安全情报

以下主题提供安全情报的概述，包括用于将流量和基本设置列入阻止名单和允许名单。

关于安全情报

作为防御恶意互联网内容的第一道防线，安全情报使用信誉情报快速阻止与IP地址、URL和域名的连接。这称为 列入安全情报阻止列表。

在系统执行需要更多资源的评估之前，安全情报是访问控制的第一阶段。使用阻止列表通过快速排除不需要检测的流量来提高性能。

注释 不能使用阻止列表阻止快速路径流量。预过滤器评估发生 在安全情报过滤之前。使用快速路径的流量会绕过所有的进一步评估，包括安全情报。

虽然您可以配置自定义阻止列表，但思科提供对定期更新的情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。

您可以使用“不阻止”列表和仅监控“阻止”阻止列表细化安全情报阻止列表。这些机制可以使流量免于列入阻止名单，但 **不会** 自动信任匹配流量或对其使用快速路径。 添加到 "不阻止 "列表中的流量或在安全情报阶段被监控的流量会被有意地与其他访问控制进行进一步分析。

相关主题

安全情报

安全情报的最佳实践

- 配置访问控制策略以阻止由思科提供的安全情报源所检测到的威胁。请参阅配置示例：安全情报阻止，第 9 页。
- 如果要使用自定义威胁数据来补充思科提供的安全情报源，或手动阻止新出现的威胁：
  - 对于 IP 地址，请使用自定义安全情报列表和源，或者网络对象或组。要创建这些内容，请参阅安全情报和网络及其子主题。要将其用于安全情报，请参阅配置安全情报，第 4 页。安全情报策略中使用的网络对象需要 IPS 许可证。
  - 对于 URL 和域，请使用自定义安全情报列表和源，而不是对象或组。请参阅手动 URL 过滤选项中的详细信息
  - 您还可以将条目从事件添加到阻止列表。请参阅全局和域安全情报列表。
- 要测试新源或被动部署，请将操作从阻止设为仅监控。请参阅安全情报监控，第 10 页。
- 如果需要从安全情报阻止中排除特定站点或地址，请参阅覆盖安全情报阻止，第 11 页。
- 如果您的 Firepower 部署与 SecureX 或相关工具 SecureX 威胁响应（以前称为思科威胁响应或 CTR）集成，并且使用了自定义安全情报列表和源，请务必使用这些列表和源来更新安全服务交换。有关详细信息，请参阅安全服务交换联机帮助中有关配置事件自动升级的说明。有关此集成的一般信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的与思科 *SecureX*集成。
- 系统提供的安全情报类别可能会随着时间的推移而发生变化，恕不另行通知；您应该计划定期检查更改，并相应地修改策略。
- 您还应配置URL过滤，这是一项具有单独许可要求的单独功能，旨在进一步防御恶意站点。请参阅URL 过滤。

安全智能许可证要求

威胁防御 许可证

IPS

经典许可证

保护

安全情报的要求和必备条件

型号支持

Any

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

重要事项 您必须在设备上应用网络发现策略，才能成功应用 SI 策略。

安全情报来源

- 系统-提供的源

  思科提供对定期更新的域名、URL 和 IP 地址的安全情报源的访问权限。有关详细信息，请参阅安全情报。

  如果您看到名称中包含“TID”的源，则表明安全情报不会使用此源。相反，此源由 Cisco Secure Firewall 威胁智能导向器 中所述的功能使用。

- 第三方源

  （可选）可以使用第三方信誉源（通常是 Cisco Secure Firewall Management Center定期从互联网下载的动态列表）补充思科提供的源。请参阅自定义安全情报源。

- 自定义阻止列表或源（或对象或组）

  使用手动创建的列表或源来阻止特定 IP 地址、URL 或域名（对于 IP 地址，您还可以使用网络对象或组）。

  例如，如果您发现尚未被源阻止的恶意站点或地址，请将这些站点添加到自定义安全情报列表中，并将此自定义列表添加到访问控制策略的“安全情报”(Security Intelligence) 选项卡中的“阻止”列表。如自定义安全情报列表和配置安全情报，第 4 页中所述。

