在Firepower模块中配置入侵策略和签名配置（机上管理）

目录

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。

: FirePOWER**Configuration > 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。

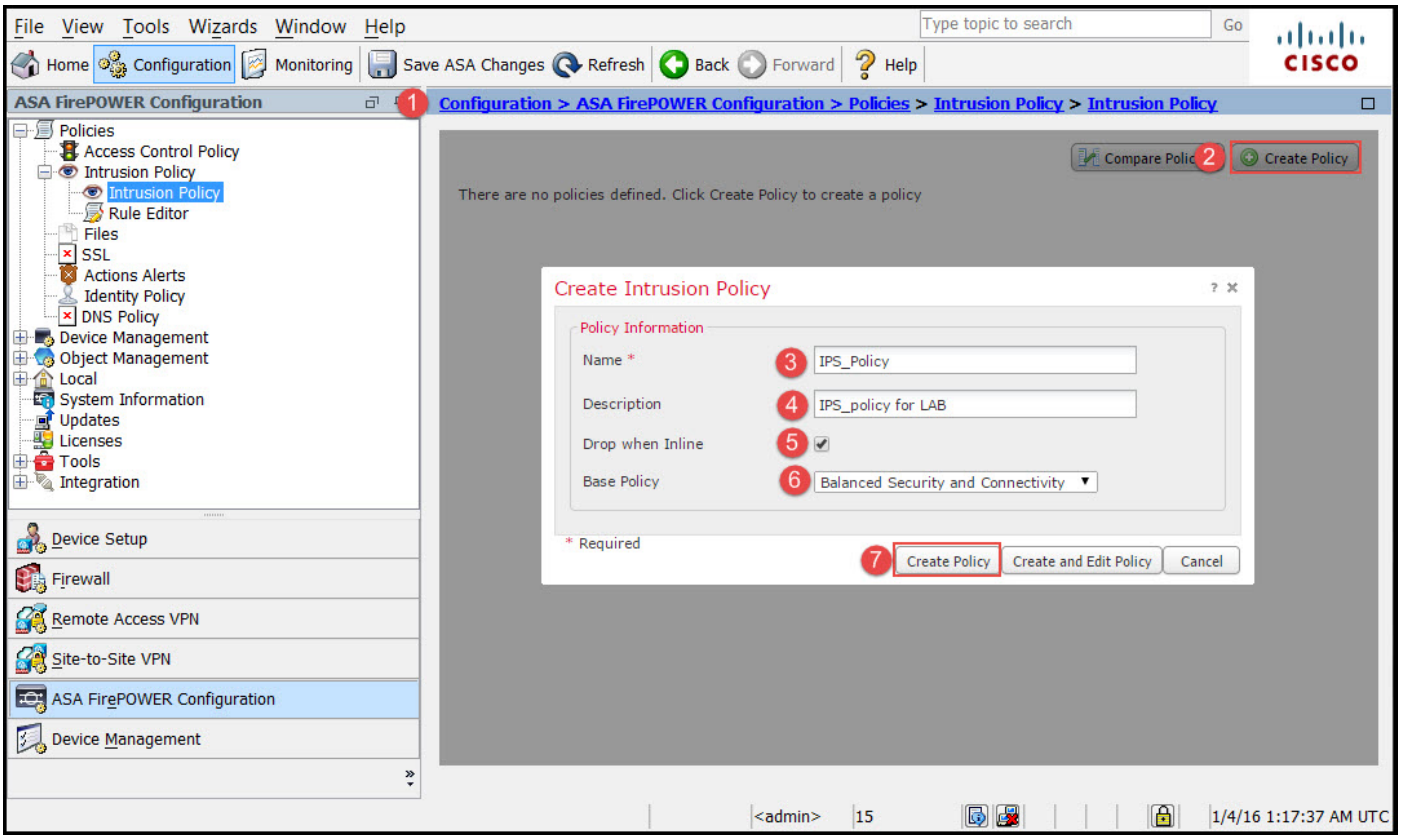
步骤4.输入入侵策**略**的说明（可选）。

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



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

There are no policies defined. Click Create Policy to create a policy

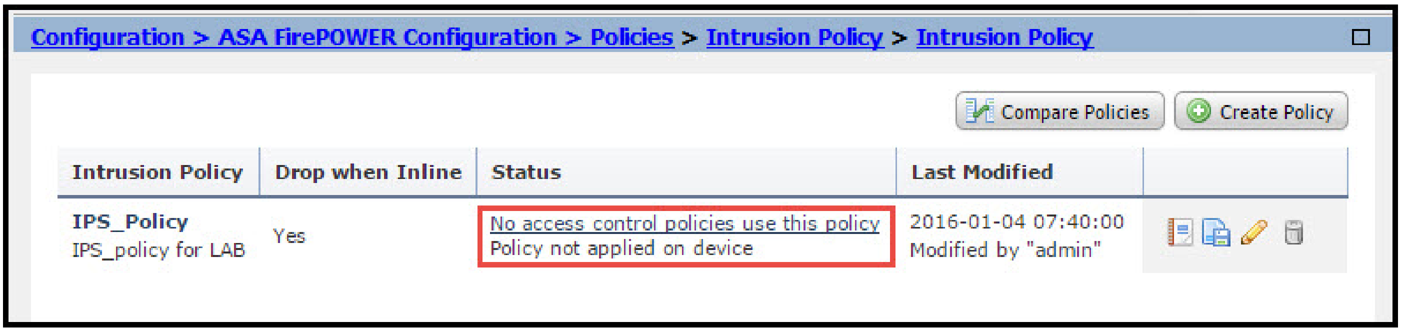
Create Intrusion Policy

Policy Information

Name *	IPS_Policy
Description	IPS_policy for LAB
Drop when Inline	☑
Base Policy	Balanced Security and Connectivity

