目录

简介

本文描述Cisco安全智能/IP地址列入黑名单IP的名誉和的配置(阻塞)，当低声望IP地址时曾经自定义/自动加料。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA (可适应安全工具)防火墙知识， ASDM (可适应安全设备管理器)
- 火力设备知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA运行软件版本5.4.1的火力模块(ASA 5506X/5506H-X/5506W-X， ASA 5508-X， ASA 5516-X)以上
- ASA火力模块(ASA 5515-X， ASA 5525-X， ASA 5545-X， ASA 5555-X)运行软件版本6.0.0以上

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

Cisco安全智能包括思科TALOS团队取决于有恶劣的名誉IP地址的几有规律地更新的收藏。如果任何恶意活动起源于那些IP地址例如垃圾邮件、恶意软件，网络钓鱼攻击等，思科TALOS团队确定低名誉。

思科IP安全智能源跟踪攻击者数据库， Bogon，僵尸程序， CnC， Dga， ExploitKit，恶意软件，Open_proxy， Open_relay，网络钓鱼，答复，垃圾邮件，可疑。火力模块提供选项创建低声望IP地址自定义源。

安全智能源概述

这是关于的IP地址集种类的有些信息可以分类作为在安全智能的不同的类别。

攻击者：为漏洞连续扫描或尝试利用其他系统IP地址的集。

恶意软件：尝试传播恶意软件或积极地攻击人访问他们IP地址的集。

网络钓鱼：积极地尝试欺骗最终用户到输入保密信息类似用户名和密码主机的集。

垃圾邮件：识别主机的集，发送垃圾邮件电子邮件消息来源。