  对于IP地址，您可以选择使用网络对象而不是列表或源；有关信息，请参阅网络。（对于URL，强烈建议使用列表和源，而非其他方法。）

- 自定义不阻止列表或源

  优先于特定站点或地址的安全智能阻止。请参阅覆盖安全情报阻止，第 11 页。

- 全局阻止列表（网络、URL 和 DNS 各一个）

  查看事件时，您可以立即将事件的IP地址、URL或域添加到适用的全局阻止列表，以便安全智能处理来自该源的未来流量。请参阅全局和域安全情报列表。

- 全局不阻止列表（网络、URL 和 DNS 各一个）

  在查看事件时，如果您不希望安全情报阻止来自该源的未来流量，则可以立即将事件的 IP 地址、URL 或域添加到适用的全局不阻止列表。请参阅全局和域安全情报列表。

配置安全情报

每个访问控制策略都具有安全情报选项。您可以将网络对象、URL 对象和列表以及安全情报源和列表列入阻止列表或不阻止列表，全部都可通过安全区域进行限制。您还可以将DNS策略与访问控制策略相关联，并将域名列入阻止列表或不阻止列表。

“不阻止列表”中的对象数加上“阻止列表”中的数量不能超过 125 个 网络对象或 32767 个 URL 对象和列表。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 提示：有关最低配置建议的指南，另请参阅 配置示例：安全情报阻止，第 9 页。
- 要确保所有选项可供选择，请向管理中心添加至少一个受管设备。
- 在被动部署中，或者如果要将安全情报过滤设置为仅监控，请启用日志记录；请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的使用安全情报记录连接。
- 配置 DNS 策略以对域执行安全情报操作。有关详细信息，请参阅DNS 策略。

过程

步骤 1 在访问控制策略编辑器中，点击 **安全情报**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 您有以下选择：

- 点击 **网络** 以添加网络对象（IP 地址）。

注释　安全情报策略中使用的网络对象需要 IPS 许可证。

- 点击 **URL** 以添加 URL 对象。

步骤 3 查找要添加到“阻止”或“不阻止”列表的 **可用对象** 。您有以下选择：

- 通过在**按名称或值搜索 (Search by name or value)** 字段中输入内容，搜索可用对象。通过点击 **重新加载** （ ） 或 **清除**（ ） 来清除搜索字符串。
- 如果现有列表或源不满足需求，请点击 **添加**（ ），选择 **新建网络列表** 或 **新建 URL 列表**，然后继续操作，如 创建安全情报源 或 将新的安全情报列表上传到 Cisco Secure Firewall Management Center中所述。
- 如果现有对象不满足需求，请点击 **添加**（ ），选择 **新建网络对象** 或**新建 URL 对象**，然后继续操作，如 创建网络对象中所述。

“安全智能”会忽略使用 `/0` 掩码的 IP 地址块。

步骤 4 在**可用对象**中选择一个或多个要添加的可用对象。

步骤 5 （可选）在**可用区域**中选择一个可用区域以按区域约束所选对象。

不能按区域限制系统提供的安全情报列表。

注释　SI的 **Any** 区域列表仅适用于属于安全区域的接口。但是，有一个例外是，如果设备没有与安全区域关联的任何接口，则 **Any** 区域将匹配任何接口。

例如，如果设备上有五个接口，但没有一个接口与安全区域相关联，则将根据设备上所有接口上的流量检查分配给 **Any** 区域的任何 SI 列表。如果将一个接口添加到该设备上的安全区域，它会有效地删除其他四个接口上的 SI 检查，其中 SI 列表的区域设置为 **Any** 。如果将其他四个接口添加到安全区域，它们将由附加到 **Any** 区域的 SI 列表进行评估。

