



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

З

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.

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 <u>Secure Data Center Architecture Guide</u>, which can be found with the other PIN Architecture Guides here:

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 microsegmentation
- 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:



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	o achieve	visibility in	the data	center.
--------------------	-----------------	-----------	---------------	----------	---------

lcon	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.

lcon	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.

lcon	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.

These capabilities provide segmentation across 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.

lcon	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.

Visibility

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



Capability		Solution Component
App	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 <u>SAFE Architecture Guides</u> 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.

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.



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.

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.



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.



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.

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.

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

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.
Microsegment ation(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/pr oducts/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/p roducts/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/pr oducts/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/p roducts/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/pr oducts/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/p roducts/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/pr oducts/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/hyperconv erged-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/pr oducts/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/p roducts/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/pr oducts/collateral/security/firepowe r-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/p roducts/collateral/security/firepow er-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-hxseries/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), <u>https://www.Cisco.com/c/en/us/td/docs/hyperconverged systems/HyperFlex HX DataPlatformSoftw</u> <u>are/Installation VMWare ESXi/4 0/b HyperFlexSystems Installation Guide for VMware ESXi 4 0.h</u> <u>tml</u>. 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, <u>https://www.Cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftw</u> <u>are/HyperFlex_Preinstall_Checklist/b_HX_Data_Platform_Preinstall_Checklist.html</u>.

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

	ului) cisco)	
Cisco	HX Data Plat	form Install	er
		HyperFlex	
1	root		
1	root	•	
1	root	and conditions	

0			
 cisco	HyperFlex Installer		0 0 ⊘ ☆ ∖
		Workflow	
Select	a Workflow		
	,∕₽. ♠₽	, Ø. Ø., Ø	
	Cluster Creation with HyperFlex (Fl)	Cluster Creation with HyperFlex Edge	Cluster Expansion
	w what I'm doing, let me customize my workflow		

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



The figure below is the Dashboard for HyperFlex™ Connect.

≡ dialo HyperFle	x Conn	ect					2	SDC2-H	X-Cluste	r						•	⊁~	?	1.
Dashboard	\bigcirc	OPERATION Online	IAL STATUS																
Alarms	_//_•	RESILIENCY Healthy	HEALTH												✓ 1 Node fa	ailure can be	tolerated		
Activity	Ð	CAPACITY 11.2 TB				2.2% 257.4 GB Used	1		11 TB Fr	ee		STORAGE OPTIMIZATION	32.6%		Compression Deduplication	n 4	30%		
ANALYZE		NODES 4				4 HXAF220C- Converge	м55х 📃 d												
PROTECT	IOPS Last	1 hour											Last	Read 1.90 (Max 1	3.70 Min 0.80 Av	rg 3.51) Last Writ	:e 34.70 (Max 73	.30 Min 32.00 A	vg 46.35)
Encryption	92	15:40:00	15:43:20	15:46:40	15:50:00	15:53:20	15:56:40	16:00:00	16:03:20	16:05:40	16:10:00	16-13-20	16:16:40	16:20:00	16:23:20	16:26:40	16:30:00	16:33:20	
MANAGE System Information	Through	out (MBps)	Last 1 hour	12.10.10		19.99.20	10.001.10		10.03120			10110120		Last Read 0.02	(Max 0.22 Min 0.	00 Avg 0.05) Las	t Write 0.23 (Max	0.63 Min 0.23	Avg 0.35)
Datastores	0.8	15:40:00	15:43:20	15:46:40	15:50:00	15:53:20	15:56:40	16:00:00	16:03:20	16:06:40	16:10:00	16-13-20	16:16:40	16:20:00	16:23:20	15:25:40	16:30:00	16:33:20	
↓ Virtual Machines	Latency (msec) Last 1	hour	13.70.40	.5.50.00	.5.33.20	13.30.40			10.00.40	10.10.00			Last Read 0.21	(Max 1.04 Min 0.1	13 Avg 0.31) Las	t Write 0.91 (Max	2.55 Min 0.61	Avg 1.21)
>_ Web CLI	0.0	15:40:00	15:43:20	15:46:40	15:50:00	15:53:20	15:56:40	16:00:00	16:03:20	16:06:40	16:10:00	16:13:20	16:16:40	16:20:00	16:23:20	16:26:40	16:30:00	16:33:20	_

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-dataplatform/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, threatfocused 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.

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

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

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

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

Stealthwatch

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

Stealthwatch[™] Enterprise dramatically improves:

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

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

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

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

VMware vSphere Settings Tested
• ESXi 6.0
 2 vCPUs 16 GB of RAM 50 OB diala

To deploy these two virtual machines, we followed the Stealthwatch™ Installation Guide 7.0, <u>https://www.Cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/</u> <u>SW 7 0 Installation_and_Configuration_Guide_DV 1 0.pdf</u>.

Tetration

The <u>Cisco Tetration</u> 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 behaviorbased 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 <u>Tetration Platform support and compatibility</u> 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:

- <u>Cisco Advanced Malware Protection for Endpoints</u>
- <u>Cisco Advanced Malware Protection for Networks</u>
- <u>Cisco Threat Grid</u>

<u>Cisco Advanced Malware Protection for Endpoints (AMP4E)</u> 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.

<u>Cisco Advanced Malware Protection for Networks (AMP4N)</u> 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.

<u>Cisco Threat Grid</u> 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 datasharing and threat control platform. It allows multiple security products to work together. Security operations teams can automate to get answers faster and contain threats faster.

pxGrid primary benefits are:

Simpler integration: Use one API for open, automated data sharing and control between more than 50 security products

Instant visibility: Have all contextual and relevant data on a single screen

Fast investigations: Conduct a full analysis on one system for fast answers

Even faster responses: Stop threats instantly using the network as an enforcer

pxGrid Components:

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

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

Validation Testing

Test Case	Integration	Visibility	Segmentation	Threat Protection	Orchestration and Management	Benefits
1	ACI Multi-Site Orchestrator (MSO) and Firepower Threat Defense (FTD)					 Enables Firepower Threat Defense (FTD) to be automated by MSO and inserted between applications in an ACI Multi-Site fabric MSO simplifies configurations to multiple APIC domains deployed globally
2	Firepower Management Center (FMC) and APIC		0		Ø	 Enables Firepower Threat Defense (FTD) to be automated by APIC and inserted between applications in an ACI Multipod fabric
3	Tetration and VMware vCenter (VM attributes)					 Provides protection for east-west traffic in VMware vCenter environments Enables richer context for analysis by Tetration Analytics Appliance Provides Zero trust or allowed/blocked list model Reduces the impact of policy changes
4	Stealthwatch Enterprise and Tetration	0				 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	Ø		Ø		 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			Ø		 Automated Response Prevents further lateral movement of infection by protecting other hosts in Endpoint Group (EPG)
7	FTD Rapid Threat Containment and Tetration			V		 Automated Response Prevents further lateral movement of infection by protecting other hosts in microsegment
8	Tetration and Identity Services Engine (ISE)	Ø	Ø			 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	Ø				 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.



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



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 MSOStep 2: Setup Day 0 Operations in MSO GUIStep 3: Configure Fabric Connectivity Infrastructure (Infra) in MSO GUIStep 4: Validate Intersite Policy with the MSO DashboardStep 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

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: <u>https://github.com/Cisco-security/Cisco-Validated-Designs/tree/master/Secure-Data-Center/APIC</u>.

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

Λ	Q
4	J

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

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

℃ Return to Contents

Intersite Network overview



Step B: Setup the ACI fabric

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

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

Cisco APIC Getting Started Guide, Release 4.1, Section: Initial Setup and Fabric Initialization and Switch Discovery https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/getting-started/b-Cisco-APIC-Getting-Started-Guide-411/b-Cisco-APIC-Getting-Started-Guide-411/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/basicconfiguration/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/2x/L2 config/b Cisco APIC Layer 2 Configuration Guide/b Cisco APIC Layer 2 Configurati on Guide chapter 011.html#task A47A972D56A34061A5E0709F8AACB675

Cisco Community, Factory reset APICs and Nodes

https://community.Cisco.com/t5/application-centric/factory-reset-apic-and-nodes/tdp/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/L3configuration/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/1x/ACI Best Practices/b ACI Best Practices/b ACI Best Practices chapter 0101.html

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

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

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

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

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

Section Summary:

- Step 1: APIC Initial Configuration
- Step 2: Out-of-Band Management
- Step 3: Pod Date and Time Policy
- Step 4: VLANs
- Step 5: Initial L3Out
- Step 6: Fabric Interconnect Interfaces
- Step 7: VMM Domain

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

- Step 9: Overlay Tunnel Endpoint (TEP) for Intersite
- Step 10: Multi-Site Orchestrator (MSO) Admin Account

Step 1: APIC Initial Configuration

- a. Connect to the APICs console with a monitor and keyboard or CIMC/KVM (recommended).
- b. (Optional) If you need to factory reset your APIC controllers and switches issue the following commands.

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

Simultaneously reboot all APICs.

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

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

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

Complete the Cluster Configuration with the following information.

