Cisco SD-WAN: Enabling Firewall and IPS for Compliance

Prescriptive Deployment Guide

September, 2020

Table of contents

Introduction

About the Guide

This document provides information on the design and deployment of the Cisco SD-WAN security infrastructure specific to the compliance use case within remote sites running IOS-XE SD-WAN WAN edge platforms. The security features leveraged within this guide include Enterprise Firewall with Application Awareness and Intrusion Prevention System (IPS).

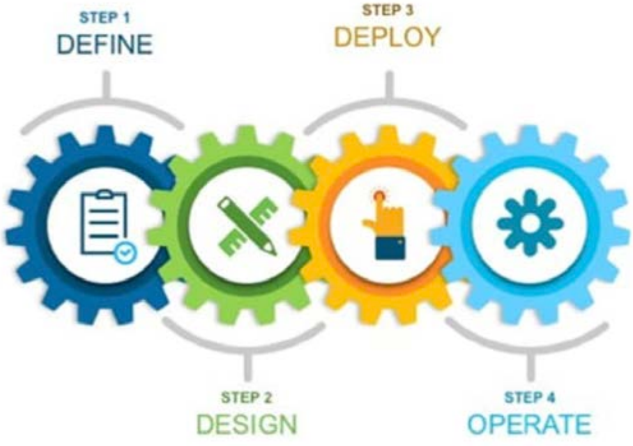
The guide explains the platforms deployed at length, highlights the best practices, and assists with the successful configuration and deployment of security features. However, the document is not exhaustive in terms of covering all possible deployment options.

This document assumes that the controllers are already deployed and integrated into vManage, the WAN edge devices are deployed and the SD-WAN overlay network is successfully established. Refer to the Cisco SD-WAN Design Guide for background information and the Cisco SDWAN Deployment Guide for information on deploying device templates to establish a Cisco SD-WAN overlay network.

This document contains four major sections:

- The **Define** section defines the shortcomings of a secure traditional WAN architecture, to then explain the benefits of deploying SD-WAN security solution.
- The **Design** section includes the use case covered in the guide, along with the design components and considerations in order to deploy the security features.
- The **Deploy** section discusses the automated deployment of the Cisco SD-WAN security features specific to the compliance use case using the vManage security policy dashboard. The section also includes the prerequisites to deploy this security solution.
- The **Operate** section explains some of the monitoring and troubleshooting methods used when Cisco SD-WAN security features, Enterprise firewall with Application Awareness, and IPS are configured.

Figure 1 Implementation Flow



Refer to **Appendix B** for the hardware models and software versions used in this deployment guide, **Appendix C** for the topology and **Appendix D** for the feature and device templates, along with the CLI-equivalent configuration for one of the WAN edge devices configured.

Audience

The audience for this document includes network design engineers, network operations personnel, and security operations personnel who wish to implement the Cisco SD-WAN security infrastructure for PCI compliance within SD-WAN enabled remote sites.

Define

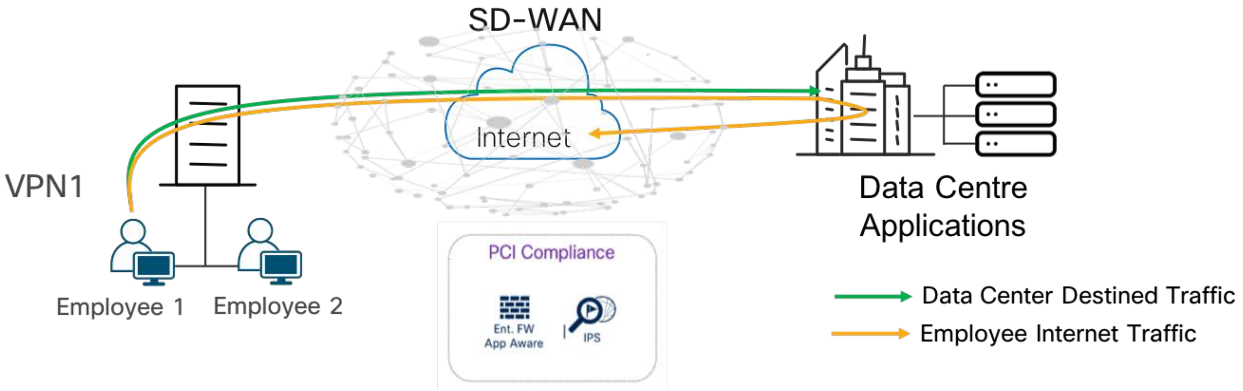
About the Solution

Companies handling credit card information are required to maintain data in a secure manner that reduces the likelihood of sensitive financial data from being stolen. If merchants fail to securely handle credit card information, that data could be hacked and used to make fraudulent purchases. Additionally, sensitive information about the cardholder could be used in identity fraud.

As the attack surface at the branch continues to increase, the need to protect sensitive information with the right security capabilities within the branch site before that data is tunneled over to the data center is critical. Companies that store, process or transmit cardholder data are required to inspect all the packets that leave the branch, by a stateful firewall and an IPS solution, and this is required before the data is tunneled over to the data center.

The solution is to deploy and maintain Cisco SD-WAN within your WAN infrastructure, which allows you to manage your SD-WAN WAN network centrally via Cisco vManage GUI and leverage the security capabilities embedded natively in the SD-WAN single-pane of management to secure traffic within the remote site before it is tunneled over to the data center.

Figure 2 PCI Compliance Traffic flow



The security capabilities available within the security policy dashboard on vManage include Enterprise Firewall with Application Awareness (Application Firewall), Intrusion Prevention System (IPS), URL-Filtering, Advanced Malware Protection (AMP), and DNS/Web-layer Security.

vManage includes predefined workflows to facilitate several use cases based on intent, such as:

1) Compliance (Application Firewall | Intrusion Prevention)

2) Guest Access (Application Firewall | URL Filtering)

3) Direct Cloud Access (Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security)

4) Direct Internet Access (Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security)

In addition, you can build your own custom policy by combining a custom variety of security features.

Within this solution, the security features available within the intent-based use case for **Compliance** are leveraged.

Benefits of Deploying SD-WAN Security for PCI Compliance

Simple and Automated Security Solution: The intent-based workflow is designed for ease of configuration and deployment of the SD-WAN security solution. The workflow allows you to fill out the template to include all of the security capabilities and deploy it on multiple devices at the same time.

Comprehensive SD-WAN Security: With security capabilities such as Enterprise Firewall with App Aware Firewall (Application Firewall) and IPS enabled on your WAN edge device, you can do the following.

5) Restrict access to certain Internet destinations for remote employees and guests, with improved application experience.

6) Protect the internal network from malware and/or malicious content in real-time.

7) Prevent any additional cost as deploying the Cisco SD-WAN security solution eliminates the need to deploy any additional equipment within your SD-WAN network to enable security features.

Centralized Management: Deploy, troubleshoot and monitor the SD-WAN overlay solution with security capabilities across WAN edge devices centrally via the Cisco vManage GUI.

Design - Cisco SD-WAN Security - Compliance Use Case

Use cases are part of the vManage security policy. Out of the four intent-based use cases available, compliance is the predominant one for enterprise customers.

Use Case #1 - Compliance

Within the compliance use case, the primary requirement is to protect sensitive data, such as card holder or patient information, against data breaches. This makes it necessary to inspect traffic before it is tunneled across to the data center. In the Cisco SD-WAN solution, although data plane traffic is encrypted and sent over a VPN tunnel, for compliance, all packets need to be subjected to a stateful firewall and an IPS solution.

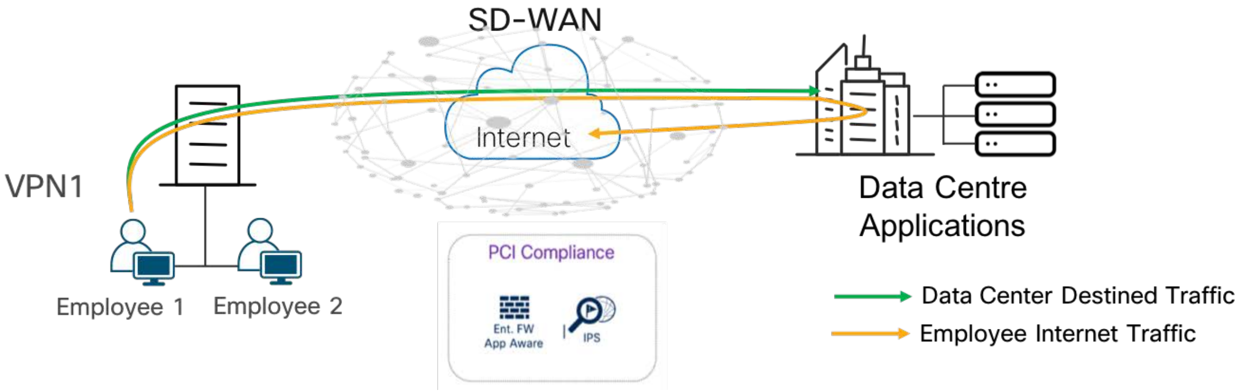
Four security pillars are required to maintain a PCI-compliant network:

Table 1 **Security Pillars**

Transport Security	IPsec VPN
Perimeter Control	Firewall
Segmentation	VPN/FW Zone
Attack Prevention	IPS

In the following figure, the traffic traversing from VPN 1 is inspected via Cisco SD-WAN security features, such as Enterprise Firewall with Application Awareness and Intrusion Prevention System before being tunneled and sent over to the datacenter (based on the destination from data center to Internet).

Figure 3 Traffic Flow – Compliance Use Case



For details regarding other use cases, refer to the SD-WAN Security Policy Design guide.

SD-WAN Security Design Components

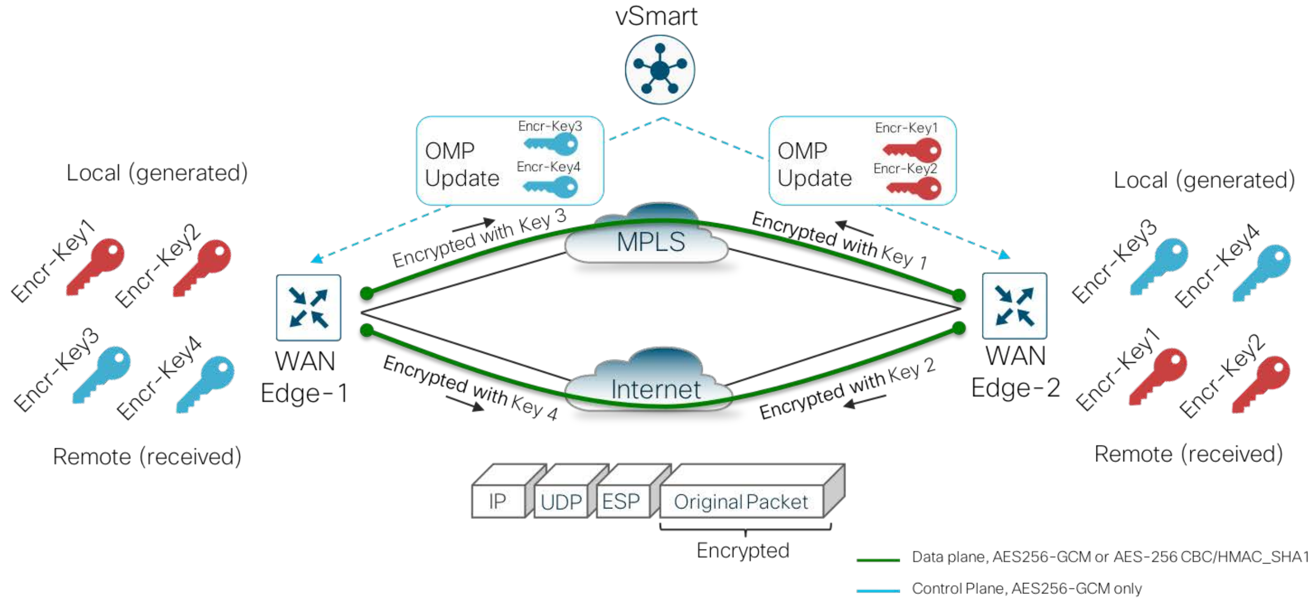
In the following section, the four security pillars required to maintain a PCI-compliant network are discussed in depth.

Transport Security

The first security pillar in PCI compliance is establishing a secure transport. IPsec connections are established across transports between Cisco WAN Edge devices via key exchange to authenticate and encrypt data packets.

In Cisco SD-WAN, once the control plane communication is established between the WAN edge device and vSmart controller, each of the WAN edge devices generates a pair of keys, an encryption key and a hashing key per transport route. In the figure, we have two transport routes, hence two encryption keys are generated from WAN Edge-1 (encryption key 1 and encryption key 2). The encryption and hashing keys are sent to the vSmart controller as an OMP update from the WAN Edge device. The controller reflects the keys towards the destined WAN Edge devices.

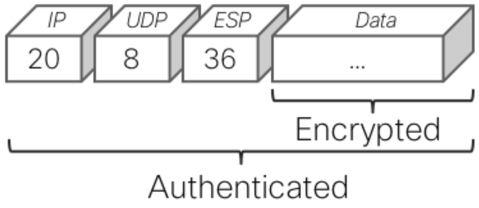
Figure 4 Data Plane Privacy and Encryption



Note that vSmart does not track or maintain keys. The keys are received by the vSmart controller as an OMP update and reflected to the receiving WAN edge device (WAN Edge-2) that stores the keys as encryption key 1 and encryption key 2 from the remote device. Similarly, WAN Edge-2 also generates its encryption keys and hashing keys, sends it to the vSmart controller as an OMP update, which then reflects the keys to WAN Edge-1, after which the IPsec connections are established over both the transports between the two WAN Edge devices, to allow for the data plane connection.

As shown in the figure below, the first packet exchanged between the two WAN edge routers is the actual encrypted data plane packet.

Figure 5 IPsec Packet



Note that to avoid attackers from predicting the keys, the WAN edge device changes the AES key used to establish the secure IPsec connection to another WAN edge device, based on the rekey timer set. By default, the rekey timer is set to 24 hours. This value is equivalent to the security association (SA) lifetime.

Secure Segmentation

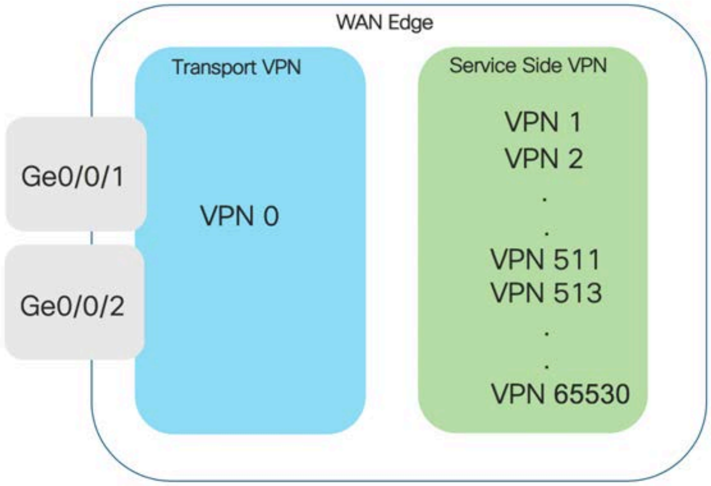
In SD-WAN security, the term segmentation is interchangeably used for **Virtual Private Network** (VPN/VRF) to segment users and **zones** to create separate security zones.

Virtual Private Network (VPN/VRF)

All Cisco SD-WAN designs are based on the use of VPN to segment the routing table, thus allowing multiple default routes to exist on the same WAN Edge device.

In Cisco SD-WAN, VPN 0 is the transport VPN and VPN 512 the management VPN. In WAN Edge devices, each VPN is a VRF and completely isolated from one another. All VPNs other than VPN 0 and VPN 512 are used to carry data traffic across the overlay network. These VPNs include, 1-511 and 513-65530, and are referred to as service-side VPNs. For these VPNs to operate, each one must have an operational interface (or sub-interface). The remainder of what is configured in these VPNs depends on the network needs.

Figure 6 VPN on WAN edge

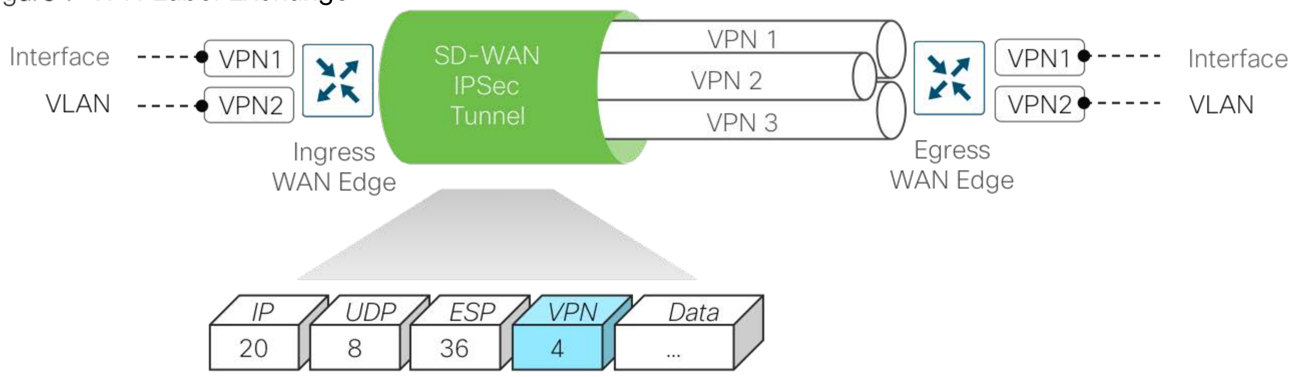


Technical Tip: Note that 65528, 65529 and 65530 are reserved VPNs. In this guide, VPN 65529 is used as a part of the IPS feature within the management virtual port group.

Within the data plane, segmentation is delivered by multiplexing traffic belonging to different VPNs inside a common IPsec tunnel between the WAN edge routers. Labels are used to identify the VPN the packet belongs to. These VPN labels are placed in the encrypted payload of the packet, and are not visible in clear text.

Ingress WAN Edge devices apply VPN labels before performing IPsec encryption. Egress WAN edge routers use VPN labels to perform lookup in the appropriate VPN routing table after the packet had been decrypted. The VPN labels are exchanged between the ingress and egress WAN Edge routers as OMP route attribute.

Figure 7 VPN Label Exchange



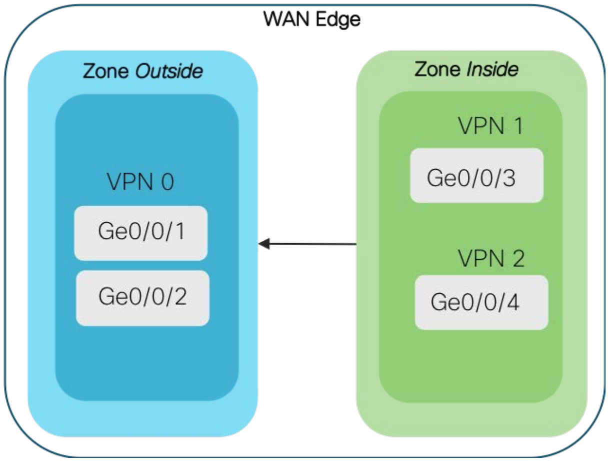
Zones

A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control the flow of all data traffic that passes between zones.

Zone configuration consists of the following components:

- ***Source zone*** is a grouping of VPNs where the data traffic flows originate.
- ***Destination zone*** is a grouping of VPNs where the data traffic flows terminate.
- ***Firewall policy*** is a localized security policy that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone.
- ***Zone pair*** is a container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

Figure 8 Zone details



The next section highlights the need for perimeter control by leveraging Zones/VPNs.

Enterprise Firewall with App Aware Policy

Enterprise Firewall with App Aware policy is a localized security policy that allows stateful inspection of data traffic flows that are matched based on the six different match criteria available within the vManage security policy dashboard. The match criteria include source data prefix, destination data prefix, source port, destination port, protocol and application/application family. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy match/action criteria set between the two zones.

Within a given firewall policy, accepted matching flows can be subjected to the following three actions:

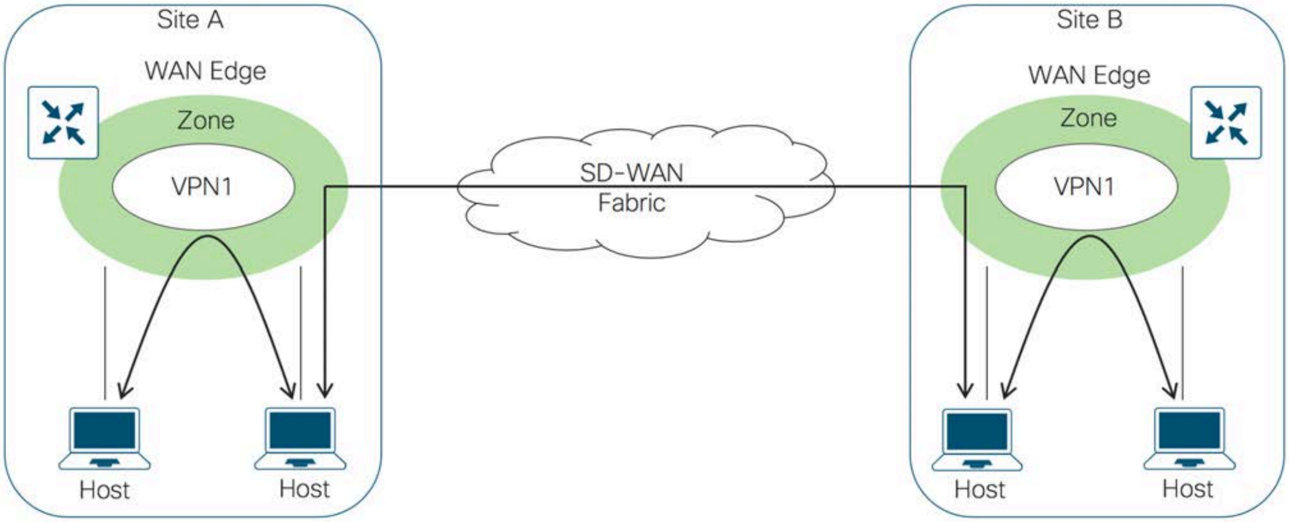
- **Inspect**: When the action is set to Inspect, the Enterprise Firewall with Application Aware policy tracks the state of the flows and creates sessions. Since it maintains the state of the flows, the return traffic is allowed and there is no need to configure a separate policy for return traffic.
- **Pass**: This action allows the router to forward the traffic from one zone to another zone. The pass action does not track the state of the flows, that is, the Firewall does not create sessions when the action is set to Pass. Pass action allows the traffic flow in only one direction.
- **Drop**: When the action is set to drop and packets match against the set match parameters. That packet will be dropped.

Based on the flow of traffic between zones, the Enterprise App Aware Firewall is further divided into ***Intra-zone-based security*** and ***Inter-zone-based security***.

Intra-zone based security

If the flow of traffic is between two zones, which are both tied to the same VPN, that is defined as an intra-zone Firewall. The following figure shows the flow of traffic between the zone-pair (VPN 1 to VPN 1).

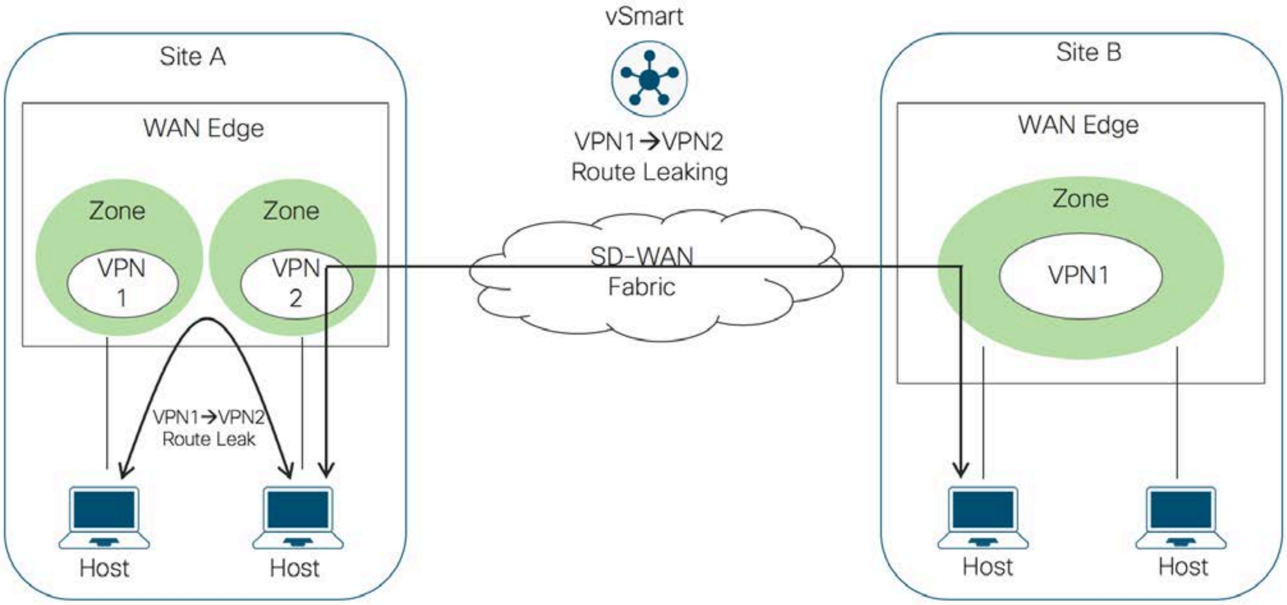
Figure 9 Intra-zone based security



Inter-zone Security

If the flow of traffic is between the two different zones tied to different VPNs, it is classified as an inter-zone firewall. The following figure shows the flow of traffic between the zone-pair (VPN 1 and VPN 2).

Figure 10 Inter-zone based security



High Speed Logging

For WAN edge devices running IOS-XE SD-WAN Code 16.12 or higher, High Speed Logging (HSL) can be enabled. When HSL is configured, firewall provides a log of packets that flow through routing devices (similar to the NetFlow Version 9 records) to an external collector, with minimum impact to packet processing. Records are sent when sessions are created and destroyed. Session records contain the full 5-tuple information that includes the source IP address, destination IP address, source port, destination port, and protocol.

In Cisco SD-WAN, firewall logs the following types of events:

- Audit: Session creation and removal notifications
- Alert: Half-open and maximum-open TCP session notifications
- Drop: Packet-drop notifications
- Pass: Packet-pass notifications
- Summary: Policy-drop and pass-summary notifications

By default, High-Speed Logging (HSL) is not enabled and firewall logs are sent to a logger buffer located in the Route Processor (RP) or the console. With HSL enabled, logs are sent to an off-box, high-speed log collector.

Technical Tip: HSL is supported only on NetFlow version 9 template and it is specific to logging IPv4 source/destination IP addresses to only one HSL destination.

Design considerations

The following are some of the considerations to look into before deploying Enterprise Firewall with App Aware feature on your WAN Edge device.

1) The following table indicates the Enterprise Firewall with Application Awareness support for various platform families with different memory configurations.

Table 2 **Supported platforms - Enterprise Firewall App Aware**

Platforms/ Features	Memory 4GB	Memory 8GB	Memory 16GB
Cisco - ISR4k	Y	Y	Y
Cisco - ISR1k*	Y	Y	N
Cisco - ASR1k	Y	Y	Y
Cisco - ENCS (ISRv)	Y	Y	Y

* Note: This does not include ISR1100-4G/6G.

2) The WAN edge devices must be running IOS-XE SD-WAN code version 16.10 or higher, and the controllers at 18.4.0 code version or higher. For details on the IOS-XE SD-WAN image upgrade along with the pre-requisites, refer to the Software Installation and Upgrade for Cisco IOS XE Routers Getting Started Guide.

3) For ease of deployment, design your IP addressing schema and preconfigure data prefixes, zones, and application families that are to be matched later in the policy.

4) While designing your zone pairs, note that a VPN can be a part of only one zone.

5) Since zone-based policies are directional and provide directional control of traffic, it's important to make sure that the direction of traffic flow between the zone-pair is as per design.

6) While designing the firewall policies, confirm that desired actions are taken on the items subject to the policy. A firewall policy consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order from lowest sequence number to highest sequence number. When a data packet matches the match conditions, the associated action or actions are taken and policy evaluation on that packet stops. Make sure to drag and drop your sequences as per your network requirements.

7) Note that, as the default sequence within the policy is set to drop if a packet matches none of the parameters in any of the policy sequences, then the packet will be dropped.

8) When the action is set to Inspect, the packets can be logged by enabling **Audit-trail** supported from 19.2 code. For more information, please refer to the Firewall High Speed Logging document.

Intrusion Prevention System

An Intrusion Prevention System (IPS) detects and blocks known network attacks. It uses previously known signatures, which are a set of rules to detect attacks originating from both external and internal sources.

Snort is the open source network Intrusion Prevention System leveraged within Cisco IOS-XE SDWAN devices to perform real-time traffic analysis and generate alerts when threats are detected on IP networks. Within the Cisco SD-WAN solution, IPS is an on-box, on-prem feature which provides PCI compliance.

Based on your network requirements, you can enable Snort either in IPS or IDS mode. Snort performs the following actions:

- Monitors network traffic and analyzes it against a defined rule set

- Performs attack classification
- Invokes actions against matched rules

In IDS mode, Snort inspects traffic and reports alerts, but does not take any action to prevent attacks. In IPS mode, in addition to intrusion detection, actions are taken to prevent attacks.

The following are the main components within the Snort IPS solution that needs to considered while designing your IPS/IDS Policy.

Snort Sensor

To enable Snort IPS, you need to download the Unified Thread Defense (UTD) Engine .ova file from software.cisco.com into the vManage virtual image repository.

The virtual container images are downloaded from vManage to the WAN Edge device to bring up the container with Snort enabled. The Snort sensor is deployed within the router as a virtual container service which monitors the traffic to detect anomalies based on the configured security policy (that includes signatures, statistics, protocol analysis, and so on) and sends log messages to the log server.

Signature Store

Signatures are a set of rules that IDS and IPS use to detect typical intrusive activity.

The signature store hosts the Cisco signature packages that are updated periodically. Validated signature packages are posted to Cisco.com. These signature packages are downloaded to sensors either periodically or on demand.

The two methods for signature update include automatic IPS signature update using vManage or manual IPS signature update using CLI commands available on the WAN Edge device. When a new signature package is updated, the Snort engine restarts and the traffic is interrupted or may bypass inspection for a short period depending on the data plane fail-open/fail-close configuration.

The **Fail-close** option drops all the IPS/IDS traffic when there is an engine failure. The **Fail-open** option allows all the IPS/IDS traffic when there is an engine failure. The default option is Fail-open.

Technical Tip: We do not support manually uploading IPS signature within the vManage virtual-image repository. If you encounter issues performing an automatic signature update from vManage running 19.2 code, update the signature manually from a WAN edge device.

Signature Set

While designing the Snort IPS policy, it is important to understand the signature levels available within your vManage IPS policy. There are three signature levels available within the vManage IPS Policy – **Security**, **Balanced** and **Connectivity**. Each of the signature levels contains a list of security vulnerabilities categorized based on the score assigned using the Common Vulnerability Scoring System (CVSS).

Note that CVSS is a free and open industry standard for assessing the severity of security vulnerabilities.

The three signature levels available within vManage IPS are as follows:

Balanced: This is the default signature set and contains rules that are from the current year and the previous two years.

This signature set is for vulnerabilities with a CVSS score of 9 or greater, and includes the categories shown in the following table.

Table 3 **Balanced Signature Set**

Category	Definition
Blacklist	Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity
Exploit-kit	Rules that are designed to detect exploit kit activity
Malware-CNC	Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data
SQL Injection	Rules that are designed to detect SQL injection attempts

Connectivity: This signature set contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.

Security: The signature set contains rules that are from the current year and the previous three years.

This signature set is for vulnerabilities with a CVSS score of 8 or greater, and includes the categories shown in the following table.

Table 4 **Security Signature Set**

Category	Definition
App-detect	Rules that look for and control the traffic of certain applications that generate network activity
Blacklist	Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity
Exploit-kit	Rules that are designed to detect exploit kit activity
Malware-CNC	Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data
SQL Injection	Rules that are designed to detect SQL Injection attempts

Before you choose the signature set, have a complete understanding of the network, devices and traffic flows that your signature set is bound to protect. There are performance-impacting signatures, hence work your way up from the balanced signature set after having whitelisted sensitive application flows. Whitelisting signatures or creating false positives is available as a part of the IPS Security policy vManage dashboard.

Here's some additional information that may help you select signature sets.

Connectivity: This is less restrictive with better performance as there are fewer rules attached to this signature level.

Balanced: This is designed to provide protection without a significant effect on system performance.

Security: This signature level offers more protection as it has more rules added, but the overall performance of your WAN edge device may be low.

Technical Tip: Presently, IPS cannot work on encrypted traffic (HTTPS).

Syslog Server

Within the Snort IPS policy the log level can be set and the consequent logs generated by the Snort sensor are sent to a syslog server configured either on a router or to a 3rd party SIEM server. The logging level ranges from 0-Emergency to 7-Debug. The higher the level, the more inclusion of granular, diagnostic information. It is ideal to stick to Warning/Error level so that there is a balance of load and information at production site.

The following logging levels are supported.

Figure 11 Alert Log Levels

Severity	Log Level	Type
0	Emergency	System is unusable
1	Alert	Immediate action needed
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant conditions
6	Info	Informational messages
7	Debug	Debug messages

Technical Tip: For WAN edge devices running 16.11 code/ vManage 19.2.0, the syslog server must be reachable via VPN 0. There is a known issue related to syslog server reachability from service-side VPN.

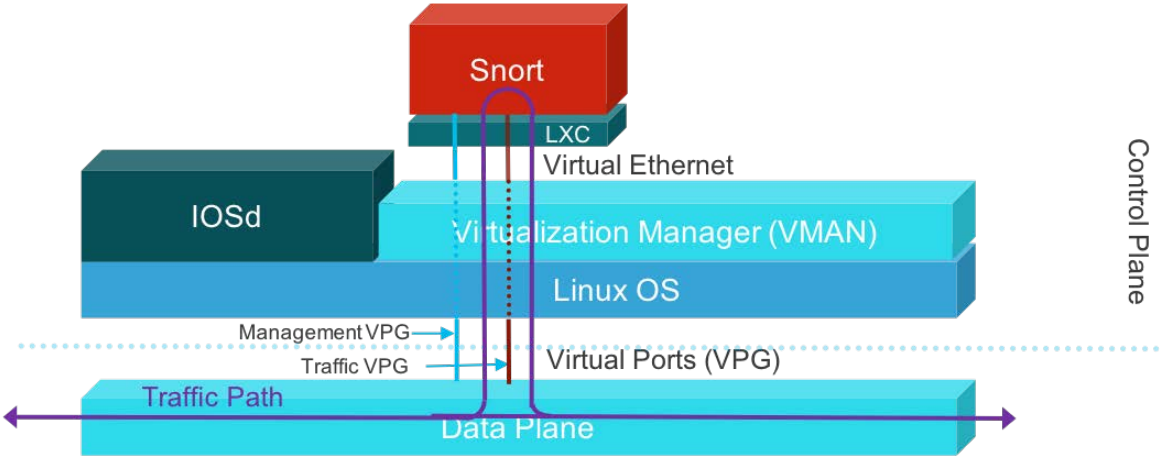
Architecture of Snort Engine

The IOS-XE SD-WAN devices have a multi-core CPU architecture, where some cores are allocated for control plane and other cores for service plane. Snort runs as a container application in the control plane infrastructure and it uses some of the CPU cores allocated for the control plane. The built-in Virtualization Manager within the control plane ensures that applications running on the containers and IOS daemon get a fair share of computer resources.

There are two virtual ports or interfaces connecting to the Snort container; the Management Virtual Port Group (Management VPG) and the Traffic Virtual Port Group. The first VirtualPortGroup interface is used for management traffic. This VPG is used to source logs to the log collector as well as to pull signature updates from Cisco.com. The second VirtualPortGroup is for data traffic between the forwarding plane and the Snort virtual container service. This VPG is used to send and receive packets that arrive on the data plane and are marked for inspection. These packets are sent back and forth to the container.

Snort traffic inspection is enabled for one or many selected target VPNs. After the policy is defined, traffic is redirected from the data plane to the container that contains the snort sensor. Snort then inspects the traffic for threats. Bad traffic is dropped and the remaining is forwarded back to the router for further processing.

Figure 12 Snort Architecture



Security App Hosting Profile

While attaching the configured IPS Policy within the device template, a sub-template titled container profile must be added. The container profile allows you to enable/disable NAT for your virtual services (IPS) and allocate the number of control plane cores for the virtual services.

NAT functionality can be enabled if the virtual services must go out to the internet for manual signature updates on WAN Edge device or if there is a need to send syslog's to an external syslog server that is not necessarily in the Data Center.

The Resource profile is set to default, which is one core. For higher throughput, you may set the resource profile to **High** allocating two cores. However, before making any changes to the resource profile, confirm the current memory status of your WAN Edge device, as the security app container cannot be installed if the device lacks memory space. Use the **show memory platform** command to note the free and physical memory status.

Design Considerations for IPS Solution

The following are some of the design considerations for deploying IPS functionality on your WAN Edge device.

1) Make sure to choose a platform that supports the IPS functionality, with the minimum required memory. Refer to the table for details.

Figure 13 Supported Platforms – IPS

Platforms/ Features	Memory 4GB	Memory 8GB (1 core)	Memory 8GB (2 core)	Memory 16GB (2 core)
Cisco – ISR4k	N/A	Y	Y	Y
Cisco – ISR1k*	N/A	Y	Y	N

Platforms/ Features	Memory 4GB	Memory 8GB (1 core)	Memory 8GB (2 core)	Memory 16GB (2 core)
Cisco - ENCS (ISRv)	N/A	Y	Y	Y

* Note: This does not include ISR1100-4G/6G. UTD features are supported only on ISR1k platforms that end with an X.

The number of cores is assigned based on the total number of cores available per device for the security app hosting profile.

Technical Tip: ASR1Ks will not get the IPS functionality. The available control plane cores are simply not sufficient to process all the packets that the ASR1K is capable of processing.

2) To enable Snort IPS, make sure your WAN Edge device is running IOS-XE SD-WAN version 16.10 or higher, along with a compatible UTD engine code and controllers are running code 18.4 or higher. Steps to understand the compatible UTD engine code are further explained in the Deploy section.

3) The Management Virtual Port Group is by default configured via vManage in VRF 65529. If the traffic from the Management port is routed via IP NAT route into the global routing table, enable NAT feature on the WAN Edge transport interface. This is required only if the virtual services must go out to the internet for manual signature updates on WAN Edge device or if there is a need to send syslog's to an external syslog server reachable from VPN 0.

4) The IP subnet of the second VirtualPortGroup (Traffic VPG) interface must not be routable on the customer network because the traffic on this interface is internal to the router. Exposing the internal subnet to the outside world is a security risk. We recommend the use of the 192.0.2.0/30 IP address range for the second VirtualPortGroup subnet.

5) As explained earlier, choose the signature set based on the network, devices, and traffic flow that your signature set is bound to protect, as several signatures impact performance.

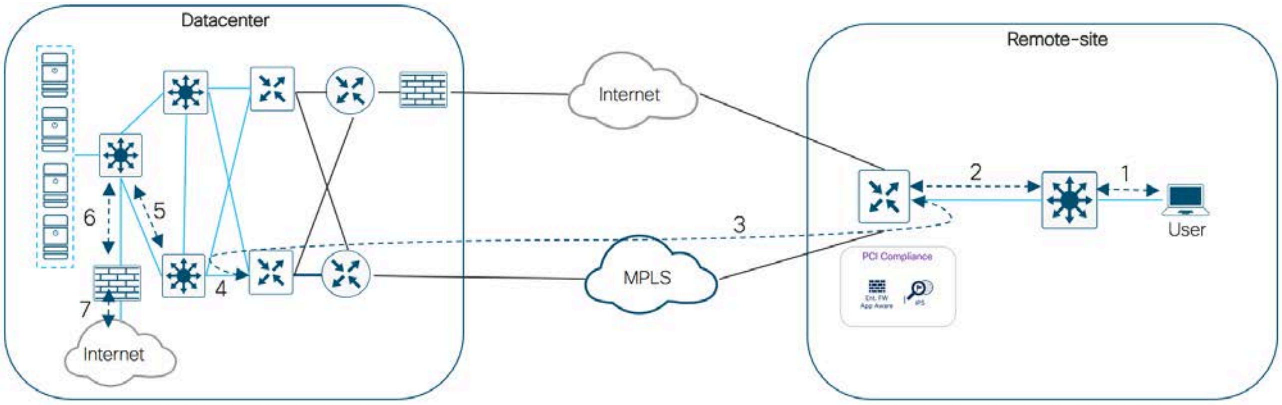
Summary of Traffic Flow on Enabling IPS

Firstly, based on the Snort IPS policy, vManage downloads the container images from the virtual image repository to the WAN Edge device and brings up the container with Snort enabled. Based on the mode and signature level configured, traffic to the target VPN is either detected or prevented. If the mode is set to prevent, then it detects the signature of the traffic and prevents the flow (if the signature is blacklisted) and based on the log level set, an equivalent report is sent to the syslog server.

SD-WAN Compliance Use Case Packet Flow

In the example network below, the remote-site is configured with a single WAN Edge router with an MPLS tunnel and Internet transport tunnel.

Figure 14 Compliance Use Case Packet flow



The first packet entering the source VPN is inspected by the enterprise firewall policy. The inspection consists of examining the layer 4 header, verifying the TCP sequence and acknowledgement numbers, verifying the TCP flags, examining the Layer 7 header of packet, and verifying that the packet conforms to the application specification. Next, UTD is invoked. Traffic is redirected from the data plane to the container that contains Snort. Snort inspects the traffic for threats and traffic with malicious signatures is dropped and the remaining traffic is forwarded back to the router for further processing. The traffic is then routed along the SD-WAN overlay towards the WAN Edge device in the datacenter and then exits out to the Internet.

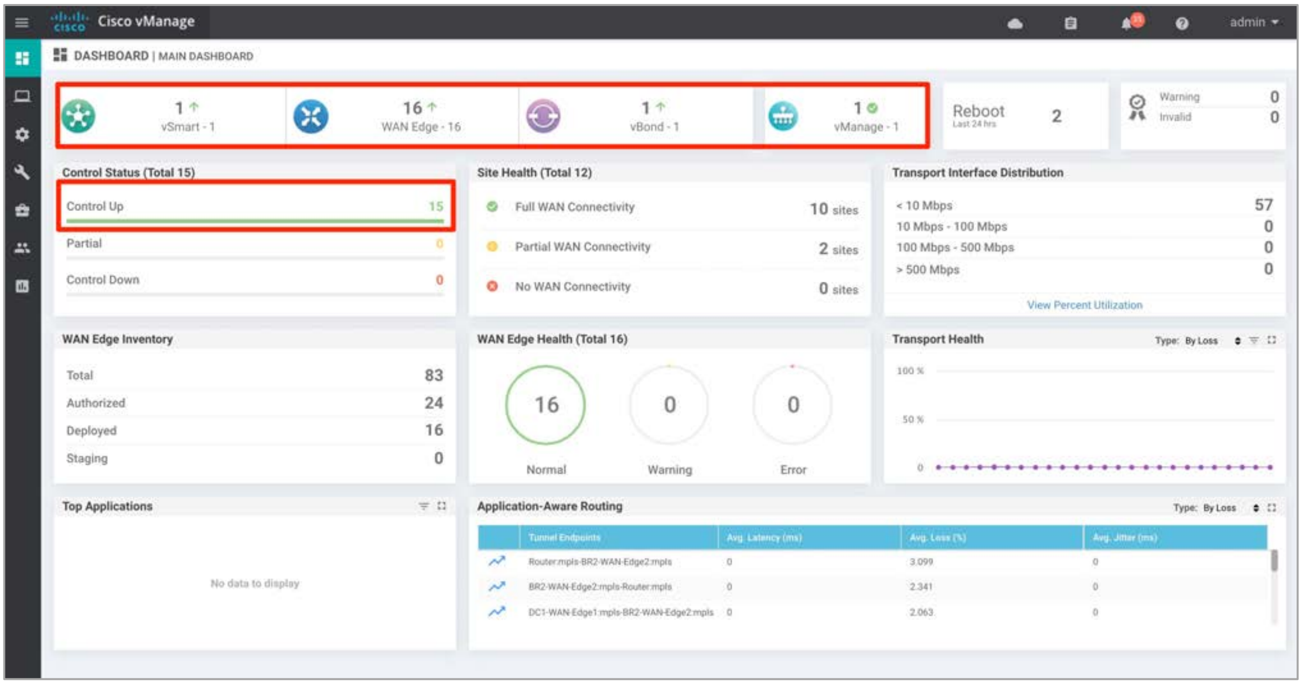
Deploy - Cisco SD-WAN Security - Compliance Use Case - Prerequisites

Prerequisites

This section of the guide focuses on the prerequisites to deploy the SD-WAN security features specific to the compliance use case.

1) Successful deployment of controllers and WAN edge devices

Step 1 Make certain the controllers and WAN Edge devices are successfully deployed and operational.



Control Status (Total 15)

Control Up	15
Partial	0
Control Down	0

Site Health (Total 12)

Full WAN Connectivity	10 sites
Partial WAN Connectivity	2 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

< 10 Mbps	57
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

WAN Edge Inventory

Total	83
Authorized	24
Deployed	16
Staging	0

WAN Edge Health (Total 16)

Normal	Warning	Error
16	0	0

Application-Aware Routing

Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	3.099	0
BR2-WAN-Edge2:mpls-Router:mpls	0	2.341	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	2.063	0

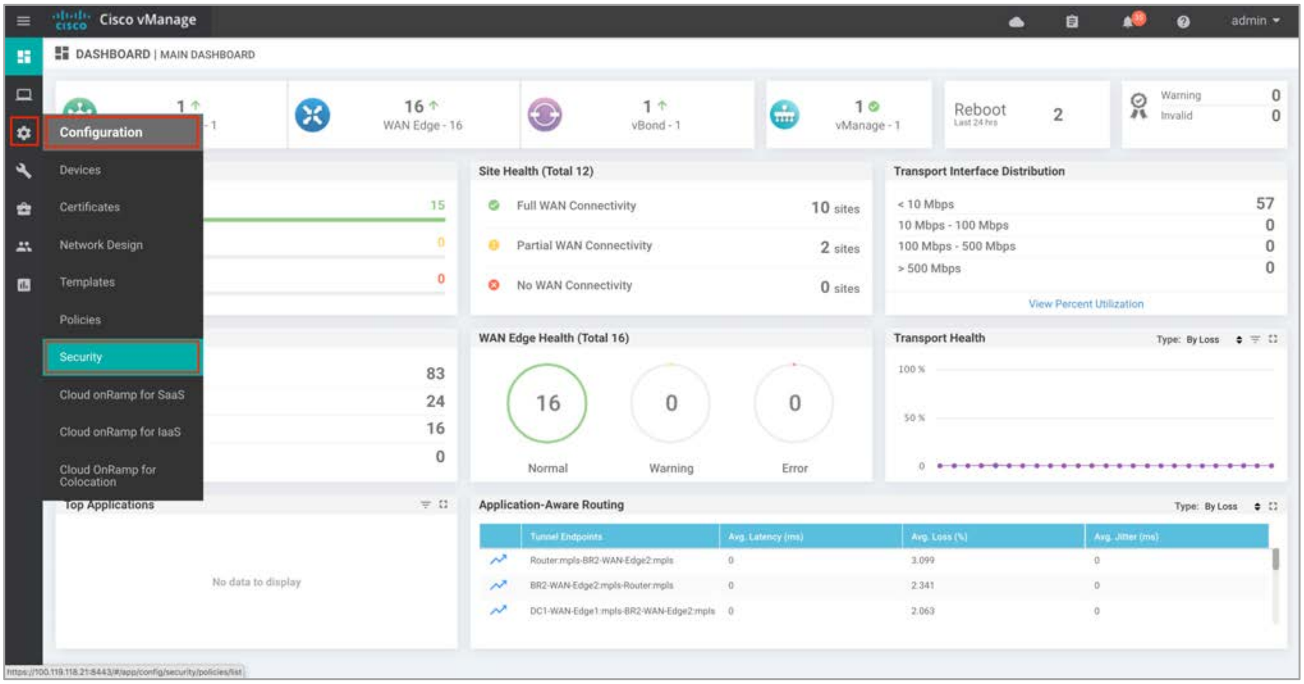
To learn more about device onboarding refer to the SD-WAN Device Onboarding Guide.

Technical Tip: Make sure to choose platforms that support the SD-WAN security features running the minimum required IOS-XE SD-WAN code with supported boot flash and DRAM memory. For details refer to the design section.

2) (Optional) Configure lists for Enterprise Firewall with App Awareness

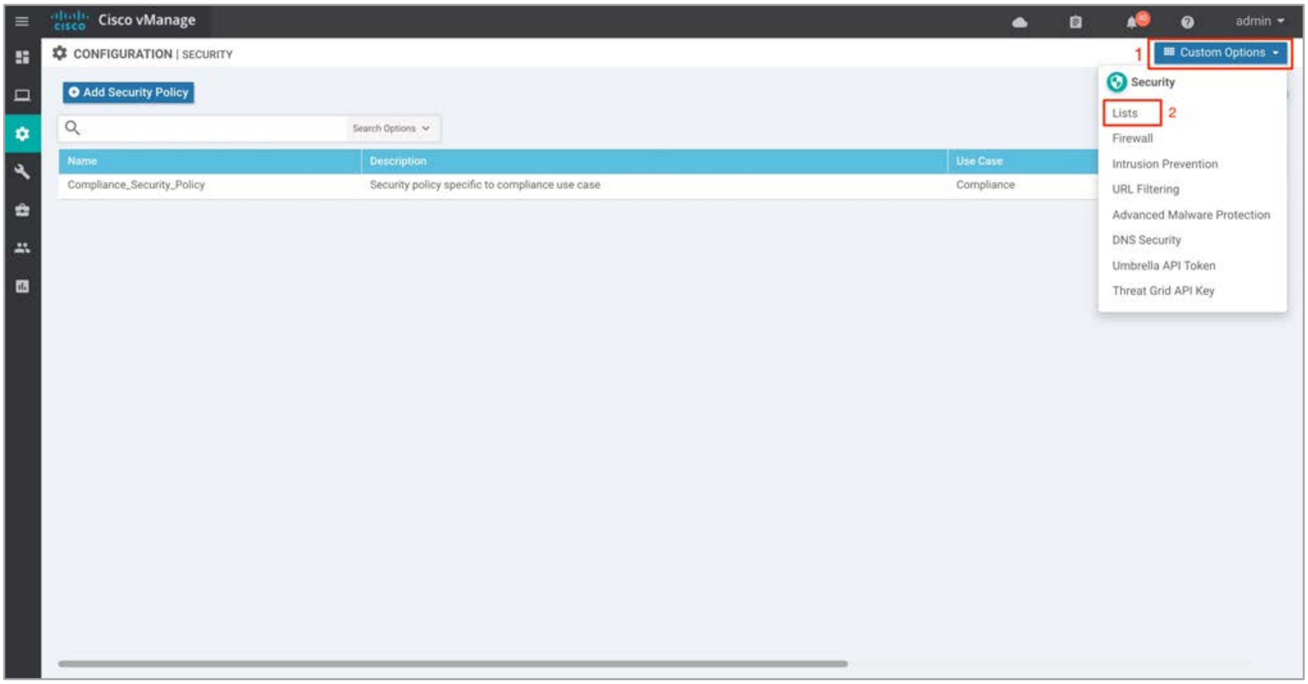
You can choose to either configure firewall zones, data prefixes, and application families prior to building the policy or at the time of building . To build zones prior to building the Enterprise Firewall with App Aware policy, follow the steps below. If not, skip to prerequisite 3.

Step 2 Navigate to **Configuration** > **Security**



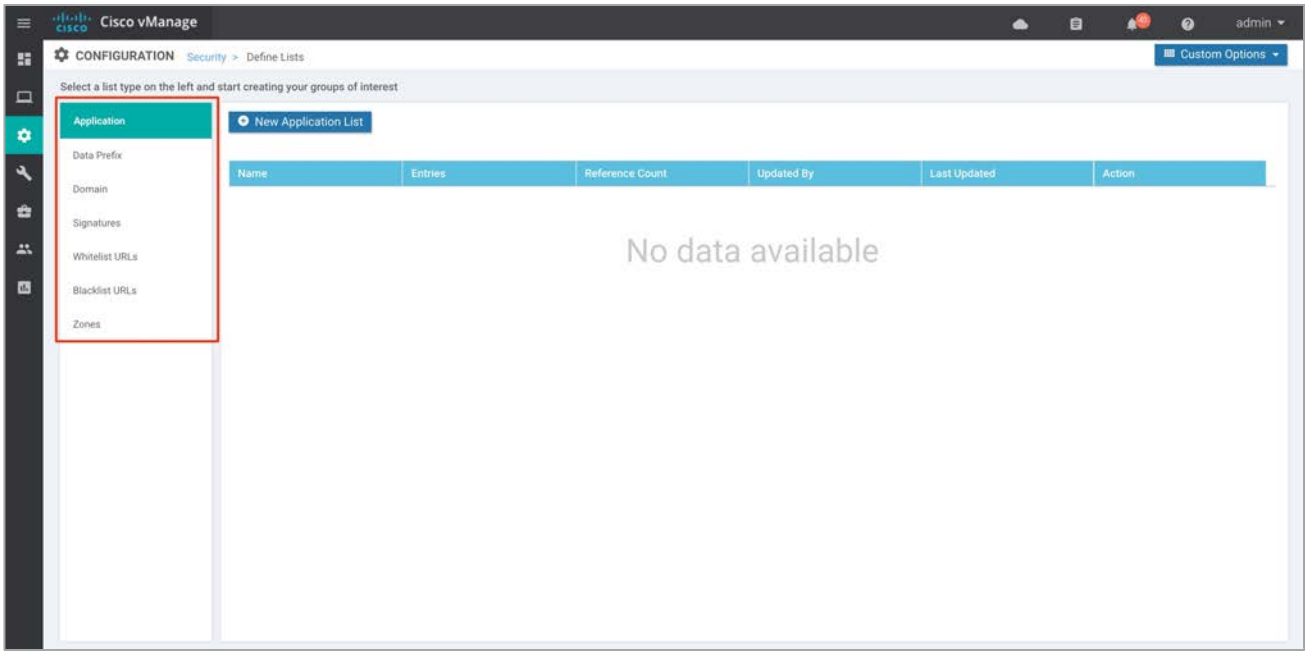
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	3.099	0
BR2-WAN-Edge2:mpls-Router:mpls	0	2.341	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	2.063	0

Step 3 Click **Custom Options**. A drop-down menu of security options appears. Click **Lists**.



Name	Description	Use Case
Compliance_Security_Policy	Security policy specific to compliance use case	Compliance

Step 4 Here, you can preconfigure lists such as **Application Lists**, **Data Prefixes**, **Signatures** and **Zones** which are later used as a part of the security policy. URLs can also be configured here, if you are configuring URL filtering.



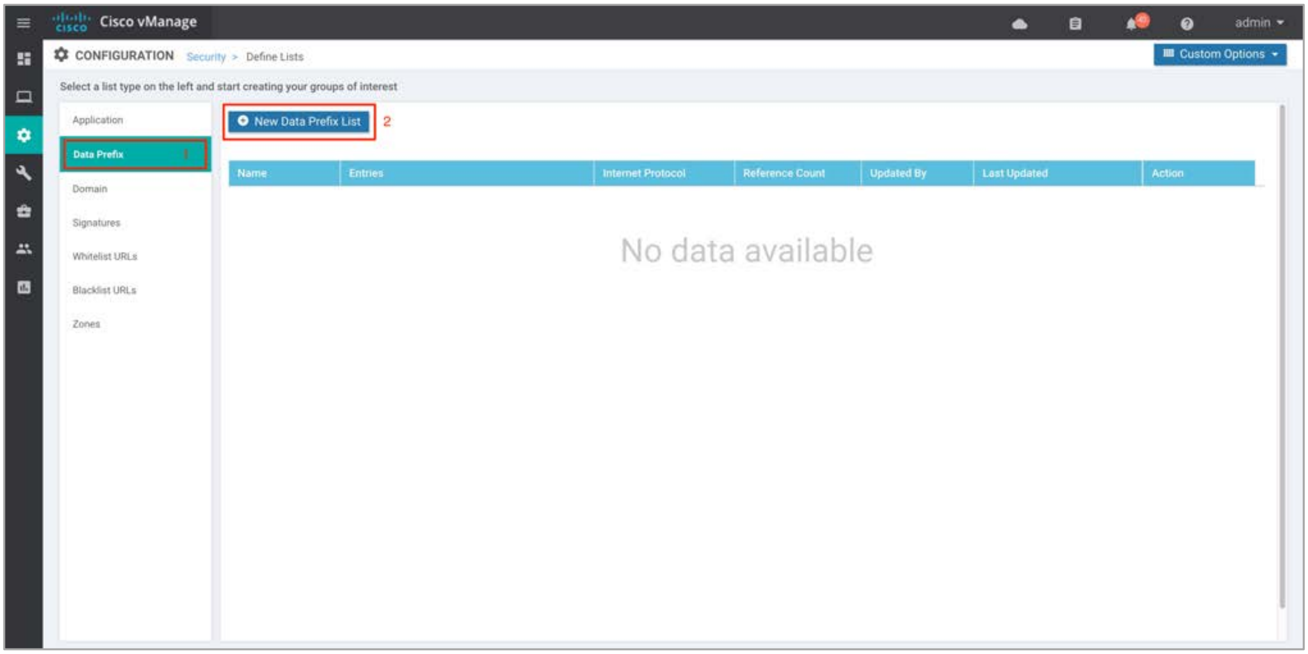
Select a list type on the left and start creating your groups of interest

Name	Entries	Reference Count	Updated By	Last Updated	Action

No data available

In this deployment, source data prefix, destination data prefix, and zones are preconfigured.

