Secure Direct Cloud Access for Cisco IOS-XE SD-WAN Devices

Prescriptive Deployment Guide

July, 2020

Contents

Introduction

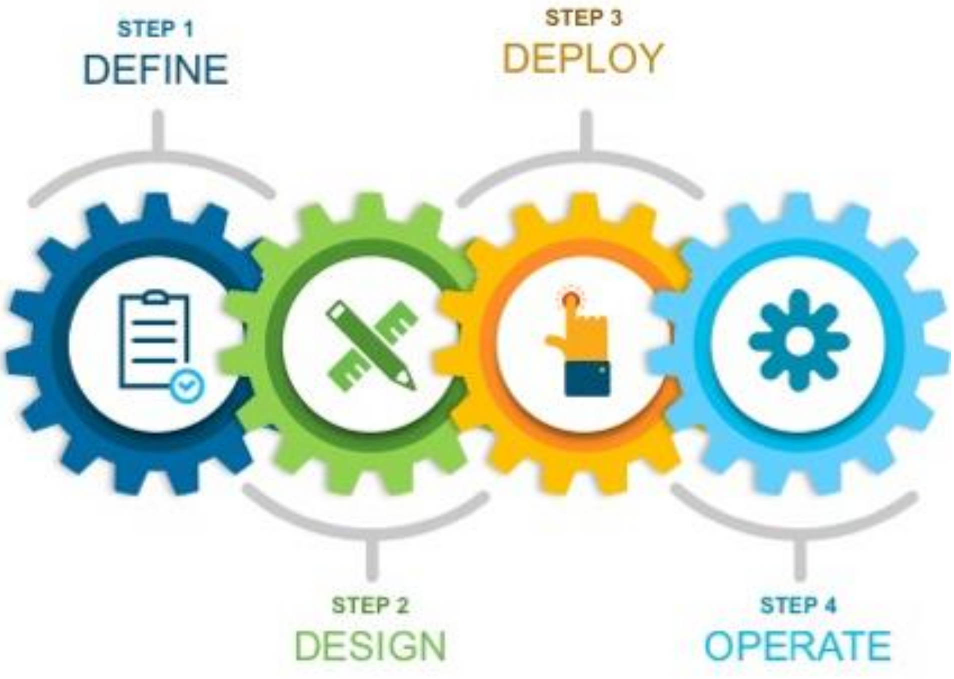
About the Guide

This document provides the design and deployment of the Cisco SD-WAN security policy specific to secure Direct Cloud Access (DCA) within remote sites running IOS-XE SD-WAN WAN Edge platforms. The security features leveraged within this guide include Enterprise Firewall with Application Awareness, Intrusion Prevention System (IPS), Advanced Malware Protection (AMP) and DNS/Web-layer Security with Umbrella Integration.

The guide explains at length the platforms deployed, highlights the best practices and assists with the successful configuration and deployment of security features. However, the document is not meant to exhaustively cover all options.

This document assumes that the controllers are already deployed and integrated into vManage NMS, 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. For the design and deployment of local Internet exit on remote site WAN Edge devices refer Cisco SD-WAN Direct Internet Access Design and Deployment Guide. For details regarding the required licenses to deploy the Cisco SD-WAN security feature set, refer to Cisco DNA Software for SD-WAN and Routing.

Figure 1. Implementation flow



This document contains four major sections:

- The Define section defines the shortcomings of a secure traditional WAN architecture, and then explains the benefits of deploying SD-WAN security policy on remote sites.
- The Design section includes the use case covered in the guide, along with the design components and considerations for the security features associated with the use case.
- The Deploy section discusses the automated deployment of the Cisco SD-WAN security features specific to the secure Direct Cloud Access (DIA) 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, Intrusion Prevention System (IPS), Advanced Malware Protection (AMP) and DNS/Web-layer Security with Umbrella Integration, is configured.

Refer to Appendix B for the hardware models and software versions used in this deployment guide, Appendix C 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 to establish secure Direct Cloud Access (DCA) within SD-WAN enabled remote sites.

Define: About the Solution

In traditional wide-area networking, Internet traffic from a branch or remote site is sent to a central location such as a data center or regional hub site. This allows for the traffic returning from the Internet to be scrubbed by a data center security stack before being sent back to the branch. This is traditionally done due to the prohibitive cost of deploying a security stack in every branch or remote site location.

However, as the demand for Internet traffic increases, more companies are utilizing cloud services such as SaaS (e.g. Office 365, Box) and IaaS. In addition, more applications are Internet-based, more business employees are teleworking, and Internet of Things (IoT) devices are demanding bandwidth as well. Backhauling traffic to a central site across the transport tunnels for Internet access causes increased bandwidth utilization from branch to the central site, along with increased latency, resulting in a degradation of overall application performance.

The solution is to enable local internet exit for guest and employee traffic at the remote site by deploying and maintaining Cisco SD-WAN within your WAN infrastructure. This allows you to manage your Cisco SD-WAN WAN network centrally via Cisco vManage GUI and leverage the security capabilities embedded natively in the Cisco SD-WAN single-pane of management.

Benefits of Enabling Local Internet Exit within the Remote Site

Some of the benefits of enabling local Internet breakout within the remote-site include,

- Improved Internet experience by eliminating latency in backhauling traffic to a central site.
- Enhanced crypto throughput and better application performance for corporate applications due to reduced load on IPsec encrypted WAN links.
- Reduced bandwidth consumption at the central site, which thereby also reduces WAN costs.
- Simplified Cisco SD-WAN template and policy configuration at the remote site to enable local Internet exit of specific application traffic, keeping business-critical applications on premium WAN links.
- Controlled access to the Internet per VPN basis, by leveraging segmentation to allow for separation of employee and guest traffic.

Within an Internet exit enabled branch or remote site, users and branch network can be secured by implementing Cisco SD-WAN security features within the remote site devices via the vManage GUI. 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 (URLF), Advanced Malware Protection (AMP), and DNS/Web-layer Security.

Based on common customer deployment scenarios, predefined workflows are added into vManage to facilitate ease of deployment for the following use cases, such as:

- Compliance Use Case: This use case caters to any organization that services customers, accepts credit card payment to be PCI compliant. In addition to the data being encrypted and sent over an IPsec tunnel, all packets are subjected to a stateful firewall and an IPS solution.

  Security features leveraged in this use case include Enterprise Firewall with Application Awareness and Intrusion Prevention System (IPS).

- Guest Access Use Case: This use case caters to companies wherein guests bring in BYOD devices and connect to an open or password protected Internet connection. To avoid any litigation, companies are liable to inspect and provide a good content filtering solution.

  Security features leveraged in this use case include Enterprise Firewall with Application Awareness and URL Filtering (URLF).

- Direct Cloud Access (DCA): This use case caters to customers who need to route some SaaS application traffic for optimal performance via local Internet exit and the rest of the Internet traffic via the HQ. The cloud traffic is inspected for malware.

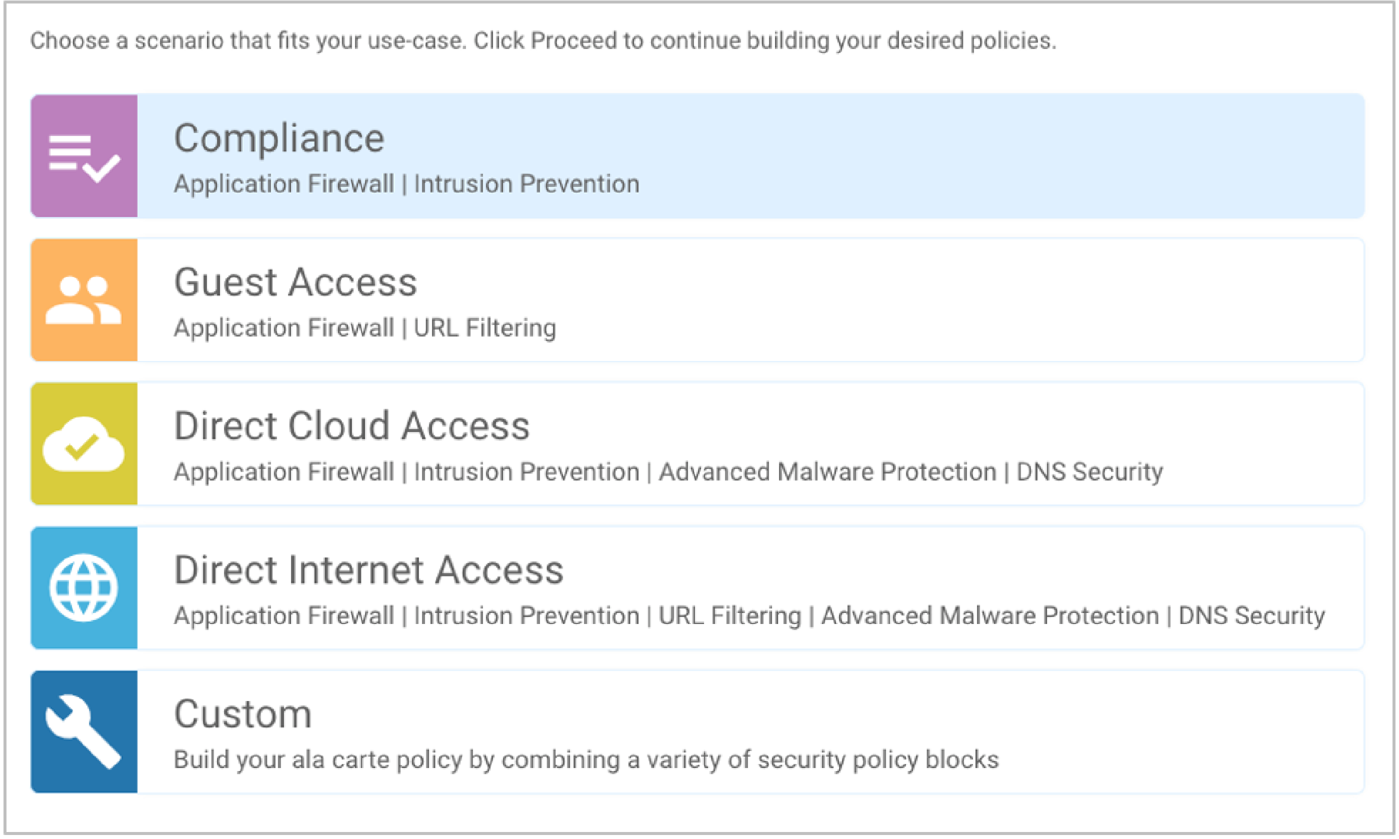
  Security features leveraged in this use case include Enterprise Firewall with Application Awareness, Intrusion Prevention System (IPS), Advanced Malware Protection (AMP) and DNS/Web-layer Security.

- Direct Internet Access (DIA): This use case caters to organizations wherein all Internet traffic from a remote site exit via the local branch Internet exit and is inspected for malware, along with content filtering etc.

  Security features leveraged in this use case include Enterprise Firewall with Application Awareness, Intrusion Prevention System (IPS), URL Filtering (URLF), Advanced Malware Protection (AMP) and DNS/Web-layer Security.

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

Figure 2. Intent-Based Use Cases



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

Within this solution, the security features available within the Direct Cloud Access (DCA) use case is explained.

Benefits of Deploying SD-WAN Security

Some of the benefits of deploying Cisco SD-WAN security policy within the remote site include:

- 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 to multiple WAN Edge devices at the same time.
- Cisco SD-WAN security solution eliminates the need to deploy any addition security appliance within your SD-WAN network, thereby, avoiding any additional costs or complications associated with designing, configuring and managing those appliances.
- Centralized management: Deploy, troubleshoot and monitor the SD-WAN overlay solution with security capabilities across the WAN Edge devices centrally via the Cisco vManage GUI.
- Comprehensive SD-WAN security: With security capabilities enabled on your WAN Edge device, you can secure the remote site with:
    - Enterprise firewall with application awareness restricts access to certain Internet destinations based on IP address/ port/ application family and more for remote employees and guests, with improved application experience.
    - Intrusion Prevention System (IPS) with deep-packet inspection mitigates network attacks by providing your network with the intelligence to accurately identify, classify, and stop or block malicious traffic in real time.
    - Advanced Malware Protection (AMP) leverages global threat intelligence, advanced sandboxing and real-time malware blocking to prevent breaches by continuously analyzing the file activity across the extended network to quickly detect, contain, and remove malware.
    - DNS/Web-layer Security with Umbrella Integration leverages cloud security platforms to improve security visibility, to detect compromised systems, and to protect users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

Design: Cisco SD-WAN Secure Direct Cloud Access

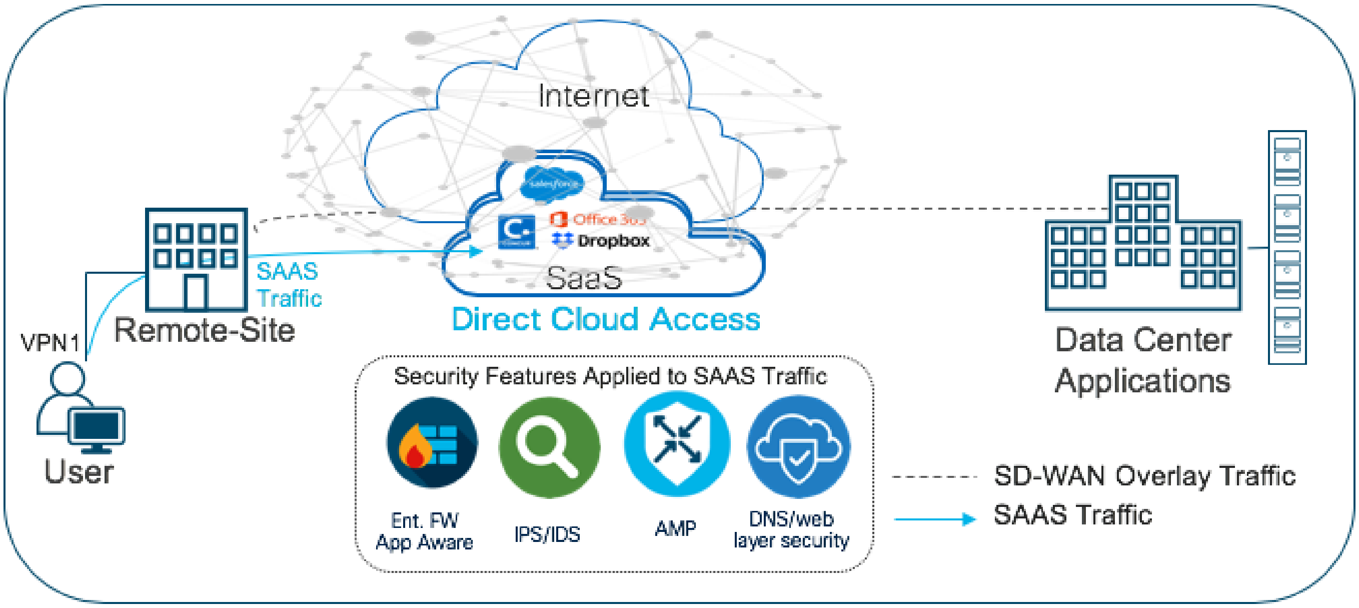
Out of the four intent-based use cases available within the vManage security policy, the use case discussed in this guide is secure Direct Cloud Access (DCA).

Use Case - Secure Direct Cloud Access

Within the direct cloud access use case, the primary requirement is to allow users to route some or all of the critical or non-critical SaaS application traffic directly from the remote site WAN Edge router via the local Internet exit. This helps to offload some of the SaaS traffic from premium WAN connections and improve application experience.

The second requirement is to thwart any potential threats that could come from cloud hosted applications and its associated file download. In this use case, Enterprise firewall with Application Awareness is configured to inspect and limit access to cloud applications, Snort IPS/IDS to inspect & block known attack or malware signatures, Advanced Malware Protection (AMP) to prevent download of malicious content or file, and DNS/Web-layer security as an additional layer of protection at the DNS layer.

Figure 3. Traffic Flow - Direct Cloud Access Use Case



The Cisco SD-WAN features leveraged within this use case include,

- Secure Segmentation via VPN/Zone to segment user traffic into zones and VPN/VRF.
- Centralized data policy to redirect some or all of the segmented user cloud traffic via local Internet exit.
- (optional) Application Awareness Route (AAR) policy to track network and path characteristics of the data plane tunnels between the WAN Edge routers and use the collected information to compute optimal paths for cloud-based SaaS traffic.
- Enterprise Firewall with Application Awareness, Intrusion Prevention System (IPS), Advanced Malware Protection (AMP) and DNS/Web-layer Security to maintain a secure Direct Cloud Access (DCA)

Technical tip

In this deployment guide, enterprise firewall policy with application awareness is leveraged for traffic allow/drop and it works similar to a localized security policy that defines the conditions that data traffic flow originating from the source zone must match to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, protocols (TCP, UDP, ICMP), and application names or families. Matching flows for prefixes, ports, and protocols can be allowed, dropped, or inspected, and their packet headers can be logged. Non-matching flows are dropped by default. However, note that applications listed in the " application/application family list to drop" will be blocked regardless of the action associated with them. It is currently not possible to create a firewall rule to allow for flow of specific applications in the 16.12/19.2 release.

Table 1. Cisco SD-WAN Features for Direct Cloud Access

Security Pillar	SD-WAN Security Feature
Segmentation	VPN and Zone
Local SAAS exit	Centralized Data Policy

Security Pillar	SD-WAN Security Feature
Controlled Redirection	Application Aware Routing (optional)
Perimeter Control	Enterprise Firewall with Application Awareness
Attack Prevention	Intrusion Prevention System
Malware Prevention	Advanced Malware Protection
Liability Protection	DNS/ Web-layer Security

Direct Internet Access Design and Deployment: For the design considerations and configuration of segmentation (VPN), centralized data policy and NAT DIA route on remote-site WAN Edge devices refer to the Cisco SD-WAN: Enabling Direct Internet Access design and deployment guide.

Application Aware Routing Design and Deployment: For the steps to configure Application Awareness Routing (AAR), refer to the configuration guide - Configuring Application-Aware Routing.

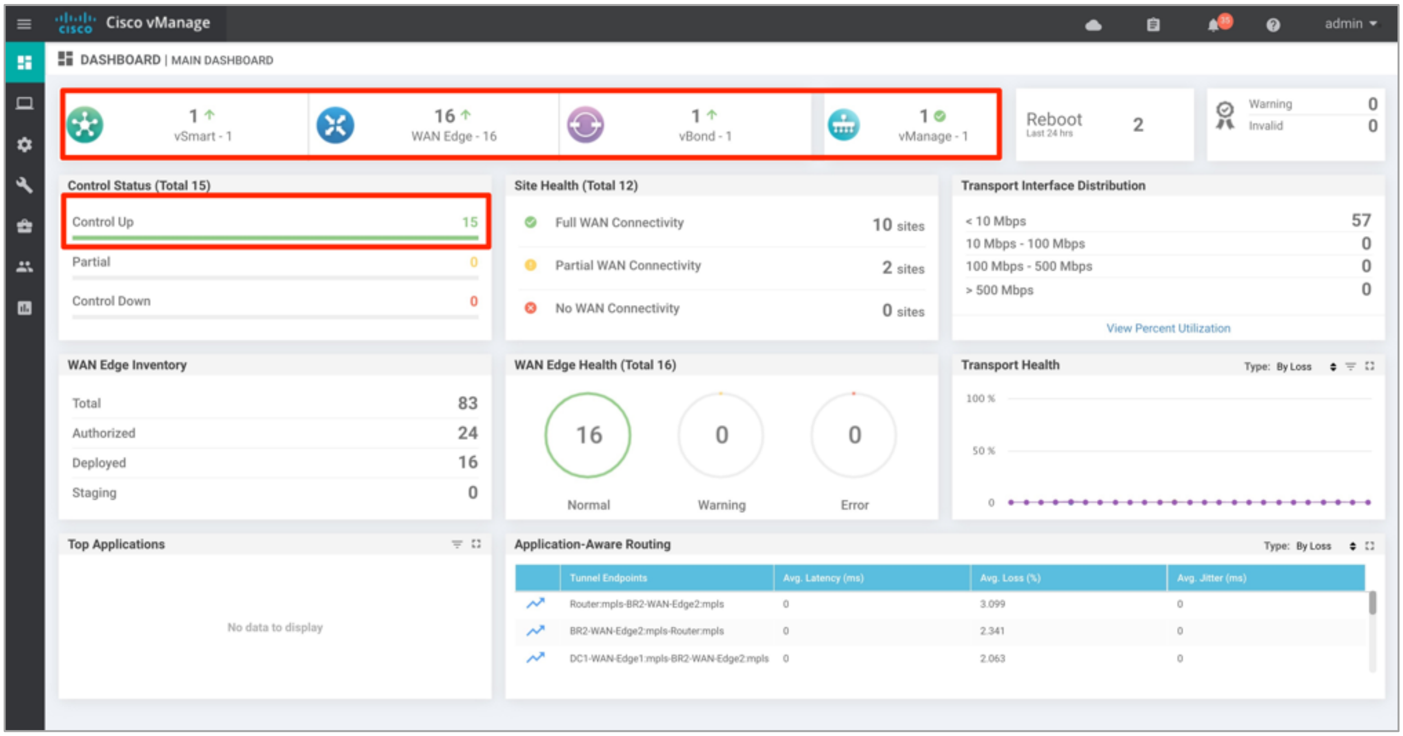
Security Policy Design: For the design components, workings and considerations of Cisco SD-WAN Security features such as, Enterprise Firewall with Application Awareness (Application Firewall), Intrusion Prevention System (IPS), URL-Filtering, Advanced Malware Protection (AMP) and DNS/Web-layer Security, refer to the Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices.

Prerequisites: Cisco SD-WAN Secure Direct Cloud Access

This section covers the prerequisites specific to secure Direct Cloud Access (DCA).

Process 1: Successful Deployment of Controllers and WAN Edge Devices

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



1 ↑	vSmart - 1
16 ↑	WAN Edge - 16
1 ↑	vBond - 1
1 ✓	vManage - 1

Reboot Last 24 hrs 2

Warning	0
Invalid	0

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

Top Applications

No data to display

Application-Aware Routing

Type: By Loss

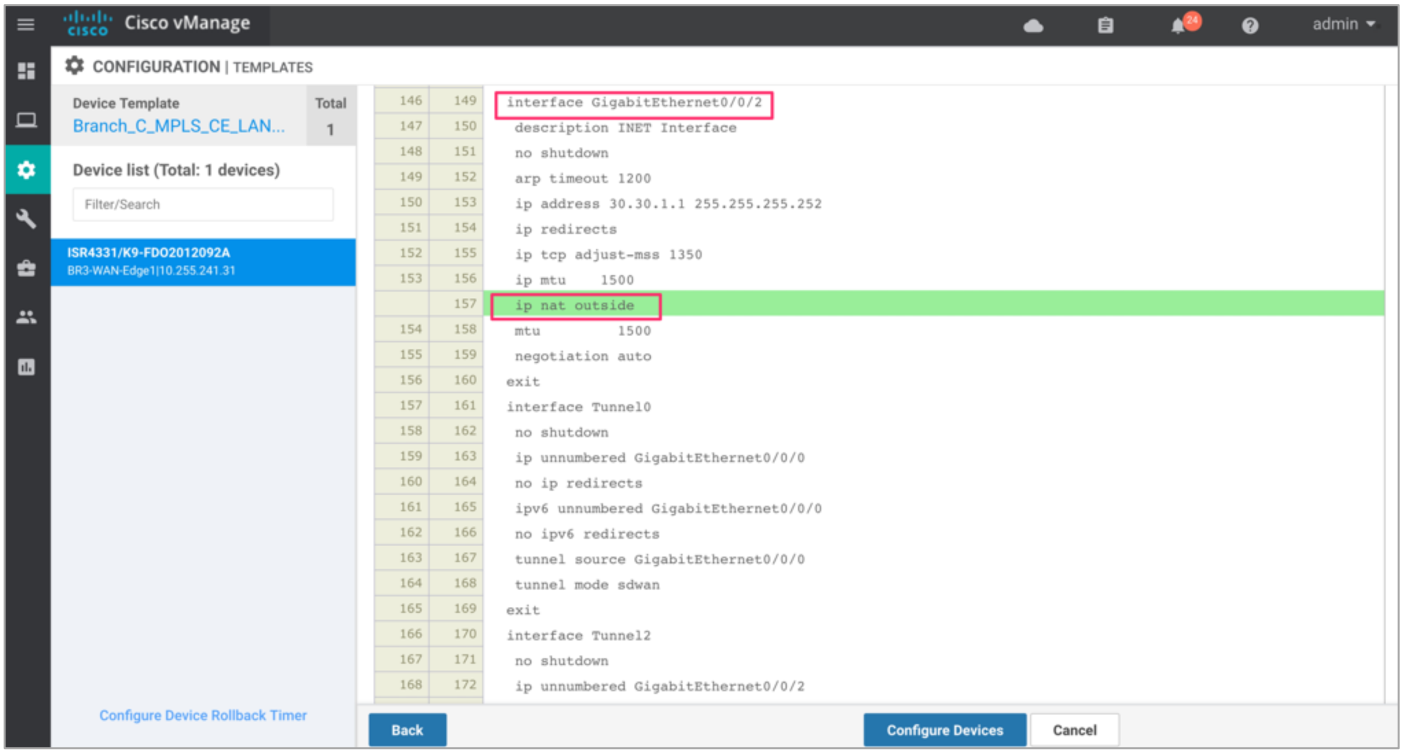
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	3.099	0
BR2-WAN-Edge2:mpls-Router:mpls	0	2.341	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	2.063	0

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 memory. For details refer to the design guide – Security Policy for Cisco IOS-XE SD-WAN Devices.

Process 2: Enable Local Internet Exit for User SAAS Traffic using Centralized Policy

Step 1. Make sure to enable the NAT feature on the Internet transport VPN 0 Interface. The NAT feature translates the user IP address to the Internet facing Interface's IP address.



Device Template: Branch_C_MPLS_CE_LAN...
Total: 1

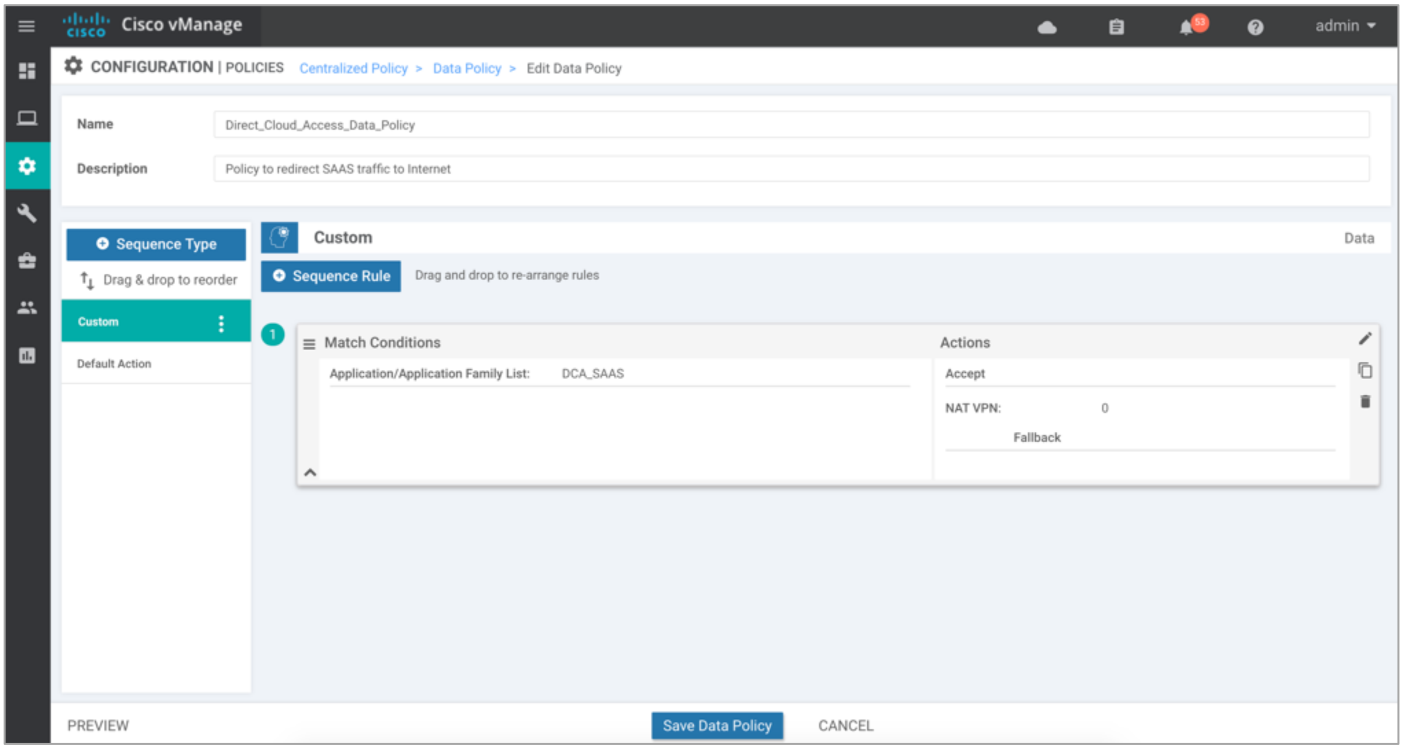
Device list (Total: 1 devices)

ISR4331/K9-FDO2012092A
BR3-WAN-Edge1|10.255.241.31

```
interface GigabitEthernet0/0/2
 description INET Interface
 no shutdown
 arp timeout 1200
 ip address 30.30.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 ip nat outside
 mtu          1500
 negotiation auto
exit
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit
interface Tunnel2
 no shutdown
 ip unnumbered GigabitEthernet0/0/2
```

Step 2. Configure centralized data policy to redirect certain application (cloud) traffic to transport VPN 0 NAT Interface. Within the data policy, application traffic matching a list of applications (SAAS_Application) is leaked from service-side VPN 1 to a NAT enabled interface in transport VPN 0. The Default Action is set to Accept.

Note: In this example, NAT Fallback feature is not enabled.



Name: Direct_Cloud_Access_Data_Policy

Description: Policy to redirect SAAS traffic to Internet

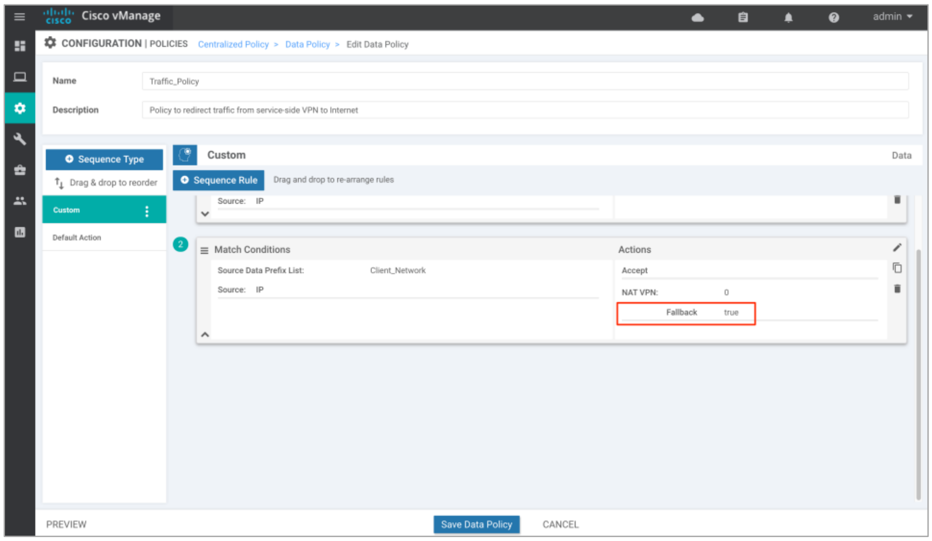
Custom — Data

Match Conditions		Actions	
Application/Application Family List:	DCA_SAAS	Accept	
		NAT VPN:	0
		Fallback	

Technical Tip

NAT Fallback feature is not supported today on IOS-XE SD-WAN WAN Edge devices. Note, regardless of whether the feature is enabled or not, the saved policy will still contain the fallback tab.

When the Fallback tab points to neither True/False, it means the tab is not enabled. When the feature is enabled, Fallback is set to True, as shown in the example figure below.



Name: Traffic_Policy

Description: Policy to redirect traffic from service-side VPN to Internet

Custom — Data

Source: IP

Match Conditions		Actions	
Source Data Prefix List:	Client_Network	Accept	
Source: IP		NAT VPN:	0
		Fallback	true

Based on your requirement, add in additional sequence rules within the traffic policy. In this policy, applications matched under SAAS_Application include Gmail, Office 365 and Facebook. Note, you can also enable local Internet breakout from the remote site by configuring a NAT DIA route to redirect traffic from service-side VPN to global, or NAT enabled transport VPN 0 Interface. For the step-by-step procedure to build NAT DIA route or centralized data policy, refer to Cisco SD-WAN: Enabling Direct Internet Access.

Technical tip
Due to First Packet Match (FPM), some application traffic may not be routed by the NAT DIA data policy, as it requires a number of packets to go through, before an application is matched.

In this guide, both the app-visibility and flow-visibility policy was enabled.

```
!
policy
 app-visibility
 flow-visibility
```

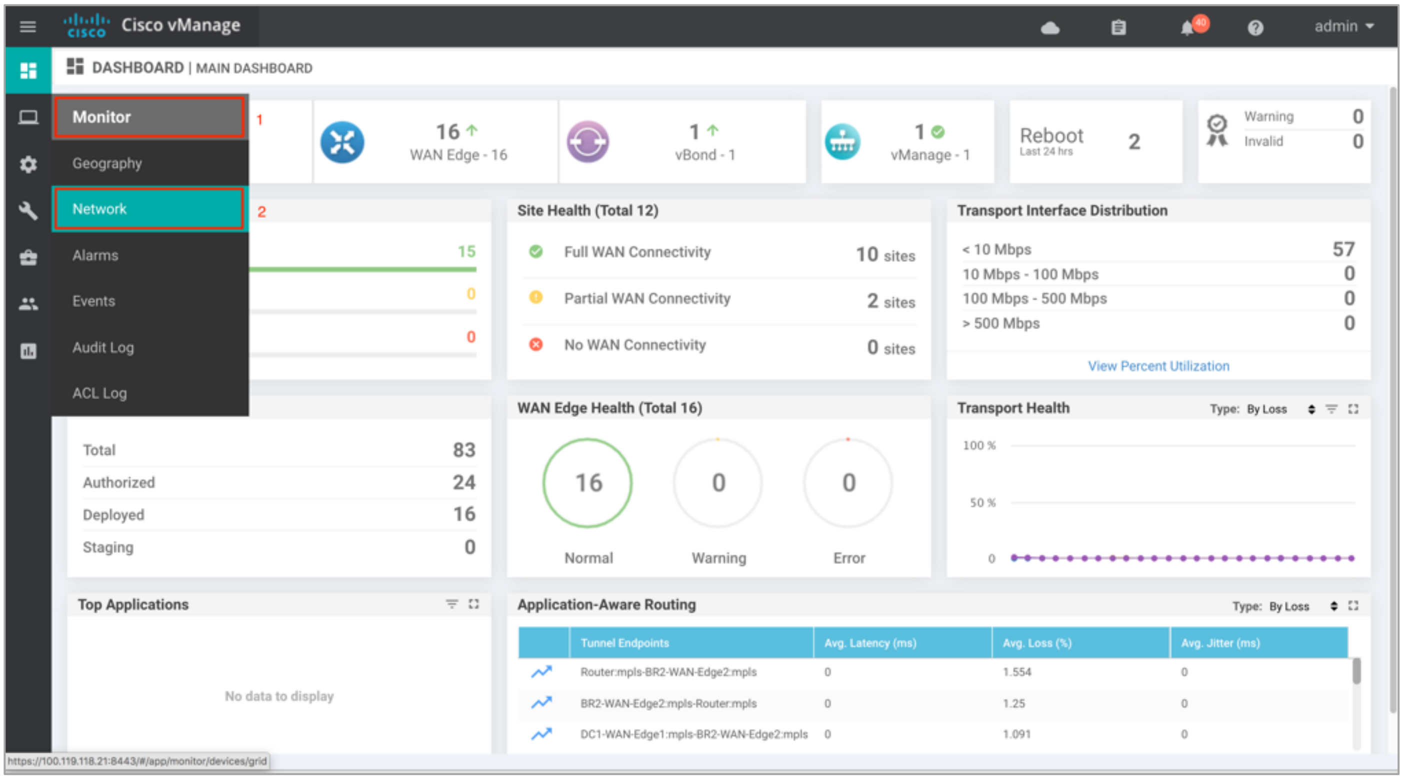
Technical tip
If you are deploying centralized data policy to enable DIA within the remote-site and also plan to configure umbrella Integration via the DNS/Web-layer security policy with target VPN as a service-side VPN, then the DNS Server IP address on the host machine must point to one of the IP addresses on the Edge device belonging to an interface which is part of the same VRF that umbrella belongs to. For instance, if the Target VPN in DNS/Web-layer Security (Umbrella integration) is configured as VPN 1 and an Interface within VPN 1 is configured as 10.1.1.1, then the DNS Server IP address on the host machine must be configured as 10.1.1.1. To use your local DNS server on the host/ client machine and still enable DIA and Umbrella integration on the WAN Edge router, then enable IP NAT route on the WAN Edge device and skip configuring centralized data policy. For the step-by-step procedures to build the NAT DIA route or centralized data policy, refer to Cisco SD-WAN: Enabling Direct Internet Access. Cause: Within the Data policy, nat-vpn0 action bypasses umbrella integration. The centralized data policy kicks in before the Umbrella redirection.

Process 3: Upload Software Virtual Image to Enable Snort

If you plan to deploy security features such as Intrusion Prevention/ Detection System (IPS/IDS), Advanced Malware Protection (AMP) or URL Filtering within the remote-site WAN Edge device, then begin by downloading the UTD Engine TAR file from the Cisco website to enable these features. Make sure to upload the downloaded TAR file to your vManage software repository prior to building the security policy.

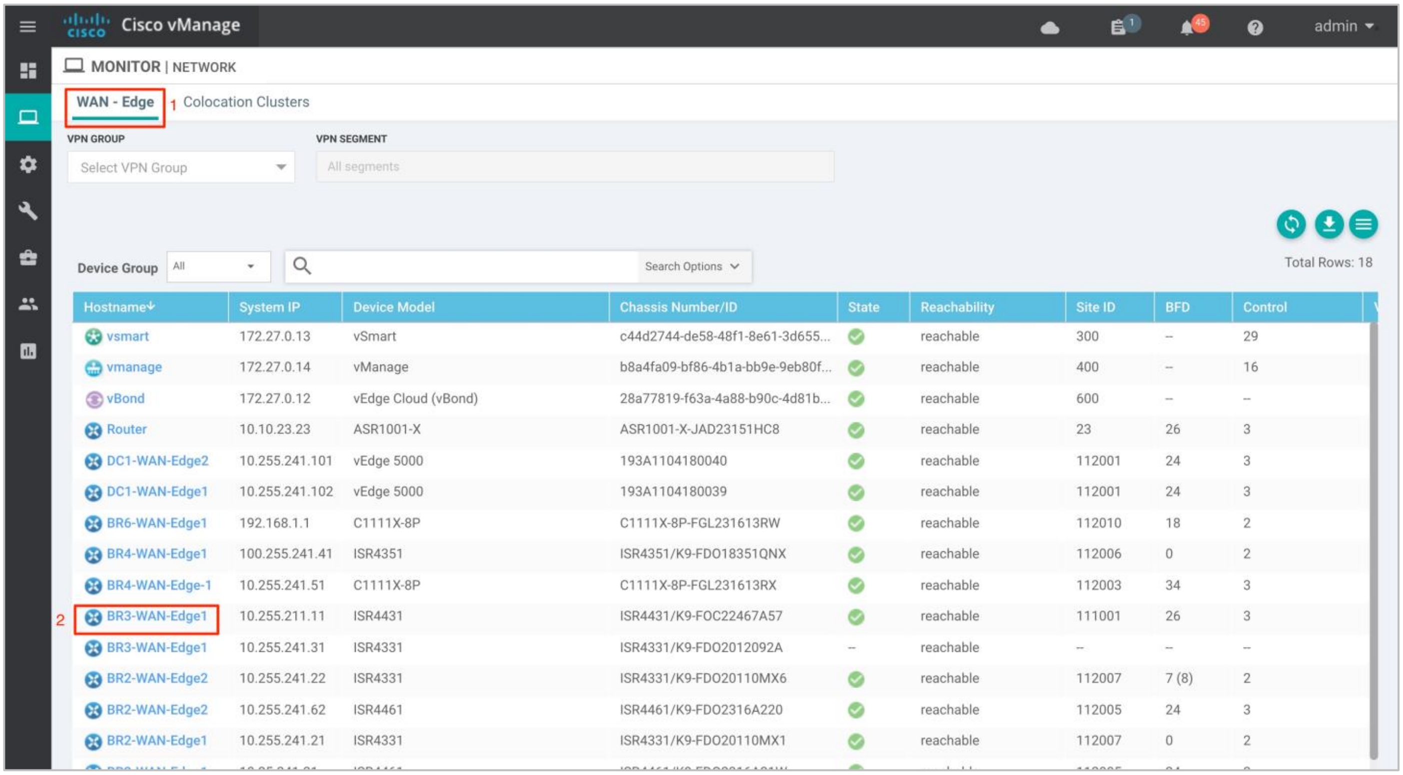
Once the configured security policy is deployed in a WAN Edge router, then the TAR file is automatically downloaded from the vManage repository into the WAN Edge device to enable the required virtual services (IPS/ AMP/ URL Filtering).

Step 1.   Upload the correct Cisco security virtual image (UTD Engine TAR File) to vManage. To make sure a compatible image is downloaded from the Cisco website, login to vManage GUI and navigate to **Monitor** > **Network**.



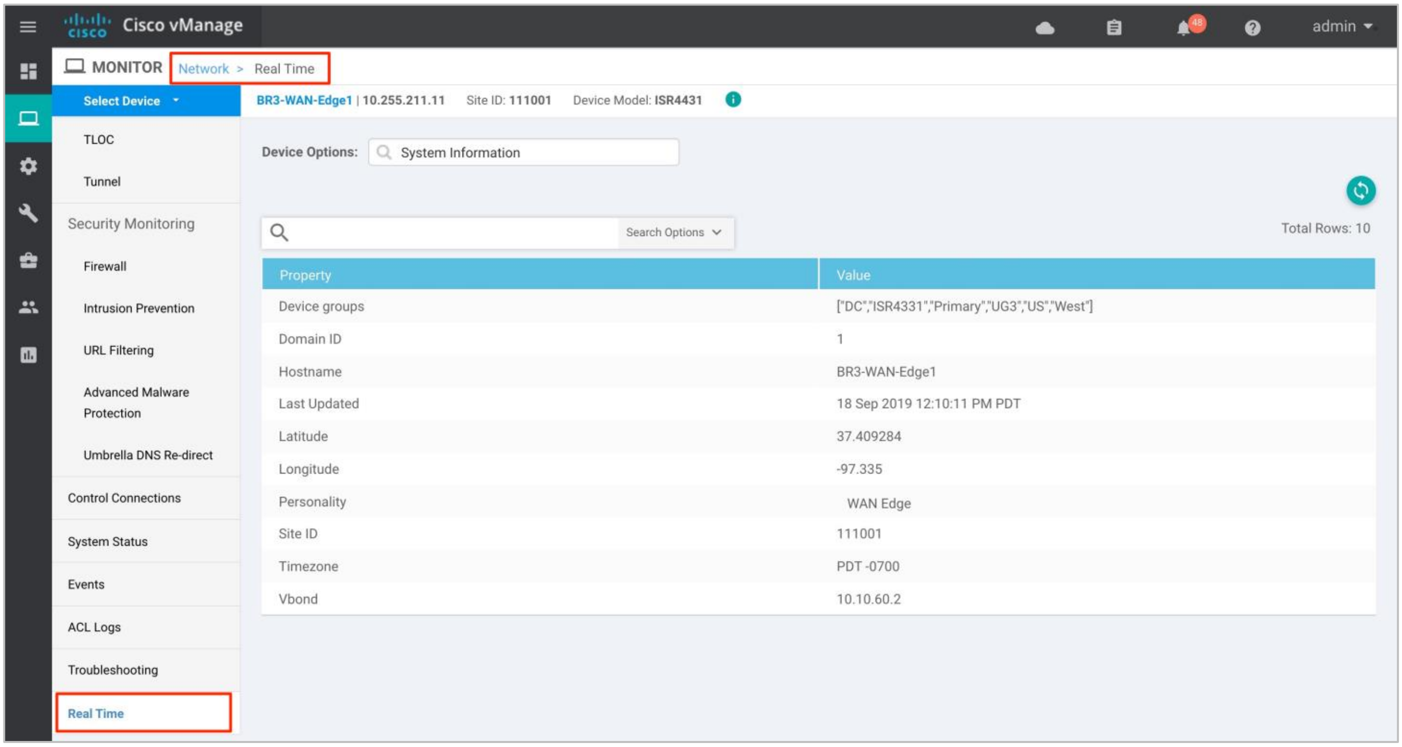
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0
BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0

Step 2. Each router image supports a specific range of versions for a hosted application. 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 on **Real Time**.



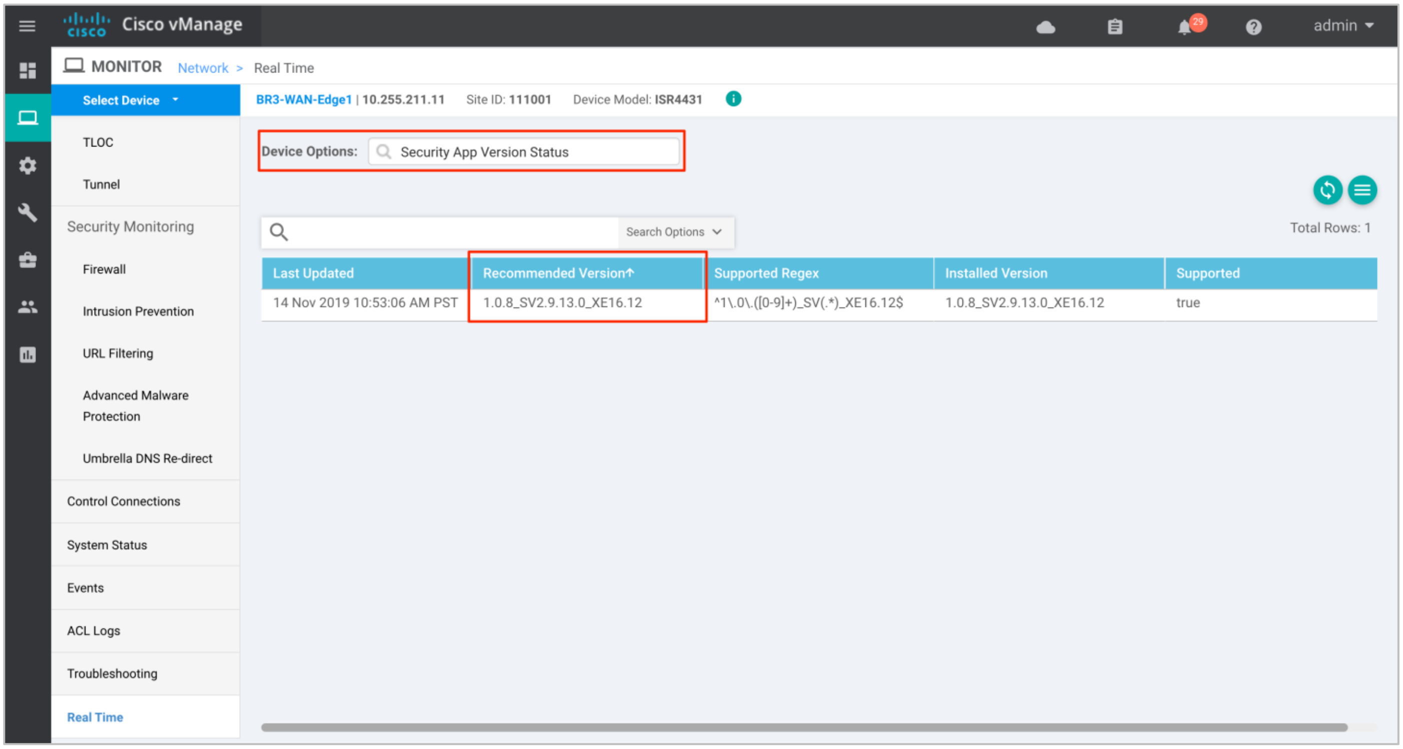
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: System Information

Total Rows: 10

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

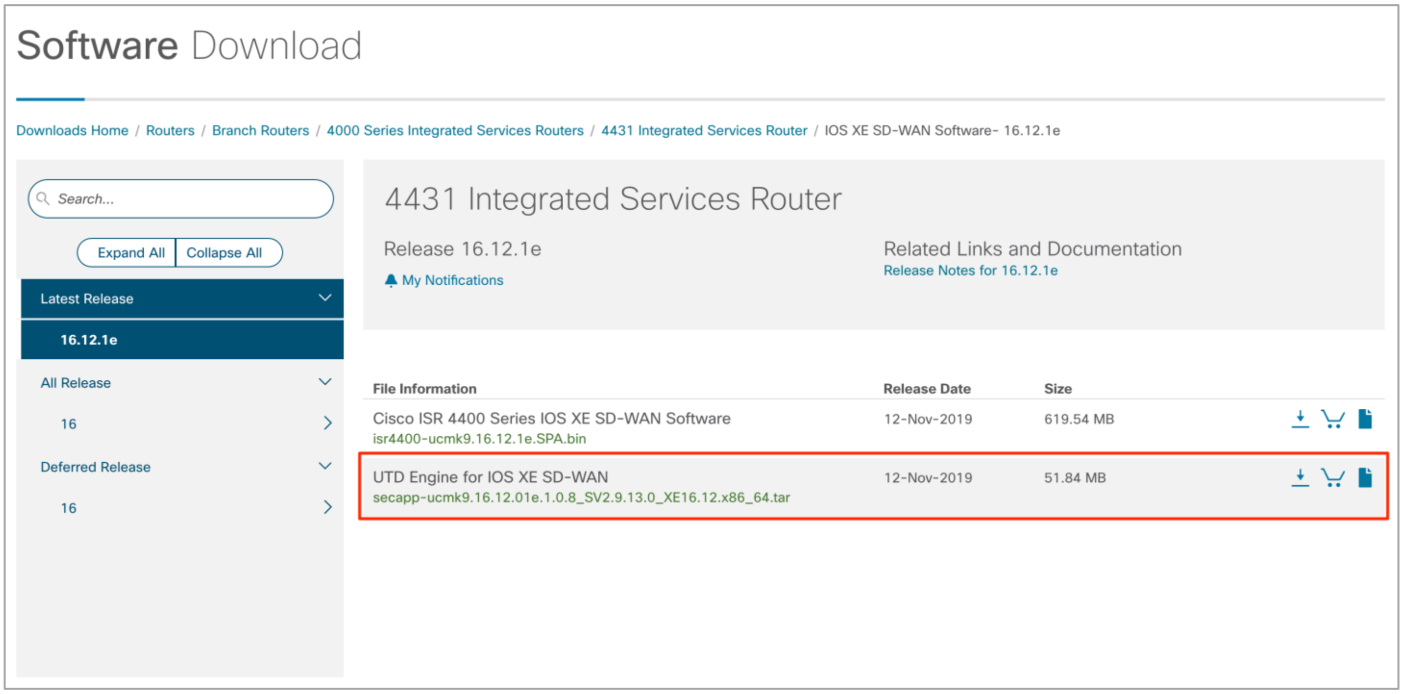
Device Options: Security App Version Status

Total Rows: 1

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

Note: The third column displays the **Supported Regex** pattern. The supported regex is the range of compatible virtual image versions for the router image.

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

4431 Integrated Services Router

Release 16.12.1e

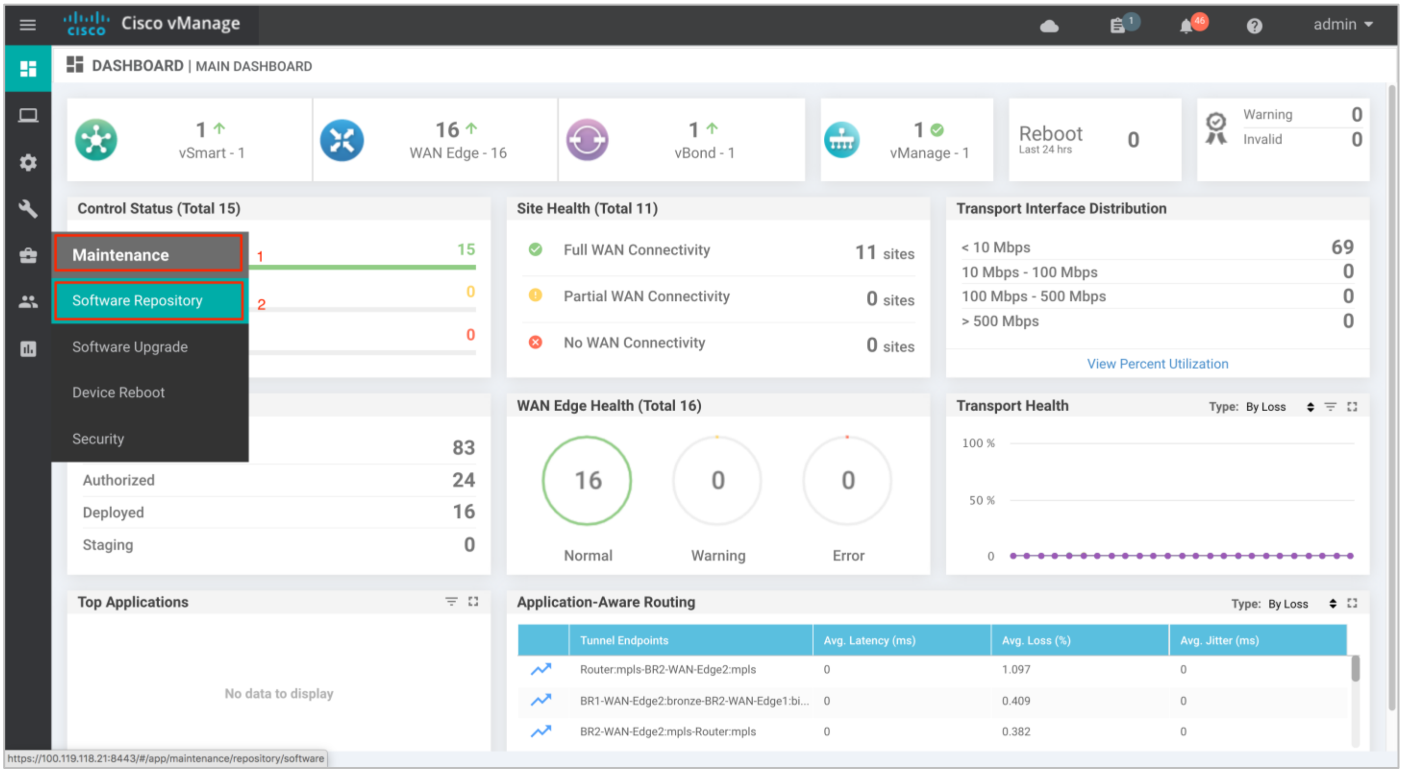
My Notifications

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**.



Control Status (Total 15)

15

0

0

	83
Authorized	24
Deployed	16
Staging	0

Site Health (Total 11)

Full WAN Connectivity	11 sites
Partial WAN Connectivity	0 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

< 10 Mbps	69
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

WAN Edge Health (Total 16)

Top Applications

No data to display

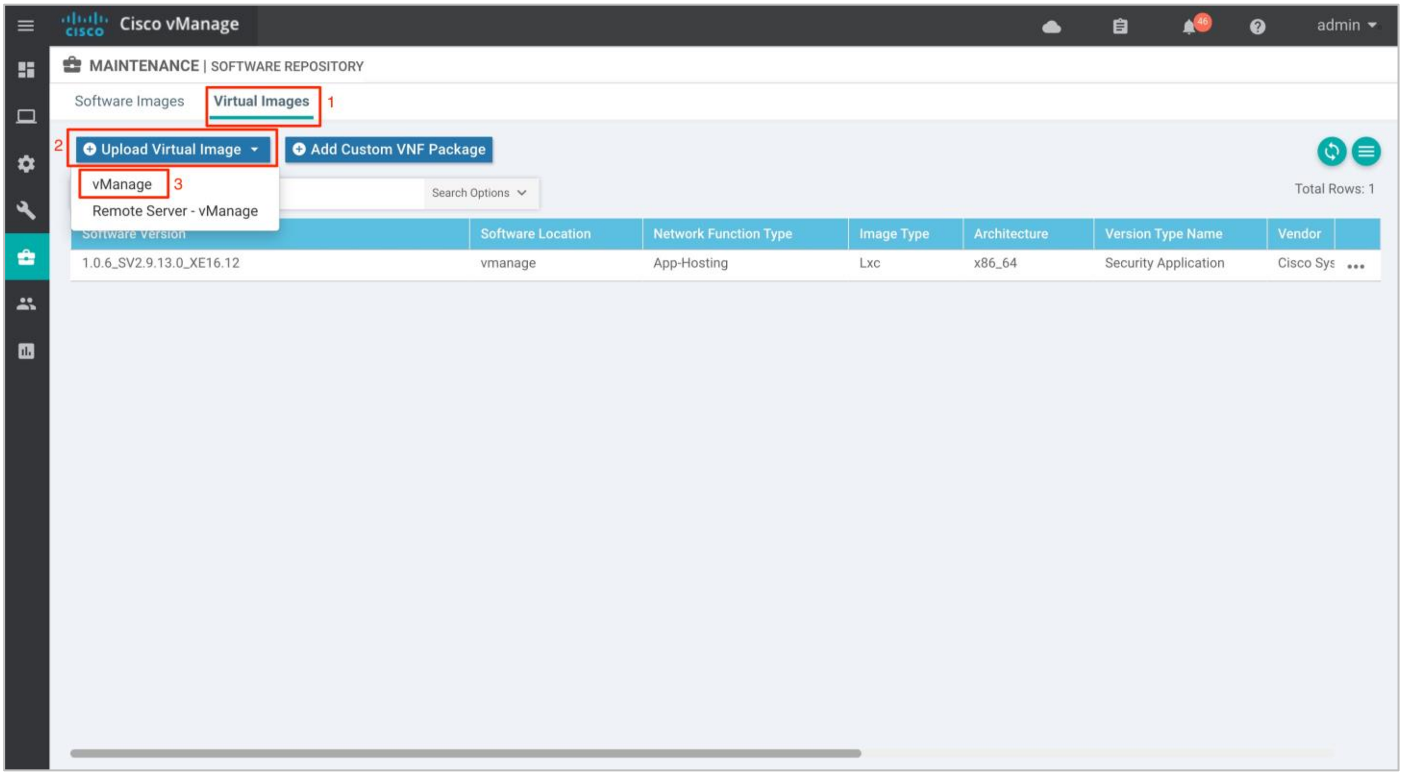
Application-Aware Routing

Type: By Loss

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

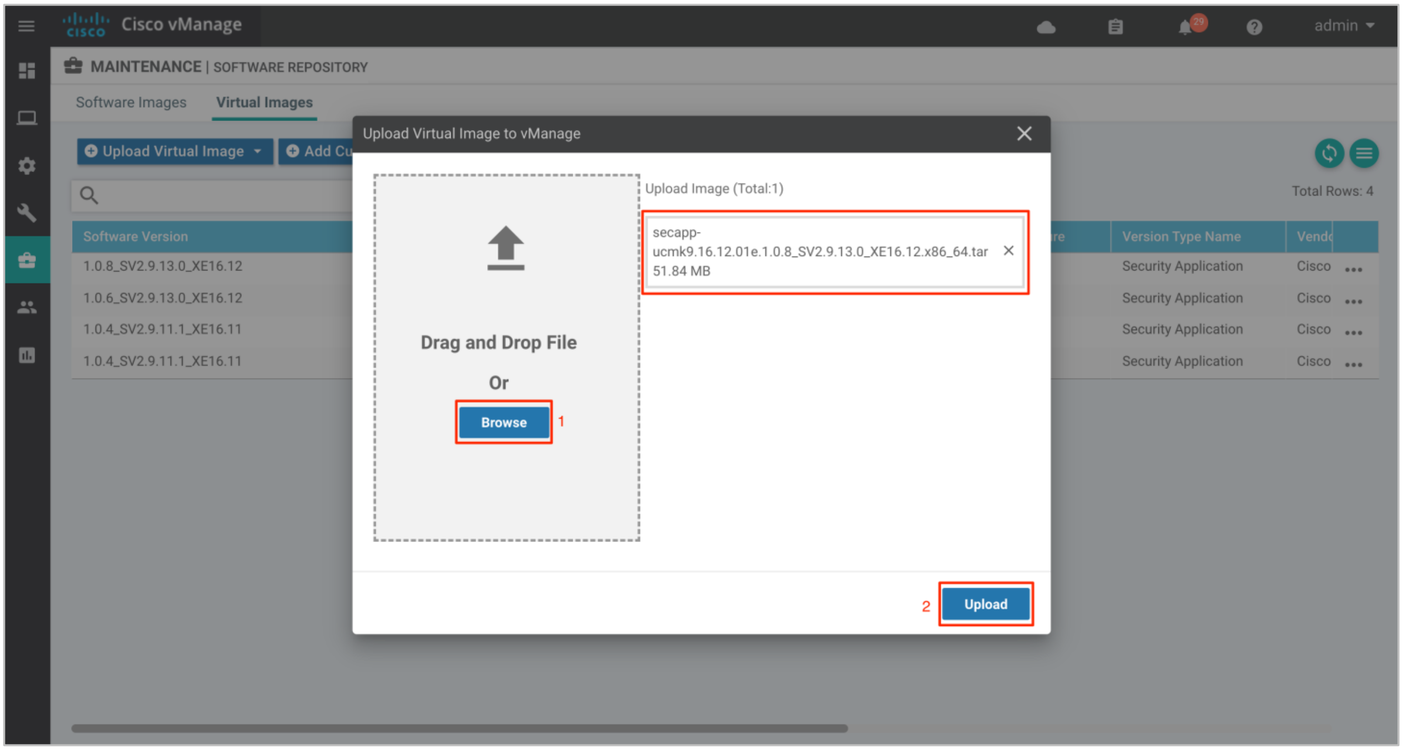
https://100.119.118.21:8443/#/app/maintenance/repository/software

Step 7. To upload the UTD file to the vManage **Software Repository**, click on **Upload Virtual Image** tab and select **vManage.**



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 on **Browse** to upload the downloaded UTD image. The image will appear on the right, and Click on **Upload** to add the image into the **Software Repository**. In case you already have the same image uploaded a **notification** of possible overwrite will populate.



Upload Image (Total:1)

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	Vendo
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

When the security policy is activated, the UTD image is automatically downloaded from the vManage virtual images software repository into the device's flash drive over a control plane connection.

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

Process 4: (Optional) Create a Security App Hosting Profile Template

As explained in the design section on attaching a configured IPS/ AMP/ URL security policy within the device template, a sub-template titled **Container Profile** must be added. The container profile template allows you to enable/disable NAT for your virtual services (IPS/ AMP/ URL Security) and allocate resources for the virtual services.

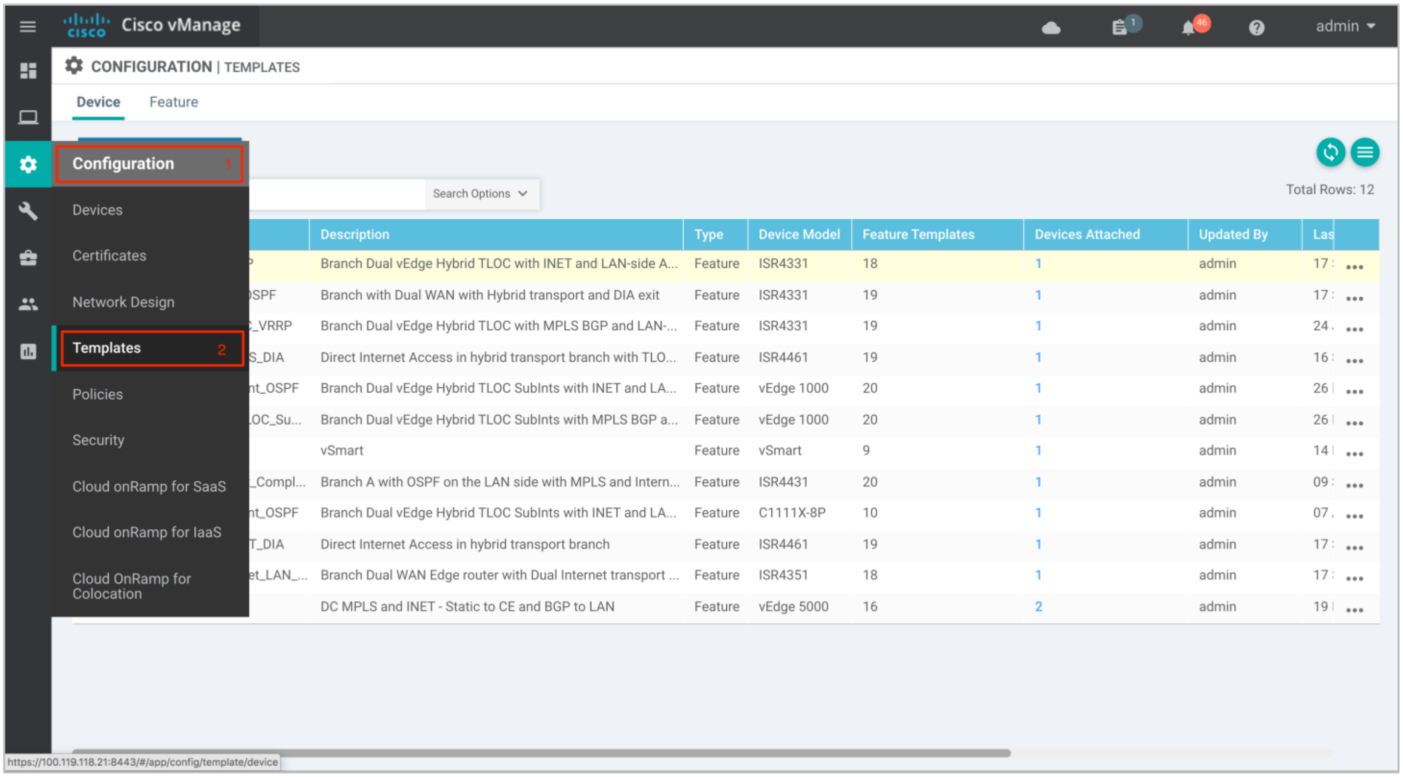
The container profile template contains:

- **Resource Profile** that is set to **Default**, which allocates one core. For higher throughput, you may set the resource profile to **High**, which allocates two cores.
- **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 syslog's to an external syslog server that is not necessarily in the Data Center.

Note: 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 the Resource Profile is set to **Default.**

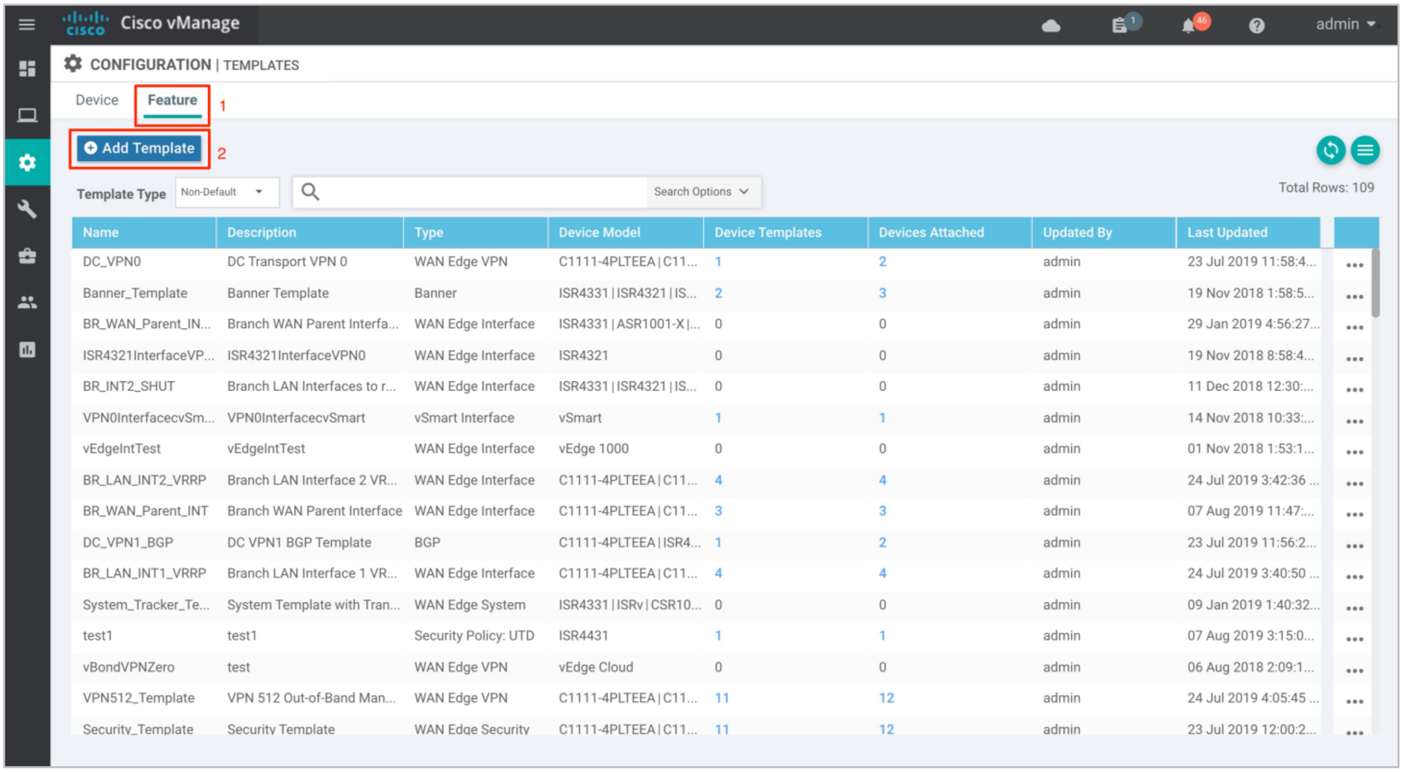
To create a new template, proceed to the steps below,

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



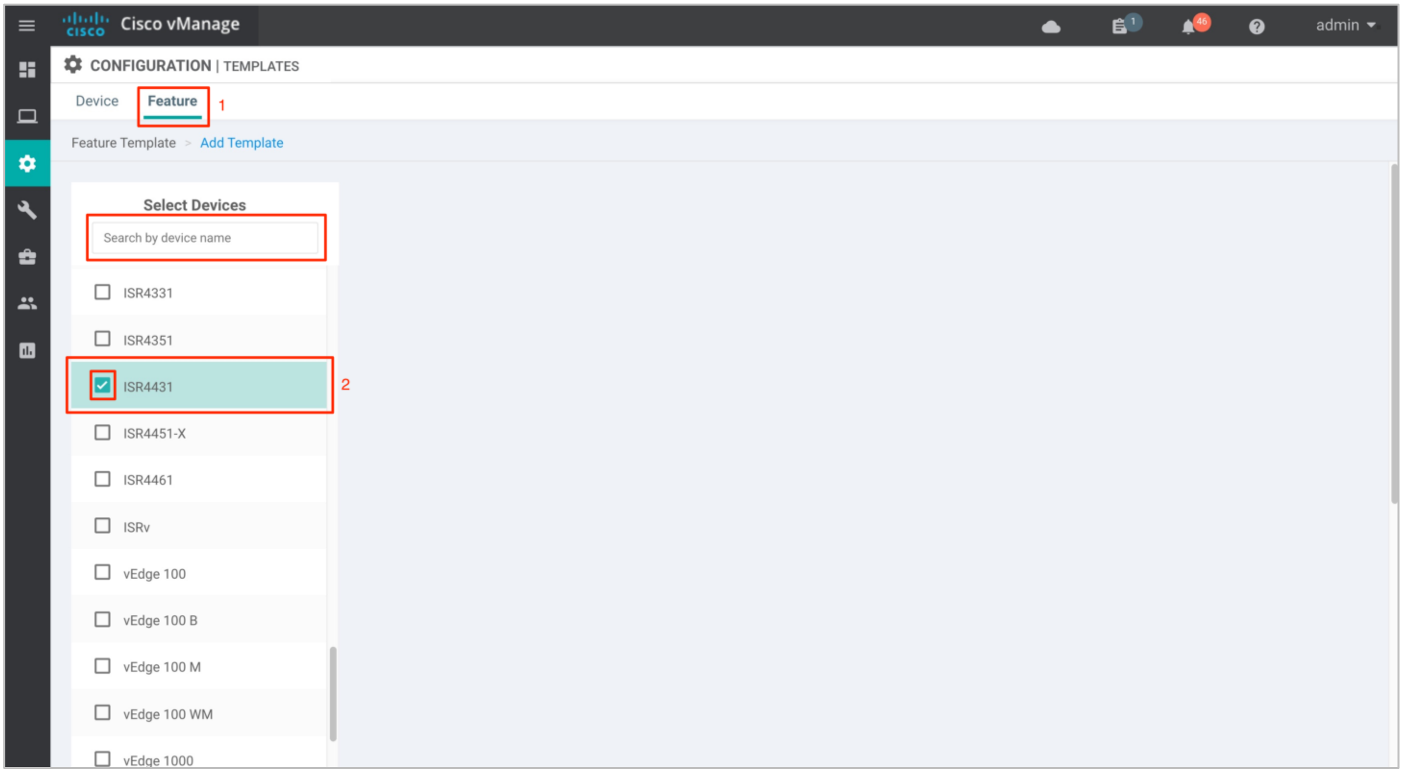
	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Las
P	Branch Dual vEdge Hybrid TLOC with INET and LAN-side A...	Feature	ISR4331	18	1	admin	17
)SPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	19	1	admin	17
_VRRP	Branch Dual vEdge Hybrid TLOC with 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 on Add **Template** to create a new feature template.

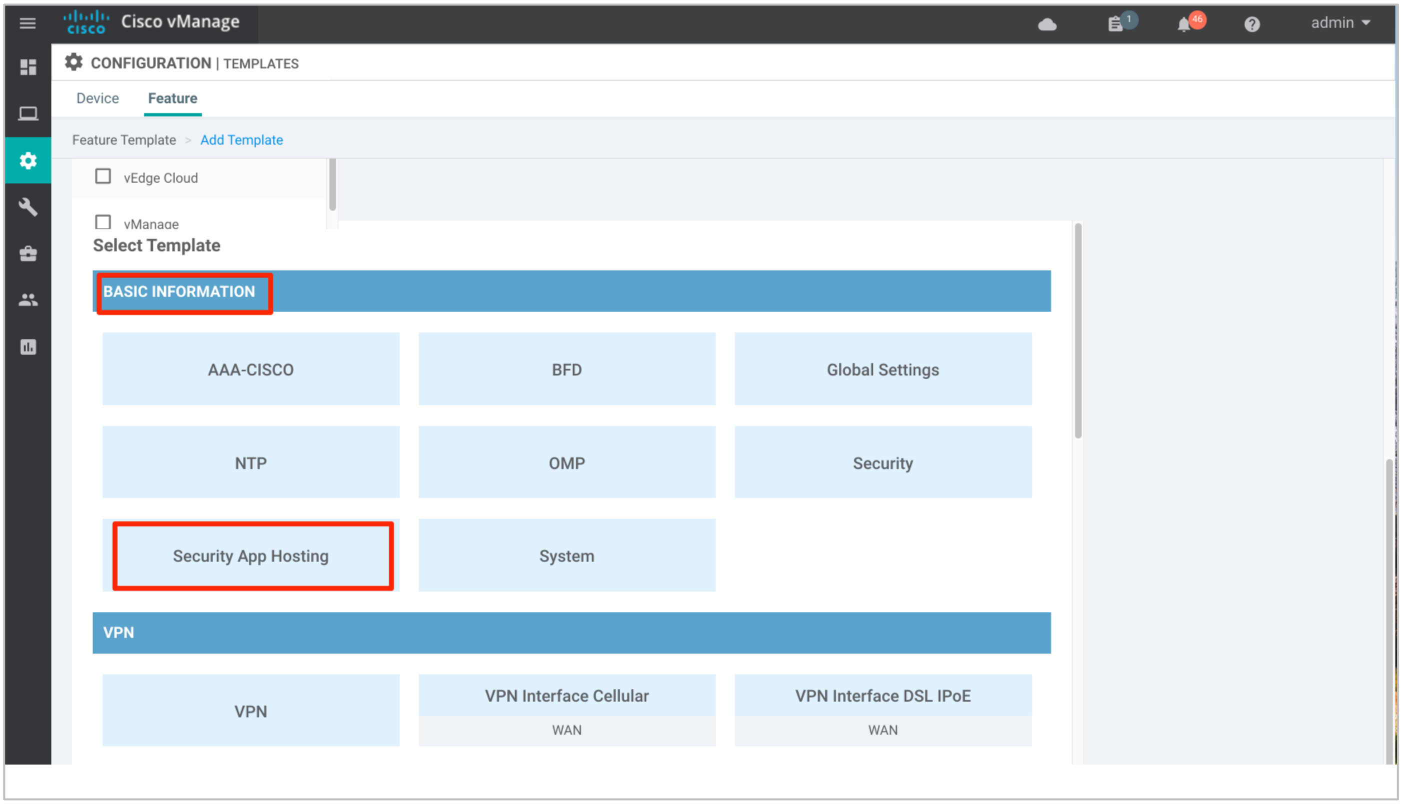


Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
DC_VPN0	DC Transport VPN 0	WAN Edge VPN	C1111-4PLTEEA | C11...	1	2	admin	23 Jul 2019 11:58:4...
Banner_Template	Banner Template	Banner	ISR4331 | ISR4321 | IS...	2	3	admin	19 Nov 2018 1:58:5...
BR_WAN_Parent_IN...	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...

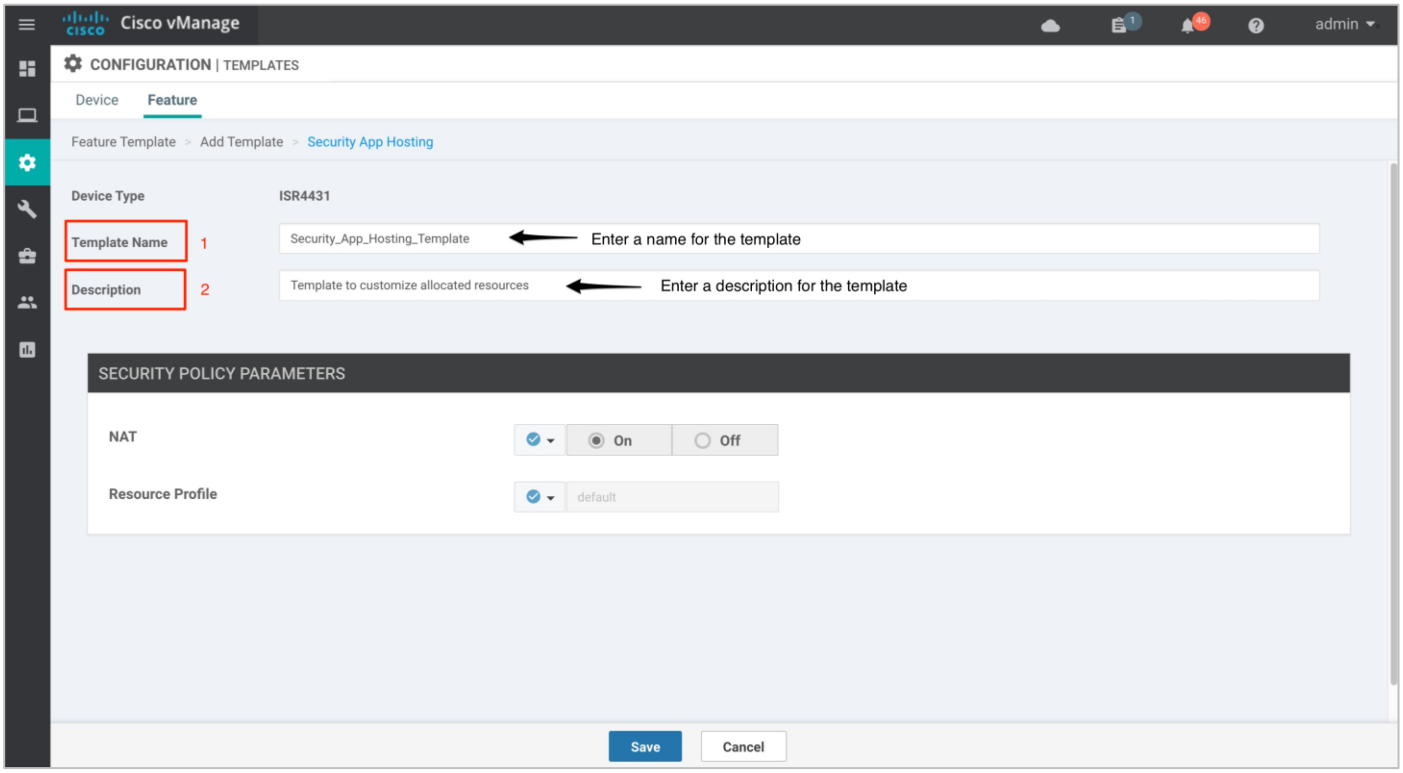
Step 3. Within **Feature Template**, select a device(s) or enter the device in the search bar.



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



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


Cisco vManage
admin
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > Security App Hosting

Device Type ISR4431

Template Name 1 Security_App_Hosting_Template ← Enter a name for the template

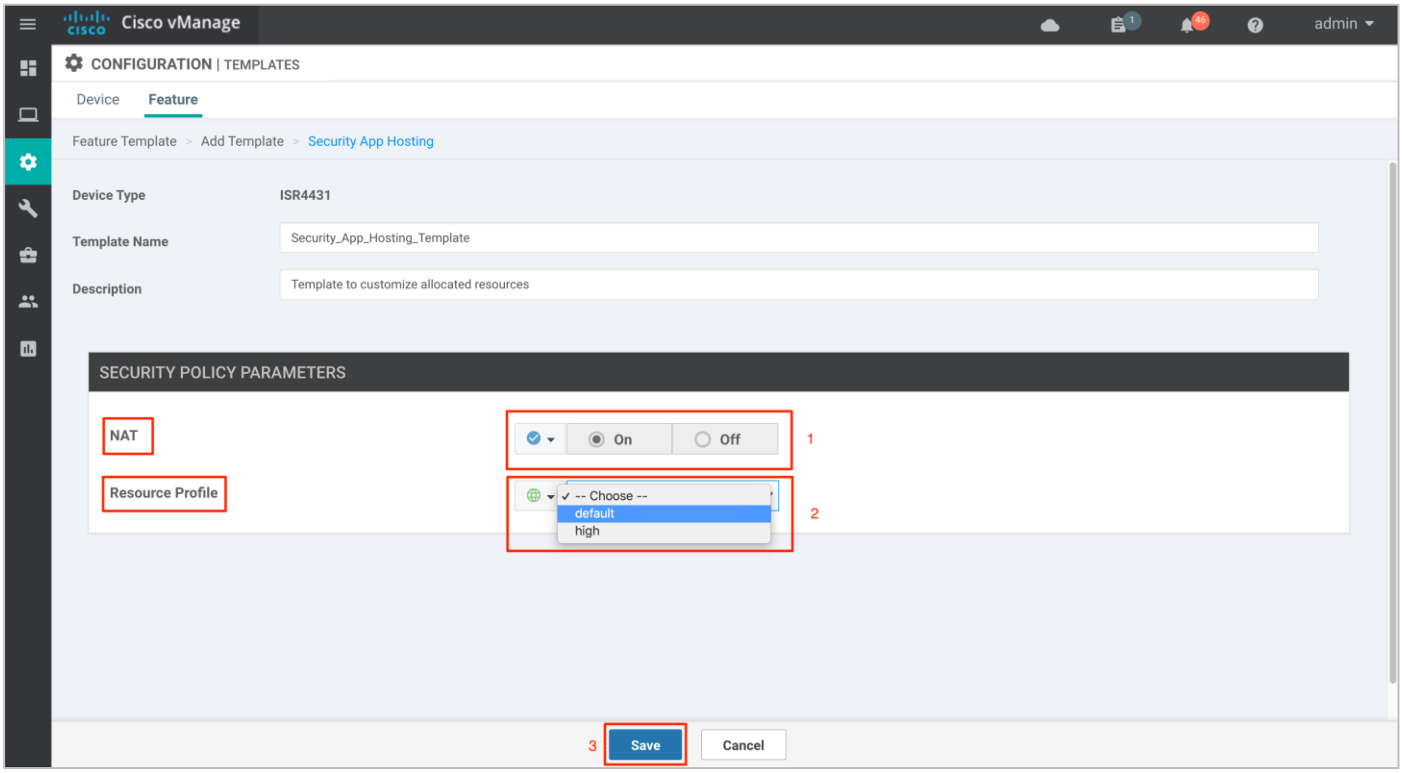
Description 2 Template to customize allocated resources ← Enter a description for the template

SECURITY POLICY PARAMETERS

NAT ● On ○ Off

Resource Profile default

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.** Please refer to the Security Policy for Cisco IOS-XE SD-WAN Devices Design Guide, before making changes to the template. Finally, **Save** the template.


Cisco vManage
admin
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > Security App Hosting

Device Type ISR4431

Template Name Security_App_Hosting_Template

Description Template to customize allocated resources

SECURITY POLICY PARAMETERS

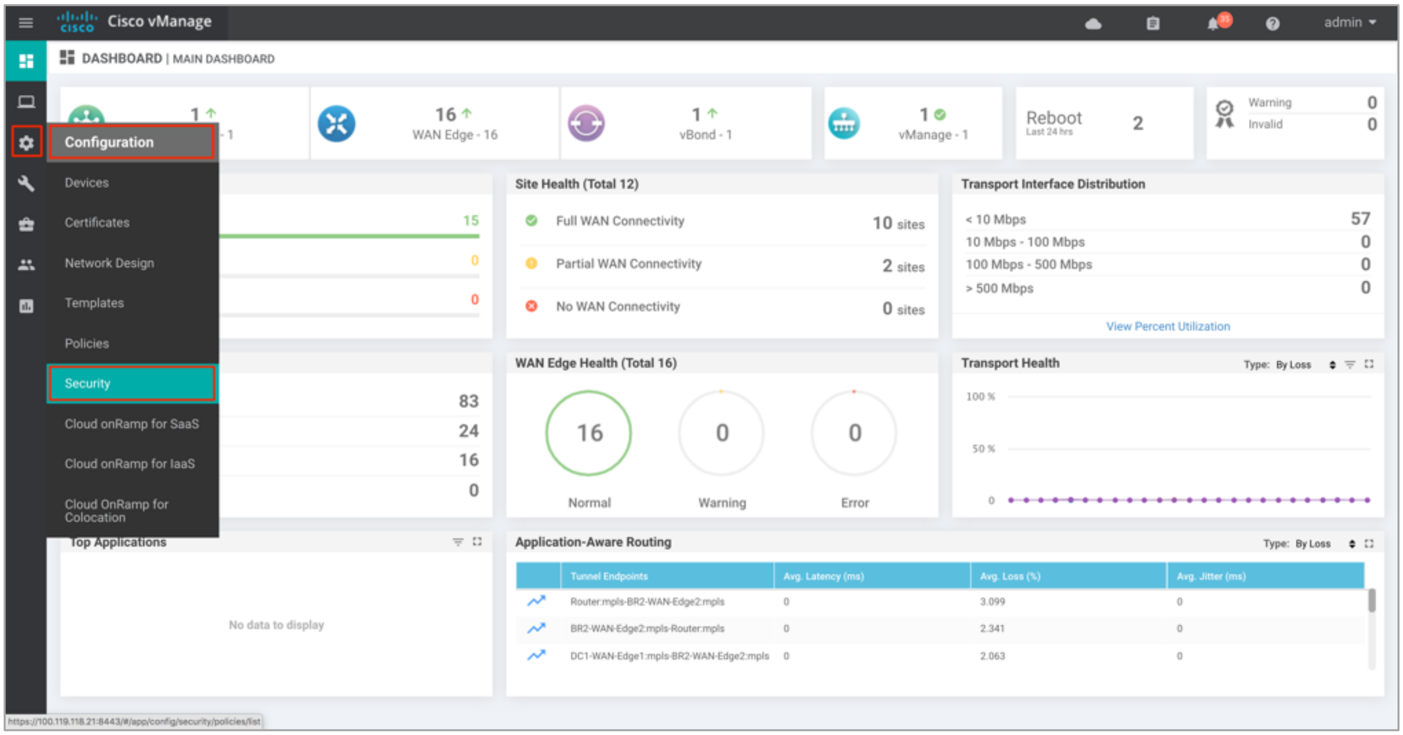
NAT ● On ○ Off

Resource Profile -- Choose -- / default / high

Process 5: Define Lists for Security Policy (Optional)

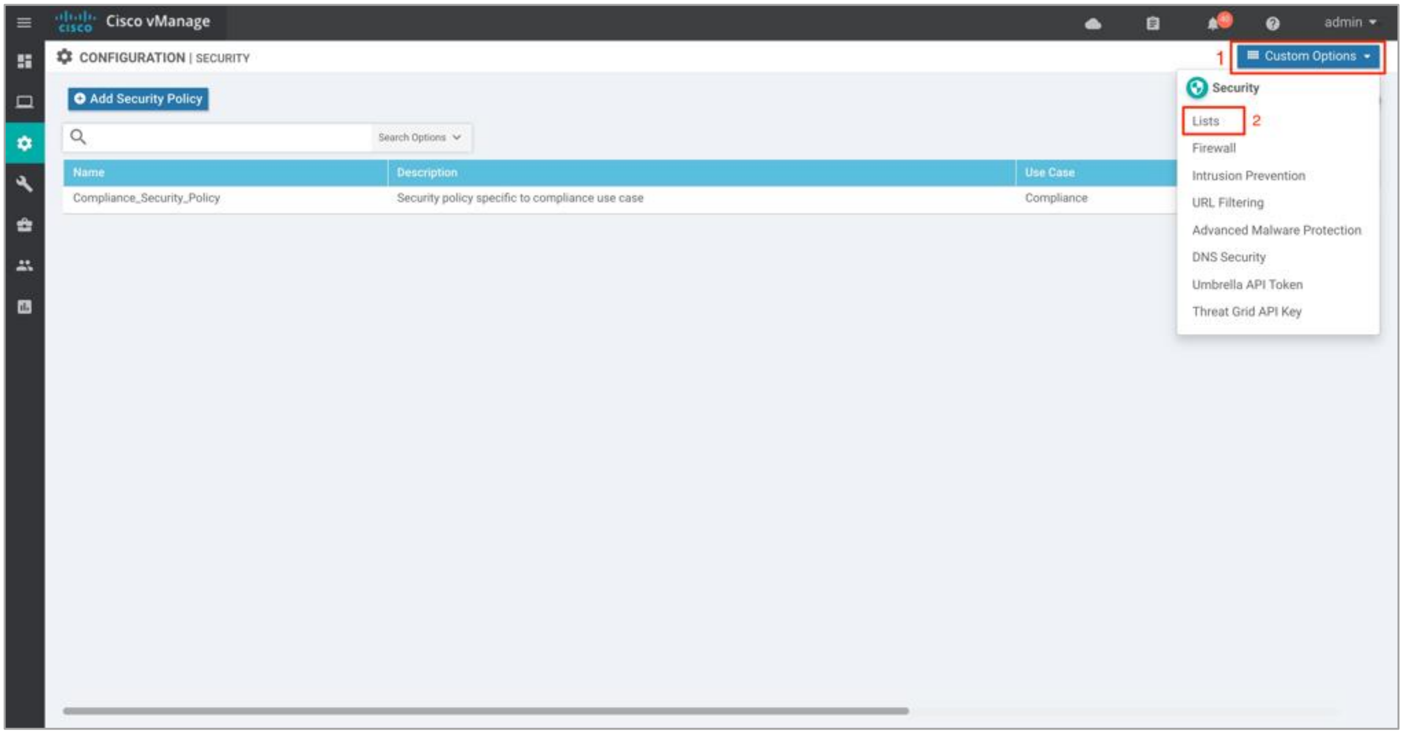
You can choose to either configure firewall zones, data prefixes, domain and application families prior to building the security policy or at the time when the policy is built.

Step 1. Navigate to Configuration > Security.



