通过ASDM（现场管理）使用思科安全情报时配置IP黑名单

目录

简介

本文档介绍使用低信誉IP地址的自定义/自动源时思科安全情报/IP地址信誉和IP黑名单（阻止）配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解ASA（自适应安全设备）防火墙、ASDM（自适应安全设备管理器）
- 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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

思科安全情报包括多个定期更新的IP地址集合，这些IP地址被思科TALOS团队确定信誉不佳。如果任何恶意活动源自IP地址（如SPAM、恶意软件、网络钓鱼攻击等），Cisco TALOS团队会确定信誉低。

思科IP安全情报源跟踪攻击者、Bogon、Bots、CnC、Dga、ExploitKit、恶意软件、Open_proxy、Open_relay、网络钓鱼、响应、垃圾邮件、可疑的数据库。Firepower模块提供创建低信誉IP地址的自定义源的选项。

安全情报源概述

以下是有关IP地址收集类型的一些详细信息，可在安全情报中分类为不同类别。

攻击者：持续扫描漏洞或尝试利用其他系统的IP地址的集合。

恶意软件：尝试传播恶意软件或主动攻击任何访问恶意软件的IP地址的集合。

网络钓鱼：主动试图欺骗最终用户输入用户名和密码等机密信息的主机集合。

垃圾邮件：已标识为发送垃圾邮件源的主机的集合。

机器人：作为僵尸网络的一部分积极参与并由已知僵尸网络控制器控制的主机的集合。

CnC:已标识为已知僵尸网络控制服务器的主机的集合。

OpenProxy:已知运行开放Web代理并提供匿名Web浏览服务的主机的集合。

OpenRelay:已知提供垃圾邮件和网络钓鱼攻击者使用的匿名邮件中继服务的主机集合。

TorExitNode:已知为Tor Anonymizer网络提供退出节点服务的主机的集合。

博贡：未分配但正在发送流量的IP地址的集合。

可疑：显示可疑活动并正在进行活动调查的IP地址的集合。

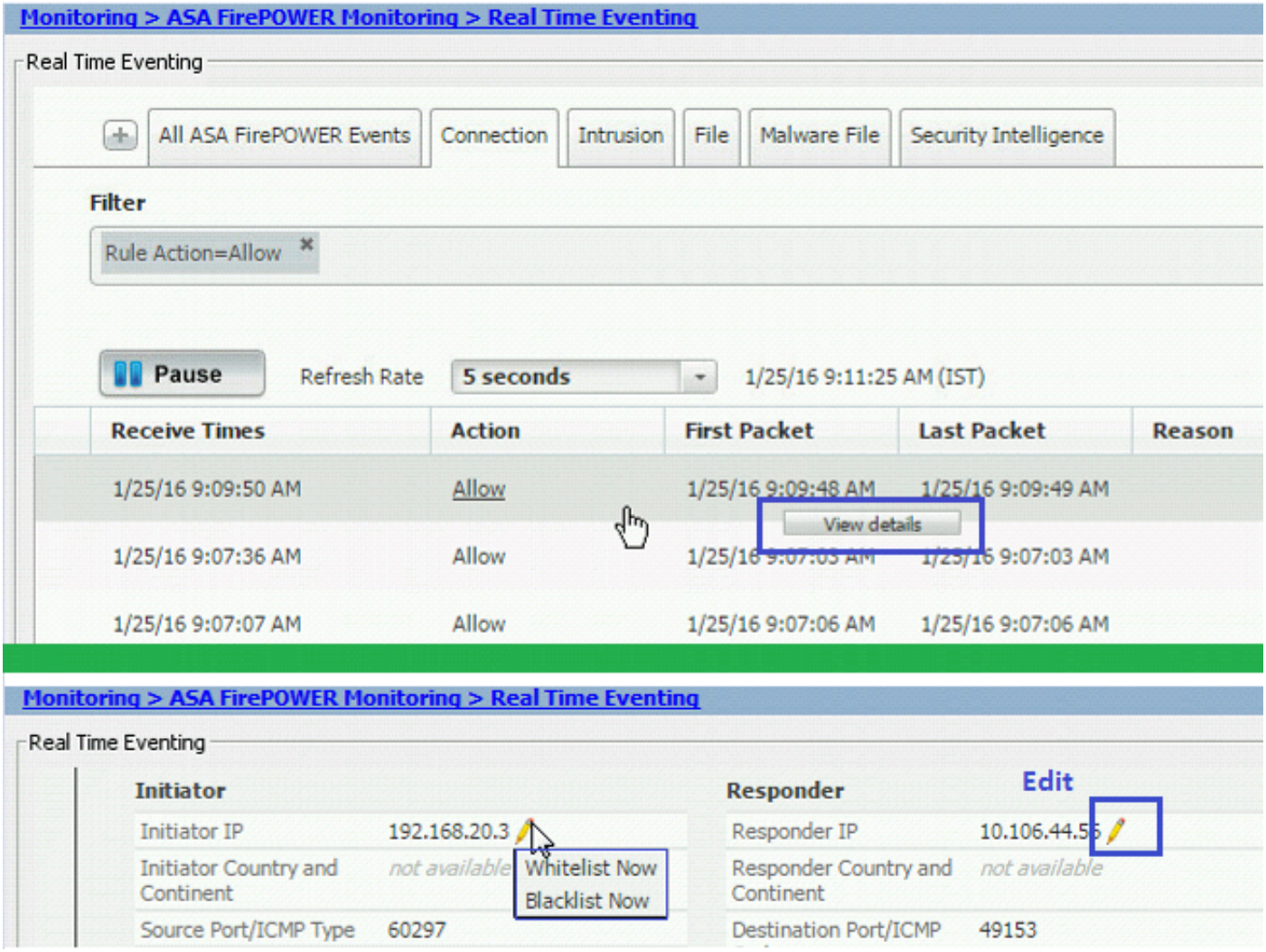
回复 :重复观察到的参与可疑或恶意行为的IP地址的集合。

手动将IP地址添加到全局黑名单和全局白名单

