Firepower資料路徑故障排除第4階段:訪問控制 策略

目錄

簡介
訪問控制策略(ACP)階段故障排除
檢查連線事件
快速緩解步驟
調試ACP
範例 1:流量匹配信任規則
範例 2:與信任規則匹配的流量被阻止
案例 3:流量被應用標籤阻止
要提供給TAC的資料
下一步:SSL策略層故障排除

簡介

本文是一系列文章的一部分,這些文章介紹了如何對Firepower系統的資料路徑進行系統故障排除 ,以確定Firepower的元件是否影響流量。請參閱<u>概述文章</u>,瞭解有關Firepower平台架構的資訊 ,以及指向其他資料路徑故障排除文章的連結。

本文涵蓋Firepower資料路徑故障排除的第四階段,即訪問控制策略(ACP)。 此資訊適用於當前所有 支援的Firepower平台和版本。



訪問控制策略(ACP)階段故障排除

一般來說,確定一個流匹配的ACP規則應該非常直觀。可以檢視「連線事件」,以檢視正在執行哪 個規則/操作。如果這沒有清楚地顯示ACP對流量執行的操作,則可以在Firepower命令列介面 (CLI)上執行調試。

檢查連線事件

瞭解了入口和出口介面後,流量應匹配以及流量資訊,識別Firepower是否阻止流量的第一步是檢查 相關流量的連線事件。可在Firepower管理中心的**分析>連線>事件**下檢視這些資訊。

附註:檢查連線事件之前,請確保在ACP規則中啟用日誌記錄。日誌記錄在每個訪問控制策略 規則中的「日誌記錄」頁籤以及安全情報頁籤中配置。確保將可疑規則配置為將日誌傳送到「 事件檢視器」。 這也適用於預設操作。

