配置和驗證URL過濾

目錄

簡介 必要條件 <u>需求</u> <u>採用元件</u> 設定 網路圖表 <u>配置URL過濾策略的元件</u> <u>建立感興趣的URL清單</u> 建立安全策略 <u>將安全策略應用於裝置</u> <u>修改URL篩選</u> 刪除URL篩選 驗證 從vManage GUI監控URL過濾 <u>疑難排解</u> 相關資訊

簡介

本文檔介紹如何使用Cisco Catalyst Manager GUI在Clsco IOS-XE®路由器上配置和驗證URL過濾。

必要條件

在vManage中上傳具有當前Cisco IOS-XE代碼的相容UTD軟體虛擬映像。有關在cEdge路由器上安裝UTD安全虛擬映像的說明,請檢視相關資訊部分。

Cisco Edge路由器必須處於vManaged模式,並且必須預先連線模板。

需求

思科建議您瞭解以下主題:

- Cisco SD-WAN Overlay會啟動初始配置。
- URL過濾配置Cisco Catalyst Manager GUI。

採用元件

本檔案根據這些軟體和硬體版本:

- Cisco Catalyst SD-WAN Manager 20.14.1版。
- Cisco Catalyst SD-WAN控制器版本20.14.1。
- 思科邊緣路由器版本17.14.1。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



配置URL過濾策略的元件

本文根據以下示例要求,說明了如何根據類別、信譽或按域阻止/允許清單配置URL過濾以阻止/允許 特定客戶端HTTPS流量:

- 阻止來自訪客VPN Web類別上的客戶端的此HTTPS請求:
 - 遊戲
 - 賭博
 - 駭客
 - 非法毒品
- 必須阻止來自訪客VPN上具有Web信譽小於或等於60的客戶端到網站的任何HTTPS URL請求。
- 訪客VPN上的客戶端對網站的HTTP(s)請求阻止了Facebook、Instagram和YouTube,同時允 許訪問google.com和yahoo.com。

要配置URL過濾:

建立感興趣的URL清單

1. 在Cisco SD-WAN Manager選單上,導航到左側面板中的Configuration > Security頁籤。

2	Monitor								
*	Configuration	Configuration Groups	1						
*	Tools	Policy Groups	nne	s .	Applicat	lions	Security	Logs	Multicloud
¢	Maintenance	Service Insertion							
-	Administration	Topology Cloud OnRamp for SaaS				١	NAN Edges		
	Marifleure	Cloud OnRamp for Multicloud		1			8		
	worknows	Devices		Managel	r		Reachable		•
	Reports	Network Hierarchy Certificates							
ılıl	Analytics	Certificate Authority							
Ø	Explore	Templates	orm	ing Site	s v				
		Policies Security							
		Unified Communications		SITE	400	1.67			
		Network Design		SITE_	100	1.6			
		Cloud onRamp for laaS	ites	SITE	0.87				
			ŝ		0.83				
		Good		SITE_	200				

要建立或管理Allowlist URL List或Blocklist URL List,請從頁面右上角的Custom Options下拉選單 中選擇Lists。

≡	dialis Catalyst SD	-wan	Q 💷 │ ႙ admin1
1 1 1 1 1	Monitor Configuration		Security Lists Policies/Profiles Umbrella Registration
*	Tools	Q. Search	Threat Grid API Key
30	Maintenance	Add Security Delley Add United Security Delley	
å,	Administration		Total Dourse 5 1) JOL
÷Ð	Workflows		

按一下左側窗格中的Allow URLs Lists,並建立New Allow URL List。

Security > Define Lists							
Select a list type on the left and	start creating your groups of	interest					
Application Data Prefix	New Allow URL Lis	t					
Domain Signatures	Name	Entries	Reference Count	Updat∉			
Allow URL Lists				No data availa			
Block URL Lists							
Zones							
Port							
Protocol							
Rule Set							
Geo Location							
Object Group							
Identity							

