Secure Cloud for Azure (IaaS)

Design Guide

June 2021

Contents

Abstract

This design guide aligns with the Cisco® 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 the Azure cloud.

Scope

This document illustrates the design and security aspects of an application hosted in Azure Cloud. 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
- Azure Network Security Groups (NSG)
- Cisco Firepower Next-Generation Firewalls (NGFW)
- Cisco Adaptive Security Appliance (ASA)
- Cisco Defense Orchestrator (CDO)
- Azure Web Application Firewall (WAF) and DDOS prevention
- 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 Azure cloud components and services.

- Azure Virtual Network (VNET) and Subnets
- Azure Route Tables
- Azure Database for MySQL
- Azure Virtual Machine Scale Sets (VSS)
- Azure Virtual Machines
- Azure Internal Load balancer (Standard)
- Azure External Load balancer (Standard)
- Azure Storage Containers
- Azure Resource Manager (ARM) Templates
- Azure Private Links

- Azure Front Doors (AFD)

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 SAFE home page.

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 Azure public cloud.

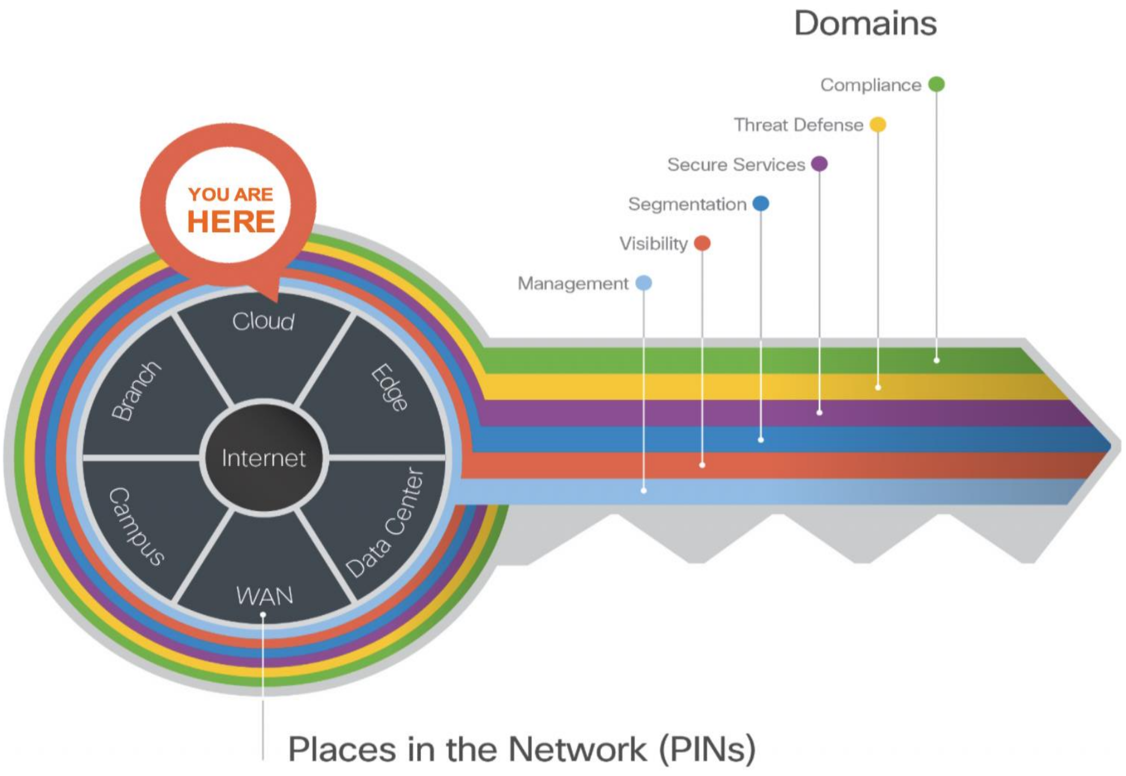


Figure 1.
Key to SAFE framework

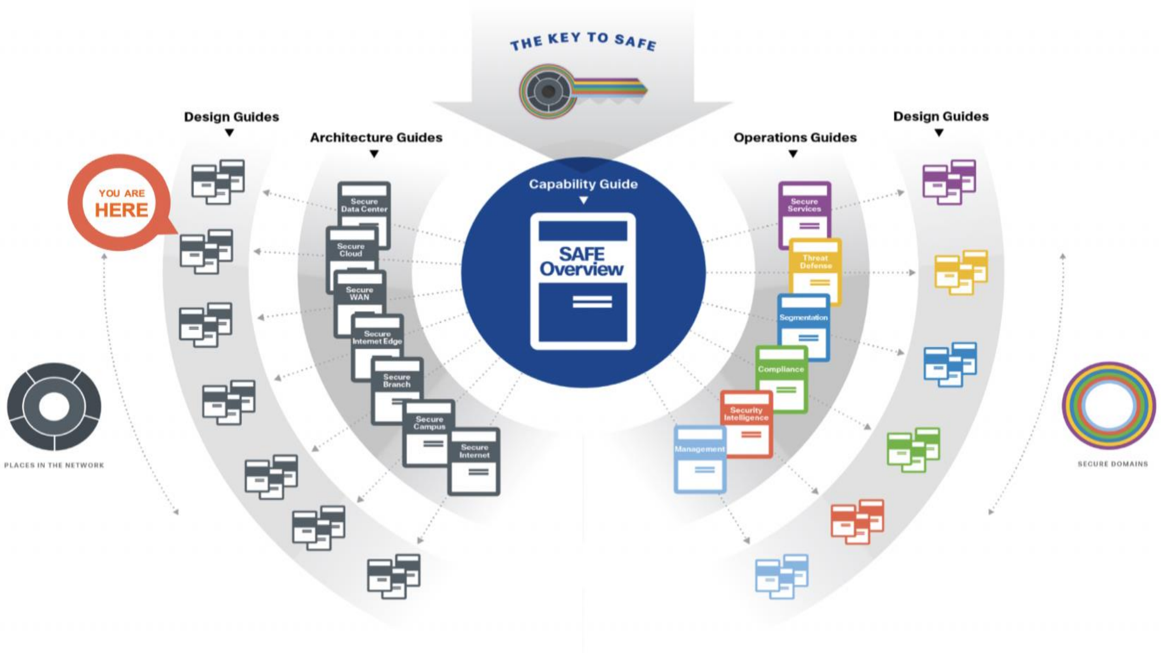


Figure 2.
SAFE Guidance Hierarchy

For more information on SAFE framework and architecture/design guides, check out the SAFE documentation (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 the Azure cloud:

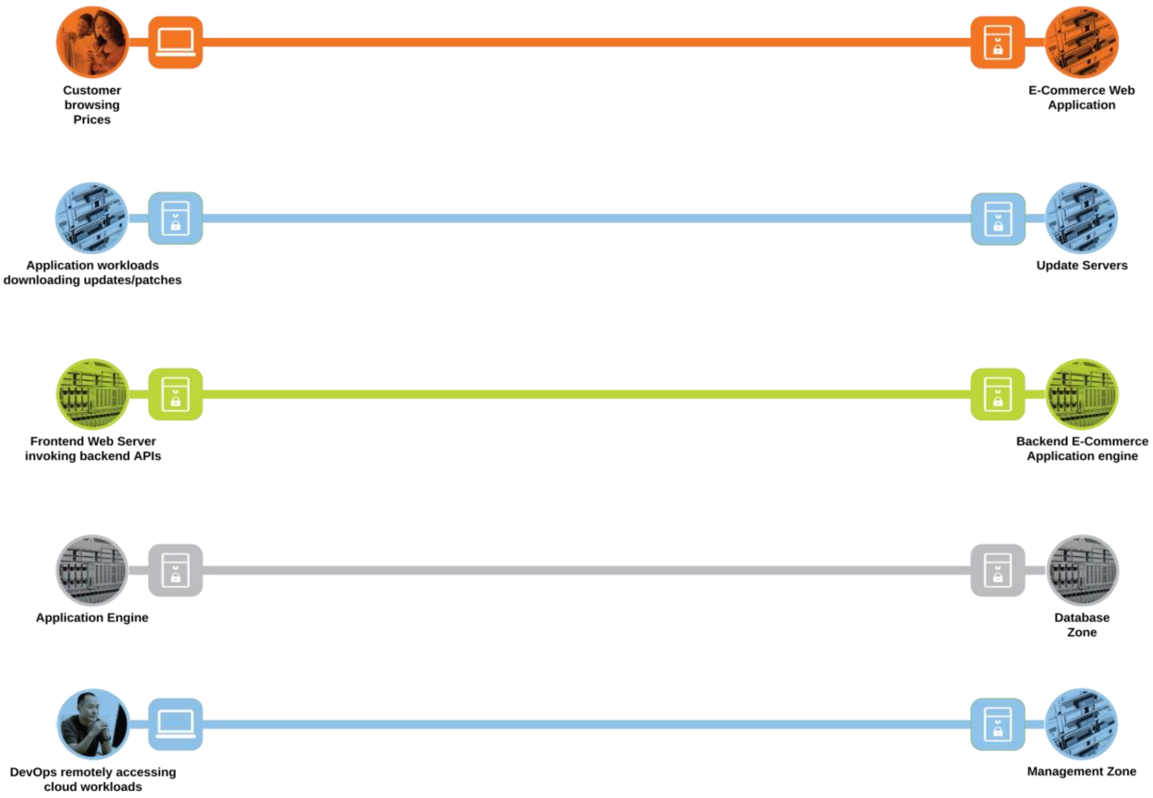

Customer browsing Prices
E-Commerce Web Application
Application workloads downloading updates/patches
Update Servers
Frontend Web Server invoking backend APIs
Backend E-Commerce Application engine
Application Engine
Database Zone
DevOps remotely accessing cloud workloads
Management Zone

Figure 3.
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 Azure 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 Azure cloud. For example- the frontend web servers will make HTTP requests to backend application engine or the application engine workloads will make API calls among themselves
- Application workloads transacting data with 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 can be showcased as below.

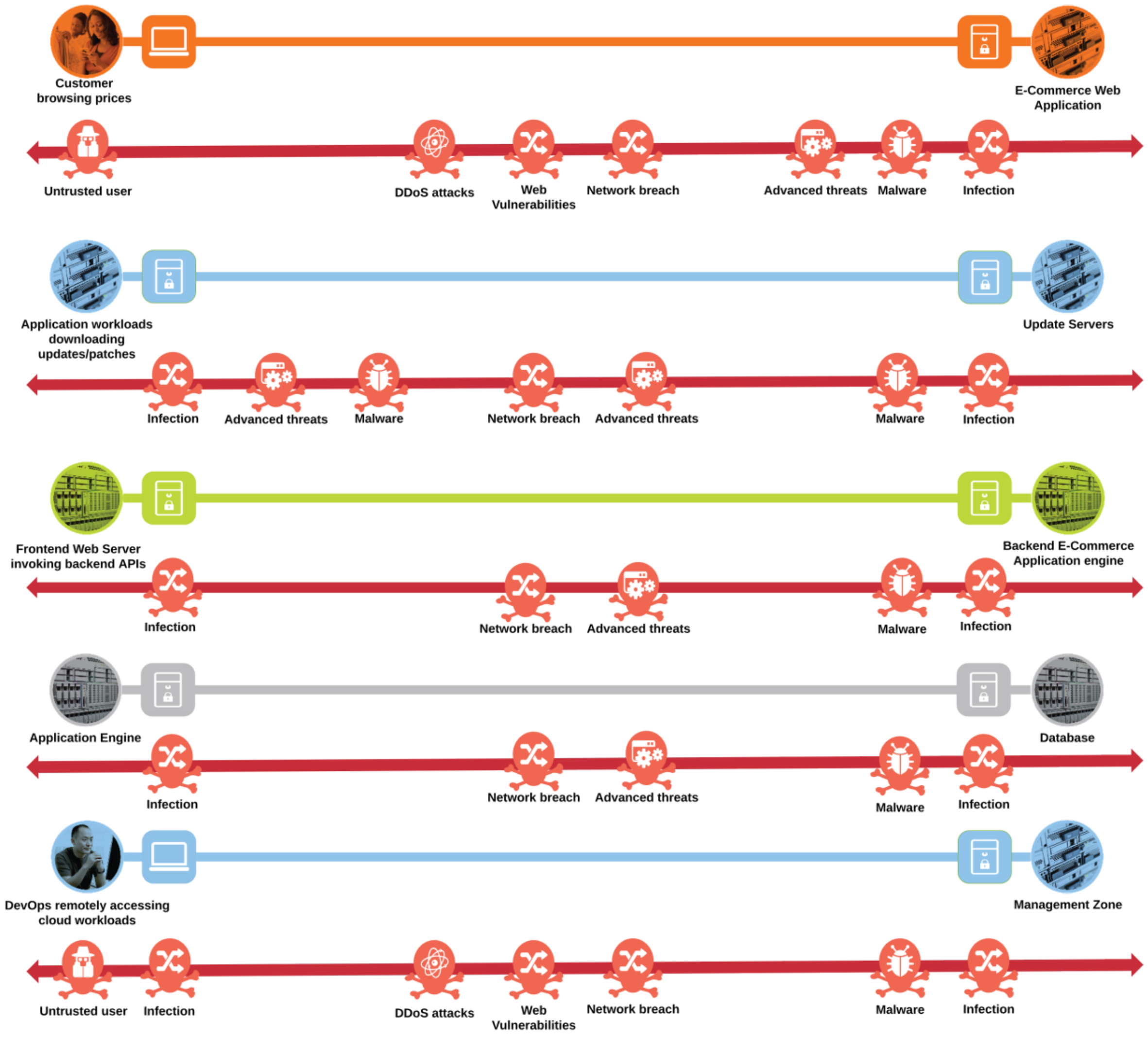


Figure 4.
Public cloud attack surface

- 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 Azure 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 Azure

Solution Overview

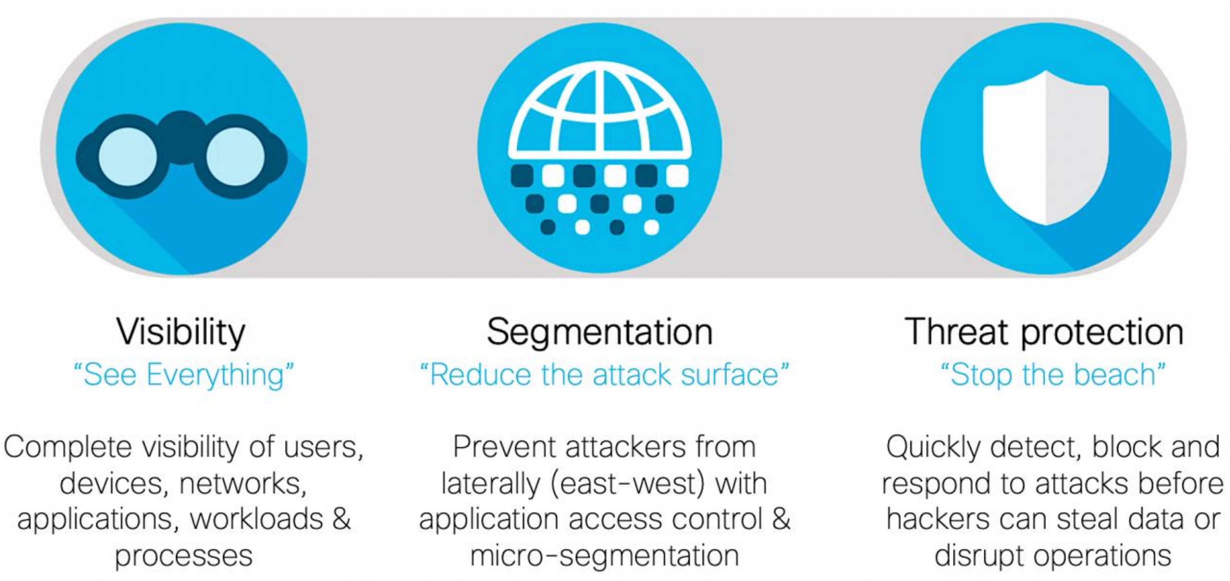
Cisco's security approach for the modern cloud applications allows companies to achieve:

- Improved resiliency to enable cloud availability and secure services
- Operational efficiency from automated provisioning and flexible, integrated security
- Advanced threat protection from Cisco TALOS – 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



Visibility

"See Everything"

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

Segmentation

"Reduce the attack surface"

Prevent attackers from laterally (east-west) with application access control & micro-segmentation

Threat protection

"Stop the beach"

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

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.

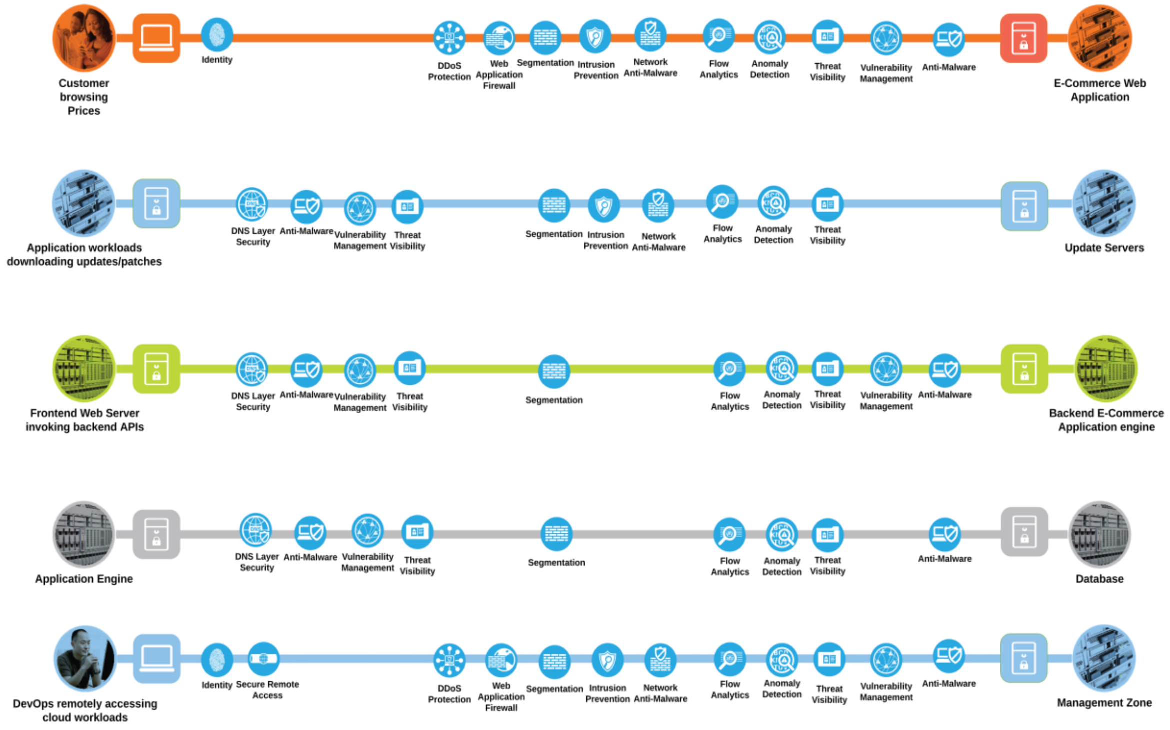


Figure 5.
Secure business flows

Cisco’s Secure Architecture for Azure

The tiered 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 document, we are securing a tiered web application in the Azure 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.

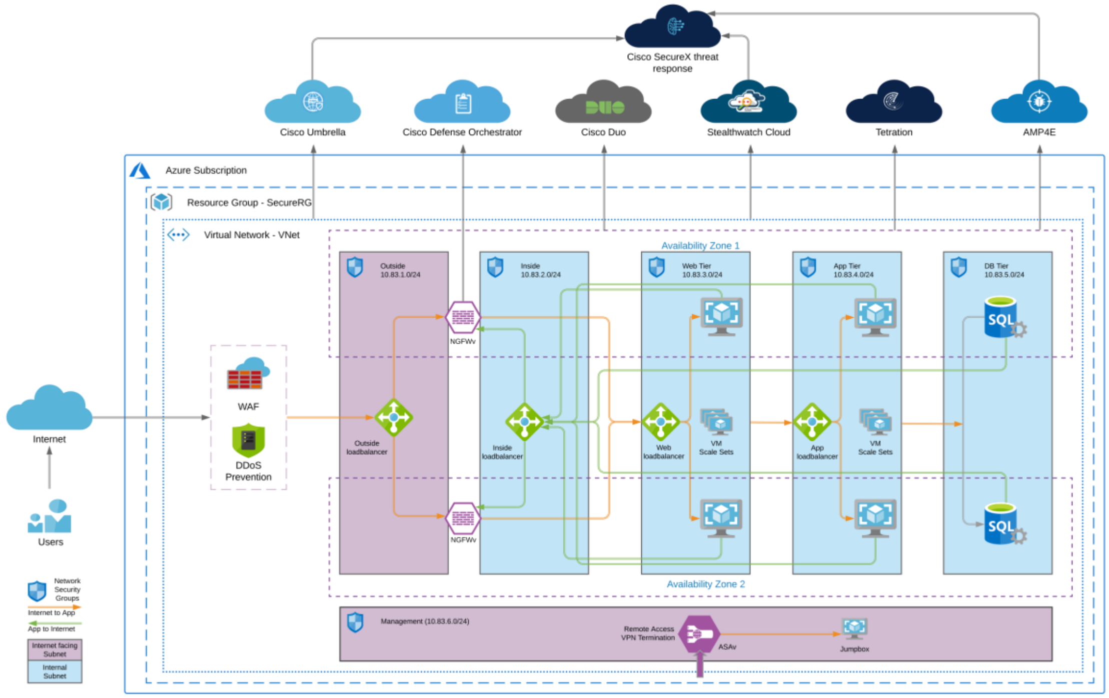


Figure 6.
Cisco Secure Cloud Reference Architecture

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 Capability		Security Solutions
	Attackers or malicious users accessing restricted resources and information.		Identity based access	Cisco Duo – 2FA
	Massively scaled attacks that overwhelm services.		DDoS prevention	Azure DDoS prevention Radware DDoS prevention
	Attacks against poorly developed applications and web vulnerabilities.		Web Application Firewalls	Azure Web Application Firewall Radware Web Application Firewall
	Network breach causing unauthorized access and malformed packets between and within application in the cloud.		Segmentation	Cisco Firepower NGFWv Azure Network Security Groups Cisco Tetration
	Zero-day malware attacks and other forms of covert threats.		Threat visibility	Cisco Stealthwatch Cisco Tetration Cisco AMP4E Cisco Firepower NGFWv
	Attacks using worms, viruses, or other techniques.		Intrusion Prevention	Cisco Firepower NGFWv Cisco AMP4E
	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
	Malware distribution across networks.		Network Anti-Malware	Cisco Firepower NGFWv

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

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

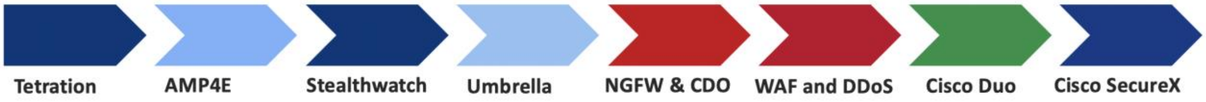
- Customer browsing an e-commerce web application
  - Access to the web application is secured using Duo – Multi-Factor Authentication (MFA)
  - WAF and DDoS Services protect against web vulnerabilities and denial of service attacks. In this document, we will demonstrate two options for WAF and DDoS protection- Azure cloud native service and Radware cloud service. Based on your preference, you could choose either
  - Network segmentation is done using next-generation firewalls (NGFW) to protect against any network or perimeter level breaches. NGFWs also provide next-generation IPS and AMP capabilities along with stateful firewall, AVC (Application Visibility and Control) and URL filtering.
  - At the macro level, workloads are segmented into various tiers using Azure Network Security Groups. 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 Azure 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
- Application workloads downloading updates/patches from update servers
  - Application workloads are segmented into App and Web tier using Azure Network Security Groups. 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 Azure Network Security Group)
  - 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

    - Network segmentation is achieved using Cisco Firepower next-generation firewalls to protect against any network or perimeter level breaches. NGFWs also provide network IPS and AMP capabilities, that would prevent any malicious file download right at the network perimeter

- Systems communicating east/west within the Azure cloud
    - Workloads are segmented into tiers at the macrolevel using Azure Network Security Groups. 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 within an application tier
    - 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
    - Azure Network 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 Secure Remote Worker design guide for detailed information on secure remote access designs and deployments
    - Management zone is segmented using Azure Network Security Groups. This provides the control knob for restricting access to workloads or the various 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 for greater visibility into the Azure cloud and workload activity. Then, we will look into Umbrella DNS layer security at the Azure VNET level.

Afterwards, we move to perimeter protection using Cisco Firepower NGFW (policy orchestrated by Cisco Defense Orchestrator), WAF and DDoS protection. We will explore two different options for WAF and DDoS protection – Azure Cloud Native Service and Radware Cloud.

Lastly, we will delve into securing authentication to our application using Duo MFA.

To connect all these security pieces together, we will look at Cisco SecureX threat response integrations to get a unified view of the Azure cloud security.

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. 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.

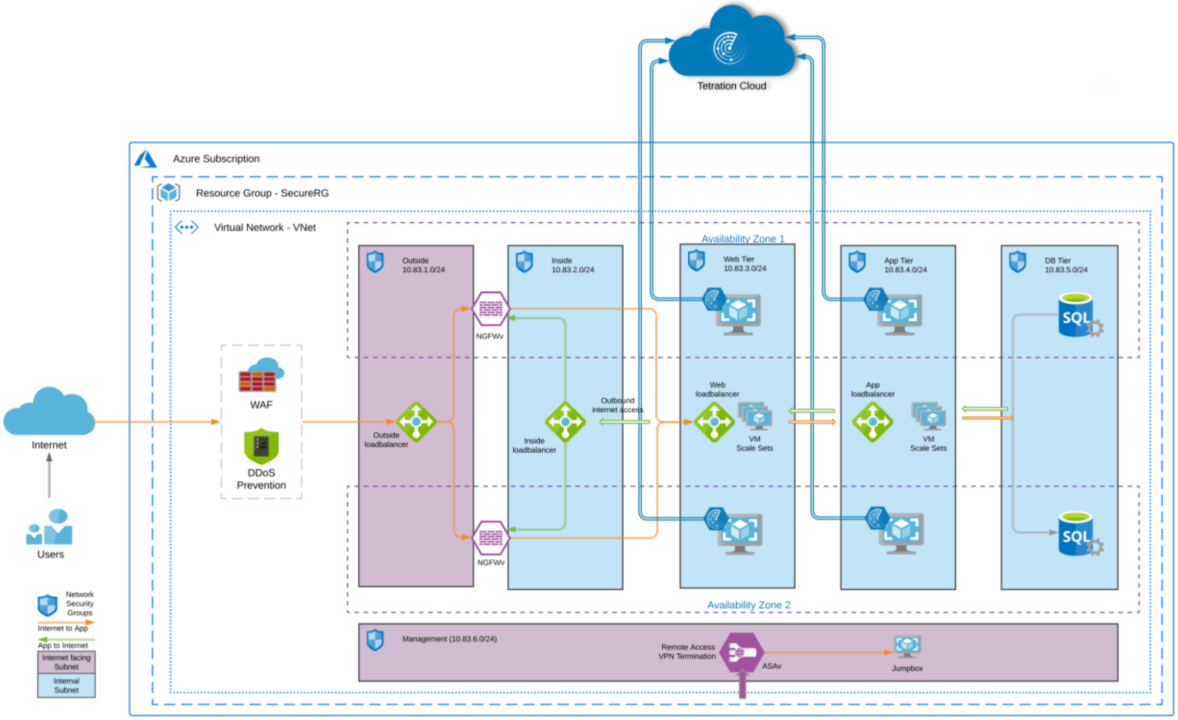


Figure 7.
Cisco Tetration

In this specific architecture, Web and Application tier has workloads in Virtual Machine Scale Sets (VSS). To enable the auto-provisioning of Tetration agents, we used the custom scripts provided under Azure VM extensions. When the VSS deploys a new workload, the custom 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.

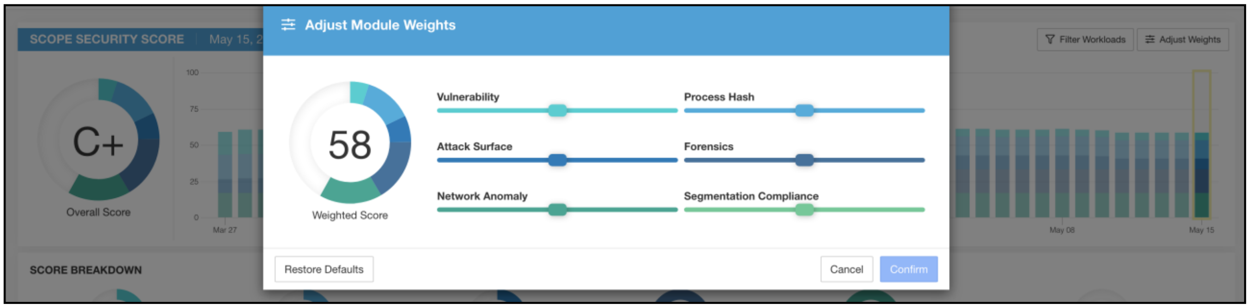


Figure 8.
Tetration Dashboard – Weighted Score

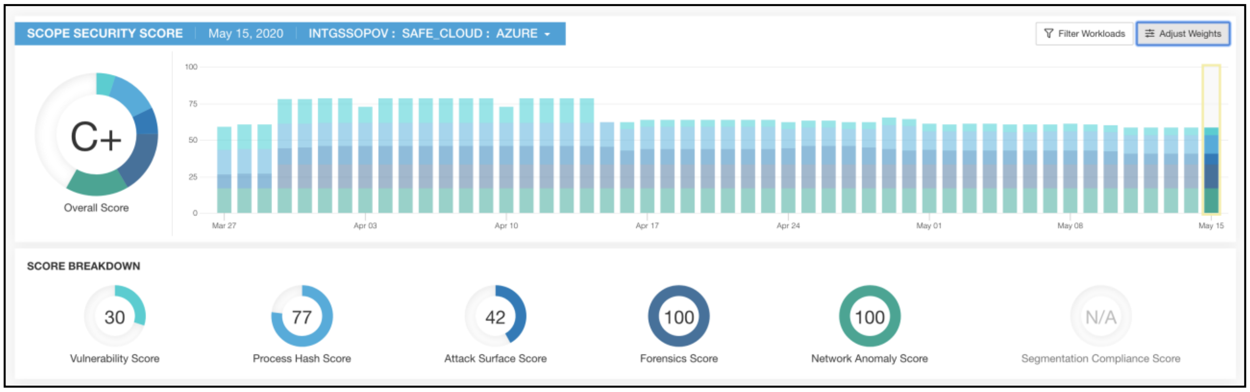


Figure 9.
Tetration Dashboard – Compliance Score Board

Refer to the Tetration documentation 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 Cisco TALOS, 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.

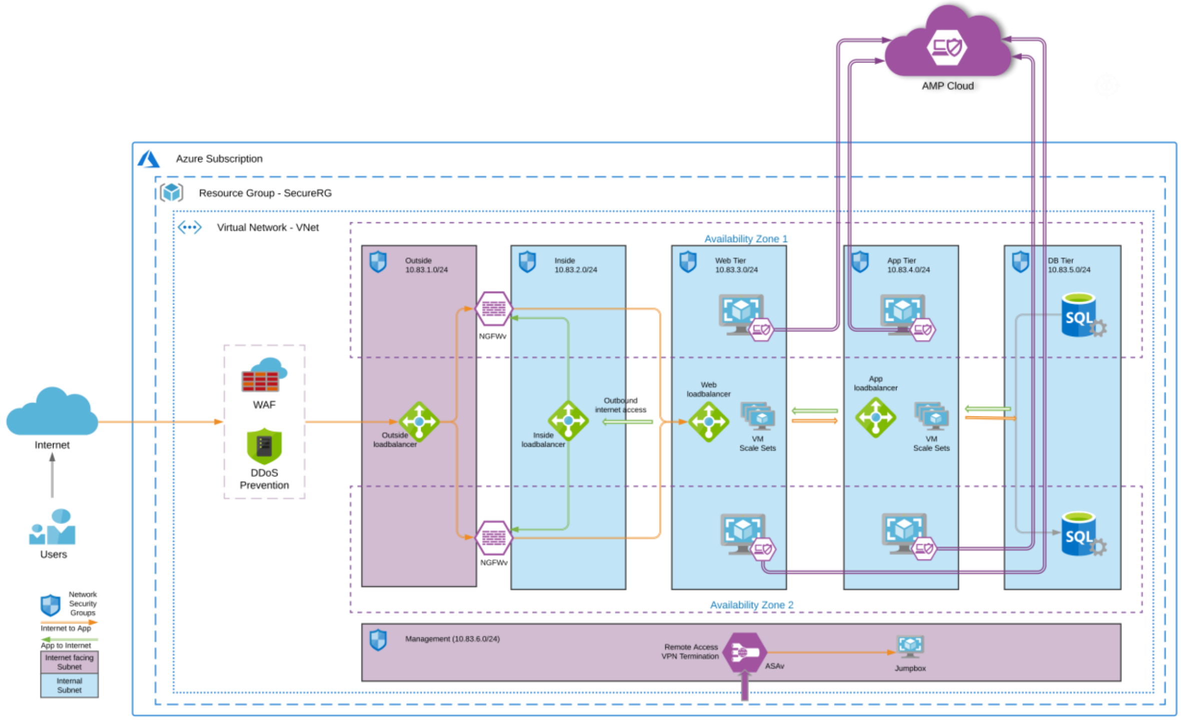
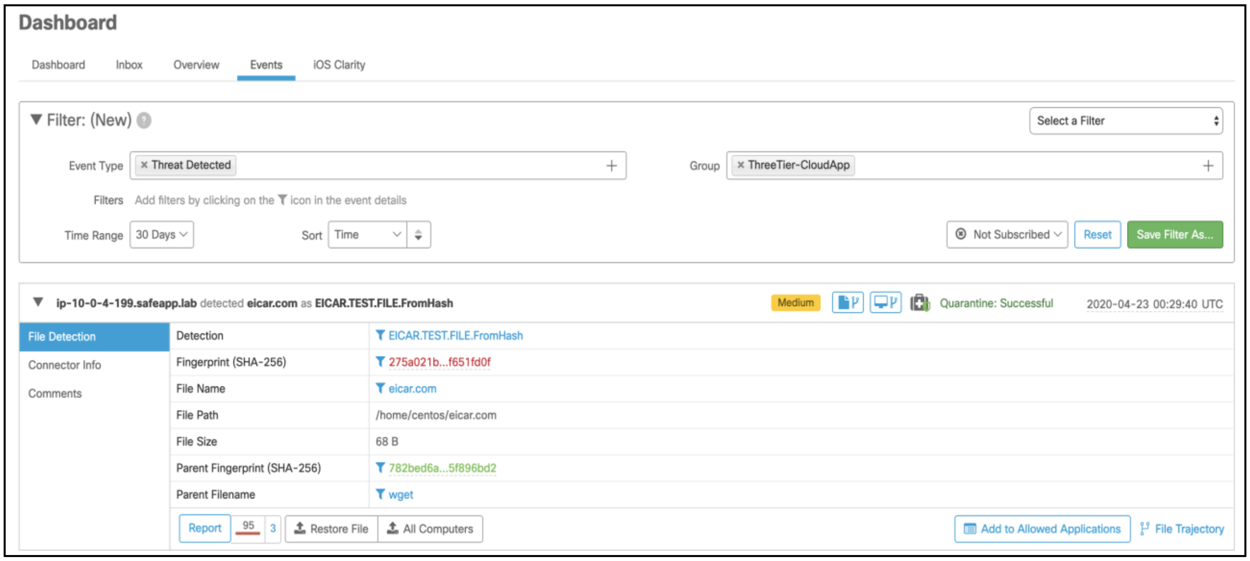


Figure 10.
Cisco Advanced Malware Protection for Endpoints

In this specific architecture, just like the Tetration agent, the web and application workloads in VSS are auto-provisioned with AMP4E agents using custom scripts option available via Azure VM extensions. When the VSS deploys a new workload, the custom 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.



▼ Filter: (New)

Event Type: × Threat Detected

Group: × ThreeTier-CloudApp

Filters: Add filters by clicking on the icon in the event details

Time Range: 30 Days

Sort: Time

▼ ip-10-0-4-199.safeapp.lab detected eicar.com as EICAR.TEST.FILE.FromHash — Quarantine: Successful — 2020-04-23 00:29:40 UTC

Detection	EICAR.TEST.FILE.FromHash
Fingerprint (SHA-256)	275a021b...f651fd0f
File Name	eicar.com
File Path	/home/centos/eicar.com
File Size	68 B
Parent Fingerprint (SHA-256)	782bed6a...5f896bd2
Parent Filename	wget

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 Azure cloud.

Stealthwatch Cloud pulls the Network Security Group (NSG) flow logs from the designated Azure storage containers. It learns the Azure environment and baselines the resources. NSG flow logs have the flow information associated with various Azure 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 Azure service. In other words, SWC performs dynamic entity modeling and organizes all the Azure 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 NSG flow logs, Stealthwatch Cloud also consumes other telemetry sources like Azure Activity logs for additional context and alerting.

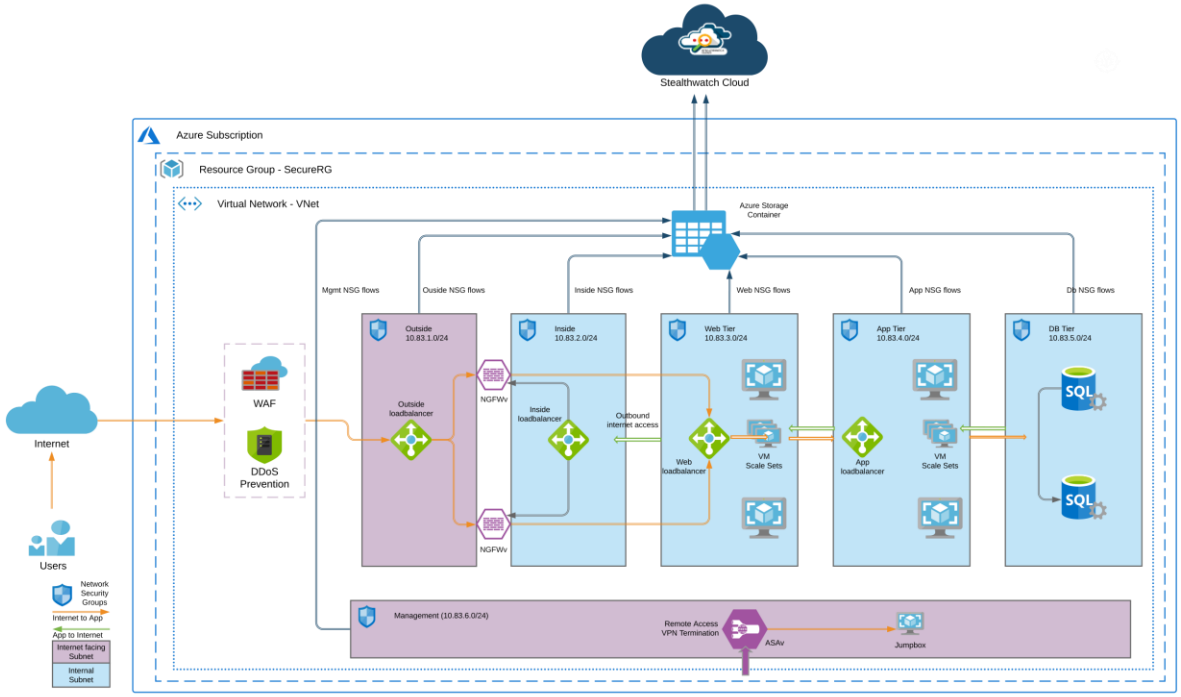
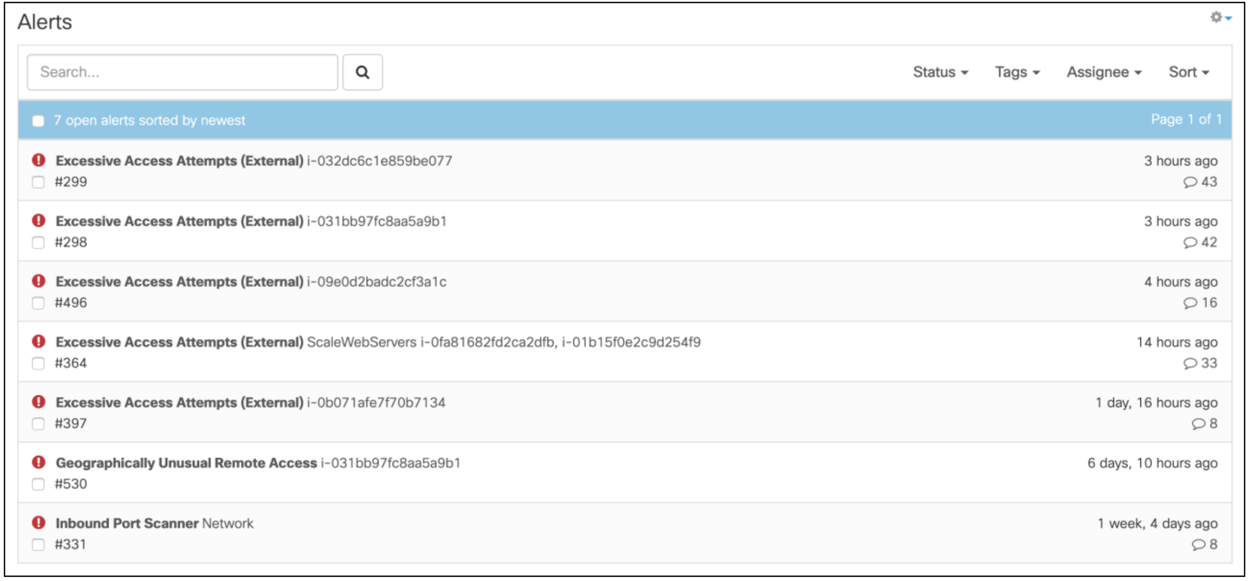


Figure 12.
Cisco Stealthwatch cloud

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 Azure cloud include:

- Azure Activity Log IP Watchlist Hit - This is triggered by an IP address that matched a user-defined or an integrated watchlist. This alert may indicate that an unauthorized user has gained access to Azure
- Azure Activity Log Watchlist Hit – This alert is triggered when Azure Activity Log reports an event on a user-supplied watchlist
- Azure Permissive Storage Account – If the storage accounts are identified by Azure Security Center as having unrestricted firewall settings then this alert is triggered
- Azure Security Event - Triggers when Azure Security Center reports a medium or high severity event
- Azure Virtual Machine in Unused Location - Triggers when an Azure Virtual Machine has been created in a previously unused location



□ 7 open alerts sorted by newest

Excessive Access Attempts (External) i-032dc6c1e859be077 — 3 hours ago
□ #299 — 43

Excessive Access Attempts (External) i-031bb97fc8aa5a9b1 — 3 hours ago
□ #298 — 42

Excessive Access Attempts (External) i-09e0d2badc2cf3a1c — 4 hours ago
□ #496 — 16

Excessive Access Attempts (External) ScaleWebServers i-0fa81682fd2ca2dfb, i-01b15f0e2c9d254f9 — 14 hours ago
□ #364 — 33

Excessive Access Attempts (External) i-0b071afe7f70b7134 — 1 day, 16 hours ago
□ #397 — 8

Geographically Unusual Remote Access i-031bb97fc8aa5a9b1 — 6 days, 10 hours ago
□ #530

Inbound Port Scanner Network — 1 week, 4 days ago
□ #331 — 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 Azure Virtual Network (VNET).

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 Umbrella documentation. It also gives you the flexibility to apply the policies to specific identities. For example, you could have one set of rules for your Azure cloud application and another set for a different site.

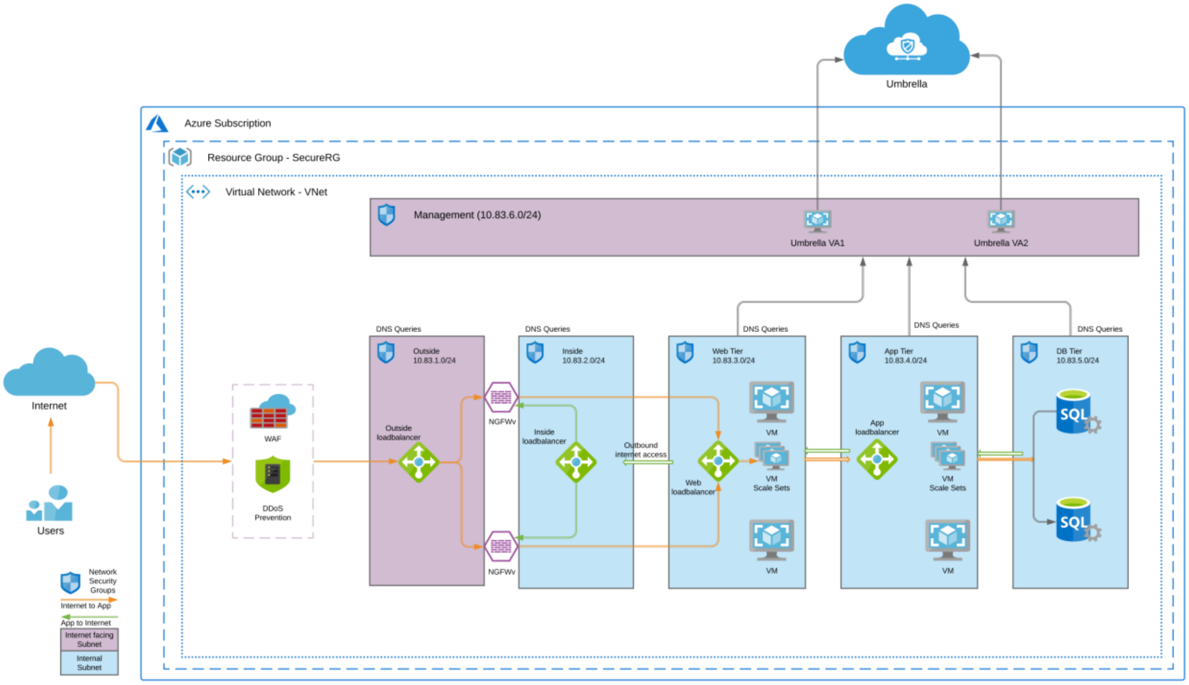
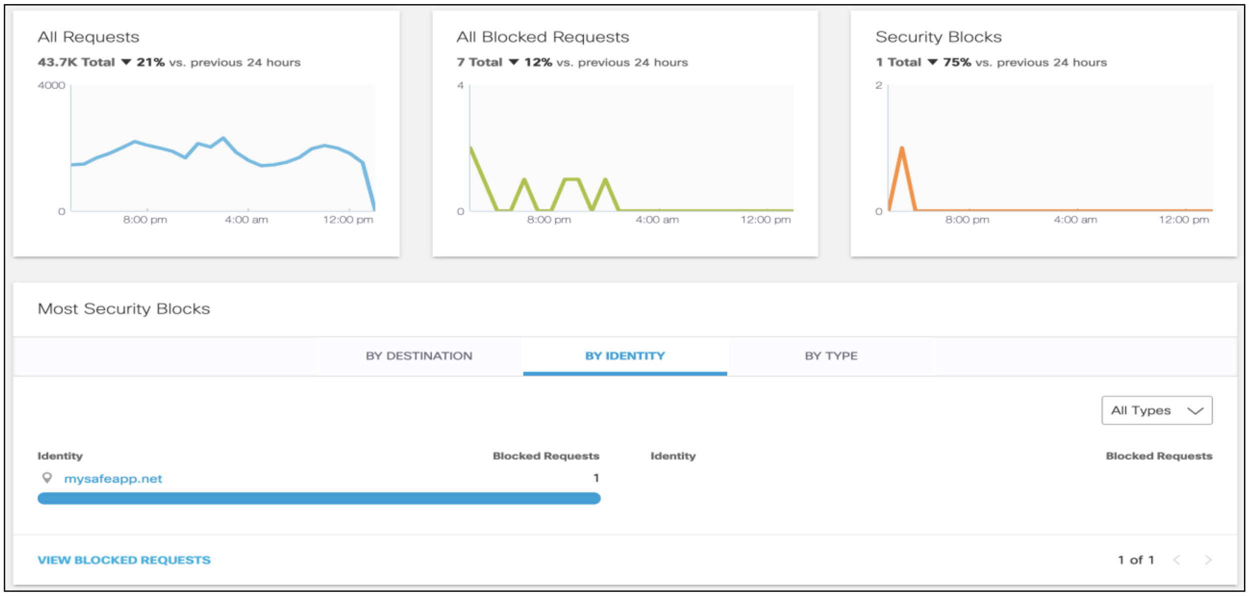


Figure 14.
Cisco Umbrella – DNS layer Security

We deploy Umbrella Virtual Appliances (VA) in the Management tier of the Azure VNET. These VAs act as DNS forwarders to Umbrella. The Azure VNET offers the option to configure custom DNS settings, allowing us to point the cloud resources in a given VNET to Umbrella VAs instead of Azure local DNS. Every resource, that is launched into the VNET, 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

All Blocked Requests
7 Total ▼ 12% vs. previous 24 hours

Security Blocks
1 Total ▼ 75% vs. previous 24 hours

Most Security Blocks

BY DESTINATION | BY IDENTITY | BY TYPE

All Types

Identity	Blocked Requests	Identity	Blocked Requests
mysafeapp.net	1		

VIEW BLOCKED REQUESTS

1 of 1

Figure 15.
Umbrella – DNS Traffic Monitoring

Cisco Firepower Next-Generation Firewall and Adaptive Security Appliance

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). 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 Management tier, 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 Secure Remote Worker 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. Cisco Defense Orchestrator helps to correct issues such as unused, duplicate, and inconsistent objects hence ensuring consistent policies for firewalls.