	0	Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🤱 System Help + Global \ admin + Context Explorer Connections + Events Intrusions + Files + Hosts + Users + Vulnerabilities + Correlation + Custom + Lookup + Search																		
	Bootmark This Page Record Designer Dashbard Vere Bootmarks Search •																			
	Connection Events (mitch workflow)																			
INFORMATION PROVINCE SUPERVISE SU	<u>C</u>	onnection	s with Application De	tails > Table View of Co	nnection E	cents					2017-05-11 13:54:32 - 201	Expanding								
Image:	No	o Search (arch Constraints (<u>Edit Search</u>)																	
• Fund Packet Base Main Base Base<		Jung to •																		
NULL NULL <th< th=""><th></th><th></th><th>• First Packet</th><th>Last Packet</th><th>Action</th><th>Reason</th><th>Initiator IP</th><th>Initiator</th><th>Responder IP</th><th>Responder</th><th>Ingress Security Zone</th><th>Egress Security Zone</th><th>Source Port /</th><th>Destination Port /</th><th>Application</th><th>Client</th><th>Web Application</th><th></th><th></th><th></th></th<>			• First Packet	Last Packet	Action	Reason	Initiator IP	Initiator	Responder IP	Responder	Ingress Security Zone	Egress Security Zone	Source Port /	Destination Port /	Application	Client	Web Application			
Image: Source of the state of the	5		2017-05-11 14:54:32	2017-05-11 14:55:02	Allow		192.168.1.200		73.173.197.235	USA		And a state of the	60084 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing			
 2012-05-1114-53.24		L ()	2017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		73.173.197.235	USA			60082 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing			
 2012-55:11:15:25 2012-55:11:15:25 2012-55:11:15:26 2012-55:11:15:26		1 0	2017-05-11 14:53:40	2017-05-11 14:53:55	Allow		192.168.1.200		10.83.181.139				60077 / tcp	135 (loc-srv) / tcp	DCE/RPC	Epmag				
Sul2-Scill4:Sli2 Sul2-Scill4:Sli2 <th< td=""><td>1</td><td>L 🗆</td><td>2017-05-11 14:52:40</td><td>2017-05-11 14:52:55</td><td>Allow</td><td></td><td>192.168.1.200</td><td></td><td>10.83.181.139</td><td></td><td></td><td></td><td>60069 / tcp</td><td></td><td></td><td>(</td><td></td><td></td><td></td><td></td></th<>	1	L 🗆	2017-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		10.83.181.139				60069 / tcp			(
Solit Solit <th< td=""><td>1</td><td></td><td>2017-05-11 14:51:40</td><td>2017-05-11 14:51:53</td><td>Allow</td><td></td><td>192.168.1.200</td><td></td><td>10.83.181.139</td><td></td><td></td><td></td><td>60064 / tcp</td><td>Connection Events</td><td></td><td>(unnamed search)</td><td></td><td>Private</td><td>Save Save As New Search</td><td></td></th<>	1		2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		192.168.1.200		10.83.181.139				60064 / tcp	Connection Events		(unnamed search)		Private	Save Save As New Search	
S 2012-05-11 14:50:2 More Site 10:2 More More Uran More Uran <th< td=""><td>4</td><td></td><td>2017-05-11 14:51:24</td><td>2017-05-11 14:51:24</td><td>Allow</td><td></td><td>192.168.1.200</td><td></td><td>172.217.26.206</td><td>SA USA</td><td></td><td></td><td>60058 / tcp</td><td>Sections</td><td></td><td>Networking</td><td></td><td></td><td></td><td></td></th<>	4		2017-05-11 14:51:24	2017-05-11 14:51:24	Allow		192.168.1.200		172.217.26.206	SA USA			60058 / tcp	Sections		Networking				
 2012-05-111445024 2012-05-111445024 2012-05-11144502 2012-05-11144502	1		2017-05-11 14:50:40	2017-05-11 14:50:55	Allow		192.168.1.200		10.83.181.139				60056 / tcp	General Information Networking		Initiator IP* Responder IP*	192.168.1.200		192.168.1.0/24, 1192.168.1.3, 2001:db8:8 192.168.1.0/24, 1192.168.1.3, 2001:db8:8	