僵尸程序：积极参与作为僵尸网络一部分，主机的集，和是由已知僵尸程序网控制器控制的。

CnC ：识别作为已知僵尸网络的控制服务器主机的集。

OpenProxy ：知道运行开放Web代理和提供匿名Web浏览服务主机的集。

OpenRelay ：知道提供中继服务的匿名电子邮件主机的集由垃圾邮件和网络钓鱼攻击者使用了。

TorExitNode ：知道提供突岩Anonymizer网络的退出Services节点主机的集。

Bogon ：没有分配，然而IP地址的集发送流量。

可疑：显示可疑活动并且在活动调查外IP地址的集。

答复：重复被观察了参与可疑或有恶意的行为IP地址的集。

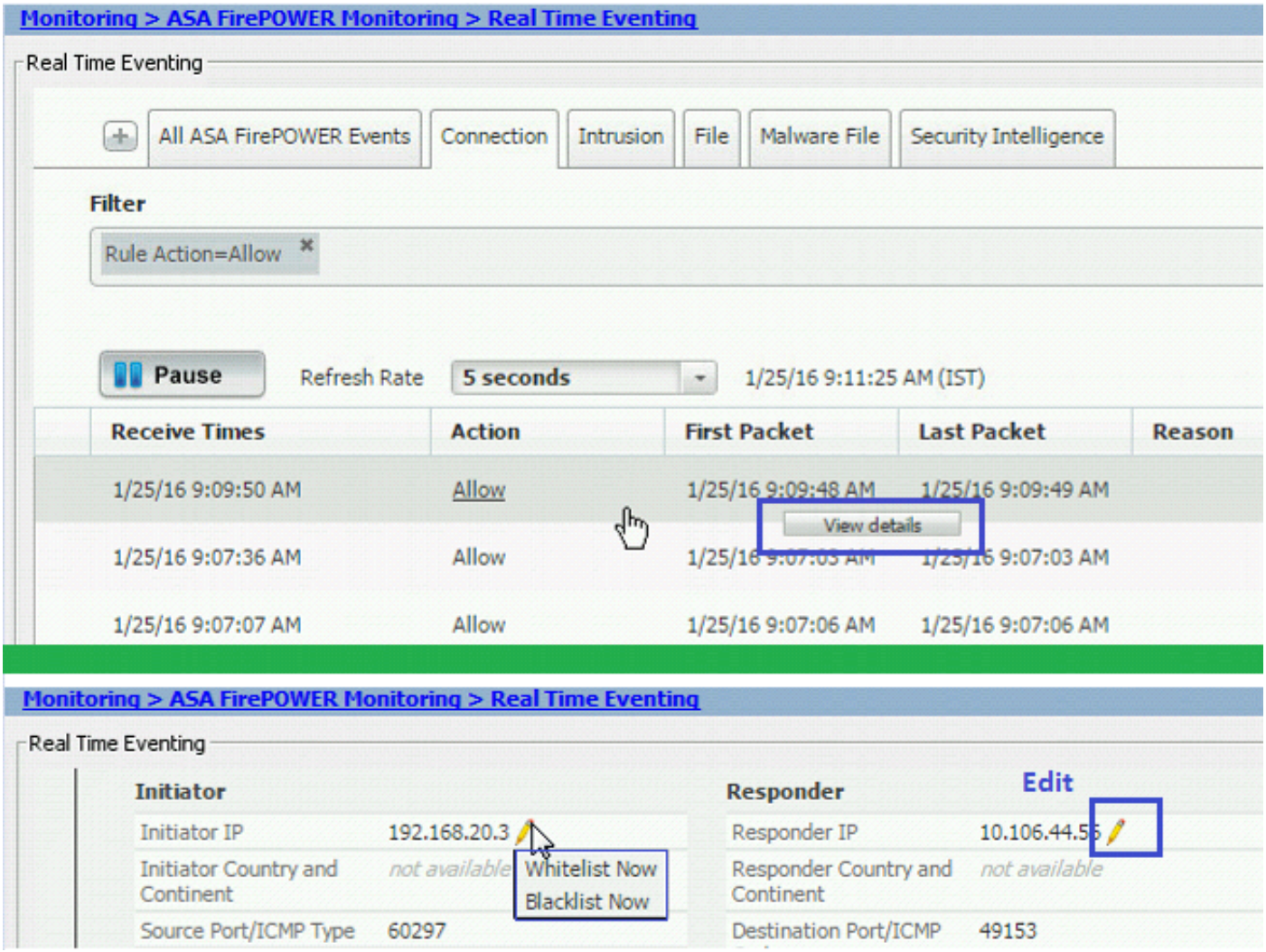
请手工添加IP地址全局黑名单和全局WHITELIST

火力模块给您添加某一IP地址全局黑名单，当您知道时他们是某恶意活动的一部分。IP地址可能也被添加到全局WHITELIST，如果要允许流量到由黑名单IP地址阻塞的某些IP地址。如果添加任何IP地址全局黑名单/全局WHITELIST，立即生效，不用需要运用策略。

为了添加IP地址全局黑名单全局WHITELIST，导航到**Monitoring> ASA火力Monitoring>实时Eventing**，盘旋在连接事件的鼠标和选择**视图详细信息**。

您能添加来源或目的IP地址到全局黑名单全局WHITELIST。如镜像所显示，点击**Edit按钮**并且**当前**

选择**Whitelist当前/黑名单**添加IP地址对各自列表。



为了验证来源或目的IP地址被添加到全局黑名单全局WHITELIST，请导航对**Configuration> ASA火力Configuration>对象Management>安全智能> Network Lists和源**并且编辑全局**黑名单全局Whitelist**。您能也使用删除按钮从列表删除所有IP地址。