* Required

您可以注意到策略已配置，但是，它未应用于任何设备。

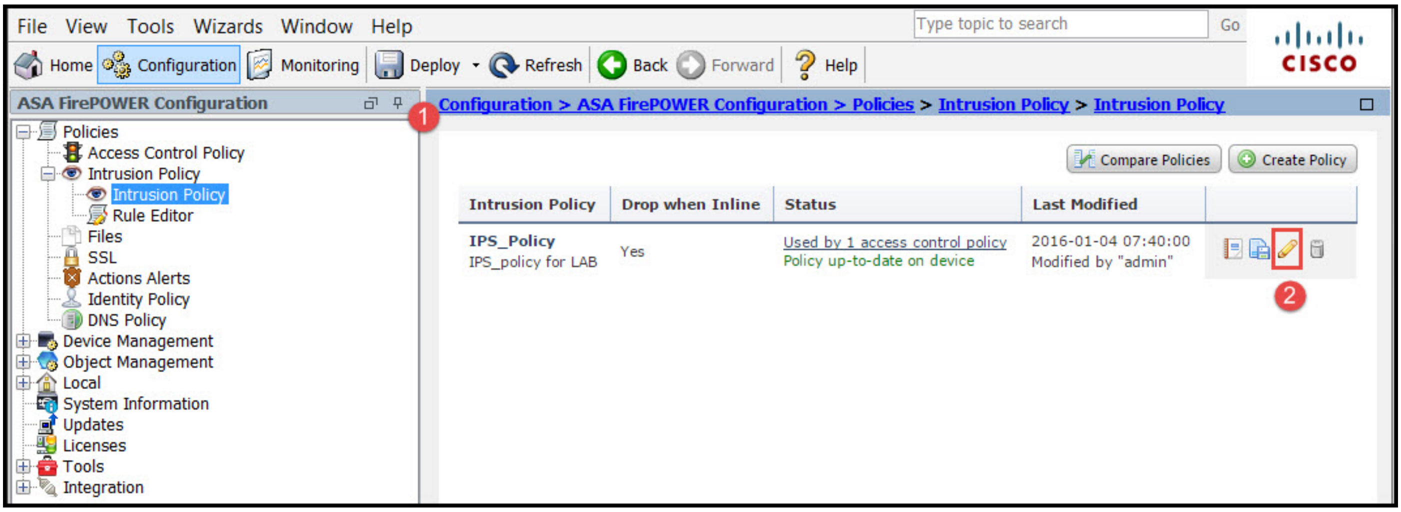


Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

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。



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

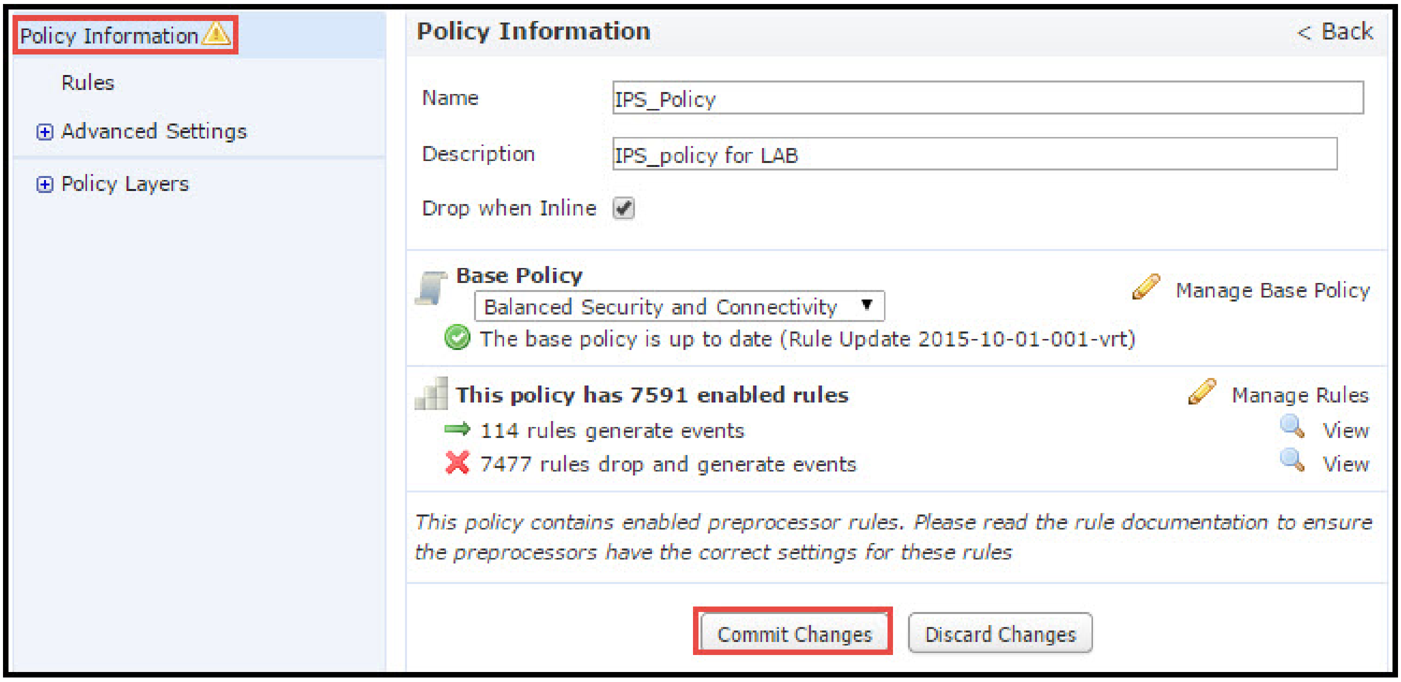
Intrusion Policy	Drop when Inline	Status	Last Modified	
IPS_Policy IPS_policy for LAB	Yes	Used by 1 access control policy Policy up-to-date on device	2016-01-04 07:40:00 Modified by "admin"	

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。

1. 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

Name: IPS_Policy

Description: IPS_policy for LAB

Drop when Inline ☑

Base Policy: Balanced Security and Connectivity

The base policy is up to date (Rule Update 2015-10-01-001-vrt)

This policy has 7591 enabled rules

114 rules generate events

7477 rules drop and generate events

This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules

步骤1.4.使用过滤条选项进行签名过滤

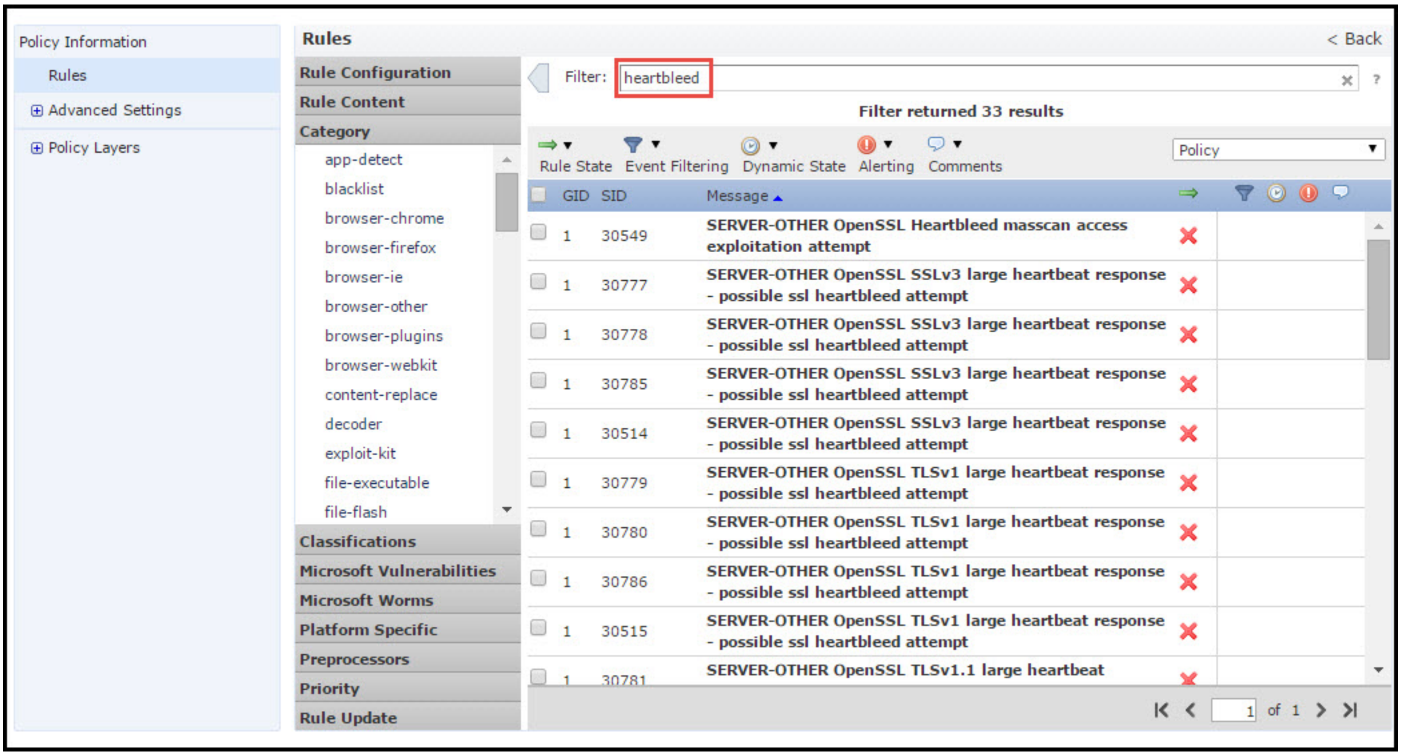
导航面板**中的**“规则”选项，系统将显示“规则管理”页。规则数据库中有数千个规则。筛选条提供了一个很好的搜索引擎选项，可有效搜索规则。