Step 5 To configure a data prefix list, select **Data Prefix** and then click **New Data Prefix List**.

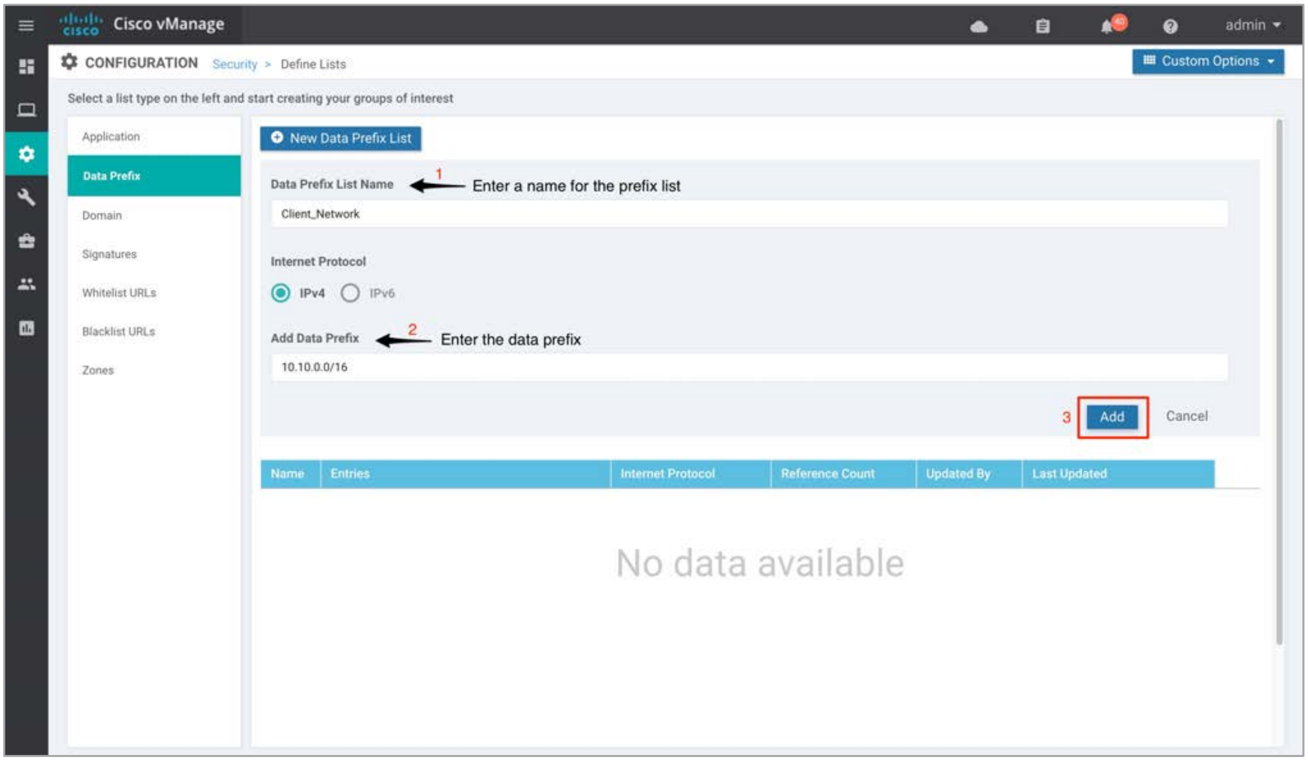


Select a list type on the left and start creating your groups of interest

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action

No data available

Step 6 Enter a name under **Data Prefix List Name**, along with the data prefix under **Add Data Prefix**. Enter prefix details and click **Add**.



Data Prefix List Name: Client_Network

1 Enter a name for the prefix list

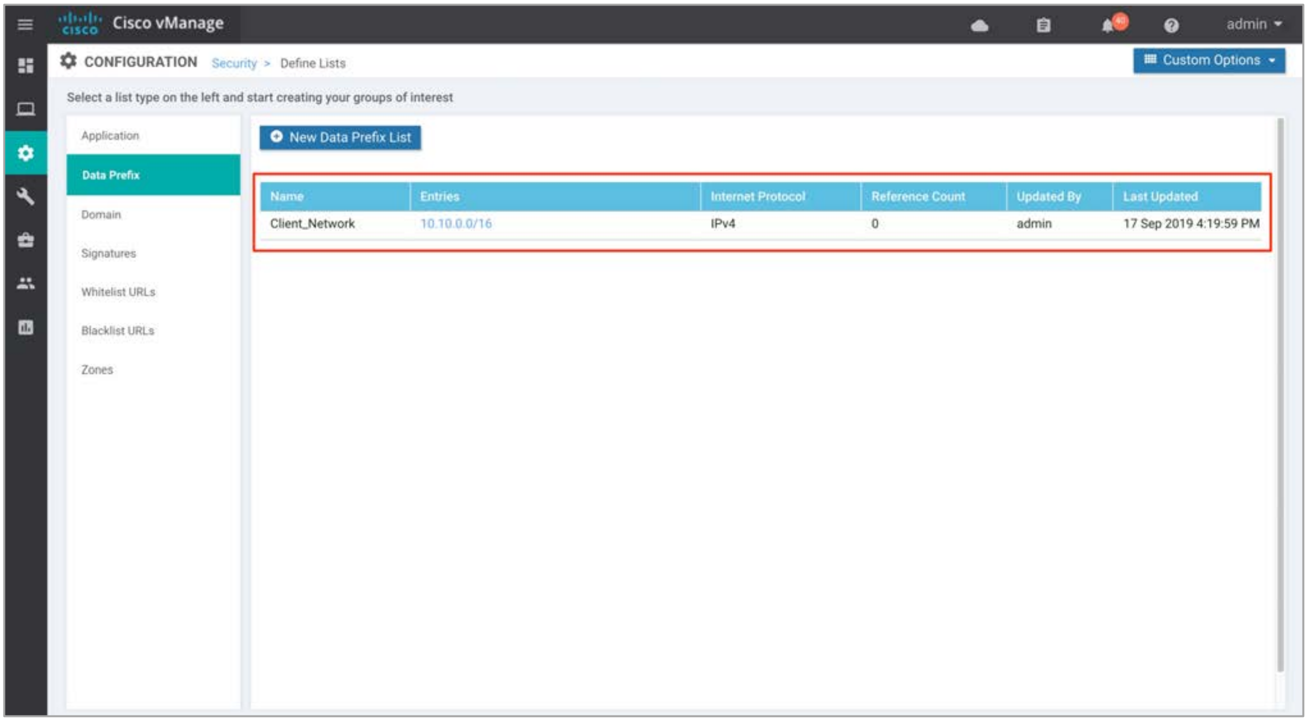
Internet Protocol: ● IPv4 ○ IPv6

Add Data Prefix: 10.10.0.0/16

2 Enter the data prefix

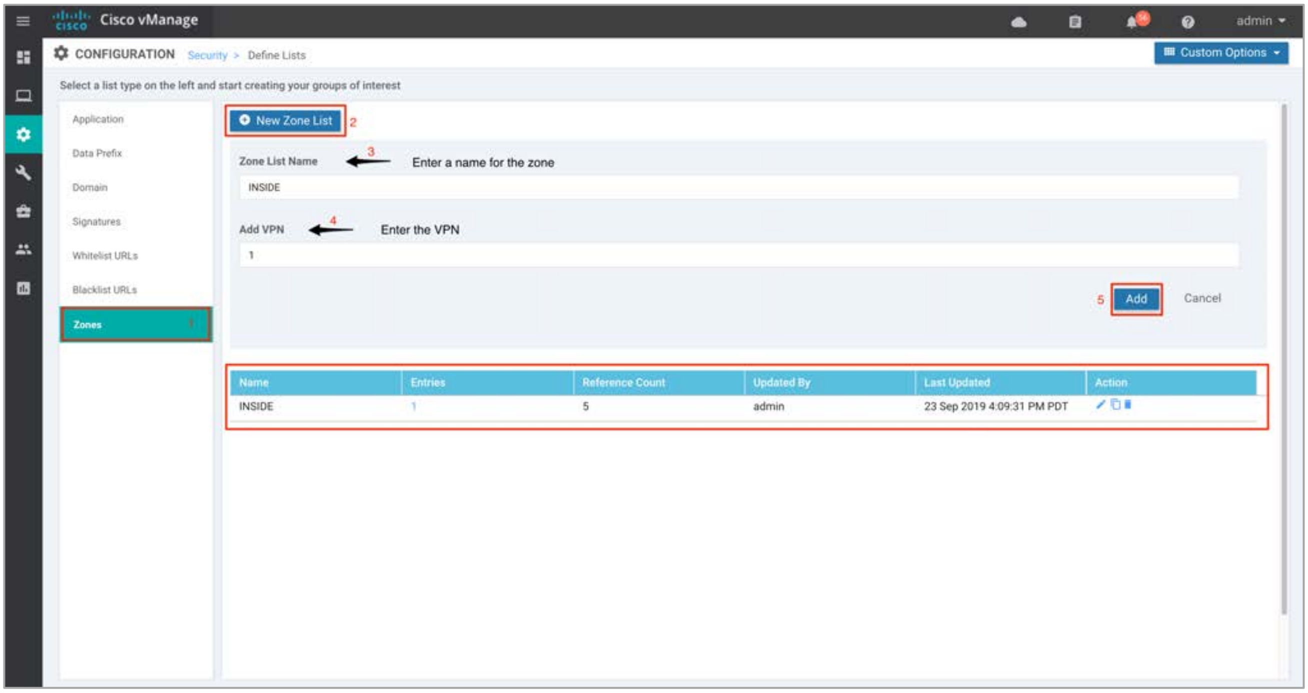
Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated

No data available



Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated
Client_Network	10.10.0.0/16	IPv4	0	admin	17 Sep 2019 4:19:59 PM

Step 7 Similarly, configure a zone. Select **Zones** and then click **New Zone List.** Enter a name within **Zone List** Name and add VPNs within **Add VPN.** Finally, click **Add.**



Select a list type on the left and start creating your groups of interest

Zone List Name: INSIDE

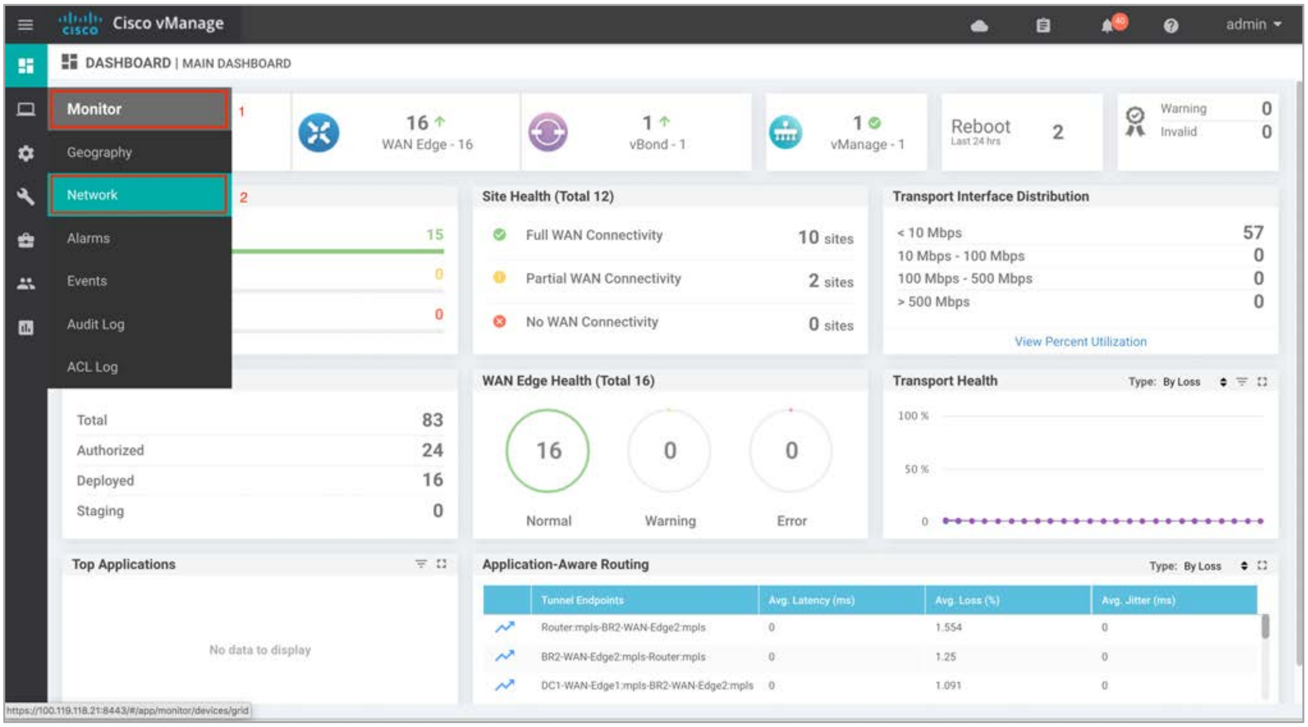
Add VPN: 1

Name	Entries	Reference Count	Updated By	Last Updated	Action
INSIDE	1	5	admin	23 Sep 2019 4:09:31 PM PDT	

3) Upload Virtual Image for Snort IPS

The IPS/IDS feature set is contained within a TAR file, which can be downloaded from the Cisco website. Make sure you upload the UTD engine TAR file for IOS-XE SD-WAN to your vManage software repository prior to building the policy to enable the virtual services.

Step 1 Upload the correct Cisco Security Virtual Image to vManage. To make sure a compatible image is downloaded from Cisco website, login to vManage GUI and Navigate to **Monitor** > **Network.**



Site Health (Total 12)

Full WAN Connectivity	10 sites
Partial WAN Connectivity	2 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

< 10 Mbps	57
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

Total	83
Authorized	24
Deployed	16
Staging	0

WAN Edge Health (Total 16)

Normal	Warning	Error
16	0	0

Transport Health

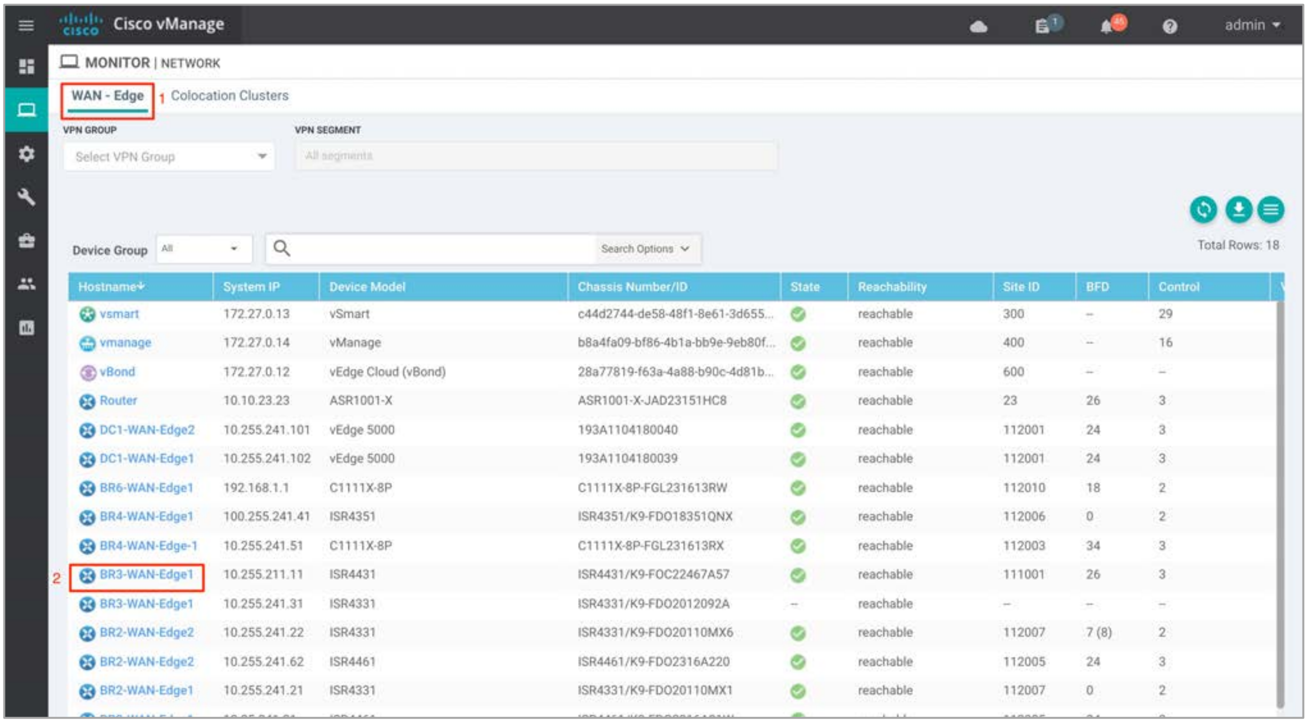
Top Applications

No data to display

Application-Aware Routing

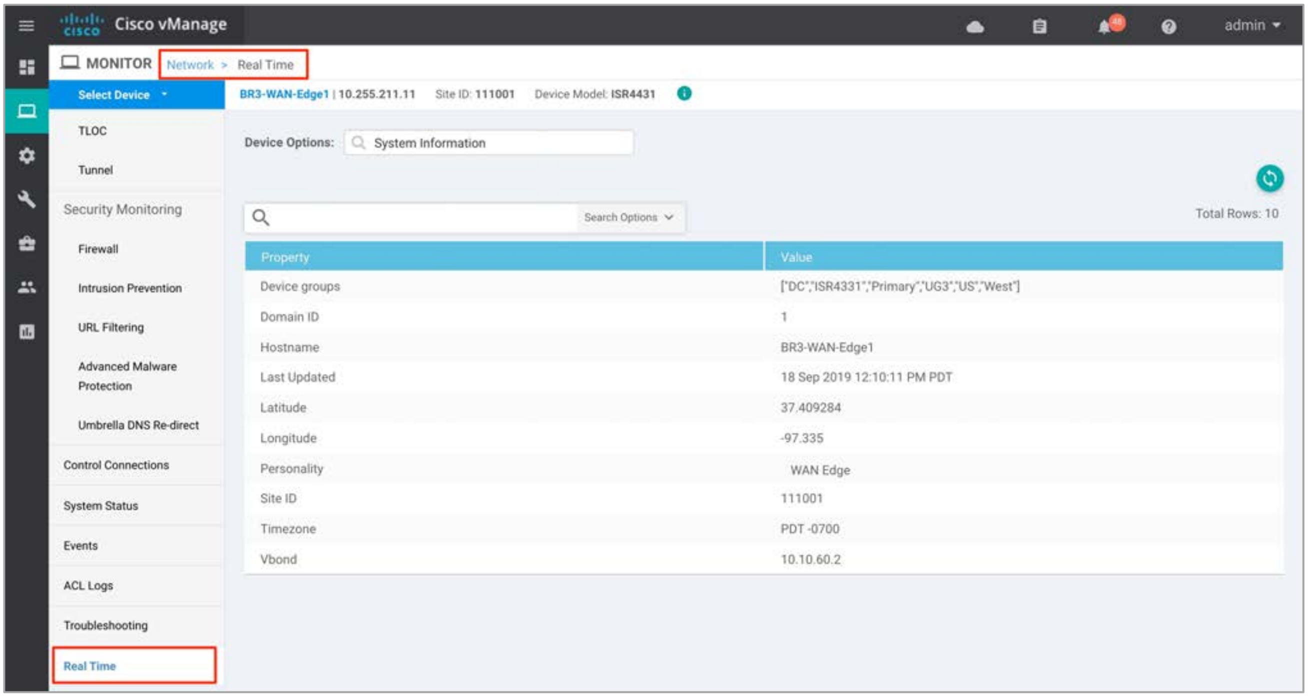
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0
BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0

Step 2 Each router image supports a specific range of versions for a hosted application. For IPS, you can find the range of supported versions (and the recommended version) for a device within its Device Options page. Click on the specific **WAN-Edge** device to which the virtual image will be added.



Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control
vsmart	172.27.0.13	vSmart	c44d2744-de58-48f1-8e61-3d655...	✓	reachable	300	–	29
vmanage	172.27.0.14	vManage	b8a4fa09-bf86-4b1a-bb9e-9eb80f...	✓	reachable	400	–	16
vBond	172.27.0.12	vEdge Cloud (vBond)	28a77819-f63a-4a88-b90c-4d81b...	✓	reachable	600	–	–
Router	10.10.23.23	ASR1001-X	ASR1001-X-JAD23151HC8	✓	reachable	23	26	3
DC1-WAN-Edge2	10.255.241.101	vEdge 5000	193A1104180040	✓	reachable	112001	24	3
DC1-WAN-Edge1	10.255.241.102	vEdge 5000	193A1104180039	✓	reachable	112001	24	3
BR6-WAN-Edge1	192.168.1.1	C1111X-8P	C1111X-8P-FGL231613RW	✓	reachable	112010	18	2
BR4-WAN-Edge1	100.255.241.41	ISR4351	ISR4351/K9-FDO18351QNX	✓	reachable	112006	0	2
BR4-WAN-Edge-1	10.255.241.51	C1111X-8P	C1111X-8P-FGL231613RX	✓	reachable	112003	34	3
BR3-WAN-Edge1	10.255.211.11	ISR4431	ISR4431/K9-FOC22467A57	✓	reachable	111001	26	3
BR3-WAN-Edge1	10.255.241.31	ISR4331	ISR4331/K9-FDO2012092A	–	reachable	–	–	–
BR2-WAN-Edge2	10.255.241.22	ISR4331	ISR4331/K9-FDO20110MX6	✓	reachable	112007	7 (8)	2
BR2-WAN-Edge2	10.255.241.62	ISR4461	ISR4461/K9-FDO2316A220	✓	reachable	112005	24	3
BR2-WAN-Edge1	10.255.241.21	ISR4331	ISR4331/K9-FDO20110MX1	✓	reachable	112007	0	2

Step 3 Within **Network**, click **Real Time**.

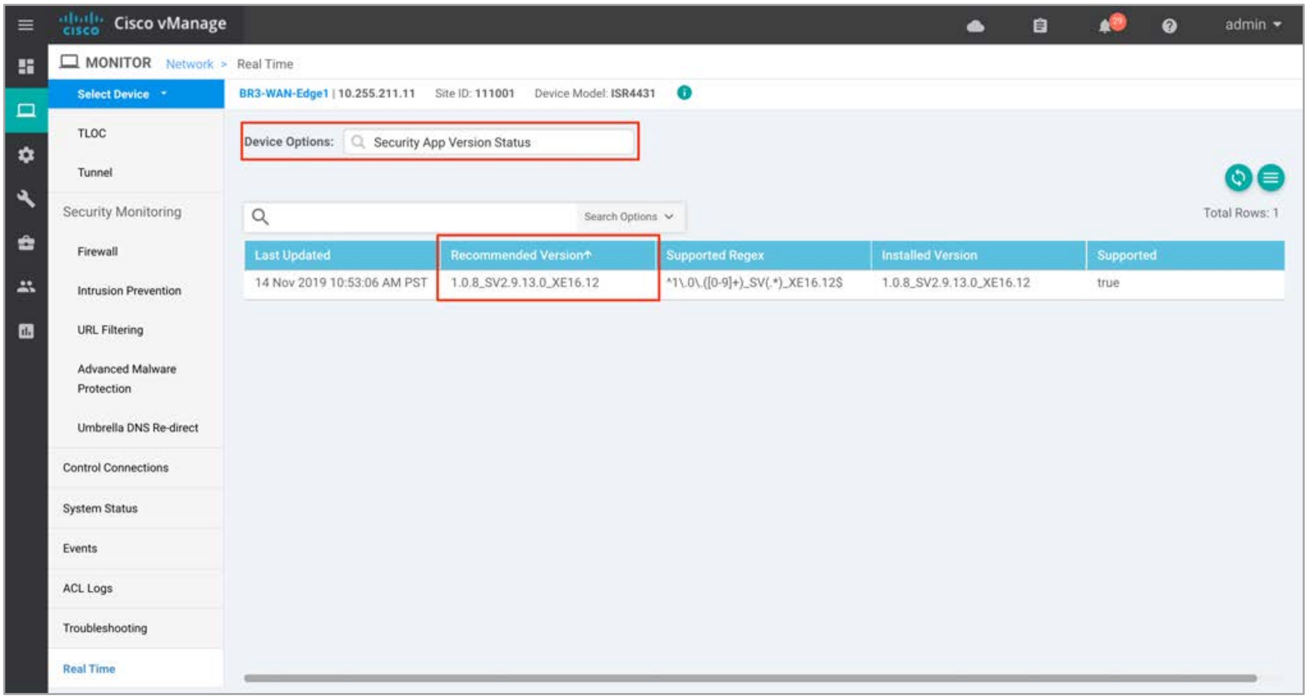


BR3-WAN-Edge1 | 10.255.211.11   Site ID: 111001   Device Model: ISR4431

Device Options: System Information

Property	Value
Device groups	["DC","ISR4331","Primary","UG3","US","West"]
Domain ID	1
Hostname	BR3-WAN-Edge1
Last Updated	18 Sep 2019 12:10:11 PM PDT
Latitude	37.409284
Longitude	-97.335
Personality	WAN Edge
Site ID	111001
Timezone	PDT -0700
Vbond	10.10.60.2

Step 4 Within the **Device Options**, enter **Security App Version Status**. Within the **Recommended Version**, you will find the recommended UTD Image that must be downloaded for that specific device.

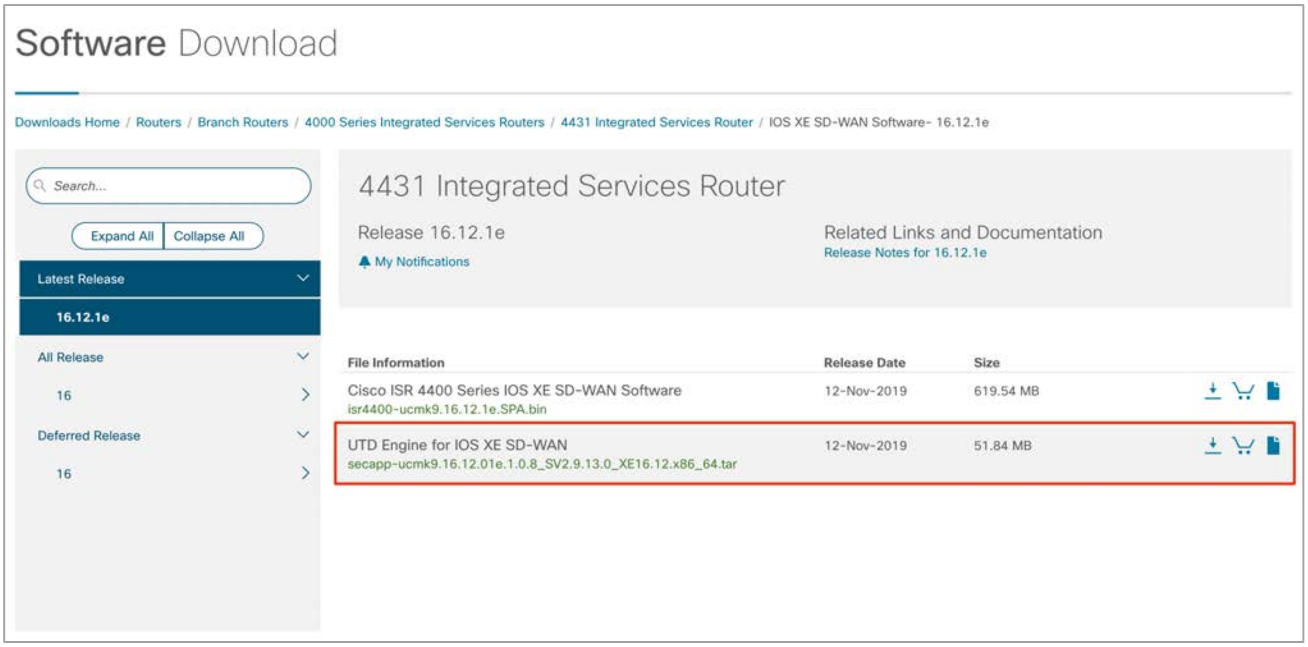


BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: Security App Version Status

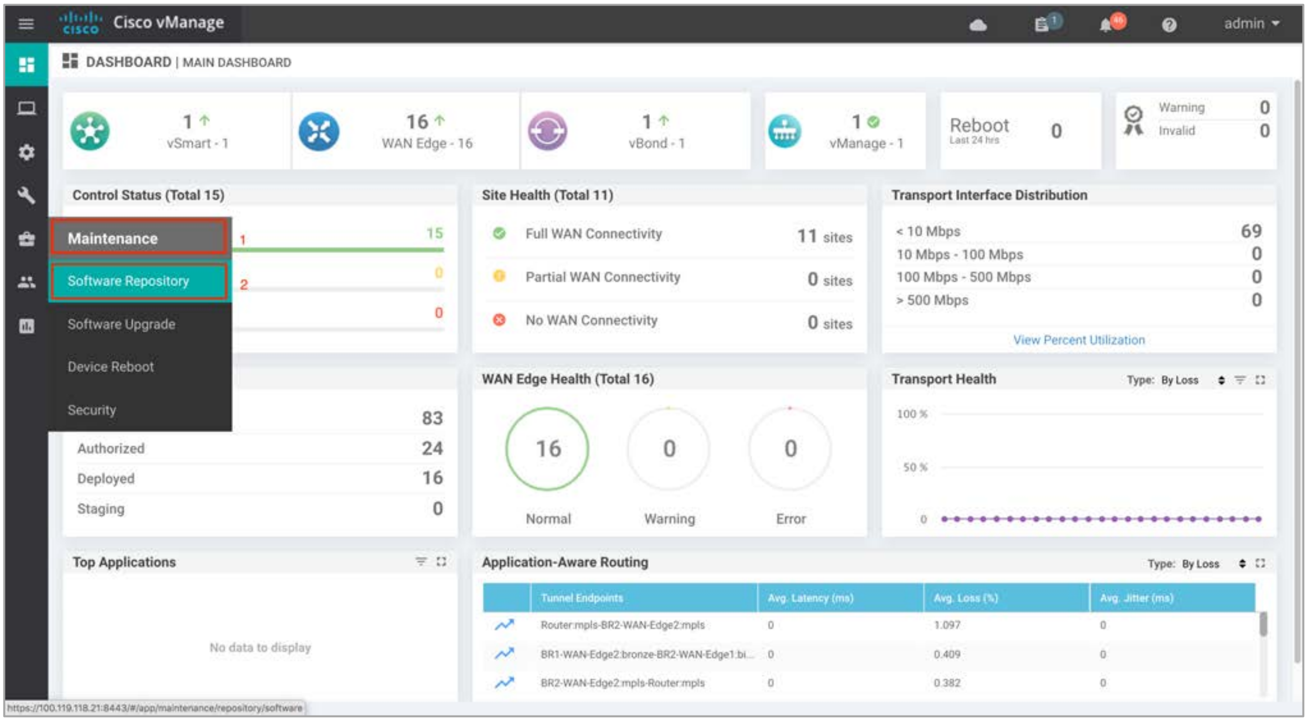
Last Updated	Recommended Version	Supported Regex	Installed Version	Supported
14 Nov 2019 10:53:06 AM PST	1.0.8_SV2.9.13.0_XE16.12	^1\.0\.([0-9]+)_SV(.*)_XE16.12$	1.0.8_SV2.9.13.0_XE16.12	true

Step 5 From the Software Download page, locate the image **UTD Engine for IOS XE SD-WAN**. Click the download icon on the right-hand side of the window to download the UTD image file.


Software Download
Downloads Home / Routers / Branch Routers / 4000 Series Integrated Services Routers / 4431 Integrated Services Router / IOS XE SD-WAN Software- 16.12.1e
Search...
Expand All
Collapse All
Latest Release
16.12.1e
All Release
16
Deferred Release
16
4431 Integrated Services Router
Release 16.12.1e
My Notifications
Related Links and Documentation
Release Notes for 16.12.1e

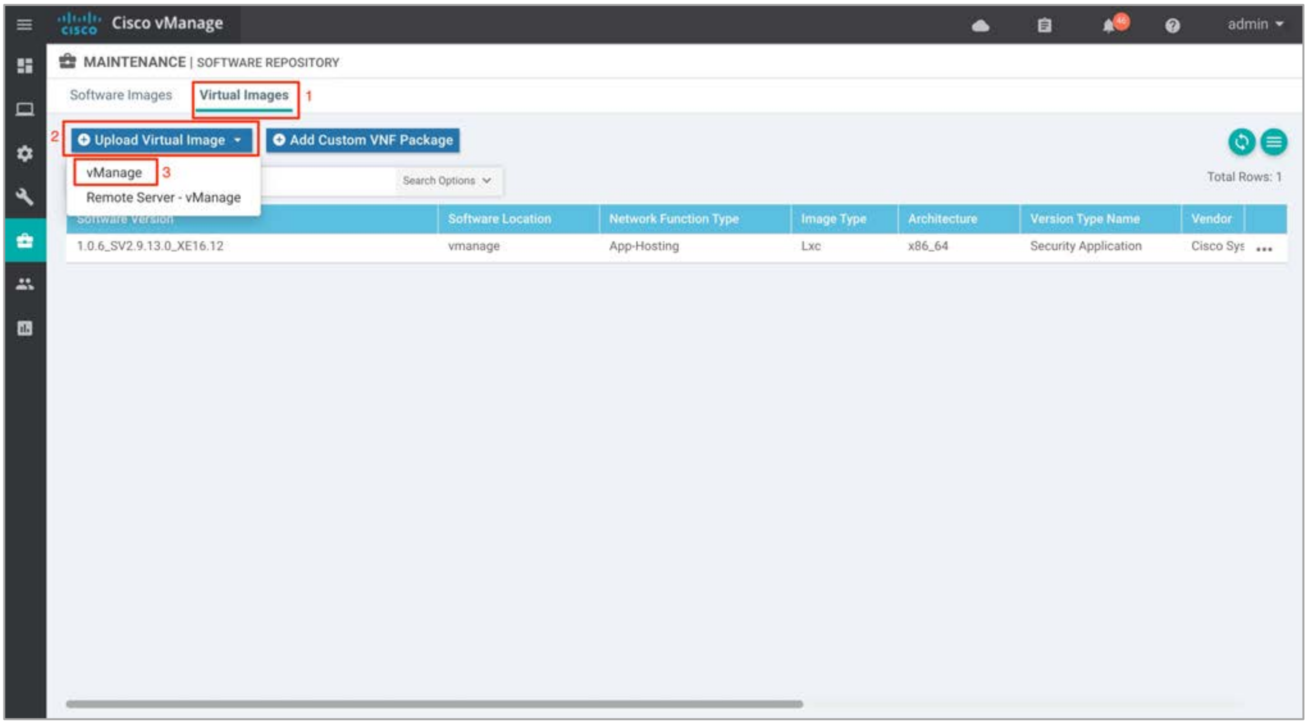
File Information	Release Date	Size
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.1e.SPA.bin	12-Nov-2019	619.54 MB
UTD Engine for IOS XE SD-WAN secapp-ucmk9.16.12.01e.1.0.8_SV2.9.13.0_XE16.12.x86_64.tar	12-Nov-2019	51.84 MB

Step 6 Within the vManage dashboard, select **Maintenance** > **Software Repository**.



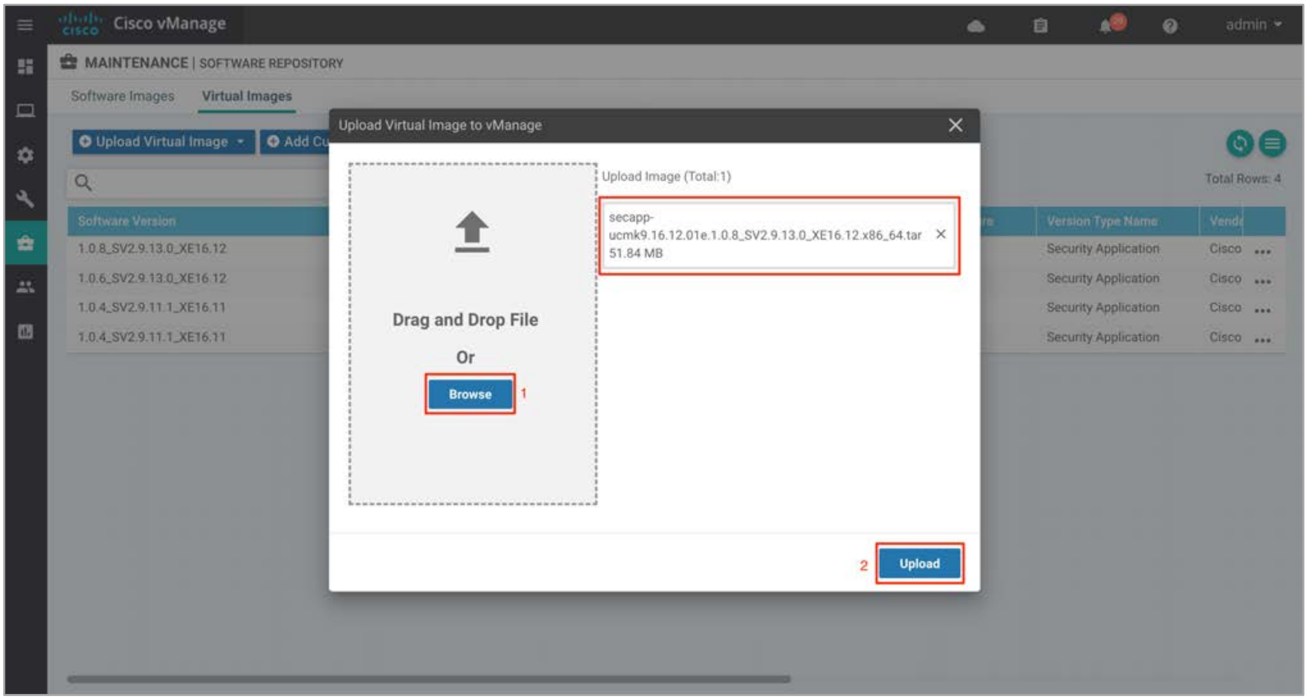
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	1.097	0
BR1-WAN-Edge2:bronze-BR2-WAN-Edge1:bi...	0	0.409	0
BR2-WAN-Edge2:mpls-Router:mpls	0	0.382	0

Step 7 To upload the UTD file to the vManage **Software Repository**, click the **Upload Virtual Image tab** and select **vManage**. The **Virtual Image** is downloaded into the WAN Edge device over a control plane connection.



Software Version	Software Location	Network Function Type	Image Type	Architecture	Version Type Name	Vendor
1.0.6_SV2.9.13.0_XE16.12	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Sys

Step 8 Next, click **Browse** to upload the downloaded UTD image. The image appears on the right. Click **Upload** to add the image into the **Software Repository**. If you already have the same image uploaded, a notification of possible overwrite populates.



secapp-ucmk9.16.12.01e.1.0.8_SV2.9.13.0_XE16.12.x86_64.tar
51.84 MB

Software Version	Version Type Name	Vend
1.0.8_SV2.9.13.0_XE16.12	Security Application	Cisco
1.0.6_SV2.9.13.0_XE16.12	Security Application	Cisco
1.0.4_SV2.9.11.1_XE16.11	Security Application	Cisco
1.0.4_SV2.9.11.1_XE16.11	Security Application	Cisco

Technical Tip: To delete the software image from your vManage software repository, select the software image, click the **More** actions icon and click **Delete**. Note that the UTD image can be upgraded via vManage to a later code as long as the latest code is uploaded to the **Software Repository**.

4) **(Optional) Create a Security App Hosting Profile Template**

As explained in the design section on attaching a configured IPS Policy within the device template, a sub-template titled container profile must be added. This container profile template allows you to enable/disable NAT for your virtual services (IPS) and allocate resources for the virtual services.

Container Profile template contains:

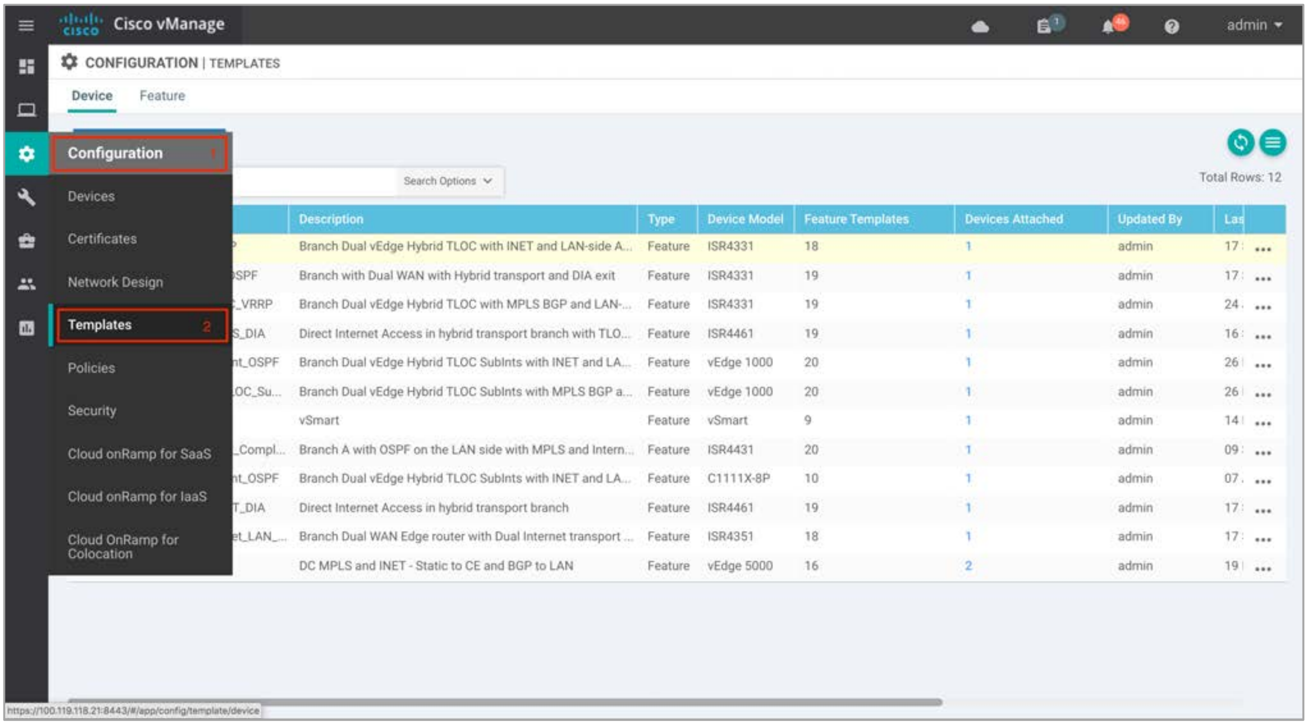
6) **Resource Profile** that is set to default of one core. For higher throughput, you may set the resource profile to High allocating two cores.

7) **NAT** functionality can be enabled if virtual services must go out to the Internet for manual signature updates or if there is a need to send syslogs to an external syslog server that is not necessarily in the data center.

If you do not wish to alter the values, skip building the template and use the default Security App Hosting Profile template wherein NAT is by default turned **ON** and Resource Profile is set to **Default.**

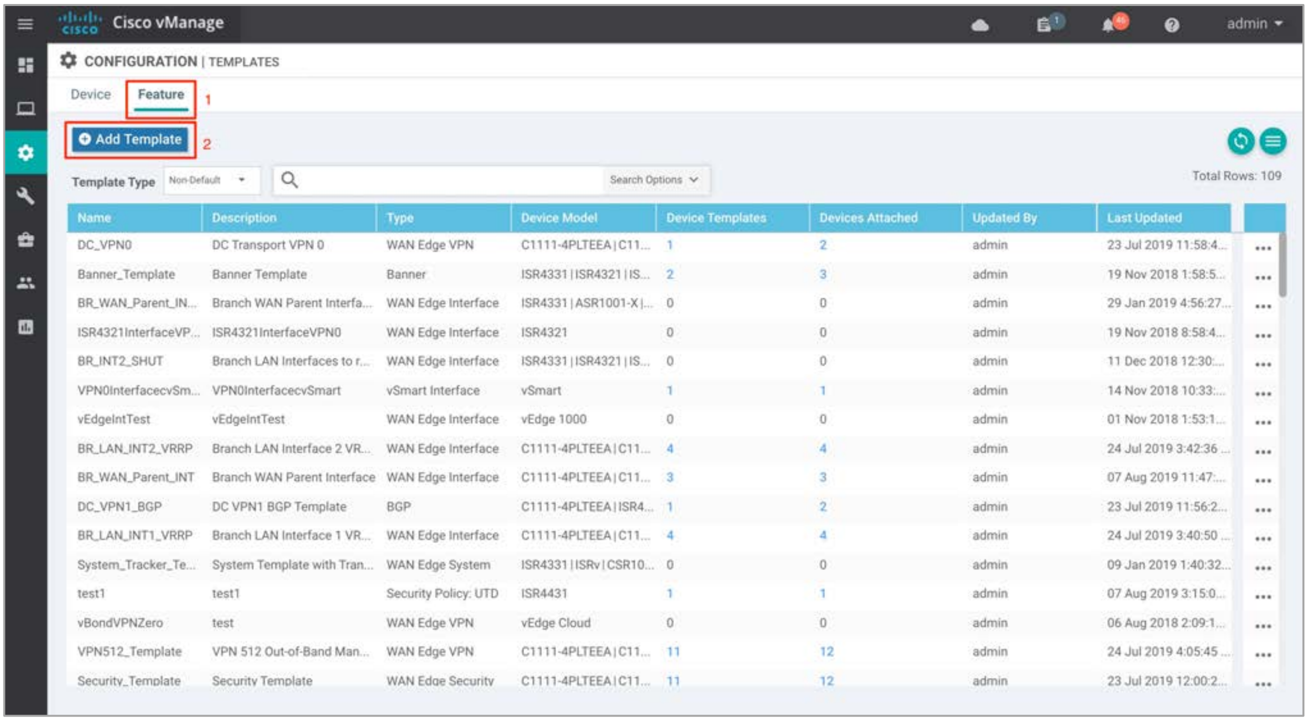
To create a new template, follow the steps below.

Step 1 Navigate to **Configuration** > **Templates**.



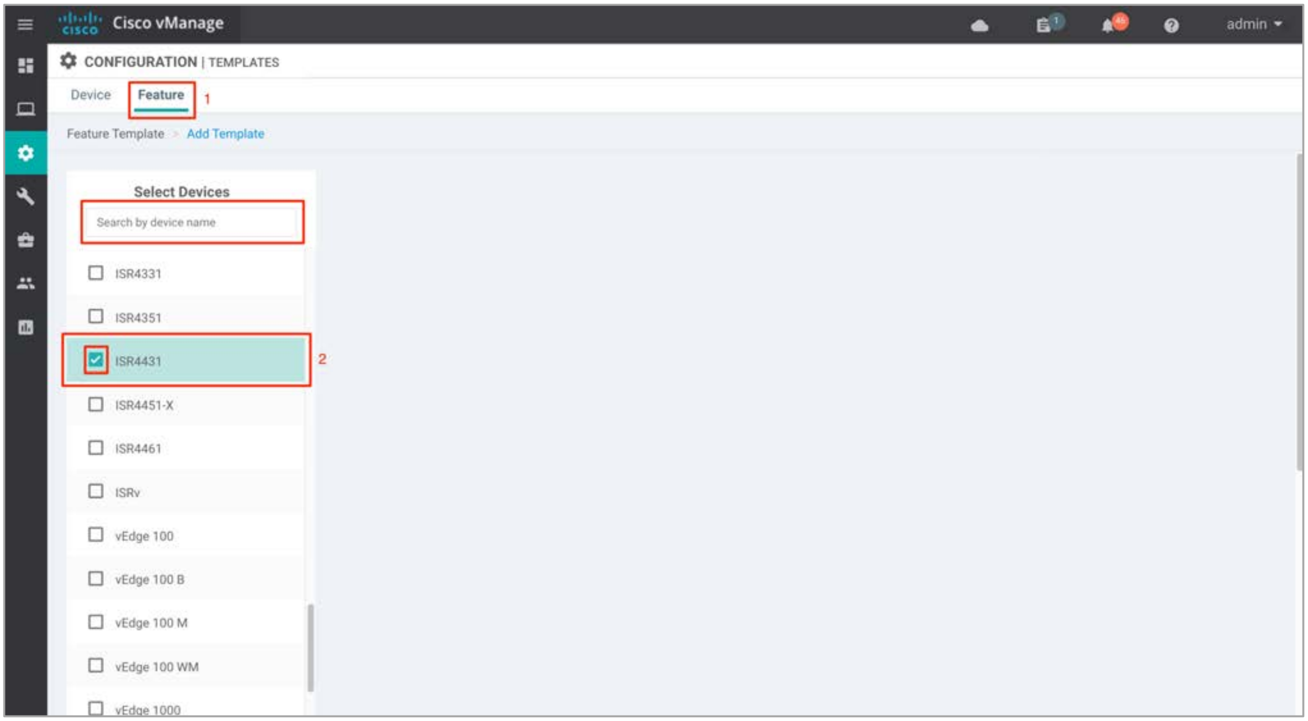
	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Las
P	Branch Dual vEdge Hybrid TLOC with INET and LAN-side A...	Feature	ISR4331	18	1	admin	17
SPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	19	1	admin	17
_VRRP	Branch Dual vEdge Hybrid TLOC with MPLS BGP and LAN-...	Feature	ISR4331	19	1	admin	24
S_DIA	Direct Internet Access in hybrid transport branch with TLO...	Feature	ISR4461	19	1	admin	16
nt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LA...	Feature	vEdge 1000	20	1	admin	26
OC_Su...	Branch Dual vEdge Hybrid TLOC SubInts with MPLS BGP a...	Feature	vEdge 1000	20	1	admin	26
	vSmart	Feature	vSmart	9	1	admin	14
_Compl...	Branch A with OSPF on the LAN side with MPLS and Intern...	Feature	ISR4431	20	1	admin	09
nt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LA...	Feature	C1111X-8P	10	1	admin	07
T_DIA	Direct Internet Access in hybrid transport branch	Feature	ISR4461	19	1	admin	17
et_LAN_...	Branch Dual WAN Edge router with Dual Internet transport ...	Feature	ISR4351	18	1	admin	17
	DC MPLS and INET - Static to CE and BGP to LAN	Feature	vEdge 5000	16	2	admin	19

Step 2 Select **Feature** and click **Add Template** to create a new feature template.

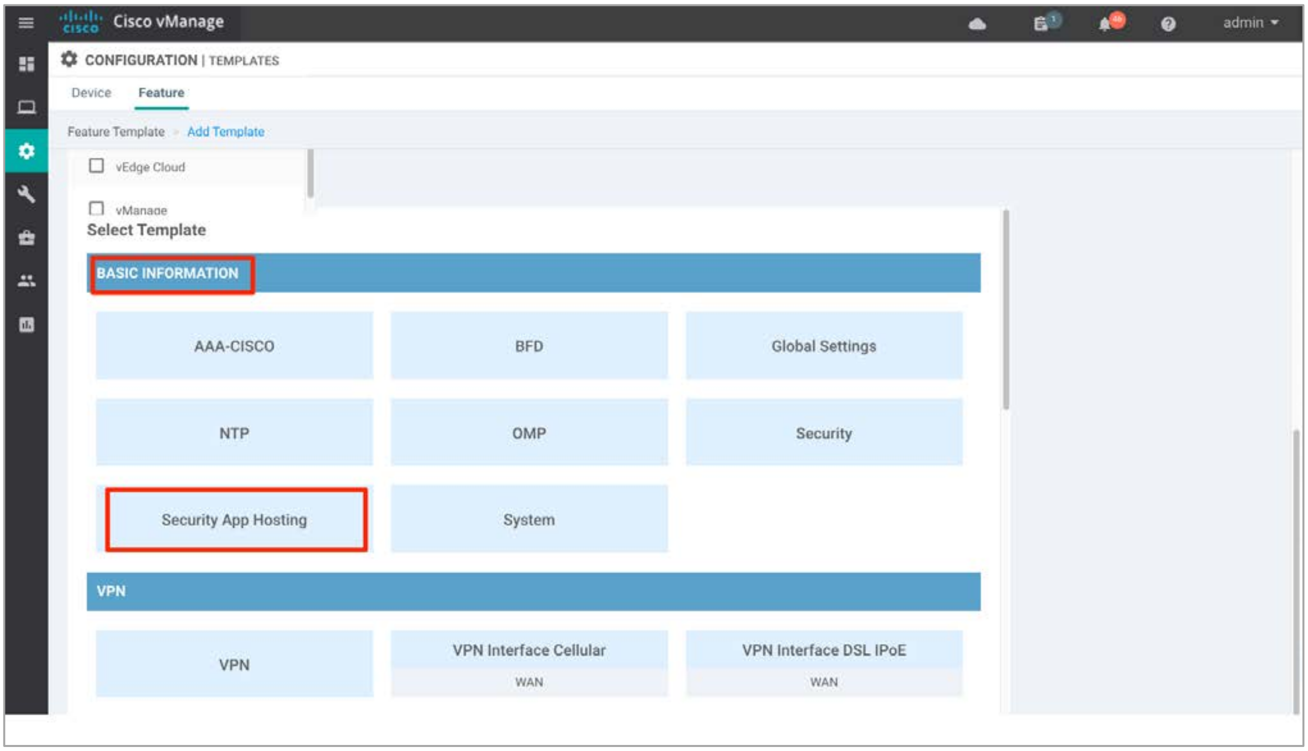


Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
DC_VPN0	DC Transport VPN 0	WAN Edge VPN	C1111-4PLTEEA | C11...	1	2	admin	23 Jul 2019 11:58:4...
Banner_Template	Banner Template	Banner	ISR4331 | ISR4321 | IS...	2	3	admin	19 Nov 2018 1:58:5...
BR_WAN_Parent_IN...	Branch WAN Parent Interfa...	WAN Edge Interface	ISR4331 | ASR1001-X |...	0	0	admin	29 Jan 2019 4:56:27...
ISR4321InterfaceVP...	ISR4321InterfaceVPN0	WAN Edge Interface	ISR4321	0	0	admin	19 Nov 2018 8:58:4...
BR_INT2_SHUT	Branch LAN Interfaces to r...	WAN Edge Interface	ISR4331 | ISR4321 | IS...	0	0	admin	11 Dec 2018 12:30:...
VPN0InterfacecvSm...	VPN0InterfacecvSmart	vSmart Interface	vSmart	1	1	admin	14 Nov 2018 10:33:...
vEdgeIntTest	vEdgeIntTest	WAN Edge Interface	vEdge 1000	0	0	admin	01 Nov 2018 1:53:1...
BR_LAN_INT2_VRRP	Branch LAN Interface 2 VR...	WAN Edge Interface	C1111-4PLTEEA | C11...	4	4	admin	24 Jul 2019 3:42:36 ...
BR_WAN_Parent_INT	Branch WAN Parent Interface	WAN Edge Interface	C1111-4PLTEEA | C11...	3	3	admin	07 Aug 2019 11:47:...
DC_VPN1_BGP	DC VPN1 BGP Template	BGP	C1111-4PLTEEA | ISR4...	1	2	admin	23 Jul 2019 11:56:2...
BR_LAN_INT1_VRRP	Branch LAN Interface 1 VR...	WAN Edge Interface	C1111-4PLTEEA | C11...	4	4	admin	24 Jul 2019 3:40:50 ...
System_Tracker_Te...	System Template with Tran...	WAN Edge System	ISR4331 | ISRv | CSR10...	0	0	admin	09 Jan 2019 1:40:32...
test1	test1	Security Policy: UTD	ISR4431	1	1	admin	07 Aug 2019 3:15:0...
vBondVPNZero	test	WAN Edge VPN	vEdge Cloud	0	0	admin	06 Aug 2018 2:09:1...
VPN512_Template	VPN 512 Out-of-Band Man...	WAN Edge VPN	C1111-4PLTEEA | C11...	11	12	admin	24 Jul 2019 4:05:45 ...
Security_Template	Security Template	WAN Edge Security	C1111-4PLTEEA | C11...	11	12	admin	23 Jul 2019 12:00:2...