- 在URL List Name欄位中,輸入最多包含32個字元(僅限字母、數字、連字型大小和底線)的 清單名稱。
- 在URL欄位中,輸入要包含在清單中的URL,並以逗號分隔。還可以使用導入按鈕從可訪問的 儲存位置增加清單。
- 完成後,按一下Add。

Select a list type on the left and start creating your groups of interest					
Application Data Prefix	New Allow URL List				
Domain	Allow URL List Name*				
Signatures	Guest_Allow				
Allow URL Lists	Add Allow URL *				
Block URL Lists	wwwl.googlel.com, wwwl.yahool.com				
Zones					
Port					
Protocol					
Rule Set					
Geo Location	Add Cancel				
Object Group					



注意:可以考慮在允許清單和阻止清單中為域名使用regex模式

按一下左側窗格中的Block URLs Lists,然後建立New Block URL List。

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

oplication ata Prefix	New Block UR	LList	
omain	Name	Entries	Reference (
gnatures Iow URL Lists			
lock URL Lists			
nes			
rt			
stocol			
le Set			
o Location			
ject Group			
ntity			

- 在「URL清單名稱」欄位中,輸入最多包含32個字元(僅限字母、數字、連字型大小和底線)的清單名稱
- 在URL欄位中,輸入要包含在清單中的URL,並以逗號分隔。還可以使用導入按鈕從可訪問的 儲存位置增加清單。
- 完成後,按一下Add。

New Block URL List	
Block URL List Name*	
Guest_Block	
Add Block URL *	بې mport د.
wwwi,youtubei,com,wwwi,facebooki,com,instagram.com	

Add Cancel

建立安全策略

2. 在Cisco SD-WAN Manager選單上,導航到Configuration > Security,然後按一下Add new security policy。將打開「增加安全策略」嚮導,並顯示各種使用案例場景或使用清單中的現有策略 。選擇custom,然後按一下Proceed在嚮導中增加URL過濾策略。



注意:在增加安全策略中,選擇支援URL過濾的方案(訪客訪問、直接網際網路訪問或自 定義)。

在增加安全策略嚮導,按一下下一步,直到顯示URL過濾窗口。 現在轉到URL Filtering > Add URL Filtering Policy > Create New以建立URL過濾策略。按一下下一步



按一下Target VPNs以便在Add Target VPNs嚮導中增加所需的VPN數量。

Add URL Filtering Policy				
	Target		Policy Behavior	
	0 VPNs	Blacked Categories: - Wab Moderate Reputation: Risk Whitefat URLs: -	Action: Block Page	
	Target VPNs	Blackfist URLs: -	Block Page Server	Alerts
URL Filtering - Policy Rule Configuration ③	Ad	d Target VPNs	×	
Policy Name Msximum of 32 characters	VPN	Ns 12		
Web Categories Block Select one or m	ore web categories		_	
Web Reputation Moderate Risk 👻		Save Cl	nanges Cancel	
Advanced >				

- 在Policy Name欄位中輸入策略名稱。
- 從Web Categories(Web類別)下拉選單中選擇其中一個選項,選擇Block(阻止),則會阻止與您選擇的類別匹配的網站。

Block -阻止與您選擇的類別匹配的網站。 Allow -允許與您選擇的類別匹配的網站。

從下拉選單中選擇一個Web信譽(Web Reputation),並將其設定為中度風險(Moderate Risk)。 信譽 得分等於或低於60分的所有URL都會被阻止。

高風險:信譽得分0到20。 可疑:信譽分數為0到40。 中等風險:信譽得分為0到60。 低風險:信譽得分為0到80。 值得信任:信譽得分為0到100。

Add URL Filtering Policy						
		Target			Policy Behavior	
		1 VPNs Target VPNs	_	Blocked Categories: 5 Wab Moderate Reputation: Risk Whitelist URLs: - Blackist URLs: -	Action: Block Page Block Page Server	Blackfer: Disabled Whitefer: Disabled Reputation/Category: Disa Alerts
URL Filtering - Policy	Rule Configuration 🕕			web Filter		
Policy Name	Guest_Access					
Web Categories	Block	ames × oamblino × hac	ickino × abu	sed-drucs		
Web Reputation	Moderate Risk					
Advanced >						