Sul2-55-11 Sul2-55-11 <td></td> <td>L D</td> <td>2017-05-11 14:50:24</td> <td>2017-05-11 14:50:24</td> <td>Allow</td> <td></td> <td>192.168.1.200</td> <td></td> <td>172.217.26.206</td> <td>usa 🔜</td> <td></td> <td></td> <td>60050 / tcp</td> <td>Geolocation</td> <td></td> <td>Original Client 37*</td> <td></td> <td></td> <td>192.168.1.0/24, 1192.168.1.3, 2001:db8:8</td> <td></td>		L D	2017-05-11 14:50:24	2017-05-11 14:50:24	Allow		192.168.1.200		172.217.26.206	usa 🔜			60050 / tcp	Geolocation		Original Client 37*			192.168.1.0/24, 1192.168.1.3, 2001:db8:8	
• •			2017-05-11 14:50:23	2017-05-11 14-50-53	Allow		192.168.1.200		73, 173, 197, 235	III USA			60051 / trp	Device		Initiator / Responder IP			192.168.1.0/24, 1192.168.1.3, 2001:088:8	
Out/SPELIA Out/SPE			2012.05.11.14.40.42	2012.05.11.14.40.42	Allow					A LUCA			60043 / http	Application		Initiator / Original Clene IP Initiator / Responder / Original Cl	ert IP		192.168.1.0/24, (192.168.1.3, 2001:008.8., 192.168.1.0/24, (192.168.1.3, 2001:008.8.,	
• 2012-55:11:45:42 2012-55:11:45:		• •	2017-05-11 14:49:47	2017-05-11 14:49:47	ALC:N		192.100.1.200		WE 172.217.20.200	<u>1028</u>			5500437 tcp	URL		Ingress Security Zone			My Security Zone	
Image: Solution of the	1	•	2017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		10.83.181.139				60046 / tcp	Netflow		Egress Security Zone			My Security Zone	11
 2022-65:1144492 2022-65:114492 	4	↓ □	2017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		72.246.56.139	JUSA			60041 / tcp	Quố		Ingress / Egress Security Zone Source But / ICMP Type			My Security Zone 1-1024, 6000-6011, IR0	
 2012-05-11144845 2012-05-1114485 2012-05-114485 2012-05-114485 2012-05-114485 2012-05-114485 2012-05-1144855 2012-05-11448555 2012-05-11448555 2012-05-11448555			2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		73.173.197.235	💷 USA			60040 / tcp			Destination Port / ICMP Code*			1-1024, 6000-6011, 190	
 2012-05-1114-48-02 2012-05-1114-47-02 2012-05-1114-47-02	4	ا ا	2017-05-11 14:48:40	2017-05-11 14:48:55	Allow		# 192.168.1.200		10.83.181.139				60037 / tcp	Cished		Protocal*			tcp, udp	
 2012-05-11 14:48:16 2012-05-11 14:48:	1	L 🗆	2017-05-11 14:48:32	2017-05-11 14:48:32	Allow		192.168.1.200		172.217.26.206	USA			60031 / tcp			DNS Query DNS Bernoren			suspideus.com, evit*	
Image: Second			2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192.168.1.200		73.173.197.235	usa 🔜			60034 / tcp	Predefined Searches		DNS Record Type			A, PTR	
• •			2017-05-11 14:47:46	2012-05-11 14:48:16	Allow		102 168 1 200		73 173 107 235				60030 / trp			DNS TTL			43200	
• 01/-02-11/34/218 001/-02-11/34/218 0002/118 01/-02-11/34/218				2017-02-11 14.40.10	COLOR IN					A REAL PROPERTY AND INCOME.			1000201 top			DNS Sinkhole Name			Ny Sinkhole	
 2012-05-111442113 2012-05-111442143 2012-05-11144213 2012-05-111442134 2012-0		• •	2017-05-11 14:47:40	2017-05-11 14:47:55	Allow		M 192.168.1.200		B 10.83.181.139				500277 tcp	Risky Applications with Lov	v business	VLAN ID			10	
Image: Second Part 14:47/15 2017-05-1114:47/15 2017	1	• •	2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		MI 192.168.1.200		間 72.246.56.169	USA USA			60022 / tcp			Geolocation				
\$ 2012-05-11.14:45:45 2012-05-11.14:45:15 Allow # 132.158.1.200 # 123.123.197.235 Hubber 1 Descent 400 T Descent 400	4		2017-05-11 14:47:15	2017-05-11 14:47:45	Allow		192.168.1.200		73.173.197.235	USA USA			60021 / tcp	Standard Hall		Initiator Country			USA, United States, United*	
			2017-05-11 14:46:45	2017-05-11 14:47:15	Allow		192.168.1.200		73.173.197.235	JUSA			60017 / tcp	Standard SSL		Responder Country			USA, United States, United*	
Original Oters Country USA, United States, United*			Received and a second				-	_	-							Original Client Country			USA, United States, United*	
Tell copil on Tellop/pat/24/24/24/24/24/10/Init/j.bit/24/24/24/10/Init/j.bit/24/24/24/10/Init/j.bit/24/24/24/10/Init/j.bit/24/24/24/24/Init/j.bit/24/24/24/24/Init/j.bit/24/24/24/24/24/24/24/24/24/24/24/24/24/	u	ist login on	Tuesday, 2017-04-25 at	12:42:21 PM from rtp-flip	ey-88111.	isco.com										Instator / Responder Country			USA, United States, United*	

