The bridge to possible

Design Guide Cisco Public

Secure Cloud for AWS (laaS)

Design Guide

June 2021

Contents

Abstract	4
Scope	4
SAFE Architecture - Introduction	5
Cloud Business Flows	6
Public Cloud Attack Surface	8
Solution Overview	9
What is our security approach?	9
Secure Cloud Business Flows	10
Cisco's Secure Architecture for AWS	
Secure Cloud Architecture	11
Business flows in Cisco's Reference Architecture	
Security Integrations	
Cisco Tetration	16
Cisco Advanced Malware Protection for Endpoints	
Cisco Stealthwatch Cloud	19
Cisco Umbrella	21
Next-Generation Firewall Virtual	22
Web Application Firewall and DDoS Prevention	24
Cisco Duo	25
Cisco SecureX	26
Design Implementation	
Deployment Overview:	29
Set up the AWS VPC components	
Integrating Stealthwatch Cloud	
Onboard AWS VPC to Cisco Defense Orchestrator	
Set up Umbrella DNS Security	35
Setting up the RDS database	
Setting up the App and Web Load Balancers	
Setting up Web and App Auto Scaling groups	
Setting up the Firepower Next-Generation Firewalls	
Enabling WAF and DDoS protection	56
Integration with Cisco SecureX	59
Validation Testing	60
Tetration	60
Test Case 1: Creating an application workspace for AWS cloud application	61

66 67 69 72 72 73 73 75 75
67 69 72 72 73 73 75 75 76
.69 .72 .72 .73 .73 .75 .75 .75
69 .72 .72 .73 .73 .73 .75 .75 .76
.72 .72 .73 .73 .75 .75 .75
72 .73 .73 .75 .75 .75
.73 .73 .75 .75 .75
.73 .75 .75 .75
.75 .75 .76
.75 .76
.76
.77
. 79
.79
.80
.81
.81
83
.83
.84
.84
.85
،۔ ،۔ ، ، ، ،

Abstract

This design guide aligns with the <u>Cisco[®]</u> Secure Cloud Architecture guide. The Secure Cloud Architecture guide explains the secure architecture for cloud applications, critical business flows; attack surfaces and corresponding security controls required for the cloud environment. This guide proposes a Cisco Validated Design (CVD) for security in a tiered application architecture. The solution proposed in this guide leverages Cisco security controls along with Cloud-Native security controls to achieve the desired security posture for applications in AWS.

Scope

This document illustrates the design and security aspects of an application hosted in AWS. Along with the design and security specifications, this document also delves into the details of implementation and validation steps for the proposed architecture.

This guide covers the following security controls.

- Cisco Tetration
- Cisco Advanced Malware Protection for Endpoints (AMP4E)
- Cisco Stealthwatch Cloud (SWC)
- Cisco Umbrella
- Cisco Firepower Next-Generation Firewalls Virtual (NGFWv)
- Cisco Adaptive Virtual Security Appliance (ASAv)
- Cisco Defense Orchestrator (CDO)
- AWS Web Application Firewall (WAF) and Shield service
- Radware Cloud Web Application Firewall (WAF) and DDOS prevention
- Cisco Duo Beyond
- Cisco SecureX threat response

For setting up the web application, we used the following AWS cloud components and services.

- AWS Virtual Private Networks (VPC)
- AWS Route Tables
- AWS Internet Gateway
- AWS Relational Database Service (RDS) Service
- AWS Auto Scale
- AWS Elastic Cloud Compute (EC2) Service
- Network Load Balancer
- Amazon Simple Storage Service (S3)
- Amazon Machine Image (AMI)
- AWS Route53

- AWS API Gateway
- AWS Lambda Service
- AWS Identity and Access Management (IAM)

SAFE Architecture - Introduction

As your data flows from an increasing number of devices to your data center or private/public cloud, you must understand your data flow, to be able to protect it. Cisco SAFE is an architectural approach that helps you visualize this transit of the data in terms of business flows, understand the attack surface associated with these flows and hence, devise appropriate capabilities to secure them. This framework provides complete guidance from the initial identification of business flows in a given architecture to securing it and then deploying and validating the solution.

These validated designs provide guidance that is complete with configuration steps that ensure secure deployments for your organization. Cisco Validated Designs (CVDs) for various SAFE PINs can be found at <u>SAFE home page</u>.

Cisco SAFE simplifies network security by providing solution guidance using the concept of 'Places in the Network' (PINs). This design guide is a recommended threat defense architecture for the Cloud PIN (see figure 1). Within the Cloud PIN, this design guide specifically covers the AWS cloud.









Figure 2. SAFE Guidance Hierarchy

For more information on SAFE framework and architecture/design guides, check out the <u>SAFE documentation</u> (select architecture/design tab).

Cloud Business Flows

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

This solution addresses the following business flows for a typical tiered web application hosted in AWS:





Cloud business flows

- Customer browsing an e-commerce web application. The customer, sitting somewhere out on the Internet, browses the e-commerce web application hosted in the AWS cloud
- Application workloads downloading updates/patches from update servers outside the cloud (Internet).
 Application workloads sitting in the cloud need to reach out to various update servers to fetch the updates and patches at regular intervals
- Systems communicating east/west within the AWS cloud. For example- the frontend web servers will
 make HTTP requests to backend application engine or the application workloads will make API calls
 among themselves
- · Application workloads transacting data with the database server within the cloud
- DevOps remotely accessing the management zone for workload management/update/patching purposes

Public Cloud Attack Surface

The secure cloud design protects systems by applying security controls to the attack surface found in the public cloud. The attack surface in public cloud spans the business flows used by humans, devices, and the network.

Threats include; rogue identity, DDoS, web vulnerabilities, infections, and advanced persistent threats allowing hackers the ability to take control of your devices and networks.

Considering the business flows elaborated in the last section (Figure 3), a deep dive into the attack surface for each of those business flows is shown below.



Figure 4.

Public cloud attack surface

• An untrusted/compromised user, out on the Internet, may try to exploit the cloud application or flood it with fake traffic to render it incapable of serving the genuine users

- The workloads need to communicate with update servers out on the untrusted public network. An attacker might compromise workloads to download malware to the application environment or upload crucial data to malicious servers
- Systems communicating east/west within the AWS cloud may spread the infection from one workload to another within the cloud, eventually compromising the whole application
- An attacker may compromise the application workloads to steal or corrupt data stored on the database servers
- A malicious user may try to gain the same privileged access as DevOps to compromise the complete application environment in AWS

Solution Overview

Cisco's security approach for the modern cloud applications allows companies to achieve:

- Improved resiliency to enable cloud availability and secure services
- Operational efficiency from automated provisioning and flexible, integrated security
- Advanced threat protection from <u>Cisco TALOS</u> industry-leading threat intelligence to stay up to date, informed, and secure

What is our security approach?

Specific capabilities are necessary to protect the public cloud and build the appropriate layers of defense. These capabilities work together to create several layers of defense protecting the cloud applications. The top priorities or the three pillars that we keep in mind while designing the secure public cloud solutions are:

- 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 access control and micro-segmentation
- **Threat Protection** Stop the breach by deploying multi-layered threat sensors strategically in the public cloud to quickly detect, block, and dynamically respond to threats



Secure Cloud Business Flows

Developing a defense-in-depth architecture requires identifying existing threats and applying appropriate security capabilities to thwart them. Business flows and the corresponding attack surface and threat patterns that we defined earlier (Figures 3 and 4) are mapped to their corresponding security controls as below.



Figure 5. Secure business flows

Cisco's Secure Architecture for AWS

The tiered application architecture has been a popular underlying principle for web application deployment for over a decade now and it remains equally relevant to date.

The multi-tier architecture provides a general framework to ensure decoupled and independently scalable application components. Each tier is separately developed, scaled, maintained and secured.

In the simplest tiered architecture form, the web applications would have the following layers:

Web tier: The end-user directly interacts with this layer. This tier has all the static web content.

Application tier: This tier is responsible for translating the user actions to application functionality. This tier carries the core application code components. For example, application code performing the read/write database operations.

Database tier: Storage tier or the database tier holds the data relevant to the application.

In this design, we are securing a tiered web application in the AWS cloud. We add various security capabilities and controls, that we established in the previous sections, to a tiered web application model to make it much more robust, secure and transparent in its security posture.

Secure Cloud Architecture

The Cisco Secure Cloud reference architecture solution includes all the security capabilities that we illustrated in previous sections.



Figure 6.

Cisco Secure Cloud Reference Architecture

Business flows in Cisco's Reference Architecture

Considering the design above, all the threats, corresponding security capabilities and solutions required to attain those capabilities can be mapped as below.

Threat		Security Capa	ability	Security Solutions	
.	Attackers or malicious users accessing restricted resources and information.		Identity based access	Cisco Duo - 2FA	
<u>@</u>	Massively scaled attacks that overwhelm services.		DDoS prevention	Radware DDoS prevention	
<u></u>	Attacks against poorly developed applications and web vulnerabilities.		Web Application Firewalls	Radware Web Application Firewall	

Threat		Security Capa	ability	Security Solutions
<u></u>	Network breach causing unauthorized access and malformed packets between and within application in the cloud.		Segmentation	Cisco Firepower NGFWv Cisco Tetration
	Zero-day malware attacks and other forms of covert threats.		Threat visibility	Cisco Stealthwatch Cisco Tetration Cisco AMP4E Cisco Firepower NGFWv
<u>Q</u>	Attacks using worms, viruses, or other techniques.	9	Intrusion Prevention	Cisco Firepower NGFWv Cisco AMP4E
<u></u>	Infections, attackers using a compromised workload to spread the damage.		Micro- segmentation	Cisco Tetration
	Malware distribution among workloads or between servers.		Anti-malware	Cisco Firepower NGFWv Cisco AMP4E
	Traffic, telemetry, and data exfiltration from successful attacks. Covert threats.		Flow Analytics	Cisco Stealthwatch Cisco Tetration Cisco Umbrella
@	Exploiting privileged access to run shell code		Process Anomaly Detection & Forensics	Cisco Stealthwatch Cloud Cisco Tetration Cisco AMP4E
<u>Q</u>	Malware distribution across networks.		Network Anti- Malware	Cisco Firepower NGFWv
<u>.</u>	Exploiting unpatched or outdated applications.		Vulnerability Assessment and Workload Inventory	Cisco Tetration
	Redirection of session to malicious domains.		DNS Layer Security	Cisco Umbrella - DNS Layer Security

Threat		Security Capa	ability	Security Solutions
	Exposed services and data theft.		VPN Gateway or Concentrator	Cisco ASAv Cisco Firepower NGFWv

At this point, we have established the attack surface and, the capabilities and security solutions that we needed to secure the business flows mentioned previously.

- Customer browsing an e-commerce web application
 - Access to the web application is secured using Duo Multi-Factor Authentication (MFA)
 - WAF and DDoS Services protect against web vulnerabilities and denial of service attacks. In this document, we will demonstrate Radware cloud WAF and DDoS service
 - Perimeter segmentation is done using next-generation firewalls (NGFW) to protect against any network level breaches. NGFWs also provide next-generation IPS and AMP capabilities along with stateful firewall, AVC (Application Visibility and Control) and URL filtering
 - Micro-segmentation of workloads is done using the Tetration policy enforcement agents. This would prevent any malware or malicious movement within the pool of workloads in a specific tier
 - Stealthwatch Cloud provides enhanced threat visibility into workload activity and the AWS cloud. It looks for any anomalous activity within the application environment. It also facilitates the flow analytics
 - Tetration agents allow us to gain a deep visibility into vulnerable packages and processes on the workloads that an attacker may leverage. It also provides a very robust network flow analytics for workload communications
 - AMP4E detects and quarantines any malware that may infect the workloads
- · Workloads downloading updates/patches from update servers
 - Workloads are segmented into App and Web tier using Tetration Enforcement agents. No direct inbound public access is allowed to the App and Web servers, management access is allowed only from the management tier (also controlled via Tetration)
 - DNS layer security is achieved using Cisco Umbrella. This prevents any accidental or deliberate exposure to a malicious domain
 - · Stealthwatch Cloud and Tetration provide enhanced threat visibility and flow analytics
 - · AMP4E detects and quarantines any malware that may get downloaded to application workloads
- Systems communicating east/west within the AWS cloud
 - Workloads are micro-segmented using Tetration Enforcement agents. Web, App, Database and Inside tier has no direct inbound public access/addresses. Only Management and the Outside tier is allowed Public IP addressing, hence exposing them to untrusted public network/internet
 - Micro-segmentation within Web and App tier is done using the Tetration enforcement agents. This
 restricts any internal movement among the workloads
 - DNS layer security using Umbrella provides visibility into workload activity
 - Stealthwatch Cloud and Tetration provide enhanced threat visibility and flow analytics for this flow. They also look for any anomalous movement within the application environment or among the workloads within a tier. Tetration agents provide deep visibility into the workloads
 - AMP4E protects against malware spread

- Application engine transacting data with database server within the cloud
 - AWS Security Groups restrict access to the database. Only App tier is allowed to communicate with database tier
 - DNS layer security using Umbrella
 - Stealthwatch Cloud and Tetration provide enhanced threat visibility and flow analytics. They also look for any anomalous movement within the application environment or among the workloads within a tier. Tetration agents provide deep visibility into the workloads
 - AMP4E protects the application workloads against any malware infection
- DevOps remotely accessing the management zone for workload management/update/patching purposes
 - Anyconnect VPN mobility client is used to provide Secure Remote Access to the management tier. An ASA or NGFWv can be used for VPN termination. We tested a standalone ASAv for this design. Refer to the <u>Secure Remote Worker</u> design guide for detailed information on secure remote access designs and deployments
 - Management zone is segmented using Tetration enforcement agents. This provides the control knob for restricting access to workloads or the various other tiers
 - Stealthwatch Cloud and Tetration provide enhanced threat visibility and flow analytics. They also look for any anomalous movement or activity within the application environment or from the management tier. Tetration agents provide deep visibility into the workloads
 - · AMP4E protects the jump servers and workloads against any malware infection

Security Integrations

Let's look at each of the security integrations in this secure design in more depth, we will start from the security controls on the workload itself and go all the way to the edge of our public cloud web application.



We start by looking at workload security using Tetration and Advanced Malware Protection, followed by an agentless deployment of Stealthwatch cloud for greater visibility into the AWS environment and workload activity. Then, we will look into Umbrella DNS layer security at the AWS VPC level.

Afterwards, we move to perimeter protection using Cisco Firepower NGFWv (policy orchestrated by Cisco Defense Orchestrator). We will also explore WAF and DDoS protection using Radware Cloud service.

Lastly, we will secure the access to our cloud application using Duo Multi-Factor Authentication.

To connect all these security controls to a single pane of glass, we will look at Cisco SecureX integrations.

Cisco Tetration

Tetration has a SaaS offering that provides the capability to do micro-segmentation in a highly flexible manner along with an in-depth visibility into the workloads.

Tetration offers visibility and enforcement agents that are installed on the workloads. The enforcement agents provide an additional capability to enforce policies.

Tetration can dynamically learn various ongoing changes in the cloud workload environment and enforce an adaptive micro-segmentation. The Tetration portal allows us to create workspaces and graphical views for applications and enforce security from the web application point of view unlike the traditional network perspective.

The Tetration platform supports multi-cloud and hybrid environments and hence, make the whole process of security operations seamless across the board.



Figure 7.



In this specific architecture, Web and Application tier has workloads in Auto Scaling Groups. To enable the auto-provisioning of Tetration agents, we used the <u>User Data</u> option provided for EC2 Instances. When the Auto Scaling Group deploys a new workload, the shell script will install the Tetration agent on it as part of the initialization process. Refer to the implementation section of this guide for more details.

Once the Tetration agent on the new workload is registered with the Tetration cloud (SaaS), it starts exporting the network flow and process information to the Tetration cloud engine for analysis. Tetration ensures Cisco's Zero Trust model by offering key features like:

- Policy enforcement (Micro-segmentation)
- Visibility into workload process activity
- Network flow visibility
- Software vulnerability reports

- Forensic analysis
- Behavior deviations

Based on all these features and more, the Tetration dashboard provides us with a very convenient and flexible scoring mechanism to monitor the security compliance of cloud applications. Tetration considers six parameters to calculate this score (Figure 8), and these parameters can be adjusted based on one's preference or requirements.

SCOPE SECURITY SCORE May 15, 2	Æ Adjust Module Weig	jhts		\[\] \[Filter Workloads \] \[\] \[Adjust Weights \]
100		Vulnerability	Process Hash	
C+) ∞	58	Attack Surface	Forensics	
Overall Score	Weighted Score	Network Anomaly	Segmentation Compliance	May (0 May 15
SCORE BREAKDOWN	Restore Defaults		Cancel Confirm	

Figure 8.

Tetration Dashboard - Weighted Score



Figure 9.

Tetration Dashboard - Compliance Score Board

Refer to the <u>Tetration documentation</u> for more detailed information on cloud workload protection.

Cisco Advanced Malware Protection for Endpoints

The AMP4E agents installed on the cloud workloads provide us protection against zero-day attacks. Powered by <u>Cisco TALOS</u>, AMP4E not only relies on antivirus, but also uses machine learning and file reputation to block both file-based and file-less attacks. It also enables you to isolate the infected host before the malware is spread onto the others in the network. Advanced Malware Protection also supports taking forensic snapshots that help immensely with the security investigations.



Figure 10.

Cisco Advanced Malware Protection for Endpoints

In this specific architecture, just like the Tetration agent, the web and application workloads in Auto Scaling Group are auto-provisioned with AMP4E agents using <u>User Data</u> option available under Auto Scaling Group configuration. When the Auto Scaling Group deploys a new workload, a shell script will install the AMP4E agent on the workload as part of the initialization process.

As soon as AMP4E agent on the new workload registers with the AMP cloud, the workload is continuously monitored and reported for any malicious activity. AMP's host isolation feature comes in very handy to contain any spread of malware in the cloud workloads.

Dachboard				
Dashboard				
Dashboard Inbox	Overview Events iOS Clarity			
▼ Filter: (New)			Select a Filter	\$
Event Type	Threat Detected	+	Group XThreeTier-CloudApp	+
Filters Ad	d filters by clicking on the $\overline{\mathbb{T}}$ icon in the ever	nt details		
Time Range 30	Days ~ Sort Time	✓ [‡]	Not Subscribed Reset Save Filter As	
▼ in-10-0-4-199 sat	ann in datactad aicer com as EICAD TEG	ST Ell E FromHach	Marilian DV DV PA Austantiae Surgestia 2020.04.22.00.20.40	
File Detection	Detection			510
Connector Info	Eingerprint (SHA-256)	275a021bf651fd0f		
Commente	File Name	▼ eicar.com		
Commenta	File Path	/home/centos/eicar.com		
	File Size	68 B		
	Parent Fingerprint (SHA-256)	T 782bed6a5f896bd2		
	Parent Filename	T wget		
	Report 95 3 & Restore File	e 🕹 All Computers	Add to Allowed Applications	:tory

Figure 11. AMP Dashboard - Threat monitoring

Cisco Stealthwatch Cloud

Stealthwatch Cloud (SWC) helps overcome the visibility challenge, especially in public cloud environments. It provides an agentless deployment in the AWS cloud.

Stealthwatch Cloud pulls the VPC flow logs from the designated S3 bucket. It learns the AWS environment and baselines the resources. VPC flow logs have the flow information associated with various AWS resources, even for those that are not strictly tied to a static IP address. SWC is capable of correlating the IPs and then tying them back to their origin AWS service. In other words, SWC performs dynamic entity modeling and organizes all the AWS resources based on the functions that they're performing. For example, the entity could be categorized as a firewall, an application server or a load balancer and so on. This type of resource profiling and modeling is extremely important to look for any suspicious activity within the cloud application environments.

In addition to VPC flow logs, Stealthwatch Cloud also consumes other telemetry sources like AWS IAM, CloudTrail, EC2, ElasticCache, Inspector, GuardDuty, RDS, S3, Auto Scale, Elastic Load Balancing service for additional context and alerting.



Figure 12. Cisco Stealthwatch cloud

Once the Stealthwatch Cloud finishes identifying the entities, it baselines their behavior over a fixed period of time. As soon as the baselining is completed, any unexpected behavioral change of the entities and the way different cloud services communicate with each other is alerted on. This helps to maintain deep visibility into the cloud environment and hence, track and prevent any unauthorized transfer of data or resource access.

Some of the common Stealthwatch alerts related to the AWS services include:

- AWS API Watchlist IP Hit This alert is triggered when an AWS API is accessed by an IP on a usersupplied watchlist.
- AWS Config Rule Violation This alert uses the AWS Config Compliance observation and indicates that the resource is not compliant with configured AWS Config rules
- AWS Login Failures This alert is triggered when a user tries and fails to log in to the AWS Console several times
- AWS Inspector Findings Triggers when AWS Inspector reports a high severity event. This alert indicates that the resource is not complying with AWS best practices
- AWS Lambda Invocation Spike- Triggers when AWS Lambda function is invoked a record number of times. This alert may indicate a DoS attack.

Alerts				0-
Search Q	Status -	Tags 👻	Assignee - Sort -	,
7 open alerts sorted by newest			Page 1 of	f 1
Excessive Access Attempts (External) i-032dc6c1e859be077 #299			3 hours ag	10 13
Excessive Access Attempts (External) i-031bb97fc8aa5a9b1 #298			3 hours ag	2
Excessive Access Attempts (External) i-09e0d2badc2cf3a1c #496			4 hours ag	0 6
Excessive Access Attempts (External) ScaleWebServers i-0fa81682fd2ca2dfb, i-01b15f0e2c9d254f9 #364			14 hours ag \bigcirc 3	10 13
Excessive Access Attempts (External) i-0b071afe7f70b7134 #397			1 day, 16 hours ag O	0 8
Geographically Unusual Remote Access i-031bb97fc8aa5a9b1 #530			6 days, 10 hours ag	jo
Inbound Port Scanner Network #331			1 week, 4 days ag	0 8

Figure 13. Stealthwatch Cloud - Alerts

Cisco Umbrella

Cisco Umbrella offers flexible cloud-delivered security. It combines multiple security functions into one solution. Cisco Umbrella solutions provide DNS-layer security, secure web gateway, cloud-delivered firewall, cloud access security broker (CASB), and interactive threat intel. This document covers Umbrella DNS-layer protection for the workloads in the AWS Virtual Private Cloud (VPC).