Firepower模块允许您在知道某些IP地址是某些恶意活动的一部分时，将其添加到全局黑名单。如果要允许流量到某些IP地址（被黑名单IP地址阻止），IP地址也可以添加到全局白名单。如果将任何IP地址添加到全局黑名单/全局白名单，则该地址将立即生效，无需应用策略。

要将IP地址添加到全局黑名单/全局白名单，请导航到**Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**，将鼠标悬停在连接事件上并选择**View Details**。

您可以将源或目标IP地址添加到全局黑名单/全局白名单。单击**Edit**按钮，然后选**择Whitelist Now/Blacklist Now** ，将IP地址添加到相应的列表，如图所示。



要验证源或目标IP地址是否已添加到全局黑名单/全局白名单，请导航至**Configuration > ASA Firepower Configuration > Object Management > Security Intelligence > Network Lists and Feeds**，并编**辑全局黑名单/全局白名单**。您还可以使用删除按钮从列表中删除任何IP地址。

创建黑名单IP地址的自定义列表

Firepower允许您创建可用于黑名单（阻止）的自定义网络/IP地址列表。 有三种方法可以执行此操作：

1. 您可以将IP地址写入文本文件（每行一个IP地址），并可以将文件上传到Firepower模块。要上传文件，请导航至**Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds，然后**点击**Add Network Lists and Feeds** **名称：** 指定自定义列表的名称。 **type： 从下拉列表中选**择“列表”。 **上传列表：** 选择**Browse**以在系统中查找文本文件。选择“**上载”**选项以上载文件。
2. 您可以将任何第三方IP数据库用于Firepower模块联系第三方服务器以获取IP地址列表的自定义列表。要进行配置，请导航至**Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds**，然后单击**Add Network Lists**

