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 Secure Firewall Management Center发送外部事件警报：

使用告警响应配置外部告警

警报响应是一种配置，用于定义与外部服务器或服务（如邮件服务器、简单网络管理协议 (SNMP) 服务器、系统日志服务器或 Webhook 端点）的连接。通过防火墙管理中心中的警报响应，您可以将防火墙管理中心中的安全事件通知发送到外部监控服务器或指定收件人。这些配置被称为“响应”，因为它们是根据 Firewall Threat Defense 设备检测到的事件来发送告警。

告警响应配置流程

要从防火墙管理中心发送外部警报，请执行以下操作：

1. 为支持的协议（SNMP、系统日志、邮件、Webhook）创建警报响应。指定所需参数，如服务器地址、端口、凭证和消息格式。
2. 将警报响应分配给特定警报类型或事件类别，以便根据事件特征发送警报。

您可以配置多个警报响应，向不同的监控服务器和/或人员（收件人）发送不同类型的警报。

防火墙管理中心 使用告警响应将告警发送至外部系统。相比之下，由单独入侵规则触发的 SNMP 和系统日志告警由被管设备直接发送。有关详细信息，请参阅入侵事件的外部警报。 防火墙管理中心也会发送入侵电子邮件告警，其不使用告警响应。

外部告警类型

创建告警响应后，您可以使用它从防火墙管理中心发送外部告警。

表 *1:* 支持警报响应的外部警报配置

事件和警报类型	有关详细信息，请参阅
按影响标志划分的入侵事件	配置影响标志警报，第 9 页
按类型划分的发现事件	配置发现事件警报，第 10 页
由 恶意软件防御 检测到的恶意软件和追溯性恶意软件事件（“基于网络”）	配置恶意软件防护告警，第 10 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

带警报响应的外部警报的前提条件

在 防火墙管理中心 中创建具有警报响应的外部警报之前，请确保您满足这些要求。

型号支持

任意

支持的域

任意

用户角色

- 管理员

向外部系统通知响应警报响应的准则

遵循以下关于通知外部系统警报响应的准则。

- 根据您的 Firewall Threat Defense 版本和设备型号，警报响应可能不是发送系统日志消息的最佳方式。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 设备配置指南和配置安全事件系统日志消息的最佳实践中的关于系统日志。

- 创建新警报响应时，它将自动启用。如果要暂时停止生成警报，请禁用警报响应而不是删除它。
- 修改警报响应时，更改会立即生效。但是，如果您使用警报响应来将连接日志发送到 SNMP 陷阱或系统日志服务器，请部署配置以确保应用您的更改。

警报响应

使用服务器地址、端口、凭证和消息格式等所需参数，为支持的协议（SNMP、系统日志、邮件和 Webhook）创建警报响应。

创建 SNMP 警报响应

使用 SNMP 版本 SNMPv1、SNMPv2 或 SNMPv3 在 防火墙管理中心 中配置 SNMP 警报响应，以监控网络事件。

注释 为 SNMP 协议选择 SNMP 版本时，请注意：

- SNMP 警报响应的推荐版本是 SNMPv3，因为它支持高级加密。
- SNMPv2 仅支持只读社区。SNMPv3 仅支持只读用户并提供 AES128 加密。
- 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。

Before you begin

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**管理** > **警报**。

步骤 2 从**创建警报**下拉列表中，选择**创建 SNMP 警报**。

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。

注意
如果在此字段中输入了无效的 IPv4 地址（例如 192.169.1.456），则 防火墙管理中心 不会发出警告。相反，防火墙管理中心 会将无效地址视为主机名。

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

这些协议可用：

- **SNMPv1** 或 **SNMPv2**：在**社区字符串**字段中输入只读 SNMP 社区名称，然后跳到此任务的最后一步。

  注释
  此字段允许的字符包括字母数字字符、下划线 (_)、连字符 (-)、星号 (+) 和美元符号 ($)。允许的最大长度为 128 个字符。

- 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。指定私有密码可以保护隐私，但同时也需要指定身份验证密码。

