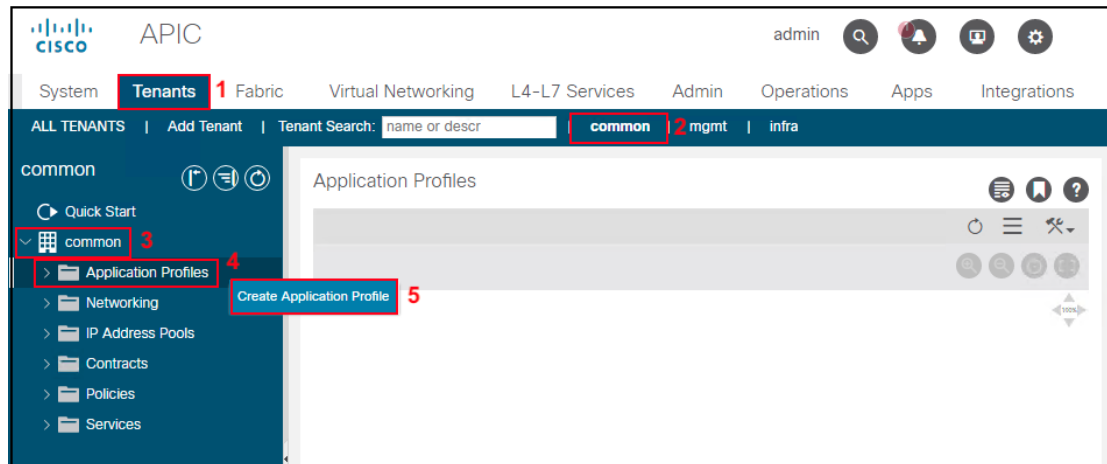
NetFlow Monitor Policies:

NetFlow IP Filter Type	NetFlow Monitor Policy
------------------------	------------------------

Previous Cancel **Finish** **1**

74

- 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)**.

The screenshot shows the 'Create Application Profile' form. The 'Name' field is 'SDC1-FTD-CCL' (labeled 1). The 'Alias' field is empty. The 'Description' field is 'optional'. The 'Tags' field is empty. The 'Monitoring Policy' is 'select a value'. Below the form is a table of EPGs (labeled 2). The table has columns: Name, Alias, BD, Domain, Switching Mode, Static Path, Static Path VLAN, Provided Contract, and Consumed Contract. The first row is highlighted, showing 'SDC1-FTD-CCL' (labeled 2), an empty Alias, 'SDC1-FTD' (labeled 3), 'phys (Phys)' (labeled 4), and an empty Switching Mode. Below the table are 'Update' (labeled 5) and 'Cancel' buttons. At the bottom right are 'Cancel' and 'Submit' (labeled 6) buttons.

Name	Alias	BD	Domain	Switching Mode	Static Path	Static Path VLAN	Provided Contract	Consumed Contract
SDC1-FTD-CCL		SDC1-FTD	phys (Phys)		102/1/1,102/110/1		select an o	select an o

- 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.

Interface	Type	Admin ...	Operation...	Insta...	VLAN	Admin Dup...	Auto Nego...	Operation ...	Admin State
MGMT	Management								<input checked="" type="checkbox"/>
Port-channel1	data	10gbps	10gbps	SDC1-F...		Full Duplex	no	up	<input checked="" type="checkbox"/>
Port-channel48	cluster	10gbps	10gbps	SDC1-F...		Full Duplex	no	up	<input checked="" type="checkbox"/>
Ethernet1/7								up	<input checked="" type="checkbox"/>
Ethernet1/8								up	<input checked="" type="checkbox"/>
Ethernet1/3	mgmt	10gbps	10gbps	SDC1-F...		Full Duplex	no	up	<input checked="" type="checkbox"/>
Ethernet1/4	data	10gbps	10gbps			Full Duplex	no	admin-down	<input checked="" type="checkbox"/>
Ethernet1/5	data	10gbps	10gbps			Full Duplex	no	admin-down	<input checked="" type="checkbox"/>
Ethernet1/6	data	10gbps	10gbps			Full Duplex	no	admin-down	<input checked="" type="checkbox"/>
Ethernet2/1	data	40gbps	40gbps			Full Duplex	no	sfp-not-pres...	<input checked="" type="checkbox"/>

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

Name	Model	Ver...	Chassis	Licenses	Access Control P...
SDC1-FTD-C1 Cluster					
sdc1-ftd-1(Master) 10.16.6.51 - Routed	FTD on Firepower 9300 SM-36	6.4.0	SDC1-FTD-1.cisco-x.com:4	Base, Threat (2 more...)	SDC-Multisite-FTD-C1
sdc1-ftd-2 10.16.6.52 - Routed	FTD on Firepower 9300 SM-36	6.4.0	SDC1-FTD-2.cisco-x.com:4	Base, Threat (2 more...)	SDC-Multisite-FTD-C1
SDC2-FTD-C1 Cluster					
sdc2-ftd-1(Master) 10.17.6.51 - Routed	FTD on Firepower 4110	6.4.0	SDC2-FTD-1.cisco-x.com:4	Base, Threat (2 more...)	SDC-Multisite-FTD-C1
sdc2-ftd-2 10.17.6.52 - Routed	FTD on Firepower 4110	6.4.0	SDC2-FTD-2.cisco-x.com:4	Base, Threat (2 more...)	SDC-Multisite-FTD-C1

76

- 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.

The screenshot shows the 'Logical Device List' in the FCM interface. The 'Security Module 1,2,3' is clustered. The first instance, SDC1-FTD1, is highlighted with a red box. Its status is 'online'. The 'Attributes' section shows 'CLUSTER-ROLE' as 'master'.

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.4.0.102		10.16.6.51	10.16.4.1	Ethernet1/3	online
Interface Name Port-channel1 Port-channel48						
Type data cluster						
Attributes Cluster Operational Status : in-cluster FIREPOWER-MGMT-IP : 10.16.6.51 CLUSTER-ROLE : master CLUSTER-IP : 127.2.1.1 MGMT-URL : https://10.9.10.41/ UUID : 0a837a74-a0ad-11e8-bc2e-8c84775ccdb						
FTD	6.2.3.83		10.16.6.53	10.16.4.1	Ethernet1/3	Security module not pres...
Interface Name Port-channel1 Port-channel48						
Type data cluster						
FTD	6.2.3.83		10.16.6.55	10.16.4.1	Ethernet1/3	Security module not pres...
Interface Name Port-channel1 Port-channel48						
Type data cluster						

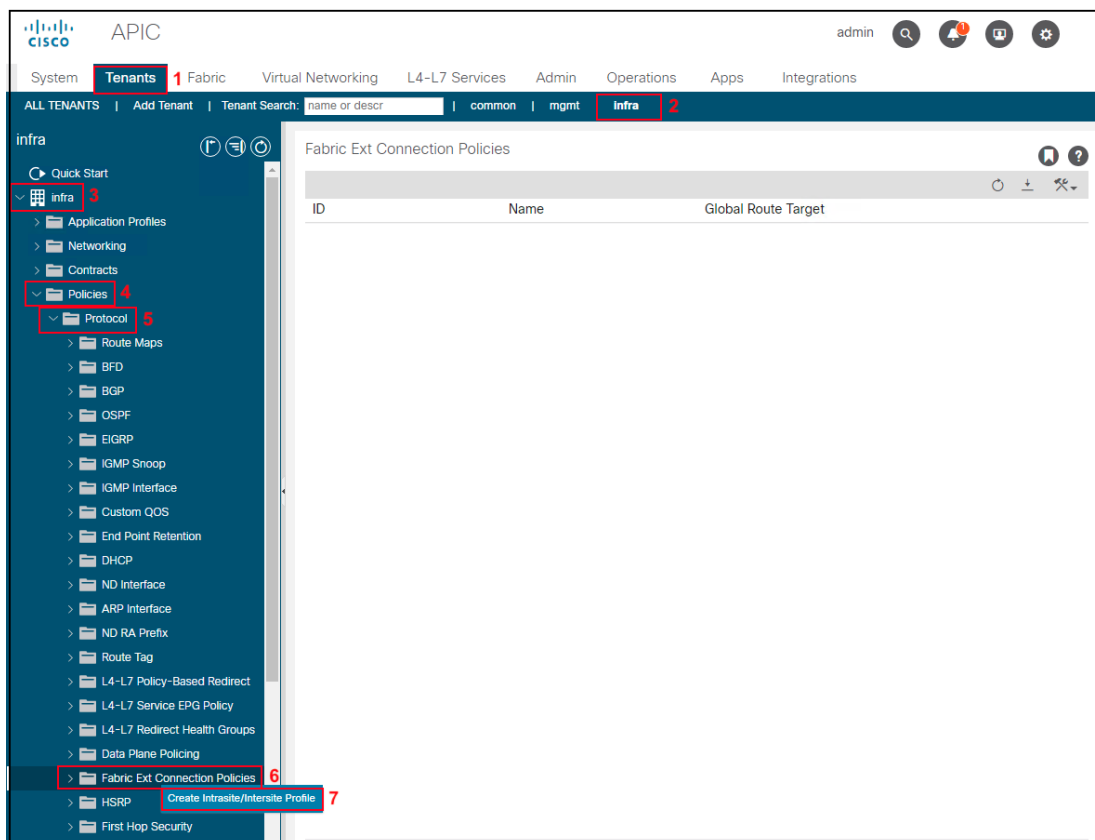
SDC1-FTD2 is the slave

The screenshot shows the 'Logical Device List' in the FCM interface. The first instance, SDC1-FTD1, is highlighted with a red box. Its status is 'online'. The 'Attributes' section shows 'CLUSTER-ROLE' as 'slave'.

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.4.0.102		10.16.6.52	10.16.4.1	Ethernet1/3	online
Interface Name Port-channel1 Port-channel48						
Type data cluster						
Attributes Cluster Operational Status : in-cluster FIREPOWER-MGMT-IP : 10.16.6.52 CLUSTER-ROLE : slave CLUSTER-IP : 127.2.2.1 MGMT-URL : https://10.9.10.41/ UUID : cb5d8bb6-a0af-11e8-8413-89a8e6bb6f7e						
FTD	6.2.3.83		10.16.6.54	10.16.4.1	Ethernet1/3	Security module not present
FTD	6.2.3.83		10.16.6.56	10.16.4.1	Ethernet1/3	Security module not present

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)**.



78

- 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).

The screenshot shows the 'Create Intrasite/Intersite Profile' form. The form is titled 'Create Intrasite/Intersite Profile' and has a close button (X) and a help button (?). The form is divided into several sections:

- Fabric ID:** 1
- Name:** (empty text field)
- Community:** extended:as2-nn4:5:16 (1) (highlighted with a red box). Below it, an example is shown: Ex: extended:as2-nn4:5:16.
- Site/Pod Peering Profile:**
 - Peering Type:** Full Mesh (selected) and Route Reflector (unselected).
 - Password:** (empty text field)
 - Confirm Password:** (empty text field)
- Pod Connection Profile:** (2) (highlighted with a red box). It contains a table with two columns: Pod ID and Dataplane TEP.

Pod ID	Dataplane TEP
1	10.21.100.100/32 (3) (highlighted with a red box)

Below the table, there are two buttons: Update (4) (highlighted with a red box) and Cancel.
- Fabric External Routing Profile:** (5) (highlighted with a red box). It contains a table with two columns: Name and Subnet.

Name	Subnet
------	--------

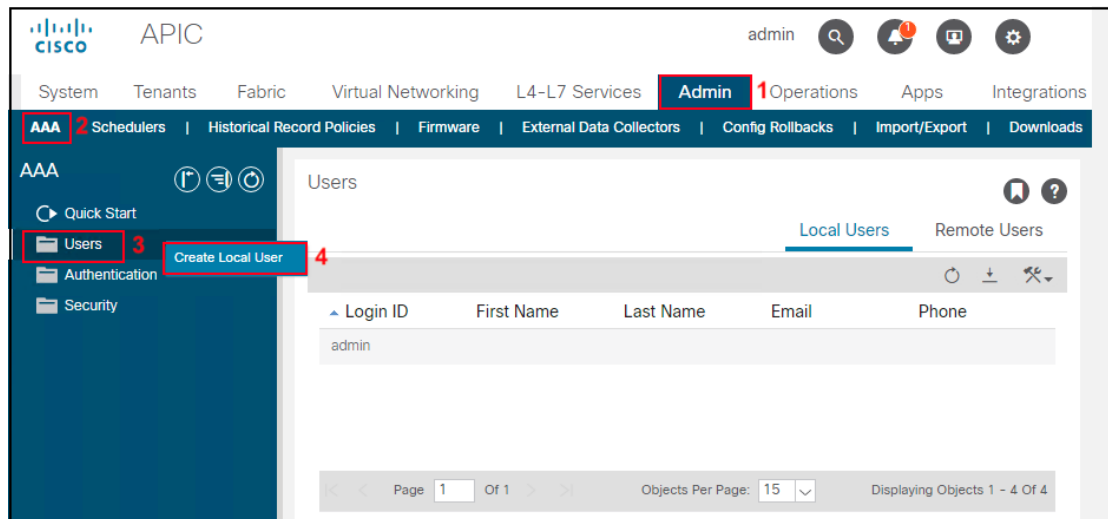
At the bottom of the form, there are two buttons: Cancel and Submit (5) (highlighted with a red box).

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)**.

Create Local User

STEP 1 > User Identity

1. User Identity | 2. Security | 3. Roles

Login ID: mso-admin (1)

Password: (2)

Confirm Password: (2)

First Name: _____

Last Name: _____

Phone: _____

Email: _____

User Certificate Attribute: _____

Description: optional

Account Status: ☒ Active ☐ Inactive

Account Expires: ☒ No ☐ Yes

Previous Cancel **Next (3)**

80

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

STEP 2 > Security

1. User Identity 2. Security 3. Roles

Security Domain:

<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	all	
<input type="checkbox"/>	common	
<input type="checkbox"/>	mgmt	

1

User Certificates:

Name	Expiration Date	State
------	-----------------	-------

SSH Keys:

Name	Key
------	-----

Previous Cancel 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)**.

Create Local User

STEP 3 > Roles

1. User Identity 2. Security 3. Roles

Domain all:

Role Name Role Privilege Type

admin 2 Write 3

4 Update Cancel

Previous Cancel Finish

5

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)	<ul style="list-style-type: none">• 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

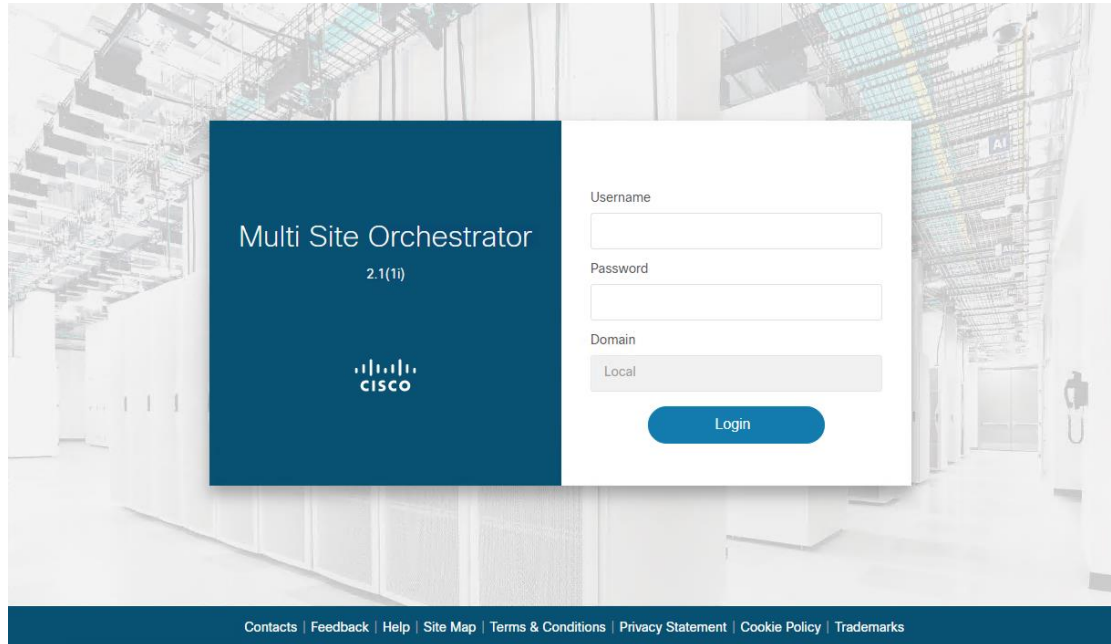
Note: In step 2 in the link above, use the root account when logging into MSO with SSH.

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

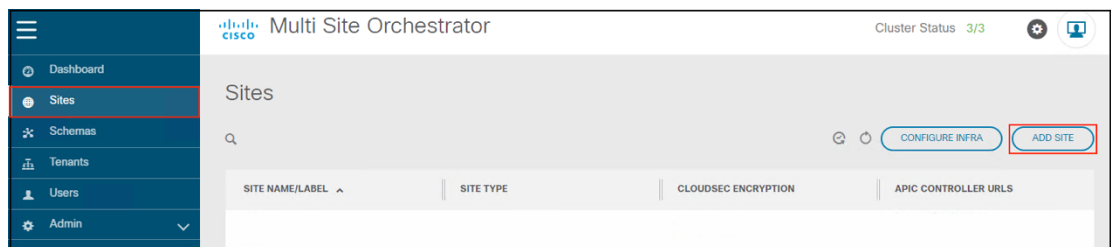
https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211_chapter_011.html

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**



83

- 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**.

Add Site

Connection Settings

* NAME
San Francisco

LABELS
Select or Create a Label.

* APIC CONTROLLER URL
https://10.16.1.11
https://10.16.1.12
https://10.16.1.13

+ APIC CONTROLLER URL

* USERNAME
mso-admin

* PASSWORD

SPECIFY LOGIN DOMAIN FOR SITE
Off

* APIC SITE ID
1

> GEOGRAPHICAL LOCATION

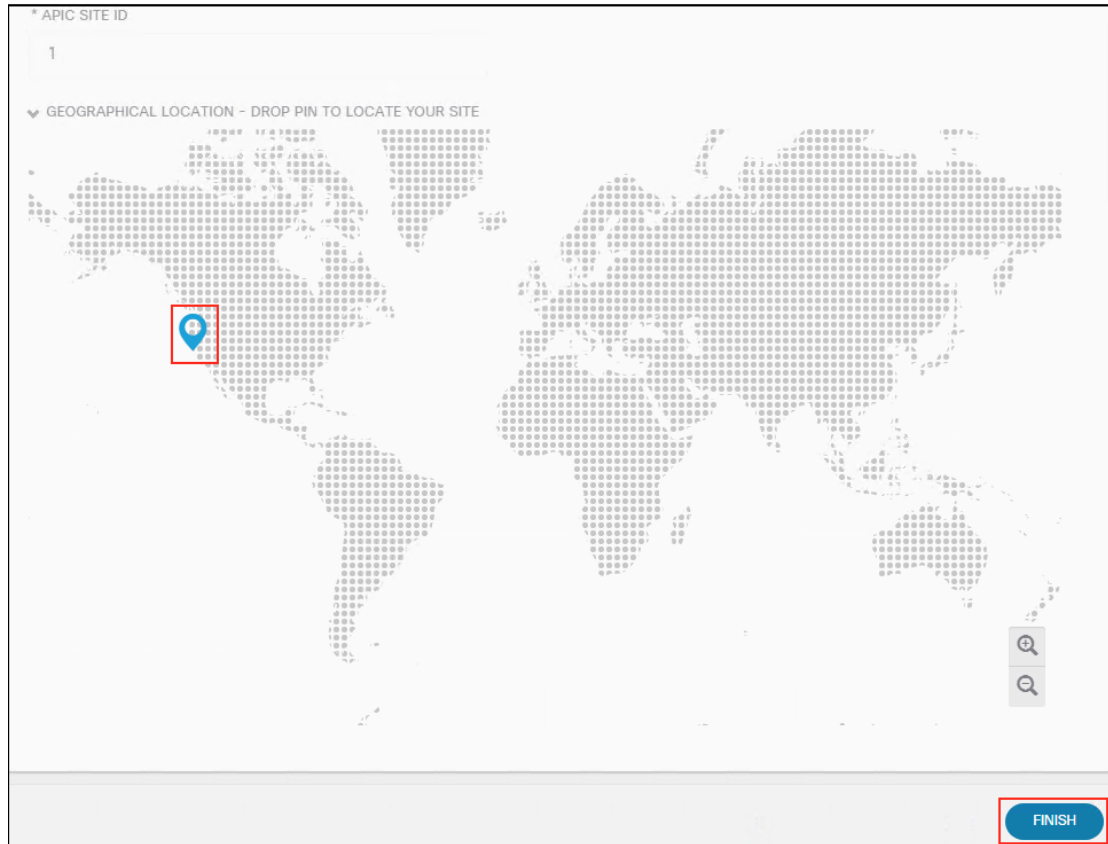
SAVE

- d. Drop a pin on the San Francisco location on a map and click **FINISH**.

* APIC SITE ID

1

▼ GEOGRAPHICAL LOCATION - DROP PIN TO LOCATE YOUR SITE



12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

1357

1358

1359

1360

1361

1362

1363

1364

1365

1366

1367

1368

1369

1370

1371

1372

1373

1374

1375

1376

1377

1378

1379

1380

1381

1382

1383

1384

1385

1386

1387

1388

1389

1390

1391

1392

1393

1394

1395

1396

1397

1398

1399

1400

1401

1402

1403

1404

1405

1406

1407

1408

1409

1410

1411

1412

1413

1414

1415

1416

1417

1418

1419

1420

1421

1422

1423

1424

1425

1426

1427

1428

1429

1430

1431

1432

1433

1434

1435

1436

1437

1438

1439

1440

1441

1442

1443

1444

1445

1446

1447

1448

1449

1450

1451

1452

1453

1454

1455

1456

1457

1458

1459

1460

1461

1462

1463

1464

1465

1466

1467

1468

1469

1470

1471

1472

85

- 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.

Add Site

Connection Settings

* NAME
New York

LABELS
Select or Create a Label.

* APIC CONTROLLER URL
https://10.17.1.11

https://10.17.1.12

https://10.17.1.13

APIC CONTROLLER URL

* USERNAME
mso-admin

* PASSWORD

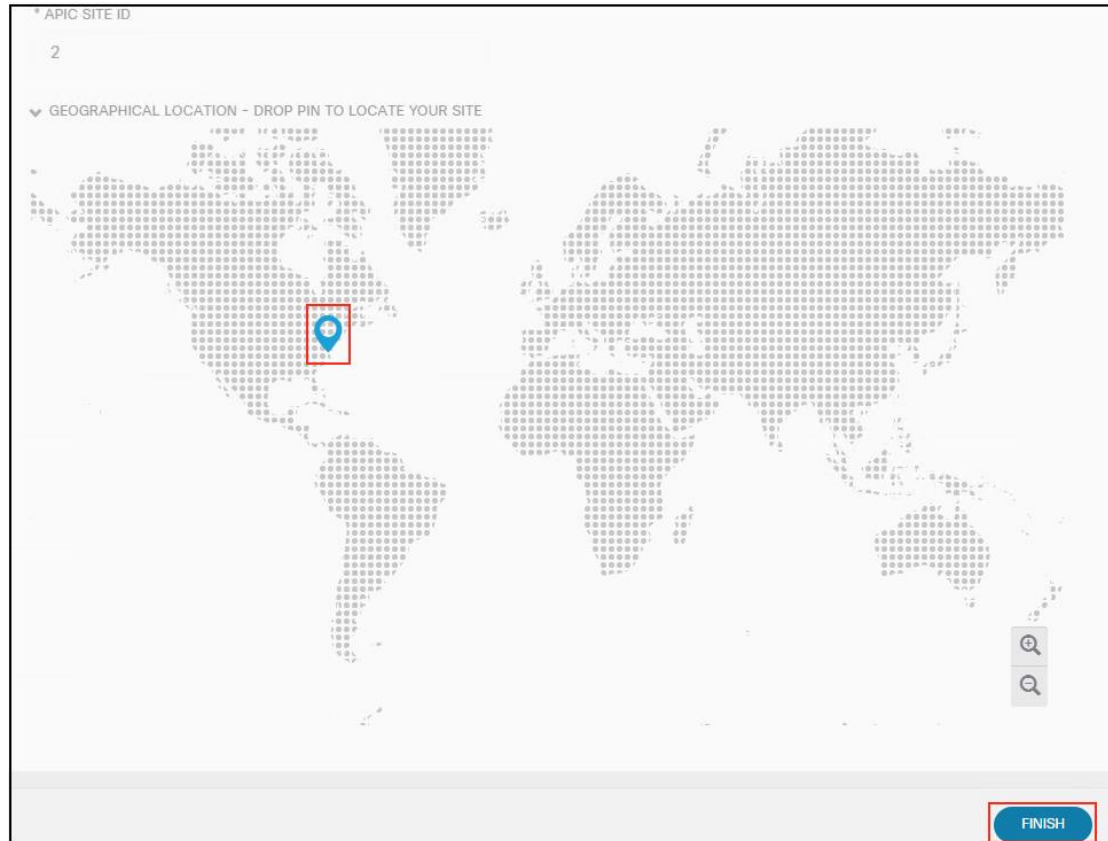
SPECIFY LOGIN DOMAIN FOR SITE
Off

* APIC SITE ID
2

GEOGRAPHICAL LOCATION

SAVE

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

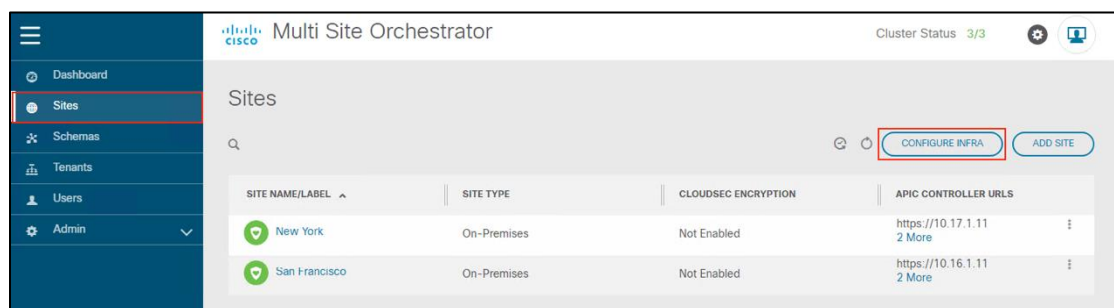


Step 3: Configure Fabric Connectivity Infrastructure (Infra) in MSO GUI

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**.



87

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

The screenshot shows the 'Fabric Connectivity Infra' application interface. The left sidebar contains a 'SETTINGS' section with 'General Settings' highlighted in blue, and a 'SITES' section listing 'San Francisco' and 'New York', both marked as 'DISABLED'. The main content area is titled 'Control Plane BGP' and contains the following settings:

- BGP PEERING TYPE:** A dropdown menu set to 'full-mesh'.
- KEEPALIVE INTERVAL (SECONDS):** A text input field containing '60'.
- HOLD INTERVAL (SECONDS):** A text input field containing '180'.
- STALE INTERVAL (SECONDS):** A text input field containing '300'.
- GRACEFUL HELPER:** A toggle switch that is turned 'On'.
- MAXIMUM AS LIMIT:** A text input field containing '0'.
- BGP TTL BETWEEN PEERS:** A text input field containing '16'.

88

- 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.

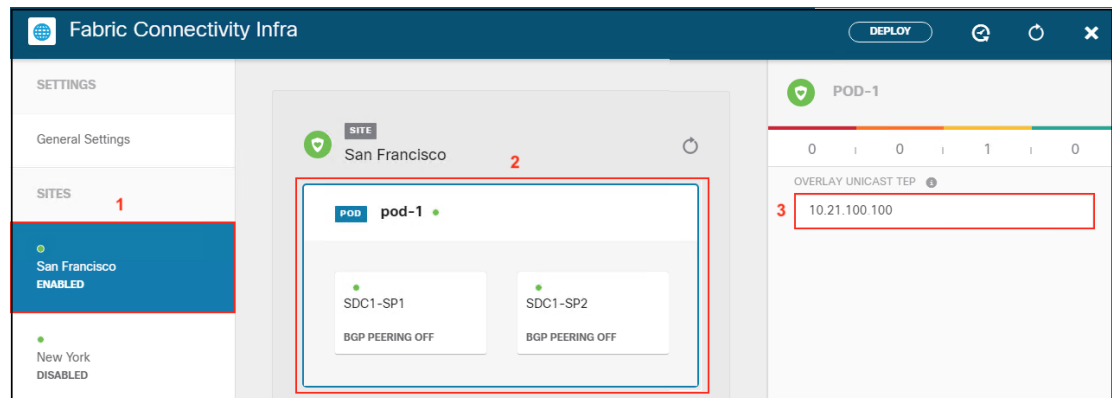
The screenshot displays the 'Fabric Connectivity Infra' web interface. On the left, the 'SITES' panel (labeled 1) shows 'San Francisco' as 'ENABLED' and 'New York' as 'DISABLED'. The main area (labeled 2) shows the 'San Francisco' site configuration, including a 'POD pod-1' and two switches, 'SDC1-SP1' and 'SDC1-SP2', both with 'BGP PEERING OFF'. On the right, the 'SAN FRANCISCO SETTINGS' panel contains various configuration options, many of which are highlighted with red boxes and numbers:

- 3**: 'ACI MULTI-SITE' toggle is set to 'On'.
- 4**: 'APIC SITE ID' is set to '1'.
- 5**: 'OVERLAY MULTICAST TEP' is set to '10.21.100.200'.
- 6**: 'BGP AUTONOMOUS SYSTEM NUMBER' is set to '65001'.
- 7**: 'OSPF AREA ID' is set to '0'.
- 8**: 'OSPF AREA TYPE' is set to 'regular'.
- 9**: 'EXTERNAL ROUTED DOMAIN' is set to 'SDC1-L3OUT'.
- 10**: 'ADD POLICY' button is highlighted.

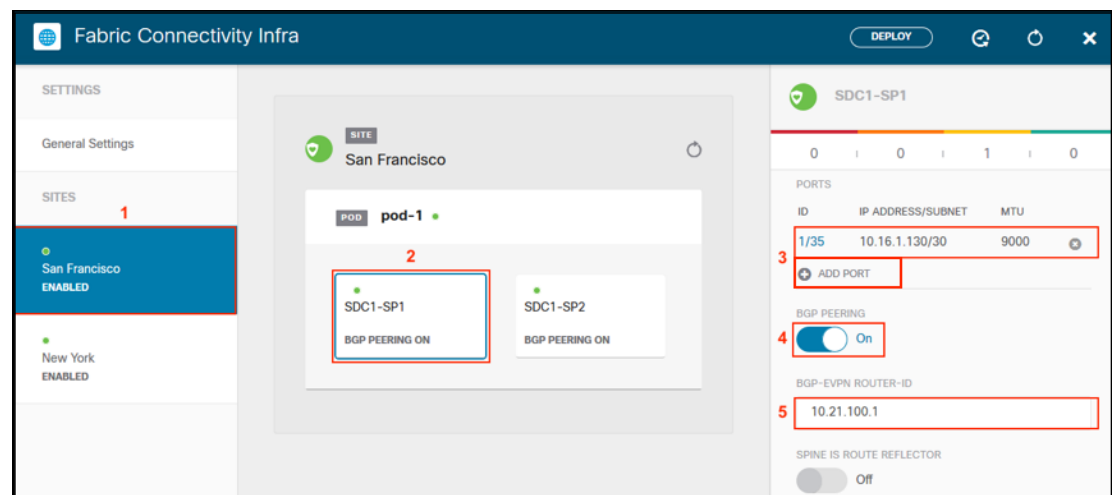
The 'OSPF POLICIES' table at the bottom shows two existing policies: 'msc-ospf-policy-d...' with 'point-to-point' network type, and 'common/default' with 'unspecified' network type.

89

- 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).

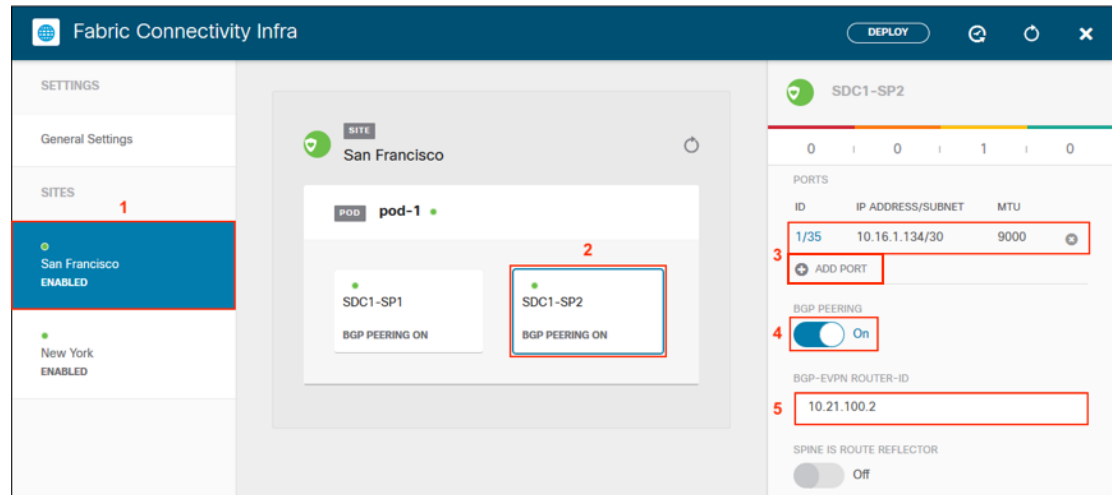


- e. Fill in San Francisco Spine 1 specific settings. Select San Francisco in the left panel (1), select Spine 1 in POD (2). Click ADD PORT, enter the port, IP address, subnet and MTU for the intersite connection in Spine 1 (3). Enable BGP peering (4). Set the Control Plane TEP IP address(5).

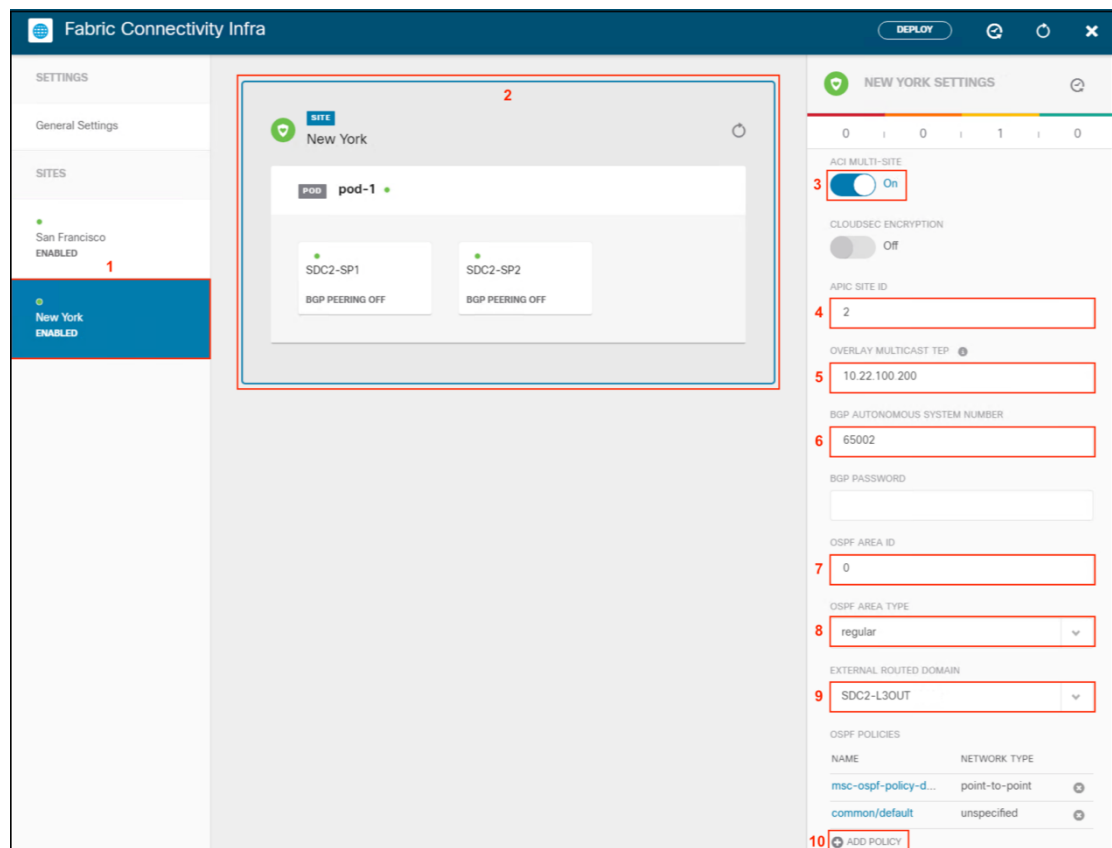


90

- 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).

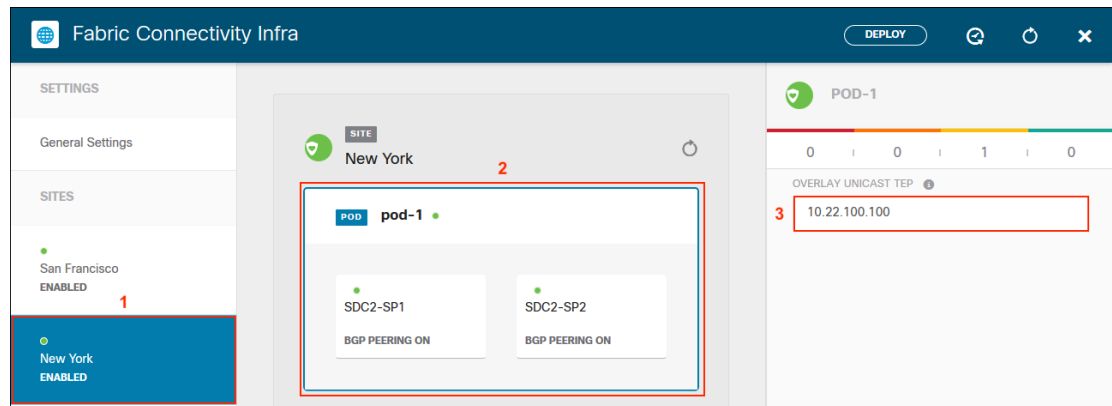


- g. Select Site New York and fill in the site specific settings in the right panel. Enable ACI Multi-Site (3) and set the APIC ID (4), Data Plane Multicast TEP address (5), BGP ASN (6), OSPF area ID (7), OSPF area type (8) and External Routed Domain (9). Select Add Policy (10) to create a new OSPF policy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

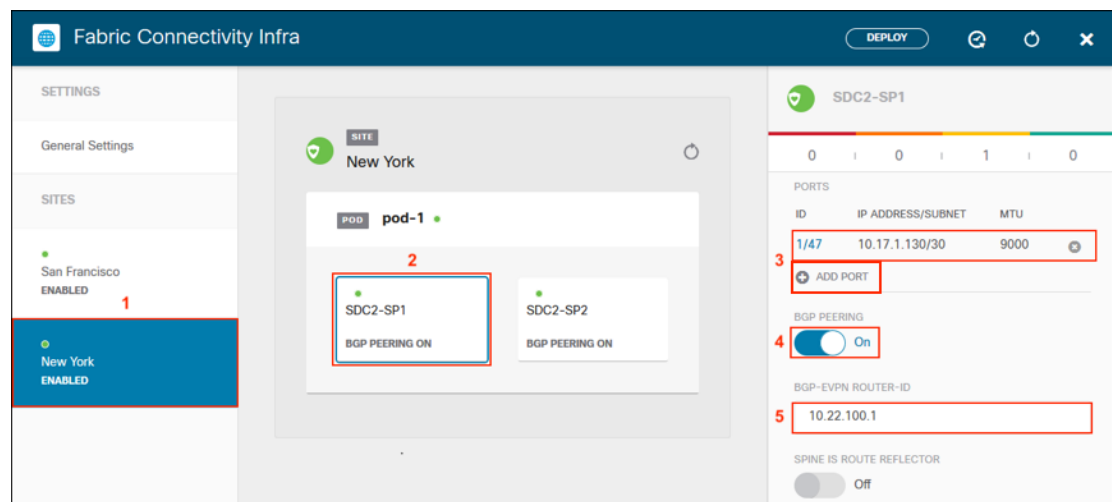


91

- 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)

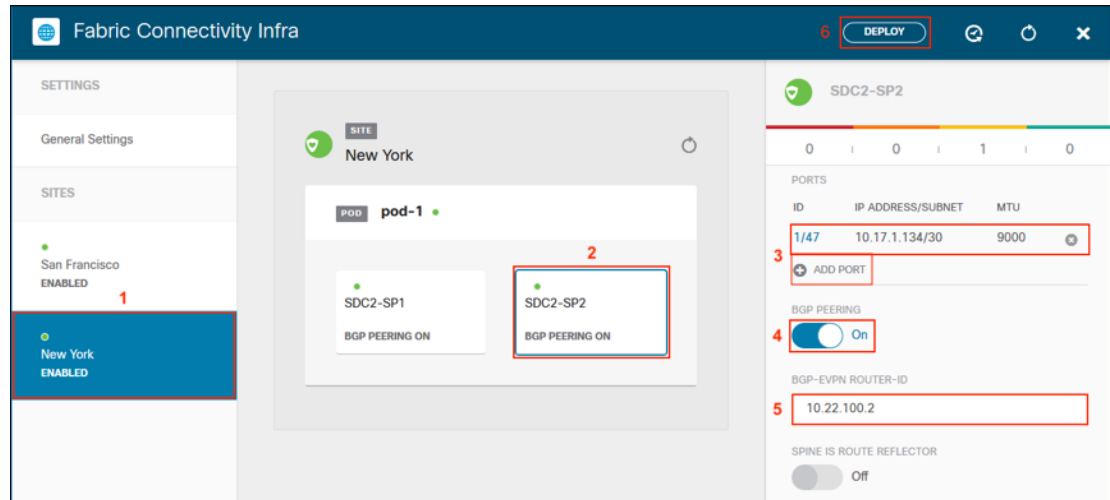


- i. Fill in New York Spine 1 specific settings. Select New York in the left panel (1), select Spine 1 in POD (2). Click ADD PORT, enter the port, IP address, subnet and MTU for the intersite connection in Spine 1 (3). Enable BGP peering (4). Set the Control Plane TEP IP address(5).



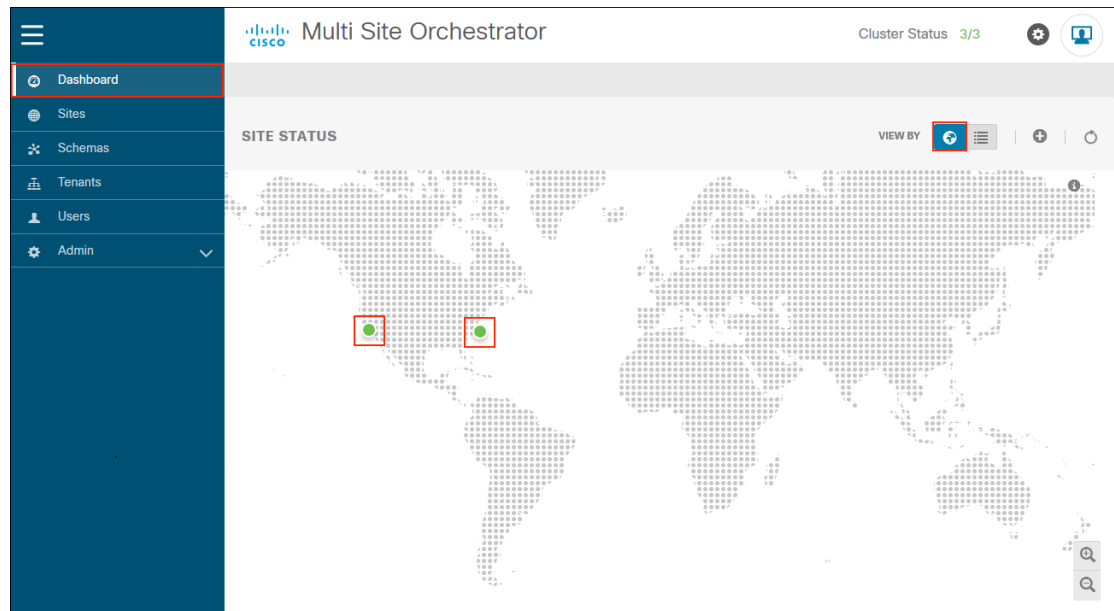
92

- 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.



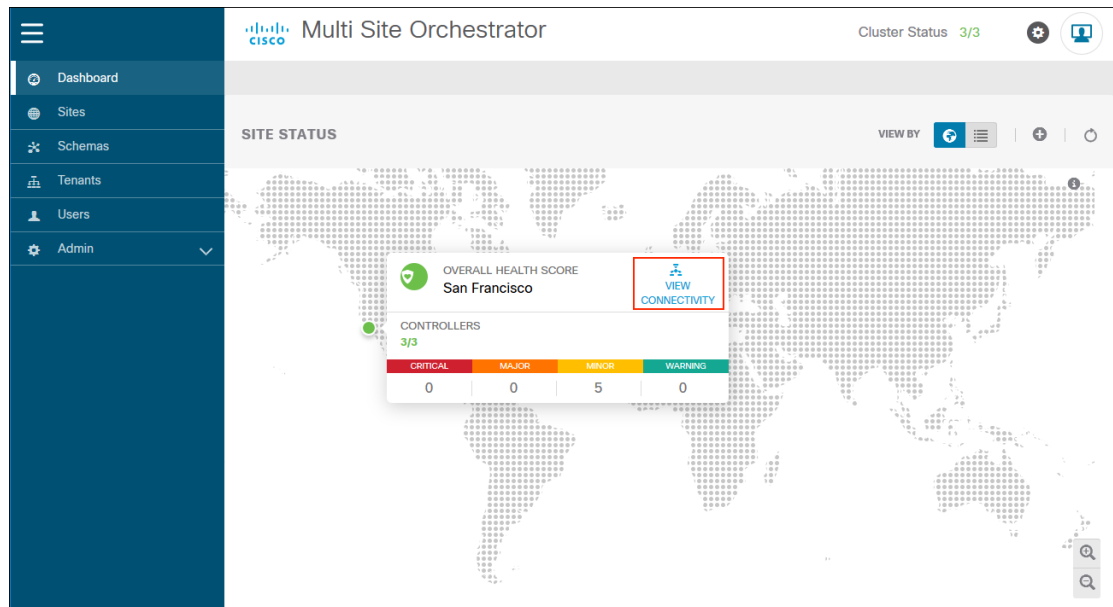
Step 4: Validate Intersite Policy with the MSO Dashboard

- 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.



93

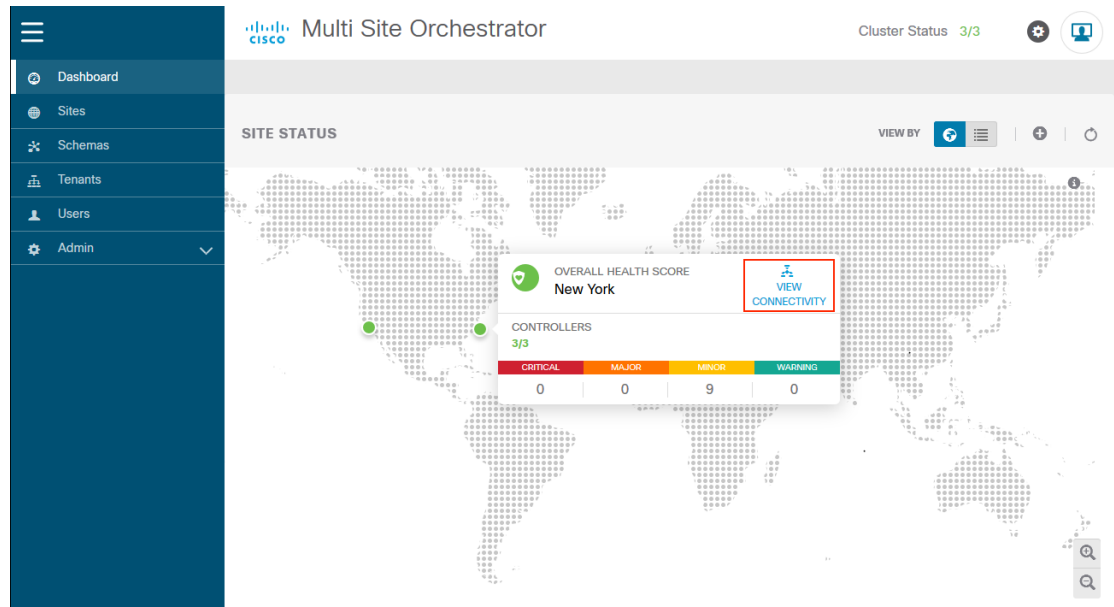
- b. Hover over the San Francisco Site to view the health score. **Select View Connectivity** to confirm the status of the **intersite** connection.



- 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.



95

- 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.

The screenshot shows the Multi Site Orchestrator (MSO) GUI. The left sidebar contains navigation links: Dashboard, Sites, Schemas, Tenants, Users, and Admin. The main content area is titled 'Multi Site Orchestrator' and shows 'Cluster Status 3/3'. The 'SITE STATUS' section displays a table with columns: SITE NAME, CONTROLLER STATE, CONNECTIVITY, CLO ENCI, CRITICAL, MAJOR, MINOR, and WARNING. Two sites are listed: San Francisco and New York. The 'SCHEMA HEALTH' section is currently empty, and a modal window titled 'About the HeatMap' is displayed, explaining that the heatmap represents the health of deployed Multi-Site Schemas and connected Sites. A 'GO TO SCHEMAS' button is visible at the bottom of the modal.

SITE NAME	CONTROLLER STATE	CONNECTIVITY	CLO ENCI	CRITICAL	MAJOR	MINOR	WARNING
San Francisco	3/3	+	1	0	0	5	0
New York	3/3	+	1	0	0	9	0

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

The screenshot shows the 'Tenants' page in the Multi Site Orchestrator GUI. The left sidebar is the same as the previous screenshot. The main content area is titled 'Tenants' and shows a search bar and an 'ADD TENANT' button. Below this is a table with columns: NAME, DESCRIPTION, ASSIGNED TO S..., ASSIGNED TO ..., ASSIGNED TO S..., and CONSISTENCY SCHEDULER. One tenant is listed: 'common' with a description 'Common tenant for use with al...'. The 'ASSIGNED TO S...' column shows '2', '1', and '0' for different categories.

NAME	DESCRIPTION	ASSIGNED TO S...	ASSIGNED TO ...	ASSIGNED TO S...	CONSISTENCY SCHEDULER
common	Common tenant for use with al...	2	1	0	Set Schedule

96

- 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)**.

The screenshot displays a web interface for configuring a tenant. It is divided into four main sections: General Settings, Associated Sites, Associated Users, and Consistency Checker Scheduler Settings. Red boxes and numbers 1 through 5 highlight the steps for adding a tenant: 1. Setting the display name to 'Tenant A' in the General Settings section. 2. Selecting 'San Francisco' and 'New York' under the 'SITE' column in the Associated Sites table. 3. Selecting 'TenantA' for both sites in the 'SECURITY DOMAINS' column. 4. Selecting the 'admin (Admin User)' under the 'USER' column in the Associated Users table. 5. Clicking the 'SAVE' button at the bottom right of the page.

General Settings	
* DISPLAY NAME	
1	Tenant A
Internal Name: TenantA	
DESCRIPTION	

Associated Sites	
<input checked="" type="checkbox"/> SITE	SECURITY DOMAINS
2 <input checked="" type="checkbox"/> San Francisco	3 TenantA
<input checked="" type="checkbox"/> New York	TenantA

Associated Users	
<input checked="" type="checkbox"/> USER	STATUS
4 <input checked="" type="checkbox"/> admin (Admin User) Local	Active

Consistency Checker Scheduler Settings	
<input checked="" type="checkbox"/> DISABLE SCHEDULER	
SELECT TIME	
12:00	AM

5 SAVE

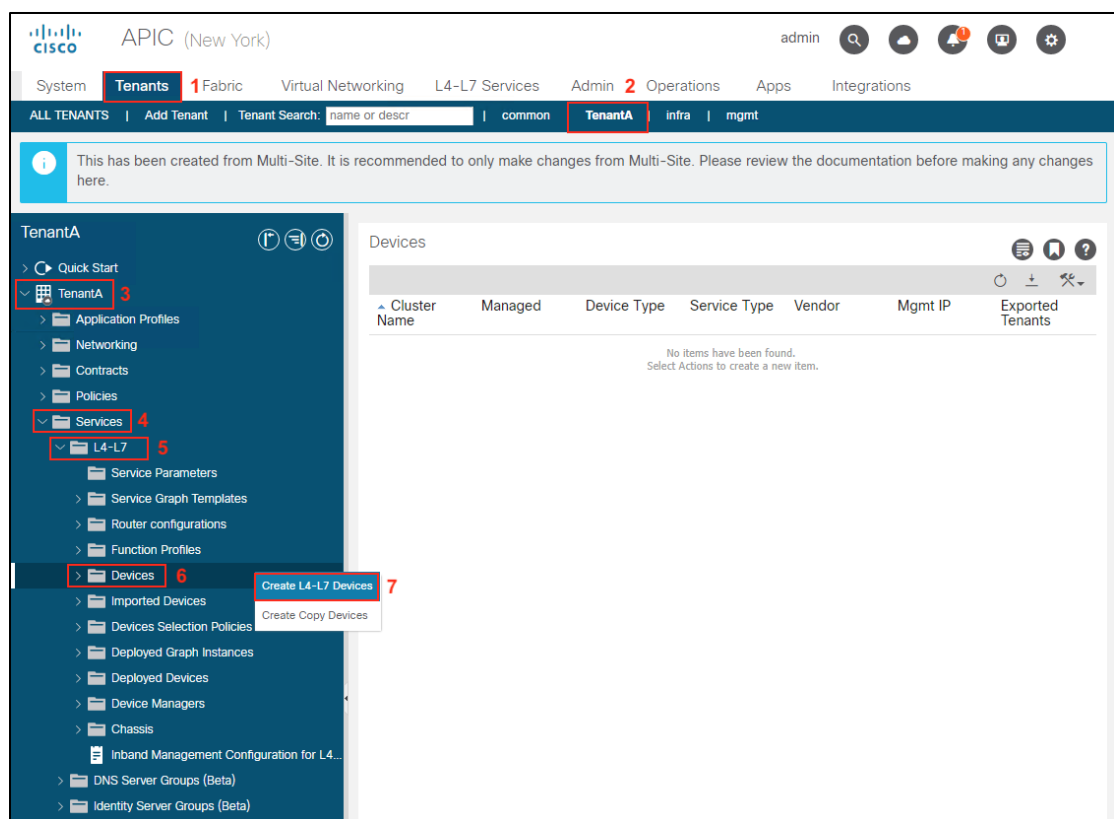
Step D: Deploy one-arm FTD cluster, PBR and L3Out policy on Tenant in APIC GUI

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)**.



98

- 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).

99

- 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.

The screenshot shows the 'Devices' configuration page in Cisco APIC. The 'Cluster Interfaces' section is expanded, showing a table with the following data:

Name	Concrete Interfaces	Encap
one-arm	Device/[Device]	vlan-1199

Below the table are 'Update' and 'Cancel' buttons. At the bottom of the page are 'Show Usage', 'Reset', and 'Submit' buttons.

- 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

The screenshot shows the 'L4-L7 Devices - SDC2-FTD-C1' configuration page in Cisco APIC. The 'General' tab is active, showing the following configuration:

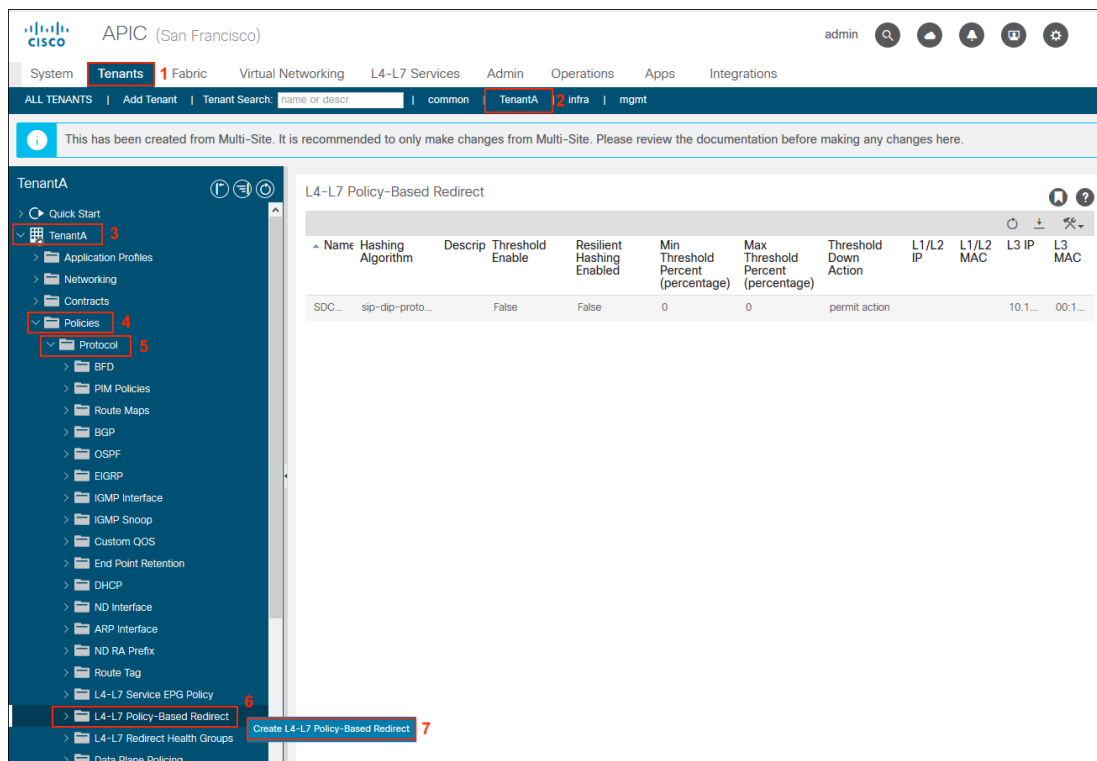
- Name: SDC2-FTD-C1
- Alias:
- Service Type: Firewall
- Device Type: PHYSICAL
- Physical Domain: phys
- Promiscuous Mode: ☐
- Context Aware: Multiple/Single
- Function Type: GoThrough/GoTo

The 'Policy' tab is also visible. The 'Devices' and 'Cluster Interfaces' sections are shown on the right, with 'one-arm' interface configured with 'Device/[Device]' and 'vlan-2199'.

100

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)**.



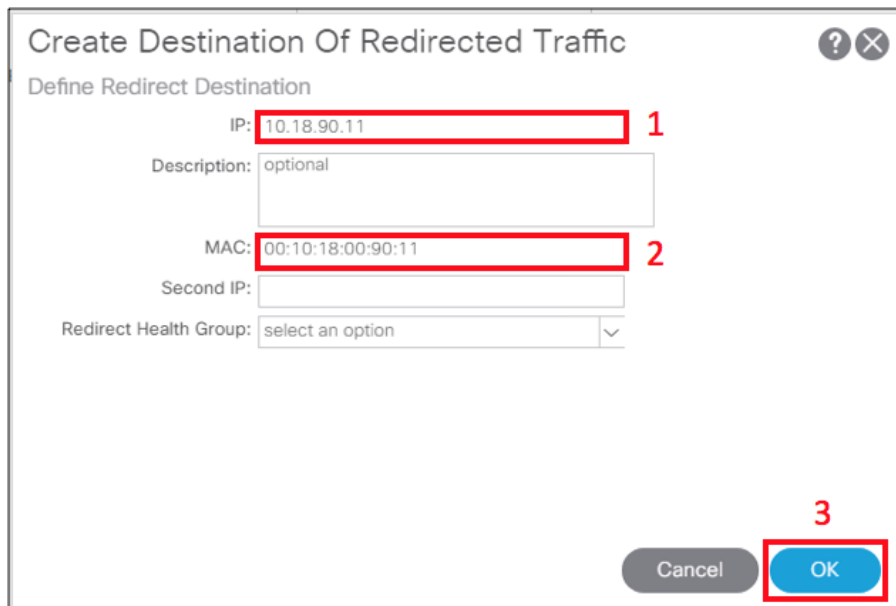
- b. Create L4-L7 Policy Based Redirect policy called **SDC1-FTD-SERVICE** (1) and add **Destination** policy (2).

The screenshot shows the 'Create L4-L7 Policy-Based Redirect' dialog box. The 'Name' field is set to 'SDC1-FTD-SERVICE' (1). The 'Description' field is set to 'optional'. The 'Destination Type' is set to 'L3'. The 'IP SLA Monitoring Policy' is set to 'select an option'. The 'Enable Pod ID Aware Redirection' checkbox is unchecked. The 'Hashing Algorithm' is set to 'sip-dip-prototype'. The 'Resilient Hashing Enabled' checkbox is unchecked. The 'Enable Anycast' checkbox is unchecked. The 'L3 Destinations' table is empty, and a '+' button is visible to add a new destination (2).

IP	MAC	Redirect Health Group	Additional IPv4/IPv6	Description	Oper Status
----	-----	-----------------------	----------------------	-------------	-------------

101

- 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.



Create Destination Of Redirected Traffic

Define Redirect Destination

IP: 10.18.90.11 **1**

Description: optional

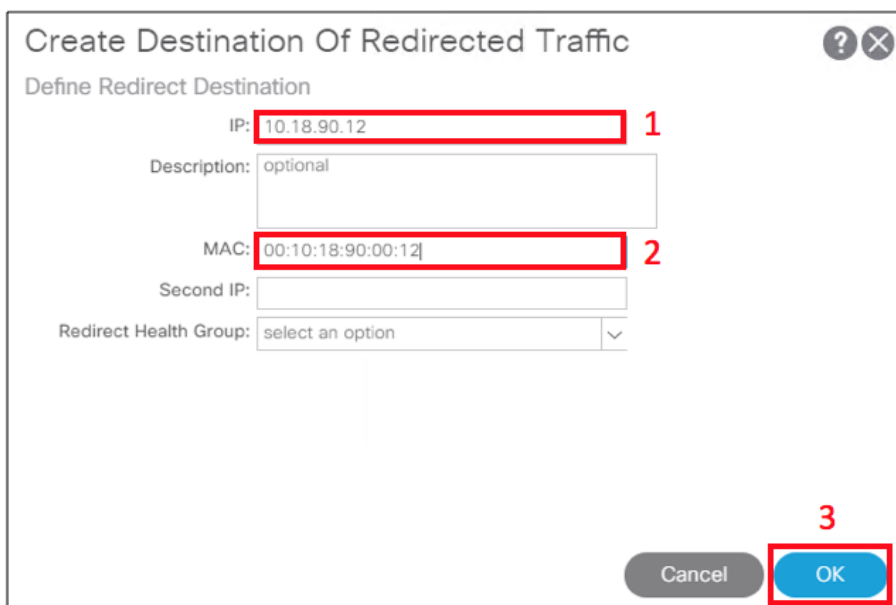
MAC: 00:10:18:00:90:11 **2**

Second IP:

Redirect Health Group: select an option

Cancel OK **3**

- 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.



Create Destination Of Redirected Traffic

Define Redirect Destination

IP: 10.18.90.12 **1**

Description: optional

MAC: 00:10:18:90:00:12 **2**

Second IP:

Redirect Health Group: select an option

Cancel OK **3**

102

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

Create L4-L7 Policy-Based Redirect

Name: SDC1-FTD-SERVICE

Description: optional

Destination Type: L1 L2 **L3**

IP SLA Monitoring Policy: select an option

Enable Pod ID Aware Redirection: ☐

Hashing Algorithm: dip sip **sip-dip-prototype**

Resilient Hashing Enabled: ☐

Enable Anycast: ☐

L3 Destinations:

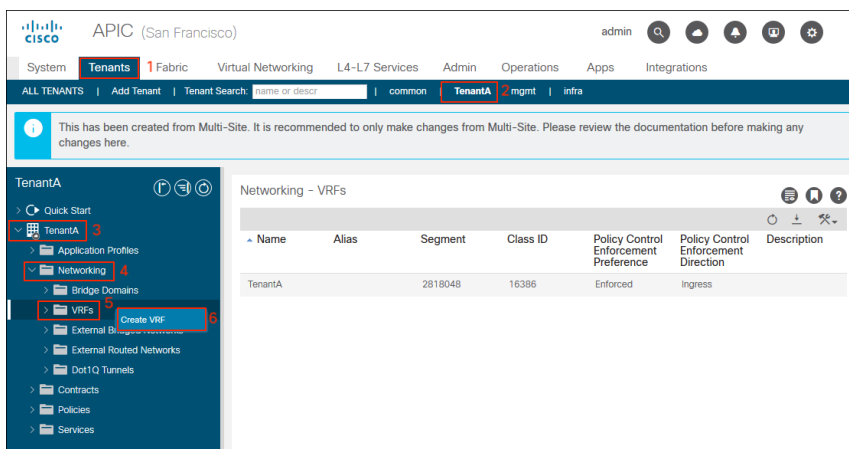
IP	MAC	Redirect Health Group	Additional IPv4/IPv6	Description	Oper Status
10.18.90...	00:10:18...				Enabled

Cancel Submit

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_CA462A15DDFF4A85A1382D5F6589CB59. We created the VRF under the tenant and followed Step 4 in the guide.

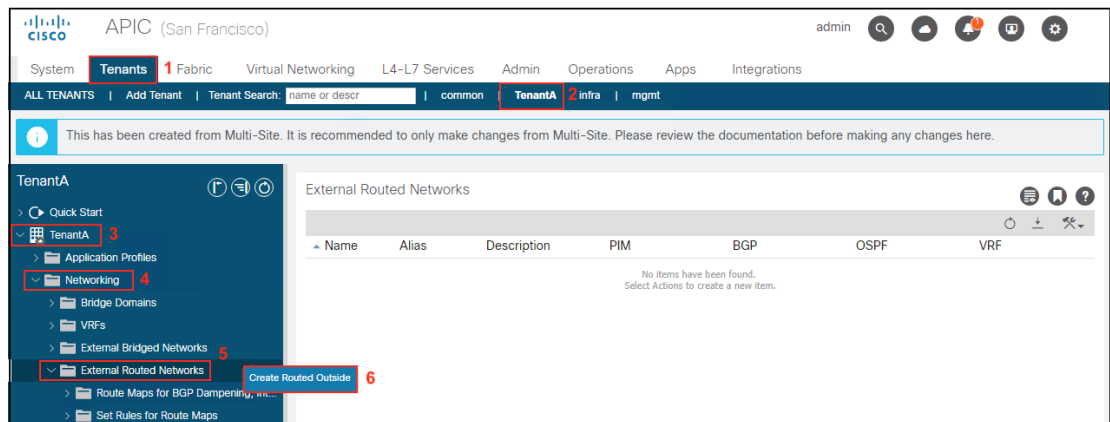
To create the VRF, navigate to Tenant (1)-><tenant-name> (2)-><tenant-name> (3)->Networking (4)->VRF (5), right-click and select Create VRF (6).



103

- 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)**.



104

- 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).

105

- f. Select the **Node ID SDC1-LF1(Node-101)** and enter the **Router ID 10.16.255.129** (2) and click OK (3).

Select Node

Node ID: SDC1-LF1 (Node-101) 1

Router ID: 10.16.255.129 2

Use Router ID as Loopback Address: ☒

Loopback Addresses:

IP

Static Routes:

IP Address	Next Hop IP	Track Policy
------------	-------------	--------------

Cancel OK 3

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

Select Node

Node ID: SDC1-LF2 (Node-102) 1

Router ID: 10.16.255.130 2

Use Router ID as Loopback Address: ☒

Loopback Addresses:

IP

Static Routes:

IP Address	Next Hop IP	Track Policy
------------	-------------	--------------

Cancel OK 3

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

Create Node Profile

Name: SDC1-L3OUT

Description: optional

Target DSCP: Unspecified

Nodes:

Node ID	Router ID	Static Routes	Loopback Address
topology/pod-1/...	10.16.255.129		10.16.255.129
topology/pod-1/...	10.16.255.130		10.16.255.130

OSPF Interface Profiles:

Name	Description	Interfaces	OSPF Policy
------	-------------	------------	-------------

Cancel

OK

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

Create Interface Profile

STEP 1 > Identity

1. Identity

2. Protocol Profiles

3. Interfaces

Name: SDC1-L3OUT

Description: optional

ND policy: select a value

ARP policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

QoS Priority: Unspecified

Custom QoS Policy: select a value

NetFlow Monitor Policies:

NetFlow IP Filter Type	NetFlow Monitor Policy
------------------------	------------------------

Config Protocol Profiles: ☒

Previous

Cancel

Next

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

Create Interface Profile

STEP 2 > Protocol Profiles

1. Identity2. Protocol Profiles3. Interfaces

OSPF Profile

Authentication Type: No authentication

Authentication Key:

Confirm Key:

OSPF Policy: select a value

BFD Interface Profile

Authentication Type: No authentication

BFD Interface Policy: select a value

HSRP Interface Profile

Enable HSRP:

HSRP version: version 1version 2

HSRP Interface Policy: select a value

HSRP Interface Groups:

Name	Group ID	IP	MAC	Group Name	Group Type	IP Obtain Mode
------	----------	----	-----	------------	------------	----------------

Previous

Cancel

Next

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

Create Interface Profile

STEP 3 > Interfaces

1. Identity2. Protocol Profiles3. Interfaces

Routed InterfacesSVIRouted Sub-Interface

SVI Interfaces

Path	IP Address	MAC Address	MTU (bytes)
------	------------	-------------	-------------

Previous

Cancel

OK

108

- I. 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).