通過按一下「編輯搜尋」並按唯一的源(啟動器)IP進行過濾,您可以看到Firepower檢測到的流。 「操作」列對此主機的流量顯示「允許」。

如果Firepower有意阻止流量,則操作將包含「阻止」一詞。 按一下「連線事件的表檢視」可提供 更多資料。如果操作為「Block」,則可以檢視連線事件中的以下欄位:

- 原因
- 訪問控制規則

快速緩解步驟

為了快速緩解據信由ACP規則引起的問題,可以執行以下操作:

- 為相關流量建立具有「信任」或「允許」操作的規則,並將其置於ACP的最頂端,或者在所有 塊規則之上。
- 使用包含「Block」一詞的操作暫時禁用所有規則
- 如果Default Action設定為「Block All Traffic」,請暫時將其切換到「Network Discovery Only」

附註:這些快速緩解需要策略更改,而並非在所有環境中都如此。建議先嘗試使用系統支援跟 蹤來確定流量匹配的規則,然後再進行策略更改。

調試ACP

通過> system support firewall-engine-debug CLI實用程式可以針對ACP操作執行進一步的故障排除 。

附註:在Firepower 9300和4100平台上,可以通過以下命令訪問有關外殼:

connect module 1主控台 Firepower-module1> connect ftd 對於多例項,可以使用以下命令訪問邏輯裝置CLI。 **# connect module 1 telnet** Firepower-module1> **connect ftd ftd1** 正在連線到容器ftd(ftd1)控制檯……輸入「exit」以返回啟動CLI >

system support firewall-engine-debug實用程式包含由ACP評估的每個資料包的條目。它顯示發生 的規則評估過程,以及規則匹配或不匹配的原因。

附註:在6.2及更高版本中,可以運行**系統支援跟蹤**工具。它使用相同的引數,但包含更多詳 細資訊。當提示輸入「Enable firewall-engine-debug too?」時,請務必輸入「y」。

範例 1:流量匹配信任規則

在下面的示例中,使用system support firewall-engine-debug評估SSH會話的建立。

這是Firepower裝置上運行的ACP。

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applic	Sourc	Dest P	URLs	ISE/S Attrib	Acti	V
-	Mandatory - JG AC	(all) (1-6)												
1	Trust ssh for host	Any	Any	2192.168.0.7	Any	Any	Any	Any	Any	🥜 SSH	Any	Any	⇒ Tru	ist 🛈 🐚
2	inspect	Any	Any	👳 10.0.0/8 🗜	Any	Any	Any	Any	Any	Any	Any	Any	🛹 Allo	owiji 🐚
3	trust server backup	Any	Any	2 192.168.62.3	2 10.123.175.22	Any	Any	Any	Any	Any	Any	Any	⇒ Tru	ist 🛈 🗓

ACP有三個規則。

- 1. 第一條 規則是信任來自192.168.0.7的所有流量與SSH使用的目標埠。
- 2. 第二個規則根據XFF報頭資料檢查源自10.0.0.0/8的所有流量(如網路對象旁邊的圖示所示
 -),其中網路條件匹配
- 3. 第三條 規則信任從192.168.62.3到10.123.175.22的所有流量

在故障排除場景中,正在分析從192.168.62.3到10.123.175.22的SSH連線。

預期會話與AC規則3「信任伺服器備份」匹配。 問題在於,此作業階段需要多少封包才能與此規則 相符。第一個資料包中是否需要所有資訊來確定AC規則或需要多個資料包?如果是,需要多少個資 料包?

在Firepower CLI上,輸入以下內容以檢視ACP規則評估流程。

>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages

提示:最好在運行firewall-engine-debug時填寫儘可能多的引數,以便僅顯示感興趣的調試消

在下面的調試輸出中,您會看到正在評估的會話的前四個資料包。

SYN

SYN, ACK

ACK

第一個SSH資料包(客戶端到伺服器)



這是一個進一步說明調試邏輯的圖表。

- 1. SYN 192.168.62.3 → 10.123.175.22
- 2. SYN,ACK 10.123.175.22 → 192.168.62.3
- 3. ACK 192.168.62.3 → 10.123.175.22
- 4. SSH 192.168.62.3 → 10.123.175.22

Starts evaluation at 'inspect' rule

Service identified as SSH No match 'inspect' rule (non-http) Match 'trust server backup' rule and Trust flow

對於此流,裝置需要4個資料包才能匹配規則。

以下是偵錯輸出的詳細說明。

- ACP評估過程從「檢查」規則開始,因為「主機的信任ssh」規則不匹配,因為IP地址不符合要求。這是一個快速匹配,因為判斷此規則是否匹配所需的所有資訊都存在於第一個資料包 (IP和埠)中
- 在識別應用之前,無法確定流量是否與「inspect」規則匹配,因為在HTTP應用流量中發現X-Forwarded-For(XFF)資訊,但應用尚未知,因此這會將規則2的會話置於掛起狀態,掛起應用 資料。
- 在第四個資料包中標識應用後,「inspect」規則將產生不匹配結果,因為應用是SSH而不是 HTTP
- •然後根據IP地址匹配「信任伺服器備份」規則。

總之,連線需要4個資料包來匹配會話,因為它必須等待防火牆識別應用程式,因為規則2中含有應 用程式約束。 如果規則2隻有來源網路,而不是XFF,則這將需要1個封包來匹配作業階段。

