ıılııılıı cısco

Prescriptive Deployment Guide Cisco Public

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

Prescriptive Deployment Guide

May, 2020

Contents

Introduction	3
Define	5
Design - Cisco SD-WAN Secure Guest Access	8
Prerequisites - Cisco SD-WAN Secure Guest Access	10
Process 1: Successful Deployment of Controllers and WAN Edge Devices	10
Process 2: Enable Local Internet Exit for Guest Traffic using NAT DIA Route	10
Process 3: Upload Software Virtual Image to Enable Snort	12
Process 4: (Optional) Create a Security App Hosting Profile Template	16
Process 5: (Optional) Define Lists for the Security Policy	20
Deploy - Cisco SD-WAN Secure Guest Access	25
Process 1: Create Security Policy	25
Process 3: Attach the Security Policy to the Device Template.	43
Operate - Cisco SD-WAN Secure Guest Access	50
Process 1: Monitor the Enterprise Firewall with Application Awareness Feature via vManage NMS	50
Process 4: Monitor URL Filtering Feature via vManage NMS	60
Process 5: Monitor URL Filtering via Syslog Server	70
Appendix A: New in this Guide	71
Appendix B: Hardware and Software Used for Validation	72
Appendix C: Cisco WAN Edge Configuration Summary (Templates)	73
Appendix D: Glossary	88
Feedback	89

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 <u>Cisco</u> <u>SD-WAN Design Guide</u> for background information and the <u>Cisco SDWAN Deployment Guide</u> 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 <u>Cisco SD-WAN Direct Internet Access Design and</u> <u>Deployment Guide</u>. For details regarding the required licenses to deploy the Cisco SD-WAN security feature set, refer to <u>Cisco DNA Software for SD-WAN and Routing</u>.



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 <u>Cisco SD-</u><u>WAN: Enabling Direct Internet Access</u> 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 <u>Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices</u>.

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.

cisco VM	anage									•	•	ê	4 ³⁵	Ø	admin 👻
DASHBOARD	MAIN DASHBOARD														
3	1 ↑ vSmart - 1	8	16 ↑ /AN Edge - 16		3	1 个 vBond - 1	G	1 ⊘ vManag	e - 1	Reboot Last 24 hrs	2	2	Ŷ	Warning Invalid	0
Control Status (T	otal 15)		_	Site He	ealth (Total 12)				Transpo	rt Interface Dis	stributio	n			
Control Up			15	٢	Full WAN Conne	ctivity		10 sites	< 10 Mk	ops is - 100 Mbps					57 0
Partial 0				0	Partial WAN Con	nectivity		2 sites	100 Mb	ps - 500 Mbps					0
Control Down 0			0	8	No WAN Connec	tivity		0 sites	> 500 Mbps				0		
									View Percent Utilization						
WAN Edge Invent	tory			WAN Edge Health (Total 16)				Transport Health			Type: By Loss	• = 0			
Total			83		\frown			·	100 %						
Authorized			24	((16) 0	0		50%							
Deployed			16				50 %								
Staging			0		Normal	Warning	E	rror	0	• • • • • •	•••	••••	•••	••••	
Top Applications			≂ Ω	Applica	ation-Aware Rout	ing								Type: By	Loss 🗢 🖸
					Tunnel Endpoints		Avg. Latency (r	ms)	Avg. L	oss (%)		Avg.	. Jitter (ms)	
				~	Router:mpls-BR2-V	VAN-Edge2:mpls	0		3.099			0			
No data to display			BR2-WAN-Edge2:mpls-Router:mpls 0				2.341			0					
				~	DC1-WAN-Edge1:n	npls-BR2-WAN-Edge2:mpls	0		2.063			0			
	Control Status (T Control Status (T Control Up Partial Control Down WAN Edge Invent Total Authorized Deployed Staging Top Applications	Cisco vManage DASHBOARD MAIN DASHBOARD Name vSmart - 1 Control Status (Total 15) Control Up Partial Control Down WAN Edge Inventory Total Authorized Deployed Staging Top Applications No data to disp		1 ^ 16 ^ VSmart - 1 X Control Status (Total 15) 16 ^ Control Up 15 Partial 0 Control Down 0 WAN Edge Inventory 16 Total 83 Authorized 24 Delaysed 16 Staging 0 Top Applications = 12 No data to display 10	1 ^ I I ^ I I ^ I I ^ I I ^ I I ^ I I I I I I I I I I I I I I I I I I I	1 ^ vSmart -1 16 ^ WAN Edge - 16 Control Status (Total 15) Site Health (Total 12) Control Up 15 Partial 0 Control Down 0 WAN Edge Inventory WAN Edge Health (Total 12) WAN Edge Inventory WAN Edge Health (Total 12) Total 83 Authorized 24 Deloyed 16 Staging 0 No data to display Application-Aware Rout No data to display R2:WAN Edge In	Image: Cisco vManage DASHBOARD MAIN DASHBOARD Image: Norman L - 1 Image: No	Internet Endpoints Interne	Market Cicco VManage DASHBOARD MAIN DASHBOARD Main of the status (Intal 15) I for the status (Intal 15) Control Up 15 Partial 0 Control Down 0 WAN Edge Inventory 16 Total 83 Authorized 16 Partial 0 0 0 sites WAN Edge Inventory WAN Edge Health (Total 16) 0 0 0 Total 83 Authorized 16 0	Market Cisco vManage DASHBOARD MAIN DASHBOARD Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 Image: 1 <thimage: 1<="" th=""> <thimage: 1<="" th=""> Image: 1</thimage:></thimage:>	Additional product of the	AshHboard Manage DashHboard Manage 1 ^ VSmart-1 2	Algo and a region Algo and a region <th>Algorithment Algorithment Algorithment <th>A Cook Wanage A DSHBOARD I MAN NASHBOARD A DSHBOARD I MAN NASHBOARD A DSHBOARD I MAN NASHBOARD A DASHBOARD I MAN NASHBOARD Control Usatus (Cetal 15) Control Usatus (Cetal 15) Control Usatus (Cetal 15) Control Down Partial MAR Edge Inventory Total A authorized Capapications No data to display No data to display No data to display Normal Wan Edge Integen Reserve Normal Wan Edge Integen Reserve Wan Edge Integen Reserve </th></th>	Algorithment Algorithment <th>A Cook Wanage A DSHBOARD I MAN NASHBOARD A DSHBOARD I MAN NASHBOARD A DSHBOARD I MAN NASHBOARD A DASHBOARD I MAN NASHBOARD Control Usatus (Cetal 15) Control Usatus (Cetal 15) Control Usatus (Cetal 15) Control Down Partial MAR Edge Inventory Total A authorized Capapications No data to display No data to display No data to display Normal Wan Edge Integen Reserve Normal Wan Edge Integen Reserve Wan Edge Integen Reserve </th>	A Cook Wanage A DSHBOARD I MAN NASHBOARD A DSHBOARD I MAN NASHBOARD A DSHBOARD I MAN NASHBOARD A DASHBOARD I MAN NASHBOARD Control Usatus (Cetal 15) Control Usatus (Cetal 15) Control Usatus (Cetal 15) Control Down Partial MAR Edge Inventory Total A authorized Capapications No data to display No data to display No data to display Normal Wan Edge Integen Reserve Normal Wan Edge Integen Reserve Wan Edge Integen Reserve

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 – <u>Security Policy for Cisco IOS-XE SD-WAN Devices</u>.

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.

_	diality circumstances													
≡ .	cisco Cisco vivianage				sada 🖬 👘 🚱 adamin 🕶									
::		ES												
	Device Template	Total	146	149	interface GigabitEthernet0/0/2									
	Branch_C_MPLS_CE_LAN	1	147	150	description INET Interface									
			148	151	no shutdown									
•	Device list (Total: 1 devices)		149	152	arp timeout 1200									
	Filter/Search		150	153	ip address 30.30.1.1 255.255.255.252									
~			151	154	ip redirects									
<u> </u>	ISR4331/K9-FD02012092A		152	155	ip tcp adjust-mss 1350									
	BR3-WAN-Edge1 10.255.241.31		153	156	ip mtu 1500									
				157	ip nat outside									
-			154	158	mtu 1500									
678			155	159	negotiation auto									
			156	160	exit									
			157	161	interface Tunnel0									
			158	162	no shutdown									
			159	163	ip unnumbered GigabitEthernet0/0/0									
			160	164	no ip redirects									
			161	165	ipv6 unnumbered GigabitEthernet0/0/0									
			162	166	no ipv6 redirects									
			163	167	tunnel source GigabitEthernet0/0/0									
			164	168	tunnel mode sdwan									
			165	169	exit									
			166	170	interface Tunnel2									
			167	171	no shutdown									
			168	172	ip unnumbered GigabitEthernet0/0/2									
	Configure Device Rollback Time	er	Back		Configure Devices Cancel									

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	Туре	Variable/Value
Pagia Configuration	VPN	Global	2
Basic Configuration	Name	Global	Service Guest VPN
	Prefix	Device Specific	vpn1_br_static_nat_route_prefix maskbits**
IPv4 Route	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 <u>Cisco SD-WAN: Enabling Direct Internet</u> <u>Access</u>.

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**.

≡	Cisco vManage							•		.	0	admin 👻
::	DASHBOARD MAIN DA	ASHBOARD										
□ \$	Monitor Geography	1 🔀 1 WAN	6 ↑ Edge - 16	•	1 ↑ vBond - 1	1 C	ge - 1	eboot Ist 24 hrs	2	<u> </u>	Warning Invalid	0
ع	Network	2	Site H	ealth (Total 12)			Transport In	nterface Dis	stribution			
÷	Alarms		15	Full WAN Conn	ectivity	10 sites	< 10 Mbps	100 Mbps				57
÷	Events		0	Partial WAN Co	nnectivity	2 sites	100 Mbps - 500 Mbps					0
•••	Audit Log		0	No WAN Connectivity 0 sites			× 000 Mbp	Vie	w Percent Ut	ilization		0
	ACL Log	ACL Log			WAN Edge Health (Total 16)					Туре:	By Loss 🖨	ŦΩ
	Total		83	\frown	\frown	\frown	0 50 %					
	Authorized		24	16	0 (0						
	Staging		0	Normal	Warning	Error	0 •••		• • • • • •		• • • • •	•••
	Top Applications		≂ 🛛 Applic	ation-Aware Ro	uting					Ту	pe: By Loss	¢ 🗆
	No data to display			Tunnel Endpoint	5	Avg. Latency (ms)	Avg. L	Loss (%)		Avg. Jitter (n	ns)	
				Router:mpls-BR2	-WAN-Edge2:mpls	0	1.554		D			
				BR2-WAN-Edge2	mpls-Router:mpls	0	1.25 0					
https://10	0.119.118.21:8443/#/app/monitor/devices,	s/grid	~	DC I-WAN-Edge I	.mpis-okz-waiv-cuge2:mpis	U	1.091			U		

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.

≡	Cisco vManag	;e					● E ¹	4	🕜 ad	min 👻
::		К								
	WAN - Edge 1 Coloca	tion Clusters								
	VPN GROUP	VPN	SEGMENT							
\$	Select VPN Group	▼ All	segments							
عر									00	
2										99
4	Device Group All	- Q		Search Options 🗸					Total Ro	ows: 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	0	reachable	300	-	29	
	😁 vmanage	172.27.0.14	vManage	b8a4fa09-bf86-4b1a-bb9e-9eb80f	0	reachable	400	-	16	
	(vBond	172.27.0.12	vEdge Cloud (vBond)	28a77819-f63a-4a88-b90c-4d81b	0	reachable	600		-	
	8 Router	10.10.23.23	ASR1001-X	ASR1001-X-JAD23151HC8	0	reachable	23	26	3	
	BC1-WAN-Edge2	10.255.241.101	vEdge 5000	193A1104180040	0	reachable	112001	24	3	
	B DC1-WAN-Edge1	10.255.241.102	vEdge 5000	193A1104180039	0	reachable	112001	24	3	
	BR6-WAN-Edge1	192.168.1.1	C1111X-8P	C1111X-8P-FGL231613RW	0	reachable	112010	18	2	
	BR4-WAN-Edge1	100.255.241.41	ISR4351	ISR4351/K9-FD018351QNX	0	reachable	112006	0	2	
	BR4-WAN-Edge-1	10.255.241.51	C1111X-8P	C1111X-8P-FGL231613RX	0	reachable	112003	34	3	
	2 BR3-WAN-Edge1	10.255.211.11	ISR4431	ISR4431/K9-F0C22467A57	0	reachable	111001	26	3	
	BR3-WAN-Edge1	10.255.241.31	ISR4331	ISR4331/K9-FD02012092A	-	reachable	-	-	-	
	BR2-WAN-Edge2	10.255.241.22	ISR4331	ISR4331/K9-FD020110MX6	0	reachable	112007	7 (8)	2	
	BR2-WAN-Edge2	10.255.241.62	ISR4461	ISR4461/K9-FD02316A220	0	reachable	112005	24	3	
	BR2-WAN-Edge1	10.255.241.21	ISR4331	ISR4331/K9-FD020110MX1	0	reachable	112007	0	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.

≡	Cisco vManage				▲ Ê	<u>¢</u> @ Ø	admin 🔫			
	MONITOR Network >	Real Time								
	Select Device 🔹	Select Device BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Device Model: ISR4431 Image: Comparison of Comp								
-	TLOC									
\$	Tunnel		<u> </u>				0e			
عر	Security Monitoring	Q	Search Option	s 🗸			Total Rows: 1			
ĉ	Firewall	Last Updated	Recommended Version↑	Supported Regex	Installed Version	Supported				
*	Intrusion Prevention	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				
	URL Filtering			-						
-	Advanced Malware									
	Protection									
	Umbrella DNS Re-direct									
	Control Connections									
	System Status									
	Events									
	ACL Logs									
	Troubleshooting									
	Real Time									

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

Software Download											
Downloads Home / Routers / Branch Routers / 4000 Series Integrated Services Routers / 4431 Integrated Services Router / IOS XE SD-WAN Software- 16.12.1e											
Search Expand All Collapse All Latest Release) ``	4431 Integrated Services Router Release 16.12.1e ♠ My Notifications	Related Links Release Notes for 1								
All Release	~	File Information	Release Date	Size							
16	>	Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.1e.SPA.bin	12-Nov-2019	619.54 MB	± \: 🖬						
Deferred Release	>	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**.

≡	Cisco vManage				•	€ 1 ≜	🕜 admin 🕶		
8	DASHBOARD MAIN DASHE	BOARD							
□ ≎			6 1 ↑ vBond - 1	t vMana	ge - 1 Reboot	0	Warning O Invalid O		
عر	Control Status (Total 15)		Site Health (Total 11)	Transport Interface Distribution					
ĉ	Maintenance 1	15	Full WAN Connectivity	11 sites	< 10 Mbps 10 Mbps - 100 Mbps		69 0		
*	Software Repository 2	0	9 Partial WAN Connectivity	100 Mbps - 500 Mbps		0			
	Software Upgrade	0	8 No WAN Connectivity	> 500 Mbps		0			
_					Vie	w Percent Utilization			
	Device Reboot		WAN Edge Health (Total 16)		Transport Health	By Loss 💠 \Xi 🖸			
	Security	83	\square	\frown	100 %				
	Authorized Deployed	24 16		0	50 %				
	Staging	0	Normal Warning	Error	0	• • • • • • • • • •	•••••		
	Top Applications	≂ α	Application-Aware Routing			Ţ	/pe: By Loss 💠 🖸		
			Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)		
			Router:mpls-BR2-WAN-Edge2:mpls	0	1.097	0	1		
	No data	to display	BR1-WAN-Edge2:bronze-BR2-WAN-Edge1:bi	0	0.409	0			
			BR2-WAN-Edge2:mpls-Router:mpls	0	0.382	0			

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

≡	cisco vManage				•	ê	¢@	Ø	admin 👻		
::	MAINTENANCE SOFTWARE REPOSITORY										
	Software Images Virtual Images 1										
	2 O Upload Virtual Image O Add Custom VNF Package										
.	vManage 3	Search Options 🗸	arch Ontions					Total Rows: 1			
٩	Remote Server - vManage		Natural English Tara	Income Trans	4-14	Manalan		Ň			
÷	1.0.6_SV2.9.13.0_XE16.12	vmanage	App-Hosting	Lxc	x86_64	Security A	Application	c	isco Sys		
									1000 - 10000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1		

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.