步骤 6 点击 **添加到不阻止列表** 或 **添加到阻止列表**，或者点击所选对象并将其拖至任一列表。

要从阻止列表或不阻止列表中删除对象，请点击 **删除**（ ） 。要删除多个对象，请选择这些对象并右键点击 **删除所选项**。

步骤 7 （可选）通过右键点击**阻止列表**下的对象，然后选择**仅监控**（**不阻止**），将列入阻止列表的对象设置为仅监控。

不能将系统提供的全域安全情报列表设置为仅监控。

步骤 8 从 **DNS 策略 (DNS Policy)** 下拉列表中选择 DNS 策略。

步骤 9 点击**保存 (Save)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

相关主题

安全情报
Snort 重新启动场景

安全情报选项

使用访问控制策略编辑器中的“安全情报”(Security Intelligence) 选项卡配置网络（IP 地址）和 URL 安全情报，以及将访问控制策略与您在其中为域配置了安全智能的 DNS 策略相关联。

可用对象

可用对象包括：

- 由系统提供的源填充的安全情报类别。

  有关详细信息，请参阅安全情报类别，第 7 页。

- 由系统提供的全局阻止和不阻止列表。

  有关说明，请参阅安全情报来源，第 3 页。

- 在“对象”(Object) >“对象管理”(Object Management) >“安全情报”(Security Intelligence) 下创建的安全情报列表和源。

  有关说明，请参阅安全情报来源，第 3 页。

- 在“对象”(Object) >“对象管理”(Object Management) 下的相应页面上配置的网络和 URL 对象及组。这些对象与上一个项目符号中的安全情报对象有所不同。

  有关网络对象的详细信息，请参阅网络。（对于 URL，请使用安全情报列表或源，而不是对象或组。）

可用区

除系统提供的全局列表之外，您可以按照区域限制安全情报过滤。

例如：为了提高性能，您可能想要锁定执行目标。作为更具体的示例，您可以只阻止处理邮件流量的安全区域的垃圾邮件。

如要在多个区域上实施对象的安全情报过滤，对于每个区域，都必须将对象分别添加至阻止或不组织列表。

DNS 策略

要使用安全情报来匹配 DNS 流量，您必须为安全情报配置选择 DNS 策略。

使用阻止或不阻止列表，或者根据 DNS 列表或源来监控流量还要求您：

- 配置 DNS 安全情报列表和源。请参阅安全情报。
- 创建 DNS 策略。有关详细信息，请参阅创建基本 DNS 策略。
- 配置引用 DNS 列表或源的 DNS 规则。有关详细信息，请参阅创建和编辑 DNS 规则。

- 由于 DNS 策略部署为访问控制策略的一部分，因此必须将两个策略均进行关联。有关详细信息，请参阅DNS 策略部署。

不阻止列表

请参阅覆盖安全情报阻止，第 11 页。

要选择列表中的所有对象，请右键点击对象。

阻止列表

请参阅 配置示例：安全情报阻止，第 9 页 和本章中的其他主题。

有关阻止列表中的视觉指示的说明，请参阅阻止列表图标，第 9 页。

要选择列表中的所有对象，请右键点击对象。

日志记录

启用安全情报日志记录（默认情况下处于启用状态）会记录由访问控制策略的目标设备处理的所有受阻和受监控的连接。然而，系统不会记录不阻止列表匹配项；对不阻止列表上的连接的日志记录取决于其最终性质。必须首先为阻止列表中的连接启用日志记录，然后才能将该列表中的对象设置为仅监控。

要启用、禁用或查看日志记录设置，请右键点击阻止列表中的对象。

相关主题

全局和域安全情报列表
安全情报列表和多租户

安全情报类别

安全情报类别由 安全情报中所述的系统提供的源确定。

这些类别用于以下位置：

- 访问控制策略的“安全情报”选项卡上的“网络”子选项卡
- 访问控制策略的“安全情报”选项卡上“网络”选项卡旁边的 “URL” 子选项卡
- 在 DNS 策略配置页面的 DNS 选项卡上的 DNS 策略中
- 在流量与上述位置的阻止或监控配置匹配时生成的事件中

注释 如果您的组织使用 Cisco Secure Firewall 威胁智能导向器：查看事件时，您可能会看到指示 TID 已执行操作的类别，例如 `TID URL 阻止`。