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。

我们建议您使用十六进制版本的 防火墙管理中心 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

如果您使用 SNMP 警报响应将连接日志发送到 SNMP 陷阱服务器，则在修改 SNMP 警报响应后，必须部署配置更改。

系统日志警报响应

系统日志警报响应是与外部系统日志服务器建立连接。它使您能够发送由防火墙管理中心检测到的各种事件触发的警报。

有关系统日志和配置步骤的详细信息，请参阅系统文档。如果您使用 UNIX，请查看 **syslog** 和 **syslog.conf** 的 **man** 页面以了解概念和配置信息。

设施和严重性

配置系统警报响应时，可指定与系统日志消息相关联的设施和严重性，以确保它们得到系统日志服务器的正确处理：

- 设施指定创建系统日志消息的子系统。严重性定义了系统日志消息的严重性。
- 实际系统日志消息不会显示设施和严重性。接收系统日志消息的系统会使用这些值对消息进行分类。
- 创建系统日志警报响应时，可以选择任何类型的设施。但是，您应选择与系统日志服务器兼容的设施，因为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** 文件应指示哪些设施保存到了服务器的哪些日志文件上。

注释 系统日志消息中的设施和严重性值不用于过滤事件类型。

系统日志告警设施

此表列出您可选择的系统日志工具。

表 *2:* 系统日志工具

设施	说明
AUTH	与安全和授权关联的消息。
AUTHPRIV	与安全和授权关联的受限访问消息。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	由时钟后台守护程序生成的消息。 运行 Linux 操作系统的系统日志服务器使用 **CRON** 工具。
DAEMON	由系统后台守护程序生成的消息。
FTP	由文件传输协议 (FTP) 后台守护程序生成的消息。
KERN	内核生成的消息。在许多系统中，这些消息出现时会传送至控制台进行打印。
LOCAL0-LOCAL7	内部进程生成的消息。

设施	说明
LPR	打印子系统生成的消息。
邮件	由邮件系统生成的消息。
NEWS	由网络新闻子系统生成的消息。
NTP	由网络时间协议 (NTP) 后台守护程序生成的消息。
安全	审核子系统生成的消息。
SOLARIS-CRON	由时钟后台守护程序生成的消息。 运行 Windows 操作系统的系统日志服务器使用 **CLOCK** 工具。
SYSLOG	系统日志后台守护程序生成的消息。
用户	用户级进程生成的消息。
UUCP	Unix 到 Unix 复制程序 (UUCP) 子系统生成的消息。

系统日志严重性级别

此表列出可供选择的标准系统日志严重级别。

表 *3:* 系统日志严重性级别

严重性级别	说明
ALERT	应立即更正的状况。
CRIT	严重的状况。
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。
信息	参考性消息。
通知	需要注意但非错误的状况。
警告	警告消息

创建系统日志警报响应

创建系统日志警报响应以连接到外部系统日志服务器。这使您能够将事件警报发送到具有可自定义严重性和设备设置的外部系统日志服务器。

在许多情况下，不建议使用此程序发送系统日志消息。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 设备配置指南

Before you begin

确认系统日志服务器可接受远程消息。

过程

步骤 1 选择**管理** > **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**。

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
如果输入无效的 IPv4 地址（例如 192.168.1.456），防火墙管理中心会将其视为主机名且不显示警告。

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**列表中，选择设备。有关详细信息，请参阅系统日志告警设施，第 5 页。

步骤 7 从**严重性**列表中，选择严重性。有关详细信息，请参阅系统日志严重性级别，第 6 页。

步骤 8 在**标记**字段中，输入要随系统日志消息一起显示的标记名称。

例如，如果您希望发送到系统日志的所有消息前都带有“FromMC”，请在该字段中输入“FromMC”。

步骤 9 点击**保存**。

下一步做什么

- 如果您使用系统日志警报响应将连接日志发送到系统日志服务器，则必须在修改这些警报响应后部署配置更改。
- 要在安全事件中使用系统日志告警响应，必须在策略中指定告警响应，并为安全事件系统日志配置位置。有关详细信息，请参阅安全事件系统日志的配置位置。