Select SVI

Path Type: ☐ Port ☐ Direct Port Channel ☒ **Virtual Port Channel** 1

Path: **SDC1-L3OUT** 2

Description: optional

Encap: **VLAN** 1197 3

Encap Scope: ☐ VRF ☒ Local

Auto State: ☒ disabled ☐ enabled

Mode: ☐ Access (802.1P) ☒ Trunk ☐ Access (Untagged)

Side A IPv4 Primary / IPv6 Preferred Address: **10.16.255.129/29** 4

Side A IPv4 Secondary / IPv6 Additional Addresses:

Address	IPv6 DAD
10.15.255.131/29	enabled

Side A Link-Local Address:

Side B IPv4 Primary / IPv6 Preferred Address: **10.16.255.130/29** 6

Side B IPv4 Secondary / IPv6 Additional Addresses:

Address	IPv6 DAD
10.16.255.131/29	enabled

Side B Link-Local Address:

MAC Address: 00:22:BD:F8:19:FF

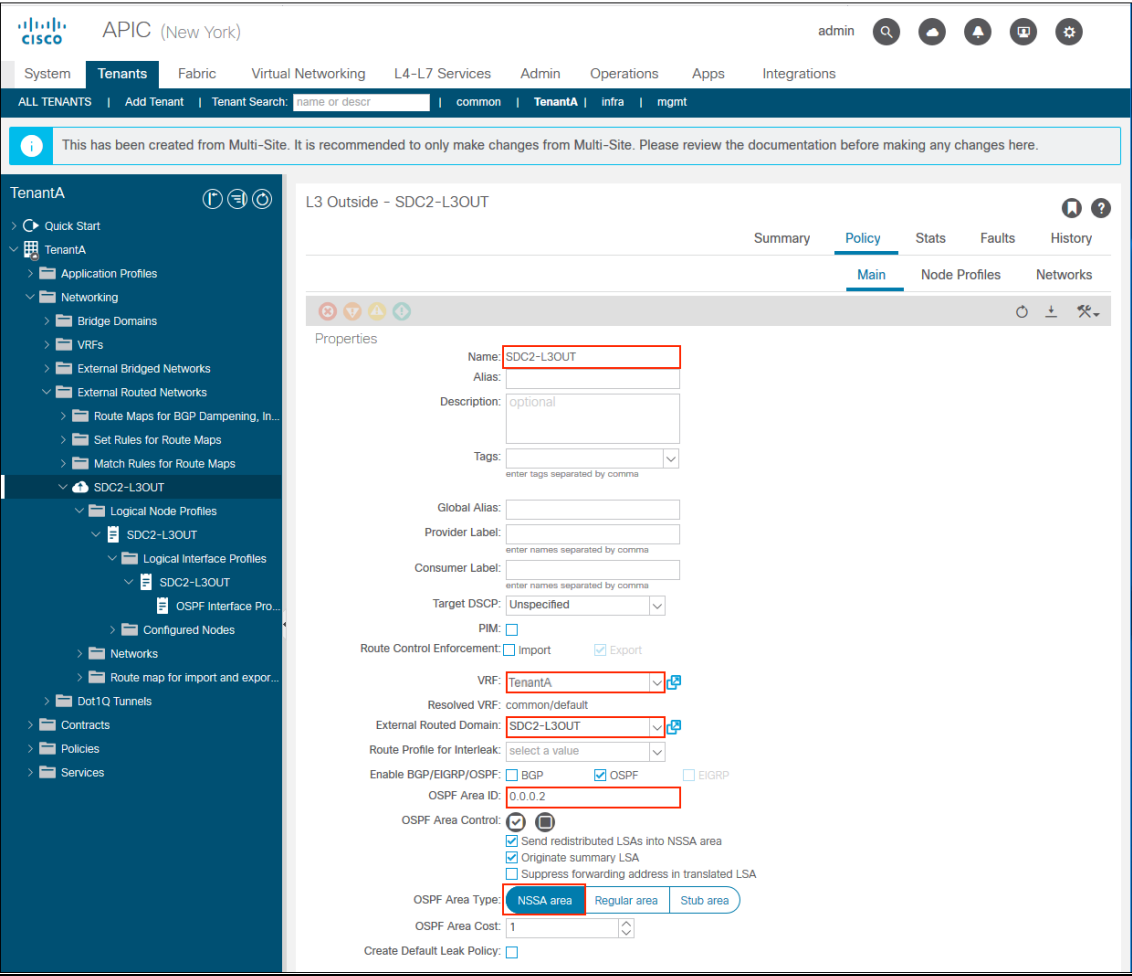
MTU (bytes): inherit

Target DSCP: Unspecified

Cancel **OK** 8

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

SDC2-L3OUT configuration



SDC2-L3OUT Node Profile

APIC (New York)

admin

System

Tenants

Fabric

Virtual Networking

L4-L7 Services

Admin

Operations

Apps

Integrations

ALL TENANTS

Add Tenant

Tenant Search:

common

TenantA

infra

mgmt

This has been created from Multi-Site. It is recommended to only make changes from Multi-Site. Please review the documentation before making any changes here.

TenantA

Quick Start

TenantA

Application Profiles

Networking

Bridge Domains

VRFs

External Bridged Networks

External Routed Networks

Route Maps for BGP Dampening, In...

Set Rules for Route Maps

Match Rules for Route Maps

SDC2-L3OUT

Logical Node Profiles

SDC2-L3OUT

Logical Interface Profiles

SDC2-L3OUT

OSPF Interface Pro...

Configured Nodes

Networks

Route map for import and expor...

Dot1Q Tunnels

Contracts

Policies

Services

Logical Node Profile - SDC2-L3OUT

Policy

Faults

History

Properties

Name: SDC2-L3OUT

Description: optional

Alias:

Target DSCP: Unspecified

Nodes:

Node ID	Router ID	Loopback Address
topology/pod-1/node-101	10.17.255.101	10.17.255.101
topology/pod-1/node-102	10.17.255.102	10.17.255.102

Create BGP Protocol Profile: ☐

Show Usage

Reset

Submit

111

SDC2-L3OUT SVI configuration

SVI

Policy

Faults

History

Properties

Path: topology/pod-1/protopaths-101-102/pathep-[SDC2-L3OUT]

Path Description:

Description: optional

Encap: VLAN

2197

Integer Value

Encap Scope: VRF Local

Auto State: disabled enabled

Mode: Access (802.1P) Trunk Access (Untagged)

Side A IPv4 Primary / IPv6 Preferred Address: 10.17.255.129/29

Side A IPv6 DAD: disabled enabled

Side A IPv4 Secondary / IPv6 Additional Addresses:

Address

IPv6 DAD

10.17.255.131/29

enabled

Side A Link-Local Address: ::

Side B IPv4 Primary / IPv6 Preferred Address: 10.17.255.130/29

Side B IPv6 DAD: disabled enabled

Side B IPv4 Secondary / IPv6 Additional Addresses:

Address

IPv6 DAD

10.17.255.131/29

enabled

Side B Link-Local Address: ::

MAC Address: 00:22:BD:F8:19:FF

MTU (bytes): 1500

Target DSCP: Unspecified

Show Usage

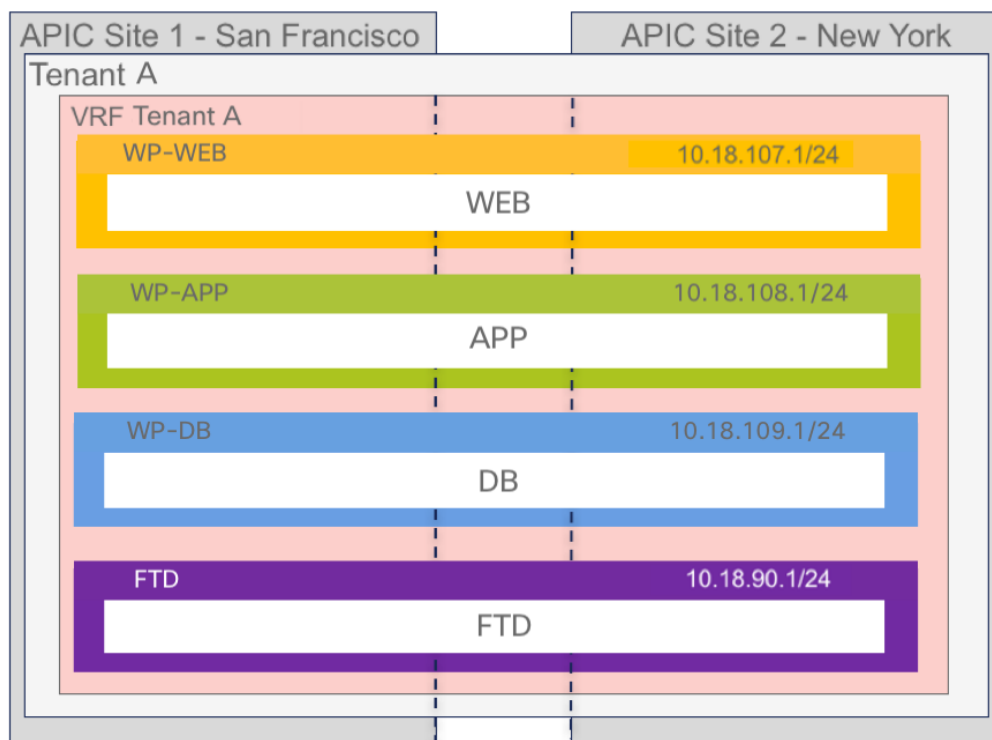
Close

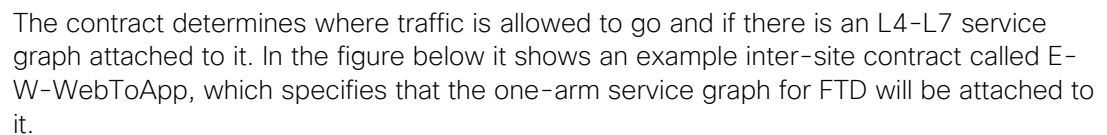
Submit

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 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





Stretched Bridge Domain with Inter-Site Contract Example



114

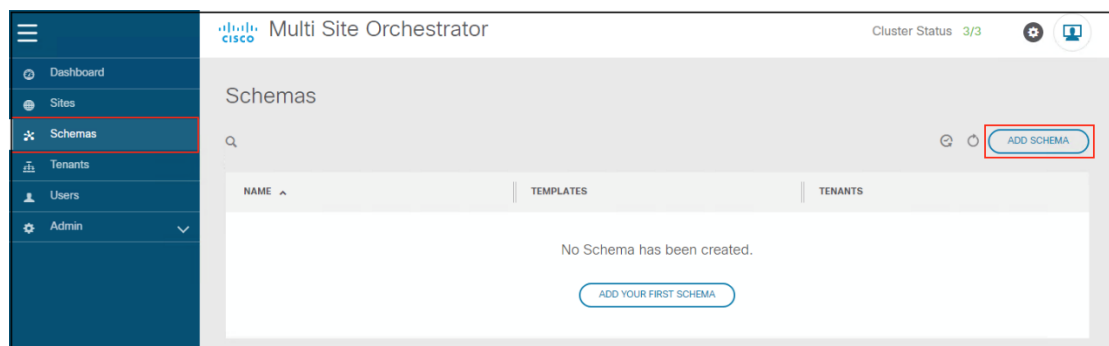
Section Summary:

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.

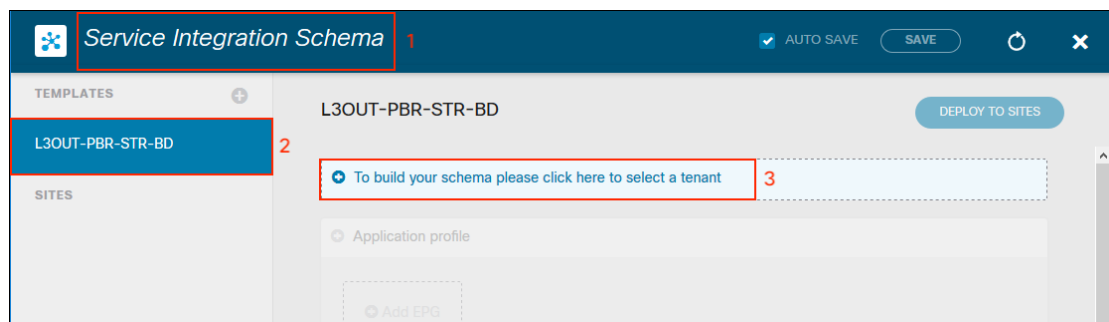
- Step 1: Create schema
- Step 2: Add Sites
- Step 3: Import VRF
- Step 4: Create Service Graph
- Step 5: Create External EPG
- Step 6: Create Filters
- Step 7: Create Bridge Domains
- Step 8: Create Contracts
- Step 9: Create Application Profile
- Step 10: Add contracts to External EPG

Step 1: Create Schema

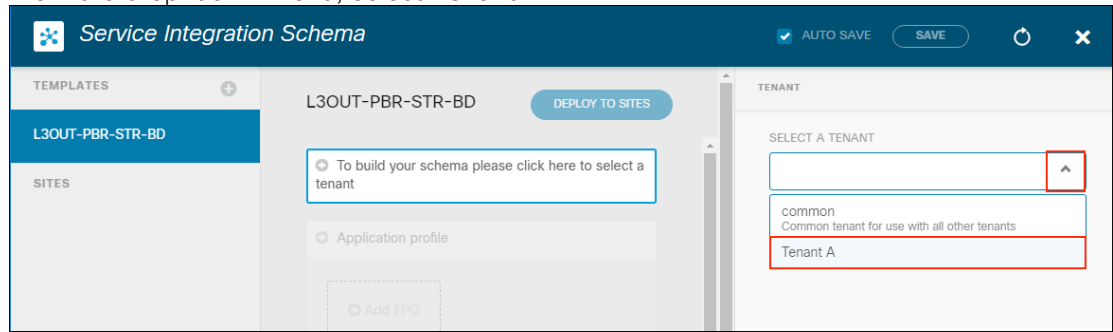
- a. To create a schema, in the MSO home screen, navigate to **Schemas** in left pane, and then select **ADD Schema** on the right.



- 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**.

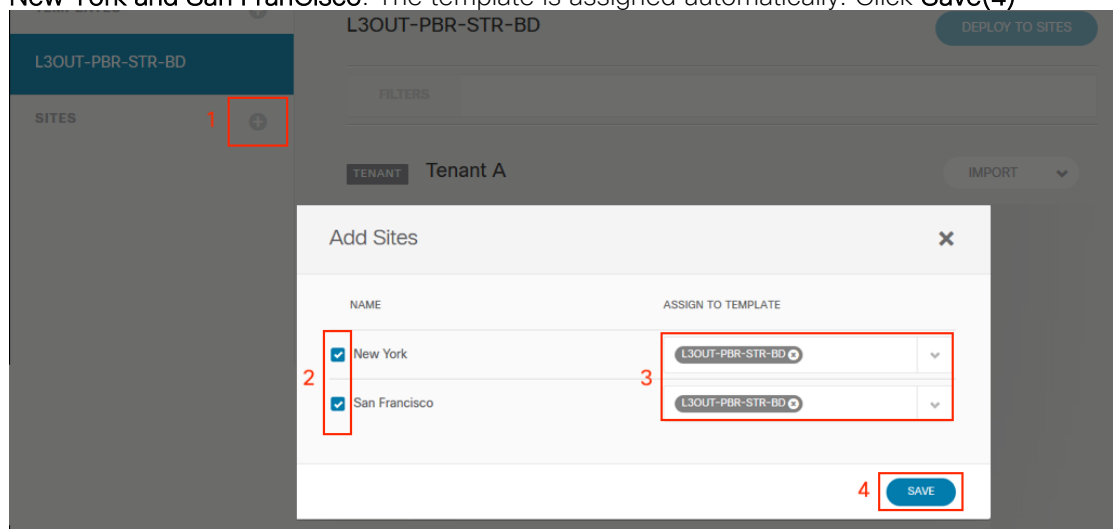


- c. From the drop-down menu, select **Tenant A**



Step 2: Add Sites

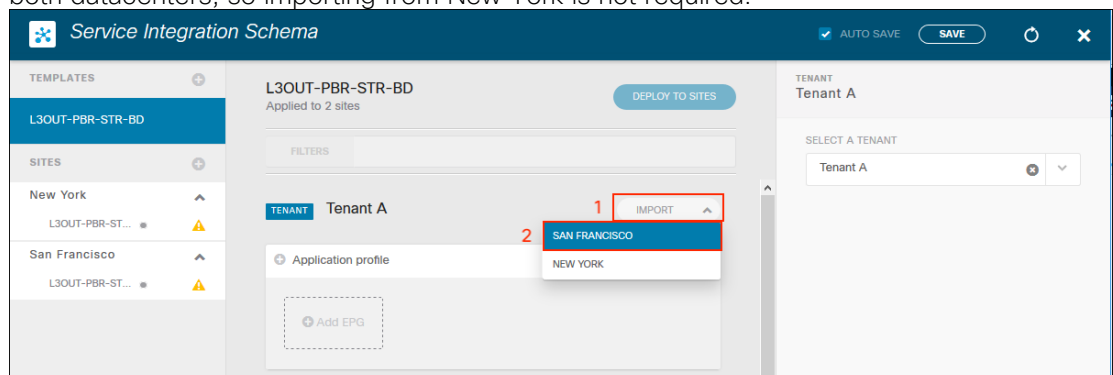
- a. Add sites to the schema. Click the **+ sign(1)** next to **SITES** and click the **check boxes(2)** for **New York** and **San Francisco**. The template is assigned automatically. Click **Save(4)**



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.



116

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

Import from San Francisco

POLICY TYPE

APPLICATION PROFILE0 out of 0

EPG0 out of 0

EXTERNAL EPG0 out of 0

CONTRACT0 out of 0

FILTER0 out of 0

VRF1 out of 1

BD0 out of 1

SERVICE GRAPHS0 out of 0

SELECT TO IMPORT

1☒ TenantA

Q

INCLUDE RELATIONS

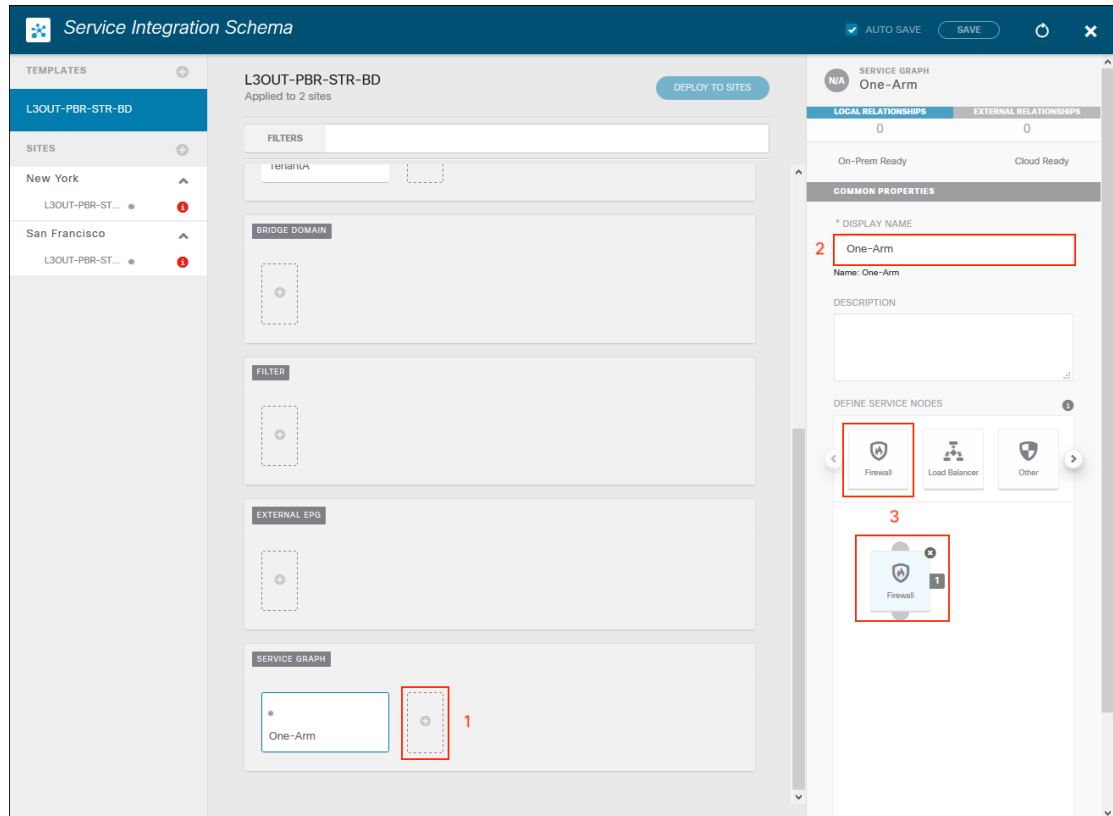
3

IMPORT

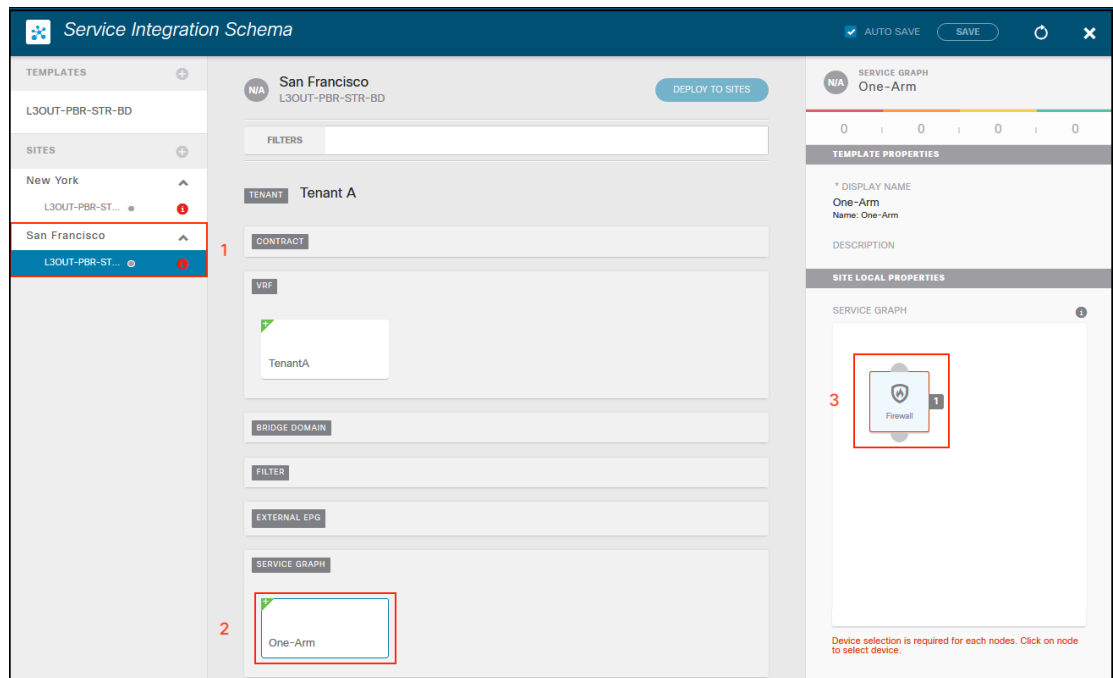
117

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)**.



118

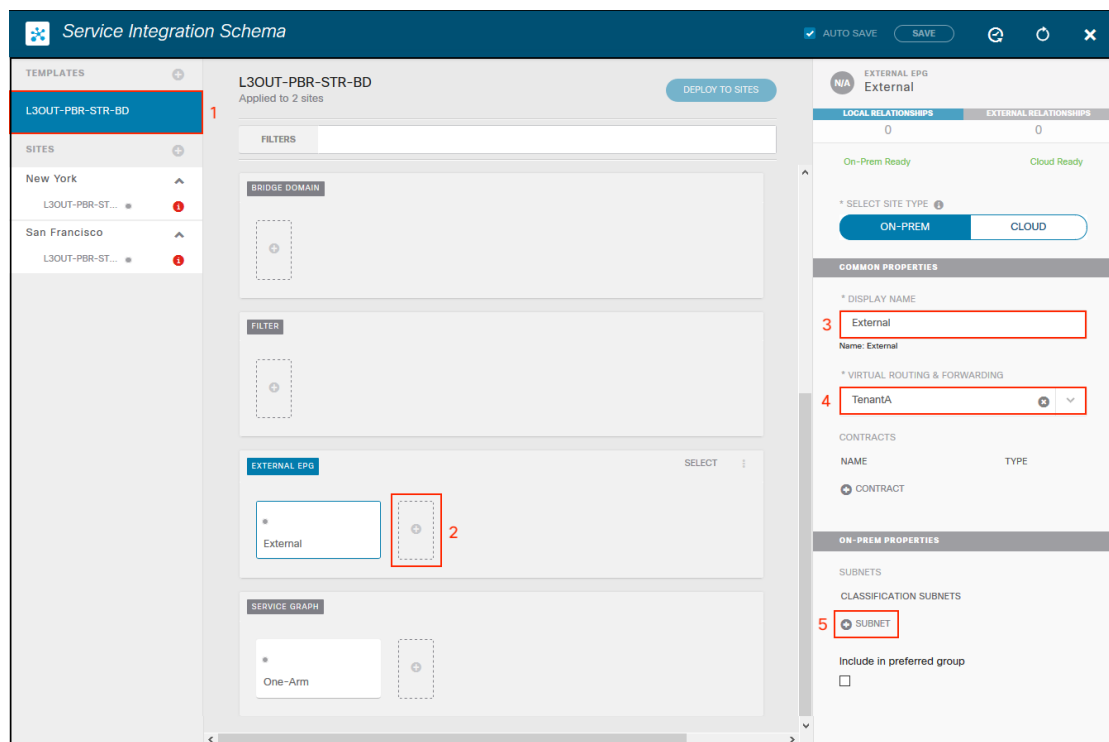
- c. From the drop-down menu, select the **SDC1-FTD-C1** firewall and click **SAVE**



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

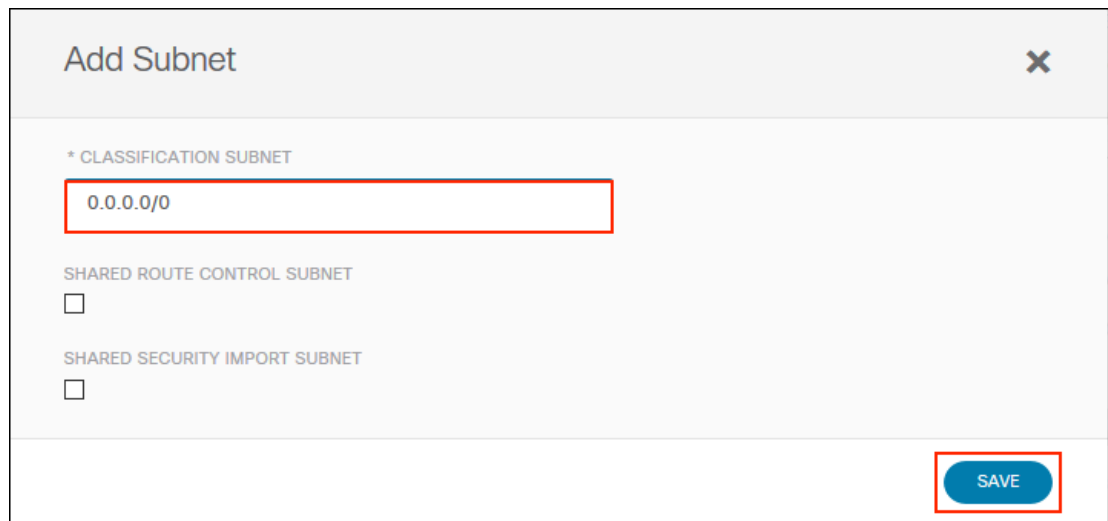
Step 5: Create External EPG

- 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.



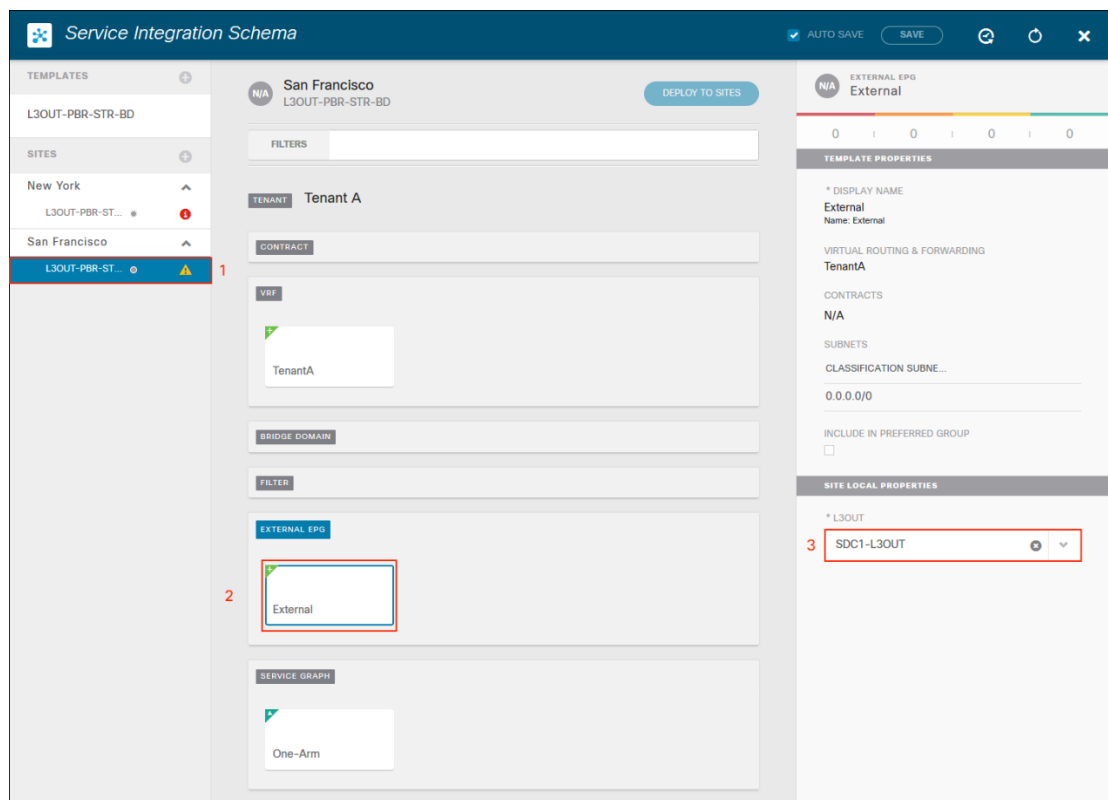
119

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



The 'Add Subnet' dialog box is shown. It has a title bar with a close button (X). The main content area contains three sections: '* CLASSIFICATION SUBNET' with a text input field containing '0.0.0.0/0', 'SHARED ROUTE CONTROL SUBNET' with an unchecked checkbox, and 'SHARED SECURITY IMPORT SUBNET' with an unchecked checkbox. At the bottom right, there is a blue 'SAVE' button.

- 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.



The 'Service Integration Schema' interface is shown. The left sidebar has a 'SITES' section with 'San Francisco' selected. The main area shows 'San Francisco' details, including 'L3OUT-PBR-STR-BD'. The 'EXTERNAL EPG' section is highlighted with a red box and a red '2'. The right sidebar shows 'EXTERNAL EPG' details, including 'CLASSIFICATION SUBNET' with '0.0.0.0/0' and 'SITE LOCAL PROPERTIES' with 'L3OUT' dropdown set to 'SDC1-L3OUT' (highlighted with a red box and a red '3').

- d. Repeat step c. for the New York site

120

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**.

The screenshot displays the 'Service Integration Schema' interface. On the left, the 'TEMPLATES' sidebar shows 'L3OUT-PBR-STR-BD' selected, marked with a red box and the number 1. Below it, the 'SITES' section lists 'New York' and 'San Francisco', each with a sub-entry 'L3OUT-PBR-ST...' and a yellow warning triangle. The main area is titled 'L3OUT-PBR-STR-BD' and 'Applied to 2 sites'. It contains three sections: 'BRIDGE DOMAIN' with a dashed box, 'FILTER' with a text input 'N-S' (boxed with a blue border) and a '+' sign (boxed with a red border and labeled 2), and 'EXTERNAL EPG' with a text input 'External' and a dashed box. On the right, the 'FILTER' details panel shows 'N-S' as the filter name. Under 'COMMON PROPERTIES', the '* DISPLAY NAME' field contains 'N-S' (boxed with a red border and labeled 3). Under 'ENTRIES', the 'ENTRY' field is highlighted with a red box and labeled 4.

121

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

The screenshot shows a modal window titled "Add Entry" with a close button (X) in the top right corner. The window is divided into two main sections: "COMMON PROPERTIES" and "ON-PREM PROPERTIES".

COMMON PROPERTIES

- * NAME**: A text input field containing "permit-all", highlighted with a red border.
- DESCRIPTION**: An empty text input field.
- ETHERTYPE**: A dropdown menu with "unspecified" selected.
- IP PROTOCOL**: A dropdown menu with "unspecified" selected.
- DESTINATION PORT RANGE FROM**: A text input field with "unspecified".
- DESTINATION PORT RANGE TO**: A text input field with "unspecified".

ON-PREM PROPERTIES

- ☐ MATCH ONLY FRAGMENTS
- ☐ STATEFUL
- ARP FLAG**: A dropdown menu with "unspecified" selected.
- SOURCE PORT RANGE FROM**: A text input field.

At the bottom right of the dialog, there is a blue button labeled "SAVE", which is highlighted with a red border.

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

The screenshot shows a "FILTER" bar with a blue tab labeled "FILTER". Below the tab, there are three filter cards: "N-S", "E-W", and "Telemetry". Each card has a small dot icon in the top left corner. The "E-W" and "Telemetry" cards are highlighted with red borders. To the right of these cards is a dashed box containing a plus sign icon, indicating a button to add more filters.

122

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 **+** sign under GATEWAY IP (4).

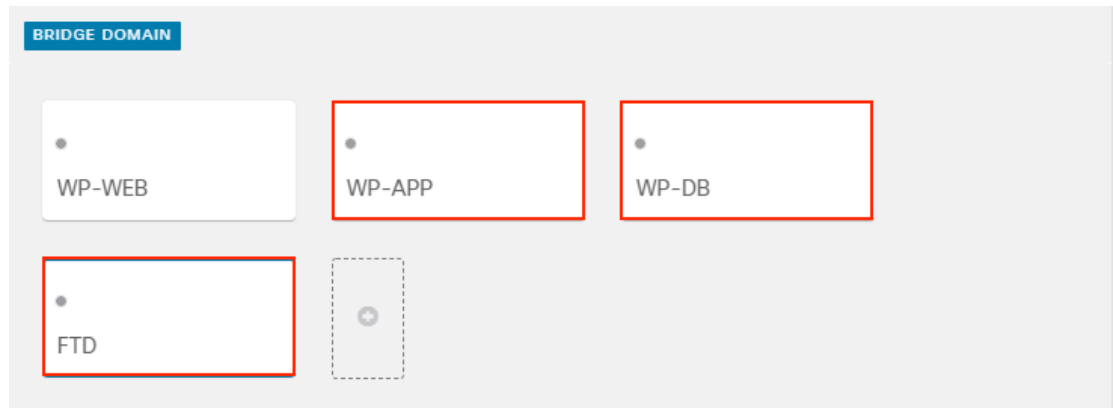
The screenshot shows the 'Service Integration Schema' interface. On the left, a sidebar lists 'TEMPLATES' and 'SITES'. The main area displays the 'L3OUT-PBR-STR-BD' configuration. The 'BRIDGE DOMAIN' section is highlighted, showing a list of domains with a '+' sign (1) next to 'WP-WEB'. The right-hand panel shows the configuration details for 'WP-WEB'. The 'DISPLAY NAME' field (2) is set to 'WP-WEB'. The 'VIRTUAL ROUTING & FORWARDING' dropdown (3) is set to 'TenantA'. The 'GATEWAY IP' section (4) shows a '+' sign next to the 'SUBNET' option.

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

The 'Add Subnet' dialog box is shown. The '* GATEWAY IP' field contains '10.18.107.1/24'. The 'SCOPE' section has two radio buttons: 'Private to VRF' and 'Advertised Externally' (selected). The 'SHARED BETWEEN VRF'S' checkbox is unchecked. The 'NO DEFAULT SVI GATEWAY' checkbox is unchecked. The 'QUERIER' checkbox is unchecked. A 'SAVE' button is located at the bottom right.

123

- 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).

The screenshot shows the 'Service Integration Schema' configuration page. The main panel displays the configuration for 'Tenant A'. The 'CONTRACT' section is highlighted, and a red box (1) is around the '+' sign. The right panel shows the configuration for the 'N-S-ExtToWeb' contract. Red boxes (2), (3), (4), and (5) are placed around the 'DISPLAY NAME', 'FILTER', 'SERVICE GRAPH', and 'Firewall' icon respectively. The 'SERVICE GRAPH' diagram shows a 'Consumer EPG' connected to a 'Provider EPG' via a 'Firewall' node.

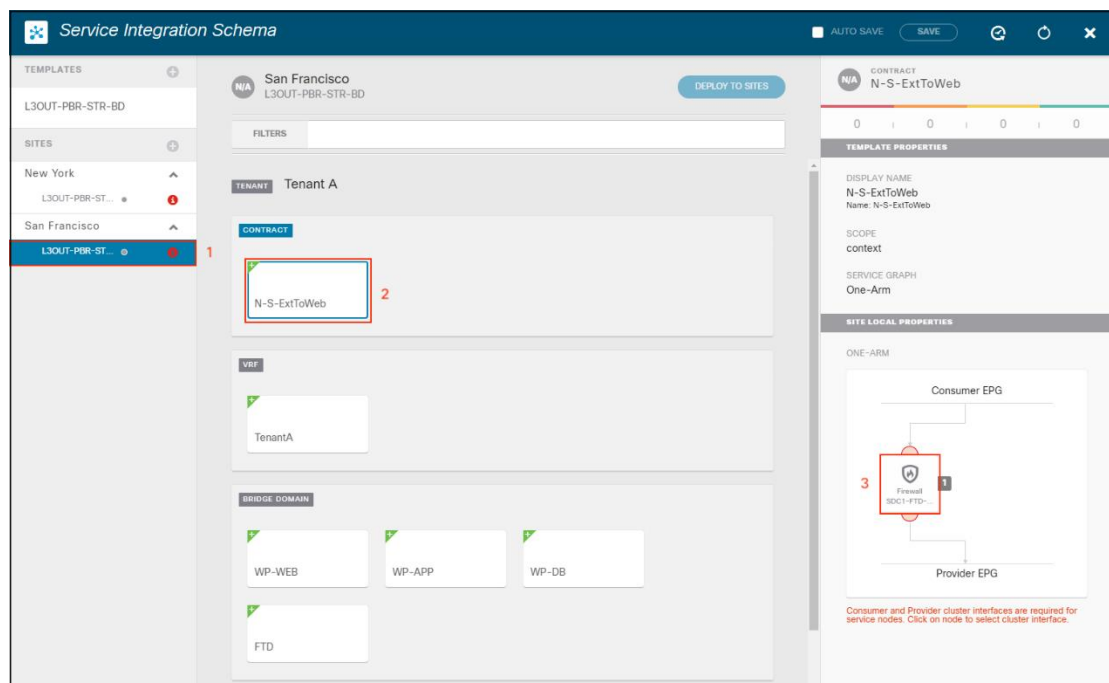
124

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



The 'Configure Firewall' dialog box shows a diagram at the top with 'Consumer EPG' connected to a 'Firewall' icon, which is then connected to 'Provider EPG'. Below this, the 'CONSUMER CONNECTOR' section has a 'BRIDGE DOMAIN' dropdown menu with 'WP-WEB' selected. The 'PROVIDER CONNECTOR' section has a 'BRIDGE DOMAIN' dropdown menu with 'FTD' selected. A 'DONE' button is located at the bottom right.

- 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)**.




The 'Service Integration Schema' interface shows a left sidebar with 'TEMPLATES' and 'SITES'. Under 'SITES', 'San Francisco' is selected (1). The main area shows 'Tenant A' with a 'CONTRACT' section where 'N-S-ExtToWeb' is selected (2). Below the contract, there are sections for 'VRF' (TenantA) and 'BRIDGE DOMAIN' (WP-WEB, WP-APP, WP-DB, FTD). On the right, the 'TEMPLATE PROPERTIES' and 'SITE LOCAL PROPERTIES' are shown. The 'ONE-ARM' diagram shows the 'Consumer EPG' connected to a 'Firewall' icon (3), which is then connected to the 'Provider EPG'.

125

- 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**

Configure SDC1-FTD-C1



CONSUMER CONNECTOR

* CLUSTER INTERFACE

one-arm

REDIRECT POLICY

TenantA/SDC1-FTD-SERVICE

PROVIDER CONNECTOR

* CLUSTER INTERFACE

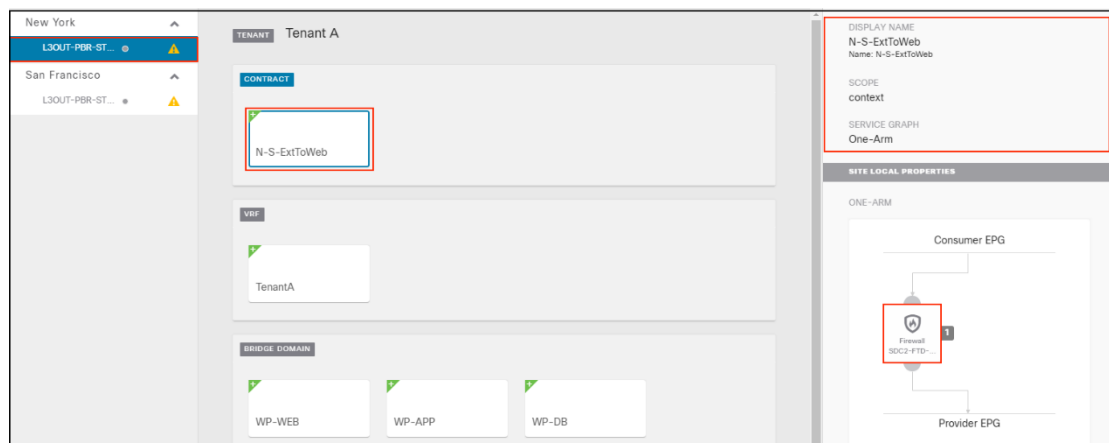
one-arm

REDIRECT POLICY

TenantA/SDC1-FTD-SERVICE

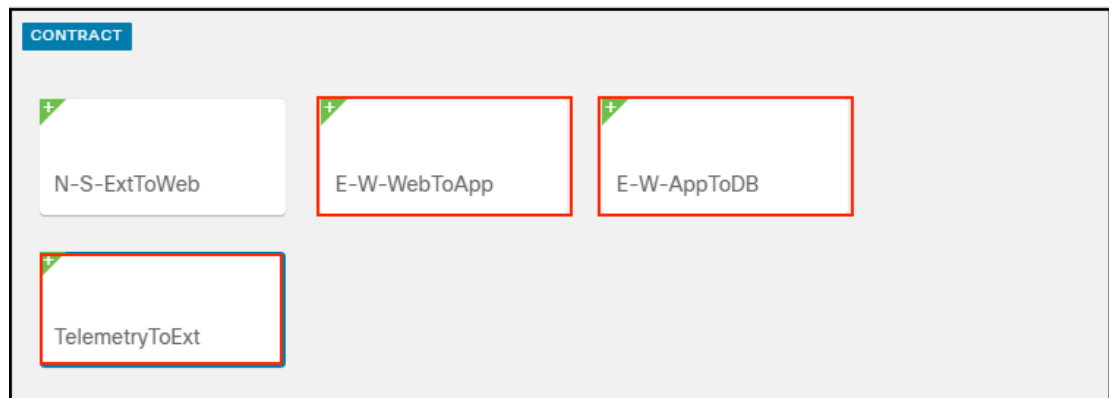
DONE

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



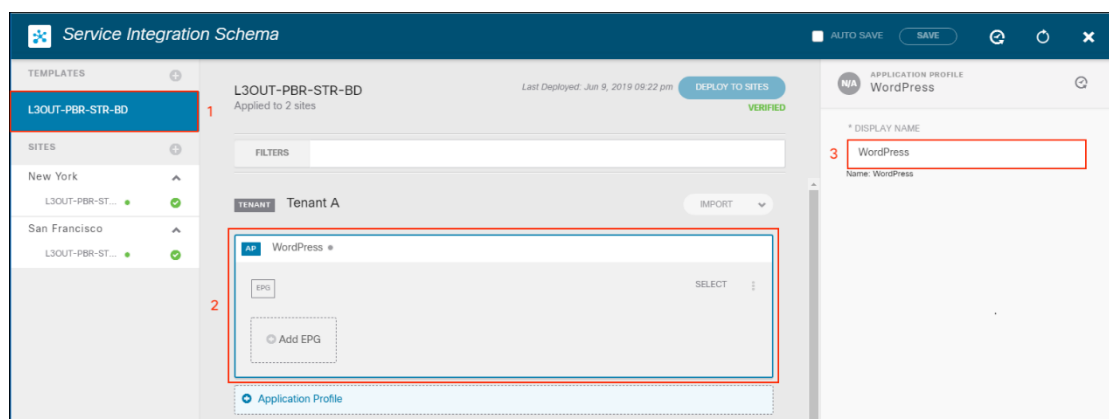
126

- 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.



127

- 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.

The screenshot shows the 'Service Integration Schema' interface. On the left, a sidebar lists templates and sites. The main area is titled 'L3OUT-PBR-STR-BD' and shows a configuration for 'Tenant A'. In the 'EPG' section, a new EPG named 'WEB' is being added, indicated by a red box and the number '1'. The 'CONTRACT' section shows a table of contracts with columns 'NAME' and 'TYPE'. The 'ON-PREM PROPERTIES' section shows a 'BRIDGE DOMAIN' dropdown set to 'WP-WEB' (indicated by a red box and the number '5') and a 'SUBNET' dropdown set to '10.18.107.1/24' (indicated by a red box and the number '6').

NAME	TYPE
E-W-Web IoApp	consu...
N-S-ExtIoWeb	provider
telemetryIoExt	consu...

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

APP EPG

The screenshot shows the 'Service Integration Schema' interface for 'Tenant A'. In the 'EPG' section, a new EPG named 'APP' is being added, indicated by a red box. The 'CONTRACT' section shows a table of contracts with columns 'NAME' and 'TYPE'. The 'ON-PREM PROPERTIES' section shows a 'BRIDGE DOMAIN' dropdown set to 'WP-APP' (indicated by a red box) and a 'SUBNET' dropdown set to '10.18.108.1/24' (indicated by a red box).

NAME	TYPE
E-W-Web IoApp	provider
E-W-App IoDB	consu...
telemetryIoExt	consu...

DB EPG

TENANT Tenant A

IMPORT

AP WordPress

EPG

WEB

APP

DB

Telemetry

Add EPG

Application Profile

CONTRACT

N-S-ExtToWeb

E-W-WebToApp

E-W-AppToDB

PROVIDED

TelemetryToExt

CONSUMED

COMMON PROPERTIES

* DISPLAY NAME

DB

Name: DB

CONTRACTS

NAME	TYPE
E-W-AppToDB	provider
TelemetryToExt	consu...

CONTRACT

ON-PREM PROPERTIES

* BRIDGE DOMAIN

WP-DB

SUBNETS

GATEWAY IP

10.18.109.1/24

SUBNET

Telemetry EPG

FILTERS

TENANT Tenant A

IMPORT

AP WordPress

EPG

WEB

APP

DB

Telemetry

Add EPG

Application Profile

CONTRACT

N-S-ExtToWeb

E-W-WebToApp

E-W-AppToDB

TelemetryToExt

CONSUMED

COMMON PROPERTIES

* DISPLAY NAME

Telemetry

Name: Telemetry

CONTRACTS

NAME	TYPE
TelemetryToExt	consu...

CONTRACT

ON-PREM PROPERTIES

* BRIDGE DOMAIN

FTD

SUBNETS

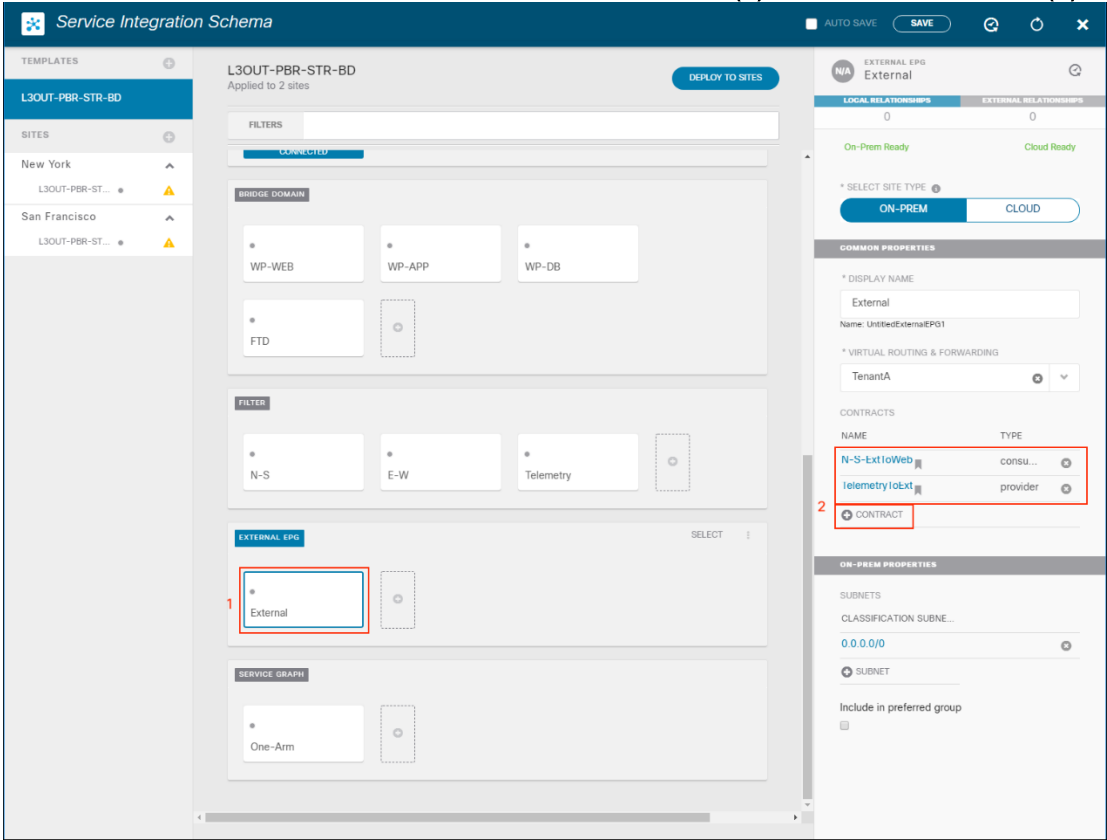
GATEWAY IP

SUBNET

USEG EPG

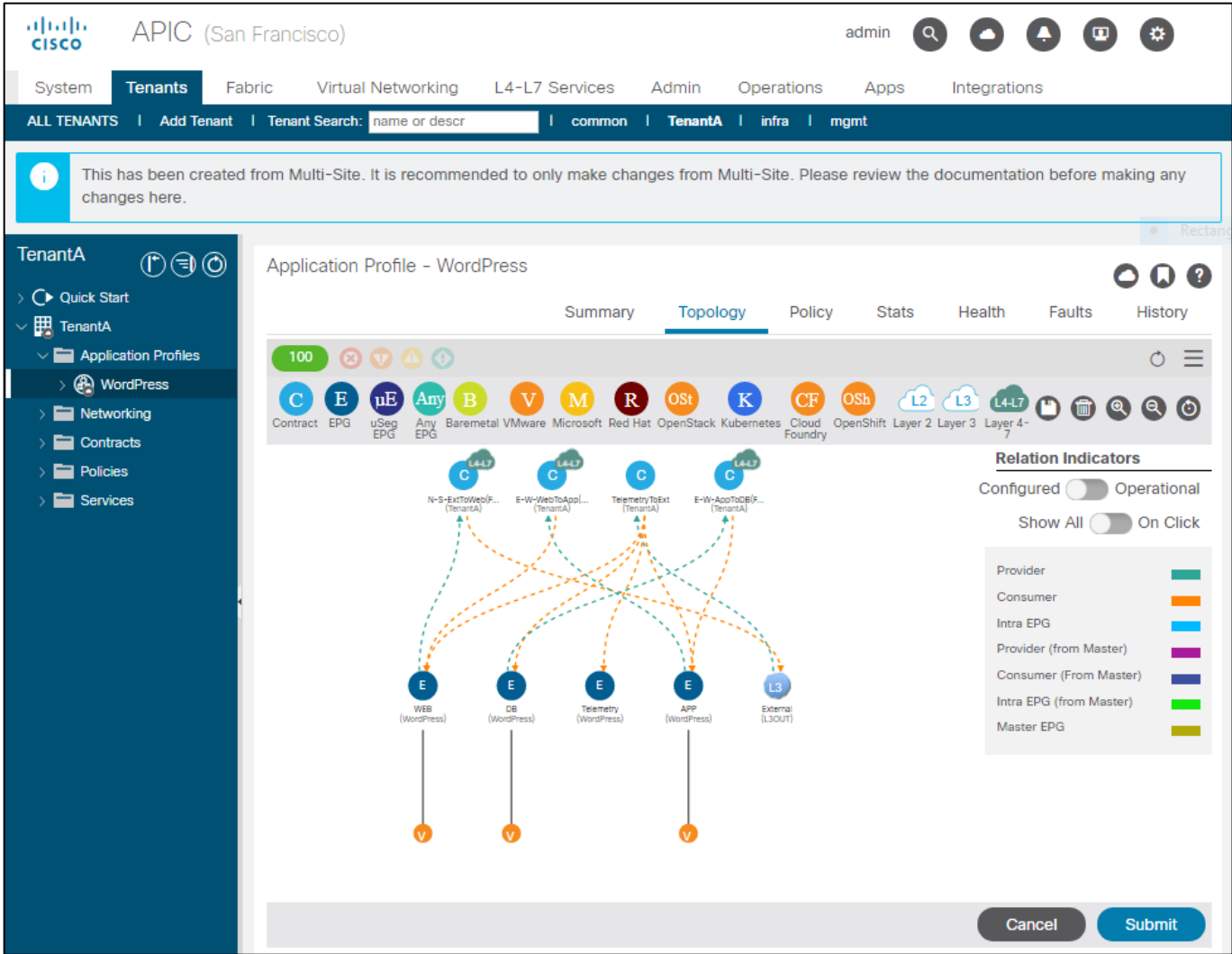
Step 10: Add contracts to External EPG

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



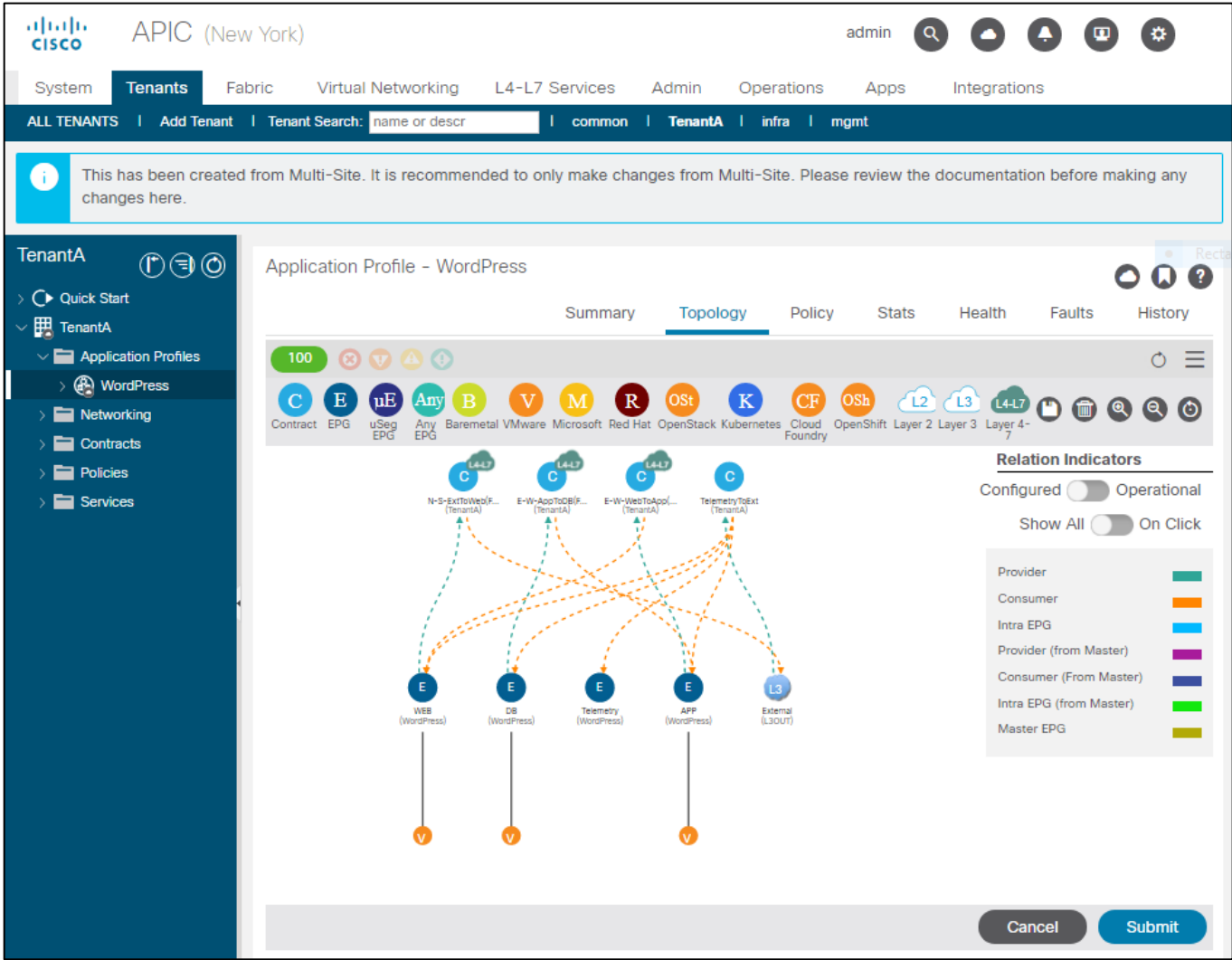
Step F: Verify Schema in APIC GUI

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



131

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

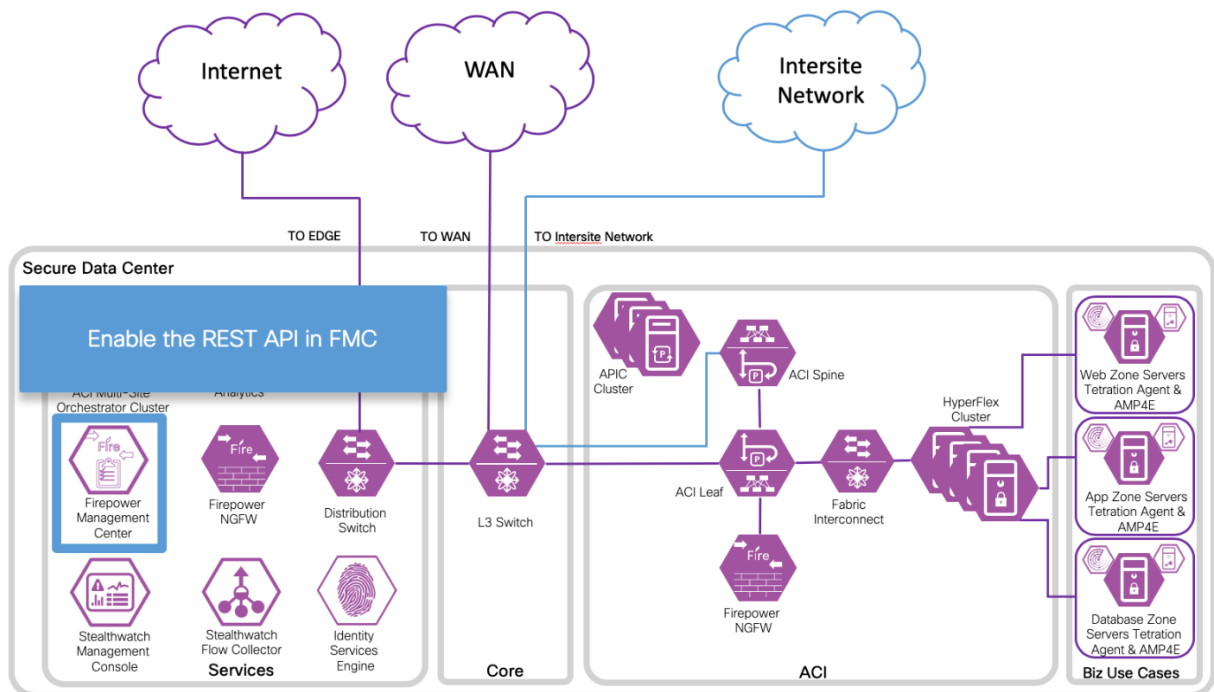


Test Case 2 – Firepower Management Center and APIC

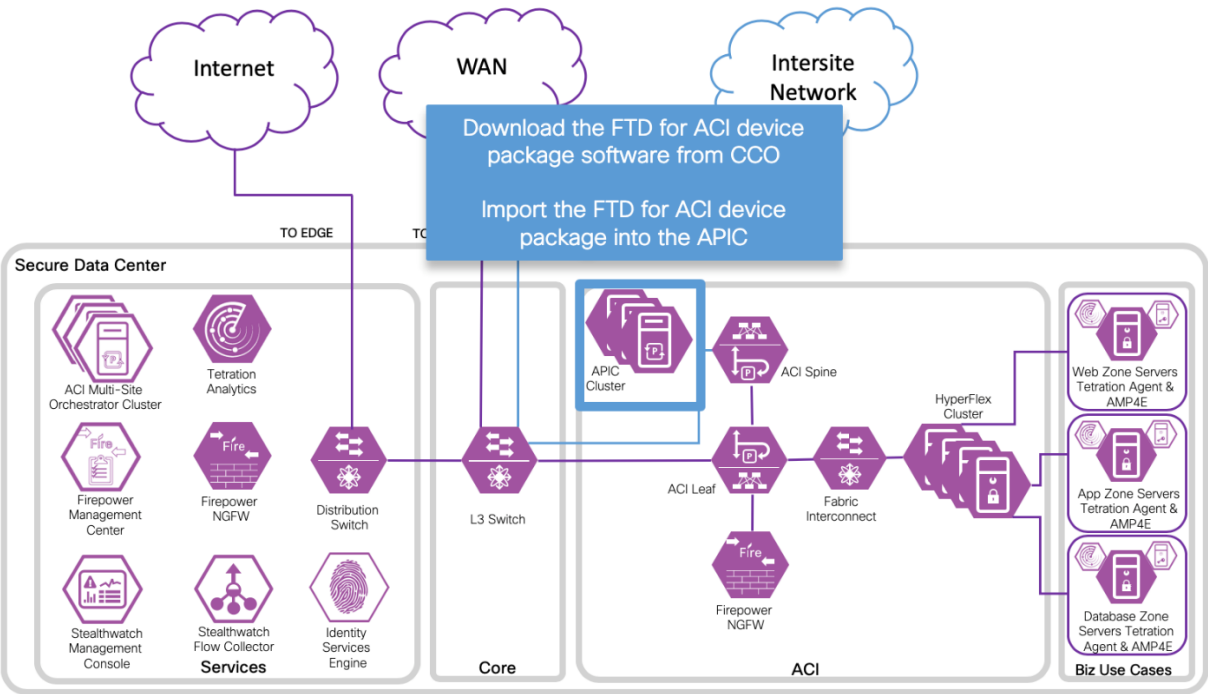
This integration involves building out a Multipod design with a single pod. The purpose of this test case is to confirm that the Firepower Threat Defense (FTD) device package works as expected with ACI. We selected a one-arm policy based redirect design similar to test case 1, but we tested with FTDv 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:

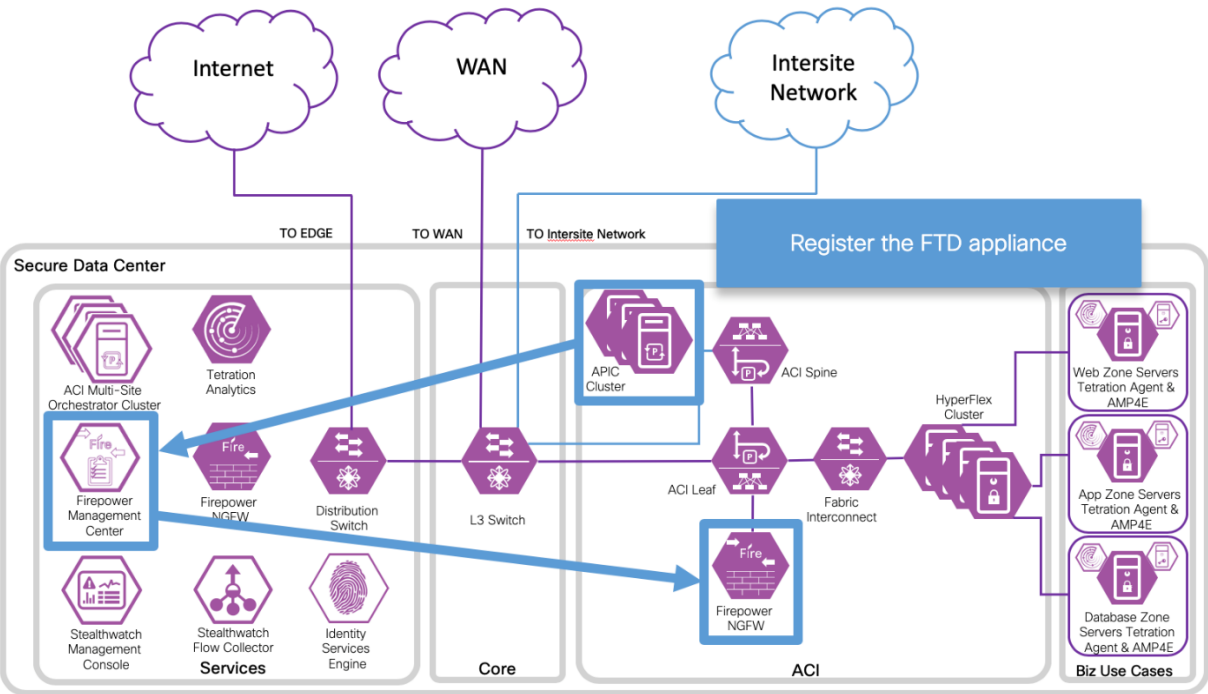
1. Enable the REST API in FMC.



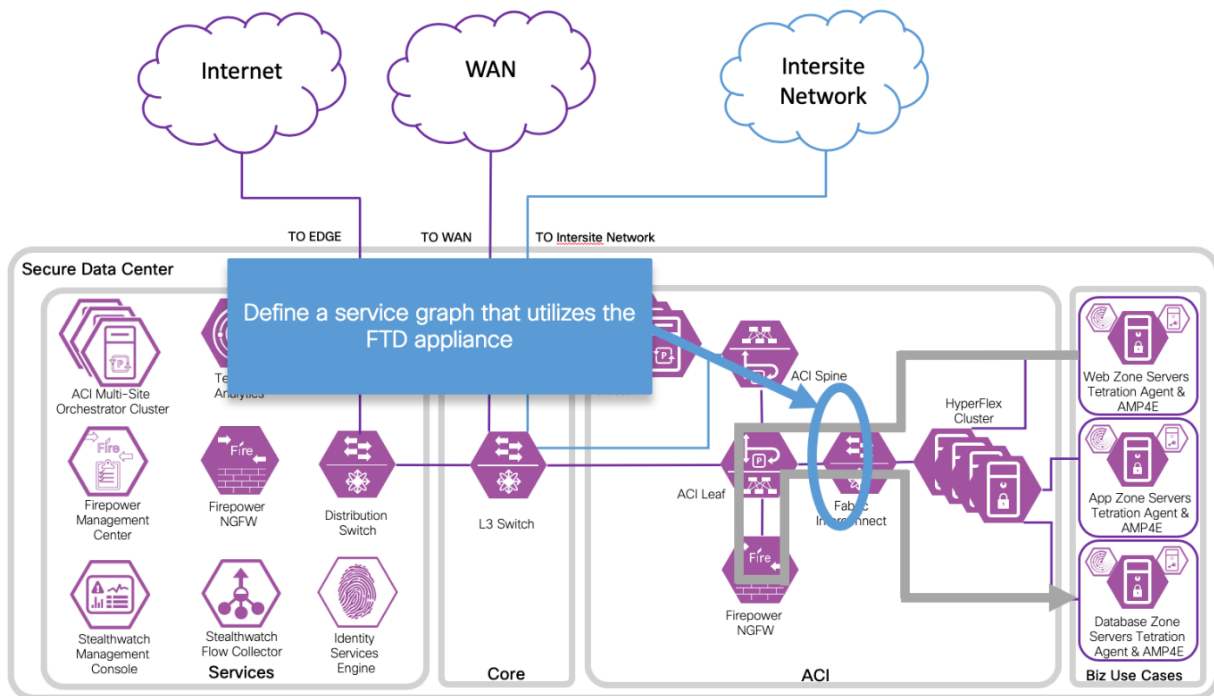
2. Download the FTD for ACI device package software from CCO and Import into APIC.



3. Register the FTD appliance.



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.

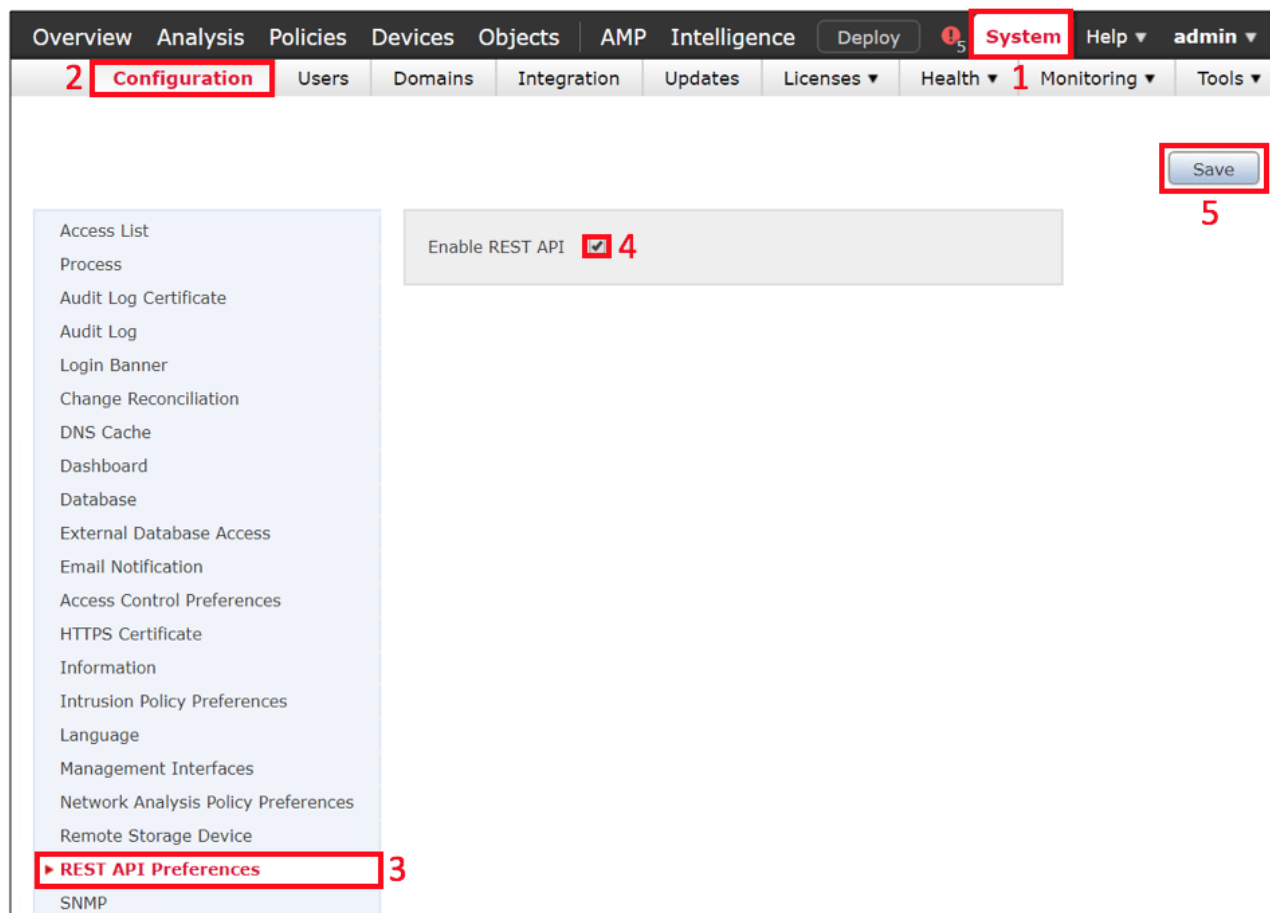
The APIC required configuration steps in Test Case 1 are assumed to have already been implemented.

