Security 周天 2020-12-25 Published

Network Topology

An overseas office needs to configure an application-based security policy to block YouTube. Since t here are no access conditions for youtube in China, the following is an experience case of configuring an application-based security policy to block WeChat.

The configuration method of blocking youtube and blocking WeChat is the same, the difference is that the classification of the application is different, you can find this application by searching youtube in the application search box.

The following matrix shows the hardware and software versions to which this configuration guide is a pplicable:

Hardware	Software version
F5030-D, F5060-D, F5080-D, F5000-AK515, F5000-AK525	E9620 or newer version
F5030, F5030-6GW, F5060, F5080, F5000-M, F5000-A, F5000-AI-20, F5000-AI-40, F5000-V30	E9628 or newer version
F5010, F5020-GM, F5020, F5040, F5000-C, F5000-S	E9342 or newer version
F1000-AI-20, F1000-AI-30, F1000-AI-50	E9345 or newer version
F1000-AI-60, F1000-AI-70, F1000-AI-80, F1000-AI-90	E8601 or newer version
F1005, F1010, F1003-L, F1005-L	E9536 or newer version
F1020, F1020-GM, F1030, F1030-GM, F1050, F1060, F1070, F 1070-GM, F1080, F1000-V70	E9345 or newer version

Restrictions and guidelines

When you configure a security policy, follow these restrictions and guidelines:

·Update the APR signature library to the latest version.

V7-APR-1.0.110 or newer version

-For the applications in a security policy to be identified, you must allow the dependent protocols of th e applications to pass through.

Configuration Steps

Analysis

·This security policy **p** can prohibit prohibit users from using WeChat.

Configure security policy **pass** to allow common protocols for APR to identify applications correctly.

Configure the security policies in the following order:

а. р

b. pass

Procedure

- 1. Assign IP addresses to interfaces and add the interfaces to security zones.
- # On the top navigation bar, click Network.
- # From the navigation pane, select Interface Configuration > Interfaces.
- # Click the Edit icon for GE 1/0/1.
- # In the dialog box that opens, configure the interface:
- a. On the IPv4 Address tab, enter the IP address and mask of the interface. In this example,
- enter 2.2.2.1/24.
- b. Click OK.
- # Configure the IP addresses of GE 1/0/2, in the same way you configure GE 1/0/1.
- 2. Configure security zones.
- # On the top navigation bar, click Network.
- # From the navigation pane, click Security Zones.
- # Click the Edit icon for security zone Untrust.
- # In the dialog box that opens, add GE 1/0/1 to the security zone.
- # Click the Edit icon for security zone Trust.
- # In the dialog box that opens, add GE 1/0/2 to the security zone.
- 3. Configure application groups.
- # On the top navigation bar, click Objects.
- # From the navigation pane, select APP Security > APP Recognition > Application Groups.

Click Create.

In the dialog box that opens, configure an application group named test:

- ¡ Enter group name test.
- i Add wechat applications in the IM category to the Selected Applications pane.
- i Click OK.

on Group		
test test		«(1-63 chars) (0-127 chars)
ry (count)) a) ning_Media(l(12)	Risk type Risk level Vulnerability Image: Comparison of the system of the s	
lications tu	 Filter Selected Applications(51.) Trilian UUV0jP Vsee WangYiPaoPao WeChat WeLove WeLove WhatsApp YbGin 	
	test test ry (count)) 3) ming_Media(I(12)	test test test ry (count) y (count) Uulnerability Malware-vehicle Data-loss Bandwidth-consu C Filter C Filter Selected Applications(51) Trillian WVChat WeChat Wechat

- 4. Configure a security policy named pass.
- # On the top navigation bar, click **Policies**.
- # From the navigation pane, select Security Policies > Security Policies.

Click Create.

- # In the dialog box that appears, configure the security policy:
- i Enter policy name **pass**.
- i Select source zone Any.
- i Select destination zones Any.
- i Select policy type IPv4.
- i Select action Permit.
- # Click OK.
- 5. Configure a security policy named **p**.
- $\ensuremath{\#}$ On the top navigation bar, click $\ensuremath{\textbf{Policies}}$.
- # From the navigation pane, select Security Policies > Security Policies.

