在Firepower模块中配置入侵策略和签名配置(机 上管理)

目录

简介 <u>先决条件</u> 要求 使用的组件 背景信息 配置 步骤1.配置入侵策略 步骤1.1.创建入侵策略 步骤1.2.修改入侵策略 步骤1.3.修改基本策略 步骤1.4.使用过滤条选项进行签名过滤 步骤1.5.配置规则状态 步骤1.6.事件过滤器配置 步骤1.7.配置动态状态 步骤2.配置网络分析策略(NAP)和变量集(可选) 步骤 3: 配置访问控制以包括入侵策略/NAP/变量集 步骤4.部署访问控制策略 步骤5.监控入侵事件 验证 故障排除 相关信息

简介

本文档介绍FirePOWER模块的入侵防御系统(IPS)/入侵检测系统(IDS)功能以及在FirePOWER模块 中制定检测策略的各种入侵策略元素。

先决条件

要求

Cisco 建议您了解以下主题:

*了解自适应安全设备(ASA)防火墙、自适应安全设备管理器(ASDM)。

* FirePOWER设备知识。

使用的组件

本文档中的信息基于以下软件和硬件版本:

运行软件版本5.4.1及更高版本的ASA FirePOWER模块(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)。

运行软件版本6.0.0及更高版本的ASA FirePOWER模块(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

FirePOWER IDS/IPS旨在检查网络流量并识别任何表示网络/系统攻击的恶意模式(或签名)。如 果ASA的服务策略在监控模式(混杂)下特别配置,则FirePOWER模块在IDS模式下工作,而在内 联模式下工作。

FirePOWER IPS/IDS是一种基于签名的检测方法。IDS模式下的FirePOWER模块在签名与恶意流量 匹配时生成警报,而IPS模式下的FirePOWER模块生成警报并阻止恶意流量。

: FirePOWERConfiguration > ASA FirePOWER Configuration > License

配置

步骤1.配置入侵策略

步骤1.1.创建入侵策略

要配置入侵策略,请登录到自适应安全设备管理器(ASDM)并完成以下步骤:

步骤1.导航至Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy。

步骤2.单击"创**建策略"**。

步骤3.输入入侵策略的名称。

步骤4.输入入侵策**略**的说明(可选)。

步骤5.指定Drop when Inline(内联时丢弃)选项。

步骤6.从下拉列**表中选**择基本策略。

步骤7.单击"创建策略"以完成入侵策略的创建。

:Drop when InlineInline

<u>File View Tools Wizards Window H</u> elp		Type topic to search	Go ululu
🔥 Home 🦓 Configuration 🔯 Monitoring 🔚 Save ASA Change	es 🔇 Refresh 🔇 Back 🔘 Forward 🢡 He	lp	CISCO
ASA FirePOWER Configuration 🗗 竹 Configuration	on > ASA FirePOWER Configuration > Policie	<u>s > Intrusion Policy</u> > <u>Intrusion Policy</u>	
Policies Access Control Policy Thrusion Policy Rule Editor Files SSL	no policies defined. Click Create Policy to create a pol	icy	Create Policy
	Create Intrusion Policy	?	×
VNS Policy Device Management	Policy Information		
Object Management Local	Name * 3 IPS_Policy		
System Information	Description	or LAB	
Licenses	Drop when Inline 5		
	Base Policy 6 Balanced Se	ecurity and Connectivity	
Device Setup	* Required	Create Policy Create and Edit Policy Cance	
Firewall			
Remote Access VPN			
Site-to-Site VPN			
ASA FirePOWER Configuration			
Device Management			
» *			
	<admin> 15</admin>	😡 🛃 🔢 📔 🔒	/4/16 1:17:37 AM UTC

您可以注意到策略已配置,但是,它未应用于任何设备。

figuration > ASA	A FirePOWER Config	uration > Policies > Intrusion Policy :	> Intrusion Policy				
Create Policies Create Policy							
Intrusion Policy	Drop when Inline	Status	Last Modified				
IPS_Policy IPS_policy for LAB	Yes	No access control policies use this policy Policy not applied on device	2016-01-04 07:40:00 Modified by "admin"	🕒 🕞 🥒 🖯			

步骤1.2.修改入侵策略

要修改入侵策略,请导航至Configuration>ASA FirePOWER Configuration>Policies>Intrusion Policy>Intrusion Policy**,然**后选择Edit选项。