and Feeds

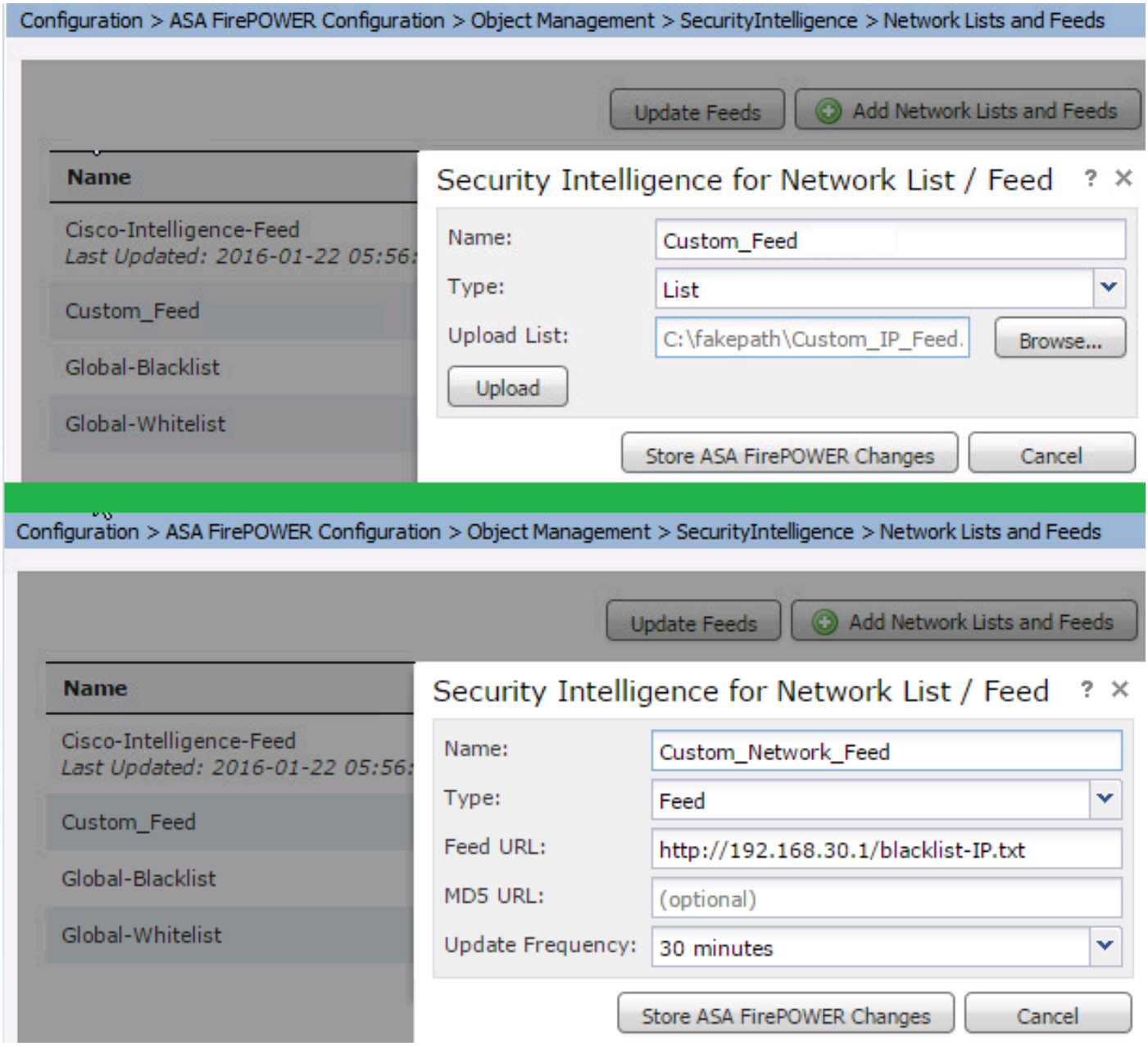
名称：指定自定义源的名称。

type：从下拉列表中选择Feed选项。

源URL:指定Firepower模块应连接并下载源的服务器的URL。

MD5 URL:指定哈希值以验证源URL路径。

更新频率：指定系统连接到URL源服务器的时间间隔。



