Secure Guest Access for Cisco IOS-XE SD-WAN Devices

Prescriptive Deployment Guide

May, 2020

Contents

Introduction

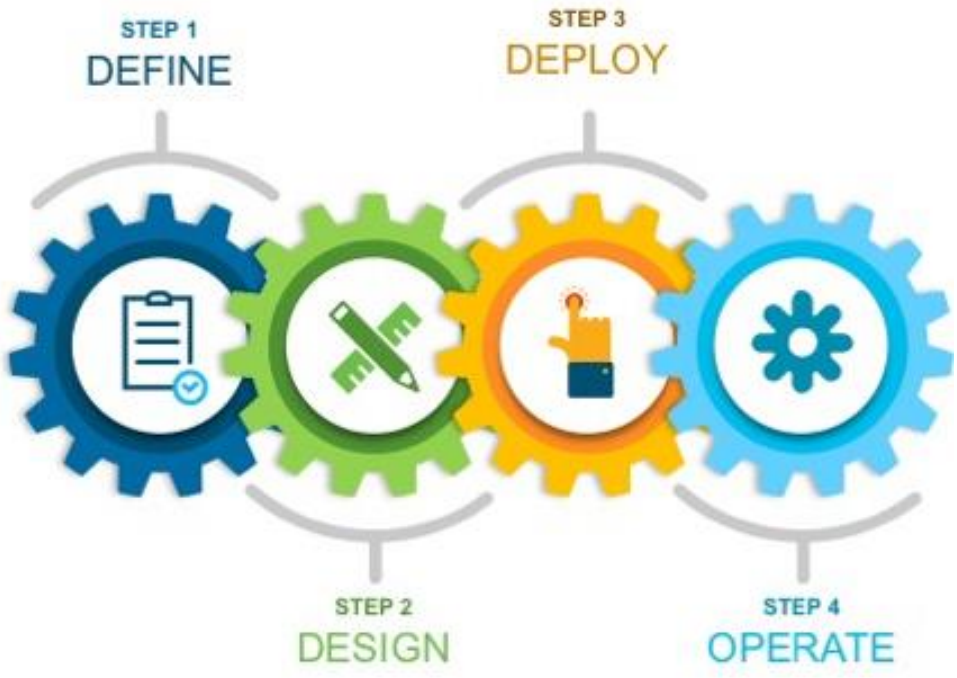
About the Guide

This document provides the design and deployment of the Cisco SD-WAN security policy specific to secure guest access within remote sites running IOS-XE SD-WAN WAN Edge platforms. The security features leveraged within this guide include Enterprise Firewall with Application Awareness and URL Filtering (URLF).

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 guest access use case using the vManage security policy dashboard. The section also includes the prerequisites to deploy this security solution.
- The Operate section explains some of the monitoring and troubleshooting methods used when Cisco SD-WAN security features, Enterprise Firewall with Application Awareness and URL Filtering (URLF), 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 guest access 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, routing guest user traffic from remote site to data center poses extreme security risk for the entire organization. The solution is to enable local Internet exit for guest 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.
- 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 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.

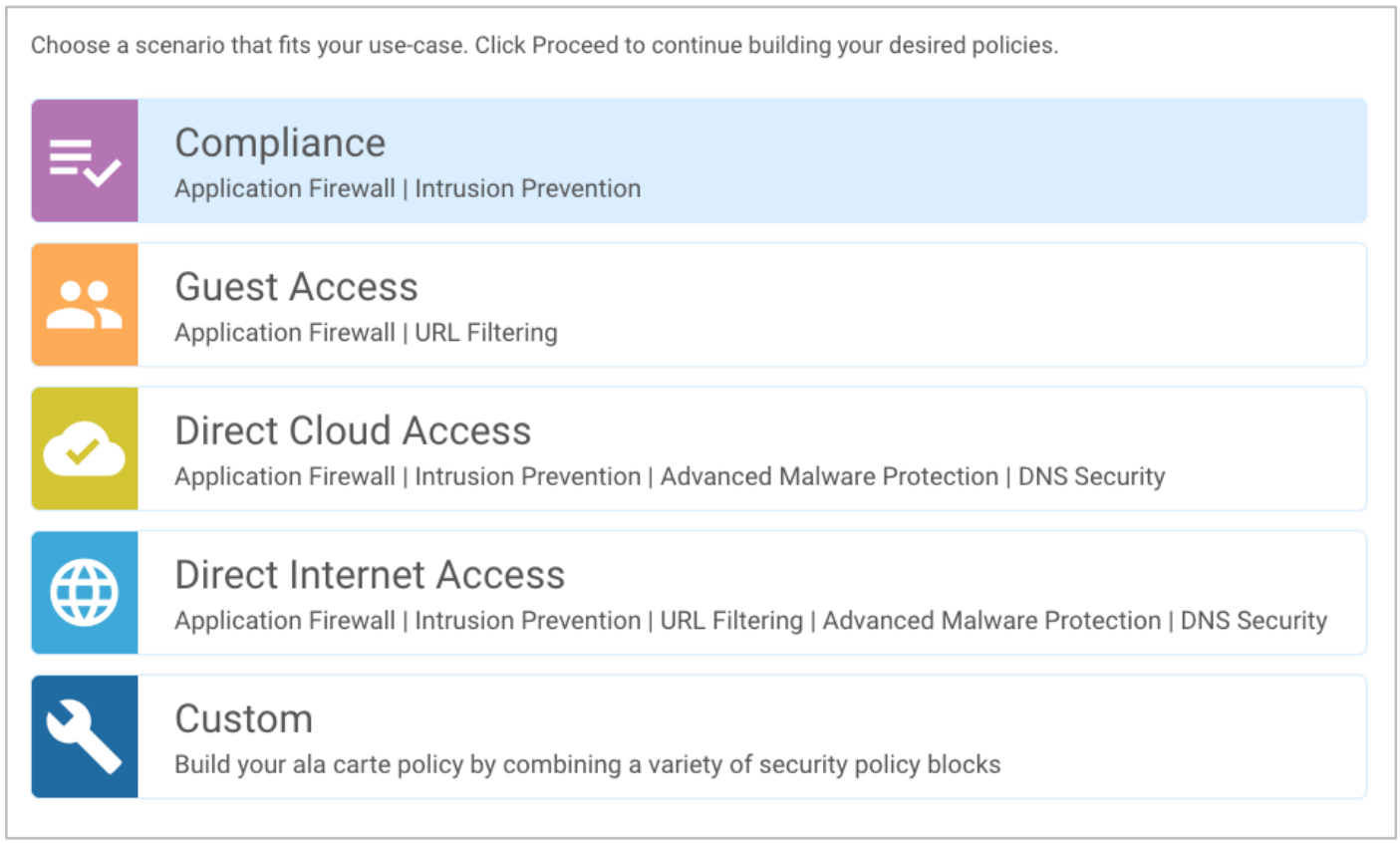
Security features leveraged in this use case include Enterprise Firewall with Application Awareness, Intrusion Prevention System (IPS), Advanced Malware Protection (AMP) and DNS/Web-layer Security.

- 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



Within this solution, the security features available within the guest access use cases 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.
- Incur no additional cost, as deploying the Cisco SD-WAN security solution eliminates the need to deploy any addition equipment within your SD-WAN network to enable security features.

- Centralized management: Deploy, troubleshoot and monitor the SD-WAN overlay solution with security capabilities across 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.
  - URL Filtering (URLF) enforces acceptable user control to block or allow web traffic based on 82+ different categories and web reputation scores, with the added option to blacklist/whitelist web traffic.

Design – Cisco SD-WAN Secure Guest Access

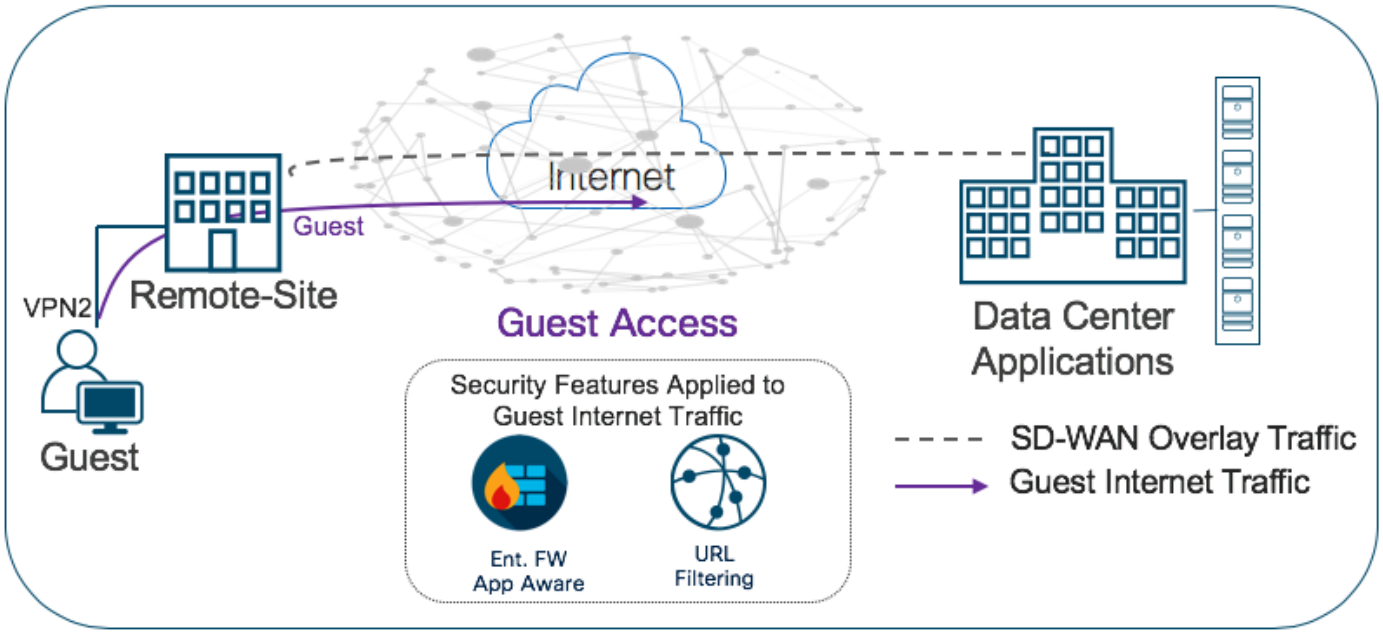
Out of the four intent-based use cases available within the vManage security policy, the use case discussed in this guide is secure guest access

Use Case - Secure Guest Access

Within the guest access use case, the primary requirement is to allow guest users to access Internet directly from the remote site, to offload Internet traffic from premium WAN connections and to improve application experience.

The second requirement is to secure the guest Internet traffic and branch network, by enabling advanced security features such as Enterprise Firewall with Application Awareness to inspect and limit traffic, and URL Filtering (URLF) for content filtering either directly on the WAN Edge router, or by routing Internet traffic through a cloud security provider.

Figure 3. Traffic Flow - Secure Guest Access Use Case



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

- Secure Segmentation via VPN/Zone to segment guest traffic into zones and VPN/ VRF.
- NAT DIA route for local Internet exit of segmented guest Internet traffic. Optionally, you can also use centralized data policy to redirect some or all guest Internet traffic.
- Enterprise Firewall with Application Awareness and URL Filtering to maintain a secure guest access network.

Table 1. Cisco SD-WAN Features to Enable Secure Guest Access

Security Pillar	SD-WAN Security Feature
Segmentation	VPN and Zone

Security Pillar	SD-WAN Security Feature
Local Internet Exit	Centralized Data Policy/ NAT DIA Route
Perimeter Control	Enterprise Firewall with Application Awareness
Liability Protection	URL Filtering

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.

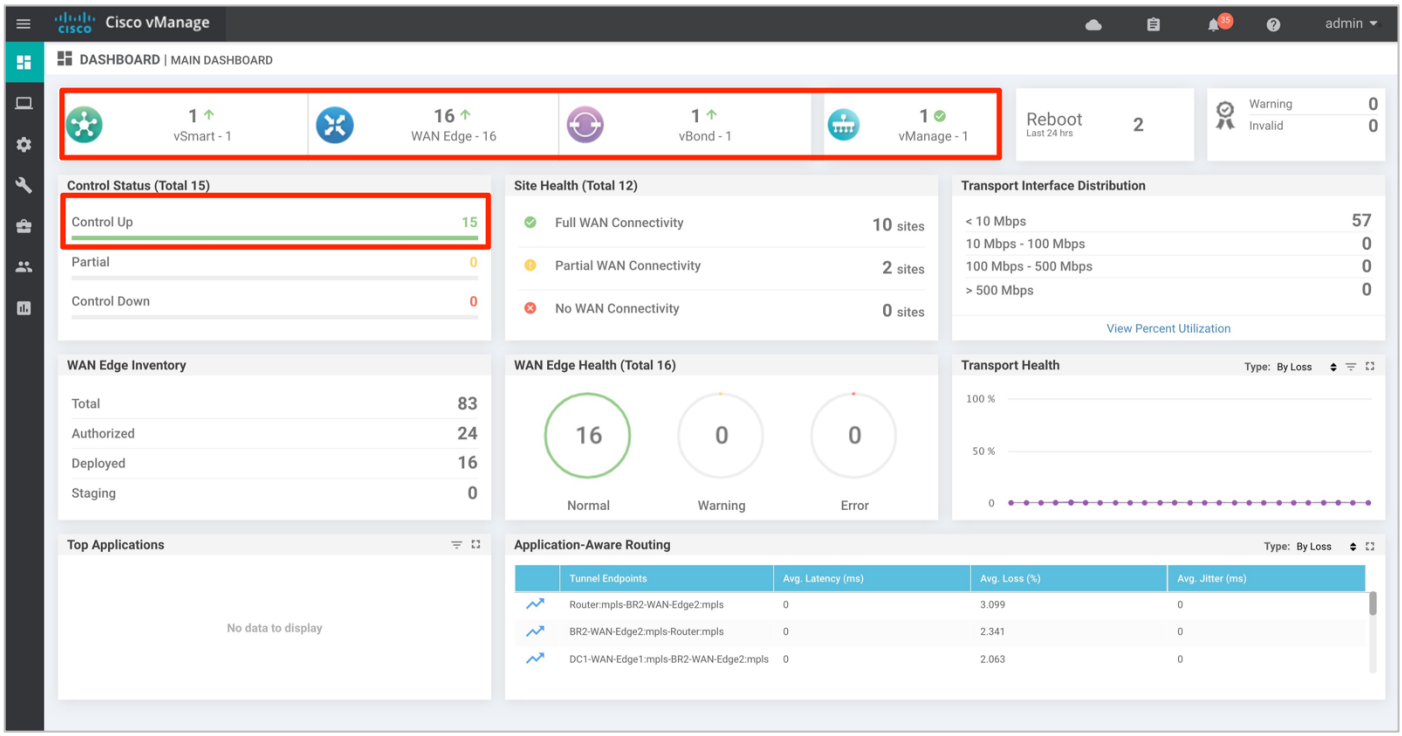
Security Policy Design: For the design components, workings and considerations of Cisco SD-WAN security features such as, Enterprise Firewall with Application Awareness (Application Firewall) and URL-Filtering, refer to the Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices.

Prerequisites - Cisco SD-WAN Secure Guest Access

This section covers the prerequisites specific to secure guest access.

Process 1: Successful Deployment of Controllers and WAN Edge Devices

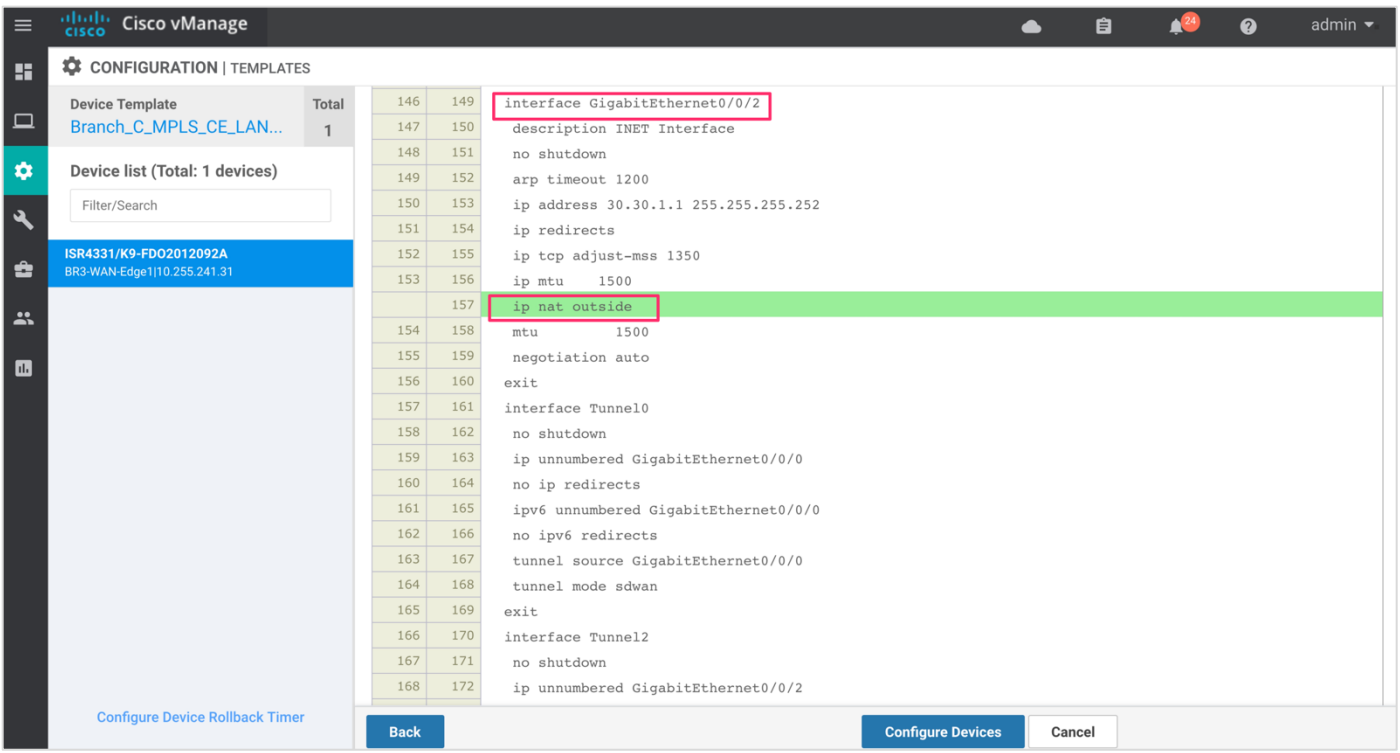
Step 1. Make sure the controllers and WAN Edge devices are successfully deployed and operational.



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 Guest Traffic using NAT DIA Route

Step 1. Make sure to the enable 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.



Step 2. Next, configure NAT VPN route. Following is the VPN feature template to redirect guest access traffic from service VPN 2 to transport VPN 0.

Section	Parameter	Type	Variable/Value
Basic Configuration	VPN	Global	2
	Name	Global	Service Guest VPN
IPv4 Route	Prefix	Device Specific	vpn1_br_static_nat_route_prefix|maskbits**
	Gateway	Radio Button	VPN
	Enable VPN	Global	On

**vpn1_br_static_nat_route_prefix|maskbits = 0.0.0.0/0

Based on this configuration, when a packet hits an interface within Service VPN, VPN 2 (Guest VPN/VRF), it will be forwarded to the NAT enabled interface in transport VPN 0.

Technical Tip
If you have a routing protocol configured between the service side NAT and the LAN (core/distribution) device, redistribute the NAT DIA route into the routing protocol. For instance, if you have configured OSPF configured, make sure to redistribute NAT route within the OSPF feature template.

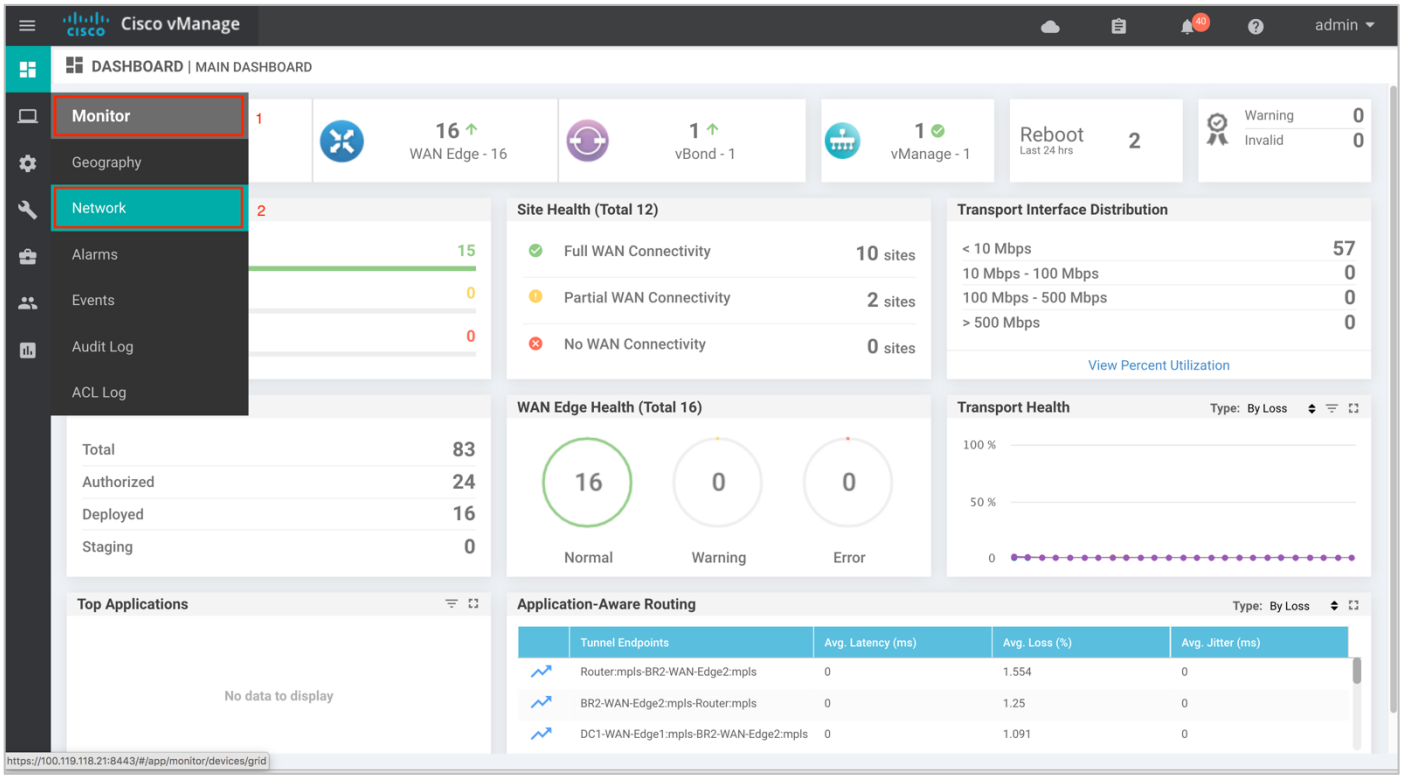
Note, you can also configure local Internet breakout using centralized data policy. For detailed step-by-step configuration of NAT DIA route or centralized data policy, refer to Cisco SD-WAN: Enabling Direct Internet Access.

Process 3: Upload Software Virtual Image to Enable Snort

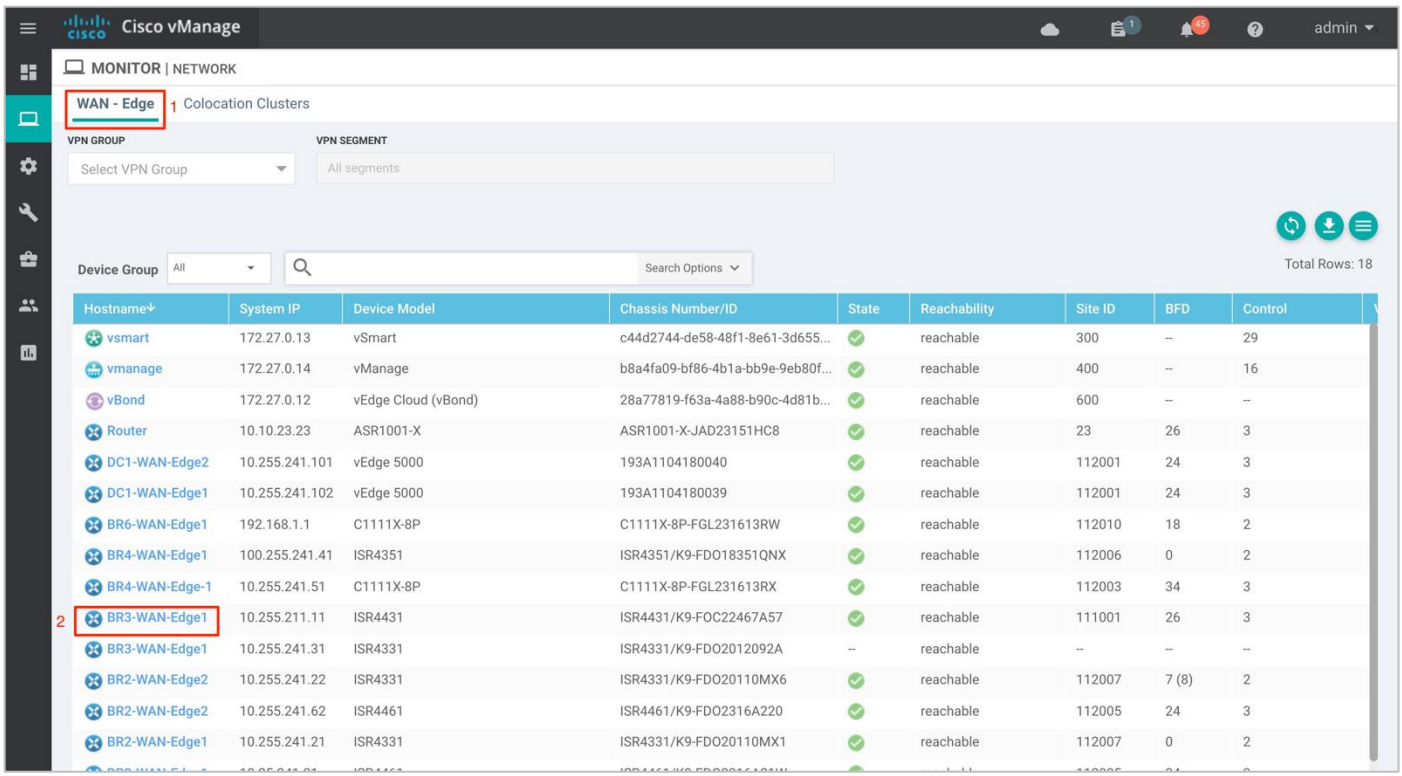
If you plan to deploy security features such as Intrusion Prevention/ Detection System (IPS/IDS), Advanced Malware Protection (AMP) or URL Filtering within the remote-site WAN Edge device, then begin by downloading the UTD Engine TAR file from the Cisco website to enable these features. Make sure to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

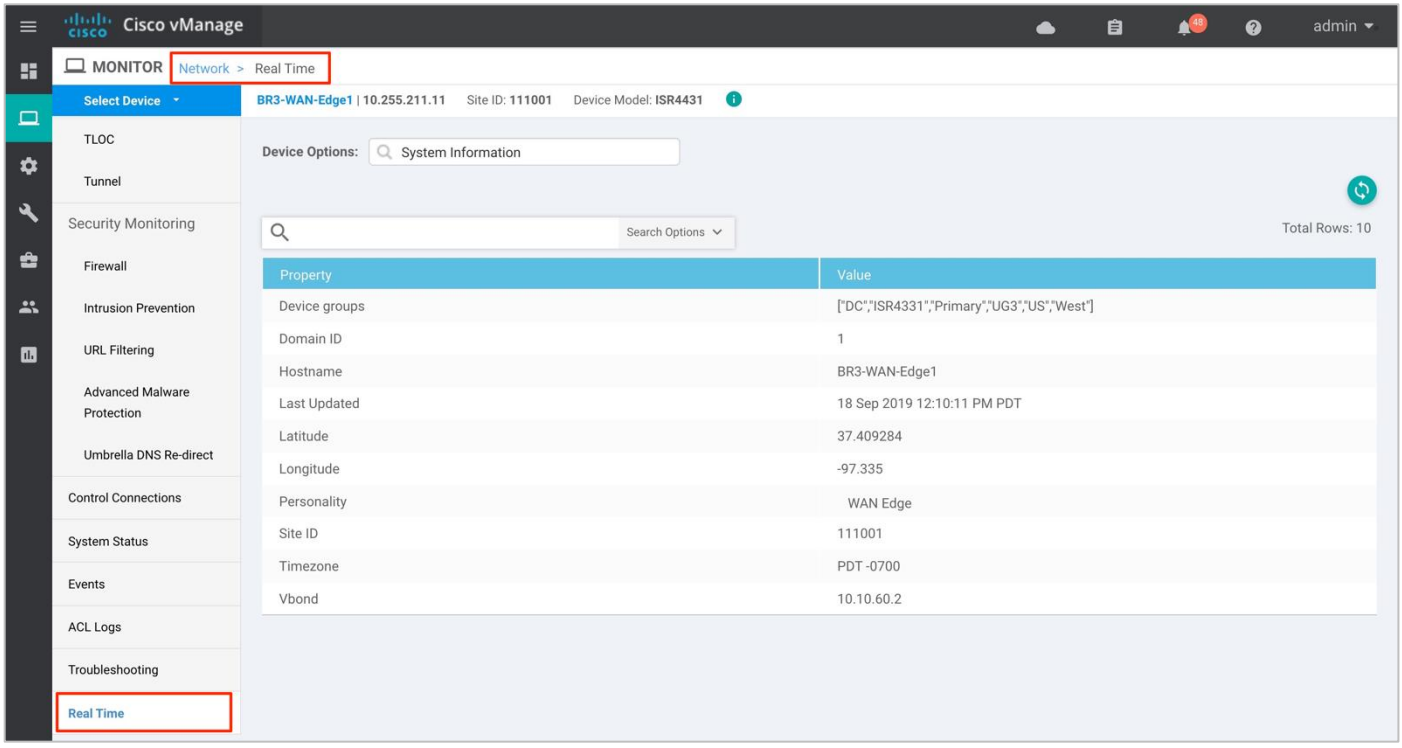
Step 1. Upload the correct Cisco security virtual image (UTD Engine TAR File) to vManage. To make sure a compatible image is downloaded from the Cisco website, login to vManage GUI and navigate to **Monitor** > **Network**.



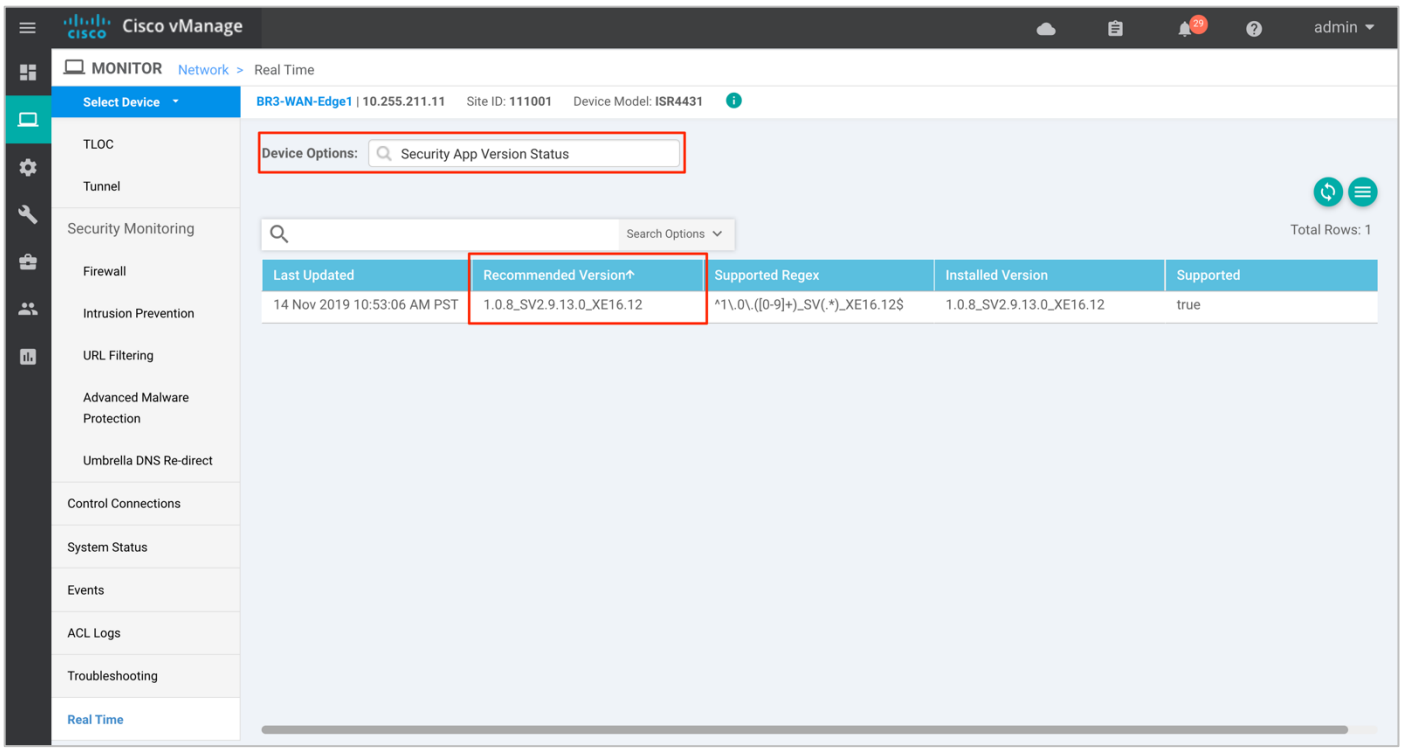
Step 2. Each router image supports a specific range of versions for a hosted application. You can find the range of supported versions (and the recommended version) for a device within its **Device Options** page. Click on the specific **WAN Edge** device to which the virtual image will be added.



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

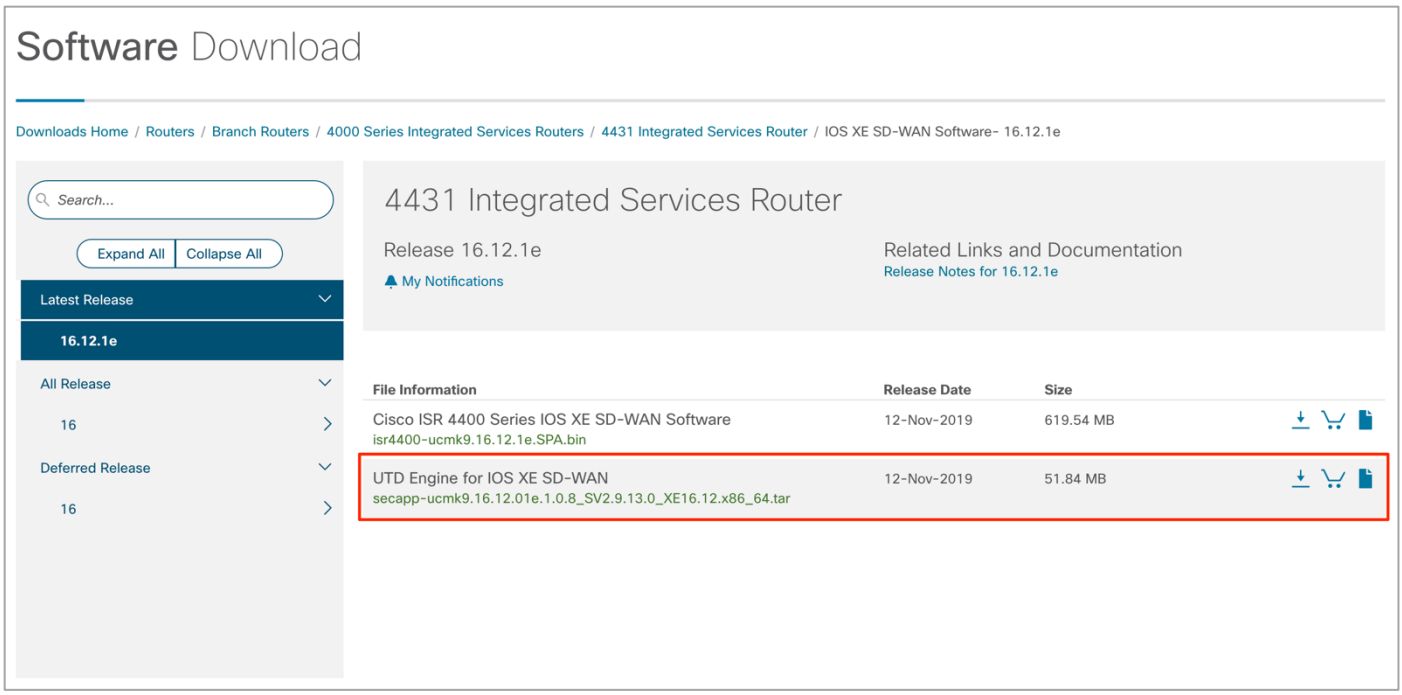


Step 4. Within the **Device Options**, enter **Security App Version Status**. Within the **Recommended Version**, you will find the recommended UTD Image that must be downloaded for that specific device.

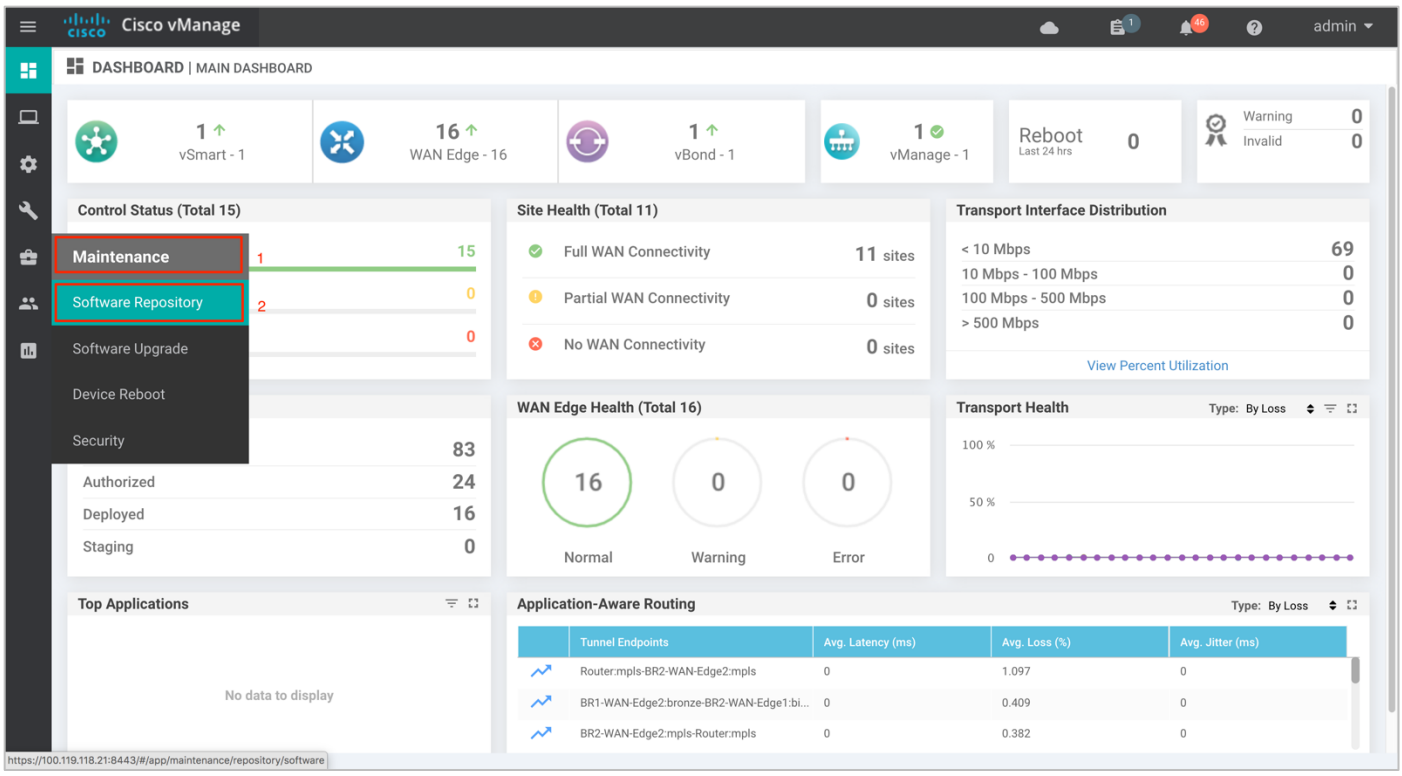


Note: The third column displays the **Supported Regex** pattern. The supported regex is the range of compatible virtual image versions for the router image.

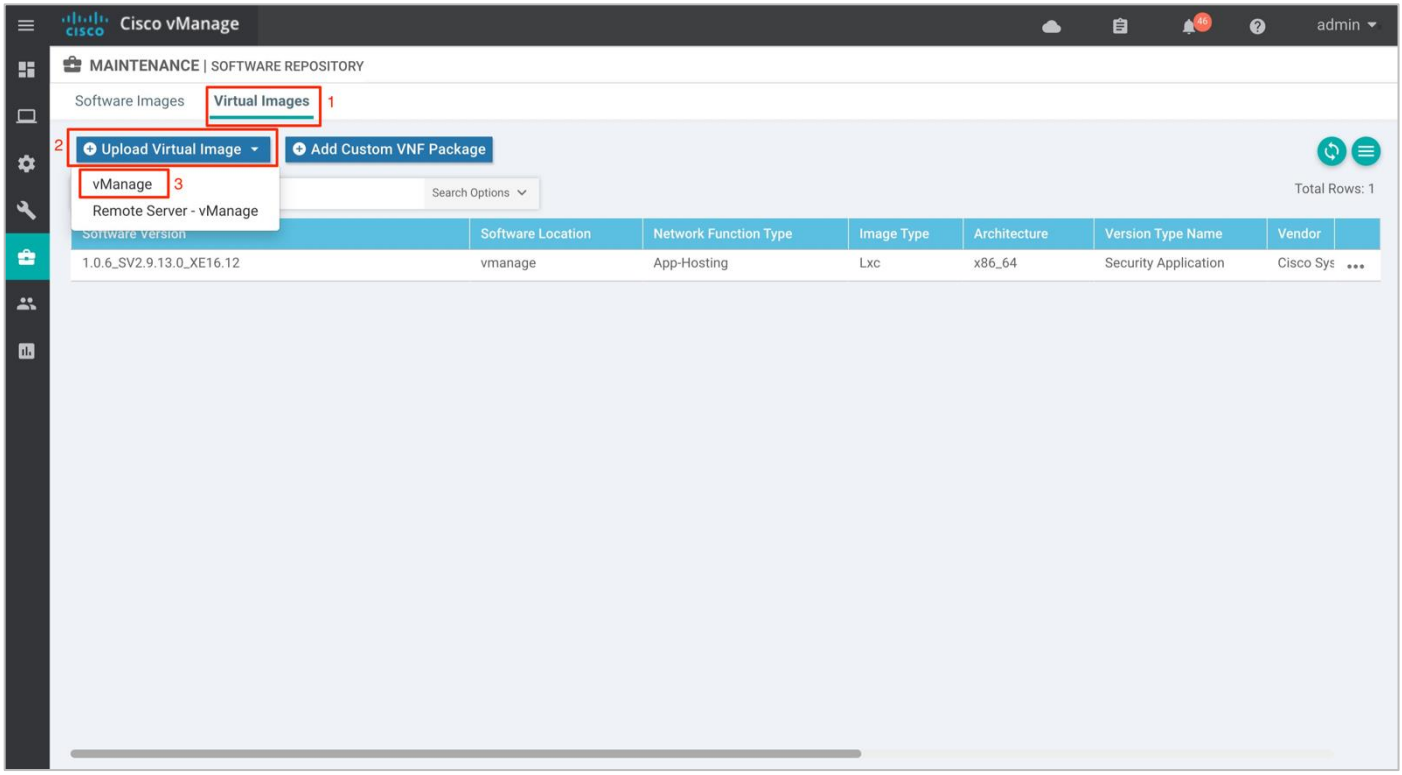
Step 5. From the Software Download page, locate the image **"UTD Engine for IOS XE SD-WAN"**. Click the download icon on the right-hand side of the window to download the UTD image file.



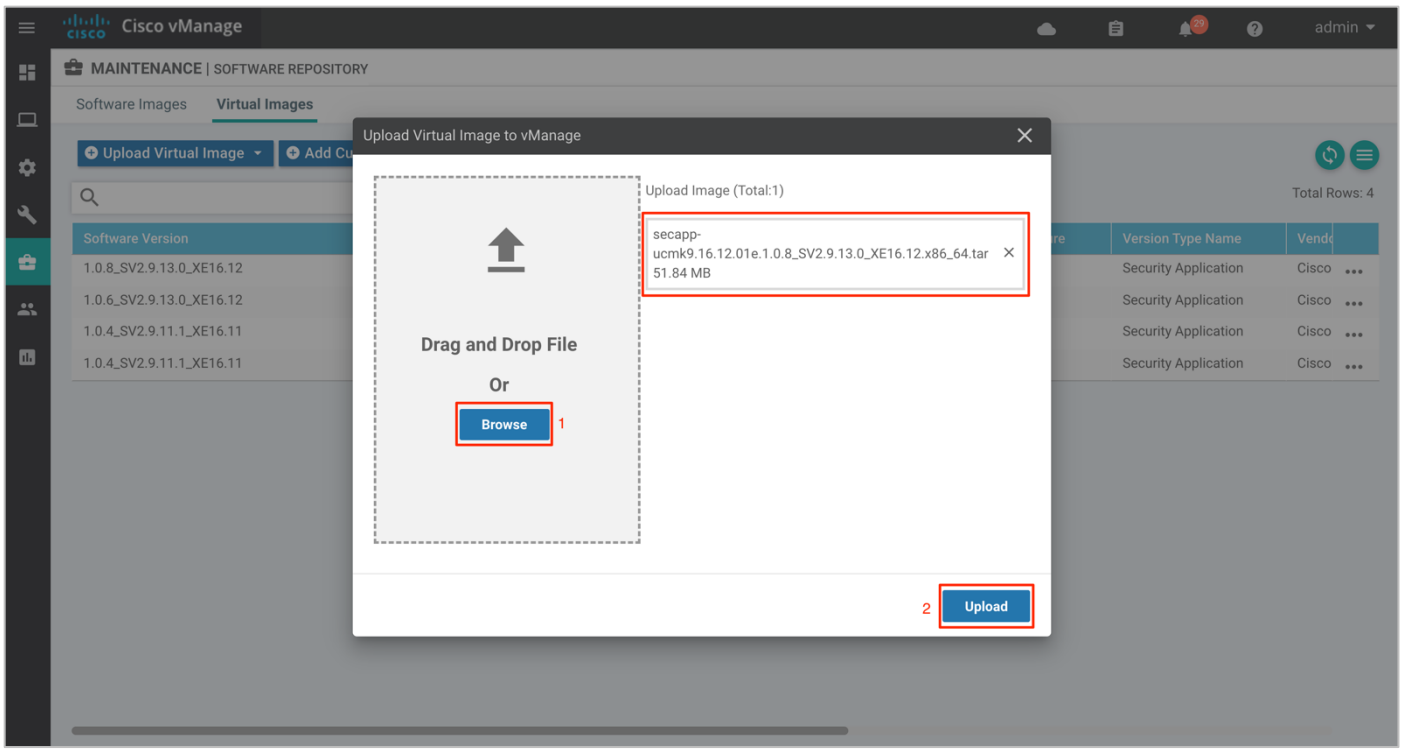
Step 6. Within the vManage dashboard, select **Maintenance** > **Software Repository**.



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



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.



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 URL Filtering 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 (URL Filtering) and allocate resources for the virtual services.