We use CDO to manage both NGFWv and ASAv, providing centralized management.

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. Azure marketplace offering is available under the name 'Cisco Firepower NGFW Virtual (NGFWv)'.

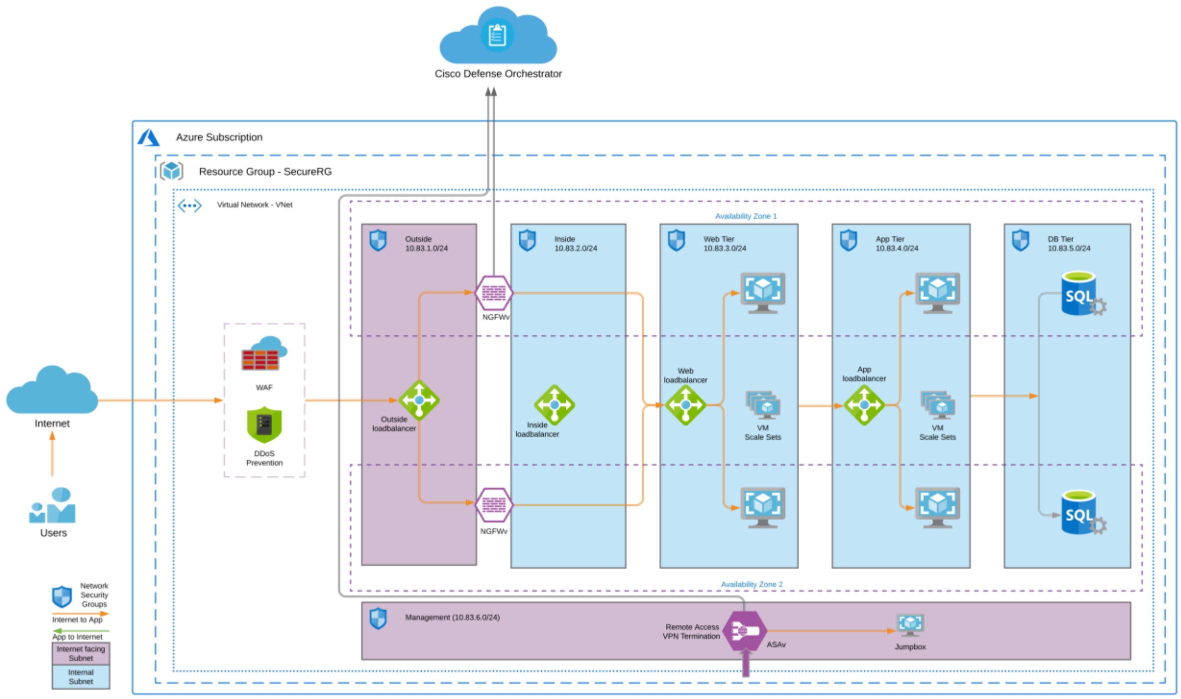


Figure 16.
NGFWv - Traffic flow from Internet User to application

User to application traffic flow

When the user out on the Internet tries to browse the cloud-hosted web application, it lands on ‘Outside’ 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 Azure Network Security Group) and load balances traffic onto the pool of outside interfaces of next-generation firewalls. The NGFW receiving the request then forwards this traffic to ‘Web’ load balancer, to be load-balanced on to web servers bundled in Web Virtual Machine Scale Set (VSS).

Before the traffic leaves the inside interface of the firewall (in the Inside tier), the source of this packet is translated (Network Address Translation) to inside interface IP of the firewall 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 dynamic 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.

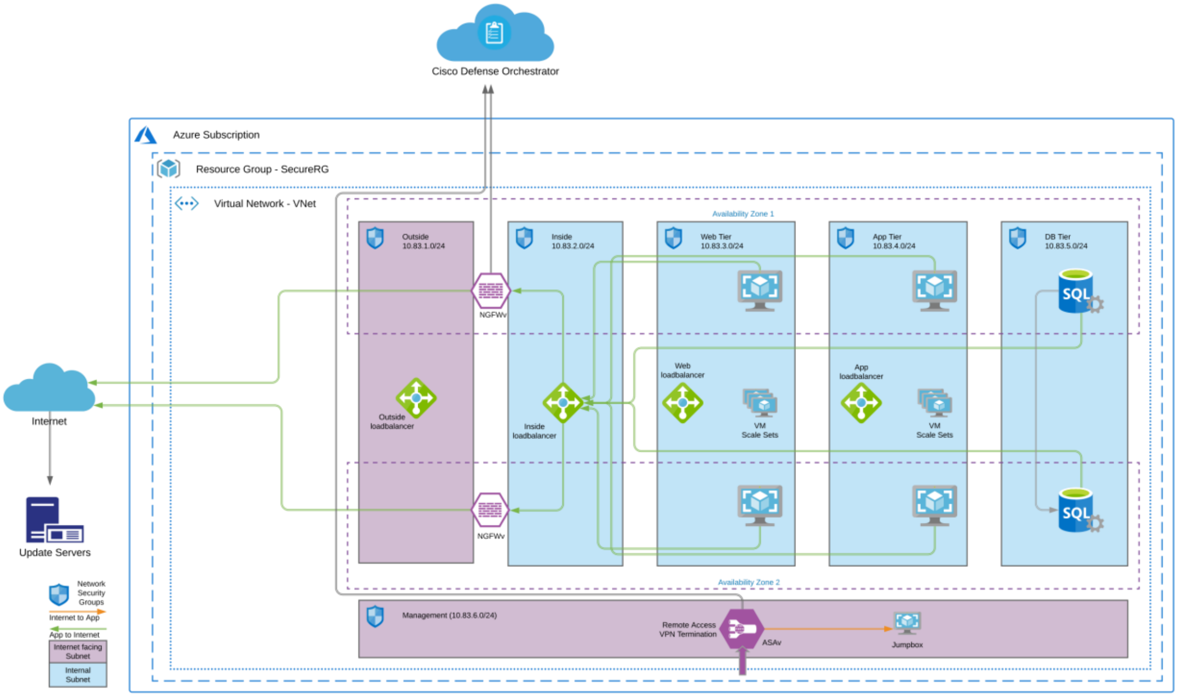


Figure 17.
NGFWv - Traffic flow from workloads out to the Internet

Application to update servers

For the traffic or requests initiated from the Web or Application tier, we use the Azure Route Tables to point the default route to ‘Inside’ load balancer sitting in the Inside tier. The ‘Inside’ load balancer load-balances all the outgoing requests to inside interfaces of the firewalls. The firewalls then route the traffic out to the Internet destination/update server after port address translation (PAT) to the outside interfaces. The outside firewall interfaces are assigned public IPs.

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. For this design, we validated two different solutions i.e. Azure WAF & DDOS service and Radware Cloud WAF & DDoS service.

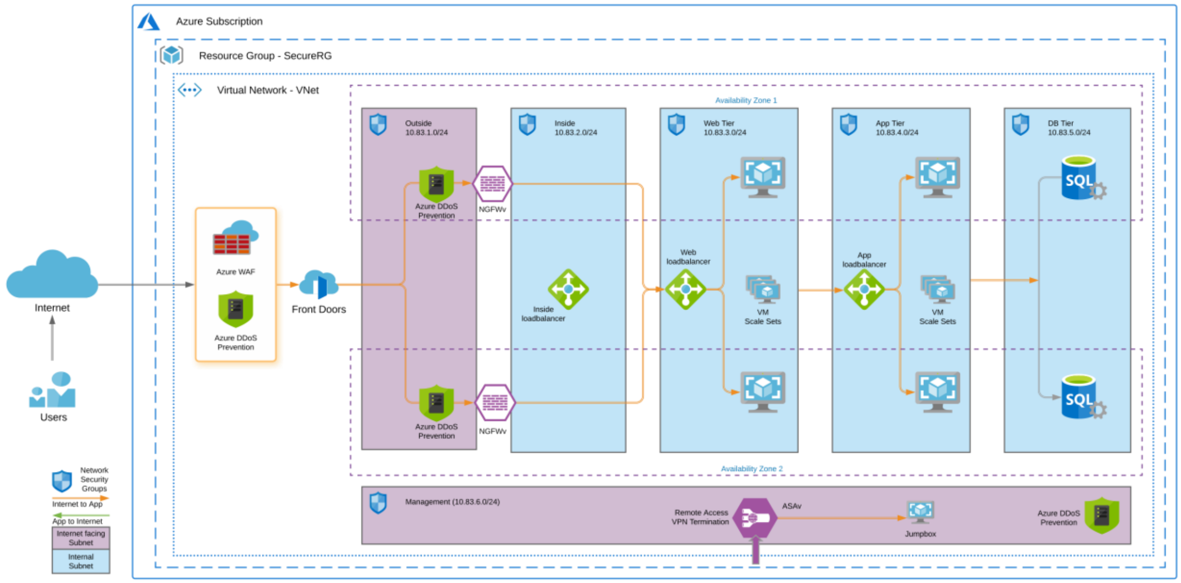


Figure 18.
Azure WAF and DDoS protection

Azure offers WAF and DDoS as native services that controls access to the application by allowing or blocking web requests. This protects web applications from common web exploits. In addition to web traffic protection, DDoS component provide network flow monitoring to protect against DDoS attacks.

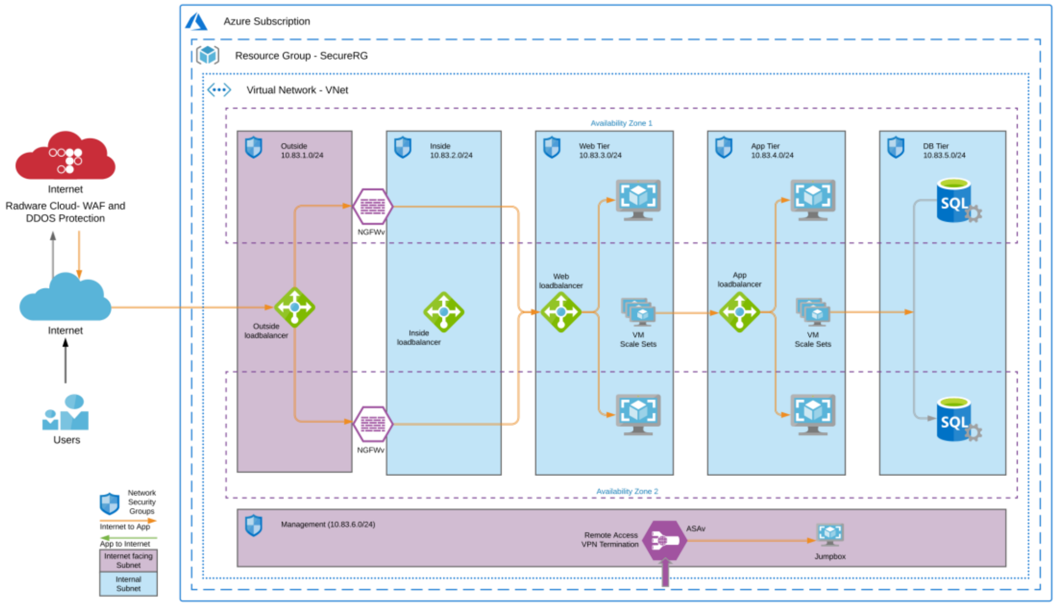


Figure 19.
Radware Cloud – WAF and DDoS Prevention

Radware's Cloud Security Services offer easy-to-deploy cloud-based security that can be integrated with your cloud environments to provide proactive, automated protection from advanced threats. Radware provides applications hosted in the cloud with the protection from the full breadth of DDoS attacks with real-time mitigation and no added latency in peacetime.

Radware acts as a man in the middle. 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 Azure 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

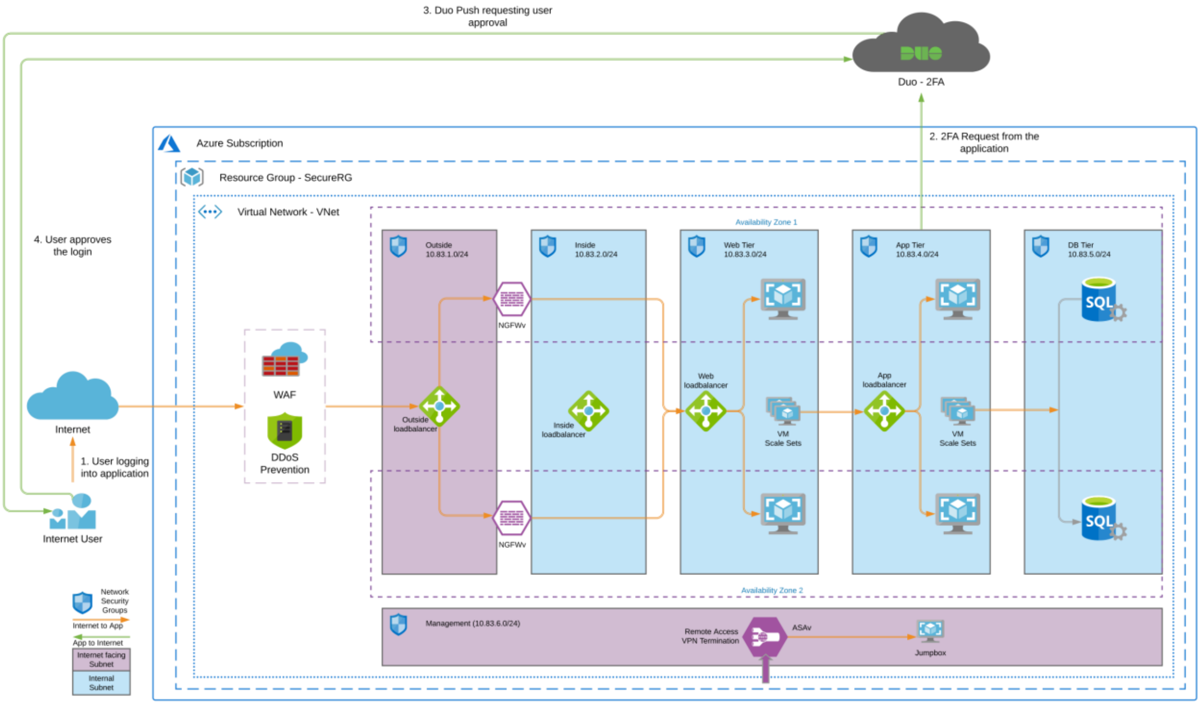
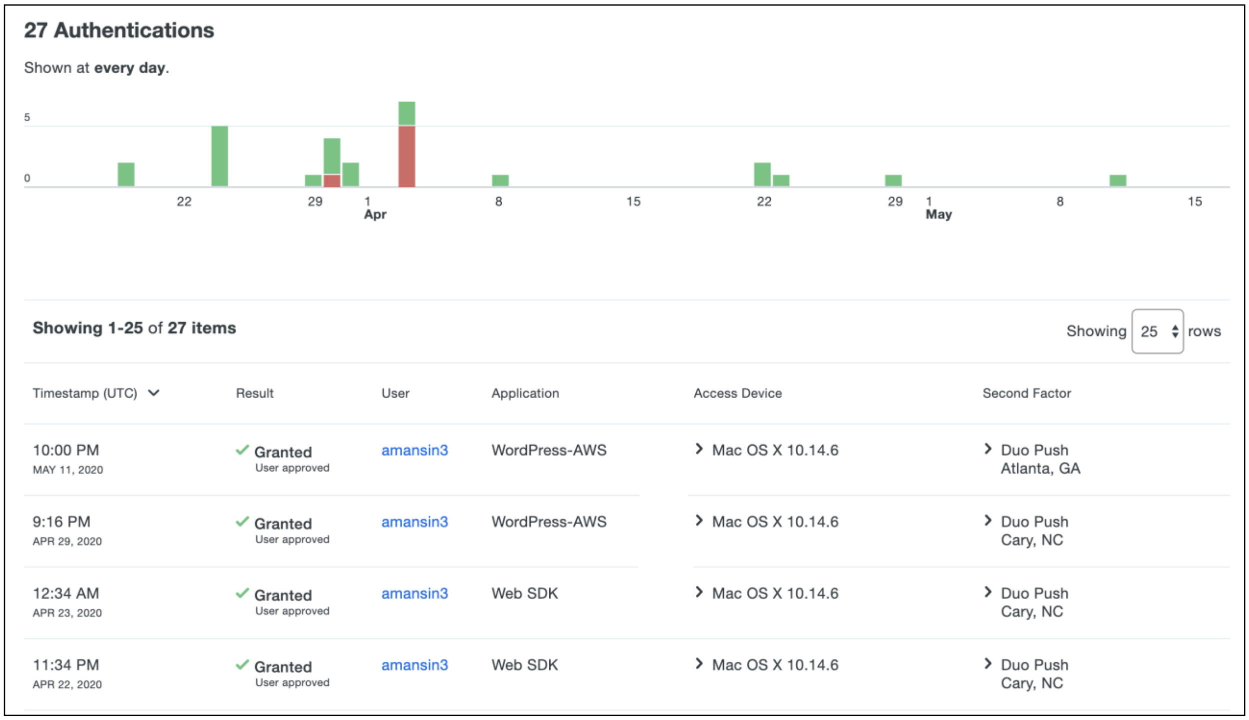


Figure 20.
Duo MFA Push

In this design, we used Duo’s Multi-Factor Authentication (MFA) for our Azure 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, Azure sync, Active Directory sync, and OpenLDAP sync. Duo admin portal allows a highly convenient way to track any user activity.



27 Authentications

Shown at **every day**.

Showing 1-25 of **27 items**

Showing 25 rows

Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
10:00 PM MAY 11, 2020	✓ Granted User approved	amansin3	WordPress-AWS	Mac OS X 10.14.6	Duo Push Atlanta, GA
9:16 PM APR 29, 2020	✓ Granted User approved	amansin3	WordPress-AWS	Mac OS X 10.14.6	Duo Push Cary, NC
12:34 AM APR 23, 2020	✓ Granted User approved	amansin3	Web SDK	Mac OS X 10.14.6	Duo Push Cary, NC
11:34 PM APR 22, 2020	✓ Granted User approved	amansin3	Web SDK	Mac OS X 10.14.6	Duo Push Cary, NC

Figure 21.
Duo - User Activity

Cisco SecureX threat response

Cisco SecureX threat response 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

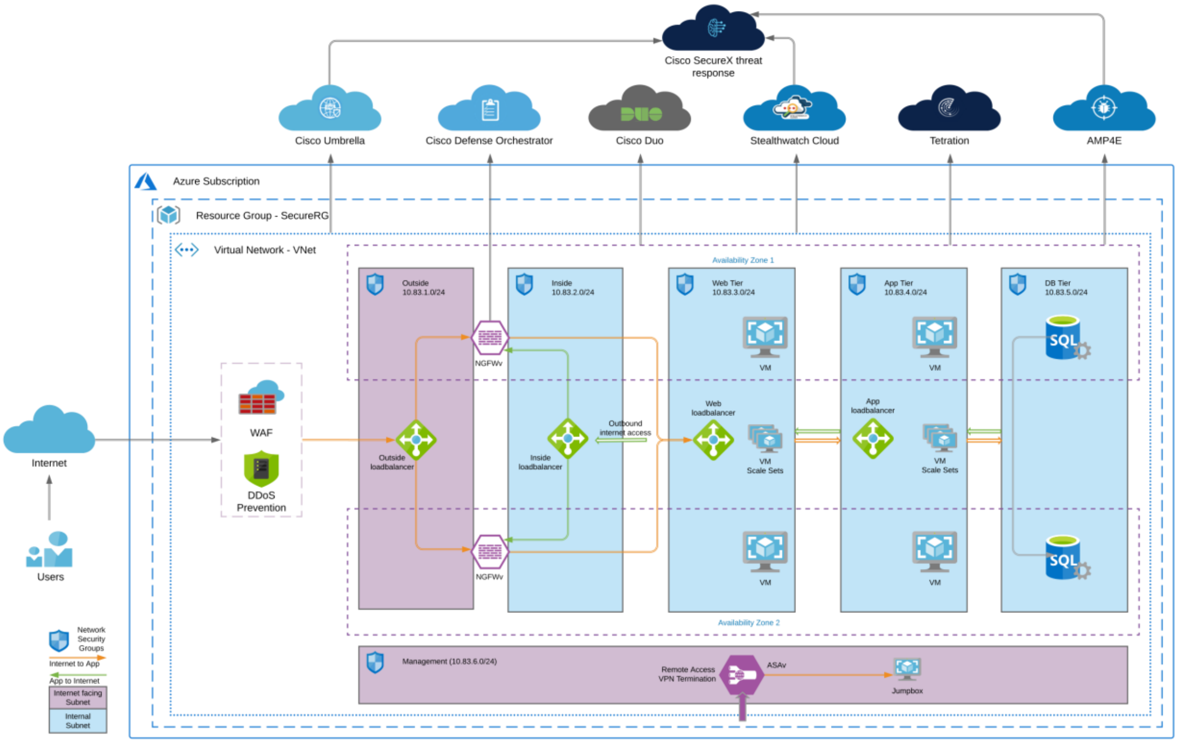
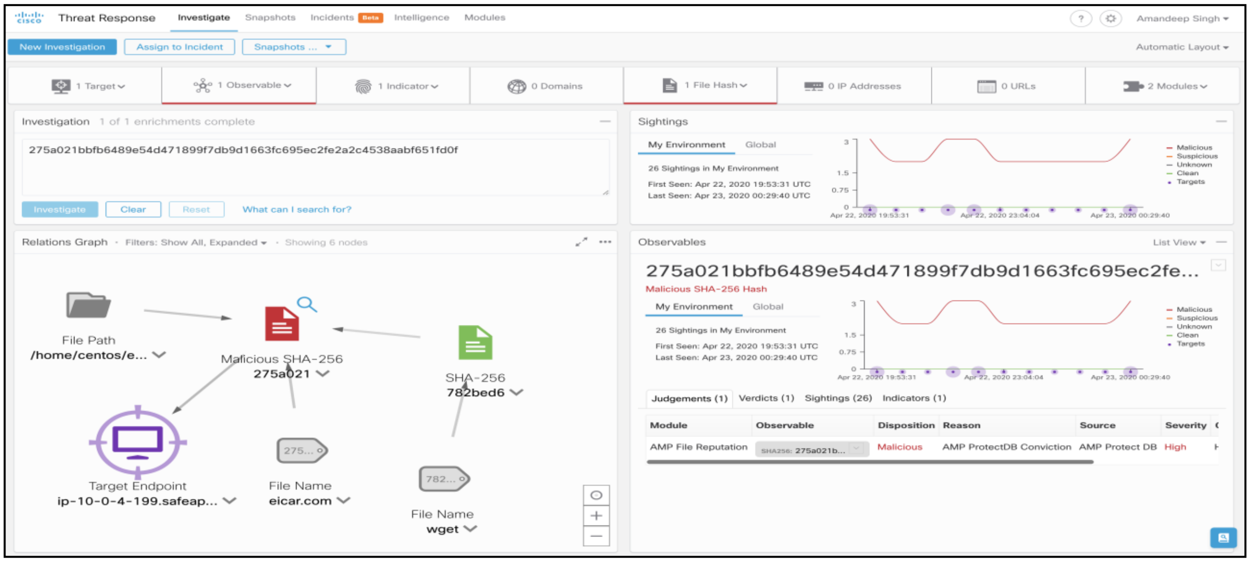


Figure 22.
Cisco SecureX threat response

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



275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

26 Sightings in My Environment
First Seen: Apr 22, 2020 19:53:31 UTC
Last Seen: Apr 23, 2020 00:29:40 UTC

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe...

26 Sightings in My Environment
First Seen: Apr 22, 2020 19:53:31 UTC
Last Seen: Apr 23, 2020 00:29:40 UTC

Module	Observable	Disposition	Reason	Source	Severity
AMP File Reputation	SHA256: 275a021b...	Malicious	AMP ProtectDB Conviction	AMP Protect DB	High

Figure 23.
Cisco SecureX threat response – Threat Hunting

Design Implementation

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

We will start by setting up the Azure VNET (Virtual Network) as per the tiered architecture specifications. Once our VNET is ready, we will integrate the Stealthwatch Cloud and set up the Umbrella VAs in the management tier and update the DNS server settings for the VNET.

We will then set up the Azure MySQL database and bring up VSS's (Virtual Machine Scale Sets) for the App and Web workloads followed by setting up the load balancers for each VSS.

Lastly, we will configure the firewalls, enable WAF and DDoS protection and then conclude our set up with Cisco SecureX threat response 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 Azure Virtual Network
- Integrate Stealthwatch Cloud to Azure environment
- Set up the Umbrella Virtual Appliances
- Set up Azure Database for MySQL servers
- Set up the App and Web Virtual machine Scale Sets (Includes Tetration, AMP4E and Duo Integration)
- Set up the App and Web load balancers
- Set up Cisco Firepower Next-Generation Firewalls and Cisco Defense Orchestrator
- Enable Web Application Firewall and DDoS prevention (Azure and Radware)
- Set up Cisco SecureX threat response

Set up the Azure Virtual Network

In this section, we will create a new Azure VNET and configure all the associated components that we need for our deployment.

Implementation procedure:

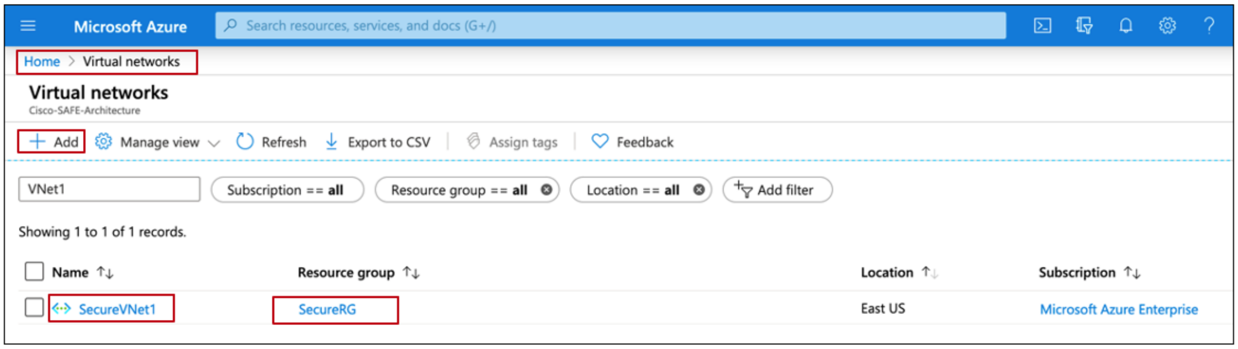
Step 1. Create the VNet

Step 2. Create the Network Security Groups

Step 3. Set up the Routing Tables

Step 4. Define the Subnets

Step 1. Create the VNet - Log on to the Azure portal and add a new VNet in the 'Resource Group' and region of your choice. We had created a new 'Resource Group' for this specific implementation, but you can use an existing one. We chose the IPV4 CIDR block as 10.83.0.0/16.



Virtual networks
Cisco-SAFE-Architecture

VNet1

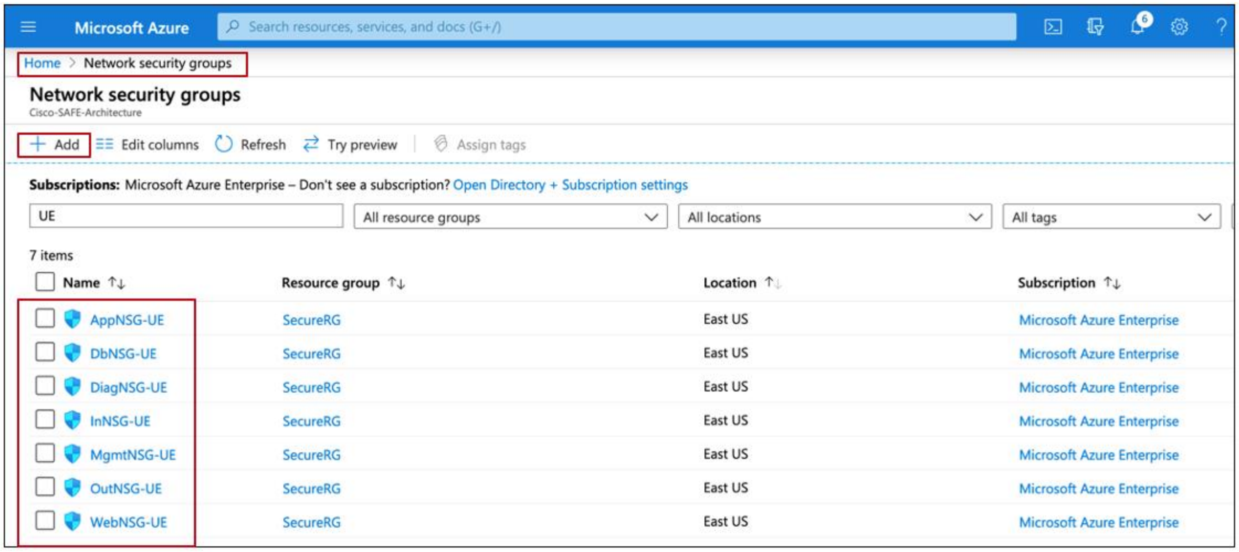
Showing 1 to 1 of 1 records.

Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
SecureVNet1	SecureRG	East US	Microsoft Azure Enterprise

Follow the Azure documentation for more details on Azure ‘Virtual networks’.

Step 2. **Create the Network Security Groups –** Go to ‘Network Security Groups’ on the Azure portal, click on ‘add’ to set up NSGs corresponding to each tier in the design. Set up the access rules as per your application requirements.

Based on our lab environment, we allowed TCP port 80 inbound to ‘Outside’ tier, to allow internet users to browse the application. Also, we opened TCP port 22 for specific source IPs to allow inbound access to management zone. For all other NSGs, we used the default settings which allow communication within the VNET, inbound load balancer probes, and outbound internet access for any resource deployed in the NSGs.



Network security groups
Cisco-SAFE-Architecture

Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Open Directory + Subscription settings

UE

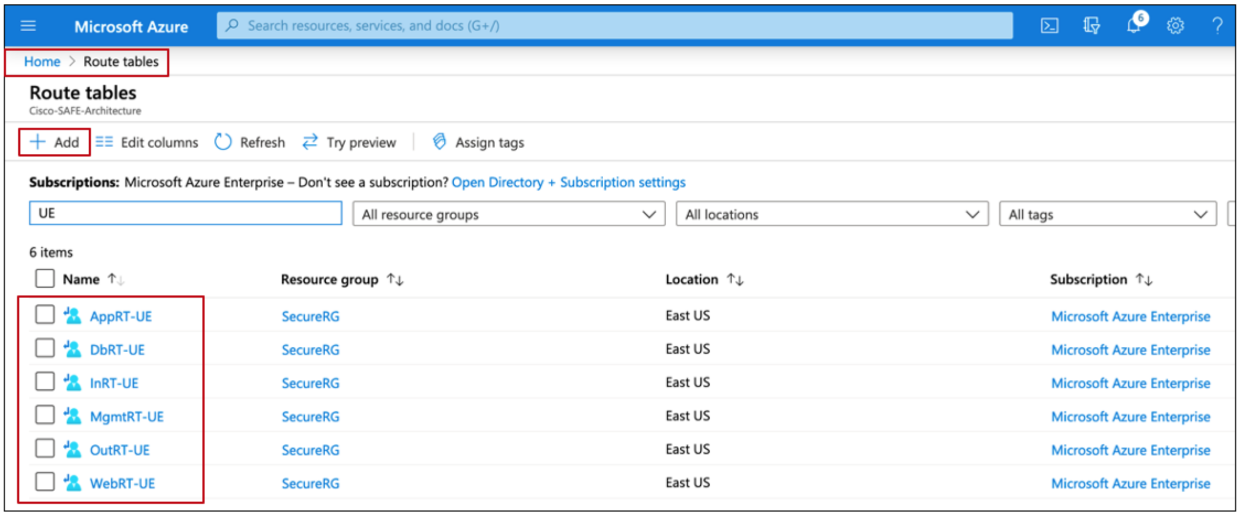
7 items

Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
AppNSG-UE	SecureRG	East US	Microsoft Azure Enterprise
DbNSG-UE	SecureRG	East US	Microsoft Azure Enterprise
DiagNSG-UE	SecureRG	East US	Microsoft Azure Enterprise
InNSG-UE	SecureRG	East US	Microsoft Azure Enterprise
MgmtNSG-UE	SecureRG	East US	Microsoft Azure Enterprise
OutNSG-UE	SecureRG	East US	Microsoft Azure Enterprise
WebNSG-UE	SecureRG	East US	Microsoft Azure Enterprise

Follow the Azure documentation for more details on Azure ‘Network Security Groups’.

Step 3. **Set up the Route tables –** Go to ‘Route tables’ on the Azure portal and create the routing tables for each tier. There is one routing table for each tier. The default routes allow all access among different tiers/subnets and to the outbound internet.

For now, we will leave the routes as default but when we get to firewall deployment, we will update some of these routing tables to force the traffic through our firewall for scanning and inspection.



Route tables
Cisco-SAFE-Architecture

Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Open Directory + Subscription settings

UE | All resource groups | All locations | All tags

6 items

Name	Resource group	Location	Subscription
AppRT-UE	SecureRG	East US	Microsoft Azure Enterprise
DbRT-UE	SecureRG	East US	Microsoft Azure Enterprise
InRT-UE	SecureRG	East US	Microsoft Azure Enterprise
MgmtRT-UE	SecureRG	East US	Microsoft Azure Enterprise
OutRT-UE	SecureRG	East US	Microsoft Azure Enterprise
WebRT-UE	SecureRG	East US	Microsoft Azure Enterprise

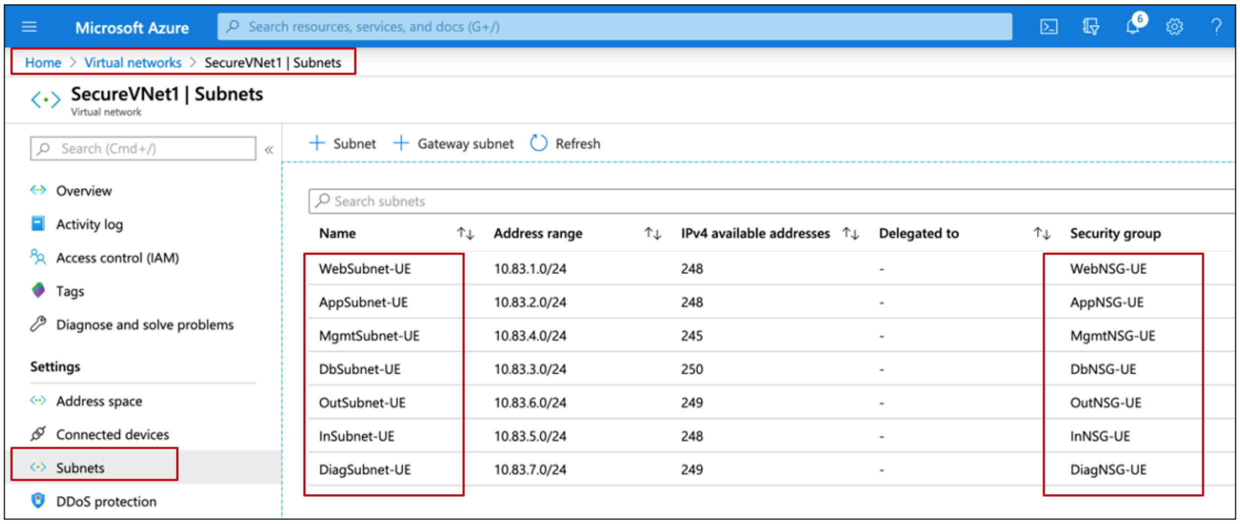
Follow the Azure documentation here for more detailed information on Azure traffic routing and route tables.

Step 4. Define the Subnets - At this point we have all the building blocks to define the subnets in our newly created VNET.

Based on the tiered architecture, we defined one subnet for each tier- web, application, database, management, inside and outside.

IPV4 CIDR Block	Azure Region	Tier
10.83.1.0/24	US-East	Database
10.83.2.0/24	US-East	Application
10.83.3.0/24	US-East	Web
10.83.4.0/24	US-East	Management
10.83.5.0/24	US-East	Inside
10.83.6.0/24	US-East	Outside
10.83.7.0/24	US-East	Diagnostic (for NGFWv deployment)

Go to 'Virtual Networks' and select the VNET created in Step 1. From the panel on the left-hand side, select 'Subnets' and then click on '+ Subnet' to add all the subnets above. Ensure that the subnet created is tied to the appropriate NSG.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual networks > SecureVNet1 | Subnets

SecureVNet1 | Subnets
Virtual network

Name	Address range	IPv4 available addresses	Delegated to	Security group
WebSubnet-UE	10.83.1.0/24	248	-	WebNSG-UE
AppSubnet-UE	10.83.2.0/24	248	-	AppNSG-UE
MgmtSubnet-UE	10.83.4.0/24	245	-	MgmtNSG-UE
DbSubnet-UE	10.83.3.0/24	250	-	DbNSG-UE
OutSubnet-UE	10.83.6.0/24	249	-	OutNSG-UE
InSubnet-UE	10.83.5.0/24	248	-	InNSG-UE
DiagSubnet-UE	10.83.7.0/24	249	-	DiagNSG-UE

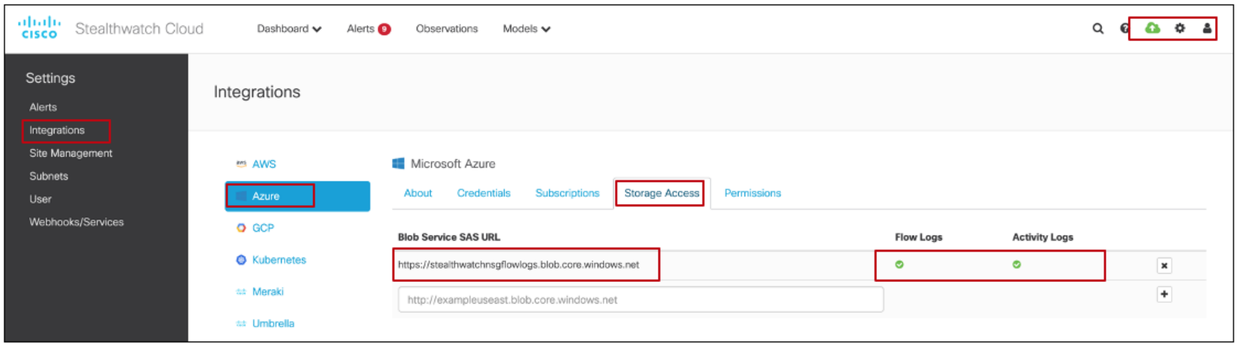
Integrating Stealthwatch Cloud

Implementation procedure:

Step 1. Set up the NSG flow logs and integrate Stealthwatch Cloud.

Step 1. **Set up the NSG flow logs and integrate Stealthwatch Cloud –** Follow the steps illustrated in Cisco Stealthwatch Azure Quick Start Guide to create the NSG flow logs and push them to the Stealthwatch cloud to be analyzed. Based on this flow log information, the Stealthwatch Cloud would generate security alerts and observations on any activity within the VNET.

After the SWC integration is done, go to ‘Settings > Integrations >Azure > Storage Access’ on SWC portal and you should see green check marks indicating a successful integration.



Integrations

Blob Service SAS URL	Flow Logs	Activity Logs
https://stealthwatchnsgflowlogs.blob.core.windows.net	✓	✓
http://exampleuseast.blob.core.windows.net		

Setting up Cisco Umbrella

Implementation procedure:

Step 1. **Set up the Umbrella Virtual Appliance (VA) image**

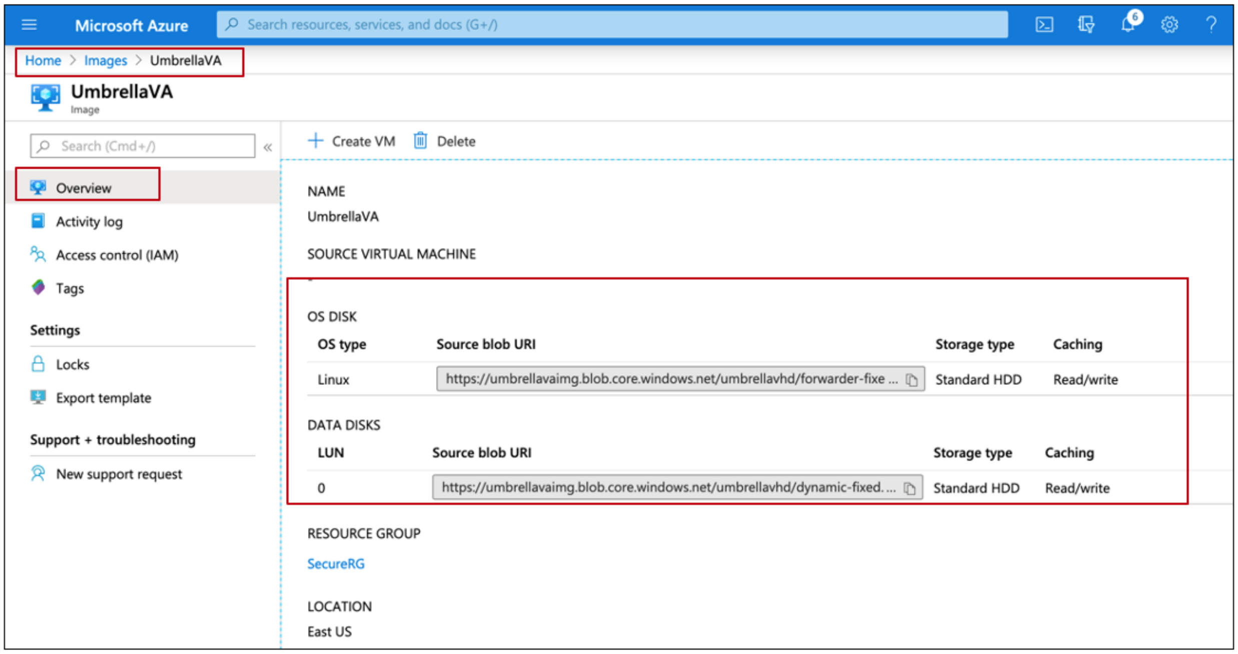
Step 2. **Create the Umbrella VA instances**

Step 3. **Configure the local DNS on Umbrella VA instances**

Step 4. **Set up the policies to exempt internal domains**

Step 5. **Update the DNS server settings for VNET**

Step 1. **Set up the Umbrella Virtual Appliance image –** Follow the Umbrella documentation to deploy Virtual appliances (VA) in the Azure cloud. As per the documentation, create an Azure Image and then use it to launch VA instances.



NAME
UmbrellaVA

SOURCE VIRTUAL MACHINE
-

OS DISK

OS type	Source blob URI	Storage type	Caching
Linux	https://umbrellavaimg.blob.core.windows.net/umbrellavhd/forwarder-fixe ...	Standard HDD	Read/write

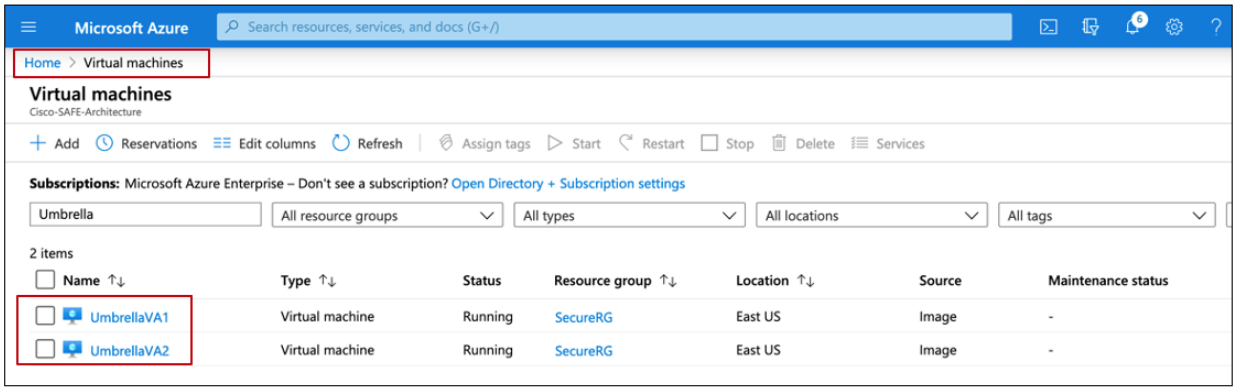
DATA DISKS

LUN	Source blob URI	Storage type	Caching
0	https://umbrellavaimg.blob.core.windows.net/umbrellavhd/dynamic-fixed. ...	Standard HDD	Read/write

RESOURCE GROUP
SecureRG

LOCATION
East US

Step 2. **Create the Umbrella VA instances –** Create two VA instances using the Azure Image set up in Step1 and place these appliances in the management tier. We assign the static IP addresses 10.83.4.100 and 10.83.4.101 to these Umbrella Virtual Appliances. These VAs will act as DNS forwarders for the resources in our Azure application environment.



