平台设置

威胁防御 设备的平台设置用于配置您可能希望在多台设备之间共享其值的一系列无关功能。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

平台设置简介

平台设置策略是用于定义受管设备的可能类似于您的部署中其他受管设备的方面（例如时间设置和外部身份验证）的共享功能集或参数集。

通过共享策略，可以同时配置多个受管设备，从而在部署中提供一致性并精简管理工作。对平台设置策略的任何更改都会影响已应用该策略的所有受管设备。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

例如，您的组织的安全策略可能会要求您的设备在用户登录时显示“无授权使用”(No Unauthorized Use) 消息。通过平台设置，您可以在平台设置策略中设置一次登录横幅。

在单一管理中心上具有多个平台设置策略也有好处。例如，如果您具有在不同情况下使用的不同邮件中继主机，或者如果要测试不同的访问列表，则可以创建多个平台设置策略并在其之间切换，而非编辑单个策略。

平台设置策略的要求和必备条件

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

管理平台设置策略

使用“平台设置”页面（**设备** > **平台设置**）管理平台设置策略。此页面指示每个策略的设备类型。“状态”(Status) 列显示策略的设备目标。

过程

步骤 1 选择**设备** > **平台设置**。

步骤 2 对于现有策略，您可以**复制**（）、**编辑**（）或**删除**（）策略。

注意 不应删除上一次部署于任何目标设备的策略，即使该策略已过时。在完全删除该策略之前，最好是将其他策略部署到这些目标。

步骤 3 要创建新策略，请点击**新建策略 (New Policy)**。

a) 从下拉列表中选择设备类型。

- **Firepower 设置** 为典型托管设备创建共享策略。
- **威胁防御设置** 以创建 威胁防御 托管设备的共享策略。

b) 为新策略输入**名称 (Name)** 和**说明 (Description)**（可选）。

c) 或者，选择要应用策略的**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)**（或拖放）以添加所选设备。可以在**搜索 (Search)** 字段中输入搜索字符串以缩小设备列表。

d) 点击**保存**。

系统创建策略，并打开以进行编辑。

步骤 4 要更改策略的目标设备，请点击要编辑的平台设置策略旁边的 **编辑**（ ） 图标。

a) 点击**策略分配 (Policy Assignment)**。
b) 要将设备、高可用性对或设备组分配给策略，请在**可用设备 (Available Devices)** 列表中将其选中，然后点击**添加到策略 (Add toPolicy)**。还可以进行拖放。
c) 要删除设备分配，请点击**所选设备 (Selected Devices)** 列表中的设备、高可用性对或设备组旁边的 **删除**（ ）。
d) 点击**确定 (OK)**。

下一步做什么

- 部署配置更改。

配置 ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP 检测可防止恶意用户模拟其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

当启用 ARP 检测查时，威胁防御设备 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 威胁防御设备 会丢弃数据包。
- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 威胁防御设备 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。

注释 即使此参数设置为 flood，专用诊断接口也绝不会以泛洪方式传输数据包。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**ARP 检测**。

步骤 3 将条目添加到 ARP 检查表。

a) 点击**添加**以创建新条目，如果该条目已存在，则点击**编辑**。

b) 选择所需的选项。

- **已启用检查** - 对选定接口和区域执行 ARP 检查。
- **已启用洪流** - 是否将不匹配静态 ARP 条目的 ARP 请求以洪流形式自除原始接口或专用管理接口以外的所有接口发出。此为默认行为。

  如果您不选择以洪流形式发出 ARP 请求，则只允许与静态 ARP 条目完全匹配的请求。
- **安全区域** - 添加包含要在其上执行所选操作的接口的区域。区域必须为交换区域。对于不在区域中的接口，您可以在“所选安全区域”列表下方的字段中键入接口名称，然后点击**添加 (Add)**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 4 根据添加静态 ARP 条目中所述添加静态 ARP 条目。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置横幅

您可以将消息配置为在用户连接到设备命令行界面 (CLI) 时显示这些用户。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**横幅**。