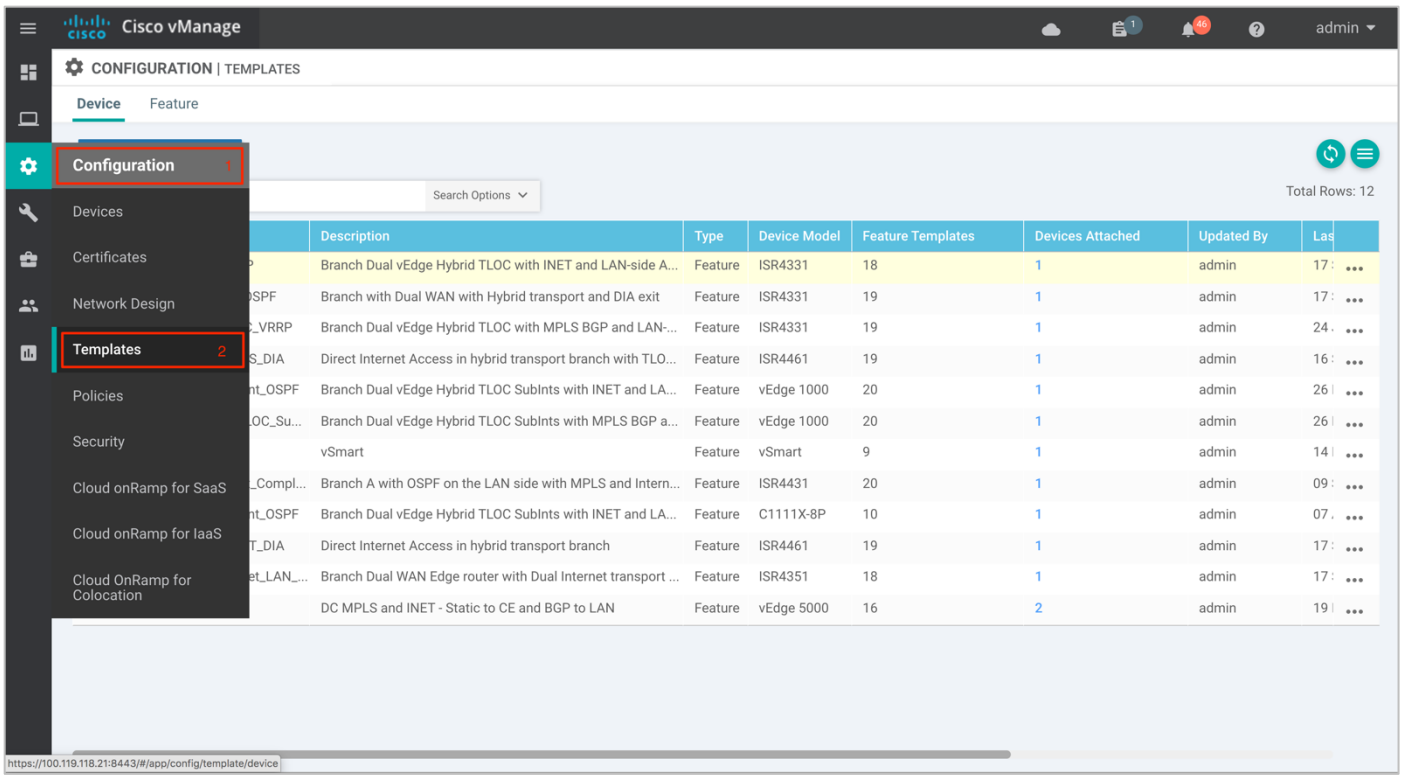
The container profile template contains:

- **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.

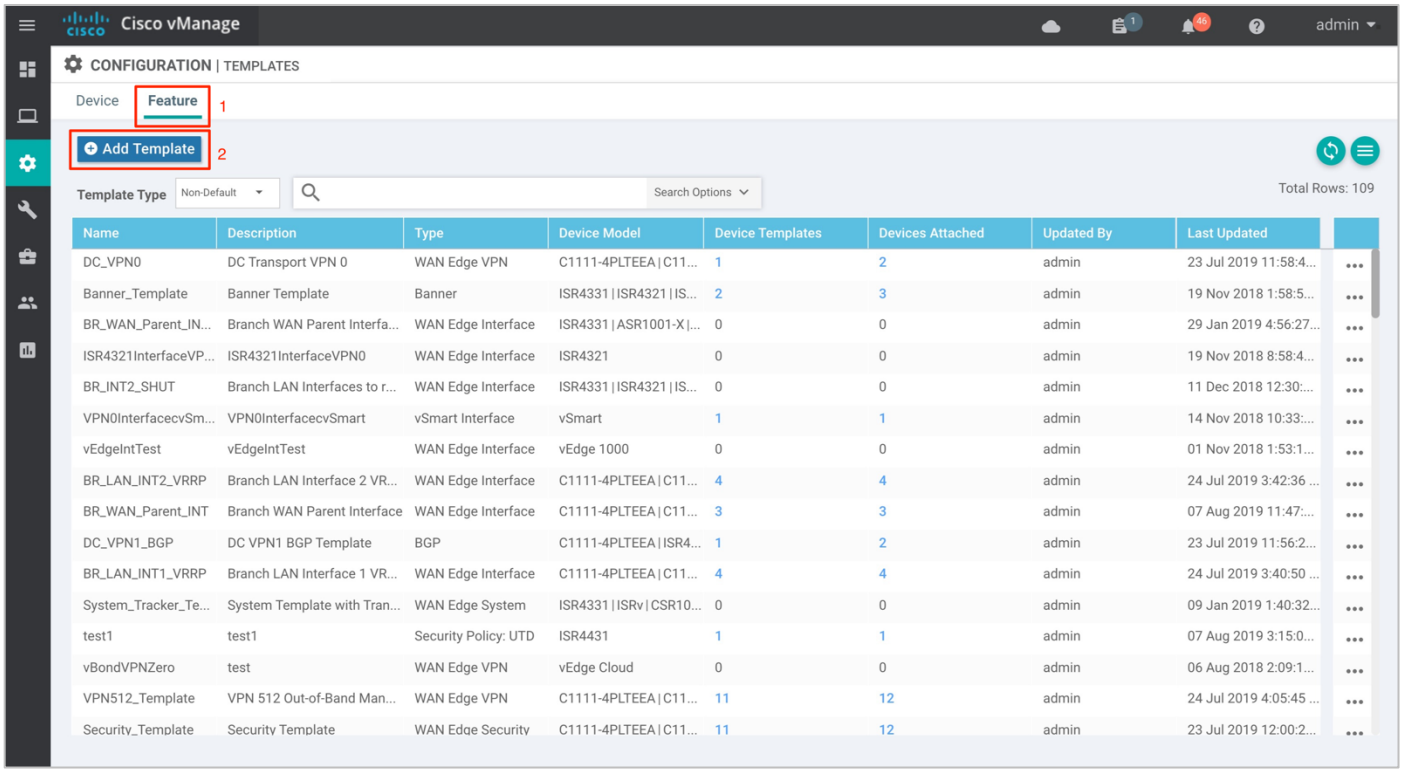
Note: If you do not wish to alter the values, skip building the template and use the default Security App Hosting Profile template wherein NAT is by default turned **ON** and the Resource Profile is set to **Default**.

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

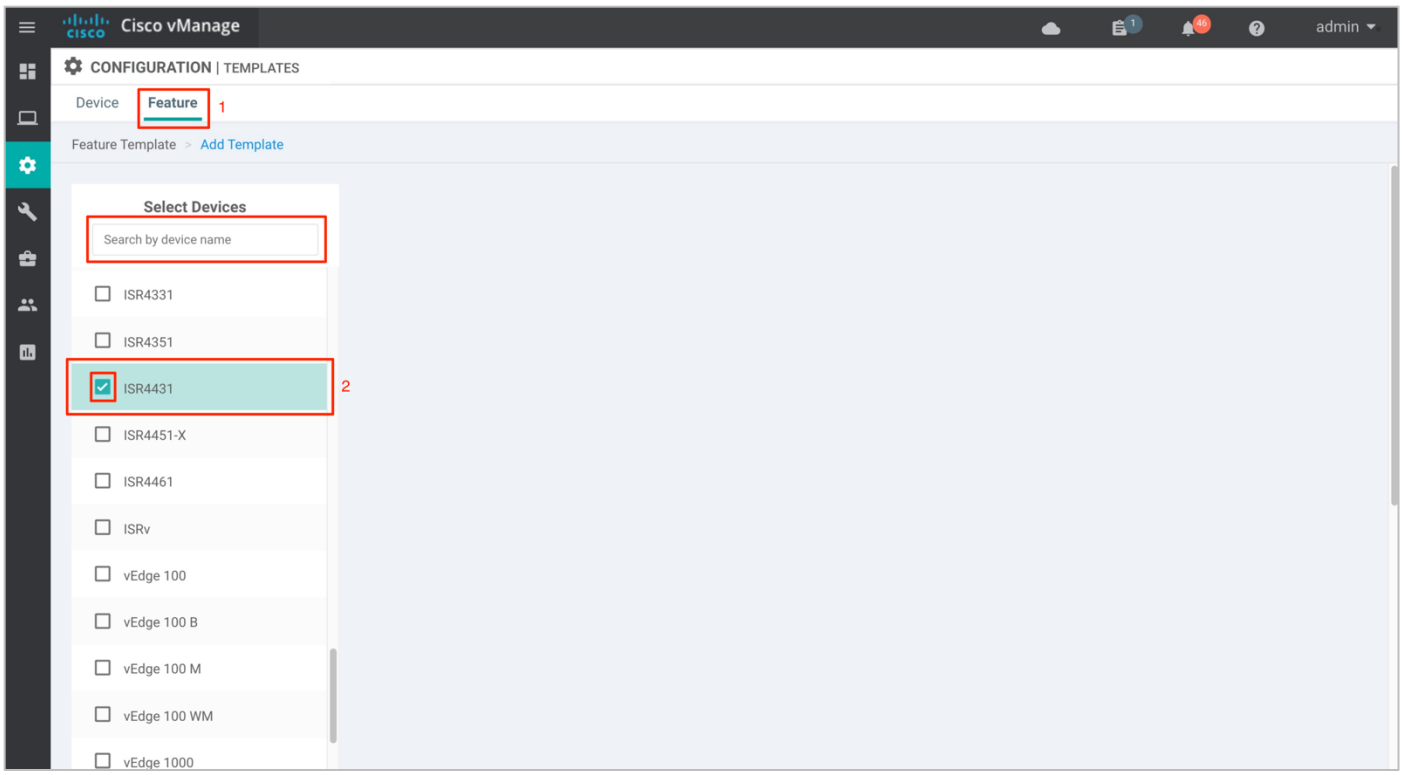
Step 1. Navigate to **Configuration** > **Templates**.



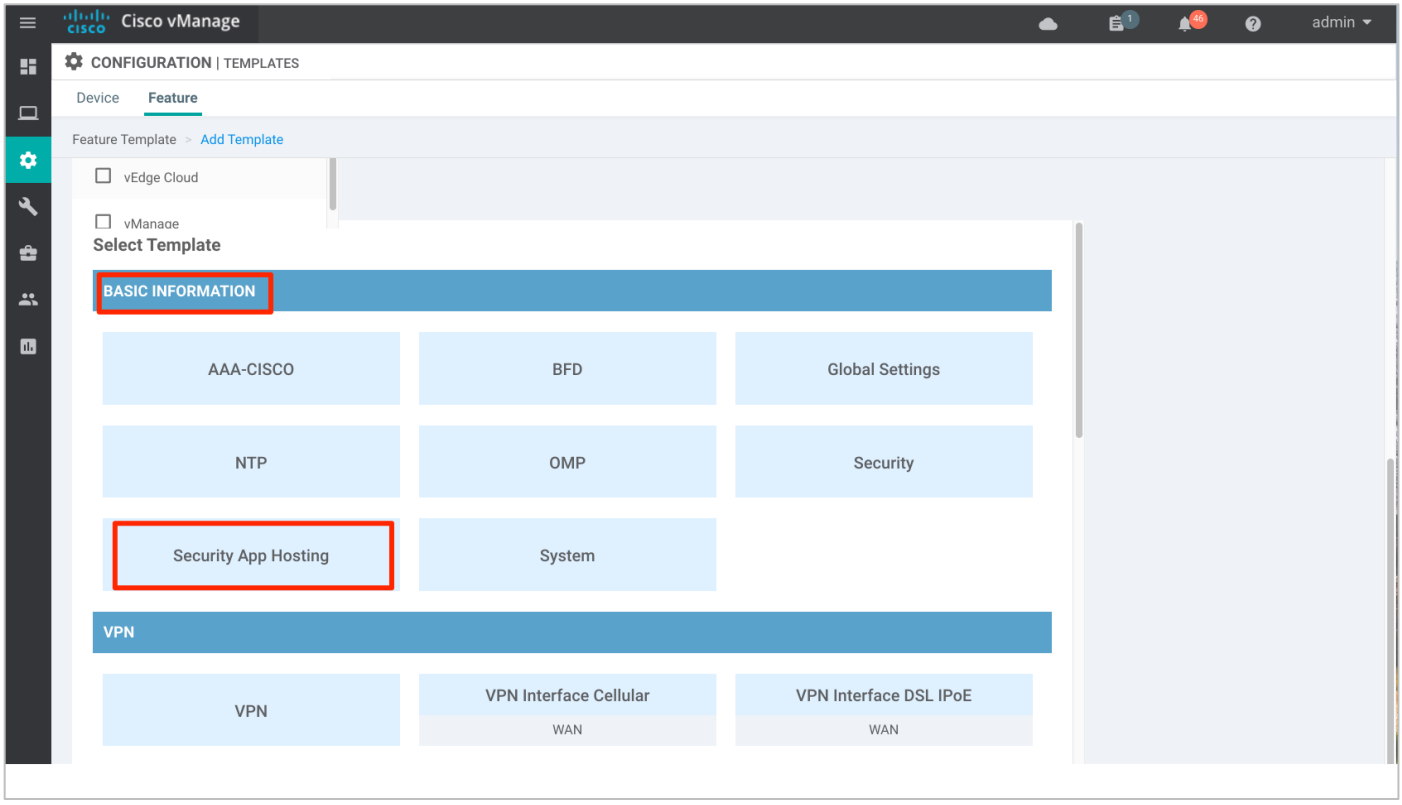
Step 2. Select **Feature** and click on Add **Template** to create a new feature template.



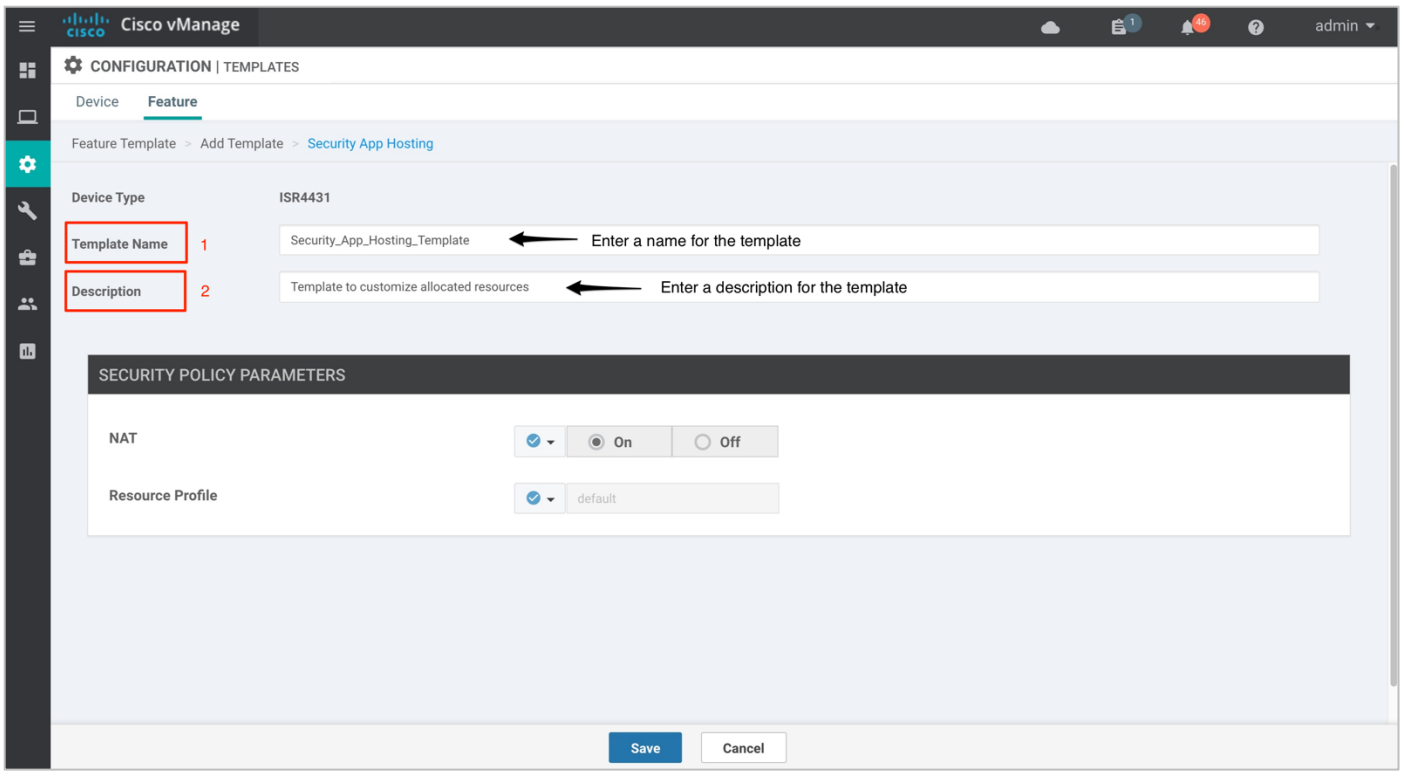
Step 3. Within **Feature Template**, select a device(s) or enter the device in the search bar.



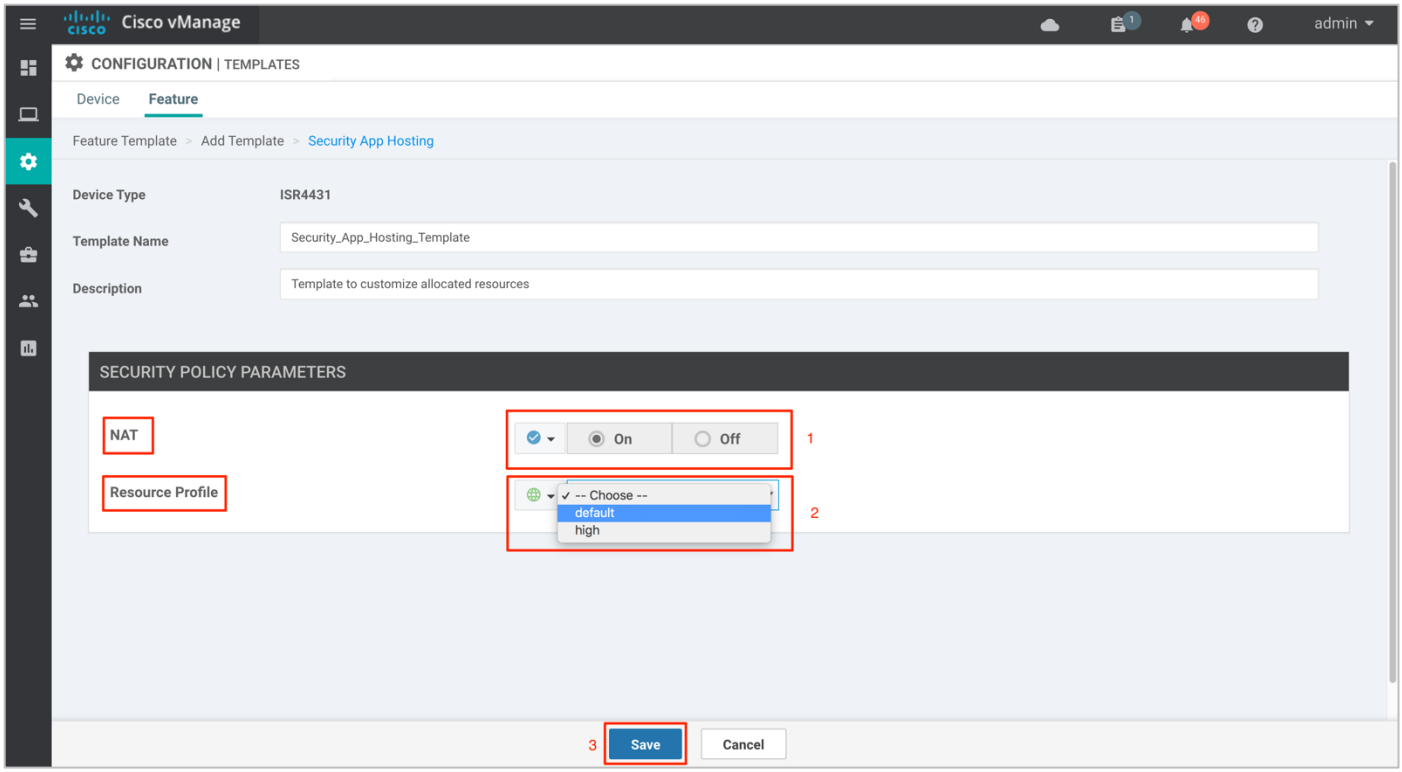
Step 4. Next, select **Security App Hosting** to create the template.



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



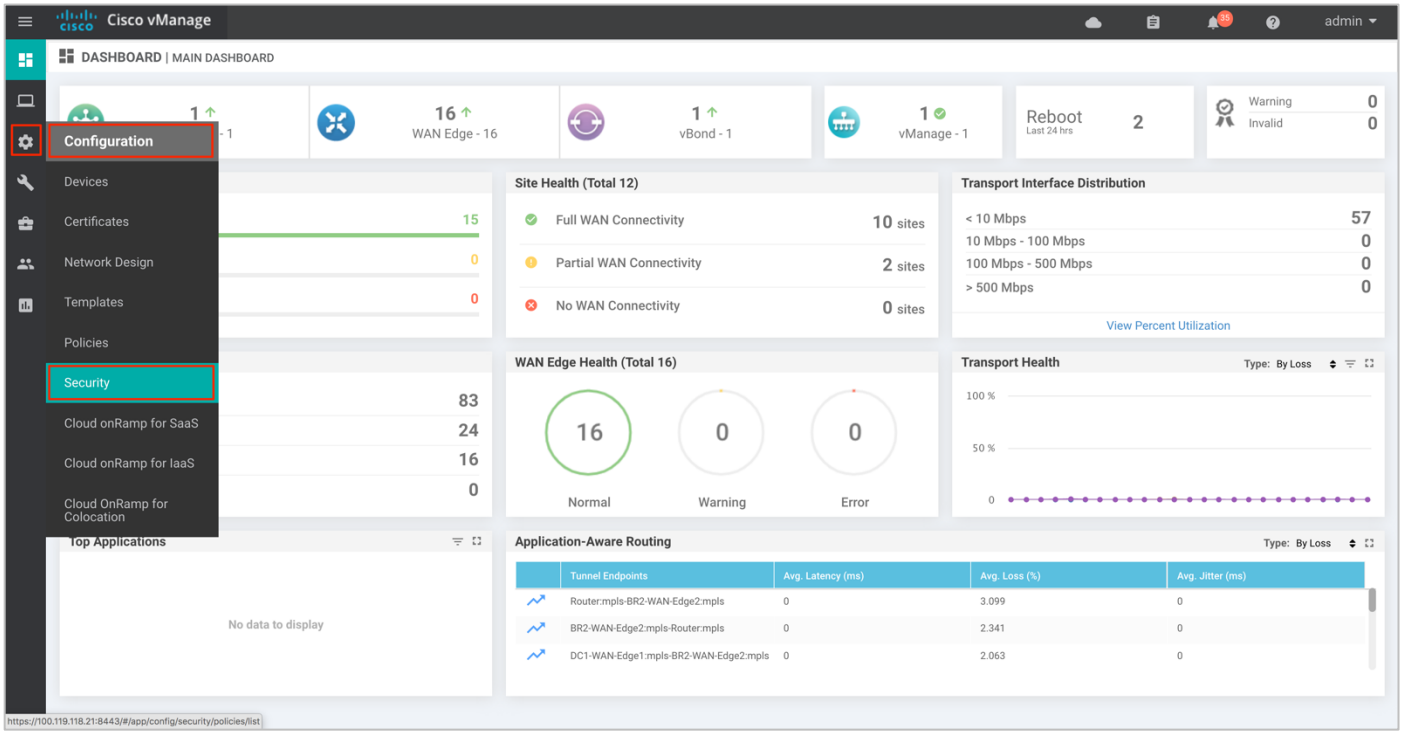
Step 6. Customize the security policy parameters if required. Enable or disable **NAT** feature, based on your use case. For higher throughput or if more packets need to be inspected, set the **Resource Profile** to **High**. Please refer to the Security Policy for Cisco IOS-XE SD-WAN Devices Design Guide, before making changes to the template. Finally, **Save** the template.



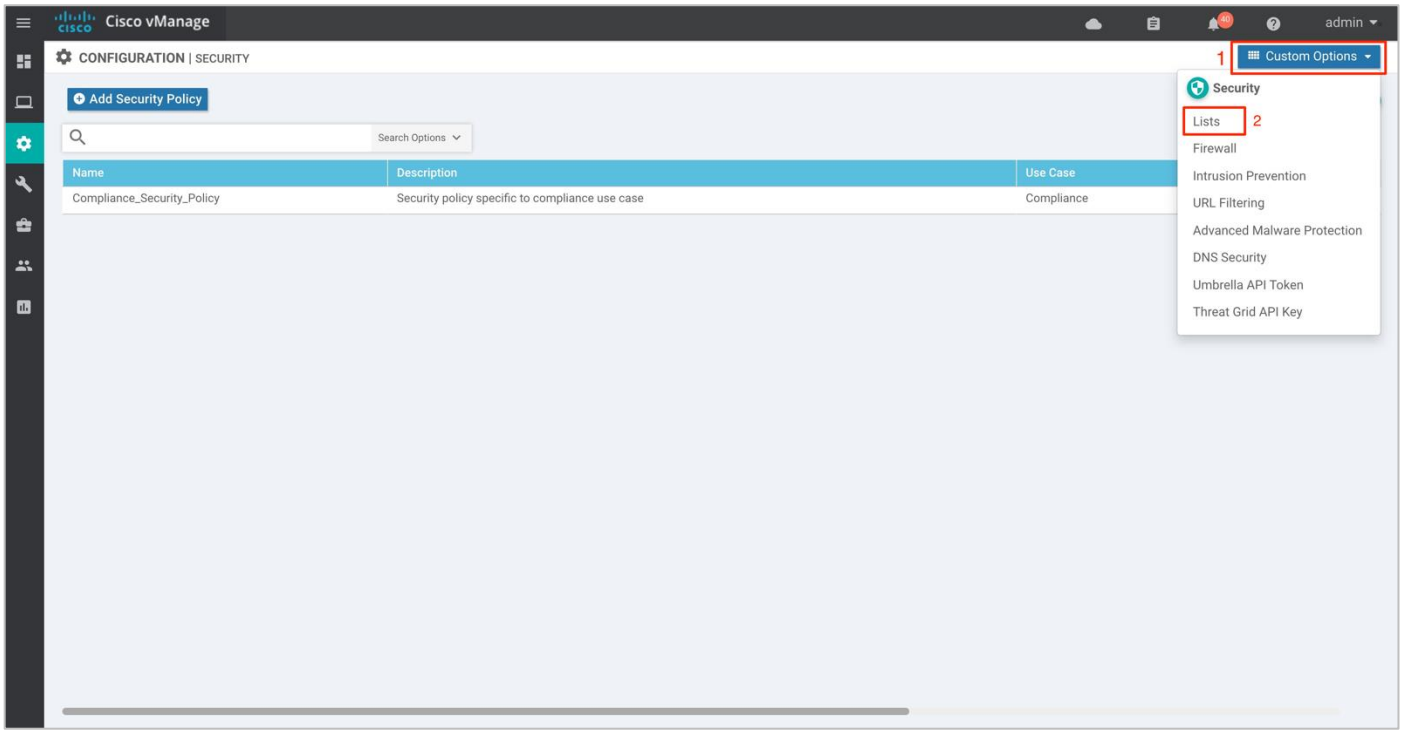
Process 5: (Optional) Define Lists for the Security Policy

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

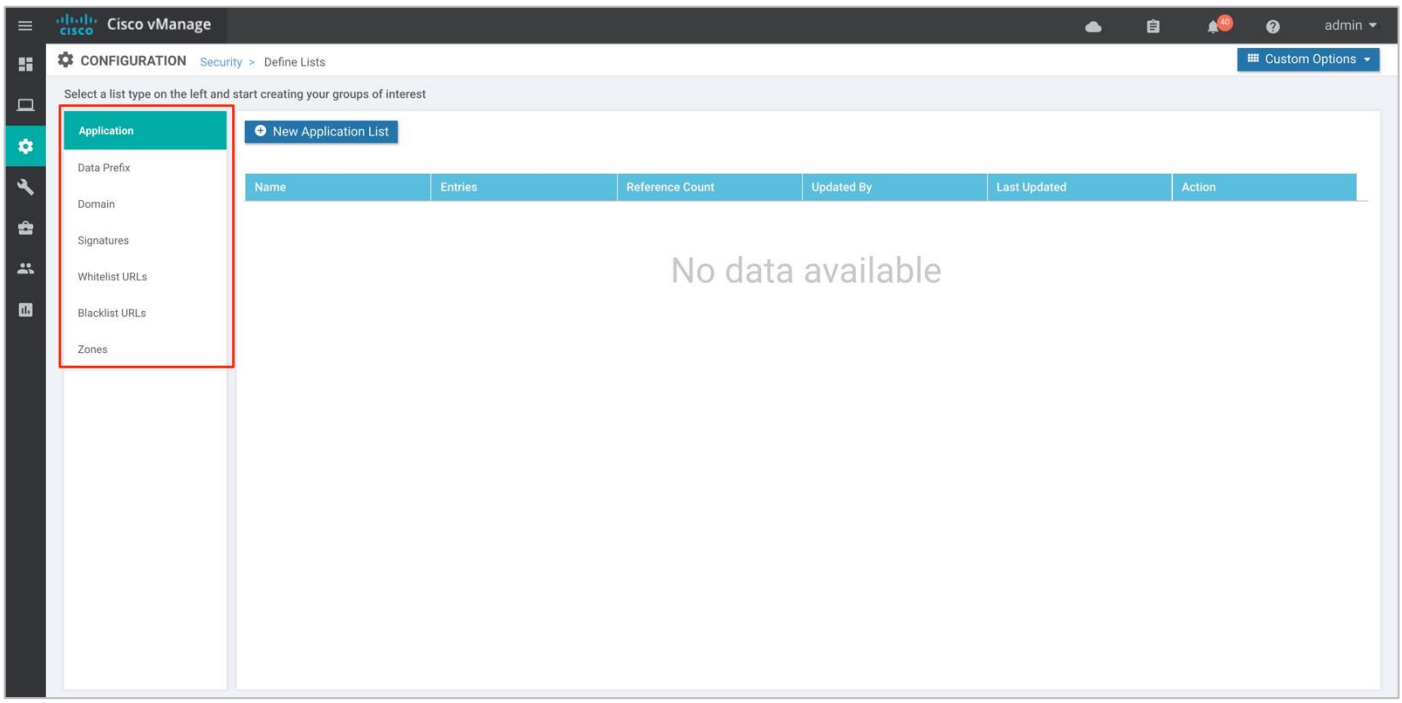
Step 1. Navigate to **Configuration** > **Security**.



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



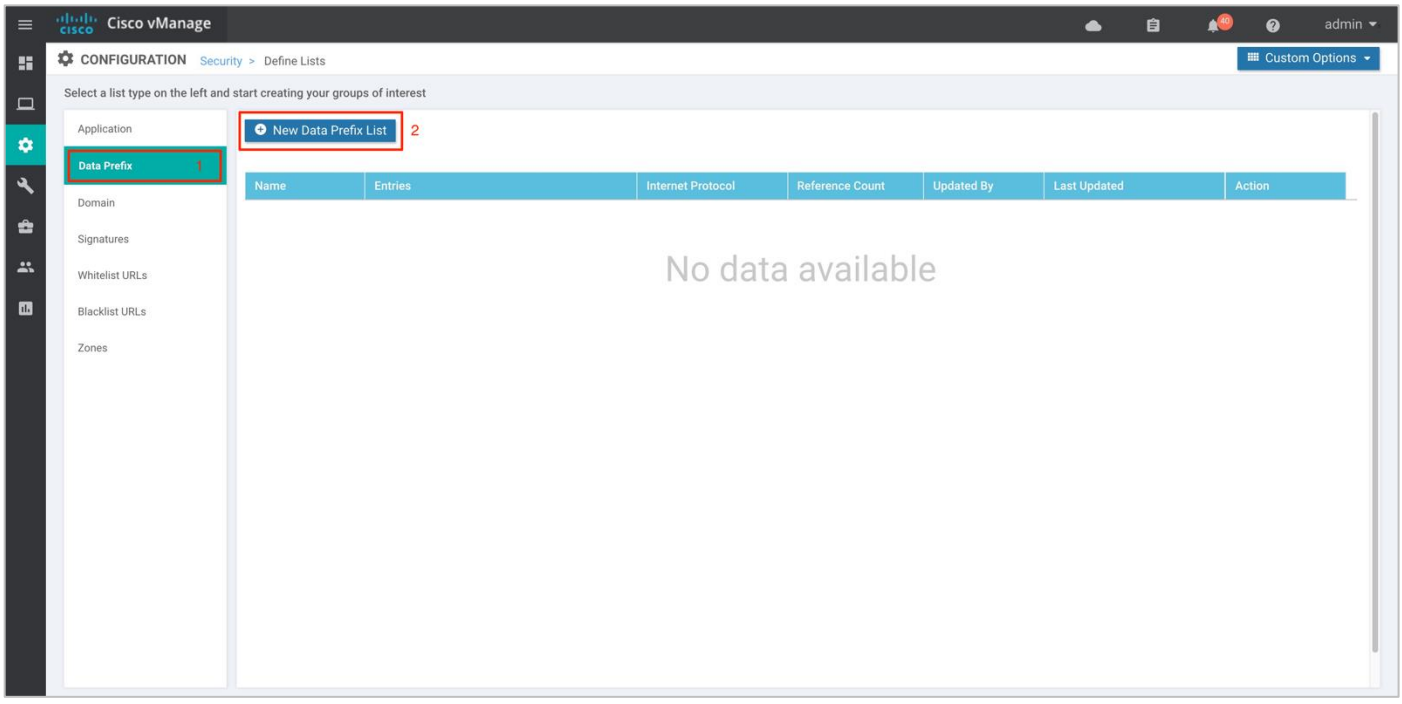
Step 3. Here, you can preconfigure lists such as **Application Lists**, **Data Prefixes**, **Signatures** and **Zones** which are later used as a part of the security policy. URLs can also be configured here, if configuring URL filtering.



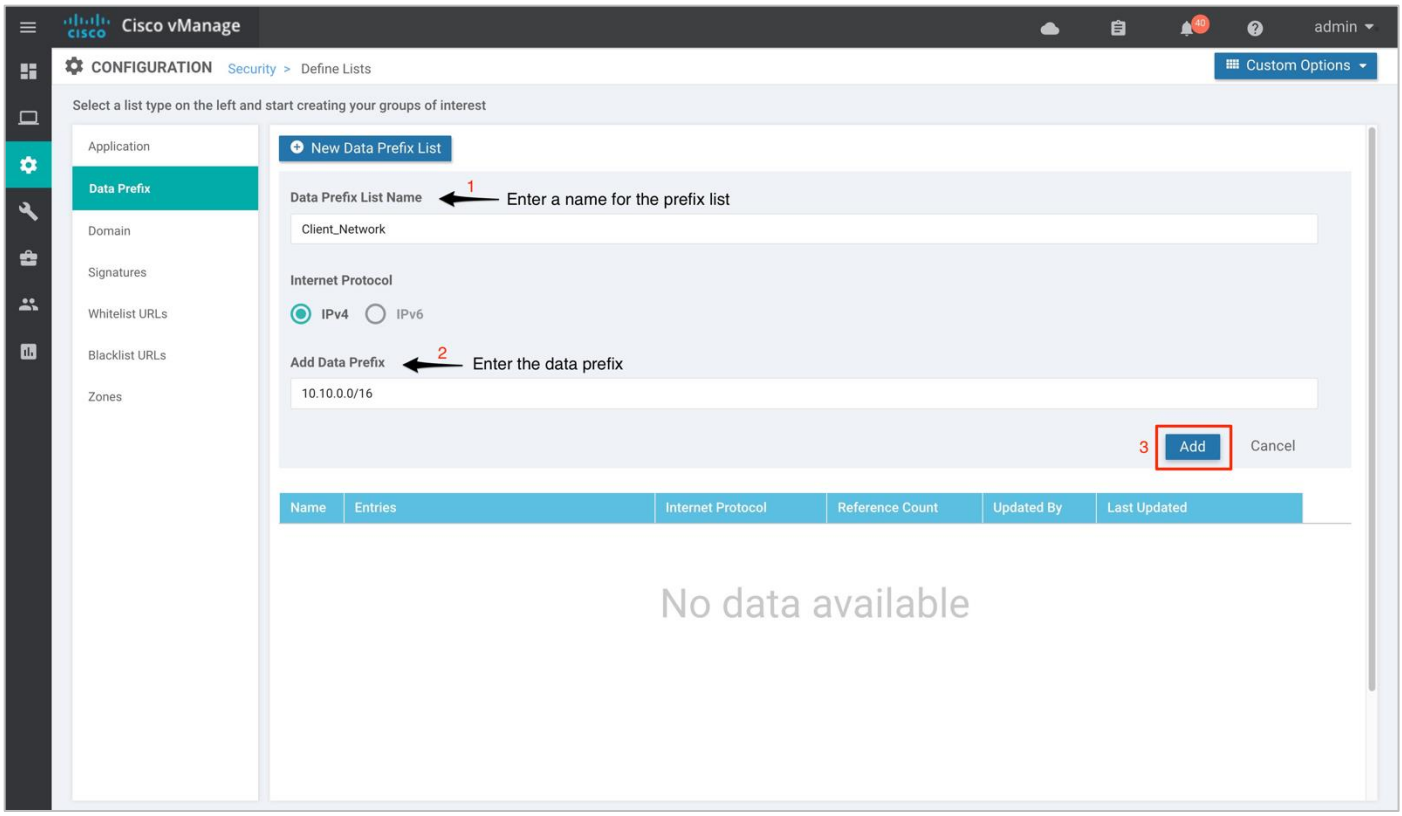
Technical Tip
Applications matched within a firewall policy is always dropped, regardless of what the action condition states.

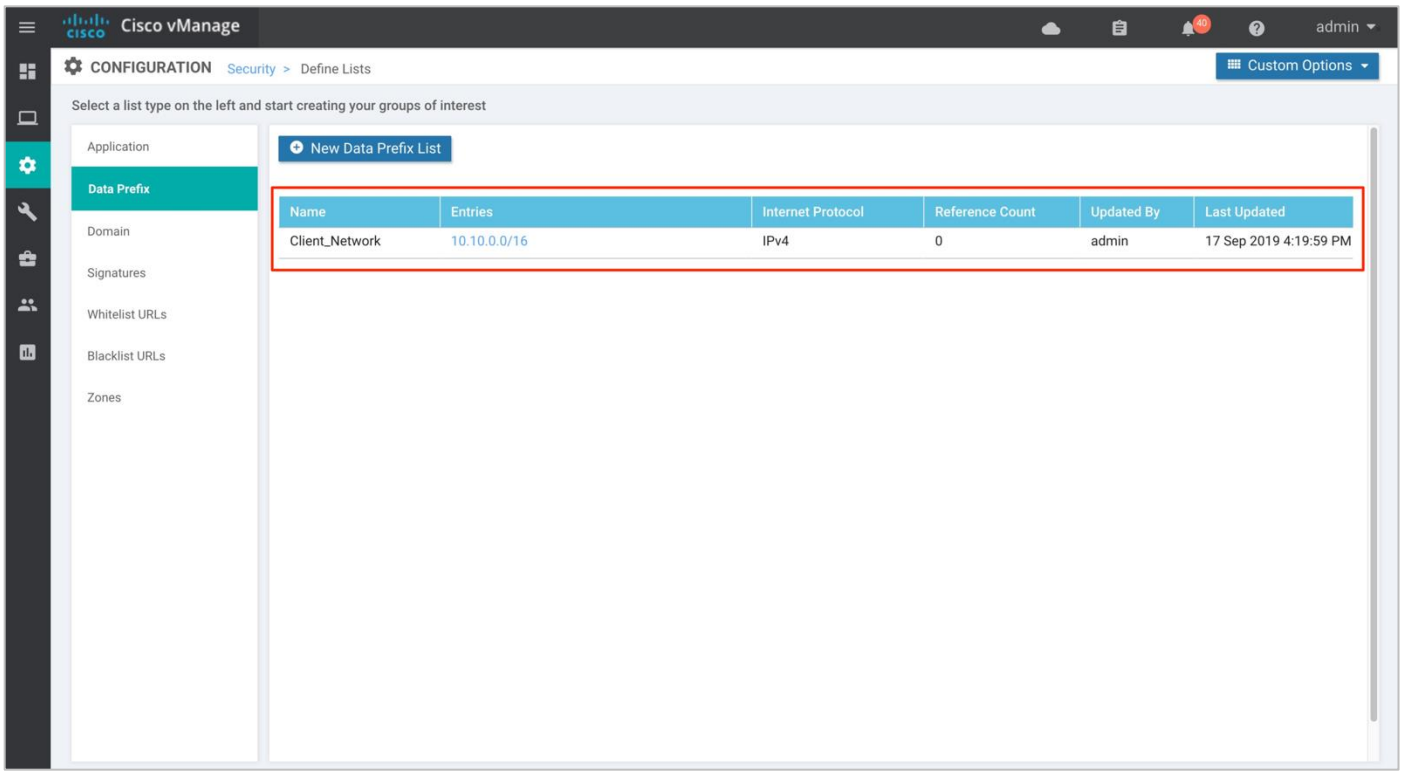
Procedure 1. (Optional) Configure lists for Enterprise Firewall with Application Awareness

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



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**.



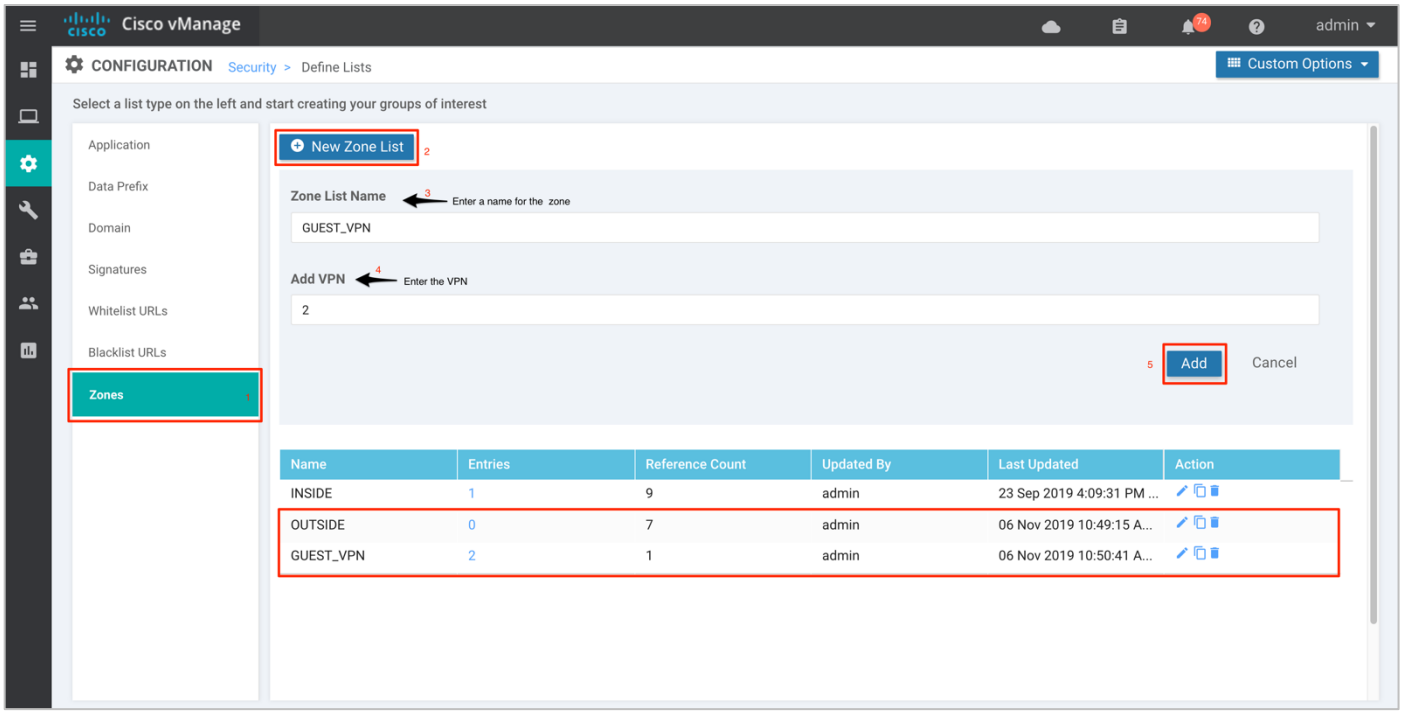


The lists configured under Data Prefix include,

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.**



The list of zones configured for guest access use case.

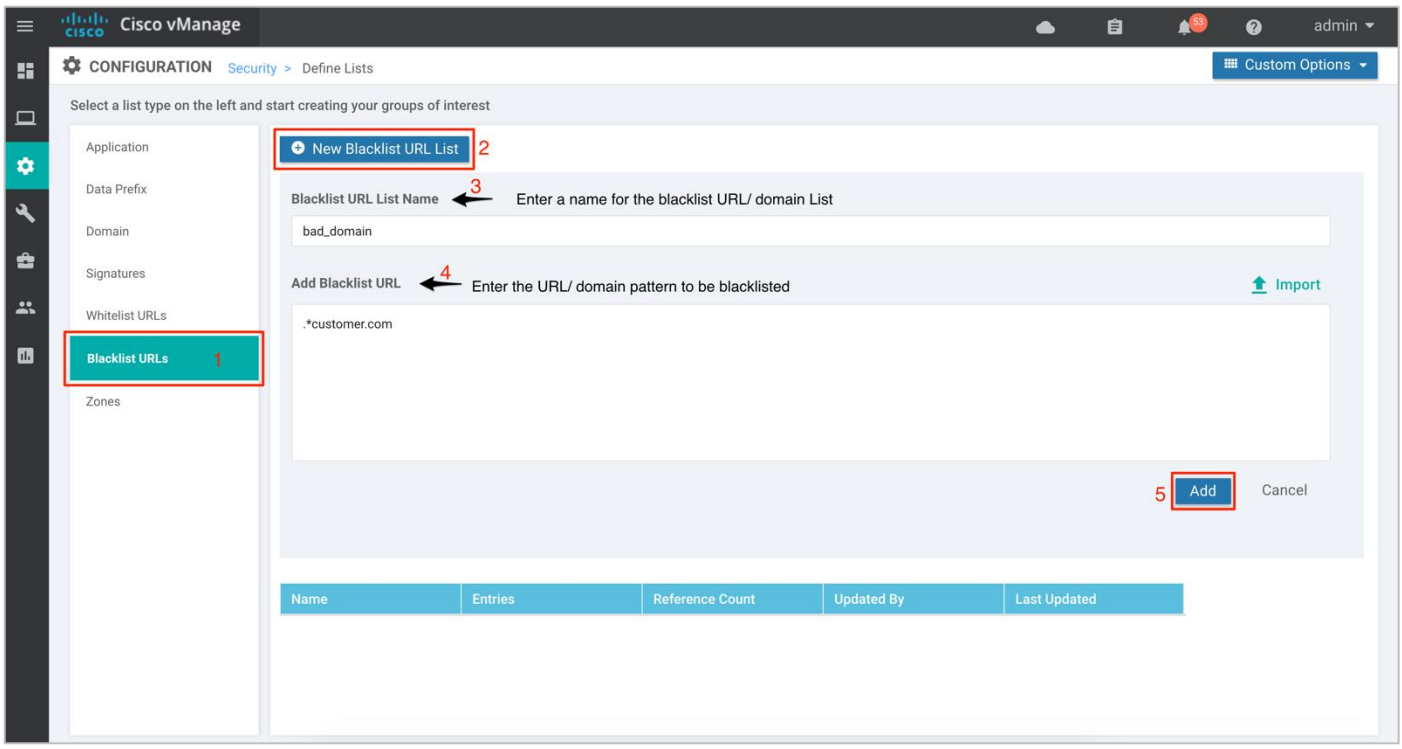
Table 3. Zone List

Data Prefix	Associated Prefix
GUEST_VPN	2
OUTSIDE	0

Procedure 2. (Optional) Configure URL Blacklists/ Whitelists for URL Filtering

Similarly, blacklist or whitelist websites to be used later in the URL security policy.

Step 1. Select **Blacklist/ Whitelist URLs** and then click on **New Blacklist/ Whitelist URL List.** Enter a name within **Blacklist/ Whitelist URL List Name** and add the domain or URL within **Add Blacklist/ Whitelist URL.** Finally, click **Add**.

