含警报响应的外部警报

以下主题介绍如何使用警报响应从 Cisco Secure Firewall Management Center发送外部事件警报：

Cisco Secure Firewall Management Center 警报响应

通过 SNMP、系统日志或邮件发送外部事件通知有助于重要系统监控。Cisco Secure Firewall Management Center使用可配置的警报响应与外部服务器交互。警报响应是一种配置，用于表示与电子邮件、SNMP或系统日志服务器的连接。它们称为响应的原因在于，可将它们用于发送警报，以响应由Cisco Secure Firewall检测到的事件。可以配置多个警报响应，以便向不同的监控服务器和/或人员发送不同类型的警报。

注释 根据您的设备和 Cisco Secure Firewall 版本，警报响应可能不是发送系统日志消息的最佳方式。请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的关于系统日志一章和配置安全事件系统日志消息的最佳实践。。

注释 使用警报响应的警报是由 Cisco Secure Firewall Management Center发送的。不使用警报响应的入侵电子邮件警报也是由 Cisco Secure Firewall Management Center发送的。相比之下，基于单个入侵规则触发的 SNMP 和 系统日志警报是由托管设备直接发送的。有关详细信息，请参阅入侵事件的外部警报。

在大多数情况下，外部警报中的信息与您记录到数据库中的任何相关联事件中的信息相同。但是，无论是何种基础事件类型，对于关联规则中包含连接跟踪器的关联事件警报，您收到的信息都与流量量变曲线更改警报相同。

可在“警报”页面（**策略措施** > **行动** > **警报**）上创建和管理警报响应。新的警报响应自动启用。要暂停警报生成，可以禁用警报响应，而非将它们删除。

对警报响应所做的更改会立即生效，但将连接日志发送到 SNMP 陷阱或系统日志服务器时除外。

支持警报响应的配置

创建警报响应后，可以使用它从 Cisco Secure Firewall Management Center发送以下外部警报。

警报/事件类型	了解更多信息
按影响标志划分的入侵事件	配置影响标志警报， 第 8 页
按类型划分的发现事件	配置发现事件警报， 第 9 页
由 恶意软件防护 检测到的恶意软件和追溯性恶意软件事件（“基于网络”）	配置 恶意软件防护警报， 第 9 页
按关联策略违规划分的关联事件	将响应添加到规则和允许名单
按日志记录规则或默认操作（不支持邮件警报）划分的连接事件	您可以记录的其他连接
按运行状况模块和严重性级别划分的运行状况事件	创建运行状况监控警报

警报报告的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员

创建 SNMP 警报响应

可使用 SNMPv1、SNMPv2 或 SNMPv3 为 设备创建 SNMP 警报响应。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

如果想要使用 SNMP 监控 64 位值，则必须使用 SNMPv2 或 SNMPv3。SNMPv1 不支持 64 位监控。

开始之前

- 如果网络管理系统需要 防火墙管理中心的管理信息库 (MIB) 文件，则可在 `/etc/sf/DCEALERT.MIB` 处获取该文件。

过程

步骤 1 选择**策略措施** > **行动** > **警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建 SNMP 警报 (Create SNMP Alert)**。

步骤 3 编辑 SNMP 警报配置字段：

a) **名称**-输入名称以指定 SNMP 响应。

b) **陷阱服务器**-输入 SNMP 陷阱服务器的主机名或 IP 地址。

注释
如果在此字段中输入了无效的 IPv4 地址（例如 192.169.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

c) **版本**-从下拉列表中，选择要使用的 SNMP 版本。SNMPv3 是默认设置。

选项包括：

- **SNMPv1** 或 **SNMPv2**：在 **社区字符串** 字段中输入只读 SNMP 社区名称，然后跳至程序末尾。

  注释
  不包含特殊字符 (< > / % # & ? ' 等）在 SNMP 社区字符串名称中。

- 对于 **SNMP v3**：在 **用户名** 字段中，输入要使用 SNMP 服务器对其进行身份验证的用户的名称并继续下一步。

d) **身份验证协议**-从下拉列表中选择要用于身份验证的协议。

选项包括：

- **MD5**- 消息摘要 5 (MD5) 散列功能。

- **SHA**—安全散列算法 (SHA) 散列函数。

e) **身份验证密码**-输入用于身份验证的密码。

f) **隐私协议**－从下拉列表中选择要用于加密私有密码的协议。

选项包括：

- **DES**-在对称密钥块算法中使用 56 位密钥的数据加密标准 (DES)。
- **AES**-在对称密码算法中使用 56 位密钥的高级加密标准 (AES)。
- **AES128**-在对称密码算法中使用 128 位密钥的 AES。密钥越长，其提供的安全性就越高，但性能会随之降低。