135

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).



136

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>

The screenshot shows the Cisco Software Download page for the Firepower Management Center Virtual Appliance. The page includes a search bar, expand/collapse buttons, and a list of releases. The latest release, 1.0.3.13, is highlighted. Below the release list, there is a table with file information.

File Information	Release Date	Size
Cisco FTD Device Package - Fabric Insertion (FI) 1.0.3.13 for Cisco APIC 3.2(11) & FMC 6.2.3	04-JUN-2018	0.12 MB

The file name is `ftd-fi-device-pkg-1.0.3.13.zip`.

- 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).

The screenshot shows the Cisco APIC interface. The navigation path is highlighted with red boxes and numbers: 1. **L4-L7 Services**, 2. **Packages**, 3. **L4-L7 Service Device Types**, and 4. **Import Device Package**.

Vendor	Model	Version	Functions
CISCO	ASA	1.3	Firewall
CISCO	ASA_FI	1.3	Firewall
CISCO	CloudMode	1.0	FW, LB
CISCO	FTD_FI	1.0	FTD

137

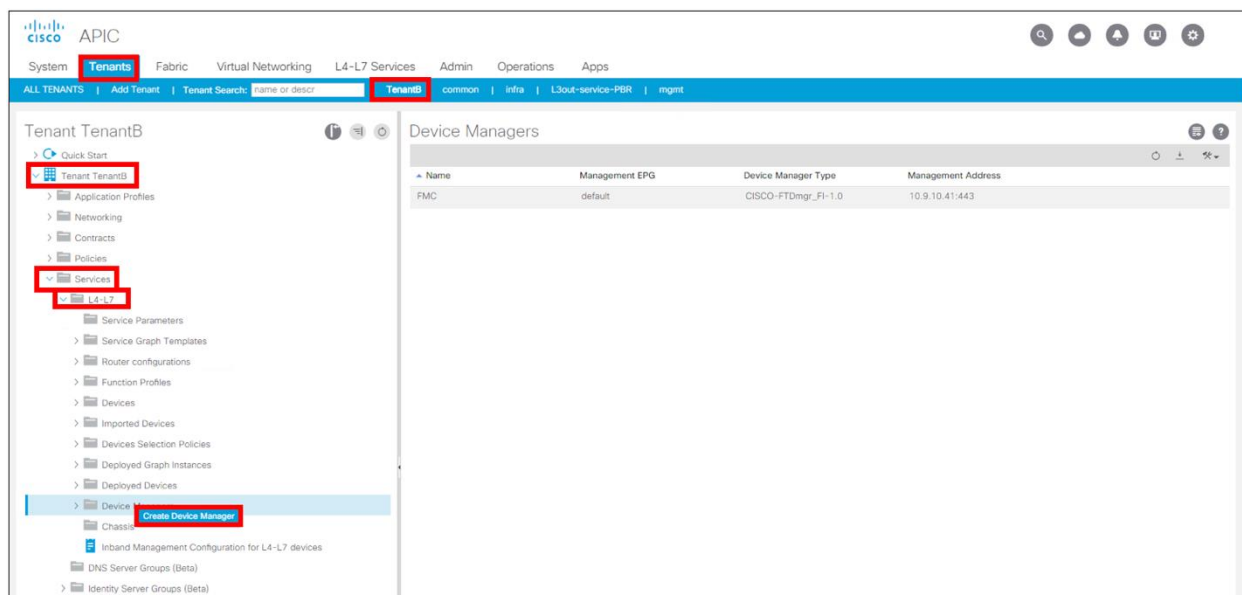
- c. View FTD device package. Navigate to **L4-L7 Services** (1)->**Packages** (2)->**L4-L7 Service Device Types** (3) and select **Cisco-FTD-FI-1.0** (4).

The screenshot displays the Cisco APIC web interface. At the top, the navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services' (marked with a red box and '1'), 'Admin', 'Operations', and 'Apps'. Below this, the 'Inventory' and 'Packages' (marked with a red box and '2') tabs are visible. On the left sidebar, under 'Packages', the 'L4-L7 Service Device Ty...' (marked with a red box and '3') is expanded, showing a list of packages: 'CISCO-ASA-1.3', 'CISCO-ASA_FI-1.3', 'CISCO-CloudMode-1.0', and 'CISCO-FTD-FI-1.0' (marked with a red box and '4'). The main content area shows the details for 'L4-L7 Service Device Type - CISCO-FTD_FI-1.0'. The 'General' tab is active, displaying properties such as Vendor (CISCO), Model (FTD_FI), Capabilities (GoThrough, GoTo), Major Version (1.0), Minor Version (3.13), Minimum Required Controller Version (1.0), Logging Level (DEBUG), Package Name (device_script.py), and Interface Labels (external, internal, mgmt). At the bottom right, there are buttons for 'Show Usage', 'Reset', and 'Submit'.

138

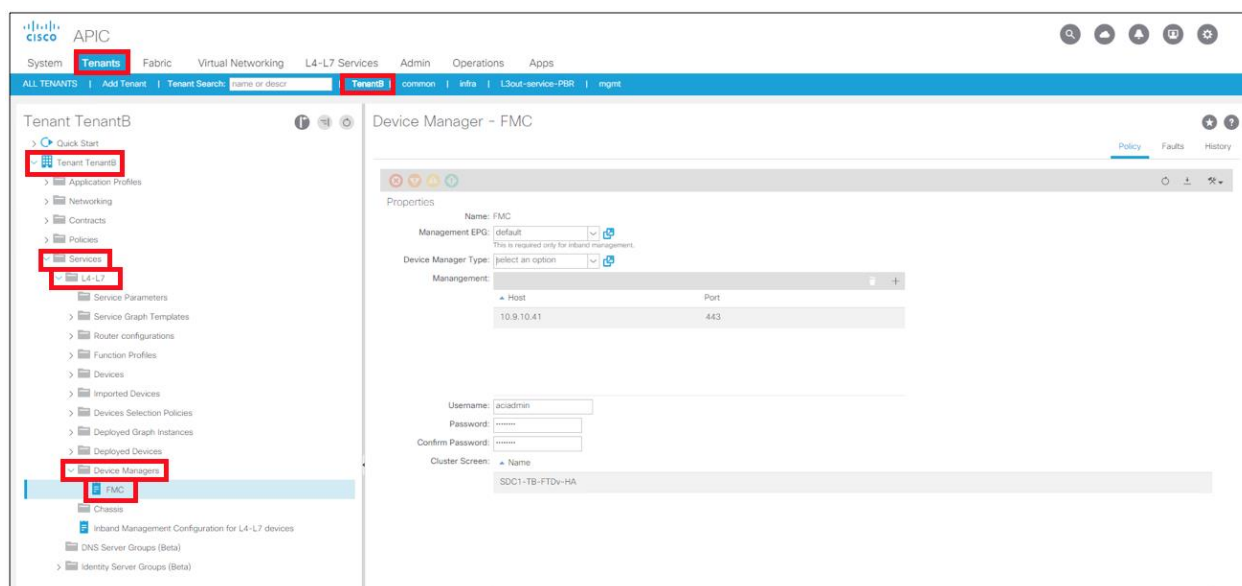
Step 3

- 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.

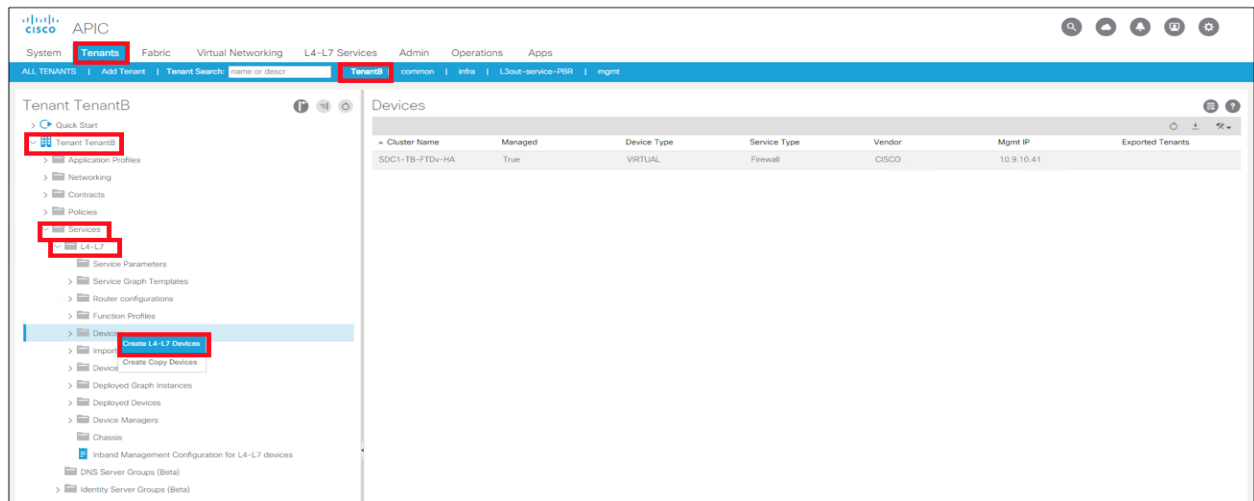
Note: It is recommended to setup unique credentials in FMC for APIC so that it can be identified easily in the FMC audit logs.



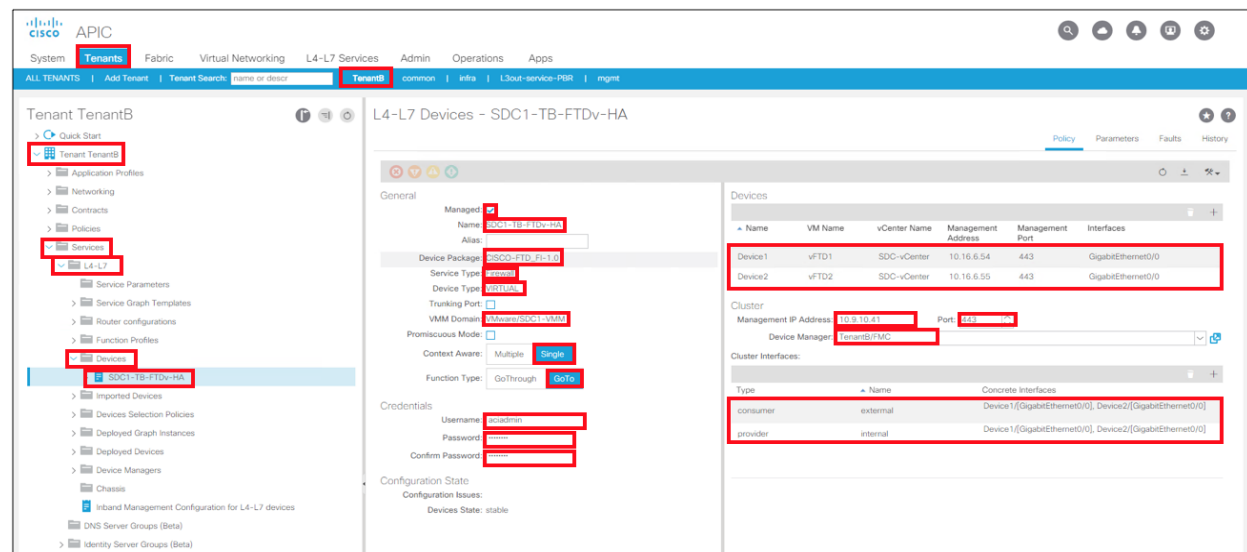
139

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.



140

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).

The screenshot shows the Cisco APIC web interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', and 'Apps'. The 'Tenants' tab is selected, and the 'TenantB' tenant is chosen from the dropdown. The left sidebar shows the navigation tree for 'TenantB', with 'Services' (3), 'L4-L7' (4), 'Function Profiles' (5), and 'FTDv' (6) highlighted. The right pane displays the 'L4-L7 Services Function Profile Group - FTDv' configuration page. The 'Properties' section shows 'Name: FTDv' and 'Alias:'. The 'Service Function Profiles' table lists four profiles: 'FTDv-InlineMode', 'FTDv-RoutedMode', 'FTDv-RoutedMode-onearm', and 'FTDv-TransparentMode', all associated with the 'FTD' function. A right-click context menu is open over the 'FTDv' item in the left sidebar, with the option 'Create L4-L7 Services Function Profile' (7) highlighted.

Name	Associated Function
FTDv-InlineMode	FTD
FTDv-RoutedMode	FTD
FTDv-RoutedMode-onearm	FTD
FTDv-TransparentMode	FTD

- 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/RouteModeForFTD. 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.

Create L4-L7 Services Function Profile

Create Function Profile

Name: FTDv-RouteMode-onearm 1

Description: optional

Copy Existing Profile Parameters: 2

Profile: CISCO-FTD-FI-1.0/RouteModeForFTD 3

Features and Parameters

Note: In order to automatically apply new values to the parameters of an existing graph instance when users modify function profiles, the name of the top folder must end with "-Default".

Features

Basic Parameters

All Parameters

Interfaces

All

4

Folder/Parameter	Name	Hint	Path from Schema	Value	Mandatory	Locked	Shared
Device Config	Device						
Access Policy	ACIAccPolicyR...				false	false	
Bridge Group Int...							
Inline Set							
Interface	externalInterface				false	false	
Interface	internalInterface				false	false	
Security Zone	ConsSZRT				false	false	
Security Zone	ProvSZRT				false	false	
Function Config	Function						
Access Policy C...	AccessPolicyF...				false	false	

5

Cancel

Submit

142

- 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.

L4-L7 Services Function Profile - FTDv-RoutedMode-onearm

General Faults History

Properties

Name: FTDv-RoutedMode-onearm

Description:

Associated Function: CISCO-FTD_FI-1.0/FTD

Features and Parameters

Features

Interfaces

All

Folder/Parameter	Name	Hint	Path from Schema	Value	Mandatory	Locked	Shared
Device Config	Device						
Access Policy	SDC1-TB-FTDv-HA				false	false	
Access Rules	App-to-DB				false		
Destination Interface	DBZone				false		
DestinationZone	DBZone		externalinterface/int_security_zone		false	false	
Source Interface	AppZone				false		
SourceZone	AppZone		externalinterface/int_security_zone		false	false	
Bi-Directional	bidirectional		true		false	false	
Access Rules	Outside-to-Web				false		
Destination Interface	WebZone				false		
DestinationZone	WebZone		externalinterface/int_security_zone		false	false	
Source Interface	OutsideZone				false		
SourceZone	OutsideZone		externalinterface/int_security_zone		false	false	
Bi-Directional	Bi-Directional		true		false	false	
Access Rules	Web-to-App				false		
Destination Interface	AppZone				false		
DestinationZone	AppZone		externalinterface/int_security_zone		false	false	
Source Interface	WebZone				false		
SourceZone	WebZone		externalinterface/int_security_zone		false	false	
Bi-Directional	bidirectional		true		false	false	
Interface	externalinterface				false	false	
Security Zone	OneArm				false	false	
Function Config	Function						

143

- d. Create One Arm Function Profile – Interface, Security Zone, Access Policy Configuration, External and Internal Interface Configuration. The Interface policy for the external interface 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 external interface.

L4-L7 Services Function Profile - FTDv-RoutedMode-onearm

General Faults History

Properties

Name: FTDv-RoutedMode-onearm

Description:

Associated Function: CISCO-FTD_FI-1.0/FTD

Features and Parameters

Features

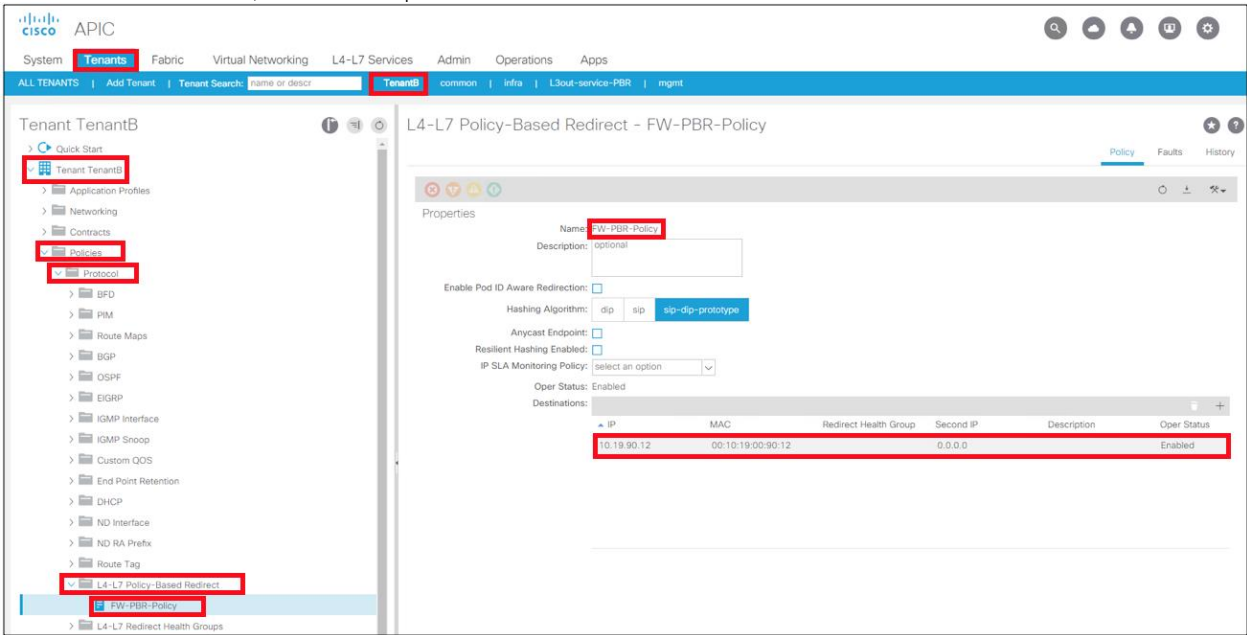
Interfaces

All

Folder/Parameter	Name	Hint	Path from Schema	Value	Mandatory	Locked	Shared
Device Config	Device						
Access Policy	SDC1-TB-FTDv-HA				false	false	
Interface	externalInterface				false	false	
IPv4 Address Configuration	IPv4Config				false		
Use Static IP	static				false		
IP Address	address			10.19.90.12/24	true	false	
Static Routes List	StaticRoute				false		
IPv4 Static Route	IPv4StaticRoute				false		
Metric	metric			1	false	false	
Gateway	gateway			10.19.90.1	true	false	
Network	network			0.0.0.0/0	true	false	
Interface Security Zone	int_security_zone				false		
Security Zone	security_zone			OneArm	false	false	
Enabled	enabled			true	false	false	
Logical Name	ifname			Consumer	false	false	
Security Zone	OneArm				false	false	
Type	type			ROUTED	false	false	
Function Config	Function						
Access Policy Configuration	AccessPolicyFolder				false	false	
Access Policy Configuration	InAccessPolicyRel			SDC1-TB-FTDv-HA	false	false	
External Interface Configuration	ExtConfig				false	false	
Interface Configuration	ExtConfigRel			externalInterface	false	false	
Internal Interface Configuration	IntConfig				false	false	
Interface Configuration	InConfigRel			externalInterface	false	false	

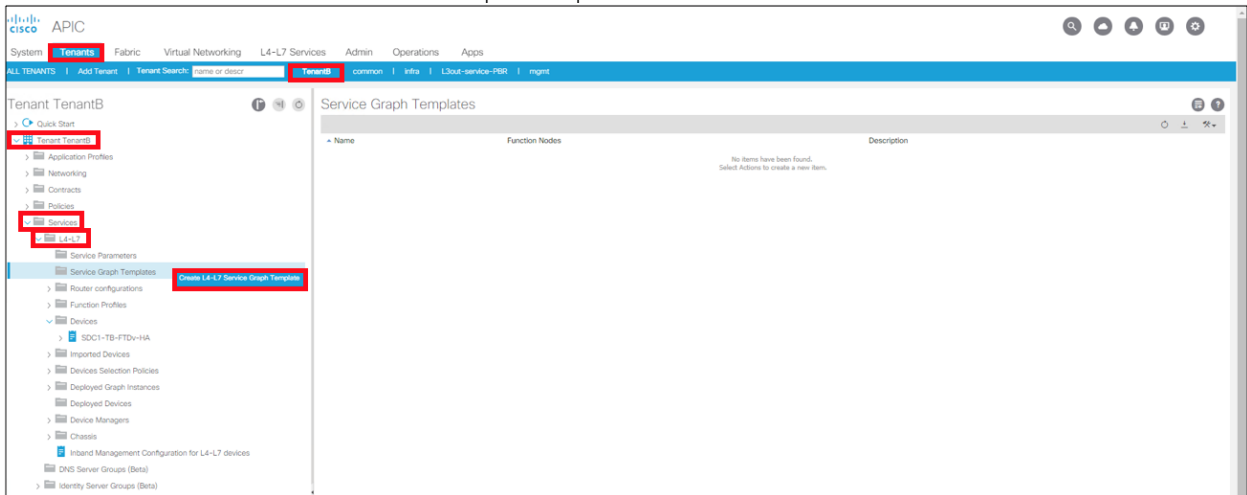
Step 6

- 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.



145

b. Create One Arm PBR Service Graph with FTDv HA

Create L4-L7 Service Graph Template

Drag device clusters to create graph nodes.

Device Clusters

- svcType: FW
- TenantB/SDC1-TB-FTDv-HA (Managed)

Service Graph Name: SDC-OneArm

Graph Type: ☒ Create a New Graph ☐ Clone an Existing Graph

Consumer EPG — C — SDC1-TB-F... — P — Provider EPG

FTDv-HA

SDC1-TB-FTDv-HA Information

Firewall: ☒ Routed ☐ Transparent

Profile: TenantB/FTDv/FTDv-RoutedMode-one

Route Redirect: ☒

Cancel Submit

Step 8

a. Apply L4-L7 Service Graph

APIC

System: **Tenants** Fabric Virtual Networking L4-L7 Services Admin Operations Apps

ALL TENANTS | Add Tenant | Tenant Search: Name or device | **TenantB** | common | Infra | L4-L7-service-PBR | mgmt

Tenant TenantB

- Quick Start
- Tenant Templates
- Application Profiles
- Networking
- Contracts
- Policies
- Network
- Service Parameters
- Service Graph Templates
- SDC-OneArm
- Router configuration
- Function Profiles
- Devices
- SDC1-TB-FTDv
- Imported Devices
- Devices Selection
- Deployed Graphs
- Deployed Devices
- Device Managers
- Chassis
- Inband Management Configuration for L4-L7 devices
- DNS Server Groups (Beta)
- Identity Server Groups (Beta)

Apply L4-L7 Service Graph Template

L4-L7 Service Graph Template - SDC-OneArm

Topology Policy Faults History

Consumer EPG — C — SDC1-TB-F... — P — Provider EPG

FTDv-HA

SDC1-TB-FTDv-HA Information

Firewall: Routed

Profile: FTDv-RoutedMode-onearm

Route Redirect: true

146

b. Create Outside-to-Web Contract

Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

1. Contract 2. Graph

Config a Contract Between EPGs

EPGs Information

Consumer EPG / External Network:

Provider EPG / Internal Network:

Contract Information

Contract: ☒ Create A New Contract ☐ Choose An Existing Contract Subject

Contract Name:

No Filter (Allow All Traffic): ☒

Previous Cancel Next

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

Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

1. Contract 2. Graph 3. SDC1-TB-FTDv-HA Configuration

Config a Service Graph

Service Graph Template:

Consumer

EPG

TB-Ext-EPG

Provider

EPG

Web-EPG

SDC1-TB-F... FTDv-HA

Policy-based Routing: true

Consumer Connector

Type: ☒ General ☐ Route Peering

BD:

L3 Destination (VIP): ☒

Redirect Policy:

Cluster Interface:

Provider Connector

Type: ☒ General ☐ Route Peering

BD:

L3 Destination (VIP): ☒

Redirect Policy:

Cluster Interface:

Previous Cancel Next

147

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

Apply L4-L7 Service Graph Template To EPGs

STEP 3 > SDC1-TB-FTDv-HA Configuration

1. Contract 2. Graph 3. SDC1-TB-FTDv-HA Configuration

Config parameters for the selected device

Profile Name: FTDv-RoutedMode-onearm

Features

Required Parameters All Parameters

Interfaces

All

Folder/Parameter	Name	Value	Write Domain
Device Config	Device		
Access Policy	SDC1-TB-FTD...		
Bridge Group Interface			
Inline Set			
Interface	externalInterface		
Security Zone	OneArm		
Type	type	ROUTED	
Function Config	Function		
Access Policy Configuration	AccessPolicyF...		
Bridge Group Interface Configuration			
External Interface Configuration	ExtConfig		
Internal Interface Configuration	IntConfig		

RED indicates parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

Previous Cancel Finish

e. Create Web-to-App Contract

Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

1. Contract 2. Graph

Config a Contract Between EPGs

EPGs Information

Consumer EPG / External Network: TenantB/opencart/epg-Web-EPG

Provider EPG / Internal Network: TenantB/opencart/epg-App-EPG

Contract Information

Contract: Create A New Contract Choose An Existing Contract Subject

Contract Name: Web-to-App

No Filter (Allow All Traffic): ☒

148

f. Create App-to-DB Contract

Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

Config a Contract Between EPGs

EPGs Information

Consumer EPG / External Network: **TenantB/opencart/epg-App-EPG** Provider EPG / Internal Network: **TenantB/opencart/epg-DB-EPG**

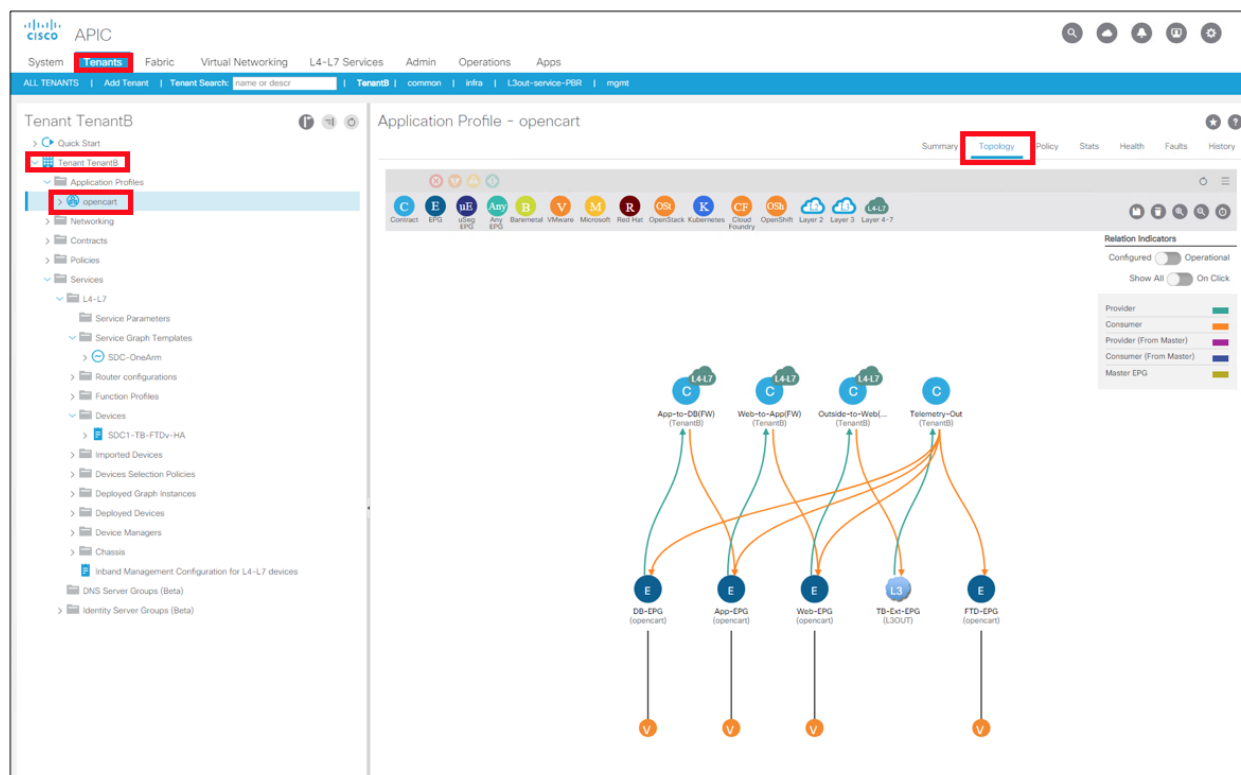
Contract Information

Contract: ☒ Create A New Contract ☐ Choose An Existing Contract Subject

Contract Name: **App-to-DB**

No Filter (Allow All Traffic): ☒

g. Application Profile Topology for OpenCart



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

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligence

Device ManagementNATVPNQoSPlatform SettingsFlexConfigCertificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By : GroupAll (12)Error (0)Warning (0)Offline (1)Normal (11)Deployment Pending (0)

Name	Model	Version	Licenses	Access Control Policy	Group
Ungrouped (8)					
AWS-NGFW01 10.20.241.100 - Routed	Cisco Firepower Threat Defense for AWS	6.2.3	Base, Threat, Malware, URL Filtering	AWS-Web-Blog	
AWS-NGFW02 10.20.242.100 - Routed	Cisco Firepower Threat Defense for AWS	6.2.3	Base, Threat, Malware, URL Filtering	AWS-Web-Blog	
FTD-CAMP-HA Cisco Firepower 4110 Threat Defense High Availabilit					
FW-DC-1 10.16.4.26 - Routed	Cisco Firepower 4110 Threat Defense	6.2.3	Base, Threat, Malware, URL Filtering	SDC-Services	
FW-DMZ-1 10.16.4.25 - Routed	Cisco Firepower 4110 Threat Defense	6.2.3	Base, Threat, Malware, URL Filtering	Internet-Edge	
SDC1-FTD-C1 Cisco Firepower 9000 Series SM-36 Threat Defense C					
SDC2-FTD-C1 Cisco Firepower 4110 Threat Defense Cluster					
TB-FTDv-HA Cisco Firepower Threat Defense for VMWare High Ave					
vFTD-1(Primary, Active) 10.16.6.54 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3.6	Base, Threat, Malware, URL Filtering	SDC1-TB-FTDv-HA	
vFTD-2(Secondary, Standby) 10.16.6.55 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3.6	Base, Threat, Malware, URL Filtering	SDC1-TB-FTDv-HA	

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.

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligence

Device ManagementNATVPNQoSPlatform SettingsFlexConfigCertificates

TB-FTDv-HA

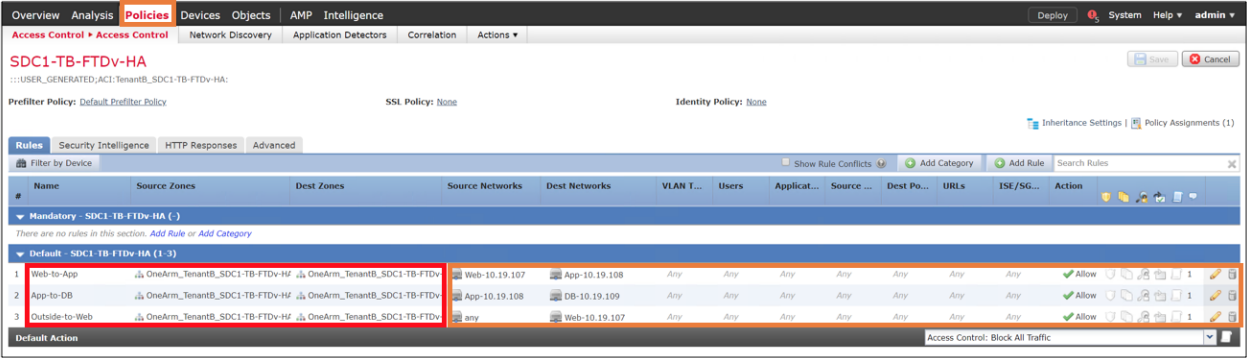
Cisco Firepower Threat Defense for VMWare

SummaryHigh AvailabilityDeviceRouting**Interfaces**Inline SetsDHCP

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0	Consumer_TenantB_SDC1-TB-FTD...	Physical	OneArm_TenantB_SDC1-TB-FTDv-HA	0010.1900.9012	10.19.90.12/24(Static)
	GigabitEthernet0/1		Physical			
	GigabitEthernet0/2		Physical			
	GigabitEthernet0/3		Physical			
	GigabitEthernet0/4		Physical			
	GigabitEthernet0/5		Physical			
	GigabitEthernet0/6		Physical			
	GigabitEthernet0/7		Physical			
	GigabitEthernet0/8		Physical			
	Diagnostic0/0	diagnostic	Physical			

150

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



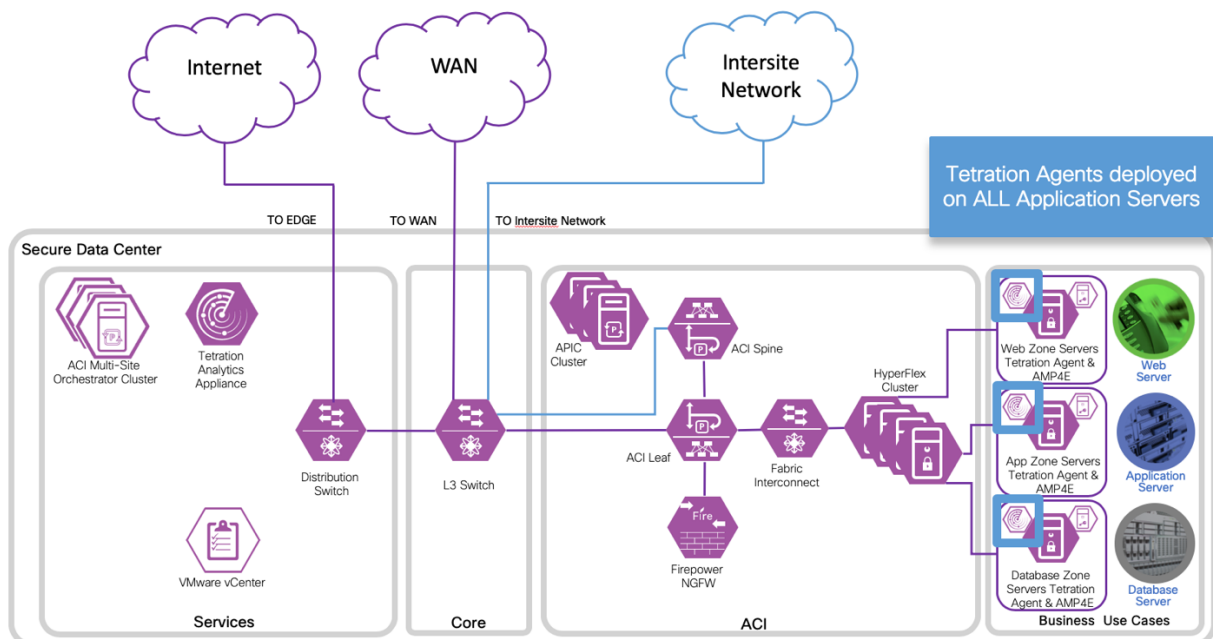
Test Case 3 – Tetration and VMware vCenter

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 Virtual 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 case 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 Virtual Appliance. Refer to **VMware vSphere Distributed Switch (VDS) and NetFlow** section in Test Case 4.

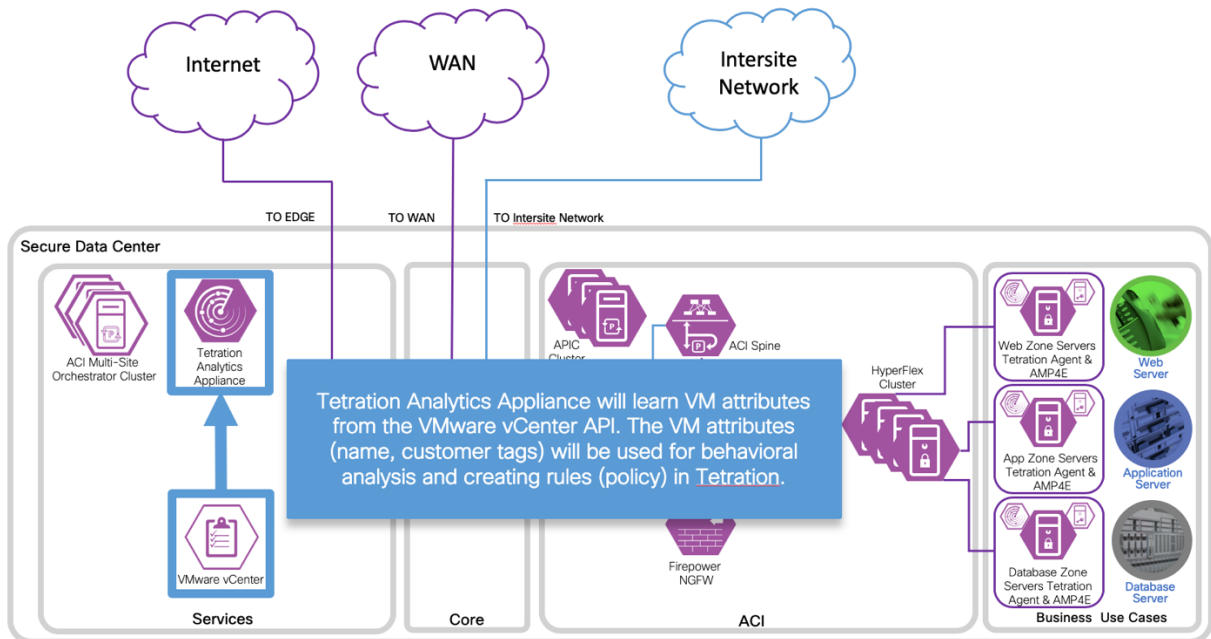
Test Description:

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

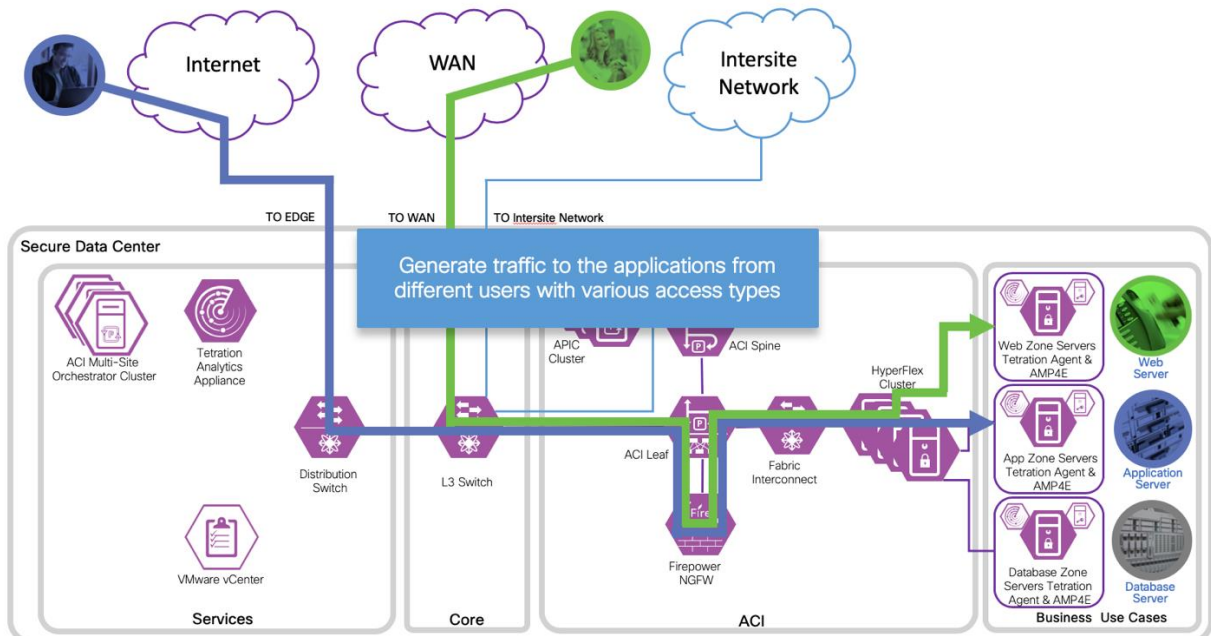


152

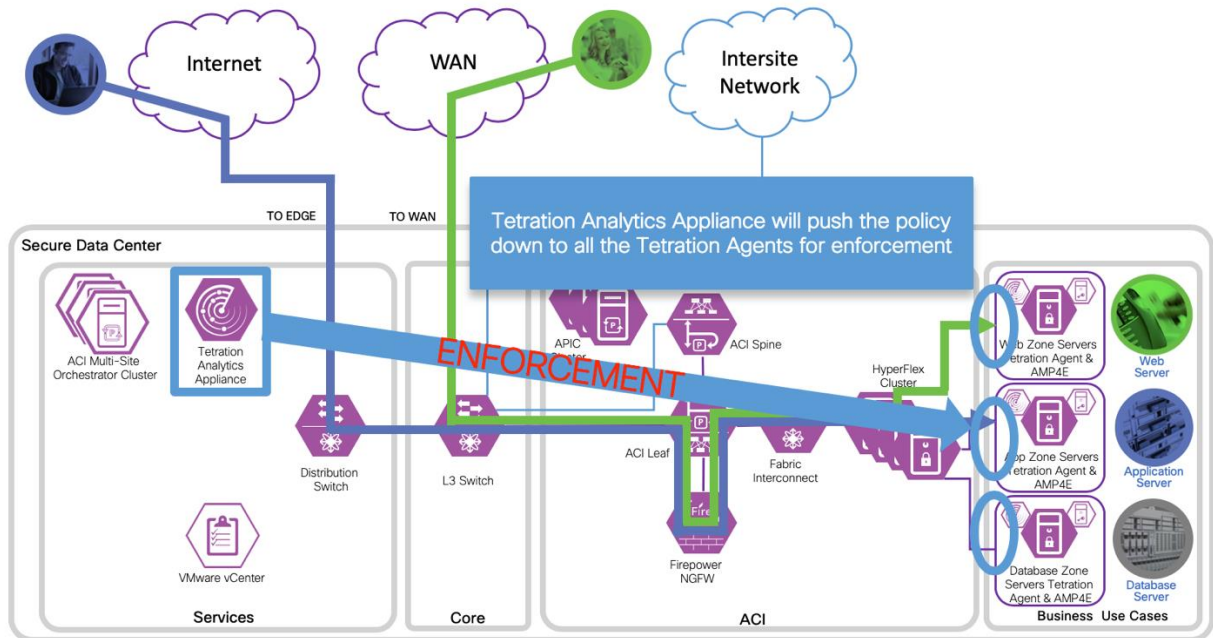
2. Tetration Analytics Appliance will learn VM attributes from the VMware vCenter API. The VM attributes (name, customer tags) will be used for behavioral analysis and creating rules (policy).



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.



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 Server 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.

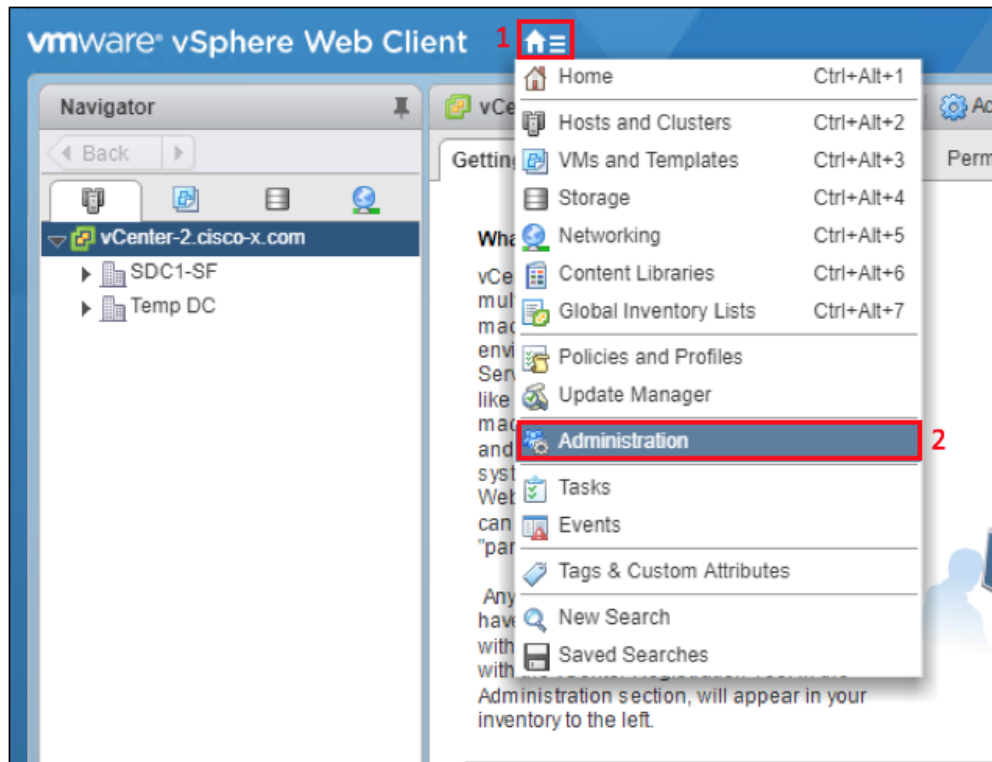
Deploying a Deep Visibility/Enforcement Linux Agent, https://<your-tetration-analytics-appliance-ip-address>/documentation/ui/software_agents/deployment.html#deploying-a-deep-visibility-enforcement-linux-agent.

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.

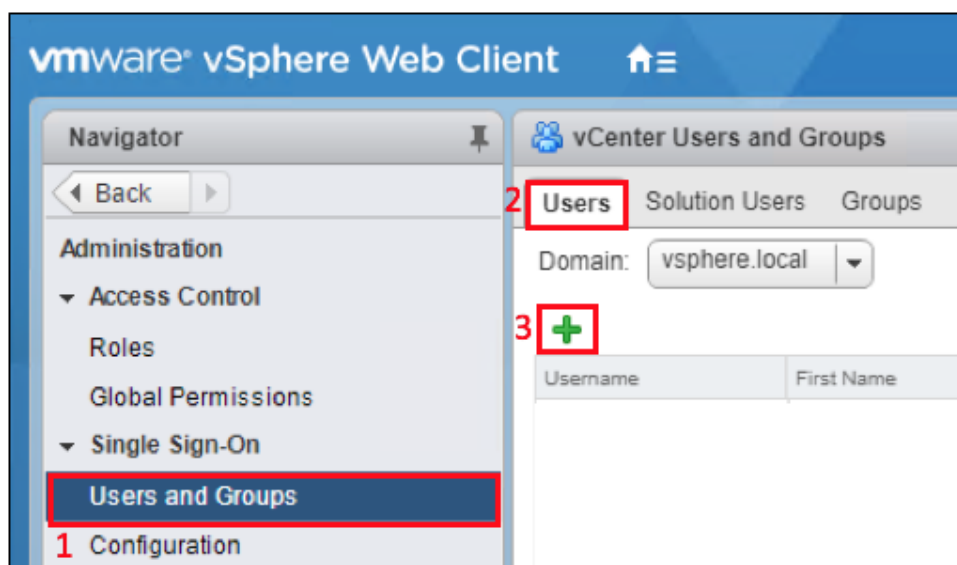
154

Step 2

- a. Setup Tetraton Analytics Appliance and vCenter integration. In vCenter, create login credentials specifically for Tetraton 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.



155

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

tetadmin1 - Edit

Enter values for this user, including the password.

User name:

Current Password:

Password:

Confirm password:

First name:

Last name:

Email address:

Description:

OK Cancel

- 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).

vmware vSphere Web Client

Launch vSphere Client (HTML5) | Administrator@VSPHERE.LOCAL | Help

vCenter Users and Groups

Users Solution Users **Groups** 2

Group Name	Domain	Description
ExternalIDUsers	vsphere.local	Well-known external IDP users' group, which registers e...
ComponentManager Administrators	vsphere.local	Component Manager Administrators
DCAAdmins	vsphere.local	
LicenseService Administrators	vsphere.local	License Service Administrators
ActAsUsers	vsphere.local	Act-As Users
Administrators	vsphere.local	
DCClients	vsphere.local	
CAAdmins	vsphere.local	
SystemConfiguration.Administrators	vsphere.local	Well-known configuration users' group which contains all...
SolutionUsers	vsphere.local	Well-known solution users' group, which contains all solu...
SystemConfiguration.BashShellAdministrators	vsphere.local	Access bash shell and manage local users on nodes
Users	vsphere.local	

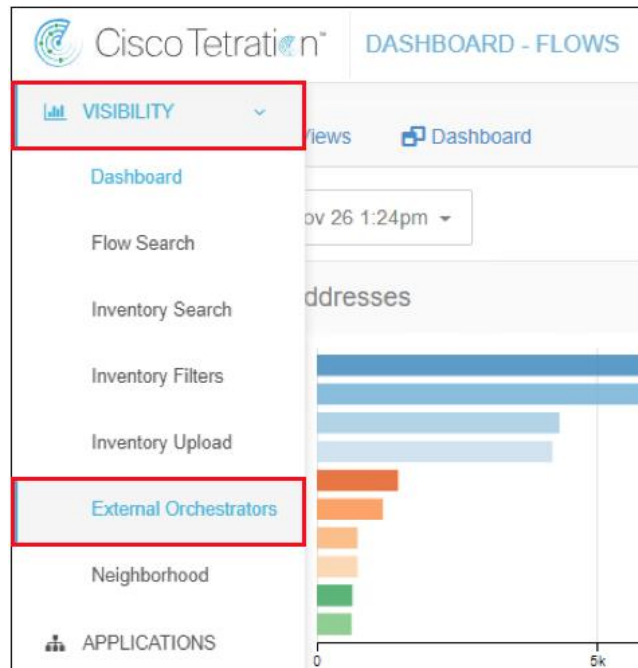
12 items Export Copy

Group Members

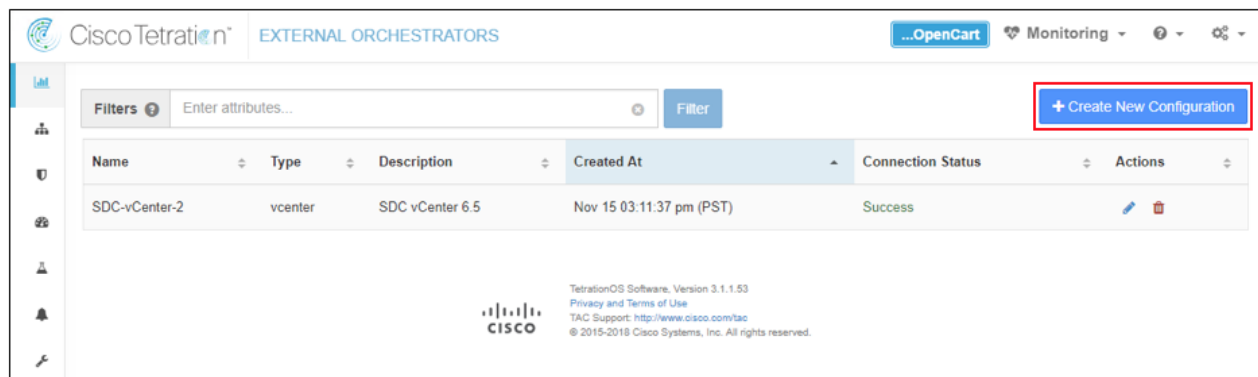
User/Group	Description/Full name	Domain	Member Type
Administrator	Administrator vsphere.local	vsphere.local	User
aciadmin1	ACI Admin	vsphere.local	User

156

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



- f. Select Create New Configuration



157

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

The screenshot shows the 'Edit External Orchestrator Configuration' dialog box with the 'Basic Config' tab selected. The 'Type' dropdown is set to 'vcenter'. The 'Name' field contains 'SDC-vCenter-2'. The 'Description' field contains 'SDC vCenter 6.5'. The 'Delta Interval (s)' field contains '60'. The 'Full Snapshot Interval (s)' field contains '3600'. The 'Username' field contains 'tetadmin1@vsphere.local'. The 'Password' field contains 'Password for the orchestration endpoint'. The 'Insecure' checkbox is unchecked.

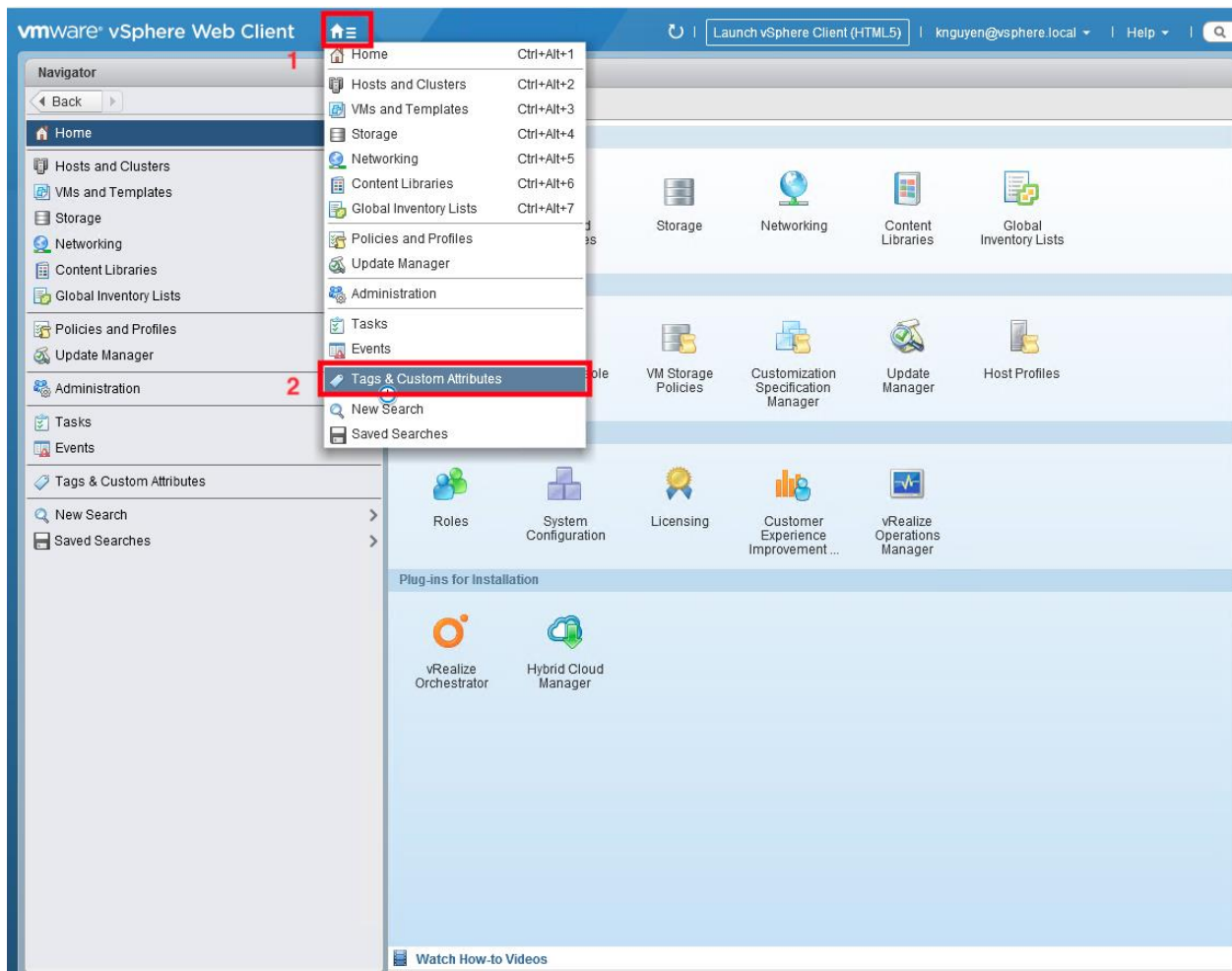
- h. In the Hosts Lists, Select the plus sign and enter the hostname (or IP address) and port.

The screenshot shows the 'Edit External Orchestrator Configuration' dialog box with the 'Hosts List' tab selected. The 'Hosts List' section shows a plus sign button, a text input field containing a hostname ending in '.com', a port input field containing '443', and a close button (X).

158

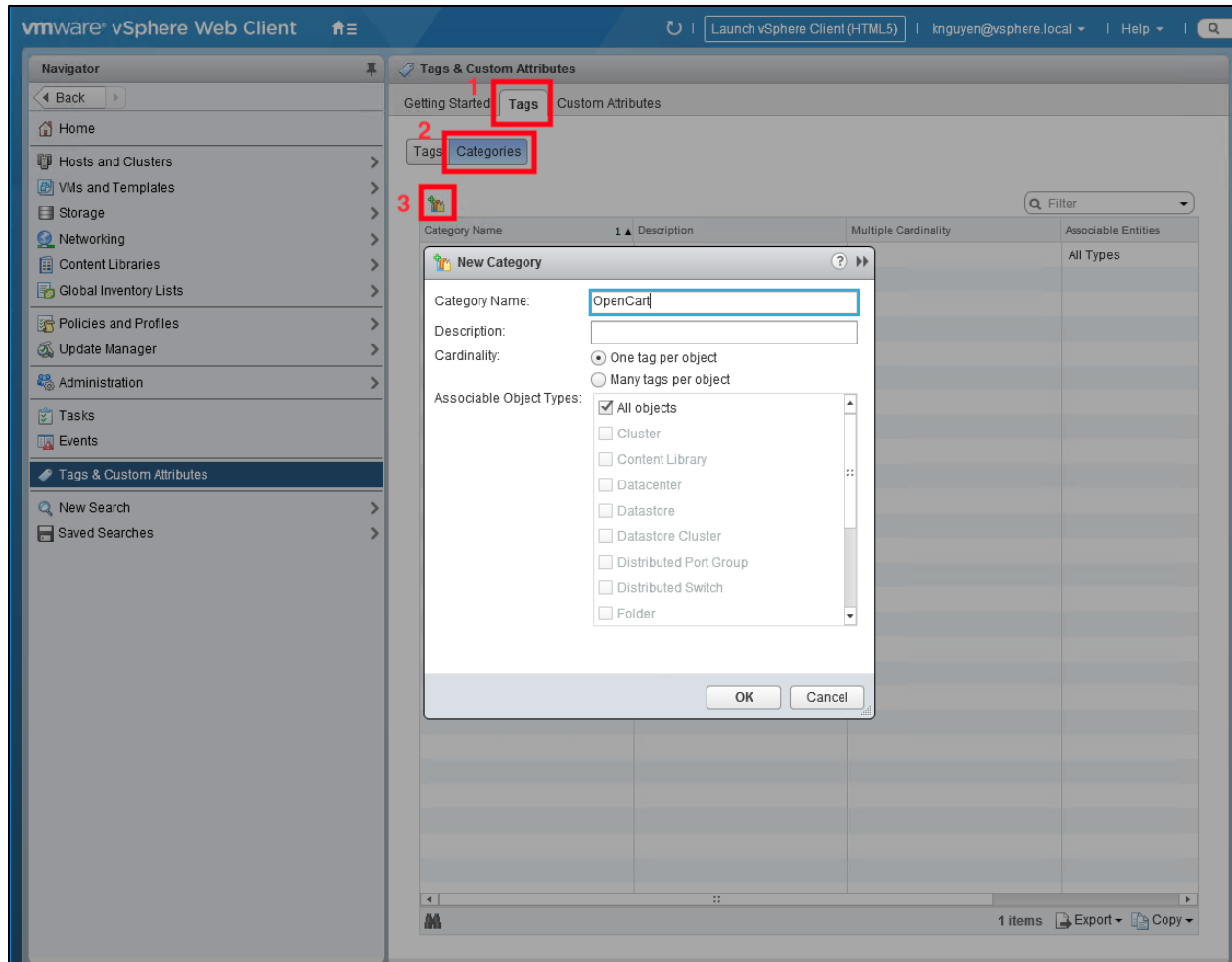
Step 3

- 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)**.

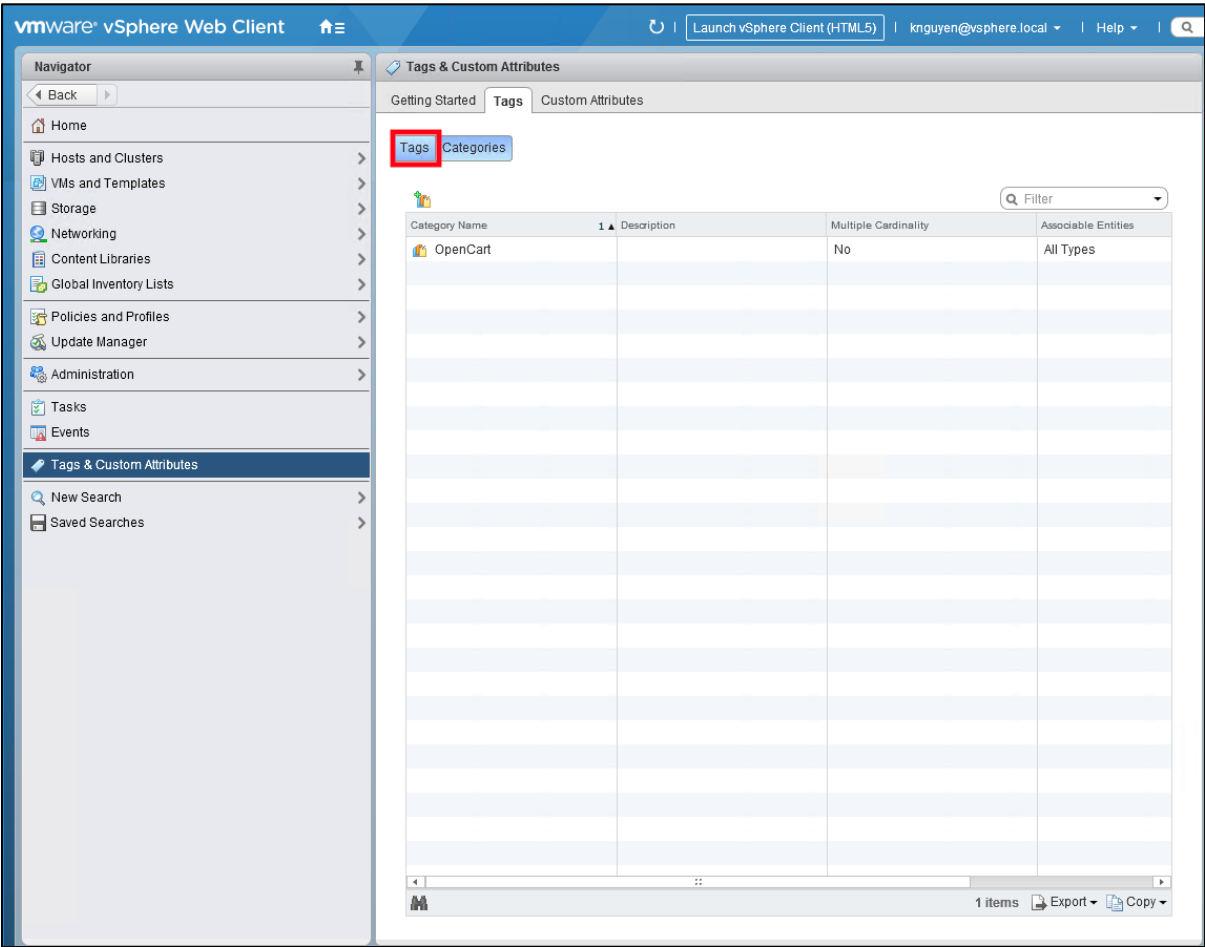


159

- 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.

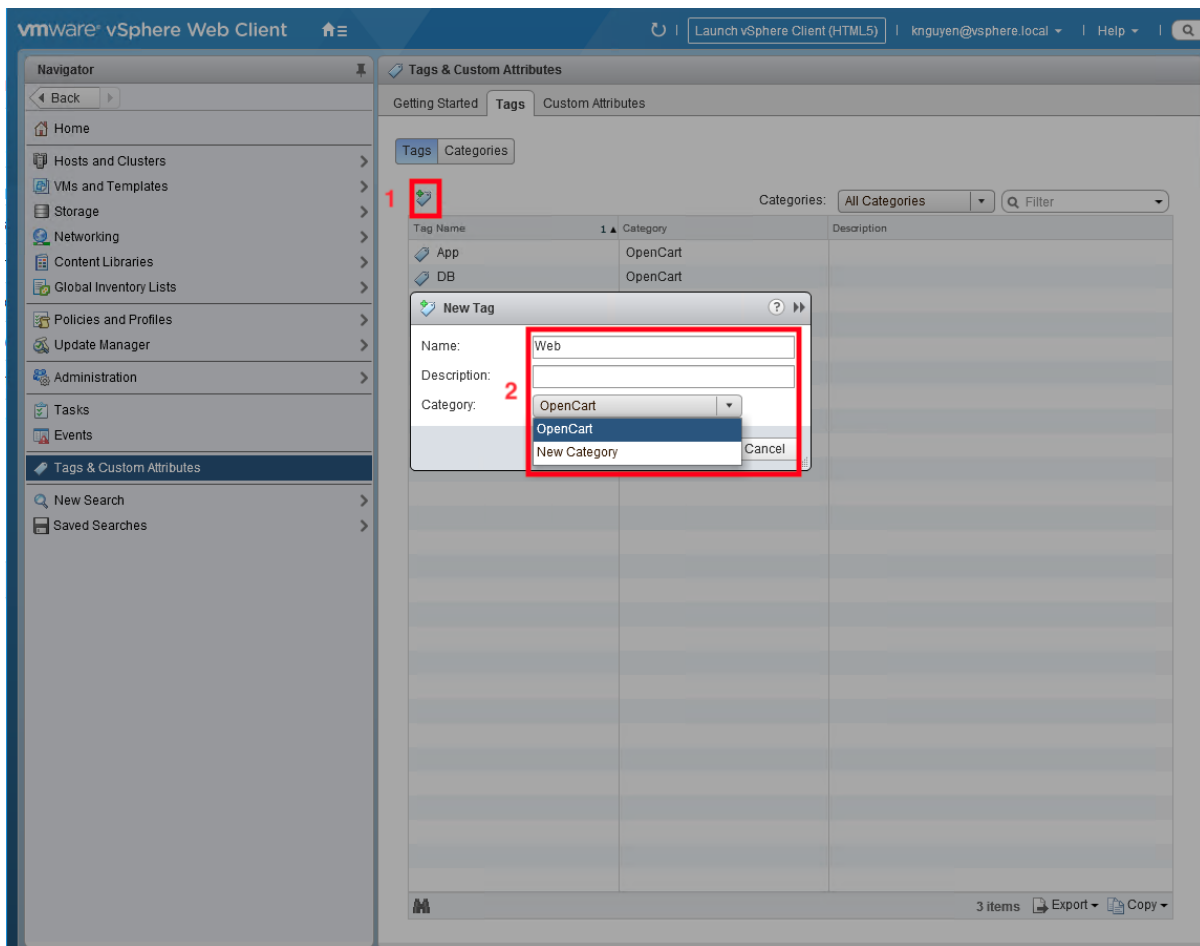


c. Select **Tags** tab.



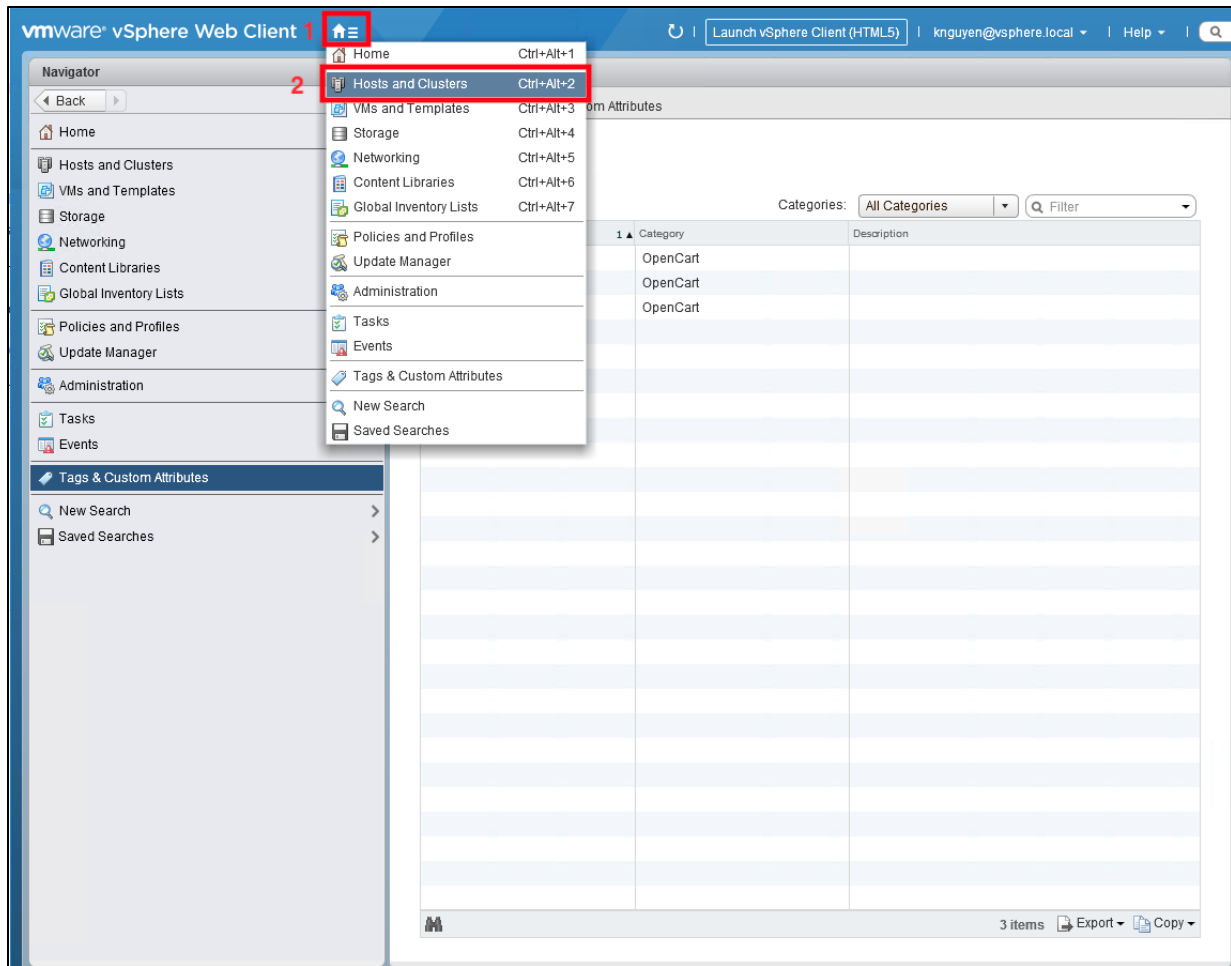
161

- 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.