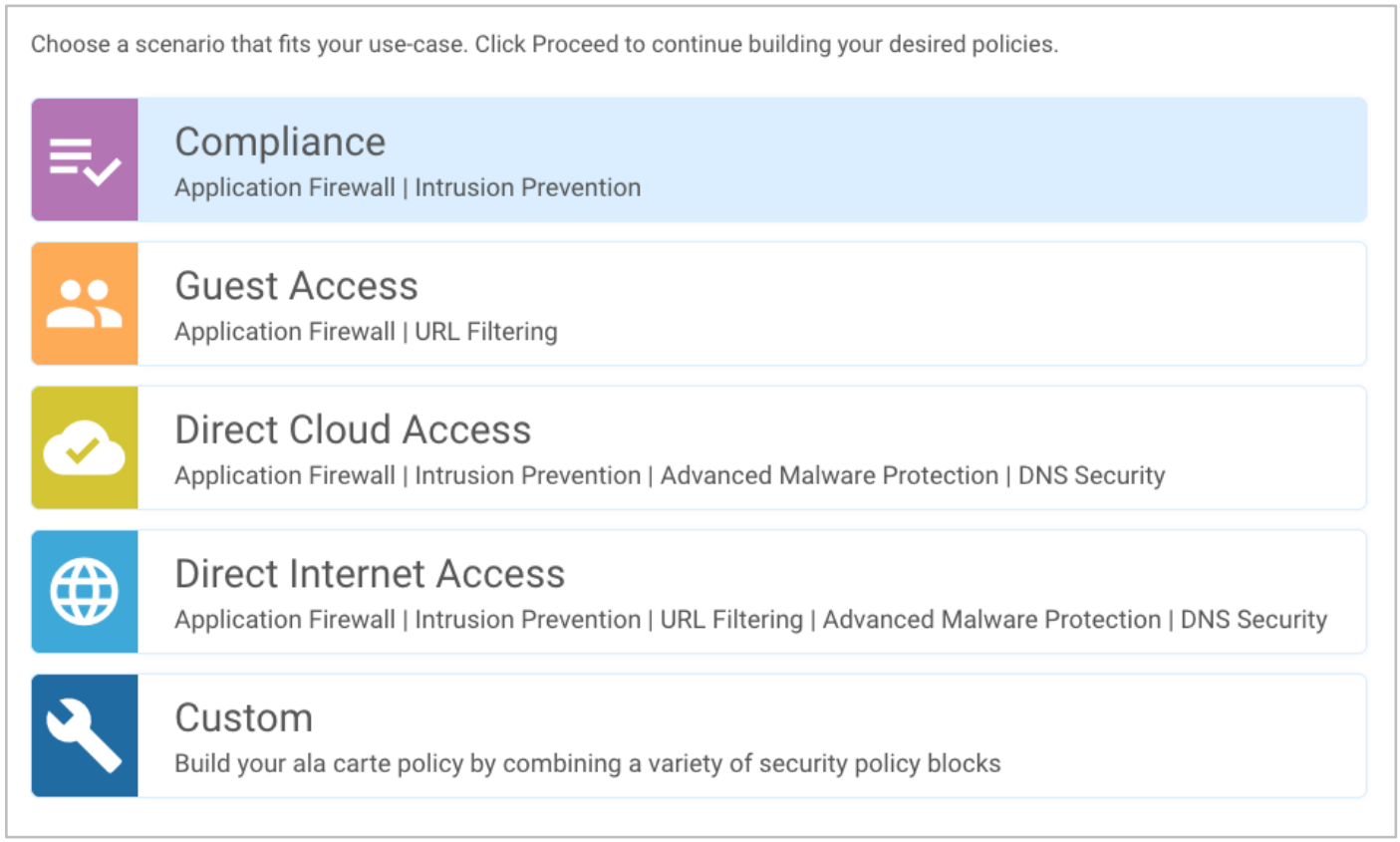


Technical Tip
Some of the possible combinations to whitelist or blacklist domain/URL is .*customer.com, .*.customer.com.

Deploy - Cisco SD-WAN Secure Guest Access

This section covers the steps to deploy Cisco SD-WAN security features specific to the guest access use case. The features discussed include Enterprise Firewall with Application Awareness (Application Firewall) and URL Filtering.

Figure 4. Intent-Based Use Cases



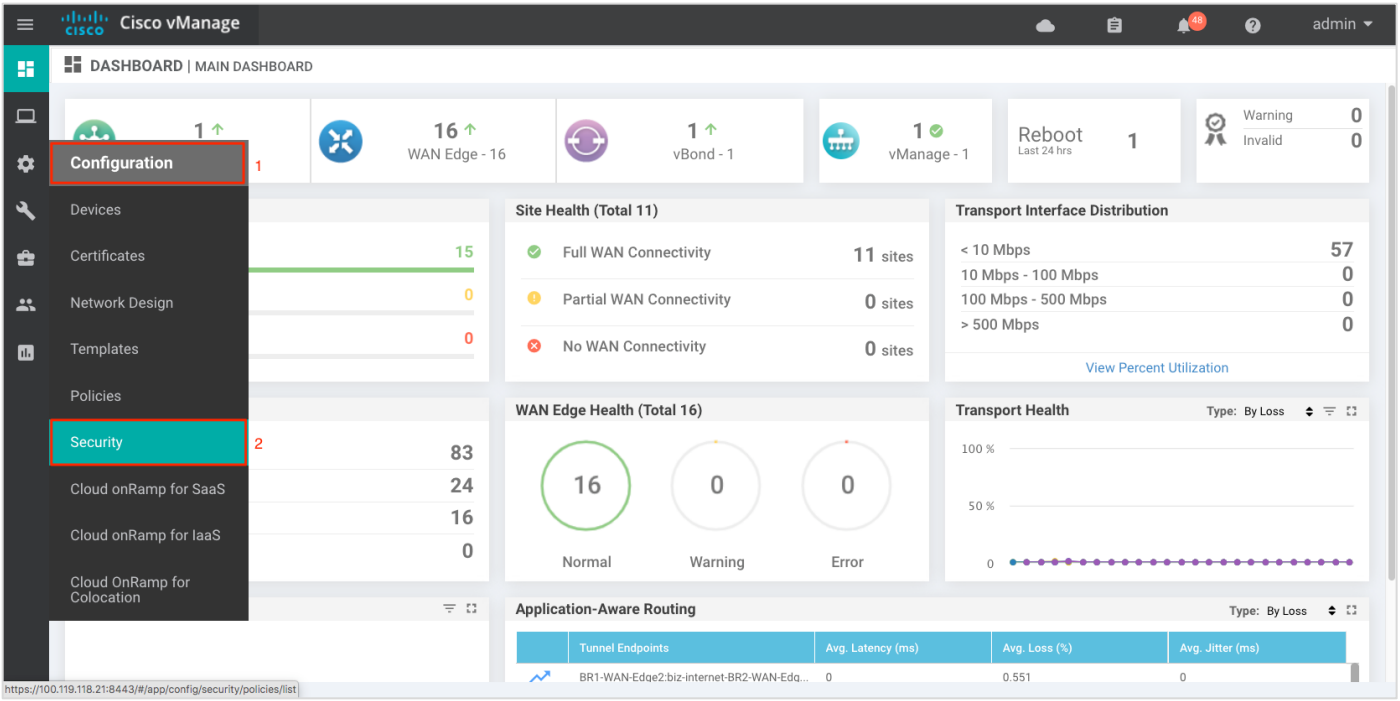
Configuration Workflow

- Make sure the prerequisites explained previously are added.
- Create the security policy containing **Enterprise Firewall with Application Awareness** (**Application Firewall**), and **URL Filtering** (**URLF**).
- Attach the security policy to the **Device Template**.
- Attach the **Security App Hosting** (Container Profile) feature template to the device template.

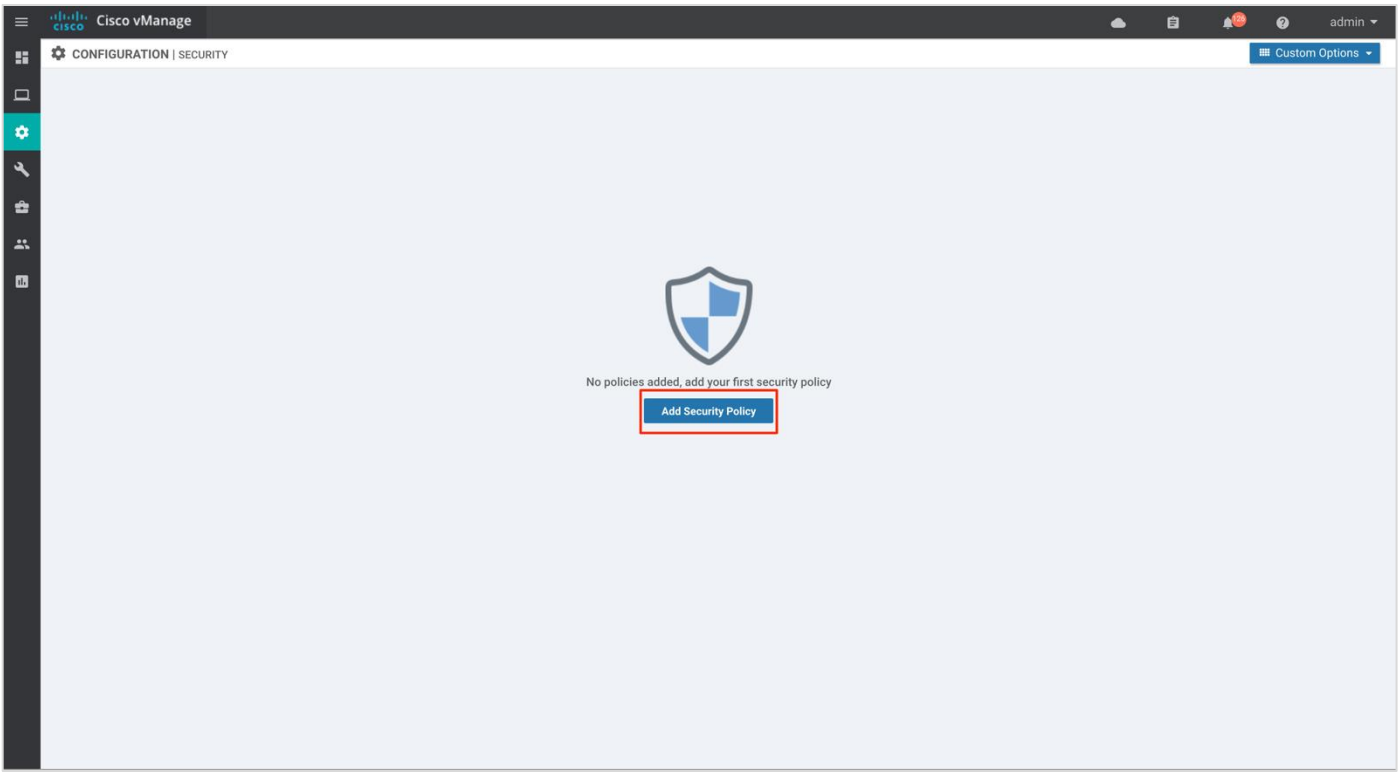
Process 1: Create Security Policy

Configure security parameters such as Enterprise Firewall with Application Awareness and URL Filtering.

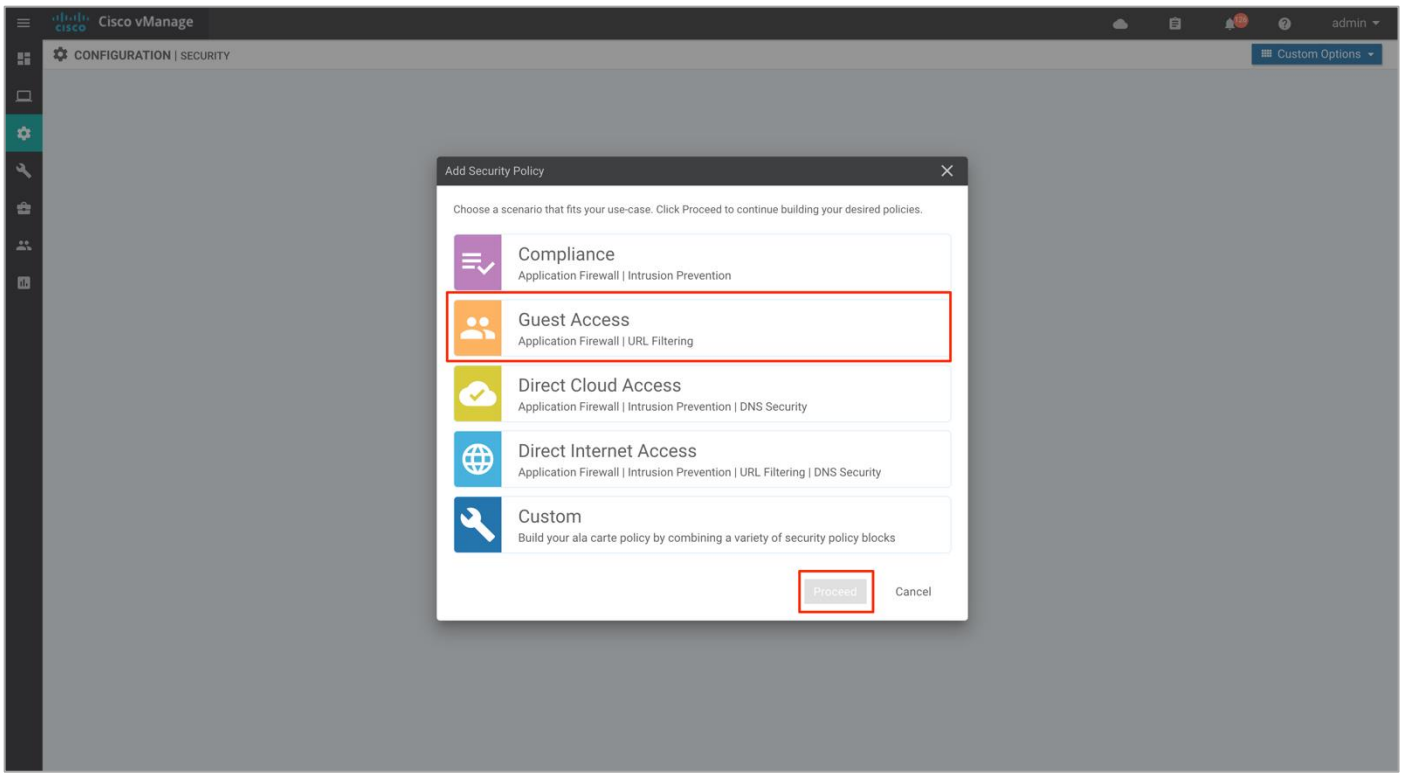
Step 1. In Cisco vManage NMS, navigate to **Configuration** > **Security** in the left side panel.



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

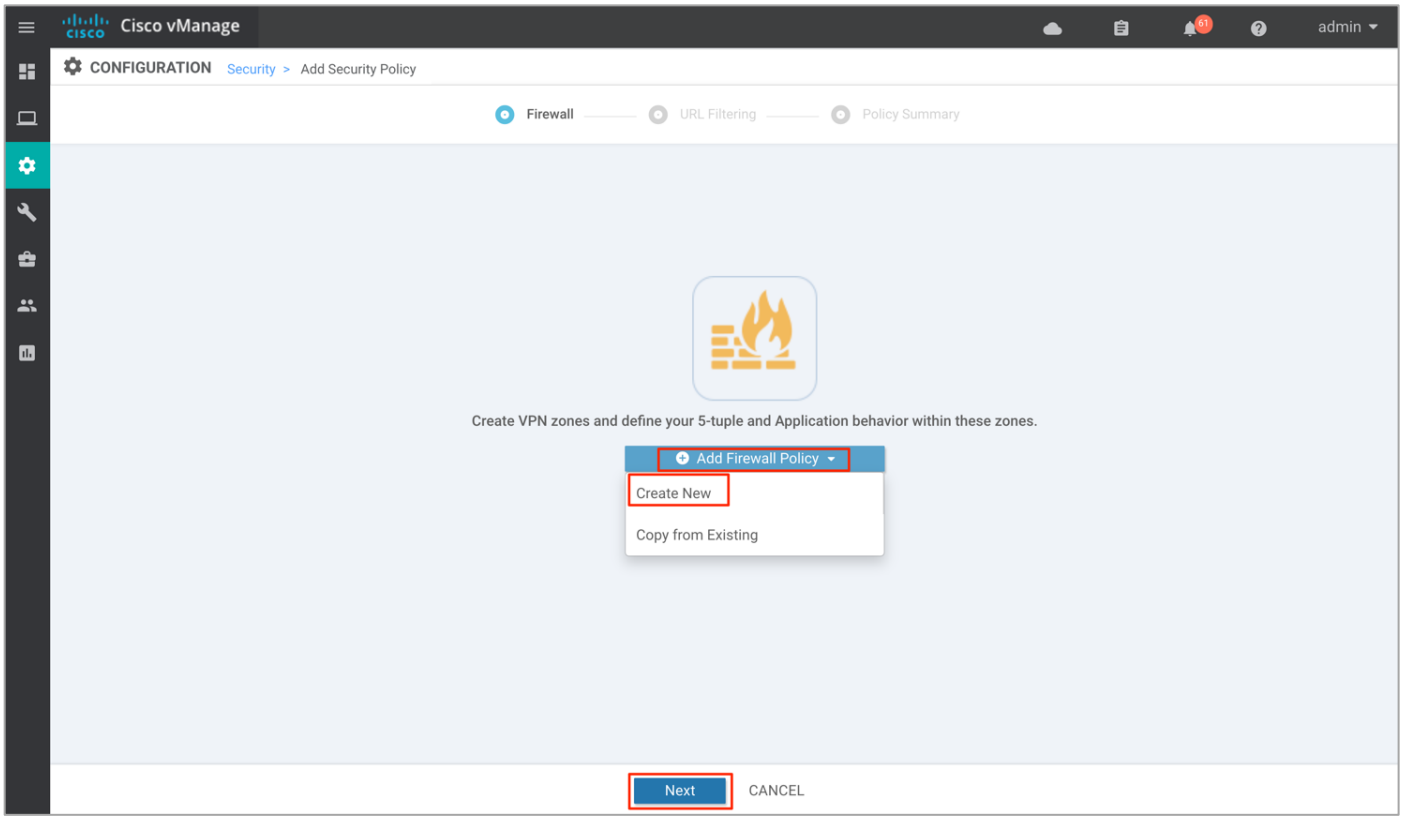


Step 3. The security policy wizard displays a list of intent-based use cases. From the given list, choose **Guest Access** and click **Proceed**.

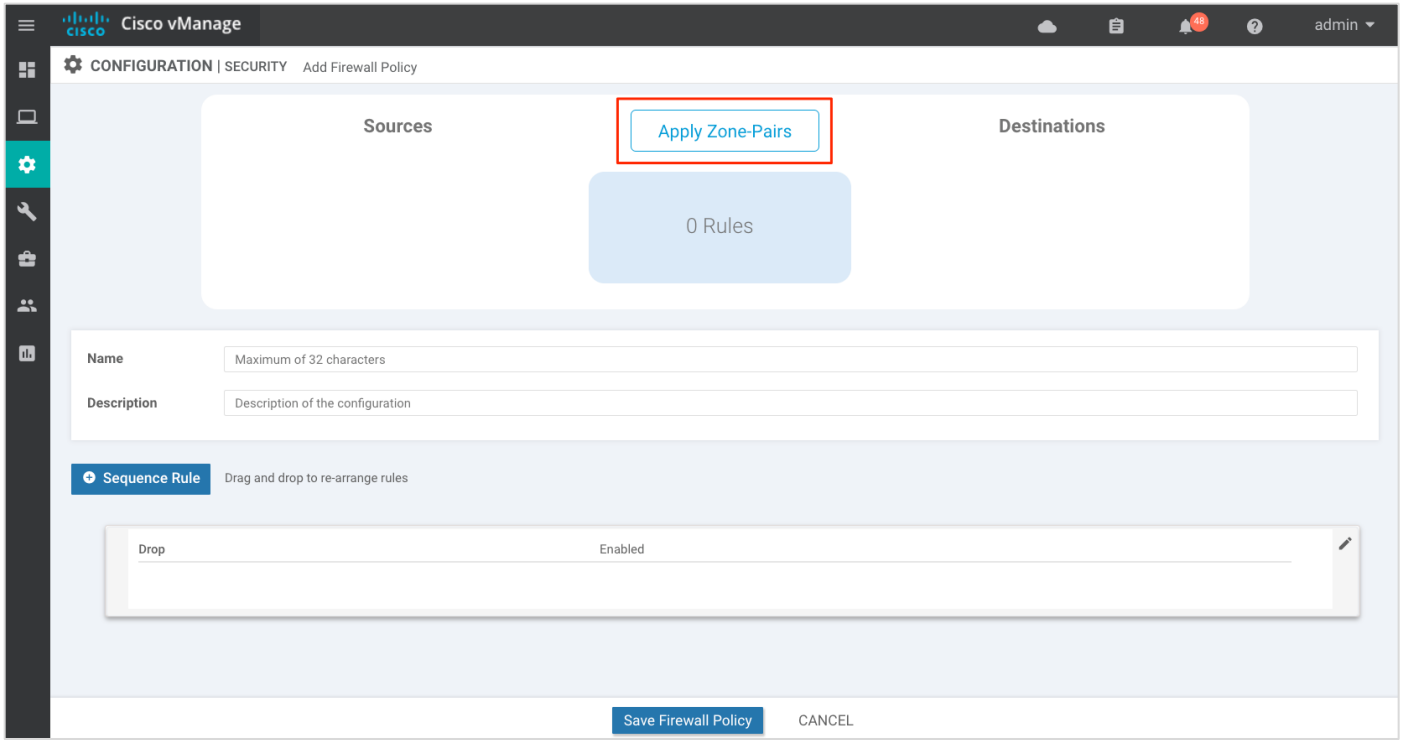


Procedure 1. Configure Enterprise Firewall with Application Awareness

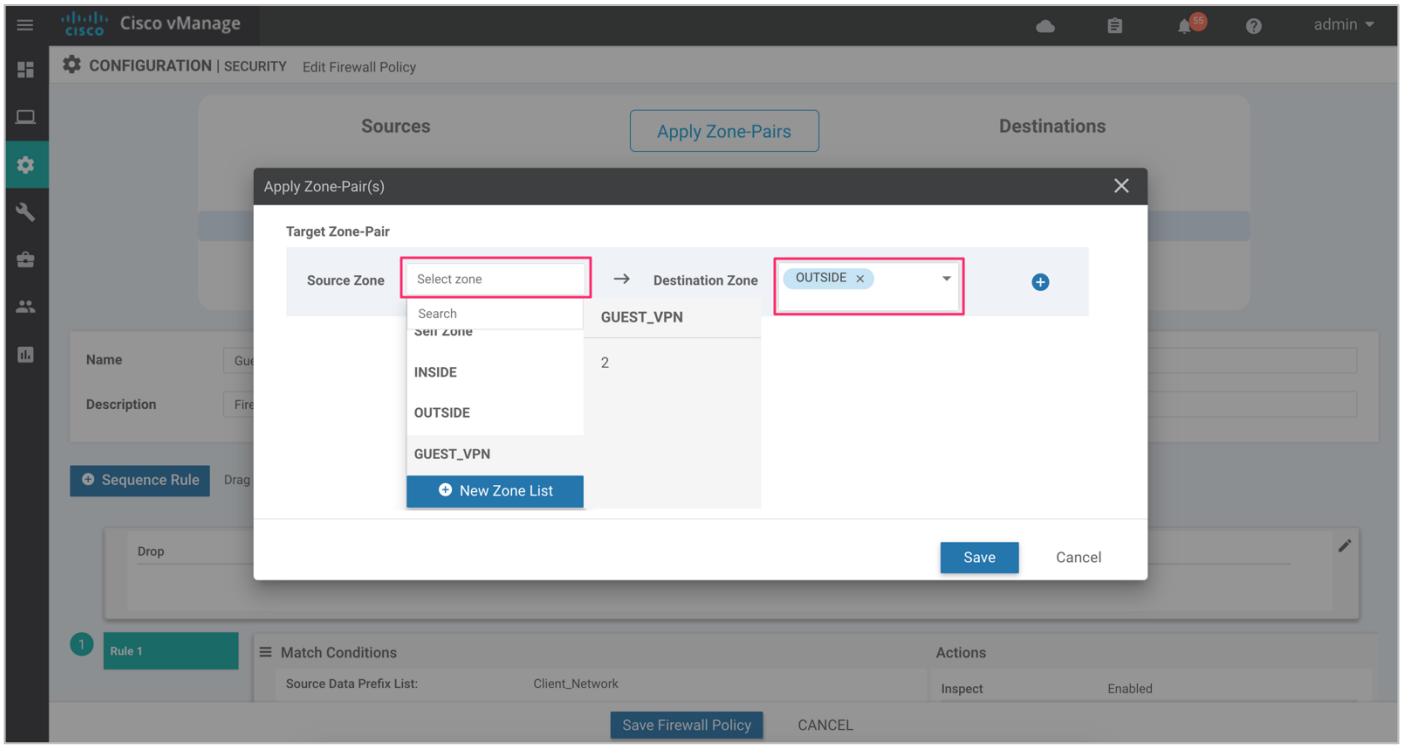
Step 1. Click **Add Firewall Policy,** create a new firewall policy by selecting **Create New** and click **Next**. However, if you have preconfigured a firewall policy, simply click on **Copy from Existing**.



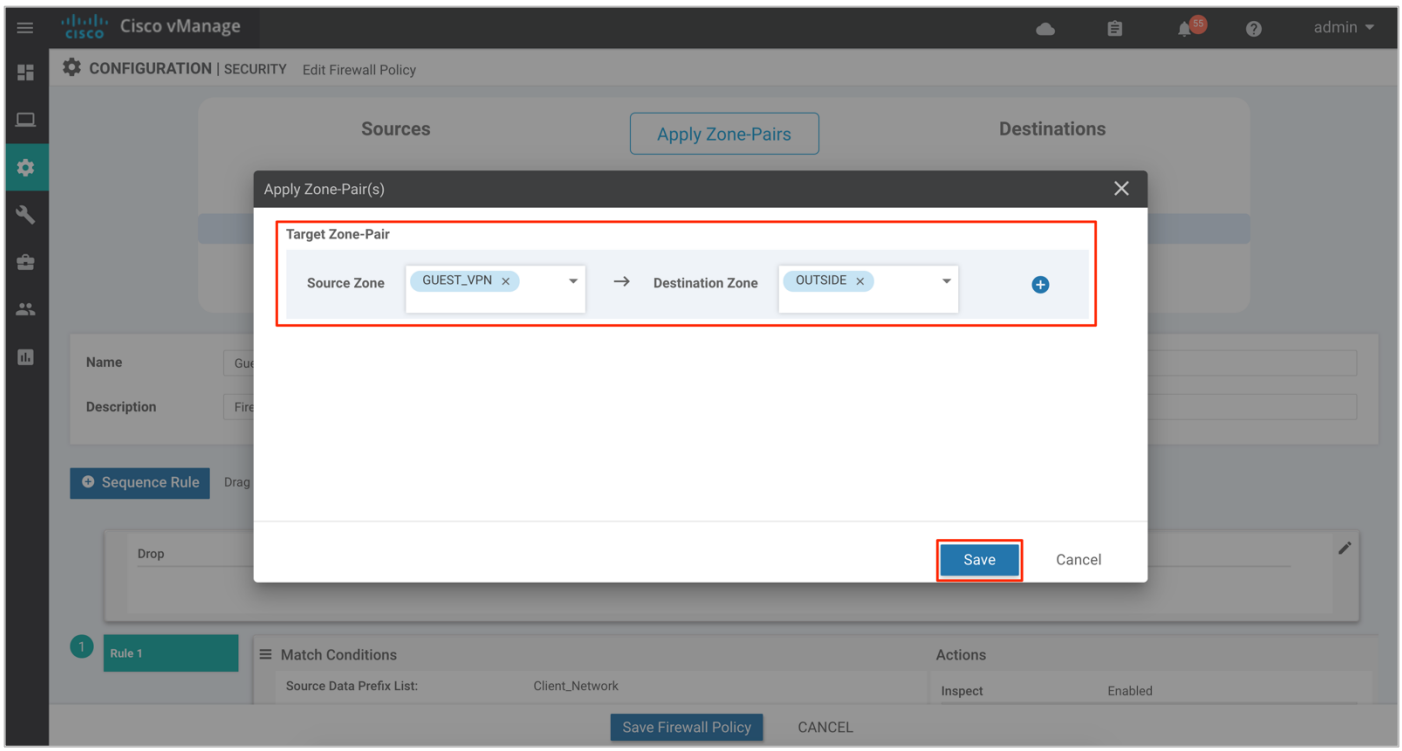
Step 2. Click on **Apply Zone-Pairs** to create your zone-pairs.



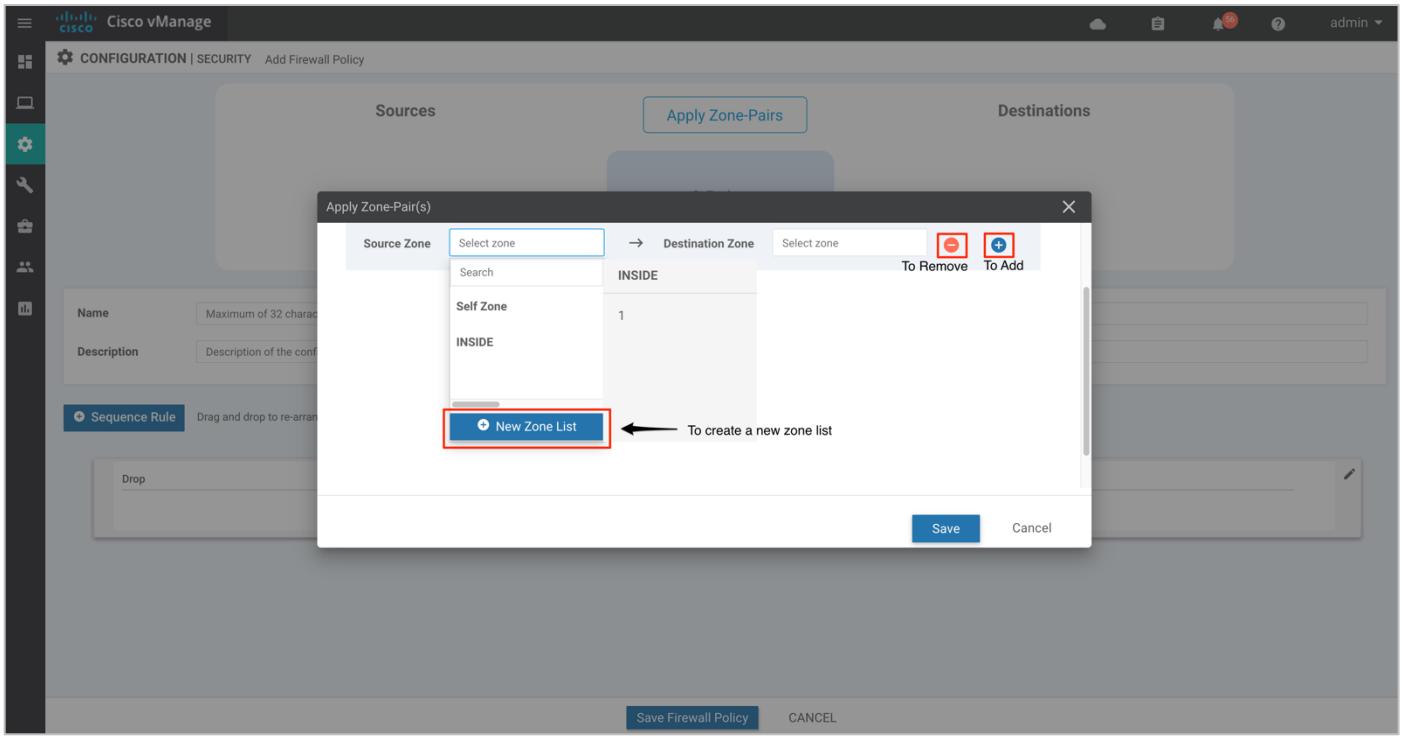
Step 3. Add the created zones to **Source Zone** and **Destination Zone**, and click **Save**.



Step 4. After the zone pair is created, 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. Here's an example to understand it better,

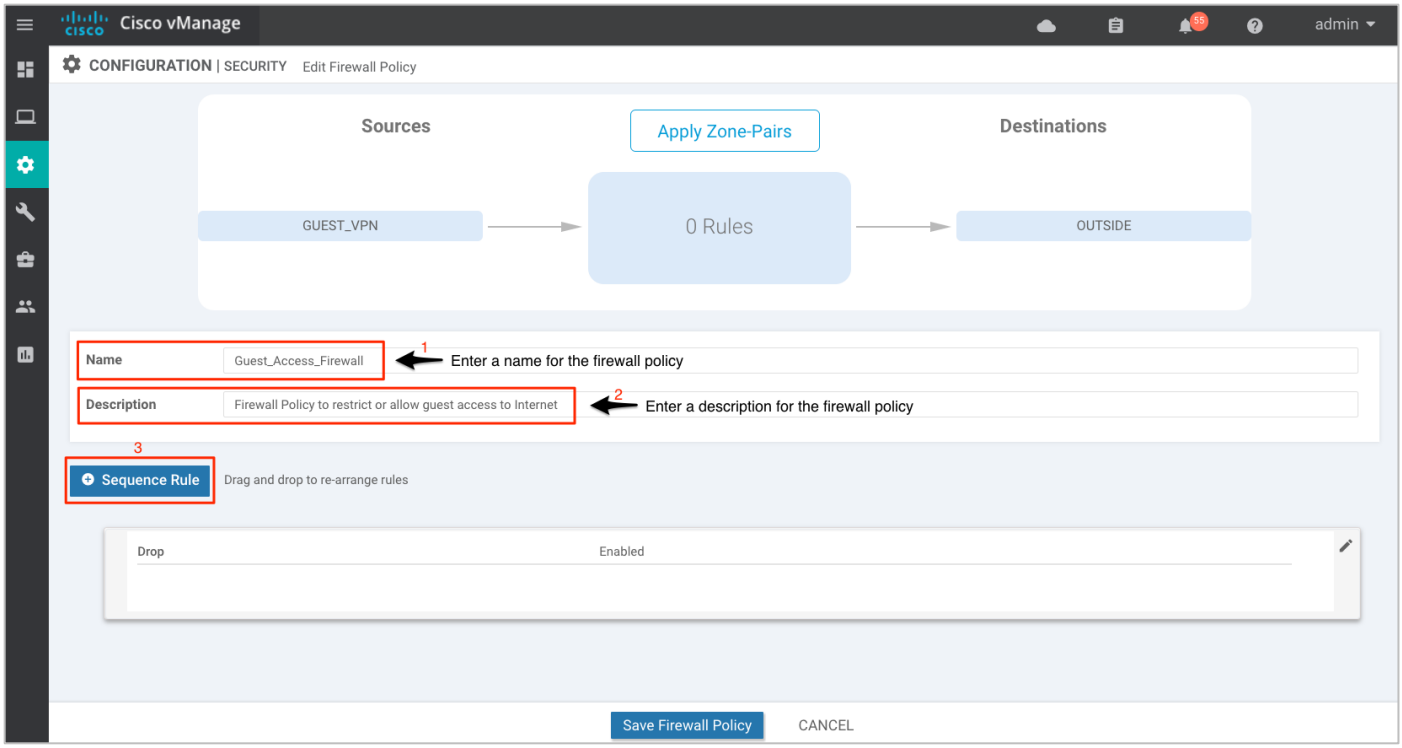


Technical Tip

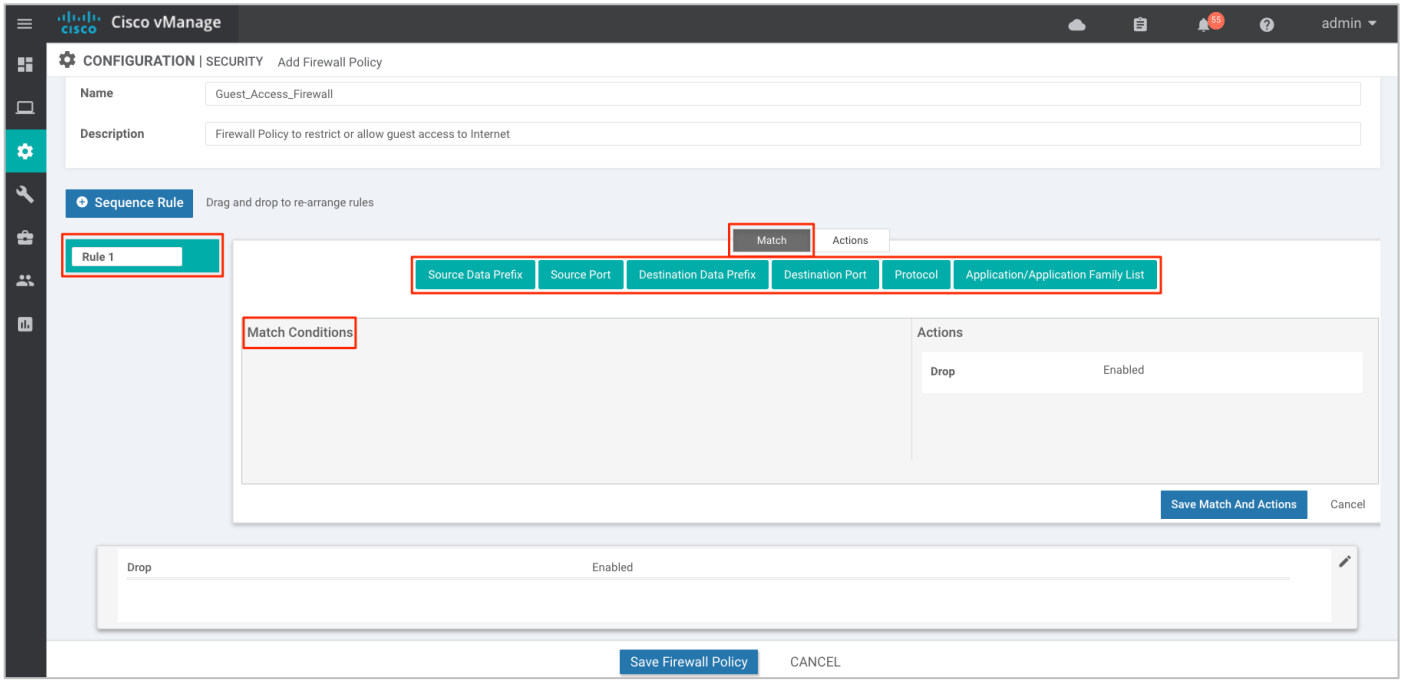
Starting from Cisco SD-WAN Release 19.2 and IOS XE Release 16.12, the Self Zone option is added in the Source Zone field. Self-zone is a self-defined zone that protects the packet going to or coming from the device. A zone pair that includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the

device.

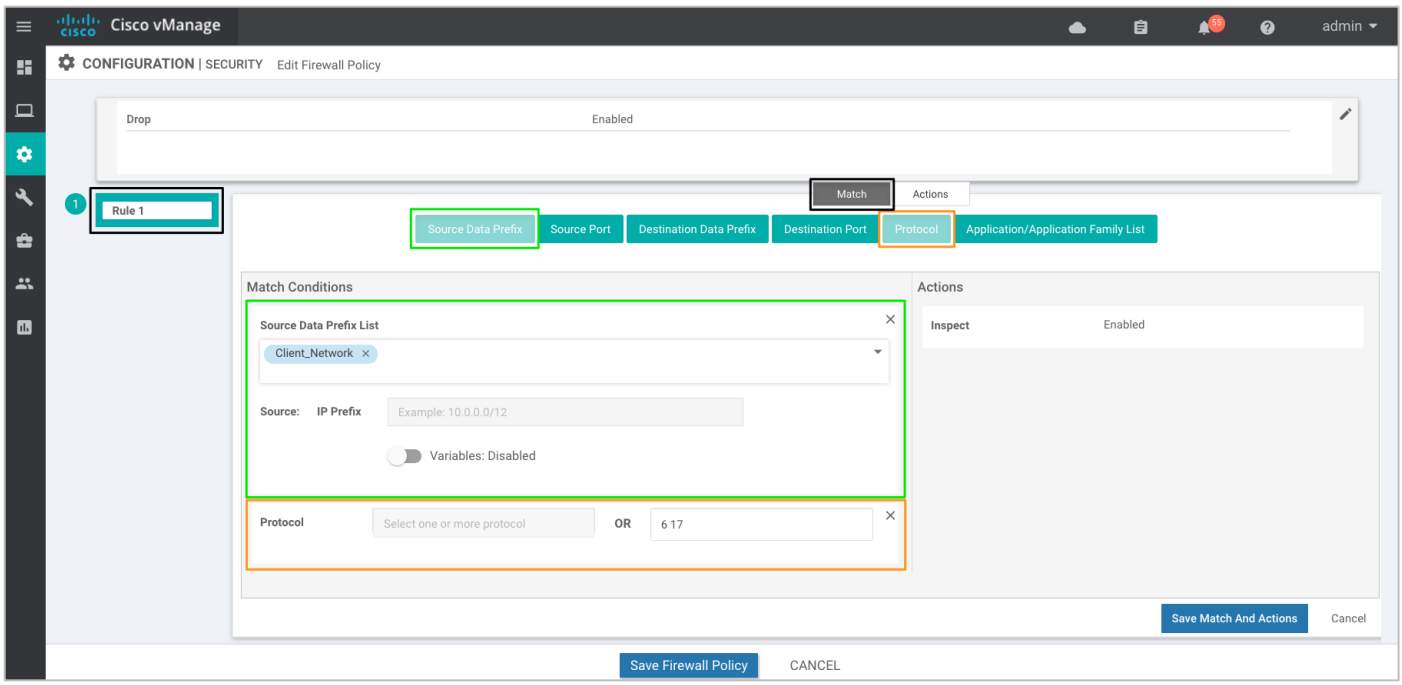
Step 5. Enter a **Name** and **Description** in the field for the firewall policy, next click on **Sequence Rule** to add policy rules.



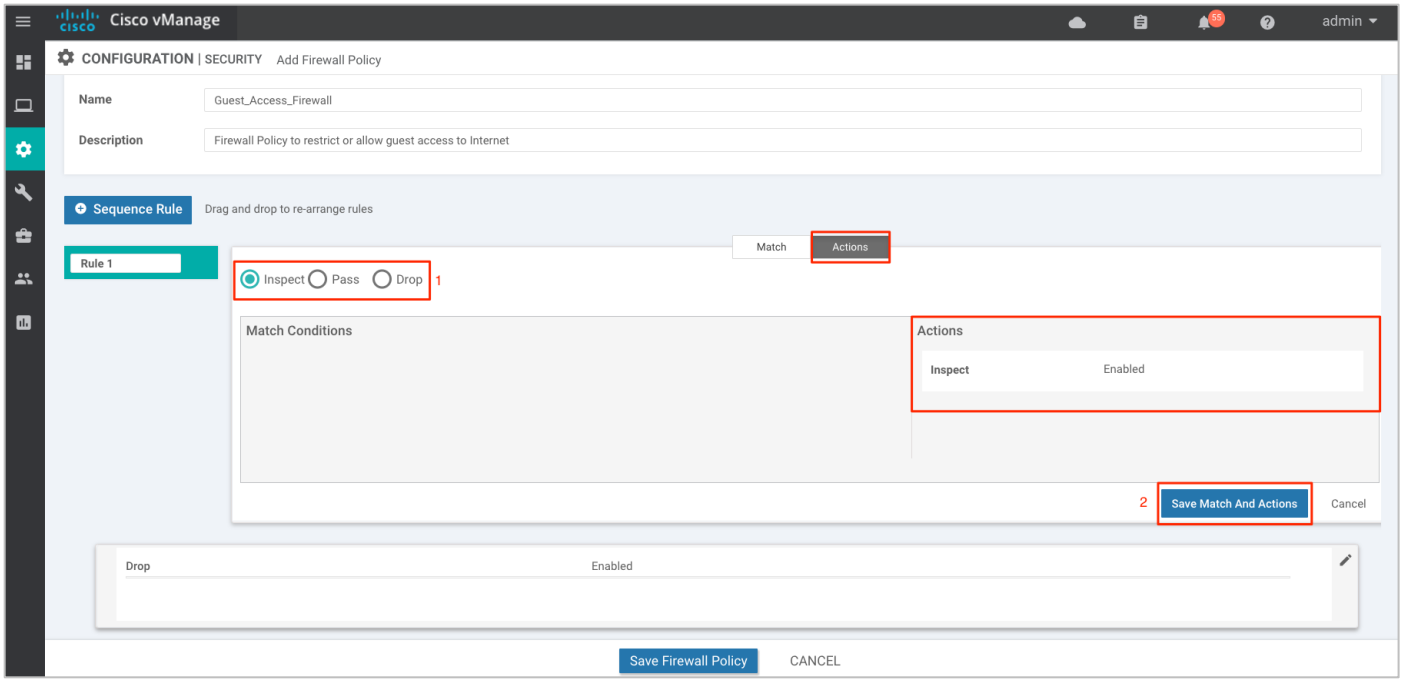
Step 6. The **Match** tab is selected by default. Click a match condition: **Source Data Prefix**, **Source Port**, **Destination Data Prefix, Destination Port**, **Protocol**, **Application/Application Family List**. You can select and configure more than one match condition in a sequence.



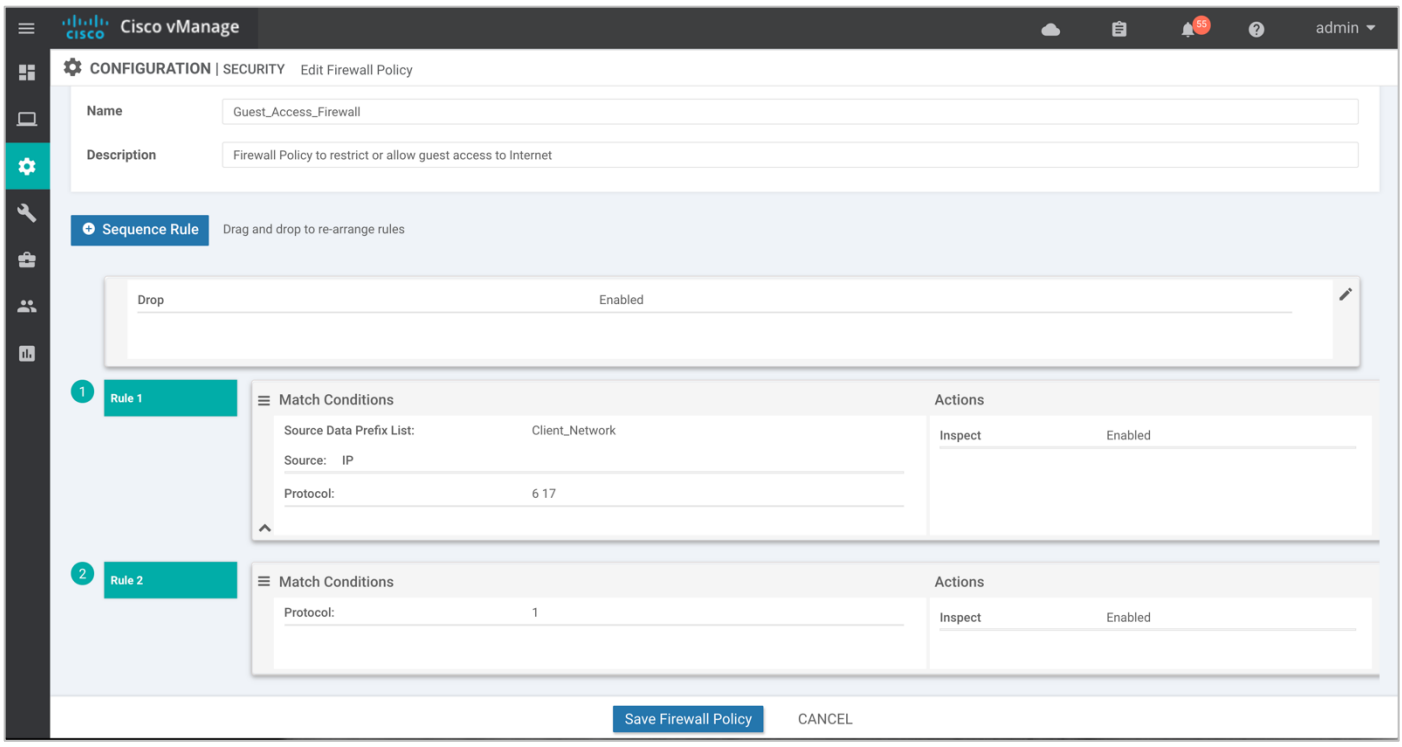
Here's an example of sequence rule within the Enterprise Firewall with Application Awareness policy deployed.