The Umbrella DNS policies allow you to dictate block policy for a variety of pre-defined web categories. More details on web categories can be found in <u>Umbrella documentation</u>. It also gives you the flexibility to apply the policies to specific identities. For example, you could have one set of rules for your AWS cloud application and another set for a different site.





We deploy Umbrella Virtual Appliances (VA) in the Management tier of the AWS VPC. These VAs act as DNS forwarders to Umbrella. The AWS VPC offers the option to configure custom DNS settings (<u>DHCP Options Set</u>), allowing us to point the cloud resources in a given VPC to Umbrella VAs instead of AWS local DNS. Every resource, that is launched into the VPC, will use these Umbrella DNS forwarders, to provide a control knob for the DNS layer security.

All Requests 43.7K Total ▼ 21% vs. previous 24 hours 4000 i	All Bloc 7 Total ▼	ked Requests 12% vs. previous 24 hours		Security Blocks 1 Total ▼ 75% vs. previou:	s 24 hours
0 8:00 pm 4:00 am 12:00 pm	。 	8:00 pm 4:00 am	12:00 pm	0	4:00 am 12:00 pm
Most Security Blocks					
В	Y DESTINATION	BY IDENTITY	BY TYP	E	
					All Types 🗸
Identity	Bloc	ked Requests Identity			Blocked Requests
♀ mysafeapp.net		1			

Figure 15.

Umbrella - DNS Traffic Monitoring

Next-Generation Firewall Virtual

Cisco[®] Firepower Next-Generation Firewall Virtual (NGFWv) appliance combines Cisco's network firewall with advanced next-gen IPS, URL filtering, AVC and malware detection (AMP) capabilities. In this design, we use NGFWv to secure the network perimeter from all sorts of threats from public Internet. This ensures that we have

security controls like filtering, intrusion prevention and malware detection right at the gateway to the cloud application.

To provide secure remote access to the workloads and database instance, we use Cisco ASAv as a VPN headend. Cisco ASAv offers secure remote access capabilities using Anyconnect VPN mobility client. You could also use NGFWv for this purpose. For detailed information on secure remote access deployments, refer to the <u>Secure Remote Worker</u> SAFE design guide.

Cisco Defense Orchestrator (CDO) is used for management and policy orchestration. CDO provides one security policy, faster deployment, and smart configuration management. It eliminates the time-consuming complexity of managing policies across multiple FTDs and ASAs.

If you choose to use AWS Security Groups alone for segmentation (without any next-generation firewalls), the reference design is shared in Appendix A of this document. Cisco also provides CloudFormation templates and scripts for deploying an auto-scaling group of FTDv appliances. This guide does not cover the auto scaling solution, please refer to the <u>Cisco documentation</u> for more details.

Note: The terms Next-Generation Firewall (NGFW) and Firepower Threat Defense (FTD) are used interchangeably throughout this guide. Both these terms refer to Cisco Firepower Next-Generation Firewalls in the context of this document. AWS marketplace offering is available under the name 'Cisco Firepower NGFW Virtual (NGFWv)'.



Figure 16.

NGFWv - Traffic flow from Internet User to application

User to application traffic flow

When the user out on the Internet tries to browse the cloud-hosted web application, it lands on Outside Network Load Balancer after being scanned by WAF and DDoS protection system for any malicious activity. The destination IP at this point is the public IP of the Outside load balancer. Outside load balancer sits in the Outside tier (segmented using AWS Security Group) and load balances traffic onto the pool of outside interfaces of Firepower Threat Defense (FTD) appliances. The FTD appliance receives the request and then forwards the traffic to 'Web' Network Load Balancer, to be load-balanced on to the Auto-Scaled group of web servers.

Before the traffic leaves the inside interface of the FTDv (in the Inside tier), the source of the web request is translated (Network Address Translation) to FTD's inside interface IP and the destination is changed to 'Web' load balancer IP. The source IP is translated here to ensure traffic symmetry.

Web server receiving this incoming request, after being load-balanced by the Web load balancer, fetches the content from app workloads and returns the final response directly to the firewall which forwarded the initial request. At this point, firewall routes this response back to the end-user via the outside interface.

Web Application Firewall and DDoS Prevention

Public cloud has become a common place to host critical applications and make these applications available to end-users (internal or external). As a result, it is essential to ensure these applications receive the same level of protection from distributed denial of service (DDoS) and advanced web attacks that on-premises applications do.

Radware Cloud WAF service protects web applications from common web exploits. Radware's Cloud Security Services offer easy-to-deploy cloud-based security that can be integrated with any cloud environments to provide proactive, automated protection from advanced threats. The Cloud WAF service provides full coverage against OWASP top 10 attacks along with protection against 0-day web attacks. In addition to web traffic protection, DDoS component provide network flow monitoring to protect against the full breadth of DDoS attacks with real-time mitigation and no added latency in peacetime.



Figure 17. Radware Cloud - WAF and DDoS Prevention

Deployment is hassle free, application's domain name points to the Radware Cloud service. Traffic is first routed to the Radware Cloud and scanned for any malicious activity. Post-inspection, the traffic is forwarded to the origin servers in the AWS cloud. Refer to the implementation section of this guide for more deployment level details.

Cisco Duo

Cisco Duo provides secure access to applications and data, no matter where the users are, on any device, and from anywhere. Cisco Duo's secure access solution creates trust in users, devices, and the applications they access. Cisco Duo provides the following functions:

- Multi-Factor Authentication: Verify the identity of all users with Duo's strong multi-factor authentication
- Single Sign-on: Seamless, single dashboard access to all applications
- Remote Access: Secure access to cloud and on-premises applications and servers, with or without VPN
- · Device Trust: Check that user devices meet security standards before granting them access
- Adaptive Access Policies: Set policies to allow or block access attempts by a user or a device, based on contextual factors



Figure 18. Duo MFA Push

In this design, we used Duo's Multi-Factor Authentication (MFA) for our AWS cloud application. Multi-factor authentication from Duo protects the cloud applications by using a second source of validation, like a phone or token, to verify user identity before granting access. MFA not just allows you to build a zero-trust framework but is also essential for compliance purposes. Duo provides native integration for any application. Refer to the implementation section of this guide for more details.

Admins have several options when it comes to enrolling new users in Duo, such as self-enrollment, Active Directory sync, and OpenLDAP sync. Duo admin portal allows a highly convenient way to track any user activity.



Figure 19.

Duo - User Activity

Cisco SecureX

Cisco SecureX leverages the integrated security architecture to accelerate investigations by automating and aggregating threat intelligence and data across your security infrastructure in one unified view. Some of the key features are:

- Aggregated threat intelligence: Integrates threat intelligence from Cisco TALOS and third-party sources to automatically research indicators of compromise (IOCs) and confirms threats quickly
- Automated enrichment: Automatically adds context from integrated Cisco Security products, so that you instantly know which of your systems was targeted and how
- Incident tracking: Provides the capability you need to collect and store key investigation information, and to manage and document your progress and findings
- Interactive visualizations Shows your results on intuitive, configurable graphs for better situational awareness and quick conclusions
- Seamless drill down Makes deeper investigations easy using integrated Cisco Security products. A single click takes you inside Cisco AMP for Endpoints
- Direct remediation Lets you take corrective action directly from its interface. Block suspicious files, domains, and more without having to log in to another product



Figure 20.

Cisco SecureX threat response

In this architecture, we are receiving information from Stealthwatch Cloud, Umbrella, AMP and Tetration to provide threat intelligence, contextual approach, and threat hunting capabilities. Integrations for and Radware Cloud WAF and DDoS service are also available. Refer to the <u>Cisco SecureX</u> documentation for more details on available Cisco and third-party integrations.



Figure 21. Cisco SecureX Dashboard



Figure 22.

Cisco SecureX threat response - Threat Hunting

Design Implementation

Now that we have established the design specifics of our tiered application in the AWS cloud, we will begin implementing and setting up the secure AWS application.

We will start by setting up the AWS VPC (Virtual Private Cloud) as per the tiered architecture specifications. We will then integrate the Stealthwatch Cloud and onboard the VPC to CDO for Security Group management. After that we will set up the Umbrella VAs in the management tier and update the DNS server settings for the VPC.

Once the AWS VPC and related integrations are finished, we will configure an RDS database instance and bring up the Auto Scaling Groups for the Application and Web workloads (with Tetration, AMP4E agents and Duo MFA plugin). We will then set up the Network Load Balancers for Web and Application Auto Scaling Groups. At this point we will have a fully functional application running in the AWS cloud.

In the last step, we will configure the firewalls, enable WAF and DDoS protection and then conclude our set up with Cisco SecureX integration.

Note: Cisco Tetration, AMP, Cisco SecureX threat response, Stealthwatch Cloud, Umbrella, Duo and CDO offer EU based locations for customers having to follow EU rules.



Deployment Overview:

- Set up the AWS VPC components
- Integrate Stealthwatch Cloud for VPC monitoring
- Onboard the AWS VPC to CDO for AWS Security Group management
- Set up Umbrella DNS Security
- Set up the AWS RDS database instance
- Set up the Auto Scaled Application and Web Workloads (Tetration, AMP4E agent and Duo MFA plugin installation) with App and Web NLBs
- Set up Cisco Firepower Next-Generation Firewalls with CDO onboarding
- Enable Radware cloud web application firewall and DDoS prevention service
- Set up Cisco SecureX

Note: Before you begin, make sure you have the appropriate privileges to create all the VPC components. Follow the <u>AWS Documentation</u> for more information on IAM service.

Set up the AWS VPC components

We will create a new AWS VPC and configure all the associated components that we need for our deployment in this section.

Implementation procedure:

- Step 1. Create the VPC
- Step 2. Set up the Subnets
- Step 3. Set up the Internet gateway
- Step 4. Set up the NAT gateways
- Step 5. Set up the Routing Tables
- Step 6. Create the Security Groups
- **Step 1.** Create the VPC Log on to the AWS console and select the VPC service, click on Create VPC and fill in the required details. We chose the IPV4 CIDR block as 10.0.0.0/16.

aws Services ~	🗸 Resource Groups 🗸 🌐 EC2 😩 VPC 📫 S3 🌎 RDS 🤚 WAF & Shield 💡 IAM 🔸
New VPC Experience Tell us what you think	Create VPC Actions *
VPC Dashboard New	Q. Filter by tags and attributes or search by keyword
Filter by VPC:	Name VPC ID A State VP4 CIDR DHCP options set
Q Select a VPC	SecureVPC vnc-09906c2d738f8ee55 available 10.0.0.0/16 dont-0h3e0b9fc980de9dc1mvDHCPontions
VIRTUAL PRIVATE	
Your VPCs	
Subnets	

Follow the <u>AWS documentation</u> for more details on AWS VPCs.

Step 2. Set up the Subnets – Based on the tiered architecture, we defined two subnets for each tier – one for each AWS Availability Zone.

IPV4 CIDR Block	AWS Region	Tier
10.0.0/25	US-East-1a	OutSubnet1a
10.0.0.128/25	US-East-1b	OutSubnet1b
10.0.1.0/25	US-East-1a	InSubnet1a
10.0.1.128/25	US-East-1b	InSubnet1b
10.0.2.0/24	US-East-1a	WebSubnet1a
10.0.3.0/24	US-East-1b	WebSubnet1b
10.0.4.0/24	US-East-1a	AppSubnet1a
10.0.5.0/24	US-East-1b	AppSubnet1b
10.0.6.0/24	US-East-1a	DbSubnet1a
10.0.7.0/24	US-East-1b	DbSubnet1b
10.0.8.0/24	US-East-1a	MgmtSubnet1a
10.0.9.0/24	US-East-1b	MgmtSubnet1b

Go to VPC Dashboard > Subnets and create all these subnets and name them appropriately.

aws Services	 Resource Groups 	т 🌔 ЕС2 😫	VPC 📫 S3 🏮 RDS	🦺 WAF & Shi	ield 💡 IAI	и 🛧
New VPC Experience	Create subnet Ac	tions 👻				
VPC Dashboard	Q VPC : vpc-09906	c2d738f8ee55 💿 Add filte	r			
Filter by VPC:	Name	State VPC	Ŧ	IPv4 CIDR	Availability	Route table
Select a VPC	OutSubnet1a	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.0/25	us-east-1a	rtb-04bbc6ead9b89cc7e OutRT
VIRTUAL PRIVATE CLOUD	OutSubnet1b	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.0.128/25	us-east-1b	rtb-04bbc6ead9b89cc7e OutRT
Your VPCs	InSubnet1a	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.1.0/25	us-east-1a	rtb-0c39282a55777aa6a InRT
Subnets	InSubnet1b	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.1.128/25	us-east-1b	rtb-0c39282a55777aa6a InRT
Route Tables	WebSubnet1a	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.2.0/24	us-east-1a	rtb-06e9ee921f86210f1 WebRT
Internet Gateways	WebSubnet1b	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.3.0/24	us-east-1b	rtb-06e9ee921f86210f1 WebRT
Egress Only Internet	AppSubnet1a	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.4.0/24	us-east-1a	rtb-009dd8d9d77ce6484 AppRT1a
Gateways	AppSubnet1b	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.5.0/24	us-east-1b	rtb-0ceabb06d101a29a7 AppRT1b
DHCP Options Sets	DbSubnet1a	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.6.0/24	us-east-1a	rtb-01afe24ceb70f1bcf DbRT1a
Elastic IPs	DbSUbnet1b	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.7.0/24	us-east-1b	rtb-0f8e156a897fd5aea DbRT1b
Managed Prefix Lists	MgmtSubnet1a	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.8.0/24	us-east-1a	rtb-090e220f3128124c2 MgmtRT
Endpoints	MgmtSubnet1b	available vpc-0990	6c2d738f8ee55 SecureVPC	10.0.9.0/24	us-east-1b	rtb-090e220f3128124c2 MgmtRT
Endpoint Services						
NAT Gateways						
Peering Connections						

Step 3. Set up the Internet gateway – Navigate to VPC Dashboard > Internet Gateways to create an Internet Gateway for providing Internet access to Public resources in the VPC.

Note: We will use this Internet Gateway as the next hop for default routes in Firewall Route table (For Inside and Outside subnets) and the Management Route Table (For Management Subnets) respectively.

aws Services ~	Resource Groups 🗸 🥠 EC2 😩 VPC 📫 S3 🌒 RDS 🌗 WAF & Shield 🧍 IAM 🖈
New VPC Experience Tell us what you think	VPC > Internet gateways
VIRTUAL PRIVATE CLOUD Your VPCs	Internet gateways (1/1) Info Q. Filter internet gateways
Subnets Route Tables	☑ Name ▼ Internet gateway ID ▼ State ▼ VPC ID
Egress Only Internet Gateways New	✓ InternetGW igw-0033a8e740993f9e1

Follow the AWS documentation for more details on AWS Internet Gateway components.

Step 4. Set up the NAT gateways - Navigate to VPC Dashboard > NAT Gateway to create NAT Gateways for providing Internet access to all resources in private subnets.

Note: We will use these NAT Gateways as the next hop for default routes in Web, App and Db Route tables.

aws Services ▼	
New VPC Experience	Create NAT Gateway Actions *
Carrier Gateways	Q Filter by tags and attributes or search by keyword
DHCP Options Sets	Name v Status v VPC Subnet
Elastic IPs	NATGW1b available vpc-09906c2d738f8ee55 SecureVPC subnet-0766d766ccfa85994 OutSubnet1b
Managed Prefix Lists	NATGW1a available vpc-09906c2d738f8ee55 SecureVPC subnet-085f3f55148fca9dd OutSubnet1a
Endpoints	
NAT Gateways	
Peering Connections	
SECURITY	

Step 5. Set up the Routing Tables - Go to VPC Dashboard > Route Tables and create the routing tables with subnet associations as per the table below.

Route Table Name	Subnets	Default Route
FirewallRT	OutSubnet1a, OutSubnet1b InSubnet1a, InSubnet1b	Internet Gateway
WebRT1a	WebSubnet1a	NAT Gateway1a
WebRT1b	WebSubnet1b	NAT Gateway1b
AppRT1a	AppSubnet1a	NAT Gateway1a
AppRT1b	AppSubnet1b	NAT Gateway1b
DbRT1a	DbSubnet1a	NAT Gateway1a
DbRT1a	DbSubnet1b	NAT Gateway1b
MgmtRT	MgmtSubnet1a, MgmtSubnt1b	Internet Gateway

aws Services ▼						
New VPC Experience	Create route table	Actions *				
VPC Dashboard	Q VPC : vpc-09906	Add filter				
Filter by VPC:	Name •	Route Table ID	 Explicit subnet association 	Main	VPC ID	Ŧ
Q Select a VPC	AppRT1a	rtb-009dd8d9d77ce6484	subnet-0ba19ec3047bd6892	No	vpc-09906c2d738f8ee55 SecureVPC	
VIRTUAL PRIVATE CLOUD	AppRT1b	rtb-0ceabb06d101a29a7	subnet-089e1c7c4904fd15a	No	vpc-09906c2d738f8ee55 SecureVPC	
Your VPCs	DbRT1a	rtb-01afe24ceb70f1bcf	subnet-03a30430a54ea57f4	No	vpc-09906c2d738f8ee55 SecureVPC	
Subnets	DbRT1b	rtb-0f8e156a897fd5aea	subnet-06c70886741037ce7	No	vpc-09906c2d738f8ee55 SecureVPC	
Route Tables	FirewallRT	rtb-04bbc6ead9b89cc7e	4 subnets	Yes	vpc-09906c2d738f8ee55 SecureVPC	
Internet Gateways	MgmtRT	rtb-090e220f3128124c2	2 subnets	No	vpc-09906c2d738f8ee55 SecureVPC	
Egress Only Internet	WebRT1a	rtb-06e9ee921f86210f1	subnet-0dfe62e16b1eef97d	No	vpc-09906c2d738f8ee55 SecureVPC	
Gateways	WebRT1b	rtb-0081770fdca7170c4	subnet-06953c1c1acdf22e0	No	vpc-09906c2d738f8ee55 SecureVPC	
DUCP Ontions Sets						
Elastic IPs						

For the Firewall and Management Route Tables, create the default route pointing to the Internet Gateway created previously. For the Web, App and Db Route Tables, create the default route pointing to the NAT Gateways created for each Availability Zone.

As per the AWS network design, we cannot load balance the outbound flows. If you decide to deploy a single firewall per availability zone then you can always use firewall inside interface ENI as next hop for default routes, to send outbound flows to firewalls. However, we recommend adding multiple firewalls in each availability zone to avoid any single point of failure.

aws Services ▼						
New VPC Experience	Create route table	Actions V				
VPC Dashboard	Q VPC : vpc-0990	6c2d738f8ee55 💿 Add filter				
Filter by VPC:	Name	Reute Table ID	Explicit subpat association	Main	VBCID	_
Q Select a VPC	Name	Route Table ID	Explicit subliet association	Walli	VPC ID	
	AppRT1a	rtb-009dd8d9d77ce6484	subnet-0ba19ec3047bd6892	No	vpc-09906c2d738f8ee55	SecureVPC
CLOUD	AppRT1b	rtb-0ceabb06d101a29a7	subnet-089e1c7c4904fd15a	No	vpc-09906c2d738f8ee55	SecureVPC
Your VPCs	DbRT1a	rtb-01afe24ceb70f1bcf	subnet-03a30430a54ea57f4	No	vpc-09906c2d738f8ee55	SecureVPC
Subnets	DbRT1b	rtb-0f8e156a897fd5aea	subnet-06c70886741037ce7	No	vpc-09906c2d738f8ee55	SecureVPC
Route Tables	FirewallRT	rtb-04bbc6ead9b89cc7e	4 subnets	Yes	vpc-09906c2d738f8ee55	SecureVPC
Internet Gateways	MgmtRT	rtb-090e220f3128124c2	2 subnets	No	vpc-09906c2d738f8ee55	SecureVPC
Egress Only Internet	WebRT1a	rtb-06e9ee921f86210f1	subnet-0dfe62e16b1eef97d	No	vpc-09906c2d738f8ee55	SecureVPC
Gateways	WebRT1b	rtb-0081770fdca7170c4	subnet-06953c1c1acdf22e0	No	vpc-09906c2d738f8ee55	SecureVPC
Carrier Gateways						
Elastic IPs						
Managad Prefix Liete						
Endpointe	Route Table: rtb-04b	bc6ead9b89cc7e				
Endpoint Senices						
NAT Gateways	Summary	Routes Subnet Asso	ciations Edge Associations	Route Propagation	Tags	
Peering Connections	Edit routes					
SECURITY						
Network ACLs		View All rout	es 🔻			
Security Groups						
 VIRTUAL PRIVATE NETWORK (VPN) 	Destination		Targ	et	٤	Status
Customer Gateways	10.0.0/16		local		а	ctive
Virtual Private Gateways	0.0.0.0/0		igw-	0033a8e740993f9e1	a	ctive
Site-to-Site VPN Connections						

Step 6. Create the Security Groups - Go to **'VPC Dashboard > Security Groups'**, set up a Security Group corresponding to each tier in the design. Set up the inbound access rules as per the application requirements. We used the following inbound rules.

webSG	
Port	Reason
TCP port 80	Allow HTTP access from the inside subnets to web servers
TCP port 22	Allow SSH access from mgmtSG

appSG	
Port	Reason
TCP port 80	Allow HTTP access from workloads within application tier subnets (allows load balancer health checks). Allow HTTP access from web tier subnets.
TCP port 22	Allow SSH access from mgmtSG

dbSG	
Port	Reason
TCP port 3306	Allow MYSQL/Aurora traffic from appSG

mgmtSG	
Port	Reason
TCP port 22	Allow SSH access from internet
UDP 53	Allow DNS traffic from appSG, webSG, dbSG and mgmtSG

firewallSG	
Port	Reason
All traffic	Allow all access from internet, we will control the traffic using firewall access lists.