Fabric name: SDC1 Fabric

Number of controllers in the fabric: 3

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

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

Address pool for TEP addresses: 10.21.0.0/16

VLAN ID for infra network: 1999

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

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

Management default gateway: 10.16.1.1

Enable strong passwords? Y

Enter the password for admin: XXXXXXXX

Reenter the password for admin: XXXXXXXX

Repeat this step for SDC1-APIC2 and SDC1-APIC3

Example of a completed Cluster Configuration

```
Cluster configuration ...
Enter the fabric name [SDC1Fabric1]:
Enter the fabric ID (1-128) [1]:
Enter the fabric ID (1-128) [1]:
Enter the POD ID (1-12) [1]:
Is this a standby controller? [NO]:
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]:
Dut-of-band management configuration ...
Enable IPv6 for Out of Band Mgmt Interface? [N]:
Enter the IPv4 address [10.16.1.11/24]:
Enter the interface speed/duplex mode [auto]:
admin user configuration ...
Enable strong passwords? [V]:
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).

ululu cisco	APIC						admin	0	
System	Tenants	1 Fabric	Virtual Networking	L4-L7 Serv	vices	Admin	Operations	Apps	Integrations
ALL TENANTS	6 Add Ten	iant Tena	ant Search: name or descr	C	ommon	infra	mgmt 2		
mgmt	$(\mathbf{\tilde{T}})$	OE	Out-of-Band Manager	nent					0.0
✓ () Quick Sta	art 3 Ind Managemen	t Access				Node & I	P Addresses	External Ho	osts Access
= Out-c	of-Band Manage	ement Acc	4						Ċ <u>+</u>
🗸 🎹 mgmt 🤇	Configure Out-of	-Band Manage	ement Access 5						
> 🚞 Applic	cation Profiles		Nodes:						i +
> 🚞 Netwo	orking			Node	IPV4	4 Address	IPV4 Gateway	IPV6 Address	IPV6 Gateway
> 🚞 IP Ad	dress Pools								
> 🚞 Contr	acts								
> 🚞 Polici	es								
> 🚞 Servic	ces								
> 🚞 Node	Management E	PGs							
> 🚞 Extern	nal Managemen	t Network							
> 🚞 Node	Management A	ddresses							
> 🚞 Mana	ged Node Conn	ectivity Gr							

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



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

reate Out-of-	Band	Man	agement	Access					?>
EP 2 > Nodes				1. Overview	2. Nodes	3. IP Addresses	4. External Hosts	5. Access	6
Select Nodes By:	Specif	c Ra	nge						
Nodes:									
	Selec	All							
	Select	ID	Name	Role					
		1	SDC1-APIC1	controller					
		2	SDC1-APIC2	controller					
		3	SDC1-APIC3	controller					
	V	101	SDC1-LF1	leaf					
	V	102	SDC1-LF2	leaf					
	V	201	SDC1-SP1	spine					
	V	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	2. Nodes	3. IP Addresses	4. External Hosts	5. Access	6. Confirmation				
Starting Out-Of-Band IPV4 Address:	10.16.1.17/24 address/mask		1 Starting Ou	t-Of-Band IPV6 Address: address/mask							
Out-Of-Band IPV4 Gateway:	10.16.1.1		2 Out-Of-Band	IPV6 Gateway:							
Node Id	Name	I	Pv4 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 28											
STEP 4 > External Hosts	1.		2. Nodes		3. IP Addresses		4. External Hosts	5. Access	6	6. Confirmation	
External Hosts:										⊞ +	
	IP										

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

Create Out-of-Banc	Managen	nent Access				? ⊗		
STEP 5 > Access		1 2. Nodes	3. IP Addresses	4. External Hosts	5. Access	6. Confirmation		
Filters						☆ +		
EtherType		IP Protocol	Source Port		Destination Port			

g. Review and click Finish.



Step 3: Pod Date and Time Policy

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

cisco A	PIC									admin	٩	0		۵
System Ter	nants Fabric 1	Virtual	Networking	L4-L7 Se	ervices	Admin	Operations	Apps	Integra	ations				
Inventory	Fabric Policies	Access P	olicies											
Policies		\overline{O}	Date and Tir	ne Policy -	Policy de	efault								
C ▶ Quick Start					r oney a									
> E Pods													Ő,	<u>+</u> **+
> 🚞 Switches			Properties	Name:	default									A
> 🖿 Modules				Description:	optional									
> 🚞 Interfaces														
~ 🚞 Policies 3			Adminis	trative State:	disabled	enabled								
~ 🖿 Pod 4														
Date an	d Time			Server State:	disabled	enabled								
	y default		Authent	ication State:	disabled	enabled								
	ment Access		Authent	tication Keys:										+
	inent Access				ID		Key		Trusted		Au	thenticatio	on Type	
> E Switch		4						No items h	ave been fou	nd.				
> interface								Select Actions	to create a ne	ew item.				
> 🔚 Global														
> 📩 Monitoring														
> 🧮 Troublesho	oting													7
> 🚞 Geolocation	n			NTP Servers:										+
> 🚞 Macsec					Host Name	/IP Address	Preferred	l Minii	mum	Maximum	Manag	gement EF	PG	
> 🔚 Analytics	> 🖿 Analytics							Polli	ng Interval	Polling Interval				
🚞 Tenant Quo	ota													
> 🗖 Tags														*
										Show Usage				ubmit

- 50
- b. Enter the IP address (1) of your NTP server, select default for the Management EPG (2) and click Submit (3).

Create Provider	S	3 8
Name:	10.9.255.1	
Description:	optional	
Preferred:		
Minimum Polling Interval:	4	
Maximum Polling Interval:	6	
Management EPG:	default (Out-of-Band) 🛛 2 🗸 🛂	
		3
		Cancel Submit

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).

aliali cisco	APIC					kngu	iyen Q	()	
Syster	m <mark>1</mark> Tenants	Fabric	Virtual Networking	L4-L7 Services	Admin	Operations	Apps	Integrat	ions
QuickSta	art Dashboard	Control	lers System Settings	2Smart Licensing	Faults	Config Zones	Events	Audit Log	Active Sessions
System	Settings	$\bigcirc \bigcirc$	Datetime Format - I	Date and Time					0 0
> 🚞 Quo	ota								O <u>+</u>
	C Connectivity Prefer	ences	Properties						
E Sys	tem Alias and Bannel	S Encountion	Display Forn	nat: local utc					
E BD	Enforced Exception L	ist	Time Zo	ne: America/Los_Ange	les			\sim	
= Fab	ric Security		Offset Sta	ate: America/Inuvik				^	
= BGF	P Route Reflector			America/Iqaluit					
E Cor	ntrol Plane MTU			America/Jamaio	a				
E co	OP Group			America/Juneau	i i				
= End	point Controls	•		America/Kentuc	ky/Louisvill	le			
Fab	ric Wide Setting			America/Kentuc	ky/Montice	ello			
E Loa	d Balancer			America/Kralen	dijk				
	t Tracking			America/La_Pa	2				
	tem Global GIPo			America/Lima					
= Date	e and Time 3			America/Los A	naeles 🔺				
E API	C Passphrase				3			•	
								_	5
						Show U	sage	Reset	Submit
4		×							

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).

alialia cisco	APIC								admin	٩	٩		٥
System	Tenants Fabric	1 Virtual Ne	etworking	L4-L7 Services	Admin	Operations	Apps	Integrations					
Inve	entory Fabric Policies	2 Access Poli	cies										
Policies	Ċ		Pods - Po	licy Groups									0
C Quick S	Start											Ó	+ **-
Pods Polic Polic Polic Profi	3 4 cy Groups Create Pod Policy (Group 5	 Name 	Date Time Policy	ISIS Policy	COO Polic	P Group /	BGP Route Reflector Policy	Management Access Policy	SNMP Policy		MACs Policy	sec
> Switche	95 S					Sel	No items hav ect Actions to	re been found. create a new item.					

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

Create Pod Policy	/ Group
Name:	SDC1-policy-group
Description:	optional
Date Time Policy:	erauli 2 🗸
ISIS Policy:	select a value
COOP Group Policy:	select a value
BGP Route Reflector Policy:	select a value
Management Access Policy:	select a value
SNMP Policy:	select a value
MACsec Policy:	select a value
	3
	Cancel Submit

 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).

cisco APIC					admin Q	(? 🖸	٢
System Tenants Fabric	1Virtual Networking	4-L7 Services	Admin	Operations	Apps	Integrations	
Inventory Fabric Policies	2 Access Policies						
Policies	Pod Selector - default	:					00
Quick Start ✓					Policy	Faults	History
> 🔄 Policy Groups	8 🗸 🛆 🕐					Õ	<u>+</u> %+
Profiles 4	Properties						
Pod Profile default	Name: Description	default					
> Switches	•						
> Modules	Type:	ALL					
> 🚞 Interfaces	Fabric Policy Group:	SDC1-policy-grou	р		~ 🗗		
> 🚞 Policies		SDC1-policy-g fabric/functorof	roup		7		•
> 🛅 Tags		Create Pod Polic	cy Group			Reset	Submit

Step 4: VLANs

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

cisco	APIC						admin	٩	0		٥
System	Tenants	Fabric	1 Virtual Networkin	g L4-L7 S	Services	Admin	Operations	Apps	Inte	egrations	;
Inve	ntory Fat	oric Policies	Access Policies 2								
Policies	Ē		Pools - VLAN								
> C Quick St	lart								νι ΔΝ	Opera	ational
> 🚞 Switche	s								V L/ IIV	open	
> 🚞 Modules										Ö <u>+</u>	. **+
> 🚞 Interface	es		 Name 	Allocation	Encap	Blocks		Descrip	otion		
> 🚞 Policies				Mode							
~ 🚞 Pools											
> 🖬 VLAN	, 4										
> 🖿 VXLA	Create VLA	N Pool 5									
> 🖿 VSA	N										
> 🖿 VSA	N Attributes										
> 🚞 Multi	cast Address										
> 🖿 Physical	and External D	omains									

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

Create Ranges						? ×
Type: VLAN	1		2			
Range: VLAN	√ 1000	- VLAN	√ 1099			
3	Integer Valu	e	Integer Val	ne		
Allocation Mode: Dyna	mic Allocation	Inherit allocMod	e from parent	Static Allocation)	
Role: Exter	nal or On the wire	e encapsulations	Internal			4
					Cancel	ОК

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).

Create Ranges			? ⊗
Type: VLAN Range: VLAN V 1100	1 2 VLAN V 1199 Integer Va	lue	
Allocation Mode: Dynamic Allocation	Inherit allocMode from parent	Static Allocation 3	
Role: External or On the v	vire encapsulations Internal		4
		Cancel	ОК

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).



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-L30UT	1					
Associated Attachable Entity Profile:	select a value		\sim				
VLAN Pool:	SDC1-VLAN-PO	OL2(static) 2	~ 🔁				
Security Domains:					Q	+	
	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).

cisco	APIC					admin Q	()	*
System	Tenants	Fabric 1 Virtual	Networking	L4-L7 Services	Admin	Operations	Apps In	tegrations
Inve	ntory Fabi	ric Policies Access	Policies 2					
Policies		1	Attachable A	Access Entity Profile	es			
Ouick S	tart						Ó	<u>+</u> **+
> 📩 Switche	S		 Name 	Infrastruct	ure VLAN	Policy Groups	Descriptio	on
> Modules	5			Enabled				
> 🚞 Interface	es							
✓								
> 🚞 Swit	ch							
> 🚞 Inter	face							
🗸 🚞 Glob	al 4							
> 🚞 A	ttachable Acces	ss Entity Profiles 5		_				
> 🚞 Q	OS Class	Create Attachat	le Access Entity Pro	file 6				
> 🚞 D	HCP Relay							

- 55
- 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					?	×
STEP 1 > Profile			1. Profile	2. Assoc	ciation To Inter	faces	
Name: S	SDC1-L3OUT 1]					
Description: 0	ptional						
Enable Infrastructure VLAN:]						2
Domains (VMM, Physical or External) To Be Associated						1	+
To Interfaces: [Domain Profile		Encapsulation				
S	SDC1-L30UT (L3) 3	~					
		4 Update	Cancel				
EPG DEPLOYMENT (All Selected	ed EPGs will be deployed on all the interface	es associated.)					
							+
Application EPGs		Encap	Prir	mary Encap	Mode		
				vious	Cancel	5 Next	

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

Create Attac	hable A	Access Enti	ty Profile			? &
STEP 2 > Associa	ation To Int	erfaces			1. Profile	2. Association To Interfaces
Interface Policy Group	Туре	Associated Attachable Access Entity Profile	Switches / Fexes	Interfaces	Select Interfaces	
SDC1-FI-A	VPC				All Specific None 1	
			101,102	1/47		
SDC1-FI-B	VPC				All Specific None 2	
			101,102	1/48		
					Previ	ious Cancel Finish

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).

cisco APIC				admin		
System Tenants Fabric 1 Virtual 1	Networking	L4-L7 Servic	es Admin	Operation	s Apps	Integrations
Inventory Fabric Policies Access I	Policies 2					
Policies	Policy Group	s - Leaf Acce	ess Port			9
> C > Quick Start						ch 1 86
> 🖬 Switches						0 ⊻ X.
> 🖬 Modules	 Name 	Link Level Policy	CDP Policy	LLDP Policy	STP Interface	Monitoring Policy
		,	. eney	. eney	Policy	. eney
Policy Groups 5						
> 🖿 Leaf Access Port						
> PC Interface Create Leaf Access Po	ort Policy Group	7				
> EVPC Interface						
> E PC/VPC Override	I< < Page	1 Of 1 >	Objects	Per Page: 15	 Displaying 	g Objects

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.

Submit.		
Create Leaf Access Po	ort Policy Group	? ×
Name:	SDC1-L3OUT 1	A .
Description:	optional	
Link Level Policy:	1G 2 \sim 🖓	
CDP Policy:	CDP-Enable 3 🗸 🗸	
MCP Policy:	select a value	
CoPP Policy:	select a value	
LLDP Policy:	select a value	
STP Interface Policy:	select a value	
Storm Control 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	
Monitoring Policy:	select a value	
Priority Flow Control Policy:	select a value	
Fibre Channel Interface Policy:	select a value	
PoE Interface Policy:	select a value	
Slow Drain Policy:	select a value	
MACsec Policy:	select a value	
802.1x Port Authentication Policy:	select a value	
DWDM Policy:	select a value	5
Attached Entity Profile:	SDC1-L3OUT 4 🗸 🗸	J *
		Cancel 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)**.

Configure Interface, PC, and VPC		08
Configured Switch Interfaces	Select Switches T	as To Configure Interfaces: Quick Advanced
1 + Switches Interfaces IF Type Attached Device Type	Switches:	2 Switch Profile Name: Switch101_Profile
		Id Name Type Click '+' to configure switch interfaces
		V 101 SDC1-LF1 leaf 3
		102 SDC1-LF2 leaf
		Cancel

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

Configure Interface, PC, and VPC		0	×
Configured Switch Interfaces	Select Switches To Configure Interfaces: Qu	Jick Advanced	-
+ Transformer Switches Interfaces IF Type Attached Device Type	Switches:	Switch Profile Name: Switch 101_Profile Click '+' to configure switch interfaces Cancel Save	

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).

Configure Interface, PC, and VPC		? 🛛
Configured Switch Interfaces	Select Switches To Configure Interfaces: Quick Advanced	-
+	Switches: 101 Switch Profile Name: Switch101_Profile	
	Interface Type: Individual PC VPC FC FC PC	
	interfaces Selector Name: Switch101_1-ports-9	
	Interface Policy Group: Create One Choose One 2 Policy Group Name: SDC1-I 3CUT 3	4
		Save

 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.

ի։ cis	.ılı. sco	APIC							а	dmin Q			\$	
Sy	stem	1 Tenants	Fabric	Vir	tual Network	ing L4-L	.7 Services	s Adm	in Op	erations	Apps	Inte	egratio	ns
Quid	kStart	Dashboard	Cont	rollers	System Sett	ings <mark>2</mark> Sma	t Licensing	Faults	Config	JZones	Events	Audit L	og	Active §
Syst	em Se	ttings (F) (I O	BGP	Route Refle	ector Policy	- BGP Ro	ute Refle	ctor					
> 🖿	Quota	onnectivity Prefe	rences			,				Polic	y Fau	lts	Histor	y
E	System	Alias and Banne	ers	8								Ŏ	+ %	×.+
F	Global /	AES Passphrase	Encryptior	Pro	perties									
H	BD Enfo	orced Exception I	List			Nam	e: default							
E	Fabric S	Security				Descriptio	n: optional							
E	Control	Plane MTU												
	Endpoir	nt Controls			Autonomous	System Numbe	r: 65001	4	$\hat{}$				5	
F	Fabric V	Vide Setting	•	•	Route	Reflector Node	s:					ti i	+	
F	Port Tra	acking					Pod ID	Node ID	Node	Descriptio	on			
F	System	Global GIPo							Name					
F	Date an	id Time												
Ē	APIC Pa	assphrase												
Ē	BGP Ro	oute Reflector	3											
F	COOP	Group												_
	Load Ba	alancer												•
Ē	Precisio	on Time Protocol												
									Showl	Jsage				
4			Þ	_										_

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

Create Route R	eflector Node		0 8
Spine Node:	U	~ P	
Description:	SDC1-SP1 Pod-1/201	1	
	SDC1-SP2 Pod-1/202		
			2
			Cancel Submit

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

Create Route R	eflector Node			0 ×
Spine Node:	SDC1-SP2	~ 🗗		
Description:	SDC1-SP1 Pod-1/201			
	SDC1-SP2 Pod-1/202		1	
				2
				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).

cisco	APIC						admin Q		
System	Tenants	Fabric	1Virtual	Networking	L4-L7 Services	Admin	Operations	Apps	Integrations
Inven	tory Fabric	Policies	Access	Policies 2					
Policies		\mathbb{O}	•	Policy Grou	ps - VPC Interfa	ce			0
> C Quick Sta	art		^						○ ± **-
> Switches				 Name 		Link Aggreg Type	gation	Link CD Level Pol	P MCP Port LL c Polic Chan Pc
Interfaces	s 3							Polic	Polic
> 🖬 Spine	Interfaces								
> Pro	ofiles								
~ 🚞 Po	licy Groups 5								
> 🖬 、 🖬	Leaf Access Po	rt	1						
> =	VPC Interface	, .							
> 🖿	PC/VPC Overrie	Create VI	PC Interface P	Policy Group 7					
> 🖿	Leaf Breakout F	Port Group							
> 	FC Interface FC PC Interface	•							
> 🚞 Ov	verrides								
> 🚞 Policies				•					•
> Pools				IK K Pag	e 1 Of 1 >	Objects	Per Page: 15 🗸	Displayir	ng Objects 1 - 5 Of 5

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	e 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	
			4 🗸
		Cancel	Submit

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

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

cisco	APIC							admin	Q 🔇		*	
System	Tenants 1	Fabric	Virtual Networking	L4-L7 Services	Admin	Operations	Apps	Integ	grations			
Inve	entory Fab	ric Policies	Access Policies 2									
Policies		© = O	Quick Start									
> C Quick St	tart <mark>3</mark>											•
> 🚞 Switches	s		Sum	mary		Steps			Se	e Also		
> 🚞 Modules												
> 🚞 Interface	es		Access policies	overn the	Configure in-ban	d management acces	is 📑		Physical Inter	ace (Link	Level)	
> 🖿 Policies			operation of intel	faces that	Configure out-of-	band management	_	. =				
> 🚞 Pools			fabric. The syste	m provides a	access				LACP			
> 🚞 Physical	and External D	omains	policies enable o	onfiguring (Create a CDP (or	other) interface polic	У	LACP Member				
			Administrators w	ho have fabric (Create a traffic st	orm control policy			Spanning Tre	e Interface	•	
			administrator priv create new acce	vileges can ss policies				-0	Storm Contro			
			according to the	r requirements.	Configure an inte	rface, PC, and VPC	4		Port Security			
			administrators to	select the (Duick configure p	ort interface			SPAN			

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).

Configure	e Interfac	e, PC, a	nd VPC						? ×
Configured S	witch Interfac	es		Select Switches T	To Configure Interfaces:	Quick Advar	nced		-
Switches	Interfaces	IF Type	+ 1 Attached Device Type	Switches:	101-102		<mark>∠</mark> 2	Switch Profile Name: Switch101-102_Profile	- 1
× ⊡ 101						Name	Туре	Click '+' to configure switch	- 1
	1/9	Individual	L3 (VLANs: 1100-1199)		V 101	SDC1-LF1	leaf	a a linternaces	- 1
					🔽 102	SDC1-LF2	leaf		- 1
									4
								Cancel Sa	ive

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)

Co	onfigured Sv	witch Interfac	es								
				+ 🗊	Select two swi	itches	to be paired	for VPC.			
	Switches	Interfaces	IF Type	Attached Device Type	Only switches	with	interfaces in	the same VPC polic	y group	can be	paired together.
	~□ ¹⁰¹				VPC Domain ID:	2	12		$\hat{\checkmark}$		
		1/9	Individual	L3 (VLANs: 1100-1199)	Switch 1:	3	101		\sim		
	►101,1				Switch 2:	4	102		~		
									_	Ċ	5
							🔲 ld	Name	Туре		Save
							101	SDC1-LF1	leaf		
							102 102	SDC1-LF2	leaf		
VF	PC Switch P	airs									
				1 + 💼							
	VPC Domai	in Id 🔺	Switch 1	Switch 2							
											Cancel Submit

- 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).

-	-						
C	onfigure	e Interfac	e, PC, a	ind VPC			? ×
Co	onfigured Sv	vitch Interface	es		Select Sw	vitches To Configure Interfaces: Quick Advanced	
				+ 🛍	Switches:	101-102 Switch Profile Name: Switch101-102 Profile	
	Switches	Interfaces	IF Type	Attached Device Type		2	
	✓ 101					Click '+' to configure switch	
1	-	1/9	Individual	L3 (VLANs: 1100-1199)			
	<mark>∼</mark> ∎101,1				1		
						۲ ⁻	
						Cancel	Save

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).

Configure	Interfac	e, PC, a	nd VPC				? ×
Configured Sv	vitch Interface	es		Select Switches To Cor	nfigure Interfaces: Quick Advance	d	
Switches	Interfaces	IF Type	+ 💼 Attached Device Type	Switches:	101-102 2	Switch Profile Name: Switch101-102_Profile	
∽ ∎101				Interface Type:	Individual PC VPC FC	FC PC	
	1/9	Individual	L3 (VLANs: 1100-1199)	Interfaces:	1/47 3	Interface Selector Name: Switch101-102_1-ports-47	
✓■101,1	1			Interface Policy Group:	Create One Choose One 4		
				Policy Group Name:	SDC1-FI-A V	6	- 1
					SDC1-FI-A infra/funcprof	5 Cancel Save	
					SDC1-FI-B infra/funcprof		

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.

cisco.	UCS Manager	(<u>)</u> 0	₩ 🐴 🚯 0 0 0			Q 9 1 8 8 6
æ	All	Servers / Service Profile Temp / roo	ot / Service Template T / vNICs / v	NIC eth2		
	Servers Service Profiles	General VLANs Statistics	Faults Events VLAN Groups			
器	 Service Profile Templates root () 		Name	eth2		
	Service Template Template-ESXI-SP	0 0 0 0	MAC Address MAC Pool	Derived SDC1-MAC-Pool		
₽	 ISCSI VNICS vHBAs 	Actions	MAC Pool Instance	Fabric A	 Fabric B 	Enable Failover
≡	vNICsvNIC eth0	Change MAC Address Modify VLANs	Owner : Type : CDN Source	Logical Ether		
	vNIC eth1 vNIC eth2	Modify VLAN Groups Bind to a Template	Oper CDN Name Equipment			
-0	 Dynamic vNiCs VLAN Groups 	Reset MAC Address	MTU :	9000 NONE		
	VLAN Group ACI VLANs		Template Name : Redundancy Peer :	ACI-FI-A-FailOvr		
	vNIC eth3Dynamic vNICs		States Operational Speed : State :	Line Rate Not Applied		
	 VLAN Groups VLAN Group ACI 		Adapter Policy :	VMWare 🔻		
	VLANs ► Sub-Organizations		Adapter Policy Instance	<pre>org-root/eth-profile-VMWare </pre>		
	PoliciesPools		Vos Policy Instance : Network Control Policy :	ACI-CDP-Enable V		
	 ▼ Schedules ▶ default 		Pin Group :	FI-A-B-PC-1		
	exp-bkup-outdate		Stats Threshold Policy : Threshold Policy Instance :	default org-root/thr-policy-default		
	► infra-fw		Virtual Host Interface Placemer Desired Placement Actual Assignment Cennection Pallelee	Any T		
			Dynamic vNIC UsNIC VI	ΛQ		
			Dynamic vNIC Connection Policy Dynamic vNIC Connection Policy	: <not set=""> ¥</not>		
			Order : Desired Order : Actual Order :	4 Unspecified		
					Save C	hanges Reset Values

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).

cisco	APIC							admin Q			
System	Tenants	Fabric	1 Virtual	Networking	L4-L7	Services	Admin	Operations	Apps	Integration	s
Inver	ntory Fabr	ric Policies	Access I	Policies 2							
Policies		Ē	\odot	Attachable	Access E	Entity Profil	es				?
> C Quick St	art									0 ± %	*
> Switches	5			 Name 		Infrastruct Enabled	ure VLAN	Policy Groups	De	scription	
> 🚞 Interface	s			default		true					
└ Policies				SDC1-L3OUT		false		SDC1-L3OUT			
> 🚞 Switc	h										
> 📩 Interf	ace al 4										
> 🖬 At	ttachable Acces	s Entity Profiles	5		_						
> 🚞 Q	OS Class	Create	e Attachabl	e Access Entity Pro	ofile 6						
> 🖿 Di	HCP Relay										

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

Create Attachable	e Access Entity Profile					?	\otimes
STEP 1 > Profile			1. Profile 2	. Associati	on To Interfa	aces	
Name: Description:	SDC1-VMM 1 optional						
Enable Infrastructure VLAN:							
Domains (VMM, Physical or External) To Be Associated							+
EPG DEPLOYMENT (All Self	ected EPGs will be deployed on all the interfaces associ	ated.)					
							+
Application EPGs		Encap	Primary E	псар	Mode		
			Previous	Can	icel	2 Next	

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

Create Attac	hable A	ccess Enti	ty Profile)		08
STEP 2 > Associa	tion To Inte	rfaces			1. Profile	e 2. Association To Interfaces
Interface Policy Group	Туре	Associated Attachable Access Entity Profile	Switches / Fexes	Interfaces	Select Interfaces	
SDC1-L3OUT	Individual	SDC1-L30			 All Specific None 	
			101	1/9		
SDC1-FI-A	VPC				 All Specific None 	
			101,102	1/47		
SDC1-FI-B	VPC				 All Specific None 	
			101,102	1/48		
						1
						Previous Cancel Finish

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 <u>Cisco ACI Virtualization Guide 4.1</u>, <u>Chapter Cisco ACI with VMWare VDS Integration</u> 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).

cisco	APIC						admin Q		
System	Tenants	Fabric	Virtua	l Networking	1L4-L7 Services	Admin	Operations	Apps	Integrations
				Inventory 2					
Inventory		•	Provide	er - VMware					0 0
C Quick St	tart								O +
	omains 3		Brono	rtion					
> 🚞 Micro	osoft		Flope	Nar	ne: VMware				
> 🚞 Oper	nStack			vCenter Domai	ns:				
> 🚞 Red	Hat 4				Name				
> 🚞 VMw	are			-					
> 🚞 Containe	er Doma	vCenter Dom	ain	5					
	Save a	IS							

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	0	×
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:	4	11
	Profile Name Username Description	
		1
	5	
vCenter:	÷ 🕆 🕆	
	Name IP Type Stats Collection	1
Ded Observations		
Port Channel Mode.		
vSwitch Policy:	CDP LLDP Neither	
NetFlow Exporter Policy:	c select an option	
	8	
	Cancel	

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:		
Confirm Password:		
		4
	Cancel	ОК

- 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 Co	ntroller			? ×
vCenter Controller				
Name:	SDC1-vCenter		1	
Host Name (or IP Address):	10.17.208.20		2	
DVS Version:	DVS Version 6.5	\sim	3	
Stats Collection:	Disabled Enabled			
Datacenter:	SDC1-VMM		4	
Management EPG:	select an option	\sim		
Associated Credential:	vCenter-Admin	\sim	5	
				6 Cancel OK

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

cisco	APIC						admin Q	0		\$
System	Tenants	Fabric 1	Virtual	Networking	L4-L7 Services	s Admin	Operations	Apps	Integ	grations
Inven	itory Fabri	ic Policies	Access	Policies 2						
Policies			ð	Attachable a	Access Entity Pr	ofiles				
→ C • Quick Sta	art								0 +	. **-
> Switches				 Name 	Infrastr Enable	ucture VLAN d	Policy Groups	Des	scription	
> 🚞 Interface	s			default	true					
Policies				SDC1-VMM	false					
> 📰 Switch	h			SDC1-L3OUT	false		SDC1-L3OUT			
> 📑 Interfa	ace Al 4									
> 🖿 At	tachable Acces	s Entity Profiles	5							
> 🗖 Q(OS Class	Create	Attachab	le Access Entity Pro	ofile 6					
> 🚞 DH	ICP Relay									

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

opuale (+) and N							
Create Attachable	e Access Entity Profile					?	×
STEP 1 > Profile			1. Profile	2. Associa	tion To Inter	faces	
Name:	SDC1-FTD-C1	1					
Description:	optional						
Enable Infrastructure VLAN:							2
Domains (VMM, Physical or External) To Be Associated						Î	+
To Interfaces:	Domain Profile		Encapsulation				_
	phys (Physical)	~	3				
		4 Update	Cancel				
EPG DEPLOYMENT (All Sele	acted EPGs will be deployed on all the interface	s associated.)					
							+
Application EPGs		Encap	Prima	ry Encap	Mode		
						5	
				us Ca	ancel	Next	

 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).

cisco	APIC						admin Q			•
System	Tenants	Fabric	1Virtual N	etworking	L4-L7 Services	Admin	Operations	Apps	Integ	rations
Inve	entory Fab	oric Policies	Access Po	licies 2						
Policies		\bigcirc		Policy Group	os - VPC Interfac	е				0
> C Quick S	start		^						0 +	**-
> 🖬 Switche	es -			 Name 		Link Aggreg	gation	Link CDF	MCP	Port LL
Module:	es 3					туре		Polic Polic	C POlic	Polic
> 🚞 Spin	e Interfaces			SDC1-FI-A		VDC		C		
🗸 🚞 Leaf	Interfaces			SDC1-EI-B		VDC		С		1
> 🗖 P	Profiles					100				
	Policy Groups	5								
	Lear Access PC Interface	Port	1							
>	VPC Interface									
> 🗖	PC/VPC Over	Create VF	C Interface Pol	icy Group 7						
> 🖬	Leaf Breakou	t Port Group								
> 🗖	FC Interface									
> 🖬	FC PC Interfa	ice								
> 🖬 C	Overrides									
> Policies				1 Page	1 Of 1	Objects	Per Page: 15	Displayin	n Objects	1 - 5 Of 5
> Pools				Page		Objects	Terrage. 15 V	Displayin	y objects	1-5015

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	e Policy Group		?⊗
Name:	SDC1-FTD1-CCL	1	<u> </u>
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 🗸 🗸	2	
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	
			4 -
		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.

cisco	APIC							admin Q	0		\$
System	Tenants	Fabric	Virtual N	letworking	L4-L7 Servi	ices	Admin	Operations	Apps	Integ	grations
Inve	ntory Fabr	ric Policies	Access Po	olicies							
Policies		1	\odot	Policy Group	os - VPC Inte	erface					0
> C Quick St	tart		^							↑ ↓	
Switches Modules	s ;			 Name 		L T	ink Aggreg ype	ation	Link Level Polic	CDP MCP Polic Polic	Port LI Chan Pi Polic
	e Interfaces										
V 🗖 Leaf	Interfaces			SDC1-FI-A		v	рс			C	L
> 🗖 Pi	rofiles			SDC1-FI-B		V	рс			C	L
~ 🚞 P	olicy Groups			SDC1-FTD-D/	ATA	v	рс				L
> 🚞	Leaf Access F	Port		SDC1-FTD1-0	DOL	V	рс				L
> 🖿	PC Interface		4	SDC1-FTD2-0	DOL	v	рс				L
~ 🗖	VPC Interface										
	SDC1-FI-A	4									
	SDC1-FI-E	3									
	SDC1-FTE	01-CCL									
		DATA									
. =		ride									
	Leaf Breakout	Port Group		4							+
,	FC Interface			I< < Page	1 Of 1 >		Objects I	Per Page: 15 🧹	Displ	aying Objects	1 - 5 Of 5
	EC PC Interfac	20	-								

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.

cisco	APIC		admir	• • • • •
System	Tenants1 Fabric	Virtual Networking L4-L7 Ser	vices Admin Operations Apps In	tegrations
Inve	ntory Fabric Policies	Access Policies 2		
Policies		Quick Start		A
> C Quick St	art <mark>3</mark>			~
> 🚞 Switches	5	Summary	Steps	See Also
> 🔚 Modules				
> 🚞 Interface	es	Access policies govern the	Configure in-band management access	Physical Interface (Link Level)
> E Policies		operation of interfaces that provide external access to the	Configure out-of-band management	LLDP
> 🚞 Pools		fabric. The system provides	access	LACP
> 🚞 Physical	and External Domains	policies enable configuring	Create a CDP (or other) interface policy	LACP Member
		Administrators who have fabric	Create a traffic storm control policy	Spanning Tree Interface
		create new access policies	Configure on interface, PC, and VPC	Storm Control
		according to their requirements. The APIC enables	Configure an interface, PC, and VPC 4	Port Security
		administrators to select the	Quick configure port interface	SPAN

- 71
- g. To create the VPC, select the newly created **Switch Profile 101,102 (1)** and in the work pane, click the **+ sign (2)**.

Configure	Interfac	e, PC, a	nd VPC					98	
Configured Switch Interfaces			Select Swit	Select Switches To Configure Interfaces: Quick Advanced					
Switches	Interfaces	IF Type	+ 🛱 Attached Device Type L3 (VLANs: 1100-1199)	Switches:	101-102	2 Switch Pi	rofie Name: Switch101-102_Profile Click *+* to configure switch interfaces		
2	1/47 1/48	VPC VPC					Cancel	ve	

 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)

Configur	e Interfa	ce, PC, a	nd VPC				
Configured S	Switch Interfa	ces		Select Switches To Con	figure Interfaces: Quick Advance	d	-
Switchos	Interfaces	IE Turpo	+ 🗇	Switches:	101-102 1 ~	Switch Profile Name: Switch101-102_Profile	
V == 101	Interfaces	ii iype	Attached Device Type	Interface Type:	Individual PC VPC FC	FC PC	
	1/9	Individual	L3 (VLANs: 1100-1199)	Interfaces:	1/7 2	Interface Selector Name: Switch101-102_1-ports-7	
∼ ∎101,1.		VPC		Interface Policy Group:	Select interfaces by typing, e.g. 1/17-18. Create One Choose One 3		
	1/48	VPC		Policy Group Name:	SDC1-FTD1-CCL	5	
					SDC1-FI-A infra/funcprof	Cancel Save	
					SDC1-FI-B infra/funcprof		
			1 - 40-		SDC1-FTD-DATA infra/funcprof		
VPC Doma	ain Id	Switch 1	Switch 2		SDC1-FTD1-CCL	4	
12	1	01	102		SDC1-FTD2-CCL infra/funcprof		l
						6 Cancel Submit	

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).

cisco	APIC								adm	nin Q		•	\$
System	Tenants 1 Fabric	١	/irtual Networl	king	L4-L7	Services	Admin	Ор	erations	Apps	Inte	grations	
ALL TENANTS	Add Tenant Tena	ant S	earch: name or	descr		commo	n <mark>2</mark> mgmt	infr	а				
common	€€		Networking -	Bridge	e Doma	ains						(900
Ouick Sta	rt Ta											Ŏ	<u>+</u> %+
> Applic	ation Profiles		 Name 	Alias	Туре	Segm: VF	F	Multic Addre	Custom MAC Address	L2 Unkno Unicas	ARP Floodi	Unica: S Routin	ubnet
> E Bri	dge Domains 5		default		reg	160		225	00:22:BD:F8	Har	False	True	
> 🚞 VR	Fs Create Bridge Domain	6											
> 🚞 Ext	ernal Bridged Networks	4											
> 🚞 Ext	ernal Routed Networks												
> 🚞 Do	t1Q Tunnels												
> 🚞 IP Add	iress Pools												
> 🚞 Contra	acts												
> 🚞 Policie	IS												
> 🚞 Servic	es		I< C Page	1 0	of 1 🔿		Ot	ojects Per I	Page: 15 🗸		Dis	playing Obje	cts 1 - 2 Of 2

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

Create Bridge Doma	iin			2 8
STEP 1 > Main		1. Main	2. L3 Configurations	3. Advanced/Troubleshooting
Name:	SDC1-FTD-CCL 1			
Alias:				
Description:	optional			
Tags:	~			
Turne	enter tags separated by comma			
Type:	tc regular			
Advertise Host Routes:				
VRF.	Certauit VC			
Forwarding.				
Endpoint Retention Policy.	This policy only applies to local L2 L3 and			
	remote L3 entries			
IGMP Snoop Policy:	select a value			
MLD Snoop Policy:	select a value 🗸			
				2
				IS Cancel Next
- 73
- I. Uncheck Unicast Routing (1) and click Next (2).

Oranta Dridera Darra						
Create Bridge Doma	In					? ×
STEP 2 > L3 Configurations		1. Main	2. L3 Configurations	3. Advanced/Troublesh	nooting	
Unicast Routing:	Enabled 1					<u></u>
ARP Flooding:	Enabled					
Config BD MAC Address:	✓					- 1
MAC Address:	00:22:BD:F8:19:FF					- 1
Subnets:						+
	Gateway Address	Scope	Primary ID Address	Subnet Control		
	datendy Address	00000	Thinkiyii Address	Subiliti Sontion		- 1
						- 1
						- 1
						-1
IP Data-plane Learning:	no yes					- 1
Limit IP Learning To Subnet:						- 1
DHCP Labels:						+
	Name	Scope		DHCP Option Policy		-
						- 1
						- 1
						- 1
Associated L3 Oute:						
Associated ES Outs.						+
	L3 Out					- 1
					2	-
			Pr	evious Cancel	Nex	d

m. Click Finish (1).

reate Bridge Domain			00
TEP 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 Monit	tor Policy
			1
			Previous Cancel Finish

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).

cisco	APIC				admin Q		
System	Tenants 1 Fabric	Virtual Networking	L4-L7 Services	Admin	Operations	Apps	Integrations
ALL TENANT	S Add Tenant Tena	ant Search: name or descr	common	2 mgmt	infra		
common	€€	Application Profiles					₿ () ()
C► Quick St	art .						○ ☰ **-
> 🖬 Common	cation Profiles						
> 🚞 Netw	orking Create App	lication Profile 5					4100x}-
> 🚞 IP Ad	Idress Pools						
> 🚞 Cont	racts						
> 🚞 Polic	ies						
> 🚞 Servi	ces						

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).

Create	Applicat	ion Profile						? ×
	Name:	SDC1-FTD-CCL		1				
	Alias:							
	Description:	optional						
	Tags:	enter tags separated by co	mma	\sim				
Mon	itoring Policy:	select a value		\sim				
EPGs								
								÷ +
Name	Alias	BD 3	Domain 4	Switching Mode	Static Path	Static Path VLAN	Provided Contract	Consumed Contract
SDC1-FTD-	CCL	SDC1-FTD-	√ phys (Physi	~	102/1/1,102/110/	1,	select an ol 🗸	select an ol 🗸