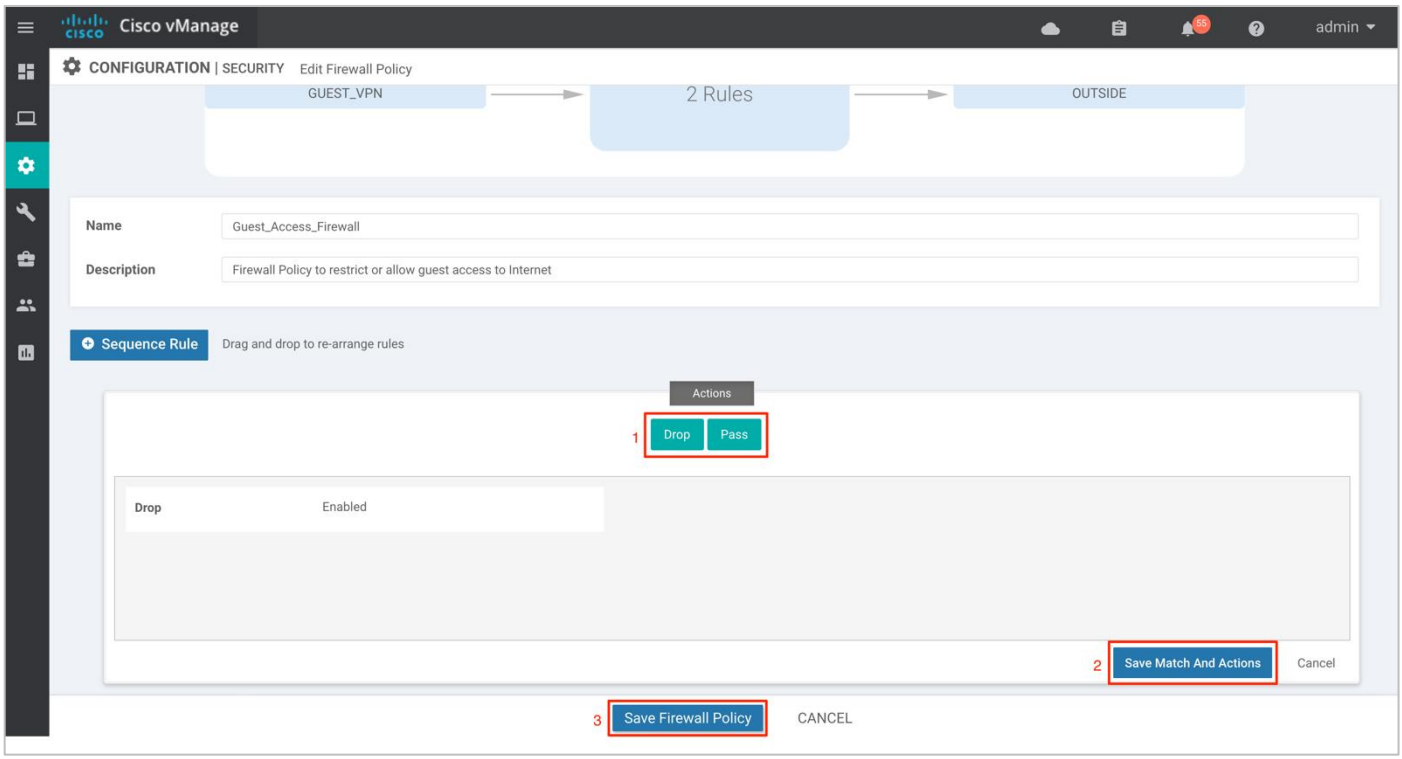
Step 7. Next, click on **Actions** tab and enter the actions to take if the traffic matches. We have enabled **Inspect**.



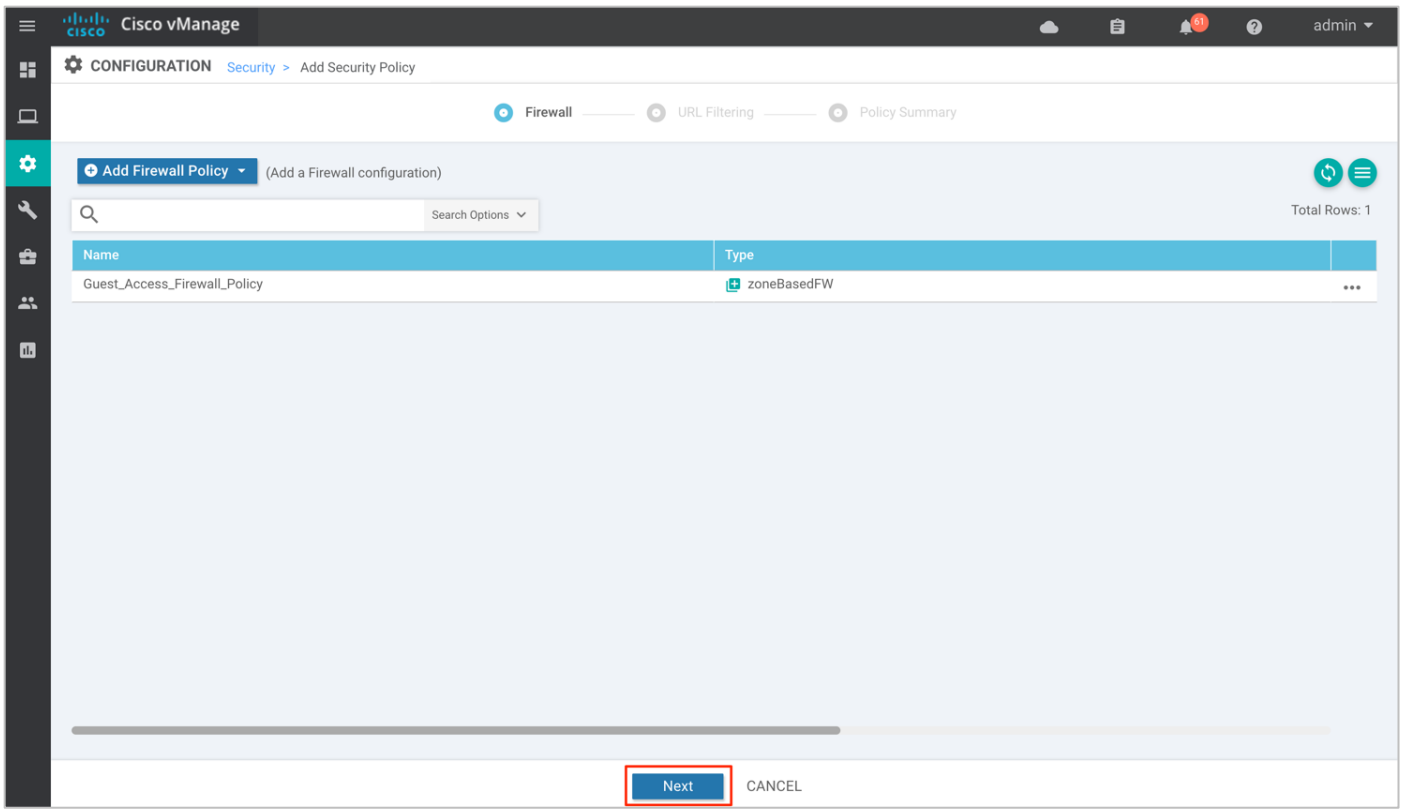
Note, in this deployment, the following sequence rules were added.



Step 8. (Optional) If a packet matches none 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.

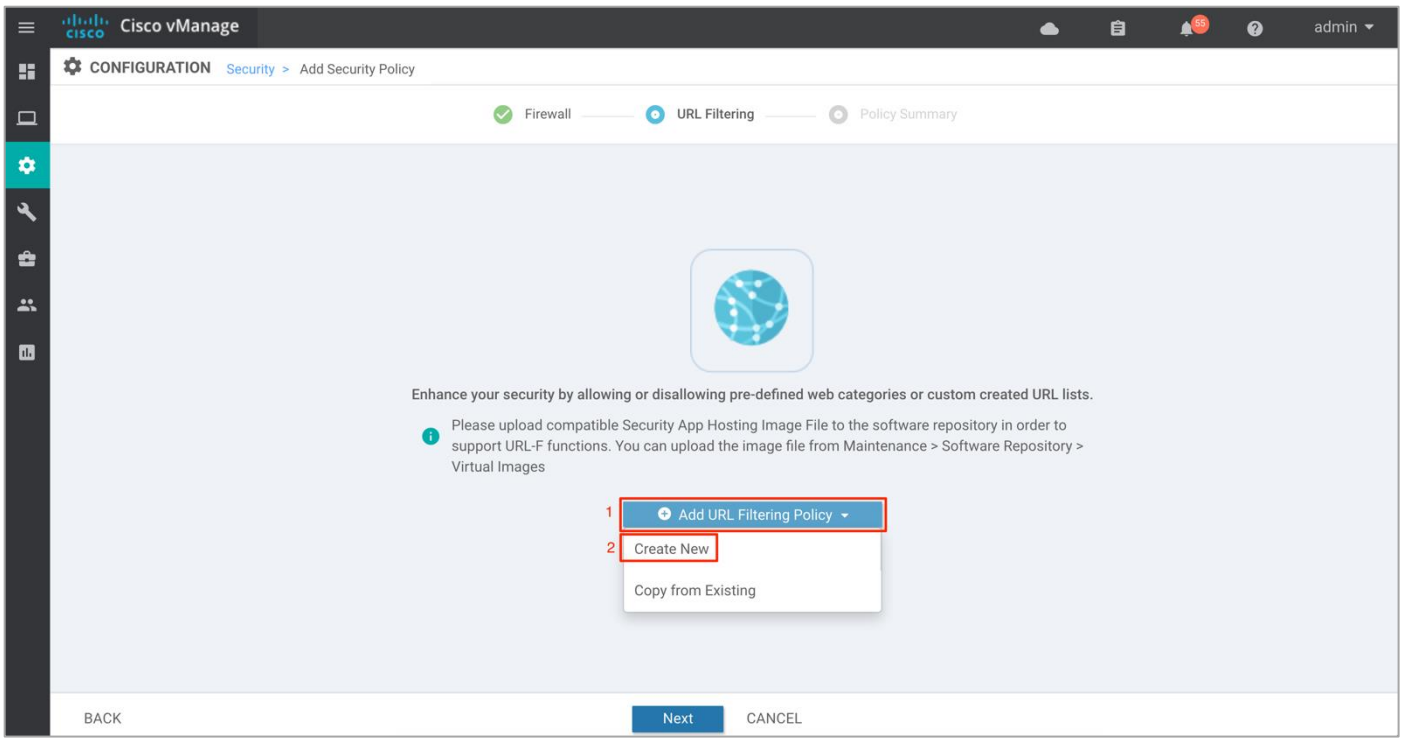


Step 9. Click **Next** to select the **URL Filtering Policy** tab.



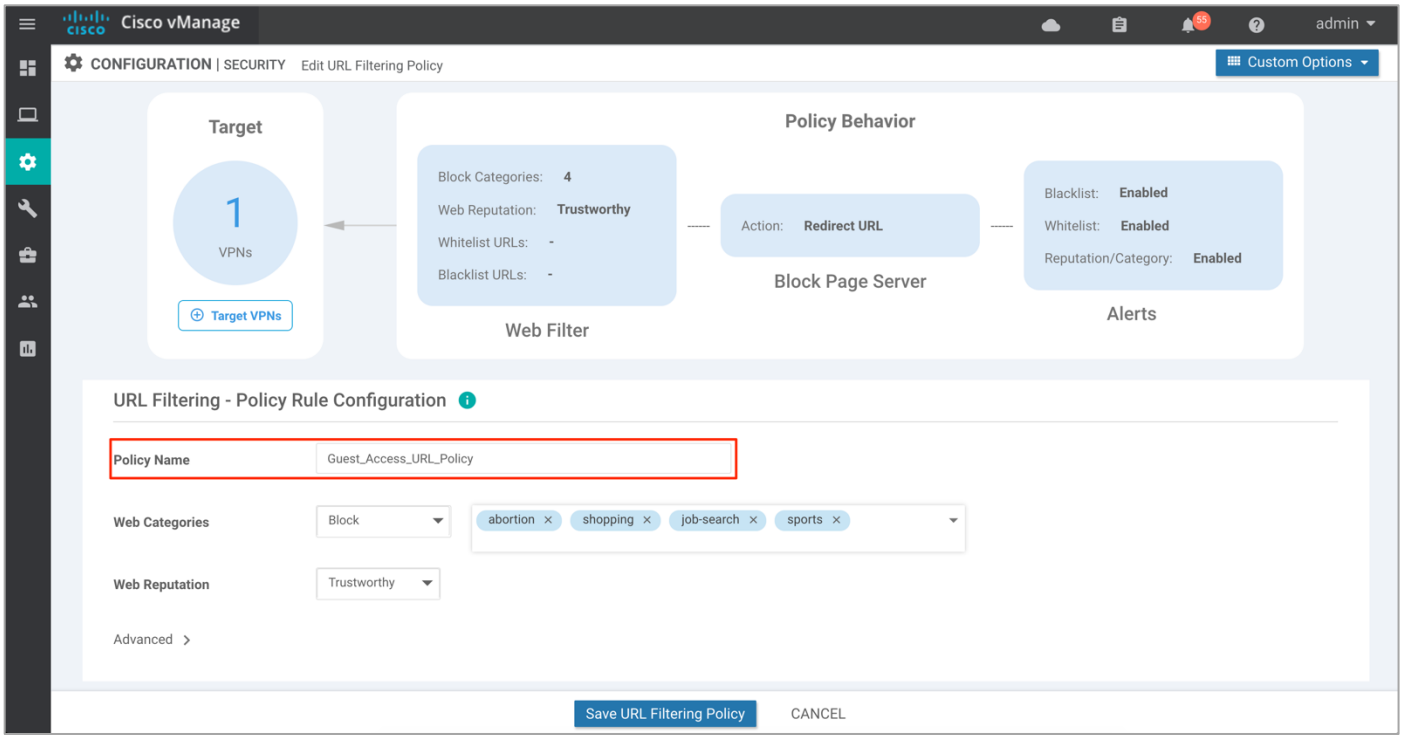
Procedure 2. Configure URL Filtering Policy

Step 1. Click **Add URL Filtering Policy** to allow or drop pre-defined web categories or custom created URL lists and click **Next**.



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

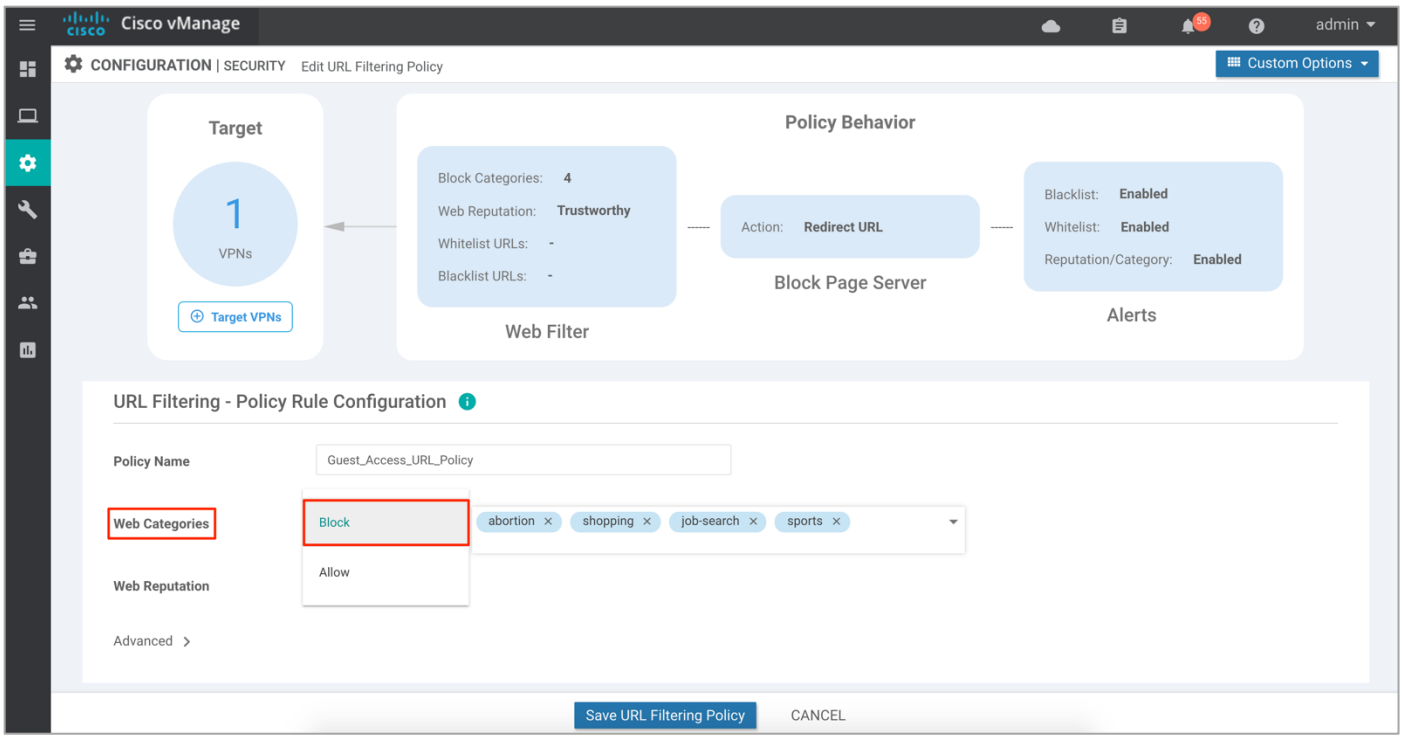
Step 2. Enter a policy name in the **Policy Name** field.



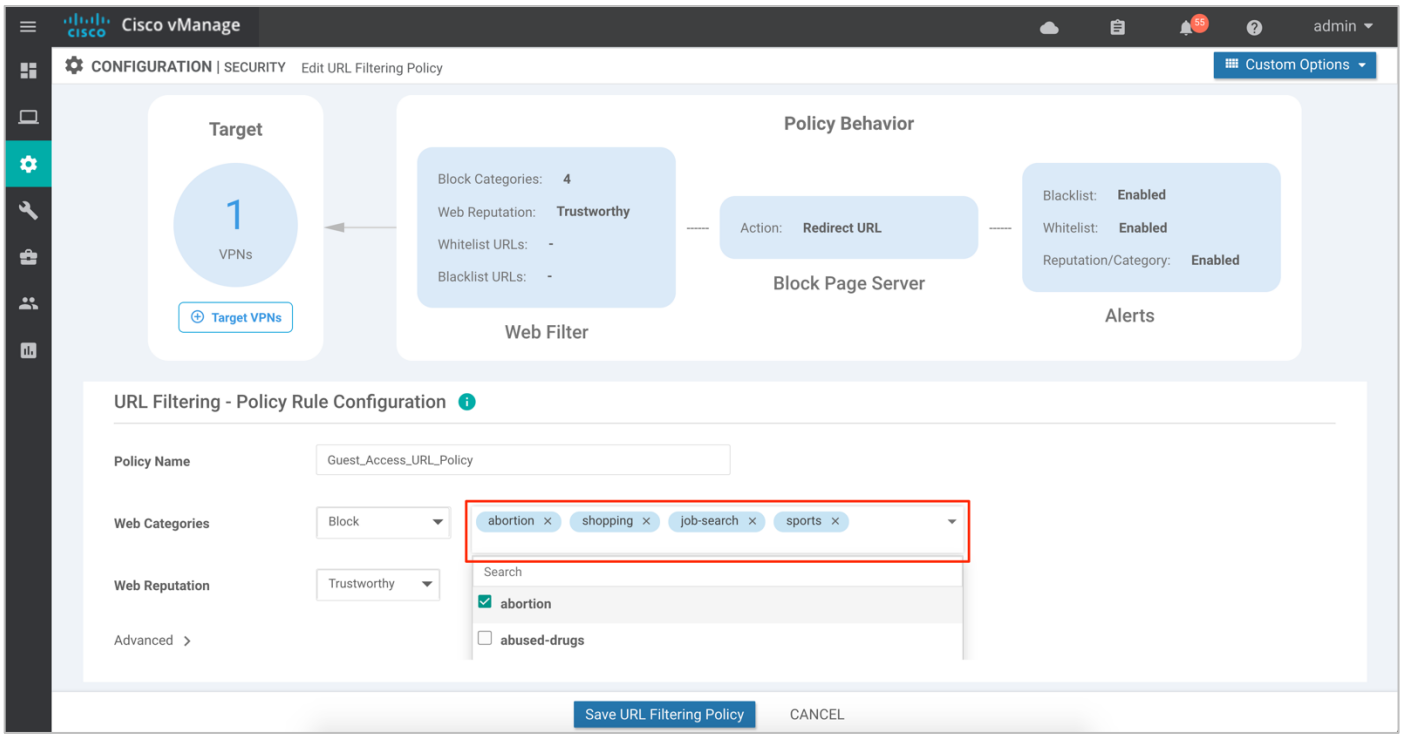
Step 3. Choose one of the following options from the **Web Categories** drop-down:

Block: To block websites that match the selected categories.

Allow: To allow websites that match the selected categories.



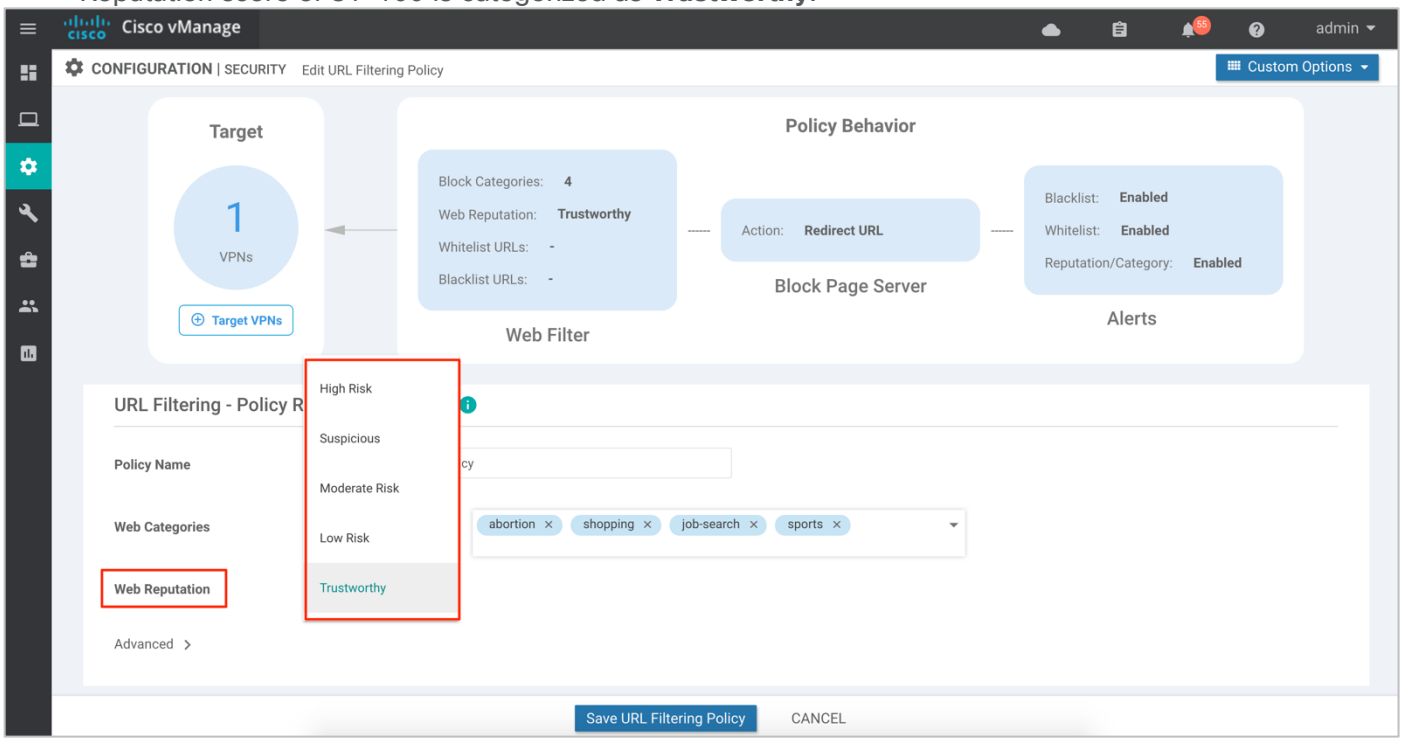
Step 4. Select one or more categories to block or allow from the **Web Categories list**. To understand the list of categories, refer to [Categories Data Sheet.]



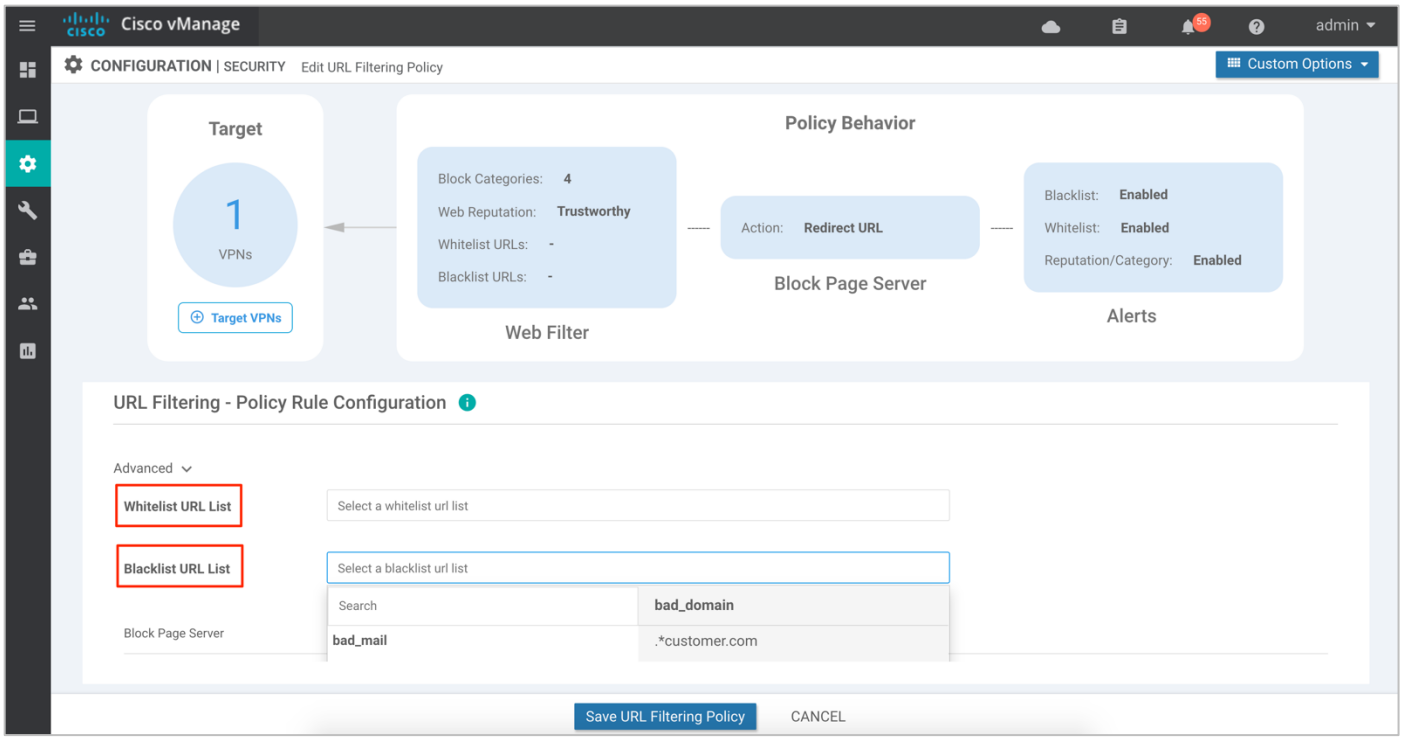
Step 5. Select a Web Reputation from the drop-down. The options are:

- Reputation score of 01-20 is categorized as **High Risk**.
- Reputation score of 21-40 is categorized as **Suspicious**.
- Reputation score of 41-60 is categorized as **Moderate Risk**.

- Reputation score of 61-80 is categorized as **Low Risk**.
- Reputation score of 81-100 is categorized as **Trustworthy**.

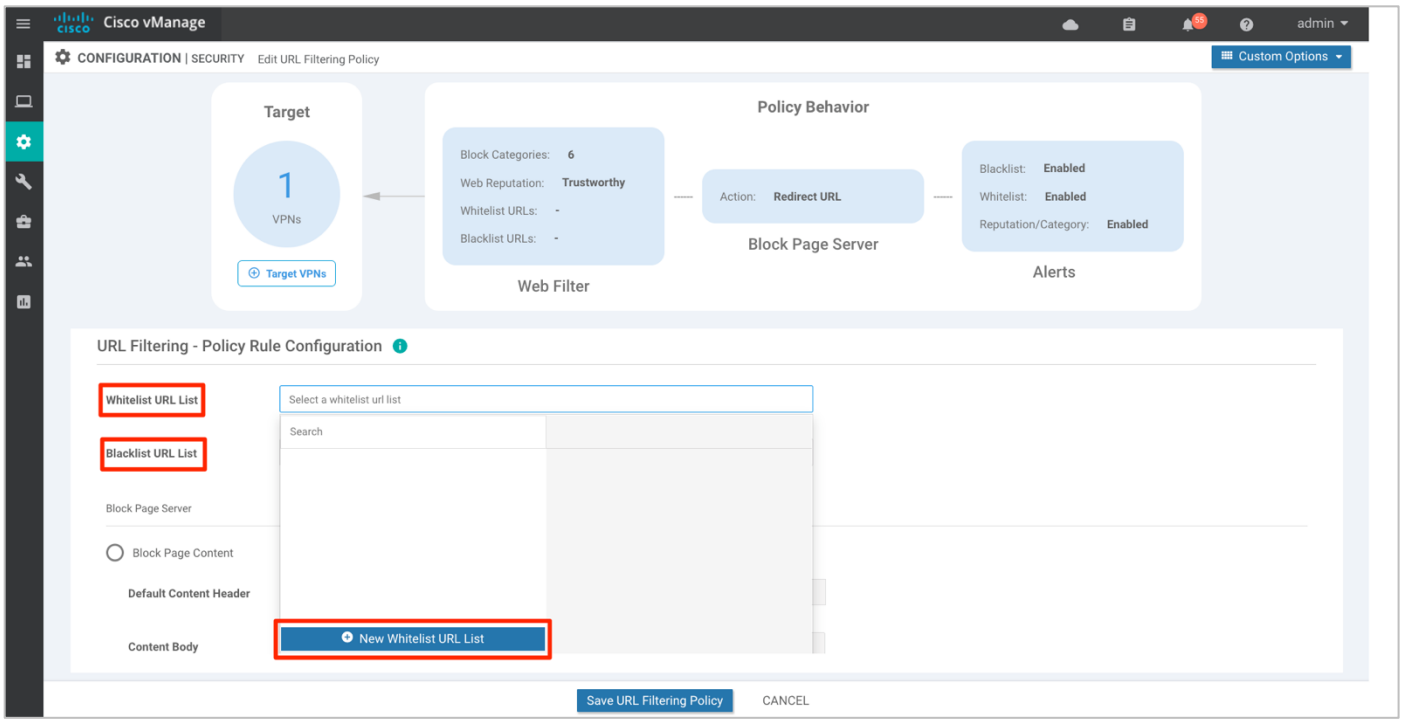


Step 6. (Optional) To whitelist or blacklist specific URLs or domains, click on the **Advanced** tab and within Whitelist/ Blacklist URL lists add in preconfigured URL lists or create new ones as needed.



Note: If you did not preconfigure URL Blacklists/ Whitelists you can create new URL lists, by following the steps below:

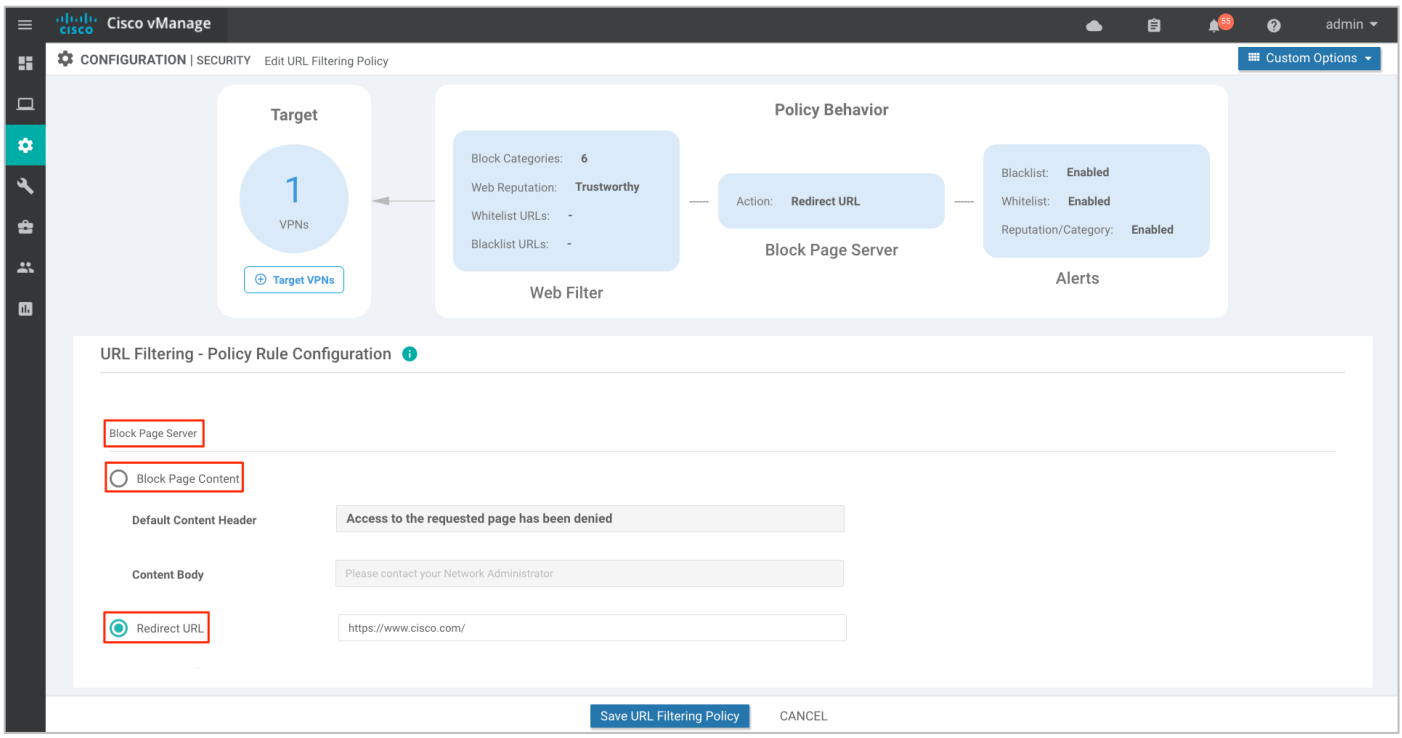
Click on +New Whitelist URL List or +New Blacklist URL List at the bottom of the drop-down and enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only), followed by entering the actual URL or domain in the following tab.



Step 7. (Optional) In the **Block Page Server** pane, choose an option to designate what happens when a user visits a URL that is blocked.

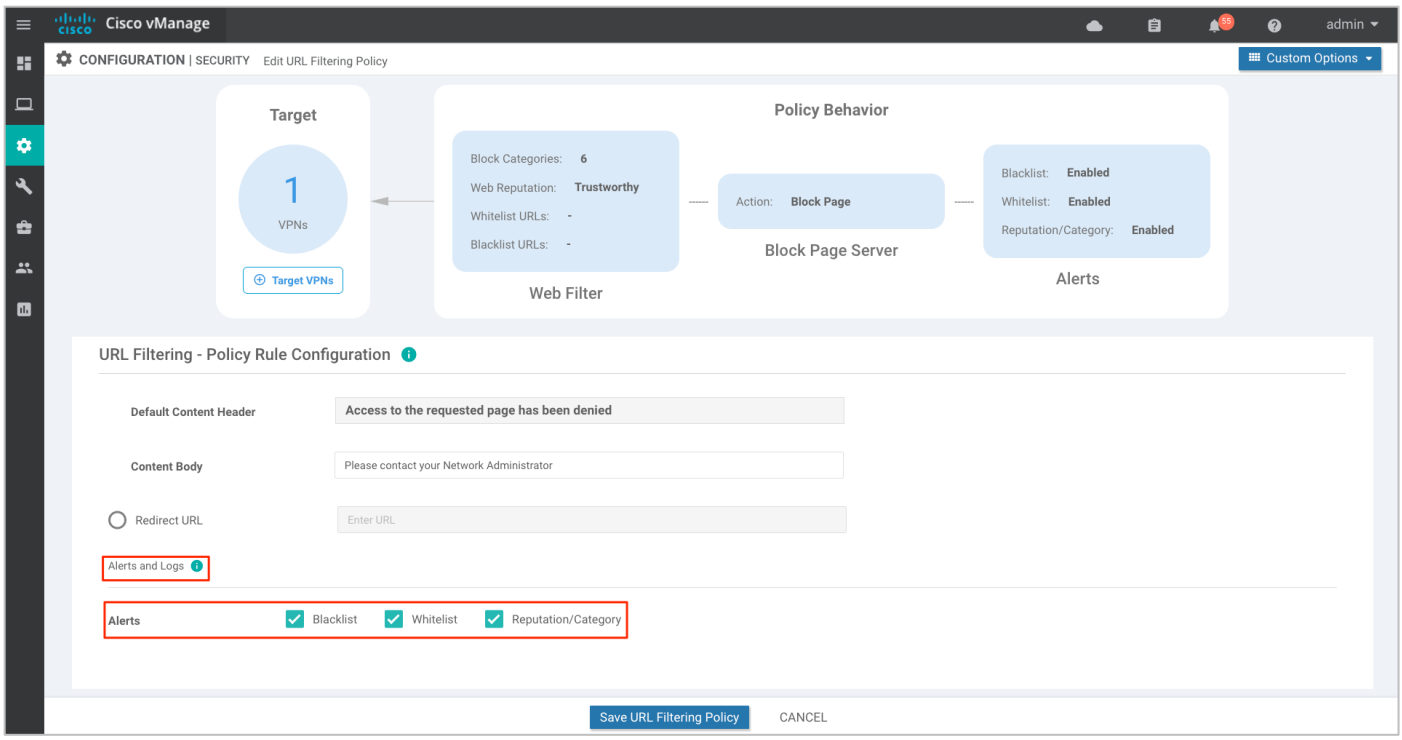
- **Block Page Content:** Choose this option to display a message that access to the page has been denied.
- **Redirect URL:** Choose the option to display another page.

If you choose **Block Page Content**, users see the content header "**Access to the requested page has been denied**" in the Content Body field, enter text to display under this content header. The default content body text is "**Please contact your Network Administrator**" If you choose the option **Redirect URL**, enter a URL to which users are redirected.

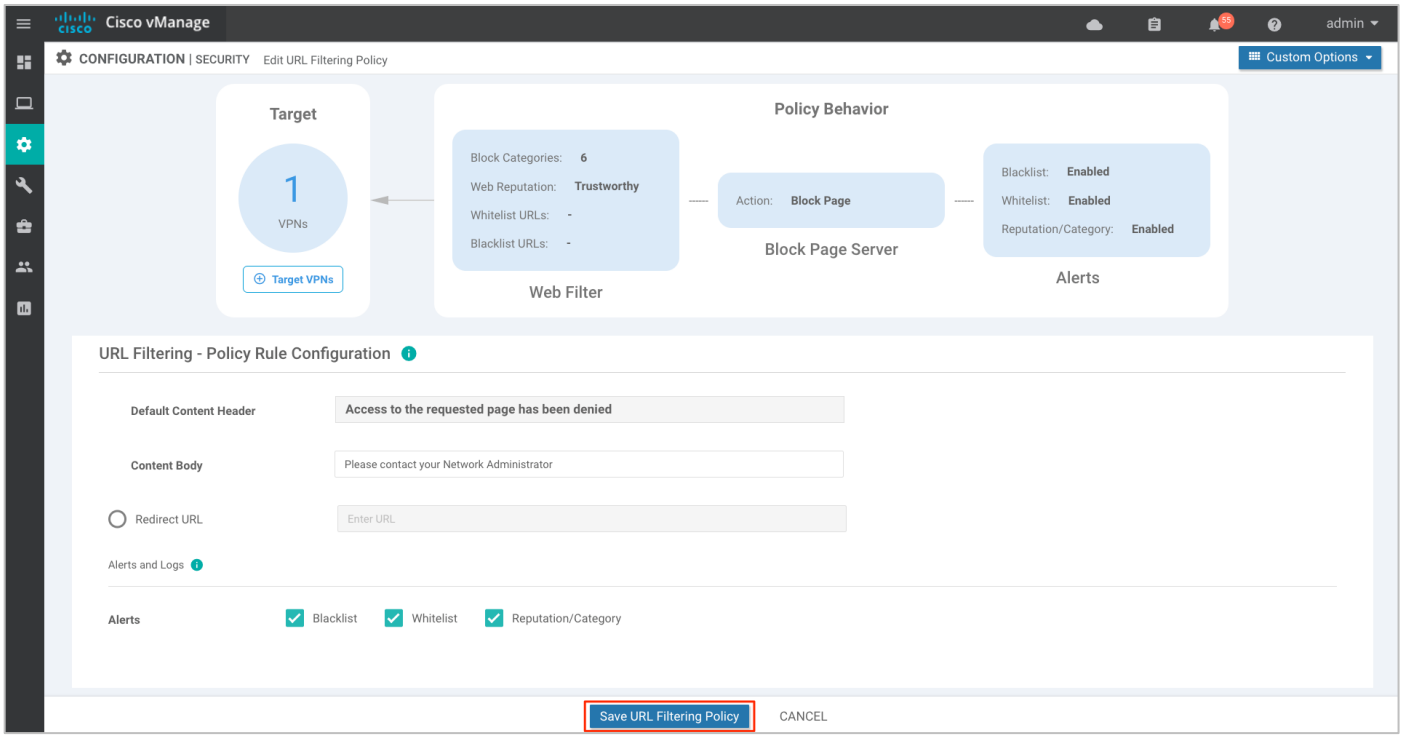


Step 8. (Optional) In the **Alerts and Logs** pane, select one of the following types of **Alerts**,

- Blacklist: Exports an alert as a syslog message if a user tries to access a URL that is configured in the Blacklist URL List.
- Whitelist: Exports an alert as a syslog message if a user tries to access a URL that is configured in the Whitelist URL List.
- Reputation/Category: Exports an alert as a syslog message if a user tries to access a URL that has a reputation that is configured in the Web Reputation field or that matches a blocked or allowed web category.

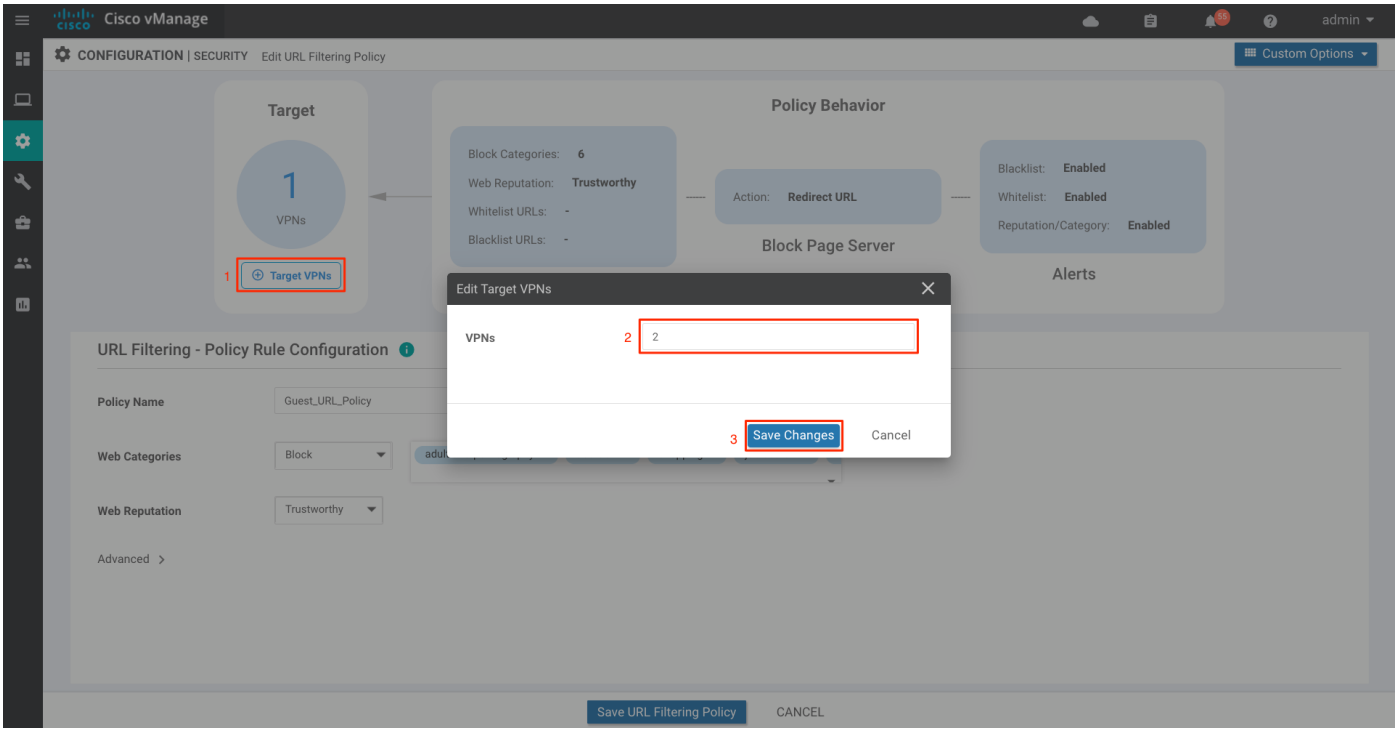


Step 9. Click **Save URL filtering Policy** to add a URL filtering policy.

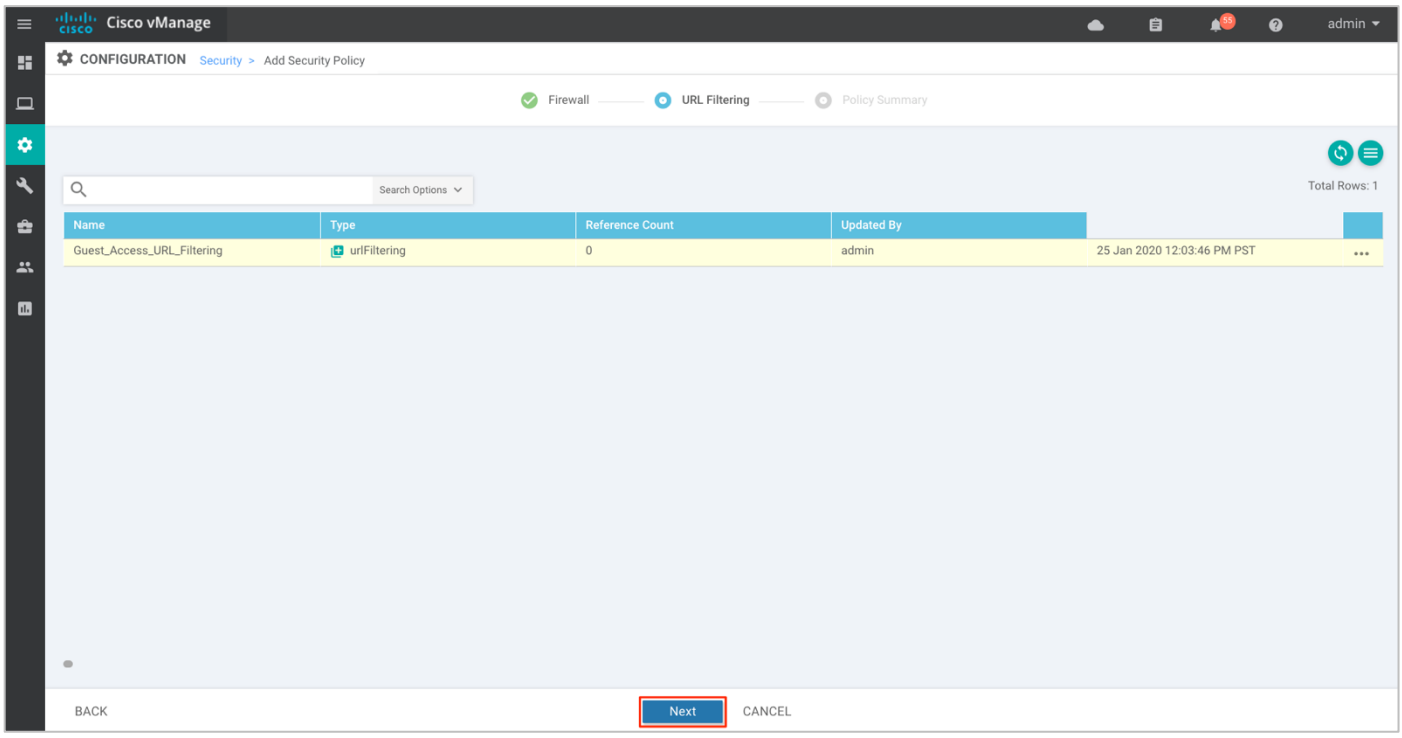


Step 10. Next, enter the VPNs affected by the policy. Within Target VPNs wizard, click on **Target VPNs** and enter the VPN number next to **VPNs** label.