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。

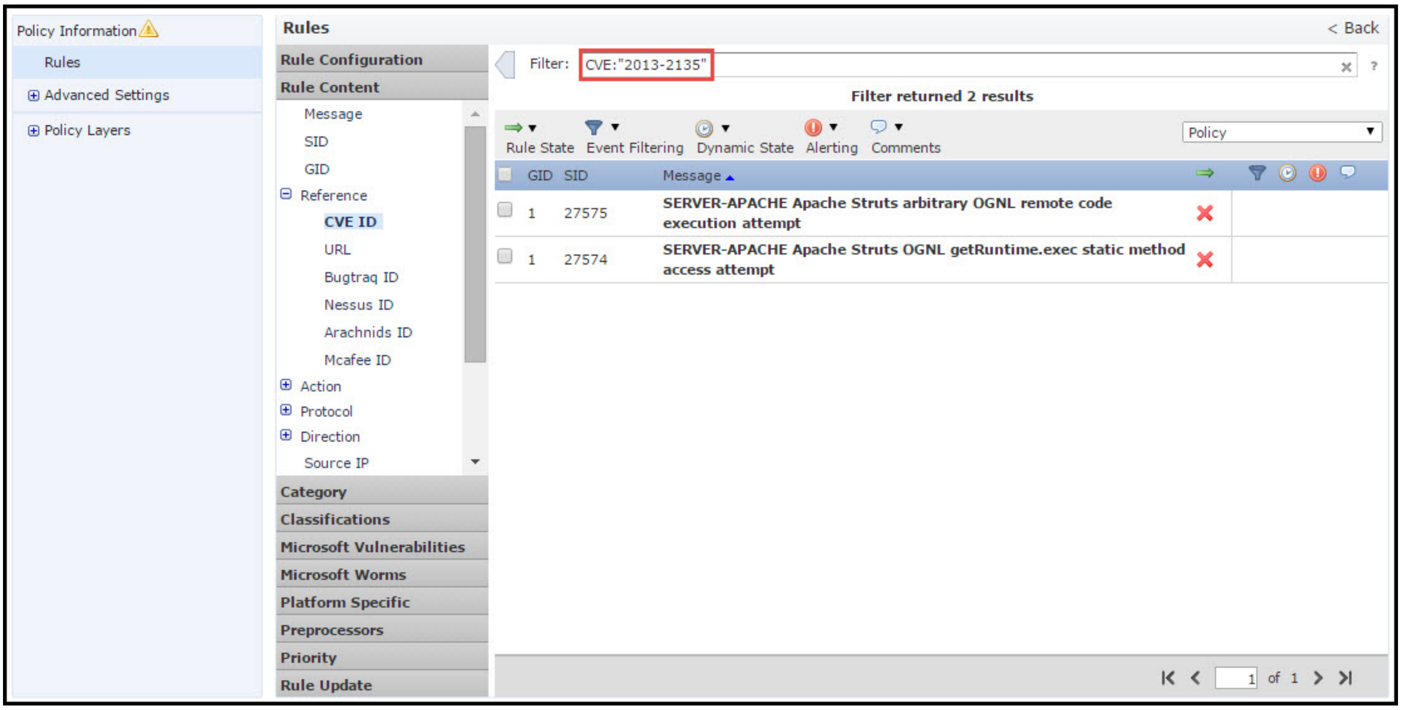


Filter: heartbleed

Filter returned 33 results

GID	SID	Message	
1	30549	SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt	✗
1	30777	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	30785	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	✗
1	30514	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	✗
1	30779	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	✗
1	30780	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	✗
1	30786	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	✗
1	30515	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	✗
1	30781	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	✗

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>**。



Filter: CVE:"2013-2135"

Filter returned 2 results

GID	SID	Message	
1	27575	SERVER-APACHE Apache Struts arbitrary OGNL remote code execution attempt	✗
1	27574	SERVER-APACHE Apache Struts OGNL getRuntime.exec static method access attempt	✗

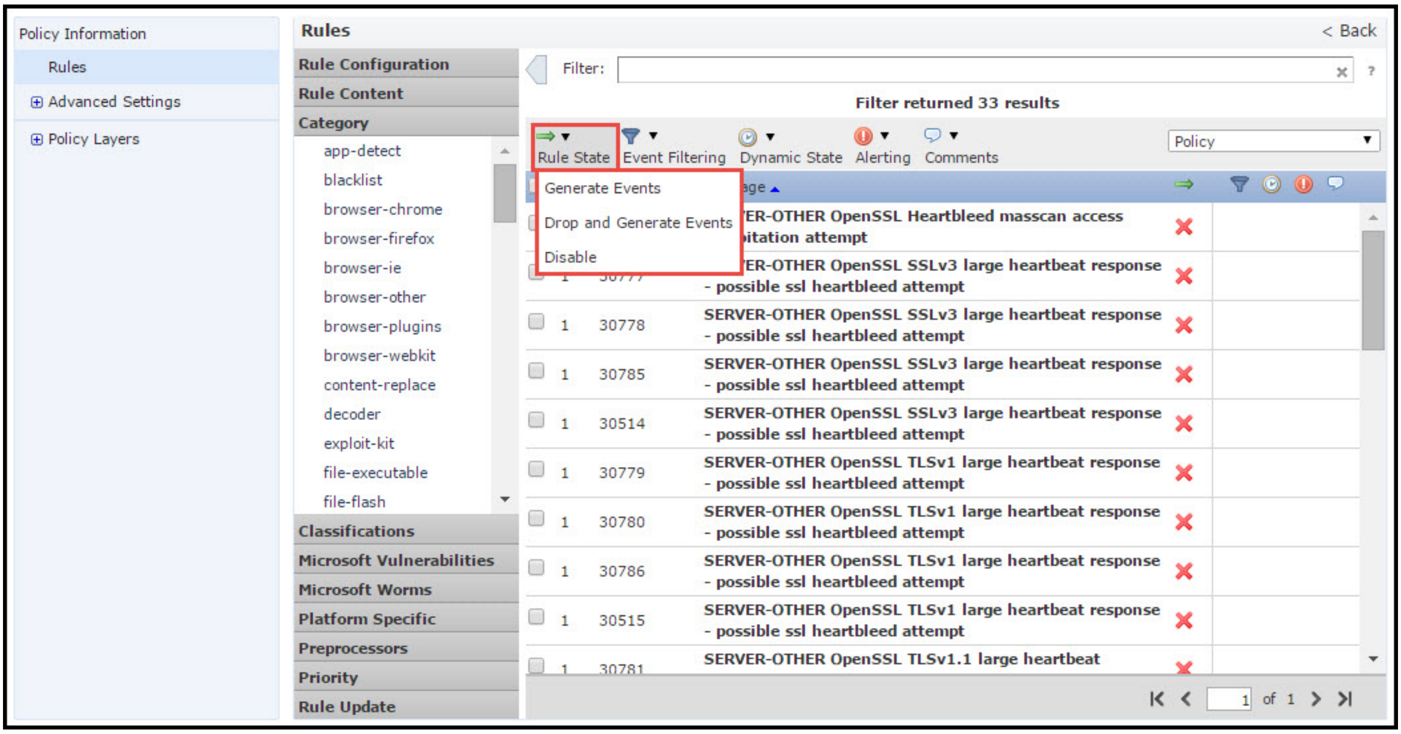
步骤1.5.配置规则状态

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。



			Message ▲
□			...ER-OTHER OpenSSL Heartbleed masscan access ...itation attempt
□	1	30777	...ER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
□	1	30778	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
□	1	30785	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
□	1	30514	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
□	1	30779	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
□	1	30780	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
□	1	30786	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
□	1	30515	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
□	1	30781	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat

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**。

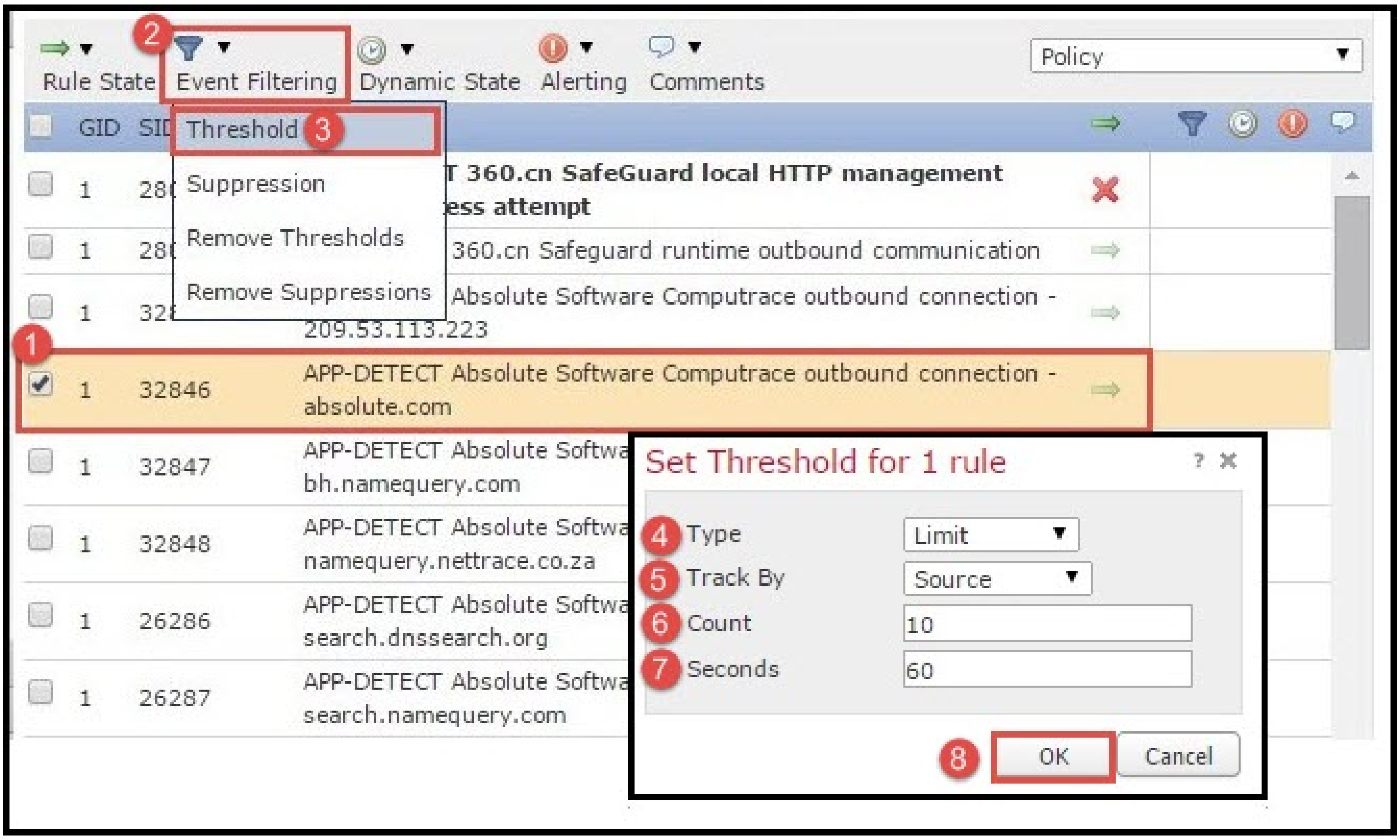
步骤4.从下拉列**表中**选择Type。（限制或阈值或两者）。

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	SID	
□	1	28	T 360.cn SafeGuard local HTTP management ess attempt
□	1	28	360.cn Safeguard runtime outbound communication
□	1	32	Absolute Software Computrace outbound connection - 209.53.113.223
☑	1	32846	APP-DETECT Absolute Software Computrace outbound connection - absolute.com
□	1	32847	APP-DETECT Absolute Softwa bh.namequery.com
□	1	32848	APP-DETECT Absolute Softwa namequery.nettrace.co.za
□	1	26286	APP-DETECT Absolute Softwa search.dnssearch.org
□	1	26287	APP-DETECT Absolute Softwa search.namequery.com