≡	cisco vManage			•	Ê	<u>¢</u> 29	0	admin 🔻
5	MAINTENANCE SOFTWARE REPOSITO	RY						
	Software Images Virtual Images							
~	🕈 Upload Virtual Image 👻 🗲 Add Cu	Upload Virtual Image to vManage	×	-				0
Č	Q		Upload Image (Total:1)					Total Rows: 4
4	Software Version	•	secapp-	ire				Vendo
÷	1.0.8_SV2.9.13.0_XE16.12	_	ucmk9.16.12.01e.1.0.8_SV2.9.13.0_XE16.12.x86_64.tar × 51.84 MB		Secur	ity Applicatio	'n	Cisco 🐽
	1.0.6_SV2.9.13.0_XE16.12				Secur	ity Applicatio	in	Cisco
	1.0.4_SV2.9.11.1_XE16.11	Drag and Drop File			Secur	ity Applicatio	n on	Cisco
		Or Browse 1	2 Upload					

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.

=	Cisco vManage						▲ É	0	<u>4</u>	2	adm	iin 🔻
	CONFIGURATION TE	MPLATES										
-	Device Feature											
-	Orafirmation										0	
*	Configuration		Search Options 🗸							Tota	al Row	ıs: 12
ع	Devices		Description	Туре	Device Model	Feature Templates	Devices Attach	ed	Updated E	By	Las	
÷	Certificates	2	Branch Dual vEdge Hybrid TLOC with INET and LAN-side A	Feature	ISR4331	18	1		admin		17:	•••
	Network Design	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.	•••
•••	Templates 2	S_DIA	Direct Internet Access in hybrid transport branch with TLO_{\cdots}	Feature	ISR4461	19	1		admin		16:	••••
	Policies	nt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LA	Feature	vEdge 1000	20	1		admin		26	
		.0C_Su	Branch Dual vEdge Hybrid TLOC SubInts with MPLS BGP a	Feature	vEdge 1000	20	1		admin		26	•••
	Security		vSmart	Feature	vSmart	9	1		admin		14	•••
	Cloud onRamp for SaaS	_Compl	Branch A with OSPF on the LAN side with MPLS and Intern	Feature	ISR4431	20	1		admin		09:	•••
	Cloud on Ramp for JaaS	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:	•••
	Cloud OnRamp for Colocation	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	•••
https://100	110 110 21:0442/#/app./config/template	davias		_								



≡	cisco VMana	age					•	61	≜ ⁴⁶	0	admin 🝷
		TEMPLATES									
	Device Feature	1									
\$	Add Template	2									0
a.	Template Type Non-Det	fault - Q		Search Op	otions 🗸					Tota	l Rows: 109
	Name	Description	Туре	Device Model	Device Templates	Devices Attached	Updated I	Ву	Last Up	dated	
ĉ	DC_VPN0	DC Transport VPN 0	WAN Edge VPN	C1111-4PLTEEA C11	1	2	admin		23 Jul 2	019 11:58:4	•••
*	Banner_Template	Banner Template	Banner	ISR4331 ISR4321 IS	2	3	admin		19 Nov 3	2018 1:58:5.	
	BR_WAN_Parent_IN	Branch WAN Parent Interfa	WAN Edge Interface	ISR4331 ASR1001-X	0	0	admin		29 Jan 2	2019 4:56:27	7 •••
	ISR4321InterfaceVP	ISR4321InterfaceVPN0	WAN Edge Interface	ISR4321	0	0	admin		19 Nov 3	2018 8:58:4.	
	BR_INT2_SHUT	Branch LAN Interfaces to r	WAN Edge Interface	ISR4331 ISR4321 IS	0	0	admin		11 Dec 2	2018 12:30:.	
	VPN0InterfacecvSm	VPN0InterfacecvSmart	vSmart Interface	vSmart	1	1	admin		14 Nov 3	2018 10:33:.	
	vEdgeIntTest	vEdgeIntTest	WAN Edge Interface	vEdge 1000	0	0	admin		01 Nov 3	2018 1:53:1.	
	BR_LAN_INT2_VRRP	Branch LAN Interface 2 VR	WAN Edge Interface	C1111-4PLTEEA C11	4	4	admin		24 Jul 2	019 3:42:36	
	BR_WAN_Parent_INT	Branch WAN Parent Interface	WAN Edge Interface	C1111-4PLTEEA C11	3	3	admin		07 Aug 2	2019 11:47:.	
	DC_VPN1_BGP	DC VPN1 BGP Template	BGP	C1111-4PLTEEA ISR4	1	2	admin		23 Jul 2	019 11:56:2	
	BR_LAN_INT1_VRRP	Branch LAN Interface 1 VR	WAN Edge Interface	C1111-4PLTEEA C11	4	4	admin		24 Jul 2	019 3:40:50	
	System_Tracker_Te	System Template with Tran	WAN Edge System	ISR4331 ISRv CSR10	0	0	admin		09 Jan 2	2019 1:40:32	2
	test1	test1	Security Policy: UTD	ISR4431	1	1	admin		07 Aug 2	2019 3:15:0.	
	vBondVPNZero	test	WAN Edge VPN	vEdge Cloud	0	0	admin		06 Aug 2	2018 2:09:1.	
	VPN512_Template	VPN 512 Out-of-Band Man	WAN Edge VPN	C1111-4PLTEEA C11	11	12	admin		24 Jul 2	019 4:05:45	
	Security_Template	Security Template	WAN Edge Security	C1111-4PLTEEA C11	11	12	admin		23 Jul 2	019 12:00:2	

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

≡	cisco vManage
	CONFIGURATION TEMPLATES
	Device Feature 1
-	Feature Template > Add Template
	Select Devices
,	Search by device name
	ISR4331
	ISR4351
	ISR4431
	L 15K4451-X
	SR4461
	ISRv
	vEdge 100
	vEdge 100 B
	vEdge 100 M
	vEdge 100 WM
	VEdge 1000

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

≡	cisco vManage			•	É)	<u>¢</u> 40	0	admin 👻
::	CONFIGURATION TEMPLATES							
	Device Feature							
	Feature Template > Add Template							
4	VEdge Cloud							
4	VManage							
÷	Select Template			_				
*	BASIC INFORMATION							
	AAA-CISCO	BFD	Global Settings					
	NTP	OMP	Security					
	Security App Heating	Sustam						
	Security App Hosting	System						
	VPN							
	VPN	VPN Interface Cellular	VPN Interface DSL IPoE					
	VI IX	WAN	WAN					

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

≡ _	cisco vManage					E1	4 4	0	admin 🔻
	CONFIGURATION TEMPL	ATES							
	Device Feature								
	Feature Template > Add Templa	ate > Security App Hosting							
ः २	Device Type	ISR4431							
÷	Template Name 1	Security_App_Hosting_Template	+	 Enter a name for the template 					
	Description 2	Template to customize allocated reso	ources .	Enter a description for the template					
<u>×</u>									
		AMETERS							
	SECONTITIOEIOTTAN								_
	NAT		 - 	On Off					
	December Dec61a								
	Resource Profile		✓	default					
				Save Cancel					

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

≡	Cisco vManage				•	É1	4 40	0	admin 🔻
::	CONFIGURATION TEMPL	ATES							
	Device Feature								
-	Feature Template > Add Templa	ate > Security App Hosting							
ت عر	Device Type	ISR4431							
÷	Template Name	Security_App_Hosting_Template							
*	Description	Template to customize allocated reso	ources						
•	SECURITY POLICY PAR	AMETERS							
	NAT		🖉 🕶 💿 On 🔿 Off] 1					
	Resource Profile		(∰ ✓ ✓ Choose default high	2					
				-					
			3 Save Cancel						

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**.

≡	Cisco vManage						•	Ê	<u>¢</u> 8 Ø	admin 🛨
5	DASHBOARD MAIN DA	ASHBOARD								
□ ☆	Configuration	-1	16 ↑ WAN Edge - 16	۲	1 个 vBond - 1	1 vMana	Reboot Last 24 hrs	2	Warning Invalid	0 0
٩	Devices			Site Health (Total 12))		Transport Interface Distr	ibution		
÷	Certificates		15	Full WAN Cont	nectivity	10 sites	< 10 Mbps 10 Mbps - 100 Mbps			57 0
*	Network Design		0	Partial WAN C	connectivity	2 sites	100 Mbps - 500 Mbps			0
	Templates		0	8 No WAN Conn	ectivity	0 sites	> 500 Mbps			0
	Policies							View Percent Uti	ilization	
				WAN Edge Health (To	otal 16)		Transport Health		Type: By L	oss ♦ = []
	Security		83	\frown		· · ·	100 %			
	Cloud onRamp for SaaS		24	(16)	(0)	(o)				
	Cloud onRamp for laaS		16				50 %			
	Cloud OnRamp for Colocation		0	Normal	Warning	Error	0	••••	•••••	••••
	Top Applications		∓ 0	Application-Aware Re	outing				Type:	By Loss 💠 🖸
				Tunnel Endpoir	nts	Avg. Latency (ms)	Avg. Loss (%)	Avç	g. Jitter (ms)	
				Router:mpls-BF	2-WAN-Edge2:mpls	0	3.099	0		
		No data to display		BR2-WAN-Edge	2:mpls-Router:mpls	0	2.341	0		
				DC1-WAN-Edge	e1:mpls-BR2-WAN-Edge2:mpls	0	2.063	0		

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

≡	cisco vManage		٠	Ê	*	0	admin 👻
::	CONFIGURATION SECURITY				1 -	Custom C	ptions -
	Add Security Policy				😗 Security	/	
-	Q	Search Options 🗸			Lists	2	
	Name	Description	Use Case		Firewall Intrusion Pr	evention	
~	Compliance_Security_Policy	Security policy specific to compliance use case	Compliance		URL Filterin	g	
ŝ					Advanced N	Aalware Pro	tection
**					DNS Securi	ty	
					Umbrella Al	PI Token	
					Threat Grid	API Key	
							_

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.

=	Cisco vManage						▲ É	I 🔎	🕜 adm	in 🔻
::	CONFIGURATION Secur	ity > Define Lists							Eustom Options	s 🕶
	Select a list type on the left and	start creating your groups of interes	t							
*	Application									
a	Data Prefix	Name	Entries	Reference Count	Lindsted By	Last Lindated		Action		
	Domain	NUTTE		Reference count	opdated by	Last optimed		Action		
-	Signatures									
*	Whitelist URLs			No data	available					
	Blacklist URLs									
	Zones									

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.

≡	Cisco vManage						•	â	\$	admin 👻
::	CONFIGURATION Secur	rity > Define Lists							🗰 Cus	tom Options 👻
	Select a list type on the left and	l start creating your	groups of interest							
*	Application	New Data	Prefix List 2							
	Data Prefix 1	_	and a second sec							_
*	Domain	Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated		Action	
÷	Signatures									
*	Whitelist URLs			No dat	a availab	le				
•	Blacklist URLs									
	Zones									

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**.

≡	Cisco vManage					•	8	🥺 📀	admin 🔻
::	CONFIGURATION Securi	ty > Define Lists						🎟 Cus	stom Options 👻
	Select a list type on the left and	start creating your groups of interest							
	Application	✤ New Data Prefix List							
••• •	Data Prefix	Data Prefix List Name	 Enter a name for the 	ne prefix list					
	Domain	Client_Network							
Ê	Signatures	Internet Protocol							
*	Whitelist URLs	● IPv4 ○ IPv6							
•	Blacklist URLs	Add Data Prefix + 2 Ent	ter the data prefix						
	Zones	10.10.0/16							
							3	dd Ca	ncel
		Name Entries		Internet Protocol	Reference Count	Updated By	Last Updated		
				No data	available				

≡	e la	Cisco vManage				•	â	*	? adm	in 🔻
::	4	CONFIGURATION Secu	rity > Define Lists						Custom Options	s •
	5	Select a list type on the left and	d start creating your groups	of interest						
\$		Application	New Data Prefix I	List						
٩		Data Prefix	Name	Entries	Internet Protocol	Reference Count	Updated By	Last	Jpdated	
ŝ		Signatures	Client_Network	10.10.0.0/16	IPv4	0	admin	17 Se	p 2019 4:19:59 PN	1
*		Whitelist URLs								
•		Blacklist URLs								
		Zones								

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**.

≡	Cisco vManage					▲ Ê	4 24	Ø	admin 🔻
::	CONFIGURATION Securi	ity > Define Lists						III Custom	Options 👻
	Select a list type on the left and	start creating your groups	s of interest						
	Application	• New Zone List	2						
**	Data Prefix	Zone List Name	3						
3	Domain	GUEST_VPN	Enter a name for the zone						
÷	Signatures								
÷	Whitelist URLs	2	er the VPN						
	Blacklist URLs							1	
	Zonos					5	Add	Cancel	
	Zones 1								
		Name	Entries	Reference Count	Updated By	Last Updated	Action		
		INSIDE	1	9	admin	23 Sep 2019 4:09:31 PM	/01		
		OUTSIDE	0	7	admin	06 Nov 2019 10:49:15 A	/01		
		GUEST_VPN	2	1	admin	06 Nov 2019 10:50:41 A	/ 🗇 🕯		
									_

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**.

≡	Cisco vManage						â (<mark>.</mark> 89 (🧿 admin 🛩
	CONFIGURATION Securit	ty > Define Lists							Custom Options 👻
	Select a list type on the left and s	start creating your groups of int	erest						
÷	Application	🕀 New Blacklist URL List	2						
3	Data Prefix	Blacklist URL List Name	Enter a name for t	he blacklist URL/ domain Li	ist				
`	Domain	bad_domain							
ĉ	Signatures	Add Blacklist URL 4	Enter the URL/ domain p	attern to be blacklisted					1 Import
*	Whitelist URLs	.*customer.com							
•	Blacklist URLs 1								
	Zones								
							5	Add	Cancel
		Name	Entries	Reference Count	Updated By	Last Updated			

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.

≡	cisco vManage		l 🖨 🕌 @ admin ◄
	B DASHBOARD MAIN DASHBOARD		
□ ¢	1 ↑ 16 ↑ Configuration 1	6 € 1 ↑ vBond - 1 € vMana	Reboot 1 Warning 0 Invalid 0
عر	Devices	Site Health (Total 11)	Transport Interface Distribution
÷	Certificates 15	Full WAN Connectivity 11 sites	< 10 Mbps 57 10 Mbps - 100 Mbps 0
*	Network Design	Partial WAN Connectivity 0 sites	100 Mbps - 500 Mbps 0
•	Templates 0	No WAN Connectivity 0 sites	> 500 Mbps U View Percent Utilization
	Policies	WAN Edge Health (Total 16)	Transport Health Type: By Loss ♦ = □
	Security 2 83	\frown \frown \frown	100 %
	Cloud onRamp for SaaS 24		50 %
	Cloud onRamp for laaS	Normal Warning Error	0
	Cloud OnRamp for Colocation 🗧 🛙	Application-Aware Routing	Type: By Loss ◆ 🕻
		Tunnel Endpoints Avg. Latency (ms)	Avg. Loss (%) Avg. Jitter (ms)
https://10	110 119 71:9442/#/app/config/equity/policies/list	BR1-WAN-Edge2:biz-internet-BR2-WAN-Edg 0	0.551 0

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**.