If you wish to add more VPNs, separate each VPN with a comma. Finally, click on Save Changes and Save URL Filtering Policy.

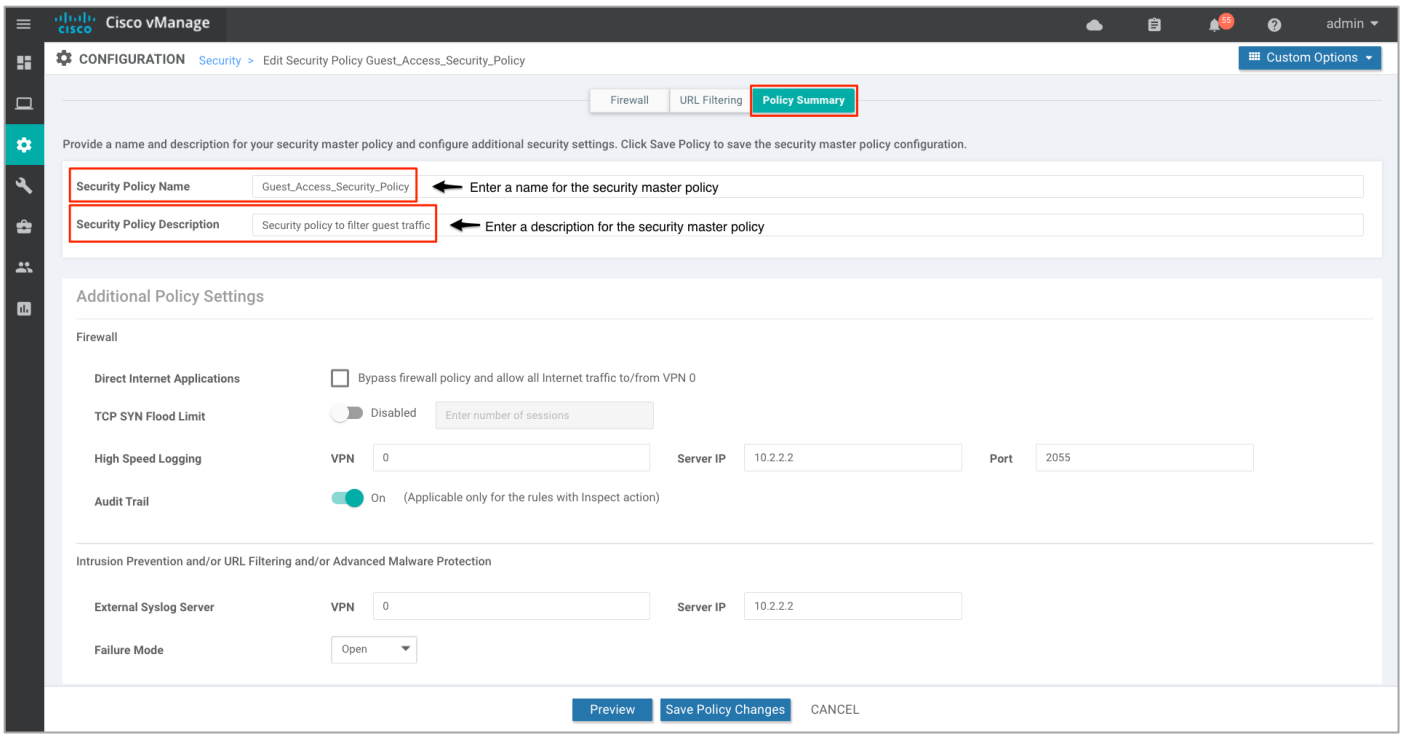


Step 11. Click **Next** to configure the master security policy.



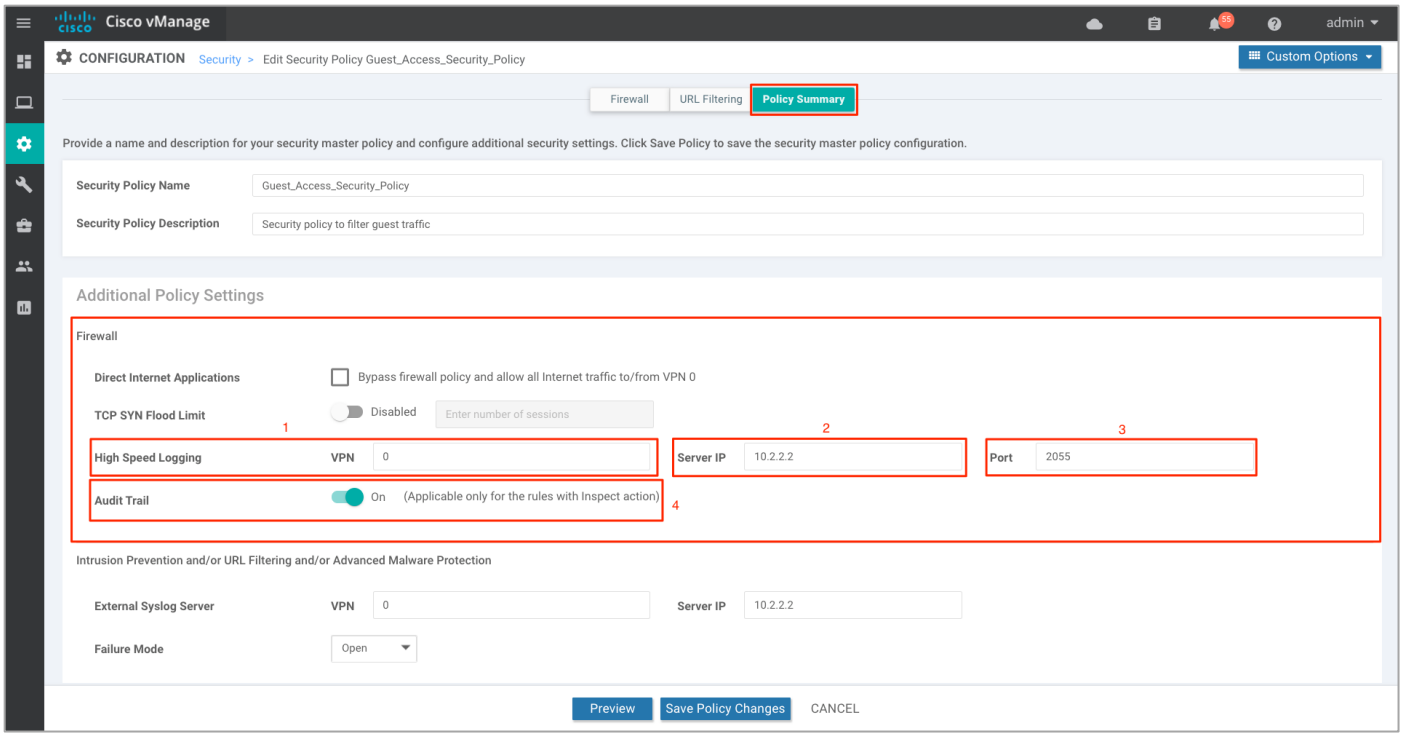
Procedure 3. Configure Policy Summary

Step 1. Within **Policy Summary**, provide a name and description for your security master policy.

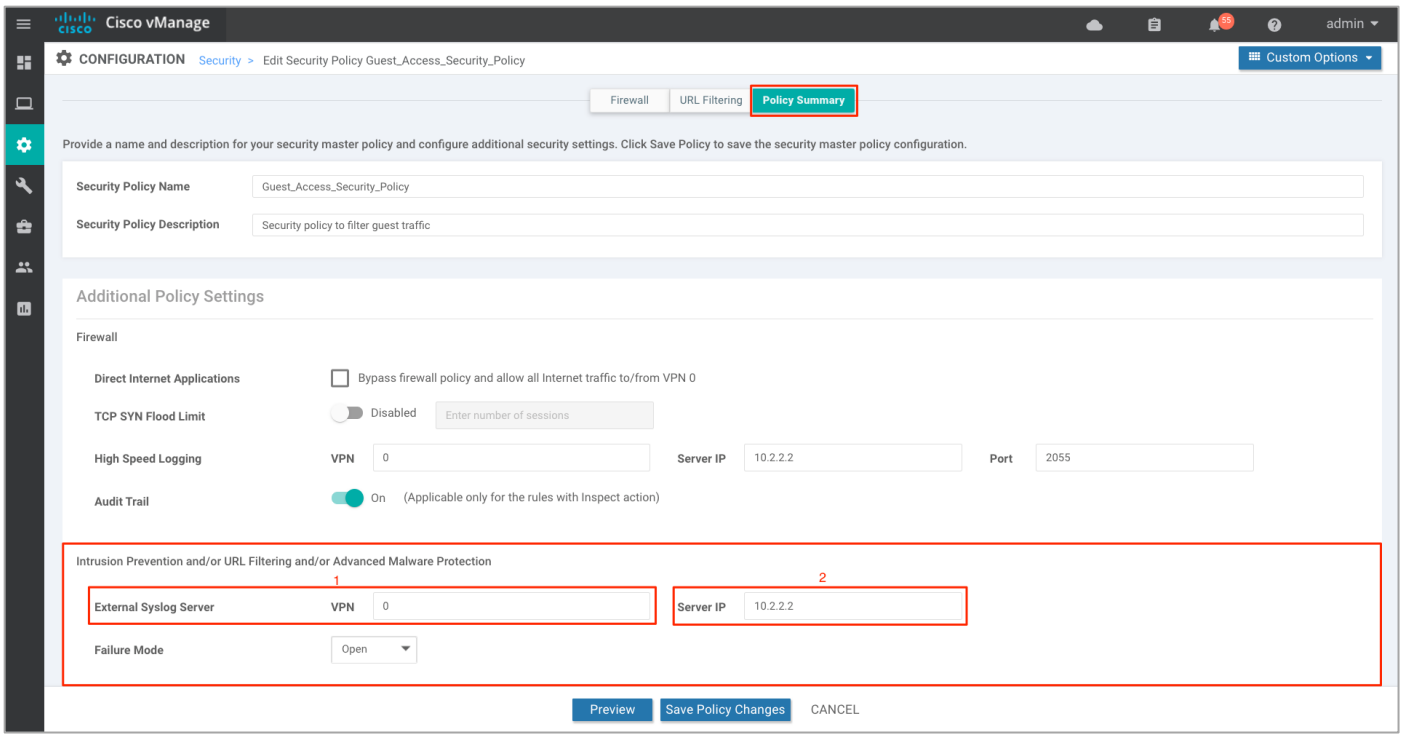


Step 2. To log firewall packets that flow through routing devices (similar to the NetFlow Version 9 records) to an external collector enable **High Speed Logging** and enable **Audit Trail** to record the start, stop, and duration of a connection or session, and the source and destination IP addresses.

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.



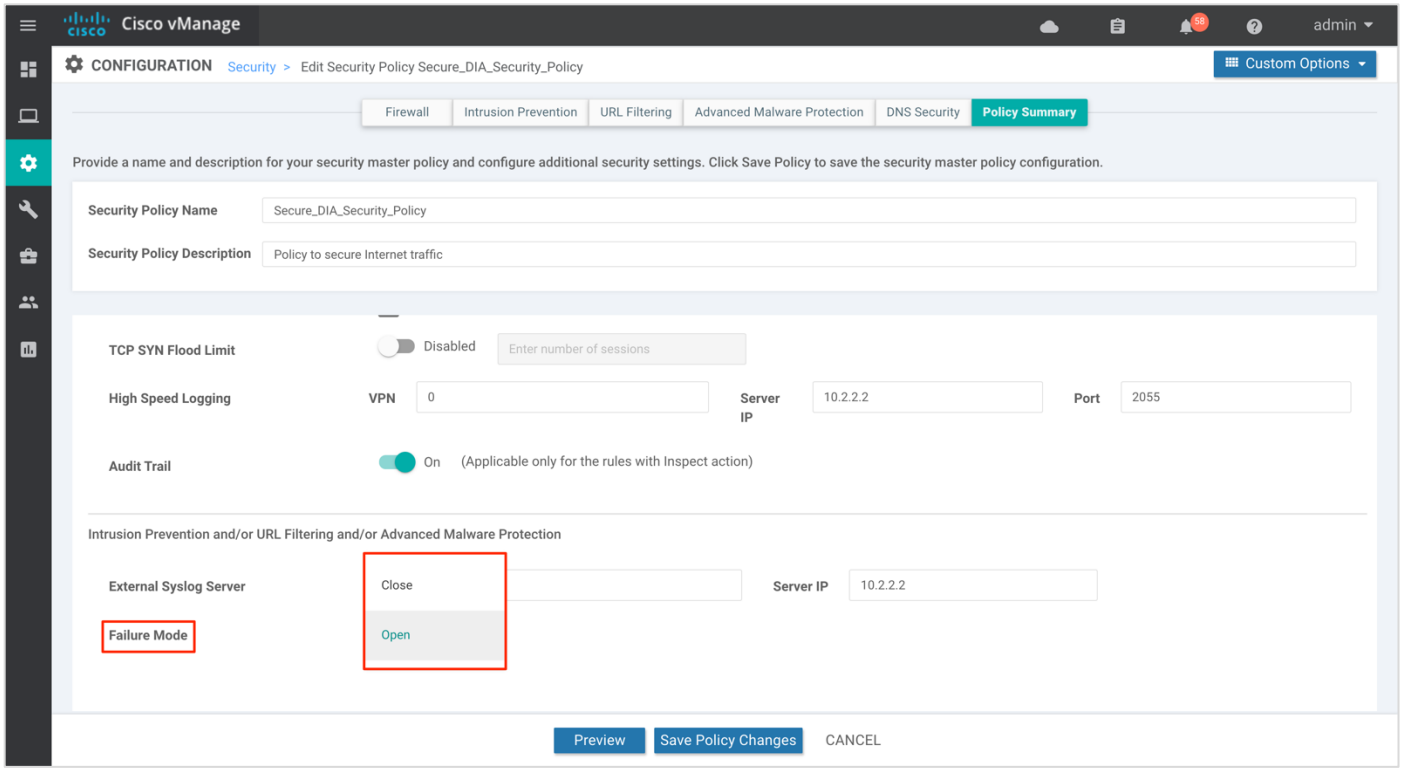
Step 3. Under the **Intrusion Prevention/ URL Filtering/ Advanced Malware Protection** section, you can fill in details to send URL syslogs to your **External Syslog Server**. Here, the **External Syslog Server** is set within VPN 0, hence the **VPN** label in **VPN** tab is **0**, followed by Server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



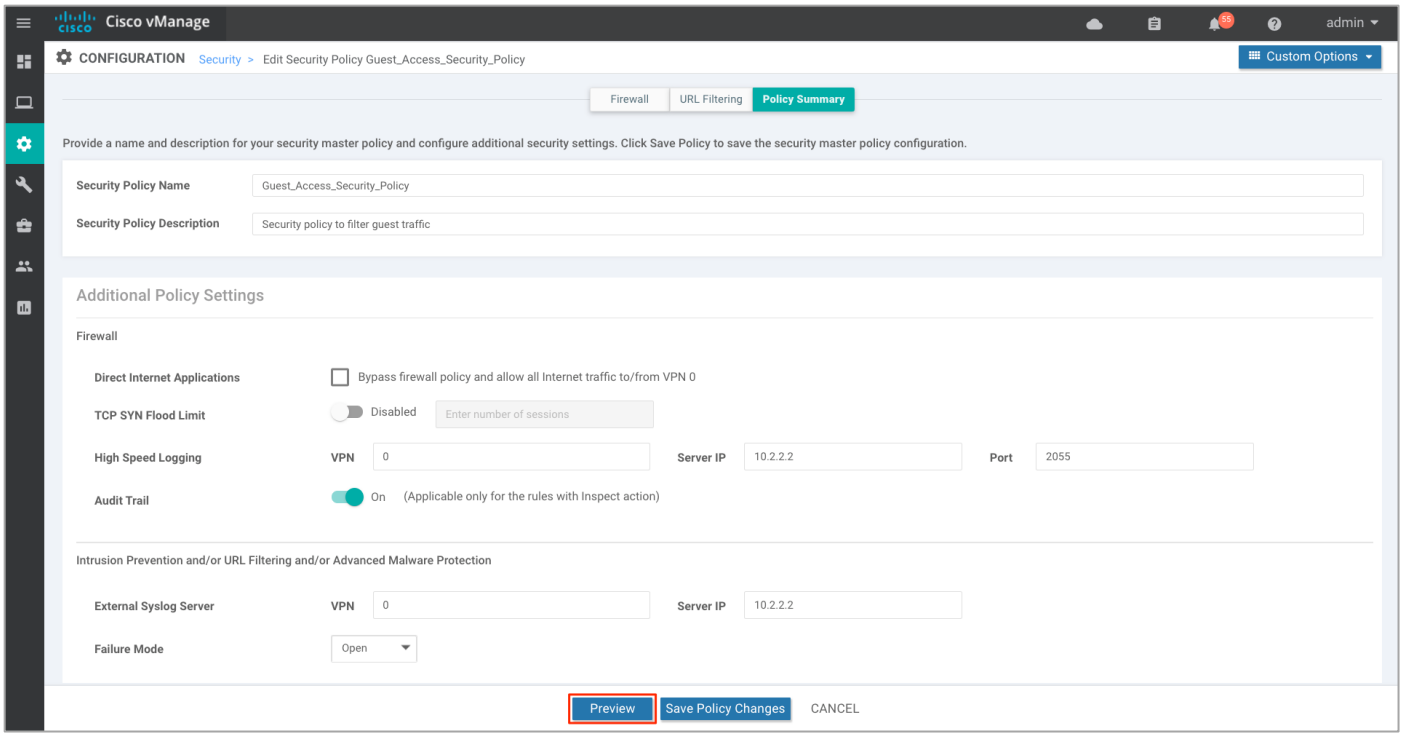
Step 4. Set the **Failure Mode** to either **Open** or **Close**.

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.

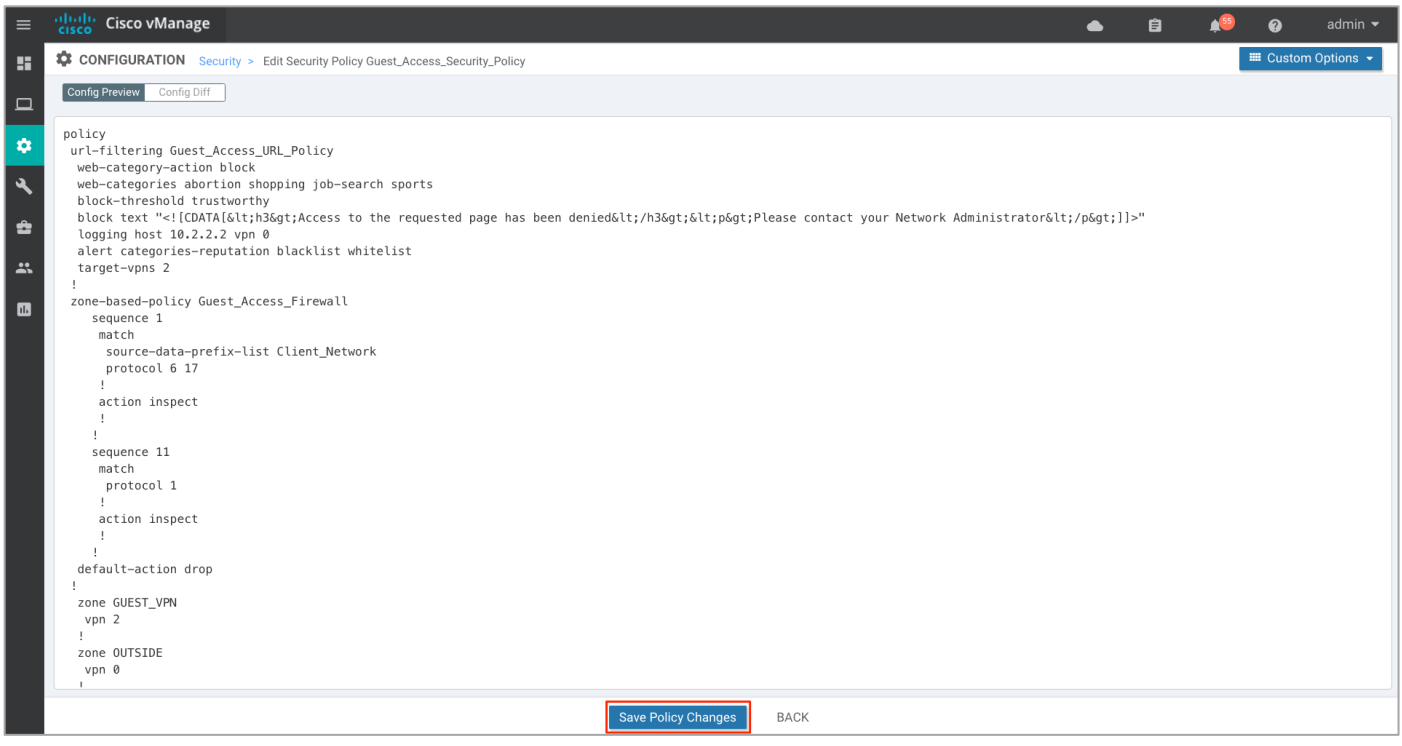
Enable fail-close, if security is the concern and select the option fail-open, only if connectivity is the concern. Select one among the two based on the design. For more details, refer to the [Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices].



Step 5. Click on **Preview** to view the CLI equivalent for the policy to be deployed.



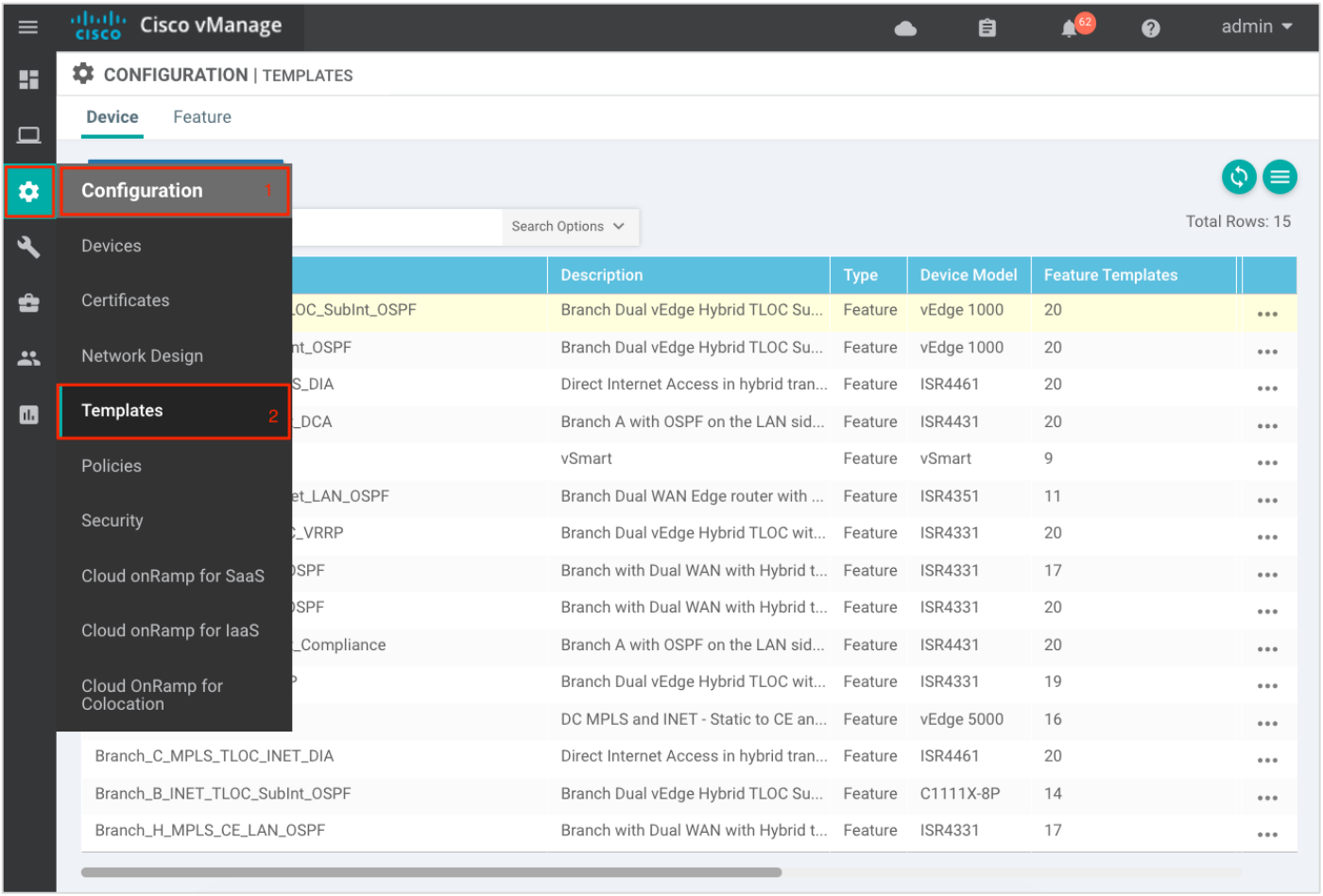
Step 6. Finally, click Save Policy Changes.



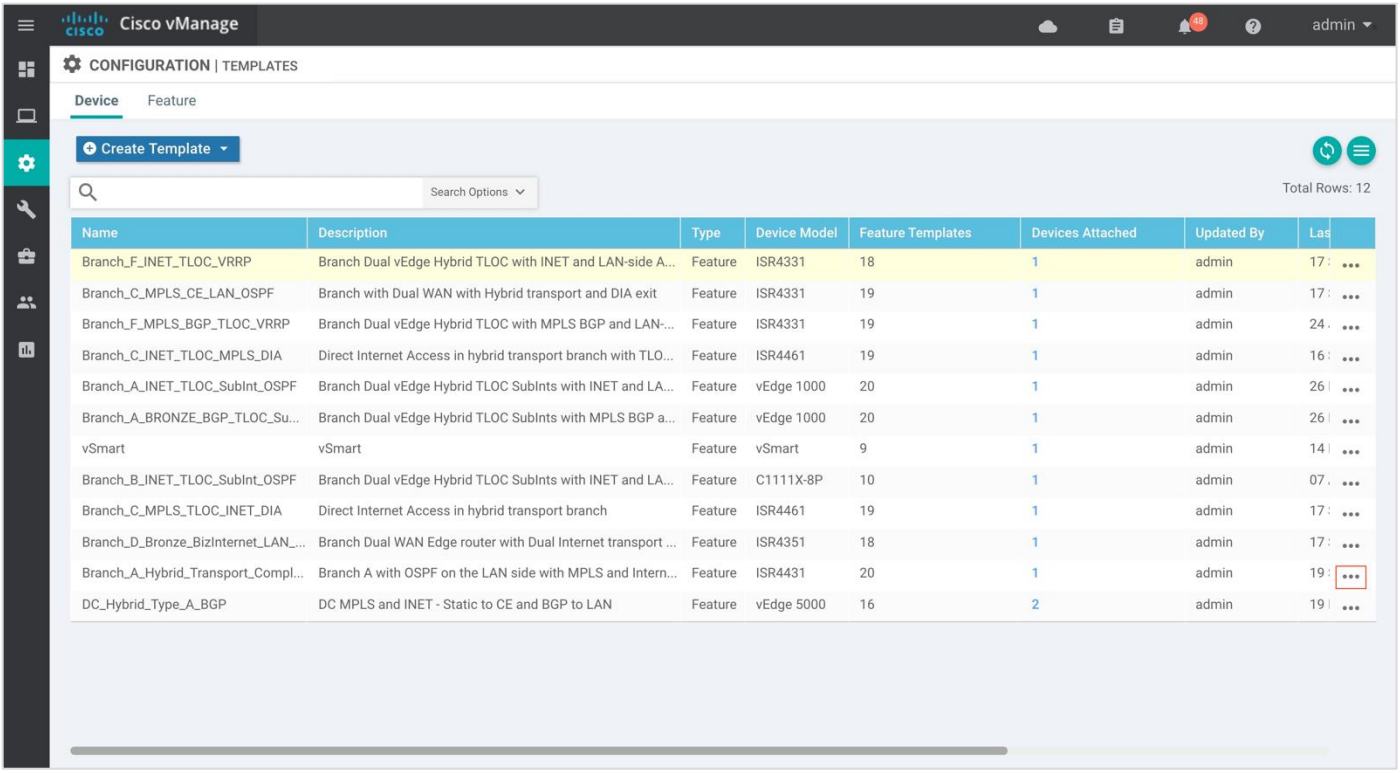
Process 3: Attach the Security Policy to the Device Template.

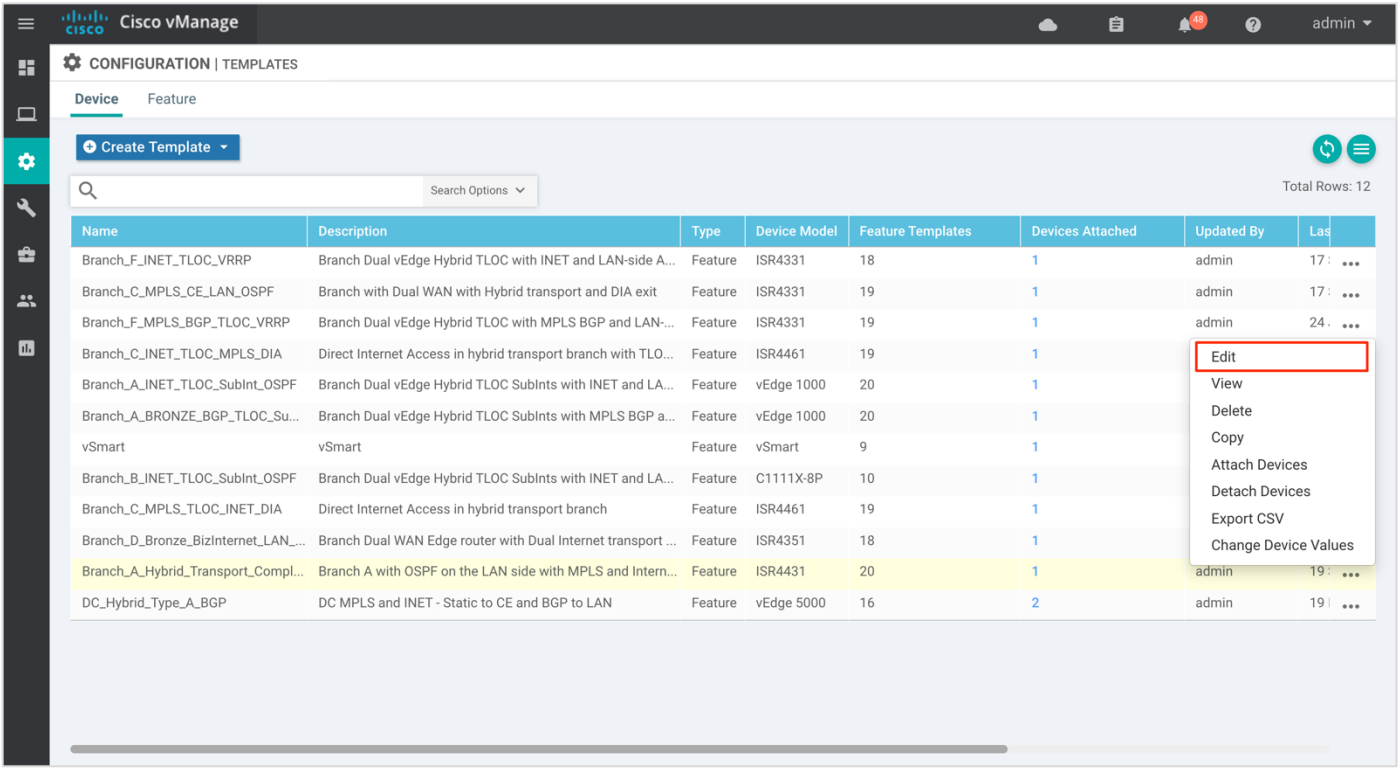
To apply the configured security policy to a remote-site WAN Edge device, follow the steps listed below.

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

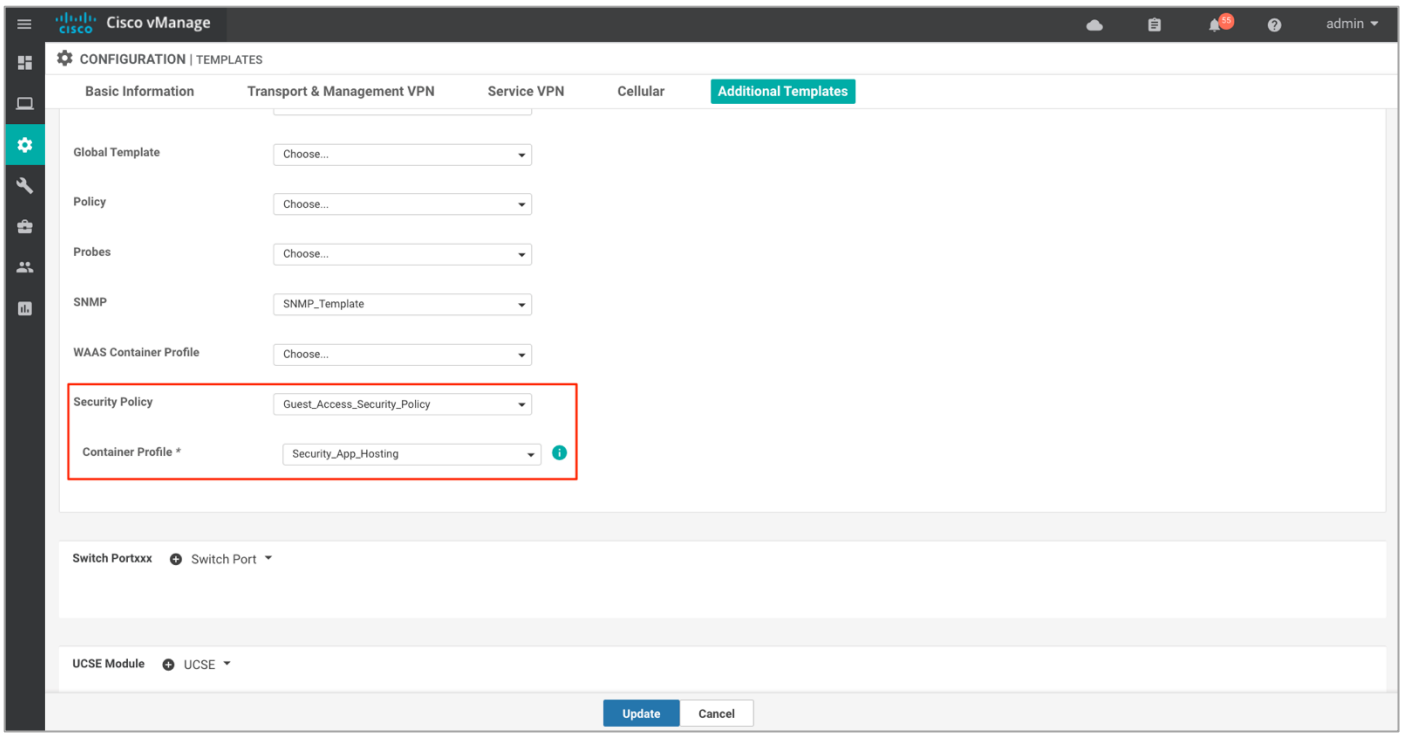


Step 2. To attach the security policy to a **Device Template**, click on the **three dots** found on the right side of the template and select **Edit** from the drop-down options.

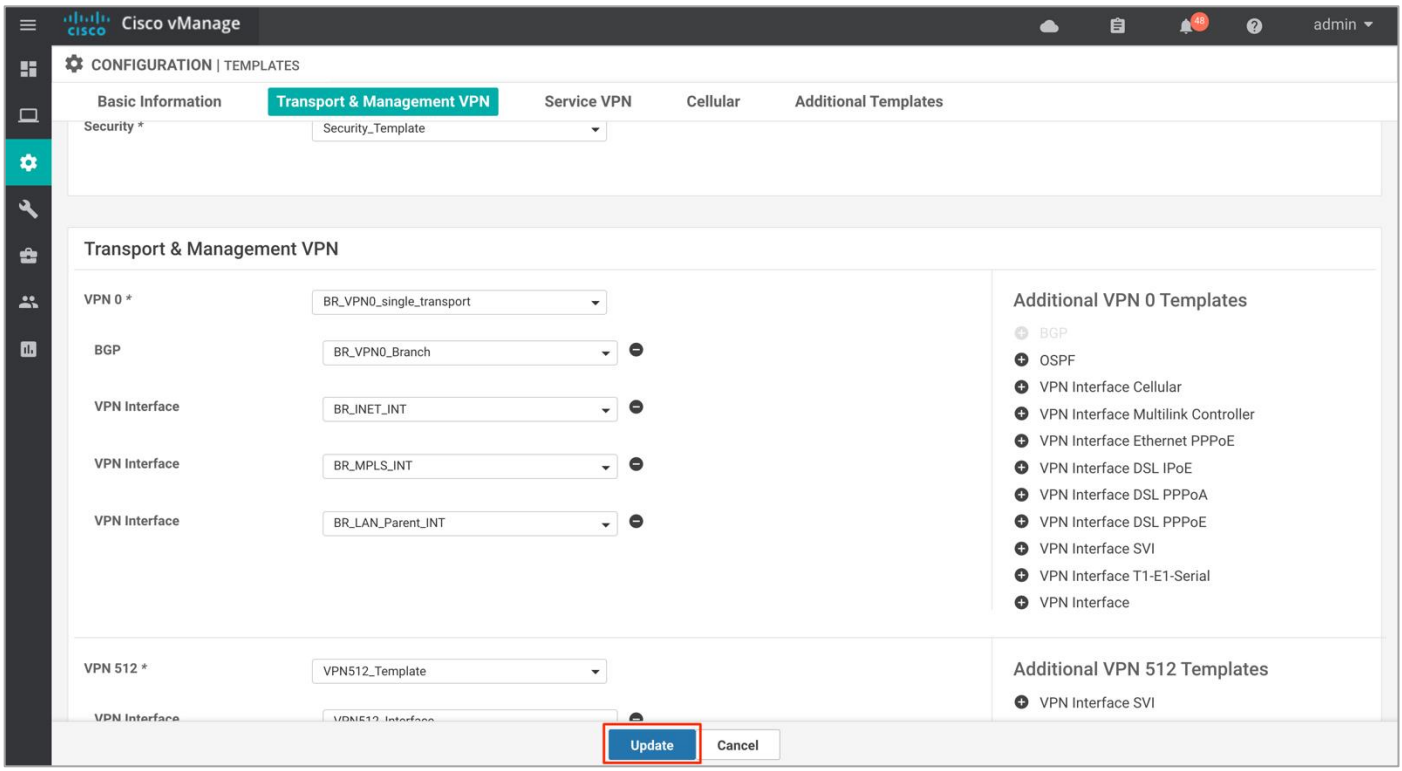




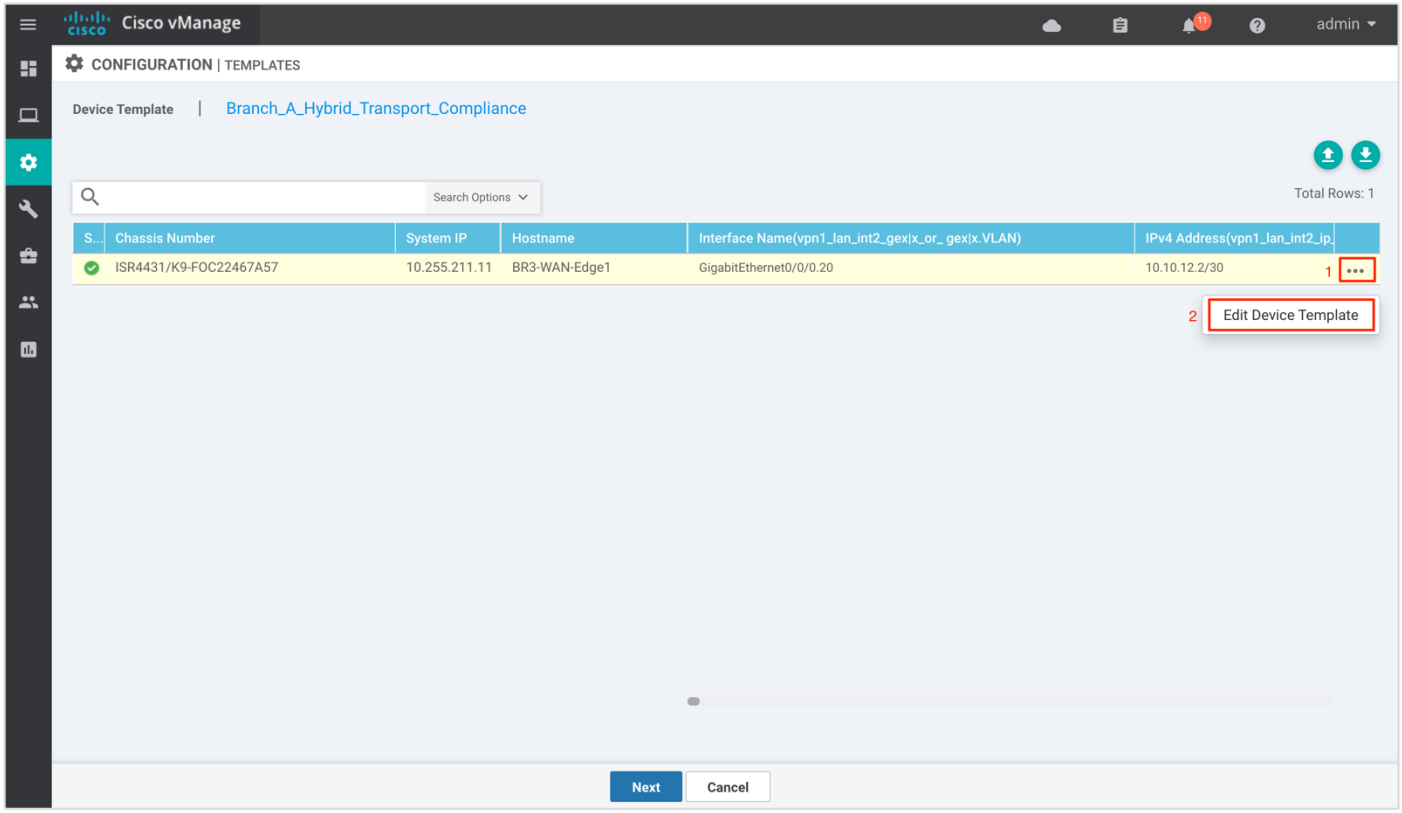
Step 3. Within the Device Template, navigate to Additional Templates and attach the **Security Policy** (**Guest_Access_Security_Policy**), along with the **Container Profile*** (**Security_App_Hosting**).

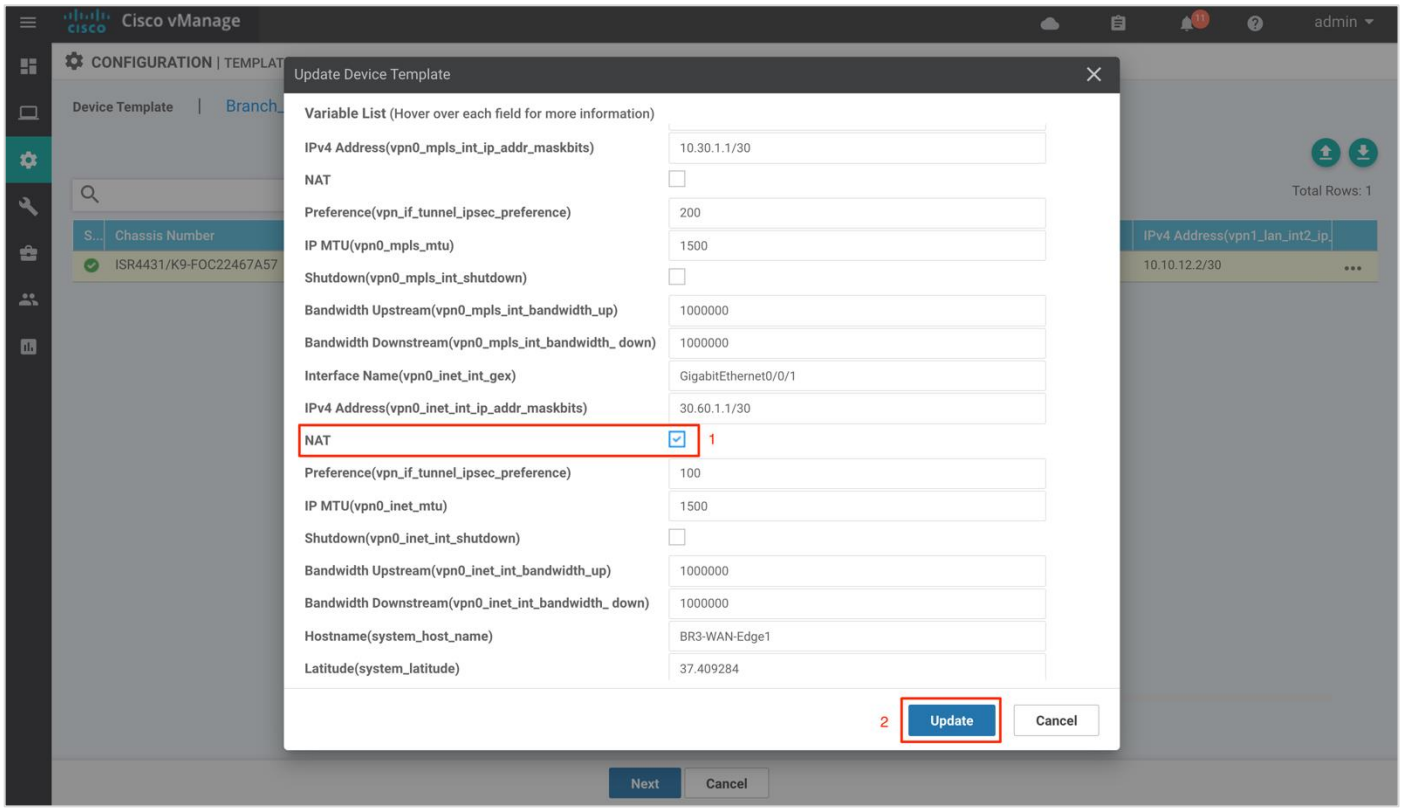


Step 4. Click **Update** to update the device template.