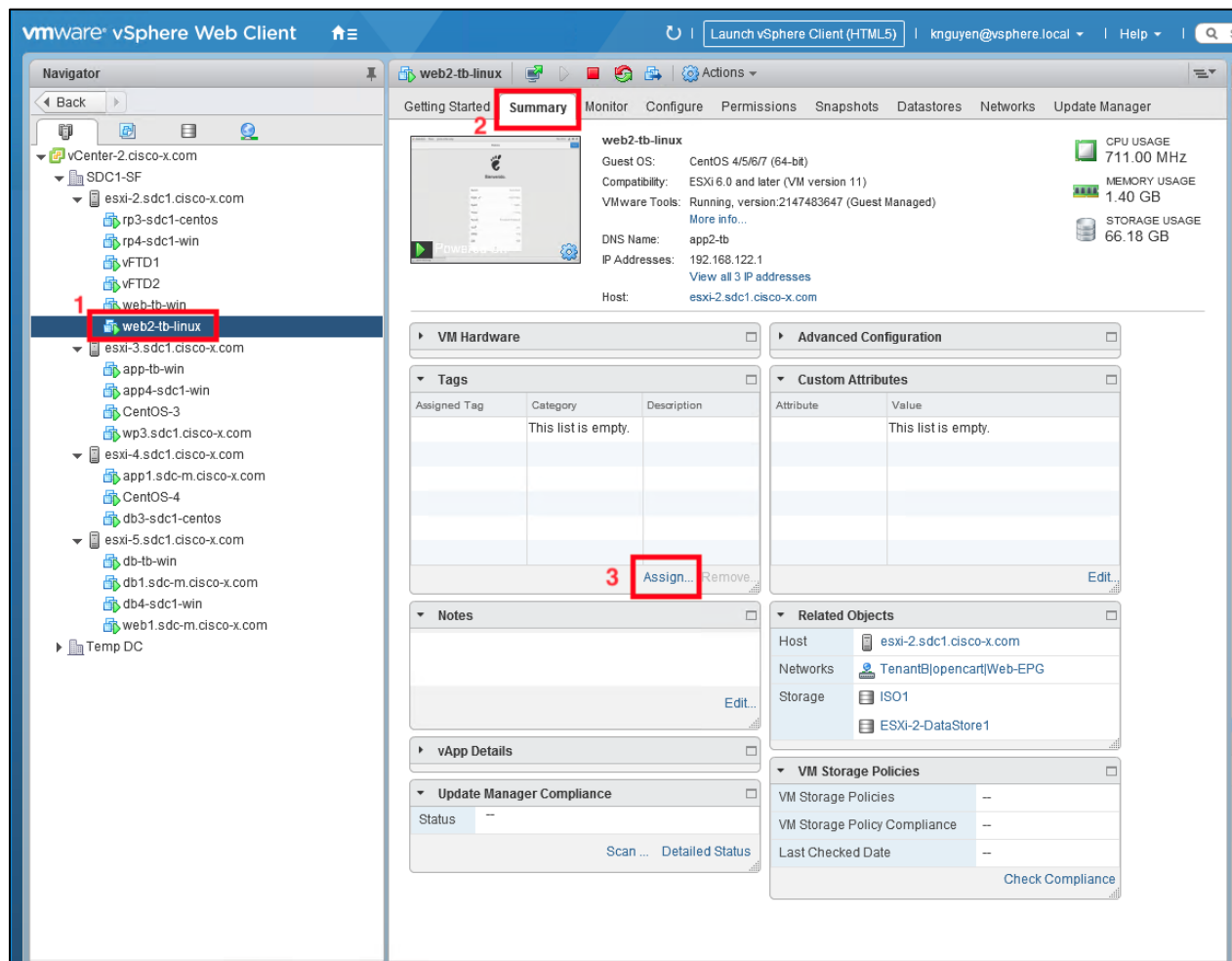
162

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

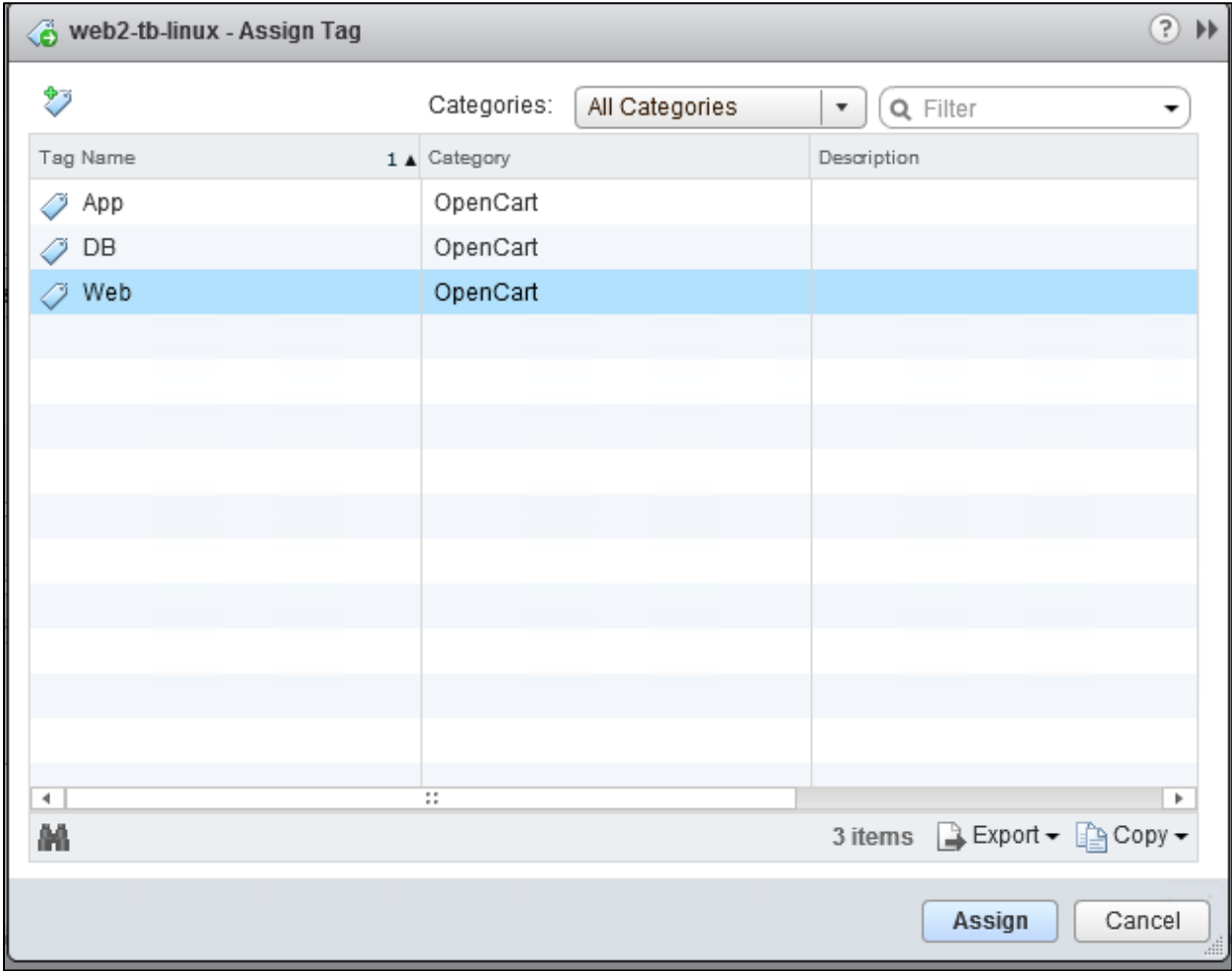


163

- 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).

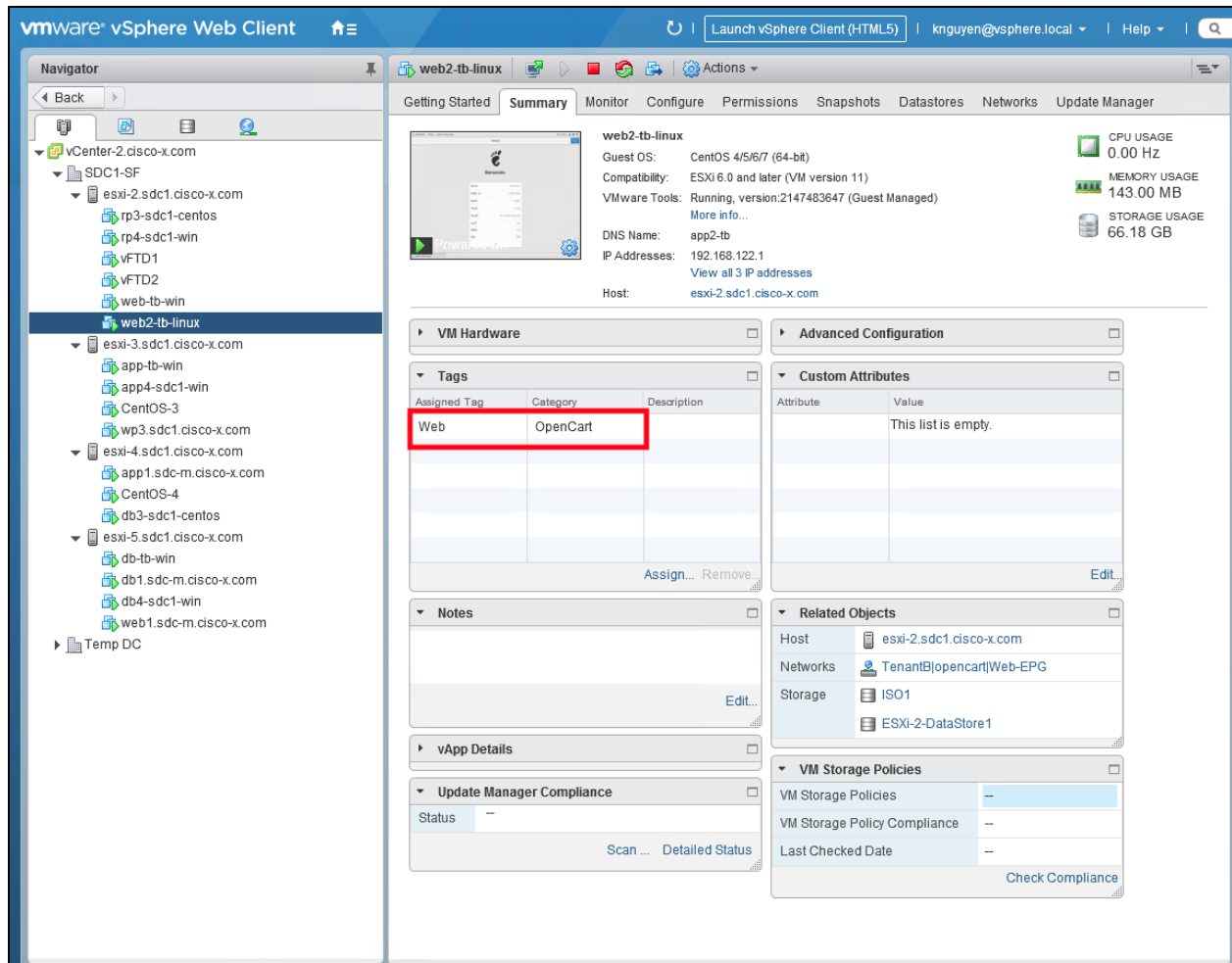


- g. In the Assign Tag dialog box, select the **tag to assign** and then select **Assign**. In this case we assigned the Web tag to the web2-tb-linux host.

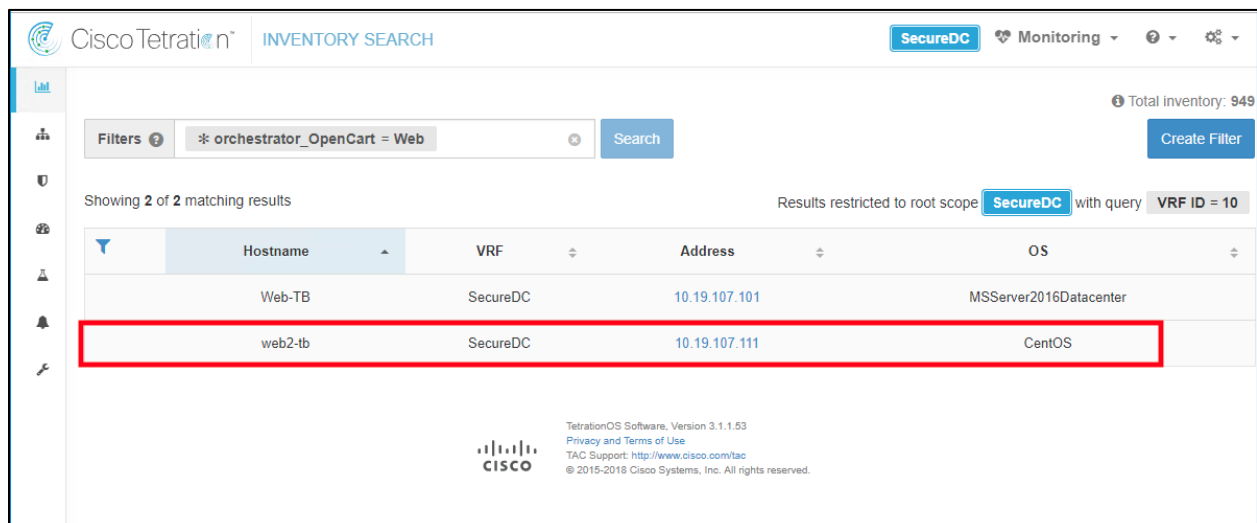


165

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.



166

Step 4

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

The screenshot displays the Cisco Tetration DASHBOARD - FLOWS interface. The top right corner features a user menu for Ken Nguyen, with the 'Scopes' option highlighted by a red box and labeled '2'. A red box labeled '1' highlights the 'Gears icon' in the top right corner. The dashboard includes several charts: 'Top Provider Addresses' (a horizontal bar chart showing IP addresses), 'Top Provider Ports' (a horizontal bar chart showing port numbers), 'Top Provider Hostnames' (a horizontal bar chart showing hostnames), and 'SRTT Distribution' (a horizontal bar chart showing latency ranges). The bottom of the dashboard displays the Cisco logo and version information: 'TetrationOS Software, Version 3.1.1.53', 'Privacy and Terms of Use', 'TAC Support: <http://www.cisco.com/tac>', and '© 2015-2018 Cisco Systems, Inc. All rights reserved.'

167

- 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)**.

The screenshot shows the Cisco Tetration SCOPES interface. The 'Scope Details' dialog box is open, and the 'Create' button is highlighted with a red box and labeled '3'. The 'Commit Scope Updates' button is highlighted with a red box and labeled '4'. The 'Create New Scope' button is highlighted with a red box and labeled '1'. The 'Cancel' button is also visible.

Scope Details

Name: OpenCart

Description: Enter a description (optional)

Policy Priority: Last

Parent Scope: SecureDC

Query: * orchestrator_OpenCart = Web or * orchestrator_OpenCart = App or * orchestrator_OpenCart = DB

Buttons: Create (3), Commit Scope Updates (4), Create New Scope (1), Cancel

- c. View the Scope created called OpenCart.

The screenshot shows the Cisco Tetration SCOPES interface. The 'OpenCart' scope is listed in the table below.

Name	Query	Ability	Total Children	Actions
OpenCart	* orchestrator_OpenCart = Web or * orchestrator_OpenCart = App or * orchestrator_OpenCart = DB	Owner	0	Edit Delete

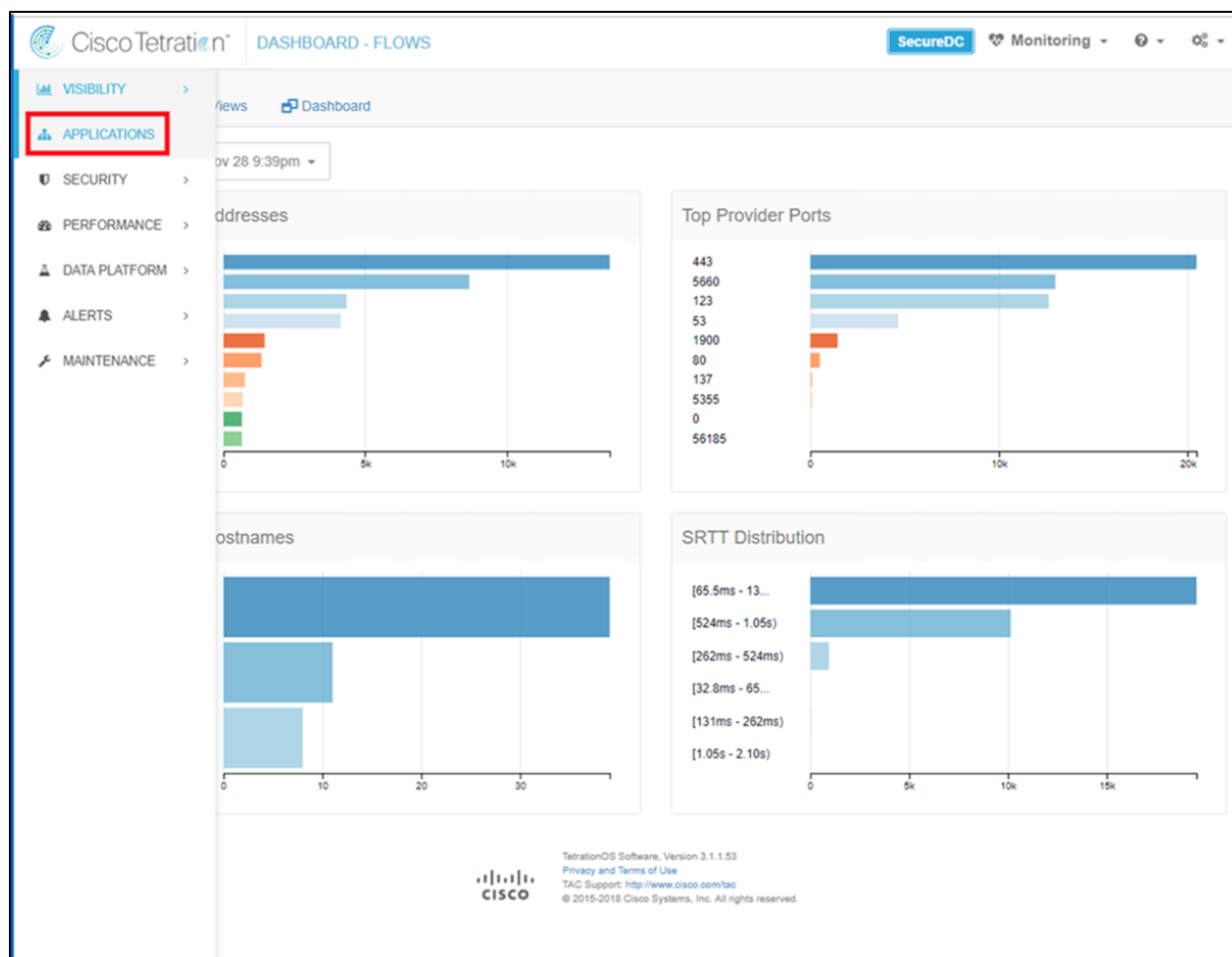
View Deleted Scopes

TetrationOS Software, Version 3.1.1.53
Privacy and Terms of Use
TAC Support: <http://www.cisco.com/tac>
© 2015-2018 Cisco Systems, Inc. All rights reserved.

168

Step 5

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



169

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

1 Create New Application Workspace

2

Name:

Scope:

Description:

☒ Dynamic Mode

Dynamic	Status	Name	Scope	Policy Requests	Updated	Creator	Actions
✓	PRIMARY 🔴 LIVE	SecureDC Rules	SecureDC	2	1:59 PM	Chris McHenry	

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

Create New Application Workspace

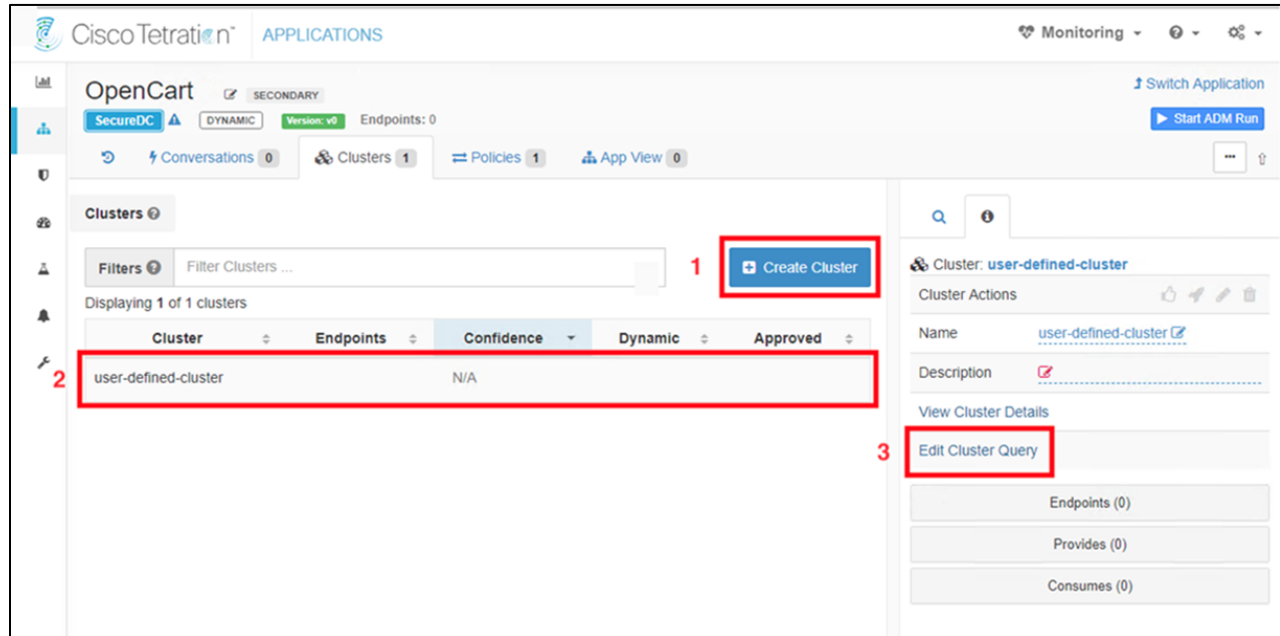
Filters

Dynamic	Status	Name	Scope	Policy Requests	Updated	Creator	Actions
✓	PRIMARY 🔴 LIVE	SecureDC Rules	SecureDC	2	1:59 PM	Chris McHenry	
✓	PRIMARY 🔴 LIVE	OpenCart	SecureDC : OpenCart		11:51 AM	Chris McHenry	

170

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.



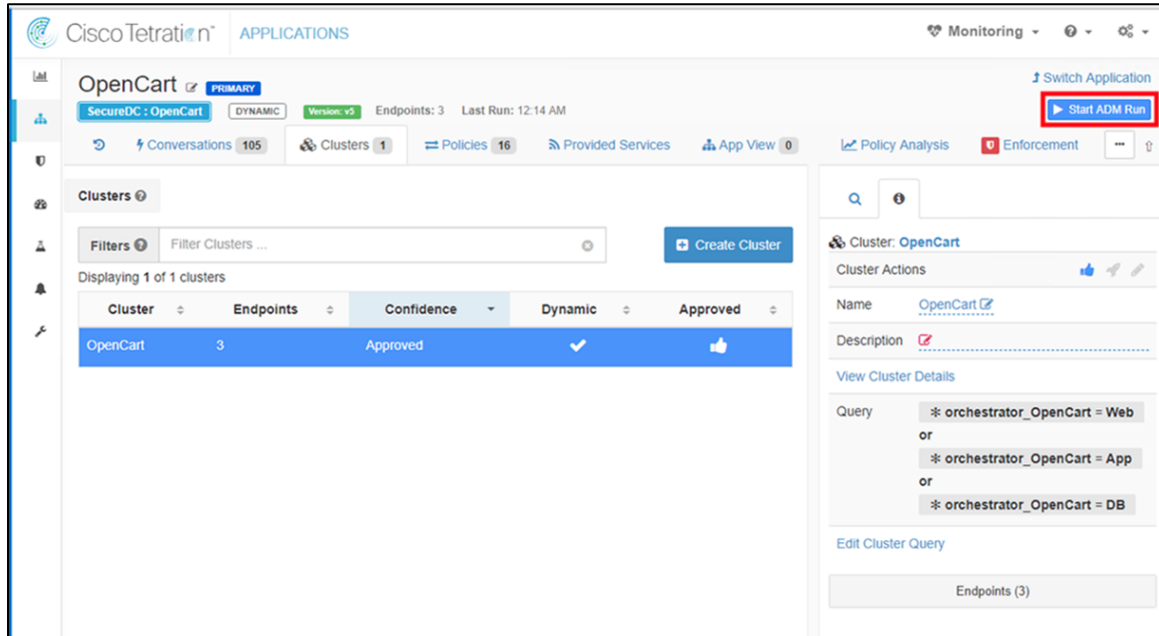
- a. The query dialog box will appear, provide the name and query parameters. **TIP:** Click the ? next to Query for available options. Select **Save** when done. **Note:** The query must specify the VM tag since wildcarding the VM tag for example **orchestrator_opencart=*** is not supported.

The 'Edit Cluster' dialog box is shown. It has three main sections: 'Name', 'Description', and 'Query'. The 'Name' field contains 'OpenCart'. The 'Description' field contains the placeholder text 'Enter a description (optional)'. The 'Query' field contains the query: '* orchestrator_OpenCart = Web or * orchestrator_OpenCart = App or * orchestrator_OpenCart = DB'. At the bottom right, there are 'Save' and 'Cancel' buttons.

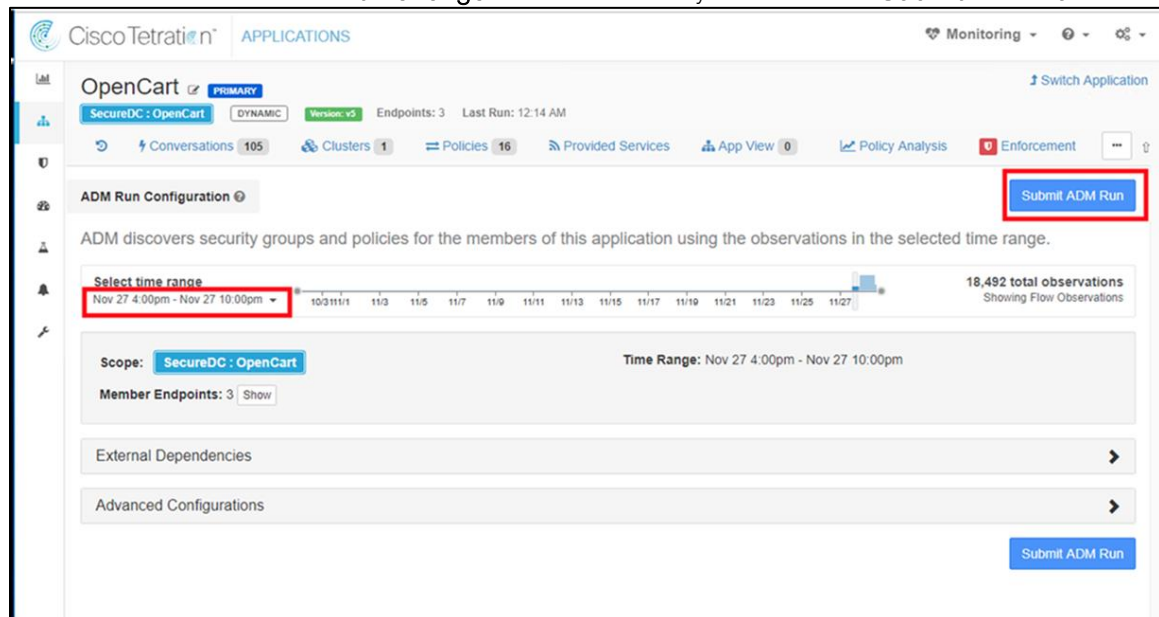
171

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**.



172

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

The screenshot shows the Cisco Tetration Applications page for 'OpenCart'. The 'Policies' tab is selected and highlighted with a red box. The page displays a table of policies with columns: Priority, Action, Consumer, Provider, and Services. The table lists five policies, all with an 'ALLOW' action. The 'Consumer' column shows 'OpenCart' and 'SecureDC', and the 'Provider' column shows 'SecureDC' and 'OpenCart'. The 'Services' column lists various protocols and ports like TCP: 80 (HTTP), UDP: 53 (DNS), TCP: 443 (HTTPS), ICMP, and TCP: 3306 (MySQL).

Priority	Action	Consumer	Provider	Services
100	ALLOW	OpenCart	SecureDC	TCP : 80 (HTTP) ...
100	ALLOW	OpenCart	SecureDC : DNS	UDP : 53 (DNS)
100	ALLOW	OpenCart	SecureDC : Tetration	TCP : 443 (HTTPS) ...
100	ALLOW	SecureDC	OpenCart	ICMP ...
100	ALLOW	OpenCart	OpenCart	TCP : 3306 (MySQL) ...

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**.

The screenshot shows the Cisco Tetration Applications page for 'OpenCart' with the 'Enforcement' tab selected. The 'Enforce Policies' button is highlighted with a red box. The page displays a line graph showing 'Flow Observations' over time, with a peak around 11:35 AM. The graph is filtered for 'Flow Observations' and shows 'Permitted' (blue) and 'Rejected' (grey) data points. The 'Enforced Policy Version' is [p2]. The 'Total Observations' are 18,913. The 'Top Hostnames' section shows 'Consumer Hostnames' and 'Provider Hostnames' with a bar chart.

Consumer Hostnames	Provider Hostnames
Web-TB	Unknown
App-TB	Web-TB
DB-TB	DB-TB
Unknown	

173

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

Enforce Policies

Select the version of policies to enforce.

Version Latest Policies ▼

Reason for action

Describe the new version (p3):

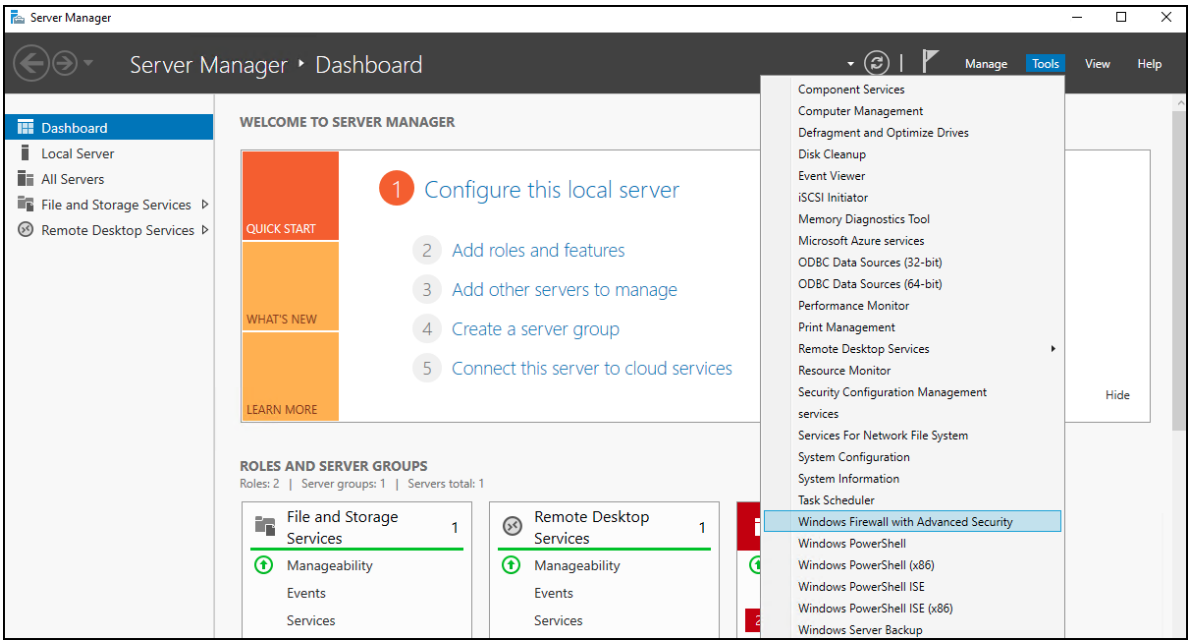
Name

Description

New host firewall rules will be inserted and any existing rules will be deleted on the relevant hosts. Please click accept to continue.

Accept and Enforce **Cancel**

- 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**.



175

- 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	64.100.1.190-64...	TCP	Any	5660	Any
Tetration GoldenRule 3	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	64.100.1.190-64...	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	#000::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 -p 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 --state 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 --state NEW,ESTABLISHED -m comment --comment "PolicyId=5bfef1a9497d4f422fdef82b" -j ACCEPT
```

Test Case 4 – Stealthwatch and Tetration

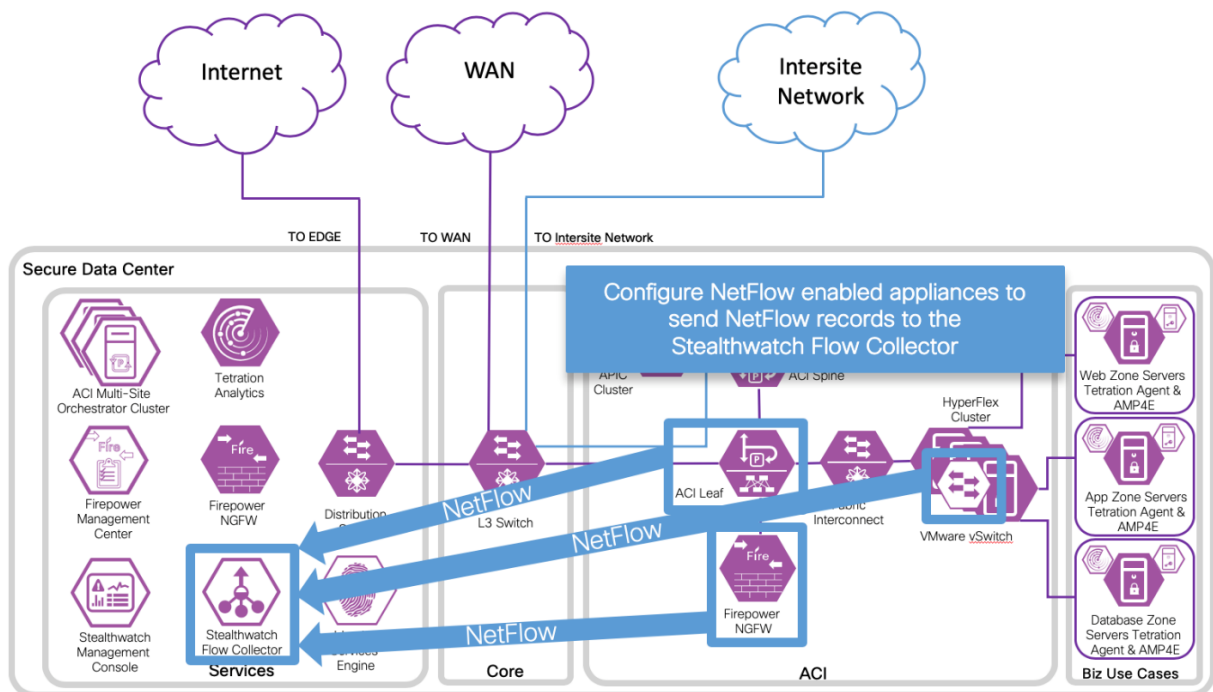
The “pivot” or “cross launch” from Stealthwatch to Tetration was tested and the details of the implementation are provided. This integration also involved enabling the sending of NetFlow records on data center appliances to Stealthwatch Flow Collector. NetFlow was enabled on the VMware vSphere Distributed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

About NetFlow

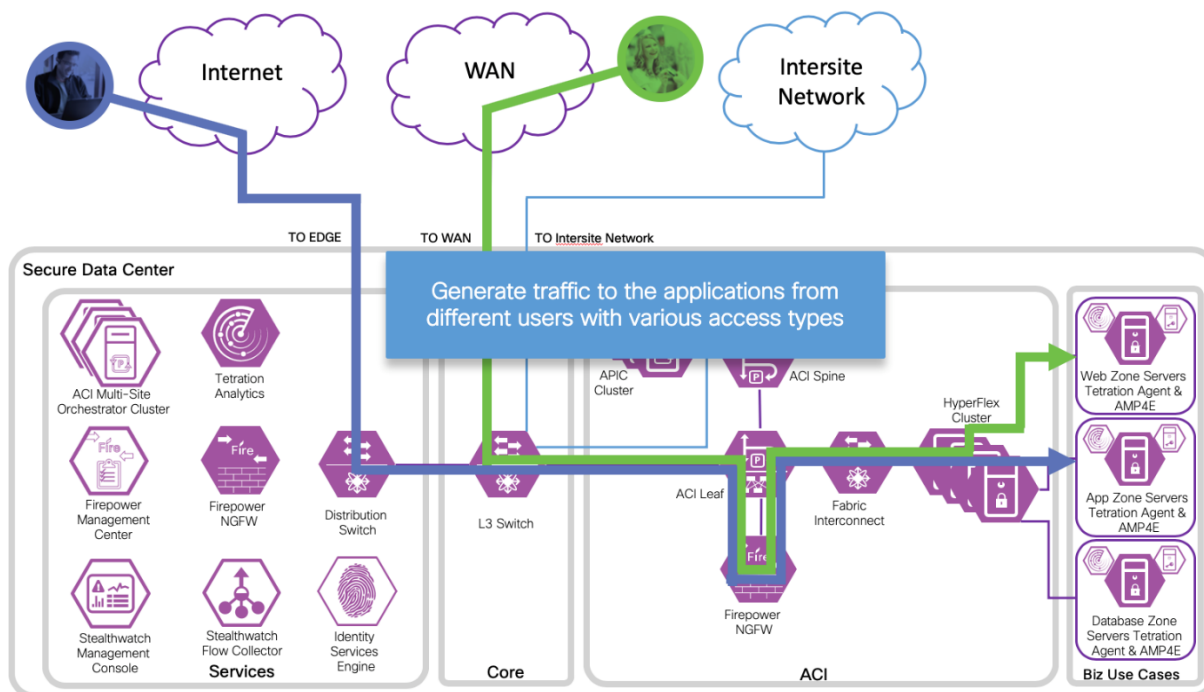
The NetFlow technology provides the metering base for a key set of applications, including network traffic accounting, usage-based network billing, network planning, as well as denial of services monitoring, network monitoring, outbound marketing, and data mining for both service providers and enterprise 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:

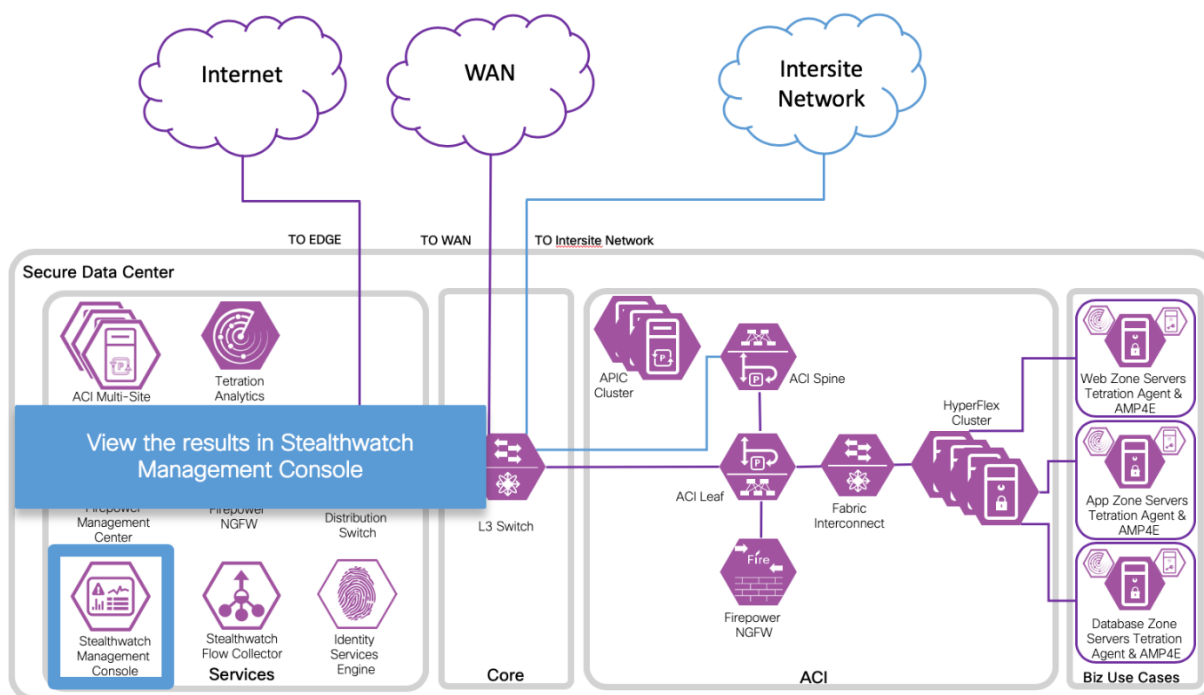
1. On the NetFlow enabled appliances (VMware VDS, Nexus 9300 and Firepower NGFW) enable NetFlow and deliver the NetFlow records to Stealthwatch Flow Collector



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

178

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" );

};

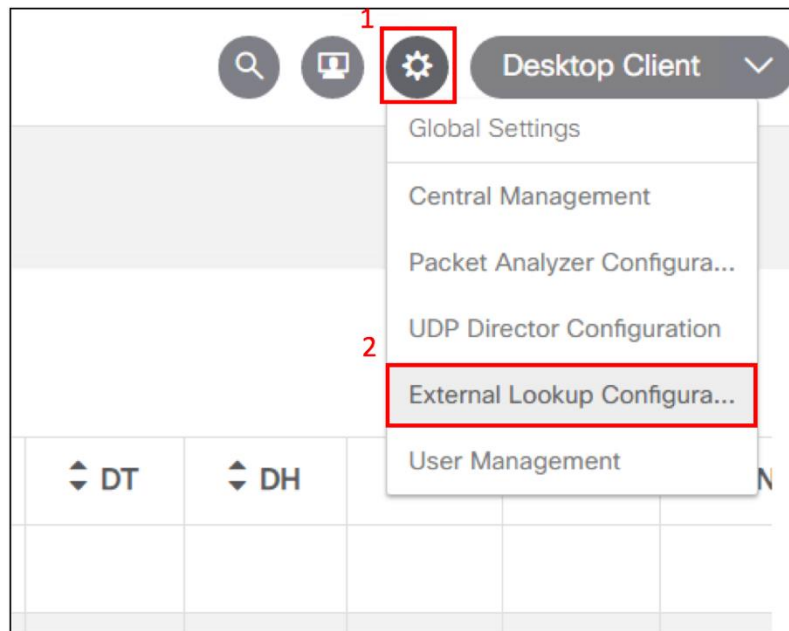
query = baseUrl + query + " ";

return query;
```

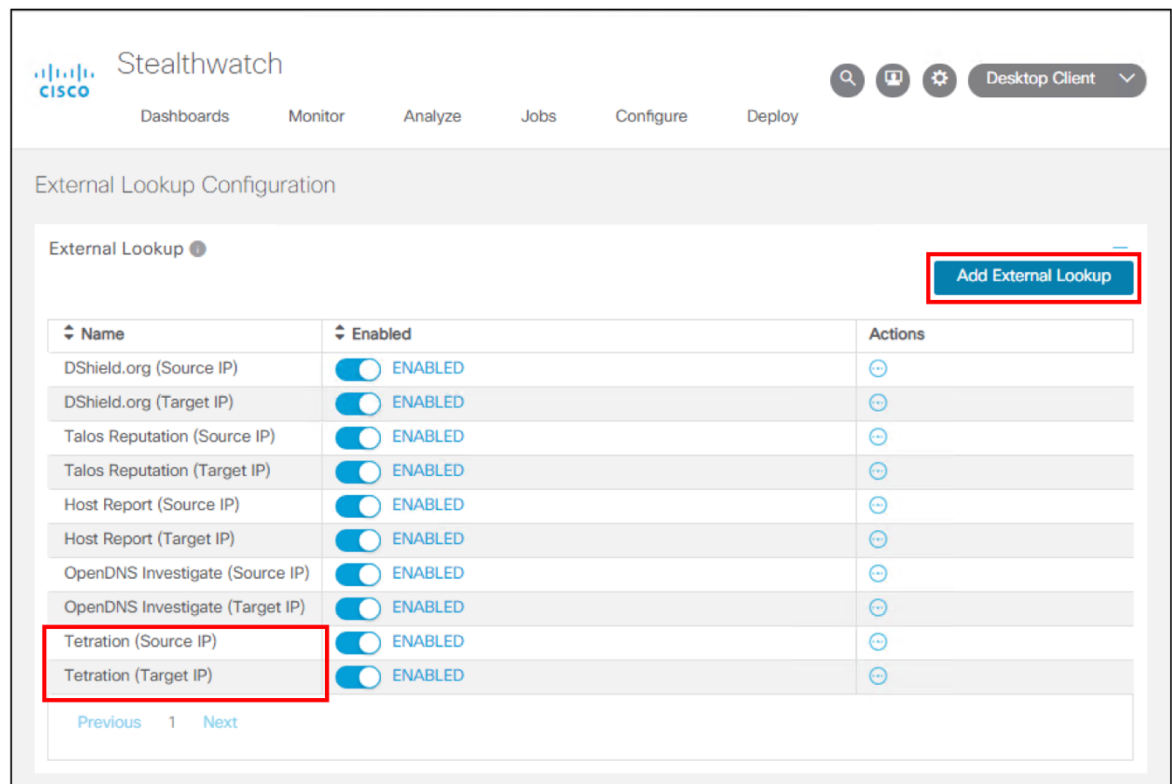
180

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.



181

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**.

Stealthwatch

Dashboards Monitor Analyze Jobs Configure Deploy

External Lookup Configuration

External Lookup ⓘ + Add External Lookup

External Lookup : Tetration (Source IP) ⓘ

NAME: *
Tetration (Source IP) ☒ Enable lookup of internal IP addresses

BASE URL: *
https://[redacted]/#/host/profile/10/

QUERY PARAMETER MAPPING:

PARAMETER NAME: / STEALTHWATCH ATTRIBUTE NAME: Source IP Address ☐ Required +

URL SCRIPT BUILDER FILE UPLOAD: ⓘ
Tetration (Source IP).config

182

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**.

Stealthwatch

Dashboards Monitor Analyze Jobs Configure Deploy

External Lookup Configuration

External Lookup ⓘ + Add External Lookup

External Lookup : Tetration (Target IP) ⓘ

NAME: *
Tetration (Target IP) ☒ Enable lookup of internal IP addresses

BASE URL: *
https://[redacted]/#/host/profile/10/

QUERY PARAMETER MAPPING:

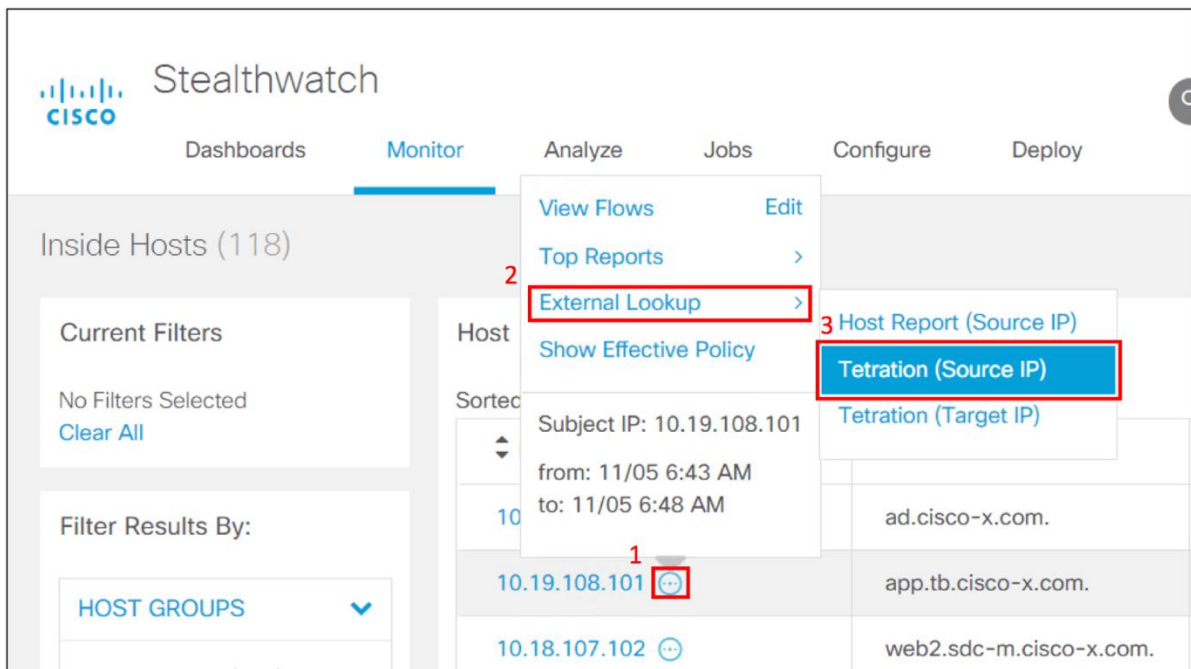
PARAMETER NAME: / STEALTHWATCH ATTRIBUTE NAME: Target IP Address ☐ Required +

URL SCRIPT BUILDER FILE UPLOAD: ⓘ
Tetration (Target IP).config

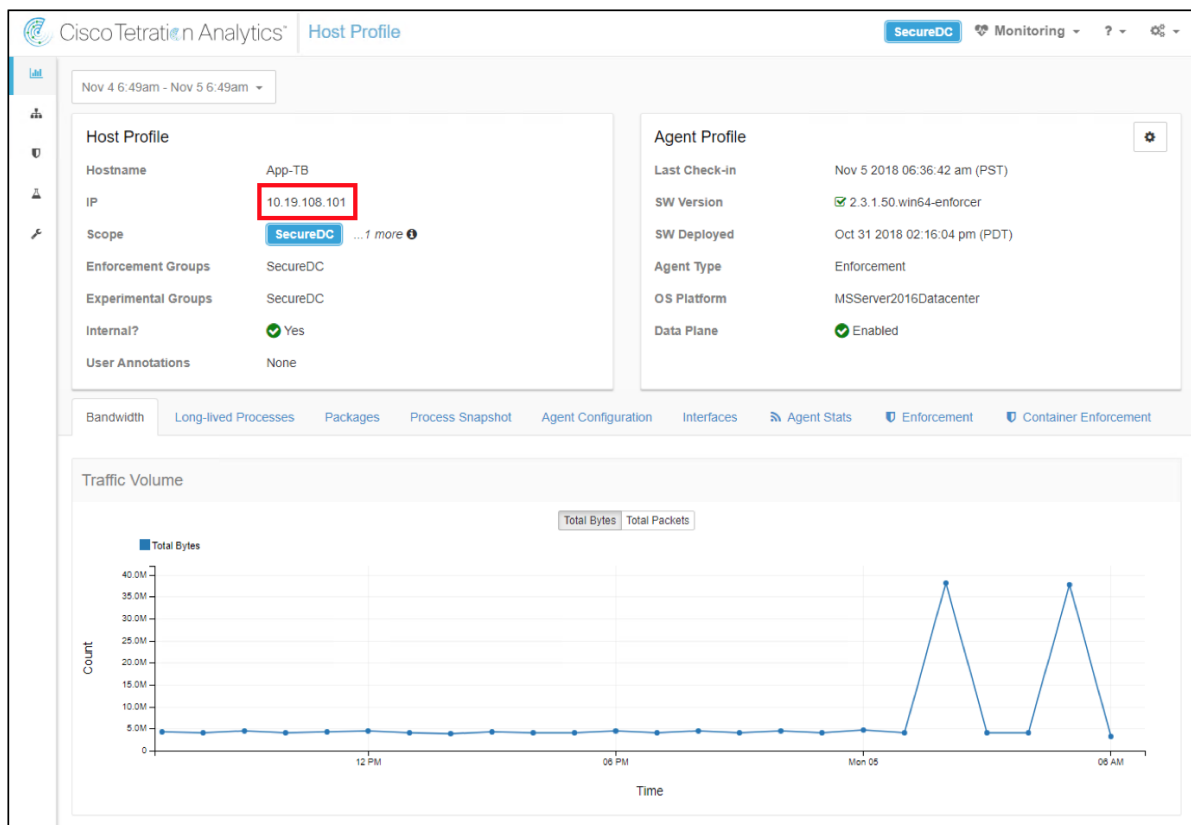
183

Step 5

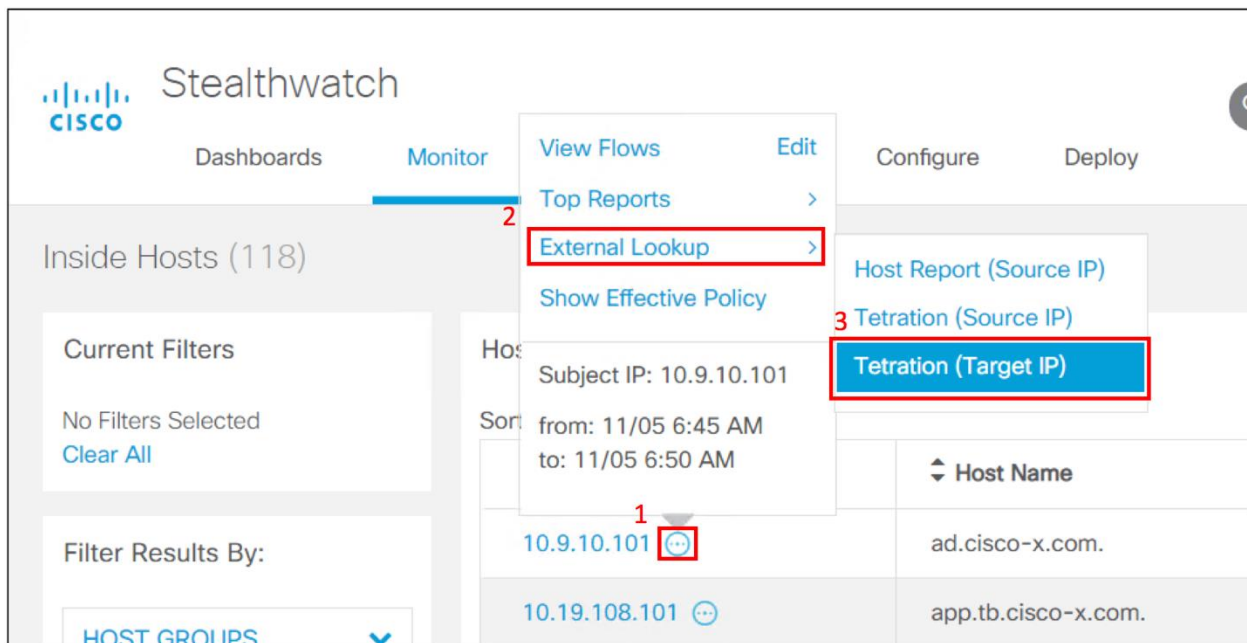
- a. Use Tetration (Source IP) External Lookup. Select the **sphere** next to the Source IP address that you want to investigate further in Tetration (1)->External Lookup(2)->Tetration (Source IP)(3).



- 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.



- 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:

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

F
A
V

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

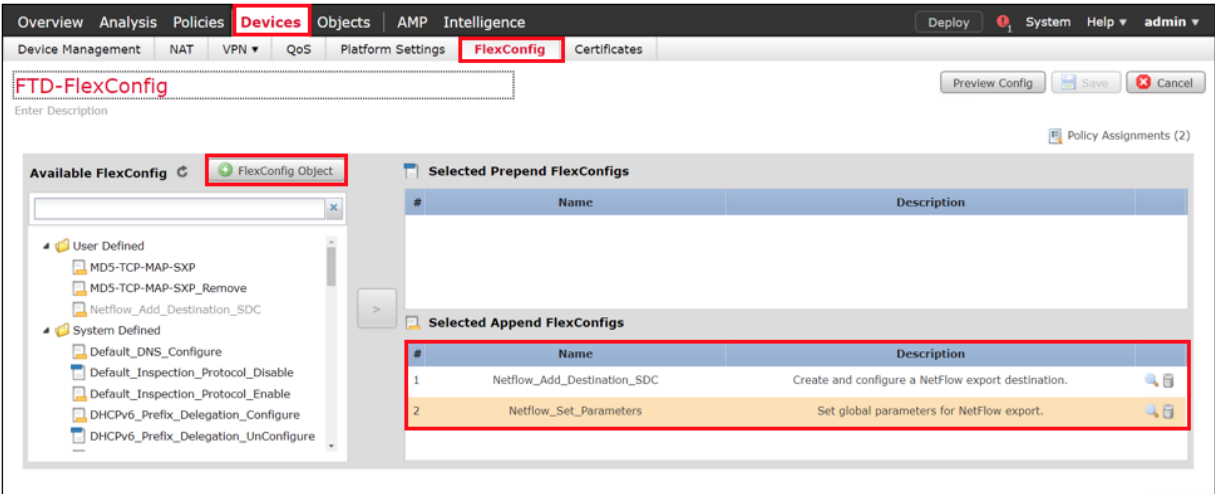
Firepower Threat Defense and NetFlow

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.

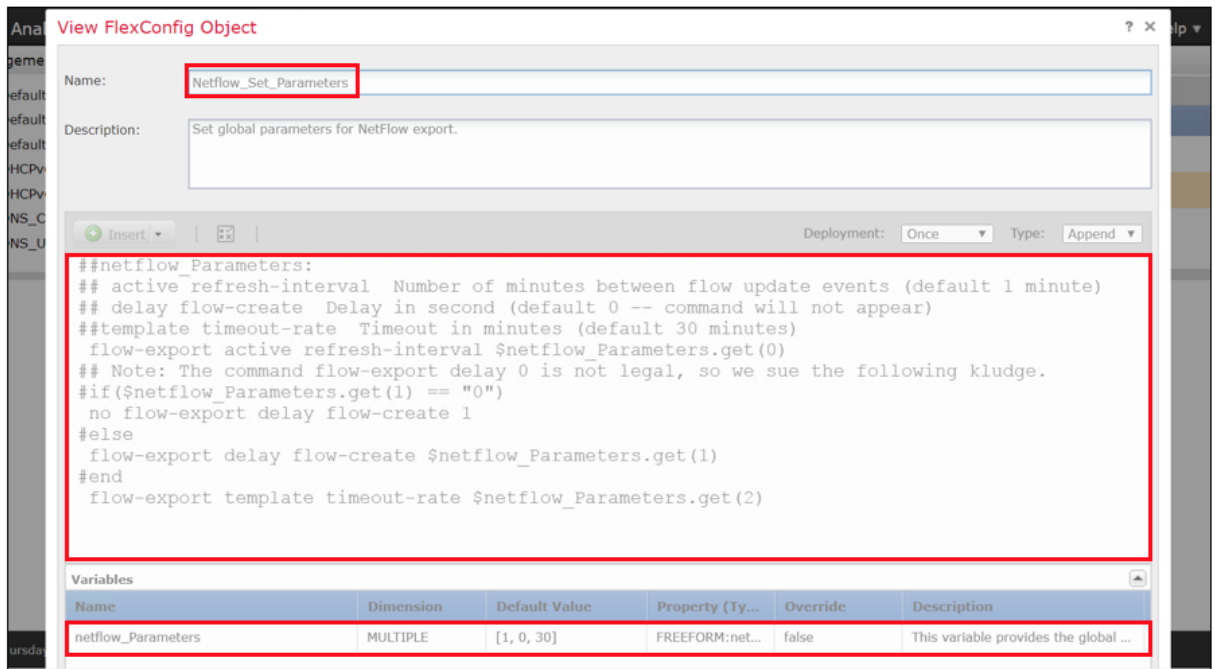
Configuring NetFlow Secure Event Logging (NSEL) on Cisco Firepower Threat Defense
<https://community.Cisco.com/t5/security-documents/configuring-nsel-netflow-on-Cisco-firepower-threat-defense-ftd/ta-p/3646300>

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

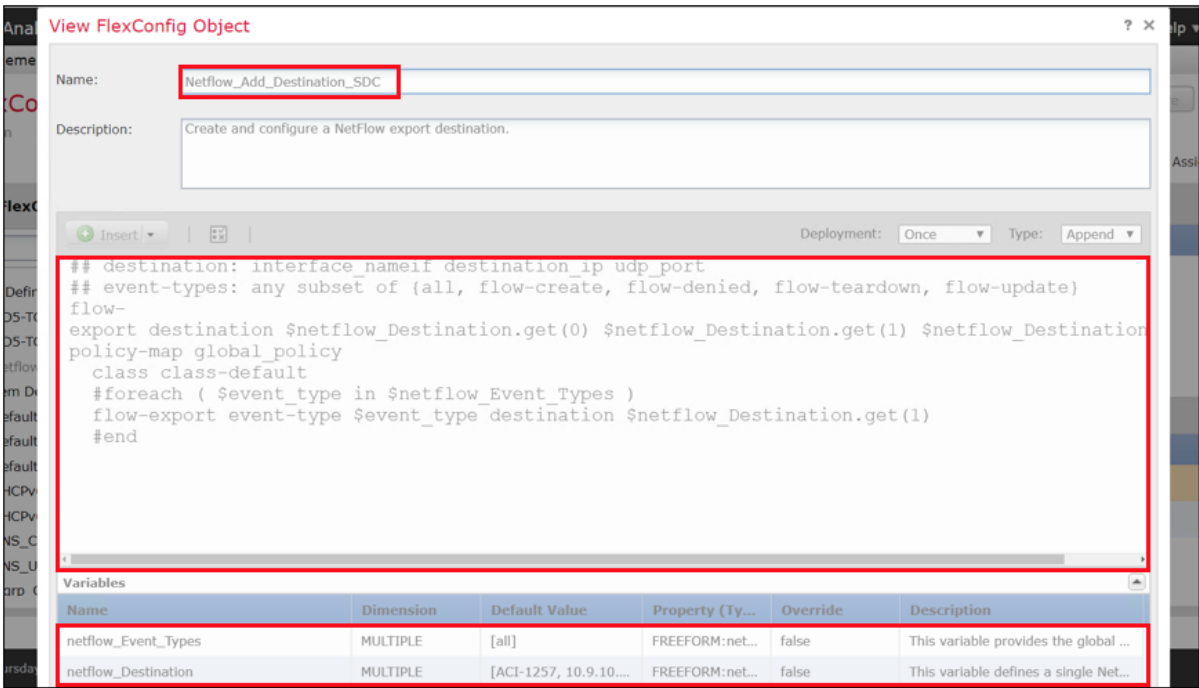
- Step 1
- a. Create **two FlexConfig Objects** that will be used to enable NetFlow on Firepower Threat Defense, **Netflow_Add_Destination_SDC** and **Netflow_Set_Parameters**. To create a FlexConfig Object in Firepower Management Center, navigate to **Devices-> FlexConfig** and select **plus sign** to create FlexConfig Object.



- b. Create FlexConfig Object **Netflow_Set_Parameters** FlexConfig.



c. Create FlexConfig Object `Netflow_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_API_C_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

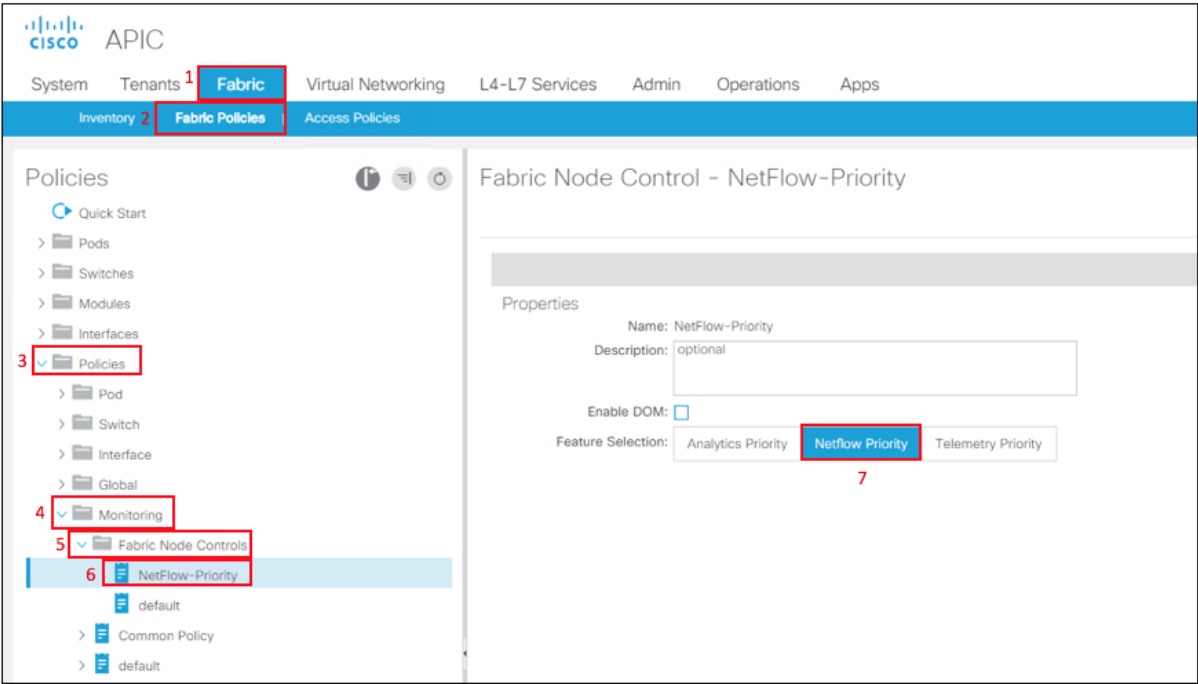
In the Work pane, select Right-Click > Create Fabric Node Control
- Step 4

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.



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.

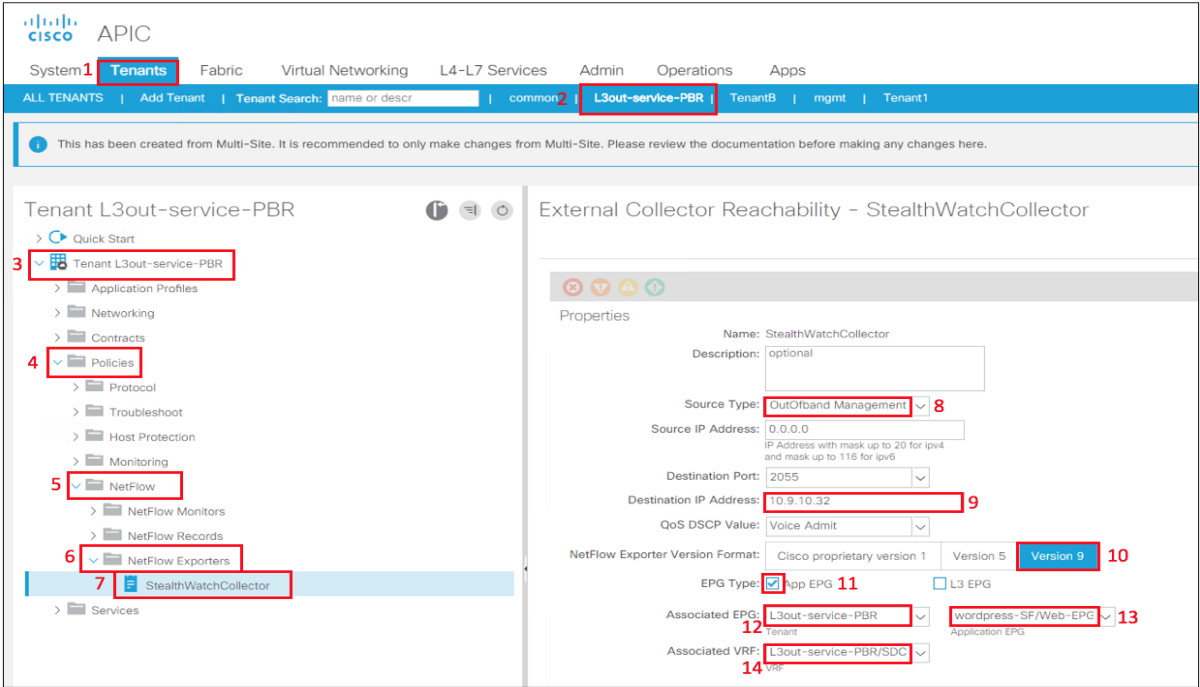
Procedure

- 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).