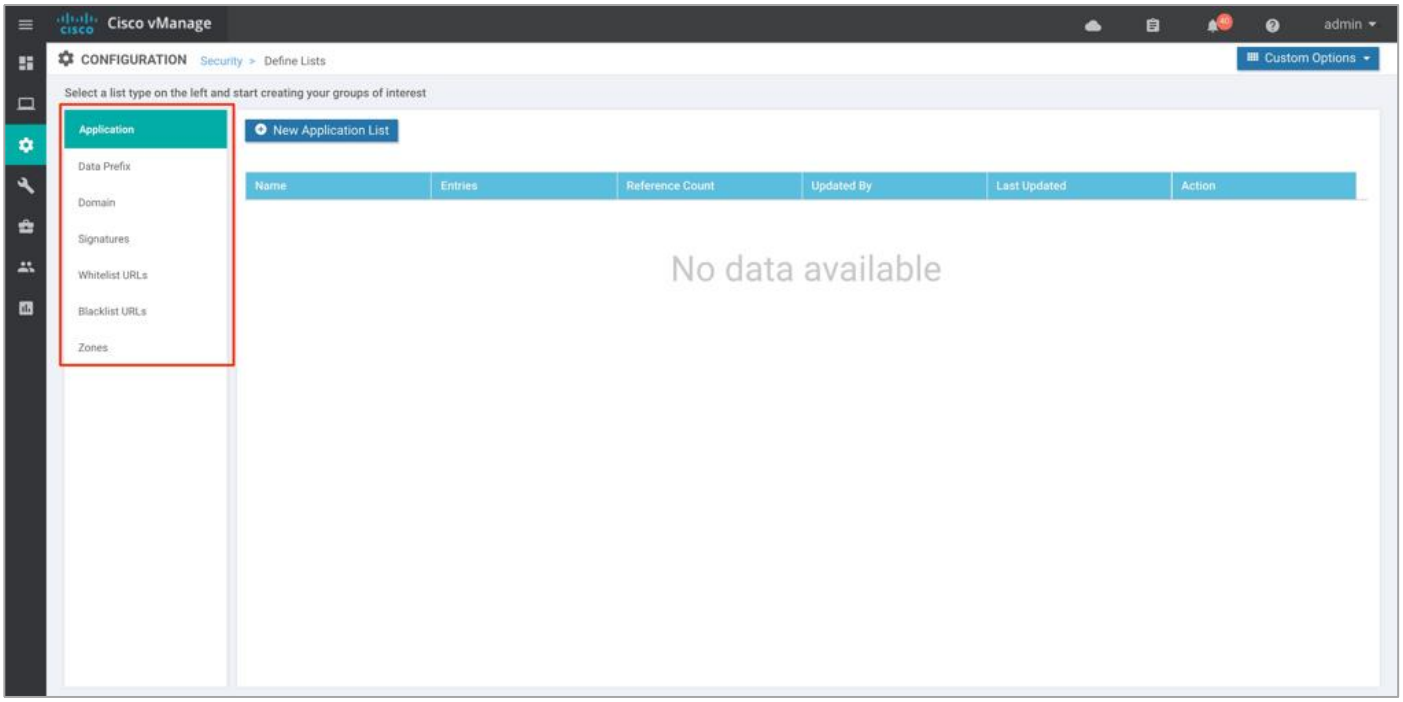
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	3.099	0
BR2-WAN-Edge2:mpls-Router:mpls	0	2.341	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	2.063	0

Step 2. Click **Custom Options.** A drop down of security options will appear. Click **Lists.**



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

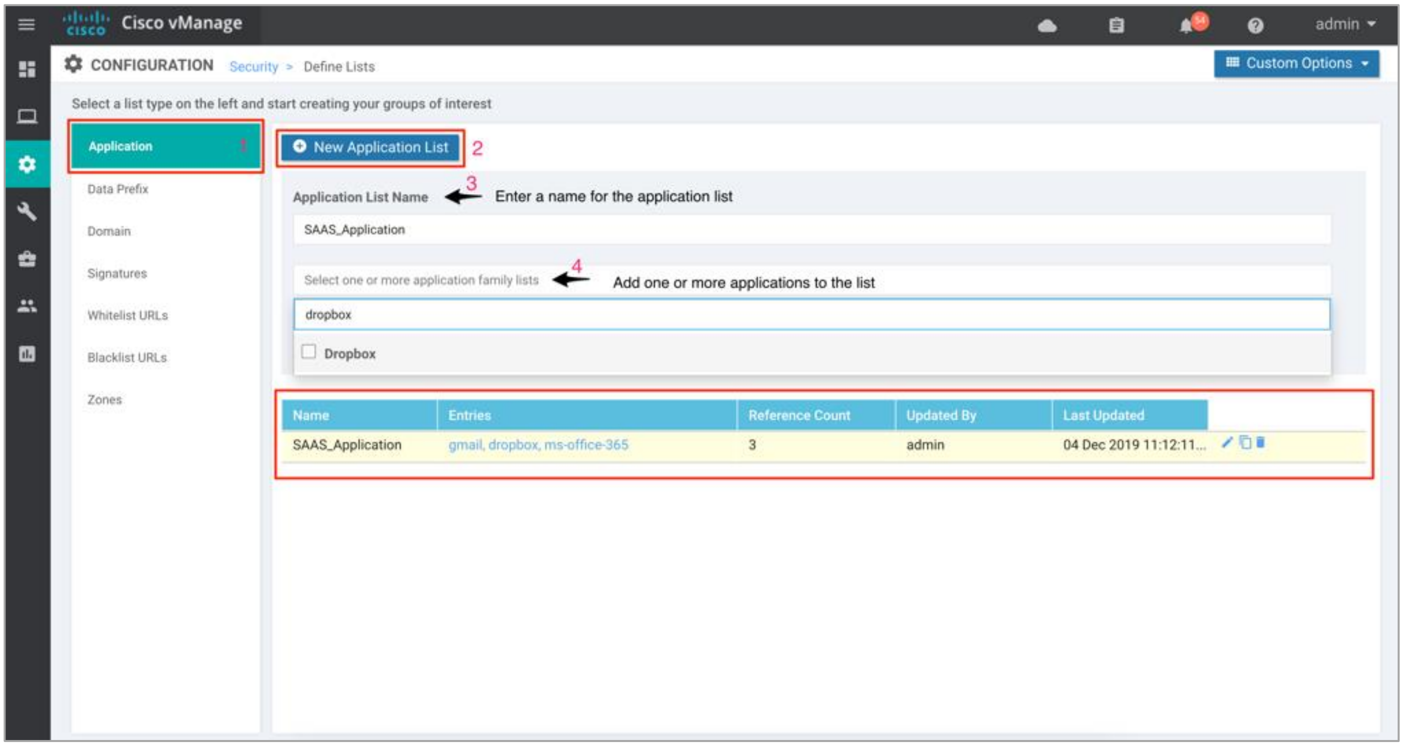
Step 3. Here, you can preconfigure lists such as Application **Lists**, **Data Prefixes**, **Signatures** and **Zones** which are later used as a part of the security policy.



Technical Tip
Applications matched within a firewall policy is always dropped, regardless of what the action condition states.

Procedure 1. Configure Lists for Enterprise Firewall with Application Awareness (Optional)

Step 1. To configure a data prefix list, select **Data Prefix** and then click on **New Data Prefix List**.



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

1 Application

2 New Application List

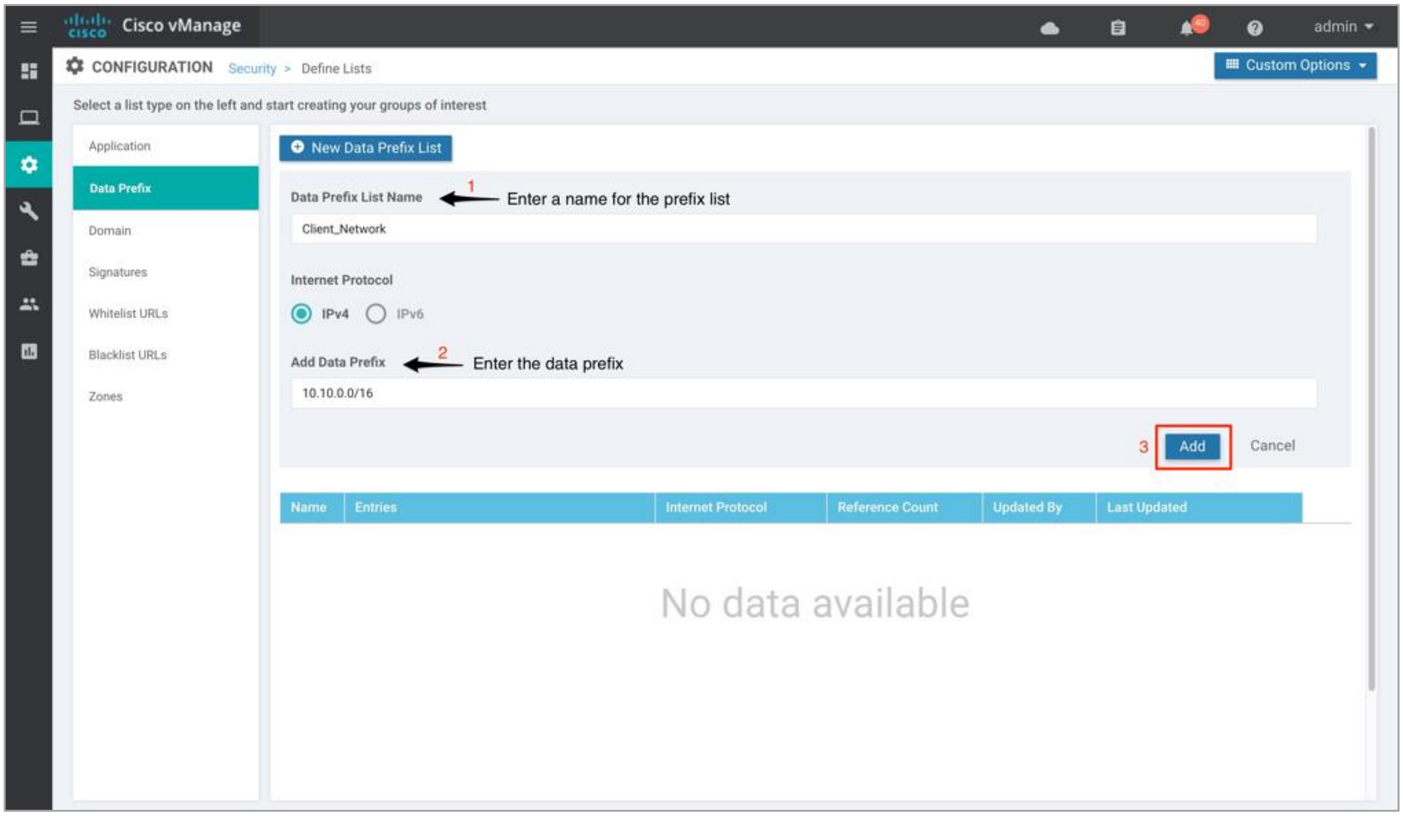
3 Application List Name: SAAS_Application — Enter a name for the application list

4 Select one or more application family lists: dropbox — Add one or more applications to the list

□ Dropbox

Name	Entries	Reference Count	Updated By	Last Updated
SAAS_Application	gmail, dropbox, ms-office-365	3	admin	04 Dec 2019 11:12:11...

Step 2. Enter a name under **Data Prefix List Name**, along with the data prefix under **Add Data Prefix.** Enter prefix details and click **Add.**



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

1 Data Prefix List Name: Client_Network — Enter a name for the prefix list

Internet Protocol: ● IPv4 ○ IPv6

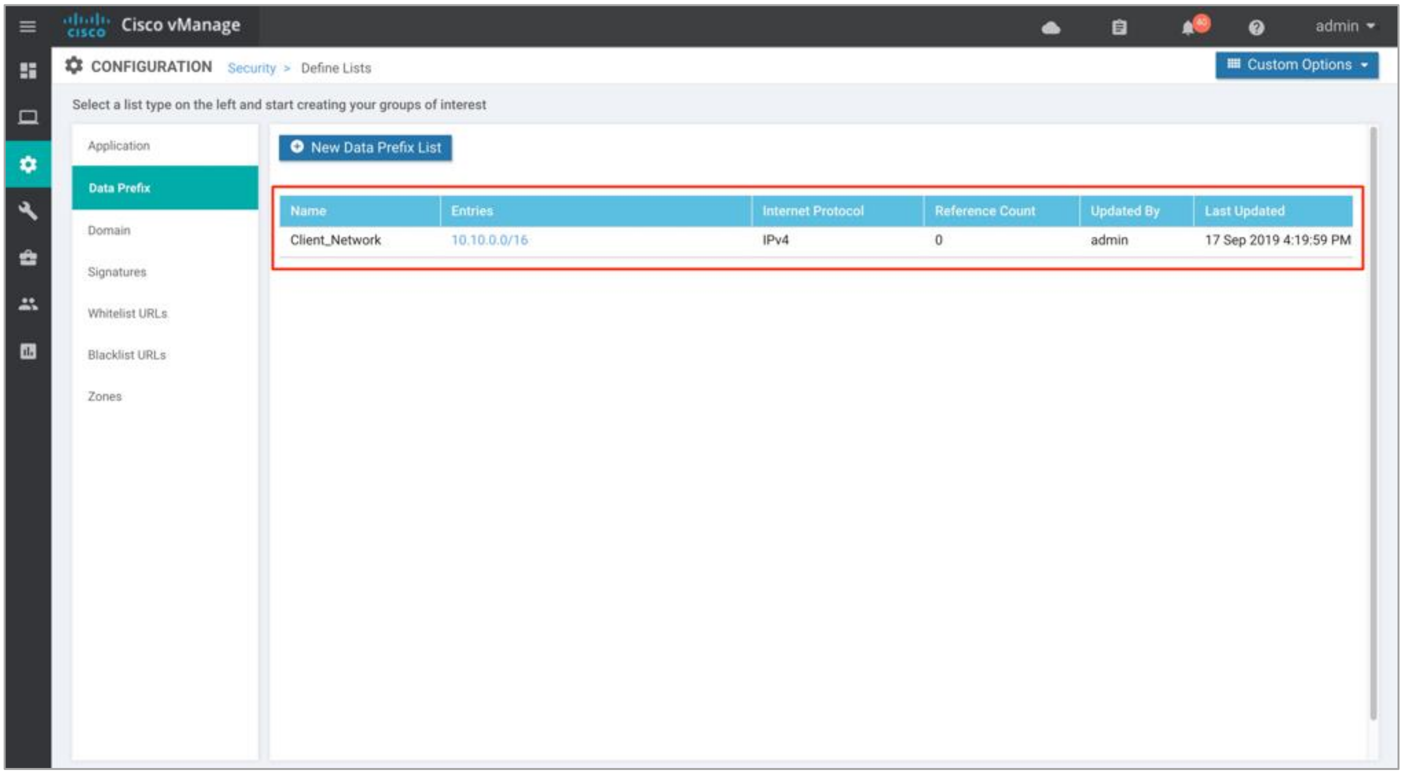
2 Add Data Prefix: 10.10.0.0/16 — Enter the data prefix

3 Add

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated

No data available

The lists configured under Data Prefix include,



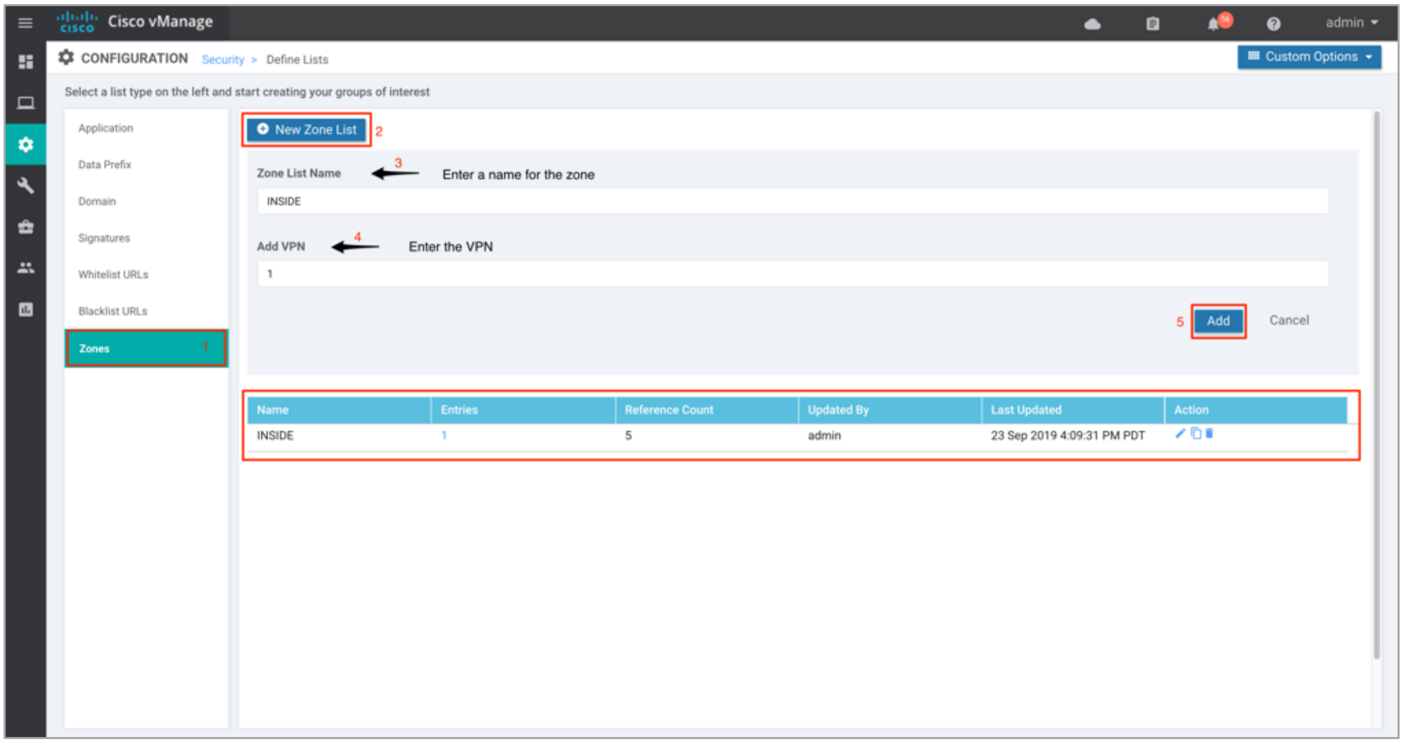
Select a list type on the left and start creating your groups of interest

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

Table 2. Data Prefix list

Data Prefix	Associated Prefix
Client_Network	10.10.0.0/16

Step 3. Similarly, configure a zone. Select **Zones** and then click on **New Zone List.** Enter a name within **Zone List** Name and add VPN’s 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	

The list of zones configured for Direct Cloud Access (DCA) use case.

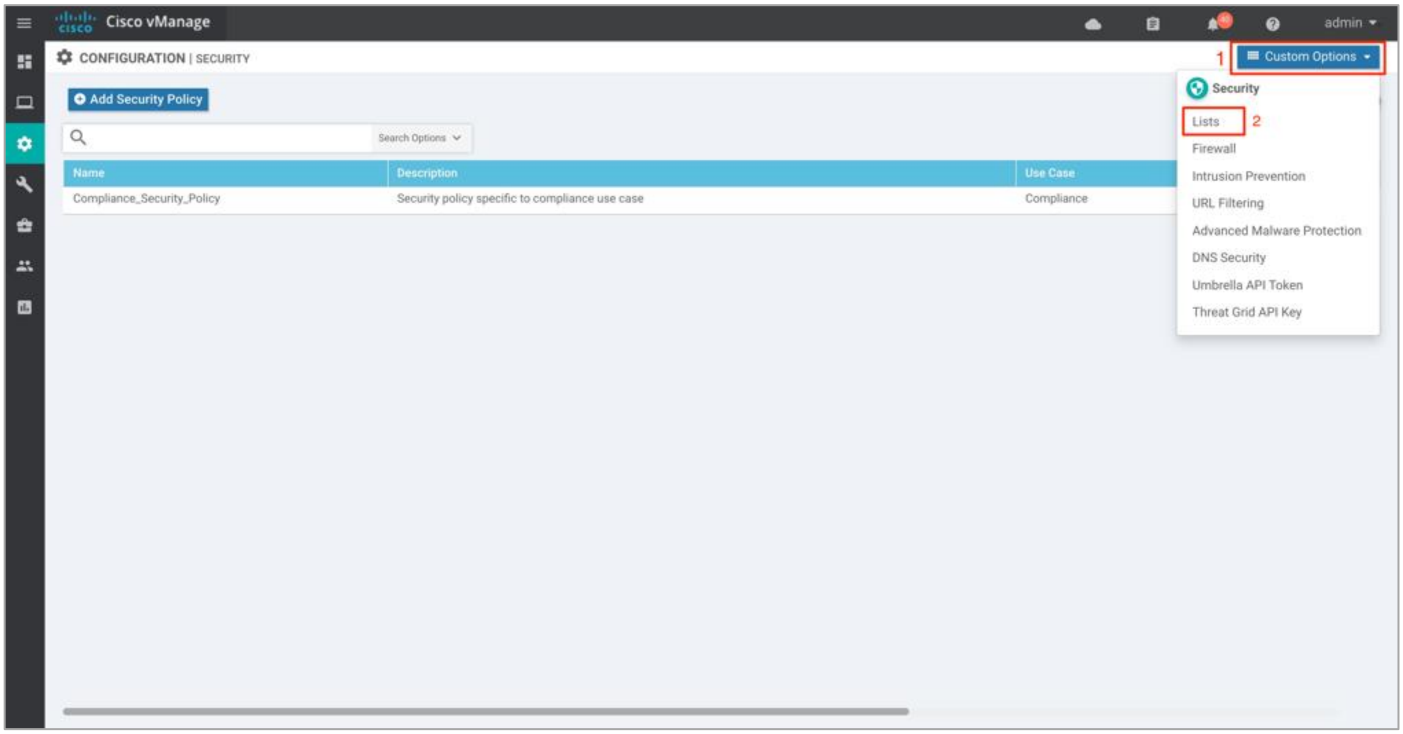
Table 3. Data Prefix list

Zone	Associated VPN
INSIDE	1
OUTSIDE	0

Procedure 2. Define Domain Lists. (Optional)

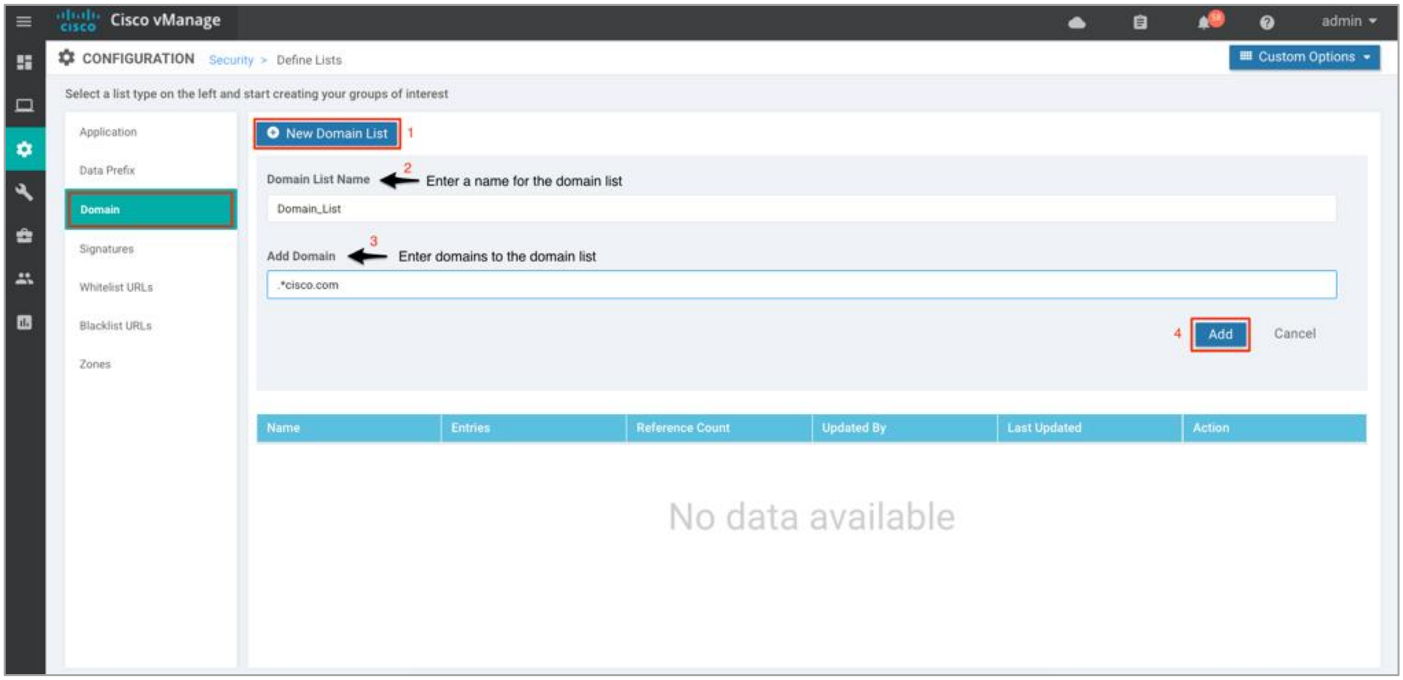
Define domain lists through the vManage security configuration wizard that must be bypassed by the DNS server configured within DNS Security.

Step 1. In the security screen, click on the **Custom Options** drop-down and click on **Lists.**



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

Step 2. Select **Domain** from the left pane, enter a domain name and add domain names to the list. Finally, **Add** the list of domain names.



Domain List Name ← Enter a name for the domain list

Domain_List

Add Domain ← Enter domains to the domain list

.*cisco.com

Name	Entries	Reference Count	Updated By	Last Updated	Action

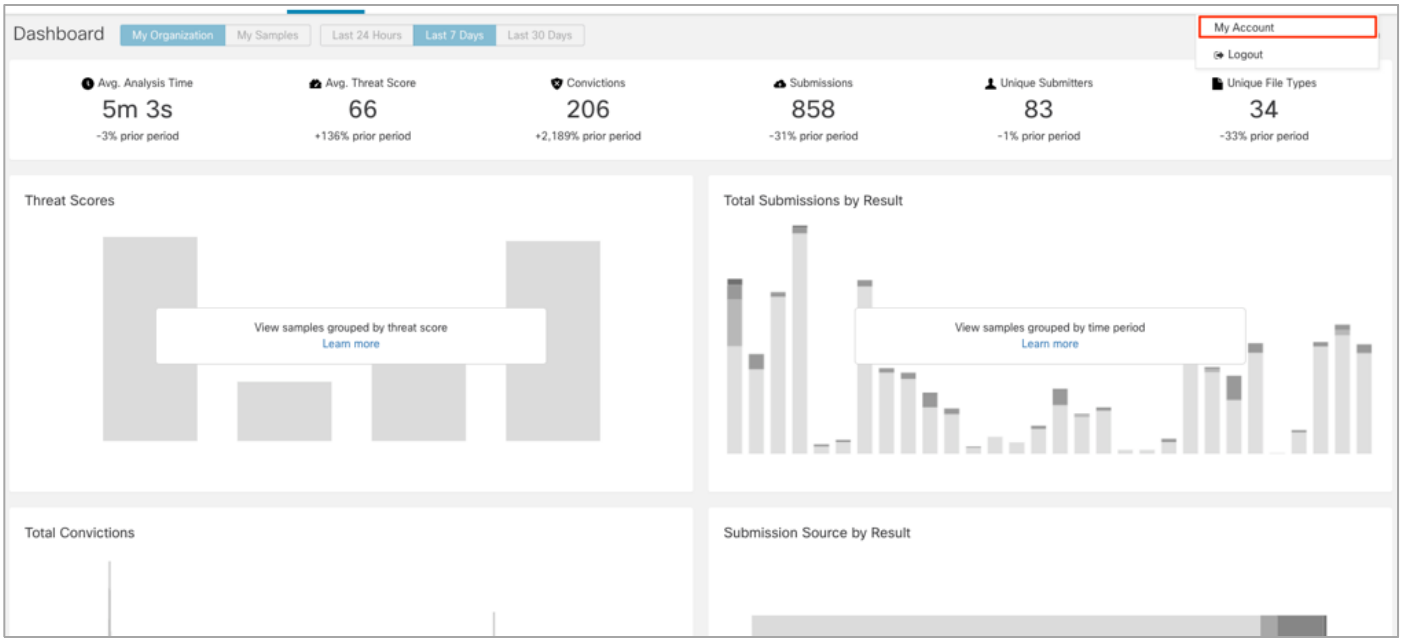
No data available

Note, no domain lists were configured in this deployment.

Process 6: Configure Threat Grid API Key

Once you have an active Threat Grid (TG) account with access/role set as device-admin, configure the Threat Grid (TG) API key on WAN Edge device.

Step 1. Log into the Cisco AMP Threat Grid dashboard and click on **My Account**.



Avg. Analysis Time 5m 3s -3% prior period

Avg. Threat Score 66 +136% prior period

Convictions 206 +2,189% prior period

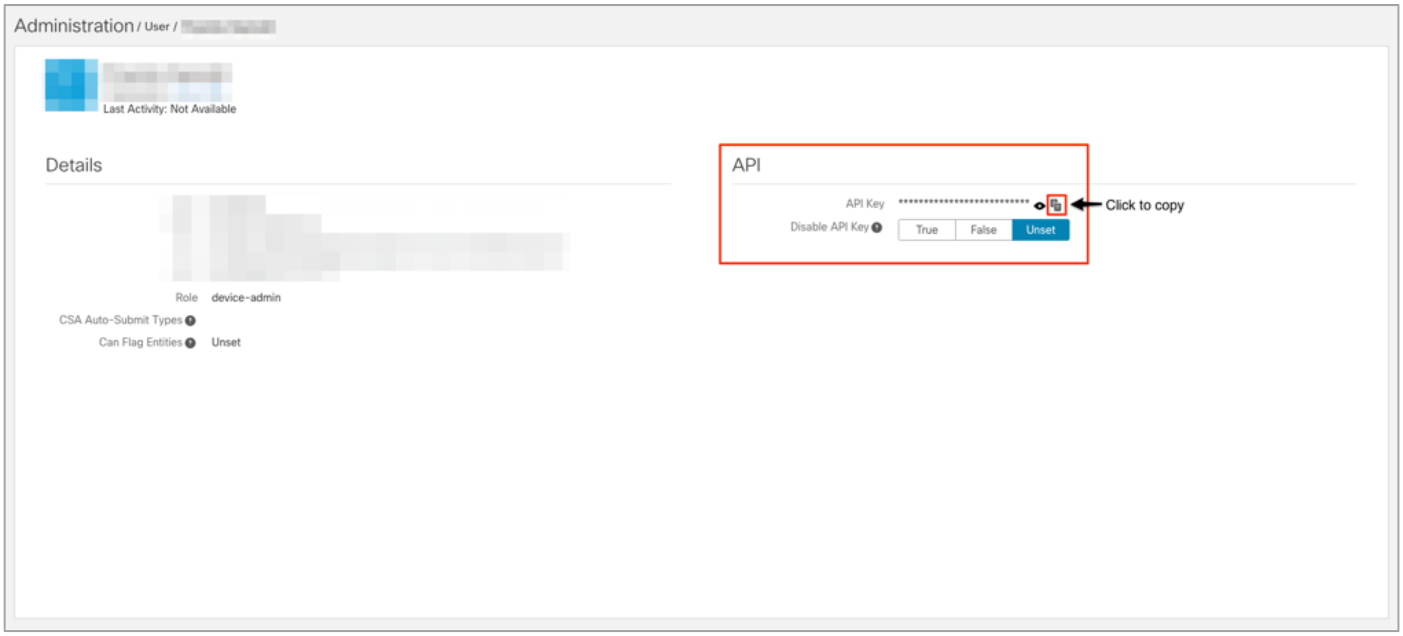
Submissions 858 -31% prior period

Unique Submitters 83 -1% prior period

Unique File Types 34 -33% prior period

Threat Scores
View samples grouped by threat score
Learn more
Total Submissions by Result
View samples grouped by time period
Learn more
Total Convictions
Submission Source by Result

Step 2. Under your **Account Details**, an API key may already be visible if you've created one already. Click on the **copy icon** to copy the API Key.


Administration / User / [redacted]
Last Activity: Not Available
Details
API
Click to copy

[redacted]

Role device-admin

CSA Auto-Submit Types

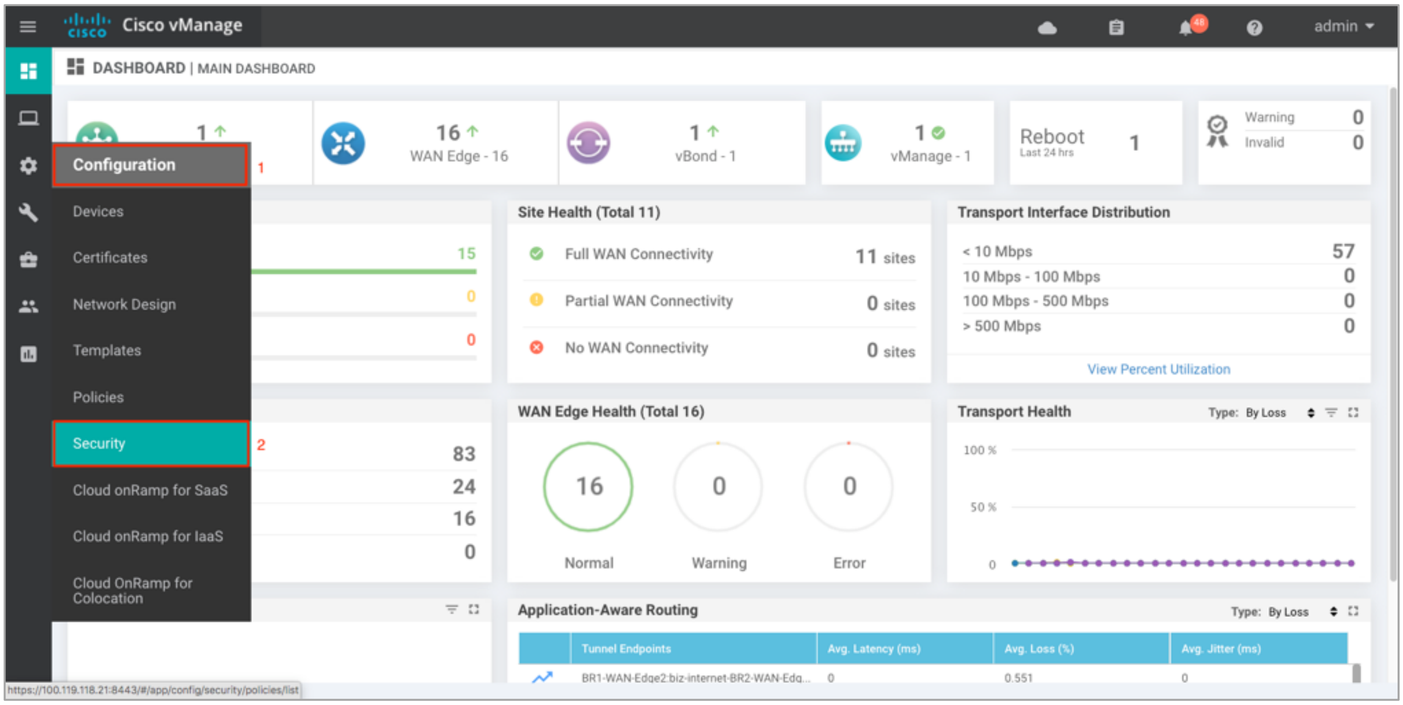
Can Flag Entities Unset

API Key ***************************

Disable API Key True False [✓ Unset]

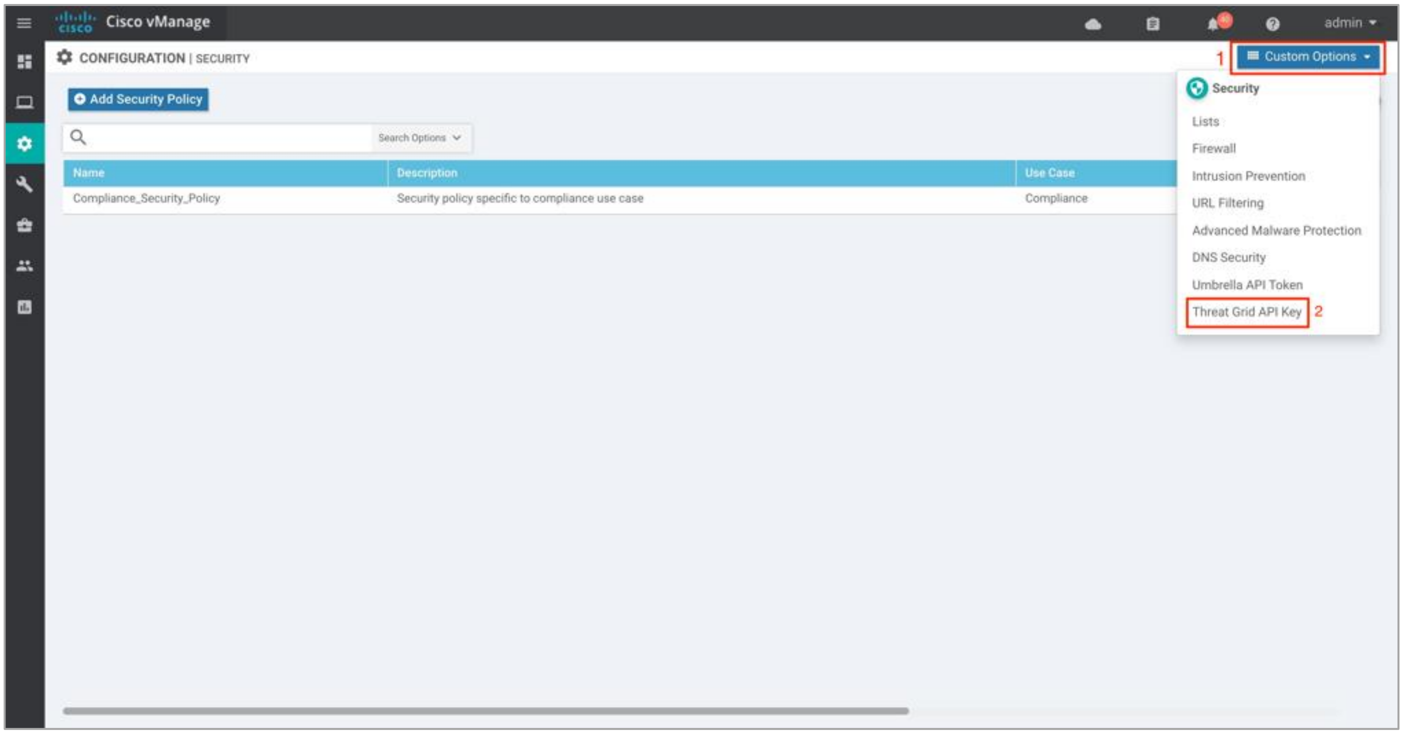
If you do not have an API key available, click **Generate New API Key**. Your API key should then be visible under **User Details** > **API Key**.

Step 3. Log into Cisco vManage and navigate to **Configuration** > **Security** in the left side panel.



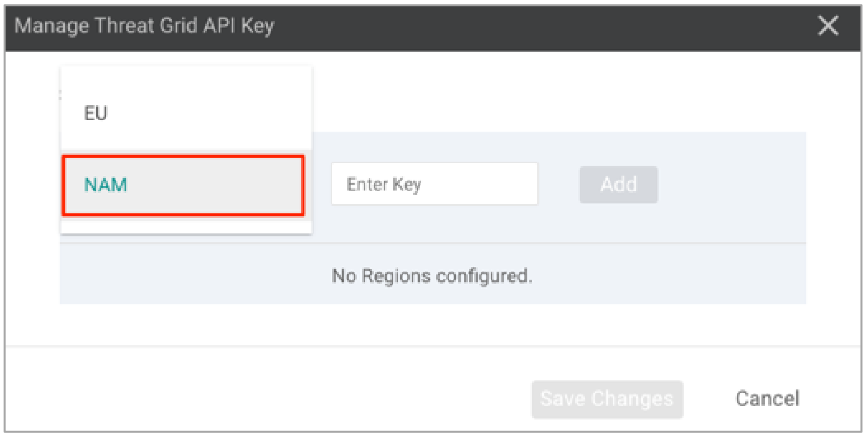
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BR1-WAN-Edge2:biz-internet-BR2-WAN-Edg...	0	0.551	0

Step 4. In the security screen, click on the **Custom Options** drop-down and select **Threat Grid API Key**.

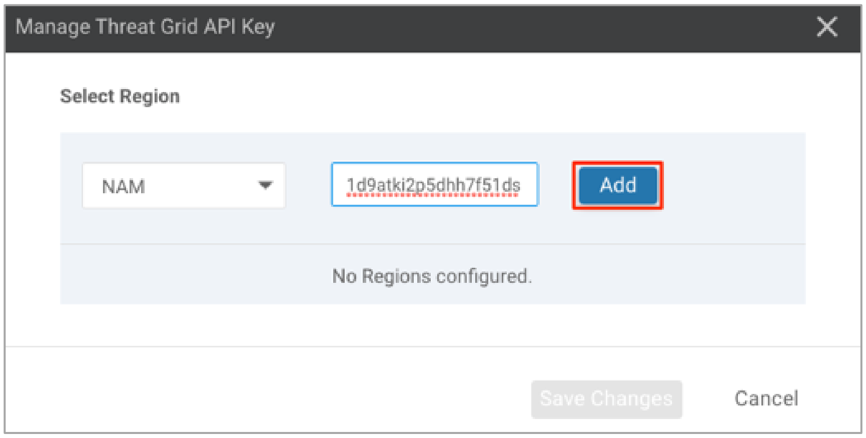


Name	Description	Use Case
Compliance_Security_Policy	Security policy specific to compliance use case	Compliance

Step 5. In the **Manage Threat Grid API key** pop-up box, choose a region from the **Region** drop-down and enter the API key in the **Key** field.

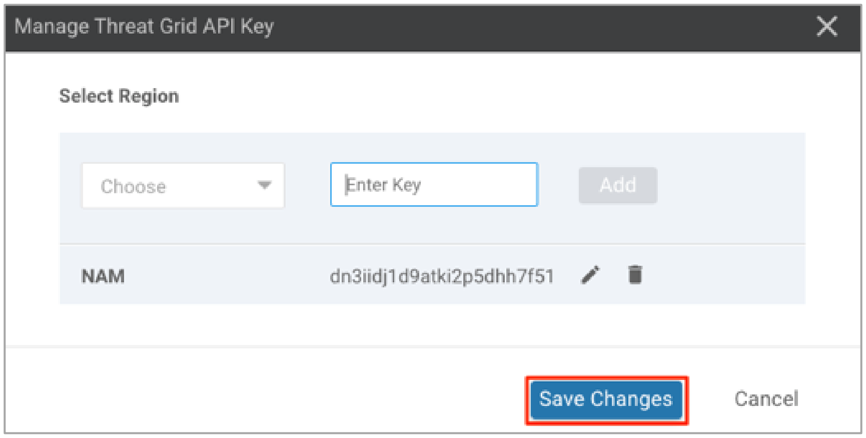


Step 6. Click Add and Save Changes.



Select Region: NAM

1d9atki2p5dhh7f51ds

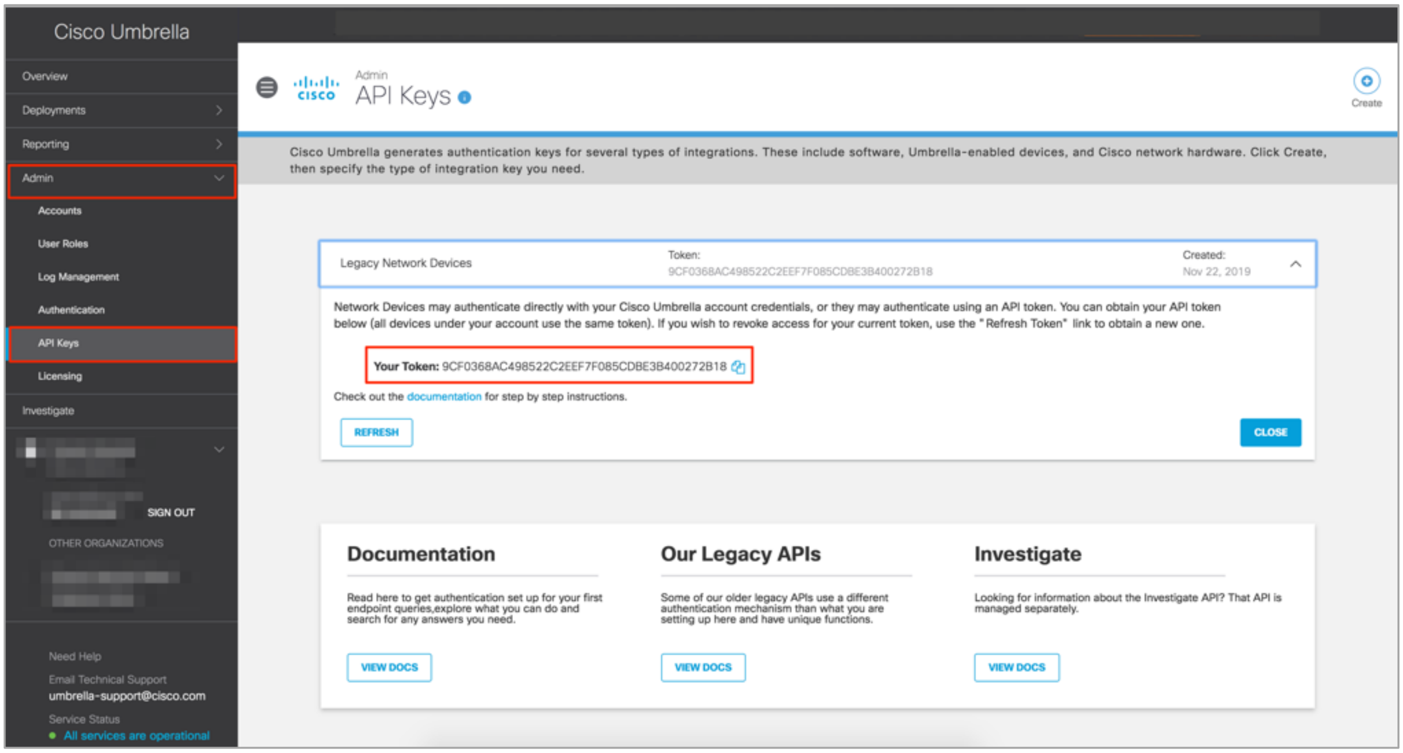


NAM	dn3iidj1d9atki2p5dhh7f51

Process 7: Configure Umbrella API Token

Make sure you have an active Umbrella account with reachability from the WAN Edge device to the Cisco Umbrella DNS servers. Configure the Umbrella API token from the Umbrella portal using the vManage security policy wizard.

Step 1. Log in to the Umbrella account, navigate to **Admin** and click on API Keys. Within Admin API Keys dashboard, Copy **Your Token.**



[redacted]

Need Help

Email Technical Support
umbrella-support@cisco.com

Service Status
● All services are operational

Cisco Umbrella generates authentication keys for several types of integrations. These include software, Umbrella-enabled devices, and Cisco network hardware. Click Create, then specify the type of integration key you need.

Legacy Network Devices	Token:	Created:
	9CF0368AC498522C2EEF7F085CDBE3B400272B18	Nov 22, 2019

Network Devices may authenticate directly with your Cisco Umbrella account credentials, or they may authenticate using an API token. You can obtain your API token below (all devices under your account use the same token). If you wish to revoke access for your current token, use the " Refresh Token" link to obtain a new one.

Your Token: 9CF0368AC498522C2EEF7F085CDBE3B400272B18

Check out the documentation for step by step instructions.

Documentation

Read here to get authentication set up for your first endpoint queries,explore what you can do and search for any answers you need.

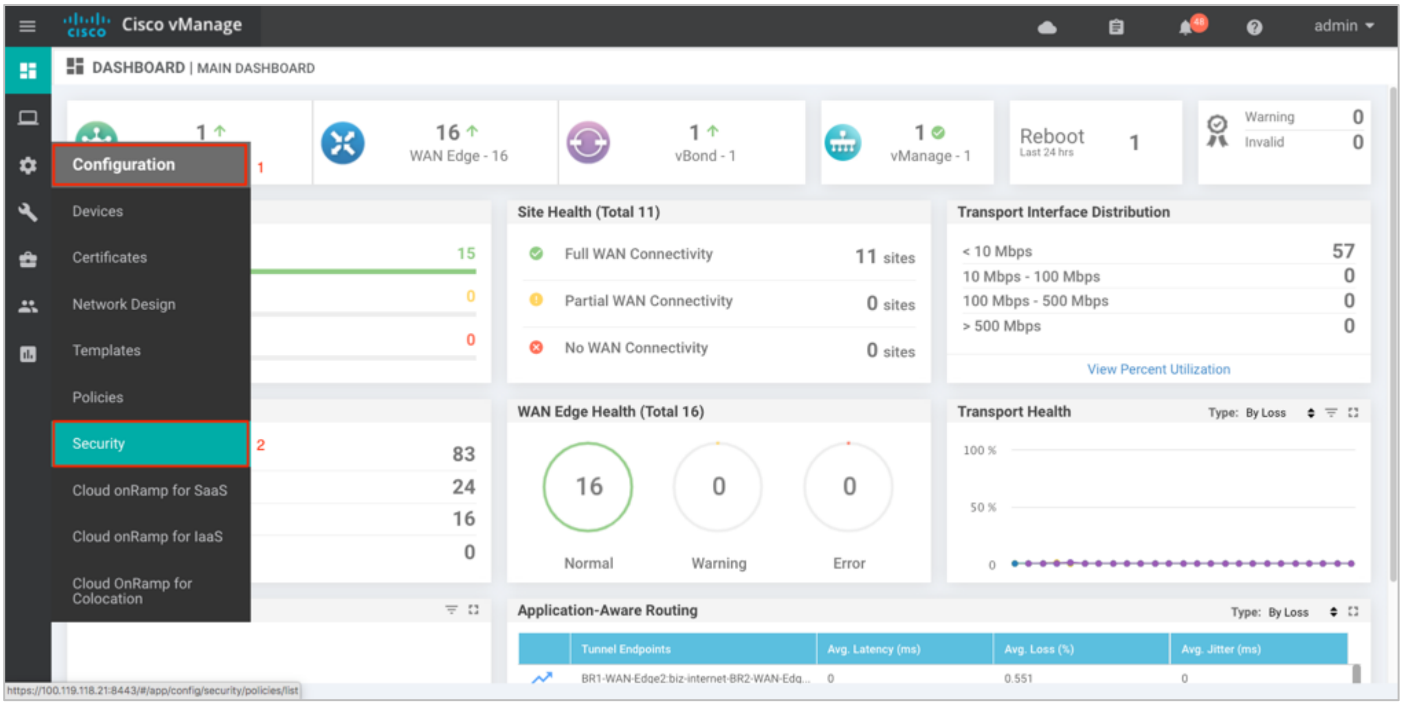
Our Legacy APIs

Some of our older legacy APIs use a different authentication mechanism than what you are setting up here and have unique functions.

Investigate

Looking for information about the Investigate API? That API is managed separately.

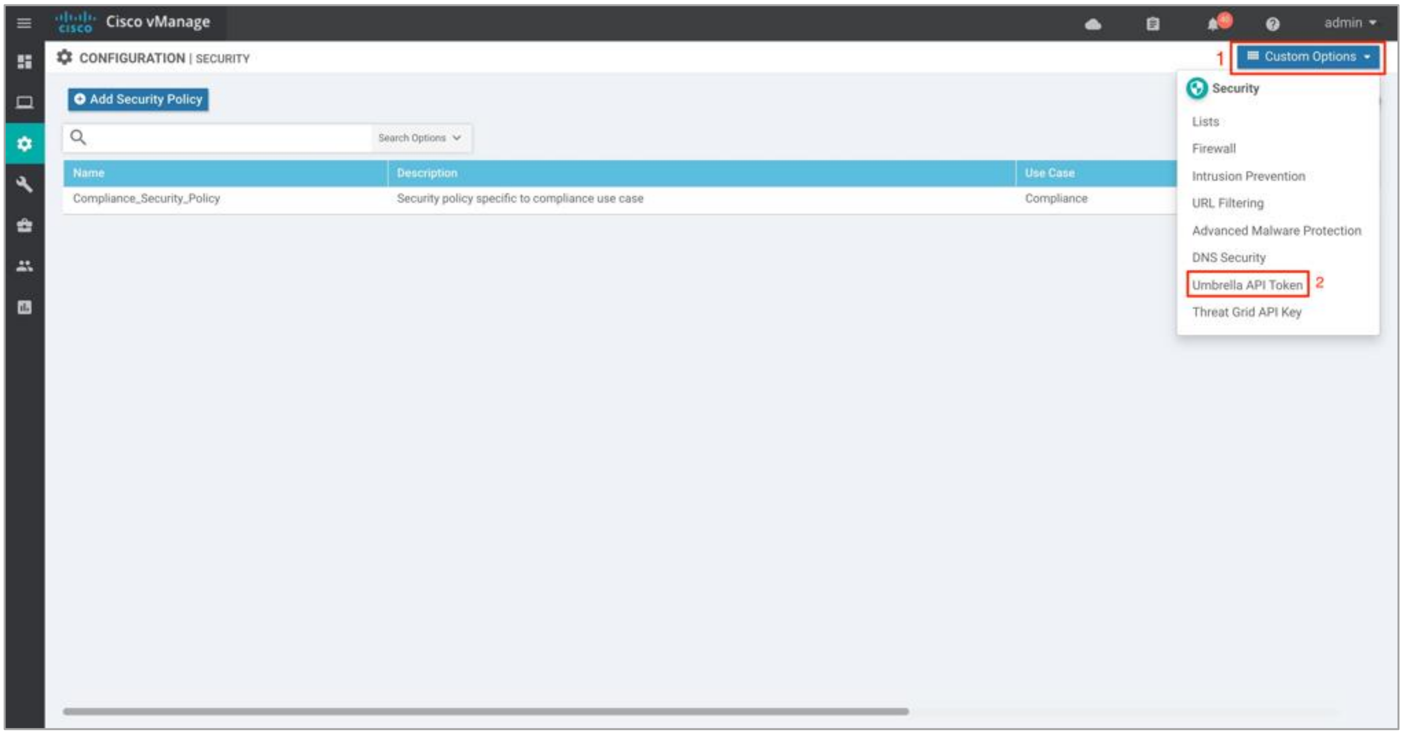
Step 2. Next, log in to Cisco vManage and navigate to **Configuration** > **Security** in the left side panel.



Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BR1-WAN-Edge2:biz-internet-BR2-WAN-Edg...	0	0.551	0

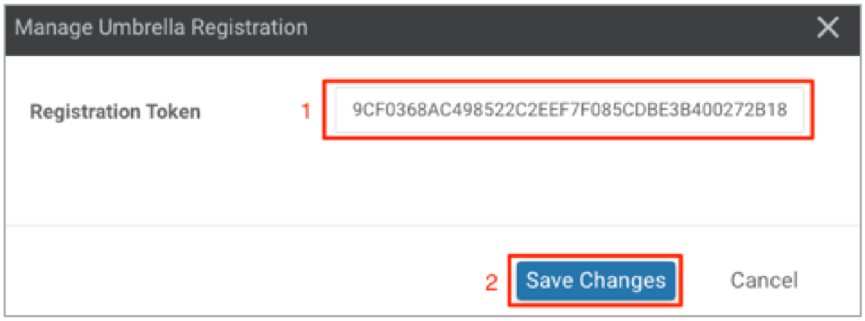
https://100.119.118.21:8443/#/app/config/security/policies/list

Step 3. In the security screen, click on the **Custom Options** drop-down list and select **Umbrella API Token**.



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

Step 4. Enter **Registration Token number** in the field and click **Save Changes** to configure the Umbrella API Token.

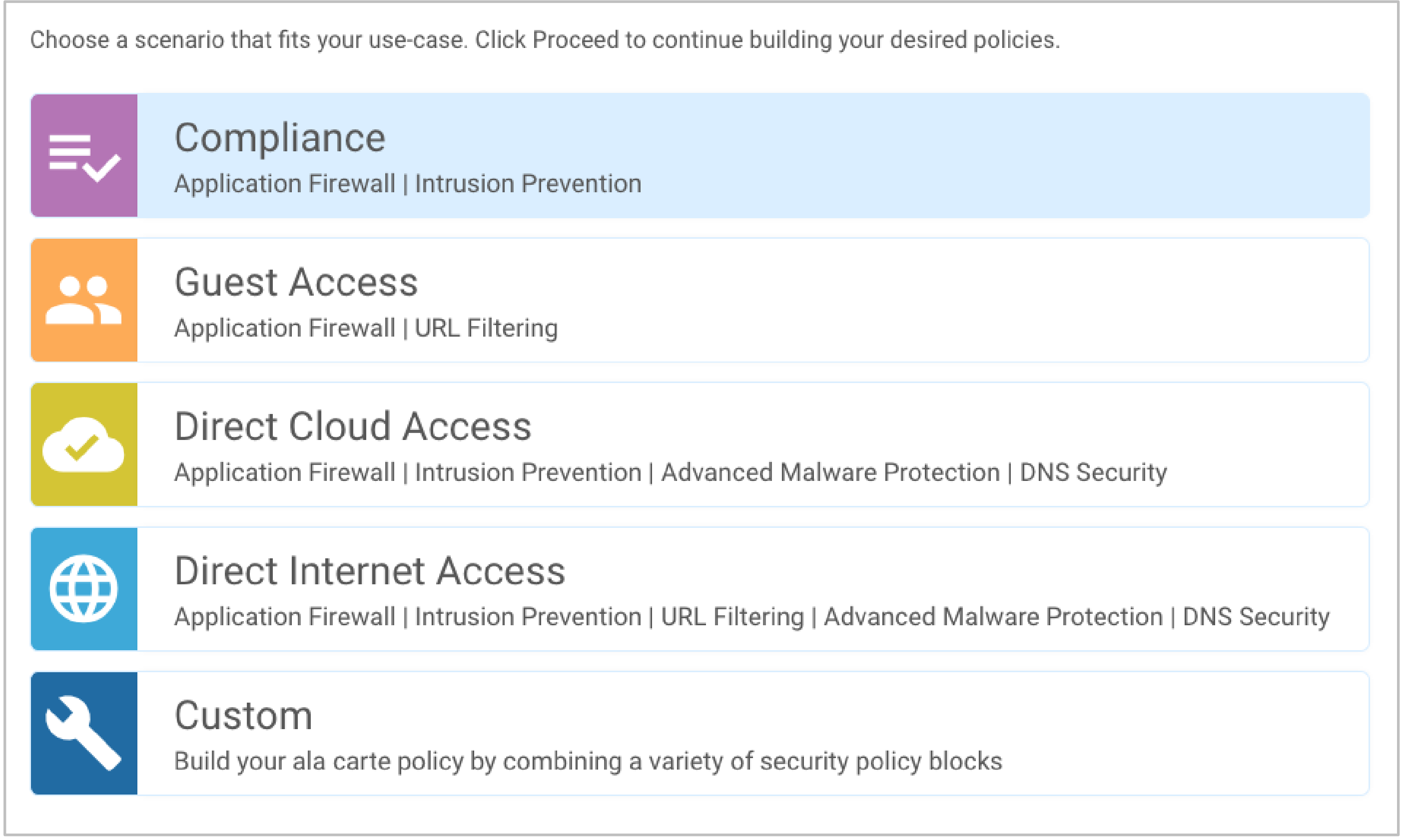


Registration Token: 9CF0368AC498522C2EEF7F085CDBE3B400272B18

Deploy: Cisco SD-WAN Secure Direct Cloud Access

This section covers the steps to deploy Cisco SD-WAN security features specific to the Direct Cloud Access (DCA) use case. The features discussed include Enterprise Firewall with Application Awareness (Application Firewall), Intrusion Prevention (IPS), Advanced Malware Protection (AMP) and DNS/ Web-Layer Security.

Figure 4. Intent-Based Use Cases



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

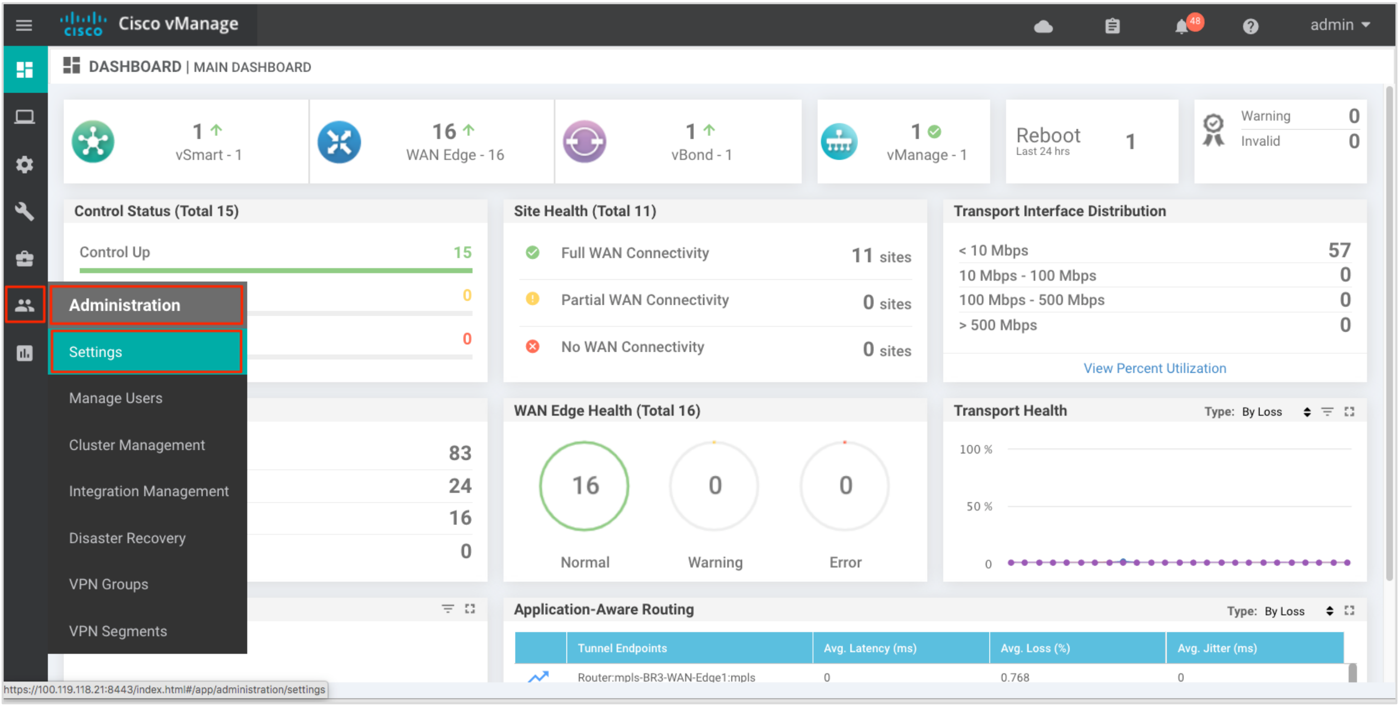
Custom
Build your ala carte policy by combining a variety of security policy blocks

Configuration Workflow

- Make sure the prerequisites explained previously are added.
- Enable the IPS signature automatic updates using vManage.
- Create the security policy containing Enterprise Firewall with App Aware (Application Firewall), Intrusion Prevention (IPS), Advanced Malware Protection (AMP) and DNS/ Web-layer Security feature.
- Attach the security policy to the Device Template.
- Attach the Security App Hosting (Container Profile) 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 left side panel.



1 vSmart - 1 | 16 WAN Edge - 16 | 1 vBond - 1 | 1 vManage - 1 | Reboot Last 24 hrs 1 | Warning 0 Invalid 0

Control Status (Total 15)
Control Up 15

Site Health (Total 11)
Full WAN Connectivity 11 sites
Partial WAN Connectivity 0 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

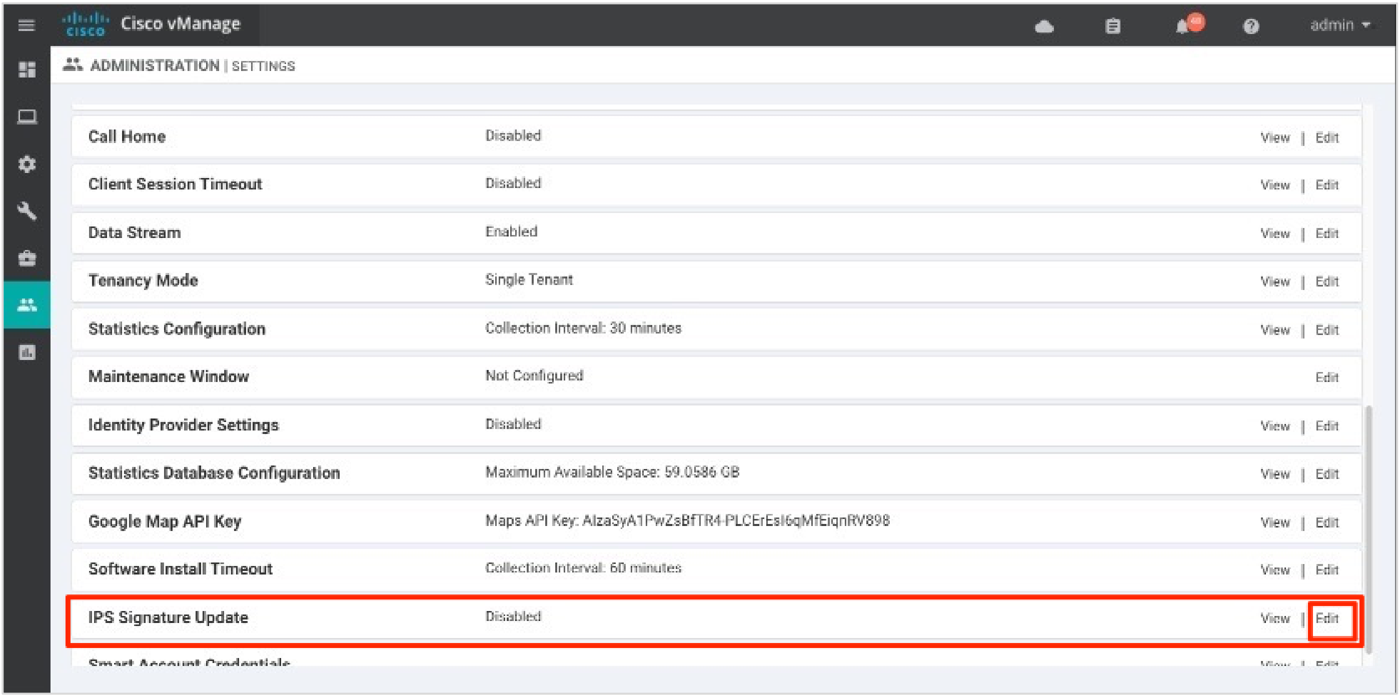
WAN Edge Health (Total 16)
16 Normal, 0 Warning, 0 Error

Transport Health

Application-Aware Routing

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR3-WAN-Edge1:mpls	0	0.768	0

Step 2. Click Edit to enable IPS Signature Update.

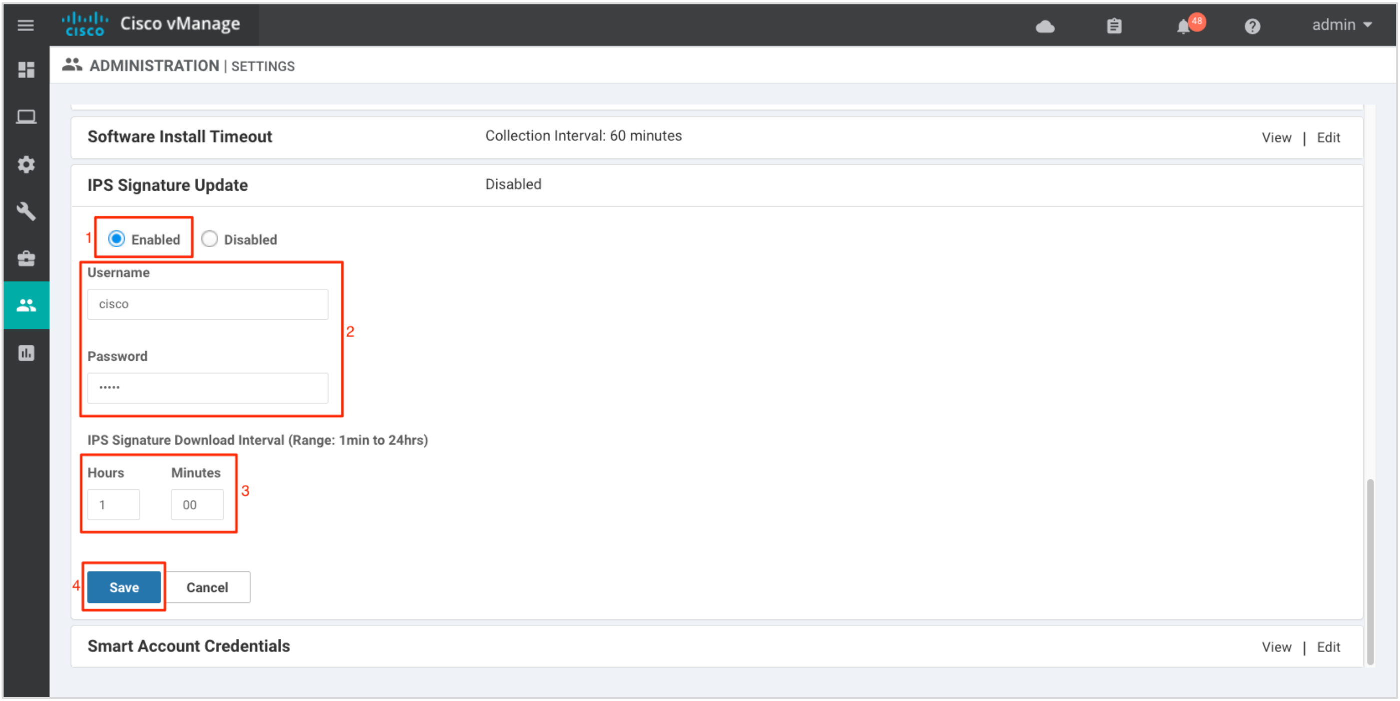


Call Home	Disabled	View | Edit
Client Session Timeout	Disabled	View | Edit
Data Stream	Enabled	View | Edit
Tenancy Mode	Single Tenant	View | Edit
Statistics Configuration	Collection Interval: 30 minutes	View | Edit
Maintenance Window	Not Configured	Edit
Identity Provider Settings	Disabled	View | Edit
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 your Cisco CEC u**sername** 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 have reachability to cloudsso2.cisco.com from vManage GUI – VPN 0 transport interface.

Note: To verify if the signatures are being updated, refer to the operate section for the troubleshooting steps.



Software Install Timeout — Collection Interval: 60 minutes — View | Edit

IPS Signature Update — Disabled

1 ● Enabled ○ Disabled

Username: cisco

Password: •••••

2

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

Hours: 1 Minutes: 00

3

4 Save Cancel

Smart Account Credentials — View | Edit

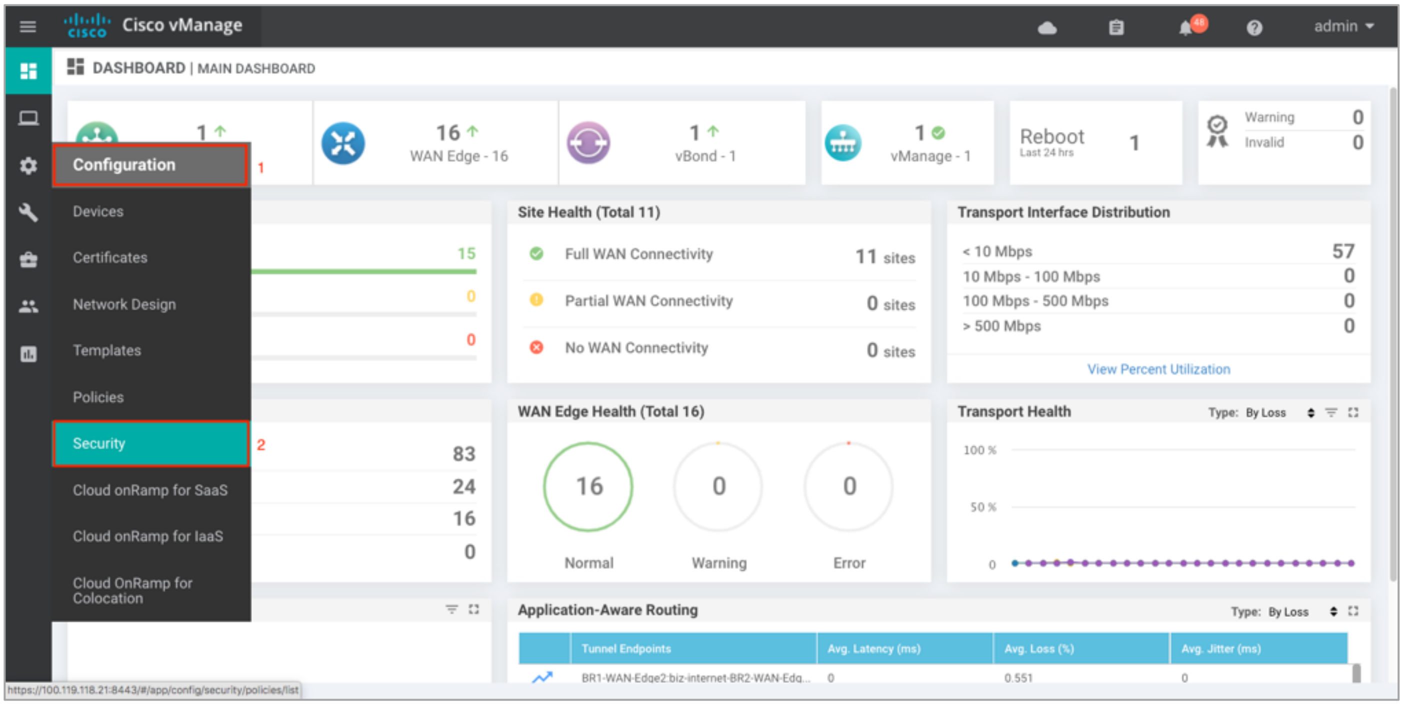
Technical Tip

To manually update the signature package via CLI on a WAN Edge device that has reachability to the Internet, you can either enter utd signature update server cisco username <username> password <password>. To manually update the signature package on a WAN Edge device with no internet access, download the signature package from CCO and upload the file to the WAN Edge device. Next, enter utd signature update file bootflash:<signature.pkg>.

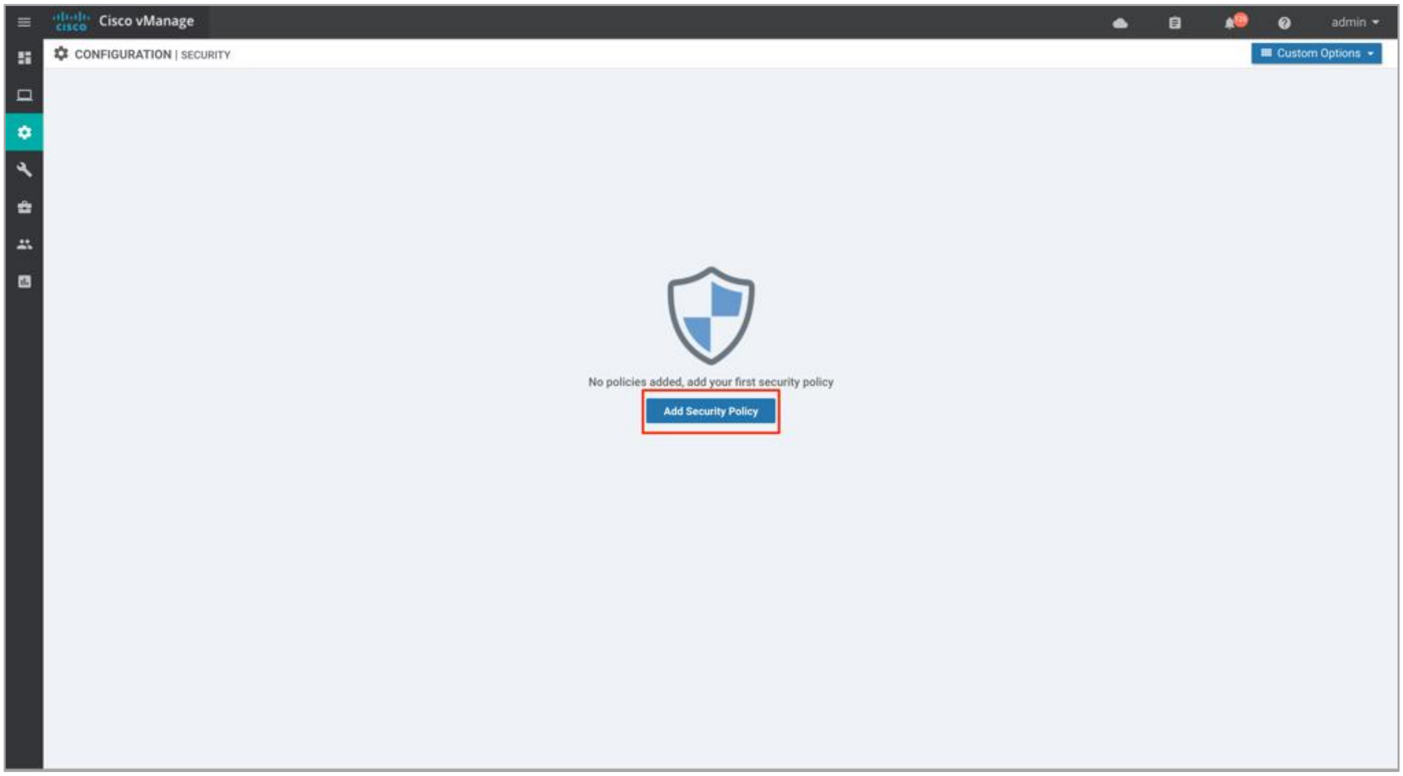
Process 2: Create Security Policy

Configure security parameters such as Enterprise Firewall with Application Awareness, Intrusion Prevention System (IPS), Advanced Malware Protection (AMP) and DNS/ Web-layer Security.

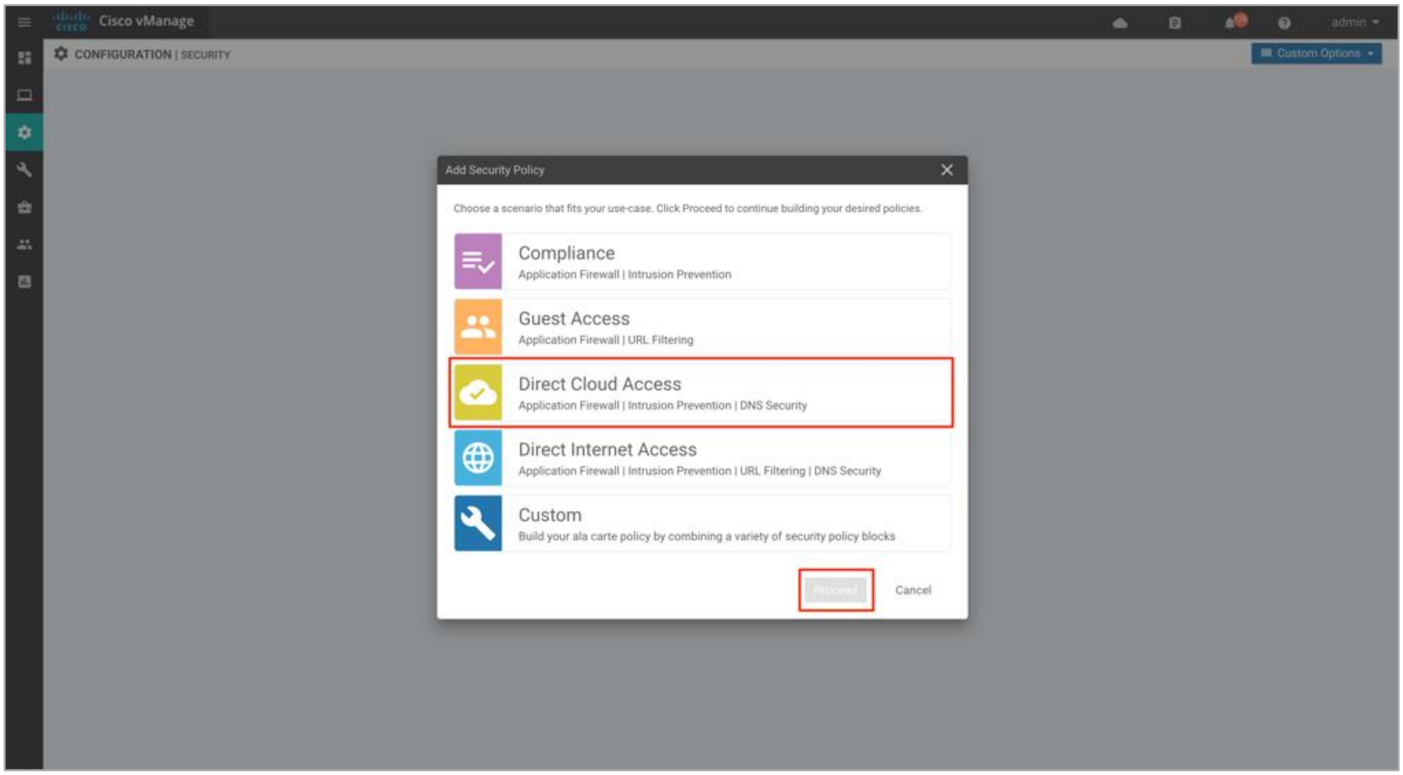
Step 1. In Cisco vManage NMS, navigate to **Configuration** > **Security** in the left side panel.



Step 2. Click **Add Security Policy** to create a new security policy.



Step 3. The security policy wizard displays a list of intent-based use cases. From the given list, choose **Direct Cloud Access** and click **Proceed**.



Add Security Policy

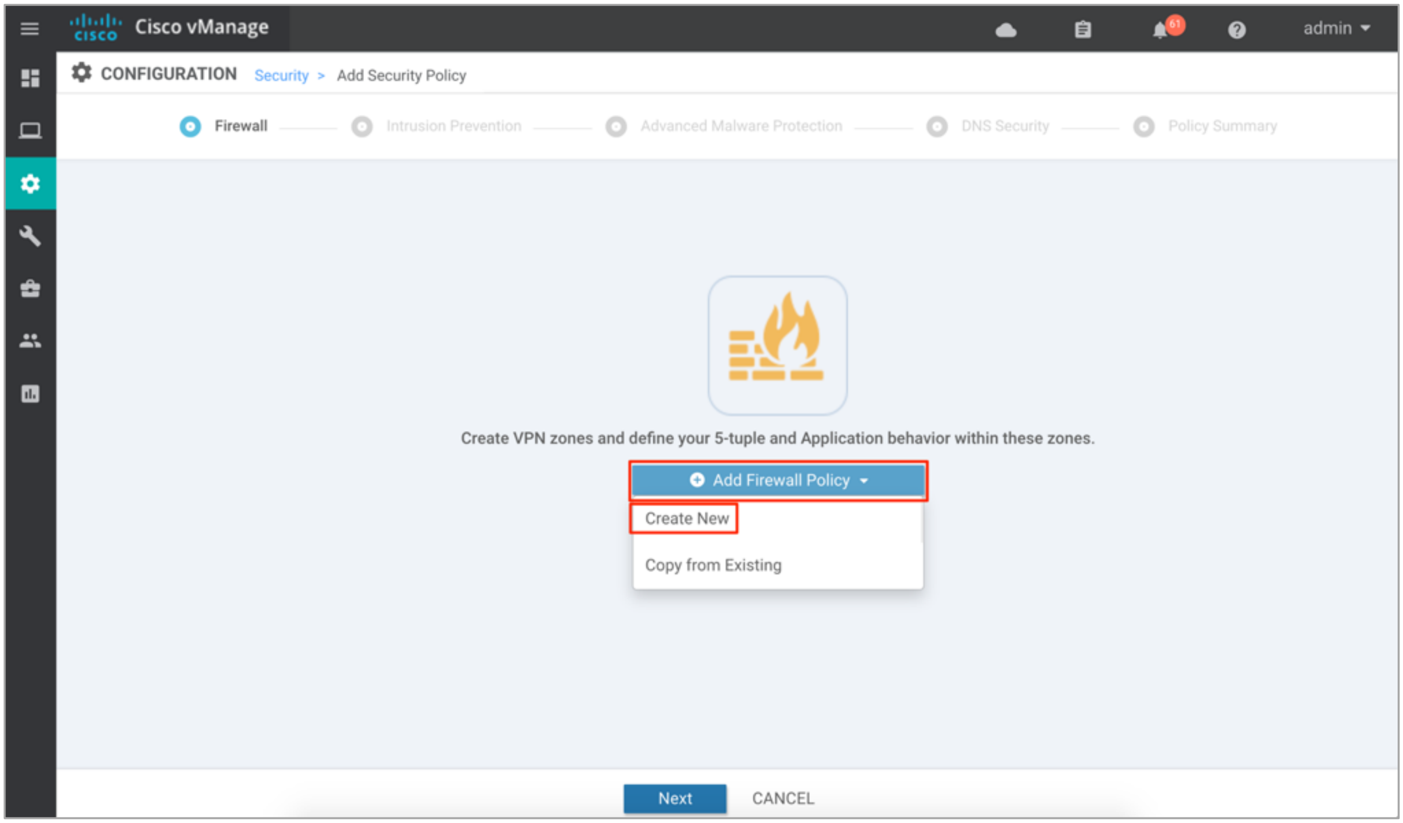
Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- 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

Proceed Cancel

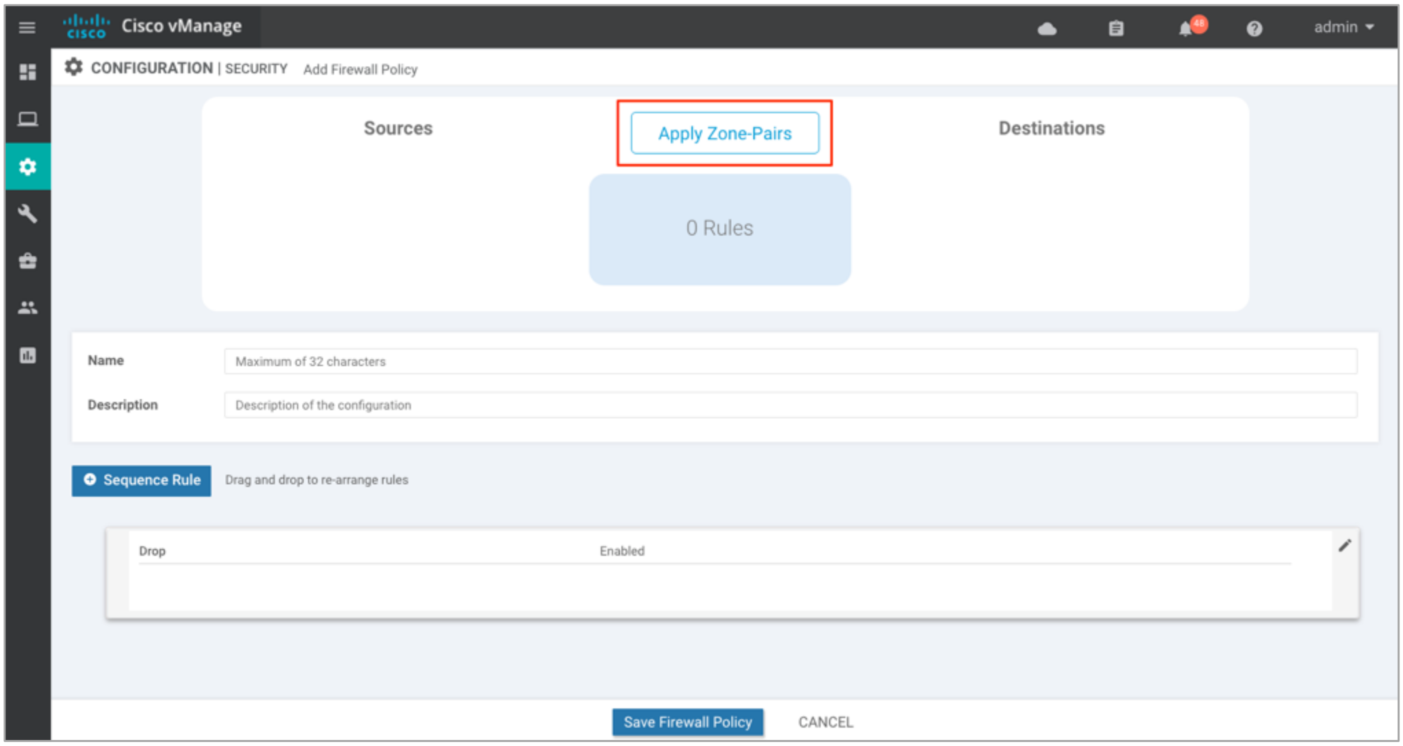
Procedure 1. Configure Enterprise Firewall with Application Awareness

Step 1. Click **Add Firewall Policy,** create a new firewall policy by selecting **Create New** and click **Next.** However, if you have preconfigured a firewall policy, simply click on **Copy from Existing.**

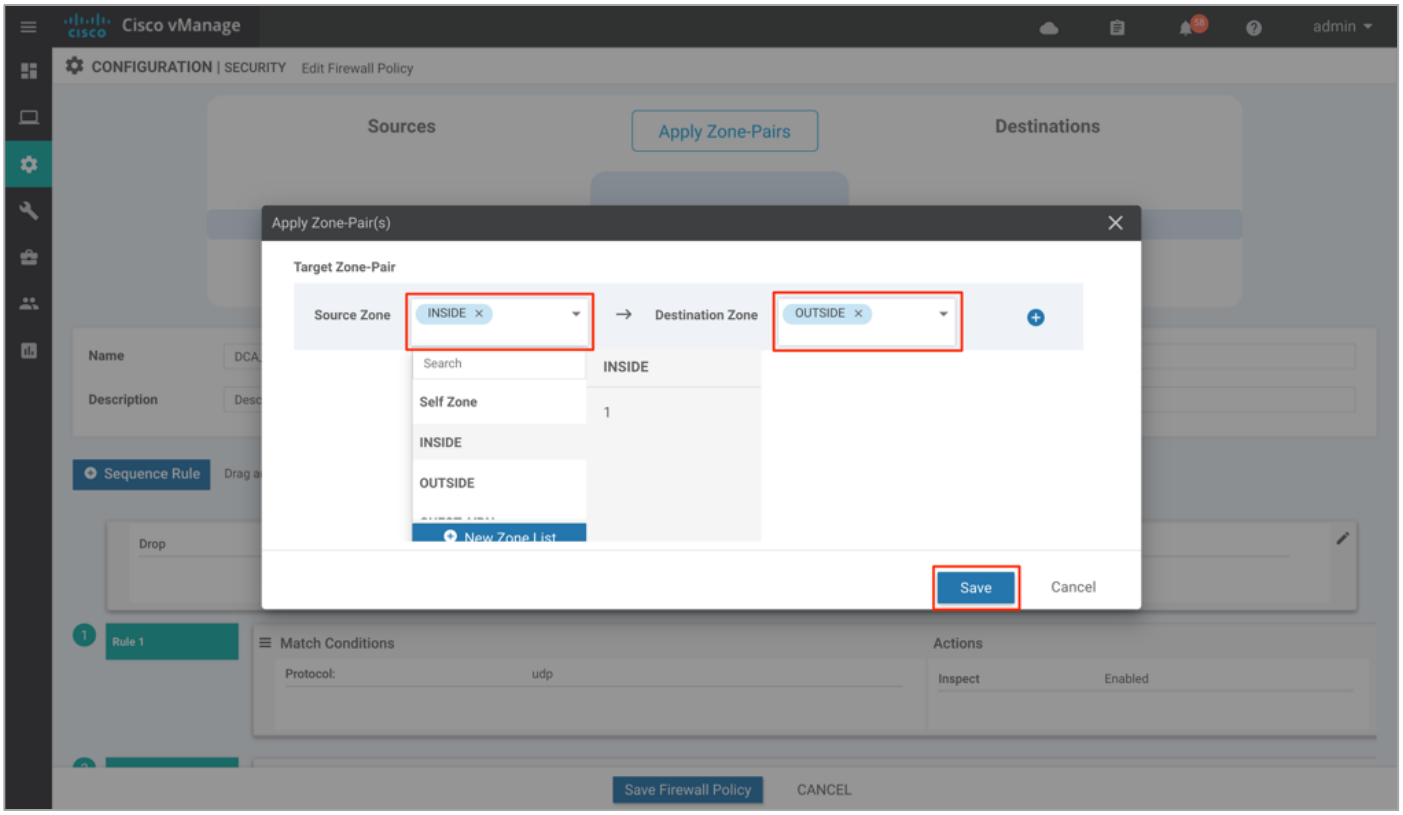


Create VPN zones and define your 5-tuple and Application behavior within these zones.

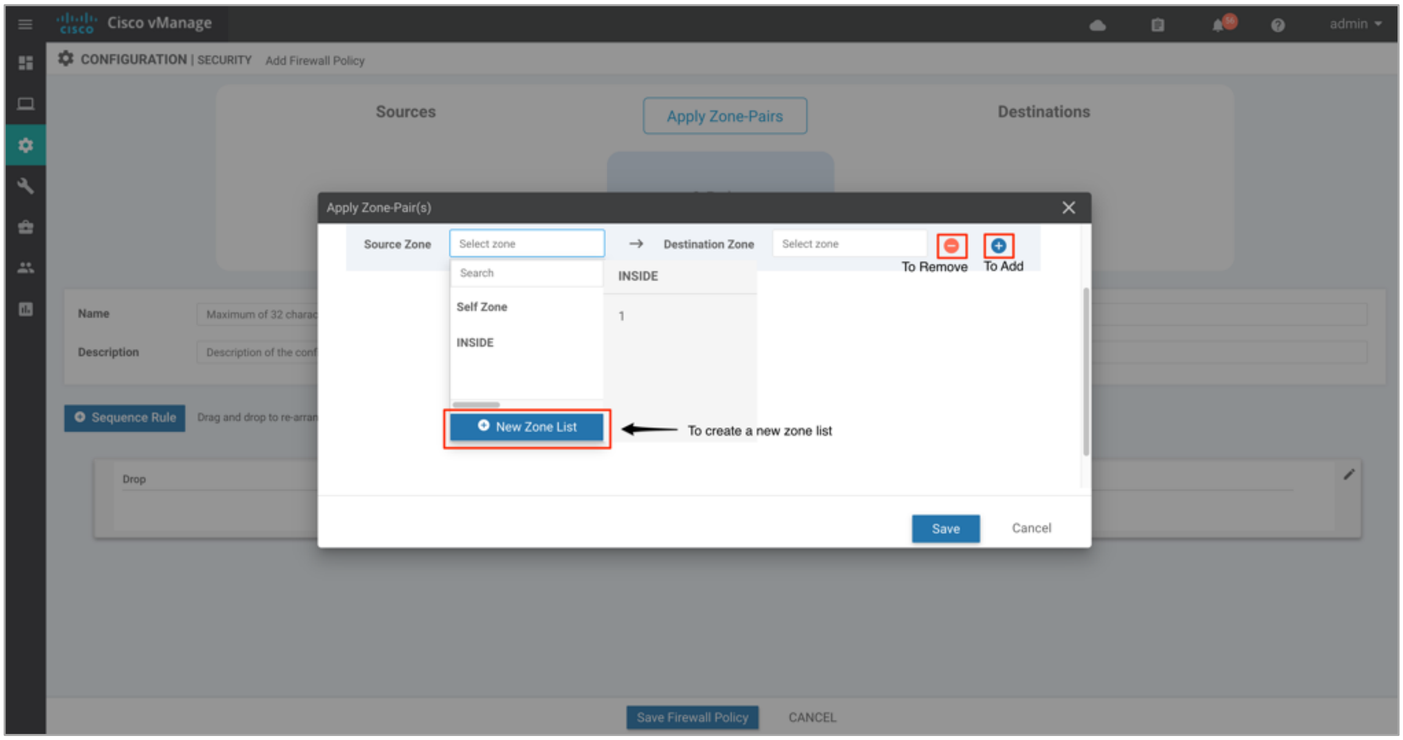
Step 2. Click on **Apply Zone-Pairs** to create your zone-pairs.



Step 3. Add the created zones to **Source Zone** and **Destination Zone**, and click **Save.**



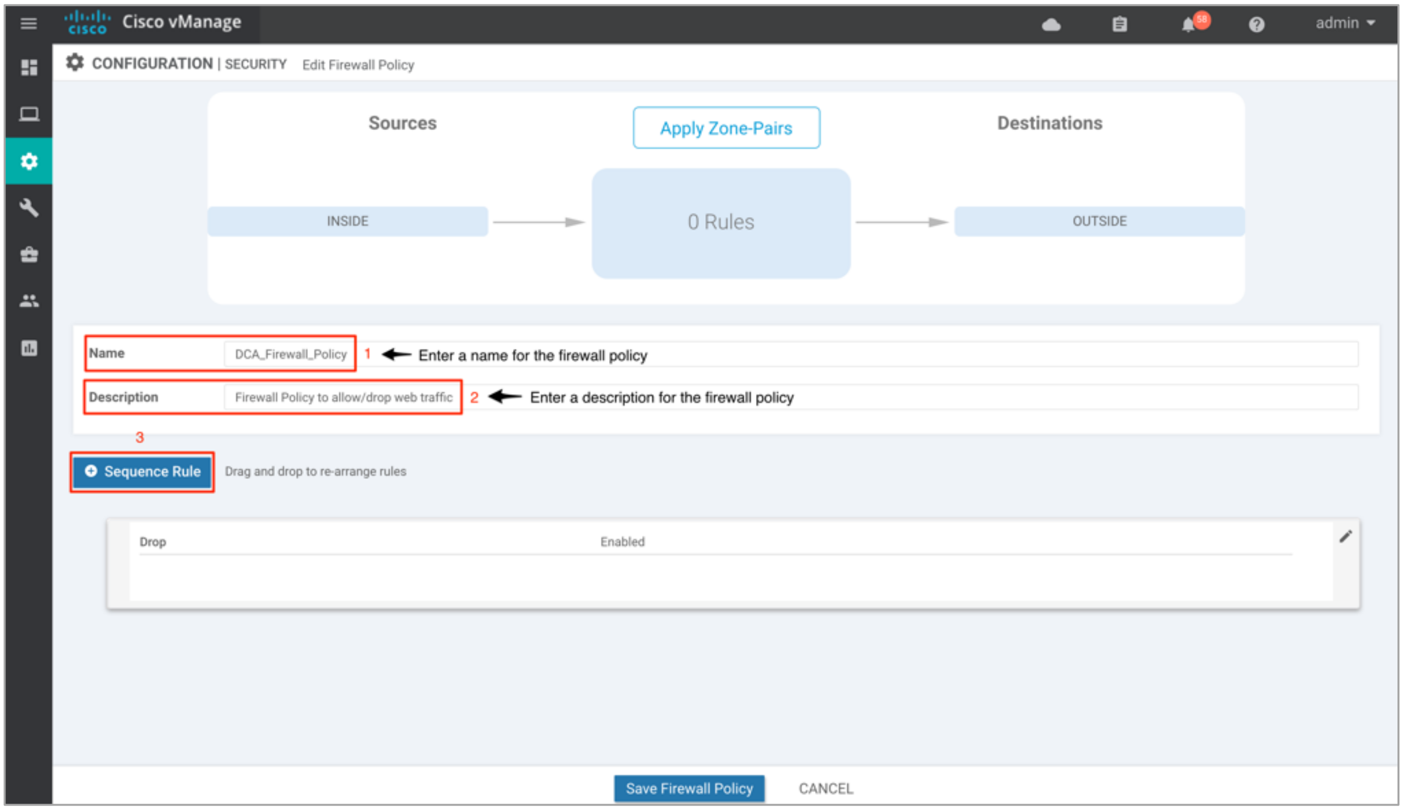
Note: If you wish to create a new zone, click on the **New Zone List**, and to add additional zone-pair click on the (+) sign. To remove a zone pair, click on (-) sign. See the following example:



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 that protects the packet going to or coming 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 4. Enter a **Name** and **Description** in the field for the firewall policy, next click on **Sequence Rule** to add policy rules.