Note: AWS Elastic Network Load Balancer (NLB) preserves the source IP of incoming connections from web tier workloads, hence we need to allow the source subnets specifically. We cannot use Security Groups to allow traffic from NLB, we must use subnets. Follow the <u>AWS Documentation</u> for more information on Security Group requirements for NLB.

aws Services - F	Resource Groups 👻 🏾	🖡 EC2 🛛 😫 VPC	🏟 S3 🌒 RDS	👃 WAF & Shield	💡 IAM 🛛 🛠
New VPC Experience Tell us what you think	VPC > Security Groups				
DHCP Options Sets New Elastic IPs New Managed Prefix Lists New Endpoints	Security Groups (1 /7) Info ps			
Endpoint Services	■ Name ▼	Security group ID		V	Description
NAT Gateways	VebSG	sg-082bf0e9529a23	efa vpc-09906c2	2d738f8ee55	SG for workloads in web tier
Peering Connections	MgmtSG	sg-0b55db462c834e	f86 vpc-09906c2	2d738f8ee55	SG for management tier
▼ SECURITY					
Network ACLs					
Security Groups New	sa-082hf0e9529a23efa.	WebSG			
VIRTUAL PRIVATE NETWORK (VPN)	Details Inbound	rules Outbound ru	iles Tags		
Customer Gateways					
Virtual Private Gateways					
Site-to-Site VPN Connections	Inbound rules				
Client VPN Endpoints	Туре	Protocol	Port range	Source	Description - optional
▼ TRANSIT GATEWAYS Transit Gateways	НТТР	тср	80	0.0.0/0	allow HTTP from internet
Transit Gateway Attachments	SSH	тср	22	0.0.0/0	allow SSH from Management tier
Transit Gateway Route	HTTPS	ТСР	443	0.0.0/0	allow HTTPS from internet
Transit Gateway Multicast					

Follow the AWS documentation for more details on AWS Security Groups.

Integrating Stealthwatch Cloud

Implementation procedure:

- Step 1. Set up the VPC flow logs and integrate Stealthwatch Cloud.
- Step 1. Set up the VPC flow logs and integrate Stealthwatch Cloud Follow the steps illustrated in Cisco Stealthwatch <u>AWS Quick Start Guide</u> to create the VPC flow logs and other required AWS resources for Stealthwatch cloud monitoring.

After the Stealthwatch cloud integration is done, click on the cloud icon on the top right hand side of the SWC portal and you should see an AWS sensor with a green check mark against it, indicating a successful integration.

cisco Stealthwatch Cle	OUC Dashboard 🗸 A	lerts 12 Observations Models ✓		Q 0 🙆 🌣 🛔
Settings Alerts	Integrations			
Site Management Subnets User Webhooks/Services	AWS Azure GCP Kubernetes	Amazon Web Services About Credentials VPC Flow Logs Permissions AWS S3	Config ^{8eta} Auth Logs ^{8eta} Inspector	
	∞ Meraki ∞ SecureX ∞ Umbrella	S3 Flow Log Locations S3 Path securestealthwatch bucket-name/optional_suffix	Credentials saloews	× *

Onboard AWS VPC to Cisco Defense Orchestrator Implementation procedure:

Step 1. Onboard the AWS VPC to Cisco Defense Orchestrator

Step 1. Onboard the AWS VPC to Cisco Defense Orchestrator - Follow the steps illustrated in CDO Documentation to onboard the AWS VPC. Once the onboarding is complete, CDO can be used to manage the AWS Security Groups.

cisco Defense Orchestrator	Devices & Services			(↓) O → safe-architecture amansin3@cisco.com
🗮 Hide Menu	T Q vpc Displaying 1 of 1 results C 🕲 🛨		1 of 1 results C 🙂 🕂 :	AWS VPC
Devices & Services	✓ Name \$	Configuration Status A	Connectivity \$	Device Details ~
Configuration	SecureVPC AWS VPC	O Synced	Online	VPC ID vpc-09906c2d738l8ee55 Region us-east-1
Objects				O Synced
⊷å VPN >				Check for Changes

Set up Umbrella DNS Security

Implementation procedure:

- Step 1. Set up the Umbrella Virtual Appliance (VA) image
- Step 2. Create the Umbrella VA instances
- Step 3. Configure the local DNS on Umbrella VA instances
- Step 4. Set up the policies to exempt internal domains
- Step 5. Update the DHCP Options Set for VPC
- **Step 1.** Set up the Umbrella Virtual Appliance image Follow the Umbrella documentation to deploy Virtual appliances (VA) in the AWS cloud. As per the documentation, create an AWS AMI and then use it to launch VA instances.

aws Services -	Resource Groups 🗸 🌗 EC2 👙 VPC 📫 S3 🌖 RDS 🦺 WAF & Shield 💡 IAM 🔦
Spot Requests	Launch EC2 Image Builder Actions *
Savings Plans Reserved Instances	Owned by me v Q Filter by tags and attributes or search by keyword
Dedicated Hosts New	Name - AMI Name - Status - Architecture - Description
Scheduled Instances	UmbrellaVA import-ami-05b8735289511fa72 available x86_64 AWS-VMImport service: Linux - Ubuntu 16.04.3 LTS - 4.4.0-157-generic
Capacity Reservations	
▼ Images	
AMIs	
Elastic Block Store	
Volumes	

Step 2. Create the Umbrella VA instances – Create two VA instances using the AMI set up in Step1 and place these appliances in the management tier. We assign the static IP addresses 10.0.8.100 and 10.0.9.100 to these Umbrella Virtual Appliances. These VAs will act as DNS forwarders for the resources in our AWS application environment.

aws Services ~	Resource Groups 🗸 🌗 EC2 😩 VPC 📫 S3 🌎 RDS 🤳 WAF & Shield 💡 IAM 🗲
Tags	Launch Instance Connect Actions
Limits	Q Name : Umbrella 💿 Add filter
▼ Instances	Name Availability Zone Instance State Status Checks Private IP Add
Instances	UmbrellaVA1a us-east-1a orunning 2/2 checks passed 10.0.8.100
Launch Templates	UmbrellaVA1b us-east-1b Improvement of the seased UmbrellaVA1b us-east-1b Improvement of the seased UmbrellaVA1b UmbrellaVA1b UmbrellaVA1b UmbrellaVA1b UmbrellaVA1b Improvement of the sease of the sea
Spot Requests	

Once the appliances are fully up in AWS, login to the Umbrella portal and verify the green status under **Deployments > Configuration > Sites and Active Directory**.

Cisco Umbrella Mobile Devices		CISCO Deployments Sites a	and Active Directory •				Settings	Add DC	Jownload
Chromebook Users	W	Want to set up Active Directory Integration or deploy Virtual Appliances? Click Download above to get started.							
Network Tunnels									
Web Users and Groups									
Configuration		FILTERS			Q mysafeapp.net				
Domain Management									
Sites and Active Directory		Name 🔻	Internal IP	Site	Туре	Status	Versio	n	
Internal Networks		10.0.9.100	10.0.9.100	mysafeapp.net	Virtual Appliance	Imported: 4 months ago	2.7.1	0	
Root Certificate		10.0.8.100	10.0.8.100	mysafeapp.net	Virtual Appliance	Imported: 4 months ago	2.7.1	0	
SAML Configuration					Page:	1 V Results Per Page: 10 V	/ 1-2 of	2 <	>
Service Account Exceptions									

Optionally, you can create and assign a site name for your AWS VAs. This site name can be used as an identity to configure specific policies for AWS Cloud. Click on Settings on the same page to add site name and then update the VA entries above.

Cisco Umbrella	Sites and Active Directory	Settings Add I) (+)C Download			
Chromebook Users	Want to set up Active Directory Integration or deploy Virtual Appliances? Click Download above to get started.					
Network Tunnels						
Web Users and Groups						
Configuration	Section 2015 And Active Directory					
Domain Management						
Sites and Active Directory	Sites Auto-Updates					
Internal Networks	Name 🔻	Add New	Site			
Root Certificate	Default Site					
SAML Configuration						
Service Account Exceptions	Site Name					
Policies >						
Reporting >	CANCEL SAVE Page: 1 V Results Per Page: 1 V	1-3 of 3 <	>			
Admin >						

Step 3. Configure the local DNS on Umbrella Virtual Appliances – Follow the Umbrella documentation to configure local DNS on each VA. Based on the CIDR block chosen for lab VPC, the second IP address i.e. 10.0.0.2/24 is the local DNS. Set this IP as local DNS on both Umbrella VAs.

Note: We had set up Secure Remote Access to management tier using ASAv, we use the secure VPN connection to SSH into the VAs via a jump server hosted in the management tier. For more information on Secure Remote Access, refer to the Secure Remote Worker SAFE Design guide.



Step 4. Set up policies to exempt internal domains - Log on to the Umbrella portal, go to Deployments > Configuration > Domain Management and add the internal domains that
should be routed to the local AWS resolver. Based on your set up, the list of internal domains will vary.

Cisco Umbrella	Configuration Domain Management				
Networks			Add		
Network Devices	Want to route certain domains to your lo	cal resolver? You've come to the right place. Click "Add" above to get started.			
Roaming Computers					
Mobile Devices	Internal Demoles (10)	Demolos 8 (Pp. 70)			
Chromebook Users	Internal Domains (10) External	Domains & iPs (0)			
Network Tunnels	Domain Name 🛦	Description	Applies To		
Web Users and Groups	RFC-1918	Non-publicly routable address spaces used only for reverse DNS on internal networks	All Sites, All Devices		
Configuration	local	All *.local domains	All Sites, All Devices		
Domain Management	amazonaws.com	AWS Internal	All Sites, All Devices		
Sites and Active Directory	azure.com	Azure internal	All Sites, All Devices		
Internal Networks	compute internal	AWS Internal	All Sites All Devices		
Root Certificate	compute.internal	Arro internet	All Olico, All Dovices		
SAML Configuration	ec2.internal	AWS Internal	All Sites, All Devices		

Step 5. Update the DHCP Options Set for the VPC – Go to VPC Dashboard > DHCP Options Sets and create a new DHCP options set. Set the domain name servers to two IPs that we assigned to Umbrella VAs – 10.0.8.100 and 10.0.9.100.

aws Services	🗸 Resource Groups 🗸 🌗 EC2 😩 VPC 🕴 S3 🌖 RDS 🦺 WAF & Shield 💡 IAM 🔦	
New VPC Experience	Create DHCP options set Actions *	
Subnets	Q Name : myDHCPoptions	
Internet Gateways	Name DHCP options set ID Options	
Egress Only Internet Gateways	myDHCPop dopt-0b3e0b9fc980de9dc domain-name = mysafeapp.net; domain-name-servers = 10.0.8.100, 10.0.9.100;	
DHCP Options Sets		
Elastic IPs		
Managed Prefix Lists		
Endpoints		

Go to **VPC Dashboard > Your VPCs**, select the newly created VPC above and update the DHCP options set from the drop-down list. This will ensure that any instance deployed in this VPC is assigned the Umbrella VAs as DNS forwarders.

aws	Services - R	esource Groups 🗸	🌔 EC2	🔑 VPC	🕴 S3	🔋 RDS	🦺 WAF & Shield	👔 iam	*
VPCs > Edit DHCP options set									
Edit DHC	P options s	set							
	VPC ID	vpc-09906c2d738f8ee5	5						
	DHCP options set*	dopt-0b3e0b9fc980de	9dc		- C	0			
* Required									

Follow the <u>AWS documentation</u> for more details on DHCP Options Sets.

Setting up the RDS database

Implementation procedure:

- Step 1. Define the database Subnet Groups
- Step 2. Set up the RDS database instance

Step 1. Define the database Subnet Groups - Go to RDS > Subnet Groups on the AWS console, create a DB Subnet Group and add to it the Database tier subnets defined in previous steps ('dbSubnet1a' and 'dbSubnet1b').

aws Services - R	lesource Groups 🗸 🗯 S3 🌘 EC2 🚦 VPC 🕏		ậ safe-architecture @ ltrsec3052 ▾ Ohio ▾ Support ▾
Amazon RDS ×	RDS > Subnet groups > dbsubnet dbsubnet		
Databases Query Editor	Subnet group details		
Performance insights Snapshots Automated backups Reserved instances Proxies Subnet groups Parameter groups	VPC ID SecureVPC (vpc-092e2ff7c1372c4dc) ARN armaws:rdsus-east-2:305633958872:subgrp:rdbsubnet Description Subnet Group for Database Subnets		
Option groups Events	Subnets (2)		
Event subscriptions	Availability zone	Subnet ID	CIDR block
Recommendations 1	us-east-2a	subnet-03a38f56a1730262e	10.0.6.0/24
certificate updatë	us-east-2b	subnet-054684d9a7f885bff	10.0.7.0/24

Step 2. Set up the RDS database instance – Set up the database instance as per your application requirements, follow the <u>AWS documentation</u> for further help. Use the Subnet Group defined in Step 1 above. The database instance is placed in Security Group 'dbSG'.

aws Services - Re	source Groups 🗸 🕴 S3 🌗 EC2 😫 VPC 🖈	·		Ĵ safe-architecture @ Itrsec3052 ▼ Ohio ▼ Support ▼		
Amazon RDS \times	RDS > Databases > securedb					
Dashboard	securedb			Modify Actions 🔻		
Databases Query Editor	Summary					
Performance Insights Snapshots Automated backups Reserved instances Proxies	DB identifier securedb Role Instance	CPU	Info Ø Avallable Engine MySQL Community	Class db.12.micro Region & AZ us-east-Za		
Subnet groups Parameter groups Option groups	Connectivity & security Monitoring Logs & e	Connectivity & security Monitoring Logs & events Configuration Maintenance & backups Tags				
Events Event subscriptions	Connectivity & security					
Recommendations 🕦 Certificate update	Endpoint & port Endpoint secureds.c?vsbrea0jtw.us-east-2.rds.amazonaws.com Port 3306	Networking Availability zone us-east-Za VPC SecureVPC (vpc-092e2f7c1372c4d Subnet group dbsubnet Subnet: 0546844d9a78885bff subnet: 0546844d9a78885bff	c) Security VPC security dis56 (rp-) (active) Public acce No Cerrificate. Aug 22nd ,	y groups SSC1 0d96SF6364) sisbility withority a withority date 1024		

Make sure you note the username, password, endpoint hostname and port, we need these details to set up our cloud application later in this section.

Setting up the App and Web Load Balancers

Before we begin our implementation, please ensure you're familiar with these components. For information on AWS Elastic Load Balancing and health checks, check out the <u>AWS documentation</u> here. Follow the AWS documentation for detailed configuration steps for <u>Network Load Balancer</u> (NLB).

Per our tiered design, we will set up a 'Web' Network Load Balancer (NLB) for the Web Server workloads and an 'App' Network Load Balancer (NLB) for the Application workloads. We will create Target Groups for each NLB; the workloads register themselves with these Target Groups.

We will not register any instances to the Target Groups at this point but in the next section when we create the Auto Scaling Groups, we will integrate the Auto Scaling Groups with each of these blank Target Groups that we

create in this section. When the Auto Scaling process spins new instances, they will automatically register with these Target Groups.

The Load Balancers will be configured to run health checks for each instance that is launched into the Target Groups. As soon as an instance is marked healthy, the Load Balancer starts load balancing traffic to it. When the instance becomes unhealthy, it is removed from the pool.

Implementation procedure:

- Step 1. Set up the Web Network Load Balancer
- Step 2. Set up the App Network Load Balancer
- Step 1. Set up the Web Network Load Balancer The Web NLB is used to load balance web traffic coming from the Internet to the Auto Scaled pool of Web workloads. This load balancer is placed in the 'webSG' Security Group in the subnets 'WebSubnet1a' and 'WebSubnet1b'. A new Target Group 'WebServerPool' is also created as part of load balancer configuration, this will be used later while setting up Auto Scaling Group for Web Servers.

aws Services - Resource Groups - 🌗 EC2 🤑 VPC 획 S3 🍵 RDS 🧍 N	AF & Shield 💡 IAM 🛧 🗘 amansin3 👻 N. Virginia 🌱 Support 🌱
1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing 4. Register Targets 5. Review	
Step 1: Configure Load Balancer	
Basic Configuration	
To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The definition	ult configuration is an Internet-facing load balancer in the selected network with a listener that receives TCP traffic on port 80.
Name (i) WebNLB	
Scheme () Internet-facing	
Listeners	
A listener is a process that checks for connection requests, using the protocol and port that you configured.	
Load Balancer Protocol	Load Balancer Port
ТСР	80 😵
Add listener	

Assign static IP addresses in each availability zone. Make a note of these IP addresses, we will require these IPs while setting up the static NAT translations on FTD appliances in later section of this document.

Availability Zones			
Specify the Availability Zones to have specific addresses for your	enable for your load balancer.	load balancer. The load balan	cer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to
VPC ()	vpc-09906c2d	738f8ee55 (10.0.0.0/16) Secu	reVPC •
Availability Zones	🗸 us-east-1a	subnet-0dfe62e16b1eef97d	d (WebSubnet1a)
		IPv4 address (i)	Assigned from CIDR 10.0.2.0/24
		Private IPv4 address (i)	Enter IP from CIDR 10.0.2.0/24 -
			10.0.2.101
	🗹 us-east-1b	subnet-06953c1c1acdf22e	0 (WebSubnet1b) •
		IPv4 address (i)	Assigned from CIDR 10.0.3.0/24
		Private IPv4 address (i)	Enter IP from CIDR 10.0.3.0/24
			10.0.3.101

aws Service	🗸 Resource Groups 🗸 🌗 EC2 😩 VPC 획 S3 🌒 RDS 🤳 WAF & Shield 💡 IAM 🛧	↓ •
New EC2 Experience	Create Load Balancer Actions *	
Limits	Q Name : WebNLB Add filter	
INSTANCES	Name DNS name State VPC ID Availability Zones Type Type	ю
Instances	WebNLB WebNLB-cadea0d4928083e active vpc-09906c2d738f8ee55 us-east-1a, us-east-1b net	work
Instance Types		
Spot Requests		
Savings Plans		
Reserved Instances	Load balancer: WebNLB	
Dedicated Hosts	Description Listenare Monitoring Integrated services Tage	
Scheduled Instances	Peseription satericia monitoring integrated en rices ruga	
Capacity Reservations	A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can a	add, remo
 IMAGES 	Add listener Edit Delete	
AMIs		
ELASTIC BLOCK STORE	Listener ID Security policy SSL Certificate ALPN policies Default action	
Volumes	TCP:80 N/A N/A Forward to M/A Security Poor	
Snapshots	arn3a172448b3450766 + Forward to WebServerNLBP001	
Lifecycle Manager		

Step 2. Set up the App Network Load Balancer - This Load Balancer is placed in the 'appSG' Security Group in the subnets – 'appSubnet1a' and 'appSubnet1b'. A new Target Group 'AppServerPool' was also created as part of Load Balancer configuration, this will be used later while setting up the Auto Scaling Group for Application workloads.

aws Services	🗸 Resource Groups 🖌 🌗 EC2 🔑 VPC 🕴 S3 🌖 RDS 🤳 WAF & Shield 💡 IAM 🔸
New EC2 Experience	Create Load Balancer Actions ~
Limits	Q Name : AppNLB Add filter
INSTANCES	Name A DNS name State VPC ID Availability Zones Type
Instances	AppNLB AppNLB-5cad66ee8ff active vpc-09906c2d736f8ee55 us-east-1a, us-east-1b network
Launch Templates	
Spot Requests	
Savings Plans	Load balancer: AppNLB
Dedicated Hosts	
Scheduled Instances	Description Listeners Monitoring Integrated services lags
Capacity Reservations	A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add
IMAGES AMIs	Add listener Edit Delete
ELASTIC BLOCK STORE	Listener ID Security policy SSL Certificate ALPN policies Default action
Volumes Snapshots	TCP:80 N/A N/A Forward to AppServerPool
Lifecycle Manager	

Setting up Web and App Auto Scaling groups

In this section, we will set up a pool of workloads for the web and application tier. We will use the AWS Auto Scaling Groups to achieve this. As part of workload initialization, we install Tetration and AMP4E agents on the web and app workloads along with other application-specific packages, including the Duo plugin.

Implementation procedure:

- Step 1. Host the configuration files in an S3 bucket
- Step 2. Set up Launch Configurations
- Step 3. Set up the Auto Scaling Groups
- Step 4. Configure the Auto Scaling policies

Step 1. Host the configuration files in an S3 bucket - We set up an AWS S3 bucket in US East region. We upload all the files and application code that we need for our application and web workloads into this bucket. The other option is to use <u>golden images</u> with all the required applications and packages pre-installed for app and web workloads. If you choose to host config files in an S3 bucket, ensure that you set appropriate access privileges for these files.

The S3 files include:

- Config/Code files for our App and Web workloads
 - App workloads Modified Publicly available '<u>WordPress</u>' blog code with database connection information (we recorded the database credentials while setting up RDS previously). Duo Plugin was also hosted in this S3 bucket.
 - Web workloads The Web Server config file. This file has the FQDN address of App Network Load Balancer that we created in previous steps.
- AMP4E agent installer (AMP rpm and GPG). These were obtained from AMP cloud portal
- Tetration agent installer (Enforcement agent). These are downloaded from Tetration SaaS portal

Note: For Duo MFA for the cloud application, we used Duo WordPress plugin. However, if you choose to include the Duo integration in your native application, follow the <u>DUO Web SDK</u> documentation.

- **Step 2.** Set up the Launch Configurations Go to EC2 Dashboard> Auto Scaling > Launch Configuration and create launch configurations for web and application servers. For more information on creating Launch Configurations follow the <u>AWS documentation</u>.
 - For the base image/operating system, we chose CentOS
 - Under the **Advanced details** options, make sure not to assign any public IPs to the instances in the launch configuration
 - Under the same Advanced details options, we use the User Data option to initialize the EC2 instances when they are launched into the auto scaling pool. For more details on User Data option, check out the AWS documentation. As part of this initialization process, we perform the following tasks:
 - Install packages (php, wget, unzip, lsof, httpd, ipset, nginx) on the workloads. Some of these are prerequisites for AMP4E and Tetration agents. Refer to the corresponding product documentation to understand these requirements
 - Download Code/Configuration files to the respective workloads from S3 bucket
 - Download the WordPress Duo plugin from S3 bucket to the application workloads
 - · Download and install the Tetration enforcement agent to all the workloads
 - Download and install the AMP4E agent to all the workloads
 - Use the Security Groups 'webSG' and 'appSG' for Web and Application Launch Configurations respectively

aws Services	• Resource Groups •	🌗 EC2 🛛 😫 VPC 🔹 🕸 S	3 🔋 RDS 🤳 WAF	& Shield 🕴 IAM	*	
New EC2 Experience Learn more EC2 Dashboard	Create launch configuratio	n Create Auto Scaling group	Copy to launch template	Actions V		
Events	Filter: Q. Filter launch confi	aurations ×				
Tags		,				
Limits	Name	Security Groups	 IP Address Type 	~		
INSTANCES	AppServerLC	sg-004599d2fc5354bda	Private			
Instances	WebServerLC	sg-082bf0e9529a23efa	Public			
Instance Types						
Launch Templates				0.0.0		
Spot Requests	Launch Configuration: AppSe	rverLC				
Savings Plans	Details					
Reserved Instances	Details					
Dedicated Hosts						
Scheduled Instances	AMI ID	ami-0affd4508a5d2481b			Instance Type	t2.micro
Capacity Reservations	IAM Instance Profile				Kernel ID	
	Key Name	MySafeLabKey			Monitoring	false
 IMAGES 	EBS Optimized	false			Security Groups	sg-004599d2fc5354bda
AMIs	Spot Price				Creation Time	Thu Mar 19 10:51:11 GM
ELASTIC BLOCK STORE	RAM Disk ID				Block Devices	/dev/sda1
Volumes	User data	View User data			IP Address Type	Do not assign a public IP
Snapshots						
Lifecycle Manager						

Below are sample User Data scripts that we used.