类别由 Talos 从云更新，并且此列表可能会独立于 Firepower 版本进行更改。

表 *1:* 思科 ***Talos*** 情报小组 ***(Talos)*** 源类别

安全情报类别	说明
攻击者	出站恶意活动已知的活动扫描工具和主机
Banking_fraud	从事与电子银行相关的欺诈活动的网站
Bogon	Bogon 网络和未分配的 IP 地址
Bots	托管二进制恶意软件丢弃程序的站点
CnC	托管僵尸网络的命令和控制服务器的站点
加密货币挖矿活动	提供对用于挖掘加密货币的池和钱包的远程访问的主机
Dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法
Exploitkit	指定用于识别客户端中的软件漏洞的软件包
High_risk	根据来自安全图的 OpenDNS 预测安全算法进行匹配的域和主机名
IOC	观察到涉及感染指标 (IOC) 的主机
Link_sharing	未经许可共享版权文件的网站
恶意	表现出不一定属于另一种更精细的威胁类别的恶意行为的站点
恶意软件	托管恶意软件二进制或漏洞包的站点
Newly_seen	最近注册或尚未通过遥测发现的域。 **注意** 目前，此类别没有任何有效的源，已预留以供将来使用。
Open_proxy	允许匿名 Web 浏览的开放代理
Open_relay	已知用于垃圾邮件的开放邮件中继
网络钓鱼	托管网络钓鱼页面的站点
解决方案	主动参与恶意或可疑活动的 IP 地址和 URL
垃圾邮件	已知用于发送垃圾邮件的邮件主机
间谍软件	已知包含、提供或支持间谍软件和广告软件活动的网站
可疑	看似可疑并具有类似于已知恶意软件的特征的文件
Tor_exit_node	已知为 Tor Anonymizer 网络提供出口节点服务的主机

阻止列表图标

以下可视指示器可能会显示在访问控制策略的“安全情报”(Security Intelligence) 选项卡上的阻止列表中：

图标或可视指示灯	说明
阻止图标（  ）	对象被设为阻止。
监控（）	对象被设为仅监控。 请参阅 安全情报监控，第 10 页
对象以删除线文本显示	同一对象也位于不阻止列表中，该列表将覆盖该阻止。

配置示例：安全情报阻止

配置访问控制策略以阻止系统定期更新的安全情报源可检测到的所有威胁。

“阻止列表”中的对象数加上“不阻止列表”中的数量不能超过 125 个 网络对象或 32767 个 URL 对象和列表。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 要确保所有选项可供选择，请向管理中心添加至少一个受管设备。
- 配置 DNS 策略以阻止域的所有安全情报威胁类别。有关详细信息，请参阅DNS 策略。
- 如果您拥有或将要拥有要阻止的实体的自定义列表，请创建每种类型（URL，DNS，网络）的安全情报对象。请参阅安全情报。

过程

步骤 1 点击 **策略 (Policies) > 访问控制 (Access Control)**。

步骤 2 创建新的访问控制策略，或者编辑现有策略。

步骤 3 在访问控制策略编辑器中，点击 **安全情报**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 点击 **网络** 为 IP 地址添加阻止条件。

a) 在网络列表中向下滚动并选择全局列表下方列出的所有威胁类别。
b) 如果适用，请选择要阻止这些威胁的安全区域。
c) 点击 **添加到阻止列表**。
d) 如果您创建的自定义列表或源具有要阻止的地址，请使用与上述相同的步骤将这些地址添加到阻止列表。

步骤 5 点击 **URL** 以添加 URL 的阻止条件，然后重复您对网络执行的步骤。

步骤 6 从 **DNS 策略**下拉列表中选择 DNS 策略；请参阅DNS 策略概述。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 为这些连接启用日志记录；请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的使用安全情报记录连接。
- 部署配置更改；请参阅 部署配置更改。
- 要获得额外保护，请配置 URL 过滤以阻止恶意 URL。请参阅URL 过滤。