≡	Cisco vMa	nage		•	Ê	4 4	0	admin 👻
::	CONFIGURATIO	N SECURITY Add Firewall Policy						
▣		Sources	Apply Zone-Pairs	Destinatio	ns			
۰								
٩			0 Rules					
ŝ								
÷								
	Name	Maximum of 32 characters						
	Description	Description of the configuration						
	Sequence Rule	Drag and drop to re-arrange rules						
	Drop		Enabled					1
			Save Firewall Policy CANCEL	-				

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



≡	cisco VM	anage						•	ê	≜ 55	0	admin 👻
55		ON SECU	RITY Edit Firewall Poli	су								
□			Sour	ces	Apply Zone-Pa	airs	Des	stinatior	าร			
\$			Apply Zone-Pair(s)					_	×			
٩,			Target Zone-Pair									
ĉ			Source Zone	Select zone	\rightarrow Destination Zone	OUTSIDE ×	-	•				
*			Course Lone	Search	GUEST_VPN			•				
•	Name	Gue			2							
	Description	Fire		OUTSIDE								
				GUEST_VPN					- 1			
	Sequence Rul	e Drag		New Zone List								
	Drop						Save	Cance	el			1
	1 Rule 1		■ Match Conditions				Actions					
			Source Data Prefix L	ist: Client_N	etwork		Inspect		Enabled			
					Save Firewall Policy	CANCEL						

Step 4. After the zone pair is created, click Save.

=	dudu Cisco vManage								自	▲ 55	0	admin 🔻
::		Y Edit Firewall Policy									Ŭ	
ᅟᅟ		Sources			Apply Zone-Pai	irs	D	estinatio	าร			
\$	Ар	oply Zone-Pair(s)	_				_	-	×			
3		Target Zone-Pair										
*		Source Zone GUEST_V	× ×	\rightarrow	Destination Zone	OUTSIDE x	*	•				
	Name Gue											
	Description Fire											
	Sequence Rule Drag								- 1			
									_			
	Drop						Save	Canc	el			
		Match Conditions Source Data Prefix List:	Client_Net	work			Actions Inspect		Enabled			
				Save	Firewall Policy	CANCEL						

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,

≡	Cisco vMai	nage								Ê	4 50	0	admin 👻
		N SECURITY Add Firewa	all Policy										
			Sources		Apply Zone-Pa	airs		Destination	าร				
\$													
٩,			Apply Zone-Pair(s)	_			_	×					
÷			Source Zone	Select zone	\rightarrow Destination Zone	Select zone			18				
*				Search	INSIDE		To Remove	To Add					
	Name	Maximum of 32 charac		Self Zone	1								
	Description	Description of the conf		INSIDE									
	Sequence Rule	Drag and drop to re-arran		New Zone List	To create a r	new zone list							
		_			i lo cicale a l	2010 130							
	Drop												í.
		_					Save	Cancel					
					Save Firewall Policy	CANCEL							

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.		

≡	cisco VMa	inage				•	Ê	≜ ⁵⁵	0	admin 👻
::		DN SECURITY Edit Firewall Policy								
□		Sources		Apply Zone-Pairs		Destinatio	ons			
*										
3		GUEST_VPN	→	0 Rules	> [(OUTSIDE			
ĉ										
*										
	Name Guest_Access_Firewall Cuest_Access_Firewall Cuest_Access_Firewall									
	Description	Firewall Policy to restrict or allow guest ac	ccess to Internet	Enter a description for the fire	ewall policy					
	3 Sequence Rule 	Drag and drop to re-arrange rules								
	Drop			Enabled						-
				Save Firewall Policy CANC	EL					

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.

	ahah cisco	Cisco vMana	ge						•) ê	≜ 55	0	admin 🔻
::	‡ co	ONFIGURATION	SECURITY Add Firewall Policy										
	Na	me	Guest_Access_Firewall										
\$	De	scription	Firewall Policy to restrict or allow gue	est access to Internet									
عر	•	Sequence Rule	Drag and drop to re-arrange rules										
ĉ	Ru	le 1				M	atch Actions]			•		
*				Source Data Prefix	Source Port	Destination Data Prefix	Destination Port	Protocol	Application/Applicati	on Family List			
•			Match Conditions					Action	S				
								Drop		Enabled			
											Save Match A	nd Actions	Cancel
													_
		Drop			Enable	ed							
						Save Firewall Policy	CANCEL						

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

≡	cisco VManage				● É	a 🔎	0	admin 👻
	CONFIGURATION SECU	RITY Edit Firewall Policy						
□ ≎	Drop	Enabled						1
ې ۲	1 Rule 1	Source Data Prefix Source Port Destination Data Prefix Destination	Match on Port Pro	Actions	cation Family List	1		
*		Match Conditions		Actions				
•		Source Data Prefix List	×	Inspect	Enabled			
		Client_Network ×	*					
		Source: IP Prefix Example: 10.0.0.0/12						
		Protocol Select one or more protocol OR 6 17	×					
						Save Match A	nd Actions	Cancel
		Save Firewall Policy CANCE	EL					

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

≡	cisco Cisco vMa	nage				▲ Ê	* 22	0	admin 🔫
::	CONFIGURATIO	SECURITY Add Firewall Policy							
□	Name	Guest_Access_Firewall							
۵	Description	Firewall Policy to restrict or allow guest access to Internet							
√ €] :í	 Sequence Rule Rule 1 	Drag and drop to re-arrange rules	Mat	h Actions					
•		Match Conditions			Actions Inspect	Enabled			
						2	Save Match A	nd Actions	Cancel
	Drop		Enabled						1
			Save Firewall Policy	CANCEL					

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

≡	ahaha C	Cisco vMana	age						▲ Ê	1	Ø	admin 🔻
	CONF	FIGURATION	SECURI	TY Edit Firewall Policy								
	Name		Guest_	Access_Firewall								
\$	Descrip	ption	Firewal	Il Policy to restrict or allow guest a	access to Internet							
× 4 4 11	Sequence	Drop	Drag and	d drop to re-arrange rules	Enabled	1						1
	1 Rul	le 1		Match Conditions Source Data Prefix List: Source: IP Protocol:	Client_Network 6 17			Actions	Ena	bled		
	2 Rul	le 2		Match Conditions Protocol:	1			Actions Inspect	Ena	bled		
					Sa	ve Firewall Policy	CANCEL					

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.

≡	cisco	Cisco vMan	nage					٠	Ê	A 69	0	admin 🔫
::	\$ co	ONFIGURATION	SECURITY Edit Firewall Policy									
			GUEST_VPN	─ ►	2 Rules		>	OU	TSIDE			
*												
٩	Na	me	Guest Access Firewall									
÷		10 M.O.										
	De	scription	Firewall Policy to restrict or allow guest acce	ess to Internet								
<u>~</u>												
	•	Sequence Rule	Drag and drop to re-arrange rules									
					Actions							
					1 Drop Pass							
		Drop	Enabled									
									2 Save	Match And Action	ons	Cancel
					3 Save Firewall Policy	CANCEL						

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

=	cisco vManage			ê	4 61	0	admin 👻
::	CONFIGURATION Security > Add Security Policy						
▫		Firewall O URL Fil	Itering O Policy Summary				
٠	Add Firewall Policy (Add a Firewall configuration)						0
٩	Q. Search Optio	s 🗸				٦	Fotal Rows: 1
ŝ	Name		Туре				
••	Guest_Access_Firewall_Policy		🕒 zoneBasedFW				•••
``							
11							
			_				
		Next	CANCEL				

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**.

≡	Cisco vManage		🜰 🛱 峰 🍘 admin 🗸
::	CONFIGURATION SECURITY Edit URL Filte	ring Policy	III Custom Options 👻
▫	Target	Policy Behavior	
* 4	1	Block Categories: 4	Blacklist: Enabled
	VPNs	Whitelist URLs: - Action: Redirect URL	Whitelist: Enabled
-		Blacklist URLs: - Block Page Server	Reputation/Category. Enabled
	Target VPNs	Web Filter	Alerts
	URL Filtering - Policy Rule Config Policy Name Guest_Ac Web Categories Block Web Reputation Trustwort Advanced >	guration 3 cess_URL_Policy abortion × shopping × job-search × sports × • hy •	
		Save URL Filtering Policy CANCEL	

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.

≡	Cisco vManage			自	1 ⁵⁰ 0	admin 👻
	CONFIGURATION SECURITY Edit URL	_ Filtering Policy			III Custo	om Options 👻
□ ≎ ∢	Target	Policy Behavior Block Categories: 4 Web Reputation: Trustworthy	Blacklist:	Enabled		
ŝ	VPNs	Whitelist URLs: - Action: Redirect URL	Whitelist: Reputatio	Enabled	Enabled	
**	• Target VPNs	Web Filter		Alerts		
	URL Filtering - Policy Rule Co	onfiguration 🔋				
	Policy Name Gues	st_Access_URL_Policy				
	Web Categories Block	abortion x shopping x job-search x sports x +				
	Web Reputation Allow					
	Advanced >					
		Save URL Filtering Policy CANCEL				

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

≡	cisco vManage		•	Ê	≜ ⁶⁰ Ø	admin 🔫
::	CONFIGURATION SECURITY Edit	URL Filtering Policy			III Cust	om Options 👻
▫	Target	Policy Behavior				
٠		Block Categories: 4				
عر 4	1 VPNs	Web Reputation: Trustworthy Action: Redirect URL	Blacklist: Whitelist:	Enabled		
	VINS	Blacklist URLs: - Block Page Server	Reputation	n/Category:	Enabled	
*	Target VPNs	Web Filter		Alerts		
	URL Filtering - Policy Rule	e Configuration 🚯				
	Policy Name	Guest_Access_URL_Policy				
	Web Categories	Block Block abortion × shopping × job-search × sports ×				
	Web Reputation	Trustworthy Search abortion				
	Advanced >	□ abused-drugs				
		Save URL Filtering Policy CANCEL				

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	of 81-100 is categorized as T I	rustworthy.			
≡	cisco vManage			▲ Ê	1 ⁶⁹ 0	admin 🔫
::	CONFIGURATION SECURITY Edit	dit URL Filtering Policy			III Custo	m Options 👻
	Target		Policy Behavior			
♥ ペ ✿	1 VPNs	Block Categories: 4 Web Reputation: Trustworthy Whitelist URLs: - Blacklist URLs: -	Action: Redirect URL	Blacklist: Enabled Whitelist: Enabled Reputation/Category	: Enabled	
*	Target VPNs	Web Filter	Block Page Server	Alerts		
	URL Filtering - Policy R	High Risk				
	Policy Name Web Categories Web Reputation	Suspicious cy Moderate Risk Low Risk Trustworthy	job-search x sports x •			
	Advanced >					
		Save URL Filt	ering Policy CANCEL			

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.

≡	cisco vManage			•	Ê	1 55	0	admin 👻
::	CONFIGURATION SECURITY Edit URL Filteri	ng Policy					III Custo	m Options 👻
▫	Target		Policy Behavior					
٠		Block Categories: 4						
عر 4		Web Reputation: Trustworthy Whitelist URLs: -	Action: Redirect URL	 Blacklist: Whitelist:	Enabled	r Enabled		
		Blacklist URLs: -	Block Page Server	Reputatio	on/Category:	Enal	bled	
*	Target VPNs	Web Filter			Alerts			
	URL Filtering - Policy Rule Config Advanced ~ Whitelist URL List Select a V Blacklist URL List Select a b	uration 1						
	Search	1	bad_domain					
	block r age derver bad_mail		*customer.com					
		Save URL F	iltering Policy CANCEL					

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.

=	cisco vManage						 	•	â	4 69	Ø	admin 🔻
	CONFIGURATION SECURITY Edit U	URL Filtering Policy									E Custor	n Options 👻
2	Tar	rget				Policy Behavior						
2 ► ₽	T	1 PNs	Block Categories: Web Reputation: Whitelist URLs: Blacklist URLs:	5 6 Trustworthy -		Action: Redirect URL Block Page Server	 Blacklist: Whitelist: Reputation	Enabled Enabled	Enabled			
:]	• Targ	get VPNs	Web	Filter		·		Alerts				
	URL Filtering - Policy Rule (Whitelist URL List Blacklist URL List Block Page Server	Configuration Select a whitelist url list Search										
	Block Page Content Default Content Header Content Body	• New Whitelist Uf	RL List									
				Save URL Filte	ring Po	licy CANCEL						

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.

	cisco vManage									Ê	A 22	0	admin 👻
::	CONFIGURATION SECURITY Edit URL Filt	ering Policy										III Custom	Options 👻
	Target		Policy Behavior										
* * *	VPNs Target VPN	15	Block Categories: 6 Web Reputation: Trustworthy Whitelist URLs: - Blacklist URLs: - Web Filter		Action: Redirect UI Block Page	RL Server		Blacklist: Whitelist: Reputation	Enabled Enabled h/Category: Alerts	Enabled			
ua -	URL Filtering - Policy Rule Conf Block Page Server Block Page Content Block Page Content Block Page Content Block Page Content Content Body Content Body Redirect URL	Access to the req Please contact your I https://www.cisco.c	uested page has been denied Network Administrator										
			Save URL Filte	ring Po	CANCEL								

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.

	cisco vManage			•	ê	4 ⁵⁵	0	admin 🔻
::	CONFIGURATION SECURITY Edit URL Filtering Policy						III Custom	Options 👻
▫	Target		Policy Behavior					
*		Block Categories: 6		Placklist: Enabled				
٩	1 🚽	Web Reputation: Trustworthy	Action: Block Page	 Whitelist: Enabled				
ŝ	VPNs	Whitelist URLs: - Blacklist URLs: -	Block Dage Conver	Reputation/Category:	ry: Enabled			
*	Target VPNs	Web Filter	Block Page Server	Alerts				
	URL Filtering - Policy Rule Configuration • Default Content Header Access to the r Content Body Please contact yo Redirect URL Enter URL Alerts and Logs • Alerts Blacklist Vinit	equested page has been denied						
		Save URL Filte	ering Policy CANCEL					

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

	cisco vManage		📥 🖨 🏓 🍘 a	dmin 🔻
::	CONFIGURATION SECURITY Edit URL Filtering Policy		🚟 Custom Opt	ions 👻
	Target	Policy Behavior		
ت عر ش		Block Categories: 6 Web Reputation: Trustworthy Whitelist URLs: - Action: Block Page	Blacklist: Enabled Whitelist: Enabled	
	VENS	Blacklist URLs: - Block Page Server	Reputation/Category: Enabled	
** ••	Target VPNs	Web Filter	Alerts	
	URL Filtering - Policy Rule Configuration ()			
	Default Content Header Access to the	requested page has been denied		
	Content Body Please contact	our Network Administrator		
	Redirect URL Alerts and Logs			
	Alerts 🗹 Blacklist 🗸 W	nitelist 🗹 Reputation/Category		
		Save URL Filtering Policy CANCEL		

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.