			5 Up	Jate Can	cel			
								6
						(Cancel	Submit

- 75
- 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.

Overview Inter	f <mark>aces</mark> Logical	l Devices	Security Modul	les Platfo	rm Settin	gs			System To	ols Help	admin
Network Module 1 Network Module 2 On CONSOLE MGMT USB 1 2 3 4 5 6 7 8 1 2 4 1 2 4 1 2 4 1 1 2 4 1 1 2 4 1 1 2 4 1 <td< th=""><th>>]]</th></td<>											>]]
All Interfaces Har	dware Bypass										
									Add New 🔹	Filter	×
Interface	Туре	Admin	Operation	Insta	VLAN	Admin Dup	Auto Nego	Operation	Admin State		^
MGMT	Management										
Port-channel1	data	10gbps	10gbps	SDC1-F		Full Duplex	no	up		J 🖉	_
Port-channel48	cluster	10gbps	10gbps	SDC1-F		Full Duplex	no	up		J 🖉	
Ethernet1/7								up			
Ethernet1/8								up			
Ethernet1/3	mgmt	10gbps	10gbps	SDC1-F		Full Duplex	no	up		6	
Ethernet1/4	data	10gbps	10gbps			Full Duplex	no	admin-down	X	ø	
Ethernet1/5	data	10gbps	10gbps			Full Duplex	no	admin-down	X	ø	
Ethernet1/6	data	10gbps	10gbps			Full Duplex	no	admin-down	×	ø	
Ethernet2/1	data	40gbps	40gbps			Full Duplex	no	sfp-not-pres	X	i	

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

Overview Analysis Policies	Devices Objects A	MP Intelligence		Deploy	욕 System Help 🔻	r admin v
Device Management NAT	VPN VOS Platform	Settings FlexConfig	Certificates			
Device Management						
List of all the devices currently registe	red on the Firepower Manage	ment Center.				
View By : Group	All (12) Error (2)	Warning (0) Offline (2)	Normal (8) Deployment Per	nding (1)	Device	Add •
Name	Model	Ver Chassis	Licenses	Access Control P		
SDC1-FTD-C1					J 1	^
sdc1-ftd-1(Master) 10.16.6.51 - Routed	FTD on Firepower 9300 SM-36	SDC1-FTD-1.cis 6.4.0 Security Module -	co-x.com:4 ² Base, Threat (2	SDC-Multisite-FTD-C1	*	
sdc1-ftd-2 10.16.6.52 - Routed	FTD on Firepower 9300 SM-36	SDC1-FTD-2.cis 6.4.0 Security Module -	Base, Threat (2 more)	SDC-Multisite-FTD-C1	n 🔀	
⊿			P		Ø 1	
Sdc2-ftd-1(Master) 10.17.6.51 - Routed	FTD on Firepower 4110	SDC2-FTD-1.cis 6.4.0 Security Module -	Sco-x.com:4 ² Base, Threat (2 more)	SDC-Multisite-FTD-C1	*	
Sdc2-ftd-2 10.17.6.52 - Routed	FTD on Firepower 4110	5.4.0 Security Module -	Base, Threat (2	SDC-Multisite-FTD-C1	i 🔀	

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.

Ov	erview	Interfaces	Logical Devices	Security Modules	Platform Settings			Sys	tem Tools Help admin
Logi	cal Devi	ice List						Č R	efresh 🕢 Add Device
Se	curity M	Iodule 1,2,3	(1 instances)						
	Security	Module1,2,3	Clustered	Status:ok					
	Applica	ation Ver	sion R	esource Profile	Management IP	Gateway	Management Po	ort Status	
۲	FTD	6.4	0.102		10.16.6.51	10.16.4.1	Ethernet1/3	🕜 online	🕶 🎼 ¢ 🔄 /
		Interface Nam	e	1	Туре		Attributes		
		Port-channe	1		data		Cluster Operational Status	: in-cluster	
		Port-channe	48	0	cluster		FIREPOWER-MGMT-IP	: 10.16.6.51 : master	
							CLUSTER-IP	: 127.2.1.1	
							MGMT-URL	: https://10.9.10.41/	75ccdb
							0010	. 0803/8/4-8080-1160-0026-0004/	a la
	FTD	6.2	3.83		10.16.6.53	10.16.4.1	Ethernet1/3	Security module not pres	
		Interface Nam	e	1	Туре				
		Port-channe	11	c	data				
		Port-channe	48	0	cluster				
	FTD	6.2	3.83		10.16.6.55	10.16.4.1	Ethernet1/3	Security module not pres	
		Interface Nam	e	1	Туре				
		Port-channe	1	c	data				
		Port-channe	148		cluster				

SDC1-FTD2 is the slave

0	verview	Interfaces	Logical D	evices	Security Modules	Platform Settings			5	System Tools	Help admin
Lo	gical De	vice List								C Refresh	Add Device
s	ecurity	Module 1,2,3	(1 instance	s)							
	Securit	ty Module1,2,3	(Clustered	Status:ok						
	Appli	cation V	ersion		Resource Profile	Management IP	Gateway	Management I	Port Status		
6	FTD	6.	4.0.102			10.16.6.52	10.16.4.1	Ethernet1/3	🚳 online) 🍡 C 🚾 🖻
		Interface Nan	ie			Туре		Attributes			
		Port-chann	el1			data		Cluster Operational Status	: in-cluster		
		Port-chann	el48			cluster		FIREPOWER-MGMT-IP CLUSTER-ROLE CLUSTER-IP MGMT-URL UUID	: 10.16.6.52 : slave : 127.2.2.1 : https://10.9.10.41/ : cb5d8bb6-a0af-11e8-8413-89a	a8e6bb6f78	
6	# FTD	6.	2.3.83			10.16.6.54	10.16.4.1	Ethernet1/3	Security module no	ot present 🕻 🏂	
6	FTD	6.	2.3.83			10.16.6.56	10.16.4.1	Ethernet1/3	Security module no	ot 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).

alialia cisco	APIC								admin	Q	0		*
System	Tenants 1	abric	Virtua	al Networking	L4-L7 Services	Admin	Operations	Apps	Integrations				
ALL TENANTS	6 Add Tenant	t Tenan	t Search	name or descr	commo	n mgmt	infra 2						
infra		(F)(=)(0	Fabric Ext Co	onnection Policies								0.0
C Quick Sta	art		^									Ó	+ **-
∨ 🏢 infra 🛛 3				ID		Name		Global Ro	ute Target			0	- ^*
> 🧮 Applio	cation Profiles												
> 🚞 Netwo	orking												
> Contr	acts												
	es +												
	Route Mans												
> =	BFD												
> =	BGP												
> 🖿	OSPF												
> 🖿	EIGRP												
> 🖿	IGMP Snoop												
> 🖿	IGMP Interface		4										
> 🚞	Custom QOS												
> 🖿	End Point Retention	on											
> 🚞	DHCP												
> =	ND Interface												
	ARP Interface												
	L4-L7 Policy-Bas	ed Redirect											
> =	L4-L7 Service EP	G Policy											
> 🖿	L4-L7 Redirect H	ealth Groups											
> 🖿	Data Plane Policin	g											
> 🖿	Fabric Ext Connec	ction Policies	6										
> 🖿	HSRP Creat	te Intrasite/In	tersite Pr	rofile 7									
> 🖿	First Hop Security												

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).

Create Intrasite/Intersite Profile	0 0
Fabric ID: 1 Name:	A
Community: extended:as2-nn4:5:16	
Site/Pod Peering Profile	
Peering Type: Full Mesh Route Reflector	
Password:	
Confirm Password:	
Pod Connection Profile	2
	1 +
Pod ID Dataplane T	ΈΡ
1 v 10.21.100.100	0/32 3
4 Update Cancel	
Fabric External Routing Profile	
	÷ +
Name Subnet	
4	Cancel Submit

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, <u>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_C2961137_1F5549F7AD548BA528CECE3E_</u>

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).

սիսիս cisco	APIC					admin Q	()	*
System	Tenants	Fabric	Virtual Networ	king L4-L7 Se	ervices Admin	1Operations	Apps	Integrations
AAA 2 Sche	edulers Hi	istorical Reco	rd Policies Firm	ware External D	ata Collectors Co	nfig Rollbacks	Import/Export	Downloads
AAA C Quick St	ent) ()	Users			Local Us	sers Remote	Users
Authentio	Create I	Local User	4				0 1	<u>+</u> **+
Security			▲ Login ID	First Name	Last Name	Email	Phone	
			admin					
			I< < Page 1	Of 1 > >	Objects Per Pag	e: 15 🧹	Displaying Objects	1 - 4 Of 4

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

Create Local Use	r					? 🗙
STEP 1 > User Identity		1. User Identit	у	2. Security		3. Roles
Login ID:	mso-admin	1				
Password:						
Confirm Password:		2				
First Name:						
Last Name:						
Phone:						
Email:						
User Certificate Attribute:						
Description:	optional					
Account Status:	Active Inactive					
Account Expires:	No Yes					
						3
						Next
				ous Ca	ancer	Next

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

STEP 2 > Security		1. User Identity 2. Se	ecurity 3. Roles
Security Domain:			
	Name	Description	
1	🔽 all		
	common mamt		
	L. Digni		
User Certificates:			+
	Name	Expiration Date	State
SSH Kove			
SSH Keys.			+
	Name	Key	
			2
		Previous	Cancel

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	@ Ø
STEP 3 > Roles	1. User Identity 2. Security 3. Roles
Domain all:	1 m +
Role Name	Role Privilege Type
admin 2	Vrite 3
	4 Update Cancel
	Previous Cancel Finish

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, <u>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</u>

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

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

We followed the Deploying Cisco ACI Multi-Site Release 2.1(x) Using OVA Section, <u>https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-</u> <u>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</u>

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)

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

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.

		TAL
Aulti Site Orchestrator	Username	
2.1(1i)	Password	
	Domain	
uluilu cisco	Local	A Marcele Dr.
	Login	

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

≡		dude Multi Site Or	chestrator		Cluster Status 3/3	0 💶
۵	Dashboard					
	Sites	Sites				
*	Schemas	Q				ADD SITE
ф	Tenants					
L	Users	SITE NAME/LABEL	SITE TYPE	CLOUDSEC ENCRYPTION	APIC CONTROLLER URLS	· · · · ·
٠	Admin 🗸					

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	¢	×
Cor	nnection 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		
	* PASSWORD		
	Off		
	* APIC SITE ID		
	1		
	SEOGRAPHICAL LOCATION		
		SAVE	

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



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	Q	×
Conr	nection 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		ľ
		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, <u>https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-</u> <u>site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-211/Cisco-ACI-</u> <u>Multi-Site-Installation-Upgrade-Guide-211_chapter_011.html#id_52935</u>.

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

\equiv		diale Multi Site Oro	chestrator		Cluster Status 3/3	0 💶
0	Dashboard Sites	Sites				
*	Schemas	Q		C		ADD SITE
<u>ش</u> د	Tenants Users	SITE NAME/LABEL	SITE TYPE	CLOUDSEC ENCRYPTION	APIC CONTROLLER URLS	
٠	Admin 🗸	New York	On-Premises	Not Enabled	https://10.17.1.11 2 More	:
		San Francisco	On-Premises	Not Enabled	https://10.16.1.11 2 More	:

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

Fabric Connectivit	ty Infra DEPLOY Q	Q	×
SETTINGS	Control Plane BGP		
0	BGP PEERING TYPE		
General Settings	full-mesh	~	
SITES	KEEPALIVE INTERVAL (SECONDS)		
	60		
• San Francisco	HOLD INTERVAL (SECONDS)		
DISABLED	180		
	STALE INTERVAL (SECONDS)		
New York DISABLED	300		
	GRACEFUL HELPER		
	On		
	MAXIMUM AS LIMIT		
	0		
	BGP TTL BETWEEN PEERS		
	16		

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.

Fabric Connectivity Ir	nfra	(DEPLOY) Q () >	×
SETTINGS	2	SAN FRANCISCO SETTINGS	
General Settings	San Francisco	O 1 0 1 2 1 0	
SITES 1	poo pod-1 •		
o San Francisco EMABLED	SDC1-SP1 SDC1-SP2	CLOUDSEC ENCRYPTION Off APIC SITE ID	
• New York DISABLED	BGP PEEKING OFF	4 1]
		5 10.21.100 200]
		BGP AUTONOMOUS SYSTEM NUMBER	1
		BGP PASSWORD]
		OSPF AREA ID	
		7 0]
		OSPF AREA TYPE	1
		EXTERNAL ROUTED DOMAIN	1
		9 SDC1-L30UT 👻]
		OSPF POLICIES NAME NETWORK TYPE	
		msc-ospf-policy-d point-to-point	
		common/default unspecified © 10 ADD POLICY	

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).

Fabric Connectivity I	nfra				DEPLOY	Q	Q	×
SETTINGS				O P	DD-1			
General Settings	San Francisco	2	Ŏ	0	1 O 1	1	I	0
SITES 1	pop pod-1 •			OVERLAY 3 10.21.	UNICAST TEP ()			
o San Francisco								
ENABLED	SDC1-SP1	SDC1-SP2						
• New York DISABLED	BGP PEERING OFF	BGP PEERING OFF	_					

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).

Fabric Connectivi	ty Infra	
SETTINGS		SDC1-SP1
General Settings	San Francisco O	0 1 0 1 1 1 0
sites 1	100 pod-1 *	PORTS ID IP ADDRESS/SUBNET MTU
o San Francisco ENABLED	2 * SDC1-SP1 SDC1-SP2	3 1/35 10.16.1.130/30 9000 ADD PORT
• New York ENABLED	BGP PEERING ON	4 On BGP-EVPN ROUTER-ID
		5 10.21.100.1 SPINE IS ROUTE REFLECTOR Off

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).

Fabric Connectivity	y Infra	DEPLOY Q O X
SETTINGS		SDC1-SP2
General Settings	San Francisco	0 1 0 1 1 1 0
sites 1	POB pod-1 •	ID IP ADDRESS/SUBNET MTU
© San Francisco ENABLED	2 SDC1-SP1 SDC1-SP2	ADD PORT
• New York ENABLED	BGP PEERING ON BGP PEERING ON	4 On BGP-EVPN ROUTER-ID
		5 10.21.100.2 SPINE IS ROUTE REFLECTOR

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.

Fabric Connectivity In	nfra	DEPLOY & A
SETTINGS	2	NEW YORK SETTINGS
General Settings	New York	0 1 0 1 1 1 0
SITES	₽00 pod-1 *	ACI MULTI-SITE 3 On
		CLOUDSEC ENCRYPTION
San Francisco ENABLED	SDC2-SP1 SDC2-SP2	Off
0	BGP PEERING OFF BGP PEERING OFF	APIC SITE ID
New York ENABLED		4 2
		OVERLAY MULTICAST TEP
		5 10.22.100.200
		BGP AUTONOMOUS SYSTEM NUMBER
		6 65002
		BGP PASSWORD
		OSPE AREA ID
		7 0
		OSPF AREA TYPE
		8 regular 🗸
		EXTERNAL ROUTED DOMAIN
		9 SDC2-L3OUT 🗸
		OSPF POLICIES
		NAME NETWORK TYPE
		msc-ospf-policy-d point-to-point
		common/default unspecified O
		10 ADD POLICY

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)

Fabric Connectivity In the second	nfra			DEPLOY & O	×
SETTINGS				POD-1	
General Settings	New York	2	ð	0 1 0 1 1 1	0
SITES	POD pod-1 •			OVERLAY UNICAST TEP	
* San Francisco ENABLED 0 New York ENABLED	SDC2-SP1 BGP PEERING ON	SDC2-SP2 BGP PEERING ON			

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).

Fabric Connectivit	ty Infra	DEPLOY Q O X
SETTINGS		SDC2-SP1
General Settings	New York	0 1 0 1 1 1 0
SITES	pod-1 •	PORTS ID IP ADDRESS/SUBNET MTU
• San Francisco ENABLED 1	2 SDC2-SP1 SDC2-SP2	3 ADD PORT
o New York ENABLED	BGP PEERING ON BGP PEERING ON	4 On BGP-EVPN ROUTER-ID
		5 10.22.100.1 SPINE IS ROUTE REFLECTOR Off

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.

Fabric Connectivity	Infra		6 DEPLOY Q O X
SETTINGS			SDC2-SP2
General Settings	New York	Õ	
SITES	Pop pod-1 •		ID IP ADDRESS/SUBNET MTU
San Francisco ENABLED	2 5002-501	_	3 ADD PORT
o New York	BGP PEERING ON BGP PEERING O	IN	4 On
ENAGLED			5 10.22.100.2
			SPINE IS ROUTE REFLECTOR

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.



- 94
- 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.



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.

≡		diale Multi Site	e Orchestrator				Cluster Stat	us 3/3	0	
Ø	Dashboard									
•	Sites									
*	Schemas	SITE STATUS					VIEW BY	0	0	O
₫	Tenants	SITE NAME	CONTROLLER STATE	CONNECTIVITY	CLO ENC	CRITICAL	MAJOR	MINOR	WAR	NING
1	Users	San Franci	3/3	+	0	0	0	5	C)
•	Admin 🗸		2/2		0					
		New York	3/3	+	0	0	0	9	()
		SCHEMA HEALTH							¢	Ð
		-		_		_			-	
				Abo	out th	ne Heatl	Мар			
				This hea Schema	atmap wi as, to co	Il represent heal nnected Sites.	th of deployed Mul	ti-Site		
				GO TO) SCHEMAS	5				

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 TENAN**T.

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

≡		diale Mu	didde Multi Site Orchestrator					r Status 3/3	0
	Dashboard								
•	Sites	Tenants	S						
*	Schemas	Q						G 0 (A	ADD TENANT
щ	Tenants								
1	Users	NAME A		DESCRIPTION	ASSIGNED TO S	ASSIGNED TO	ASSIGNED TO S	CONSISTENCY SCH	EDULER
٠	Admin 🗸	common		Common tenant for use with al	2	1	0	Set Schedule	

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).

Gen	eral Settings		
1	* DISPLAY NAME Tenant A Internal Name: TenantA DESCRIPTION		
Asso	ociated Sites		
	SITE	SECURITY DOMAINS	
2	San Francisco	TenantA 📀	~
2	New York	TenantA 😒	~
Asso	ociated Users		
C	USER	STATUS	
4 💽	admin (Admin User)	Active	
Con	sistency Checker Scheduler Settings		
	DISABLE SCHEDULER SELECT TIME 12:00 AM		
			5 SAVE
			UNIT ON THE

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, <u>https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/L4-L7-</u> <u>services/Cisco-APIC-Layer-4-to-Layer-7-Services-Deployment-Guide-401/Cisco-APIC-</u> <u>Layer-4-to-Layer-7-Services-Deployment-Guide-401 chapter 011.html</u>

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).

cisco	APIC	(New Yor	<)					admin Q	00	
System	Tenants	1 Fabric	Virtual Netv	vorking	L4-L7 Services	Admin 2 Ope	rations Ap	ps Integ	rations	
ALL TENANTS	6 Add Te	nant Ten	ant Search: name	e or descr	common	TenantA in	ifra mgmt			
i This here	has been cr	eated from	Multi-Site. It is	recommende	ed to only make cha	anges from Multi-S	ite. Please revie	w the docume	entation before n	aking any changes
TenantA				Devices						000
> C Quick St	art									
TenantA TenantA Applie	3 cation Profiles			▲ Cluster Name	Managed	Device Type	Service Type	Vendor	Mgmt IP	Exported Tenants
> 2 (9+***) > 2 Network > 2 Contr > 2 Servit > 2 Serv	actual rollies orking acts es ces 4 -1-7 S Service Parar Service Graph Router config Function Profi Devices Selet Deployed Gra Deployed Dev Device Manaq Device Manaq Device Manaq	neters n Templates urations lies clos ction Policies ph Instances rices pers	Create L4-L7 Devi Create Copy Devic	7		N Select	o items have been for Actions to create a n	und. Jewi Rem.		TETIAIRS
تی ۲۵ 🚅 (۱۵ 🚅 (Inband Manag NS Server Grou entity Server G	gement Config ips (Beta) roups (Beta)	uration for L4							

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.

Create L4-L7 Devices				_		? ×
STEP 1 > General					. Gen	eral
General Managed: 1	Devices					*
Service Type: Firewall 3	i The device mo least 3 for clus	de can be sing ter.	le, HA or cluster. Create only one o	device for single, two for HA ar	id at	8
Device Type: CLOUD PHYSICAL 4RTUAL					1	+
Physical Domain: phys 5	Name		Interfaces			- 1
Promiscuous Mode:						
Context Aware: Multiple Single 6						
Function Type: GoThrough GoTo L7 L2						- 1
						- 1
						- 1
	Cluster					- 1
	Cluster Interfaces:			Î	+	- 1
		Name	Concrete Interfaces	Encap		
						*
				Previous	Finis	sh

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).

Create Concrete Device	❷ ⊗
Name: Device	
Interfaces	2
	圖 +
Name 3 P	th <mark>4</mark>
Device V Po	d-1/Node-101-102/SDC1-FTD-DATA
ţ	Update Cancel
	6
	Cancel

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.

Devices		
		+
Name	Interfaces	
Device	Device (Pod-1/Node-101-10	2/SDC1-FTD-DATA)
Cluster		
Cluster Interfaces:		
		i +
🔺 Name	Concrete Interfaces	Encap
one-arm	Device/[Device]	✓ vlan-1199
	Update Cancel	
	Show Usage	Reset Submit

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.

alialia cisco	APIC (New York	<)								admin	٩	0	0		\$)
System	Tenants	Fabric	Virtual Ne	tworking	L4-L7 Services	Admin	Operati	ons	Apps	Integrations							
ALL TENANT	S Add Ter	nant Tena	ant Search: na	me or descr	common	mgmt	infra	Tena	ntA								
i This	s has been cre	ated from I	Multi-Site. It is	s recommer	nded to only make ch	anges from	Multi-Site.	Please	review the	documentation	before making a	any chan	ges here				
TenantA		()30	L4-L7 D	evices - SDC2-FT	D-C1										0	
> C Quick St	tart												Delieu	Fee	lto	U ista	
🗸 📆 TenantA													Policy	Fat	lits	HISTO	ry
> 🚞 Appli	ication Profiles														Ō	<u>+</u> :	*-
> 🚞 Netw	vorking			General					Devices								
> 🚞 Cont	racts			Managed:												1	+
> 🚞 Polic	ies				Name: SDC2-	FTD-C1			 Name 		Interfaces						- 1
🗸 🚞 Servi	ices				Alias:		_		Device		Device (Pod-1	/Node-10)1-102/SE	C2-FTD-	DATA)		
~ 🖬 L	4-L7				Service Type: Firewal		4										_
-	Service Param	eters		5	Physical Domain: physic	AL			Cluster								
	Service Graph	Templates		Pro	miscuous Mode:		× 5		Cluster Inter	rfaces:							_
> 🖿	Router configu	irations		FIG	Context Aware:	sia Single											+
> 🖿	Function Profil	es			Context Aware.	pre Single	4		🔺 Name	C	Concrete Interfaces				Enca	p	_
~ 🖬	Devices				Function Type: GoT	nrough Go	To L1	L2	one-arm	[Device/[Device]				vlan	2199	
>	= SDC2-FTD	-C1															
> 🖿	Imported Devi	ces															
	Devices Select	tion Policies															
> 🖿	Deployed Grap	oh Instances															
> 🖿	Deployed Devi	ces															
	Device Manag	ers															
> 🖿	Chassis																
=	Inband Manag	ement Config	uration for														
> 🚞 D	NS Server Group	ps (Beta)															
> 🖬 Id	lentity Server Gr	oups (Beta)															_

SDC2 FTD Cluster One-Arm configuration

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).

Create L4-L7 Policy-	Base	d R	edirec	t			?	×
Name	SDC1	-FTD-S	ERVICE	1				
Description	optio	nal						
Destination Type:	L1	L2	L3					
IP SLA Monitoring Policy	select	an opt	ion	\sim				
Enable Pod ID Aware Redirection:								
Hashing Algorithm:	dip	sip	sip-dip	o-prototype				
Resilient Hashing Enabled:								
Enable Anycast								2
L3 Destinations							1	+
	IP		MAC	Redirect Health Group	Additional IPv4/IPv6	Description	Oper Status	
					Con		Submit	

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 Destinat	ion Of Redirected Traffic	? >
Define Redirect Destin	ation	
IP:	10.18.90.11	1
Description:	optional	
MAC:	00:10:18:00:90:11	2
Second IP:		
Redirect Health Group:	select an option 🗸	
		2
		3
		Cancel OK

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 Destinat	tion Of Redirected Traffic	? ×
Define Redirect Destin	nation	
IP:	10.18.90.12	
Description:	optional	
MAC:	00:10:18:90:00:12 2	
Second IP:		
Redirect Health Group:	select an option V	
		3
	Cancel	ОК

e.

102

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

Create L4-L7 Policy-E	Based Re	edirect				?	×
Name:	SDC1-FTD-S	ERVICE					
Description:	optional						
Destination Type:	L1 L2	L3					
IP SLA Monitoring Policy:	select an opt	ion	\sim				
Enable Pod ID Aware Redirection:							
Hashing Algorithm:	dip sip	sip-dip-pr	ototype				
Resilient Hashing Enabled:							
Enable Anycast:							
L3 Destinations:						Ī	+
	IP	MAC	Redirect Health Group	Additional IPv4/IPv6	Description	Oper Status	
	10.18.90	00:10:18				Enable	d
				Can	cel	ubmit	

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/2x/L3 config/b Cisco APIC Layer 3 Configuration Guide/b Cisco APIC Layer 3 Config uration Guide chapter 011.html#task CA462A15DDFE4A85A1382D5F6589CB59. We created the VRF under the tenant and followed Step 4 in the guide.

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

CISCO APIC (San Francisco	o)				admin Q	00	
System Tenants 1 Fabric Vi	rtual Networking	L4-L7 Service	es Admin	Operations	Apps Integ	grations	
ALL TENANTS Add Tenant Tenant Se	arch: name or descr	com	mon TenantA	2 mgmt infra	l.		
i This has been created from Multi- changes here.	Site. It is recomme	nded to only make	e changes from N	lulti-Site. Please i	eview the docum	entation before m	aking any
TenantA (P) (C) (O)	Networking -	/RFs					
> CP Quick Start							0 🛓 🎌 -
Application Profiles	 Name 	Alias	Segment	Class ID	Policy Control Enforcement Preference	Policy Control Enforcement Direction	Description
> Bridge Domains	TenantA		2818048	16386	Enforced	Ingress	
External Routed Networks							
> Contracts							
> 🚍 Policies							
> 🚞 Services							

1	03

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

Create VRF		? 🛇
STEP 1 > VRF		1. VRF
Name:	TenantA 1	^
Alias		
Description:	c optional	
Tags		
1030.	enter tags separated by comma	
Policy Control Enforcement Preference:	Enforced Unenforced	
Policy Control Enforcement Direction:	C Egress Ingress	
BD Enforcement Status:		
Endpoint Retention Policy:	select a value	
	This policy only applies to remote L3 entries	
Monitoring Policy:	Select a value	
DNS Labels:		
Deute Tee Delieu	enter names separated by comma	
Route Tag Policy.	select a value	
IP Data-plane Learning:	C Disabled Enabled	
Create A Bridge Domain:	□ 2	
Configure BGP Policies:		
Configure OSPF Policies:		
Configure EIGRP Policies:		3 🗸
	Previous Cancel	Finish

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).

CISCO APIC (San Francisco)						admin C		0		۵
System Tenants 1 Fabric Virtual I	Networking l	4-L7 Services	Admin Op	erations Apps	Integrations					
ALL TENANTS Add Tenant Tenant Search:	name or descr	commo	n TenantA 2 i	nfra mgmt						
This has been created from Multi-Site. I	t is recommende	d to only make c	hanges from Multi-	Site. Please review the	documentation k	pefore making	any chan	ges here		
TenantA () ()	External Rou	ted Networks							6	00
> C Quick Start									0	· ~ -
V 🔣 TenantA 3	 Name 	Alias	Description	PIM	BGP	OSP		V	RF -	
> C Application Profiles				No items have b	en found					
Networking 4				Select Actions to crea	ite a new item.					
External Bridged Networks										
External Routed Networks	uted Outside 6									
> E Route Maps for BGP Dampening, mc										
> 🚞 Set Rules for Route Maps										

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).

Create Routed Ou	utside		?⊗
STEP 1 > Identity		1. Identity 2. External EP	G Networks
Name:	SDC1-L3OUT	Provider Label:	*
Alias:		enter names separated by comma	
Description:	optional	Consumer Label: enter names separated by comma	
		BGP EIGRP SPF 4	
Taga		OSPF Area ID: 0.0.0.2 5	
Tays.	enter tags separated by comma	OSPF Area 🗹 Send redistributed LSAs into NSSA area	
PIM:		Control: Originate summary LSA	
Route Control Enforcement:	Import Zexport	6 Usuppress forwarding address in translated LSA	
Target DSCP	Unspecified	OSPF Area Type: NSSA area Regular area Stub area	
VRE	TenentA	OSPF Area Cost: 1	
External Pouted Domain:		2	
Deute Deefle fee leterleele		3	
Route Prome for Interleak.	select a value		
Route Control For Dampe	ning:		
Note conterror bumpe	ing.		- +
	Address Family Type	Route Dampening Policy	
Nodes and Interfaces Prot	tocol Profiles		7
			tin 🕂
Name	Description	DSCP Nodes	
			-
		Previous	Next

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

Create Node Pr	ofile			(?	×
Name:	SDC1-L3OUT		71			
Description:	optional					
Target DSCP:	Unspecified		~			2
Nodes:				1	Ì	+
	Node ID	Router ID	Static Routes	Loopback Address		
OSPF Interface Profiles:						+
	Name	Description	Interfaces	OSPF Policy		
				Cancel OK)

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

Select Node		?⊗
Node IE	D: SDC1-LF1 (Node-101) V 1	
Router IE	2 10.16.255.129 2	
Use Router ID as Loopback Address	s: 🖌	
Loopback Addresses:		i +
	P	
Static Routes:		+
	IP Address Next Hop IP Track Pol	licy
-		3
		Cancel OK

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

Select Node				?	X
Node IE): SDC1-LF2 (Node-102) 🗸 🗸	I			
Router IE	0: 10.16.255.130	2			
Use Router ID as Loopback Address	SI 🔽				
Loopback Addresses:				Û	+
	IP				
Static Poutos:					
Static Routes.					+
	IP Address	Next Hop IP	Track Policy		
				3	
			Cancel	OK	

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

Create Node Pr	ofile				?	X
Name:	SDC1-L3OUT					
Description:	optional					
Target DSCP:	Unspecified		~			
Nodes:					1	+
	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	ОК	

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

Create Interface Profile	e					?	×
STEP 1 > Identity		1. Identity	2. Pro	otocol Profiles	3.1	Interfaces	
Name:	SDC1-L3OUT						
Description:							
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 V						
Custom QoS Policy:	select a value						
NetFlow Monitor Policies:						Ŵ	+
	NetFlow IP Filter Type		NetFlo	w Monitor Policy			
Config Protocol Profiles:							
				Previous	Cancel	Next	

j. In Step 2, click Next.

Create Interface	e Profile						(?×
STEP 2 > Protocol Pro	ofiles			1. Identity	2. Protocol Pro	files	3. Interfaces	
OSPF Profile Authentication Type:	No authenticati	on	\sim					
Authentication Key:								
Confirm Key:								
OSPF Policy:	select a value		\sim					
BFD Interface Profile								
Authentication Type:	No authenticati	on	\sim					
BFD Interface Policy:	select a value		\sim					
HSRP Interface Profile								
Enable HSRP:								
HSRP version:	version 1	version 2						
HSRP Interface Policy:								
HSRP Interface Groups:							Ť	+
	Name	Group ID	IP	MAC	Group Name	Group Type	IP Obtain Mode	
					Previous	Cance	el Nex	

k. In Step 3, select $\ensuremath{\text{SVI}}$ and click the + sign.

Create Interfa	ace Profile				8 8
STEP 3 > Interface	S	1. Identity	2. Protocol F	Profiles	3. Interfaces
		Ro	uted Interfaces	SVI	Routed Sub-Interface
SVI Interfaces					+
Path	IP Address	MAC Addre	ess	MTU	(bytes)
			Prev	vious	Cancel OK

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		00
Path Type:	Port Direct Port Channel Virtual Port C	hannel 1
Path:	SDC1-L3OUT	
Description:	optional	
Encap:	VLAN VIAN 1197 3	
Encap Scope:	VRF Local	
Auto State:	disabled enabled	
Mode:	Access (802.1P) Trunk Access (Untag	(ged)
Side A IPv4 Primary / IPv6 Preferred Address:	10.16.255.129/29 4	
Side A IPv4 Secondary / IPv6 Additional Addresses:	t	<u> </u>
	Address IPv6 DA	D
	10.15.255.131/29 enabled	5
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:	t	± +
	Address IPv6 DA	D
	10.16.255.131/29 enabled	1 7
Side B Link-Local Address:		
MAC Address:	00:22:BD:F8:19:FF	
MTU (bytes):	inherit	
Target DSCP:	Unspecified 🗸	
		8
		Cancel
m. Repeat steps a through I to configure the SDC2-L3OUT. Refer to screenshots below details.

SDC2-L3OUT configuration

CISCO APIC (New York)			а	dmin Q	0	•	\$
System Tenants Fabric Virtua	al Networking L4-L7 Services	Admin Operations	Apps Integration	ıs			
ALL TENANTS Add Tenant Tenant Search	name or descr common	TenantA infra mgm	t				
i This has been created from Multi-Site	e. It is recommended to only make ch	anges from Multi-Site. Please	review the documentation	on before mal	king any ch	anges here	
Transfer							
	L3 Outside - SDC2-L3OUT						00
> 🗘 Quick Start			Summary	Policy	Stats	Faults	History
TenantA			,				
Application Profiles				Main	Node Pr	ofiles	Networks
Networking Rridge Domains	8 🗸 🛆 🕐					Ó	<u>+</u> **-
	Properties						
External Bridged Networks	Name:	SDC2-L3OUT					
External Routed Networks	Allas:						
> 💳 Route Maps for BGP Dampening, In	Description:	optional					
> 🚞 Set Rules for Route Maps							
> 🚞 Match Rules for Route Maps	Tags:	✓					
V 🔿 SDC2-L3OUT		enter tags separated by comma					
Logical Node Profiles	Global Alias:						
V = SDC2-L3OUT	Provider Label:						
Logical Interface Profiles	Consumer Label:	enter names separated by comma					
✓		enter names separated by comma					
OSPF Interface Pro	Target DSCP:	Unspecified ~					
Configured Nodes	PIM: Route Control Enforcement:	Import Export					
> Networks							
Koute map for import and export	VRF:	TenantA V					
	Resolved VRF: External Routed Domain:	SDC2-I 3OUT					
> = Policies	Route Profile for Interleak:	select a value					
> 💳 Services	Enable BGP/EIGRP/OSPF:	BGP OSPF					
	OSPF Area ID:	0.0.0.2					
	OSPF Area Control:	0					
		Send redistributed LSAs into NS	SA area				
		Suppress forwarding address in	translated LSA				
	OSPF Area Type:	NSSA area Regular area	Stub area				
	OSPF Area Cost	1					
	Create Default Leak Policy:						

SDC2-L3OUT Node Profile

APIC (New York)				admin			۵
System Tenants Fabric Virtua	al Networking L4-L7 Service	es Admin Opera	itions Apps	Integrations			
ALL TENANTS Add Tenant Tenant Search	name or descr	nmon TenantA infra	mgmt				
(i) This has been created from Multi-Site	e. It is recommended to only mal	ke changes from Multi-Site	e. Please review the	documentation before m	aking any ch	anges here.	
TenantA (F) (T) (T)	Logical Node Profile - SD	C2-L3OUT					0.0
> 🕞 Quick Start					D.F		U U
🗸 🧱 TenantA					Policy	Faults	History
Application Profiles	8 🗸 🛆 🕐					Ó	<u>+</u> %-
V Providence Networking	Properties						
> Bridge Domains	Name: Description:	SDC2-L3OUT					
> VKFs	boonpion.						
External Bridged Networks	A.P						
	Alias:	Lipppoolfied					
Set Rules for Route Maps	Target DSCP:	Unspecified	<u> </u>				
> 📩 Match Rules for Route Maps	Noues.	Nodo ID	Poutor ID	Loonback Address			
V 📤 SDC2-L3OUT		topology/pod=1/podo=101	10.17.255.101	10.17.255.101			
Logical Node Profiles		topology/pod-1/node-101	10.17.255.101	10.17.255.101			
✓		topology/pod-1/hode-102	10.17.255.102	10.17.255.102			
💛 🚞 Logical Interface Profiles							
✓ ■ SDC2-L3OUT							
SPF Interface Pro							
> Configured Nodes	Create BGP Protocol Profile:						
E Reute men for import and even							
Koute map for import and export							
> Contracts							
> Policies							
> 🚞 Services							
				Show Usag	ge Ré		

SDC2-L3OUT SVI configuration

SVI				(. ?	×
		Р	olicy	Faults	Hist	ory
8 🗸 🔇				Q	<u>+</u>	**-
Properties						
Path:	topology/pod-1/protpaths-101-102/pat	thep-[SDC2-L30	UT]			
Path Description:						
Description:	optional					
Encap:	VLAN VINCE 2197					
Encap Scope:	VRF Local					
Auto State:	disabled enabled					
Mode:	Access (802.1P) Trunk Acces	s (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				til 1	+	
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	Clos	se		

Step D: Add Schema with Multi-Site Orchestrator GUI

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



Multi-Site Schema for Stretched Bridge Domain across multiple sites





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





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.

≡		dude Multi Site Orchestrator		Cluster Status 3/3
0 0	Dashboard Sites	Schemas		
* —	Schemas Tenants	۹		C O ADD SCHEMA
	Users	NAME A	TEMPLATES	TENANTS
\$	Admin 🗸		No Schema has been created.	

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.

🔀 Service Integratio	n Schema 1	AUTO SAVE SAVE O X
TEMPLATES	L3OUT-PBR-STR-BD	DEPLOY TO SITES
L3OUT-PBR-STR-BD	2	
SITES	• To build your schema please click here to select a tenant	3
	 Application profile 	
	O Add EPG	

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

👷 Service Integrati	on Schema	AUTO SAVE SAVE 🔿 🗙
TEMPLATES	L3OUT-PBR-STR-BD DEPLOY TO SITES	TENANT
L3OUT-PBR-STR-BD	To build your schema please click here to select a	SELECT A TENANT
SITES	tenant	common Common tenant for use with all other tenants
		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)

	L3OUT-PBR-STR-BD	
L3OUT-PBR-STR-BD	EI TEPS	
	TENANT TENANT A	IMPORT 👻
	Add Sites	×
	NAME ASSIGN TO TEMPLATE	_
	New York	~
	San Francisco	~

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.

🔀 Service Inte	egratio	n Schema		AUTO SAVE	Ø	×
TEMPLATES	0	L3OUT-PBR-STR-BD	DEPLOY TO SITES	TENANT Tenant A		
L3OUT-PBR-STR-BD		Applied to 2 sites		SELECT A TENANT		
SITES	0			Tenant A	8 ~	
New York	^	TENANT Tenant A		^		
L3OUT-PBR-ST 👳	A		2 SAN FRANCISCO			
San Francisco	^	Application profile	NEW YORK			
L3OUT-PBR-ST 🝵	A	Add EPG				

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

Import from S	Import from San Francisco			
POLICY TYPE		SELECT TO IMPORT	Q	INCLUDE RELATIONS
APPLICATION PROFILE	0 out of 0	1 🔽 TenantA		
EPG	0 out of 0			
EXTERNAL EPG	0 out of 0			
CONTRACT	0 out of 0			
FILTER	0 out of 0			
VRF	1 out of 1	2		
BD	0 out of 1			
SERVICE GRAPHS	0 out of 0			
				3 IMPORT

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.

_※ Service Integrat	on Schema	🔽 AUTO SAVE SAVE 🔿 🗙
TEMPLATES	L3OUT-PBR-STR-BD	DEPLOY TO SITES VIA One-Arm
L3OUT-PBR-STR-BD	Applied to 2 sites	LOCAL RELATIONSHIPS EXTERNAL RELATIONSHIPS
SITES	FILTERS	
New York	Tenanta	On-Premi Ready Cloud Ready
L3OUT-PBR-ST 👳 🚯		UUMMUN PRUPERTIES
San Francisco 🔥	BRIDGE DOMAIN	* DISPLAY NAME