Set Threshold for 1 rule

Type: Limit
Track By: Source
Count: 10
Seconds: 60

OK　Cancel

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：

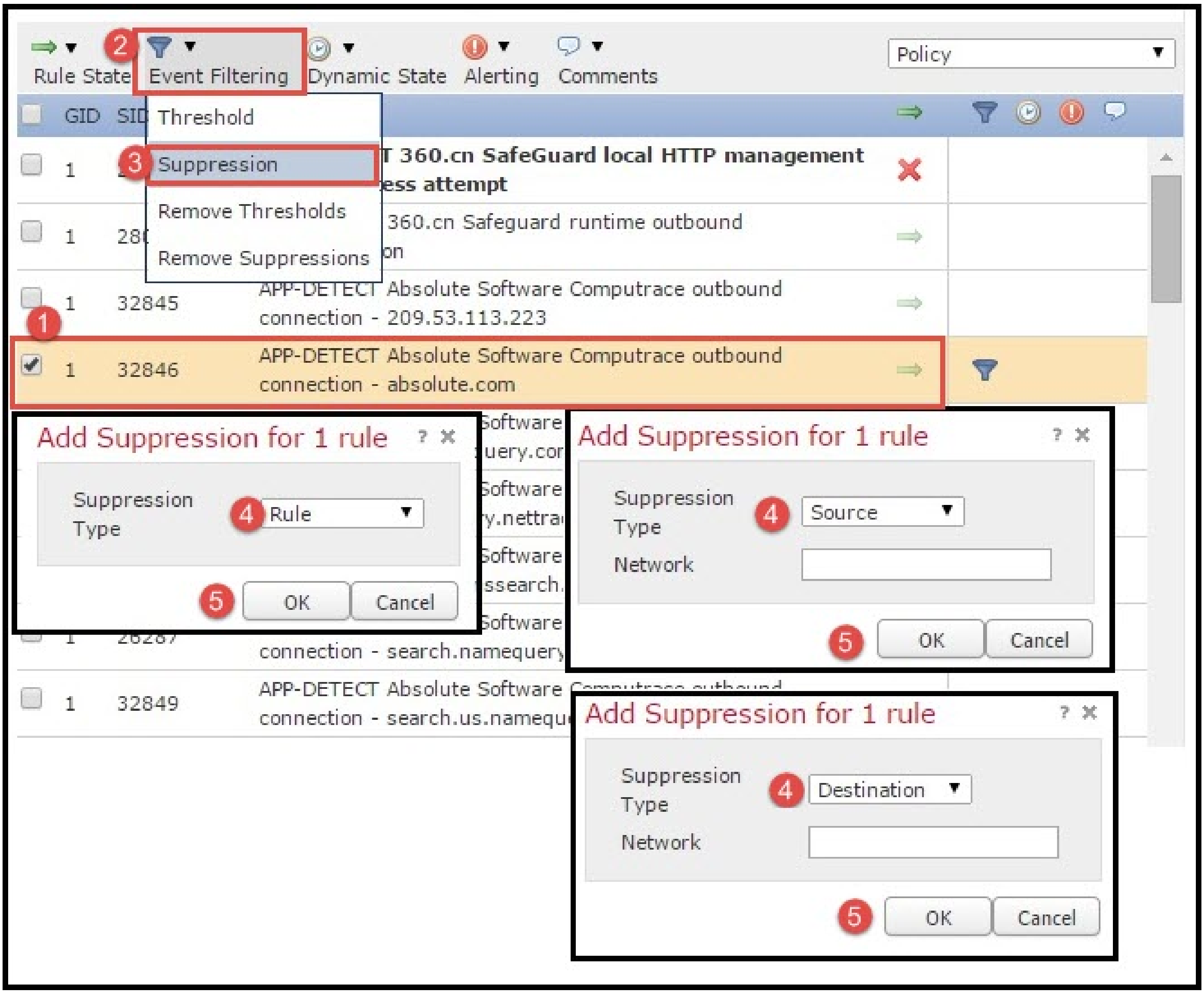
步骤1.选择**要为其配**置事件阈值的规则。

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。



GID	SID	Message
1	2	T 360.cn SafeGuard local HTTP management ess attempt
1	28	360.cn Safeguard runtime outbound on
1	32845	APP-DETECT Absolute Software Computrace outbound connection - 209.53.113.223
1	32846	APP-DETECT Absolute Software Computrace outbound connection - absolute.com
1	26287	connection - search.namequery
1	32849	APP-DETECT Absolute Software Computrace outbound connection - search.us.namequ

Add Suppression for 1 rule

Suppression Type: Rule

Add Suppression for 1 rule

Suppression Type: Source

Network:

Add Suppression for 1 rule

Suppression Type: Destination

Network:

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。

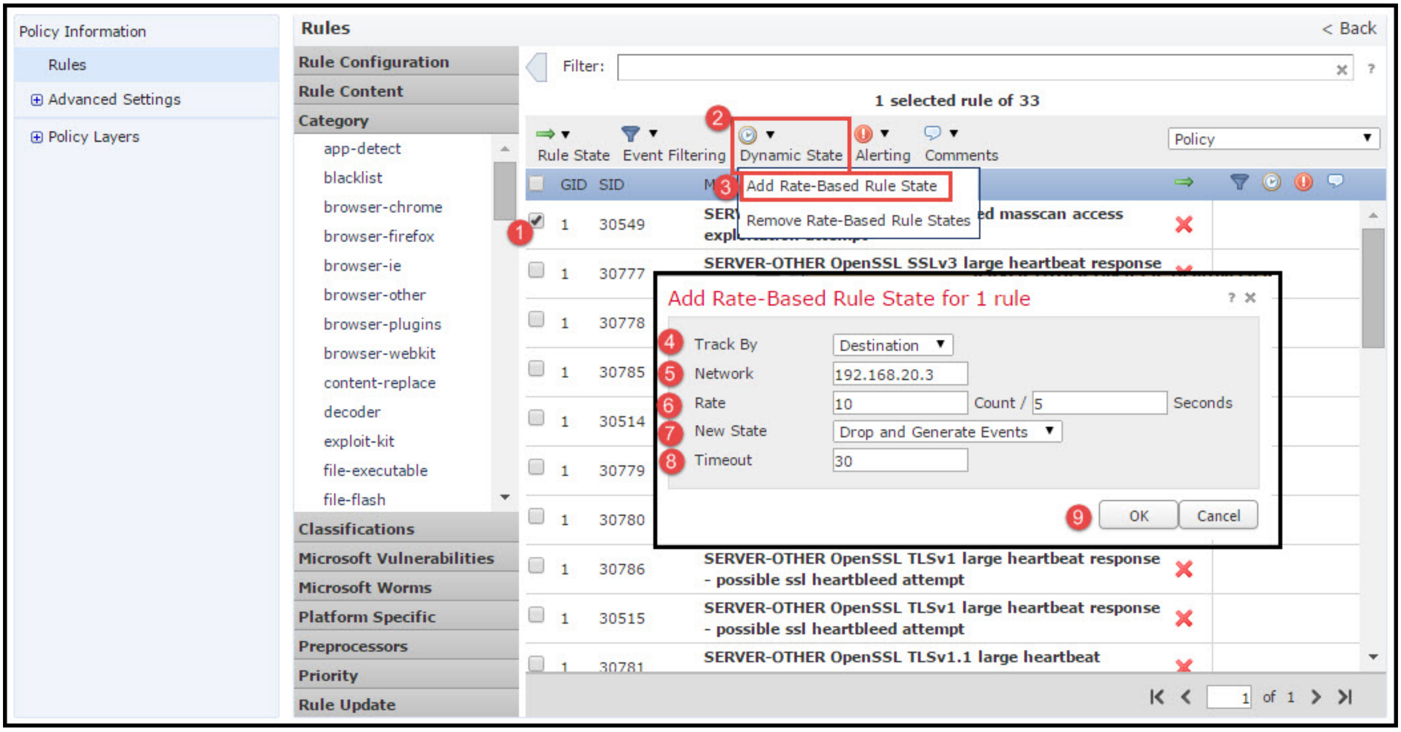
导航至 **规则** 选项。选择要为其启用动态状态的规则，然后选择选项**动态状态>添加基于速率的规则状态。**

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。**



Add Rate-Based Rule State for 1 rule

Track By	Destination
Network	192.168.20.3
Rate	10 Count / 5 Seconds
New State	Drop and Generate Events
Timeout	30

GID	SID	Message
1	30549	SER… masscan access expl…
1	30777	SERVER-OTHER OpenSSL SSLv3 large heartbeat response
1	30778	
1	30785	
1	30514	
1	30779	
1	30780	
1	30786	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
1	30515	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
1	30781	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat

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。

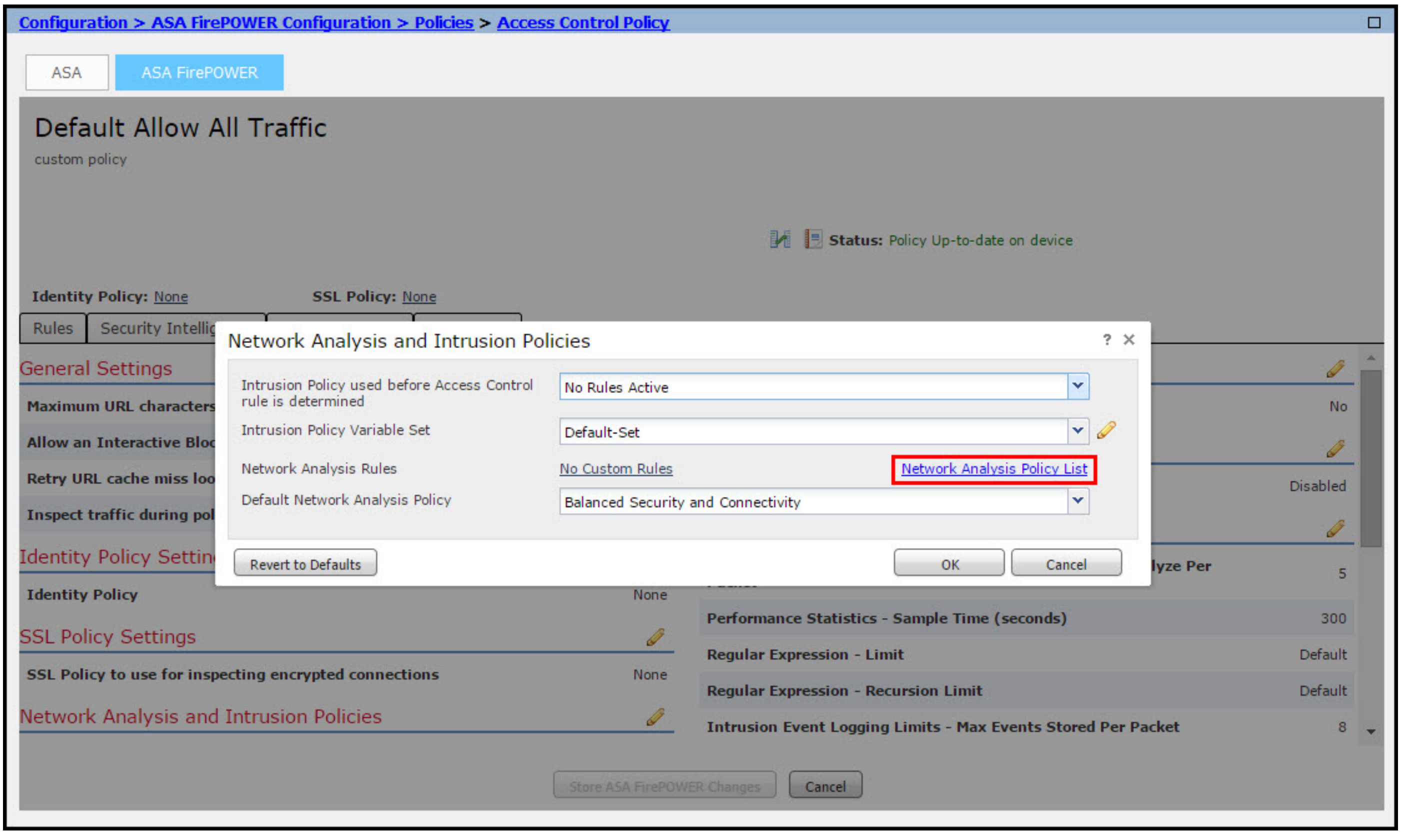
NAP对IP数据报进行分片重组，提供TCP状态检查和数据流重组以及校验和验证。预处理器将对流量进行规范化，验证和验证协议标准。

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 FirePOWER Configuration > Policies > Access Control Policy

ASA | ASA FirePOWER

Default Allow All Traffic

custom policy

Status: Policy Up-to-date on device

Identity Policy: None   SSL Policy: None

Rules | Security Intellig

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined	No Rules Active
Intrusion Policy Variable Set	Default-Set
Network Analysis Rules	No Custom Rules　Network Analysis Policy List
Default Network Analysis Policy	Balanced Security and Connectivity

Revert to Defaults　OK　Cancel

General Settings

Maximum URL characters	No
Allow an Interactive Bloc	
Retry URL cache miss loo	Disabled
Inspect traffic during pol	

Identity Policy Settin

Identity Policy	None

SSL Policy Settings

SSL Policy to use for inspecting encrypted connections	None

Network Analysis and Intrusion Policies

lyze Per	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default
Regular Expression - Recursion Limit	Default
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

Store ASA FirePOWER Changes　Cancel

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。

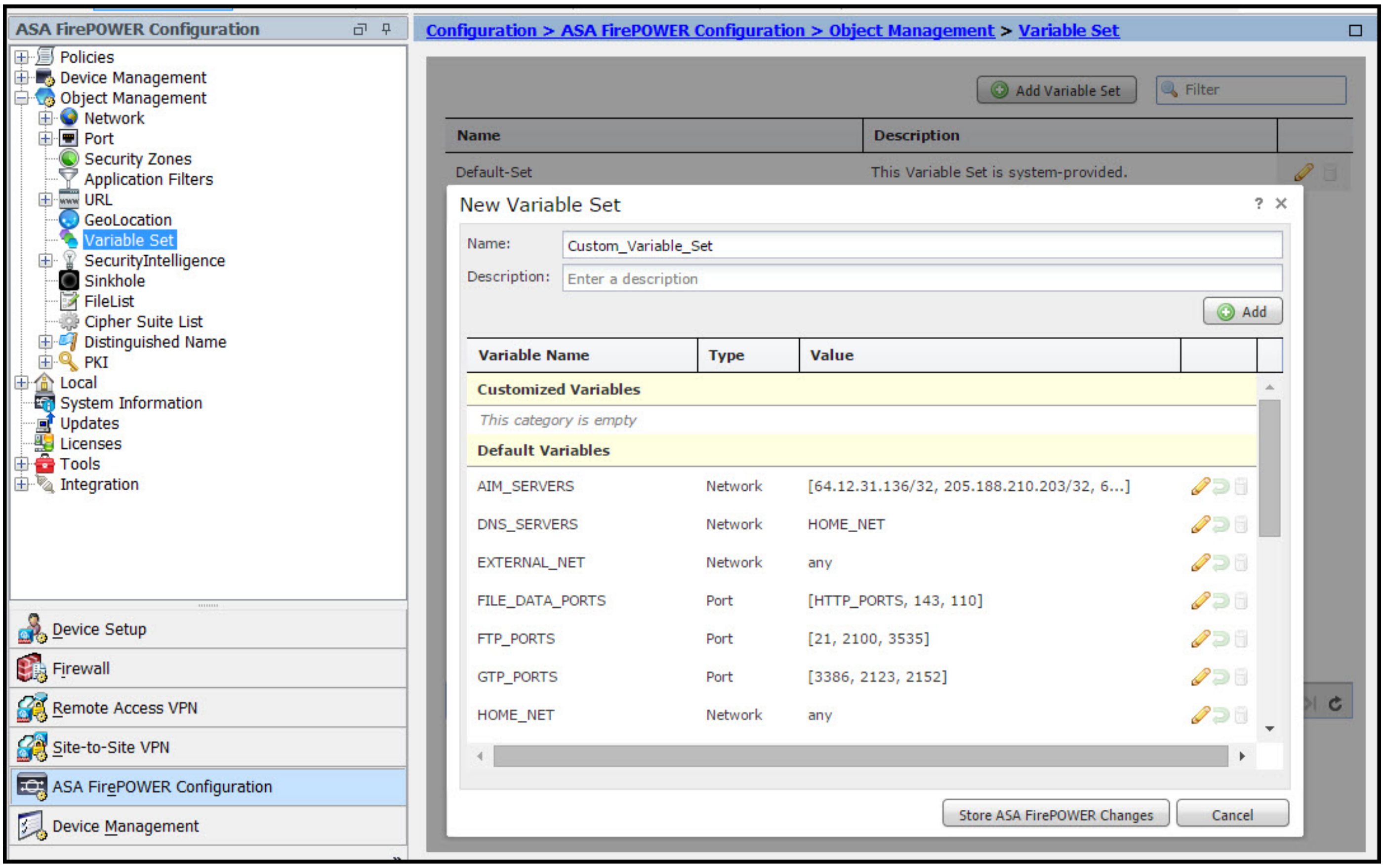
变量集已配置了默认选项（网络/端口）。 如果要更改默认配置，请添加新的变量集。

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。



Name	Description
Default-Set	This Variable Set is system-provided.