File View Tools Wizards Window Help			Type topic to	search	G0
Home 🍓 Configuration 🔯 Monitoring 🗐 Deplo	oy 👻 💽 Refresh 🄇	Back 🔘 Forward	🦓 Help		CISCO
ASA FirePOWER Configuration	Configuration > ASA	A FirePOWER Configu	ration > Policies > Intrusion	Policy > Intrusion Poli	cy 🗆
Policies				Compare Policies	Create Policy
	Intrusion Policy	Drop when Inline	Status	Last Modified	
Files SSL SSL Variable SSL SSL Variable SSL SSL Solution Solution System Information Vpdates Licenses Tools Market SSL Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Sol	IPS_Policy IPS_policy for LAB	Yes	<u>Used by 1 access control policy</u> Policy up-to-date on device	2016-01-04 07:40:00 Modified by "admin"	2

步骤1.3.修改基本策略

"入侵策略管理"(Intrusion Policy Management)页面提供了更改"内联时基本策略/丢弃"(Base Policy/Drop when Inline/ Save and Discard)选项的选项。

基本策略包含一些系统提供的策略,这些策略是内置策略。

- 平衡的安全性和连接性:在安全性和连接性方面,这是最佳策略。此策略启用了约7500个规则,其中一些仅生成事件,而其他则生成事件并丢弃流量。
- 2. 安全性高于连接:如果您的首选项是安全性,则可以选择安全性高于连接策略,这会增加启用 的规则数。
- 3. 安全连接:如果您的首选项是连接而非安全,则可以选择连接而非安全策略,这将减少已启用 规则的数量。
- 4. Maximum Detection 选择此策略以获取最大检测。
- 5. No Rule Active 此选项禁用所有规则。您需要根据安全策略手动启用规则。

Policy Information 🖄	Policy Information	< Back				
Rules ⊕ Advanced Settings	Name IPS_Policy Description IPS_policy_for_LAB					
⊕ Policy Layers	Drop when Inline Base Policy Manage Ba					
	Balanced Security and Connectivity The base policy is up to date (Rule Update 20 This policy has 7501 epobled rules	115-10-01-001-vrt)				
	 ⇒ 114 rules generate events X 7477 rules drop and generate events 	View View				
	This policy contains enabled preprocessor rules. Plea the preprocessors have the correct settings for thes	ase read the rule documentation to ensure se rules				
	Commit Changes Di	iscard Changes				

步骤1.4.使用过滤条选项进行签名过滤

导航面板**中的**"规则"选项,系统将显示"规则管理"页。规则数据库中有数千个规则。筛选条提供了一个很好的搜索引擎选项,可有效搜索规则。

您可以将任何关键字插入到过滤器栏,然后系统为您获取结果。如果需要查找安全套接字层 (SSL)heartbleed漏洞的签名,可以在过滤条中搜索关键字heartbleed,它将获取heartbleed漏洞的 签名。

提示:如果在筛选条中使用了多个关键字,则系统会使用AND逻辑将它们组合在一起以创建 复合搜索。

您还可以使用签名ID(SID)、生成器ID(GID)、类别(Category)搜索规则:DOS等

规则有效地分为多种方式,例如基于类别/分类/ Microsoft漏洞/ Microsoft蠕虫/平台特定。这种规则 关联有助于客户轻松获得正确的签名,并帮助客户有效调整签名。

Policy Information	Rules					< B	Jack
Rules	Rule Configuration	Filter: heartbleed				ж	?
⊕ Advanced Settings	Rule Content						
Policy Lavers	Category	⇒ , , , , , , , , , , , , , , , , , , ,	Delieu				
E Policy Layers	app-detect	Rule State Event Filtering Dynamic State Alerting Comments	Policy				-
	blacklist	GID SID Message	=	7	•		
	browser-chrome browser-firefox	1 30549 SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt	×				
	browser-ie	1 30777 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×				
	browser-plugins	1 30778 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×				
	browser-webkit content-replace	1 30785 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×				
	decoder	1 30514 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×				
	file-executable	1 30779 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×				
	file-flash Classifications	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×				
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response	×				
	Microsoft Worms	- possible ssl heartbleed attempt	^				
	Platform Specific	1 30515 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×				
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	×				
	Rule Update	к	<	1	of 1	> >	1