L3OUT-PBR-ST 🙍 🚯		Name: One-Arm
	0	DESCRIPTION
	FILTER	h.
		DEFINE SERVICE NODES
	0	
		Firewall Load Balancer Other
	EXTERNAL EPG	3
		0
		Firowall
	SERVICE GRAPH	
	* One-Arm	

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).

_张 Service Inte	egration	Schema	AUTO SAVE SAVE 🔿 🗙
TEMPLATES	0	San Francisco Lacit de Berlov to Sites	NA SERVICE GRAPH One-Arm
L3OUT-PBR-STR-BD		Looi-Fbr-sik-bb	
SITES	0	FILTERS	
New York L3OUT-PBR-ST @	^ 8	TENANT Tenant A	* DISPLAY NAME One-Arm Name: One-Arm
San Francisco	^	1 CONTRACT	DESCRIPTION
L3OUT-PBR-ST 🕤	9	VBF	SITE LOCAL PROPERTIES
		TenantA	
		BRIDGE DOMAIN	- reveal
		EXTERNAL EPG	
		2 One-Arm	Device selection is required for each nodes. Click on node to select device.

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

Select Devices		×
Firewall	SDC1-FTD-C1	
		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.

🔀 Service Integ	ration S	Schema			AUTO SAVE SAVE	e o ×
TEMPLATES	•	L3OUT-PBR-STR-BD	DEPLOY TO SITES		N/A External EPG External	
L3OUT-PBR-STR-BD	1				LOCAL RELATIONSHIPS	EXTERNAL RELATIONSHIPS
SITES	0	FILTERS			U	0
New York	~	PRIDE DOMAIN		^	On-Prem Ready	Cloud Ready
L3OUT-PBR-ST	0	UNDUC DOMAIN			* SELECT SITE TYPE	
San Francisco	^				ON-PREM	CLOUD
L3OUT-PBR-ST ·	0	0		h	COMMON PROPERTIES	
					* DISPLAY NAME	
		FILTER			3 External	
					Name: External	
		0			* VIRTUAL ROUTING & FOR	WARDING
					4 TenantA	0 ×
					CONTRACTS	
		EXTERNAL EPG	SELECT ;		NAME	TYPE
					CONTRACT	
		* 0 2		١.		
		External		U.	UN-PREM PROPERTIES	
					SUBNETS	
		SERVICE GRAPH			5 O SUBNET	
		• One-Arm			Include in preferred group)
	<			>		

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

Add Subnet	×
* CLASSIFICATION SUBNET O.0.0/0 SHARED ROUTE CONTROL SUBNET SHARED SECURITY IMPORT SUBNET	
SA	VE

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.

TEMPLATES L3OUT-PBR-STR-BD SittEs New York L3OUT-PBR-ST	
L3OUT-PBR-STR-BD SITES New York L3OUT-PBR-ST. • • San Francisco LSOUT-PBR-ST. • • I San Francisco I Substrate I I I I I I I I I I I I I	0 I 0 I 0 I 0 TEMPLATE PROPERTIES * DISPLAY NAME External Name: External VIRTUAL ROUTING & FORWARDING TenantA CONTRACTS
SITES New York L3OUT-PBR-ST	TEMPLATE RAPERTIES * DISPLAY NAME External Name: Edemal VIRTUAL ROUTING & FORWARDING TenantA CONTRACTS
New York LJOUT-PBR-ST	* DISPLAY NAME External Name: External VIRTUAL ROUTING & FORWARDING TenantA CONTRACTS
San Francisco	VIRTUAL ROUTING & FORWARDING TenantA CONTRACTS
PILTER EXTERNAL EPG	N/A SUBNETS CLASSIFICATION SUBNE 0.0.0.0/0 INCLUDE IN PREFERRED GROUP
2 External SERVICE GRAPH	SITE LOCAL PROPERTIES *LOUT 3 SDC1-L3OUT

d. Repeat step c. for the New York site

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.

_送 Service Inte	🔀 Service Integration Schema							Q	Ō	×
TEMPLATES	0		L3OUT-PBR-STR-BD	DEPLOY TO SITES		filter N-S				
L3OUT-PBR-STR-BD		1	Applied to 2 sites		h	LOCAL RELATION	SHIPS	EXTERNAL	RELATIONS	HIPS
SITES	Θ		FILTERS			COMMON PROPE	RTIES			
New York	^		BRIDGE DOMAIN		^	* DISPLAY NAM	E			_
L3OUT-PBR-ST	A					N-S Name: N-S				
L3OUT-PBR-ST	Â		0			ENTRIES				
						NAME	ETHERT	YPE		
			FILTER		1	C ENTRY				
			• 2		ł					
			EXTERNAL EPG	SELECT :	L					
			• External							

- 121
- b. Enter **permit-all** in the name field and click **SAVE**.

permit-all		
DESCRIPTION		
ETHERTYPE		
unspecified	~	
IP PROTOCOL		
unspecified	~	
DESTINATION PORT RANGE FROM		
unspecified		
DESTINATION PORT RANGE TO		
unspecified		
ON-PREM PROPERTIES		
MATCH ONLY FRAGMENTS		
STATEFUL		
ARP FLAG		
unspecified	~	

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

F	ILTER			
	• N-S	• E-W	• Telemetry	0
				L

Step 7: Create Bridge Domains

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

_業 Service Inte	egratior	n Schema	■ AUTO SAVE SAVE Q O X
TEMPLATES	0	L3OUT-PBR-STR-BD	BRIDGE DOMAIN WP-WEB
L3OUT-PBR-STR-BD		Applied to 2 sites	LOCAL RELATIONSHIPS EXTERNAL RELATIONSHIPS
SITES	0	FILTERS	0 0 COMMON PROPERTIES
New York	^		* DISPLAY NAME
L3OUT-PBR-ST	A		2 WP-WEB
San Francisco	~	• O TenantA	Name: WP-WEB
L3OUT-PBR-ST	A		ON-PREM PROPERTIES
			* VIRTUAL ROUTING & FORWARDING
		BRIDGE DOMAIN	3 TenantA S V
		• WP-WEB 0 1	L2 STRETCH
			INTERSITE BUM TRAFFIC ALLOW
		PILYER	OPTIMIZE WAN BANDWIDTH
		• • • • • • • • • • • • • • • • • • •	L3 MULTICAST 💿
			L2 UNKNOWN UNICAST
		EXTERNAL EPG SELECT	proxy 🗸
		_	SUBNETS
			GATEWAY IP
		External	4 O SUBNET

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

Add Subnet	×
* GATEWAY IP	
10.18.107.1/24	
DESCRIPTION	
SCOPE Private to VRF Advertised Externally SHARED BETWEEN VRF'S	
NO DEFAULT SVI GATEWAY	
QUERIER	
	SAVE

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).

B	RIDGE DOMAIN			
	• WP-WEB	• WP-APP	• WP-DB	
	• FTD	•		

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).

Service Integration S	chema	
TEMPLATES O	L3OUT-PBR-STR-BD DEPLOY TO STEE	LOCAL RELATIONSHIPS EXTERNAL RELATIONSHIPS
L3OUT-PBR-STR-BD	Applied to 2 sites	0 0
SITES O	FILTERS	On-Prem Ready Cloud Ready
New York	TENANT Tenant A MPORT V	* DISPLAY NAME 2 N-S-ExtToWeb
San Francisco 🔺	Application profile	Name: N-S-ExtToWeb
LJOUT-PBR-ST •	O Add EPG	SCOPE VIT V APPLY BOTH DIRECTIONS
	CONTRACT * N-S-ExtToWeb 1	PLTER CHAIN NAME DIRECTIVE ACTION N-Sig none O FLTER
	* TenantA	SERVICE GRAPH 4 One-Arm Consumer EPG
	BRIDDE DOMAIN	
	* * * WP-WEB WP-APP WP-DB	5 Frewall
	* FTD	Provider EPG
4		Consumer and Provider connector configurations are required for service nodes. Click on node to select connector settings.

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

Configure Firewall				×
	Consumer EPG	Firewall	Provider EPG	
CONSUMER CONNECTOR				
* BRIDGE DOMAIN				
WP-WEB		0 ×		
PROVIDER CONNECTOR				
* BRIDGE DOMAIN 📕 🚯				
FTD		0 ×		
				DONE

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

🔀 Service Inte	egration S	Schema	AUTO SAVE SAVE @ O X
TEMPLATES	0	San Francisco	N-S-ExtToWeb
L3OUT-PBR-STR-BD		L3001-PBR-SIR-BD	
SITES	0	FILTERS	TEMPLATE PROPERTIES
New York L3OUT-PBR-ST	^ 0	Tenant A	DISPLAY NAME N-S-ExtToWeb Name: N-S-ExtToWeb
San Francisco	^	CONTRACT	SCOPE
L3OUT-PBR-ST 💿	• 1	N-S-ExtToWeb 2	context service graph One-Arm
			SITE LOCAL PROPERTIES
		VRF	ONE-ARM
		P TenantA	Consumer EPG
		BRIDGE COMAIN	SDC1-FTD
		WP-WEB WP-APP WP-D8	Provider EPG
		FTD	Consumer and Pirovider cluster interfaces are required for service nodes. Click on node to select cluster interface.

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 Firewall Provider PPG	
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.

New York L3OUT-PBR-ST o	^ 	TENANT Tenant A		ŕ	DISPLAY NAME N-S-ExtToWeb Name: N-S-ExtToWeb
San Francisco L3OUT-PBR-ST	^ _	V-S-ExtToWeb			SCOPE context SERVICE GRAPH One-Arm SITE LOCAL PROPERTIES
		VBF TenantA			ONE-ARM
		BRIDEE DOMAIN WP-WEB	WP-DB		Provider EPG

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

CONTRACT			
N-S-ExtToWeb	E-W-WebToApp	F-W-AppToDB	
-			
TelemetryToExt			

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.

😵 Service Inte	egratic	n Schema		AUTO SAVE SAVE	Q	¢	×
	0	L3OUT-PBR-STR-BD Last Depkyed: Jun 9, 2019 08:22 pm DEPLOY TO SITES Applied to 2 sites warmen	ED	NA APPLICATION PROFILE WordPress			Q
SITES	0	FILTERS		* DISPLAY NAME 3 WordPress Name: WordPress			
L3OUT-PBR-ST •	õ	TRANIT Tenant A MPORT V	Å				
San Francisco	õ	an WordPress *					
		2 SELECT :					
		Application Profile	1				

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.

_業 Service Inte	egration	Schema	_ AL	UTO SAVE SAVE	Q	Q	×
TEMPLATES	0	L3OUT-PBR-STR-BD DEPLOY TO STITES	(Â
L3OUT-PBR-STR-BD		Applied to 2 sites	12		EXTERNAL REL	ATIONSHIP	5
SITES	0	FILTERS		On-Prem Ready	Clo	ud Ready	
New York	^	TEMANT Tenant A	j.	COMMON PROPERTIES			
San Francisco	A	WordPress e		* DISPLAY NAME			.
L3OUT-PBR-ST	A		2	WEB			
		PO SELECT		CONTRACTS			
		• Add EPG 1		NAME	TYPE		. 1
				E-W-WebToApp	consu	Θ	
		Application Profile	4	N-S-ExtToWeb	provider	0	
				TelemetryToExt	consu	0	
		CONTRACT	3	CONTRACT			1
			lle.	ON-PREM PROPERTIES			
		N-S-ExtToWeb E-W-WebToApp E-W-AppToDB		* BRIDGE DOMAIN			
		PROVIDED CONSUMED	5	WP-WEB	¢	• ·	
		• •		SUBNETS			
		CONSUMED		GATEWAY IP			
			6	10.18.107.1/24		0	
		VBF		SUBNET			. 1
				USEG EPG			
		TenantA		USEG ATTR			
				N/A			
		BRIDGE DOMAIN		INTRA EPG ISOLATION			
				 Enforced Unenforced 			

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

APP EPG

TENANT TENANT A		IMPORT	•	COMMON PROPERTIES		
AP WordPress				APP		
EPG		SELECT	8	Name: APP		
WEB APP DB	• Telemetry	O Add EPG		E-W-WebToApp	provider	۵
				E-W-AppToDB TelemetryToExt	consu	0
CONTRACT				CONTRACT		
				ON-PREM PROPERTIES		
N-S-ExtToWeb E-W-WebToApp	 E-W-AppToDB CONSUMED 			* BRIDGE DOMAIN	0	~
• Telemetru/ToEvt		-		SUBNETS GATEWAY IP		
CONSUMED				10.18.108.1/24		Θ

DB EPG

		COMMON PROPERTIES	
TENANT Tenant A	IMPORT 🗸	* DISPLAY NAME	
AP WordPress		DB	
	SELECT :	Name: DB	
		NAME	TYPE
• • • • • • • • • • • • • • • • • • •	C Add EPG	E-W-AppToDB	provider 😋
	<u> </u>	Telemetry ToExt	consu 🕲
Application Profile		CONTRACT	
CONTRACT		ON-PREM PROPERTIES	
• • •		* BRIDGE DOMAIN	
N-S-ExtToWeb E-W-WebToApp E-W-AppToDB		WF-DB	0
PROVIDED	_	SUBNETS GATEWAY IR	
• O		10.18.109.1/24	0
CONSUMED		SUBNET	
CONSUMED		SUBNET	

Telemetry EPG

	0	0
FILTERS	On-Prem Ready	Cloud Ready
A	COMMON PROPERTIES	
TENANT Tenant A	* DISPLAY NAME	
AP WordPress	Telemetry	
	Name: Telemetry	
EPG SELECT	CONTRACTS	
	NAME	TYPE
WEB APP DB Telemetry OAdd EPG	Telemetry ToExt	consu 😨
	CONTRACT	
O Application Profile		
	ON-PREM PROPERTIES	
CONTRACT	* BRIDGE DOMAIN	
	FTD	o ~
• • •		
N-S-ExtToWeb E-W-WebToApp E-W-AppToDB	SUBNETS	
	GATEWAY IP	
	SUBNET	
TelemetryToExt	USEG EPG	
CONSUMED		

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).

🔀 Service Inte	egration	Schema			3 ×
TEMPLATES	0	L3OUT-PBR-STR-BD	LOY TO SITES	External EPG External	Q
L3OUT-PBR-STR-BD		Applied to 2 sites		LOCAL RELATIONSHIPS EXTERNAL R	LATIONSHIPS
SITES	0	FILTERS		On-Drom Ready) ourd Roady
New York	^	CONNECTED		▲ On-Piell Ready C	ouu neauy
L3OUT-PBR-ST	A	BRIDGE DOMAIN		* SELECT SITE TYPE	
San Francisco	^			ON-PREM CLOU	
L3OUT-PBR-ST	A			COMMON PROPERTIES	
		WP-WEB WP-APP WP-DB		* DISPLAY NAME	
				External	
		FTD		Name: UntitledExternalEPG1	
				TenantA	a v
		FILTER			-
				NAME TYPE	
		• • • •		N-S-ExtToWeb consu.	. 0
		N-S E-W Telemetry		Telemetry ToExt provid	r ©
				2 CONTRACT	
		EXTERNAL EPG	ECT !		
				ON-PREM PROPERTIES	
		1 External		SUBNETS	
				CLASSIFICATION SUBNE	-
		SERVICE OD ANA		O SUBNET	0
		JERTILE URAPH			
				Include in preferred group	
		One-Arm			
	4		•	*	

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.



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

APIC (Nev	v York) admin 🝳 🛆 🗭 😨 🐯
System Tenants Fa	bric Virtual Networking L4-L7 Services Admin Operations Apps Integrations
ALL TENANTS Add Tenant	I Tenant Search: name or descr I common I TenantA I infra I mgmt
i This has been created changes here.	from Multi-Site. It is recommended to only make changes from Multi-Site. Please review the documentation before making any
TenantA () ()	Application Profile - WordPress
> C • Quick Start ∨ Ⅲ. TenantA	Summary Topology Policy Stats Health Faults History
Application Profiles	● =
	Contract EPG USe Any B V M R OSt K CF OSh 12 13 447 C m Q Q Q O
 Contracts Policies Services 	Relation Indicators Configured Operational Show All On Click Provider Intra EPG Provider (from Master)
	WEB CB Teemetry APP Exemal Consumer (From Master) (WordPress) (WordPress) (WordPress) Exemal Intra EPG (from Master)
	V V V Cancel Submit

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 <u>https://www.Cisco.com/c/en/us/td/docs/security/firepower/APIC/quick-start/quide/ftd-apic-gsg-103.html</u>.

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

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

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

Implementation Procedure

Step 1

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).

Overview Analysis Policies I	Devices O	bjects AMP	Intelligence	e Deploy	0 0 Syste	em Help 🔻	admin 🔻
2 Configuration Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻 1	Monitoring 🔻	Tools 🔻
							Savo
							Jave
Access List	Carble D						5
Process	Enable R						
Audit Log Certificate							
Audit Log							
Login Banner							
Change Reconciliation							
DNS Cache							
Dashboard							
Database							
External Database Access							
Email Notification							
Access Control Preferences							
HTTPS Certificate							
Information							
Intrusion Policy Preferences							
Language							
Management Interfaces							
Network Analysis Policy Preferences							
Remote Storage Device							
► REST API Preferences	3						
SNMP							

Step 2

a. Download Firepower Threat Defense Device package from Cisco.com, https://software.Cisco.com/download/home/286259687/type/286320228/release/1.0.3.1 3

cisco	Products & Servio	ces Support	How to Buy	Training & Events	Partners	Q			
Software Download									
Downloads Hon / Firepower Th	e / Security / Fire reat Defense Device	walls / Firewall Manag Package for ACI- 1.0	ement / Firepowe 3.13	er Management Center	Virtual Appliance				
C Search Expand Al Latest Relea	Collapse All se ~	Firepov Release 1.	wer Man ^{0.3.13}	agement (Relater Quick Sta Release 1 XML exar	Center V d Links and E Int Guide Notes for 1.0.3.13 mples	Irtual App	liance		
All Release	~								
1.0	>	File Information Cisco FTD Dev 1.0.3.13 for Ci a ftd-fi-device-pk	ice Package - F sco APIC 3.2(1I) g-1.0.3.13.zip	abric Insertion (FI)) & FMC 6.2.3	Release Date 04-JUN-2018	Size 0.12 MB	ظ ب		

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).

cisco APIC				٩	00		*
System Tenants Fabric	virtual Net	working 1 L4	L-L7 Services	Admin Op	perations	Apps	
		Inven	tory Packages	2			
Packages 🕞 🗉 💿	L4-L7 Ser	vice Devid	ce Types				9
C Quick Start						0	<u>+</u> **+
3 V 🔤 L4-L7 Service Device Ty	Vendor	🔺 Model	Version	Functions			
> CISCO-ASA-1.3	rt Device Package	4 _{ASA}	1.3	Firewall			
> CISCO-ASA_FI-1.3	ade Devices Package	ASA_FI	1.3	Firewall			
> CISCO-CloudMode-1.0	CISCO	CloudMode	1.0	FW, LB			
> E CISCO-FTD_FI-1.0	CISCO	FTD_FI	1.0	FTD			

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).

cisco APIC		
System Tenants Fabri	c Virtual Networking 1 L4-L7 Services Admin Operations Apps	
	Inventory Packages 2	
Packages () = 0 Quick Start 2 = L4-L7 Service Device Ty	L4-L7 Service Device Type - CISCO-FTD_FI-1.0	? жу
> CISCO-ASA-1.3	· · · · · · · · · · · · · · · · · · ·	
CISCO-ASA_FI-1.3 CISCO-CloudMode-1.0	Properties Vendor: CISCO uluulu Model: FTD_Fl 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 Interface Labels: Name external internal mgmt	

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.

cisco APIC					٩	0	0	•	٩
System Tenants Fabric Virtual Networking L4-L7 Servic	es Admin	Operations Apps							
ALL TENANTS Add Tenant Tenant Search: name or descr	antB common	infra L3out-service-PBR m	gmt						
Tenant TenantB 🚯 🗐 💿	Device Ma	nagers							0 0
> 💽 Quick Start								0	<u>+</u> **
V 🧱 Tenant TenantB	 Name 	Management EPG	Device Manager Type	Management Address					
> Application Profiles	FMC	default	CISCO-FTDmgr_FI-1.0	10.9.10.41:443					
> in Networking									
> Contracts									
> III Policies									
V Services									
✓ III L4-L7									
Service Parameters									
> IIII Service Graph Templates									
> IIII Router configurations									
> Imil Function Profiles									
> me Devices									
> Imported Devices									
> Devices Selection Policies									
Deployed Graph Instances									
> Deployed Devices									
Create Device Manager									
Inhand Management Configuration for L4-L7 devices									
DNS Server Groups (Beta)									
> 🔛 Identity Server Groups (Beta)									

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.

cisco APIC						٩	0	0	•	0
System Tepants Fabric Virtual Networking 4-17 Serv	ices Admin Operatio	ons 4	Anns							
ALL TENANTS Add Tenant Tenant Search: pame or descr	anantă i common i infra i	L 13out-se	ervice-PBR I mamt							
Tenant TenantB 🕥 🕤 💿	Device Manager -	- FMC								00
> O Quick Start								Policy	Faults	History
- III Terrant Terrant8							-	_		
> Application Profiles	0000								0 1	*-
> 📰 Networking	Properties									
> E Contracts	Name:	FMC								
) 🛅 Policies	Management EPG:	This is requir	v 🛃							
V IIII Services	Device Manager Type:	pelect an	option 🗸 🛃							
✓	Manangement:				+					
Service Parameters		A Host		Port						
> 🔚 Service Graph Templates		10.9.10.	41	443						
> Router configurations										
> Function Profiles										
> IIII Devices										
> 🛅 Imported Devices										
> The Devices Selection Policies	Osemanie.	aciadmin								
> E Deployed Graph Instances	Confirm Password									
> Deployed Devices	Cluster Screen	Name								
V III Device Managers		SDO1.T	P. CTDL. UA							
FMC-			D-CIDV-IM							
Chasais										
Inband Management Configuration for L4-L7 devices										
DNS Server Groups (Beta)										
> 🔚 Identity Server Groups (Beta)										

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.

cisco APIC						٩	0000
System Tenants Fabric Virtual Networking L4-L7 Serv	ices Admin Opera	ations Apps					
ALL TENANTS Add Tenant Tenant Search: name or descr Te	enantB common infra	L3out-service-PE	IR mgmt				
	-						
Tenant TenantB 🚺 🗐 💿	Devices						0 🖯
> 🗘 Quick Start							0 ± ***
V 🧱 Tenant TenantB	 Cluster Name 	Managed	Device Type	Service Type	Vendor	Mgmt IP	Exported Tenants
> Application Profiles	SDC1-TB-FTDv-HA	True	VIRTUAL	Firewall	CISCO	10.9.10.41	
> Retworking							
> Contracts							
> Policies							
✓ IIIII Services							
✓ □ L4-L7							
Service Parameters							
> Service Graph Templates							
> Router configurations							
> Function Profiles							
> Device							
> Em Import							
> Device							
> E Deployed Graph Instances							
> Deployed Devices							
> Device Managers							
Chassis							
Inband Management Configuration for L4-L7 devices	1						
DNS Server Groups (Beta)							
> 🔚 Identity Server Groups (Beta)							

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.

cisco APIC						٩	0	0	•	0
System Tenants Fabric Virtual Networking L4-L	.7 Services Admin Operations Apps									
ALL TENANTS Add Tenant Tenant Search: name or descr	TenantB common infra L3out-service-PBR mgmt									
Tenant TenantB) ⊚ L4-L7 Devices - SDC1-TB-FTDv-HA									00
> 🗘 Quick Start						Policy	Paran	neters	Faults	History
Tenant TenantB Definition Profiles	8 🗸 🕲								0 ±	***
> 🔛 Networking	General	Devices								
> Contracts	Managed: 🜌									+
> Policies	Name: SDC1-TB-FTDy-HA	 Name 	VM Name	vCenter Name	Management Address	Management Port	Interfac	es		
V Services	Device Package: CISCO-ETD_EI-1.0	Device 1	vFTD1	SDC-vCenter	10.16.6.54	443	Gigabit	Ethernet()/0	
✓ □ L4-L7	Service Type: arewall	Device2	vFTD2	SDC-vCenter	10.16.6.55	443	Gigabit	Ethernet	0/0	
Service Parameters	Device Type: VIRTUAL									
> Service Graph Templates	Trunking Port:	Cluster				-				
> Router configurations	VMM Domain: VMware/SDC1-VMM Promisculaus Mode:	Management I	P Address: 10.9.	10.41	Port: 443	el.				
> IIII Function Profiles	Context Aware: Multiple Signle	Of the Interference	e Manager: Tena	ILD/FMC						_~ ℃
Devices	Hungard Colline	Cluster Interface	15:							
SDC1-TB-FTDv-HA	Function Type: GoThrough GoTo	Type		 Name 	Concr	ete Interfaces				Ŧ
> Imported Devices	Credentials	consumer		external	Devic	e1/[GigabitEthernet()/0], Devid	ce2/[Giga	bitEtherne	t0/0]
> Devices Selection Policies	Username: aciadmin				Devic	e1/(GigabitEthemet(VOL Devic	se2/lGina	bitEtherne	10/01
> Deployed Graph Instances	Password:	provider		internal						
> Deployed Devices	Confirm Password:									
> Device managers	Configuration State									
Indexed Management Conferentian for L4.1.7 devices	Configuration Issues:									
 Initiana wanagement Contiguration for L4-L7 devices DNS Secure Groups (Reta) 	Devices State: stable									
Diva derver Groups (Beva)										
 identity server groups (Beta) 										



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).

cisco APIC			
System1 Tenants Fabric Virtual Networking	L4-L7 Services 2	Admin Operations	Apps
ALL TENANTS Add Tenant Tenant Search: name or descr	TenantB	common infra L3out	-service-PBR mgmt
Tenant TenantB () () () () () () () () () () () () ()	4-L7 Services Fi	unction Profile Gro	oup - FTDv
> Application Profiles	8 7 4 0		
 Networking Contracts Policies Services 	Properties Name: Alias: Description: Service Function Profiles:	FTDv	
4		 Name 	Associated Function
Service Parameters		FTDv-InlineMode	FTD
Service Graph Templates		FTDv-RoutedMode	FTD
5 V Function Profiles		FTDv-RoutedMode-onearm	FTD
V 🛢 ASAV		FTDv-TransparentMode	FTD
ASAv-RoutedModelPv4 ASAv-RoutedModelPv4Cloud ASAv-RoutedModelPv4Cloud ASAv-RoutedModelPv4HA ASAv-TransparentModelPv4HA FTDv FTDv FTDv FTDv FTDv Asete FTDv Create L4-L7 Services Function Profil	8		

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

Create L4-L7	7 Se	ervices F	unction Profile							?⊗
Create Function Pr	ofile									
		Name: FTDv-	RoutedMode-onearm 1							
	Descr	iption: optiona	al							
Copy Existing Profile	Param	neters: 🔽 2								
F	F	Profile: CISCO	-FTD_FI-1.0/RoutedModeFor	FTD 3			✓ 4			
 Features and Paramet 	ters —		Note: In order to sutomatics	ally apply paw yalue	e to the naram	paters of an existing graph in	etanca whan usars mod	the function		
			profiles, the name of the top	o folder must end w	rith "-Default".	leters of an existing graph in	Istance when users mou	ny function		
Features		Basic Parame	ters All Parameters							
Interfaces			Folder/Parameter	Name	Hint	Path from Schema	Value	Mandatory	Locked	Shared
All			V Device Config	Device						^
			> Access Policy	ACIAccPolicyR					false	false
1			> 📄 Bridge Group Int							
			> 🔛 Inline Set							
			> 📄 Interface	externalInterface					false	false
			> interface	internalInterface					false	false
			> E Security Zone	ConsSZRT					false	false
			> E Security Zone	ProvSZRT					false	false
			V Function Config	Function						
			> E Access Policy C	AccessPolicyF					false	false 🔻
									_	5
								Car	ncel	Submit

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 external interface is used in creating the policy, which implements the one-arm deployment.

L4-L7 Services F	unction Profile - FTDv-Ro	outedMode-o	nea	m				•
						General	Faults	History
8 👽 🛆 🕦						/	0 ±	**
Properties								
Name:	FTDv-RoutedMode-onearm							
Description:								
Associated Function:	CISCO-FTD_FI-1.0/FTD							
Features and Pa	rameters							
Features	Basic Parameters All Parameters							
Interfaces	Folder/Parameter	Name	Hint	Path from Schen	Value	Mandatory	 Locked 	Shared
All	V E Device Config	Device			-			
	Access Policy	SDC1-TB-FTDv-HA					false	false
	~ 🚞 Access Rules	App-to-DB					false	
	V 🔚 Destination Interface	DBZone					false	
	E 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	
	V 🔚 Access Rules	Outside-to-Web					false	
	V Destination Interface	WebZone					false	
	E 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	UneArm					false	false
	> Function Config	Function						

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

4-L7 Services	Function Profile - FTDv-Ro	utedMode-onearm				00
				General	Faults	History
80000				/	0 ±	**-
Properties Nan Descriptie	ne: FTDv-RoutedMode-onearm on:					
eatures and F	Parameters					
Features	Bais Duranters All Descriptor					
Interfaces	Folder/Parameter	Name Hint Pa fro Sc	th Value m hema	Mandatory	 Locked 	Shared
Al	V 🚞 Device Config	Device				
	> Access Policy	SDC1-TB-FTDv-HA			false	false
	✓	externalInterface			false	false
	V 🚞 IPv4 Address Configuration	IPv4Config			false	
	V 🔚 Use Static IP	static			false	
	F IP Address	address	10.19.90.12/24	true	false	
	V Static Routes List	StaticRoute			false	
	V 📰 IPv4 Static Route	IPv4StaticRoute			false	
	F Metric	metric	1	false	false	
	F Gateway	gateway	10.19.90.1	true	false	
	F Network.	network	0.0.0/0	true	false	
	Interface Security Zone	int_security_zone			false	
	E Security Zone	security_zone	OneArm	false	false	
	Enabled	enabled	true	false	false	
	E Logical Name	ifname	Consumer	false	false	
	Security Zone	UneArm			talse	false
	Т уре	type	ROUTED	false	false	
	V 🚞 Function Config	Function				
	✓	AccessPolicyFolder			false	false
	Access Policy Configuration	InAccessPolicyRel	SDC1-TB-FTDv-HA	false	false	
	External Interface Configuration	ExtConing			raise	raise
	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.

cisco APIC		
System Reports Fabric Virtual Networking L4-L7 Serv	ces Admin Operations Apps	
ALL TENANTS Add Tenant Tenant Search: name or descr T	ment common i infa i 13out-service-PBR i mont	
Tenant TenantB 🚯 🕥 🔿	Service Graph Templates	60
> 💽 Quick Start		0 ± %-
V 🗰 Tenant TenantB	Name Function Nodes Description	
> Application Profiles	No items have been found.	
> E Networking	Select Actions to create a new Rem.	
> Contracts		
> E Policies		
V Services		
~ 🔚 L4-L7		
Service Parameters		
Service Graph Templates Create L4-L7 Service Graph Template		
> Router configurations		
> Eurotion Profiles		
V Devices		
> SDC1-TB-FTDV-HA		
> IIIII Imported Devices		
Devices Selection Policies		
Deployed Graph Instances		
Deproyed Devices		
> Charles		
Inband Management Configuration for L4-L7 devices		
DNS Server Groups (Beta)		
> 🔚 Identity Server Groups (Beta)		
b. Create One Arm PBR Service Graph with FTDv HA

Create I 4-I 7 Service Graph Te	mplate		08
Drag device clusters to create graph nodes.	inplace		
Davico Clustors	Service Graph Name: SDC-OneArm Graph Type: Oreate a New Graph	Clone an Existing Graph	
svcType: FW ImantB/SDC1-TB-FTDv-HA (Managed)	Consumer	C P SDC1-TB-F	Provider
	SDC1-TB-FTDv-HA Information	FTDV-HAI	
	Firewall: Routed Control Route Redirect:	Transparent edMcde-one 🔽 🛃	
			Cancel

Step 8

a. Apply L4-L7 Service Graph

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		
Consumer EPG / External Network: TenantB/TB-L3OUT/TB-Ext-EPG 🗸 🗗 Provider EPG / Internal Network: TenantB/opencant/epg-Web-EPG 🗸 🗗 🕕		
Contract Information		
Contract Contract O Choose An Existing Contract Subject		
Contract Name: Outside-to-Web		
No Filter (Allow All Traffic):		
Prev	ous Cancel	Next

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

Apply L4-L7 Service Graph Template To EPGs	08
STEP 2 > Graph	1. Contract 2. Graph 3. SDC1-TB-FTDv-HA Configuration
Config a Service Graph	
Service Graph TenantB/SDC-OneArm V	
Consumer (FPG TB-Ext-EPG FTDv-HA	Provider EPG Web-EPG
Policy-based Routing: true Consumer Connector Type: @ General @ Route Peering	1
BD: TenantB/FTD-BD	
L3 Destination (VIP): Redirect Policy: TenantB/FW-PBR-Policy Cluster Interface: Levtermal	
Provider Connector Type: © General © Route Peering	
BD: TenantB/FTD-BD	
L3 Destination (VIP): Redirect Policy: TenantB/FW-PBR-Policy	
Cluster Interface: Internal	v
	Previous Cancel Next

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

STEP 3 > SDC1-TB-FTDv-HA Configuration Config parameters for the selected device Profile Name: FIDv-RoutedMode-onearm Features Required Parameters All Interfaces Folder/Parameter Al Device Cos Device Cos Devi	All Parameters r Config ess Policy je Group Interface i Set lace	Name Device SDC1-TB-FTD	1. Contract 2. Graph Value	3. SDC1-TB-FTDv-HA Configuration Write Domain
Config parameters for the selected device Profile Name: FTDV-RoutedMode-onearm Features Required Parameters Interfaces Folder/Parameter Al Device Co Device Co	r Config ess Policy ye Group Interface t Set lace	Name Device SDC1-TB-FTD	Value	Write Domain
Profile Name: FTDv-RoutedMode-onearm C Features Required Parameters All Interfaces Folder/Parameter Al Device Co S > Device Co S = S = Device Co S	r Config Less Policy ye Group Interface t Set Jace	Name Device SDC1-TB-FTD	Value	Write Domain
Features Required Parameters All Interfaces Folder/Parameter All > Device Co > > All > > Endge > > Interface > > Typ > > Function Co 	r Config Less Policy ye Group Interface t Set lace	Name Device SDC1-TB-FTD	Value	Write Domain
Interfaces Folder/Parameter	r Config Iss Policy ye Group Interface I Set Jace	Name Device SDC1-TB-FTD	Value	Write Domain
Interfaces Folder/Parameter Al Let a constrain the second secon	r Config iss Policy je Group Interface i Set Jace	Name Device SDC1-TB-FTD	Value	Write Domain
All	Config iss Policy je Group Interface i Set lace	Device SDC1-TB-FTD		ŕ
Image: Second secon	es Policy je Group Interface i Set lace	SDC1-TB-FTD		
> ■ Bridge > ■ Inline S > ■ Interfac ✓ Securit ✓ ■ Typ ● ✓ ■ Function C ✓ ■	je Group Interface Set Jace			
 ⇒ interfac ⇒ interfac ✓ Securit ✓ Typ ✓ Function C 	e Set Vace			
→ interfac	face			
✓		externalinterface		
Typ	rity Zone	OneArm		
😑 🗸 🔛 Function C	ype	type	ROUTED	
	Config	Function		
Access	ess Policy Configuration	AccessPolicyF		
> 🛅 Bridge	e Group Interface Configuration			
Sim Externa	nal Interface Configuration	ExtConfig		
> 🔤 Internal	nal Interface Configuration	IntConfig		-

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-EP3 🗸 🔮 🕕		
Contract Information Contract ID Create A New Contract Choose An Existing Contract Subject Contract Name: Web-to-App No Filter (Allow All Traffic): 7		

f. Create App-to-DB Contract

Apply L4-L7 Service Graph Template To EPGs		08
STEP 1 > Contract	1. Contract	2. Graph
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 Contract Contract Contract Contract 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.

Overview Analysis Policies Devices Obje	ects AMP Intelli	gence				Deploy	02 System	Help 🔻	admin 🔻
Device Management NAT VPN VQoS	Platform Settings	FlexConfig	Certificates						
Device Management List of all the devices currently registered on the Firepower M	anagement Center.								
View By : Group All (12) Error	(0) Warning (0) (Offline (1)	Normal (11) D	eployment Pending (0)		Search	n Device		Add 👻
Name	Model	Version	Licenses	Access Control Policy	Group				
4 💋 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			0	*	
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 Availability	it						0° 4* 1	Ø	
FW-DC-1 10.16.4.26 - Routed	Cisco Firepower 4110 Threat Defense	6.2.3	Base, Threat, Malware, URL Filtering	SDC-Services			0	R	
FW-DMZ-1 10.16.4.25 - Routed	Cisco Firepower 4110 Threat Defense	6.2.3	Base, Threat, Malware, URL Filtering	Internet-Edge			0 6	*	
SDC1-FTD-C1 Cisco Firepower 9000 Series SM-36 Threat Defense	c						a 6		
SDC2-FTD-C1 Cisco Firepower 4110 Threat Defense Cluster							0 6		
B-FTDv-HA Cisco Firepower Threat Defense for VMWare High Av	νē						@ 4* (¢ €	
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.

Over	view Analysis Po	licies Devices	Objects	AMP Intel	ligence			Deploy 🕛 System H	lelp 🔻 admin 🔻
Devic	e Management	IAT VPN V	QoS Platfo	rm Settings	FlexConfig	Certificates			
TB-F	TDv-HA							E Si	ave 🛛 😢 Cancel
Cisco Fi	repower Threat Defense	for VMWare							
Sum	mary High Availa	bility Device	Routing	Interfaces	Inline Sets	DHCP			
								area Sync Device	Add Interfaces •
St	Interface	Logical Name		Туре	Security Zones		MAC Address (Active/Standby)	IP Address	
Θ	GigabitEthernet0/0	Consumer_TenantB	_SDC1-TB-FTD	. Physical	OneArm_Tenant	B_SDC1-TB-FTDv-HA	0010.1900.9012	10.19.90.12/24(Static)	ø
0	🕼 GigabitEthernet0/1			Physical					ø
0	₿ GigabitEthernet0/2			Physical					ø
0	🔯 GigabitEthernet0/3			Physical					a
0	😰 GigabitEthernet0/4			Physical					6
0	🕅 GigabitEthernet0/5			Physical					Ø
0	😰 GigabitEthernet0/6			Physical					Ø
Θ	GigabitEthernet0/7			Physical					9
Θ	GigabitEthernet0/8			Physical					۹,
θ	Diagnostic0/0	diagnostic		Physical					Ø

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

	!	0					,								
Overview Analysis	Policies Devices Objects	AMP Intelligence									De	ploy 0 ₅	System H	elp 🔻 ad	lmin v
Access Control + Access	Control Network Discovery	Application Detectors Co	orrelation Actions •												
SDC1-TB-FTDV-	HA antB_SDC1-TB-FTDv-HA:												E Sa	ve 🛛 🙁	Cancel
Prefilter Policy: Default Prefi	iter Policy	SSL Po	licy: None		Identity	Policy: Non	le								
											Te Ir	heritance Se	ttings 📑 Poli	cy Assignme	ents (1)
Rules Security Intellig	ence HTTP Responses Advanc	ed													
B Filter by Device							Show P	tule Conflicts 🌜	Add 🔾	Category	Add Rule	Search Rul	85		×
Name #	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T	Users	Applicat	Source	Dest Po	URLs	ISE/SG	Action	😈 🐚 🔎 😈		
➡ Mandatory - SDC1-TB-	FTDv-HA (-)														
There are no rules in this sec	tion. Add Rule or Add Category														
▼ Default - SDC1-TB-FTD	v-HA (1-3)														
1 Web-to-App	A OneArm_TenantB_SDC1-TB-FTDv-H	H# 🚠 OneArm_TenantB_SDC1-TB	-FTDv- 📰 Web-10.19.107	📰 App-10.19.108	Any	Any	Any	Any	Any	Any	Any	🛹 Allow	00.81	1 [] 1	6
2 App-to-DB	A OneArm_Tenant8_SDC1-TB-FTDv-H	H# 🚠 OneArm_TenantB_SDC1-TB	-FTDv- 📰 App-10.19.108	📰 DB-10.19.109	Any	Any	Any	Any	Any	Any	Any	Allow	00.81	1 .	08
3 Outside-to-Web	A OneArm_TenantB_SDC1-TB-FTDv-H	H/ 🚠 OneArm_TenantB_SDC1-TB	-FTDv-	💭 Web-10.19.107	Any	Any	Any	Any	Any	Any	Any	🛹 Allow	UDBI	1	1 8
Default Action									A	cess Control:	Block All Traffi				~

Test Case 3 – Tetration and VMware vCenter

There are three distinct parts to this integration:

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

guidance in test cast 4 for how to enable NetFlow in VDS for ACI and in non-ACI environments that can be used to send to Cisco Tetration NetFlow Virtural Appliance. Refer to VMware vSphere Distributed Switch (VDS) and NetFlow section in Test Case 4.

Test Description:

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



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 Sever 2016 and CentOS Linux 7.4 enforcement agents in all those 3 tier applications. We followed the documentation that is in the Tetration Analytics Appliance.

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

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

Step 2

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

vmware [®] vSphere Web	o Cli	ent 1			
		6	Home	Ctrl+Alt+1	
Navigator	.	🕑 vCe	Hosts and Clusters	Ctrl+Alt+2	C Act
A Back		Gettin	VMs and Templates	Ctrl+Alt+3	Permi
🔰 🖻 目 🔮	2	Ē	Storage	Ctrl+Alt+4	
		Wha ≶	Networking	Ctrl+Alt+5	
▶ DC1-SF		vCe [Content Libraries	Ctrl+Alt+6	