步骤 3 配置横幅。

下面是关于横幅的几点提示和要求。

- 只允许使用 ASCII 字符。您可以使用换行符（按 Enter），但不能使用制表符。
- 通过包含变量 **$(hostname)** 或 **$(domain)**，可以动态添加设备的主机名或域名。
- 虽然横幅上没有绝对长度限制，但如果没有足够的系统内存来处理横幅消息，则 Telnet 或 SSH 会话将关闭。
- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用“欢迎”或“请”等措辞，因为它们像是在邀请入侵者。以下横幅为未经授权的访问设置正确的语调：

```
You have logged in to a secure device.
```

```
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。有两种适用于不同类型流量的 DNS 服务器设置：数据流量和特殊管理流量。数据流量包括使用需要进行 DNS 查找的 FQDN 的任何服务，例如访问控制规则和远程访问 VPN。特殊管理流量包括管理接口上发出的流量，例如配置和数据库更新。此程序仅适用于 数据 DNS 服务器。有关 管理 DNS 设置，请参阅 CLI **configure network dns servers** 和 **configure network dns searchdomains** 命令。.

为了确定 DNS 服务器通信的正确接口，受管设备使用路由查找，但使用哪种路由表取决于您启用 DNS 的接口。有关详细信息，请参阅下面的接口设置。

您可以选择配置多个 DNS 服务器组，并使用它们来解析不同的 DNS 域。例如，您可能有一个使用公共DNS服务器的可捕获默认组，用于与互联网的连接。然后，您可以配置一个单独的组，以将内部 DNS 服务器用于内部流量，例如，与 example.com 域中的计算机的任何连接。因此，使用您的组织的域名与FQDN的连接将使用内部DNS服务器进行解析，而与公共服务器的连接则使用外部DNS服务器。这些解析由使用数据 DNS 解析的任何功能使用，例如 NAT 和访问控制规则。

您可以使用受信任 DNS 服务器选项卡为 DNS 监听配置受信任 DNS 服务。DNS 监听用于将应用域映射到IP，以便检测第一个数据包上的应用。除了配置受信任的DNS服务器之外，您还可以将 DNS 组，DHCP 池，DHCP 中继和 DHCP 客户端中已配置的服务器作为受信任的 DNS 服务器。

注释 对于基于应用的 PBR，必须配置受信任的 DNS 服务器。您还必须确保 DNS 流量以明文格式通过 威胁防御 （不支持加密 DNS），以便解析域以检测应用。

开始之前

- 确保已创建一个或多个 DNS 服务器组。有关详细信息，请参阅创建 DNS 服务器组对象。
- 确保您已创建用于连接到 DNS 服务器的接口对象。
- 确保受管设备具有适当的静态路由或动态路由来访问 DNS 服务器。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)** 并创建或编辑威胁防御策略。

步骤 2 点击 **DNS**。

步骤 3 点击 **DNS 设置** 选项卡。

步骤 4 选中 **启用按设备 DNS 域名解析**。

步骤 5 配置 DNS 服务器组。

a) 在 DNS 服务器组列表中执行以下任一操作：

- 要将值添加到列表，请点击 **添加**。如果在现有服务器组列表中配置了 30 个过滤器域，则无法添加其他组。
- 要编辑组的设置，请点击组旁边的 **编辑**（ ）。
- 要删除组，请点击该组旁边的 **删除**（ ）。删除组不会删除 DNS 服务器组对象，只是将其从此列表中删除。

b) 在添加或编辑组时，请配置以下设置，然后点击 **确定**：

- **选择 DNS 组**-选择现有 DNS 服务器组对象，或点击 + 创建新的 DNS 服务器组对象。
- **作为默认**-选择此选项可使此组成为默认组。任何与其他组的过滤器不匹配的DNS解析请求都将使用此组中的服务器进行解析。
- **过滤域**-仅对于非默认组，是逗号分隔的域名列表，例如example.com，example2.com。不能包含空格。

  该组将仅用于这些域的DNS解析。您可以在添加到此DNS平台设置策略的所有组中最多输入 30 个单独的域。每个名称最多可包含 127 个字符。

  请注意，这些过滤器域与该组的默认域名无关。过滤器列表可以与默认域不同。

步骤 6 （可选） 输入 **过期条目计时器** 和 **轮询计时器** 值，以分钟计。

这些选项仅适用于在网络对象中指定的 FQDN。这些不适用于其他功能中使用的 FQDN。

- **到期条目计时器** 指定DNS条目的最短生存时间（TTL），以分钟为单位。如果到期计时器长于条目的TTL，则TTL增加到到期条目时间值。如果TTL比到期计时器长，则将忽略到期条目时间值：在这种情况下，不会向TTL添加额外时间。到期后，该条目将从DNS查找表中删除。删除条目要求重新编译表，使频繁删除能够增加设备上的处理负载。因为某些DNS条目可以有非常短的TTL（短至3秒），所以您能够使用此设置实际上延长TTL。默认值为1分钟（即，所有分辨率的最小TTL为1分钟）。范围为 1 至 65535 分钟。

  请注意，对于运行7.0或更早版本的系统，到期时间实际上会添加到TTL中：它不指定最小值。

- **轮询计时器** 指定设备查询 DNS 服务器以解析网络对象中定义的 FQDN 的时间限制。在轮询 DNS 计时器到期时或解析的 IP 条目的 TTL 到期时（以先到者为准），定期解析 FQDN。

步骤 7 在所有接口或特定接口上启用 DNS 查找。这些选择还会影响所使用的路由表。

请注意，在接口上启用 DNS 查找与指定用于查找的源接口不同。威胁防御 始终使用路由查询来确定源接口。

- 未选择任何接口 - 在所有接口上启用 DNS 查找，包括管理接口和管理专用接口。威胁防御 检查数据路由表，如果未找到路由，则回退到管理专用路由表。
- 选择了特定接口而不是**同时通过诊断/管理接口启用 DNS 查找 (Enable DNS Lookup via diagnostic interface also)** 选项 - 在指定接口上启用 DNS 查找。威胁防御 仅检查数据路由表。
- 选择了特定接口并且选择了**同时通过诊断/管理接口启用 DNS 查找 (Enable DNS Lookup via diagnostic interface also)** 选项 - 在指定接口和 诊断 接口上启用 DNS 查找。威胁防御 检查数据路由表，如果未找到路由，则回退到管理专用路由表。
- 仅限 **通过诊断启用 DNS 查找 接口及** 选项-在 诊断上启用 DNS 查找。威胁防御 仅检查管理专用路由表。 确保在 **设备** > **设备管理** > **编辑设备** > **接口** 页面上为诊断接口配置 IP 地址。

步骤 8 要配置受信任的 DNS 服务器，请点击 **受信任的 DNS 服务器** 选项卡。

步骤 9 默认情况下，在 DHCP 池，DHCP 中继，DHCP 客户端或 DNS 服务器组中配置的现有DNS服务器作为受信任DNS服务器。如果要排除其中任何一个，请取消选中相应的复选框。

步骤 10 要添加受信任的 DNS 服务器，请在 **指定 DNS 服务器**下，点击 **编辑**。

步骤 11 在 **选择 DNS 服务器** 对话框中，选择主机对象作为受信任 DNS 服务器或直接指定受信任 DNS 服务器的 IP 地址：

a) 要选择现有主机对象，请在 **可用主机对象**下，选择所需的主机对象，然后点击 **添加** 以将其包含到 **所选DNS服务器**中。有关添加主机对象的信息，请参阅 创建网络对象。

b) 要直接提供受信任 DNS 服务器的 IP 地址（IPv4 或 IPv6），请在给定文本字段中输入地址，然后点击 **添加** 以将其包含到 **所选 DNS 服务器**中。

c) 点击**保存 (Save)**。添加的DNS服务器显示在 **受信任的 DNS 服务器** 页面中。