Click Create.

- # In the dialog box that appears, configure the security policy:
- ¡ Enter policy name p.
- i Select source zone Any.
- i Select destination zones Any.
- i Select policy type IPv4.
- i Select action Deny.
- i Select application group test.
- i Select logging Enable.

dit Security Policy				@×
IPv4 address(?)				•
Destination IP Address object grou IPv4 address⑦	qı	Any	¥	(Edit)
Service				
Service object group	р	Any	Ŧ	[Edit]
Protocol/Port numb	er	Any	¥	
Application	tes	t, test	¥	(Edit)
Terminal	An	1	Ŧ	[Edit]
User	An	1	Ŧ	
Time range	An	1	Ŧ	
VRF	Pul	blic network	¥	
		Content security		

Logging	Enable	Olisable	
Policy hit counting	Enable		
Session aging	Enable		
Persistent session aging?	Enable		
Policy status	Enable	O Disable	
Redundancy analysis (?)			

Click OK.

					Dash	A board	Q Monite			erts 1	ertwork .	(E) System										
Security Policies	Secur																					
Security Policies	() CH	uter 🛞	Iniert+ X	Delete 🔯		More	• 🛞 En	able stats •	O Disable	stats e 🗆	S Enable	S Disable	To Cear	1945		6/14	e your k	ey~orde	Q,	Search 1	Advance	ed search
Redundancy Analysis Policy Hit Analysis	To has Suppo	e the secu red total p	rity policy co	nfiguration 😁	take effe	n, you each ty	must click pe 5000.	Activate	To have the	e content	security conf	iguration 😗	Like effect	L, you m	et click	Subr	ait . vudi	Dry statu	n (Gray	Already inv	alid: Red	
Policy Optimization		Name	Sec zone	Dut zone	Type	ю	Desc	Src addre	Dut addr	Seni.	Application	Termi	User	Action	Co 1	Mate	Traffic	Enab.,	Left	Ves Se.,	Lfec.	Lift.
Attack Defense		• *	Any	Any	1714	5		Any	Any	Any	a chest	Any	Any	0		225	2			Ves	Yes	C
Zero Trust		e pess	Any	Any	1714	2		Any	Any	Any	Any	Any	Any	Pr.		318.	7		0	Ven	Ves	1
Threat Intelligence																						
A Policy-based NAT																						
A Interface NAT																						
A Interface NAT																						
A Interface NAT Application Audit Audit Policies																						
Ainterface NAT Application Audit Audit Policies Keyword Groups																						
Application Audit Audit Policies Knyword Groups Ander Manageme																						
Application Audit Audit Policies Keyword Groups Bandwidth Manageme Dicad Balancing																						
Autorrace NAT Standard Real Coups Audit Policies Knywood Groups Bandwidth Manageme Load Balancing Setshare Control																						
Alinterface NAT El Application Audit Audit Policies Knyword Groups Bandwidth Manageme Load Balancing Server Connection Det																						
Anterface NAT Add Policies Add Policies Knyword Groups Bandwidth Manageme Gload Balancing Shetshare Control Server Connection Det Server Connection Det Server Connection Det																						

- 6. Configure an audit policy named test.
- # On the top navigation bar, click **Policies**.
- # From the navigation pane, select $\mbox{\bf Application}\ \mbox{\bf Audit} > \mbox{\bf Audit}\ \mbox{\bf Policies}.$
- # Click Create.
- # In the dialog box that appears, configure the application audit policy:
- ¡ Enter policy name test.
- i Select source zone Any.
- i Select destination zones Any.
- i Select policy type Audit.