Step 3

Configuring a Tenant NetFlow Record Policy

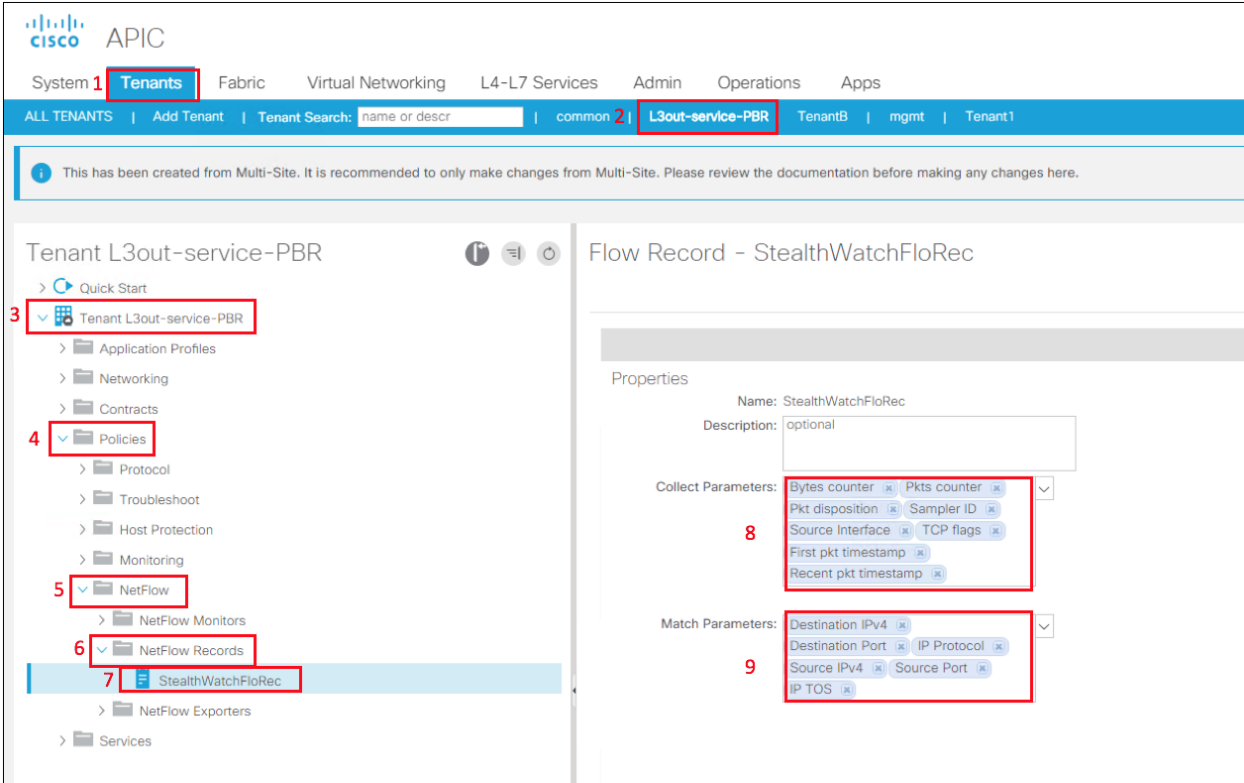
About NetFlow Record Policies

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 <i>Tenant_Name</i> > Policies > NetFlow. |
| Step 4 | Right-Click NetFlow Records and select Create Flow Record . |
| Step 5 | <p>In the Create NetFlow Record dialog box, fill in the fields as required, except as specified below:</p> <p>For the Collect Parameters drop-down list, you can select multiple parameters.</p> <p>For the Match Parameters drop-down list, you can select multiple parameters.</p> <p>If you select multiple parameters, your choices must be one of the following combinations or a subset of one of the combinations:</p> <p>Source IPv4, Destination IPv4, Source Port, Destination Port, IP Protocol, VLAN, IP TOS</p> <p>Source IPv6, Destination IPv6, Source Port, Destination Port, IP Protocol, VLAN, IP TOS</p> <p>Ethertype, Source MAC, Destination MAC, VLAN</p> <p>Source IP, Destination IP, Source Port, Destination Port, IP Protocol, VLAN, IP TOS, where Source IP/Destination IP qualifies both IPv4 and IPv6.</p> |

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

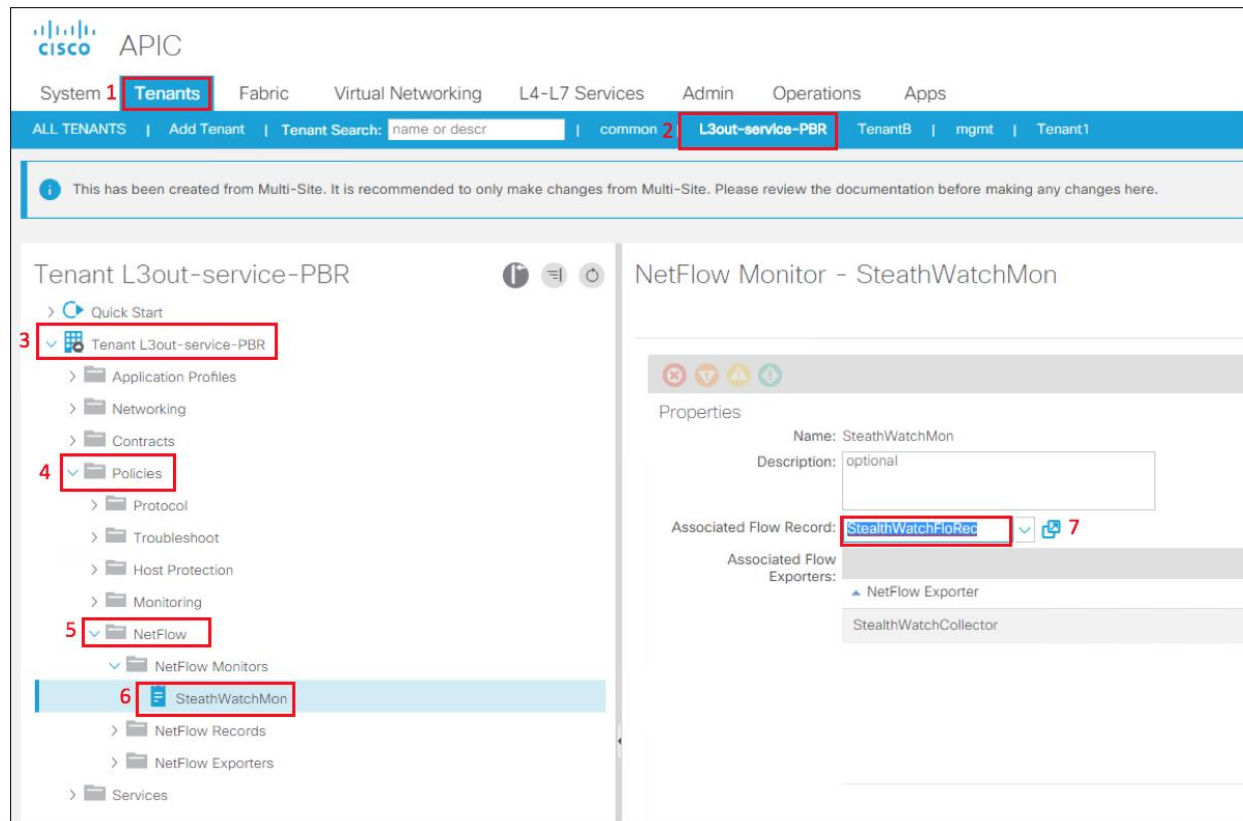
The following procedure configures a tenant NetFlow monitor policy using the advanced GUI mode.

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 **SteathWatchMon** that we tested. It is associated to the flow record called **SteathWatchFloRec(7)**.



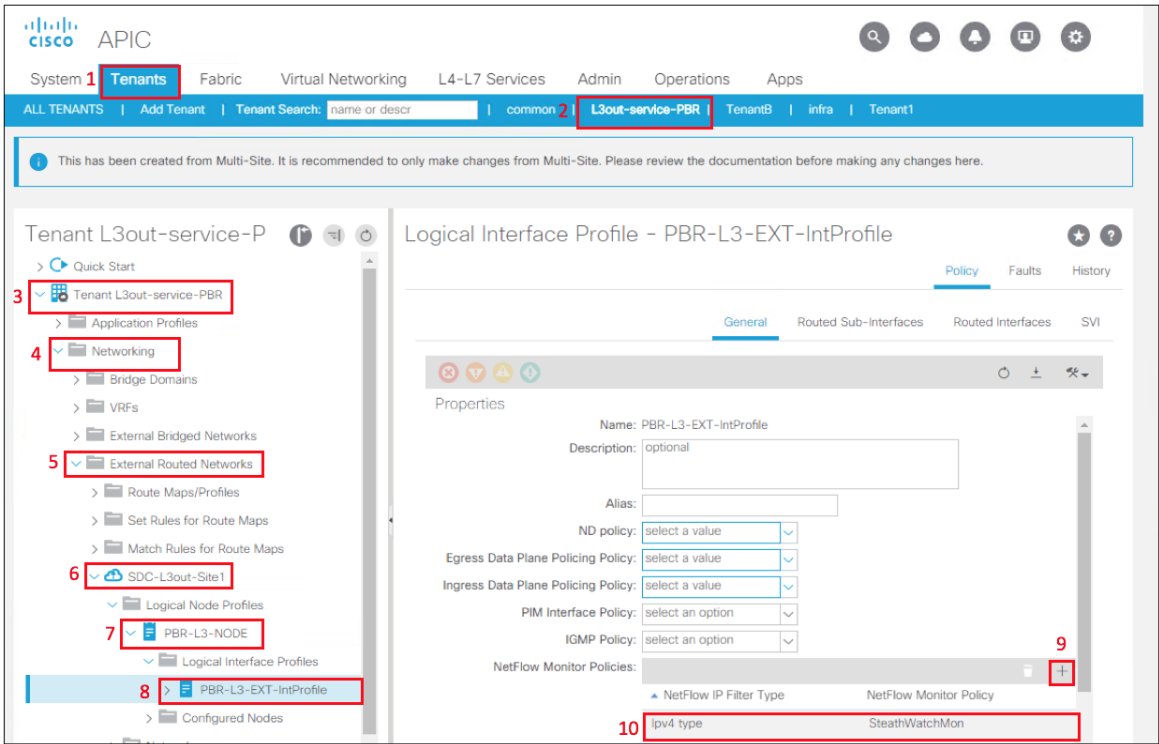
Step 5

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)**.



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

D

D

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/3-2/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

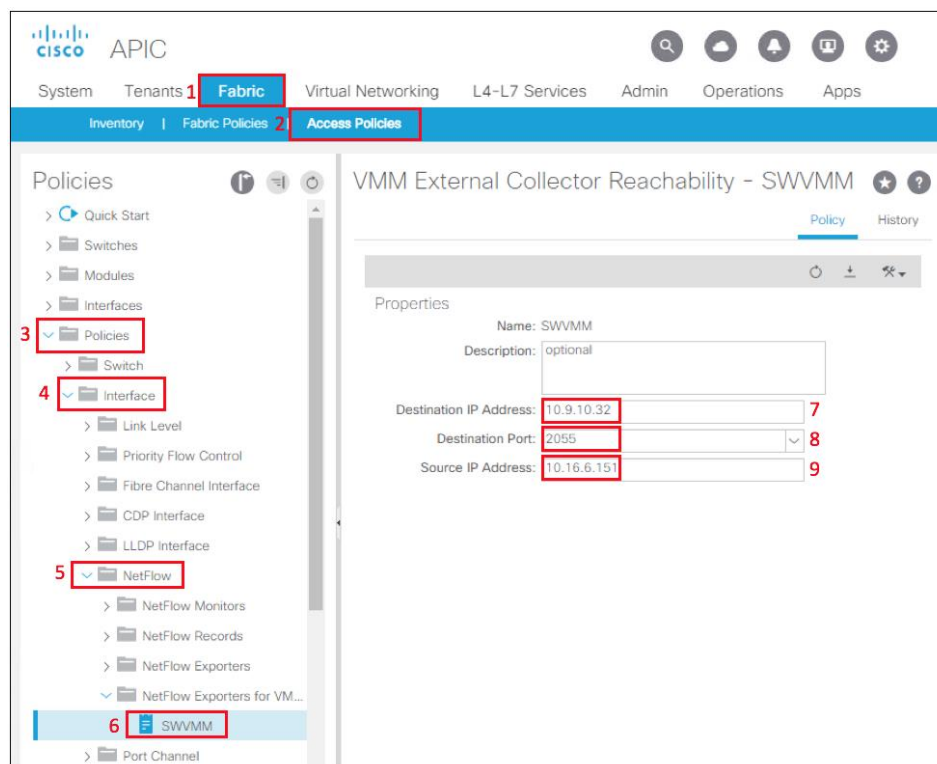
Configuring a NetFlow Exporter Policy for VM Networking Using GUI

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

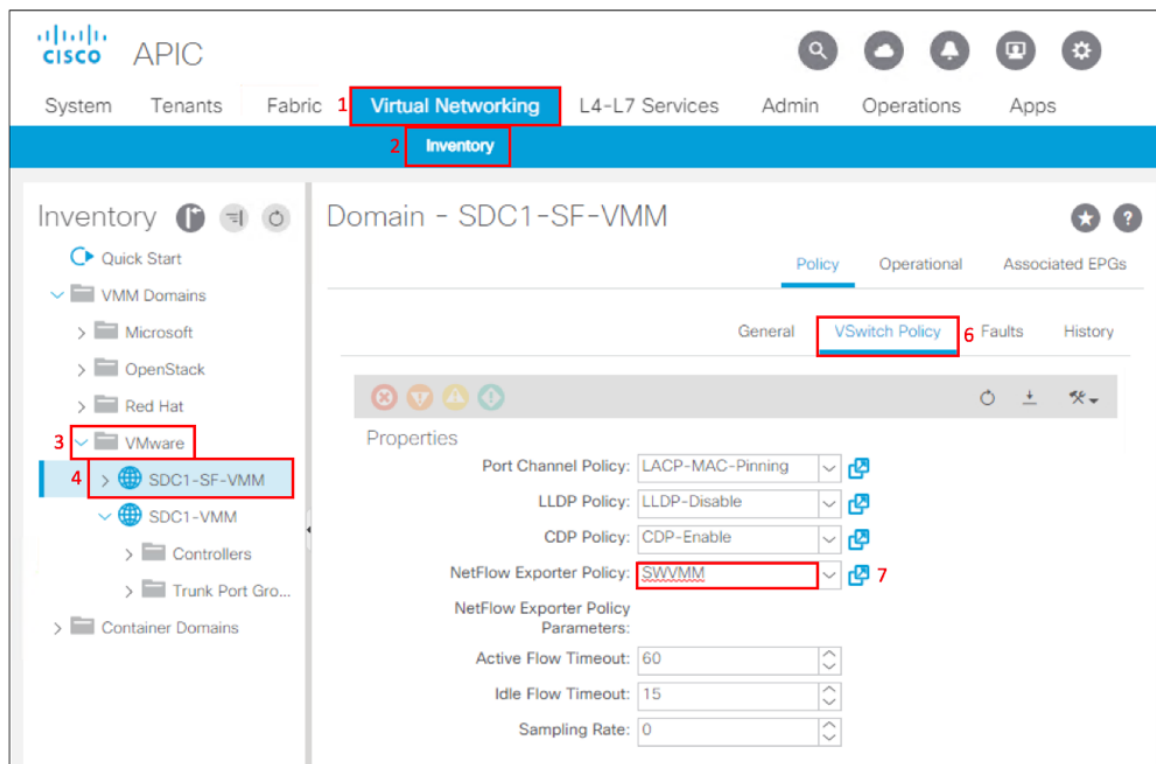
- Step 1 On the menu bar, select **Virtual Networking > Inventory**.
- Step 2 In the Navigation pane, expand the **VMM Domains** folder, Right-Click **VMware**, and select **Create vCenter Domain**.
- Step 3 In the **Create vCenter Domain** dialog box, fill in the fields as required, except as specified:
- In the **NetFlow Exporter Policy** drop-down list, select the desired exporter policy or create a new one.
 - 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.

- 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 SWMM(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.

Add VMM Domain Association

VMM Domain Profile: SDC1-VMM

Deploy Immediacy: Immediate On Demand

Resolution Immediacy: Immediate On Demand Pre-provision

Delimiter:

Enhanced Lag Policy: select an option

Allow Micro-Segmentation: ☒

VLAN Mode: Dynamic Static

Primary VLAN for Micro-Seg: vlan-122
For example, vlan-1

Secondary VLAN for Micro-Seg: vlan-132
For example, vlan-1

Port Binding: Dynamic Binding Ephemeral Default Static Binding

Netflow: Disable Enable

Allow Promiscuous: Reject

Forged Transmits: Reject

MAC Changes: Reject

Cancel Submit

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-3CF9AEFB-08B0-47F5-A3B6-ADD8A919DFA0.html#GUID-3CF9AEFB-08B0-47F5-A3B6-ADD8A919DFA0>

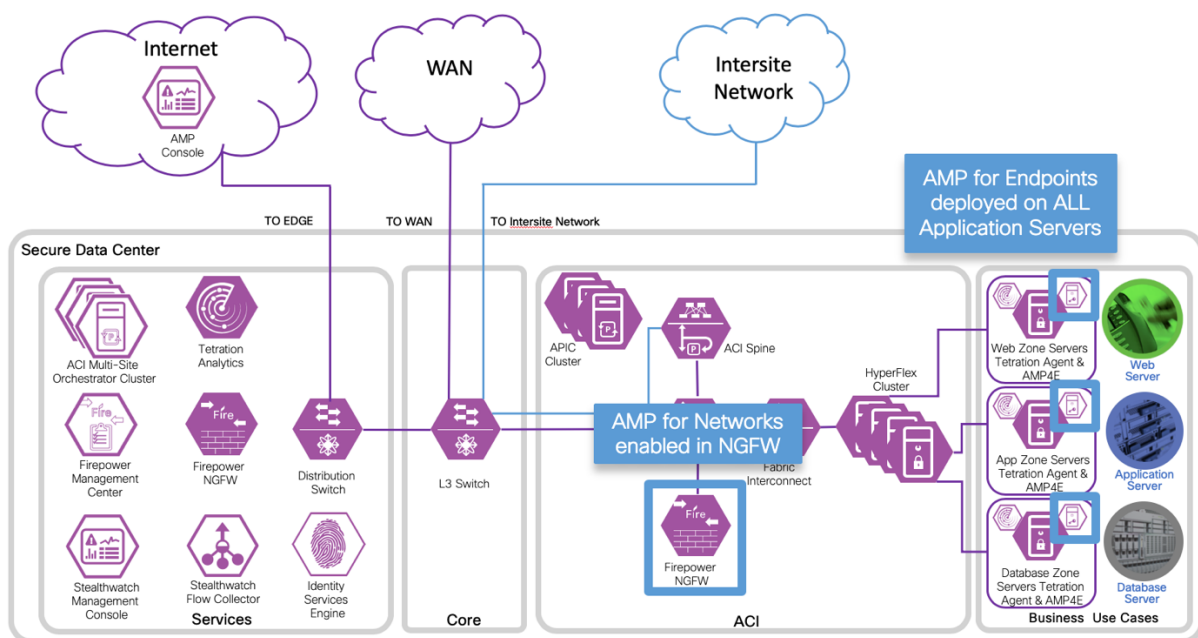
Test Case 5 – AMP and Firepower Threat Defense

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.

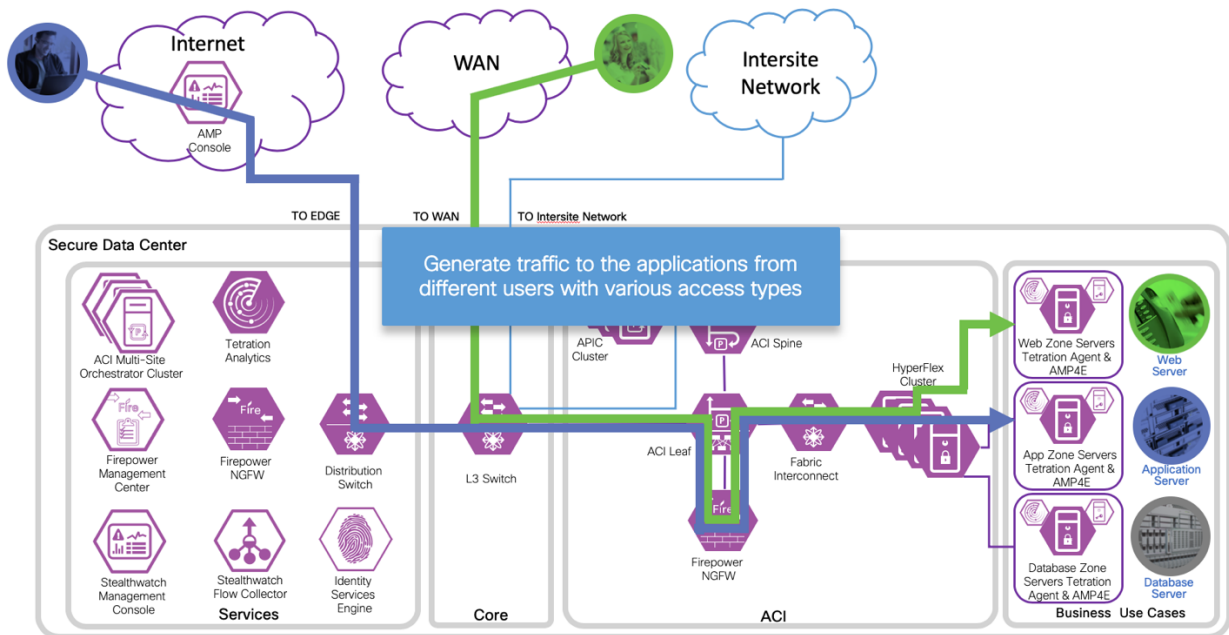
We tested with AMP Public Cloud, so we viewed the results in the AMP4E portal.

Test Description:

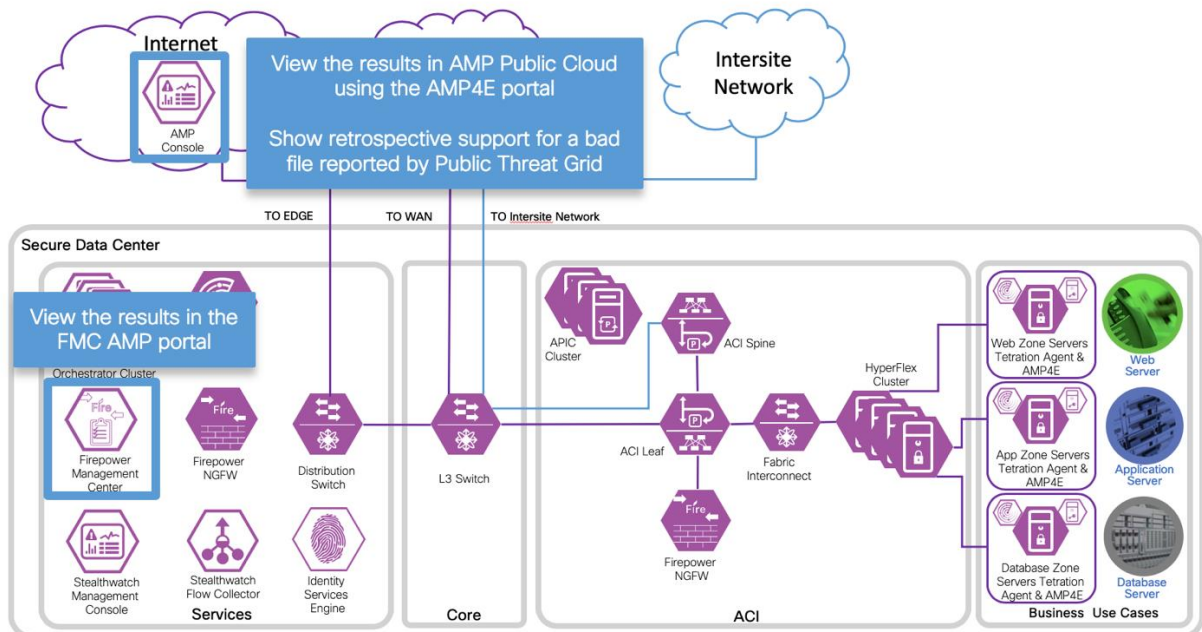
1. AMP4E will be deployed on all the application servers, and AMP4N will be enabled in NGFW.



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.



200

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.

InternetFilePolicy
File policy to and from Internet

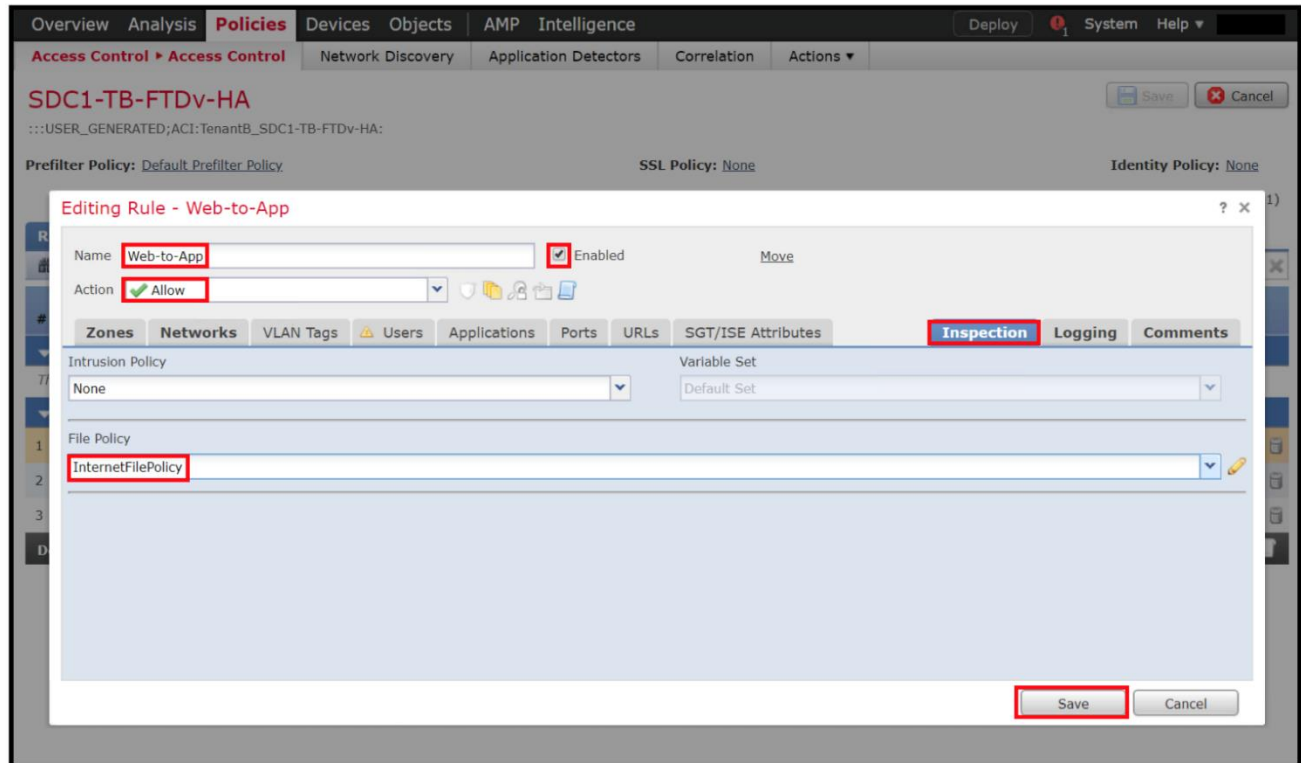
Rules Advanced

No access control policies use this Malware & File policy **Add Rule**

File Types	Application Protocol	Direction	Action
Category: Local Malware Analysis Capable Category: Dynamic Analysis Capable Category: System files Category: Graphics (6 more...)	Any	Download	Block Malware with Reset Spero Analysis Dynamic Analysis
Category: PDF files Category: Office Documents	Any	Upload	Block Files with Reset
Category: Local Malware Analysis Capable Category: Dynamic Analysis Capable Category: System files Category: Graphics (6 more...)	Any	Any	Detect Files

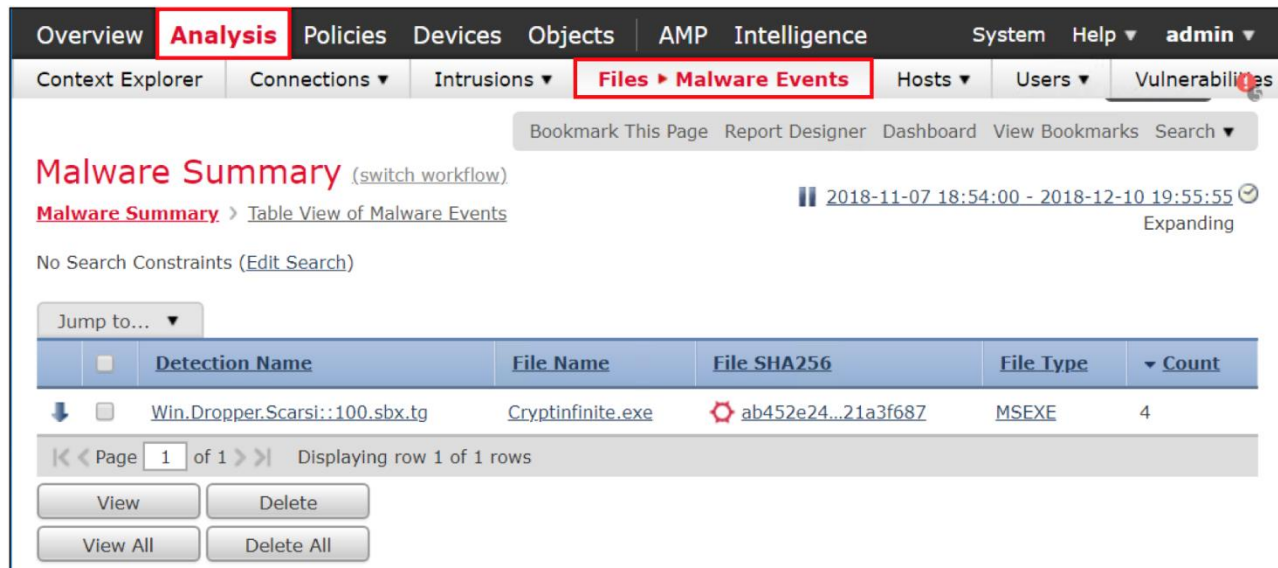
201

- 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 and 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**.



202

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

The screenshot shows the 'File Summary' page under the 'Analysis' tab. The 'Files > File Events' sub-tab is selected. The page displays a table with one row of data for 'Executables' (MSEXE) categorized as 'Malware', with an action of 'Malware Block' and a count of 4. The table is titled 'File Summary' and includes a 'Table View of File Events' link. A date range filter is set to '2018-11-07 18:54:00 - 2018-12-10 19:57:42'. The page also features a 'Jump to...' dropdown and pagination controls showing 'Page 1 of 1'.

Category	Type	Disposition	Action	Count
Executables	MSEXE	Malware	Malware Block	4

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

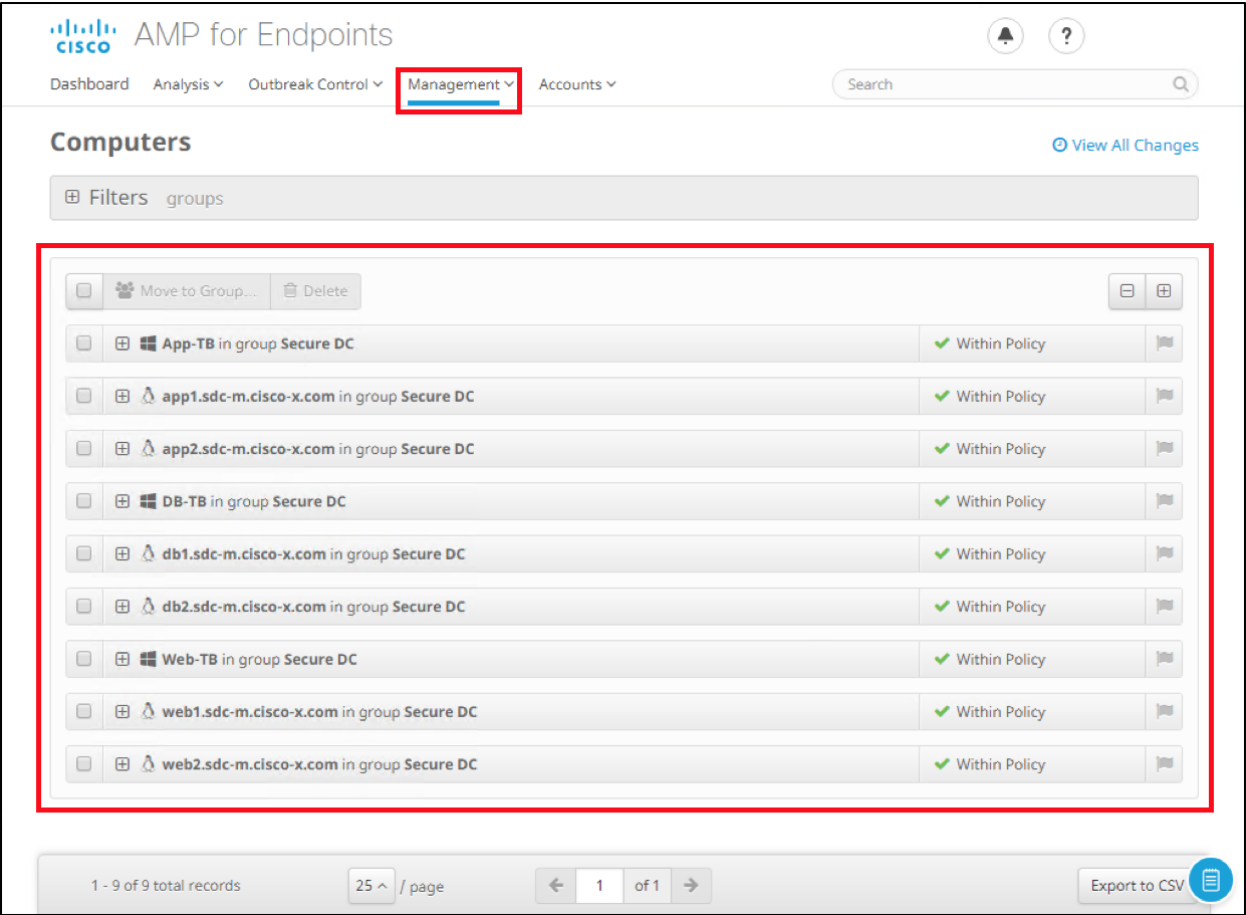
The screenshot shows the 'Network File Trajectory' page under the 'Analysis' tab. The 'Files > Network File Trajectory' sub-tab is selected. The page displays two tables: 'Recently Viewed Files' and 'Recent Malware'. Both tables show a single entry for 'Cryptinfinite.exe' (MSEXE) categorized as 'Malware', with a count of 4 events. The 'Recently Viewed Files' table includes a search bar for 'Enter a SHA256 hash, IP address or file name'. The 'Recent Malware' table also shows the same entry.

Time	File SHA256	File Names	File Type	Disposition	Events
2018-11-08 15:21:15	ab452e24...21a3f687	Cryptinfinite.exe	MSEXE	Malware	4

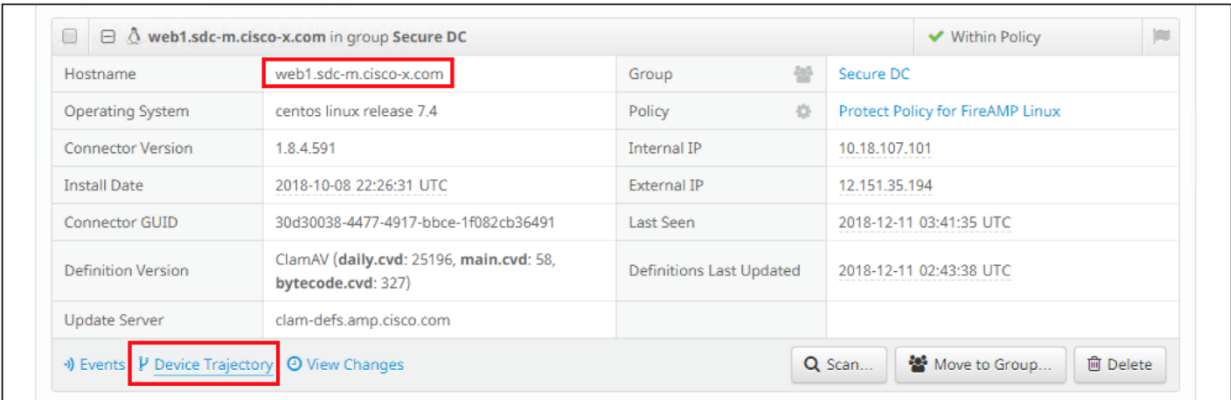
Time	File SHA256	File Names	File Type	Disposition	Events
2018-11-08 15:21:15	ab452e24...21a3f687	Cryptinfinite.exe	MSEXE	Malware	4

203

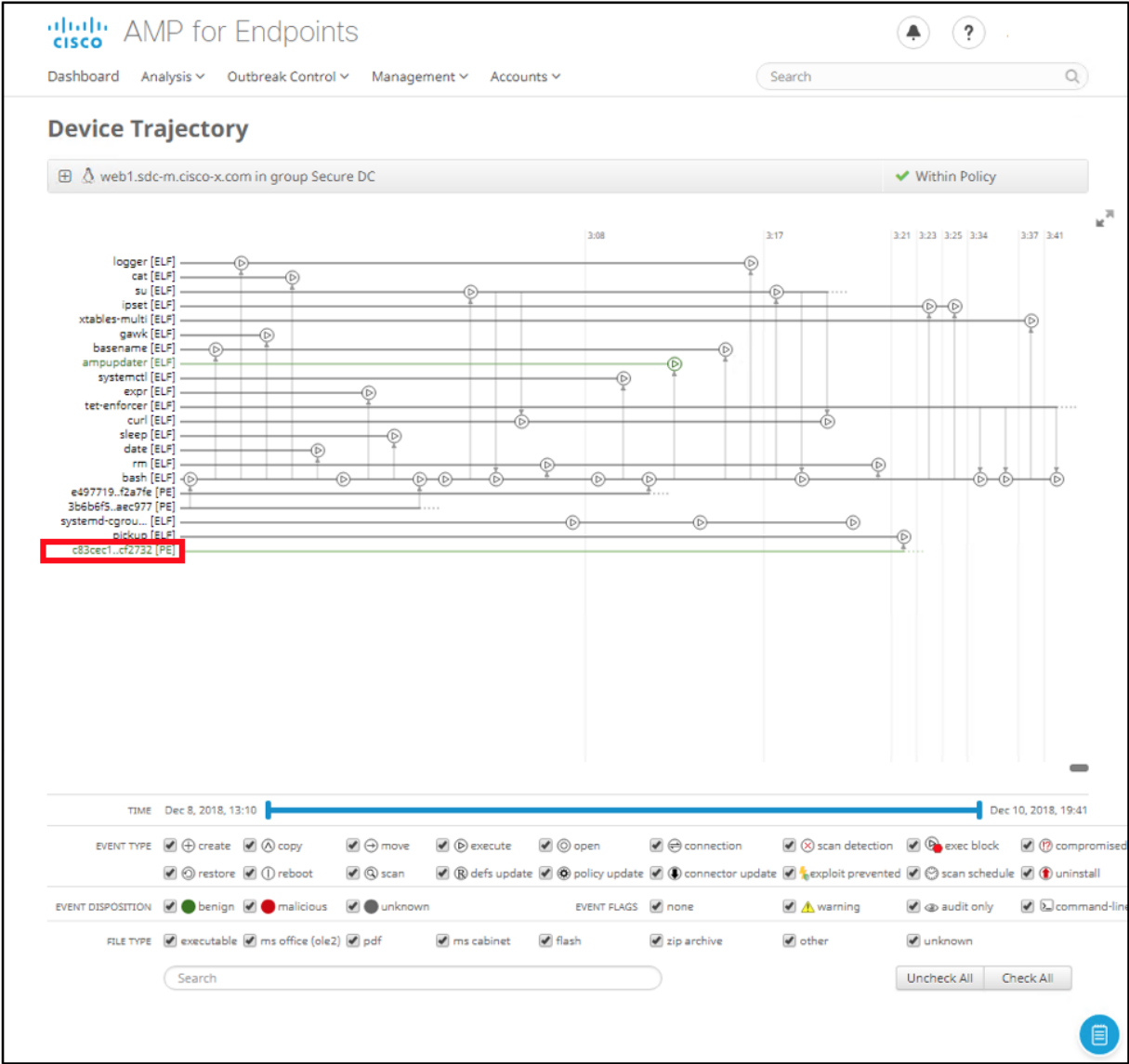
d. View AMP for Endpoint portal. View all the hosts in the **Secure DC** group.



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.

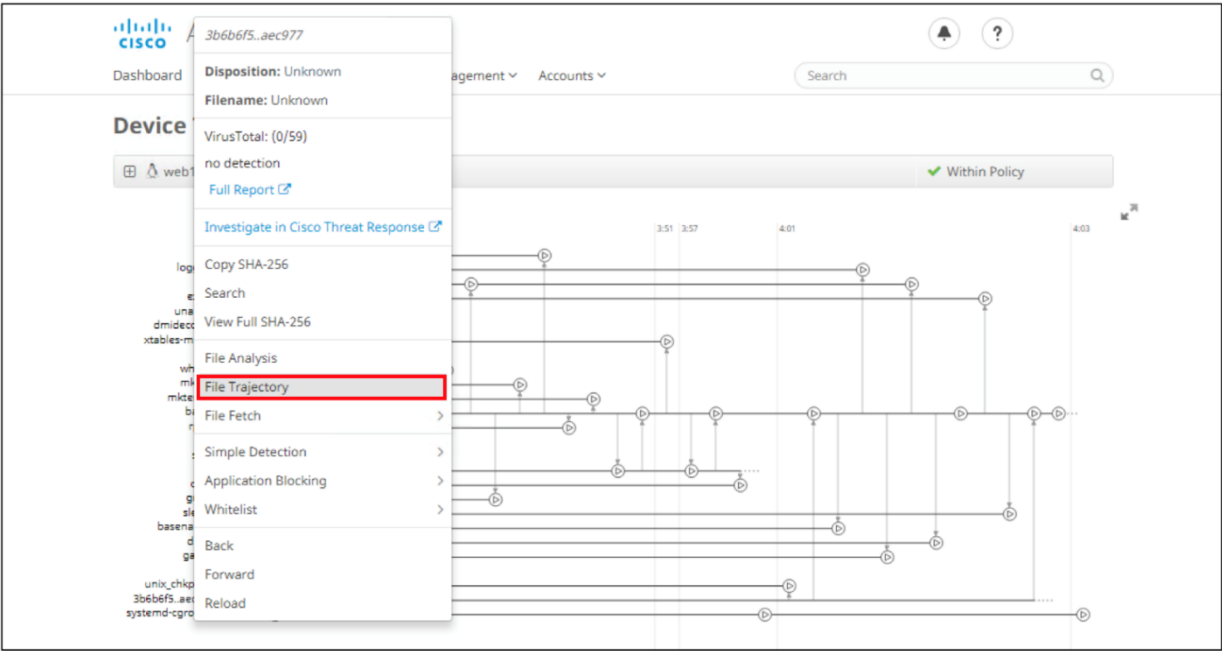


f. View Device Trajectory. To view File Trajectory, select a **file** to investigate.

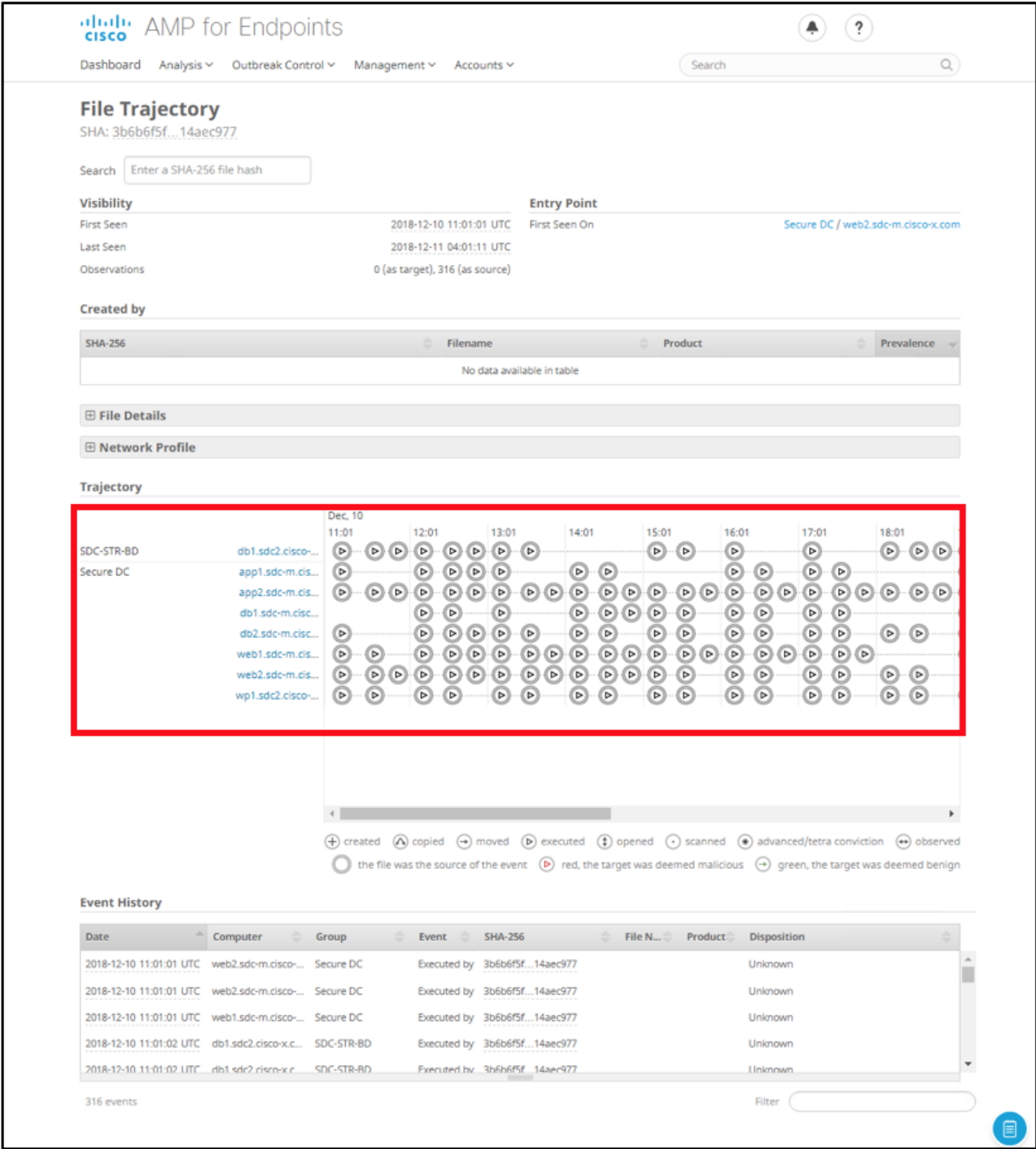


205

g. Select **File Trajectory**.



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

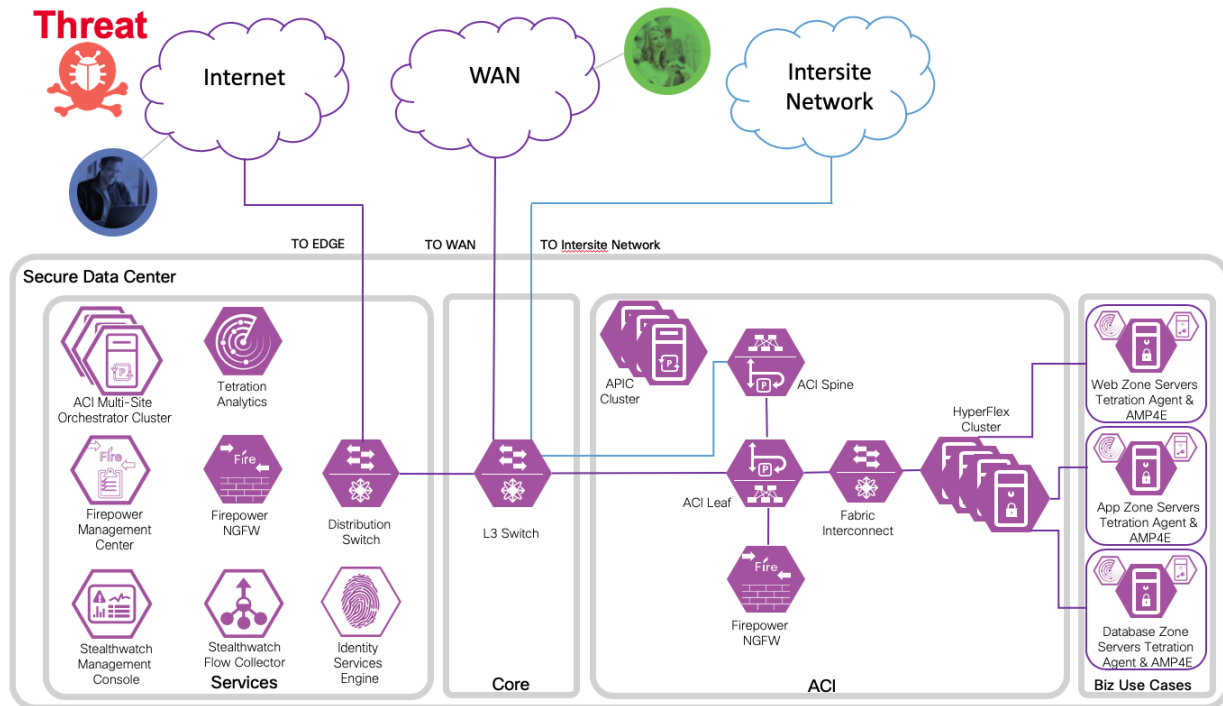


Test Case 6 – FTD Rapid Threat Containment and APIC

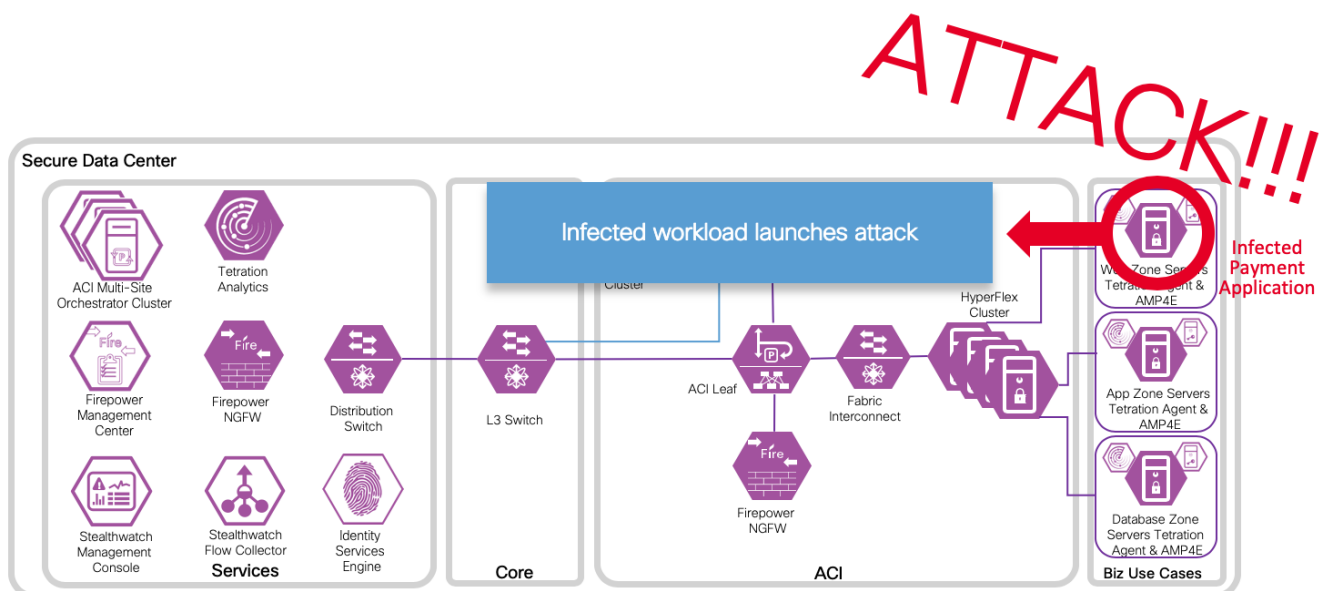
This integration involves identifying an attacker in FMC based on AMP4E, AMP4N, NGIPS and extract the IP address of the attacker. FMC will use this information in the APIC Remediation module to push out policy to quarantine this host.

Test Description:

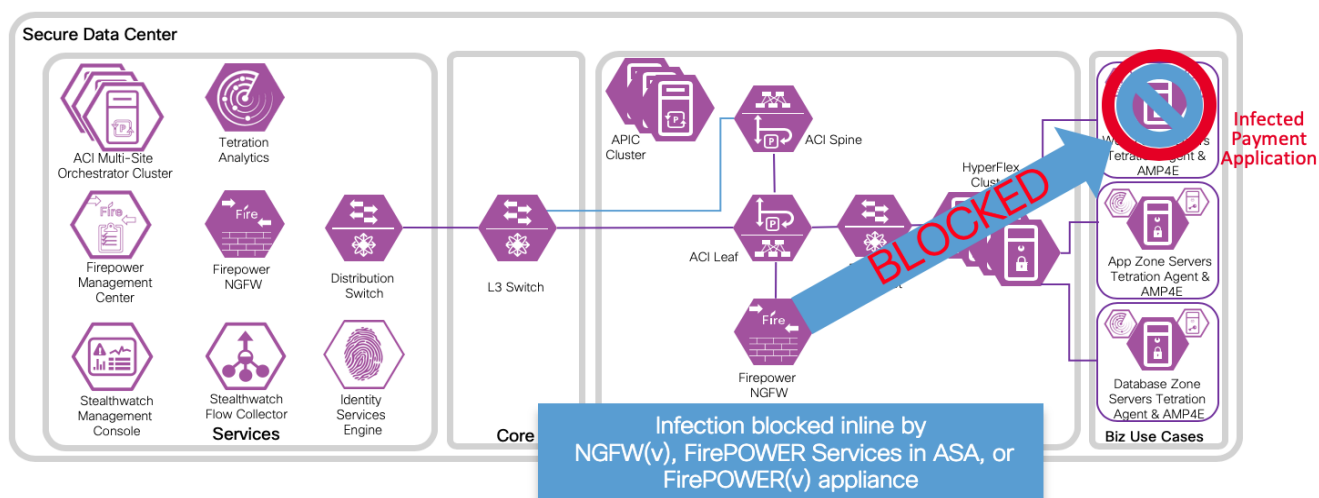
1. Threat is coming from Internet, on FMC, setup the APIC/Firepower Remediation Module.



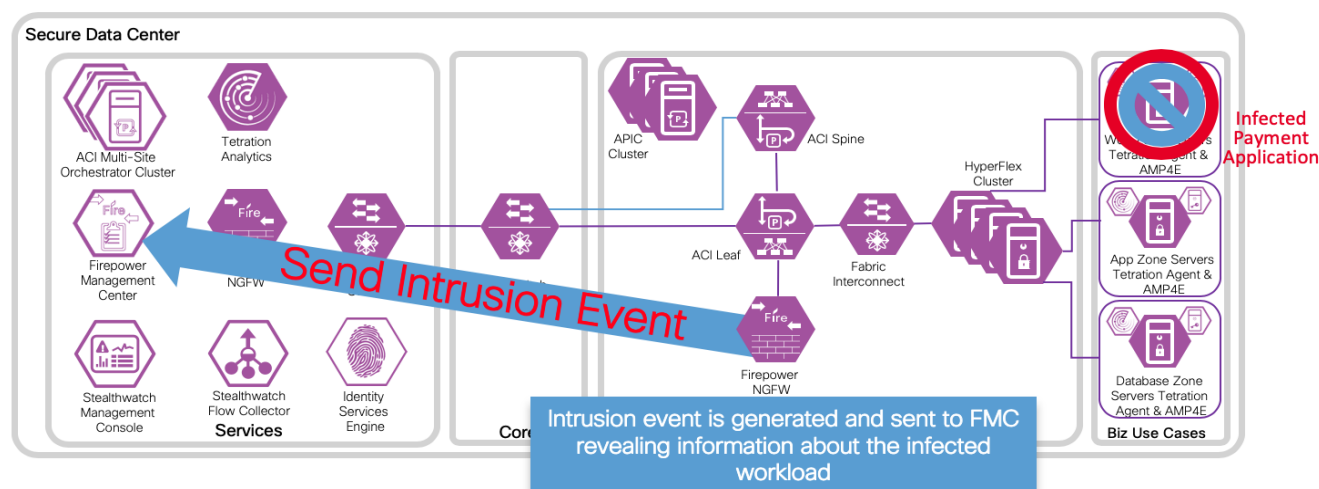
2. An endpoint with an infected application in an EPG launches an attack.



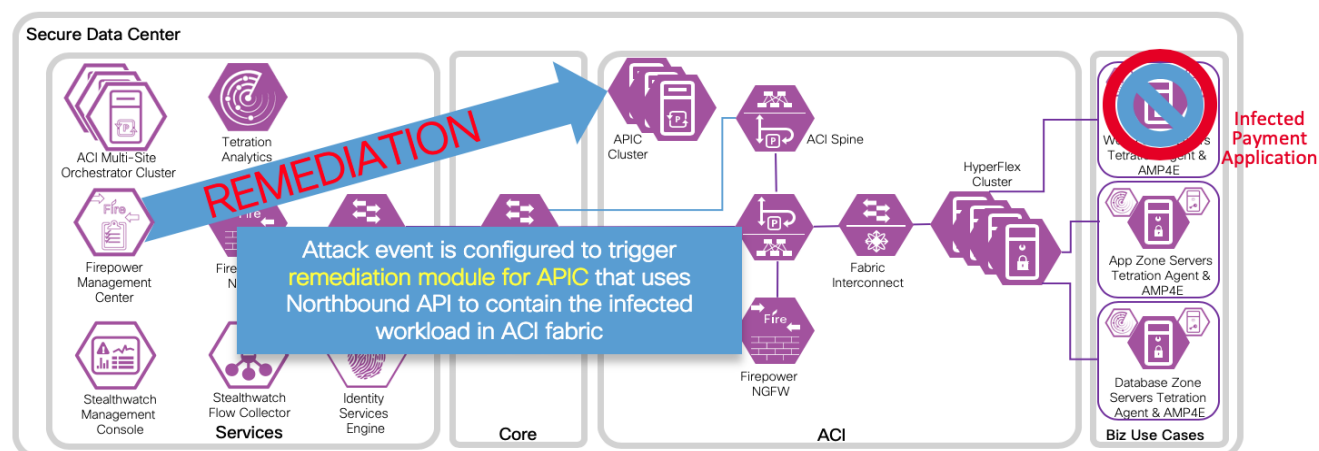
3. The attack is blocked inline by Cisco Firepower Threat Defense.



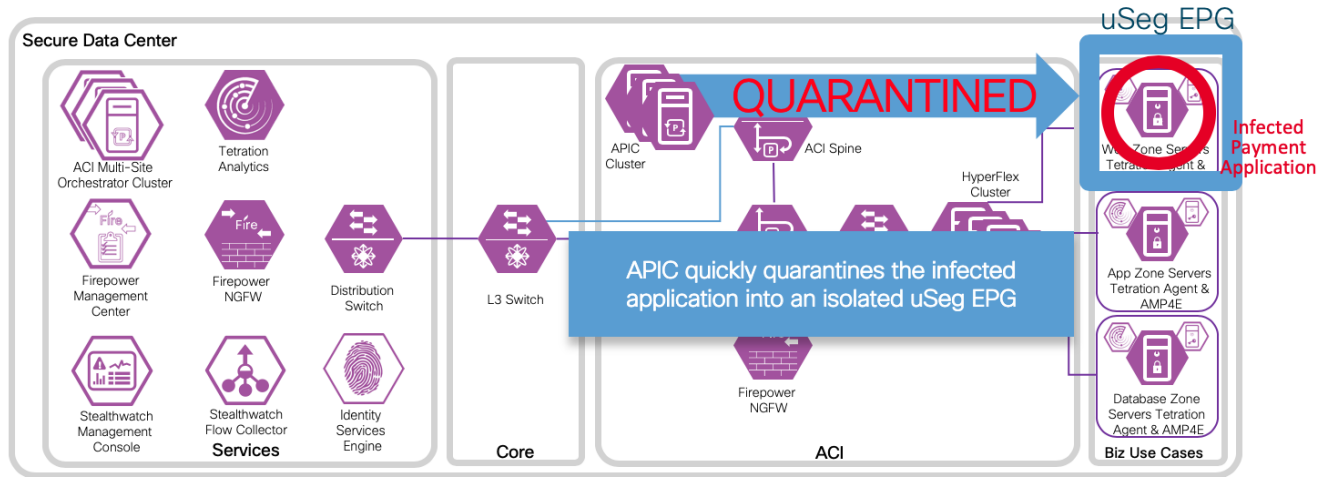
4. An attack event is generated and sent to the FMC. The attack event includes information about the infected endpoint.



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.



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

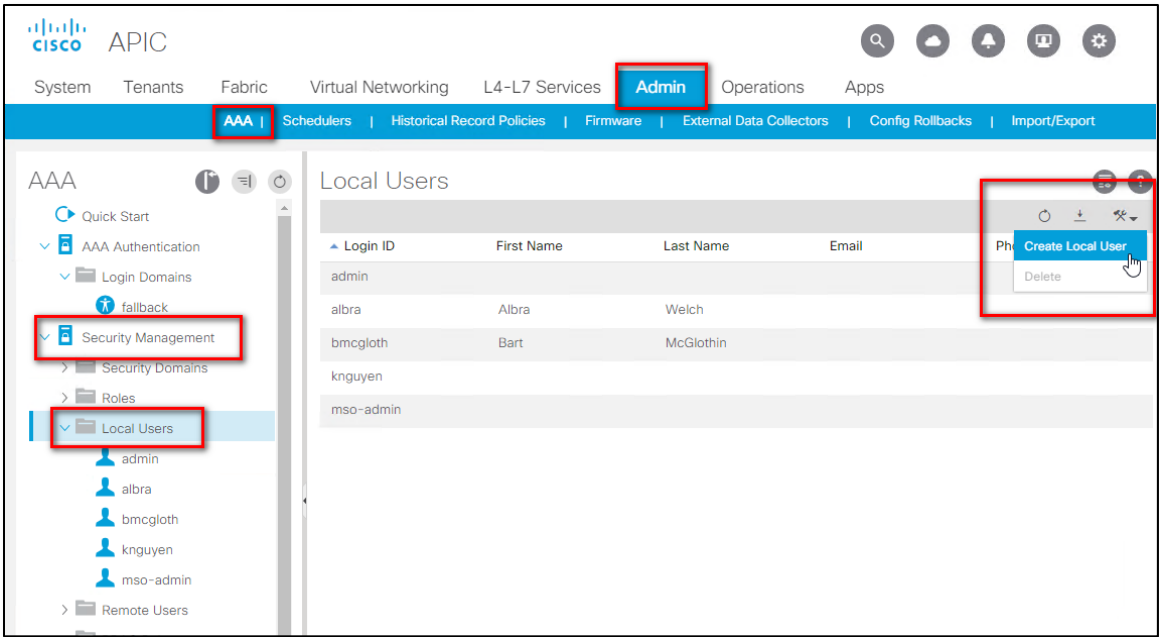
The remediation module uses credentials to authenticate and implement the uSeg request from the Firepower Management Center. These credentials can be created in the AAA provider, or as a local user as outlined in the steps below.

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**.

The screenshot shows the 'Create Local User' wizard. The title is 'Create Local User'. Below the title, there are three steps: '1. User Identity' (highlighted), '2. Security', and '3. Roles'. The current step is 'STEP 1 > User Identity'. The form is titled 'Specify the User Identity' and contains the following fields:

- Login ID: FMC-RTC
- Password:
- Confirm Password:
- First Name: FirepowerMC
- Last Name: RapidThreatContainment
- Phone:
- Email:
- Description: optional

Below the form, there are two sections:

- Account Status: ☒ Active ☐ Inactive
- Account Expires: ☒ No ☐ Yes

At the bottom right, there are three buttons: 'Previous', 'Cancel', and 'Next' (highlighted with a red box).

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

Create Local User

1. User Identity

2. Security

3. Roles

STEP 2 > Security

Enter the Security Information for this User

Security Domain:

Name	Description
<input checked="" type="checkbox"/> all	
<input type="checkbox"/> common	
<input type="checkbox"/> mgmt	
<input type="checkbox"/> MS_EXT_L3_Domain	
<input type="checkbox"/> T1 L3 Domain	

User Certificates:

Name	Expiration Date	State
------	-----------------	-------

SSH Keys:

Name	Key
------	-----

Previous

Cancel

Next

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

Create Local User

1. User Identity

2. Security

3. Roles

STEP 3 > Roles

Select the Roles for each Security Domain

Domain all:

Role Name	Role Privilege Type
admin	Write

Update

Cancel

Previous

Cancel

Finish

- d. Repeat for each site.

212

Installation

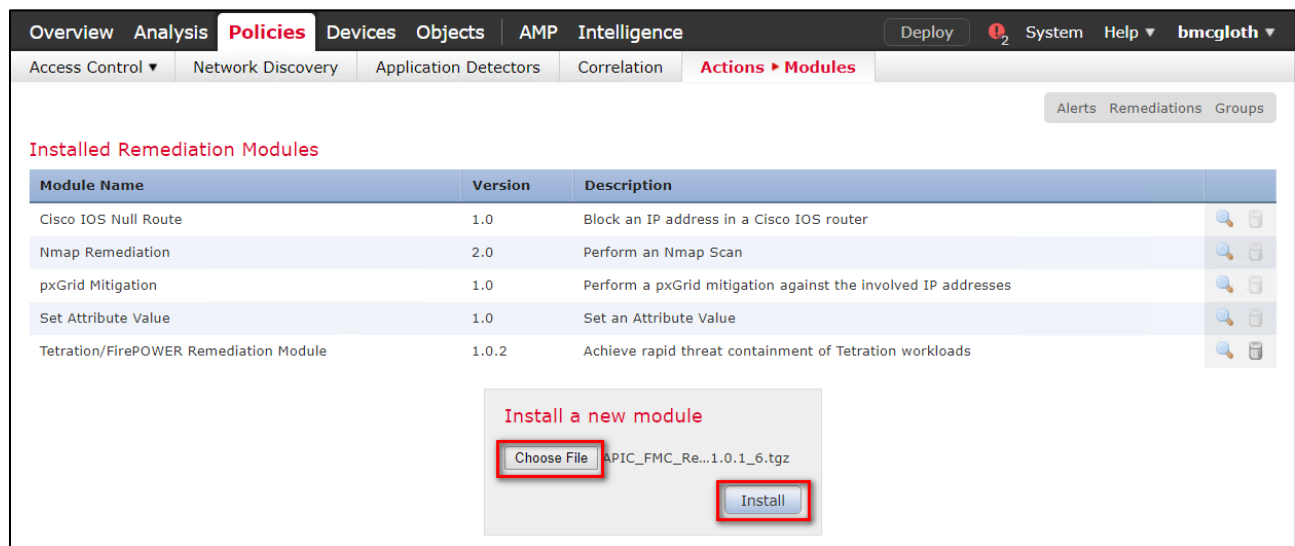
To download and install the Cisco Firepower Management Center Remediation Module for APIC, complete the following procedure:

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:

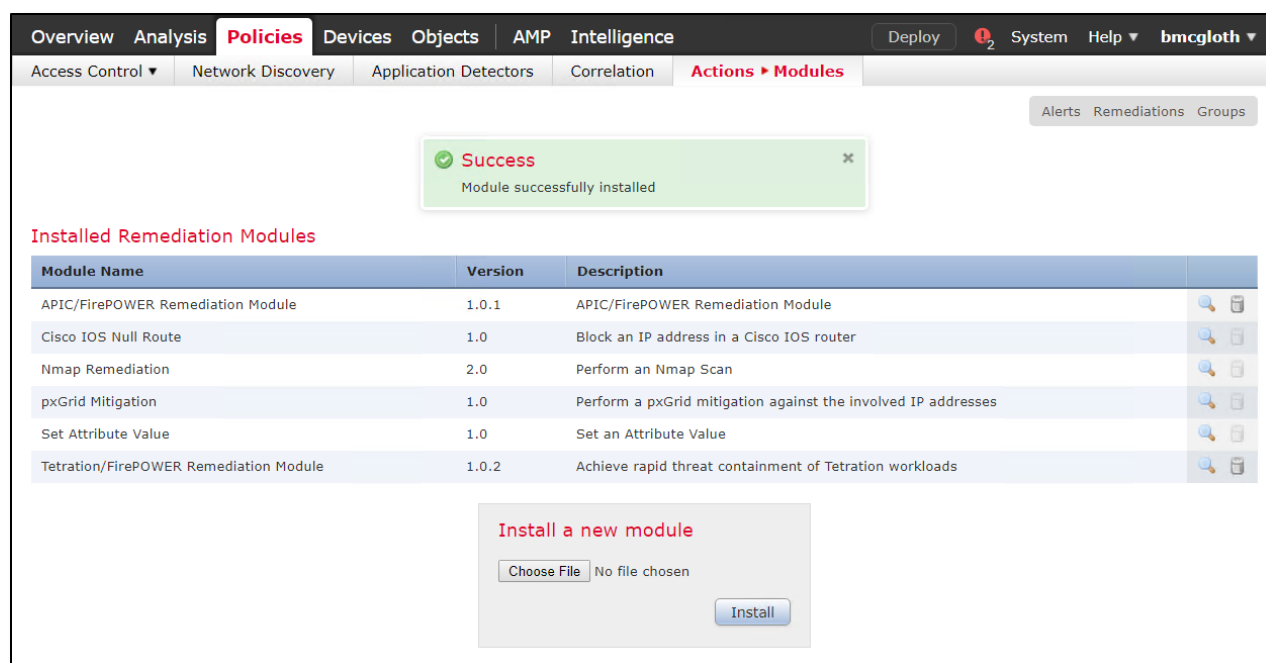
- In the FMC GUI, navigate to **Policies > Actions > Modules**.
- In the **Install a new module** dialog box, click **Choose File** as shown below.
- Select the file for the remediation module that was downloaded in Step 1.
- Click **Install**.



NOTE:

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

213



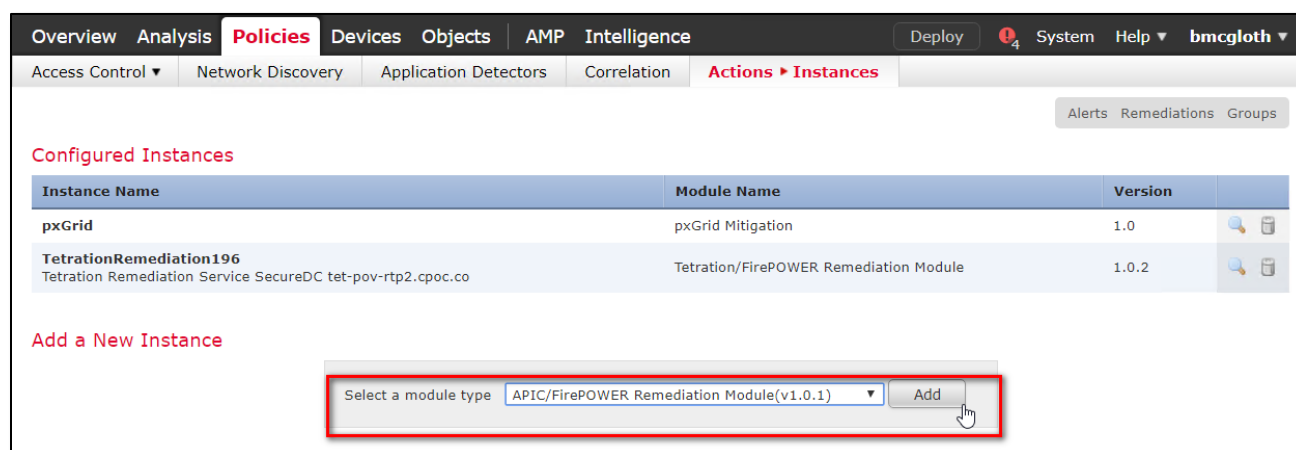
When successfully installed, the Cisco Firepower Management Center Remediation Module for APIC is displayed in the list of installed remediation modules.

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:

- Navigate to **Policies > Actions > Instances**.
- Select the remediation module in the drop-down list, and click **Add**.



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

214

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

The screenshot shows the 'Edit Instance' form in the Palo Alto Networks management console. The form is titled 'Edit Instance' and is part of the 'Actions > Instances' section. It contains the following fields:

- Instance Name: ACIuSeg-SDC1
- Module: APIC/FirePOWER Remediation Module(v1.0.1)
- Description: Rapid Threat Containment using micro-segmentation for SDC-1
- APIC server username: FMC-RTC
- APIC server password: (masked with dots)
- APIC cluster instance 1 IP: 10.17.4.11
- APIC cluster instance 2 IP: 10.17.4.12
- APIC cluster instance 3 IP: 10.17.4.13
- APIC cluster instance 4 IP: (empty)
- APIC cluster instance 5 IP: (empty)

The 'Create' button is highlighted with a red box.

- 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.