注释 每个策略最多可以配置 12 个 DNS 服务器。

步骤 12 （可选）要使用主机名或 IP 地址搜索已添加的 DNS 服务器，请使用 **指定 DNS 服务器** 下的搜索字段。

步骤 13 点击**保存 (Save)**。

下一步做什么

要将 FQDN 对象用于访问控制规则，请创建一个 FQDN 网络对象，然后将其分配给访问控制规则。有关说明，请参阅创建网络对象。

为 SSH 配置外部身份验证

注释 您必须具有管理员权限才能执行此任务。

在为管理用户启用外部身份验证时，威胁防御会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

共享外部身份验证对象

管理中心 和 威胁防御 设备可使用外部身份验证对象。管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。请注意， 威胁防御 支持在 RADIUS 服务器上定义用户，而 管理中心 要求您在外部身份验证对象中预定义用户列表。您可以选择针对 威胁防御使用预定义列表方法，但如果要在 RADIUS 服务器上定义用户，则必须为 威胁防御 和 管理中心创建单独的对象。

注释 威胁防御 和 管理中心 的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御 的较小超时范围（对于 LDAP 为 1-30 秒，对于 RADIUS 为 1-300 秒）。如果将超时设置为更高的值，则 威胁防御 外部身份验证配置将不起作用。

为设备分配外部身份验证对象

对于 管理中心，请直接在 **系统** > **用户** > **外部身份验证**启用外部身份验证对象；此设置仅会影响 管理中心 的使用情况，无需为了受管设备的使用而启用此设置。对于 威胁防御 设备，必须在部署到设备的平台设置中启用外部身份验证对象，并且每个策略只能激活一个外部认证对象。已启用 CAC 身份验证的 LDAP 对象也不能用于 CLI 访问。

威胁防御 支持的字段

只有外部身份验证对象中一个子集的字段可用于 威胁防御 SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于 管理中心，则将使用这些字段。此程序仅涵盖 威胁防御 支持的字段。有关其他字段，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 《配置 管理中心 外部身份验证》。

用户名

用户名必须为使用字母数字字符加句点 (.) 或连字符 (-) 的 Linux 有效用户名，且仅可使用小写字母。不支持其他特殊字符，例如 at 符号 (@) 和斜线 (/)。不能为外部身份验证添加**管理员**用户。只能在管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在 CLI 中添加他们。请注意，内部用户只能在 CLI 中添加，不能在管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 威胁防御 首先对照此内部用户检查密码，如果失败，再检查 AAA 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。 对于 RADIUS 服务器上定义的用户，请务必将权限级别设置为与任何内部用户相同的权限级别；否则您无法使用外部用户密码登录。

特权等级

LDAP 用户始终具有“配置”权限。RADIUS 用户可定义为“配置”或“基本”用户。

开始之前

- 管理接口上的 SSH 访问默认处于启用状态。要在数据接口上启用 SSH 访问，请参阅配置安全外壳 ，第 19 页。诊断接口上不支持 SSH。
- 请告知 RADIUS 用户以下操作，使他们合理设定预期：

- 外部用户首次登录时，威胁防御 会创建所需的结构，但不能同时创建用户会话。用户只需再次进行身份验证，即可启动会话。用户将看到与以下消息类似的消息：“已识别新的外部用户名。请重新登录以启动会话。”
- 同样地，如果自上次登录以来，用户的 Service-Type 授权发生了更改，则用户将需要重新进行身份验证。用户将看到与以下消息类似的消息：“您的授权权限已更改。请重新登录以启动会话。”

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 点击**管理外部身份验证服务器**链接。

您还可以通过点击 **系统** > **用户** > **外部身份验证**打开外部身份验证屏幕。

步骤 4 配置 LDAP 身份验证对象。

a) 点击**添加外部身份验证对象 (Add External Authentication Object)**。

b) 将**身份验证方法**设置为 **LDAP**

c) 输入**名称**和可选**说明**。

d) 从下拉列表中选择**服务器类型**。

e) 对于**主服务器**，输入**主机名/IP 地址**。

注释 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

f) （可选）更改**端口**使用的默认值。

g) （可选）输入**备份服务器**参数。

h) 输入 **LDAP 特定参数**。

- **基础 DN** - 为要访问的 LDAP 目录输入基本可分辨名称。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN**，然后从下拉列表中选择相应的基本可分辨名称。
- **基本过滤器** - 例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且纽约办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索纽约办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。
- **用户名** - 为有足够凭证浏览 LDAP 服务器的用户输入可分辨的名称。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。
- **密码**和**确认密码** - 输入并确认用户的密码。
- （可选）**显示高级选项** - 配置以下高级选项。

- **加密** - 点击**无**、**TLS** 或 **SSL**。

  注释 如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或 **TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件**选择一个证书。
- （未使用）**用户名模板** - 威胁防御 未使用。
- **超时**-输入滚动到备份连接之前等待的秒数（1-30 秒）。默认值为 30。

  注释 威胁防御 和 管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 威胁防御 外部身份验证配置将不起作用。

i) （可选）如果要使用用户可分辨类型之外的外壳访问属性，请设置 **CLI 访问属性** 。例如，在 Microsoft Active Directory Server 上，通过在 **CLI 访问属性** 字段中键入 `sAMAccountName` 来使用 `sAMAccountName` 外壳访问属性检索外壳访问用户。

j) 设置 **CLI 访问过滤器**。

选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选择**与基本过滤器相同 (Same as Base Filter)**。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

LDAP 服务器上的名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

k) 点击**保存 (Save)**。