在高級中,根據需要從Allowlist URL List或blocklist URL List下拉選單中選擇現有清單或建立新清單

Advanced 🗸

Whitelist URL List	Select a whitelist url list				
	Search	Guest_Allow			
Blacklist URL List	Guest_Allow	www\.google\.com			
Block Page Server		www\.yahoo\.com			
O Block Page Content					
Default Content Header	New Allow URL List				
Contont Body					

Blacklist URL List	Select a blacklist url list				
	Search	Guest_Block			
Block Page Server	Guest_Block	www\.youtube\.com			
O Block Page Content		www\.facebook\.com			
Default Content Header		instagram.com			
Content Body	New Block URL List				
🔿 Redirect URL 🕠					

如果需要,請更改「阻止頁面內容」下的內容正文,並確保已選擇所有警報。

按一下Save URL filtering策略以增加URL過濾策略。

URL Filtering	- Policy	Rule	Configuration	0
----------------------	----------	------	---------------	---

Advanced 🗸		
Whitelist URL List	Guest_Allow ×	
Blacklist URL List	Guest_Block ×	
Block Page Server		
O Block Page Content		
Default Content Heade	Access to the requested page has been denied	
Content Body	Please contact your Network Administrator)
🔿 Redirect URL 🕕	Enter URL)
Alerts and Logs (i)		
Alerts	🧭 Blacklist 🕑 Whitelist 🗹 Reputation/Category	
		Save URL Filtering Policy Cancel

按一下Next,直到顯示「Policy Summary」頁。

在各自的欄位中輸入安全策略名稱和安全策略說明。

	Firewall Intrusion Prevention URL Filtering Advanced Maiware Protection DNS Security TLS/SSL Decryption Policy Summary Structure Content on the Policy Struct
Provide a name and descriptic	on for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.
Security Policy Name	Guest_URL_Policy
Security Policy Description	Guest URL Policy
	(2000-000-000-000-000-000-000-000-000-00
Additional Policy Settings	
Intrusion Prevention and/or URL	Filtering and/or Advanced Malware Protection
External Syslog Server	VPN Enter a VPN O Server IP Example: 10.0.0.1
Pailure Mode	(Abar)
Back	Preview Save Policy Cancel
將安全策略歷	應用於裝置

要將安全策略應用到裝置,請執行以下操作:

從Cisco SD-WAN Manager選單中,選擇Configuration > Templates。



按一下Device Templates,然後按一下Edit on Device Template。

Configuration											
Device Templates Feature Templ	ates										
Q 300 × Search											V
Create Template ~											
Template Type Non-Default 🗸										Total Rows: 1 of §	9 t3 @
lame	Description	Туре	Device Model	Device Role	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	common.template!	Status
c862ea4-e57e-4616-8bc7-88d2d2978	Device template of Site300-cE1 w	Feature	C8000v	SDWAN Edge	25	Disabled	1	admin	24 Jul 2024 11	In Sync	
											Edit
											View
											Delete
											Сору
											Enable Draft Mo
											Attach Devices
											Detach Devices
											Export CSV

Change Device Valu

按一下Additional Templates。

Configuration	
Device Templates	Feature Templates
Device Model*	C8000v
Device Role*	SDWAN Edge
Template Name*	fc862ea4-e57e-4616-8bc7-88d2d2978089
Description*	Device template of Site300-cE1 with Site ID: 300
Basic Information	Transport & Management VPN Service VPN Cellular Additional Templates Switchport

• 從Security Policy下拉選單中,選擇之前在Guest_URL_Policy下配置的策略名稱,然後按一下 Update。

Policy	VIP07_DPI_Visibility		
Probes	Choose 🔻		
Tenant	Choose 🔻		
Security Policy	Guest_URL_Policy		
Container Profile *	Factory_Default_UTD_Template ()		
Switch Port Switch Port			
		Update	Cancel