≡	disco vManage			自	▲ 55	Ø	admin 🔻
	CONFIGURATION SECURITY Edit URL Filtering Policy				Ì	Eustom	Options 👻
□	Target	Policy Behavior					
۵		Block Categories: 6					
ج م		Web Reputation: Trustworthy Action: Redirect URL Whitelist: Whitelist URLs: -	Enabled Enabled				
		Blacklist URLs: - Block Page Server	n/Category:	Enabled			
	1 ① Target VPNs	Edit Target VPNs X	Alerts				
	URL Filtering - Policy Rule Configuration Policy Name Guest_URL_Policy Web Categories Block Web Reputation Trustworthy Advanced >	VPNs 2 2 3 Save Changes Cancel					
		Save URL Filtering Policy CANCEL					

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

≡	cisco vManage				•	â	* 20	0	admin 🔻
::	CONFIGURATION Security > Add Security	rity Policy							
▫			Sirewall ORL Filtering	Policy Summary					
٠									0
3	Q	Search Options 🗸							Total Rows: 1
÷	Name	Туре	Reference Count	Updated By					
	Guest_Access_URL_Filtering	🕒 urlFiltering	0	admin	25 Ja	n 2020 12:0	3:46 PM PST		•••
_									
	•								
	BACK		Next	ANCEL					

Procedure 3. Configure Policy Summary

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

C CSC OVMarage C CNCRCURATION Security Policy Quest_Access_Security_Policy C CONRCURATION Security Policy Quest_Access_Security_Policy Frevail UIL: Fittering Ruley Summer; Provide a name and description for your security master policy and configure additional security master policy to save the security master policy configuration. Security Policy Quest_Access_Security_Policy Guest_Access_Security_Dolicy to fitter quest traffic Enter a name for the security master policy Security Policy Settings Frewail Direct Internet Applications Provide a name and description for the security master policy Additional Policy Settings Frewail Direct Internet Applications Prove additional Policy Settings Frewail Direct Internet Applications Prove additional Policy Cuest_Access_Security on the rules with Inspect actions High Speed Logging VPN On Additional addres Protection External Syslog Server VPN One Rever IP 10222 Port 2055 Server IP 10222 Port 20	deale as a second								
© CONFIGURATION Security Policy Quest_Access_Security_Policy Edution Quest_Access_Security_Policy Fereval URL Filtering Preval With Filtering Security Policy Name Quest_Access_Security_Policy Enter a name for the security master policy Enter a description for your security master policy Additional Policy Settings Firevall Firevall <td< th=""><th>cisco vManage</th><th></th><th></th><th></th><th></th><th>•</th><th>Ê</th><th>1⁶⁵</th><th>🍘 admin 🕶</th></td<>	cisco vManage					•	Ê	1 ⁶⁵	🍘 admin 🕶
Prevail URL Filter Prevail Prevail	CONFIGURATION Security > Edit	Security Policy Guest_Access_Security_Policy							Custom Options 👻
Provide a name and description for your security matter policy and onfigure additional security matter policy configuration. Security Policy Name Guest, Access, Security, Policy of fitter guest traffic the security master policy Getting Policy Settings Fitere all Firevall Breed Logging VPN Guest Access Multication and/or VRLF. Fittering and/or Advanced Malware Protection Intrusion Prevention and/or VRLF. Fittering and/or Advanced Malware Protection External Sysiog Server VPN Guest Policy Server VPN Guest Protection Server IP 10.2.2 Port 205		Firewa	all URL Filterin	Policy Summary					
Security Policy Name Guest_Access_Security, Policy Enter a name for the security master policy Security Policy Description Security policy to fitter guest traffic Chdditional Policy Settings Firewall Direct Internet Applications gypass frewall policy and allow all internet traffic to/from VPN 0 TOP SVN Flood Limit gypass frewall policy of or the rules with Inspect action) High Speed Logging VPN on (Applicable only for the rules with Inspect action) Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection External Syslog Server VPN Open 2rever Starter Mode Open 2ncel Supprogramma Supprogramma CANCEL	Provide a name and description for your se	ecurity master policy and configure additional security settings. Clic	k Save Policy to sa	ve the security master policy configuration	I.				
Security Polley Description Security polley to filter guest tarfic	Security Policy Name Gues	st_Access_Security_Policy Enter a name for the security	master policy						
Additional Policy Settings	Security Policy Description Secu	urity policy to filter guest traffic	security master p	olicy					
Additional Policy Settings Firewall Direct Internet Applications Disabled Enter number of sessions High Speed Logging VPN 0 Server IP 10.2.2. Port 2055 Audit Trail Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection External Syslog Server VPN 0 Server IP 10.2.2. 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. Post 2055 2055 2055 Audit Trail Concel Server IP 10.2.2. 2055 </th <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>									
Firewall Direct Internet Applications Bypass firewall policy and allow all Internet traffic to/from VPN 0 TCP SYN Flood Limit Disabled Enter number of sessions High Speed Logging VPN 0 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 Failure Mode Open Preview Save Policy Changes CANCEL	Additional Policy Settings								
Direct Internet Applications Bypass firewall policy and allow all Internet traffic to/from VPN 0 TCP SYN Flood Limit Disabled High Speed Logging VPN 0 Server IP 10.2.2 Port Audit Trail Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection External Syslog Server VPN 0 Server IP 10.2.2 Prote 2055 Cancel 2055	Firewall								
TCP SYN Flood Limit Disabled Enter number of sessions High Speed Logging VPN 0 Server IP 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 Port VPN VPN 0 CANCEL	Direct Internet Applications	Bypass firewall policy and allow all Internet traffic to/f	rom VPN 0						
High Speed Logging VPN 0 Server IP 10.2.2.2 Port 2055 Audit Trail ••• 0 (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 • Preview Save Policy Changes CANCEL	TCP SYN Flood Limit	Disabled Enter number of sessions							
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 10.2.2.2 Failure Mode Open • Preview Save Policy Changes CANCEL CANCEL	High Speed Logging	VPN 0	Server IP	10.2.2.2	Port	2055			
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 Preview Save Policy Changes CANCEL	Audit Trail	On (Applicable only for the rules with Inspect act	ion)						
Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection External Syslog Server VPN 0 Server IP 10.2.2. Failure Mode Open Preview Save Policy Changes CANCEL		-							
External Syslog Server VPN 0 Server IP 10.2.2.2 Failure Mode Open Preview Save Policy Changes CANCEL	Intrusion Prevention and/or URL Filterin	ng and/or Advanced Malware Protection							
Failure Mode Open Preview Save Policy Changes CANCEL	External Syslog Server	VPN 0	Server IP	10.2.2.2					
Preview Save Policy Changes CANCEL	Failure Mode	Open 👻							
Preview Save Policy Changes CANCEL									
		Preview	Save Policy (Changes CANCEL					

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.

≡	cisco vManage			•	Ê	A 22	0	admin 🔻
::	CONFIGURATION Security > Edit Security Policy Guest_Access_Security_Policy						III Custom	Options 👻
▣		Firewall URL Filterin	g Policy Summary					
٢	Provide a name and description for your security master policy and configure additional	security settings. Click Save Policy to se	we the security master policy configuratio	n.				
٩	Security Policy Name Guest_Access_Security_Policy							
÷	Security Policy Description Security policy to filter guest traffic							
*								
678	Additional Policy Settings							
	Firewall							
	Direct Internet Applications Bypass firewall policy and allow	all Internet traffic to/from VPN 0						
	TCP SYN Flood Limit Disabled Enter number of	essions						
	1 High Speed Logging VPN 0	Server IP	2	Port 2055	3		٦	
	Audit Trail	4						
	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 🔻							
		Preview Save Policy	Changes CANCEL					

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**.

	cisco vManage	▲ Ê	🔎 🕜 adr	
::	CONFIGURATION Security :	Edit Security Policy Guest_Access_Security_Policy	Eustom Optio	ns 👻
		Firewall URL Filtering Policy Summary		
*	Provide a name and description for	your security master policy and configure additional security settions. Click Save Policy to save the security master policy configuration		
*		you seeiny make poncy are compare administration of a second second second second makes poncy comparation.		
٩	Security Policy Name	Guest_Access_Security_Policy		
ĉ	Security Policy Description	Security policy to filter guest traffic		
*				
m	Additional Policy Setting	38		
	Firewall			
	Direct Internet Applications	Bypass firewall policy and allow all Internet traffic to/from VPN 0		
	TCP SYN Flood Limit	Disabled Enter number of sessions		
	High Speed Logging	VPN 0 Server IP 10.2.2 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		
	Failure Mode	Open 💌		
		Preview Save Policy Changes CANCEL		

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 <u>Security Policy Design Guide for</u> <u>Cisco IOS-XE SD-WAN Devices</u>.

≡	Cisco vManage							•	Ê	1 58	0	admin 🔫
::	CONFIGURATION Secur	rity > Edit Secur	rity Policy Secu	re_DIA_Security_Policy							III Custor	n Options 👻
□			Firewall	Intrusion Prevention	URL Filtering	Advanced Malware Protection	DNS Security	Policy Summary				
\$	Provide a name and description	for your security	y master policy	and configure additior	al security settir	ngs. Click Save Policy to save t	he security master	r policy configuratio	n.			
عر	Security Policy Name	Secure_DIA_Sec	curity_Policy									
÷	Security Policy Description	Policy to secure	e Internet traffic									
*												
	TCP SYN Flood Limit		Disa	bled Enter number	of sessions							
	High Speed Logging		VPN 0			Server 10.2.2.2		Po	rt 2	055		
	Audit Trail	Audit Trail On (Applicable only for the rules with Inspect action)										
	Intrusion Prevention and/or U	JRL Filtering and	/or Advanced N	Nalware Protection								
	External Syslog Server		Close			Server IP 1	0.2.2.2					
	Failure Mode		Open									
				P	review Sav	e Policy Changes CANC	EL					

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

≡	cisco vManage		Ê	4 55	0	admin 👻
::	CONFIGURATION Security	Edit Security Policy Guest_Access_Security_Policy			I Custom	Options 👻
		Firewall URL Filtering Policy Summary				
\$	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.				
عر	Security Policy Name	Guest_Access_Security_Policy				
÷	Security Policy Description	Security policy to filter guest traffic				
	Additional Policy Setting	15				
	Firewall					
	Direct Internet Applications	Bypass firewall policy and allow all Internet traffic to/from VPN 0				
	TCP SYN Flood Limit	Disabled Enter number of sessions				
	High Speed Logging	VPN 0 Server IP 10.2.2 Port 2055				
	Audit Trail	On (Applicable only for the rules with Inspect action)				
	Intrusion Prevention and/or URL	iltering and/or Advanced Malware Protection				
	External Syslog Server	VPN 0 Server IP 10.2.2				
	Failure Mode	Open				
		Preview Save Policy Changes CANCEL				

Step 6. Finally, click Save Policy Changes.

≡	cisco vManage	•	Ê	4 55	Ø	admin 🔻
::	CONFIGURATION Security > Edit Security Policy Guest_Access_Security_Policy				Custom	Options 👻
	Config Preview Config Diff					
≎ ∢ ⊕ ≍	policy url-filtering Guest_Access_URL_Policy web-category-action block web-categories abortion shopping job-search sports block-threshold trustworthy block text "<![CDATA[<h3>Access to the requested page has been denied</h3><p>Please contact your Network Administrator< logging host 10.2.2.2 vpn 0 alert categories-reputation blacklist whitelist target-vpns 2	/p>]]:	>"			
	<pre>i zone-based-policy Guest_Access_Firewall sequence 1 match source-data-prefix-list Client_Network protocol 6 17 i action inspect i sequence 11 match protocol 1 action inspect i conc GUEST_VPN vpn 2 i zone GUEST_VPN vpn 0 vn 0</pre>					
	Save Policy Changes BACK					

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.

≡	cisco vManage				Ê	. <mark>≜</mark> 62 Ø	admin 🔻
	CONFIGURATION TE	MPLATES					
	Device Feature						
٠	Configuration 1						
૨	Devices	Sea	arch Options 🗸				Total Rows: 15
			Description	Туре	Device Model	Feature Templates	
ĉ	Certificates	.OC_SubInt_OSPF	Branch Dual vEdge Hybrid TLOC Su	Feature	vEdge 1000	20	
	Network Design	nt_OSPF	Branch Dual vEdge Hybrid TLOC Su	Feature	vEdge 1000	20	
1	-	S_DIA	Direct Internet Access in hybrid tran	Feature	ISR4461	20	
	Templates 2	LDCA	Branch A with OSPF on the LAN sid	Feature	ISR4431	20	
	Policies		vSmart	Feature	vSmart	9	•••
		et_LAN_OSPF	Branch Dual WAN Edge router with	Feature	ISR4351	11	
	Security	C_VRRP	Branch Dual vEdge Hybrid TLOC wit	Feature	ISR4331	20	
	Cloud onRamp for SaaS	SPF	Branch with Dual WAN with Hybrid t	Feature	ISR4331	17	
		SPF	Branch with Dual WAN with Hybrid t	Feature	ISR4331	20	
	Cloud onRamp for laaS	Compliance	Branch A with OSPF on the LAN sid	Feature	ISR4431	20	
	Cloud OnRamp for	>	Branch Dual vEdge Hybrid TLOC wit	Feature	ISR4331	19	
	Colocation		DC MPLS and INET - Static to CE an	Feature	vEdge 5000	16	
	Branch_C_MPLS_TLOC_IN	ET_DIA	Direct Internet Access in hybrid tran	Feature	ISR4461	20	
	Branch_B_INET_TLOC_Sub	Int_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.

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).

	Cisco vManage					•	Ê	4 ⁵⁵	?	admin 🔫
		LATES								
	Basic Information	Transport & Management VPN	Service VPN	Cellular	Additional Templates					
*	Global Template	Choose	•							
≺ ≞	Policy	Choose	•							
÷	Probes	Choose	•							
	SNMP	SNMP_Template	-							
	WAAS Container Profile	Choose	•							
	Security Policy	Guest_Access_Security_Policy	•							
	Container Profile *	Security_App_Hosting	• 0							
	Switch Portxxx 🕒 Switch	Port 👻								
	UCSE Module 🔮 UCSE 👻									
				Update	Cancel					

Step 4. Click Update to update the device template.

≡	Cisco vManage					•	Ê	4 0	0	admin 🔫
::	CONFIGURATION TEMP	LATES								
□	Basic Information Security *	Transport & Management VPN Security_Template	Service VPN	Cellular	Additional Templates					
۵										
٩										
÷	Transport & Managen	nent VPN								
*	VPN 0 *	BR_VPN0_single_transport	•			Addition	al VPN 0	Template	es	
•	BGP	BR_VPN0_Branch	- 0			BGP OSPF				
	VPN Interface	BR_INET_INT	• 0			VPN InVPN In	terface Cel terface Mu	lular Itilink Contro	oller	
	VPN Interface	BR_MPLS_INT	- 0			VPN InVPN In	terface Eth terface DSI	ernet PPPoE L IPoE	Ξ	
	VPN Interface	BR_LAN_Parent_INT	- 0			VPN In VPN In VPN In	terface DSI terface DSI	L PPPoA L PPPoE		
						VPN InVPN In	terface T1- terface	E1-Serial		
	VPN 512 *	VPN512_Template	•			Addition	al VPN 5	i12 Templ	lates	
	VPN Interface	VDNE12 Interface				O VPN In	terface SVI	ĺ		
			Upda	te Cancel						

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**.