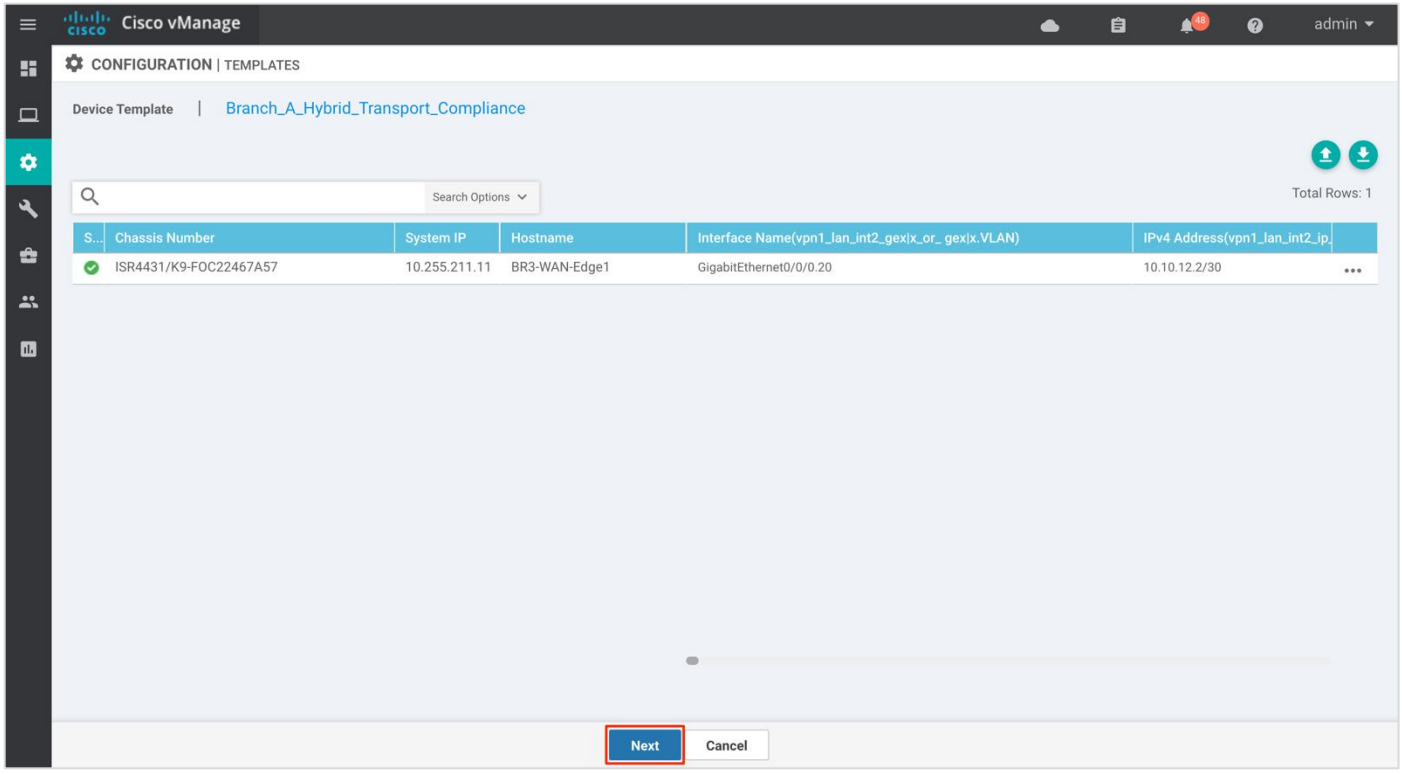
Step 5. Make sure **NAT** is already configured on the WAN Internet transport Interface. To do so click on the three dots and select **Edit**.



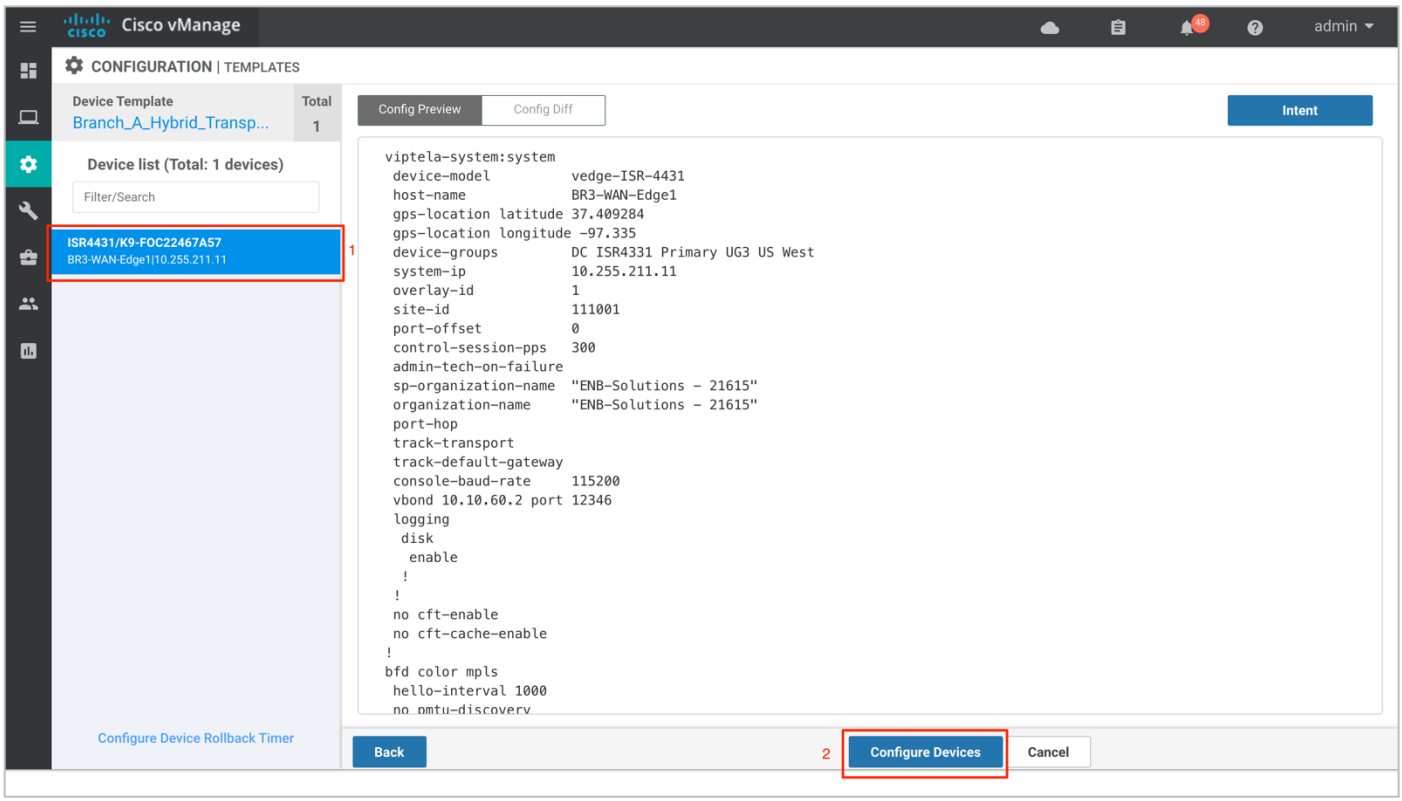


Note: If NAT feature is not currently configured as a variable in your interface feature template, you will need to modify the **WAN Interface Feature Template** to enable **NAT**. You can do this before or after deploying the security policy.

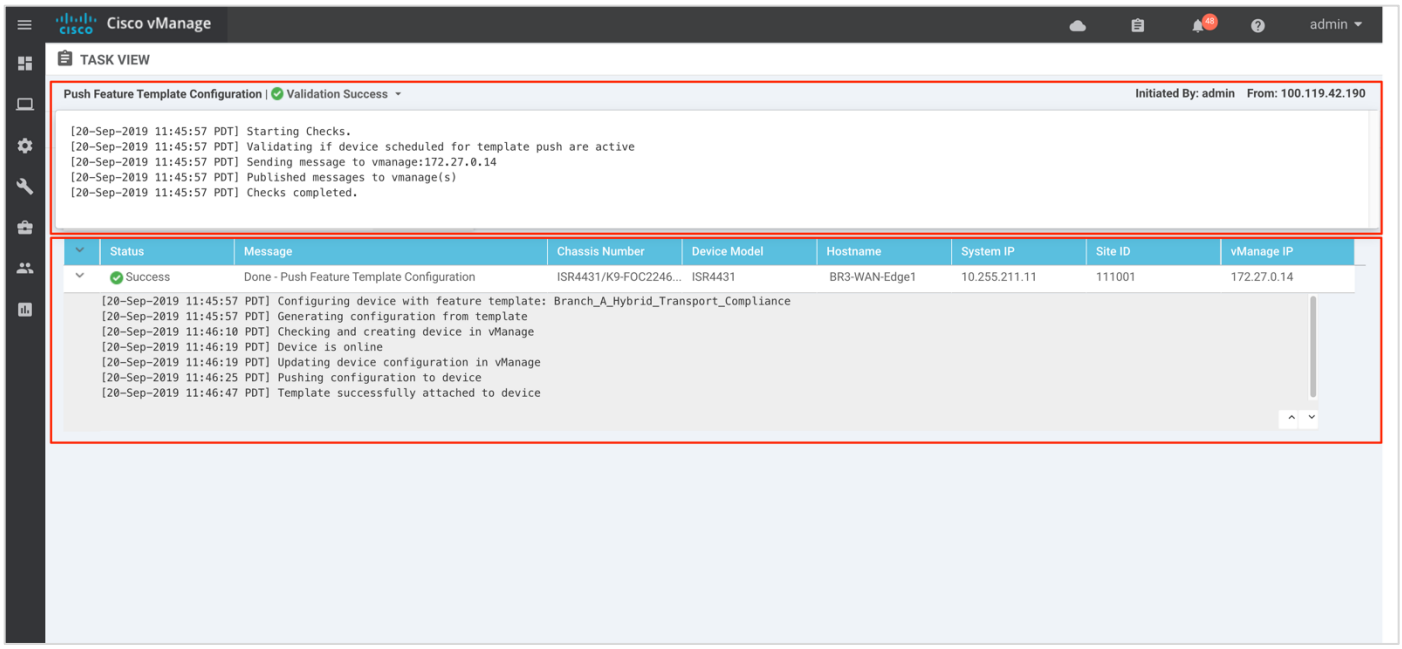
Step 6. Once, the changes are made click **Next**.



Step 7. 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.



Step 8. 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.



Operate - Cisco SD-WAN Secure Guest 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 and URL categories allowed, and dropped.

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.

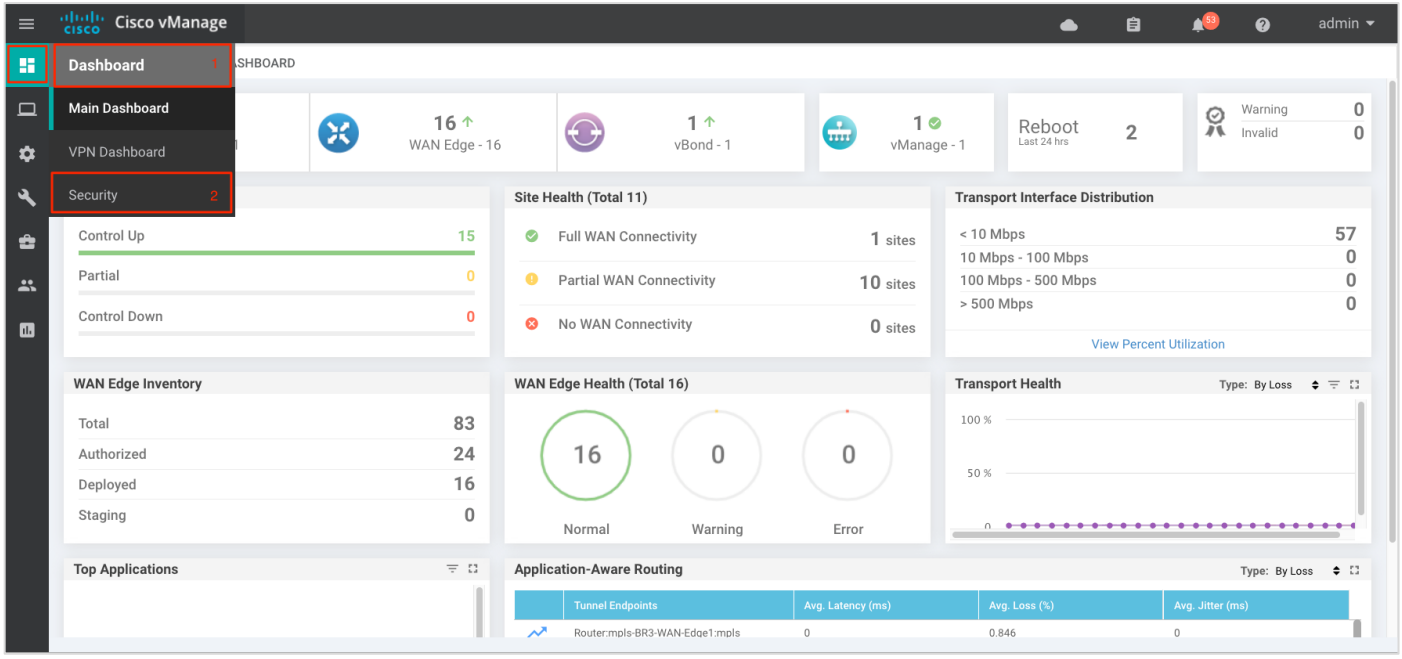
Process 1: Monitor the Enterprise Firewall with Application Awareness Feature via vManage NMS

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

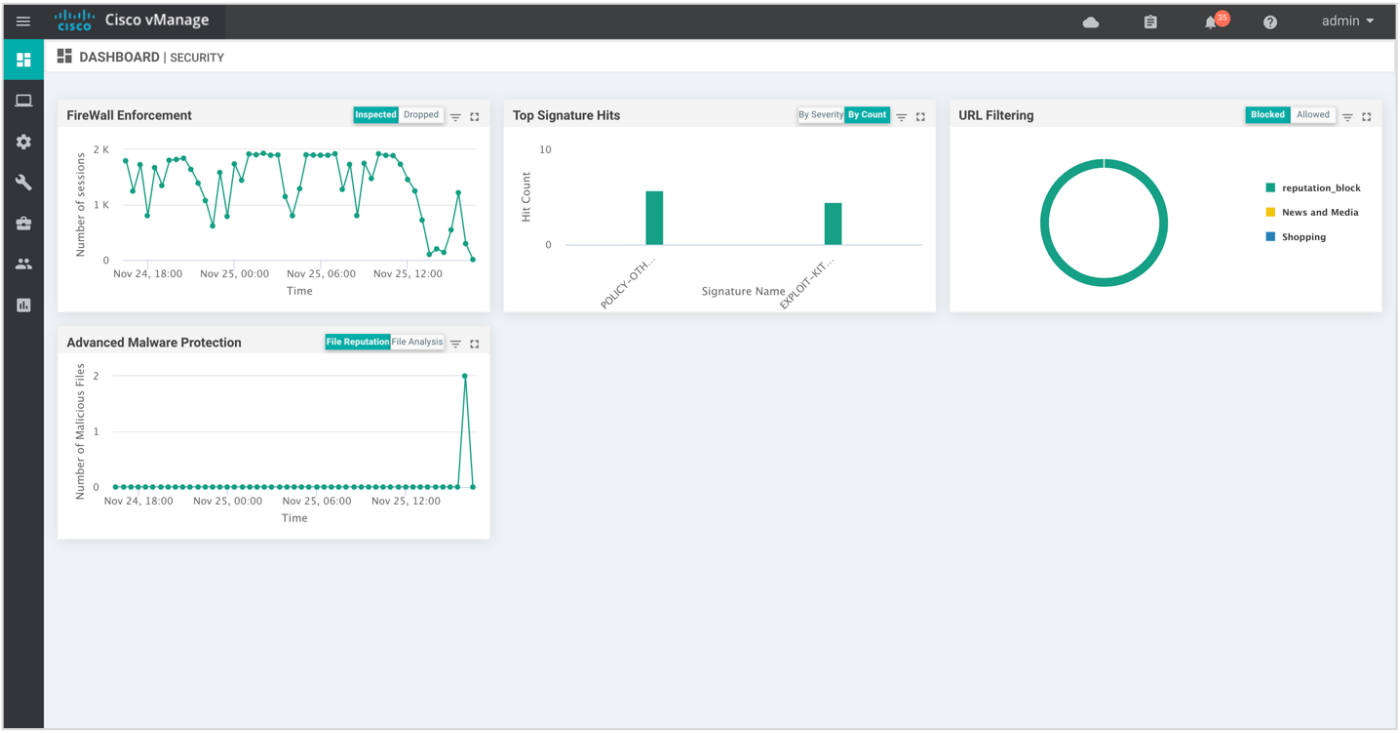
Procedure 1. Monitor the Firewall Feature via vManage Main Dashboard

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

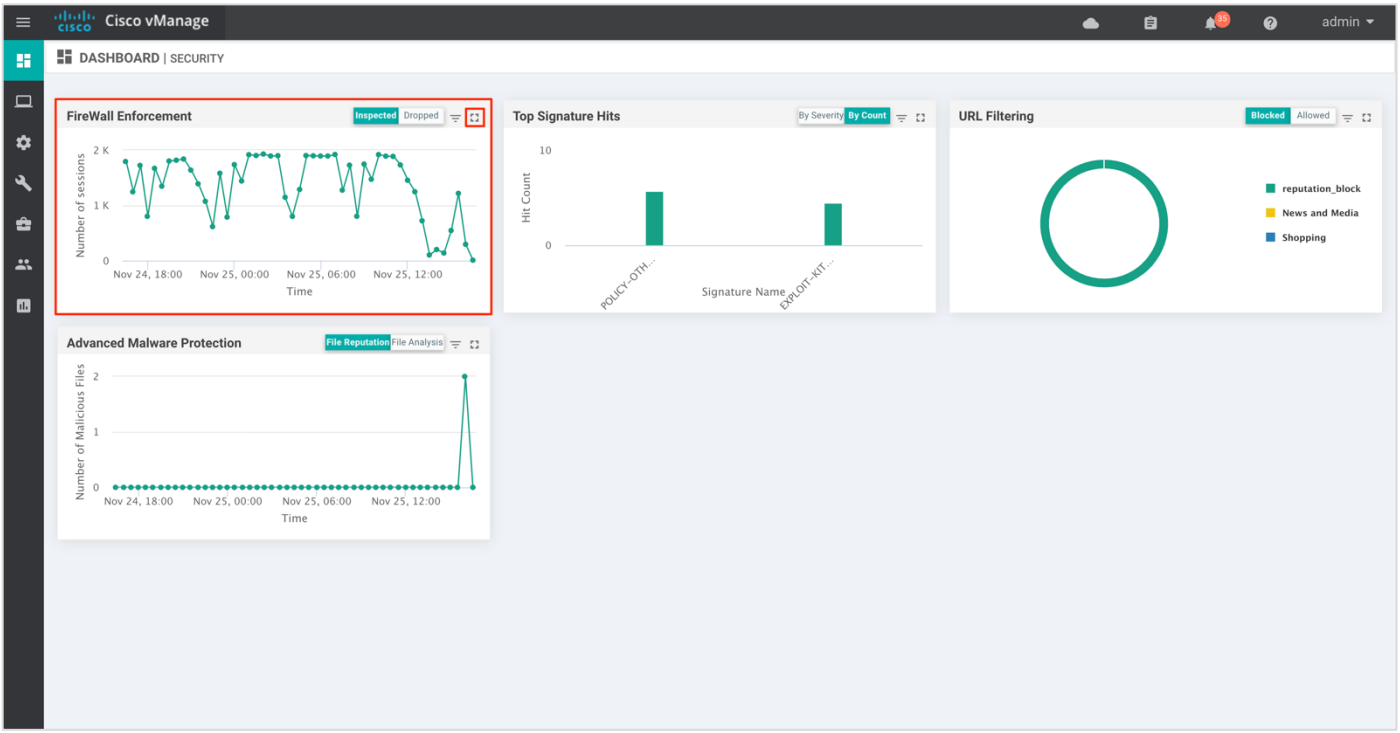
Step 1. Navigate to **Dashboard** > **Security**.



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

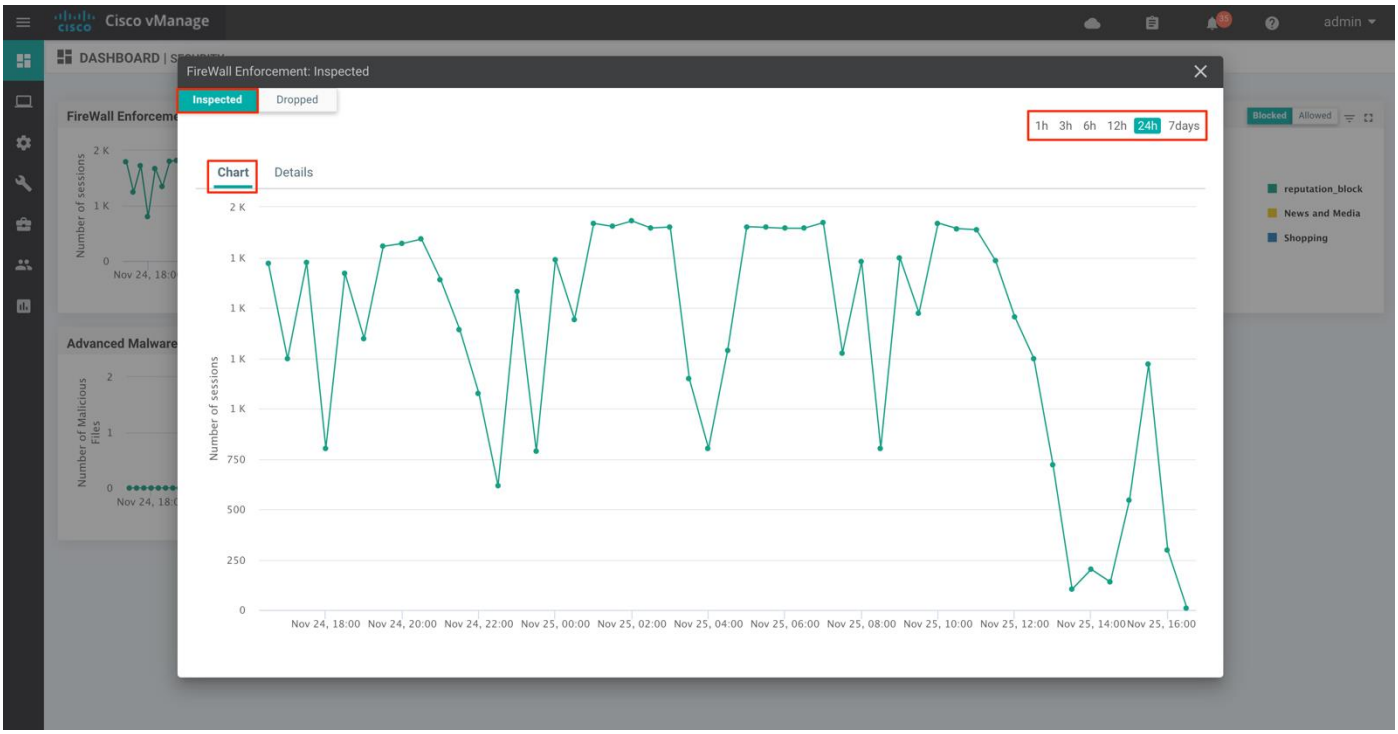


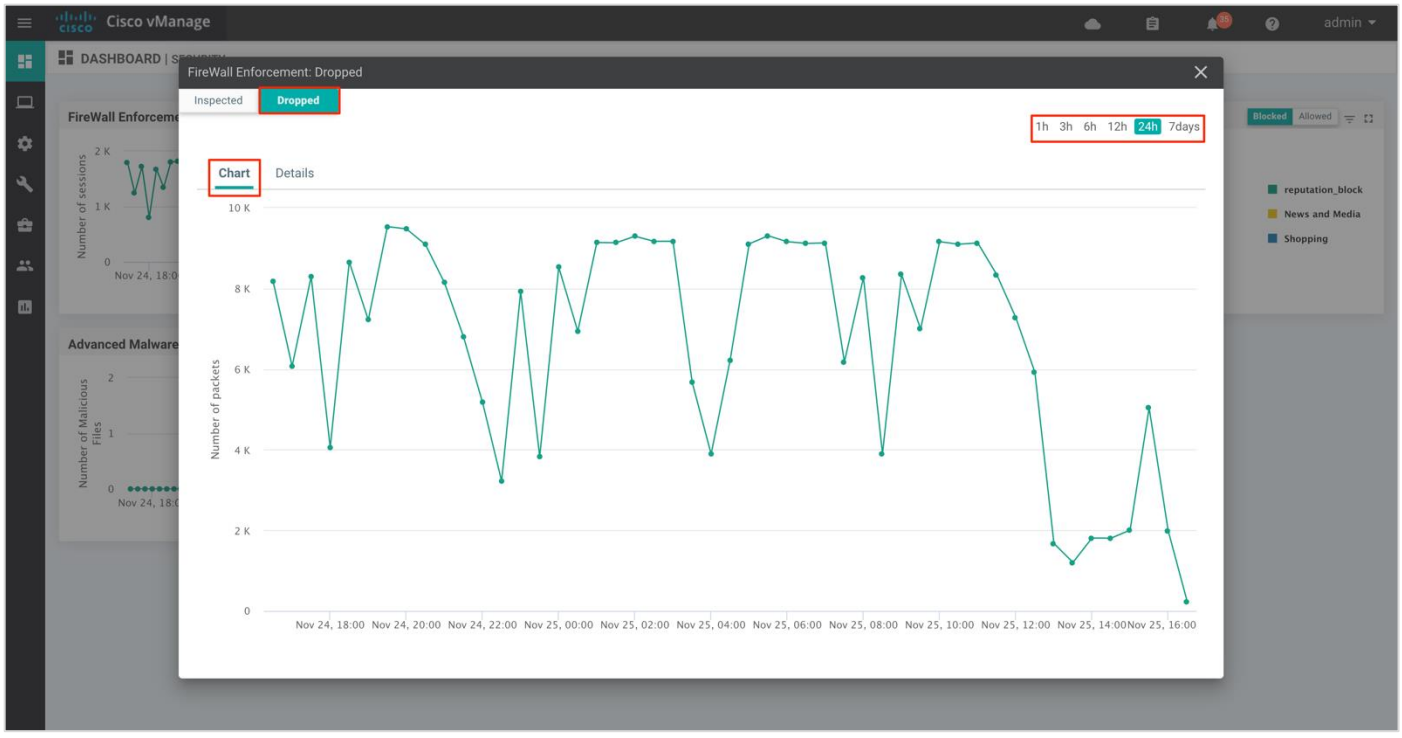
Step 3. To take a closer look into the **Firewall Enforcement** graph, click on the **square box []** on the top right.



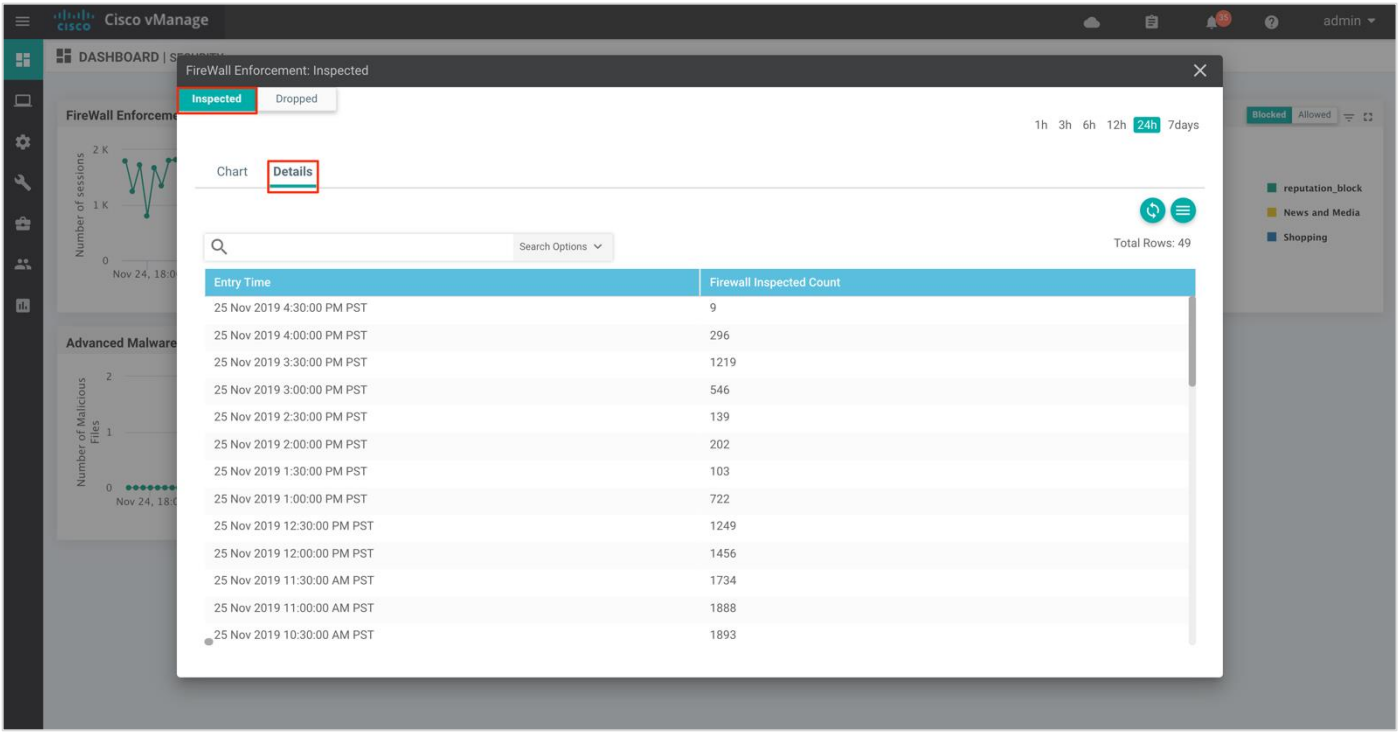
Step 4. Drilling down into the graph provides more information. Toggle between inspected and dropped packets and click on **1h, 3h, 6h, 12h, 24h (default)** or **7 days** to view the hourly, daily or weekly firewall statistics.

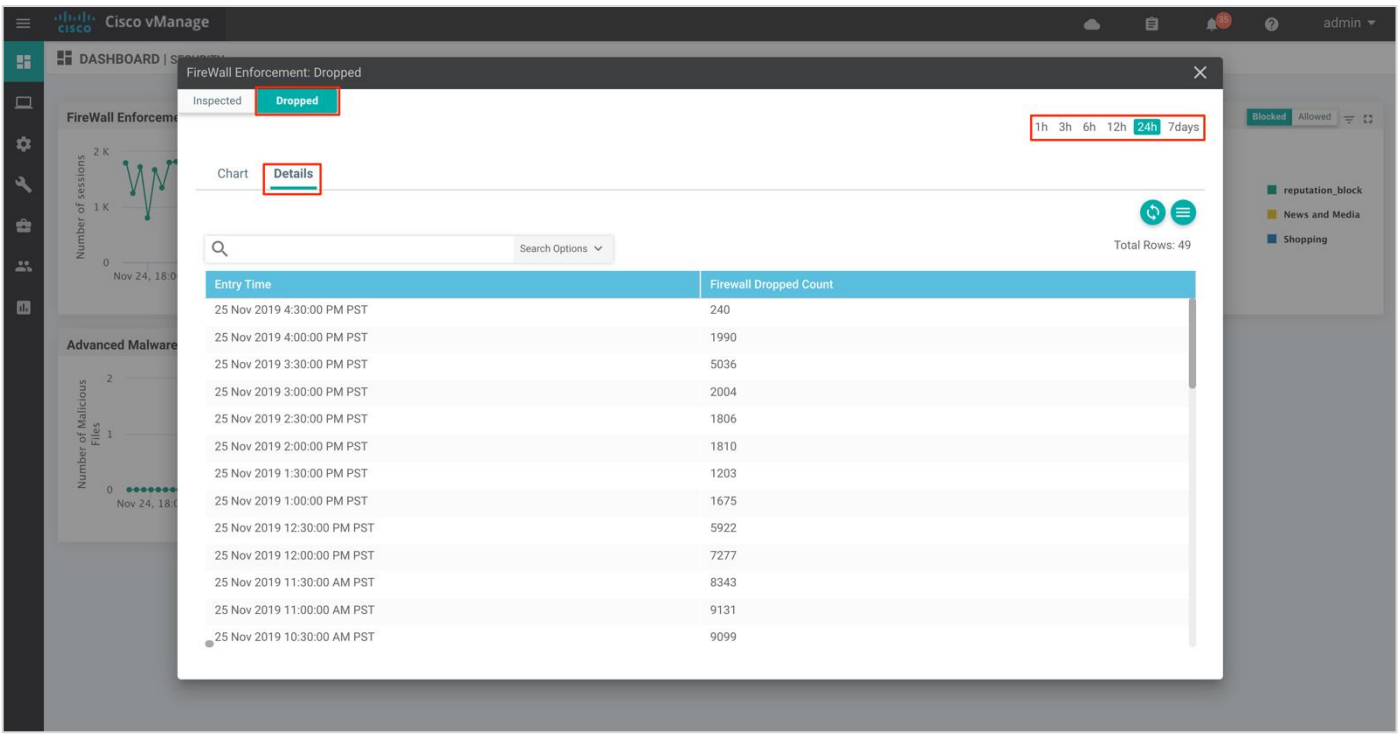
Chart displays the graphical representation of the firewall statistics for both traffic inspected and traffic dropped.





Details displays the **Firewall Inspected/Dropped Count**.





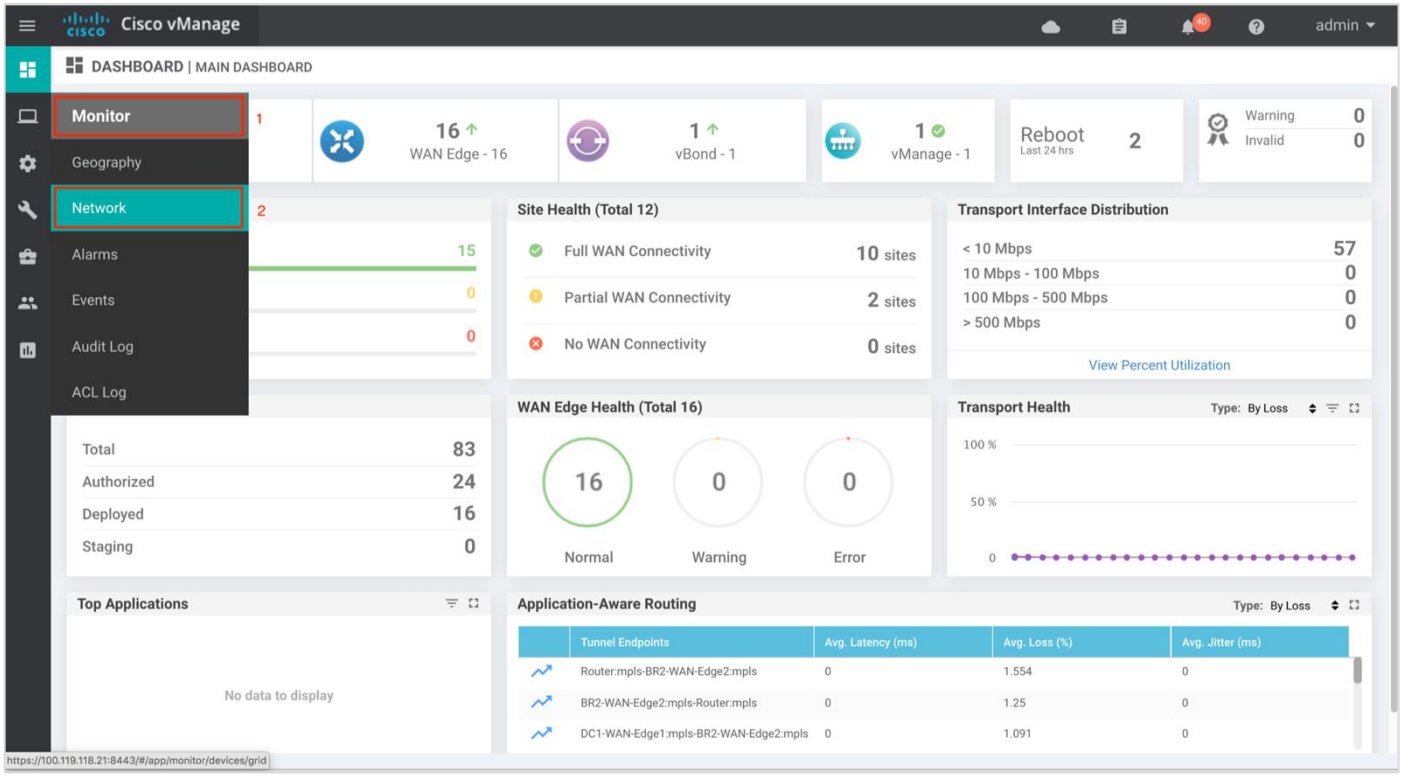
Technical Tip

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

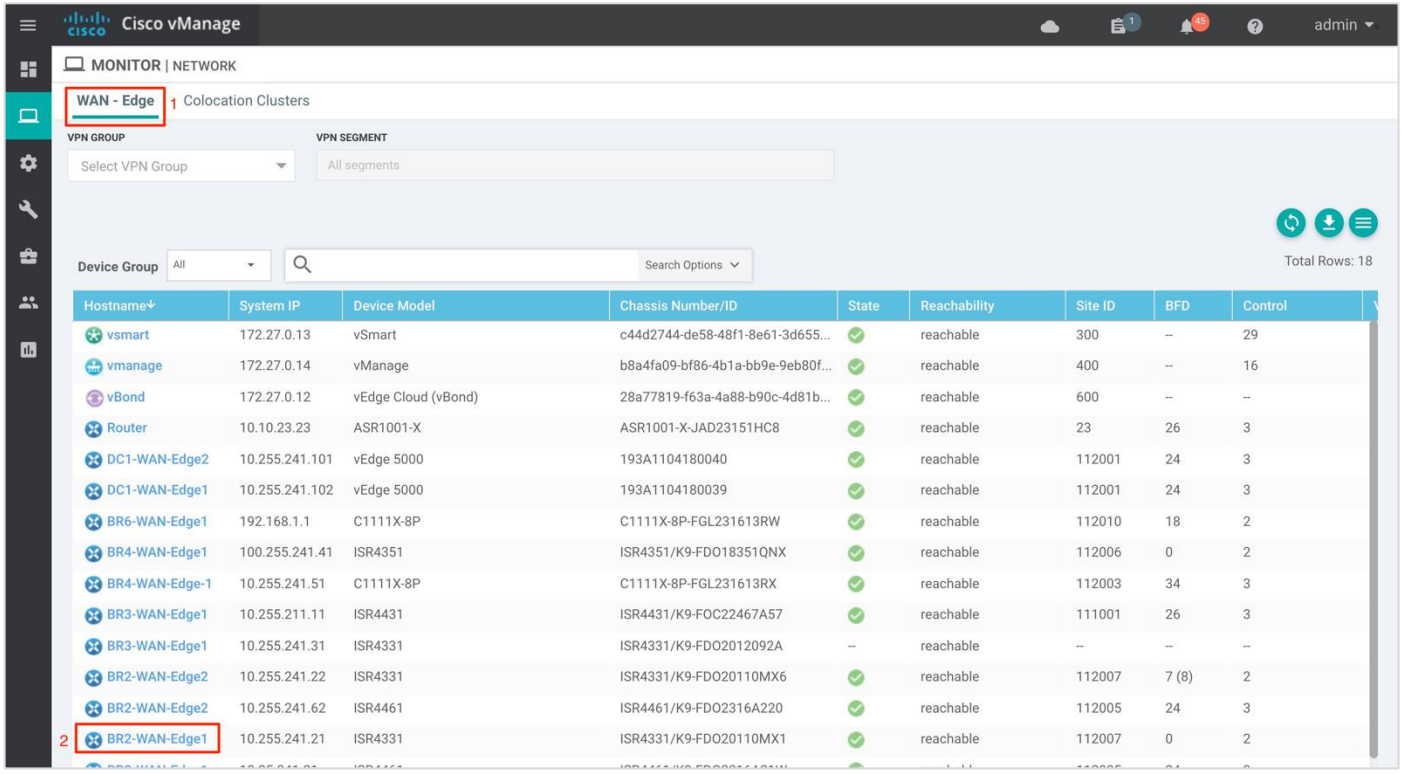
Procedure 2. Monitor the Firewall Feature via vManage Monitor Dashboard

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

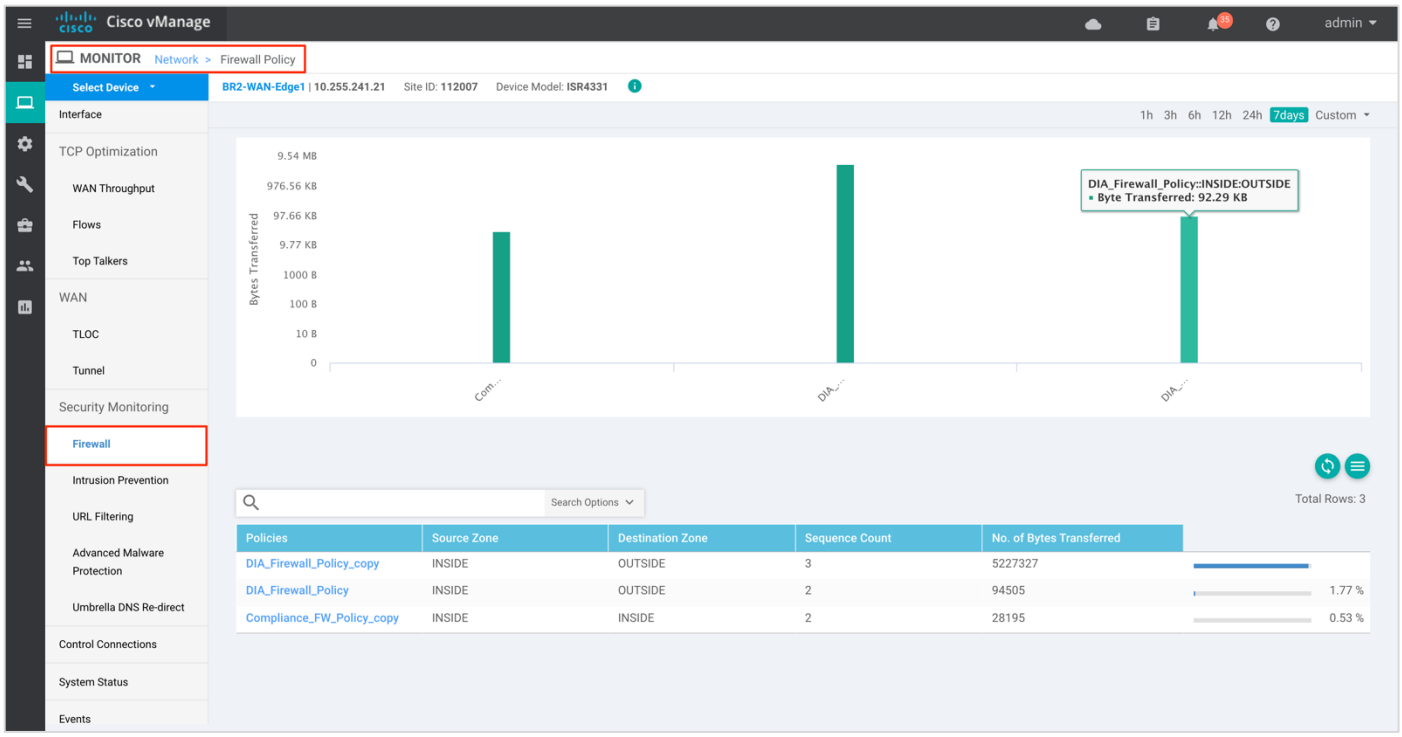
Step 1. Navigate to **Network** within **Monitor** available on the left pane and click on the WAN Edge device you wish to monitor.



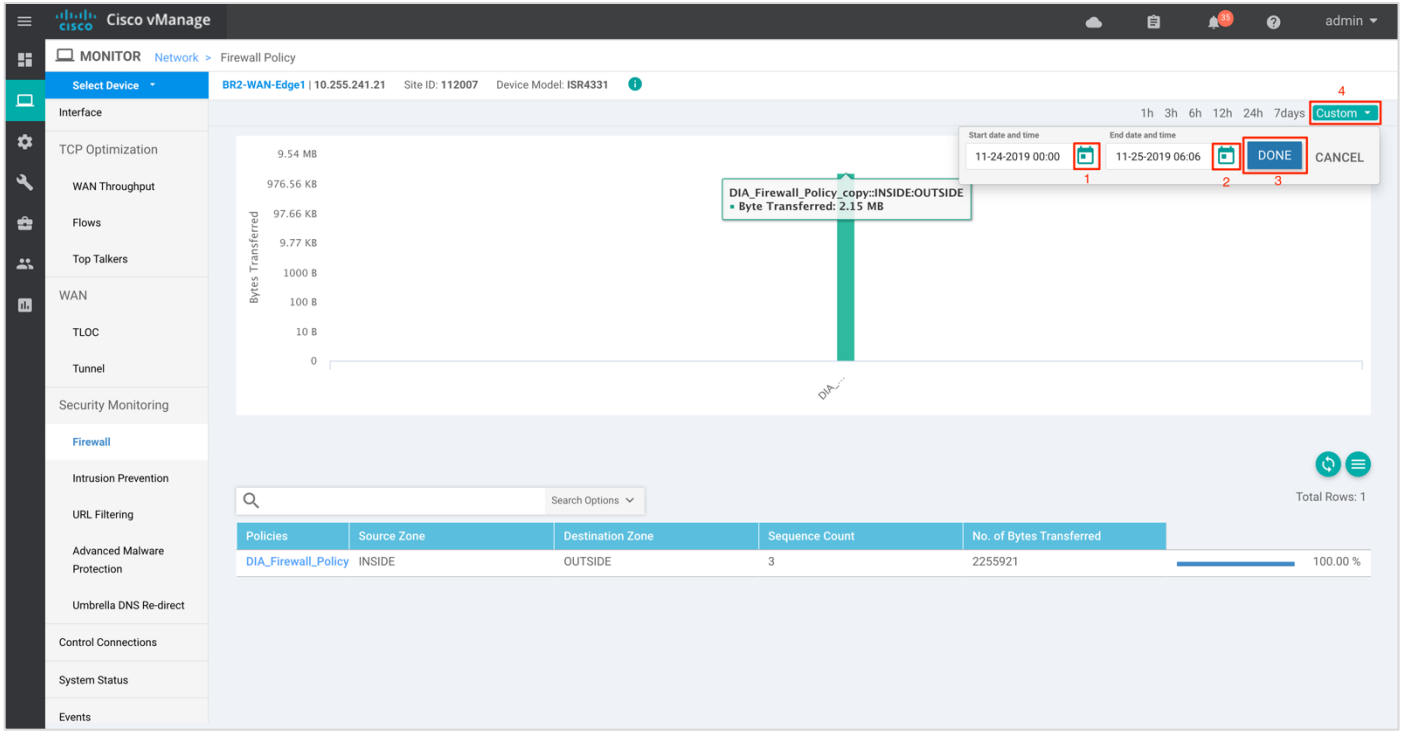
Step 2. Click on a specific WAN Edge device to monitor the firewall policy.



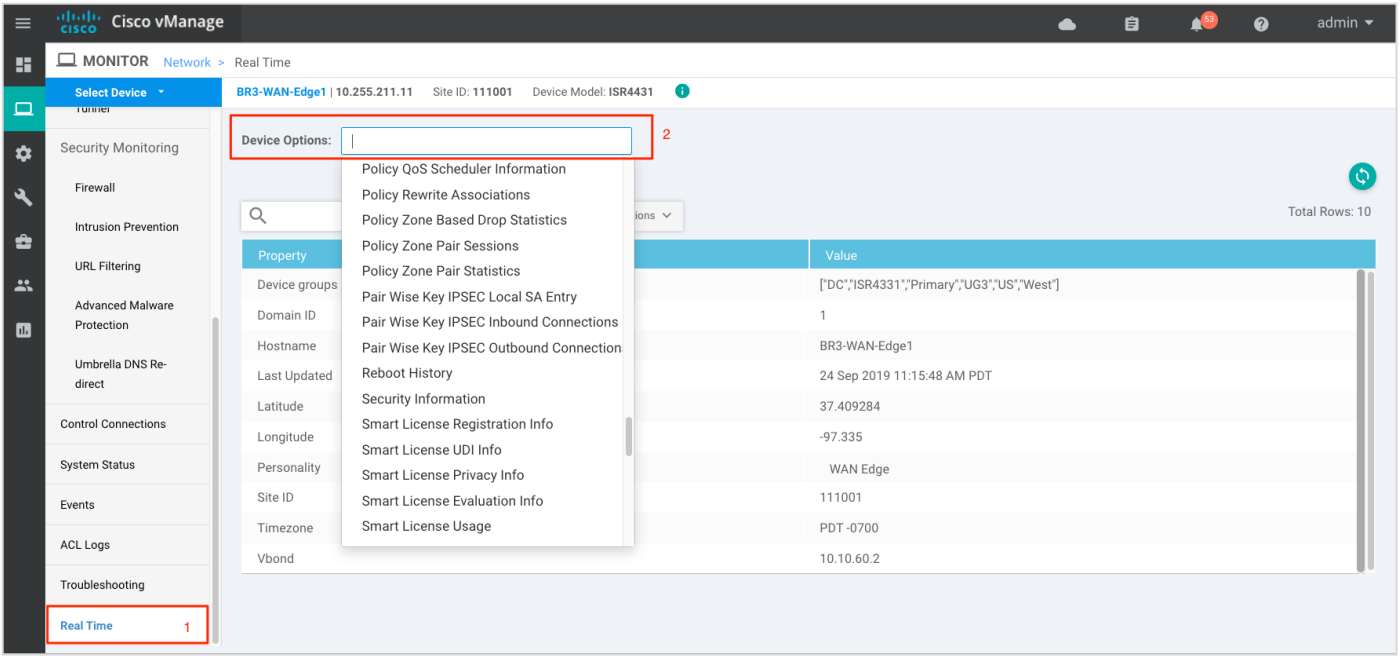
Step 3. Click on **Firewall Policy** tab under **Security Monitoring** from the left pane. Within the dashboard, you can view statistics for all the firewall policies created.



