Firepower数据路径故障排除第4阶段:访问控制 策略

目录

<u>简介</u> <u>访问控制策略(ACP)阶段故障排除</u> <u>检查连接事件</u> <u>快速缓解步骤</u> <u>调试ACP</u> <u>示例 1:流量匹配信任规则</u> <u>示例 2:与信任规则匹配的流量被阻止</u> <u>情形 3:应用标记阻止的流量</u> <u>向TAC提供的数据</u> <u>下一步:排除SSL策略层故障</u>

简介

本文是一系列文章的一部分,这些文章说明如何系统地排除Firepower系统上的数据路径故障,以确 定Firepower的组件是否可能影响流量。有关Firepower平台架构的信<u>息以及指向其他数据路径故障</u> <u>排除</u>文章的链接,请参阅概述文章。

本文介绍Firepower数据路径故障排除的第四阶段,即访问控制策略(ACP)。 此信息适用于当前支持 的所有Firepower平台和版本。



访问控制策略(ACP)阶段故障排除

一般来说,确定流匹配的ACP规则应该是相当直接的。可以查看Connection Events,以查看正在实施哪些规则/操作。如果这不能清楚地显示ACP对流量执行的操作,则可在Firepower命令行界面 (CLI)上执行调试。

检查连接事件

在了解了入口和出口接口的流量应匹配以及流信息后,确定Firepower是否正在阻止流量的第一步是 检查相关流量的连接事件。在Firepower管理中心的"分析">"连接">"事件"下可以**查看这些信息。**

注意:在检查连接事件之前,请确保在ACP规则中启用日志记录。日志记录在每个Access Control Policy规则的"Logging"(记录)选项卡中以及Security Intelligence(安全情报)选项 卡中配置。确保将可疑规则配置为将日志发送到"事件查看器"。 这也适用于默认操作。

0	Dverview Analysis Policies Devices Objects AMP Intelligence Deploy 🤵 System Help + Global \ admin +																		
	And Capital Connections - Carlins in Section - Carlins - Carlins - Connect - Carlins - Connect - Stellar																		
С																			
C	annections with Application Details > Table View of Connection Events 0 0 2012-05-111.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.15.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-11.25.51.2 - 2012-05-100-100-100-100-100-100-100-100-100-																		
No Search Constraints (Eds Search)																			
	Jump to.																		
	-	• First Packet	Last Packet	Action	Reason	Initiator IP	Initiator	Responder IP	Responder	Ingress	Egress	Source Port /	Destination Port /	Application	Client	Web Application			
							Country		Country	Security Zone	Security Zone	ICMP Type	ICMP Code	Protocol					
-		2017-05-11 14:54:32	2017-05-11 14:55:02	Allow		192.168.1.200		12.173.197.235	M USA			60084 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing			
4		2017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		73.173.197.235	SA USA			60082 / tcp	80 (http) / tcp	HTTP :	Web browser	Web Browsing			
-		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	Epmap				
4		2017-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		10.83.181.139				60069 / tcp	Connection Events		(unnamed search)		Private	Save Save As New Search	
		2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		192.168.1.200		10.83.181.139				60064 / tcp							-
4		2017-05-11 14:51:24	2017-05-11 14:51:24	Allow		192.168.1.200		172.217.26.206	USA			60058 / tcp	Sections		Networking				
1	L 🗆	2017-05-11 14:50:40	2017-05-11 14:50:55	Allow		192.168.1.200		10.83.181.139				60056 / tcp	Networking		Responder IP*	192.168.1.200	-	192.168.1.0/24, 1192.168.1.3, 2001:008:8. 192.168.1.0/24, 1192.168.1.3, 2001:008:8	
		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 3P*			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	USA			60051 / tcp	Device		Initiator / Responder IP			192.168.1.0/24, 1192.168.1.3, 2001:084:8	h
		2017-02-11 14:30:12	2017-02-11 14.20.22	COLUMN I		TRAINING A DOG			MAD			5000.00.00.00.00	SSL Application		Initiator / Original Client IP Initiator / Responder / Original Clie	eri 19		192.168.1.0/24, 1192.168.1.3, 2001:db8:8. 192.168.1.0/24, 1192.168.1.3, 2001:db8:8.	2
	• •	2017-05-11 14:49:47	2017-05-11 14:49:47	Allow		MI 192.168.1.200		172.217.26.205	<u>usa</u>			50043 / tcp	URL		Ingress Security Zone			My Security Zone	
1		2017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		H 10.83.181.139				60046 / tcp	Netflow		Egress Security Zone			Hy Security Zone	
4		2017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		72.246.56.139	M USA			60041 / tcp	QuS		Ingress / Egress Security Zone			Hy Security Zone	
-		2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		13.173.197.235	💶 USA			60040 / tcp	- Ken Kennels		Destination Part / ICMP Code*			1-1024, 6000-6011, 180	
4	•	2017-05-11 14:48:40	2017-05-11 14:48:55	Allow		192.168.1.200		10.83.181.139				60037 / tcp			Protocol*			tcp, udp	
1		2017-05-11 14:48:32	2017-05-11 14:48:32	Allow		192.168.1.200		172.217.26.206	USA			60031 / tcp	Gropar		DNS Query			suspicious.com, evil*	
		2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192 168 1 200		73 173 107 235				60034 / http			DNS Record Type			A, PTR	
		2017-02-11 14:40:10	2017-02-11 11-10-10	CHINER.		A LOD LIGHT DOG			Seato			100000 / 1000	Predefined Searches		DNS TTL			43200	
	• •	2017-05-11 14:47:46	2017-05-11 14:48:16	Allow		192.168.1.200		13.173.197.235	<u>usa</u>			500.30 / tcp			DNS Sinkhole Name			Ny Sinkhole	
		2017-05-11 14:47:40	2017-05-11 14:47:55	Allow		H 192.168.1.200		H 10.83.181.139				60027 / tcp	Risky Applications with Low	Dusiness .	HTTP Response Code			200	
1		2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		192.168.1.200		12.246.56.169	usa usa			60022 / tcp			Geolocation				
4		2017-05-11 14:47:15	2017-05-11 14:47:45	Allow		192.168.1.200		73.173.197.235	SA USA			60021 / tcp	Standard Mail		Initiator Country			USA, United States, United*	
	L 🗆	2017-05-11 14:46:45	2017-05-11 14:47:15	Allow		192.168.1.200		73.173.197.235	USA			60017 / tcp	Standard SSL		Responder Country			USA, United States, United*	
						-		-							Original Client Country			USA, United States, United*	
La	ait login on Tuesday, 2017-04-25 at 12-04-25 at 12-04-25 Mit from rtp-ftplay-68111.cition.com																		
- 10															Wheld constrains summaries and m	ranha			