CONFIGURATION TEMPLATES	1			
Device Template Branch_A_	_Hybrid_Transport_Compliance			
-				
Q	Search Options 🗸			Total
S Chassis Number	System IP Hostname	Interface Name(vpn1_lan_int2_gex x_or_ gex x.VLAN)	IPv4 Address(vpn1_l	an_int2_i
ISR4431/K9-F0C22467A57	10.255.211.11 BR3-WAN-Edge1	GigabitEthernet0/0/0.20	10.10.12.2/30	
			2 Edit De	vice Terr
		•		
	Next	Cancel		
Cisco vManage			e 📶 🗛	9
CONFIGURATION TEMPLAT				
La construction de la constructi	Jpdate Device Template		×	
Device Template Branch_	Jpdate Device Template Variable List (Hover over each field for more information)		×	
Device Template Branch_	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits)	10.30.1.1/30	×	
Device Template Branch_	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT	10.30.1.1/30	×	
Device Template Branch_	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference)	10.30.1.1/30	×	Total
Device Template Branch_	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_mtu)	10.30.1.1/30 200 1500	X IPv4 Address(vpn1_la	Total an_int2_ip
Device Template Branch. Q S Chassis Number ISR4431/K9-F0C22467A57	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_mtu) Shutdown(vpn0_mpls_int_shutdown)	10.30.1.1/30 200 1500	X IPv4 Address(vpn1_la 10.10.12.2/30	Total an_int2_i
Device Template Branch_ Q S Chassis Number ISR4431/K9-FOC22467A57	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Shutdown(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	10.30.1.1/30 200 1500	X IPv4 Address(vpn1_k 10.10.12.2/30	Total an_int2_ip
Device Template Branch_ Q. S Chassis Number ISR4431/K9-F0C22467A57	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_mtu) Shutdown(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	10.30.1.1/30 200 1500 1000000 1000000	X IPv4 Address(vpn1_la 10.10.12.2/30	Total an_int2_ip
Q S Chassis Number ISR4431/K9-FOC22467A57	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_mtu) Shutdown(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_qex)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1	X IPv4 Address(vpn1_k 10.10.12.2/30	Total an_int2_i;
Device Template Branch.	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_mtu) Shutdown(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthemet0/0/1 30.60.1.1/30	X IPv4 Address(vpn1_la 10.10.12.2/30	Total
Device Template Branch.	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits) NAT	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1 30.60.1.1/30 ¥	X IPv4 Address(vpn1_la 10.10.12.2/30	Total
Device Template Branch.	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Shutdown(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthemet0/0/1 30.60.1.1/30 21 100	X IPv4 Address(vpn1_k 10.10.12.2/30	Total
Device Template Branch.	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn0_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_int_i)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1 30.60.1.1/30 21 100 100	X IPv4 Address(vpn1_Lt 10.10.12.2/30	Total
Device Template Branch_	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_mtu)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1 30.60.1.1/30 ☑ 1 100 1500	X IPv4 Address(vpn1_k 10.10.12.2/30	Total
Q S Chassis Number ISR4431/K9-F0C22467A57	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_mtu) Shutdown(vpn0_inet_int_shutdown) Bandwidth Upstream(vpn0_inet_int_shutdown)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1 30.60.1.1/30 ☑ 1 100 1500 □	X IPv4 Address(vpn1_k 10.10.12.2/30	Total
Device Template Branch.	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_int_shutdown) Bandwidth Upstream(vpn0_inet_int_bandwidth_up) Shutdown(vpn0_inet_int_shutdown) Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1 30.60.1.1/30 ☑ 1 100 1500 ☑ 1 1000000 1000000	X IPv4 Address(vpn1_la 10.10.12.2/30	Total an_int2_ip
Device Template Branch	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPv4 Address(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_int_shutdown) Bandwidth Upstream(vpn0_inet_int_bandwidth_up) Bandwidth Upstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1 30.60.1.1/30 ☑ 1 100 1500 □ 1 100 1500	X IPv4 Address(vpn1_la 10.10.12.2/30	Total
Device Template Branch.	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPV4 Address(vpn0_inet_int_gex) IPV4 Preference(vpn_if_tunnel_ipsec_preference) IP mTU(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_int_shutdown) Bandwidth Upstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthemet0/0/1 30.60.1.1/30 1 100 1500 1 1000 1500 1 1000000 BR3-WAN-Edge1	X IPv4 Address(vpn1_k 10.10.12.2/30	Totall
Device Template Branch.	Jpdate Device Template Variable List (Hover over each field for more information) IPv4 Address(vpn0_mpls_int_ip_addr_maskbits) NAT Preference(vpn.if_tunnel_ipsec_preference) IP MTU(vpn0_mpls_int_shutdown) Bandwidth Upstream(vpn0_mpls_int_bandwidth_up) Bandwidth Downstream(vpn0_mpls_int_bandwidth_down) Interface Name(vpn0_inet_int_gex) IPV4 Address(vpn0_inet_int_gex) IPV4 Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_int_ip_addr_maskbits) NAT Preference(vpn_if_tunnel_ipsec_preference) IP MTU(vpn0_inet_int_shutdown) Bandwidth Upstream(vpn0_inet_int_bandwidth_up) Bandwidth Upstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up) Bandwidth Downstream(vpn0_inet_int_bandwidth_up)	10.30.1.1/30 200 1500 1000000 1000000 GigabitEthernet0/0/1 30.60.1.1/30 1 100 1500 1 100 1500 8R3-WAN-Edge1 37.409284	X IPv4 Address(vpn1_k 10.10.12.2/30	Total an_int2_ip

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.

≡	- di Ci	sco vManage				•	ê	¥@	Ø	admin 👻				
::	φ	CONFIGURATION TEMPLATES												
	D	Device Template Branch_A_Hybrid_T	ransport_Complia	nce										
*										00				
		Q	Search Optio	ns 🗸					Image: Weight of the second					
		S Chassis Number	System IP	Hostname	Interface Name(vpn1_lan_int2_gex x_or_gex x.VLAN)			IPv4 Address(vpn1_lan	_int2_ip_				
-		SR4431/K9-F0C22467A57	10.255.211.11	BR3-WAN-Edge1	GigabitEthernet0/0/0.20			10.10.12.2/30						
*														
					•									
				Next	Cancel									

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.

≡	cisco vManage				•	â	4 49	0	admin 👻
::	CONFIGURATION TEMPLATES								
	Device Template T Branch_A_Hybrid_Transp	Config Preview Config Diff							Intent
۵	Device list (Total: 1 devices)	viptela-system:system	l.						
٩	Filter/Search	host-name BR3-WAN-Edge1 gps-location latitude 37.409284	•						
÷	ISR4431/K9-F0C22467A57 BR3-WAN-Edge1 10.255.211.11	gps-location longitude -97.335 device-groups DC ISR4331 Pri system-ip 10.255.211.11	imary UG3 US West						
*		overlay-id 1 site-id 111001							
		port-offset 0 control-session-pps 300 admin-tech-on-failure sp-organization-name "ENB-Solutions port-hop track-transport track-default-gateway console-baud-rate 115200 vbond 10.10.60.2 port 12346 logging	5 - 21615" 5 - 21615"						
		disk enable ! no cft-enable no cft-cache-enable ! bfd color mpls hello-interval 1000 no_pmtu-discovery							
	Configure Device Rollback Timer	Back	2	Configure Devices	Cancel				

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.

≡	olio CIS	ulu ico	Cisco vManage						•	ê	4	0	admin 👻
::	Ê	TA	SK VIEW										
	Push Feature Template Configuration 🖉 Validation Success 🔹 Initiated By: a										By: admin	From: 10	D.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] Validate messages to vmanage(s)												
÷													
*		~	Status	Message	Chassis Number	Device Model	Hostname BP3-WAN-Edge1	System IP	Sit	e ID	1	Manage IP	
			[20-Sep-2019 11:45:5] [20-Sep-2019 11:45:5] [20-Sep-2019 11:46:11 [20-Sep-2019 11:46:11] [20-Sep-2019 11:46:14] [20-Sep-2019 11:46:4] [20-Sep-2019 11:46:4]	7 PDT] Configuring device with feature template: 7 PDT] Generating configuration from template 9 PDT] Checking and creating device in vManage 9 PDT] Device is online 9 PDT] Updating device configuration in vManage 5 PDT] Pushing configuration to device 7 PDT] Template successfully attached to device	Branch_A_Hybrid_Tran	nsport_Compliance						^	v

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**.

≡	Cisco vManage				•	Ê	" ⁶⁹ Ø	admin 👻
	Dashboard 1	SHBOARD						
□	Main Dashboard	1 6 个	1↑	– 10	Reboot	2	Warning	0
\$	VPN Dashboard	WAN Edge - 1	6 vBond - 1	vManag	e - 1 Last 24 hrs	2	4 P Invalia	0
عر	Security 2		Site Health (Total 11)		Transport Interface Dist	ribution		
÷	Control Up	15	S Full WAN Connectivity	1 sites	< 10 Mbps			57
*	Partial	0	9 Partial WAN Connectivity	10 sites	10 Mbps - 100 Mbps 100 Mbps - 500 Mbps			0
67	Control Down	0	8 No WAN Connectivity	0 sites	> 500 Mbps			0
					Vie	ew Percent Uti	lization	
	WAN Edge Inventory		WAN Edge Health (Total 16)		Transport Health		Type: By Loss	♦ 〒 □
	Total	83	\frown	\frown	100 %			<u> </u>
	Authorized	24	(16) (0)	0	50 %			
	Deployed	16			50%			
	Staging	0	Normal Warning	Error		••••	•••••	
	Top Applications	∓ 0	Application-Aware Routing				Type: By Lo	ss 💠 🖸
		1	Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Av	rg. 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.

≡	cisco VManag	e			•	Ê	1 00	0	admin 🔻
•	FireWall Enforcements	eWall Enforcement: Inspected spected Dropped Chart Details			1h 3h 6h	12h <mark>24h</mark> 7d	×	Blocked	Allowed 👳 🕄
: B	0 Nov 24, 18:0	٩	Search Options 🗸			Total Rows: 4	9	Ne	ws and Media
		Entry Time 25 Nov 2019 4:30:00 PM PST		Firewall Inspected Count 9					
	Advanced Malware	25 Nov 2019 4:00:00 PM PST		296					
	2	25 Nov 2019 3:30:00 PM PST		1219					
	cious	25 Nov 2019 3:00:00 PM PST		546			1		
	es	25 Nov 2019 2:30:00 PM PST		139					
	EIII FIII	25 Nov 2019 2:00:00 PM PST		202					
	dumb	25 Nov 2019 1:30:00 PM PST		103					
	- 0 ••••••• Nov 24, 18:0	25 Nov 2019 1:00:00 PM PST		722					
		25 Nov 2019 12:30:00 PM PST		1249			1.1		
		25 Nov 2019 12:00:00 PM PST		1456					
		25 Nov 2019 11:30:00 AM PST		1734			1.1		
		25 Nov 2019 11:00:00 AM PST		1888					
		25 Nov 2019 10:30:00 AM PST		1893			1.1		

	cisco VMana	ge			▲ ₿ 4	🐌 👩 admin 🕶
	DASHBOARD S	ireWall Enforcement: Dropped			×	
ц Ф	FireWall Enforceme	Inspected Dropped			1h 3h 6h 12h <mark>24h</mark> 7days	Blocked Allowed 👳 🕻
√ \$I	1 K	Chart Details	Search Ontions y		Total Rows: 49	 reputation_block News and Media Shopping
	Z 0 Nov 24, 18:0	Entry Time		Firewall Dropped Count		
		25 Nov 2019 4:30:00 PM PST		240		
	Advanced Malware	25 Nov 2019 4:00:00 PM PST		1990		
	2	25 Nov 2019 3:30:00 PM PST		5036		
	cious	25 Nov 2019 3:00:00 PM PST		2004		
	Mali	25 Nov 2019 2:30:00 PM PST		1806		
	Fill	25 Nov 2019 2:00:00 PM PST		1810		
	Numt	25 Nov 2019 1:30:00 PM PST		1203		
	Nov 24, 18:0	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 n	nonitor.									

≡	Cisco vManage				•	ê 🍂	9 0	admin 🔫
86	DASHBOARD MAIN DASH	IBOARD						
□	Monitor 1	16 ^	▲ 1↑	10	Reboot	2	Warning	0
۵	Geography	WAN Edge - 1	6 vBond - 1	vManage	e - 1 Last 24 hrs	2		Ū
٩	Network 2		Site Health (Total 12)		Transport Interface [Distribution		
÷	Alarms	15	S Full WAN Connectivity	10 sites	< 10 Mbps			57
	Events	0	9 Partial WAN Connectivity	2 sites	10 Mbps - 100 Mbps 100 Mbps - 500 Mbj	s ps		0
	Audit Log	0	8 No WAN Connectivity	0 sites	> 500 Mbps			0
					V	/iew Percent Utiliz	ation	_
	ACL Log		WAN Edge Health (Total 16)		Transport Health		Type: By Loss	♦ = 0
	Total	83	\cap	\frown	100 %			
	Authorized	24	(16) 0	0	50 %			
	Deployed	16			30 %			
	Staging	0	Normal Warning	Error	0 •••••	• • • • • • • •	•••••	••••
	Top Applications	≂ Ω	Application-Aware Routing				Type: By Lo	ss 🗢 []
			Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg	. Jitter (ms)	
			Router:mpls-BR2-WAN-Edge2:mpls	0	1.554	0		
	No data	a to display	BR2-WAN-Edge2:mpls-Router:mpls	0	1.25	0		
			DC1-WAN-Edge1:mpls-BR2-WAN-Edge2:mpls	0	1.091	0		
https://10	0.119.118.21:8443/#/app/monitor/devices/grid							

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

≡	cisco vMana	ge					● É ¹	1	? a	idmin 👻
		RK								
	WAN - Edge 1 Coloca	ation Clusters								
ш.	VPN GROUP	VPN	SEGMENT							
\$	Select VPN Group		segments							
a										
										90
\$	Device Group All	- Q		Search Options 🗸					Total I	Rows: 18
*	HostnameΨ	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	
-	😵 vsmart	172.27.0.13	vSmart	c44d2744-de58-48f1-8e61-3d655	0	reachable	300	-	29	
w	😁 vmanage	172.27.0.14	vManage	b8a4fa09-bf86-4b1a-bb9e-9eb80f	0	reachable	400	-	16	
	() vBond	172.27.0.12	vEdge Cloud (vBond)	28a77819-f63a-4a88-b90c-4d81b	0	reachable	600		-	
	Router	10.10.23.23	ASR1001-X	ASR1001-X-JAD23151HC8	0	reachable	23	26	3	_
	B DC1-WAN-Edge2	10.255.241.101	vEdge 5000	193A1104180040	0	reachable	112001	24	3	
	B DC1-WAN-Edge1	10.255.241.102	vEdge 5000	193A1104180039	0	reachable	112001	24	3	_
	BR6-WAN-Edge1	192.168.1.1	C1111X-8P	C1111X-8P-FGL231613RW	0	reachable	112010	18	2	
	BR4-WAN-Edge1	100.255.241.41	ISR4351	ISR4351/K9-FD018351QNX	0	reachable	112006	0	2	_
	BR4-WAN-Edge-1	10.255.241.51	C1111X-8P	C1111X-8P-FGL231613RX	0	reachable	112003	34	3	
	BR3-WAN-Edge1	10.255.211.11	ISR4431	ISR4431/K9-F0C22467A57	0	reachable	111001	26	3	_
	BR3-WAN-Edge1	10.255.241.31	ISR4331	ISR4331/K9-FD02012092A	-	reachable		-	-	
	BR2-WAN-Edge2	10.255.241.22	ISR4331	ISR4331/K9-FD020110MX6	0	reachable	112007	7 (8)	2	
	BR2-WAN-Edge2	10.255.241.62	ISR4461	ISR4461/K9-FD02316A220	0	reachable	112005	24	3	
	2 BR2-WAN-Edge1	10.255.241.21	ISR4331	ISR4331/K9-FD020110MX1	0	reachable	112007	0	2	
	·	10.05.044.04	100.11/1	100 11/1 /// FD 0001 / 1010	-		110005	~ 1	~	

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.