Web server initialization script:

#!/bin/bash	
sudo yum install -y wget	
sudo yum install -y unzip	
sudo yum install -y lsof//	lsof utility is required for enforcing tetration policies
sudo yum install -y ipset//	ipset utility is required for enforcing tetration policies
sudo yum install -y nginx//	Installing nginx

#Setting up the web server and updating it with hosted configuration file. sudo mv nginx.conf nginx.conf.backup sudo wget https://safelabfiles.s3.us-east-2.amazonaws.com/config/nginx.conf sudo systemctl restart nginx sudo systemctl enable nginx

#Downloading the Tetration enforcement agent from AWS S3 bucket and installing it.

sudo wget https:// safelabfiles.s3.us-east-2.amazonaws.com/config/tetration_installer_intgssopov_enforcer_linux.sh sudo chmod 755 tetration_installer_intgssopov_enforcer_linux.sh sudo ./tetration_installer_intgssopov_enforcer_linux.sh --skip-pre-check

#Downloading the AMP4E agent hosted in an AWS S3 bucket and installing it.

sudo wget https:// safelabfiles.s3.us-east-2.amazonaws.com/config/cisco.gpg
sudo rpm --import ./cisco.gpg
sudo wget https:// safelabfiles.s3.us-east-2.amazonaws.com/config/AWS_rhel-centos7fireamplinux_connector.rpm
sudo yum install -y AWS_rhel-centos-7fireamplinux_connector.rpm

Application server initialization script:

#!/bin/bash sudo yum install -y wget sudo yum install -y unzip sudo yum install -y lsof// lsof utility is required for enforcing tetration policies sudo yum install -y ipset// ipset utility is required for enforcing tetration policies sudo yum install -y httpd// Installing httpd #Setting up the HTTPD server and downloading the application code and Duo plugin hosted in AWS S3 bucket. sudo systemctl start httpd sudo systemctl enable httpd sudo setsebool -P httpd can network connect 1//Allow outbound connections from HTTPD daemon sudo wget https://safelabfiles.s3.us-east-2.amazonaws.com/wordpresscodefile.zip -P /var/www/html/ sudo unzip /var/www/html/wordpresscodefile.zip sudo wget https://downloads.wordpress.org/plugin/duo-wordpress.2.5.4.zip -P /var/www/html/wp-content/plugins sudo unzip /var/www/html/wp-content/plugins/duo-wordpress.2.5.4.zip sudo systemctl restart httpd

#Downloading the Tetration enforcement agent from AWS S3 bucket and installing it.

sudo wget https://safelabfiles.s3.us-east-2.amazonaws.com/config/tetration_installer_intgssopov_enforcer_linux.sh sudo chmod 755 tetration_installer_intgssopov_enforcer_linux.sh sudo ./tetration_installer_intgssopov_enforcer_linux.sh --skip-pre-check

#Downloading the AMP4E agent hosted in an AWS S3 bucket and installing it.

sudo wget https://safelabfiles.s3.us-east-2.amazonaws.com/config/cisco.gpg
sudo rpm --import ./cisco.gpg
sudo wget https://safelabfiles.s3.us-east-2.amazonaws.com/config/AWS_rhel-centos7fireamplinux_connector.rpm

sudo yum install -y AWS rhel-centos-7fireamplinux connector.rpm

Step 3. Set up the Auto Scaling Groups – Create two Auto Scaling Groups using the Launch Configurations created in the previous step, one for the Web servers and another one for the Application servers. For more information on creation of Auto Scaling groups, follow the <u>AWS</u> <u>documentation</u>.

Once the Auto Scaling Groups are created, select each group and click on edit. In the edit menu, update the target groups and health check types. For Web Server Auto Scaling group, set the target group to 'WebServerPool' as created during the Web NLB set up. Also, update the health check type to **ELB** to integrate the Auto Scaling Group with Load Balancer. Repeat the same steps for the App Server Auto Scaling Group, use the target group 'AppServerPool' created during App NLB set up.

🗸 Resource Groups 🗸 🦚	EC2 🌐 VPC 🗯 S3 📲	RDS	🗍 WAF & Shield 💡 IAM 🐴	Ą
Create Auto Scaling group Act	Edit details - ScaleWe	ebSer	vers ×	
Filter: Q Filter Auto Scaling grou	Launch Instances Using	(i)	Launch Template Launch Configuration	
Name + Lau	Launch Configuration	()	WebServerLC *	Health Check
ScaleAppServers App	Desired Capacity	(j)	2	1,800
	Min	(i)	2	
	Max Availability Zone(s)	(i) (i)	2 us-east-1a × us-east-1b ×	
Auto Scaling Group: ScaleWebServ	Subnet(s)	(j)	subnet-06953c1c1acdf22e0(10.0.3.0/24) x WebSubnet1b us-east-1b	
Details Activity History Sc			subnet-0dfe62e16b1eef97d(10.0.2.0/24) X WebSubnet1a us-east-1a	
Launch Configuration	Classic Load Balancers	(i)		s-east-1b c1c1acdf22e0,subn
Desired Capacity	Target Groups	(i)	WebServerPool ×	ef97d
Min Max	Health Check Type	(i)	ELB •	ol
	Health Check Grace Period	(i) (i)	1800	
	Termination Policies	() ()	Default ×	
	Suspended Processes			
			Cancel	

Crea	te Auto Scaling group	Actions ¥									÷	¢ 0
Filter	Q, Filter Auto Scaling	groups	×							K <	1 to 2 of 2 Auto Scaling Groups	\rightarrow $>$
	Name *	Launch Configuration /	· Instances ·	Desired ~	Min 👻	Max –	Availability Zones	Ť	Default Cooldown	✓ Health Check Grac ✓		
	ScaleWebServers	WebServerLC	2	2	2	2	us-east-1a, us-east-1b		300	1,800		
	ScaleAppServers	AppServerLC	2	2	2	2	us-east-1a, us-east-1b		300	1,800		
Auto	Scaling Group: ScaleWel	Scaling Policies	nstances Mon	itoring 1	Notification	ns Tai	Schadulad Action					
							ga Geneduled Action	ns	Lifecycle Hooks			
	Launch Configura	tion () WebServe	rLC				Availability Zone(ns s) (j	Lifecycle Hooks us-east-1a, us-	east-1b	Edit	
	Launch Configura Desired Capa	tion (i) WebServe	rLC				Availability Zone(ns s) (j s) (j	Lifecycle Hooks us-east-1a, us- subnet-06953c 0dfe62e16b1ee	east-1b 1c1acdf22e0,subnet- if97d	Edit	
	Launch Configura Desired Capa	tion (i) WebServe	ягLC				Availability Zone(Subnet(ns s) (j s) (j rs (j	Lifecycle Hooks us-east-1a, us- subnet-06953c 0dfe62e16b1ec	east-1b 1c1acdf22e0,subnet- zf97d	Edit	
	Launch Configura Desired Capa	tion () WebServe	erLC				Availability Zone(Availability Zone(Subnet(Classic Load Balancer Target Group	ns (i) (i) (i) (i) (i) (i) (i) (i) (i) (i)	Lifecycle Hooks us-east-1a, us- subnet-06953c 0dfe62e16b1ee WebServerPoo	east-1b 1c1acdf22e0,subnet- f97d	Edit	

Step 4. Configure the scaling policies - On the Auto Scaling Groups page, select each group and click on Scaling policies tab to add the scaling policies. For testing purpose, we used Simple Scaling of adding or removing one instance when average CPU Utilization exceeds 90% or remains

below a minimum value of 10%. The desired state was set to two instances at a given point of time.

Click on **Add policy** and select **Create a simple scaling policy**. Fill in the policy name, alarm (you will need to create a new alarm) and action as per the requirement.

Create Auto Scaling group	Actions *										Ð	¢	6
Filter: Q, Filter Auto Scali	ng groups	×							K	< 1 to 2 of 2 Auto Scaling	Groups	> 3	>1
Name *	Launch Configuration / ~	Instances ~	Desired ~	Min ~	Max ~	Availability Zones	Ŧ	Default Cooldown	Health Check Grac~				
ScaleWebServers	LC-WebServerConfig	2	2	2	4	us-east-2a, us-east-2b		300	1,800				I
ScaleAppServers	LC-AppServerConfig	2	2	2	4	us-east-2a, us-east-2b		300	1,800				
						000							_
Add policy												Ð	
HighCPUScale											Actions	~	
Higher Oscale											Actions		
Policy type:	Simple scaling												
Execute policy when:	ScaleWebServers-High-	CPU-Utilization											
	for the metric dimension	eshold: CPUUti	Ization >= 9) for 900 s	econds	10 10							
	for the metric dimensio	ns Autoocanny	Groupreame	= 0001041	00001001	5							
Take the action:	Add 1 capacity units												
And then wait:	300 seconds before all	owing another s	caling activi	ty									
LowCPU											Actions	*	
Policy type:	Simple scaling												
Execute policy when:	ScaleWebServers-Low-0	CPU-Utilization											
	breaches the alarm thre	eshold: CPUUti	ization < 10	for 900 se	conds								
	for the metric dimensio	ins AutoScaling	GroupName	= ScaleV	epserver	S							

Follow the <u>AWS documentation</u> for more further details on scaling policies.

Setting up the Firepower Next-Generation Firewalls

In this section, we will set up a pair of Cisco Firepower Next-Generation Firewalls at the network perimeter and onboard them to Cisco Defense Orchestrator for management. As an alternate option, you could also use Cisco FMC (Firepower Management Center) available via the AWS marketplace (or an on-premise FMC) for management purposes.

Once the firewalls are set up, we will enable public access to the application via an 'Outside' Network Load Balancer.

Implementation procedure:

- Step 1. Set up the AWS Environment for NGFWv
- Step 2. Deploy NGFWv EC2 instances
- Step 3. Onboard the NGFWv to CDO
- Step 4. Configure interfaces, routes, NAT and access control on NGFWv
- Step 5. Set up the Outside Network Load Balancer
- **Step 1.** Set up the AWS Environment for NGFW- To deploy Firepower Threat Defense Virtual we need to set up the Network Interfaces for the appliance and allocate Elastic IPs to be assigned to the Management and Outside Interfaces. We use the IP addressing as defined in table below.

NGFWv	Interface Name	IPV4 Address	AWS NIC	Firepower Interface
Safengfw1	Management	10.0.8.200	NICO	Management

NGFWv	Interface Name	IPV4 Address	AWS NIC	Firepower Interface
Safengfw1	Diagnostic	10.0.8.0/24 (DHCP)	NIC1	Diagnostic
Safengfw1	Outside	10.0.0.10	NIC2	Gig0/0
Safengfw1	Inside	10.0.1.10	NIC3	Gig0/1
Safengfw2	Management	10.0.9.200	NICO	Management
Safengfw2	Diagnostic	10.0.9.0/24 (DHCP)	NIC1	Diagnostic
Safengfw2	Outside	10.0.0.138	NIC2	Gig0/0
Safengfw2	Inside	10.0.1.138	NIC3	Gig0/1

Navigate to **EC2 Dashboard > Network Interfaces** and **Create Network Interfaces** for inside and outside interfaces of each FTDv appliance.

aws Services	~ I	Resource Groups 🐱	🌗 EC2 😫 VPC 関 S	3 🏮 RDS 🤳 WAF &	Shield 💡 IAI	∧ ★	
New EC2 Experience	Cre	eate Network Interface	Attach Detach Delete	Actions V			
Events	Q	search : ngfw 💿 Add fi	ter				
Tags Limits		Name ~	Network interface ID *	VPC ID ~	Zone ~	Status ~	Primary private -
INSTANCES		SafeNGFW2Inside	eni-000bd99144ef094d3	vpc-09906c2d738f8ee55	us-east-1b	🥚 in-use	10.0.1.138
Instances		SafeNGFW1Inside	eni-03daeb9c10ee534f2	vpc-09906c2d738f8ee55	us-east-1a	🥥 in-use	10.0.1.10
Instance Types		SafeNGFW2Outside	eni-0a48ceba673394268	vpc-09906c2d738f8ee55	us-east-1b	🥚 in-use	10.0.0.138
Launch Templates		SafeNGFW1Outside	eni-0ff8ff7a293222550	vpc-09906c2d738f8ee55	us-east-1a	🥚 in-use	10.0.0.10
Spot Requests							
Savings Plans							

Select the network interfaces that were created and right click on Change Source/Dest. Check to disable it.

aws Services ▼				
New EC2 Experience X Create	Network Interface Attach Detach De	Actions V		
EC2 Dashboard New Q se	earch : ngfw 🚳 Add filter			
Events New N	lame · Network interface ID	+ VPC ID -	Zone - Status	 Primary private -
Tags	afeNGFW2Inside eni-000bd99144ef094d3	vpc-09906c2d738f8ee55	us-east-1b 🥥 in-us	e 10.0.1.138
Limits	afeNGFW1Inside eni-03daeb9c10ee534f2	vpc-09906c2d738f8ee55	us-east-1a 🥥 in-us	e 10.0.1.10
▼ Instances S	afeNGFW2Outside eni-0a48ceba673394268	vpc-09906c2d738f8ee55	us-east-1b 🥥 in-us	e 10.0.0.138
Instances Si	afeNGFW1Outside eni-0ff8ff7a293222550	vpc-09906c2d738f8ee55	us-east-1a 🥥 in-us	e 10.0.0.10
Instance Types	Ohenne	annes (Deet Oheels V		
Launch Templates	Change	Source/Dest. Check X		
Spot Requests	Network In	terface eni-000bd99144ef094d3		
Savings Plans	Source/dest			
Reserved Instances	304108/4852	 Disabled 		
Dedicated Hosts New	· · · · · · · · · · · · · · · · · · ·			
Scheduled Instances		Cancel Save		
Capacity Reservations				
▼ Images				

Navigate to EC2 Dashboard > Elastic IPs and click on Allocate New Address to allocate two elastic IPs.

New EC2 Experience	11														
Learn more		Alloc	ate new addres	Actions '										÷	۰.
INSTANCES		Q,	Private IP Addr	ess : '10.0.0.10'	Private IP	Address : '10.0.0.138'	3 Add filter						< < 1 to :	2 of 2	> >
Instances	4		Name ~	Allocation ID		~ Instance	~	Private IP address	Scope	Ť	Association ID		~	Netwo	rk Bord
Instance Types			NGFW2Out	eipalloc-075fb	31c69ac435a			10.0.0.138	vpc		eipassoc-0ac12834c38829780			us-eas	i-1
Launch Templates			NGFW1Out	eipalloc-00088	003dfa2f8a32			10.0.0.10	vpc		eipassoc-06125ba81030abde4			us-eas	-1
Spot Requests															
Savings Plans															
Reserved Instances															
Dedicated Hosts															
Scheduled Instances															
Canacity Reservations															

Step 2. Select each of the newly assigned Elastic IP addresses and associate them with Outside Network interfaces created in previous step.

aws Services ▼								
Addresses > Associate address								
Associate address								
elect the instance OR network interface to which you want to associate this Elastic IP address (54.198.47.255) Resource type Instance								
Resource type Instance Vetwork interface								
Network interface eni-0c9b2ca598b3bee5d C								
Private IP 10.0.10								
Reassociation 🗌 Allow Elastic IP to be reassociated if already attached 0								
Warning If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.								
* Required	Cancel Associate							

Step 2. Deploy NGFWv EC2 instances – Navigate to EC2 AWS console and click on launch and choose an AMI for Cisco Firepower NGFW virtual appliance. Choose the Instance Type.

aws Services	 Resource G 	roups 🗸 🏮 EC2	😫 VPC 🛛 🕸 S3	📕 RDS	👃 WAF & Shield	🕴 iam	*	Ę	amansin3 🛩	N. Virginia 👻	Support 👻
1. Choose AMI 2. Choose Instan Step 1: Choose an A An AMI is a template that contains your own AMIs.	Ce Type 3. Config Amazon Ma the software config	4. Add Storag Add	e 5. Add Tags 6 Al) application server, and	i. Configure Security applications) rec	y Group 7. Review	tance. You can s	select an AMI provided b	by AWS, our user commu	nity, or the AWS M	Cane Marketplace; or yo	c el and Exit ou can select one of
Q, Cisco Firepower										Search by Systems	× Manager parameter
Quick Start (0)									K	< 1 to 3 of 3	Products > >
My AMIs (0) AWS Marketplace (3)	cisco	Cisco Firepower NGF	W Virtual (NGFWv) - us versions By Cisco Syste	BYOL ms, Inc.	5/19/20						Select
Community AMIs (0)		The Cisco Firepower NGFV physical and virtual worklo	V Virtual appliance exten ads.	ds comprehensive	e threat protection into vir	ualized environme	ents, providing superior thr	reat defense and visibility	ind consistent secu	rity across	
 Categories All Categories Infrastructure Software (3) Architecture 64-bit (x86) (3) Operating System 	cisco	More info Cisco Firepower Manu ****** (7) 8.8.0-90 Previo Linux/Unix, Other 6.8.0-90 [64- Cisco Firepower Managerr your costs by streamlining More info	agement Center (FM us versions By Cisco Syste bit (x86) Amazon Machine im ent Center manages net operations and automati	Cv) BYOL ms, Inc. age (AMI) Updated: work security and ng many common	5/19/20 operational functions for ily recurring security analy	Cisco NGIPS and I	NGFW products. It automa nent tasks.	atically aggregates and co	rrelates information	. Reduce	Select
All Linux/Unix Other (3) Software Pricing Plans Bring Your Own License (2) Annual (1) Hourly (1)	cisco	Cisco Firepower NGF ****** (0) 8.6.0-90 Previo Starting from \$2.16/hr or from \$ Linux/Unix, Other 6.0.0-90 [44- Seamleessity extend Cisco*s filtering, application visibilit More info	W Virtual (NGFWv) us versions [By Citco Syste 12,914.00/vr (22% savings) / bit (x80) Amazon Machine Im i industry-leading securit ty and control, VPN, and	ms, Inc. or software + AWS us age (AMI) Updated: y to the cloud. Pro more.	age fees 5/19/20 ovides advanced threat de	fense options inclu	luding next generation IPS,	, security intelligence, adv	inced malware prot	ection, URL	Select

Click **Next** to configure the Instance:

Change the Network to match your previously created VPC.

Change the **Subnet** to match your previously created management subnet. You can specify an IP address or use auto-generate.

Network (j	vpc-09906c2d738f8ee55 SecureVPC Create new VPC No default VPC found. Create a new default VPC.
Subnet (j)	subnet-030ec74ce029d3865 MgmtSubnet1a us-et_ 245 IP Addresses available Create new subnet
Auto-assign Public IP 🧃	Enable

Click the Add Device button under Network interfaces to add the eth1 network interface.

Change the **Subnet** to match your previously created management subnet that is used for eth0.

✓ Network interfaces ①										
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs					
eth0	New network interfac ᅌ	subnet-030ec74 0	10.0.8.200	Add IP	Add IP					
eth1	New network interfac ᅌ	subnet-030ec74 🗘	Auto-assign	Add IP		8				

Under Advanced Details, add the default login information as User data.

 Advanced Details 		
Metadata accessible	(i)	Enabled
Metadata version	i	V1 and V2 (token optional)
Metadata token response hop limit	(j)	1
User data	(j)	OAs text ○ As file ○ Input is already base64 encoded
		#Sensor {

Click **Next** to **Add Storage**. You can accept the default or change the volume. Click **Next** again to add a **Tag**, this step is optional as well.

Lastly, Select **Next** again to **Configure Security Group**. Click **Select an existing Security Group** and choose the previously configured Firewall Security Group.

1. Choose AMI	2. Choose Instance Type 3. Co	nfigure Instance 4. Add Storage 5. Add Tags 6	3. Configure Security Group 7. Review		
Step 6: Co A security group rules that allow u	onfigure Security Gi is a set of firewall rules that cont inrestricted access to the HTTP a Assign a security group:	YOUP of the traffic for your instance. On this page, you can nd HTTPS ports. You can create a new security group Create a new security group 9 Select an existing security group	add rules to allow specific traffic to reach your instan p or select from an existing one below. Learn more al	ce. For example, If you want to set up a web server a bout Amazon EC2 security groups.	nd allow Internet traffic to reach your instance, add
Security	Group ID	Name	Description		Actions
sg-004599	d2fc5354bda	AppSG	SG for app tier		Copy to new
sg-02b316	8a219536b31	d-90677579df_controllers	AWS created security group for d-90677579df d	irectory controllers	Copy to new
sg-0c0a34	c073d72bda1	DbSG	SG for database tier		Copy to new
sg-068a6a	9e1621f48ae	default	default VPC security group		Copy to new
sg-0be45b	aca20974d36	FirewallSG	Security Group for Firewalls		Copy to new
sg-0abe4f	2af86d6c095	FrontSG	Frontend SG		Copy to new
sg-0b55db	462c834ef86	MgmtSG	SG for management tier		Copy to new
sg-082bf0	e9529a23efa	WebSG	SG for workloads in web tier		Copy to new
Inbound rules	for sg-0be45baca20974d36 (Sel	ected security groups: sg-0be45baca20874d36)			
Type (i)		Protocol ()	Port Range (i)	Source (i)	Description (i)
All traffic		All	All	0.0.0/0	
All traffic		All	All	::/0	

Click **Review and Launch**. Repeat the same steps to launch the second FTDv appliance, make sure you select management subnets corresponding to second Availability Zone.

	aws s	Services	s ¥	Re	esource Grou	ps ~	EC2	😫 VP	c 📫 S3	🔋 RDS	🦺 WAF & Shield	👔 IAM	*
C	New EC2 Experience Learn more	e		Laun	ich Instance	- Co	onnect	Actions ¥					
	EC2 Dashboard			Q,	VPC ID : vpc-0	9906c2d7	38f8ee55	search :	ngfw 💿 Add filte	ər			
	Events							_					
	Tags		۰.		Name	î	Availabilit	y Zone 👻	Instance State 👻	Status Ch	iecks *		
	Limits				SafeNGFW1		us-east-1a		running	2/2 ch	ecks passed		
-	INSTANCES				SafeNGFW2		us-east-1b		running	🥝 2/2 ch	ecks passed		
1	Instances												
	Instance Types												
	Launch Templates												
	Spot Requests												

Select the newly configured FTDv appliance and click **Actions**, select **Networking > Attach Network Interface** to attach the outside and inside Network Interfaces created in Step 1.