Femp DC		mul	Global Inventory Lists	Ctrl+Alt+7	
		envi 💡	Policies and Profiles		
		like d	Update Manager		
		mac	Administration		2
		syst	Taska		1
		Wet 🖉	Tasks		
		"par –	Events		l l
		() () () () () () () () () ()	7 Tags & Custom Attribute	s	
		have 🤇	New Search		
		with with	Saved Searches		
		Admin	istration section, will appe bry to the left.	ear in your	

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



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

tetadmin1 - Edit		?
Enter values for this u	user, including the password.	
User name:	tetadmin1	
Current Password:		
Password:	***	0
Confirm password:	***	
First name:	Tetration	
Lastname:	Admin	
Email address:		
Description:		
	OK	Cancel

 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 Cli	ient n ≘		U Launch vSphere	Client (HTML5) Administrator@VSPHERE.LOCAL • Help
Navigator I	🐣 vCenter Users and Groups			
Back	Users Solution Users Groups 2			
Administration + Access Control	+ / X Group Name	Domain		Q Filter
Roles	ExternalIDPUsers	vsphere.local	1	Well-known external IDP users' group, which registers e
Global Permissions	ComponentManager.Administrators	vsphere.local	1	Component Manager Administrators
✓ Single Sign-On	DCAdmins	vsphere.local		
Users and Groups	LicenseService.Administrators	vsphere.local	1	License Service Administrators
1 Configuration	ActAsUsers	vsphere.local		Act-As Users
Licensing 3	Administrators	vsphere.local		
Licenses	DCClients	vsphere.local		
Reports	CAAdmins	vsphere.local		
- Solutions	SystemConfiguration.Administrators	vsphere.local		Well-known configuration users' group which contains all
Client Plug-Ins	SolutionUsers	vsphere.local		Well-known solution users' group, which contains all solu
vCenter Server Extensions	SystemConfiguration.BashShellAdministra	ators vsphere.local	1	Access bash shell and manage local users on nodes
- Deployment	Users	vsphere.local	1	
System Configuration >				
Customer Experience Im				
- Support				
Upload File to Service Re				
	46			12 items 🔒 Export 👻 🏠 Copy 🗸
	Group Members			
4				Q Filter
	User/Group	Description/Full name	Domain	Member Type
	Administrator	Administrator vsphere.local	vsphere.local	User
	aciadmin1	ACI Admin	vsphere.local	User

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

🧭 Cisco Tetrati	DASHBOARD - FLOWS
🔟 VISIBILITY 🗸 🗸	fiews 🗗 Dashboard
Dashboard	
Flow Search	ov 26 1:24pm 👻
Inventory Search	ddresses
Inventory Filters	
Inventory Upload	
External Orchestrators	
Neighborhood	
APPLICATIONS	0 5k

f. Select Create New Configuration

œ.	Cisco Tetr	rati«n"	EXTERN	al o	RCHESTRATORS				OpenCart	🎨 Monitorin	g ¥	0 -	Q0 -
<u>س</u> ۴	Filters 😡	Enter attrib	outes				S Filter			+ Crea	te Ne	w Config	uration
U	Name	¢	Туре	¢	Description	÷	Created At	•	Connection Status	\$	Ac	tions	¢
æ	SDC-vCenter	-2	vcenter		SDC vCenter 6.5		Nov 15 03:11:37 pm (PST)		Success		1	Û	
<u> </u>							TetrationOS Software, Version 3.1.1.53						
					(1) (1) (1) (1)		Privacy and Terms of Use TAC Support: http://www.cisco.com/tac © 2015-2018 Cisco Systems, Inc. All rights reserved.						
ŗ													

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

Edit External Orchestrator Configuration	
Typ Basic Config	e vcenter -
Hosts List Nam	e SDC-vCenter-2
Descriptio	n SDC vCenter 6.5
Delta Interval (s	i) 60
Full Snapsho Interval (s	it 3600
Usernam	e tetadmin1@vsphere.local
Passwor	d Password for the orchestration endpoint
Insecur	e 🗆

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

Edit External Orch	estrator Configuration	
Basic Config	Hosts List + .com 443 X	<u></u>
Hosts List		

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).

vmware [,] vSphere Web Client	î€			ت ا لـ	aunch vSphere Client ((HTML5) kn	guyen@vsphere.local 👻	l Help -	1 Q
Navigator 1	Home Hosts	and Clusters	Ctrl+Alt+1 Ctrl+Alt+2 Ctrl+Alt+3						
n Home	Stora	je	Ctrl+Alt+4						
 IF Hosts and Clusters IF VMs and Templates IF Storage Networking Content Libraries IF Global Inventory Lists 	 Netwo Conte Globa Polici Upda Admir 	orking nt Libraries I Inventory Lists es and Profiles ee Manager nistration	Ctrl+Alt+5 Ctrl+Alt+6 Ctrl+Alt+7 d 33	Storage	Networking	Content Libraries	Global Inventory Lists		
Policies and Profiles	Tasks	5		8					
Administration 2	 Tags Q New S Saved 	& Custom Attributes Search	ole	VM Storage Policies	Customization Specification Manager	Update Manager	Host Profiles		
Events									
Tags & Custom Attributes		25		2	1 8				
 New Search Saved Searches 	>	Roles	System Configuration	Licensing	Customer Experience Improvement	vRealize Operations Manager			
		Plug-ins for Insta	llation						
		O,	4						
		vRealize Orchestrator	Hybrid Cloud Manager						
		Watch How-to	Videos						

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.

vmware [®] vSphere Web Client	ft≡		U Launch vSphere	Client (HTML5) knguyen@	/sphere.local 🕶 Help 👻 🔍
Navigator	Ŧ	🤊 Tags & Custom Attributes			
A Back		Getting Started Tags Cust	tom Attributes		
🚰 Home		2			
Hosts and Clusters	>	Tags Categories			
VMs and Templates	>				
Storage	>		t . Description	Multiple Continuity	Q Filler
Q Networking	>	Category Name		and the cardinanty	All Types
Content Libraries	>	Mew Category		4 §	
Global Inventory Lists	<u> </u>	Category Name:	OpenCart		
Policies and Profiles	>	Description:			
🚳 Update Manager	>	Cardinality:	 One tag per object 		
Section 44 Administration	>	Associable Object Types:	 Many tags per object 		
🗊 Tasks		Abbolable object types.	All objects	^	
wents			Cluster		
Tags & Custom Attributes			Datacenter		
Q New Search	>				
Saved Searches	>		Datastore Cluster		
			Distributed Port Group		
			Distributed Switch		
			Folder	•	
			ОК	Cancel	
		•			Þ
		24			1 items 📑 Export 🗕 🏠 Copy 🗸

c. Select Tags tab.

vmware [®] vSphere Web Client	† ≡		U Laund	h vSphere Client (HTML5) knguyen@	vsphere.local 🕶 Help 👻 🝳
Navigator	Ŧ	🧳 Tags & Custom Attr	ibutes		
Back		Getting Started Tags	Custom Attributes		
付 Home					
Hosts and Clusters	>	Tags Categories			
VMs and Templates	>	\$			
Storage	>	Category Name	1 . Description	Multiple Cardinality	Associable Entities
Q Networking	>	Category Name	I A Description	No	All Types
Content Libraries	>	C opendar			, an i jpoo
Global Inventory Lists	>				
Policies and Profiles	>				
🚳 Update Manager	>				
administration	>				
🗊 Tasks					
The Events					
Tags & Custom Attributes					
🔍 New Search	>				
Saved Searches	>				
		4	::		Þ
		44			1 items 📑 Export 🗝 Copy 🕶

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.

vmware vSphere Web Client				U Launch vSphere Client	(HTML5) knguyen(@vsphere.local 🕶 Help 👻 🝳
Navigator	Ŧ	🧭 Tags & Custom Attri	ibutes			
A Back		Getting Started Tags	Custom Attri	butes		
🛱 Home						
Hosts and Clusters	>	Tags Categories				
Ø VMs and Templates	>					
Storage	>	1 🖉		Categories:	All Categories	▼ Q Filter ▼
Q Networking	>	Tag Name	1 🖌	Category	Description	
🗐 Content Libraries	>	App		OpenCart		
🐻 Global Inventory Lists	>		_	Opencian		
Policies and Profiles	>	🏷 New Tag		(?) >>		
🚳 Update Manager	>	Name:	Web			
🍇 Administration	>	Description:				
🕄 Tasks		Category:	OpenCart	•		
w Events			OpenCart			
Tags & Custom Attributes			New Category	Cancel		
Q New Search	>					
Saved Searches	>					
-						
		44				3 items 🕒 Export 👻 🏠 Copy 🗸

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

vmware [®] vSphere Web Client 1	≜		ויס	Launch vSphere Client	(HTML5) kng	uyen@vsphere.local 👻	Help + 🔍
Navigator	Home	Ctrl+Alt+1					
4 Back	Hosts and Clusters	Ctrl+Alt+2					
	VMs and Templates	Ctrl+Alt+3	om Attributes				
A Home	Storage	Ctrl+Alt+4					
Hosts and Clusters	Metworking	Ctrl+Alt+5					
VMs and Templates	Content Libraries	Ctrl+Alt+6		Cotogorias			
Storage	Global Inventory Lists	Ctri+Ait+7		Calegories.	All Categories		•
🧕 Networking	Policies and Profiles		1 A Category		Description		
Content Libraries	🚳 Update Manager		OpenCart				
nventory Lists	🍇 Administration		OpenCart				
Policies and Profiles	😴 Tasks		OpenCan				
🔊 Update Manager	Events						
Kadministration	🧭 Tags & Custom Attributes	3					
Taska	🔍 New Search						
Evente	层 Saved Searches						
Lventa		_					
Tags & Custom Attributes							
🔍 New Search	>						
- Saved Searches	>						
	86					3 items 🔒 Expo	ort 👻 📑 Copy 🗸
						·	

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).

vmware [®] vSphere Web Client	U Launch vSphere Client (HTML5) knguyen@vsphere.local • Help • Q
Navigator I	🚯 web2-tb-linux 🛛 💕 🕞 🛢 🇐 📇 🛛 🎯 Actions 🗸 🗮
Image: Second	Getting Started Summary Monitor Configure Permissions Snapshots Datastores Networks Update Manager
 Gottal Destant SDC1-SF SDC1-SF SDC1-SF gesxi-2.sdc1.cisco-x.com gesxi-2.sdc1-centos gesxi-2.sdc1-centos<td>Guest 05: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Compatibility: ESXI 6.0 and later (VM version 11) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) VMware 100: Running, version:2147483647 (Guest Managed) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) DNS Name: app2-tb Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Image: PAddresses: 192 (163.122.1) View all 3 IP addresses Image: Cent05 4/5/67 (64-bit) Host: esxH-2.sdc1.cisco-x.com Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit)</td>	Guest 05: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Compatibility: ESXI 6.0 and later (VM version 11) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) VMware 100: Running, version:2147483647 (Guest Managed) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) DNS Name: app2-tb Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Image: PAddresses: 192 (163.122.1) View all 3 IP addresses Image: Cent05 4/5/67 (64-bit) Host: esxH-2.sdc1.cisco-x.com Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit) Image: Cent05 4/5/67 (64-bit)
	VM Hardware Advanced Configuration
 app-tb-win app-4-sdc1-win centOS-3 wp3.sdc1.cisco-x.com app1.sdc-m.cisco-x.com centOS-4 db3-sdc1-centos sxi-5.sdc1.cisco-x.com db3-sdc1-centos db3-sdc1-centos db4-sdc1-win db4-sdc1-win db4-sdc1-win web1.sdc-m.cisco-x.com meth.sdc-m.cisco-x.com 	 Tags Assigned Tag Category Description This list is empty. This list is empty. This list is empty. Attribute Value This list is empty. This list is empty. This list is empty. Edit. • Related Objects Host esxi-2 sdc1.cisco-x.com Networks Storage ISO1
	ESXi-2-DataStore1
	VApp Details VM Storage Policies
	VIdate Manager Compliance VM Storage Policies - Status
	VM Storage Policy Compliance Scan Detailed Status Last Checked Date
	Check Compliance

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.

📀 web2-tb-linux - Ass	sign Tag			(?)
*	Categories:	All Categories	▼ Q Filter	•
Tag Name	1 A Category		Description	
🧭 Арр	OpenCart			
🧳 DB	OpenCart			
Web	OpenCart			
4				•
м			3 items 📑 Export 🗕 👔	🚡 Сору 🛨
			Assign	Cancel

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

vmware [®] vSphere Web Client	Ŭ Launch vSphere Client (HTML5) knguyen@vsphere.local + Help + Q
Navigator	🚯 web2-tb-linux 📑 🕞 🔳 🇐 🖧 🎯 Actions 🗸 🚍
A Back	Getting Started Summary Monitor Configure Permissions Snapshots Datastores Networks Update Manager
 Back ♥ vCenter-2 cisco.x.com ♥ sDC1-SF ♥ sSC1-SF ♥ sSC1-SF ♥ sSC1-set ♥ rp3.sdc1-centos ♥ vFTD2 ♥ web2tb-linux ♥ esxi-3.sdc1.cisco.x.com ♥ app-1b-win ♥ app-4.sdc1-win ♥ CentOS-3 ♥ wp3.sdc1.cisco.x.com ♥ app1.sdc1.cisco.x.com ♥ app1.sdc1.cisco.x.com ♥ centOS-4 ♥ db3-sdc1-centos ♥ esxi-5.sdc1.cisco.x.com ♥ db1-b-win ♥ db1-b-win ♥ db1.sdc-m.cisco.x.com ♥ db1.sdc-1.win ♥ web1.sdc1-win ♥ web1.sdc1-win ♥ web1.sdc-1.win ♥ web1.	Getting Started Summary Monitor Configure Permissions Snapshots Datastores Networks Update Manager Web24b-linux Guest OS CentOS 4/567 (64-bit) Compatble CentOS 4/567 (64-bit) Memory UsAge Compatble Summary Monitor Compatble CentOS 4/567 (64-bit) Memory UsAge Compatble Summary Editors CentOS 4/567 (64-bit) Memory UsAge Compatble Summary Monitor Memory UsAge Memory UsAge VMware Tools: Reinface Memory UsAge For UsAge 66.18 GB DNS Name: app2-tb Padresses Storage 66.18 GB Notes Ipp2 Catagory Description Advanced Configuration Edit Augended Tag Catagory Description Advanced Configuration Edit Augended Tag Catagory Description Advanced Configuration <t< td=""></t<>
	Check Compliance

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

Ċ	CiscoTet	rati@n*	INVENTORY	SEARCH						SecureDC	😍 Monitoring 👻	G	- (¢° -
<u>lant</u>											6	Tota	l inven	itory: 949
њ	Filters 😢	* orchest	trator_OpenC	art = Web		0	Search						Creat	e Filter
U	Showing 2 o	f 2 matching res	sults						Results restricte	ed to root scope	SecureDC with qu	ery	VRF II	D = 10
£26	T	Ho	stname		VRF	÷		Address	÷		05			÷
<u> </u>		١	Web-TB		SecureDC			10.19.107.101		M	SServer2016Datacente	r		
ب د		N	web2-tb		SecureDC			10.19.107.111			CentOS			
-					cisco	Tetration Privacy TAC Su © 2015-	nOS Software, and Terms of U ipport: http://ww -2018 Cisco Sy	Version 3.1.1.53 Jse w.cisco.com/tac stems, Inc. All rights r	reserved.					

Step 4

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



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

	Cisco Tetra	atien	SCOPES	SecureDC 😵 Monitorin	g • @ • ¢°, • 1
Last	1			Commit Scope Updates	Create New Scope
4		Sec	ana Dataila	4	Y Cancel
U		50	ope Details		× Cancer
29			Name	OpenCart	
Ā			Description	Enter a description (optional)	
				t.	
ŗ		2	Policy Priority 😡	Last	
			Parent Scope	SecureDC 🕼	
			Query 😡	* orchestrator_OpenCart = Web or * orchestrator_OpenCart = App or * orchestrator_OpenCart = DB	
			3	S Create	
		Secu	reDC 🔺 🌶 🤊		
		Filter	rs 😧 Filter Scopes		٢
	Name		•	Query Ability	

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

(C) LM	Cisco Tetra	atien	SCOPES			SecureDC	V Monitori	ng - ©	0 - 0° -
ሐ		SecureDO	A 🖌 🤊			Commit Sco	ope Updates	Create	New Scope
U		Filters 😡	Filter Scopes						٥
Ð	Name		Que	ry	Ability	o Total	Children ¢		
⊥ ▲	OpenCart		* orchestrator_OpenCart = Web or * orchestrator_OpenCart = DB	* orchestrator_OpenCart = App or	Owner		0	C Edit	Pelete
۶				View Deleted Scopes 3					
			uluili. cisco	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.					

Step 5

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



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

C	С	isco Tetrati« n°	APPLICATIO	NS							SecureDO	•	Monitoring	•	0 ·	¢°° +
Last												Enf	orcement Histor	ry	Setting	is 🕶
ф	1	Create New Applica	tion Workspace													*
U Ba		Name OpenCart						Scope Secure	DC 🗷							
Ă	2	Description Enter Application D	escription					🗹 Dynar	mic Mode ©							
ŗ		Create Application	Cancel													
	[Filters 🚱 Filter App	lications													0
		▼ Dynamic ⇔ S	tatus \$	Name	≑ Sco	pe		¢	Policy Requests	¢	Updated	•	Creator	¢	Actions	
		× .	PRIMARY ULIVE	SecureDC Rules	S	ecureDC	A		2		1:59 PM		Chris McHenry		Û	
					.1 1.1 1 cisco	Tetrati Privac TAC S © 2019	onOS Software, \ y and Terms of U upport: http://www 5-2018 Cisco Sys	/ersion 3.1.1. se w.cisco.com/t tems, Inc. All	53 ao I rights reserved.							

c. View the Application Workspace created called OpenCart.

Ċ.	Cisco Tetratien"	APPLICATION	IS					SecureDC	•	🕫 Monitoring	. 6		¢° -
ы									Enf	orcement History		Settings	•
4 5	Create New Applica	ation Workspace											>
8	Filter Optications												
Ā	▼ Dynamic ⇔ S	Status ¢	Name	¢	Scope	¢	Policy Requests	Updated	÷	Creator	¢ A	ctions	
	~	PRIMARY ULIVE	SecureDC Rules		SecureDC		2	1:59 PM		Chris McHenry	1	Û	
۶	~ 1	PRIMARY ULIVE	OpenCart		SecureDC : OpenCart			11:51 AM		Chris McHenry	1	Û	
					TetrationOS Software, Versi	on 3.1.	1.53						
				.1 1.1 CISC	Privacy and Terms of Use TAC Support: http://www.cis © 2015-2018 Cisco System	co.com s, Inc. /	Vlac Ul rights reserved.						

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.

Cisco Tetratien" APPLICATIONS	🕫 Monitoring 👻 🙆 👻
OpenCart SECONDARY SecureDC OVNAMIC Version: 0 Fonversations 0 Clusters 1 App View 0	± Switch Application ► Start ADM Run
Clusters Filter Clusters Filters Filter Clusters Displaying 1 of 1 clusters Cluster Endpoints Confidence Dynamic Approved	Q Image: Cluster: user-defined-cluster Cluster Actions Image: Cluster
2 user-defined-cluster N/A	Description View Cluster Details Edit Cluster Query Endpoints (0) Provides (0) Consumes (0)

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.

Edit Cluster	
Name	OpenCart
Description	Enter a description (optional)
Query 😡	<pre>* orchestrator_OpenCart = Web or * orchestrator_OpenCart = App or ③ * orchestrator_OpenCart = DB</pre>
	Save Cancel

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.

C.	CiscoTetratien APPLICATIONS				ę	Monitoring - 😡 - 🎝 -
Lant	OpenCart 🕝 PRIMARY					1 Switch Application
ф	SecureDC : OpenCart DYNAMIC Version:	S Endpoints: 3 Last Run	: 12:14 AM			Start ADM Run
U	D F Conversations 105	ters 1 Policies 16	Provided Service	s 👍 App View 0	Policy Analys	is D Enforcement 🔐 🕅
B	Clusters @				Q 0	
Ā	Filters 🕢 Filter Clusters		٥	Create Cluster	& Cluster: OpenC	art
	Displaying 1 of 1 clusters				Cluster Actions	4 4 1
عر	Cluster	Confidence -	Dynamic 🗘	Approved ¢	Name Ope	enCart 🗭
ŕ	OpenCart 3	Approved	≁		Description 🕝	
					View Cluster Deta	ils
					Query *	orchestrator_OpenCart = Web
					*	orchestrator_OpenCart = App
					or	
					*	orchestrator_OpenCart = DB
					Edit Cluster Quer	(
						Endpoints (3)

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

C	Cisco Tetratien Monitoring - O - O -
(a)	OpenCart @ PRIMARY 1 Switch Application
ф	SecureDC : OpenCart DYNAMIC Version: 12:14 AM
U	⑦ If Conversations 105
-	ADM Run Configuration
۵	ADM discovers security groups and policies for the members of this application using the observations in the selected time range.
	Select time range 18,492 total observations Nov 27 4.00pm - Nov 27 10.00pm - 1031101 103 107 109 1011 1013 1017 1019 1021 1023 1025 1027 Showing Flow Observations
r	Scope: SecureDC : OpenCart Time Range: Nov 27 4:00pm - Nov 27 10:00pm Member Endpoints: 3 Show Show Show
	External Dependencies
	Advanced Configurations
	Submit ADM Run

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

OpenC SecureDC	Cart @ PR	IMARY DYNAMIC Version: V	Endpoints: 3				J Switch Ap
5 4	Conversation	s 105 💩 Clus	ters 1 = Policies 16	Reprovided Services 🔒 Ap	op View 0	Policy Analysis	Enforcement
6 🔳	M I	Duick Analy	sis Filters 😧 Filter Po	licies	0	Q ()	
Absolute	Policies 0	Default Policies	5 Catch All DENY	Add Defau	It Policy		
Windows f	irewalls place	DENY rules on top in	mpacting the results below. See	User Guide for more information.		Search over en	dpoints, clusters, policies
Windows f	Action	DENY rules on top in Consumer	Provider	User Guide for more information. Services		Search over en	dpoints, clusters, policies.
Windows 1 Priority 100	Action	Consumer	Provider	User Guide for more information. Services TCP : 80 (HTTP)	ß	Search over en	dpoints, clusters, policies.
Windows 1 Priority 100 100	Action ALLOW	Consumer OpenCart OpenCart	Provider SecureDC SecureDC DNS	Services TCP : 80 (HTTP) UDP : 53 (DNS)	8	Search over en	dpoints, clusters, policies.
Windows f Priority 100 100 100	Action ALLOW ALLOW ALLOW	DENY rules on top in Consumer OpenCart OpenCart	Provider SecureDC A SecureDC: DNS SecureDC: Tetration	User Guide for more information. Services TCP : 80 (HTTP) UDP : 53 (DNS) TCP : 443 (HTTPS)	8 8 8	Search over en	dpoints, clusters, policies.
Windows 1 Priority 100 100 100 100 100	Action ALLOW ALLOW ALLOW ALLOW	Consumer OpenCart OpenCart OpenCart SecureDC	Provider Provider SecureDC SecureDC SecureDC: DNS SecureDC: Tetration OpenCart	Services TCP : 80 (HTTP) UDP : 53 (DNS) TCP : 443 (HTTPS) ICMP	8 8 8	Search over en	dpoints, clusters, policies.

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**.

C	Cisco Tetratien APPLICATIONS	🎨 M	onitoring - 😡 - 🍫 -
<u>[46]</u>			t Switch Application
ф	SecureDC: OpenCart DYNAMIC Version: v2 J Endpoints: 3 Last Run: Nov 28, 11:57 PM		Start ADM Run
U	⑦ ⁴ Conversations 105 & Clusters 1 = Policies 16 N Provided Services ▲ App View	0 Policy Analysis	Enforcement 🔐 🕅
20	Enforced Policy Version: [p2]	Alerts Stop Policy Enforce	ement Enforce Policies
۵ ۹	Select time range Nov 28 11:34am - Nov 28 12:34pm - 10/14 10/21 10/28 11/4 11/11 11/18	11/25	18,913 total observations Showing Flow Observations
بر	Filters 🕢 Enter attributes O	Filter Flows	
	Permitted Rejected	Top Hostnames - Contrib Observations. Web-TB App-TB DB-TB Unknown	uting to the selected Flow Provider Hostnames Unknown Web-TB DB-TB m

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	Enter a reason for this action (optional)
	Describe the new version (p3):
Name	Enter a name (optional)
Description	Enter a description (optional)
New host firewall rules will be hosts. Please click accept to o	inserted and any existing rules will be deleted on the relevant 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**.



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

Windows Firewall with Advance	Inbound Rules												
Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Progr	Local Address	Remote Address	Protoc	Local Port	Remote Port	Authorized Use
Cutbound Rules	Tetration GoldenRule 1	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	64.100.1.198-64	TCP	Any	5660	Any
Connection Security Kules	Tetration GoldenRule 3	Tetration Policy Group	Private	Yes	Allow	No	Any	Any	64.100.1.198-64	TCP	Any	5640	Any
in monitoring	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	Ves	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
	C 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	Ves	Allow	No	Any	10.19.107.101	Any	UDP	53 123	Any	Any
	Tetration Rule 35	Tetration Policy Group	Private	Ves	Allow	No	Any	10,19,107,101	Any	UDP	Any	53, 123	Any
	Tetration Rule 37	Tetration Policy Group	Private	Ves	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	Ves	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	Ves	Allow	No	Any	10.19.107.101	23 105 70 77 31	ICMPu4	Any	Any	Any
	Tetration Rule 47	Tetration Policy Group	Private	Ves	Allow	No	Any	10,19,107,101	10.9.10.19	UDP	137-138	Any	Any
	Tetration Rule 49	Tetration Policy Group	Private	Ves	Allow	No	Any	10.19.107.101	10.9.10.102	UDP	53	Any	Any
	Tetration Rule 5	Tetration Policy Group	Private	Ves	Allow	No	Any	10 19 107 101	10.19.107.101.1	TCP	Any	3306 8080	Any
	Tetration Rule 51	Tetration Policy Group	Drivate	Vec	Allow	No	Any	10 19 107 101	10.9.10.100.10	TCP	443	Any	Any
	Tetration Rule 52	Tetration Policy Group	Drivate	Ver	Allow	No	Any	10 10 107 101	10.9.10.100, 10	LIDP	52 127.	Any	Amu
	Tetration Rule 56	Tetration Policy Group	Private	Ves	Allow	No	Amy	2001-0-9438	Any	TCP	80 443	Any	Any
	Tetration Rule 58	Tetration Policy Group	Drivate	Ver	Allow	No	Any	2001-0-0439-	Any	TCP	Amu	80 443 5660	Any
	Tetration Rule 60	Tetration Policy Group	Drivate	Ver	Allow	No	Ame	2001-0-0429-	Any	LIDP	52 122	Anu	Anu
	Tetration Rule 62	Tetration Policy Group	Drivate	Ver	Allow	No	Amy	2001-0-0-420	Any	UDP	0.000	52 122	Any
	Tetration Rule 64	Tetration Policy Group	Private	Ver	Allow	No	Any	2001-0-0439	Any	ICMP-4	Any	33, 123	Any
	Tetration Pule 66	Tetration Policy Group	Drivate	Ver	Allow	No	Any	2001-0-0429	Any	ICMD-4	Any	Any	Any
	Tetration Rule 7	Tetration Policy Group	Drivate	Ver	Allow	No	Any	10 19 107 101	10 10 107 101 1	LIDD	123 127	Any	Any
	Tetration Rule 0	Tetration Policy Group	Private	Ver	Allow	No	Any	10.19.107.101	Anu	LIDP	Ami	122 127 442	Any
	Tetration Califbula 1	Tetration Policy Group	Drivate	Ver	Allow	No	Ame	Am.	255 255 255 255	Anu	Amy	Amu	Any
	Tatration SalfRule 11	Tetration Policy Group	Drivate	Ver	Allow	No	Any	Any	10 10 107 255	Any	Any	Any	Any
	Tatation SelfPule 2	Tetration Policy Group	Private	Ver	Allow	No	Any	Any	224 0 0 0 /4	Any	Any	Any	Any
	Tetration Serrule 3	Tetration Policy Group	Private	New Yes	Allow	NI	Any	Any	£204.0.0.0/4	Any	Any	Any	Any
	retration SelfKule 5	retration Policy Group	Private	res	Allow	NO.	Any	Апу	muuc/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.

<pre>[root@web2-tb ~]# iptables -S</pre>
-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 NFLOGnflog-group 50880
-A OUTPUT -1 TA GOLDEN OUTPUT
-A OUTPUT -1 TA-OUTPUT
-A OUTPUT -1 TA CAST
-A QUTPUT -1 NFLOGnflog-group 50880
-A TA CAST -m addrtypedst-type BROADCAST -1 ACCEPT
-A TA CAST -m addrtypedst-type MULTICAST -i ACCEPT
-A TA CAST -1 RETURN
-A TA DROP -1 NFLOGnflog-group 50660
-A TA DROP -1 DROP
-A TA GOLDEN INPUT -i lo -i ACCEPT
-A TA GOLDEN INPUT -p tcp -m setmatch-set ta b11a75d589e301459a6fb909ff60 src -m multiportsports 5660 -m conntrackctstate ESTABLISHED -i ACCEPT
-A TA GOLDEN INPUT -p tcp -m setmatch-set ta f5a83dd0cb816615ab0dd908e43e src -m multiportsports 5640 -m conntrackctstate ESTABLISHED -i ACCEPT
-A TA GOLDEN INPUT -p tcp -m setmatch-set ta 61ce598c76a8d629f3a8288b461d src -m multiportsports 443 -m conntrackctstate ESTABLISHED -i ACCEPT
-A TA GOLDEN INPUT -1 RETURN
-A TA GOLDEN OUTPUT -O LO -1 ACCEPT
-A TA GOLDEN OUTPUT -p tcp -m setmatch-set ta bl1a75d589e301459a6fb909ff60 dst -m multiportdports 5660 -m constrackctstate NEW ESTABLISHED -i ACCEPT
-A TA GOLDEN OUTPUT -p tcp -m setmatch-set ta f5a83dd0cb816615ab0dd908e43e dst -m multiportdports 5640 -m conntrackctstate NEW,ESTABLISHED -i ACCEPT
-A TA GOLDEN OUTPUT -p tcp -m setmatch-set ta 61ce598c76a8d629f3a8288b461d dst -m multiportdoorts 443 -m copptrackctstate NEW ESTABLISHED -i ACCEPT
-A TA GOLDEN OUTPUT -1 RETURN
-A TA TNPILT -p tro -m setmatch-set ta 4327ad3e3a2174b2acd49d6266c2 src -m setmatch-set ta d39506a842bc089e9657d81b9a5f dst -m multiportsports 443_5660 -m constrack -
state FSTARI ISHED -m commentcomment "PolicyId=5hfef1a9497/d4f422fdef82d" -i ACCEPT
A TA INPUT -p tcp -m setmatch-set ta a8312b0bf8e54ca326c9291073b2 src -m setmatch-set ta d39506a842bc089e9657d81b9a5f dst -m multiportdports 3306.8080 -m constrack
tstate NEW.ESTABLISHED -m commentcomment "PolicyId=5bfef1a9497d4f422fdef82b" -i 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

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.lnteger');

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

};

query = baseUrl + query + " ";

return query;

Step 2

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

	۹ 🕻		Desktop Client V					
			Global Settings					
			Central Management					
			Packet Analyzer Configura					
		2	UDP Director Configuration					
			External Lookup Configura					
≎ DT	‡ DH		User Management					

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

Stealthwatch					Q	top Client
Dashboards N	Nonitor Analyze	Jobs	Configure	Deploy		
kternal Lookup Configura	tion					
External Lookup 🔘					Add Exte	rnal Lookup
Name	Enabled				Actions	
DShield.org (Source IP)	ENABLED				\odot	
DShield.org (Target IP)					\odot	
Talos Reputation (Source IP)	ENABLED				Θ	
Talos Reputation (Target IP)	ENABLED				\odot	
Host Report (Source IP)	ENABLED				Θ	
Host Report (Target IP)	ENABLED				\odot	
OpenDNS Investigate (Source If	P) ENABLED				\odot	
OpenDNS Investigate (Target IP) ENABLED				\odot	
Tetration (Source IP)	ENABLED				\odot	
Tetration (Target IP)					\odot	
Previous 1 Next						
Step 3

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.

altala cisco	Stealthwatch Dashboards	h Monitor	Analyze	Jobs	Configure	Deploy		Desktop Client V
Externa	l Lookup Config	uration						
Externa	al Lookup 🜒							+ Add External Lookup
Externa	al Lookup : Tetratior	n (Source IP)	0					
NAME: * Tetrati	on (Source IP)					Enable looku	up of internal IP ad	dresses
BASE UR	/	/#/host/profile	/10/					
QUERY		G:						
/		Sou	rce IP Address	OTE NAME.	\sim	Required		+
URL SC	RIPT BUILDER FILE UP	LOAD:			Browse			
							Canc	el Save

Step 4

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 CISCO Dashboards Mor	nitor Analyze	Jobs	Configure	Deploy	Q U	Desktop Client V
External Lookup Configuration	วท					
External Lookup 0						+ Add External Lookup
External Lookup : Tetration (Tar	get IP) 🕕					
NAME: * Tetration (Target IP)				Enable look	kup of interna	al IP addresses
BASE URL: * https://	st/profile/10/					
QUERY PARAMETER MAPPING:						
PARAMETER NAME:	STEALTHWATCH ATTRIBUT	TE NAME:	\sim	Required		+
URL SCRIPT BUILDER FILE UPLOAD	•					
Tetration (Target IP).config		BI	rowse			
						Cancel Save

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).

aliala cisco	Stealthwatc	h Monitor	Analyze	Jobs	Configure	Deploy
Inside I	Hosts (118)	2	View Flows Top Reports	Edit >		
Curren	t Filters	Host	Show Effective	up > e Policy	3 Host Report	(Source IP)
No Filter Clear Al	rs Selected	Sortec	Subject IP: 10	0.19.108.101	Tetration (Ta	rget IP)
Filter R	esults By:	10	to: 11/05 6:48	3 AM	ad.cisco	-x.com.
HOST	GROUPS	✓ 10	.19.108.101		app.tb.c	isco-x.com.
	(10	.18.107.102 😁)	web2.sc	lc-m.cisco-x.com.

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.

	45011 - 1404 5 0.450				
Host F	Profile		Agent Profile		
Hostnar	me	Арр-ТВ	Last Check-in	Nov 5 2018 06:36:42 am (PST)	
IP		10.19.108.101	SW Version	2.3.1.50.win64-enforcer	
Scope		SecureDC 1 more 3	SW Deployed	Oct 31 2018 02:16:04 pm (PDT)	
Enforce	ement Groups	SecureDC	Agent Type	Enforcement	
Experin	nental Groups	SecureDC	OS Platform	MSServer2016Datacenter	
Internal	1?	📀 Yes	Data Plane	C Enabled	
User Ar	anotations	News			
Bandwid	th Long-lived I	None Processes Packages Process Snapshot Agr	ent Configuration Interfaces 🔊 /	Agent Stats 🛛 🛡 Enforcement 🛛 🗘 Container En	nforce
Bandwid	th Long-lived I	None Processes Packages Process Snapshot Age	ent Configuration Interfaces 🔊 /	Agent Stats 🛡 Enforcement 🛡 Container En	nforcer
Bandwid	total Bytes	None Processes Packages Process Snapshot Age	Total Bytes Total Packets	Agent Stats 🛡 Enforcement 🛡 Container En	nforcer
Bandwid Traffic	th Long-lived I Volume	None Processes Packages Process Snapshot Age	Total Bytes Total Packets	Agent Stats U Enforcement U Container En	nforce
Bandwid Traffic	the Long-lived I Volume Total Bytes	None Processes Packages Process Snapshot Age	Total Bytes Total Packets	Agent Stats V Enforcement V Container En	nforcer
Bandwice Traffic	the Long-lived I Volume Total Bytes	Processes Packages Process Snapshot Age	Total Bytes Total Packets	Agent Stats	nforcer
Bandwice Traffic 1 40 35 30 5 5 25 20	the Long-lived I UVolume Total Bytes Down Sown Down Down Down Down Down Down Down D	Processes Packages Process Snapshot Age	ent Configuration Interfaces 🔊 /	Agent Stats	nforcer
Bandwice Traffic 40 35 25 25 20 15	the Long-lived I Volume Total Bytes Dot On	Processes Packages Process Snapshot Age	Total Bytes Total Packets	Agent Stats	nforcer
Bandwid Traffic ¹	Total Bytes	Processes Packages Process Snapshot Age	Total Bytes Total Packets	Agent Stats	nforce

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:

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

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

Firepower Threat Defense and NetFlow

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

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

Firepower Management Center FlexConfig Overview: https://www.Cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmcconfig-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.

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 🏮 System Help 🔻	admin 🔻
Device Management NAT VPN VPN QoS Platfo	orm Settings FlexConfig Certificates		
FTD-FlexConfig Enter Description		Preview Config Save	🙁 Cancel
		🖳 Policy Assig	nments (2)
Available FlexConfig C StexConfig Object	Selected Prepend FlexConfigs		
×	# Name	Description	
User Defined MD5-TCP-MAP-SXP MD5-TCP-MAP-SXP_Remove Netflow_Add_Destination_SDC System Defined	> Selected Append FlexConfigs		
Default_DNS_Configure	# Name	Description	
Default_Inspection_Protocol_Disable	1 Netflow_Add_Destination_SDC	Create and configure a NetFlow export destination.	۹, 🗊
DHCPv6_Prefix_Delegation_Configure	2 Netflow_Set_Parameters	Set global parameters for NetFlow export.	9.0
DHCPv6_Prefix_Delegation_UnConfigure			

b. Create FlexConfig Object Netfow_Set_Parameters FlexConfig.

	g Object						
Name:	Netflow_Set_Parameters						
Description:	Set global parameters for	NetFlow export.					
O Insert -	**				Deployment:	Once v Type: A	Append 🔻
## active	refresh-interva	al Number (lav in seco	of minutes bet nd (default 0	ween flow upo	late events	(default 1 minut ear)	te)
<pre>## active ## delay ##templat flow-exp ## Note: #if(\$netf no flow- #else flow-exp #end flow-exp</pre>	refresh-interv. flow-create De. e timeout-rate ort active refre The command flow low_Parameters.e export delay flow- ort delay flow-o ort template time	Al Number d lay in secon Timeout in esh-interval v-export del get(1) == "(ow-create 1 create \$net neout-rate \$	of minutes bet nd (default 0 minutes (defa L \$netflow_Par Lay 0 is not 1 0") flow_Parameter Snetflow_Param	<pre>ween flow up(command wi ult 30 minute ameters.get(() egal, so we s s.get(1) eters.get(2)</pre>	Hate events (11 not app (35) (7) (7) (7) (7) (7) (7) (7) (7) (7) (7	(default 1 minutear)	te)
<pre>## active ## delay ##template flow-exp ## Note: #if(\$netf no flow- #else flow-exp #end flow-exp Variables Name</pre>	refresh-interv. flow-create De. e timeout-rate ort active refre The command flow low_Parameters.e export delay flow- ort delay flow-o ort template tir	Al Number of lay in secon Timeout in esh-interval y-export del get(1) == "(Dw-create 1 create \$netion neout-rate \$	of minutes bet nd (default 0 minutes (defa 1 \$netflow_Par lay 0 is not 1 0") flow_Parameter Enetflow_Param Default Value	<pre>ween flow up(command wi ult 30 minute ameters.get(() egal, so we s s.get(1) eters.get(2) Property(Tv</pre>	<pre>date events (11 not app ss))) sue the fol Override</pre>	(default 1 minut ear) lowing kludge.	te)

c. Create FlexConfig Object Netfow_Add_Destination_SDC FlexConfig.

Name:	Netflow Add Destination	SDC					
	Craste and configure a NatElow export dectination						
escription:	Create and configure a Ne	tFlow export desti	nation.				
🔘 Insert 💌					Deployment	: Once 🔻 Type: Append	
#TOrea	ch (Sevent type	in Snetflo	w Event Types)				
#IOTEA flow-e #end Variables	ch (\$event_type xport event-type	in \$netflo \$event_typ	w_Event_Types) e destination \$	netflow_Dest	tination.g	et(1)	
#IOTEA flow-e #end Variables Name	ch (\$event_type xport event-type	in \$netflo \$event_typ Dimension	w_Event_Types) e destination \$ Default Value	netflow_Dest	tination.g	et(1) Description	