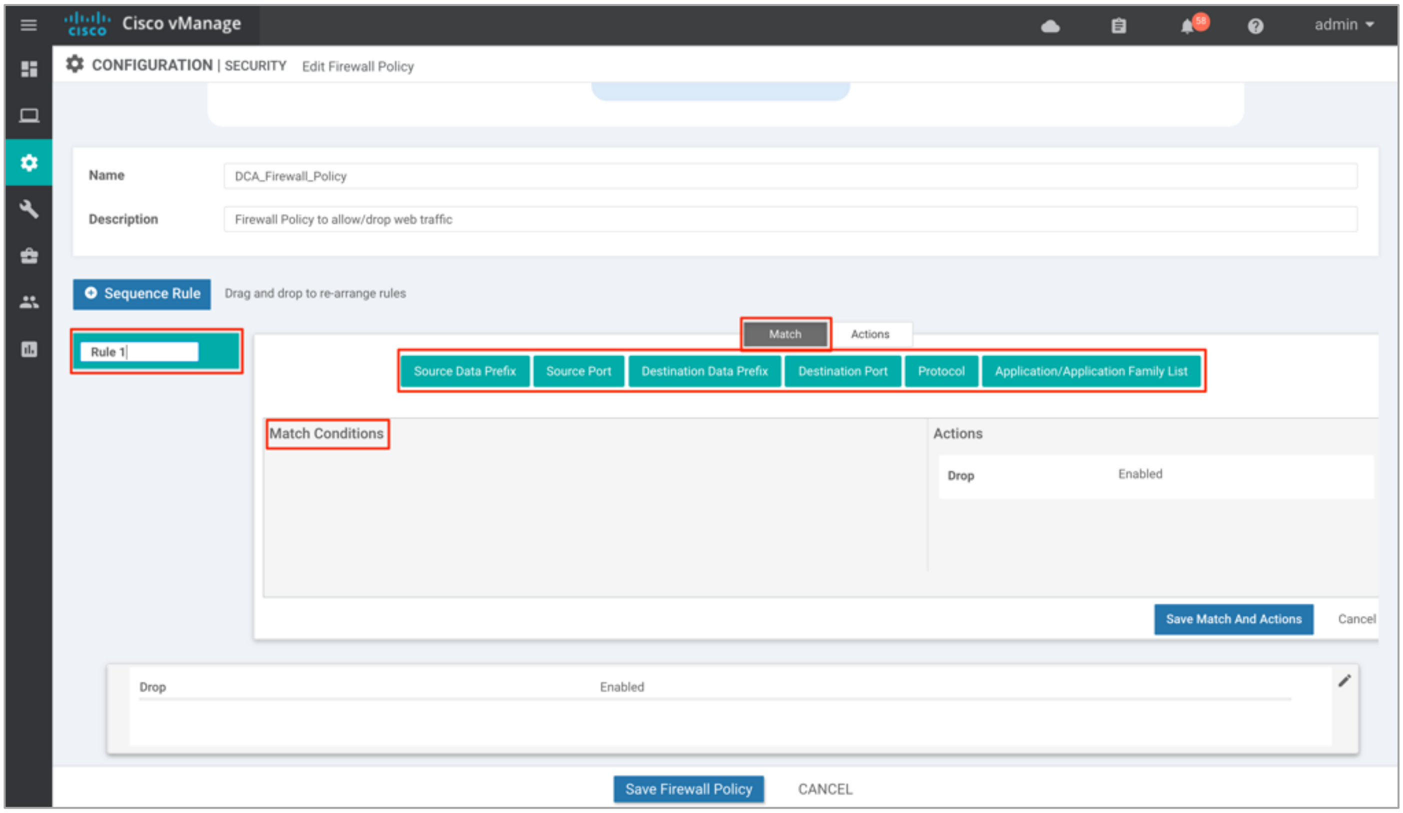
Name DCA_Firewall_Policy 1 Enter a name for the firewall policy

Description Firewall Policy to allow/drop web traffic 2 Enter a description for the firewall policy

3 Sequence Rule Drag and drop to re-arrange rules

Drop Enabled

Step 5. 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 condition in a sequence.



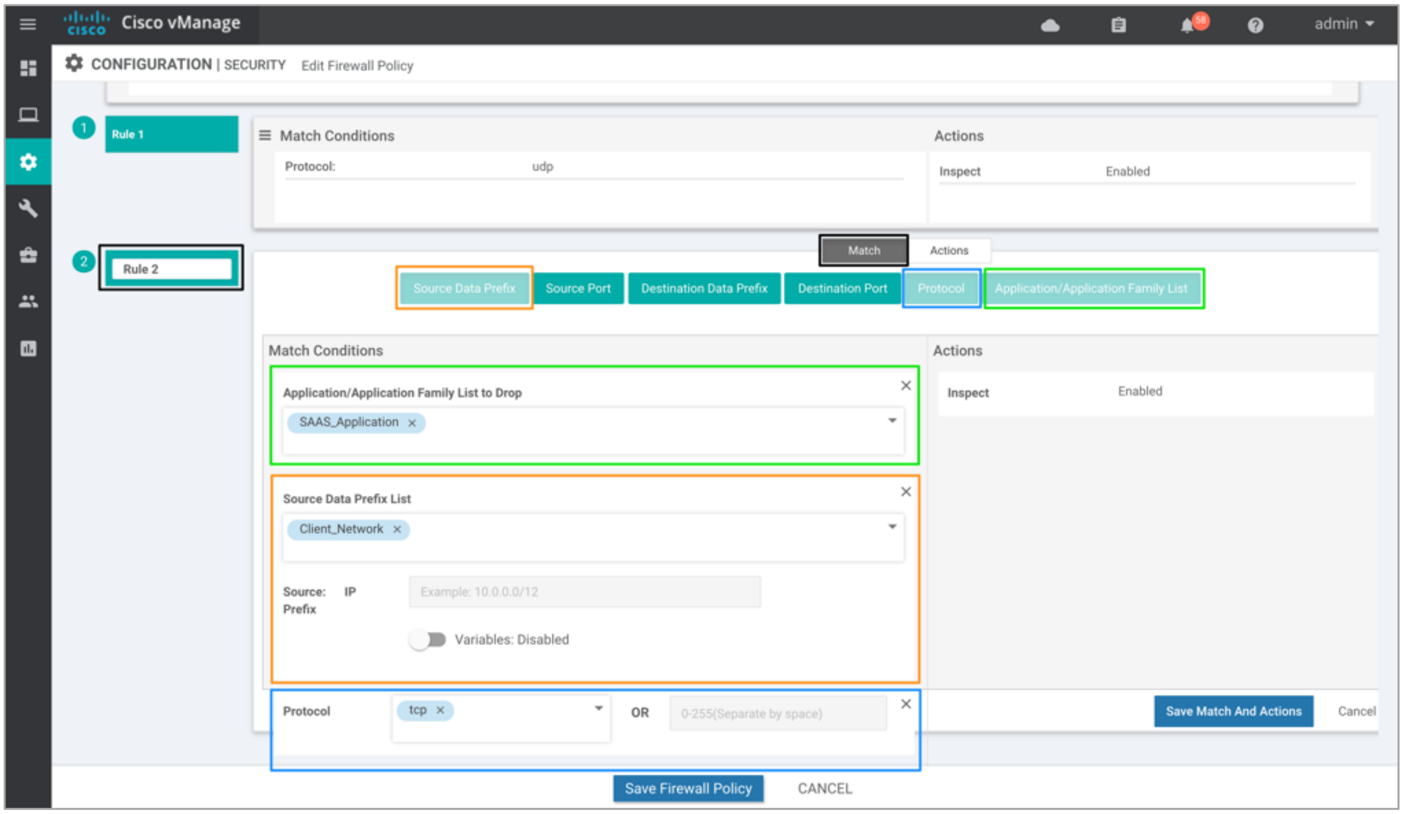
Name DCA_Firewall_Policy

Description Firewall Policy to allow/drop web traffic

Drop Enabled

Drop Enabled

Here’s an example of sequence rule within the Enterprise Firewall with Application Awareness policy deployed.



Match Conditions

Protocol: udp

Actions

Inspect Enabled

Match Conditions

Application/Application Family List to Drop: SAAS_Application

Source Data Prefix List: Client_Network

Source: IP Prefix: Example: 10.0.0.0/12

Variables: Disabled

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

Actions

Inspect Enabled

In this firewall policy, we inspect both TCP flows and traffic originating from the Client_Network. Any application traffic matching the applications listed in the " Application list to drop" will be dropped regardless of the action condition.

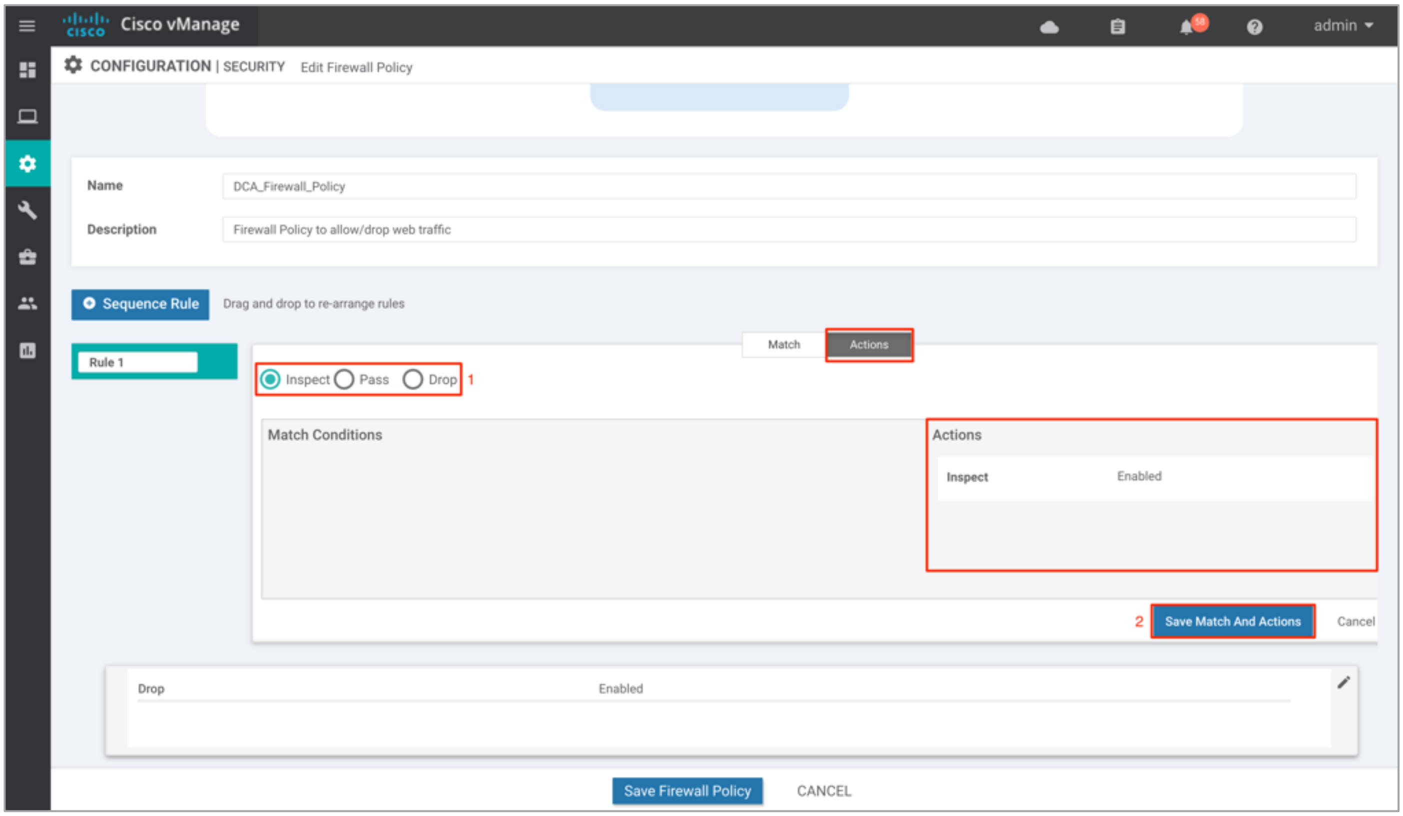
Firewall CLI:

```
class-map match-any SAAS_Application-cm0_
match protocol dropbox
match protocol gmail
match protocol ms-office-365
!
policy-map type inspect avc SAAS_Application-pm_
class SAAS_Application-cm0_
deny
!
policy-map type inspect DCA_Firewall_Policy_1
class DCA_Firewall_Policy_1-seq-1-cm_
inspect
!
class DCA_Firewall_Policy_1-seq-11-cm_
inspect
service-policy avc SAAS_Application-pm_
```

```
        !
        class class-default drop
        !
        !
```

The firewall policy inspects traffic that matches the " DCA_Firewall_Policy_1-seq-11-cm_" class based on L3/L4 information and the traffic is permitted, unless it matches the defined " Application list to drop”.

Step 6. Next, Click on **Actions** tab and enter the actions to take if the traffic matches. We have enabled **Inspect**.



Name: DCA_Firewall_Policy

Description: Firewall Policy to allow/drop web traffic

● Inspect ○ Pass ○ Drop

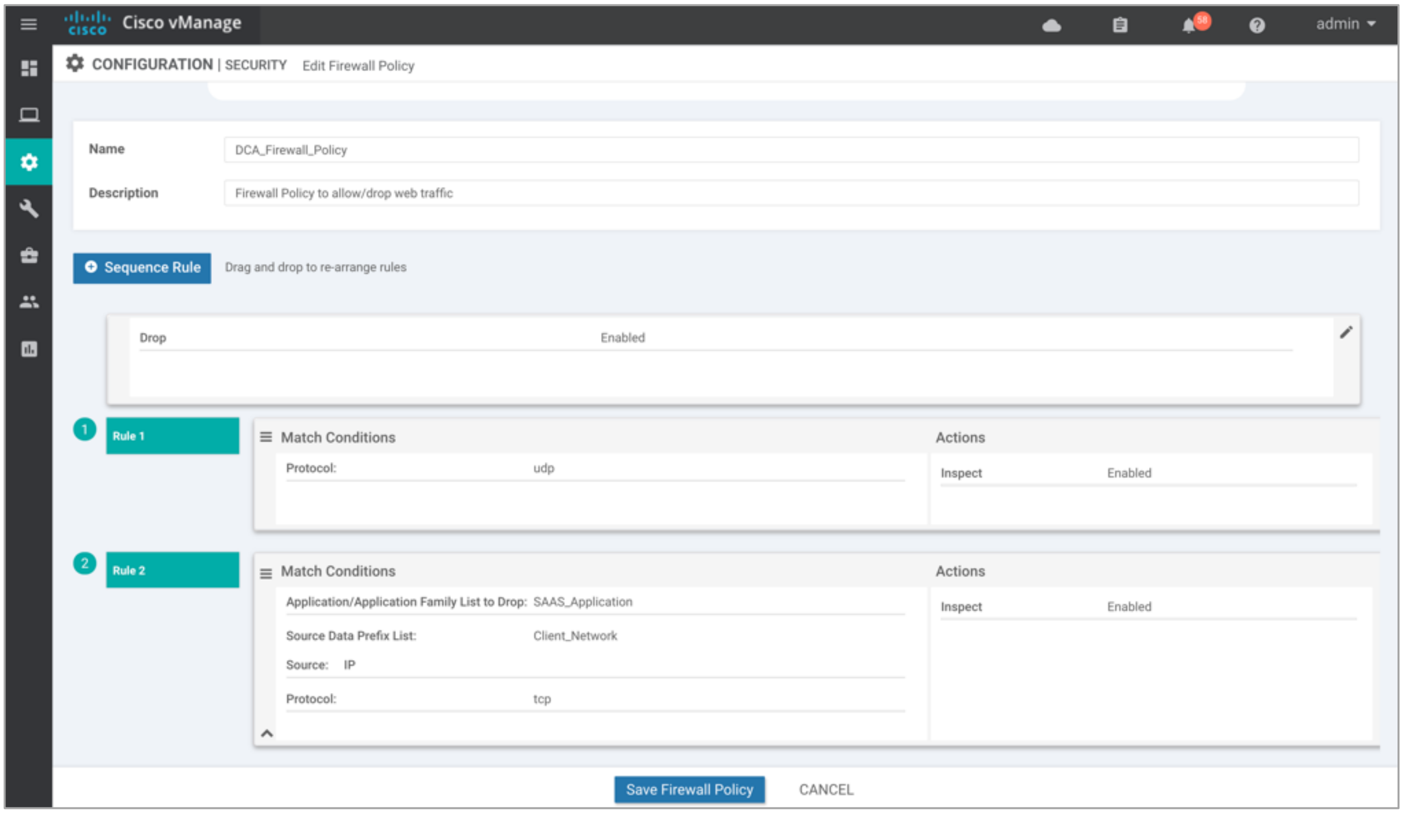
Match Conditions

Actions

Inspect Enabled

Drop Enabled

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


Cisco vManage
admin
CONFIGURATION | SECURITY   Edit Firewall Policy
Sequence Rule
Drag and drop to re-arrange rules
Save Firewall Policy
CANCEL

Name: DCA_Firewall_Policy

Description: Firewall Policy to allow/drop web traffic

Drop: Enabled

1 Rule 1

Match Conditions
- Protocol: udp

Actions
- Inspect: Enabled

2 Rule 2

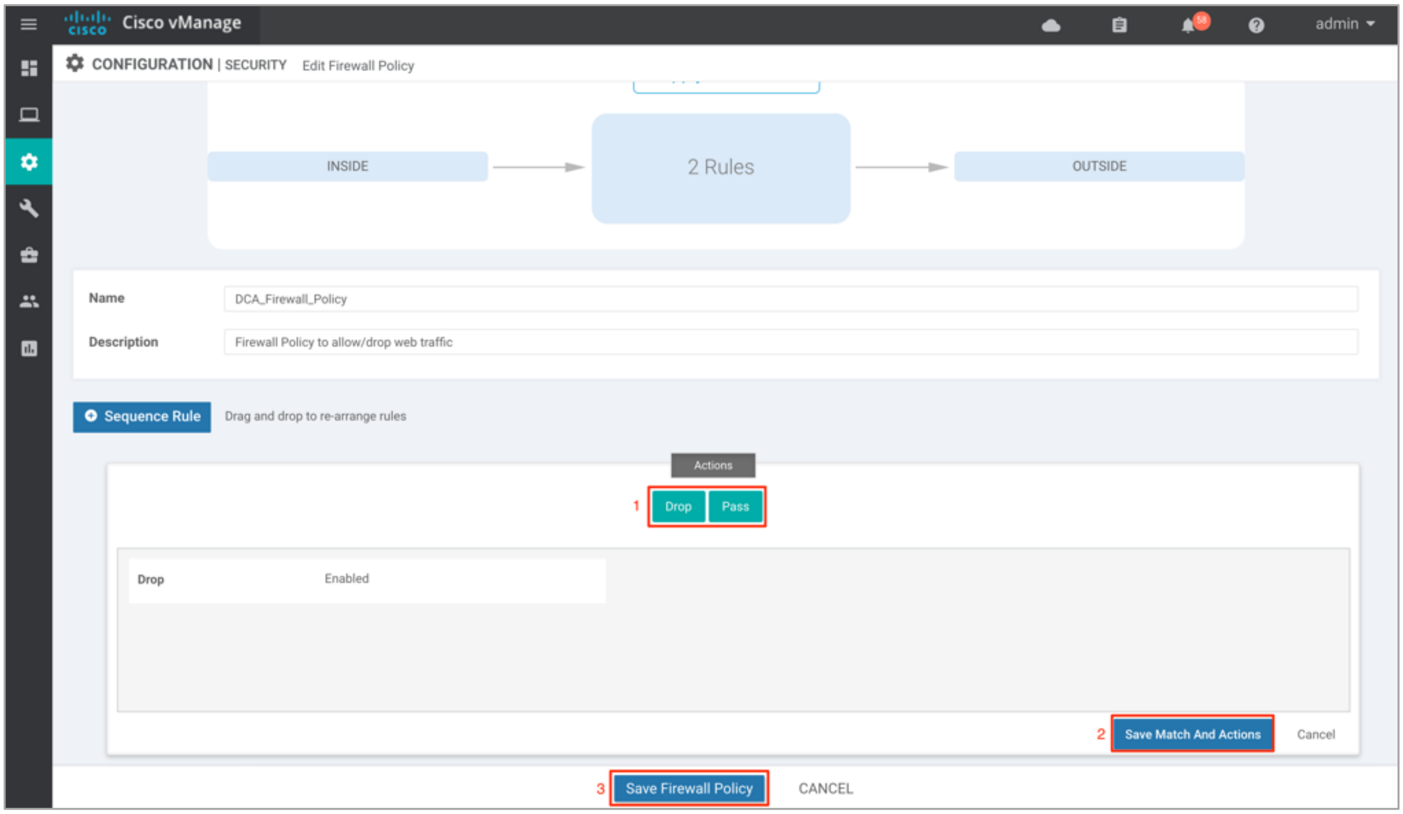
Match Conditions
- Application/Application Family List to Drop: SAAS_Application
- Source Data Prefix List: Client_Network
- Source: IP
- Protocol: tcp

Actions
- Inspect: Enabled

Within SAAS_Application, we have matched one SAAS application that is to be dropped.

Step 7. (Optional) If a packet matches none of the parameters in any of the policy sequences, you define a default action to be taken on the packet. So, once you have the sequence rules configured, continue to edit the default action to either **Drop** or **Pass** and click **Save Match And Actions** to save the changes made. Finally, save the configured firewall policy.

In this deployment, the default action is set to **Drop**.

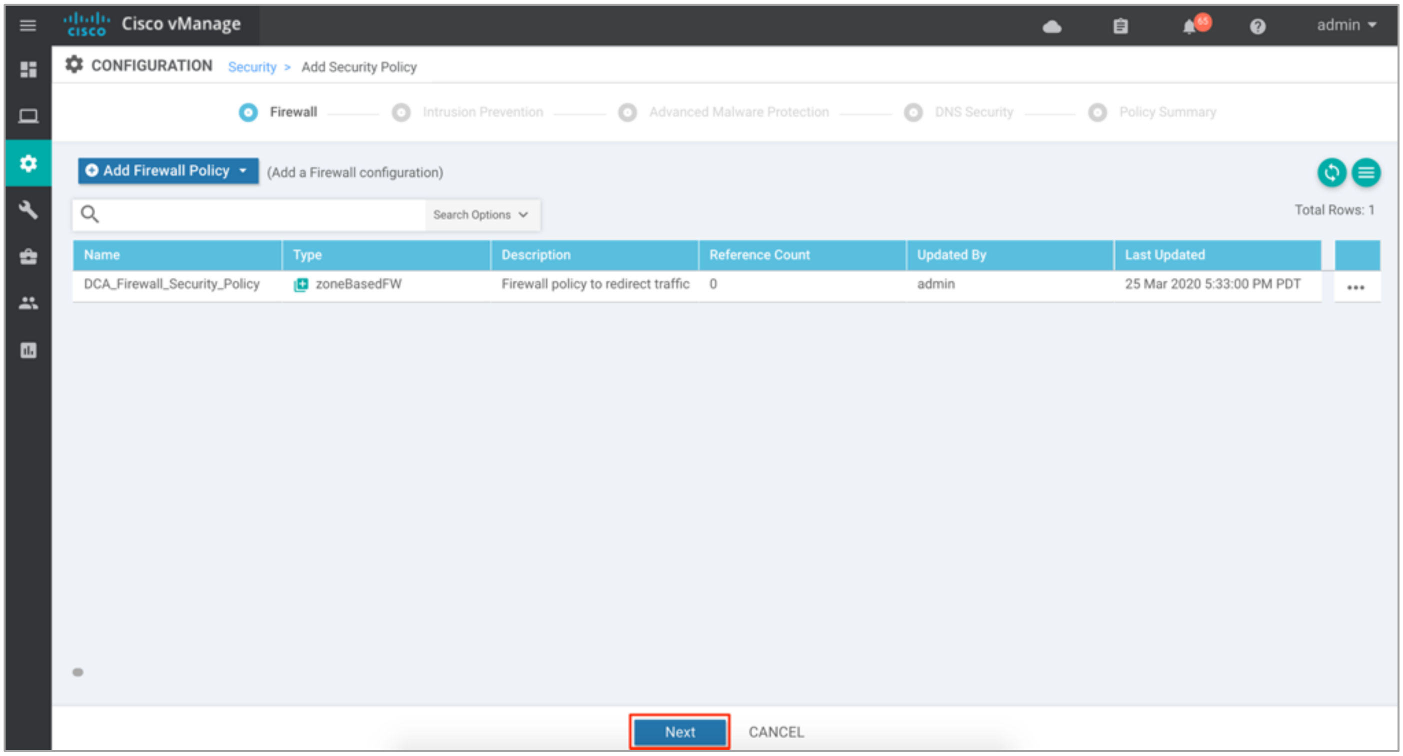


Name: DCA_Firewall_Policy

Description: Firewall Policy to allow/drop web traffic

Drop: Enabled

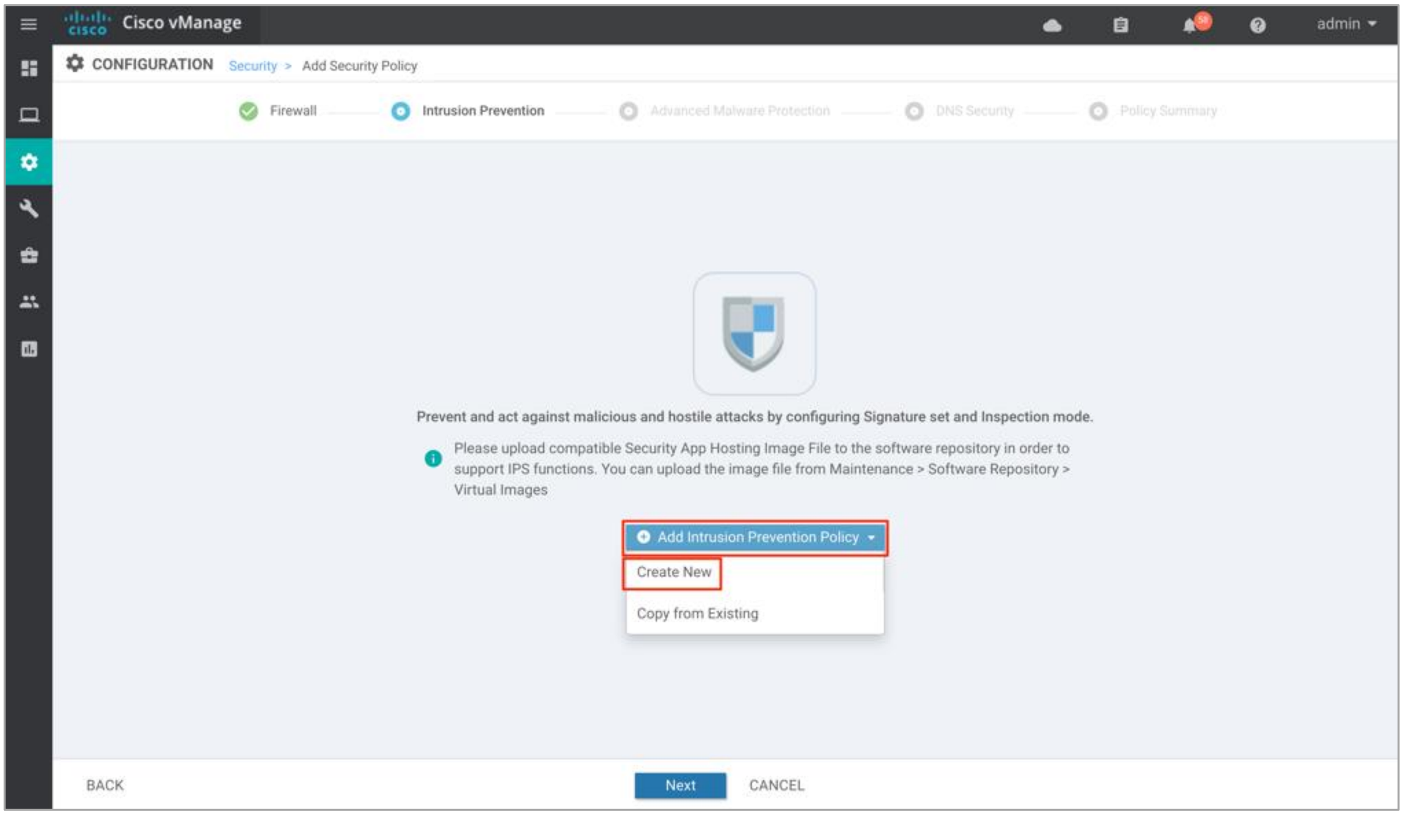
Step 8. Click **Next**, to configure the **Intrusion Prevention Policy**.



Name	Type	Description	Reference Count	Updated By	Last Updated
DCA_Firewall_Security_Policy	zoneBasedFW	Firewall policy to redirect traffic	0	admin	25 Mar 2020 5:33:00 PM PDT

Procedure 2. Configure Intrusion Prevention Policy

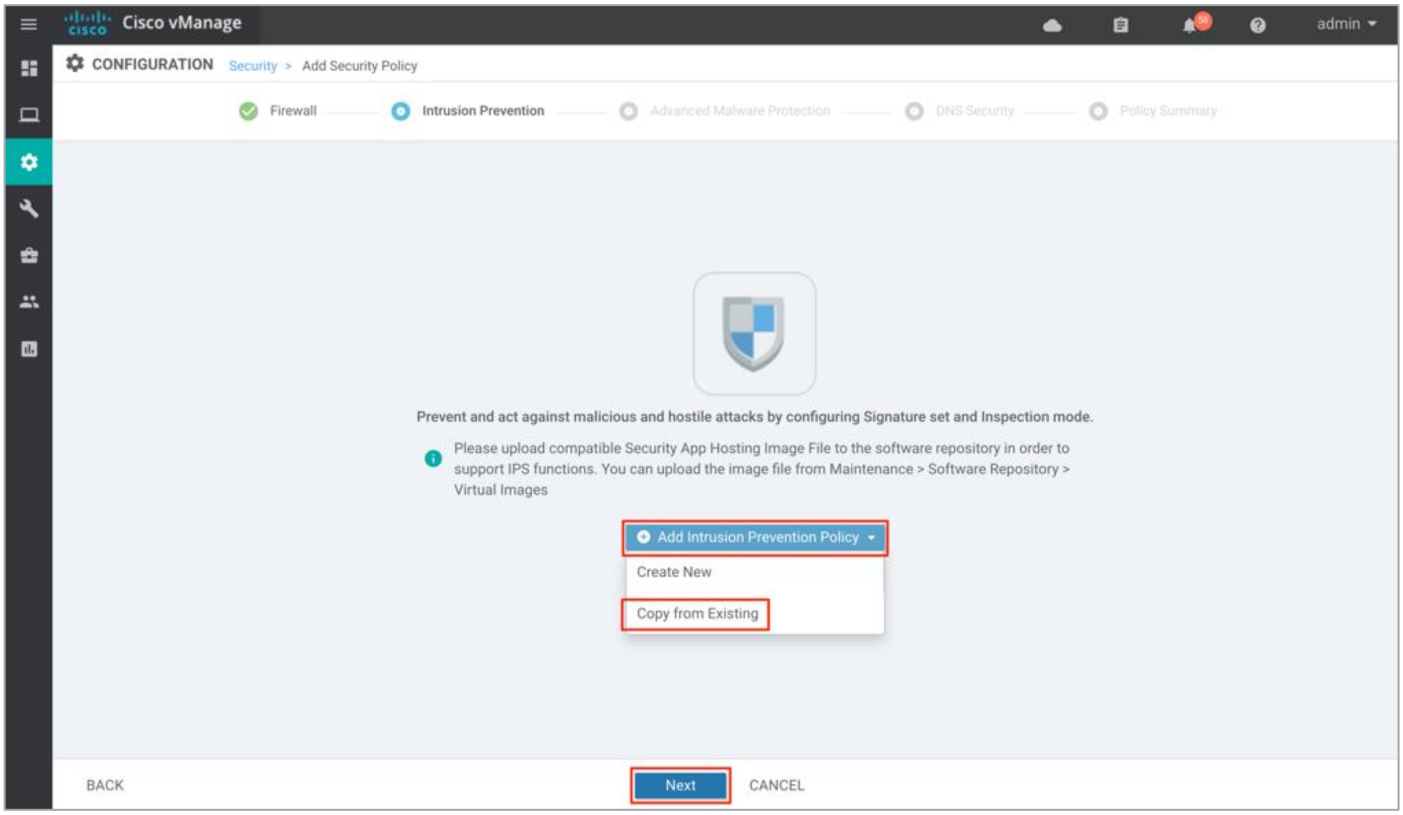
Step 1. Click on **Add Intrusion Prevention Policy** to enable Snort IPS, select **Create New** to create a new IPS policy and click **Next.**



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

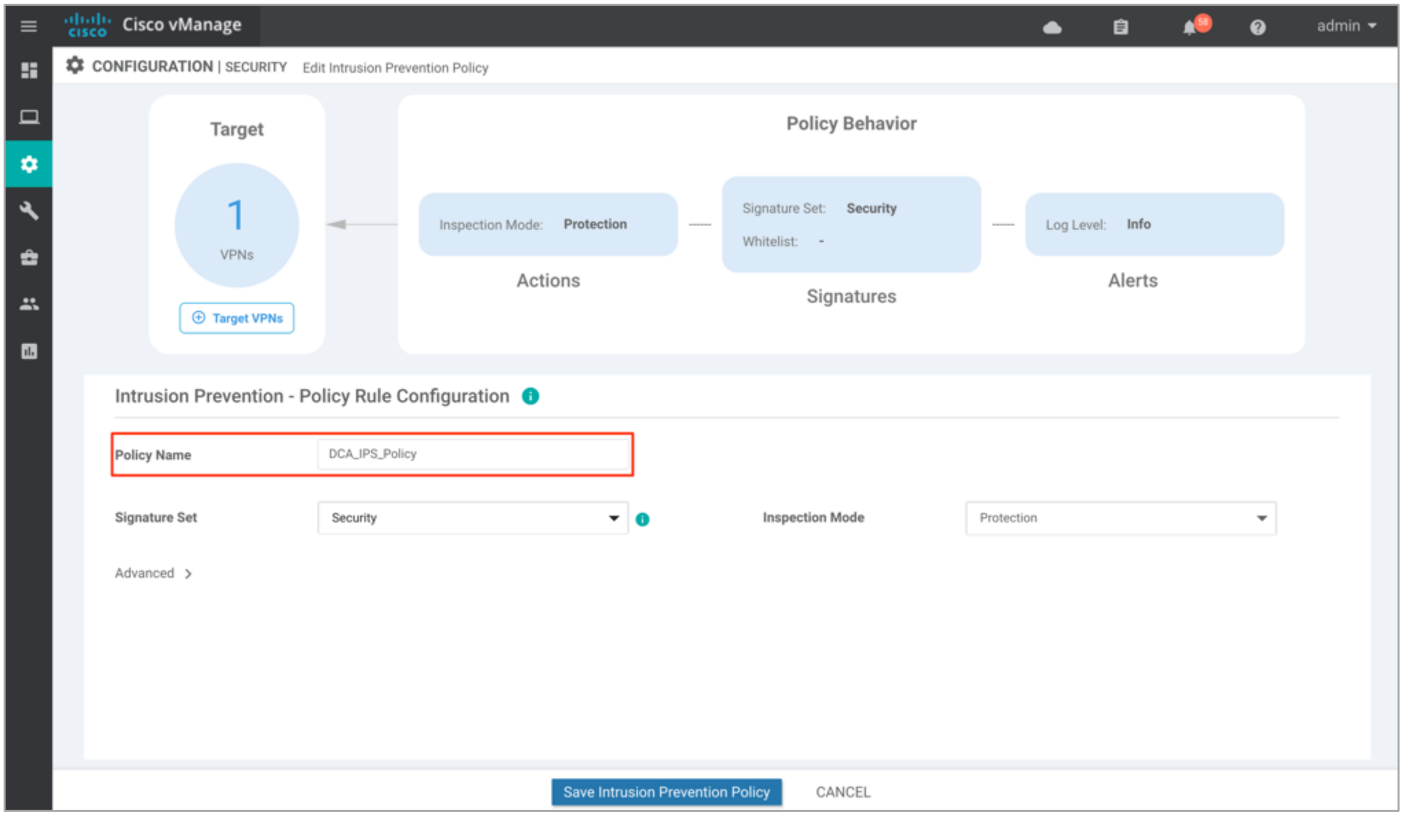
Note: If you wish to export an existing policy, simply click on **Copy from Existing**, fill in the policy details and then **Next.**



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 2. Enter a policy name in the **Policy Name** field.



Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Info

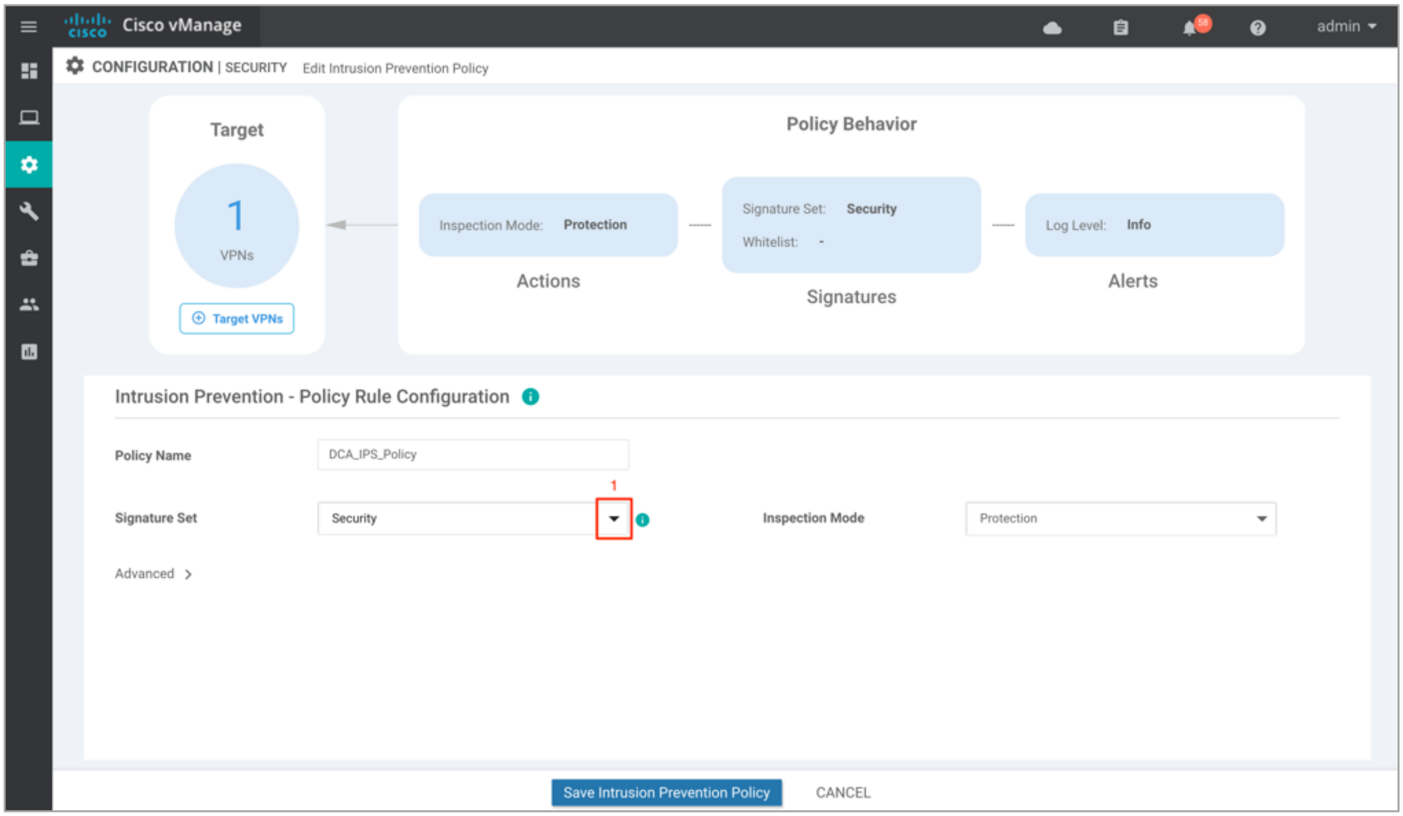
Intrusion Prevention - Policy Rule Configuration

Policy Name: DCA_IPS_Policy

Signature Set: Security

Inspection Mode: Protection

Step 3. Select a **Signature Set** that defines the rules for evaluating traffic from the **Signature Set** drop-down.



Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Info

Intrusion Prevention - Policy Rule Configuration

Policy Name: DCA_IPS_Policy

Signature Set: Security

Inspection Mode: Protection

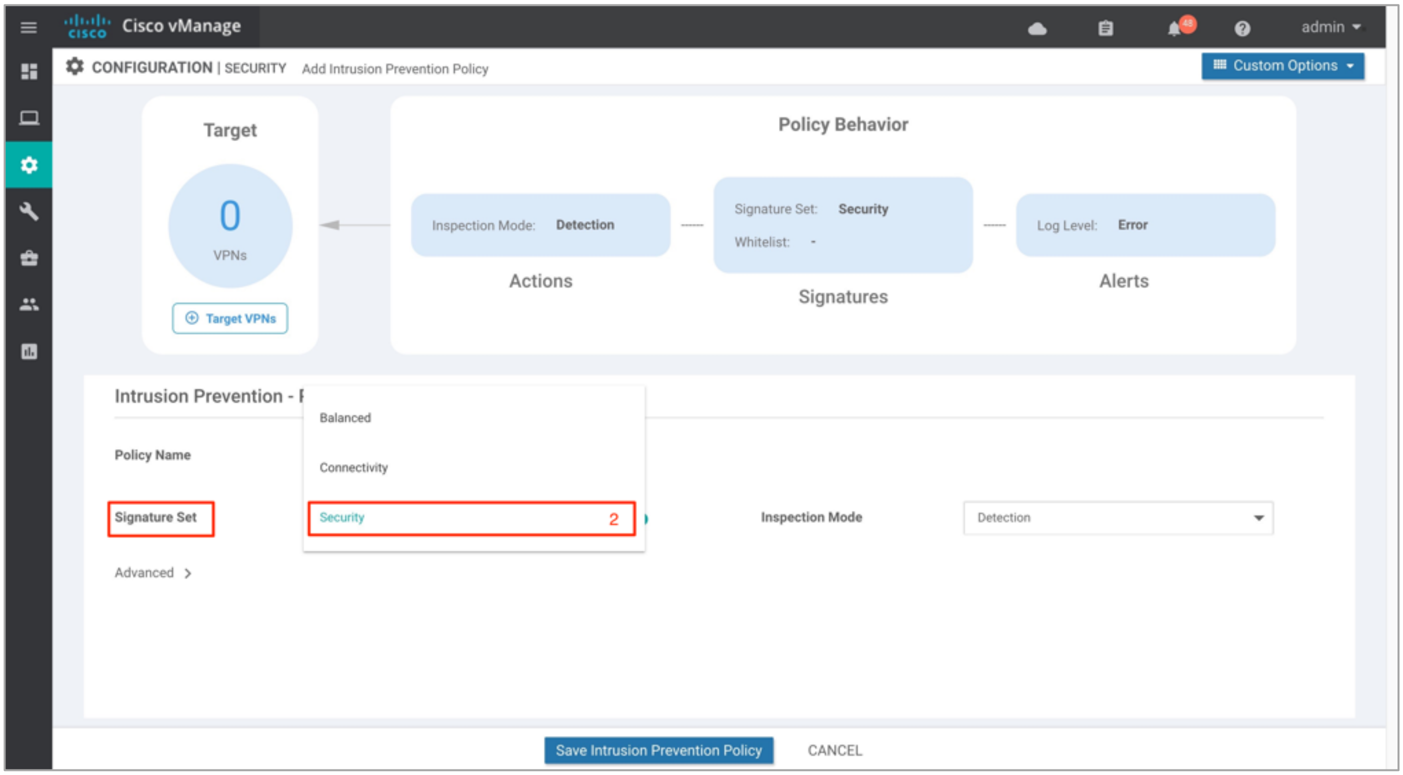
Step 4. In the Signature Set field, choose the desired signature set:

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.

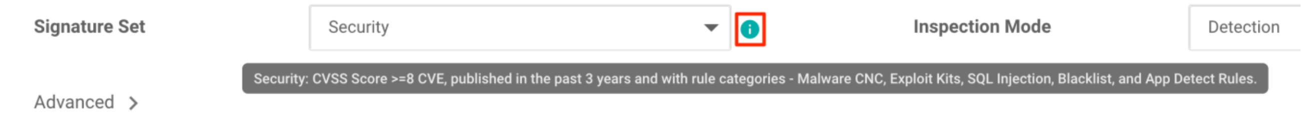
Security: With more added rules, this signature level offers the most protection.

Signature set refer to rules/signatures that have been developed, tested and approved by the Talos Security Intelligence and Research Team (Talos). Connectivity has the least number of signatures, Security has the most number of signatures and Balanced striking a 'balance'. For more information on Signature Set refer to the Security Policy for Cisco IOS-XE SD-WAN Devices Design Guide.



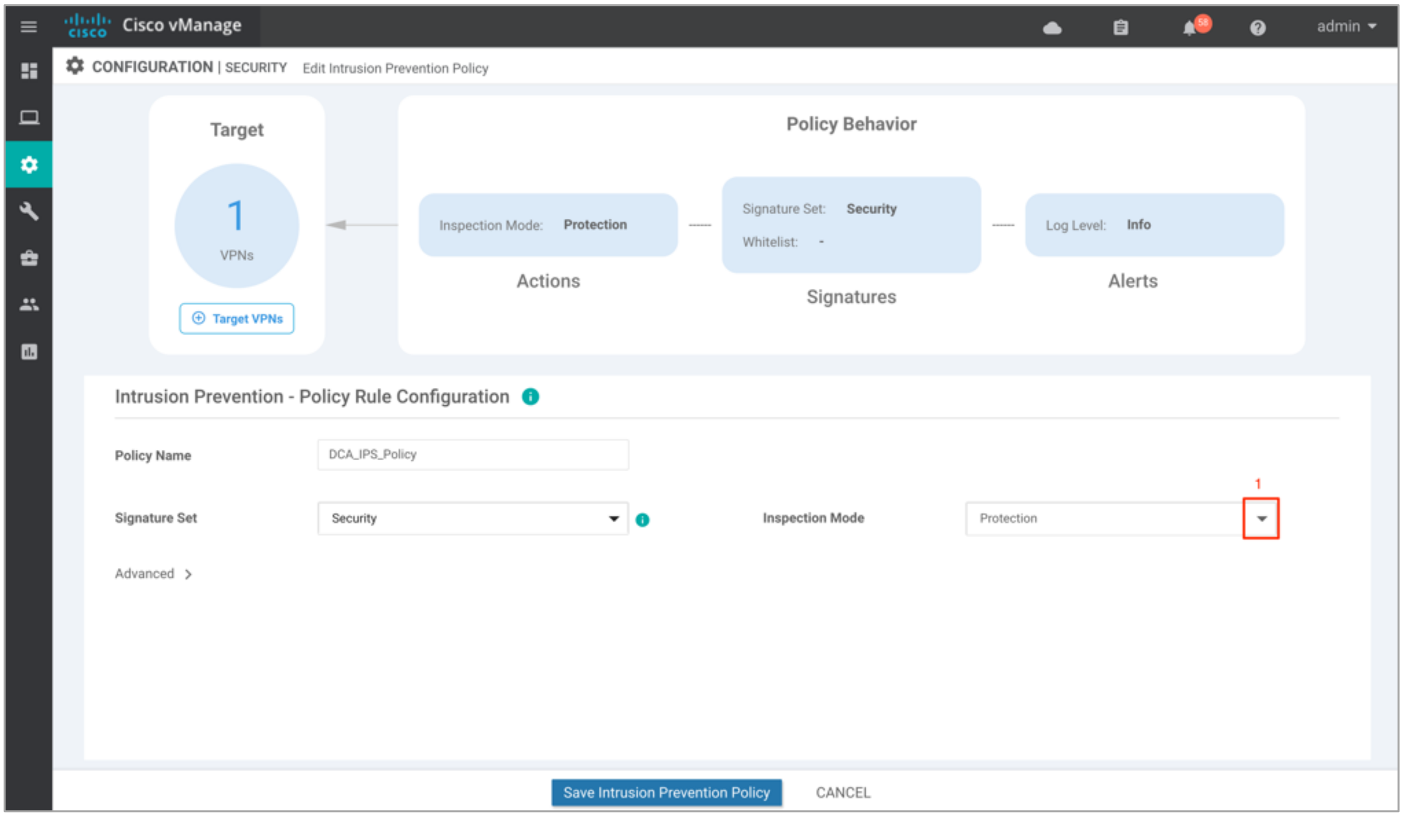
Technical Tip

To understand the CVSS score of a signature set, hover over the (!) found 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 5. Select the mode of operation from the **Inspection Mode** drop-down. By default, the mode of operation is set to **Detection.**



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

Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Info

Intrusion Prevention - Policy Rule Configuration

Policy Name: DCA_IPS_Policy

Signature Set: Security

Inspection Mode: Protection

Advanced >

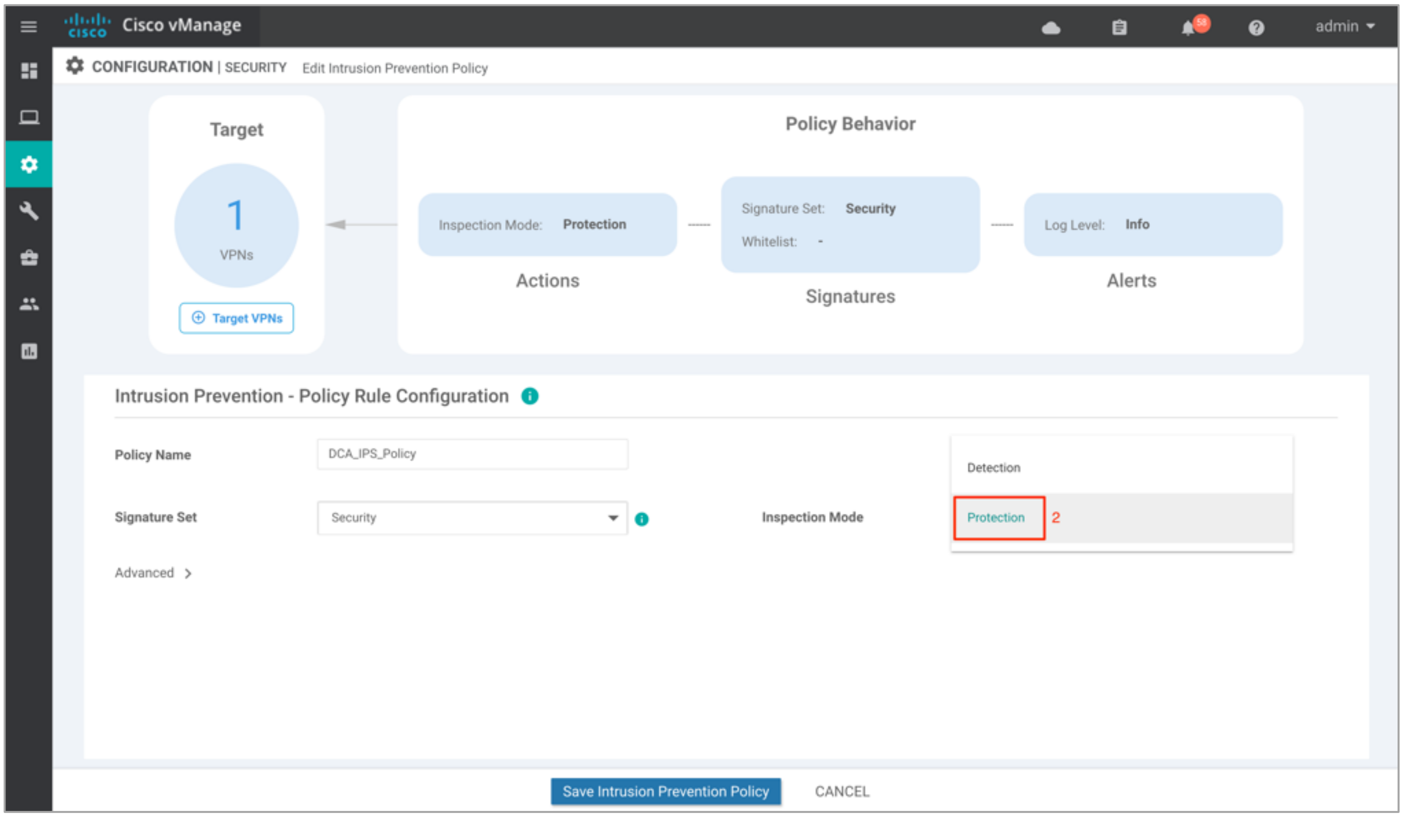
Step 6. The following options will populate:

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

Protection: Choose this option for intrusion protection mode.

In Detection mode (IDS), Snort inspects the traffic and reports alerts, but does not take any action to prevent attacks. In Protection mode (IPS), in addition to Intrusion detection, actions are taken to prevent attacks.

In this deployment guide, the Inspection Mode is set to Protection.



Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Info

Intrusion Prevention - Policy Rule Configuration

Policy Name: DCA_IPS_Policy

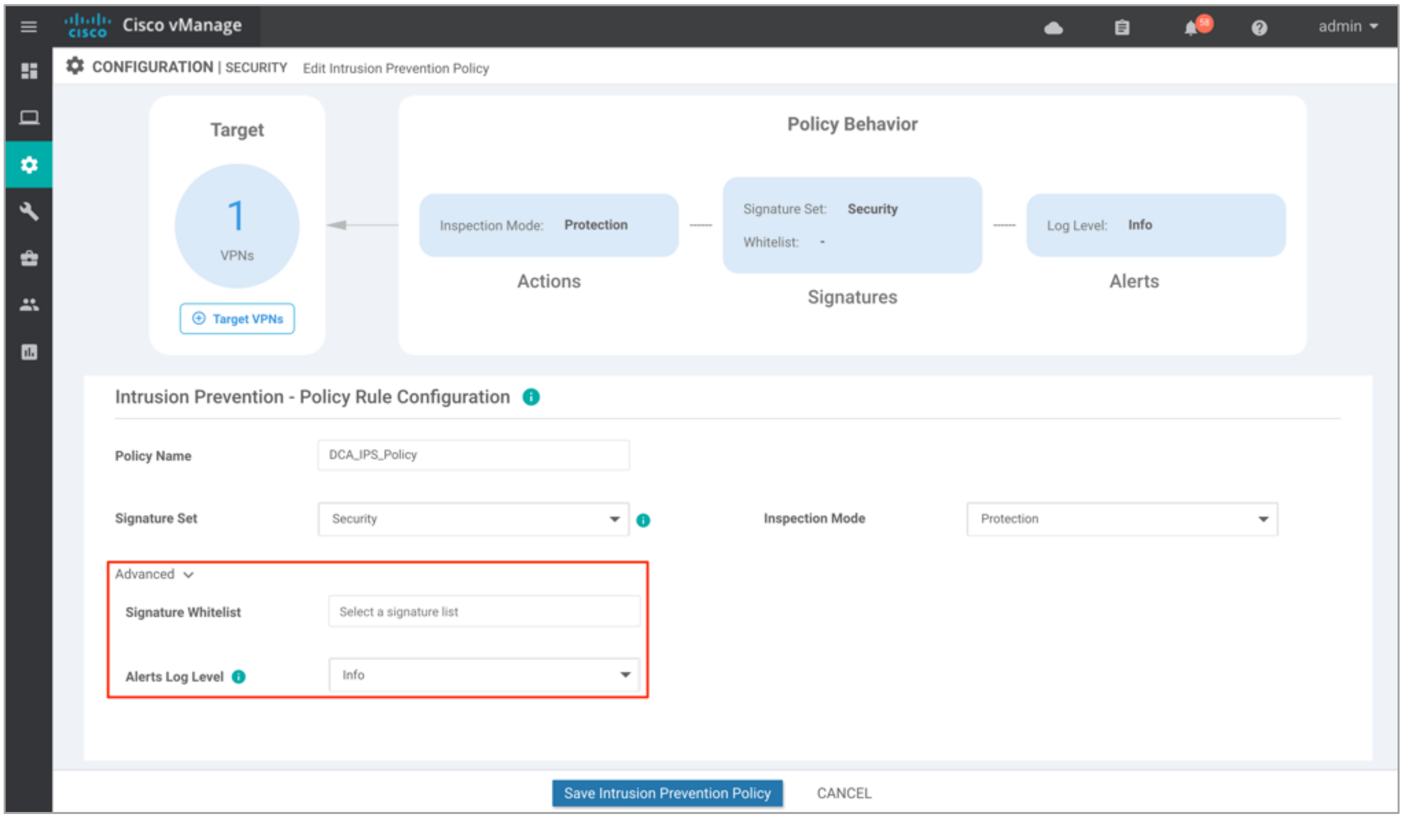
Signature Set: Security

Inspection Mode: Protection

Step 7. Click on **Advanced** tab, to whitelist signatures within **Signature Whitelist** and set the **Alerts Log Level**.

Signatures are whitelisted to reduce the number of false positives i.e. to reduce the chance of a non-harmful file being detected as a malware.

The signature whitelist format on vManage is Generator Identifiers (GID): Signature Identifiers (SID). For additional information on whitelisting signatures refer to the Security Policy for Cisco IOS-XE SD-WAN Devices Design Guide.



Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Info

Intrusion Prevention - Policy Rule Configuration

Policy Name: DCA_IPS_Policy

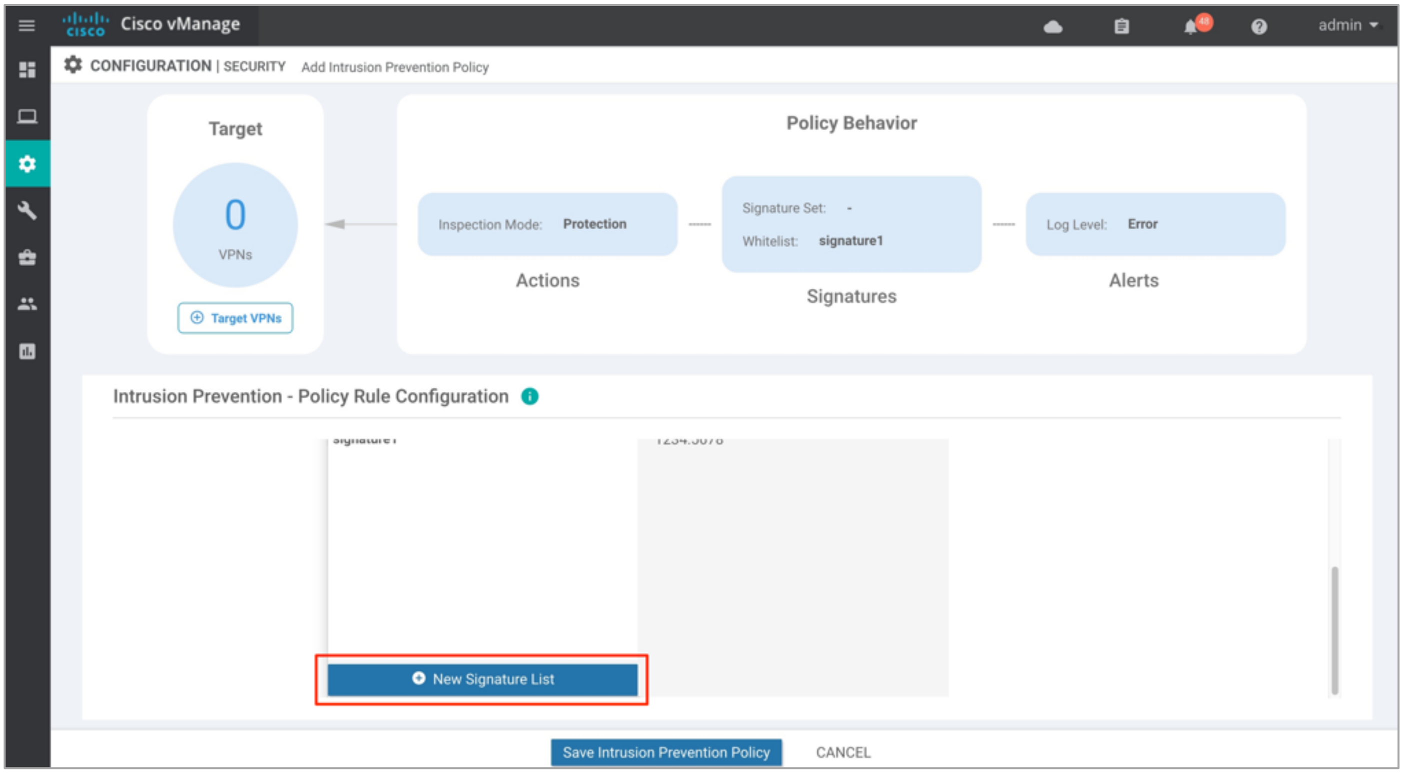
Signature Set: Security

Inspection Mode: Protection

Signature Whitelist: Select a signature list

Alerts Log Level: Info

Step 8. To create a new signature list, click on **Signature Whitelist** and within the drop-down, click on **New Signature List**.



Inspection Mode: Protection

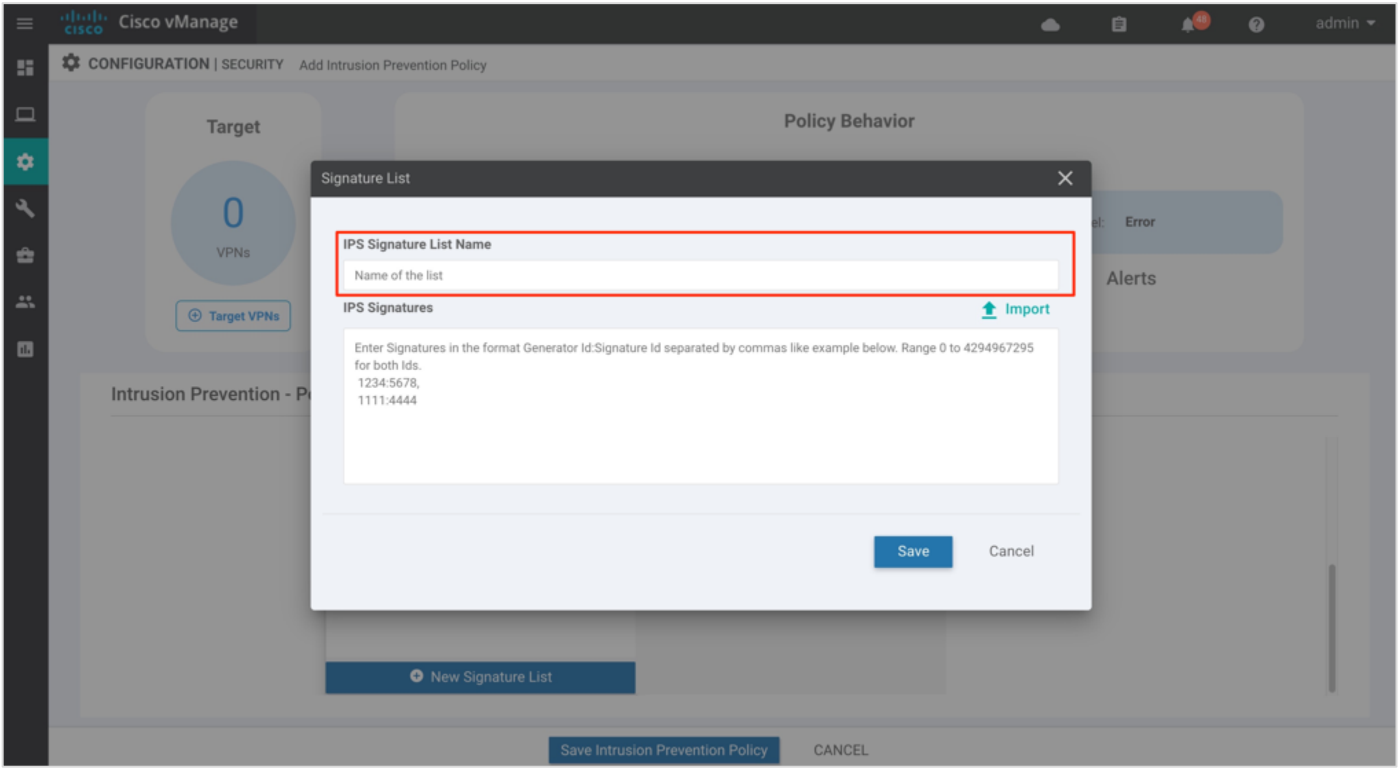
Signature Set: -

Whitelist: signature1

Log Level: Error

Intrusion Prevention - Policy Rule Configuration

Step 9. In this **IPS Signature List Name** field, enter a name consisting of up to 32 characters (letters, numbers, hyphens and underscores only).



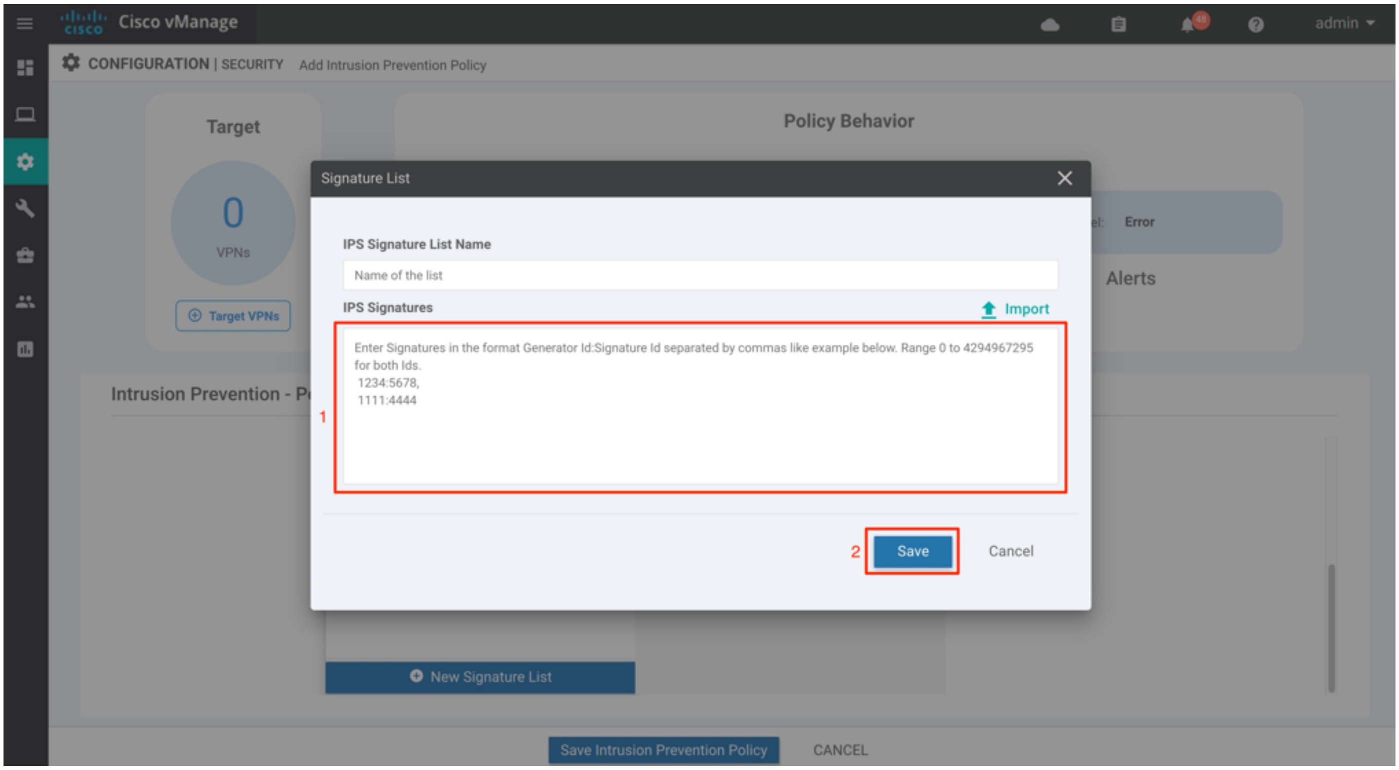
IPS Signature List Name

Name of the list

IPS Signatures

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 10. Within the IPS Signature field, enter signatures in the format Generator ID:Signature ID, separated with commas and click **Save** to save the configured Signature List.



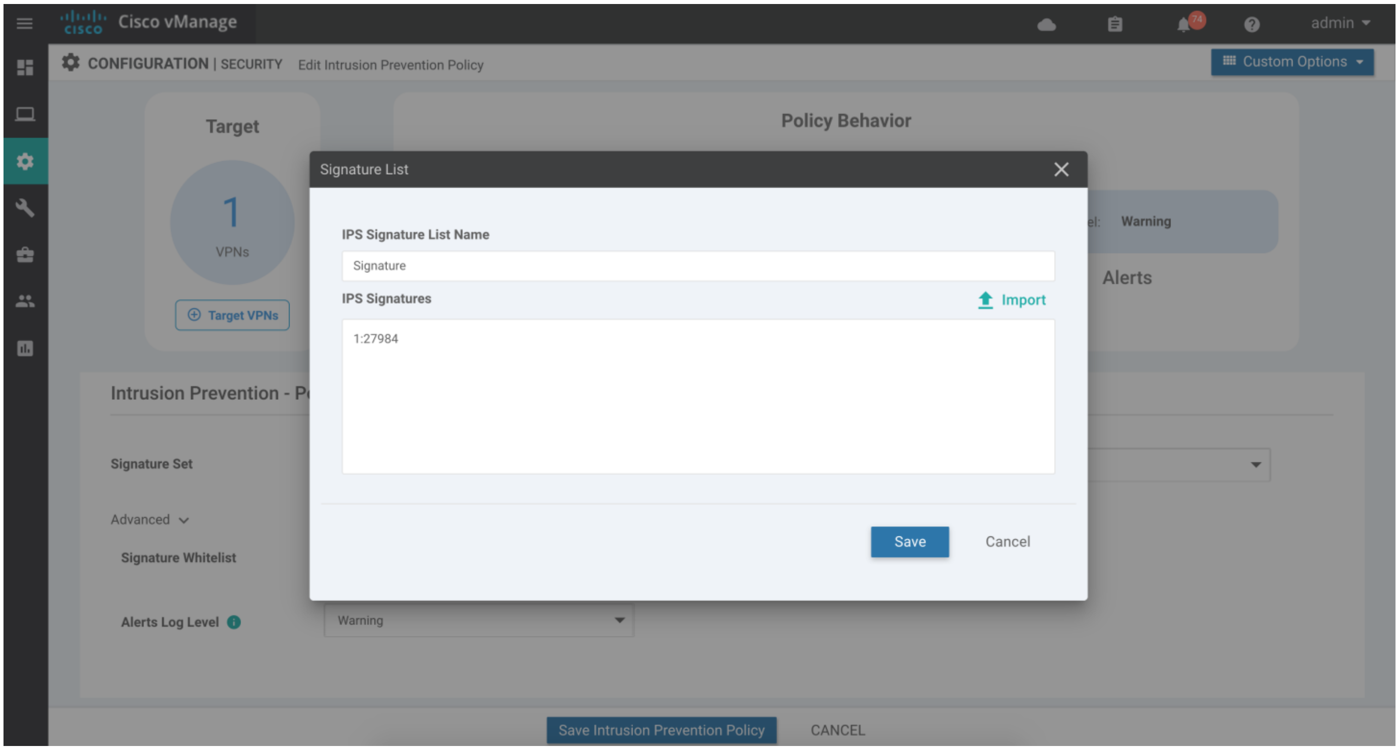
IPS Signature List Name

Name of the list

IPS Signatures

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

For example, APP-DETECT signature is whitelisted as GID:SID – 1:27984.



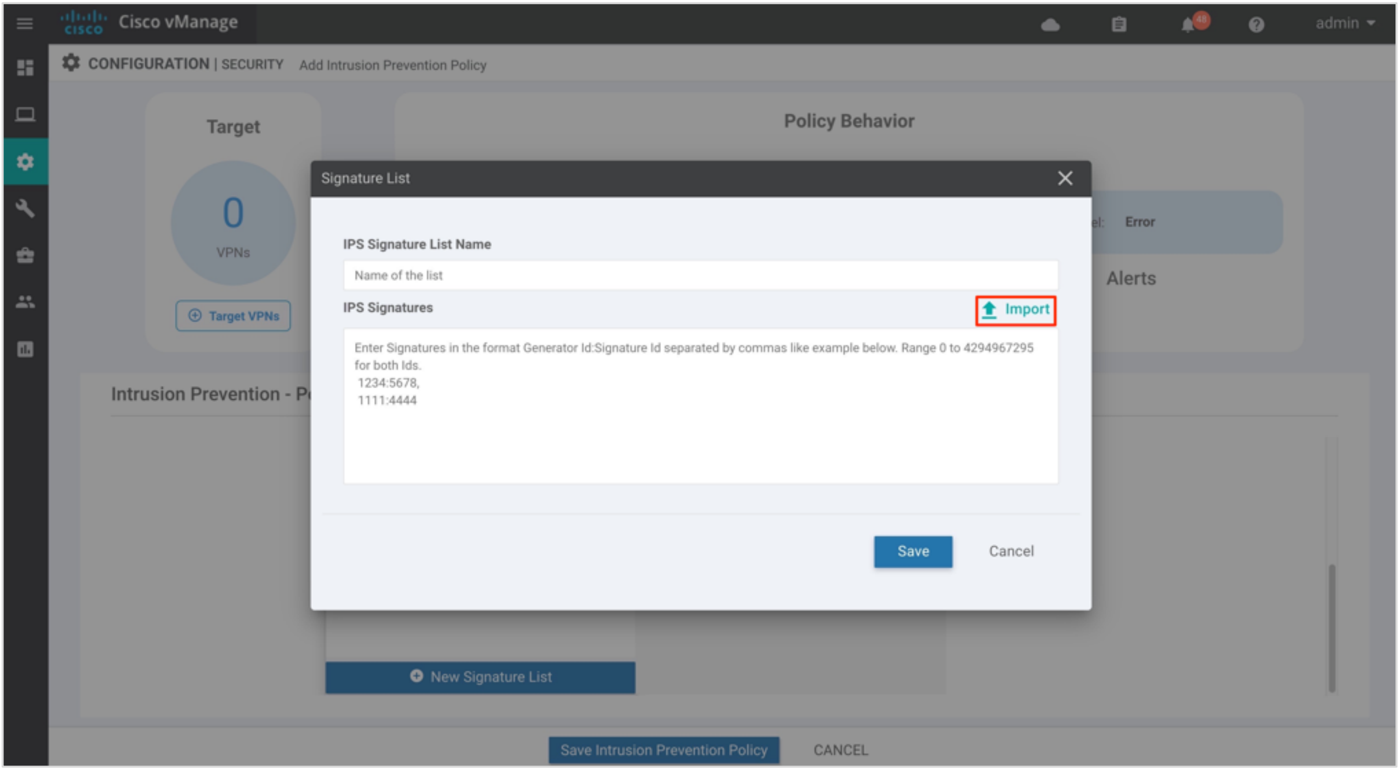
IPS Signature List Name: Signature

IPS Signatures: 1:27984

Technical Tip

One of the methods to find the GID and SID associated with a given signature rule in a signature set prior to deploying IPS functionality on the remote-site WAN Edge router, is to download the signature package from Cisco Software Central and then rename the downloaded file format from .pkg to .tar. Next, extract the renamed TAR file twice and click on the Rules folder contained in the unzipped file to view the signature rules associated with the signature sets. Within each signature rule, you can look for Signature ID (SID) and Generator ID (GID) associated with the Signatures to be whitelisted. The other is to copy SID's and GID's from the generated alert logs or to download the .pkg file into the edge devices flash drive, then enter command utd threat-inspection signature active-list write-to bootflash:<filename.txt> threat-inspection profile <ips profile>.

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



IPS Signature List Name

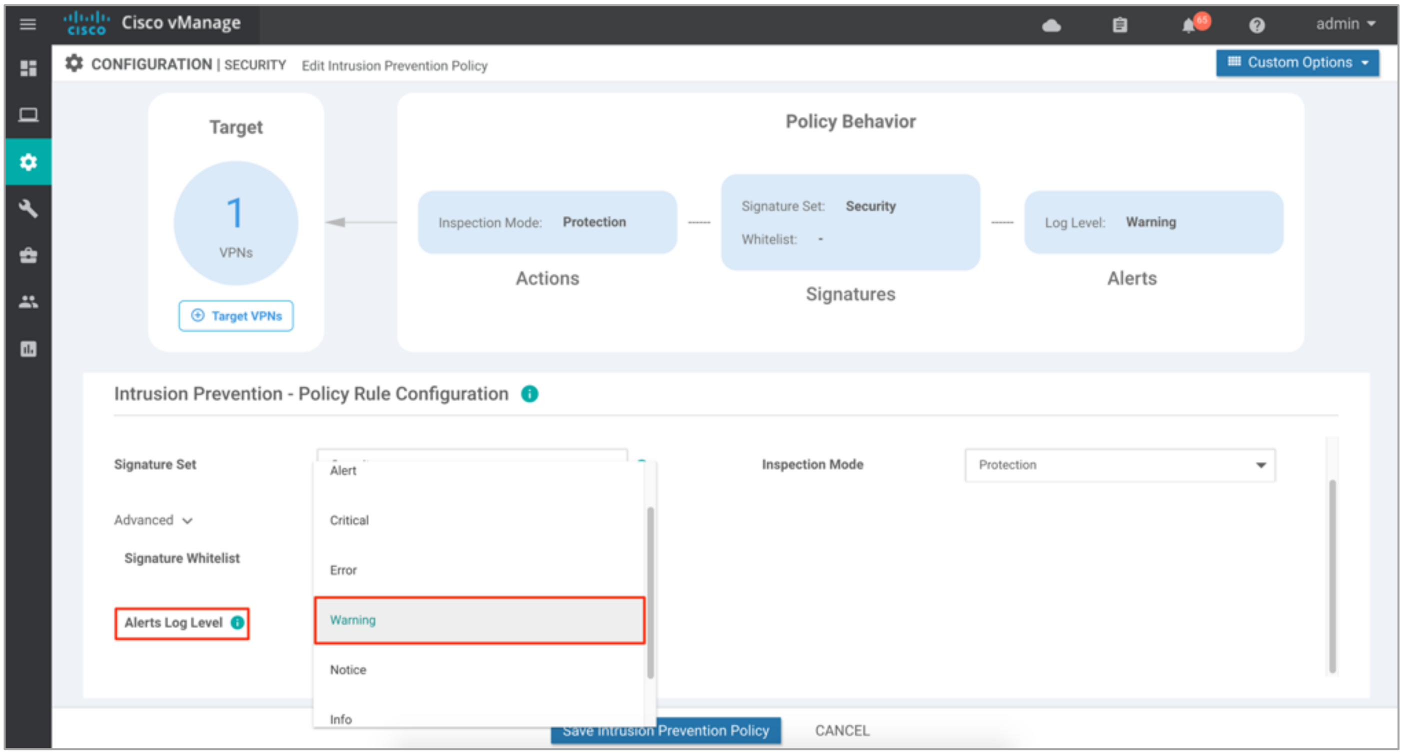
Name of the list

IPS Signatures

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

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 11. Select an alert level for syslog's from the **Alert Log Level** drop-down. Within the drop-down you will find 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.



Cisco vManage

CONFIGURATION | SECURITY Edit Intrusion Prevention Policy

Target: 1 VPNs

Policy Behavior

Inspection Mode: Protection — Actions

Signature Set: Security, Whitelist: - — Signatures

Log Level: Warning — Alerts

Intrusion Prevention - Policy Rule Configuration

Signature Set

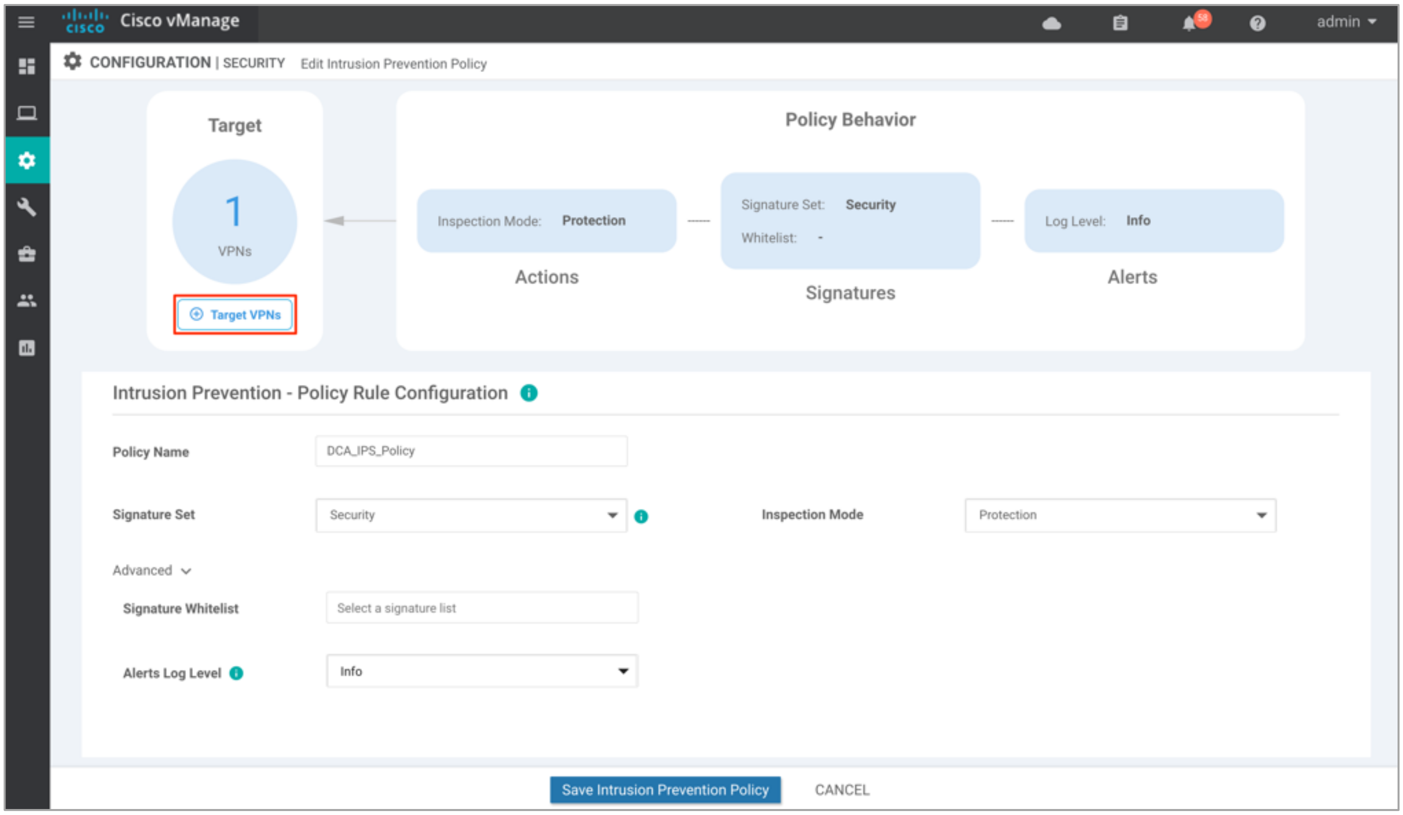
Advanced

Signature Whitelist

Alerts Log Level: Alert, Critical, Error, Warning (selected), Notice, Info

Inspection Mode: Protection

Step 12. Next, set the **Target VPNs.** Click on **Target VPNs** to add VPNs in the Target VPNs wizard.



Cisco vManage

CONFIGURATION | SECURITY Edit Intrusion Prevention Policy

Target: 1 VPNs

Policy Behavior

Inspection Mode: Protection — Actions

Signature Set: Security, Whitelist: - — Signatures

Log Level: Info — Alerts

Intrusion Prevention - Policy Rule Configuration

Policy Name: DCA_IPS_Policy

Signature Set: Security

Inspection Mode: Protection

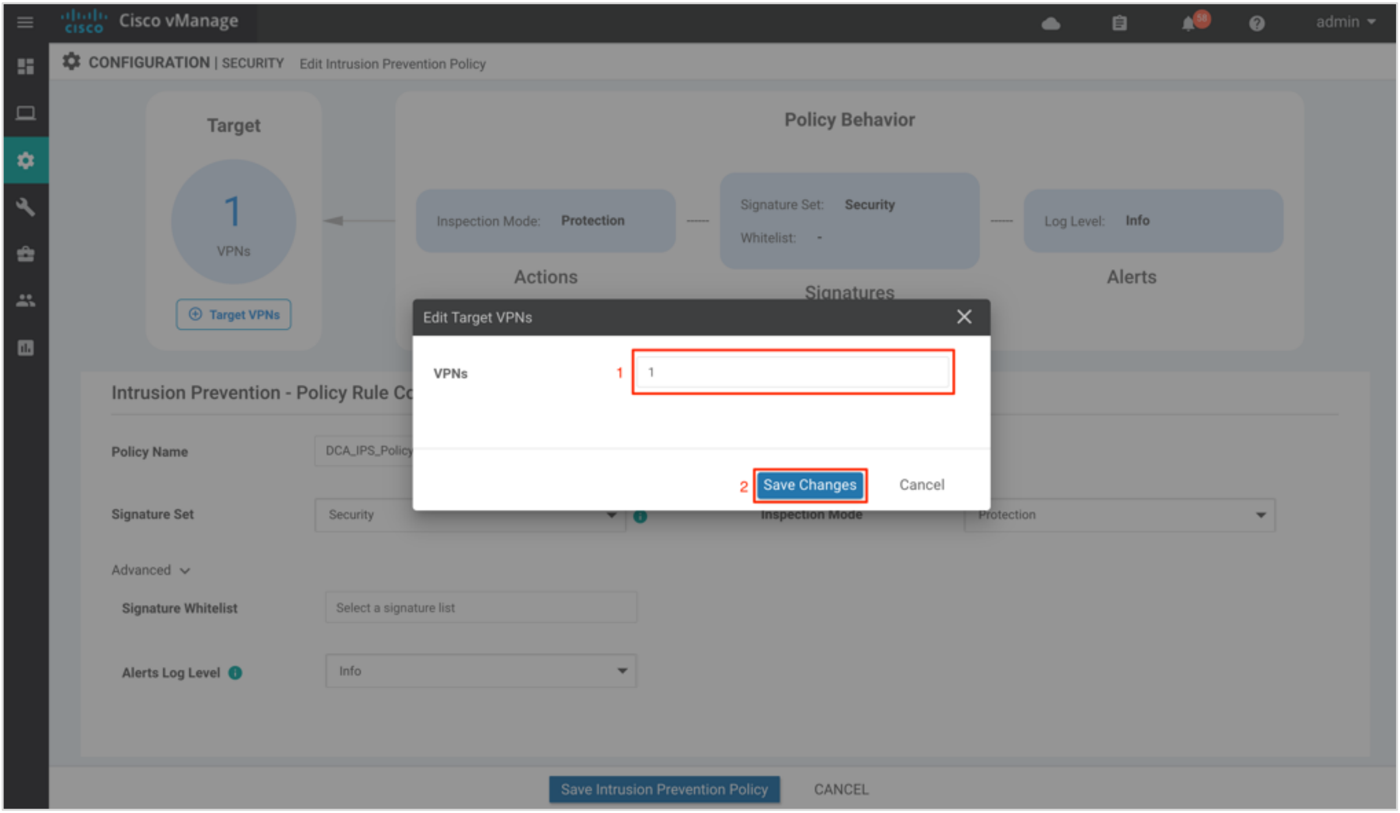
Advanced

Signature Whitelist: Select a signature list

Alerts Log Level: Info

Step 13. Within the tab on the right, enter the VPN number next to **VPNs**. You can enter a single, or multiple service-side VPN or VPN 0. If you wish to add more VPNs, separate each VPN with commas. Finally, click on **Save Changes**.

In this example, VPN label added within the tab is VPN 1.


Cisco vManage
admin
CONFIGURATION | SECURITY Edit Intrusion Prevention Policy
Target
1
VPNs
Target VPNs
Policy Behavior
Inspection Mode: Protection
Actions
Signature Set: Security
Whitelist: -
Signatures
Log Level: Info
Alerts
Intrusion Prevention - Policy Rule Co
Save Intrusion Prevention Policy
CANCEL

Edit Target VPNs

1 VPNs: 1

2 Save Changes Cancel

Policy Name: DCA_IPS_Policy

Signature Set: Security

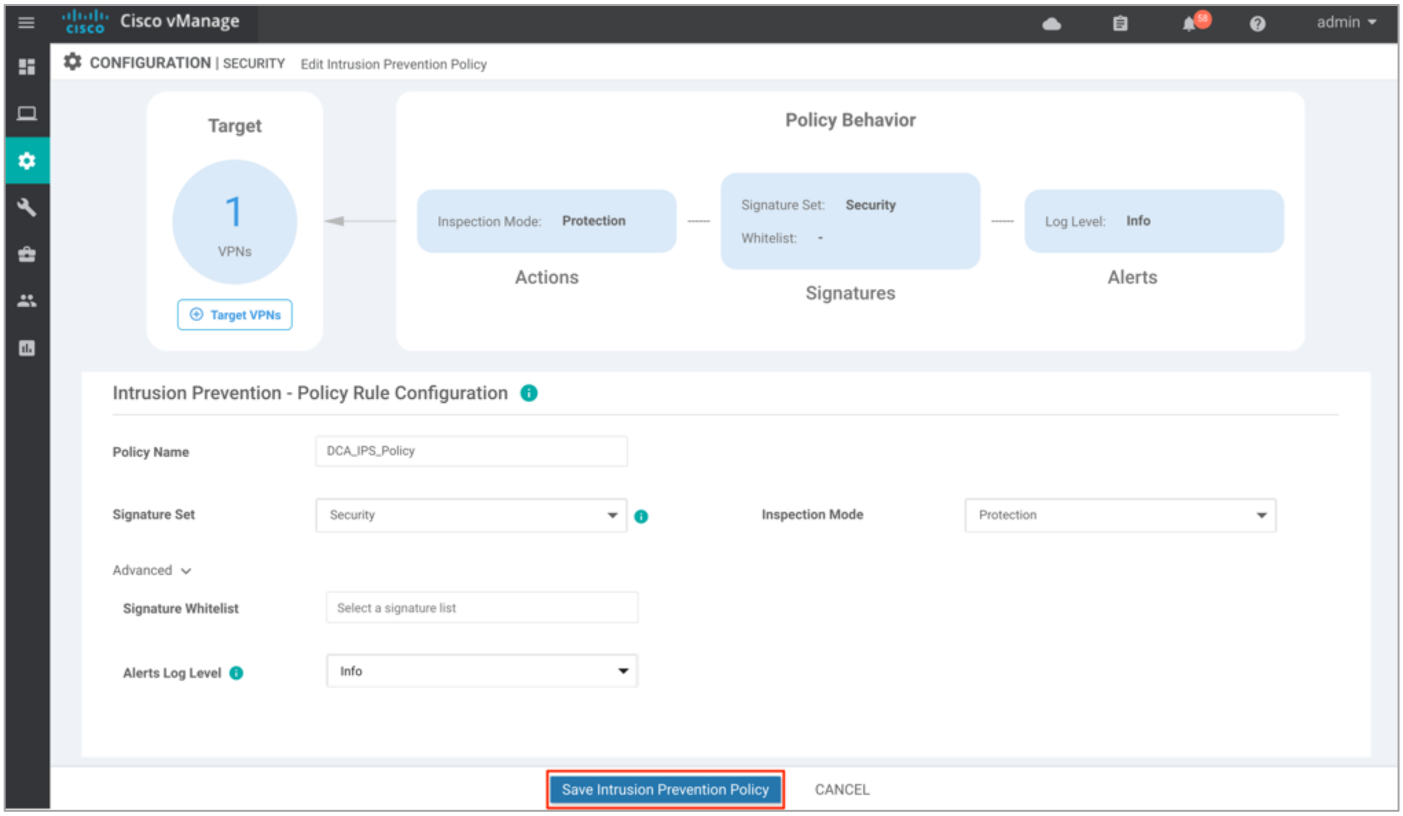
Inspection Mode: Protection

Advanced

Signature Whitelist: Select a signature list

Alerts Log Level: Info

Step 14. Click on **Save Intrusion Prevention Policy** to add the configured Intrusion Prevention security policy.