通过点击"编辑搜索"(Edit Search)并按唯一源(发起方)IP过滤,您可以看到Firepower检测到的流 。"操作"列显示此主机的流量的"允许"。

如果Firepower有意阻止流量,则操作将包含"阻止"一词。 单击"连接事件的表视图"可提供更多数据 。如果操作为"阻止",则可以查看连接事件中的以下字段:

- 原因
- 访问控制规则

快速缓解步骤

为了快速缓解据信由ACP规则引起的问题,可以执行以下操作:

- 为相关流量创建具有"信任"或"允许"操作的规则,并将其置于ACP的最顶部,或高于所有阻止规则。
- 使用包含"阻止"一词的操作临时禁用任何规则
- 如果Default Action(默认操作)设置为"Block All Traffic(阻止所有流量)",请将其临时切换 到"Network Discovery Only(仅网络发现)"

注意:这些快速缓解要求进行策略更改,而这些更改在所有环境中都可能实现。建议先尝试使 用系统支持跟踪来确定流量匹配的规则,然后再进行策略更改。

调试ACP

可通过> system support firewall-engine-debug CLI实用程序对ACP操作执行进一步的故障排除。

注意:在Firepower 9300和4100平台上,可通过以下命令访问相关外壳:

connect module 1 console
Firepower-module1> connect ftd
>

对于多实例,可使用以下命令访问逻辑设备CLI。 **# connect module 1 telnet** Firepower-module1> **connect ftd ftd1** 正在连接到容器ftd(ftd1)控制台……输入"exit"以返回引导CLI >

系统**支持防火墙引擎调试实**用程序为ACP评估的每个数据包都具有一个条目。它显示规则评估过程 以及规则匹配或不匹配的原因。

注意:在版本6.2及更高版本中,**系统支持跟**踪工具可以运行。它使用相同的参数,但包含更 多详细信息。当出现"Enable firewall-engine-debug too?(**也启用防火墙引擎 — 调试?)"提示时 ,请务必**输入"y"。

示例 1:流量匹配信任规则

在以下示例中,使用system support firewall-engine-debug评估SSH会话的建立。

这是在Firepower设备上运行的ACP。

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applic	Sourc	Dest P	URLs	ISE/S Attrib	Acti	•
-	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	⇒ Trư	ist 🗍 🐚
2	inspect	Any	Any	👳 10.0.0/8 🗜	Any	Any	Any	Any	Any	Any	Any	Any	🛹 Allo	ow🥡 🐚
3	trust server backup	Any	Any	2192.168.62.3	👼 10.123.175.22	Any	Any	Any	Any	Any	Any	Any	⇒ Trư	ist 🛈 🐚