按一下裝置,確保配置正確,然後按一下Config Diff和Side Diff。按一下Configure Devices。

Device Template Total fc862ea4-e57e-4616-8 1	Config Preview Config Diff	tent
Device list (Total: 1 devices)	Local Configuration vs. New Configuration	
Fliter/Search	1 1 system	
	2 2 ztp-status in-progress	
C8K-C18B1FE2-C69F-A311-DEA7-	3 3 device-model vedge-C8000V	
462A878B089A Ste300-cE111301	4 gps-location latitude -23.60911	
Configure Devi-	5 5 gps-location longitude -46.69768	
ooningare bonin	7 7 Avarianti 1	
	8 8 site-id 300	
	9 9 no transport-gateway enable	
	10 10 port-offset 0	
	11 11 control-session-pps 300	
	12 12 admin-tech-on-failure	
	389	
	390 nattern www.google.com	
	391 Dettern www.google.com	
	pactern www.yanot.com	
	393	
	parameter-map type regex Guest_BIOCK-DI_	
	pattern instagram.com	
	pattern www.facebook.com	
	pattern www.youtube.com	
	377	
	444 web-filter block page profile block-Guest_Access	
	400 text Access to the requested page has been denied. Please contact your Ne Administrator	twork
	446 exit	
	web-filter url profile Guest_Access	
	440 blacklist	
	4450 parameter-map regex Guest_Block-bl	
	exic exic	
	453 abused-drugs	
	400 gaabling 400 gaabling	
	456 hacking	
	457 shopping 450	
	459 block page-profile block-Guest Access	
	460 log level error	
	461 reputation 462 block-threshold moderate-risk	
	460 exit	
	444 whitelist	
	466 exit	
	467 exit	
	460 utd global 469	
	470 policy utd-policy-vrf-12	
	471 all-interfaces	
	472 vrf 12 473 web-filter url profile Guest Access	
	474 exit	
	Back Configure Devices Cancel	

vManage已成功使用安全策略配置裝置模板,並在邊緣裝置上安裝UTD軟體套件。

Push Feature Ter	nplate Configuration 🖉 Validation succe	155	View Logs
Total Task: 1 Su	ccess : 1		Host: Site300-cE1(1.1.30.1) Site ID: 300
Device Group (1)		Device C8000v Model:
Q Search Table	Меззаре	Chassis Number	[26-Jul-2024 13:55:55 PDT] Configuring device with feature template: fc862ea4-e57e-4616-8bc7-88d2d2978089 [26-Jul-2024 13:55:58 PDT] Checking and creating device in Manager [26-Jul-2024 13:55:59 PDT] Device is online [26-Jul-2024 13:55:06 PDT] Device is online [26-Jul-2024 13:55:06 PDT] Updating device configuration in Manager [26-Jul-2024 13:55:06 PDT] Earling configuration to device
Success	Template successfully atta	C9K:C16B1FE2-C699F-A311-DEA7-46;	[26-Jul-2024 13:56:12 PDT] Successfully notified device to pull configuration [26-Jul-2024 13:56:13 PDT] Device Parind ICX [26-Jul-2024 13:56:35 PDT] Device Started ICX [26-Jul-2024 13:56:35 PDT] Device Successfully downloaded package for appld utd [26-Jul-2024 13:56:35 PDT] Device Successfully installed appld utd [26-Jul-2024 13:56:35 PDT] Device Successfully installed appld utd [26-Jul-2024 13:56:35 PDT] Device Successfully installed appld utd [26-Jul-2024 13:56:37 PDT] Device Successfully installed appld utd [26-Jul-2021 13:56:37 PDT] Device Successfully verified applds: utd [26-Jul-2021 13:56:37 PDT] Device Successfully verified applds: utd [26-Jul-2021 13:58:07 PDT] Device Successfully verified applds: utd [26-Jul-2024 13:58:07 PDT] Device Successfully verified applds: utd [26-Jul-2024 13:58:07 PDT] Device Successfully verified applds: utd [26-Jul-2024 13:58:07 PDT] Terplate successfully attached to device