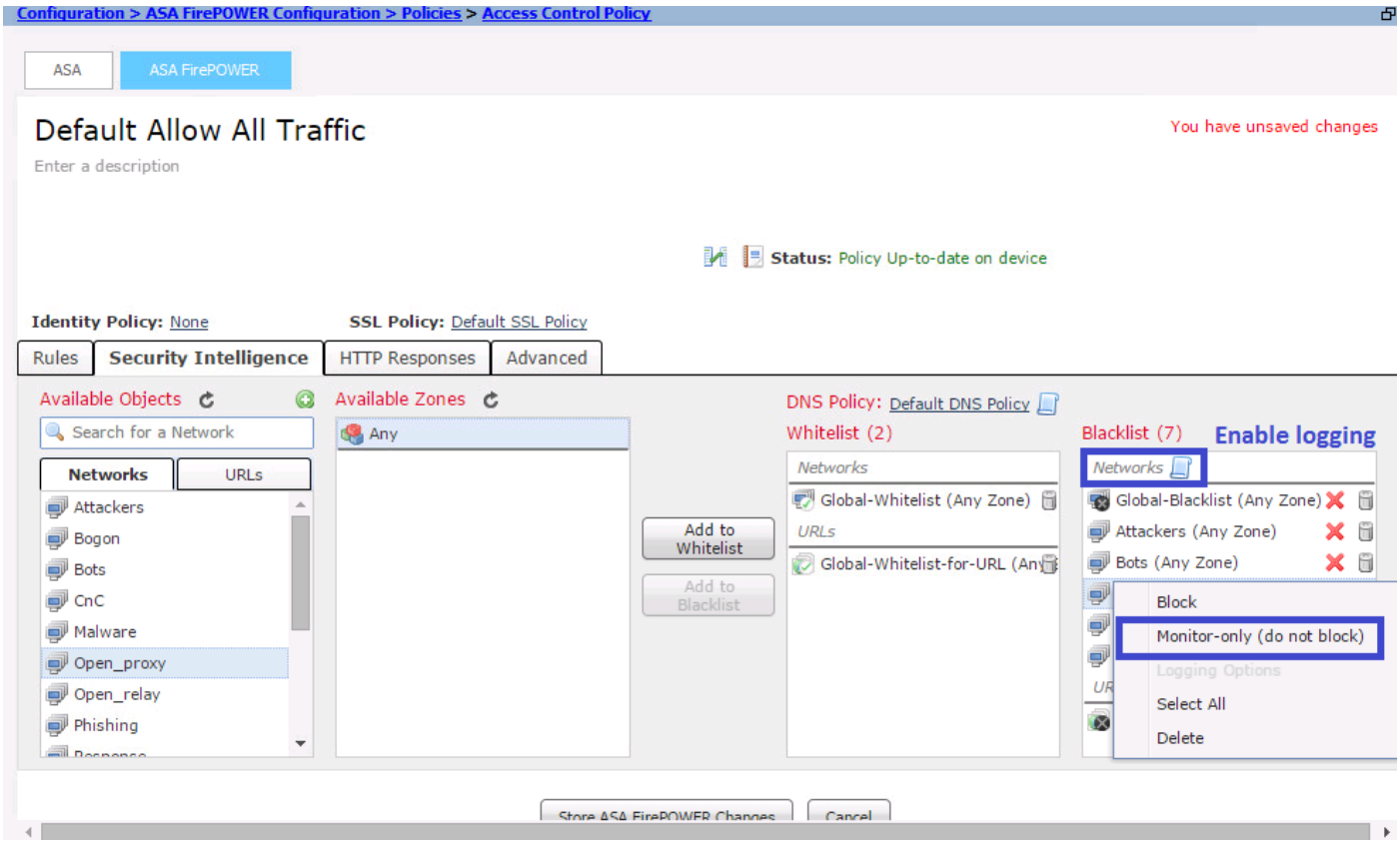
配置安全情报

要配置安全情报，请导航至**Configuration > ASA Firepower Configuration > Policies > Access Control Policy，选**择安**全情报**选项卡。