您还可以使用CVE编号搜索以查找涵盖这些规则的规则。您可以使用语法CVE:<cve-number>。

Policy Information 🛆	Rules		< Back
Rules	Rule Configuration	Filter: CVE:"2013-2135"	× ?
⊕ Advanced Settings	Rule Content	Filter returned 2 results	
⊕ Policy Layers	Message A SID	⇒ ▼ ▼ ▼	Policy •
	GID Reference	GID SID Message ▲	
	CVE ID	1 27575 SERVER-APACHE Apache Struts arbitrary OGNL remote code execution attempt	×
	URL Bustrag ID	1 27574 SERVER-APACHE Apache Struts OGNL getRuntime.exec static method access attempt	×
	Nessus ID		
	Arachnids ID		
	Mcafee ID		
	Action		
	Protocol		
	Direction		
	Source IP 🔹		
	Category		
	Classifications		
	Microsoft Vulnerabilities		
	Microsoft Worms		
	Platform Specific		
	Preprocessors		
	Priority		
	Rule Update	K	< 1 of 1 > >

步骤1.5.配置规则状态

导航至 **规则** 选项。。选择规则,然后选择选**项Rule State**以配置规则的状态。可以为规则配置三种 状态:

1.生成事件:此选项在规则与流量匹配时生成事件。

2.丢弃**并生成事件:当**规则匹配流量时,此选项会生成事件并丢弃流量。

3.禁用:此选项禁用规则。

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter:	x ?
⊕ Advanced Settings	Rule Content	Filter returned 33 results	
 Advanced Settings Policy Layers 	Rule Content Category app-detect blacklist browser-chrome browser-firefox browser-ie browser-other browser-plugins browser-webkit content-replace decoder exploit-kit file-flash Classifications	Filter returned 33 results Filter returned 33 results Filter returned 33 results Rule State Events Filtering Dynamic State Alerting Comments Generate Events Sige A Drop and Generate Events ER-OTHER OpenSSL Heartbleed masscan access itation attempt Disable ER-OTHER OpenSSL SSLv3 large heartbeat response 1 30777 - possible ssl heartbleed attempt 1 30778 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt 1 30778 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt 1 30514 SERVER-OTHER OpenSSL TSV3 large heartbeat response - possible ssl heartbleed attempt 1 30779 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt 1 30779 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt 1 30779 SERVER-OTHER OpenSSL TLS	Policy ▼ ⇒ ▼ ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ × ≥ ×
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response	· •
	Microsoft Worms	- possible ssl heartbleed attempt	<u>^</u>
	Platform Specific	1 30515 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	¥ -
	Rule Update	le	< 1 of 1 > >

步骤1.6.事件过滤器配置

入侵事件的重要性可以基于发生频率或源或目标IP地址。在某些情况下,在事件发生一定次数之前 ,您可能不关心该事件。例如,在某人尝试登录到某台服务器,直到其失败一定次数后,您才可能 担心。在其他情况下,您可能只需要看到几次规则命中,以检查是否存在普遍问题。

有两种方法可以实现此目标:

1.事件阈值。

2.事件抑制。

事件阈值

您可以根据事件发生次数设置指示事件显示频率的阈值。您可以根据事件和策略配置阈值。

配置事件阈值的步骤:

步骤1.选择要为其配置事件阈值的规则。

步骤2.单击Event Filtering(事件过滤)。

步骤3.单击Threshold。

步骤4.从下拉列表中选择Type。(限制或阈值或两者)。

步骤5.从"跟踪依据"下拉框中选**择跟踪**方式。(源或目标)。

步骤6.输入Count of events 以达到阈值。

步骤7.输入计数重置**前**经过的秒数。

步骤8.单击OK完成。

]	GID	SIL T	nreshold 3		\Rightarrow		0	0	5
3	1	280 SI	uppression	T 360.cn SafeGuard local HTTP managem ess attempt	nent 🗙				
)	1	280 Re	emove Thresholds	360.cn Safeguard runtime outbound commu	nication 🛛 🔿				
0	1	328 Re	emove Suppressions 209.53.113	Absolute Software Computrace outbound con 223	inection - 🛶				
9	1	32846	APP-DETEC absolute.co	Absolute Software Computrace outbound con	inection - 🔿				
)	1	32847	, APP-DETEC bh.namequ	Absolute Softwa Set Threshold for 1 r	rule	?	×		
0	1	32848	APP-DETEC namequery.	Absolute Softwa Type Limi	it 🔻				
9	1	26286	APP-DETEC search.dns	Absolute Softwa Count 10					
9	1	26287	, APP-DETEC search.nam	Absolute Softwa Seconds 60					