#IOTEA flow-e #end Variables Name netflow_Event	ch (\$event_type xport event-type	in \$netflo \$event_typ Dimension MULTIPLE	<pre>w_Event_Types) e destination \$ Default Value [all]</pre>	netflow_Dest Property (Ty FREEFORM:net	tination.g Override false	et (1) Description This variable provides the global	

ACI and NetFlow

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

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.

cisco APIC		
System Tenants ¹ Fabric	Virtual Networking	L4-L7 Services Admin Operations Apps
Inventory 2 Fabric Policies	Access Policies	
Policies Quick Start Dods	• •	Fabric Node Control - NetFlow-Priority
> Switches		Properties
> Modules > Interfaces 3 v Policies		Properties Name: NetFlow-Priority Description: Optional
> Switch		Enable DOM:
> Interface		Feature Selection: Analytics Priority Netflow Priority Telemetry Priority
 Global Monitoring Fabric Node Controls NetFlow-Priority default default default 		7

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 T<i>enant_Name</i> > 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).

System 1 Tenants Fabric Virtual Networking L4-L7 Servi	ces Admin Operations Apps						
ALL TENANTS Add Tenant Tenant Search: name or descr co	mmon2 L3out-service-PBR TenantB mgmt Tenant1						
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.							
Tenant L3out-service-PBR	External Collector Reachability - StealthWatchCollector						
Contract L3out-service-PBR Application Profiles							
> 📰 Networking	Properties						
> Contracts	Name: StealthWatchCollector						
	Source Type: OutOfband Management V 8						
> Hosticality	Source IP Address: 0.0.0.0						
> 🖬 Monitoring	IP Address with mask up to 20 for ipv4 and mask up to 116 for ipv6						
5 v 🕅 NetFlow	Destination Port: 2055						
> EN NetFlow Monitors	OoS DSCP Value: Voice Admit						
> NetFlow Records							
V NetFlow Exporters	Electron Exporter Version Format: Cisco prophetary version 1 Version 5 Version 9 10						
Stealth WatchCollector							
Services	Associated EPG: L3out-service-PBR wordpress-SF/Web-EPG 13 12 Tenant Application EPG						
	Associated VRF: L3out-service-PBR/SDC ~ 14 VRF						

Step 3

Configuring a Tenant NetFlow Record Policy

About NetFlow Record Policies

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

Procedure

Step 1	On the menu bar, select Tenants > All Tenants .
Step 2	In the Work pane, double-click the tenant's name.
Step 3	In the Navigation pane, select Tenant T <i>enant_Name ></i> Policies > NetFlow.
Step 4	Right-Click NetFlow Records and select Create Flow Record.
Step 5	In the Create NetFlow Record dialog box, fill in the fields as required, except as specified below:
	For the Collect Parameters drop-down list, you can select multiple parameters.
	For the Match Parameters drop-down list, you can select multiple parameters.
	If you select multiple parameters, your choices must be one of the following combinations or a subset of one of the combinations:
	Source IPv4, Destination IPv4, Source Port, Destination Port, IP Protocol, VLAN, IP TOS
	Source IPv6, Destination IPv6, Source Port, Destination Port, IP Protocol, VLAN, IP TOS
	Ethertype, Source MAC, Destination MAC, VLAN
	Source IP, Destination IP, Source Port, Destination Port, IP Protocol, VLAN, IP TOS, where Source IP/Destination IP qualifies both IPv4 and IPv6.

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



Step 4

Configuring a Tenant NetFlow Monitor Policy

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

Procedure

- Step 1 On the menu bar, select Tenants > All Tenants.
- Step 2 In the Work pane, double-click the **tenant's name**.
- Step 3 In the Navigation pane, select **Tenant Tenant_Name > Policies > NetFlow**.
- Step 4 Right-Click NetFlow Monitors and select Create Flow Monitor.
- Step 5 In the **Create NetFlow Monitor** dialog box, fill in the fields as required.

You can associate a maximum of two flow exporters with the monitor policy.

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

cisco APIC	
System 1 Tenants Fabric Virtual Networking L4-L7 Servin	ces Admin Operations Apps
ALL TENANTS Add Tenant Tenant Search: name or descr. co	mmon 2 L3out-service-PBR TenantB mgmt Tenant1
This has been created from Multi-Site. It is recommended to only make changes from the second sec	om Multi-Site. Please review the documentation before making any changes here.
Tenant L3out-service-PBR ()	NetFlow Monitor - SteathWatchMon
3 V Tenant L3out-service-PBR	8 7 4 8
> Networking	Properties Name: SteathWatchMon
4 Policies	Description: optional
> Troubleshoot	Associated Flow Record: StealthWatchFlotter V 7
> Host Protection	Associated Flow Exporters: NetFlow Exporter
5 V RetFlow	StealthWatchCollector
V NetFlow Monitors	
6 SteathWatchMon	
NetFlow Records	•
> Services	

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).

cisco APIC			٩	00		٥
System 1 Tenants Fabric Virtual Networ	king L4-L7 Services Admin	Operations A	pps			
ALL TENANTS Add Tenant Tenant Search: name or	descr. common 2 L3out-se	ervice-PBR TenantB	infra Tenan	1		
This has been created from Multi-Site. It is recommended	to only make changes from Multi-Site. Please	e review the documentati	on before making any	changes here.		
Tenant L3out-service-P 🌘 🗊 🔊	Logical Interface Profile	- PBR-L3-EX	T-IntProfile			• •
Quick Start				Policy	Faults	History
> Application Profiles		General	Routed Sub-Interfa	ces Routed	nterfaces	SVI
4 Vetworking	8 7 4 0				ð <u>+</u>	*-
> VRFs	Properties					
External Bridged Networks S External Routed Networks	Name: Description:	PBR-L3-EXT-IntProfile optional				Î
> 🛅 Route Maps/Profiles	Alian					
> 🚞 Set Rules for Route Maps	Alias.	select a value				
> Atch Rules for Route Maps	Egress Data Plane Policing Policy:	select a value				
6 v 📣 SDC-L3out-Site1	Ingress Data Plane Policing Policy:	select a value				
V Logical Node Profiles	PIM Interface Policy:	select an option				
7 🗸 🧧 PBR-L3-NODE	IGMP Policy:	select an option	\sim			9
Logical Interface Profiles	NetFlow Monitor Policies:					+
8 > E PBR-L3-EXT-IntProfile		 NetFlow IP Filter Type 	e NetFlov	w Monitor Policy		
> Configured Nodes	10	lpv4 type	Steath	WatchMon		

VMware vSphere Distributed Switch (VDS) and NetFlow

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

eploy NetFlow with ACI on VMware VDS

eploy NetFlow without ACI on VMware VDS

Deploy NetFlow with ACI on VMware VDS

In this case you would configure NetFlow in APIC as it has a connection to VMware vCenter as a Virtual Machine Manager (VMM). The following guidance was based on the guidance in ACI Virtualization Guide 3.2(2),

https://www.Cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3x/virtualization/b ACI Virtualization Guide 3 2 2/b ACI Virtualization Guide 3 2 2 cha pter 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.

D

D

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).

cisco APIC	
System Tenants 1 Fabric	Virtual Networking L4-L7 Services Admin Operations Apps
Inventory Fabric Policies 2	Access Policies
Policies Quick Start Switches Switches Switches Switch Policies Constraints Policies Link Level Switch Fibre Channel Interface Fibre Channel Interface CoP Interface LLDP Interface LLDP Interface MetFlow Monitors NetFlow Records NetFlow Exporters for VM. Policies Port Channel	OMM External Collector Reachability - SWVMM Policy History → ★ ★ Properties Name: SWVMM Description: Optional Destination IP Address: 10.9.10.32 7 Destination Port: 2055 8 8 Source IP Address: 10.16.6.151 9

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

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

Procedure

Step 1	On the menu bar, select Virtual Networking > Inventory .
Step 2	In the Navigation pane, expand the VMM Domains folder, Right-
	Click VMware, and select Create vCenter Domain.
Step 3	In the Create vCenter Domain dialog box, fill in the fields as
	required, except as specified:
	a. In the NetFlow Exporter Policy drop-down list, select the
	desired exporter policy or create a new one.
	b. In the Active Flow Timeout field, enter the desired active
	flow timeout, in seconds. The Active Flow
	Timeout parameter specifies the delay that NetFlow waits
	after the active flow is initiated, after which NetFlow sends
	the collected data. The range is from 60 to 3600. The
	default value is 60.

	c. In the Idle Flow Timeout field, enter the desired idle flow
	timeout, in seconds. The Idle Flow Timeout parameter
	specifies the delay that NetFlow waits after the idle flow is
	initiated, after which NetFlow sends the collected data. The
	range is from 10 to 300. The default value is 15.
	d. (VDS only) In the Sampling Rate field, enter the desired
	sampling rate. The Sampling Rate parameter specifies how
	many packets that NetFlow will drop after every collected
	packet. If you specify a value of 0, then NetFlow does not
	drop any packets. The range is from 0 to 1000. The default
	value is 0.
Step 4	Click Submit .

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

Virtual Networking L4-L7			
	Services Admin	Operations	Apps
2 Inventory			
Omain – SDC1–SF–VM Properties Port Channel Policy: LLDP Policy: CDP Policy: NetFlow Exporter Policy: NetFlow Exporter Policy: Parameters: Active Flow Timeout: Idle Flow Timeout: Sampling Rate:	IM Polic General LACP-MAC-Pinning LLDP-Disable CDP-Enable SWWMM 60 15 0 0	y Operational VSwitch Policy 6 2 2 2 2 2 3 3 3	★ ? Associated EPGs Faults History O ± ★
	2 Inventory Demain - SDC1-SF-VM Commain - SDC1-SF-VM Properties Port Channel Policy: LLDP Policy: CDP Policy: CDP Policy: NetFlow Exporter Policy: NetFlow Exporter Policy: Parameters: Active Flow Timeout: Idle Flow Timeout: Sampling Rate:	2 Inventory pomain - SDC1-SF-VMM Polic General (2) (2) (2) (2) (2) (2) (2) (2) (3) (3) Properties Port Channel Policy: LLDP Policy: LLDP-Disable CDP Policy: CDP-Enable NetFlow Exporter Policy: SWVMM NetFlow Exporter Policy: SWVMM NetFlow Exporter Policy: SWVMM Idle Flow Timeout: 60 (4) (2) Sampling Rate: (0)	2 Inventory point Second State Policy Operational General VSwitch Policy VSwitch Policy 6 Operational VSwitch Policy Properties Port Channel Policy: LACP-MAC-Pinning Properties Port Channel Policy: LLDP-Disable CDP Policy: CDP-Enable CDP NetFlow Exporter Policy: SwyMM T NetFlow Exporter Policy: SwyMM T Idle Flow Timeout: 60 Idle Flow Timeout: Idle Flow Timeout: 15 Sampling Rate:

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	Associa	ntion		• •
VMM Domain Profile:	SDC1-VMM			~ (2
Deploy Immediacy:	Immediate	On Demand		
Resolution Immediacy:	Immediate	On Demand	Pre-provision)
Delimiter:				
Enhanced Lag Policy:	select an optic	on	\sim	
Allow Micro-Segmentation:				
VLAN Mode:	Dynamic	Static		
Primary VLAN for Micro-Seg:	vlan-122	1		
Secondary VLAN for Micro- Seg:	Vlan-132	-1		
Port Binding:	Dynamic Bind	ding Epheme	eral Default	Static Binding
Netflow:	Disable	Enable		
Allow Promiscuous:	Reject		\sim	
Forged Transmits:	Reject		\sim	
MAC Changes:	Reject		\sim	
			Cance	el 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, <u>https://docs.vmware.com/en/VMware-</u> <u>vSphere/6.0/com.vmware.vsphere.networking.doc/GUID-55FCEC92-74B9-4E5F-ACC0-</u> <u>4EA1C36F397A.html</u>

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

Test Case 5 – AMP and Firepower Threat Defense

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

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

Test Description:

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



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.



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

Step 2

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.

Overview Analysis <mark>Policies</mark> D	evices Objects	AMP Intelligence	Deploy 01 System Help 🔻	
Access Control ► Malware & File	Network Discovery	Application Detectors	Correlation Actions •	
InternetFilePolicy File policy to and from Internet				
Rules Advanced				
			No access control policies use this Malware & File policy.	ld 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	J 🖗
Category: PDF files	Any	Upload	X Block Files with Reset	<i>i</i>
Category: Local Malware Analysis Capable Category: Dynamic Analysis Capable Category: System files Category: Graphics (6 more)	Any	Any	I Detect Files	6

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

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 🕒 System Help 🔻
Access Control > Access Control Network Discovery	Application Detectors Correlation Actions •	
SDC1-TB-FTDV-HA		Save Save
:::USER_GENERATED;ACI:TenantB_SDC1-TB-FTDv-HA:		
Prefilter Policy: Default Prefilter Policy	SSL Policy: None	Identity Policy: None
Editing Rule - Web-to-App		? × ¹⁾
R	E Eashlad Maur	
Name web-to-App		×
Action Allow		
Zones Networks VLAN Tags 🛆 Users Ap	oplications Ports URLs SGT/ISE Attributes	Inspection Logging Comments
Intrusion Policy	Variable Set	
None	▼ Default Set	×
File Policy		
InternetFilePolicy		v 🦉 🚆
2		
3		
D		
		Save Cancel

Step 3

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

Overview	Analys	sis Policies	Devices	Obje	cts AMP	Intelligence	s	ystem He	lp 🔻 admin 🔻
Context Exp	lorer	Connections v	Intrusio	ns 🔻	Files ► Ma	ware Events	Hosts 🔻	Users v	Vulnerabili
				Bookn	nark This Page	Report Designer	Dashboard	View Bookm	arks Search 🔻
Malware Summary (switch workflow) Malware Summary > Table View of Malware Events No Search Constraints (Edit Search) Jump to									
	Detection	Name		File Na	me	File SHA256		File Type	▼ Count
1 II 1	Vin.Droppe	er.Scarsi::100.sbx	.tg	<u>Cryptinfi</u>	nite.exe	🔆 ab452e2421a	a3f687	MSEXE	4
< < Page	1 of 1 >	> Displaying r	ow 1 of 1 ro	ws					
View View All		Delete Delete All							

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

Overview An	alysis Policie	es Devices Ob	jects AMP Intellig	ence System	Help 🔻 admin 🔻					
Context Explorer	Connections	▼ Intrusions ▼	Files ► File Events	Hosts 🔻 Users 🔻	Vulnerabilities 📲					
		E	Bookmark This Page Report	Designer Dashboard Vie	w Bookmarks Search					
File Summ	ary (switch wo	rkflow)		2018-11-07 18:54:00 - 2	018-12-10 19:57:42 🕑					
File Summary > 1	able View of File E	vents	-		Expanding					
No Search Constra	No Search Constraints (<u>Edit Search</u>)									
Jump to 🔻										
Cate	<u>jory</u>	Туре	Disposition	Action	Count					
Execu	tables	MSEXE 🧧	Malware	Malware Block	4					
≪ ≪ Page 1 o	f 1 > > Displayi	ng row 1 of 1 rows								
View	Delete									
View All	Delete All),								

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

Overview Analys	sis Policies Devices	Objects AMP	Intelligence	System He	lp 🔻 admin 🔻
Context Explorer	Connections Intrusi	ons ▼ Files ▶ Netw	ork File Trajecto	ory Hosts 🔻	Users 🔹 V 🕐 ei
Q Enter a SHA256 has	h, IP address or file name				
Recently Viewed F	iles				
Time	File SHA256	File Names	File Type	Disposition	Events
2018-11-08 15:21:15	ab452e2421a3f687	Cryptinfinite.exe	MSEXE	Malware	4
Recent Malware					
Time	File SHA256	File Names	File Type	Disposition	Events
2018-11-08 15:21:15	ab452e2421a3f687	Cryptinfinite.exe	MSEXE	Malware	4

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

dult AMP for Endpoints		?
Dashboard Analysis V Outbreak Control V Management V Accounts V	Search	Q
Computers	Ø	View All Changes
Move to Group		
🔲 🕀 🛲 App-TB in group Secure DC	✓ Within Policy	100
E	✓ Within Policy	100
① ① ① ① ①	✓ Within Policy	14
🔲 🕀 🗮 DB-TB in group Secure DC	✓ Within Policy	14
B	✓ Within Policy	14
□ ⊞ Å db2.sdc-m.clsco-x.com in group Secure DC	✓ Within Policy	100
B # Web-TB in group Secure DC	✓ Within Policy	100
□ 🕀 Δ web1.sdc-m.clsco-x.com in group Secure DC	✓ Within Policy	100
□ 🕀 🎄 web2.sdc-m.clsco-x.com in group Secure DC	✓ Within Policy	14
1 - 9 of 9 total records 25 ^ / page		Export to CSV

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.

Hostname	web1.sdc-m.cisco-x.com	Group 😁	Secure DC			
Operating System	centos linux release 7.4	Policy 🔅	Protect Policy for FireAMP Linux			
Connector Version	1.8.4.591	Internal IP 10.18.107.101				
Install Date	2018-10-08 22:26:31 UTC	External IP	12.151.35.194			
Connector GUID	30d30038-4477-4917-bbce-1f082cb36491	Last Seen	2018-12-11 03:41:35 UTC			
Definition Version	ClamAV (daily.cvd: 25196, main.cvd: 58, bytecode.cvd: 327)	Definitions Last Updated	2018-12-11 02:43:38 UTC			
Update Server	clam-defs.amp.cisco.com					

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



g. Select File Trajectory.



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

Dashboard Analysis	or Endpoir	nts				۲	?
busiloodra valaysis	 Outbreak Control 	ol 🗸 Management	 Accounts 		Search		Q
File Trajector SHA: 3b6b6f5f14ae	'y ec977						
Search Enter a SHA-25	i6 file hash						
Visibility				Entry Point			
First Seen		2018-1	2-10 11:01:01 UTC	First Seen On		Secure DC /	web2.sdc-m.cisco-x.com
Last Seen		2018-1	2-11 04:01:11 UTC				
Observations		0 (as targe	t), 316 (as source)				
Created by							
SHA-256			Filename		Product		🗘 Prevalence 🤟
			No data av	ailable in table			
🕀 File Details							
Network Profile							
Trajectory							
najectory		Dec 10					
		11:01 12	:01 13:0	14:01	15:01 1	6:01 17:01	18:01
SDC-STR-BD	db1.sdc2.cisco			•	D D	D D	D D D
Secure DC	app1.sdc-m.cis						
	db1.sdc-m.cisc	0000		0000			00000
	db2.sdc-m.cisc	D	Ó Ø Ø Ø	D D	õ õ õ	õõ õ	õ o o
	web1.sdc-m.cis	D-D-0)	• • • • • • • •		$\mathbf{D} \odot \mathbf{D} \odot \mathbf{O}$	00
	web2.sdc-m.cis	D D D	$\mathbf{O} \mathbf{O} \mathbf{O} \mathbf{O}$	••••••••••••••••••••••••••••••••••••••			<u> </u>
	wp1.sdc2.cisco	D D 0	• • • •	• • • • •		D D 0	D D D
							•
		(+) created (A) co	pied \ominus moved	♦ executed (‡	opened 💿 scanned	 advanced/tetra c 	onviction 💮 observed
		O the file was	e source of the ev	ent 🕟 red, the t	arget was deemed malicio	us 🕣 green, the ta	rget was deemed benign
Event History							
Date A	Computer 😄	Group 🔶 E	vent 🗘 SHA-2	56 🗧	File N Product	Disposition	¢
2018-12-10 11:01:01 UTC	web2.sdc-m.cisco 5	iecure DC E	xecuted by 3b6b6	f5f14aec977		Unknown	
2018-12-10 11:01:01 UTC	web2.sdc-m.cisco S	Secure DC E	xecuted by 3b6b6	f5f14aec977		Unknown	
2018-12-10 11:01:01 UTC	web1.sdc-m.cisco 5	Secure DC E	xecuted by 3b6b6	f5f14aec977		Unknown	
	dist ada ⁰ alara yan d	DC-STR-BD E	vecuted by 3b6b6	FEF 14200077		Linknown	
2018-12-10 11:01:02 UTC	001.50C2.CISCO-X.C 2		Accored by 50000	DI 14800377			
2018-12-10 11:01:02 UTC 2018-12-10 11:01:02 UTC	db1.sdc2.cisco-x.c	DC-STR-BD F	xecuted by 3b6b6	f5f 14aer977		Unknown	

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.



Seturn to Contents

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



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



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



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.

cisco APIC		_			000
System Tenants Fabric V	/irtual Networking	L4-L7 Services	Admin Operations	Apps	
AAA Scheo	dulers Historical Reco	ord Policies Firmware	External Data Collecto	ors Config Rollbacks	Import/Export
AAA () = O	Local Users				
AAA Authentication	▲ Login ID	First Name	Last Name	Email	Phe Create Local User
✓ I Login Domains	admin				Delete
🚺 fallback	albra	Albra	Welch		
✓	bmcgloth	Bart	McGlothin		
> Security Domains	knguyen				
> Roles	mso-admin				
Local Users					
- bmcaloth					
🔔 mso-admin					
> Remote Users					

Step 2

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

Create	Local Use	er					? ×
STEP 1 > U	Jser Identity		1. User Identity	y	2. Security		3. Roles
Specify the	e User Identity	,	_				
	Login ID:	FMC-RTC					
	Password:						
Co	onfirm Password:						
	First Name:	FirepowerMC					
	Last Name:	RapidThreatContainment					
	Phone:						
	Email:						
	Description:	optional					
	Account Status:	Active Inactive					
A	Account Expires:	No Yes					
				Previou	is Ca	ancel	Next

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

Create Local U	ser							?	\otimes
STEP 2 > Security				1. User Iden	tity	2. Security	3.	Roles	
Enter the Security Info	rmati	on for this User							
Security Domain:									
		Name	De	escription					
		all							
		common							
		mgmt							1
		MS_EXT_L3_Domain							
		T1 L3 Domain							-
User Certificates:									+
	Name	9	Expirat	tion Date		State			
SSH Keys:									+
	Name	9	Key						
					D i				
					Previou	is Canc	cel	Next	

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

Create Local U	ser				? ×
STEP 3 > Roles			1. User Identity	2. Security	3. Roles
Select the Roles for e	ach Security Domain				
Domain all:	ocal User les oles for each Security Domain Domain all: Role Name admin				i +
	Role Name				
	User 1. User Identity 2. Security r each Security Domain all: Role Name Role Privilege Type admin Virite Cancel		~		
			Update Cancel		
			Previ	ious Can	cel Finish

d. Repeat for each site.

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:

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.

Overview Analysis Policies Devices Obje	cts AMP	Intelligence Deploy	0, s	ystem	Help 🔻	bmcgloth 🔻
Access Control Network Discovery Application	Detectors	Correlation Actions > Modules				
Installed Remediation Modules				Alerts	Remediat	ions Groups
Module Name	Version	Description				
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router				۹
Nmap Remediation	2.0	Perform an Nmap Scan				۹. 🗄
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP add	resses			۹. 6
Set Attribute Value	1.0	Set an Attribute Value				۹ 🖥
Tetration/FirePOWER Remediation Module	1.0.2	Achieve rapid threat containment of Tetration workloads	5			۹ 🗎
	Install Choose	a new module				

NOTE:

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

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

Overview Analy	rsis Policies Dev	vices Obje	cts AMP	Intelligence		Deploy	02	System	Help 🔻	bmcgloth 🔻
Access Control •	Network Discovery	Application	Detectors	Correlation	Actions Modules					
								Alerts	Remedia	ations Groups
		0	Success Module succes	sfully installed	×					
Installed Remed	iation Modules									
Module Name			Version	Description						
APIC/FirePOWER Ren	nediation Module		1.0.1	APIC/FirePOW	ER Remediation Module					۹
Cisco IOS Null Route			1.0	Block an IP ad	dress in a Cisco IOS router					۹
Nmap Remediation			2.0	Perform an Nm	nap Scan					۹ 🖬
pxGrid Mitigation			1.0	Perform a pxG	rid mitigation against the in	volved IP add	resses			۹
Set Attribute Value			1.0	Set an Attribut	e Value					۹ 🔒
Tetration/FirePOWER	Remediation Module		1.0.2	Achieve rapid	hreat containment of Tetrat	tion workloads				۵, 🗊
			Install Choose	a new modu	le en Install					

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

Configuration

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

- Step 1 Create an instance of the remediation module for each APIC Cluster in your network:
 - a. Navigate to Policies > Actions > Instances.
 - b. Select the remediation module in the drop-down list, and click Add.

Overview Analysis Policies Devices Objects AM	IP Intelligence Deploy (🎝 System Help 🔻 bmcgloth 🔻
Access Control Network Discovery Application Detectors	Correlation Actions > Instances	
		Alerts Remediations Groups
Configured Instances		
Instance Name	Module Name	Version
pxGrid	pxGrid Mitigation	1.0 🔍 🗒
TetrationRemediation196 Tetration Remediation Service SecureDC tet-pov-rtp2.cpoc.co	Tetration/FirePOWER Remediation Module	1.0.2 🔍 🗒
Add a New Instance Select a module type APIC/	FirePOWER Remediation Module(v1.0.1)	

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

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

Overview Analysis Policies	s Devices Objects AMP	Intelligence	Deploy	₽ ₂ System H	lelp 🔻 bmcgloth 🔻
Access Control Network Disc	overy Application Detectors	Correlation Actions	Instances		
				Alerts I	Remediations Groups
	Edit Instance				
	Instance Name	ACIuSeg-SDC1			
	Module	APIC/FirePOWER	Remediation Module(v1.0.1	.)	
		Rapid Threat Co micro-segmenta	ntainment using tion for SDC-1		
	Description				
	APIC server username	FMC-RTC			
	APIC server password Retype to confirm	••••••			
	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				
	APIC cluster instance 5 IP				
		Create	ncel		

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.

Overview Analysis Policies	Devices Ol	bjects	AMP	Intelligen	ce		Deploy	•	System	Help 🔻	bmcgloth 🔻
Access Control Network Disco	very Applicat	tion Detect	tors	Correlation	Actions •	Instances					
									Alerts	Remedia	tions Groups
		Succ Create	ess d new ir	nstance ACIus	Geg-SDC1	×					
	Edit Instanc	e									
	Instance Name				ACIuSeg-SDC1						
	Module				APIC/FirePOWER	Remediation M	odule(v1.0.1)				
	Description				Rapid Threat Cor micro-segmentat	itainment using ion for SDC-1)				
	APIC server user	name			FMC-RTC						
	APIC server pass Retype to confirm	word			•••••						
	APIC cluster inst	ance 1 IP			10.17.4.11						
	APIC cluster inst	ance 2 IP			10.17.4.12						
	APIC cluster inst	ance 3 IP			10.17.4.13						
	APIC cluster inst	ance 4 IP									
	APIC cluster inst	ance 5 IP									
					Save	ncel					
	Configured F	Remediat	tions								
	Remediation I	Name		Remediatio	n Type	Descriptio	n				
			No co	nfigured reme	diations available	_	_				
	Add a ne	ew remediat	tion of ty	ype Quaranti	ne an End Point or	APIC V	dd				

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

Overview Analysis Policies De	vices Objects AMP	Intelligence	Deploy	. 06	System	Help 🔻	bmcgloth 🔻
Access Control Network Discovery	Application Detectors	Correlation Actions > Instances					
					Alert	Remedi	ations Groups
	Edit Remediation						
	Remediation Name	ACIQuarantineEP-SDC1					
	Remediation Type	Quarantine an End Point on API	С				
		Quarantine the endpoint with A uSeq policy change	PIC				
	Description						
		Create Cancel					
		Create					

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

Overview Analysis Policies De	vices Objects AMP	Intelligence	Deploy	0, System	Help 🔻 bmcgloth 🔻
Access Control Network Discovery	Application Detectors	Correlation Actions Instances			
	Success	K		Alert	s Remediations Groups
	Created new r	remediation ACIQuarantineEP-SDC1			
	Edit Remediation				
	Remediation Name	ACIQuarantineEP-SDC1			
	Remediation Type	Quarantine an End Point on A	PIC		
		Quarantine the endpoint with uSeg policy change	APIC		
	Description				
		Save Cancel Do	ne		

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

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

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

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

- a. Navigate to Policies > Access Control then Edit the policy.
- b. Click Edit Rule (for example, Log-Connections-CnC or Web Traffic).
- c. On the Logging tab, select Log at Beginning of Connection.

Important

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

Overview Analysis Po	licies Devices Objects AMP Intelligence Deploy (🎝 System Help 🔻 bmcgloth ▼
Access Control > Access C	ontrol Network Discovery Application Detectors Correlation Actions •	
SDC-Multisite-FTE	D-C1 You have unsave	ed changes 🔡 Save 😢 Cancel
Prefilter Policy: Default Prefilte	r Bolicy: None Identity Policy: None	
Rules Security Intellig	Editing Rule - Log-Connections-CnC ? X Name Log-Connections-CnC Sealed Move	2 Settings Policy Assignments (2)
Mandatory - SDC-Multi	Action Ac	
1 Block-teinet Any 2 Clean-System Any 3 Web-Traffic Any 4 Log-Connections Any 9 Default - SDC Multilate There are no rules in this set Default Action	Log at Beginning of Connection Log at End of Connection File Events: Log riles Send Connection Events to: Send Volvewr Syslog Select as Syslog Alert Configuration SNMP Trap Select an SNMP Alert Configuration NMP Trap Select an SNMP Alert Configuration	
	Save Cancel	

d. Click Save.
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**.

Overview Analysis	Policies Devices C	bjects AMP	Intelligence	Deploy 🧕	System Help 🔻	bmcgloth 🔻
Access Control • Ne	twork Discovery Applica	ation Detectors	Correlation Action	is T		
					Alerts Remedia	ations Groups
Policy Management	Rule Management	White List	Traffic Profiles			
Rule Information		O Add C	Connection Tracker	Add User Qualification	Add Host Profile C	Qualification
Rule Name	Quarantine_by_CnC					
Rule Description	Connections to CnC or Attack	ers trigger this rule				
Rule Group	Ungrouped T					
Select the type of If a connection even OR V X Sect X Sect X Sect	f event for this rule at either the begin condition 0 0 Add complex urity Intelligence Category urity Intelligence Category	nning or the end of t condition v i i v i	he connection V and it i s V CnC s V Attackers	meets the following con	ditions:	
Rule Options					💿 Add Ina	ctive Period
Snooze	If this rule generates an even	it, snooze for0	hours 🔻			
Inactive Periods	There are no defined inactive	periods. To add an i	nactive period, click "Add In	nactive Period".		
					Save	Cancel

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: <u>https://www.Cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/security_intelligence_blacklisting.html</u>

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

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

Overview Analy	ysis 🖡	Policies	Devices	Objects	AMP	Intelligence		Deploy	0,2	System	Help 🔻	bmcgloth 🔻
Access Control 🔻	Netwo	ork Discov	ery Appl	ication Dete	ctors	Correlation	Actions •					
										Alerts	Remedia	ations Groups
Policy Manager	nent	Rule M	anagement	White	e List	Traffic Profil	es					
Correlation Policy Information Save Cancel Policy Name Compromised Server												
Policy Description		If CnC i	s tripped, FMC	: will trigger a	a quarant	ine of the source h	ost					
Default Priority		None •	'								_	
Policy Rules												Add Rules
Rule						Responses				Prie	ority	
Quarantine by Connections to C	CnC nC or At	tackers trigg	ger this rule			This rule does no	t have any res	ponses.		De	fault 🔻	i

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

Overview Analysis Policies Dev	ices Objects AMP Intelligence	Deploy 🧕 System Help 🔻 bmcgloth 🔻
Access Control Network Discovery	Application Detectors Correlation Actions •	
		Alerts Remediations Groups
Policy Management Rule Manage	ement White List Traffic Profiles	
Correlation Policy Information Policy Name Compromised Policy Description Default Priority Policy Rules Rule	Responses for Quarantine_by_CnC Assigned Responses ACIQuarantineEP-SDC1 Unassigned Responses 2	Save Cancel
Quarantine by CnC Connections to CnC or Attackers trigger th	ACIQuarantineEP-SDC2 LabLog Quarantine_SourceIP Shutdown TetrationUnQuarantineEP	pdate Cancel

g. Click Update.

Overview Analysis P	olicies Devices Objects AM	IP Intelligence	Deploy 🍋 System Help 🔻 bmcgloth 🔻					
Access Control Netwo	rk Discovery Application Detectors	Correlation Actions •						
			Alerts Remediations Groups					
Policy Management	Rule Management White List	Traffic Profiles						
Correlation Policy Information You have unsaved changes Save Cancel								
Policy Name	Compromised Server							
Policy Description	If CnC is tripped, FMC will trigger a quar	antine of the source host						
Default Priority	None 🔻							
Policy Rules			O Add Rules					
Rule		Responses	Priority					
Quarantine by CnC Connections to CnC or Atta	ackers trigger this rule	ACIQuarantineEP-SDC1 (Remediation) ACIQuarantineEP-SDC2 (Remediation)	Default 🔻 🍘 🗒					

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.

Overv	view	Analysis Polic	ies Devices O	bjects A	MP Intelli	gence		Deploy	/ 0 3 S	System	Help 🔻 bm	cgloth 🔻
Contex	kt Exp	lorer Connection	Intrusions	Files •	Hosts 🔻	Users 🔻	Vulnerabilit	ties • Cor	relation 🕨	Status	Custom	 Lookup
							Book	mark This Page	Report De	esigner Vi	ew Bookmarks	Search
Rem	nedi	ation Status										0
<u>Table V</u>	/iew o	of Remediations						11 <u>20</u>	018-10-31 1	0:55:05 -	<u>2018-11-01 1</u> Ex	0:55:05 🕑 panding
No Sear	No Search Constraints (<u>Edit Search</u>)											
Jump	o to	•										
0		▼ <u>Time</u> X	<u>Remediation</u> <u>Name</u>	× <u>Policy</u>	×	<u>Rule</u> ×	Res	<u>sult Message</u>	×			
4 (2018-11-01 10:51:35	ACIQuarantineEP-SI	DC1 Comproi	mised Server	Quarantine by	<u>/ CnC Succ</u>	cessful complet	ion of reme	diation		
4 (2018-11-01 10:51:35	ACIQuarantineEP-SI	OC2 Comproi	mised Server	<u>Quarantine</u> by	<u>/ CnC "Rec</u>	quired info is n	ot found bas	sed on the	IP of the incid	ent source, ca
< < P	Page	1 of 1 >> Displa	ving rows 1–2 of 2 row	/s								
\	View	Delete										
Vie	ew All	Delete All										

Step 4 Go to the APIC GUI:

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

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

CISCO APIC System Tenants Fabric Virtual Networking L4-L7 Services Ar	min Operations Apps	
ALL TENANTS Add Tenant Tenant Search: name or descr common	enant1 L3out-service-PBR TenantB Infra	
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.	
Tenant L3out-service-PBR Image: Control of the service of the ser	PG - quarantine-Web-EPG1	Summary Policy Operational Stats Health Faults History Citere End-Points C Infound Access Policies Controlts. Controller End-Points.
> 🖬 Application EPGs	<mark>⊙ ⊙</mark> △ ○ I e	0 ±
V 📷 uSeg EPGs	End Point IP A MAC Learning Hosti Source	ng Server Reporting Interface Multicast Encap Controller Address Name
Eomains (Mits and Bane Mikrais) Static Leafs Static Leafs Granacts Static Endpoint Static Endpoint Static Endpoint	web1adc-m 10.18.107.101 00.50.56.AE keaned ear-	5 adc1.clsco-x.com SDC-vCenter 10.17.4.88 (vmm) - vtar-121(P) Pod-1/Node-101-102/VPC-FIvtar-131(S)

Step 5 What to do next

Once you clean the quarantined host and it is no longer infected, you can remove the microsegmentation 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.

cisco	APIC									
System	Tenants	Fabric	Virtual Networking	L4-L7 S	Services	Admi	n Operatio	ns Apps		
ALL TENANT	rS Add Ten	ant Tenar	nt Search: name or descr		common	Ten	ant1 L3out-	service-PBR	TenantB infra	1
i This ha	as been created	from Multi-Site	e. It is recommended to or	nly make chang	ges from Mul	i-Site. Pl	lease review the c	antine-W/	efore making any cl	hanges her
	ck Start		DIX				a quare			