从Network Available Object中选择源，移到Whitelist/ **Blacklist列**以允许/阻止与恶意IP地址的连接。

您可以点击图标并启用映像中指定的日志记录。

如果只想为恶意IP连接生成事件而不是阻止连接，请右键单击源，选择**仅监控（不阻止）**，如图所示：

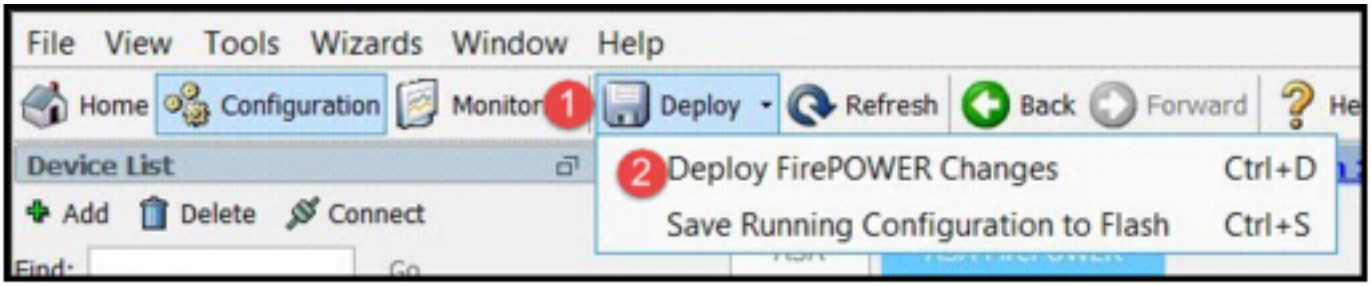


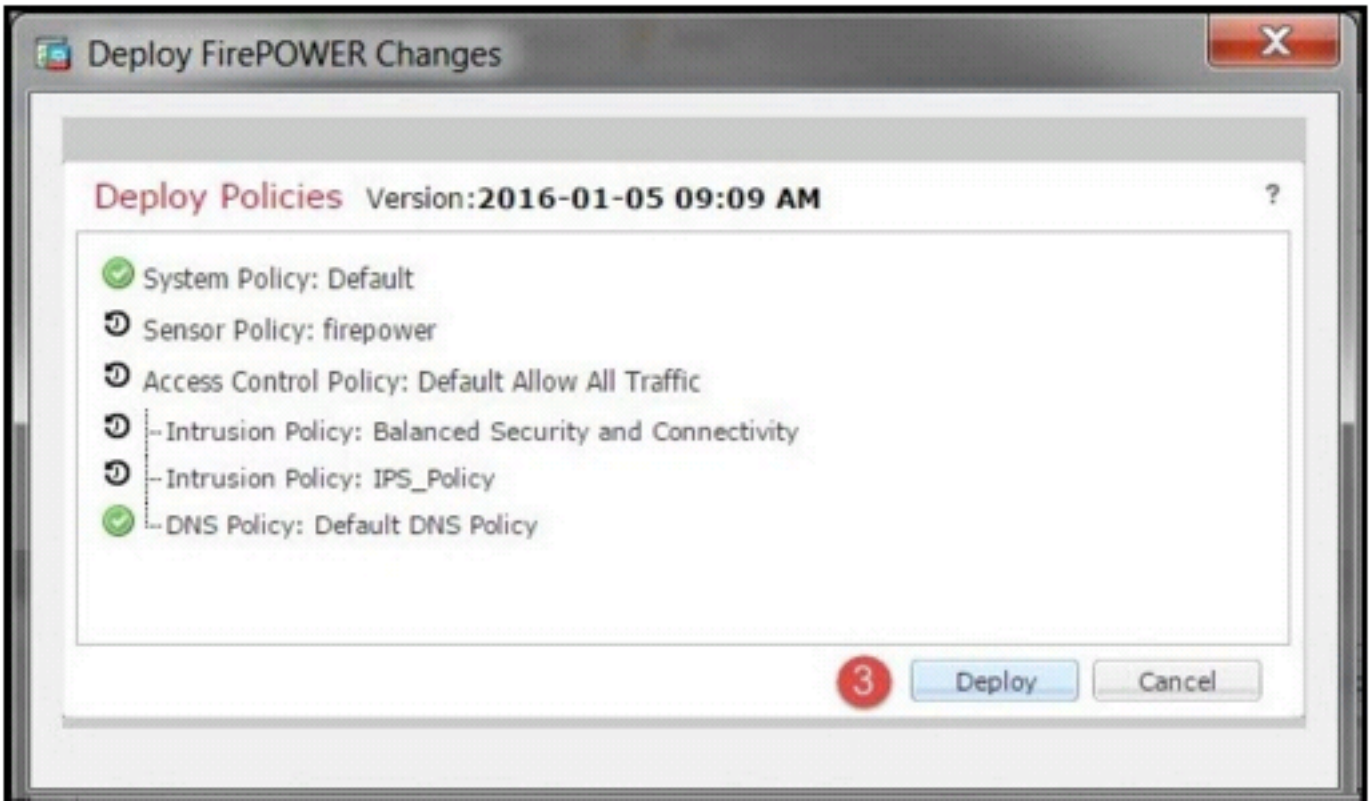
选择Store ASA Firepower Changes（存储ASA Firepower更改）选项以保存AC策略更改。

部署访问控制策略

要使更改生效，必须部署访问控制策略。在应用策略之前，请参阅指示设备上的访问控制策略是否已过期。

要将更改部署到传感器，请执行以下操作：c单击**Deploy**，然后选择**Deploy FirePOWER Changes**，然后在弹出窗口中选择**Deploy**以部署更改。