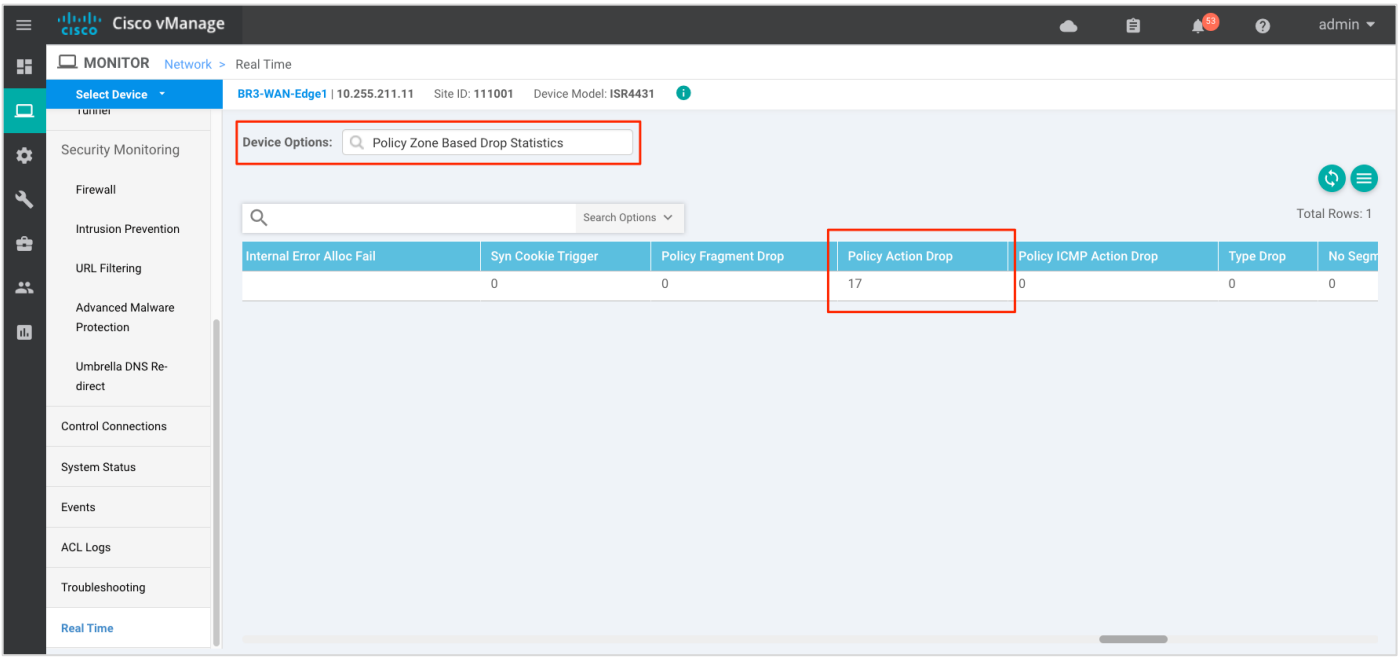
Step 4. As explained previously, the statistics within the **Network** > **Firewall** dashboard can be viewed either hourly, daily, weekly or for a customized period. To customize the time period, select **Custom** and then the click on the calendar icon, to input the **Start date and time** followed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



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.



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.



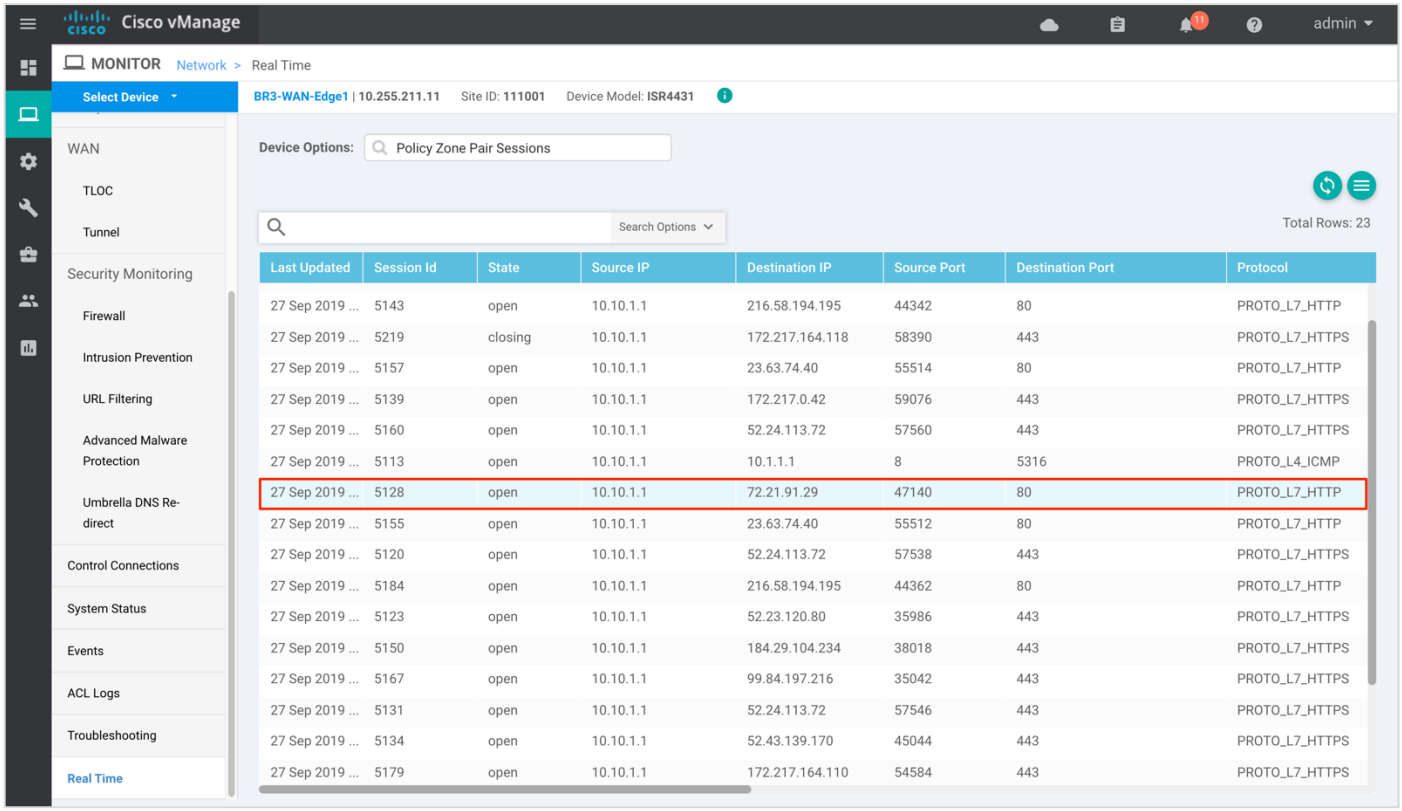
Some of the other examples of packet drops include, ***TCP Invalid TCP initiator*** when the first packet from a TCP initiator is not a SYN (Non-initial TCP segment is received without a valid session). For instance, the initial SYN packet has the ACK flag set or ***Syn flood*** due to a TCP SYN flood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

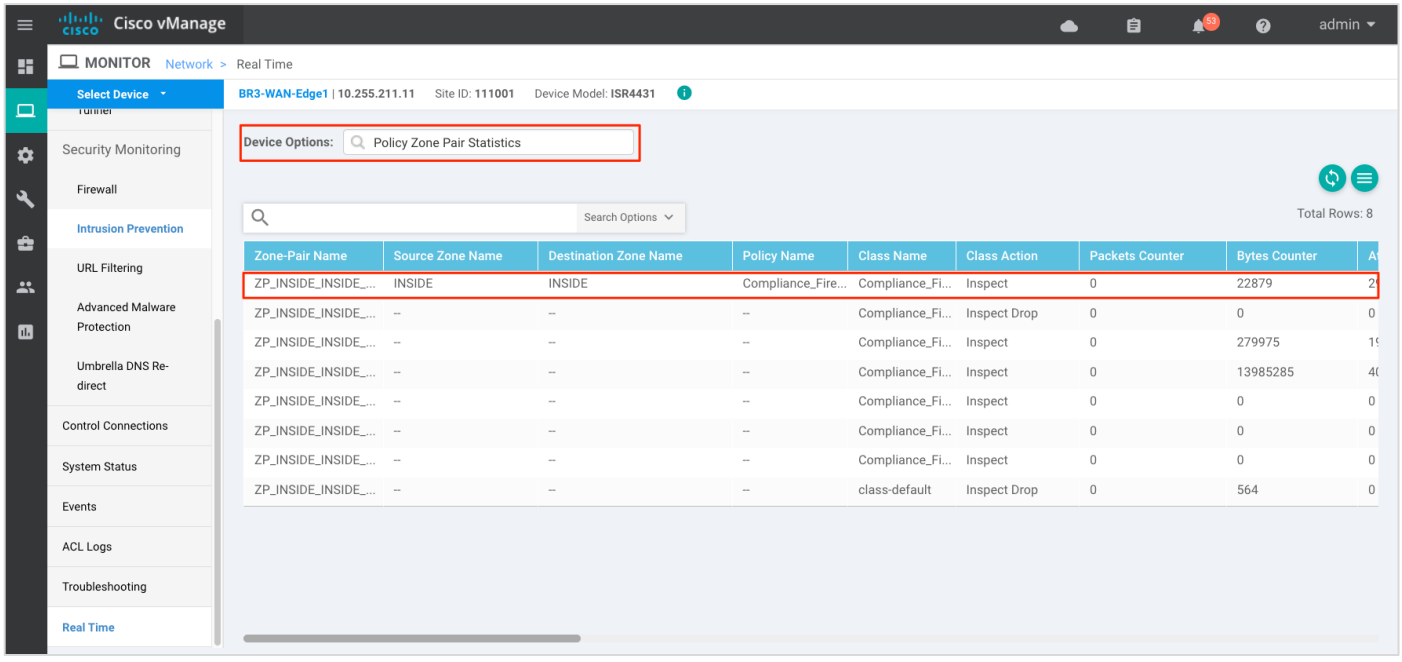
The output displays the state of the session. It can be open, opening, closing or closed. For each individual session you can also find the session update timestamp, along with the source/ destination IP, source/

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.



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.

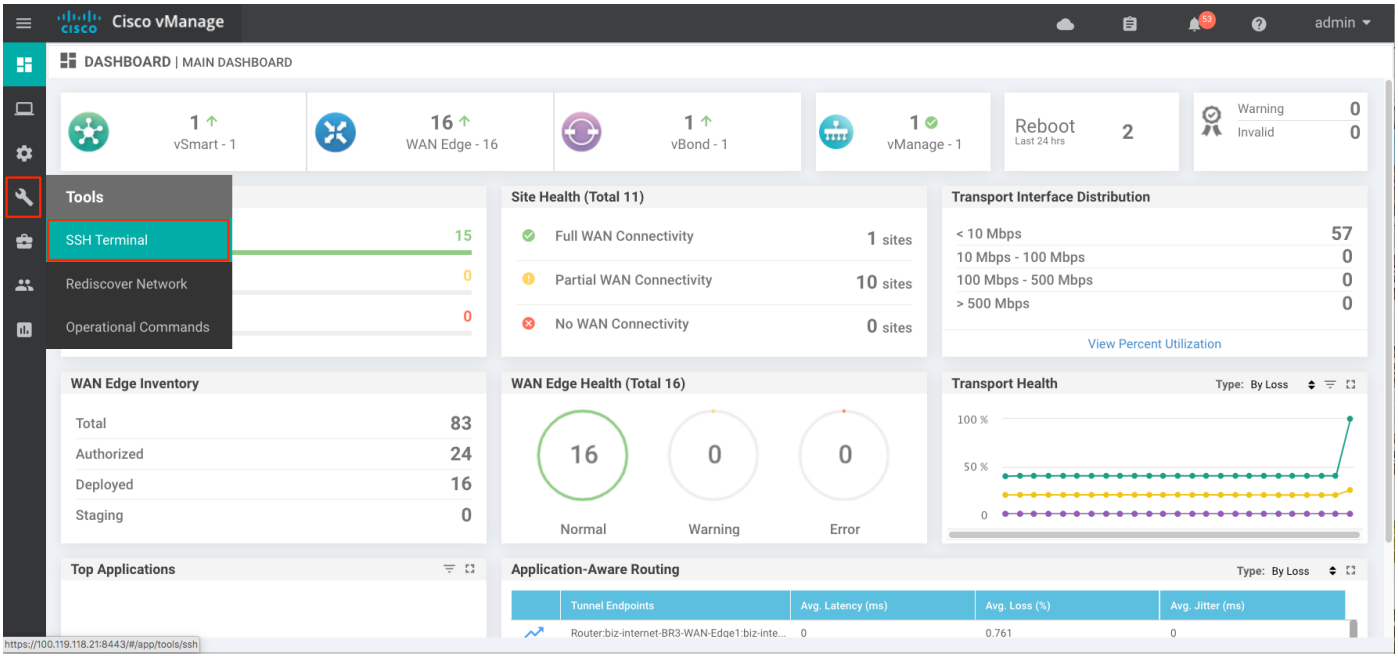
In the figure, notice the action applied for two out of eight is inspect and drop.



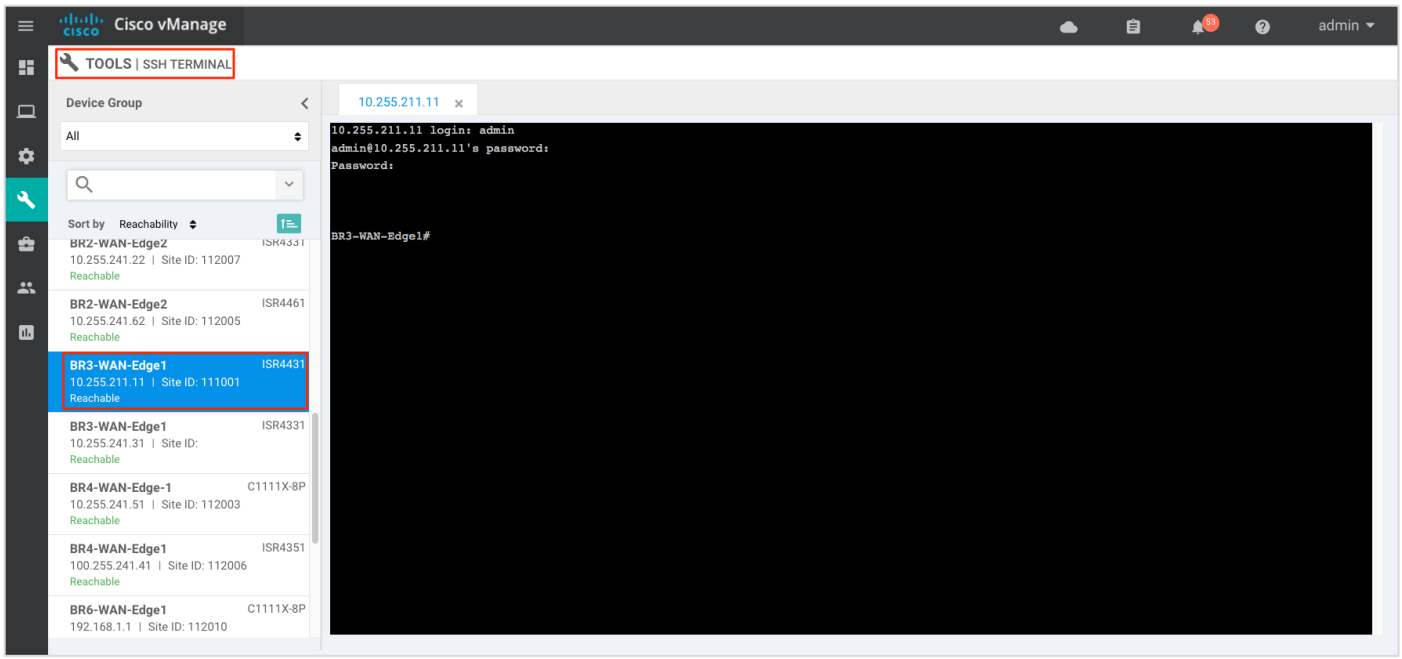
Procedure 3. Monitor the Firewall Feature and Statistics via vManage SSH Server Dashboard

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

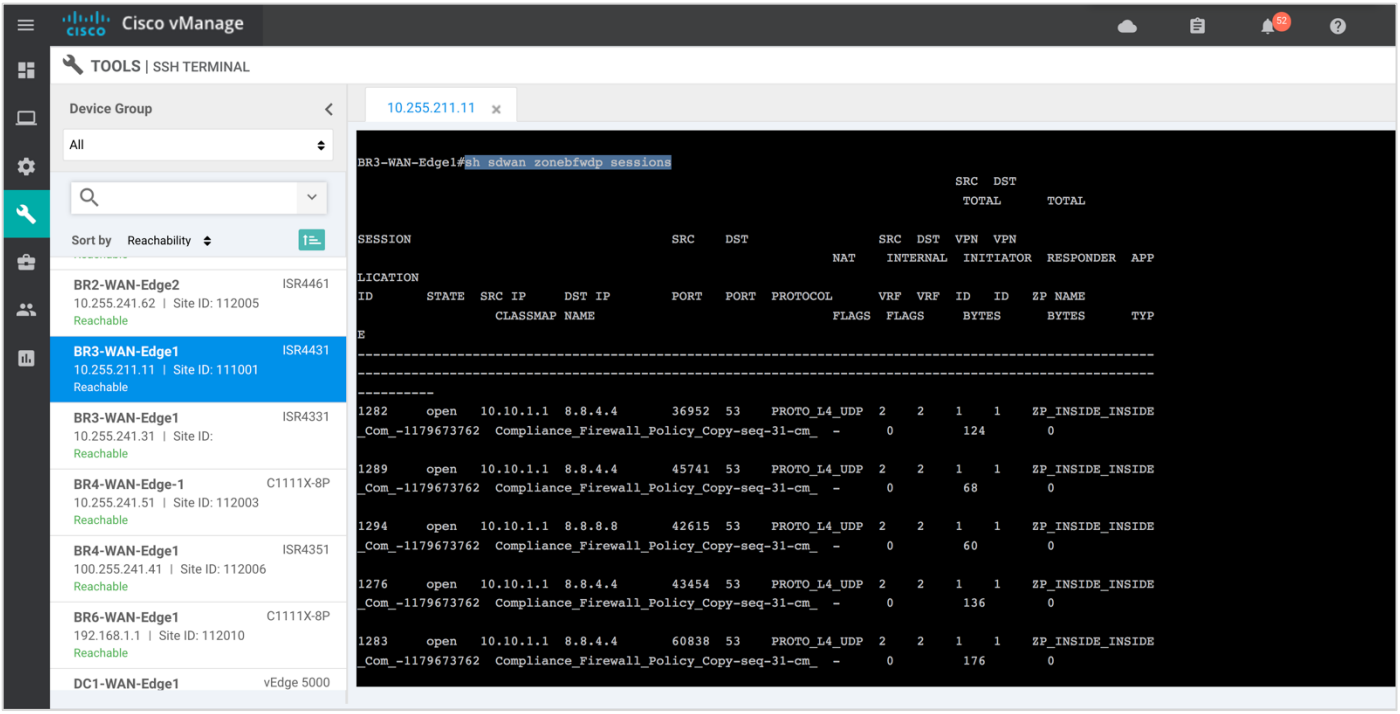
Step 1. Navigate to **Tools** > **SSH Terminal** available on the left pane.



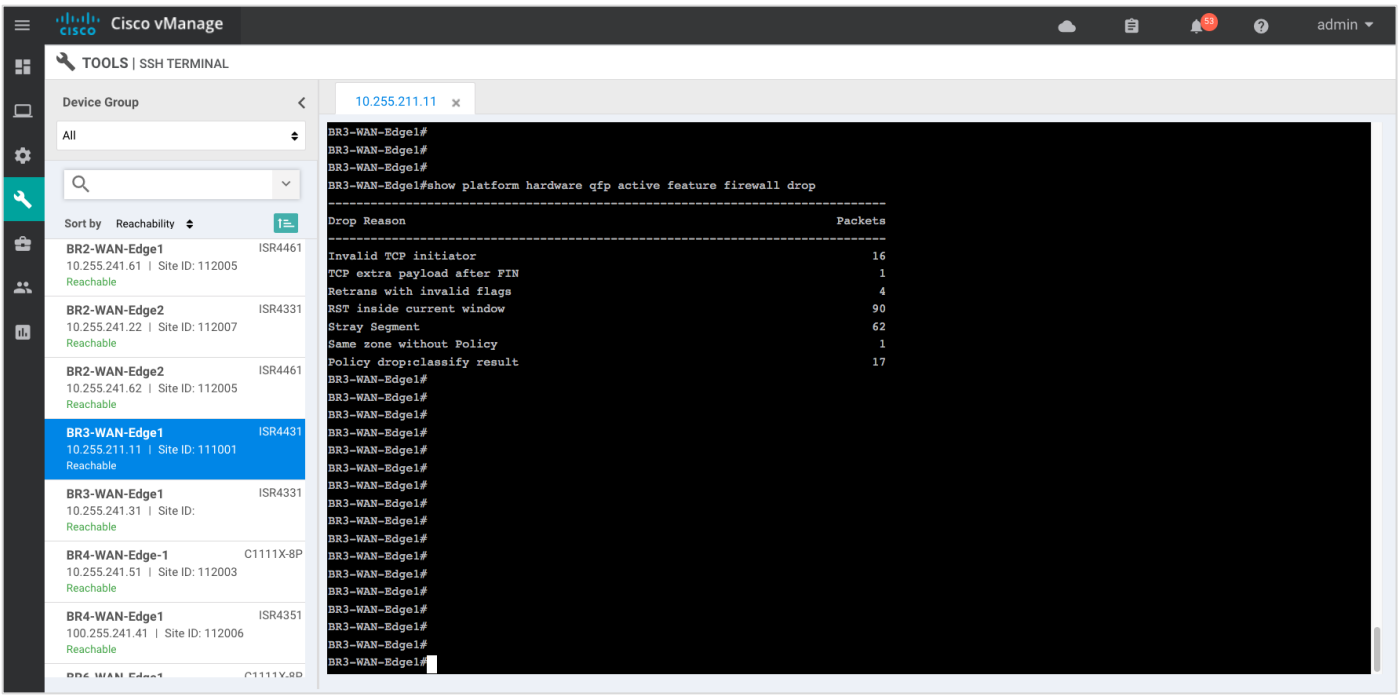
Step 2. Select the device from the list devices, and login.



Step 3. To view the existing firewall sessions, enter the CLI command – ***Show sdwan zonebfwdp sessions***.

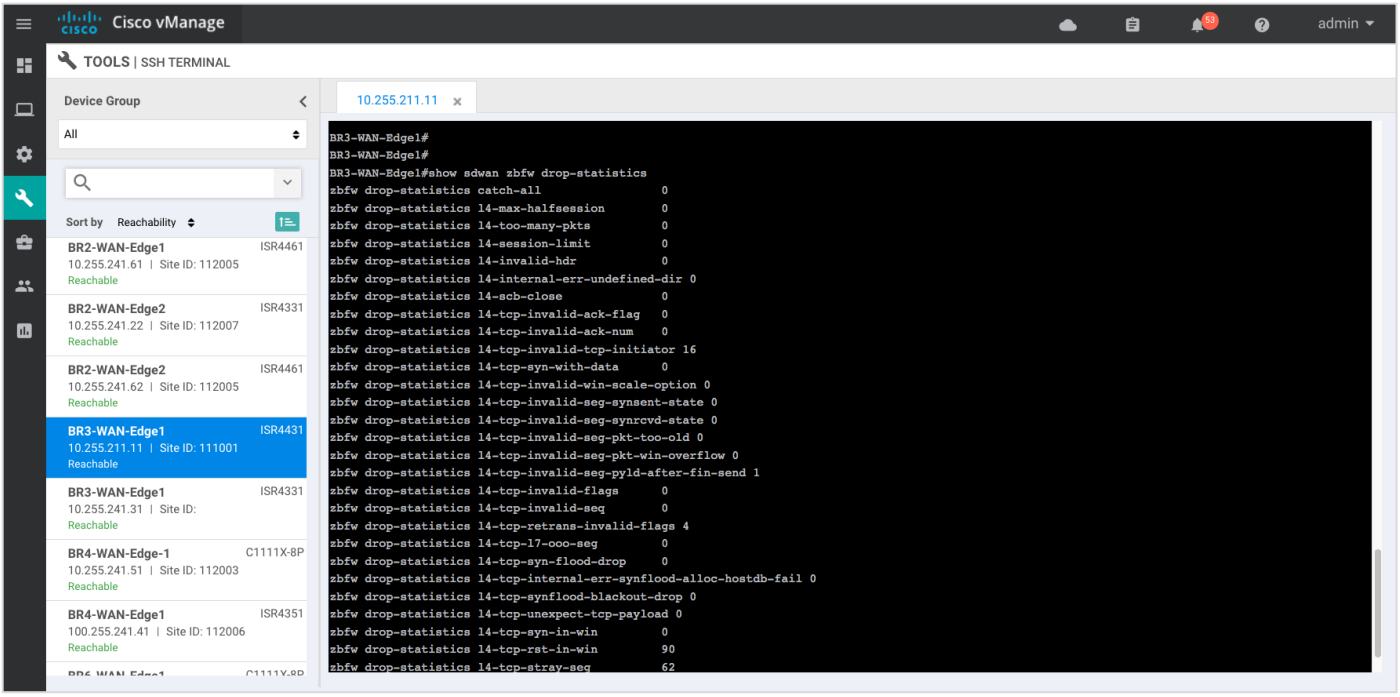


Step 4. To view the firewall drop counters, enter the CLI command – ***Show platform hardware qfp active feature firewall drop.***

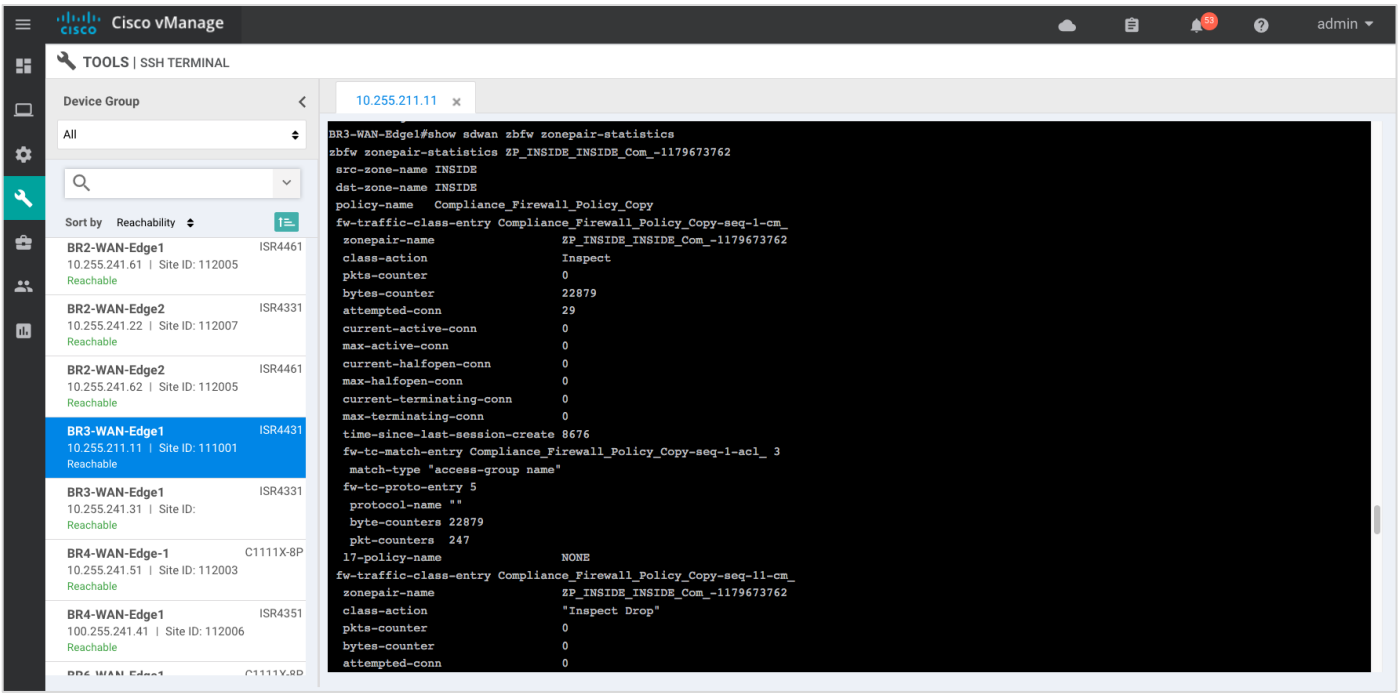


Technical Tip
Clear the drop counters before troubleshooting firewall packet drop. To do so, use the command ***Show platform hardware qfp active feature firewall drop clear***.

Step 5. To view the overall firewall, drop statistics, enter the CLI command – **Show sdwan zbfw drop-statistics.**



Step 6. To view the zone-pair statistics, enter the CLI command - ***Show sdwan zbfw zonepair-statistics***.



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.

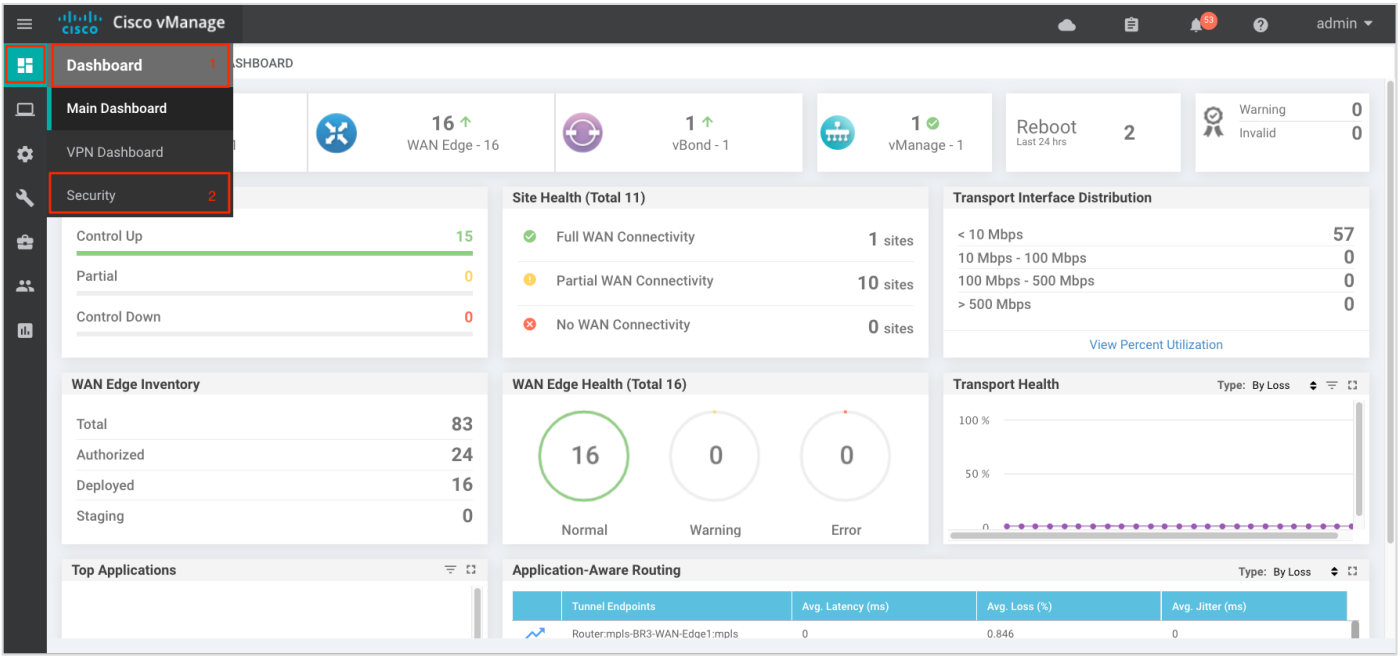
Process 4: Monitor URL Filtering Feature via vManage NMS

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

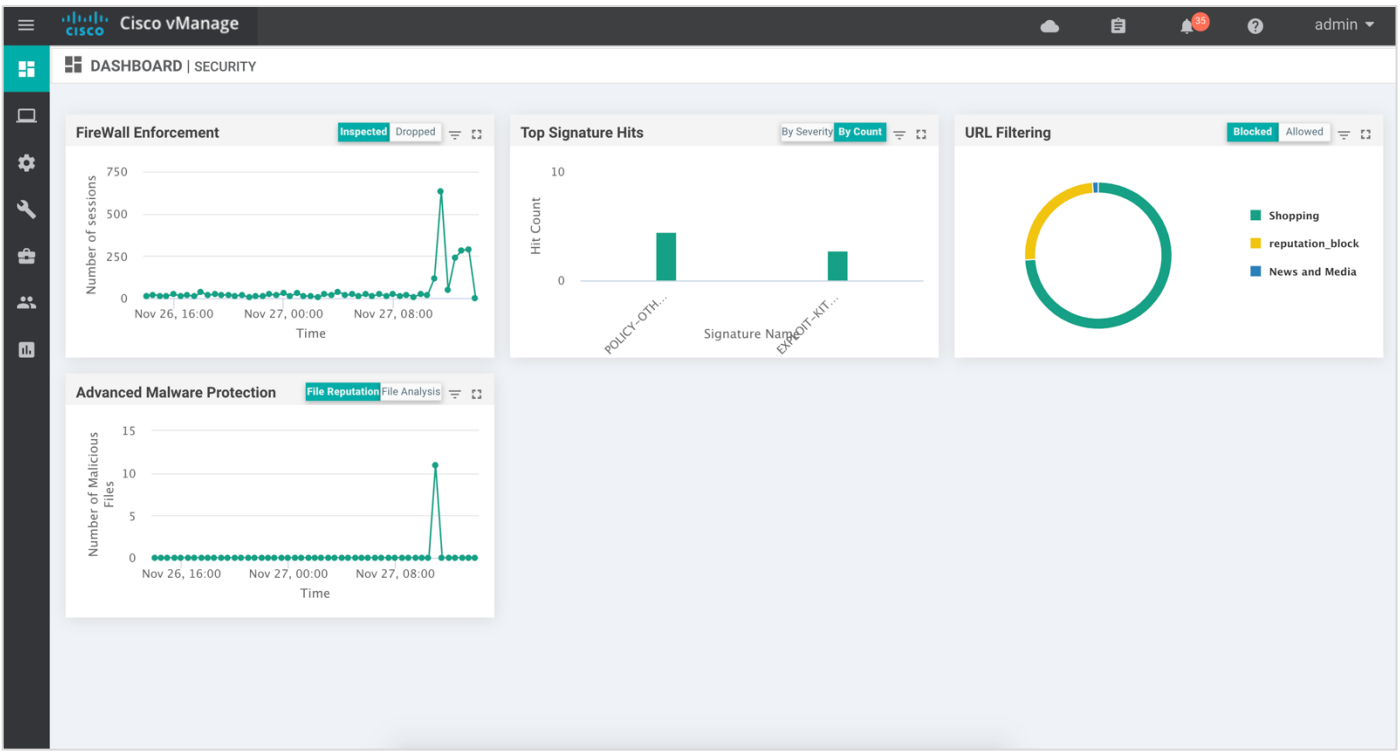
Procedure 1. Monitor URL Filtering Signature Violations via vManage Main Dashboard

Using vManage NMS, you can monitor the URL Filtering feature for a WAN Edge device by web categories using the following steps.

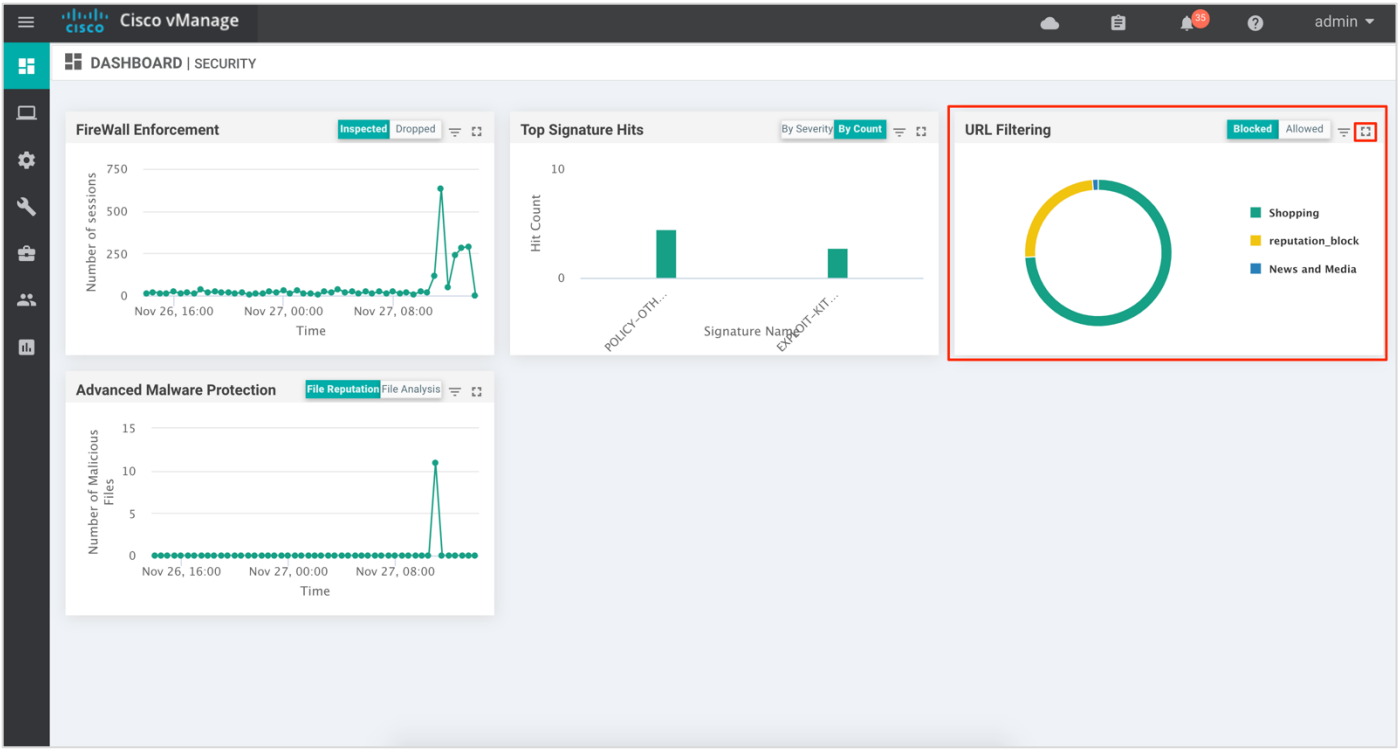
Step 1. Navigate to Dashboard > Security.



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

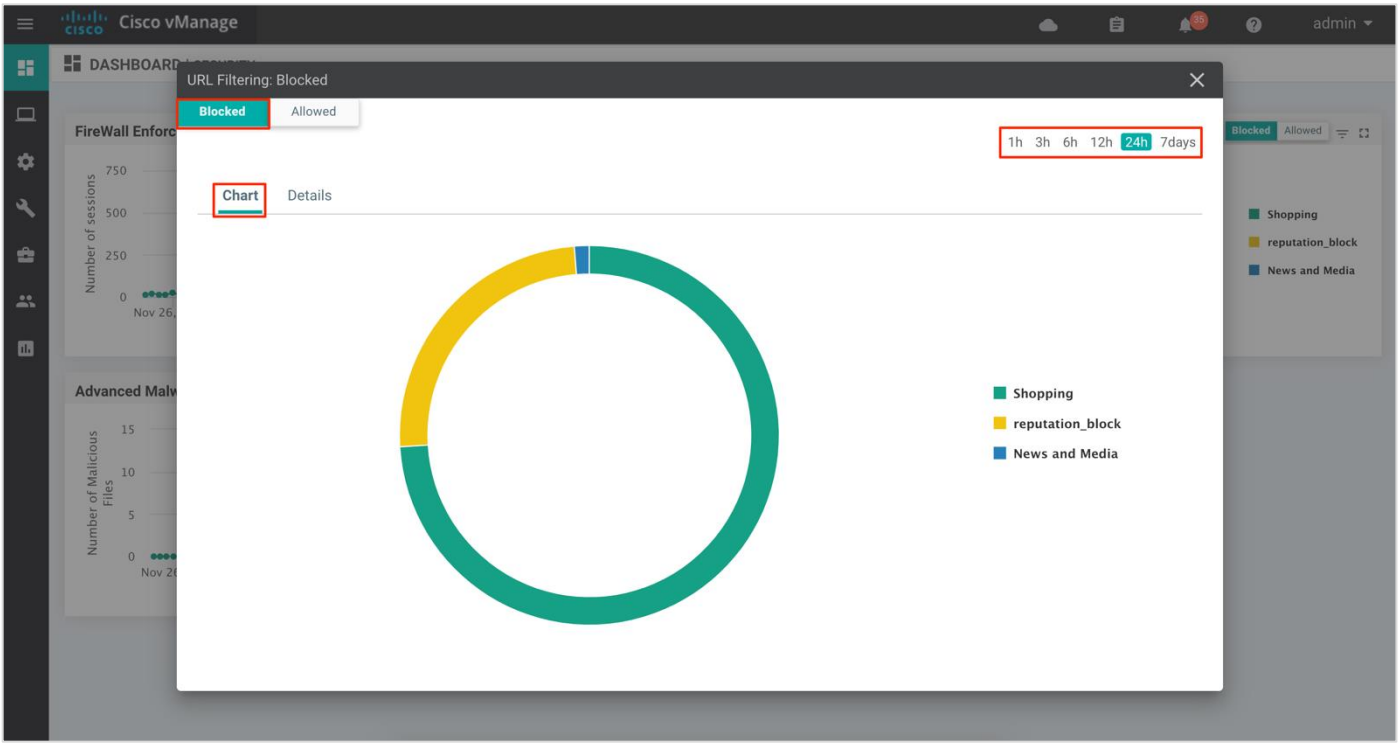


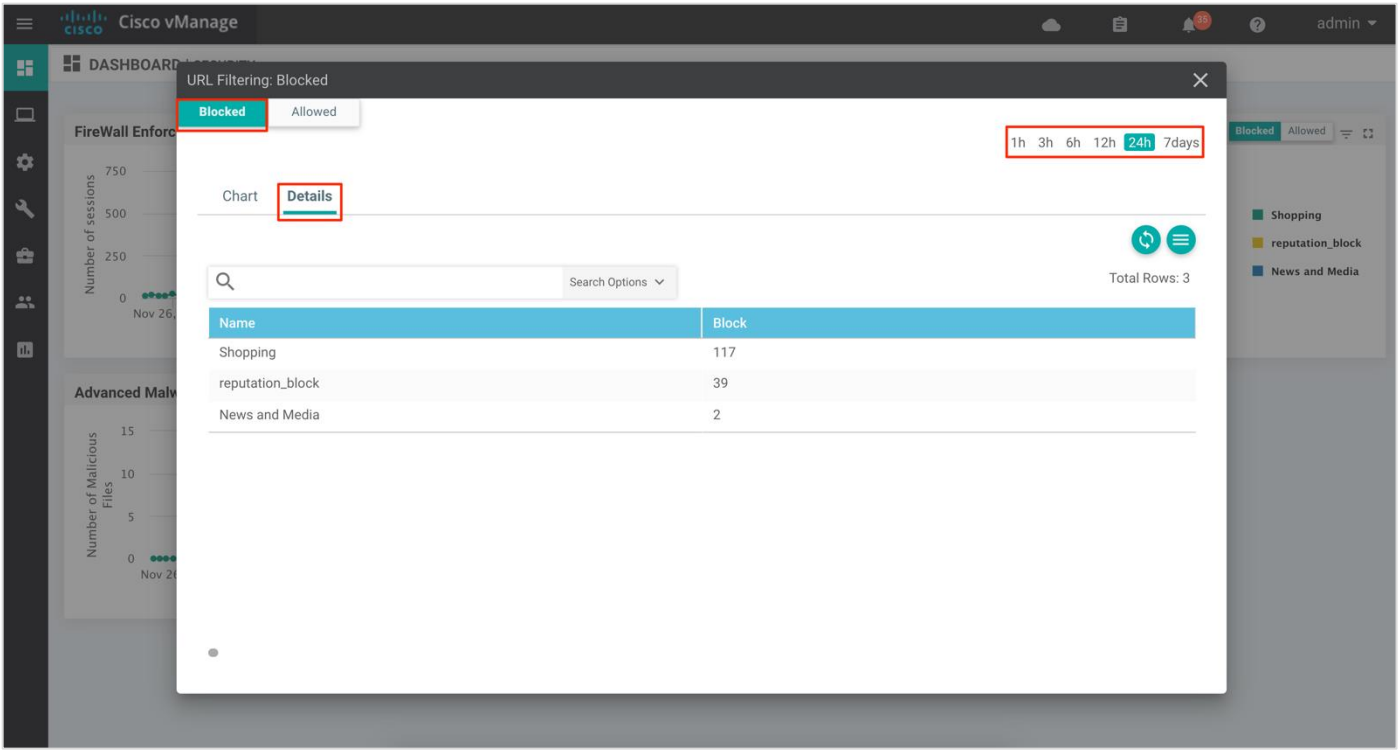
Step 3. To take a closer look into the Web Categories within URL Filtering, click on the square box [] on the top right.



Drill down into the URL Filtering graph for more information on the categories blocked and allowed for 1h, 3h, 6h, 12h, 24h (default) or 7 days.