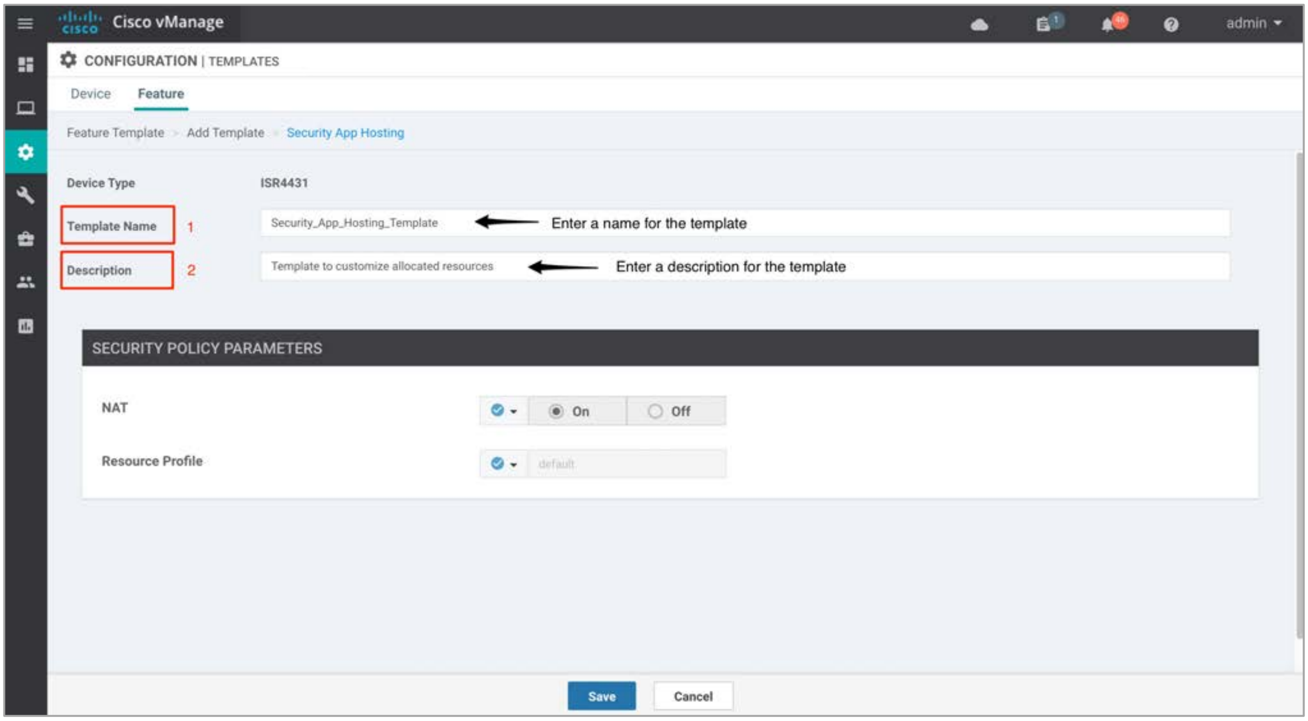
Step 3 Within the **Feature Template**, select a device(s) or enter the device in the search bar.



Step 4 Next, select **Security App Hosting** to create the template.



Step 5 Within the **Feature Template**, enter a name and description for the template.



Device Type ISR4431

Template Name 1 Security_App_Hosting_Template ← Enter a name for the template

Description 2 Template to customize allocated resources ← Enter a description for the template

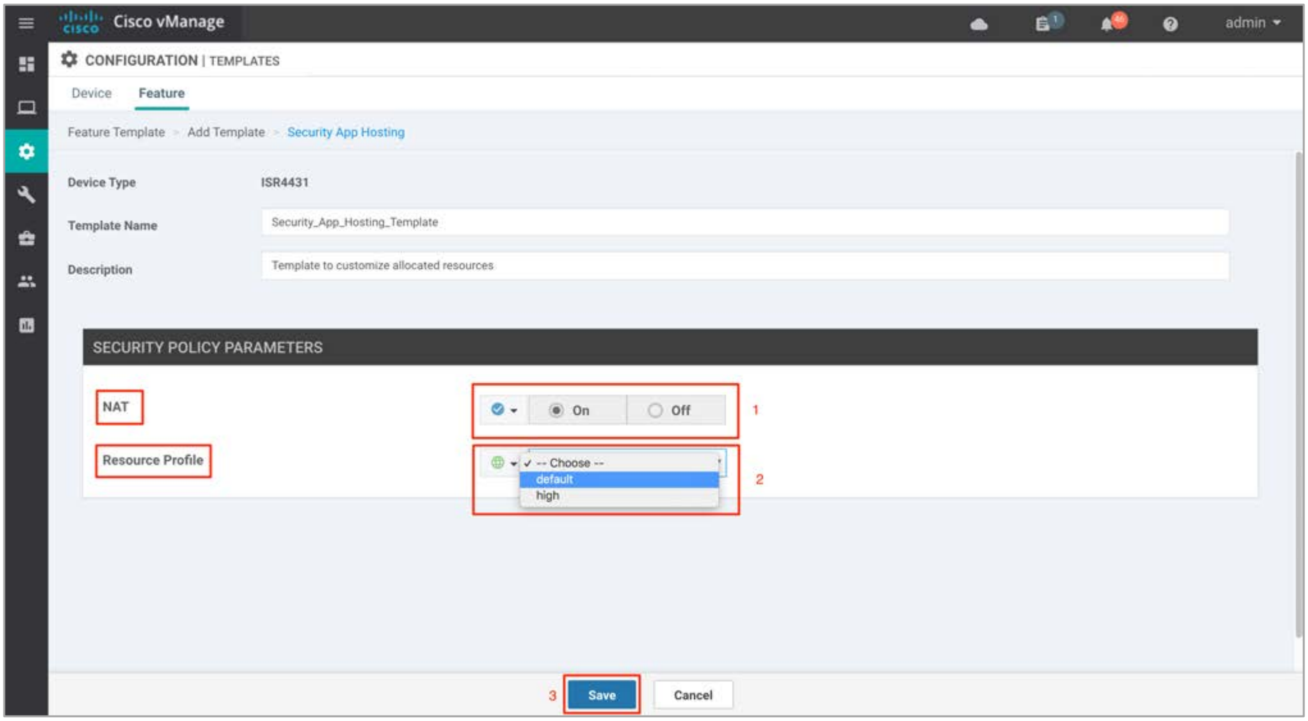
SECURITY POLICY PARAMETERS

NAT ● On ○ Off

Resource Profile default

Cisco vManage
admin
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template › Add Template › Security App Hosting
Save
Cancel

Step 6 Customize the security policy parameters if required. Enable or disable **NAT** feature, based on your use case. For higher throughput or if more packets need to be inspected, set the **Resource Profile** to **high**. Refer to the Design section within Snort IPS, before making changes to the template. Finally, **Save** the template.



Device Type ISR4431

Template Name Security_App_Hosting_Template

Description Template to customize allocated resources

SECURITY POLICY PARAMETERS

NAT ● On ○ Off 1

Resource Profile -- Choose -- / default / high 2

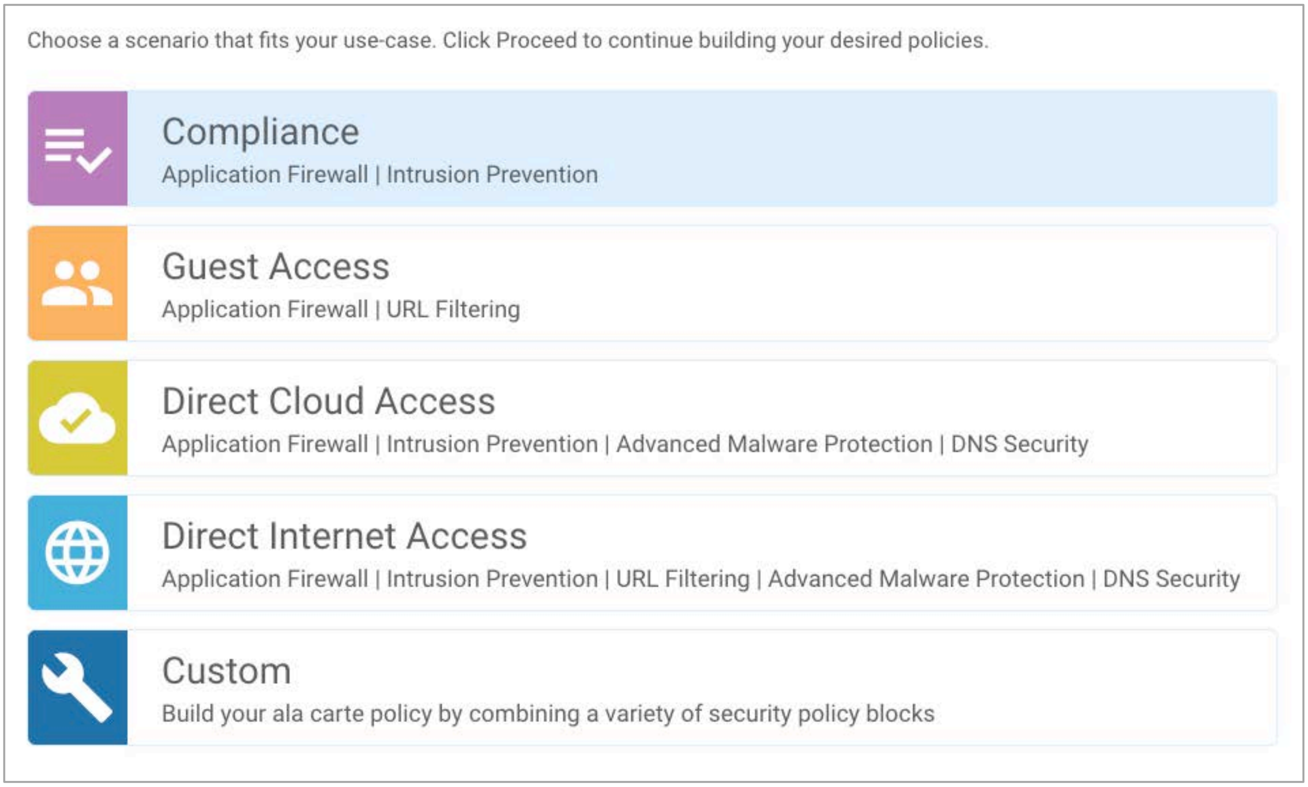
Cisco vManage
admin
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template › Add Template › Security App Hosting
3
Save
Cancel

In this deployment, the security policy parameters are set as follows.

Feature	Type	Set
NAT	Global	On
Resource Profile Default	Global	Default

Deploy - Cisco SD-WAN Security - Compliance Use Case

The SD-WAN security solution is easy to deploy using the intent-based use cases available on vManage GUI.



Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

Compliance
Application Firewall | Intrusion Prevention

Guest Access
Application Firewall | URL Filtering

Direct Cloud Access
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security

Direct Internet Access
Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security

Custom
Build your ala carte policy by combining a variety of security policy blocks

This section of the guide provides the steps to deploy security features specific to the complaicne user case. The features discussed include Enterprise Firewall with App Awareness (Application Firewall) and Intrusion Prevention.

Configuration Workflow

1) Make sure all the prerequisites mentioned in the previous section are added.

2) Enable the IPS signature automatic update using vManage.

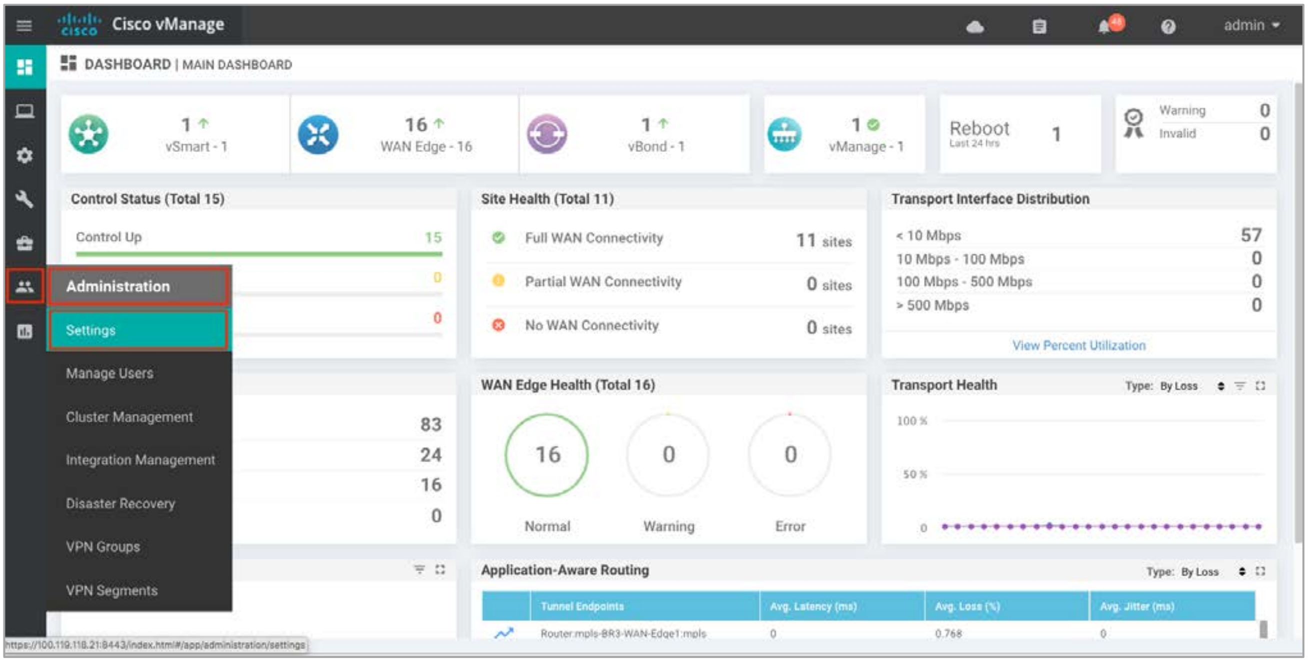
3) Create the Enterprise Firewall with App Aware and IPS Policy.

4) Attach the security policy to the device template.

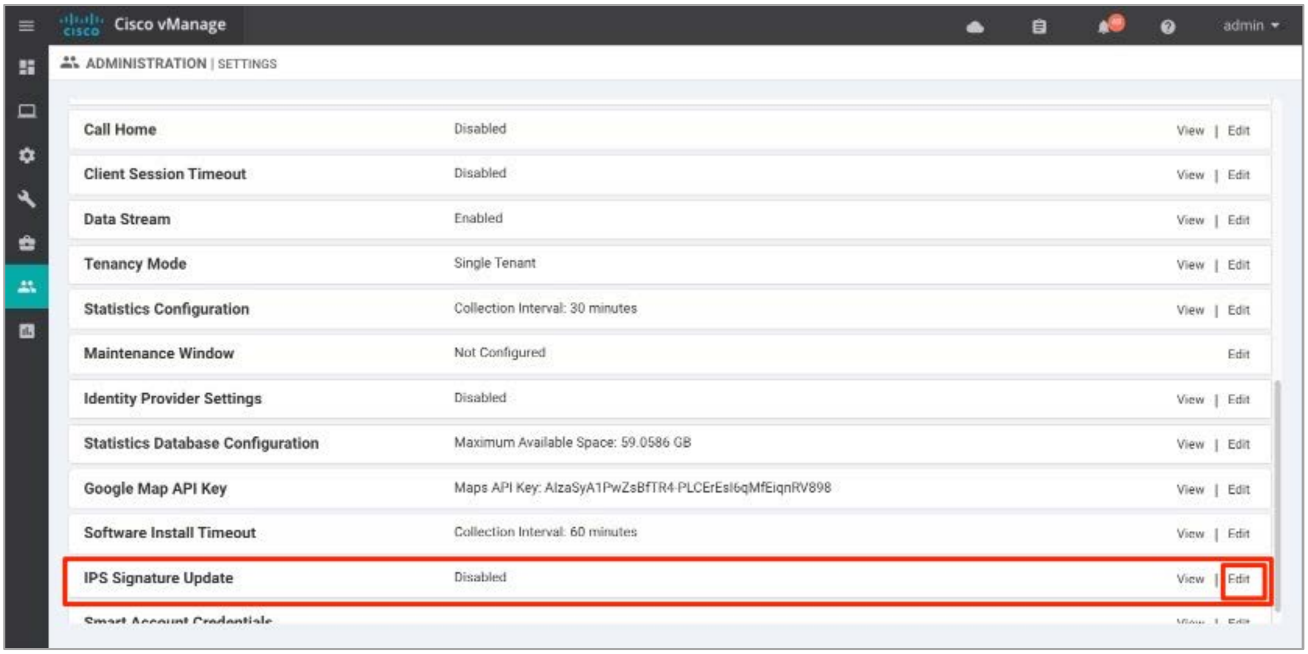
5) Attach the Security App Hosting Feature Template to the device template.

Process 1: IPS Signature Update

Step 1 To enable the automatic IPS signature update, navigate to **Administration** > **Settings** tab in the panel on the left side.



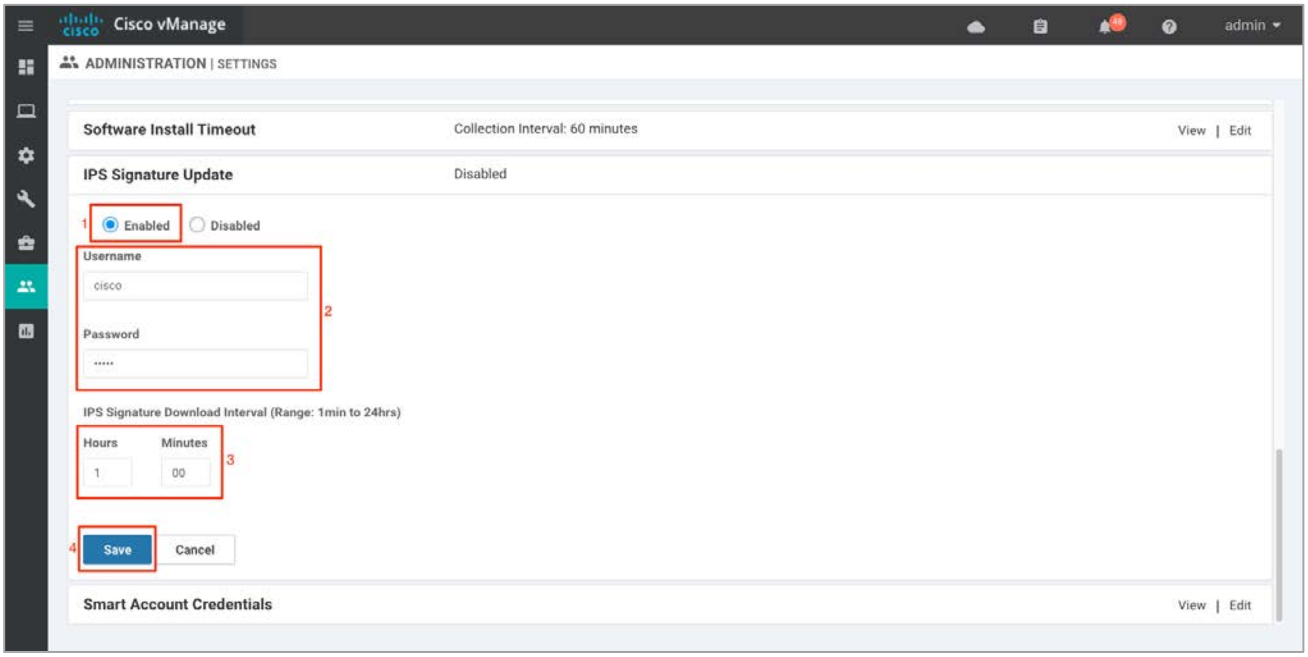
Step 2 Click **Edit** to enable signature update



Call Home	Disabled	View | Edit
Client Session Timeout	Disabled	View | Edit
Data Stream	Enabled	View | Edit
Tenancy Mode	Single Tenant	View | Edit
Statistics Configuration	Collection Interval: 30 minutes	View | Edit
Maintenance Window	Not Configured	Edit
Identity Provider Settings	Disabled	View | Edit
Statistics Database Configuration	Maximum Available Space: 59.0586 GB	View | Edit
Google Map API Key	Maps API Key: AIzaSyA1PwZsBfTR4-PLCErEsl6qMfEiqnRV898	View | Edit
Software Install Timeout	Collection Interval: 60 minutes	View | Edit
IPS Signature Update	Disabled	View | Edit
Smart Account Credentials		View | Edit

Step 3 Enter Cisco Username and Password, and set the **IPS Signature Download Interval** from 1 minute to 24 hours. In this guide, the time interval is set to 1 hour.

For successful signature update, make sure you can reach cloudsso2.cisco.com from vManage GUI – VPN 0 transport interface.



Software Install Timeout: Collection Interval: 60 minutes

IPS Signature Update: Disabled

● Enabled ○ Disabled

Username: cisco

Password: •••••

IPS Signature Download Interval (Range: 1min to 24hrs)

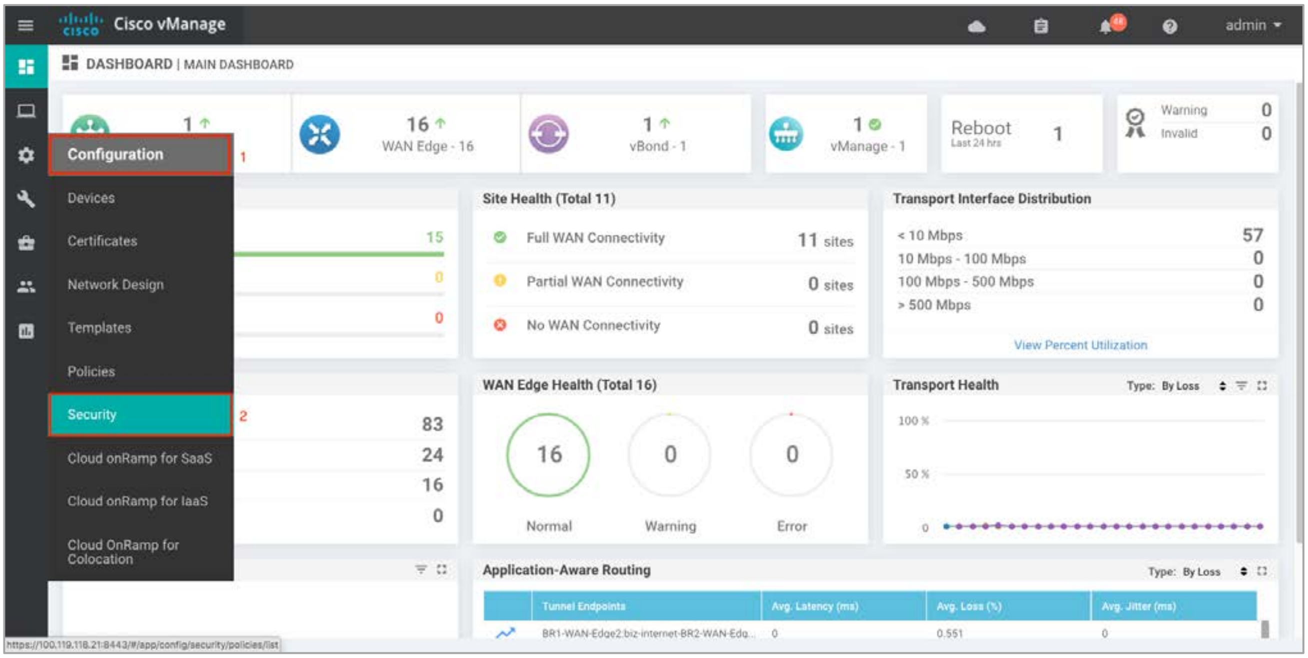
Hours: 1 Minutes: 00

Smart Account Credentials

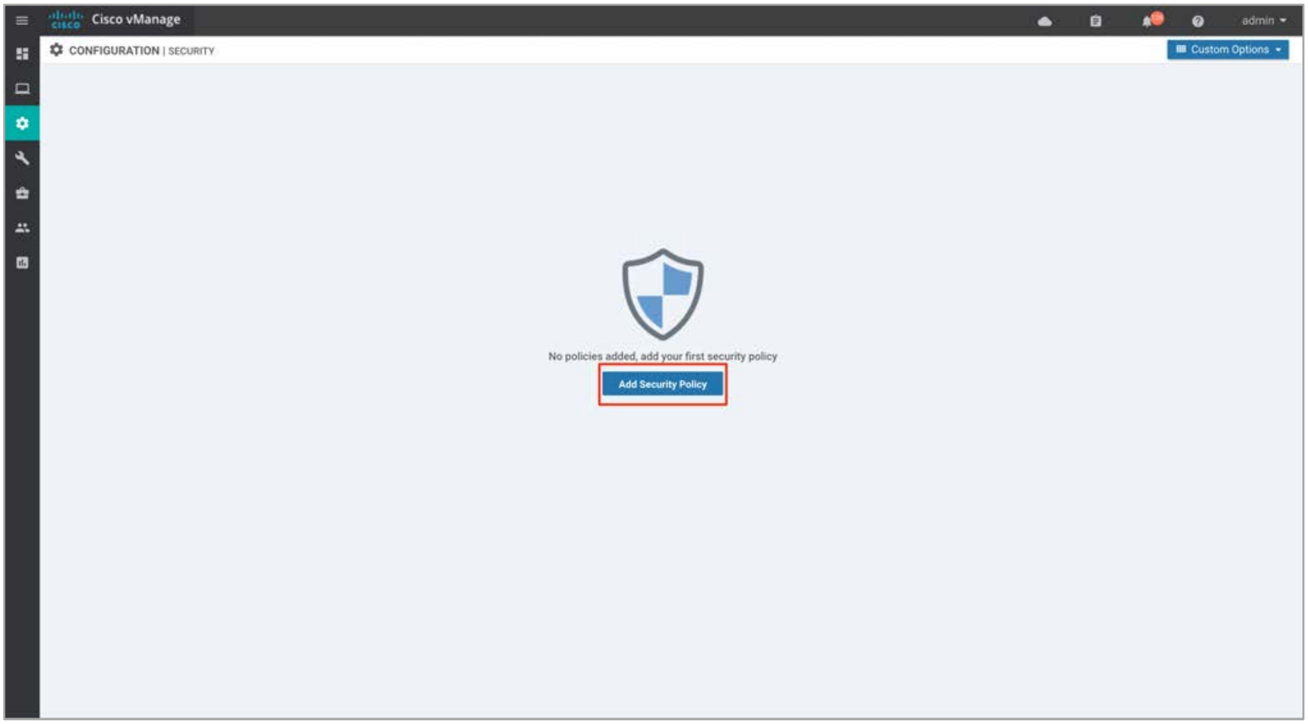
Technical Tip: If your IPS signature automatic update from the vManage NMS fails, the workaround is to enable manual signature updates from your WAN Edge device using the following CLI command `utd threat-inspection signature update server cisco username <username> password <password>.` However, before entering the CLI, make sure you either have reachability to CCO from VPN 0 or a policy to route traffic from VPN 65529 to a VPN ID that has access to the internet.

Process 2: Create Security Policy - Enterprise Firewall with App Awareness (Application Firewall) and IPS Policy.

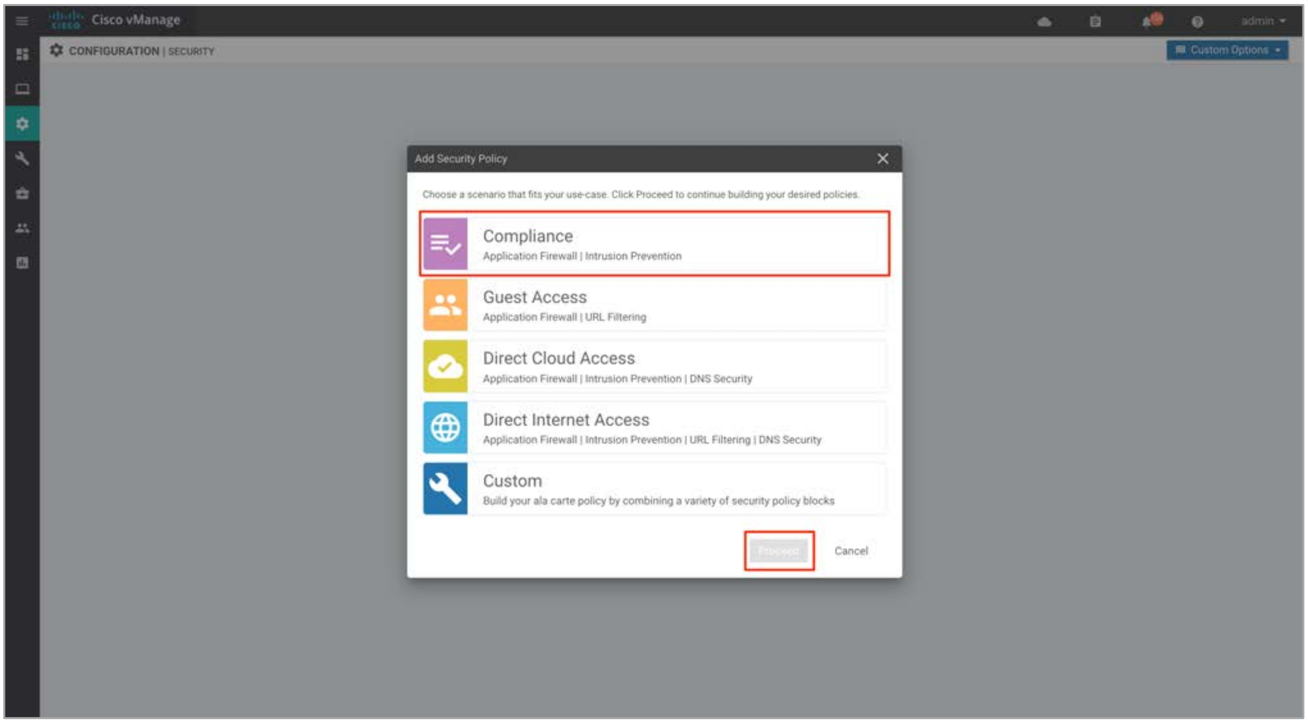
Step 4 In Cisco vManage NMS, navigate to **Configuration** > **Security** in the left side panel.



Step 5 Click **Add Security Policy** to create a new security policy.



Step 6 The security policy wizard displays a list of intent-based use cases. Choose **Compliance** and click **Proceed**.



Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

Compliance
Application Firewall | Intrusion Prevention

Guest Access
Application Firewall | URL Filtering

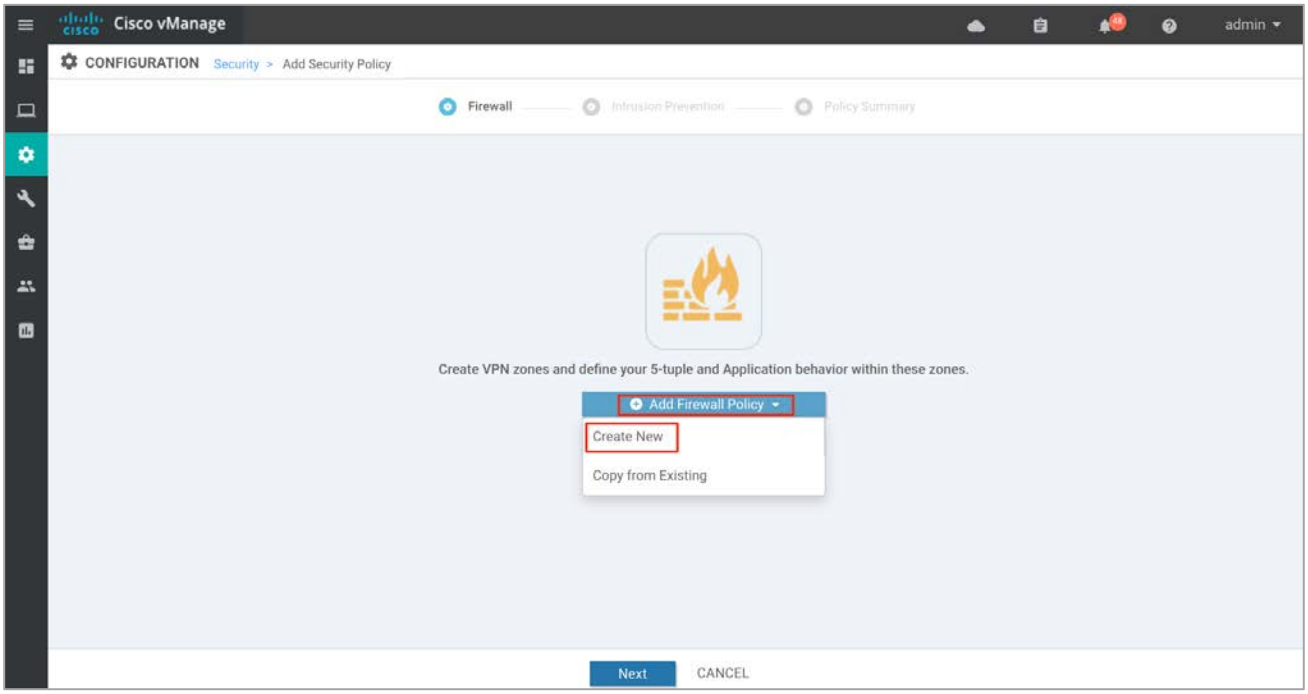
Direct Cloud Access
Application Firewall | Intrusion Prevention | DNS Security

Direct Internet Access
Application Firewall | Intrusion Prevention | URL Filtering | DNS Security

Custom
Build your ala carte policy by combining a variety of security policy blocks

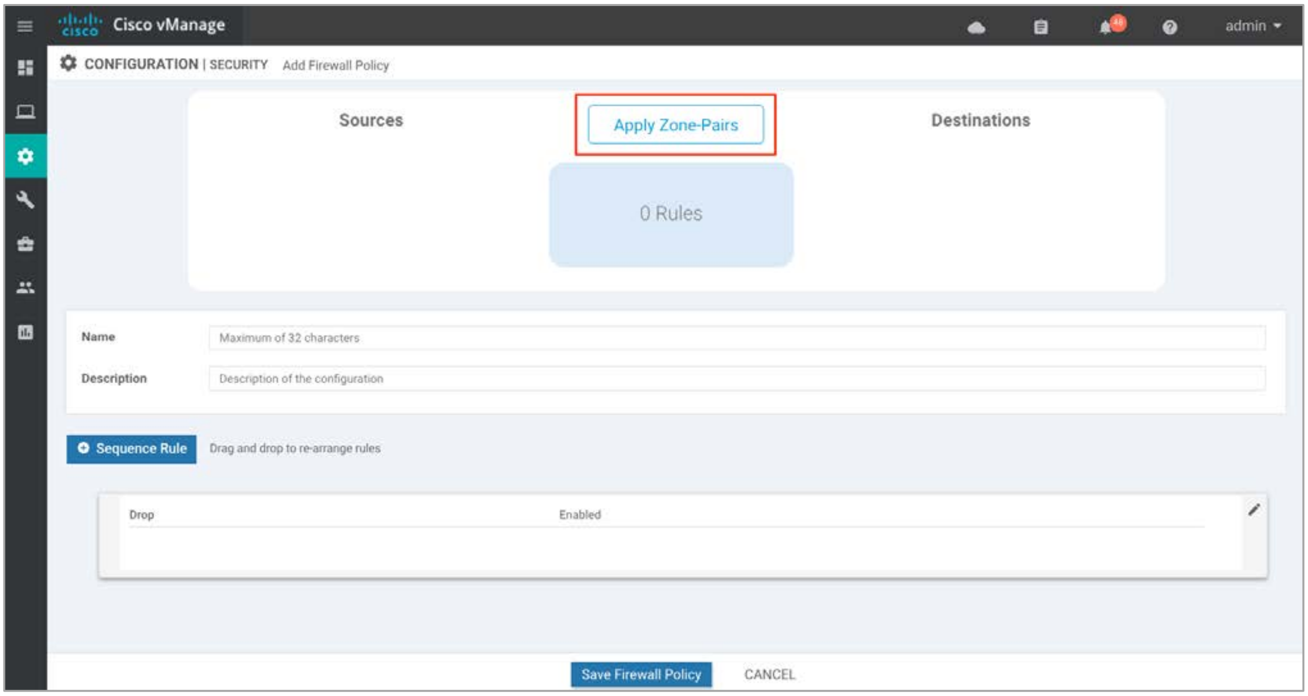
Process 2: Part 1 - Configure Enterprise Firewall with Application Aware

Step 7 Click **Add Firewall Policy** and create a new firewall policy by selecting **Create New**. However, if you have preconfigured a firewall policy, simply click **Copy from Existing**.



Create VPN zones and define your 5-tuple and Application behavior within these zones.

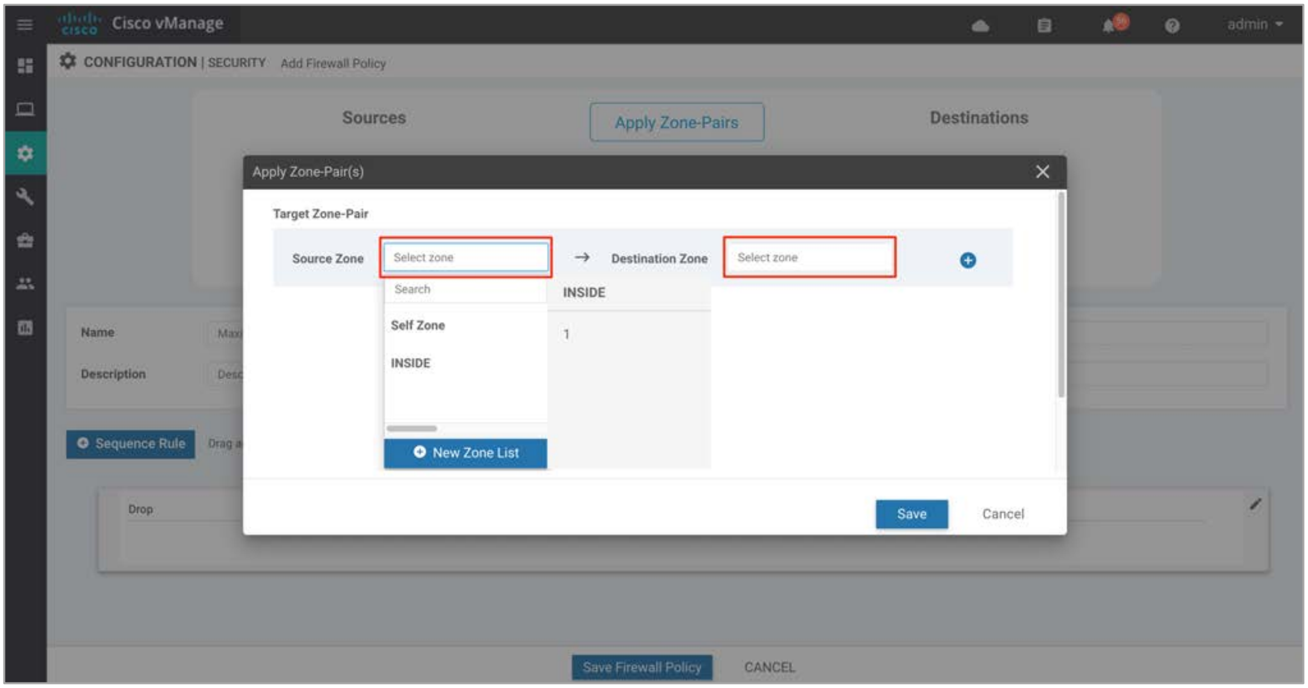
Step 8 Click **Apply Zone-Pairs** to create your zone-pairs.



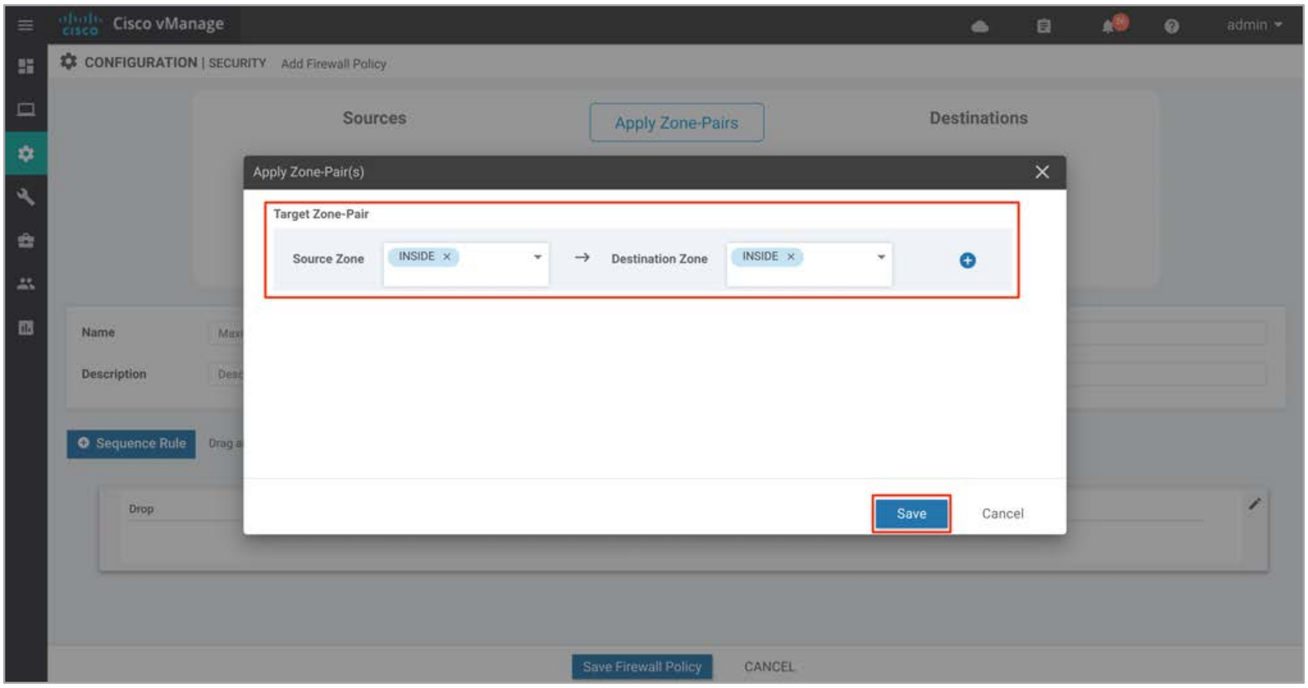
Name	Maximum of 32 characters
Description	Description of the configuration

Drop Enabled

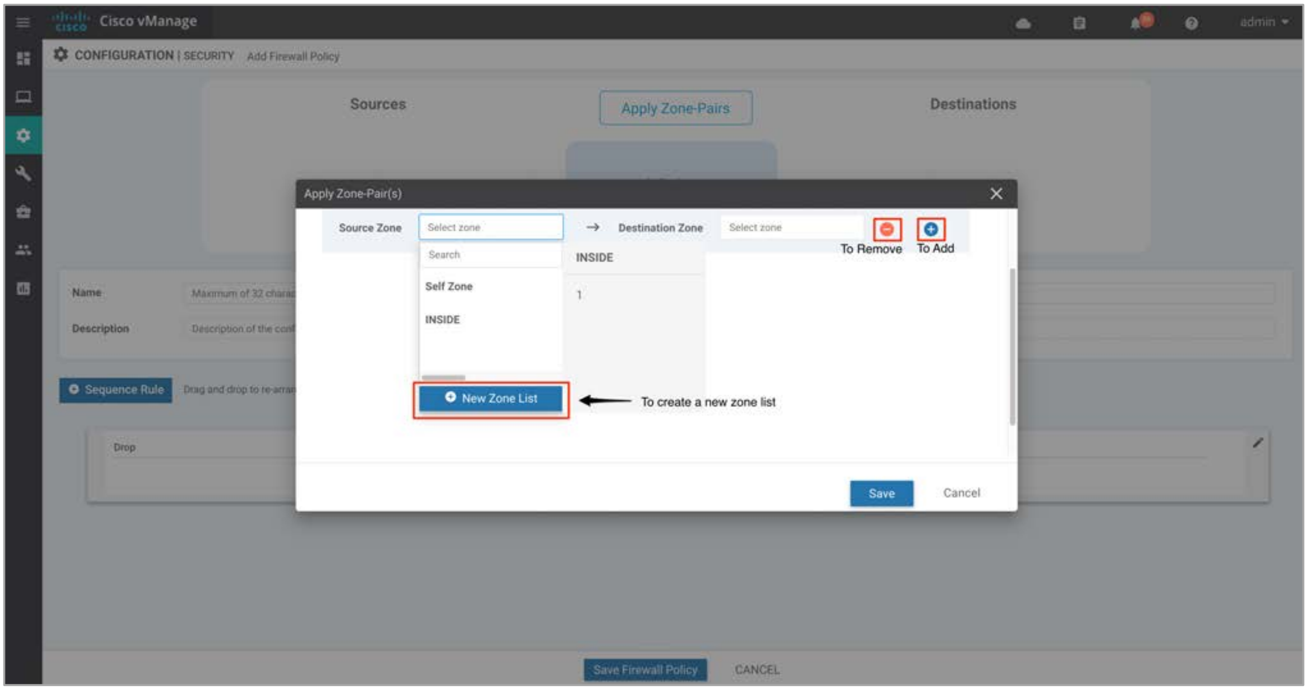
Step 9 Add the created zones to **Source Zone** and **Destination Zone**.



Step 10 After the zone pair is created, click **Save.**



Note: If you wish to create a new zone, click **New Zone List**, and to add additional zone-pair click on the (**+**) sign. To remove a zone pair, click the (**–**) sign. The following screenshot demonstrates this.



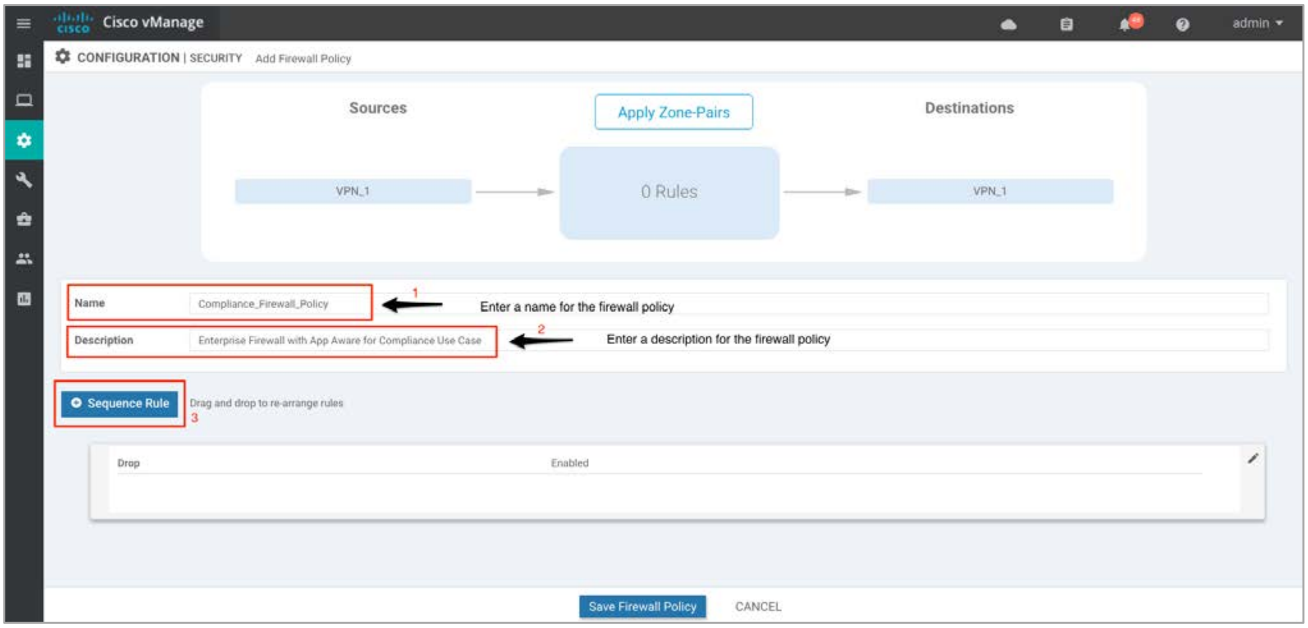
To Remove

To Add

To create a new zone list

Technical Tip: Starting from Cisco SD-WAN release 19.2 and IOS XE release 16.12, the Self Zone option is added in the Source Zone field. Self-zone is a self defined zone in the firewall that is associated with the VPN for punt and inject interface. It protects the packet going to or coming from the device. When the router infrastructure provides this VPN for the punt and inject interface, the VPN is bound to the self-zone and then a zone-pair is created with the self-zone. Subsequently, a policy can be specified to impose rules on the incoming and outgoing traffic from the device. A zone pair that includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the device.

Step 11 Enter a **Name** and **Description** in the field for the firewall policy. Next, click **Sequence Rule** to add policy rules.



Name Compliance_Firewall_Policy

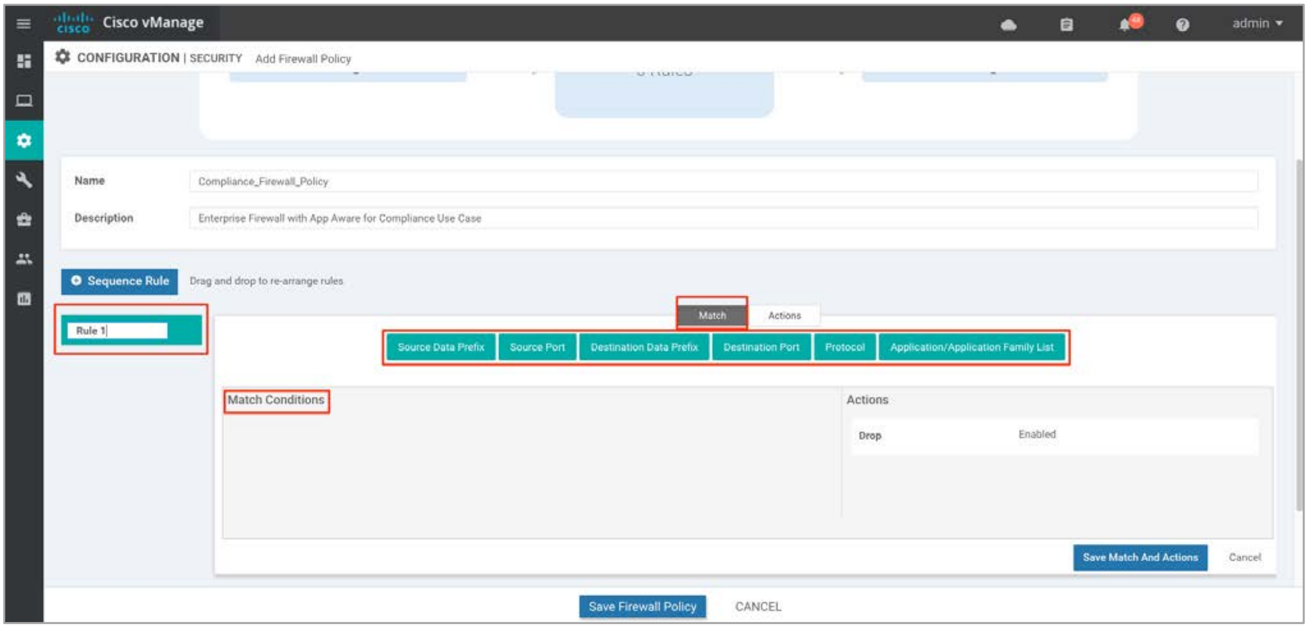
Description Enterprise Firewall with App Aware for Compliance Use Case

1 Enter a name for the firewall policy

2 Enter a description for the firewall policy

3

Step 12 The Match tab is selected by default. Click a match condition: **Source Data Prefix**, **Source Port**, **Destination Data Prefix, Destination Port**, **Protocol**, **Application/Application Family List**. You can select and configure more than one match conditions in a sequence.



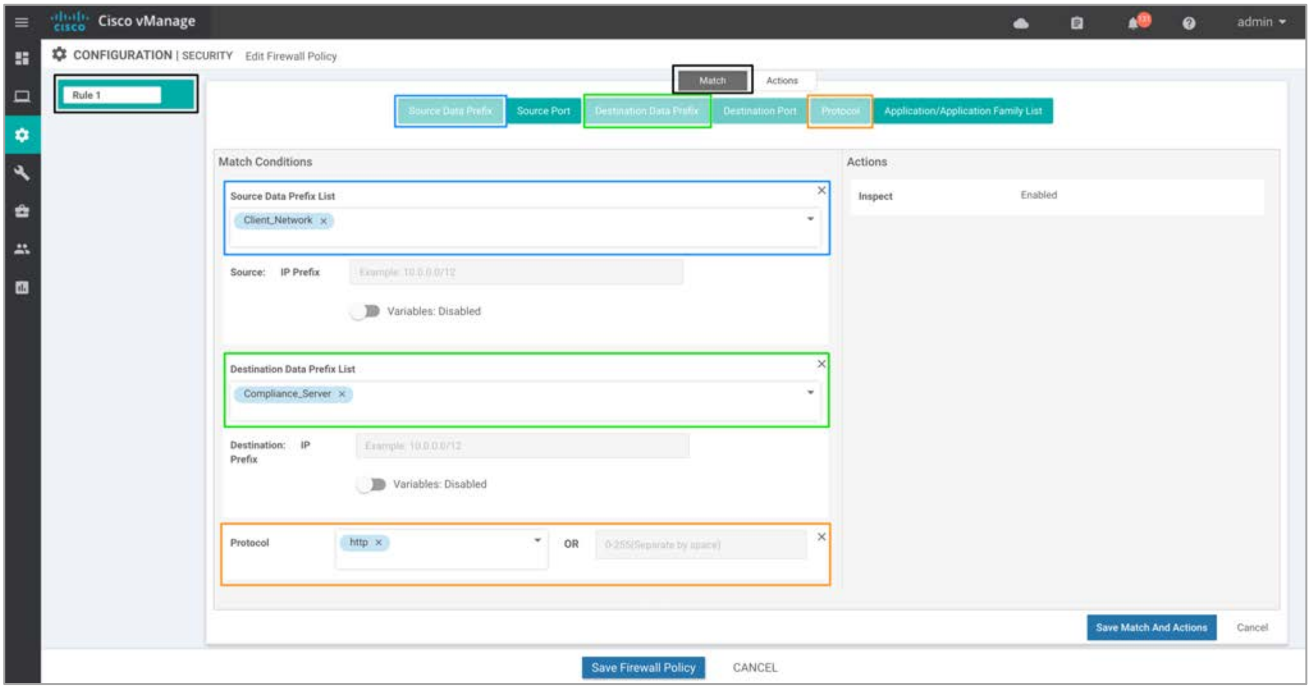
Name: Compliance_Firewall_Policy

Description: Enterprise Firewall with App Aware for Compliance Use Case

Rule 1

Drop: Enabled

Here’s an example of a sequence rule within the Enterprise Firewall with App Aware policy deployed.



Rule 1

Source Data Prefix List: Client_Network

Source: IP Prefix: Example: 10.0.0.0/12

Variables: Disabled

Destination Data Prefix List: Compliance_Server

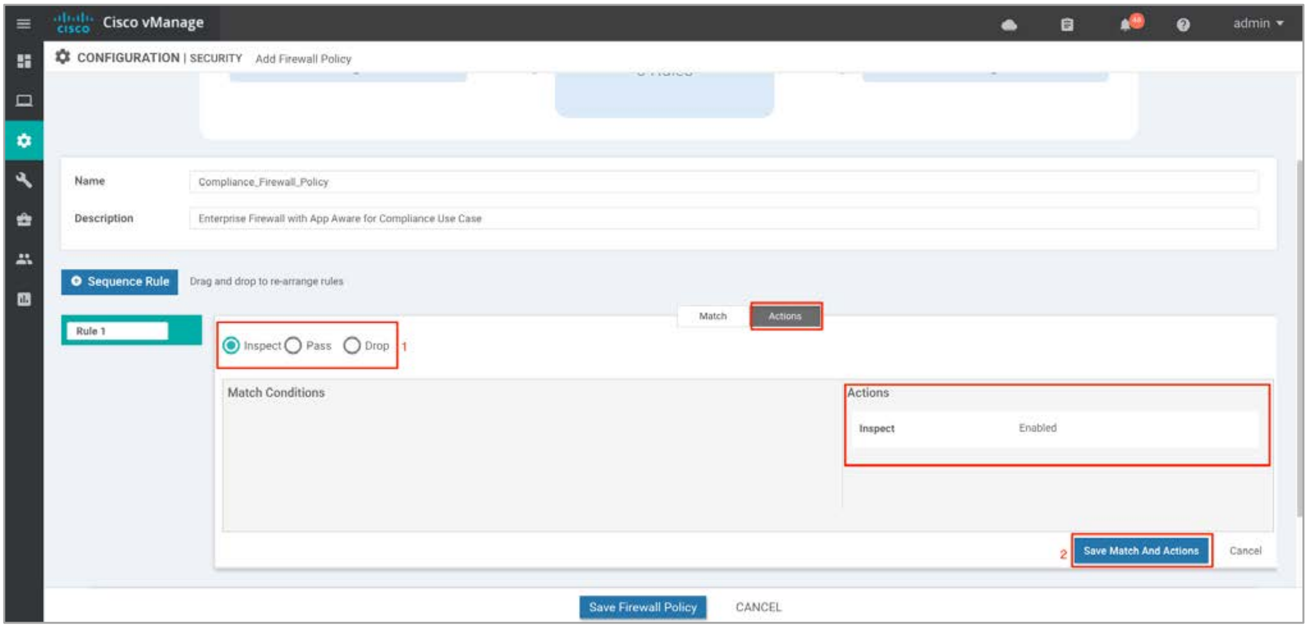
Destination: IP Prefix: Example: 10.0.0.0/12

Variables: Disabled

Protocol: http OR 0-255(Separate by space)

Inspect: Enabled

Step 13 Next, Click the **Actions** tab and enter the action or actions to take if the traffic matches. We have enabled **Inspect**.