	Audit Audit						
Enable	2						
Source sec-zone	Any					₩ (Ed	it
Destination sec-zone	Any					- (Ed	it)
Source IP address	Any					₩ (Ed	it]
Destination IP address	Any					- (Ed	it)
Service	Any					Ψ (Ed	it]
User	Any					÷	
	Any						
Time range	Any					w	
Audit rule*							
🕀 Create 🛛 🗙 Delete 🛛	Default rule action: 💿 i	Permit O Der	ny Match	n mode: 💿 In	-order 🔿 Al		
Rule ID Appli E	leha Behavior c	Match type	Oper	Keyword	Loggi	Action	Edit
1 We	All Audit all	Keyword	Incl	arry	Ena	Per	Ø

Configure an **audit rule** to perform refined auditing on the behaviors and behavior contents of appli cations. This item can be configured only for an Audit-type policy.

- i Click Create.
- ¡ Enter rule ID 1.
- i Select application IM > WeChat.
- i Select behavior All behaviors.
- i Select behavior content Audit all.
- i Select logging Enabled.

Edit Audit Rule		@×
Rule ID	1	* (1-64)
Application	IM ~ WeChat	¥
Behavior	All behaviors 👻 Behavior content Audit all	¥
Match type	Keyword Number	
Keyword	Include 👻 any	¥
Email protection	C Enable	
Action	Permit	¥
Logging	Enabled	~
	Apply Cancel	

HBC inter			Deshboard N		Digenta		(E) System					9 atris =	000
© Security Policies	Audit Policy												
- Security Policies	Create X	Delete 🔒 Copy 🛞 Ex	uble 🚫 Diuble	- Move Defau	h policy action: 🐞 Pe	enit : De	w.				Enter your i	ayvords	Q, Search
- Redundancy Analysis	To have the cost	iguration ⁽¹⁾ take effect, yo	w must click Submit	E.									
Policy Hit Analysis	Name Name	Source security zone	Destination securit	Source IP add	Destination IP add.	Senice	Application	User	Status	Application se.	Time range	Type	1.dt
Policy Optimization	test.	Any	Any	Any	Any	Any	Any	Any	0	0	Any	Audit	1
Attack Defense													
Ø Zero Trust													
Carl Threat Intelligence													
A Policy-based NAT													
AInterface NAT													
© # Application Audit													
Audit Policies													
Keyword Groups													
Bandwidth Manageme													
Coad Balancing													
Control													
Server Connection Det													
Application Proxy													
	In the Page	1 of 1 -> ->>	Entries per page 25									Displayie	191-1 of 1

Verifying the configuration

Verify that the users can not use WeChat, open WeChat cannot display QR codes, and can not log on by scanning QR codes.

微信		¢	×
	请使用微信扫一扫以登录		

Verify that security polices can be hit correctly by selecting **Monitor** > **Security Logs** > **Security P olicy Logs**. The following are examples of security policy hitting:

HBC 🔤				Cash Jooserd Monster	Police	0.00	ets Network	C System						
Application Analysis	Security Policy Log Liv													
Security Logs	C Rehesh Import	& Export	📫 Clear	Search results: 2020-1	11-18 00:00	00-17:07:49	09 metching logs.					£.4	Advanced se	arch
Blacklist Logs	Time *	Source	Destinat.	Security policy	Rule 1D	Protocol	Application	Source IP address	Source	Destination IP addre	Destinat.	Number of rul	Action	
Single-Packet Attack L	2020-11-18 17:04	Trust	United		5	TCP	WeChat	10.00.2	1733	122.192.127.61	443	.8	Deny	ň
- Scanning Attack Logs	2020-11-18 17:03	Trust	Unitrust		1	TCP	WeChat	50.00.2	1714	223.166.152.105	8080	9	Deny	1
Flood Attack Logs	2020-11-18 17:03	Trust	United		1	TCP	WeChat	10.00.2	1711	116128333.001	443	7	Deny	1
Threat Logs	2020-11-18 17:01	Trust	United		1	TCP	WeChat	10.0.0.2	1709	116.128.133.102	80	9	Deny	1
Reputation Logs	2020-11-18 17:03	Trunt	United	2	1	TCP	WeChat	30.00.2	1708	116.128.133.100	8080	9	Deny	1
URL Filtering Logs	2020-11-18 17:03	Trust	Unervit		1	TCP	Wethat	10.00.2	1706	116.128.171.219	80	9	Deny	1
File Filtering Logs	2020-11-18 17:01-	Trunt	Untryst		1	TCP	WeChat	10.0.0.2	1705	220.194.91.159	443	6	Deny	1
Security Policy Logs	2020-11-18 17:03	Trust	Unitsuit		1	TCP	WeChat	30.0.0.2	1704	116.128.363.195	80		Deny	1
Sandbox Logs	2020-11-18 17:02	Trunt	Untrust		1	TCP	WeChat	10.0.0.2	1700	101.89.15.100	80	6	Deny	1
NAT Logs	2020-11-18 17:02	Trust	Unitrat		1	TCP	WeOwt	10.00.2	1702	116.128.133.100	8080	.9	Deny	
SSL VPN User Access L	2020-11-18 17:02	Trust	Untrust		1	TCP	WeChat	10.0.0.2	1697	223.166.152.106	443	.9	Deny	
SSL VPN Access Resou	2020-11-18 17:02	Trust	United		1	TCP	WeChat	50.00.2	2692	223.166.152.100	80		Deny	
Terminal Logs	2020-11-18 17:02	Trust	Unerval		1	TCP	WeChat	10.0.0.2	3684	116.126.171.39	80	9	Deny	
C Application Audit Lo	2020-11-18 17:02	Trust	Untrial		1	TCP	WeChat	30.00.2	1683	116.128.363.191	80		Deny	
Cevice Logs	2020-11-18 17:02	Trust	Unervat		1	TCP	WeChat	50.00.2	5676	223.166.152.100	80		Deny	
• Statistics	IF E Pape 1	of 3 🏓	-H Entrie	s per page 25 •								Display/	ing 1 - 25 of	60

Verify that application audit policy can be hit correctly by selecting **Monitor** > **Application Audit L og** > **IM Application Logs**. The following are examples of application audit policy:

HBC inte			• •	Dilices Objects	Detwork System				
Application Audit Lo	BM Logs El Search C Refer	h 🗈 Import 🖹 Expor	🔮 Clear Search resu	# 2020-11-18 has 9 log ent	ies .				
- Community Loos	User	Application	Account	Behavior	Action	System	Terminal	Time	Details
Search Engine Long	50.0.0.2	WeChat		Login	Parmit			2020-11-18 16:58:13	-
Mallow	10.00.2	WeOut		Login	Permit			2020-11-18 16:58:05	
File Transfer Loop	55.6.0.2	Welhat		Login	Parmit			2020-11-18 16:57:56	
- DVT and Grack Long	10.00.2	WeChat		Login	Drop			2020-11-18 16:54:29	
Other Application Long	10.0.0.2	Wethat		Login	Drop			2020-11-18 16:54:22	
0.0 Device Law	10.00.2	WeChat		Login	Drop			2020-11-18 16:54:10	
Device Logs	10.00.2	Wethat		Login	Drop			2020-11-18 16:53:50	
Statistics	10.00.2	WeChat		Login	Drop			2020-11-18 16:51:42	
Et Botnet Analysis	10.0.0.2	WeDut		Login	Drop			2020-11-18 16:53.18	
Asset Security									
threat Case Manage									
Reports									
Sessions									
TLB Session Informati									
DNC Carba	in in Page 1	d1 + + 25 •						Displayie	1g1-9 of 9

Log [Details		×
-Lo	og information		
Ti	me: 2020-11-18 16:54:29	Action: Drop	
U	ser/User group: 10.0.0.2/10.0.0.2	Source IP address: 10.0.0.2	
D	estination IP address: 101.89.15.106	System :	
Te	erminal :		
-A	pplication information		
A	pplication: WeChat	Behavior: Login	
A	ccount information		
A	ccount:		

Key Configuration

Summary

In addition to configuring security policies, application audit policies must also be configured.

The configuration method of blocking youtube and blocking WeChat is the same, the difference is that the classification of the application is different, you can find this application by searching youtube in the application search box.