Some of the categories blocked are displayed below,

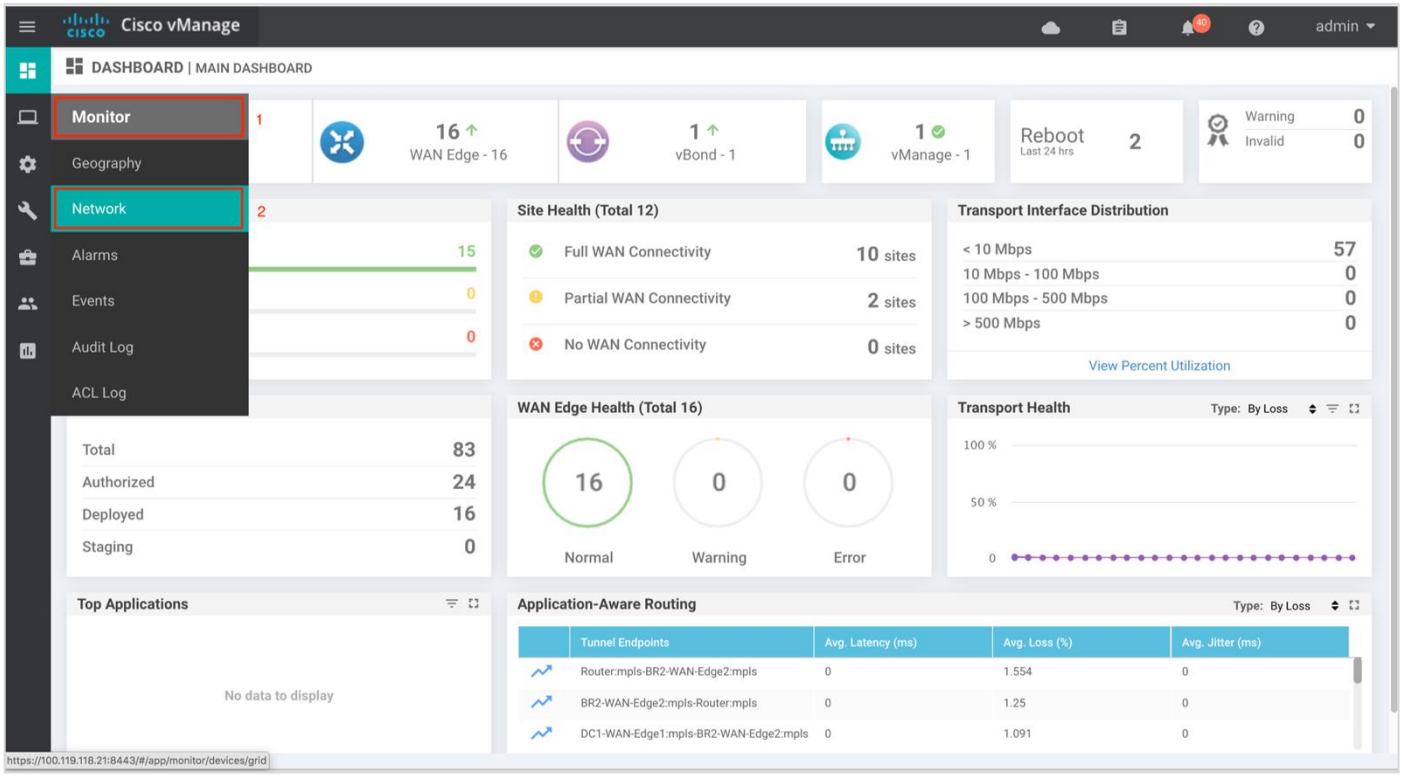




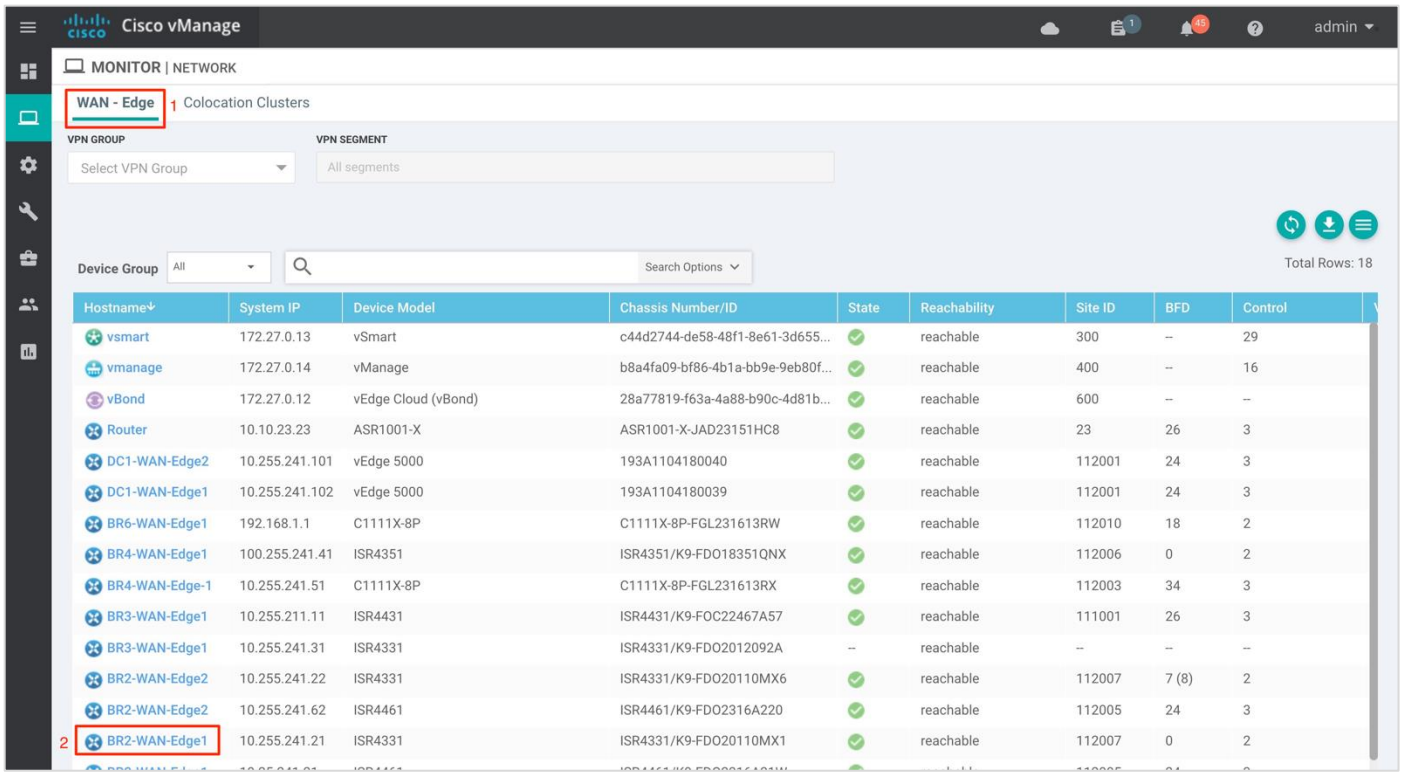
Procedure 2. Monitor URL Filtering Feature via vManage Monitor Dashboard

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

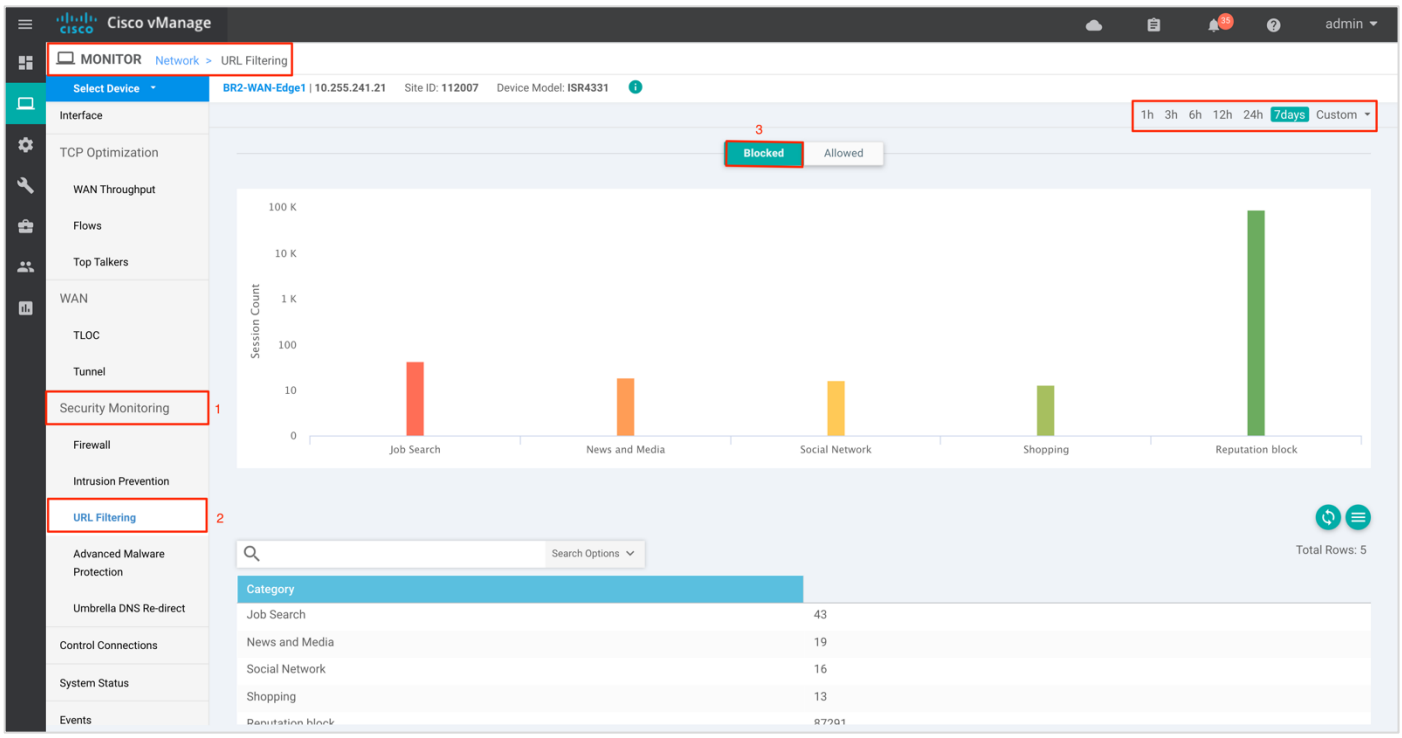
Step 1. Navigate to Network within Monitor available on the left pane and click on the WAN Edge device you wish to monitor.



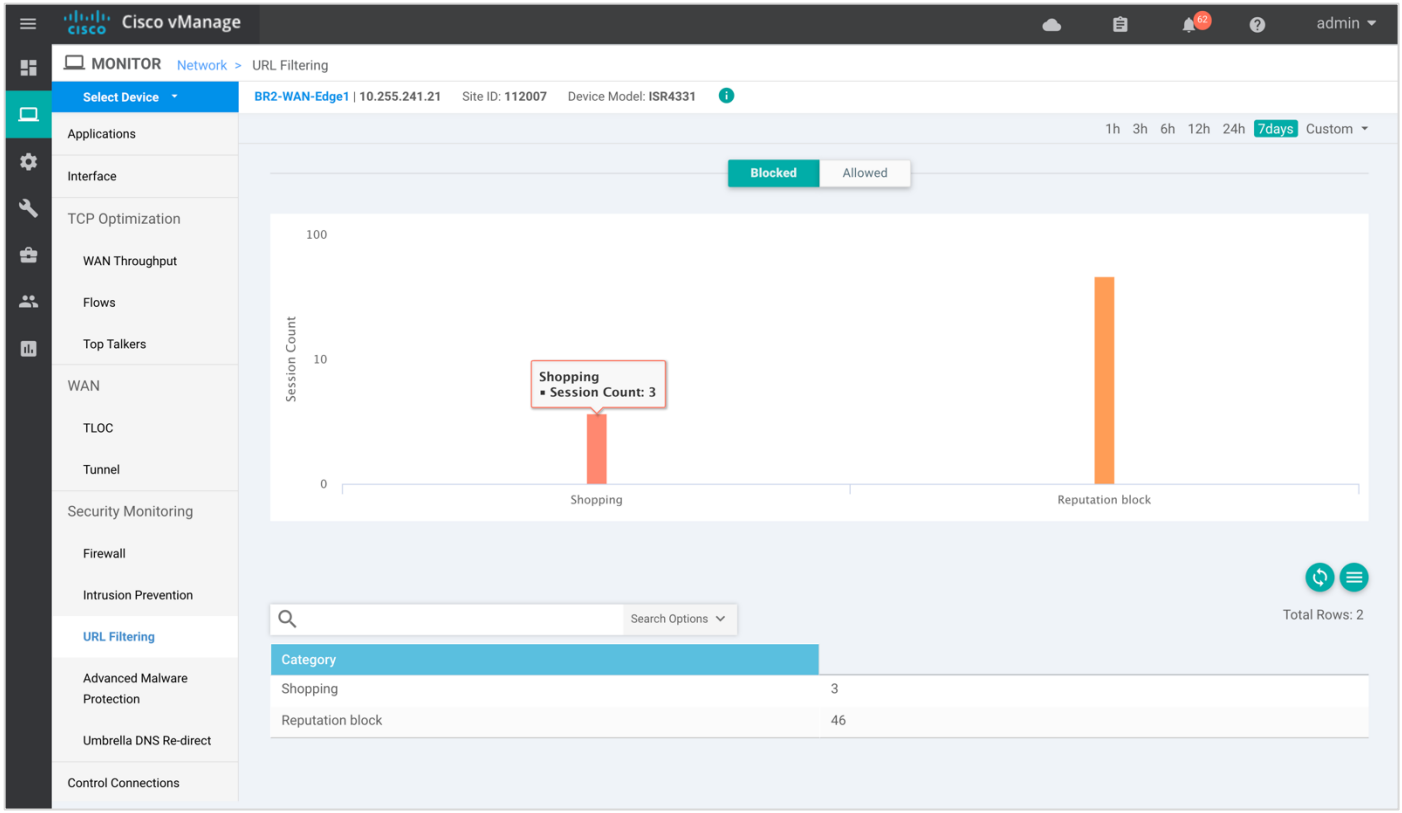
Step 2. Click on a specific WAN Edge device to monitor the URL Filtering policy.



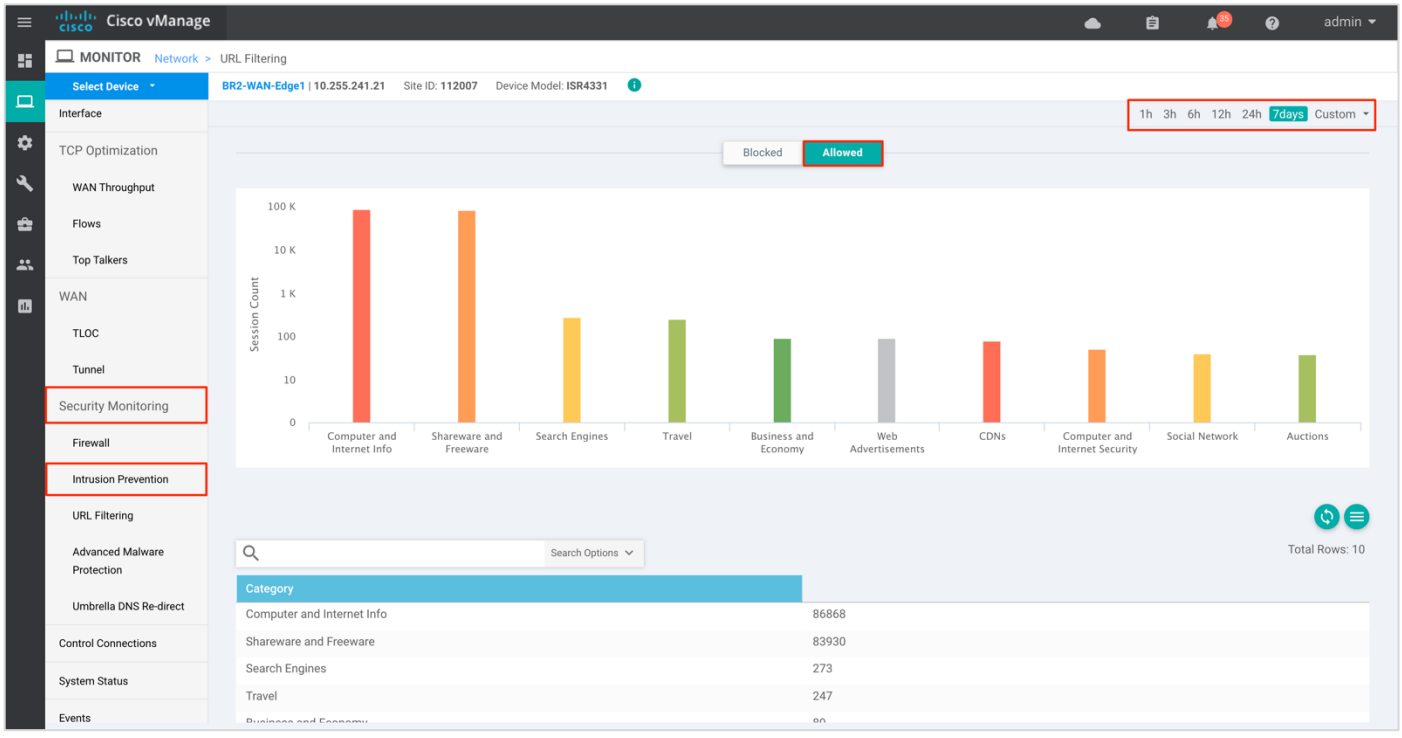
Step 3. In the left panel, under **Security Monitoring**, select **URL Filtering** tab. Click on the **Blocked** tab.



Note: The session count for the blocked URL appears by clicking on the graph.



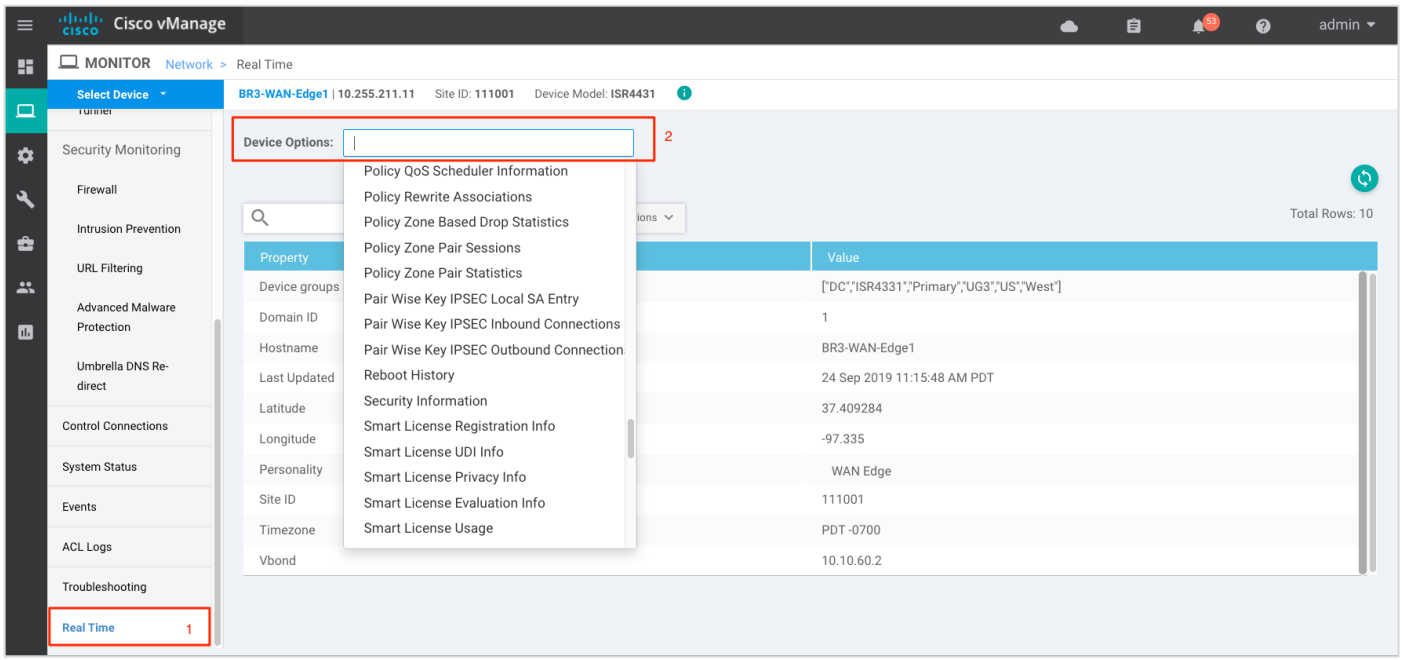
Step 4. Click on **Allowed** tab to view the session count on allowed URLs.



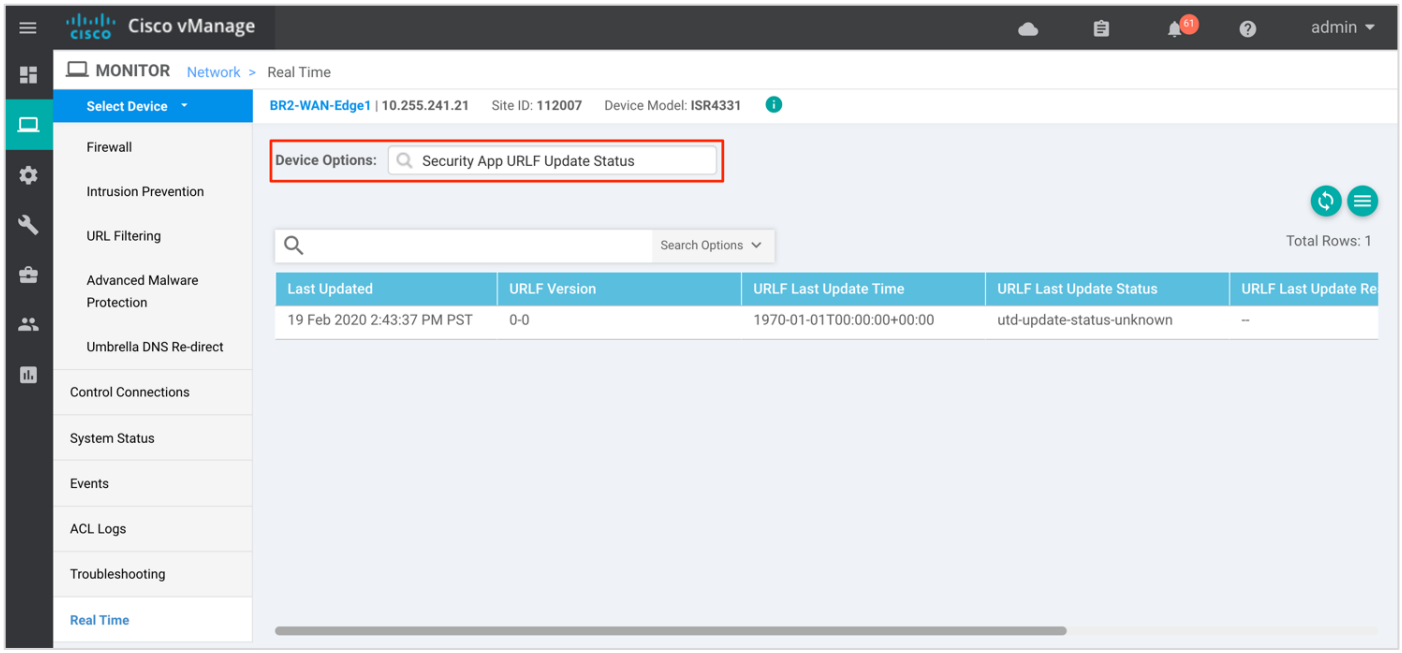
Technical Tip

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.

Step 5. Next, click on **Real Time** from the left pane. Within **Network** > **Real time** and 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.



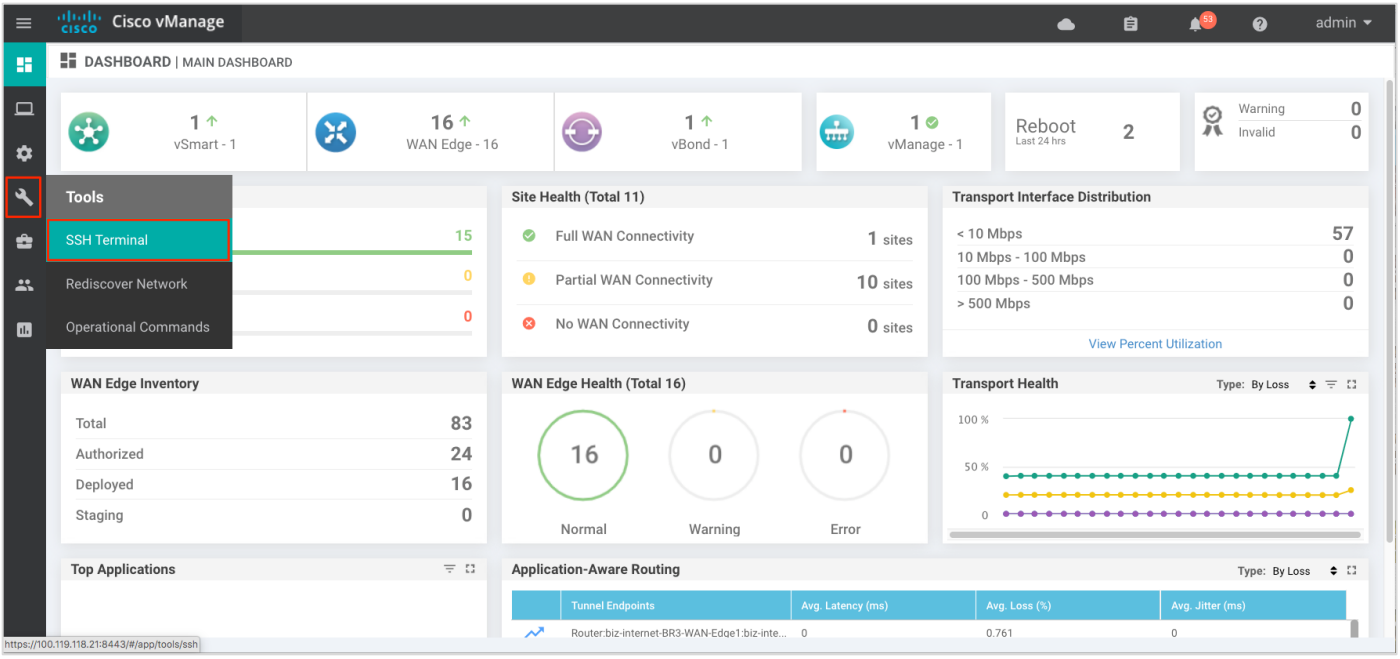
Step 6. To view the status of URL Filtering update, click on **Security App URLF Update Status**.



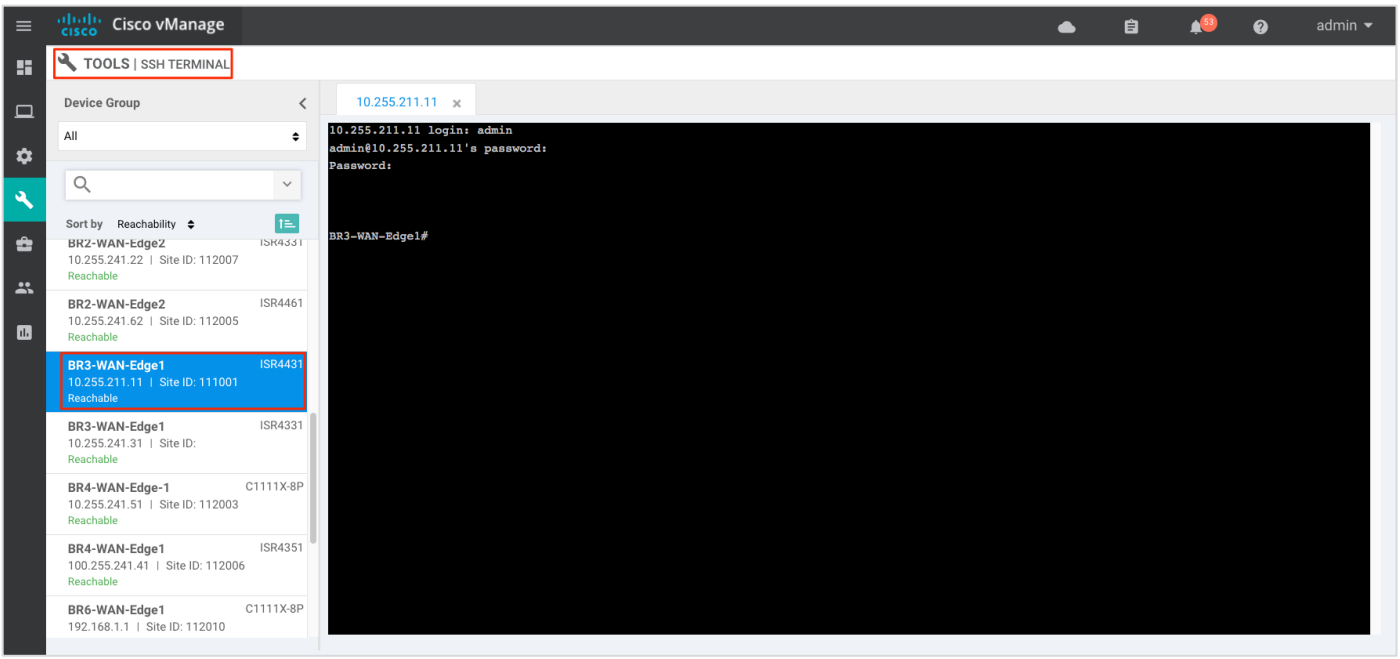
Procedure 3. Monitor URL Filtering Feature and Statistics via vManage SSH Server Dashboard

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

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

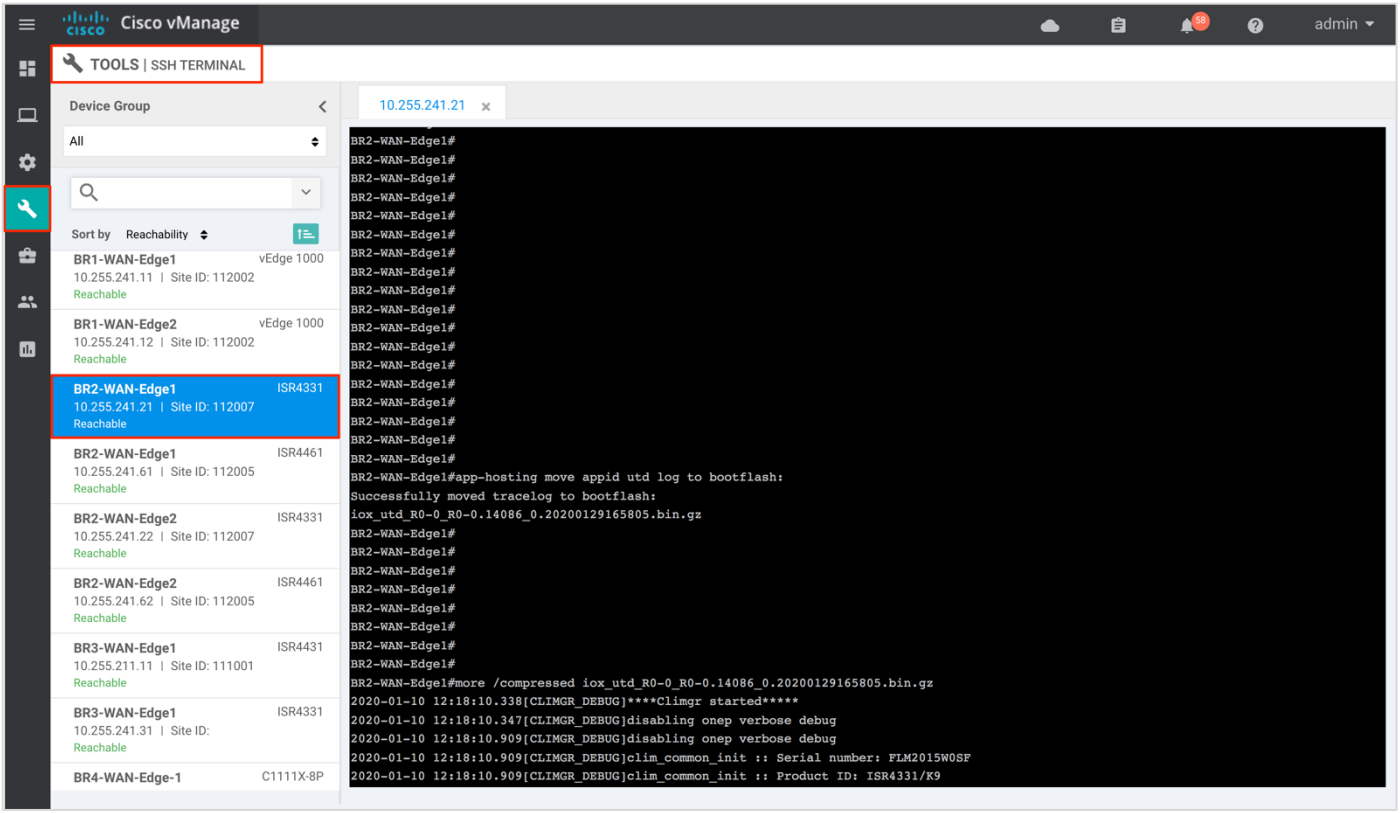


Step 2. Select the device from the list devices, and login.



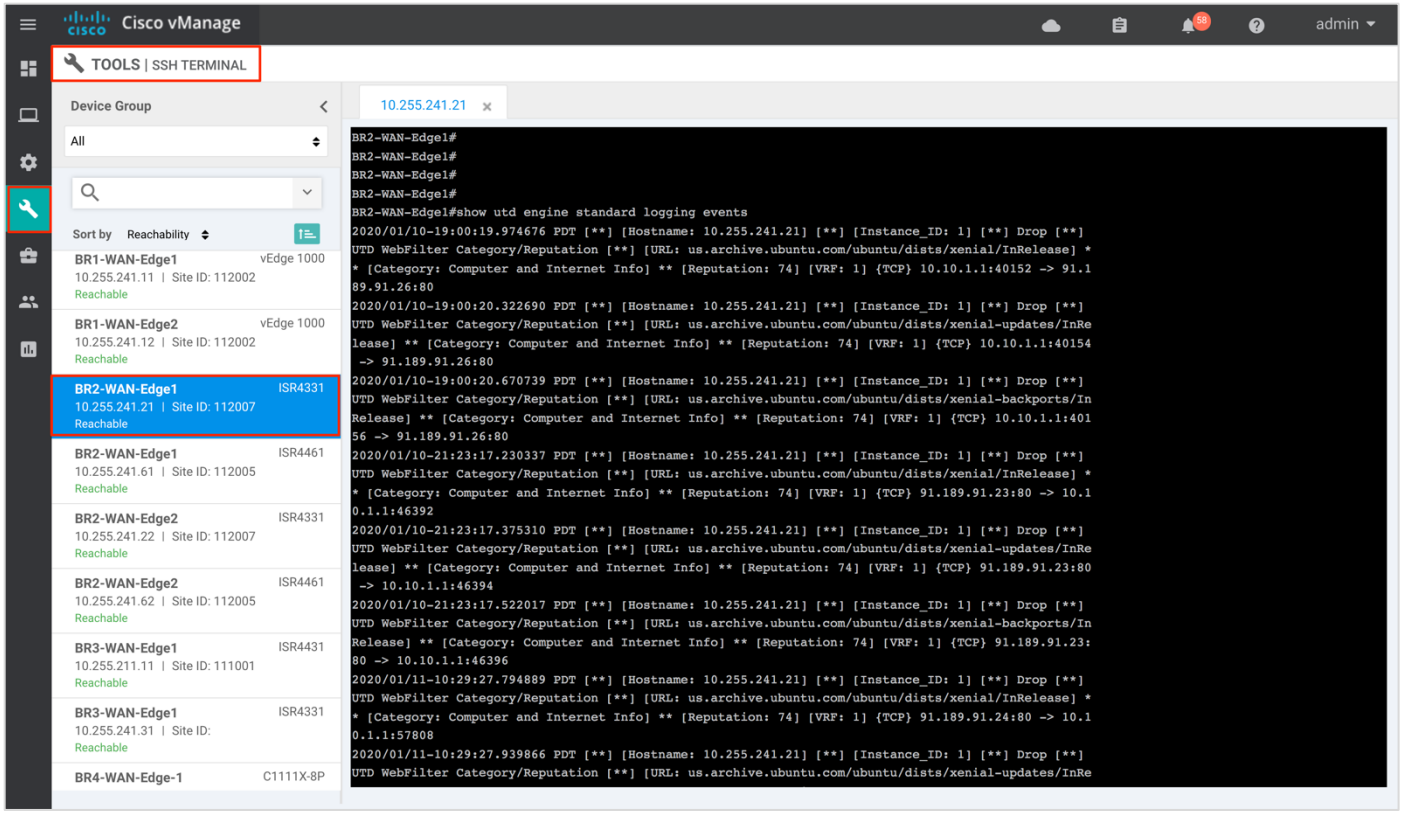
Step 3. Enter the following CLI command to view the container log file. Note, the log file is always copied into flash memory which contains error messages and other logs that may help decode the reason for failure.

- app-hosting move appid utd log to bootflash:
- more /compressed *<Filename.bin.gz>*

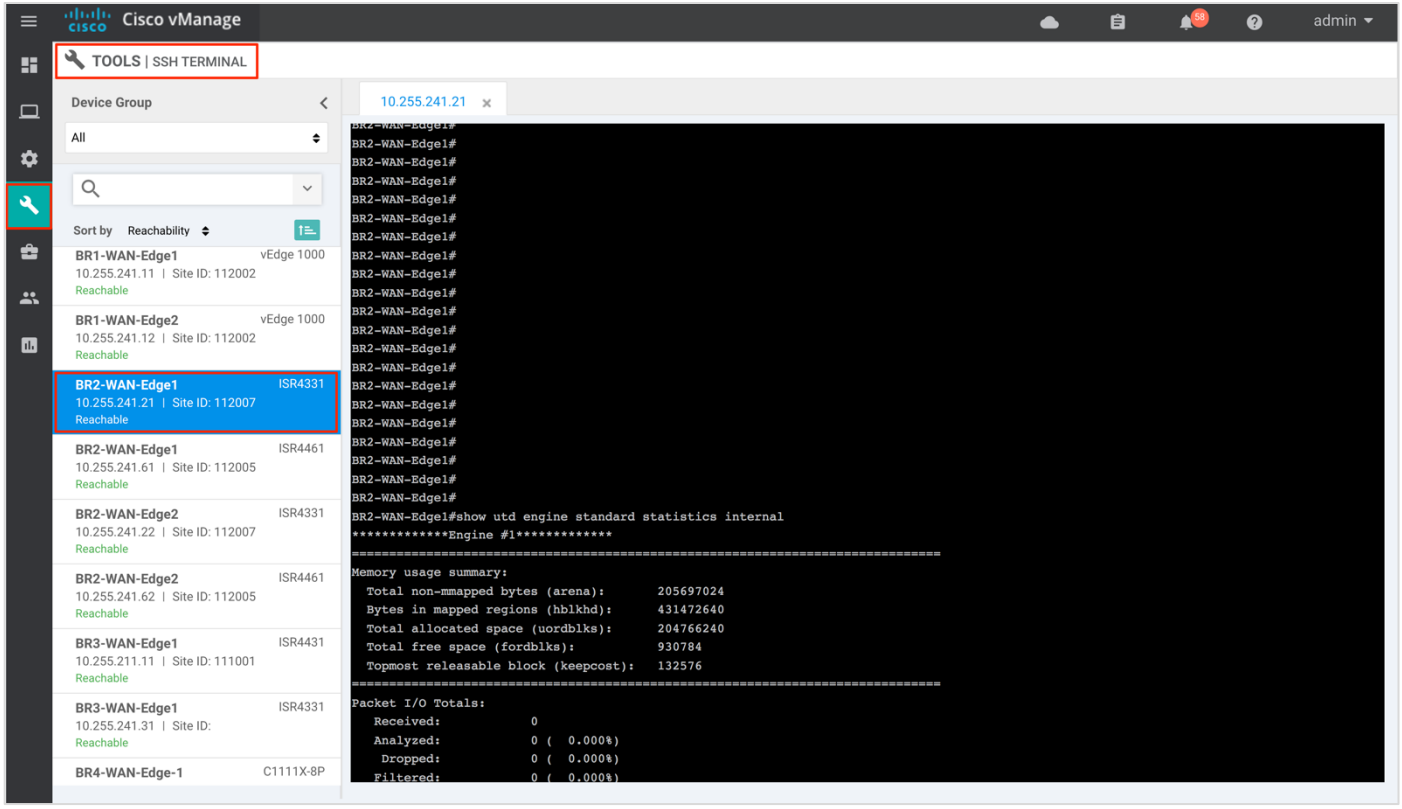


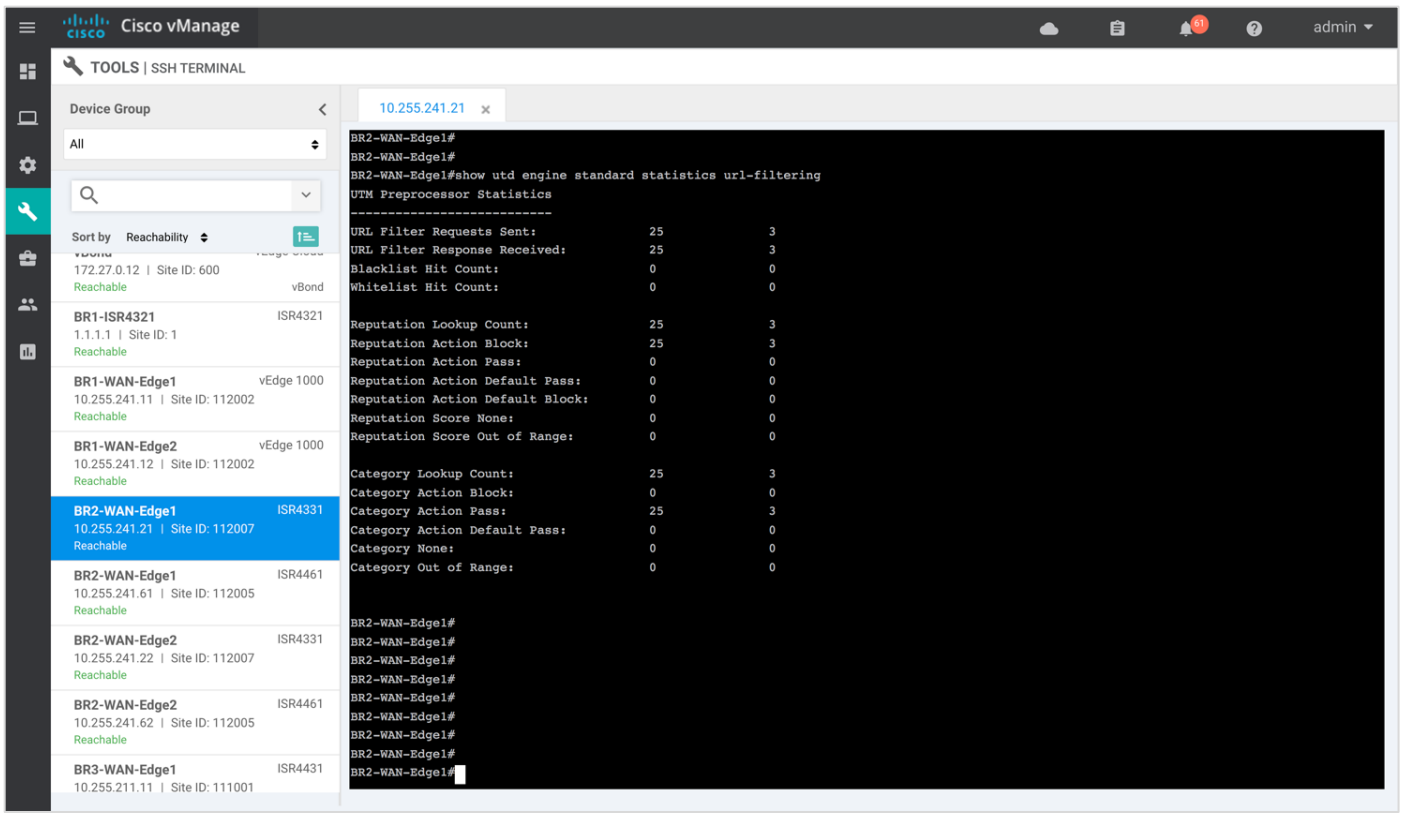
Technical Tip
The provisioned containers use OpenDNS server 208.67.222.222 and 208.67.220.220.

Step 4. To view the session events that are dropped based on category reputation or those which are either blacklisted/whitelisted, enter the CLI command – ***Show utd engine standard logging events***. However, note that the **Alerts** tab within the URL Filtering policy must be enabled to see relevant logs under this show command.



Step 5. To view the UTM preprocessor statistics that includes URL requests sent, received and more, enter the CLI command – ***Show utd engine standard statistics internal***. To view just the UTM preprocessor statistics enter CLI command – ***show utd engine standard statistics url-filtering***.





Some additional commands include, show utd engine standard config and show utd engine standard global.

Process 5: Monitor URL Filtering via Syslog Server

Log into the syslog server and view the error logs. In the logs, you can view the host IP, VRF ID, destination IP, along with details such as the reputation score of the website dropped based on the category.

Date	Time	Priority	Hostname	Message
				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] [**] [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 -> 10.10.1.1:37374

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: Guest_Access_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	Guest_VPN = VPN 2
		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	Guest_VPN
		Destination Zone	Drop-down	OUTSIDE
	Name		Entry tab	Guest Access_Firewall_Policy
	Description		Entry tab	Firewall policy to protect guest users
	Match (Rule 1)	Source Data Prefix List	Variable	Client_Network
		Protocol	Drop-down	6 17
	Actions (Rule 1)	Inspect	Radio Button	Enable
	Match (Rule 2)	Protocol	Drop-down	1

Policy sub-section	Section	Condition/Parameter	Type	Value
	Actions (Rule 2)	Inspect	Radio Button	Enabled
			Select	Log
URL Filtering	Target	VPNs	Entry tab	2
	Policy Name		Entry tab	Guest Access_URL_Filtering_Policy
	Policy Description		Entry tab	URL Filtering policy to filter guest Internet traffic
	Web Categories		Drop down	Block
	Web Categories		Drop down	Abortion, Job search, Shopping
	Web Reputation		Drop down	Low Risk
	Advanced			
	Whitelist URL List	Good_URL	Drop down	.*abcxyz.com
	Blacklist URL List	Bad_URL	Drop down	.*customer.com
	Block Page Server	Block Page Content	Radio Button	Error message
	Alerts		Radio Button	Blacklist, Whitelist, Reputation/ Category
Policy Summary	Security Policy Name		Entry tab	Guest_Access_Security_Policy
	Security Policy Description		Entry tab	Security Policy Specific to Guest Access Use Case
	Additional Policy Settings (Firewall)	High Speed Logging - VPN	Entry tab	0
		High Speed Logging - Server IP	Entry tab	10.2.2.2
		High Speed Logging - Port	Default	2055
	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 (tested both)

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
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Single_Transport
	BGP	BR_VPN0_BGP
	VPN Interface	BR_INET_INT
		BR_MPLS_INT
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_BASE
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_VPN1_INT1

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

Example Branch Configuration

The following section lists out an example branch configuration.

Guest_Access_Security_Policy

```
policy
 url-filtering Guest_Access_URL_Policy
  web-category-action block
  web-categories abortion shopping job-search sports
  block-threshold low-risk
  white-list test4
  black-list bad_domain
  block text "<![CDATA[&lt;h3&gt;Access to the requested page has been
denied&lt;/h3&gt;&lt;p&gt;Please contact your Network Administrator&lt;/p&gt;]]>"
  logging host 10.2.2.2 vpn 0
  alert categories-reputation blacklist whitelist
  target-vpns 2
 !
 zone-based-policy Guest_Access_Firewall
    sequence 1
     match
      source-data-prefix-list Client_Network
      protocol 6 17
     !
     action inspect
     !
    !
    sequence 11
     match
      protocol 1
     !
     action inspect
     !
    !
  default-action drop
 !
  zone GUEST_VPN
```

```
 vpn 2
!
zone OUTSIDE
 vpn 0
!
zone-pair ZP_GUEST_VPN_OUTSIDE__2128202431
 source-zone GUEST_VPN
 destination-zone OUTSIDE
 zone-policy Guest_Access_Firewall
!
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
 !
 url-black-list bad_url
  pattern .*customer.com
 !
 url-white-list good_url
  pattern .*.abcxyz.com
 !
!
zone-to-nozone-internet deny
failure-mode open
audit-trail on
!
```

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 Guest_Access_Firewall-seq-1-acl_
  11 permit object-group Guest_Access_Firewall-seq-1-service-og_ object-group
Client_Network any
 !
 ip access-list extended Guest_Access_Firewall-seq-11-acl_
  11 permit object-group Guest_Access_Firewall-seq-11-service-og_ any any
 !
 ip access-list extended utd-nat-acl
```

```
 10 permit ip any any
!
no ip http ctc authentication
no ip igmp ssm-map query dns
ip nat 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-all Guest_Access_Firewall-seq-1-cm_
 match access-group name Guest_Access_Firewall-seq-1-acl_
!
class-map type inspect match-all Guest_Access_Firewall-seq-11-cm_
 match access-group name Guest_Access_Firewall-seq-11-acl_
!
policy-map type inspect Guest_Access_Firewall
 class Guest_Access_Firewall-seq-1-cm_
   inspect audit-trail-pmap_
 !
 class Guest_Access_Firewall-seq-11-cm_
   inspect audit-trail-pmap_
 !
 class class-default
   drop
 !
!
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 Guest_Access_Firewall-seq-1-service-og_
 tcp
 udp
!
object-group service Guest_Access_Firewall-seq-11-service-og_
 icmp
!
clock summer-time PDT recurring
clock timezone PDT -8 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
no logging rate-limit
logging persistent
aaa authentication login default local
aaa authorization exec default local
```

```
aaa session-id common
parameter-map type inspect audit-trail-pmap_
 audit-trail on
!
parameter-map type inspect-global
 alert on
 log dropped-packets
 log flow-export v9 udp destination 10.2.2.2 2055 vrf 0
 multi-tenancy
 vpn zone security
!
parameter-map type regex bad_url-bl_
 pattern .*customer.com
!
parameter-map type regex good_url-wl_
 pattern .*.abcxyz.com
!
zone security GUEST_VPN
 vpn 2
!
zone security OUTSIDE
 vpn 0
!
zone-pair security ZP_GUEST_VPN_OUTSIDE__2128202431 source GUEST_VPN destination
OUTSIDE
 service-policy type inspect Guest_Access_Firewall
!
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
 web-filter block page profile block-Guest_Access_URL_Policy
  text <\![CDATA[&lt;h3&gt;Access to the requested page has been
denied&lt;/h3&gt;&lt;p&gt;Please contact your Network Administrator&lt;/p&gt;]]>
 !
 web-filter url profile Guest_Access_URL_Policy
  alert blacklist categories-reputation whitelist
  blacklist
   parameter-map regex bad_domain-bl_
```

```
  !
  categories block
   abortion
   job-search
   shopping
   sports
  !
  block page-profile block-Guest_Access_URL_Policy
  log level error
  reputation
   block-threshold low-risk
  !
  whitelist
   parameter-map regex test4-wl_
  !
 !
 utd global
  logging host 10.2.2.2
 !
!
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

URLF URL Filtering

VPN Virtual Private Network

NAT Network Address Translation

LAN Local Area Network

WAN Wide Area Network

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**.