Step 3. Onboard the NGFWv to CDO - Access the Firepower Device Manager (FDM) using the management IP address. Click on skip device set up and acknowledge the 90-day trial license warning (we will configure smart licensing in subsequent steps). You will land at the FDM home page.



Firepower Device	Manager	Monitoring Policies O	Dbjects D	Device: safengfw1) 🖨 🛛) (?) :	admin Administrator
O Ko	del co Firepower Threa	sof t Defense fi 6.5	VDB 309.0	Rule Update High / 2019-08-12-001-vrt Not C	Availability 🕜 configured	CONFIGURE	
	F Inside Netwo	Cisco Firepower Threat Defense (0/0 () () () () () () () () ()	for A 0	MONT E CONSOLE ISP/WAN/Gateway	Internet DNS Serve ONTP Serve	yr Yr	
Interfaces Connected Enabled 3 of 3 View All Interfaces	>	Routing There are no routes yet Create the first static route	>	Updates Geolocation, Rule, VDB, System Upgrade Security Intelligence Feeds View Configuration	sy: e, Mar Log DHC DNS	stem Settings nagement Access Iging Settings CP Server S Server	
Smart License Evaluation expires in 90 days View Configuration	90 DAYS	Backup and Restore	>	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Mar Hos NTF Cloi Reb Trat	hagement Interface stname oud Services boot/Shutdown ffic Settings	

Log on to the CDO web portal and go to **Devices and Services** and click on plus button on the top right-hand side to onboard a Firepower Threat Defense (FTD) device. We use **Registration Key** option to onboard the FTD. Fill in the name of the FTD device and follow the wizard to copy the registration key.

altala cisco	Defense Orchestrator	Onboard FTD Device	<u>↓</u>	0 -	safe-architecture
≡	Hide Menu	Follow the steps below			Cancel
÷ ۵	Devices & Services				
	uration				
۳ م	Policies >	Use Registration Key Use Credentials Discust a write using a registration key FTD Device Ontoard a control using the 3 address, or incort and, and a username and			
•@• (Joyects	Firepower Throat Defense 6.4+ Ceuce wang Firepower Device Manager parsword.			
-å• \	/PN >				
Ľ,	Femplates ASA	Device Name safengfw1			
畲丶	Migrations (BETA)	2 Database Updates Disabled			
Events	& Monitoring				
γľ×	Monitoring >	Create Registration Key Opy registration key			
	Change Log				
	lobs	Paste the registration key copied above in the Cloud Services management in FDM. Learn methods are completed above in the Cloud Services management in FDM. Learn methods are completed above.	ore 🗗		
		Next			
		Smart License			
		5 Done			

Go back to FDM portal and go to **Cloud Services** option under **System Settings**. Paste the **Registration Key**, specify the **Region** and click on **Register**.

Firepower Devi	ce Manager Monitoring Policies Objects Device: safengfw1 Device: safengfw1 Dev
System Settings ← Management Access Logging Settings DHCP Server DNS Server Management Interface	You can manage the device using Cisco Defense Orchestrator. With Cisco Defense Orchestrator, you can configure multiple devices of different types from a cloud-based configuration portal, simplifying policy consistency and deployment across your network. • If you already have a Cisco Defense Orchestrator account, log in and obtain a registration key for the device, which you can enter below. Log into Defense Orchestrator. • If you do not have an account, learn more about what Cisco Defense Orchestrator can do for you, and how to register. How cloud management works
	CUSTOMER POLICIES CLOUD DEVICE
Cloud Services Reboot/Shutdown	V GET STARTED
Traffic Settings	
URL Filtering Preferences	Region Carlos Ca

Come back to the CDO portal, click on **Next** and log into your Cisco smart licensing manager and generate the token. Paste the token and click on **Next** to finish the onboarding process.

ahaha cisco	Defense Orchestrator	Onboard FTD Device	()	0 -	safe-architecture
≡	Hide Menu	Follow the steps below			Cancel
Event	Hilde Menu Devices & Services urration Policies	Follow the steps below Image: Control of the step belo			Cancel
		Skip Next			

Repeat the same steps for the other firepower device, CDO will sync the configuration for both the devices. At this point we have successfully finished onboarding both the FTDs to CDO.

Cisco Defense Orchestrator	Devices & Services		<u>↔</u> • • •	safe-architecture _
🗮 Hide Menu	T Q safe	Displaying 2 of 2 results		C 🐵 🕇
Devices & Services	Name \$	Configuration Status 🗢	Connectivity \$	
Configuration	safengfw1 FTD	Ö Synced	 Online 	
🚱 Objects	safengfw2 FTD	Ø Synced	Online	
₀å₀ VPN >				
ASA Templates				
企 Migrations 8ETA				
Events & Monitoring				
√r Monitoring >				
Change Log				
لط Jobs				

Step 4. Configure interfaces, routes, HTTPS health probes, NAT and access control on NGFWv - We need to configure the following four components:

- Network interfaces
- Static routes
- NAT rules
- Access rules

Click on the onboarded NGFWv appliance on CDO dashboard and then go to **Interfaces** option from the menu that appears on the right-hand side of the dashboard. Make sure Gig0/0 and Gig0/1 are assigned static IP addresses and names as defined in the table in Step 1.

cisco Defense Orchestrator	Interfa	iterfaces / SafeNGFW1											
Hide Menu	🗲 Return to	um to Devices & Services											
	T Q	Search for interfaces by name, ID or IP			c 🔸								
		Name \$	Logical Name \$	State \$	Security Zone	IP Address	Interface Type		Mode				
		GigabitEthernet0/0	outside	Enabled		10.0.0.10 STATIC	Physical Interface		Routed				
	÷	GigabitEthernet0/1	inside	Enabled		10.0.1.10 STATIC	Physical Interface		Routed				
	Ð	Management0/0	diagnostic	Enabled			Physical Interface		Routed				

Go back to the same menu and go to Routing option now, set the default route pointing to the gateway on outside the subnet- 10.0.0.1. Also, add the route for internal subnets (web, app and database subnet) pointing to the gateway on the inside subnet- 10.0.1.1. Lastly, add a route for AWS Metadata Server IP address for health probes, set the next hop as the inside subnet gateway.

cisco Defense Orchestrator	Static Routes / safe	ngfw1				4	0 -	safe-arcl amansin3@	hitecture Pcisco.com				
Hide Menu	← Return to Devices & Services	to Devices & Services											
	Y Q Search for static ro	4 Search for static routes by name, interface name, network IP or gateway IP Displaying 3 of 3 results											
	Name	Interface	IP Type	Destination Networks	Gateway IP			,	Metric				
	Default	outside	IPv4	any-ipv4 0.0.0.0/0	OutsideGW1a 10.0.0.1			1	1				
	insideSubnets	inside	IPv4	InsideVPC 10.0.0.0/16	InsideGW1a 10.0.1.1			1	1				
	AWSMetaDataServer	inside	IPv4	AWSMetaDataSer 169.254.169.254/32	InsideGW1a 10.0.1.1			1	1				
Templates ASA													

Next, we set up three NAT rules. First is an optional dynamic PAT rule to allow outbound traffic to the Internet from the application workloads. You would need this rule if you decide to forward any outbound flows to the internet via NGFWv appliance. The translation would be as below.

Source: WorkloadIP:Port => OutsideFWInterfaceIP:Port

Second, a static NAT rule to expose the AWS application to the users on the internet accessing the application. We need the source translation to ensure that reply traffic is returned back to the same firewall's inside interface i.e. maintain the traffic symmetry. The destination is translated from outside interface IP of the FTD appliance in the specific availability zone to the static IP address of the Web NLB in same zone.

Source translation: InternetUserIP:Port => InsideFWInterfaceIP:Port

Destination translation: OutsideFTDIP:HTTP => WebLBIP:HTTP

In a similar manner, we pick a random health check port for FTD (example – TCP port 6612) and set up third NAT translation rule to forward the health check traffic to AWS metadata server. When Outside NLB sends TCP health probes on port 6612 to outside interface of FTD, the FTD would translate the source to Inside interface IP and destination to AWS metadata server on port 80 and forward the traffic.

Source translation: InternetUserIP:Port => InsideFWInterfaceIP:Port

Destination translation: OutsideFTDIP:HealthCheckPort => AWSMetaDataServer:HTTP

cisco Defense Orchestrator	NAT Rules	/ FTD: safe	ngfw1					4	0 -	safe-architecture amansin3@cisco.com		
Hide Menu	 Return to Devices 											
Devices & Services	T Q Sea	arch				Displaying 3 of 3 rules				с +		
Configuration				Destination	Original Packet			Translated Packet				
Dellaise .	Name	Туре	Source Interface	Interface	Source	Destination	Service	Source	Destination		Service	
Policies	Twice NAT											
Objects	MetadataServer	t⊐ Static	outside	inside		interface	HealthCheckPort	interface	AWSMetaDataServer		нттр	
s‰ VPN >	WordPressApp	ti Static	outside	inside		interface	HTTP	interface	WebNLB1a		нттр	
ASA Templates	InternetAccess	→ Dynamic	inside	outside				interface				
Migrations Migrations												

Lastly, we configure access control policies to allow traffic from inside zone to outside zone. We also allow HTTP traffic incoming from the Internet users and health probes from outside NLB.

Go to Policies > FTD Rulesets on CDO portal and click on plus button to add a an FTD ruleset. Within this newly created ruleset, add the access rules and attach it to the newly onboarded FTD appliances.

#	Name	Action	Source	Destination	Layer 7
1	InternetAccess	🗹 Trust 🛛 🖏 🕞	ZONES Inside_zone	ZONES outside_zone	Any
2	WordPressAppAccess	Allow 🖏 C ₀ 🖹	ZONES Outside_zone	ZONES Inside_zone INETS WebNLB1a IPORTS HTTP	Any
3	HealthCheck	Allow 🔩 🕞 📄	JZONES Outside_zone	I ZONES Inside_zone I NETS AWSMetaDat I PORTS HTTP	Any

Repeat the same set up for the second FTD device and then deploy all the changes.

Step 5. Set up the outside NLB - In this step, we will set up the outside NLB with the Target Group for outside interfaces of the two FTDv appliances.

aws Service	es v	Resource Groups ~	🌔 EC2	🌐 VPC	i ii sa	🛑 RDS	🦺 WAF & Shield	💡 IAM	*		4 •	amansin3 👻	N. Virginia 👻	Support 👻
1. Configure Load Balancer	2. Conf	igure Security Settings 3.	Configure Routing	4. Register	Targets	5. Review								
Step 1: Configure	e Loa	d Balancer												
Basic Configuration	n													
To configure your load balance	er, provi	de a name, select a schem	e, specify one or	r more listener	rs, and sele	ct a network.	The default configuratio	n is an Interne	t-facing load	balancer in the selected ne	stwork with a lis	tener that recei	ives TCP traffic o	on port 80.
Name ()	Outsi	deNLB												
Scheme (i)	o int ⊖int	ernet-facing ernal												
Listeners														
A listener is a process that ch	ecks for	connection requests, using	g the protocol an	nd port that yo	u configure	d.								
Load Balancer Protocol							Load Balan	cer Port						
ТСР							80							\otimes
Add listener														

Select the two availability zones and corresponding Outside Subnets that we set up previously.

Availability Zones						
Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.						
Create and manage Elastic IPs in the VPC console C*						
VPC () vpc-09906c24738f8ee55 (10.0.0.0/16) SecureVPC •						
Availability Zones 💈 us-east-1a (subnet-085/3155148Ica9dd (OutSubnet1a) =						
IPv4 address ① Assigned by AWS -						
Image: Submet-0766d766ccfa85994 (OutSubmet1b) Image: Submet-0766d766ccfa85994						

At Step 3, specify a **Name** for the **Target group** for FTD appliances. Select the **Target type** as IP and **Protocol** as TCP on Port 80. For **Health checks**, override the **Port** to 6612 (we had previously set up the FTD to redirect health probes on port 6612 to AWS metadata server). Click **Next** after making all the changes.

aws Services ▼					A
1. Configure Load Balancer	2. Cor	nfigure Security Settings	3. Configure Routing	4. Register Targets	5. Review
Step 3: Configu Your load balancer routes balancer.	ire Ro requests	outing to the targets in this ta	rget group using the p	rotocol and port that y	ou specify, and performs health checks on the targets using these health check settings. Note that each target gro
Target group					
Target group	()	New target group		•	
Name	(i)	FirewallPool			
Target	type	InstanceIP			
Protocol	(j)	TCP		•	
Port	(j)	80			
Health checks					
Protocol	()	TCP		•	
 Advanced health 	n check	< settings			
Port	(j)	 traffic port override 	6612		
Healthy threshold	(j)	3			
Unhealthy threshold	(j)	3			
Timeout	(i)	5	Sec	onds	
Interval	()	10 seconds30 seconds			

For target registration, add the Outside interface IP addresses.

WOLK 0			IP (Allowed ranges)	Port ()		
x-09906c2d738	10.0.0/	1/16)	•	: 80	🕹 Add to list	
				To be registered		
total IP addres	ises.			To be registered		Clear all
total IP addres	sses. : 80	us-east-1b	instance (i-0cc66727d96b88fd1)	To be registered		Clear all

Click Next and Review and submit the changes to finish Outside NLB creation.

aws	Services	 Resource 0 	Groups 🗸 🌗	EC2 😫 VPC	📫 S3	🔋 RDS	👃 WAF & Shield	🕴 IAM	*	L	↓ •
New EC2 Experienc	e	Create Load B	alancer Actions	5 *							
Limits		Q search : N	NLB 📀 Add filter								
INSTANCES	4	Name		DNS name	- State		- VPC ID		 Availability Zon 	es - Type	
Instances		AppNLB		AppNLB-5cad66ee	e8ff active		vpc-09906c	2d738f8ee55	us-east-1a, us-ea	ast-1b network	
Instance Types		OutsideNL	LB	OutsideNLB-c447d	b4 active		vpc-09906c	2d738f8ee55	us-east-1a, us-ea	ast-1b network	
Launch Templates		WebNLB		WebNLB-cadea0d	492 active		vpc-09906c	2d738f8ee55	us-east-1a, us-ea	ast-1b network	
Spot Requests											
Savings Plans											
Reserved Instances		Load balancer:	OutsideNLB								
Dedicated Hosts		Description	Listeners M	onitoring Integra	ated services	Tags					
Capacity Reconvetio	5			0							
Capacity Reservatio	115	Basic Conf	iguration								
IMAGES			Name	OutsideNLB							
AMIS			ARN	arn:aws:elasticlo	adbalancing:u	s-east-1:904	585389016:loadbalance	/net/Outside	NLB/c447cb42ad37e3d	1 47	
ELASTIC BLOCK STOR	RE		DNS name	OutsideNI B-c//	17cb/22d37e3	d1 elb us-eas	t-1 amazonawe com				
Volumes			DNS hame	(A Record)	+1 CD-+2 a057 65	u1.eib.u3-ea					
Snapshots			State	active							
Lifecycle Manager			Type	network							
NETWORK & SECURIT	Y		Colorean Col	internet fasian							
Security Groups			Scheme	internet-racing							
Elastic IPs			IP address type	ipv4							
Placement Groups			VPC	vpc-09906c2d7	'38f8ee55 📝						
Network Interfaces			Availability Zones	subnet-085f3f55	5148fca9dd - u	is-east-1a 📝	н. — — — — — — — — — — — — — — — — — — —				
Network Interfaces				IPv4 addres	s: Assigned by	AWS					
LOAD BALANCING				subnet-0766d76	66ccfa85994 -	us-east-1b	2				
Load Balancers				IPv4 addres	s: Assigned by	AWS	,				
larget Groups				Edit subnets							
AUTO SCALING				Eur Subilets	J						

After few mins, both the FTDs should register as targets and health status should move to healthy.

aws Services	 Resource Groups ~ 	🌗 EC2 🛛	💲 VPC 🛛 🏟 S	i3 🔋 RDS	🦺 WAF & Shield	💡 IAM 🛛 🕈		Д° amansin3 ↔	N. Virginia 👻	Support	t ~
New EC2 Experience	Create target group Acti	ons 👻								Ð	¢ 0
Limits	Q search : arn:aws:elasticle	adbalancing:us-e	ast-1: 💿 Add fi	Itor					< < 1 b	o 1 of 1	> >
INSTANCES	Name	+ Port	~ Pr	rotocol - Targ	et type 🗸 Lo	ad Balancy VPC ID	 Monitoring 				
Instances	FirewallPool	80	тс	CP ip	O	tsideNLB vpc-09906c2d738f8	ee55				
Instance Types											
Spot Requests	Target group: FirewallPool										
Savings Plans										_	
Reserved Instances	Description Targets	Health checks	Monitoring	Tags							
Dedicated Hosts	The load balancer starts rou	tina requests to	a newly registered	target as soon as	the registration proces	s completes and the target pass	ses the initial health checks. If d	emand on your targets	increases, vou c	an registe	er
Scheduled Instances	additional targets. If demand	d on your targets	decreases, you ca	n deregister targe	ts.						
Capacity Reservations	Edit										
IMAGES	Registered targets										
AMIs	negistered targets										
ELASTIC BLOCK STORE	IP address	Port	Availability Zone	0	Status	Description	- Annual annuals is suite about				
Volumes	10.0.0.138	80	us-east-1b		healthy	This target is currently passing	g target group's health checks.				
Snapshots	10.0.0.10	00	us-east-Ta		nearrny	This target is currently passing	g target group s nealth checks.				
Lifecycle Manager	Availability Zones										
NETWORK & SECURITY	Availability Zone				Target co	unt		Healthy?			
Security Groups	us-east-1b				1			Yes			
Elastic IPs	us-east-1a				1			Yes			
Placement Groups											
Key Pairs											
Network Interfaces											
LOAD BALANCING											
Load Balancers											
Target Groups											

Enabling WAF and DDoS protection

At this point we have finished setting up a fully functional cloud application. We will now add the WAF and DDOS protection capabilities in our design.

Radware Cloud WAF and DDoS services are integrated by using CNAME DNS records. Deployment is independent of any specific Cloud service providers.

Implementation procedure:

- Step 1. Onboard the application to Radware Cloud
- Step 2. Register a domain using AWS Route 53 service
- Step 3. Update the DNS setting to point traffic to Radware Cloud
- **Step 4.** Access the application
- Step 1. Onboard the application to Radware Cloud The first step to integrating Radware cloud service is to onboard the application onto the Radware cloud. On the Radware cloud portal, go to Assets > Application and click on the plus button on the upper right-hand side of the screen. Add the prompted details i.e. the Application Domain Name (www.mysafeapp.net), the Origin Server (in this case it would be the Outside network load balancer's FQDN) and the Protocol (HTTP). If your application is based on HTTPS protocol, you would need to add the certificate information as well.

Note: As part of the onboarding process, each customer can choose between immediate and learning based protection. Immediate protection will enforce a predefined security policy, preventing known attacks. In order to cover both known and unknown attacks, Radware recommends using the learning-based protection method. During the first 2 weeks (duration can vary depending on traffic), Radware evaluates traffic patterns and can automatically update both negative and positive security models by refining signatures, creating exceptions and building the allowed file extension list per application, greatly reducing false positives.

Cisco-SafeArchitecture 🗸 🛍 Dashboar	🗇 Monitor 🖓 Assets 📓 Account	F 4 0 🌒 •
	New Application	
	Display Name 🛈 mysafeapp	
	Application Domain ① www.mysafeapp.net	
	Origin Server © FQDN V Damazonaws.com	
	Region () North America (Ashburn)	
	Application Protocol ^①	
	General Information (optional)	
	Cancel Save	

Once the details are saved, the application can be seen as below.

000	Cisco-SafeArch	itecture 🗸	ណ៍ Dashboard	🗇 Monitor	🔅 Assets	Account			F 4 0	•
	Application	S		domain 🗙 Q	Showing 1 out of 3	Z 🍙 i 🛛	0 0 2 0			+
	State 📬	Name 印		Domain 🕫		Created 1	Region 14	Events (Last 7 Days) 10		
	(B)	mysafeapp	2	www.mysafe	eapp.net	2020/07/09	North America (Ashb	0	Ū	I.

Click on the application and copy the allocated **CNAME**. We need to create a DNS record for our application with this Radware CNAME.

Cisco-Safe	aArchitecture 🗸 🗃 Dashboard 🕡 Monitor 🛛 🐯 Assets 📓 Account	E 4 0 🚺 ·
← All Applications	mysafeapp www.mysafeapp.net	
Ceneral Ceneral Network Cecess Control	Protection: Learning-based Region: North America (Ashburn) ① Created: 2020/05/12 DNS Records ① radvarecould ret Co to Security Events Co to Application Analytics	ents

Step 2. Register a domain using AWS Route 53 service - On the Route 53 dashboard on AWS console, click on Create Hosted Zone to register a domain for the application. The registration process might take anywhere from few minutes to few hours to complete.

aws	Services	 Resource Groups 	🌓 EC2 🛛 😫 VPC	📫 S3 🏮 RDS 🤳	WAF & Shield 💡 IAM 🔸
Dashboard	4	Create Hosted Zone	Go to Record Sets	Delete Hosted Zone	
Hosted zones		Qsafe	X All Types	·	
Health checks		Domain Name	v	Type - Record Set Count -	Comment
Traffic flow		mysafeapp.net.		Public 6	HostedZone created by Route53 Registrar
Traffic policies Policy records					

Step 3. Update the DNS setting to point traffic to Radware Cloud – Once the domain registration is completed, go back to **Route 53** hosted domain and update the DNS record sets with Radware CNAME. After this change, it might take a few minutes for the DNS update to propagate. Once the DNS records are fully updated, the traffic will start getting redirected to Radware Cloud servers before it hits the 'origin server' in the AWS cloud.