 Qui Ten Ten 	ant L3out-service	e-PBR es =								
	> Application	n EPGs	0				8	D 🕢 🚺 丨	8	
	USeg EPGs USeg EPGs USeg USeg USeg USeg USeg USeg USeg USeg	s tine-Web-EPG nains (VMs and ic Leafs ttracts ic Endpoint g Attributes nets L7 Virtual IPs L7 IP Address I L7 Service Parameter	Add VMM Domain Associa Add Physical Domain Associa Add L2 External Domain A Add Fibre Channel Domain Add Taboo Contract Add Provided Contract Add Consumed Contract Add Consumed Contract Add Consumed Contract Create L4-L7 IP Address I Delete	ation occiation ssociation n Association nterface			End Point	IP	▲ MAC 1 00:50:56:AE:	Learnin Source learned vmm
	Contracts Policies		Post		- 1		I< < Page	1 Of 1 >		

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

Delete				@⊗
These tab affect the	oles show the nodes wher nodes and policies show	e this policy is used and th n in the tables. Are you su	ne other policies re you want to c	that use this policy. If you delete this policy, it will lelete: quarantine-Web-EPG1?
Nodes us	sing this policy	·	Policie	s using this policy
Choose Usage:	Interface 🗸	A	Name	Туре
Node Id	Name	Resources		This policy is not used by any other policy.
101	SDC1-LF1	Click to Show D		
102	SDC1-LF2	Click to Show D		
Change Glo	obal Deployment Settir	ugs		No Yes

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

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.



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-tetrationgsg-101/fmc-rm-tetration-gsg-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

C	Cisco Tetrati«I	n Analytics"	Dashboard - Flows		SecureDC	🂖 Monitoring	- ? •	0° ~
[.hd	Lill Flows	Views 🗗 Dashb	oard				Bart McC	Glothin
4							Prefer	ences
U	Oct 23 11:11am - 0	Oct 24 11:11am 👻					🖌 API Ke	^{eys} In
Ā	Top Provider A	Addresses		Top Provider Ports			📽 Users 🖪 Roles	a _e a _e
ŗ	10.9.10.100 10.9.10.102 10.9.10.101			53 (DNS) 389 (LDAP) 3288	_		⋒ Agent	Config &
	64.100.1.197 64.100.1.199			88 443 (HTTPS)			🞤 Mainte	enance
	64.100.1.198 10.9.10.110	E.		123 5660			ڻ Logou	t

Step 2

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

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

C	Cisco Tetrati@n Analytics" API Keys SecureDC * Monitoring - ? - 4	¥0 ₹							
h									
#	Create API Key								
	Description								
U	Secure Data Center Multi Site RTC with FMC								
₫	SW sensor management API to configure and monitor status of SW sensors								
, _₽ €	Users, roles and scope management. API for root scope owners to read/add/modity/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								

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.	
	ок

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

C	Cisco Tetratien Analytics" Al	PI Keys		SecureDC 💖	Monitoring - ?	▼ Q ⁰ ₀ ▼
411					Creat	e API Key
đ.	API Key	Capabilities	Description \$	Created At	Last Used 💠	
U	10112-1128-0140-011-1121-014	 flow_inventory_query user_data_unload 	Secure Data Center Multi Site BTC with	Oct 25 09:27:32 am		Ē
Δ		- user_uuu_upiouu	FMC	(101)		
ŗ						

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

a. Navigate to Visibility > Inventory Filters

- b. Click **Create Filter** to create an inventory filter to identify quarantined hosts. Create additional filters and scopas needed to identify the cleanup server, DNS servers etc.
- c. Enter a descriptive name, description and appropriate query (e.g. quarantine = yes).
- d. Click Save.

C	Cisco Tetratian An	alytics" Inve	ntorv Filters				Secur	eDC 😻 Monitoring	¥ 1	· •	Ø., -
ш	Filters () Enter attribu		Create F	ilter					C		Filter
4	Total matching filters: 9		Name	SDC Quarantine				Results restricted to roo	t scope	Secur	reDC
U	Name	Query	Description	Identify hosts with the User A	notation where quarantine = yes		Restricted?	Created At	Actio	ns	
۸	Cleanme.cisco-x.com	Address = 10.9.				17	No	Oct 10, 11:11 AM		Ô 3	
۶	OC APP Host	Address = 10.16	Query 🚱	* quarantine = yes		۵	No	Oct 10, 11:12 AM	ø	<u>î</u> 9	>
	OC DB Host	Address = 10.16	Scope	SecureDC 🖉			No	Oct 10, 11:14 AM	ø	t	
	OC VMs	Hostname = rp4		Restrict to ownership scope?	,		No	Oct 10, 11:14 AM	Carlo	t 9	
	OC WEB Host	Address = 10.16			Save	Cancel	No	Oct 10, 11:15 AM	đ	<u>ů</u> 9	>

NOTE:

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

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

C	Cisco Tetratian Analytics" Applications
<u> 111</u>	SecureDC Rules 🗷 PRIMARY
ф	SecureDC Version: 2 DYNAMIC Endpoints: 98 Last Run: 8:13 AM
U	⑦ Image: Conversations 306 Image: Clusters 26 Image: Clusters 139 Image: Clusters 139 Image: Clusters 26 Image: Clusters 2
≞	Image: Constraint of the second se
ŗ	Absolute Policies 4 Default Policies 134 Catch All ALLOW
	Windows firewalls place DENY rules on top impacting the results below. See User Guide for more information.
	Priority Action Consumer Provider Services
	20 ALLOW SDC Quarantine Cleanme.cisco-x.com

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



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

C	CiscoTet	ratien Ana	alytics" Applicatio	ns			💖 Monitoring 🗸 📍 🗸 🖏
40	Secure	DC Rules	PRIMARY				1 Switch Application
ж	SecureDC	Version: 2	Endpoints: 98 L	ast Run: 8:13 AM			Start ADM Run
U	3 40	Conversations 3	606 🚷 Clusters 26		ded Services App View 0		Policy Analysis 🛛 Enforcement 😷 🕆
Ā	¢ 🔳	Quick Analy	rsis Filters 1 Filter	r Policies		٥	Q
ŗ	Absolute F	Policies 3 D	efault Policies 134 Cat	ch All ALLOW	➡ Add Absolut	e Policy	Priority 90
	Windows fir	ewalls place DE	NY rules on top impacting the	ne results below. See User Guide	for more information.		Action DENY
	Priority	Action	Consumer	Provider	Services		Consumer
	15	ALLOW	SDC Quarantine	SecureDC : DNS	UDP : 53 (DNS)	ø	Provider SecureDC
	20	ALLOW	SDC Quarantine	Cleanme.cisco-x.com	TCP : 80 (HTTP)	C2	View Conversations
	90	DENY	SDC Quarantine	SecureDC	Inactive 🕼	ß	Service Ports: (0)
							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.

Overview Analysis Policies Devices	Objects	AMP Intelligence Deploy 🧕 System Help 🔻 bmcg	gloth 🔻
Access Control • Network Discovery App	lication Detec	ctors Correlation Actions > Modules	
		Alerts Remediations 0	Groups
Installed Remediation Modules			
Module Name	Version	Description	
APIC/FirePOWER Remediation Module	1.0.1	APIC/FirePOWER Remediation Module	. 6
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router	. 6
Nmap Remediation	2.0	Perform an Nmap Scan	. 6
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses	1
Set Attribute Value	1.0	Set an Attribute Value	. 6
	Insta Choos	se File] etration_FMCle_1.0.2.tgz	

NOTE:

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

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

Overview Anal	ysis Policies De	vices Obje	cts AMP	Intelligence	Deploy	04 System	Help 🔻 b	mcgloth 🔻
Access Control •	Network Discovery	Application	Detectors	Correlation	Actions Modules			
						Alert	s Remediatior	ns Groups
		Suc Mode	Cess le successfully	installed	×			
Installed Reme	diation Modules							
Module Name		Ve	rsion D	escription				
APIC/FirePOWER Re	emediation Module	1.	.1 AF	PIC/FirePOWER Re	mediation Module			۵
Cisco IOS Null Rout	e	1.	BI	ock an IP address	in a Cisco IOS router			۹
Nmap Remediation		2.	Pe	erform an Nmap S	can			۵
pxGrid Mitigation		1.	Pe	erform a pxGrid m	itigation against the involve	d IP addresses		۹
Set Attribute Value		1.	Se Se	et an Attribute Val	ue			۵
Tetration/FirePOWE	R Remediation Module	1.	.2 Ad	chieve rapid threat	containment of Tetration w	vorkloads		۹
			Install a n Choose File	ew module No file chosen	Install			

Configuration

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

Step 1

Cr

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

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

Overview Analysis Poli	cies Devices Objects AMP In	ntelligence Deploy	🔒 🔒 Sy	stem Help 🔻	bmcgloth 🔻
Access Control • Network	Discovery Application Detectors C	Correlation Actions > Instances			
				Alerts Remediat	ions Groups
Configured Instances					
Instance Name	Module Name			Version	
pxGrid	pxGrid Mitigation			1.0	۵
QuarantineBadEP SDC1 ACI Fabric	APIC/FirePOWER Reme	ediation Module		1.0.1	۹
QuarantineBadEP-SDC2 SDC2 ACI Fabric	APIC/FirePOWER Reme	ediation Module		1.0.1	۹
Add a New Instance					
	Select a module type Tetration/FirePOW	/ER Remediation Module(v1.0.2)			

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

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.

Overview Analy	vsis Policies Dev	vices Objects AMP	Intelligence	Deploy 🤒	System Help v bmcgloth v
Access Control •	Network Discovery	Application Detectors	Correlation Actions > Inst	ances	
					Alerts Remediations Groups
	Edit Instance Instance Module Descriptio	stance Name	TetrationRemediation1 Tetration/FirePOWER R Tetration Remediation SecureDC tet-poy-tp/	96 temediation Module(v1.0.2) Service <u>2.cpoc.co</u>	
	Tetration Scope(e.g API key Retype to c API secre Retype to c	Analytics IP g. Default) confirm tt confirm	64.1 SecureDC Create Cancel		

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.

Overview Analysis Policies	Devices Objects AMP	Intelligence	Deploy 0, S	iystem Help 🔻 bmcgloth 🔻
Access Control • Network Disco	very Application Detectors	Correlation Actions > Instances		
				Alerts Remediations Groups
		×		
	Created new i	nstance TetrationRemediation196		
Ec	dit Instance			
Ins	stance Name	TetrationRemediation196		
Мо	odule	Tetration/FirePOWER Remediat	ion Module(v1.0.2)	
		Tetration Remediation Service		
De	scription	Securebe tet-pov-rtpz.cpoc.co	,	
Tet	tration Analytics IP	64.1		
Sci	ope(e.g. Default)	SecureDC		
AP	I key	••••••	••••	
Ket	cype to confirm	•••••	••••	
AP	I secret type to confirm	******************************		
		Save		
Co	onfigured Remediations			
R	emediation Name	Remediation Type Descrip	otion	
	No co	onfigured remediations available		
	Add a new remediation of type	Quarantine an IP on Tetration Analytics 🔻	Add	

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



g. Return to the Instance configuration by clicking Done.

Overview Analysis Policies De	evices Objects AMP	Intelligence	Deploy	04 System	Help 🔻	bmcgloth 🔻
Access Control Network Discovery	Application Detectors	Correlation Actions • Instances				
				Alert	s Remedia	tions Groups
	Success Created new r	× emediation TetrationQuarantineEP				
	Edit Remediation					
	Remediation Name	TetrationQuarantineEP				
	Remediation Type	Quarantine an IP on Tetration A	nalytics			
		Quarantine the endpoint with Tetration policy change				
	Description					
		Save Cancel Done	•			

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

NOTE:

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

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

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

- a. Navigate to Policies > Access Control then Edit the policy.
- b. Click Edit Rule (for example, Log-Connections-CnC or Web Traffic).
- c. On the Logging tab, select Log at Beginning of Connection.

Important

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

		O Custom Usla - her adath -
	Control Network Discovery Application Detectors Correlation Actions *	theta a system help v bincgiotn v
SDC-Multisite-FT	D-C1 You have t	nsaved changes 🔚 Save 🕄 Cancel
Prefilter Policy: Default Prefilt	er Policy: None Identity Policy: None	
Rules Security Intellig Iffilter by Device Interview Reme Soc Name Soc Handatory - SDC-Hull Interview Bock-teinet Any Clean-System Any Generations Any Bock-teinet Soc Poleault - SDC-Hull/Site There are no rules in this sec Default Action	Editing Rule - Log-Connections-CnC Name Log-Connections-CnC Cones Maxe Action Allow Cones Networks Usg at Beginning of Connection Log at Beginning of Connection Isog at End of Connection File Events: Send Connection Events to: Syslog Select a Syslog Alert Configuration	? × > Settings Policy Assignments (2) Rules × * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
	Save	

- 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**.

Overview Analysis	Policies Devices O	bjects AMP Inte	lligence	Deploy 0, Syste	m Help 🔻 bmcgloth 🔻
Access Control Net	work Discovery Applica	tion Detectors Corr	elation Actions •		
				AI	erts Remediations Groups
Policy Management	Rule Management	White List Tra	ffic Profiles		
Rule Information		O Add Connec	tion Tracker 📀 Add User	Qualification 3 Add	Host Profile Qualification
Rule Name	Quarantine_by_CnC				
Rule Description	Connections to CnC or Attacke	ers trigger this rule			
Rule Group	Ungrouped V				
Select the type of If a connection event Add co OR V Secu X Secu X Secu	event for this rule occurs at either the begin andition Add complex of rity Intelligence Category rity Intelligence Category	ning or the end of the con condition	nection and it meets th CnC Attackers	ne following conditions:	
Rule Options					O Add Inactive Period
Snooze	If this rule generates an event	, snooze for 0 hours	V		
Inactive Periods	There are no defined inactive	periods. To add an inactive	e period, click "Add Inactive Pe	eriod".	
					Save

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-guidev623/security_intelligence_blacklisting.html

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

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

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

Overview Analysis	Policies Devices C	bjects AMP	Intelligence		Deploy	02 System	Help 🔻	bmcgloth 🔻
Access Control • Netwo	ork Discovery Applica	ation Detectors	Correlation	Actions •				
						Alert	s Remedia	tions Groups
Policy Management	Rule Management	White List	Traffic Profile	s				
Correlation Policy In Policy Name Policy Description	formation Compromised Server If CnC is tripped, FMC w	vill trigger a quarant	ine of the source ho	st			Save	Cancel
Default Priority Policy Rules	None 🔻							Add Rules
Rule			Responses			Pri	ority	
Quarantine by CnC Connections to CnC or At	tackers trigger this rule		This rule does no	t have any resp	onses.	De	efault 🔻	

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

Overview Analysis Polici	es Devices Objects AMP	Intelligence	Deploy 02	System Help 🔻 bmcgloth 🔻
Access Control • Network Dis	covery Application Detectors	Correlation Actions •		
				Alerts Remediations Groups
Policy Management Rul	e Management White List	Traffic Profiles		
Correlation Policy Info	esponses for Quarantine_by_	_CnC		Save Cancel
Policy Name Policy Description Default Priority Policy Rules Rule Quarantine by CnC Connections to CnC or Attack 1	Assigned Responses TetrationQuarantineEP Unassigned Responses QuarantineBadEP QuarantineBadEP-SDC2 Shutdown TetrationUnQuarantineEP UnQuarantine_SourceIP	2 3 Update	Cancel	Add Rules Priority Default

g. Click Update.

Overview Analys	sis Policies Devices	Objects AMP	Intelligence		Deploy 04	System	Help 🔻	bmcgloth 🔻
Access Control 🔻	Network Discovery Appli	cation Detectors	Correlation	Actions •				
						Alerts	Remedia	tions Groups
Policy Managem	ent Rule Management	White List	Traffic Profiles	5				
You have unsaved changes Save Cancel								
Policy Name	Compromised Server							
Policy Description	If CnC is tripped, FMC	will trigger a quarant	ine of the source hos	st				
Default Priority	None 🔻							
Policy Rules							\bigcirc	Add Rules
Rule			Responses			Prio	rity	
<u>Quarantine by C</u> Connections to CnC	C <u>nC</u> C or Attackers trigger this rule		TetrationQuarant	tineEP (Remediatio	on)	Defa	ault 🔻	(# 6)

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 I	Intelligence	Deploy	🤑 System Help ▼ bmcgloth ▼						
Context Explorer Connections •	Intrusions ▼ Files ▼ Hos	sts ▼ 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)										
Jump to 🔻										
□ ▼ <u>Time</u> ×	Remediation Name X	Policy X Ru	e X Result	<u>Message</u> ×						
2018-10-26 10:27:33	TetrationQuarantineEP	Compromised Server Qua	rantine by CnC Success	ful completion of remediation						
V Page 1 of 1 >> Displaying row 1 of 1 rows										
View Delete View All Delete All										

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

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

))	Cisco Tetrati@n Analytics" H	ost Profile
Lad	Oct 23 9:24pm - Oct 24 9:24pm -	
æ U	Host Profile	
л	Hostname	web1
	IP -	10.18.107.101
	Scope Enforcement Groups	SecureDC2 more
	Experimental Groups	SecureDC1 more
	Internal?	♥ Yes
	User Annotations	quarantine = yes

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.

C	Cisco Tetratian Analytic	s* Inventory Upload			SecureDC	🎨 Monitoring 👻 ? 👻	00
<u>lılıl</u>	Select a CSV file to add or delete us	Upload					
ф	Select File 🛓 Clear Annotatio	Operation			nable in	ventory and flow annotations.	
U		Add	•				
Δ					Cancel		
۶				Save Reset			

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 unquarantine 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.



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.



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>.

the dentity Services Engine Home	Context Visibility Operations Policy Administration Work Centers								
▼System ► Identity Management ► Network R	esources								
Deployment Licensing	Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings								
Deployment	Deployment Nodes								
<									
Deployment	🖊 Edit 🔯 Register 🔯 Syncup								
N Failover	Hostname Personas Role(s) Services								
	ise20 Administration, Monitoring, Policy Service, pxGrid STANDALONE ALL								

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

Enable Device Admin Service 🕡	
Enable Passive Identity Service (i)	
PxGrid ()	
Save Reset	

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

-duala- cisco	Identity Services Engine	Home	► Conte	xt Visibility	 Operations 	Policy	→ Administratio	Mork Centers
► Sy	stem Identity Management	Network	rk Resources	Device	Portal Manager	nent pxGrid S	Services Fee	d Service + Threat Centric I
All C	Clients Web Clients Capa	bilities	Live Log	Settings	Certificates	Permissions		
🖌 En	able 🥝 Disable 🕝 Approve	Group	👎 Decline	😧 Delete 👻	🛞 Refresh	Total Pending /	Approval(0) 👻	
	Client Name	Clien	t Description	1	Capabilit	ies	Statu	IS
	ise-fanout-ise20				Capabilit	ies(0 Pub, 0 Sub) Onlin	ne (XMPP)
□ ►	ise-mnt-ise20				Capabilit	ies(2 Pub, 1 Sub) Onlin	ne (XMPP)
	ise-admin-ise20				Capabilit	ies(4 Pub, 2 Sub) Onlin	ne (XMPP)
•	ise-pubsub-ise20				Capabilit	ies(0 Pub, 0 Sub) Onlin	ie (XMPP)
	firesightisetest-fmc.cisco-x.com	-2			Capabilit	ies(0 Pub, 0 Sub) Offlir	ne (XMPP)
	iseagent-firepower-2b401b7f0ct	85			Capabilit	ies(0 Pub, 0 Sub) Offlir	ne (XMPP)
	iseagent-fmc.cisco-x.com-2b401	lb			Capabilit	ies(0 Pub, 0 Sub) Offlir	ne (XMPP)
•	firesightisetest-firepower-2b401	b			Capabilit	ies(0 Pub, 0 Sub) Offlir	ne (XMPP)
	smc.cisco-x.com				Capabilit	ies(0 Pub, 0 Sub) Offlin	ne (XMPP)
4								
Conne	cted to pxGrid ise20 cisco-x com							
-		1						

Step 2 Generate a pxGrid Certificate

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

itio Ident	tity Services Engine	Iome	ility	► Policy	ninistration	Vork Centers	
System	 Identity Management 	Network Resources FD	levice Portal Managemen	t pxGrid Services	Feed Service	Threat Centric NAC	
All Clients	Web Clients Capat	es Live Log Setting	gs Certificates Pe	ermissions			
Genera	te pxGrid Certifica	5					
	l wan	Generate a single cer	tificate (without a certifica	te signing request)			•
	Common Name (C	ise20.cisco-x.com					
	Descrip	1					
	Certificate Temp	PxGrid_Certificate_Ten	nplate				
5	Subject Alternative Name (S) IP address 🔻	10.9.10.51	- +			
	Certificate Download Form	Certificate in Privacy I	Enhanced Electronic Mail	(PEM) format, key in I	PKCS8 PEM forma	t (including certificate cha	it 🔻 🤇
	Certificate Passwo						•
	Confirm Passwo						
						Reset	ate
nnected to	pxGrid ise20.cisco-x.com						

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

Opening 159131634	9799_cert.zip	×							
You have chosen t	You have chosen to open:								
1591316349	9799_cert.zip								
which is: Co	mpressed (zipped) Folder								
from: https:/	//10.9.10.51								
What should Fire	iox do with this file?								
○ <u>O</u> pen with	Windows Explorer (default) \sim								
Save File									
Do this auto	matically 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	Туре	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

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

- alta CIS	le Identi	ty Services Engi	ne Home	Context Visibility	 Operations 	▶ Policy	✓Administ	tration 🕨 V	Vork Centers
•	System	 Identity Manage 	ment Network	Resources Devic	e Portal Manageme	nt pxGrid S	ervices	Feed Service	Threat Centric NAC
_	Il Clients	Web Clients	Capabilities L	ive Log Settings	Certificates P	ermissions			
	PxGrid	Settings							
	Auton	natically approve n	ew certificate-base	d accounts					
	Use De	fault Save							
	Test								
Co	inected to p	xGrid ise20.cisco-	x.com						

Step 3 Create the Tetration Virtual Edge Appliance Configuration Bundle

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



b. Select the ISE connector from the CONNECTORS page.

0	Cisco Tetrati@n"	CONNECTORS	(
ı ال	Q Filter		
T	New & Noteworth	у	
	(Ch	F5	ISE
Δ	6	Collect telemetry from F5 BIG-IP	Collect endpoints and inventories from Cisco ISE
¢			

c. Click Enable.



d. Click Yes to start the Configuration Bundle setup.



e. Enter the appliance IP information and click Next.

C.	Cisco Tetrati@n* DEPLOY VIRTUAL APPLIANCE			Sector Se	• ⑦ • ⑧ <mark>°</mark> •
<u>با</u>	•	2			
۲	Download OVA	VM Configuration	Download Configuration Bundle	Deploy Virtual Appliance	
۵	IP Address (CIDR format)	10.9.10.81/24		+	
۵ ۵	Gateway IP address	10.9.10.1		+	
ø	Hostname (optional)				
ø	Name Server	10.9.10.110		+	
		10.9.10.111		×	
	Search Domain (optional)			+	
	Use proxy server to connect to Tetration (optional)				
	HTTP Proxy (optional)	http://www.cisco.com:8080			
	No Proxy (optional)	acme.org		+	
	Docker Bridge IP (CIDR format) (optional)	172.17.0.1/16			
	Cancel			Pre	Next

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

C	Cisco Tetratien* DEPLOY VIRTUAL APPLIANCE			
ш			3	
ሔ	Download OVA	VM Configuration	Download Configuration Bundle	
®				
б		Tetration Edge VM configurat	ion bundle (iso image) ready for deployment	
Ą		🕹 Downloa	d Configuration Bundle	
÷				
	Cancel			Previous

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**.

vm	vSpher	Actions - SDC1	earch in all environments $ ext{C}$ $ ext{(i)}$ × Administrator@CISCO-X.COM ×	
٦	Q	Vew Cluster	ACTIONS ~	
✓	c-vcenter.c SDC-IE SDC1	New Folder Distributed Switch	itor Configure Permissions Hosts & Clusters VMs Datastores Networks Updates tosts: 4 CPU Free: 250.55 GHz	,
	SDC2	New Virtual Machine Deploy OVF Template	Virtual Machines: 16 Used: 8.48 GHz Capacity: 257.04 GHz Itusters: 0 Memory Free: 1.43 TB retworks: 8 Memory Free: 1.43 TB	
		Storage Edit Default VM Compatibility	Storage Free: 1.21 TB Ubed: 1.44 TB Capacity: 2.56 TB	
		Migrate VMs to Another Net	zs ^ Tags ^	,

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

1 Select an OVF template	Select an OVF template			
2 Select a name and folder	Select an OVF template from remote URL or local file system			
3 Select a compute resource	Enter a URL to download and install the OVF package from the Internet, or browse to a			
4 Review details				
5 Select storage 6 Ready to complete	IOCATION ACCESSIBLE FROM YOUR COMPUTER, SUCH AS A IOCAI HARD DRIVE, A NETWORK Share, Or A			
	© URL			
	http://remoteserver-address/filetodeploy.ovf .ova			
	Local file Choose Files tetration-edge-3.3.2.2.ova			

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

1 Select an OVF template 2 Select a name and folder	Select a name and folder Specify a unique name and target location			
3 Select a compute resource 4 Review details	Virtual machine name: tetration-edge			_
5 Select storage 6 Ready to complete	Select a location for the virtual machine.			
	SDC1 SDC2			
			PLOK]	-

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

1 Select an OVF template 2 Select a name and folder	Select a compute resource Select the destination compute resource for this operation
3 Select a compute resource	
4 Review details	✓ □ SDC1
5 Select storage	> 10.16.6.102
6 Ready to complete	> 10.16.6.103 > 10.16.6.104
	Compatibility
	 Compatibility checks succeeded.

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

1 Select an OVF template 2 Select a name and folder	Review details verify the template details.					
4 Review details						
5 Select storage 6 Select networks	Publisher	Symantec Class 3 SHA256 Code Signing CA (Trusted certificate)				
	Download size	1.2 GB				
/ Ready to complete	Size on disk	3.1 GB (thin provisioned)				
		195.3 GB (thick provisioned)				

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	Select storage Select the storage for the configuration and disk files						
3 Select a compute resource 4 Review details	Encrypt this virtual machine (Requires Key Management Server)						
5 Select storage 6 Select networks 7 Ready to complete	Select virtual disk format:	Thic	k Provision Lazy Zer	oed 🗸			
	VM Storage Policy:	Datastore Default 🗸 🗸		_			
	Name	Capacity	Provisioned	Free	Тур		
	ESXI-3-DataStore1	446 GB	53.36 GB	402.25 GB	VI -		
	4				• •		
	Compatibility						
	 Compatibility checks sur- 	cceeded.					
	L						

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	Select networks Select a destination network for each source network.				
 3 Select a compute resource 4 Review details 	Source Network	Ŧ	Destination Network	Ŧ	
5 Select storage	VM Network		VM Network-10	× .	
6 Select networks 7 Ready to complete				1 items	
	IP Allocation Settings				
	IP allocation:	St	tatic - Manual		
	IP protocol:	IP	V4		
			_		

h. Review the VM configuration and click Finish.

Deploy OVF Template	9		
1 Select an OVF template2 Select a name and folder	Ready to complete Click Finish to start cr	reation.	
 3 Select a compute resource 4 Review details 			
✓ 5 Select storage	Provisioning type	Deploy from template	
✓ 6 Select networks 7 Peady to complete	Name	tetration-edge-1	
/ Ready to complete	Template name	Toolbox_Licenses_VA_1.3.1	
	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 V Q Search in all environments	C 🕜 v Administrator@CISCO-X.COM v 😳
Image: Solution of the sector of the sect	ESXi-3-DataStore1 ACTIONS ~ Summary Monitor Configure Permissions File Q Search	is Hosts VMs w Folder ↑ Upload Files ↑ Upload Folder PRegister VM ↓ Download C Copy to → Move to
 ESXI-3-DataStore1 ESXI-4-DataStore1 ESXI-5-DataStore1 ISO1 ISO1 	 dvsData locker a.aa.618e7283727a4b5022b418051e45400e db-tb-win Tetration Edge - VM Config bundle tetration-edge tmp wmkdump 	ame to ∑Delete ≧Inflate ▼ Size ▼ Modi ▼ Type ▼ Path ▼ xpll 10,668 12/28/ ISO Im [ESXI-3 1 items

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

🍅 File Upload								×
← → • ↑ 📘	> This PC	> Local Disk (C:) > ISO		~ ē	Search ISO			P
Organize 🔻 Ne	w folder					-		•
- Ouick accord	^ Na	ame	Туре					
Quick access	6	appliance-tetration_edge-xxxxxxxx-5e0803a5885aac59b6ffa82a.iso	UltralSO File					
This PC	_							
Desktop								
Documents	~							
	File name:	appliance-tetration_edge-xxxxxxxx5e0803a5885aac59b6ffa82a.iso		~	All Files (*.*)			\sim
					Open		Cancel	

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**.

vm	vSphere	Client	💕 Open Remote Console		Il environments		С	@ ~				٢
۵		3	Gione		📄 🕨 🖉 🤯 🔯 🛛 ACTIONS 🗸							
v 🗗 sda	c-vcenter.cisc	co-x.con	Fault Tolerance	٠	onfigure Permissions Datastores Networks Updates							
	SDC-IE SDC1		VM Policies	•	VM SDRS Rules							^
> [10.16.6.102		Template		ADD EDIT DELETE							ш
~ [10.16.6.103	n-edge	Compatibility	•	Name y Description y	Enable	ed		~	Datactora Cluster		ń.
	WinServ	/erTest-	Export System Logs		Hame y Description y	LINGUN	eu.			Datastore cluster	1	-
	10.16.6.104		Edit Settings			7						
> 🗈	SDC2		Move to folder			1.5						~
Recent	Tasks A	larms	Rename									*

 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.

		ADD NEW DEVICE
/ Goreentioner G	Lor Logie Farance	,
> Network adapter 1	VM Network 10 \vee	Connected
CD/DVD drive 1	Datastore ISO File 🗸 🗸	Connected 😣
Status	Connect At Power On	
CD/DVD Media	[ESXi-3-DataStore1] Tetra	E
Device Mode	Emulate CD-ROM 🗸 🗸	
Virtual Device Node	IDE 0 V IDE(0:0) CD/DVD drive 1	~
> Video card	Specify custom settings 🗸	

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

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



Step 5 Configure the ISE Connector

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


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

C.	Cisco Tetratien ⁻ CONNECT	ÖR	🕈 SAFE_DATACENTER 🗸 🛛 💝 Monitoring 🖌 🛞 🗸
ы		ISE 🥑	< Browse Connectors
윪		Info ISE Instances LDAP Endpoint Log	
۲			Add Instance Config
Δ			
Ą			
¢	Enabled on January 5, 2020		
B	M Tetration Edge Appliance		
	Delete		
	Capabilities		
	User Insights Inventory Enrichment		
	Endpoint Insights		
	Software Compliance Posture		
	MDM Insights		

- c. Complete the ISE Connector configuration.
 - 1. In the Name field, type </BE-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.

C.	Cisco Tetratien" CONNECTOR	R	SAFE_DATACENTER → Ø Monitoring → Ø → Ø ⁶ →
<u>μ</u>		ISE 💿	< Browse Connectors
ŝ		Info ISE Instances LDAP	Endpoint Log
۲			
Θ			Add Instance Comp
⊿		New ISE instance	
¢		Name	tet-edge-ise1
ø	Enabled on January 5, 2020		
B	Delete	ISE Client Certificate	Enter Client Certificate Copy and paste the content of the Client Certificate
	Capabilities	ISE Client Key	Enter Client Key
	User Insights Inventory Enrichment		Copy and paste the content of the Client Key
	Endpoint Insights		
	Software Compliance Posture	ISE Server CA Certificate	Enter Server CA Certificate Copy and paste the content of the CA Key
	MDM Insights		
		ISE Hostname	ise20.cisco-x.com
		ISE Node Name	ise20.cisco-x.com
		Cancel Config Creation	Venity & Save Configs

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

C	CiscoTetratien CONNECTO	R	SAFE_DATACENTER + 🛞 Monitoring + 🛞 + 🖓 +
Lat		ISE Ø	< Browse Connectors
5		Info ISE Instances LDA	P Endpoint Log
۲			
Ø			
凸		Enter Configs	Select Discovered Attributes Review and Apply Configs
¢		LDAP Username	Change LDAP Username
÷	Enabled on January 5, 2020	DAR Password	
B	Tetration Edge Appliance	LDAF Fassword	
	Delete	LDAP Server	ad2.cisco-x.com
	Capabilities	LDAR Bort	200
	Endpoint Insights	LDAP POR	303
	Software Compliance Posture	Use SSL	
	MDM Insights	Verify SSL	
		LDAP Server CA Cert (optional)	B
		LDAP Server Name (optional)	Enter LDAP Server Name
		LDAP Base DN	cn=users,dc=cisco-x,dc=com
		LDAP Filter String	(&(objectClass=user))
		Snapshot Sync Interval (in hours) (optional)	24
		Use Proxy to reach LDAP	
		Proxy Server to reach LDAP (optional)	http://1.1.1.1:8080
		Cancel	Next

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

Ċ.	CiscoTetratien"	CONNECTOR	✿ SAFE_DATACENTER ▼	🛞 Monitoring 🗸 🔞 🗸
Lat		ISE 🧇		< Browse Connectors
8		Info ISE Instances LDA	P Endpoint Log	
۲				
a			2	
Д		Enter Configs	Select Discovered Attributes	Review and Apply Configs
¢		LDAP Username Attribute	cn	•
÷	Enabled on January 5, 20	2020		
B	Tetration Edge Appliance	e LDAP Attributes to Fetch	cn × memberOf × name ×	
	Delete			
	Capabilities			
	User Insights Inventory En	nrichment		
	Endpoint Insights			
	Software Compliance Postur	ure		
	MDM Insights			
		Cancel		Previous

c. Review and click Save & Apply Configs.

C.	Cisco Tetratien' CONNECTOR		SAFE_DATACEN	ITER - 🛞 Monitoring - 🕐 - 🕸 -
<u>1.11</u> 688		Enter Configs	Select Discovered Attributes	3 Review and Apply Configs
® ()		LDAP Username		
A		LDAP Password		
ø	Enabled on January 5, 2020	LDAP Server	ad2.cisco-x.com	
Ð	s [™] Tetration Edge Appliance	LDAP Port	389	
	Delete	Use SSL	×	
	User Insights Inventory Enrichment	Verify SSL	×	
	Endpoint Insights Software Compliance Posture	LDAP Server CA Cert		
	MDM Insights	LDAP Server Name		
		LDAP Base DN	cn=users,dc=cisco-x,dc=com	
		LDAP Filter String	(&(objectClass=user))	
		LDAP Username Attribute	cn	
		LDAP Attributes to Fetch	cn memberOf name	
		Snapshot Sync Interval (in hours)	24	
		Use Proxy to reach LDAP	×	
		Proxy Server to reach LDAP		
		Cancel		Previous 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	Туре
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 lcon to expand the menu. Click the greater sign (>) to expand the VISIBILITY menu and select Inventory Upload.



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

٢	Cisco Tetratien" INVENTORY UPLOAD	SAFE_DATACENTER → ^(*) Monitoring → ^(*)
ы		
*	Managing inventory annotations on the TINTGSSOPOV scope.	Select annotation columns to enable on inventory and flows.
۲	Tetration will generate alerts on any inventory matching an annotation prefixed with 'lookout_'.	Application
Ø	Upload	✓ Location [↑]
四	Select File 🔬 Download Annotations 🚣	le Region □ I Tier □
0	Select a CSV file to add or delete annotations.	✓ Type ①
\$	Show more ①	Save Reset
ß	Assign Assign Annotations	
	Manually assign annotations to an IP or subnet.	
	Search	
	Search by IP or Subnet Search	
	Danger Zone	
	Clear All Annotations	

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.



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

đ	Cisco Tetra	atien"	SCOPES		(SAFE_DATACEN	TER 👻 🛞 Monito	oring -	? •	©° -
[ad	· ·							_	_	
***	\square							Create	e New Sco	оре
۲	\square	TINT(GSSOPOV 🔁							
۵		Filters	Filter Scop	9S						8
凸	Name 🔶			Query	Ability ‡	Total Child	ren ¢			
¢	T SAFE	CLOUD		* Type contains Cloud	Owner	3	C Edit			
¢				View I	Deleted Scopes					
ß										

- 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

ope Details		× Canc
Name	SAFE_DATACENTER	
Description	Enter a description (optional)	
Policy Priority 😡	Natural	
Parent Scope	O INTGSSOPOV -	
Sub-Type	No selection	
Query 😡	* Type = Datacenter	
	☑ Create	

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

Step 9 Create Inventory Filters

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



b. Click Create Filter.

	Cisco Tetrati« n'	INVENTORY FILTERS		SAFE_DATACENTER ✓ SAFE_DATACENTER ✓ SAFE_DATACENTER	oring - 🔿 - 🕸 -
Lot					
	Filters 🕢 Ente	r attributes	Search		Create Filter
۲	Total matching filters	7		Results restricted to root s	cope 🕈 INTGSSOPOV
