Cisco FireSIGHT系统的安全情报阻止或列入黑名单的IP地址

目录

简介

安全情报功能允许您根据源IP地址或目标IP地址指定可以流经网络的流量。如果要在流量接受访问控制规则分析之前将特定IP地址列入黑名单（拒绝进出），则此功能特别有用。本文档介绍如何处理Cisco FireSIGHT系统阻止或列入黑名单的IP地址时的场景。

先决条件

要求

思科建议您了解Cisco FireSIGHT管理中心。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- 思科FireSIGHT管理中心
- 思科Firepower设备
- 具备Firepower(SFR)的Cisco ASA模块
- 5.2 或更高软件版本

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。

情报源与情报列表的区别

在FireSIGHT系统中使用安全情报功能有两种方法：

安全情报源

安全情报源是防御中心从HTTP或HTTPS服务器下载的IP地址的动态集合。为帮助您构建黑名单，思科提供*安全情报源*，该源代表漏洞研究团队(VRT)确定的信誉不佳的IP地址。

安全情报列表

与源相比，安全情报列表是一个简单的静态IP地址列表，您可以手动上传到FireSIGHT管理中心。

合法IP地址被阻止或列入黑名单

验证IP地址是否在安全情报源中

如果IP地址被安全情报源黑名单阻止，您可以按照以下步骤进行验证：

步骤 1：访问Firepower设备或服务模块的CLI。

步骤 2：运行以下命令。将<IP_Address>替换为要搜索的IP地址：

```
admin@Firepower:~$ grep
```

例如，如果要搜索IP地址198.51.100.1，请运行以下命令：

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

如果此命令返回您提供的IP地址的任何匹配项，则表明IP地址存在于安全情报源黑名单中。

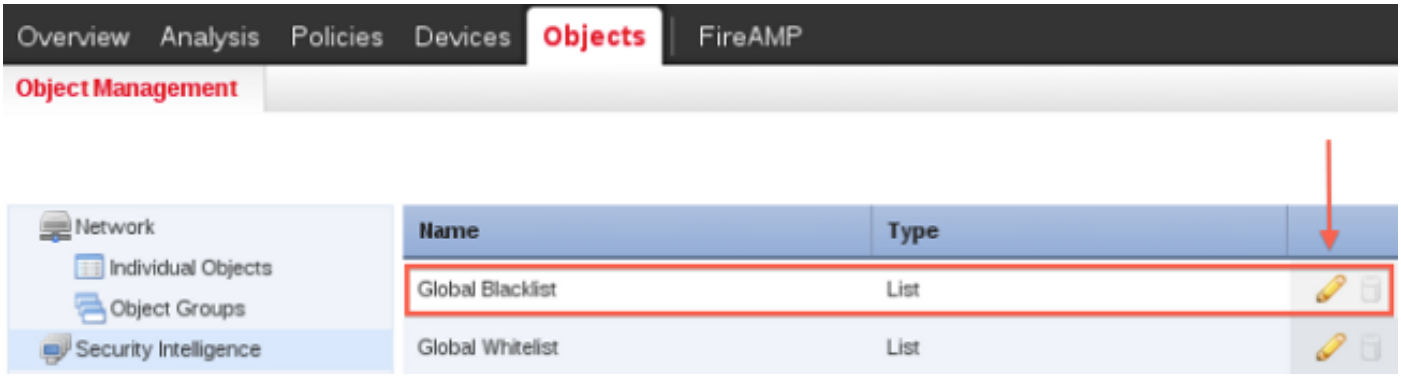
检查黑名单

要查找可能列入黑名单的IP地址列表，请执行以下步骤：

步骤 1：访问FireSIGHT管理中心的Web界面。

步骤 2：导航至**对象>对象管理>安全情报**。

步骤 3：单击铅笔*图*标打开或编辑全**局黑名单**。系统将显示一个弹出窗口，其中包含IP地址列表。



使用已阻止或列入黑名单的IP地址

如果安全情报源阻止或列入黑名单的特定IP地址，您可以考虑以下任一选项来允许它。

选项 1：安全情报白名单

您可以将安全情报列入黑名单的IP地址列入白名单。白名单将覆盖其黑名单。FireSIGHT系统使用访问控制规则评估具有列入白名单的源或目标IP地址的流量，即使IP地址也列入黑名单。因此，当黑名单仍然有用，但范围太广，并且错误地阻止要检查的流量时，可以使用白名单。

例如，如果信誉良好的源错误地阻止了您对重要资源的访问，但总体上对您的组织有用，则您可以仅将不正确分类的IP地址列入白名单，而不是从黑名单中删除整个源。

> **警告**：在访问控制策略中进行任何更改后，必须将策略重新应用到受管设备。

选项 2：按安全区域实施安全情报过滤器

为了增加粒度，可以根据连接中的源或目标IP地址是否驻留在特定安全区域中来实施安全情报过滤。

要扩展上述白名单示例，您可以将未正确分类的IP地址列入白名单，但随后使用组织中需要访问这些IP地址的人员使用的安全区域限制白名单对象。这样，只有有业务需要的人才能访问列入白名单的IP地址。例如，您可能希望使用第三方垃圾邮件源将电子邮件服务器安全区域上的流量列入黑名单。

选项 3：监控，而不是黑名单

如果您不确定要将特定IP地址还是一组地址列入黑名单，则可以使用“仅监控”设置，该设置允许系统将匹配连接传递给访问控制规则，但也会将匹配项记录到黑名单。请注意，不能将全局黑名单设置为仅监控

请考虑在使用该源实施阻止之前要测试第三方源的场景。将源设置为仅监控时，系统允许系统进一步分析本应被阻止的连接，但也会记录这些连接的记录以供评估。

使用“仅监控”设置配置安全情报的步骤：

1. 在访问控**制策略**的“安全情报”(Security Intelligence)选项卡上，单击日志记录图标。系统将显示Blacklist Options对话框。
2. 选中**Log Connections**复选框以在流量满足安全情报条件时记录连接开始事件。

3. 指定将连接事件发送到何处。
4. 单击**OK**以设置日志记录选项。系统将再次显示Security Intelligence选项卡。
5. Click **Save**.必须应用访问控制策略，更改才能生效。

选项 4：联系思科技术支持中心

在以下情况下，您始终可以联系思科技术支持中心：

- 您对上述选项1、2或3有疑问。
- 您需要对安全情报列入黑名单的IP地址进行进一步研究和分析。
- 您需要解释为什么IP地址被安全情报列入黑名单。