步骤 5 对于LDAP，如果以后在LDAP服务器上添加或删除用户，必须刷新用户列表并重新部署平台设置。

a) 依次选择**系统** > **用户** > **外部身份验证**。

b) 点击 LDAP 服务器旁边的 **刷新** （ ） 。

如果用户列表发生变化，您将看到一条消息，建议您为设备部署配置更改。Firepower 威胁防御平台设置还会显示它在“*x* 个目标设备上过时。"

c) 部署配置更改；请参阅部署配置更改。

步骤 6 配置 RADIUS 身份验证对象。

a) 使用 Service-Type 属性在 RADIUS 服务器上定义用户。

以下是受支持的 Service-Type 属性值：

- 管理员 (6) - 提供 CLI 的配置访问授权。这些用户可以在 CLI 中使用所有命令。
- NAS 提示 (7) 或除级别 6 以外的任何级别 - 提供 CLI 的基本访问授权。这些用户可以使用只读命令，例如**show**命令，用于监控和故障排除。

名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

或者，您可以在外部身份验证对象中预定义用户（参见步骤6.j，第 11 页）。要在为 威胁防御 使用 Service-Type 属性的同时对 威胁防御 和 管理中心 使用相同的 RADIUS 服务器，请创建可识别相同 RADIUS 服务器的两个外部身份验证对象：其中一个对象包括预定义的 **CLI 访问过滤器** 用户（用于 管理中心），另一个对象则将 **CLI 访问过滤器** 留空（用于 威胁防御）。

b) 在 管理中心 中，点击**添加外部身份验证对象**。
c) 将**身份验证方法**设置为 **RADIUS**。
d) 输入**名称**和可选**说明**。
e) 对于**主服务器**，输入**主机名/IP 地址**。

注释 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

f) （可选） 更改**端口**使用的默认值。
g) 输入 **RADIUS 服务器密钥**。
h) （可选） 输入**备份服务器**参数。
i) 输入 **RADIUS 特定参数**。
   - **超时（秒）** - 输入滚动到备份连接之前等待的秒数。默认值为 30。
   - **重试次数** - 输入在滚动到备份连接之前应当尝试主服务器连接的次数。默认值为 3。
j) （可选）不使用 RADIUS 定义的用户，在 **CLI 访问过滤器**下，在 **管理员 CLI 访问用户列表** 字段中输入一个逗号分隔的用户名列表。例如，输入 **`jchrichton`**、**`aerynsun`**、**`rygel`**。

   您可能想要使用 威胁防御 的 **CLI 访问过滤器** 方法以便对 威胁防御 和其他平台类型使用相同的外部身份验证对象。请注意，如果想要使用 RADIUS 定义的用户，则必须将 **CLI 访问过滤器** 留空。

   请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

   - 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
   - 全部小写
   - 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

注释　　如果要在 RADIUS 服务器上仅定义用户，则必须将此部分留空。

k) 点击**保存 (Save)**。

步骤 7 返回 **设备** > > **平台设置** > **外部身份验证**。

步骤 8 点击 **刷新**（ ）可查看新添加的任何对象。

为 LDAP 指定 SSL 或 TLS 加密时，必须上传证书才能进行连接；否则，此窗口中将不会列出该服务器。

步骤 9 点击要使用的外部身份验证对象旁边的 **滑块已启用**（ ）。只能启用一个对象。

步骤 10 点击**保存 (Save)**。

步骤 11 部署配置更改；请参阅部署配置更改。

配置分段处理

默认情况下，威胁防御设备允许每个 IP 数据包最多包含 24 个分段，以及最多 200 个等待重组的分段。如果您有定期对数据包进行分段的应用（如 NFS over UDP），可能需要让分段位于您的网络上。但如果您没有对流量进行分段的应用，则我们建议您通过将**链**设置为 1 来禁止分段。分段数据包通常用作拒绝服务 (DoS) 攻击。

注释　这些设置将为已分配此策略的设备建立默认值。可以通过选择接口配置中的**覆盖默认分段设置**，为设备上的特定接口覆盖这些设置。在编辑接口时，可以找到**高级 (Advanced)** > **安全配置 (Security Configuration)** 上的选项。选择**设备 (Devices)** > **设备管理 (Device Management)**，编辑 威胁防御设备，然后选择**接口 (Interfaces)** 以编辑接口属性。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**碎片设置 (Fragment Settings)**。

步骤 3 配置以下选项。如果希望使用默认设置，请点击**重置为默认值**。

- **大小（块）** - 来自所有连接的可能正在等待重组的总体数据包分段的最大数量。默认值为 200 个分段。
- **链（分段）** - 可将一个完整 IP 数据包分段为数据包的最大数量。默认为 24 个数据包。将此选项设置为 1 将禁止分段。
- **超时（秒）** - 等待整个分段数据包到达所需的最大秒数。默认值为 5 秒。如果在此时间内未收到所有分段，则将放弃所有分段。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 HTTP

如果希望允许到 威胁防御设备上的一个或多个接口的 HTTPS 连接，则请配置 HTTPS 设置。可以使用 HTTPS 来下载用于故障排除的数据包捕获。

开始之前

- 当您使用 Cisco Secure Firewall Management Center管理 威胁防御时，针对 威胁防御的 HTTP 访问选线仅可用于查看数据包捕获文件。威胁防御没有用于在此管理模式下进行配置的 Web 接口。
- 只能使用 **configure user add** 命令在 CLI 中配置 HTTPS 本地用户。默认情况下，有一个您在初始设置期间为其配置密码的 **admin** 用户。不支持 AAA 外部身份验证。
- 此配置仅适用于数据接口，包括您配置为仅管理的任何接口。它主题不适用于专用管理接口。物理管理接口在“诊断”逻辑接口与“管理”逻辑接口之间共享；此配置仅适用于“诊断”逻辑接口（如果使用）或其他数据接口。管理逻辑接口与设备上的其他接口分离。它用于设置设备并将其注册到 管理中心。它具有独立 IP 地址和静态路由。
- 要使用 HTTPS，无需允许主机 IP 地址的访问规则。只需按照本部分配置 HTTPS。
- 只能将 HTTPS 用于可访问的接口；如果 HTTPS 主机位于外部接口上，则只能向该外部接口直接发起管理连接。
- 不能在同一接口上为同一 TCP 端口同时配置 HTTPS 和 AnyConnect 远程访问 SSL VPN 。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。如果必须在同一接口上同时配置这两项功能，则请使用不同的端口。例如，在端口 4443 上打开 HTTPS。
- 需要网络对象，用于定义将要允许建立到设备的 HTTPS 连接的主机或网络。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象** > **对象管理**以配置对象。

注释 不能使用系统提供的**任意**网络对象组。而应使用**任意 ipv4** 或**任意 ipv6**。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择 **HTTP**。