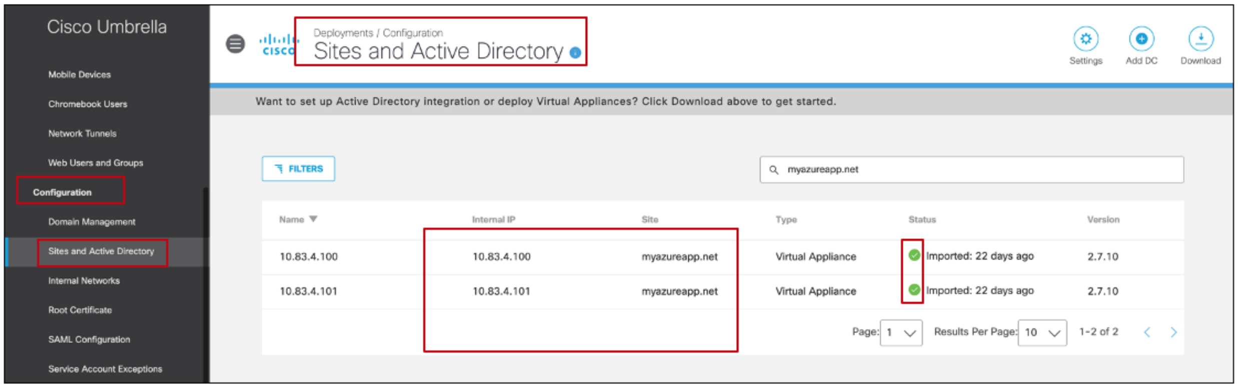
Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Open Directory + Subscription settings

Umbrella | All resource groups | All types | All locations | All tags

2 items

Name	Type	Status	Resource group	Location	Source	Maintenance status
UmbrellaVA1	Virtual machine	Running	SecureRG	East US	Image	-
UmbrellaVA2	Virtual machine	Running	SecureRG	East US	Image	-

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

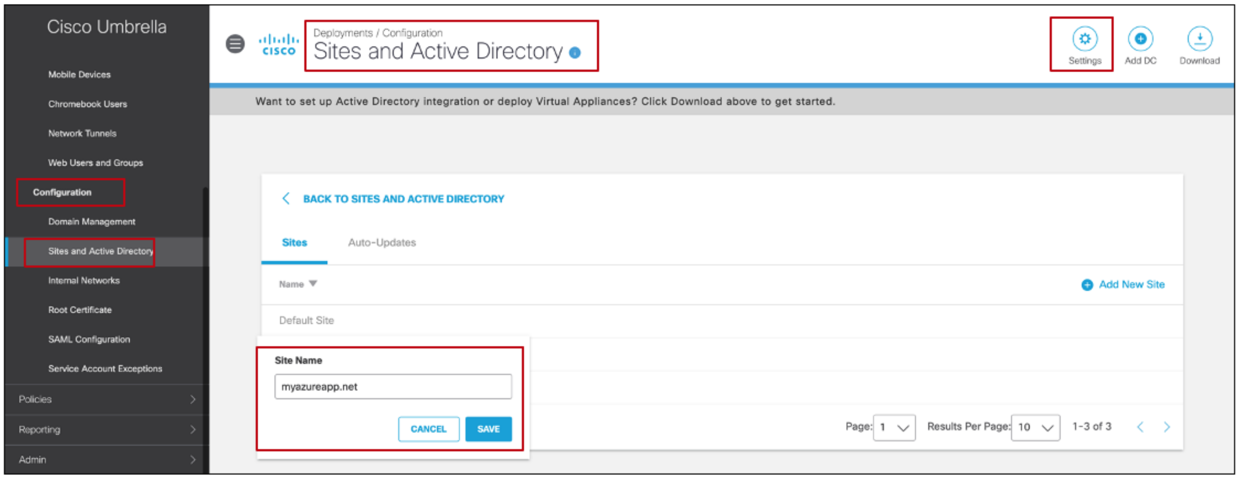


Want to set up Active Directory integration or deploy Virtual Appliances? Click Download above to get started.

Name	Internal IP	Site	Type	Status	Version
10.83.4.100	10.83.4.100	myazureapp.net	Virtual Appliance	● Imported: 22 days ago	2.7.10
10.83.4.101	10.83.4.101	myazureapp.net	Virtual Appliance	● Imported: 22 days ago	2.7.10

Page: 1 Results Per Page: 10 1-2 of 2

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

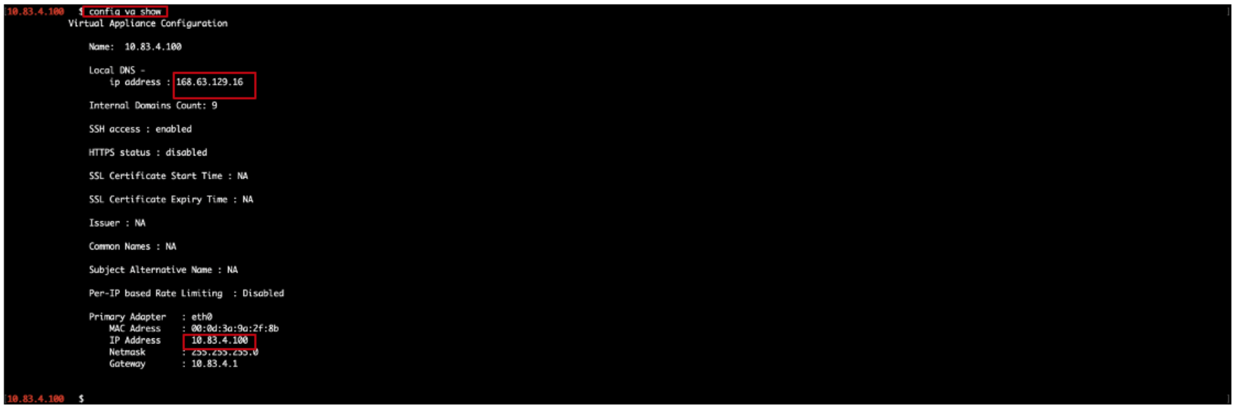


Want to set up Active Directory integration or deploy Virtual Appliances? Click Download above to get started.

Site Name: myazureapp.net

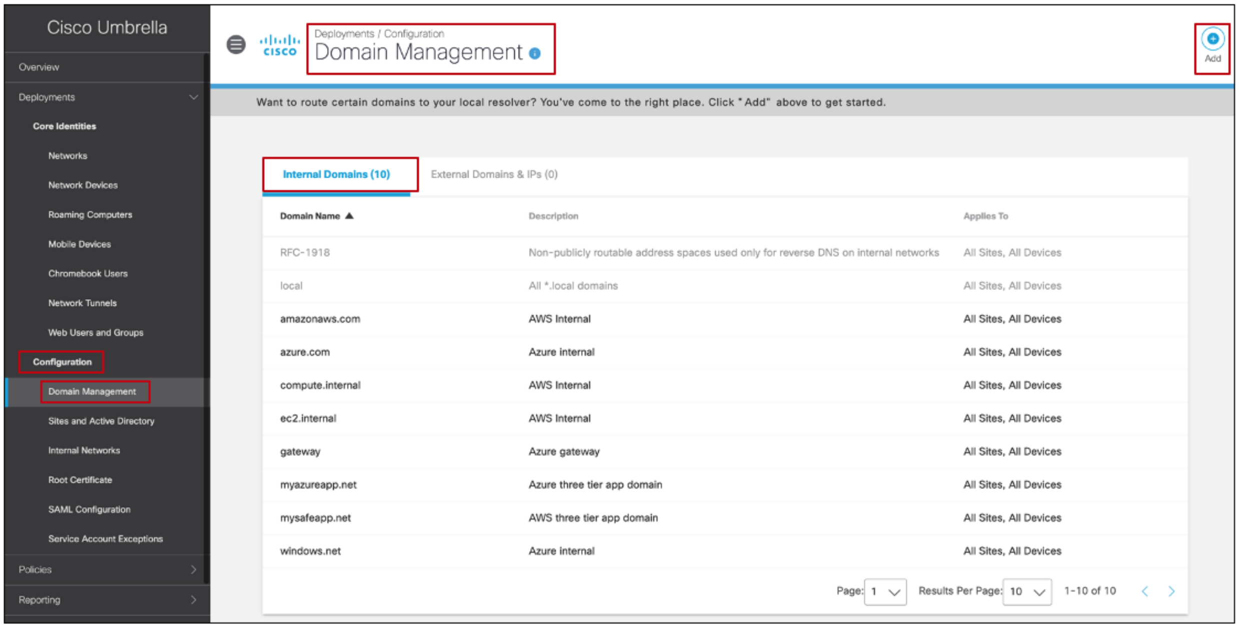
Step 3. Configure the local DNS on Umbrella Virtual Appliances - Follow the [Umbrella documentation]() to configure local DNS on each VA. Access to the recursive resolvers in Azure is provided via the virtual IP 168.63.129.16. Set this IP as local DNS on both Umbrella VAs.

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 zone.



```
10.83.4.100   $ config va show
          Virtual Appliance Configuration

             Name:  10.83.4.100

             Local DNS -
                ip address : 168.63.129.16

             Internal Domains Count: 9

             SSH access : enabled

             HTTPS status : disabled

             SSL Certificate Start Time : NA

             SSL Certificate Expiry Time : NA

             Issuer : NA

             Common Names : NA

             Subject Alternative Name : NA

             Per-IP based Rate Limiting  : Disabled

             Primary Adapter    : eth0
                MAC Adress      : 00:0d:3a:9a:2f:8b
                IP Address      : 10.83.4.100
                Netmask         : 255.255.255.0
                Gateway         : 10.83.4.1

10.83.4.100   $
```

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 Azure resolver. Based on your set up, the list of internal domains will vary.

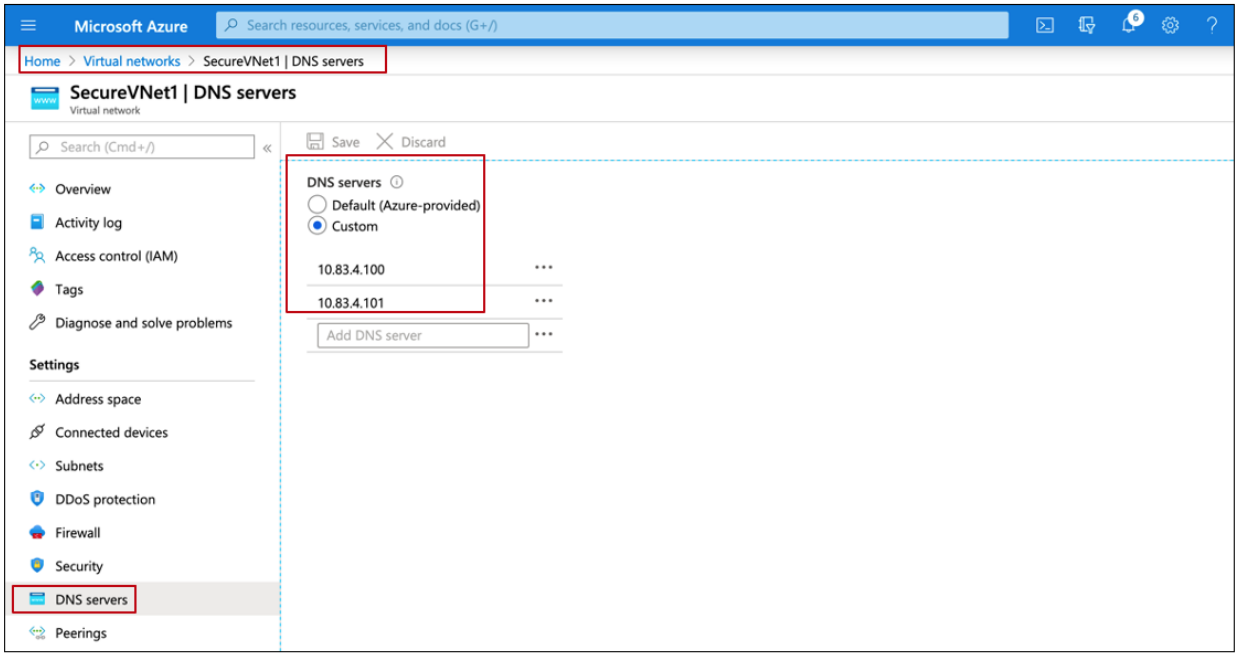


Want to route certain domains to your local resolver? You've come to the right place. Click "Add" above to get started.

Domain Name ▲	Description	Applies To
RFC-1918	Non-publicly routable address spaces used only for reverse DNS on internal networks	All Sites, All Devices
local	All *.local domains	All Sites, All Devices
amazonaws.com	AWS Internal	All Sites, All Devices
azure.com	Azure internal	All Sites, All Devices
compute.internal	AWS Internal	All Sites, All Devices
ec2.internal	AWS Internal	All Sites, All Devices
gateway	Azure gateway	All Sites, All Devices
myazureapp.net	Azure three tier app domain	All Sites, All Devices
mysafeapp.net	AWS three tier app domain	All Sites, All Devices
windows.net	Azure internal	All Sites, All Devices

Page: 1 Results Per Page: 10 1-10 of 10

Step 5. **Update the DNS server settings for VNET -** Go to the VNET that we created previously and update the 'DNS server' settings. We use the custom DNS option to add the Umbrella VA IP addresses. This will ensure that any instance deployed in this VNET is assigned the Umbrella VAs as DNS forwarders.



DNS servers
○ Default (Azure-provided)
● Custom

10.83.4.100
10.83.4.101

Setting up the Azure Database for MySQL servers

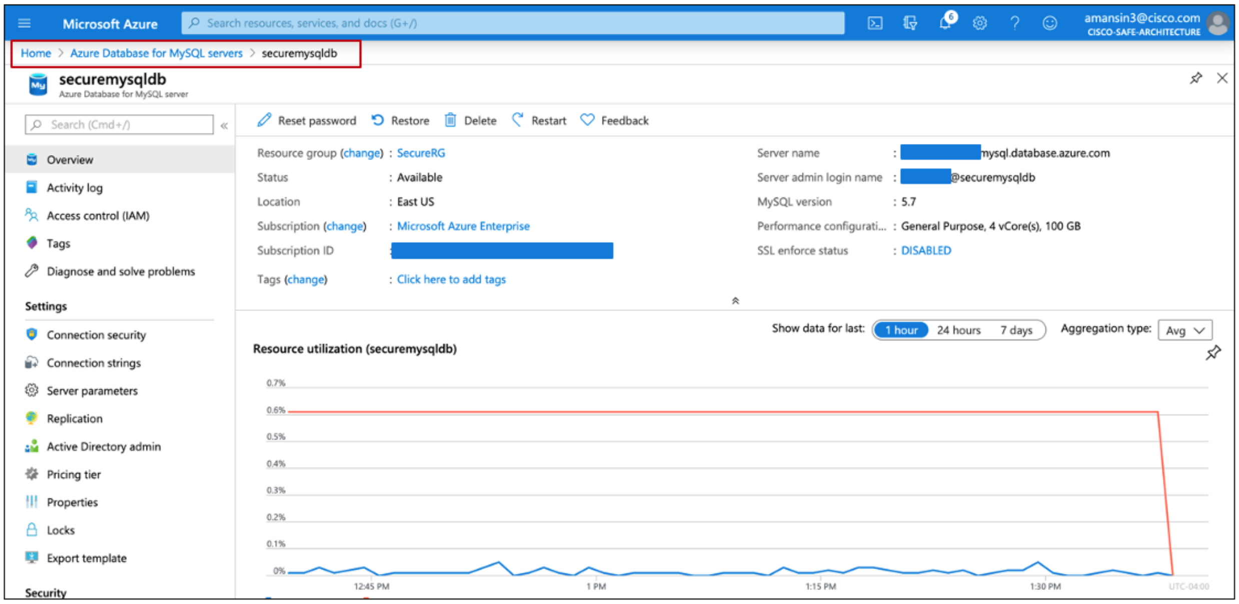
Implementation procedure:

Step 1. **Set up Azure database for MySQL server**

Step 2. **Create a private link to the database**

Step 1. **Set up Azure Database for MySQL server -** We set up an instance of MySQL database, this can vary based on application requirements. Follow the Azure documentation for help with setting up a MySQL server in Azure.

As part of the initial database set up, you will need to specify an admin username and password. Make sure you remember these credentials; we will need them while setting up the application servers for connections with the database.



Resource group (change) : SecureRG

Status : Available

Location : East US

Subscription (change) : Microsoft Azure Enterprise

Subscription ID : [redacted]

Tags (change) : Click here to add tags

Server name : [redacted]mysql.database.azure.com

Server admin login name : [redacted]@securemysqldb

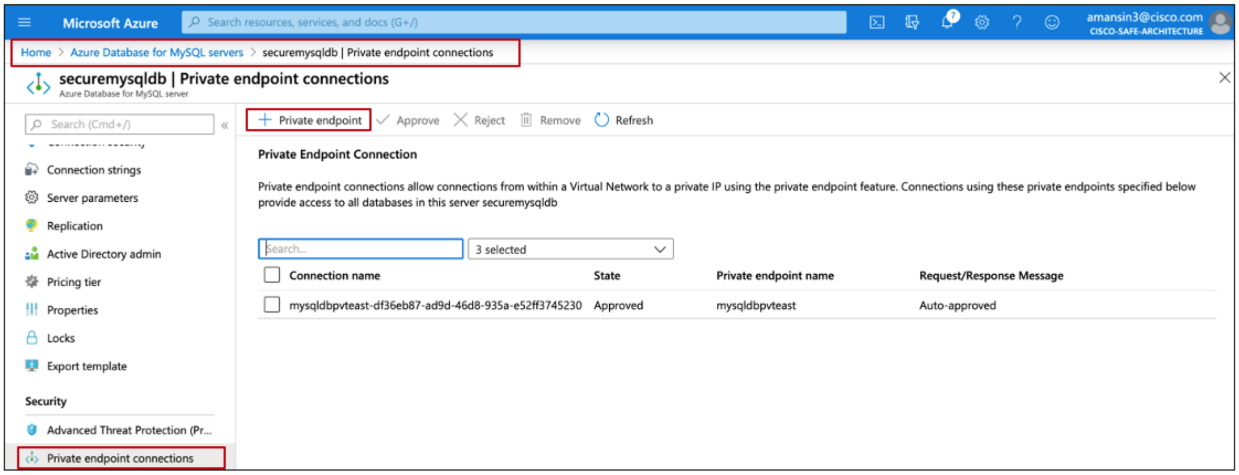
MySQL version : 5.7

Performance configurati... : General Purpose, 4 vCore(s), 100 GB

SSL enforce status : DISABLED

Step 2. **Create a Private Endpoint to the database –** Go to the newly created database under 'Azure Database for MySQL servers' and select 'Private endpoints connections' from the panel on the left-hand side. Click on '+ Private endpoint' to create a private endpoint link to this newly created MySQL database server.

Azure Private Link enables you to privately access Azure PaaS Services. This ensures that the database is not exposed to public access. This link would be set up via the database subnet and hence database NSG rules would apply. As per the default settings, inbound access from all Azure resources and unfiltered outbound access to Internet is allowed. These rules should be fined tuned to make sure that only the application subnet is allowed access to database.



Microsoft Azure
Search resources, services, and docs (G+/)
amansin3@cisco.com
CISCO-SAFE-ARCHITECTURE
Home > Azure Database for MySQL servers > securemysqldb | Private endpoint connections
securemysqldb | Private endpoint connections
Azure Database for MySQL server
Search (Cmd+/)
Connection strings
Server parameters
Replication
Active Directory admin
Pricing tier
Properties
Locks
Export template
Security
Advanced Threat Protection (Pr...
Private endpoint connections
+ Private endpoint
Approve
Reject
Remove
Refresh
Search...
3 selected

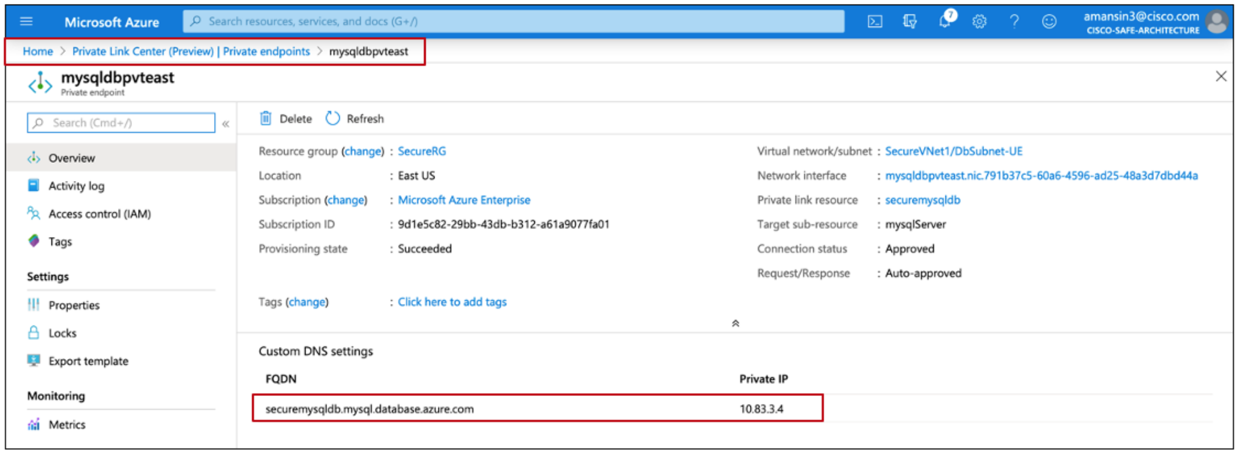
Private Endpoint Connection

Private endpoint connections allow connections from within a Virtual Network to a private IP using the private endpoint feature. Connections using these private endpoints specified below provide access to all databases in this server securemysqldb

Connection name	State	Private endpoint name	Request/Response Message
mysqldbpvteast-df36eb87-ad9d-46d8-935a-e52ff3745230	Approved	mysqldbpvteast	Auto-approved

A Private link allows DNS integration to assign an FQDN to the database server instance. This FQDN would resolve to a dynamically assigned IP address in database subnet, enabling access to the database server. Make sure you keep a note of this FQDN along with the admin username and password configured in Step 1.

You can go to the 'Private Link Center' to get detailed information about the newly created private link.



Microsoft Azure
Search resources, services, and docs (G+/)
amansin3@cisco.com
CISCO-SAFE-ARCHITECTURE
Home > Private Link Center (Preview) | Private endpoints > mysqldbpvteast

mysqldbpvteast
Private endpoint

Resource group (change) : SecureRG
Location : East US
Subscription (change) : Microsoft Azure Enterprise
Subscription ID : 9d1e5c82-29bb-43db-b312-a61a9077fa01
Provisioning state : Succeeded

Tags (change) : Click here to add tags

Virtual network/subnet : SecureVNet1/DbSubnet-UE
Network interface : mysqldbpvteast.nic.791b37c5-60a6-4596-ad25-48a3d7dbd44a
Private link resource : securemysqldb
Target sub-resource : mysqlServer
Connection status : Approved
Request/Response : Auto-approved

Custom DNS settings

FQDN	Private IP
securemysqldb.mysql.database.azure.com	10.83.3.4

Check out the Azure documentation to learn more about private links.

Setting up the Virtual Machine Scale Sets

In this section, we will set up a pool of workloads for the web and application tier. We will use the Azure Virtual Machine Scale Set (VSS) service 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.

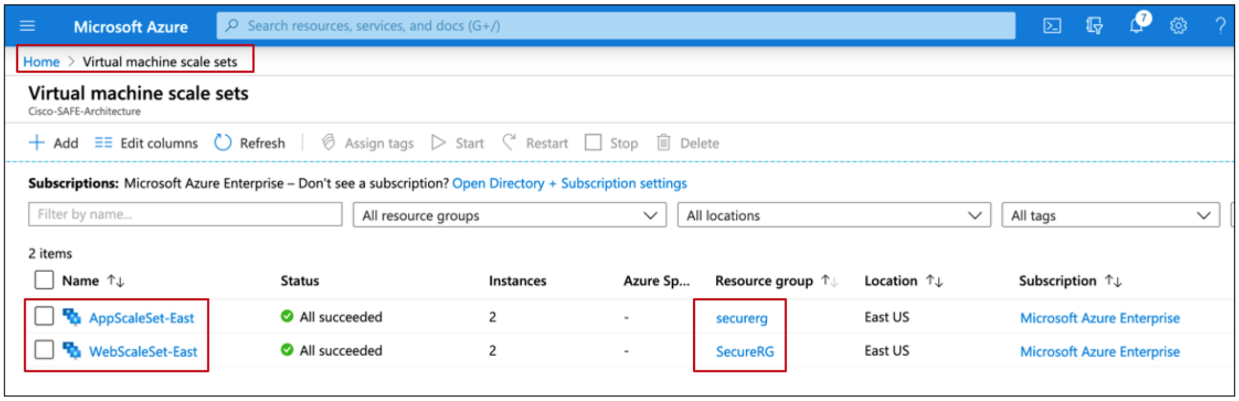
Implementation procedure:

Step 1. **Create VSS for app and web servers**

Step 2. **Install Azure VM extension for workload initialization**

Step 1. **Create VSS for app and web servers -** Go to 'Virtual Machine Scale Sets' in the Azure portal and click on 'add' to create a VSS for both web and app workloads in the Resource Group created for application.

- The geographical regions remain the same, i.e. US East
- For availability zone, make sure you check the required number of zones. Since this design is zone redundant with two availability zones, we selected zone 1 and zone 2 in US East region. This ensures that when workloads are launched in the VSS they are distributed across the two zones
- For the base image/operating system we chose CentOS, we later used custom scripts to initialize them with required packages, code and security agents. You could also use a golden image with all the required applications and packages pre-installed to skip the custom scripts. For the purpose of this document, we have validated the custom scripts option
- Under networking options, choose appropriate subnets for app and web VSS (app subnet for app VSS and web subnet for web VSS without any public IPs). Leave the Network Security Group to basic settings since we use the NSGs at subnet level.



Virtual machine scale sets
Cisco-SAFE-Architecture

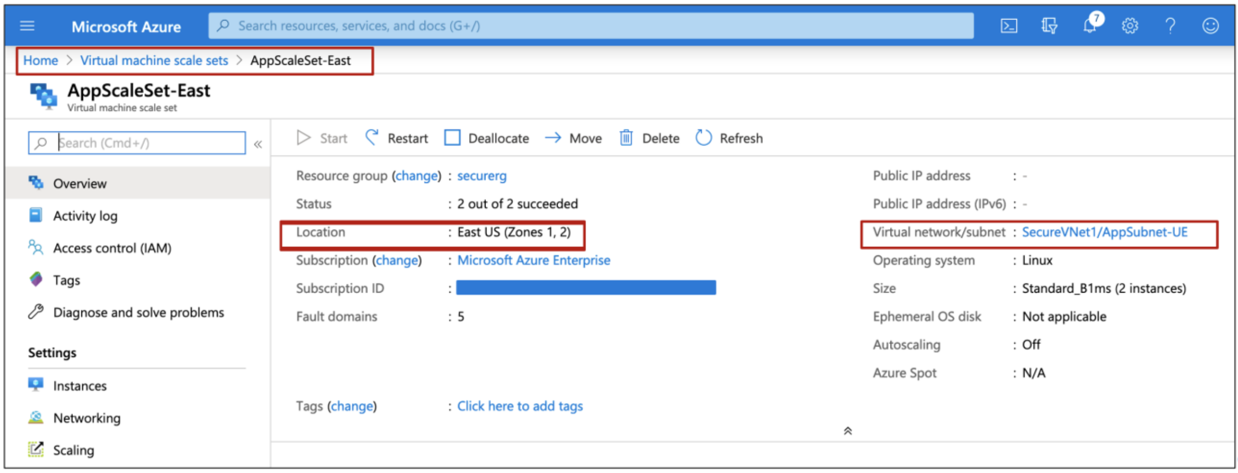
Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Open Directory + Subscription settings

2 items

Name	Status	Instances	Azure Sp...	Resource group	Location	Subscription
AppScaleSet-East	✓ All succeeded	2	-	securerg	East US	Microsoft Azure Enterprise
WebScaleSet-East	✓ All succeeded	2	-	SecureRG	East US	Microsoft Azure Enterprise

For detailed information on all other parameters regarding Virtual Machine Scale Set creation, check out the Azure documentation.

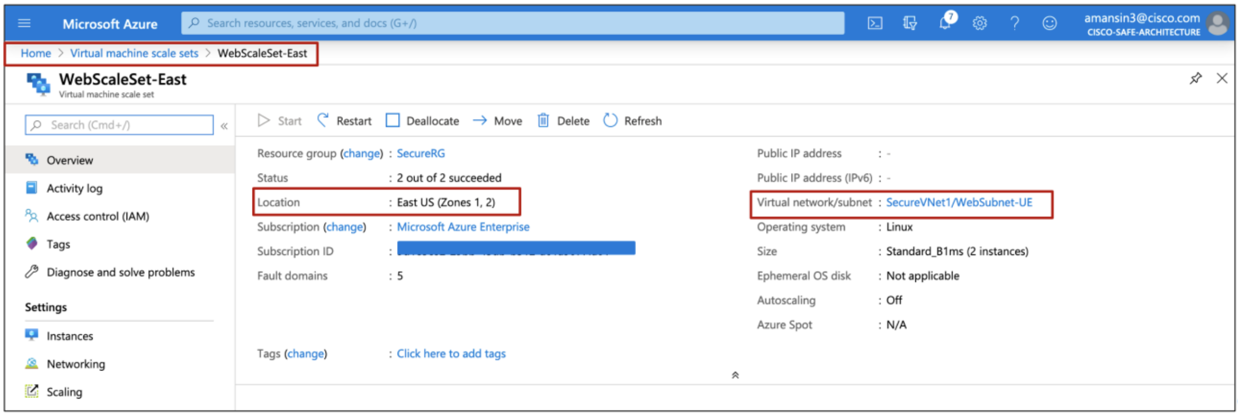
In the snapshot below for app and web VSS, you can see the location set to US east regions with redundancy in zone 1 and zone 2.



AppScaleSet-East
Virtual machine scale set

Resource group (change) : securerg
Status : 2 out of 2 succeeded
Location : East US (Zones 1, 2)
Subscription (change) : Microsoft Azure Enterprise
Subscription ID : [redacted]
Fault domains : 5
Tags (change) : Click here to add tags

Public IP address : -
Public IP address (IPv6) : -
Virtual network/subnet : SecureVNet1/AppSubnet-UE
Operating system : Linux
Size : Standard_B1ms (2 instances)
Ephemeral OS disk : Not applicable
Autoscaling : Off
Azure Spot : N/A

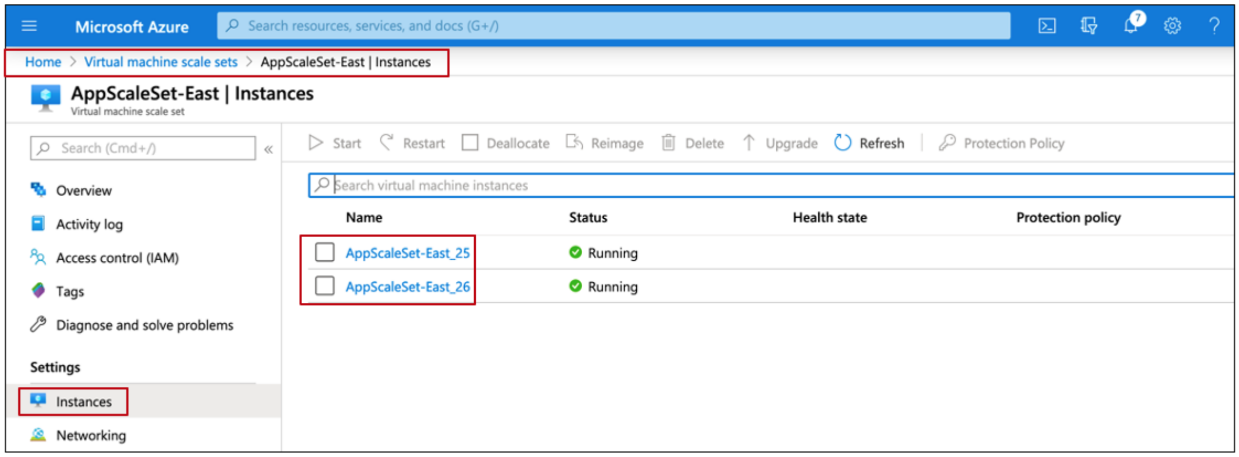


WebScaleSet-East
Virtual machine scale set

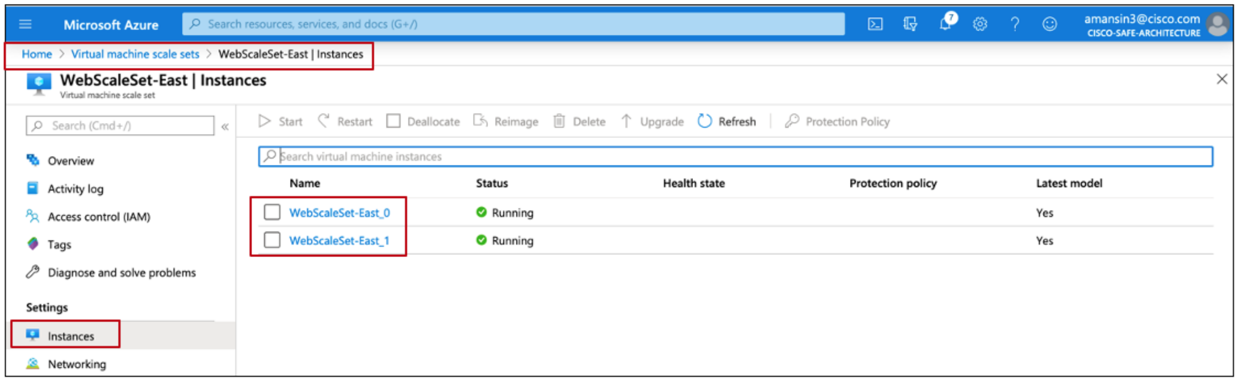
Resource group (change) : SecureRG
Status : 2 out of 2 succeeded
Location : East US (Zones 1, 2)
Subscription (change) : Microsoft Azure Enterprise
Subscription ID : [redacted]
Fault domains : 5
Tags (change) : Click here to add tags

Public IP address : -
Public IP address (IPv6) : -
Virtual network/subnet : SecureVNet1/WebSubnet-UE
Operating system : Linux
Size : Standard_B1ms (2 instances)
Ephemeral OS disk : Not applicable
Autoscaling : Off
Azure Spot : N/A

At this point, we have two base workloads each, in app and web VSS. We haven’t set up the application on these workloads yet, we will do that in our next step.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual machine scale sets > AppScaleSet-East | Instances
AppScaleSet-East | Instances
Virtual machine scale set
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Instances
Networking
Start
Restart
Deallocate
Reimage
Delete
Upgrade
Refresh
Protection Policy
Search virtual machine instances

Name	Status	Health state	Protection policy
□ AppScaleSet-East_25	✓ Running		
□ AppScaleSet-East_26	✓ Running		


Microsoft Azure
Search resources, services, and docs (G+/)
amansin3@cisco.com
CISCO-SAFE-ARCHITECTURE
Home > Virtual machine scale sets > WebScaleSet-East | Instances
WebScaleSet-East | Instances
Virtual machine scale set
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Instances
Networking
Start
Restart
Deallocate
Reimage
Delete
Upgrade
Refresh
Protection Policy
Search virtual machine instances

Name	Status	Health state	Protection policy	Latest model
□ WebScaleSet-East_0	✓ Running			Yes
□ WebScaleSet-East_1	✓ Running			Yes

Step 2. **Install Azure VM extension for workload initialization –** We set up a ‘Storage Account’ in US East region, same region as our application location. We upload all the files that we need for our application and web workloads into this storage account. If you choose to host config files in this manner, ensure that you set appropriate access privileges for these files.

These files include:

- Shell scripts (appservers and webservers) for initializing the application and web workloads
- Config files for our application and web workloads
    - App workloads – App configuration file has information about database connection (we recorded the details for this while setting up database previously).
    - Web workloads – Along with various other details, the web config file has the IP address of app VSS load balancer. We set apart the IP- 10.83.2.100 for the app load balancer. We haven’t created the load balancers yet; we will do that in the next step and assign them the IPs
- AMP4E agent installer (AMP rpm and GPG). These were obtained from AMP portal
- Tetration agent installer (Enforcer and visibility). These are downloaded from Tetration portal

The initialization shell scripts 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 configuration files/code for the respective workloads.
  - For the application server, we used a publicly available ‘WordPress’ blog code. We download the zipped code from the WordPress site and then update the database config file from Azure Storage Account we set up above.
  - For web server, download the modified web configuration file from Azure Storage Account we set up above.
- Download and unzip the Duo plugin (available for ‘WordPress’ blogs) to the application workloads.
- Download and install the Tetration enforcement agent from Azure Storage Account we set up above.
- Download and install the AMP4E agent from Azure Storage Account we set up above.

Note: If you choose to include the Duo integration in your native application, follow the DUO Web SDK documentation.

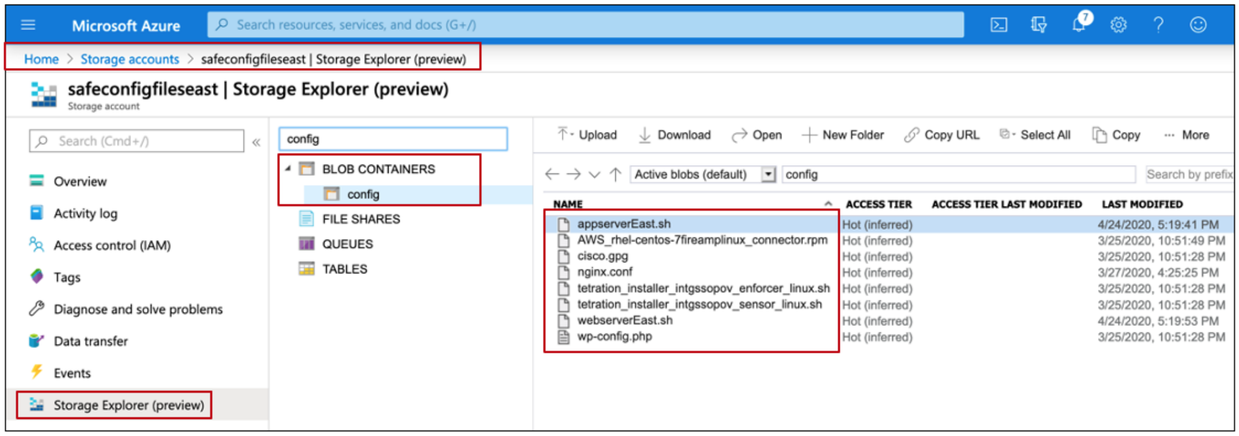
Below are sample initialization scripts that we used.

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.blob.core.windows.net/config/nginx.conf
sudo systemctl restart nginx
sudo systemctl enable nginx

#Downloading the Tetration enforcement agent from Azure Storage account and installing it.
sudo wget https://
safelabfiles.blob.core.windows.net/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 Azure Storage account and installing it.
sudo wget https:// safelabfiles.blob.core.windows.net/config/cisco.gpg
sudo rpm --import ./cisco.gpg
sudo wget https:// safelabfiles.blob.core.windows.net/config/AWS_rhel-centos-
7fireamplinux_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 Azure Storage Account.
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
cd /home/centos/
sudo systemctl restart httpd

#Downloading the Tetration enforcement agent from Azure Storage Account and installing it.
sudo wget https://safelabfiles.blob.core.windows.net/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 Azure Storage Account and installing it.
sudo wget https://safelabfiles.blob.core.windows.net/config/cisco.gpg
sudo rpm --import ./cisco.gpg
sudo wget https://safelabfiles.blob.core.windows.net/config/AWS_rhel-centos-7fireamplinux_connector.rpm
sudo yum install -y AWS_rhel-centos-7fireamplinux_connector.rpm
```

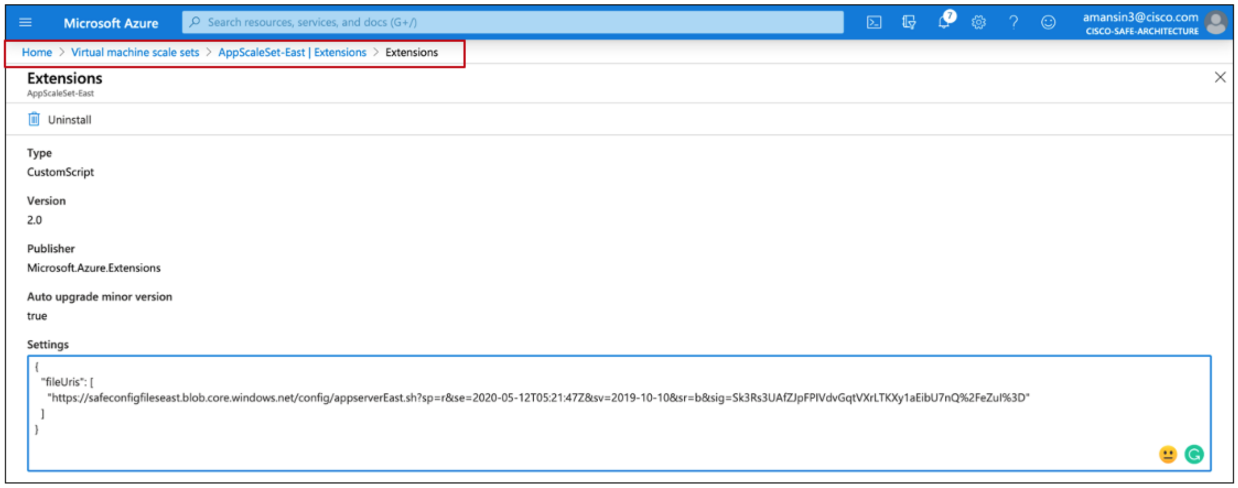


Home > Storage accounts > safeconfigfileseast | Storage Explorer (preview)

safeconfigfileseast | Storage Explorer (preview)
Storage account

NAME	ACCESS TIER	ACCESS TIER LAST MODIFIED	LAST MODIFIED
appserverEast.sh	Hot (inferred)		4/24/2020, 5:19:41 PM
AWS_rhel-centos-7fireamplinux_connector.rpm	Hot (inferred)		3/25/2020, 10:51:49 PM
cisco.gpg	Hot (inferred)		3/25/2020, 10:51:28 PM
nginx.conf	Hot (inferred)		3/27/2020, 4:25:25 PM
tetration_installer_intgssopov_enforcer_linux.sh	Hot (inferred)		3/25/2020, 10:51:28 PM
tetration_installer_intgssopov_sensor_linux.sh	Hot (inferred)		3/25/2020, 10:51:28 PM
webserverEast.sh	Hot (inferred)		4/24/2020, 5:19:53 PM
wp-config.php	Hot (inferred)		3/25/2020, 10:51:28 PM

Now that we have all the files hosted in Azure Storage Account, we will install the extensions. Go to 'Virtual Machine Scale Sets > [app VSS] > Extensions' and click on add. Choose 'Custom Script for Linux' from the panel on the left-hand side. Create the extension by choosing the web shell script from the Azure Storage Account we created earlier.



Home > Virtual machine scale sets > AppScaleSet-East | Extensions > Extensions

Extensions
AppScaleSet-East

Type
CustomScript

Version
2.0

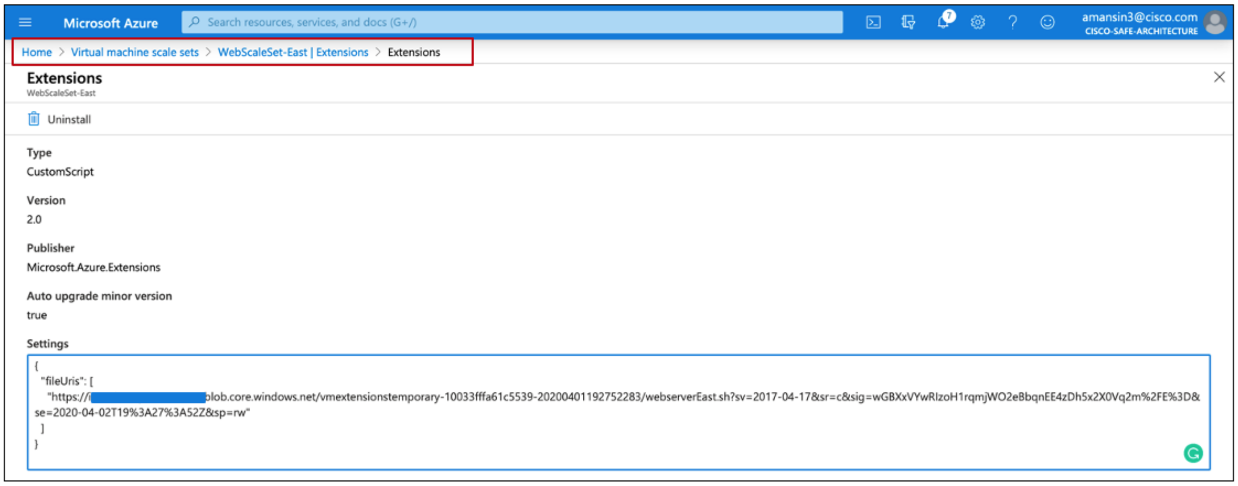
Publisher
Microsoft.Azure.Extensions

Auto upgrade minor version
true

Settings