Intrusion Prevention - Policy Rule Configuration

Policy Name: DCA_IPS_Policy

Signature Set: Security

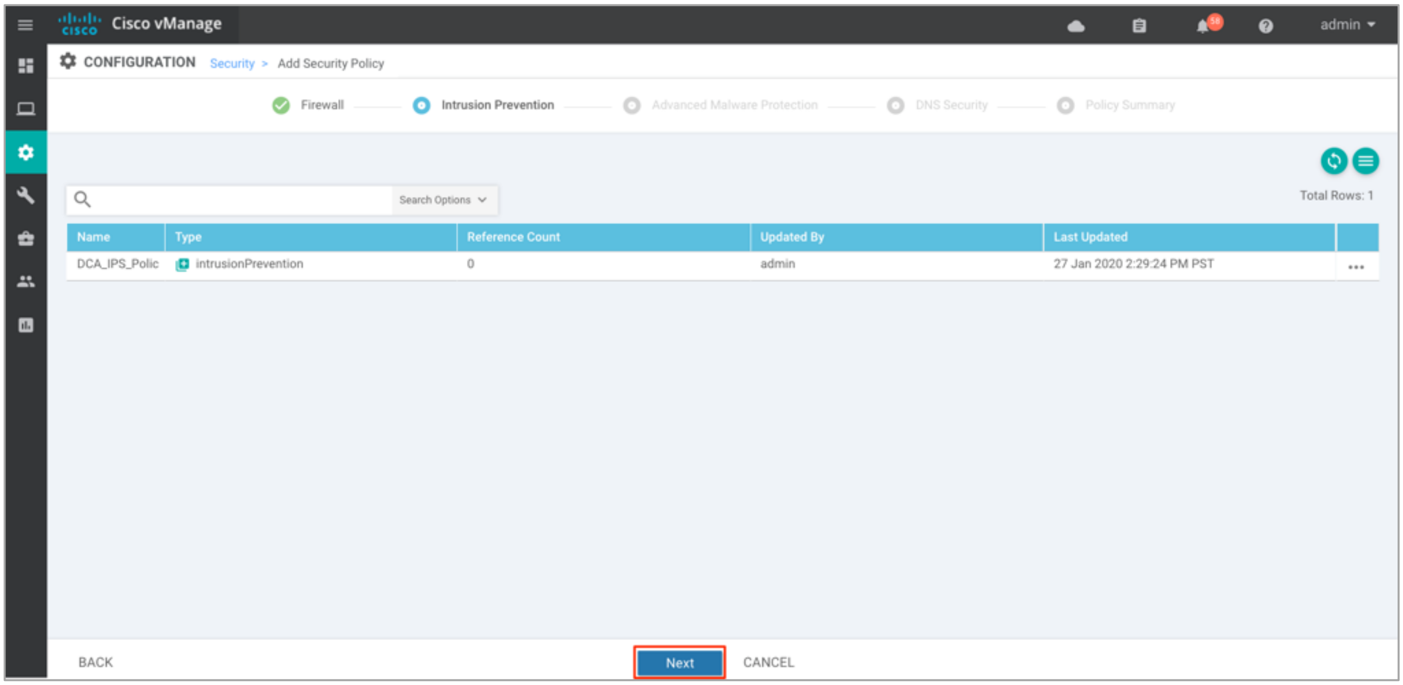
Inspection Mode: Protection

Advanced

Signature Whitelist: Select a signature list

Alerts Log Level: Info

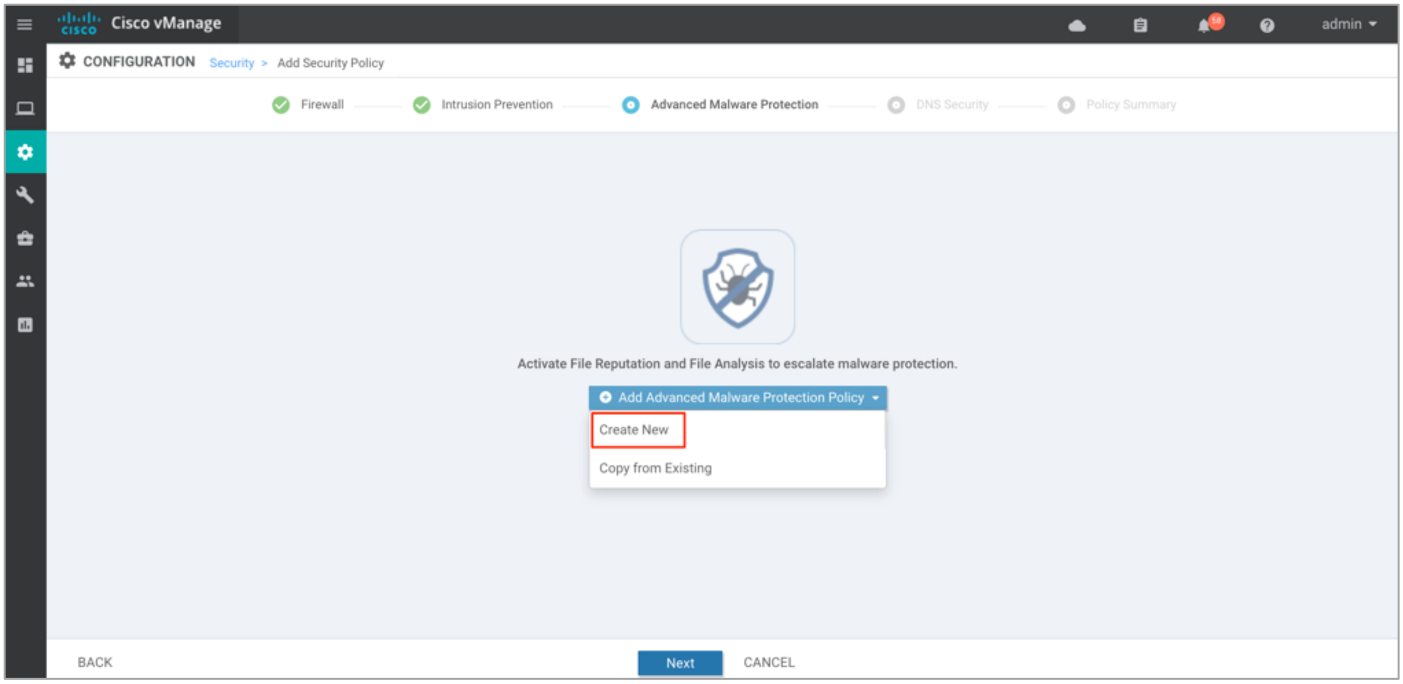
Step 15. Click **Next** as needed to select the **Advanced Malware Protection** tab.



Name	Type	Reference Count	Updated By	Last Updated
DCA_IPS_Polic	intrusionPrevention	0	admin	27 Jan 2020 2:29:24 PM PST

Procedure 3. Advanced Malware Protection Policy

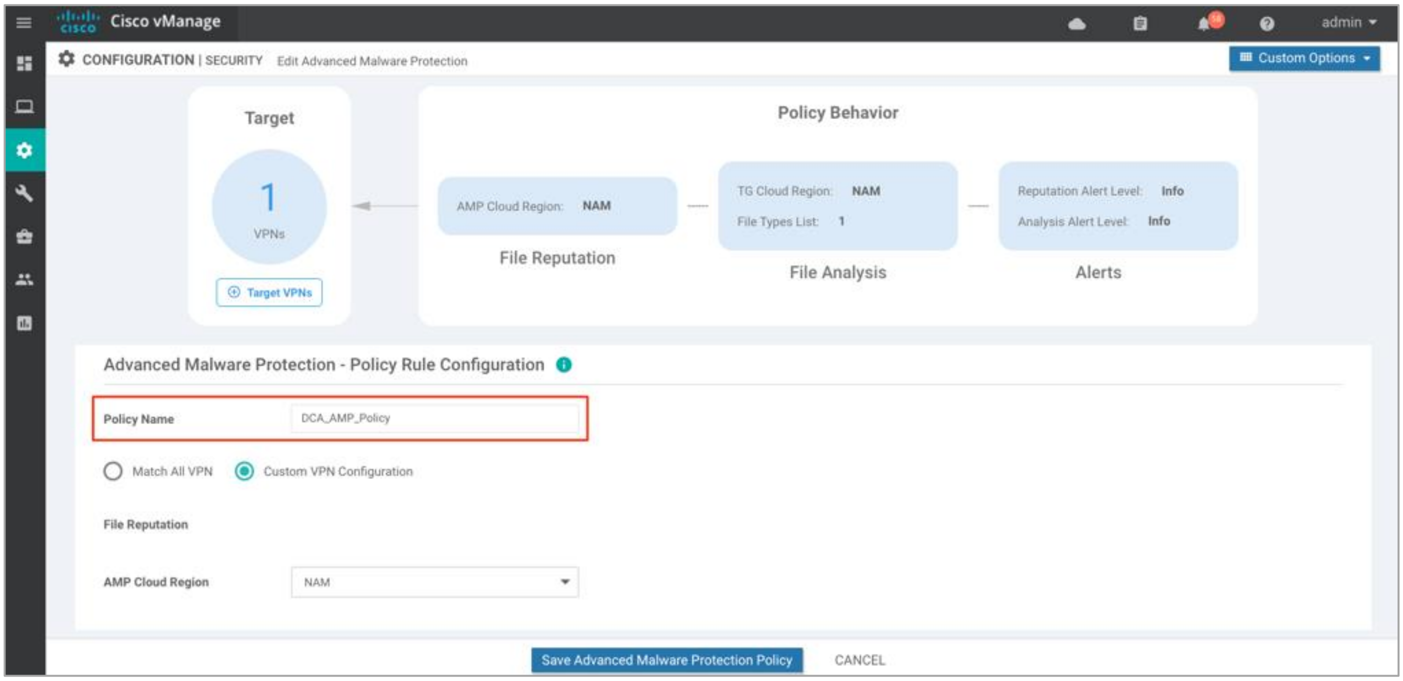
Step 1. In the Advanced Malware Protection tab, click the **Add Advanced Malware Protection Policy** drop-down and select **Create New**. Finally, click **Next**.



Activate File Reputation and File Analysis to escalate malware protection.

Note: You can also export the policy by clicking on **Copy from Existing** and click **Next.**

Step 2. In the **Policy Name** field, enter a name for the AMP policy. The name can be up to 128 characters and can contain only alphanumeric characters.



AMP Cloud Region: NAM

TG Cloud Region: NAM
File Types List: 1

Reputation Alert Level: Info
Analysis Alert Level: Info

Advanced Malware Protection - Policy Rule Configuration

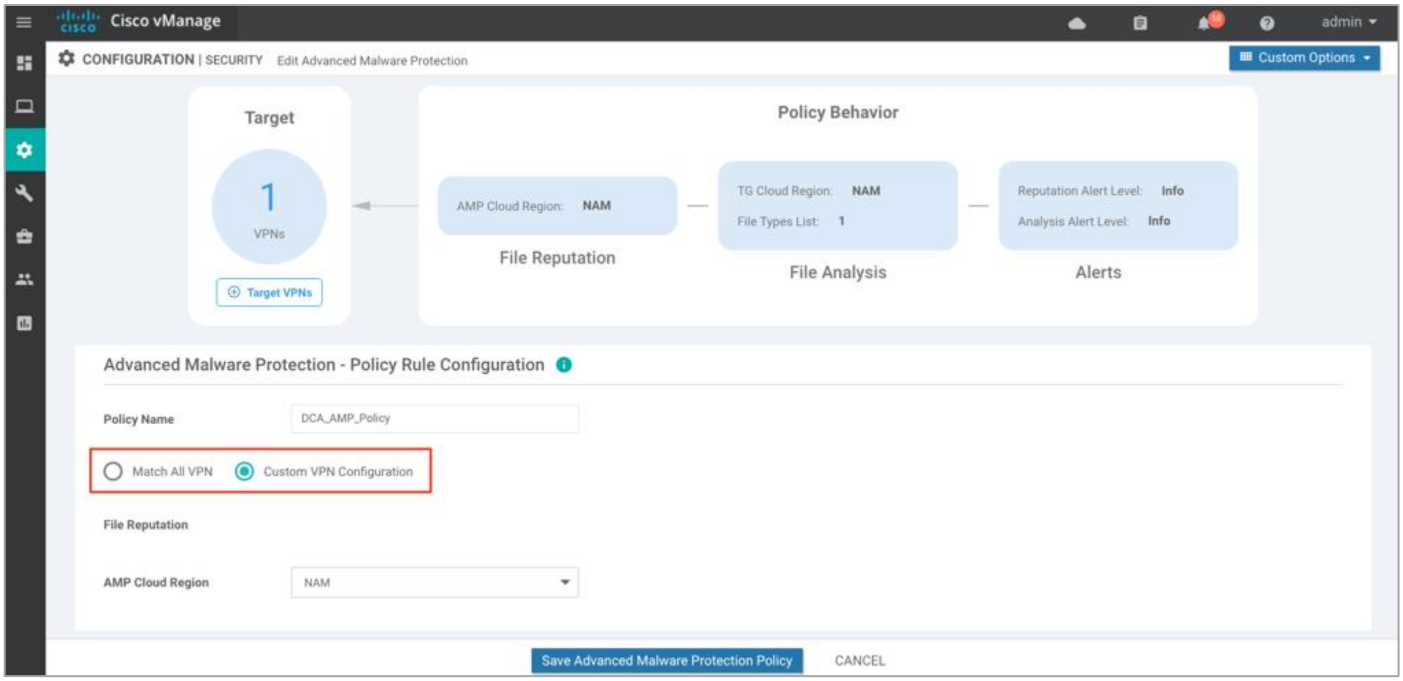
Policy Name: DCA_AMP_Policy

○ Match All VPN ● Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

Step 3. Select either **Match All VPN** to apply the policy to all VPNs or choose **Custom VPN Configuration** to input the specific VPNs.



AMP Cloud Region: NAM

TG Cloud Region: NAM
File Types List: 1

Reputation Alert Level: Info
Analysis Alert Level: Info

Advanced Malware Protection - Policy Rule Configuration

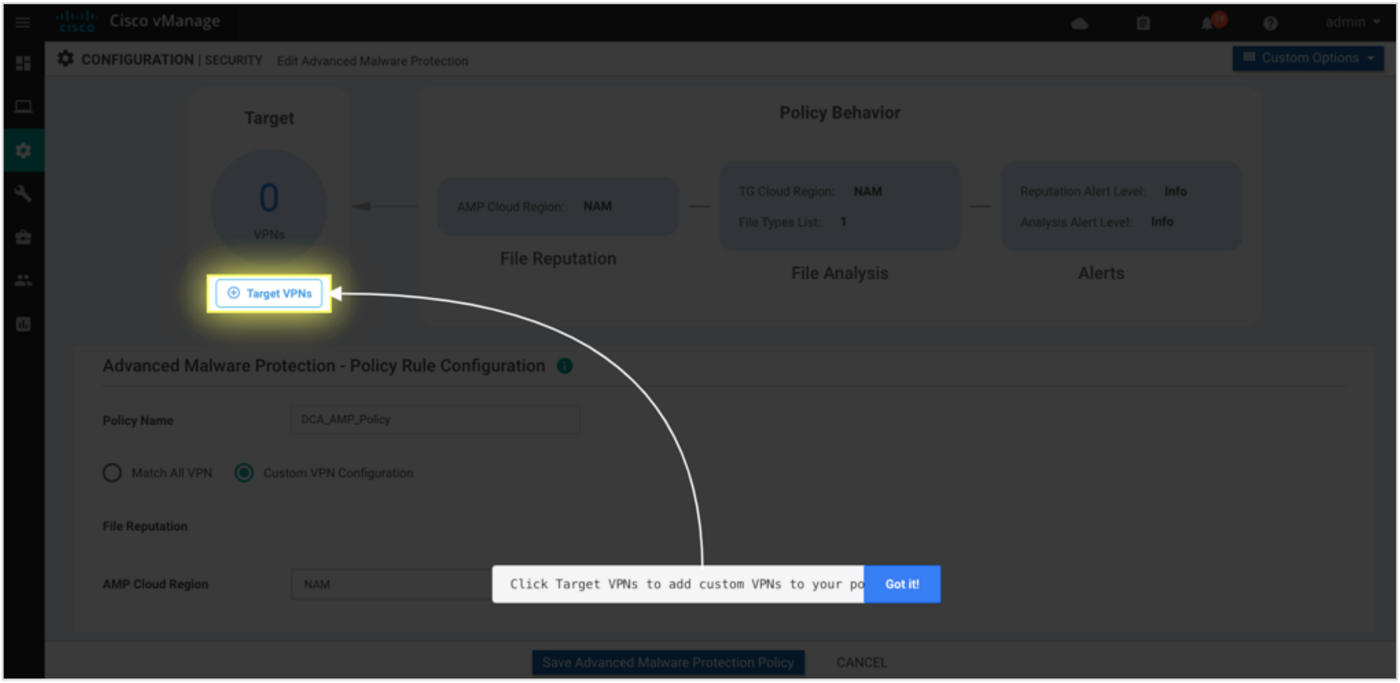
Policy Name: DCA_AMP_Policy

○ Match All VPN ● Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

If you choose **Custom VPN Configuration**, you are redirected to the page below.



Advanced Malware Protection - Policy Rule Configuration

Policy Name: DCA_AMP_Policy

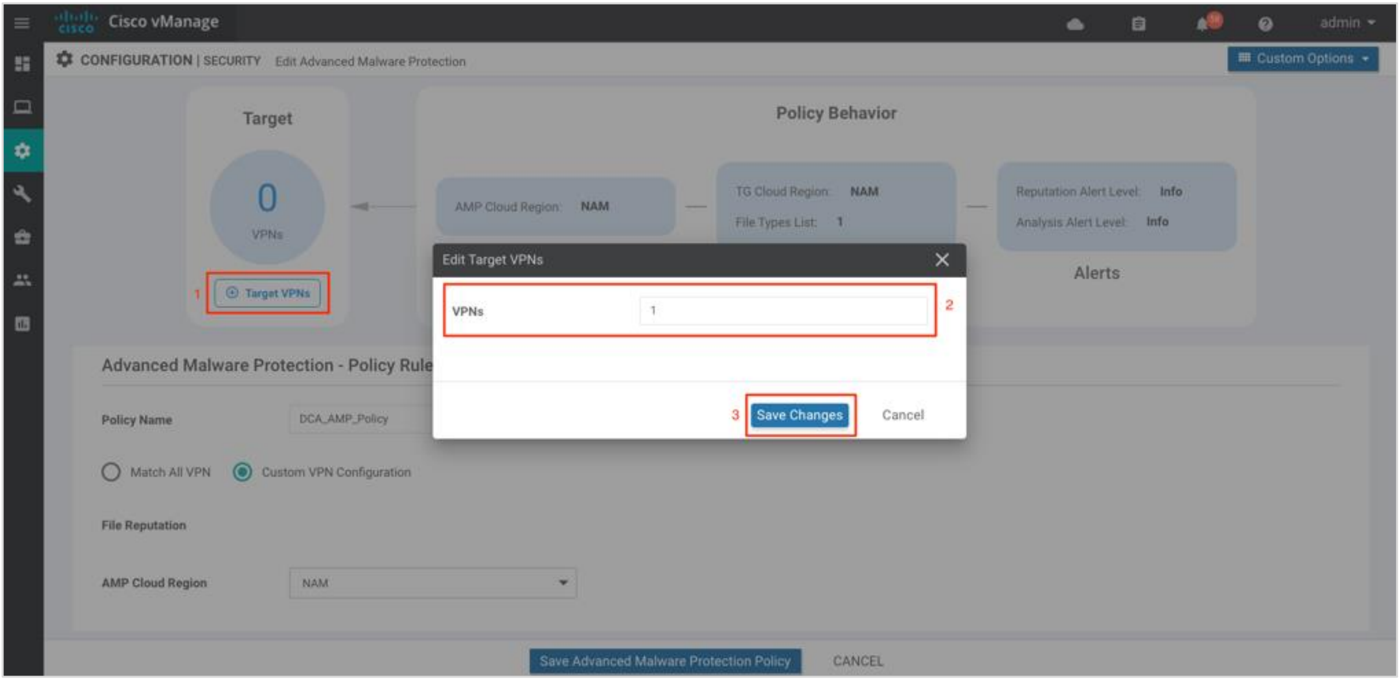
○ Match All VPN ● Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

Click Target VPNs to add custom VPNs to your po

Step 4. Click on **Target VPNs**, and enter the VPN ID against **VPNs**. Finally, click on **Save Changes**.



VPNs: 1

Advanced Malware Protection - Policy Rule

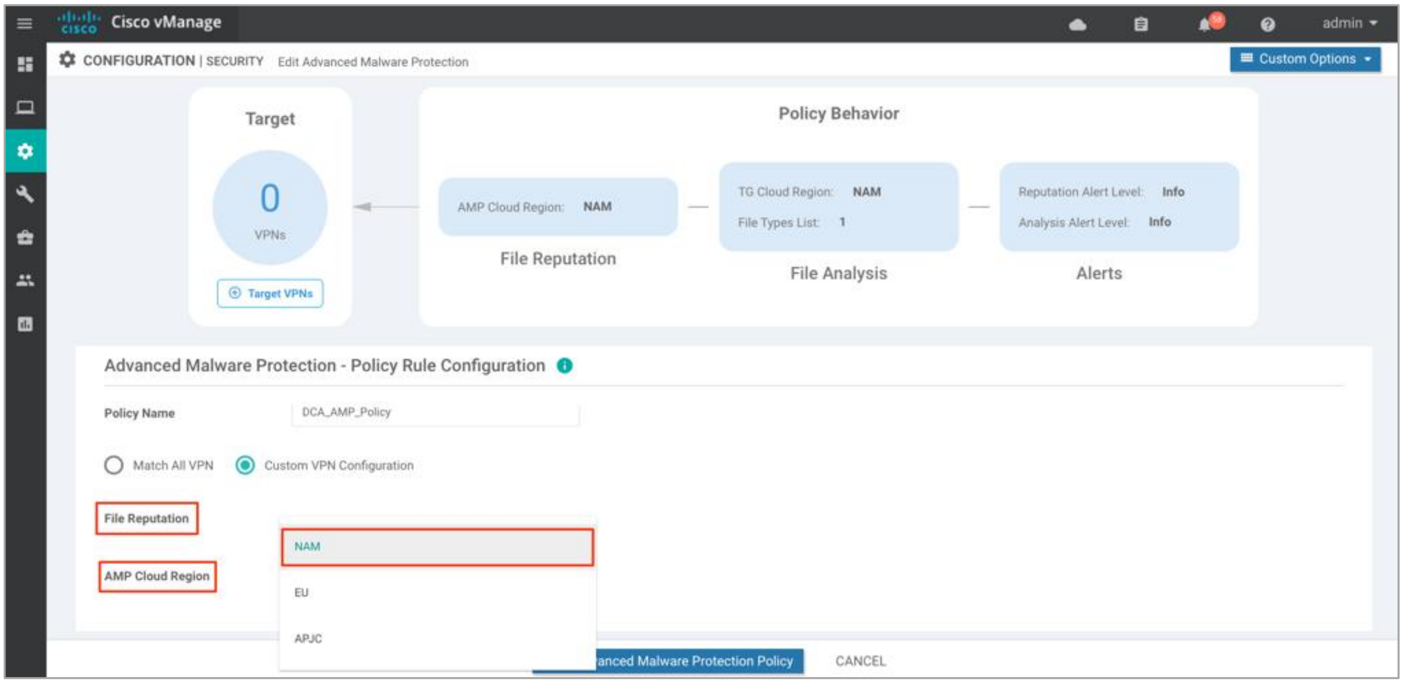
Policy Name: DCA_AMP_Policy

○ Match All VPN ● Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

Step 5. Within **File Reputation**, select a global region from the **AMP Cloud Region** drop down.



AMP Cloud Region: NAM

TG Cloud Region: NAM
File Types List: 1

Reputation Alert Level: Info
Analysis Alert Level: Info

Advanced Malware Protection - Policy Rule Configuration

Policy Name: DCA_AMP_Policy

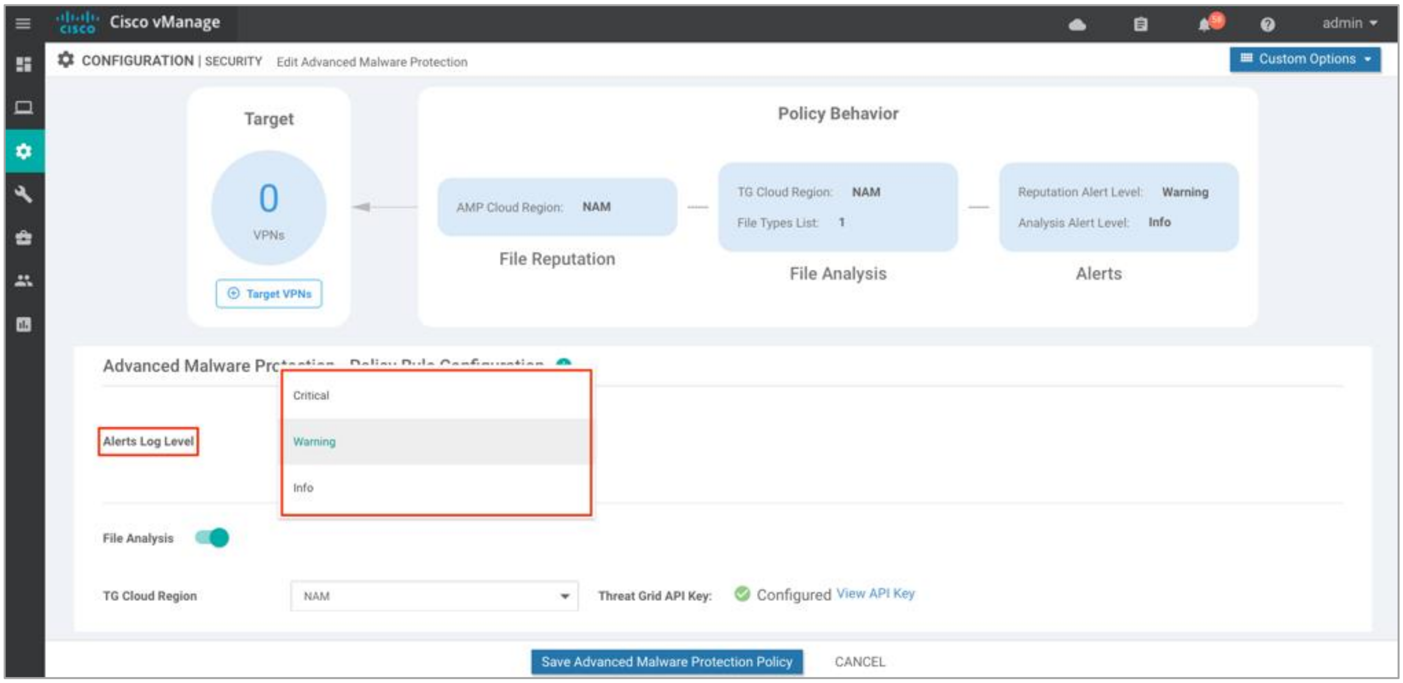
○ Match All VPN ● Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

- NAM
- EU
- APJC

Step 6. Within the **Alerts Log Level** drop down, select one among the three severity levels – **Critical**, **Warning** or **Info**. It is ideal to stick to the **Warning** severity level for balance of load and information at production site. The **Info** severity level generates multiple notifications and can affect system performance and hence may not be ideal for real-time traffic.



AMP Cloud Region: NAM

TG Cloud Region: NAM
File Types List: 1

Reputation Alert Level: Warning
Analysis Alert Level: Info

Advanced Malware Protection - Policy Rule Configuration

Alerts Log Level: Warning

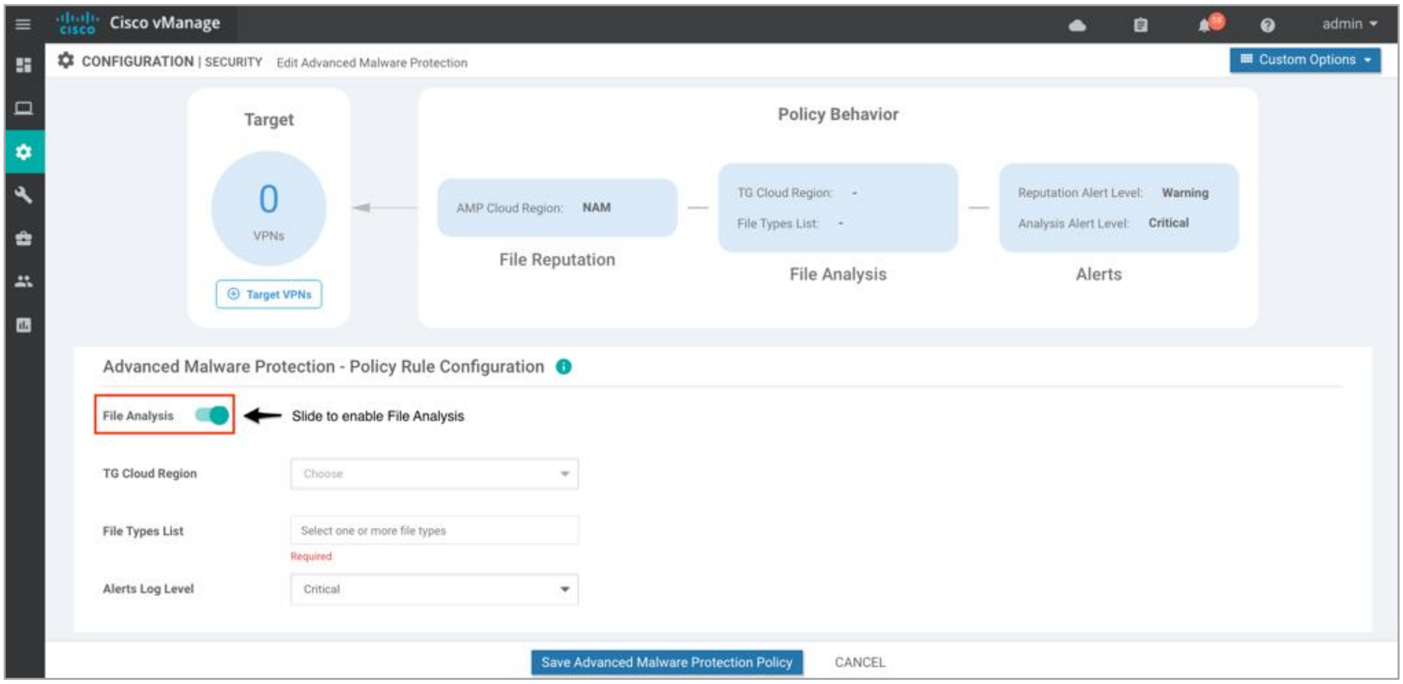
- Critical
- Warning
- Info

File Analysis: ON

TG Cloud Region: NAM

Threat Grid API Key: ✓ Configured

Step 7. Click on **File Analysis** and slide the tab.


Cisco vManage
admin
CONFIGURATION | SECURITY Edit Advanced Malware Protection
Custom Options
Target
0
VPNs
Target VPNs
Policy Behavior
File Reputation
File Analysis
Alerts
Slide to enable File Analysis
Save Advanced Malware Protection Policy
CANCEL

AMP Cloud Region: NAM

TG Cloud Region: -

File Types List: -

Reputation Alert Level: Warning

Analysis Alert Level: Critical

Advanced Malware Protection - Policy Rule Configuration

File Analysis

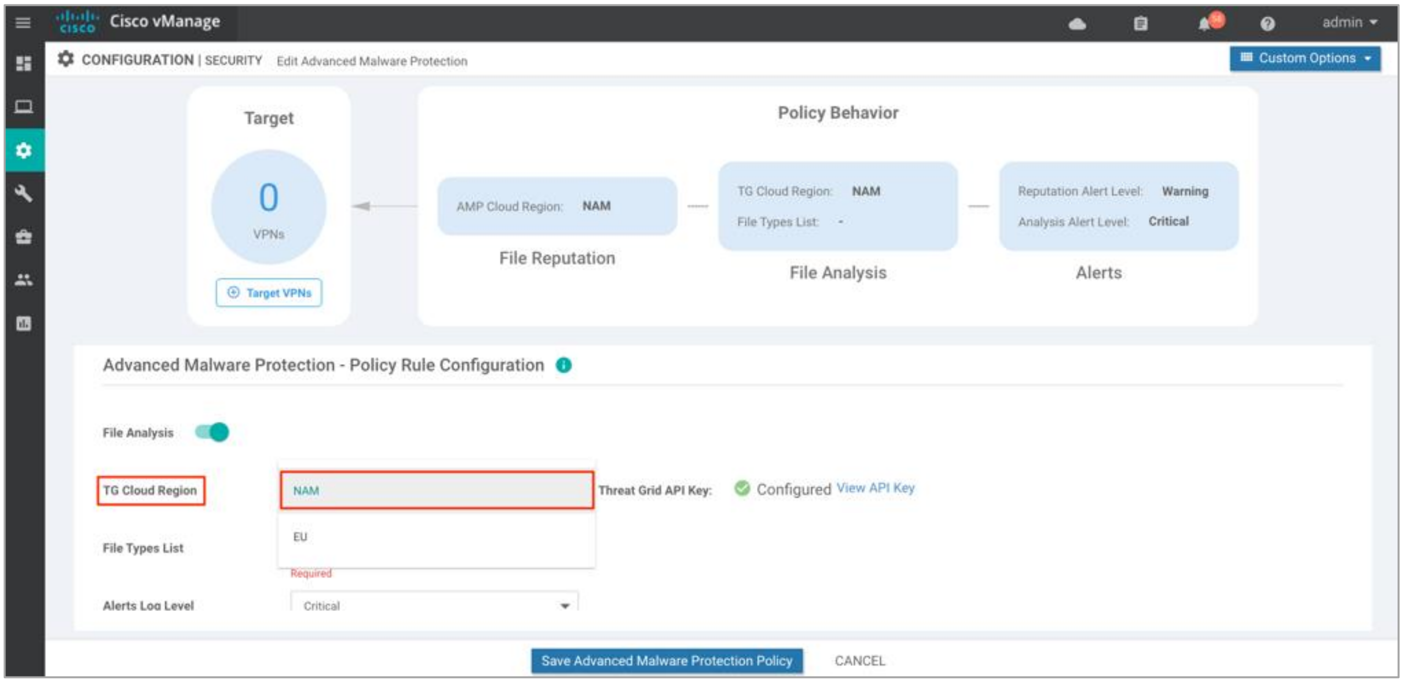
TG Cloud Region: Choose

File Types List: Select one or more file types (Required)

Alerts Log Level: Critical

Note: To enable Threat Grid, please make sure you have the procured appropriate DNA subscription license.

Step 8. From the **TG Cloud Region** dropdown, select a global region.



AMP Cloud Region: NAM

TG Cloud Region: NAM

File Types List: -

Reputation Alert Level: Warning

Analysis Alert Level: Critical

Advanced Malware Protection - Policy Rule Configuration

File Analysis

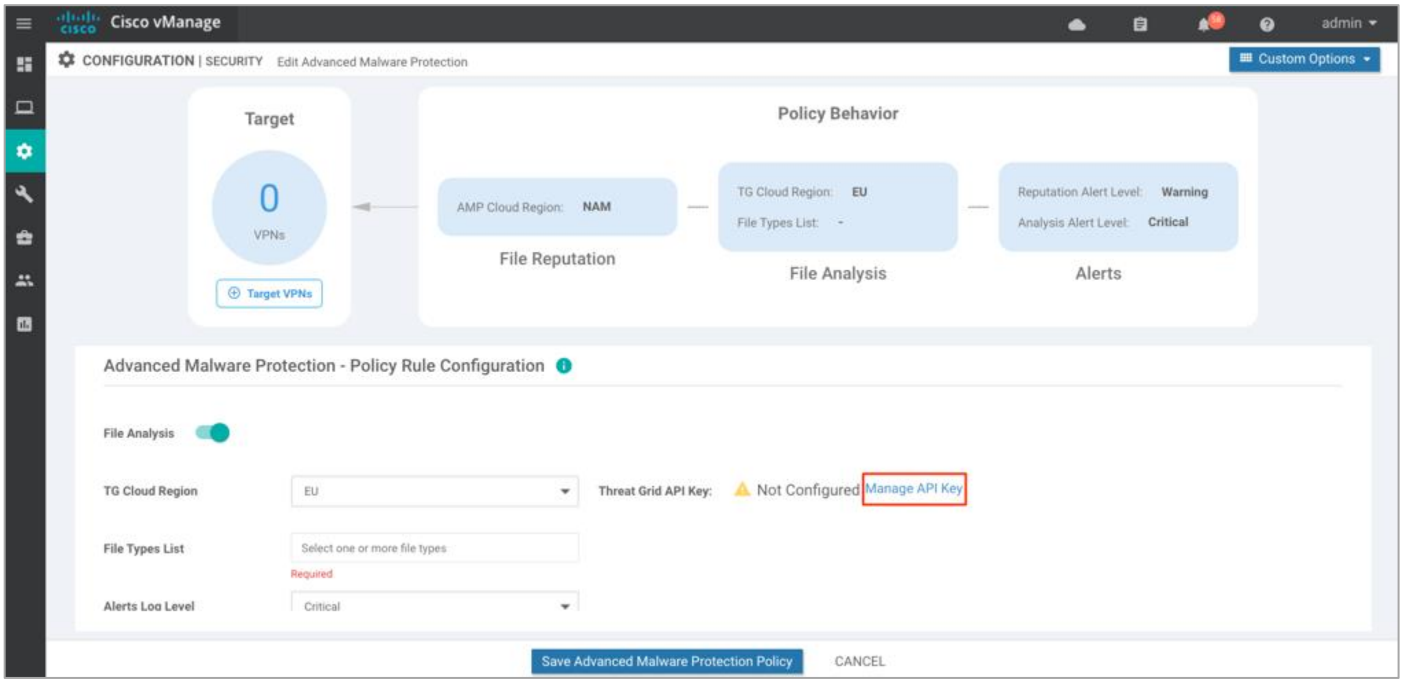
TG Cloud Region: NAM / EU

Threat Grid API Key: Configured

File Types List: Required

Alerts Log Level: Critical

Step 9. If the Thread Grid API key was not previously added, click on **Manage API Key.**



AMP Cloud Region: NAM

TG Cloud Region: EU

File Types List: -

Reputation Alert Level: Warning

Analysis Alert Level: Critical

Advanced Malware Protection - Policy Rule Configuration

File Analysis

TG Cloud Region: EU

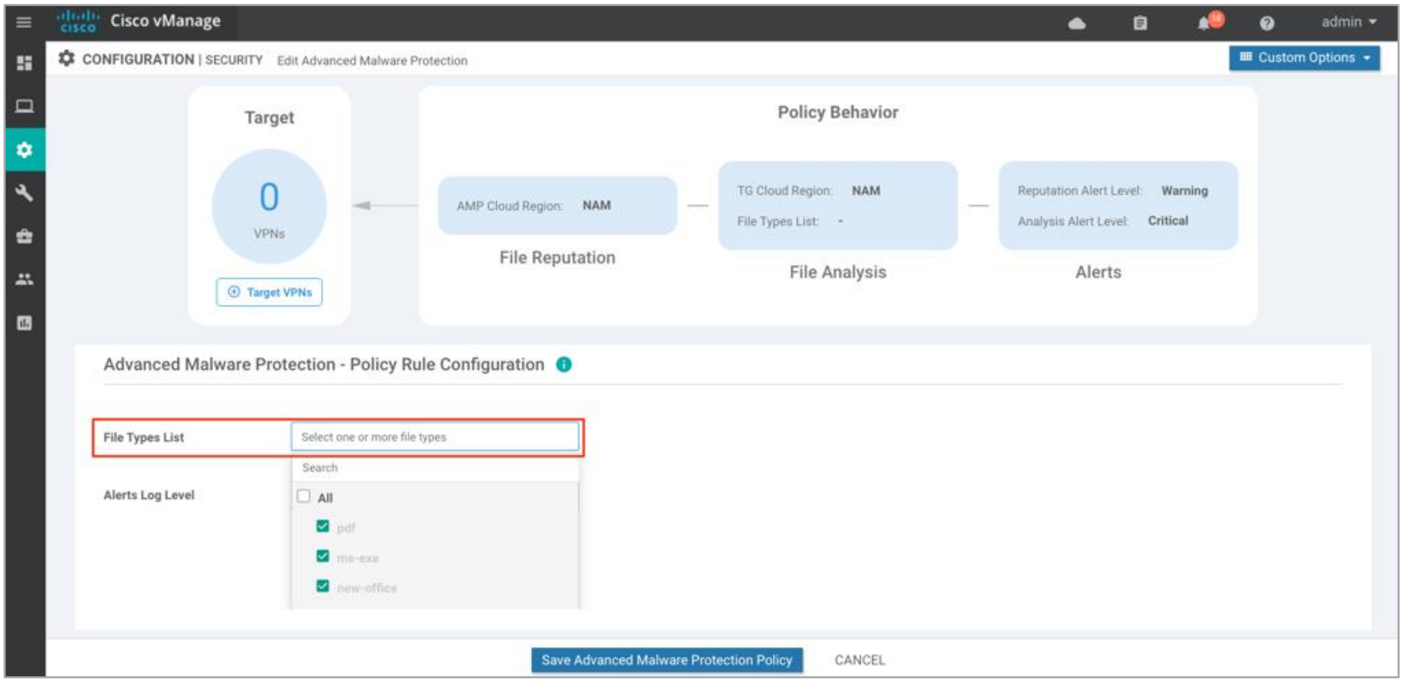
Threat Grid API Key: Not Configured

File Types List: Select one or more file types

Required

Alerts Log Level: Critical

Step 10. Within **File Types List**, select the file types to be analyzed.



AMP Cloud Region: NAM

TG Cloud Region: NAM

File Types List: -

Reputation Alert Level: Warning

Analysis Alert Level: Critical

Advanced Malware Protection - Policy Rule Configuration

File Types List: Select one or more file types

Alerts Log Level

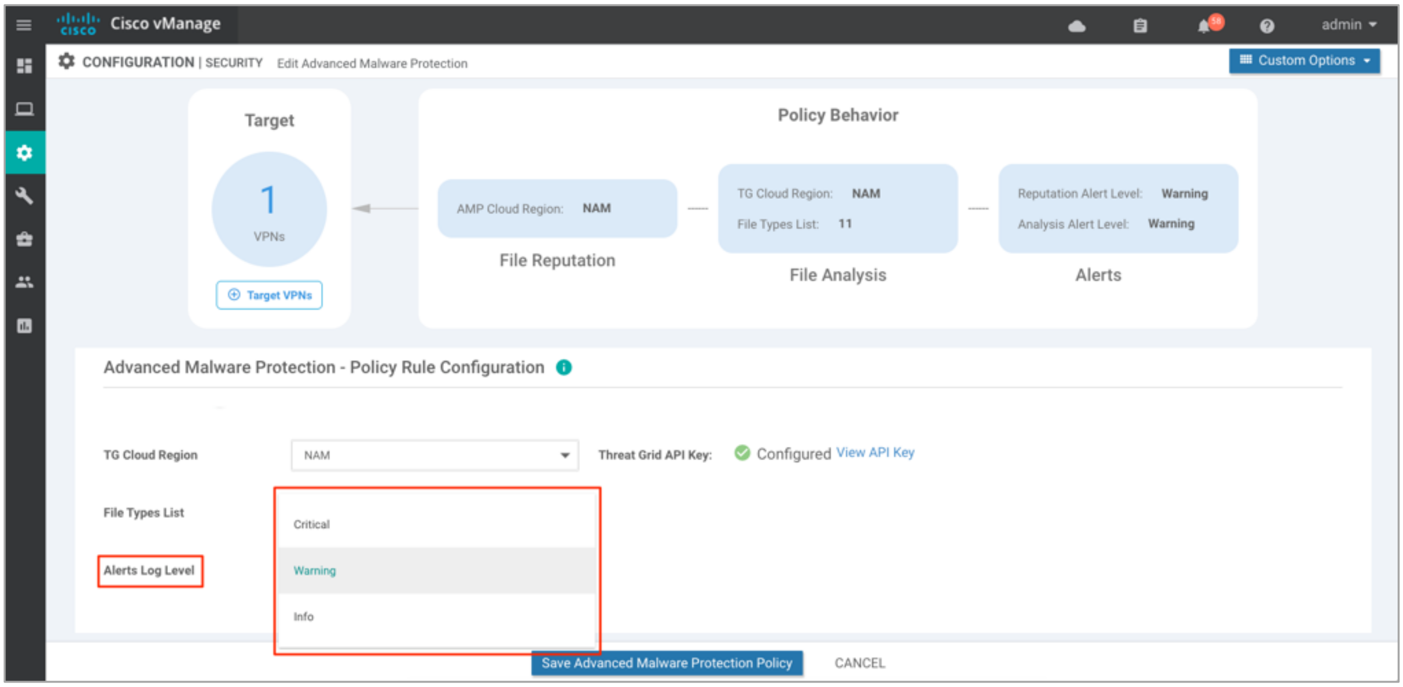
□ All

☑ pdf

☑ ms-exe

☑ new-office

Step 11. From the **Alerts Log Level** drop down, select a severity level. (Critical, Warning or Info) Just as explained for File Reputation, It is ideal to stick to **Warning** severity level for balance of load and information at production site.



Advanced Malware Protection - Policy Rule Configuration

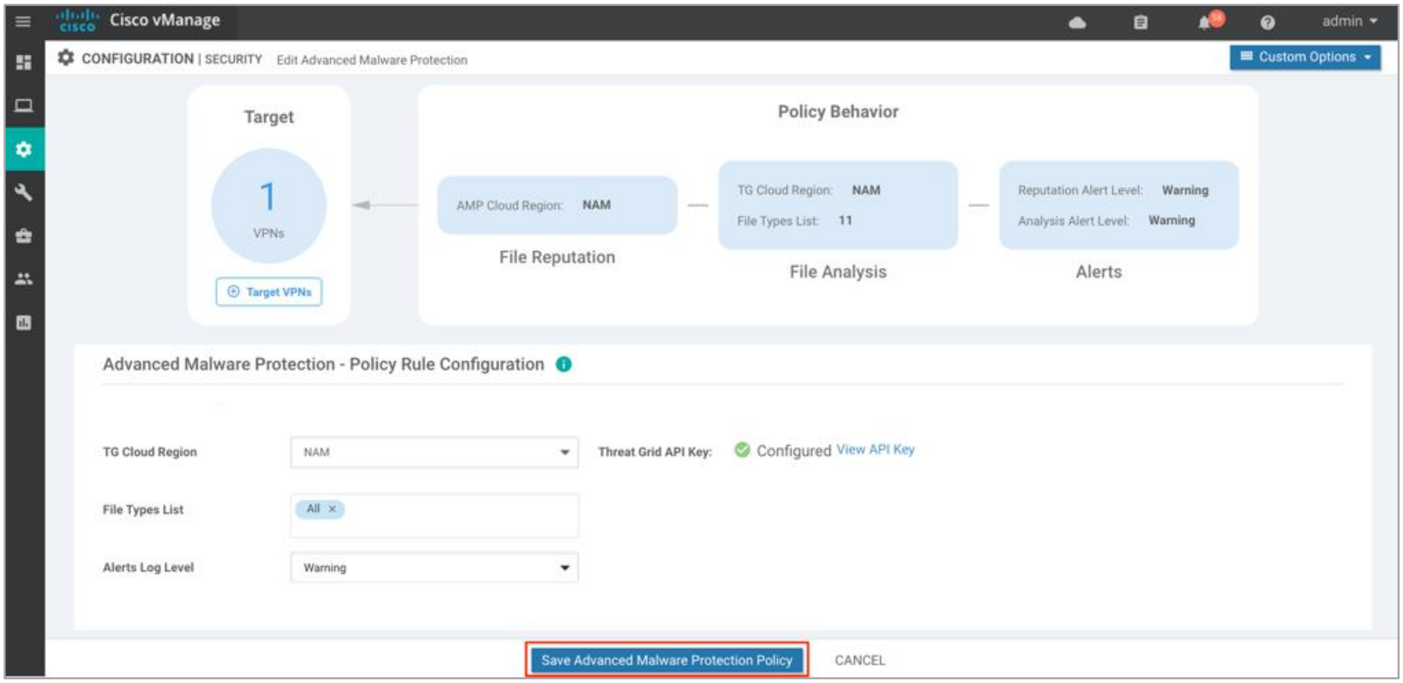
TG Cloud Region: NAM

Threat Grid API Key: Configured View API Key

File Types List

Alerts Log Level

Step 12. Click on **Save Advanced Malware Protection Policy**.



Advanced Malware Protection - Policy Rule Configuration

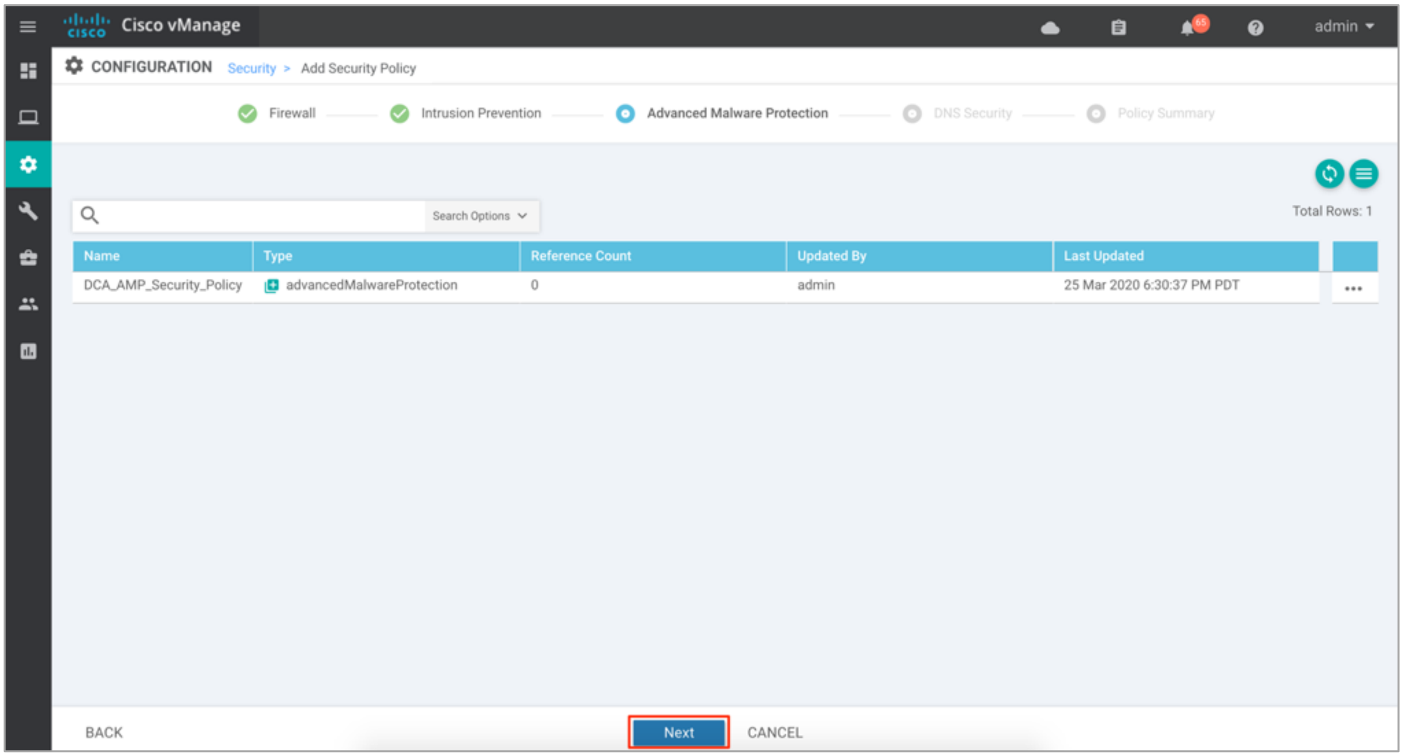
TG Cloud Region: NAM

Threat Grid API Key: Configured View API Key

File Types List: All

Alerts Log Level: Warning

Step 13. Click **Next** to configure DNS/ Web-Layer security policy.

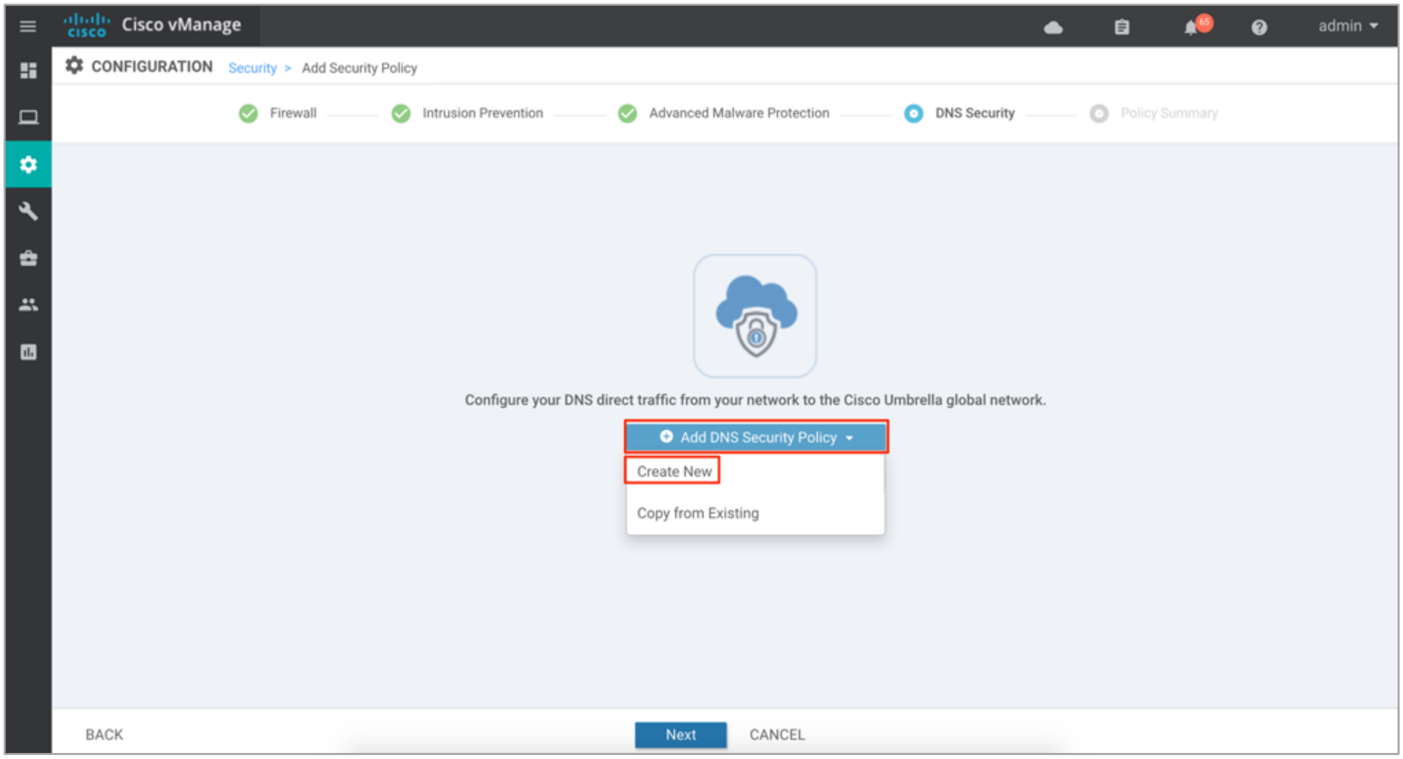


Name	Type	Reference Count	Updated By	Last Updated
DCA_AMP_Security_Policy	advancedMalwareProtection	0	admin	25 Mar 2020 6:30:37 PM PDT

Procedure 4. DNS/ Web-layer Security Policy

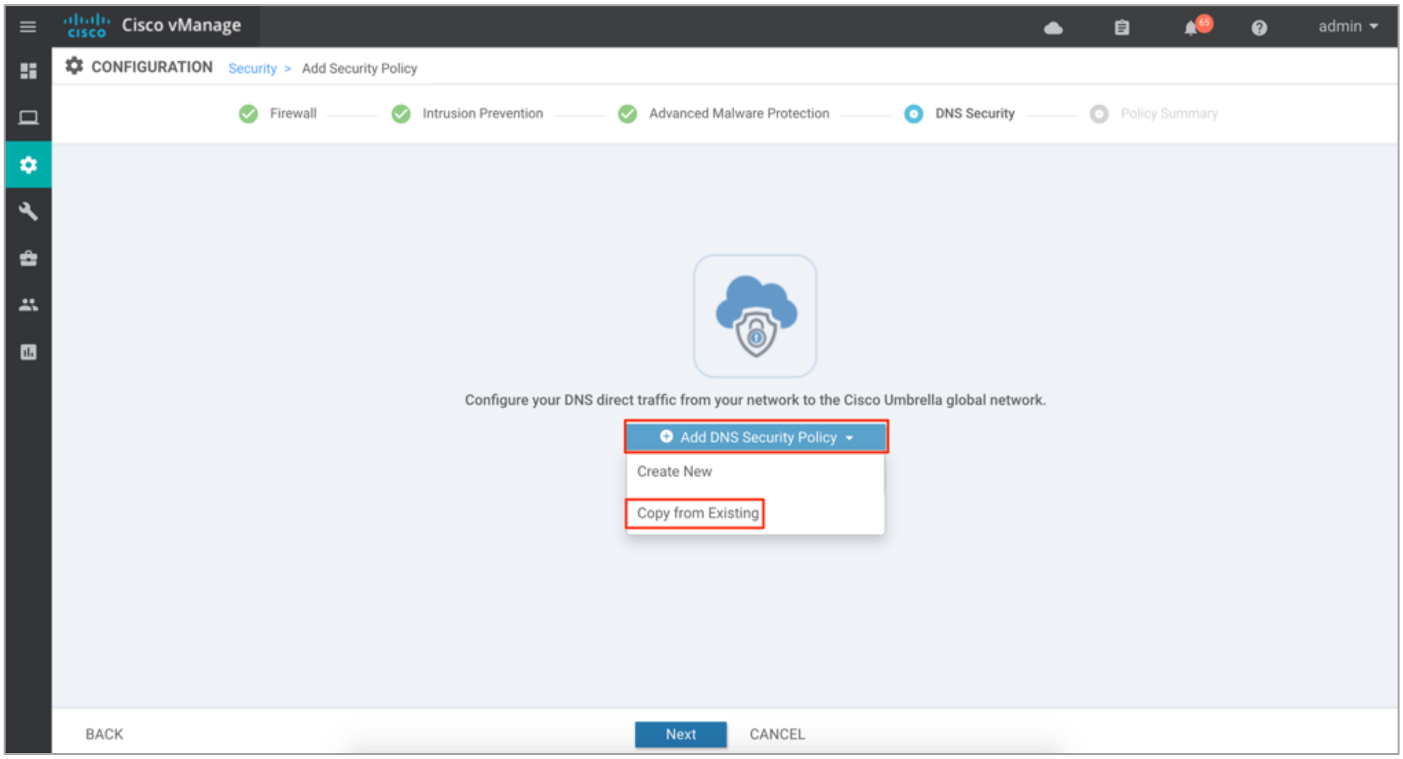
The following steps enable DNS Security policy with Umbrella Integration.

Step 1. In the Security Policy wizard, click on **Add DNS Security Policy** and select **Create New** to add a new DNS/Web-Layer security policy. Finally, click **Next.**



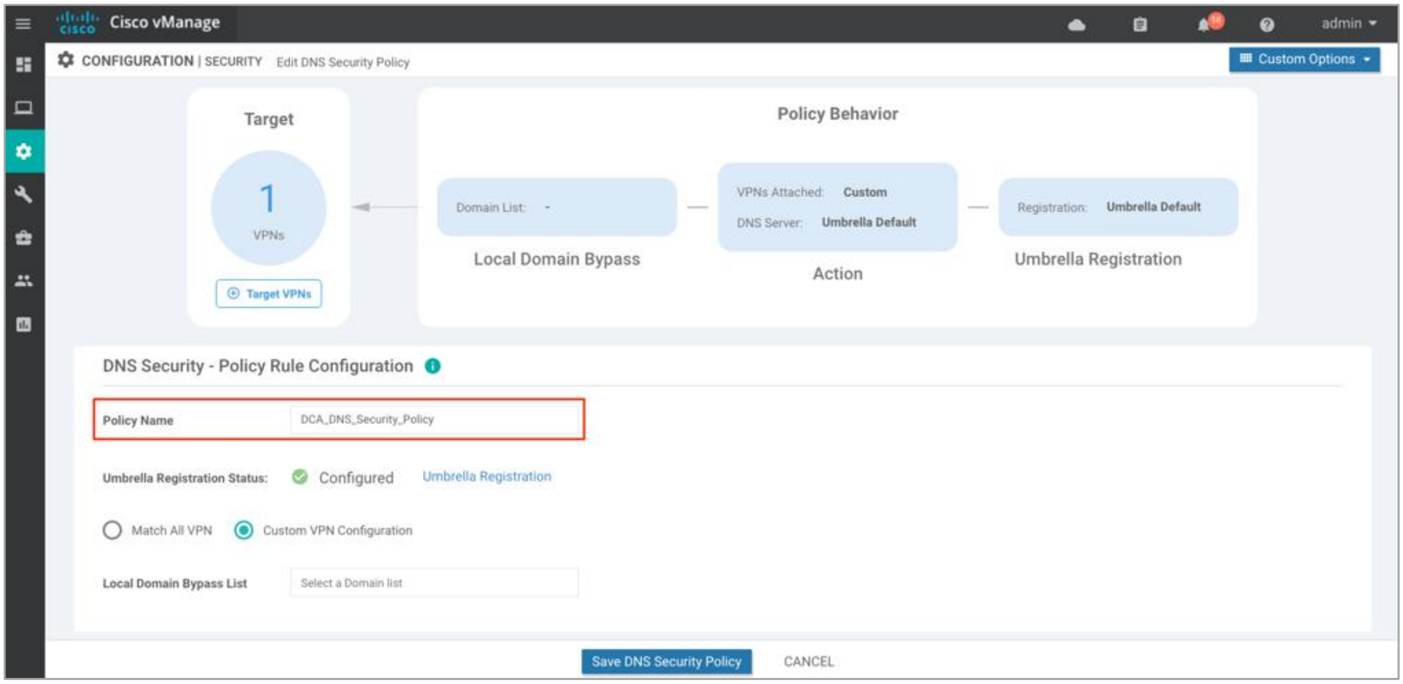
Configure your DNS direct traffic from your network to the Cisco Umbrella global network.

Note: Alternatively, click on **Copy from Existing** to export an existing DNS Security Policy and click **Next**.



Configure your DNS direct traffic from your network to the Cisco Umbrella global network.

Step 2. Enter a policy name in the **Policy Name** field.



DNS Security - Policy Rule Configuration

Policy Name: DCA_DNS_Security_Policy

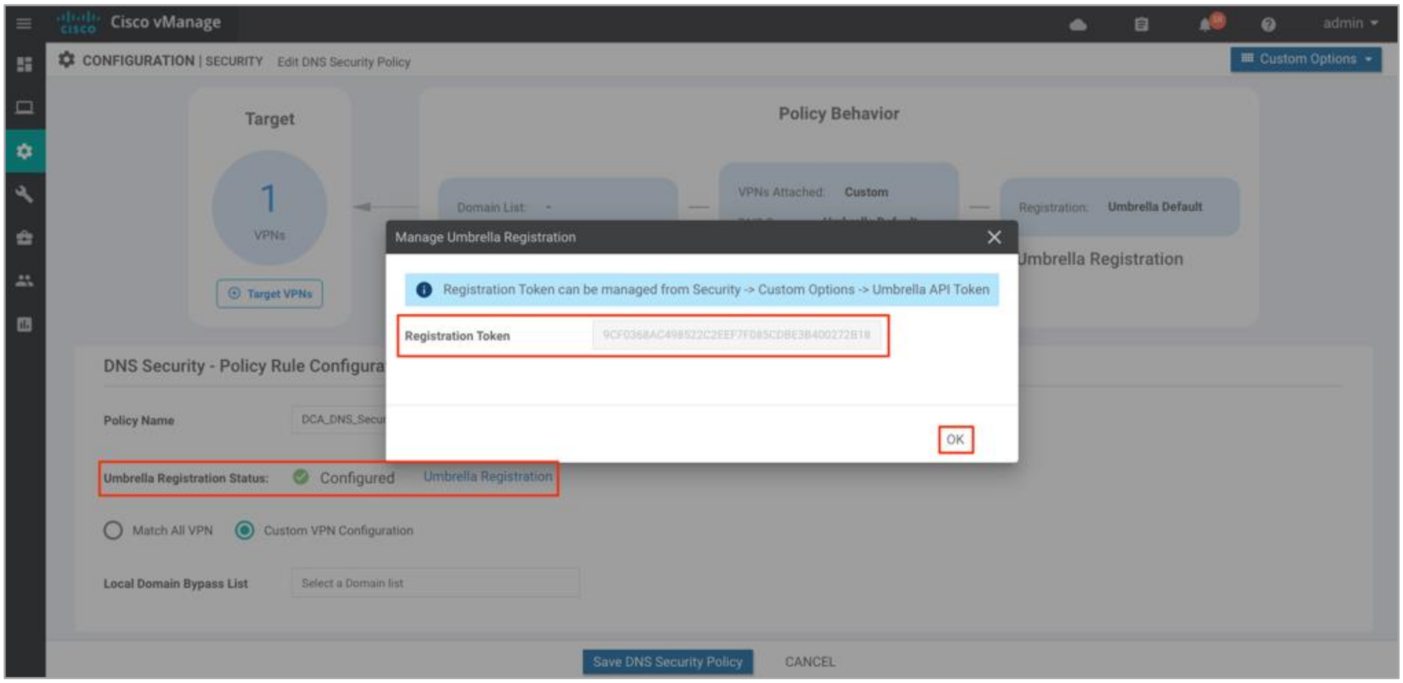
Umbrella Registration Status: Configured

○ Match All VPN ● Custom VPN Configuration

Local Domain Bypass List: Select a Domain list

Step 3. The **Umbrella Registration Status** displays the status about the API Token configuration.

Note: If the Umbrella Registration Status displays as Not Configured, then click on **Manage Umbrella** Registration and add **Registration Token**.



Manage Umbrella Registration

Registration Token can be managed from Security -> Custom Options -> Umbrella API Token

Registration Token 9CF0368AC498522C2EEF7F085CDBE38400272B18

OK

DNS Security - Policy Rule Configura

Policy Name DCA_DNS_Secur

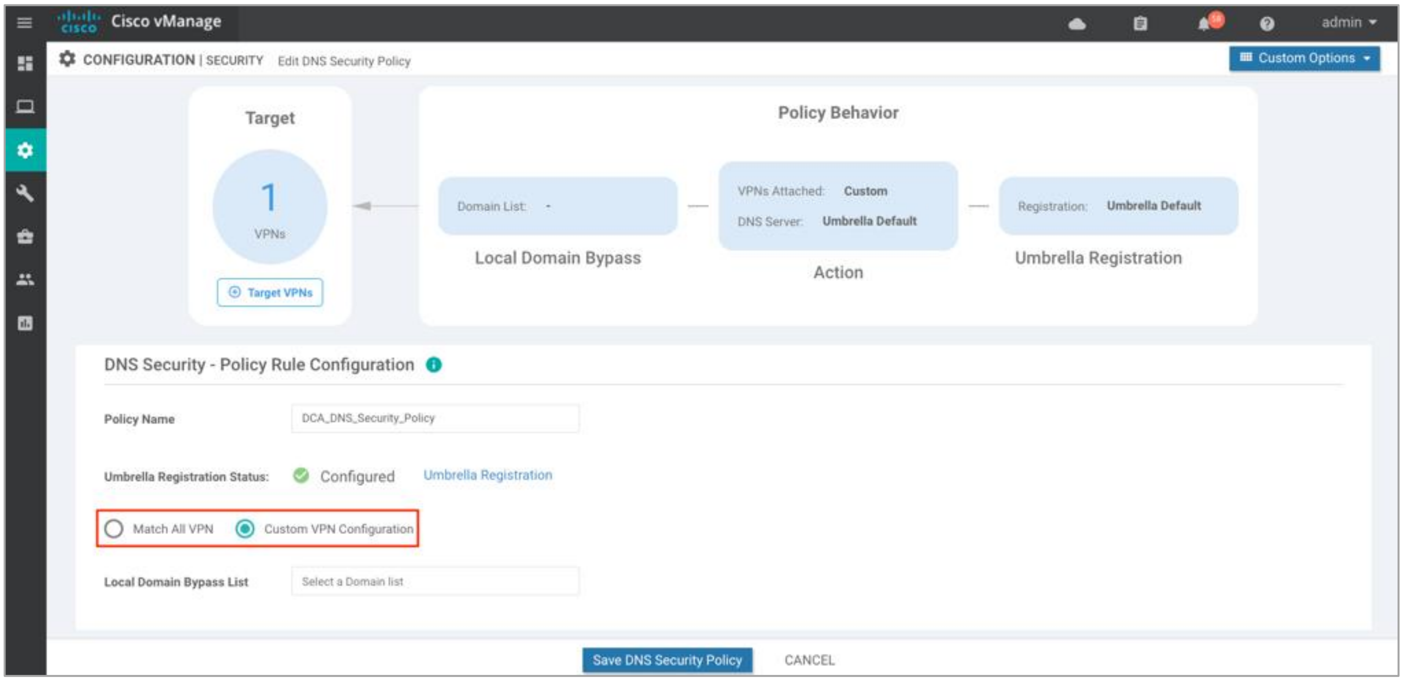
Umbrella Registration Status: Configured Umbrella Registration

○ Match All VPN ● Custom VPN Configuration

Local Domain Bypass List Select a Domain list

Save DNS Security Policy CANCEL

Step 4. Select either **Match All VPN** to keep the same configuration for all the available VPNs or select **Custom VPN Configuration** to add **Target VPNs** to your policy.



DNS Security - Policy Rule Configuration

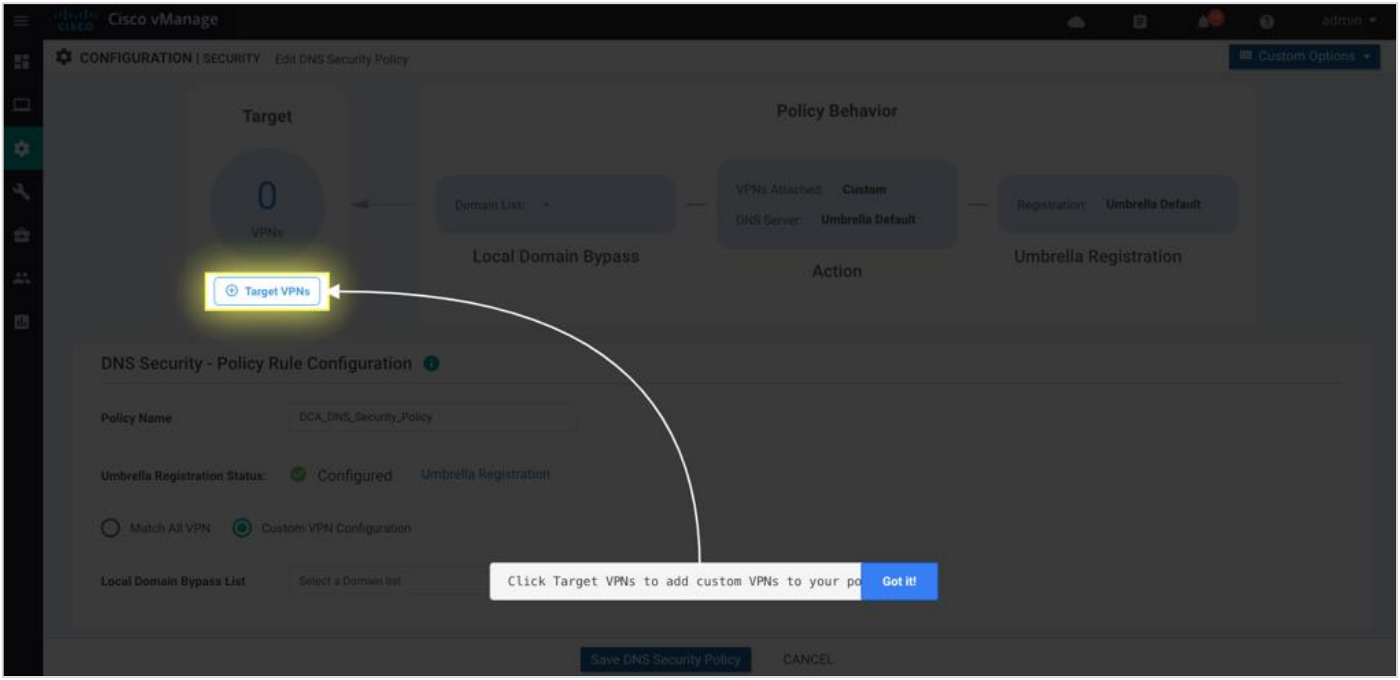
Policy Name DCA_DNS_Security_Policy

Umbrella Registration Status: Configured Umbrella Registration

○ Match All VPN ● Custom VPN Configuration

Local Domain Bypass List Select a Domain list

Save DNS Security Policy CANCEL



DNS Security - Policy Rule Configuration

Policy Name: DCA_DNS_Security_Policy

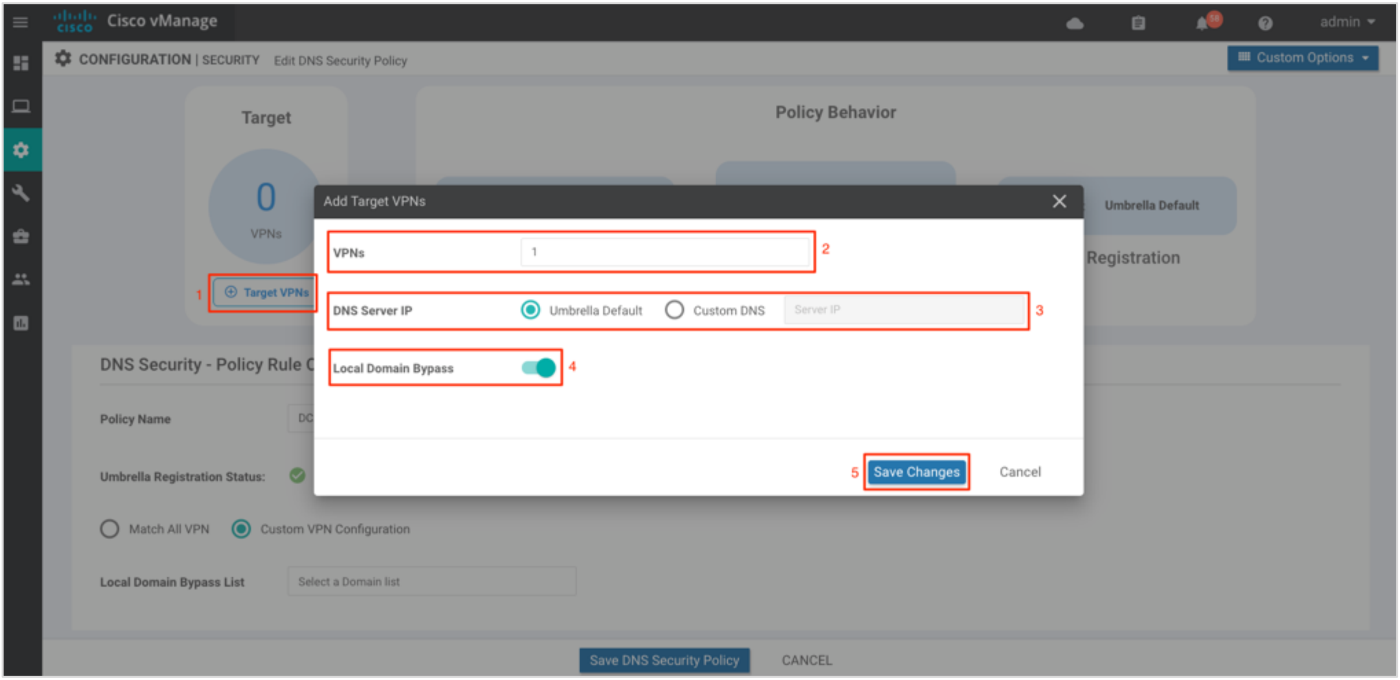
Umbrella Registration Status: Configured Umbrella Registration

○ Match All VPN ● Custom VPN Configuration

Local Domain Bypass List: Select a Domain list

Click Target VPNs to add custom VPNs to your po Got it!

Step 5. Within the **Target VPNs** wizard, add target VPNs within the **VPNs** tab. Select the **DNS Server IP** to redirect DNS traffic to **Umbrella DNS Server** resolvers or **Customer DNS** Server IP address and enable/disable **Local Domain Bypass**. Finally, click on **Save Changes**.



Add Target VPNs

VPNs: 1

DNS Server IP: ● Umbrella Default ○ Custom DNS Server IP

Local Domain Bypass: on

Save Changes Cancel

DNS Security - Policy Rule C

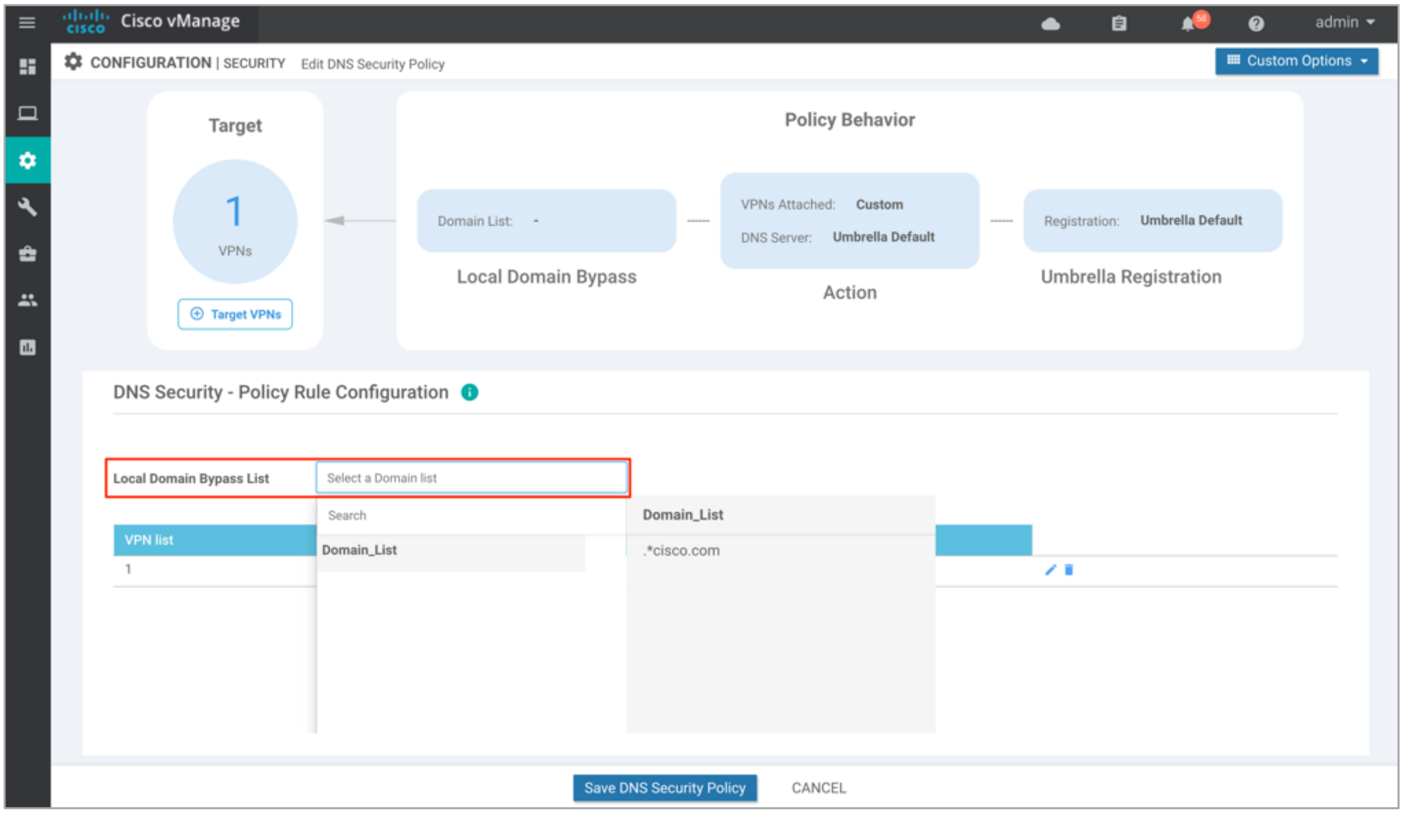
Policy Name: DC

Umbrella Registration Status: ✓

○ Match All VPN ● Custom VPN Configuration

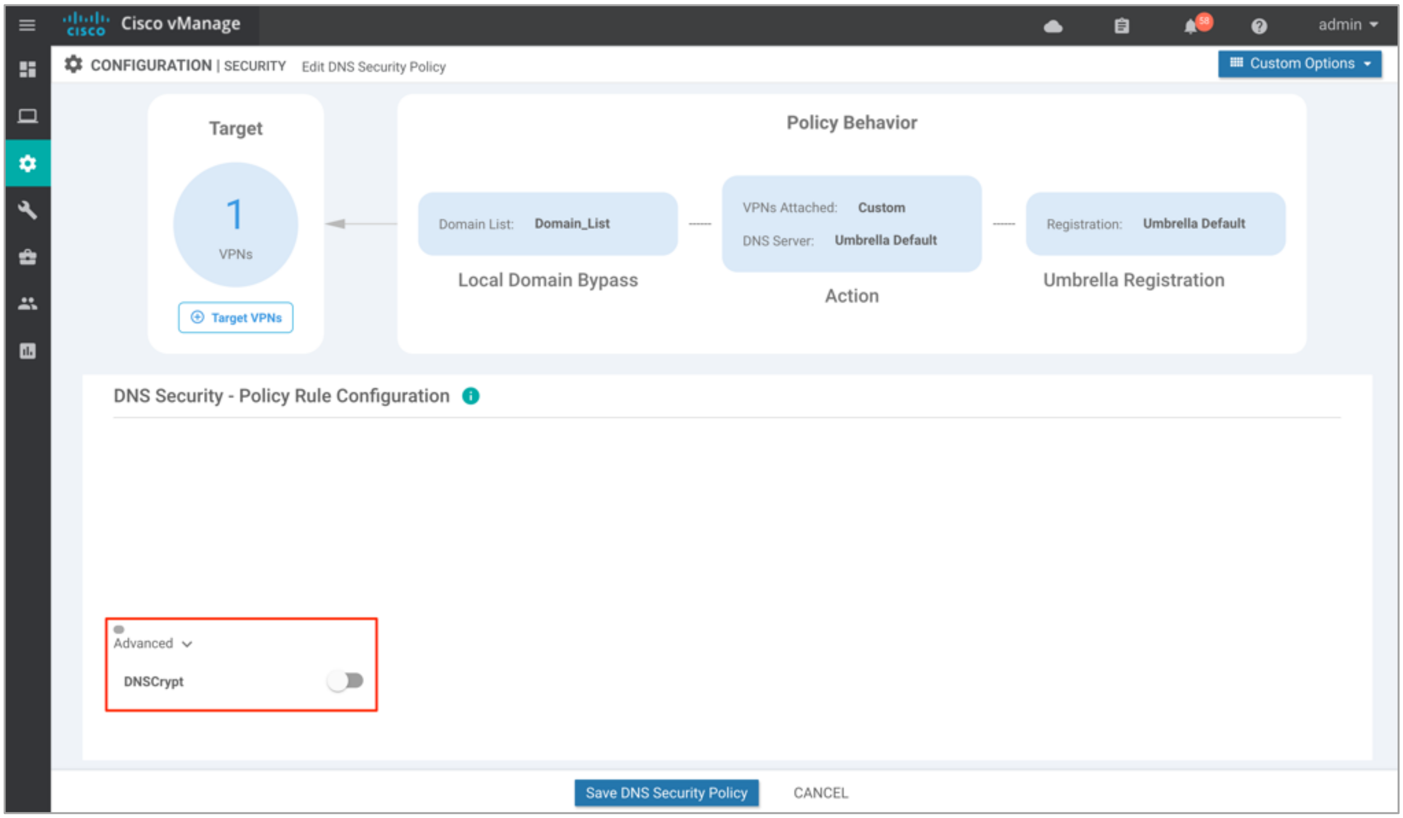
Local Domain Bypass List: Select a Domain list

Step 6. (Optional) Select the domain bypass from the **Local Domain Bypass List** drop-down as shown. Some of the possible regex patterns/formats to enter domain lists on vManage include, .*cisco.com, .*.cisco.com



Note: You can also create new regex patterns by clicking on **New Domain List.** Note, in this guide, **Local Domain Bypass List** is not enabled.

Step 7. Click on the **Advanced** tab to enable or disable the **DNSCrypt**. By default, the DNSCrypt is enabled. Note, DNSCypt encrypts DNS packets with EDNS (Device ID and Client IP) data and is supported only for Umbrella. Finally, click on **Save DNS Security Policy**.



Domain List: Domain_List

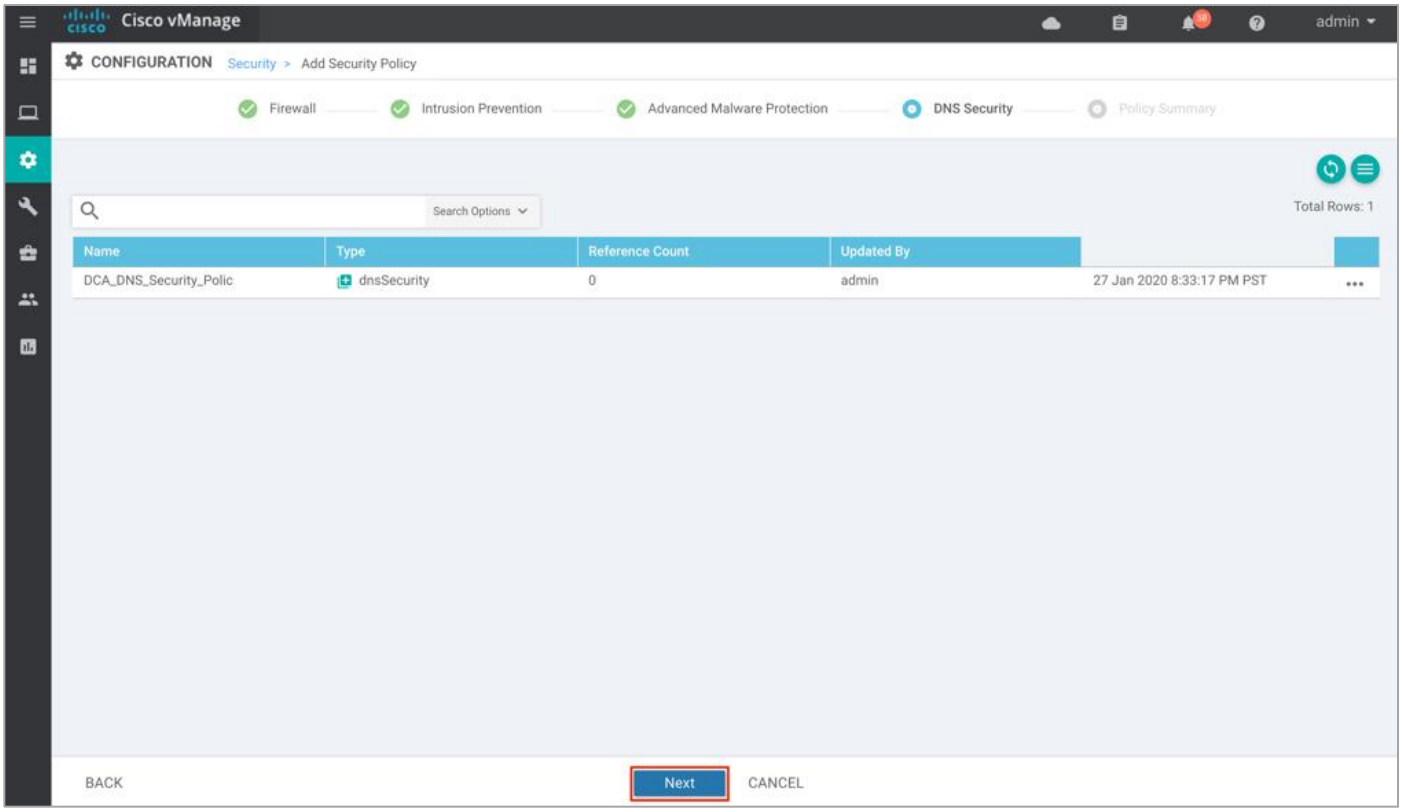
VPNs Attached: Custom

DNS Server: Umbrella Default

Registration: Umbrella Default

DNSCrypt

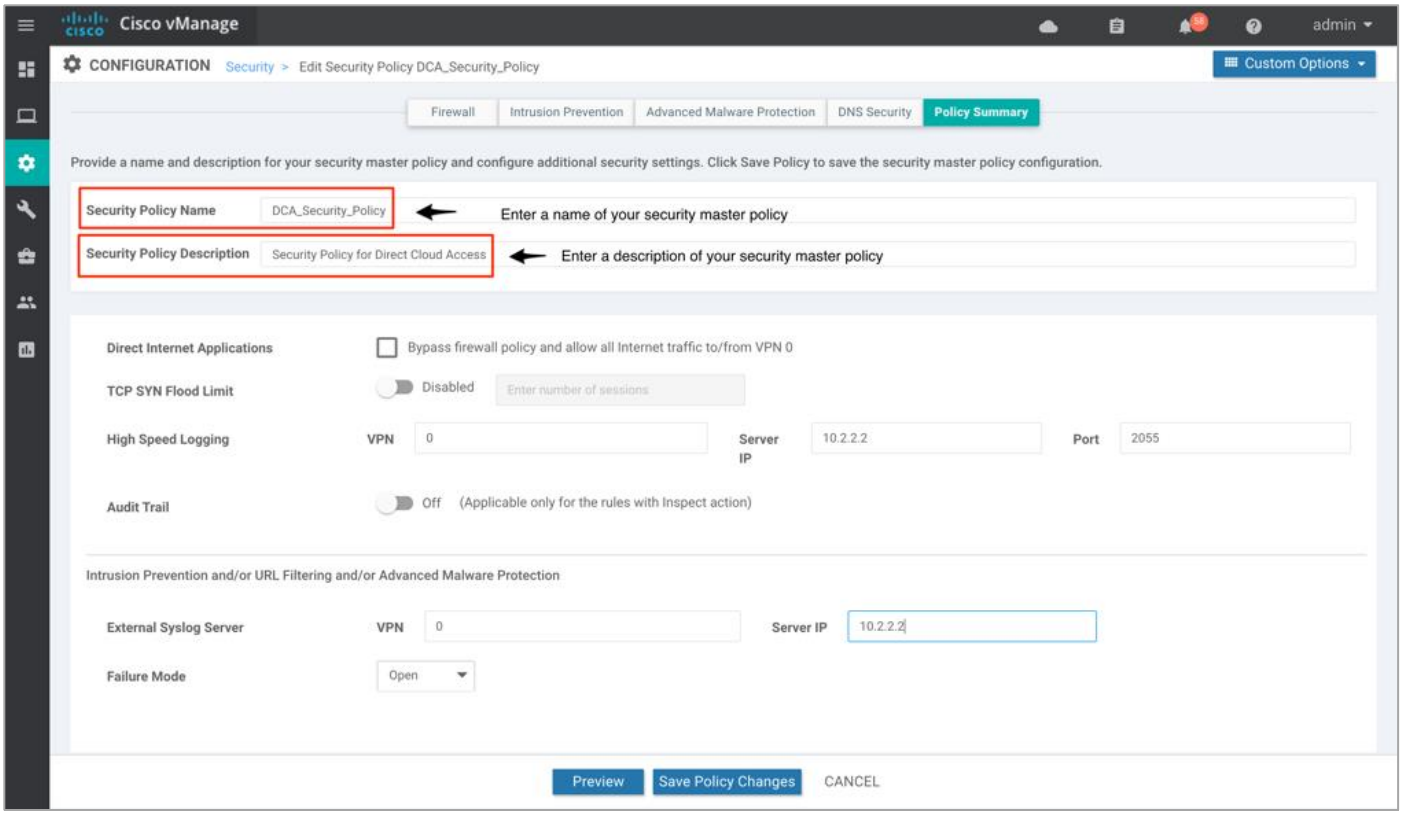
Step 8. Click **Next** to configure the **Policy Summary**.



Name	Type	Reference Count	Updated By		
DCA_DNS_Security_Polic	dnsSecurity	0	admin	27 Jan 2020 8:33:17 PM PST	•••

Procedure 5. Configure Policy Summary

Step 1. Within **Policy Summary**, 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: DCA_Security_Policy — Enter a name of your security master policy

Security Policy Description: Security Policy for Direct Cloud Access — Enter a description of your security master policy

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 10.2.2.2, Port 2055

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

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

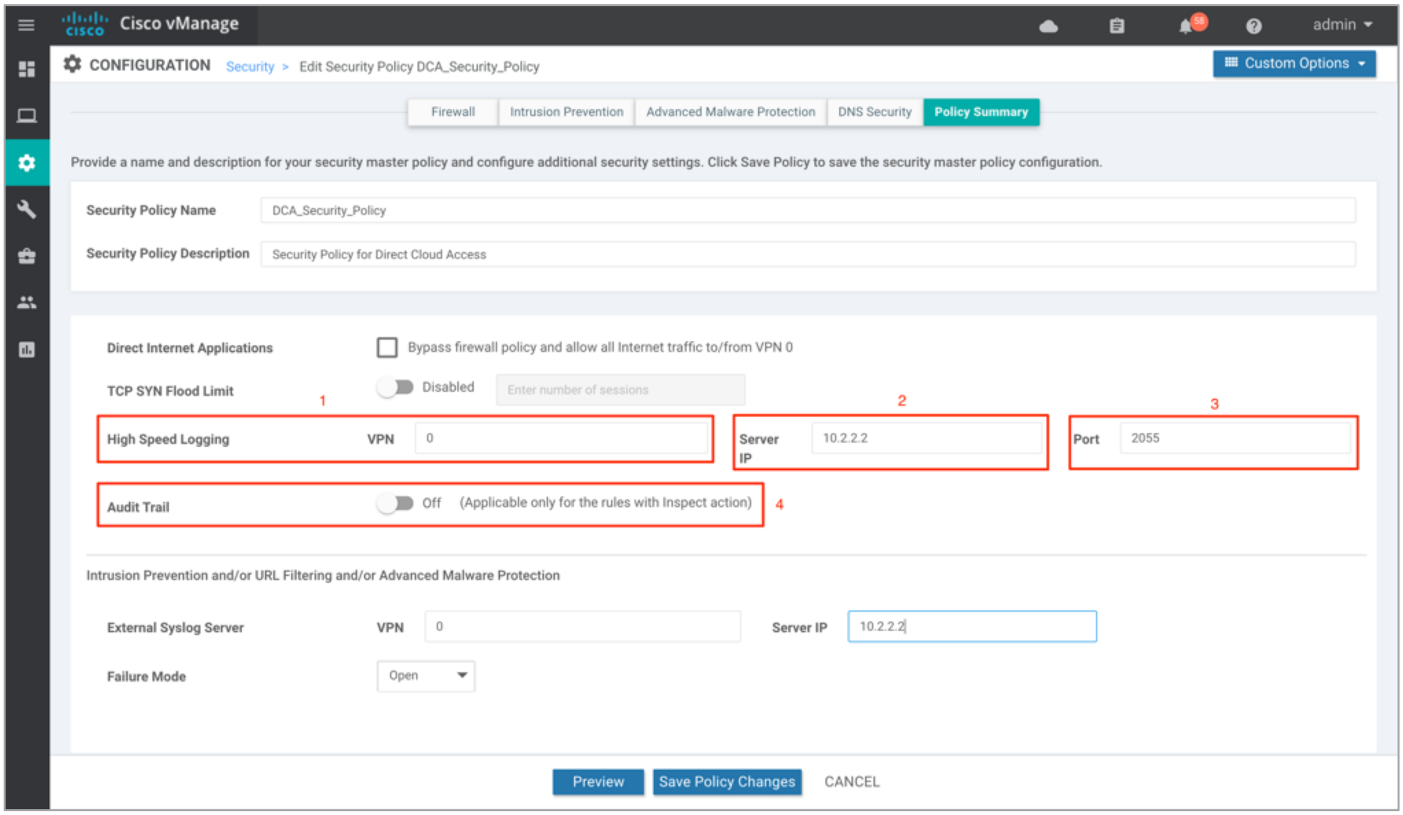
External Syslog Server: VPN 0, Server IP 10.2.2.2

Failure Mode: Open

Step 2. To log firewall packets that flow through routing devices (similar to the NetFlow Version 9 records) to an external collector enable **High Speed Logging** and enable **Audit Trail** to record the start, stop, and duration of a connection or session, and the source and destination IP addresses.

Within **High Speed Logging**, next to **VPN** tab enter the VPN label and against **Server IP** enter the IP Address of your server.