≡	Cisco vManage						ê 📫	@	admin 🔻
::	MONITOR Network >	 Firewall Policy 							
	Select Device 🔹	BR2-WAN-Edge1 10.255.241.21 Sit	te ID: 112007 Device Mod	lel: ISR4331 🕕					
<u> </u>	Interface					1	lh 3h 6h 12h 2	4h <mark>7days</mark> Cu	ustom 👻
\$	TCP Optimization	9.54 MB			_				
٩	WAN Throughput	976.56 KB				DIA_Firewa Byte Tran	all_Policy::INSIDE:C .nsferred: 92.29 KB	UTSIDE	
ŝ	Flows	97.66 KB							
*	Top Talkers	9.77 КВ ЕВТ 1000 В							
•	WAN	100 B							
	TLOC	10 B							
	Tunnel	0							
	Security Monitoring		Com		Dia.		Olari		
	Firewall								
	Intrusion Prevention							9	90
	URL Filtering	Q		Search Options 🗸				Total I	Rows: 3
	Advanced Malware	Policies	Source Zone	Destination Zone	Sequence Count	No. of Bytes Transferred			
	Protection	DIA_Firewall_Policy_copy	INSIDE	OUTSIDE	3	5227327			
	Umbrella DNS Re-direct	DIA_Firewall_Policy	INSIDE	OUTSIDE	2	94505			1.77 %
		Compliance_FW_Policy_copy	INSIDE	INSIDE	2	28195			0.53 %
	Control Connections								
	System Status								
	Events								

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**.

≡	Cisco vManage	2				•	Ê	" 19	0	admin 🔻
::	MONITOR Network	 Firewall Policy 								
	Select Device 🔫	BR2-WAN-Edge1 10.	255.241.21 Site ID: 112007	Device Model: ISR4331						4
-	Interface						1h 3h	6h 12h	24h 7days	Custom -
\$	TCP Optimization	9.54 MB				Start date and time B 11-24-2019 00:00 Image: Comparison of the second	End date and time 11-25-2019 0	6:06	DONE	CANCEL
۹.	WAN Throughput	976.56 KB			DIA Firewall Policy copy::INSIDE:OUTSID	1 E		2	3	•
ĉ	Flows	97.66 KB			Byte Transferred: 2.15 MB					
*	Top Talkers	9.77 KB 1000 В								
	WAN	Bytes 100 B								
	TLOC	10 B								
	Tunnel	0								
	Security Monitoring				Ø.b.					
	Firewall									~~
	Intrusion Prevention									O
	URL Filtering	Q		Search Options 🗸					T	otal Rows: 1
	Advanced Malware	Policies	Source Zone	Destination Zone	Sequence Count	No. of Bytes Transferred				
	Protection	DIA_Firewall_Po	licy INSIDE	OUTSIDE	3	2255921				100.00 %
	Umbrella DNS Re-direct									
	Control Connections									
	System Status									
	Events									

Step 5. Click on **Real Time** from the left pane of the monitor dashboard. Within **Network** > **Real time**, a popup 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	2					Ê	4 53	0	admin 👻
	MONITOR Network :	> Real Time								
	Select Device 🔫	BR3-WAN-Edge1 1	0.255.211.11 Site ID: 111001 Device Model: IS	SR4431 🚺						
•	Security Monitoring	Device Options:		2						
عر	Firewall	0	Policy QoS Scheduler Information Policy Rewrite Associations						Tot	co ral Rows: 10
"	Intrusion Prevention	Q	Policy Zone Based Drop Statistics	ions 🗸					101	
	URL Filtering	Property Device groups	Policy Zone Pair Sessions Policy Zone Pair Statistics		Value	s+"]				11
	Advanced Malware Protection	Domain ID	Pair Wise Key IPSEC Local SA Entry Pair Wise Key IPSEC Inbound Connections	s	1	ir j				
		Hostname	Pair Wise Key IPSEC Outbound Connection	n	BR3-WAN-Edge1					
	Umbrella DNS Re- direct	Last Updated	Reboot History		24 Sep 2019 11:15:48 AM PDT					
		Latitude	Security Information		37.409284					
	Control Connections	Longitude	Smart License Registration Info Smart License UDI Info		-97.335					
	System Status	Personality	Smart License Privacy Info		WAN Edge					
	Events	Site ID	Smart License Evaluation Info		111001					
		Timezone	Smart License Usage		PDT -0700					
	ACL Logs	Vbond			10.10.60.2					
	Troubleshooting									
	Real Time 1									

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.

≡	Cisco vManage					•	ê	1 53	Ø	admin 🔻
::	MONITOR Network >	Real Time								
	Select Device 👻	BR3-WAN-Edge1 10.255.211.11 Site ID: 1	11001 Device Model: ISR4	431 ()						
\$	Security Monitoring	Device Options: Q Policy Zone Based	Drop Statistics]						
a	Firewall									© =
	Intrusion Prevention	Q	Search Opt	ions 🗸		7				Fotal Rows: 1
	URL Filtering	Internal Error Alloc Fail	Syn Cookie Trigger	Policy Fragment Drop	Policy Action Drop	Policy ICMP Ac	tion Drop	т	ype Drop	No Segn
*	Advanced Malware Protection		0	0	17	0		0		0
	Umbrella DNS Re- direct									
	Control Connections									
	System Status									
	Events									
	ACL Logs									
	Troubleshooting									
	Real Time									

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 <u>ZBFW troubleshoot Guide</u> 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.

≡	Cisco vManage						•	ê	(1)	0	admin 👻
::	MONITOR Network >	Real Time									
	Select Device 👻	BR3-WAN-Edge1 10.255.211.11	Site ID: 111001	Device Model: ISR4431							
\$	WAN	Device Options: Q Policy Zor	e Pair Sessions								
a	TLOC										© E
•	Tunnel	Q		Search Options $\mathbf{\vee}$						To	otal Rows: 23
2	Security Monitoring	Last Updated Session Id	State	Source IP	Destination IP	Source Port	Destination Po	ort		Protocol	
*	Firewall	27 Sep 2019 5143	open	10.10.1.1	216.58.194.195	44342	80			PROTO_L	7_HTTP
		27 Sep 2019 5219	closing	10.10.1.1	172.217.164.118	58390	443			PROTO_L	7_HTTPS
-	Intrusion Prevention	27 Sep 2019 5157	open	10.10.1.1	23.63.74.40	55514	80			PROTO_L	7_HTTP
	URL Filtering	27 Sep 2019 5139	open	10.10.1.1	172.217.0.42	59076	443			PROTO_L	7_HTTPS
	Advanced Malware	27 Sep 2019 5160	open	10.10.1.1	52.24.113.72	57560	443			PROTO_L	7_HTTPS
	Protection	27 Sep 2019 5113	open	10.10.1.1	10.1.1.1	8	5316			PROTO_L	4_ICMP
	Umbrella DNS Re-	27 Sep 2019 5128	open	10.10.1.1	72.21.91.29	47140	80			PROTO_L	7_HTTP
	direct	27 Sep 2019 5155	open	10.10.1.1	23.63.74.40	55512	80			PROTO_L	7_HTTP
	Control Connections	27 Sep 2019 5120	open	10.10.1.1	52.24.113.72	57538	443			PROTO_L	7_HTTPS
		27 Sep 2019 5184	open	10.10.1.1	216.58.194.195	44362	80			PROTO_L	7_HTTP
	System Status	27 Sep 2019 5123	open	10.10.1.1	52.23.120.80	35986	443			PROTO_L	7_HTTPS
	Events	27 Sep 2019 5150	open	10.10.1.1	184.29.104.234	38018	443			PROTO_L	7_HTTPS
	ACL Logs	27 Sep 2019 5167	open	10.10.1.1	99.84.197.216	35042	443			PROTO_L	7_HTTPS
		27 Sep 2019 5131	open	10.10.1.1	52.24.113.72	57546	443			PROTO_L	7_HTTPS
	Troubleshooting	27 Sep 2019 5134	open	10.10.1.1	52.43.139.170	45044	443			PROTO_L	7_HTTPS
	Real Time	27 Sep 2019 5179	open	10.10.1.1	172.217.164.110	54584	443			PROTO_L	7_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.

≡	Cisco vManage							● Ê	¢ ⁶⁹ Ø	admin 🔻
	MONITOR Network >	Real Time								
	Select Device 👻	BR3-WAN-Edge1 10.255.2	11.11 Site ID: 111001	Device Model: ISR4431 (i						
\$	Security Monitoring	Device Options: Q Po	olicy Zone Pair Statistics							
3	Firewall									
	Intrusion Prevention	Q		Search Options 🗸						Total Rows: 8
ê		Zone-Pair Name	Source Zone Name	Destination Zone Name	Policy Name	Class Name	Class Action	Packets Counter	Bytes	Counter A
*	URL Filtering	ZP_INSIDE_INSIDE	INSIDE	INSIDE	Compliance_Fire	Compliance_Fi	Inspect	0	22879	21
_	Advanced Malware	ZP_INSIDE_INSIDE				Compliance_Fi	Inspect Drop	0	0	0
11	Flotecuon	ZP_INSIDE_INSIDE	-			Compliance_Fi	Inspect	0	27997	5 19
	Umbrella DNS Re-	ZP_INSIDE_INSIDE	-	-	-	Compliance_Fi	Inspect	0	13985	285 4(
		ZP_INSIDE_INSIDE	-			Compliance_Fi	Inspect	0	0	0
	Control Connections	ZP_INSIDE_INSIDE	-	-	-	Compliance_Fi	Inspect	0	0	0
	System Status	ZP_INSIDE_INSIDE	-	-	-	Compliance_Fi	Inspect	0	0	0
	Evente	ZP_INSIDE_INSIDE	-	-	-	class-default	Inspect Drop	0	564	0
	Events									
	ACL Logs									
	Troubleshooting									
	Real Time									

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.

≡	cisco vManage		📥 🛱 🄎 🕢 admin 🗸
	DASHBOARD MAIN DASHBOARD		
□ ¢	1 ↑ vSmart - 1 16 ↑ WAN Edge - 1	VBond - 1	ge - 1 Reboot 2 Warning 0 Invalid 0
٩	Tools	Site Health (Total 11)	Transport Interface Distribution
ŝ	SSH Terminal 15	Full WAN Connectivity 1 sites	< 10 Mbps 57 10 Mbps - 100 Mbps 0
*	Rediscover Network 0	Partial WAN Connectivity 10 sites	100 Mbps - 500 Mbps 0
	Operational Commands	No WAN Connectivity 0 sites	> 500 Mbps 0
			View Percent Utilization
	WAN Edge Inventory	WAN Edge Health (Total 16)	Transport Health Type: By Loss ♦ = □
	Total 83	\frown \frown	100 %
	Authorized 24	(16) (0) (0)	50 %
	Deployed 16		· · · · · · · · · · · · · · · · · · ·
	Staging 0	Normal Warning Error	0 ••••••••••••••••
	Top Applications \mp D	Application-Aware Routing	Type: By Loss 💠 🖸
		Tunnel Endpoints Avg. Latency (ms)	Avg. Loss (%) Avg. Jitter (ms)
https://100	2.119.118.21:8443/#/app/tools/ssh	Router:biz-internet-BR3-WAN-Edge1:biz-inte 0	0.761 0

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

≡	Cisco vManage						•	Ê	A 23	0	admin 🔻
::	K TOOLS SSH TERMINAL										
	Device Group	<	10.255.211.11 ×								
-	All	¢	10.255.211.11 login: admin@10.255.211.11'	admin s password:							
म्म २	Q	~	Password:								
	Sort by Reachability \$	t=	BR3-WAN-Edge1#								
# 	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	1584331	and the adjour								
	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									

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

	ale de						
=	cisco VManage				Ê	≜ ⁵²	0
::	TOOLS SSH TERMINAL						
	Device Group	<	10.255.211.11 x				
ń	All	¢	BR3-WAN-Edgel≉sh sdwan zonebfwdp sessions				
۰ بر	Q	~	SRC DST TOTAL TOTAL				
ĉ	Sort by Reachability \$	t=	SESSION SRC DST SRC DST VPN VPN NAT INTERNAL INITIATOR RESPONDE	R APP			
*	BR2-WAN-Edge2 10.255.241.62 Site ID: 112005 Reachable	ISR4461	LICATION ID STATE SRC IP DST IP PORT PORT PROTOCOL VRF VRF ID ID ZP NAME CLASSMAP NAME FLAGS FLAGS BYTES BYTES F	TYP			
11	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Reachable	ISR4431					
	BR3-WAN-Edge1 10.255.241.31 Site ID: Reachable	ISR4331	1282 open 10.10.1.1 8.8.4.4 36952 53 PROTO_L4_UDP 2 2 1 1 ZP_INSIDE_ _Com1179673762 Compliance_Firewall_Policy_Copy-seq-31-cm 0 124 0	INSIDE			
	BR4-WAN-Edge-1 (0) 10.255.241.51 Site ID: 112003 Reachable	C1111X-8P	1289 open 10.10.1.1.1 8.8.4.4 45741 53 PROTO_L4_UDP 2 1 I P_INSIDE_ om1179673762 Compliance_Firewall_Policy_Copy_seq-31-cm_ 0 68 0 1294 open 10.10.1.1.8.8.8.8 42615 53 PPOTO_L4_UDP 2 1 1 PP INSIDE_	INSIDE			
	BR4-WAN-Edge1 100.255.241.41 Site ID: 112006 Reachable	ISR4351	Com1179673762 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			
	BR6-WAN-Edge1 0 192.168.1.1 Site ID: 112010 Reachable	C1111X-8P		INSIDE			
	DC1-WAN-Edge1 v	/Edge 5000					

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

≡	Cisco vManage				•	Ê	1	Ø	admin 👻
::	K TOOLS SSH TERMINAL								
	Device Group	<	10.255.211.11 ×						
*	All	¢	BR3-WAN-Edgel# BR3-WAN-Edgel#						
۰۰ م	Q	~	BR3-WAN-Edgel# BR3-WAN-Edgel#show platform hardware qfp active	feature firewall drop					
	Sort by Reachability 🖨	t=.	Drop Reason	Packets					
	BR2-WAN-Edge1 10.255.241.61 Site ID: 112005 Reachable	ISR4461	Invalid TCP initiator TCP extra payload after FIN Retrana with invalid flags	16 1 4					
	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	ISR4331	RST inside current window Stray Segment Same zone without Policy	90 62 1					
	BR2-WAN-Edge2 10.255.241.62 Site ID: 112005 Reachable	ISR4461	Policy drop:classify result BR3-WAN-Edgol# BR3-WAN-Edgol# D93-WAN-Edgol#	17					
	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Reachable	ISR4431	BR3-WAN-Edgel# BR3-WAN-Edgel# BR3-WAN-Edgel#						
	BR3-WAN-Edge1 10.255.241.31 Site ID: Reachable	ISR4331	BR3-WAN-Edgel# BR3-WAN-Edgel# BR3-WAN-Edgel# DP3-WAN-Edgel#						
	BR4-WAN-Edge-1 10.255.241.51 Site ID: 112003 Reachable	C1111X-8P	BR3-WAN-Edgel# BR3-WAN-Edgel# BR3-WAN-Edgel#						
	BR4-WAN-Edge1 100.255.241.41 Site ID: 112006 Reachable	ISR4351	BR3-WAN-Edgel# BR3-WAN-Edgel# BR3-WAN-Edgel# D23-WAN-Edgel#						
	DD4 WAN Edge1	01111Y.9D	BRO-MROBUSCE						