修改URL篩選

要修改URL過濾策略,請執行以下步驟:

1. 從Cisco SD-WAN Manager選單中選擇Configuration > Security。

2. 在「Security」螢幕中,按一下Custom Options下拉選單,然後選擇Policies/Profiles。

									O Security	
20	Monitor								Lists	, í
*	Configuration								Umbrella Registratio	xn I
*	Tools	Q Search							Threat Grid API Key	
\$	Maintenance									
80	Administration	Add Security Polic	y Add Unified Sec	urity Policy						
Ð	Workflows								Total Rows: 3	0 ©
	Reports	Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated	_
	Anabelian	VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	D	admin	12 Apr 2024 9:32:39 PM	

按一下左側頁籤上的URL Filtering,針對要修改的所需策略,按一下3點(...),然後選擇Edit。

Security > URL Filtering					10 The second se	Options v
Select a list type on the left an	d start creating your policies and/or pro	lles				
Firewall	Q Search					V
URL Filtering	Add URL Filtering Policy \vee	(Add a URL Filtering configuration)				
Advanced Matware Protection					Total Rows: 2	t) 🖗
TLS/SSL Decryption	Name	Mode	Reference Count	Updated By	Last Updated	
TLS/SSL Profile	Guest_Access	security	1	admin	24 Jul 2024 11:03:40 PM GMT	
Advanced Inspection Profile	URL-F	security	1	admin	24 Jul 2024 8:14:21 PM GMT	
						Graphical Preview View
					[Edit

URL Filtering - Policy Rule Configuration Policy Mode Security Policy Name Guest_Access Web Categories Blockabused-drugs × games × gambbling × social-network × hact , , , , , , , , , , , , , , , , , , ,		Target 1 VPNs Target VPNs	Block Categories: 5 Web Moderate Reputation: Risk Whitelist: Guest_All Blacklist: Guest_All Blacklist: Guest_Blo Web Filter Block Page Server
	URL Filtering - Poli Policy Mode Policy Name Web Categories	cy Rule Configuration ③ Security ④ Guest_Access Block abused-drugs × gar	nes × gambling × social-network × haci

根據需要修改策略,然後按一下Save URL Filtering Policy。

刪除URL篩選

要刪除URL過濾策略,必須首先從安全策略分離策略:

從Cisco SD-WAN Manager選單中,選擇Configuration > Security。

將URL過濾策略與安全策略分離:

• 對於包含URL過濾策略的安全策略,請點選3點(...),然後點選編輯。

Add Security Policy	Add Unified Secu	arity Policy					
							Total Rows: 3 📢 🎊
Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39 PM
Security-IPS-URLF-AMP	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:49:01 PM
Guest_URL_Policy	Guest_URL_Policy	Custom	security	1	1	admin	24 Jul 2024 11:03:25 PN •••
							View
							Preview
							Edit
							Delete

接著顯示[原則摘要]頁面。按一下URL Filtering(URL過濾)頁籤。

對於要刪除的策略,請點選3點(...),然後選擇分離。

按一下Save Policy Changes。



Preview Save Policy Changes Cancel

要刪除URL過濾策略:

在Security螢幕中,點選Custom Options下拉選單(在Windows 2000中為Linux系統),選擇 Policies/Profiles,然後選擇URL Filtering。

		🚺 The ne	twork is out of co	mpliance due to licensing	g, please click here for m	nore actions.				Security	
20	Monitor								ſ	Lists	
*	Configuration								L	Policies/Profiles Umbrella Registratio	m
*	Tools	٩	Search							Threat Grid API Key	
\$	Maintenance										
20	Administration	Ad	d Security Pol	licy Add Unifie	d Security Policy						
-Ð	Workflows									Total Rows: 3	() ③
	Reports	Name		Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated	
ılıl	Analytics	VIP22	Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39	
Ø	Explore	Securi	ty-IPS-URLF-A	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:49:01	
		Guest,	URL_Policy	Guest_URL_Policy	Custom	security	1	1	admin	25 Jul 2024 4:23:52	