Note, 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: DCA_Security_Policy

Security Policy Description: Security Policy for Direct Cloud Access

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

TCP SYN Flood Limit: Disabled | Enter number of sessions

1 High Speed Logging — VPN: 0 | 2 Server IP: 10.2.2.2 | 3 Port: 2055

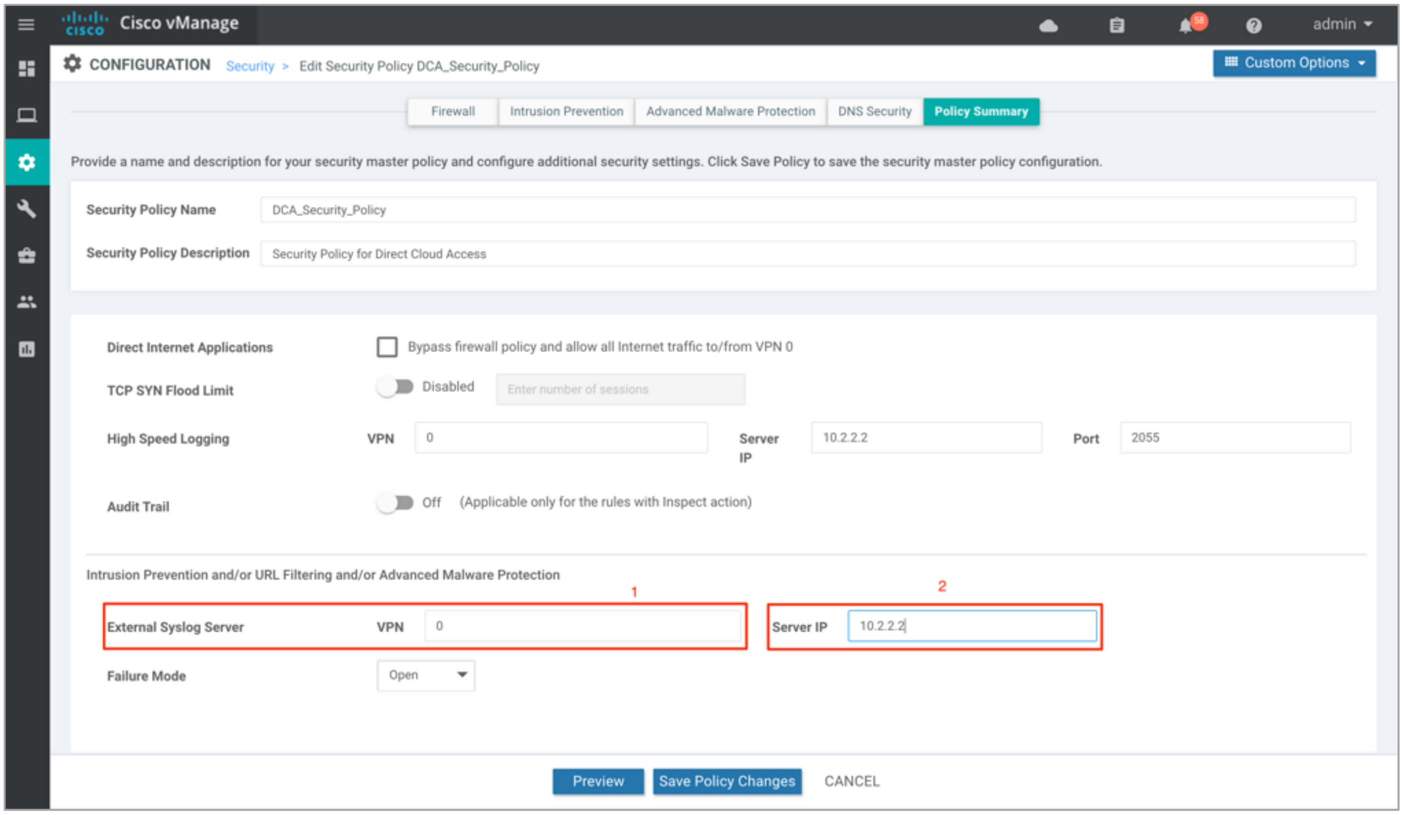
4 Audit Trail: Off (Applicable only for the rules with Inspect action)

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 3. Under the **Intrusion Prevention/ URL Filtering/ Advanced Malware Protection** section, you can fill in details to send logs to your **External Syslog Server.** Here, the **External Syslog Server** is set within VPN 0, hence the **VPN** label in **VPN** tab is **0**, followed by Server IP address next to **Server IP**.



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: DCA_Security_Policy

Security Policy Description: Security Policy for Direct Cloud Access

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: 10.2.2.2 | Port: 2055

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

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

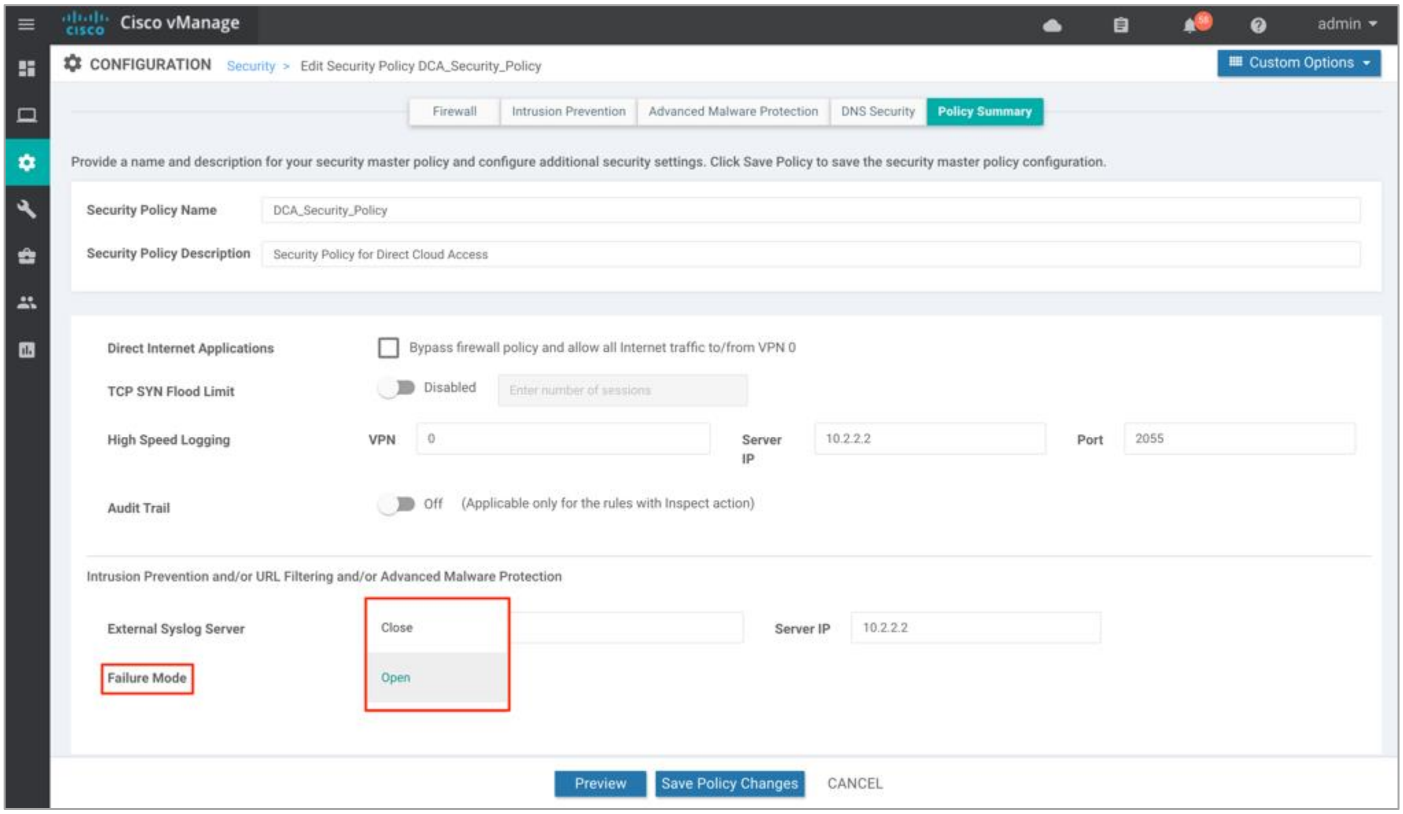
1 External Syslog Server — VPN: 0 | 2 Server IP: 10.2.2.2

Failure Mode: Open

Step 4. Set the **Failure Mode** to either **Open** or **Close**.

Note: If the Snort engine fails for any reason, and the device is set in fail-open mode, then the traffic bypasses all security features. In fail-close mode, traffic is dropped when an engine failure is detected.

Enable fail-close if security is the concern and select the option fail-open only if connectivity is the concern. Select one among the two based on the design. For more details, refer to the Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices.



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: DCA_Security_Policy

Security Policy Description: Security Policy for Direct Cloud Access

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 10.2.2.2, Port 2055

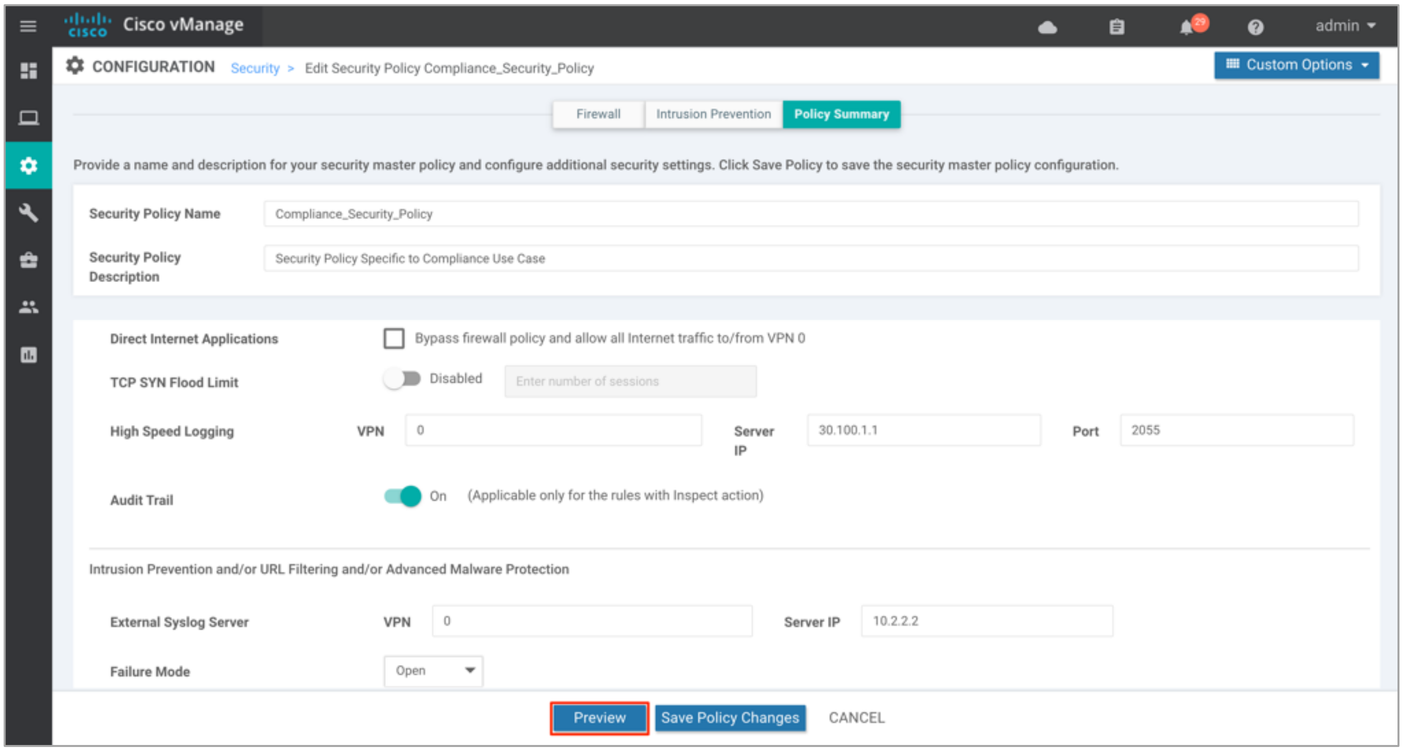
Audit Trail: Off (Applicable only for the rules with Inspect action)

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 5. Click on **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

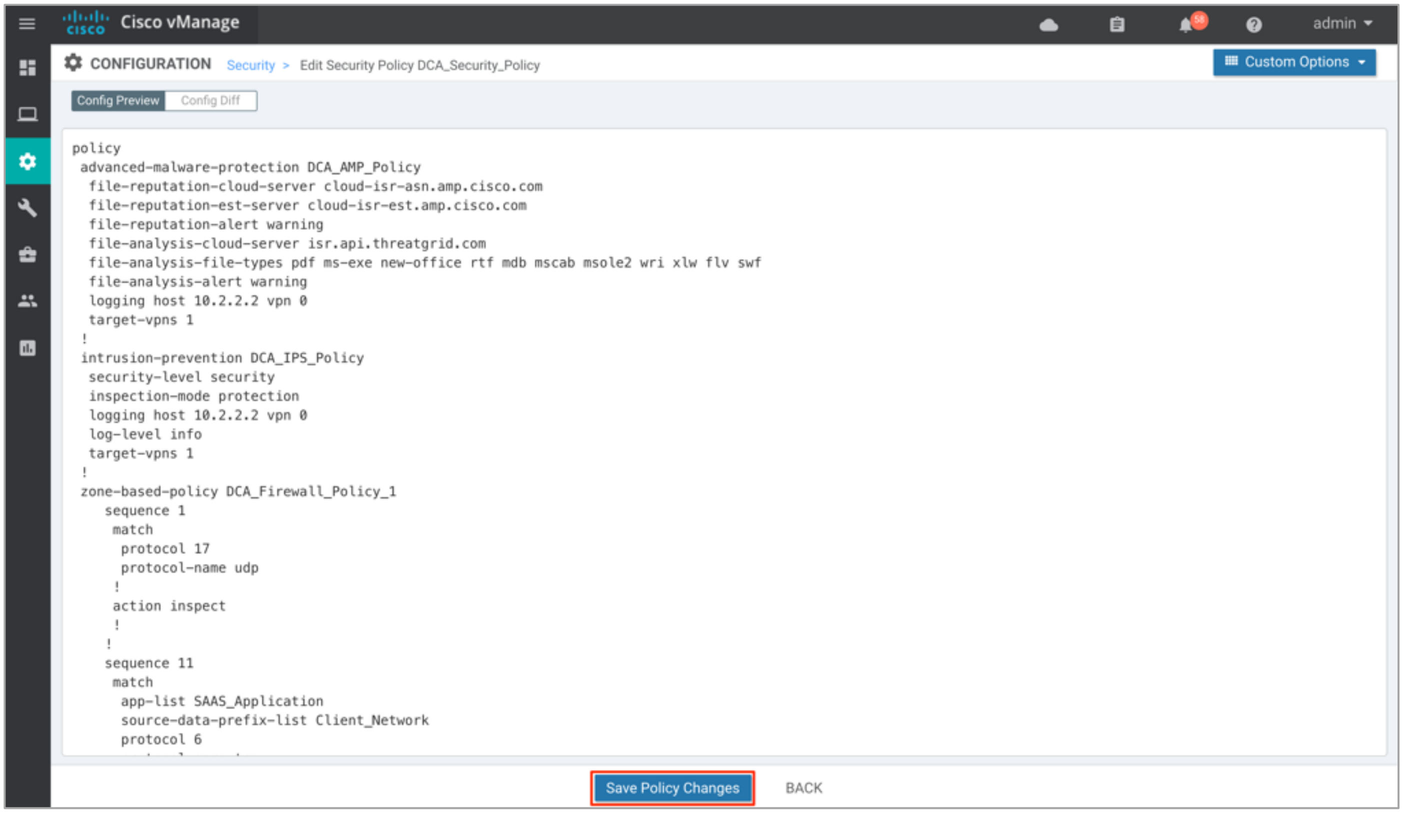
Audit Trail: On (Applicable only for the rules with Inspect action)

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 6. Finally, click **Save Policy Changes**.

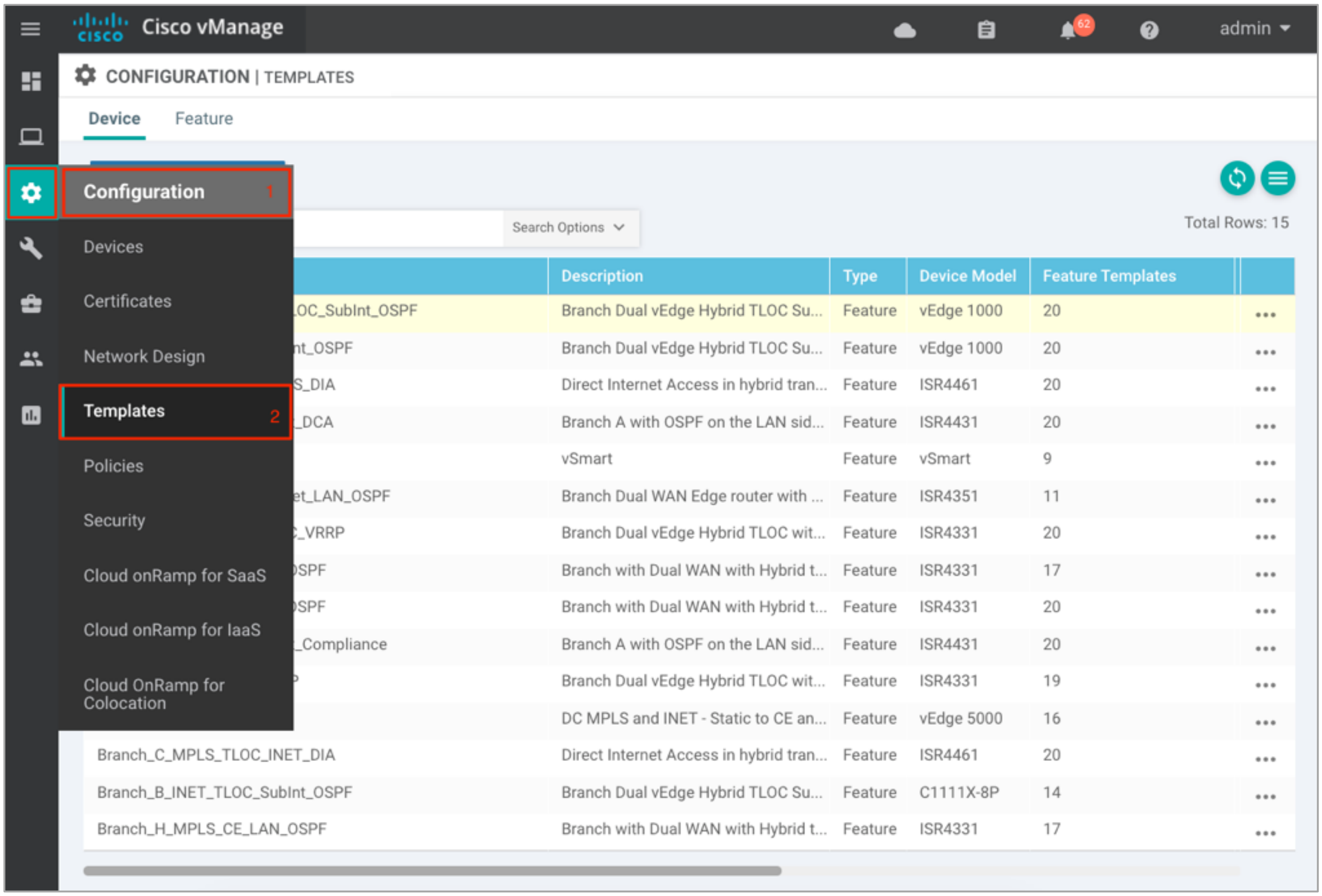


```
policy
 advanced-malware-protection DCA_AMP_Policy
  file-reputation-cloud-server cloud-isr-asn.amp.cisco.com
  file-reputation-est-server cloud-isr-est.amp.cisco.com
  file-reputation-alert warning
  file-analysis-cloud-server isr.api.threatgrid.com
  file-analysis-file-types pdf ms-exe new-office rtf mdb mscab msole2 wri xlw flv swf
  file-analysis-alert warning
  logging host 10.2.2.2 vpn 0
  target-vpns 1
 !
 intrusion-prevention DCA_IPS_Policy
  security-level security
  inspection-mode protection
  logging host 10.2.2.2 vpn 0
  log-level info
  target-vpns 1
 !
 zone-based-policy DCA_Firewall_Policy_1
    sequence 1
     match
      protocol 17
      protocol-name udp
     !
     action inspect
     !
    !
    sequence 11
     match
      app-list SAAS_Application
      source-data-prefix-list Client_Network
      protocol 6
```

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

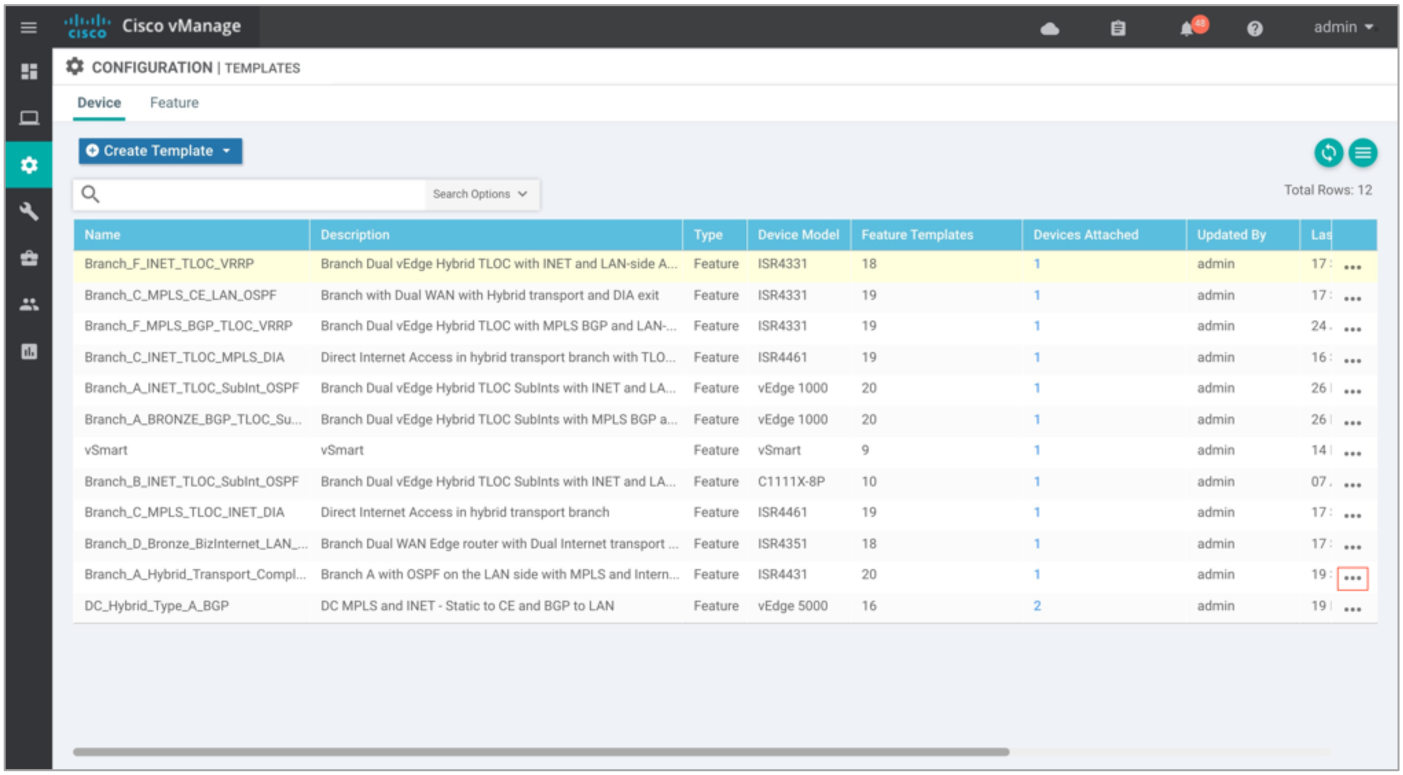
To apply the configured security policy to a remote-site WAN Edge device, follow the steps listed below.

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

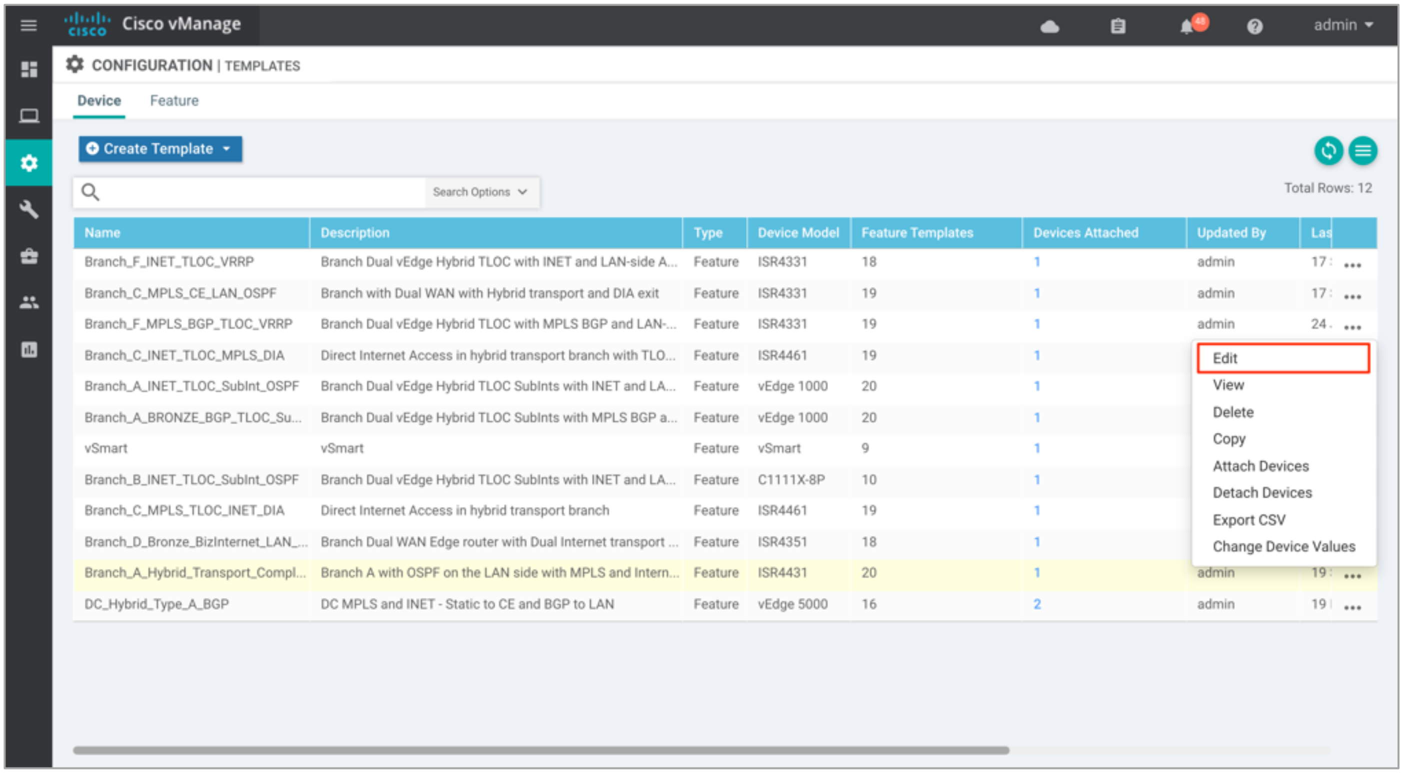


	Description	Type	Device Model	Feature Templates	
OC_SubInt_OSPF	Branch Dual vEdge Hybrid TLOC Su...	Feature	vEdge 1000	20	•••
nt_OSPF	Branch Dual vEdge Hybrid TLOC Su...	Feature	vEdge 1000	20	•••
S_DIA	Direct Internet Access in hybrid tran...	Feature	ISR4461	20	•••
_DCA	Branch A with OSPF on the LAN sid...	Feature	ISR4431	20	•••
	vSmart	Feature	vSmart	9	•••
et_LAN_OSPF	Branch Dual WAN Edge router with ...	Feature	ISR4351	11	•••
_VRRP	Branch Dual vEdge Hybrid TLOC wit...	Feature	ISR4331	20	•••
SPF	Branch with Dual WAN with Hybrid t...	Feature	ISR4331	17	•••
SPF	Branch with Dual WAN with Hybrid t...	Feature	ISR4331	20	•••
_Compliance	Branch A with OSPF on the LAN sid...	Feature	ISR4431	20	•••
P	Branch Dual vEdge Hybrid TLOC wit...	Feature	ISR4331	19	•••
	DC MPLS and INET - Static to CE an...	Feature	vEdge 5000	16	•••
Branch_C_MPLS_TLOC_INET_DIA	Direct Internet Access in hybrid tran...	Feature	ISR4461	20	•••
Branch_B_INET_TLOC_SubInt_OSPF	Branch Dual vEdge Hybrid TLOC Su...	Feature	C1111X-8P	14	•••
Branch_H_MPLS_CE_LAN_OSPF	Branch with Dual WAN with Hybrid t...	Feature	ISR4331	17	•••

Step 2. To attach the security policy to a **Device Template**, click on the **three dots** found on the right side of the template and select **Edit** from the drop-down options.

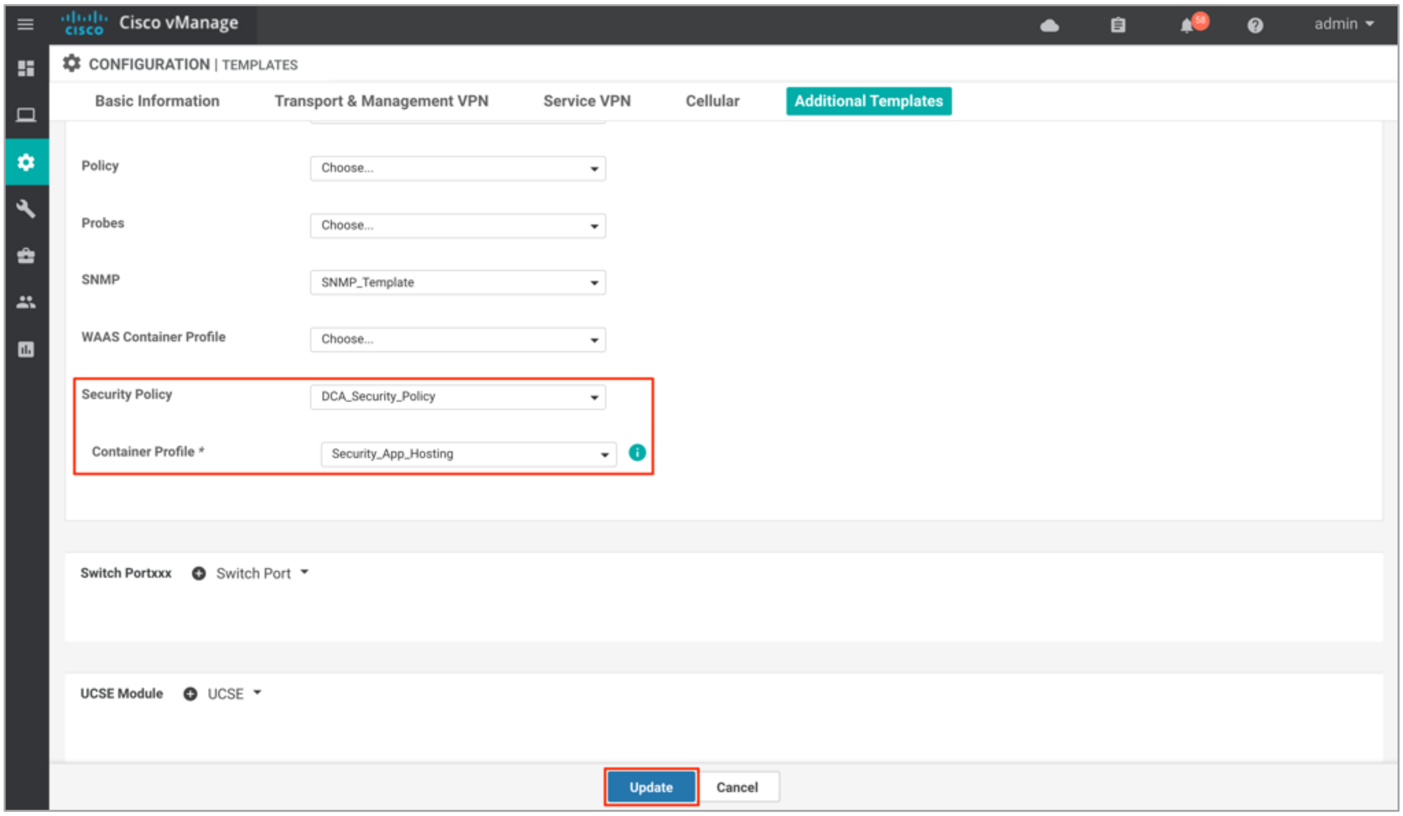


Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Las
Branch_F_INET_TLOC_VRRP	Branch Dual vEdge Hybrid TLOC with INET and LAN-side A...	Feature	ISR4331	18	1	admin	17
Branch_C_MPLS_CE_LAN_OSPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	19	1	admin	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 3. Within the Device Template, navigate to Additional Templates and attach the **Security Policy** (DCA_Security_Policy), along with the **Container Profile*** (Security_App_Hosting). Finally, click **Update.**



Policy: Choose...

Probes: Choose...

SNMP: SNMP_Template

WAAS Container Profile: Choose...

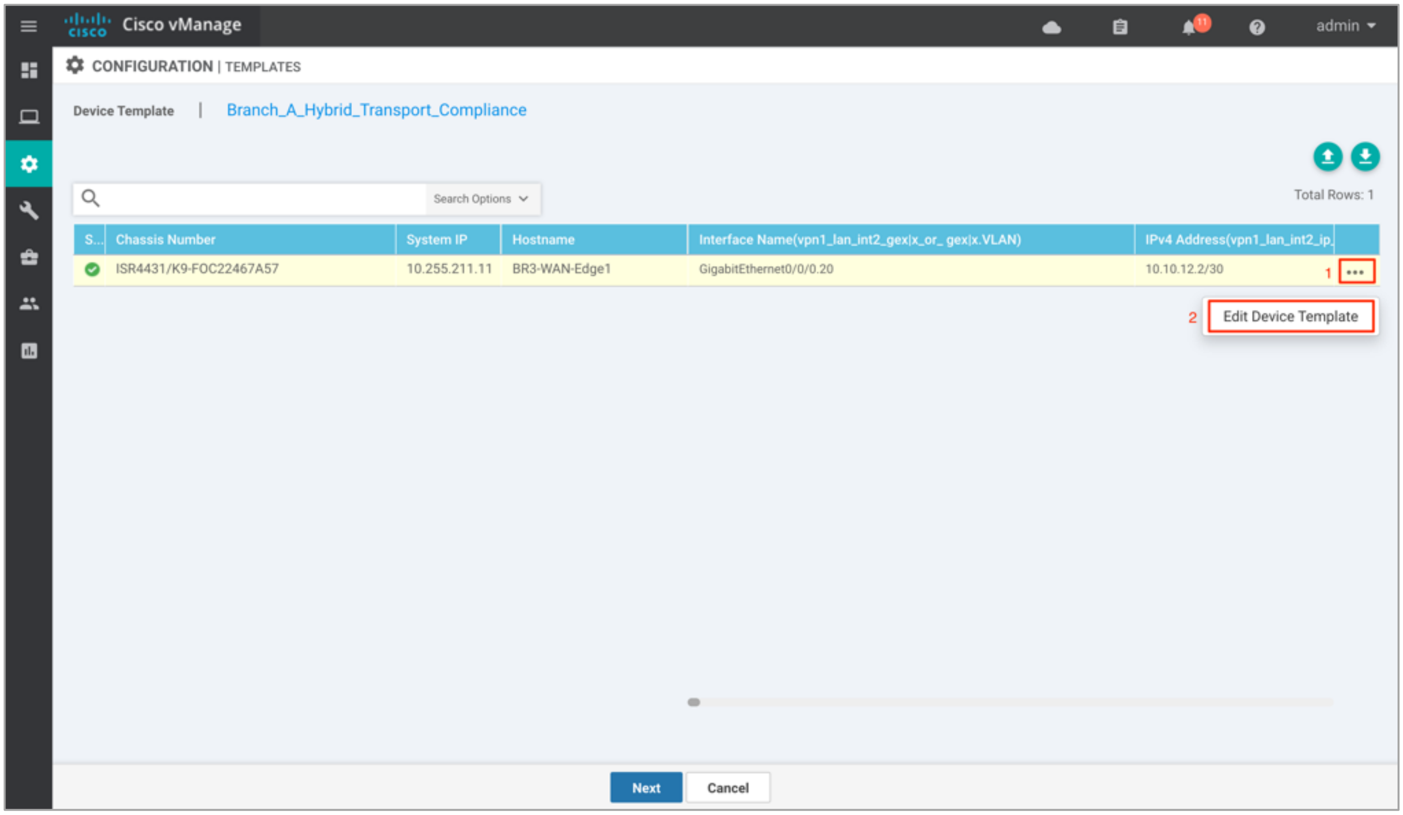
Security Policy: DCA_Security_Policy

Container Profile *: Security_App_Hosting

Switch Portxxx: Switch Port

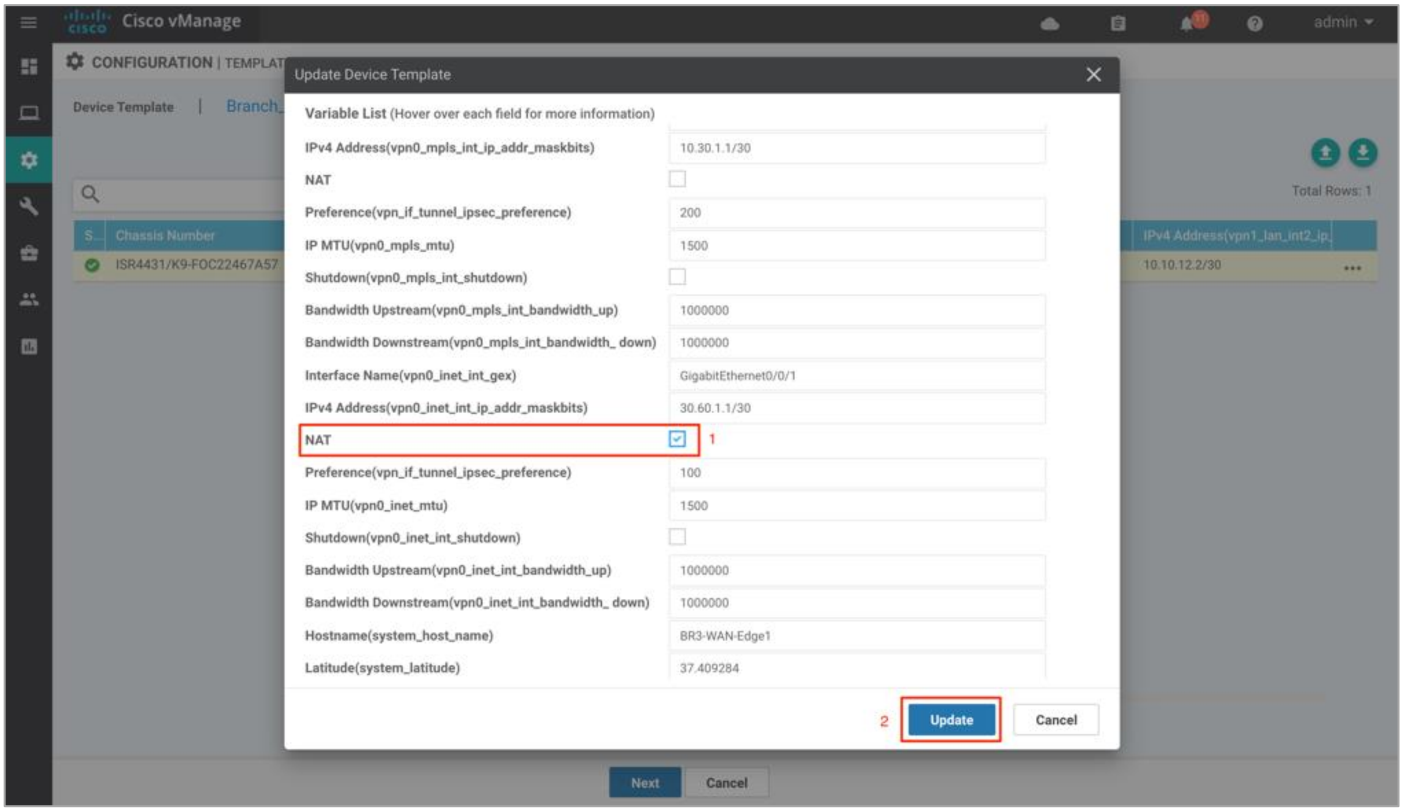
UCSE Module: UCSE

Step 4. Make sure **NAT** is already configured on the WAN Internet transport Interface. To do so click on 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

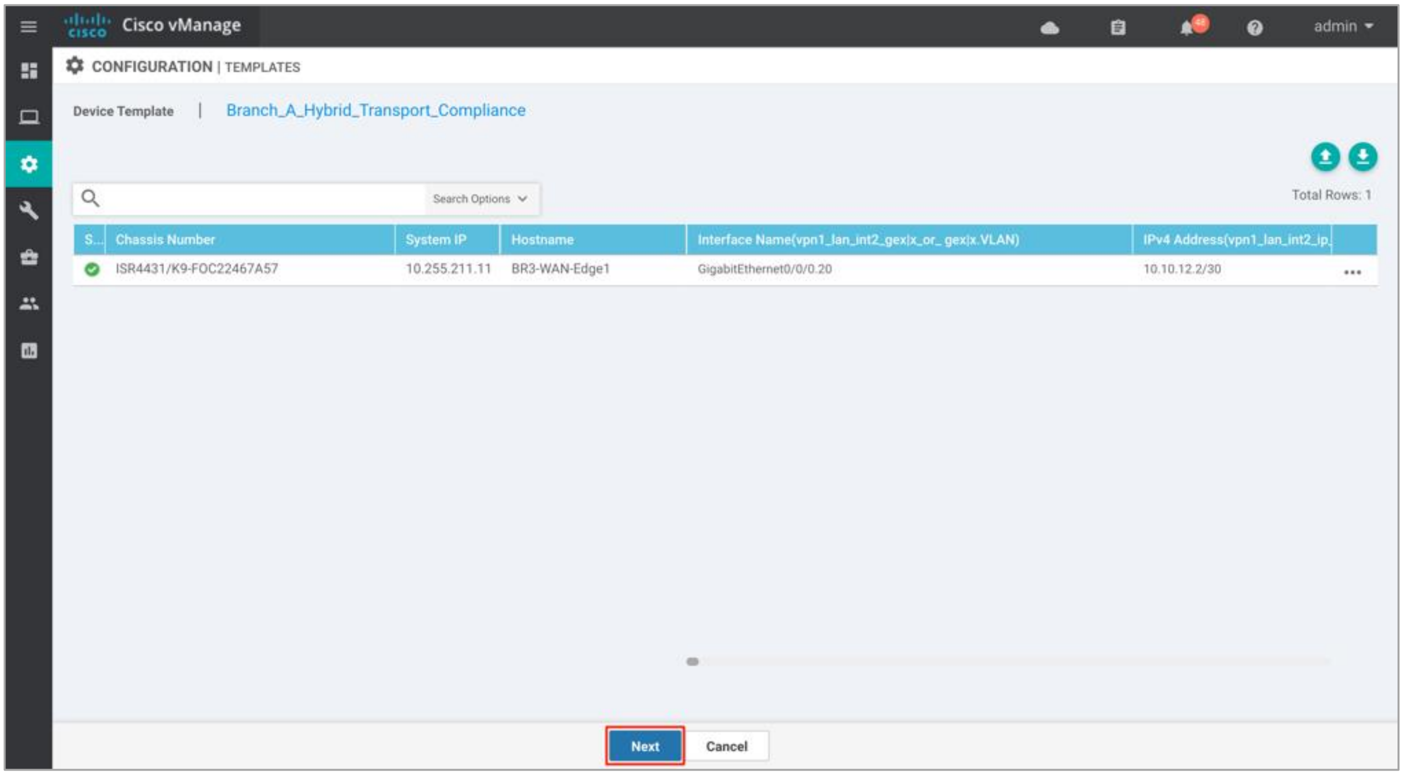
Variable List (Hover over each field for more information)

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: If 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.** You can do this before or after deploying the security policy.

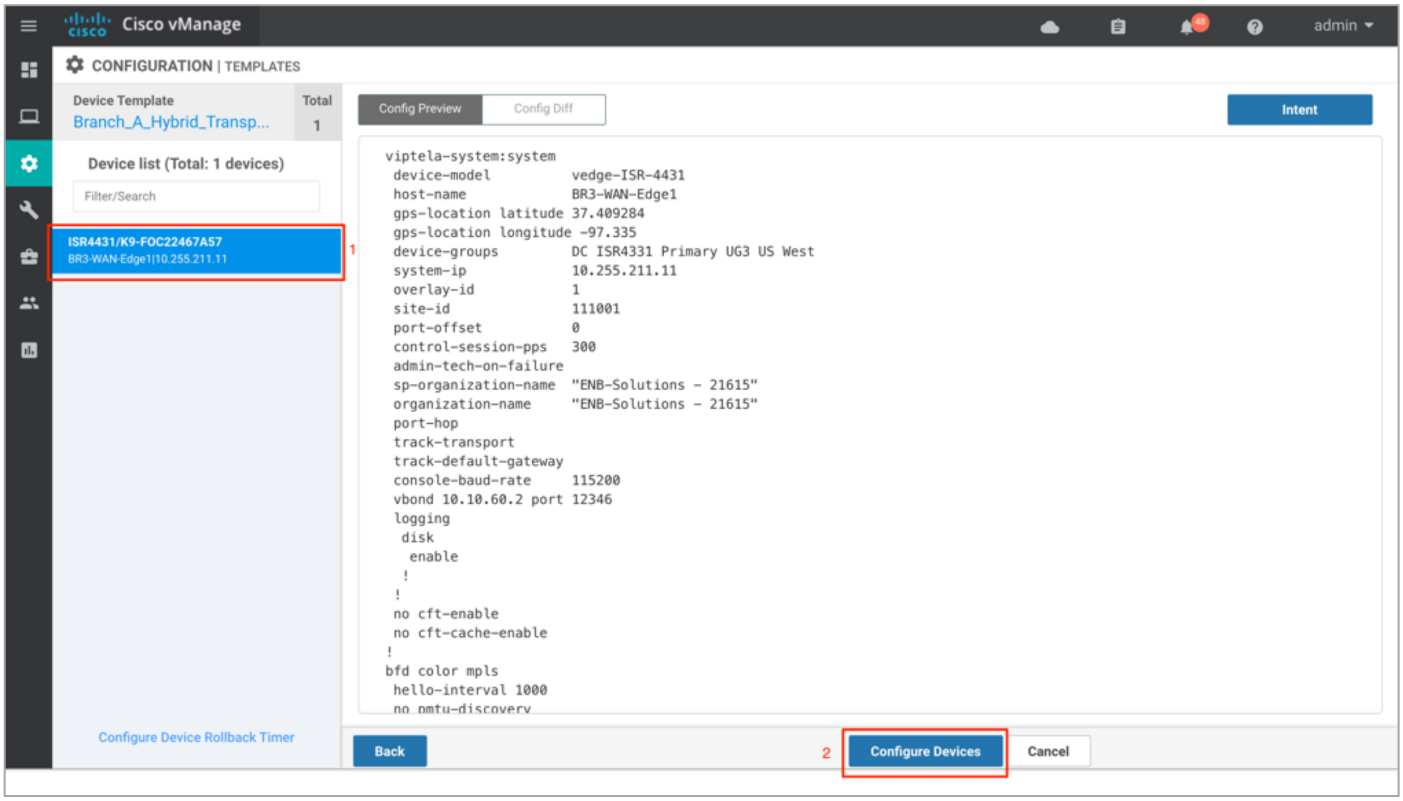
Step 5. Once, the changes are made click **Next.**



Device Template | Branch_A_Hybrid_Transport_Compliance

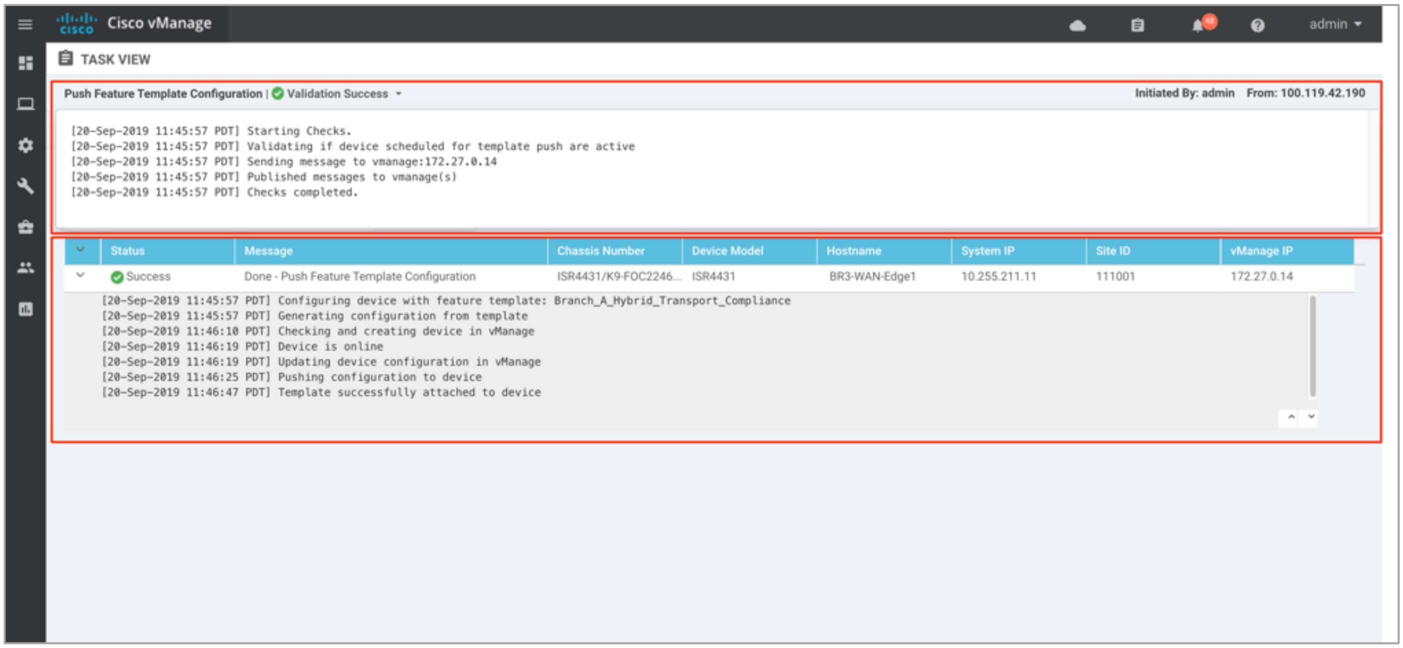
S...	Chassis Number	System IP	Hostname	Interface Name(vpn1_lan_int2_gex|x_or_ gex|x.VLAN)	IPv4 Address(vpn1_lan_int2_ip_
✓	ISR4431/K9-FOC22467A57	10.255.211.11	BR3-WAN-Edge1	GigabitEthernet0/0/0.20	10.10.12.2/30

Step 6. 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
Device list (Total: 1 devices)
Filter/Search
ISR4431/K9-FOC22467A57
BR3-WAN-Edge1|10.255.211.11
1
Config Preview
Config Diff
Intent
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 7. The **Task View** screen will display 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 Secure Direct Cloud Access

Using the vManage GUI, you can monitor, troubleshoot and manage the Cisco SD-WAN security features deployed. The 3 main ways to troubleshoot the security features is via,

vManage Main Dashboard: The vManage main dashboard displays the graphical view of all the packets inspected, dropped by the firewall, signature violations for IPS, files transferred along with its disposition for AMP.

vManage Monitor Dashboard: The vManage monitor dashboard displays the graphical and real time statistics of the traffic inspected by the security features configured.

vManage SSH Server Dashboard: The vManage SSH server dashboard provides the option to manage the WAN Edge device via CLI.

Note: You can also configure a syslog server and scan through the logs gathered within the server to monitor your WAN Edge device.

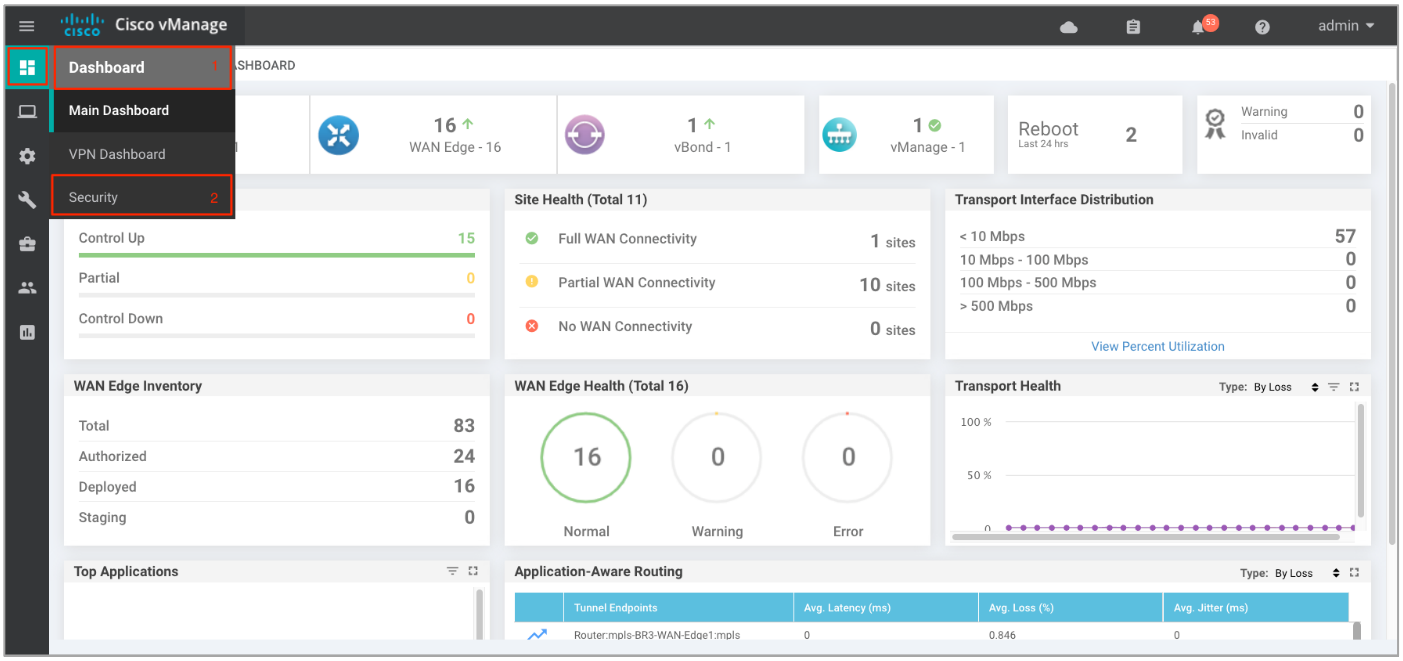
Process 1: Monitor the Enterprise Firewall with Application Awareness Feature via vManage NMS

Monitor, manage and troubleshoot the Enterprise Firewall with Application Awareness feature via vManage NMS.

Procedure 1. Monitor the Firewall Feature via vManage Main Dashboard

Using the vManage NMS dashboard, you can view the firewall statistics via dashboard.

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



16 WAN Edge - 16

1 vBond - 1

1 vManage - 1

Reboot Last 24 hrs 2

Warning 0

Invalid 0

Control Up	15
Partial	0
Control Down	0

Site Health (Total 11)

Full WAN Connectivity	1 sites
Partial WAN Connectivity	10 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)

16 Normal

0 Warning

0 Error

Transport Health Type: By Loss

100 %

50 %

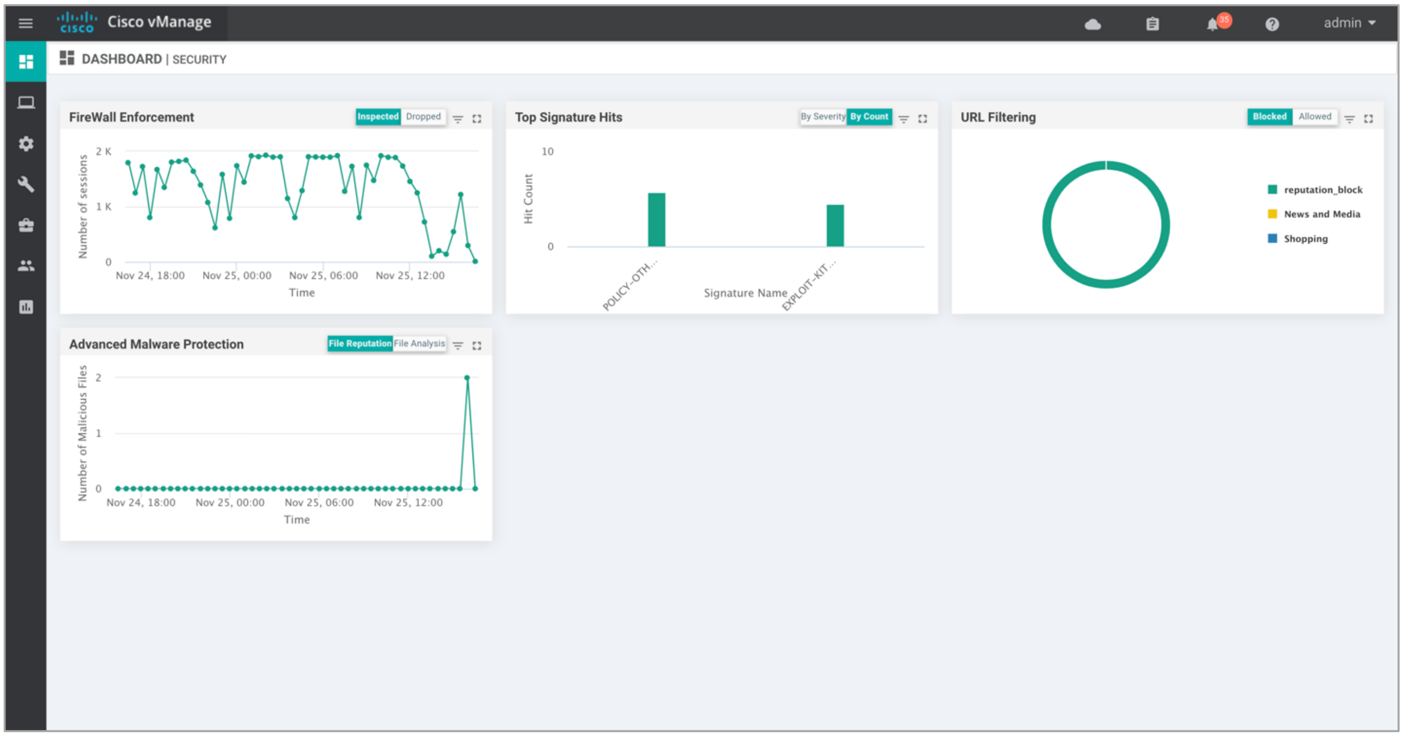
0

Top Applications

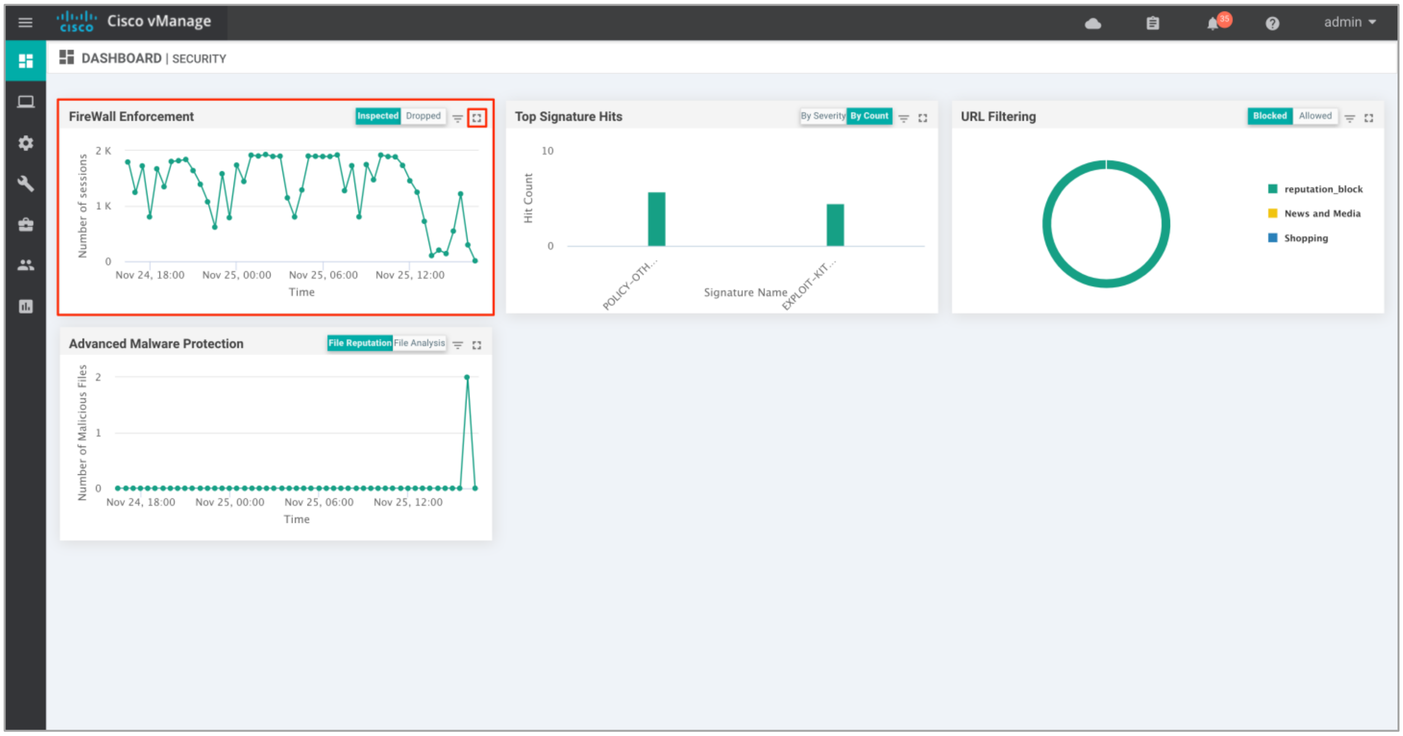
Application-Aware Routing Type: By Loss

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.

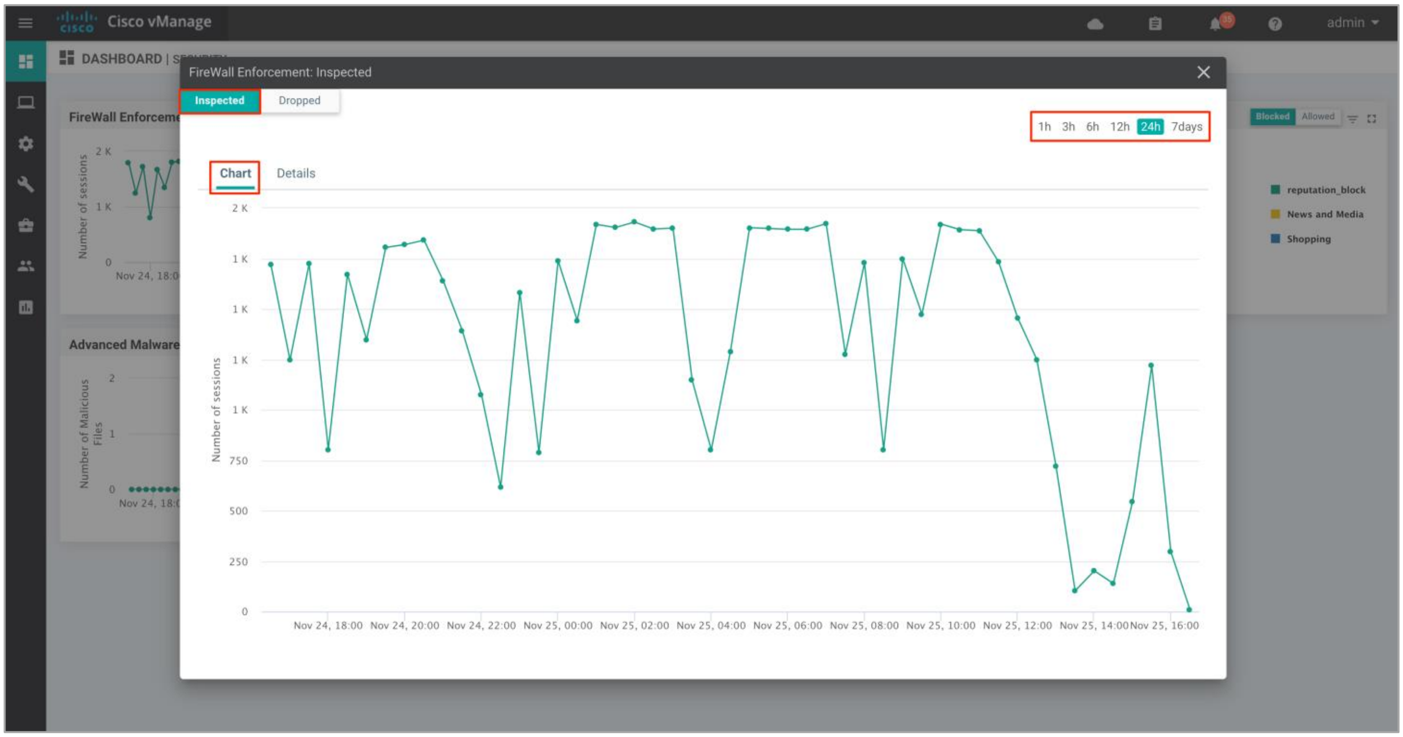


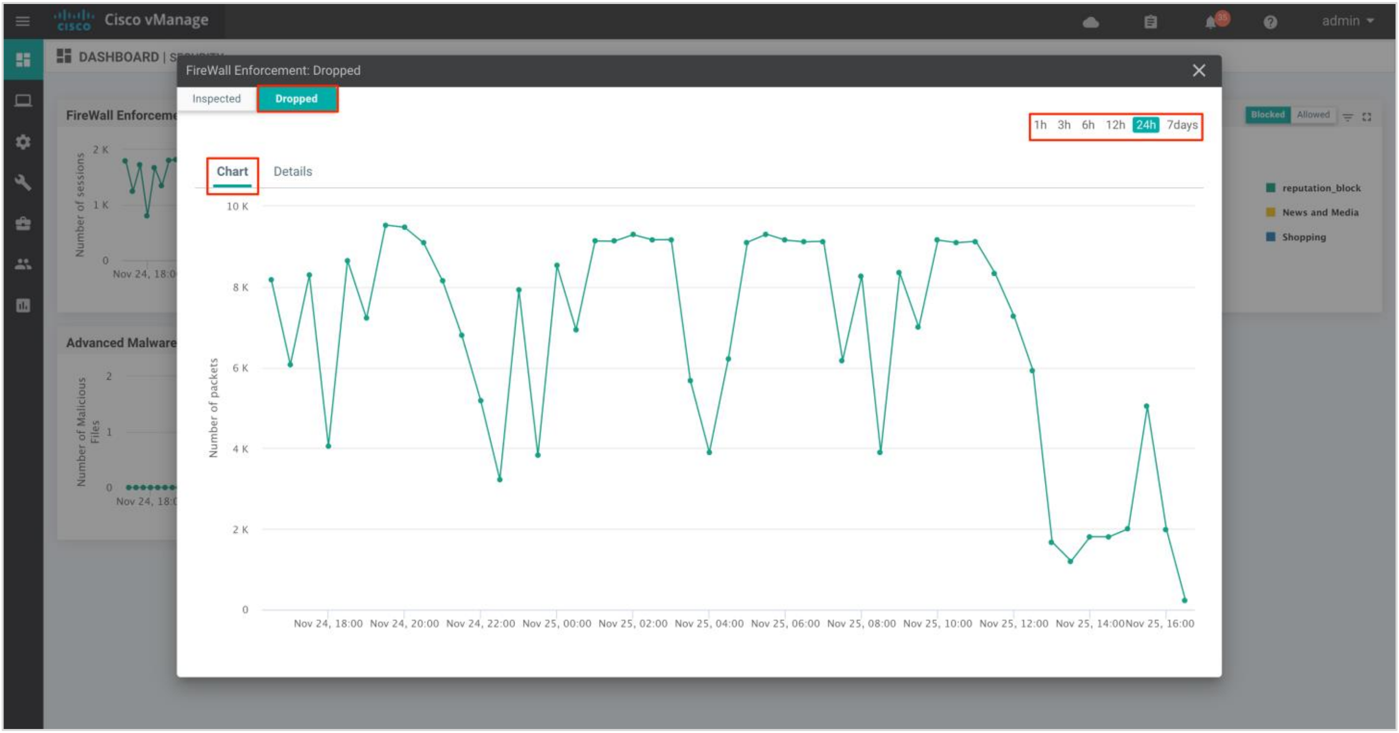
Step 3. To take a closer look into the **Firewall Enforcement** graph, click on the **square box []** on the top right.



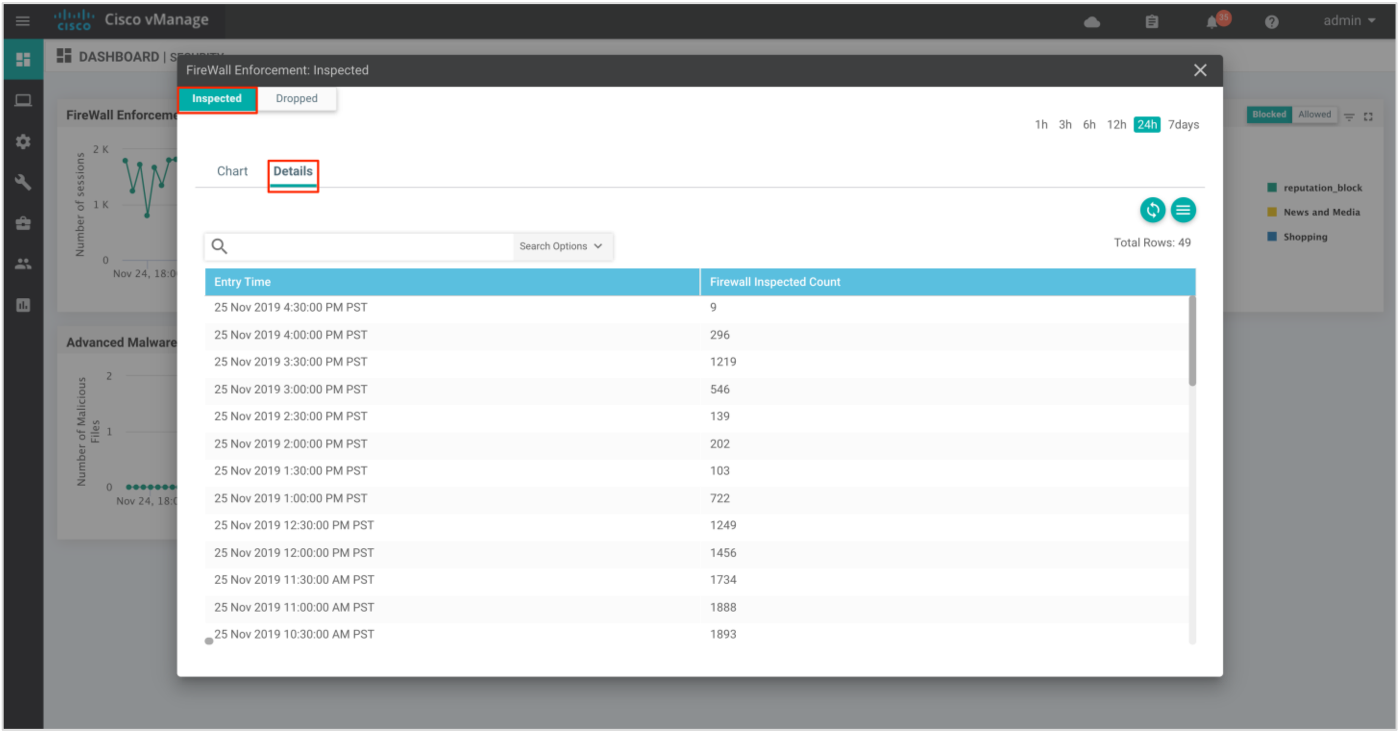
Step 4. Drilling down into the graph provides more information. Toggle between inspected and dropped packets and click on **1h, 3h, 6h, 12h, 24h (default)** or **7 days** to view the hourly, daily or weekly firewall statistics.

Chart displays the graphical representation of the firewall statistics for both traffic inspected and traffic dropped.





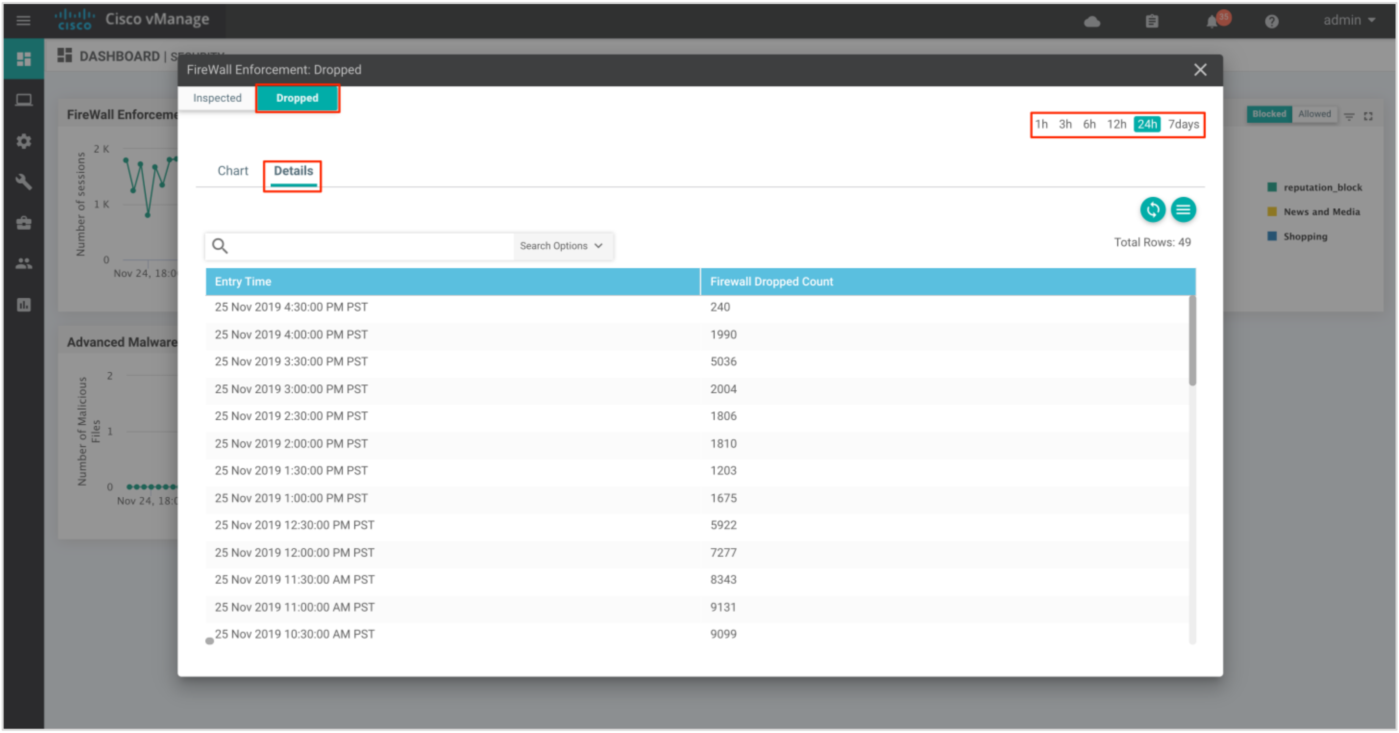
Details displays the Firewall Inspected/Dropped Count.



FireWall Enforcement: Inspected

Total Rows: 49

Entry Time	Firewall Inspected Count
25 Nov 2019 4:30:00 PM PST	9
25 Nov 2019 4:00:00 PM PST	296
25 Nov 2019 3:30:00 PM PST	1219
25 Nov 2019 3:00:00 PM PST	546
25 Nov 2019 2:30:00 PM PST	139
25 Nov 2019 2:00:00 PM PST	202
25 Nov 2019 1:30:00 PM PST	103
25 Nov 2019 1:00:00 PM PST	722
25 Nov 2019 12:30:00 PM PST	1249
25 Nov 2019 12:00:00 PM PST	1456
25 Nov 2019 11:30:00 AM PST	1734
25 Nov 2019 11:00:00 AM PST	1888
25 Nov 2019 10:30:00 AM PST	1893



FireWall Enforcement: Dropped

Total Rows: 49

Entry Time	Firewall Dropped Count
25 Nov 2019 4:30:00 PM PST	240
25 Nov 2019 4:00:00 PM PST	1990
25 Nov 2019 3:30:00 PM PST	5036
25 Nov 2019 3:00:00 PM PST	2004
25 Nov 2019 2:30:00 PM PST	1806
25 Nov 2019 2:00:00 PM PST	1810
25 Nov 2019 1:30:00 PM PST	1203
25 Nov 2019 1:00:00 PM PST	1675
25 Nov 2019 12:30:00 PM PST	5922
25 Nov 2019 12:00:00 PM PST	7277
25 Nov 2019 11:30:00 AM PST	8343
25 Nov 2019 11:00:00 AM PST	9131
25 Nov 2019 10:30:00 AM PST	9099

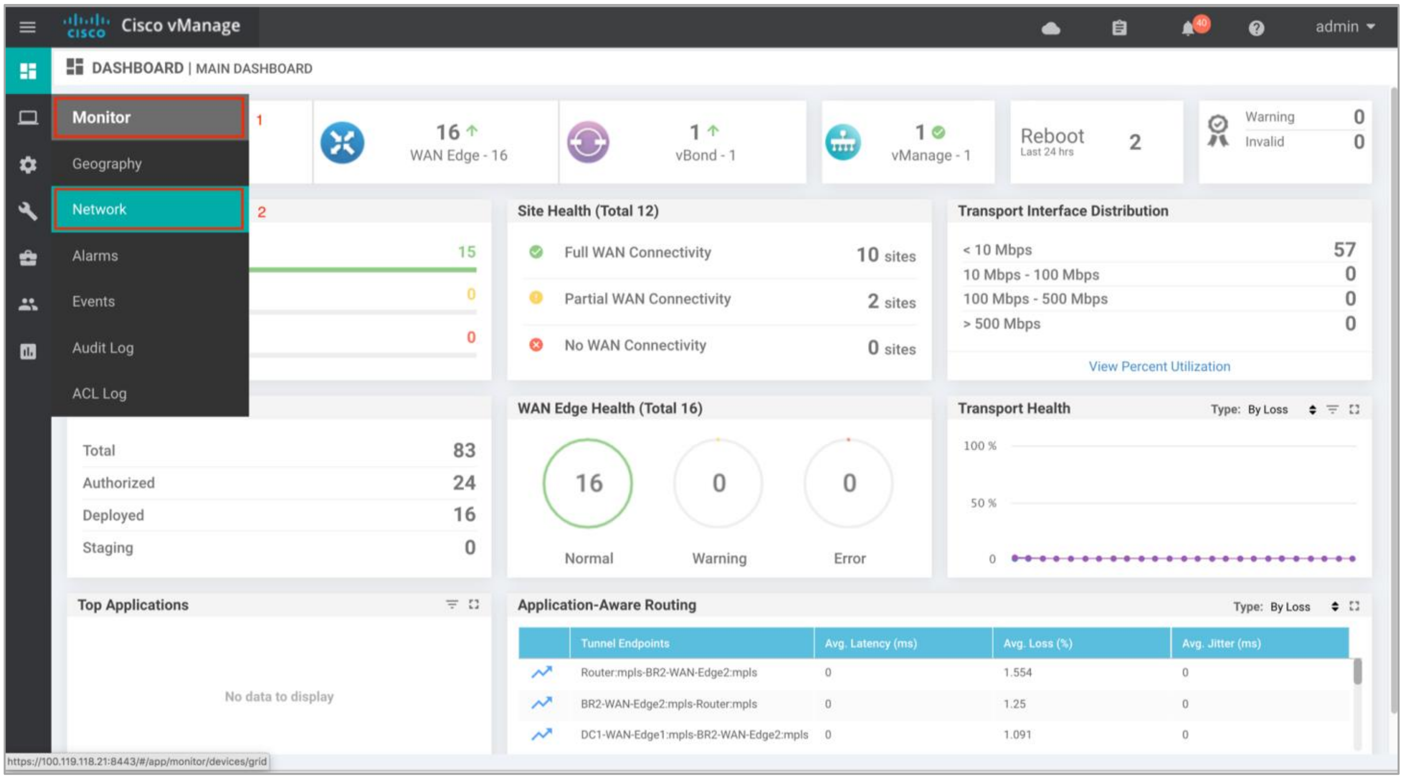
Technical Tip

To view the details such as IP address of the packet inspected or dropped, click on the peaks of the graphical representation.

Procedure 2. Monitor the Firewall Feature via vManage Monitor Dashboard

Using the vManage NMS dashboard, you can view the Enterprise Firewall with Application Awareness statistics via the monitor dashboard.

Step 1. Navigate to **Network** within **Monitor** available on the left pane and click on the WAN Edge device you wish to monitor.



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

Total	83
Authorized	24
Deployed	16
Staging	0

WAN Edge Health (Total 16)

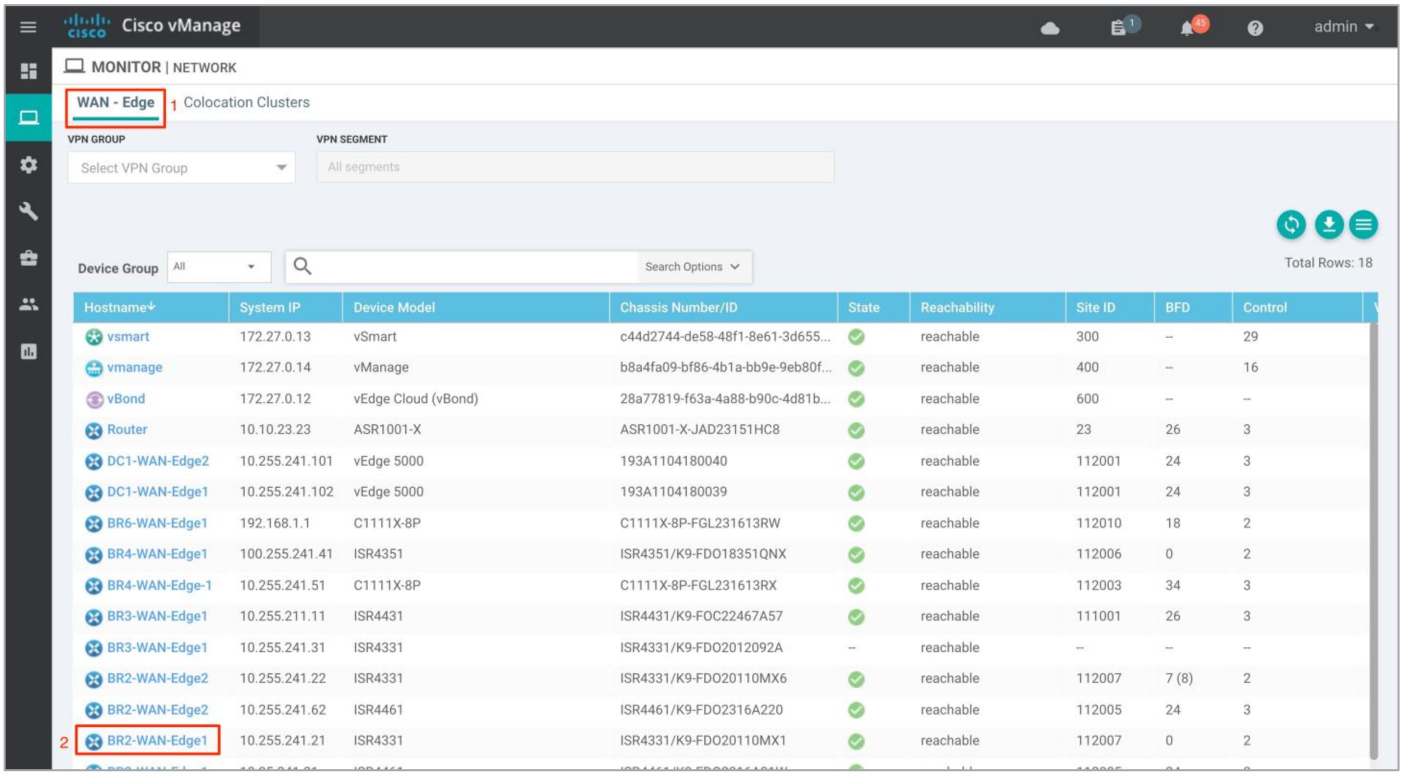
Normal	Warning	Error
16	0	0

Transport Health

Application-Aware Routing

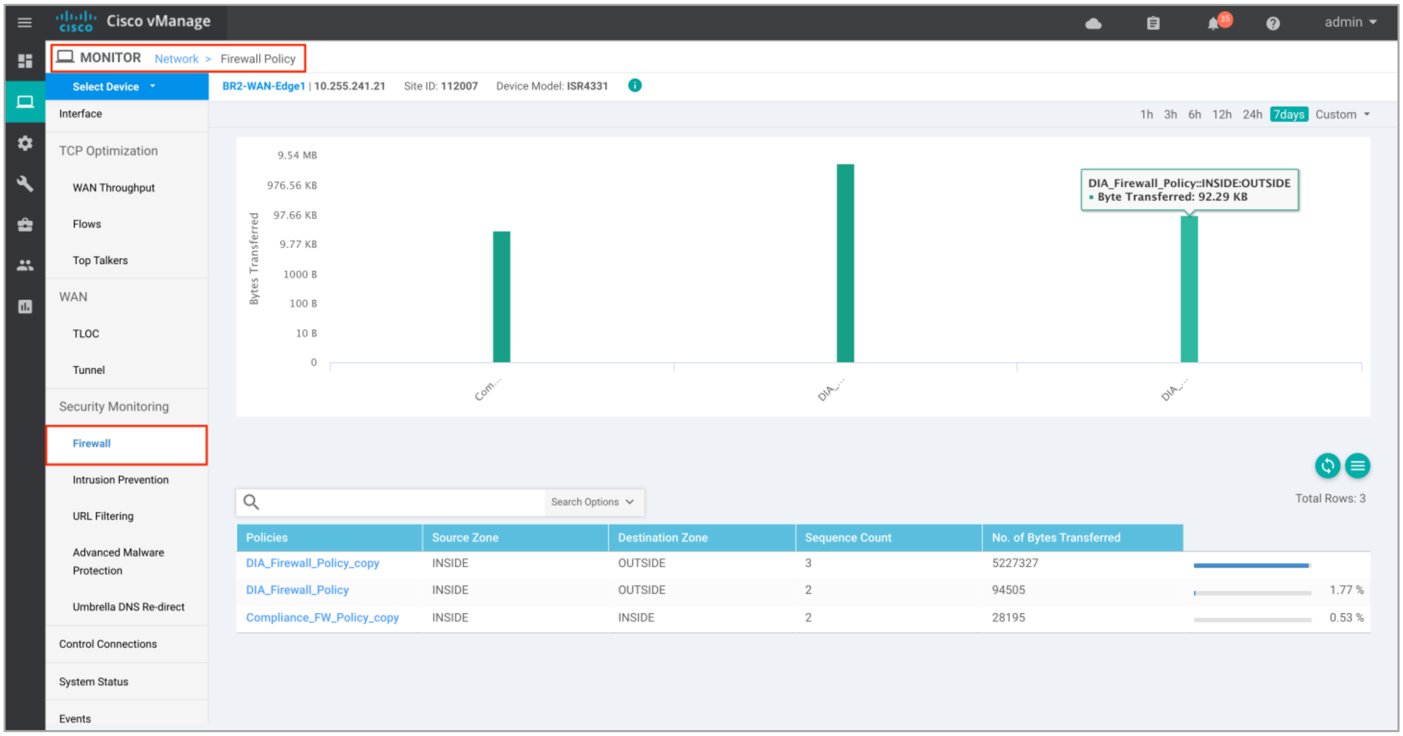
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0
BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0

Step 2. Click on a 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

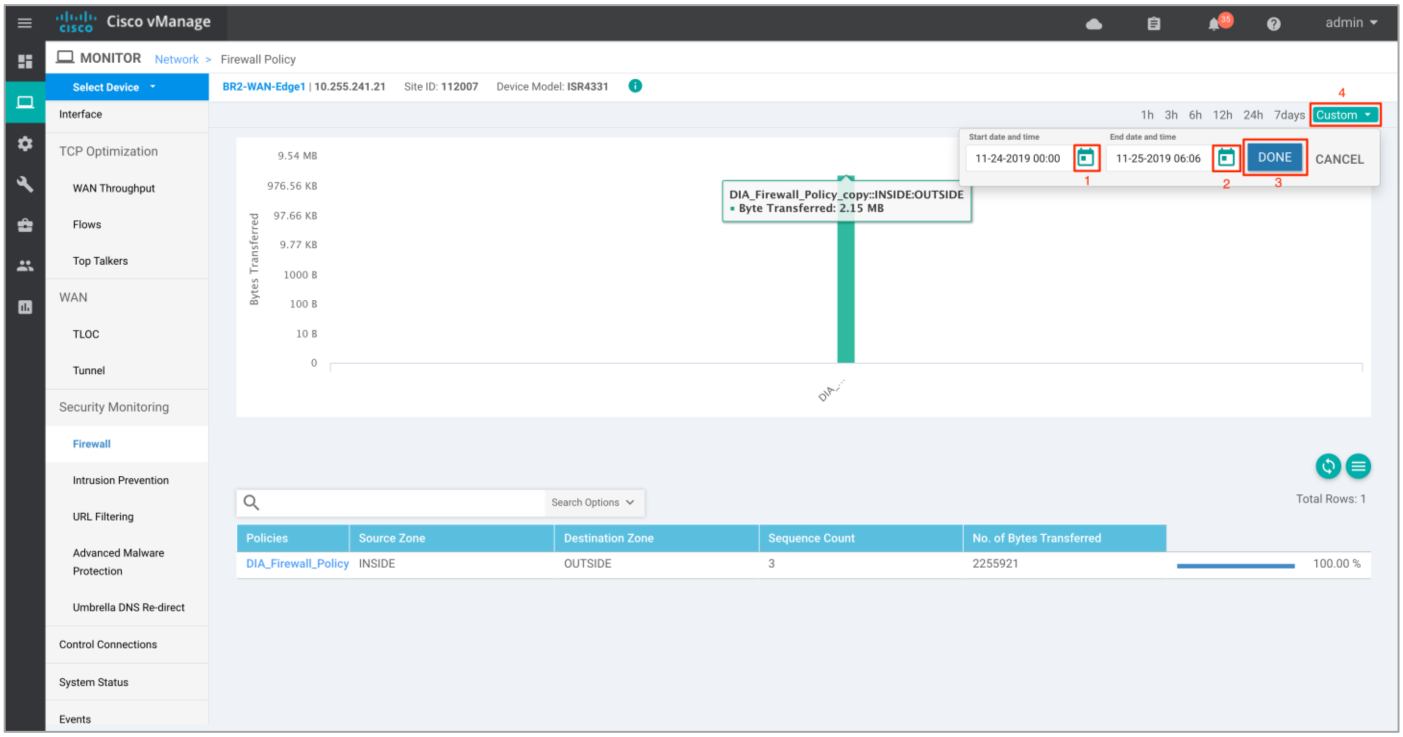
Step 3. Click on **Firewall Policy** tab under **Security Monitoring** from the left pane. Within the dashboard, you can view statistics for all the firewall policies created.



BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

Policies	Source Zone	Destination Zone	Sequence Count	No. of Bytes Transferred	
DIA_Firewall_Policy_copy	INSIDE	OUTSIDE	3	5227327	
DIA_Firewall_Policy	INSIDE	OUTSIDE	2	94505	1.77 %
Compliance_FW_Policy_copy	INSIDE	INSIDE	2	28195	0.53 %

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



Start date and time: 11-24-2019 00:00

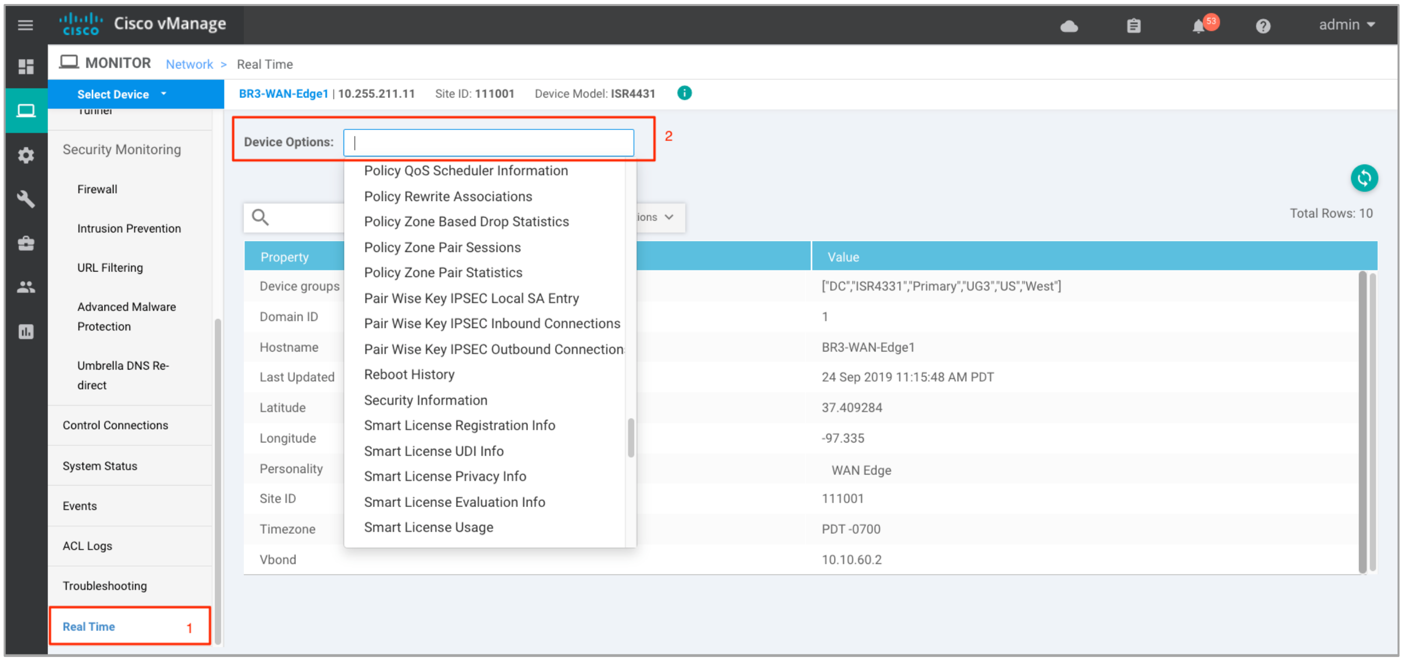
End date and time: 11-25-2019 06:06

DONE CANCEL

DIA_Firewall_Policy_copy::INSIDE:OUTSIDE
• Byte Transferred: 2.15 MB

Policies	Source Zone	Destination Zone	Sequence Count	No. of Bytes Transferred	
DIA_Firewall_Policy	INSIDE	OUTSIDE	3	2255921	100.00 %

Step 5. Click on **Real Time** from the left pane of the monitor dashboard. Within **Network** > **Real time**, a pop-up screen will appear with **Device Options**. Click on the search tab to populate a list of options that can be chosen to monitor, troubleshoot and manage your device.