在将事件过滤器添加到规则后,您应该能够看到规则指示旁边的过滤器图标,该图标显示为此规则 启用了事件过滤。

事件抑制

可以根据源/目标IP地址或每条规则抑制指定的事件通知。

注意:为规则添加事件抑制时。签名检查工作正常,但如果流量与签名匹配,系统不会生成事件。 如果指定特定源/目标,则事件不仅会针对此规则的特定源/目标显示。如果选择抑制完整规则,则系 统不会为此规则生成任何事件。

配置事件阈值的步骤:

步骤1.选择要为其配置事件阈值的规则。

步骤2.单击"事件过滤"。

步骤3.单击"抑制"。

步骤4.从下拉**列表中选择**Suppression Type。(规则或源或目标)。

步骤5.单击OK完成。

⇒ ▼ 2 ▼ ▼ Rule State Event Filte	ering Dynamic Sta	ote Alerting C	⊃ ▼ Tomments	F	olicy			•
🧾 GID SID Threshol	d				⇒ 🐬	۰ 🕕	9	
1 Suppress	sion T 36	i0.cn SafeGua attempt	ard local HTTP ma	anagement	K			
1 280 Remove	Thresholds 360 Suppressions on	.cn Safeguard	runtime outbound	-	⇒			
1 32845	APP-DETECT Abs connection - 209	olute Software .53.113.223	Computrace outbo	und	⇒			
1 32846	APP-DETECT Abs connection - abs	olute Software olute.com	Computrace outbo	und	⇒			
Add Suppression Suppression Type 5	n for 1 rule 7 Rule OK Cance Connection - sear APP-DETECT Abs connection - sear	software uery.cor Software y.nettra Software ssearch. Software ch.namequery olute Software rch.us.nameque	Add Suppression Type Network Add Suppression Type Suppression Type Network	sion for 1 ru 4 Source 5 sion for 1 ru 4 Destinati	le ок Jle ок	? × Cancel ? > Cancel	:	

将事件过滤器添加到此规则后,您应该能够看到一个过滤器图标,其中计数为2,该图标位于规则指 示旁边,显示为此规则启用了两个事件过滤器。

步骤1.7.配置动态状态

它是一种功能,如果指定的条件匹配,我们可以在其中更改规则的状态。

假设暴力攻击破解密码。如果签名检测到密码失败尝试,规则操作是生成事件。系统继续生成密码 失败尝试的警报。对于这种情况,您可以使用**动态**状态,其中**生成事**件的操作可更**改为丢弃并生成** 事件以阻止暴力攻击。

导航至 **规则** 选项。选择要为其启用动态状态的规则,然后选择选项**动态状态>添加基于速率的规则** 状态。

要配置基于速率的规则状态,请执行以下操作:

- 1. 选择要为其配置事件阈值的规则。
- 2. 单击"Dynamic State(动态状态)"。
- 3. 单击Add Rate-Based Rule State。
- 4. 从跟踪依据(Track By)下拉框中选择要如何跟踪规则状态。(规则或源或目标)。
- 5. 输入Network。可以指定单个IP地址、地址块、变量或逗号分隔列表,该列表由这些地址的任

意组合组成。

- 6. 输入Count of events和时间戳(以秒为单位)。
- 7. 选择**要为规**则定义的新状态。
- 8. 输入Timeout,在此之后恢复规则状态。
- 9. 单击 OK 完成操作。



步骤2.配置网络分析策略(NAP)和变量集(可选)

配置网络分析策略

网络访问策略也称为预处理器。预处理器执行数据包重组并规范化流量。它有助于识别网络层和传 输层协议异常,以识别不适当的报头选项。

NAP对IP数据报进行分片重组,提供TCP状态检查和数据流重组以及校验和验证。预处理器将对流 量进行规范化,验证和验证协议标准。

每个预处理器都有自己的GID编号。它表示数据包已触发的预处理器。

要配置网络分析策略,请导航至Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy > Advanced > Network Analysis and Intrusion Policy