```
{
  "fileUris": [
    "https://safeconfigfileseast.blob.core.windows.net/config/appserverEast.sh?sp=r&se=2020-05-12T05:21:47Z&sv=2019-10-10&sr=b&sig=Sk3Rs3UAfZJpFPlVdvGqtVXrLTKXy1aEibU7nQ%2FeZul%3D"
  ]
}
```

After adding the extension, go back to VSS and make sure you select all the running instances and click on upgrade to finish the installation.



Home > Virtual machine scale sets > WebScaleSet-East | Extensions > Extensions

Extensions
WebScaleSet-East

Type
CustomScript

Version
2.0

Publisher
Microsoft.Azure.Extensions

Auto upgrade minor version
true

Settings

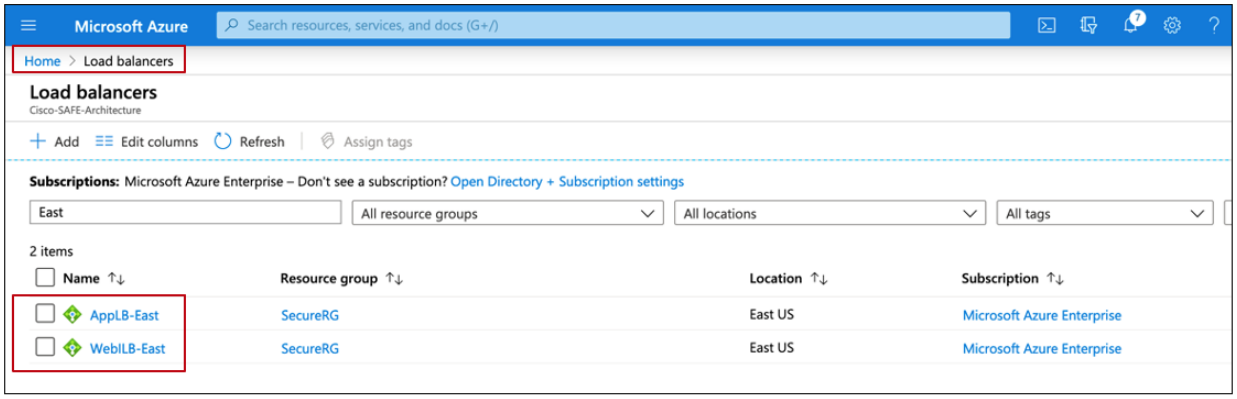
```
{
  "fileUris": [
    "https://[redacted]blob.core.windows.net/vmextensionstemporary-10033fffa61c5539-20200401192752283/webserverEast.sh?sv=2017-04-17&sr=c&sig=wGBXxVYwRlzoH1rqmjWO2eBbqnEE4zDh5x2X0Vq2m%2FE%3D&
se=2020-04-02T19%3A27%3A52Z&sp=rw"
  ]
}
```

Repeat the same steps for web VSS.

Setting up the App and Web load balancers

At this point we have a highly available pool of web and app workloads running in the corresponding Virtual Machine Scale Sets in web and app tier. Now, we need to create load balancers to load balance traffic onto these two Virtual Machine Scale Sets. We will create a web load balancer in web tier which receives web traffic from users and then load balances it onto the web servers running in web VSS in the Web tier. We will also create an app load balancer sitting in front of the app workloads in the App tier. When the Nginx web servers in web VSS receive web requests from web load balancer, they will forward them to app load balancer to be distributed onto the app workloads in app VSS.

Go to 'Azure load balancer' service and click on 'add' to create the web and app load balancer. Make sure you select the type as 'Internal' and SKU as 'Standard'. We need 'Standard' SKU to be able to integrate these load balancers with the zone redundant Virtual Machine Scale Sets.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancers

Load balancers
Cisco-SAFE-Architecture

+ Add | Edit columns | Refresh | Assign tags

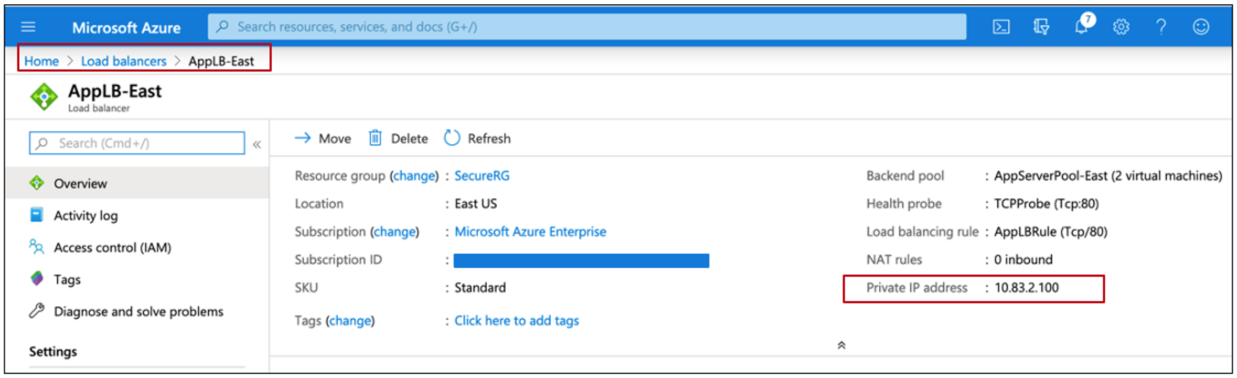
Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Open Directory + Subscription settings

East | All resource groups | All locations | All tags

2 items

Name	Resource group	Location	Subscription
□ AppLB-East	SecureRG	East US	Microsoft Azure Enterprise
□ WebILB-East	SecureRG	East US	Microsoft Azure Enterprise

We assigned these load balancers with static IPs 10.83.1.100 and 10.83.2.100 in web and app subnet respectively. We had specified 10.83.2.100 in our web server configuration file in the previous step; hence web servers would make the requests to app load balancer IP if they need to fetch any dynamic content from app servers.

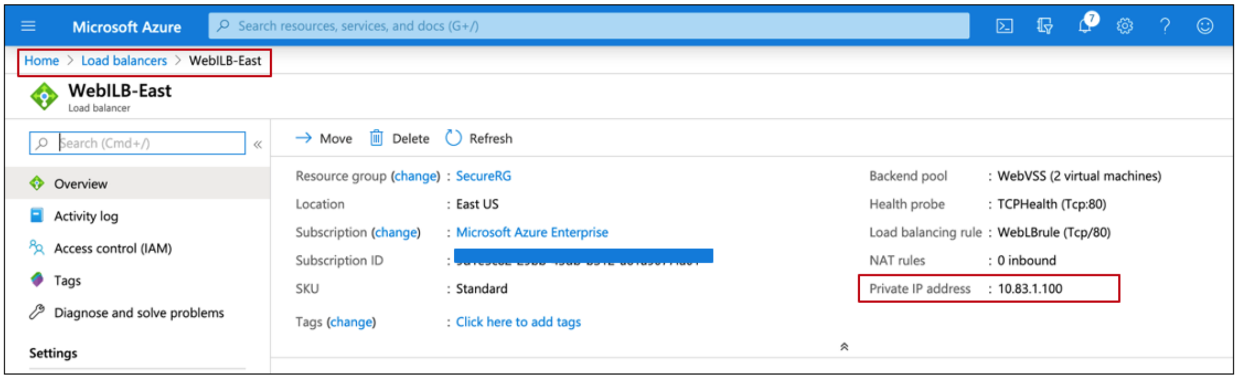


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancers > AppLB-East

AppLB-East
Load balancer

Resource group (change)	: SecureRG
Location	: East US
Subscription (change)	: Microsoft Azure Enterprise
Subscription ID	: [redacted]
SKU	: Standard
Tags (change)	: Click here to add tags

Backend pool	: AppServerPool-East (2 virtual machines)
Health probe	: TCPProbe (Tcp:80)
Load balancing rule	: AppLBRule (Tcp/80)
NAT rules	: 0 inbound
Private IP address	: 10.83.2.100



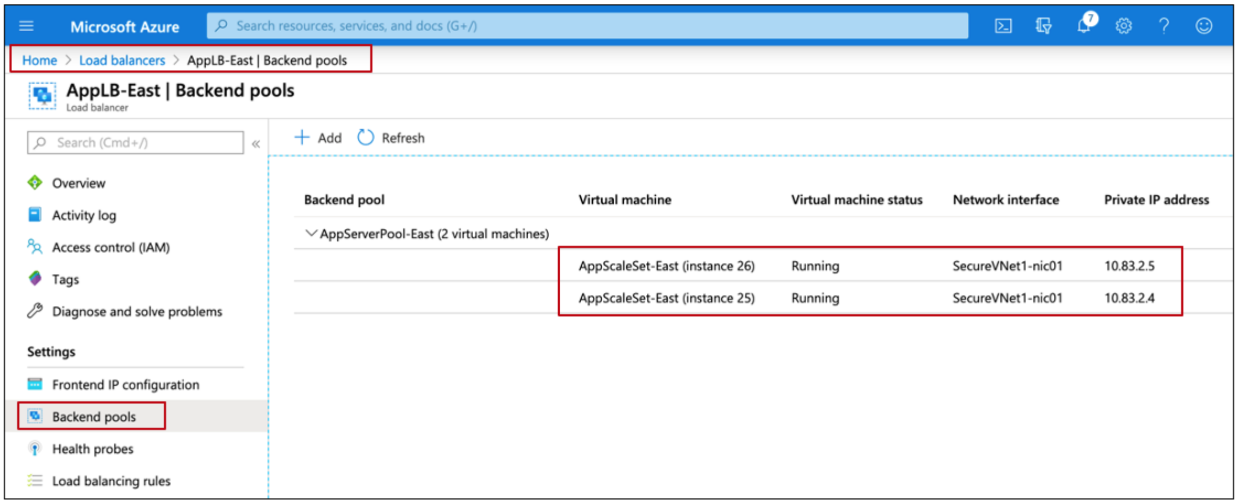
Home > Load balancers > WebILB-East

WebILB-East
Load balancer

Resource group (change)	: SecureRG	Backend pool	: WebVSS (2 virtual machines)
Location	: East US	Health probe	: TCPHealth (Tcp:80)
Subscription (change)	: Microsoft Azure Enterprise	Load balancing rule	: WebLBrule (Tcp/80)
Subscription ID	: [redacted]	NAT rules	: 0 inbound
SKU	: Standard	Private IP address	: 10.83.1.100
Tags (change)	: Click here to add tags		

To finish our load balancer configuration, we need to add the backend pool, health probes and load balancing rules. For backend pools, we will add corresponding VSS for each load balancer. Make sure to upgrade VSS instances once the load balancer configuration is finished.

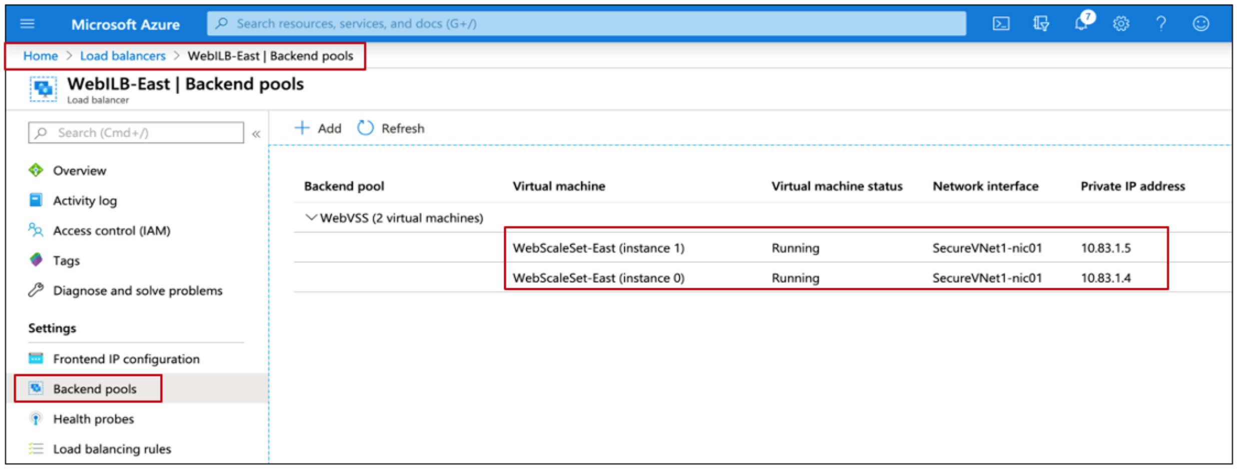
Refer to the Azure documentation for detailed steps on how to set up internal load balancers. Once the backend pool, the health probes and load balancing rules as set up, the app and web VSS instances would show as below under the load balancer service.



Home > Load balancers > AppLB-East | Backend pools

AppLB-East | Backend pools
Load balancer

Backend pool	Virtual machine	Virtual machine status	Network interface	Private IP address
AppServerPool-East (2 virtual machines)				
	AppScaleSet-East (instance 26)	Running	SecureVNet1-nic01	10.83.2.5
	AppScaleSet-East (instance 25)	Running	SecureVNet1-nic01	10.83.2.4



Home > Load balancers > WebILB-East | Backend pools

WebILB-East | Backend pools
Load balancer

Backend pool	Virtual machine	Virtual machine status	Network interface	Private IP address
WebVSS (2 virtual machines)				
	WebScaleSet-East (instance 1)	Running	SecureVNet1-nic01	10.83.1.5
	WebScaleSet-East (instance 0)	Running	SecureVNet1-nic01	10.83.1.4

Setting up the Firepower Next-Generation Firewalls

In this section of the document, 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. You could also use Cisco FMC (Firepower Management Center) available via the Azure marketplace (or an on-premise FMC) for management purposes.

Once the firewalls are set up, we will expose our application to public Internet via an External Azure load balancer. We will also set up an Internal Azure load balancer and update the App and Web tier routing tables to load-balance the outbound traffic from workloads to the Next-Generation Firewalls.

Implementation procedure:

Step 1. Deploy NGFWv using Azure Templates

Step 2. Onboard the NGFWv to CDO

Step 3. Configure interfaces, routes, health probes, NAT and access control on NGFWv

Step 4. Set up the inside and outside load balancers

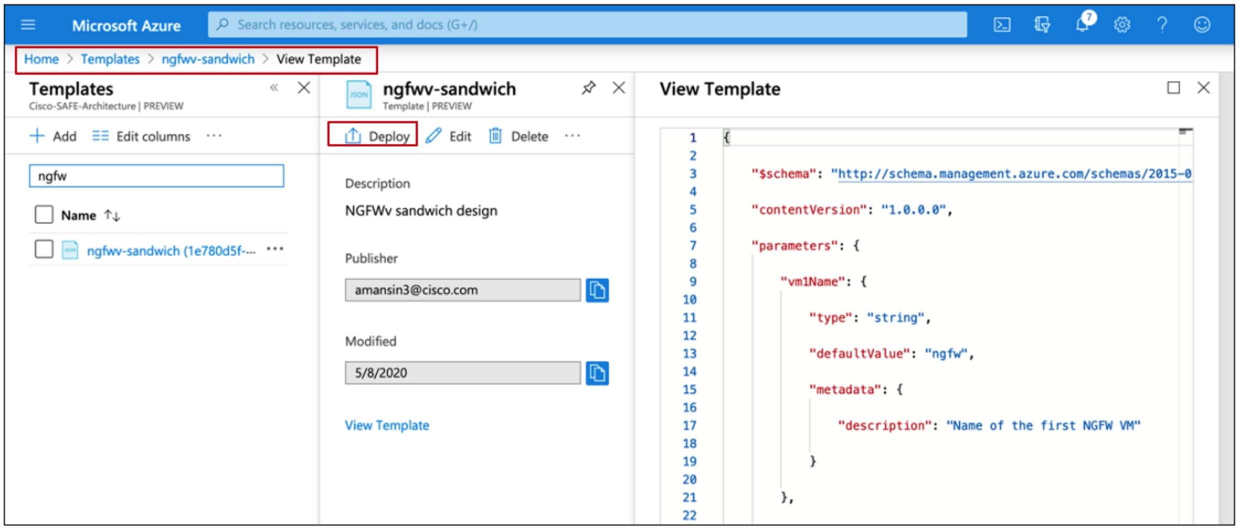
Step 5. Access the application

Step 1. Deploy NGFWv using Azure templates – Download the NGFW template available at GitHub. Go to 'Azure Templates' service on the Azure portal and add this template to deploy two Cisco Firepower Next-Generation Firewalls. Once you click on deploy, you will need to provide the IP addresses; we used the following IP addressing.

NGFWv	Interface Name	IPV4 Address	Azure NIC	Firepower Interface
Safengfw1	Management	10.83.4.10	NIC0	Management
Safengfw1	Diagnostic	10.83.7.10	NIC1	Diagnostic
Safengfw1	Inside	10.83.5.10	NIC2	Gig0/0
Safengfw1	Outside	10.83.6.10	NIC3	Gig0/1
Safengfw2	Management	10.83.4.11	NIC0	Management
Safengfw2	Diagnostic	10.83.7.11	NIC1	Diagnostic
Safengfw2	Inside	10.83.5.11	NIC2	Gig0/0
Safengfw2	Outside	10.83.6.11	NIC3	Gig0/1

Other details that you would be prompted for, while deploying the FTDs, include Resource Group (same as our cloud application), location (US East), hostname (safengfw1 and safengfw2), access credentials, storage accounts for firewalls (Storage-General purpose V1/LRS), Virtual Network (same VNET that we created earlier for the web application) and an Availability Set.

You will need to create an availability set prior to deploying this template and specify it when prompted. Refer to Azure documentation for information on how to create an Availability Set.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Templates > ngfwv-sandwich > View Template
Templates
Cisco-SAFE-Architecture | PREVIEW
+ Add
Edit columns
Name ↑↓
ngfwv-sandwich (1e780d5f-...
ngfwv-sandwich
Template | PREVIEW
Deploy
Edit
Delete
View Template
View Template

ngfw

Description

NGFWv sandwich design

Publisher

amansin3@cisco.com

Modified

5/8/2020

```
{

    "$schema": "http://schema.management.azure.com/schemas/2015-0

    "contentVersion": "1.0.0.0",

    "parameters": {

        "vm1Name": {

            "type": "string",

            "defaultValue": "ngfw",

            "metadata": {

                "description": "Name of the first NGFW VM"

            }

        },

```

You can also customize the GitHub template to deploy the FTDs in different Availability Zones instead of an Availability Set. You will need to 'Edit' the JSON template file to remove Availability Set configuration and specify the Availability Zone for each NGFWv. Most of this lab validation was carried out using Availability Set, but we also validated the Availability Zones.

Note: An Availability Set ensures that the firewalls are deployed on separate hardware. The Availability Zones (AZ) on the other hand are two separate physical locations in the same region, connected with a high-speed link.

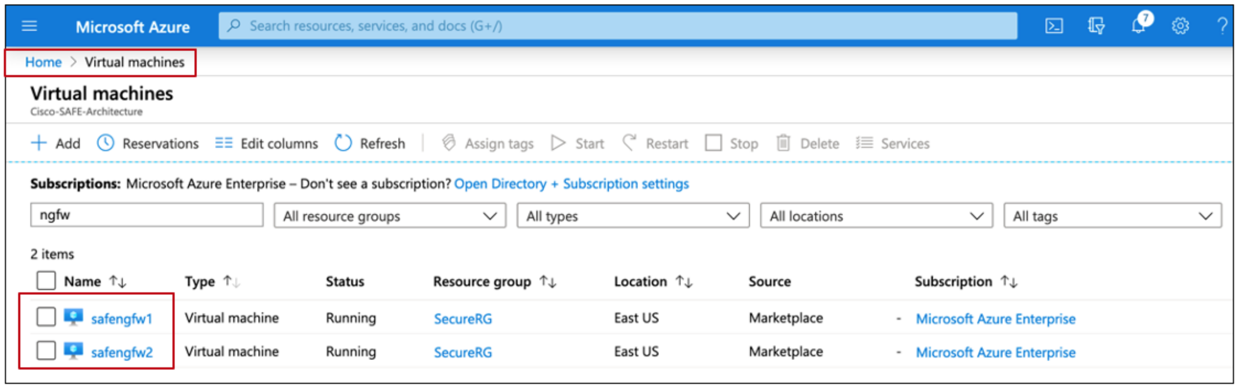
The sample template config snippet to add Availability Zones is as below:

```
"apiVersion": "2017-12-01",
"type": "Microsoft.Compute/virtualMachines",
"name": "[parameters('vm1Name')]",
"zones": [ "1"],

"apiVersion": "2017-12-01",
"type": "Microsoft.Compute/virtualMachines",
"name": "[parameters('vm2Name')]",
"zones": [ "2"],
```

You will also need to remove the following Availability Set config from the downloaded GitHub template:

```
Parameters Section:
"availabilitySetResourceGroup": {
  "type": "string",
  "defaultValue": "",
  "metadata": {
    "description": "Name of the existing Availability Set's Resource Group"
    }
},
"availabilitySetName": {
  "type": "string",
  "defaultValue": "",
  "metadata": {
  "description": "Name of the existing Availability Set"
  }
},
Resources Section:
"availabilitySet": {
  "id":
"[resourceId(parameters('availabilitySetResourceGroup'),'Microsoft.Compute/availabilitySets/
', parameters('availabilitySetName'))]"
},
```

After a successful template deployment, the FTDs would show as below.



Virtual machines

Cisco-SAFE-Architecture

Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Open Directory + Subscription settings

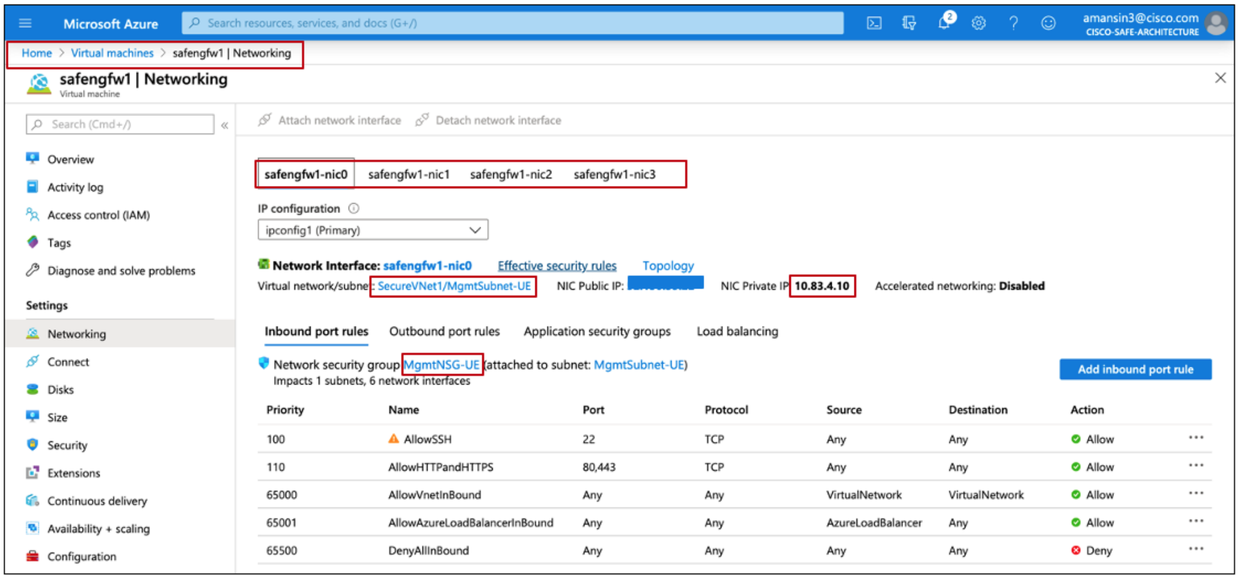
ngfw | All resource groups | All types | All locations | All tags

2 items

□ Name ↑↓	Type ↑↓	Status	Resource group ↑↓	Location ↑↓	Source	Subscription ↑↓
□ safengfw1	Virtual machine	Running	SecureRG	East US	Marketplace	- Microsoft Azure Enterprise
□ safengfw2	Virtual machine	Running	SecureRG	East US	Marketplace	- Microsoft Azure Enterprise

Each Firewall should have four network interfaces, assigned with IP addresses as specified in template while deploying.

The Management interface will be assigned a public IP address automatically, we will use this IP to do the initial set up of these newly deployed instances. Additionally, associate a public IP to NIC3 (outside interface) of each firewall manually. Follow the Azure documentation for instructions.



IP configuration: ipconfig1 (Primary)

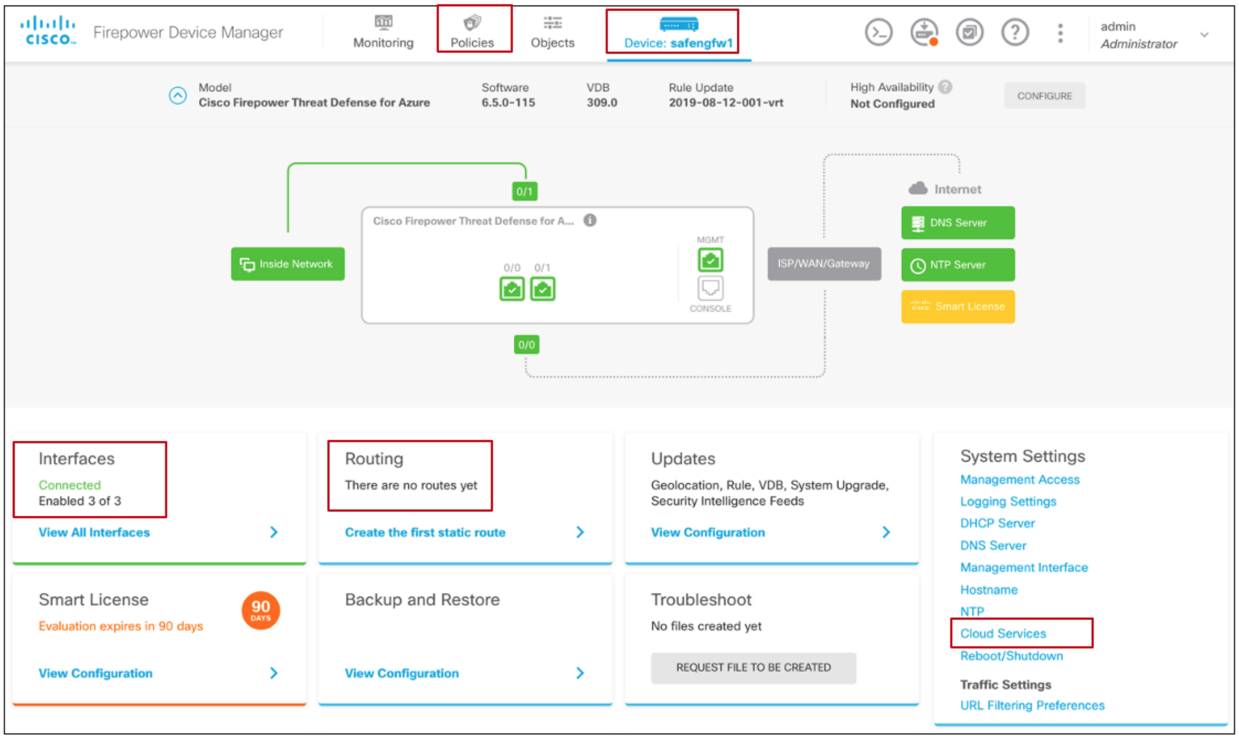
Network Interface: safengfw1-nic0 Effective security rules Topology

Virtual network/subnet: SecureVNet1/MgmtSubnet-UE NIC Public IP: [redacted] NIC Private IP 10.83.4.10 Accelerated networking: **Disabled**

Network security group MgmtNSG-UE (attached to subnet: MgmtSubnet-UE)
Impacts 1 subnets, 6 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ AllowSSH	22	TCP	Any	Any	✓ Allow
110	AllowHTTPandHTTPS	80,443	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Step 2. **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 following page.



Model: Cisco Firepower Threat Defense for Azure
Software: 6.5.0-115
VDB: 309.0
Rule Update: 2019-08-12-001-vrt
High Availability: Not Configured

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

System Settings
Management Access
Logging Settings
DHCP Server
DNS Server
Management Interface
Hostname
NTP
Cloud Services
Reboot/Shutdown

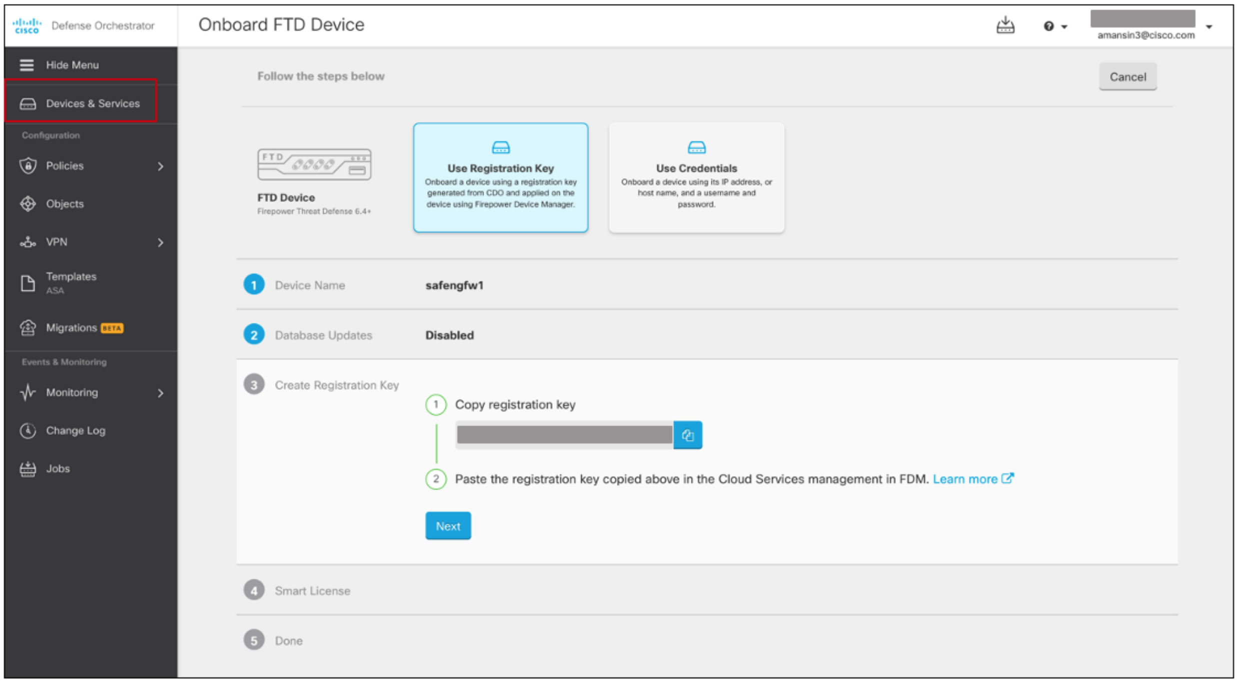
Traffic Settings
URL Filtering Preferences

Smart License
Evaluation expires in 90 days
View Configuration

Backup and Restore
View Configuration

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

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.



Onboard FTD Device

[redacted]
amansin3@cisco.com

Follow the steps below

FTD Device
Firepower Threat Defense 6.4+

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Credentials
Onboard a device using its IP address, or host name, and a username and password.

1 Device Name **safengfw1**

2 Database Updates **Disabled**

3 Create Registration Key

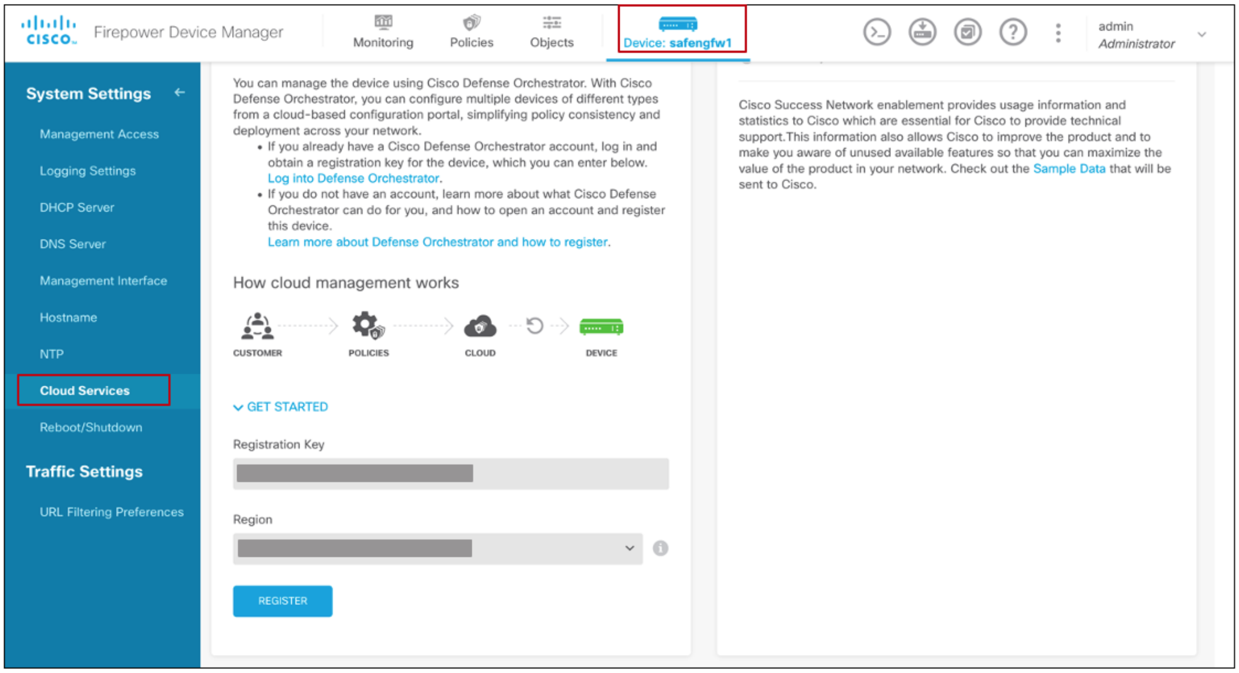
1. Copy registration key
   [redacted]
2. Paste the registration key copied above in the Cloud Services management in FDM. Learn more

Next

4 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.



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 open an account and register this device. Learn more about Defense Orchestrator and how to register.

How cloud management works

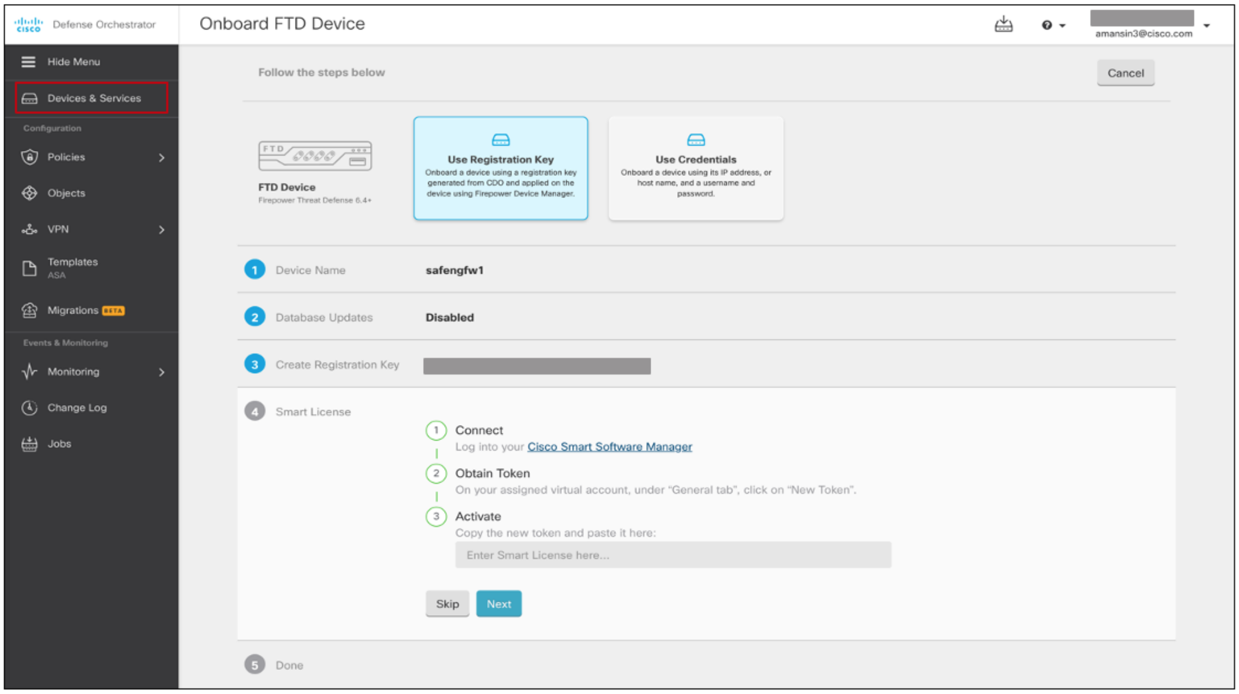
GET STARTED

Registration Key
[redacted]

Region
[redacted]

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the Sample Data that will be sent to Cisco.

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.



Onboard FTD Device

Follow the steps below

FTD Device
Firepower Threat Defense 6.4+

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Credentials
Onboard a device using its IP address, or host name, and a username and password.

1 Device Name **safengfw1**

2 Database Updates **Disabled**

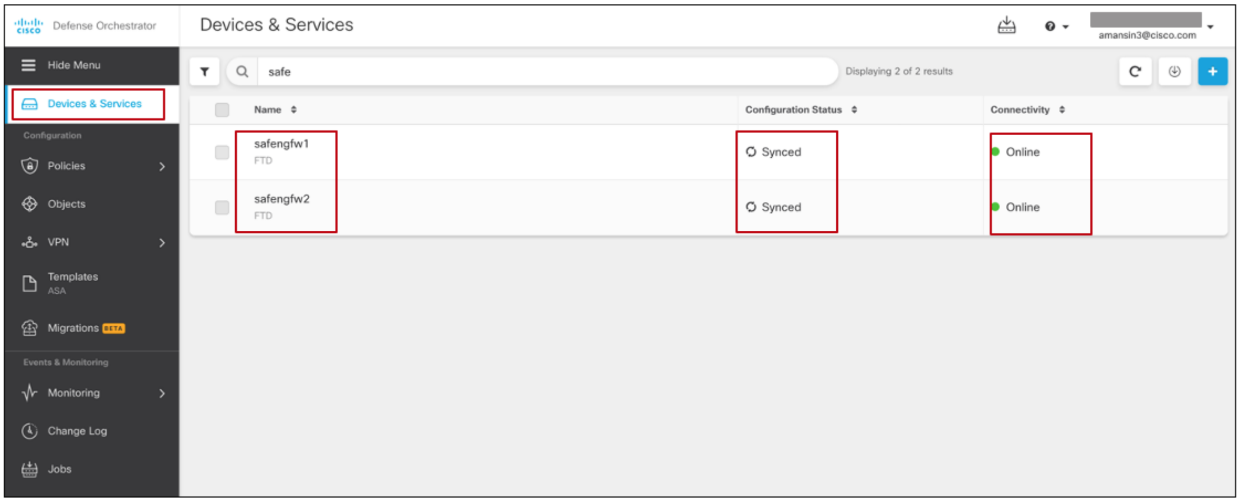
3 Create Registration Key [redacted]

4 Smart License

1. Connect
   Log into your Cisco Smart Software Manager
2. Obtain Token
   On your assigned virtual account, under "General tab", click on "New Token".
3. Activate
   Copy the new token and paste it here:
   Enter Smart License here...

5 Done

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.



Devices & Services

safe

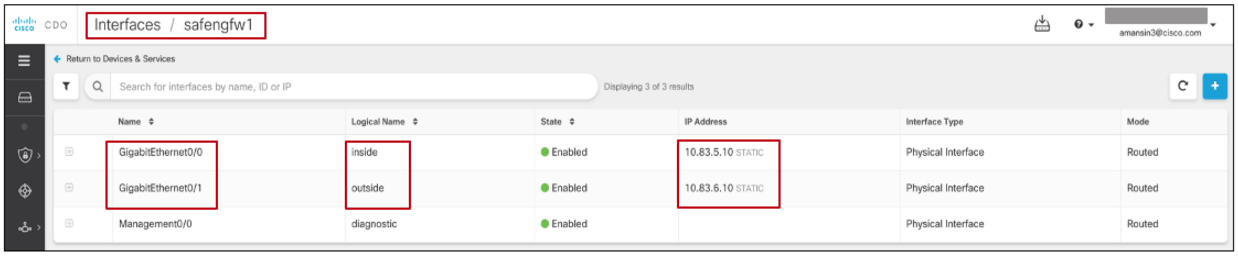
Displaying 2 of 2 results

Name	Configuration Status	Connectivity
safengfw1 FTD	Synced	Online
safengfw2 FTD	Synced	Online

Step 3. Configure interfaces, routes, HTTPS health probes, NAT and access control on NGFWv – We need to configure the following five components:

- Network interfaces
- Static routes
- Enable HTTPS on inside and outside interface for load balancer probes
- NAT rules for inbound and outbound traffic
- Access rules to allow the necessary traffic

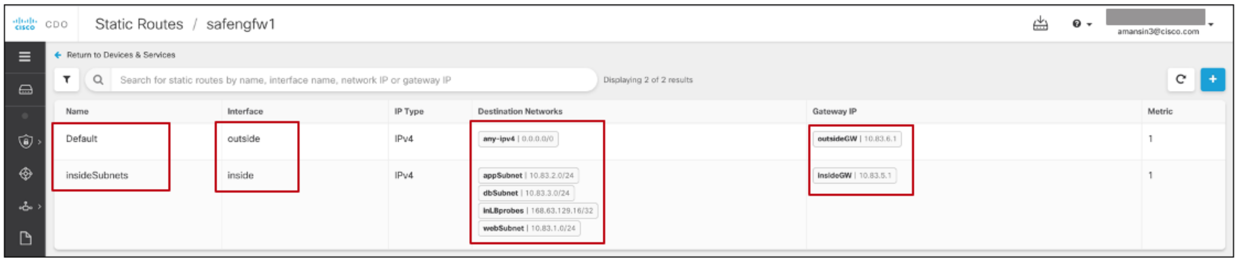
Click on the onboarded NGFW appliance on CDO dashboard and then go to 'Interfaces' option from the menu that appears on the right-hand side of the dashboard. Make sure Gig0/0 and Gig0/1 are assigned static IP addresses and names as defined in the table in Step 1.


CDO
Interfaces / safengfw1
[redacted]
amansin3@cisco.com
Return to Devices & Services
Search for interfaces by name, ID or IP

Displaying 3 of 3 results

Name	Logical Name	State	IP Address	Interface Type	Mode
GigabitEthernet0/0	inside	● Enabled	10.83.5.10 STATIC	Physical Interface	Routed
GigabitEthernet0/1	outside	● Enabled	10.83.6.10 STATIC	Physical Interface	Routed
Management0/0	diagnostic	● Enabled		Physical Interface	Routed

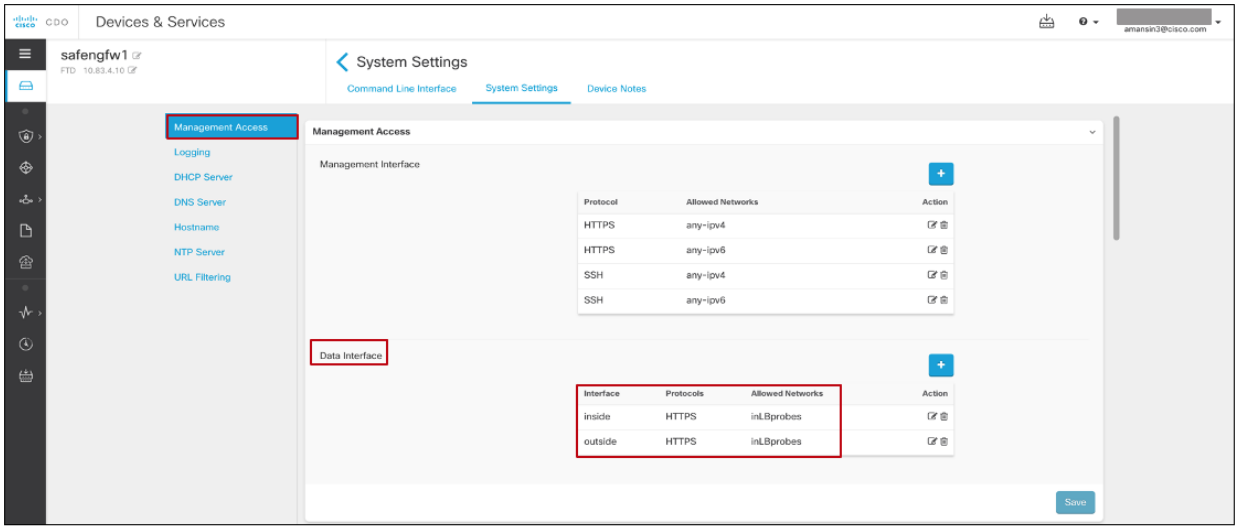
Go back to the same menu and now go to 'Routing' option, set the default route pointing to the gateway on outside the subnet- 10.83.6.1. Also, add the route for internal subnets (web, app and database subnet) pointing to the gateway on the inside subnet- 10.83.5.1. Lastly, add a route for load balancer virtual IP address that sends the health probes, set the next hop as the inside subnet gateway. Find more details about Azure load balancer health probes, refer to the Azure documentation.


CDO
Static Routes / safengfw1
[redacted]
amansin3@cisco.com
Return to Devices & Services
Search for static routes by name, interface name, network IP or gateway IP

Displaying 2 of 2 results

Name	Interface	IP Type	Destination Networks	Gateway IP	Metric
Default	outside	IPv4	any-ipv4 | 0.0.0.0/0	outsideGW | 10.83.6.1	1
insideSubnets	inside	IPv4	appSubnet | 10.83.2.0/24 dbSubnet | 10.83.3.0/24 inLBprobes | 168.63.129.16/32 webSubnet | 10.83.1.0/24	insideGW | 10.83.5.1	1

Next, we set up the inside and outside interfaces to listen on TCP port 443; we make sure that we only allow load balancer probe IP. We will need this allowed for inside and outside load balancers to do health check on inside and outside interfaces of the firewalls. Go back to the same device menu on CDO and this time, click on 'Settings'. Select the 'Data Interfaces' tab and click on 'add' to allow probes to inside and outside interfaces on port 443 from VIP sending the load balancer health probes. You might also need to update your inside NSG to allow these probes.



Management Access

Management Interface

Protocol	Allowed Networks	Action
HTTPS	any-ipv4	
HTTPS	any-ipv6	
SSH	any-ipv4	
SSH	any-ipv6	

Data Interface

Interface	Protocols	Allowed Networks	Action
inside	HTTPS	inLBprobes	
outside	HTTPS	inLBprobes	

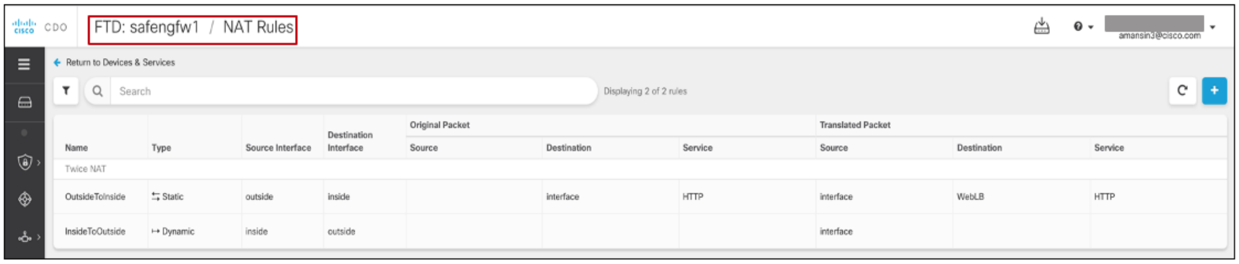
Next, we set up two NAT rules. We configure a dynamic PAT rule to allow outbound traffic to the Internet from the application workloads. The translation would be as below.