创建邮件警报响应

邮件警报响应配置使您可以通过配置的邮件中继主机发送有关严重系统事件的邮件警报。

Before you begin

- 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。

- 确保 防火墙管理中心 可以反转解析自己的 IP 地址。有些电子邮件服务器使用反向 DNS 查询来确认发件人身份，防止垃圾邮件和未经授权的访问。

按照以下步骤创建电子邮件警报响应：

过程

步骤 1 选择**管理** > **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**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**字段中，输入要显示为警报发件人的邮箱地址。

步骤 6 在**中继主机**旁边，验证列出的邮件服务器是否是要用于发送警报的服务器。

如果要更改电邮服务器，请点击 **编辑** ()。

步骤 7 点击**保存**。

创建 Webhook 警报响应

webhook 警报响应配置允许您向可以接收和处理 webhook 有效负载的外部监控系统或自定义应用程序发送 防火墙管理中心 警报。

Before you begin

- 确保 防火墙管理中心 与 Webhook 终端有网络连接。
- 要使用 TLS 身份验证，请确保您拥有所需的 CA 证书、客户端证书和客户端密钥文件以供上传。

过程

步骤 1 选择**管理** > **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。

如果您输入相对 URL，防火墙管理中心 将根据您在下一步中选择的 TLS 类型自动添加前缀 **`http://`** 或 **`https://`**。

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 CLIENT 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、CLIENT 证书和客户端证书密钥，供 CLIENT 和服务器相互身份验证。
- **无**：如果您不想配置 TLS 身份验证，请选择此选项。

步骤 6 如果使用 TLS 身份验证，请输入与 Webhook 终端身份验证所需的凭据。

步骤 7 （可选）点击**测试连接**，验证您的 Webhook 终端是否可访问且身份验证是否成功。此测试仅验证连接和身份验证。它不会测试向 Webhook 终端发送警报的能力。

步骤 8 点击**保存**。

外部警报

防火墙管理中心支持通过其警报响应功能向各类外部系统发送外部警报。将警报响应分配到特定警报类型/事件类别（如入侵影响标记、发现事件、恶意软件检出）。这种分配可确保确保按事件特征将相关警报发送到对应的外部系统

配置影响标志警报

通过配置影响标志警报，您可以在网络中检测到具有特定影响标志的入侵事件时接收通知。

影响标志通过关联入侵数据、网络发现数据和漏洞信息，帮助您评估入侵对网络造成的影响。防火墙管理中心提供了为不同影响类型选择警报响应的选项，您还可以自定义哪些影响标志会触发警报。

有关影响标志的详细信息，请参阅入侵事件影响级别。

Before you begin

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**管理** > **警报**。

步骤 2 点击 **影响标志警报**。

步骤 3 在**警报**部分中，选择要用于影响标志警报的警报响应。

要创建新警报响应，请从下拉列表中选择**新建**。

步骤 4 在**影响标志配置**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。

选中通知名称旁的复选框，以选择所有影响标志。

步骤 5 点击**保存**。

配置发现事件警报

通过配置发现事件警报，您可在网络中发生特定类型的发现事件时收到通知。防火墙管理中心提供了为不同发现事件类型选择警报响应的选项，您可以自定义触发警报的发现事件。

Before you begin

配置网络发现策略，记录您希望接收警报的发现事件类型。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 设备配置指南中的“网络发现策略”章节。

过程

步骤 1 选择**管理** > **警报**。

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

步骤 3 在**警报**部分中，选择要用于发现事件警报的警报响应。

要创建新警报响应，请从下拉列表中选择**新建**。

步骤 4 在**事件配置**部分中，选中与您希望接收警报的发现事件类型对应的复选框。

提示
选中通知名称旁的复选框，可选择所有发现事件类型。

步骤 5 点击**保存**。

配置恶意软件防护告警

配置恶意软件防护警报后，当恶意软件防护（基于网络的恶意软件事件）生成任何恶意软件事件（包括追溯性事件）时，您将收到通知。您无法对Secure Endpoint生成的恶意软件事件（基于终端的恶意软件事件）接收警报。