默认网络分析策略为平衡安全和连接,这是最佳推荐策略。还有另外三个系统提供的NAP策略可以 从下拉列表中选择。

选择选项Network Analysis Policy List以创建自定义NAP策略。

Configuration > ASA Fire	POWER Configuration > Policies > Access	s Control Policy			
ASA ASA FirePO	WER				
Default Allow A custom policy	II Traffic		M Istatus: Policy Up-to-date on device		
Identity Policy: None	SSL Policy: None				
Rules Security Intellig	Network Analysis and Intrusion Pol	icies	? ×		
General Settings Maximum URL characters	Intrusion Policy used before Access Control rule is determined	No Rules Active	v	No	Î
Allow an Interactive Bloc	Intrusion Policy Variable Set	Default-Set	▼ Ø	A	
Retry URL cache miss loo	Network Analysis Rules	No Custom Rules	Network Analysis Policy List	Disabled	
Inspect traffic during pol	Default Network Analysis Policy	Balanced Security	and Connectivity	A	
Identity Policy Settine	Revert to Defaults		OK Cancel Ivze Per		
Identity Policy		None		2	
SSL Policy Settings		Ø	Performance Statistics - Sample Time (seconds)	300	
SSL Policy to use for insp	ecting encrypted connections	None	Regular Expression - Limit	Default	
Network Analysis and	Intrusion Policies	Ø	Regular Expression - Recursion Limit	Default	
		Store ASA FirePOW	ER Changes Cancel	8	•

配置变量集

变量集用于入侵规则中,用于标识源地址、目标地址和端口。当变量更准确地反映网络环境时,规则更有效。变量在性能调整中起着重要作用。

变量集已配置了默认选项(网络/端口)。 如果要更改默认配置,请添加新的变量集。

要配置变量集,请导航至Configuration > ASA Firepower Configuration > Object Management > Variable Set。选择"添**加变量集"**选项以添加新的变量集。输入变量**集**的名称并指定说**明。**

如果任何自定义应用程序在特定端口上工作,则在"端口号"字段中定义端口号。配置network参数。

\$Home_NET指定内部网络。

\$External_NET指定外部网络。

ASA FirePOWER Configuration	Configuration >	ASA FirePOWER	Configurati	ion > Obje	ect Management > <u>Variable Set</u>		
Policies Device Management Object Management Management					O Add Variable Set	Rilter	
Port	Name				Description		
Application Filters	Default-Set				This Variable Set is system-provided.		Ø 8
	New Varia	ble Set				? >	
Variable Set	Name:	Custom_Variable_	Set				
	Description:	Enter a descriptio	n				
						💽 Add	
🕀 🚰 Distinguished Name	Variable I	Name	Туре	Value			
Local	Customize	ed Variables	÷.	24			
Updates	This categ	ory is empty					
Elicenses	Default V	ariables					
🗄 🖗 Integration	AIM_SERVE	ERS	Network	[64.12.]	31.136/32, 205.188.210.203/32, 6]	Ø98	
	DNS_SERV	ERS	Network	HOME_N	NET	/>s	
	EXTERNAL	_NET	Network	any		228	
	FILE_DATA	_PORTS	Port	[HTTP_F	PORTS, 143, 110]	Ø78	
Device Setup	FTP_PORTS	5	Port	[21, 21)	00, 3535]	2 26	
🚯 Firewall	GTP_PORT	S	Port	[3386, 3	2123, 2152]	2 76	
Kemote Access VPN	HOME_NET	r i	Network	any		Ø28 _	> 0
Site-to-Site VPN	4					•	
ASA FirePOWER Configuration							
Device Management					Store ASA FirePOWER Change	s Cancel	

步骤 3: 配置访问控制以包含入侵策略/NAP/变量集

导航至Configuration > ASA Firepower Configuration > Policies > Access Control Policy。您需要完成以下步骤:

- 1. 编辑要分配入侵策略的访问策略规则。
- 2. 选择"检查"选项卡。
- 3. 从下拉列**表中选**择入侵策略,然后从下拉列**表中选**择变量集
- 4. Click Save.

Standard Rules											
1 Access_Policy_Rule	any	Allow	VDB0 🖉 🖯								
Root Rules											0

ame Ac	cess_Policy_R	ule			🗹 Er	abled	Move	
tion 🖌	Allow		v	IPS:	IPS_Policy	Variables: Default-Set	Files: no inspection Lo	gging: no logging
Zones	Networks	🔺 Users	Applications	Ports	🔺 URLs	🔺 ISE Attributes	2 🔺 Inspection	Logging Commer
rusion P	blicy	191 (d)				Variable	Set	
S_Policy						👻 🦉 🛛 Default	Set	
a Policy								
one								
0.0244								