创建黑名单IP地址定制列表

火力允许您建立可以用于列入黑名单的自定义网络/IP地址列表(阻塞)。有三选项执行此：

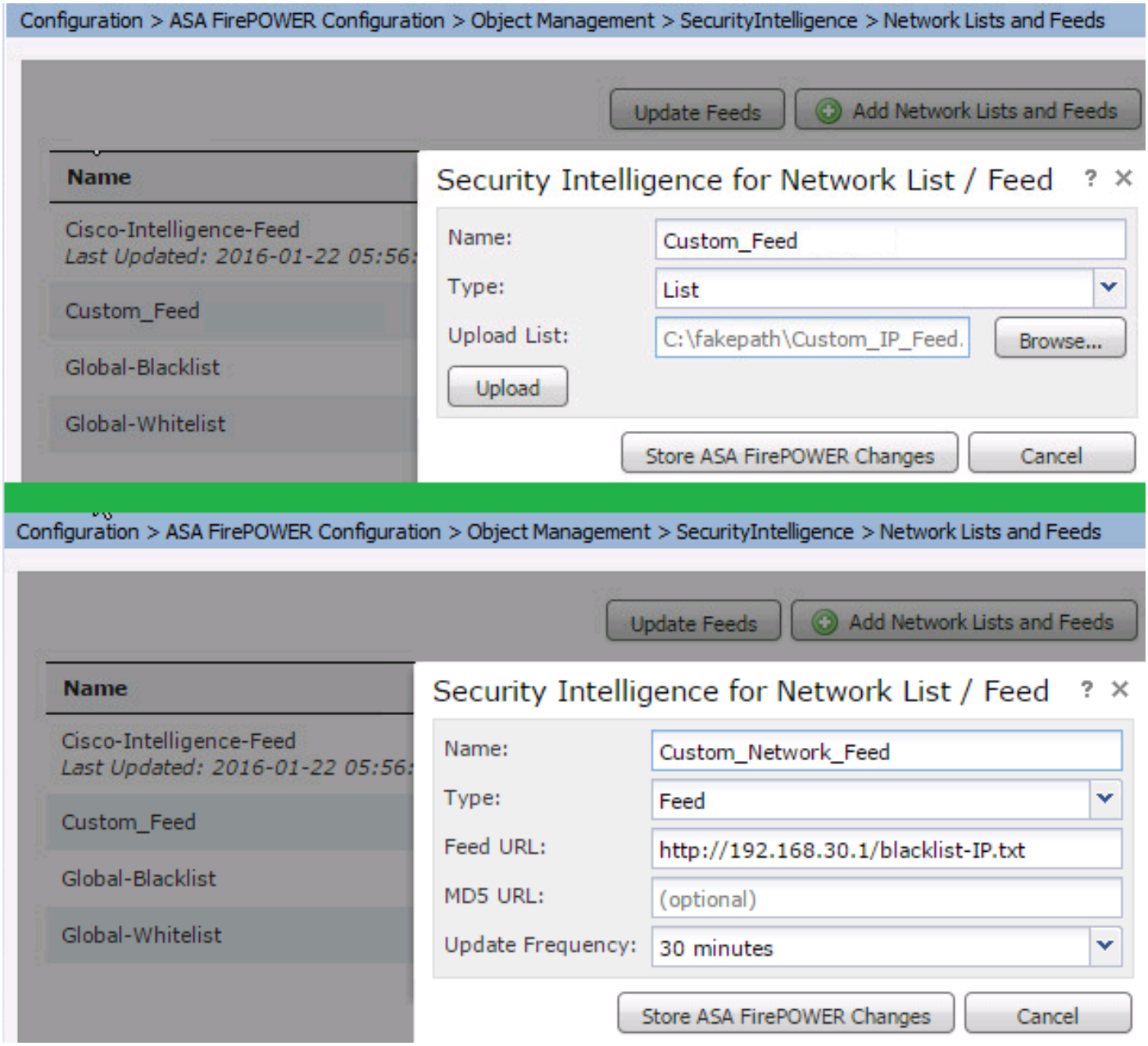
1. 您写IP地址到文本文件(每条线路一个IP地址)并且能上传文件到火力模块。为了上传文件，请导航对**Configuration> ASA火力Configuration>对象Management>安全智能> Network Lists和源**然后单击**加网络列表和源** **名称：** 指定定制列表名称。 **类型：** 选择从下拉列表的**列表。** **加载列表：** 选择**浏览**寻找在您的系统的文本文件。选择选项**加载**上传文件。
2. 您能使用所有第三方IP数据库火力模块联系第三方服务器拿来IP地址列表的定制列表。为了配置此，请导航对**Configuration> ASA火力Configuration>对象Management>安全智能> Network Lists和源**然后单击**加网络列表和源**
   名称：指定自定义源的名称。