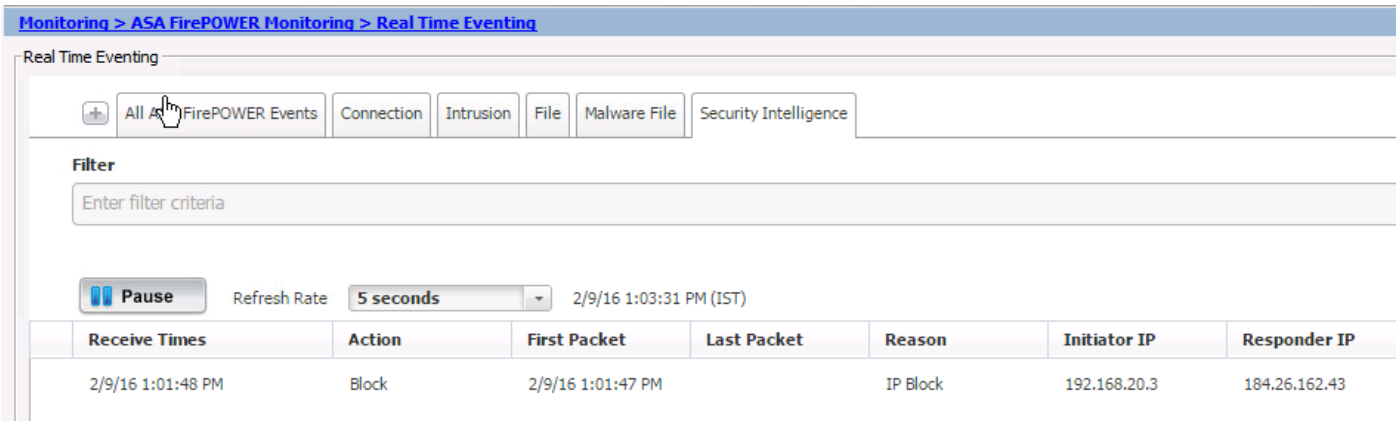


: 5.4.x“ASA FirePOWER”

> ASA Firepower>

安全情报事件监控

要通过Firepower模块查看安全情报，请导航至**Monitoring > ASA Firepower Monitoring > Real Time Eventing**。选择Security **Intelligence选**项卡。这将显示如图所示的事件：

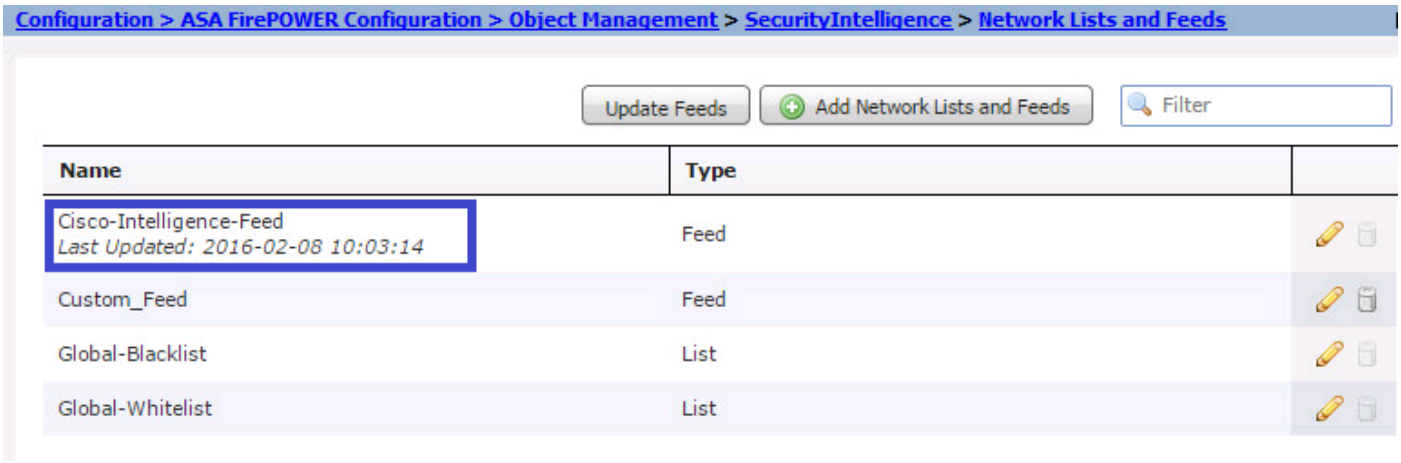


验证

当前没有可用于此配置的验证过程。

故障排除

为确保安全情报源是最新的，请导航至**Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds**，并检查上次更新源的时间。您可以选择“编辑”按钮以设置源更新的频率。



确保访问控制策略部署已成功完成。

监控安全情报，查看流量是否被阻止。

- **Cisco ASA FirePOWER**
- **- Cisco Systems**