Name: Compliance_Firewall_Policy

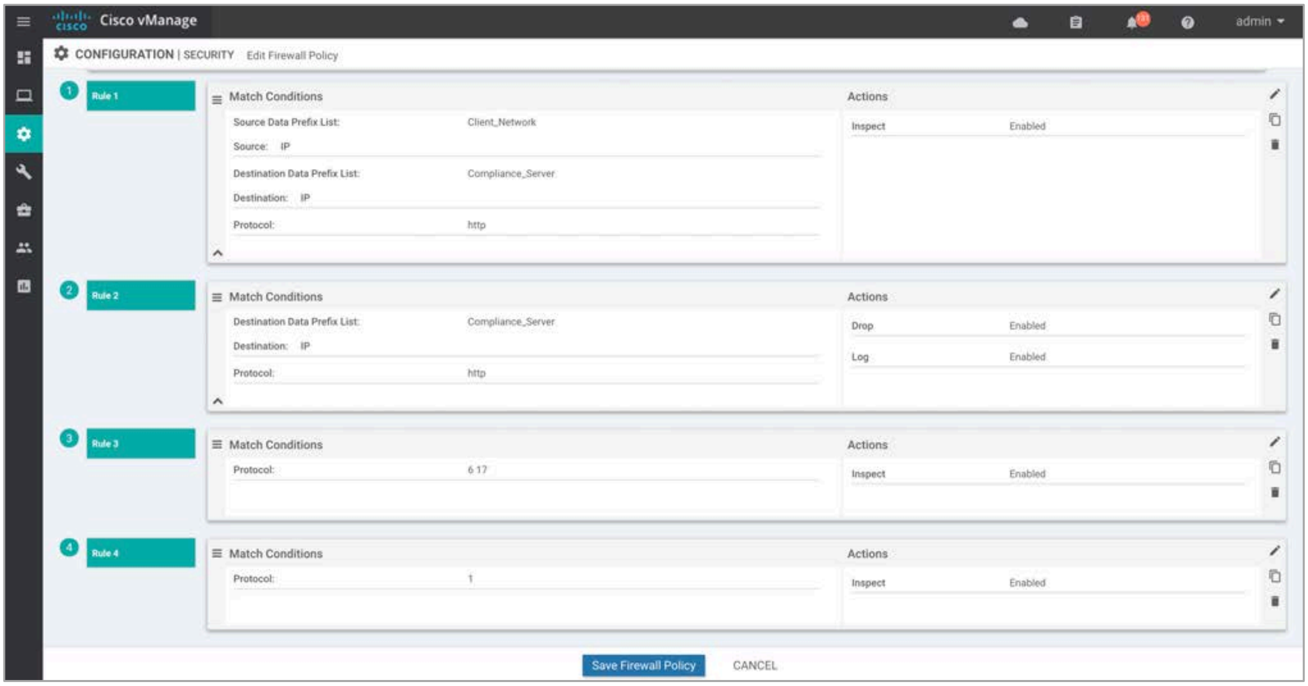
Description: Enterprise Firewall with App Aware for Compliance Use Case

● Inspect ○ Pass ○ Drop 1

Match Conditions

Actions	
Inspect	Enabled

Note that in this deployment, the following sequence rules were added.



1 Rule 1

Match Conditions		Actions	
Source Data Prefix List:	Client_Network	Inspect	Enabled
Source: IP			
Destination Data Prefix List:	Compliance_Server		
Destination: IP			
Protocol:	http		

2 Rule 2

Match Conditions		Actions	
Destination Data Prefix List:	Compliance_Server	Drop	Enabled
Destination: IP		Log	Enabled
Protocol:	http		

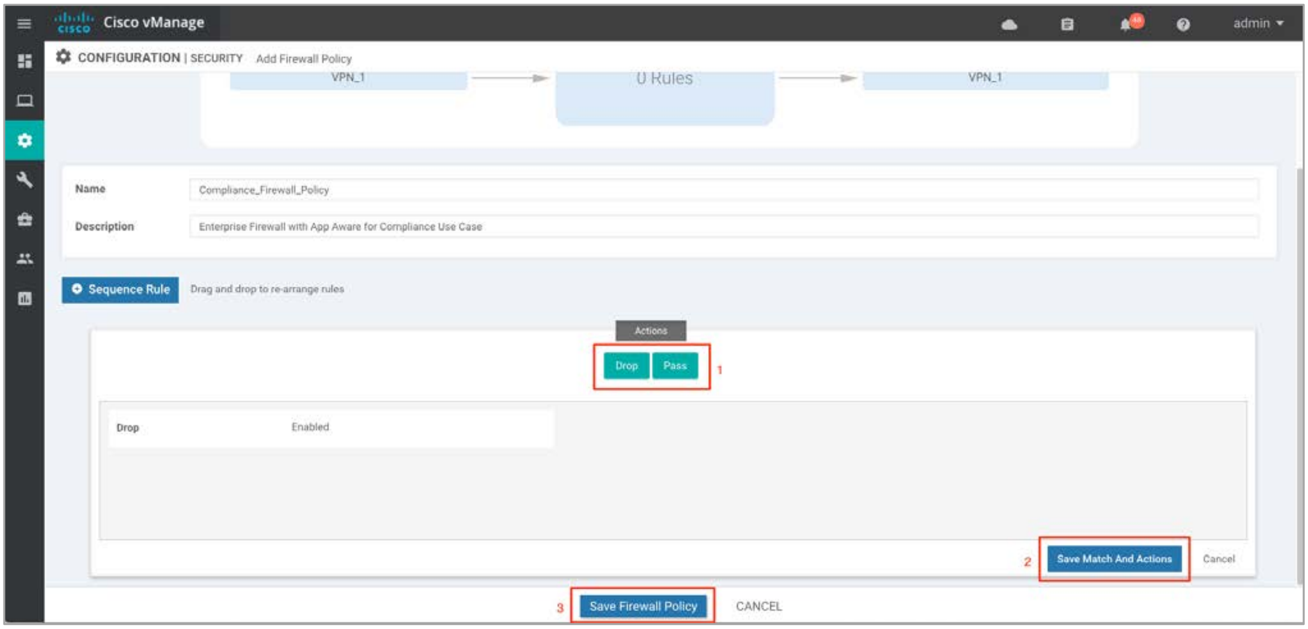
3 Rule 3

Match Conditions		Actions	
Protocol:	6 17	Inspect	Enabled

4 Rule 4

Match Conditions		Actions	
Protocol:	1	Inspect	Enabled

Step 14 (Optional) Edit the default action to **Drop** or **Pass** and click **Save Match And Actions** to save the changes. In this deployment, the default action is set to **Drop**. Finally, save the firewall policy.



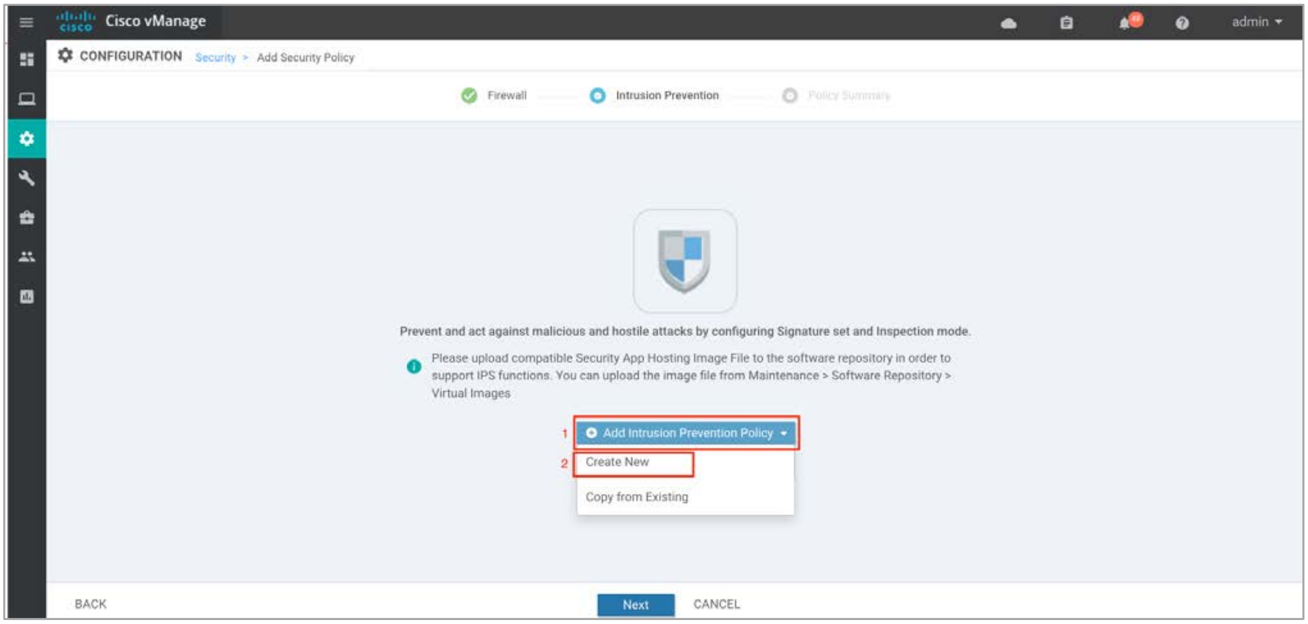
Name: Compliance_Firewall_Policy

Description: Enterprise Firewall with App Aware for Compliance Use Case

Drop: Enabled

Process 2: Part 2 - Configure Intrusion Prevention Policy

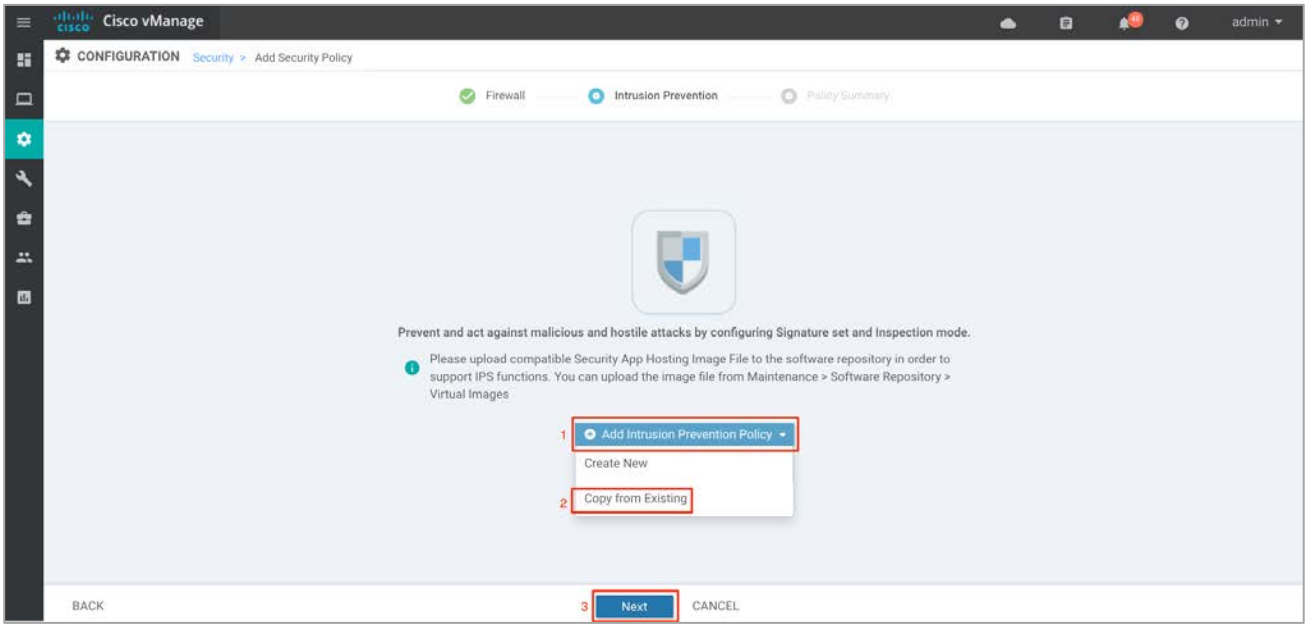
Step 15 Next, click **Add Intrusion Prevention Policy** to enable Snort IPS and select **Create New** to create a new IPS policy.



Prevent and act against malicious and hostile attacks by configuring Signature set and Inspection mode.

Please upload compatible Security App Hosting Image File to the software repository in order to support IPS functions. You can upload the image file from Maintenance > Software Repository > Virtual Images

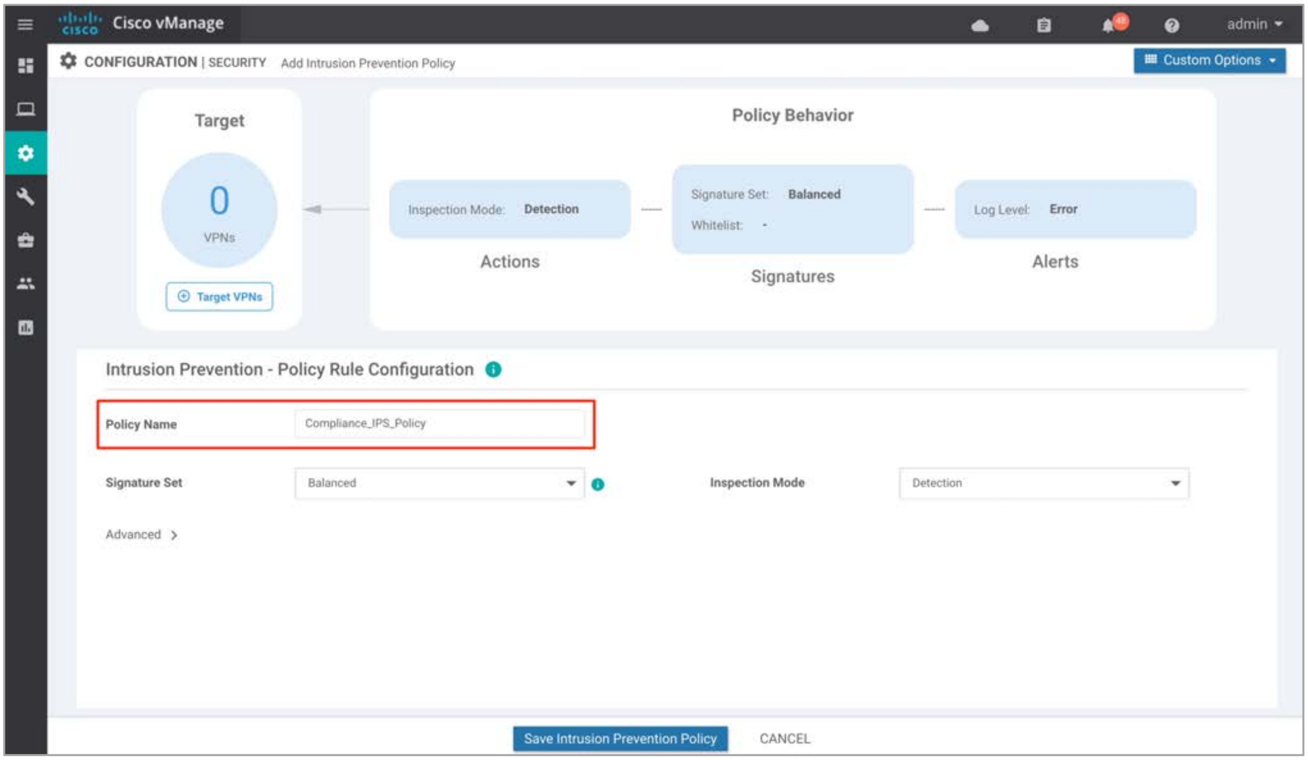
If you wish to export an existing policy, click **Copy from Existing**, fill in the policy details and click **Next.**



Prevent and act against malicious and hostile attacks by configuring Signature set and Inspection mode.

Please upload compatible Security App Hosting Image File to the software repository in order to support IPS functions. You can upload the image file from Maintenance > Software Repository > Virtual Images

Step 16 Enter a policy name in the **Policy Name** field.



Inspection Mode: Detection

Signature Set: Balanced

Whitelist: -

Log Level: Error

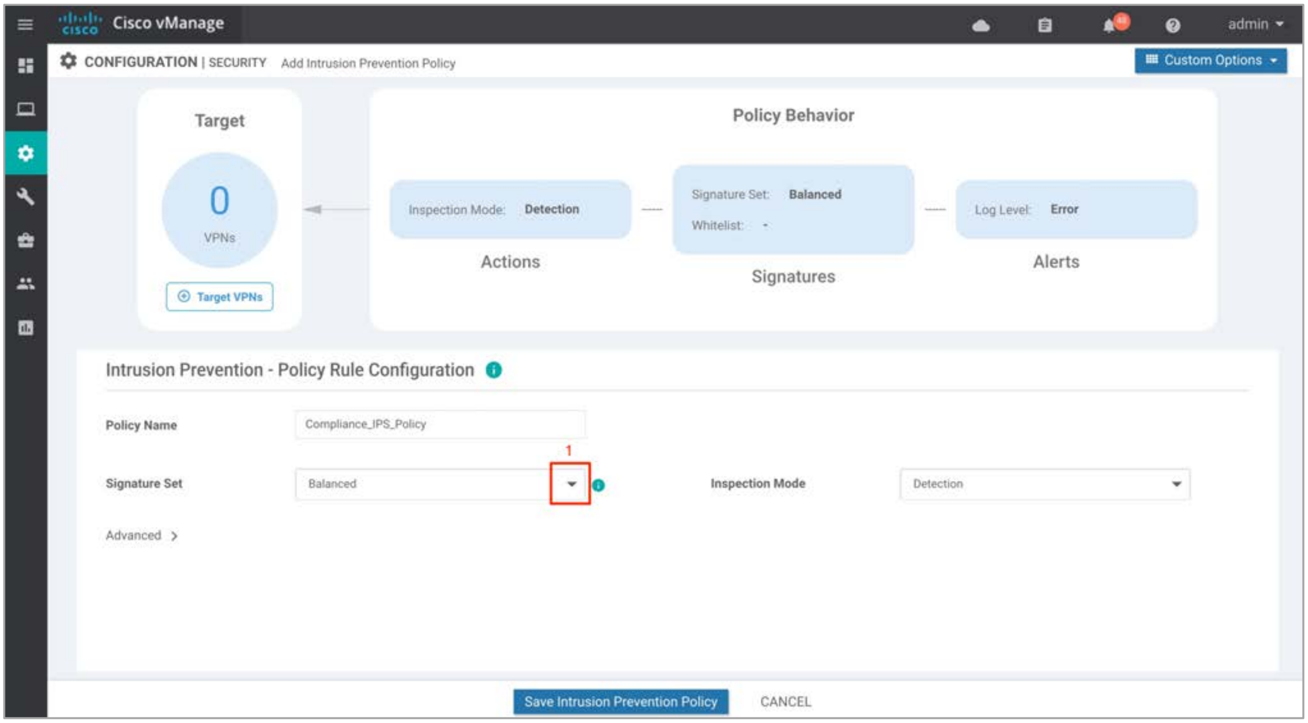
Intrusion Prevention - Policy Rule Configuration

Policy Name: Compliance_IPS_Policy

Signature Set: Balanced

Inspection Mode: Detection

Step 17 Select a signature set that defines the rules for evaluating traffic from the **Signature Set** drop-down menu.



Inspection Mode: Detection

Signature Set: Balanced

Whitelist: -

Log Level: Error

Policy Name: Compliance_IPS_Policy

Signature Set: Balanced

Inspection Mode: Detection

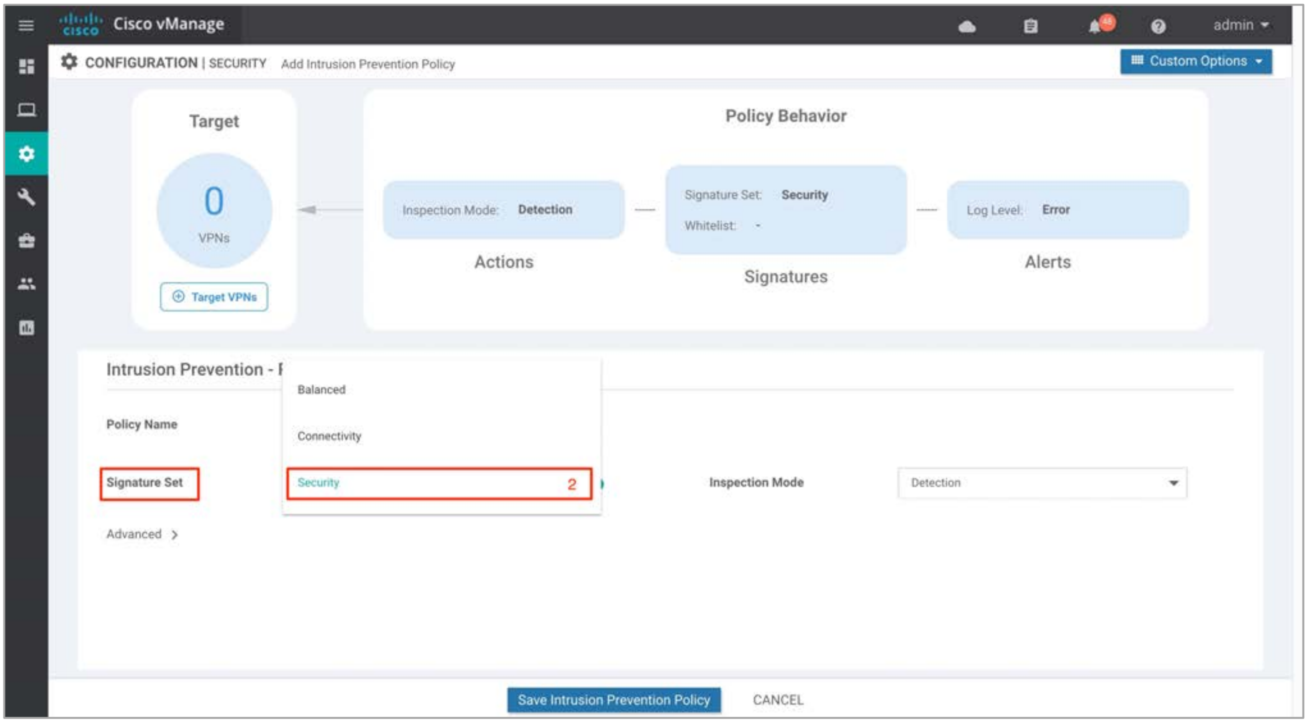
Step 18 In the **Signature Set field**, choose the desired signature set:

Connectivity: Less restrictive with better performance as there are fewer rules attached to this signature level.

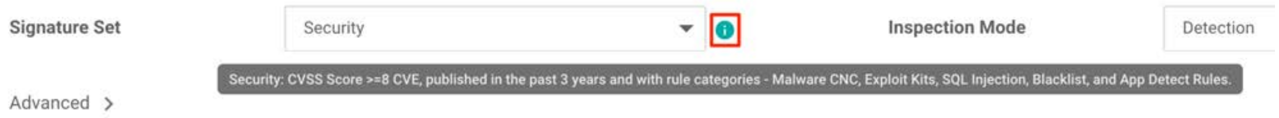
Balanced: Designed to provide protection without a significant effect on system performance.

Security: With more added rules, this signature level offers more protection, but overall performance of your WAN edge device is reduced.

The signature set represents the level of inspection applied to the traffic (that is the number of signatures) with Connectivity having the least number of signatures, Security having the most number of signatures, and Balanced striking a ‘balance’ in terms of the number of . For more information on Signature Set refer to the Design section.

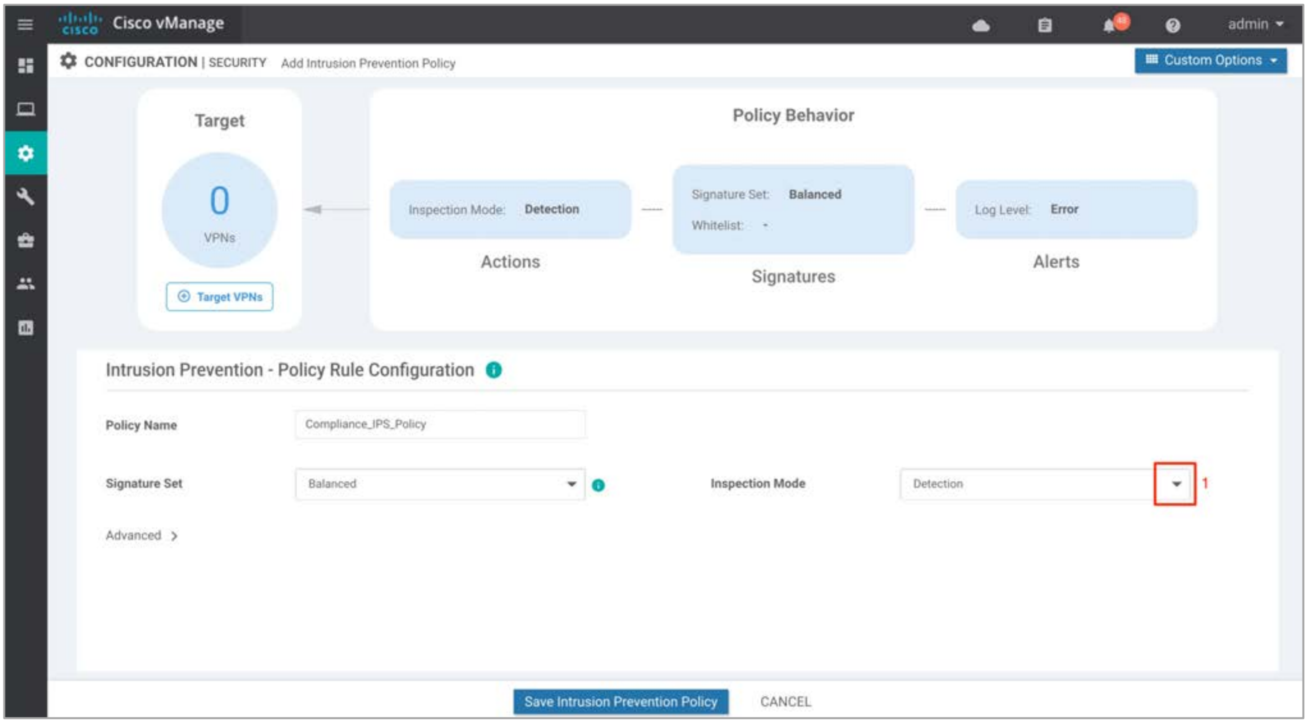


Technical Tip: To understand the CVSS score of a signature set, hover over the **!** sign on the right side of the tab.



Security: CVSS Score >=8 CVE, published in the past 3 years and with rule categories - Malware CNC, Exploit Kits, SQL Injection, Blacklist, and App Detect Rules.

Step 19 Select the mode of operation from the **Inspection Mode** drop-down menu.

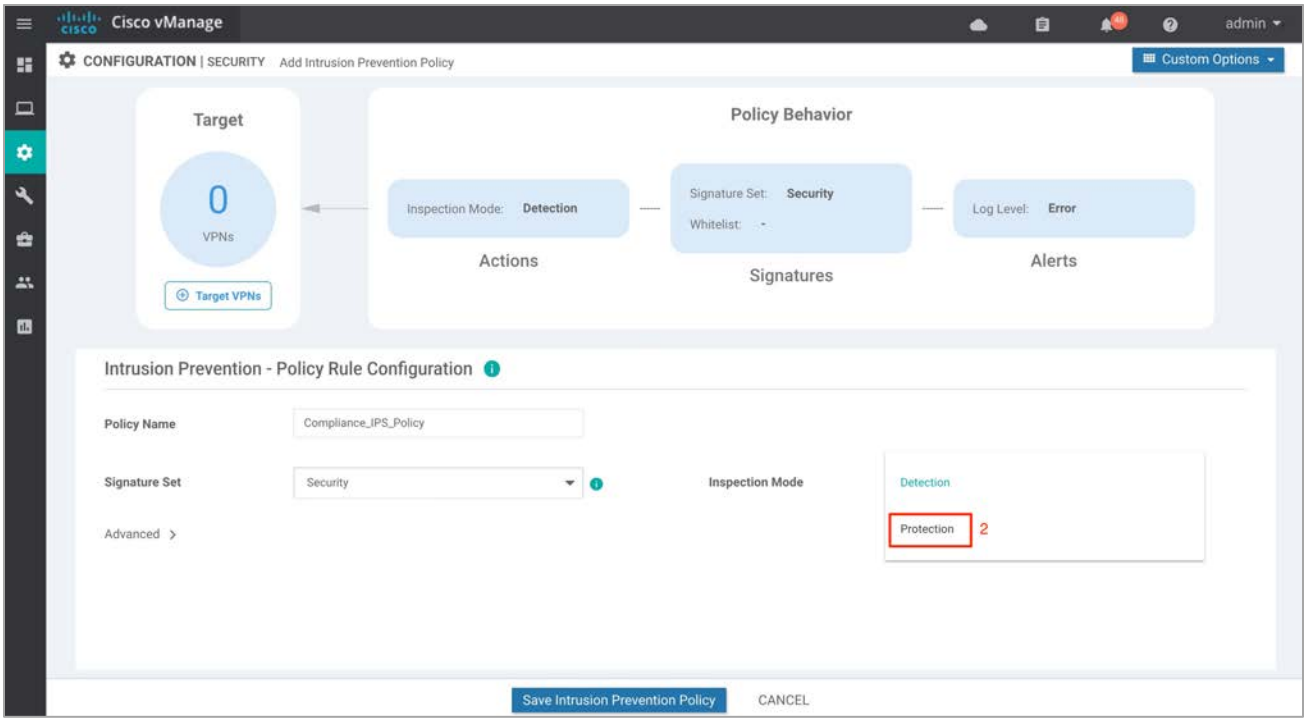


Step 20 The following options display:

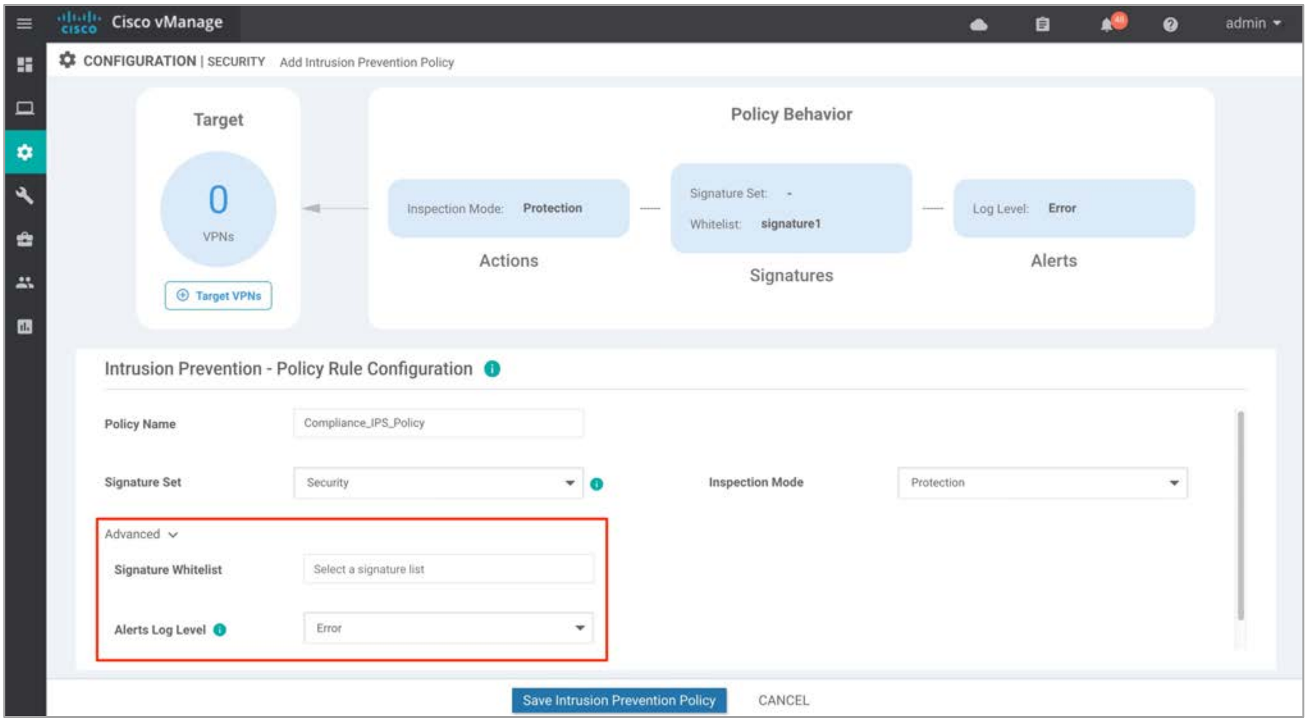
Detection: Choose this option for intrusion detection mode. (Default)

Protection: Choose this option for intrusion protection mode.

In this deployment guide, the inspection mode is set to **Protection.**



Step 21 Within the **Advanced** tab, you can choose to whitelist signatures in the **Signature Whitelist** field and set **Alerts Log Level**.


Cisco vManage
admin
CONFIGURATION | SECURITY Add Intrusion Prevention Policy
Target
0
VPNs
Target VPNs
Policy Behavior
Actions
Signatures
Alerts
Save Intrusion Prevention Policy
CANCEL

Inspection Mode: Protection

Signature Set: -

Whitelist: signature1

Log Level: Error

Intrusion Prevention - Policy Rule Configuration

Policy Name: Compliance_IPS_Policy

Signature Set: Security

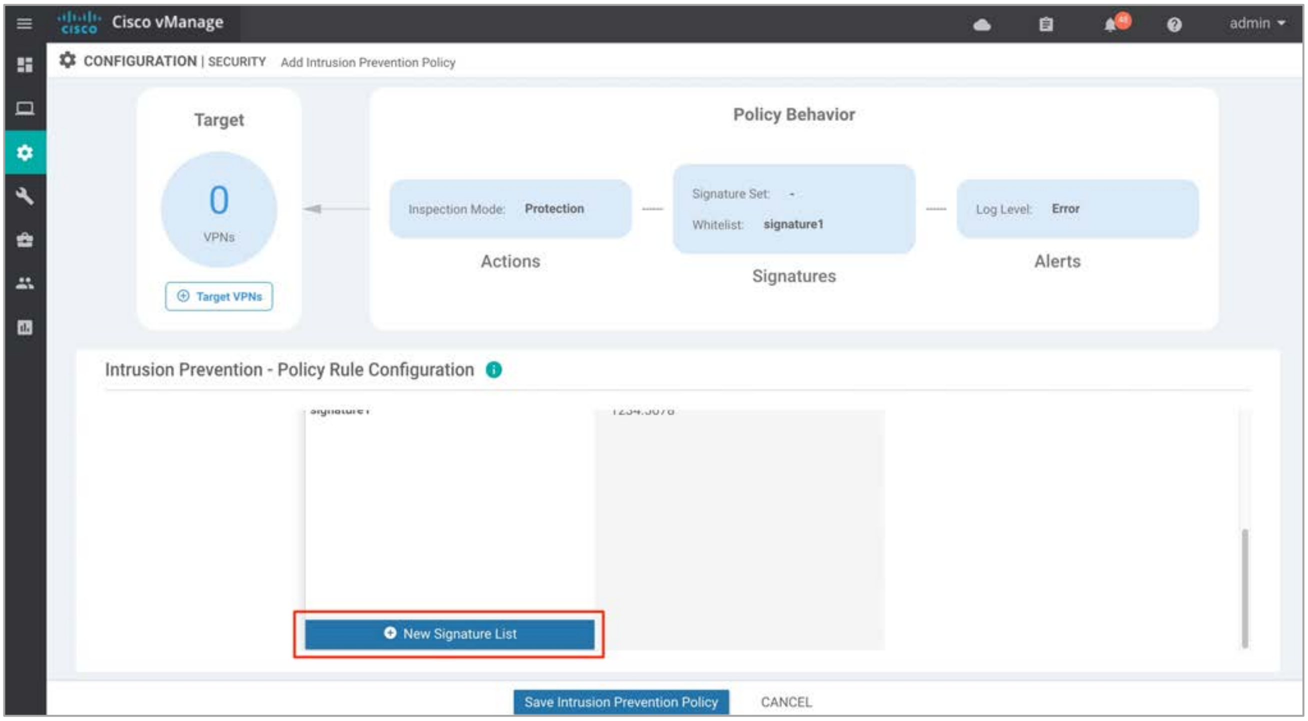
Inspection Mode: Protection

Advanced

Signature Whitelist: Select a signature list

Alerts Log Level: Error

Step 22 To create a new signature list, click **Signature Whitelist** and choose **New Signature List** in the drop-down menu.



Inspection Mode: Protection

Signature Set: -

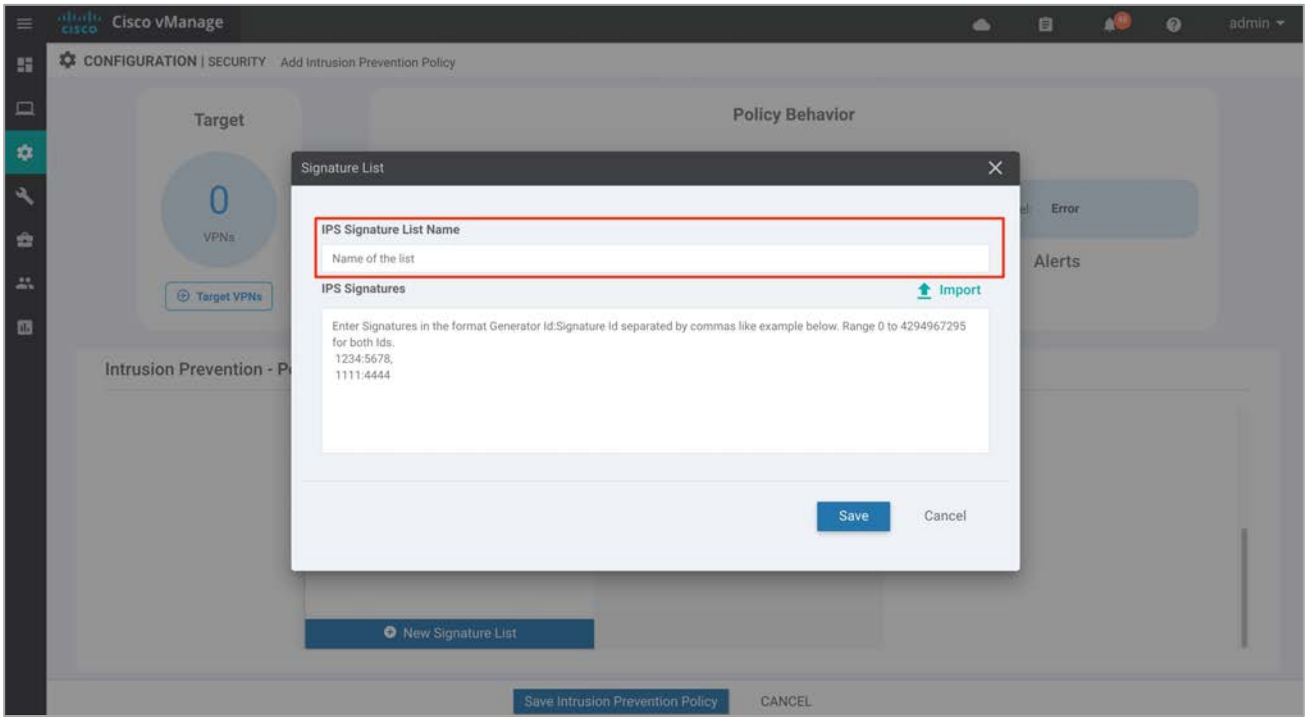
Whitelist: signature1

Log Level: Error

Intrusion Prevention - Policy Rule Configuration

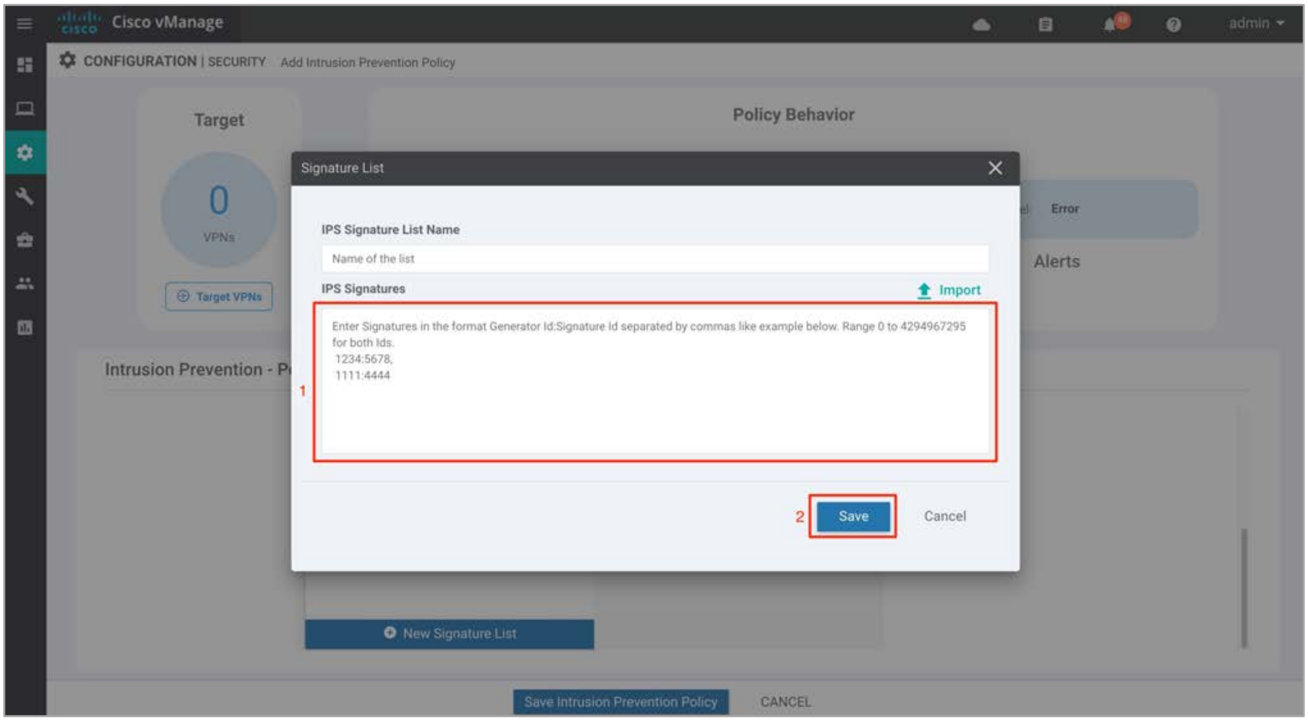
signature1 12345678

Step 23 In this IPS Signature List Name field, enter a name consisting of up to 32 characters (letters, numbers, hyphens and underscores only).



Enter Signatures in the format Generator Id:Signature Id separated by commas like example below. Range 0 to 4294967295 for both Ids.
1234:5678,
1111:4444

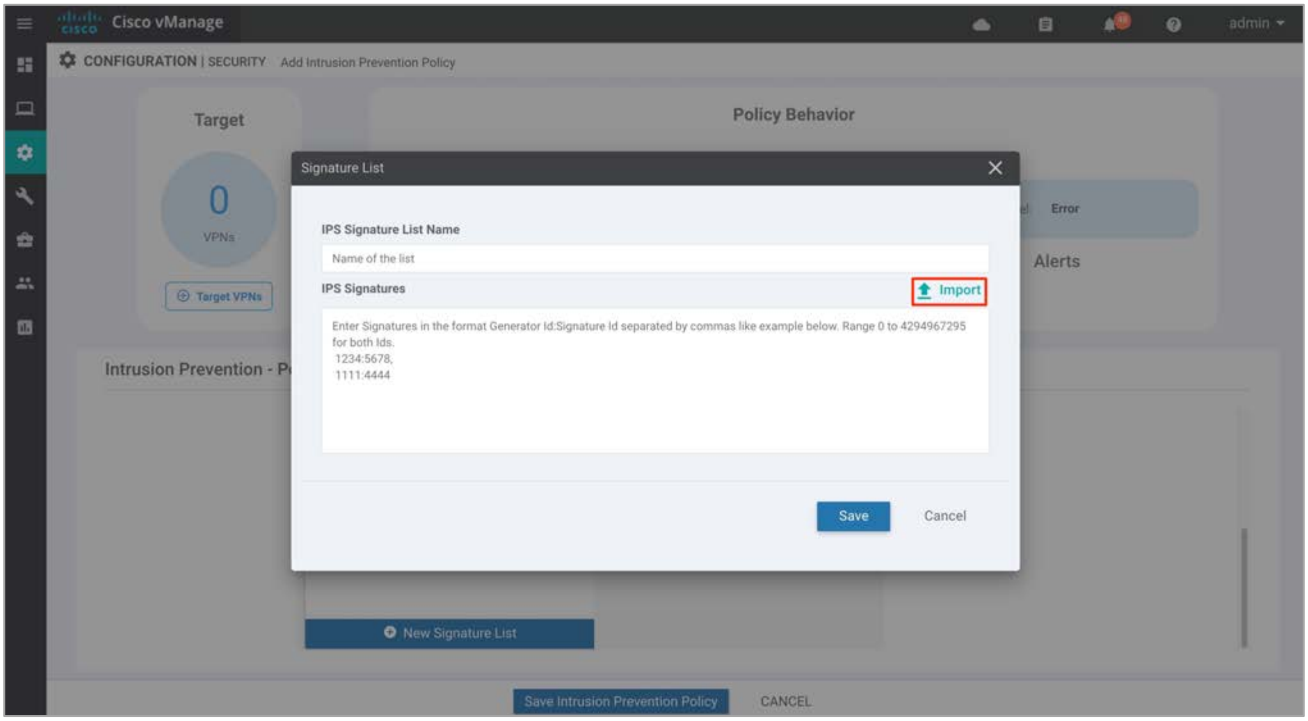
Step 24 Within the IPS Signature field, enter signatures in the following format. Generator ID:Signature ID, separated with commas and click **Save** to save the configured signature list.



Enter Signatures in the format Generator Id:Signature Id separated by commas like example below. Range 0 to 4294967295 for both Ids.
1234:5678,
1111:4444

In this deployment guide, no signatures have been whitelisted.

Note: You can also choose to import whitelisted signatures by clicking the **Import** button to retrieve a file from an accessible storage.



Signature List

IPS Signature List Name

Name of the list

IPS Signatures — Import

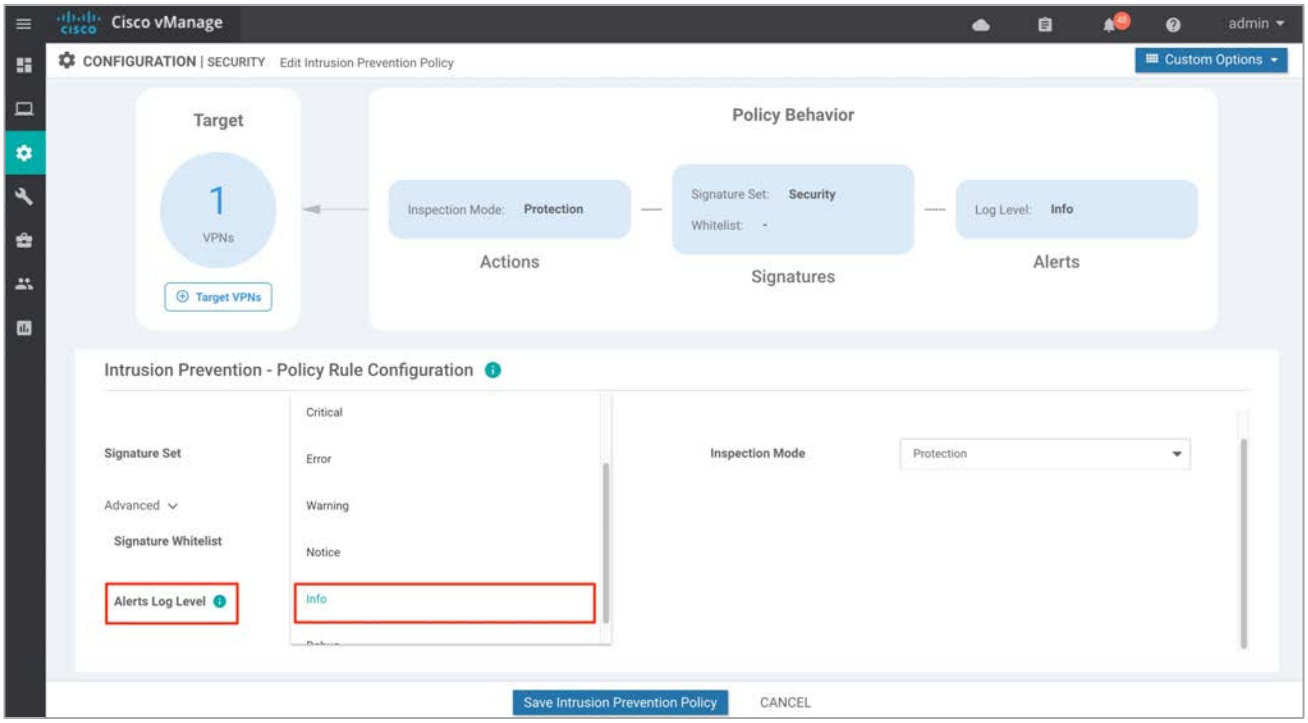
Enter Signatures in the format Generator Id:Signature Id separated by commas like example below. Range 0 to 4294967295 for both Ids.
1234:5678,
1111:4444

Save — Cancel

Technical Tip: You can also create and manage the IPS signature whitelist by navigating to **Lists** from custom options available in the Security policy GUI.

Step 25 Select an alert level for syslogs from the **Alert Log Level** drop-down menu. The drop-down menu has the following options: Emergency (Severity = 0), Alert (Severity = 1), Critical (Severity = 2), Error (Severity = 3), Warning (Severity = 4), Notice (Severity = 5), Info (Severity = 6), Debug (Severity = 7) (Severity/Priority). The alerts are exported as syslog messages.

In this guide, the **Alert Log Level** is set to **Info**.



Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Info

Intrusion Prevention - Policy Rule Configuration

Signature Set

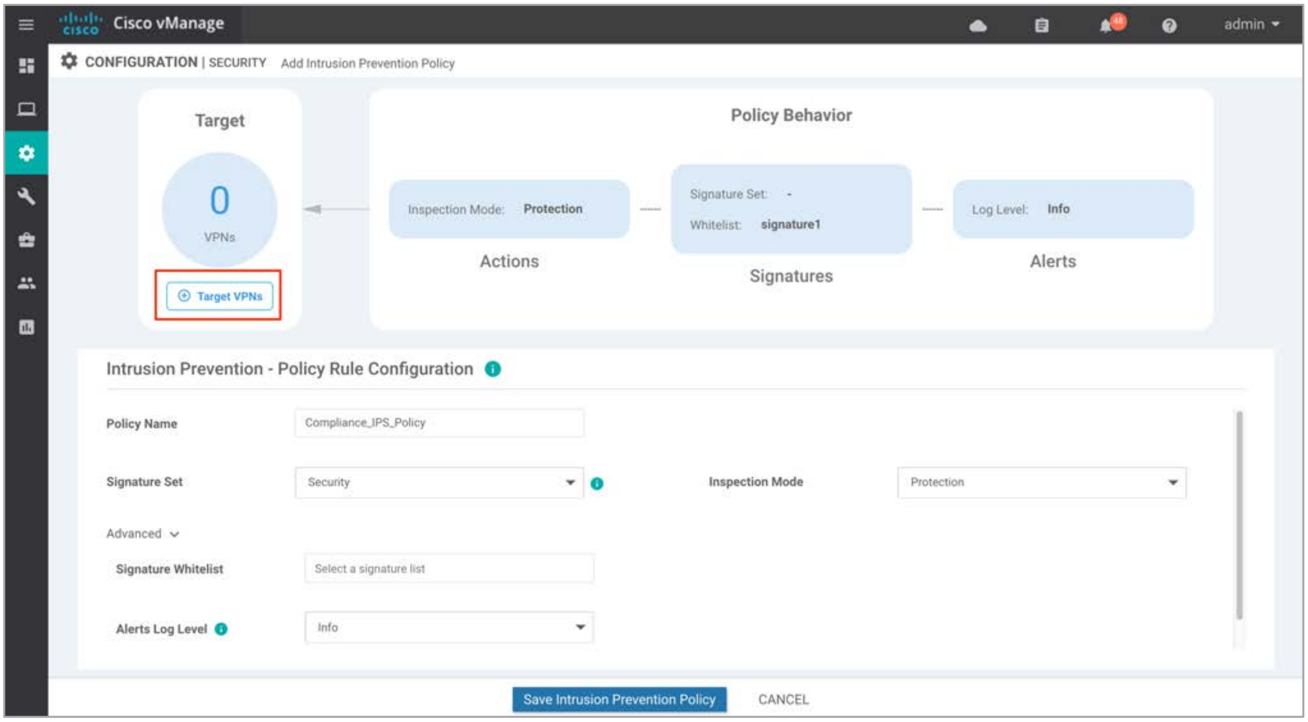
Advanced

Signature Whitelist

Alerts Log Level: Info

Inspection Mode: Protection

Step 26 Next, set the target vpns**.** Click **Target VPNs** to add VPNs in the Target VPNs wizard.


Cisco vManage
admin
CONFIGURATION | SECURITY Add Intrusion Prevention Policy
Target
0
VPNs
Target VPNs
Policy Behavior
Actions
Signatures
Alerts
Save Intrusion Prevention Policy
CANCEL

Inspection Mode: Protection

Signature Set: -

Whitelist: signature1

Log Level: Info

Intrusion Prevention - Policy Rule Configuration

Policy Name: Compliance_IPS_Policy

Signature Set: Security

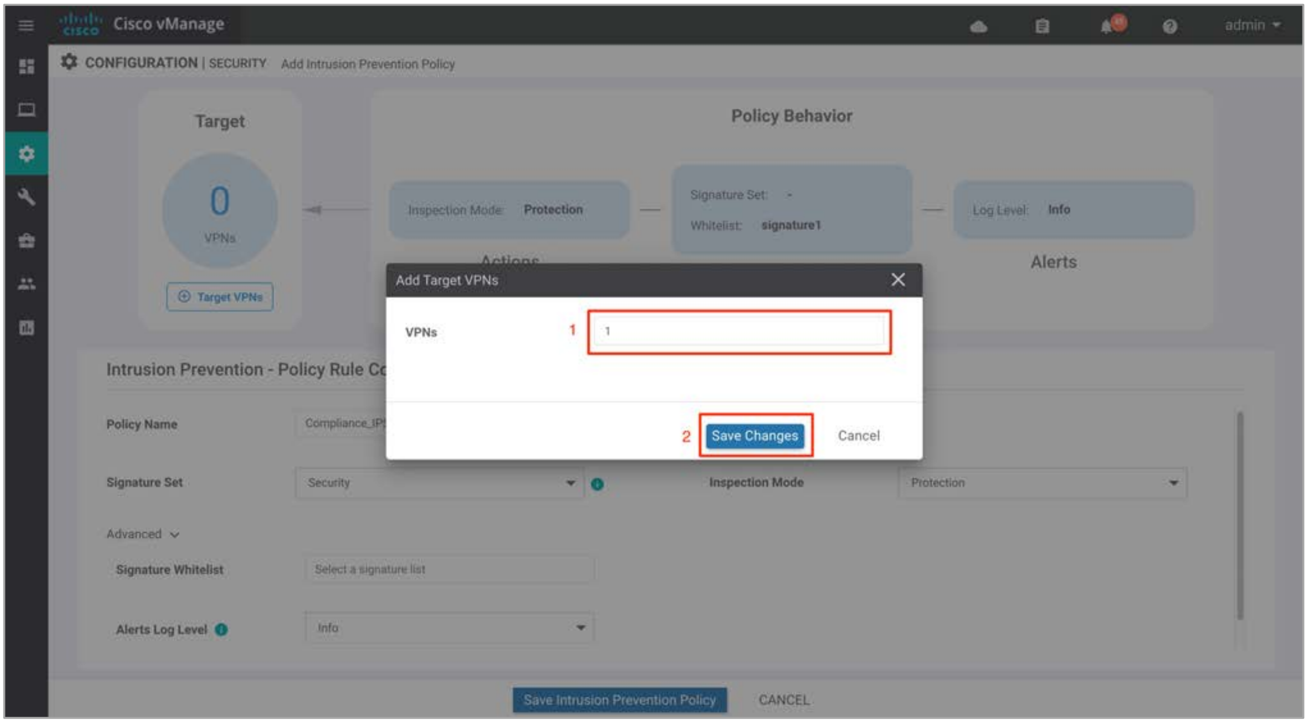
Inspection Mode: Protection

Advanced

Signature Whitelist: Select a signature list

Alerts Log Level: Info

Step 27 In the tab on the right, enter the VPN number next to **VPNs**. The VPN label added in the tab is VPN 1. However, if you wish to add more VPNs, separate each VPN with commas. Click **Save Changes**.