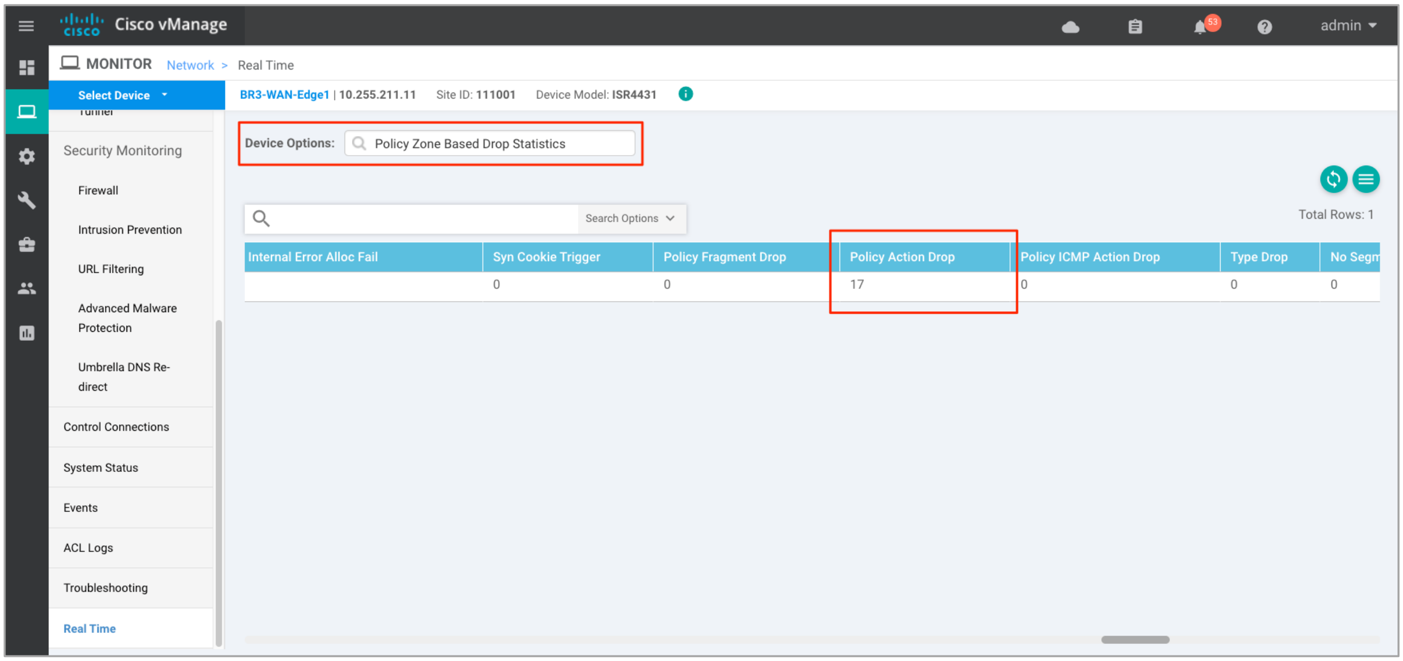


Device Options:

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

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 drop statistics, click on **Policy Zone Based Drop Statistics**. This output displays counters that explains reasons for packet drops. In the figure, notice 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

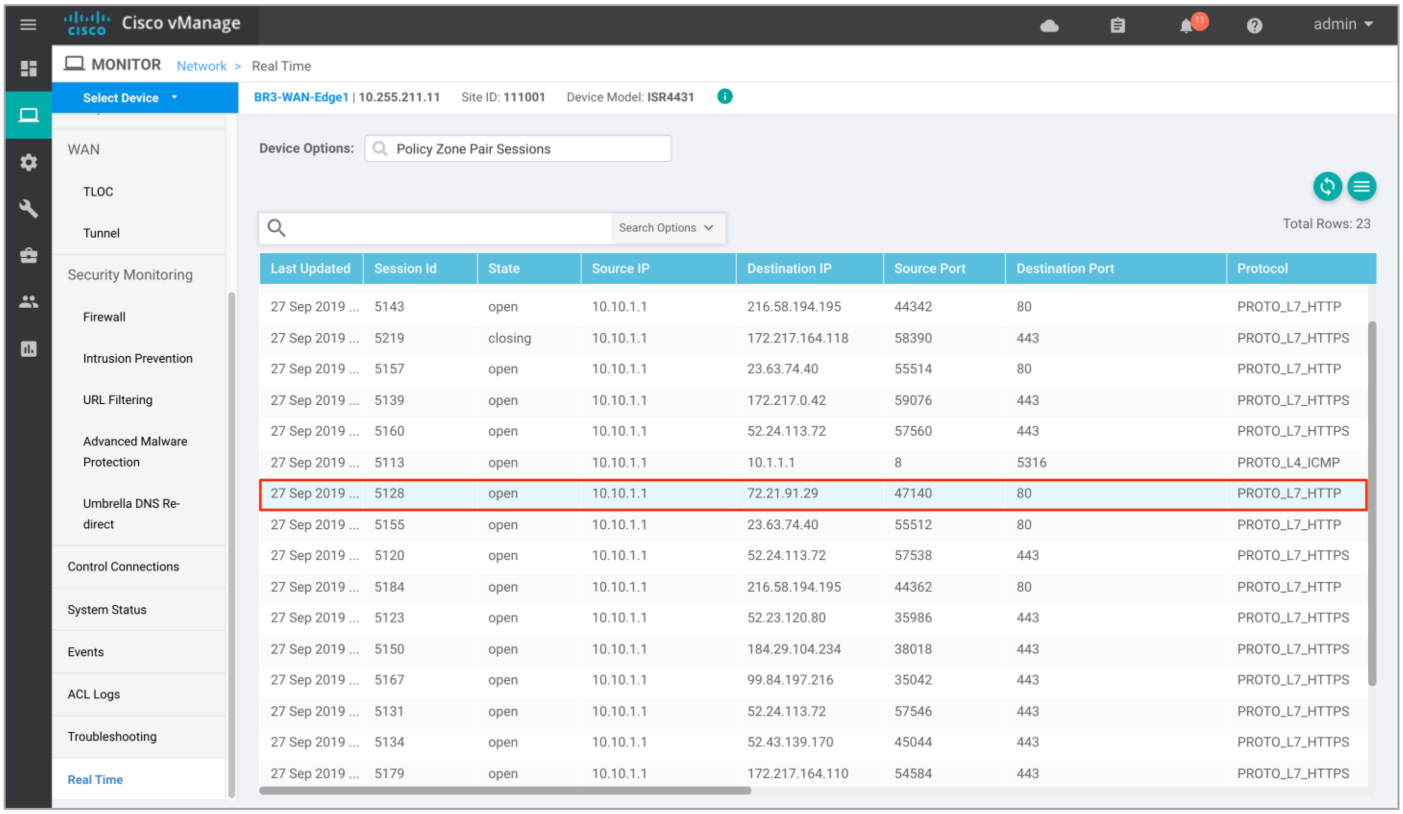
Internal Error Alloc Fail	Syn Cookie Trigger	Policy Fragment Drop	Policy Action Drop	Policy ICMP Action Drop	Type Drop	No Segm
	0	0	17	0	0	0

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 get an understanding on firewall drop reasons and explanations. Although the document caters to IOS-XE WAN Edge devices, the explanation for packet drops may be useful.

Step 7. To view the zone pair session details, click on **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 class-map which will be 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

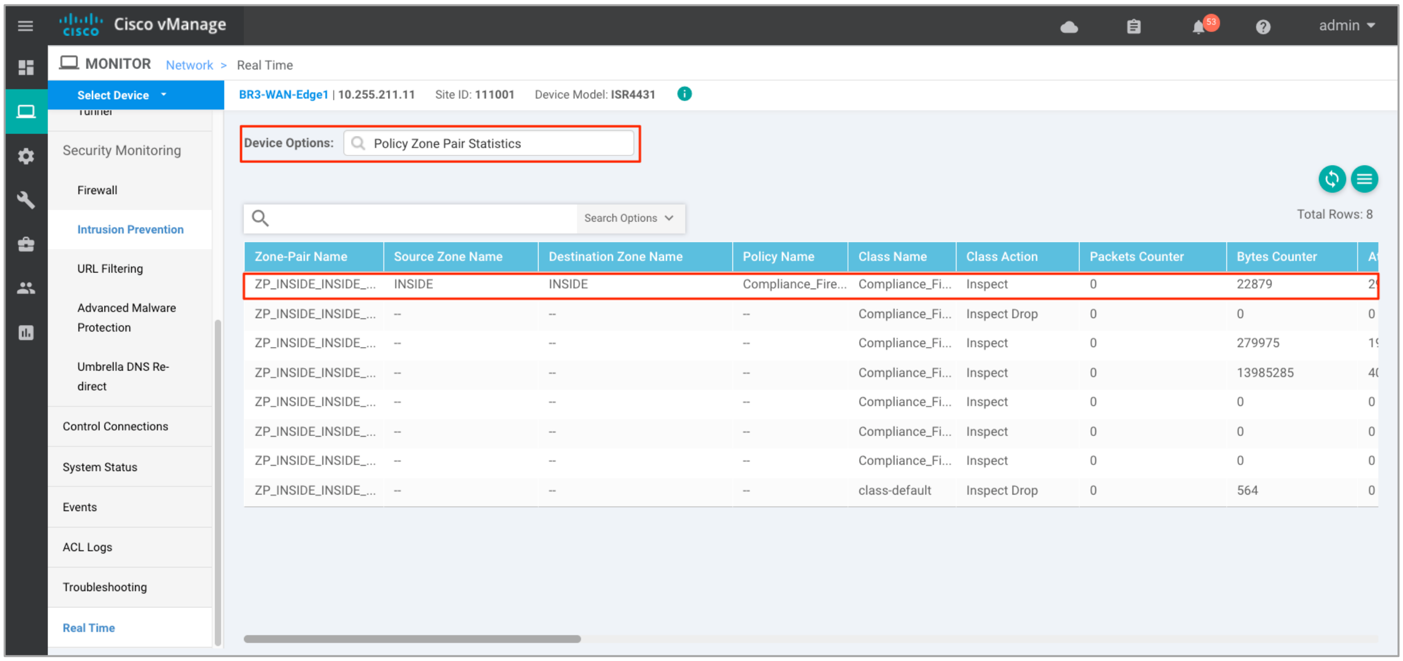
Device Options: Policy Zone Pair Sessions

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

Step 8. To view the zone pair statistics, click on **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 the action applied for two out of eight is inspect and drop.



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

Device Options: Policy Zone Pair Statistics

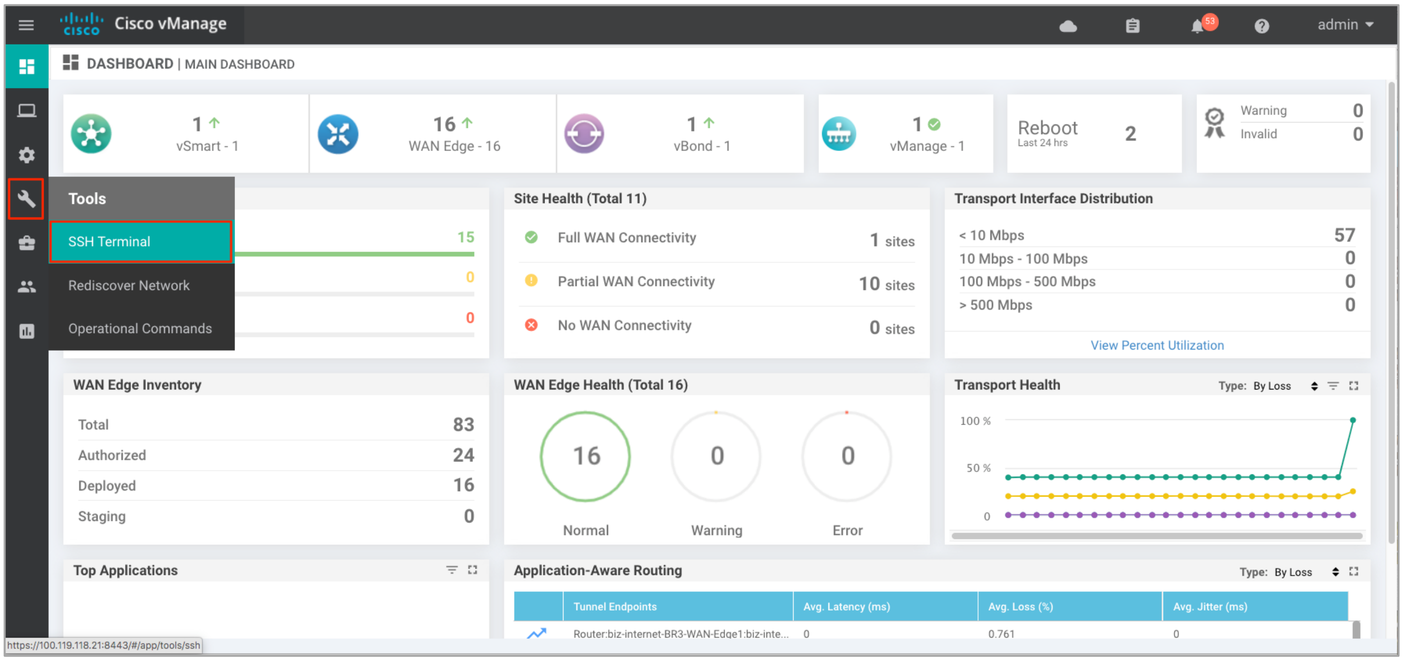
Total Rows: 8

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

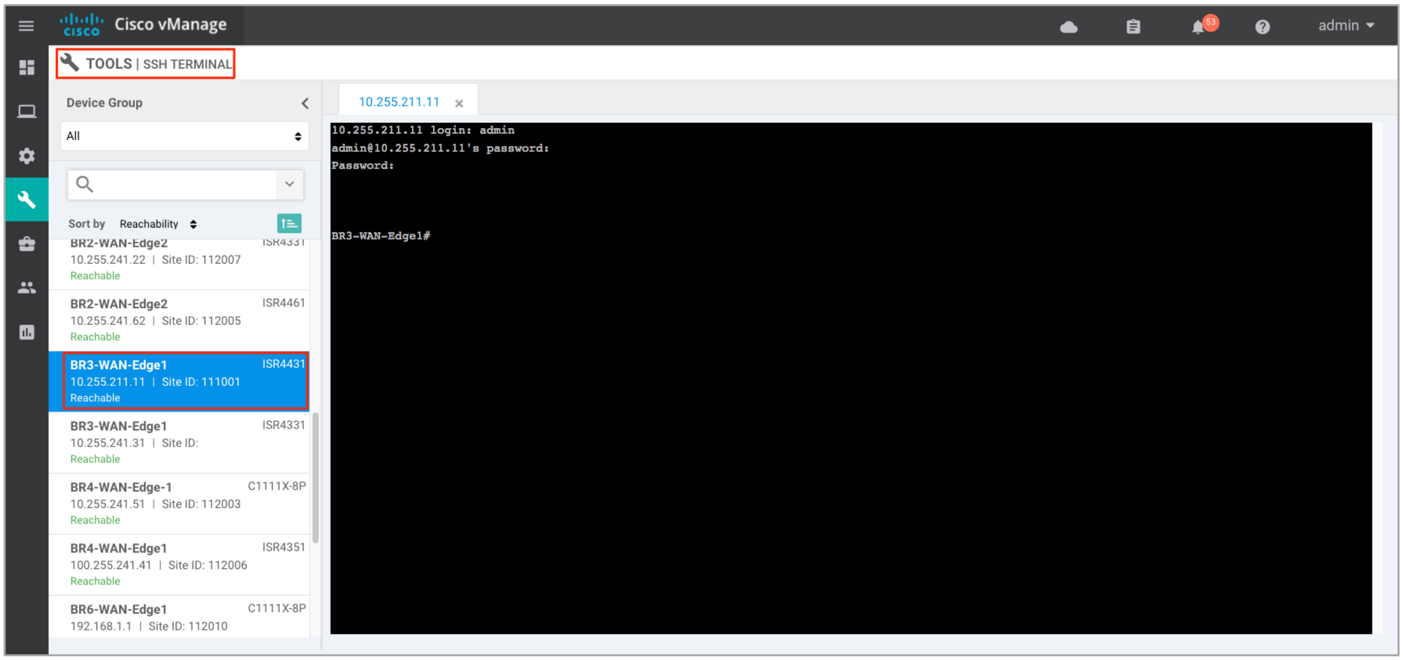
Procedure 3. Monitor the Firewall Feature and Statistics via vManage SSH Server Dashboard

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

Step 9. Navigate to **Tools** > **SSH Terminal** available on the left pane.

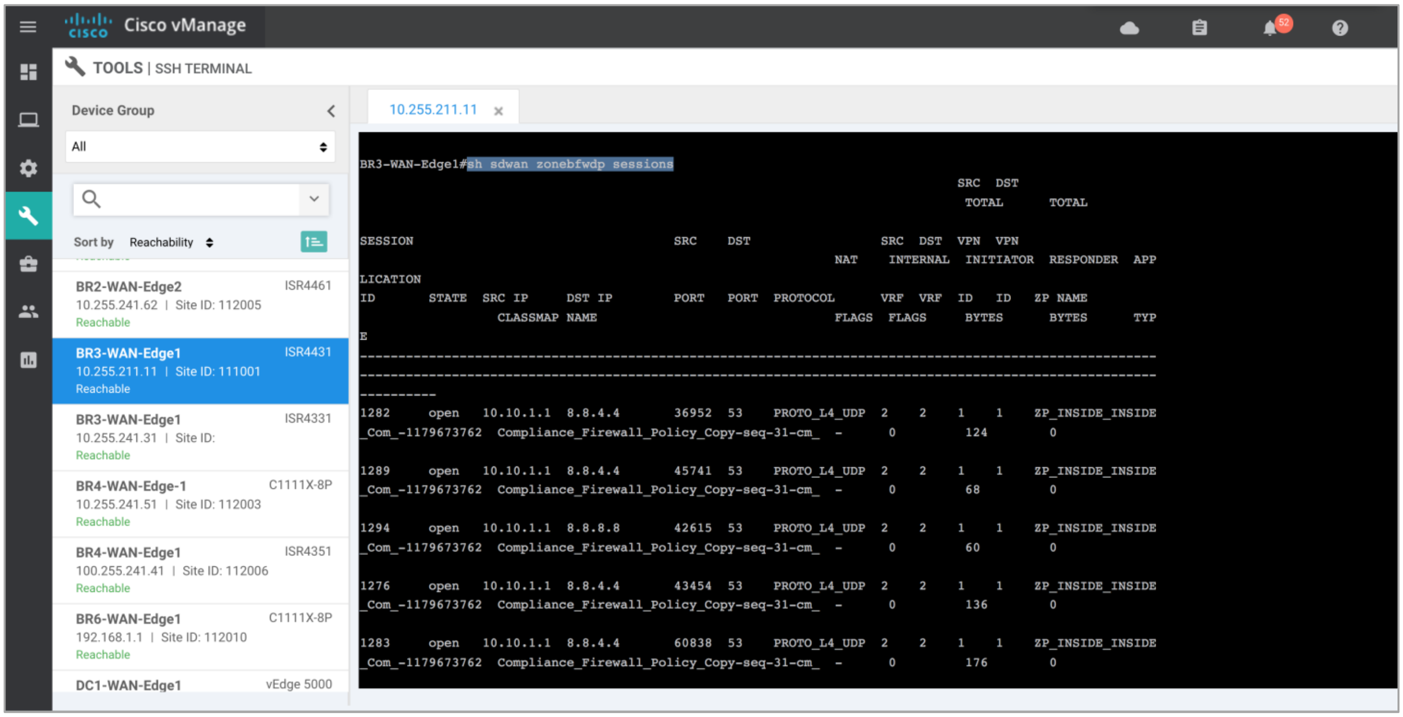


Step 10. Select the device from the list devices, and login.


Cisco vManage
admin
TOOLS | SSH TERMINAL
Device Group
All
Sort by Reachability
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
BR6-WAN-Edge1 C1111X-8P 192.168.1.1 | Site ID: 112010
10.255.211.11

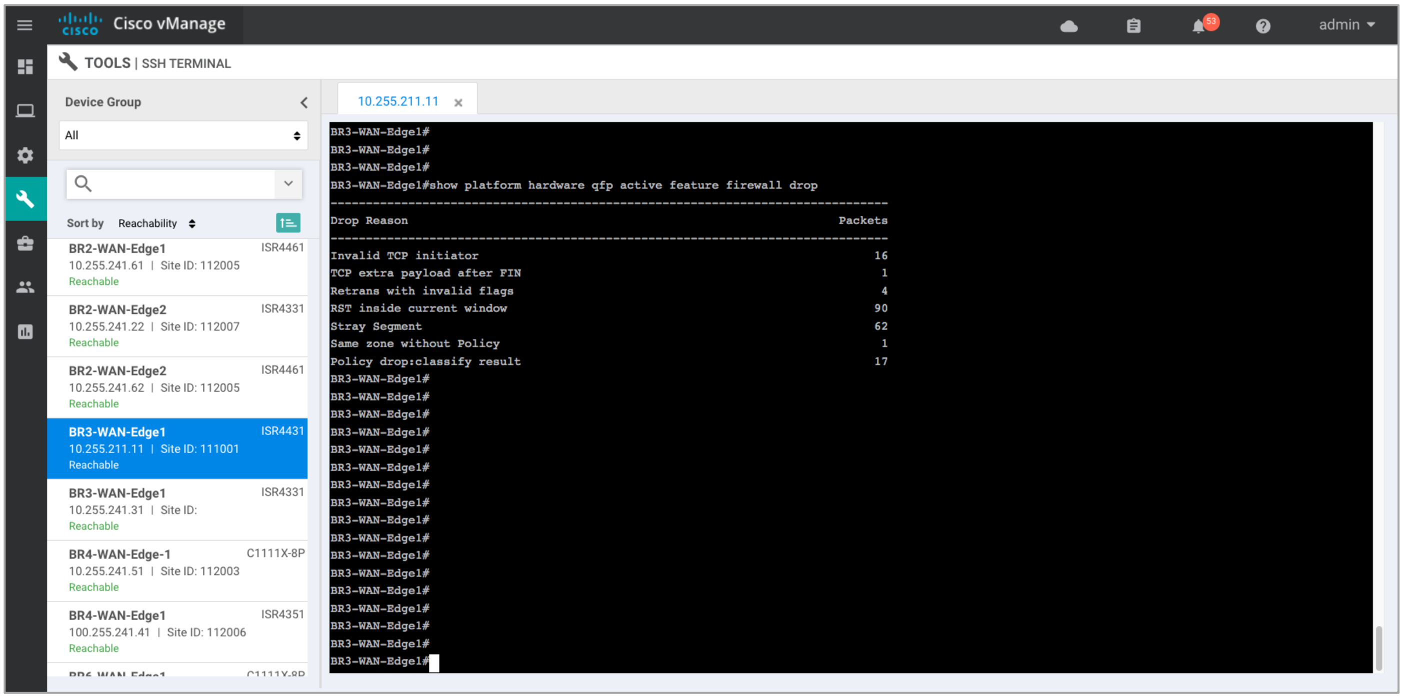
```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:



BR3-WAN-Edge1#
```

Step 11. To view the existing firewall sessions, enter the CLI command – ***Show sdwan zonebfwdp sessions***.


Cisco vManage
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
10.255.211.11

```
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 12. To view the firewall drop counters, enter the CLI command – ***Show platform hardware qfp active feature firewall drop.***

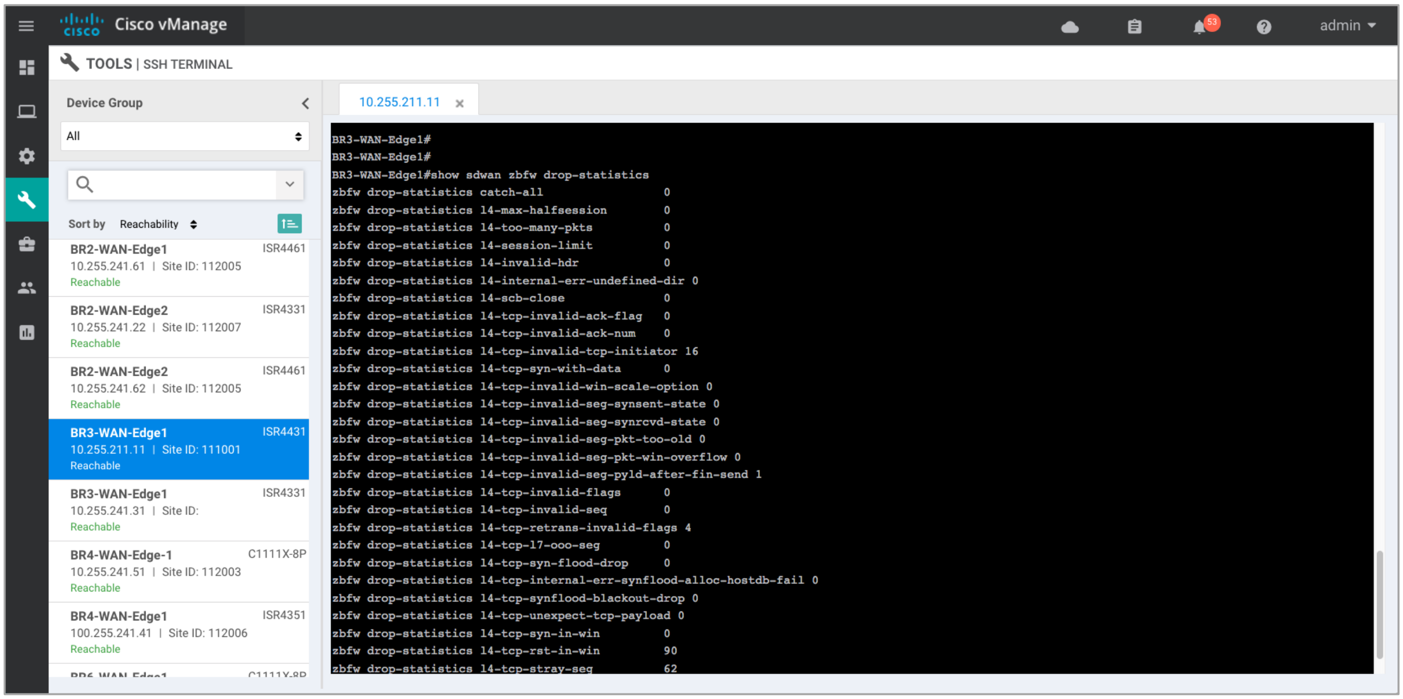

Cisco vManage
admin
TOOLS | SSH TERMINAL
Device Group
All
Sort by Reachability
BR2-WAN-Edge1 ISR4461 10.255.241.61 | Site ID: 112005 Reachable
BR2-WAN-Edge2 ISR4331 10.255.241.22 | Site ID: 112007 Reachable
BR2-WAN-Edge2 ISR4461 10.255.241.62 | Site ID: 112005 Reachable
BR3-WAN-Edge1 ISR4431 10.255.211.11 | 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

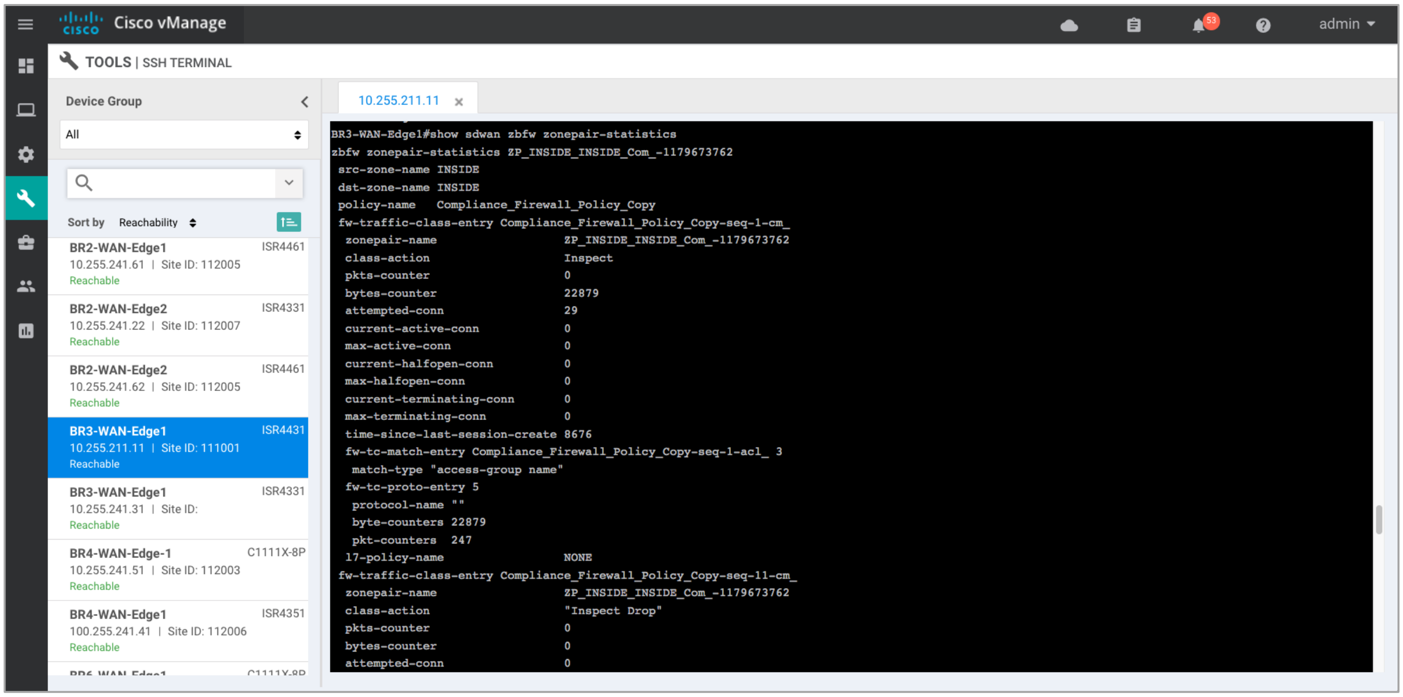
Clear the drop counters before troubleshooting firewall packet drop. To do so, use the command ***Show platform hardware qfp active feature firewall drop clear***.

Step 13. To view the overall firewall, drop statistics, enter the CLI command - ***Show sdwan zbfw drop-statistics***.



```
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 14. To view the zone-pair statistics, enter the CLI command - ***Show sdwan zbfw zonepair-statistics***.



```
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
```

Outside the listed CLI commands, some of the other useful CLI commands include ***show log*** and ***show zone security*** to view error logs and zone pairs.

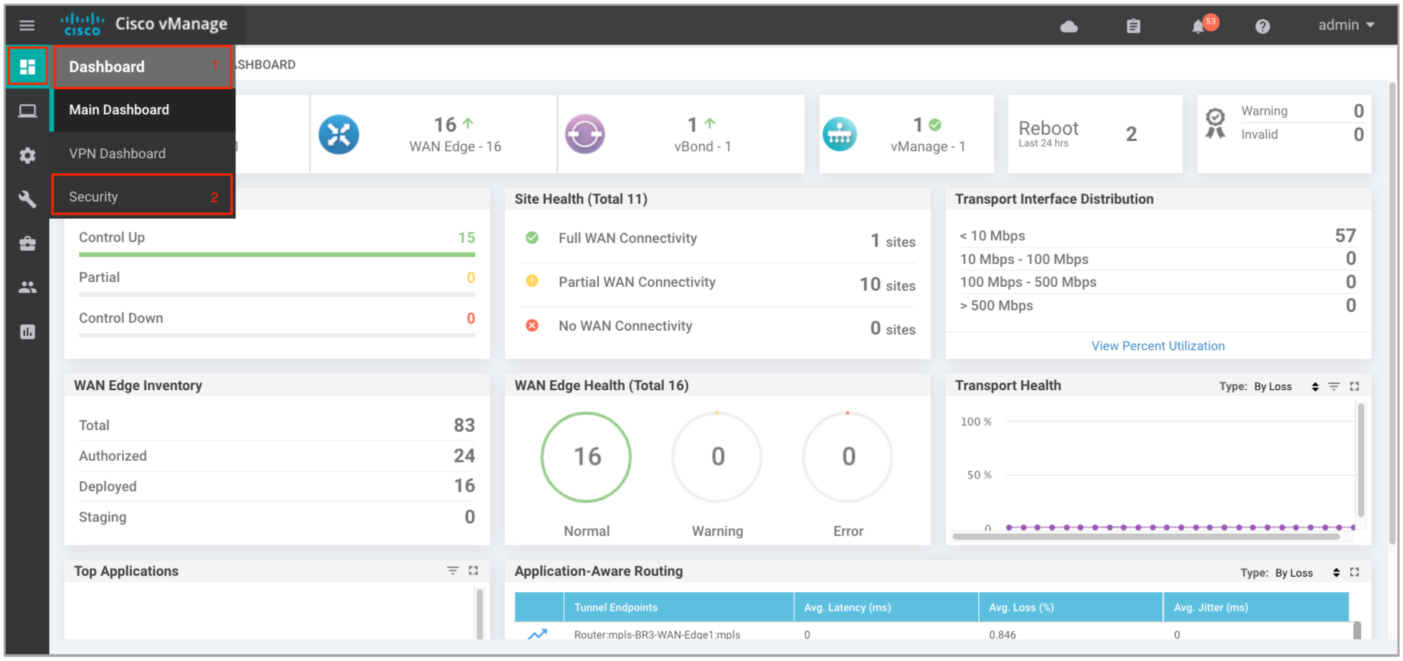
Process 2: Monitor IPS Feature via vManage NMS

Using the vManage NMS dashboard, you can monitor the IPS feature via vManage NMS.

Procedure 1. Monitor IPS Signature Violations via vManage Main Dashboard

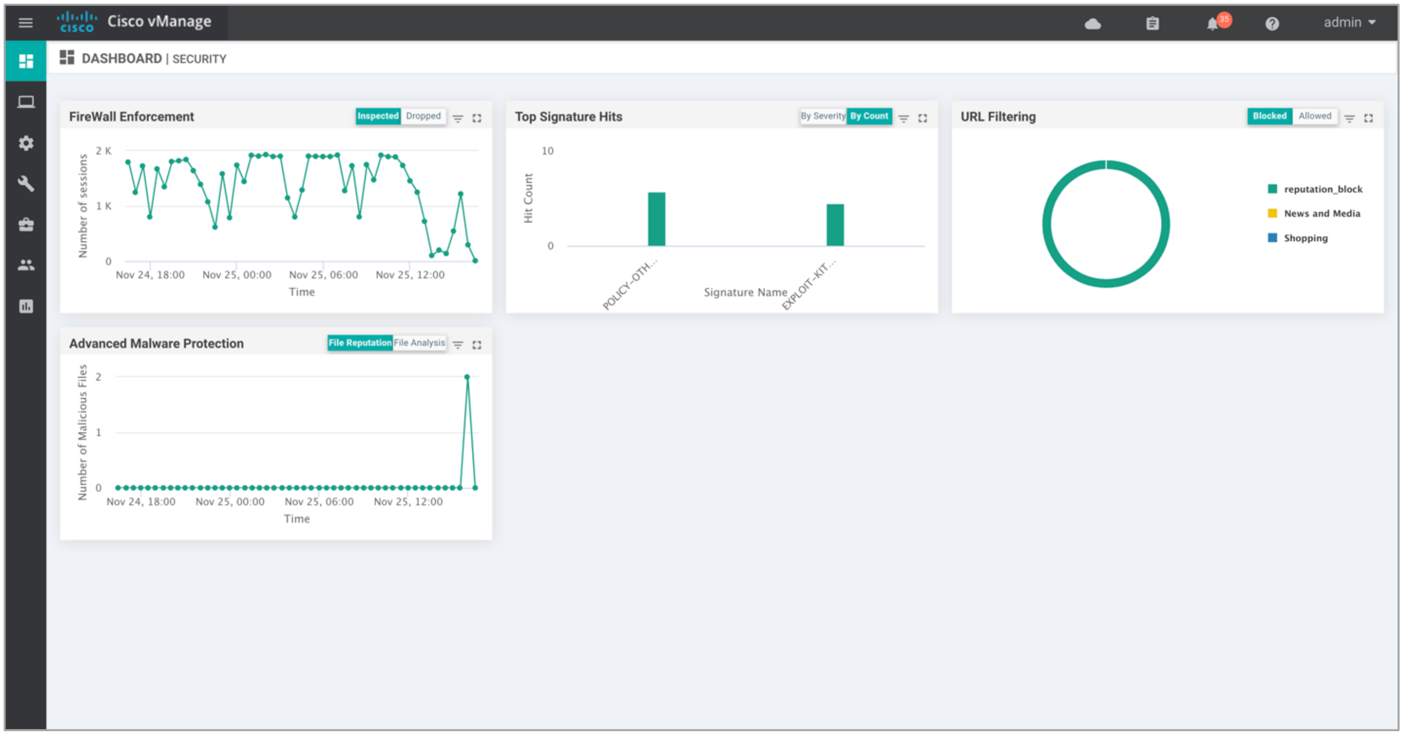
Using the vManage NMS, you can monitor the IPS Signature Violations and drill down into the vManage Main Dashboard.

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



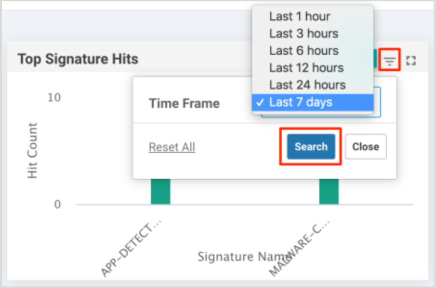
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR3-WAN-Edge1:mpls	0	0.846	0

Step 2. The following screenshot displays the overall security dashboard.

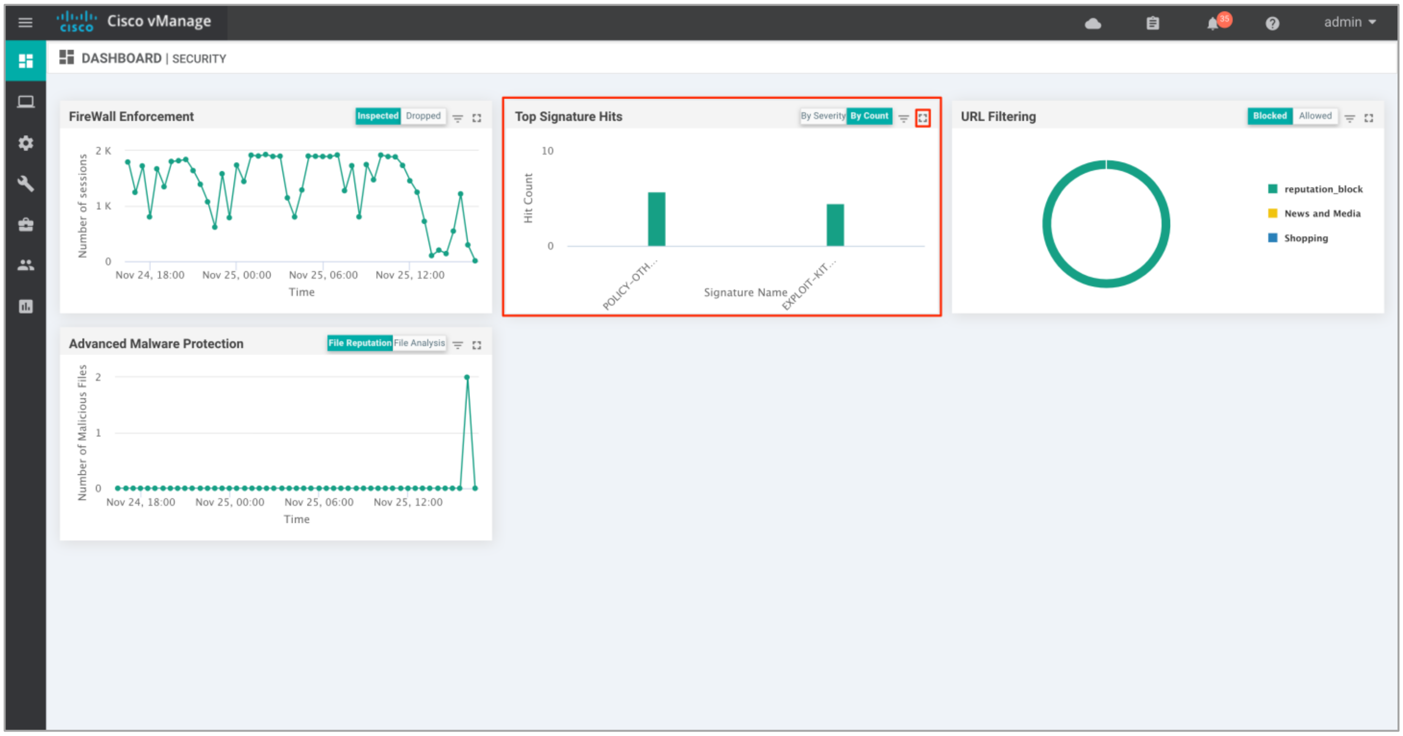


Technical Tip

Within the IPS graphical display, drill down for hourly, daily and weekly graphical representation.

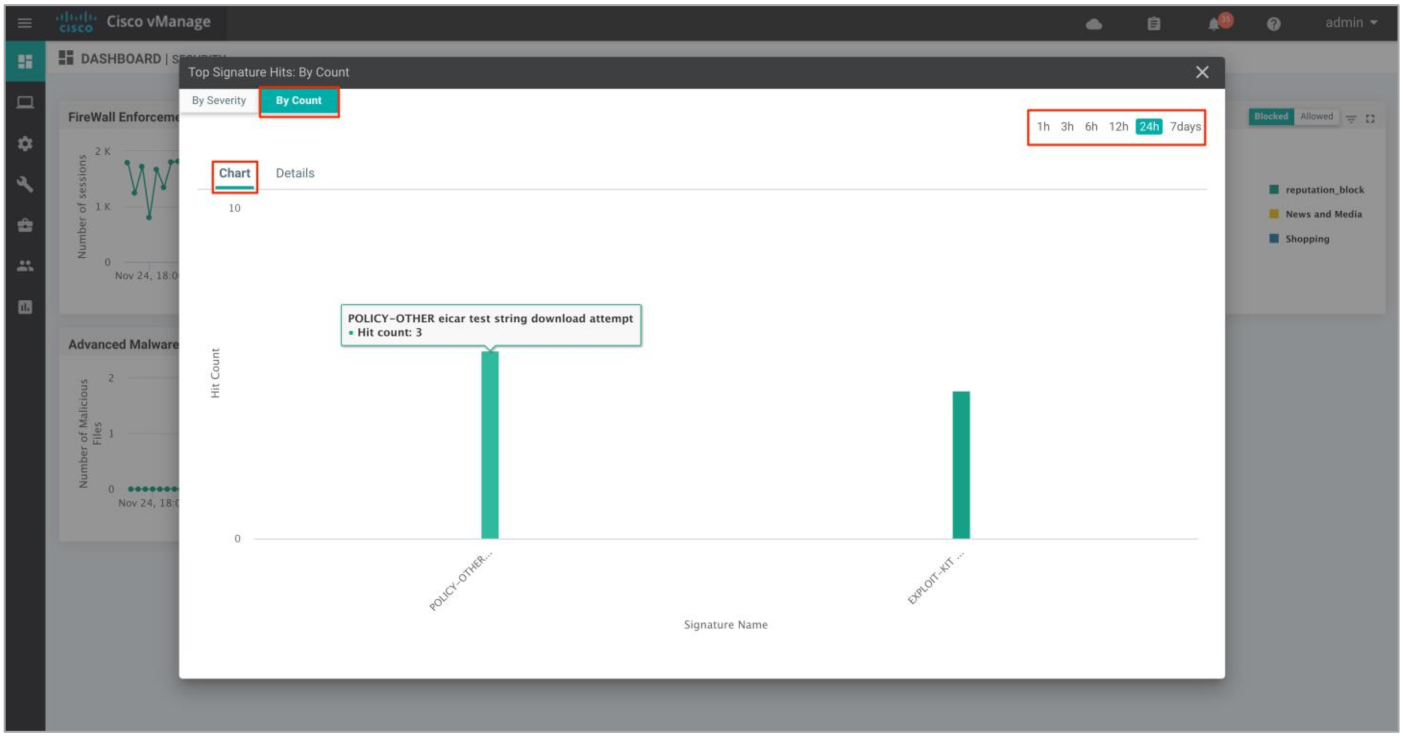


Step 3. To take a closer look into the **Top Signature Hits** graph, click on the square box **[]** on the top right.

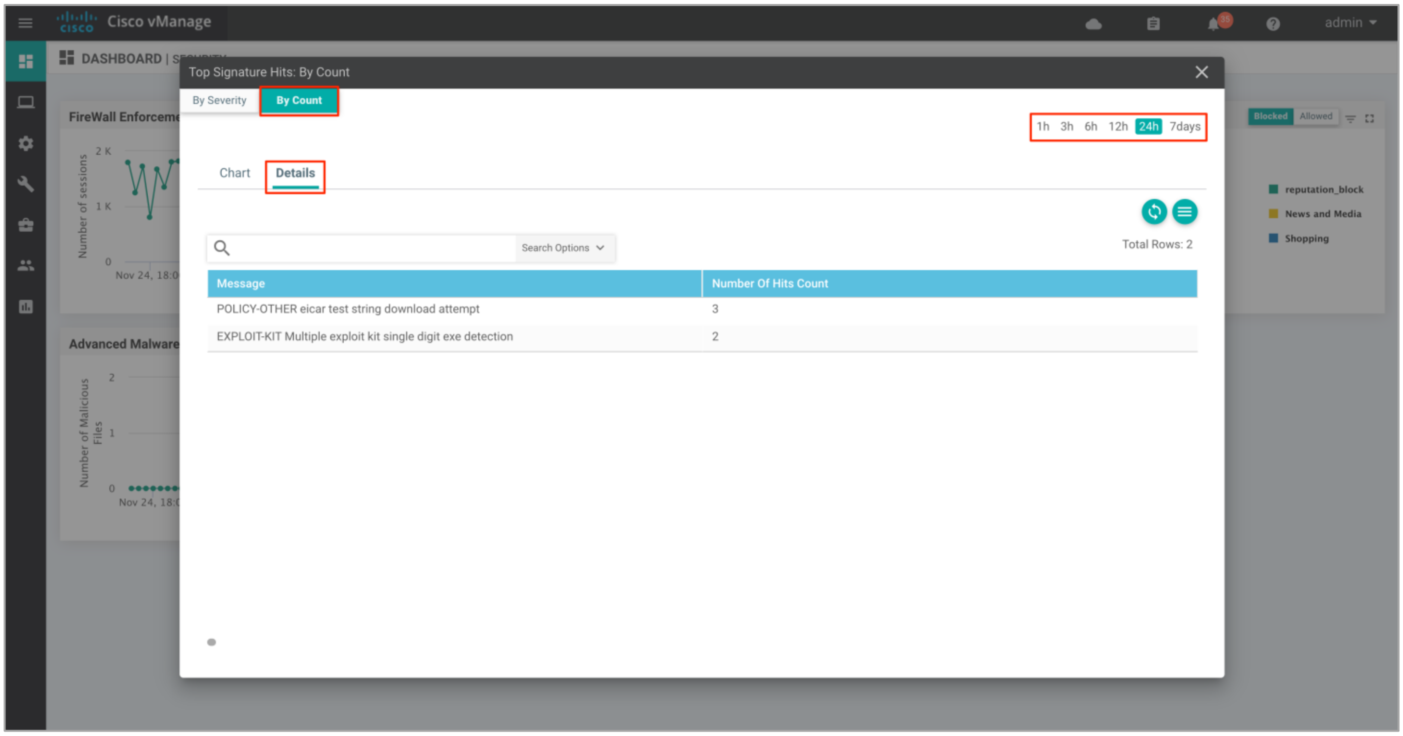


Drilling down into firewall graph provides more information. View top signature hits By Severity or By Count for 1h, 3h, 6h, 12h, 24h (default) or 7days.

Within By Count, the Chart tab displays the graphical representation of the Top Signature Hits.

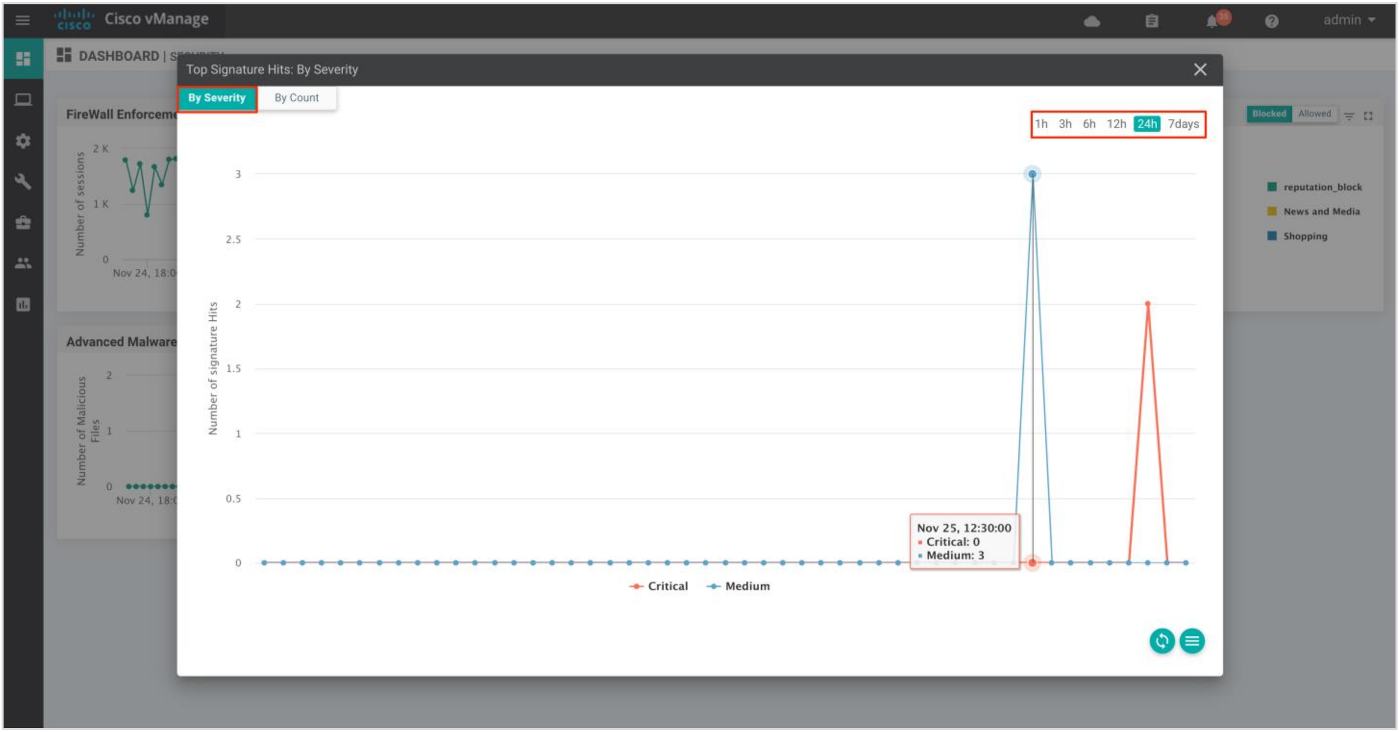


Within **By Count**, the **Details** tab displays the hit count per signature.



Message	Number Of Hits Count
POLICY-OTHER eicar test string download attempt	3
EXPLOIT-KIT Multiple exploit kit single digit exe detection	2

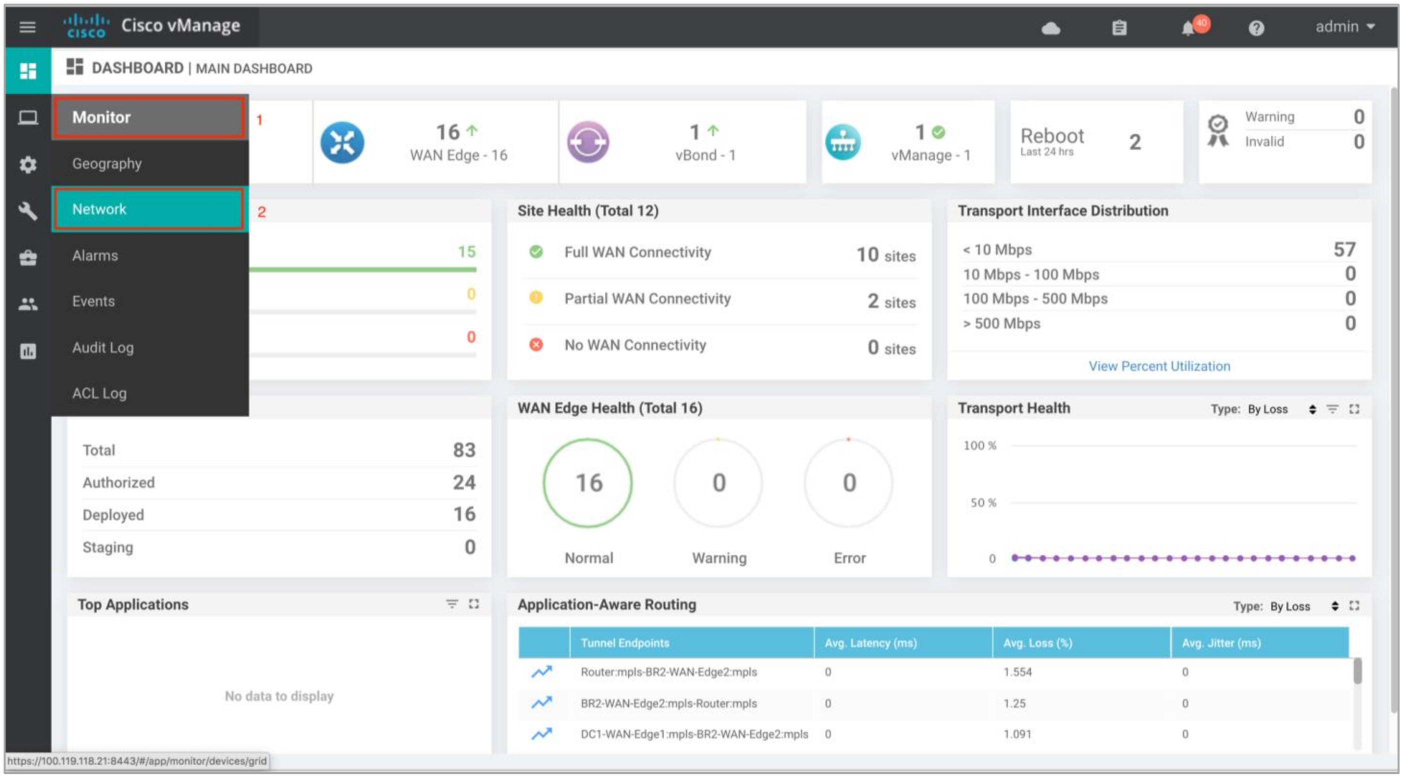
Within **By Severity**, view the number of major and minor signature hits.



Procedure 2. Monitor IPS Feature via vManage Monitor Dashboard

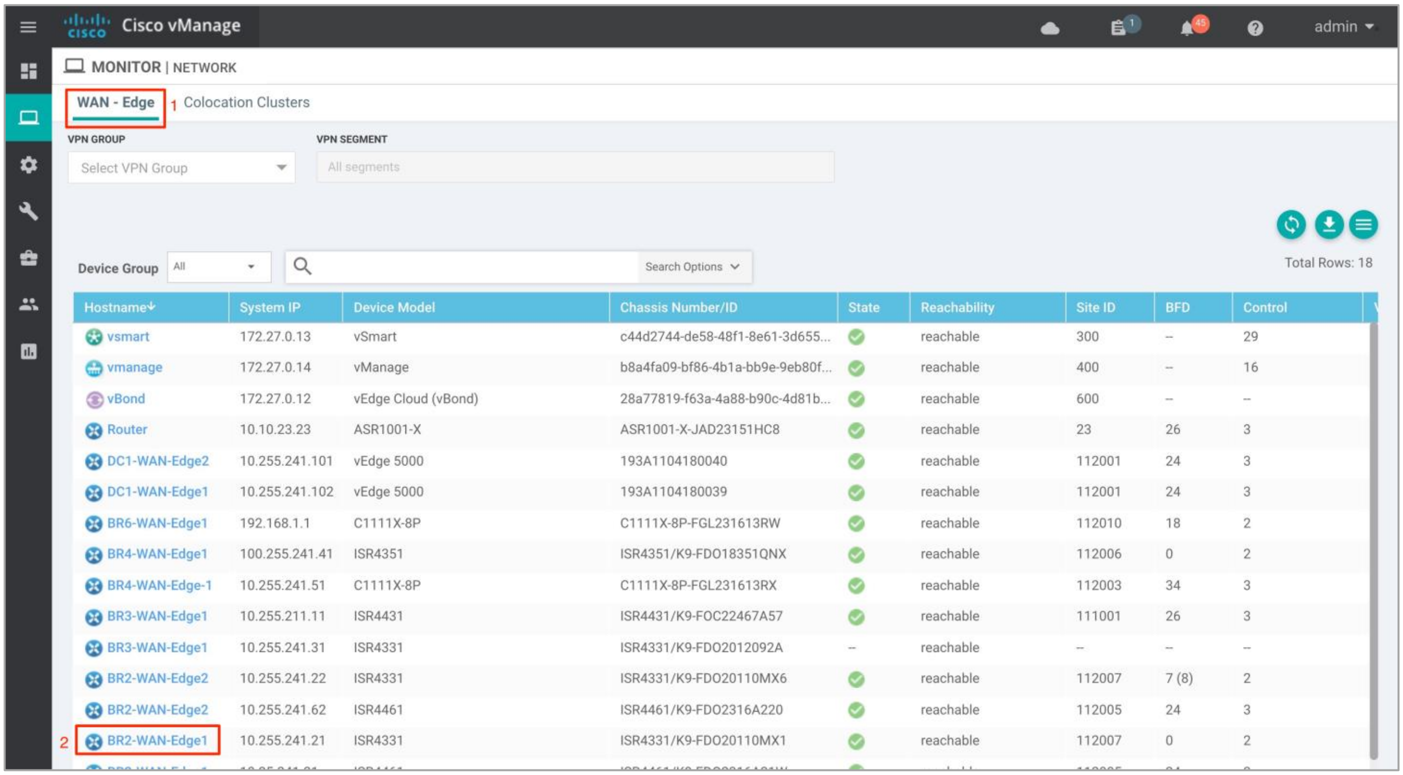
Using the vManage NMS dashboard, you can view the IPS feature via the monitor dashboard contained within vManage.

Step 1. Navigate to **Network** within **Monitor** available on the left pane and click on the WAN Edge device you wish to monitor.



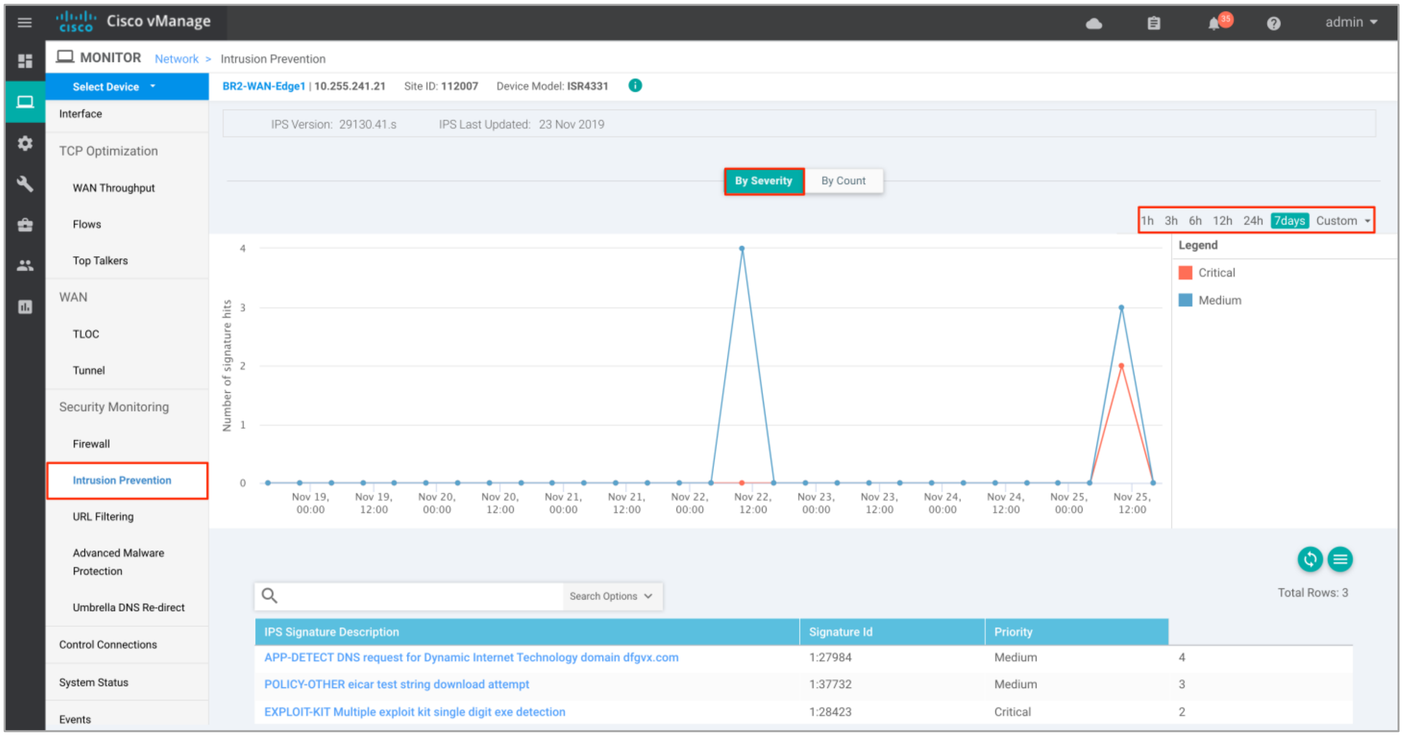
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0
BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0

Step 2. Click on a specific WAN Edge device to monitor the IPS 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 3. Click on **Intrusion Prevention** tab under **Security Monitoring** from the left pane. Within the dashboard, you can view top signature hits.

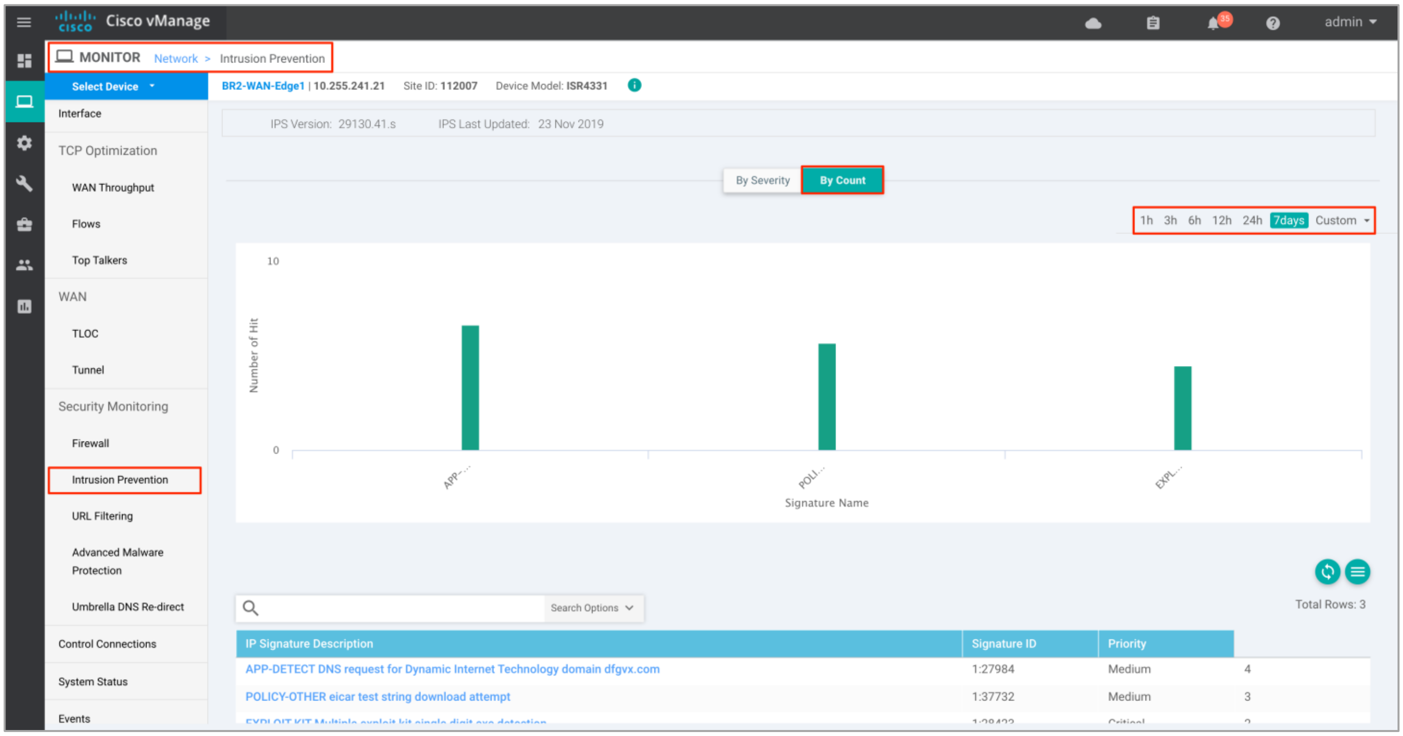


BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

IPS Version: 29130.41.s IPS Last Updated: 23 Nov 2019

IPS Signature Description	Signature Id	Priority	
APP-DETECT DNS request for Dynamic Internet Technology domain dfgvx.com	1:27984	Medium	4
POLICY-OTHER eicar test string download attempt	1:37732	Medium	3
EXPLOIT-KIT Multiple exploit kit single digit exe detection	1:28423	Critical	2

Step 4. The statistics within **Network** > **Intrusion Prevention** dashboard can be viewed either hourly, daily, weekly or for a customized period.



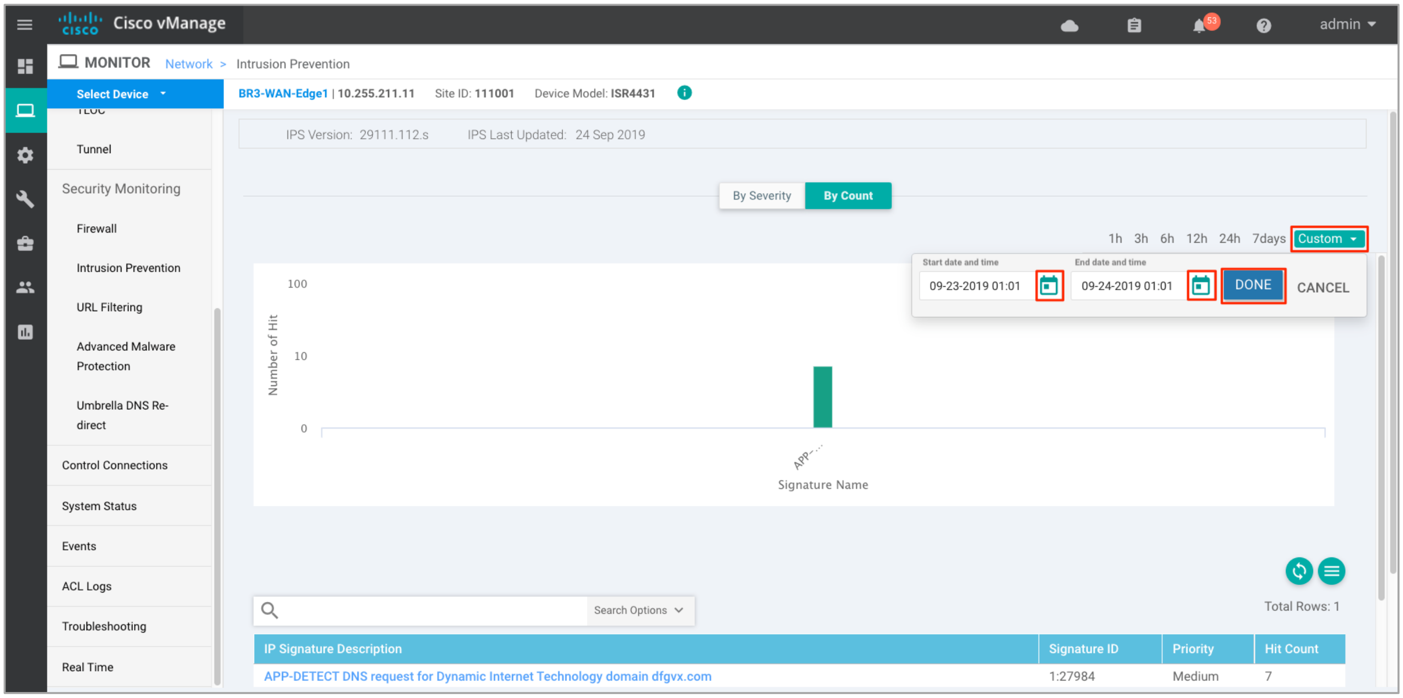
BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

IPS Version: 29130.41.s IPS Last Updated: 23 Nov 2019

Total Rows: 3

IP Signature Description	Signature ID	Priority	
APP-DETECT DNS request for Dynamic Internet Technology domain dfgvx.com	1:27984	Medium	4
POLICY-OTHER eicar test string download attempt	1:37732	Medium	3
EXPLOIT KIT Multiple exploit kit single digit exe detection	1:28423	Critical	2

Step 5. To customize the time period, select **Custom** and click on 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

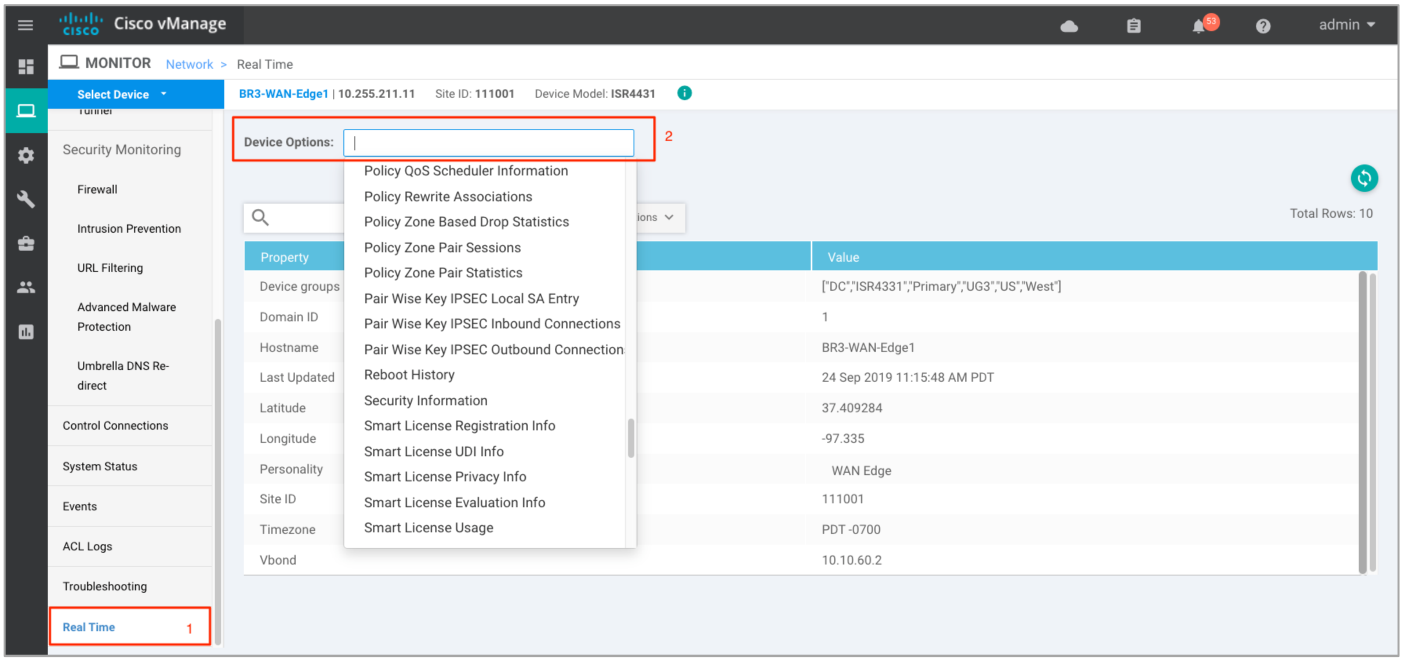
Start date and time: 09-23-2019 01:01

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

Total Rows: 1

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

Step 6. Next, click on **Real Time** from the left pane. Within **Network** > **Real time** and pop-up screen will appear with **Device Options.** Click on 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
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

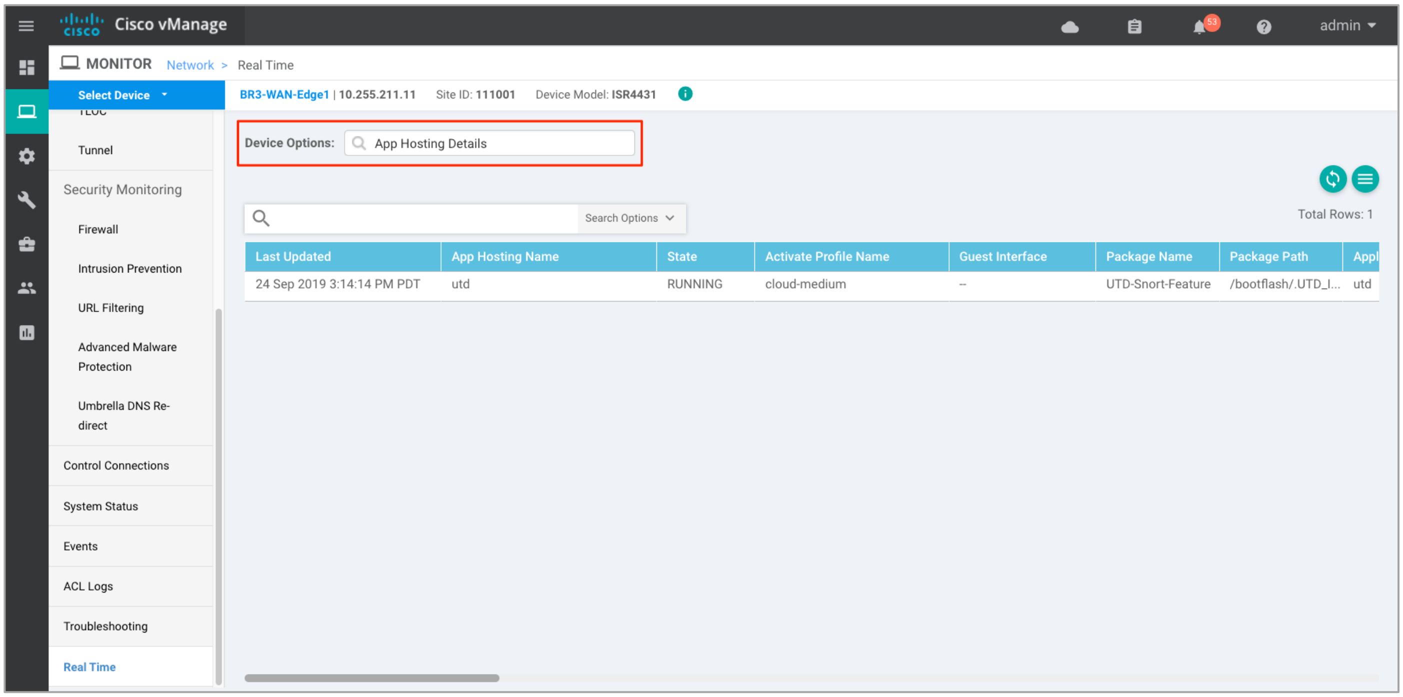
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

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 7. To view the details regarding the App hosting such as the state, package name, application installed version, memory and CPU reservation, click on **App Hosting Details**.



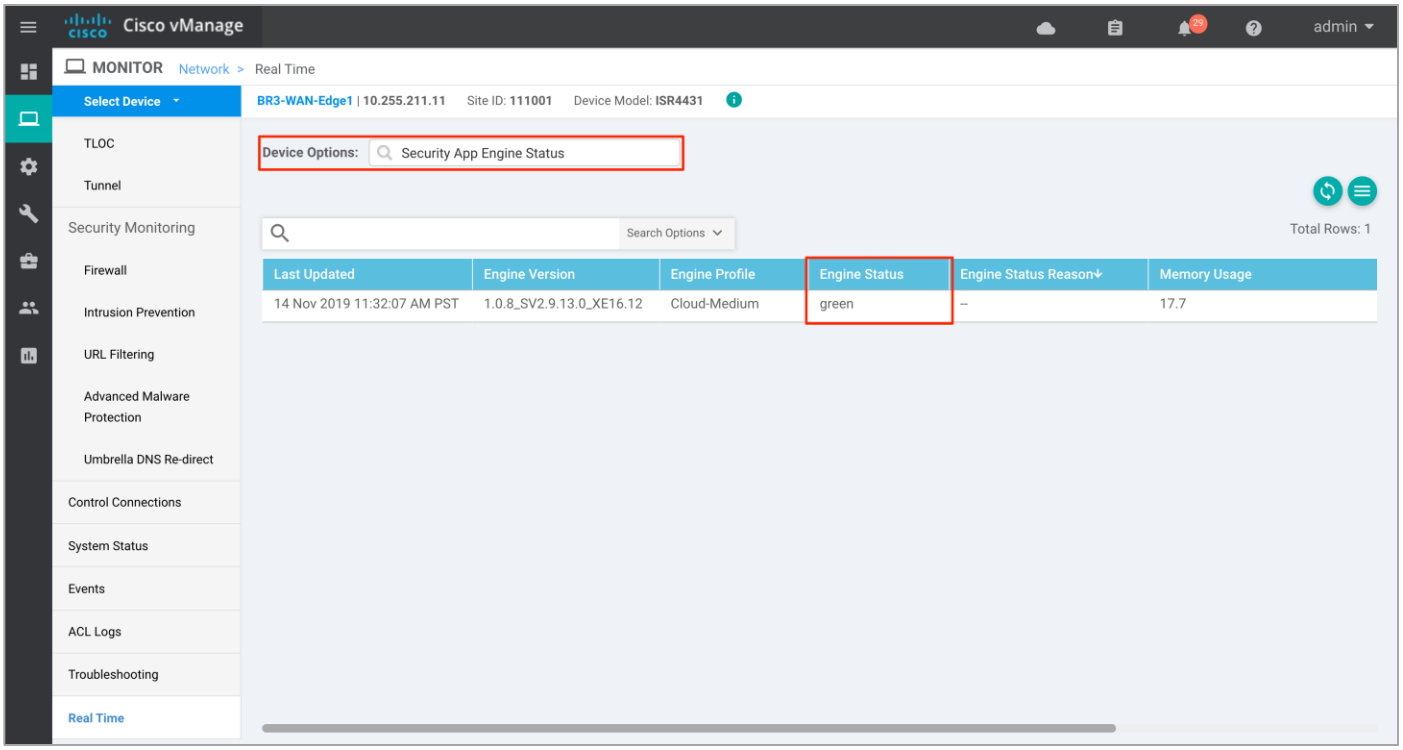
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

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 8. 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.



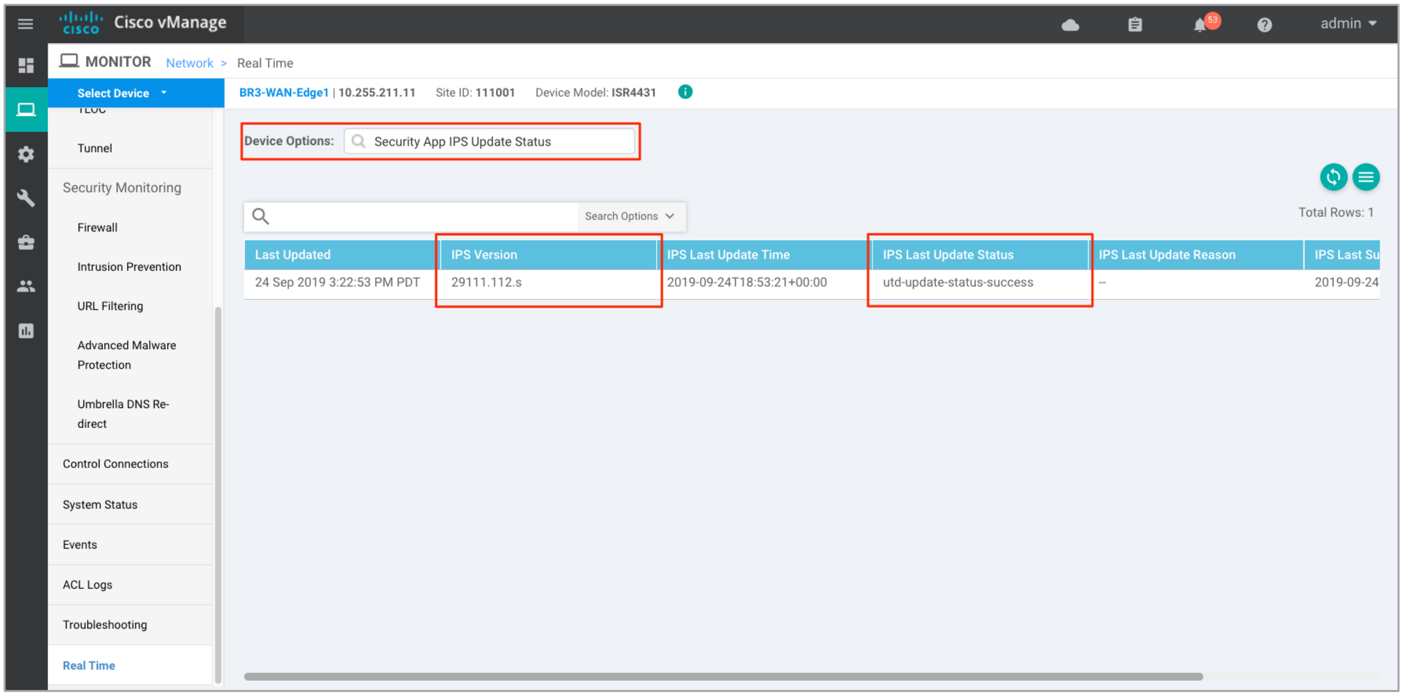
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

Device Options: Security App Engine Status

Total Rows: 1

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 9. To view the IPS signature update status, click **Security App IPS Update Status.** Ensure the IPS version ends with a .s (subscriber signature set) and not a .c (community signature set). 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

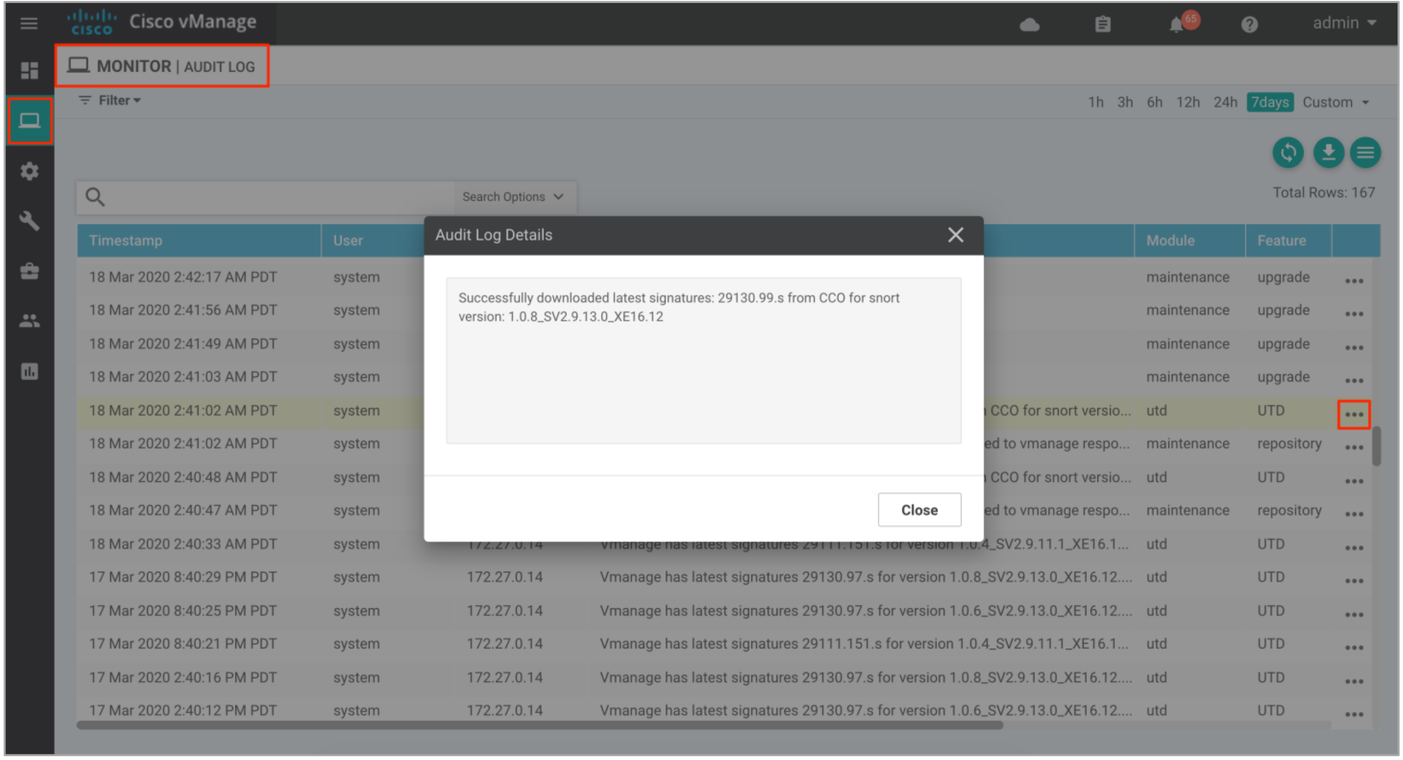
Total Rows: 1

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

Step 10. To make sure signature download from vManage to WAN Edge device was successful, navigate to **Monitor** and click on **Audit Log.** Within the logs, click on the three dot **(...)** that is located on the right end of each log statement. The pop-up screen will display either of these messages,

- Successfully downloaded latest signatures: <signature.s> from CCO for snort version: <UTD version>

This indicates the download of the signature set was successful.



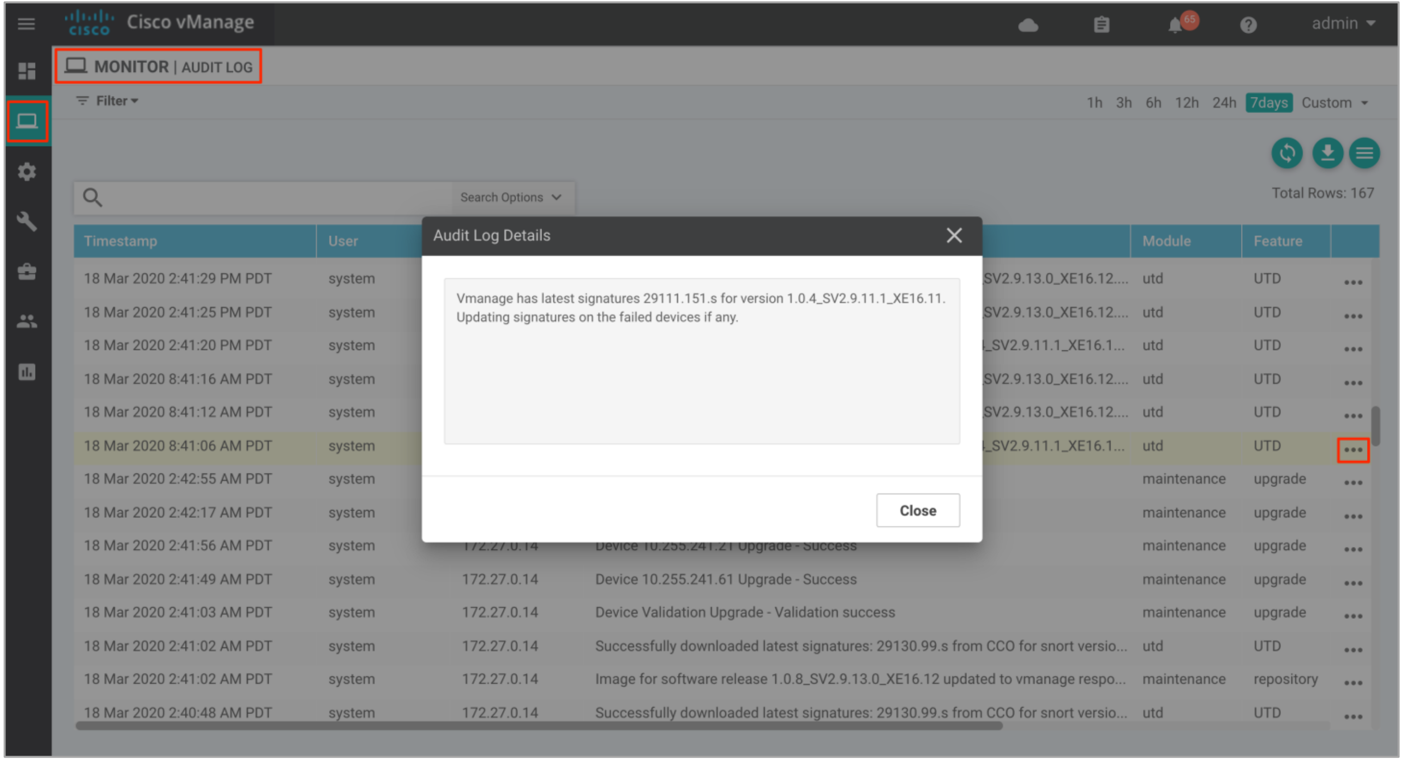
Audit Log Details

Successfully downloaded latest signatures: 29130.99.s from CCO for snort version: 1.0.8_SV2.9.13.0_XE16.12

Timestamp	User			Module	Feature
18 Mar 2020 2:42:17 AM PDT	system			maintenance	upgrade
18 Mar 2020 2:41:56 AM PDT	system			maintenance	upgrade
18 Mar 2020 2:41:49 AM PDT	system			maintenance	upgrade
18 Mar 2020 2:41:03 AM PDT	system			maintenance	upgrade
18 Mar 2020 2:41:02 AM PDT	system		CCO for snort versio...	utd	UTD
18 Mar 2020 2:41:02 AM PDT	system		ed to vmanage respo...	maintenance	repository
18 Mar 2020 2:40:48 AM PDT	system		CCO for snort versio...	utd	UTD
18 Mar 2020 2:40:47 AM PDT	system		ed to vmanage respo...	maintenance	repository
18 Mar 2020 2:40:33 AM PDT	system	172.27.0.14	Vmanage has latest signatures 29111.151.s for version 1.0.4_SV2.9.11.1_XE16.1...	utd	UTD
17 Mar 2020 8:40:29 PM PDT	system	172.27.0.14	Vmanage has latest signatures 29130.97.s for version 1.0.8_SV2.9.13.0_XE16.12....	utd	UTD
17 Mar 2020 8:40:25 PM PDT	system	172.27.0.14	Vmanage has latest signatures 29130.97.s for version 1.0.6_SV2.9.13.0_XE16.12....	utd	UTD
17 Mar 2020 8:40:21 PM PDT	system	172.27.0.14	Vmanage has latest signatures 29111.151.s for version 1.0.4_SV2.9.11.1_XE16.1...	utd	UTD
17 Mar 2020 2:40:16 PM PDT	system	172.27.0.14	Vmanage has latest signatures 29130.97.s for version 1.0.8_SV2.9.13.0_XE16.12....	utd	UTD
17 Mar 2020 2:40:12 PM PDT	system	172.27.0.14	Vmanage has latest signatures 29130.97.s for version 1.0.6_SV2.9.13.0_XE16.12....	utd	UTD

- vManage has latest signatures <signature.s> for version <UTD version>. Updating signatures on the failed devices if any

  This indicates the WAN Edge device is already running the latest signature set and hence the signature set need no further update.



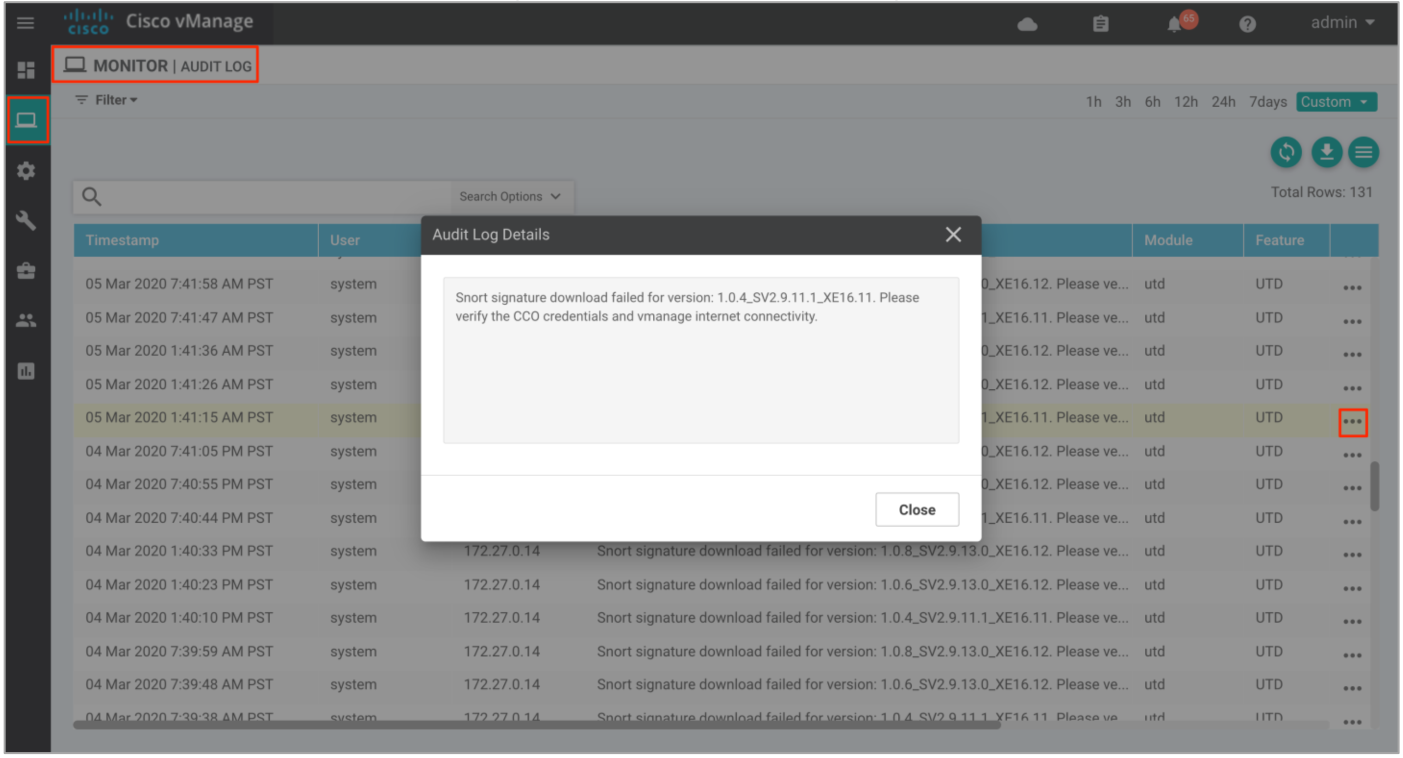
Audit Log Details

Vmanage has latest signatures 29111.151.s for version 1.0.4_SV2.9.11.1_XE16.11. Updating signatures on the failed devices if any.