New Variable Set

Name: Custom_Variable_Set

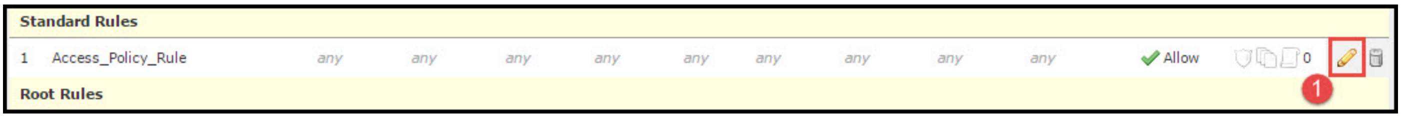
Description: Enter a description

Variable Name	Type	Value
Customized Variables		
This category is empty		
Default Variables		
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
EXTERNAL_NET	Network	any
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]
HOME_NET	Network	any

步骤 3：配置访问控制以包含入侵策略/NAP/变量集

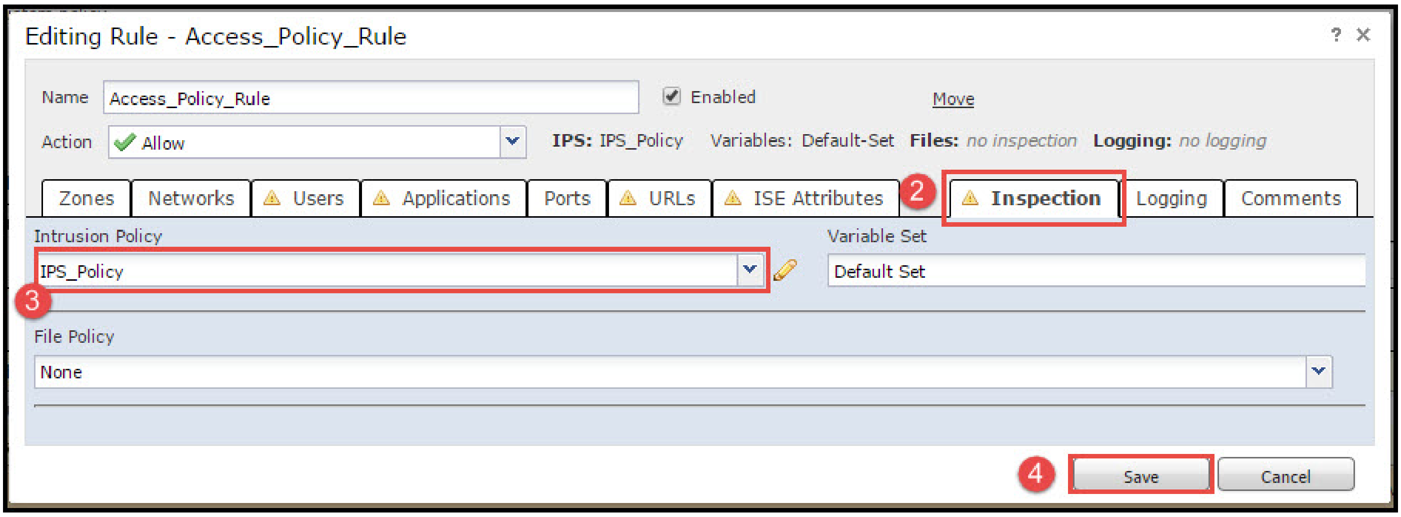
导航至**Configuration > ASA Firepower Configuration > Policies > Access Control Policy。**您需要完成以下步骤：

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	any	any	any	any	any	any	any	any	✓ Allow

Root Rules


Editing Rule - Access_Policy_Rule

Name Access_Policy_Rule ☑ Enabled Move

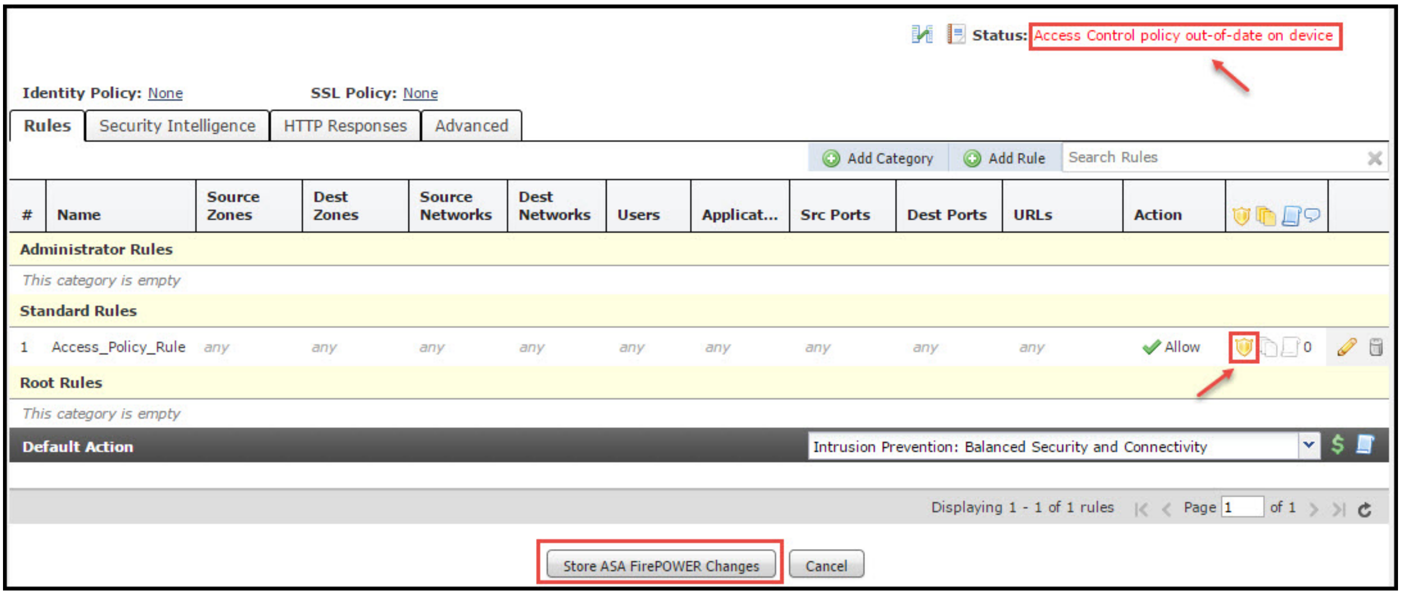
Action ✓ Allow IPS: IPS_Policy Variables: Default-Set **Files:** *no inspection* **Logging:** *no logging*

Intrusion Policy: IPS_Policy

Variable Set: Default Set

File Policy: None

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。



Status: Access Control policy out-of-date on device

Identity Policy: None SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat...	Src Ports	Dest Ports	URLs	Action	
Administrator Rules												
This category is empty												
Standard Rules												
1	Access_Policy_Rule	any	any	any	any	any	any	any	any	any	✓ Allow	0
Root Rules												
This category is empty												