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.**

≡	Cisco vManage					•	Ê	1 53	0	admin 🔻
	TOOLS SSH TERMINAL									
	Device Group	<	10.255.211.11 ×							
_	All	¢	BR3-WAN-Edge1#							
रू २	Q	~	BR3-WAN-Edgel# BR3-WAN-Edgel#show s zbfw drop-statistics	adwan zbfw drop-statisti s catch-all	cs 0					
	Sort by Reachability 🖨	t=.	zbfw drop-statistics	s 14-max-nairsession s 14-too-many-pkts	0					
*	BR2-WAN-Edge1 10.255.241.61 Site ID: 112005 Reachable	ISR4461	zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics	3 14-session-limit 3 14-invalid-hdr 3 14-internal-err-undefi	0 0 ned-dir 0					
08	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	ISR4331	zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics	3 14-scb-close 3 14-tcp-invalid-ack-fla 3 14-tcp-invalid-ack-num 3 14-tcp-invalid-tcp-ini	0 g 0 . 0 tiator 16					
	BR2-WAN-Edge2 10.255.241.62 Site ID: 112005 Reachable	ISR4461	zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics	3 14-tcp-syn-with-data 3 14-tcp-invalid-win-sca 3 14-tcp-invalid-seg-syn	0 le-option 0 sent-state 0					
	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Reachable	ISR4431	zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics	3 14-tcp-invalid-seg-syn 5 14-tcp-invalid-seg-pkt 6 14-tcp-invalid-seg-pkt 7 14-tcp-invalid-seg-pkt 7 14-tcp-invalid-seg-pkt	rcvd-state 0 -too-old 0 -win-overflow 0 d-after-fin-send 1					
	BR3-WAN-Edge1 10.255.241.31 Site ID: Reachable	ISR4331	zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics	<pre>s l4-tcp-invalid-flags s l4-tcp-invalid-seq s l4-tcp-retrans-invalid</pre>	0 0 -flags 4					
	BR4-WAN-Edge-1 10.255.241.51 Site ID: 112003 Reachable	C1111X-8P	zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics	3 14-tcp-17-000-seg 3 14-tcp-syn-flood-drop 4 14-tcp-internal-err-sy 4 14-tcp-synflood-blacko 4 14-tcp-synflood-blacko	0 0 nflood-alloc-hostdb-fail 0 ut-drop 0					
	BR4-WAN-Edge1 100.255.241.41 Site ID: 112006 Reachable	ISR4351	zbfw drop-statistics zbfw drop-statistics zbfw drop-statistics	<pre>s 14-tcp-symitod-blacko s 14-tcp-symitod-blacko s 14-tcp-symin-in-win s 14-tcp-rst-in-win</pre>	yload 0 0 90					
	DD4 WAN Edgal	01111Y_9D	zbfw drop-statistics	s 14-tcp-stray-seg	62					

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

≡	Cisco vManage		•	Ê	≜ ⁵³	0	admin 👻
	K TOOLS SSH TERMINAL						
	Device Group	✓ 10.255.211.11 ×					
*	All	◆ BR3-WAN-Edgel#show sdwan zbfw zonepair-statistics zbfw zonepair-statistics ZP INSIDE INSIDE Com -1179673762					
۰ د	Q	Src-zone-name INSIDE dst-zone-name INSIDE					
	Sort by Reachability 🖨	policy-name Compliance_Firewall_Policy_Copy f= fw-traffic-class-entry Compliance_Firewall_Policy_Copy-seg-1-cm					
	BR2-WAN-Edge1 10.255.241.61 Site ID: 112005 Reachable	ISR4461 zonepair-name zP_INSIDE_ISIDE_com11/96/3/62 elass-action Inspect pkts-counter 0 pkts-counter 20870					
•	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	ISR4331 attempted-conn 29 current-active-conn 0 max-active-conn 0					
	BR2-WAN-Edge2 10.255.241.62 Site ID: 112005 Reachable	ISR4461 current-halfopen-conn 0 max-halfopen-conn 0 current-terminating-conn 0					
	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Reachable	ISR4431 time-since-last-session-create 8676 fw-tc-match-entry Compliance_Firewall_Policy_Copy-seq-1-acl_ 3 match-type "access-group name"					
	BR3-WAN-Edge1 10.255.241.31 Site ID: Reachable	ISR4331 fw-tc-proto-entry 5 protocol-name ** byte-counters 22879					0
	BR4-WAN-Edge-1 10.255.241.51 Site ID: 112003 Reachable	pkt-counters 247 17-policy-name NONE fw-traffic-class-entry Compliance_Firewall_Policy_Copy-seq-11-cm_ zonepair-name 2P_INSIDE_Com1179673762					
	BR4-WAN-Edge1 100.255.241.41 Site ID: 112006 Reachable	ISR4351 class-action "Inspect Drop" pkts-counter 0 bytes-counter 0					
	DD4 WAN Edgal	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 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.

≡	Cisco vManage		٠	Ê	<u>¢</u> ® Ø	admin 🔫
	Dashboard 1	SHBOARD				
□	Main Dashboard	😭 16 ^ 🚓 1 ^ 🚗 1 @	Reboot	2	Warnin Invalid	g 0 0
۵	VPN Dashboard	WAN Edge - 16 VBond - 1 VManage - 1	Last 24 hrs	_		_
٩	Security 2	Site Health (Total 11) Tra	ansport Interface Dist	ribution		
÷	Control Up	15 Section	10 Mbps			57
*	Partial	0 Partial WAN Connectivity 10 sites 10	0 Mbps - 100 Mbps 00 Mbps - 500 Mbps			0
-	Control Down	0 8 No WAN Connectivity 0 sites	500 Mbps			0
			Vie	ew Percent L	Jtilization	
	WAN Edge Inventory	WAN Edge Health (Total 16) Tra	ansport Health		Type: By Lo	ss ♦ = []
	Total	83	0 %			
	Authorized	24 (16) 0 0	0 %			
	Deployed					
	Staging	Normal Warning Error	0	• • • • •	• • • • • • •	•••••
	Top Applications	□ Application-Aware Routing			Туре: Е	ly 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 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,

	cisco vManage	٠		¢@		
5	URL Filtering: Blocked			×		
0 *	FireWall Enforce	1h 3h 6h	12h <mark>24h</mark>	7days	Blocked	Allowed 👳 🖬
≪ ₽ :	500 Letails				Sho	pping utation_block vs and Media
	Nov 26.	Chaming				
		 Snopping reputation News and 	_block Media			
	Nov 21					

≡	Cisco VI	Nanage			•	â	¥@	@ a	dmin 👻
	DASHBOARD	URL Filtering: Blocked				_	×		
	FireWall Enforc	Blocked Allowed			1h 3h 6h	12h 24h 7	'days	Blocked Allowed	. ≠ 0
\$	750	Chart Details							
3	r of sess					0	8	Shopping	ı_block
	aq 250 Z 0 0000	Q, Se	earch Options 🗸			Total Row	s: 3	News and	Media
m	Nov 26,	Name		Block					
	Advanced Malv	reputation_block		39					
	S 15	News and Media		2					
	of Malic Files								
	Number								
	Nov 26								
		0							

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.

≡	Cisco vManage								•	Ê	* @	0	admin 🔫
-	DASHBOARD MAIN D	ASHBOARD											
□	Monitor	1	16 ^		\bigcirc	1 ↑	. 10		Reboot	2	0	Warning Invalid	0
\$	Geography		WAN Edge - 16)	•	vBond - 1	vManag	ge - 1	Last 24 hrs				
٩	Network	2		Site H	lealth (Total 1	2)		Transp	ort Interface [Distribution	1		
÷	Alarms		15	0	Full WAN Co	nnectivity	10 sites	< 10 N	lbps				57
*	Events		0	0	Partial WAN	Connectivity	2 sites	10 Mb 100 M	ps - 100 Mbps lbps - 500 Mbp	s os			0
	Audit Log		0	0	No WAN Cor	nectivity	0 sites	> 500	Mbps				0
-									V	liew Percent	Utilization		
	ACL Log			WAN	Edge Health (*	Fotal 16)		Transp	ort Health		Тур	e: By Loss	♦ 〒 □
	Total		83	/	\frown	\frown	\frown	100 %					
	Authorized		24	(16)	0	0	50 %					
	Deployed		16		\smile								
	Staging		0		Normal	Warning	Error	0	•••••	• • • • •	• • • • •	••••	••••
	Top Applications		⇒ 0	Applic	cation-Aware	Routing						Type: By Lo	ss 🗢 🖸
					Tunnel Endpo	pints	Avg. Latency (ms)		Avg. Loss (%)		Avg. Jitter	r (ms)	
				~	Router:mpls-	BR2-WAN-Edge2:mpls	0		1.554		0		
	No	data to display	ý	~	BR2-WAN-Ed	ge2:mpls-Router:mpls	0		1.25		0		
				~	DC1-WAN-Ed	ge1:mpls-BR2-WAN-Edge2:mp	ols O		1.091		0		

≡	Cisco vManag	ge					● 6 ¹	≜	🥐 admin 🗸
::		ĸ							
	WAN - Edge 1 Coloca	ation Clusters							
-	VPN GROUP	VPN	SEGMENT						
\$	Select VPN Group		l segments						
عر									A AA
~									GGA
*	Device Group All	- Q		Search Options 🗸					Total Rows: 18
**	Hostname≁	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control V
678	😵 vsmart	172.27.0.13	vSmart	c44d2744-de58-48f1-8e61-3d655	0	reachable	300	-	29
w	😁 vmanage	172.27.0.14	vManage	b8a4fa09-bf86-4b1a-bb9e-9eb80f	0	reachable	400	-	16
	(3) vBond	172.27.0.12	vEdge Cloud (vBond)	28a77819-f63a-4a88-b90c-4d81b	0	reachable	600	-	-
	Router	10.10.23.23	ASR1001-X	ASR1001-X-JAD23151HC8	0	reachable	23	26	3
	C1-WAN-Edge2	10.255.241.101	vEdge 5000	193A1104180040	0	reachable	112001	24	3
	C1-WAN-Edge1	10.255.241.102	vEdge 5000	193A1104180039	0	reachable	112001	24	3
	BR6-WAN-Edge1	192.168.1.1	C1111X-8P	C1111X-8P-FGL231613RW	0	reachable	112010	18	2
	BR4-WAN-Edge1	100.255.241.41	ISR4351	ISR4351/K9-FD018351QNX	0	reachable	112006	0	2
	BR4-WAN-Edge-1	10.255.241.51	C1111X-8P	C1111X-8P-FGL231613RX	0	reachable	112003	34	3
	BR3-WAN-Edge1	10.255.211.11	ISR4431	ISR4431/K9-F0C22467A57	0	reachable	111001	26	3
	BR3-WAN-Edge1	10.255.241.31	ISR4331	ISR4331/K9-FD02012092A	-	reachable		-	-
	BR2-WAN-Edge2	10.255.241.22	ISR4331	ISR4331/K9-FD020110MX6	0	reachable	112007	7 (8)	2
	BR2-WAN-Edge2	10.255.241.62	ISR4461	ISR4461/K9-FD02316A220	0	reachable	112005	24	3
	2 BR2-WAN-Edge1	10.255.241.21	ISR4331	ISR4331/K9-FD020110MX1	0	reachable	112007	0	2
		10.05.041.01	100 4441		-		110005	0.4	â

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.

≡	cisco Cisco vManage		• É) 🍂	• ?	admin 🔫
::	MONITOR Network >	URL Filtering				
	Select Device 🔻	BR2-WAN-Edge1 10.255.241.21 Site ID: 112007 Device Model: ISR4331 ()				
	Applications		1h	3h 6h 1	2h 24h 7	days Custom 👻
\$	Interface	Blocked Allowed				
ય	TCP Optimization	100				
ĉ	WAN Throughput	100	_			
*	Flows	E E				
	Top Talkers					
	WAN	Shopping • Session Count: 3				
	TLOC					
	Tunnel	0				
	Security Monitoring	Shopping	Reputation	olock		
	Firewall					00
	Intrusion Prevention					
	URL Filtering	Q Search Options V				Total Rows: 2
	Advanced Malware	Category 2				
	Protection	Benutation block 46				
	Umbrella DNS Re-direct	40 40				
	Control Connections					

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.

≡	Cisco vManage		📥 🖨 🍋 🤪 admin 🗸
::	MONITOR Network >	Real Time	
	Select Device 👻	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Device Model: ISR4431 ()	
\$	Security Monitoring	Device Options: 2 Policy QoS Scheduler Information	
4	Firewall	Policy Rewrite Associations	•
	Intrusion Prevention	Q Policy Zone Based Drop Statistics Ions ✓	Total Rows: 10
	URL Filtering	Property Policy Zone Pair Sessions Value	ue
*		Device groups Pair Wise Key IPSEC Local SA Entry	",'ISR4331","Primary","UG3","US","West"]
	Protection	Domain ID Pair Wise Key IPSEC Inbound Connections 1	
—		Hostname Pair Wise Key IPSEC Outbound Connection BR3-	WAN-Edge1
	direct	Last Updated Reboot History 24 Se	ep 2019 11:15:48 AM PDT
		Latitude Security Information 37.40	09284
	Control Connections	Smart License Registration Info	335
	System Status	Personality Smart License Drivacy Info WA	AN Edge
	Events	Site ID Smart License Evaluation Info 1110	301
		Timezone Smart License Usage PDT	-0700
	ACL Logs	Vbond 10.10	0.60.2
	Troubleshooting		
	Real Time 1		

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

≡	Cisco vManage				٠	Ê	≜ @	0	admin 👻
::	MONITOR Network >	Real Time							
	Select Device 🔹	BR2-WAN-Edge1 10.255.241.21	Site ID: 112007 Device	Model: ISR4331 (i)					
*	Firewall	Device Options: Q Security Ap	p URLF Update Status						
عر	URL Filtering	Q		Search Options 🖌				т	otal Rows: 1
±	Advanced Malware Protection	Last Updated 19 Feb 2020 2:43:37 PM PST	URLF Version 0-0	URLF Last Update Time 1970-01-01T00:00:00+0	URLF La	st Update Sta ate-status-unk	tus nown	URLF La	ist Update Re
_	Umbrella DNS Re-direct								
	Control Connections								
	System Status								
	Events								
	ACL Logs								
	Troubleshooting								
	Real Time					-			

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.