```
Source: WorkloadIP:Port => OutsideFWInterfaceIP:Port
```

We configure another static NAT rule to do the following translation for traffic from the Internet users accessing the application:

```
Source translation: InternetUserIP:Port => InsideFWInterfaceIP:Port

Destination translation: OutsideLBIP:HTTP => WebLBIP:HTTP
```

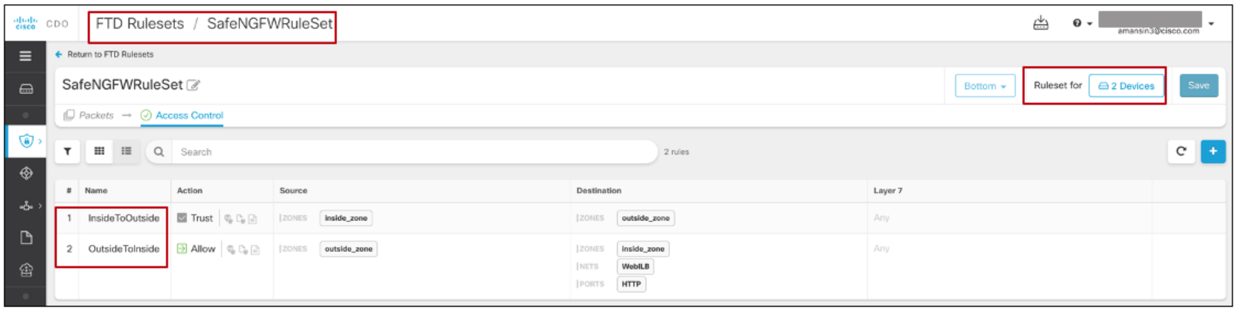
We need the source translation above to ensure that reply traffic is returned back to the same firewall's inside interface i.e. maintain the traffic symmetry. The destination is translated from public IP of outside load balancer to the IP address of the web load balancer i.e. 10.83.1.100. Web load balancer receives all the incoming traffic for the cloud application and distributes to the web servers in web VSS.



Name	Type	Source Interface	Destination Interface	Original Packet Source	Original Packet Destination	Original Packet Service	Translated Packet Source	Translated Packet Destination	Translated Packet Service
Twice NAT									
OutsideToInside	⇆ Static	outside	inside		interface	HTTP	interface	WebLB	HTTP
InsideToOutside	↦ Dynamic	inside	outside				interface		

Lastly, we assign inside interface to inside zone and outside interface to outside zone. Then, we configure access control policies to allow traffic from inside zone to outside zone. We also allow HTTP traffic incoming from the Internet users who are trying to access the cloud application.

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.



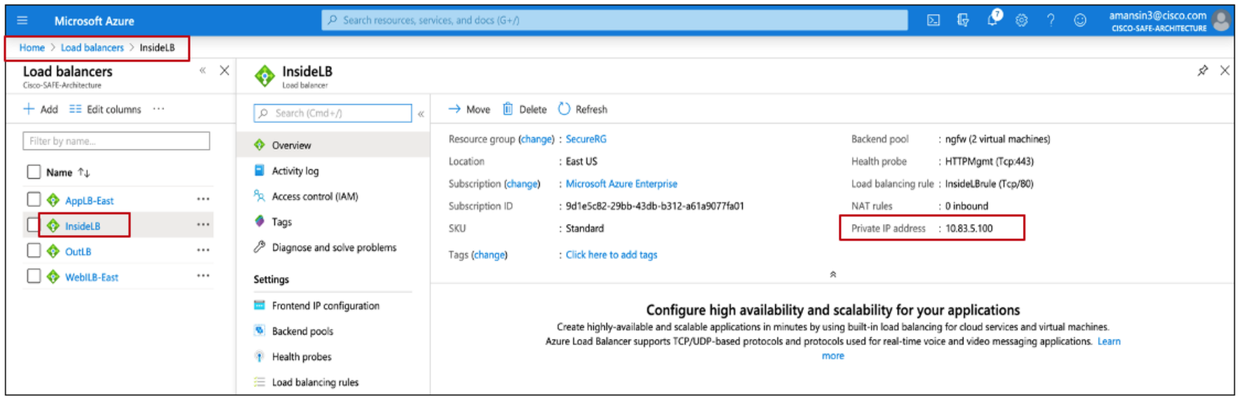
#	Name	Action	Source	Destination	Layer 7
1	InsideToOutside	Trust	ZONES inside_zone	ZONES outside_zone	Any
2	OutsideToInside	Allow	ZONES outside_zone	ZONES inside_zone NETS WebILB PORTS HTTP	Any

After this, we deploy all the changes and repeat the same for the second FTD device.

Step 4. Set up the 'inside' and 'outside' load balancers – In this step, we will set the 'inside' and 'outside' load balancers and the update the Azure Route Tables for web and app tier to point the default route to the 'inside' load balancer.

Go to 'Load balancer' service on the Azure portal. Click on 'add' to create an 'inside' load balancer. We assigned the static IP address 10.83.5.100 to the load balancer.

Refer to the Azure documentation for detailed information on creating load balancer. Make sure to choose 'Standard' SKU, it's required to integrate with highly available (Zone Redundant) resources like our firewall deployment.



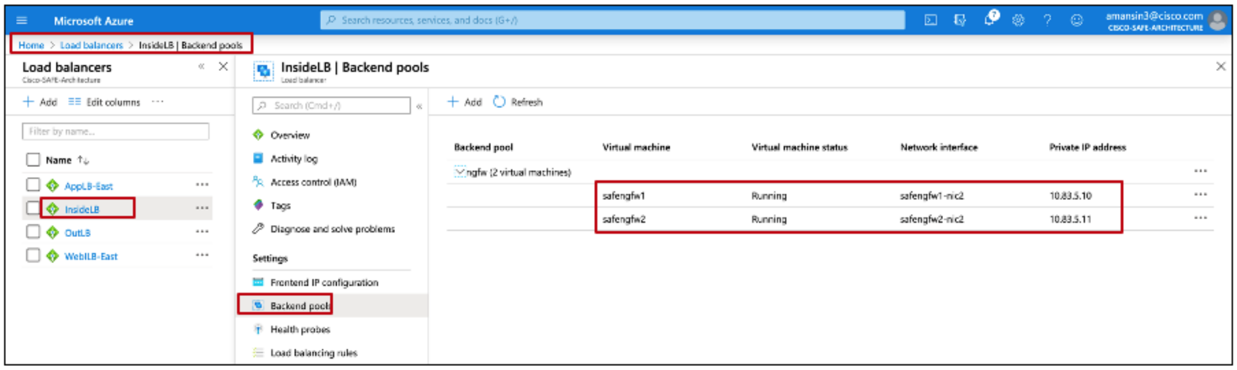
Resource group (change)	: SecureRG
Location	: East US
Subscription (change)	: Microsoft Azure Enterprise
Subscription ID	: 9d1e5c82-29bb-43db-b312-a61a9077fa01
SKU	: Standard
Tags (change)	: Click here to add tags

Backend pool	: ngfw (2 virtual machines)
Health probe	: HTTPMgmt (Tcp:443)
Load balancing rule	: InsideLBrule (Tcp/80)
NAT rules	: 0 inbound
Private IP address	: 10.83.5.100

Configure high availability and scalability for your applications

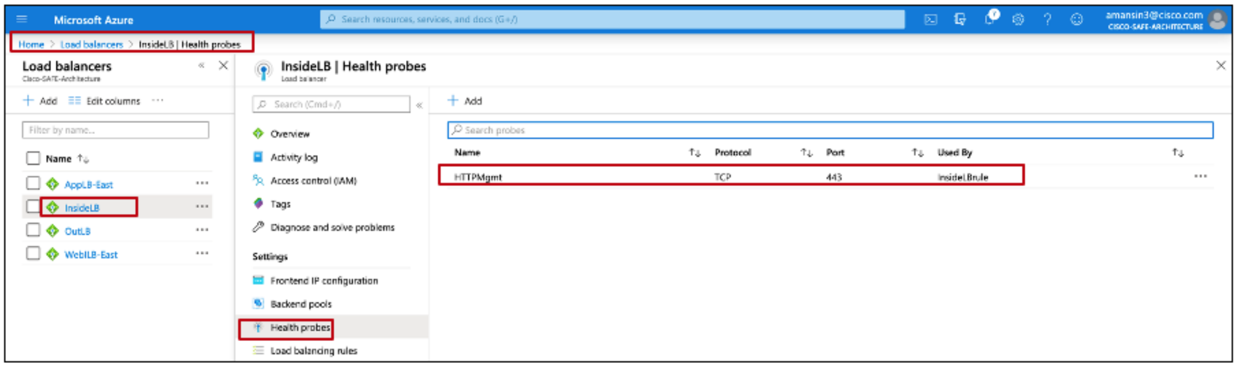
Create highly-available and scalable applications in minutes by using built-in load balancing for cloud services and virtual machines. Azure Load Balancer supports TCP/UDP-based protocols and protocols used for real-time voice and video messaging applications. Learn more

After the load balancer is created, add the backend pool. Click on the add button and add the inside firewall interfaces to the pool.



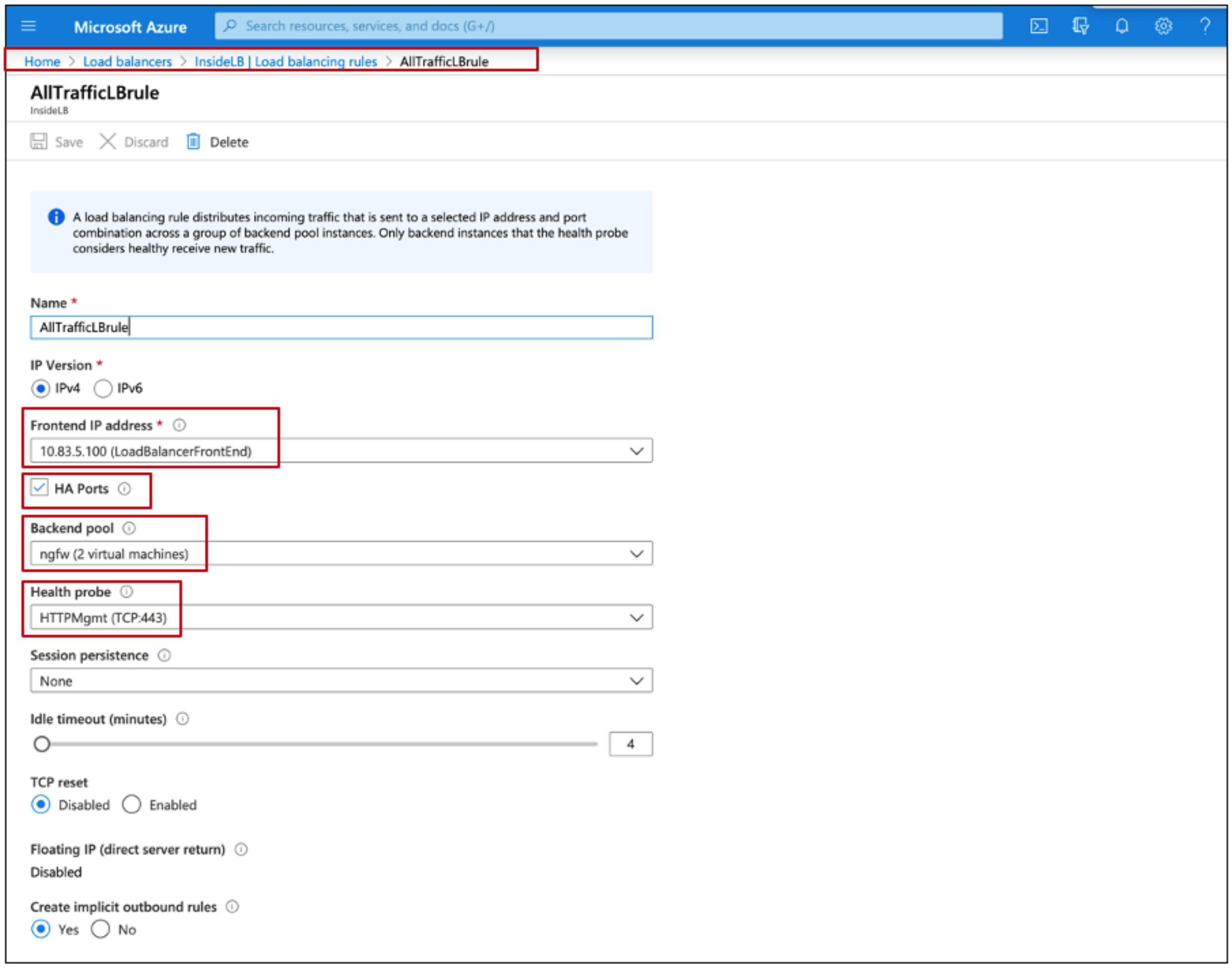
Backend pool	Virtual machine	Virtual machine status	Network interface	Private IP address
ngfw (2 virtual machines)				
	safengfw1	Running	safengfw1-nic2	10.83.5.10
	safengfw2	Running	safengfw2-nic2	10.83.5.11

After adding the backend pool, next step is to define the probes to monitor the health status of inside interfaces. We had set up the FTD appliances to listen on port 443 from load balancer IP addresses, hence we set up the health probe for TCP port 443.



Name	Protocol	Port	Used By
HTTPMgmt	TCP	443	InsideLBrule

Last step is to configure the load balancing rule. For 'inside' load balancer, make sure to check the HA port option so that the load balancer can receive traffic for all the TCP and UDP ports.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancers > InsideLB | Load balancing rules > AllTrafficLBrule

AllTrafficLBrule
InsideLB

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *: AllTrafficLBrule

IP Version *: ● IPv4 ○ IPv6

Frontend IP address *: 10.83.5.100 (LoadBalancerFrontEnd)

☑ HA Ports

Backend pool: ngfw (2 virtual machines)

Health probe: HTTPMgmt (TCP:443)

Session persistence: None

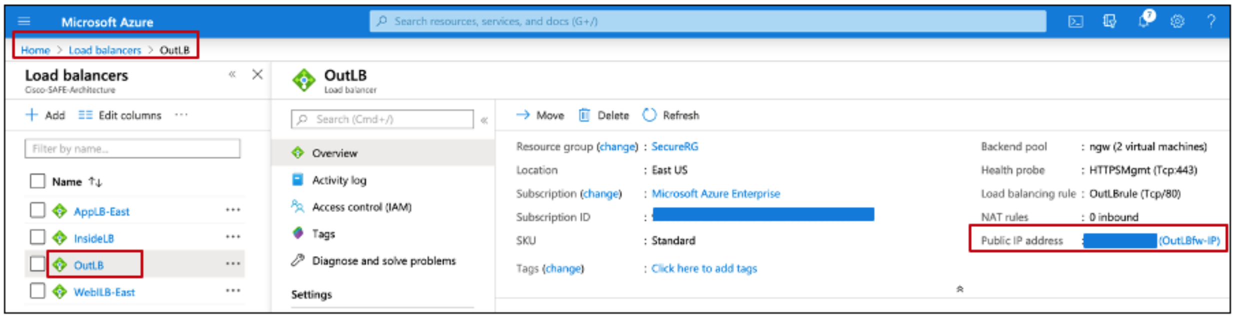
Idle timeout (minutes): 4

TCP reset: ● Disabled ○ Enabled

Floating IP (direct server return): Disabled

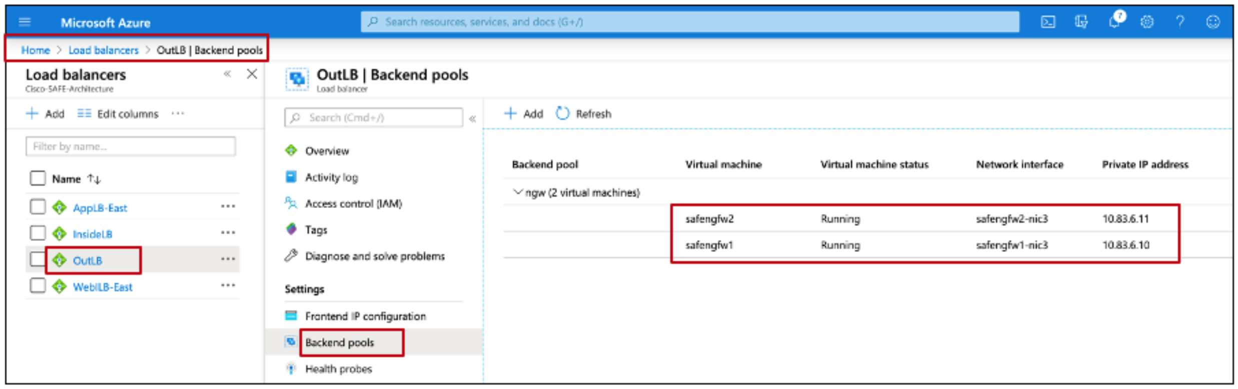
Create implicit outbound rules: ● Yes ○ No

In a similar manner, we set up the 'outside' load balancer. The only major difference is that this is a public load balancer and hence is assigned a public IP. This public IP will be used to access our cloud application.



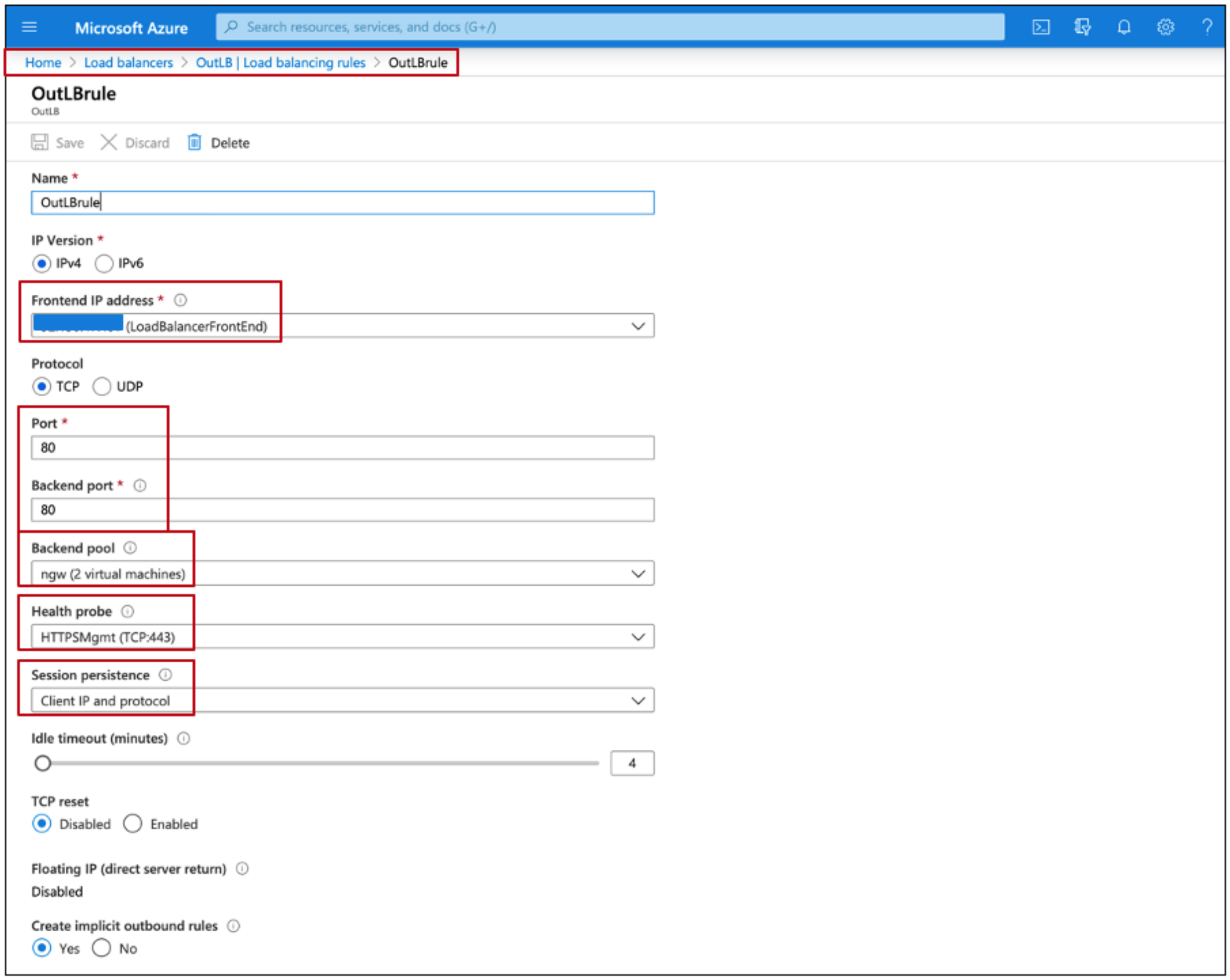
Resource group (change)	: SecureRG
Location	: East US
Subscription (change)	: Microsoft Azure Enterprise
Subscription ID	: [redacted]
SKU	: Standard
Tags (change)	: Click here to add tags
Backend pool	: ngw (2 virtual machines)
Health probe	: HTTPSMgmt (Tcp:443)
Load balancing rule	: OutLBrule (Tcp/80)
NAT rules	: 0 inbound
Public IP address	: [redacted] (OutLBfw-IP)

The backend pool will consist of the outside interfaces of the firewall.



Backend pool	Virtual machine	Virtual machine status	Network interface	Private IP address
ngw (2 virtual machines)				
	safengfw2	Running	safengfw2-nic3	10.83.6.11
	safengfw1	Running	safengfw1-nic3	10.83.6.10

The load balancer rule is set up to listen on TCP port 80 and forward the traffic to the backend pool consisting of outside interfaces of NGFWv devices on the same TCP port 80. Make sure to set the session persistence to 'Client IP and protocol' to ensure that traffic for the same session is forwarded to the same NGFW.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancers > OutLB | Load balancing rules > OutLBrule
OutLBrule
OutLB
Save
Discard
Delete

Name *
OutLBrule

IP Version *
● IPv4 ○ IPv6

Frontend IP address *
[redacted] (LoadBalancerFrontEnd)

Protocol
● TCP ○ UDP

Port *
80

Backend port *
80

Backend pool
ngw (2 virtual machines)

Health probe
HTTPSMgmt (TCP:443)

Session persistence
Client IP and protocol

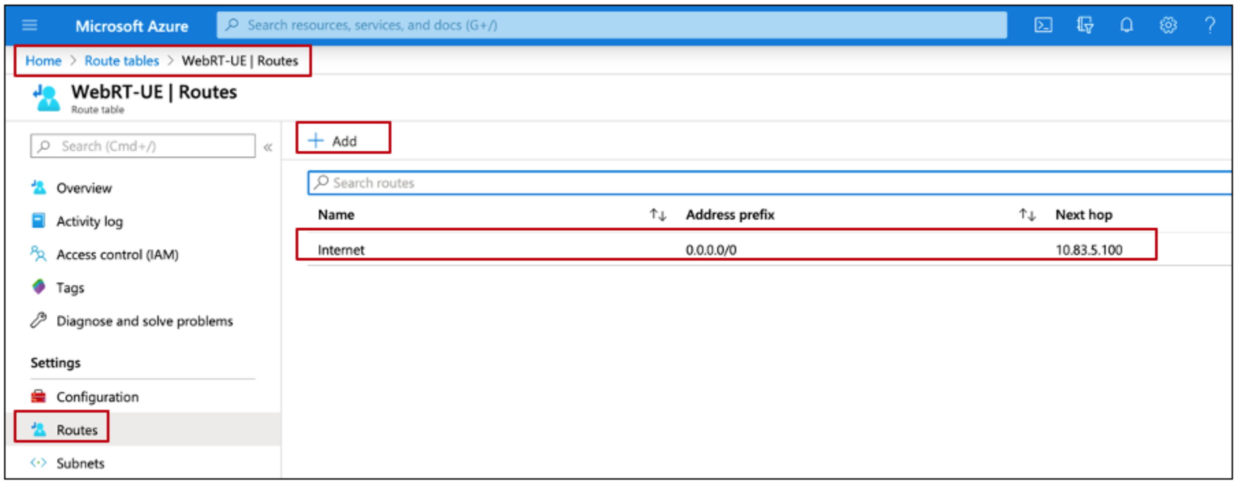
Idle timeout (minutes)
4

TCP reset
● Disabled ○ Enabled

Floating IP (direct server return)
Disabled

Create implicit outbound rules
● Yes ○ No

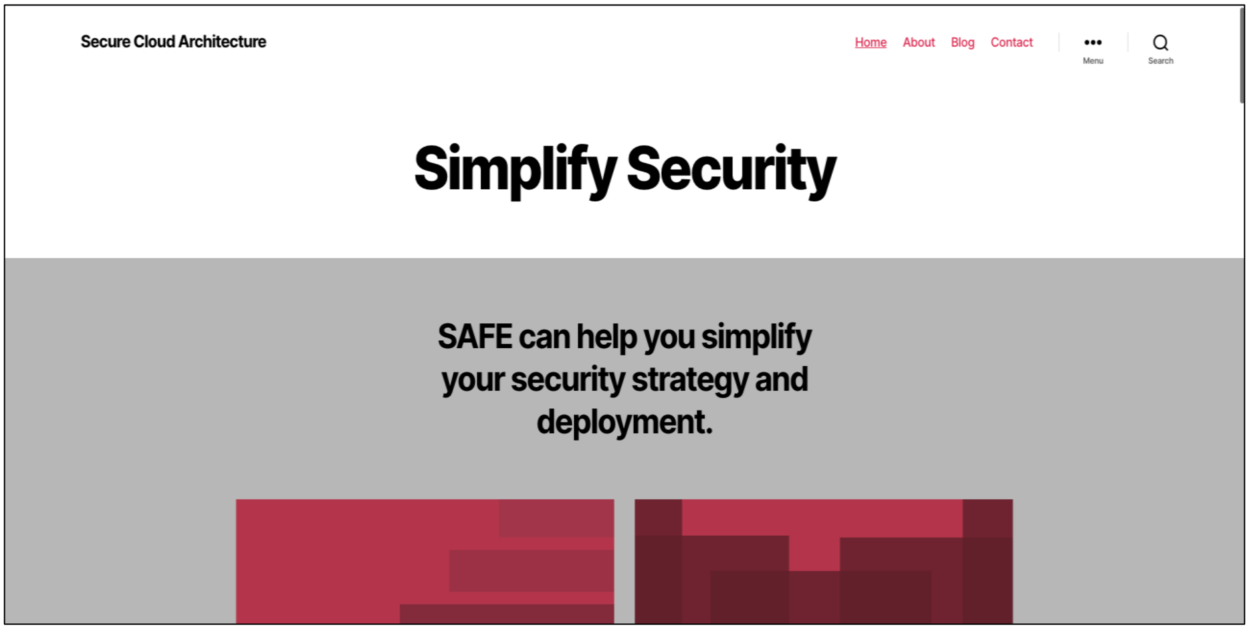
Now that we have the inside and outside load balancers set up, we need to update the routing tables for the Web and App tier to force the outbound traffic for Internet to inside interfaces of NGFW devices. We add the default routes in the web and app routing table with next hop as 10.83.5.100 i.e.. the 'inside' load balancer, this ensures load balancing of outbound internet traffic to inside interfaces of the NGFW devices.



WebRT-UE | Routes
Route table

Name	Address prefix	Next hop
Internet	0.0.0.0/0	10.83.5.100

Step 4. **Access the application -** The last step to setting up this application is to register a domain for the application and add an ‘A’ record to point the domain name to the public IP address of the ‘outside’ load balancer. When we access the newly registered domain name for the Azure application, we are prompted for the initial set up and then we land on cloud application home page as below.



Simplify Security

SAFE can help you simplify your security strategy and deployment.

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. For the purpose of this document, we will demonstrate two different options for adding these capabilities, you can pick either of these two options:

OPTION 1: Azure WAF and DDoS protection

Azure WAF can be deployed with Azure Application Gateway, Azure Front Doors, and Azure Content Delivery Network (CDN) service from Microsoft. We incorporate Azure Front Doors service to validate WAF integration with our application. Based on different application set ups, Azure native WAF may or may not be an available option for WAF capabilities. Refer to the Azure documentation for more details about Azure WAF service.

Azure provides two tiers for DDoS protection, Basic and Standard. Azure Front Doors platform is by default protected by Azure Basic DDoS Protection. For further security, Standard DDoS protection is enabled at the VNET level to protect any resource with a public IP in outside and management tiers. While Basic service is enabled by default at the VNET level also, Standard tier needs to be enabled manually. Find more details in Azure documentation here.

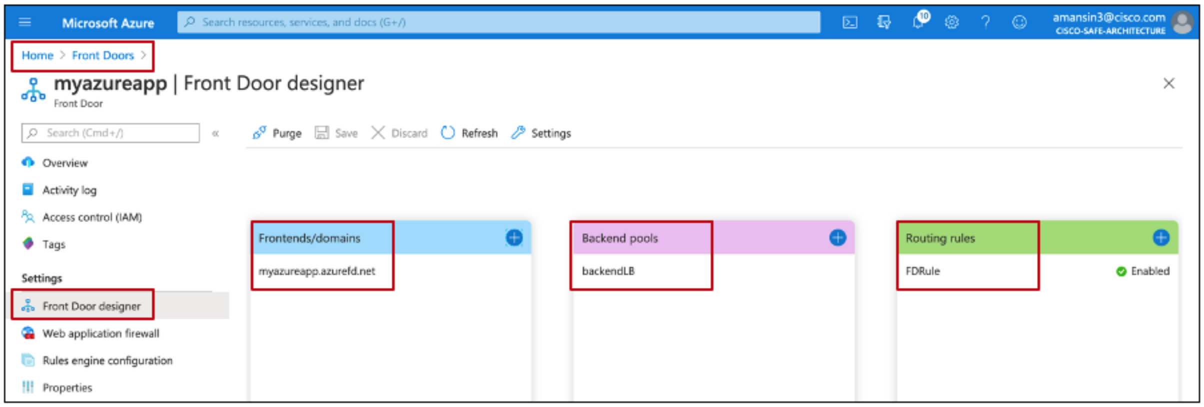
Implementation procedure:

Step 1. Setting up Azure WAF service

Step 2. Setting up Azure DDoS protection for VNET

Step 1. Setting up Azure WAF service – Go to 'Front Doors' service on the Azure portal and click on 'add' to create a new Front Door service for the newly set up cloud application. Configuring Front Door service involves three steps -you will need to specify a domain name for the application, the backend pool which consists of outside interfaces of the NGFWs and lastly the traffic routing rules.

Azure Front Door will receive the traffic from internet users and load balance it to the outside interfaces of NGFWs. Make sure you enable session affinity at 'Frontend/domain' level if your application is stateful. For detailed steps on how to create Azure Front Doors, check out the Azure documentation.

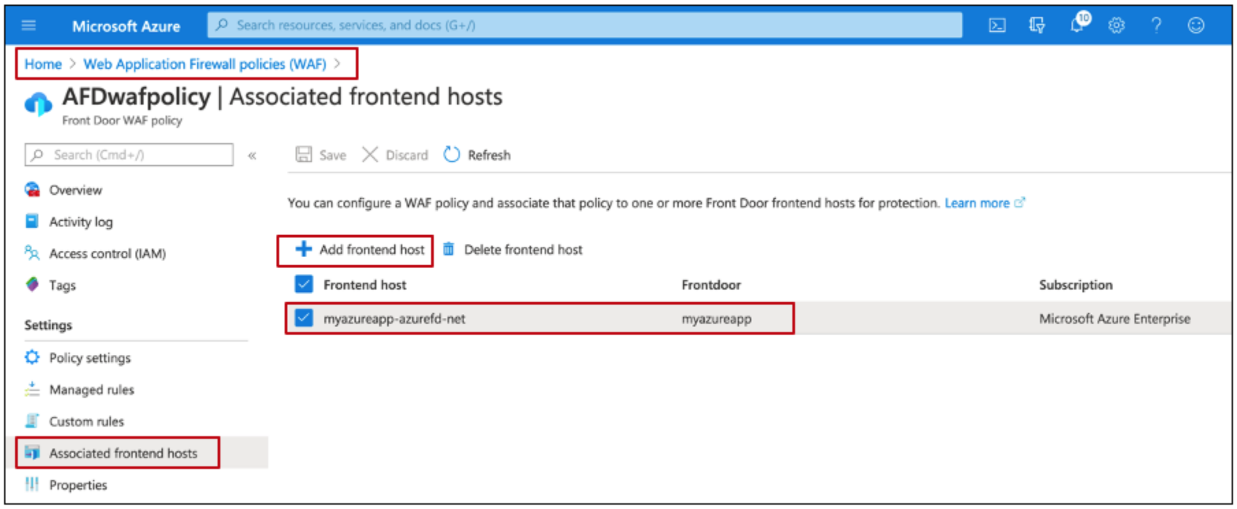


Frontends/domains	Backend pools	Routing rules
myazureapp.azurefd.net	backendLB	FDRule ✓ Enabled

Optionally, you can customize the domain name for your Front Door, refer to Azure documentation.

To lock down the application to accept traffic only from this specific Front Door, you can use ACL on Firewall to lock down the access to Front Door backend IP space. Refer to the Q&A page here for more details on AFD IP space.

Now that we have our Front Door set up complete, we will enable the Azure WAF. Go to 'Web Application Firewall Policies' on the Azure portal and click on 'add' to enable the WAF service for Front Door that we created above.



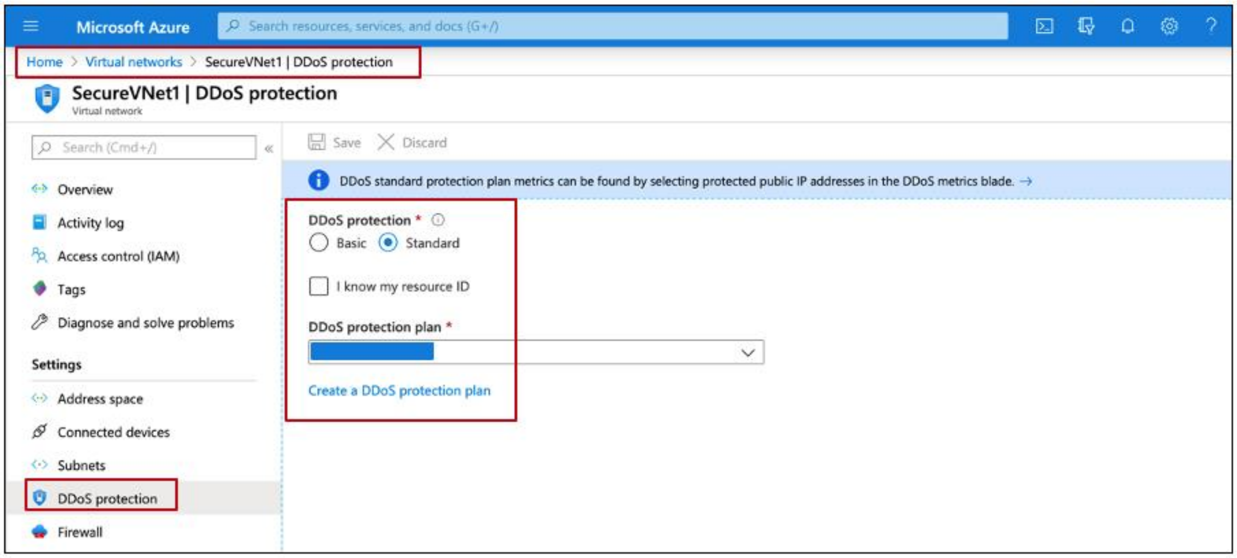
AFDwafpolicy | Associated frontend hosts

Front Door WAF policy

You can configure a WAF policy and associate that policy to one or more Front Door frontend hosts for protection.

☑ Frontend host	Frontdoor	Subscription
☑ myazureapp-azurefd-net	myazureapp	Microsoft Azure Enterprise

Step 2. Setting up Azure DDoS protection for VNET - For enabling the Standard tier DDoS capability, go to 'Virtual Networks' on the Azure portal and select the VNET created for the cloud application. On the left-hand side panel, select DDoS to enable the Standard tier. For detailed instructions on how to configure DDoS, refer to the Azure documentation.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual networks > SecureVNet1 | DDoS protection
Search (Cmd+/)
Save
Discard
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
DDoS protection
Firewall
Create a DDoS protection plan

SecureVNet1 | DDoS protection

Virtual network

DDoS standard protection plan metrics can be found by selecting protected public IP addresses in the DDoS metrics blade. →

DDoS protection *

○ Basic ● Standard

☐ I know my resource ID

DDoS protection plan *

OPTION 2: Radware Cloud Service for WAF and DDOS protection.

Radware Cloud WAF and DDoS services are integrated by using CNAME DNS records. Its independent of any specific Azure Cloud service. For Radware integration, we use DNS to forward traffic to Radware cloud. After scanning the traffic, it is redirected to the Public IP of 'outside' load balancer.

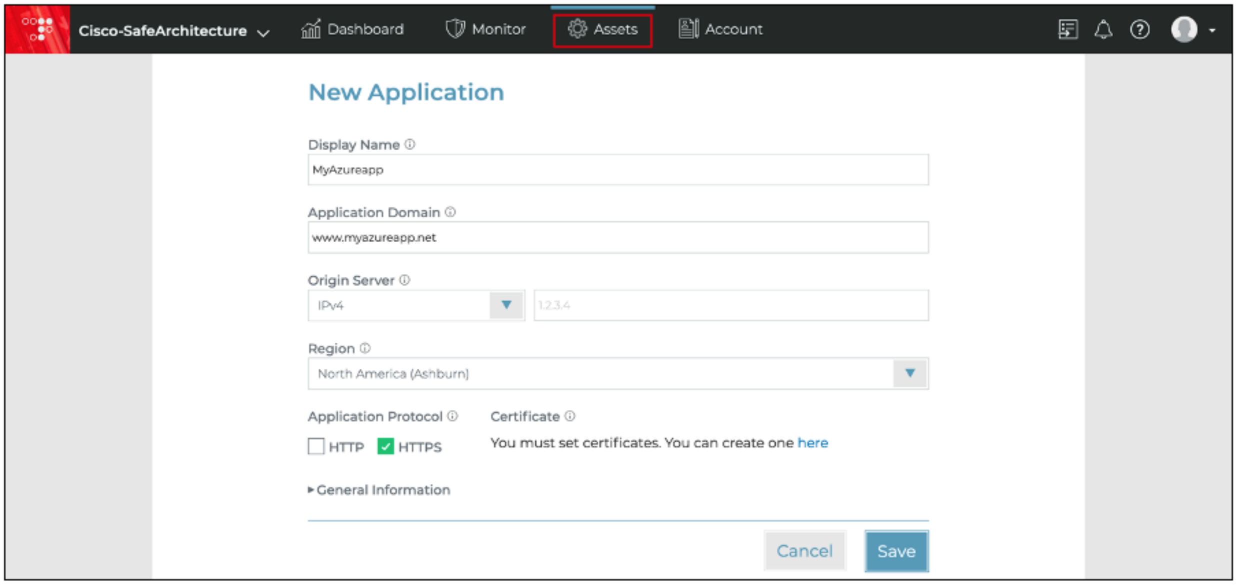
Implementation procedure:

Step 1. Onboard the application to Radware Cloud

Step 2. Update the DNS setting to point traffic to Radware Cloud

Step 1. Onboard the application to Radware Cloud - The first step to integrating Radware cloud service in your environment is to add 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.myazureapp.net), the origin server (in this case it would be the 'outside' load balancer's public IP address) and the protocol (HTTP). If your application is based on HTTPS protocol, you would need to add the certificate information as well.

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.



New Application

Display Name: MyAzureapp

Application Domain: www.myazureapp.net

Origin Server: IPv4 1.2.3.4

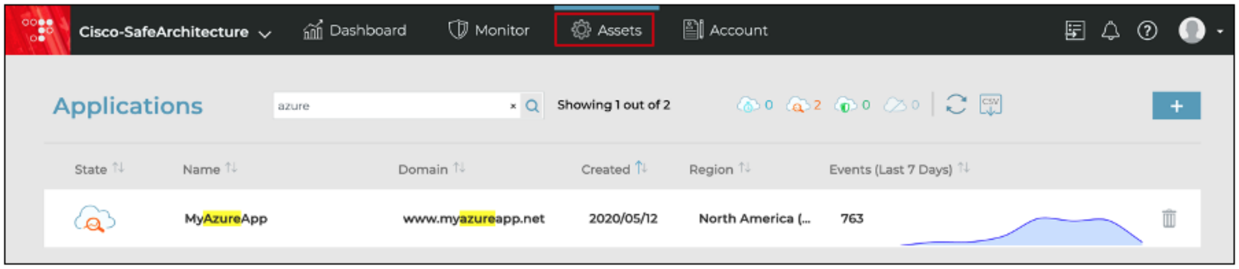
Region: North America (Ashburn)

Application Protocol: □ HTTP ☑ HTTPS

Certificate: You must set certificates. You can create one here

▸General Information

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



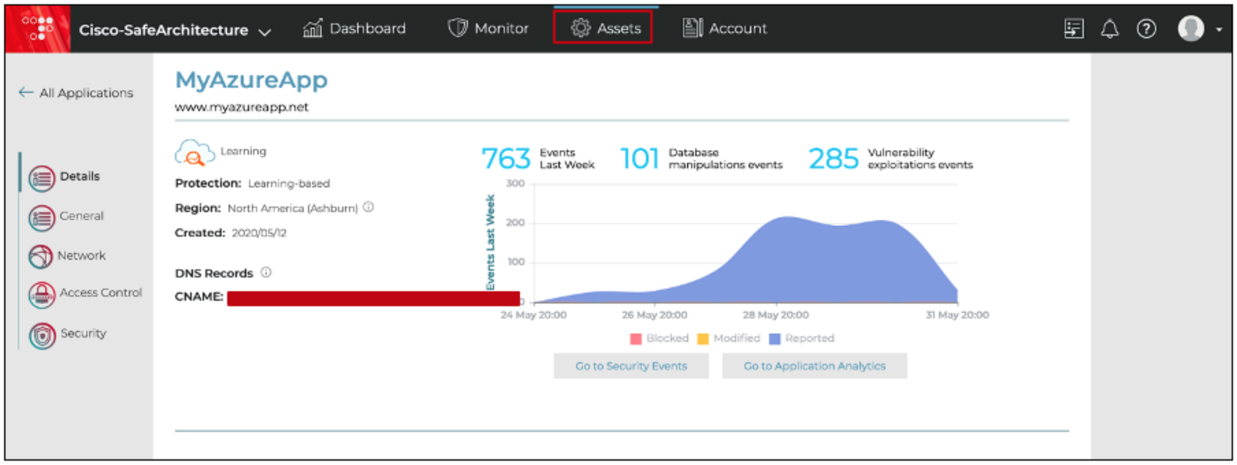
Applications

azure

Showing 1 out of 2

State	Name	Domain	Created	Region	Events (Last 7 Days)
	MyAzureApp	www.myazureapp.net	2020/05/12	North America (...	763

Click on the application and copy the allocated CNAME. We need to update the DNS records for our application with this Radware CNAME.



MyAzureApp

www.myazureapp.net

Protection: Learning-based

Region: North America (Ashburn)

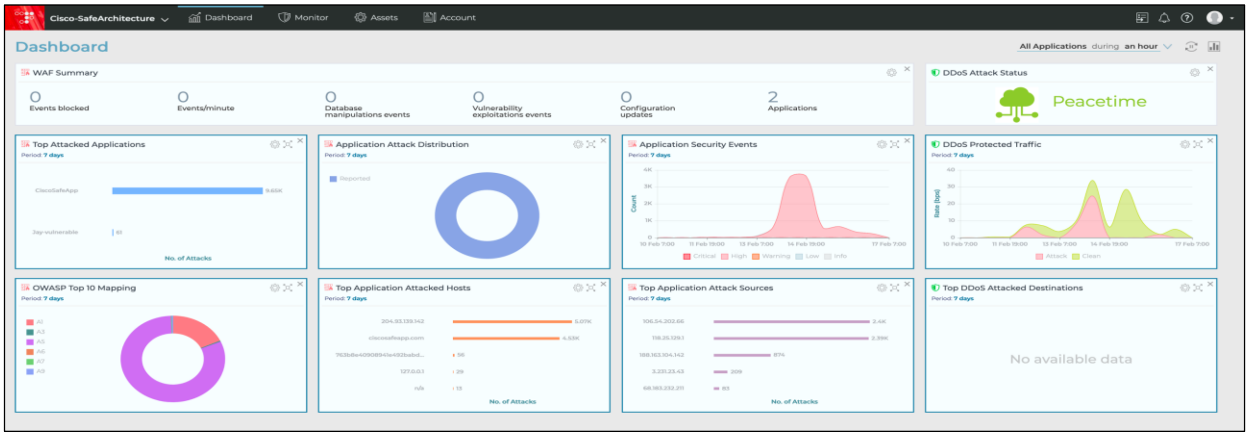
Created: 2020/05/12

DNS Records

CNAME: [redacted]

Step 2. **Update the DNS setting to point traffic to Radware Cloud** – Update the DNS record sets for the application domain with Radware CNAME (from the previous step) and corresponding IP address. 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 Azure cloud. 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 Radware Cloud WAF Quick Start guide (login required).

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



Integrating with Cisco SecureX threat response

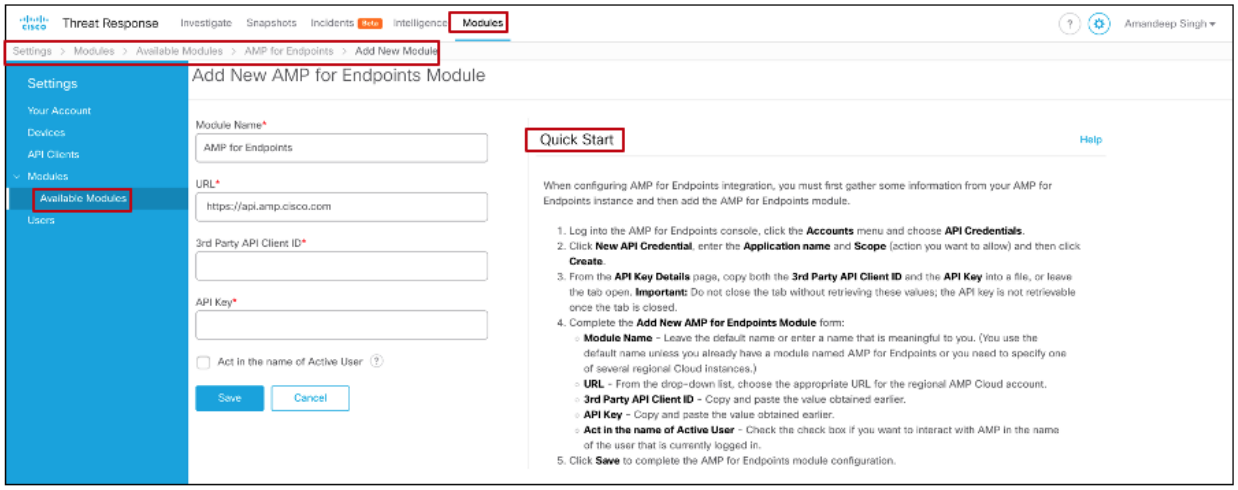
In this last implementation step, we will enable the AMP4E and Umbrella modules in the threat response portal to get a unified view into the Azure environment. We create API keys in AMP4E and Umbrella portals and then configure those keys in the threat response dashboard.

Implementation procedure:

Step 1. **Add the AMP4E module**

Step 2. **Add the Umbrella modules**

Step 1. **Add the AMP4E module –** Log on to the threat response dashboard and go to available modules, add a new AMP4E module. Threat response displays all the steps on how to integrate the AMP module once you click on 'add module' as shown in the snapshot below.



Add New AMP for Endpoints Module

Module Name*: AMP for Endpoints

URL*: https://api.amp.cisco.com

3rd Party API Client ID*

API Key*

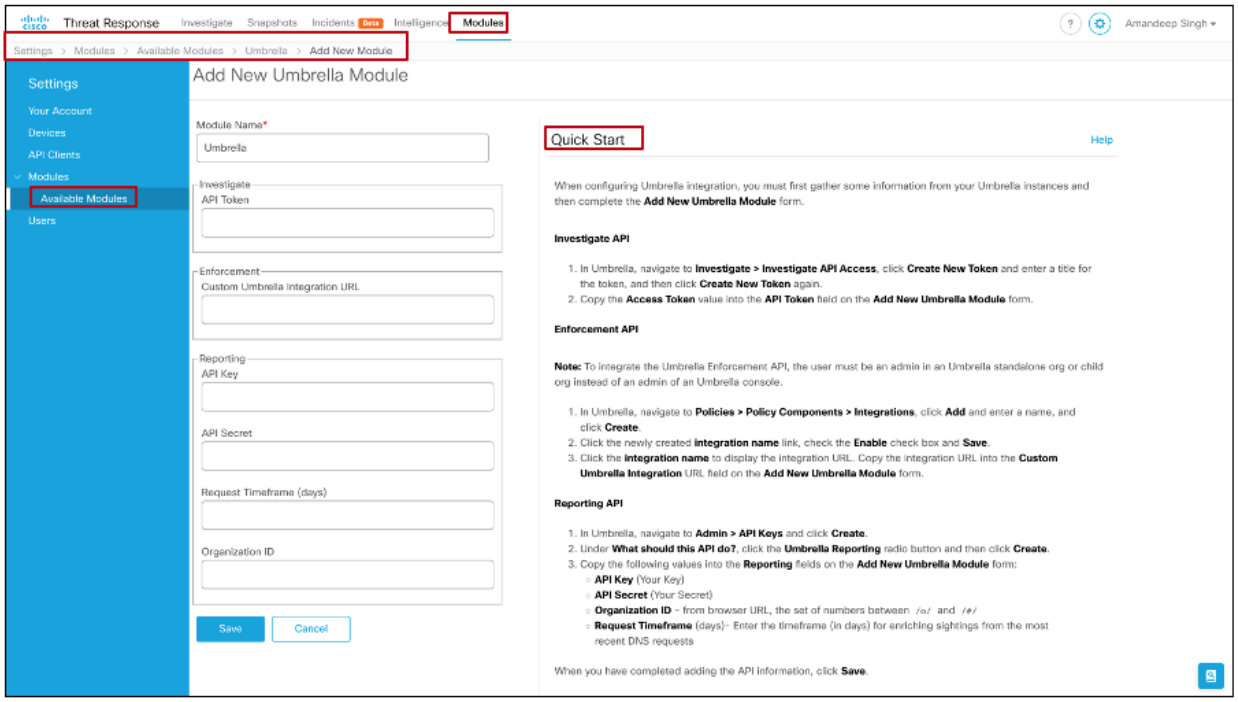
□ Act in the name of Active User

Quick Start

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**.
2. Click **New API Credential**, enter the **Application name** and **Scope** (action you want to allow) and then click **Create**.
3. 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 Module** form:
   - **Module Name** – Leave the default name or enter a name that is meaningful to you. (You use the default name unless you already have a module named AMP 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** – Copy and paste the value obtained earlier.
   - **Act in the name of Active User** – Check the check box 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. **Add the Umbrella module –** Go to available modules again, this time, add a new Umbrella module. In a similar manner as AMP4E, the integration steps are listed on the threat response page. Create the API keys in the Umbrella portal as instructed and then add the it in the threat response configuration page.



Add New Umbrella Module

Module Name*: Umbrella

Investigate
API Token

Enforcement
Custom Umbrella Integration URL

Reporting
API Key
API Secret
Request Timeframe (days)
Organization ID

Quick Start

When configuring Umbrella integration, you must first gather some information from your Umbrella instances and then complete the **Add New Umbrella Module** form.

Investigate API

1. In Umbrella, navigate to **Investigate > Investigate API Access**, click **Create New Token** and enter a title for the token, and then click **Create New Token** again.
2. Copy the **Access Token** value into the **API Token** field on the **Add New Umbrella Module** form.

Enforcement API

Note: To integrate the Umbrella Enforcement API, the user must be an admin in an Umbrella standalone org or child org instead of an admin of an Umbrella console.

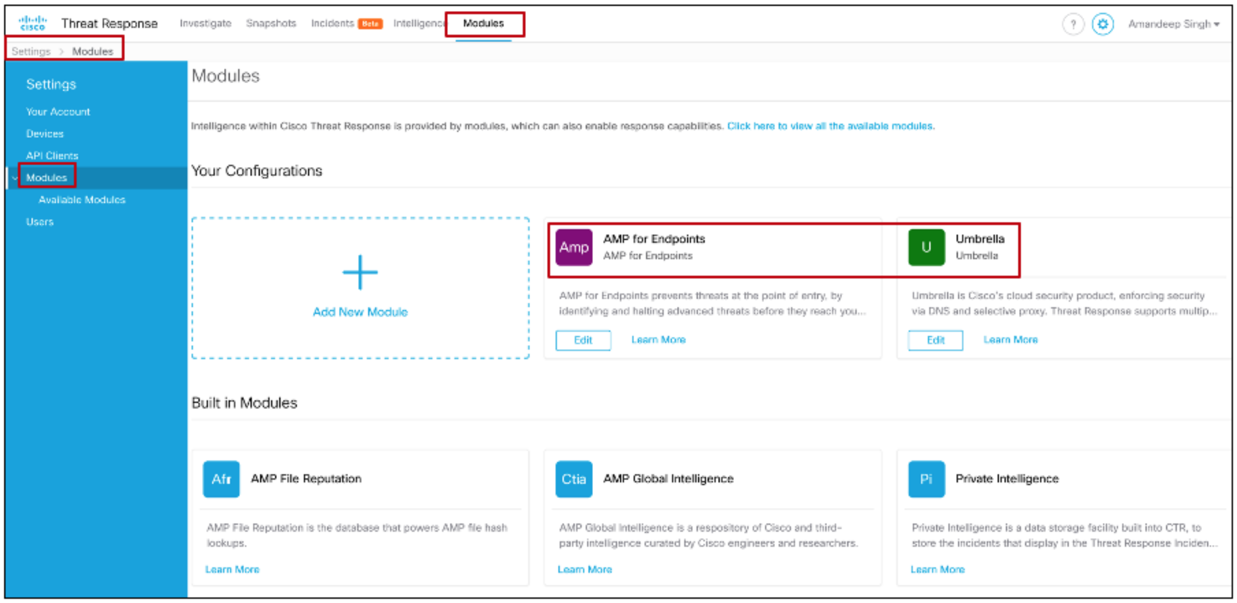
1. In Umbrella, navigate to **Policies > Policy Components > Integrations**, click **Add** and enter a name, and click **Create**.
2. Click the newly created **integration name** link, check the **Enable** check box and **Save**.
3. Click the **integration name** to display the integration URL. Copy the integration URL into the **Custom Umbrella Integration** URL field on the **Add New Umbrella Module** form.

Reporting API

1. In Umbrella, navigate to **Admin > API Keys** and click **Create**.
2. Under **What should this API do?**, click the **Umbrella Reporting** radio button and then click **Create**.
3. Copy the following values into the **Reporting** fields on the **Add New Umbrella Module** form:
   - **API Key** (Your Key)
   - **API Secret** (Your Secret)
   - **Organization ID** – from browser URL, the set of numbers between `/o/` and `/#/`
   - **Request Timeframe** (days)- Enter the timeframe (in days) for enriching sightings from the most recent DNS requests

When you have completed adding the API information, click **Save**.

After we have saved the module configurations, the modules will be listed under ‘Module’ as below.



Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. Click here to view all the available modules.

Your Configurations

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach you...

Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multip...

Built in Modules

AMP File Reputation is the database that powers AMP file hash lookups.

AMP Global Intelligence is a respository of Cisco and third-party intelligence curated by Cisco engineers and researchers.

Private Intelligence is a data storage facility built into CTR, to store the incidents that display in the Threat Response Inciden...

Validation Testing

Tetration

Validation procedure overview:

- Test Case 1 – Creating the workspace for Azure cloud application
- Test Case 2 – Using ADM to discover the policies for Azure workloads and setting up an app view
- Test Case 3 – Enforcing the policies on workloads
- Test Case 4 – Discovering the vulnerable packages on the Azure workloads

Test case 1: Creating an application workspace for Azure cloud application

This test case involves defining annotations for the Azure environment. These annotated attributes are used later to segregate the tiers and segments within the Azure VNET 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

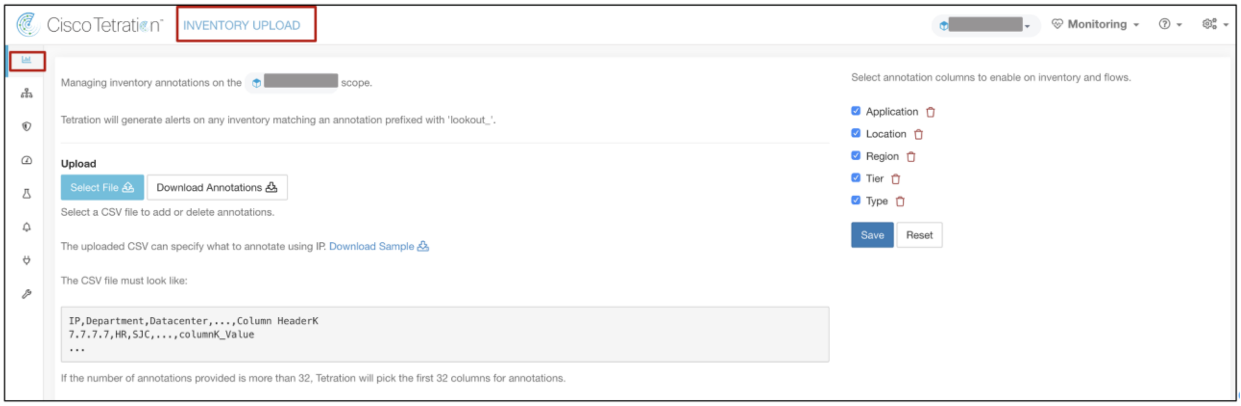
Step 1. **Build an inventory –** Define the attributes that would help you segregate your tiered application workloads in the cloud and hence construct policies for them. We will upload a CSV file with workload annotations for this purpose.

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

Table 1. Azure Cloud Inventory

IP	Application	Region	Tier	Type
10.83.1.0/24	Safe3tierApp	US-East	WebServer	Azure-Cloud
10.83.2.0/24	Safe3tierApp	US-East	AppServer	Azure-Cloud
10.83.3.0/24	Safe3tierApp	US-East	Database	Azure-Cloud
10.83.4.0/24	Safe3tierApp	US-East	Management	Azure-Cloud
10.83.5.0/24	Safe3tierApp	US-East	Inside	Azure-Cloud
10.83.6.0/24	Safe3tierApp	US-East	Outside	Azure-Cloud
10.83.7.0/24	Safe3tierApp	US-East	Diagnostic	Azure-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.



Managing inventory annotations on the [redacted] scope.

Tetration will generate alerts on any inventory matching an annotation prefixed with 'lookout_'.

Upload

Select File | Download Annotations

Select a CSV file to add or delete annotations.

The uploaded CSV can specify what to annotate using IP. Download Sample

The CSV file must look like:

```
IP,Department,Datacenter,...,Column HeaderK
7.7.7.7,HR,SJC,...,columnK_Value
...
```

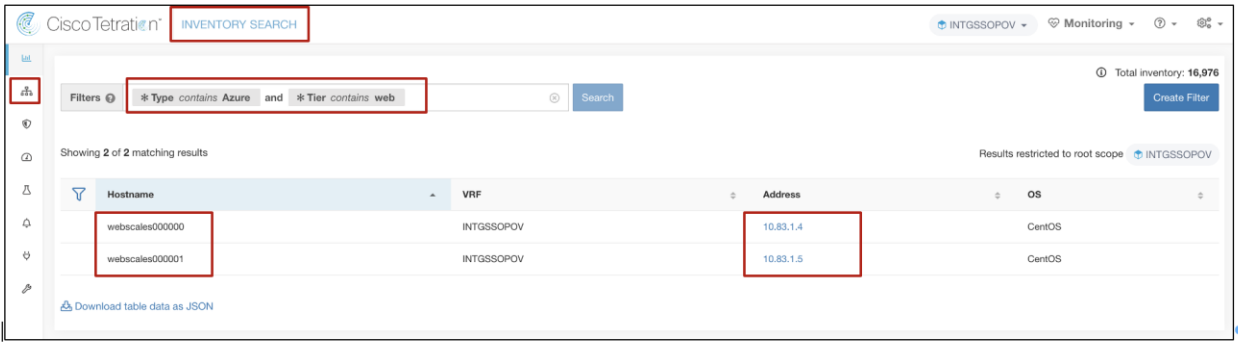
If the number of annotations provided is more than 32, Tetration will pick the first 32 columns for annotations.

Select annotation columns to enable on inventory and flows.

☑ Application
☑ Location
☑ Region
☑ Tier
☑ Type

Save | Reset

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



Filters: * Type *contains* Azure and * Tier *contains* web | Search

Total inventory: **16,976**

Create Filter

Showing **2** of **2** matching results

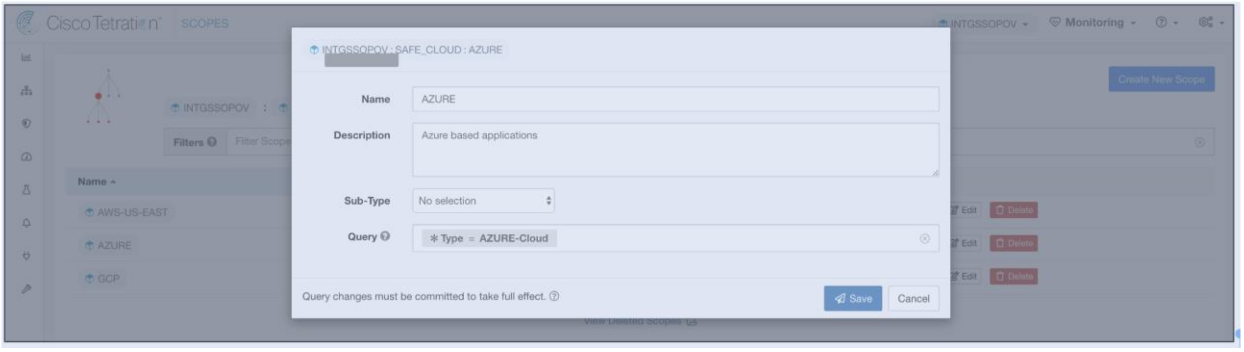
Results restricted to root scope INTGSSOPOV

Hostname	VRF	Address	OS
webscales000000	INTGSSOPOV	10.83.1.4	CentOS
webscales000001	INTGSSOPOV	10.83.1.5	CentOS

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 Azure cloud. We will make use of the annotations/filters that we constructed in Step 1. We created the scope ‘Azure-US-EAST’, which includes all the workloads from our tiered app in ‘US-East’ region in Azure 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.



INTGSSOPOV : SAFE_CLOUD : AZURE [redacted]

Name: AZURE

Description: Azure based applications

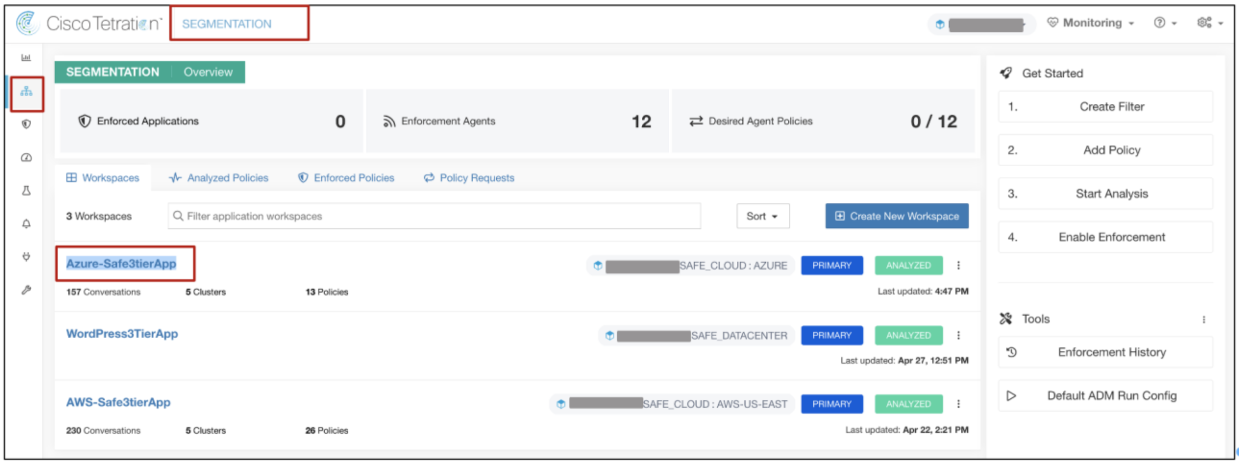
Sub-Type: No selection

Query: ✻ Type = AZURE-Cloud

Query changes must be committed to take full effect.

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 Azure 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.



Enforced Applications 0

Enforcement Agents 12

Desired Agent Policies 0 / 12

1. Create Filter
2. Add Policy
3. Start Analysis
4. Enable Enforcement

3 Workspaces

Azure-Safe3tierApp — [redacted]SAFE_CLOUD : AZURE — PRIMARY — ANALYZED
157 Conversations 5 Clusters 13 Policies Last updated: 4:47 PM

WordPress3TierApp — [redacted]SAFE_DATACENTER — PRIMARY — ANALYZED
Last updated: Apr 27, 12:51 PM

AWS-Safe3tierApp — [redacted]SAFE_CLOUD : AWS-US-EAST — PRIMARY — ANALYZED
230 Conversations 5 Clusters 26 Policies Last updated: Apr 22, 2:21 PM

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 Azure 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:

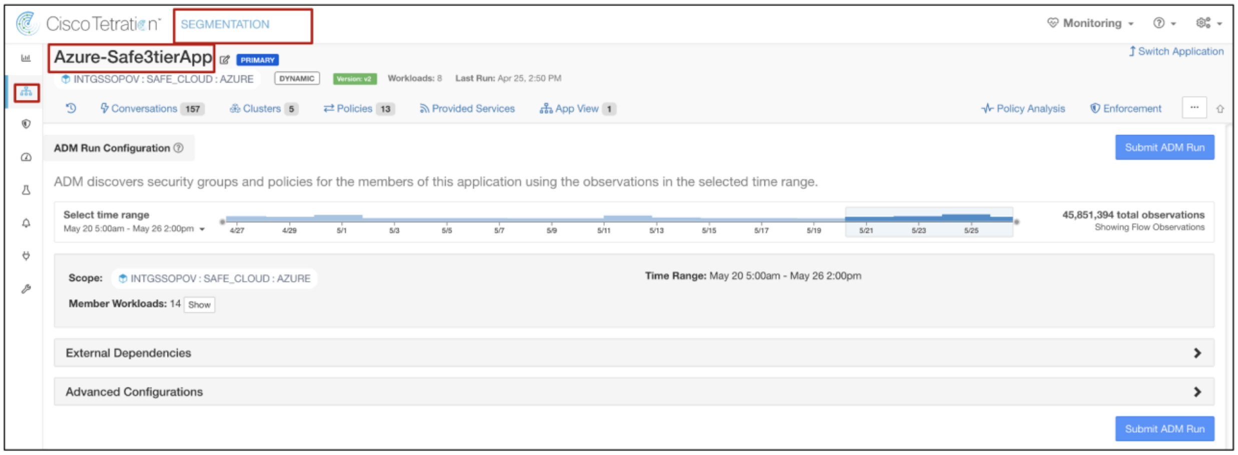
Step 1. Discover policies using ADM

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.



Azure-Safe3tierApp

INTGSSOPOV : SAFE_CLOUD : AZURE

Workloads: 8 Last Run: Apr 25, 2:50 PM

ADM Run Configuration

ADM discovers security groups and policies for the members of this application using the observations in the selected time range.

Select time range
May 20 5:00am - May 26 2:00pm

45,851,394 total observations
Showing Flow Observations

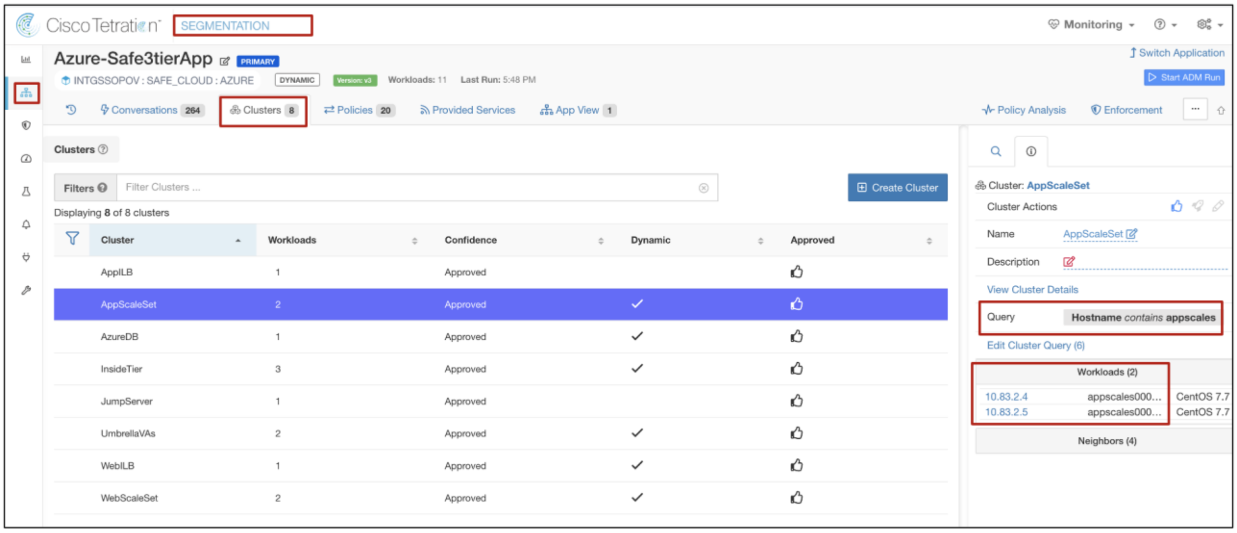
Scope: INTGSSOPOV : SAFE_CLOUD : AZURE

Member Workloads: 14

Time Range: May 20 5:00am - May 26 2:00pm

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 Virtual Machine Scale Sets like the web and application servers.



Azure-Safe3tierApp

INTGSSOPOV : SAFE_CLOUD : AZURE

Workloads: 11 Last Run: 5:48 PM

Displaying 8 of 8 clusters

Cluster	Workloads	Confidence	Dynamic	Approved
ApplLB	1	Approved		👍
AppScaleSet	2	Approved	✓	👍
AzureDB	1	Approved	✓	👍
InsideTier	3	Approved	✓	👍
JumpServer	1	Approved		👍
UmbrellaVAs	2	Approved	✓	👍
WebILB	1	Approved	✓	👍
WebScaleSet	2	Approved	✓	👍

Cluster: AppScaleSet

Name AppScaleSet

Description

Query **Hostname** *contains* **appscales**

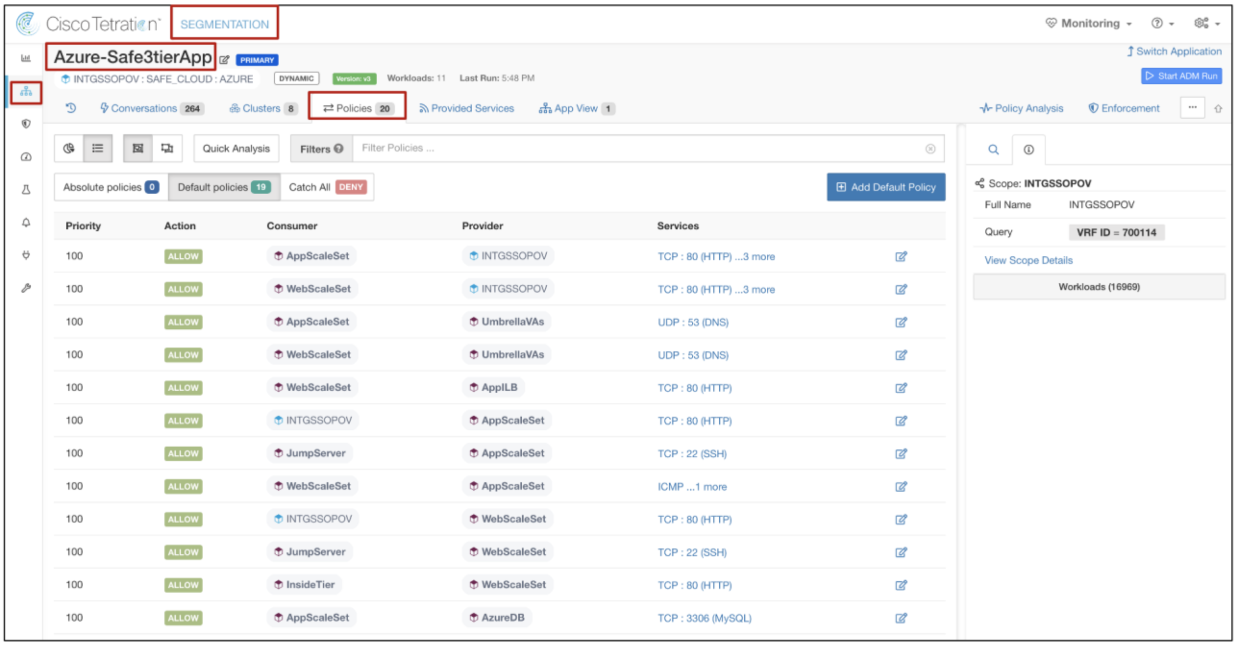
Workloads (2)

10.83.2.4	appscales000...	CentOS 7.7
10.83.2.5	appscales000...	CentOS 7.7

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 workloads via firewall’s inside interface
- Traffic between the workloads
    - Web servers to app load balancer
    - App load balancer to app servers
    - App servers to database
- Management tier to all the workloads

- Outbound internet access from all the workloads for updates/patches, DNS, DHCP, NTP



Azure-Safe3tierApp PRIMARY

INTGSSOPOV : SAFE_CLOUD : AZURE DYNAMIC Version: v3 Workloads: 11 Last Run: 5:48 PM

Absolute policies 0 | Default policies 19 | Catch All DENY

Priority	Action	Consumer	Provider	Services
100	ALLOW	AppScaleSet	INTGSSOPOV	TCP : 80 (HTTP) ...3 more
100	ALLOW	WebScaleSet	INTGSSOPOV	TCP : 80 (HTTP) ...3 more
100	ALLOW	AppScaleSet	UmbrellaVAs	UDP : 53 (DNS)
100	ALLOW	WebScaleSet	UmbrellaVAs	UDP : 53 (DNS)
100	ALLOW	WebScaleSet	ApplLB	TCP : 80 (HTTP)
100	ALLOW	INTGSSOPOV	AppScaleSet	TCP : 80 (HTTP)
100	ALLOW	JumpServer	AppScaleSet	TCP : 22 (SSH)
100	ALLOW	WebScaleSet	AppScaleSet	ICMP ...1 more
100	ALLOW	INTGSSOPOV	WebScaleSet	TCP : 80 (HTTP)
100	ALLOW	JumpServer	WebScaleSet	TCP : 22 (SSH)
100	ALLOW	InsideTier	WebScaleSet	TCP : 80 (HTTP)
100	ALLOW	AppScaleSet	AzureDB	TCP : 3306 (MySQL)

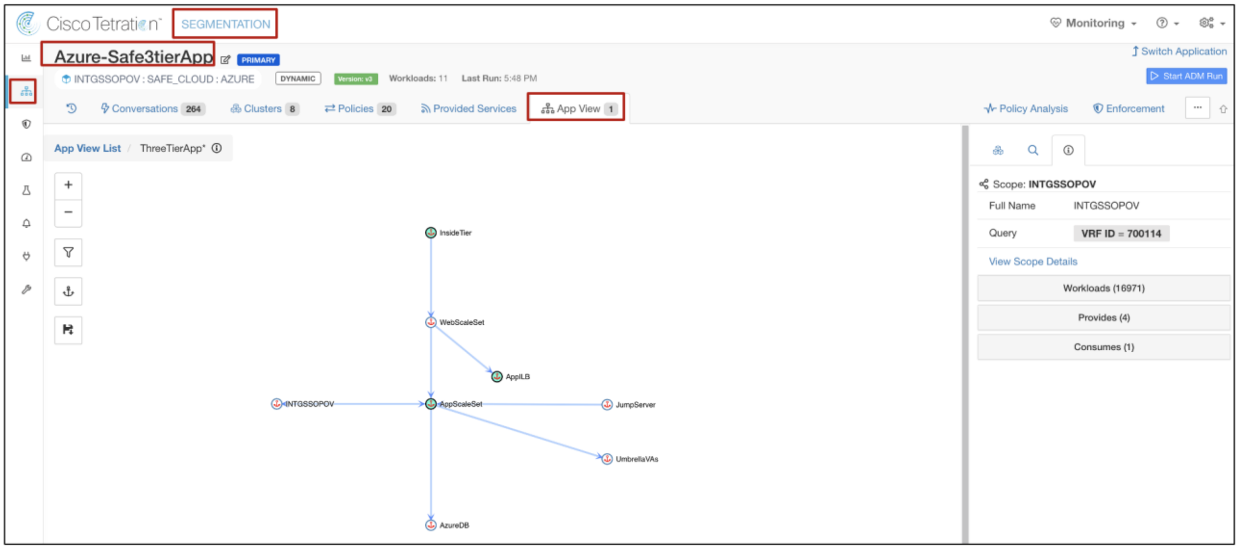
Scope: INTGSSOPOV

Full Name	INTGSSOPOV
Query	VRF ID = 700114

View Scope Details

Workloads (16969)

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.



Azure-Safe3tierApp PRIMARY

INTGSSOPOV : SAFE_CLOUD : AZURE DYNAMIC Version: v3 Workloads: 11 Last Run: 5:48 PM

Scope: INTGSSOPOV

Full Name	INTGSSOPOV
Query	VRF ID = 700114

View Scope Details

Workloads (16971)

Provides (4)

Consumes (1)

Test case 3: Enforcing the policies on workloads.

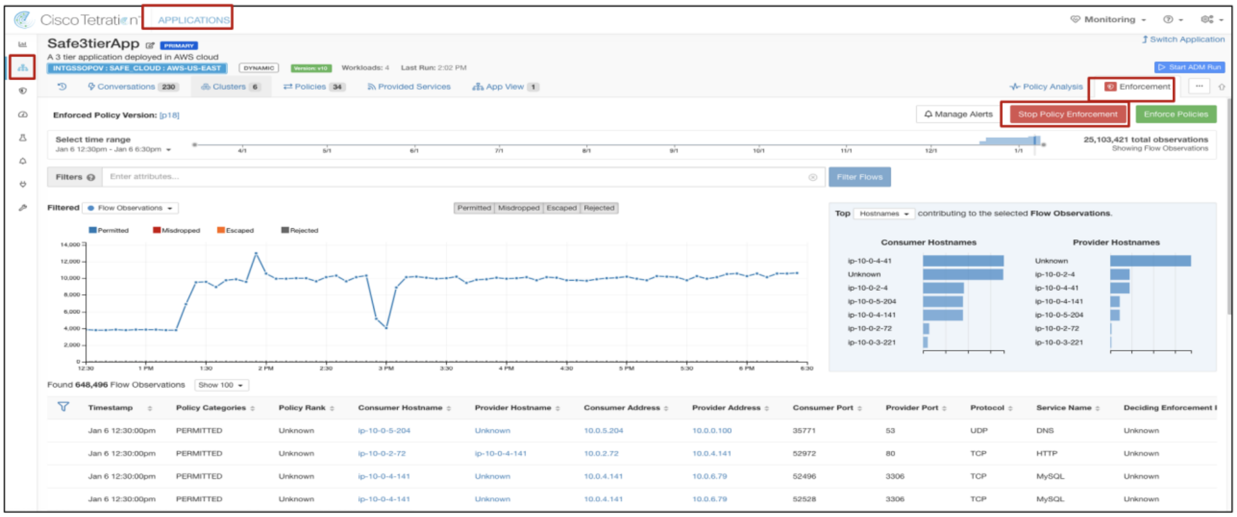
This test case focuses on enforcing the policy set that we formulated in Test Case 2. We will publish the policies and verify if those are enforced as expected.

Validation procedure:

Step 1. Publish the policies

Step 2. Verify policy enforcement on workloads

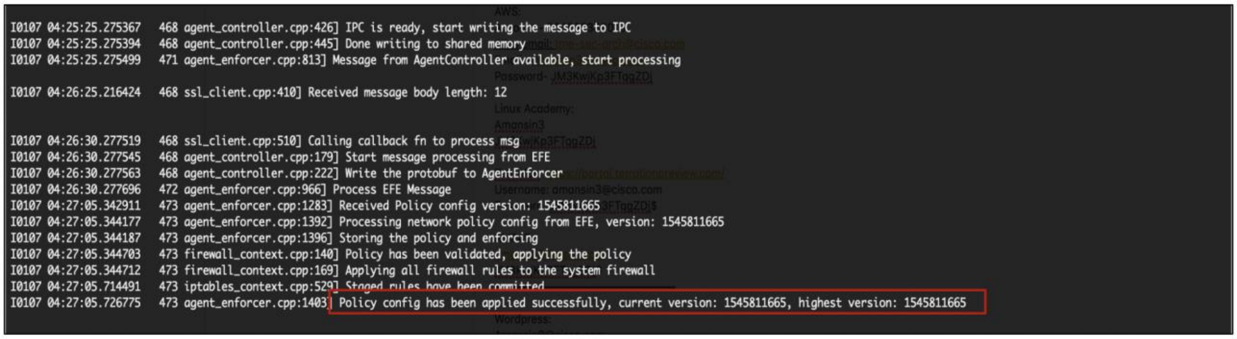
Step 1. **Publish the policies –** Select the ‘Enforcement’ tab on the Tetration portal within the application workspace and click on ‘Enforce Policies’.



Found **648,496** Flow Observations

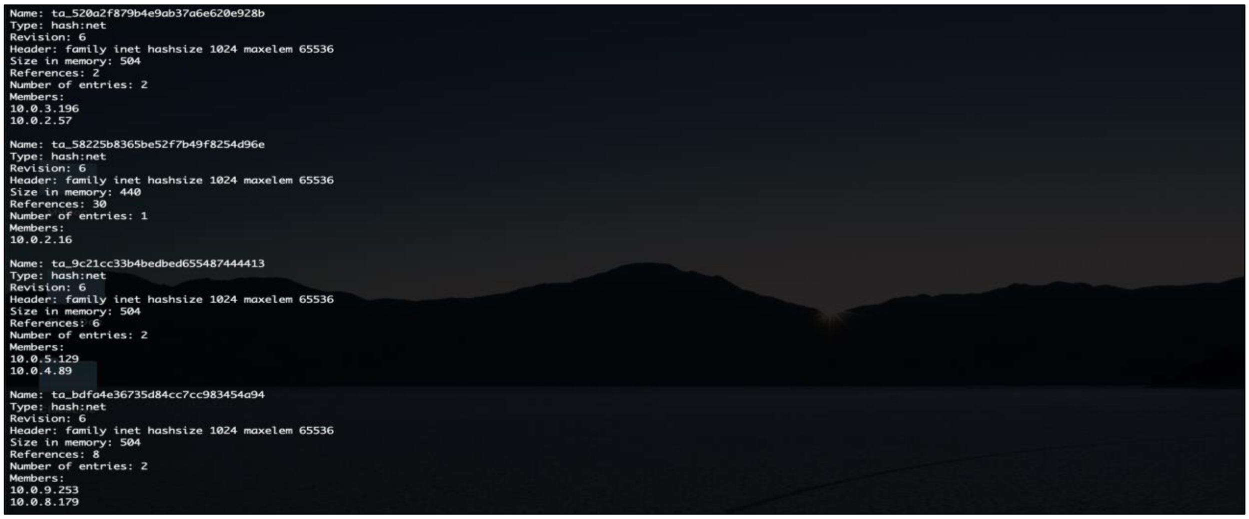
Timestamp	Policy Categories	Policy Rank	Consumer Hostname	Provider Hostname	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Service Name	Deciding Enforcement I
Jan 6 12:30:00pm	PERMITTED	Unknown	ip-10-0-5-204	Unknown	10.0.5.204	10.0.0.100	35771	53	UDP	DNS	Unknown
Jan 6 12:30:00pm	PERMITTED	Unknown	ip-10-0-2-72	ip-10-0-4-141	10.0.2.72	10.0.4.141	52972	80	TCP	HTTP	Unknown
Jan 6 12:30:00pm	PERMITTED	Unknown	ip-10-0-4-141	Unknown	10.0.4.141	10.0.6.79	52496	3306	TCP	MySQL	Unknown
Jan 6 12:30:00pm	PERMITTED	Unknown	ip-10-0-4-141	Unknown	10.0.4.141	10.0.6.79	52528	3306	TCP	MySQL	Unknown

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   468 agent_controller.cpp:426] IPC is ready, start writing the message to IPC
I0107 04:25:25.275394   468 agent_controller.cpp:445] Done writing to shared memory
I0107 04:25:25.275499   471 agent_enforcer.cpp:813] Message from AgentController available, start processing

I0107 04:26:25.216424   468 ssl_client.cpp:410] Received message body length: 12


I0107 04:26:30.277519   468 ssl_client.cpp:510] Calling callback fn to process msg
I0107 04:26:30.277545   468 agent_controller.cpp:179] Start message processing from EFE
I0107 04:26:30.277563   468 agent_controller.cpp:222] Write the protobuf to AgentEnforcer
I0107 04:26:30.277696   472 agent_enforcer.cpp:966] Process EFE Message
I0107 04:27:05.342911   473 agent_enforcer.cpp:1283] Received Policy config version: 1545811665
I0107 04:27:05.344177   473 agent_enforcer.cpp:1392] Processing network policy config from EFE, version: 1545811665
I0107 04:27:05.344187   473 agent_enforcer.cpp:1396] Storing the policy and enforcing
I0107 04:27:05.344703   473 firewall_context.cpp:140] Policy has been validated, applying the policy
I0107 04:27:05.344712   473 firewall_context.cpp:169] Applying all firewall rules to the system firewall
I0107 04:27:05.714491   473 iptables_context.cpp:529] Staged rules have been commited
I0107 04:27:05.726775   473 agent_enforcer.cpp:1403] 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.



```
Name: ta_520a2f879b4e9ab37a6e620e928b
Type: hash:net
Revision: 6
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 504
References: 2
Number of entries: 2
Members:
10.0.3.196
10.0.2.57

Name: ta_58225b8365be52f7b49f8254d96e
Type: hash:net
Revision: 6
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 440
References: 30
Number of entries: 1
Members:
10.0.2.16

Name: ta_9c21cc33b4bedbed655487444413
Type: hash:net
Revision: 6
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 504
References: 6
Number of entries: 2
Members:
10.0.5.129
10.0.4.89

Name: ta_bdfa4e36735d84cc7cc983454a94
Type: hash:net
Revision: 6
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 504
References: 8
Number of entries: 2
Members:
10.0.9.253
10.0.8.179
```

Test case 4: Discovering the vulnerable packages on the Azure workloads.

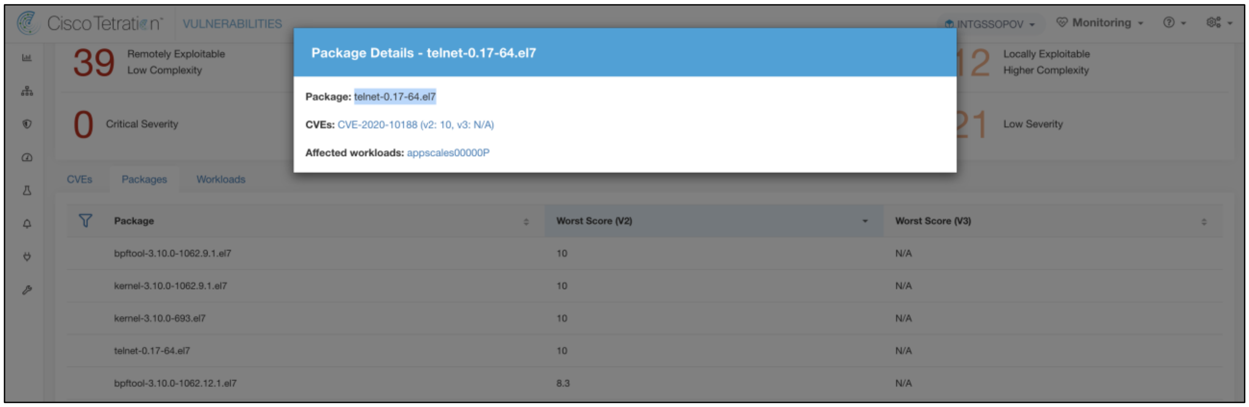
This test case looks for vulnerable packages/software installed on various workloads in our Azure cloud. We identify a vulnerable package/software on our workloads, patch those and then rerun the report.

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 'telnet-0.17-64.el7' as shown below.



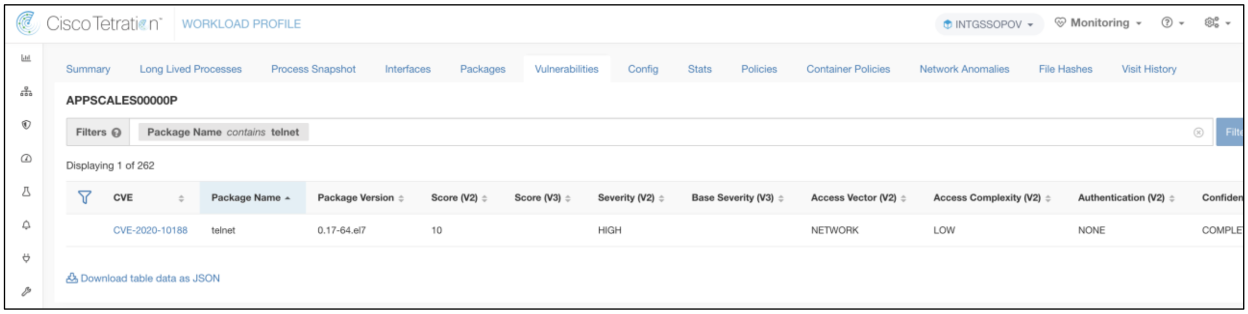
Package Details - telnet-0.17-64.el7

Package: telnet-0.17-64.el7

CVEs: CVE-2020-10188 (v2: 10, v3: N/A)

Affected workloads: appscales00000P

Package	Worst Score (V2)	Worst Score (V3)
bpftool-3.10.0-1062.9.1.el7	10	N/A
kernel-3.10.0-1062.9.1.el7	10	N/A
kernel-3.10.0-693.el7	10	N/A
telnet-0.17-64.el7	10	N/A
bpftool-3.10.0-1062.12.1.el7	8.3	N/A



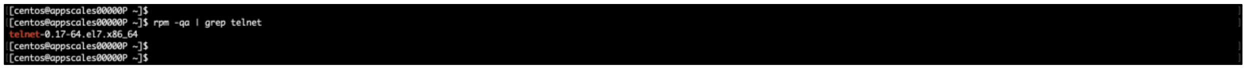
APPSCALES00000P

Filters: Package Name *contains* telnet

Displaying 1 of 262

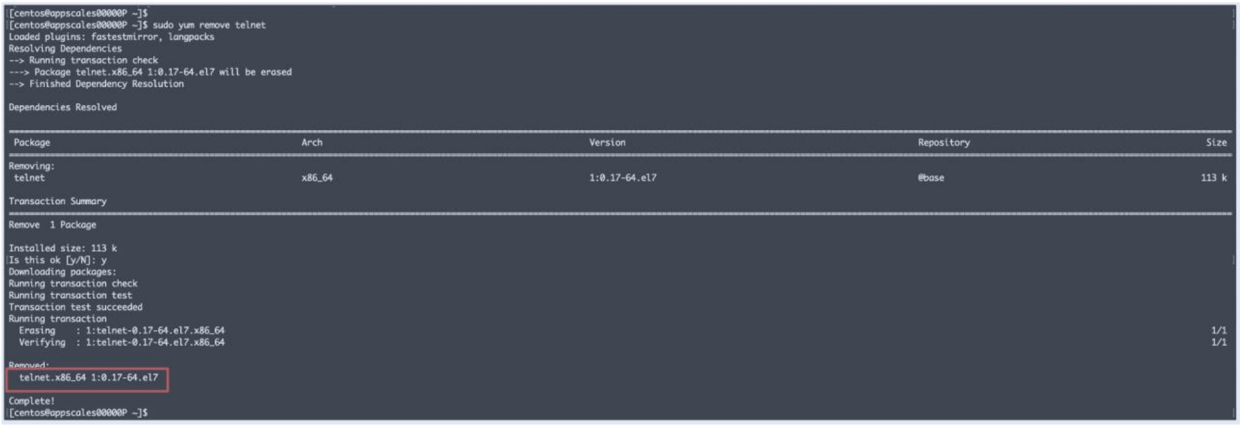
CVE	Package Name	Package Version	Score (V2)	Score (V3)	Severity (V2)	Base Severity (V3)	Access Vector (V2)	Access Complexity (V2)	Authentication (V2)	Confiden
CVE-2020-10188	telnet	0.17-64.el7	10		HIGH		NETWORK	LOW	NONE	COMPLE

We see that the workload 'appscales00000P' is affected by this CVE. Logon to this workload and verify the telnet package.



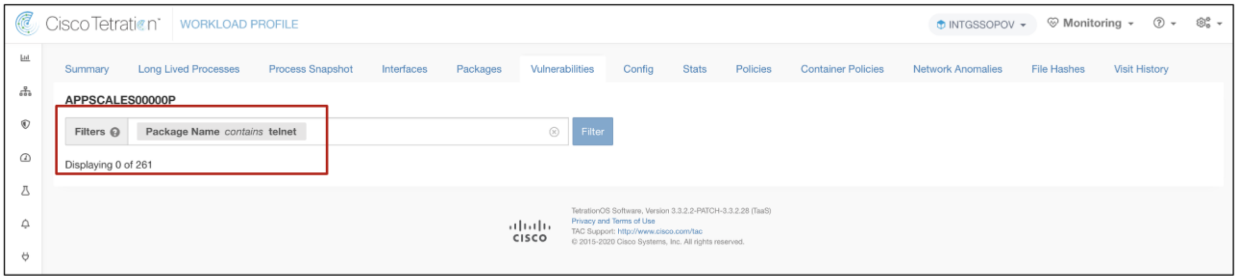
```
[centos@appscales00000P ~]$
[centos@appscales00000P ~]$ rpm -qa | grep telnet
telnet-0.17-64.el7.x86_64
[centos@appscales00000P ~]$
[centos@appscales00000P ~]$
```

Step 2. Fix the vulnerability and rerun the report – We uninstall the telnet package from this workload.