Default Action: Intrusion Prevention: Balanced Security and Connectivity

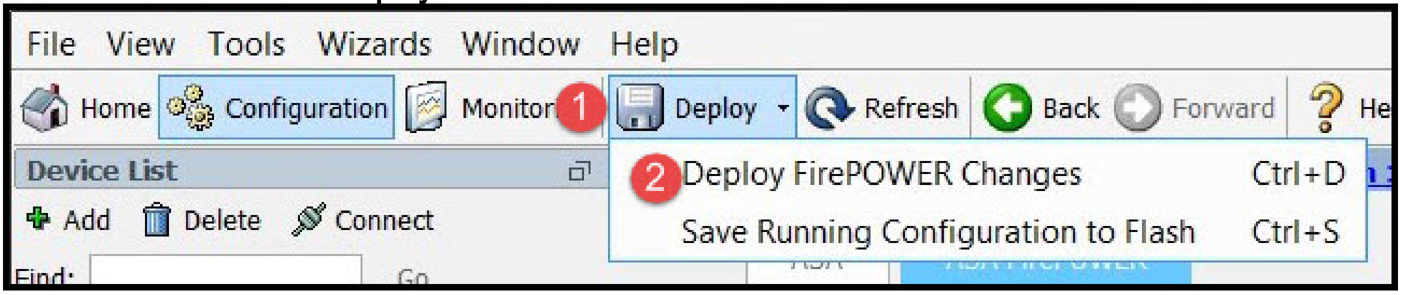
Displaying 1 - 1 of 1 rules Page 1 of 1

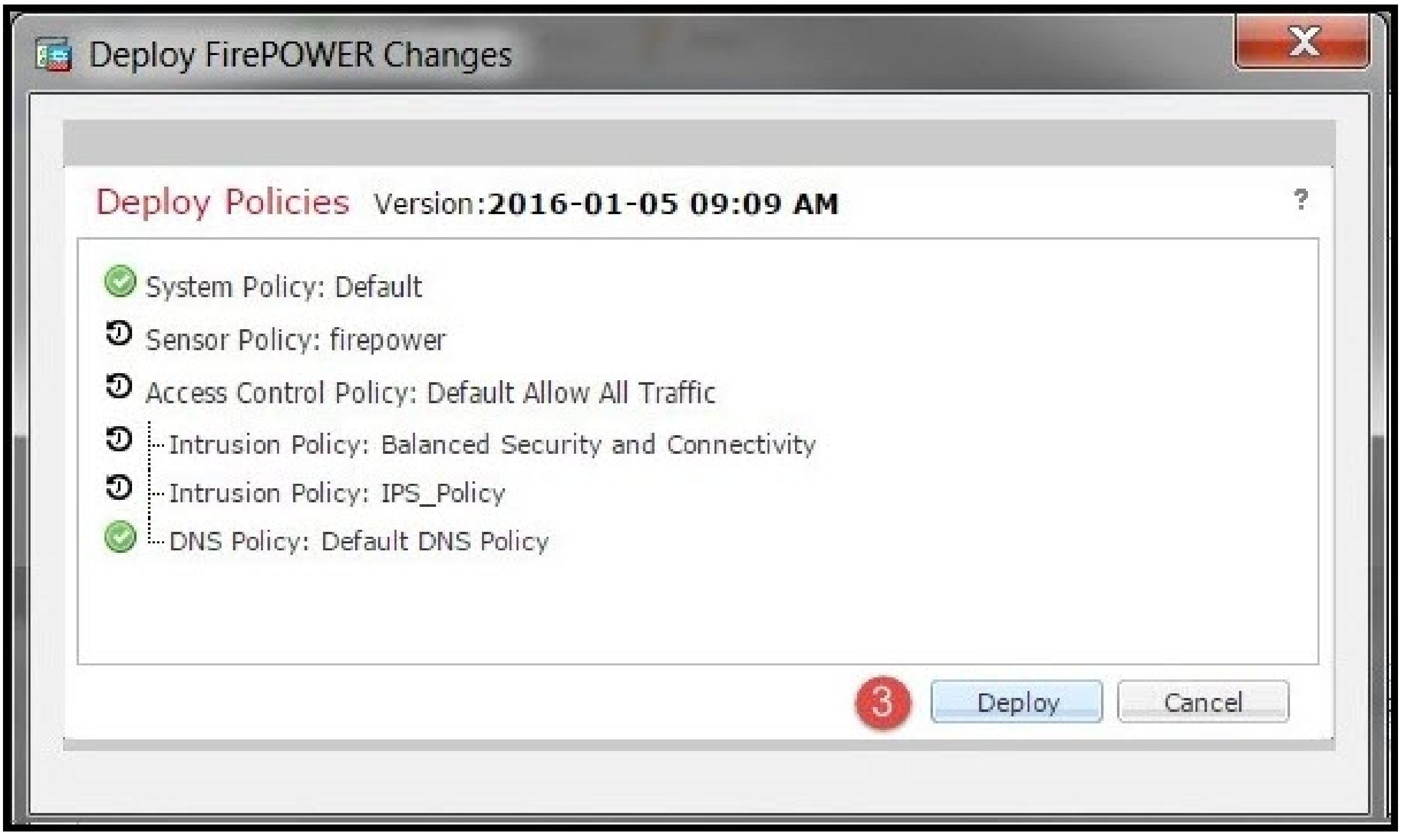
单击Store ASA FirePOWER changes（**存储ASA FirePOWER更改**）以保存更改。

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 09:09 AM

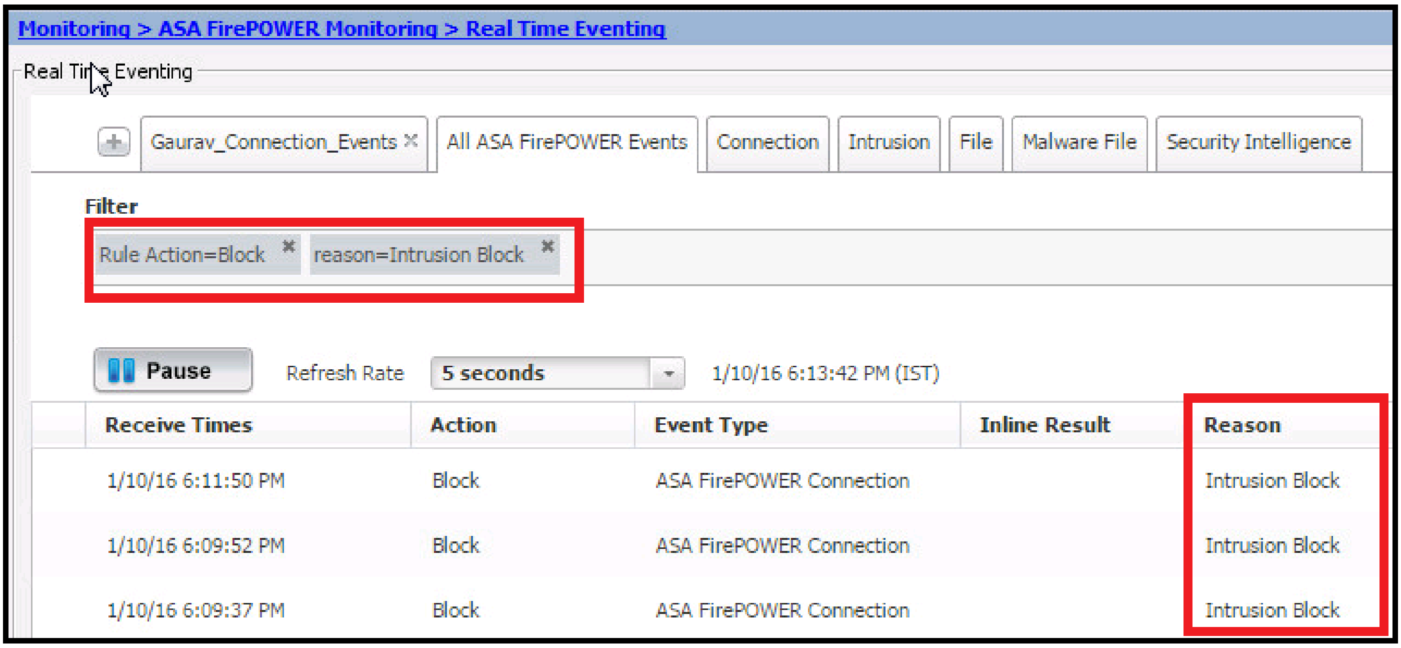
- System Policy: Default
- Sensor Policy: firepower
- Access Control Policy: Default Allow All Traffic
  - Intrusion Policy: Balanced Security and Connectivity
  - Intrusion Policy: IPS_Policy
  - DNS Policy: Default DNS Policy

: 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**。



Filter: Rule Action=Block, reason=Intrusion Block

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 Block
1/10/16 6:09:52 PM	Block	ASA FirePOWER Connection		Intrusion Block
1/10/16 6:09:37 PM	Block	ASA FirePOWER Connection		Intrusion Block

验证

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