步骤 3 选中**启用 HTTP 服务器 (Enable HTTP Server)** 复选框以启用 HTTP 服务器。

步骤 4 （可选） 更改 HTTP 端口。默认值为 443。

步骤 5 标识允许 HTTP 连接的接口和 IP 地址。

使用此表来限制哪些接口将接受 HTTP 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址** - 用于标识允许建立 HTTP 连接的主机或网络的网络对象或组。从下拉列表中选择一个对象，或者点击 + 以添加新的网络对象。
- **安全区域** - 添加包含将允许进行 HTTP 连接的接口的区域。对于不在区域中的接口，可以在**所选安全区域** 列表下方的字段中键入接口名称，然后点击 **添加**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 ICMP 访问规则

默认情况下，您可以使用 IPv4 或 IPv6 将 ICMP 数据包发送到任何接口，以下情况例外：

- 威胁防御 不响应定向至广播地址的 ICMP 回显请求。
- 威胁防御 仅响应发送至流量进入的接口的 ICMP 流量；不能通过某个接口将 ICMP 流量发送至远端接口。

为了保护设备免受攻击，您可以使用 ICMP 规则将接口的 ICMP 访问限制为特定主机、网络或 ICMP 类型。ICMP 规则的工作原理与访问规则类似，将对规则进行排序，与数据包匹配的第一条规则将定义操作。

如为某个接口配置任何 ICMP 规则，则将隐式拒绝 ICMP 规则添加至 ICMP 规则列表的末尾，从而更改默认行为。因此，如果想要仅拒绝几种消息类型，则须在 ICMP 规则列表的末尾纳入一条允许任何消息类型的规则，以便允许剩余的消息类型。

我们建议，始终为 ICMP 不可到达消息类型（类型 3）授予权限。拒绝 ICMP 不可达消息会禁用 ICMP 路径 MTU 发现，从而可能阻止 IPsec 和 PPTP 流量。此外，IPv6 中的 ICMP 数据包用于 IPv6 邻居发现进程。

开始之前

确保规则中所需的对象已经存在。选择**对象** > **对象管理**以配置对象。您需要网络对象或组来定义所需的主机或网络，并且需要端口对象来定义要控制的 ICMP 消息类型。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择 **ICMP**。

步骤 3 配置 ICMP 规则。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **操作** - 许可（允许）还是拒绝（丢弃）匹配的流量。
- **ICMP 服务** - 标识 ICMP 消息类型的端口对象。
- **网络 (Network)** - 标识您要控制其访问权限的主机或网络的网络对象或组。
- **安全区域 (Security Zones)** - 添加包含您所保护的接口的区域。对于不在区域中的接口，可以在**所选安全区域 (Selected Security Zones)** 列表下方的字段中键入接口名称，然后点击 **添加 (Add)**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 4 （可选。）设置对 ICMPv4 无法访问的消息的速率限制。

- **速率限制** - 设置不可达消息的速率限制，该限制介于每秒 1 至 100 条消息之间。默认值为每秒 1 条消息。
- **突发大小** - 设置突发速率，其值介于 1 至 10 之间。系统会发送此数量的回复，但在达到速率限制之前不会发送后续回复。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SSL 设置

注释 您必须具有管理员权限并在分叶域中才能执行此任务。

必须确保您运行的是 Cisco Secure Firewall Management Center的完全许可版本。如果是在评估模式下运行 Cisco Secure Firewall Management Center 时，“SSL 设置”将被禁用。此外，当许可的 Cisco Secure Firewall Management Center 版本不符合导出标准时，“SSL 设置”将被禁用。如果您使用的是带有 SSL 的远程接入 VPN，则您的智能帐户必须启用强加密功能。有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 许可证类型和限制 。

过程

步骤 1 选择**设备 > 平台设置**，并创建或编辑 威胁防御策略。

步骤 2 选择 **SSL**。

步骤 3 将条目添加到**添加 SSL 配置**表中。

a) 点击**添加**以创建新条目，如果该条目已存在，则点击**编辑**。

b) 从下拉列表中选择所需的安全配置。

- **协议版本** - 指定在建立远程接入 VPN 会话时要使用的 TLS 协议。
- **安全级别** - 指示希望为 SSL 设置的安全定位类型。

步骤 4 根据您选择的协议版本选择**可用算法**，然后点击**添加**以针对所选协议包括这些算法。有关详细信息，请参阅关于 SSL 设置，第 16 页。

这些算法根据您选择的协议版本列出。每个安全协议标识用于设置安全级别的唯一算法。

步骤 5 点击**确定**以保存更改。

下一步做什么

选择 **部署** > **部署** 然后点击 **部署** 以将策略部署到所分配的设备。

关于 SSL 设置

威胁防御设备使用安全套接字层 (SSL) 协议和传输层安全 (TLS) 对来自远程客户端的远程访问 VPN 连接支持安全消息传输。通过 SSL 设置窗口，您可以配置在通过 SSL 远程 VPN 访问传输邮件过程中协商和使用的 SSL 版本和加密算法。

在以下位置配置 SSL 设置：

设备 > 平台设置 > SSL

字段

充当服务器时的最低 SSL 版本- 指定在充当服务器时， 威胁防御 设备使用的最低 SSL/TLS 协议版本。例如，用作远程访问 VPN 网关时。

TLS 版本—从下拉列表中选择以下 TLS 版本之一：

TLS V1	接受 SSLv2 客户端问候并协商 TLSv1（或更高版本）。
TLSV1.1	接受 SSLv2 客户端问候并协商 TLSv1.1（或更高版本）。
TLSV1.2	接受 SSLv2 客户端问候并协商 TLSv1.2（或更高版本）。

DTLS 版本—根据所选的 TLS 版本，从下拉列表中选择 DTLS 版本。默认情况下，DTLSv1 在 威胁防御 设备上配置，您可以根据需要选择 DTLS 版本。

注释 确保 TLS 协议版本高于或等于所选的 DTLS 协议版本。TLS 协议版本支持以下 DTLS 版本：

TLS V1	DTLSv1
TLSV1.1	DTLSv1
TLSV1.2	DTLSv1、DTLSv1.2

Diffie-Hellman 组—从下拉列表中选择一个组。可用选项为 Group1 - 768 位模数、Group2 - 1024 位模数、Group5 - 1536 位模数、Group14 - 2048 位模数、224 位素数阶和 Group24 - 2048 位模数、256 位素数阶。默认值为 Group1。

椭圆曲线 Diffie-Hellman 组 - 从下拉列表中选择一个组。可用选项为 Group19 - 256 位 EC、Group20 - 384 位 EC 和 Group21 - 521 位 EC。默认值为 Group19。

TLSv1.2 增加了对以下密码的支持：

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

注释 ECDSA 和 DHE 密码具有最高优先级。

SSL 配置表可用于指定要在 Cisco Secure Firewall Threat Defense设备上支持的协议版本、安全级别和密码算法。

协议版本 - 列出 Cisco Secure Firewall Threat Defense设备支持和用于 SSL 连接的协议版本。可用的协议版本有：

- 默认

- TLSV1
- TLSV1.1