對於要刪除的策略,請點選3點(...),然後點選刪除。

按一下OK。

Security > URL Filtering					tin Custom (Options 🗸
Select a list type on the left and	start creating your policies and/	or profiles				
Firewall Intrusion Prevention	Q Search					7
URL Filtering Advanced Malware Protection DNS Security	Add URL Filtering Polic	y√ (Add a URL Filtering co	nfiguration)		Total Rows: 2	t) @
TLS/SSL Decryption	Name	Mode	Reference Count	Updated By	Last Updated	
TLS/SSL Profile	Guest_Access	security	0	admin	24 Jul 2024 11:03:40 PM GMT	
Advanced Inspection Profile	URL-F	security	1	admin	24 Jul 2024 8:14:21 PM GMT	Graphical Prev
						Edit Delete

Select a list type on the left and s	tart creating your policies and/or pr	ofiles	
Firewall			
Intrusion Prevention	Q Search		_
URL Filtering	Add URL Filtering Policy		
Advanced Malware Protection		Are you sure you want to delete the	
DNS Security		policy?	
TLS/SSL Decryption	Name	This policy will be deleted immediately. You cannot undo the action.	pdated By
TLS/SSL Profile	Guest_Access		dmin
Advanced inspection Profile	URL-F		dmin
		Cancer	

驗證

驗證是否已安裝Cisco UTD版本。

<#root>

Site300-cE1#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.14\$
UTD Installed Version:

1.0.2_SV3.1.67.0_XE17.14

在位於訪客VPN上的客戶端PC上,如果您嘗試打開google.com和yahoo.com,則允許這些訪問。

🔞 🖨 🔲 🛛 Google - Chromium					
G Google	× +				
\leftrightarrow \rightarrow C \cong google.com					
About Store			Gma	il Images	
	۹ ۱		\$		
		Google Search I'm Feeling Lucky			

<#root>

Site300-cE1#show utd engine standard logging events | in google 2024/07/24-13:22:38.900508 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass

[**]

UTD WebFilter Allowlist

[**] [

URL: www.google.com

] [VRF: 12] {TCP} 10.32.1.10:55310 -> 142.250.189.196:443 2024/07/24-13:24:03.429964 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass

[**]

UTD WebFilter Allowlist

[**] [

URL: www.google.com

] [VRF: 12] {TCP} 10.32.1.10:55350 -> 142.250.189.196:443

8 🖲 🗊 Yaho	oo Mail, Weathe	r, Search,	Politics, News,	Finance, Sports & Videos - Ch	romium				
Yahoo	Mail, Weather, Se	× +							
$\leftrightarrow \rightarrow G$	🗎 yahoo.com							☆ .	. :
	3								
			-	vahaal					
		News	Finance	yanoo;	Sports	More ~	Mail	Sign in	
				-					
		Б							
		Search	the web			Q			

```
Site300-cE1#show utd engine standard logging events | in yahoo
2024/07/24-13:20:45.238251 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Pass [

**]

UTD WebFilter Allowlist

[**] [

URL: www.yahoo.com

] [VRF: 12] {TCP} 10.32.1.10:48714 -> 69.147.88.8:443 2024/07/24-13:20:45.245446 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass

[**]

UTD WebFilter Allowlist

[**] [

URL: www.yahoo.com

] [VRF: 12] {TCP} 10.32.1.10:48716 -> 69.147.88.8:443

從位於訪客VPN上的客戶端PC上,如果您嘗試打開信譽得分較低的網頁,或者從其中一個被阻止的 Web類別打開,URL過濾引擎將拒絕HTTPs請求。



```
Site300-cE1#show utd engine standard logging events | in mal
2024/07/24-13:32:18.475318 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Drop