g) **隐私密码**-输入 SNMP 服务器所需的隐私密码。如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。

h) **引擎 ID**-使用偶数数字（十六进制表示法）输入 SNMP 引擎的标识符。

使用 SNMPv3 时，系统使用引擎 ID 值对消息进行编码。SNMP 服务器需要使用该值对消息进行解码。

思科建议您使用十六进制版本的 防火墙管理中心的 IP 地址。例如，如果 防火墙管理中心 的 IP 地址为 10.1.1.77，请使用 0a01014D0。

步骤 4 点击**保存**。

下一步做什么

更改会立即生效，但如果使用警报响应发送连接日志，则必须在编辑这些警报响应后部署配置更改。

创建系统日志警报响应

配置系统警报响应时，可指定与系统日志消息相关联的严重性和消息来源，以确保它们得到系统日志服务器的正确处理。消息来源指明创建消息的子系统，严重性界定消息的严重性。消息来源和严重性不显示在系统日志中的实际消息中，而是告知接收系统日志消息的系统如何对消息进行归类。这些字段允许您设置从 管理中心 Web接口配置的系统日志事件中的严重性和工具，但这些字段不能用于过滤事件类型。

提示 有关系统日志如何运行及如何对其进行配置的更多详细信息，请参阅系统文档。在 UNIX 系统上，`syslog` 和 `syslog.conf` 的 `man` 页面提供了概念信息和配置说明。

虽然在创建系统日志警报响应时可选择任何类型的设施，但是应根据系统日志服务器选择合适的设施；并非所有系统日志服务器都支持所有设施。对于 UNIX 系统日志服务器，`syslog.conf` 文件应指示哪些设备保存到了服务器的哪些日志文件上。

系统日志信息通过 UDP 或 TCP 传输，具体取决于系统日志服务器的配置。

开始之前

- 在许多情况下，不建议使用此程序发送系统日志消息。
- 确认系统日志服务器可接受远程消息。

过程

步骤 1 选择**策略措施** > **行动** > **警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建系统日志警报 (Create Syslog Alert)**。

步骤 3 输入警报的**名称 (Name)**。

步骤 4 在**主机 (Host)** 字段中，输入系统日志服务器的主机名或 IP 地址。

注释
如在此字段中输入了无效的 IPv4 地址（例如 192.168.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

步骤 5 在**端口 (Port)** 字段中，输入服务器用于系统日志消息的端口。默认情况下，此值为 514。

步骤 6 从**设施 (Facility)** 列表中，选择系统日志警报设施，第 5 页中所述的设施。

步骤 7 从**严重性 (Severity)** 列表中，选择系统日志严重性级别，第 6 页中所述的严重性。

步骤 8 在**标记 (Tag)** 字段中，输入要与系统日志消息一起显示的标记名称。

例如，如果要在发送到系统日志的所有消息前加上 `FromMC`，请在字段中输入 `FromMC`。

步骤 9 点击**保存**。

下一步做什么

更改会立即生效，但以下情况除外：

如果你使用警报响应来发送连接日志到系统日志服务器，你必须在编辑这些警报响应后部署配置更改。

如果您将此警报响应用于安全事件，则必须在策略中指定此警报响应。请参阅安全事件系统日志的配置位置。

系统日志警报设施

下表列出了可选择的系统日志设施。

表 *1:* 可用的系统日志设施

设施	说明
AUTH	与安全和授权关联的消息。

设施	说明
AUTHPRIV	与安全和授权关联的访问受限的消息。在很多系统上，这些消息会转发至一个安全文件。
控制台	警报消息。
CRON	时钟后台守护程序生成的消息。 请注意，运行 Linux 操作系统的系统日志服务器将使用 CRON 消息来源。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
邮件	邮件系统生成的消息。
NEWS	网络新闻子系统生成的消息。
NTP	NTP 后台守护程序生成的消息。
安全	审核子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
SOLARIS-CRON	时钟后台守护程序生成的消息。 请注意，运行 Windows 操作系统的系统日志服务器将使用 CLOCK 消息来源。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志严重性级别

下表列出可选择的标准系统日志严重性级别。

表 *2:* 系统日志严重性级别

级别	说明
ALERT	应立即更正的状况。
CRIT	严重的状况。

级别	说明
DEBUG	包含调试信息的消息。
EMERG	向所有用户广播的紧急状况。
ERR	错误状况。
INFO	参考性消息。
通知	需要注意但非错误的状况。
警告	警告消息。