Note: To eliminate direct origin attacks, Radware recommends configuring the perimeter firewall to only allow the Cloud WAF to access the application origin server directly. The service IP addresses can be requested from Radware Support Team. For more information, check out the <u>Radware Cloud WAF Quick</u> <u>Start guide</u> (login required).

✓ Resource Groups ✓ () EC2 ⊕ VPC	🏮 S3 🛛 🏮	RDS 🦺 WAF & Shield 💡 IAM	*		ậ amansin3 ▾ Global ▾ Support ▾
Back to Hosted Zones Create Record Set	nport Zone Fil	Delete Record Set Test Record	i Set		C \$ 0
QRecord Set Name X Any Type	Aliases Only	Weighted Only K K Display	ring 1 to 6 out of 6 Record Sets 🗦	>>1	Edit Record Set
Name	Type V	/alue	Evaluate Target Health	Health C	Type: CNAME – Canonical name
mysafeapp.net.	A A	ALIAS www.mysafeapp.net. (z08809141txn0vvyapy	No -		Alias: Yes No
mysafeapp.net.	n: NS n: n:	is-1151.awsdns-15.org. is-331.awsdns-41.com. is-1616.awsdns-10.co.uk. is-689.awsdns-22.net.			TTL (Seconds): 300 1m 5m 1h 1d Value: .radwarecloud.net
mysafeapp.net.	SOA n	ns-1151.awsdns-15.org. awsdns-hostmaster.amazoi			The domain name that you want to
api.mysafeapp.net.	A A	ALIAS d-ivv5gdnnm4.execute-api.us-east-1.amazon	No -		resolve to instead of the value in the Name field.
8f626afaa6edbf115595a696603ef545.api.mysafeapp.net.	CNAME _	c3bafc13108b60ab875b07438f9990a8.nhqijqilxf.ac	*		www.example.com
www.mysafeapp.net.		.radware		•	Routing Policy: Simple
					Route 53 responds to queries based only on the values in this record. Learn More

Step 4. Access the web application – Go to this newly registered domain URL in the browser, you will be prompted to do the initial application setup, after the initial set up the application home page should load as below.



Integration with Cisco SecureX

In this last deployment step, we will enable the Umbrella, Stealthwatch Cloud and Tetration and AMP4E modules in the SecureX portal to get a unified view into the AWS environment. We create API keys in the product portals and then configure those keys in the threat response dashboard.

Implementation procedure:

- Step 1. Add Integration modules
- Step 2. Save the module
- **Step 1.** Add Integration modules Log on to the SecureX dashboard and go to Integration modules tab, click on Add a New Module and select from the available modules. SecureX dashboard displays all the steps on API key generation and integration for each available module.

CISCO SECUREX Dashboard Integration Modules A	Iministration	Amandeep Singh \
My Integration Modules		
Add New AMP for Endpoints Module		
Module Name	Quick Start	
AMP for Endpoints		
URL [®] https://api.amp.oisco.com 3rd Party API Client ID API Key [®]	When configuring AMP for Endpoints integration, you must first gather some information from your AMP for Endpoints instance and then add the AMP for Endpoints module. 1. Log into the AMP for Endpoints console, click the Accounts menu and choose API Credentials. Credentials. 2. Click New API Credential, enter the Application name and Scope (action you want to allow) and then click Create. From the API Key Details page, copy both the 3rd Party API Client ID and the API Key into a file, or leave the tab open. Important: Do not close the tab without retrieving these values; the API key is not retrievable once the tab is closed. 4. Complete the Add New AMP for Endpoints Modula form: - Module Name - Leave the default name or enter a name that is meaningful to	
Act in the name of Active User	you. (You use the default name unless you already have a module named AMP	
When selected. Casco Travert Response will act in the name of the currently logged in user. For this to work, the and Party API Client ID and the API Key must be administrator credentials. More information is available in our	for Endpoints or you need to specify one of several regional Cloud instances.) • URL - From the drop-down list, choose the appropriate URL for the regional AMP Cloud account.	
	 3rd Party API Client ID - Copy and paste the value obtained earlier. API Key Compared paste the value obtained patient. 	
Cancel Save	 Arr resy copy and passe the value obtained earlier. Act in the name of Active User - Check the check hox if you want to interact with AMP in the name of the user that is currently logged in. 	
	5 Click Save to complete the AMP for Endpoints module configuration	

Step 2. Save the module – Click on **Save** to complete the integration. In a similar manner add all the remaining modules. After we have saved the module configurations, the modules will be listed under **Integration Modules** tab as below.

CISCO SECURE X Dashboard Integration Modules	Administration	Amandeep Singh ~
Integrations SecureX uses modules to integrate with other Cisco security products and third-party	solutions. Click here to view all the available modules.	
Your Configurations		
	AMP for Endpoints Solutegrated	Cisco Tetration - Application-First Workload Mintegrated Cisco Tetration - Application-First Workload Protection
Add New Module		
	Edit Learn More	
l		
F Firepower SIntegrated	So SecureX Orchestrator SocureX Orchestrator	Swc Stealthwatch Cloud Integrated Stealthwatch Cloud
Firepower provides complete and unlifed management over firewalls, application control, intrusion provention, URL filtering, and advanced		
Edit Learn More	Edit Learn More	Edit Learn More
Umbrella Integrated Umbrella Umbrella Umbrella Integrated	Radware Cloud WAF Service Integrated Radware Cloud WAF Service	
selective proxy. Threat Response supports multiple Umbrella functions Edit Learn More	an easy to use, hassie free service.	
restor SECURE X III Home		III 📓 🗟 🤇 Enter logs, IPs, domains, etc. 🔤 🗖 🌣 💿 +

Validation Testing

Tetration

Validation procedure overview:

- Test Case 1 Creating the workspace for AWS cloud application
- Test Case 2 Using ADM to discover the policies for AWS workloads and setting up an app view

- Test Case 3 Enforcing the policies on workloads
- Test Case 4 Discovering the vulnerable packages on the AWS workloads

Test Case 1: Creating an application workspace for AWS cloud application

This test case involves defining annotations for the AWS environment. These annotated attributes are used later to segregate the tiers and segments within the AWS VPC and hence define a workspace for our tiered cloud application.

Validation procedure:

- Step 1. Build an inventory
- Step 2. Define scopes
- Step 3. Create a workspace
- Step 1. Build an inventory Define the attributes that would help you segregate your tiered application workloads in the cloud and hence construct policies for them. We will use a combination of two different methods to add user annotations 1) Upload a CSV file 2) Auto generate annotations using external AWS orchestration.

1.1: Based on the architecture of our tiered application (elaborated in the previous sections of this document), the following annotations were used (Table: AWS Cloud Inventory). Save this in a CSV file format.

IP	Application	Region	Tier	Туре
10.0.2.0/24	Safe3tierApp	US-East-2	WebServer	AWS-Cloud
10.0.3.0/24	Safe3tierApp	US-East-2	WebServer	AWS-Cloud
10.0.4.0/24	Safe3tierApp	US-East-2	AppServer	AWS-Cloud
10.0.5.0/24	Safe3tierApp	US-East-2	AppServer	AWS-Cloud
10.0.6.0/24	Safe3tierApp	US-East-2	Database	AWS-Cloud
10.0.7.0/24	Safe3tierApp	US-East-2	Database	AWS-Cloud
10.0.8.0/24	Safe3tierApp	US-East-2	Management	AWS-Cloud
10.0.9.0/24	Safe3tierApp	US-East-2	Management	AWS-Cloud

1.2: Now, log into the Tetration cloud portal and go to 'Visibility > Inventory Upload'. Click on 'Select File' and 'add' the CSV file.

C.	CiscoTetrati@n* INVENTORY UPLOAD	/ • 😌 Monitoring • 🗊 • 😂 •
сн Сов	Managing inventory annotations on the	Select annotation columns to enable on inventory and flows. Application Location Brancing Control Contro
Ø ⊥ ¢ ¢	Upload Select File A Download Annotations A Select a CSV file to add or delete annotations. The uploaded CSV can specify what to annotate using IP. Download Sample A The CSV file must look like:	G Regon () G Ter () G Type () Save Reset
	IP,Department,Datacenter,,Columm HeaderK 7.7.7.7,HR,SJC,,colummK_Value If the number of annotations provided is more than 32, Tetration will pick the first 32 columns for annotations.	

1.3: Go to 'Visibility > External Orchestrator'. Click on 'Create New Configuration' and fill in the required details as shown below.

Note: - You will need to create an Access Key in your AWS account to be used in this configuration. Follow AWS documentation for more details on access key creation.

۵.	Cisco Tetrati« n°	EXTER	RNAL ORCHESTRAT	ORS						AWS-US-EAST +	Solution	⑦ ▼ ⊕ ⁰ ₀ ▼
ш ¢	Filter © Enter attributes () Filter										+ Create N	ew Configuration
۲	Name	÷	Туре	÷	Descrip	tion	Created At	-	Connection Status	÷	Actions	÷
Ø	AWS		aws		AWS Ck	bud	Jan 8 10:25:57 am (EST)		Success		00	
۵ م							Configu	ration Details				
¢						aws_access_key_id						
D						aws_region	us-east-2					
						delta_interval	60					
						description	AWS Cloud					
						dns_zones						
						full_snapshot_interval	3600					
						hosts_list						
						id	5e15f485497d4f7ed9551	bcl				
						insecure	true					
						name	AWS					
						type	aws					

1.4: After a few minutes, you can go to 'Visibility > Inventory Search' and test the filters generated, based on annotations from the Step 1.2 and 1.3 above.

0	Cisco Tetratign" INVENTORY SEARCH			AWS-US-EAST • 🛞 Monitoring • 🛞 • 🕮
ш				③ Total inventory: 12,765
#	Filters @ *Tier = Database or *orchestrator_Name = W	ebServer or *orchestrator_Name = AppServer	Search	Create Filter
Ð				
۵	Showing 5 of 5 matching results			Results restricted to root scope
ß	V Hostname	▲ VRF	Address	0 OS 0
۵	ip-10-0-2-16		10.0.2.16	CentOS
	ip-10-0-3-126		10.0.3.126	CentOS
	ip-10-0-4-89		10.0.4.89	CentOS
1	ip-10-0-5-129		10.0.5.129	CentOS
			10.0.6.79	
	A Download table data as JSON			

Step 2. Define scopes - We will define a scope to group together all the workloads in our tiered application in the AWS cloud. We will make use of the annotations/filters that we constructed in Step 1. We created the scope 'AWS-US-EAST', which includes all the workloads from our tiered app in 'US-East' region in AWS Cloud.

Click on the settings icon in the top right corner of the portal and then go to 'Scopes' option. Click on 'Create New Scope' and fill in the name of the Scope and a query as below.

	Cisco Tetratie n'	SCOPES			A	WS-US-EAST - S Monitoring -	
E H	Ā	INTGSSOPOV : SAFE CLOUD 2	INTGSSOPOV : SAF	E CLOUD : AWS-US-EAST		Cre	ate New Scope
9 9	4 4 A	Filters O Filter Scopes	Description	AWS based cloud application			
囚	Name -	Query			ty : Tota	l Children :	
0	AWS-US-EAST	* Type = AWS-Cloud ar	Query Θ	*Type = AWS-Cloud and *Application = Safe3tierApp and *Region = US-East-2	er O	CE Edit Delete	
	AZURE	* Type = AZURE-Cloud			er O	Call Edit	
	GCP	* Type = GCP-Cloud		4 Save Cancel	er O	C2 Edt D Drivte	
-				View Deleted Scopes T2			

Step 3. Create a workspace - Application workspaces are the containers for defining, analyzing and enforcing policies for a particular application. We will create a workspace for our tiered AWS cloud application in this step.

Click on 'Segmentation' and then click on 'Create New Workspace'. Give the workspace a name and select the Scope that we created in Step 2.

🦲 c	Sisco Tetratien	APPLICATIONS						•	Monitoring • ⑦ •
<u>س</u>	APPLICATIONS	Overview						<table-cell> Ge</table-cell>	t Started
สั ภ	Enforced App	lications	1	Enforcement Agents	8		2/8	1.	Create Filter
2					-			2.	Add Policy
7	Workspaces	√- Analyzed Policies	Enforced Policies	Policy Requests				3.	Start Analysis
2	1 Workspace	Q, Filter application worksp	baces			Sort -	Create New Workspace	4.	Enable Enforcement
>	Safe3tierApp					iAFE_CLOUD : AWS	PRIMARY ENFORCED		
	230 Conversations	2 Clusters	34 Policies				Last updated: Jan 7, 5:55 PM	X Too	ala
								Ð	Enforcement History
								⊳	Default ADM Run Config

At this point, we have successfully built the inventory, created a scope and defined a workspace for our tiered cloud application.

Test Case 2: Using ADM to discover the policies for AWS workloads and setting up an app view

This test case validates the use of 'ADM' to automatically discover the policies based on flow and other data received from workloads. We will refine the discovered workload clusters and update the inventory filters to eventually come up with a set of policies that can be enforced on our cloud workloads.

Validation procedure:

- Step 1. Discover policies using ADM
- Step 2. Refine inventory filters, clusters and policies
- Step 3. Create the App View
- **Step 1. Discover policies using ADM -** Before running the ADM, ensure that all types of traffic flows are generated in the application environment. This would provide ADM the required data to generate an accurate policy set and hence ensure that we don't miss any critical but less common traffic flows.

Go to the newly created workspace and click on 'Start ADM Run' on the top right corner, select a suitable time range to ensure that you cover all the traffic flows.



Step 2. Refine inventory filters, clusters and policies – Post the ADM run, policies and clusters would be generated. At this point, we manually update and customize all the cluster queries and approve them.

2.1: Go to 'Clusters' tab, click on any of the clusters, the panel on the right-hand side will show the cluster details like name, description, cluster query, workloads, neighbors. Update name and description to make it more intuitive, update the cluster query if need be. For example, we updated the cluster query for auto scaled workloads. We used previously defined annotation to dynamically identify the workloads in Auto Scaling groups for the web and application servers.

	Cisco Tetratien APPLICATIONS											
ш	A 2 the application dependence in AME aloud					Ĵ Switch Application						
ф	n a see again.com/compressions/compre											
Ð	0 D Conversations 200 & Clusters 6 z# Policies 34 N Provided Services at App View 1 🖓 Policy Analysis D Enforcement 📼 🕁											
۵	Clusters 🗇				Q (I)							
Δ	Filters I Filter Clusters			E Create Cluster	Gluster: Web S	ervers						
¢	Displaying 6 of 6 clusters				Cluster Actions	090						
÷	Cluster - Workloads	Confidence	Dynamic	≎ Approved ≎	Name	Web Servers 2						
	API Gateway 1	N/A	~		Description	Web Servers 🖉						
0					View Cluster De	stails						
	API Server 1	N/A	~		Query	* orchestrator_aws:autoscaling:groupName = ScaleWebServers						
	AppLB 2	N/A	\checkmark		Edit Cluster Qu	ery (4)						
	Application Servers 2	N/A	~			Workloads (2)						
	NetworkLB 2	N/A	~		10.0.2.117	ip-10-0-2-117 CentOS 7.6						
					10.0.3.85	ip-10-0-3-85 CentOS 7.6						
	Web Servers 2	N/A	*			Neighbors (3)						

2.2: Click on 'Policies' tab, review the policies keeping the workload flows in mind. We considered the following flows for policies:

- · User requests incoming to Web Servers via Application Load Balancer
- Traffic between the workloads
 - · Web Servers to Network Load Balancer
 - Network Load Balancer to App Servers
 - App Servers to RDS Database instance
- Management tier to all the workloads
- Outbound internet access from all the workloads for updates/patches, DNS, DHCP, NTP



Step 3. Create the App View – Go to 'App view' tab and click on 'Create New App View'. Pin the workloads on the right-hand side panel to include them in your diagram. Double click on each pinned cluster on the view to automatically draw the traffic flows.



Test Case 3: Enforcing the policies on workloads.

This test case focuses on enforcing the policy set that we formulated in Test Case 2. We will publish the policies and verify if those are enforced as expected.

Validation procedure:

- **Step 1.** Publish the policies
- Step 2. Verify policy enforcement on workloads
- **Step 1. Publish the policies –** Select the 'Enforcement' tab on the Tetration portal within the application workspace and click on 'Enforce Policies'.



Step 2. Verify policy enforcement on workloads - Since we had CentOS based workloads, we monitored the '/usr/local/tet/log/tet-enforcer.log' to see if policies are successfully enforced. A simple ping or telnet test can also be used to verify the lockdown of ports and protocols.

I0107 04:25:25.275367 I0107 04:25:25.275394 I0107 04:25:25 275499	468 agent_controller.cpp:426] IPC is ready, start writing the message to IPC 468 agent_controller.cpp:445] Done writing to shared memory million and include a start processing
10101 011251251215155	Password - MSkingpage [gr25]
10107 04:26:25.216424	468 ssl_client.cpp:410] Received message body length: 12
	Linux Academy.
T0107 04:26:30.277519	468 ssl client.com:5101 Callina callback in to process maximum client.com
10107 04:26:30.277545	468 agent_controller.cpr:179] Start message processing from EFE
10107 04:26:30.277563	468 agent_controller.cpp:222] Write the protobuf to AgentEnforcer international and an and a second se
10107 04:26:30.277696	472 agent_enforcer.cpp:966] Process EFE Message Lisemanne amonsinillectica com
10107 04:27:05.342911	4/3 ggent_enforce.cpp:1263] Received Policy contrig Version: 1549811605 = 002005
10107 04:27:05.344187	473 agent_entrer, top: 13961 Storing the policy and enforcing
10107 04:27:05.344703	473 firewall_context.cpp:140] Policy has been validated, applying the policy
10107 04:27:05.344712	473 firewall_context.cpp:169] Applying all firewall rules to the system firewall
10107 04:27:05.714491	473 iptables_context.cpp:529] Staged rules have been committed
10107 04:27:05.726775	4/3 dgent_enforcer.cpp:1403j Policy config has been applied successfully, current version: 1545811665, highest version: 1545811665

Use the CLI command 'ipset list' to view the ipset firewall settings enforced by Tetration agent on the CentOS workloads.

Nome: to.520a2f879b4e9ab37a6e620e928b Type: hash:net879b4e9ab37a6e620e928b Revision: 6 Header: family inter hashsize 1024 maxelem 65536 Size in memory: 504 References: 2 Number of entries: 2 Members: 10:0.3.196	
Name: ta_58225b8365be52f7b49f8254d96e Type: hash:net Revision: family inet hashsize 1024 maxelem 65536 Size in memory: 440 References: 30 Number of entries: 1 Members: 10.0.2.16	
Nome: to_9c21cc33b4bedbed655487444413 Revision: i6 Header: family inte hashsize 1024 maxelem 65536 Size in memory: 504 References: 6 Number of entries: 2 Members: 10: 0.5.129	
Nome: to_bdfode36735d84cc7cc983454o94 Type: hosh:net36735d84cc7cc983454o94 Revision: 6 Header: fomily intel hashsize 1024 maxelem 65536 Size in memory: 504 Reference: 8 Number of entries: 2 Members: 10:0.9.233 10:0.9.243	

Test Case 4: Discovering the vulnerable packages on the AWS workloads.

This test case looks for vulnerable packages/software installed on various workloads in the AWS. We identify a vulnerable package/software on our workloads, patch those and then rerun the report.

Validation procedure:

- Step 1. Check the vulnerability report
- Step 2. Fix a vulnerability and rerun the report
- Step 1. Check the vulnerability report Go to 'Security > Vulnerabilities', click on 'Packages' tab to see all the vulnerable packages installed on various workloads in our three-tier application. For the sake of this test, let's consider 'libcurl-7.29.0-51.e17' as shown below.

		Package Details - libcurl-7.29.0-5	1.el7			AWS-US-EAST •	⁹ Monitoring ≁ ③ ∗ ⊜ _e ∘
ш гћ ©	CVSS V2 DISTRIBUTION - INTGSSOPOV : SAFE, C	Package: libcuri-7.29.0-51.el7 CVEs: CVE-2018-14618 (v2: 10, v3: 9.8), CVE-2018-14618 (v2: 10, v2: 9.8), CVE-2018-14618 (v2: 9.8),	2017-8817 (v2: 7.5, v3: 9.	8), CVE-2016-5421 (v2: 7.5, v3: 9.8), CVE-2016-6622 (v2: 7.5	v3:)	
۵ ۲ ۵		5.6, CVE-2014-3620 (vč. 5, vš. NA), CVE-201 7.5), CVE-2014-3620 (vč. 5, vš. NA), CVE-201 N/A), CVE-2014-2522 (vč. 4, vš. N/A), CVE-201 Affected workleads: ip-10-0-2-117, ip-10-0-2-	9-5436 (v2: 5, v3: N/A), 9-5436 (v2: 4, 6, v3: 7.8), 0 3-6422 (v2: 4, v3: N/A) -4, ip-10-0-3-85, ip-10-0-	VVE-2017-1000204 (v2. s, v3. r.3), VVE-20101 141 (v2. s, v6 VVE-2017-1000100 (v2: 4.3, v3: 6.5), CVE-2013-4545 (v2: 4.3 4-212, (p-10-0-6-110 XVallaDity Impact	v3:	Impact	Authentication
0 19	245 Remotely Exploitable Low Complexity	206 Remotely Exploitable Higher Complexity	436 Locaty Exploitable Low Complexity			99 Locally Exploitable Higher Complexity	
	O Critical Severity	300 High Severity	eventy 548 Medium Seventy			138 Low Severity	
	CVEs Packages Workloads						
	V Package		Worst Score (V2)	•	Worst Score (V	3)	
	linux_kemel-3.10.0-957.1.3.el7.x86_64		10		9.8		
	linux_kernel-3.10.0-693.el7.x86_64	10 9.8			9.8		
	linux_kernel-3.10.0-1062.9.1.el7.x86_64		10		9.8		
	libcurt-7.29.0-51.ef7		10 9.8				

We see that the workload 'ip-10-0-2-4' is affected by this CVE. Logon to this workload and verify the libcurl package.



Step 2. Fix the vulnerability and rerun the report – We update the libcurl package from this workload to the latest version which has the fix to the CVEs listed in step.



Wait for a few minutes after the uninstall, go back to Tetration portal and check the vulnerability report again. We can see that none of the CVEs related to libcurl show up anymore.