≡	cisco vManage		📥 🖨 🏚 🥹 admin 🗸
-	DASHBOARD MAIN DASHBOARD		
□ \$	1 ↑ 16 ↑ vSmart - 1 WAN Edge - 1	• 1 ↑ vBond - 1 • • • • • • • • • • • • • • • • • •	Reboot 2
عر	Tools	Site Health (Total 11)	Transport Interface Distribution
â	SSH Terminal 15	Second Se	<10 Mbps 57
*	Rediscover Network 0	Partial WAN Connectivity 10 sites	100 Mbps - 500 Mbps 0
•	Operational Commands	No WAN Connectivity 0 sites	> 500 Mbps U View Percent Utilization
	WAN Edge Inventory	WAN Edge Health (Total 16)	Transport Health Type: By Loss 💠 후 다
	Total 83	\frown \frown \frown	100%
	Authorized 24		50 %
	Deployed 16		
	Staging 0	Normal Warning Error	0 •••••••••
	Top Applications 👳 D	Application-Aware Routing	Type: By Loss 💠 🖸
		Tunnel Endpoints Avg. Latency (ms)	Avg. Loss (%) Avg. Jitter (ms)
https://10	0.119.118.21:8443/#/app/tools/ssh	Router:biz-internet-BR3-WAN-Edge1:biz-inte 0	0.761 0

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

≡	Cisco vManage			•	Ê	≜ 53	Ø	admin 🔻
	K TOOLS SSH TERMINAL							
	Device Group	<	10.255.211.11 ×					
~	All	÷	10.255.211.11 login: admin adminê10.255.211.11's password:					
* •	Q	~	Password:					
	Sort by Reachability 🖨	t=.	BD2_WAN_Frinc1#					
. .	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	1584331						
	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						

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>

≣	Cisco vManage																																																É	3	ļ	58	?)	а	dm	iin	•
::	CTOOLS SSH TERMINAL																																																									
	Device Group	<	10.255.241.21	×																																																						
\$	All	\$	BR2-WAN-Edge1# BR2-WAN-Edge1#																																																							
۰ ۹	Q	~	BR2-WAN-Edge1# BR2-WAN-Edge1#																																																							
	Sort by Reachability \$	t≡.	BR2-WAN-Edge1# BR2-WAN-Edge1#																																																							
	BR1-WAN-Edge1 10.255.241.11 Site ID: 112002 Reachable	vEdge 1000	BR2-WAN-Edge1# BR2-WAN-Edge1# BR2-WAN-Edge1#																																																							
	BR1-WAN-Edge2 10.255.241.12 Site ID: 112002 Reachable	vEdge 1000	BR2-WAN-Edgel# BR2-WAN-Edgel# BR2-WAN-Edgel# BR2-WAN-Edgel#																																																							
	BR2-WAN-Edge1 10.255.241.21 Site ID: 112007 Reachable	ISR4331	BR2-WAN-Edge1# BR2-WAN-Edge1# BR2-WAN-Edge1#																																																							
	BR2-WAN-Edge1 10.255.241.61 Site ID: 112005 Reachable	ISR4461	BR2-WAN-Edge1# BR2-WAN-Edge1# BR2-WAN-Edge1#app Successfully move	p-host: ed trad	sti	stin	ti	ti ac	:i	:i	ic	in	in ce	ng	g I	mo	ove to	e aj o b	app	oid	uto	d 1	100	g	to	o b	000	otf	Ela	ısł																												
	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	ISR4331	iox_utd_R0-0_R0-0 BR2-WAN-Edge1# BR2-WAN-Edge1#	0.1408	086	86	86	86	36	86	6	6	6_	_0	0.2	.20	020	001	129	165	580)5.È	biı	n.	.gz	Z																																
	BR2-WAN-Edge2 10.255.241.62 Site ID: 112005 Reachable	ISR4461	BR2-WAN-Edge1# BR2-WAN-Edge1# BR2-WAN-Edge1# BR2-WAN-Edge1#																																																							
	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Reachable	ISR4431	BR2-WAN-Edge1# BR2-WAN-Edge1# BR2-WAN-Edge1#mor	re /com	com	com	om	om	om	om	m	mj	mp	pr	res	ess	sed	d i	iox	_ut	td_I	_R0-	-0_)_R	R0-	-0.	.14	1 08	36_	_0 .	20)2(001	12	29	916	658	805	15.	.bi	in	1. <u>9</u>	gz	Z														
	BR3-WAN-Edge1 10.255.241.31 Site ID: Reachable	ISR4331	2020-01-10 12:18: 2020-01-10 12:18: 2020-01-10 12:18: 2020-01-10 12:18: 2020-01-10 12:18:	:10.33 :10.34 :10.90	338 347 909 909	838 847 909 909	38 47 09	38 47 09 09	38 17 09	8 7 9 9	8 7 9	8 7 9 9	8 [7 [9 [9 [[C [C	CF1 CF1 CF1	GIM GIM GIM GIM	MGR MGR MGR MGR	R_D R_D R_D R_D	DEB DEB DEB	BUG] BUG] BUG] BUG]]***]dis]dis]cl	**C sab sab	Cl: bl: bl:	im in in	ngr ng ng nmo	r s on on	ner ner ner	art pv pv nit	red ver ver	bo	se se	e d e d	lek lek	bu bu 1	ug ug n	J J	mbe	er		FI	LM	121	01	1.51	W03	SF												
	BR4-WAN-Edge-1	C1111X-8P	2020-01-10 12:18:	:10.90	909	909	09	09	9	9	9	9	9 [[0	CLI	LIM	MGR	R_D	DEB	BUG]]cl.	im		com	nmo	on	ir	nit	: :	:	Pr	:00	duc	ct	t	II	D:	IS	SR	843	33	31/	/ K	K 9														

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.

≡	cisco vManage					•	ê	.	9	admin 👻
	TOOLS SSH TERMINAL									
	Device Group	<	10.255.241.21 ×							
~	All	÷	BR2-WAN-Edge1# BR2-WAN-Edge1#							
* •	Q Sort by Reachability ¢	 ✓ 	BR2-WAN-Edgel# BR2-WAN-Edgel# BR2-WAN-Edgel#Show utd engine s 2020/01/10-19:00:19.974676 PDT UTD WebEiler Category/Security	standard logging events [**] [Hostname: 10.255.241	.21] [**] [Instance_ID: 1] [*	**] Drop [**]				
# *	BR1-WAN-Edge1 10.255.241.11 Site ID: 112002 Reachable	vEdge 1000	<pre>Category: Computer and Inter 89.91.26:80 2020/01/10-19:00:20.322690 PDT</pre>	<pre>con [] [OKL: us.archive.u cnet Info] ** [Reputation: [**] [Hostname: 10.255.241</pre>	.21] [**] [Instance ID: 1] [*	**] Drop [**]				
1	BR1-WAN-Edge2 10.255.241.12 Site ID: 112002 Reachable	vEdge 1000	UTD WebFilter Category/Reputat: lease] ** [Category: Computer a -> 91.189.91.26:80	on [**] [URL: us.archive.u and Internet Info] ** [Repu	buntu.com/ubuntu/dists/xenial tation: 74] [VRF: 1] {TCP} 10	L-updates/InRe				
	BR2-WAN-Edge1 10.255.241.21 Site ID: 112007 Reachable	ISR4331	2020/01/10-19:00:20.670739 PDT UTD WebFilter Category/Reputat: Release] ** [Category: Computer 56 -> 91.189.91.26:80	[**] [Hostname: 10.255.241 Lon [**] [URL: us.archive.u and Internet Info] ** [Rep	.21] [**] [Instance_ID: 1] [* buntu.com/ubuntu/dists/xenia] putation: 74] [VRF: 1] {TCP}	**] Drop [**] L-backports/In 10.10.1.1:401				
	BR2-WAN-Edge1 10.255.241.61 Site ID: 112005 Reachable	ISR4461	2020/01/10-21:23:17.230337 PDT UTD WebFilter Category/Reputat: * [Category: Computer and Inter	[**] [Hostname: 10.255.241 Lon [**] [URL: us.archive.u rnet Info] ** [Reputation:	.21] [**] [Instance_ID: 1] [* buntu.com/ubuntu/dists/xenia] 74] [VRF: 1] {TCP} 91.189.91.	**] Drop [**] L/InRelease] * .23:80 -> 10.1				
	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	ISR4331	0.1.1:46392 2020/01/10-21:23:17.375310 PDT UTD WebFilter Category/Reputat:	[**] [Hostname: 10.255.241 Lon [**] [URL: us.archive.u	.21] [**] [Instance_ID: 1] [* buntu.com/ubuntu/dists/xenia]	**] Drop [**] L-updates/InRe				
	BR2-WAN-Edge2 10.255.241.62 Site ID: 112005 Reachable	ISR4461	-> 10.10.1.1:46394 2020/01/10-21:23:17.522017 PDT UTD WebFilter Category/Reputat:	[**] [Hostname: 10.255.241 lon [**] [URL: us.archive.u	.21] [**] [Instance_ID: 1] [* puntu.com/ubuntu/dists/xenial	**] Drop [**] L-backports/In				
	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Reachable	ISR4431	Release] ** [Category: Computer 80 -> 10.10.1.1:46396 2020/01/11-10:29:27.794889 PDT	<pre>r and Internet Info] ** [Rep [**] [Hostname: 10.255.241]</pre>	<pre>putation: 74] [VRF: 1] {TCP} .21] [**] [Instance_ID: 1] [*</pre>	91.189.91.23:				
	BR3-WAN-Edge1 10.255.241.31 Site ID: Reachable	ISR4331	<pre>'' category: Computer and Inter 0.1.1:57808 2020/01/11-10:29:27.939866 PDT</pre>	<pre>con [**] [OKL: US.arChive.u cnet Info] ** [Reputation: [**] [Hostname: 10.255.241</pre>	.21] [**] [Instance ID: 1] [*	**] Drop [**]				
	BR4-WAN-Edge-1	C1111X-8P	UTD WebFilter Category/Reputat:	ion [**] [URL: us.archive.u	buntu.com/ubuntu/dists/xenial	L-updates/InRe				

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**.

≡	cisco VManage			•	Ê	4 59	0	admin 🔫
	TOOLS SSH TERMINAL							
	Device Group	<	10.255.241.21 ×					
~	All	\$	BRZ=WAN=Edgel# BRZ=WANEdgel#					
** •	٩	~	BRZ-wAN-Edgel# BRZ-wAN-Edgel# BRZ-wAN-Edgel#					
	Sort by Reachability 🖨	te.	BR2-WAN-Edgel# BR2-WAN-Edgel#					
	BR1-WAN-Edge1 10.255.241.11 Site ID: 112002 Reachable	vEdge 1000	BR2-WAN-Edge1# BR2-WAN-Edge1# BR2-WAN-Edge1#					
	BR1-WAN-Edge2 10.255.241.12 Site ID: 112002 Reachable	vEdge 1000	BR2-WAN-Edgel# BR2-WAN-Edgel# BR2-WAN-Edgel# BR2-WAN-Edgel#					
	BR2-WAN-Edge1 10.255.241.21 Site ID: 112007 Reachable	ISR4331	BR2-WAN-Edgel# BR2-WAN-Edgel# BR2-WAN-Edgel#					
	BR2-WAN-Edge1 10.255.241.61 Site ID: 112005 Reachable	ISR4461	BR2-WAN-Edgel# BR2-WAN-Edgel# BR2 WAN-Edgel#					
	BR2-WAN-Edge2 10.255.241.22 Site ID: 112007 Reachable	ISR4331	DR2-max-buggif BR2-WAN-Edgel#show utd engine standard statistics internal ************Engine #1************					
	BR2-WAN-Edge2 10.255.241.62 Site ID: 112005 Reachable	ISR4461	Memory usage summary: Total non-mmapped bytes (arena): 205697024 Bytes in mapped regions (hblkhd): 431472640 Total allocated grace (wordblick): 204726640					
	BR3-WAN-Edge1 10.255.211.11 Site ID: 111001 Reachable	ISR4431	Total free space (fordblks): 930784 Total free space (fordblks): 930784 Topmost releasable block (keepcost): 132576					
	BR3-WAN-Edge1 10.255.241.31 Site ID: Reachable	ISR4331	Packet I/O Totals: Received: 0 Analyzed: 0 (0.000%)					
	BR4-WAN-Edge-1	C1111X-8P	Dispiped: 0 (0.000%) Filtered: 0 (0.000%)					

≡	Cisco vManage					•	Ê	≜ @	0	admin 🔫
::	K TOOLS SSH TERMINAL									
	Device Group	<	10.255.241.21 ×							
	All	÷	BR2-WAN-Edge1#							
\$			BKZ-WAN-Edgel#		unl filteni					
	Q	~	UTM Preprocessor Statistics	ard statisti	cs uri-riitering					
٩, ۱										
	Sort by Reachability 🖨	t=.	URL Filter Requests Sent:	25						
e	ADOID	Lugo ologu	URL Filter Response Received:	25	3					
_	172.27.0.12 Site ID: 600		Blacklist Hit Count:	0	0					
••	Reachable	vBond	Whitelist Hit Count:	0	0					
÷.	BR1-ISR4321	ISR4321								
	1.1.1.1 Site ID: 1		Reputation Lookup Count:	25	3					
11.	Reachable		Reputation Action Block:	25	3					
	DD1 WAN Edge1	vEdge 1000	Reputation Action Pass:	0	0					
	BR I-WAN-Edge I	vedge 1000	Reputation Action Default Pass:	0	0					
	Reachable		Reputation Accion Default Block:	0	0					
	Redonable		Reputation Score Out of Pange:	0	0					
	BR1-WAN-Edge2	vEdge 1000	Reputation boole out of Mangel							
	10.255.241.12 Site ID: 112002		Category Lookup Count:	25	3					
	Reachable		Category Action Block:	0	0					
	BR2-WAN-Edge1	ISR4331	Category Action Pass:	25	3					
	10.255.241.21 Site ID: 112007		Category Action Default Pass:		0					
	Reachable		Category None:							
	PP2 WAN Edge1	ISP///61	Category Out of Range:							
	10 255 241 61 Site ID: 112005	13R4401								
	Reachable									
			BR2-WAN-Edge1#							
	BR2-WAN-Edge2	ISR4331	BR2-WAN-Edge1#							
	10.255.241.22 Site ID: 112007		BR2-WAN-Edge1#							
	Reachable		BR2-WAN-Edge1#							
	BR2-WAN-Edge2	ISR4461	BR2-WAN-Edge1#							
	10.255.241.62 Site ID: 112005		BR2-WAN-Edge1#							
	Reachable		BR2-WAN-Edgel#							
	BR3-WAN-Edge1	ISR4431	BKZ-WAN-Edgel#							
	10.255.211.11 Site ID: 111001	10111101	BRZ-WAN-Edgel#							

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	H
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 Data Prefix	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	Туре	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	Туре	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	
Summary	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	
VPNO		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</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
 L
```

```
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 O
 !
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
L
```

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
                       10.255.241.21
  system-ip
  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 shal-hmac ah-shal-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$3VEF3VAI31MM3E$awMmxogwHvRdxoHA5u1utUOAmKPBUvUbkD4PnwNWmWk
 vrf definition 1
  description Service VPN
  rd
             1:1
  address-family ipv4
   exit-address-family
   !
  address-family ipv6
   exit-address-family
  1
  !
  vrf definition 65529
  rd 65529:1
  address-family ipv4
   exit-address-family
   1
  !
  vrf definition Mgmt-intf
  description Management VPN
  rd
              1:512
  address-family ipv4
   exit-address-family
   1
  address-family ipv6
   exit-address-family
   T
  !
  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
  L
  policy-map type inspect Guest Access Firewall
  class Guest_Access_Firewall-seq-1-cm_
     inspect audit-trail-pmap
   1
  class Guest_Access_Firewall-seq-11-cm_
    inspect audit-trail-pmap
   1
  class class-default
     drop
   !
  L
  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
            1500
  ip mtu
             1500
  mtu
  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
         1500
ip mtu
ip ospf 1 area 0
ip ospf authentication message-digest
                 point-to-point
ip ospf network
ip ospf cost
                    1
ip ospf dead-interval 40
ip ospf hello-interval 10
ip ospf message-digest-key 22 md5 0 clscol23
ip ospf priority
                   1
ip ospf retransmit-interval 5
           1500
mtu
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
           1500
mtu
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
1
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
  1
 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
 1
 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
 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 clsco123
  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
   T
  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
   1
  start
  1
  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</pre>
denied</h3&gt;&lt;p&gt;Please contact your Network Administrator&lt;/p&gt;]]>
   1
  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
                                 5
  nat-refresh-interval
  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 <u>Cisco Community</u> at <u>https://cs.co/en-cvds</u>.

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)