ACP有三条规则。

- 1. 第一条规则是信任来自192.168.0.7的任何流量,并且SSH使用目标端口。
- 第二条规则检查源自10.0.0.0/8的所有流量,其中网络条件基于XFF报头数据匹配(如网络对 象旁的图标所示)
- 3. 第三条规则信任从192.168.62.3到10.123.175.22的所有流量

在故障排除场景中,分析从192.168.62.3到10.123.175.22的SSH连接。

期望会话与AC规则3"信任服务器备份"匹配。 问题是,此会话需要多少个数据包才能匹配此规则。 是否需要第一个数据包中需要的所有信息来确定AC规则或多个数据包?如果是,需要多少?

在Firepower CLI上,输入以下命令以查看ACP规则评估流程。

>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:运行firewall-engine-debug时,最好尽可能多地填写**参数,以便仅将相关调试消息打印** 到屏幕。 在下面的调试输出中,您将看到正在评估会话的前四个数据包。

SYN

SYN, ACK

确认

第一个SSH数据包(客户端到服务器)



此图进一步说明了调试逻辑。

- 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

对于此流,设备需要4个数据包才能匹配规则。

这是调试输出的详细说明。

- ACP评估过程从"inspect"规则开始,因为"trust ssh for host"规则不匹配,因为IP地址与要求不匹配。这是快速匹配,因为确定此规则是否匹配时需要的所有信息都存在于第一个数据包(IP和端口)中
- 在识别应用之前,无法确定该流量是否与"检查"规则匹配,因为在HTTP应用流量中找到X-Forwarded-For(XFF)信息,应用尚未知,因此这会将会话置于规则2的挂起状态,即挂起的应 用数据。
- •在第四个数据包中确定应用后,"inspect"规则会导致不匹配,因为应用是SSH,而不是HTTP
- •然后根据IP地址匹配"信任服务器备份"规则。

总之,连接需要4个数据包才能匹配会话,因为它必须等待防火墙识别应用,因为规则2中包含应用 约束。

如果规则2只有源网络,而不是XFF,则这将需要1个数据包来匹配会话。

如果可能,应始终将第1层至第4层规则置于策略中所有其他规则之上,因为这些规则通常需要1个

数据包才能做出决策。但是,您也可能注意到,即使仅使用第1-4层规则,也可能不止1个数据包与 AC规则匹配,原因是URL/DNS安全情报。如果您启用了以上任一功能,则防火墙必须确定由AC策 略评估的所有会话的应用,因为它必须确定这些会话是HTTP还是DNS。然后,它必须根据黑名单 确定是否允许会话。

以下是firewall-engine-debug命令的截**断输出,该命令的相关字段以红色突出显示。**请注意用于获取 已标识的应用名称的命令。

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

示例 2: 与信任规则匹配的流量被阻止

在某些情况下,即使与ACP中的信任规则匹配,流量也可以被阻止。以下示例评估具有相同访问控 制策略和主机的流量。

Block Intrusion Block # 192.168.62.3 # 10.123.175.22 55654 / tcp 22 (ssh / tcp Image: Comparison of the server backup Image: Comparison of the server backup	L	Action ×	<u>Reason</u> ×	Initiator IP ×	Responder × IP	<u>Source Port /</u> × <u>ICMP Type</u>	<u>ICMP Code</u>	Application × Protocol	<u>Client</u> ×	<u>Intrusion</u> × <u>Events</u>	Access Control × Policy	Access Control × Rule
	Ľ	<u>Block</u>	Intrusion Block	192.168.62.3	10.123.175.22	<u>55654 / tcp</u>	22 (ssh) / tcp			1	JG AC (all)	trust server backup

如上所示,**firewall-engine-debug**输出显示流量与"Trust"匹配,而Connection Events显示由于入侵 策略规则(由于Reason列显示**Intrusion Block**而确定的**Block**操作。

出现此情况的原因是,在ACP的"高级"(Advanced)选**项卡中确定"访问控制"(Access Control)规则"设置"(Setting)之前使用的"入侵策略"(Intrusion Policy)。**在根据规则操作可以信任流量之前,相关的入 侵策略会识别模式匹配并丢弃流量。但是,ACP规则评估结果与信任规则匹配,因为IP地址确实与 "信任服务器备份"规则的条件匹配。

为了使流量不经受入侵策略检查,可将信任规则置于"检查"规则之上,这是两种情况下的最佳做法 。由于"检查"规则的匹配和不匹配需要应用标识,因此在确定访问控制规则之前使用的**入侵策略**用 于由相同规则评估的流量。将"信任服务器备份"规则置于"检查"规则之上会导致当发现第一个数据包 时流量与规则匹配,因为该规则基于IP地址,可在第一个数据包中确定。因此,在确**定访问控制规** 则之前使用的入侵策略不需要使用。