(Å	Name	Query	Ownershi	p Scope Re	stricted? Created At

- 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.

1			
Defin	e		
Name	Employees Create a query based on Inventory Attributes: Inventory is matched dynamically based on the que include Hostname, Address/Subnet, OS, and more user guide. A preview of matching inventory items will be show	ery. The tags can . The full list is in the n in the next step.	
Query 😡	* ISE_cts SecurityGroup = Employees SGT		8
	Show advanced options		

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

Det	ine	Summary	
Name	Employees		
Scope	TINTGSSOPOV		
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	

Step 10 Workspace Creation

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



b. Click the Create New Workspace.

C	Cisco Tetratien"	SEGMENTATION				INTGSS	OPOV -	⊗ Monitoring - ⑦ -	©° -
EM.	SEGMENTATION	Overview					<table-cell> Get</table-cell>	Started	
rian de la companya d	Enforced Appl	ications 1	Enforcement Agents	40		6 / 40	1.	Create Filter	
â	•						2.	Add Policy	
四	Workspaces	- Analyzed Policies	Inforced Policies	Policy Requests			3.	Start Analysis	
¢	3 Workspaces	Q Filter application wo	rkspaces	Sort	Create New	/ Workspace	4.	Enable Enforcement	
¢	AWS-Safe3tierAp	p	TINTGSSOPOV: SAFE_CL	OUD : AWS-US-EA	AST PRIMARY ANA				
ß	230 Conversations	5 Clusters	26 Policies		Last updated: I	Mar 29, 2:17 PM	10 m		
	Azure-Safe3tierA	рр	TINTGSSOPOV : SA	FE_CLOUD : AZU	JRE PRIMARY	÷	X 100!	S Enforcement History	I
	- Conversations	0 Clusters	1 Policy		Last updated: I	Mar 29, 2:17 PM	3	Enlorcement history	
							\triangleright	Default ADM Run Config	

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 ▼	ß
		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 Tetratien SEGMENTATION	⊗ Monitoring + 🕐 + 🕸 +
H 6	WordPress3TierApp @ secondary INTGSSOPOV: SAFE_DATACENTER DYNAMIC Provide x8 P Conversations Clusters 1 1 #Policies 1	Switch Application Start ADM Run
0	Clusters ①	Q (D)
<u>م</u>	Filters Image: Pilter Clusters Image: Pilter Clusters Displaying 1 of 1 clusters Image: Pilter Clusters	Cluster Actions
\$	Cluster 3 © Workloads © Confidence © Dynamic Approved ©	Name WordPress Wet 2 4
ø		View Cluster Details
		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)
	ß
Query Θ	* 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).

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.

0	Cisco Tetratien" SEGMENTATION	⊗ Monitoring - ⑦ - ⊗₀ -
Le	WordPress3TierApp III SECONDARY	Switch Application
d	INTGSSOPOV: SAFE_DATACENTER DYNAMIC Western (7	
	O Conversations Clusters 3 Z Policies 1 App View 0	0
a	ADM Run Configuration ①	Submit ADM Run
	ADM discovers security groups and policies for the members of this application using the observations in the selected time	range.
4	Select time range Apr 10 9:00am - Apr 13 10:00am - 3/17 3/19 3/21 3/23 3/25 3/27 3/29 3/31 4/1 4/3 4/5 4/7 4/9 4/11 4/13	695,816 total observations Showing Flow Observations
	Scope: INTGSSOPOV: SAFE_DATACENTER Member Workloads: 4 Show Show	
	External Dependencies	*
	Manage the granularity of ADM generated policies for services that are external to the application. @	3 hidden scopes Show All
	Reorder Naturally ③ Drag and Drop By Number	
	Coarse Fine	··· 0
	Coarse Fine	0
	Ccarse Fine	… Δ
	Advanced Configurations	>
		Submit ADM Run

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

C	Cisco Tetratien" SEGMENTATION		⊗ Monitoring -	⑦ - ⊗₀° -
Lat	WordPress3TierApp 🕼 SECONDARY		ĵ Sw	vitch Application
	TINTGSSOPOV: SAFE_DATACENTER DYNAMIC Version: vi PENDING	ADM r	results available.	×
665	⁵ ¹ / ₂ Conversations ⊕ Clusters 3 ¹ / ₄ Policies 1 ¹ / ₄ App View 0			
۲				
Ø	(e) I Filters (f) Filter Policies	8	Q 🕕	
Δ	Absolute policies Default policies Catch All DENY			۲
¢			Search over workloads, clusters,	policies.

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.

ē (Cisco Tetratie n°	SEGMEN	TATION				⊗ Mo	onitoring - 🕐 - 🕬
itte Litte	WordPress3T TINTGSSOPOV: SA Last Run: Apr 1, 12:41 PM	ierApp @	SECONDARY TER [DYNAMIC] Version/v18 W	forkloads: 5				Switch Application
۲	D & Conversation	ons 452	B Clusters 4 ₽ Policies 12	る Provided Services 品	App View 0	*	Policy Analysis	Denforcement
۵	@ ≡ ⊠	Quick	Analysis Filters O Filter P	Policies	8		۹ (۵)	
2	Absolute policies	Default polic	Catch All DENY		Add Default Policy			
*	Priority	Action	Consumer	Provider	Services	S	earch over wor	kloads, clusters, policies.
т Л	100	ALLOW	TINTGSSOPOV: SAFE	TINTGSSOPOV	ICMP4 more	Ì		
	100	ALLOW	🗇 Jumpbox 3	TINTGSSOPOV: SAFE	TCP : 22 (SSH) 2	Z		
1	100	ALL: •	Em	WordPress Web	✓ Ok X Cancel			
	100	ALLOW	C Employees	WordPress Web	TCP : 80 (HTTP)	2		
	100	ALLOW	Greate new filter 0 of 0 matching scopes shown	T WordPress App	TCP : 8080 (HTTP) [3		
	100	ALLOW	T WordPress App	T WordPress DB	TCP : 3306 (MySQL)	28		

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.

C.	Cisco Tei	trati∉n⁼	SEGMENTATION				⊗ M	onitoring 👻 🛞 .	• ©° •
ш	WordPr	ress3Tier	App 🖉 SECONDARY					1 Switch	Application
æ	INTGSS Last Run: Apr	OPOV : SAFE_ 1, 12:41 PM	DATACENTER	Version: v18 Workloads: 5				D Sta	Irt ADM Run
۲	D 9	Conversations	452	Policies 12 Provided Service	ces Of App View 0		√ Policy Analysis	Enforcement	··· û
۵	& ≔	121 P.	Quick Analysis Fil	ters I Filter Policies		\otimes	Q (1)		
۵ م	Absolute p	olicies 0	Default policies 11 Catch	AII DENY	Add Defau	It Policy	Policy Policy Actions		Û
	Priority	Action	Consumer	Provider	Services		Priority	100	
	100	ALLOW	TINTGSSOPOV : SAFE	INTGSSOPOV	ICMP4 more	ď	Action	ALLOW	
	100	ALLOW	Jumpbox	TINTGSSOPOV : SAFE	TCP : 22 (SSH)	ď	Consumer	Employees	
	100	ALLOW	Employees	TwordPress Web	ICMP1 more	ď	Provider	🛞 WordPress Web	
	100	ALLOW	WordPress App	WordPress Web	TCP : 80 (HTTP)	ď	View Conversations	rvice Ports: (2)	ows √~ ®
	100	ALLOW	TwordPress Web	TWordPress App	TCP : 8080 (HTTP)	ď		Delete A	II 🛨 Add
	100	ALLOW	WordPress App	T WordPress DB	TCP : 3306 (MySQL)	ľ	10 C ICMP 10 C TCP: 80 (H	ITTP)	

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.	Cisco Tetrati« n°	SEGMENTATION			🛞 Monitoring 👻	() • ®°	Ŧ
ы	WordPress3TierApp @ secondary						
ሐ	INTGSSOPOV: SAFE_DATACENTER DYNAMIC Version: v18 Workloads: 5 Start				Start ADM Ru	in	
	Last Run: Apr 1, 12:41 PM						
۲	D Conversations	452	₽ Policies 12	App View 0			Û

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



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

C.	Cisco Tetratien" SEGMENTATION @	Monitoring - 💮 - 🎕 -
hal	WordPress3TierApp @ FRIMARY	3 Switch Application
đ	INTGSSOPOV : SAFE_DATACENTER DYNAMIC Workloads: 5 Last Run: Apr 1, 12.41 PM	Start ADM Run
۲	D Conversations 452 ⊕ Clusters 3 ⇄ Policies 12 🕅 Provided Services 🖧 App View 0 小 Policy Analys	sis 🖲 Enforcement
۵	Enforced Policy Version: disabled ⑦	Enforce Policies
۵ ۵	Enforcement is disabled for this application. Traffic in, out and within this application's scope may still be enforced by policies from other enforced applications.	
\$	Select time range Mar 17 9:10pm - Mar 26 12:25am - 21 41	704,637 total observations Showing Flow Observations

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

Enforce Policies							
Select the version of policies to	enforce.						
Version	p1 😕						
Reason for action	Enter a reason for this action (optional)						
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

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

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

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

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

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

Test Description:

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



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



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.



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-managementcenter-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
- I. FMC Default Access Control Policy page 43 steps 1-3
- m. FMC Transport/Network Layer Preprocessor Settings page 44 steps 1-3

Step 2 Configure ACI and ISE

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

- 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

cisco	APIC (San Franci	isco)							a	dmin Q	0	•		٥
System	Tenants	Fabric	Virtual Net	tworking	L4-L7 Services	Admin	Operations	Apps	Integrations						
	AAA	Schedulers	Historica	al Record Polic	cies Firmware	External Dat	a Collectors	Config Rollb	acks Import/Exp	ort Downlo	ads				
AAA		C		User Ma	anagement - Secu	urity									00
C ↓ Quick Sta C ↓ Quick Sta	art				-		Management S	Settings	Security Domains	Roles	RBAC Rule	s	Public Ke	y Manage	ement
Authentic	cation										Key Ri	ngs	Certific	ate Auth	orities
Security			_											0 +	***
				 Name 		De	scription		FP		N	umber o	of Cer <mark>o</mark> n	ate Certifica	te Authority
				Cr	eate Certifica	ate Autho	ority							? ×	
					Name:	ad.cisco-x.co	m								
					Description:	AD Certifica	ite Services - (CA root							
					Certificate Chain:	pxI/VDwwEA NMCwRe3y7 InywdetA14 bb1WVUJGRe YSSyPMMISR K7qauANfdd t5Kyjo2uFD END C	VYKWYBBAGCN/ YVP1gyQkYXb1 NJy25511rp0 2YP6NiwLHAh4 m3xtf6nVJNI e+y809P1c2yc UVa9Q= ERTIFICATE	UBBAMCAQAw LwybHirqNoU DP&rh657eF UMGEntIV/UMGEntIV/U IpLam4Ypzcp R0Cfmj4bMp	DQYJKoZIhvcNAQEL fXcWh7tN57AWh7thXt950 QZwF5WhWEZCYWsst GJuE08eDNAQKxf3H	BQADggEBAHBg nCAJy9ClWgHs yAbZl7Q+Kwp 7BbTsc5hSx+b IPP/SvPX3vm+ +jqBOlsJLjf	DIRB S2Mh Zuqr 2dNA Prwq TNDh	ancel	, Sul	bmit	

- 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.

cisco	APIC) (San Fran	cisco)								admin	0		¢
System	Tenants	Fabric	Virtual N	Networking	L4-L7	Services	Admin	Operation	s Apps	Integrations				
	AA	A Scheduler	rs Histo	orical Record F	olicies	Firmware	External Dat	ta Collectors	Config Rollback	s Import/Expo	ort Downloads			
AAA			D()()	User	Manageme	ent - Secu	rity							
C Quick St	tart						,							
🚞 Users							h	Vanagement	Settings Se	curity Domains	Roles RE	IAC Rules	Public Key Manage	ment
Authenti	ication											Key Rings	Certificate Autho	rities
Security													0 ±	**-
				- Nar	me		Description	n	Admin Sta	te	Trust Point		Modulus Create Key F	ting
		Create Ke	ey Ring								0 8		MOD 2048 Delete	
			Name: S	SDC1-Key-Rin	9									
		D	escription:	optional										
		(Certificate:											
			L											
			Modulus:	MOD 512	MOD 1024	MOD 1530	5 MOD 204	48						
		Certificate	Authority: a	ad.cisco-x.con	1	~@								
		P	rivate Key.											
			1	you want to use i	in externally ger	nerated private k	ey, please provide	it here						
										Cancel	Submit			

- 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:

cisco	APIC	(San Franci	isco)								a	dmin	٩	0	٩		\$
System	Tenants	Fabric	Virtual Networ	rking L	4-L7 Services	Admin	Operations	s Apps	Int	tegrations							
	AAA	Schedulers	I Historical Re	cord Policie	s Firmware	External Da	ta Collectors	Config Roll	backs	Import/Exp	ort Downlo	oads					
AAA		Ē		loor Mone	acoment - See	urita (
C Quick St	tart	<u> </u>			igement - Sec	unty										Ę	
Users						1	Management	Settings	Securi	ty Domains	Roles	RBA	AC Rules	s l	Public Ke	ey Mana	gement
🚞 Authenti	ication												Key Rir	ngs	Certific	cate Aut	horities
Security													-	_		Ċ	1 40
				Name		Descriptio	n	Admin	State		Trust Point			м	lodulus	0.	· · · · ·
				default		Default self	-sianed SSL Cer	rtifi Comple	eted					M	IOD 2048		
				SDC1-Kev-	Rina			Started			ad cisco-x c	om		M	IOD 2048		
				,													_
		_															
		C	reate Certi	ificate I	Request			?	\otimes								
			Sul	bject: apic1	.sdc1.cisco-x.com												
			Alternate Subject N	Name:													
				Eate D	VS:sener1 example cor	n DNS-server2 eva	mple.com										
			Loc	cality: San F	rancisco												
			5	State: CA													
			Cou	untry: US													
			Organization N	Name: Cisco)-X												
			Organization Unit N	Name:													
			E	Email:													
			Pass	word:													
			Confirm Pass	word:													
							Cancel	Submit									

Hor

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

cisco	APIC	(San Frar								admin	٩	0		•	•
System	Tenants	Fabric	Virtual Ne	tworking	L4-L7 Ser	vices Admin	Operations	Apps	Integrations						
	AAA	Schedul	ers Historio	cal Record Po	licies Firm	ware External D	ata Collectors	Config Rollbacks	i Import/Ex	port Downloads					
AAA			\bigcirc	User M	anagement	- Security									
C Quick St	tart				anagement	coounty	Management S	Settinas Sec	curity Domains	Roles R	BAC Rule	s Pub	lic Kev	Manage	ment
Users								ortango orta							
Security	icauon /										Key Ri	ngs C	ertifica	te Autho	rities
														Q +	**-
				▲ Nam	e	Descripti	on	Admin Stat	e	Trust Point		Mod	Jlus		
				SDC1-	(ev-Ring	Delauit Se	II-Signed SSE Cen	Started		ad cisco-y com		MOD	2048		
				3001-1	(ey-King			Starteu		au.cisco-x.com		MOD	2040		
		K	ey Ring -	SDC1-	Key-Ring	J						Q¢			
										Policy	Fault	ts His	tory		
		0	0 🔿 🔿 🕐								_	Ŏ <u>+</u>	**-		
				Altern	ate Subject Names	seperated by commas							•		
			l	ocality: San	Francisco										
				State: CA											
			(Country: US											
			Organization	Name: Cisc	:0-X										
		1	Organization Uni	t Name:											
				Email:											
			Pa	ssword:											
			Confirm Pa	ssword:									- 11		
			ri	vHP t40 wV3 pIA	XYZ20hFCPhzc %8LhIZK8DLISE ip9WP17450Nqf NNCS2mSX1SZ hHQ== END CERTIF	µMSMH4DyJ84gq//m BElu9W3616ausuEQ nnQh92t6V7fN611x LbpbGAgO6hvhRoeW FICATE REQUEST	F4mPJqZv+4B59 1gAzeKjx9AnI3 ucHpL6ib/vDV7 5mmX2duzDI38A 	MTC4LC60H2bDUE H+d8xhn501p9DA rec/+zWCNerdpkS LxvbP6HEv1UUnVF	eMqKZeD ifYrXkjq M+qBrqX iLROd9Uc	ļ			ļ		
									S	now Usage	Close	Subm			

- d. Sign the CSR
 - 1. Navigate to the Certificate Authority server and choose Request a Certificate

Microsoft Active Directory Certificate Services - cisco-x-AD-CA Home Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation. Select a task:

elect a task: <u>Request a certificate</u>

View the status of a pending certificate request

Download a CA certificate, certificate chain, or CRL

2. Choose the Advanced Certificate Request

Microsoft Active Directory Certificate Services – cisco-x-AD-CA

Request a Certificate

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

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

Microsoft Active Directory Certificate Services – clsco-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-emedded VHRP6.http://kol1segiute/bid2.exet/st certificate request (CMC or PKCS #10 or PKCS #17): + + + + + + + + + + + + + + + + + + +
Certificate Template:
Web Server V
Additional Attributes:
Attributes:
Submit >

4. Choose Base 64 encode and Download Certificate

Microsoft Active Directory Certificate Services – cisco-x-AD-CA	<u>Home</u>
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 Q	0000
System Tenants	Fabric Virtual Net	working L4-L7 Services	Admin Operations	Apps Integrati	ons	
AAA	Schedulers Historica	al Record Policies Firmware	External Data Collectors	Config Rollbacks Impo	ort/Export Downloads	
ААА	\bigcirc	User Management - Sec	urity			800
O Quick Start Isers	000		Management Se	ettings Security Don	nains Roles RBAC Ru	les Public Key Management
Authentication					Key	Rings Certificate Authorities
Security						0 <u>+</u> %-
		 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 - SDC	C1-Key-Ring				008
					Policy Faults	History
	8000				c	· + **-
	Name	SDC1-Key-Ring				
	Admin State:	: Started				
	Description.	opuonai				
	Certificate	AGUAcgB2AGUAcjAOBgNVHQ8B DQV3KoZIhvcHAQELBQADggEB SAWYteGvaBnv6CTp149mFT23 fKYJDtyf/nKThpSbUEDLy6/ VCV+t2WKo5a3io1crb8D137 pNBH9vCXPjF7Hv+L83AHV (Vv2216gQvYKe03n38P2CM1 END CERTIFICATE	Af8EBAYCBaAvrEwYDVR01BAunxC AYKUtEUA+DqG0jKHMbsGYPY2y F7VL18FUrIygn6KHagVIK1104 JSN98zx22VSHkUJ1LhJHLN11 m+YDJAnhJh+KgeqJuPoLNvzQy QcF/FJouHNvFAZgBPq2J1KQ1x JLSYEXINCKZdVbah7A2gQP=	gYIKwYBBQUHAwEw uNafx/w8TYDJjuL NM/pIK3wRw3QgTN VM/jpWHJZSGhdp rNxpz/8JZ2cBJrT ;pPpTSoahL8toRW7		
	Modulus	MOD 512 MOD 1024 M	OD 1536 MOD 2048			
	Certificate Authority	ad.cisco-x.com				
	Private Key			St	iow Usage Close	Submit

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

cisco	APIC (San Franc	cisco)							1	admin	٩	0	٩		۵	
System	Tenants	Fabric	Virtual Ne	etworking	L4-L7 Services	Admin	Operations	Apps	Integration	ns							
	AAA	Schedulers	Historic	al Record Poli	cies Firmware	External Data (Collectors	Config Rollbacks	Import/	/Export D	ownload	ls					
AAA		C		User Ma	nagement - Secu	ırity									C		0
C Quick S	itart					Manag	annant Catting	Constitution	Demaine	Deles	DD	O Dula		Dublis K.	E		
🚞 Users						Manag	ement Setting	is Securi	y Domains	Roles	RBA	AC Rules	5	PUDIIC K	ey Mana	gemen	_
Authent 🚞	tication											Key Rin	ngs	Certifi	cate Au	thorities	3
Security															Ó	+ -	
				 Name 		Description		Admin State		Trust Po	oint		١	Aodulus	0	- ^	·
				default		Default self-sign	ed SSL Certi	Completed					1	MOD 2048	в		
				SDC1-Key	Ring	CA Signed certif	ficate	Completed		ad.cisco-	-x.com		1	MOD 2048	в		

- 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**

cisco	APIC (San Francis	sco)					admin Q	0 4		0
System	Tenants Fabric	Virtual Networking	4-17 Services	Admin Oper	ations Anns	Integration	2			
Inver	ntory Fabric Policies	Access Policies		- turning - opport	anono Appo	integration	-			
D										
Policies	()	🕄 🔘 🛛 Managemer	nt Access - de	fault						00
C Quick St	tart							Policy	Faulte	History
> 🚞 Pods								Policy	rauits	HIStory
> 🚞 Switche	'S								Ο.	<u>+</u> **-
> 🔚 Modules	S	Properties								
> 🚞 Interface	es		Name: defa	ult						
V 🚞 Policies			Description: opt	lonal						
V 🚞 Pod										
> 🚞 D	ate and Time	HTTP					TEL NET			
> 🚍 S	NMP		Admin State: Disa	abled			Admin State:	Disabled	~	
~ 🖿 M	lanagement Access		Port: 80				Port:	23	0	
	default		Redirect: Disa	abled			SSH		, v	
<mark>,</mark> IS	SIS Policy default	, i i i i i i i i i i i i i i i i i i i	Allow Origins: http	://127.0.0.1:8000			Admin State:	Enabled	~	
> 🚞 Swite	ch	Allow	Cradantiala	cabled Eachied			Password Auth State:	Enabled	~	
> 🚞 Interf	face	LITTES	Credendais.	Enabled			Port:	22	0	
> 🧮 Glob	al	HIIPS	Admin State: Ena	hled			Ciphers:	aes128-ct	r	
> 🚞 Moni	itoring		Port: 443					aes192-ct	r	
> 🚞 Trout	bleshooting		Allow Origins: http	V 1127.0.0.1-8000			MACs	≥ aes256-ct	r.	
> 🚞 Geol	location	•	Now Origins. The				MAGS.	Mmac-sha	2-256	
> 🚞 Macs	sec	Allov	v Credentials:	sabled Enabled				Mmac-shall	2-512	
> 🚞 Analy	ytics	S	SL Protocols:	LSv1			SSH access via WEB	-		
Tena	int Quota			LSv1.1 LSv1.2			Admin State:	Disabled	\sim	
> 📩 Tags			DH Param: 10	204 2048 4096	None		Port.	4200		
		Ad	Imin KeyRing: SDC	C1-Key-Ring	3					
		c)per KeyRing: uni/u	userext/pkiext/keyring-def	fault					
		Client C	Certificate TP: sele	ect an option						
		Clie Authen	ent Certificate	sabled Enabled						
		SSL Cipher 0	Configuration:			* +				
				D	State					
			3D	ES	Disabled	*				
			aN	IULL	Disabled					
			DL	E-PSA-AES128-SHA	Disabled					
			DF	IL NOATAESTED SHA	LISANGU					
							Show Usage	Res	et S	ubmit
									_	

Step 3 Configure ISE for ACI Integration

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

dentity Services Engine	Home	Context Visibility	 Operations 	▶ Policy	Administration	✓ Work Centers
Network Access Overview Identities Id Groups Ext Id Sources Network Resources Policy Elements Policy Sets Troubleshoot Reports Settings Dictionaries Guest Access Overview Identities Identities Identities Identities Network Devices Portals & Components Manage Accounts Policy Sets Reports Custom Portal Files Settings	TrustSec Overview Componen TrustSec F Policy Set SXP Troubleshe Reports Settings BYOD Overview Identities Identity Gr Network D Ext Id Sou Client Prov Portals & C Policy Eler Policy Set Reports Custom Po Settings	oups evices rces visioning Components ments s portal Files	 Operations Profiler Overview Ext Id Sources Network Devic Endpoint Class Node Config Feeds Manual Scans Policy Elemen Profiling Polici Policy Sets Troubleshoot Reports Settings Dictionaries Posture Overview Network Devic Client Provisio Policy Elemen Posture Policy Policy Elemen Posture Overview Network Devic Client Provisio Policy Sets Troubleshoot Reports Settings Settings 	res ning ts	 Administration Device Adm Overview Identities User Identi Ext Id Sou Network R Policy Eler Device Adi Reports Settings PassiveID Overview Providers Subscriber Certificates Troublesho Reports 	 vvork Centers ninistration ity Groups rces esources ments min Policy Sets
			. D		T. (100	

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

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

dentity Services Engine	Home	ity > Operations	► Policy ► Ac	dministration	✓ Work Centers	
Network Access Guest Access	TrustSec ► BYOD ►	Profiler Posture	Device Administration	ation Pass	siveID	
► Overview ► Components ► Trus	tSec Policy Policy Sets	SXP Troubleshoo	ot Reports ▼S	Settings		
G	Enapoint Groups (EEFOS),	and endpoint (EF) coni	guration of Cisco Ap	plication Centro	chinastructure (ACI).	
General TrustSec Settings	Enable ACI Integration	(i)				
TrustSec Matrix Settings						
Work Process Settings	ACI Cluster Details					
SXP Settings	The cluster is comprised of	multiple controllers that	provide operators ur	nified real-time r	monitoring, diagnostic	с,
ACI Settings	and configuration manager	nent capability for the AC	A TADRIC.			
	IP Address / Host name *	10.16.1.11				0
	Admin name *	ise-admin				
	Admin password *	••••				
	Tenant name *	IenantA				
	L3 Route network name *	SDC1-L3OUT				0
					Test Ostilians	
					Test Settings)
	Name Conversion					
	New EPGs created by lear	ning SGTs from ISE will I	nave this suffix appe	nded i.e. name	will appear in ACI as	
	name SGT suffix.					
	New SGT suffix *	EPG				
	New SOT SUIIX					
	New EPG suffix *	_SGT				
	SXP Propagation					
	Specify SXP Domains that SXP Domains defined on the second secon	will share their mappings he SXP Mappings page.	with ACI. Incoming	ACI mappings	will be propagated by	
	O All SXP Domains					_
	Specific SXP Domains	× default				

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.

dentity Services Engine	Home	Context Visibility Operations	Policy Administration	▼ Work Centers	
Network Access Guest Access	▼ TrustSec	BYOD Profiler Posture	Device Administration F	PassiveID	Click bere to do visibility setur
Overview Components Trus	stSec Policy	Policy Sets + SXP + Troubleshoot	Reports Settings		olicit here to do visibility setti
0	•				
Security Groups	Security G	roups			
IP SGT Static Mapping	or Policy Ex	port go to Administration > System > Backu	p & Restore > Policy Export Pa	ige	
Security Group ACLs					Selected 0
Network Devices	🖾 Edit	🕂 Add 🗵 Import 💆 Export	🕇 Trash 👻 🗿 Push	Verify Deploy	Show All
Trustsec Servers	□ Icon	Name 💵	SGT (Dec / Hex)	Description	Learned
		IoT_Utility_Power_Sys	31/001F		
		WordPress_APP_EPG	10001/2711	Learned from APIC. Suffix: _EP	G Application profil ACI
	□ ●	WordPress_DB_EPG	10007/2717	Learned from APIC. Suffix: _EP	G Application profil ACI
		WordPress_Telemetry_EPG	10006/2716	Learned from APIC. Suffix: _EP	G Application profil ACI
		PartnersSGT	38/0026		

Step 4 Create an FMC Access Control Policy

- a. Create an Access Control Policy
 - 1. Click Policies > Access Control > Access Control and click + New Policy
 - 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

Overview Analysis Po	licies Devices	Objects AM	1P Intelligence			Deploy System	n Help 🔻 admin 🔻	
Access Control > Access C	ontrol Network	Discovery Ap	plication Detectors	Correlation	Actions •			
				OI	oject Managemer	nt Intrusion Network Analysis Polic	y DNS Import/Export	
							New Policy	
Access Control Policy		Domain	St	atus		Last Modified		
New Policy					? ×	2020-08-29 07:00:55 Modified by "Firepower System"	D 🛛 🖉 🙃	
Name:	SDC1-FTD-Cluster					2020-08-29 07:00:55 Modified by "Firepower System"	Pa 🖪 🖉 🙃	
Description: Select Base Policy:	None		~			2020-08-29 07:00:55 Modified by "Firepower System"	Pa 🖪 🥒 🙃	
Default Action:	Block all traffic	Intrusion Preventi	on 🔿 Network Discov	2020-08-29 07:00:55 Modified by "Firepower System"	Pa 🖪 🥔 🛱			
Targeted Devices					2020-11-17 21:50:29 Modified by "admin"	Pa 🖪 🥔 🛱		
Select devices to wind Available Devices	hich you want to apply	this policy.	Selected Devices			2020-08-29 07:00:55 Modified by "Firepower System"	Pa 🖪 🥔 🛱	
Search by name	e or value		SDC1-FTD-C1	L		2020-08-29 07:00:55 Modified by "Firepower System"	Pa 🖪 🥔 🛱	
FTD-CAMP-HA	A.							
FW-DC-1								
SDC1-FTD-C1	1	Add to Policy						
SDC2-FTD-C1	1	(Add to Folicy						
TB-FTDv-HA								
				Save	Cancel			

- 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

Overview Analysis Policies	Devices Object	AMP Intelligence	ᠲ Deploy System Help ▼ admin ▼										
Access Control > Access Control	Network Discover	y Application Detectors Correlation	Actions 🔻										
SDC1-FTD-Cluster													
Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None													
Rules Security Intelligence HTTP Responses Logging Advanced													
Name Sou D	es Sou Des	VLA Users App Sou Des	URLs Sou Des Ac										
✓ Mandatory - SDC1-FTD-Cluster (- There are no rules in this section. Add R	-) tule or Add Category	Identity Policy ISE-SecureDC	* ×										
▼ Default - SDC1-FTD-Cluster (-)													
There are no rules in this section. Add R	tule or Add Category	Revert to Defaults 0	DK Cancel										
Default Action		Access Control: Block All Traffic											

- c. Add a rule
 - 1. Click +Add Rule
 - 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

Overview Analysis Policies Devices C	bjects AMP Intelligence													
Access Control > Access Control Network Di	scovery Application Detectors Correlation Act	ions 🔻												
You have unsaved changes 🔊 Show Warnings Analyze Hit Counts 🔚 Save Save SDC1-FTD-Cluster														
Prefilter Policy: Default Prefilter Policy. Identity Policy: SSL Policy: None Identity Policy: Security Securit														
Rules Security Intelligence HTTP Responses	Logging Advanced	Inneritance Settings Menory Assignments (1)												
Filter by Device Search Rules	:	K Show Rule Conflicts 😣 📀 Add Category 🚺 Add Rule												
Add Rule	MLA Heart Appl Sour Doct HDLe	Sour Doct Act ? X												
Name Allow Employees	Z Enabled Insert	into Default												
Action Allow	▼ ∪ Q 2 th I													
7 Time Range None 🗸 📀														
Zones Networks VLAN Tags Users	Applications Ports URLs SGT/ISE Attributes	Inspection Logging Comments												
Application Filters Clear All Filters 🗶	Available Applications (13)	Selected Applications and Filters (2) 🛛 📌 🖆 🕥												
Search by name	A http	Applications												
User-Created Filters	HTTP/SSL Tunnel	НТТР 🗒												
A sisks (Any Selected)		HTTPS												
Very Low 1217														
Medium 996	Python-httplib													
		Add Cancel												

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.

Overview Analysis Policies Devi	ces Objects AMP	Intelligence			0 Deploy System	Help 🔻 admin 🔻					
Access Control > Access Control Net	work Discovery App	lication Detectors	Correlation A	Actions 🔻							
SDC1-FTD-Cluster		You have	unsaved changes 🛛	Show Warnings	Analyze Hit Counts	Save 🔀 Cancel					
Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy											
Rules Security Intelligence HTTP Res	sponses Logging A	dvanced			alline () () Add Categ						
Filter by Device Search Rules					Add Categ	ory 🕥 Add Rule					
🖌 Add Rule						? ×					
Name Allow Employees		Enabled	Insert	into Default	•						
Action Action Time Range None	 ⊘	ita J									
Zones Networks VLAN Tags	Users Applications	Ports URLs S	GT/ISE Attributes	5	Inspection Logging	Comments					
Available Metadata 🖒		Selected Source	Metadata (1)	Selecter	d Dest Metadata (1)						
Search by name or value	Add to	EmployeesSG	т	🗒 🛛 🖨 Word	dPress_WEB_EPG	ii ii					
Security Group Tag 💙											
WORDPRESS_DB_EPG	Add to Destination										
WordPress_Telemetry_EPG											
WordPress_WEB_EPG	Y	Add a Location IF	P Address	Add							
					Add	Cancel					

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

Overvi	ew An	alysis Policies	Devices O	bjects AN	1P Inte	lligence					₽ ₆ De	ploy	System	Help 🔻 a	admin 🔻
Access	Control	► Access Control	Network Di	scovery Ap	plication I	Detectors	s Correlation	Ac	tions 🔻						
SDC1	FTD	-Cluster				You ha	ive unsaved changes	5	Show Wa	rnings	Analyze Hi	t Coun	ts 📔 S	ave 🔇 🔇	Cancel
Prefilter	Policy:	Default Prefilter Policy					SSL Policy: None						Ide	ntity Policy	/: ISE- SecureDC
_										1	Inheritan	ce Sett	ings 🖳 Po	licy Assignr	ments (1)
Rules	Secur	ity Intelligence HT	TP Responses	Logging	Advanced										
📸 Filte	r by Devi	ce 🚔 Search R	ules						X 🗌 Sho	ow Rule C	onflicts 🙆	0	Add Categor	у 🔘 А	Add Rule
" Add	Rule														? ×
Na	me	Allow Employees			Z E	nabled	I	nsert	into Defau	lt	~				
Act	ion	Allow		 U U D 	2 1 2										
7 Tin	ne Range	None	~ 📀												- 2
D Z	ones	Networks VLAN Ta	ags Users	Applications	Ports	URLs	SGT/ISE Attribu	tes			Inspectio	on I	Logging	Commen	ts
File Sen	Log at Beg Log at End Events: Log Files d Connect	ginning of Connection d of Connection tion Events to:													
												Д	vdd	Cancel	

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

Overview Analysis Policies Devices Object	s AMP Intelligen	ce		De	ploy System	Help 🔻	admin 🔻						
Access Control Access Control Network Discover	y Application Detect	ors Correlation	Actions •										
SDC1-FTD-Cluster			You have unsaved ch	anges Analyze H	it Counts 📔	Save	Cancel						
Prefilter Policy: Default Prefilter Policy		SSL Policy: None			Iden	tity Policy:	<u>ISE-</u> SecureDC						
				Inheritan	ce Settings 🖳 I	Policy Assign	ments (1)						
Rules Security Intelligence HTTP Responses Lo	Rules Security Intelligence HTTP Responses Logging Advanced												
📸 Filter by Device 🛛 ≓ Search Rules			v Rule Conflicts 😡	ts 😣 (Add Category 🛛 🗿 Add Rule									
Name #	Applications So	ource SGT	Dest SGT	Action	a 🔍 🗈 🔎	1	*						
➡ Mandatory - SDC1-FTD-Cluster (-)													
There are no rules in this section. Add Rule or Add Category													
▼ Default - SDC1-FTD-Cluster (1-2)													
1 Allow Employees	HTTP HTTPS	EmployeesSGT	PwordPress_WEB_	EI 🖋 Allow	a v D .	2 📩 🗾 o	a 🖉						
2 Block Contractors	HTTP HTTPS	ContractorsSGT	PwordPress_WEB_	EI 🗙 Block	a 🗉 🗅 <i>Я</i>	e 💼 🗾 o	Ø						
Default Action			Access Control: Block	: All Traffic			× \$ 📑						

7. Click Save and Deploy

Step 5 Test Results

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



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

C 🛦 Not secure 10.9.10.41/events/index.cgi?table=rua_event Q 🏠 (
Overview Analysis Policies Devices Objects AMP Intelligence Q Deploy System Help 🕶 adr													
Context Explorer Connection	Context Explorer Connections • Intrusions • Files • Hosts • Users > Users Activity Correlation • Advanced • Search												
User Activity <u>Table View of Events</u> > <u>Users</u> No Search Constraints (<u>Edit Search</u>)	User Activity Bookmark This Page Report Designer Dashboard View Bookmarks Search • User Activity I 2020-11-23 00:00:00 - 2020-11-23 01:25:02 C Table View of Events > Users I 2020-11-23 00:00:00 - 2020-11-23 01:25:02 C No Search Constraints (Edit Search) Expanding												
☐ ▼ <u>Time</u> ×	Event ×	<u>Username</u> ×	<u>Realm</u> ×	Discovery X Application	Authentication Type	X IP Address X	Start × Port	<u>Security</u> X <u>Group</u> Tag	Endpoint × Profile	Endpoint X Location	Device ×		
2020-11-23 00:37:28	<u>User Login</u>	Bob	SecureDC	DAP	Passive Authenticatio	on 📑 10.9.110.102		ContractorsSGT	Belkin-Device	10.9.255.19	fmc.cisco-x.com		
♣ ☐ <u>2020-11-23 00:36:51</u>	<u>User Login</u>	Aaron	SecureDC	LDAP	Passive Authenticatio	on 🗃 10.9.110.101		EmployeesSGT	Belkin-Device	10.9.255.19	fmc.cisco-x.com		
I of 1 >> Displat	ying rows 1–2 o	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.

Ove	Dverview Analysis Policies Devices Objects AMP Intelligence Objects AMP Intelligence Objects AMP Intelligence																		
Conte	ext Expl	orer Connectio	ns ► Eve	ents In	trusions •	Files ¥ Ho	sts 🔹 Use	ers Correlation	 Advance 	ed 🕶 🖇	Search								
	Bookmark This Page. Report Designer: Dashboard. Wew Bookmarks: Search •															Search ¥			
Cor	Connection Events (witch workflow)																		
Conn	ections	with Application Det	tails > Tal	ble View of C	Connection E	vents											1 2020-11-22.00	:00:00 - 2020-11-2	Expanding
► Sea	irch Cons	traints (Edit Search Sa	ave Search	1)															101000000000000000000000000000000000000
Jur	np to	•																	
	_ E	irst Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port/ ICMP IYPS	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	▼ URL Category	URL Reputation
4	2	020-11-23 01:59:20		Allow		10.9.110.101		10.18.107.101		ACI-PBR	ACI-PBR	64192 / tcp	80 (http) / tcp	HTTP	Edge		http://wp1.sdc-m.cisco-x.com/		Unknown
4	2	020-11-23 01:59:11		Allow		10.9.110.101		10.18.107.101		ACI-PBR	ACI-PBR	<u>49681 / tcp</u>	80 (http) / tcp	HTTP	Edge		http://wp1.sdc-m.cisco-x.com/		Unknown
4	2	020-11-23 01:52:30		Block		10.9.110.102		10.18.107.101		ACI-PBR	ACI-PBR	<u>54718 / tcp</u>	<u>80 (http) / tcp</u>	HTTP	Eirefox		http://wp1.sdc-m.cisco-x.com/		Unknown

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/hyperflexhx-series/datasheet-c78-736784.pdf

Cisco Multi-Site ACI Architecture Whitepaper

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

Cisco Application Centric Infrastructure Data Sheet

https://www.Cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policyinfrastructure-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-centricinfrastructure/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-seriesswitches/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-seriesswitches/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/tetrationanalytics/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

291

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.win 64-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

SAFE Design Guide

292

ıılıılı cısco

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)