- TLSV1.2
- DTLSv1
- DTLSv1.2

安全级别—列出 威胁防御设备支持和用于 SSL 连接的加密安全级别。

如果您的 威胁防御 设备具有评估许可证，默认情况下安全级别为“低”。使用 威胁防御 智能许可证时，默认安全级别为“高”。您可以选择以下选项之一来配置所需的安全级别：

- **All** 包括 NULL-SHA 等所有密码。
- **Low** 包括除 NULL-SHA 之外的所有密码。
- **Medium** 包括所有密码，但 NULL-SHA、DES-CBC-SHA、RC4-SHA 和 RC4-MD5（这是默认密码）除外。
- **Fips** 包括所有符合 FIPS 的密码，但 NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA 除外。
- **High** 只包含带有 SHA-2 加密的 AES-256，并适用于 TLS 版本 1.2 和默认版本。
- **Custom** 包括您在 Cipher algorithms/custom string 框中指定的一个或多个密码。此选项使您可以使用 OpenSSL 密码定义字符串对密码套件进行全面控制。

密码算法/自定义字符串- 列出 威胁防御 设备支持和用于 SSL 连接的加密算法。有关使用 OpenSSL 的密码的详细信息，请参阅 https://www.openssl.org/docs/apps/ciphers.html

威胁防御设备指定用于受支持密码的优先级顺序：

仅受 TLSv1.2 支持的密码

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256

DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

TLSv1.1 或 TLSv1.2 不支持的密码

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

配置安全外壳

如果在数据接口（例如外部）上启用了管理中心访问，则应使用此程序在该接口上启用SSH。本节介绍如何启用 威胁防御上一个或多个 数据 接口的 SSH 连接。 诊断逻辑接口上不支持 SSH。

注释 管理接口上默认已启用 SSH，但此屏幕不会影响管理 SSH 访问。

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到管理中心。数据接口的SSH与管理接口的SSH共用内部和外部用户列表。其他设置单独进行配置：对于数据接口，使用此屏幕启用SSH和访问列表；数据接口的SSH流量使用常规路由配置，并不是所有静态路由均在设置时或CLI中配置。

对于管理接口，要配置 SSH 访问列表，请参阅 Cisco Secure Firewall Threat Defense 命令参考中的 **configure ssh-access-list** 命令。要配置静态路由，请参阅 **configure network static-routes** 命令。默认情况下，在初始设置时通过管理接口配置默认路由。

要使用 SSH，您也不需要允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。

您只能SSH到可访问接口；如果SSH主机位于外部接口上，则只能直接向外部接口发起管理连接。

注释 在您连续三次尝试使用 SSH 登录 CLI 失败后，设备会终止 SSH 连接。

开始之前

- 可以使用 **configure user add** 命令在 CLI 中配置 SSH 内部用户，请参阅 在 CLI 中添加内部用户。默认情况下，有一个您在初始设置期间为其配置密码的 **admin** 用户。还可以通过在平台设置中配置**外部身份验证**，在 LDAP 或 RADIUS 上配置外部用户。请参阅为 SSH 配置外部身份验证，第 7 页。
- 您需要定义允许与设备建立 SSH 连接的主机或网络网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象** > **对象管理**以配置对象。

注释 不能使用系统提供的 **any** 网络对象。而是使用 **any-ipv4** 或 **any-ipv6**。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**安全外壳 (Secure Shell)**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

使用此表可以限制哪些接口将接受 SSH 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址**-用于标识允许建立 HTTPS 连接的主机或网络的网络对象 或组 。从下拉列表中选择一个对象，或者点击 + 以添加新的网络对象。
- **安全区域** - 添加包含将允许进行 SSH 连接的接口的区域。对于不在区域中的接口，可以在**所选安全区域** 列表下方的字段中键入接口名称，然后点击 **添加**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SMTP

如果在“系统日志”设置中配置了邮件警报，则必须标识 SMTP 服务器。为“系统日志”配置的源邮件地址必须是 SMTP 服务器上的有效帐户。

开始之前

确保存在用于定义主 SMTP 服务器和辅助 SMTP 服务器的主机地址的网络对象。依次选择**对象** > **对象管理**，以定义对象。或者，也可以在编辑策略时创建对象。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 点击 **SMTP 服务器**。

步骤 3 选择标识**主服务器 IP 地址**的网络对象，以及可选的**辅助服务器 IP 地址**。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SNMP

简单网络管理协议 (SNMP) 为在 PC 或工作站上运行的网络管理工作站定义了一种监控许多类型的设备（包括交换机、路由器和安全设备）的运行状况和状态的标准方法。您可以使用 SNMP 页面来配置防火墙设备，以便通过 SNMP 管理工作站进行监控。

简单网络管理协议 (SNMP) 支持从中心位置监控网络设备。思科安全设备支持使用 SNMP 版本 1、2c 和 3 进行网络监控，也支持陷阱和 SNMP 读取访问，但不支持 SNMP 写入访问。

SNMPv3 支持使用 DES（已弃用）、3DES、AES256、AES192 和 AES128 的只读用户和加密。

注释 DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于 威胁防御运行 6.6 及更低版本的 。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 管理中心 管理任何运行版本 7.0+ 的 威胁防御，则将使用 DES 加密的平台设置策略部署到这些 威胁防御将会失败。

注释 SNMP 配置仅支持路由和诊断接口。

注释 要创建发送至外部 SNMP 服务器的警报，请访问**策略 (Policies)** > **操作 (Action)** > **警报 (Alerts)**

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择 **SNMP**。

步骤 3 启用 SNMP 并配置基本选项。

- **启用 SNMP 服务器** - 是否向配置的 SNMP 主机提供 SNMP 信息。您可以取消选择此选项，以便在保留配置信息的同时禁用 SNMP 监控。
- **读取社区字符串、确认** - 输入在向 威胁防御设备发送请求时，SNMP 管理工作站使用的密码。SNMP 社区字符串是 SNMP 管理工作站与受管的网络节点之间的共享密钥。安全设备使用此密码确定传入的 SNMP 请求是否有效。密码是区分大小写的字母数字字符串，最多可包含 32 个字符；不允许使用空格和特殊字符。