在可能的情況下,應始終將第1-4層規則置於策略中的所有其他規則之上,因為這些規則通常需要 1個資料包才能做出決定。但是,您可能也注意到,即使僅使用第1-4層規則,匹配交流規則可能也 不會只使用1個資料包,這是因為URL/DNS安全情報。如果其中任何一個啟用,防火牆必須確定由 AC策略評估的所有會話的應用程式,因為它必須確定它們是HTTP還是DNS。然後,它必須根據黑 名單確定是否允許會話。

以下是firewall-engine-debug命令的截斷輸出,其中相關欄位以紅色突出顯示。記下用於獲取已標識 的應用程式名稱的命令。

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect' , and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect' , XFF wait for AppId
[omitted for brevity]
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect' , and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 846 , payload -1, client 200000846 , misc 0, user 9999997, icmpType 0, icmpCode 0 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
[! How to map service/application ID to name] > expert \$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data 846 SSH 32 0 0 ssh

範例 2: 與信任規則匹配的流量被阻止

Block

在某些情況下,儘管匹配了ACP中的信任規則,仍可以阻止流量。以下示例評估具有相同訪問控制 策略和主機的流量。

Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp			1	JG AC (all)	trust server backup
Action ×	<u>Reason</u> ×	Initiator IP ×	Responder X IP	Source Port / × ICMP Type	Destination Port / × ICMP Code	Application × Protocol	<u>Client</u> ×	Intrusion × Events	Access Control × Policy	Access Control × Rule
	92.168.62.3-5 92.168.62.3-5 92.168.62.3-5	4650 > 10.123.1 4650 > 10.123.1 4650 > 10.123.1	75.22-22 6 AS 1 75.22-22 6 AS 1 75.22-22 6 AS 1	0 no match ru 0 no match ru 0 match rule	ule order 3, 'Trust s ule order 4, 'inspect order 5, 'trust serve	sh for host', s ', XFF non-htt r backup', act	rc network a p iion Trust	and GEO		
1	92.168.62.3-5	4650 > 10.123.1	75.22-22 6 AS 1	I 0 Starting with	n minimum 0, id 0 and	d IPProto first v	vith zones 1 -	-> 2, geo 0 ->	0, vlan 0, inline	
E T	Session was his happened irewall engine	deleted becaus I before AC rule e will re-evalua	se we hit a drop e was matched te from top of A	IPS rule and bl (Intrusion polic C policy to find	lacklisted the flow. y before AC rule ma l a rule for logging o	atch dropped) decision]				
1 1 1 1	92.168.62.3-5 92.168.62.3-5 hline sgt tag: u 92.168.62.3-5 92.168.62.3-5	4650 > 10.123.1 4650 > 10.123.1 htagged, ISE sg 4650 > 10.123.1 4650 > 10.123.1	75.22-22 6 AS 1 75.22-22 6 AS 1 t id: 0, svc 0, pa 75.22-22 6 AS 1 75.22-22 6 AS 1	10 New sessio 10 Starting wit yload 0, client 0, 10 pending rul 10 Deleting set	n h minimum 4, 'insp misc 0, user 999999 e order 4, 'inspect', ssion	ect', and IPPro 7, icmpType 0, XFF wait for <i>i</i>	oto first with z , icmpCode 0 AppId	ones 1 -> 2,	geo 0 -> 0, vlan (),

如上所示,firewall-engine-debug輸出顯示流量與「信任」匹配,而連線事件顯示由於入侵策略規則 導致的**阻止**操作(由於「原因」列顯示**入侵阻止**而確定)。

發生這種情況的原因是在訪問控制規則被確定在ACP上Advanced頁籤中的Setting之前使用的入侵 策略。在根據規則操作對流量進行信任之前,相關入侵策略會識別模式匹配並丟棄流量。但是,由 於IP地址與「信任伺服器備份」規則的條件匹配,因此ACP規則評估的結果與信任規則匹配。

為了使流量不經過入侵策略檢測,可以將信任規則置於「inspect」規則之上,這是兩種情況下的最 佳實踐。由於應用程式標識對於「檢查」規則的匹配和不匹配是必需的,因此確定訪問控制規則之