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligenceDeploy6SystemHelpbmccloth

Access ControlNetwork DiscoveryApplication DetectorsCorrelationActions ▶ InstancesAlertsRemediationsGroups

SuccessCreated new instance ACIUseg-SDC1

Edit Instance

Instance NameACIUseg-SDC1

ModuleAPIC/FirePOWER Remediation Module(v1.0.1)

DescriptionRapid Threat Containment using micro-segmentation for SDC-1

APIC server usernameFMC-RTC

APIC server passwordRetype to confirm

APIC cluster instance 1 IP10.17.4.11

APIC cluster instance 2 IP10.17.4.12

APIC cluster instance 3 IP10.17.4.13

APIC cluster instance 4 IP

APIC cluster instance 5 IP

SaveCancel

Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		
Add a new remediation of type Quarantine an End Point on APIC		Add

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

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligenceDeploy6SystemHelpbmccloth

Access ControlNetwork DiscoveryApplication DetectorsCorrelationActions ▶ InstancesAlertsRemediationsGroups

Edit Remediation

Remediation NameACIQuarantineEP-SDC1

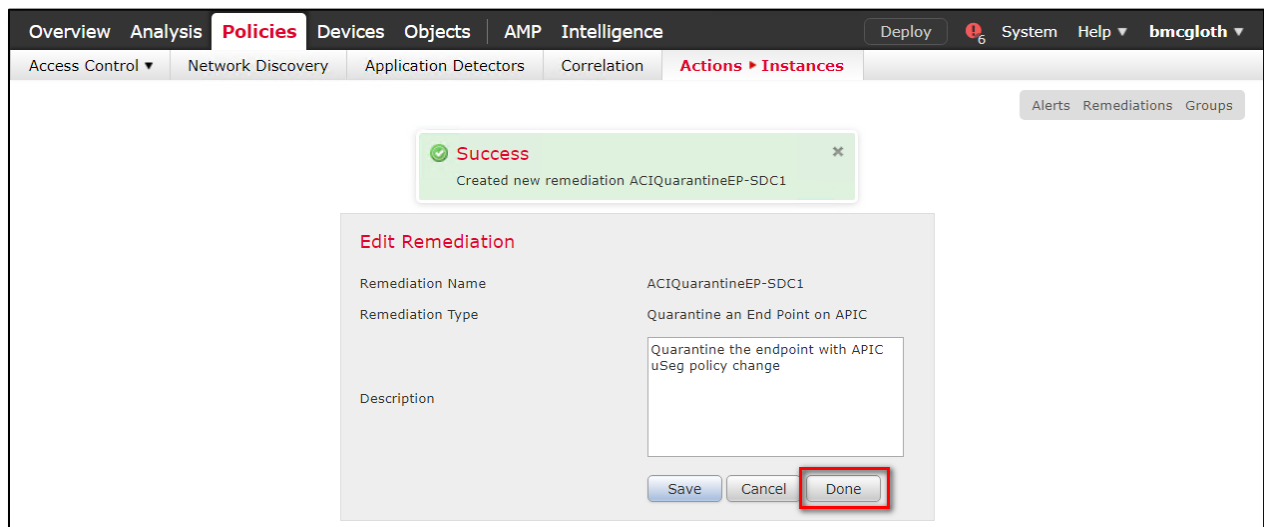
Remediation TypeQuarantine an End Point on APIC

DescriptionQuarantine the endpoint with APIC uSeg policy change

CreateCancel

216

- 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.

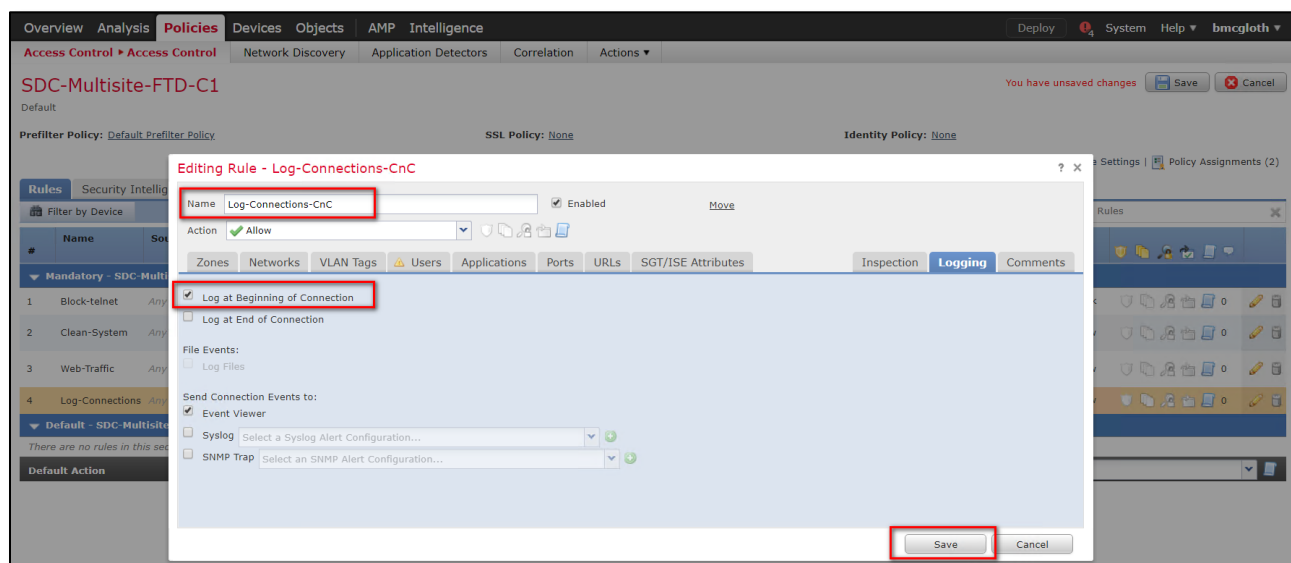
Step 3 Configure the policy to log connections to be tested for intrusion, in this example we identify CnC traffic.

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

- Navigate to **Policies > Access Control** then **Edit** the policy.
- Click **Edit Rule** (for example, Log-Connections-CnC or Web Traffic).
- 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**.

217

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**.

The screenshot shows the Cisco Firepower Rule Management interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, and Intelligence. The Policies tab is active, and the Correlation section is selected. The Rule Management sub-tab is active, showing the configuration for a rule named 'Quarantine_by_CnC'.

Rule Information:

- Rule Name: Quarantine_by_CnC
- Rule Description: Connections to CnC or Attackers trigger this rule
- Rule Group: Ungrouped

Select the type of event for this rule:

If a connection event occurs at either the beginning or the end of the connection and it meets the following conditions:

Conditions:

- Security Intelligence Category is CnC
- Security Intelligence Category is Attackers

Rule Options:

- Snooze: If this rule generates an event, snooze for 0 hours
- Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

The **Save** button is highlighted in red.

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:

218

- Navigate to **Policies > Correlation > Policy Management**.
- Click **Create Policy**.
- Enter a **Policy Name** (in this example, **Compromised Server**) and **description** (optional).
- From the **Default Priority** drop-down list, select a priority for the policy. Select **None** to use rule priorities only.
- Click **Add Rules**, select the correlation rule you previously configured in Step 3 (in this example, **Quarantine_by_CnC**), and click **Add**.

Correlation Policy Information

Policy Name:

Policy Description:

Default Priority:

Policy Rules

Rule	Responses	Priority
Quarantine_by_CnC Connections to CnC or Attackers trigger this rule	This rule does not have any responses.	Default

Add Rules

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

Responses for Quarantine_by_CnC

Assigned Responses

ACIQuarantineEP-SDC1

Unassigned Responses

ACIQuarantineEP-SDC2
LabLog
Quarantine_SourceIP
Shutdown
TetrationUnQuarantineEP

Update **Cancel**

- Click **Update**.

219

Correlation Policy Information

You have unsaved changes **Save** **Cancel**

Policy Name:

Policy Description:

Default Priority:

Policy Rules

Rule	Responses	Priority
<u>Quarantine by CnC</u> Connections to CnC or Attackers trigger this rule	ACIQuarantineEP-SDC1 (Remediation) ACIQuarantineEP-SDC2 (Remediation)	Default

[Add Rules](#)

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.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy 3 System Help bmcglath

Context Explorer Connections Intrusions Files Hosts Users Vulnerabilities Correlation Status Custom Lookups

Bookmark This Page Report Designer View Bookmarks Search

Remediation Status

Table View of Remediations

2018-10-31 10:55:05 - 2018-11-01 10:55:05 Expanding

No Search Constraints (Edit Search)

Jump to...

	Time	Remediation Name	Policy	Rule	Result Message
2018-11-01 10:51:35	ACIQuarantineEP-SDC1	Compromised Server	Quarantine by CnC	Successful completion of remediation	
2018-11-01 10:51:35	ACIQuarantineEP-SDC2	Compromised Server	Quarantine by CnC	"Required info is not found based on the IP of the incident source, c"	

Page 1 of 1 of 2 rows

ViewDelete

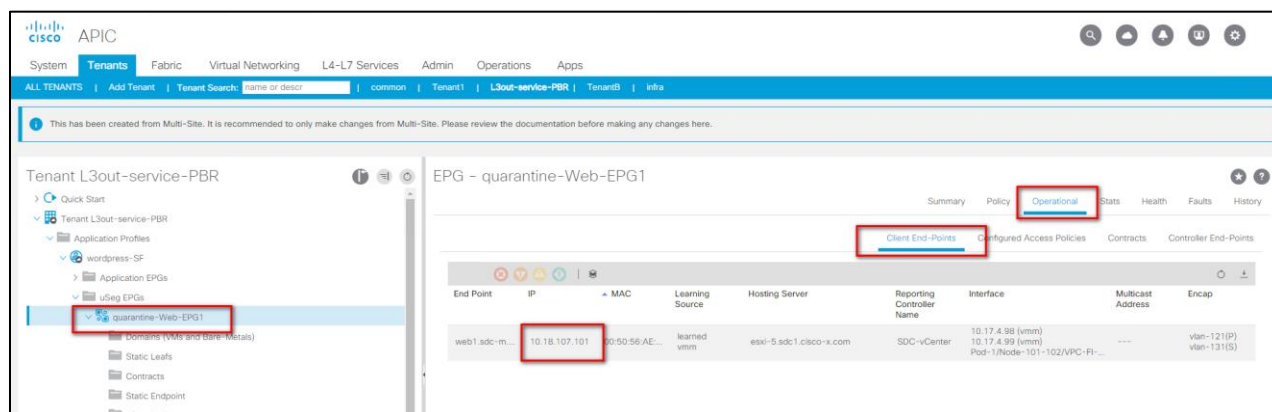
View AllDelete All

Step 4 Go to the APIC GUI:

- Navigate to **Tenant > Application Profiles > uSeg EPGs**.
- Select the newly created quarantine EPG (in this example, quarantine-Web-EPG1).

220

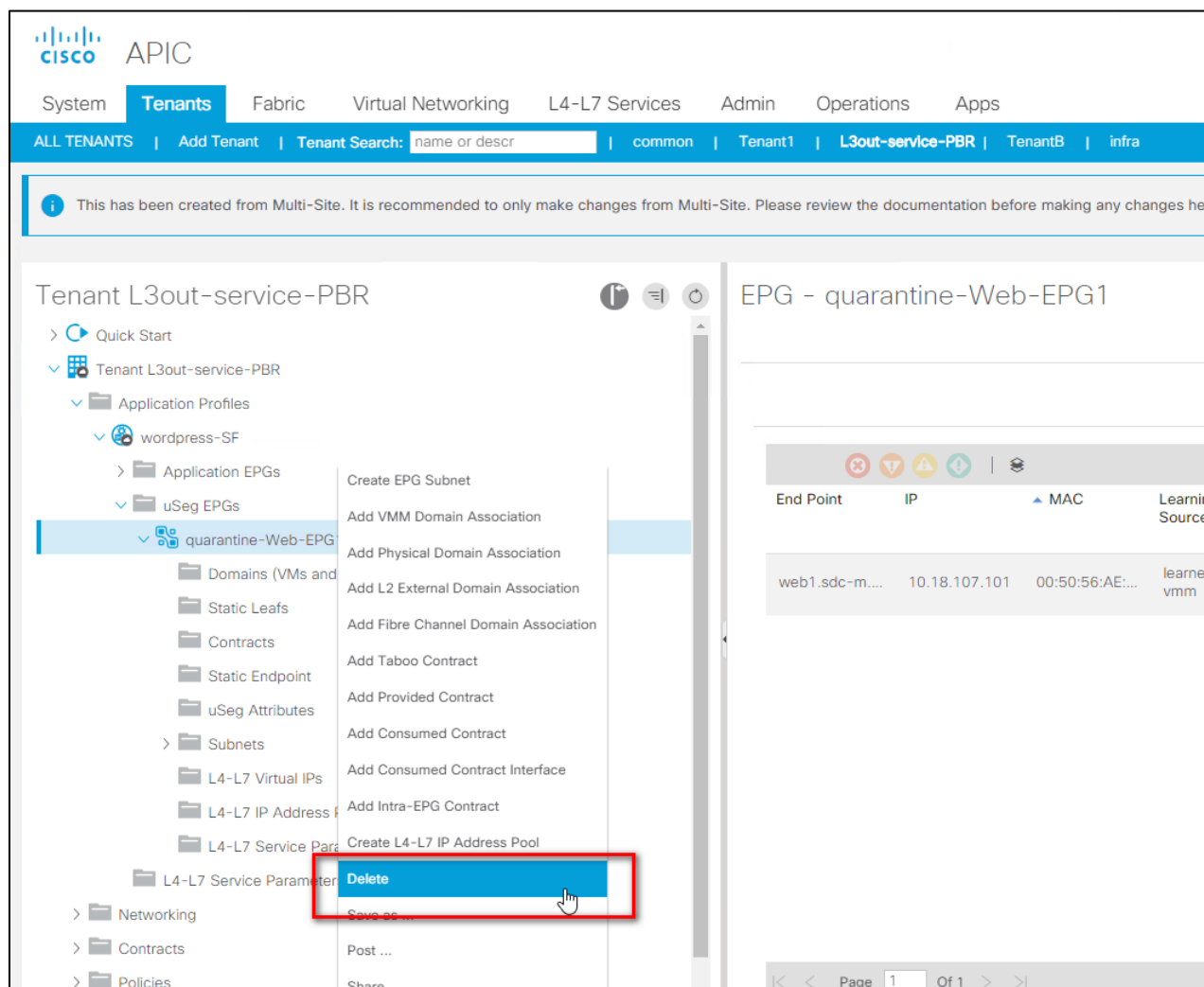
- c. Select **Operational** > **Client End-Points** and verify the correct server IP quarantined.



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.



221

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

Delete

?

✕

These tables show the nodes where this policy is used and the other policies that use this policy. If you delete this policy, it will affect the nodes and policies shown in the tables. Are you sure you want to delete: quarantine-Web-EPG1?

Nodes using this policy

Choose Usage: Interface

Node Id

Name

Resources

101

SDC1-LF1

[Click to Show D...](#)

102

SDC1-LF2

[Click to Show D...](#)

Policies using this policy

Name

Type

This policy is not used by any other policy.

Change Global Deployment Settings

No

Yes

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

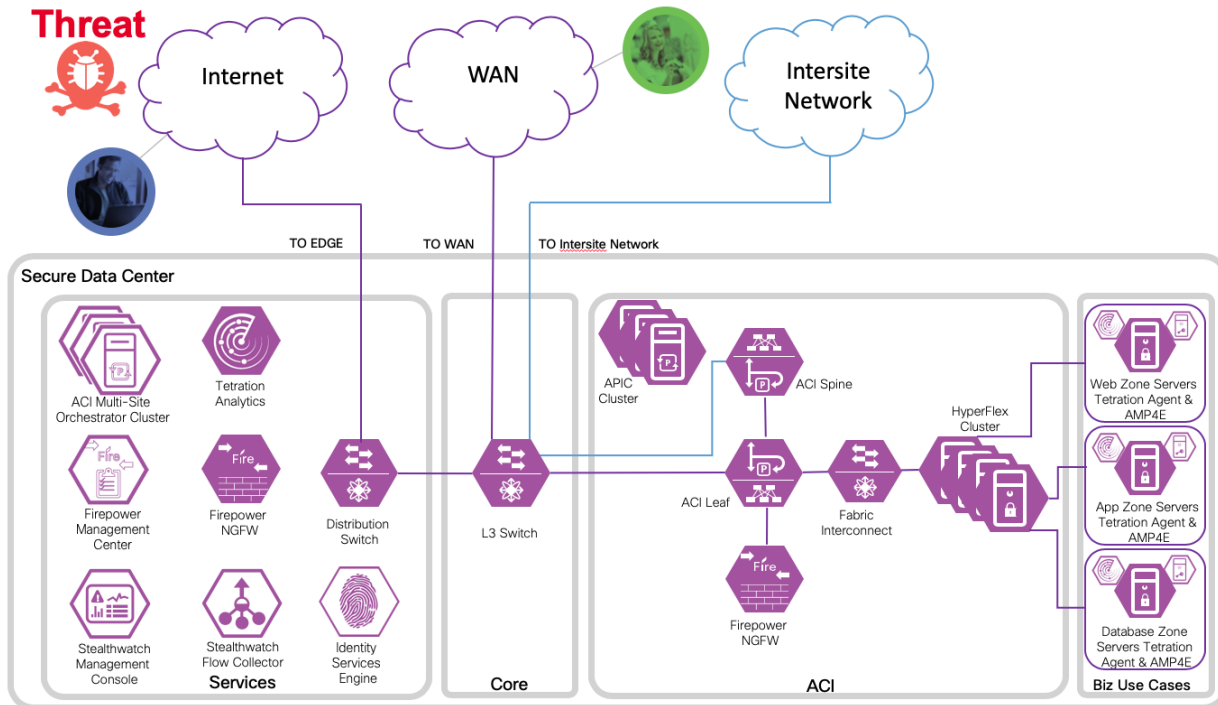
Return to Contents

Test Case 7 – FTD Rapid Threat Containment with Tetration

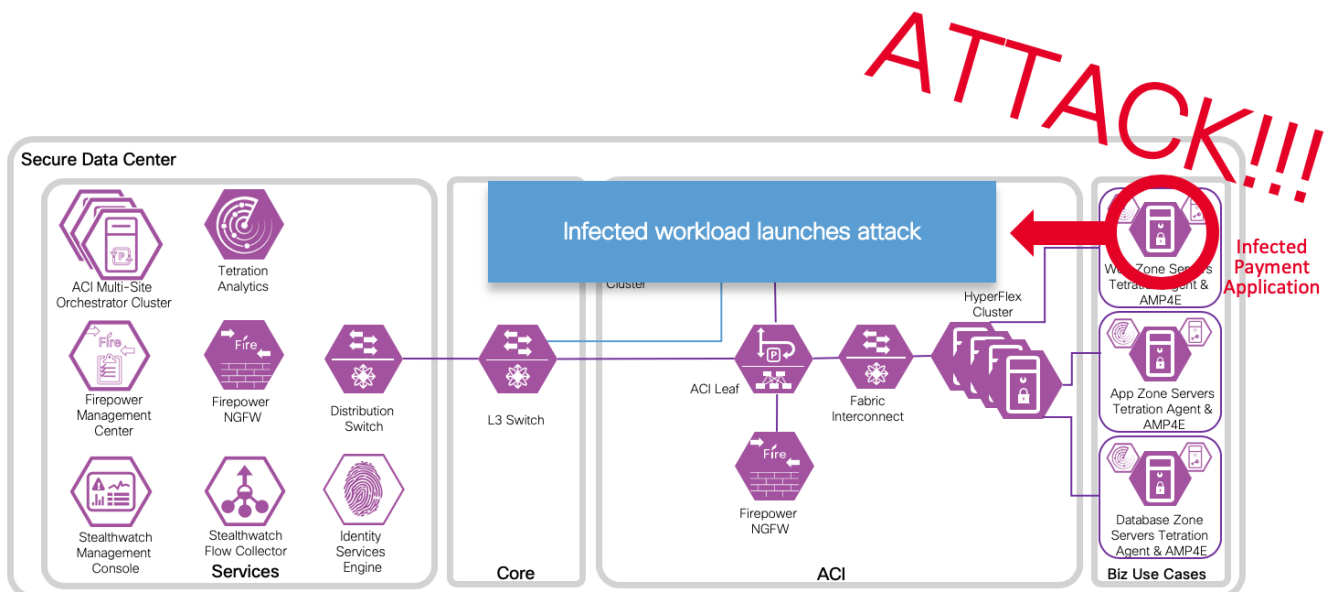
This integration involves identifying an attacker in FMC based on AMP4E, AMP4N, NGIPS and extract the IP address of the attacker. FMC will use this information in the Tetration Remediation module to push out policy to quarantine this host.

Test Description:

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

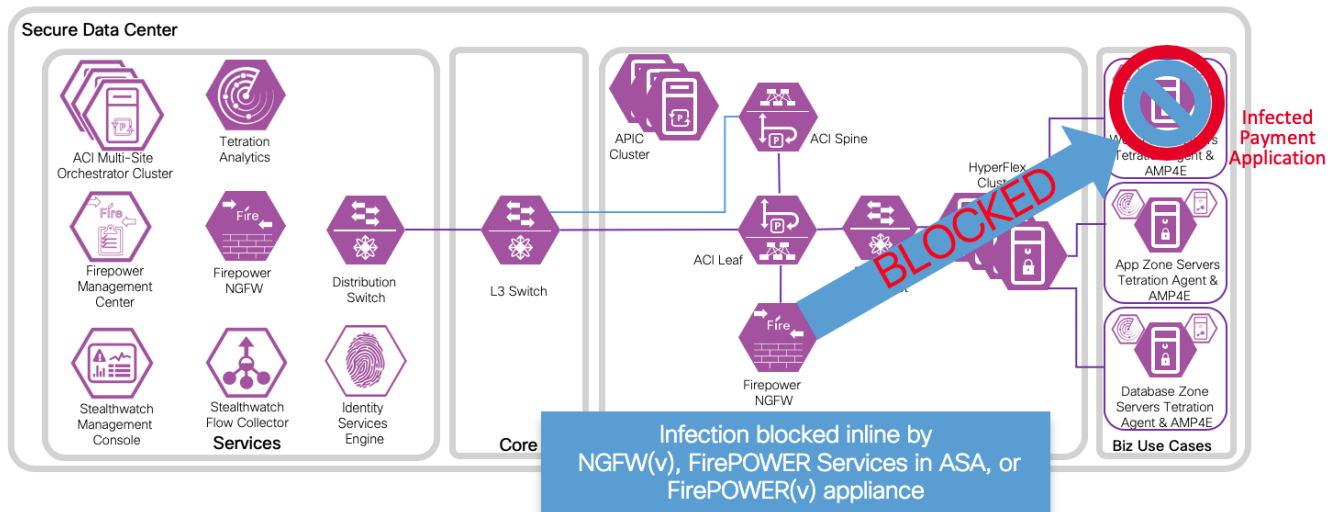


2. An endpoint with an infected application launches an attack.

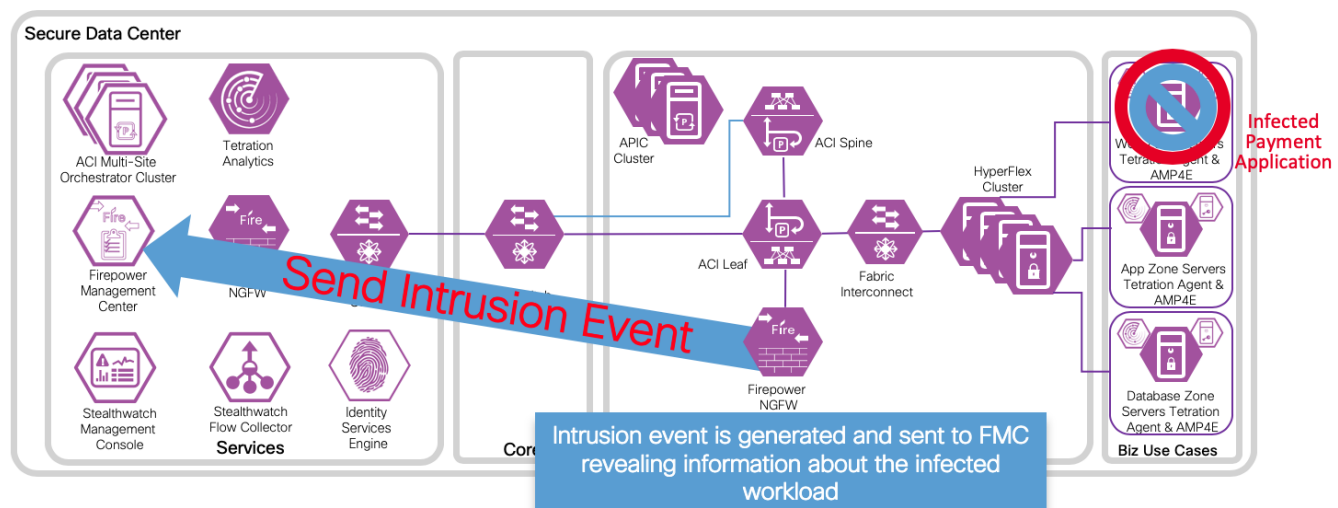


223

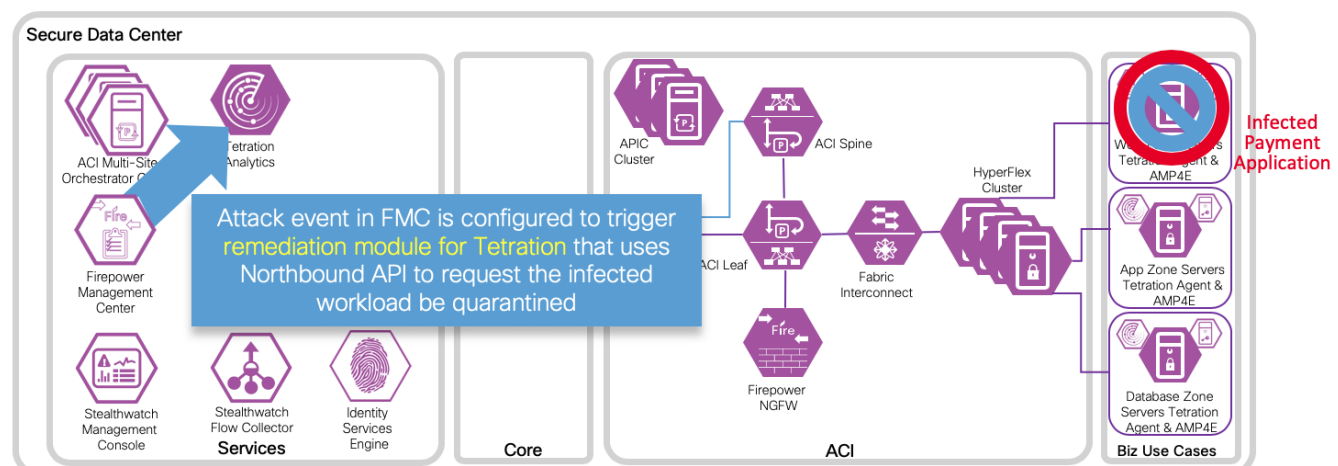
3. The attack is blocked inline by Cisco Firepower Threat Defense.



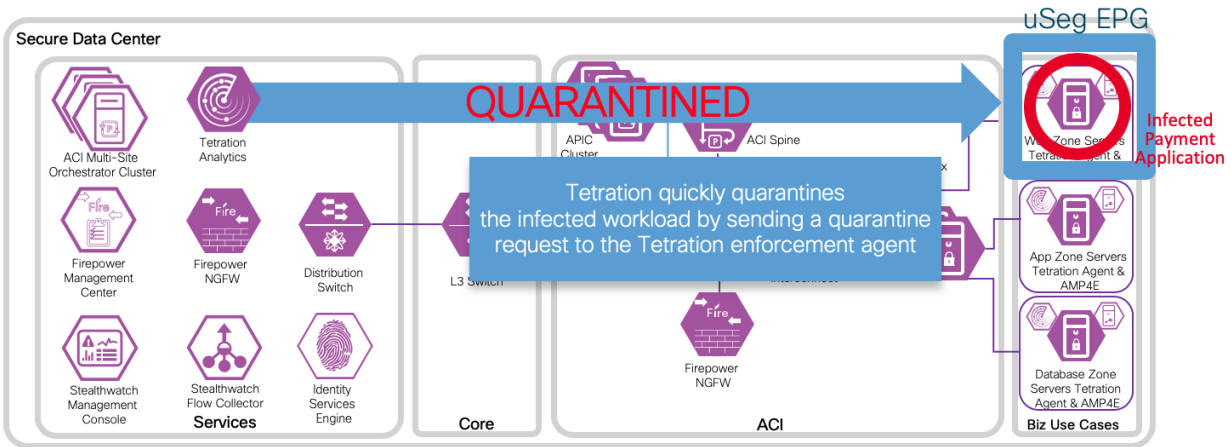
4. An attack event is generated and sent to the FMC. The attack event includes information about the infected endpoint.



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



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

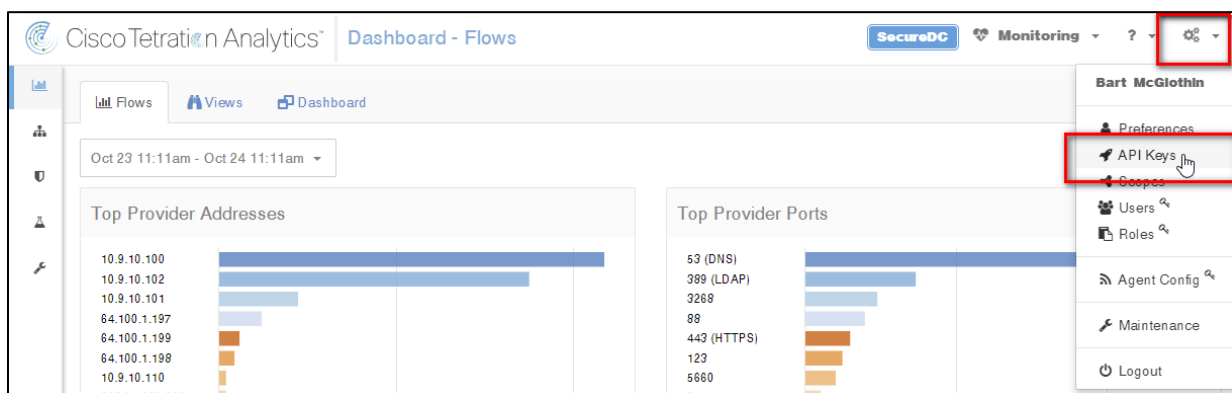
The API key and secret must first be created in TA by a site admin, customer support, or a root scope owner role. Copy that information for use in configuration steps to follow.

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.

225

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

Cisco Tetration Analytics

API Keys

SecureDC

Monitoring

?

Create API Key

Description

Secure Data Center Multi Site RTC with FMC

☐ SW sensor management: API to configure and monitor status of SW sensors

☒ Flow and inventory search: API to query flows and inventory items in Tetration cluster

☐ Users, roles and scope management: API for root scope owners to read/add/modify/remove users, roles and scopes

☒ User data upload: API for root scope owners to upload data for annotating flows and inventory items

☐ Applications and policy management: API to manage applications and enforce policies

☐ External system integration: API to allow integration with external systems

Create

Cancel

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

API Key Created

API Key: a100856

API Secret: 8387

Download

Please make note of the API secret, this is the only time it will be displayed.

OK

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

Cisco Tetration Analytics

API Keys

SecureDC

Monitoring

?

Create API Key

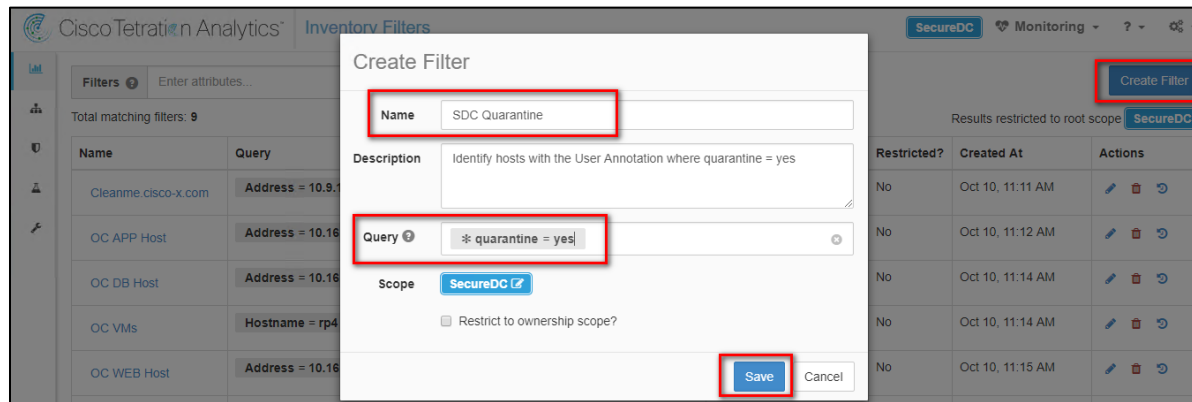
API Key	Capabilities	Description	Created At	Last Used	
	<ul style="list-style-type: none">flow_inventory_queryuser_data_upload	Secure Data Center Multi Site RTC with FMC	Oct 25 09:27:32 am (PDT)		

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**

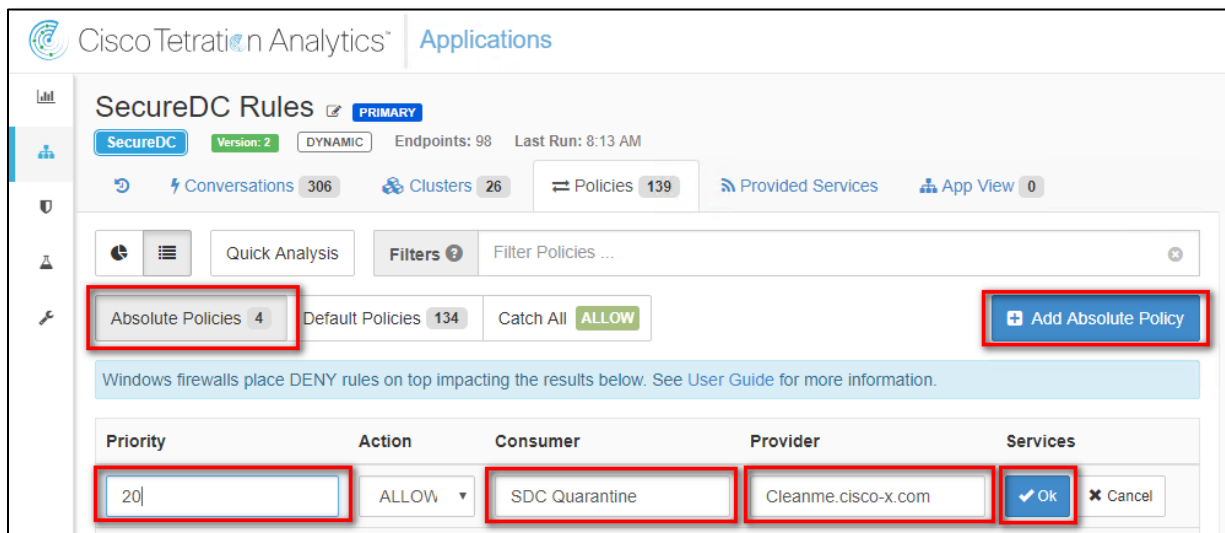
226

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

- Navigate to **Applications > [Workspace] > Policies > Absolute Policies** and click the **Add Absolute Policy** button.
- Set a priority, specify the consumer as the **SDC Quarantine filter** we created earlier, specify the provider as the **<your-remediation-server> filter**.



- Click **OK**
- 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.

Service Ports: (0)

TCP

80

✓

✕

No services defined.

- 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.

Cisco Tetration Analytics

Applications

Monitoring

SecureDC Rules

SecureDC

Version: 2

DYNAMIC

Endpoints: 98

Last Run: 8:13 AM

Conversations 306

Clusters 26

Policies 138

Provided Services

App View 0

Quick Analysis

Filters

Filter Policies ...

Absolute Policies 3

Default Policies 134

Catch All ALLOW

Add Absolute Policy

Windows firewalls place DENY rules on top impacting the results below. See User Guide for more information.

Priority	Action	Consumer	Provider	Services
15	ALLOW	SDC Quarantine	SecureDC : DNS	UDP : 53 (DNS)
20	ALLOW	SDC Quarantine	Cleanme.cisco-x.com	TCP : 80 (HTTP)
90	DENY	SDC Quarantine	SecureDC	Inactive

Policy

Priority 90

Action DENY

Consumer SDC Quarantine

Provider SecureDC

View Conversations

ANY

Port e.g. 80-100

✓

✕

No services defined.

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**.

228

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy 4 System Help bmcgloth

Access Control Network Discovery Application Detectors Correlation **Actions > Modules**

Alerts Remediations Groups

Installed Remediation Modules

Module Name	Version	Description
APIC/FirePOWER Remediation Module	1.0.1	APIC/FirePOWER Remediation Module
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value

Install a new module

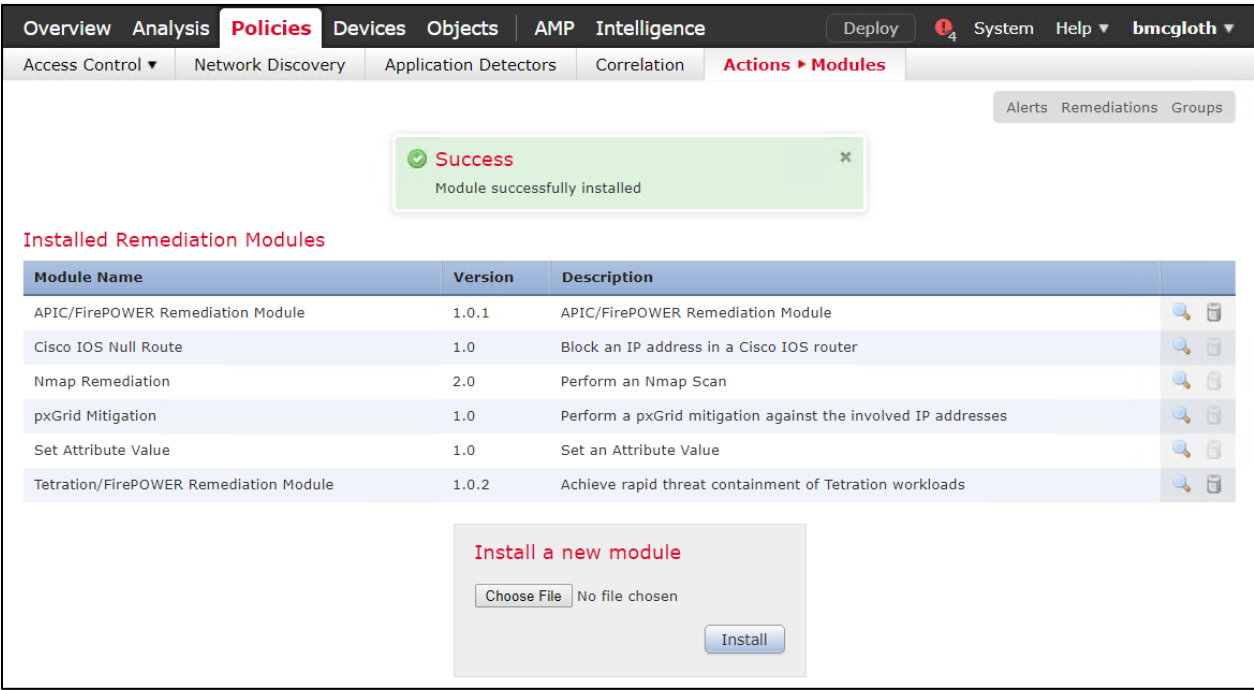
Choose File tetration_FMC...le_1.0.2.tgz Install

NOTE:

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

229

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:

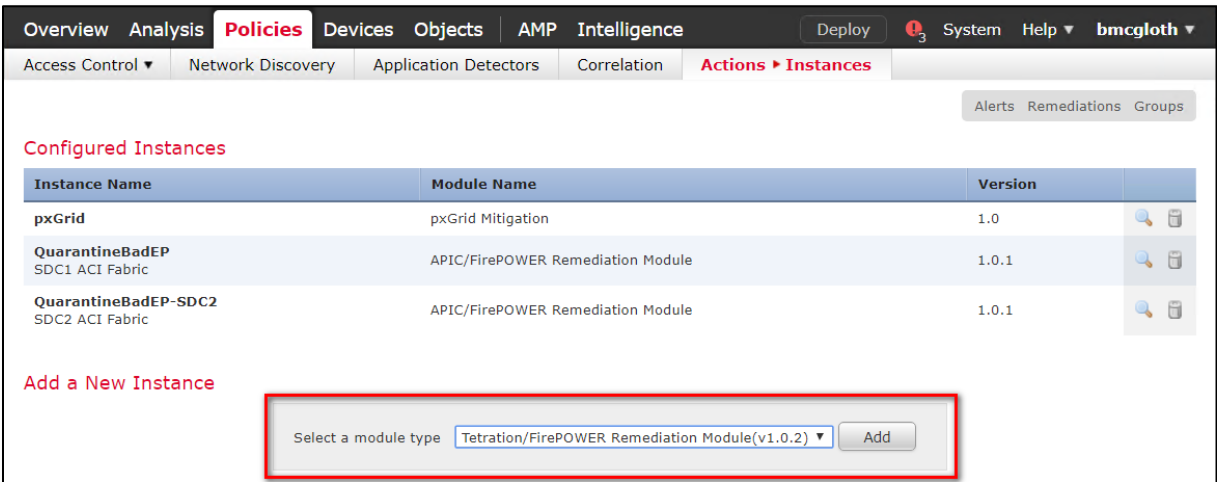
Step 1

Create 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**.

230

- 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.

The screenshot shows the 'Edit Instance' form in the Palo Alto Networks management console. The form is titled 'Edit Instance' and is part of the 'Actions > Instances' section. It contains the following fields and values:

- Instance Name:** TetrationRemediation196
- Module:** Tetration/FirePOWER Remediation Module(v1.0.2)
- Description:** Tetration Remediation Service
SecureDC tet-pov-rtp2.cpoc.co
- Tetration Analytics IP:** 64.1
- Scope(e.g. Default):** SecureDC
- API key:** [Redacted]
- API secret:** [Redacted]

The 'Create' button is highlighted with a red box.

231

- 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.

The screenshot shows the 'Edit Instance' page for 'TetrationRemediation196'. A green success message at the top states 'Created new instance TetrationRemediation196'. The form fields include:

- Instance Name: TetrationRemediation196
- Module: Tetration/FirePOWER Remediation Module(v1.0.2)
- Description: Tetration Remediation Service SecureDC tet-pov-rtp2.cpoc.co
- Tetration Analytics IP: 64.1...
- Scope(e.g. Default): SecureDC
- API key: [Redacted]
- API secret: [Redacted]

At the bottom, the 'Configured Remediations' section shows a table with no entries. Below the table, a dropdown menu is set to 'Quarantine an IP on Tetration Analytics', and the 'Add' button is highlighted with a red box.

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

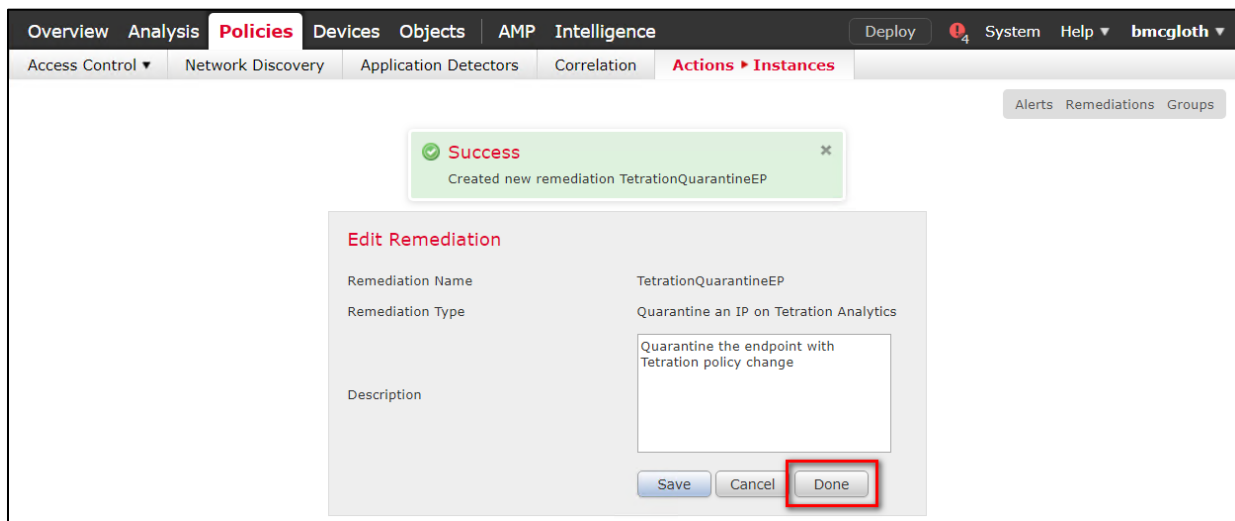
The screenshot shows the 'Edit Remediation' page. The form fields include:

- Remediation Name: TetrationQuarantineEP (highlighted with a red box)
- Remediation Type: Quarantine an IP on Tetration Analytics
- Description: Quarantine the endpoint with Tetration policy change

At the bottom, the 'Create' button is highlighted with a red box.

232

- 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.

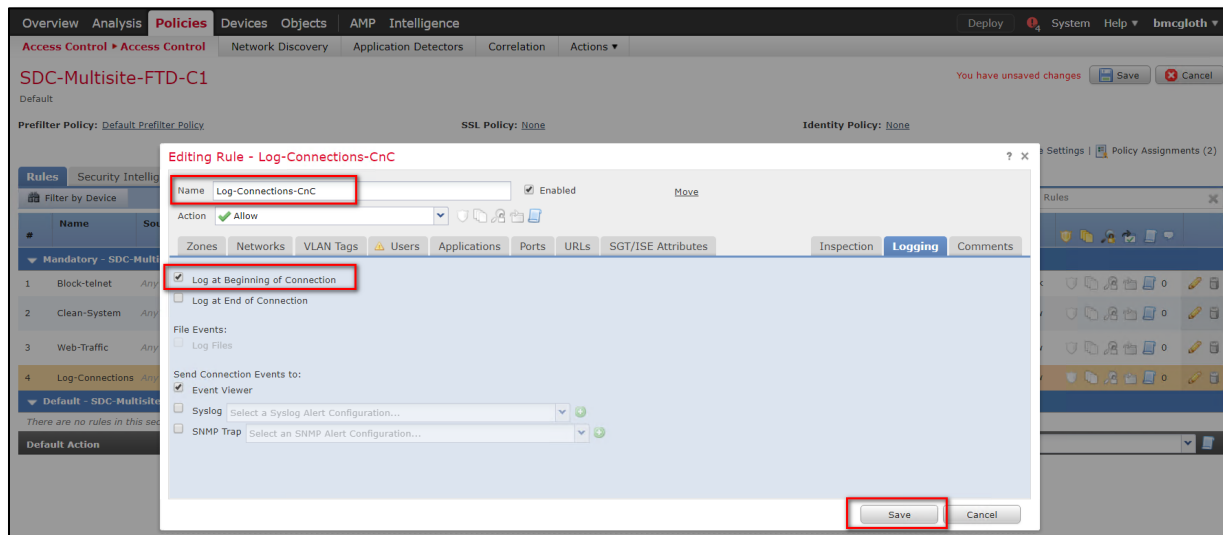
Step 2 Configure the policy to log connections to be tested for CnC traffic.

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

- Navigate to **Policies > Access Control** then **Edit** the policy.
- Click Edit Rule (for example, Log-Connections-CnC or Web Traffic).
- 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.



233

- 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**.

The screenshot displays the Cisco Firepower Rule Management interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, and Intelligence. The Policies tab is active, showing sub-tabs for Access Control, Network Discovery, Application Detectors, Correlation (selected), and Actions. The Correlation sub-tab is active, showing sub-tabs for Policy Management, Rule Management (selected), White List, and Traffic Profiles. The Rule Management sub-tab is active, showing the configuration for a rule named 'Quarantine_by_CnC'. The Rule Information section shows the Rule Name as 'Quarantine_by_CnC', Rule Description as 'Connections to CnC or Attackers trigger this rule', and Rule Group as 'Ungrouped'. The Select the type of event for this rule section shows the event type as 'a connection event occurs' and the event location as 'at either the beginning or the end of the connection'. The conditions section shows two conditions: 'Security Intelligence Category is CnC' and 'Security Intelligence Category is Attackers', with the operator set to 'OR'. The Rule Options section shows the Snooze option set to 0 hours and the Inactive Periods section with a message: 'There are no defined inactive periods. To add an inactive period, click "Add Inactive Period"'. The Save button is highlighted with a red box.

- 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**.

234

- 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**.

Correlation Policy Information

Policy Name:

Policy Description:

Default Priority:

Policy Rules

Rule	Responses	Priority
Quarantine_by_CnC Connections to CnC or Attackers trigger this rule	This rule does not have any responses.	Default

Add Rules

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

Responses for Quarantine_by_CnC

Assigned Responses

TetrationQuarantineEP

Unassigned Responses

QuarantineBadEP
QuarantineBadEP-SDC2
Shutdown
TetrationUnQuarantineEP
UnQuarantine_SourceIP

Update

- g. Click **Update**.

235

Correlation Policy Information

Policy Name:

Policy Description:

Default Priority:

Policy Rules

Rule	Responses	Priority
Quarantine by CnC Connections to CnC or Attackers trigger this rule	TetrationQuarantineEP (Remediation)	Default

You have unsaved changes **Save** **Cancel**

Save

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.

Overview

Analysis

Policies

Devices

Objects

AMP

Intelligence

Deploy

3

System

Help

bmcglath

Context Explorer

Connections

Intrusions

Files

Hosts

Users

Vulnerabilities

Correlation > Status

Custom

Lookup

Search

Bookmark This Page

Report Designer

View Bookmarks

Search

Remediation Status

Table View of Remediations

No Search Constraints (Edit Search)

2018-10-25 10:19:34 - 2018-10-26 10:27:53

Expanding

Jump to...

	Time	Remediation Name	Policy	Rule	Result Message
	2018-10-26 10:27:33	TetrationQuarantineEP	Compromised Server	Quarantine by CnC	Successful completion of remediation

<< Page 1 of 1 >>

Displaying row 1 of 1 rows

View

Delete

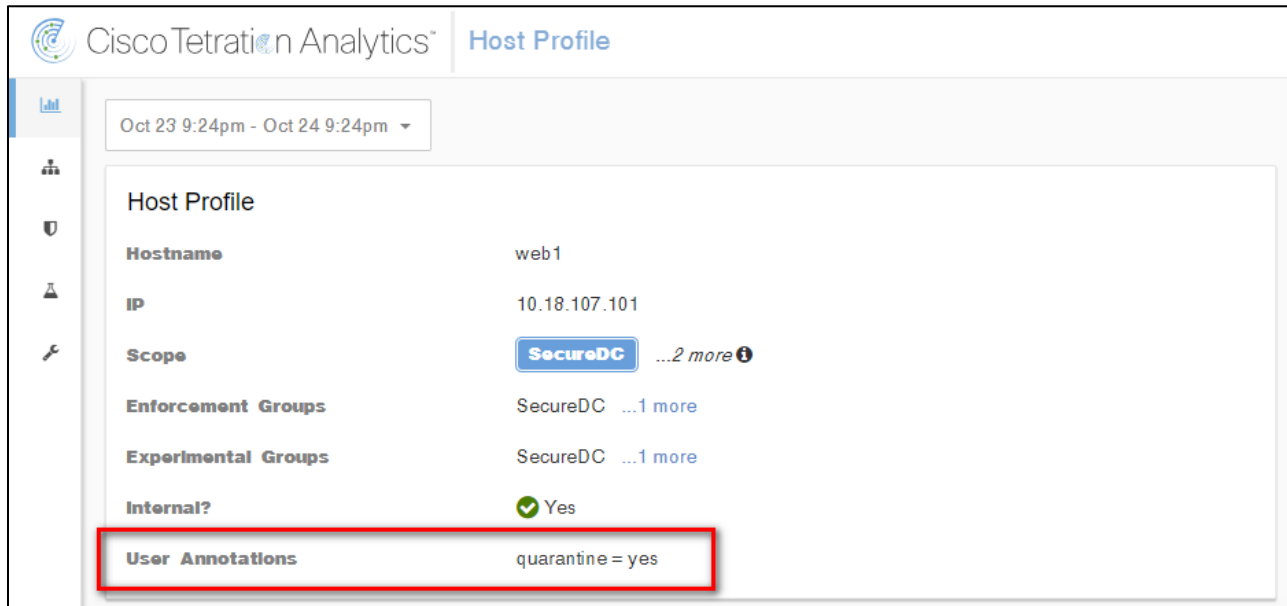
View All

Delete All

236

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

- Navigate to **Visibility > Inventory Search**.
- Enter the IP address of the infected host, and click **Search**.
- In User Annotations, you should see **quarantine = yes** annotated to the IP address of the infected host.



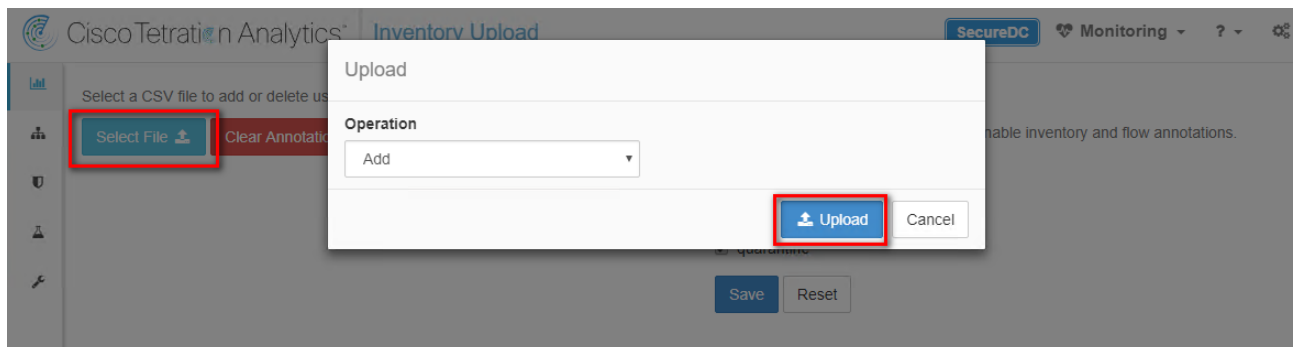
Step 5 What to do next

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.

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.

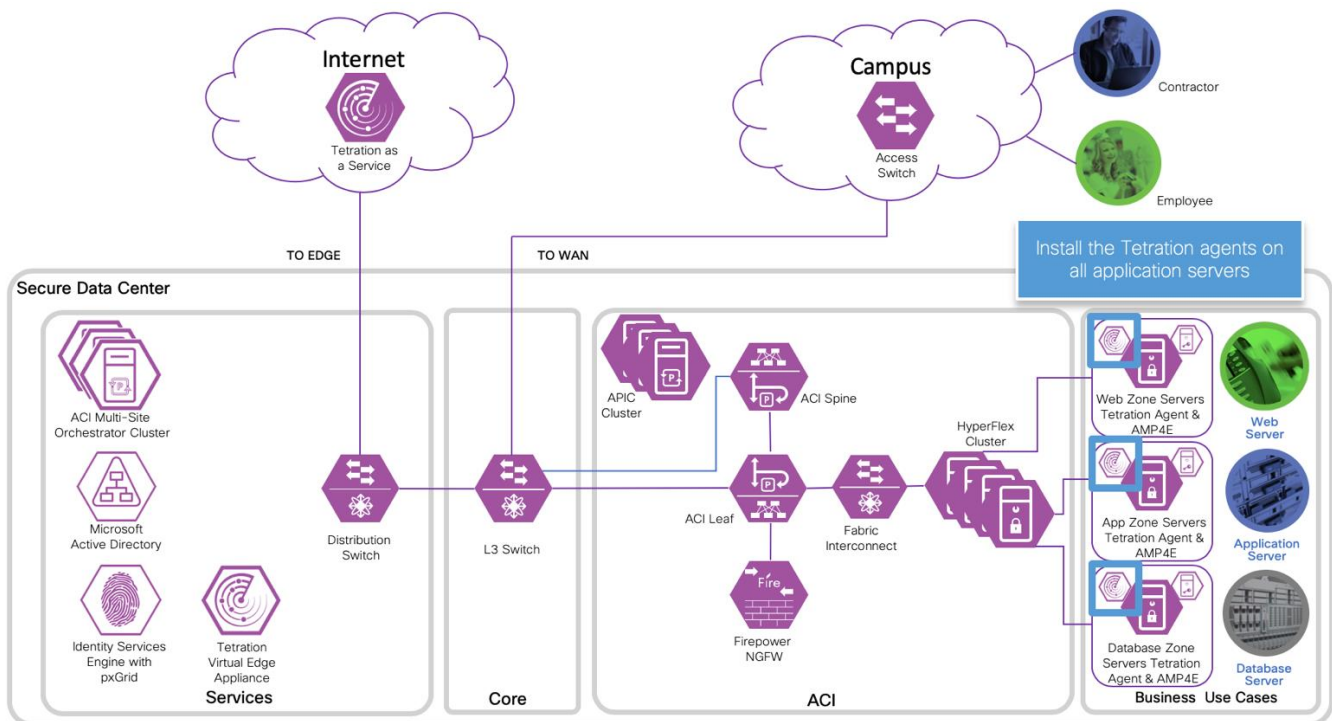
Test Description:

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.

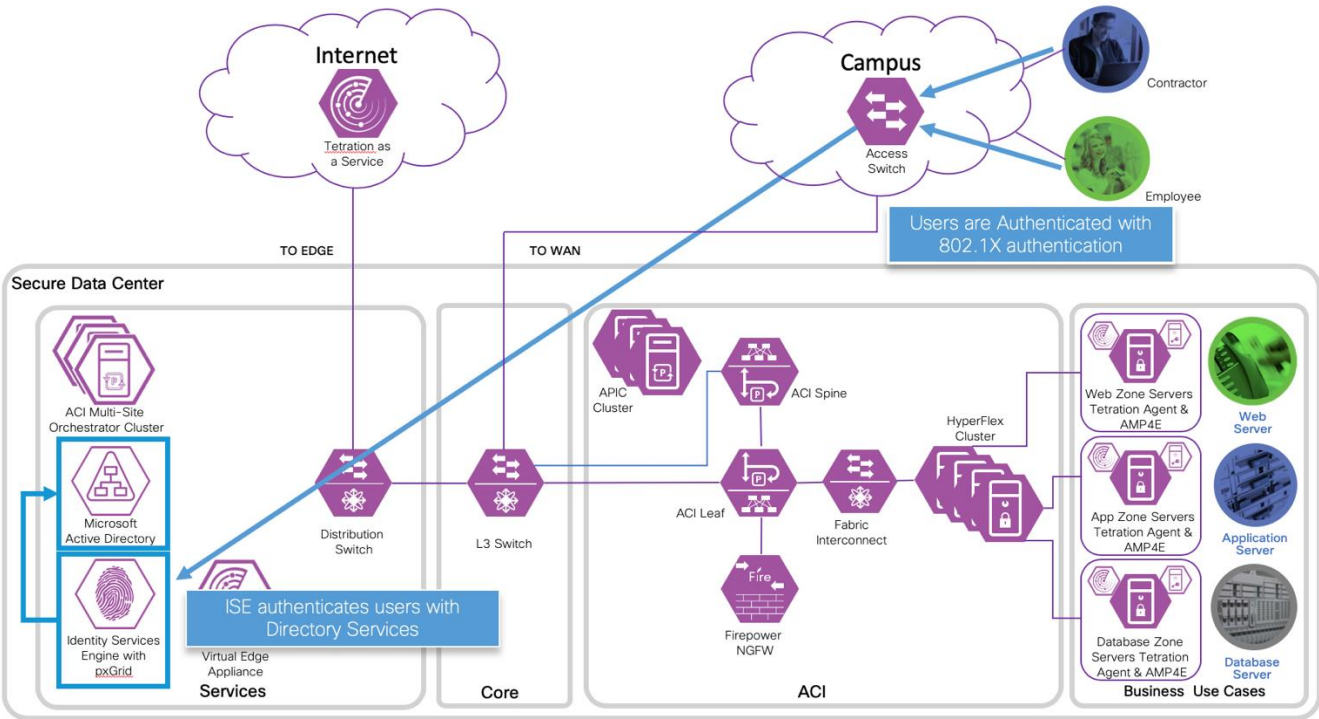
The important thing to note is the group Employees used in the policy is a Tetration filter. The filter is updated in near real time with changes in endpoint states, as users log on and off the network. These updates are provided by ISE through pxGrid and the Tetration Virtual Edge Appliance. This enables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

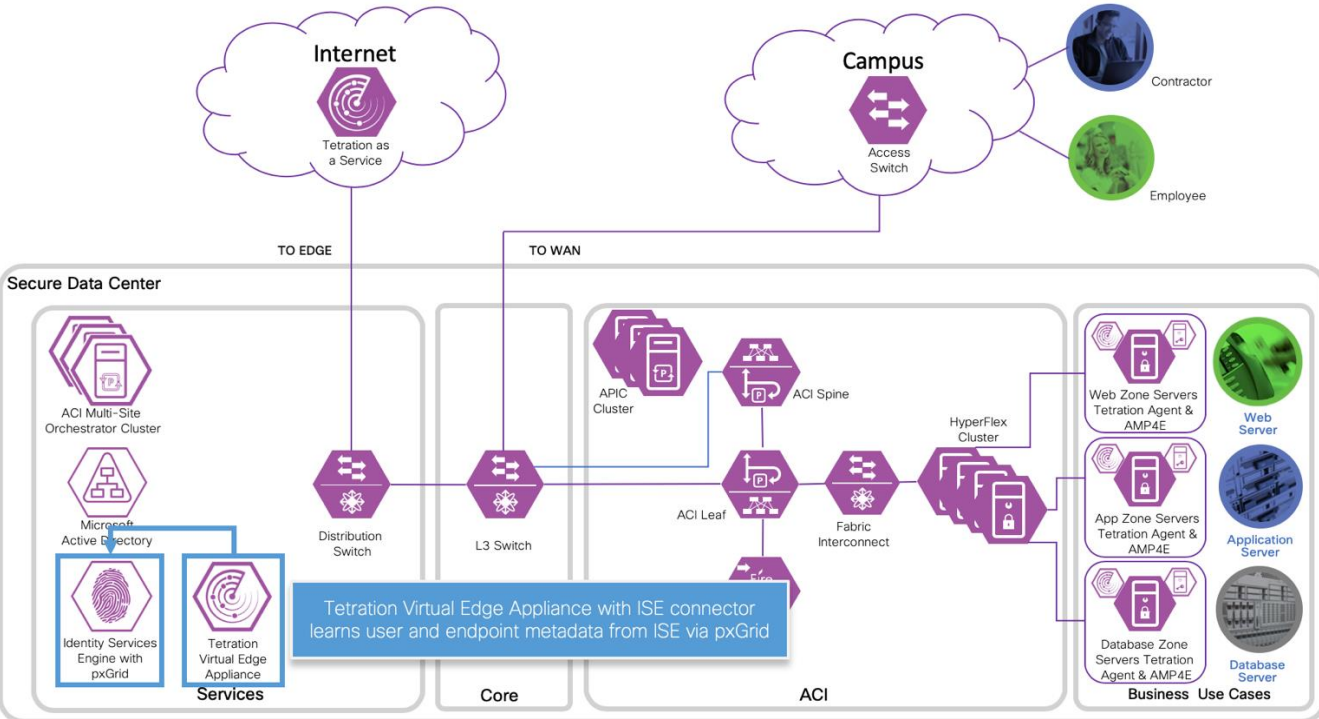


238

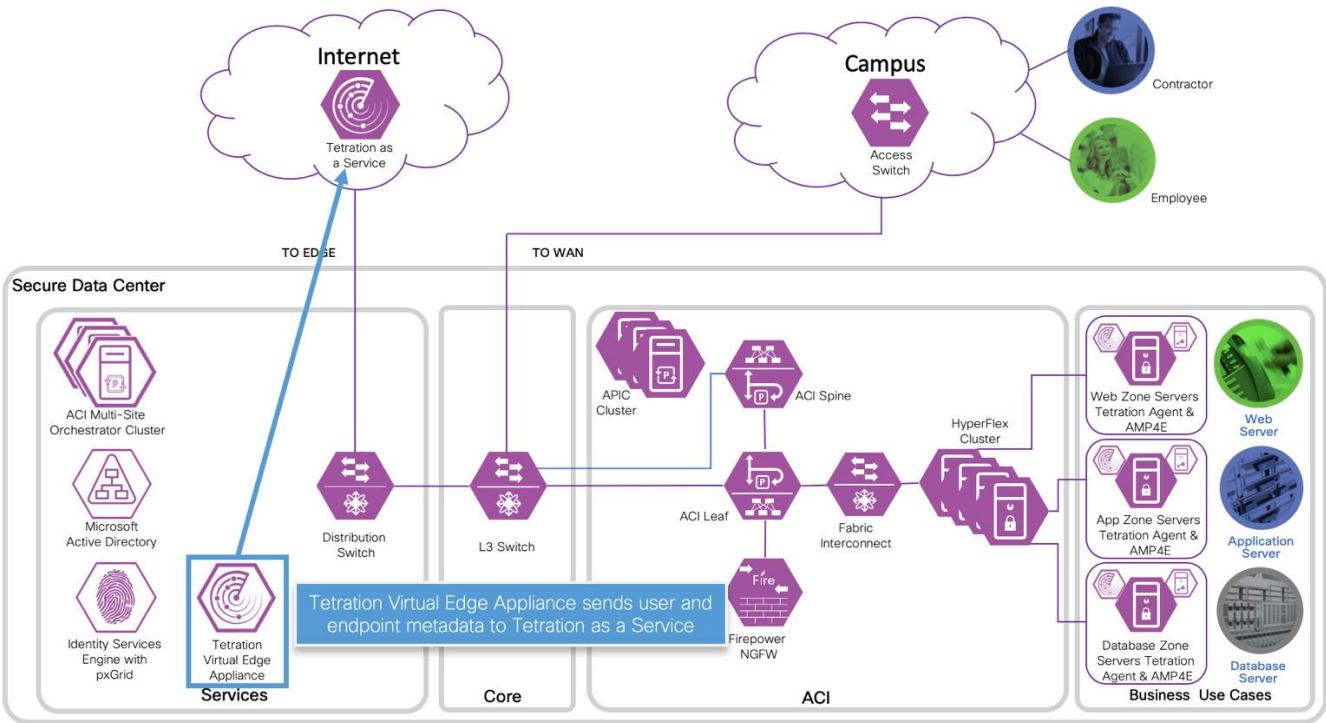
2. Endpoints are authenticated using the 802.1X protocol at the access switch or access point. ISE provides the RADIUS service for the authentication. ISE uses Directory Services to authenticate and learn endpoint and user metadata.



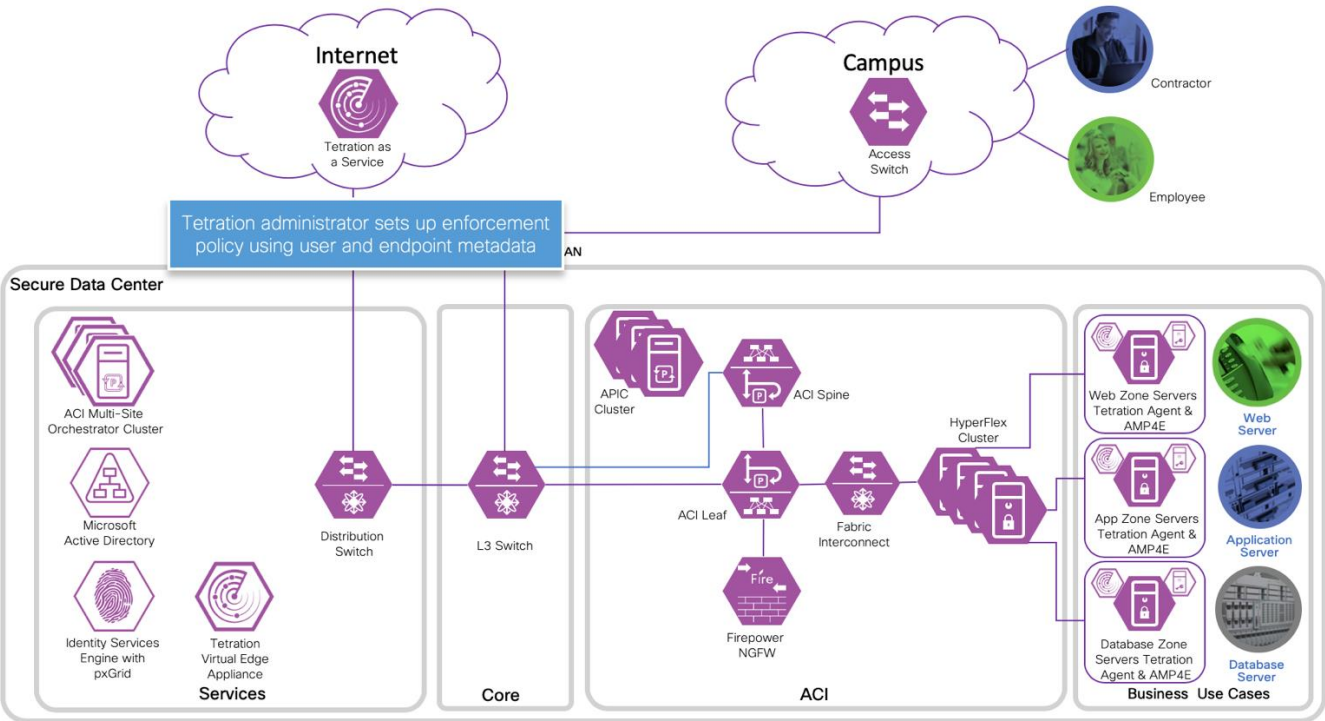
3. The Tetration Virtual Edge Appliance learns endpoint and user metadata from ISE over pxGrid.