因为入侵策略已添加到此访问策略规则。您可以在金色中看到指示已启用入侵策略的屏蔽图标。

									🖌 📃 Sta	tus: Access Con	trol policy out-	of-date on devic	e
Ide	ntity Policy: None		SSL Policy: N	one									
Ru	es Security In	telligence	HTTP Responses	Advanced									
								🕜 Add Ca	tegory 📀 A	dd Rule Search	n Rules		×
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat	Src Ports	Dest Ports	URLs	Action	Ç 🗋 🎒	
Adr	inistrator Rules	63			Се	5	2			20			10 A
Thi	category is empty												
Sta	ndard Rules												
1	Access_Policy_Rule	any	any	any	any	any	any	any	any	any	Allow	0 [] [] 🔍	0
Roo	Rules										/	1	
Thi	category is empty												
De	ault Action							Intrusion P	revention: Balar	iced Security and	d Connectivity	*	\$ 🔳
									Displaying	1 - 1 of 1 rules	s < < Page	e 1 of 1 >	> C
					Store	ASA FirePOW	ER Changes	Cancel					

单击Store ASA FirePOWER changes (存储ASA FirePOWER更改)以保存更改。

步骤4.部署访问控制策略

现在,您必须部署访问控制策略。在应用策略之前,您会在设备上看到访问控制策略过期的指示。 要将更改部署到传感器:

- 1. 单击Deploy。
- 2. 单击"Deploy FirePOWER Changes (部署FirePOWER更改)"。
- 3. 在弹出窗口中单击Deploy。



Deploy Policies Version:2016-01-05.0	9.09 VW	
System Policy: Default	3.03 API	
 Sensor Policy: firepower 		
D Access Control Policy: Default Allow All Traffic		
D Intrusion Policy: Balanced Security and Con	nectivity	
Intrusion Policy: IPS_Policy		
ONS Policy: Default DNS Policy		

: 5.4.xApply ASA FirePOWER ChangesASA FirePOWER

> ASA Firepower>

步骤5.监控入侵事件

要查看FirePOWER模块生成的入侵事件,请导航至 Monitoring > ASA FirePOWER Monitoring > Real Time Eventing。

Gaurav_Connection_Events × All ASA FirePOWER Events Connection Intrusion File Malware File Security Intel Filter Rule Action=Block * reason=Intrusion Block * Pause Refresh Rate 5 seconds 1/10/16 6:13:42 PM (IST) Receive Times Action Event Type Inline Result Reason 1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion Intrusion							
Filter Rule Action=Block * reason=Intrusion Block * Pause Refresh Rate 5 seconds 1/10/16 6:13:42 PM (IST) Receive Times Action Event Type Inline Result Reason 1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion	Gaurav_Connection_Events	All ASA FirePOWER Even	Connection	Intrusion	File	Malware File	Security Intelliger
Rule Action=Block * reason=Intrusion Block * Pause Refresh Rate 5 seconds 1/10/16 6:13:42 PM (IST) Receive Times Action Event Type Inline Result Reason 1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion	2r						
Pause Refresh Rate 5 seconds 1/10/16 6:13:42 PM (IST) Receive Times Action Event Type Inline Result Reason 1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion	le Action=Block * reason=I	ntrusion Block ×					
Pause Refresh Rate 5 seconds 1/10/16 6:13:42 PM (IST) Receive Times Action Event Type Inline Result Reason 1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion							
Pause Refresh Rate 5 seconds 1/10/16 6:13:42 PM (IST) Receive Times Action Event Type Inline Result Reason 1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion							
Receive Times Action Event Type Inline Result Reason 1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion							
1/10/16 6:11:50 PM Block ASA FirePOWER Connection Intrusion	Pause Refresh Rate	5 seconds	1/10/16 6:13	:42 PM (IST)			
	Pause Refresh Rate	S seconds	1/10/16 6:13	:42 PM (IST)	Inl	line Result	Reason
1/10/16 6:09:52 PM Block ASA FirePOWER Connection Intrusion	Pause Refresh Rate eceive Times /10/16 6:11:50 PM	E 5 seconds C C C C C C C C C C C C C C C C C C C	1/10/16 6:13 Tent Type	:42 PM (IST)	In	line Result	Reason Intrusion Bloc
	Pause Refresh Rate eceive Times /10/16 6:11:50 PM /10/16 6:09:52 PM	S seconds Action Block Action	1/10/16 6:13 ent Type GA FirePOWER Co GA FirePOWER Co	:42 PM (IST) onnection	In	line Result	Reason Intrusion Bloc

当前没有可用于此配置的验证过程。

故障排除

步骤1.确保正确配置了规则状态。

步骤2.确保访问规则中包含正确的IPS策略。

步骤3.确保正确配置了变量集。如果变量集配置不正确,则签名将与流量不匹配。

步骤4.确保访问控制策略部署成功完成。

步骤5.监控连接事件和入侵事件,以验证流量是否达到正确的规则。

Cisco ASA FirePOWER

- Cisco Systems