2	Cisco Tetrat		ROFILE									AWS-US-	-EAST - 🛞 Monitoring -	? •	\$° +
ы	Summary	Long Lived Processes	Process Snapshot	Interfaces	Packages	Vulnerabilities	Config	Stats	Policies	Container Policies	Network Anomalies	File Hashes	Visit History		
å	IP-10-0-2-4														
۲	Filters @	Package Name contains	libcurl			8	Filter								
۵	Displaying 0 of	858													
₫															
¢						.11.11.	TetrationUS Sc Privacy and Te TAC Support: I	ottware, Version 3.3 irms of Use http://www.cisco.co	22-PATCH-3.3.2.10	(1885)					
¢						cisco	© 2015-2020 (Cisco Systems, Inc.	All rights reserved.						
ß															

Advanced Malware Protection for Endpoints

Test Case: Quarantine a suspicious file

This test case involves the detection of using AMP for endpoint 'simple custom detections' to quarantine a suspicious PDF file.

Validation procedure:

- Step 1. Setting up AMP4E policy to quarantine a suspicious file
- Step 2. Verifying the deletion of a suspicious file
- **Step 3.** Setting up AMP4E policy to quarantine a suspicious file For the validation purpose, we consider a 1 MB PDF file that we will block list using AMP 'Simple Custom Detections'. We will then try to download the same PDF file on a cloud workload and assert that our policy works as expected.

As per our initial AMP4E set up, we had configured the group 'Secure Cloud' (Management > Groups) for our workloads in the AWS cloud.

CISCO AMP for En	dpoints (Advantage)					? Ama	ndeep Singh $^{\checkmark}$
Dashboard Analysis ~ Outbr	eak Control V Management V Ad	ccounts \vee		Search			Q
< Edit Group: Secure Cloud							
Name	Secure Cloud			Computers			
Description	Cloud workloads			8 direct members	app.lab		
Parent Group		\$		∆ ip-10-0-3-18.mysa	afeapp.ne	et	
Windows Policy	Default Policy (Protect Policy)	\$		 △ ip-10-0-4-199.safe △ ip-10-0-5-169.mys 	eapp.lab safeapp.r	net	
Android Policy	Default FireAMP Android	\$		 webscales000000 webscales000001 	 ∆ webscales000000 ∆ webscales000001 		
Mac Policy	Protect Policy for FireAMP Mac	\$		No child members			
Linux Policy	CloudApp-LinuxPolicy			Assign computers to groups on the Computers page			mputers page
iOS Policy	Protect 🗘						
	Cancel	Save					
Child Groups			Add Child Group	os			
SORT <	Select All Dese	elect All	SORT ^ ~	Search		Select All	Deselect All
			DMZ Shared Serv Domain Controller Industrial Worksta Orbital Group Protect Secure Campus Secure DC Server Triage	rices r ittions			
	Remove Selec	cted >	< Add Selecte	d			

Note: During our implementation phase we had used the AMP4E agent tied to this specific group 'Secure Cloud', which we had created as part of the initial AMP4E set up (not elaborated in this guide, follow

AMP4E documentation for detailed steps on setting up AMP4E policies). All the workloads in AWS VPC register with AMP Cloud under this specific group.

It can be seen in the snapshot above that we tied the specific group to Linux policy 'CloudApp-LinuxPolicy'. Go to 'Management > Policies' and select the specific Linux policy.

CloudApp-LinuxPolicy Policy for linux workloads in Cloud					
Modes and Engines		Exclusions	Proxy	Groups	
Files Network ClamAV	Quarantine Audit On	Not Configured	Not Configured	Secure Cloud	
Outbreak Control					
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network	
CloudApp-CSD		Not Configured	Not Configured	Not Configured	
③ View Changes Modified 2020-05-27 17:12:00 UTC Serial Number 237					

Note: We had preconfigured the Linux policy associated with AMP4E group 'Secure Cloud'. We also tied a new Simple Custom Detection 'CloudApp-CSD' to the Linux policy. If there was no initial config on AMP console, then you would see default policies here.

As we see in the snapshot, the Linux policy above is tied to Simple Custom Detections 'CloudApp-CSD' (Outbreak Control > Simple).

Go to 'Outbreak Control > Simple Custom Detections' and click on edit 'CloudApp-CSD' to upload the PDF file that we want to block list in the AWS cloud environment. Uploading the PDF file will add the SHA value to the SCD policy and quarantines the file associated with it from all the cloud workloads registered under the specific group.

Analysis V Outbreak Control V Management V Accounts	Search C
Custom Detections - Simple	() View All Chang
	Create CloudApp-CSD Update Name
IoT Demo Created by Andrew Mcphee • 2020-05-21	Add SHA-256 Upload File Upload Set of SHA-256s
Used in policies: 🗱 Industrial Workstation Policy Used in groups: Industrial Workstations	Upload a file to be added to your list (20 MB limit)
() View Changes	File file-example_PDF_1MB.p Browse
CloudApp-CSD 8 files Created by Amandeep Singh • 2020-01-10 Used in policies: A CloudApp-LinuxPolicy Used in groups: Secure Cloud	17:09:46 UTC Note 17:09:46 UTC
() View Changes	Files included
Quick SCD 0 files Created by Bart McGlothin - 2016-05-27 Used in policies: Audit Policy, Audit Policy for FireAMP Linux, Audit Policy Mac, Controller Policy, Controller Policy, Controller Policy, Protect Policy, Protect Policy, Protect Policy, Triage Pol Policy for FireAMP Mac Used in groups: Audit, Domain Controller, Orbital Group, Protect, Secure Cloud, S Server, Triage	03:37:38 UTC 90fb3386b4868558 620c375e2475043a 620c375eb4868558 620c375eb4868558
() View Changes	Delete Added by Amandeep Singh • 2020-05-27 17:16:15 UTC
	Delete
	a882c4021222e2bf
	acd3385d18847584
	f 4db09b6fc2c029b
	1612e6edacec1f98
	a10056967cdc9137

Step 4. Verify the deletion of the suspicious program – Log on to a cloud workload, we picked one of the web servers in Web Auto Scaling Group. We downloaded the PDF file that we block listed above. We can see that the file is immediately quarantined by the AMP agent on the workload.

<pre>[centosHwebscales000000 -]\$ mget https://file-examples.com/mp-content/uploads/2017/10/file-example_DPF_106.pdf ~2020-05-27 19:46:43- https://file-examples.com/mp-content/uploads/2017/10/file-example_DPF_106.pdf Resolving file-examples.com (file-examples.com) 1185.138.88.81:443 connected. HTP request second.com/mp-comples.com) 1185.138.88.81:443 connected. HTP request second.com/mp-content/uploads/2017/10/file-example_DPF_106.pdf Length: 1042157 (10180) (opplication/pdf) Soving to: 'file-example_CPF_UB.pdf'</pre>				
1001	>] 1,042,157	1.43MB/s	in 0.7s	
2828-85-27 13:46:42 (1.43 MB/s) - 'file-example_P0F_1MB.pdf' saved [1842157/1842157]				
[CentosMediscal es080000 _]5 [CentosMediscal es080000 _]5 ls -lh [CentosMediscal es080000 _]5 ls -lh [CentosMediscal es080000 _]5 ls -lh [CentosMediscal es080000 _]5 ls -lh [CentosMediscal es08000 _]5 ls -lh [CentosMediscal es08000 _]5 ls -lh [CentosMediscal es080000 _]5 ls -lh [CentosMediscal es080000 _]5 ls -lh				

We also confirm the quarantine event from the event logs on the AMP Cloud portal. Log on to the AMP Cloud portal and go to 'Analysis > Event', we see a 'Quarantine successful' event post our steps above.

▼ webscales0000	000 detected file-example_PDF_1MB.pdf as	Simple_Custom_Detection	Medium	2020-05-27 17:17:19 UTC
File Detection	Detection	T Simple_Custom_Detection		
Connector Info	Fingerprint (SHA-256)	▼ 5e4d40fcbb4be37a		
Comments	File Name	T file-example_PDF_1MB.pdf		
	File Path	/home/centos/file-example_PDF_1MB.pdf		
	File Size	1017.73 KB		
	Parent Fingerprint (SHA-256)	T 782bed6a5f896bd2		
	Parent Filename	▼ wget		
	Report _25 1	le 🛓 All Computers	Add to Allowed A	pplications

Stealthwatch Cloud

Test Case: Monitor suspicious activity

This test case involves using the Stealthwatch cloud to monitor the activity within the AWS cloud environment.

Validation procedure:

- Step 1. Monitor suspicious activity in Stealthwatch Cloud
- **Step 1. Monitor suspicious activity in Stealthwatch Cloud -** Login to the Stealthwatch cloud portal. Go to 'alerts', we see the alert 'Excessive Access Attempts' as shown below. This alert indicated that there were numerous attempts to get SSH access from an unexpected geo location, which is a suspicious behavior.

CISCO Stealthwatch Clou	Dashboard V Alerts 🔕 Observations Models V		Q 0 🚹 🌣 🛔			
	lerts	0.				
	Search Q	Status - Tags - Assignee - Sort -				
	9 open alerts sorted by newest					
	Excessive Access Attempts (External) I-032dc6c1e859be077 #299	2 hours ago Q 44				
	Excessive Access Attempts (External) -031bb97/c8as5s9b1 #298					
	Excessive Access Attempts (External) ScaleWebServers i=0fa81682fd2ca2dfb, i=01 #364	b15f0e2c9d254f9 6 hours ago				
	Excessive Access Attempts (External) i-09e0d2badc2cf3a1c #496	11 hours ago \$ 26				
	Inbound Port Scanner Network #331 Excessive Access Attempts (External) I-0b071afe7f70b7134 #397					
	Permissive AWS Security Group Created (Amazon Web Services) 904585389016(answami #727					
	Geographically Unusual Remote Access ScaleWebServers i-0fa81682fd2ca2dfb, i-0 #695	1 week, 4 days ago				
	Geographically Unusual Remote Access I-031bb97fc8aa5a9b1 #530	2 weeks, 4 days ago				
	≛ CSV	First Previous 1 Next Last				
	Access Attempts (Extern	nal) 🗸			ScaleWebServe	ers
---	--	---	--	--	---	-----
Sta	tus Open					
	ID 364					
Descript	tion Device has many failed access a trigger this alert. The alert uses	attempts from an exte the Multiple Access F	rnal device. For example ailures observation and	e, a remote device trying repeatedly to acce may indicate the device is compromised.	ess an internal server using SSH or Telnet v	vou
Upda	ted May 27, 2020 12:00:00 PM					
Crea	ted Apr 29, 2020 8:00:00 AM					
	IPs at the time of alert: 10.0.3.	18, 10.0.2.34, 18.234	4.175.79			
	Hostname at the time of alert:	i-Ofa81682fd2ca2dfb	o, i-01b15f0e2c9d254f9			
Assig	nee 🛔 Nobody 🗸					
Tag	S *					
	After reviewing an alert, clo	osing it will let the rest	t of your team know it's	been resolved. In addition, closing alerts se	nds important feedback.	×
Supporting Ob Vultiple Access I Device had multiple 20 record	 After reviewing an alert, close Alert Close Alert Servations Failures Observation (a.g., FTP, SSH, Ids per page 	osing it will let the rest	t of your team know it's	been resolved. In addition, closing alerts se	nds Important feedback.	×
Supporting Ob Multiple Access I Device had multiple 20 record Time -	 After reviewing an alert, close Alert Close Alert Servations Failures Observation a failed application (e.g., FTP, SSH, India per page Device \$ 	RDP) access attemp	t of your team know it's ts. Profile ≑	been resolved. In addition, closing alerts se	nds Important feedback. search Failed Attempts \$	×
Supporting Ob: Multiple Access i Device had multiple 20 record Time - 5/27/20 12:00 PM	 After reviewing an alert, close Alert Close Alert Servations Failures Observation • a failed application (e.g., FTP, SSH, Ids per page Device • ScaleWebServers • 	RDP) access attemp Port \$ 22 (ssh)	t of your team know it's ts. Profile ≑ SSHServer	been resolved. In addition, closing alerts se Connected Device ≎ 218.59.234.3 ▼	nds Important feedback. search Failed Attempts \$ 93	×
Supporting Ob: Multiple Access Device had multiple 20 record Time - 5/27/20 12:00 PM 5/26/20 10:00 PM	 After reviewing an alert, clear control of the servations Failures Observation I and application (e.g., FTP, SSH, I de par page Device I and application (e.g., FTP, SSH, I de par page ScaleWebServers I and a server s	RDP) access attemp Port \$ 22 (ssh) 22 (ssh)	t of your team know it's tts. Profile \$ SSHServer SSHServer	Connected Device ◆ ■ 218.59.234.3 ▼ ■ 37.49.226.64 ▼	nds Important feedback. search Failed Attempts \$ 93 73	×
Supporting Ob: //ultiple Access //ultiple Access /// record Time - 5/27/20 12:00 PM 5/26/20 10:00 PM 5/26/20 3:00 PM	 After reviewing an alert, close Alert Close Alert Servations Failures Observation (e.g., FTP, SSH, Ids per page Device (e.g., FTP, SSH, Ids per page) ScaleWebServers (e.g., Ids ScaleWebServers) ScaleWebServers (e.g., Ids ScaleWebServers) ScaleWebServers (e.g., Ids ScaleWebServers) 	RDP) access attemp Port \$ 22 (ssh) 22 (ssh) 22 (ssh)	t of your team know it's ts. Profile \$ SSHServer SSHServer SSHServer	Connected Device \$ Image: 218.59.234.3 * Image: 37.49.226.64 * Image: 37.49.226.157 *	nds Important feedback. search Failed Attempts + 93 73 64	×

Cisco Umbrella

Test Case: DNS security

This test case involves adding DNS layer security to the AWS workloads. We created a DNS policy for our tiered application workloads to block malicious domains. To verify the blocks, we accessed a test domain 'examplemalwaredomain.com' and then confirmed the same from Umbrella reporting.

Validation procedure:

- Step 1. Set up DNS policy for AWS workloads
- Step 2. Confirm if malware domain is blocked
- **Step 1.** Set up DNS policy for AWS workloads Go to 'Policies > Management > DNS Policies', add a new policy and make sure 'Malware' is set to block under security settings. Save the change.

Cisco Umbrella	Policies / Management DNS Policies •	d Test
Deployments >	Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed,	
Policies ~	Policies are entorced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in t order you'd like. More policy inforca the bround in this article.	the
Management		
DNS Policies	r veuor	ESTER
Firewall Policy	Sorted by Order of Enforcement	
Web Policies	AWS_WorkloadsPolicy Protection Applied To Contains Last Modified DNS Policy 1 Identity 2 Policy Settings Jan 13, 2020	
Destination Lists		
Content Categories	Policy Name AVS WorkstandsPolicy	
Application Settings		
Security Settings	1 Simo 2 Sectionation Lats Enforced	
Block Page Appearance	Edit Identity T Ables Lat Edit Identity Edit	
Integrations	Commend and Control Collegians, Markey, Marking Attacks, plus 3 (T) File Analysis Not Enabled	
Selective Decryption Lists	more will be blacked to black	
Reporting >	Umbrella Default Block Page Applied	
Admin >	Content Setting Applied: High Bocks adaptice: High Bocks a	
Investigate	Edit Disable	
Amandeep Singh > CVD Team - Security Architecture	U No Application Settings Applied Enable	
	Advanced Settings	
Documentation Support Platform	DELETE POLICY CANCEL EAVE	
Learning Center		

Cisco Umbrella	1 AWS_WorkloadsPolicy	Protection DNS Policy	Applied To 1 Identity	Contains 2 Policy Settings	Last Modified Jan 13, 2020	^
Overview						
Deployments >	Security Settings					
Policies 🗸	Ensure identities using this policy ar	re protected by selecting or cr	ating a security setting	g. Click Edit Setting to mak	e changes to any exist	ing
Management	settings, or select Add New Setting	from the dropdown menu.				
DNS Policies	Select Setting	*				
Firewall Policy	reationingury					
Web Policies	Categories To Block					
Policy Components	Malware Websites and other servers the	at host malicious software, drive-	by downloads/exploits,	mobile threats and more.		
Destination Lists	Newly Seen Domains					
Content Categories	Domains that have become activity	tive very recently. These are ofte	n used in new attacks.			
Application Settings	Command and Control Callbac Prevent compromised devices	cks From communicating with attack	ers' infrastructure.			
Security Settings	Phishing Attacks					
Block Page Appearance	Fraudulent websites that aim to	o trick users into handing over pe	rsonal or financial inform	hation.		
Integrations	Dynamic DNS Block sites that are hosting dyn	namic DNS content.				
Selective Decryption Lists Reporting	Potentially Harmful Domains Domains that exhibit suspicious	is behavior and may be part of ar	attack.			
Admin >	DNS Tunneling VPN VPN services that allow users I regarding access and data tran	to disguise their traffic by tunneli nsfer.	ng it through the DNS pr	otocol. These can be used t	o bypass corporate polici	ies
Amandeep Singh Cv/D Team - Security Architecture	Cryptomining Cryptomining allows organizati	ions to control cryptominer acces	s to mining pools and w	eb miners.	CANCEL	SAVE

Step 2. Confirm if malware domain is blocked – Run 'nslookup' on a test malware domain as shown in snapshot below. Utility returns Umbrella block page IP address as below.



To further confirm the block action, select 'Reporting > Activity Search' and filter the accessed malware domain. Events show the action as 'Blocked'.

Cisco Umbrella			Reporting / Core Report	0										
Overview	0	cisco	Activity Sea	irch								🛱 JAN	12 - JAN 13 • (+) Downlos	d Schedule
Deployments >														
Policies >		0	Q, Search request acti	vity		Advanced -	CLEAR					Columns	Domain Requests (DM	IS) 🔻
Reporting >														
Core Reports			1 DOWNN O Reampena	waredomain.co	om 🗙									
Activity Search		FILTER BY:		Q	Viewing activity fro	om Jan 12, 2020 at 2:	04 PM to Jan 13	2020 at 2:04 PM			Page: 1	 Results per page: 	50 - 1 - 18 of 18	
Admin >		Response	,	Select All				Identity Used by Policy						
Investigate			wed ked		Identity	Destination		0	Internal IP	External IP	Action	Categories Application	Date & Time ∨	
Amandeep Singh CillD Taxes - Security Architecture		🗆 😑 Prax	ied		Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Blocked	Malware	Jan 13, 2020 at 2:03 PM	Θ
ovo reant- occurry prenactore		Event Tvn	10	Colored All	Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Blocked	Malware	Jan 13, 2020 at 1:48 PM	Θ
			plication	Select All	Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Blocked	Malware	Jan 13, 2020 at 1:29 PM	Θ
Documentation		Cor So Cor	ntent Category		Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Blocked	Malware	Jan 13, 2020 at 1:29 PM	Θ
Learning Center			itination List		Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Blocked	Malware	Jan 13, 2020 at 1:29 PM	Θ
Privacy Policy		 Im Sec 	curity Category		Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Blocked	Malware	Jan 13, 2020 at 1:29 PM	Θ
Terms Of Service					Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Allowed	Malware	Jan 13, 2020 at 1:27 PM	Ξ
Cisco Systems		Identity T	уре	Select All	Default Site	examplemalwaredor	nain.com	Default Site	10.0.2.117	3.136.23.50	Allowed	Malware	Jan 13, 2020 at 1:27 PM	Θ

Cisco Defense Orchestrator

Test Case: Enforce Security Group policy using CDO

In this test case, we will try to lock down the outbound access for our cloud workloads for specific TCP ports. We will use CDO to manage the AWS Security Groups. We already onboarded the AWS VPC to the CDO in the implementation section of this document.

Validation procedure:

- Step 1. Configure and enforce the access policy
- Step 2. Verify the access block
- **Step 1. Configure and enforce the access policy** We log on to a Web Server workload and try to access a non-standard TCP port on a server on the Internet. We can see in the snapshot below that the Web Server workload is able to connect at this point.

sevent and the
os8webscales000000 ~]\$ telnet portquiz.net 666
g 52.47.209.216
cted to portquiz.net.
e character is '^]'.
ction closed by foreign host.
os@webscales000000 ~]\$
osilwebscales00000 ~]\$

We want to block outbound access to such random TCP ports from our Web workloads. Log on to the CDO portal and go to 'Policies > AWS VPC policies', we can see that the 'WebSG' policy allows the Web workloads to access any destination on any port on the Internet.

cisco Defense Orchestrator	AWS V	PC Policies / av	vs-vpc								€ - sat	Ie-architecture ansin3@cisco.com
Hide Menu	 Return to Pr 	olicies							>	webSG_inbo	und_2	
Devices & Services	Packet	s								Security Group Tag	,s	~
Configuration	т Ш	III Q Search						C		Name	webSG	
Policies >										Actions		
Objects	frontendSG									/ Edit		
	Direction	Name	Action	Source		Dest	lination (TOP or)			Remove		
	Inbound	frontendSG_inbound_1	1 Allon	N Pers	173.38.117.75/32		TOP22			Rule Details		~
욥 Migrations erra	Inbound	frontendSG_inbound_2	Allow	M SECURI GROUP	ITY app56	[POR	UDP:53			Remark		
Events & Monitoring	Inbound	frontendSG_inbound_3	i 🕀 Allos	N SECURI GROUP	TTY web5G	[POR	UDP:53			Allow SSH access		
↓ Monitoring ↓	Outbound	frontendSG_outbound,	,1 🖸 Allow	N Any		INET	S Any IPv4			Objects Used		~
Change Log	mgmtSG									⊕ Any IPv4		v
🖽 Jobs	Direction	Name	Action	Source		Destina	ation	_		@ TCP:22		~
	Inbound	mgmtSG_inbound_1	Allow	INETS	Any IPv4	[PORTS	TCP:3389			Resources		
	Outbound	mgmtSG_outbound_1	Allow			INETS	Any IPv4			Instances		
								_		Q Search for in		3 results
	Direction	Name	Action	Source		Destinat	tion	•		Name	ID	
	Inbound	webSG inbound 1	Allow	INETS G	Anv IPv4		TCP-80			WebServer	i-0e96f0f0f14	32febb
	Inhound	unblo ishound 2	CI Allow	inere G	And Date of the second s		T001			APIGateway	i-0ba038ce7b	9bdde56
	moound	websd_indound_2					IUPIZZ U			WebServer	i-09ac236ba4	id16e7ce
	Inbound	webSG_inbound_3	⊇ Allow	NETS	Juny IPv4		TCP:443					
	Inbound	webSG_inbound_4	Allow	INETS	Any IPv4		ICMP:ANY					
	Outbound	webSG_outbound_1	Allow			INETS	Any IPv4					
	Default Act	tion O Block										

cisco Defense Orchestrator	AWS VPC Policies / aws	s-vpc				Ð -	safe-architecture amansin3@cisco.com
E Hide Menu	 Return to Policies 	Edit Security Group Rule (webSG)		×	>	webSG_inbound_2	
Devices & Services	Packets → Security Groups	Name	Remark	Action		Security Group Tags	~
Configuration	T III Q Search	webSG_inbound_2	Allow SSH access	🔁 Allow 👻	C	Name webSG	
Policies	frontendSG					Actions	
Objects	Direction Name	Source	Destination	1 10/075		Edit Remove	
-å VPN →	Inbound frontendSG_inbound_1	173.38.117.75/32		TCP-22		Rule Datails	
Migrations ente	Inbound frontendSG_inbound_2					Remark	Ť
Events & Monitoring	Inbound frontendSG_inbound_3			Cancel Save		Allow SSH access	
√ Monitoring >	Outbound frontendSG_outbound_1	🔁 Allow Any	INETS Any IPv4			Objects Used	÷
Change Log	mgmtSG					⊕ Any IPv4	~
🖽 Jobs	Direction Name	Action Source	Destination			⊕ TCP:22	~

We update the policy to lock it down to just the HTTP and HTTPS ports going out to the internet. After making the policy change, click on the notification on the top right-hand side of the portal to push the changes to the specific FTD devices.

cisco Defense Orchestrator	aws-vpc / Pending Changes			0 -	safe-architecture amansin3@cisco.com
🗮 Hide Menu	🔶 Return to Devices & Serve	05			
Devices & Services	Legend: Removed A	Ided Edited	Cancel Discard All Deploy Now		
Configuration	1 change				
Policies >	Status: Pending Last	Deploy: - Changed by: anoncombine concord			
Objects	CHANGES	DEPLOYED VERSION	PENDING VERSION		
-& VPN >	L3 Access Rules	L3 Access Rules			
Migrations (113)		#1 webSG_inbound_2			
Events & Munitoring		Source Networks			
Monitoring →		name: 'Any IPv4' type: NETWORK_OBJECT	name: 173.38.117.75/32 type: NETWORK_OBJECT		
Change Log					
adol. (***					

Step 2. Verify the access block - Now that we have updated the policy, we will try and attempt to verify the access. We SSH to a web server again and try to access websites on a random TCP port 666. We can see the connection timing out or getting blocked now. We can also see that an outbound access to a server on the internet on standard HTTP and HTTPS is still allowed.