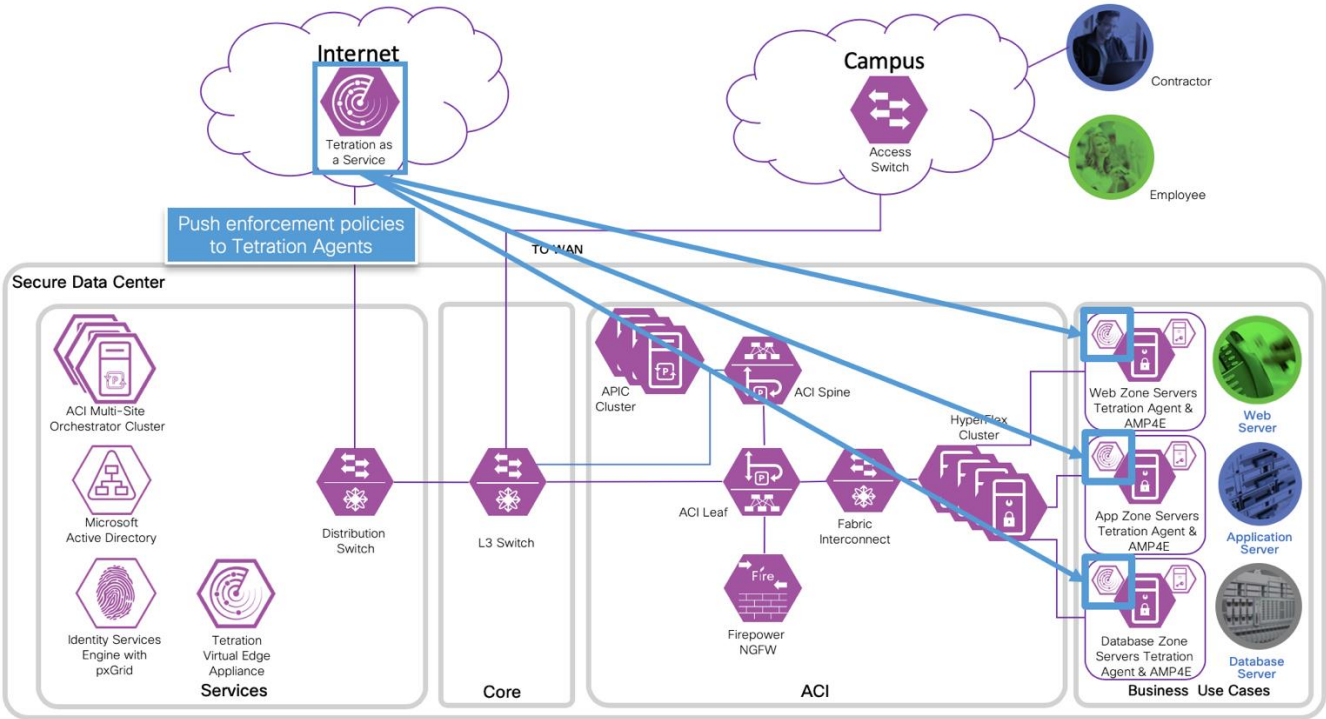
4. Tetration Virtual Edge Appliance streams the endpoint and user metadata to Tetration. The data is updated in near real time to reflect the endpoints current state.



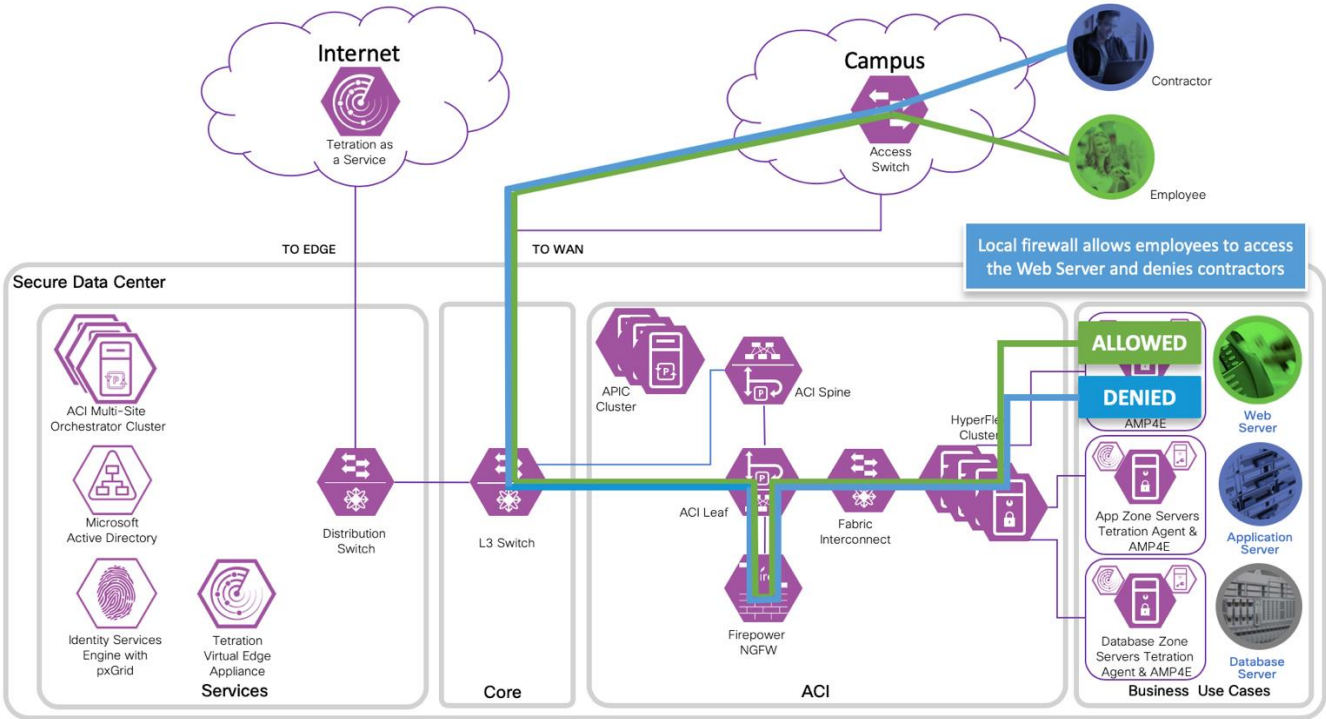
5. The Tetration administrator creates policies using Application Dependency Mapping (ADM) tool or manually. The metadata from ISE can be used as filters in Tetration policies.



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.



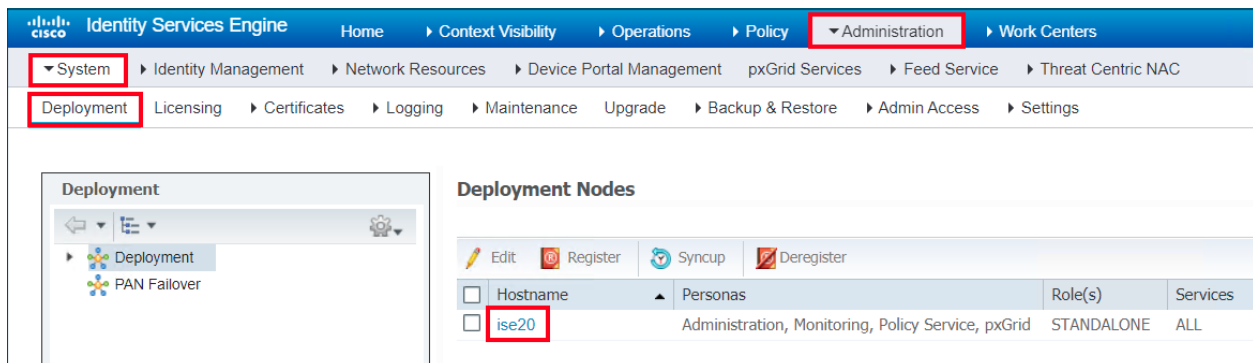
241

Procedure

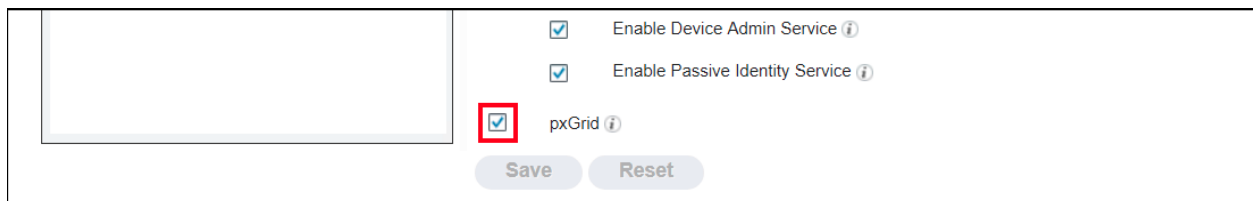
-
- Step 1 Enable ISE pxGrid
 - Step 2 Generate a pxGrid Certificate
 - Step 3 Create the Tetration Virtual Edge Appliance Configuration Bundle
 - Step 4 Deploy the Tetration Virtual Edge Appliance
 - Step 5 Configure the ISE Connector
 - Step 6 LDAP Configuration
 - Step 7 Annotation Inventory Upload
 - 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>**.

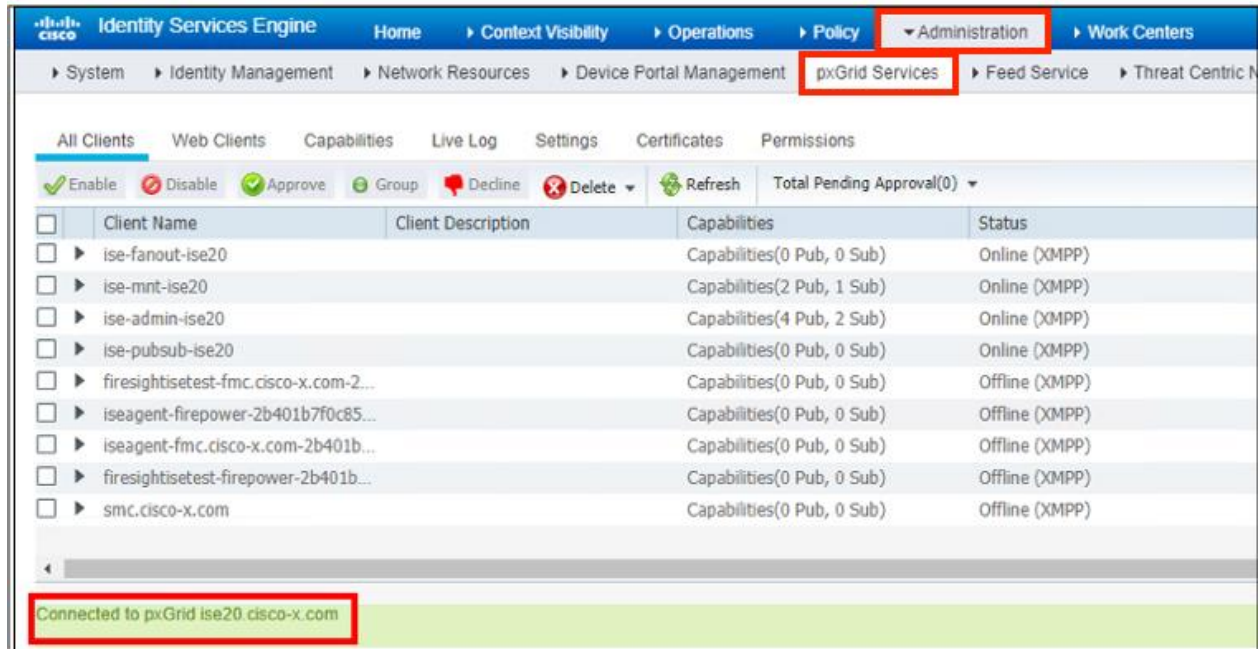


- b. At the end of the **Edit Node** page, check the box to enable pxGrid.



242

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



Step 2 Generate a pxGrid Certificate

- Navigate to the Certificates tab
- Complete the form to generate the pxGrid Certificate.
 - Use the dropdown menu in the **I want to** field and select **Generate a single certificate (without a certificate signing request)**
 - In the **Common Name (CN)** field: Type the **<FQDN>**
 - In the **Subject Alternative Name (SAN)**:
 - select **IP address**
 - Type **<ISE server IP address>**
 - Using the **Certificate Download Format** menu, select **Certificate in Privacy Enhanced Electronic Mail (PEM)**, key in PKCS8....
 - In the **Certificate Password**, field, Type **<certificate password>**
 - In the **Confirm Password** field, Type **<certificate password>**
 - Click **Create**

Identity Services Engine

HomeContext VisibilityOperationsPolicyAdministrationWork Centers

SystemIdentity ManagementNetwork ResourcesDevice Portal ManagementpxGrid ServicesFeed ServiceThreat Centric NAC

All ClientsWeb ClientsCapabilitiesLive LogSettingsCertificatesPermissions

Generate pxGrid Certificates

I want to *Generate a single certificate (without a certificate signing request)

Common Name (CN) *ise20.cisco-x.com

Description

Certificate TemplatePxGrid_Certificate_Template

Subject Alternative Name (SAN)IP address10.9.10.51

Certificate Download Format *Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)

Certificate Password *

Confirm Password *

ResetCreate

Connected to pxGrid ise20.cisco-x.com

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

Opening 1591316349799_cert.zip

You have chosen to open:

1591316349799_cert.zip

which is: Compressed (zipped) Folder

from: https://10.9.10.51

What should Firefox do with this file?

Open withWindows Explorer (default)

Save File

☐ Do this automatically for files like this from now on.

OK

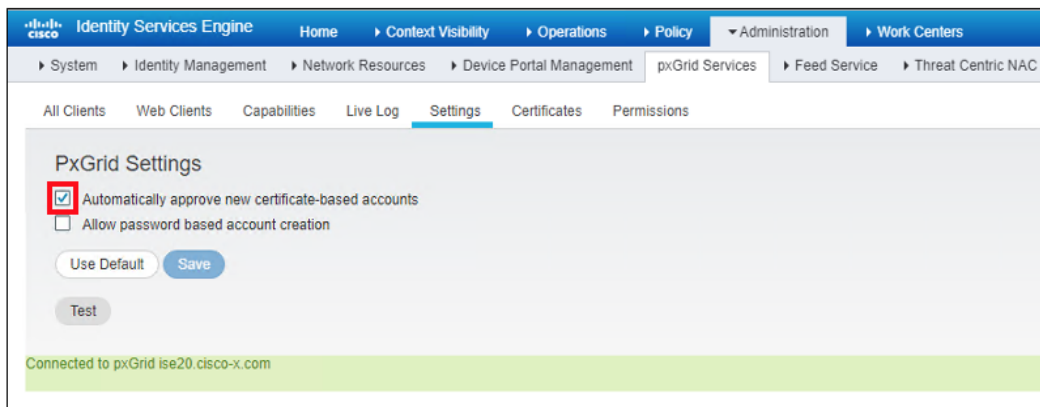
Cancel

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

Name	Date modified	Type	Size
CertificateServicesEndpointSubCA-ISE20_	12/1/2019 5:19 PM	Security Certificate	2 KB
CertificateServicesNodeCA-ISE20_	12/1/2019 5:19 PM	Security Certificate	2 KB
CertificateServicesRootCA-ISE20_	12/1/2019 5:19 PM	Security Certificate	2 KB
ise20.cisco-x.com_	12/1/2019 5:19 PM	Security Certificate	2 KB
ise20.cisco-x.com_10.9.10.51	12/1/2019 5:19 PM	Security Certificate	2 KB
ise20.cisco-x.com_10.9.10.51.key	12/1/2019 5:19 PM	KEY File	2 KB

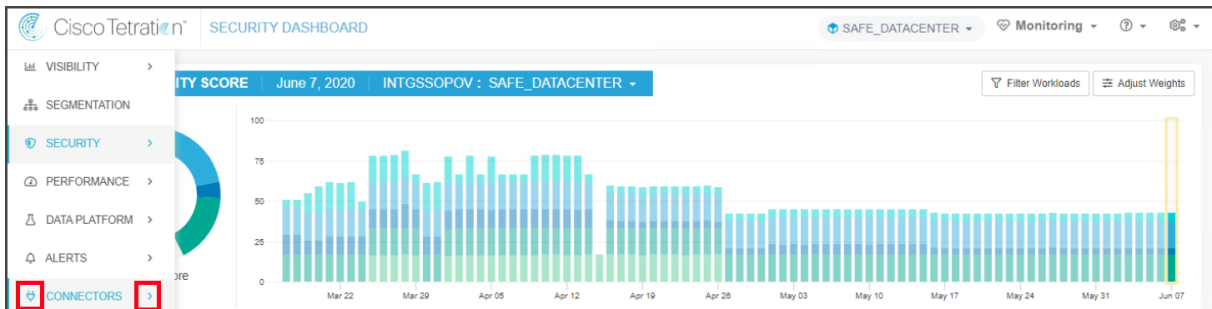
244

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

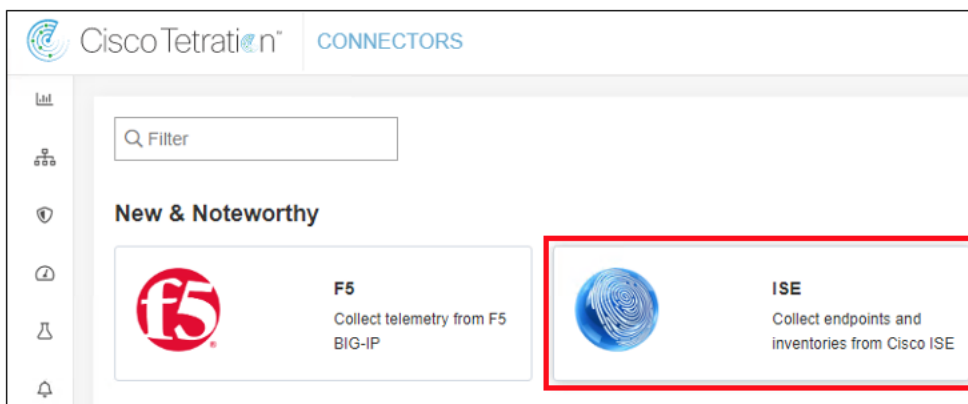


Step 3 Create the Tetration Virtual Edge Appliance Configuration Bundle

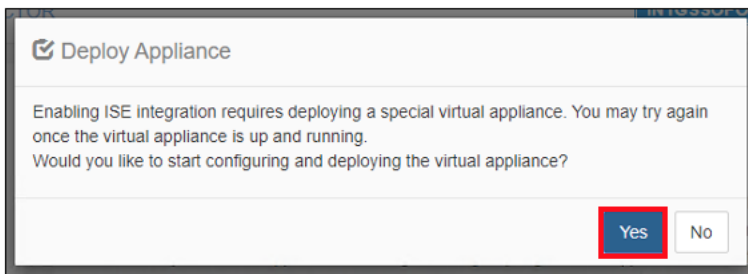
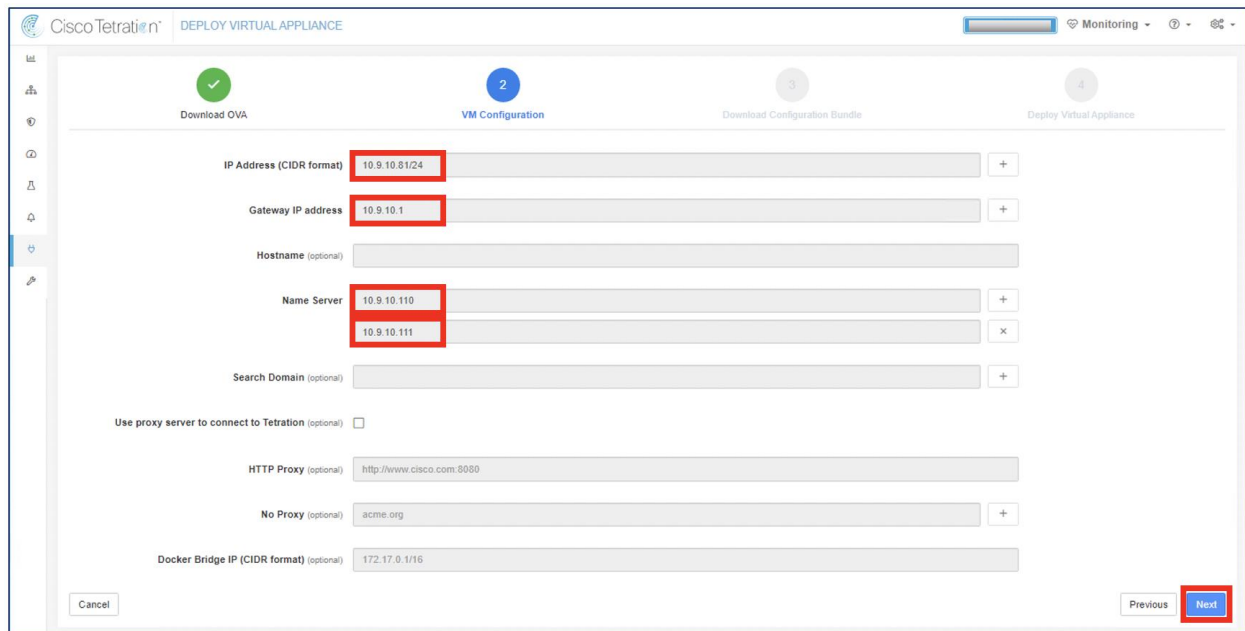
- a. From the Tetration Management portal, hover over the **Connectors** icon to expand the menu. Select **Connectors**.



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

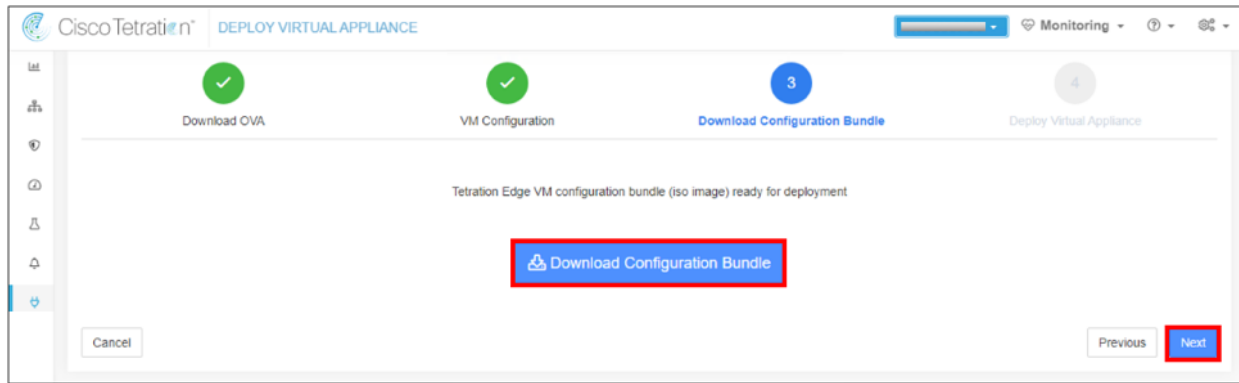


245

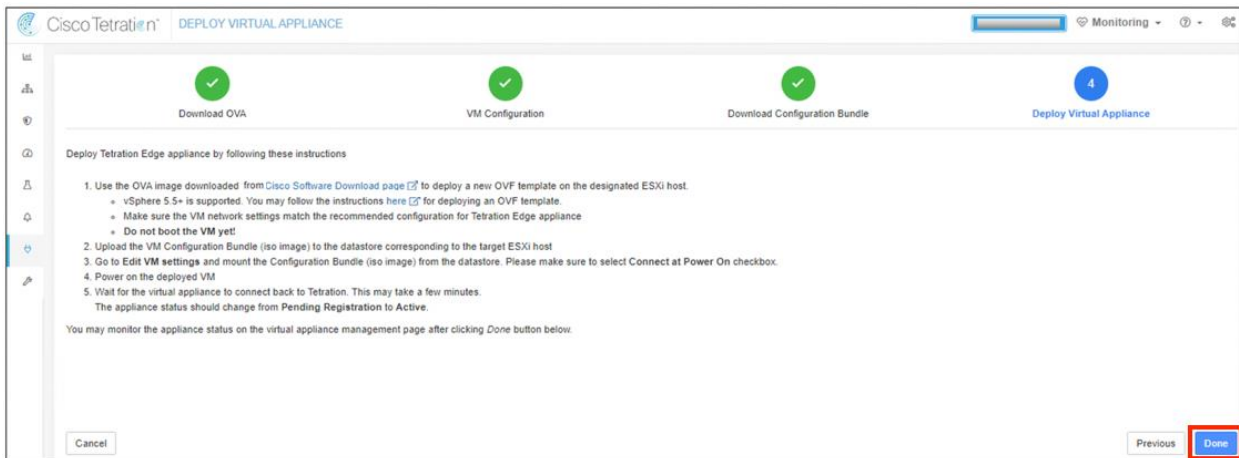
c. Click **Enable**.d. Click **Yes** to start the Configuration Bundle setup.e. Enter the appliance IP information and click **Next**.

246

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

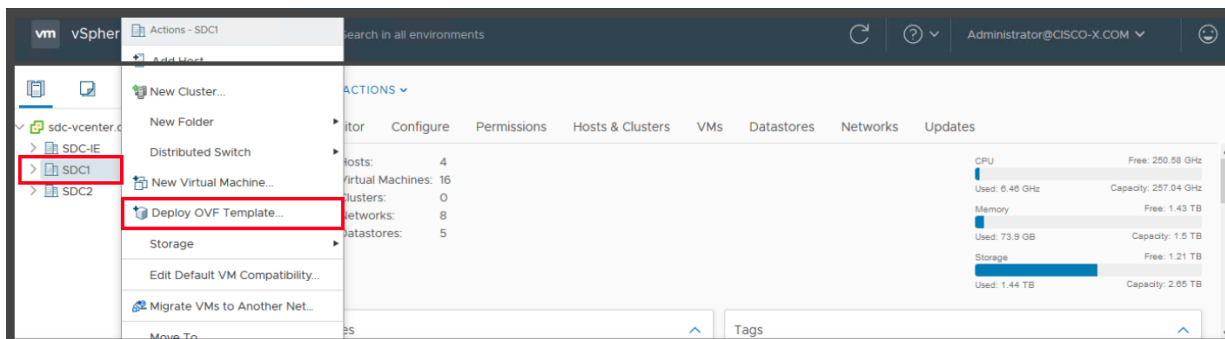


- g. This page provides an overview of the deployment steps. Review and click **Done**.



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**.



247

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

Processor Type: Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

http | <https://remoteserver-address/filetoinstall.ovf> | .ova

☒ Local file

Choose Files tetration-edge-3.3.2.2.ova

CANCEL BACK **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**.

Processor Type: Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: **tetration-edge**

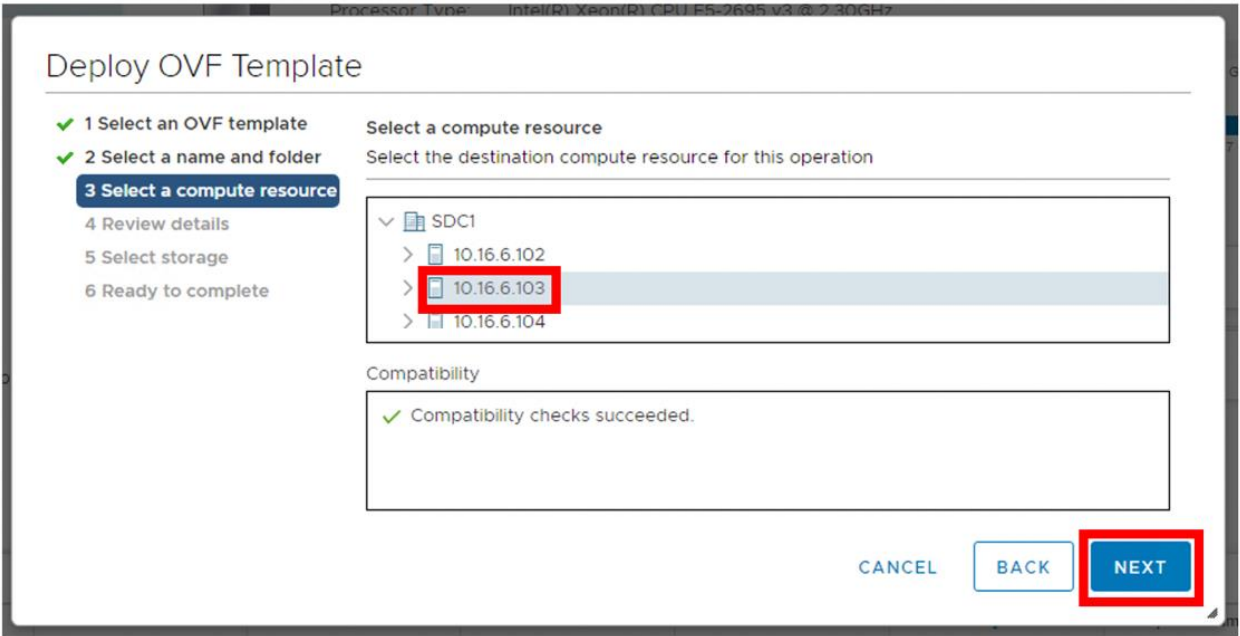
Select a location for the virtual machine.

- ✓ sdc-vcenter.cisco-x.com
 - > **SDC1**
 - > SDC2

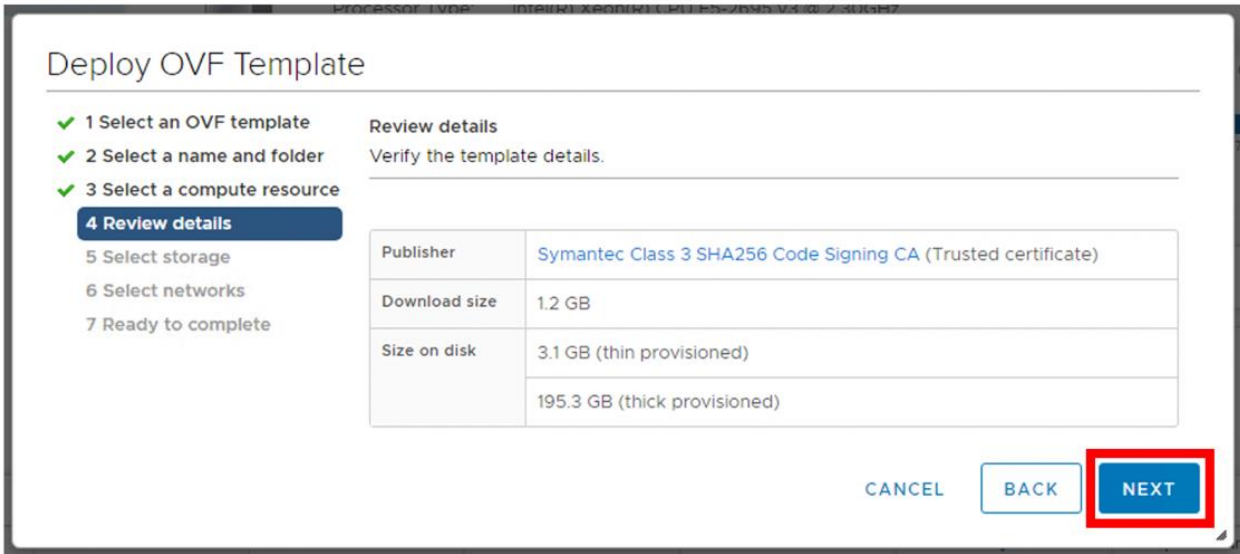
CANCEL BACK **NEXT**

248

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**.

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format:

Thick Provision Lazy Zeroed

VM Storage Policy:

Datastore Default

Name	Capacity	Provisioned	Free	Type
ESXi-3-DataStore1	446 GB	53.36 GB	402.25 GB	VMFS

Compatibility

✓

 Compatibility checks succeeded.

CANCEL

BACK

NEXT

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

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network-10

IP Allocation Settings

IP allocation:

Static - Manual

IP protocol:

IPv4

CANCEL

BACK

NEXT

250

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

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

✓ 5 Select storage

✓ 6 Select networks

7 Ready to complete

Ready to complete

Click Finish to start creation.

Provisioning type	Deploy from template
Name	tetration-edge-1
Template name	Toolbox_Licenses_VA_13.1
Download size	1.1 GB
Size on disk	8.0 GB
Folder	SDC1
Resource	10.16.6.103
Storage mapping	1
All disks	Datastore: ESXi-3-DataStore1; Format: Thick provision lazy zeroed
Network mapping	1
VLAN 3079	VM Network 10
IP allocation settings	
IP protocol	IPv4

CANCEL

BACK

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**.

vm vSphere Client

Menu

Search in all environments

Administrator@CISCO-X.COM

ESXi-3-DataStore1

ACTIONS

Summary

Monitor

Configure

Permissions

Files

Hosts

VMs

Search

New Folder

Upload Files

Upload Folder

Register VM...

Download

Copy to

Move to

Name	Size	Modi...	Type	Path
appli...	10,668 ...	12/28/...	ISO Im...	[ESXi-3-...

ESXi-3-DataStore1

.dvsData

locker

.naa.618e7283727a4b5022b418051e45400e

.sdd.sf

db-tb-win

Tetration Edge - VM Config bundle

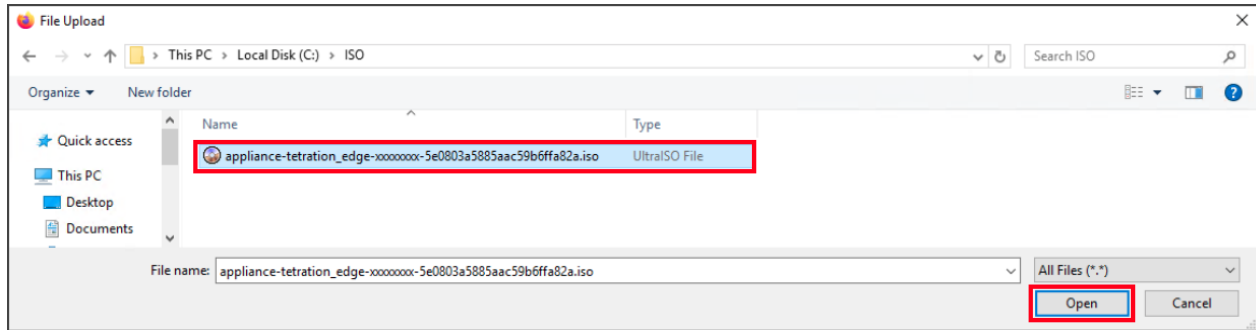
tetration-edge

tmp

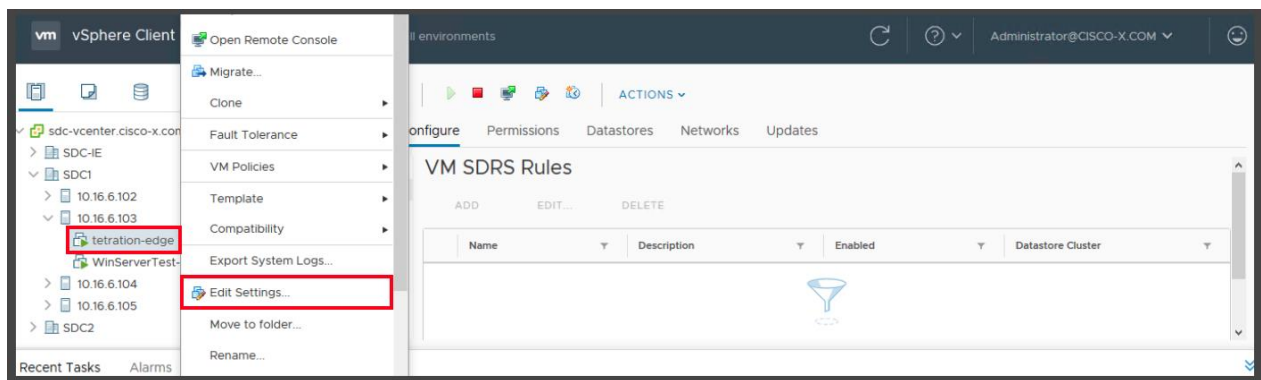
vmkdump

251

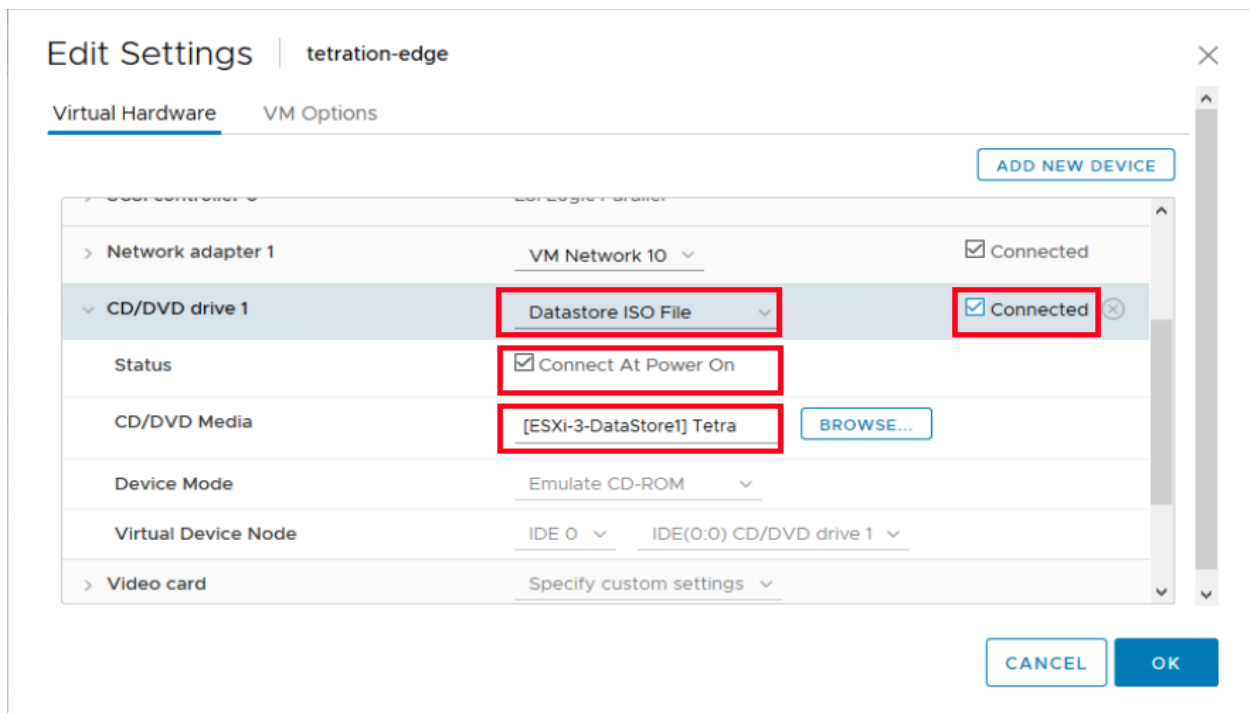
- j. In the pop-up windows, select the Configuration Bundle ISO file and click **Open**.



- 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**.



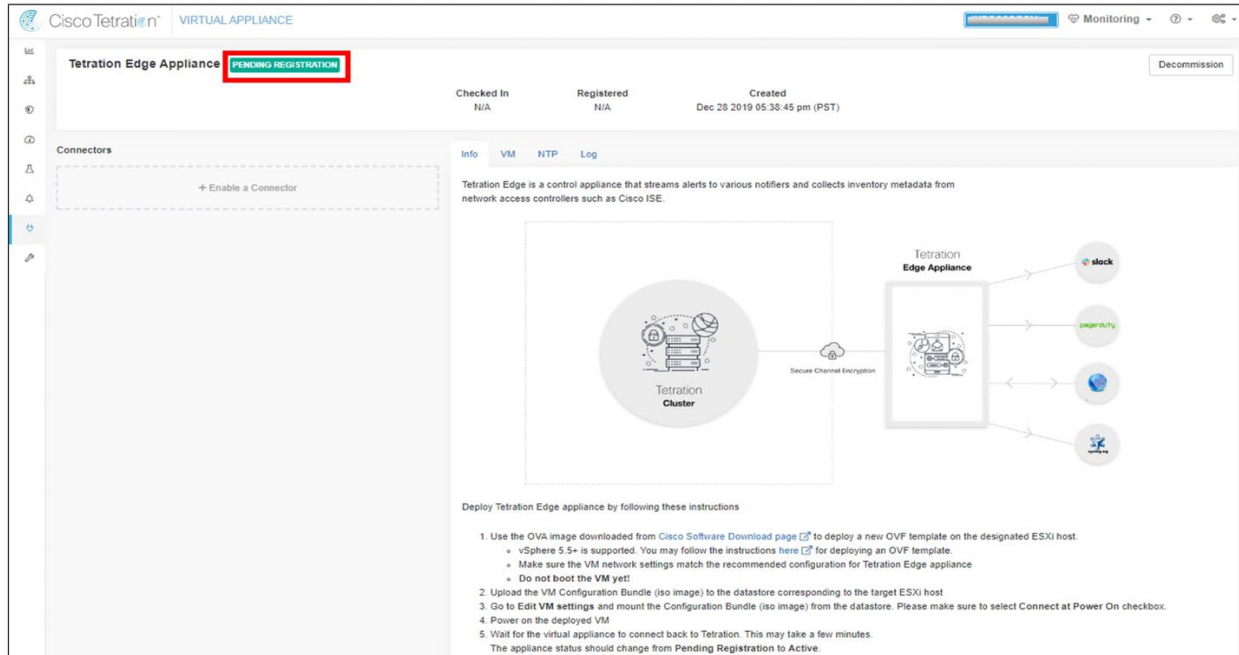
- l. Use the dropdown menu in the CD/DVD drive 1 field, select the **Datastore ISO File** and check **Connected** box. In the Status field, check the **Connected At Power On** box. In the CD/DVD field, click **BROWSE** and select the Configuration Bundle ISO (**appliance-tetration_edge-<unique string>.iso**)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



252

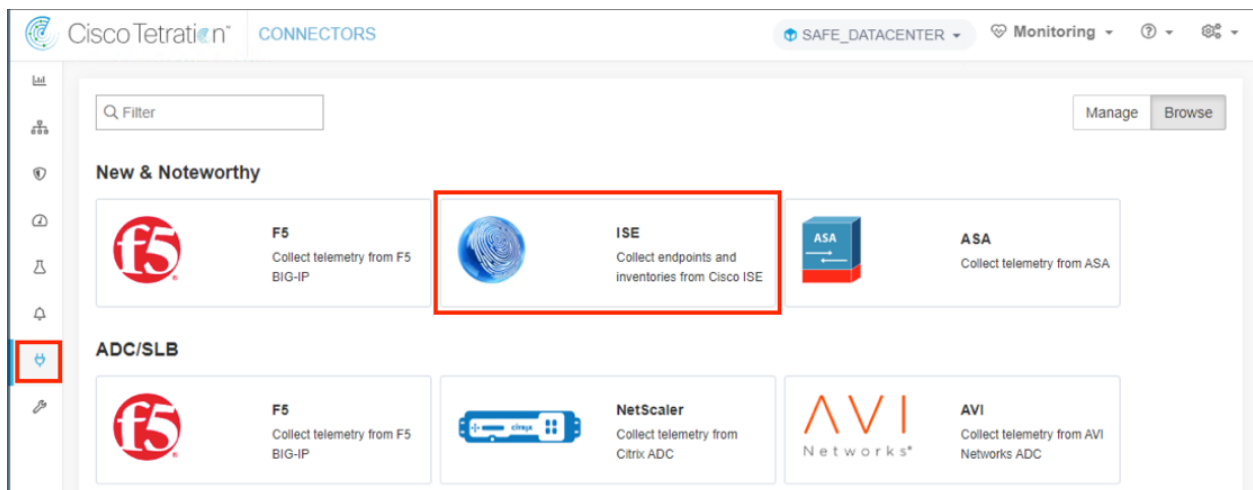
m. In the vCenter, power on the virtual machine.

Note: The Tetration Virtual Edge appliance will self-configure and self-register 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.



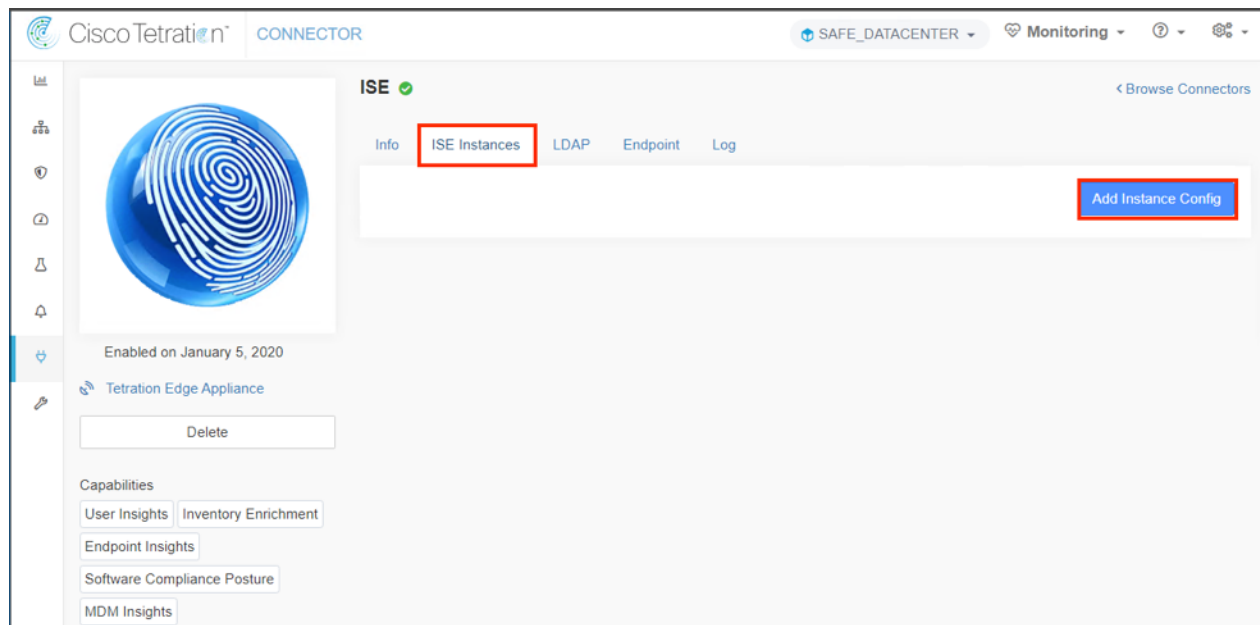
Step 5 Configure the ISE Connector

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



253

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



254

- 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.

The screenshot displays the Cisco Tetration CONNECTOR web interface. On the left, a sidebar shows the 'Tetration Edge Appliance' status as 'Enabled on January 5, 2020' with a 'Delete' button. Below this, 'Capabilities' include 'User Insights', 'Inventory Enrichment', 'Endpoint Insights', 'Software Compliance Posture', and 'MDM Insights'. The main panel is titled 'ISE' and contains tabs for 'Info', 'ISE Instances', 'LDAP', 'Endpoint', and 'Log'. An 'Add Instance Config' button is in the top right. The 'New ISE instance' form has the following fields, each with a red border and red text instructions:

- Name:** tet-edge-ise1
- ISE Client Certificate:** Enter Client Certificate. Copy and paste the content of the Client Certificate.
- ISE Client Key:** Enter Client Key. Copy and paste the content of the Client Key.
- ISE Server CA Certificate:** Enter Server CA Certificate. Copy and paste the content of the CA Key.
- ISE Hostname:** ise20.cisco-x.com
- ISE Node Name:** ise20.cisco-x.com

At the bottom of the form are 'Cancel Config Creation' and 'Verify & Save Configs' buttons.

255

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**

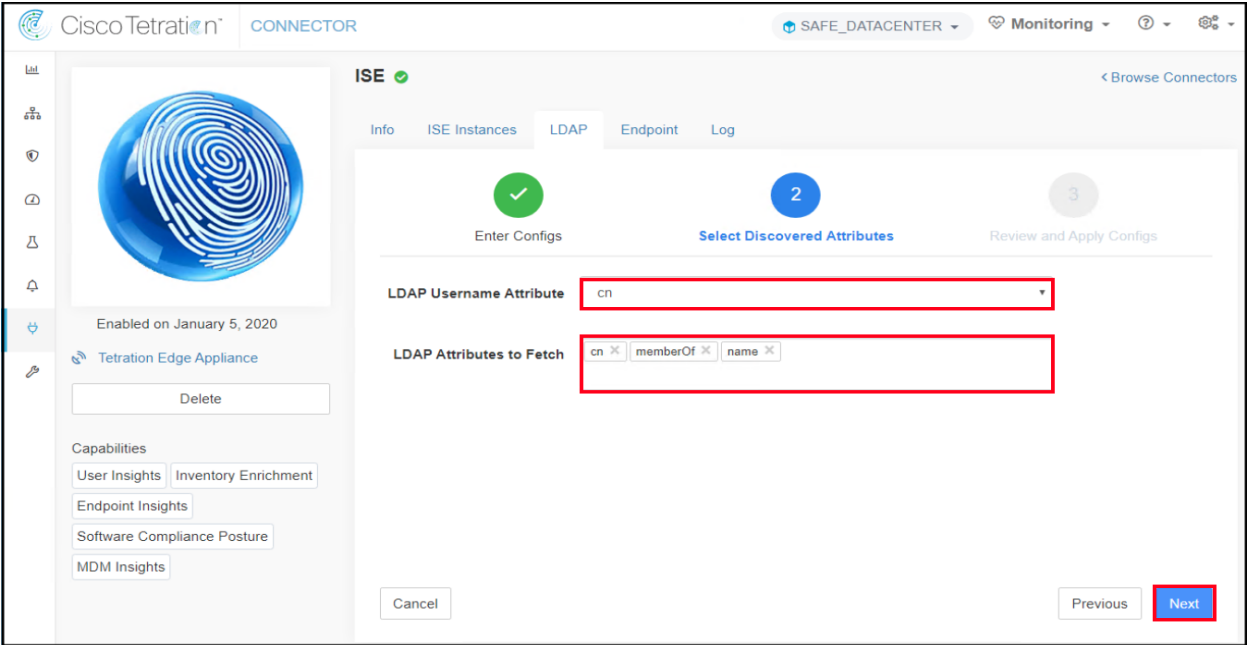
The screenshot displays the Cisco Tetration CONNECTOR interface for configuring an ISE connector. The 'LDAP' tab is selected under the 'ISE' section. The configuration process is divided into three steps: 1. Enter Configs, 2. Select Discovered Attributes, and 3. Review and Apply Configs. The 'Enter Configs' step is currently active. The configuration fields are as follows:

- LDAP Username:** Masked with asterisks. A 'Change LDAP Username' link is present.
- LDAP Password:** Masked with asterisks.
- LDAP Server:** ad2.cisco-x.com
- LDAP Port:** 389
- Use SSL:** ☐
- Verify SSL:** ☐
- LDAP Server CA Cert:** (optional)
- LDAP Server Name:** Enter LDAP Server Name (optional)
- LDAP Base DN:** cn=users,dc=cisco-x,dc=com
- LDAP Filter String:** (&(objectClass=user))
- Snapshot Sync Interval (in hours):** 24 (optional)
- Use Proxy to reach LDAP:** ☐
- Proxy Server to reach LDAP:** http://1.1.1.1:8080 (optional)

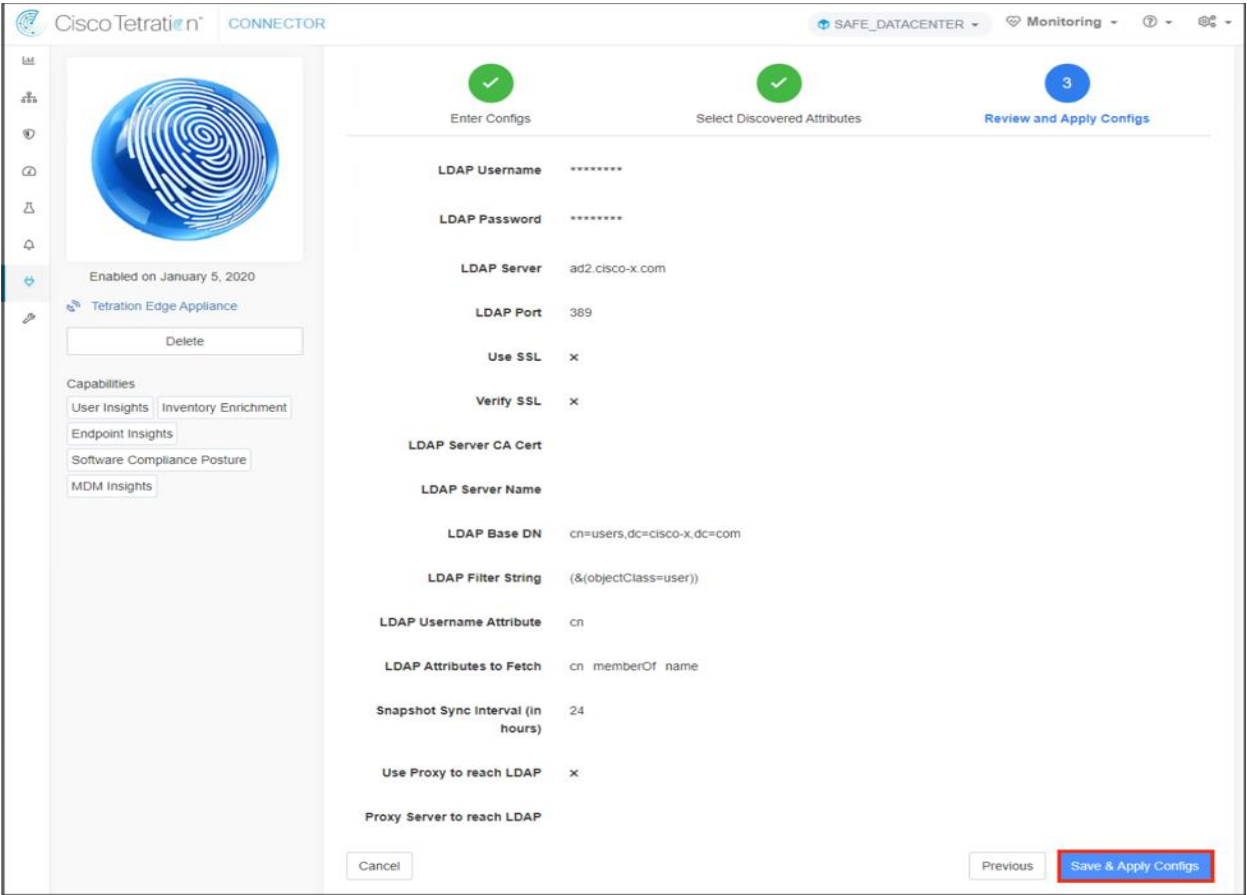
A 'Next' button is located at the bottom right of the configuration area, highlighted with a red box.

256

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.

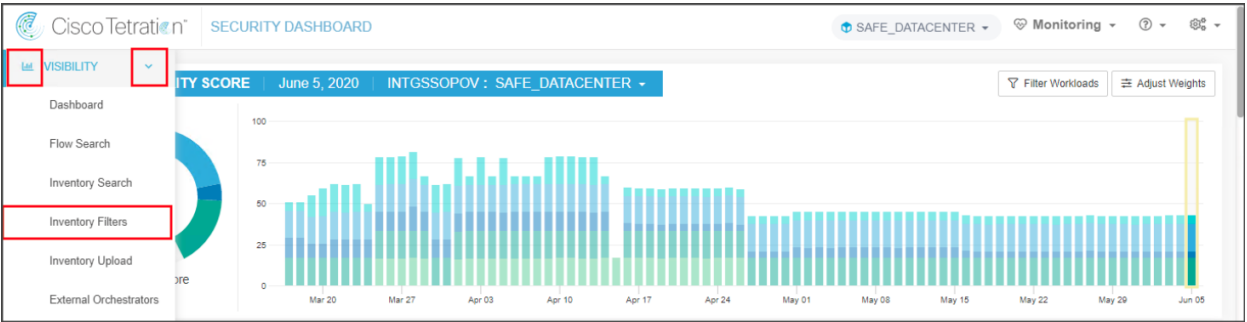
Spreadsheet Application

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

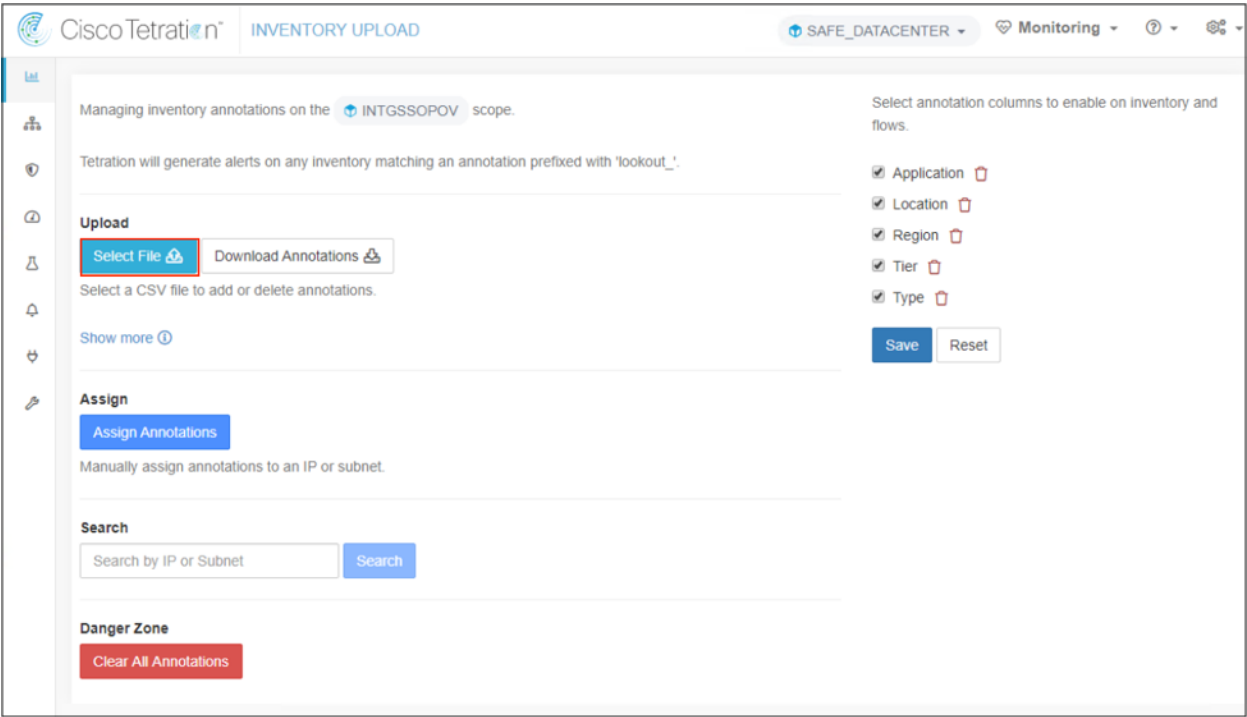
```
IP,Application,Location,Region,Tier,Type
10.18.107.0/24,WordPress,,Web,DataCenter
10.18.108.0/24,WordPress,,Application,DataCenter
10.18.109.0/24,WordPress,,Database,DataCenter
10.9.110.0/24,,,Users,Campus
```

- 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**.



258

- 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

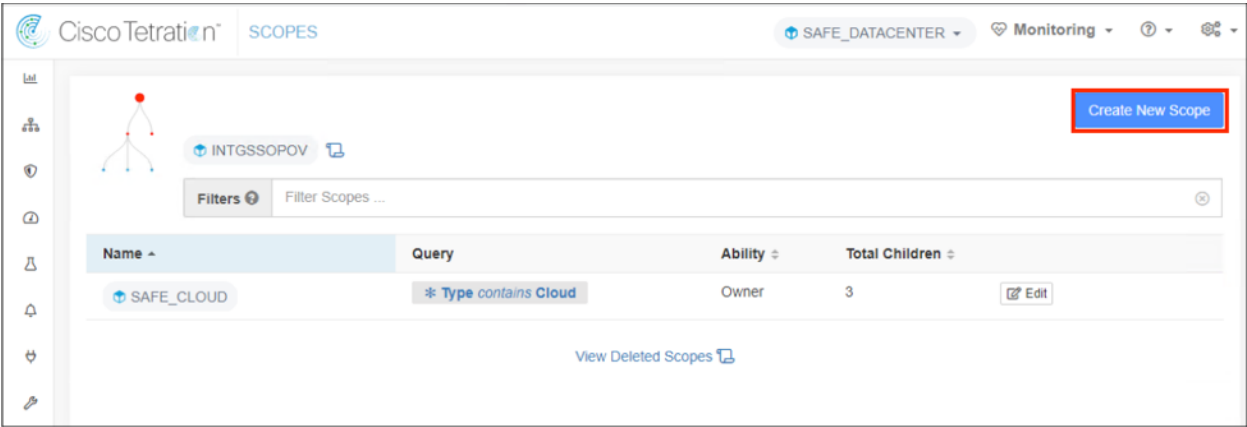
Step 8 Create Scope

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



259

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**

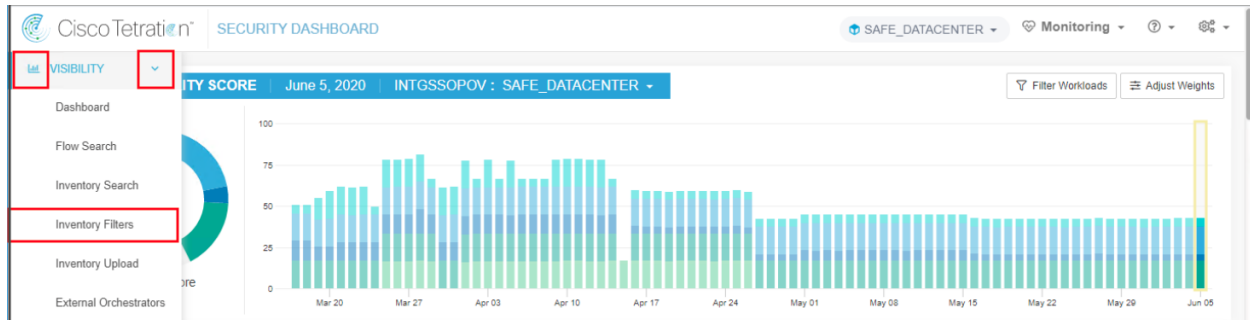
A screenshot of the 'Scope Details' form. The form has a 'Cancel' button in the top right. The fields are: 'Name' (containing 'SAFE_DATACENTER'), 'Description' (with placeholder text 'Enter a description (optional)'), 'Policy Priority' (a dropdown menu set to 'Natural'), 'Parent Scope' (a dropdown menu set to 'INTGSSOPOV'), 'Sub-Type' (a dropdown menu set to 'No selection'), and 'Query' (containing '* Type = Datacenter'). A 'Create' button is at the bottom left. A red box highlights the 'Name' field, and another red box highlights the 'Query' field.

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

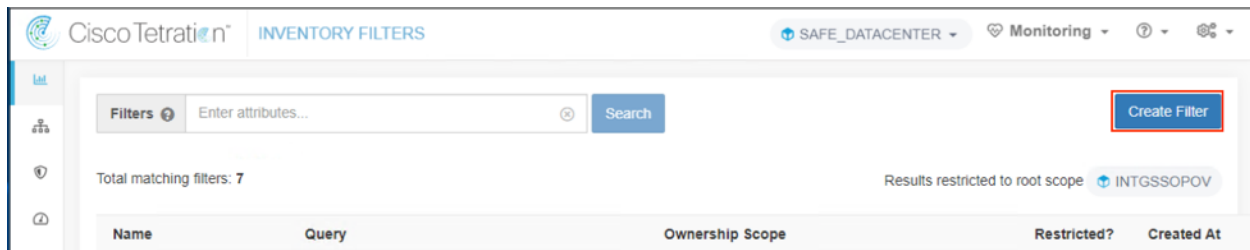
260

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.

261

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

Create an Inventory Filter

Define 2 Summary

Name: Employees

Scope: + INTGSSOPOV

Query: * ISE_ctsSecurityGroup = EmployeesSGT

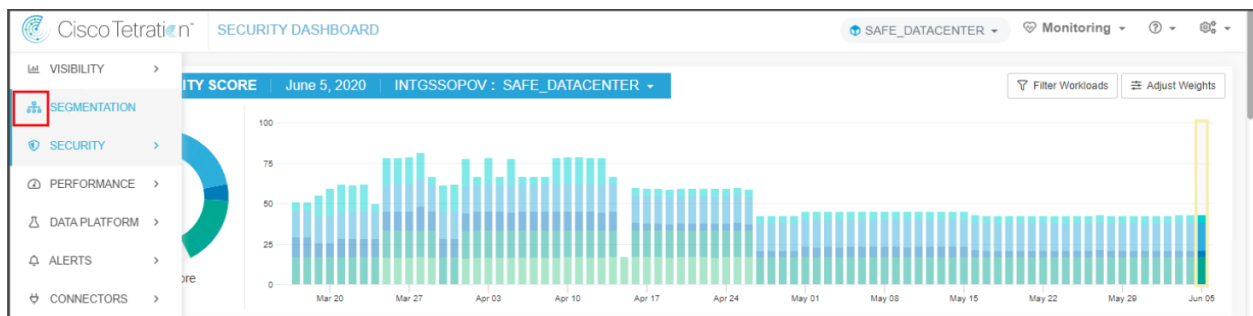
Inventory item preview: Showing 2 of 2 total.

Hostname	IP Address	OS
host-10.9.110.101	10.9.110.101	Belkin Device
host-10.9.110.103	10.9.110.103	Belkin Device

Cancel Previous **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**.

Cisco Tetration[™] SEGMENTATION

INTGSSOPOV Monitoring ?

SEGMENTATION Overview

1 Enforced Applications 40 Enforcement Agents 6 / 40 Desired Agent Policies

Workspaces Analyzed Policies Enforced Policies Policy Requests

3 Workspaces Filter application workspaces Sort **Create New Workspace**

AWS-Safe3TierApp INTGSSOPOV : SAFE_CLOUD : AWS-US-EAST PRIMARY ANALYZED
230 Conversations 5 Clusters 26 Policies Last updated: Mar 29, 2:17 PM

Azure-Safe3TierApp INTGSSOPOV : SAFE_CLOUD : AZURE PRIMARY
- Conversations 0 Clusters 1 Policy Last updated: Mar 29, 2:17 PM

Get Started

- Create Filter
- Add Policy
- Start Analysis
- Enable Enforcement

Tools

- Enforcement History
- Default ADM Run Config

262

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

Create a New Application Workspace

Name: WordPress3TierApp

Description: Enter a description (optional)

Scope: SAFE_DATACENTER

Create Cancel

- 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.

Cisco Tetragon SEGMENTATION

WordPress3TierApp SECONDARY

INTGSSOPOV: SAFE_DATACENTER DYNAMIC Version: v6

Conversations Clusters 1 Policies 1 App View 0

Clusters

Filters Filter Clusters ...

Displaying 1 of 1 clusters

Cluster	Workloads	Confidence	Dynamic	Approved
user-defined-cluster		N/A		

Create Cluster

Cluster: WordPress Web

Cluster Actions

Name: WordPress Web

Description

View Cluster Details

Edit Cluster Query

Workloads (0)

Provides (0)

Consumes (0)

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

Edit Cluster

Name: WordPress Web

Description: Enter a description (optional)

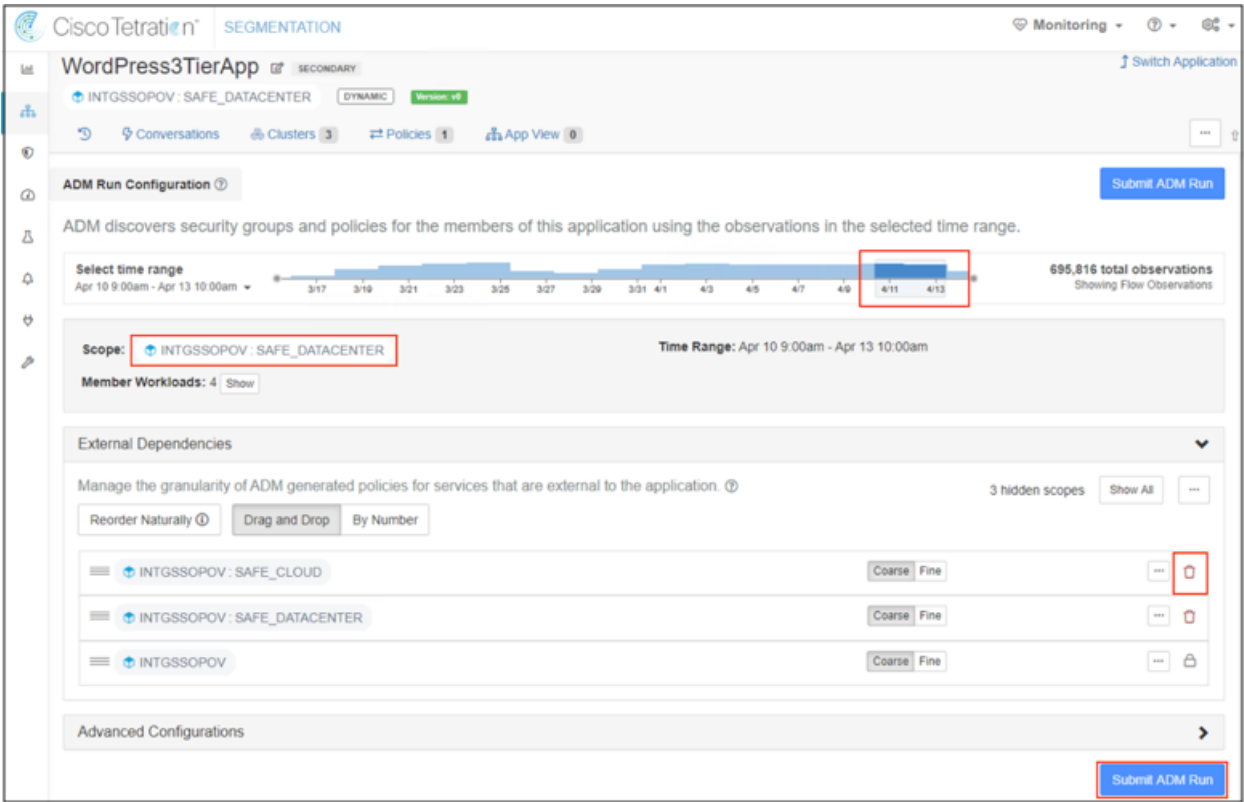
Query: * Type = Web

Save Cancel

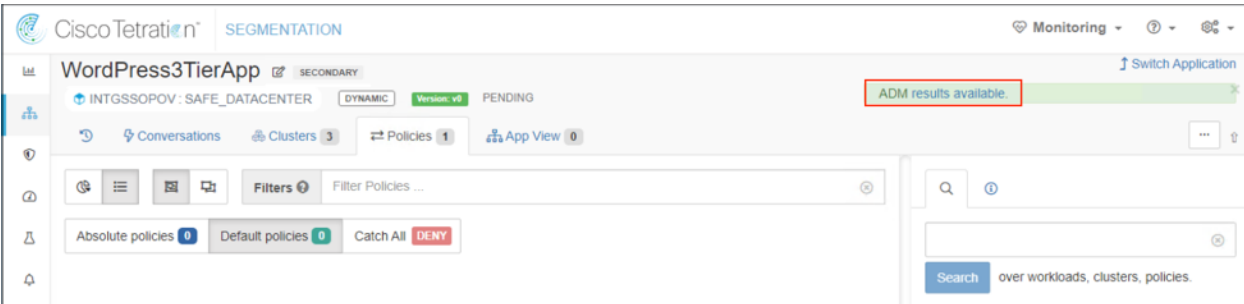
- f. Repeat these steps to create the additional clusters, Application and DB. When all clusters have been defined, click **Start ADM Run** (6).

263

- 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.