Cisco vManage
admin
CONFIGURATION | SECURITY Add Intrusion Prevention Policy
Target
0
VPNs
Target VPNs
Policy Behavior
Actions
Alerts
Add Target VPNs
1
2
Save Changes
Cancel
Intrusion Prevention - Policy Rule Co
Advanced
Save Intrusion Prevention Policy
CANCEL

Inspection Mode: Protection

Signature Set: -

Whitelist: signature1

Log Level: Info

VPNs: 1

Policy Name: Compliance_IP

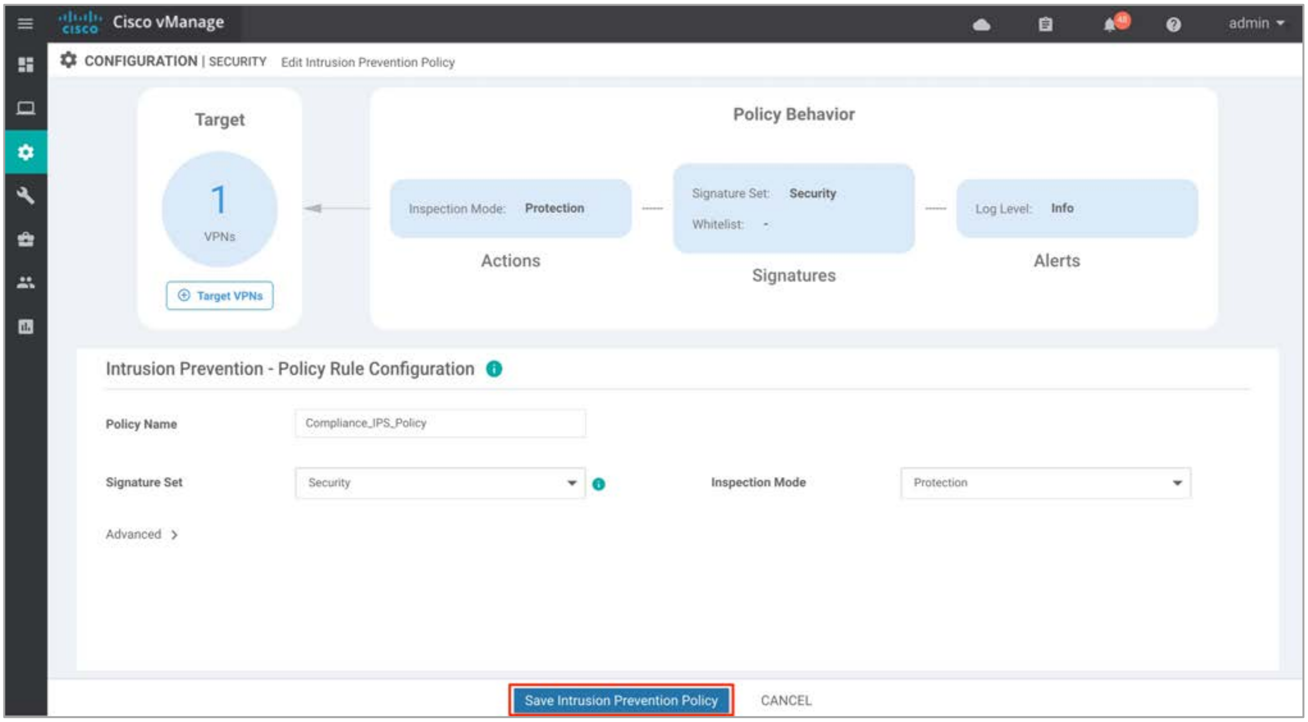
Signature Set: Security

Inspection Mode: Protection

Signature Whitelist: Select a signature list

Alerts Log Level: Info

Step 28 Click **Save Intrusion Prevention Policy** to add the configured Intrusion Prevention security policy.



Cisco vManage
admin
CONFIGURATION | SECURITY Edit Intrusion Prevention Policy
Target
1
VPNs
Target VPNs
Policy Behavior
Actions
Signatures
Alerts
Intrusion Prevention - Policy Rule Configuration
Advanced
Save Intrusion Prevention Policy
CANCEL

Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Info

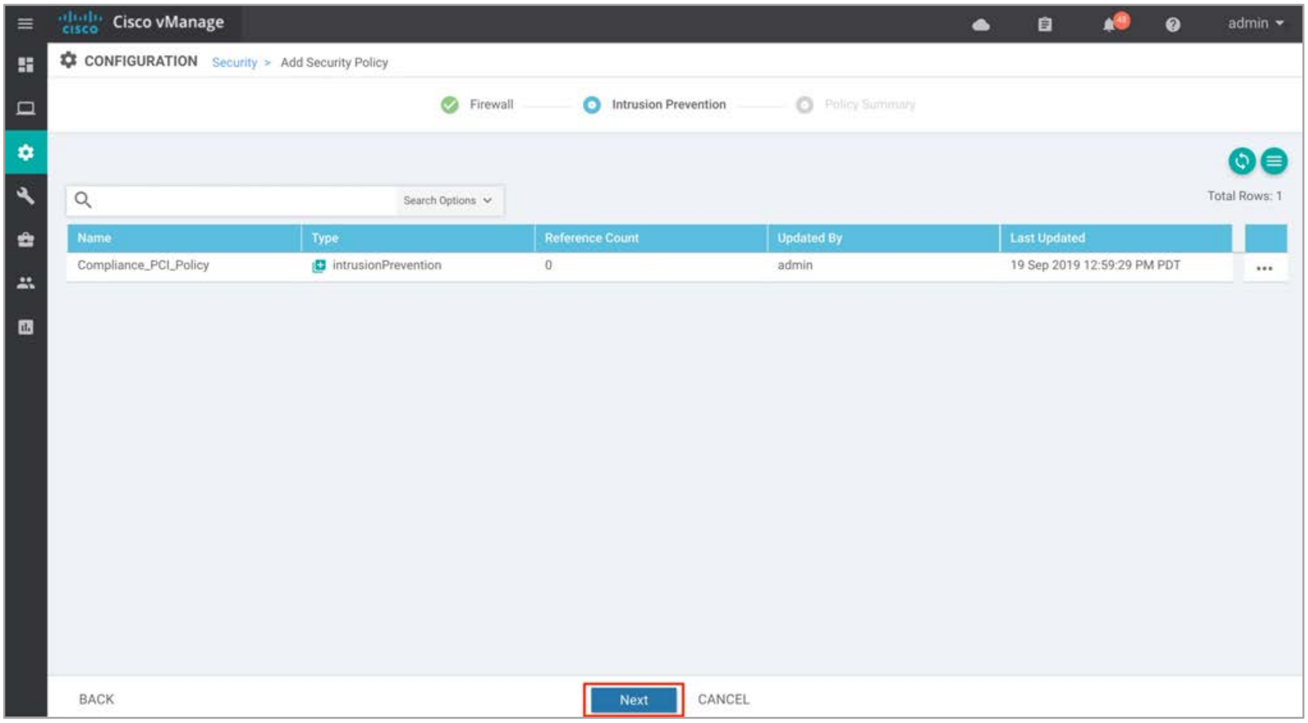
Policy Name: Compliance_IPS_Policy

Signature Set: Security

Inspection Mode: Protection

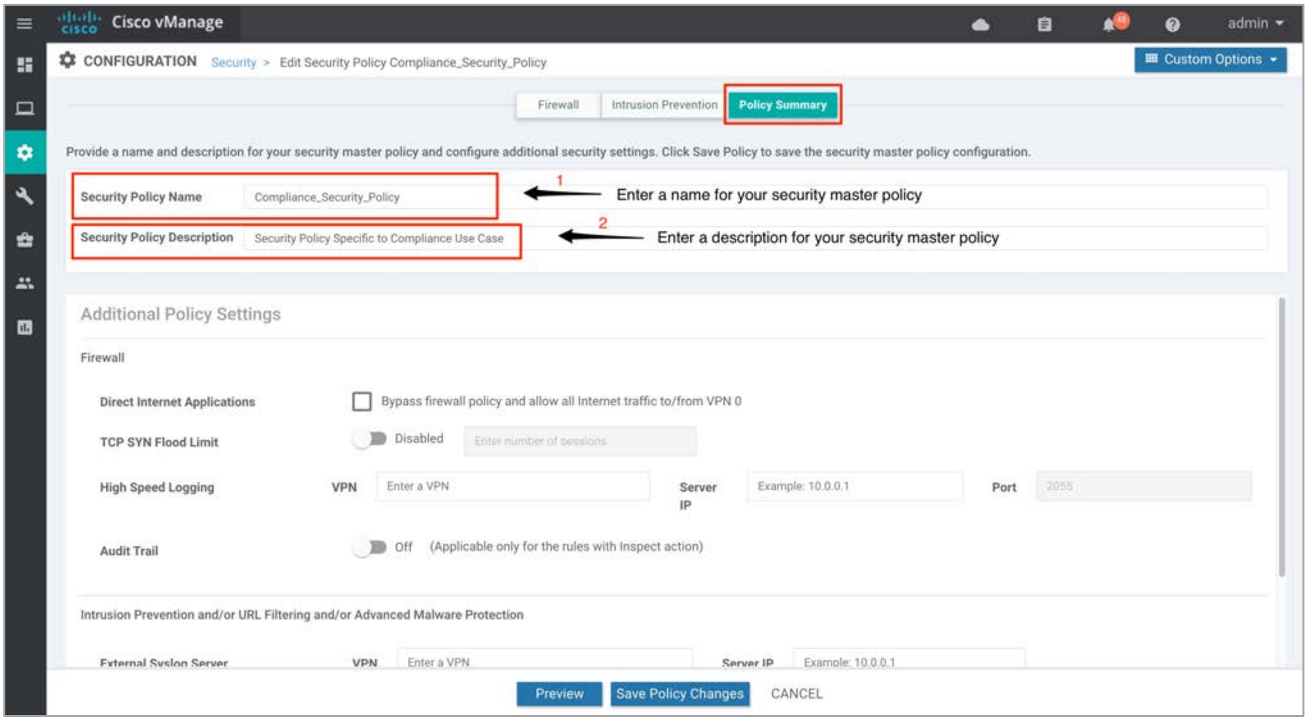
Process 2: Part 3 - Configure Policy Summary

Step 29 Click **Next** to configure the policy summary.



Name	Type	Reference Count	Updated By	Last Updated
Compliance_PCI_Policy	intrusionPrevention	0	admin	19 Sep 2019 12:59:29 PM PDT

Step 30 In the **Policy Summary** section, provide a name and description for your security master policy.



Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name: Compliance_Security_Policy — Enter a name for your security master policy

Security Policy Description: Security Policy Specific to Compliance Use Case — Enter a description for your security master policy

Additional Policy Settings

Firewall

Direct Internet Applications: □ Bypass firewall policy and allow all Internet traffic to/from VPN 0

TCP SYN Flood Limit: Disabled — Enter number of sessions

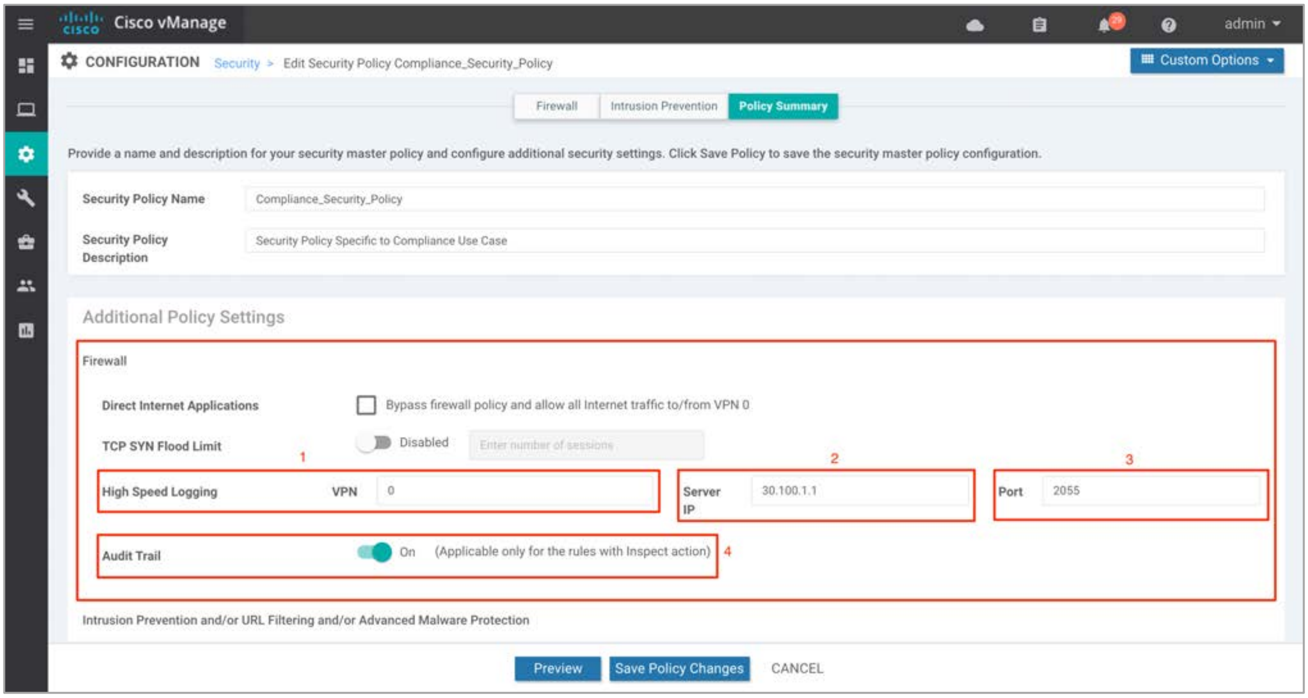
High Speed Logging: VPN Enter a VPN — Server IP Example: 10.0.0.1 — Port 2055

Audit Trail: Off (Applicable only for the rules with Inspect action)

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

External Syslog Server: VPN Enter a VPN — Server IP Example: 10.0.0.1

Step 31 To log firewall traffic, enable **Audit Trail** and enter the **VPN**, **Server IP** and **Port** information for High Speed Logging. Note that this feature is supported on WAN Edge devices running code 16.12 or a later code.



Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name: Compliance_Security_Policy

Security Policy Description: Security Policy Specific to Compliance Use Case

Additional Policy Settings

Firewall

Direct Internet Applications: □ Bypass firewall policy and allow all Internet traffic to/from VPN 0

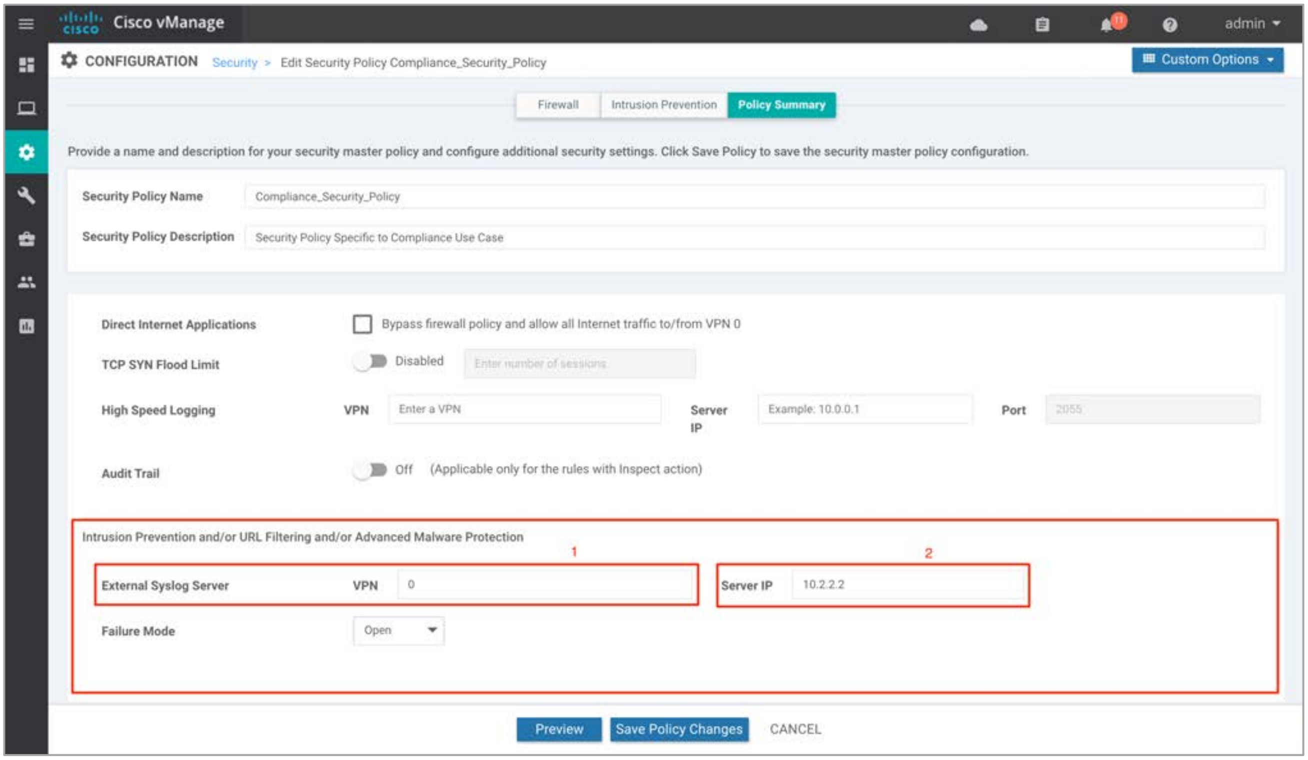
TCP SYN Flood Limit: Disabled, Enter number of sessions

High Speed Logging: VPN 0; Server IP 30.100.1.1; Port 2055

Audit Trail: On (Applicable only for the rules with Inspect action)

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

Step 32 Under the **Intrusion Prevention** section, you can add details to send logs to your external syslog server. Here, the **External Syslog Server** is set within VPN 0, hence the **VPN** label in the **VPN** tab is **0**, followed by Server IP address against the **Server IP** tab.



Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name: Compliance_Security_Policy

Security Policy Description: Security Policy Specific to Compliance Use Case

Direct Internet Applications: □ Bypass firewall policy and allow all Internet traffic to/from VPN 0

TCP SYN Flood Limit: Disabled, Enter number of sessions

High Speed Logging: VPN Enter a VPN; Server IP Example: 10.0.0.1; Port 2055

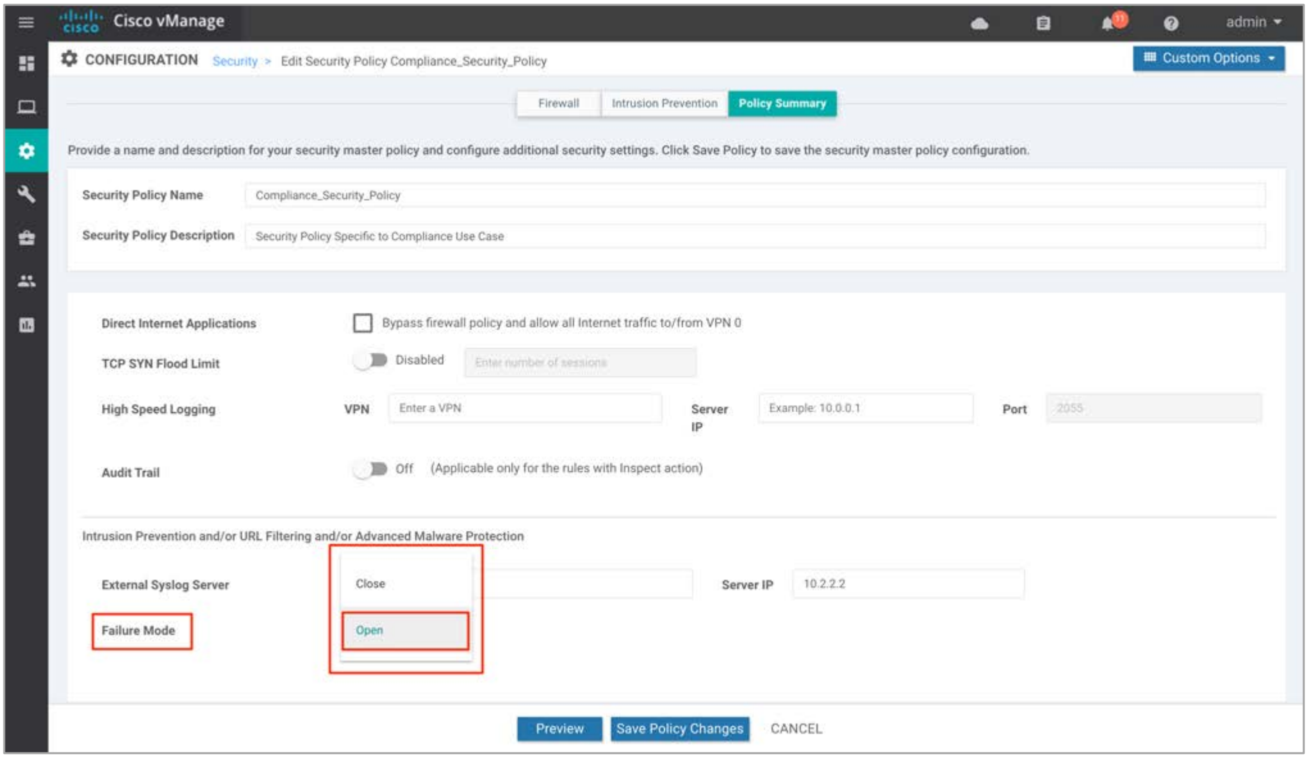
Audit Trail: Off (Applicable only for the rules with Inspect action)

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

External Syslog Server: VPN 0; Server IP 10.2.2.2

Failure Mode: Open

Step 33 Set the **Failure Mode** to either **Open** or **Close**. To avoid service interruption during signature updates, the failure mode is set to **Open.**



Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name: Compliance_Security_Policy

Security Policy Description: Security Policy Specific to Compliance Use Case

Direct Internet Applications: □ Bypass firewall policy and allow all Internet traffic to/from VPN 0

TCP SYN Flood Limit: Disabled — Enter number of sessions

High Speed Logging: VPN: Enter a VPN — Server IP: Example: 10.0.0.1 — Port: 2055

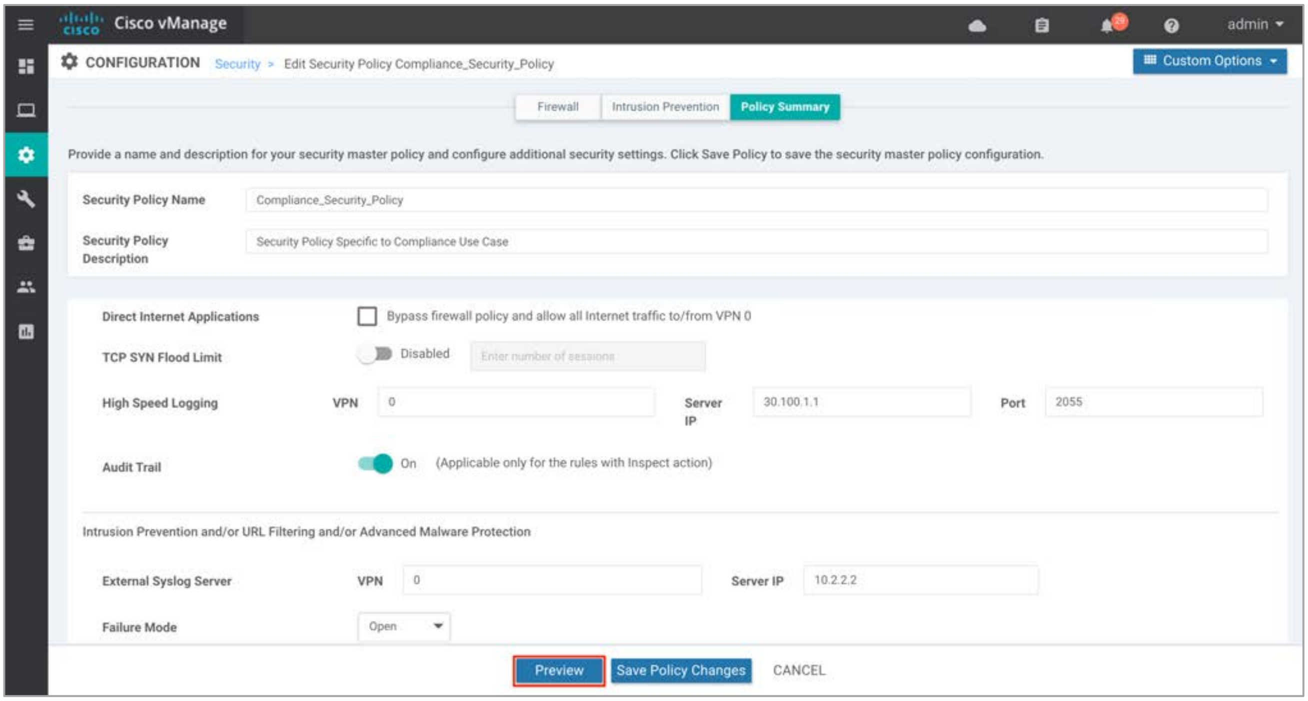
Audit Trail: Off (Applicable only for the rules with Inspect action)

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

External Syslog Server — Server IP: 10.2.2.2

Failure Mode: Close / Open

Step 34 Click **Preview** to view the CLI equivalent for the policy to be deployed.



Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name: Compliance_Security_Policy

Security Policy Description: Security Policy Specific to Compliance Use Case

Direct Internet Applications: □ Bypass firewall policy and allow all Internet traffic to/from VPN 0

TCP SYN Flood Limit: Disabled — Enter number of sessions

High Speed Logging: VPN: 0 — Server IP: 30.100.1.1 — Port: 2055

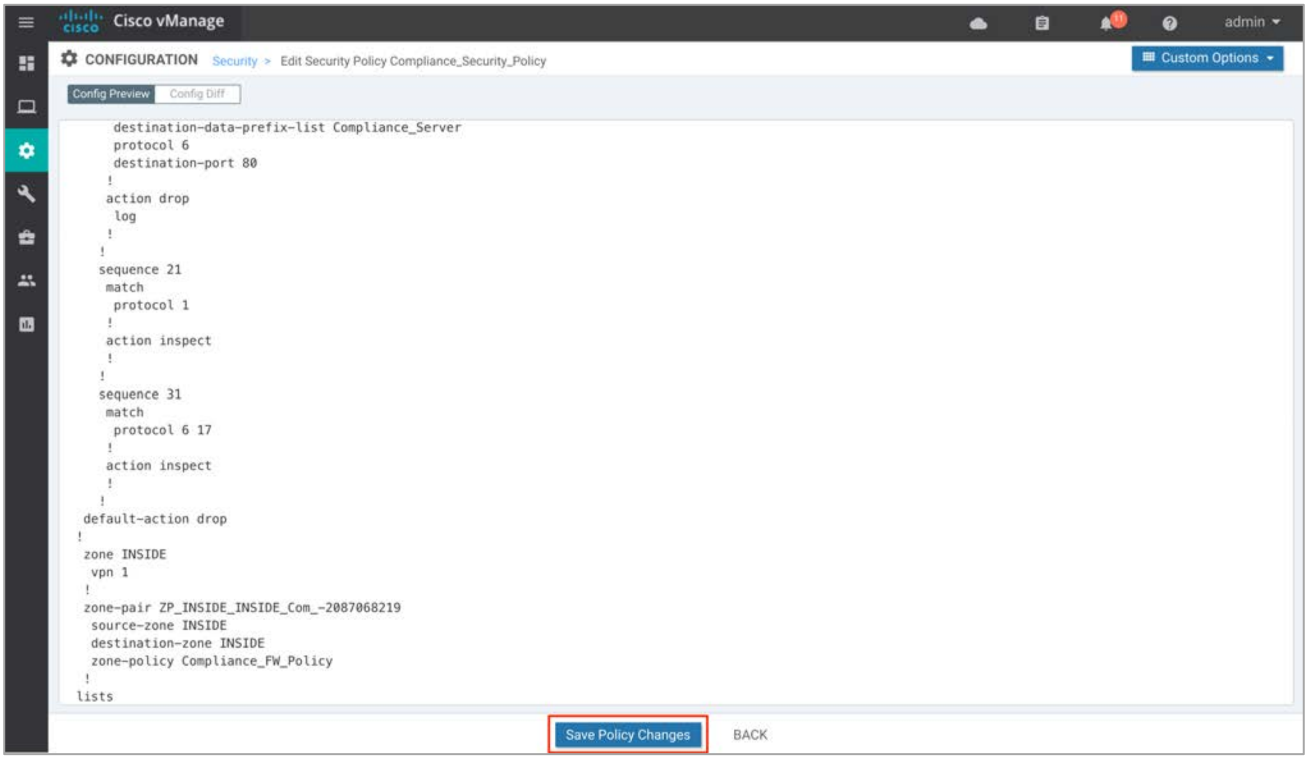
Audit Trail: On (Applicable only for the rules with Inspect action)

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

External Syslog Server: VPN: 0 — Server IP: 10.2.2.2

Failure Mode: Open

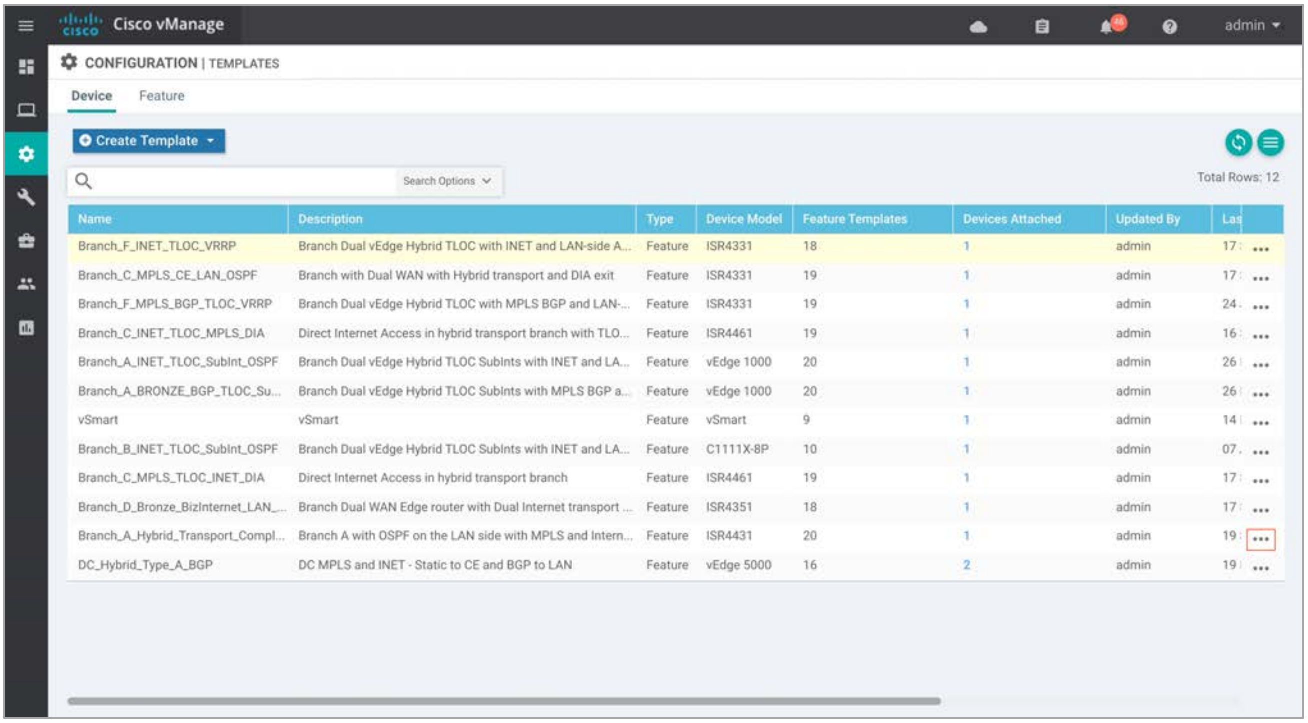
Step 35 Finally, click **Save Policy Changes.**



```
     destination-data-prefix-list Compliance_Server
     protocol 6
     destination-port 80
    !
    action drop
     log
    !
   !
   sequence 21
    match
     protocol 1
    !
    action inspect
    !
   !
   sequence 31
    match
     protocol 6 17
    !
    action inspect
    !
   !
 default-action drop
!
 zone INSIDE
  vpn 1
 !
 zone-pair ZP_INSIDE_INSIDE_Com_-2087068219
  source-zone INSIDE
  destination-zone INSIDE
  zone-policy Compliance_FW_Policy
 !
lists
```

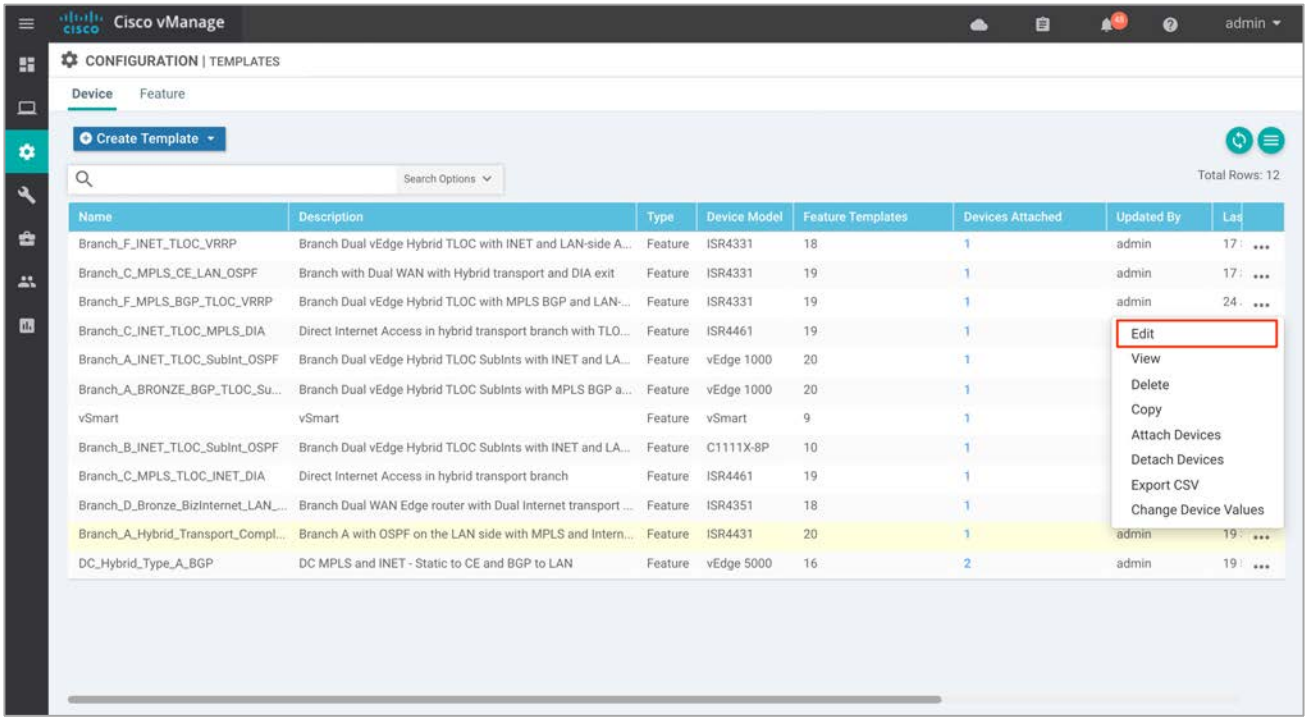
Process 3: Attach the Security Policy to the Device Template.

Step 36 To attach the security policy to a **Device Template**, click the three dots (**…**)found on the right side of the template and select **Edit** from the drop-down menu.



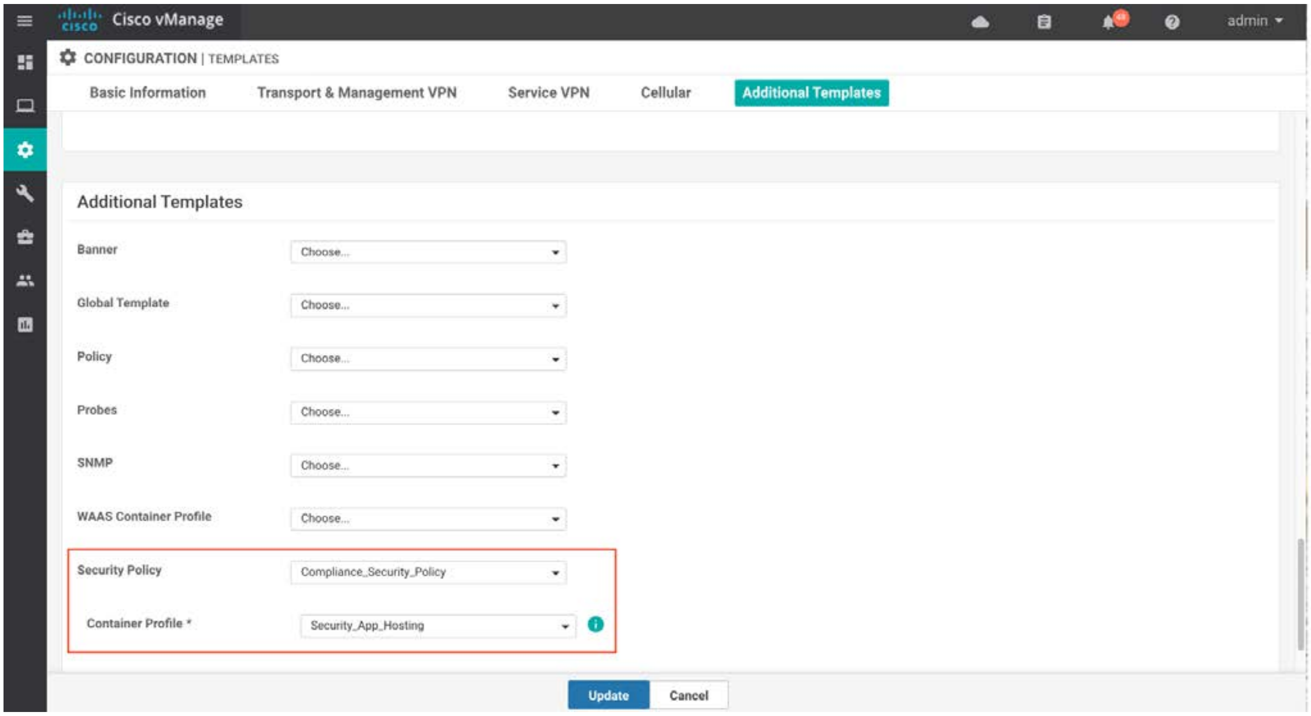
Total Rows: 12

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Las
Branch_F_INET_TLOC_VRRP	Branch Dual vEdge Hybrid TLOC with INET and LAN-side A...	Feature	ISR4331	18	1	admin	17 •••
Branch_C_MPLS_CE_LAN_OSPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	19	1	admin	17 •••
Branch_F_MPLS_BGP_TLOC_VRRP	Branch Dual vEdge Hybrid TLOC with MPLS BGP and LAN-...	Feature	ISR4331	19	1	admin	24 •••
Branch_C_INET_TLOC_MPLS_DIA	Direct Internet Access in hybrid transport branch with TLO...	Feature	ISR4461	19	1	admin	16 •••
Branch_A_INET_TLOC_SubInt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LA...	Feature	vEdge 1000	20	1	admin	26 •••
Branch_A_BRONZE_BGP_TLOC_Su...	Branch Dual vEdge Hybrid TLOC SubInts with MPLS BGP a...	Feature	vEdge 1000	20	1	admin	26 •••
vSmart	vSmart	Feature	vSmart	9	1	admin	14 •••
Branch_B_INET_TLOC_SubInt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LA...	Feature	C1111X-8P	10	1	admin	07 •••
Branch_C_MPLS_TLOC_INET_DIA	Direct Internet Access in hybrid transport branch	Feature	ISR4461	19	1	admin	17 •••
Branch_D_Bronze_BizInternet_LAN_...	Branch Dual WAN Edge router with Dual Internet transport ...	Feature	ISR4351	18	1	admin	17 •••
Branch_A_Hybrid_Transport_Compl...	Branch A with OSPF on the LAN side with MPLS and Intern...	Feature	ISR4431	20	1	admin	19 •••
DC_Hybrid_Type_A_BGP	DC MPLS and INET - Static to CE and BGP to LAN	Feature	vEdge 5000	16	2	admin	19 •••



Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Las
Branch_F_INET_TLOC_VRRP	Branch Dual vEdge Hybrid TLOC with INET and LAN-side A...	Feature	ISR4331	18	1	admin	17
Branch_C_MPLS_CE_LAN_OSPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	19	1	admin	17
Branch_F_MPLS_BGP_TLOC_VRRP	Branch Dual vEdge Hybrid TLOC with MPLS BGP and LAN-...	Feature	ISR4331	19	1	admin	24
Branch_C_INET_TLOC_MPLS_DIA	Direct Internet Access in hybrid transport branch with TLO...	Feature	ISR4461	19	1		
Branch_A_INET_TLOC_SubInt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LA...	Feature	vEdge 1000	20	1		
Branch_A_BRONZE_BGP_TLOC_Su...	Branch Dual vEdge Hybrid TLOC SubInts with MPLS BGP a...	Feature	vEdge 1000	20	1		
vSmart	vSmart	Feature	vSmart	9	1		
Branch_B_INET_TLOC_SubInt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LA...	Feature	C1111X-8P	10	1		
Branch_C_MPLS_TLOC_INET_DIA	Direct Internet Access in hybrid transport branch	Feature	ISR4461	19	1		
Branch_D_Bronze_BizInternet_LAN_...	Branch Dual WAN Edge router with Dual Internet transport ...	Feature	ISR4351	18	1		
Branch_A_Hybrid_Transport_Compl...	Branch A with OSPF on the LAN side with MPLS and Intern...	Feature	ISR4431	20	1	admin	19
DC_Hybrid_Type_A_BGP	DC MPLS and INET - Static to CE and BGP to LAN	Feature	vEdge 5000	16	2	admin	19

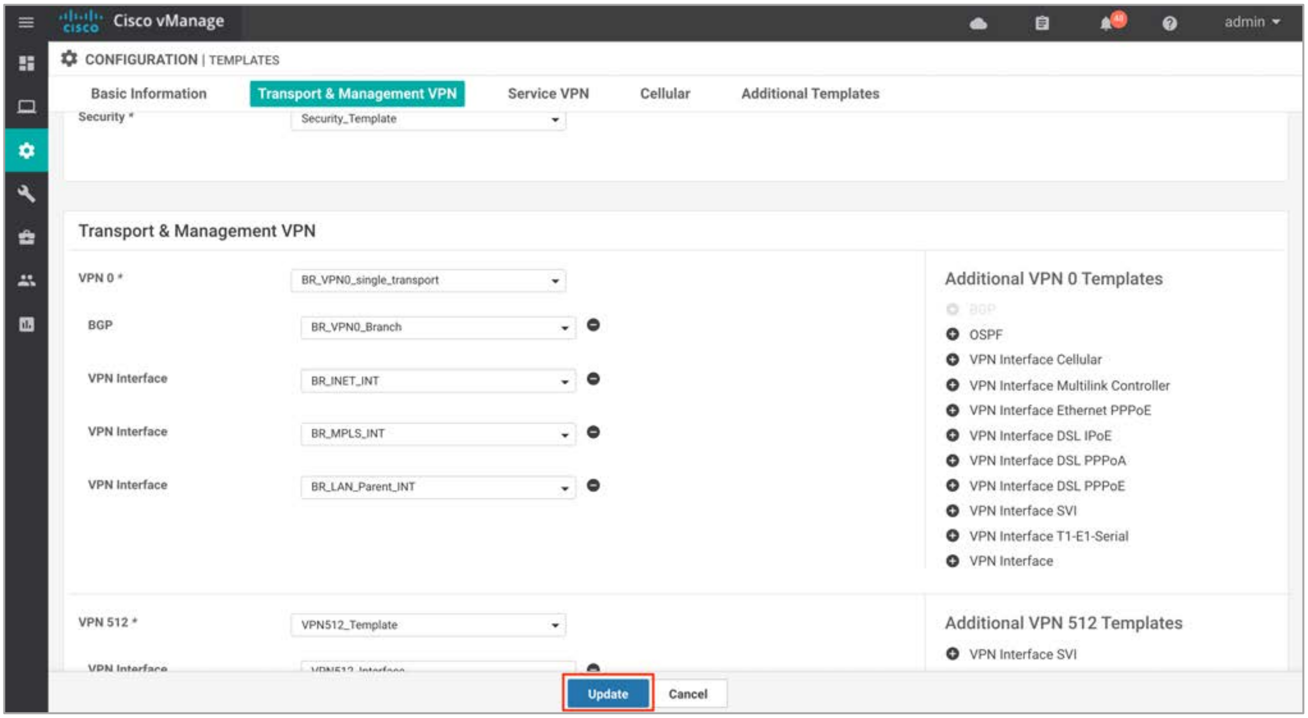
Step 37 Within the device template, navigate to **Additional Templates** and attach the **Security Policy** (**Compliance_Security_Policy)** along with the **Container Profile** (**Security_App_Hosting**).



Additional Templates

Banner	Choose...
Global Template	Choose...
Policy	Choose...
Probes	Choose...
SNMP	Choose...
WAAS Container Profile	Choose...
Security Policy	Compliance_Security_Policy
Container Profile *	Security_App_Hosting

Step 38 Click **Update** to update the device template.

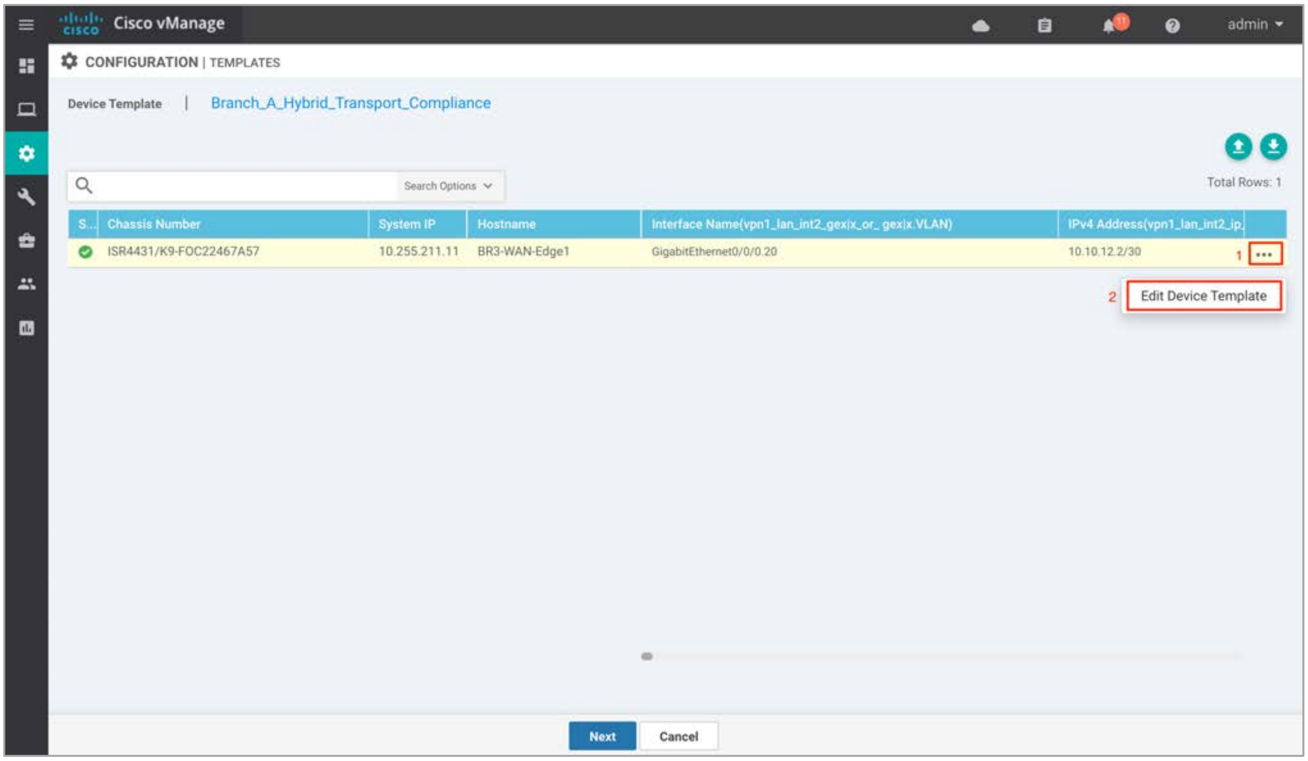


Security * Security_Template

Transport & Management VPN

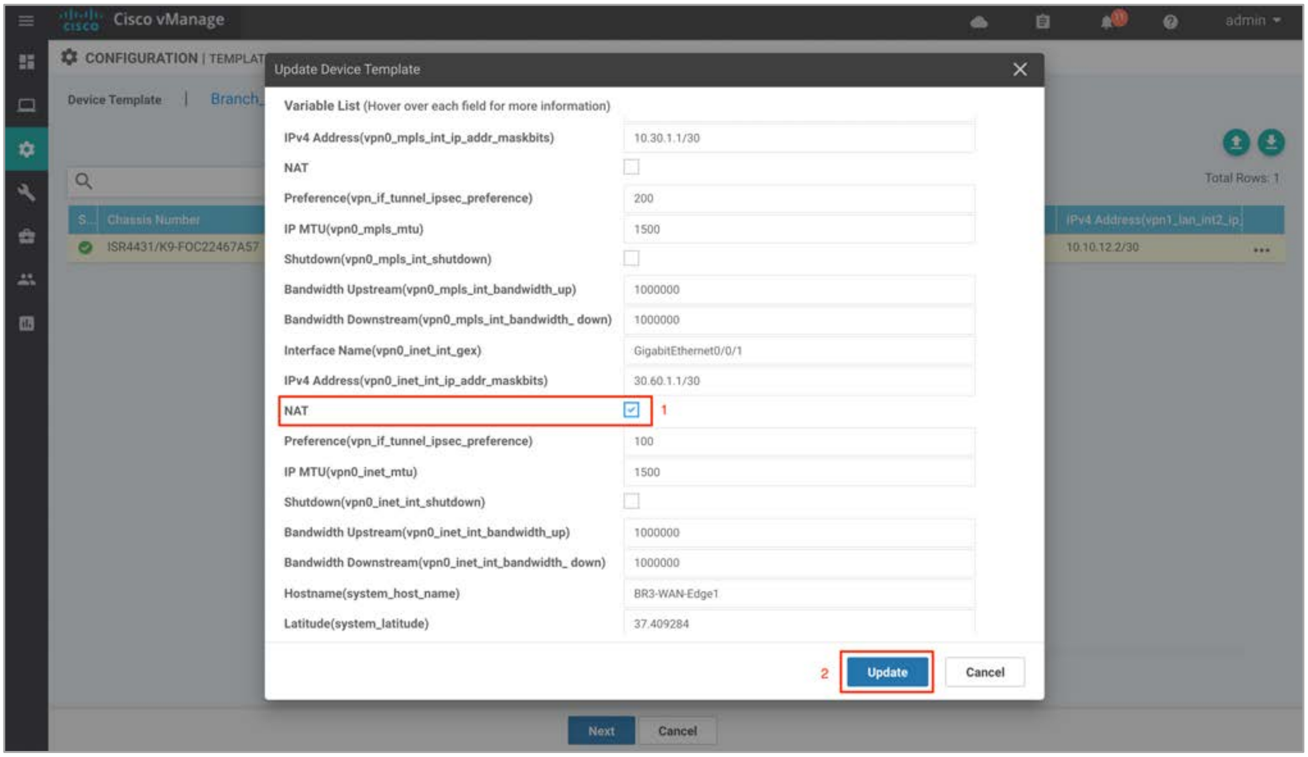
VPN 0 *	BR_VPN0_single_transport
BGP	BR_VPN0_Branch
VPN Interface	BR_INET_INT
VPN Interface	BR_MPLS_INT
VPN Interface	BR_LAN_Parent_INT
VPN 512 *	VPN512_Template
VPN Interface	VPN512_Interface

Step 39 Proceed to configure NAT on your VPN 0 WAN interface if the syslog server is reachable from VPN 0 or if you need to manually download signature updates using CLI on your WAN edge device. To do so click the three dots and select **Edit**.



Device Template | Branch_A_Hybrid_Transport_Compliance

S...	Chassis Number	System IP	Hostname	Interface Name(vpn1_lan_int2_gex|x_or_ gex|x.VLAN)	IPv4 Address(vpn1_lan_int2_ip_
✓	ISR4431/K9-FOC22467A57	10.255.211.11	BR3-WAN-Edge1	GigabitEthernet0/0/0.20	10.10.12.2/30



Update Device Template

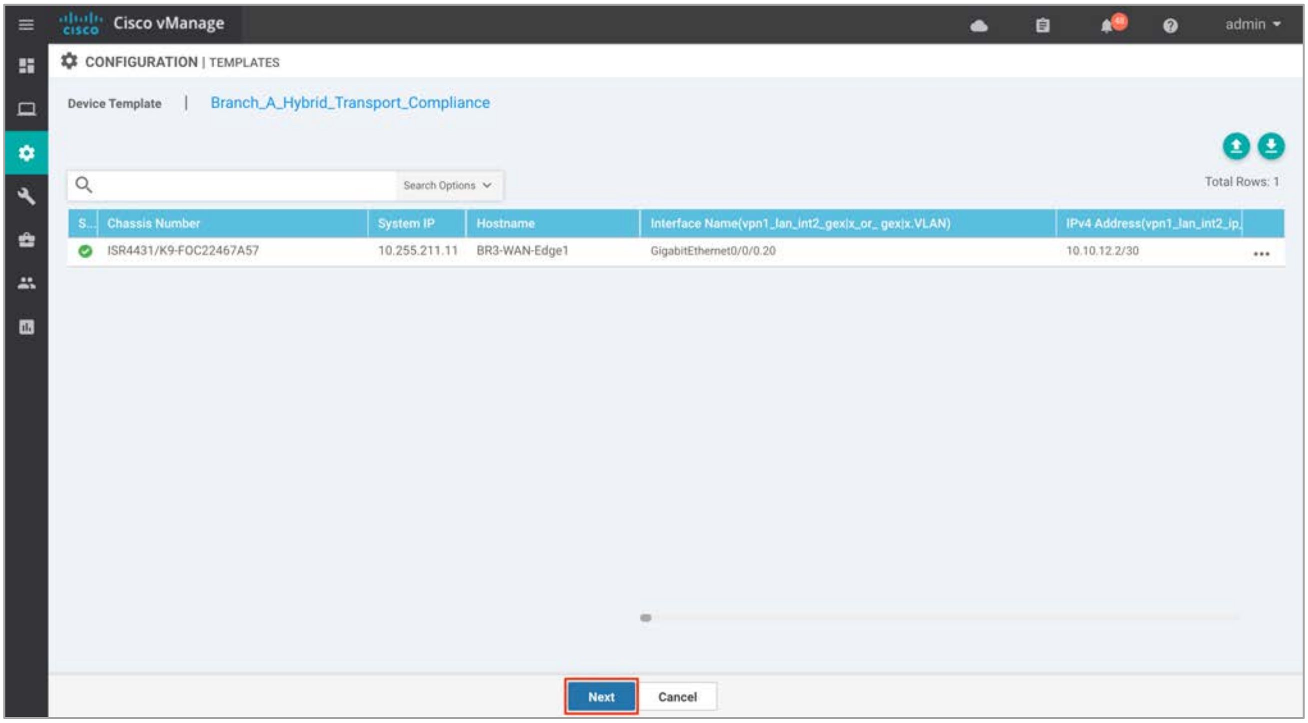
Variable List (Hover over each field for more information)

IPv4 Address(vpn0_mpls_int_ip_addr_maskbits)	10.30.1.1/30
NAT	□
Preference(vpn_if_tunnel_ipsec_preference)	200
IP MTU(vpn0_mpls_mtu)	1500
Shutdown(vpn0_mpls_int_shutdown)	□
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_ down)	1000000
Interface Name(vpn0_inet_int_gex)	GigabitEthernet0/0/1
IPv4 Address(vpn0_inet_int_ip_addr_maskbits)	30.60.1.1/30
NAT	☑ 1
Preference(vpn_if_tunnel_ipsec_preference)	100
IP MTU(vpn0_inet_mtu)	1500
Shutdown(vpn0_inet_int_shutdown)	□
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_inet_int_bandwidth_ down)	1000000
Hostname(system_host_name)	BR3-WAN-Edge1
Latitude(system_latitude)	37.409284

2 Update Cancel

Note that if the NAT feature is not currently configured as a variable in your interface feature template, you will need to modify the **WAN Interface Feature Template** to enable NAT by clicking the checkbox. You can do this before or after deploying the security policy.

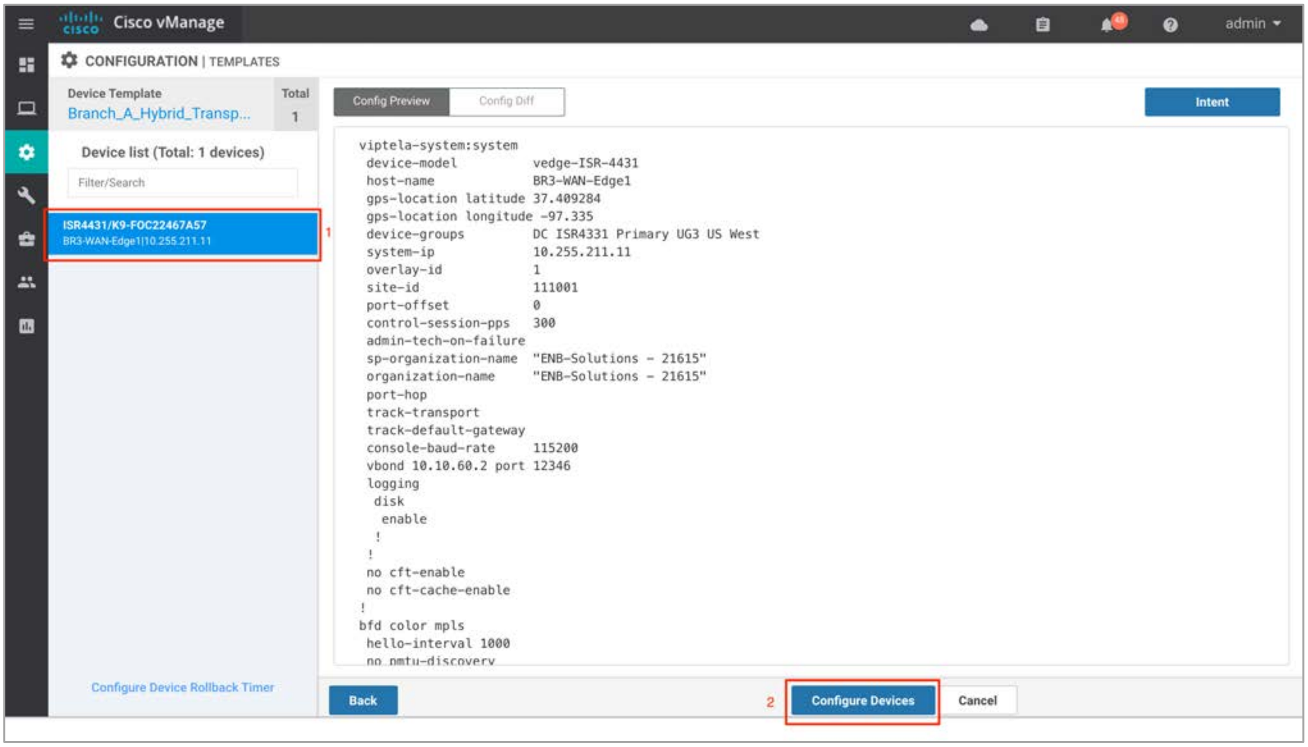
Step 40 Once the changes are made, click **Next**.