情形 3: 应用标记阻止的流量

在此场景中,用户报告cnn.com被阻止。但是,没有阻止CNN的具体规则。连接事件(Connection Events)与**firewall-engine-debug**输出一起显示阻止的原因。

首先,连接事件在应用字段旁边有一个信息框,显示有关应用的信息以及Firepower如何对所述应用 进行分类。

▼ <u>First Packet</u> × <u>Last</u> 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	54308 / tcp	80 (http) / tcp	TTP <u>HTTP</u>	CNN.com	Medium	Medium	http://cnn.com/
CNN.cor Turner Broa Type Risk Business I Categories Tags	dcasting Syste elevance	em's news websit Wel Ver Hig mui disp W Wikipedia	e. b Application y Low h itimedia (TV/vide olays ads G Google	20], news ¥Y Yahoo!	Bing					

考虑到此信息,将运行firewall-engine-debug。在调试输出中,流量根据应用标记被阻止。

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 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, 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 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session

即使没有明确阻止http://cnn.com的规<u>则</u>,标记**的**显示广告在ACP规则的"应**用"**选项卡内被阻止。

Name block by tag Move Action ¥ Block with reset Image: Comments Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Application Filters Clear All Filters Available Applications (759) Selected Applications and Filters (1) Image: Comments Application Filters Clear All Filters Available Applications (759) Selected Applications and Filters (1) Image: Comments Search by name Image: Clear All Filters Valiable Applications (759) Selected Applications and Filters (1) Image: Clear All Filters Search by name Image: Clear All Filters Valiable Applications (759) Selected Applications and Filters (1) Image: Clear All Filters Search by name Image: Clear All Filters Image: Clear All Filters </th <th>Editing</th> <th>Rule - block by tag</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>? ></th>	Editing	Rule - block by tag									? >
Zones Networks VLAN Tags Jusces Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Application Filters Clear All Filters Available Applications (759) C Selected Applications and Filters (1) C C Search by name Search by name Search by name Filters Filters Filters Stormon Industrial Protocol 1 ClickTale C C Filters Tags: displays ads Filters Console gaming 25 CNBC O C Filters Tags: displays ads Filters Console gaming 25 CNBC O C C Filters C	Name Action	block by tag		V V D 21	🕑 Enabled	М	love				
Application Filters Clear All Filters Available Applications (759) Selected Applications and Filters (1) Search by name ClickTale Conneon Industrial Protocol Content provider Search by name Searc	Zone	s Networks VLAN Tag	s 🔺 Users	Applications	Ports URLs	SGT/ISE Att	ributes		Inspection	Logging	Comments
Search by name Search by name Image: Search by name </td <td>Applica</td> <td>tion Filters Clear A</td> <td>All Filters 💢</td> <td>Available Applica</td> <td>tions (759) 🗳</td> <td></td> <td></td> <td>Selec</td> <td>ted Applications</td> <td>and Filters (</td> <td>1) 🧏 🖆 🔘</td>	Applica	tion Filters Clear A	All Filters 💢	Available Applica	tions (759) 🗳			Selec	ted Applications	and Filters (1) 🧏 🖆 🔘
Image: Second Arr 19 Image: Second Arr 19 Image: Second Arr 19 Image: Second Arr 10	🔍 Sea	rch by name		🔍 Search by nam	ne			Filte	rs		
Save Cancel		 Solution and the sector of the	19 53 7 44 01 1 25 28 21 759 2 280 58 27 23 7 249 39 11	ClickTale ClickTale Clip2Net Clip2Net Uploa CloudFlare CNBC CNET CNET CNET TV CNTV CNTV CNTV CNTZ Cognitive Mato CollegeHumor Collider CollegeHumor Collider Comcast Comedy Centr	ad ch ral unction ewing 101-200 of 759		Add to Ru	le	ags: displays ads		
										Save	Cancel

向TAC提供的数据

数据	

说明

从Firepower设备检查流量的文件故障排除 http://www.cisco.com/c/en/us/support/docs/security/sourcefire-系统支持firewall-engine-debug和system-有关说明,请参阅本文 support-trace输出

访问控制策略导出

导航至**系统>工具>导入/导**出,选择访问控制策略,然后单击导

警告:如果ACP包含SSL策略,请在导出之前从ACP中删除SSL策略,以避免泄露敏感PKI信 息

下一步:排除SSL策略层故障

如果SSL策略正在使用,而访问控制策略故障排除未显示问题,则下一步是排除SSL策略故障。