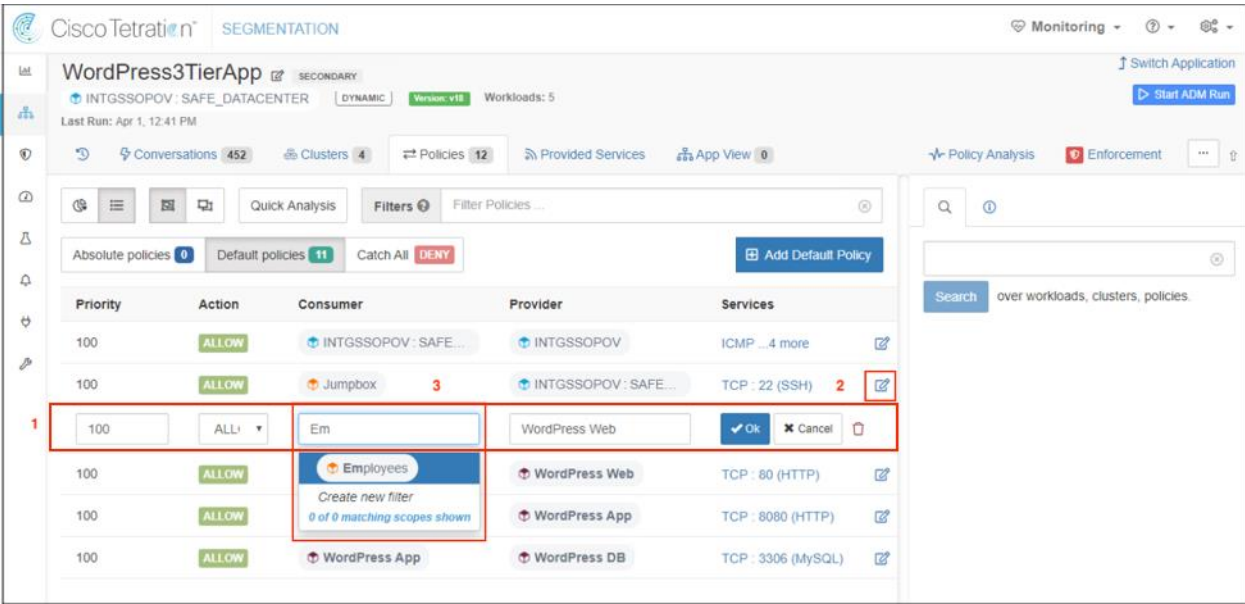


- h. When the ADM Run completes, the message **ADM RESULTS AVAILABLE** is display. Click it to view the policies created by ADM.



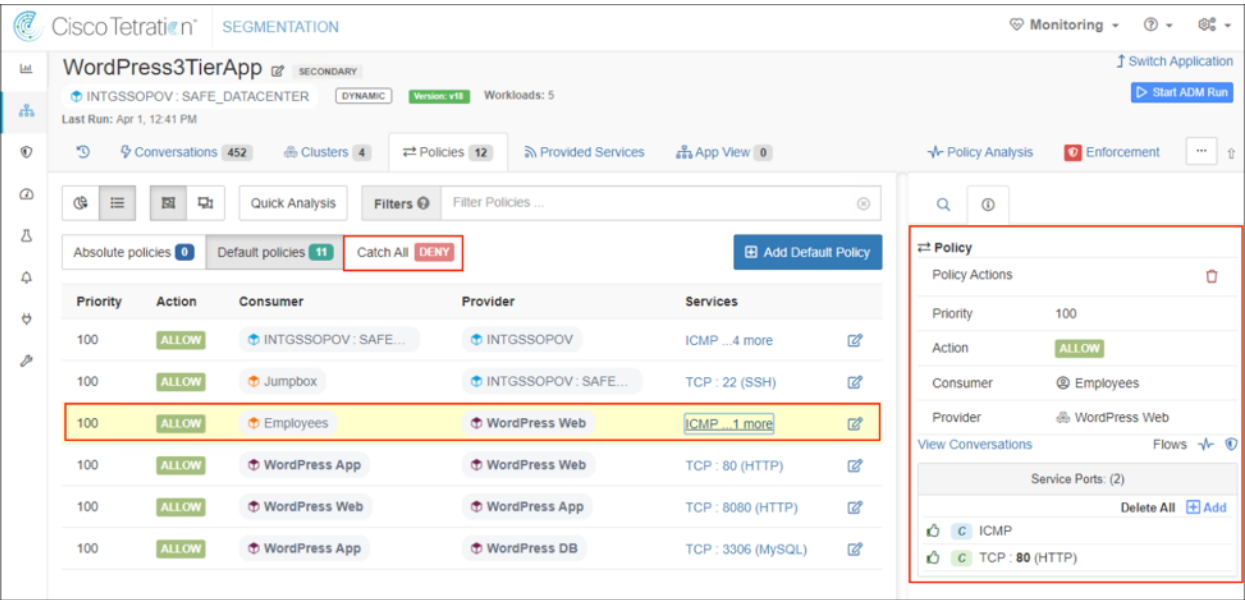
264

- 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.

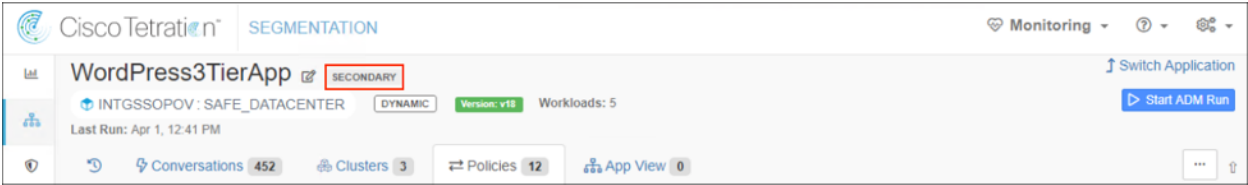
In this test case, users in the Employees group are ALLOW to access the web server and users in the Contractors group are DENY by the Catch All DENY policy.



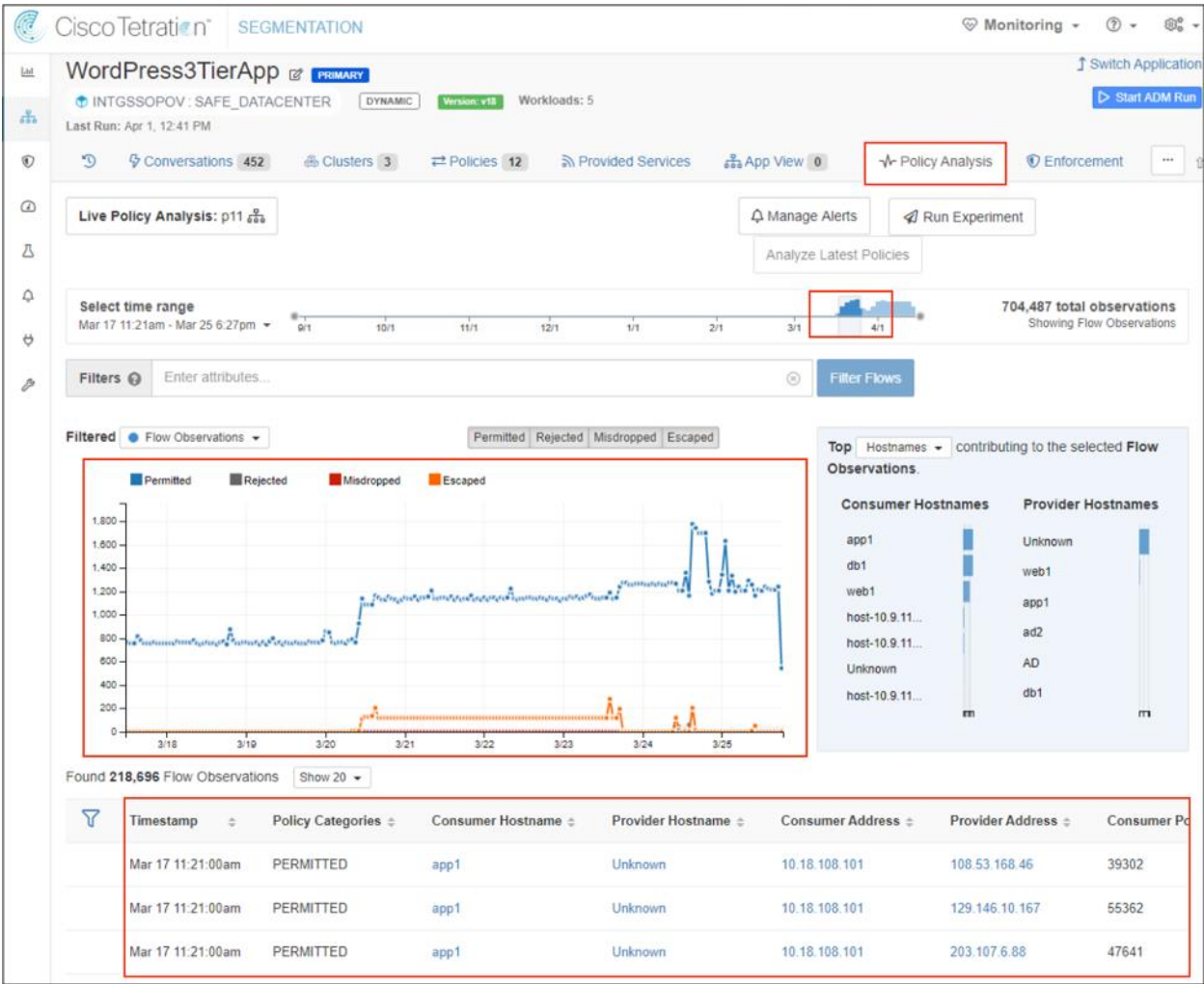
265

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.

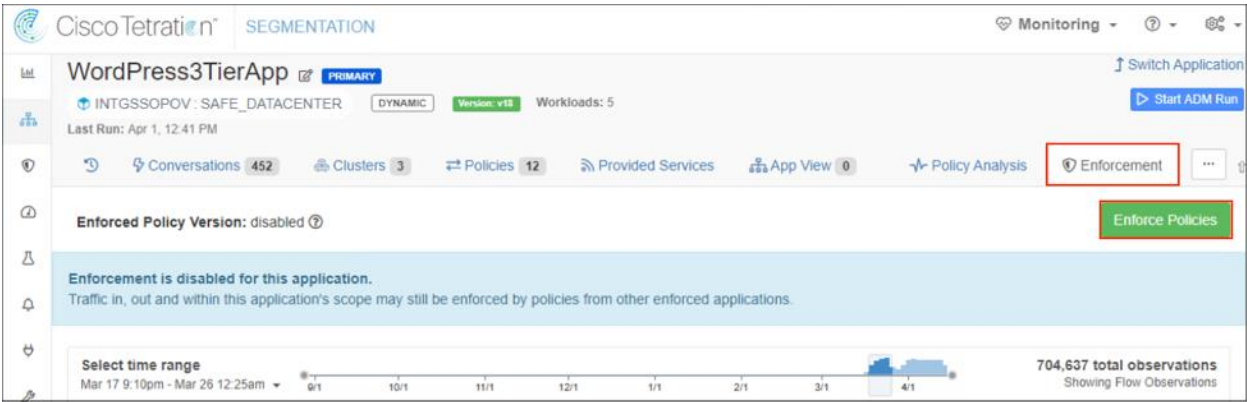


- c. Click Policy Analysis tab and select a Time Range to apply the policies. The results are displayed below.



266

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**.

Enforce Policies

Select the version of policies to enforce.

Version

Reason for action

New host firewall rules will be inserted and any existing rules will be deleted on the relevant hosts. Please click accept to continue.

Accept and Enforce

Cancel

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).

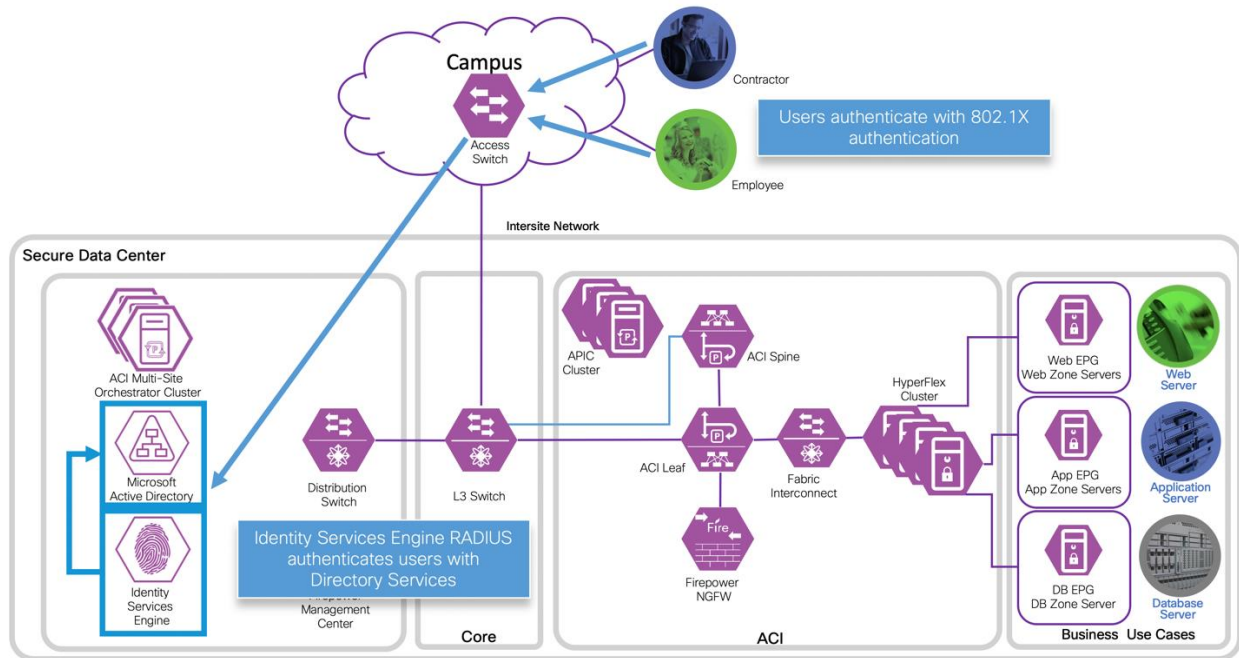
Devices not capable of Cisco TrustSec can subscribe to Cisco Platform Exchange (pxGrid) to propagate SGTs. pxGrid is an open and scalable Security Product Integration Framework (SPIF) that enables ecosystem partners to exchange contextual information unidirectionally or bidirectionally. Cisco pxGrid 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 Threat 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.

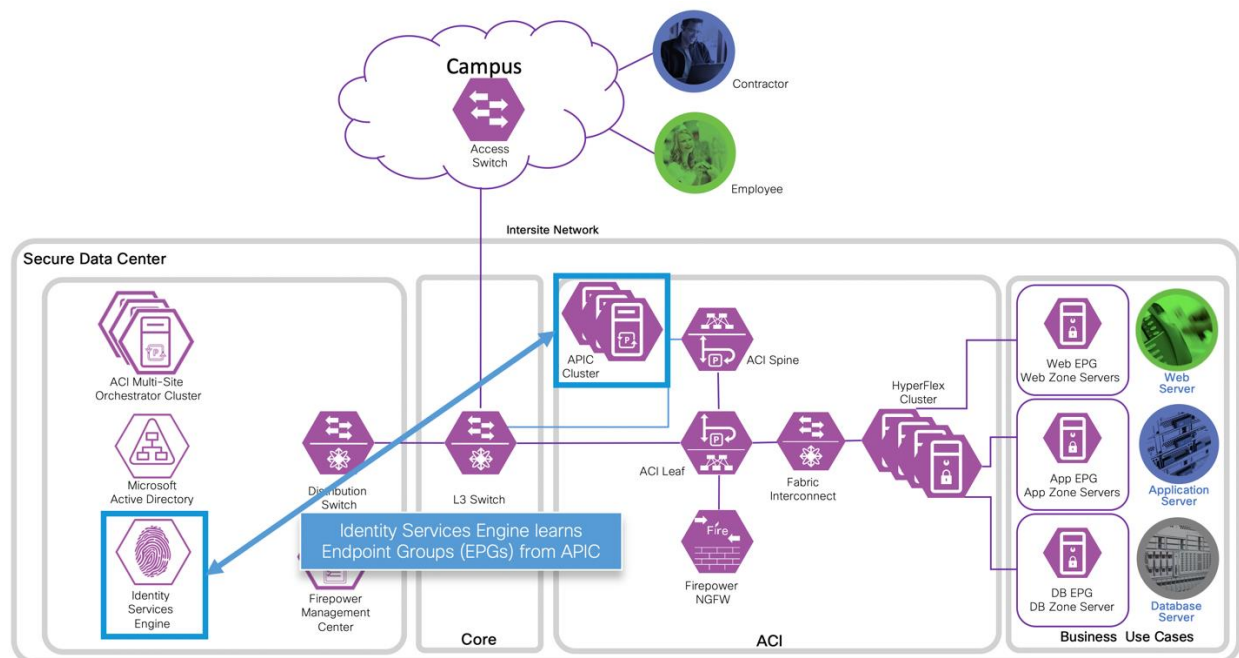
268

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.

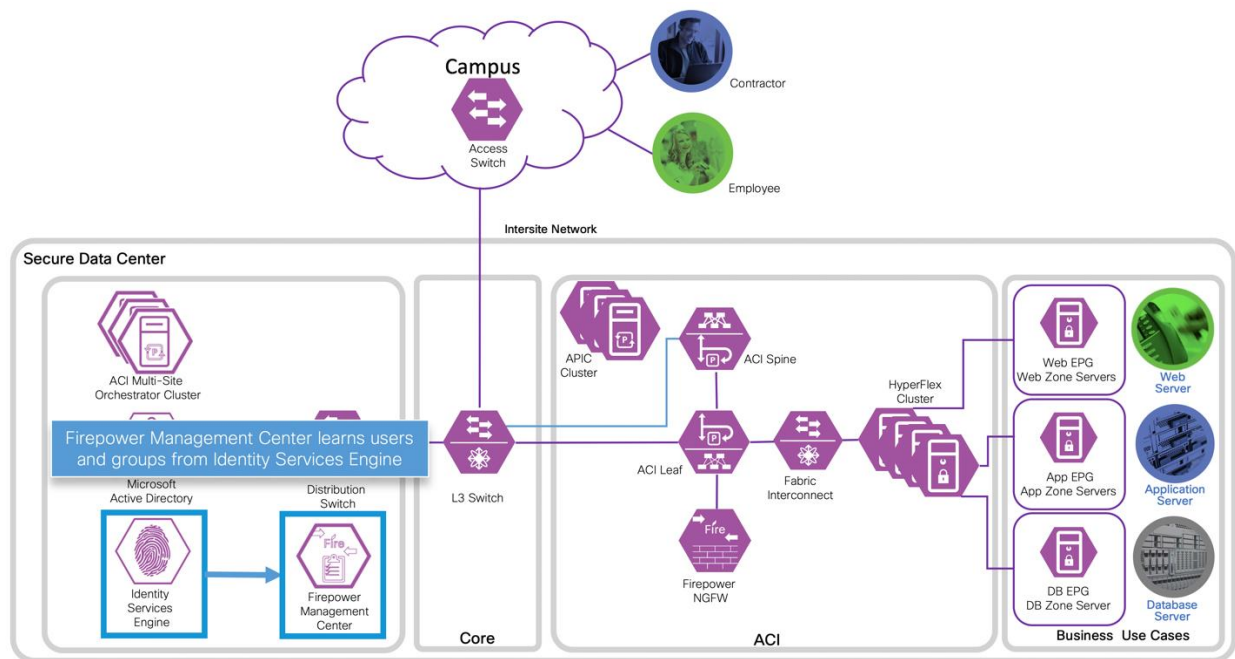


2. ISE and ACI are integrated and exchange SGTs and EPGs. ISE creates a corresponding SGT for each EPG. ACI also creates a corresponding EPG for each SGT.

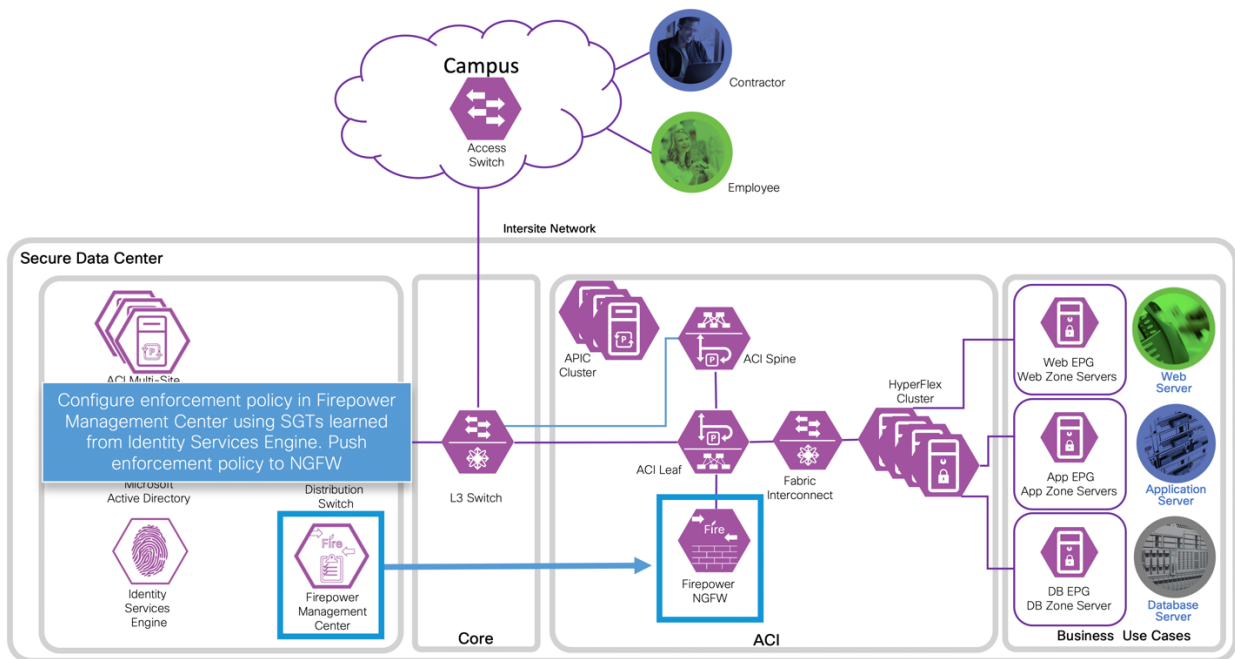


269

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

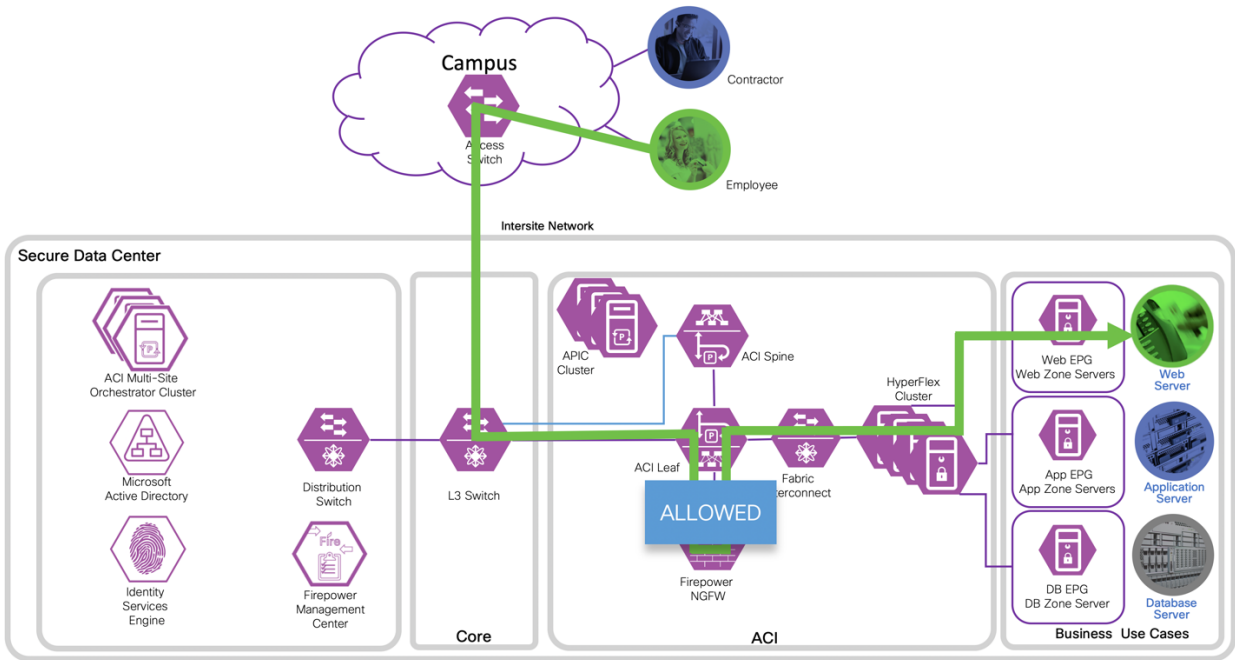


4. The SGTs are used in FMC access policy rules and are deployed to the FTD. When endpoints move within the network, FMC is updated by pxGrid with the endpoint latest metadata (e.g. IP address). FMC updates Firepower NGFW with no manual change to the access policy is required.

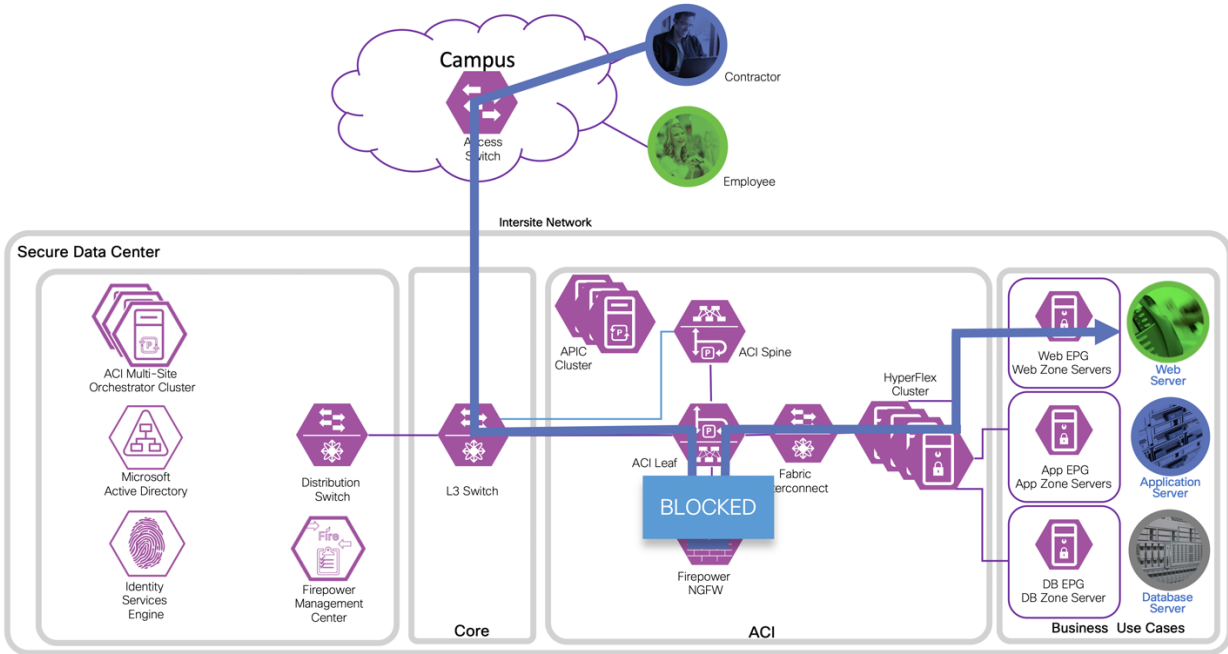


270

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.



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

272

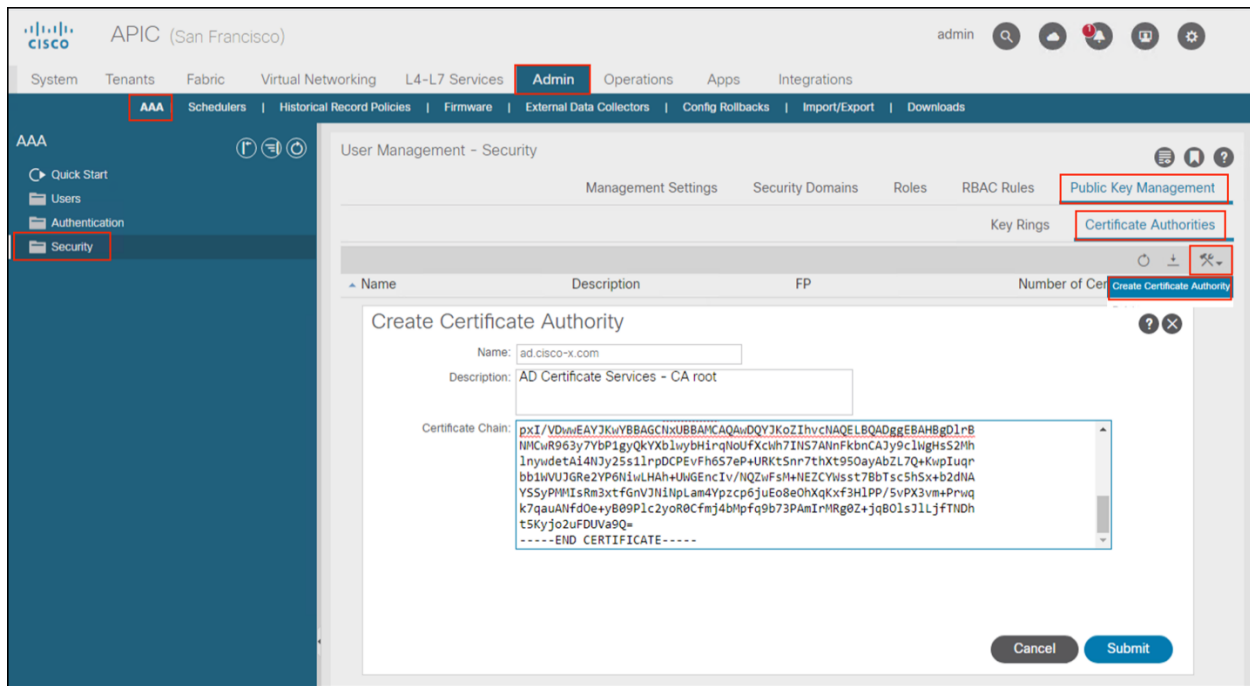
Step 2 Configure ACI and ISE

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



273

- 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*.

The screenshot shows the Cisco APIC (San Francisco) Admin console. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, Apps, and Integrations. The left sidebar shows the AAA configuration tree with options for Quick Start, Users, Authentication, and Security. The main content area is titled 'User Management - Security' and includes sub-tabs for Management Settings, Security Domains, Roles, RBAC Rules, and Public Key Management. The 'Public Key Management' tab is active, showing a table of Key Rings and Certificate Authorities. A 'Create Key Ring' dialog box is open, allowing the user to configure a new key ring. The dialog includes fields for Name, Description, Certificate, Modulus, Certificate Authority, and Private Key. The 'Name' field is filled with 'SDC1-Key-Ring'. The 'Description' field is filled with 'optional'. The 'Certificate' field is empty. The 'Modulus' field has a dropdown menu with options: MOD 512, MOD 1024, MOD 1536, and MOD 2048. The 'Certificate Authority' field is filled with 'ad.cisco-x.com'. The 'Private Key' field is empty. The 'Submit' button is highlighted in blue.

274

- 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:

APIC (San Francisco)

admin

System Tenants Fabric Virtual Networking L4-L7 Services Admin Operations Apps Integrations

AAA Schedulers Historical Record Policies Firmware External Data Collectors Config Rollbacks Import/Export Downloads

AAA

Quick Start Users Authentication Security

User Management - Security

Management Settings Security Domains Roles RBAC Rules Public Key Management

Key Rings Certificate Authorities

Name	Description	Admin State	Trust Point	Modulus
default	Default self-signed SSL Certif...	Completed		MOD 2048
SDC1-Key-Ring		Started	ad.cisco-x.com	MOD 2048

Create Certificate Request

Subject: apic1.sdc1.cisco-x.com

Alternate Subject Name:

Locality: San Francisco

State: CA

Country: US

Organization Name: Cisco-x

Organization Unit Name:

Email:

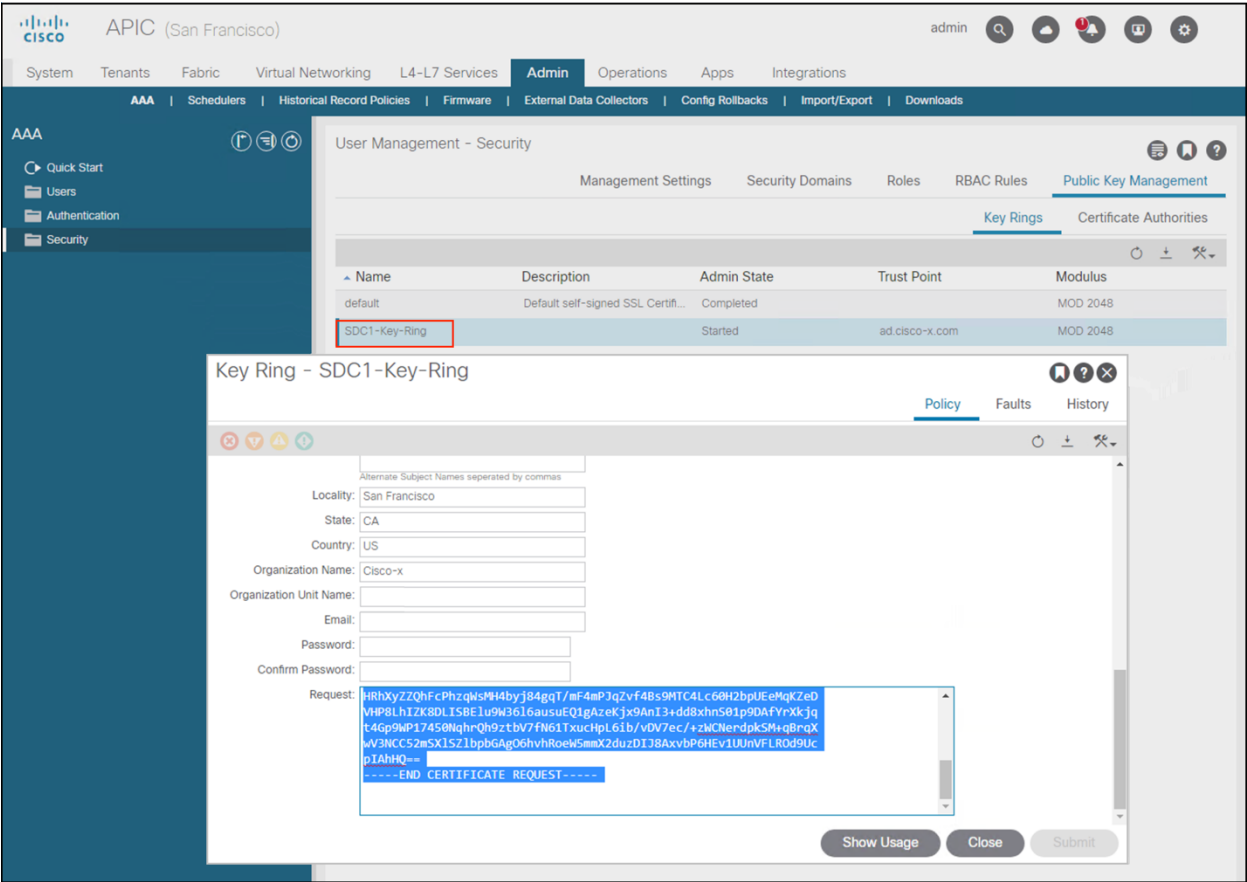
Password:

Confirm Password:

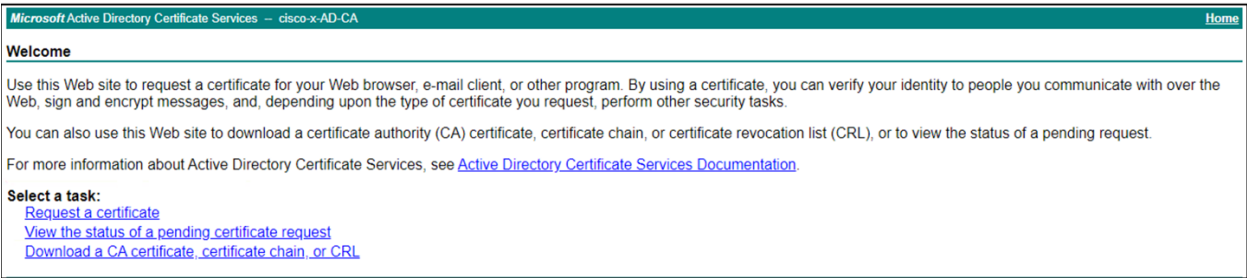
Cancel Submit

275

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**.

Microsoft Active Directory Certificate Services — cisco-x-AD-CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
HRXyZQhfcPhzqvH4byj84ga7mf4eP7qZv~
VHP8hI2K8DL58E1u9u3e16ausuEQ1gAzeKj~
t4gp9uP17450Nqh-Qh9ztbV7fN61TxcuHPL6ib
wV3NC52m5X1S21bpBAG06hvRoei5mmX2duzi
p1AhHq==
-----END CERTIFICATE REQUEST-----
```

Certificate Template: Web Server

Additional Attributes:

Attributes:

Submit >

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

Microsoft Active Directory Certificate Services — cisco-x-AD-CA Home

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

[Download certificate](#)

[Download certificate chain](#)

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**

Cisco APIC (San Francisco) admin

System | Tenants | Fabric | Virtual Networking | L4-L7 Services | **Admin** | Operations | Apps | Integrations

AAA | Schedulers | Historical Record Policies | Firmware | External Data Collectors | Config Rollbacks | Import/Export | Downloads

User Management - Security

Management Settings | Security Domains | Roles | RBAC Rules | **Public Key Management**

Key Rings | Certificate Authorities

Name	Description	Admin State	Trust Point	Modulus
default	Default self-signed SSL Certifi...	Completed		MOD 2048
SDC1-Key-Ring		Started	ad.cisco-x.com	MOD 2048

Key Ring - SDC1-Key-Ring

Policy | Faults | History

Name: SDC1-Key-Ring

Admin State: Started

Description: optional

Certificate:

```
AQUAcgB2AGUAcJA0BghVHQ8BAf8EBAMCBAwEwYDVR01BAwvCgYIKuYBBQUHAgEw
DQYJKoZIhvcNAQELBQADggEBAKUTeUa+DqG6jKHb5GYPY2yulafx/v8TYD3juL
5A8vte6vaBnv6Ctp149mPTzJF7VL1Bfur1vgndkkaagYIK118A8M/p1K3uRu3QgTn
nfxY1DtVf/nkThp5BUEdLy6/w35H9B2xa2V5ukUJILhJLNL1Vh/1pwAH3Z5GhdP
VCV+t2MK05a3io1crbBD137Ym+YD3AnhJh+KgeqJupOLNvzQyrNxpz/8J22c83rT
pH8H9vCXPf7FHV+L84AHYUqC/F1ouHwFAZgBPQZ1K1xpPpT5oahL8toRn7
/Uvz216QyyYXe03nJ8PzChiyLSYeXInCkZdvah7A2gQpY=
-----END CERTIFICATE-----
```

Modulus: MOD 512 | MOD 1024 | MOD 1536 | **MOD 2048**

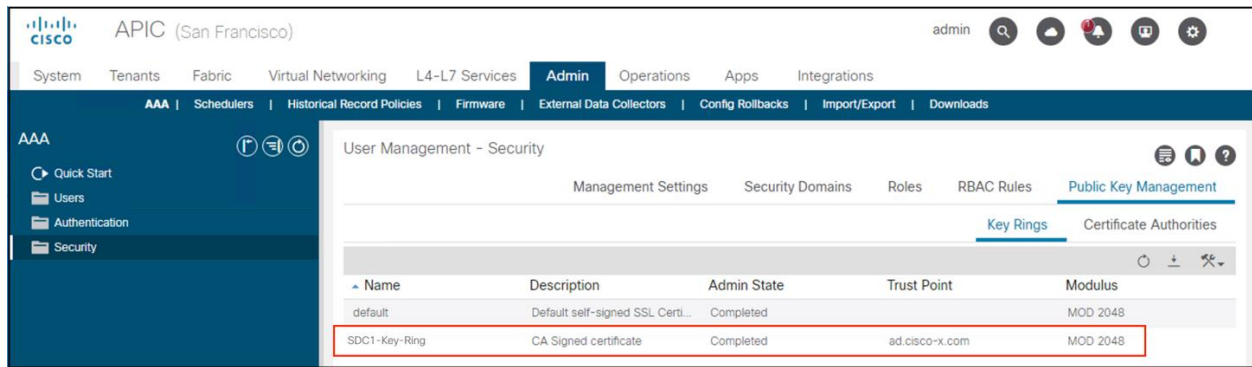
Certificate Authority: ad.cisco-x.com

Private Key:

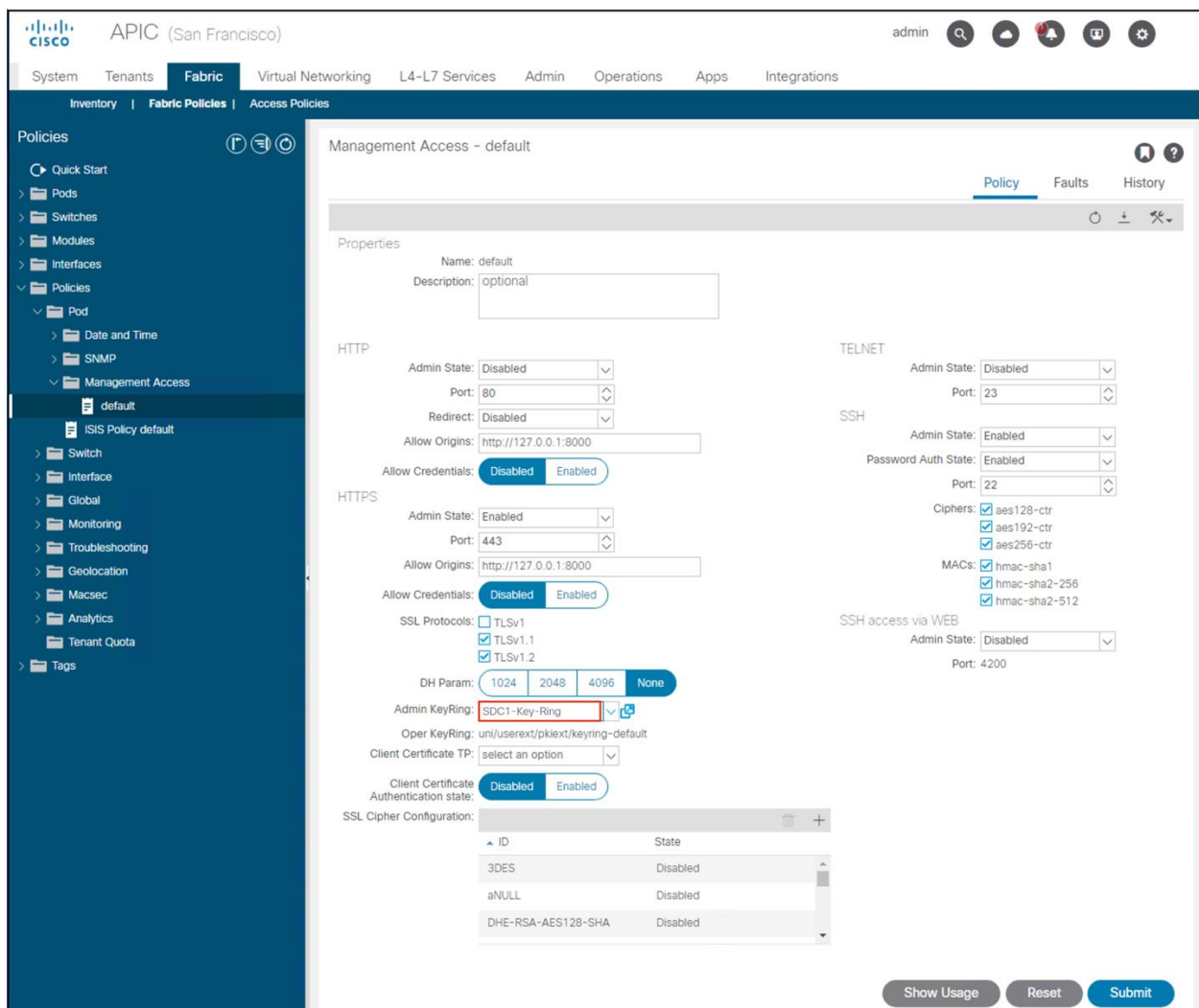
Show Usage **Close** **Submit**

277

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



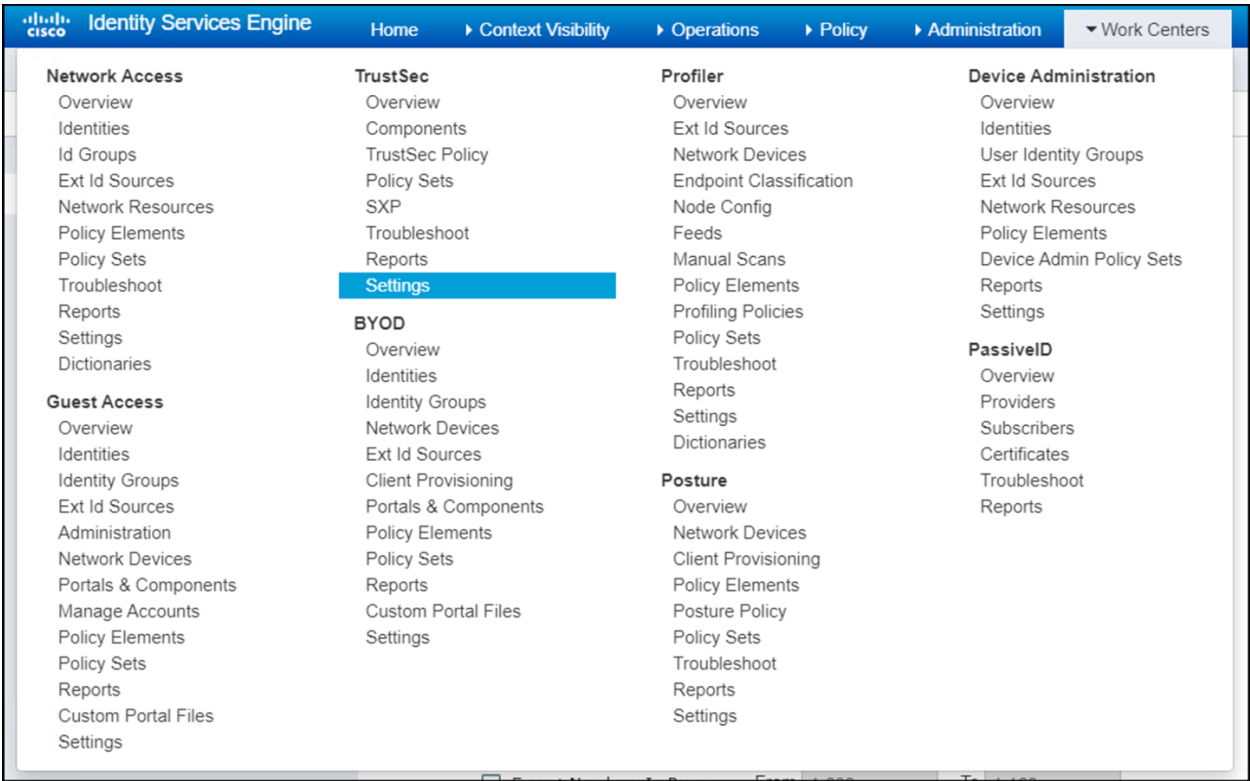
- f. Apply the key ring to HTTP policy
1. Navigate to **Fabric > Fabric Policies > Policies > Pod > Management Access > Default**
 2. Change the Admin KeyRing to the one created and click **Submit**



278

Step 3 Configure ISE for ACI Integration

- a. Enable ACI Integration
1. From the ISE management portal, navigate to **Work Centers > TrustSec > Settings**



2. In the Navigation Pane, choose **ACI Settings**
 - a. Complete the **ACI Cluster Details** configuration
 - b. Click **Test Settings** to verify the connection to ACIUnder the Name Conversion section, note the SGT and EPG suffixes

Cisco

Identity Services Engine

HomeContext VisibilityOperationsPolicyAdministrationWork Centers

Network AccessGuest AccessTrustSecBYODProfilerPostureDevice AdministrationPassiveID

OverviewComponentsTrustSec PolicyPolicy SetsSXPTroubleshootReportsSettings

General TrustSec Settings

TrustSec Matrix Settings

Work Process Settings

SXP Settings

ACI Settings

Endpoint Groups (EPGs), and endpoint (EF) configuration or Cisco Application Centric Infrastructure (ACI).

☒ Enable ACI Integration ⓘ

ACI Cluster Details

The cluster is comprised of multiple controllers that provide operators unified real-time monitoring, diagnostic, and configuration management capability for the ACI fabric.

IP Address / Host name *

10.16.1.11 ⓘ

Admin name *

ise-admin

Admin password *

.....

Tenant name *

TenantA ⓘ

L3 Route network name *

SDC1-L3OUT ⓘ

Test Settings

Name Conversion

New EPGs created by learning SGTs from ISE will have this suffix appended i.e. name will appear in ACI as name SGT suffix.

New SGT suffix *

_EPG

New EPG suffix *

_SGT

SXP Propagation

Specify SXP Domains that will share their mappings with ACI. Incoming ACI mappings will be propagated by SXP Domains defined on the SXP Mappings page.

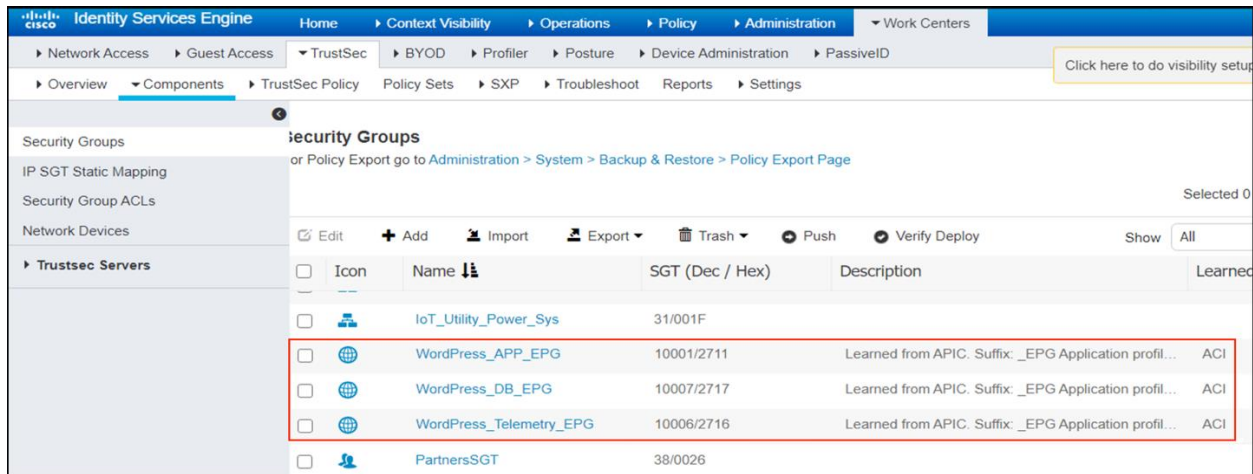
☐ All SXP Domains

☒ Specific SXP Domains

x default

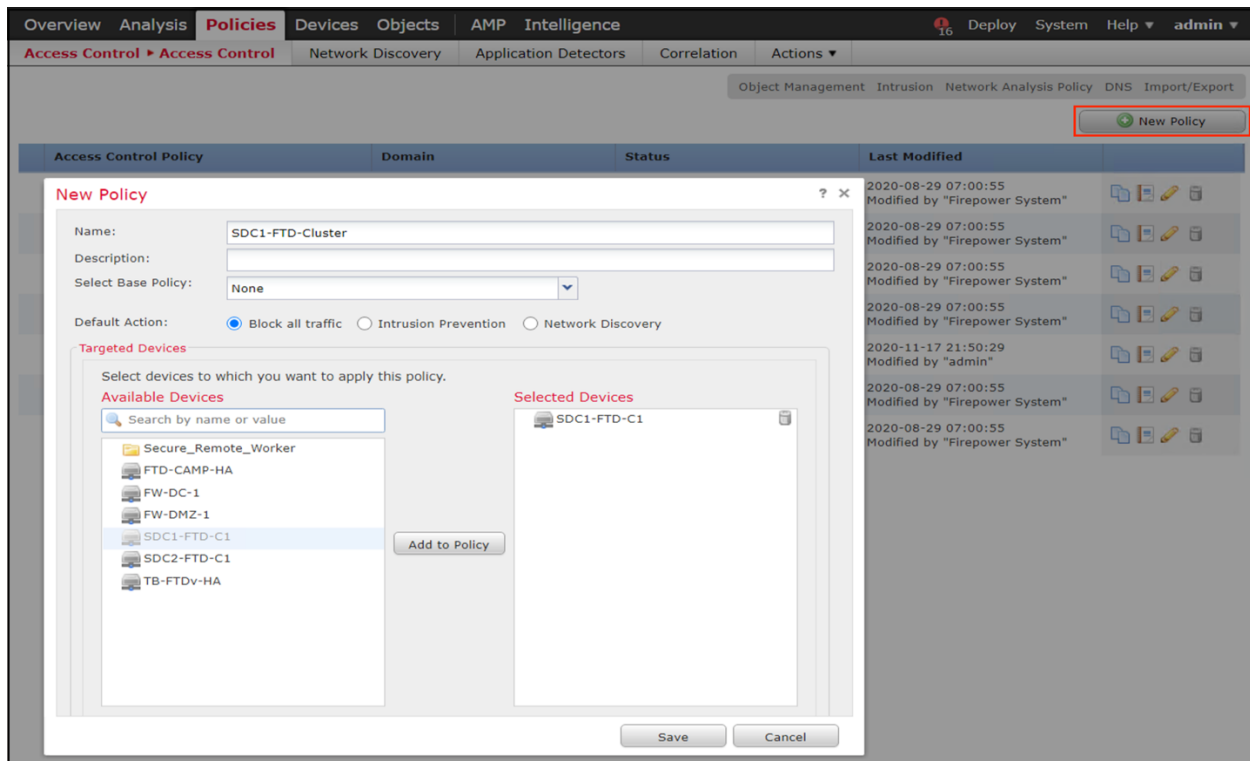
280

- 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.



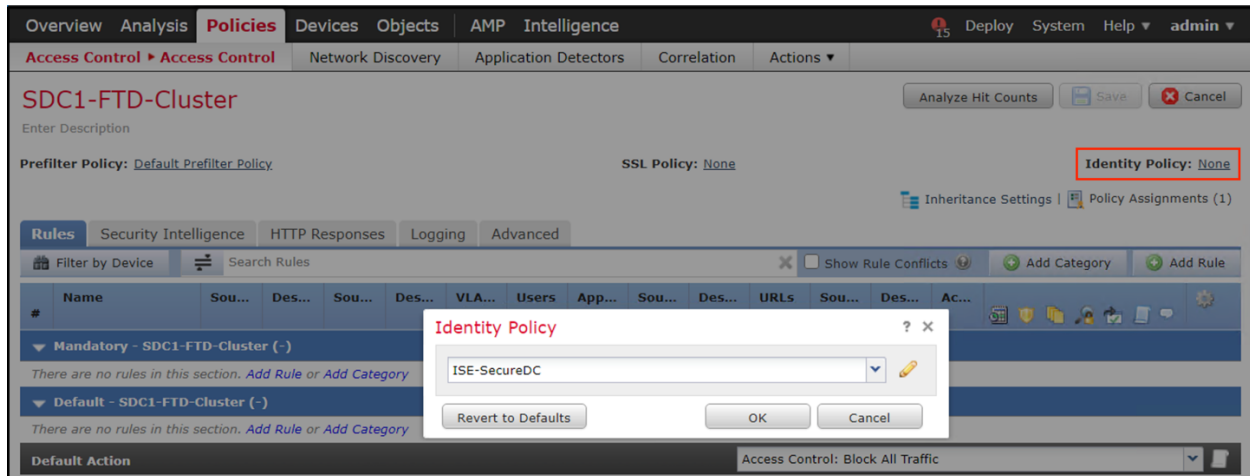
Step 4 Create an FMC Access Control Policy

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

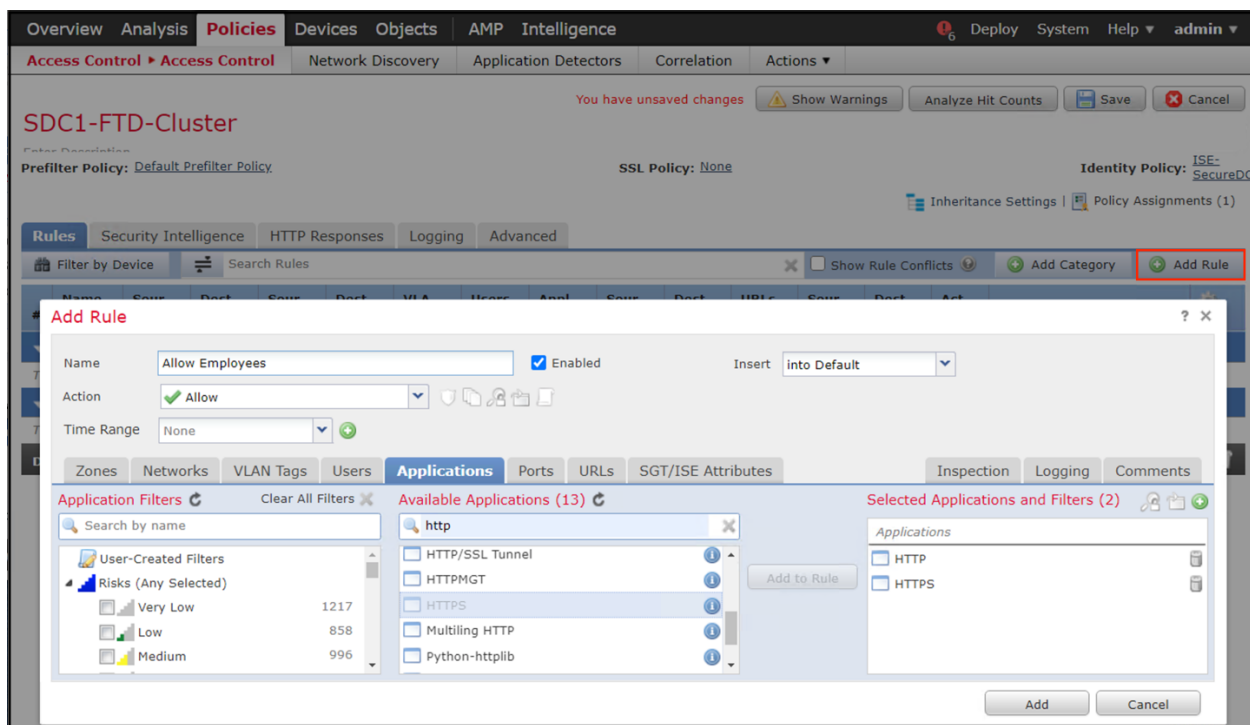


281

- 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**



282

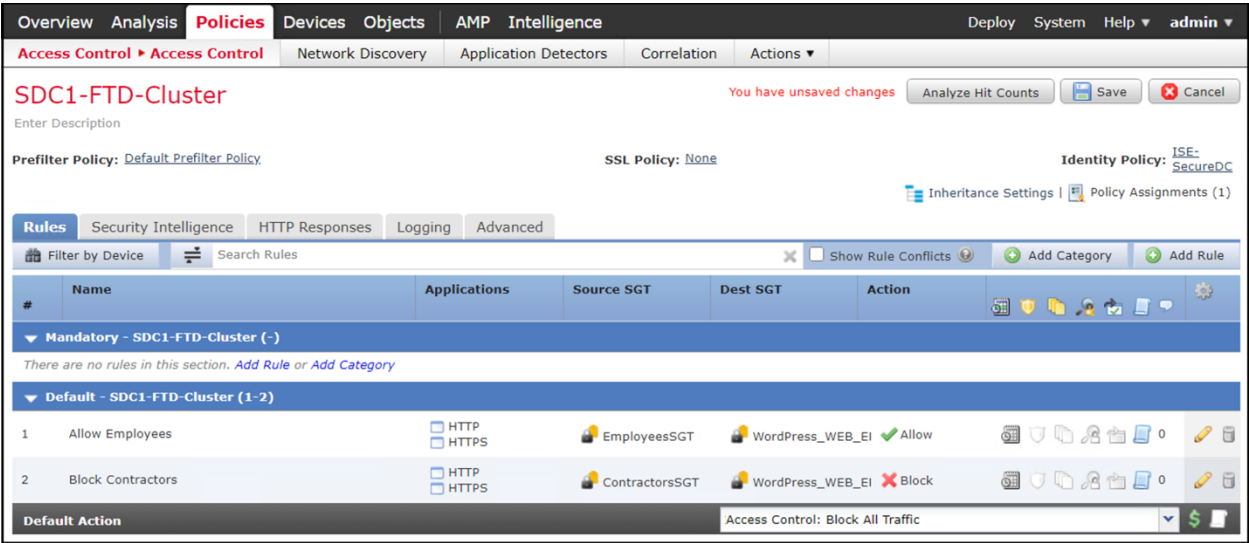
4. Choose the **SGT/ISE Attributes** tab. Under **Available Metadata**, choose **Security Group Tag** in the drop-down menu. Choose the source and click **Add to Source**. Repeat the step to add the destination.

The screenshot shows the Palo Alto Networks GUI for the 'SDC1-FTD-Cluster'. The 'Policies' tab is active, and the 'Add Rule' dialog box is open. The 'SGT/ISE Attributes' tab is selected. The 'Available Metadata' section shows 'Security Group Tag' selected. The 'Selected Source Metadata' section shows 'EmployeesSGT' and the 'Selected Dest Metadata' section shows 'WordPress_WEB_EPG'. The 'Add Rule' dialog box has the following fields: Name: 'Allow Employees', Action: 'Allow', Time Range: 'None', and 'Enabled' checkbox checked. The 'Add Rule' dialog box also has tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'SGT/ISE Attributes', 'Inspection', 'Logging', and 'Comments'.

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

The screenshot shows the Palo Alto Networks GUI for the 'SDC1-FTD-Cluster'. The 'Policies' tab is active, and the 'Add Rule' dialog box is open. The 'Logging' tab is selected. The 'Log at Beginning of Connection' checkbox is checked. The 'Add Rule' dialog box has the following fields: Name: 'Allow Employees', Action: 'Allow', Time Range: 'None', and 'Enabled' checkbox checked. The 'Add Rule' dialog box also has tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'SGT/ISE Attributes', 'Inspection', 'Logging', and 'Comments'.

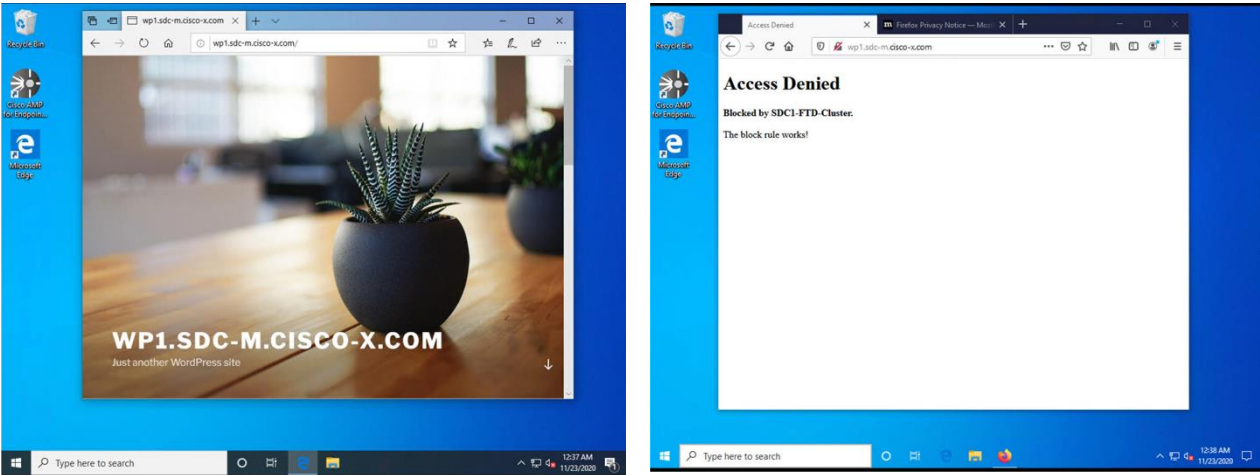
6. Repeat the steps to create a block rule for Contractors



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.



284

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

← → ↻ ⚠ Not secure | 10.9.10.41/events/index.cgi?table=rua_event

Apps AMP Dashboard AMP for Endpoint Secure DC SRW IoT dCloud Server - VM... Services Campus

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligenceDeploySystemHelpadmin

Context ExplorerConnectionsIntrusionsFilesHostsUsersUser ActivityCorrelationAdvancedSearch

Bookmark This PageReport DesignerDashboardView BookmarksSearch

User Activity

Table View of EventsUsers2020-11-23 00:00:00 - 2020-11-23 01:25:02Expanding

No Search Constraints (Edit Search)

	Time	Event	Username	Realm	Discovery Application	Authentication Type	IP Address	Start Port	Security Group Tag	Endpoint Profile	Endpoint Location	Device
↓	2020-11-23 00:37:28	User Login	Bob	SecureDC	LDAP	Passive Authentication	10.9.110.102		ContractorsSGT	Belkin-Device	10.9.255.19	fmc.cisco-x.com
↓	2020-11-23 00:36:51	User Login	Aaron	SecureDC	LDAP	Passive Authentication	10.9.110.101		EmployeesSGT	Belkin-Device	10.9.255.19	fmc.cisco-x.com

< < Page 1 of 1 > > Displaying rows 1-2 of 2 rows

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.

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligenceDeploySystemHelpadmin

Context ExplorerConnectionsEventsIntrusionsFilesHostsUsersCorrelationAdvancedSearch

Bookmark This PageReport DesignerDashboardView BookmarksSearch

Connection Events (switch workflow)

Connections with Application DetailsTable View of Connection Events2020-11-22 00:00:00 - 2020-11-23 02:07:06Expanding

Search Constraints (Edit Search Save Search)

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation
↓	2020-11-23 01:59:20		Allow		10.9.110.101		10.18.107.101		ACL-PBR	ACL-PBR	64192 / tcp	80 / http / tcp	HTTP	Edge		http://wp1.sdc-m.cisco-x.com/		Unknown
↓	2020-11-23 01:59:11		Allow		10.9.110.101		10.18.107.101		ACL-PBR	ACL-PBR	49681 / tcp	80 / http / tcp	HTTP	Edge		http://wp1.sdc-m.cisco-x.com/		Unknown
↓	2020-11-23 01:52:30		Block		10.9.110.102		10.18.107.101		ACL-PBR	ACL-PBR	54718 / tcp	80 / http / tcp	HTTP	Firefox		http://wp1.sdc-m.cisco-x.com/		Unknown

285

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.

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>

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:

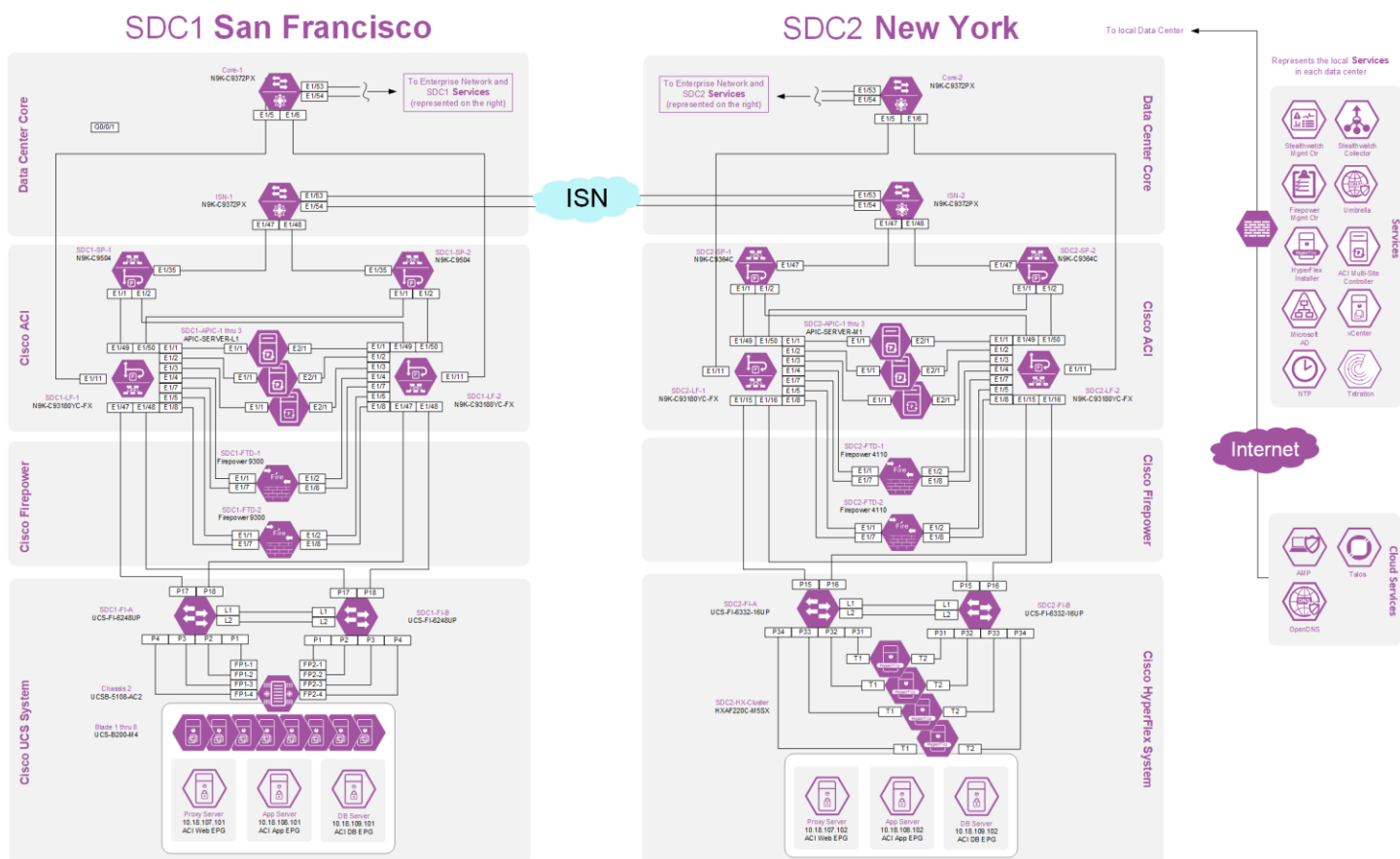
<https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html>

Cisco TrustSec:

<https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html>

Appendix A

Secure Data Center Lab Diagram



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

290

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

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



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

↩ Return to Contents