Before you begin

- 您必须具有恶意软件防御许可证才能配置恶意软件防护警报。
- 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。

过程

步骤 1 选择**管理** > **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。

要创建新警报响应，请从下拉列表中选择**新建**。

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由Secure Endpoint生成的事件。

步骤 5 点击**保存**。

外部警报与警报响应配置故障排除

当外部通知未按预期工作时，使用这些故障排除步骤在防火墙管理中心中执行外部警报和警报响应配置。

警报不是从 防火墙管理中心 发送的

1. 验证警报响应是否已在**警报**页面 (**管理** > **警报**) 中启用，并且正确链接到相关策略或事件类型。
2. 检查 SNMP 陷阱服务器、系统日志服务器、邮件地址或 Webhook URL 是否准确。
3. 确保在进行更改后部署配置。

连接日志不会发送到系统日志服务器。

1. 通过将访问控制策略配置为包含日志记录选项并选择适当的系统日志服务器，确保启用将连接日志转发到远程系统日志服务器。有关详细信息，请参阅使用访问控制规则记录连接。
2. 如果在编辑警报响应和访问控制规则后未部署配置更改，则连接日志可能不会发送到系统日志服务器。保存并部署所有更改，以应用更新的设置。

未传送或邮件服务器拒绝了邮件警报

邮件警报可能会因邮件服务器策略或反向 DNS 查找失败而被拒绝。

1. 验证邮件中继主机配置。有关详细信息，请参阅配置邮件中继主机和通知地址。

   您还可以从 防火墙管理中心 CLI 检查邮件中继主机配置的错误消息。导航至 **expert**，然后输入命令 **cat /var/log/messages | grep -i "email\|smtp"** 以查看邮件中继主机配置错误消息：

   ```
   > expert
   admin@firepower:~$ cat /var/log/messages | grep -i "email\|smtp"
   Oct 16 17:57:38 firepower msmtp: host=example.host.com tls=on auth=off
   from=alertfmc760@****.com recipients=example@org.com mailsize=286 smtpstatus=250
   smtpmsg='250 2.0.0 Ok: queued as ****' exitcode=EX_OK
   ```

2. 验证您的 DNS 服务器是否可访问，以及它们是否可以解析邮件中继主机名：

   ```
   admin@firepower:~$ ping example.host.com
   ping: example.host.com: Name or service not known
   ```

3. 验证 防火墙管理中心 可以反转解析自己的 IP 地址。

Webhook 警报响应连接测试失败

1. 验证从 防火墙管理中心 到 Webhook 终端的网络连接。
2. 确认 TLS 身份验证设置和证书（CA、客户端证书、客户端密钥）已正确上传且有效。
3. 在 防火墙管理中心 中，点击 **管理** > **警报**，编辑 Webhook 警报响应，并使用**测试连接**选项验证连接和身份验证。

带警报响应的外部警报历史记录

下表总结了 Cisco Secure Firewall Management Center 各版本中警报响应的外部警报介绍和发展情况。

表 *4:* 功能历史记录

功能	防火墙管理中心最低版本 版本	**Firewall Threat Defense**最低版本 版本	详细信息
创建 Webhook 警报响应。	7.7.0	任意	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。 新增/修改的屏幕：选择**管理**>**警报**，然后从**创建警报**下拉菜单中选择**创建 Webhook 警报**。
将有关安全事件的警报从 防火墙管理中心 发送到外部监控服务器。	6.4.0	任意	此版本引入了警报响应配置和外部警报功能，使 防火墙管理中心 能够向外部监控系统发送警报。发生特定事件时，可以将警报响应配置为通过邮件、系统日志或SNMP发送通知。这些警报选项允许与监控和管理工具集成，以便及时获得外部通知。 新增/修改的屏幕：选择**管理** > **警报**。

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。

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。

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。

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。