创建邮件警报响应

开始之前

- 确保 Cisco Secure Firewall Management Center 可以反转解析自己的 IP 地址。某些邮件服务器可能会执行反向 DNS 查找来验证发件人的身份，以此作为防止垃圾邮件和未经授权访问的一项措施。
- 配置邮件中继主机，如配置邮件中继主机和通知地址中所述。

注释 不可以使用邮件警报记录连接。

过程

步骤 1 选择**策略措施** > **行动** > **警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建邮件警报 (Create Email Alert)**。

步骤 3 为警报响应输入**名称 (Name)**。

步骤 4 在**收件人 (To)** 字段中，输入要将警报发送到其中的邮箱地址（用逗号分隔）。

步骤 5 在**发件人 (From)** 字段中，输入要显示为警报发件人的邮箱地址。

步骤 6 在 **Relay Host** 旁，验证列出的邮件服务器是要用于发送警报的服务器。

提示
要更改电邮服务器，请点击 **编辑** ()。

步骤 7 点击**保存**。

创建 Webhook 警报响应

防火墙管理中心 支持 Webhook 警报配置，允许您将 防火墙管理中心 警报与可以接收和处理 Webhook 负载的外部系统或自定义应用集成。

开始之前

- 确保 防火墙管理中心 与 Webhook 终端有网络连接。
- 如果计划使用 TLS 身份验证，请确保有必要的 CA 证书、客户端证书和客户端密钥文件可供上传。

过程

步骤 1 选择**策略** > **警报**。

步骤 2 从**创建警报**下拉菜单中，选择**创建 Webhook 警报**。

步骤 3 在**名称**字段中，为 Webhook 警报响应输入描述性名称。

步骤 4 在 **URL** 字段中，输入 Webhook 终端的 URL。

步骤 5 从“TLS 类型”下拉列表中，选择 TLS 身份验证类型。您有这些选择：

- **客户端**：选择此选项配置单向 TLS 身份验证。上传 CA 证书，供客户端验证服务器的真实性。
- **双向**：选择此选项配置双向 TLS 身份验证。上传 CA 证书、客户端证书和客户端证书密钥，供客户端和服务器相互身份验证。
- **无**：选择此选项不配置 TLS 身份验证。

步骤 6 如果使用 TLS 身份验证，请指定与 Webhook 终端身份验证所需的凭据。

步骤 7 （可选）点击**测试连接**以验证与 Webhook 终端的连接和身份验证。

步骤 8 点击**保存**。

配置影响标志警报

可将系统配置为只要出现带有特定影响标志的入侵事件就会发出警报。影响标志可通过将入侵数据、网络发现数据和漏洞信息相关联来帮助评估入侵对网络的影响。

您必须具有 IPS 智能许可证才能配置这些警报。

过程

步骤 1 选择**策略措施** > **行动** > **警报**。

步骤 2 点击 **影响标志警报**。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示
要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**影响配置 (Impact Configuration)** 部分中，选中相应复选框为每个影响标志指定要接收的警报。

有关影响标志的定义，请参阅入侵事件影响级别。

步骤 5 点击**保存**。

配置发现事件警报

可将系统配置为只要出现特定类型的发现事件就会发出警报。

开始之前

- 将网络发现策略配置为记录要为其配置警报的发现事件类型，如 《Cisco Secure Firewall Management Center 设备配置指南》中 网络发现策略 中所述

过程

步骤 1 选择**策略措施** > **行动** > **警报**。

步骤 2 点击 **发现事件警报 (Discovery Event Alerts)**。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示
要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**事件配置 (Events Configuration)** 部分中，选中与要为每种发现事件类型接收的警报对应的复选框。

步骤 5 点击**保存**。

配置 恶意软件防护警报

可将系统配置为只要恶意软件防护生成任何恶意软件事件（包括回溯性事件）（即，生成“基于网络的恶意软件事件”），就向您发出警报。无法对 Cisco Secure Endpoint 生成的恶意软件事件（“基于终端的恶意软件事件”）发出警报。

开始之前

- 配置文件策略以执行恶意软件云查找并将该策略与访问控制规则相关联，。 有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的访问控制概述。
- 您必须具有 恶意软件防御 许可证才能配置这些警报。

过程

步骤 1 选择**策略措施** > **行动** > **警报**。

步骤 2 点击 **高级恶意软件防护警报**。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示
要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**事件配置 (Event Configuration)** 部分中，选中与要为每种恶意软件事件类型接收的警报对应的复选框。

请注意，**所有基于网络的恶意软件事件 (All network-based malware events)** 包括**追溯性事件 (Retrospective Events)**。

（根据定义，基于网络的恶意软件事件不包括 Cisco Secure Endpoint 生成的事件。）

步骤 5 点击**保存**。

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。