[**]

UTD WebFilter Category/Reputation

[**] [

URL: malware.wicar.org/data/firefox_proto_crmfrequest.html

] ** [Category: Malware Sites] ** [Reputation: 10] [VRF: 12] {TCP} 10.32.1.10:40154 -> 208.94.116.246:8

在位於訪客VPN上的客戶端PC上,如果您嘗試打開facebook,instagram和youtube將被阻止。



```
Site300-cE1#show utd engine standard logging events | in face
2024/07/24-13:05:25.622746 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
Drop
[**]
UTD WebFilter blocklist
[**] [
URL: www.facebook.com
] [VRF: 12] {TCP} 10.32.1.10:55872 -> 157.240.22.35:443
2024/07/24-13:05:25.638612 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
Drop
[**]
UTD WebFilter blocklist
[**] [
UTD WebFilter blocklist
[**] [
URL: www.facebook.com
] [VRF: 12] {TCP} 10.32.1.10:55876 -> 157.240.22.35:443
```



Site300-cE1#show utd engine standard logging events | in insta 2024/07/24-13:09:07.027559 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

] [VRF: 12] {TCP} 10.32.1.10:58496 -> 157.240.22.174:443 2024/07/24-13:09:07.030067 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

] [VRF: 12] {TCP} 10.32.1.10:58498 -> 157.240.22.174:443 2024/07/24-13:09:07.037384 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

```
Drop
```

```
[**]
```

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

] [VRF: 12] {TCP} 10.32.1.10:58500 -> 157.240.22.174:443

S www.youtu	be.com ×	+
\leftrightarrow \rightarrow G () youtube.com	

ľ	1	Ľ
l	2	2

This site can't be reached

The connection was reset.

Try:

- · Checking the connection
- · Checking the proxy and the firewall

ERR_CONNECTION_RESET

<#root>

Site300-cE1#show utd engine standard logging events | in youtube 2024/07/24-13:10:01.712501 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.youtube.com

] [VRF: 12] {TCP} 10.32.1.10:54292 -> 142.250.72.206:443 2024/07/24-13:10:01.790521 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.youtube.com

] [VRF: 10] {TCP} 10.30.1.10:37988 -> 142.250.72.206:443 2024/07/24-13:11:11.400417 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.youtube.com

] [VRF: 12] {TCP} 10.32.1.10:54352 -> 142.250.72.206:443

從vManage GUI監控URL過濾

您可以使用這些步驟,按網路類別即時或歷史地監控每台裝置的URL過濾。

監控Cisco IOS XE Catalyst SD-WAN裝置上被阻止或允許的URL:

1. 在Cisco SD-WAN Manager選單中,選擇Monitor > Devices > Select Device

~∕⊲	Monitor	0	verview		$\overline{}$				
2	Configuration	D	evices	~					
*	Tools	Tunnels Applications Security			Tunnels	Applications	Security	Logs	Multic
\$	Maintenance				licensing				
20	Administration	VPN Logs		LICENSING					
-	Workflows	М	ulticloud						
=	Reports	SD-AVC Cloud Connector Compliance		nector					
Ш	Analytics	_							
Ø	Explore		Hostname	Devi	ce Model	Site Name	System IP	Health	n ©
			vManage	Man	ager	SITE_1	1.1.1.1	0	
			vBond	Valio	lator	SITE_1	1.1.1.2	Ø	
			vSmart-1	Con	troller	SITE_1	1.1.1.3	0	

2. 在左窗格的「安全監控」下,按一下「URL過濾」。URL過濾資訊顯示在右窗格中。

- 按一下Blocked。系統將顯示阻止URL上的會話計數。
- 按一下允許。系統將顯示允許URL上的會話計數。



疑難排解

驗證是否已安裝支援的UTD版本:

<#root>

Site300-cE1#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.14\$
UTD Installed Version:

1.0.2_SV3.1.67.0_XE17.14 <<<<<<<<



注意: UTD安裝的版本不能處於「不受支援」狀態。

檢查UTD是否處於onrunning狀態。

Site300-cE1#show app-hosting list App id State utd RUNNING

驗證UTD健康狀況為綠色。

<#root>

Site300-cE1#show utd engine standard status Engine version : 1.0.2_SV3.1.67.0_XE17.14 Profile : Cloud-Low

: System memory Usage : 11.70 % Status : Green Number of engines : 1 Engine Running Health Reason _____ Engine(#1): None Yes Green Overall system status: Green Signature update status: _____ Current signature package version: 29.0.c Last update status: None Last successful update time: None Last failed update time: None Last failed update reason: None Next update scheduled at: None Current status: Idle

驗證是否已啟用URL過濾功能。

<#root>

Site300-cE1#show platform hardware qfp active feature utd config Global configuration NAT64: disabled Drop pkts: disabled Multi-tenancy: enabled Data plane initialized: yes TLS Decryption Policy: disabled Divert controller mode: enabled Unified Policy mode: disabled SN threads: 12 CFT inst_id 0 feat id 4 fo id 4 chunk id 19 Max flows: 165000 SN Health: channel: Threat Defense : Green SN Health: channel: Service : Down Flow-logging Information: _____ State : disabled Context Id: 3, Name: 3 : 12 Ctx Flags: (0xc50001) Engine: Standard State : Enabled SN Redirect Mode : Fail-open, Divert Threat-inspection: Not Enabled

Domain Filtering : Not Enabled

URL Filtering : Enabled

File Inspection : Not Enabled All Interfaces : Enabled

要顯示URL過濾日誌,請運行show utd engine standard logging events url-filtering命令。

```
Site300-cE1#show utd engine standard logging events url-filtering
2024/07/24-20:36:58.833237 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:37:59.000400 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:37:59.030787 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:38:59.311304 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:38:59.311304 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:38:59.343273 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```



注意:運行clear utd engine standard logging events命令清除舊事件。

將輸入/輸出資料包檢查到UTD容器,查詢延遲。

Site300-cE1#show utd engine standard statistics url-filtering vrf name 12 internal

UTM Preprocessor URLF Statistics

URL Filter Requests Sent:	50
URL Filter Response Received:	50
blocklist Hit Count:	27
Allowlist Hit Count:	0
Reputation Lookup Count:	50
Reputation Action Block:	0
Reputation Action Pass:	50
Reputation Action Default Pass:	0
Reputation Action Default Block:	0
Reputation Score None:	0
Reputation Score Out of Range:	0
Category Lookup Count:	50

Category	Action	Block:		15
Category	Action	Pass:		35
Category	Action	Default	Pass:	0
Category	Action	Default	Block:	0
Category	None:			0
Category	Out of	Range:		0

UTM Preprocessor URLF Internal Statistics

Total Packets Received:	1335
SSL Packet Count:	56
HTTP Header Count:	22
Action Drop Flow:	69
Action Reset Session:	0
Action Block:	42
Action Pass:	503
Action Offload Session:	0
Invalid Action:	0
No UTM Tenant Persona:	0
No UTM Tenant Config:	0
URL Lookup Response Late:	150
URL Lookup Response Very Late:	21
URL Lookup Response Extremely Late:	0
URL Lookup Response Status Invalid:	0
Response Does Not Match Session:	0
No Response When Freeing Session:	0
First Packet Not From Initiator:	0
No HTTP Header:	0
Invalid Action:	0
Send Error Fail Open Count:	0
Send Error Fail Close Count:	0
Lookup Error Fail Open Count:	0
Lookup Error Fail Close Count:	0
Lookup Timeout Fail Open Count:	0
Lookup Timeout Fail Close Count:	0

相關資訊

- <u>Cisco Catalyst SD-WAN安全配置指南</u>
 <u>在cEdge路由器上安裝UTD安全虛擬映像</u>
- 透過UTD和URL過濾排除資料路徑處理故障

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。