   类型：从下拉列表的挑选选项**源。**

   源URL ：指定火力模块应该连接服务器的URL并且下载源。

MD5 URL ：指定Hash值验证源URL路径。

更新频率：指定系统连接到URL源服务器的时间间隔。



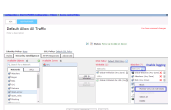
配置安全智能

为了配置安全智能，请导航对**Configuration> ASA火力Configuration>策略>访问控制策略，**选择**安全智能**选项卡。

从网络可用的对象选择源，移动对**Whitelist/黑名单**列准许/块对有恶意的IP地址的连接。

您能在镜像上指定单击图标和启用日志。

如果要生成有恶意的IP连接的事件而不是阻塞连接，则请用鼠标右键单击在源，选择**只监控的(不块**)如镜像所显示， ：

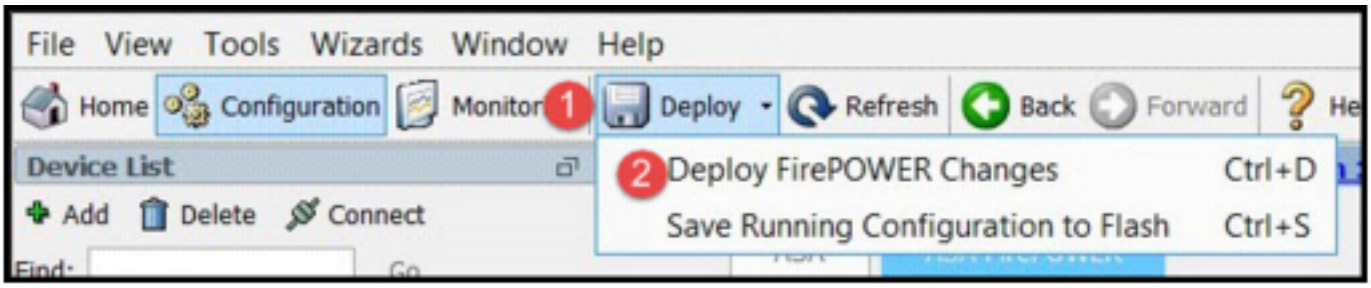


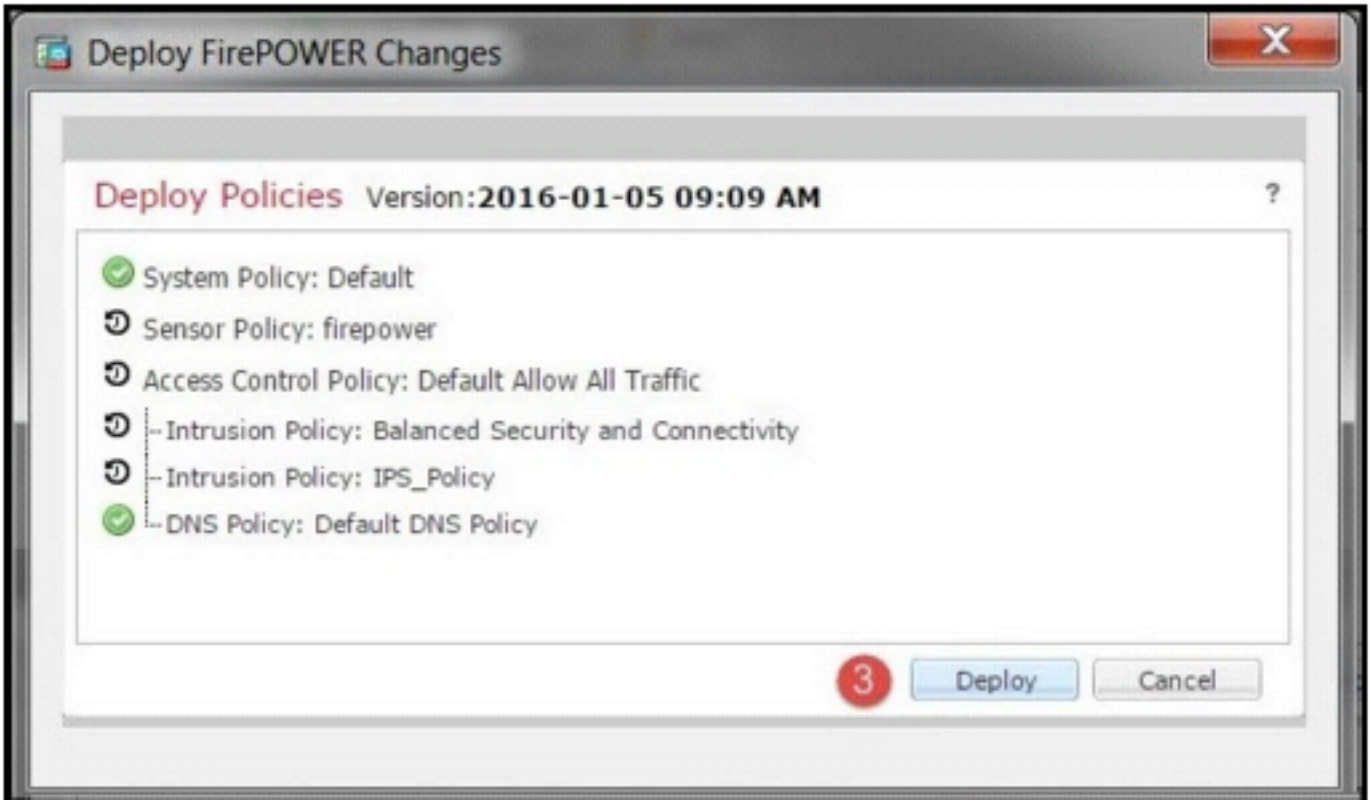
选择选项存储ASA火力更改保存AC策略变更。

实施访问控制策略

使更改生效，您必须实施访问控制策略。在您运用策略前，请参阅的征兆是否访问控制策略是过时的在设备。