Device Template | Branch_A_Hybrid_Transport_Compliance

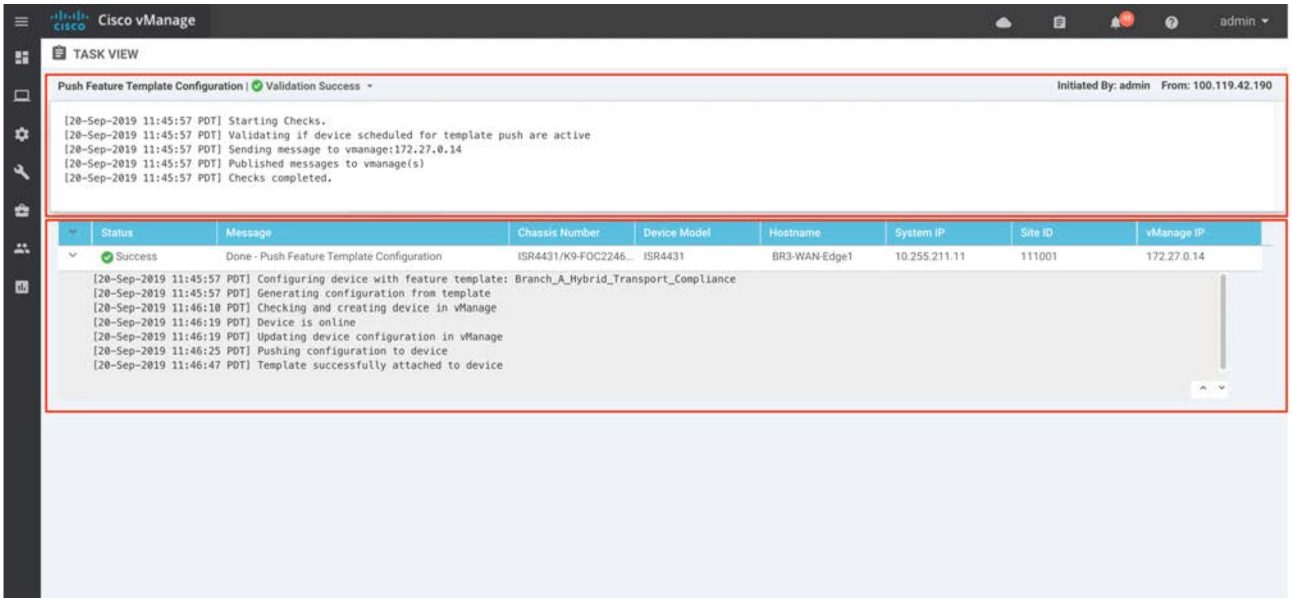
S...	Chassis Number	System IP	Hostname	Interface Name(vpn1_lan_int2_gex|x_or_ gex|x.VLAN)	IPv4 Address(vpn1_lan_int2_ip.
✓	ISR4431/K9-FOC22467A57	10.255.211.11	BR3-WAN-Edge1	GigabitEthernet0/0/0.20	10.10.12.2/30

Step 41 Finally, select the WAN Edge device from the **Device list** on the right panel to preview the configuration and then click **Configure Devices** to configure the device with the security policy along with the container profile.


Cisco vManage
admin
CONFIGURATION | TEMPLATES
Device Template
Branch_A_Hybrid_Transp...
Total
1
Config Preview
Config Diff
Intent
Device list (Total: 1 devices)
Filter/Search
ISR4431/K9-FOC22467A57
BR3-WAN-Edge1|10.255.211.11
1
Configure Device Rollback Timer
Back
2
Configure Devices
Cancel

```
viptela-system:system
 device-model          vedge-ISR-4431
 host-name             BR3-WAN-Edge1
 gps-location latitude 37.409284
 gps-location longitude -97.335
 device-groups         DC ISR4331 Primary UG3 US West
 system-ip             10.255.211.11
 overlay-id            1
 site-id               111001
 port-offset           0
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate     115200
 vbond 10.10.60.2 port 12346
 logging
  disk
   enable
  !
 !
 no cft-enable
 no cft-cache-enable
!
bfd color mpls
 hello-interval 1000
 no pmtu-discovery
```

Step 42 The Task View screen displays the results. Look for the status of the template to verify if the template was successfully attached to the device.



Push Feature Template Configuration | Validation Success Initiated By: admin From: 100.119.42.190

```
[20-Sep-2019 11:45:57 PDT] Starting Checks.
[20-Sep-2019 11:45:57 PDT] Validating if device scheduled for template push are active
[20-Sep-2019 11:45:57 PDT] Sending message to vmanage:172.27.0.14
[20-Sep-2019 11:45:57 PDT] Published messages to vmanage(s)
[20-Sep-2019 11:45:57 PDT] Checks completed.
```

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
✓ Success	Done - Push Feature Template Configuration	ISR4431/K9-FOC2246...	ISR4431	BR3-WAN-Edge1	10.255.211.11	111001	172.27.0.14

```
[20-Sep-2019 11:45:57 PDT] Configuring device with feature template: Branch_A_Hybrid_Transport_Compliance
[20-Sep-2019 11:45:57 PDT] Generating configuration from template
[20-Sep-2019 11:46:10 PDT] Checking and creating device in vManage
[20-Sep-2019 11:46:19 PDT] Device is online
[20-Sep-2019 11:46:19 PDT] Updating device configuration in vManage
[20-Sep-2019 11:46:25 PDT] Pushing configuration to device
[20-Sep-2019 11:46:47 PDT] Template successfully attached to device
```

Operate - Cisco SD-WAN Security – Compliance Use Case

Using the vManage GUI, you can monitor, troubleshoot and manage the SD-WAN security features deployed. Following are some of the ways of doing this.

Process 1: Monitor Enterprise Firewall with Application Awareness Using vManage NMS

Method 1: Monitor the firewall feature using the main dashboard of vManage– The vManage dashboard displays an overall graphical view of packets inspected and dropped over a period of time, with the option to further investigate.

Method 2: Monitor the firewall feature using the vManage Monitor dashboard– Within the vManage Monitor dashboard, you can view both graphical and real time statistical data of Enterprise Firewall with Application Awareness feature running on specific WAN edge devices.

Method 3: Monitor the firewall feature and statistics using vManage SSH Server Dashboard– vManage NMS provides the option to manage devices through CLI using the SSH Server Dashboard. Using this method, you can monitor and manage the Enterprise Firewall with Application Awareness feature for individual WAN edge devices using CLI show commands and other debug tools.

Process 2: Monitor the IPS feature Using vManage NMS

Method 1: Monitor IPS signature violations using vManage Main Dashboard– vManage dashboard displays an overall graphical view of Intrusion Prevention System (IPS) signature violations by severity and by count.

Method 2: Monitor IPS using vManage Monitor Dashboard– Within the vManage Monitor dashboard, you can view both graphical and real time statistical data of the IPS feature running on a specific WAN edge device.

Method 3: Monitor IPS and statistics using vManage SSH Server Dashboard– To monitor IPS for individual WAN edge devices using CLI commands.

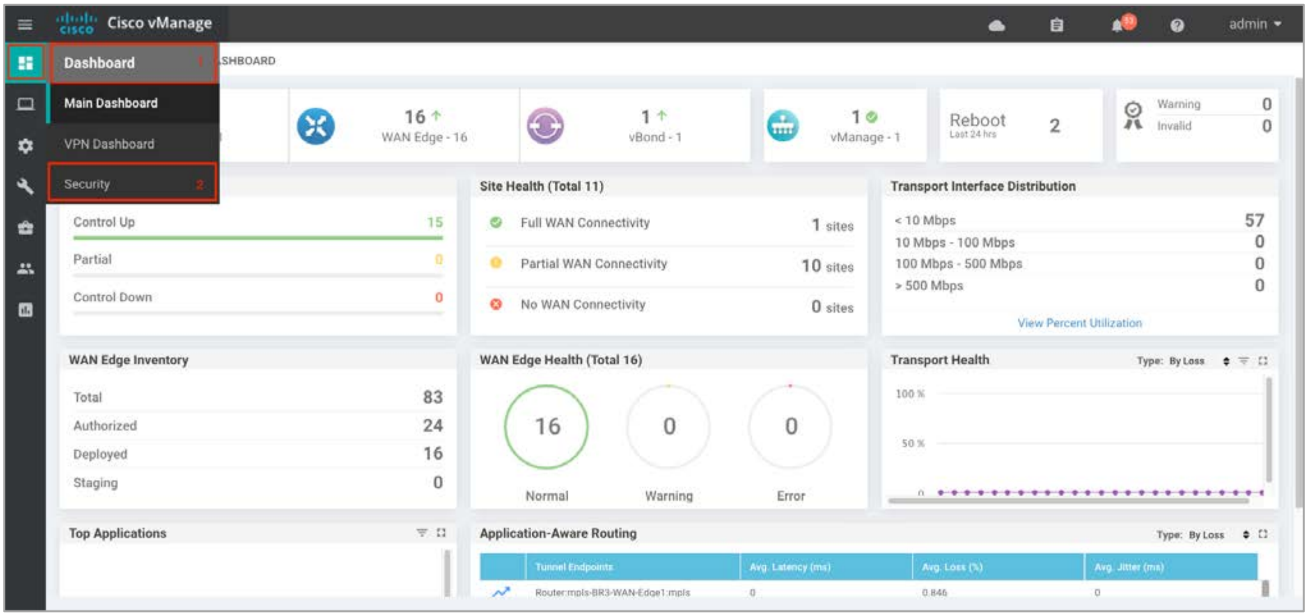
Process 3: Monitor IPS signature violations using Syslog server: If you have a syslog server configured, scan the logs gathered within the server to monitor the IPS signature violations on your WAN edge device.

Process 1: Monitor the Enterprise Firewall with App Aware Feature Using vManage

Method 1: Monitor the Firewall Feature via vManage Main Dashboard

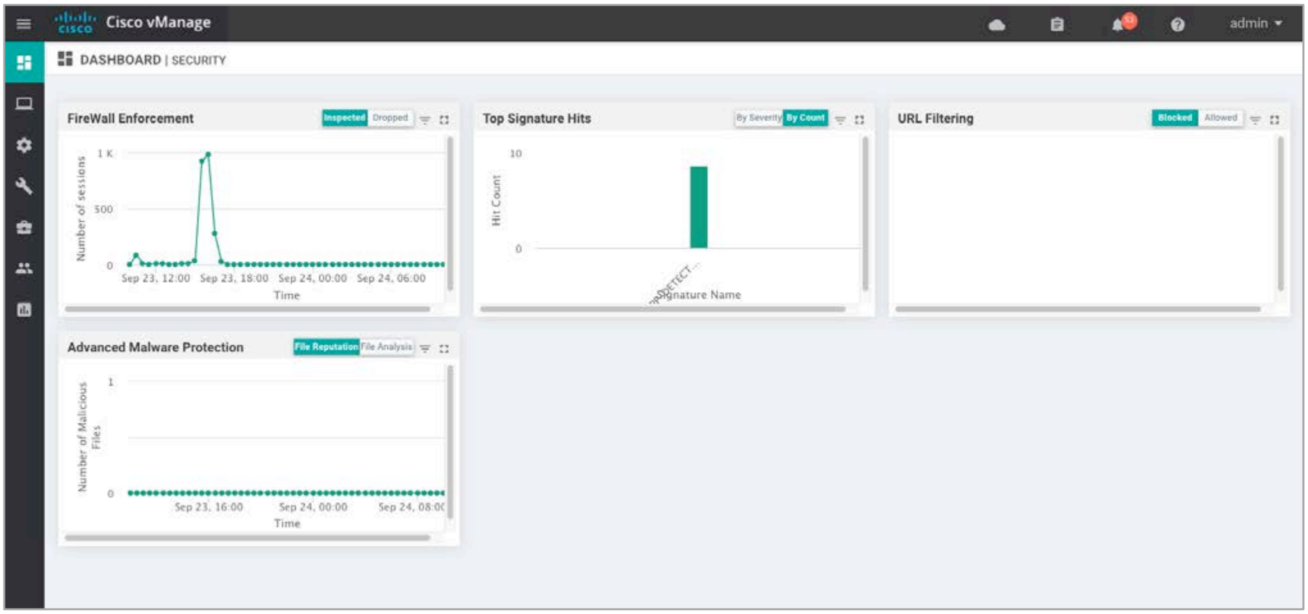
Using the vManage NMS dashboard, you can view the Firewall statistics through the Dashboard.

Step 1 Navigate to **Dashboard** > **Security.**

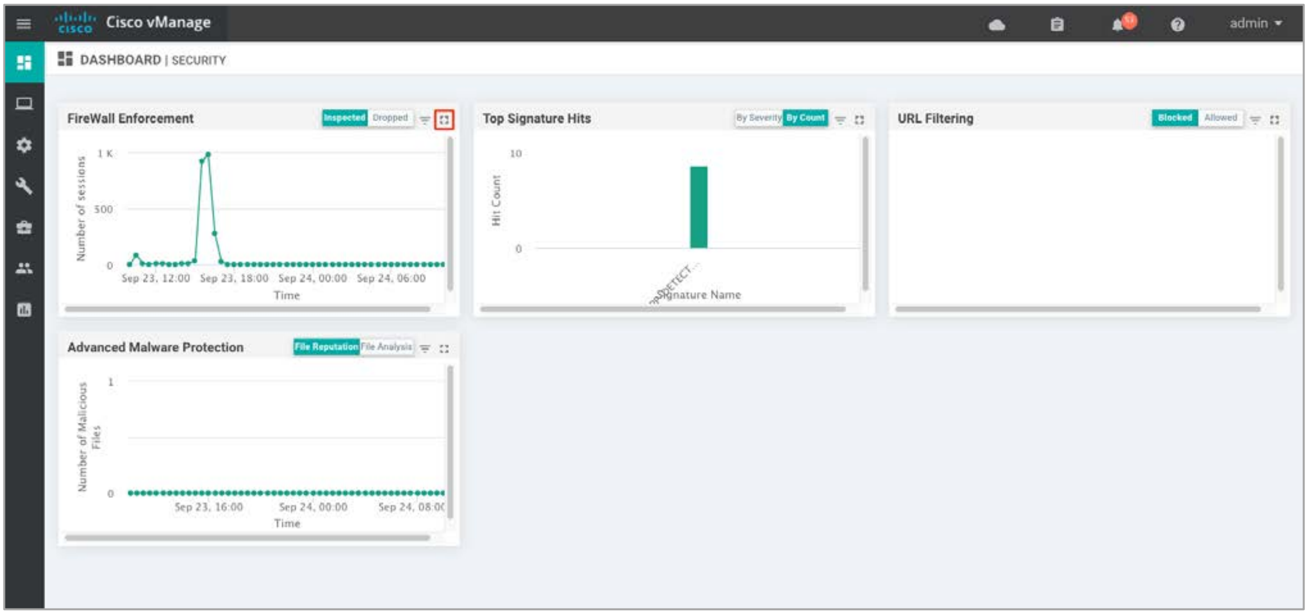


Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR3-WAN-Edge1:mpls	0	0.846	0

Step 2 The following screenshot of the security dashboard shows **Firewall Enforcement** activity and **Top Signature Hits** data.

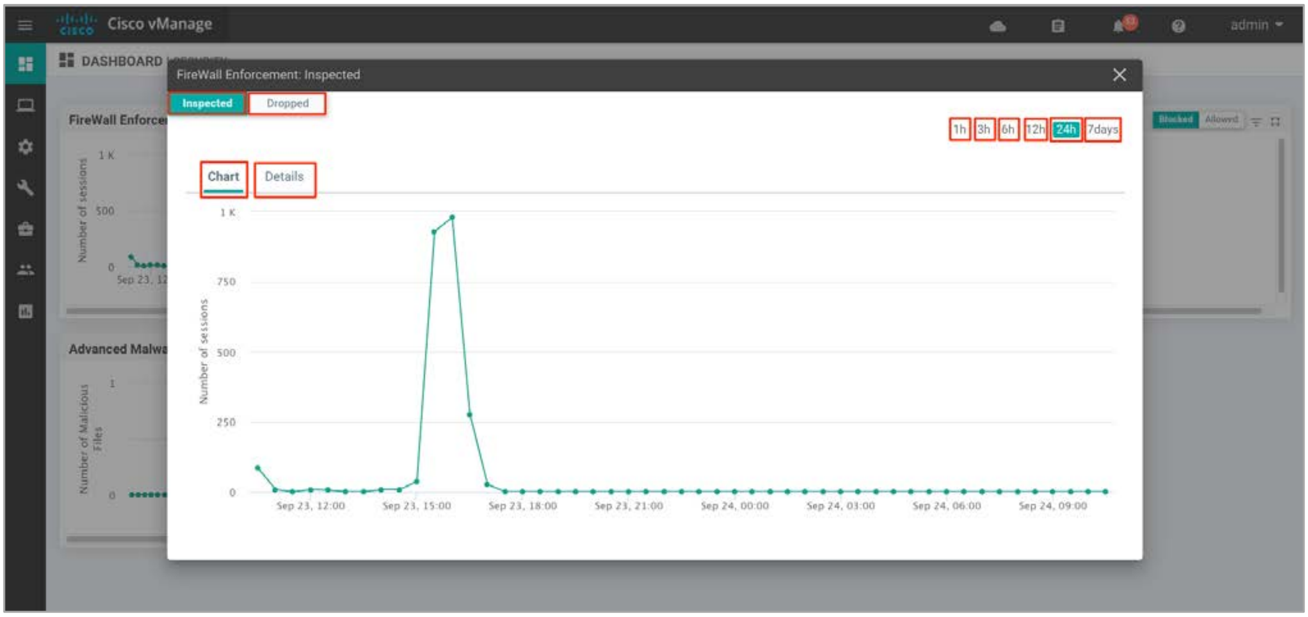


Step 3 To take a closer look into the Firewall Enforcement graph, click the square box [] on the top right.

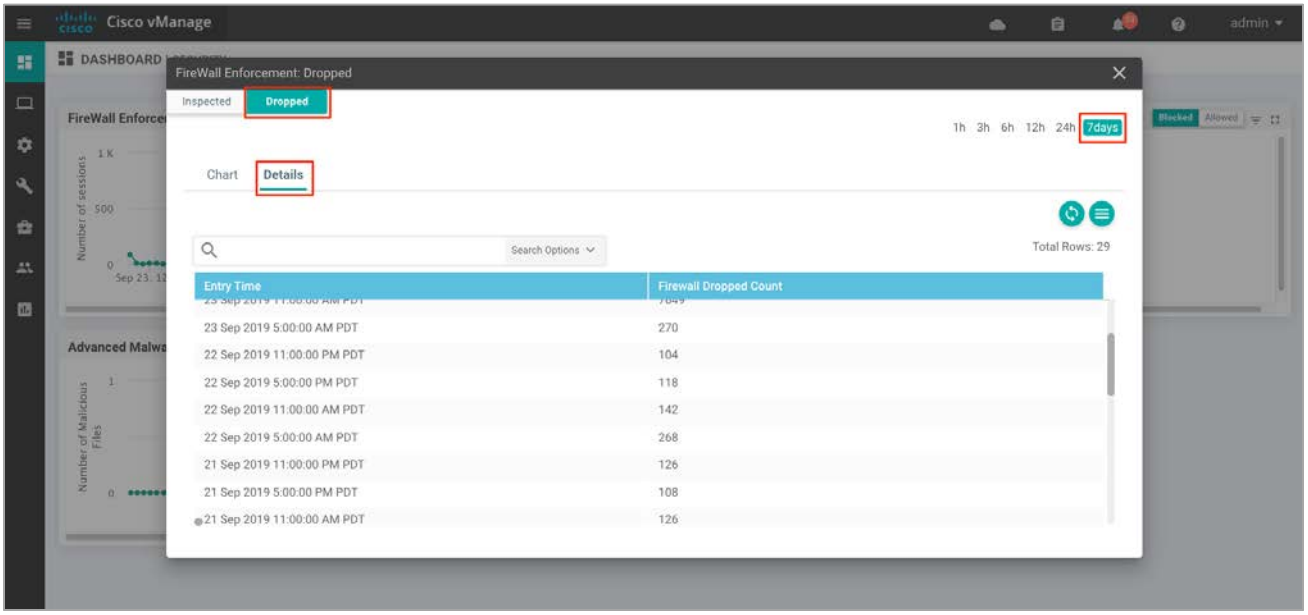


Step 4 Further analyze the graph for more information. Toggle between inspected and dropped packets and click on 1h, 3h, 6h, 12h, 24h (default) or 7 days to view the hourly, daily, or weekly firewall statistics.

The **Chart** tab displays the graphical representation of the firewall statistics for both inspected and dropped packets.



The **Details** tab displays the Firewall Dropped Count.



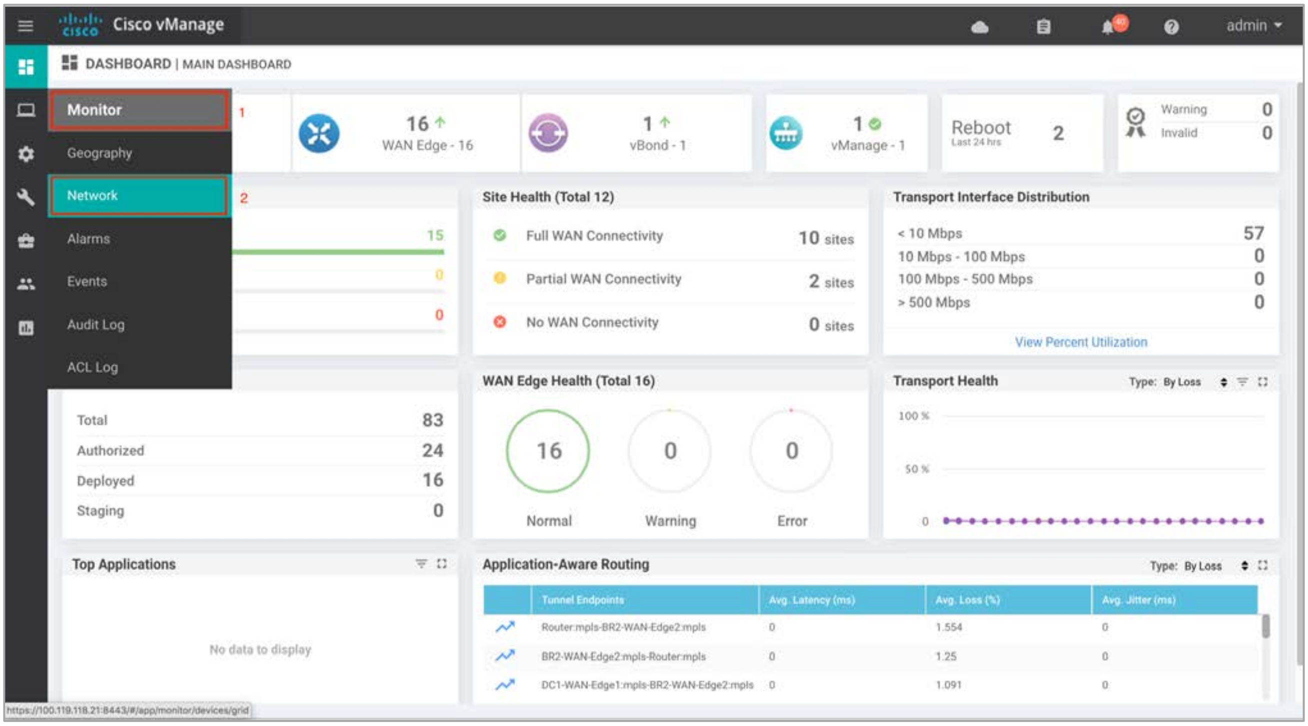
Total Rows: 29

Entry Time	Firewall Dropped Count
23 Sep 2019 5:00:00 AM PDT	270
22 Sep 2019 11:00:00 PM PDT	104
22 Sep 2019 5:00:00 PM PDT	118
22 Sep 2019 11:00:00 AM PDT	142
22 Sep 2019 5:00:00 AM PDT	268
21 Sep 2019 11:00:00 PM PDT	126
21 Sep 2019 5:00:00 PM PDT	108
21 Sep 2019 11:00:00 AM PDT	126

Technical Tip: To view details such as IP address of the packet inspected or dropped, click the peaks of the graph.

Method 2: Monitor the Firewall Feature Using vManage Monitor Dashboard

Step 5 Navigate to **Network** under the **Monitor option** available on the left pane.



Site Health (Total 12)

Full WAN Connectivity	10 sites
Partial WAN Connectivity	2 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

< 10 Mbps	57
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

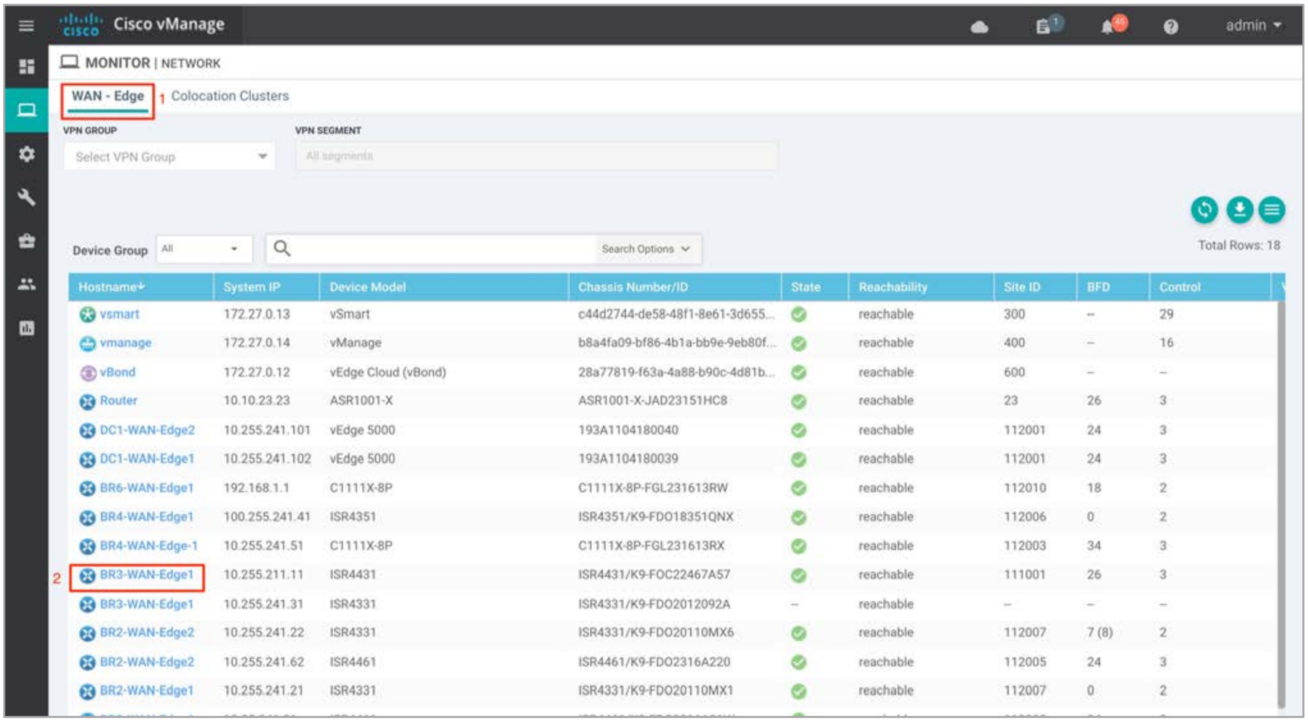
View Percent Utilization

Total	83
Authorized	24
Deployed	16
Staging	0

Application-Aware Routing — Type: By Loss

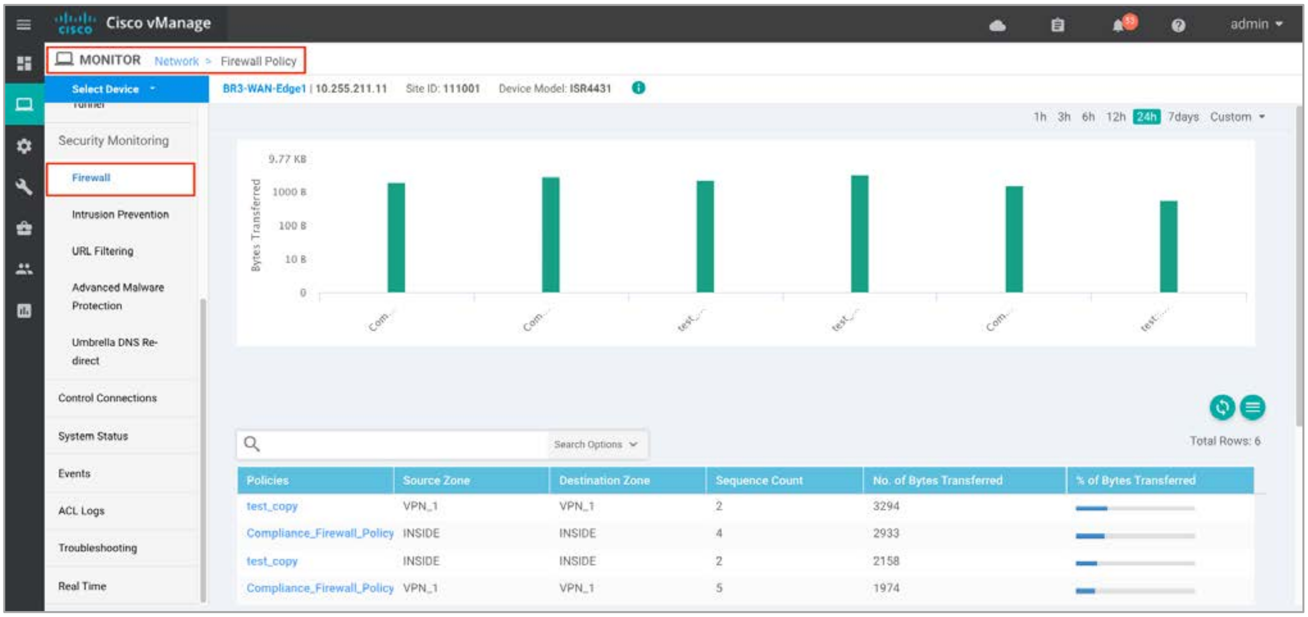
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0
BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0

Step 6 Click the specific WAN Edge device to monitor the firewall policy.



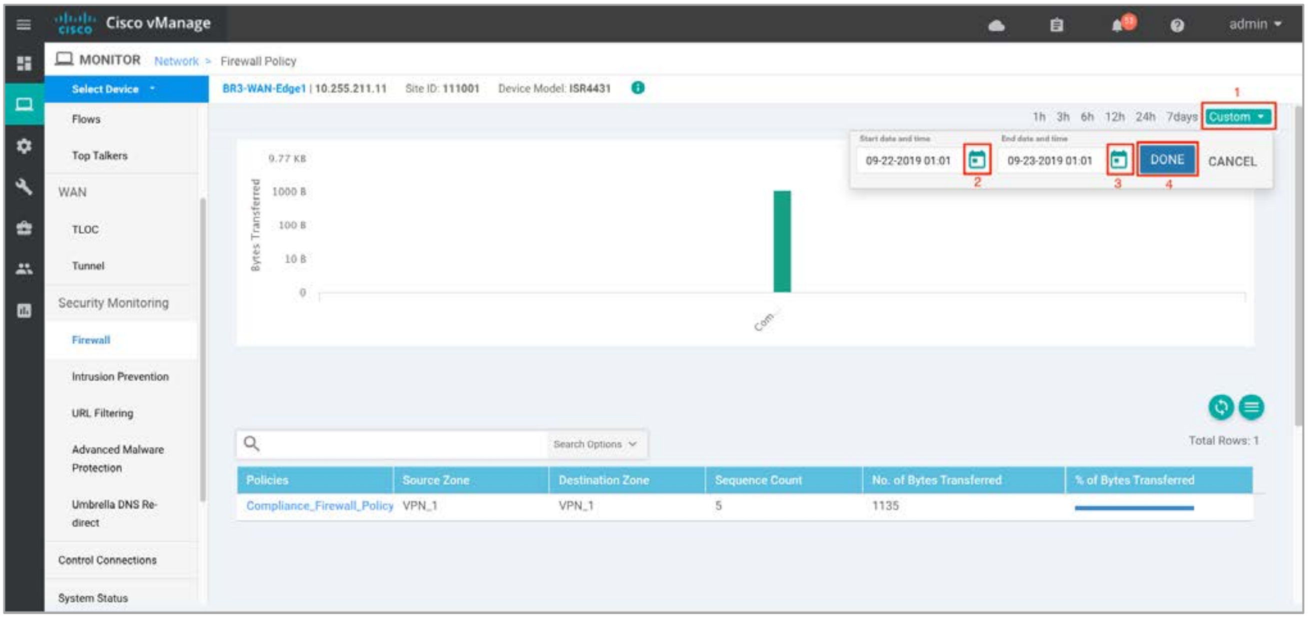
Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control
vsmart	172.27.0.13	vSmart	c44d2744-de58-48f1-8e61-3d655...	✓	reachable	300	--	29
vmanage	172.27.0.14	vManage	b8a4fa09-bf86-4b1a-bb9e-9eb80f...	✓	reachable	400	--	16
vBond	172.27.0.12	vEdge Cloud (vBond)	28a77819-f63a-4a88-b90c-4d81b...	✓	reachable	600	--	--
Router	10.10.23.23	ASR1001-X	ASR1001-X-JAD23151HC8	✓	reachable	23	26	3
DC1-WAN-Edge2	10.255.241.101	vEdge 5000	193A1104180040	✓	reachable	112001	24	3
DC1-WAN-Edge1	10.255.241.102	vEdge 5000	193A1104180039	✓	reachable	112001	24	3
BR6-WAN-Edge1	192.168.1.1	C1111X-8P	C1111X-8P-FGL231613RW	✓	reachable	112010	18	2
BR4-WAN-Edge1	100.255.241.41	ISR4351	ISR4351/K9-FDO18351QNX	✓	reachable	112006	0	2
BR4-WAN-Edge-1	10.255.241.51	C1111X-8P	C1111X-8P-FGL231613RX	✓	reachable	112003	34	3
BR3-WAN-Edge1	10.255.211.11	ISR4431	ISR4431/K9-FOC22467A57	✓	reachable	111001	26	3
BR3-WAN-Edge1	10.255.241.31	ISR4331	ISR4331/K9-FDO2012092A	--	reachable	--	--	--
BR2-WAN-Edge2	10.255.241.22	ISR4331	ISR4331/K9-FDO20110MX6	✓	reachable	112007	7 (8)	2
BR2-WAN-Edge2	10.255.241.62	ISR4461	ISR4461/K9-FDO2316A220	✓	reachable	112005	24	3
BR2-WAN-Edge1	10.255.241.21	ISR4331	ISR4331/K9-FDO20110MX1	✓	reachable	112007	0	2

Step 7 Click the **Firewall Policy** tab under **Security Monitoring** from the left pane. On the dashboard, you can view statistics for all the firewall policies created.



Policies	Source Zone	Destination Zone	Sequence Count	No. of Bytes Transferred	% of Bytes Transferred
test_copy	VPN_1	VPN_1	2	3294	
Compliance_Firewall_Policy	INSIDE	INSIDE	4	2933	
test_copy	INSIDE	INSIDE	2	2158	
Compliance_Firewall_Policy	VPN_1	VPN_1	5	1974	

Step 8 As explained earlier in **Step 4**, the statistics within **Network** > **Firewall** dashboard can be viewed hourly, daily, weekly, or for a customized period. To customize the time period, select **Custom** and then click the calendar icon to input the **Start date and time** followed by the **End Date and time**. Finally, click **Done**.



BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

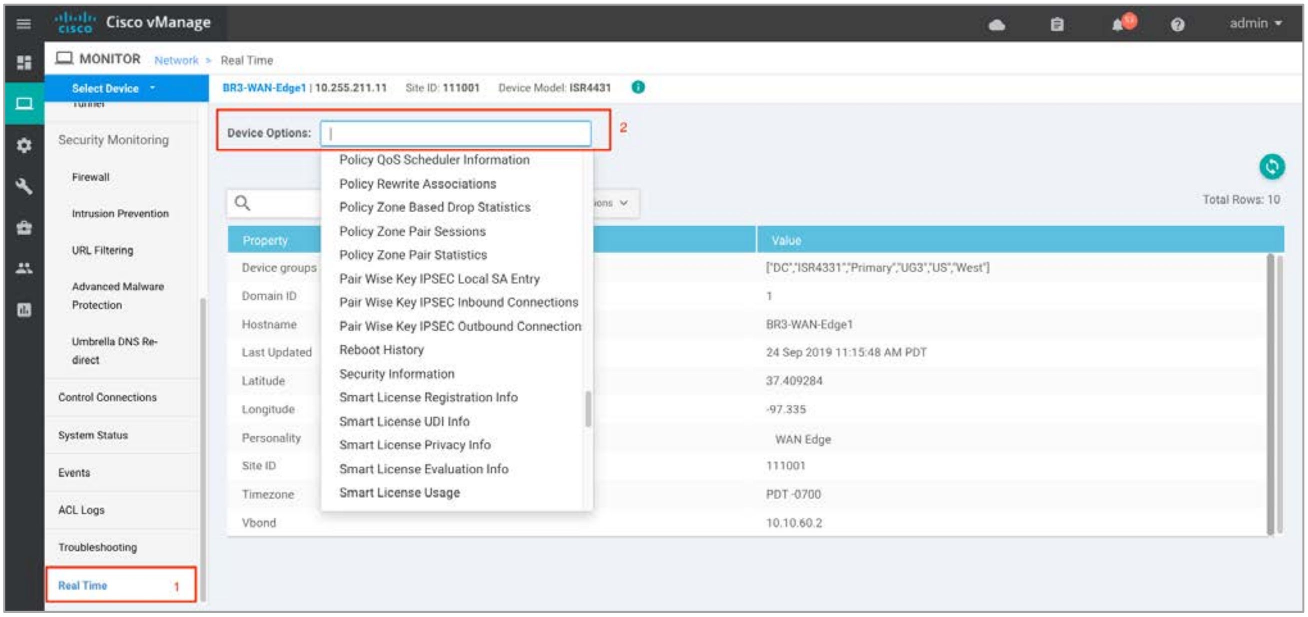
Start date and time: 09-22-2019 01:01

End date and time: 09-23-2019 01:01

Total Rows: 1

Policies	Source Zone	Destination Zone	Sequence Count	No. of Bytes Transferred	% of Bytes Transferred
Compliance_Firewall_Policy	VPN_1	VPN_1	5	1135	

Step 9 Click **Real Time** from the left pane of the monitor dashboard. Within **Network** > **Real time**, a pop-up screen appears with **Device Options**. Click the Search tab to populate a list of options that can be chosen to monitor, troubleshoot, and manage your device.

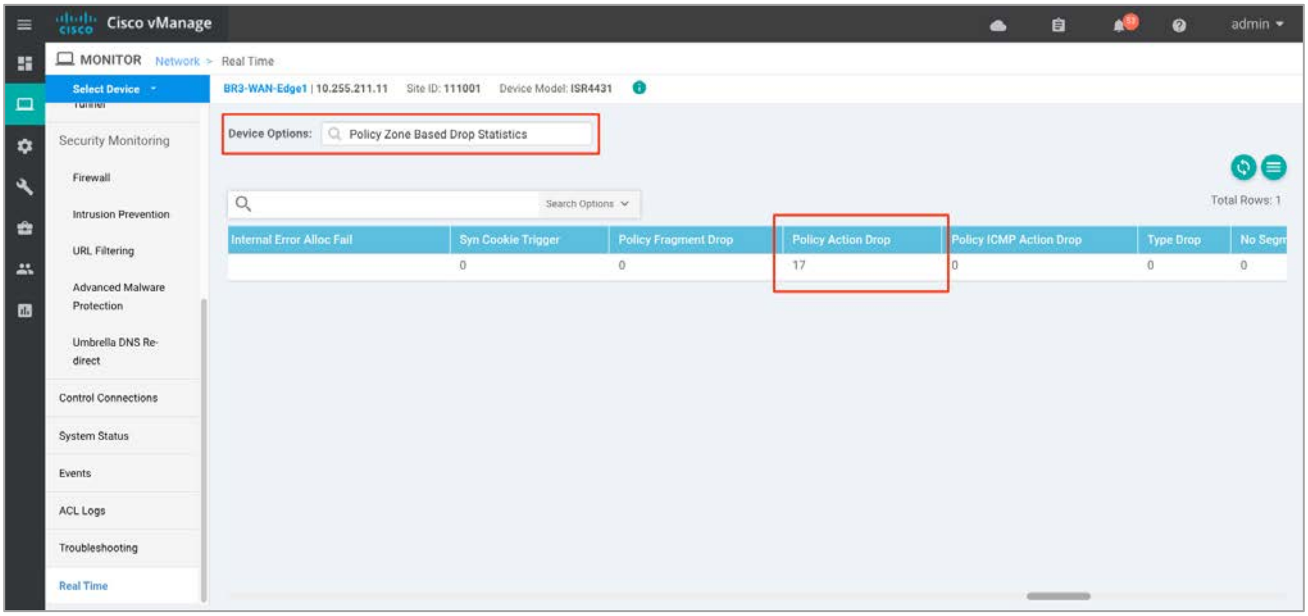

Cisco vManage
admin
MONITOR Network > Real Time
Select Device
Tunnel
Security Monitoring
Firewall
Intrusion Prevention
URL Filtering
Advanced Malware Protection
Umbrella DNS Re-direct
Control Connections
System Status
Events
ACL Logs
Troubleshooting
Real Time
1
2
Device Options:
Policy QoS Scheduler Information
Policy Rewrite Associations
Policy Zone Based Drop Statistics
Policy Zone Pair Sessions
Policy Zone Pair Statistics
Pair Wise Key IPSEC Local SA Entry
Pair Wise Key IPSEC Inbound Connections
Pair Wise Key IPSEC Outbound Connection
Reboot History
Security Information
Smart License Registration Info
Smart License UDI Info
Smart License Privacy Info
Smart License Evaluation Info
Smart License Usage

BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Total Rows: 10

Property	Value
Device groups	["DC","ISR4331","Primary","UG3","US","West"]
Domain ID	1
Hostname	BR3-WAN-Edge1
Last Updated	24 Sep 2019 11:15:48 AM PDT
Latitude	37.409284
Longitude	-97.335
Personality	WAN Edge
Site ID	111001
Timezone	PDT -0700
Vbond	10.10.60.2

Step 10 To view the drop statistics, click **Policy Zone Based Drop Statistics**. This output displays counters that explain the reason for the packet drop. In the figure, notice the drops due to the action set within the policy.



BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: Policy Zone Based Drop Statistics

Total Rows: 1

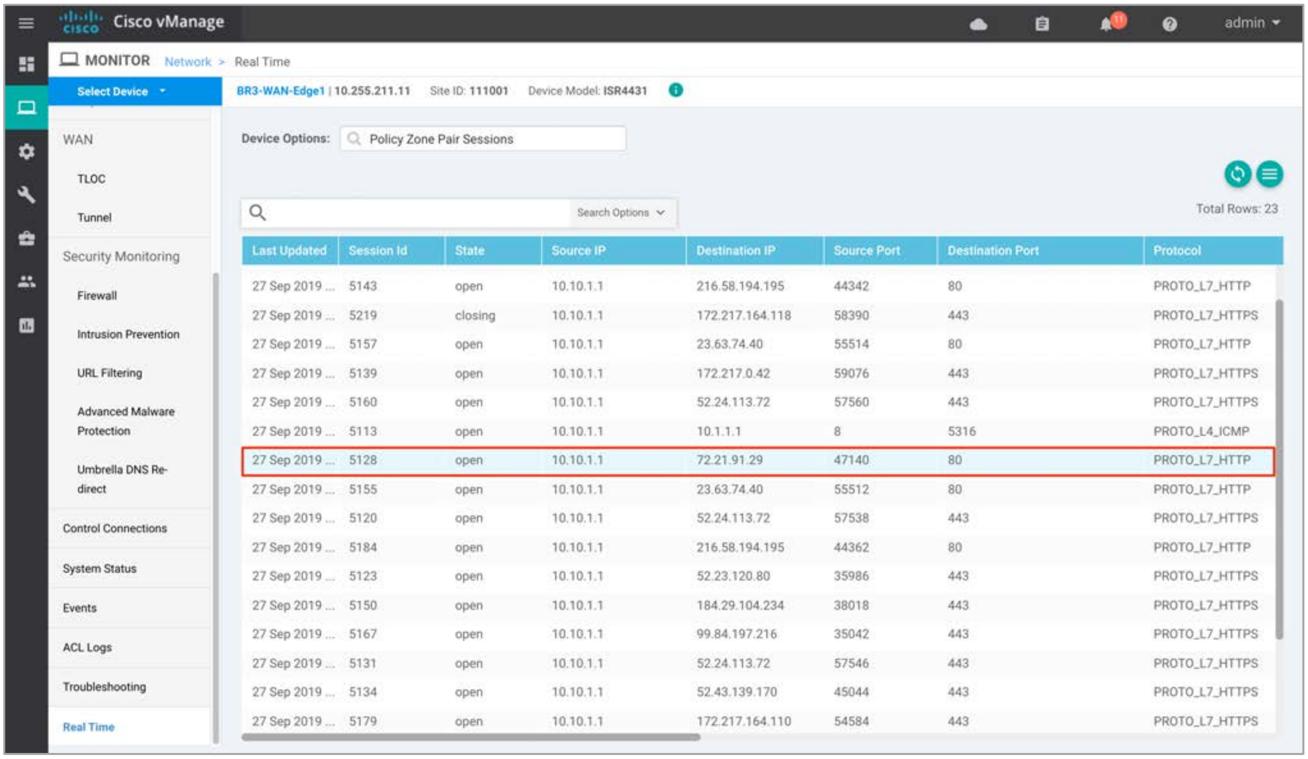
Internal Error Alloc Fail	Syn Cookie Trigger	Policy Fragment Drop	Policy Action Drop	Policy ICMP Action Drop	Type Drop	No Segm
	0	0	17	0	0	0

Some of the other examples of packet drops include, ***TCP Invalid TCP initiator*** when the first packet from a TCP initiator is not a SYN (Non-initial TCP segment is received without a valid session). For instance, the initial SYN packet has the ACK flag set or ***Syn flood*** due to a TCP SYN flood attack.

Refer to the ZBFW troubleshoot Guide to understand the reasons and explanations for firewall drops. Although the document is specific to IOS-XE devices, the explanation for packet drops may be useful.

Step 11 To view the zone pair session details, click **Policy Zone Pair Sessions**.

The output displays the state of the session. It can be open, opening, closing, or closed. For each individual session you can also find the session update timestamp along with the source/ destination IP, source/ destination port and source/ destination VPN for the flow. Scroll further to the right to find the title of the zone pair for the session, the title of the classmap which is the same as the title of the main firewall policy, followed by TCP flag, total initiator bytes, and responder bytes.

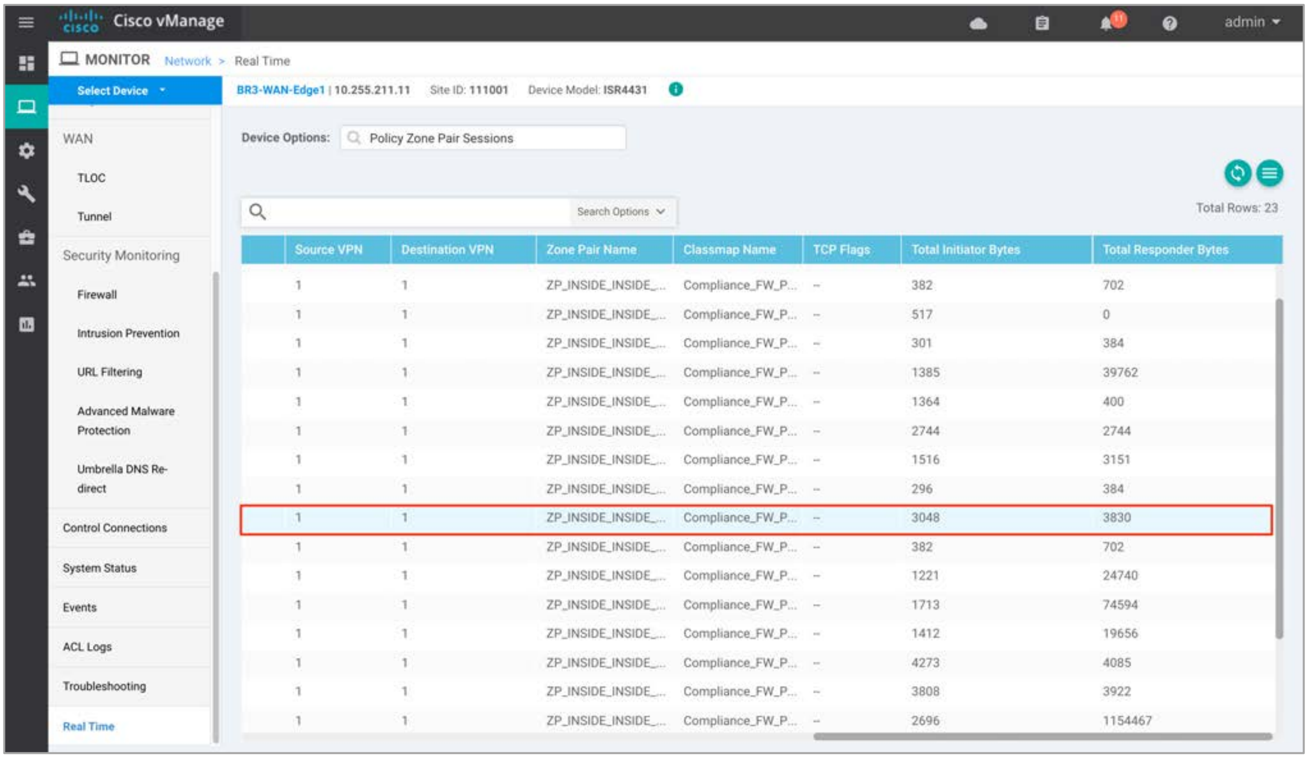


BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: Policy Zone Pair Sessions

Total Rows: 23

Last Updated	Session Id	State	Source IP	Destination IP	Source Port	Destination Port	Protocol
27 Sep 2019 ...	5143	open	10.10.1.1	216.58.194.195	44342	80	PROTO_L7_HTTP
27 Sep 2019 ...	5219	closing	10.10.1.1	172.217.164.118	58390	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5157	open	10.10.1.1	23.63.74.40	55514	80	PROTO_L7_HTTP
27 Sep 2019 ...	5139	open	10.10.1.1	172.217.0.42	59076	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5160	open	10.10.1.1	52.24.113.72	57560	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5113	open	10.10.1.1	10.1.1.1	8	5316	PROTO_L4_ICMP
27 Sep 2019 ...	5128	open	10.10.1.1	72.21.91.29	47140	80	PROTO_L7_HTTP
27 Sep 2019 ...	5155	open	10.10.1.1	23.63.74.40	55512	80	PROTO_L7_HTTP
27 Sep 2019 ...	5120	open	10.10.1.1	52.24.113.72	57538	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5184	open	10.10.1.1	216.58.194.195	44362	80	PROTO_L7_HTTP
27 Sep 2019 ...	5123	open	10.10.1.1	52.23.120.80	35986	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5150	open	10.10.1.1	184.29.104.234	38018	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5167	open	10.10.1.1	99.84.197.216	35042	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5131	open	10.10.1.1	52.24.113.72	57546	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5134	open	10.10.1.1	52.43.139.170	45044	443	PROTO_L7_HTTPS
27 Sep 2019 ...	5179	open	10.10.1.1	172.217.164.110	54584	443	PROTO_L7_HTTPS



BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

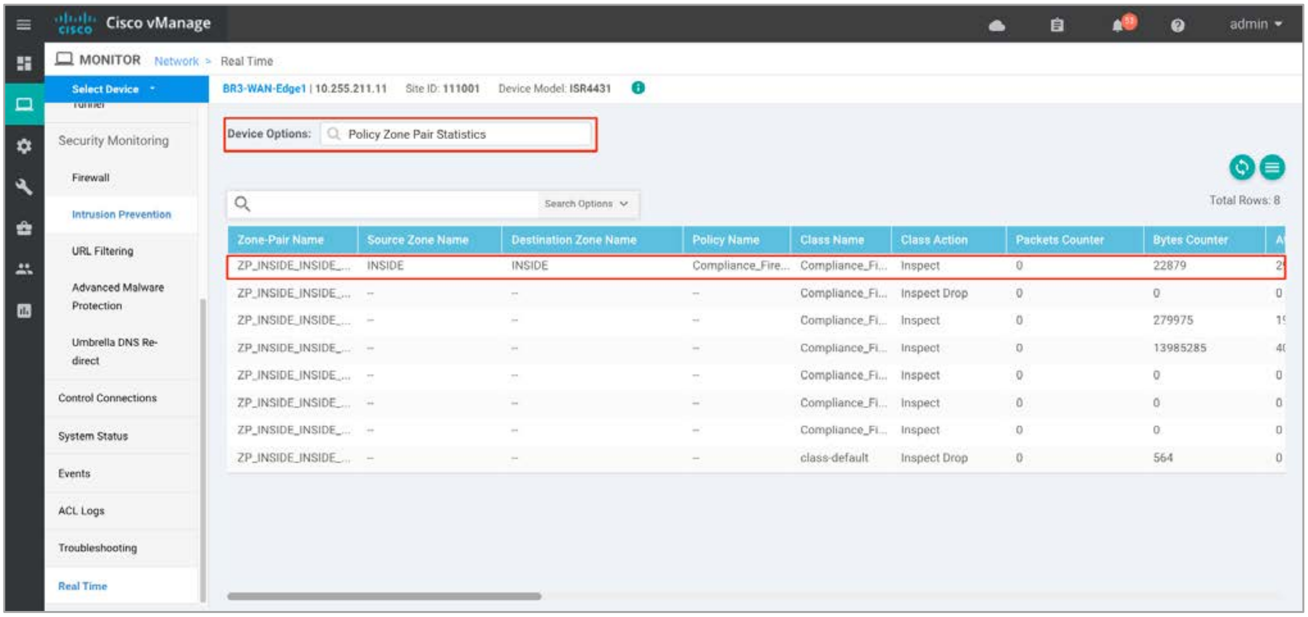
Device Options: Policy Zone Pair Sessions

Total Rows: 23

	Source VPN	Destination VPN	Zone Pair Name	Classmap Name	TCP Flags	Total Initiator Bytes	Total Responder Bytes
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	382	702
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	517	0
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	301	384
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	1385	39762
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	1364	400
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	2744	2744
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	1516	3151
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	296	384
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	3048	3830
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	382	702
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	1221	24740
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	1713	74594
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	1412	19656
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	4273	4085
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	3808	3922
	1	1	ZP_INSIDE_INSIDE_...	Compliance_FW_P...	--	2696	1154467

Step 12 To view zone pair statistics, click **Policy Zone Pair Statistics**. Within this output, you can view the byte counters, attempted/ active/ half-open/ terminating sessions per zone-pair along with the policy title, protocol of the packet ,and the action applied to the packet.

In the figure, notice that the action applied for two out of eight zone pairs is Inspect Drop.



BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: Policy Zone Pair Statistics

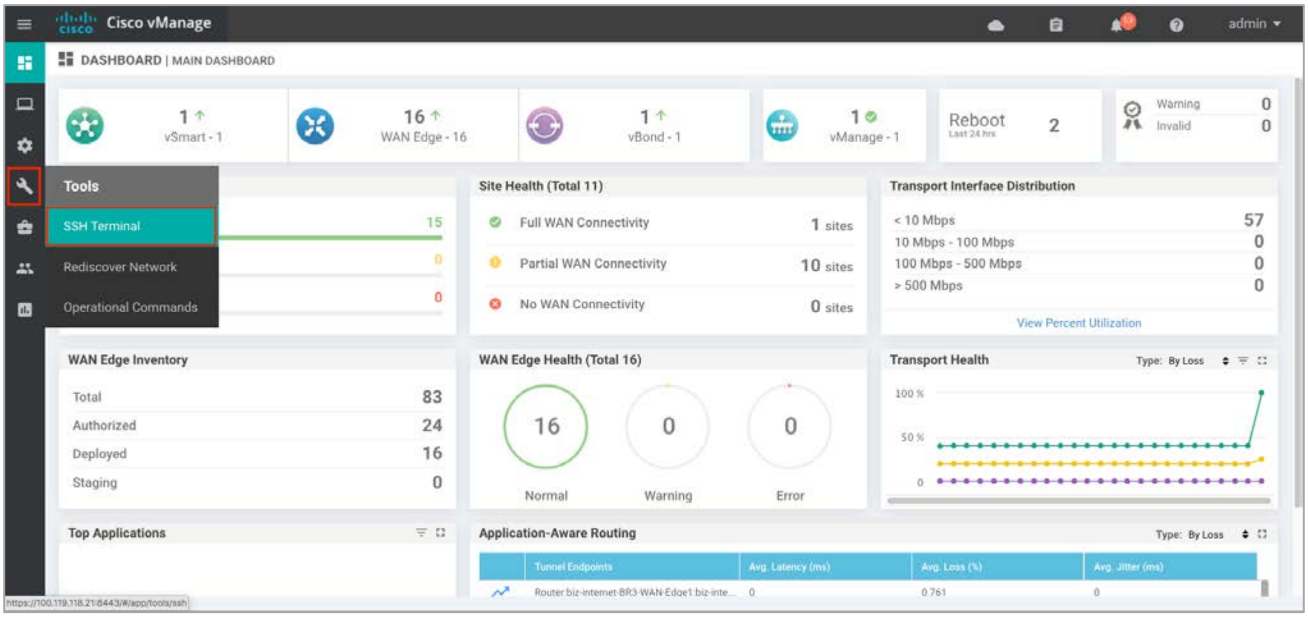
Total Rows: 8

Zone-Pair Name	Source Zone Name	Destination Zone Name	Policy Name	Class Name	Class Action	Packets Counter	Bytes Counter	A
ZP_INSIDE_INSIDE_...	INSIDE	INSIDE	Compliance_Fire...	Compliance_Fi...	Inspect	0	22879	2
ZP_INSIDE_INSIDE_...	--	--	--	Compliance_Fi...	Inspect Drop	0	0	0
ZP_INSIDE_INSIDE_...	--	--	--	Compliance_Fi...	Inspect	0	279975	1
ZP_INSIDE_INSIDE_...	--	--	--	Compliance_Fi...	Inspect	0	13985285	4
ZP_INSIDE_INSIDE_...	--	--	--	Compliance_Fi...	Inspect	0	0	0
ZP_INSIDE_INSIDE_...	--	--	--	Compliance_Fi...	Inspect	0	0	0
ZP_INSIDE_INSIDE_...	--	--	--	Compliance_Fi...	Inspect	0	0	0
ZP_INSIDE_INSIDE_...	--	--	--	class-default	Inspect Drop	0	564	0

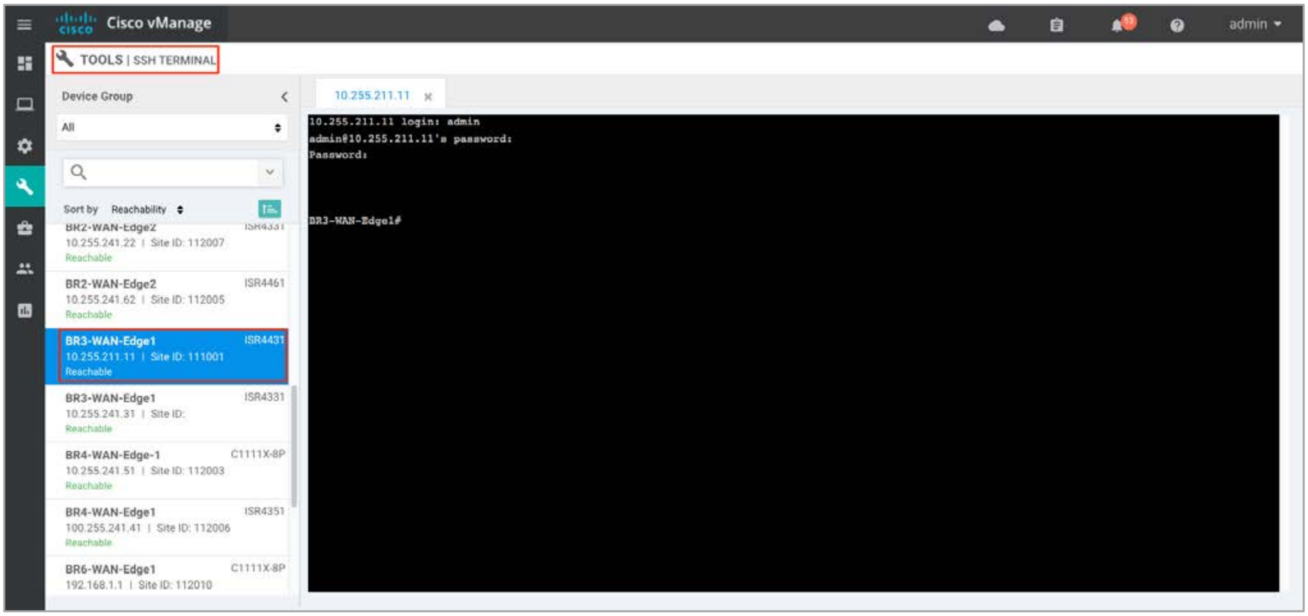
Method 3: Monitor the Firewall Feature and Statistics Using vManage SSH Server Dashboard

Using the vManage NMS dashboard, you can monitor the traffic flow through the policy using CLI commands.

Step 1 Navigate to **Tools** > **SSH Terminal** available in the left pane.

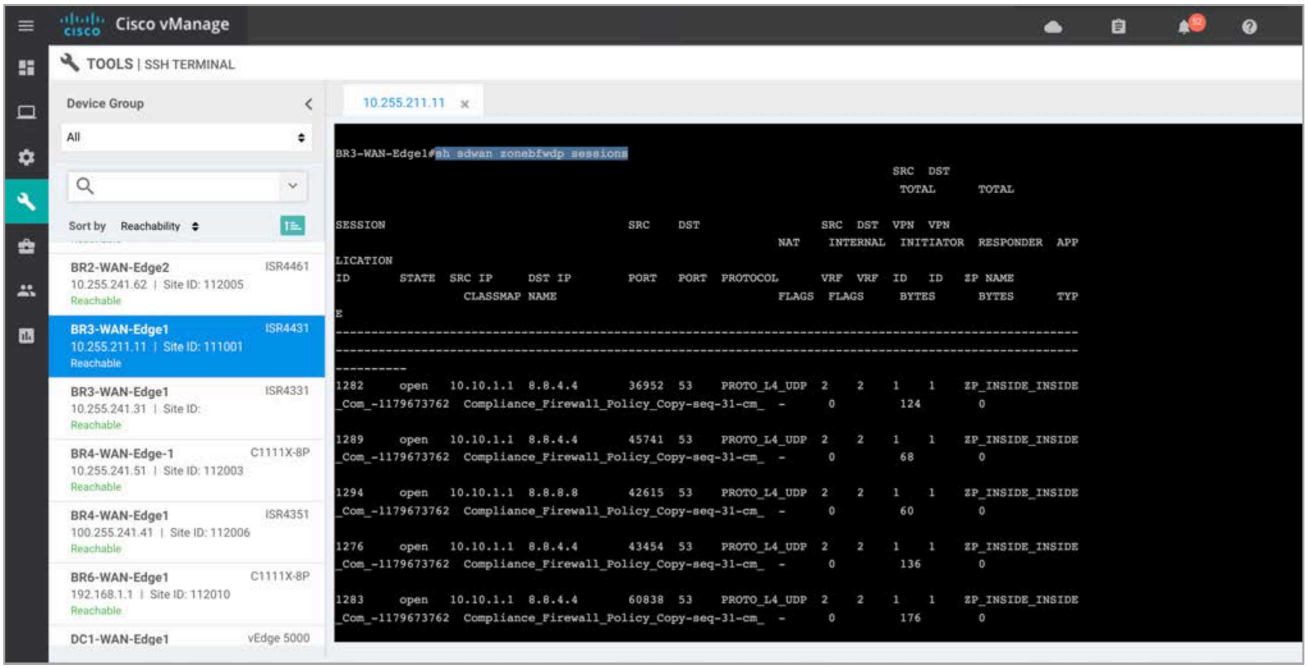


Step 2 Select the device from the list of devices and log in.



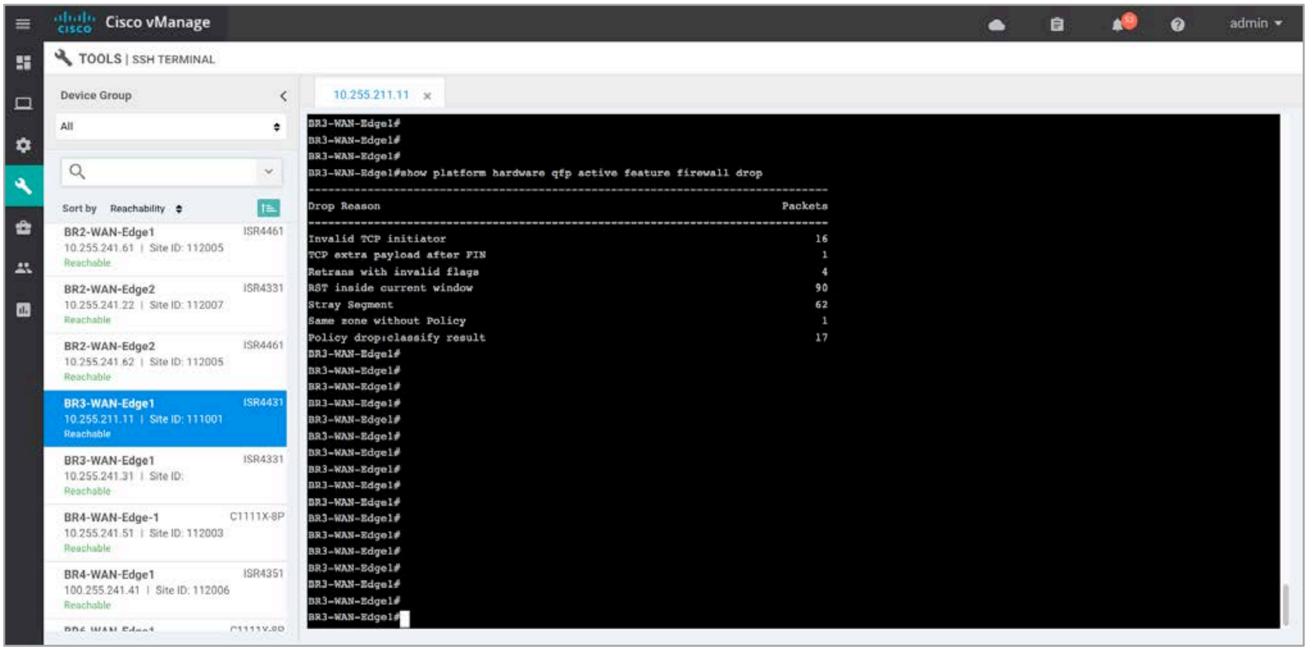
```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:

BR3-WAN-Edge1#
```

Step 3 Enter the CLI command to view the existing firewall sessions – `show sdwan zonebfwdp sessions`.



```
BR3-WAN-Edge1#sh sdwan zonebfwdp sessions
                                                                               SRC  DST
                                                                                TOTAL      TOTAL

SESSION                                   SRC    DST                 SRC  DST  VPN  VPN
                                                               NAT    INTERNAL  INITIATOR  RESPONDER  APP
LICATION
ID       STATE  SRC IP     DST IP         PORT   PORT  PROTOCOL      VRF  VRF  ID   ID   ZP NAME
                  CLASSMAP NAME                                FLAGS  FLAGS     BYTES      BYTES      TYP
E
---------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------
----------
1282     open   10.10.1.1  8.8.4.4        36952  53    PROTO_L4_UDP  2    2    1    1    ZP_INSIDE_INSIDE
_Com_-1179673762  Compliance_Firewall_Policy_Copy-seq-31-cm_   -      0         124        0

1289     open   10.10.1.1  8.8.4.4        45741  53    PROTO_L4_UDP  2    2    1    1    ZP_INSIDE_INSIDE
_Com_-1179673762  Compliance_Firewall_Policy_Copy-seq-31-cm_   -      0         68         0

1294     open   10.10.1.1  8.8.8.8        42615  53    PROTO_L4_UDP  2    2    1    1    ZP_INSIDE_INSIDE
_Com_-1179673762  Compliance_Firewall_Policy_Copy-seq-31-cm_   -      0         60         0

1276     open   10.10.1.1  8.8.4.4        43454  53    PROTO_L4_UDP  2    2    1    1    ZP_INSIDE_INSIDE
_Com_-1179673762  Compliance_Firewall_Policy_Copy-seq-31-cm_   -      0         136        0

1283     open   10.10.1.1  8.8.4.4        60838  53    PROTO_L4_UDP  2    2    1    1    ZP_INSIDE_INSIDE
_Com_-1179673762  Compliance_Firewall_Policy_Copy-seq-31-cm_   -      0         176        0
```

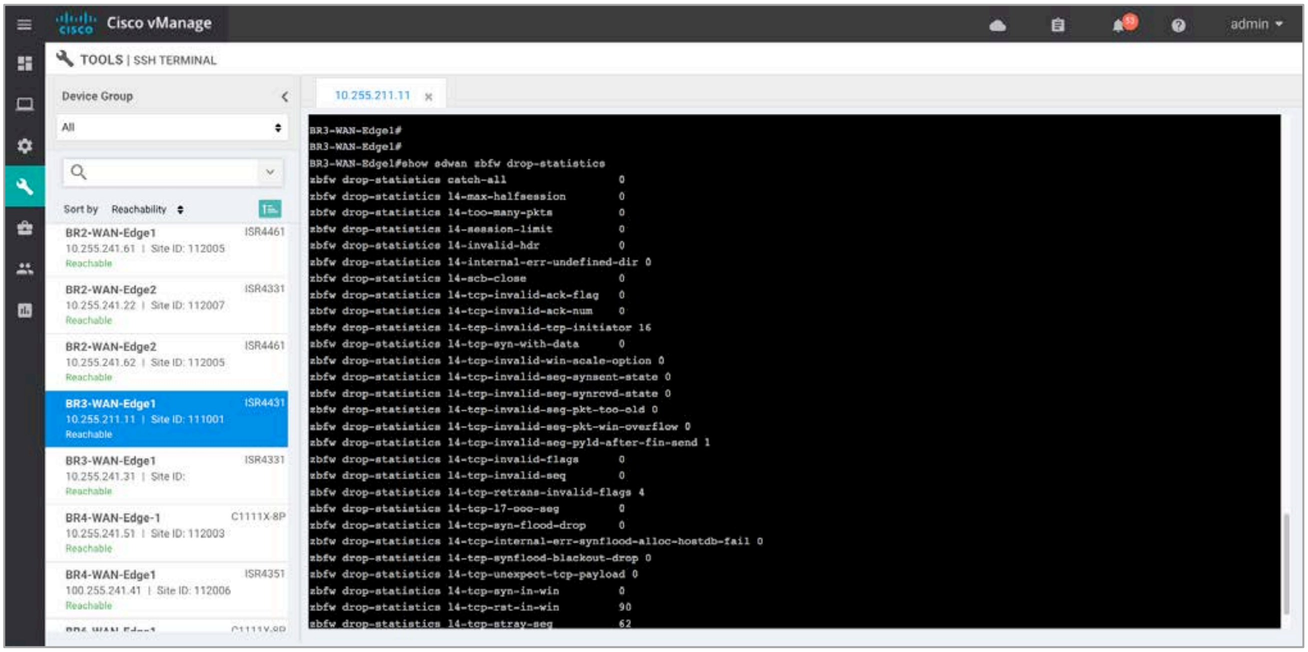
Step 4 Enter the CLI command to view the firewall drop counters - `show platform hardware qfp active feature firewall drop`.


Cisco vManage
admin
TOOLS | SSH TERMINAL
Device Group
All
Sort by Reachability
BR2-WAN-Edge1 ISR4461 10.255.241.61 | Site ID: 112005 Reachable
BR2-WAN-Edge2 ISR4331 10.255.241.22 | Site ID: 112007 Reachable
BR2-WAN-Edge2 ISR4461 10.255.241.62 | Site ID: 112005 Reachable
BR3-WAN-Edge1 ISR4431 10.255.211.11 | Site ID: 111001 Reachable
BR3-WAN-Edge1 ISR4331 10.255.241.31 | Site ID: Reachable
BR4-WAN-Edge-1 C1111X-8P 10.255.241.51 | Site ID: 112003 Reachable
BR4-WAN-Edge1 ISR4351 100.255.241.41 | Site ID: 112006 Reachable
10.255.211.11

```
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#show platform hardware qfp active feature firewall drop
-------------------------------------------------------------------------------
Drop Reason                                                              Packets
-------------------------------------------------------------------------------
Invalid TCP initiator                                                         16
TCP extra payload after FIN                                                    1
Retrans with invalid flags                                                     4
RST inside current window                                                     90
Stray Segment                                                                 62
Same zone without Policy                                                       1
Policy drop:classify result                                                   17
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#
```

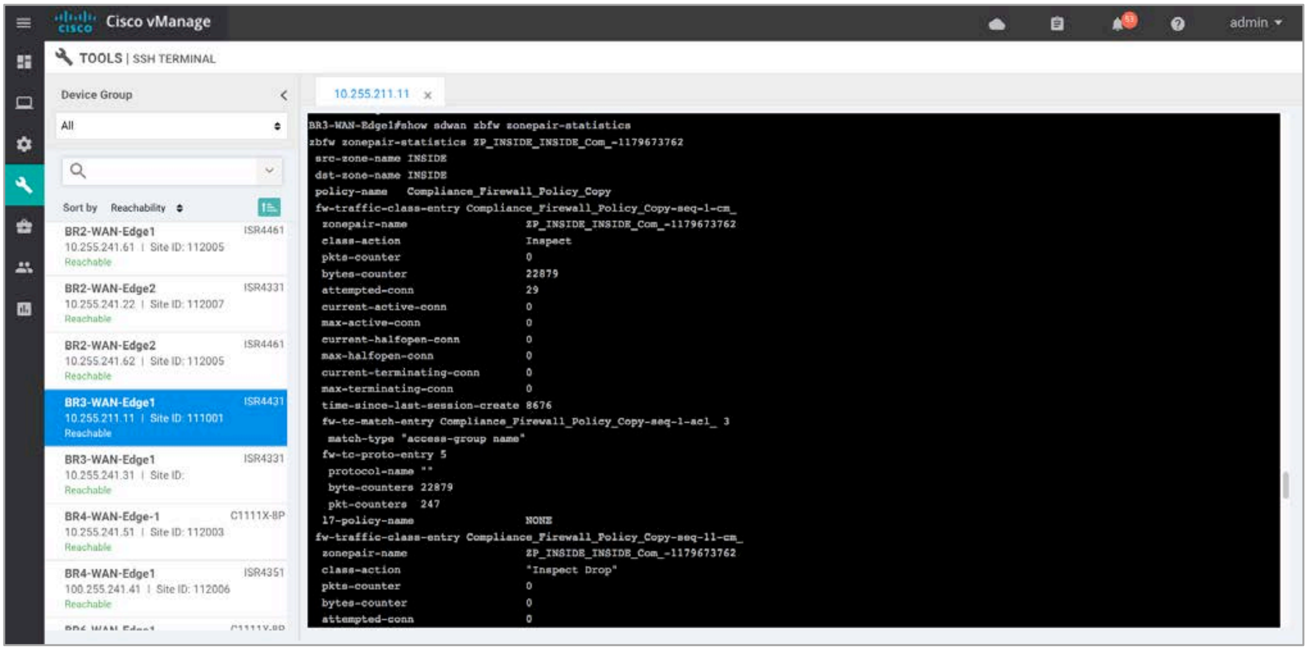
Technical Tip: Clear the drop counters before troubleshooting firewall packet drop. To do so, use the command `show platform hardware qfp active feature firewall drop clear`.

Step 5 To view the overall firewall, drop statistics, enter CLI command `show sdwan zbfw drop-statistics`.


Cisco vManage
admin
TOOLS | SSH TERMINAL
Device Group
All
Sort by Reachability
BR2-WAN-Edge1 ISR4461 10.255.241.61 | Site ID: 112005 Reachable
BR2-WAN-Edge2 ISR4331 10.255.241.22 | Site ID: 112007 Reachable
BR2-WAN-Edge2 ISR4461 10.255.241.62 | Site ID: 112005 Reachable
BR3-WAN-Edge1 ISR4431 10.255.211.11 | Site ID: 111001 Reachable
BR3-WAN-Edge1 ISR4331 10.255.241.31 | Site ID: Reachable
BR4-WAN-Edge-1 C1111X-8P 10.255.241.51 | Site ID: 112003 Reachable
BR4-WAN-Edge1 ISR4351 100.255.241.41 | Site ID: 112006 Reachable
10.255.211.11

```
BR3-WAN-Edge1#
BR3-WAN-Edge1#
BR3-WAN-Edge1#show sdwan zbfw drop-statistics
zbfw drop-statistics catch-all                 0
zbfw drop-statistics l4-max-halfsession        0
zbfw drop-statistics l4-too-many-pkts          0
zbfw drop-statistics l4-session-limit          0
zbfw drop-statistics l4-invalid-hdr            0
zbfw drop-statistics l4-internal-err-undefined-dir 0
zbfw drop-statistics l4-scb-close              0
zbfw drop-statistics l4-tcp-invalid-ack-flag   0
zbfw drop-statistics l4-tcp-invalid-ack-num    0
zbfw drop-statistics l4-tcp-invalid-tcp-initiator 16
zbfw drop-statistics l4-tcp-syn-with-data      0
zbfw drop-statistics l4-tcp-invalid-win-scale-option 0
zbfw drop-statistics l4-tcp-invalid-seg-synsent-state 0
zbfw drop-statistics l4-tcp-invalid-seg-synrcvd-state 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-too-old 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-win-overflow 0
zbfw drop-statistics l4-tcp-invalid-seg-pyld-after-fin-send 1
zbfw drop-statistics l4-tcp-invalid-flags      0
zbfw drop-statistics l4-tcp-invalid-seq        0
zbfw drop-statistics l4-tcp-retrans-invalid-flags 4
zbfw drop-statistics l4-tcp-l7-ooo-seg         0
zbfw drop-statistics l4-tcp-syn-flood-drop     0
zbfw drop-statistics l4-tcp-internal-err-synflood-alloc-hostdb-fail 0
zbfw drop-statistics l4-tcp-synflood-blackout-drop 0
zbfw drop-statistics l4-tcp-unexpect-tcp-payload 0
zbfw drop-statistics l4-tcp-syn-in-win         0
zbfw drop-statistics l4-tcp-rst-in-win         90
zbfw drop-statistics l4-tcp-stray-seg          62
```

Step 6 Enter the CLI command `show sdwan zbfw zonepair-statistics` to view the zone-pair statistics.


Cisco vManage
admin
TOOLS | SSH TERMINAL
Device Group
All
Sort by Reachability
BR2-WAN-Edge1 ISR4461 10.255.241.61 | Site ID: 112005 Reachable
BR2-WAN-Edge2 ISR4331 10.255.241.22 | Site ID: 112007 Reachable
BR2-WAN-Edge2 ISR4461 10.255.241.62 | Site ID: 112005 Reachable
BR3-WAN-Edge1 ISR4431 10.255.211.11 | Site ID: 111001 Reachable
BR3-WAN-Edge1 ISR4331 10.255.241.31 | Site ID: Reachable
BR4-WAN-Edge-1 C1111X-8P 10.255.241.51 | Site ID: 112003 Reachable
BR4-WAN-Edge1 ISR4351 100.255.241.41 | Site ID: 112006 Reachable
10.255.211.11

```
BR3-WAN-Edge1#show sdwan zbfw zonepair-statistics
zbfw zonepair-statistics ZP_INSIDE_INSIDE_Com_-1179673762
 src-zone-name INSIDE
 dst-zone-name INSIDE
 policy-name   Compliance_Firewall_Policy_Copy
 fw-traffic-class-entry Compliance_Firewall_Policy_Copy-seq-1-cm_
  zonepair-name                  ZP_INSIDE_INSIDE_Com_-1179673762
  class-action                   Inspect
  pkts-counter                   0
  bytes-counter                  22879
  attempted-conn                 29
  current-active-conn            0
  max-active-conn                0
  current-halfopen-conn          0
  max-halfopen-conn              0
  current-terminating-conn       0
  max-terminating-conn           0
  time-since-last-session-create 8676
  fw-tc-match-entry Compliance_Firewall_Policy_Copy-seq-1-acl_ 3
   match-type "access-group name"
  fw-tc-proto-entry 5
   protocol-name ""
   byte-counters 22879
   pkt-counters  247
  l7-policy-name                 NONE
 fw-traffic-class-entry Compliance_Firewall_Policy_Copy-seq-11-cm_
  zonepair-name                  ZP_INSIDE_INSIDE_Com_-1179673762
  class-action                   "Inspect Drop"
  pkts-counter                   0
  bytes-counter                  0
  attempted-conn                 0
```

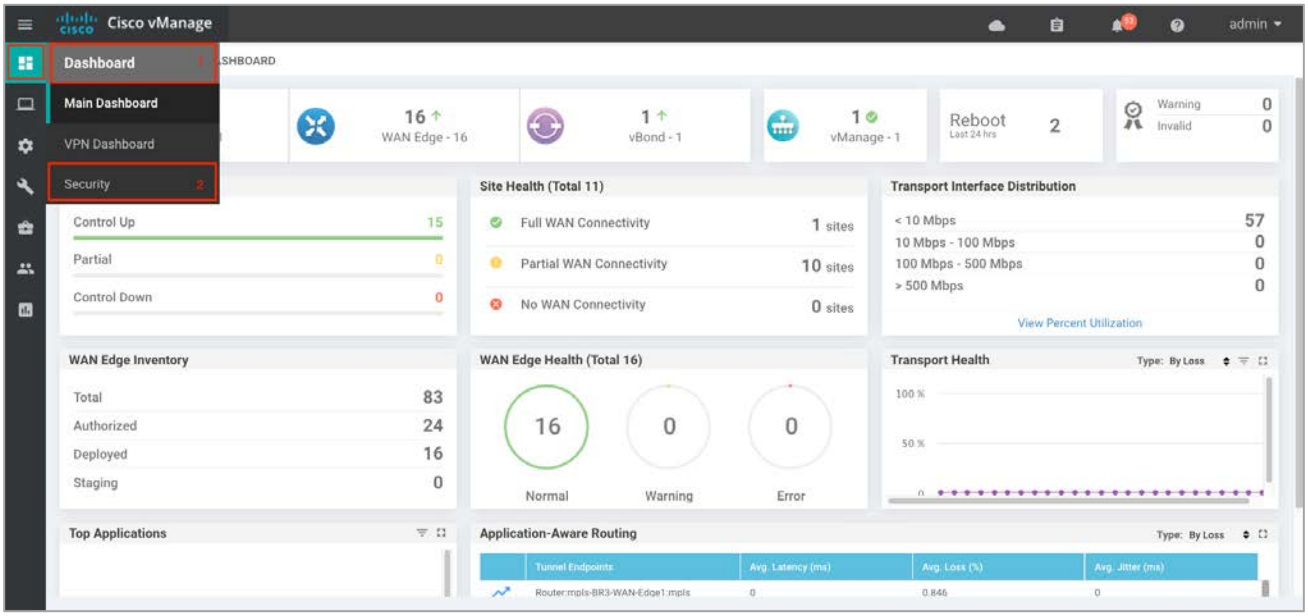
Step 7 Besides theCLI commands listed previously, some other useful CLI commands are `show log` and `show zone security` to view error logs and zone pairs.

Process 2: Monitor IPS Feature Using vManage NMS

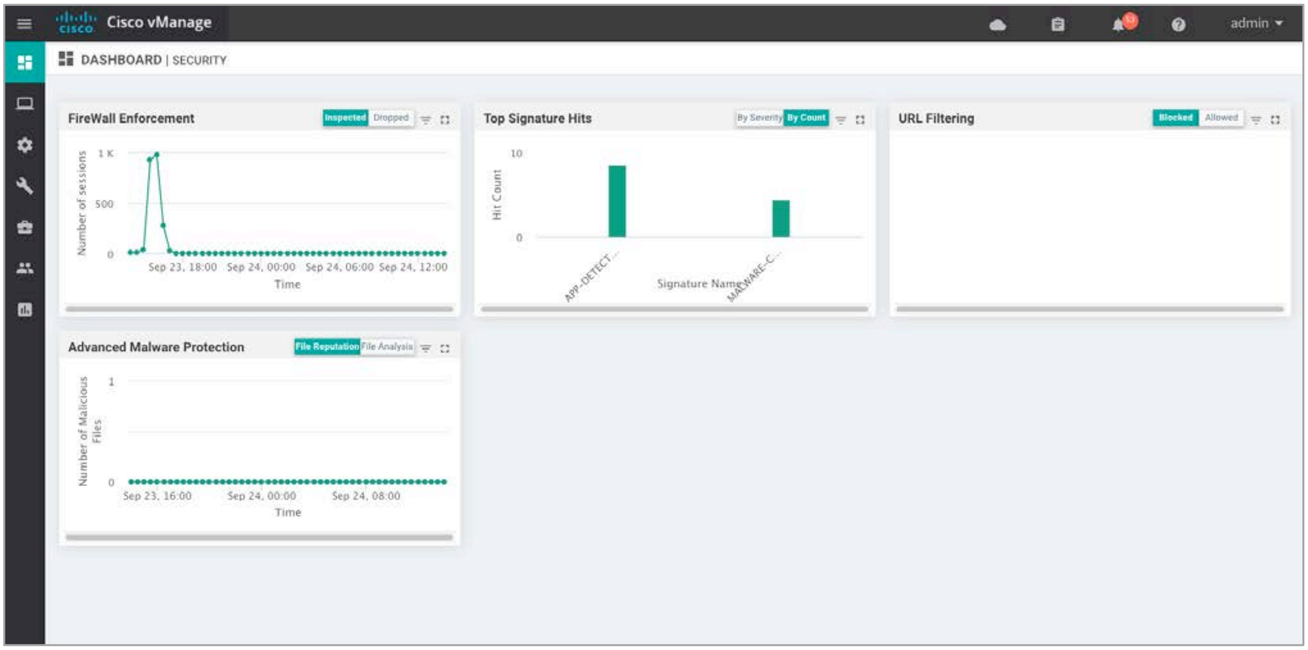
Method 1: Monitor IPS Signature Violations via vManage Main Dashboard

Using vManage NMS, you can monitor the IPS signature violations and analyze them further.

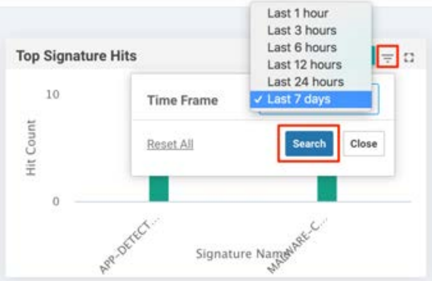
Navigate to **Dashboard** > **Security.**



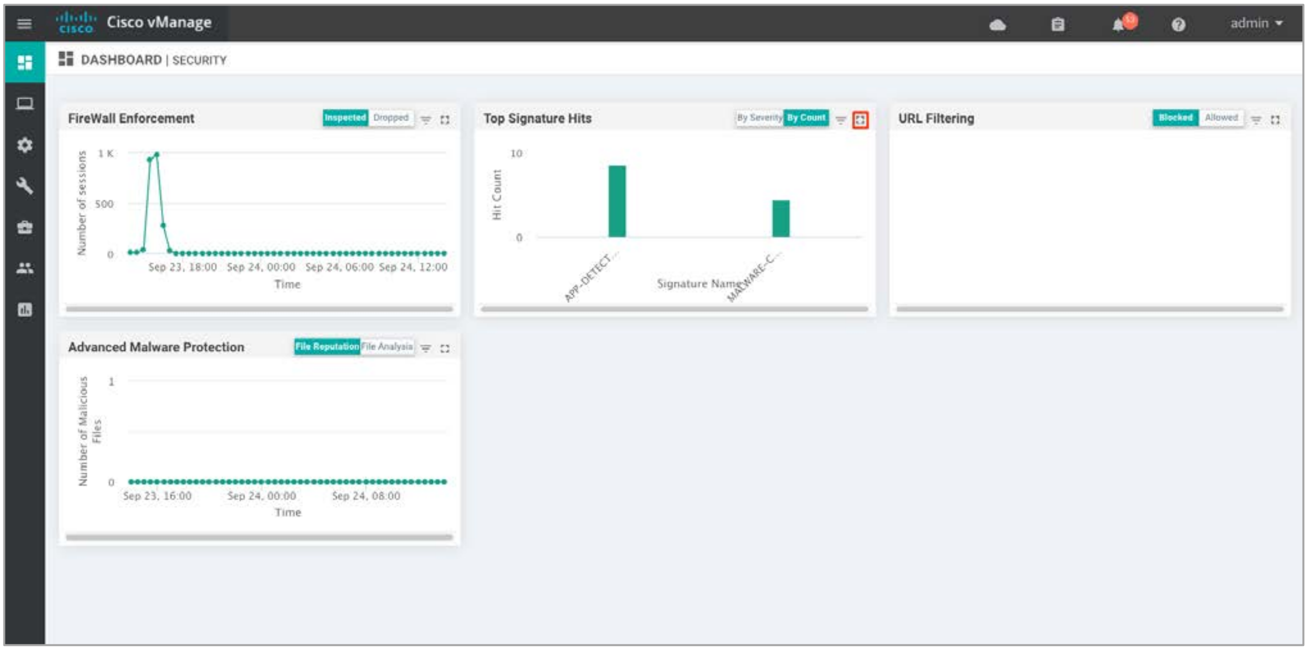
Step 8 The following screenshot of the security dashboard shows the **Top Signature Hits** data.



Technical Tip: Within the IPS graphic display, drill down for hourly, daily and weekly graphic representation.

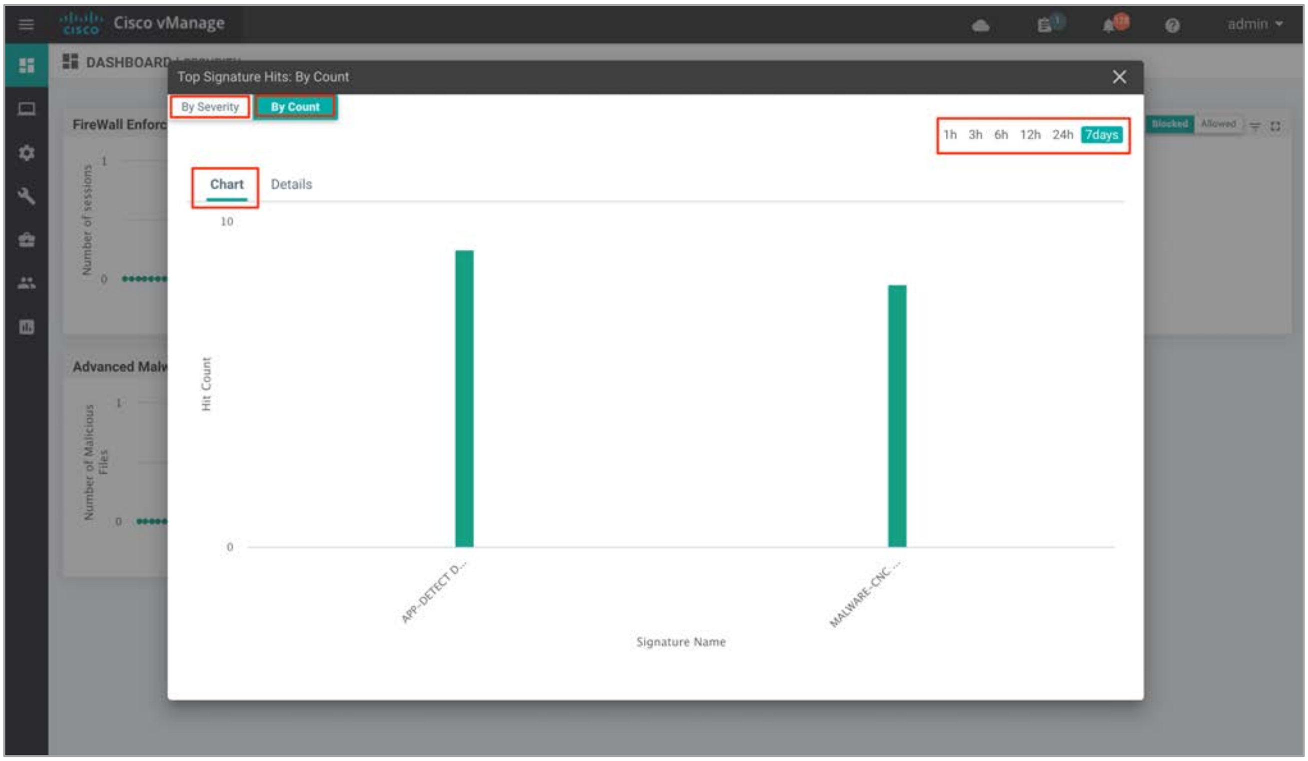


Step 9 To take a closer look at the **Signature Hits** graph, click the square box **[]** on the top right.

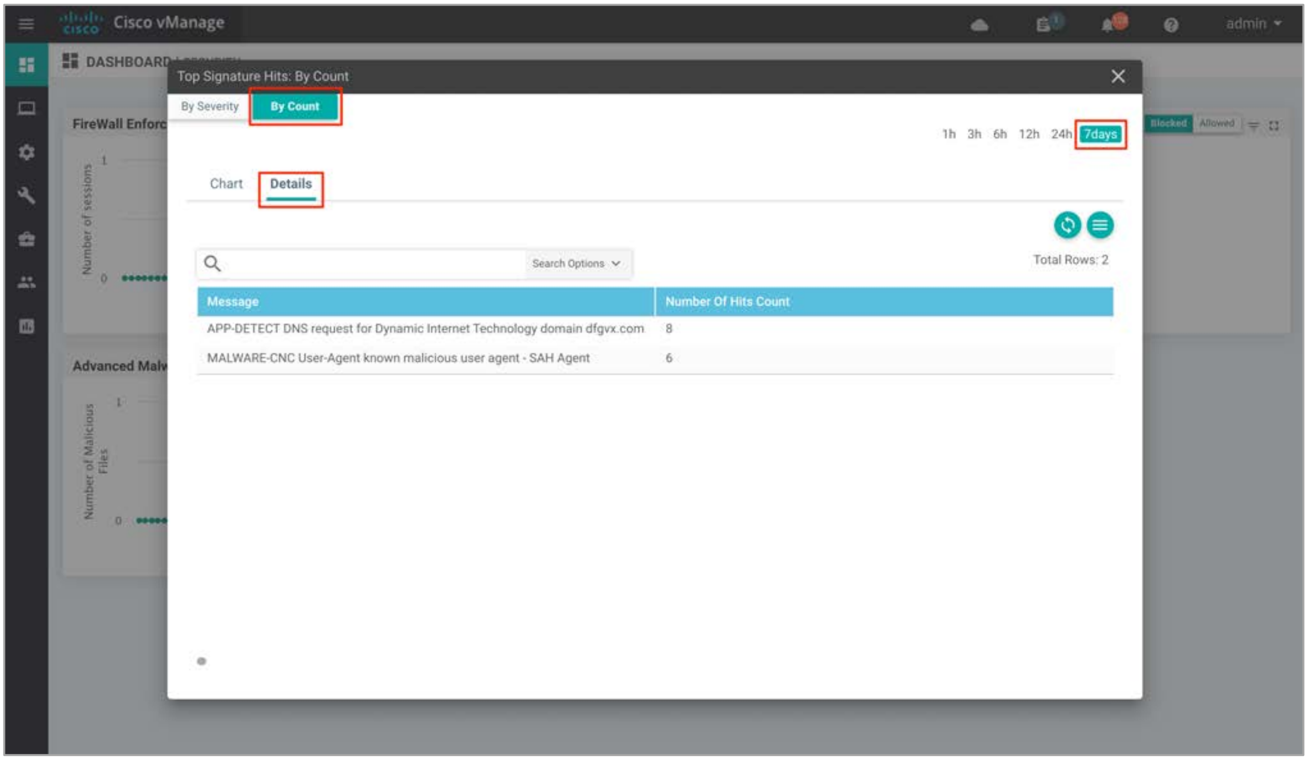


Drilling down into firewall graph provides more information. View top signature hits **By Severity** or **By Count** for 1h, 3h, 6h, 12h, 24h (default) or 7 days.

The **By Count** and **Chart** options display the graphic representation of the top signature hits.



The **By Count**, **Details** options display the hit count per signature.

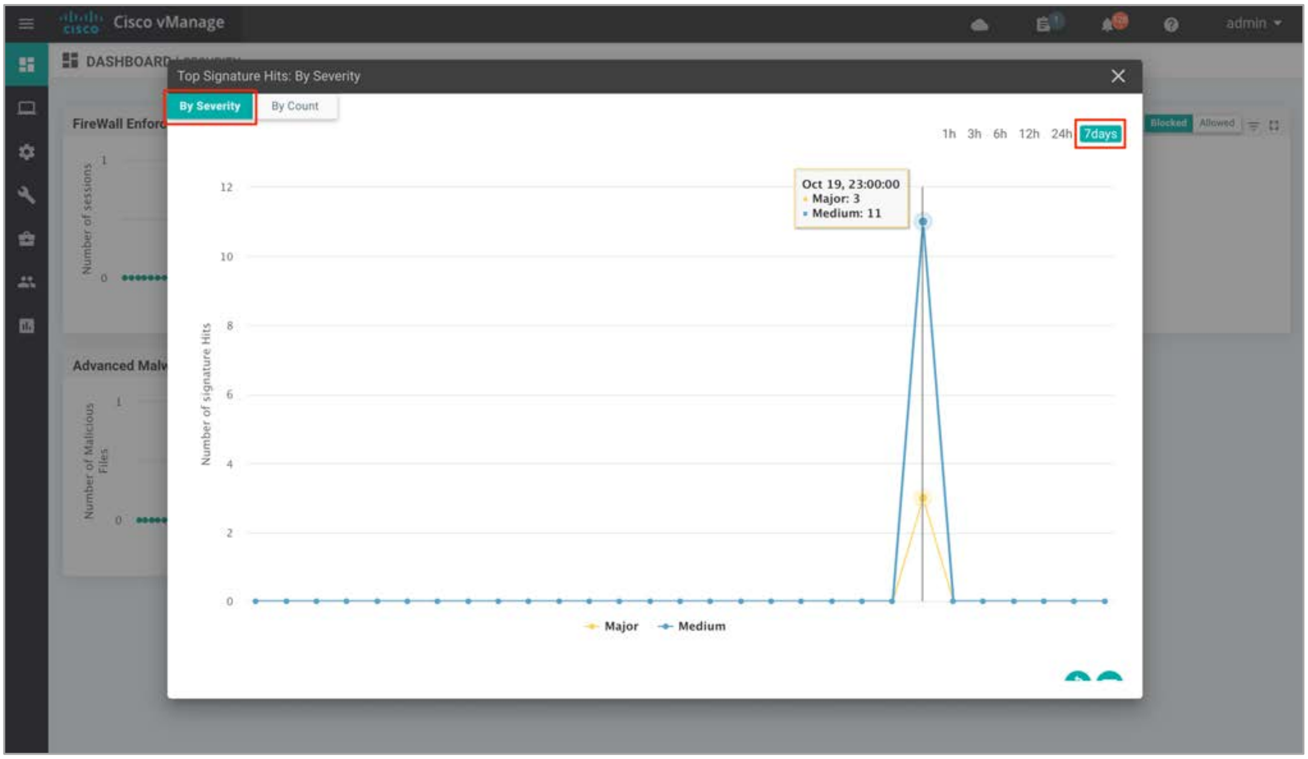


Top Signature Hits: By Count

Total Rows: 2

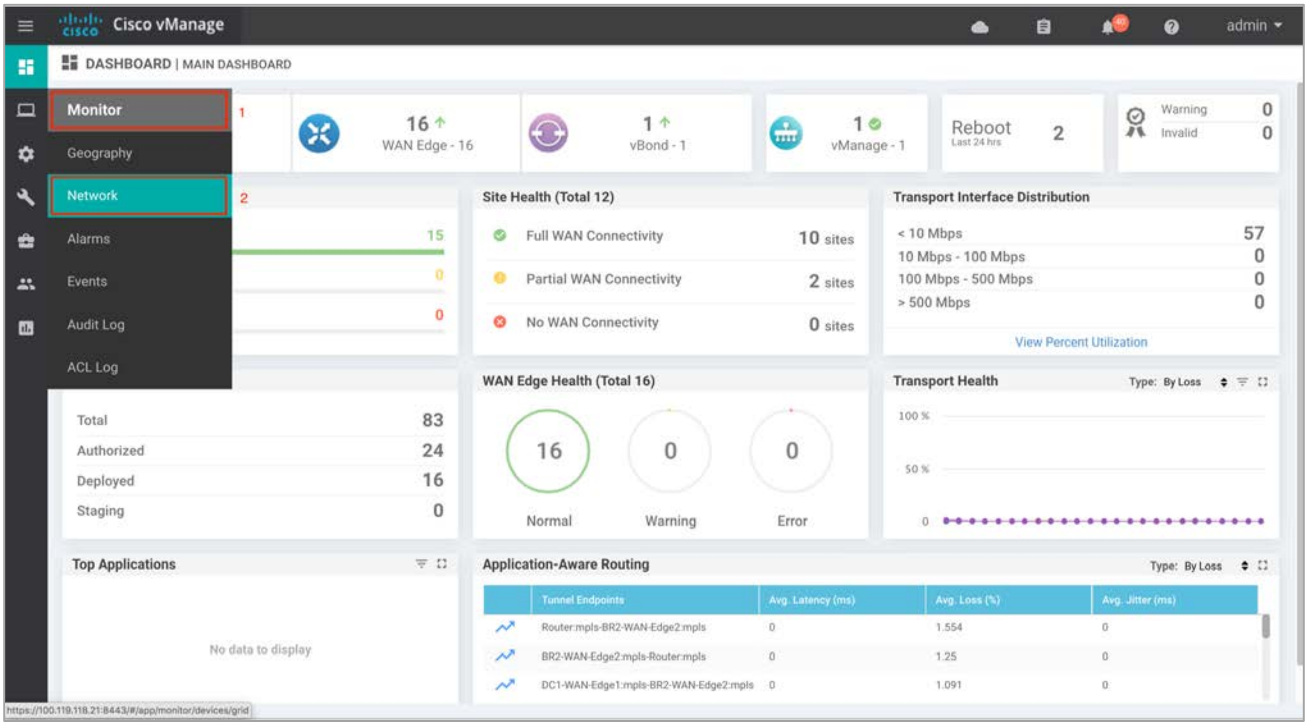
Message	Number Of Hits Count
APP-DETECT DNS request for Dynamic Internet Technology domain dfgvx.com	8
MALWARE-CNC User-Agent known malicious user agent - SAH Agent	6

The **By Severity** area shows the the number of major and minor signature hits.



Method 2: Monitor IPS Feature Using vManage Monitor Dashboard

Step 1 Navigate to **Network** from the **Monitor option** available on the left pane.


Cisco vManage
admin
DASHBOARD | MAIN DASHBOARD
Monitor
1
Geography
Network
2
Alarms
Events
Audit Log
ACL Log
https://100.119.118.21:8443/#/app/monitor/devices/grid

16 WAN Edge - 16

1 vBond - 1

1 vManage - 1

Reboot 2 Last 24 hrs

Warning 0

Invalid 0

15

0

0

Site Health (Total 12)

Full WAN Connectivity	10 sites
Partial WAN Connectivity	2 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

< 10 Mbps	57
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

Total	83
Authorized	24
Deployed	16
Staging	0

WAN Edge Health (Total 16)

16 Normal

0 Warning

0 Error

Transport Health Type: By Loss

100 %

50 %

0

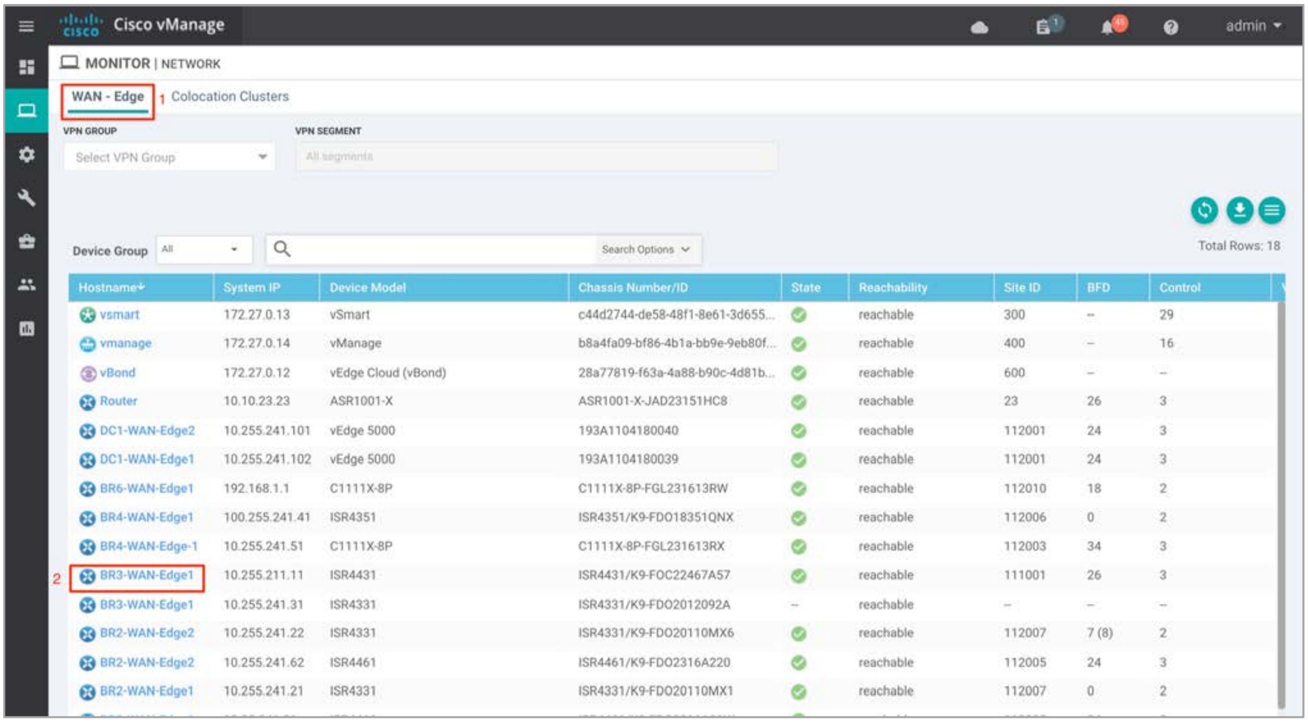
Top Applications

No data to display

Application-Aware Routing Type: By Loss

	Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
	Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0
	BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0
	DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0

Step 2 Choose a specific WAN edge device to monitor the IPS policy.



VPN GROUP: Select VPN Group

VPN SEGMENT: All segments

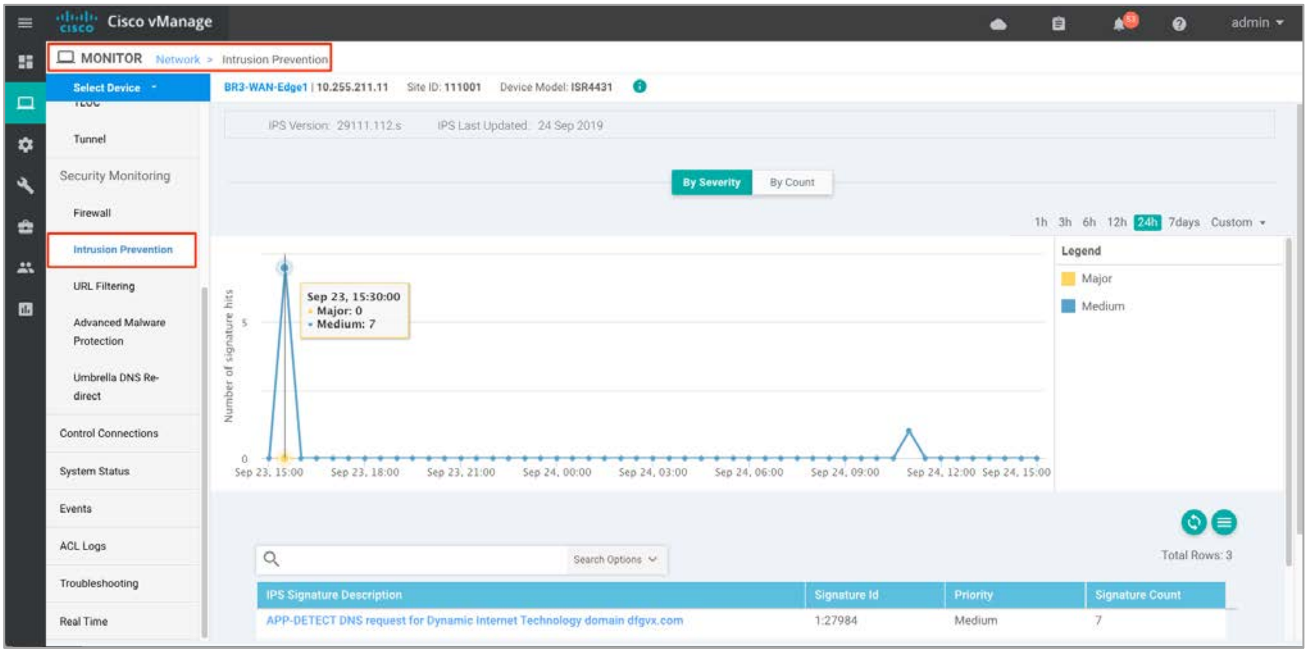
Device Group: All

Search Options

Total Rows: 18

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control
vsmart	172.27.0.13	vSmart	c44d2744-de58-48f1-8e61-3d655...	✓	reachable	300	--	29
vmanage	172.27.0.14	vManage	b8a4fa09-bf86-4b1a-bb9e-9eb80f...	✓	reachable	400	--	16
vBond	172.27.0.12	vEdge Cloud (vBond)	28a77819-f63a-4a88-b90c-4d81b...	✓	reachable	600	--	--
Router	10.10.23.23	ASR1001-X	ASR1001-X-JAD23151HC8	✓	reachable	23	26	3
DC1-WAN-Edge2	10.255.241.101	vEdge 5000	193A1104180040	✓	reachable	112001	24	3
DC1-WAN-Edge1	10.255.241.102	vEdge 5000	193A1104180039	✓	reachable	112001	24	3
BR6-WAN-Edge1	192.168.1.1	C1111X-8P	C1111X-8P-FGL231613RW	✓	reachable	112010	18	2
BR4-WAN-Edge1	100.255.241.41	ISR4351	ISR4351/K9-FDO18351QNX	✓	reachable	112006	0	2
BR4-WAN-Edge-1	10.255.241.51	C1111X-8P	C1111X-8P-FGL231613RX	✓	reachable	112003	34	3
BR3-WAN-Edge1	10.255.211.11	ISR4431	ISR4431/K9-FOC22467A57	✓	reachable	111001	26	3
BR3-WAN-Edge1	10.255.241.31	ISR4331	ISR4331/K9-FDO2012092A	--	reachable	--	--	--
BR2-WAN-Edge2	10.255.241.22	ISR4331	ISR4331/K9-FDO20110MX6	✓	reachable	112007	7 (8)	2
BR2-WAN-Edge2	10.255.241.62	ISR4461	ISR4461/K9-FDO2316A220	✓	reachable	112005	24	3
BR2-WAN-Edge1	10.255.241.21	ISR4331	ISR4331/K9-FDO20110MX1	✓	reachable	112007	0	2

Step 3 Click the **Intrusion Prevention** tab under **Security Monitoring** from the left pane. Within the dashboard, you can view top signature hits.

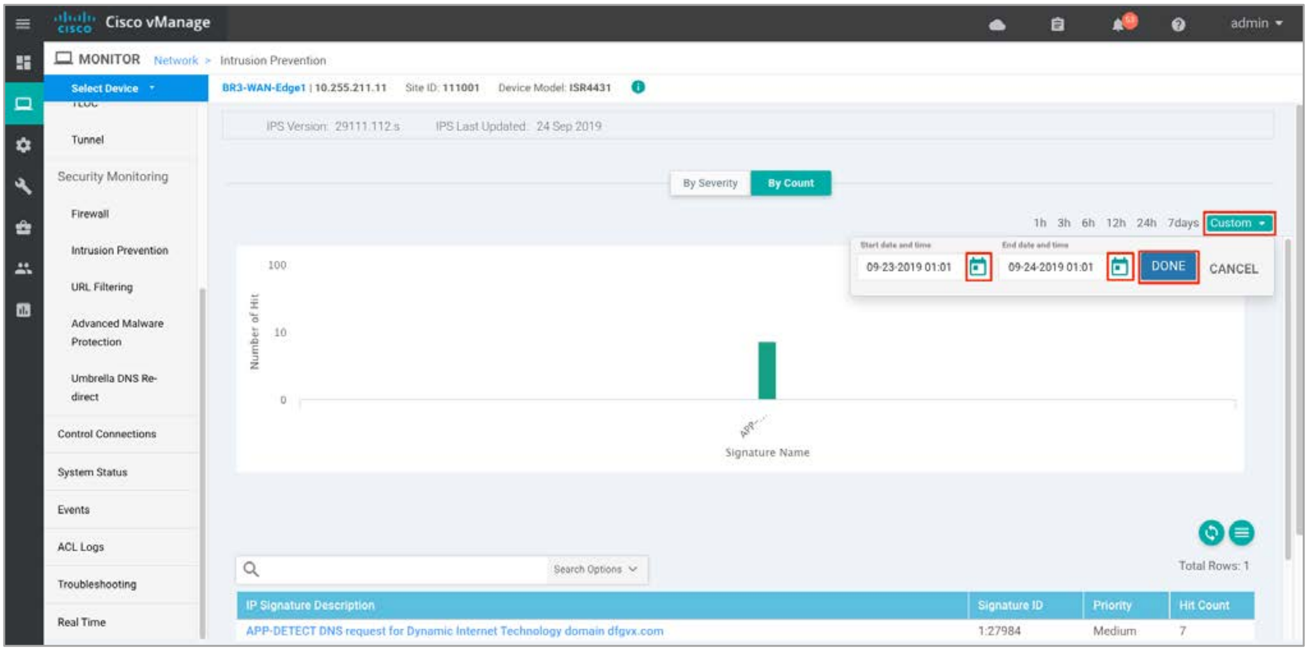


BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

IPS Version: 29111.112.s IPS Last Updated: 24 Sep 2019

IPS Signature Description	Signature Id	Priority	Signature Count
APP-DETECT DNS request for Dynamic Internet Technology domain dfgvx.com	1:27984	Medium	7

Step 4 The statistics within **Network** > **Intrusion Prevention** dashboard can be viewed hourly, daily, weekly or for a customized period. To customize the time period, select **Custom** and click the calendar icon to enter the **Start date and time** followed by **End date and time**. Finally, click **Done**.



BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

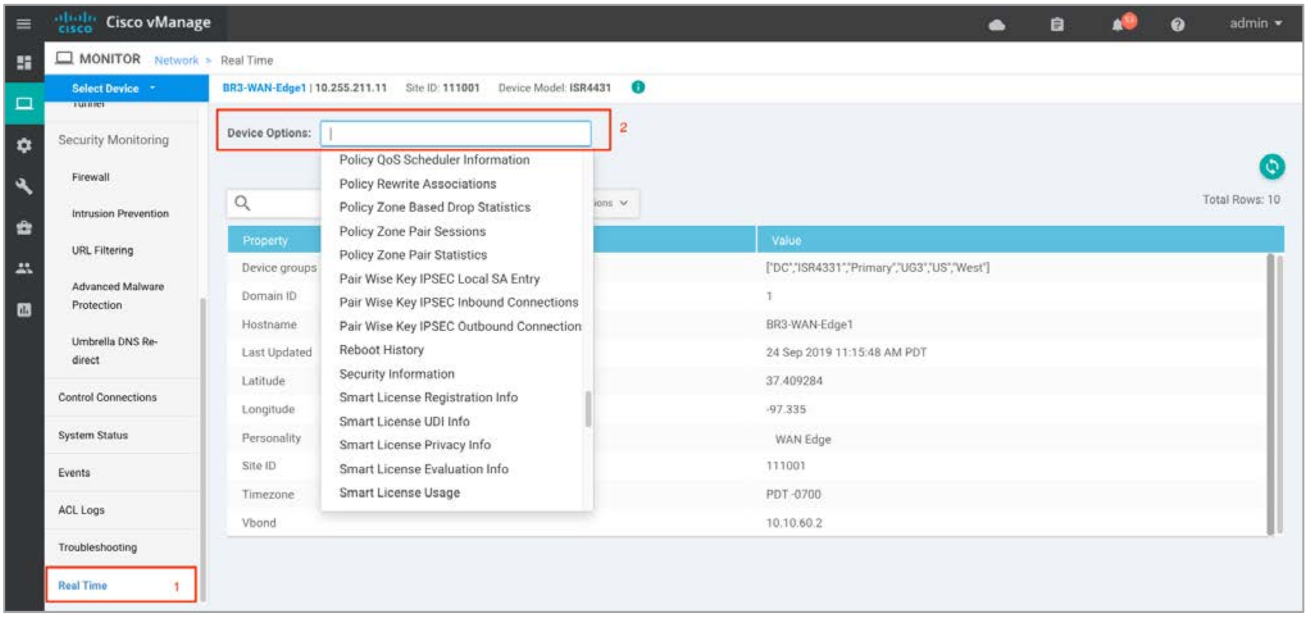
IPS Version: 29111.112.s IPS Last Updated: 24 Sep 2019

Start date and time: 09-23-2019 01:01

End date and time: 09-24-2019 01:01

IP Signature Description	Signature ID	Priority	Hit Count
APP-DETECT DNS request for Dynamic Internet Technology domain dfgvx.com	1:27984	Medium	7

Step 5 Next, click **Real Time** from the left pane. A pop-up screen appears with **Device Options**. Click the search tab to view a list of options that can be chosen to monitor, troubleshoot, and manage your device.


Cisco vManage
admin
MONITOR Network > Real Time
Select Device
Security Monitoring
Firewall
Intrusion Prevention
URL Filtering
Advanced Malware Protection
Umbrella DNS Re-direct
Control Connections
System Status
Events
ACL Logs
Troubleshooting
Real Time
1
2
Policy QoS Scheduler Information
Policy Rewrite Associations
Policy Zone Based Drop Statistics
Policy Zone Pair Sessions
Policy Zone Pair Statistics
Pair Wise Key IPSEC Local SA Entry
Pair Wise Key IPSEC Inbound Connections
Pair Wise Key IPSEC Outbound Connection
Reboot History
Security Information
Smart License Registration Info
Smart License UDI Info
Smart License Privacy Info
Smart License Evaluation Info
Smart License Usage

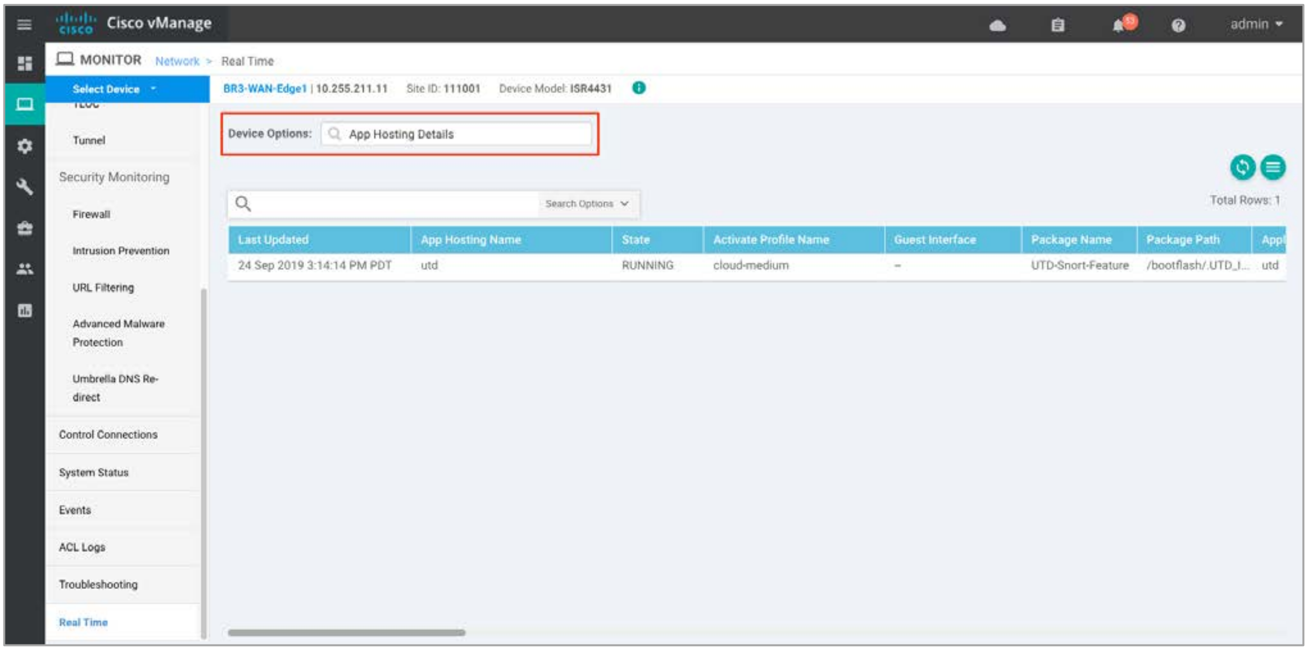
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options:

Total Rows: 10

Property	Value
Device groups	["DC","ISR4331","Primary","UG3","US","West"]
Domain ID	1
Hostname	BR3-WAN-Edge1
Last Updated	24 Sep 2019 11:15:48 AM PDT
Latitude	37.409284
Longitude	-97.335
Personality	WAN Edge
Site ID	111001
Timezone	PDT -0700
Vbond	10.10.60.2

Step 6 To view the details related to App hosting such as the state, package name, application installed version, memory, and CPU reservation, click **App Hosting Details**.



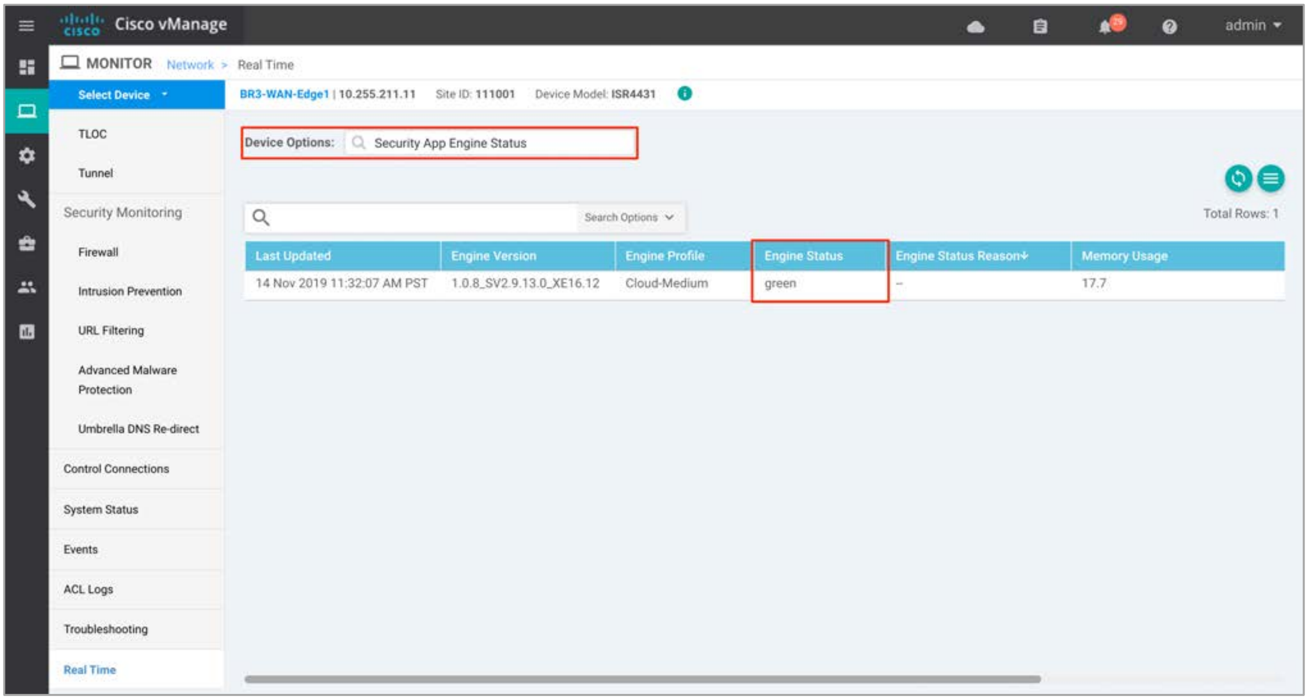
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: App Hosting Details

Total Rows: 1

Last Updated	App Hosting Name	State	Activate Profile Name	Guest Interface	Package Name	Package Path	Appl
24 Sep 2019 3:14:14 PM PDT	utd	RUNNING	cloud-medium	–	UTD-Snort-Feature	/bootflash/.UTD_I...	utd

Step 7 To view the status (Down / Green / Red) of the UTD engine, click **Security App Engine Status**. Within the output, make sure the health of the service node is green.

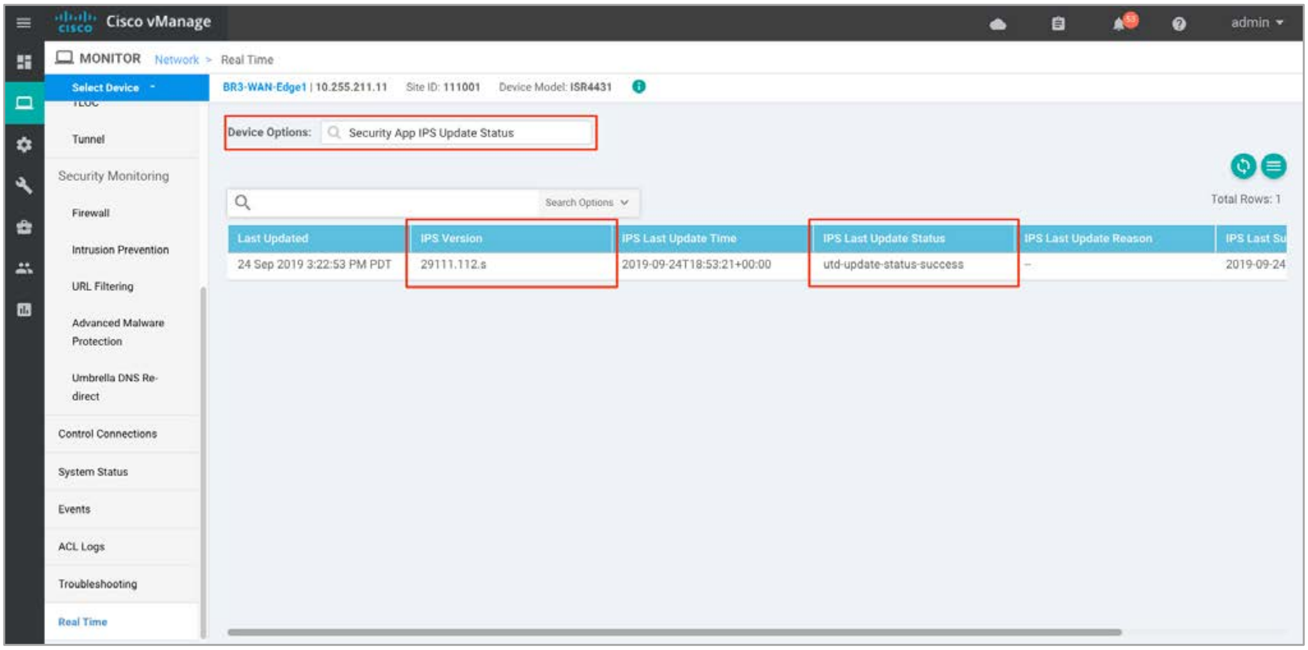


BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: Security App Engine Status

Last Updated	Engine Version	Engine Profile	Engine Status	Engine Status Reason	Memory Usage
14 Nov 2019 11:32:07 AM PST	1.0.8_SV2.9.13.0_XE16.12	Cloud-Medium	green	--	17.7

Step 8 To view the IPS signature update status, click **Security App IPS Update Status**. Ensure the IPS version ends with **.s** and not **.c**. A valid signature package version is in .s format.



BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

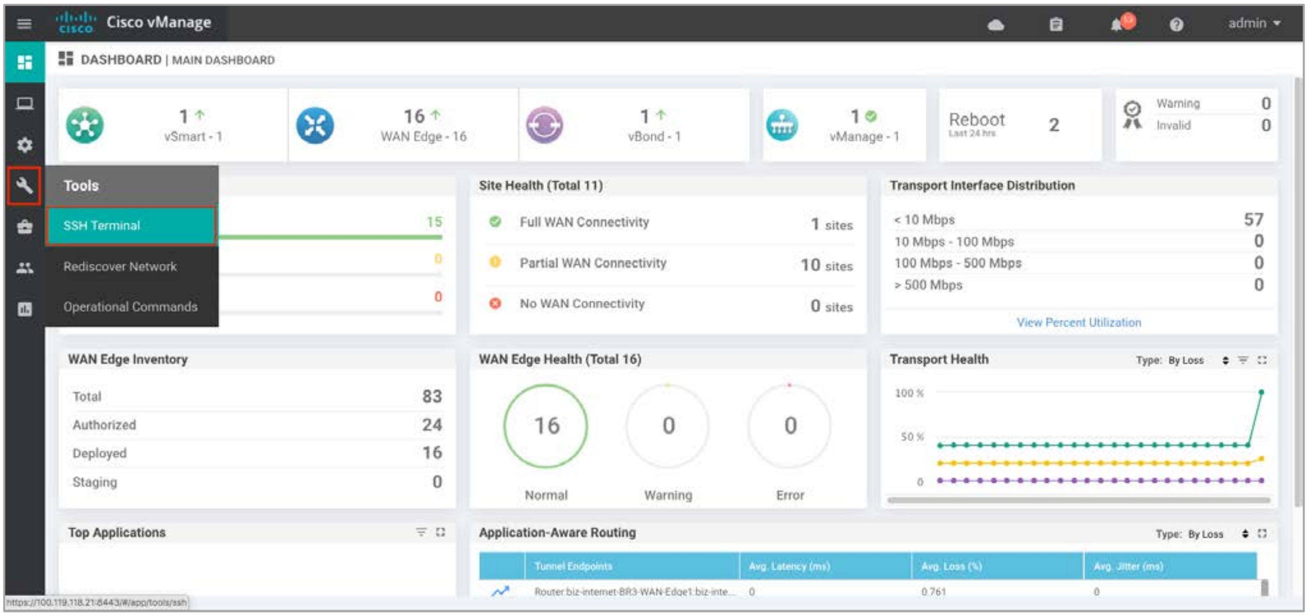
Device Options: Security App IPS Update Status

Last Updated	IPS Version	IPS Last Update Time	IPS Last Update Status	IPS Last Update Reason	IPS Last Su
24 Sep 2019 3:22:53 PM PDT	29111.112.s	2019-09-24T18:53:21+00:00	utd-update-status-success	--	2019-09-24

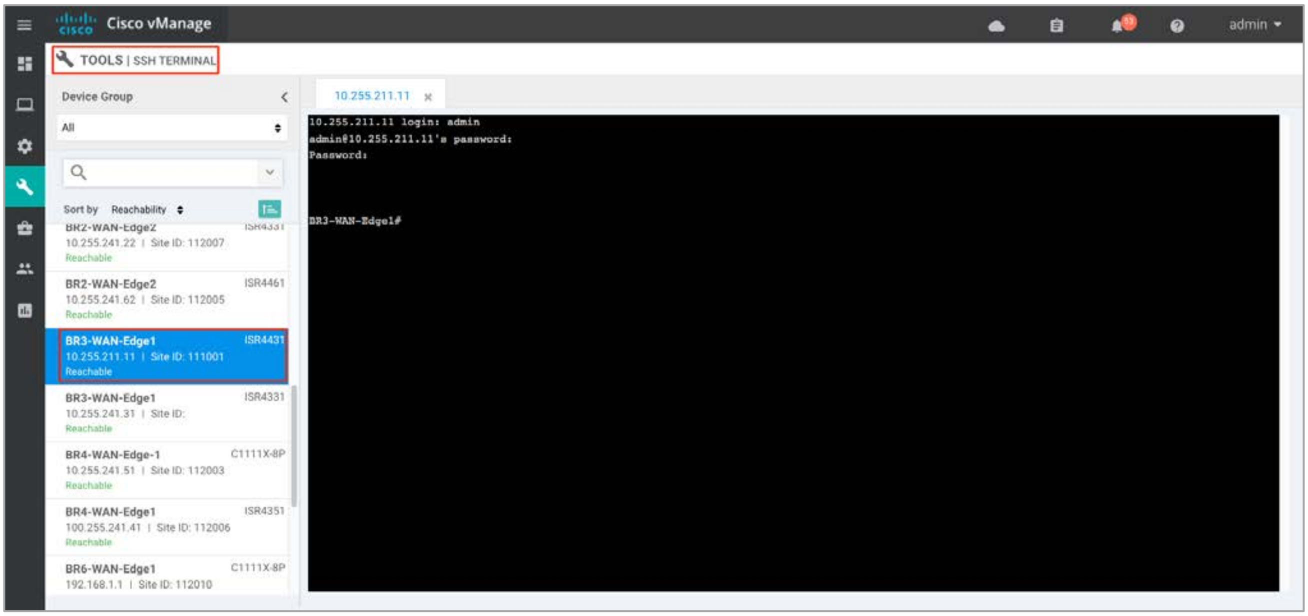
Method 3: Monitor IPS Feature and Statistics Using vManage SSH Server Dashboard

Using the vManage NMS dashboard, you can monitor the IPS feature using CLI commands.

Step 1 Navigate to **Tools** > **SSH Terminal** on the left pane.

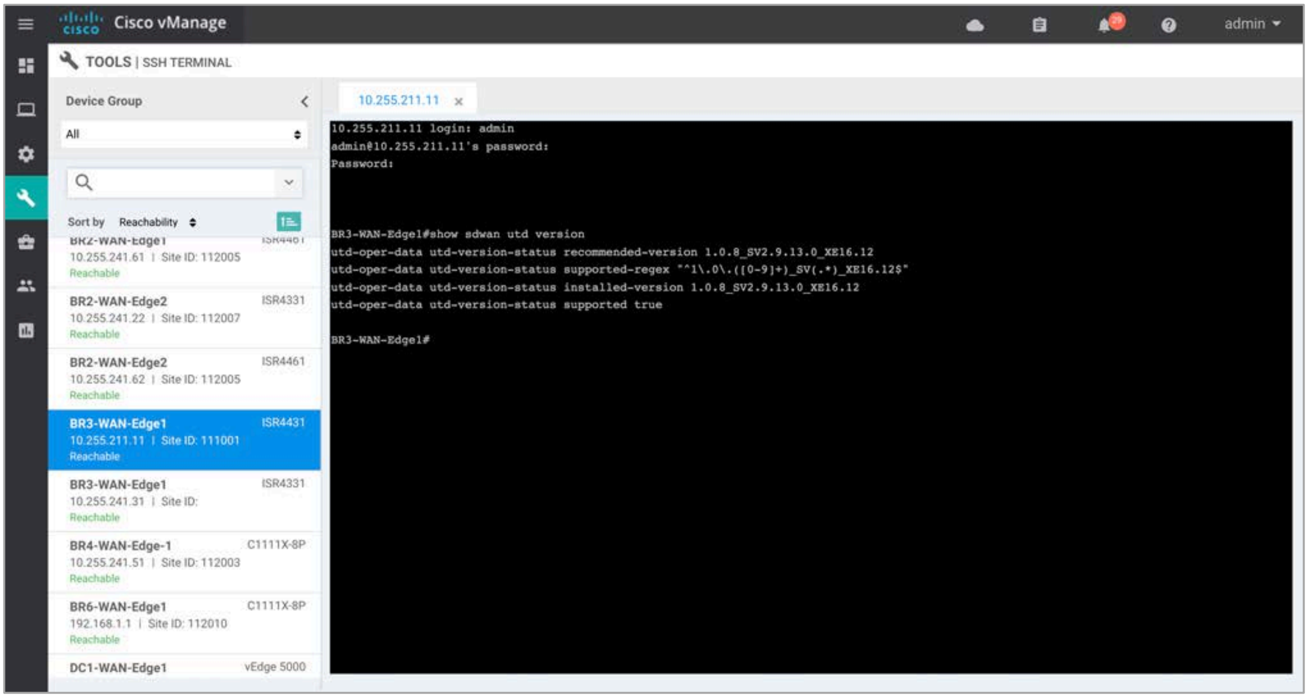


Step 2 Select the device from the list devices and log in.



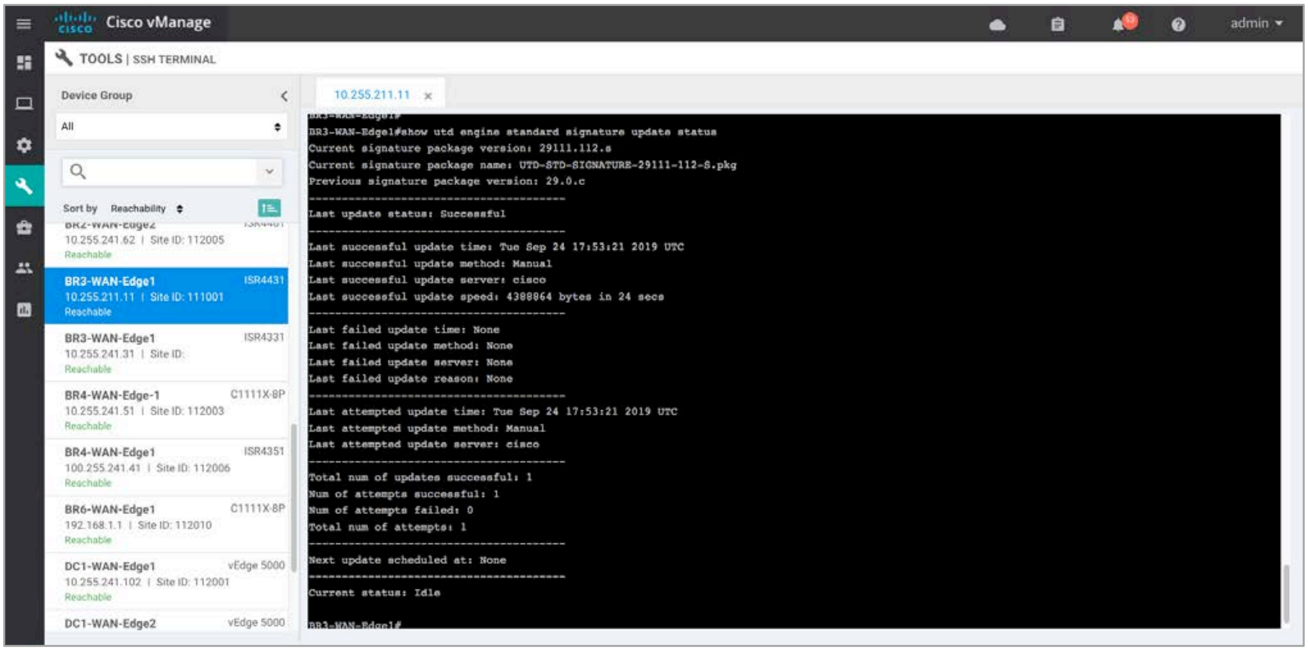
```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:



BR3-WAN-Edge1#
```

Step 3 Enter the CLI command to view the current UTD version and to test if it's supported - `show sdwan utd version`.


Cisco vManage
admin
TOOLS | SSH TERMINAL
Device Group
All
Sort by Reachability
BR2-WAN-Edge1 ISR4461 10.255.241.61 | Site ID: 112005 Reachable
BR2-WAN-Edge2 ISR4331 10.255.241.22 | Site ID: 112007 Reachable
BR2-WAN-Edge2 ISR4461 10.255.241.62 | Site ID: 112005 Reachable
BR3-WAN-Edge1 ISR4431 10.255.211.11 | Site ID: 111001 Reachable
BR3-WAN-Edge1 ISR4331 10.255.241.31 | Site ID: Reachable
BR4-WAN-Edge-1 C1111X-8P 10.255.241.51 | Site ID: 112003 Reachable
BR6-WAN-Edge1 C1111X-8P 192.168.1.1 | Site ID: 112010 Reachable
DC1-WAN-Edge1 vEdge 5000
10.255.211.11

```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:



BR3-WAN-Edge1#show sdwan utd version
utd-oper-data utd-version-status recommended-version 1.0.8_SV2.9.13.0_XE16.12
utd-oper-data utd-version-status supported-regex "^1\.0\.([0-9]+)_SV(.*)_XE16.12$"
utd-oper-data utd-version-status installed-version 1.0.8_SV2.9.13.0_XE16.12
utd-oper-data utd-version-status supported true

BR3-WAN-Edge1#
```

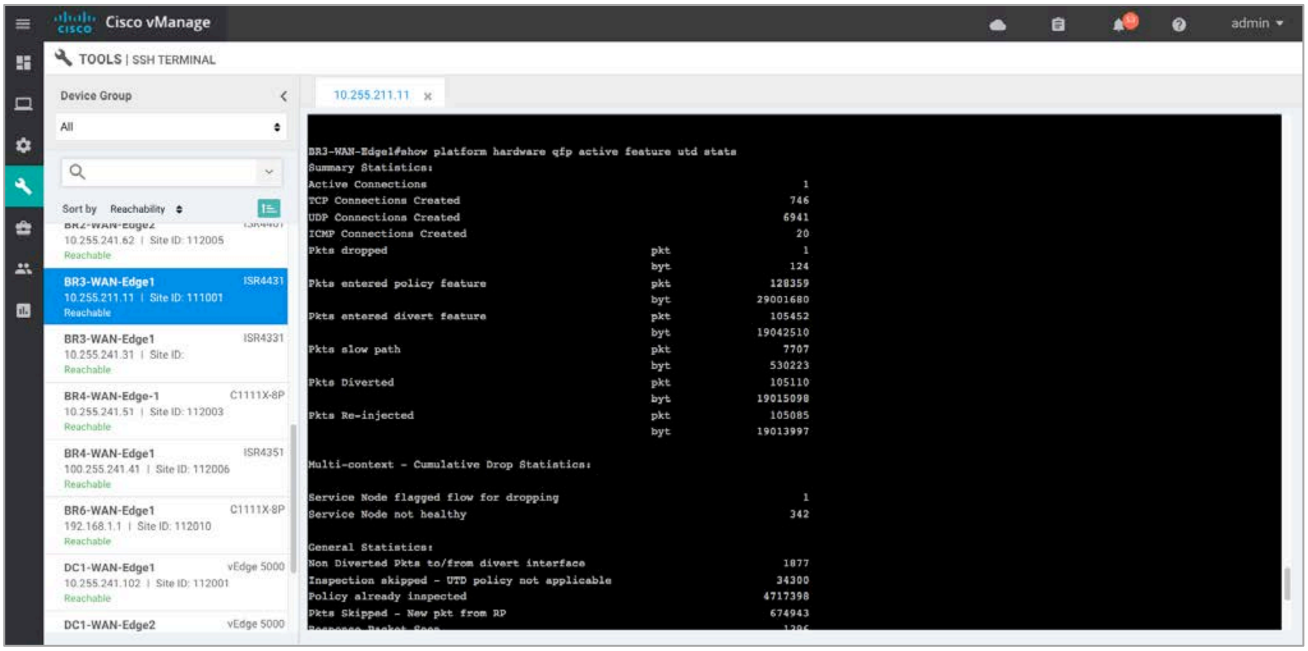
Step 4 Enter the CLI command to view the current signature package - `show utd engine standard signature update status`. The command displays the number of failed or successful signature update attempts, along with the reason for the last update.


Cisco vManage
admin
TOOLS | SSH TERMINAL
Device Group
All
Sort by Reachability
BR2-WAN-Edge2 ISR4461 10.255.241.62 | Site ID: 112005 Reachable
BR3-WAN-Edge1 ISR4431 10.255.211.11 | Site ID: 111001 Reachable
BR3-WAN-Edge1 ISR4331 10.255.241.31 | Site ID: Reachable
BR4-WAN-Edge-1 C1111X-8P 10.255.241.51 | Site ID: 112003 Reachable
BR4-WAN-Edge1 ISR4351 100.255.241.41 | Site ID: 112006 Reachable
BR6-WAN-Edge1 C1111X-8P 192.168.1.1 | Site ID: 112010 Reachable
DC1-WAN-Edge1 vEdge 5000 10.255.241.102 | Site ID: 112001 Reachable
DC1-WAN-Edge2 vEdge 5000
10.255.211.11

```
BR3-WAN-Edge1#
BR3-WAN-Edge1#show utd engine standard signature update status
Current signature package version: 29111.112.s
Current signature package name: UTD-STD-SIGNATURE-29111-112-S.pkg
Previous signature package version: 29.0.c
----------------------------------------
Last update status: Successful
----------------------------------------
Last successful update time: Tue Sep 24 17:53:21 2019 UTC
Last successful update method: Manual
Last successful update server: cisco
Last successful update speed: 4388864 bytes in 24 secs
----------------------------------------
Last failed update time: None
Last failed update method: None
Last failed update server: None
Last failed update reason: None
----------------------------------------
Last attempted update time: Tue Sep 24 17:53:21 2019 UTC
Last attempted update method: Manual
Last attempted update server: cisco
----------------------------------------
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 0
Total num of attempts: 1
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle

BR3-WAN-Edge1#
```

Technical Tip: If the current signature package version ends with **.c** instead of **.s**, try to manually update the signature from the WAN Edge device by entering the command `utd threat-inspection signature update server cisco username <username> password <password>.`

Step 5 Enter the following CLI command to view the utd packet statistics - `show platform hardware qfp active feature utd stats.` The output displays the summary of all statistics that includes General Statistics, Diversion Statistics, and Service Node Statistics (health).

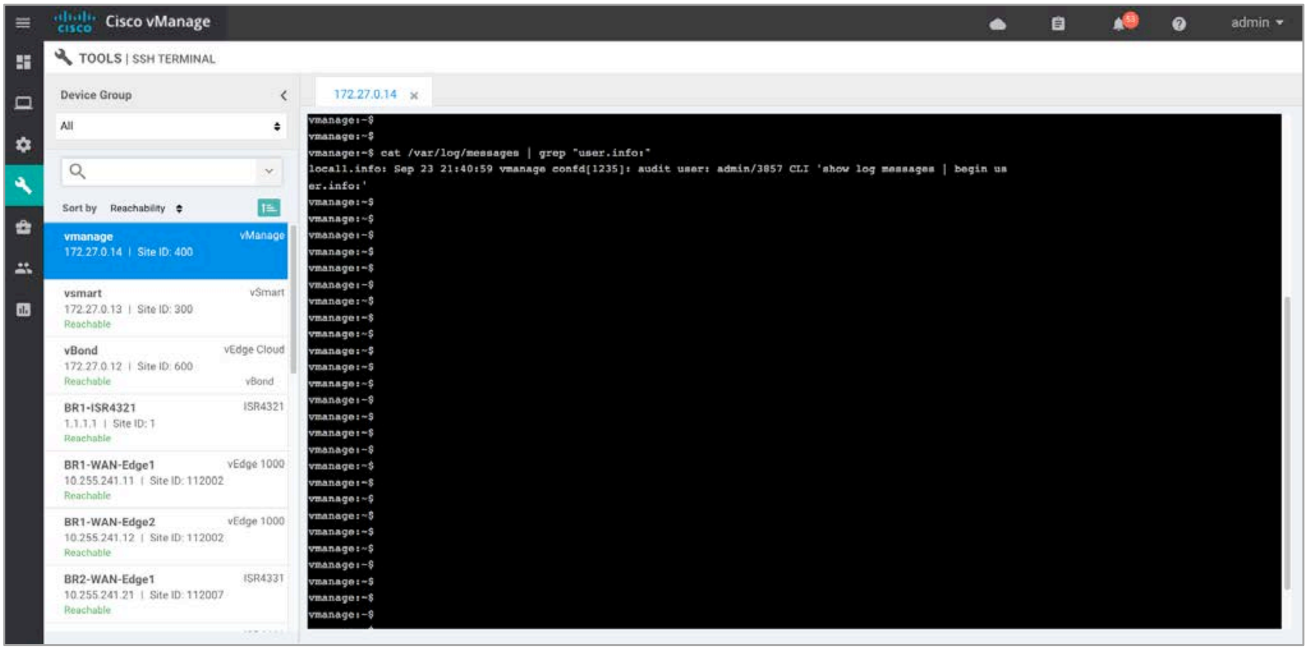


```
BR3-WAN-Edge1#show platform hardware qfp active feature utd stats
Summary Statistics:
Active Connections                                                   1
TCP Connections Created                                            746
UDP Connections Created                                           6941
ICMP Connections Created                                            20
Pkts dropped                                        pkt              1
                                                    byt            124
Pkts entered policy feature                         pkt         128359
                                                    byt       29001680
Pkts entered divert feature                         pkt         105452
                                                    byt       19042510
Pkts slow path                                      pkt           7707
                                                    byt         530223
Pkts Diverted                                       pkt         105110
                                                    byt       19015098
Pkts Re-injected                                    pkt         105085
                                                    byt       19013997

Multi-context - Cumulative Drop Statistics:

Service Node flagged flow for dropping                               1
Service Node not healthy                                           342

General Statistics:
Non Diverted Pkts to/from divert interface                        1877
Inspection skipped - UTD policy not applicable                   34300
Policy already inspected                                       4717398
Pkts Skipped - New pkt from RP                                  674943
```

Step 6 To check for automatic signature updates on vManage, enter the following commands.

```
vshell  /*To enter shell mode*/
cat /var/log/messages  /*And followed by grep command to print a subset of the output*/
exit /*To exit shell mode*/
```

For example,

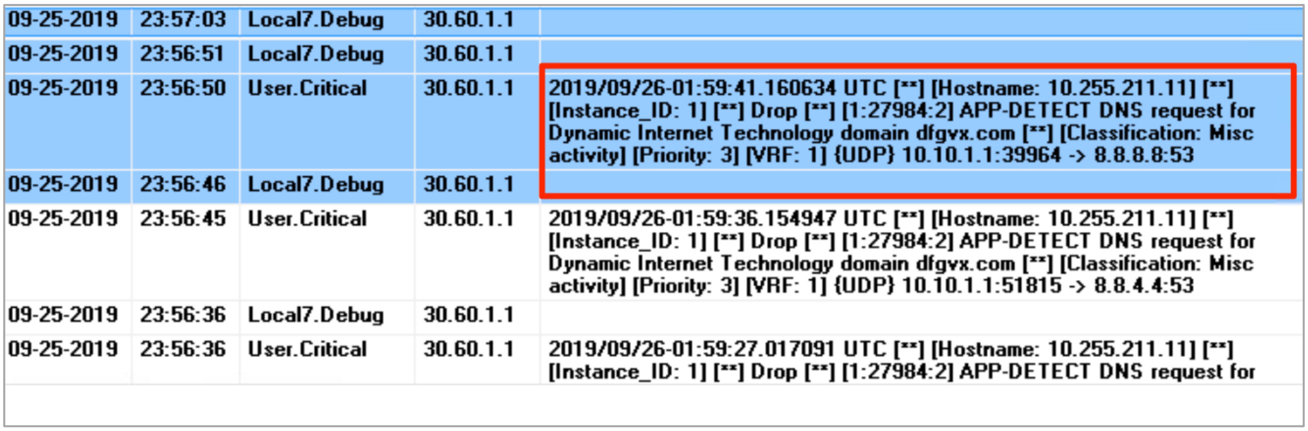


```
vmanage:~$
vmanage:~$
vmanage:~$ cat /var/log/messages | grep "user.info:"
local1.info: Sep 23 21:40:59 vmanage confd[1235]: audit user: admin/3857 CLI 'show log messages | begin us
er.info:'
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
```

Besides the CLI commands listed previously, here are some other useful commands. `show utd engine, show sdwan utd dataplane <config/global/stats>, show sdwan utd update ips and show log.`

Process 3: Monitor IPS Signature Violations Using Syslog Server

Step 1 Log in to the syslog server and view the error logs. In the logs, you can view the device IP, VRF ID, destination IP, along with details to the signature.



```
09-25-2019  23:57:03  Local7.Debug   30.60.1.1
09-25-2019  23:56:51  Local7.Debug   30.60.1.1
09-25-2019  23:56:50  User.Critical  30.60.1.1  2019/09/26-01:59:41.160634 UTC [**] [Hostname: 10.255.211.11] [**]
                                                [Instance_ID: 1] [**] Drop [**] [1:27984:2] APP-DETECT DNS request for
                                                Dynamic Internet Technology domain dfgvx.com [**] [Classification: Misc
                                                activity] [Priority: 3] [VRF: 1] {UDP} 10.10.1.1:39964 -> 8.8.8.8:53
09-25-2019  23:56:46  Local7.Debug   30.60.1.1
09-25-2019  23:56:45  User.Critical  30.60.1.1  2019/09/26-01:59:36.154947 UTC [**] [Hostname: 10.255.211.11] [**]
                                                [Instance_ID: 1] [**] Drop [**] [1:27984:2] APP-DETECT DNS request for
                                                Dynamic Internet Technology domain dfgvx.com [**] [Classification: Misc
                                                activity] [Priority: 3] [VRF: 1] {UDP} 10.10.1.1:51815 -> 8.8.4.4:53
09-25-2019  23:56:36  Local7.Debug   30.60.1.1
09-25-2019  23:56:36  User.Critical  30.60.1.1  2019/09/26-01:59:27.017091 UTC [**] [Hostname: 10.255.211.11] [**]
                                                [Instance_ID: 1] [**] Drop [**] [1:27984:2] APP-DETECT DNS request for
```

Appendix A: New in this Guide

This guide is new and is not updated from a previous version.

Appendix B: Hardware and Software Used for Validation

This guide was validated using the following hardware and software.

Table 5 **System feature template settings**

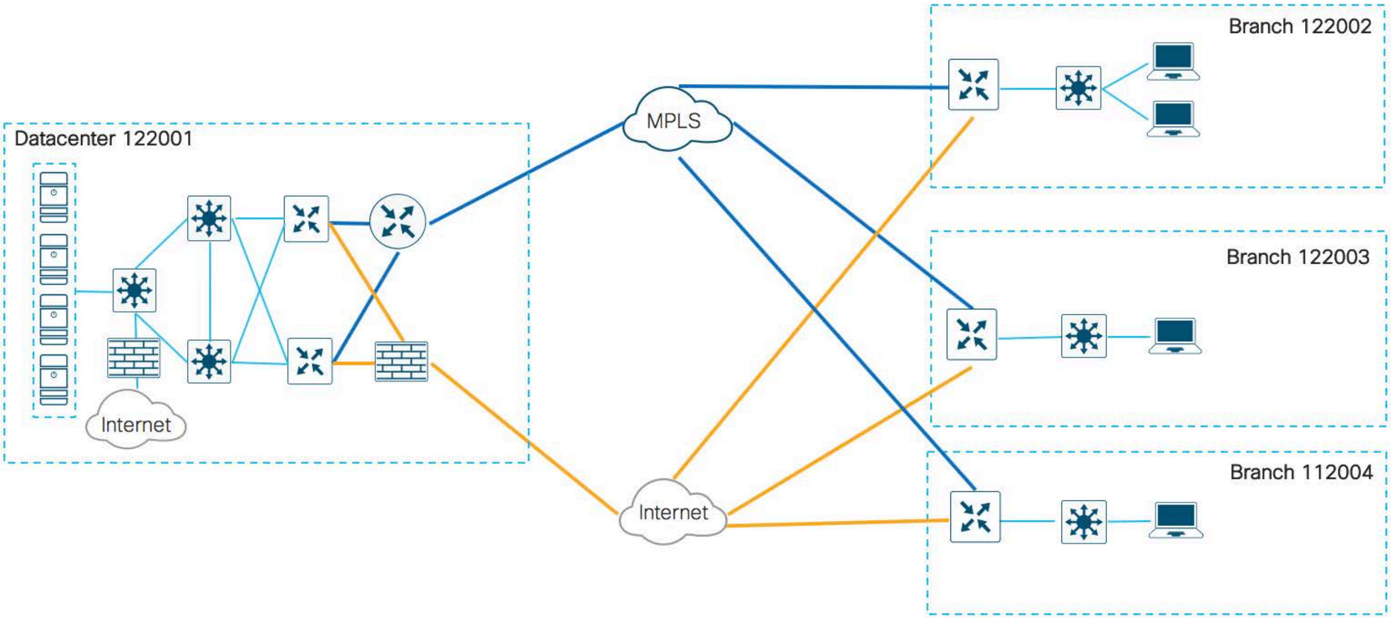
Functional Area	Product	Software Version
Cloud	Cisco vManage NMS	19.2.099
Cloud	Cisco vBond Controller	19.2.099
Cloud	Cisco vSmart Controller	19.2.099
Data center	Cisco vEdge 5000 Series Routers	19.2.099
Branch office	Cisco ISR 4431	16.12.1e
Branch office	Cisco ISR 4331	16.12.1e
Branch office	Cisco ISR c1111x-8P	16.12.1e

Appendix C: Deployment Example

Each of the WAN edge devices is running SD-WAN code, configured using the templates similar to those used in the SD-WAN deployment guide and the devices are a part of the SD-WAN overlay network.

Topology

The network diagram referred to for deploying the PCI compliance security use case.



System IP Address and Site ID

The following table lists the system IP addresses and site IDs chosen for this deployment guide.

Table 6 **Example network site IDs and system IP addresses**

Hostname	Location	Site ID	System IP
DC1-WAN-Edge1	Data Center 1/ West	122001	10.255.241.101
DC1-WAN-Edge2			10.255.241.102
BR1-WAN-Edge1	Branch 1/ West	122002	10.255.241.11
BR2-WAN-Edge1	Branch 2/ West	122003	10.255.241.21
BR3-WAN-Edge1	Branch 3/ West	122004	10.255.241.31

The following table lists the color used for each transport in this deployment guide.

Table 7 **Transport details**

Color	Transport
MPLS	MPLS Transport

Color	Transport
Biz-Internet	Internet Provider 1

Note that the LAN side of each branch contains devices configured within the private IP address range of 10.0.0.0/8 subnet.

Appendix D: Cisco WAN Edge Configuration Summary (Templates)

This section includes the security policy feature template, along with an example device template and CLI configuration specific to the Cisco WAN Edge router ISR4331 deployed within this deployment guide. To deploy other feature/device templates to establish SD-WAN overlay network, please refer to the SD-WAN Deployment Guide.

Feature Template

This section includes configured lists, the main security policy template, and its container template.

Security Policy Feature Template

Devices: All devices except vManage and vSmart

Template: Basic Information/Security

Template Name: Compliance_Security_Policy

Description: Security Policy Template

The following lists are configured for the security policy.

Table 8 **Configured Lists**

Section	List Type	Value
List	Zones	INSIDE = VPN 1
	Data Prefix	Client_Network = 10.0.0.0/8
		Compliance_Server=10.1.1.1/32

The configured lists are used in the security policy.

Table 9 **Security Policy template settings**

Policy Sub-section	Section	Condition/Parameter	Type	Value
Enterprise Firewall with App Aware	Target Zone-Pair	Source Zone	Drop-down	INSIDE
		Destination Zone	Drop-down	INSIDE
	Name		Entry tab	Compliance_Firewall_Policy
	Description		Entry tab	Enterprise Firewall with App Aware for Compliance Use Case
	Match (Rule 1)	Source Data Prefix List	Variable	Client_Network
		Destination Data Prefix List	Variable	Compliance_Server
		Protocol	Drop-down	HTTP

Policy Sub-section	Section	Condition/Parameter	Type	Value
	Actions (Rule 1)	Inspect	Radio Button	Enable
	Match (Rule 2)	Destination Data Prefix List	Variable	Compliance_Server
		Protocol	Drop-down	HTTP
	Actions (Rule 2)	Inspect	Radio Button	Enabled
			Select	Log
	Match (Rule 3)	Protocol	Entry tab	6 17
	Actions (Rule 3)	Inspect	Radio Button	Enabled
	Match (Rule 4)	Protocol	Entry tab	1
	Actions (Rule 3)	Inspect	Radio Button	Enabled
Intrusion Prevention System	Target	VPNs	Entry tab	1
	Policy Name		Entry tab	Compliance_IPS_Policy
	Signature Set		Drop down	Security
	Inspection Mode		Drop down	Protection
	Advanced	Alerts Log Level	Drop down	Error
Policy Summary	Security Policy Name		Entry tab	Compliance_Security_Policy
	Security Policy Description		Entry tab	Security Policy Specific to Compliance Use Case
	Additional Policy Settings (Firewall)	High Speed Logging – VPN	Entry tab	0
		High Speed Logging – Server IP	Entry tab	10.2.2.2
		High Speed Logging – Port	Default	2055
		Audit Trail	slide	On
	Additional Policy Settings (IPS)	External Syslog Server - VPN	Entry tab	0
		External syslog Server - Server IP		10.2.2.2
		Failure Mode	Drop down	Open

Container Profile Feature Template

Devices: All devices except vManage and vSmart

Template: Basic Information/Security

Template Name: Security_App_Hosting

Description: Security Template

Section	Type	Value
Template Name	Default	On
Template Description	Default	default

Device Template

This section lists the device template deployed, along with CLI configuration on ISR4331 router.

Device Model: ISR4331

Template Name: Branch_B_Hybrid_Transport_Single_LAN_Int

Description: Branch B with OSPF on the LAN side single port with MPLS and Internet transport

Table 1 **Branch 112002 Device Template: Branch_A_INET_TLOC_SubInt_OSPF**

Template Type	Template Sub-Type	Template Name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Single_Transport
	BGP	BR_VPN0_BGP
	VPN Interface	BR_INET_INT
		BR_MPLS_INT
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_BASE
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_VPN1_INT1

Template Type	Template Sub-Type	Template Name
Security Policy		Compliance_Security_Policy
	Container Profile	Security_App_Hosting

Example Branch Configuration

The following section lists out an example branch configuration.

Branch 122003: BR2-WAN-Edge1: Branch_B_Hybrid_Transport_Single_LAN_Int

```
viptela-system:system
   device-model           vedge-ISR-4331
   host-name              BR2-WAN-Edge1
   gps-location latitude 33.4484
   gps-location longitude -112.074
   device-groups          BRANCH Primary UG5 US West v1000
   system-ip              10.255.241.22
   overlay-id             1
   site-id                122003
   port-offset            1
   control-session-pps    300
   admin-tech-on-failure
   sp-organization-name  "ENB-Solutions - 21615"
   organization-name     "ENB-Solutions - 21615"
   no port-hop
   track-transport
   track-default-gateway
   console-baud-rate      115200
   vbond 10.10.60.2 port 12346
   logging
    disk
     enable
    !
   !
   no cft-enable
   no cft-cache-enable
  !
  bfd color mpls
   hello-interval 1000
   no pmtu-discovery
   multiplier     7
  !
  bfd color biz-internet
   hello-interval 1000
   no pmtu-discovery
   multiplier     7
  !
  bfd app-route multiplier 6
  bfd app-route poll-interval 120000
  omp
   no shutdown
   graceful-restart
  !
  security
   ipsec
    rekey               86400
    replay-window       4096
    authentication-type sha1-hmac ah-sha1-hmac
   !
  !
  no service pad
  no service tcp-small-servers
  no service udp-small-servers
  hostname BR2-WAN-Edge2
  username admin privilege 15 secret 9 $9$3VEF3VAI3lMM3E$awMmxogwHvRdxoHA5u1utUOAmKPBUvUbkD4PnwNWmWk
  vrf definition 1
   description Service VPN
   rd          1:1
   address-family ipv4
    exit-address-family
   !
   address-family ipv6
    exit-address-family
   !
  !
  vrf definition 65529
   rd 65529:1
   address-family ipv4
    exit-address-family
   !
  !
  vrf definition Mgmt-intf
   description Management VPN
   rd          1:512
   address-family ipv4
    exit-address-family
   !
   address-family ipv6
    exit-address-family
   !
  !
  no ip finger
  no ip rcmd rcp-enable
  no ip rcmd rsh-enable
  no ip dhcp use class
  ip name-server 208.67.222.222 208.67.220.220
  ip route 0.0.0.0 0.0.0.0 30.20.1.2 1
  ip access-list extended Compliance_FW_Policy_copy-seq-1-acl_
   11 permit object-group Compliance_FW_Policy_copy-seq-1-service-og_ object-group Client_Network object-
group Compliance_Server
  !
  ip access-list extended Compliance_FW_Policy_copy-seq-11-acl_
   11 permit object-group Compliance_FW_Policy_copy-seq-11-service-og_ any object-group Compliance_Server
  !
  ip access-list extended Compliance_FW_Policy_copy-seq-21-acl_
   11 permit object-group Compliance_FW_Policy_copy-seq-21-service-og_ any any
  !
  ip access-list extended Compliance_FW_Policy_copy-seq-31-acl_
   11 permit object-group Compliance_FW_Policy_copy-seq-31-service-og_ any any
  !
  ip access-list extended utd-nat-acl
   10 permit ip any any
  !
  no ip http ctc authentication
  no ip igmp ssm-map query dns
  ip nat route vrf 65529 0.0.0.0 0.0.0.0 global
  class-map type inspect match-any Compliance_FW_Policy_copy-s1-l4-cm_
   match protocol http
  !
  class-map type inspect match-any Compliance_FW_Policy_copy-s11-l4-cm_
   match protocol http
  !
  class-map type inspect match-all Compliance_FW_Policy_copy-seq-1-cm_
   match access-group name Compliance_FW_Policy_copy-seq-1-acl_
   match class-map Compliance_FW_Policy_copy-s1-l4-cm_
  !
  class-map type inspect match-all Compliance_FW_Policy_copy-seq-11-cm_
   match access-group name Compliance_FW_Policy_copy-seq-11-acl_
   match class-map Compliance_FW_Policy_copy-s11-l4-cm_
```

```
!
class-map type inspect match-all Compliance_FW_Policy_copy-seq-21-cm_
 match access-group name Compliance_FW_Policy_copy-seq-21-acl_
!
class-map type inspect match-all Compliance_FW_Policy_copy-seq-31-cm_
 match access-group name Compliance_FW_Policy_copy-seq-31-acl_
!
policy-map type inspect Compliance_FW_Policy_copy
 class Compliance_FW_Policy_copy-seq-1-cm_
   inspect
 !
 class Compliance_FW_Policy_copy-seq-11-cm_
   drop log
 !
 class Compliance_FW_Policy_copy-seq-21-cm_
   inspect
 !
 class Compliance_FW_Policy_copy-seq-31-cm_
   inspect
 !
 class class-default
   drop
 !
!
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 100.119.118.9 255.255.255.0
 ip redirects
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/0
 description Service side Interface
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.20.14.2 255.255.255.0
 ip redirects
 ip mtu    1500
 ip ospf 1 area 0
 ip ospf authentication message-digest
 ip ospf network     point-to-point
 ip ospf cost        1
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf message-digest-key 22 md5 0 c1sco123
 ip ospf priority    1
 ip ospf retransmit-interval 5
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/1
 description MPLS Interface
 no shutdown
 arp timeout 1200
 ip address 10.20.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/2
```

```
 description INET Interface
 no shutdown
 arp timeout 1200
 ip address 30.20.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1496
 mtu         1500
 negotiation auto
exit
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet0/0/1
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/1
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/1
 tunnel mode sdwan
exit
interface Tunnel2
 no shutdown
 ip unnumbered GigabitEthernet0/0/2
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/2
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/2
 tunnel mode sdwan
exit
interface VirtualPortGroup0
 no shutdown
 vrf forwarding 65529
 ip address 192.168.1.1 255.255.255.252
exit
interface VirtualPortGroup1
 no shutdown
 ip address 192.0.2.1 255.255.255.252
exit
object-group network Client_Network
 10.0.0.0 255.0.0.0
!
object-group network Compliance_Server
 host 10.1.1.1
 !
!
object-group service Compliance_FW_Policy_copy-seq-1-service-og_
 ip
!
object-group service Compliance_FW_Policy_copy-seq-11-service-og_
 ip
!
object-group service Compliance_FW_Policy_copy-seq-21-service-og_
 tcp
 udp
!
object-group service Compliance_FW_Policy_copy-seq-31-service-og_
 icmp
!
clock summer-time PDT recurring
clock timezone PDT -8 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
no logging rate-limit
logging persistent
aaa authentication login default local
aaa authorization exec default local
parameter-map type inspect audit-trail-pmap_
audit-trail on
```

```
!

parameter-map type inspect-global
 alert on
 log dropped-packets
 log flow-export v9 udp destination 10.2.2.2 2055 vrf 0


 multi-tenancy
 vpn zone security
!
zone security INSIDE
 vpn 1
!
zone-pair security ZP_INSIDE_INSIDE_Comp_1218207151 source INSIDE destination INSIDE
 service-policy type inspect Compliance_FW_Policy_copy
!
no crypto ikev2 diagnose error
no crypto isakmp diagnose error
router bgp 65111
 bgp log-neighbor-changes
 distance bgp 20 200 20
 maximum-paths eibgp 2
 neighbor 10.20.1.2 remote-as 70
 neighbor 10.20.1.2 description MPLS_PE
 neighbor 10.20.1.2 ebgp-multihop 1
 neighbor 10.20.1.2 maximum-prefix 2147483647 100
 neighbor 10.20.1.2 password 0 c1sco123
 neighbor 10.20.1.2 send-community both
 neighbor 10.20.1.2 timers 3 9
 address-family ipv4 unicast
  network 10.20.1.0 mask 255.255.255.252
  exit-address-family
 !
 timers bgp 60 180
!
router ospf 1 vrf 1
 area 0 range 10.20.14.0 255.255.255.0 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.20.14.14
 compatible rfc1583
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
!
line con 0
 login authentication default
 speed    115200
 stopbits 1
!
iox
app-hosting appid utd
 app-resource package-profile cloud-medium
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
 !
 app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
 !
 start
!
utd multi-tenancy
utd engine standard multi-tenancy
 threat-inspection profile pci-test
```

```
  threat protection
  policy security
  logging level info
 !
 utd global
  logging host 10.2.2.2
 !
 policy utd-policy-vrf-1
  all-interfaces
  vrf 1
  threat-inspection profile pci-test
 exit
!
sdwan
 interface GigabitEthernet0/0/1
  tunnel-interface
   encapsulation ipsec preference 200 weight 1
   no border
   color mpls restrict
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
   no allow-service snmp
  exit
 exit
 interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec preference 0 weight 1
   no border
   color biz-internet
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
```

```
     no allow-service snmp
    exit
   exit
   interface VirtualPortGroup0
    access-list vpg-log-server-acl in
   exit
   omp
    no shutdown
    send-path-limit  16
    ecmp-limit       16
    graceful-restart
    no as-dot-notation
    timers
     holdtime               60
     advertisement-interval 1
     graceful-restart-timer 43200
     eor-timer              300
    exit
    address-family ipv4 vrf 1
     advertise ospf external
     advertise connected
     advertise static
    !
   !
  !
  policy
   no app-visibility
   no flow-visibility
   no implicit-acl-logging
   log-frequency        1000
   lists
    data-prefix-list Client_Network
     ip-prefix 10.0.0.0/8
    !
    data-prefix-list Compliance_Server
     ip-prefix 10.1.1.1/32
    !
   !
   access-list vpg-log-server-acl
    sequence 5
     match
      destination-ip 10.2.2.2/32
      protocol       17
     !
     action accept
      count cipslog-vpn-0
      set
       local-vpn 0
      !
     !
    !
    default-action accept
   !
  !
 !
!
```

Appendix E: Glossary

IPS	Intrusion Prevention System
VPN	Virtual Private Network
NAT	Network Address Translation
LAN	Local Area Network
WAN	Wide Area Network

About this guide

Feedback & discussion

For comments and suggestions about our guides, please join the discussion on Cisco Community.