安全情报监控

监控会记录那些本应被安全智能阻止的流量的连接事件，但不会阻止流量。监控对于以下情况尤其有用：

- 在实施源之前对其进行测试。

  考虑一下这样的情况，在使用第三方源实施阻止之前，想要先对该源进行测试。将源设置为仅监控时，系统允许已被阻止的连接，以便系统能对其进行进一步的分析，但是也会记录这些连接中的每一个连接，以供进行评估。

- 被动部署，以优化性能。

  被动部署的受管设备无法影响流量；与将系统配置为阻止流量相比，没有任何优势。此外，因为阻止的连接实际上在被动部署中并未被阻止，因此，系统可能针对每条已阻止连接报告多个连接开始事件。

注释 如已配置，Cisco Secure Firewall 威胁智能导向器 可能会影响所采取的行动（监控或阻止）。有关详细信息，请参阅威胁智能导向器-管理中心 操作优先级。

要配置安全智能监控：

按照配置示例：安全情报阻止 ，第 9 页中的说明配置安全情报阻止后，右键点击阻止列表中的每个适用对象，然后选择**仅监控 (Monitor-only)**。 不能将系统提供的安全情报列表设置为仅监控。

覆盖安全情报阻止

或者，您可以使用“不阻止”列表来避免特定域、URL 或 IP 地址被安全智能列表或源阻止。

例如，您可以：

- 在信誉良好的安全智能源中覆盖偶尔的误报阻止
- 深入检查特定流量，而不是根据信誉来提前阻止流量
- 根据区域豁免其他受限事务的安全情报阻止

  例如，您可以将分类不当的URL加入“不阻止”列表中，但随后使用您的组织中需要访问这些 URL 的人员所使用的安全区域来限制“不阻止”列表对象。这样，只有有业务需要的人员才能访问“不阻止”列表中的 URL。

注释 “不阻止”列表中的条目只是阻止列表中的例外项。通过安全情报策略的任何连接都受访问控制规则的约束。因此，访问控制规则或入侵策略随后可以阻止“不阻止”列表中的条目。您的“不阻止”条目应始终是阻止列表的例外项。

过程

步骤 1 选项 1：将事件中的 IP 地址、URL 或域添加到“全局不阻止列表”。请参阅全局和域安全情报列表。

步骤 2 选项 2：使用自定义安全智能列表或源。

a) 创建自定义安全智能列表或源。请参阅自定义安全情报列表或创建安全情报源。

b) 对于 IP 地址（网络）和 URL：编辑访问控制策略，点击“安全智能”(Security Intelligence)选项卡，然后点击“网络”(Networks) 或“URLs”子选项卡中的自定义列表或源，然后点击**添加到不阻止列表 (Add to Do Not Block List)**。

c) 保存更改。

d) 对于域 (DNS)：请参阅安全情报选项，第 6 页主题中的“DNS 策略”部分。

e) 部署更改。

安全情报故障排除

请参阅以下有关安全情报故障排除的主题。

可用选项列表中缺少安全情报类别

症状：在访问控制策略的“安全情报”(Security Intelligence) 选项卡上，“可用选项”(Available Options) 下的“网络”(Networks) 选项卡中不会显示安全情报类别（例如 CnC 或漏洞攻击包）。

原因：

- 在管理中心至少添加一个托管设备之前，这些类别不会显示。您必须添加一个设备才能提取所有 TALOS 源。
- URL 过滤功能使用的类别集与安全情报功能有所不同；；您期望看到的类别可能是 URL 过滤类别。要查看 URL 过滤类别，请查看访问控制规则中的 **URLs** 选项卡。

安全情报阻止列表的历史记录

特性	Version	最低 威胁防御	详细信息
新的安全情报类别	全部	任意	Talos 添加了以下新的安全情报类别： • banking_fraud • ioc • high_risk • link_sharing • 广告的 • newly_seen • 间谍软件 您应更新访问控制和 DNS 策略以应对新类别，并定期检查将来的更改。 新增/修改的页面：安全情报选项卡、网络和 URL 子选项卡； DNS 策略中的 DNS 规则 支持的平台： 管理中心

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。