IP地址由思科FireSIGHT系统的安全智能阻塞或列入黑名单

文档ID117993

已更新：十月21， 2015

贡献用Nazmul Rajib， Cisco TAC工程师。

下载 pdf文档
打印
Feedback

相关产品

- 思科FireSIGHT管理中心750
- 思科FireSIGHT管理中心3500
- 思科FireSIGHT管理中心1500
- 思科FireSIGHT管理中心

目录

简介

安全智能功能允许您指定能穿程根据来源或目的IP地址的您的网络的流量。这是特别有用的，如果要列入黑名单-请否决流量到/从-特定IP地址，在流量对分析被服从由访问控制规则前。当IP地址由思科FireSIGHT系统时，阻塞或列入黑名单本文描述如何处理方案。

先决条件

要求

思科建议您有在思科FireSIGHT管理中心的知识。

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
- 思科ASA用Firepower (SFR)模块
- 软件版本5.2或以上

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。

在智能源和智能列表之间的区别

有两种方式使用安全智能功能在FireSIGHT System:

安全智能源

安全智能源是防御中心从HTTP或HTTPS服务器下载IP地址的动态收藏。要帮助您建立黑名单，思科提供*安全智能源*，代表漏洞研究小组取决于的IP地址(VRT)有恶劣的名誉。

安全智能列表

安全智能列表，对比与源，是您手工上传对FireSIGHT管理中心IP地址的一张简单静态列表。

合法IP地址阻塞或列入黑名单

如果IP地址在安全智能源，请验证

如果IP地址由安全智能源黑名单阻塞，您能遵从下面步骤验证此：

步骤 1：访问Firepower设备或服务模块的CLI。

步骤 2：运行以下命令。用您要搜索的IP地址替换<ip_address> ：

```
admin@Firepower:~$ grep <IP_Address> /var/sf/iprep_download/*.blf
```

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，表明IP地址是存在安全智能源黑名单。

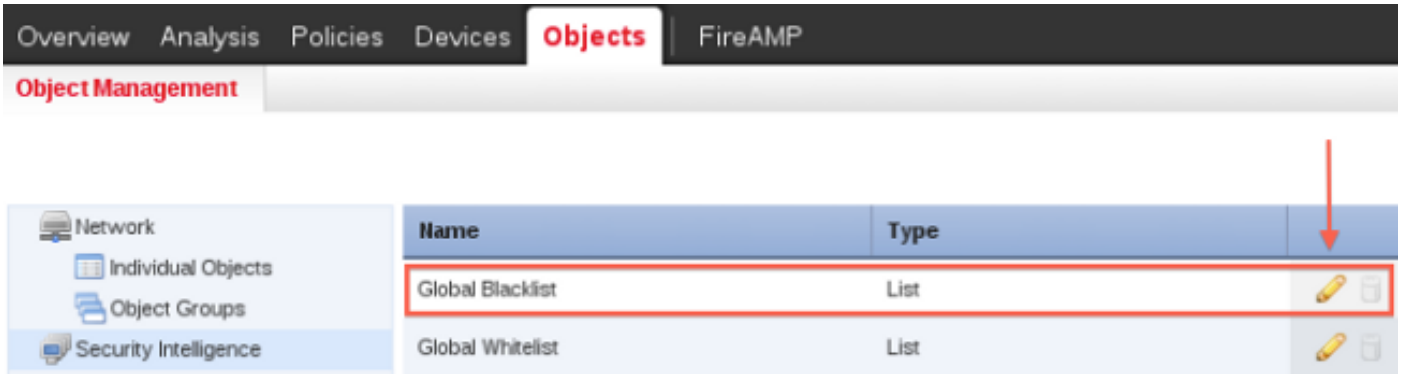
检查黑名单

要查找也许列入黑名单IP地址的列表，请遵从下面步骤：

步骤 1：对FireSIGHT管理中心的Web接口的访问。

步骤 2：导航对**对象>对象Management>安全智能**。

步骤 3：点击*铅笔*图标打开或编辑**全局黑名单**。一弹出与IP地址列表的窗口出现。



与阻止或列入黑名单的IP地址一起使用

如果特定IP地址由安全智能源阻塞或列入黑名单，您能设想以下选项中的任一个允许它。

选项 1：安全智能Whitelists

您能whitelist由安全智能列入黑名单的IP地址。whitelist改写其黑名单。使用访问控制规则，FireSIGHT系统评估与一whitelisted来源的流量或目的IP地址，即使IP地址也列入黑名单。所以，您能使用whitelist，当黑名单是有用的时，但是太清楚的在范围和不正确地阻塞您要检查的流量。

例如，如果一个名声好的源不正确地阻止您的对一种重要资源的访问，但是整体上有用的对您的组织，您能whitelist仅不正确地分类的IP地址，而不是删除整个源从黑名单。

> **Caution**:在您做在访问控制策略后的所有变动，您必须重新应用策略到受管理设备。

选项 2：由安全区强制执行安全智能过滤器

对于已添加粒度，您能强制执行基于的安全智能过滤来源或目的IP地址在连接是否位于一个特定的安全区。

另一方面要扩大whitelist以上示例，您可能whitelist不正确地分类的IP地址，但是限制whitelist对象使用需要访问那些IP地址的那些使用的安全区在您的组织。该方式，仅那些与商业需要能访问whitelisted IP地址。作为另一示例，您也许要用一个第三方垃圾邮件源列入黑名单在电子邮件服务器安全区的流量。

选项 3：箴言报，而不是黑名单

如果不肯定您是否要列入黑名单特定IP地址或套地址，您能使用“只监控的”设置，允许系统通过对访问控制规则的匹配的连接，而且记录匹配对黑名单。注意您不能设置全局黑名单到只监控的

考虑使用该源前，您要测试一个第三方源的一个方案，在您实现阻塞。当您设置源对只监控的时，系统允许将阻塞被系统进一步分析的连接，而且记录您的评估的那些连接中的每一的记录。

配置与“只监控的”设置的安全智能的步骤：

1. 在访问控制策略的**安全智能**选项卡，请点击记录日志图标。黑名单选项对话框出现。
2. 当流量符合安全智能情况时，请选择**日志连接**复选框记录开始处连接事件。
3. 在哪里指定发送连接事件。
4. 点击OK键设置您的日志选项。安全智能选项卡再出现。
5. Click **Save**.您必须申请访问控制策略您的更改生效。

选项4 ：联系方式Cisco技术支持中心

您能总是与Cisco技术支持中心联系，如果：

- 您有与上述选项1， 2或者3.的问题。
- 您想要进一步研究和分析在安全智能列入黑名单的IP地址。
- 您想要说明IP地址为什么由安全智能列入黑名单。

本文档是否是有用？有 没有

感谢您的反馈。

打开支持案例（需要思科服务合同。）

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：十月21， 2015

文档ID117993