[CentosRwebscales000000 -]\$ [CentosRwebscales000000 -]\$ Trying 52.47.209.216 telnet: connect to address 52.47.209.216: Connection timed out [CentosRwebscales000000 -]\$		1
[centosAwebscales000000 -]\$ teinet www.cisco.com 443		
<pre>Import 23.195.186.186 Connected to www.isco.com. Escape character 16 * 3]. ACconnection closed by foreign host. [CentrolWhebscoles900000 - 3] CentrolWhebscoles900000 - 3] teinet www.cisco.com 80</pre>		
rying 23.150.100.150 Connected to www.cisco.com. Escape character is ^g`. /2/2 /2 Connection closed by foreign host.		

Radware Cloud WAF and DDoS Protection

Radware Cloud portal displays all the traffic statistics related to various onboarded applications. The dashboards are fully customizable based on the requirements.

Cisco-SafeArchitecture	✓ 🚮 Dashboard 🗍 Mor	nitor 🕼 Assets 📓 Account				Ę	4 0 🌒
Dashboard						All Applications during an hour	· ·
K WAF Summary					0 ×	1 DDoS Attack Status	© ×
O Events blocked	O Events/minute	O O O O O O O O O O O O O O O O O O O	rability Configurations events updates	n Applications		Peacetime	
Top Attacked Applications Period 7 days	©××	Application Attack Distribution Period 7 days	⊘ ∺ × SApplic Period 7 day	tion Security Events	©X×	DDoS Protected Traffic Period 7 days	©x×
CiscoSafeApp 2xy-vulnerable (0	9.658	Beported	AR AR AR AR AR AR AR AR AR AR	0 11 Feb 1900 13 Feb 7000 14 Feb 1900	17 Feb 7.00	0 20 20 20 20 20 20 20 20 20 20 20 20 20	17 Feb 7:00
	No. of Attacks			📕 Critical 📕 High 📕 Warning 📕 Low 📗 Info	· [Attack 🧧 Clean	
OWASP Top 10 Mapping Period 7 days	©¤×	Top Application Attacked Hosts Period 7 days	Top Ag Period: 7 day	plication Attack Sources	©××	Top DDoS Attacked Destinations Period: 7 days	⊙××
A A A A A A A A A A A A A A A A A A A)	204.33.133.142 clocossilospp.com 7923/beie400096-fue/82.beiet. 166 1220.0.0 129 r/ds 123	4.53Y 1055-53 4.53Y 1083-53 1083-53 083052 083052	226	2.4K	No available data	

Test Case: Monitor Web and DDoS activity on Radware Cloud.

This test case involves monitoring the security events generated in the Radware Cloud portal.

Validation procedure:

- **Step 1.** Monitor Web and DDoS activity on Radware Cloud WAF and DDoS Portal.
- Step 1. Monitor Web activity and DDoS activity on Radware Cloud On the Radware Cloud portal, go to Monitor > Security Events to see all the WAF and DDOS events generated from any malicious activity targeting your application.

0000	Cisco-Sa	afeArchitecture 🧹 🛍 🗆	Dashboard 🛛 🗍 M	1onitor 🔅 Assets	칠 Accour	nt						\$?	- 🌔 -
Se	curity	Events WAF	DDoS	Sort by Time	▼ ↑↓	25 per page	•	4 4	Page 1	•	► ►	S	sv -0-
	Action	Last week	🛆 Destination		& Source	showing 1-25 ou	it of IU	000 ever Seci	urity			١	lore
	Reported 0	19 Feb 2020 18: 16: 28	CiscoSafeApp n/a	Cisco-SafeArchitecture	66.249.66.84	ites of America -	- US	IPBlock Access	from Unauthor	ized sour	ce IP		Θ
	Reported 84349982	19 Feb 2020 17: 40: 35	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Feo	deration - RU	0	Vulner Remote	abilities File Inclusion				Θ
	Reported 84349982	19 Feb 2020 17: 40: 35	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Feo	deration - RU	0	Allowe URL Ac	d File Extension	n			\odot
	Reported 84362548	19 Feb 2020 17: 38: 28	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Feo	deration - RU	0	Vulner Evasion	abilities				\odot
	Reported 84362548	19 Feb 2020 17: 38: 28	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Feo	deration - RU	0	Databa Code In	se jection				\odot

Radware's Application Analytics combines a large number of similar events and consolidating them into small, manageable sets of recurring activities. This helps to streamline response by providing additional context to security events needing attention.

1	🗸 🙆 Deshboard	Gecunty Events	Settings 🔝 Service Ov	erview .	æ 🔺 🄇	D - 1		
Security Eve	nts war cous			Stort by Time (* 11) 25 per pag	e e ins faget in an O	284		
S Action	Latt week	CS Destination	A South	C Security	More			
Reported 2567721508	26 Aug 2018 18:02:33		45,248,7775	Allowed File Extension URL Access Violation				
Reported 2544000200	26 Aug 2018 18: 01: 40		203.30.95.5 Auto	Allowed File Extension shit - AU URL Access Violation	Θ			
Haperted 2544888283	26 Aug 2018 18:00:56		203.30.95.5	E Allowed File Extension sits - AU UPL Access Volation	Θ			
Heported 21xx4000201	26 Aug 2018 17 53 19		85.02.06.146 668 Gente	Allowed File Extension Jimpdom - DB URL Assess Vehalism	Θ			
		1	∽ aấ Desh	poard 🕜 Security Events 🕼	Settings 🔛 Service Overview			8 🔺 💿
		Applicati	ion Insights		-	5. 10. W 24	Inserted Country	
			35	55 Events		13 Activi	ties	
		Allow List. Vur	relabilities Database					
		Mathod 11		Extension 11	Eventa 14		Trend	More
		087		*.angre	1821	55.47%		0
		1000		17	1659	46.84%	A	0
		GET						-

In addition, the integrated ERT Active Attacker Feed will help you identify if listed requests are legitimate or not by identifying known attackers. As Illustrated below, we are able to gain intelligence if the IP's attempting to access the phpMyAdmin pages are from known malicious IPs (with risk level assessments).





Allow List (20)	Vulnerabilities (49) Databas	ie (269)					8,449 E	vents 338	Activitie
Events Activities New Activities	2308 810 2 2 49 49 10 10 12 10 10 100		Indicate a legitimate trend for This page is used by WordPro	or public facing appli ess to automate som	cation. e tasks.	2 Mar 100 1	Mar 100 6 Mar 100		
Rule ID 11	Pattern 11	Details 1	First Seen 11	Sources 1)	Events 🔱		Trend		More
10700	md5(Evesion attempt via md5() function	2020/02/14 (21 days ago)	5	1,435	62.18%	\wedge	\wedge	\odot
9739	/wp-cron.php	An attempt to access a WordPress events scheduling script,	2020/02/17 (18 days ago)	2	396	17.16%	\sim		\odot
9238	/phpmyadmin	PHPMyAdmin Interface	2020/02/12 (23 days ago)	12	131	5.68%		\frown	Θ
9281	/admin/	Attempt to access administrative location	2020/02/14 (21 days ago)	12	46	1.99%	\sim		\odot
10756	/env	PHP frameworks sensetive file	2020/02/13 (22 days ago)	3	43	1.86%	\wedge		\odot
9687	/xmlrpc.php	Wordpress XML-RPC Pingback Attack.	2020/02/14 (21 days ago)	17	27	1.17%		~ ^	\odot
7762	index.php or func=&	PHP remote file inclusion vulnerability in FlashGameScript 1	2020/02/14 (21 days ago)	12	25	1.08%	M	~	\odot
9293	/mysql/	Attempt to access administrative location	2020/02/14 (21 days ago)	5	21	0.91%	\wedge		o
9300	/sal/	Attempt to access administrative location	2020/02/14 (20 days ago)	4	19	0.82%			0

Duo Beyond

Validation procedure overview:

- Test Case 1 Set up the cloud application for Two-Factor Authentication (2FA)
- Test Case 2 Monitor 2FA activity from Duo admin portal

Test Case 1: Set up the cloud application for Two-Factor Authentication (2FA)

This test case involves logging into the application for the first time and activating the duo plugin. Previously, during the implementation phase, we had already downloaded the plugin to application workloads using AWS User Data option. Follow the <u>Duo documentation</u> (skip step 2 under 'Install and Configure the Plugin') to activate WordPress Duo plugin. After activating the plugin, log out and log in again. This time Duo will prompt the user to enroll their phone for 2FA. After successful enrollment, user gets the ability to approve subsequent login attempts.

Validation procedure:

- Step 1. Set up Duo 2FA for a new user
- Step 2. Log onto the cloud application
- **Step 1.** Set up Duo 2FA for a new user After the initial plugin activation, the Duo MFA kicks in and since this is the first authentication attempt, the user is prompted to enroll for MFA.

What is this? If Need helic? Powered by Dus Security	Protect Your Cisco Systems Account Monodation enhances the security of your account by using a coceasing your account, even if they know your password. Operation and the providentity. This providentity and providentity on the providentity of the providentity on the providentity of the p	What type of device are you Mobile phone reconserved Mobile	ou adding?
altalta cisco	Enter your phone number United States 0	My Settings & Devices	16
nat is this? 다 ed help? wered by Duo Security	+1 Example: (201) 234-5678	What is this? cf Default Device: Android Nined html? When I log In: Automatically send this is Prevend by Due Becurity When I log In: Automatically send this is	device a Duo Push \$

Step 2. Log onto the cloud application - After the enrollment, we continue to log onto the application, this time the user is presented with Duo authentication methods instead of 'setup'. Once the user approves the authentication request, they are allowed to login.

	Ŭ	
	Choose an authentication metho	d
ahaha	Duo Push RECOMMENDED	Send Me a Push
cisco	Call Me	Call Me
<u>What is this?</u> 다 <u>Need help?</u>	Passcode	Enter a Passcode
Powered by Duo Security		

Test Case 2: Monitor 2FA activity from Duo admin portal

This test case involves monitoring the 2FA enrollment and login activity in the Duo admin portal.

Validation procedure:

- Step 1. Verify the 2FA enrolled devices
- Step 2. Track the user logins in authentication logs
- **Step 3.** Verify the 2FA enrolled devices Logon to the Duo admin portal and select '2FA Devices', the portal shows the list of enrolled devices along with other details like platform, hardware model and usernames.

Due	 Search for users, group 	ips, applications, or devices			1	Cisco Sys	stems) Amandeep Singh ~
Dashboard	Dashboard > Phones							
Device Insight	Dhanaa							
Policies	Phones							
Applications	Android					Expo	art ∽ Q	
Users	8.0	Device +	Platform A	Model A			Security Warnings	lleare 🔿
Groups	Tampered	Device		Model 🗸			Security warnings	Users 🗸
Endpoints	Tampered		Android 8.0.0			3.30.0	🐓 No warnings	admin, amansin3
2FA Devices	Unknown							
Phones	Screen Lock	Show 25 \$ phones	1-1 of 1 total					< 1 >
Hardware Tokens	Locked							
WebAuthn & U2F	Unknown							
Administrators	Disk Encryption							
Reports	Encrypted							
Settings	Unknown							
Billing	Biometrics							

Step 2. Track the user logins in authentication logs – Go to 'Dashboard > Authentication log', to track user 2FA login activity as shown in the snapshot below.

Due	 Search for users, groups 	, applications, or devic	es		c c	isco Systems		Amandeep Singh 🗸
Dashboard Device Insight Policies	Dashboard > Authentication I	∝ ion Log						Export ~
Applications	> Last 24 hours ¥ N	lo filters applied						
Groups Endpoints	6 Authentications Shown at every 15 minute	5.						
2FA Devices Administrators	2						- 1	
Reports Authentication Log Telephony Log	o 8PM	11PM	2AM	5AM Thu. Jan 16	BAM	11AM	2PM	5PM Thu. Jan 16
Administrator Actions Authentication Summary	Showing 1-6 of 6 items	i.						Showing 25 \$ rows
Denied Authentications Deployment Progress	Timestamp (UTC) 🗸	Result	User	Application	Access Device		Second Factor	
Policy Impact Settings	4:12 PM JAN 16, 2020	Granted User approved	admin	WordPress	Mac OS X 10.14.6		> Duo Push	
Billing	4:11 PM JAN 16, 2020	Granted User approved	admin	WordPress	Mac OS X 10.14.6		> Duo Push	

Cisco SecureX Threat Response

Test Case: Track Malicious Activity on threat response

In this test case, we track the life cycle of the malicious PDF that we quarantined using AMP4E in previous steps. We will use the same SHA value and see what threat response offers in terms of visibility in our environment.

Implementation procedure:

- Step 1. Investigate a malicious SHA value
- Step 2. Track the file trajectory
- **Step 1. Investigate a malicious SHA value –** Log on to the threat response portal and select 'Investigate'. Add the SHA value in provided space and click on 'Investigate'. Threat response pulls all the information about the associated file and what workloads the specific file had interacted with. Under the 'Observables' section, we can see that AMP4E detected this SHA

value as malicious based on our custom AMP policy, threat response displays the specific AMP4E policy name as well.

viluile cisco Threat Response Investigate Snapshots Incidents teo Intelligence Modules	(?) 🗱 Amandeep Singh 🕶
New Investigation Assign to Incident Snapshots *	Automatic Layout v
I Target → مُحْثُ 1 Observable → المُحَدُّ 1 Indicator → المُحَدُّ 0 Domains	I File Hash ✓ ■ 0 IP Addresses 0 URLs
Investigation 1 of 1 enrichments complete -	Sightings —
5e4d40fcd8b22453a5da2d32533b128f2565f3fc7a4d1647a93c86cdbb4be37a Investigate Clear Reset What can I search for?	My Environment Global 3 – Malicious – Malicious 6 Sightings in My Environment 1.5 – – – – Malicious – – Malicious – – Malicious – – Malicious – Liknose –
Relations Graph - Filters: Show All, Expanded + - Showing 8 nodes	Observables List View + -
File Name, file-example_p ✓ Sec ✓	SHA-256 Hash
File Name file-example_P > File Path file-example_P > File-Path file-example_P >	Module Observable Disposition Reason AMP for Endpoints SatA336: Se4d406 Malicious Added to the simple custom detections list CloudApp-CSD

Step 2. Track the file trajectory - Click on the 'SHA-256 Hash' shown in the Relations Graph. Expand the drop-down menu and click on 'File trajectory'.

Relations Graph · Filters: Show All, Expanded • · Showing 8 nodes	×*	Observables List View * -
SHA-256 Hash Sed40fcd8b22453a5da2d32533b128f25 Sed40fcd8b2245 Sed40fcd8b2245 Sed40fcd8b22453a5da2d32533b128f25 Sed40fcd8b2245 Sed40fcd8b245 Sed40fcd8	File Path pome/centos/f ∽ ath Of File Path Of	SHA-256 Hash
File Nat file-examp Remove SHA256 from custom detections 2 Relationships Tar 752	File Path /home/centos/t >	Module Observable Disposition Reason AMP for Endpoints Isstatus: Se4d40fc Malicious Added to the simple custom detections list CloudApp-CSD
Hile Name 782bed6 ✓	webscales000000 V	8

Clicking on 'File trajectory' should redirect you to AMP4E portal page which displays the trajectory of the malicious file on the specific workload. Clicking on a particular timestamp displays the related events. The event history shows all the events associated with the specific file.

Trajectory								
		May, 27 17:17			19:46			Parent
Secure Cloud	webscales000.	+ created A the file was	€ ⊕ copied ⊕ m s the source of t	Created by wget[common 782bed6a5f896bd2. Detected as Simple_Custo Path: /home/centos/file-ex At 2020-05-27 17:17:19	filename] m_Detection. kample_pdf_1 UTC	mb.pdf scanned (advanced/tetra convictio Green, the target was 	n 🕂 observ s deemed beni
Date ^	Computer	Group	Event	SHA-256	File	Pro	Disposition	
2020-05-27 17:17:19 UT	webscales000000	Secure Cloud	Created by	782bed6a5f896bd2	wget		Detected as Simple_Custom	_Detection
2020-05-27 19:46:42 UT	webscales000000	Secure Cloud	Created by	782bed6a5f896bd2	wget		Detected as Simple_Custom	_Detection

Appendix

Appendix A- AWS Security Groups with CDO

Cisco Defense Orchestrator (CDO) is used for management and policy orchestration. CDO provides one security policy, faster deployment, and smart configuration management. It eliminates the time-consuming complexity of managing policies not just across multiple FTDs and ASAs but also the AWS Security Groups. Cisco Defense Orchestrator helps to correct issues such as unused, duplicate, and inconsistent objects hence ensuring consistent policies for firewalls.

We can use CDO as a single pane to manage the AWS Security Groups, providing a centralized management solution across multiple AWS VPCs.



Appendix B- Acronyms Defined

- ALB Application Load Balancer
- AMP4E Advanced Malware Protection for Endpoints
- AVC Application Visibility and Control
- CDO Cisco Defense Orchestrator
- **CSD** Custom Simple Detection
- CVD Cisco Validated Design
- ERT Emergency Response Team
- FQDN Fully Qualified Domain Name
- IOC Indicators of Compromise
- MFA Multi-Factor Authentication
- PaaS Platform as a Service
- PIN Places in Network
- SaaS Software as a Service
- SWC Stealthwatch Cloud
- VA Virtual Appliance
- VPC Virtual Private Cloud
- 2FA Two Factor Authentication

Appendix C- AWS CloudFormation Template

The AWS CloudFormation template used for the validation testing is located on the <u>Cisco Security Validated</u> <u>Design GitHub</u>. This template can be used to automate the deployment of the networking components, database, application, and web servers. For more information on the full deployment using AWS CloudFormation, the readme in the GitHub repository goes over all the steps and how it works.

Appendix D- Software Versions

Product	Platform	Version	
Tetration	Software agent	3.3.2.35-enforcer	
AMP4E	Software agent	1.11.1.663	
Stealthwatch Cloud	Cloud Offering	SaaS	
Umbrella VAs	Appliance (EC2 Instance)	2.6.2	
CDO	Cloud Offering	SaaS	
Duo WordPress Plugin	Software Plugin	Version 2.5.5	
Radware Cloud	Cloud Offering	SaaS	
SecureX Threat Response	Cloud Offering	SaaS	
Workloads	Linux	CentOS 7.7	
RDS Database	MySQL database	mysql-5-7	
Cisco NGFWv	OS	6.6.1.90	

Appendix E- References

This section lists all the references.

- Cisco SAFE:
 <u>https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html</u>
- AWS Three Tier Architecture: <u>https://d0.awsstatic.com/whitepapers/aws-web-hosting-best-practices.pdf</u>
- Cisco Tetration:
 https://www.cisco.com/c/en/us/products/security/tetration/index.html
- Cisco Stealthwatch Cloud:
 https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html
- Cisco AMP for Endpoint:
 https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html
- Cisco Duo Beyond: <u>https://duo.com/docs/wordpress</u>
- Cisco Umbrella:
 <u>https://docs.umbrella.com/deployment-umbrella/docs/deploy-vas-in-amazon-web-services</u>
- Cisco Defense Orchestrator: <u>https://www.cisco.com/c/en/us/products/security/defense-orchestrator/index.html</u>

- Radware for AWS (WAF and DDoS):
 <u>https://www.radware.com/products/cloud-waf-service/</u>
- WordPress:
 <u>https://wordpress.org/download</u>
- NGINX: <u>https://www.nginx.com/resources/wiki/start/topics/recipes/wordpress/</u>
- AWS VPC: <u>https://aws.amazon.com/vpc</u>
- AWS Route Tables:
 https://docs.aws.amazon.com/vpc/latest/userguide/VPC Route Tables.html
- AWS Security Groups: <u>https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html</u>
- AWS RDS Database for MySQL:
 <u>https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_MySQL.html</u>
- AWS Auto Scale: <u>https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html</u>
- AWS EC2 Instances:
 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html
- AWS Elastic Load Balancing (Application and Network): <u>https://aws.amazon.com/elasticloadbalancing/</u>
- AWS S3: <u>https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html</u>
- Amazon Machine Image: <u>https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html</u>
- AWS Route 53: <u>https://aws.amazon.com/route53/features/</u>

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 https://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: https://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)