要部署对传感器的更改，请单击**部署**并且选择**部署火力更改**然后选择**部署**在弹出窗口部署更改。



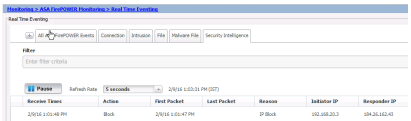


5.4.x**ASA**

Monitoring> ASAMonitoring>

安全智能？s事件监控

为了由火力模块看到安全智能，请导航对**Monitoring> ASA火力Monitoring>实时Eventing**。选择**安全智能**选项卡。如镜像所显示，这将出现事件：

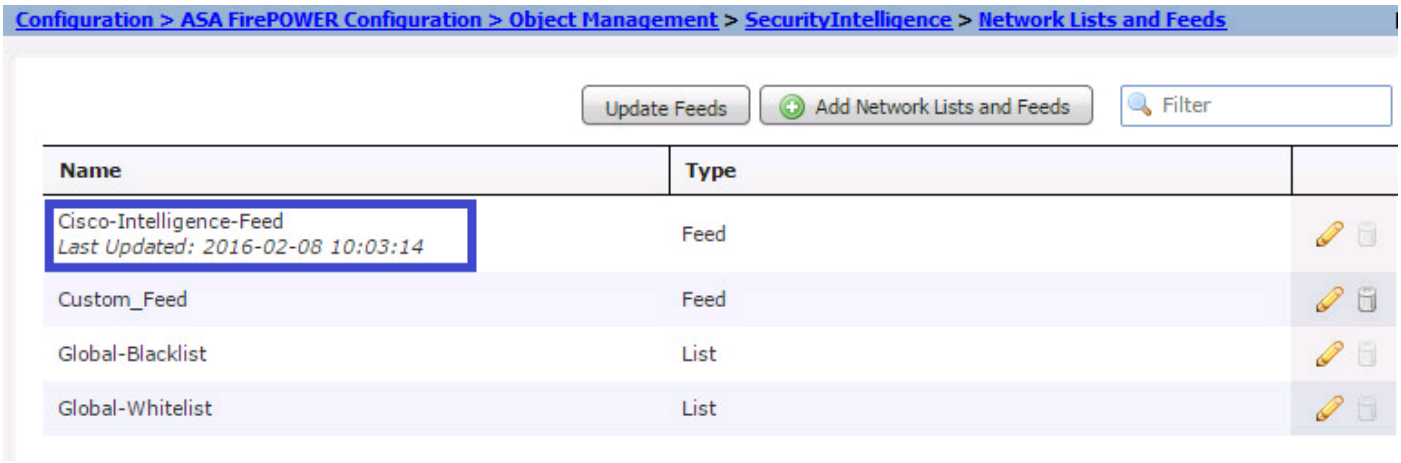


验证

当前没有可用于此配置的验证过程。

故障排除

为了保证安全智能源最新，请导航对**Configuration> ASA火力Configuration>对象Management>安全智能> Network Lists和源**并且检查时候，当源是最近更新。您能选择编辑按钮设置频率源更新。



保证访问控制策略部署顺利地完成。

监控安全智能发现流量是否阻塞。

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