- **系统管理员名称** - 输入设备管理员或其他联系人的名称。该字符串区分大小写，最多可以包含 127 个字符。接受空格，但多个空间缩为一个空格。
- **位置** - 输入此安全设备的位置（例如，54 区 42 号楼）。该字符串区分大小写，最多可以包含 127 个字符。接受空格，但多个空间缩为一个空格。
- **端口** - 输入将在其上接受传入请求的 UDP 端口。默认值为 161。

步骤 4 （仅限 SNMPv3）。添加 SNMPv3 用户，第 26 页。

步骤 5 添加 SNMP 主机，第 29 页。

步骤 6 配置 SNMP 陷阱，第 30 页。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

关于 SNMP

SNMP 是一种应用层协议，可促进网络设备之间的管理信息交换，是 TCP/IP 协议簇的一部分。 威胁防御 为使用 SNMP 版本 1、2c 和 3 的网络监控提供支持，并支持同时使用所有三个版本。利用在威胁防御 接口上运行的 SNMP 代理，您可以通过诸如 HP OpenView 之类的网络管理系统 (NMS) 监控网络设备。威胁防御 通过发出 GET 请求来支持 SNMP 只读访问。不允许 SNMP 写访问，因此您无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

您可以将 威胁防御 配置为向 NMS 发送陷阱，即针对特定事件从托管设备发送到管理站的未经请求的消息（事件通知），也可以使用 NMS 浏览安全设备上的管理信息库 (MIB)。MIB 是定义的集合，而 威胁防御 维护由每个定义的值组成的数据库。浏览 MIB 意味着从 NMS 发出 MIB 树的一系列 GET-NEXT 或 GET-BULKGET 请求以确定值。

SNMP 代理可在发生预定义为需要通知（例如，当网络中的链路开启或关闭时）的事件的情况下通知指定的管理站。它发送的通知包括用于向管理站表明其自身身份 SNMP OID。代理还会在管理站请求信息时进行回复。

SNMP 术语

下表列出在使用 SNMP 时常用的术语。

表 *1: SNMP* 术语

术语	说明
代理	在 Cisco Secure Firewall Threat Defense 上运行的 SNMP 服务器。SNMP 代理具有以下功能： • 对来自网络管理站的信息和操作请求作出响应。 • 控制对其管理信息库（即 SNMP 可以查看或更改的对象的集合）的访问。 • 不允许 SET 操作。
浏览	通过从设备上的 SNMP 代理轮询所需信息来从网络管理站监控该设备的运行状况。此活动可能包括从网络管理站发出 MIB 树的一系列 GET-NEXT 或 GET-BULK 请求以确定值。
管理信息库 (MIB)	用于收集有关数据包、连接、缓冲区、故障切换等的信息的标准化数据结构。MIB 由大多数网络设备使用的产品、协议和硬件标准来定义。SNMP 网络管理站可以浏览 MIB，并请求在出现特定数据或事件时将其发送。
网络管理站 (NMS)	设置 PC 或工作站是为了监控 SNMP 事件和管理设备。
对象标识符 (OID)	用于向设备的 NMS 表明该设备的身份并向用户指示监控和显示的信息源的系统。
陷阱	用于生成从 SNMP 代理到 NMS 的消息的预定义事件。事件包括警报条件，例如链路开启、链路关闭、冷启动、热启动、身份验证或系统日志消息。

MIB 和陷阱

MIB 特定于标准或特定于企业。标准 MIB 由 IETF 创建并记录在各种 RFC 中。陷阱报告发生在网络设备上的重大事件，大多数情况下是错误或故障。SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 ASA 软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

浏览 SNMP 对象导航器，从以下位置查找思科 MIB、陷阱和 OID：

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

此外，从以下位置通过 FTP 下载思科 OID：

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

MIB 支持的表和对象

以下部分列出了对指定 MIB 支持的表和对象。

远程接入 VPN 轮询

表 2: CISCO-REMOTE-ACCESS-MONITOR-MIB

计数器	OID	说明
活动会话	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	当前活动会话的数量。
用户	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	具有活动会话的用户数。
峰值会话	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	自系统启动以来的峰值 RA 会话数。

站点间 VPN 隧道轮询

表 3: CISCO-REMOTE-ACCESS-MONITOR-MIB

计数器	OID	说明
LAN 到 LAN 会话	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	当前活动的 LAN 到 LAN 会话数。
峰值 LAN 到 LAN 会话数	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	自系统启动以来的峰值并发 LAN 会话数。

连接轮询

表 4: CISCO-FIREWALL-MIB

计数器	OID	说明
活动连接数	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	整个防火墙当前使用的连接数。
峰值连接	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	自系统启动以来在任何时间使用的最高连接数。
每秒连接数	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	防火墙上的当前每秒连接数。

计数器	OID	说明
每秒峰值连接数	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	自系统启动以来防火墙上的每秒最高连接数。

NAT 转换轮询

表 *5: CISCO-NAT-EXT-MIB*

计数器	OID	说明
活动转换	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	NAT 设备中当前可用的地址转换条目总数。这表示从静态和动态地址转换机制创建的转换条目的汇总。
峰值活动转换	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	自系统启动以来任何时候处于活动状态的最大地址转换条目数。这表示自系统启动以来任何时候处于活动状态的地址转换条目的高水印。 该对象包括从静态和动态地址转换机制创建的转换条目。

路由表条目轮询

表 *6: IP-FORWARD-MIB*

计数器	OID	说明
活动转换	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	当前有效的 inetCidrRouteTable 条目总数。

接口双工状态轮询

表 *7: CISCO-IF-EXTENSION-MIB*

计数器	OID	说明
双工状态	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	此对象会指定给定接口上配置的双工状态。

计数器	OID	说明
检测到的双工状态	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	此对象指定给定接口上检测到的双工状态。

Snort 3 入侵事件速率轮询

表 *8: CISCO-UNIFIED-FIREWALL-MIB*

计数器	OID	说明