前使用的入侵策略(**Intrusion Policy)將用於該規則評估的流**量。將「trust server backup」規則置於「inspect」規則之上會導致在發現第一個資料包時流量與規則匹配,因為該規則基於IP地址,而第 一個資料包中可以確定該IP地址。因**此,確定訪問控制規則之前使用的**入侵策略不需要使用。

案例 3:流量被應用標籤阻止

在此案例中,使用者報告正在阻止cnn.com。不過,並沒有什麼具體的規定會阻止CNN的播出。連 線事件以及firewall-engine-debug輸出會顯示阻止的原因。

首先,「連線事件」在應用程式欄位旁邊有一個資訊框,其中顯示有關應用程式的資訊以及 Firepower對此應用程式的分類方式。

▼ First Pace	ket ×	Last × Packet	Action ×	Initiator IP ×	Responder ×	Source Port / × ICMP Type	Destination Port / × ICMP Code	Application × Protocol	Web × Application	Application × Risk	Business × Relevance	<u>URL</u> ×
2017-05-19	16:02:29		Block	192.168.62.63	151.101.65.67	<u>54308 / tcp</u>	80 (http) / tcp	HTTP HTTP	CNN.com	Medium	Medium	http://cnn.com/
	CN Turr Typ	N.com ner Broadca	sting Syste	m's news website Wel	e. p Application			1	/			
I	RIS	K	wance	Ver	y Low							
	Cat	egories	, vunce	mul	timedia (TV/vide	o), news						
I	Тад	S		disp	olays ads							
		diades Contex	xt Explorer	W Wikipedia	G Google	Yahoo!	Bing					

記住此資訊後,會執行firewall-engine-debug。在調試輸出中,根據應用標籤阻止流量。

192 168 62 63-54308 > 151 101 65 67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4. 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0.
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 1 0 Starting with minimum 4, block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vian 0, inline sgt tag: untagged, ISE sgt id: 0, svc 6/6, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 0 match rule order 4, 'block by tag', action Block
192,168.62.65-54.308 > 151.101.65.67-80 6 AS 11 0 senaing block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 11 0 Deleting session

即使沒有明確阻止<u>http://cnn.com</u>的規則,ACP規則的Applications頁籤中仍會阻止已標籤的廣告。

Editing	Rule - block by tag											? ×
Name	block by tag				🕑 Enable	d	4	love				
Action	💢 Block with reset		~	• • • • 2 4	1 🔎							
Zone	s Networks VLAN Tags	🛆 User	5	Applications	Ports	URLs	SGT/ISE Att	tributes		Inspection	Logging	Comments
Applica	tion Filters Clear All	Filters 💢	Ava	ailable Applicati	ons (759)	C			Selecter	d Applications	and Filters (1) 🧏 📩 💽
🔍 Sea	rch by name			Search by name					Filters			
	Service Service	19 🔺		_ enerogea					🛃 Tags	: displays ads		8
	🛛 💿 blog	53		ClickTale						,		U
	🛛 💿 bundles software	7		Clip2Net								
	🛛 💿 business impact	44		Clip2Net Upload			0					
	Common Industrial Protocol	1		CloudFlare			0					
	🛛 💽 console gaming	25		CNBC			0					
	🛛 💿 content provider	28		CNET								
	ecrypted traffic	21		CNET TV			0					
	🛛 💽 displays ads	759		CNN.com			0					
	🔣 eDonkey	2		CNTV			0					
	encrypts communications	280		CNZZ			Ň					
	🔣 evasive	58		Cognitive Match			Ň					
	🛛 🔜 Facebook	27										
E	🛛 💽 Facebook game	23		Collider								
E	🛛 💽 Facebook post	7		Collider			0					
	🛛 🔝 file sharing/transfer	249		Comcast			0					
	🛛 🔜 Flash	39		Comedy Central			0					
E	TP protocol	11		Commission Jun	ction		•					
F	Gnutella protocol	+ n · ·	M	View	ving 101-200) of 759						
											Save	Cancel

要提供給TAC的資料

資料

說明

注意:如果ACP包含SSL策略,請在匯出之前從ACP中刪除SSL策略,以避免洩露敏感的 PKI資訊

下一步:SSL策略層故障排除

如果正在使用SSL策略,並且訪問控制策略故障排除未發現問題,則下一步是對SSL策略進行故障 排除。

按一下<u>here</u>繼續下一篇文章。