```
[centos@appscales00000P ~]$
[centos@appscales00000P ~]$ sudo yum remove telnet
Loaded plugins: fastestmirror, langpacks
Resolving Dependencies
--> Running transaction check
---> Package telnet.x86_64 1:0.17-64.el7 will be erased
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================================
 Package                               Arch                                  Version                                    Repository            Size
================================================================================================================================================
Removing:
 telnet                                x86_64                                1:0.17-64.el7                              @base                113 k

Transaction Summary
================================================================================================================================================
Remove  1 Package

Installed size: 113 k
Is this ok [y/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Erasing    : 1:telnet-0.17-64.el7.x86_64                                                                                                   1/1
  Verifying  : 1:telnet-0.17-64.el7.x86_64                                                                                                   1/1

Removed:
  telnet.x86_64 1:0.17-64.el7

Complete!
[centos@appscales00000P ~]$
```

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 Telnet show up anymore.



APPSCALES00000P

Filters: Package Name *contains* telnet

Displaying 0 of 261

TetrationOS Software, Version 3.3.2.2-PATCH-3.3.2.28 (TaaS)
Privacy and Terms of Use
TAC Support: http://www.cisco.com/tac
© 2015-2020 Cisco Systems, Inc. All rights reserved.

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.

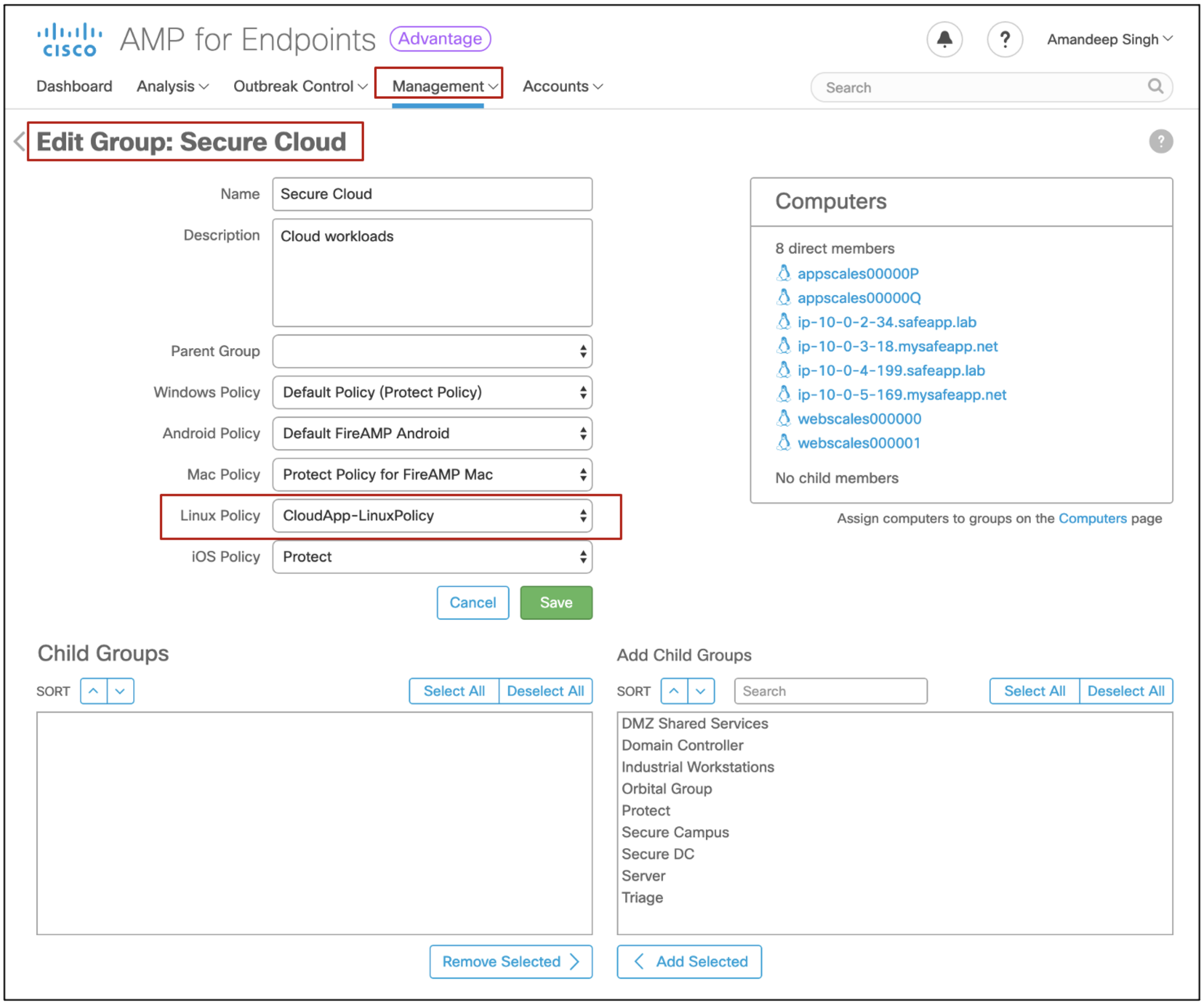
Validation procedure:

Step 1. Setting up AMP4E policy to quarantine a suspicious file

Step 2. Verifying the deletion of a suspicious file

Step 1. 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 Azure cloud.



Edit Group: Secure Cloud

Name	Secure Cloud
Description	Cloud workloads
Parent Group	
Windows Policy	Default Policy (Protect Policy)
Android Policy	Default FireAMP Android
Mac Policy	Protect Policy for FireAMP Mac
Linux Policy	CloudApp-LinuxPolicy
iOS Policy	Protect

Computers

8 direct members
- appscales00000P
- appscales00000Q
- ip-10-0-2-34.safeapp.lab
- ip-10-0-3-18.mysafeapp.net
- ip-10-0-4-199.safeapp.lab
- ip-10-0-5-169.mysafeapp.net
- webscales000000
- webscales000001

No child members

Assign computers to groups on the Computers page

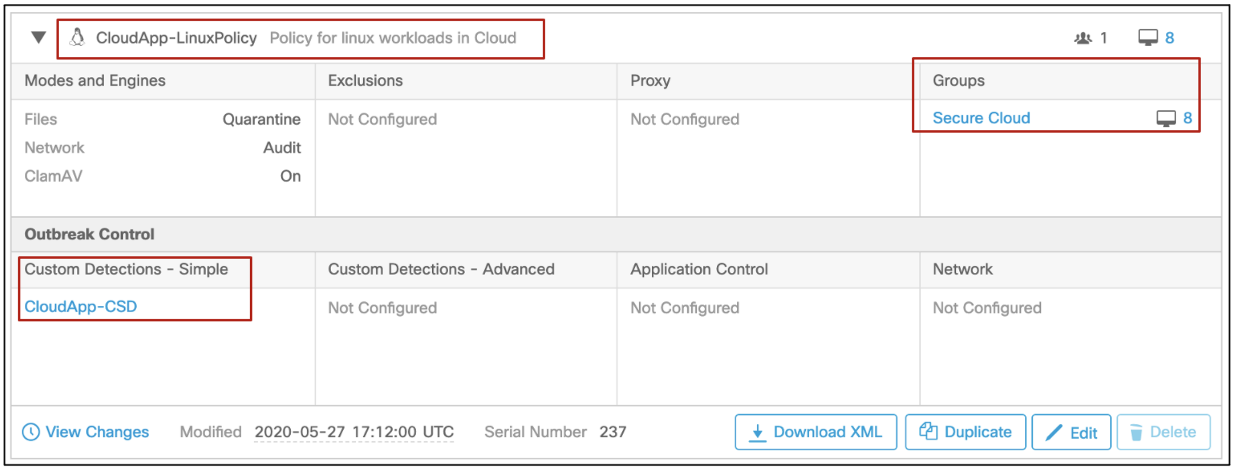
Child Groups

Add Child Groups

DMZ Shared Services
Domain Controller
Industrial Workstations
Orbital Group
Protect
Secure Campus
Secure DC
Server
Triage

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 Azure VNET 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 1 8

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	Not Configured	Not Configured	Secure Cloud 8
Network	Audit			
ClamAV	On			

Outbreak Control

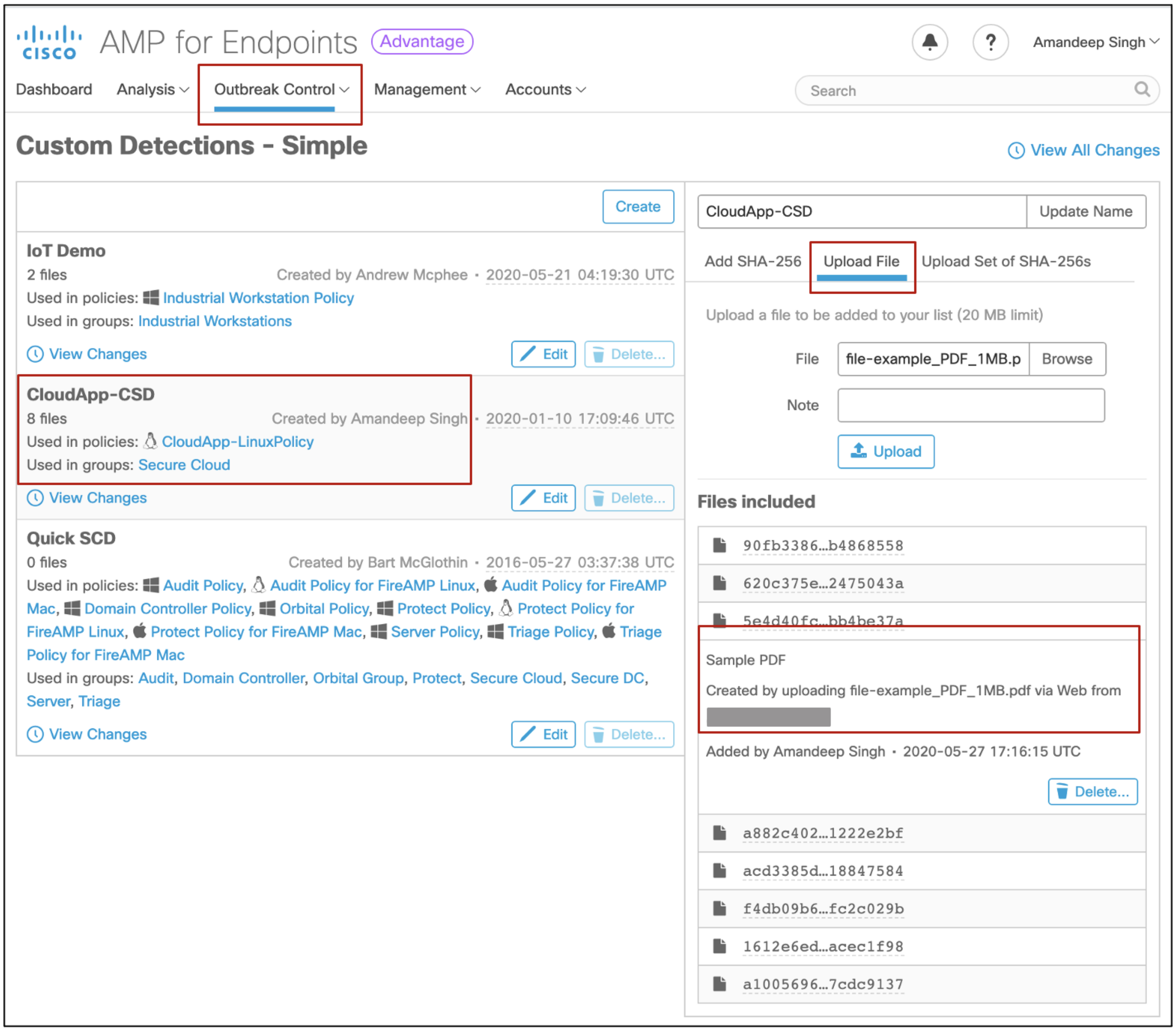
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
CloudApp-CSD	Not Configured	Not Configured	Not Configured

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 Azure 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.



Custom Detections - Simple

View All Changes

Create

IoT Demo
2 files — Created by Andrew Mcphee • 2020-05-21 04:19:30 UTC
Used in policies: Industrial Workstation Policy
Used in groups: Industrial Workstations
View Changes — Edit — Delete...

CloudApp-CSD
8 files — Created by Amandeep Singh • 2020-01-10 17:09:46 UTC
Used in policies: CloudApp-LinuxPolicy
Used in groups: Secure Cloud
View Changes — Edit — Delete...

Quick SCD
0 files — Created by Bart McGlothin • 2016-05-27 03:37:38 UTC
Used in policies: Audit Policy, Audit Policy for FireAMP Linux, Audit Policy for FireAMP Mac, Domain Controller Policy, Orbital Policy, Protect Policy, Protect Policy for FireAMP Linux, Protect Policy for FireAMP Mac, Server Policy, Triage Policy, Triage Policy for FireAMP Mac
Used in groups: Audit, Domain Controller, Orbital Group, Protect, Secure Cloud, Secure DC, Server, Triage
View Changes — Edit — Delete...

CloudApp-CSD — Update Name

Add SHA-256 — Upload File — Upload Set of SHA-256s

Upload a file to be added to your list (20 MB limit)

File: file-example_PDF_1MB.p — Browse

Note:

Upload

Files included

- 90fb3386…b4868558
- 620c375e…2475043a
- 5e4d40fc…bb4be37a

Sample PDF

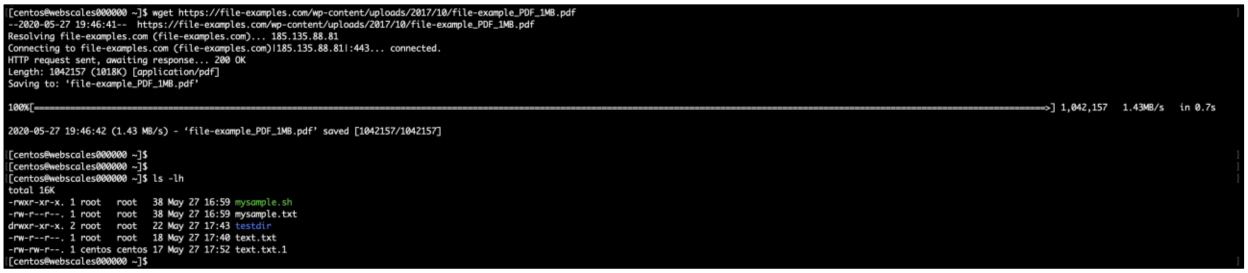
Created by uploading file-example_PDF_1MB.pdf via Web from [redacted]

Added by Amandeep Singh • 2020-05-27 17:16:15 UTC

Delete...

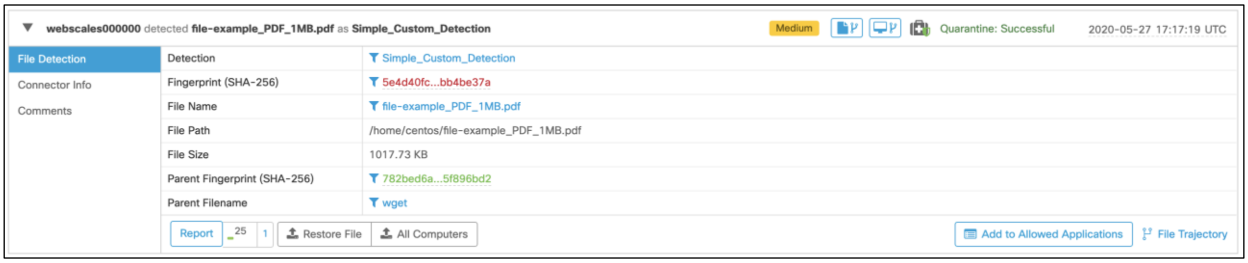
- a882c402…1222e2bf
- acd3385d…18847584
- f4db09b6…fc2c029b
- 1612e6ed…acec1f98
- a1005696…7cdc9137

Step 2. Verify the deletion of the suspicious program – Log on to a cloud workload, we picked one of the web servers in web VSS. 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.



```
[centos@webscales000000 ~]$ wget https://file-examples.com/wp-content/uploads/2017/10/file-example_PDF_1MB.pdf
--2020-05-27 19:46:41--  https://file-examples.com/wp-content/uploads/2017/10/file-example_PDF_1MB.pdf
Resolving file-examples.com (file-examples.com)... 185.135.88.81
Connecting to file-examples.com (file-examples.com)|185.135.88.81|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1042157 (1018K) [application/pdf]
Saving to: ‘file-example_PDF_1MB.pdf’

100%[=========================================================================================================================>] 1,042,157   1.43MB/s   in 0.7s

2020-05-27 19:46:42 (1.43 MB/s) - ‘file-example_PDF_1MB.pdf’ saved [1042157/1042157]

[centos@webscales000000 ~]$
[centos@webscales000000 ~]$
[centos@webscales000000 ~]$ ls -lh
total 16K
-rwxr-xr-x. 1 root   root   38 May 27 16:59 mysample.sh
-rw-r--r--. 1 root   root   38 May 27 16:59 mysample.txt
drwxr-xr-x. 2 root   root   22 May 27 17:43 testdir
-rw-r--r--. 1 root   root   18 May 27 17:40 text.txt
-rw-rw-r--. 1 centos centos 17 May 27 17:52 text.txt.1
[centos@webscales000000 ~]$
```

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.



▼ **webscales000000** detected **file-example_PDF_1MB.pdf** as **Simple_Custom_Detection** Medium Quarantine: Successful 2020-05-27 17:17:19 UTC

File Detection	Detection	Simple_Custom_Detection
Connector Info	Fingerprint (SHA-256)	5e4d40fc...bb4be37a
Comments	File Name	file-example_PDF_1MB.pdf
	File Path	/home/centos/file-example_PDF_1MB.pdf
	File Size	1017.73 KB
	Parent Fingerprint (SHA-256)	782bed6a...5f896bd2
	Parent Filename	wget

Stealthwatch Cloud

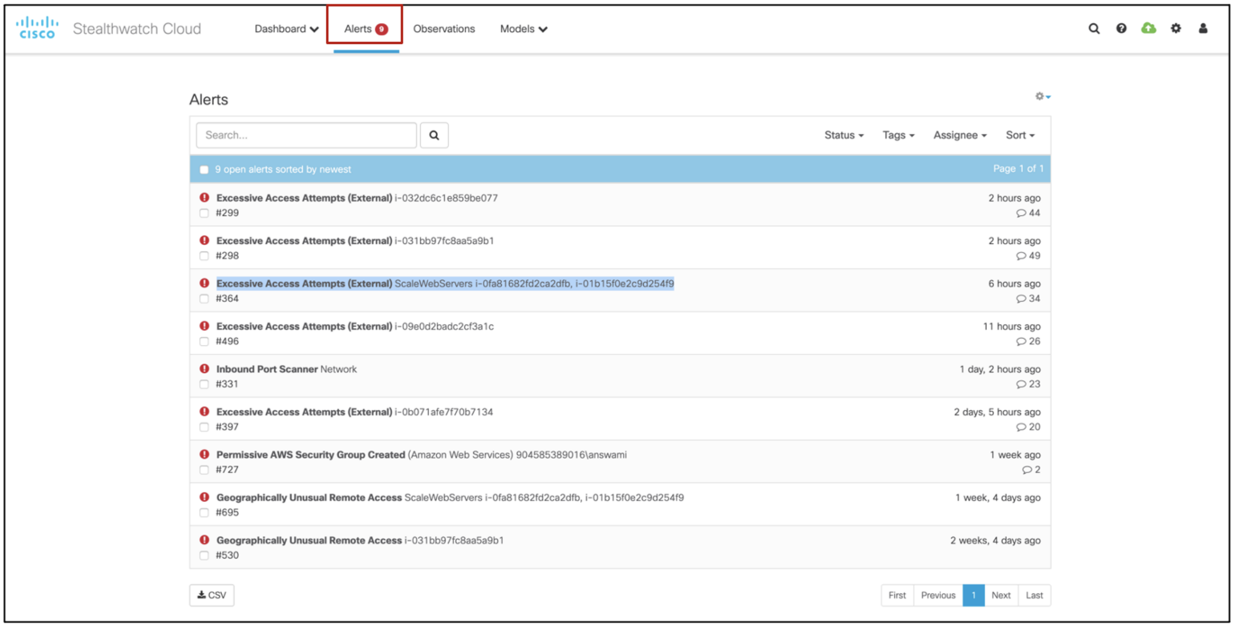
Test Case: Monitor suspicious activity

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

Validation procedure:

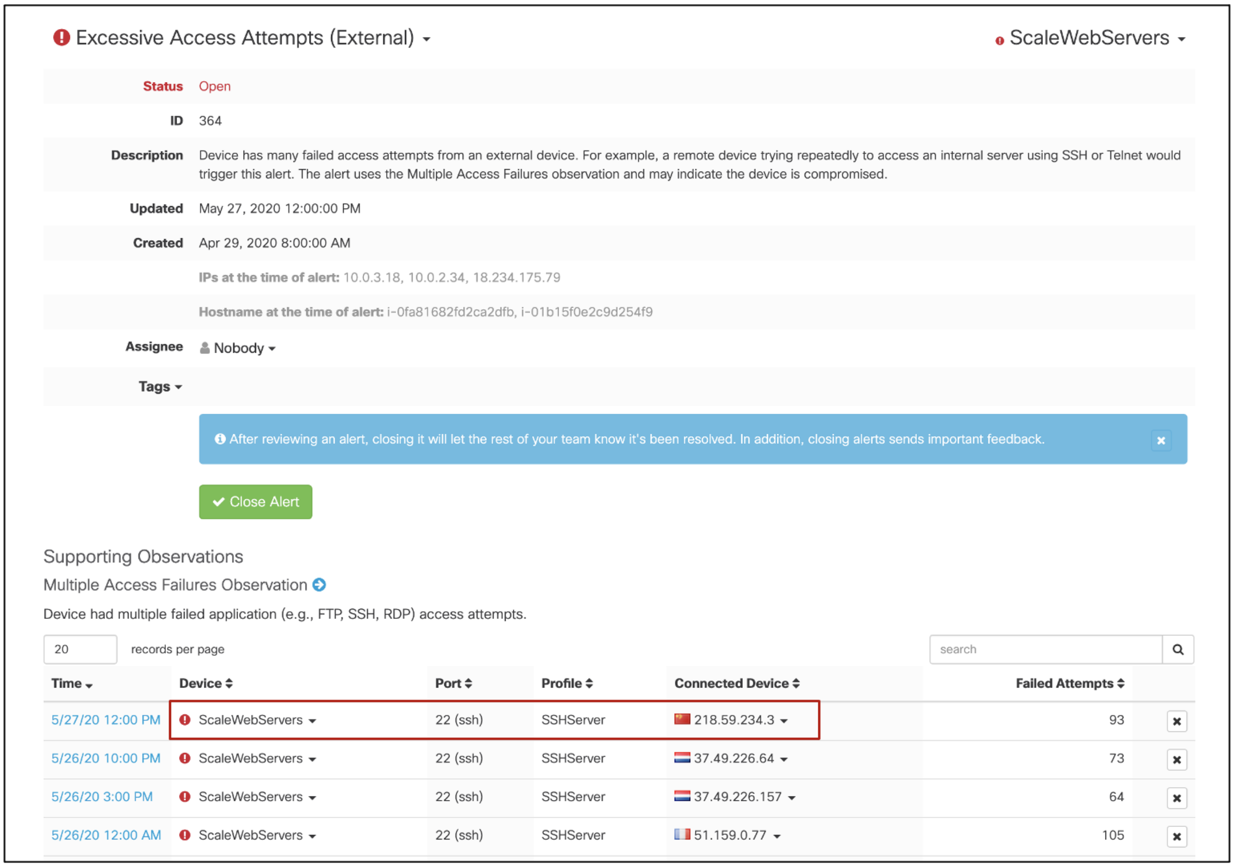
Step 1. Monitor suspicious activity in Stealthwatch Cloud

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.



9 open alerts sorted by newest — Page 1 of 1

Excessive Access Attempts (External) i-032dc6c1e859be077 #299	2 hours ago 44
Excessive Access Attempts (External) i-031bb97fc8aa5a9b1 #298	2 hours ago 49
Excessive Access Attempts (External) ScaleWebServers i-0fa81682fd2ca2dfb, i-01b15f0e2c9d254f9 #364	6 hours ago 34
Excessive Access Attempts (External) i-09e0d2badc2cf3a1c #496	11 hours ago 26
Inbound Port Scanner Network #331	1 day, 2 hours ago 23
Excessive Access Attempts (External) i-0b071afe7f70b7134 #397	2 days, 5 hours ago 20
Permissive AWS Security Group Created (Amazon Web Services) 904585389016\answami #727	1 week ago 2
Geographically Unusual Remote Access ScaleWebServers i-0fa81682fd2ca2dfb, i-01b15f0e2c9d254f9 #695	1 week, 4 days ago
Geographically Unusual Remote Access i-031bb97fc8aa5a9b1 #530	2 weeks, 4 days ago



Excessive Access Attempts (External) ▾ ScaleWebServers ▾

Status Open

ID 364

Description Device has many failed access attempts from an external device. For example, a remote device trying repeatedly to access an internal server using SSH or Telnet would trigger this alert. The alert uses the Multiple Access Failures observation and may indicate the device is compromised.

Updated May 27, 2020 12:00:00 PM

Created Apr 29, 2020 8:00:00 AM

IPs at the time of alert: 10.0.3.18, 10.0.2.34, 18.234.175.79

Hostname at the time of alert: i-0fa81682fd2ca2dfb, i-01b15f0e2c9d254f9

Assignee Nobody ▾

Tags ▾

After reviewing an alert, closing it will let the rest of your team know it's been resolved. In addition, closing alerts sends important feedback.

Supporting Observations

Multiple Access Failures Observation

Device had multiple failed application (e.g., FTP, SSH, RDP) access attempts.

20 records per page

Time ▾	Device ⇕	Port ⇕	Profile ⇕	Connected Device ⇕	Failed Attempts ⇕	
5/27/20 12:00 PM	ScaleWebServers ▾	22 (ssh)	SSHServer	218.59.234.3 ▾	93	✖
5/26/20 10:00 PM	ScaleWebServers ▾	22 (ssh)	SSHServer	37.49.226.64 ▾	73	✖
5/26/20 3:00 PM	ScaleWebServers ▾	22 (ssh)	SSHServer	37.49.226.157 ▾	64	✖
5/26/20 12:00 AM	ScaleWebServers ▾	22 (ssh)	SSHServer	51.159.0.77 ▾	105	✖

Cisco Umbrella

Test Case: DNS security

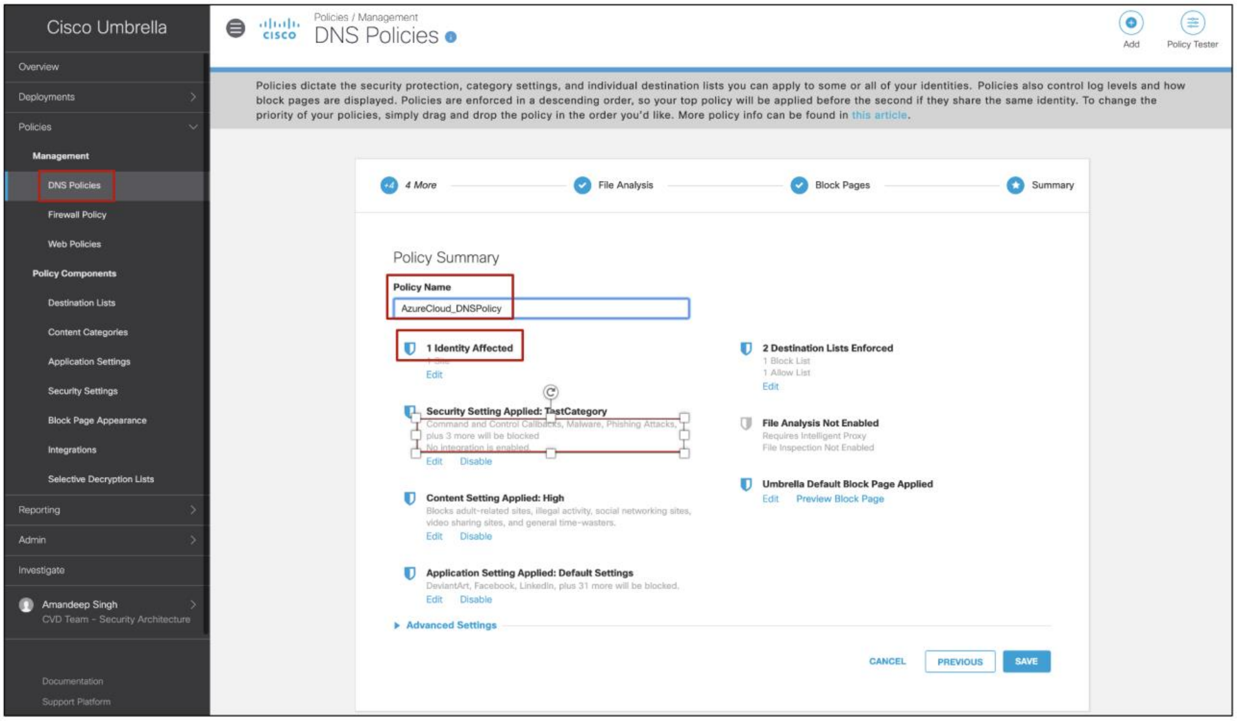
This test case involves adding DNS layer security to the Azure workloads. We created a DNS policy for our three-tier application workloads to block malicious domains. To verify the blocks, we accessed a test domain 'examplemalwaredomain.com' and then confirmed the same from Umbrella reporting.

Validation procedure:

Step 1. Set up DNS policy for Azure workloads

Step 2. Confirm if malware domain is blocked

Step 1. Set up DNS policy for Azure 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.



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 are enforced 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 the order you'd like. More policy info can be found in this article.

Policy Summary

Policy Name: AzureCloud_DNSPolicy

1 Identity Affected
1 Site
Edit

Security Setting Applied: TestCategory
Command and Control Callbacks, Malware, Phishing Attacks, plus 3 more will be blocked
No integration is enabled.
Edit Disable

Content Setting Applied: High
Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.
Edit Disable

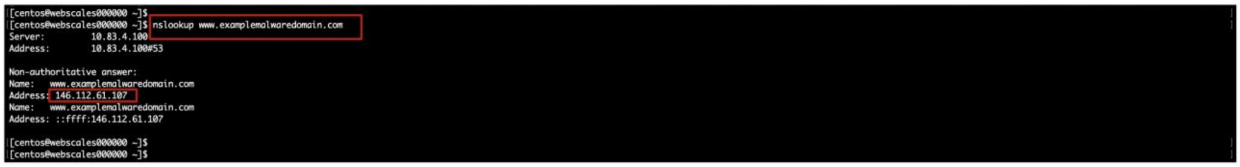
Application Setting Applied: Default Settings
DeviantArt, Facebook, LinkedIn, plus 31 more will be blocked.
Edit Disable

2 Destination Lists Enforced
1 Block List
1 Allow List
Edit

File Analysis Not Enabled
Requires Intelligent Proxy
File Inspection Not Enabled

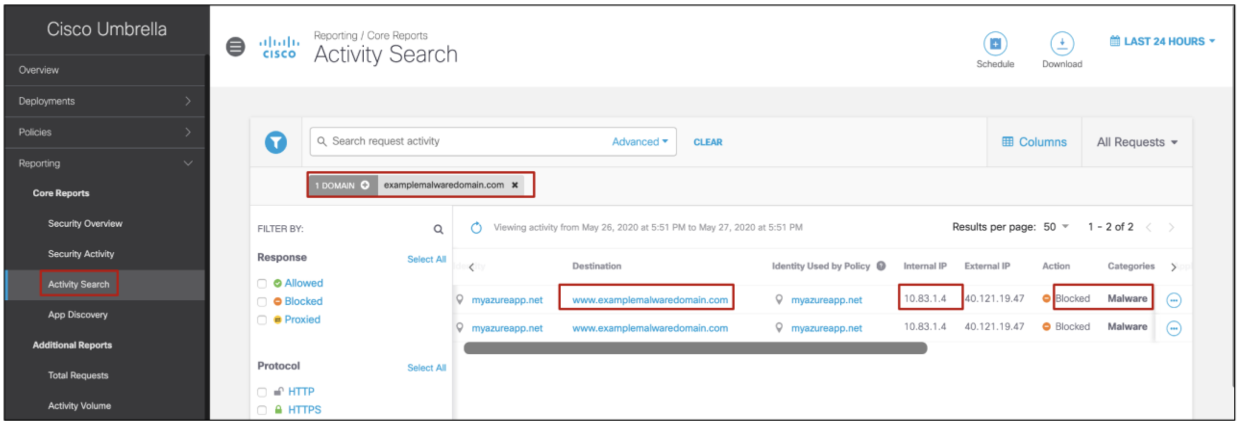
Umbrella Default Block Page Applied
Edit Preview Block Page

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.



```
[centos@webscales000000 ~]$
[centos@webscales000000 ~]$ nslookup www.examplemalwaredomain.com
Server:         10.83.4.100
Address:        10.83.4.100#53

Non-authoritative answer:
Name:   www.examplemalwaredomain.com
Address: 146.112.61.107
Name:   www.examplemalwaredomain.com
Address: ::ffff:146.112.61.107

[centos@webscales000000 ~]$
[centos@webscales000000 ~]$
```

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



1 DOMAIN: examplemalwaredomain.com

Viewing activity from May 26, 2020 at 5:51 PM to May 27, 2020 at 5:51 PM

Results per page: 50   1 - 2 of 2

Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action	Categories
myazureapp.net	www.examplemalwaredomain.com	myazureapp.net	10.83.1.4	40.121.19.47	Blocked	Malware
myazureapp.net	www.examplemalwaredomain.com	myazureapp.net	10.83.1.4	40.121.19.47	Blocked	Malware

Cisco Firepower NGFWv and CDO

Test Case: Enforce an access policy using CDO

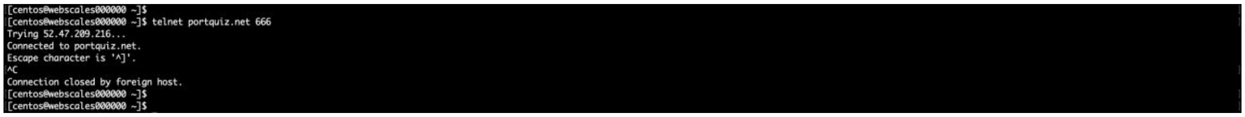
In this test case, we will try to lock down the outbound access for our cloud workloads for specific TCP ports. We will use CDO to manage the FTDs we deployed in our Azure cloud. We already onboarded the FTDs to the CDO in the implementation section of this document.

Validation procedure:

Step 1. **Configure and enforce the access policy**

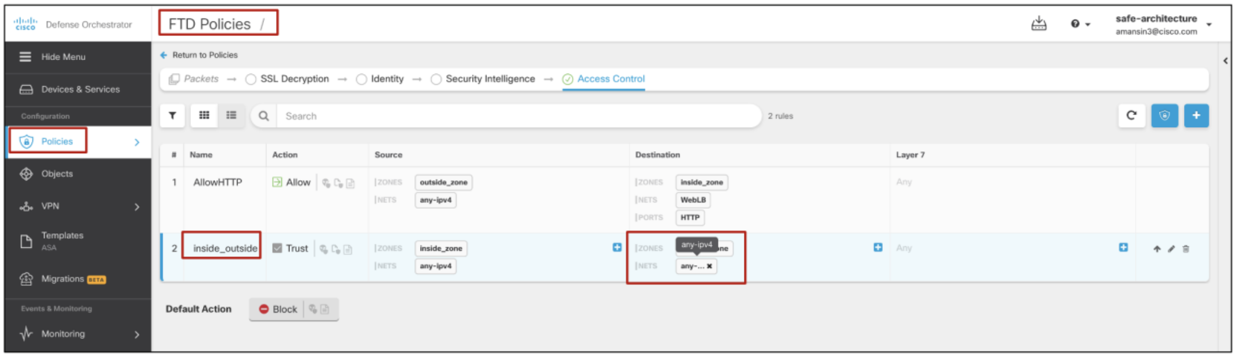
Step 2. **Verify the access block**

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.



```
[centos@webscales000000 ~]$
[centos@webscales000000 ~]$ telnet portquiz.net 666
Trying 52.47.209.216...
Connected to portquiz.net.
Escape character is '^]'.
^C
Connection closed by foreign host.
[centos@webscales000000 ~]$
[centos@webscales000000 ~]$
```

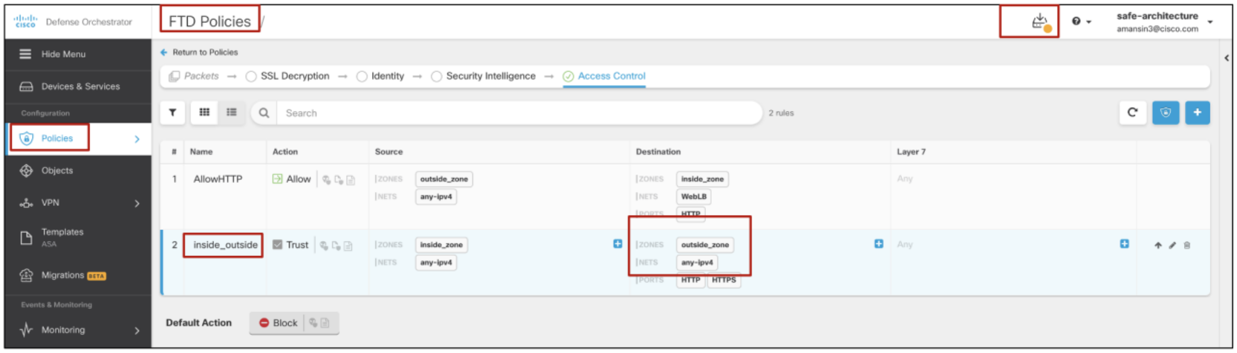
We want to block outbound access to such random TCP ports from our cloud workloads. Log on to the CDO portal and go to ‘Policies > FTD policies’ and select the policies corresponding to our Azure FTDs. We can see that the ‘inside_outside’ policy allows the cloud workloads to access any destination on any port on the Internet.



#	Name	Action	Source	Destination	Layer 7
1	AllowHTTP	Allow	ZONES outside_zone NETS any-ipv4	ZONES inside_zone NETS WebLB PORTS HTTP	Any
2	inside_outside	Trust	ZONES inside_zone NETS any-ipv4	ZONES any-ipv4 …one NETS any-… ✕	Any

Default Action ⛔ Block

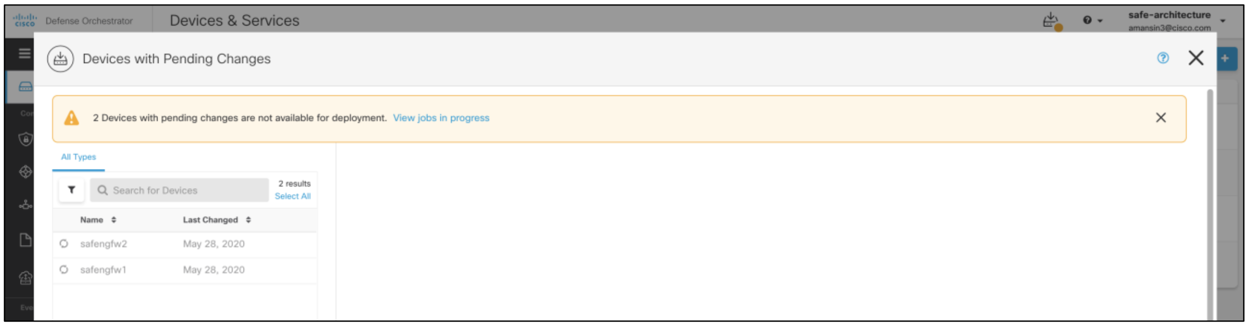
We update the policy to lock it down to just the HTTP and HTTPS ports going out to the internet.



#	Name	Action	Source	Destination	Layer 7
1	AllowHTTP	Allow	ZONES outside_zone NETS any-ipv4	ZONES inside_zone NETS WebLB PORTS HTTP	Any
2	inside_outside	Trust	ZONES inside_zone NETS any-ipv4	ZONES outside_zone NETS any-ipv4 PORTS HTTP HTTPS	Any

Default Action ⛔ Block

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.

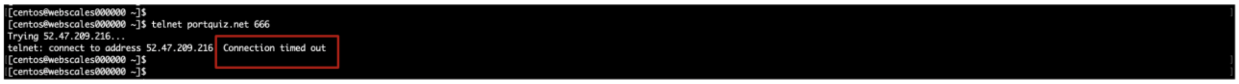


Devices with Pending Changes

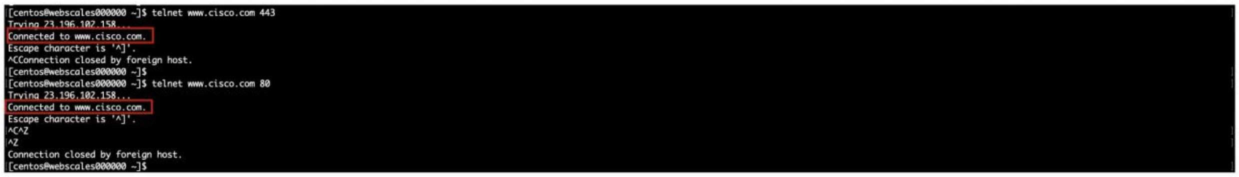
2 Devices with pending changes are not available for deployment. View jobs in progress

Name	Last Changed
safengfw2	May 28, 2020
safengfw1	May 28, 2020

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.



```
[centos@webscales000000 ~]$
[centos@webscales000000 ~]$ telnet portquiz.net 666
Trying 52.47.209.216...
telnet: connect to address 52.47.209.216  Connection timed out
[centos@webscales000000 ~]$
[centos@webscales000000 ~]$
```



```
[centos@webscales000000 ~]$ telnet www.cisco.com 443
Trying 23.196.102.158...
Connected to www.cisco.com.
Escape character is '^]'.
^CConnection closed by foreign host.
[centos@webscales000000 ~]$
[centos@webscales000000 ~]$ telnet www.cisco.com 80
Trying 23.196.102.158...
Connected to www.cisco.com.
Escape character is '^]'.
^C^Z
^Z
Connection closed by foreign host.
[centos@webscales000000 ~]$
```

Likewise, we can leverage the FTDs for network IPS and AMP capabilities.

Web Application Firewalls and DDoS Protection

Azure WAF and DDoS

Test Case: Monitor Web and DDoS activity on Azure cloud

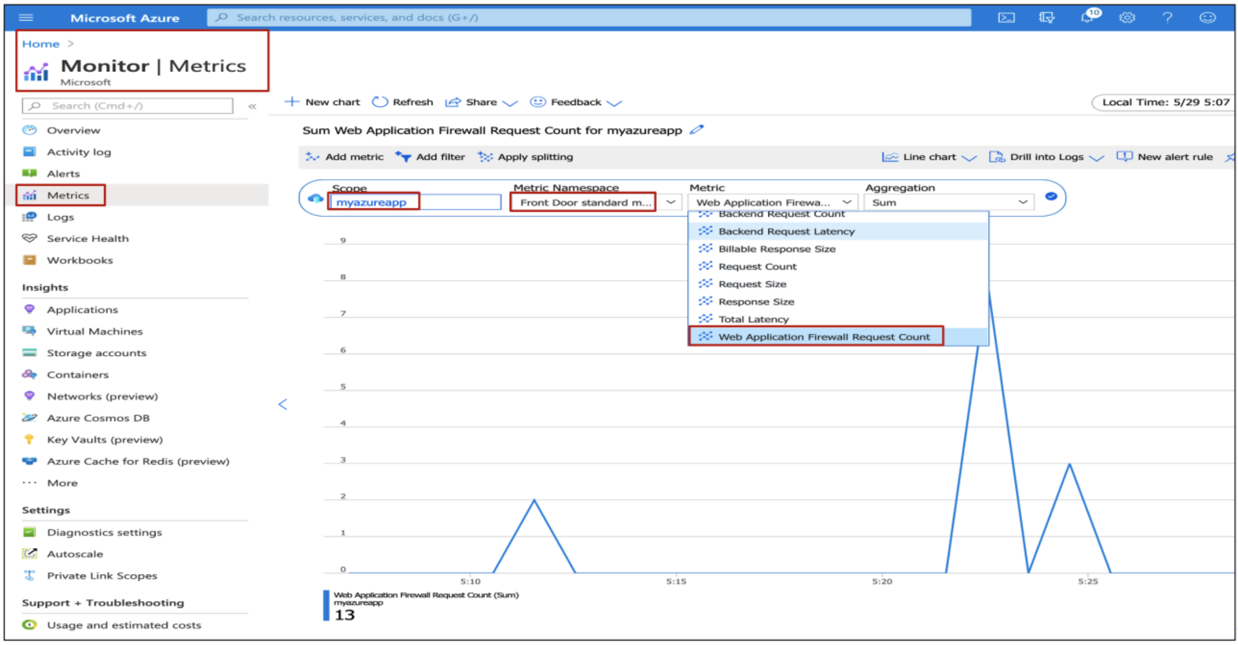
This test case involves monitoring the security events generated by the Azure cloud native WAF and DDoS service. For monitoring WAF and DDoS activity, you can either look at the Azure Metrics or do a deep dive using Azure log analytics. We will cover both the methods for each service.

Validation procedure:

Step 1. **Monitor WAF and DDoS metrics on Azure cloud**

Step 2. **Analyzing WAF and DDoS logs on Azure cloud**

Step 1. **Monitor WAF and DDoS metrics on Azure cloud –** Go to ‘Monitor’ service on the Azure portal and select metrics option on the left-hand side panel. You will be prompted to select the Scope or the service that you want to look metrics for. For viewing the metrics associated with WAF, select Azure Front Doors service that we created earlier, and then select ‘Web Application Firewall Request Count’ from the drop-down under ‘Metrics’ option, and it will allow you to plot the WAF statistics.

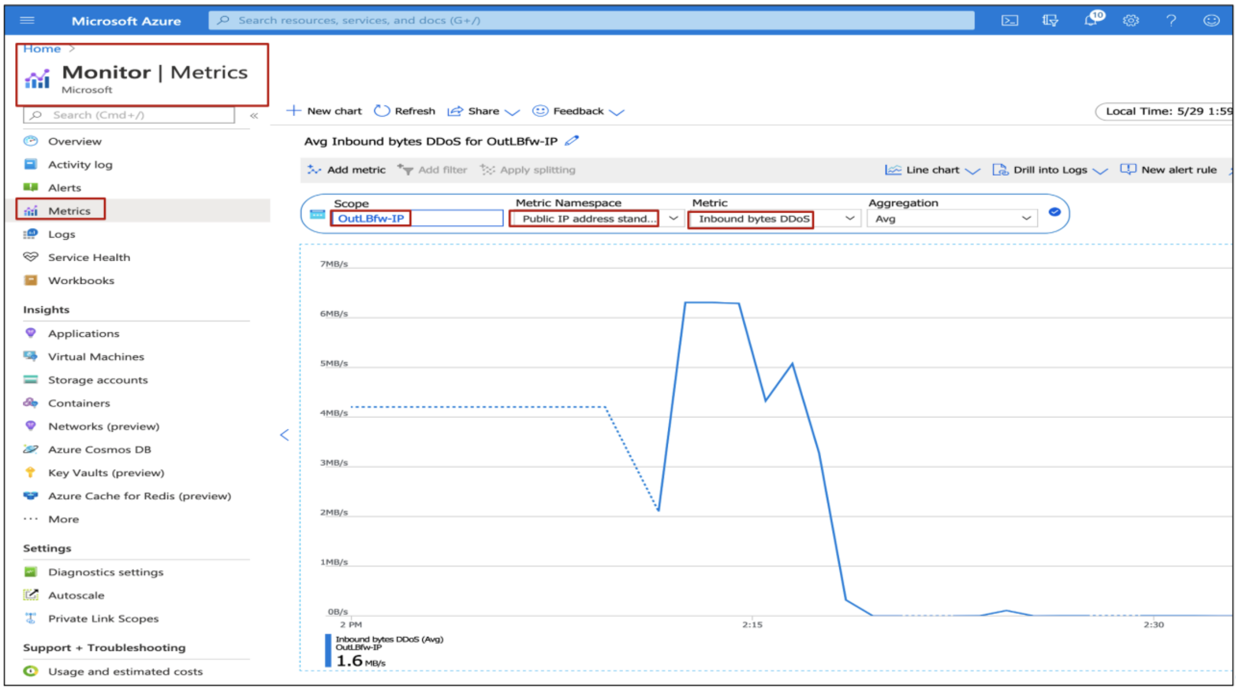


Sum Web Application Firewall Request Count for myazureapp

Scope: myazureapp
Metric Namespace: Front Door standard m...
Metric: Web Application Firewa...
Aggregation: Sum

Web Application Firewall Request Count (Sum)
myazureapp
13

In a similar manner, you can select the Public IP of the outside NGFW interfaces under Scope and plot all the DDoS related metrics.

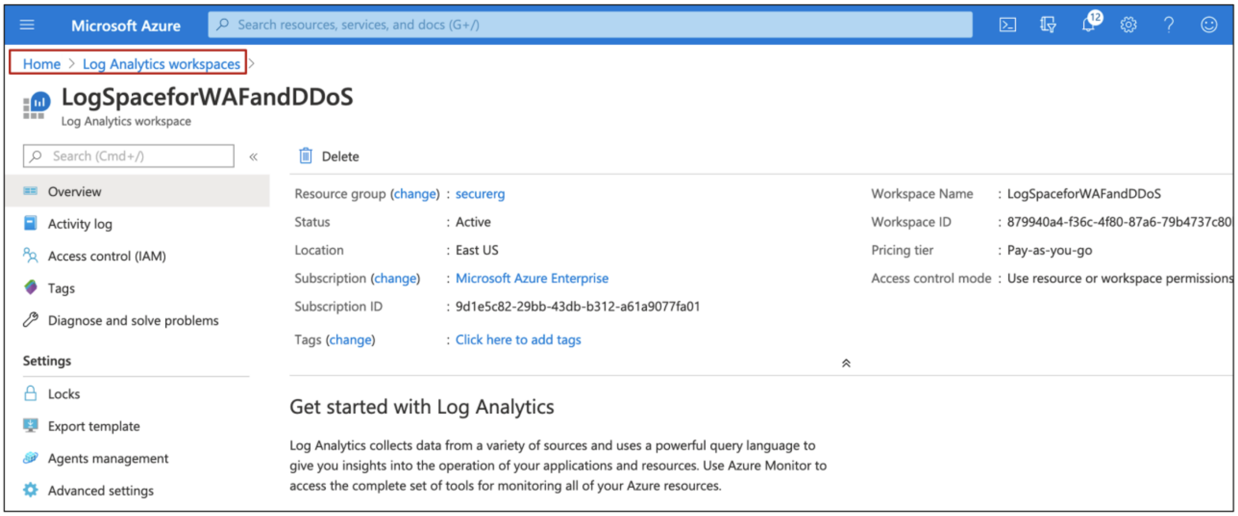


Avg Inbound bytes DDoS for OutLBfw-IP

Scope: OutLBfw-IP
Metric Namespace: Public IP address stand...
Metric: Inbound bytes DDoS
Aggregation: Avg

Inbound bytes DDoS (Avg)
OutLBfw-IP
1.6 MB/s

Step 2. **Analyzing WAF and DDoS logs on Azure cloud** – Now, we want to dive deeper into the logs, go to ‘Log Analytics workspaces’ and create a workspace for WAF and DDoS services.



Home > Log Analytics workspaces >

LogSpaceforWAFandDDoS

Log Analytics workspace

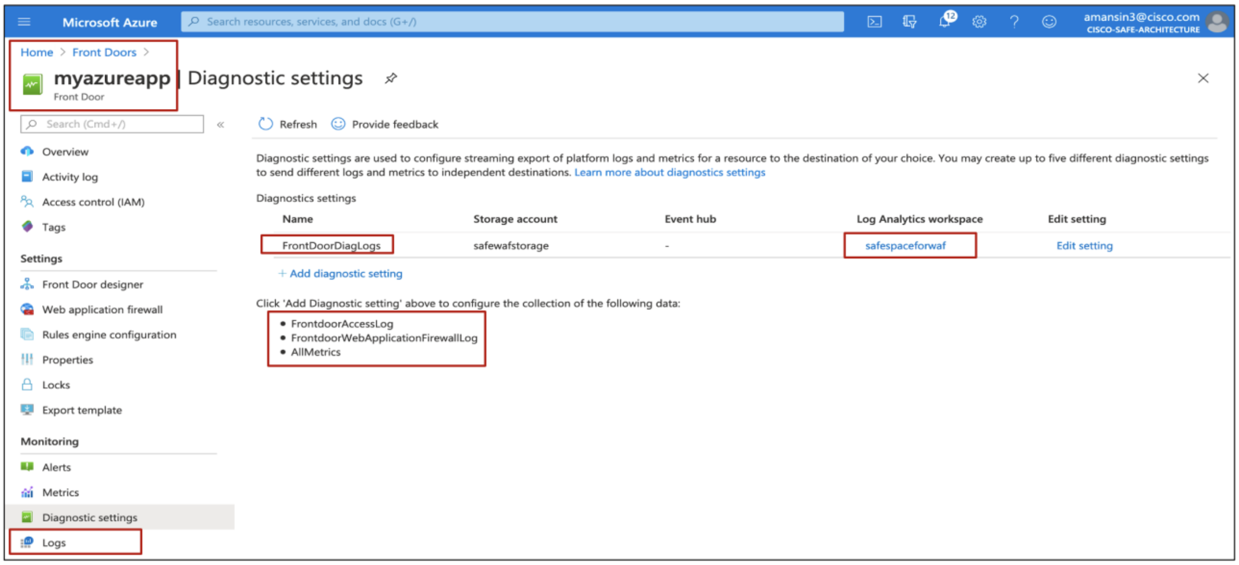
Delete

Resource group (change)	: securerg	Workspace Name	: LogSpaceforWAFandDDoS
Status	: Active	Workspace ID	: 879940a4-f36c-4f80-87a6-79b4737c80
Location	: East US	Pricing tier	: Pay-as-you-go
Subscription (change)	: Microsoft Azure Enterprise	Access control mode	: Use resource or workspace permissions
Subscription ID	: 9d1e5c82-29bb-43db-b312-a61a9077fa01		
Tags (change)	: Click here to add tags		

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

Go to ‘Azure Front Doors’ service that we created earlier and select ‘Diagnostics Settings’ from the panel on the left-hand. Click on ‘+ Add Diagnostic setting’ to add a log subscription to the log analytics space we created above. Make sure you include ‘FrontdoorAccessLog’ and ‘FrontdoorWebApplicationFirewallLog’ to the diagnostic settings.



Home > Front Doors >

myazureapp | Diagnostic settings

Front Door

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostics settings

Diagnostics settings

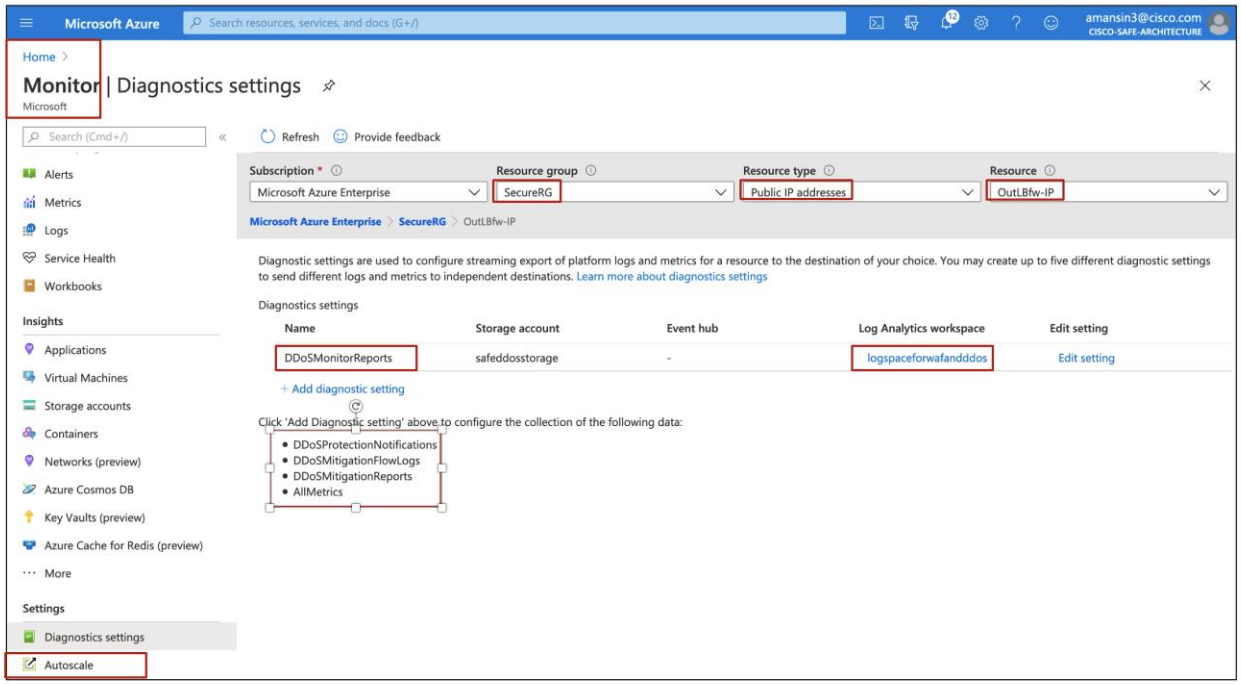
Name	Storage account	Event hub	Log Analytics workspace	Edit setting
FrontDoorDiagLogs	safewafstorage	-	safespaceforwaf	Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- FrontdoorAccessLog
- FrontdoorWebApplicationFirewallLog
- AllMetrics

Now, go to ‘Azure Monitor’ service and select the ‘Diagnostics Settings’ on the left-hand side of the panel. Select the Public IP addresses of the NGFWv from the available selection panel and then click on ‘+ Add Diagnostic setting’ to add a log subscription to the log analytics space we created above. Make sure you include ‘DDoSProtectionNotification’, ‘DDoSMitigationFlowlogs’, ‘DDoSMitigationReports’ in the diagnostic settings.



Monitor | Diagnostics settings

Microsoft

Subscription *: Microsoft Azure Enterprise

Resource group: SecureRG

Resource type: Public IP addresses

Resource: OutLBfw-IP

Microsoft Azure Enterprise > SecureRG > OutLBfw-IP

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostics settings

Diagnostics settings

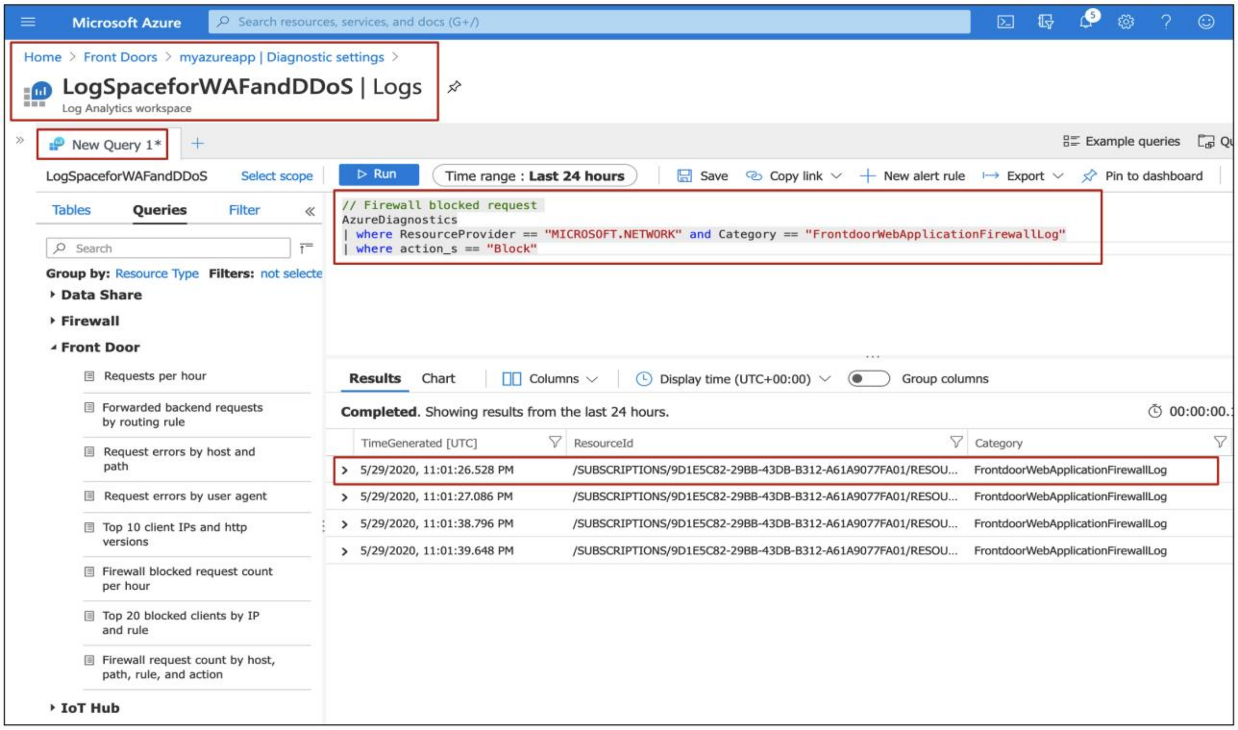
Name	Storage account	Event hub	Log Analytics workspace	Edit setting
DDoSMonitorReports	safeddosstorage	-	logspaceforwafandddos	Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- DDoSProtectionNotifications
- DDoSMitigationFlowLogs
- DDoSMitigationReports
- AllMetrics

At this point we have added both the required logs for WAF and DDoS service to our log analytics space. Now, we can run queries to look for any events related to WAF block or DDoS for a deep dive and plot custom charts and dashboards based on these queries.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Doors > myazureapp | Diagnostic settings >
New Query 1*
Example queries
Select scope
Run
Time range : Last 24 hours
Save
Copy link
New alert rule
Export
Pin to dashboard
Tables
Queries
Filter
Search
Group by: Resource Type Filters: not selecte
Data Share
Firewall
Front Door
Requests per hour
Forwarded backend requests by routing rule
Request errors by host and path
Request errors by user agent
Top 10 client IPs and http versions
Firewall blocked request count per hour
Top 20 blocked clients by IP and rule
Firewall request count by host, path, rule, and action
IoT Hub
Results
Chart
Columns
Display time (UTC+00:00)
Group columns

LogSpaceforWAFandDDoS | Logs

Log Analytics workspace

LogSpaceforWAFandDDoS