Timestamp	User			Module	Feature
18 Mar 2020 2:41:29 PM PDT	system		SV2.9.13.0_XE16.12....	utd	UTD
18 Mar 2020 2:41:25 PM PDT	system		SV2.9.13.0_XE16.12....	utd	UTD
18 Mar 2020 2:41:20 PM PDT	system		_SV2.9.11.1_XE16.1...	utd	UTD
18 Mar 2020 8:41:16 AM PDT	system		SV2.9.13.0_XE16.12....	utd	UTD
18 Mar 2020 8:41:12 AM PDT	system		SV2.9.13.0_XE16.12....	utd	UTD
18 Mar 2020 8:41:06 AM PDT	system		_SV2.9.11.1_XE16.1...	utd	UTD
18 Mar 2020 2:42:55 AM PDT	system			maintenance	upgrade
18 Mar 2020 2:42:17 AM PDT	system			maintenance	upgrade
18 Mar 2020 2:41:56 AM PDT	system	172.27.0.14	Device 10.255.241.21 Upgrade - Success	maintenance	upgrade
18 Mar 2020 2:41:49 AM PDT	system	172.27.0.14	Device 10.255.241.61 Upgrade - Success	maintenance	upgrade
18 Mar 2020 2:41:03 AM PDT	system	172.27.0.14	Device Validation Upgrade - Validation success	maintenance	upgrade
18 Mar 2020 2:41:02 AM PDT	system	172.27.0.14	Successfully downloaded latest signatures: 29130.99.s from CCO for snort versio...	utd	UTD
18 Mar 2020 2:41:02 AM PDT	system	172.27.0.14	Image for software release 1.0.8_SV2.9.13.0_XE16.12 updated to vmanage respo...	maintenance	repository
18 Mar 2020 2:40:48 AM PDT	system	172.27.0.14	Successfully downloaded latest signatures: 29130.99.s from CCO for snort versio...	utd	UTD

- Snort signature download failed for version:<UTD version>. Please verify the CCO credentials and vManage internet connectivity

  This indicates that the automatic signature download from vManage has failed.



Audit Log Details

Snort signature download failed for version: 1.0.4_SV2.9.11.1_XE16.11. Please verify the CCO credentials and vmanage internet connectivity.

Close

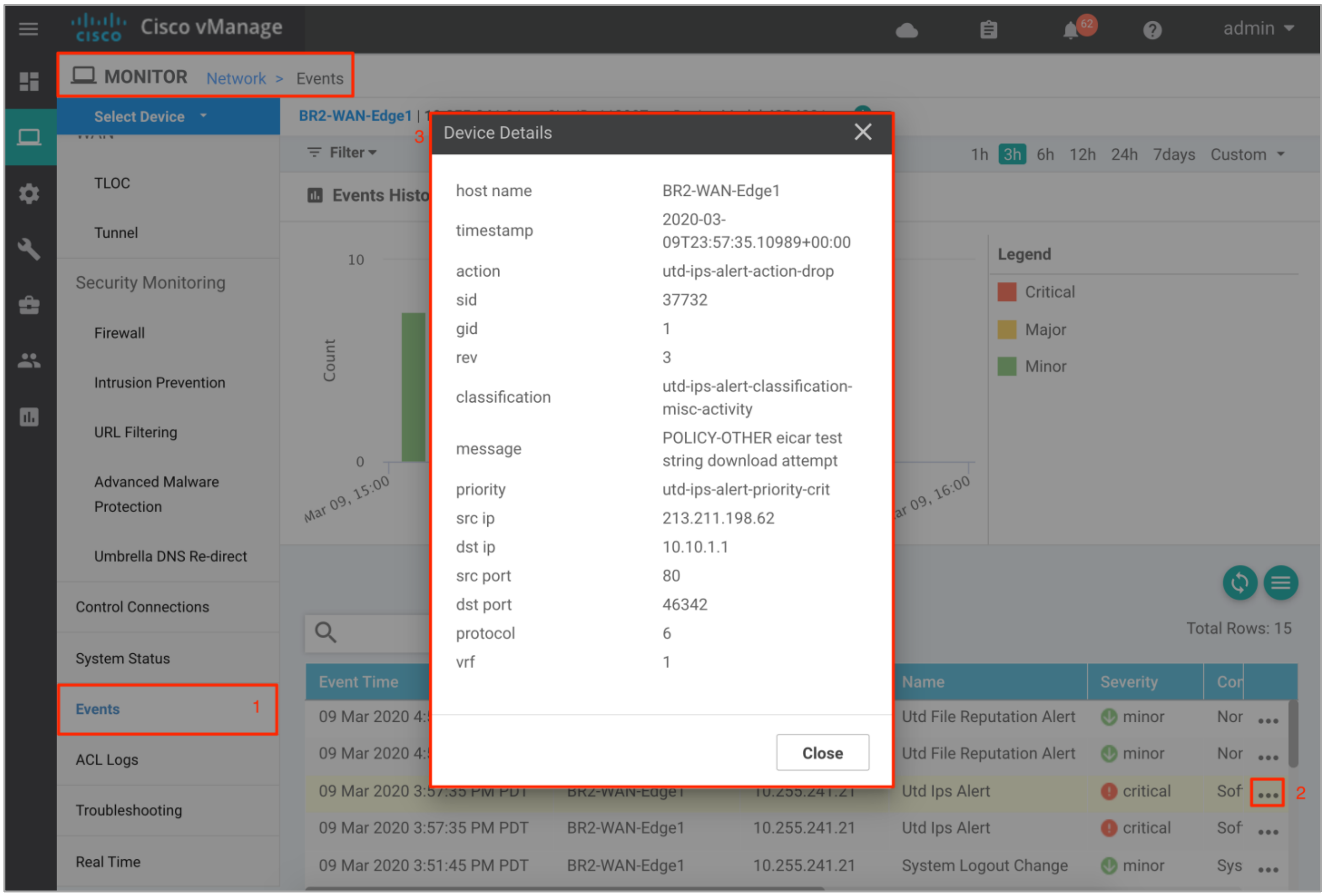
Timestamp	User			Module	Feature	
05 Mar 2020 7:41:58 AM PST	system		0_XE16.12. Please ve...	utd	UTD	•••
05 Mar 2020 7:41:47 AM PST	system		1_XE16.11. Please ve...	utd	UTD	•••
05 Mar 2020 1:41:36 AM PST	system		0_XE16.12. Please ve...	utd	UTD	•••
05 Mar 2020 1:41:26 AM PST	system		0_XE16.12. Please ve...	utd	UTD	•••
05 Mar 2020 1:41:15 AM PST	system		1_XE16.11. Please ve...	utd	UTD	•••
04 Mar 2020 7:41:05 PM PST	system		0_XE16.12. Please ve...	utd	UTD	•••
04 Mar 2020 7:40:55 PM PST	system		0_XE16.12. Please ve...	utd	UTD	•••
04 Mar 2020 7:40:44 PM PST	system		1_XE16.11. Please ve...	utd	UTD	•••
04 Mar 2020 1:40:33 PM PST	system	172.27.0.14	Snort signature download failed for version: 1.0.8_SV2.9.13.0_XE16.12. Please ve...	utd	UTD	•••
04 Mar 2020 1:40:23 PM PST	system	172.27.0.14	Snort signature download failed for version: 1.0.6_SV2.9.13.0_XE16.12. Please ve...	utd	UTD	•••
04 Mar 2020 1:40:10 PM PST	system	172.27.0.14	Snort signature download failed for version: 1.0.4_SV2.9.11.1_XE16.11. Please ve...	utd	UTD	•••
04 Mar 2020 7:39:59 AM PST	system	172.27.0.14	Snort signature download failed for version: 1.0.8_SV2.9.13.0_XE16.12. Please ve...	utd	UTD	•••
04 Mar 2020 7:39:48 AM PST	system	172.27.0.14	Snort signature download failed for version: 1.0.6_SV2.9.13.0_XE16.12. Please ve...	utd	UTD	•••
04 Mar 2020 7:39:38 AM PST	system	172.27.0.14	Snort signature download failed for version: 1.0.4_SV2.9.11.1_XE16.11. Please ve...	utd	UTD	•••

If you see this error message,

- Recheck your CCO credentials under **Settings** > **IPS Signature Update.**
- Make sure you have reachability to cloudsso2.cisco.com from both the vManage and the WAN Edge device.
- Finally, try to update the signature set manually from WAN Edge by entering ***UTD signature utd signature update server cisco username <CCO username> password <CCO password>***.

  If you do not have Internet access from your WAN Edge device, you can also manually update the signature set by downloading the signature package from https://software.cisco.com/download/home and copy the file into a FAT32 formatted USB drive. Insert the USB drive into the WAN Edge device and copy the file into flash/ bootflash. Finally, enter command ***utd threat-inspection signature update file flash:<signature_set.pkg>***

Step 11. To view the IPS signature statistics, click on **Events** from the left pane. Within **Network** > **Events**, click on the three dots **(...)** and then, click on the **Device Details** a pop-up window will appear.



host name	BR2-WAN-Edge1
timestamp	2020-03-09T23:57:35.10989+00:00
action	utd-ips-alert-action-drop
sid	37732
gid	1
rev	3
classification	utd-ips-alert-classification-misc-activity
message	POLICY-OTHER eicar test string download attempt
priority	utd-ips-alert-priority-crit
src ip	213.211.198.62
dst ip	10.10.1.1
src port	80
dst port	46342
protocol	6
vrf	1

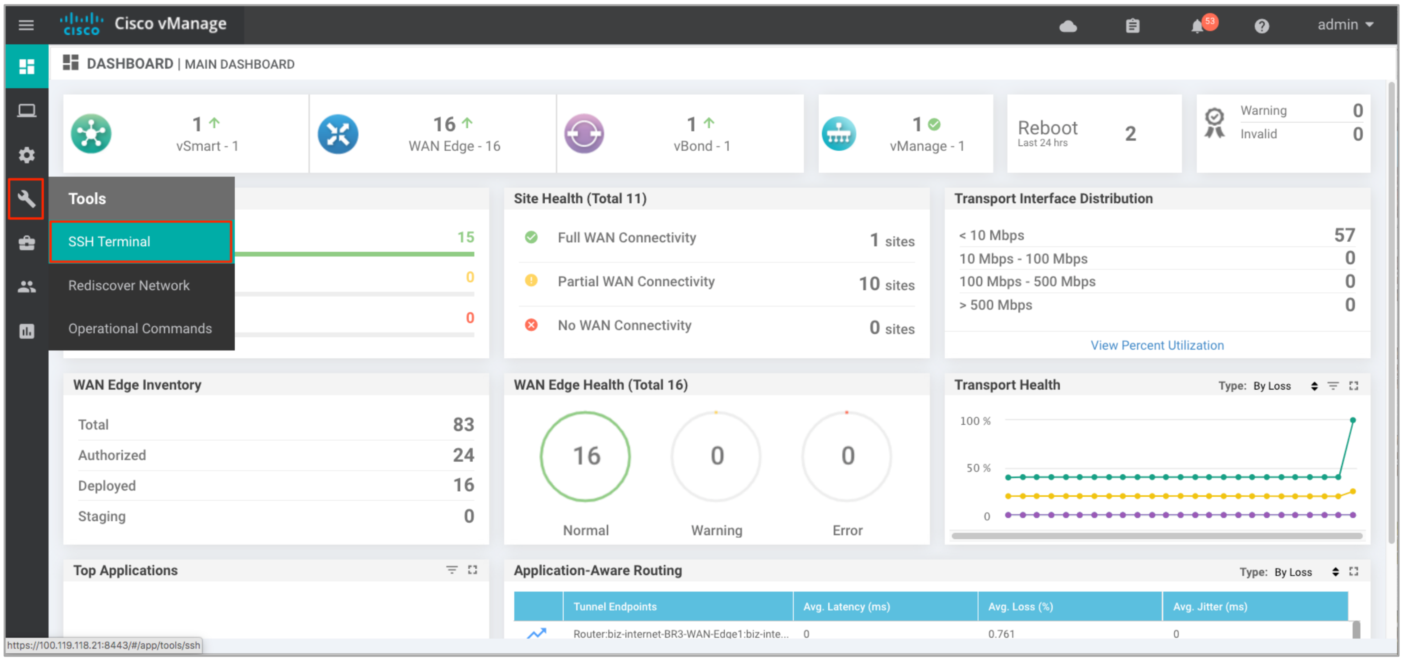
Event Time			Name	Severity	Cor
09 Mar 2020 4:			Utd File Reputation Alert	minor	Nor
09 Mar 2020 4:			Utd File Reputation Alert	minor	Nor
09 Mar 2020 3:57:35 PM PDT	BR2-WAN-Edge1	10.255.241.21	Utd Ips Alert	critical	Sof
09 Mar 2020 3:57:35 PM PDT	BR2-WAN-Edge1	10.255.241.21	Utd Ips Alert	critical	Sof
09 Mar 2020 3:51:45 PM PDT	BR2-WAN-Edge1	10.255.241.21	System Logout Change	minor	Sys

Note: The output lists the Signature ID (SID) and Generator ID (GID) associated with the signature. If you wish to whitelist this signature, enter the signature in format within the signature whitelist tab in the format - GID: SID, for e.g. 1:37732.

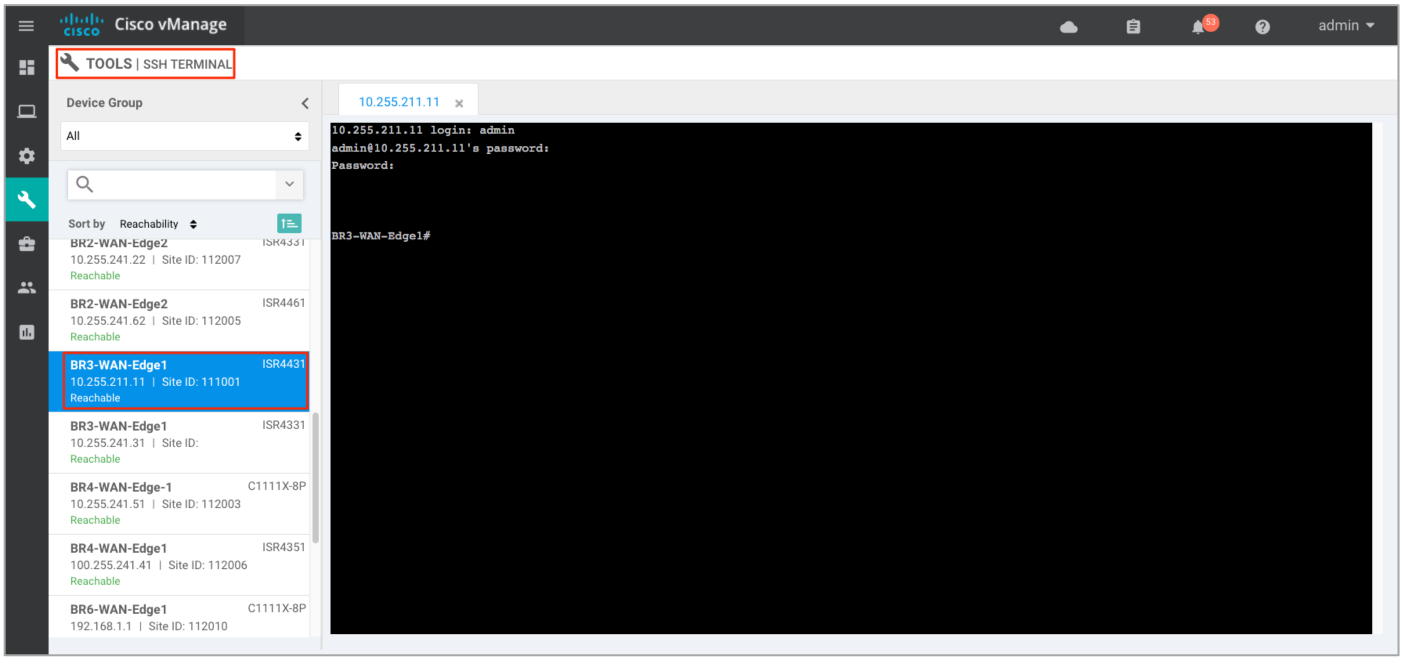
Procedure 3. Monitor IPS Feature and Statistics via vManage SSH Server Dashboard

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

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

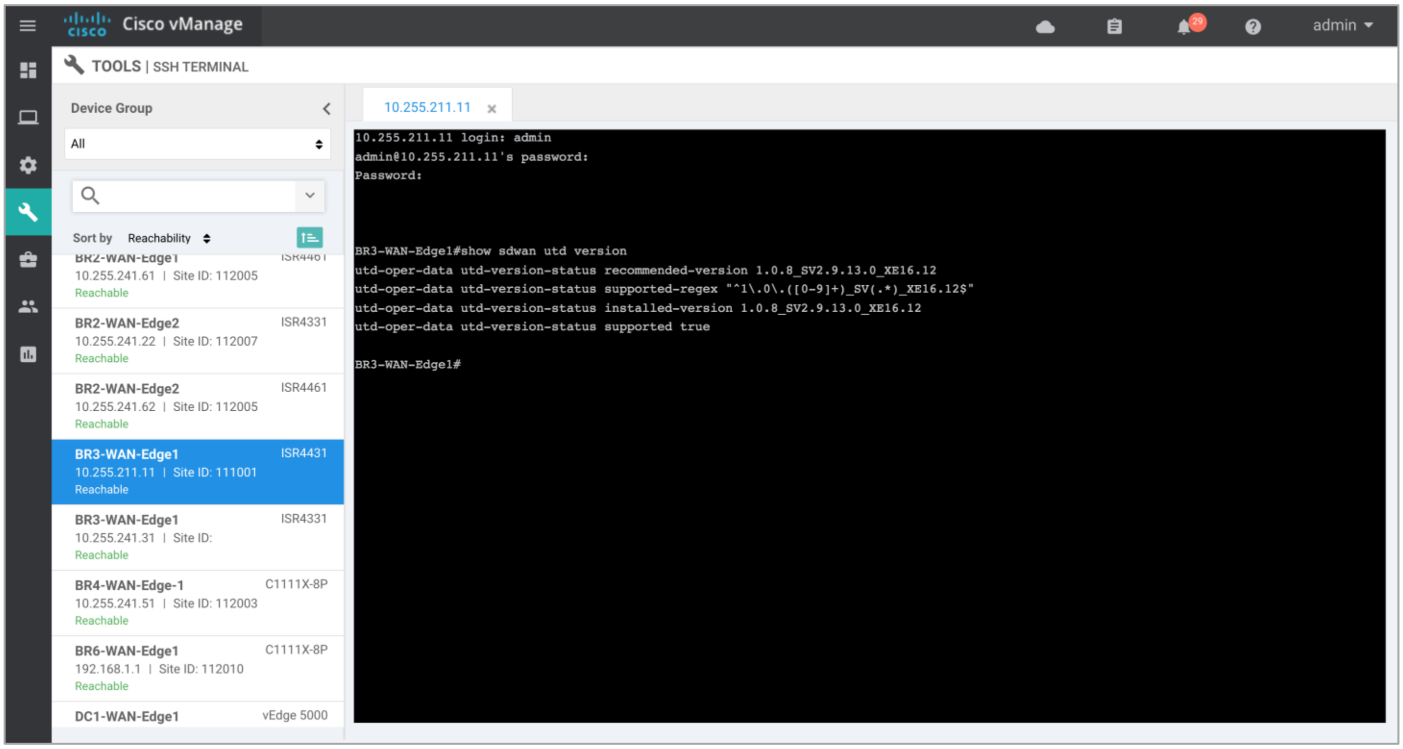


Step 2. Select the device from the list devices, and login.



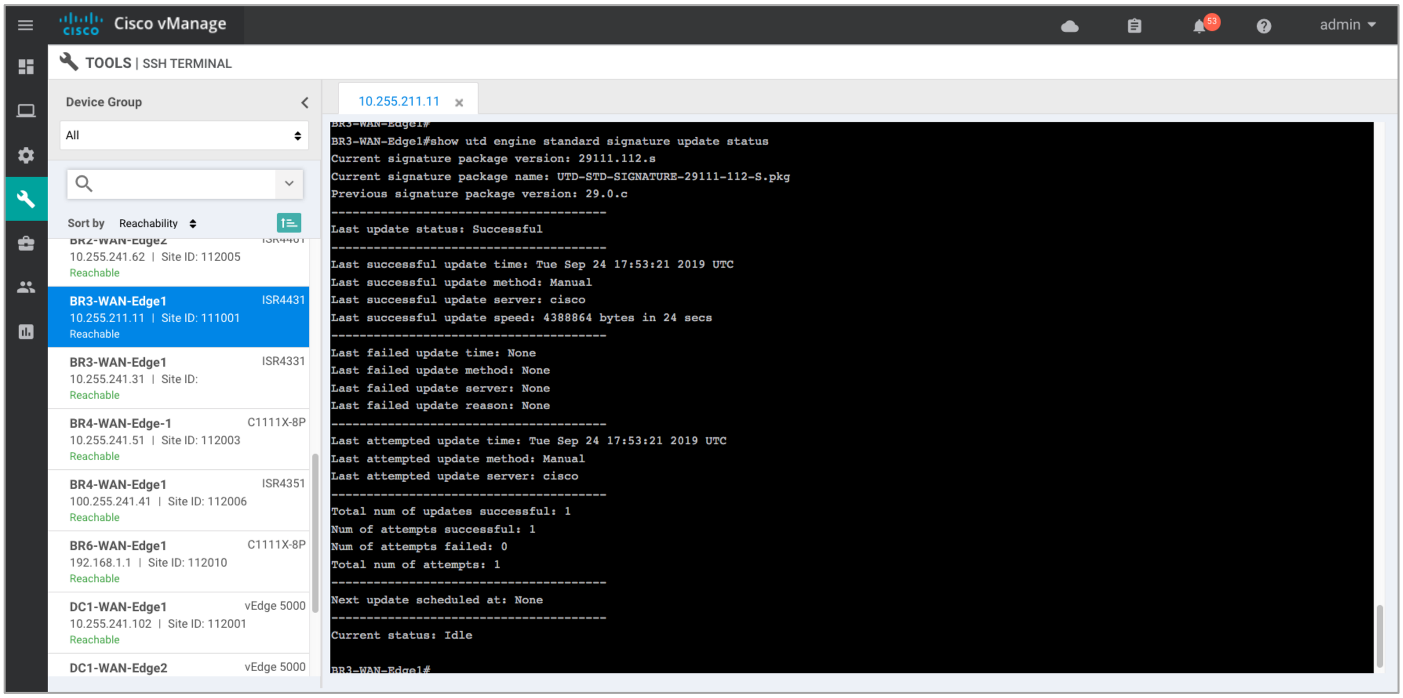
```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:



BR3-WAN-Edge1#
```

Step 3. To view the current UTD version and to test if its supported, enter the CLI command – ***Show sdwan utd version***.



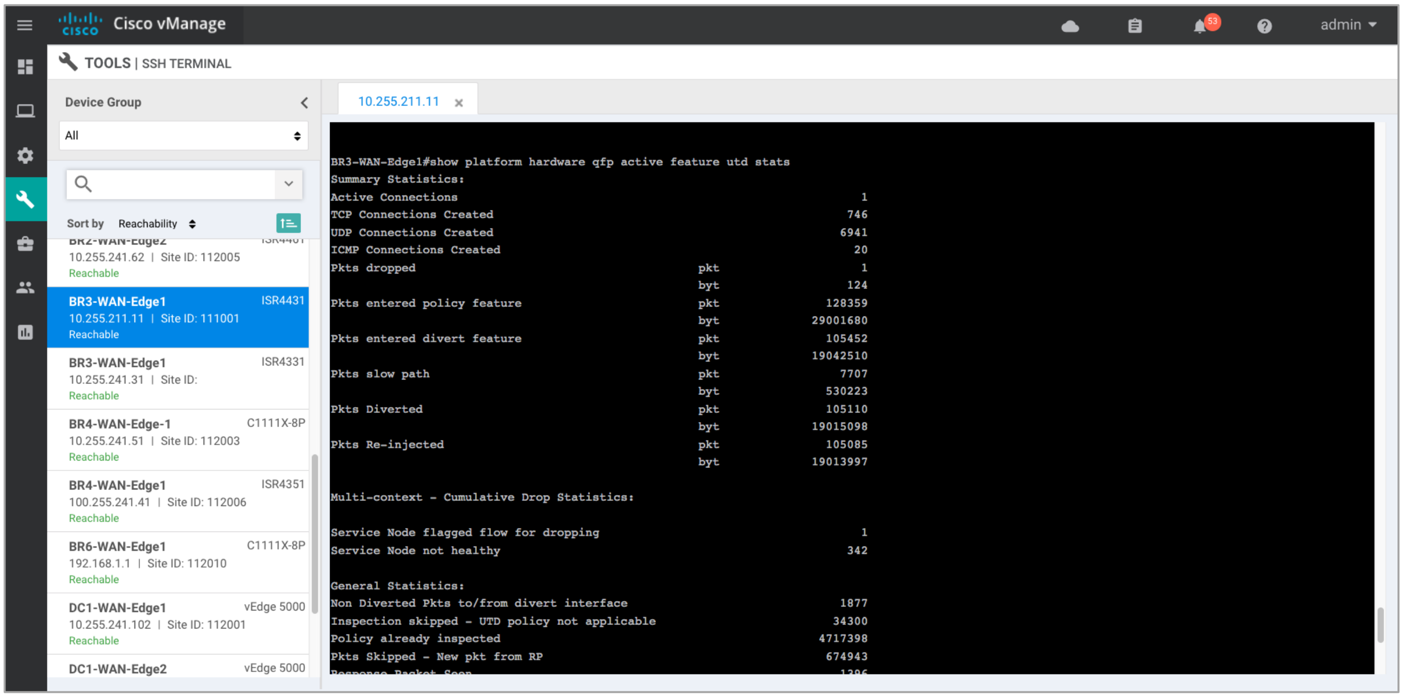
```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:



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. To view the current signature package, enter the CLI command – ***Show utd engine standard signature update status***. The command displays the number of failed/ successful signature update attempts, along with the reason for the last update.



```
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#
```

Step 5. To view the utd packet statistics, enter the following CLI command – ***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
Response Packet Seen                                              1396
```

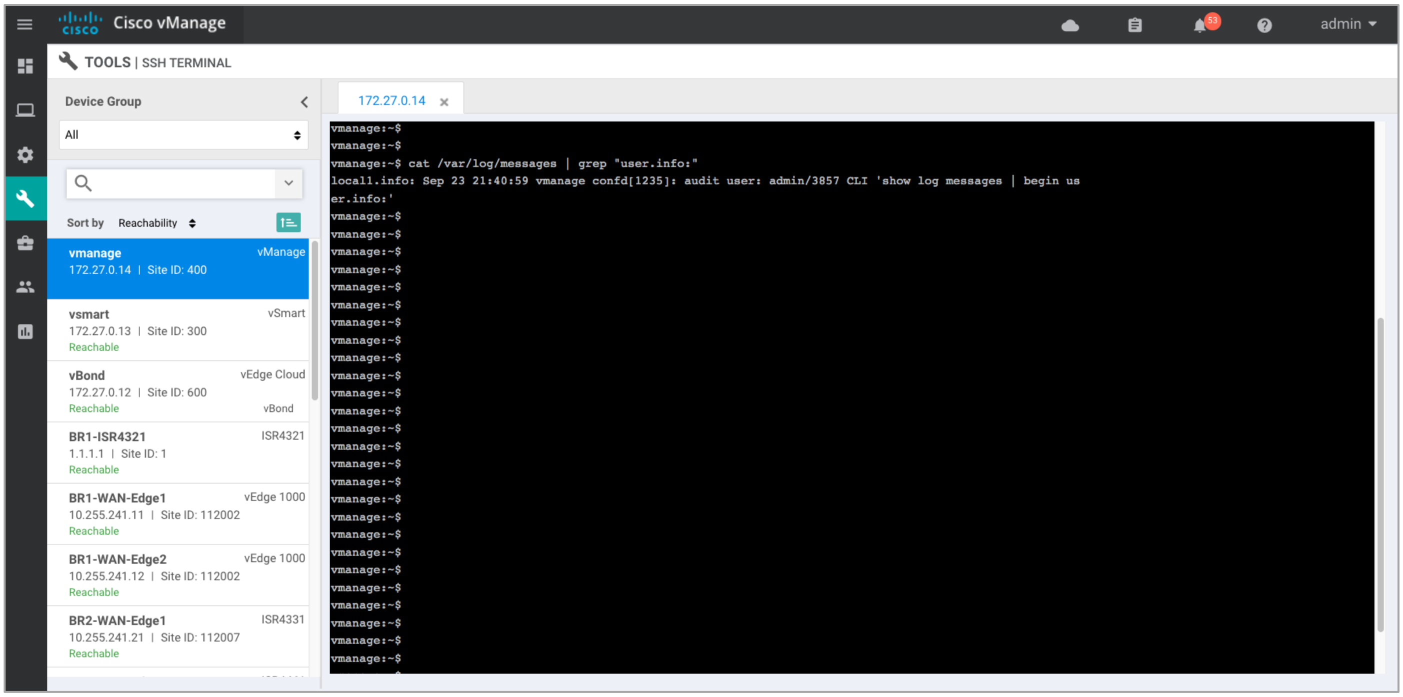
Step 6. To check for automatic signature updates on vManage, enter the following commands.

`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,

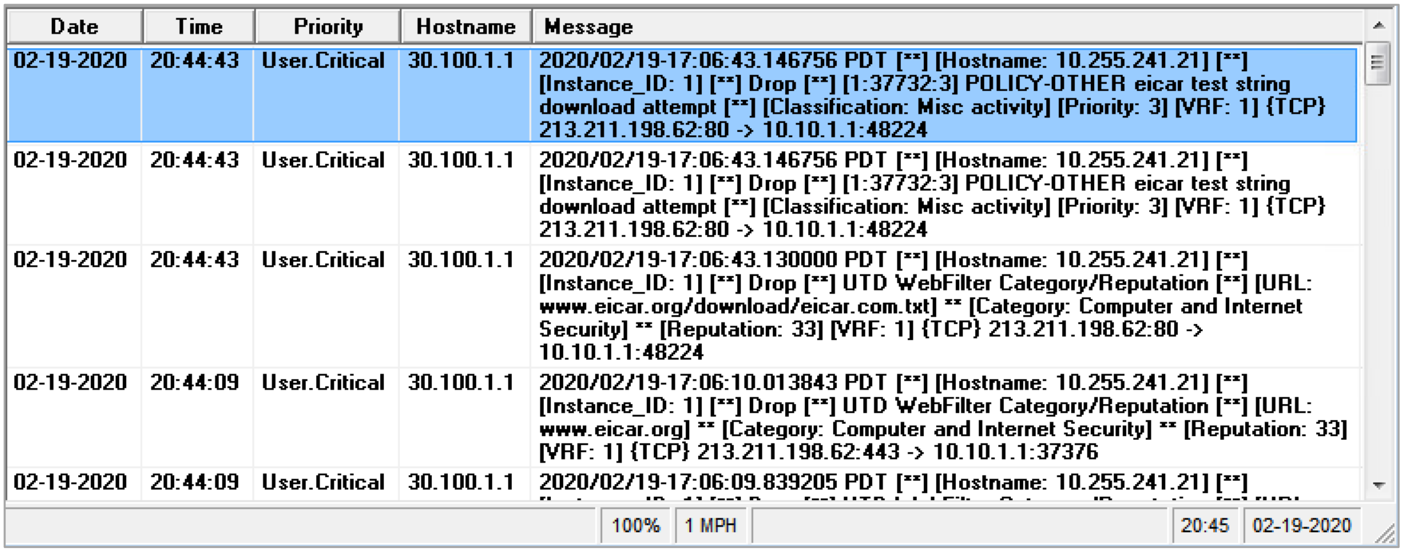


```
vmanage:~$
vmanage:~$
vmanage:~$ cat /var/log/messages | grep "user.info:"
local1.info: Sep 23 21:40:59 vmanage confd[1235]: audit user: admin/3857 CLI 'show log messages | begin us
er.info:'
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$
vmanage:~$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

Outside the listed CLI commands, some of the other commands that are useful include show utd engine, show sdwan utd data plane <config/global/stats>, show sdwan utd update IPS and show log.

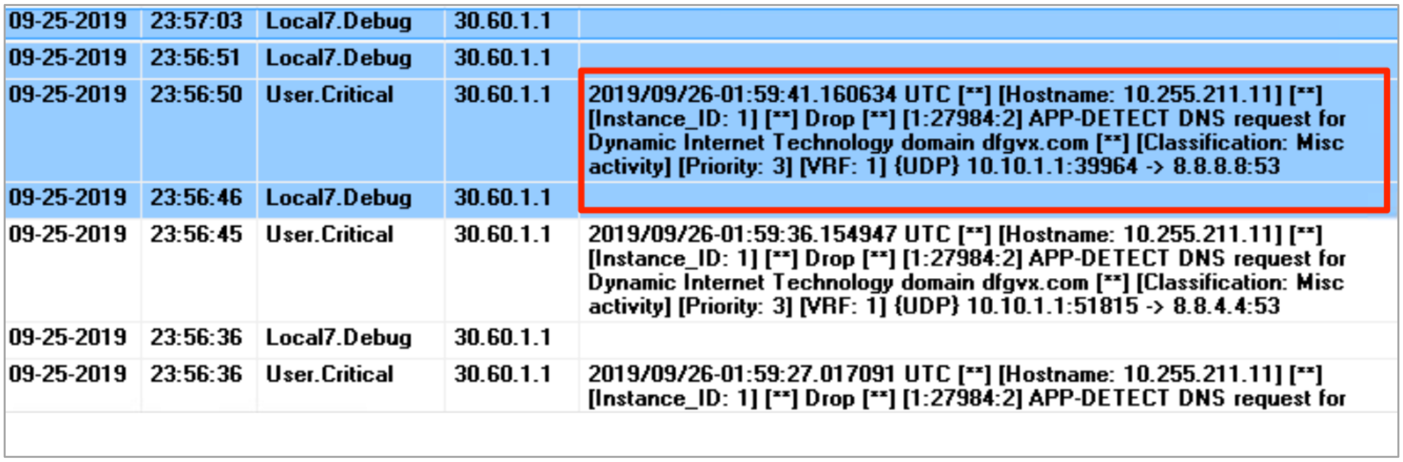
Process 3: Monitor IPS Signature Violations via Syslog Server

Step 1. Log into 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.



Date	Time	Priority	Hostname	Message
02-19-2020	20:44:43	User.Critical	30.100.1.1	2020/02/19-17:06:43.146756 PDT [**] [Hostname: 10.255.241.21] [**] [Instance_ID: 1] [**] Drop [**] [1:37732:3] POLICY-OTHER eicar test string download attempt [**] [Classification: Misc activity] [Priority: 3] [VRF: 1] {TCP} 213.211.198.62:80 -> 10.10.1.1:48224
02-19-2020	20:44:43	User.Critical	30.100.1.1	2020/02/19-17:06:43.146756 PDT [**] [Hostname: 10.255.241.21] [**] [Instance_ID: 1] [**] Drop [**] [1:37732:3] POLICY-OTHER eicar test string download attempt [**] [Classification: Misc activity] [Priority: 3] [VRF: 1] {TCP} 213.211.198.62:80 -> 10.10.1.1:48224
02-19-2020	20:44:43	User.Critical	30.100.1.1	2020/02/19-17:06:43.130000 PDT [**] [Hostname: 10.255.241.21] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: www.eicar.org/download/eicar.com.txt] ** [Category: Computer and Internet Security] ** [Reputation: 33] [VRF: 1] {TCP} 213.211.198.62:80 -> 10.10.1.1:48224
02-19-2020	20:44:09	User.Critical	30.100.1.1	2020/02/19-17:06:10.013843 PDT [**] [Hostname: 10.255.241.21] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: www.eicar.org] ** [Category: Computer and Internet Security] ** [Reputation: 33] [VRF: 1] {TCP} 213.211.198.62:443 -> 10.10.1.1:37376
02-19-2020	20:44:09	User.Critical	30.100.1.1	2020/02/19-17:06:09.839205 PDT [**] [Hostname: 10.255.241.21] [**]

100% 1 MPH 20:45 02-19-2020



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

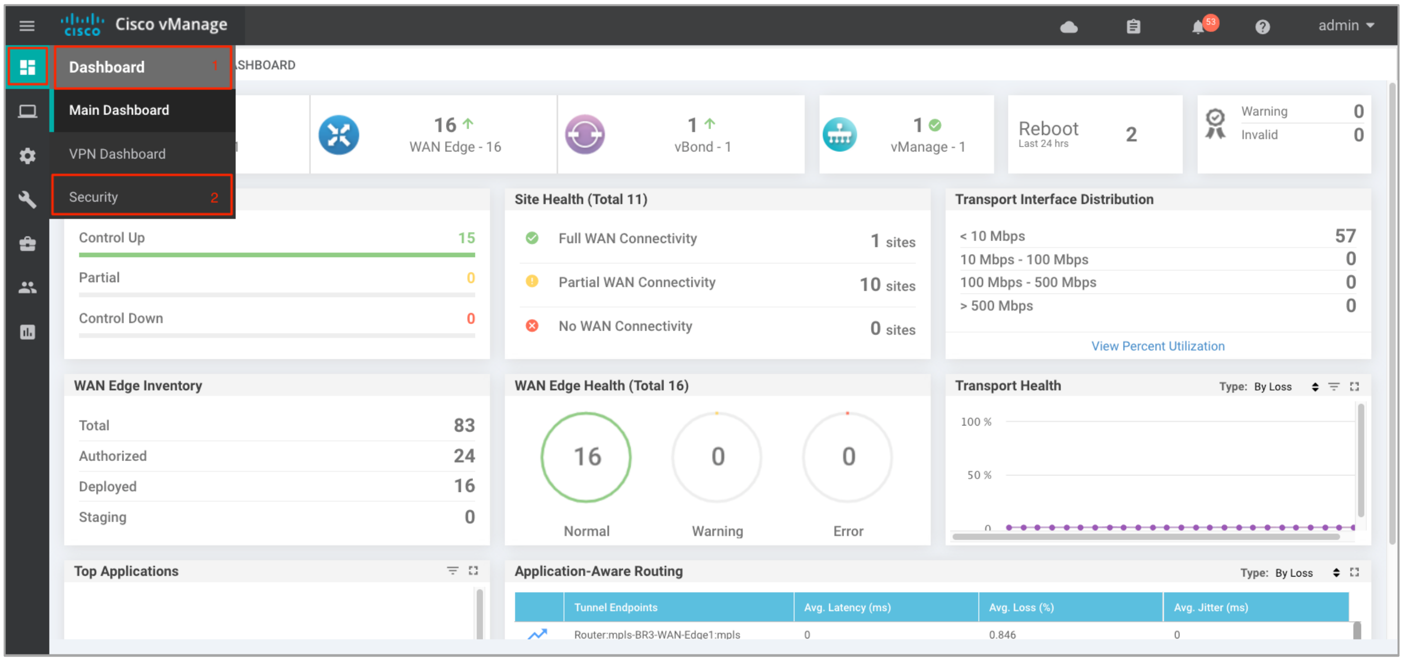
Process 4: Monitor Advanced Malware Protection Feature via vManage NMS

Using the vManage NMS dashboard, you can monitor the Advanced Malware Protection (AMP) feature via vManage NMS.

Procedure 1. Monitor Advanced Malware Protection via vManage Main Dashboard

Using vManage NMS, you can monitor for clean, malicious or unknown files and information about files that are uploaded for analysis.

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



16 WAN Edge - 16 | 1 vBond - 1 | 1 vManage - 1 | Reboot Last 24 hrs 2 | Warning 0 Invalid 0

Control Up	15
Partial	0
Control Down	0

Site Health (Total 11)

Full WAN Connectivity	1 sites
Partial WAN Connectivity	10 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

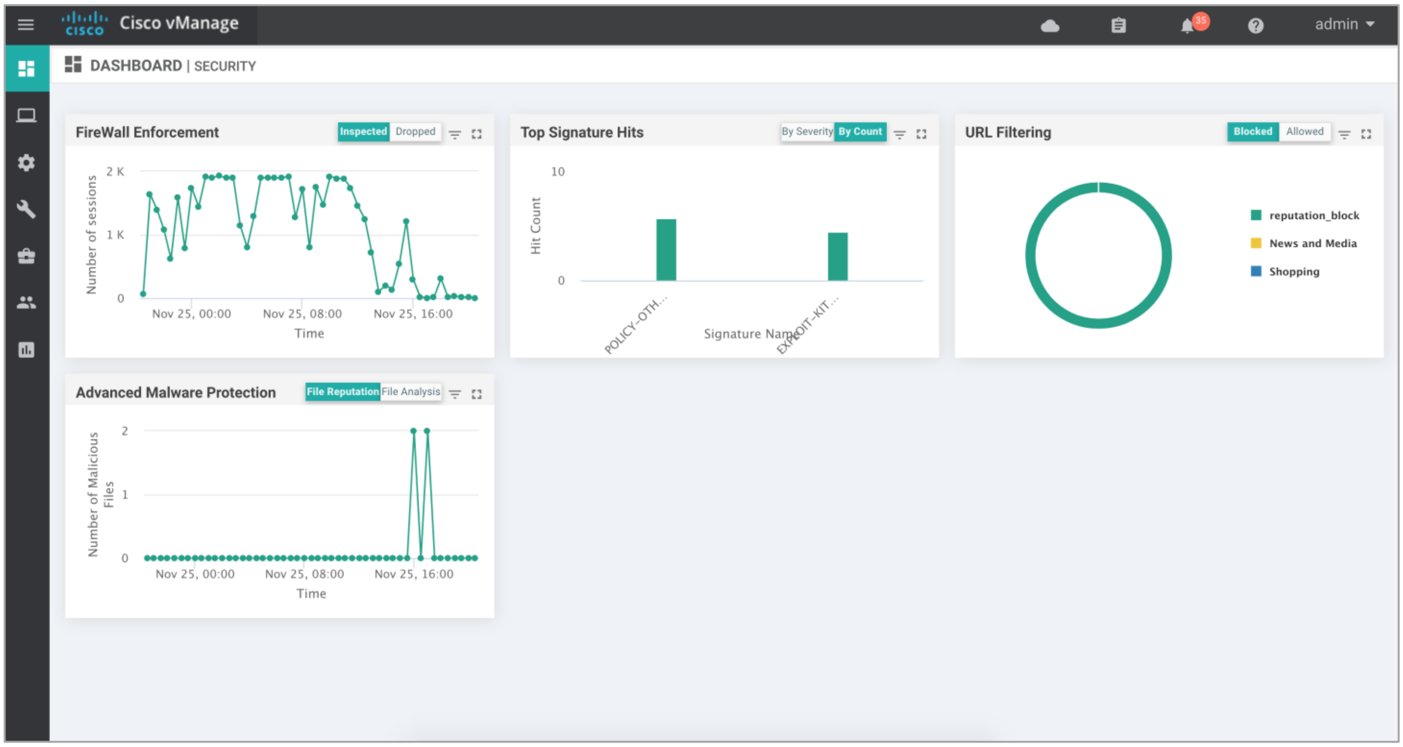
WAN Edge Health (Total 16)

Normal	Warning	Error
16	0	0

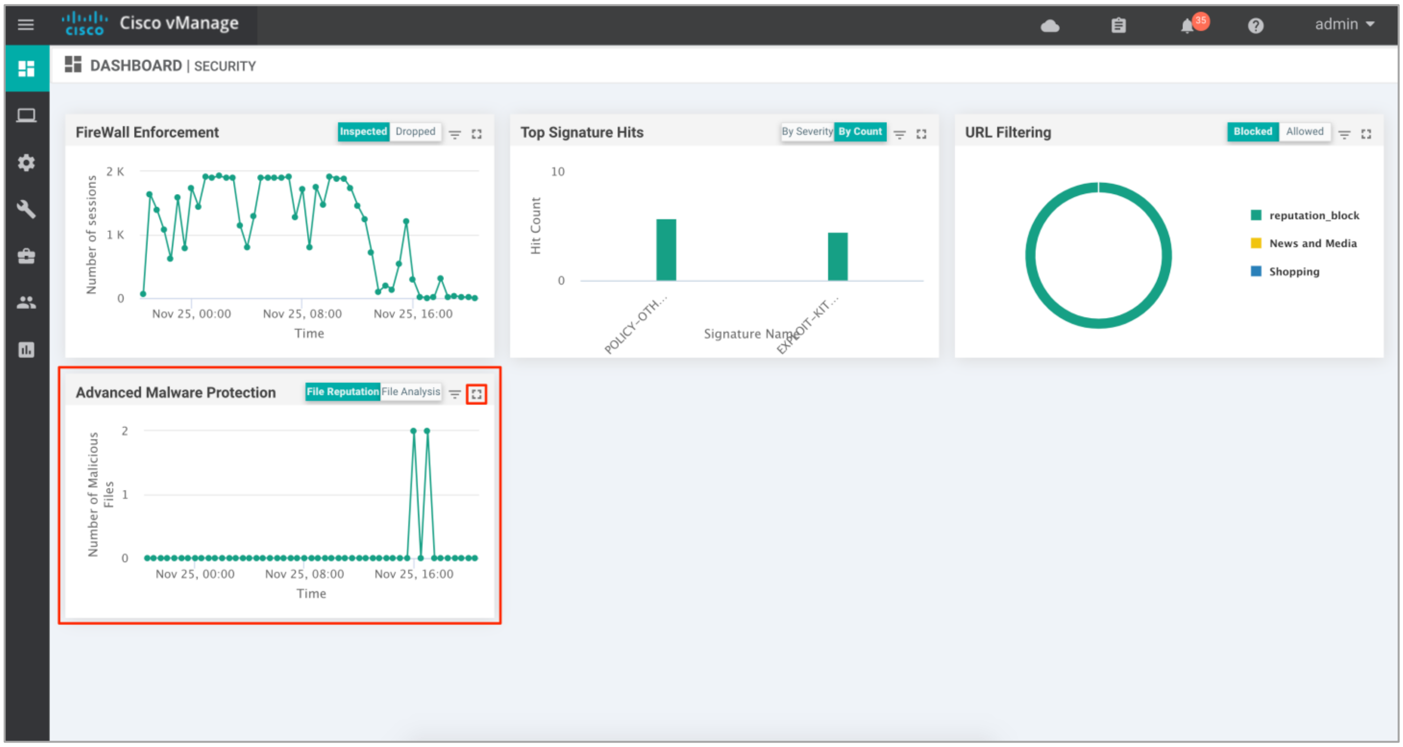
Application-Aware Routing Type: By Loss

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

Step 2. The following screenshot displays the overall security dashboard.

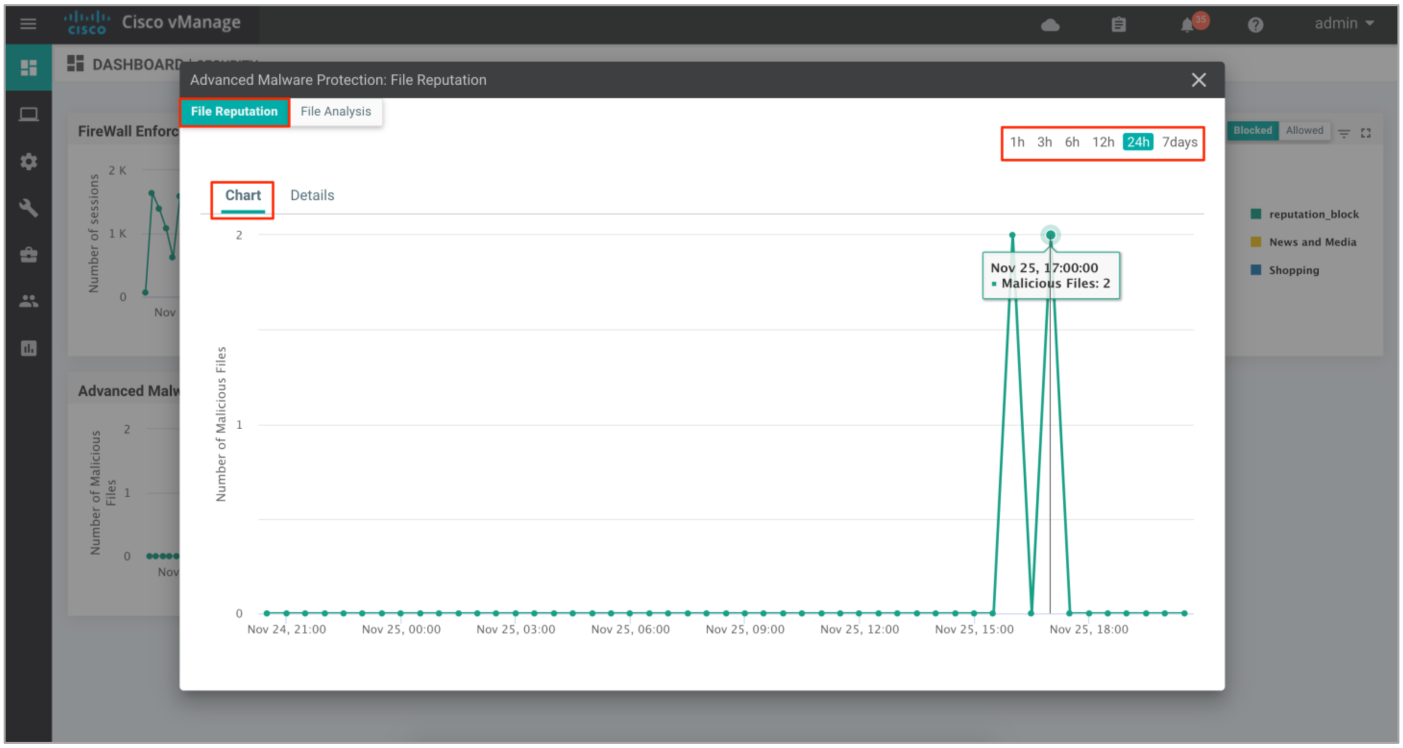


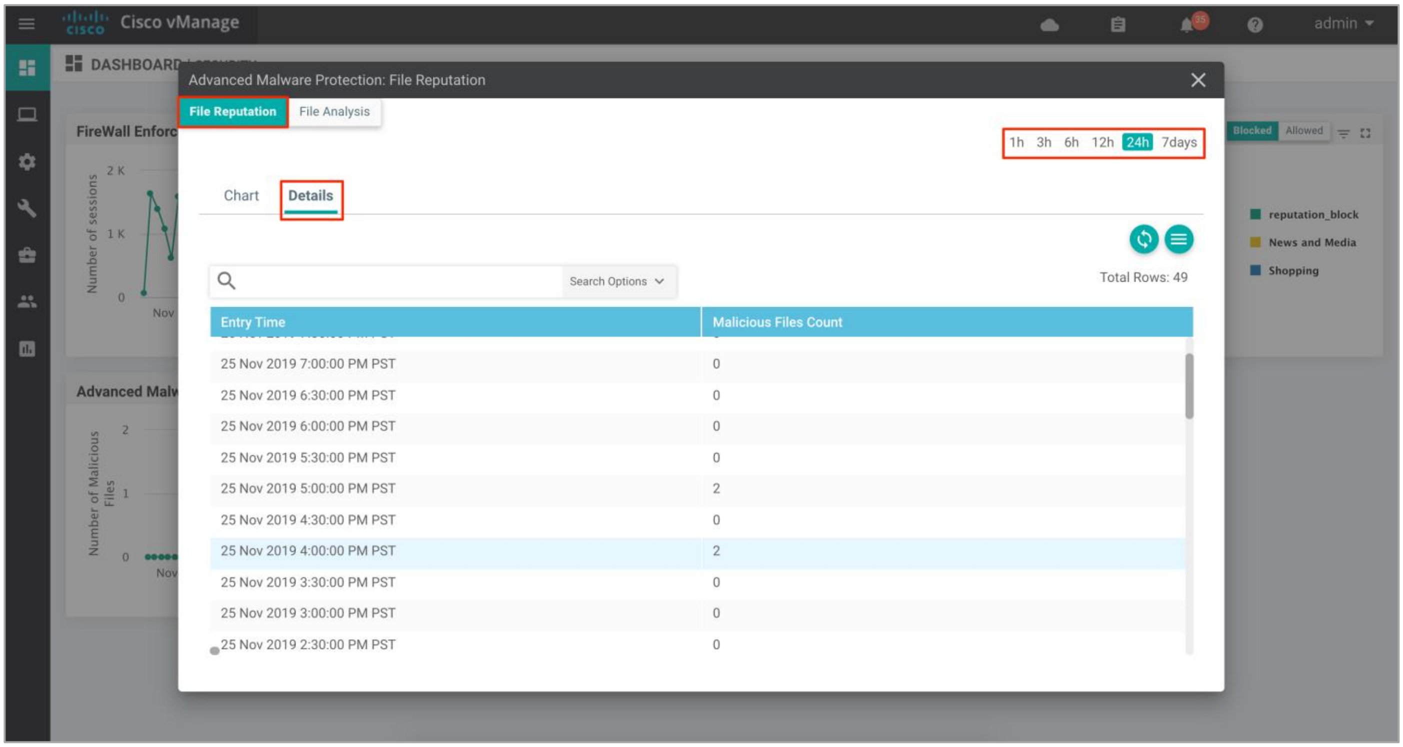
Step 3. To drill down and view the files inspected, click on the square box [] on the top right.



Drill down into the graph by choosing **1h, 3h, 6h, 12h, 24h (default)** or **7days**.

Step 4. To view the overall file reputation graph that displays the total number of files transferred and how many are malicious, clean, or unknown. This tab area also includes a table with detailed information about each file that was inspected.





Advanced Malware Protection: File Reputation

Total Rows: 49

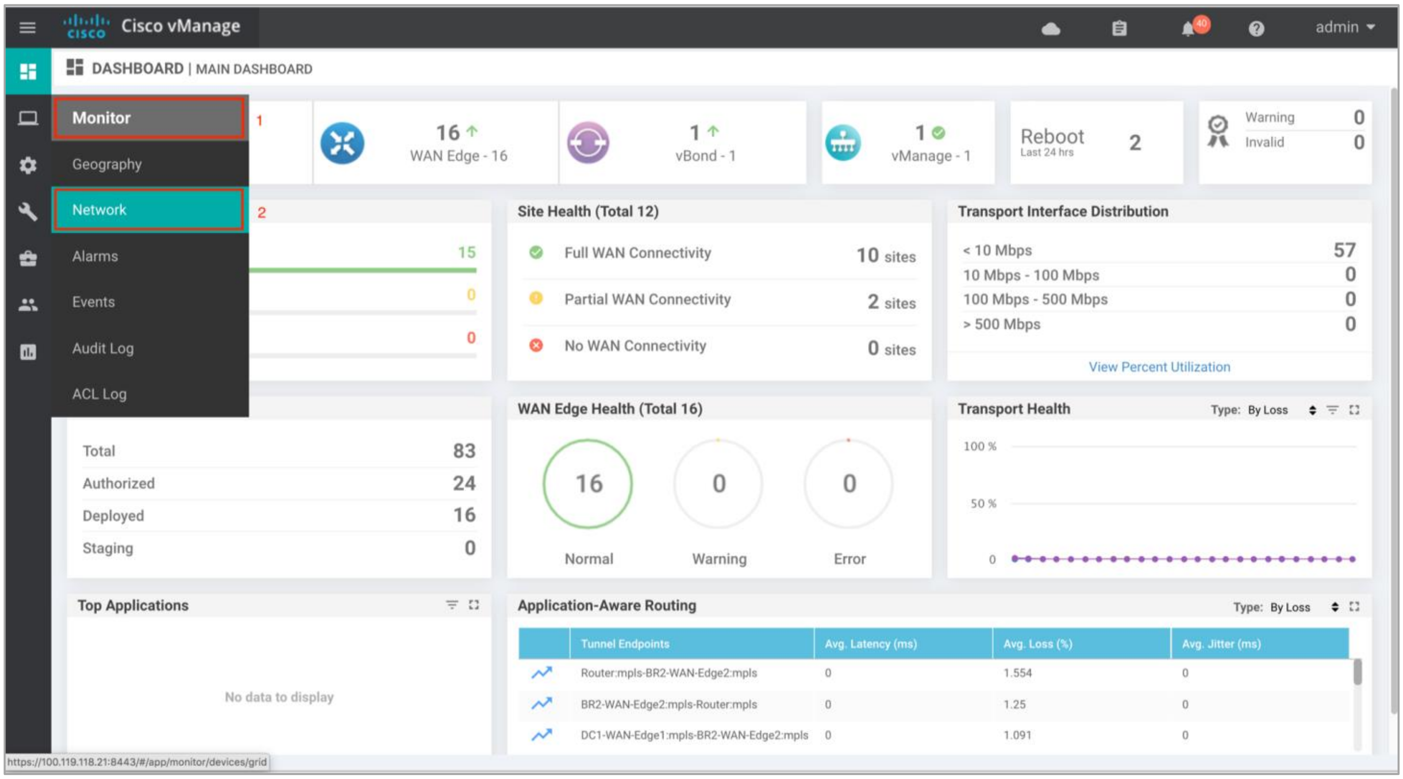
Entry Time	Malicious Files Count
25 Nov 2019 7:00:00 PM PST	0
25 Nov 2019 6:30:00 PM PST	0
25 Nov 2019 6:00:00 PM PST	0
25 Nov 2019 5:30:00 PM PST	0
25 Nov 2019 5:00:00 PM PST	2
25 Nov 2019 4:30:00 PM PST	0
25 Nov 2019 4:00:00 PM PST	2
25 Nov 2019 3:30:00 PM PST	0
25 Nov 2019 3:00:00 PM PST	0
25 Nov 2019 2:30:00 PM PST	0

Similarly, view the graph for File Analysis that displays the number of files that were uploaded to Threat Grid, and a table with detailed information about each file that was uploaded for analysis.

Procedure 2. Monitor Advanced Malware Protection Feature via vManage Monitor Dashboard

Using the vManage NMS dashboard, you can view the Advanced Malware Protection feature via the monitor dashboard contained within vManage.

Step 1. Navigate to **Network** within **Monitor** available on the left pane and click on the WAN Edge device you wish to monitor.



Cisco vManage admin

DASHBOARD | MAIN DASHBOARD

Monitor 1

Geography

Network 2

Alarms

Events

Audit Log

ACL Log

16 WAN Edge - 16

1 vBond - 1

1 vManage - 1

Reboot Last 24 hrs 2

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)

Normal	Warning	Error
16	0	0

Transport Health Type: By Loss

Top Applications

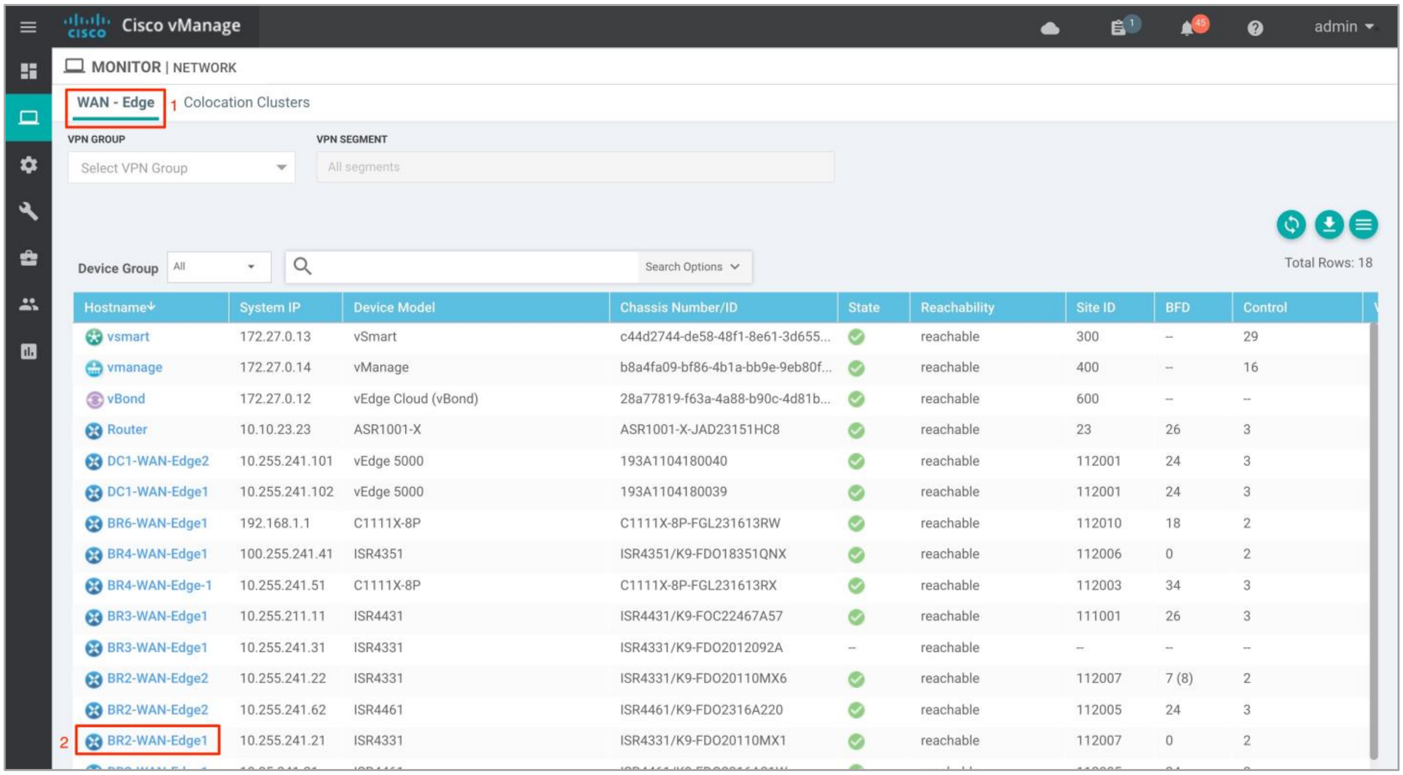
No data to display

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

https://100.119.118.21:8443/#/app/monitor/devices/grid

Step 2. Click on a specific WAN Edge device to monitor the AMP policy.



Cisco vManage admin

MONITOR | NETWORK

WAN - Edge 1 Colocation Clusters

VPN GROUP: Select VPN Group

VPN SEGMENT: All segments

Device Group: All

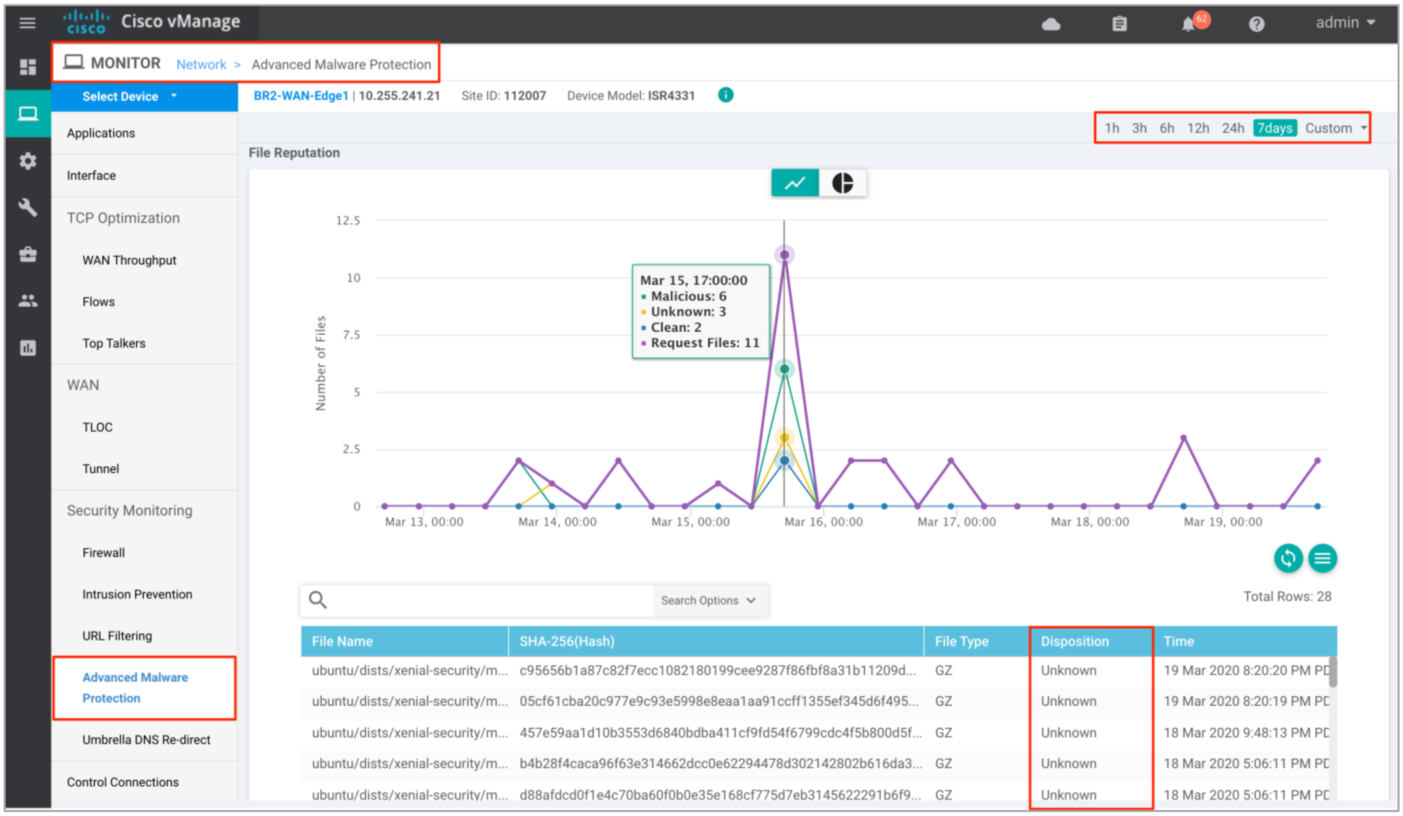
Search Options

Total Rows: 18

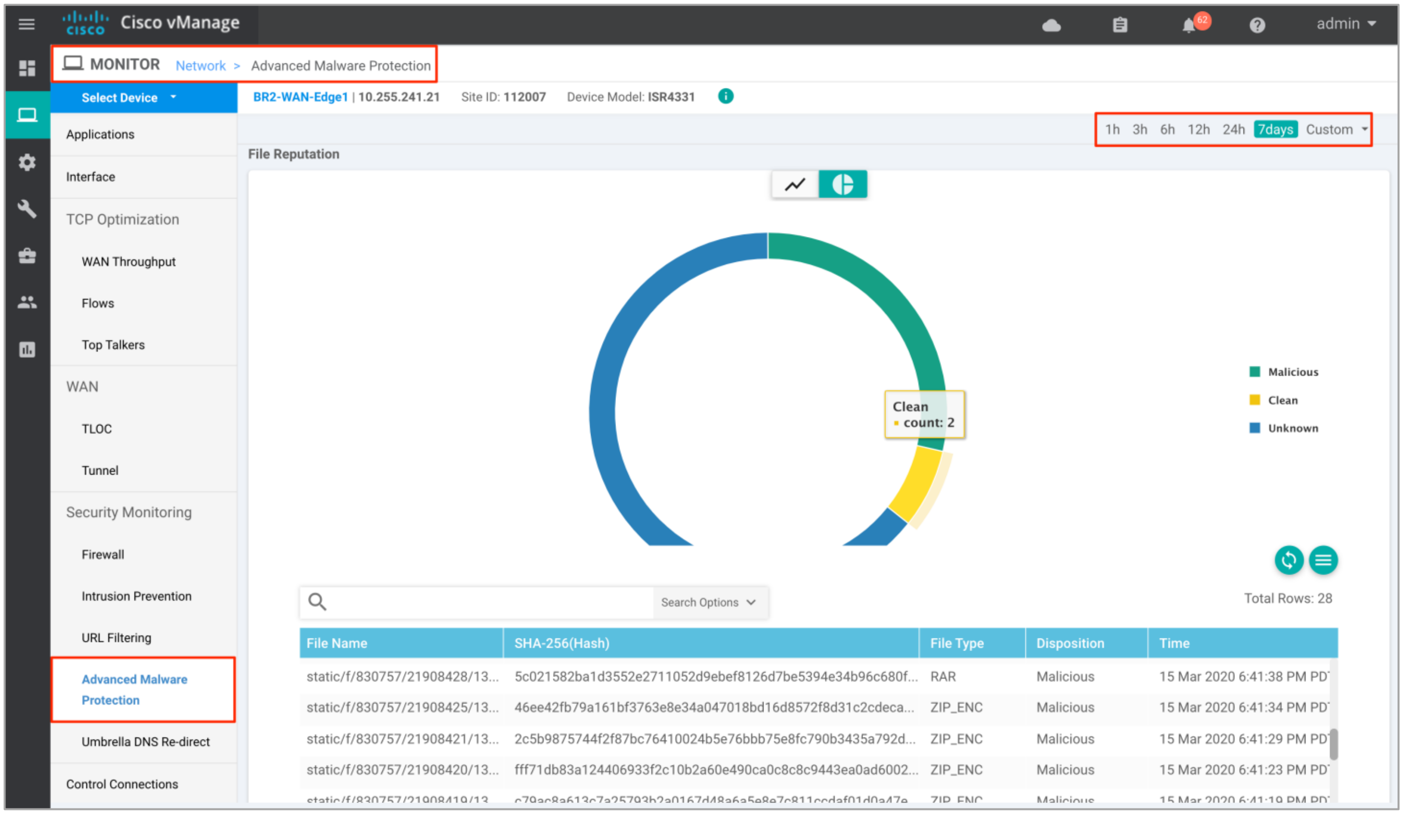
Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control
vsmart	172.27.0.13	vSmart	c44d2744-de58-48f1-8e61-3d655...	✓	reachable	300	--	29
vmanage	172.27.0.14	vManage	b8a4fa09-bf86-4b1a-bb9e-9eb80f...	✓	reachable	400	--	16
vBond	172.27.0.12	vEdge Cloud (vBond)	28a77819-f63a-4a88-b90c-4d81b...	✓	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
2 BR2-WAN-Edge1	10.255.241.21	ISR4331	ISR4331/K9-FDO20110MX1	✓	reachable	112007	0	2

Step 3. Click on Advanced Malware Protection tab under Security Monitoring from the left pane.

The graph shows the total number of files transferred and those that are malicious, clean, or unknown.

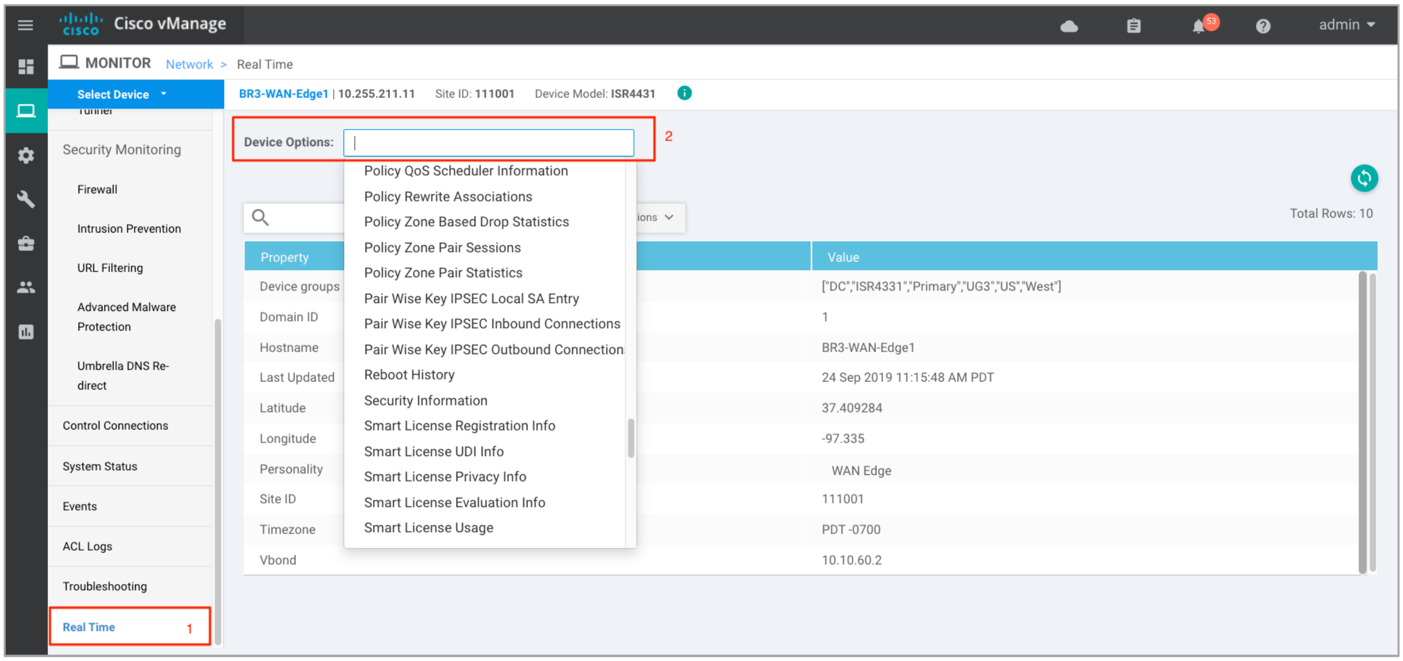


File Name	SHA-256(Hash)	File Type	Disposition	Time
ubuntu/dists/xenial-security/m...	c95656b1a87c82f7ecc1082180199cee9287f86fbf8a31b11209d...	GZ	Unknown	19 Mar 2020 8:20:20 PM PD
ubuntu/dists/xenial-security/m...	05cf61cba20c977e9c93e5998e8eaa1aa91ccff1355ef345d6f495...	GZ	Unknown	19 Mar 2020 8:20:19 PM PD
ubuntu/dists/xenial-security/m...	457e59aa1d10b3553d6840bdba411cf9fd54f6799cdc4f5b800d5f...	GZ	Unknown	18 Mar 2020 9:48:13 PM PD
ubuntu/dists/xenial-security/m...	b4b28f4caca96f63e314662dcc0e62294478d302142802b616da3...	GZ	Unknown	18 Mar 2020 5:06:11 PM PD
ubuntu/dists/xenial-security/m...	d88afdcd0f1e4c70ba60f0b0e35e168cf775d7eb3145622291b6f9...	GZ	Unknown	18 Mar 2020 5:06:11 PM PD



File Name	SHA-256(Hash)	File Type	Disposition	Time
static/f/830757/21908428/13...	5c021582ba1d3552e2711052d9ebef8126d7be5394e34b96c680f...	RAR	Malicious	15 Mar 2020 6:41:38 PM PDT
static/f/830757/21908425/13...	46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdeca...	ZIP_ENC	Malicious	15 Mar 2020 6:41:34 PM PDT
static/f/830757/21908421/13...	2c5b9875744f2f87bc76410024b5e76bbb75e8fc790b3435a792d...	ZIP_ENC	Malicious	15 Mar 2020 6:41:29 PM PDT
static/f/830757/21908420/13...	fff71db83a124406933f2c10b2a60e490ca0c8c8c9443ea0ad6002...	ZIP_ENC	Malicious	15 Mar 2020 6:41:23 PM PDT
static/f/830757/21908419/13...	c79ac8a613c7a25793b2a0167d48a6a5e8e7c811ccdaf01d0a47e...	ZIP_ENC	Malicious	15 Mar 2020 6:41:19 PM PDT

Step 4. Next, click on **Real Time** from the left pane. Within **Network** > **Real time,** a screen will appear with **Device Options**. Click on 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
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

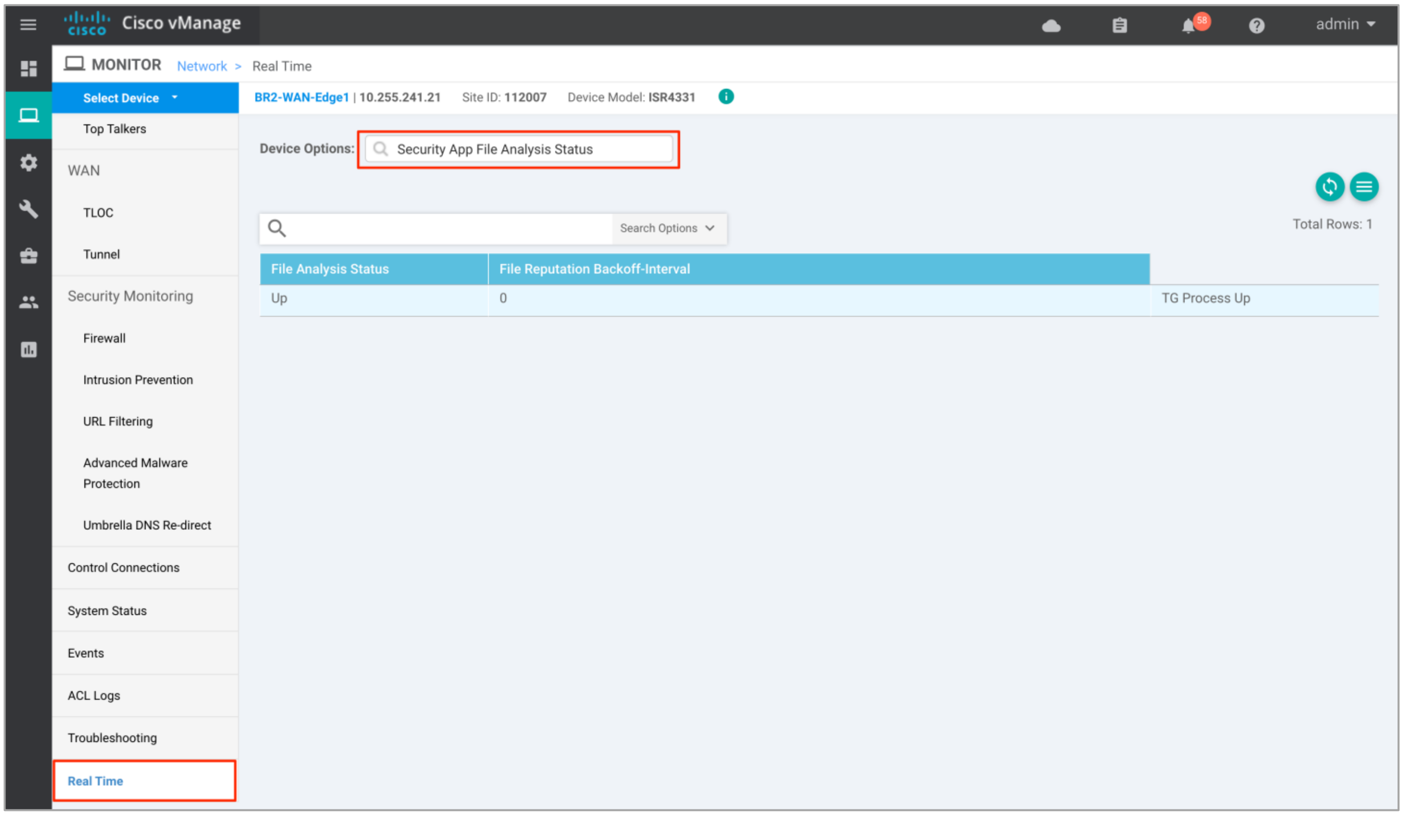
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

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 5. To view the status (TG Progress Up) of the File Analysis, click on **Security App File Analysis Status**.



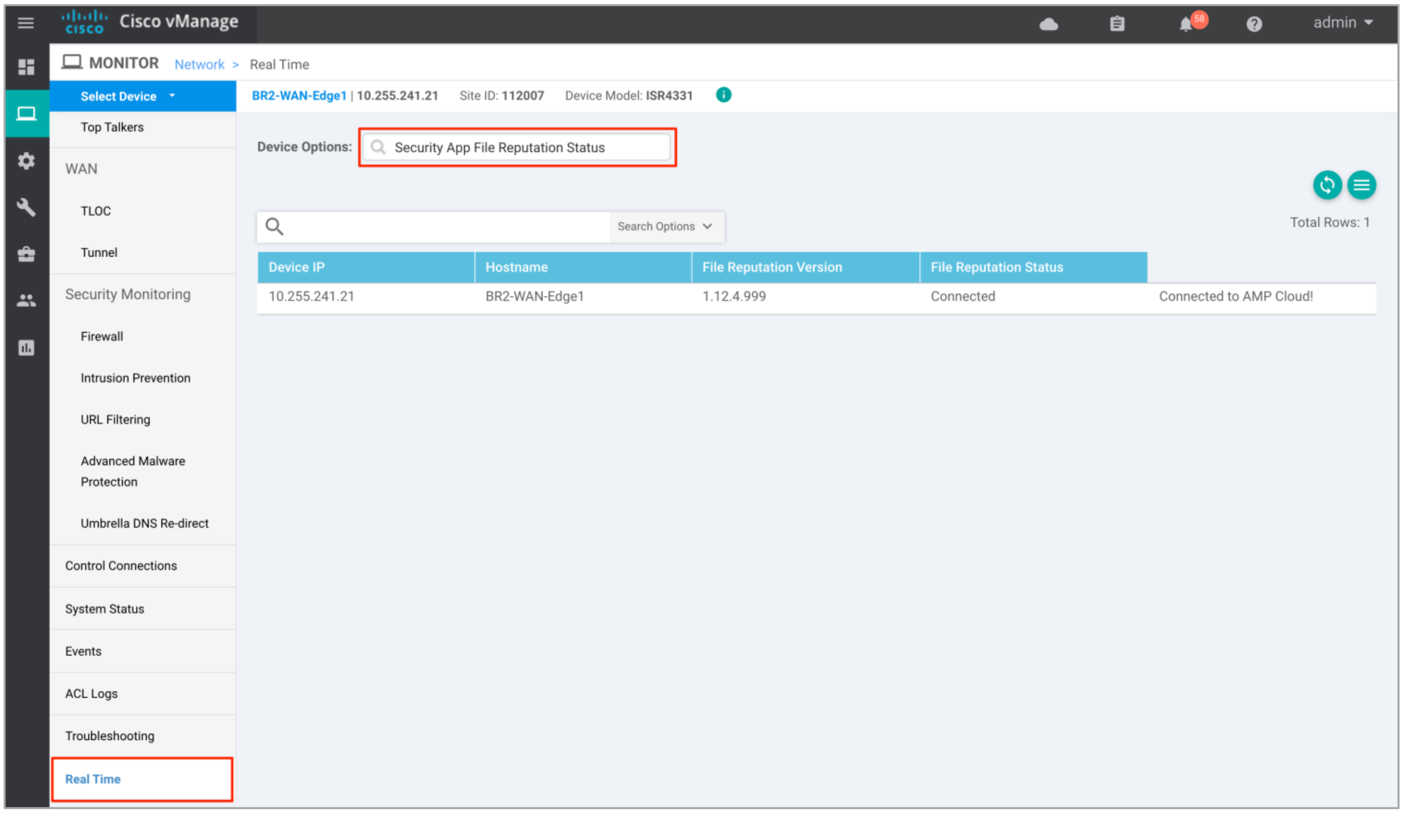
BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

Device Options: Security App File Analysis Status

Total Rows: 1

File Analysis Status	File Reputation Backoff-Interval	
Up	0	TG Process Up

Step 6. To view the status (Connected/Connected to AMP Cloud) of File Reputation, click on **Security App File Reputation Status**.



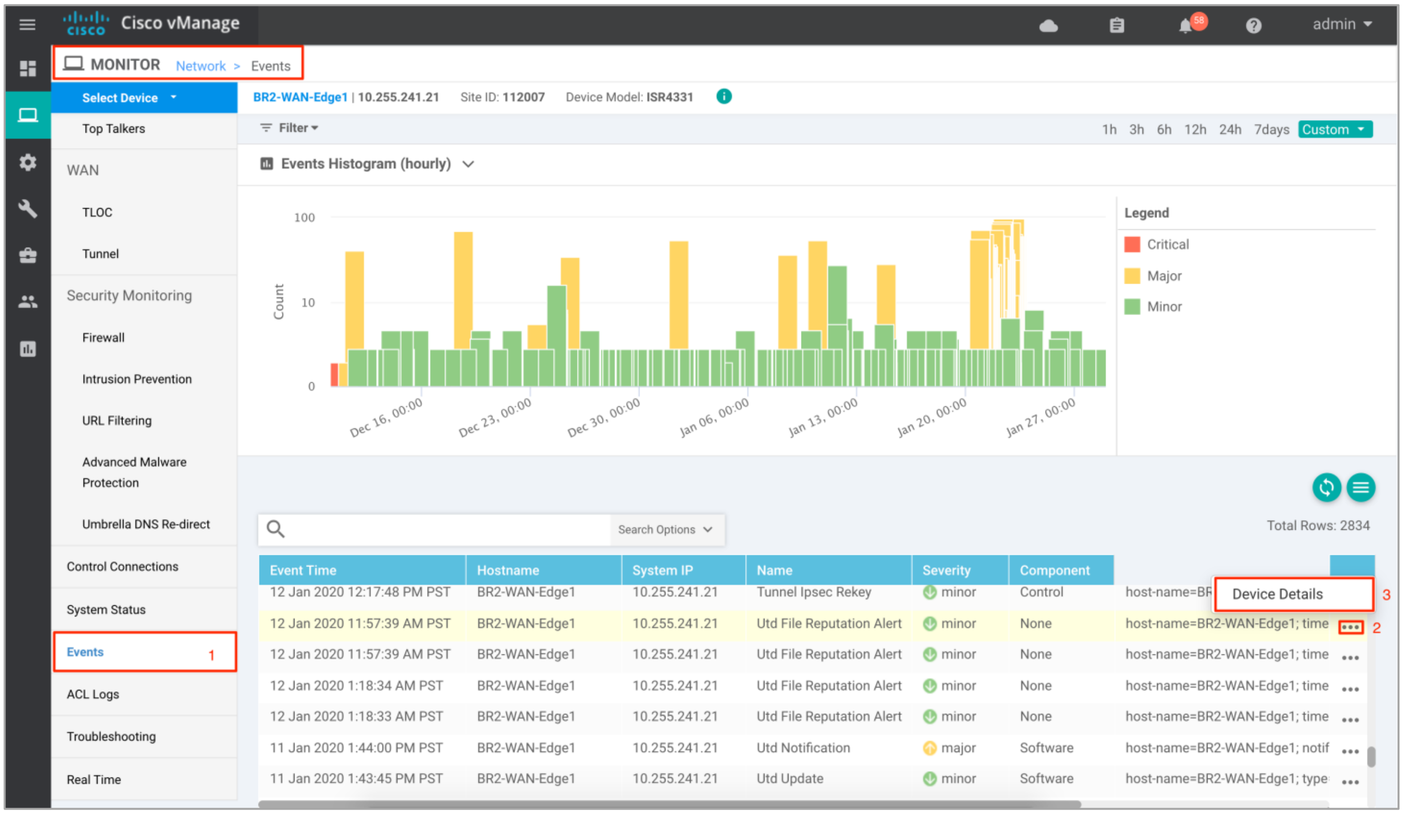
BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

Device Options: Security App File Reputation Status

Total Rows: 1

Device IP	Hostname	File Reputation Version	File Reputation Status	
10.255.241.21	BR2-WAN-Edge1	1.12.4.999	Connected	Connected to AMP Cloud!

Step 7. Next, click on **Events** from the left pane. Within **Network** > **Events**, click on the three dots **(...)** and then, click on the **Device Details** a pop-up window will appear.

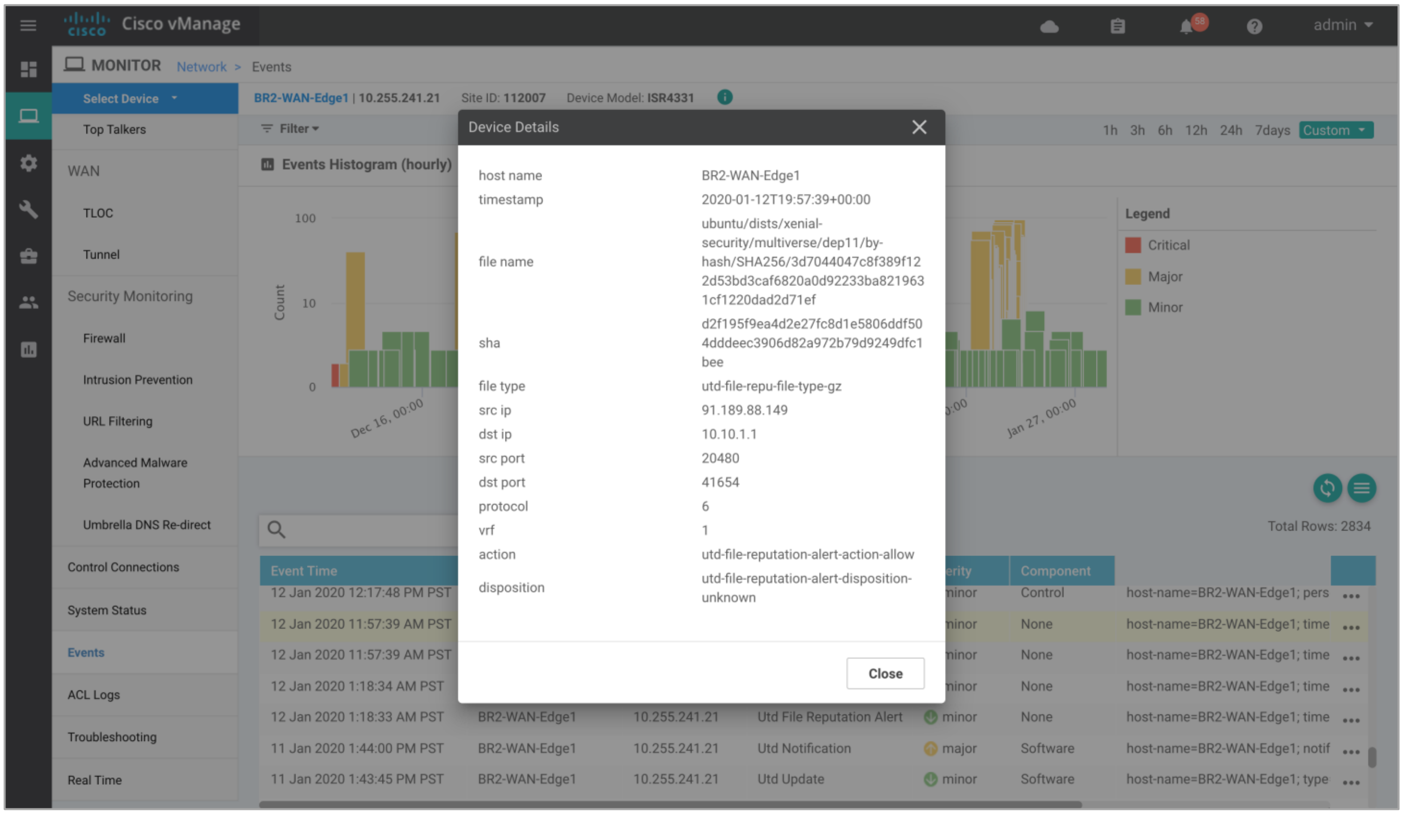


BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

Total Rows: 2834

Event Time	Hostname	System IP	Name	Severity	Component		
12 Jan 2020 12:17:48 PM PST	BR2-WAN-Edge1	10.255.241.21	Tunnel Ipsec Rekey	minor	Control	host-name=BR	
12 Jan 2020 11:57:39 AM PST	BR2-WAN-Edge1	10.255.241.21	Utd File Reputation Alert	minor	None	host-name=BR2-WAN-Edge1; time	...
12 Jan 2020 11:57:39 AM PST	BR2-WAN-Edge1	10.255.241.21	Utd File Reputation Alert	minor	None	host-name=BR2-WAN-Edge1; time	...
12 Jan 2020 1:18:34 AM PST	BR2-WAN-Edge1	10.255.241.21	Utd File Reputation Alert	minor	None	host-name=BR2-WAN-Edge1; time	...
12 Jan 2020 1:18:33 AM PST	BR2-WAN-Edge1	10.255.241.21	Utd File Reputation Alert	minor	None	host-name=BR2-WAN-Edge1; time	...
11 Jan 2020 1:44:00 PM PST	BR2-WAN-Edge1	10.255.241.21	Utd Notification	major	Software	host-name=BR2-WAN-Edge1; notif	...
11 Jan 2020 1:43:45 PM PST	BR2-WAN-Edge1	10.255.241.21	Utd Update	minor	Software	host-name=BR2-WAN-Edge1; type	...

In the pop-up window, you can find the device details that include file name, timestamp, and more.



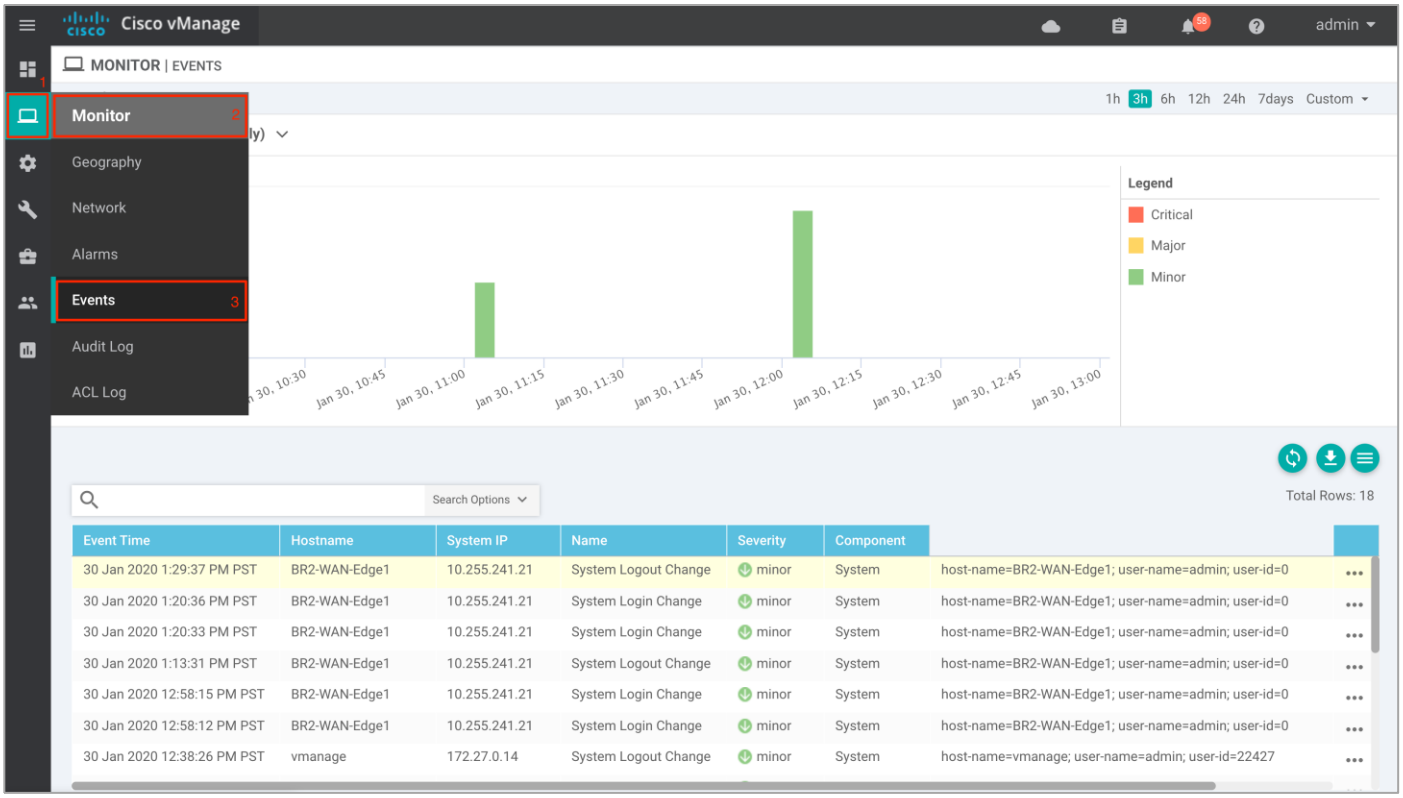
Device Details

host name	BR2-WAN-Edge1
timestamp	2020-01-12T19:57:39+00:00
file name	ubuntu/dists/xenial-security/multiverse/dep11/by-hash/SHA256/3d7044047c8f389f122d53bd3caf6820a0d92233ba8219631cf1220dad2d71ef
sha	d2f195f9ea4d2e27fc8d1e5806ddf504dddeec3906d82a972b79d9249dfc1bee
file type	utd-file-repu-file-type-gz
src ip	91.189.88.149
dst ip	10.10.1.1
src port	20480
dst port	41654
protocol	6
vrf	1
action	utd-file-reputation-alert-action-allow
disposition	utd-file-reputation-alert-disposition-unknown

Close

Event Time				erity	Component		
12 Jan 2020 12:17:48 PM PST				minor	Control	host-name=BR2-WAN-Edge1; pers	•••
12 Jan 2020 11:57:39 AM PST				minor	None	host-name=BR2-WAN-Edge1; time	•••
12 Jan 2020 11:57:39 AM PST				minor	None	host-name=BR2-WAN-Edge1; time	•••
12 Jan 2020 1:18:34 AM PST				minor	None	host-name=BR2-WAN-Edge1; time	•••
12 Jan 2020 1:18:33 AM PST	BR2-WAN-Edge1	10.255.241.21	Utd File Reputation Alert	minor	None	host-name=BR2-WAN-Edge1; time	•••
11 Jan 2020 1:44:00 PM PST	BR2-WAN-Edge1	10.255.241.21	Utd Notification	major	Software	host-name=BR2-WAN-Edge1; notif	•••
11 Jan 2020 1:43:45 PM PST	BR2-WAN-Edge1	10.255.241.21	Utd Update	minor	Software	host-name=BR2-WAN-Edge1; type	•••

Note, you can also navigate to **Events** page from the **Monitor** tab.

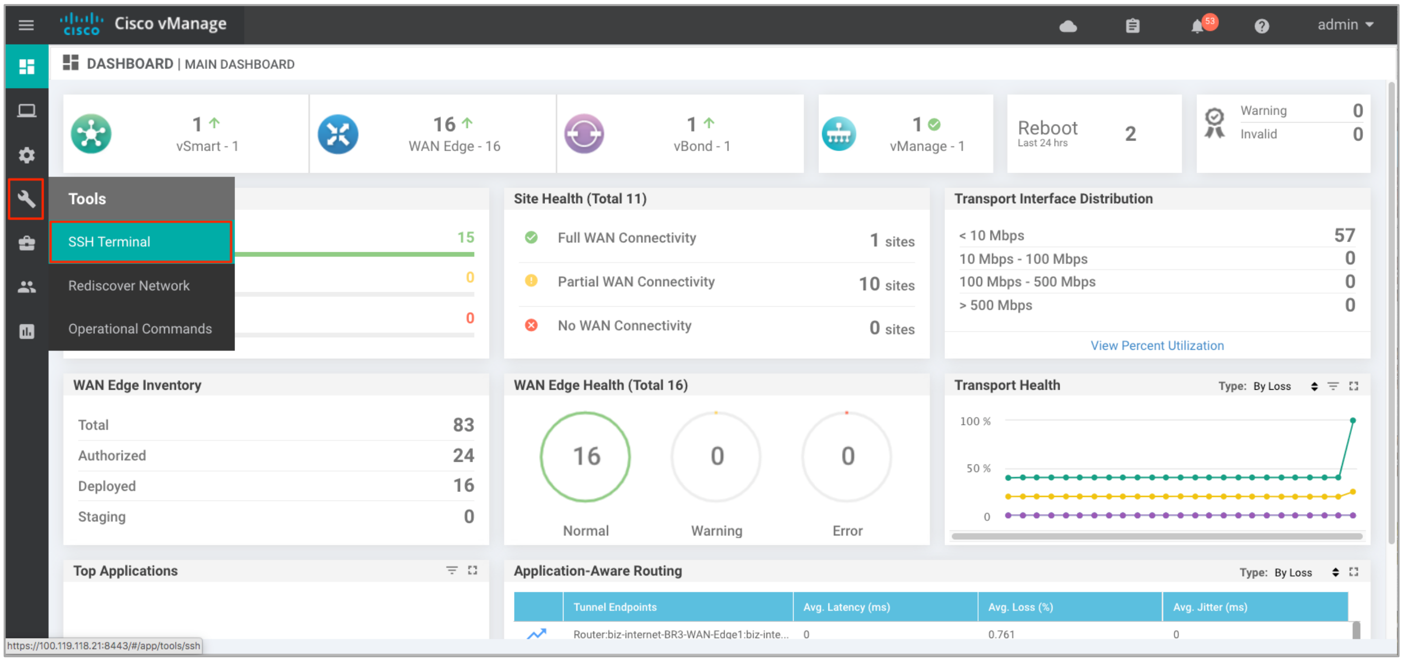


Event Time	Hostname	System IP	Name	Severity	Component		
30 Jan 2020 1:29:37 PM PST	BR2-WAN-Edge1	10.255.241.21	System Logout Change	minor	System	host-name=BR2-WAN-Edge1; user-name=admin; user-id=0	•••
30 Jan 2020 1:20:36 PM PST	BR2-WAN-Edge1	10.255.241.21	System Login Change	minor	System	host-name=BR2-WAN-Edge1; user-name=admin; user-id=0	•••
30 Jan 2020 1:20:33 PM PST	BR2-WAN-Edge1	10.255.241.21	System Login Change	minor	System	host-name=BR2-WAN-Edge1; user-name=admin; user-id=0	•••
30 Jan 2020 1:13:31 PM PST	BR2-WAN-Edge1	10.255.241.21	System Logout Change	minor	System	host-name=BR2-WAN-Edge1; user-name=admin; user-id=0	•••
30 Jan 2020 12:58:15 PM PST	BR2-WAN-Edge1	10.255.241.21	System Login Change	minor	System	host-name=BR2-WAN-Edge1; user-name=admin; user-id=0	•••
30 Jan 2020 12:58:12 PM PST	BR2-WAN-Edge1	10.255.241.21	System Login Change	minor	System	host-name=BR2-WAN-Edge1; user-name=admin; user-id=0	•••
30 Jan 2020 12:38:26 PM PST	vmanage	172.27.0.14	System Logout Change	minor	System	host-name=vmanage; user-name=admin; user-id=22427	•••

Procedure 3. Monitor Advanced Malware Protection Feature and Statistics via vManage SSH Server Dashboard

Using the vManage NMS dashboard, you can monitor the AMP feature via CLI commands.

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



1 vSmart - 1 | 16 WAN Edge - 16 | 1 vBond - 1 | 1 vManage - 1 | Reboot Last 24 hrs 2 | Warning 0 Invalid 0

Site Health (Total 11)

Full WAN Connectivity	1 sites
Partial WAN Connectivity	10 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): 16 Normal, 0 Warning, 0 Error

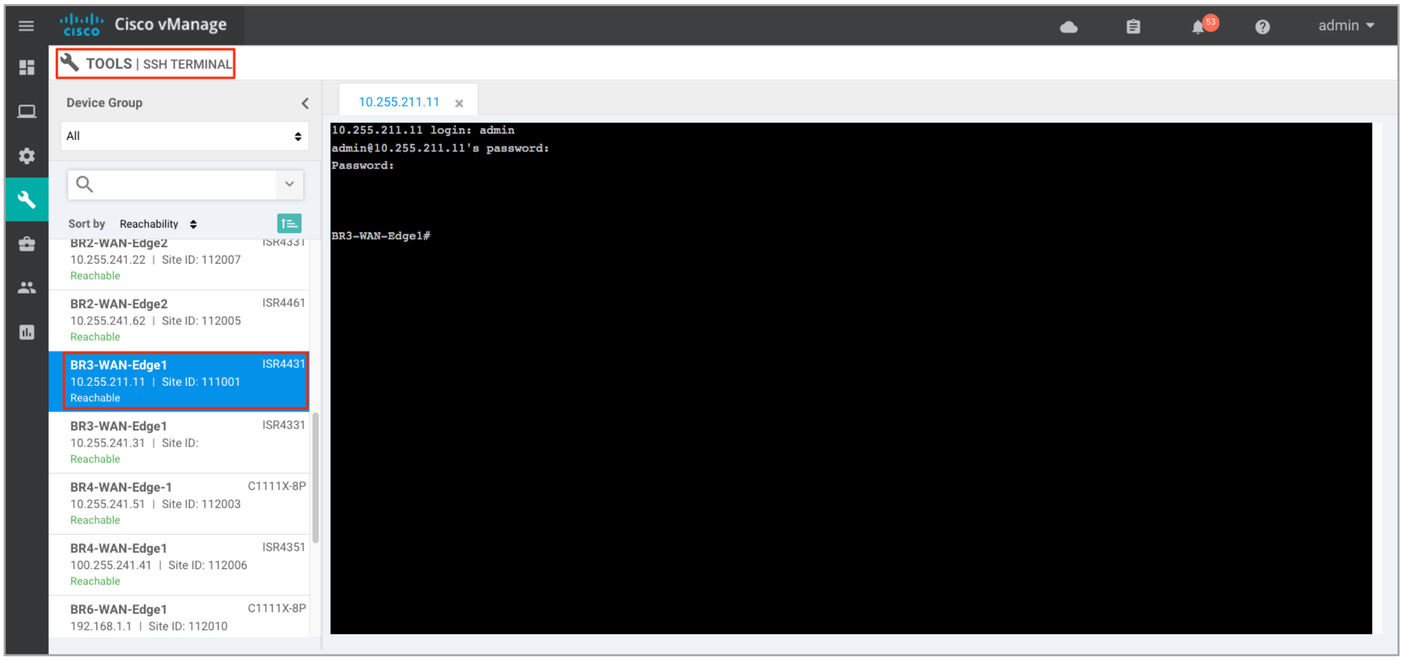
Transport Health — Type: By Loss — 100 %, 50 %, 0

Top Applications

Application-Aware Routing — Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:biz-internet-BR3-WAN-Edge1:biz-inte...	0	0.761	0

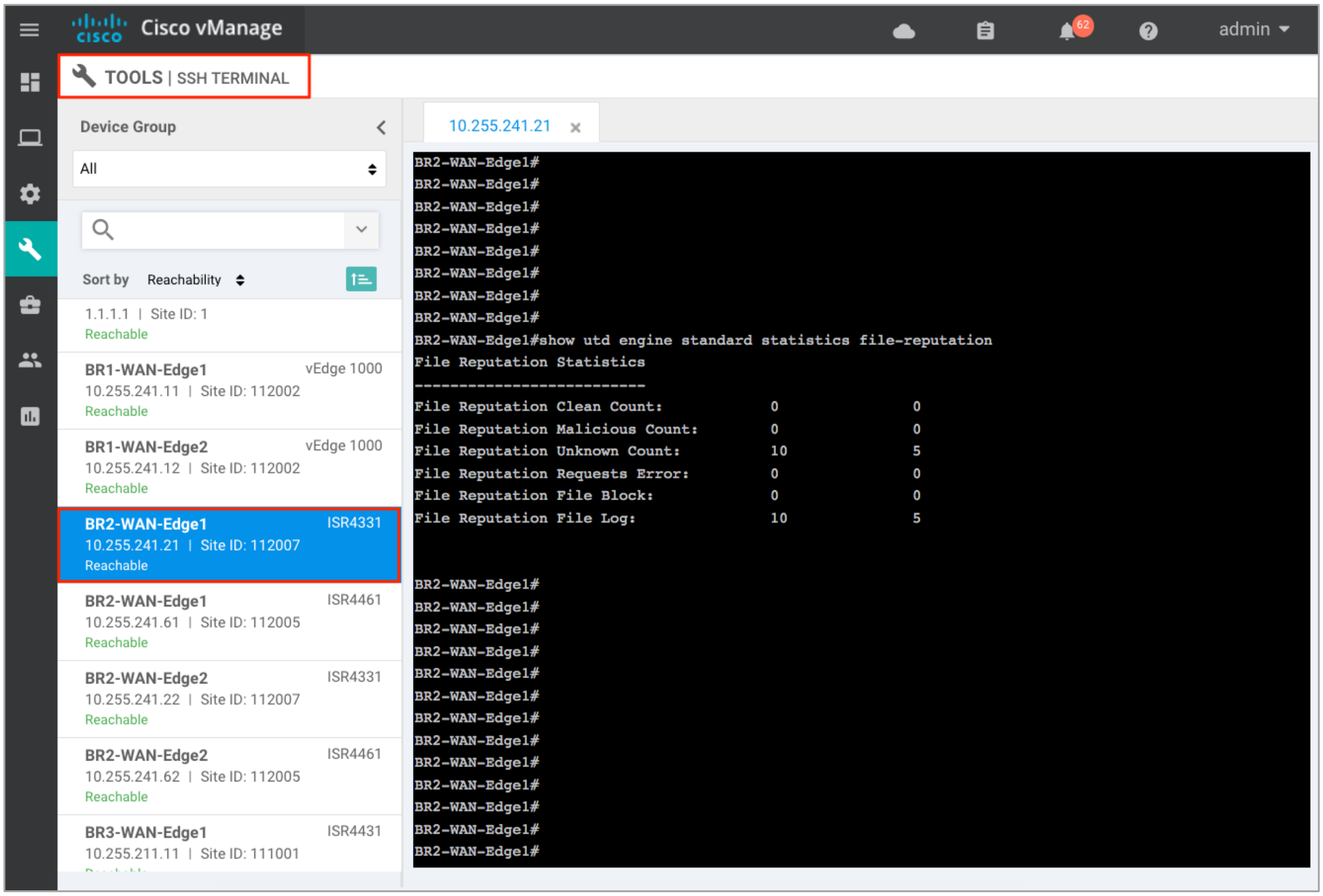
Step 2. Select the device from the list of devices, and login.



Device	Model
BR2-WAN-Edge2 10.255.241.22 | Site ID: 112007 Reachable	ISR4331
BR2-WAN-Edge2 10.255.241.62 | Site ID: 112005 Reachable	ISR4461
BR3-WAN-Edge1 10.255.211.11 | Site ID: 111001 Reachable	ISR4431
BR3-WAN-Edge1 10.255.241.31 | Site ID: Reachable	ISR4331
BR4-WAN-Edge-1 10.255.241.51 | Site ID: 112003 Reachable	C1111X-8P
BR4-WAN-Edge1 100.255.241.41 | Site ID: 112006 Reachable	ISR4351
BR6-WAN-Edge1 192.168.1.1 | Site ID: 112010	C1111X-8P

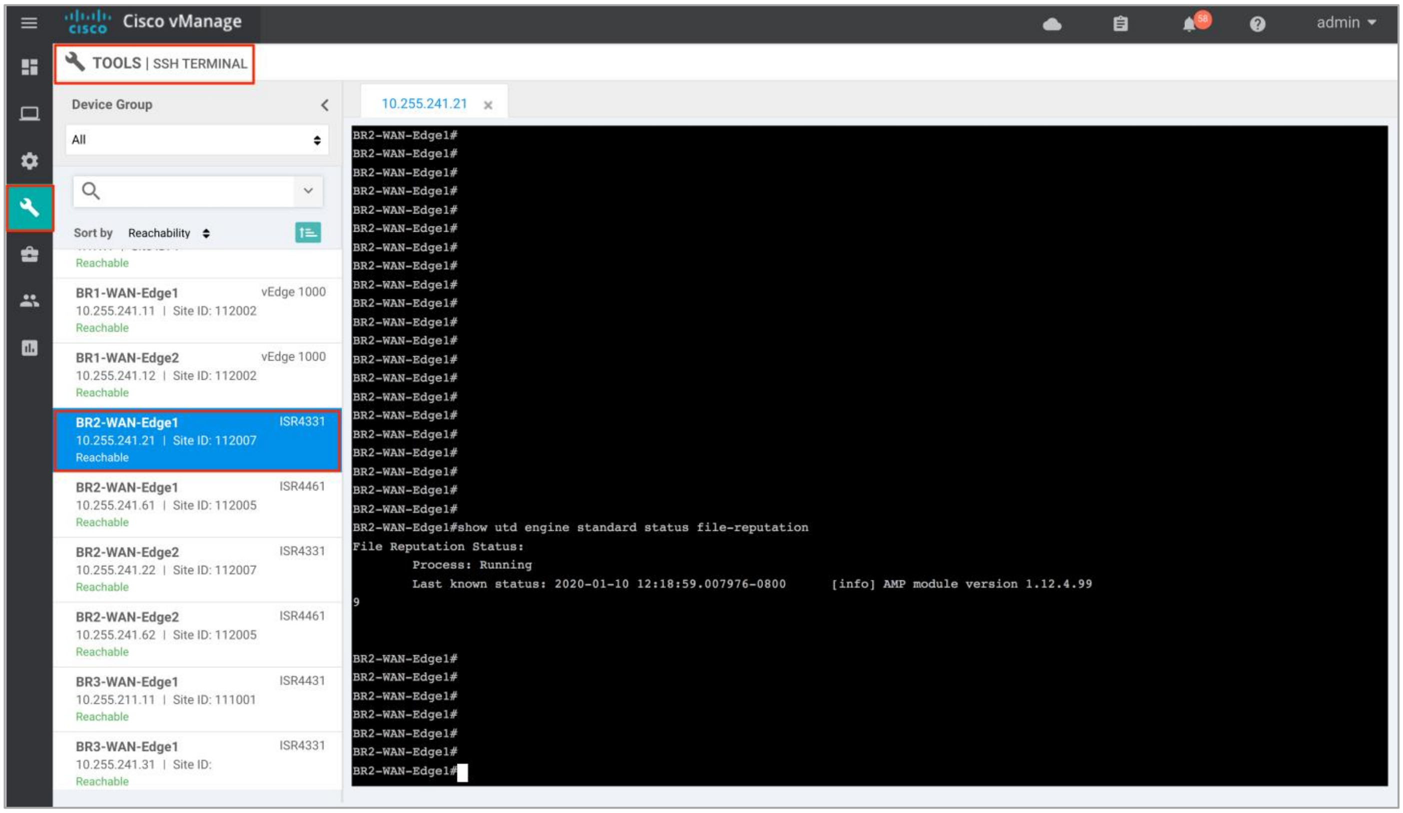
```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:



BR3-WAN-Edge1#
```

Step 3. To view the File Reputation statistics, enter the CLI command – ***show utd engine standard statistics file-reputation***. The output displays the number of clean, malicious and unknown files.



```
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show utd engine standard statistics file-reputation
File Reputation Statistics
--------------------------
File Reputation Clean Count:            0               0
File Reputation Malicious Count:        0               0
File Reputation Unknown Count:          10              5
File Reputation Requests Error:         0               0
File Reputation File Block:             0               0
File Reputation File Log:               10              5


BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
```

Step 4. To view the file reputation status, enter the CLI command – ***show utd engine standard status file-reputation***.



Reachable

BR1-WAN-Edge1 vEdge 1000
10.255.241.11 | Site ID: 112002
Reachable

BR1-WAN-Edge2 vEdge 1000
10.255.241.12 | Site ID: 112002
Reachable

BR2-WAN-Edge1 ISR4331
10.255.241.21 | Site ID: 112007
Reachable

BR2-WAN-Edge1 ISR4461
10.255.241.61 | Site ID: 112005
Reachable

BR2-WAN-Edge2 ISR4331
10.255.241.22 | Site ID: 112007
Reachable

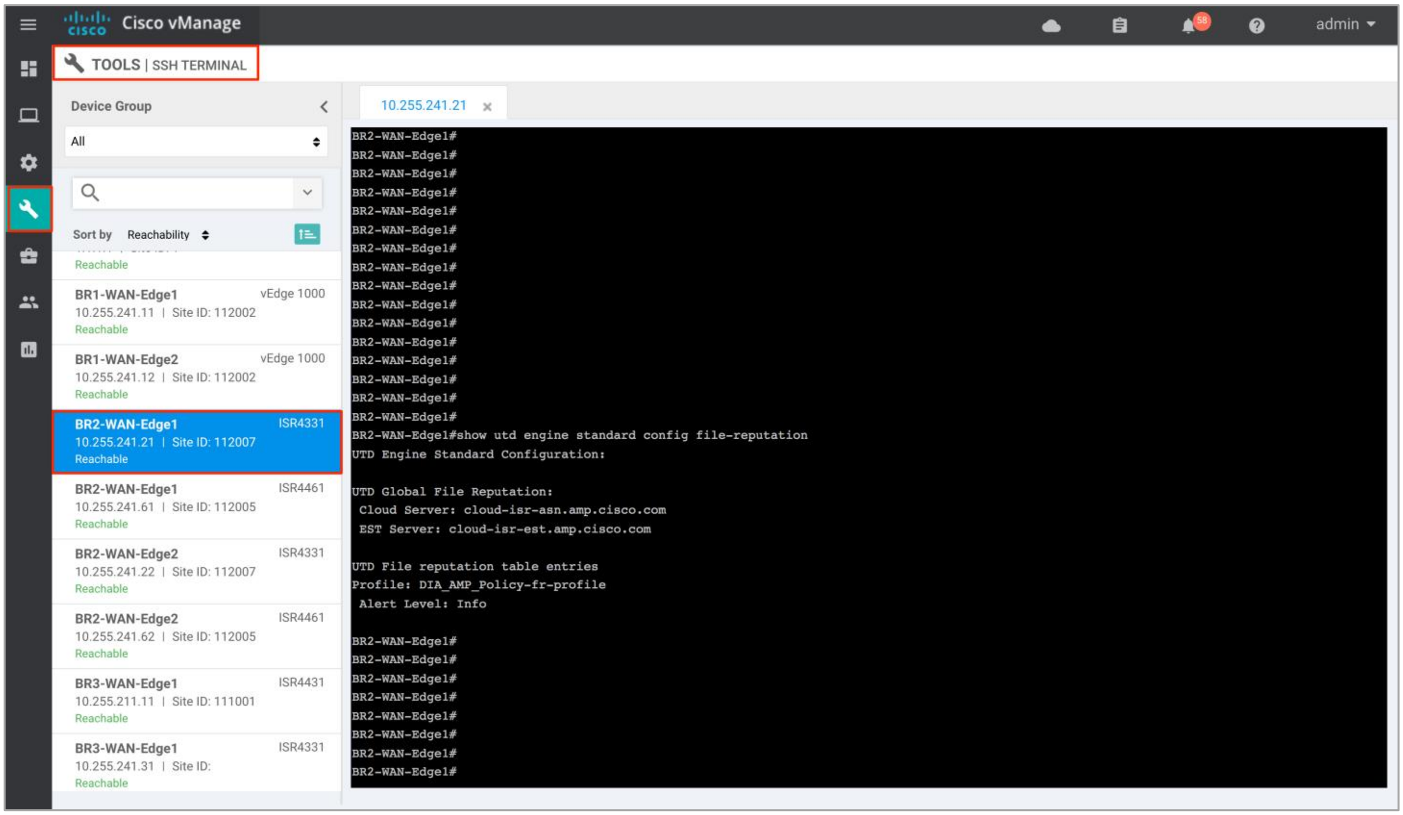
BR2-WAN-Edge2 ISR4461
10.255.241.62 | Site ID: 112005
Reachable

BR3-WAN-Edge1 ISR4431
10.255.211.11 | Site ID: 111001
Reachable

BR3-WAN-Edge1 ISR4331
10.255.241.31 | Site ID:
Reachable

```
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show utd engine standard status file-reputation
File Reputation Status:
        Process: Running
        Last known status: 2020-01-10 12:18:59.007976-0800      [info] AMP module version 1.12.4.99
9


BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
```

Step 5. To view the UTD engine standard configuration, enter the CLI command - ***show utd engine standard config file-reputation***.



Reachable

BR1-WAN-Edge1 vEdge 1000
10.255.241.11 | Site ID: 112002
Reachable

BR1-WAN-Edge2 vEdge 1000
10.255.241.12 | Site ID: 112002
Reachable

BR2-WAN-Edge1 ISR4331
10.255.241.21 | Site ID: 112007
Reachable

BR2-WAN-Edge1 ISR4461
10.255.241.61 | Site ID: 112005
Reachable

BR2-WAN-Edge2 ISR4331
10.255.241.22 | Site ID: 112007
Reachable

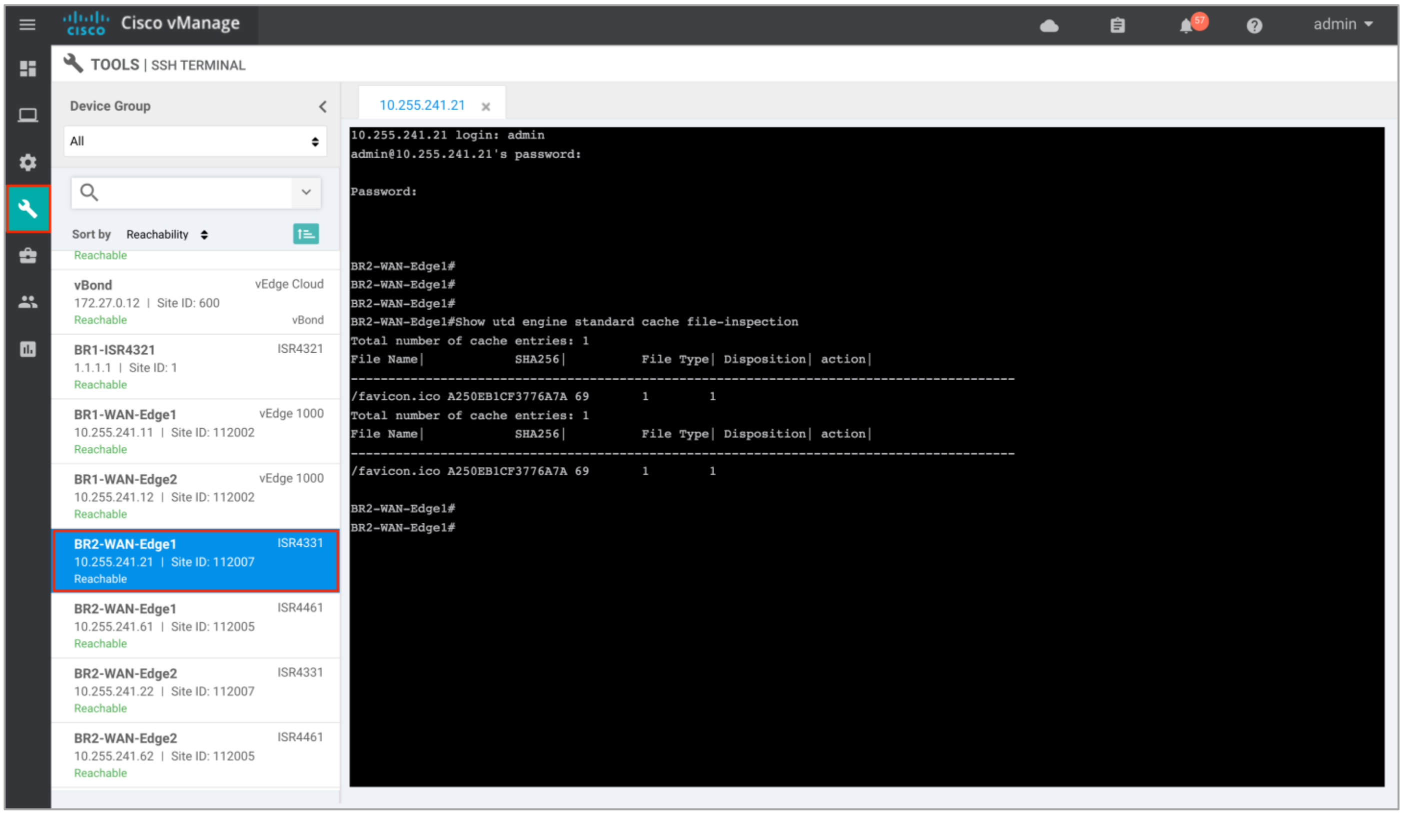
BR2-WAN-Edge2 ISR4461
10.255.241.62 | Site ID: 112005
Reachable

BR3-WAN-Edge1 ISR4431
10.255.211.11 | Site ID: 111001
Reachable

BR3-WAN-Edge1 ISR4331
10.255.241.31 | Site ID:
Reachable

```
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show utd engine standard config file-reputation
UTD Engine Standard Configuration:

UTD Global File Reputation:
 Cloud Server: cloud-isr-asn.amp.cisco.com
 EST Server: cloud-isr-est.amp.cisco.com

UTD File reputation table entries
Profile: DIA_AMP_Policy-fr-profile
 Alert Level: Info

BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
```

Step 6. To display the total number of cached entries, enter the CLI command - ***show utd engine standard cache file-inspection***.



Reachable

vBond vEdge Cloud
172.27.0.12 | Site ID: 600
Reachable vBond

BR1-ISR4321 ISR4321
1.1.1.1 | Site ID: 1
Reachable

BR1-WAN-Edge1 vEdge 1000
10.255.241.11 | Site ID: 112002
Reachable

BR1-WAN-Edge2 vEdge 1000
10.255.241.12 | Site ID: 112002
Reachable

BR2-WAN-Edge1 ISR4331
10.255.241.21 | Site ID: 112007
Reachable

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

```
10.255.241.21 login: admin
admin@10.255.241.21's password:

Password:



BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#Show utd engine standard cache file-inspection
Total number of cache entries: 1
File Name|            SHA256|          File Type| Disposition| action|
-----------------------------------------------------------------------------------------
/favicon.ico A250EB1CF3776A7A 69       1        1
Total number of cache entries: 1
File Name|            SHA256|          File Type| Disposition| action|
-----------------------------------------------------------------------------------------
/favicon.ico A250EB1CF3776A7A 69       1        1

BR2-WAN-Edge1#
BR2-WAN-Edge1#
```

Outside the listed CLI commands, some of the other commands that are useful include ***show platform hardware qfp active feature utd config*** and ***show log***.

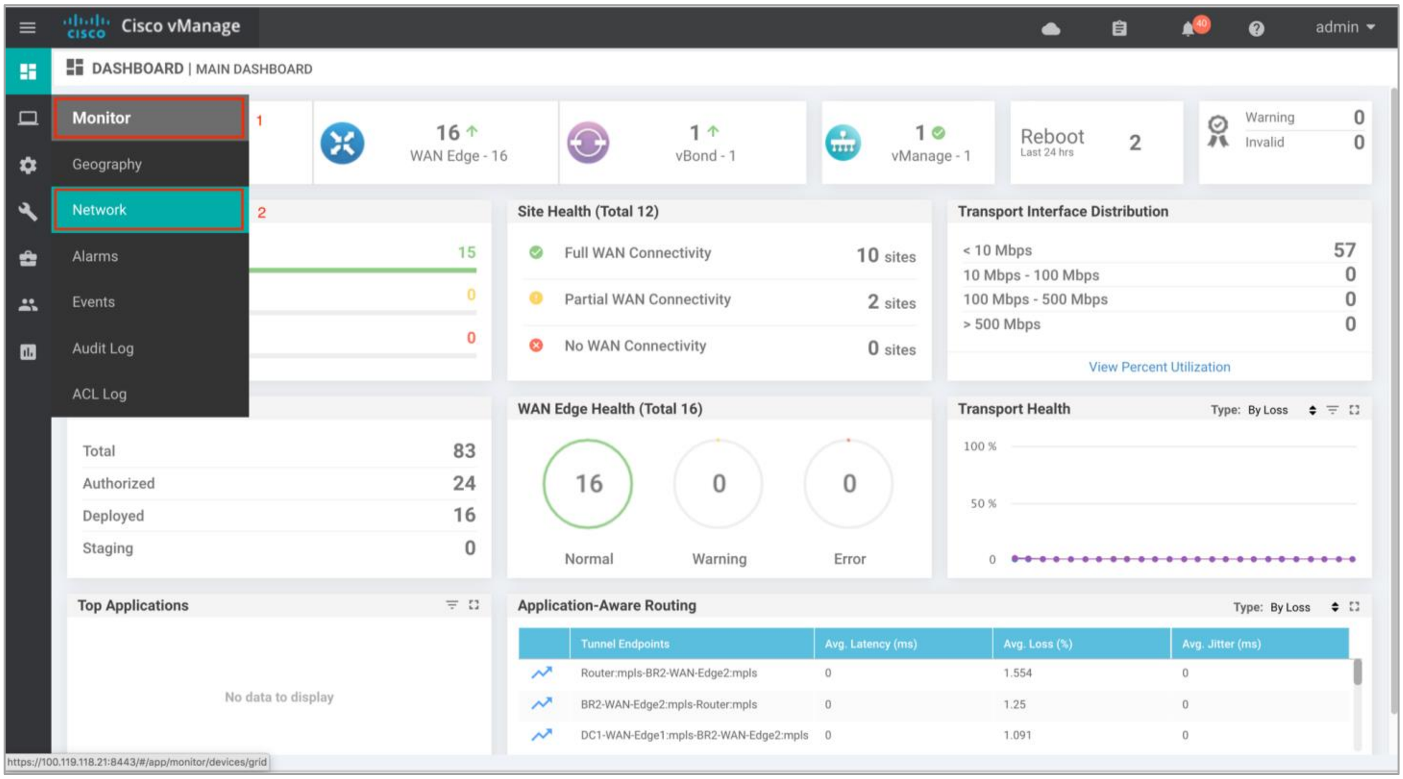
Process 5: Monitor DNS/ Web-layer Security via vManage NMS

Monitor DNS/Web-layer security using the vManage dashboard.

Procedure 1. Monitor DNS/ Web-layer Security Feature via vManage Monitor Dashboard

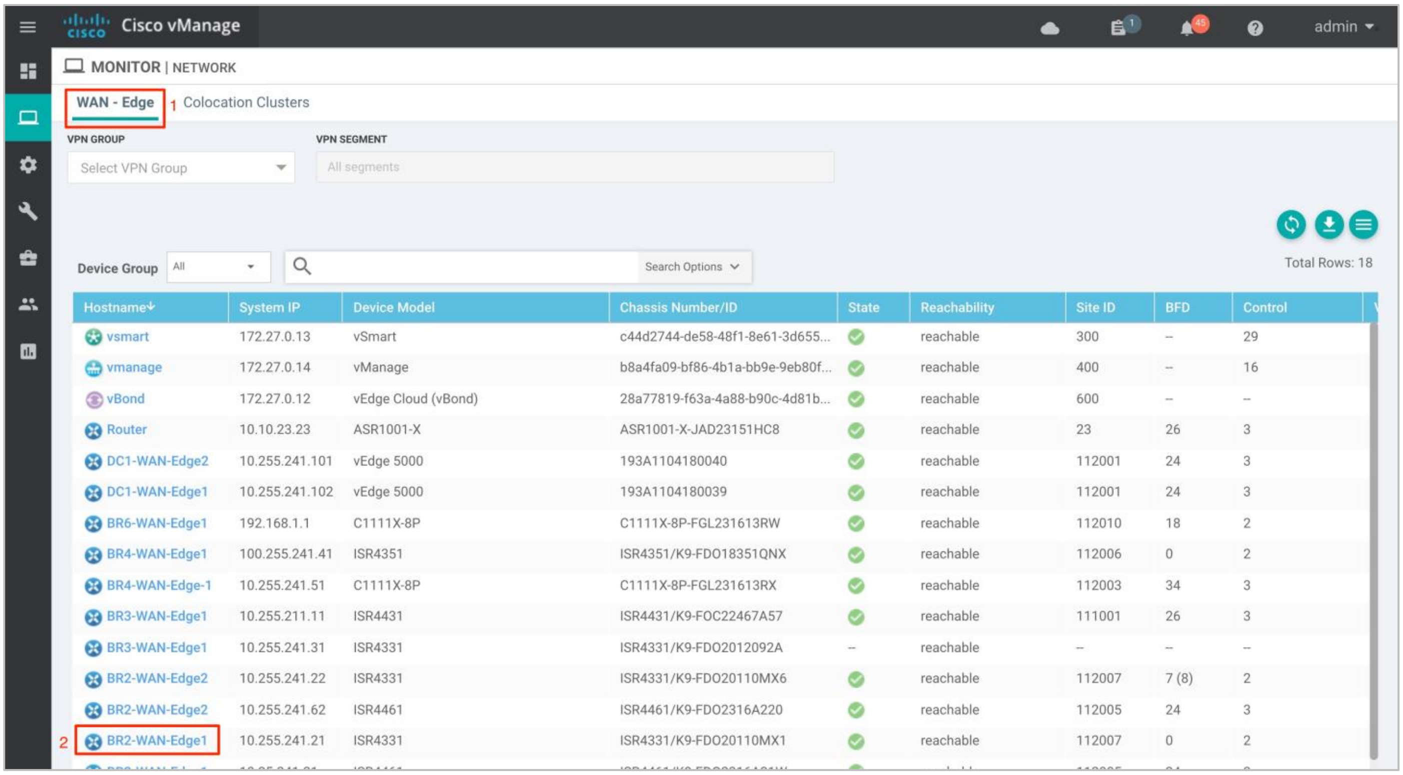
Using the vManage NMS dashboard, you can view the DNS/ Web-layer security feature via the monitor dashboard contained within vManage.

Step 1. Navigate to **Network** within **Monitor** available on the left pane and click on the WAN Edge device you wish to monitor.



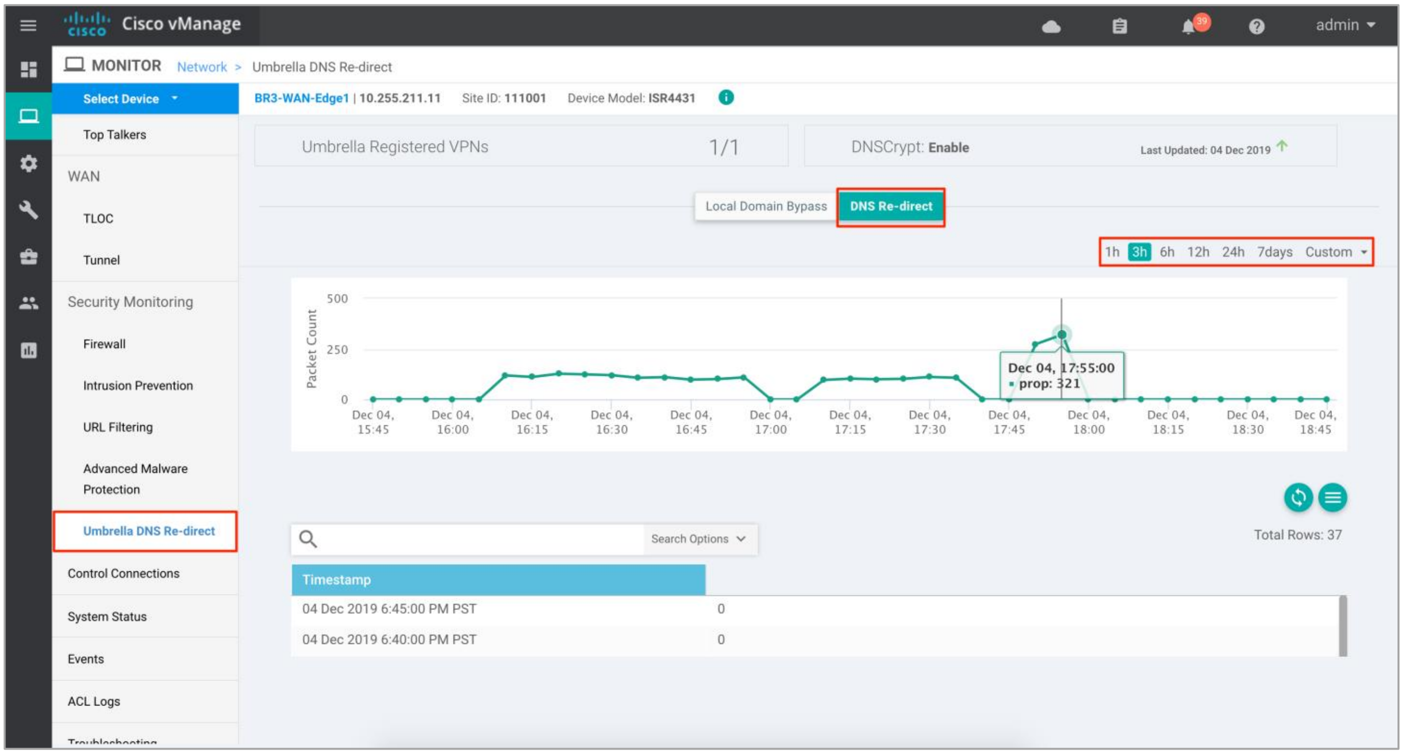
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0
BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0
DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0

Step 2. Click on a specific WAN Edge device to monitor the DNS Security 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 3. Click on the **Umbrella** DNS **Re-direct** tab under **Security Monitoring** from the left pane for the number of packets redirected to umbrella.



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

Umbrella Registered VPNs 1/1

DNSCrypt: Enable

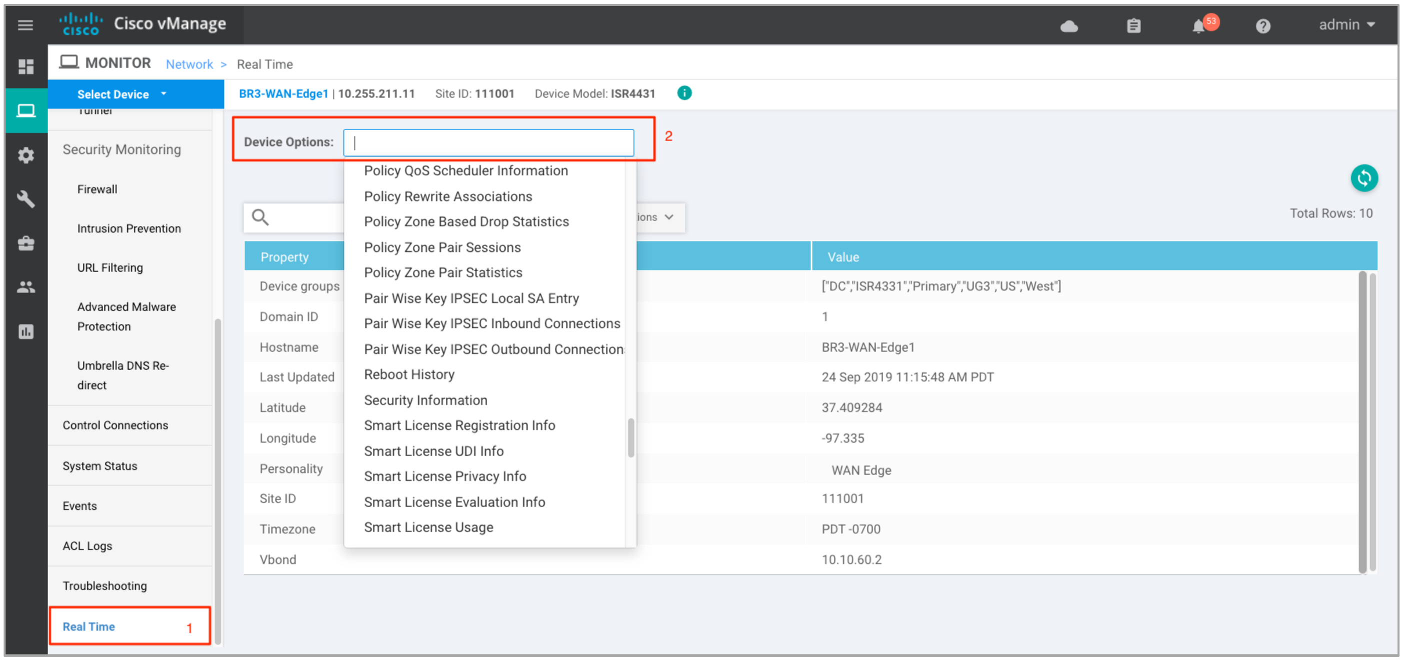
Last Updated: 04 Dec 2019

Total Rows: 37

Timestamp	
04 Dec 2019 6:45:00 PM PST	0
04 Dec 2019 6:40:00 PM PST	0

Click on **Local Domain Bypass** to view packets that bypassed umbrella or the configured remote DNS server.

Step 4. Next, click on **Real Time** from the left pane. Within **Network** > **Real time** and pop-up screen will appear with **Device Options.** Click on 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
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
Search Options

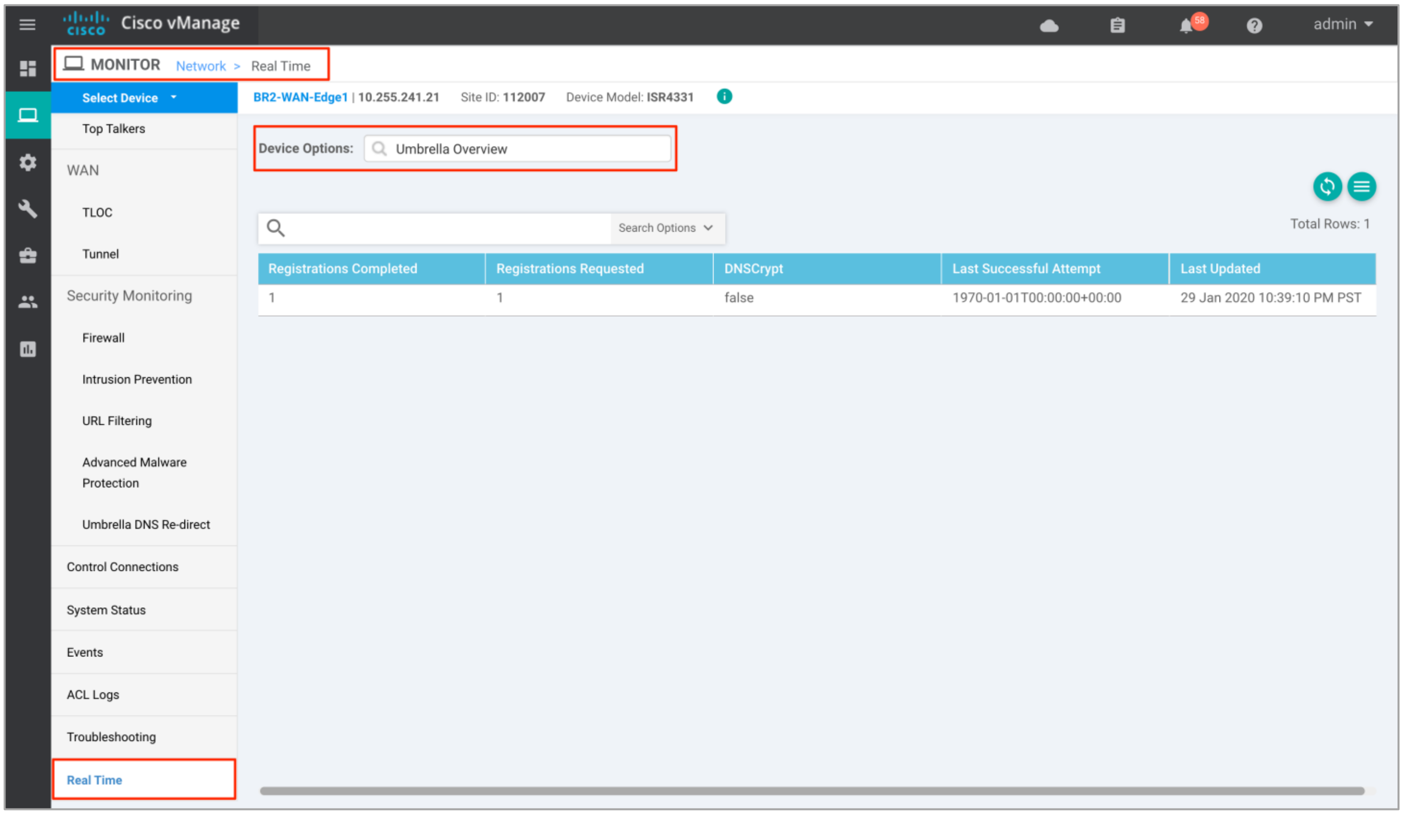
BR3-WAN-Edge1 | 10.255.211.11 Site ID: 111001 Device Model: ISR4431

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 5. For the Cisco Umbrella Connector overview, click on **Umbrella overview / Umbrella Device Registration**.

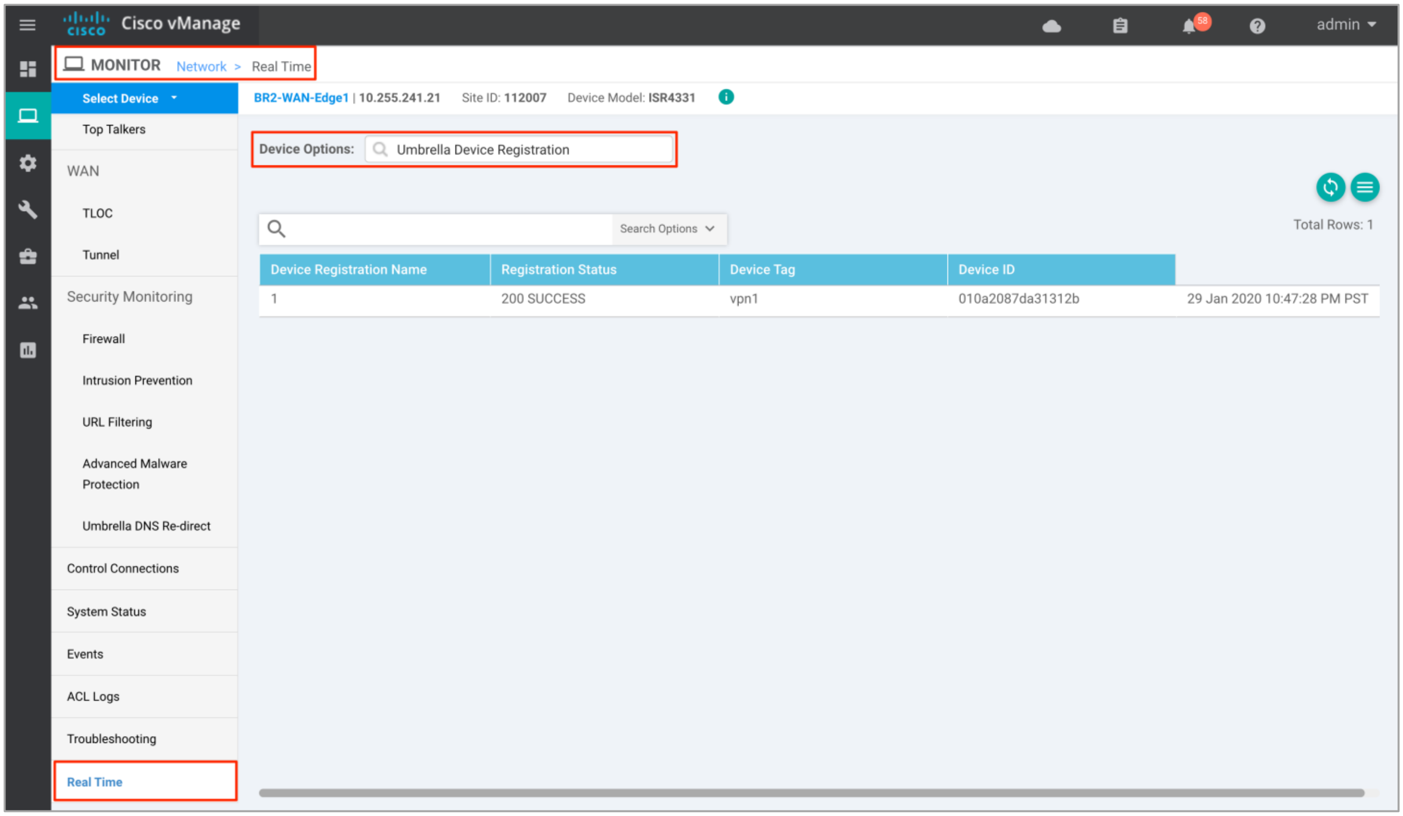


BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

Device Options: Umbrella Overview

Total Rows: 1

Registrations Completed	Registrations Requested	DNSCrypt	Last Successful Attempt	Last Updated
1	1	false	1970-01-01T00:00:00+00:00	29 Jan 2020 10:39:10 PM PST



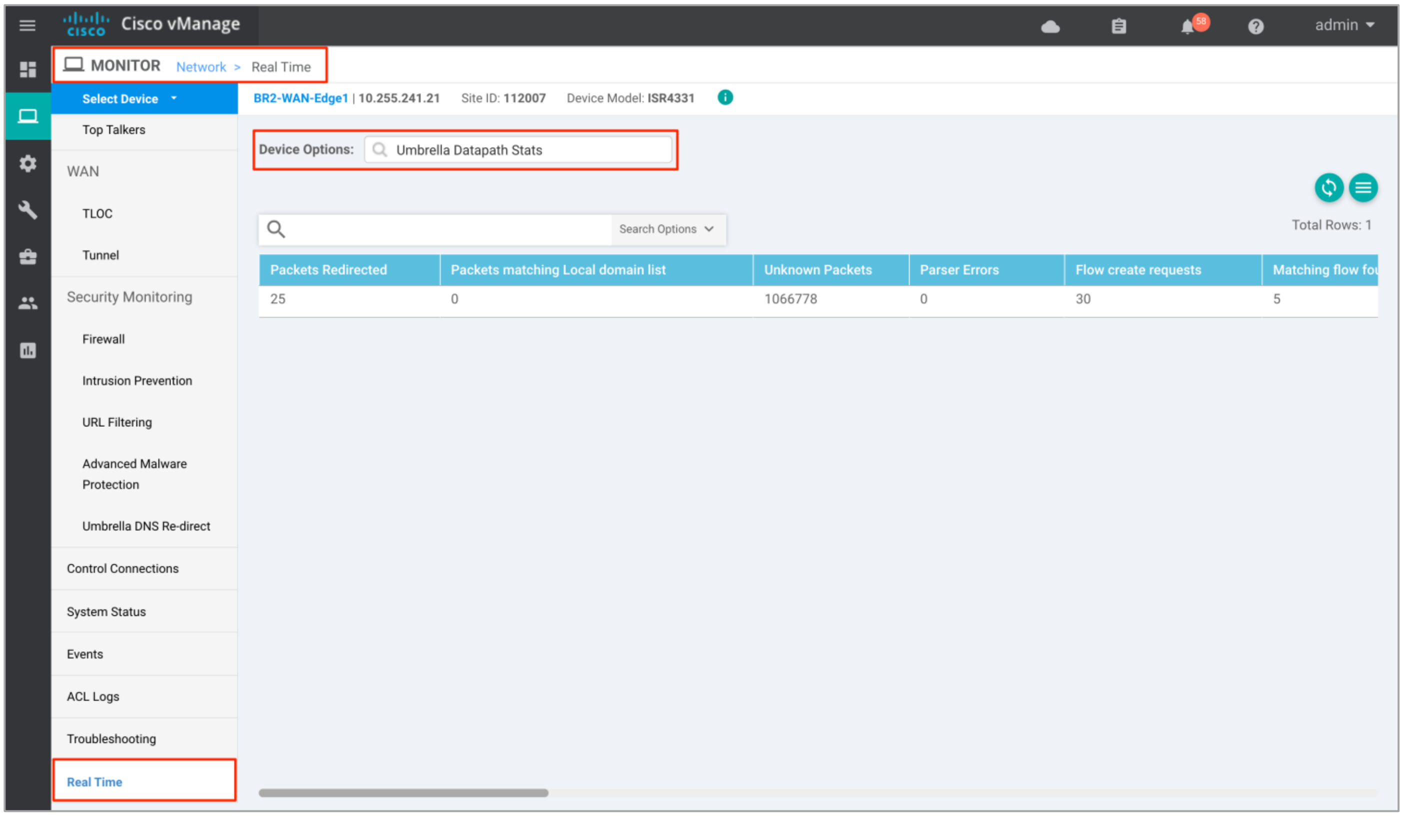
BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

Device Options: Umbrella Device Registration

Total Rows: 1

Device Registration Name	Registration Status	Device Tag	Device ID	
1	200 SUCCESS	vpn1	010a2087da31312b	29 Jan 2020 10:47:28 PM PST

Step 6. To view the packet statistics, click **Umbrella Datapath Statistics**.



BR2-WAN-Edge1 | 10.255.241.21 Site ID: 112007 Device Model: ISR4331

Device Options: Umbrella Datapath Stats

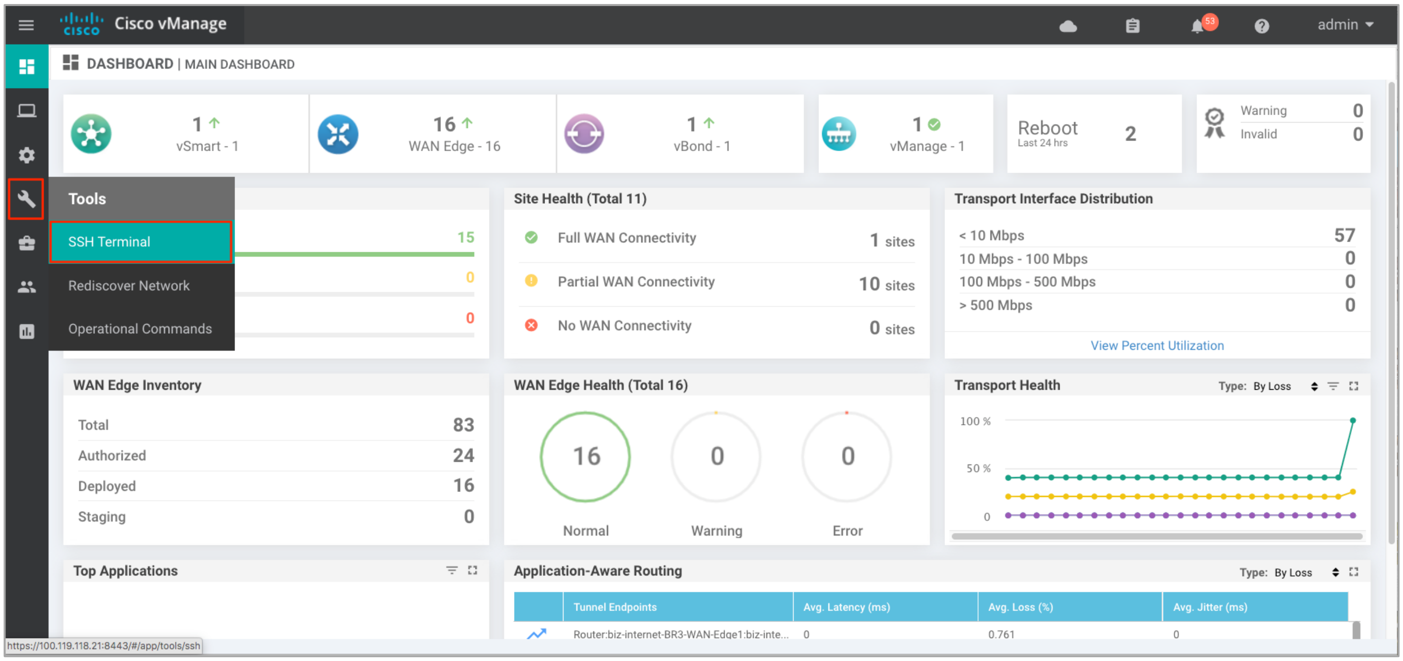
Total Rows: 1

Packets Redirected	Packets matching Local domain list	Unknown Packets	Parser Errors	Flow create requests	Matching flow fo
25	0	1066778	0	30	5

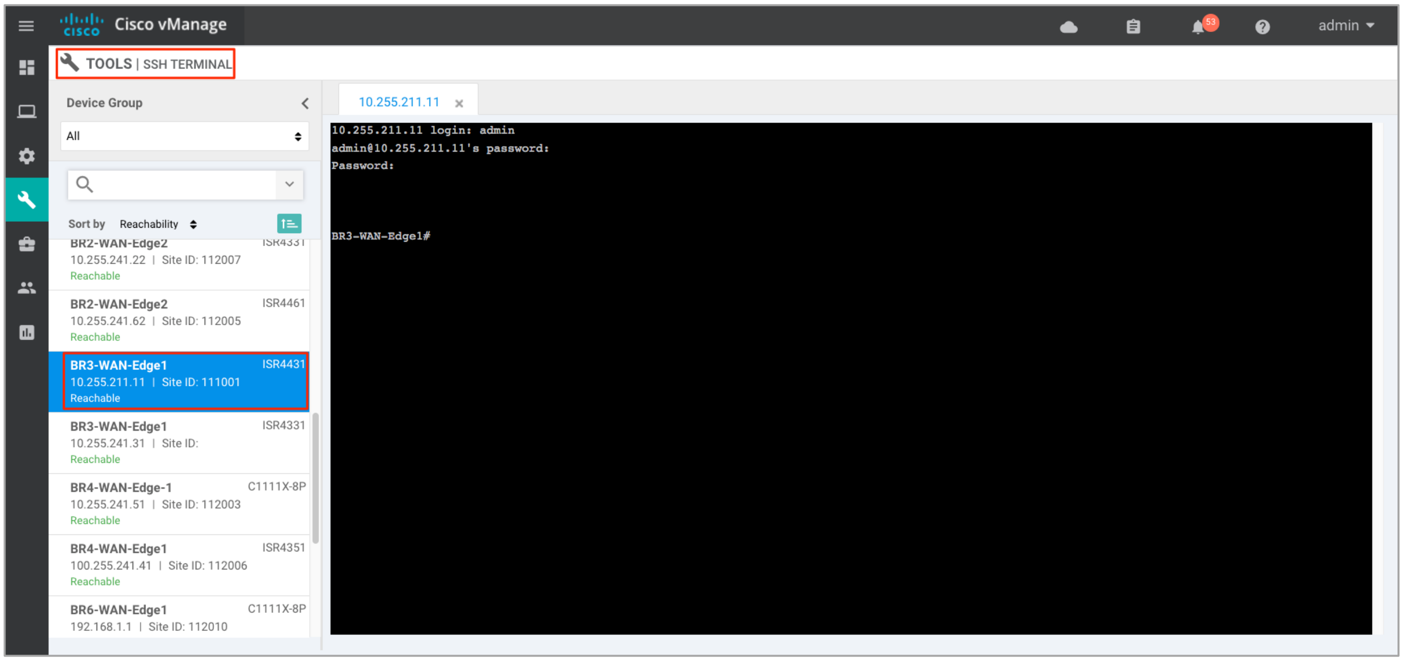
Procedure 2. Monitor DNS/ Web-layer Security Feature and Statistics via vManage SSH Server Dashboard

Using the vManage NMS dashboard, you can monitor the DNS/ Web-layer Security feature via CLI commands.

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



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

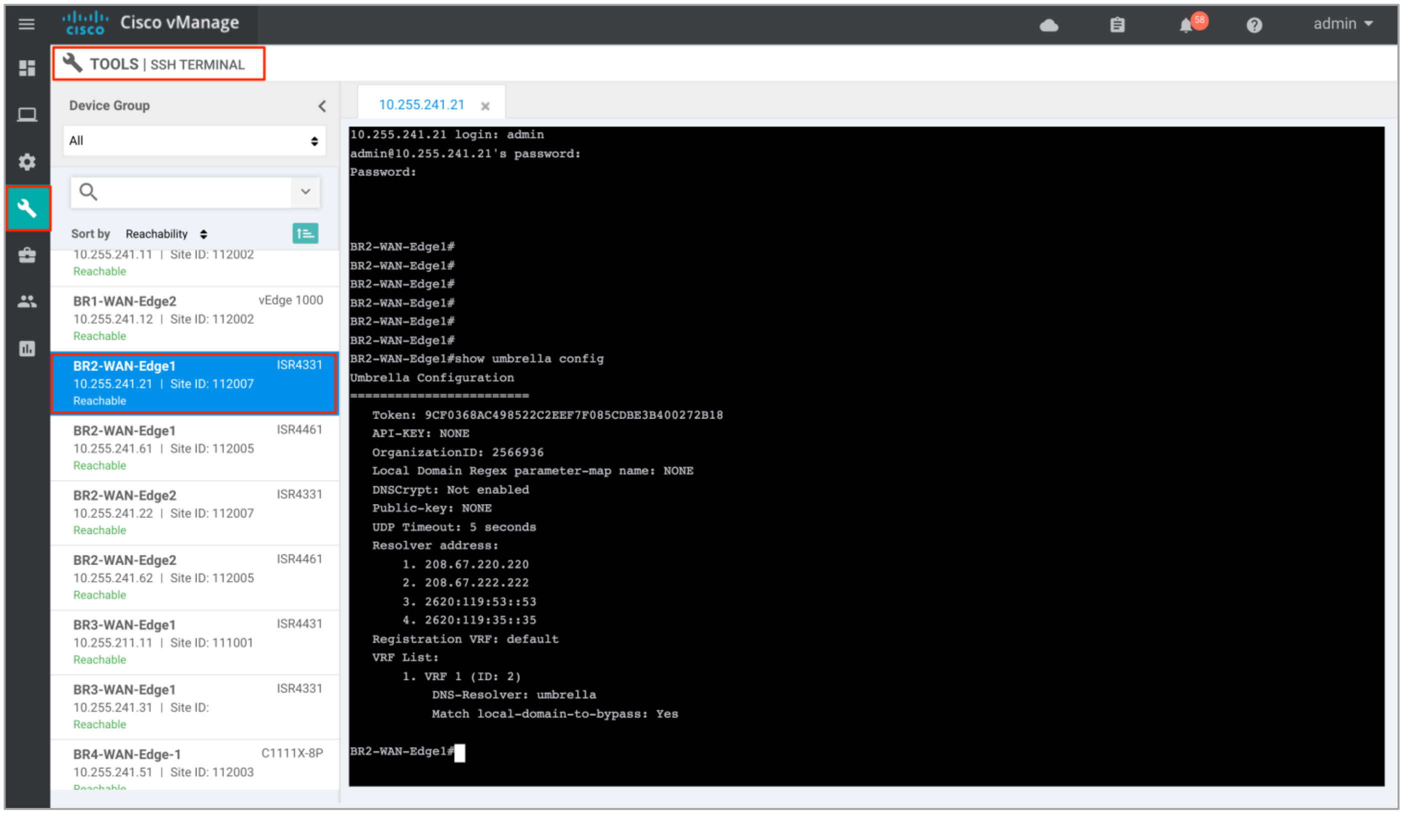


```
10.255.211.11 login: admin
admin@10.255.211.11's password:
Password:



BR3-WAN-Edge1#
```

Step 3. Enter the following CLI command to verify the Cisco Umbrella Connector configuration.

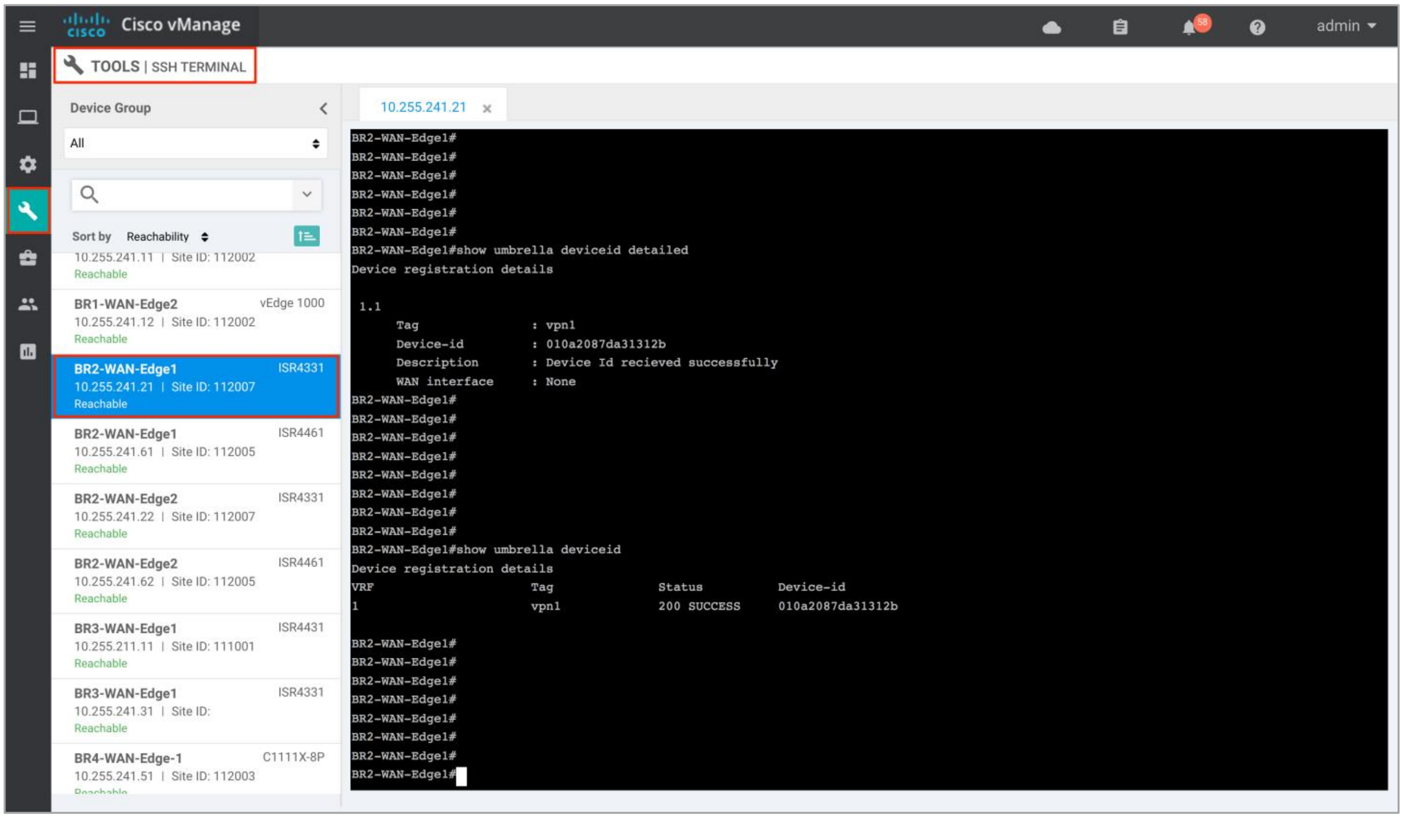
- show umbrella <config/deviceid/ dnscypt>
- show umbrella <device-registration/ dp-stats/ overview>

Output of show umbrella config:



```
10.255.241.21 login: admin
admin@10.255.241.21's password:
Password:



BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show umbrella config
Umbrella Configuration
========================
   Token: 9CF0368AC498522C2EEF7F085CDBE3B400272B18
   API-KEY: NONE
   OrganizationID: 2566936
   Local Domain Regex parameter-map name: NONE
   DNSCrypt: Not enabled
   Public-key: NONE
   UDP Timeout: 5 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
   Registration VRF: default
   VRF List:
       1. VRF 1 (ID: 2)
           DNS-Resolver: umbrella
           Match local-domain-to-bypass: Yes

BR2-WAN-Edge1#
```

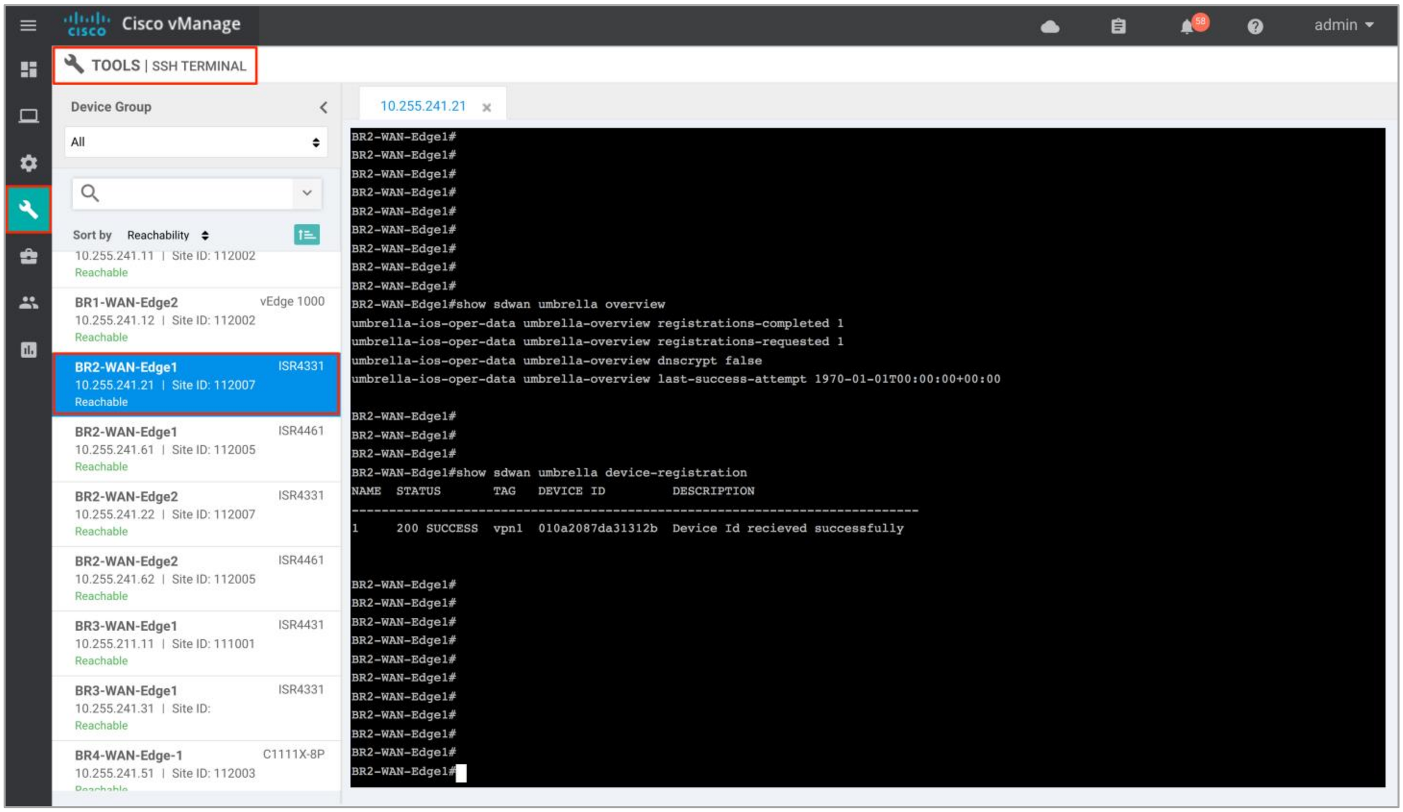
Output of show umbrella deviceid <detailed>:



```
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show umbrella deviceid detailed
Device registration details

 1.1
     Tag              : vpn1
     Device-id        : 010a2087da31312b
     Description      : Device Id recieved successfully
     WAN interface    : None
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show umbrella deviceid
Device registration details
VRF                     Tag              Status          Device-id
1                       vpn1             200 SUCCESS     010a2087da31312b

BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
```

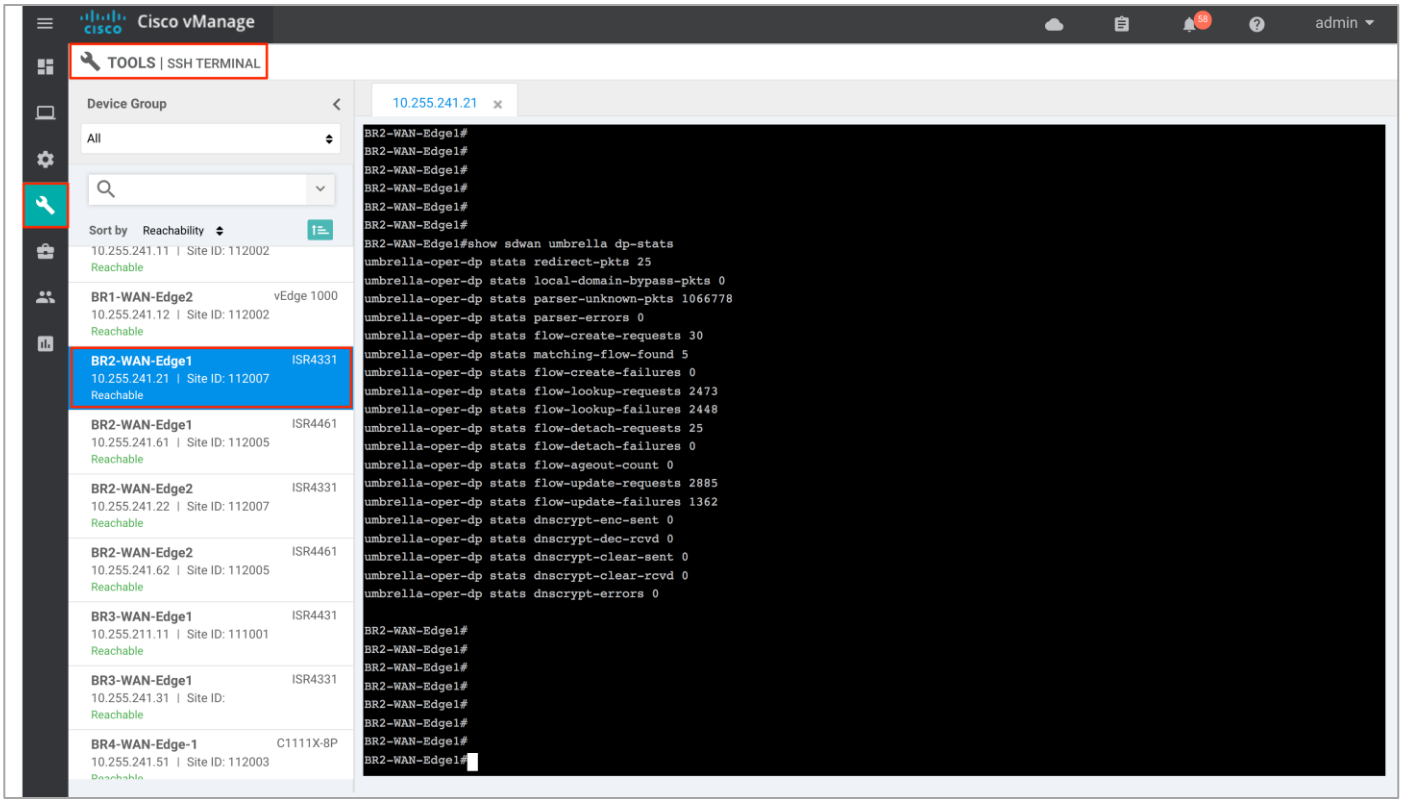
Technical Tip
Note, communication for device registration to the Cisco Umbrella server is via HTTPS. This requires a DigiCert root certificate which is auto installed on the router by default.

Output of show sdwan umbrella overview/ show sdwan umbrella device-registration:



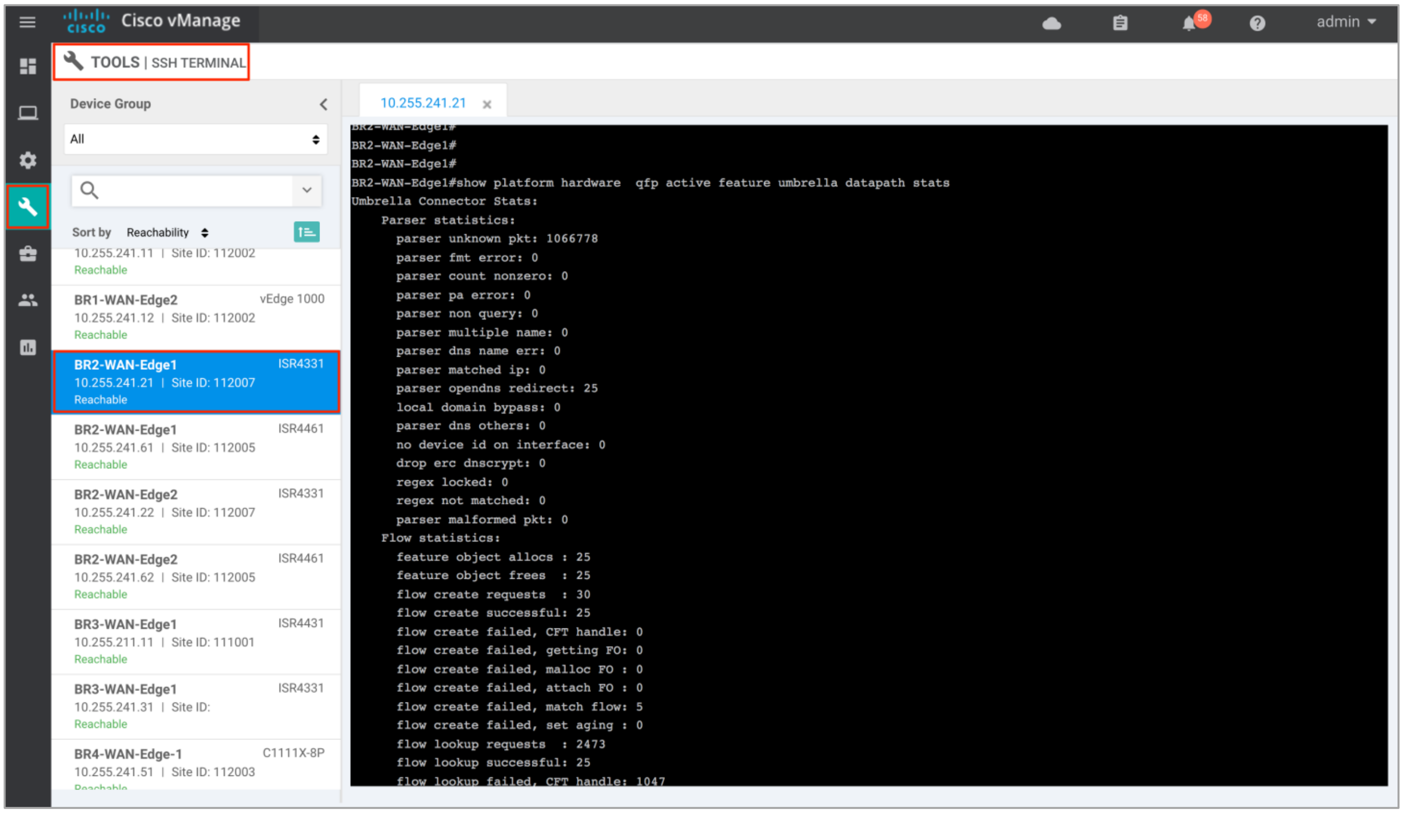
```
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show sdwan umbrella overview
umbrella-ios-oper-data umbrella-overview registrations-completed 1
umbrella-ios-oper-data umbrella-overview registrations-requested 1
umbrella-ios-oper-data umbrella-overview dnscrypt false
umbrella-ios-oper-data umbrella-overview last-success-attempt 1970-01-01T00:00:00+00:00

BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show sdwan umbrella device-registration
NAME  STATUS       TAG   DEVICE ID         DESCRIPTION
----------------------------------------------------------------------------
1     200 SUCCESS  vpn1  010a2087da31312b  Device Id recieved successfully


BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
```

Output of show sdwan umbrella dp-stats:



```
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show sdwan umbrella dp-stats
umbrella-oper-dp stats redirect-pkts 25
umbrella-oper-dp stats local-domain-bypass-pkts 0
umbrella-oper-dp stats parser-unknown-pkts 1066778
umbrella-oper-dp stats parser-errors 0
umbrella-oper-dp stats flow-create-requests 30
umbrella-oper-dp stats matching-flow-found 5
umbrella-oper-dp stats flow-create-failures 0
umbrella-oper-dp stats flow-lookup-requests 2473
umbrella-oper-dp stats flow-lookup-failures 2448
umbrella-oper-dp stats flow-detach-requests 25
umbrella-oper-dp stats flow-detach-failures 0
umbrella-oper-dp stats flow-ageout-count 0
umbrella-oper-dp stats flow-update-requests 2885
umbrella-oper-dp stats flow-update-failures 1362
umbrella-oper-dp stats dnscrypt-enc-sent 0
umbrella-oper-dp stats dnscrypt-dec-rcvd 0
umbrella-oper-dp stats dnscrypt-clear-sent 0
umbrella-oper-dp stats dnscrypt-clear-rcvd 0
umbrella-oper-dp stats dnscrypt-errors 0

BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
```

Step 4. For Umbrella connector statistics, enter the CLI command - show platform hardware qfp active feature umbrella datapath stats.



10.255.241.11 | Site ID: 112002
Reachable

BR1-WAN-Edge2 vEdge 1000
10.255.241.12 | Site ID: 112002
Reachable

BR2-WAN-Edge1 ISR4331
10.255.241.21 | Site ID: 112007
Reachable

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

```
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#
BR2-WAN-Edge1#show platform hardware  qfp active feature umbrella datapath stats
Umbrella Connector Stats:
    Parser statistics:
      parser unknown pkt: 1066778
      parser fmt error: 0
      parser count nonzero: 0
      parser pa error: 0
      parser non query: 0
      parser multiple name: 0
      parser dns name err: 0
      parser matched ip: 0
      parser opendns redirect: 25
      local domain bypass: 0
      parser dns others: 0
      no device id on interface: 0
      drop erc dnscrypt: 0
      regex locked: 0
      regex not matched: 0
      parser malformed pkt: 0
    Flow statistics:
      feature object allocs : 25
      feature object frees  : 25
      flow create requests  : 30
      flow create successful: 25
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 5
      flow create failed, set aging : 0
      flow lookup requests  : 2473
      flow lookup successful: 25
      flow lookup failed, CFT handle: 1047
```

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 4. 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: 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 End-to-End Deployment Guide.

Feature Template

Within this section, the configured lists, the main security policy template and its container template is listed.

Security Policy feature template

Devices: All devices except vManage and vSmart

Template: Basic Information/Security

Template Name: DCA_Security_Policy

Description: Security Policy Template

The following lists are configured for the security policy,

Table 5. Zone Settings

Section	List Type	Value

List	Zones	INSIDE = VPN 1
		OUTSIDE = VPN 0

	Data Prefix	Client_Network = 10.10.0.0/16

The configured lists are used in the security policy,

Table 6. Security Policy Template Settings

Policy sub-section	Section	Condition/Parameter	Type	Value
Enterprise Firewall with Application Awareness	Target Zone-Pair	Source Zone	Drop-down	INSIDE
		Destination Zone	Drop-down	OUTSIDE
	Name		Entry tab	DCA_Firewall_Policy
	Description		Entry tab	Enterprise Firewall with App Aware for DCA Use Case
	Match (Rule 1)	Source Data Prefix List	Variable	Client_Network
		Application/ Application - Family	Variable	SAAS_Application

Policy sub-section	Section	Condition/Parameter	Type	Value
		Protocol	Drop-down	TCP
	Actions (Rule 1)	Inspect	Radio Button	Enable
	Match (Rule 2)	Protocol	Drop-down	UDP
	Actions (Rule 2)	Inspect	Radio Button	Enabled
Intrusion Prevention System	Target	VPNs	Entry tab	1
	Policy Name		Entry tab	DCA_IPS_Policy
	Policy Description		Entry tab	IPS policy to protect the network from malware.
	Signature Set		Drop down	Balanced
	Inspection Mode		Drop down	Protection
	Advanced	Alerts Log Level	Drop down	Error
AMP	Policy Name		Entry tab	DCA_AMP_Policy
	Custom VPN Configuration	Target VPN	Entry tab	1
	File Reputation	AMP Cloud Region	Drop-down	NAM
		Alert Log Level	Drop-down	Warning
	File Analysis	TG Cloud Region	Drop down	NAM
	Security Policy Name	Threat Grid API Key (NAM)	Entry tab	xxxxxxxxxxxxxxxx
	Security Policy Description	File Types List	Drop-down	All
DNS/ Web-layer Security	Policy Name		Entry tab	DCA_DNS_Policy
	Umbrella Registration Status	Configured	Entry tab	Registration Token
	Custom VPN Configuration			
		VPNs	Entry tab	1
	File Analysis	DNs Server IP	Radio Button	Umbrella Default
	Security Policy Name	Local Domain Bypass	Slide	disabled
Policy Summary	Security Policy Name		Entry tab	DCA_Security_Policy
	Security Policy Description		Entry tab	Security Policy Specific to DCA Use Case
	Additional Policy Settings (Firewall)	High Speed Logging – VPN	Entry tab	0

Policy sub-section	Section	Condition/Parameter	Type	Value
		High Speed Logging – Server IP	Entry tab	10.2.2.2
		High Speed Logging – Port	Default	2055
	Additional Policy Settings (IPS/ AMP/ URL)	Audit Trail	slide	On
		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	Value
NAT	On
Resource Profile	Default/ High

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 7. 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

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

Example Branch Configuration

The following section lists out an example branch configuration.

Security Policy for DCA

```
policy
 intrusion-prevention DCA_IPS_Policy
  security-level security
  inspection-mode protection
  logging host 10.2.2.2 vpn 0
  log-level warning
  target-vpns 1
 !
 advanced-malware-protection DCA_AMP_Policy
  file-reputation-cloud-server cloud-isr-asn.amp.cisco.com
  file-reputation-est-server cloud-isr-est.amp.cisco.com
  file-reputation-alert warning
  file-analysis-cloud-server isr.api.threatgrid.com
  file-analysis-file-types pdf ms-exe new-office rtf mdb mscab msole2 wri xlw flv swf
  file-analysis-alert warning
  logging host 10.2.2.2 vpn 0
  target-vpns 1
 !
 zone-based-policy DCA_Firewall_Policy_1
    sequence 1
     match
      protocol 17
      protocol-name udp
     !
     action inspect
     !
    !
    sequence 11
     match
      app-list SAAS_Application
      source-data-prefix-list Client_Network
      protocol 6
      protocol-name tcp
     !
     action inspect
     !
    !
  default-action drop
 !
  zone INSIDE
   vpn 1
  !
  zone OUTSIDE
   vpn 0
  !
  zone-pair ZP_INSIDE_OUTSIDE_DCA_-240664430
   source-zone INSIDE
   destination-zone OUTSIDE
   zone-policy DCA_Firewall_Policy_1
  !
  high-speed-logging
   server-ip 10.2.2.2
   port 2055
   vrf 0
  !
 lists
```

```
  data-prefix-list Client_Network
   ip-prefix 10.10.0.0/16
  !
  local-app-list SAAS_Application
   app gmail
   app dropbox
   app ms-office-365
  !
 !
 zone-to-nozone-internet deny
 failure-mode open
!
exit
!
security
 umbrella
  no dnscrypt
!
exit
!
vpn 1
 dns-redirect umbrella match-local-domain-to-bypass
```

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             10.255.241.21
   overlay-id            1
   site-id               112007
   port-offset           1
   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
  !
 !
!
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-Edge1
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 8.8.4.4 8.8.8.8
ip route 0.0.0.0 0.0.0.0 30.100.1.2 1
ip access-list extended DCA_Firewall_Policy_1-seq-11-acl_
 11 permit object-group DCA_Firewall_Policy_1-seq-11-service-og_ object-group Client_Network 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 inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/1 overload
ip nat inside source list utd-nat-acl interface GigabitEthernet0/0/1 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
ip nat route vrf 65529 0.0.0.0 0.0.0.0 global
```

```
class-map type inspect match-any DCA_Firewall_Policy_1-s1-l4-cm_
 match protocol udp
!
class-map type inspect match-any DCA_Firewall_Policy_1-s11-l4-cm_
 match protocol tcp
!
class-map type inspect match-all DCA_Firewall_Policy_1-seq-1-cm_
 match class-map DCA_Firewall_Policy_1-s1-l4-cm_
!
class-map type inspect match-all DCA_Firewall_Policy_1-seq-11-cm_
 match access-group name DCA_Firewall_Policy_1-seq-11-acl_
 match class-map DCA_Firewall_Policy_1-s11-l4-cm_
!
class-map match-any SAAS_Application-cm0_
 match protocol dropbox
 match protocol gmail
 match protocol ms-office-365
!
policy-map type inspect DCA_Firewall_Policy_1
 class DCA_Firewall_Policy_1-seq-1-cm_
   inspect
 !
 class DCA_Firewall_Policy_1-seq-11-cm_
   inspect
  service-policy avc SAAS_Application-pm_
 !
 class class-default
   drop
 !
!
policy-map type inspect avc SAAS_Application-pm_
 class SAAS_Application-cm0_
  deny
 !
!
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 100.119.118.8 255.255.255.0
 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 10.20.16.2 255.255.255.0
 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 INET Interface
 no shutdown
 arp timeout 1200
 ip address 30.100.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1496
 ip nat outside
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/2
 description MPLS Interface
 no shutdown
 arp timeout 1200
 ip address 20.20.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 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
 10.10.0.0 255.255.0.0
!
object-group service DCA_Firewall_Policy_1-seq-11-service-og_
 ip
!
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
aaa session-id common
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
!
parameter-map type umbrella global
 token    9CF0368AC498522C2EEF7F085CDBE3B400272B18
 no dnscrypt
 vrf 1
  dns-resolver                 umbrella
  match-local-domain-to-bypass
 !
!
zone security INSIDE
 vpn 1
!
zone security OUTSIDE
 vpn 0
!
zone-pair security ZP_INSIDE_OUTSIDE_DCA_-240664430 source INSIDE destination OUTSIDE
 service-policy type inspect DCA_Firewall_Policy_1
!
no crypto ikev2 diagnose error
no crypto isakmp diagnose error
router bgp 65201
 bgp log-neighbor-changes
 distance bgp 20 200 20
 maximum-paths eibgp 2
 neighbor 20.20.1.2 remote-as 70
 neighbor 20.20.1.2 description MPLS Service Provider
 neighbor 20.20.1.2 ebgp-multihop 1
 neighbor 20.20.1.2 maximum-prefix 2147483647 100
 neighbor 20.20.1.2 password 0 c1sco123
 neighbor 20.20.1.2 send-community both
 neighbor 20.20.1.2 timers 3 9
 address-family ipv4 unicast
  network 20.20.1.0 mask 255.255.255.252
  exit-address-family
 !
 timers bgp 60 180
!
router ospf 1 vrf 1
 area 0 range 10.20.16.0 255.255.255.0 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.20.16.16
 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 DCA_IPS_Policy
  threat protection
  policy security
  logging level warning
 !
 utd global
  logging host 10.2.2.2
  file-reputation
   cloud-server cloud-isr-asn.amp.cisco.com
   est-server   cloud-isr-est.amp.cisco.com
  !
  file-analysis
   cloud-server isr.api.threatgrid.com
   apikey 0 rhl68q1udvb5mamp3dhde3tlov
  !
 !
 file-analysis profile DCA_AMP_Policy-fa-profile
  file-types
   pdf
   ms-exe
   new-office
   rtf
   mdb
   mscab
   msole2
   wri
   xlw
   flv
   swf
  !
  alert level warning
 !
 file-reputation profile DCA_AMP_Policy-fr-profile
  alert level warning
 !
 file-inspection profile DCA_AMP_Policy-fi-profile
  analysis profile DCA_AMP_Policy-fa-profile
  reputation profile DCA_AMP_Policy-fr-profile
 !
 policy utd-policy-vrf-1
  all-interfaces
  file-inspection profile DCA_AMP_Policy-fi-profile
```

```
  vrf 1
  threat-inspection profile DCA_IPS_Policy
 exit
!
sdwan
 interface GigabitEthernet0/0/1
  tunnel-interface
   encapsulation ipsec preference 100 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 GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec preference 0 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 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 10.10.0.0/16
    !
   !
   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 D: Glossary

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

AMP	Advanced Malware Protection
DNS	Domain Name Server

Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community at https://cs.co/en-cvds.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.