```
// Firewall blocked request
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category == "FrontdoorWebApplicationFirewallLog"
| where action_s == "Block"
```

Completed. Showing results from the last 24 hours.

00:00:00.

TimeGenerated [UTC]	ResourceId	Category
5/29/2020, 11:01:26.528 PM	/SUBSCRIPTIONS/9D1E5C82-29BB-43DB-B312-A61A9077FA01/RESOU...	FrontdoorWebApplicationFirewallLog
5/29/2020, 11:01:27.086 PM	/SUBSCRIPTIONS/9D1E5C82-29BB-43DB-B312-A61A9077FA01/RESOU...	FrontdoorWebApplicationFirewallLog
5/29/2020, 11:01:38.796 PM	/SUBSCRIPTIONS/9D1E5C82-29BB-43DB-B312-A61A9077FA01/RESOU...	FrontdoorWebApplicationFirewallLog
5/29/2020, 11:01:39.648 PM	/SUBSCRIPTIONS/9D1E5C82-29BB-43DB-B312-A61A9077FA01/RESOU...	FrontdoorWebApplicationFirewallLog

Radware Cloud WAF and DDoS

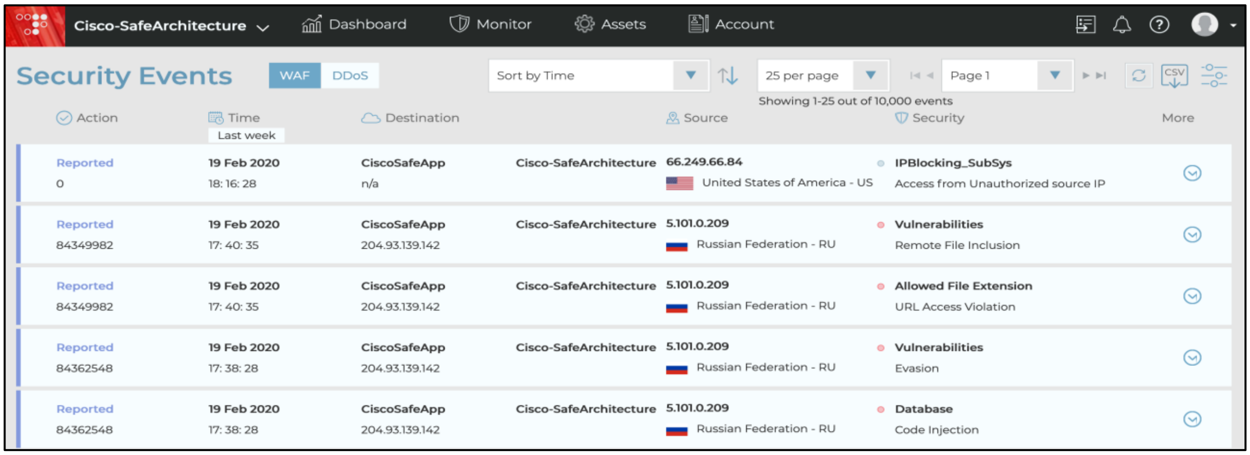
Test Case: Monitor Web and DDoS activity on Radware cloud

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.

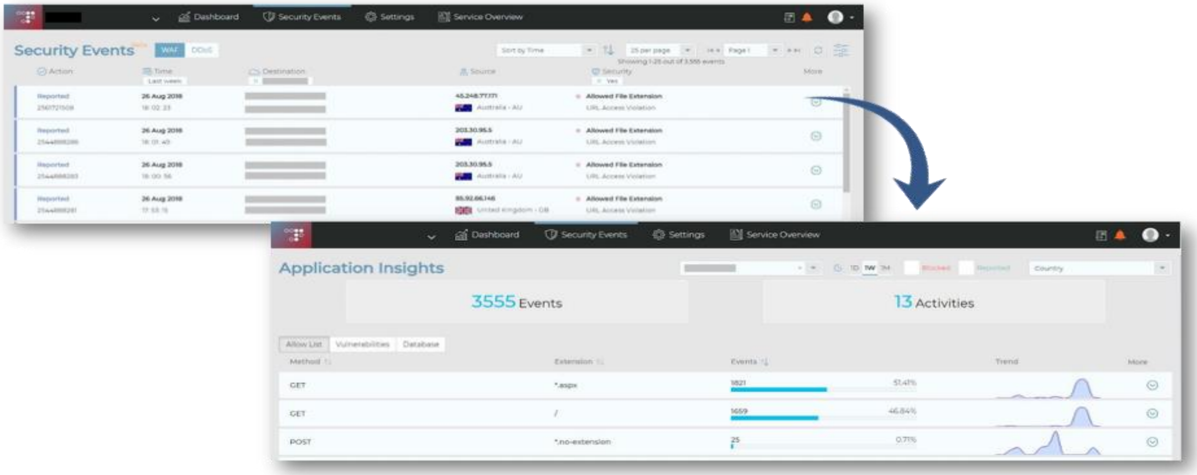
Step 1. Monitor Web activity and DDoS activity on Radware cloud – On the Radware Cloud portal, go to 'Monitor > Security Events' to see all the WAF and DDOS events generated from any malicious activity targeting your application.



Showing 1-25 out of 10,000 events

Action	Time Last week	Destination		Source	Security	More
Reported 0	19 Feb 2020 18: 16: 28	CiscoSafeApp n/a	Cisco-SafeArchitecture	66.249.66.84 United States of America - US	IPBlocking_SubSys Access from Unauthorized source IP	
Reported 84349982	19 Feb 2020 17: 40: 35	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Federation - RU	Vulnerabilities Remote File Inclusion	
Reported 84349982	19 Feb 2020 17: 40: 35	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Federation - RU	Allowed File Extension URL Access Violation	
Reported 84362548	19 Feb 2020 17: 38: 28	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Federation - RU	Vulnerabilities Evasion	
Reported 84362548	19 Feb 2020 17: 38: 28	CiscoSafeApp 204.93.139.142	Cisco-SafeArchitecture	5.101.0.209 Russian Federation - RU	Database Code Injection	

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.



Action	Time Last week	Destination	Source	Security Yes	More
Reported 2561721509	26 Aug 2018 18:02:23	[redacted]	45.248.77.171 Australia - AU	Allowed File Extension URL Access Violation	
Reported 2544888286	26 Aug 2018 18:01:49	[redacted]	203.30.95.5 Australia - AU	Allowed File Extension URL Access Violation	
Reported 2544888283	26 Aug 2018 18:00:56	[redacted]	203.30.95.5 Australia - AU	Allowed File Extension URL Access Violation	
Reported 2544888281	26 Aug 2018 17:53:15	[redacted]	85.92.66.146 United Kingdom - GB	Allowed File Extension URL Access Violation	

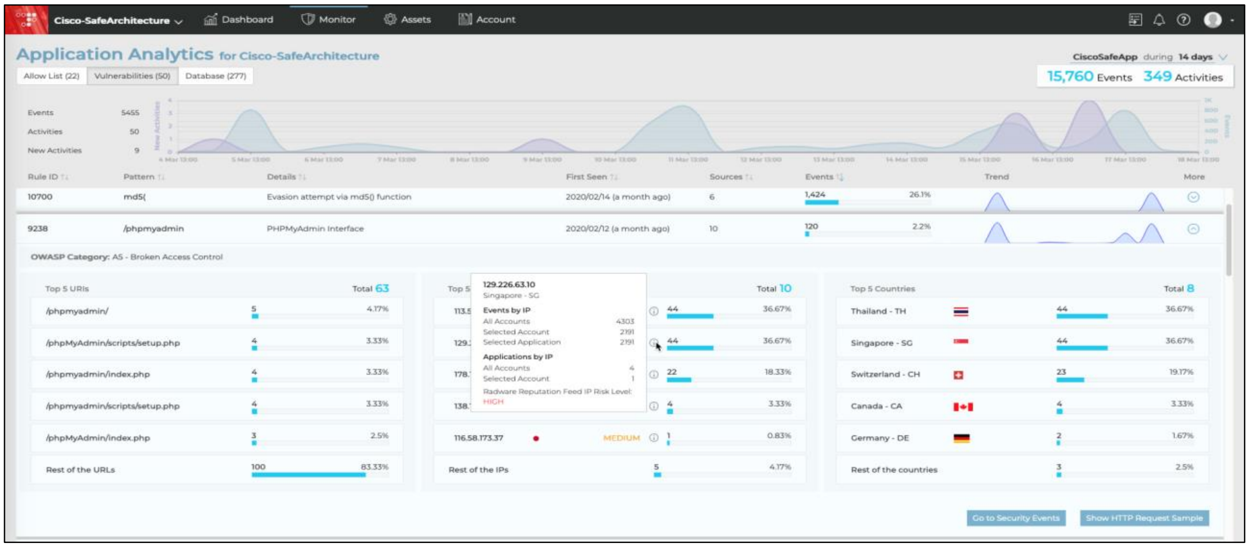
3555 Events

13 Activities

Allow List | Vulnerabilities | Database

Method	Extension	Events		Trend	More
GET	*.aspx	1821	51.41%		
GET	/	1659	46.84%		
POST	*.no-extension	25	0.71%		

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).



Application Analytics for Cisco-SafeArchitecture

Allow List (22) | Vulnerabilities (50) | Database (277)

CiscoSafeApp during 14 days

15,760 Events 349 Activities

Events	5455
Activities	50
New Activities	9

Rule ID	Pattern	Details	First Seen	Sources	Events	
10700	md5(	Evasion attempt via md5() function	2020/02/14 (a month ago)	6	1,424	26.1%
9238	/phpmyadmin	PHPMyAdmin Interface	2020/02/12 (a month ago)	10	120	2.2%

OWASP Category: A5 - Broken Access Control

Top 5 URIs		Total 63
/phpmyadmin/	5	4.17%
/phpMyAdmin/scripts/setup.php	4	3.33%
/phpmyadmin/index.php	4	3.33%
/phpmyadmin/scripts/setup.php	4	3.33%
/phpMyAdmin/index.php	3	2.5%
Rest of the URLs	100	83.33%

Top 5			Total 10
113.5		44	36.67%
129.2		44	36.67%
178.1		22	18.33%
138.1		4	3.33%
116.58.173.37	MEDIUM	1	0.83%
Rest of the IPs		5	4.17%

129.226.63.10
Singapore - SG

Events by IP

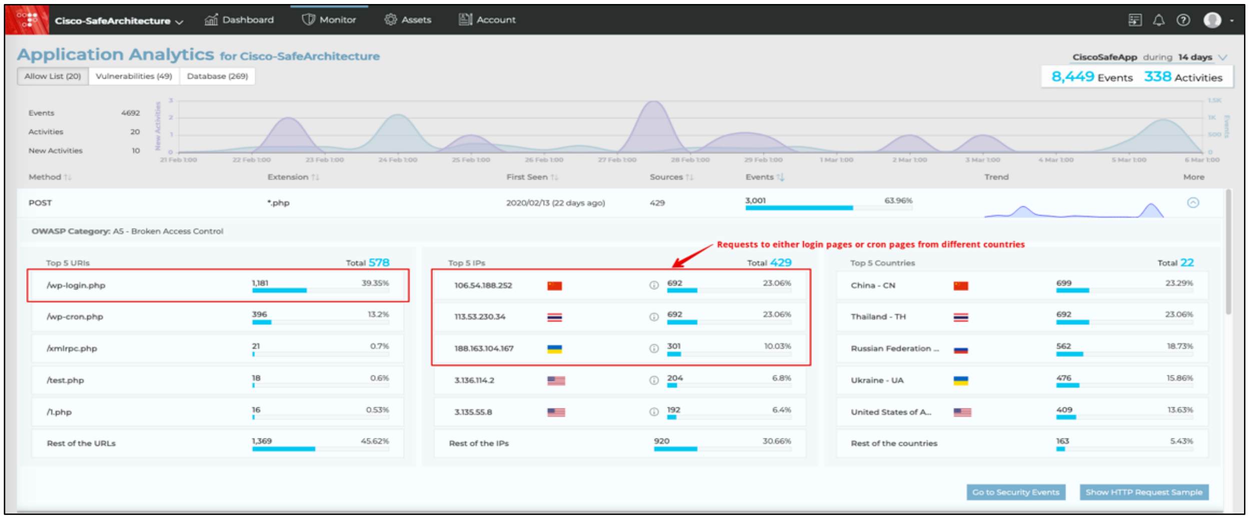
All Accounts	4303
Selected Account	2191
Selected Application	2191

Applications by IP

All Accounts	4
Selected Account	1

Radware Reputation Feed IP Risk Level: HIGH

Top 5 Countries		Total 8
Thailand - TH	44	36.67%
Singapore - SG	44	36.67%
Switzerland - CH	23	19.17%
Canada - CA	4	3.33%
Germany - DE	2	1.67%
Rest of the countries	3	2.5%



Application Analytics for Cisco-SafeArchitecture

Allow List (20) | Vulnerabilities (49) | Database (269)

CiscoSafeApp during 14 days

8,449 Events 338 Activities

Events	4692
Activities	20
New Activities	10

Method	Extension	First Seen	Sources	Events	
POST	*.php	2020/02/13 (22 days ago)	429	3,001	63.96%

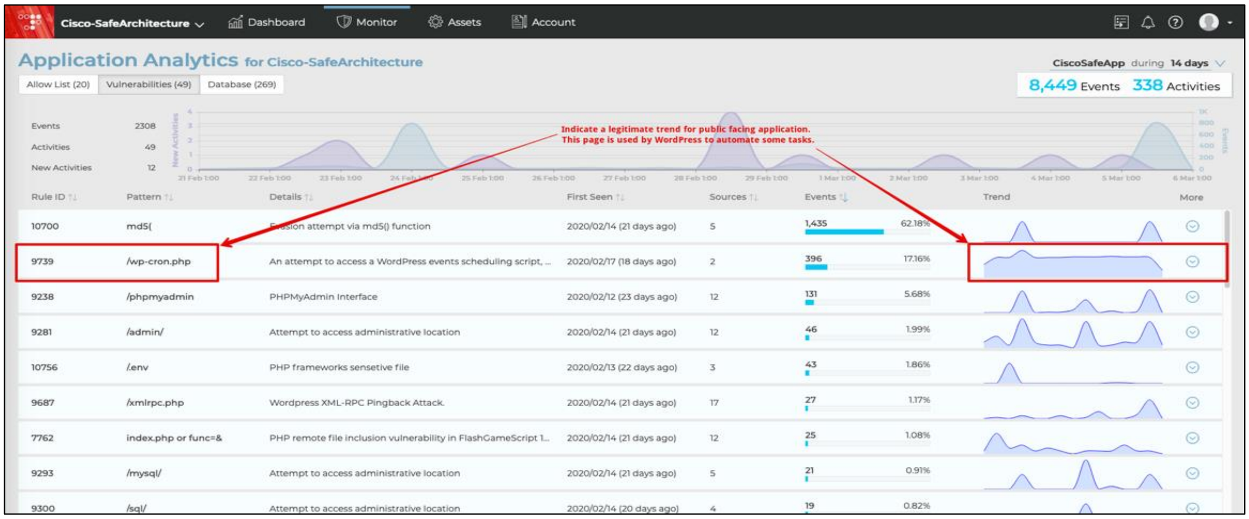
OWASP Category: A5 - Broken Access Control

Requests to either login pages or cron pages from different countries

Top 5 URIs		Total 578
/wp-login.php	1,181	39.35%
/wp-cron.php	396	13.2%
/xmlrpc.php	21	0.7%
/test.php	18	0.6%
/1.php	16	0.53%
Rest of the URLs	1,369	45.62%

Top 5 IPs		Total 429
106.54.188.252	692	23.06%
113.53.230.34	692	23.06%
188.163.104.167	301	10.03%
3.136.114.2	204	6.8%
3.135.55.8	192	6.4%
Rest of the IPs	920	30.66%

Top 5 Countries		Total 22
China - CN	699	23.29%
Thailand - TH	692	23.06%
Russian Federation ...	562	18.73%
Ukraine - UA	476	15.86%
United States of A...	409	13.63%
Rest of the countries	163	5.43%



Application Analytics for Cisco-SafeArchitecture

Allow List (20) | Vulnerabilities (49) | Database (269)

CiscoSafeApp during 14 days

8,449 Events 338 Activities

Events	2308
Activities	49
New Activities	12

Indicate a legitimate trend for public facing application.
This page is used by WordPress to automate some tasks.

Rule ID	Pattern	Details	First Seen	Sources	Events	
10700	md5(	Evasion attempt via md5() function	2020/02/14 (21 days ago)	5	1,435	62.18%
9739	/wp-cron.php	An attempt to access a WordPress events scheduling script, ...	2020/02/17 (18 days ago)	2	396	17.16%
9238	/phpmyadmin	PHPMyAdmin Interface	2020/02/12 (23 days ago)	12	131	5.68%
9281	/admin/	Attempt to access administrative location	2020/02/14 (21 days ago)	12	46	1.99%
10756	/.env	PHP frameworks sensetive file	2020/02/13 (22 days ago)	3	43	1.86%
9687	/xmlrpc.php	Wordpress XML-RPC Pingback Attack.	2020/02/14 (21 days ago)	17	27	1.17%
7762	index.php or func=&	PHP remote file inclusion vulnerability in FlashGameScript 1...	2020/02/14 (21 days ago)	12	25	1.08%
9293	/mysql/	Attempt to access administrative location	2020/02/14 (21 days ago)	5	21	0.91%
9300	/sql/	Attempt to access administrative location	2020/02/14 (20 days ago)	4	19	0.82%

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)

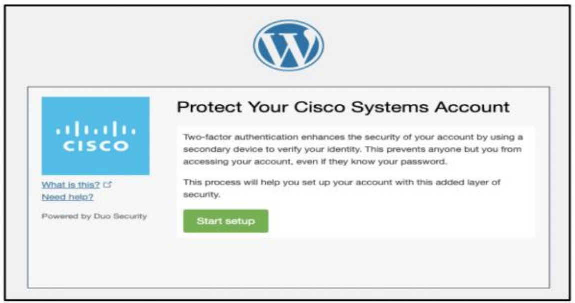
This test case involves logging into the application for the first time and activating the duo plugin. Previously, during the implementation phase, we had already downloaded the plugin to application workloads using custom scripts (Azure VM Extensions). Follow the Duo documentation (skip step 2 under '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

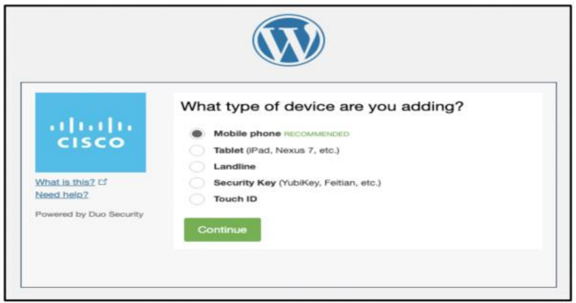
Step 1. Set up Duo 2FA for a new user - After the initial plugin activation, the Duo MFA kicks in and since this is the first authentication attempt, the user is prompted to enroll for MFA.



Protect Your Cisco Systems Account

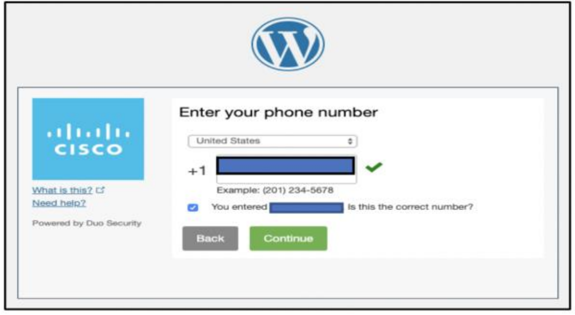
Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

This process will help you set up your account with this added layer of security.



What type of device are you adding?

● Mobile phone RECOMMENDED
○ Tablet (iPad, Nexus 7, etc.)
○ Landline
○ Security Key (YubiKey, Feitian, etc.)
○ Touch ID



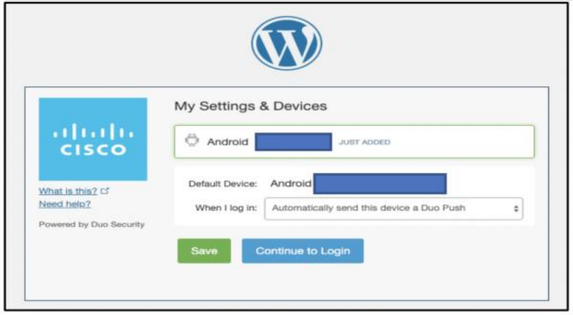
Enter your phone number

United States

+1 [redacted] ✓

Example: (201) 234-5678

☑ You entered [redacted] Is this the correct number?



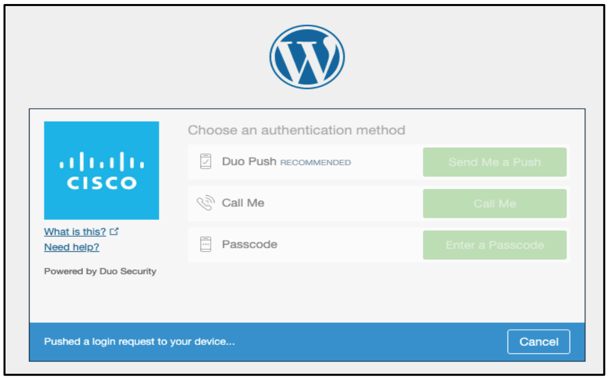
My Settings & Devices

Android [redacted] JUST ADDED

Default Device: Android [redacted]

When I log in: Automatically send this 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.



Pushed a login request to your device...

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

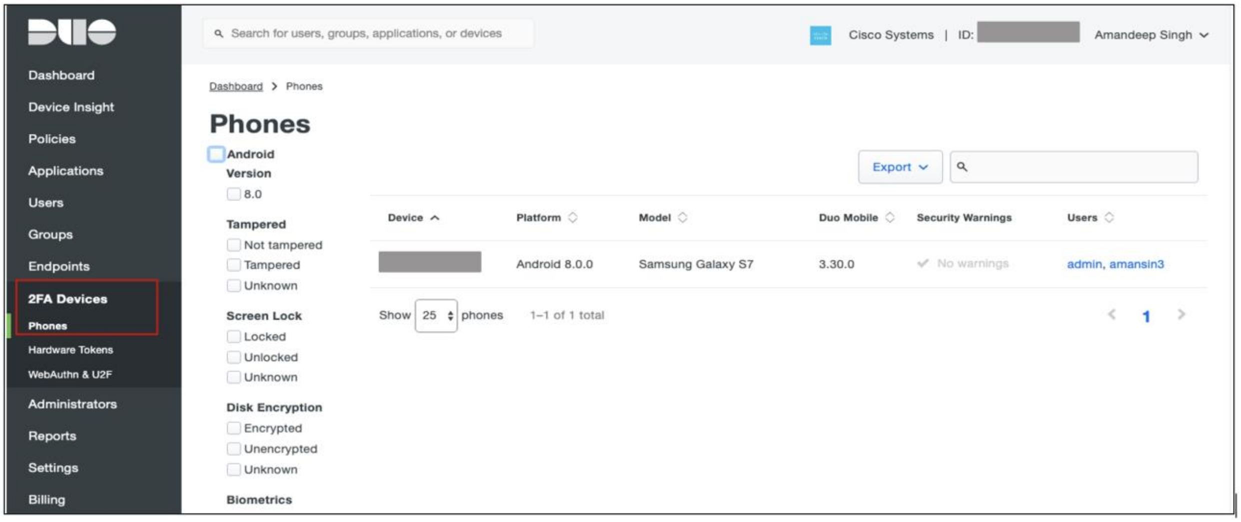
This test case involves monitoring the 2FA enrollment and login activity in the Duo admin portal.

Validation procedure:

Step 1. Verify the 2FA enrolled devices

Step 2. Track the user logins in authentication logs

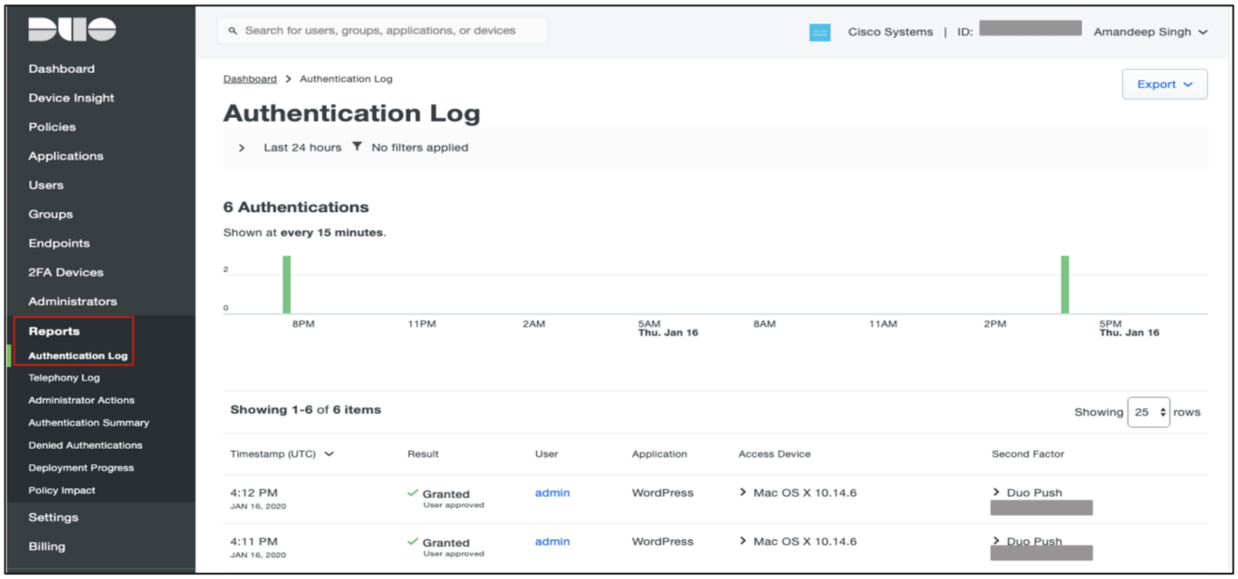
Step 1. Verify the 2FA enrolled devices – Logon to the Duo admin portal and select ‘2FA Devices’, the portal shows the list of enrolled devices along with other details like platform, hardware model and usernames.



ID: [redacted]

Device	Platform	Model	Duo Mobile	Security Warnings	Users
[redacted]	Android 8.0.0	Samsung Galaxy S7	3.30.0	✓ No warnings	admin, amansin3

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.



Authentication Log

> Last 24 hours No filters applied

6 Authentications

Shown at **every 15 minutes**.

Showing 1-6 of 6 items

Showing 25 rows

Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
4:12 PM JAN 16, 2020	✓ Granted User approved	admin	WordPress	> Mac OS X 10.14.6	> Duo Push [redacted]
4:11 PM JAN 16, 2020	✓ Granted User approved	admin	WordPress	> Mac OS X 10.14.6	> Duo Push [redacted]

Cisco SecureX Threat Response

Test Case: Track malicious Activity on threat response

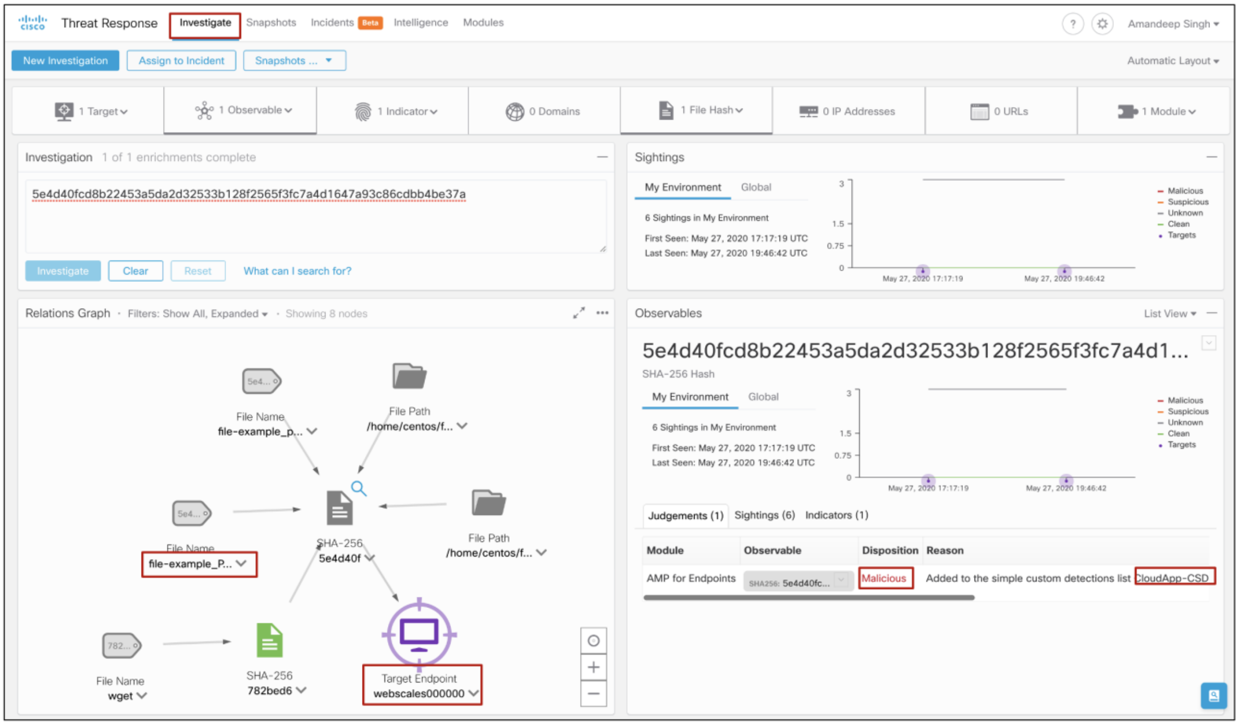
In this test case, we track the life cycle of the malicious PDF that we quarantined using AMP4E in previous steps. We will use the same SHA value and see what threat response offers in terms of visibility in our environment.

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.

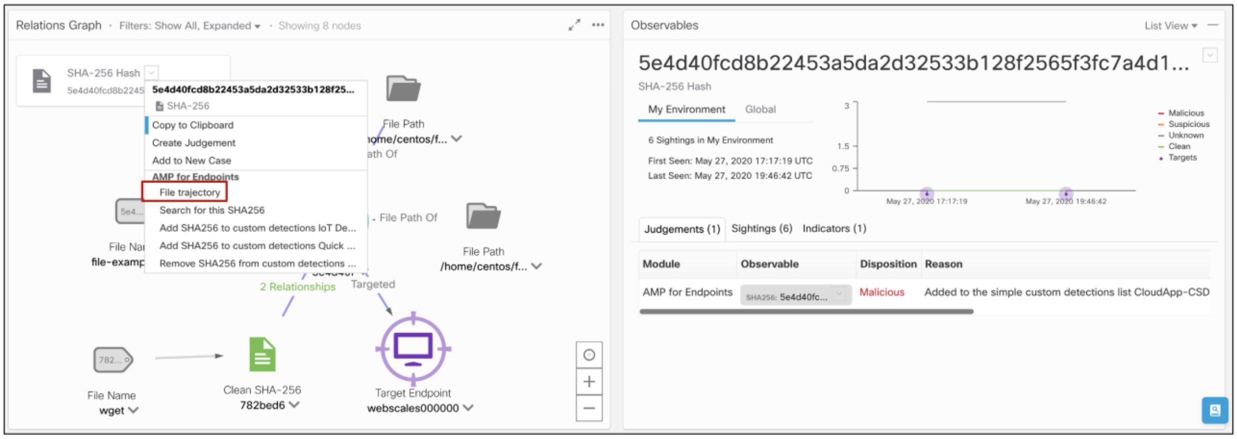


5e4d40fcd8b22453a5da2d32533b128f2565f3fc7a4d1647a93c86cdbb4be37a

5e4d40fcd8b22453a5da2d32533b128f2565f3fc7a4d1...

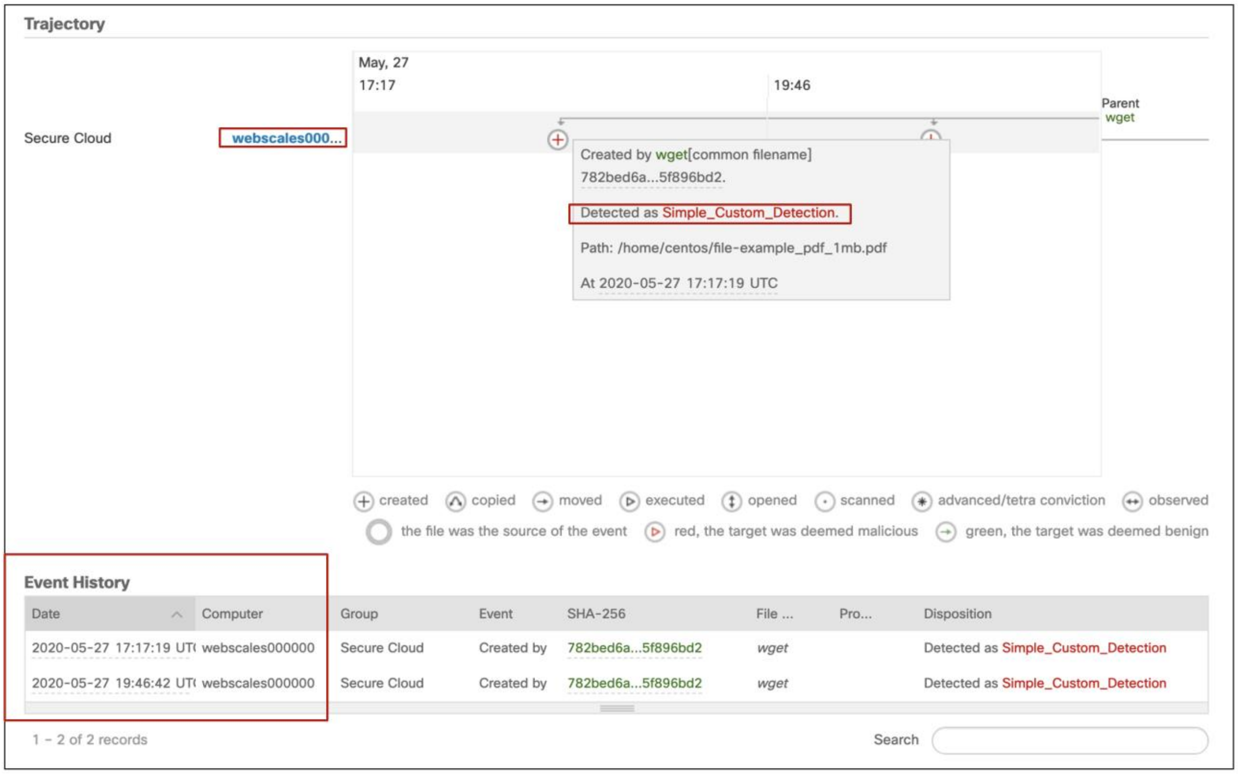
Module	Observable	Disposition	Reason
AMP for Endpoints	SHA256: 5e4d40fc...	Malicious	Added to the simple custom detections list CloudApp-CSD

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'.



Module	Observable	Disposition	Reason
AMP for Endpoints	SHA256: 5e4d40fc...	Malicious	Added to the simple custom detections list CloudApp-CSD

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
Secure Cloud
webscales000...
Parent
wget
created
copied
moved
executed
opened
scanned
advanced/tetra conviction
observed
the file was the source of the event
red, the target was deemed malicious
green, the target was deemed benign

Created by wget[common filename] 782bed6a...5f896bd2.

Detected as Simple_Custom_Detection.

Path: /home/centos/file-example_pdf_1mb.pdf

At 2020-05-27 17:17:19 UTC

Event History

Date	Computer	Group	Event	SHA-256	File ...	Pro...	Disposition
2020-05-27 17:17:19 UT(	webscales000000	Secure Cloud	Created by	782bed6a...5f896bd2	*wget*		Detected as Simple_Custom_Detection
2020-05-27 19:46:42 UT(	webscales000000	Secure Cloud	Created by	782bed6a...5f896bd2	*wget*		Detected as Simple_Custom_Detection

1 – 2 of 2 records

Search

Appendix

Appendix A- Acronyms Defined

AFD – Azure Front Doors

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

FDM – Firepower Device Manager

FMC – Firepower Management Center

FTD – Firepower Threat Defense

FQDN – Fully Qualified Domain Name

IOC – Indicators of Compromise

MFA – Multi-Factor Authentication

NGFW – Next Generation Firewall

NSG – Network Security Group

PaaS - Platform as a Service

PIN - Places in Network

SaaS - Software as a Service

SWC - Stealthwatch Cloud

VA - Virtual Appliance

VNET - Virtual Network

VSS - Virtual Machine Scale Set

2FA - Two Factor Authentication

Appendix B- 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 (Azure VM Instance)	2.6.2
Cisco NGFWv	Appliance (Azure VM Instance)	6.5.0-115
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 (Azure VSS)	Linux	CentOS 7.7
Azure Database for MySQL	MySQL database	mysql-5-7

Appendix C- References

This section lists all the references.

- **Cisco SAFE:** https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html
- **Azure N-Tier Architecture**: https://docs.microsoft.com/en-us/azure/architecture/guide/architecture-styles/n-tier
- **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 Firepower Threat Defense:**
  https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/azure/ftdv-azure-qsg.html
- **Cisco Duo Beyond:**
  https://duo.com/docs/wordpress
- **Cisco Umbrella:**
  https://docs.umbrella.com/deployment-umbrella/docs/deploy-vas-on-microsoft-azure
- **Cisco Defense Orchestrator:**
  https://www.cisco.com/c/en/us/products/security/defense-orchestrator/index.html
- **Radware for AWS (WAF and DDoS):**
  https://www.radware.com/products/cloud-waf-service/
- **NGINX:**
  https://www.nginx.com/resources/wiki/start/topics/recipes/wordpress/
- **WordPress:**
  https://wordpress.org/download
- **Azure VNET:**
  https://docs.microsoft.com/en-us/azure/virtual-network/
- **Azure Route Tables:**
  https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview
- **Azure NSG:**
  https://docs.microsoft.com/en-us/azure/virtual-network/security-overview
- **Azure Database for MySQL:**
  https://docs.microsoft.com/en-us/azure/mysql/
- **Azure VSS:**
  https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview
- **Azure Virtual Machines:**
  https://azure.microsoft.com/en-us/services/virtual-machines/
- **Azure Load balancer (Internal and External):**
  https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview
- **Azure Storage Containers:**
  https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction
- **Azure Templates:**
  https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/overview
- **Azure Private Links:**
  https://docs.microsoft.com/en-us/azure/private-link/private-link-overview
- **Azure Front Doors:**
  https://docs.microsoft.com/en-us/azure/frontdoor/

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**.

Printed in USA 06/21