Snort 3 入侵事件速率	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	在过去 300 秒内，Snort 在此防火墙上记录入侵事件的平均速率。

BGP 对等翻板陷阱通知

表 *9: BGP4-MIB*

计数器	OID	说明
BGP 对等翻板	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	当 BGP FSM 从较高编号状态移动到较低编号状态时，就会生成 BGPBackwardTransition 事件。

注释 在 ASA FirePOWER 上删除了与 CPU 监控（hrProcessorTable 和 hrNetworkTable）相关的 SNMP OID 1.3.6.1.2.1.25.3.3 和 1.3.6.1.2.1.25.3.4。您只能通过设备管理器查看和监控设备的 CPU 运行状况详细信息。

添加 SNMPv3 用户

注释 您只为 SNMPv3 创建用户。这些步骤不适用于 SNMPv1 或 SNMPv2c。

请注意，SNMPv3 只支持只读用户。

SNMP 用户具有指定的用户名、身份验证密码、加密密码以及要使用的身份验证和加密算法。

注释 将 SNMPv3 用于群集或高可用性时，如果在初始集群形成后添加新的集群设备或更换高可用性设备，则 SNMPv3 用户不会复制到新设备。您必须删除用户、重新添加，然后重新部署配置，以强制用户复制到新单元。

身份验证算法选项包括 MD5（解密，仅限预-6.5）、 SHA、SHA224、SHA256 和 SHA384。

注释 MD5 选项已被弃用。如果您的部署包括使用 6.5 之前版本创建的使用 MD5 身份验证算法的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 FTD。但是，您无法编辑这些用户并保留 MD5 身份验证算法，或使用 MD5 身份验证算法创建新用户。如果您的 管理中心 管理任何运行 7.0 以上版本的 威胁防御，则将使用 MD5 身份验证算法的平台设置策略部署到这些 威胁防御将失败。

加密算法选项是 DES（解密、仅限预-6.5）、3DES、AES256、AES192 和 AES128。

注释 DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 威胁防御。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 管理中心 管理任何运行版本 7.0+ 的 威胁防御，则将使用 DES 加密的平台设置策略部署到这些 威胁防御将会失败。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 请点击 **SNMP** > **用户 (Users)**。

步骤 3 点击 **Add**。

步骤 4 从**安全级别**下拉列表中选择用户的安全级别。

- **Auth** - 有身份验证但无隐私，意味着消息会进行身份验证。
- **No Auth** - 无身份验证且无隐私，意味着未对消息应用安全设置。
- **Priv** - 有身份验证且有隐私，意味着对消息进行身份验证和加密。

步骤 5 在**用户名**字段中输入 SNMP 用户的名字。用户名长度不得超过 32 个字符

步骤 6 在**加密密码类型**下拉列表中选择要使用的密码类型。

- **明文** - 威胁防御设备在部署到设备时仍将对密码进行加密。
- **加密** - 威胁防御设备将直接部署加密的密码。

步骤 7 在 **授权算法类型** 下拉列表中选择要使用的身份验证类型： SHA、 SHA224、 SHA256或 SHA384。

注释 MD5 选项已被弃用。如果您的部署包括使用 6.5 之前版本创建的使用 MD5 身份验证算法的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 FTD。但是，您无法编辑这些用户并保留 MD5 身份验证算法，或使用 MD5 身份验证算法创建新用户。如果您的 管理中心 管理任何运行 7.0 以上版本的 威胁防御，则将使用 MD5 身份验证算法的平台设置策略部署到这些 威胁防御将失败。

步骤 8 在**身份验证密码**字段中，输入用于身份验证的密码。如果选择“加密为加密密码类型”，则密码必须格式化为 xx:xx:xx...，其中 xx 为十六进制值。

注释 密码的长度将取决于所选的身份验证算法。对于所有密码，长度必须不能超过 256个字符。

如果选择“明文”作为“加密密码”类型，请在**确认**字段中重复该密码。

步骤 9 在**加密类型 (Encryption Type)** 下拉列表中，选择要使用的加密类型：AES128、AES192、AES256、3DES。

注释 要使用 AES 或 3DES 加密，必须在设备上安装相应的许可证。

注释 DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 威胁防御。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 管理中心 管理任何运行版本 7.0+ 的 威胁防御，则将使用 DES 加密的平台设置策略部署到这些 威胁防御将会失败。

步骤 10 在**加密密码 (Encryption Password)** 字段中输入用于加密的密码。如果选择“加密为加密密码类型”，则密码必须格式化为 xx:xx:xx...，其中 xx 为十六进制值。对于加密的密码，密码的长度取决于所选的加密类型。密码大小如下（每个 xx 是一个八进制值）：

- AES 128 需要 16 个八进制值
- AES 192 需要 24 个八进制值
- AES 256 需要 32 个八进制值
- 3DES 需要 32 个八进制值
- DES 可以是任意大小

注释 对于所有密码，长度必须不能超过 256个字符。

如果选择“明文”作为“加密密码”类型，请在**确认**字段中重复该密码。

步骤 11 点击**确定 (OK)**。

步骤 12 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

添加 SNMP 主机

使用“主机”(Host) 以在 SNMP 页面上的“SNMP 主机”(SNMP Hosts) 表中添加或编辑条目。这些条目表示允许访问 威胁防御设备的 SNMP 管理站。

最多可以添加 8192 台主机。但是，其中仅 128 台可用于陷阱。

开始之前

确保存在定义 SNMP 管理站的网络对象。选择**设备** > **对象管理**以配置网络对象。

注释 支持的网络对象包括 IPv6 主机、IPv4 主机、IPv4 范围和 IPv4 子网地址。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 点击 **SNMP** > **主机 (Hosts)**。

步骤 3 点击 **Add**。

步骤 4 在 **IP 地址**字段中，输入有效的 IPv6 或 IPv4 主机或选择定义 SNMP 管理站主机地址的网络对象。

IP 地址可以是 IPv6 主机、IPv4 主机、IPv4 范围或 IPv4 子网。

步骤 5 从 **SNMP 版本**下拉列表中选择适当的 SNMP 版本。

步骤 6 （仅限 SNMPv3。）从**用户名**下拉列表中选择您配置的 SNMP 用户的用户名。

注释 每个 SNMP 主机最多可以关联 23 个 SNMP 用户。

步骤 7 （仅限 SNMPv1、2c。）在**读取社区字符串**字段中，输入已配置的社区字符串，以便对设备进行读取访问。重新输入该字符串以进行确认。

注释 仅当与此 SNMP 工作站一起使用的字符串与**启用 SNMP 服务器**部分中定义的字符串不同时，才需要此字符串。

步骤 8 选择设备与 SNMP 管理站之间的通信类型。您可以选择以下两种类型。

- **轮询** - 管理站会定期从设备请求信息。
- **陷阱** - 在发生陷阱事件时，设备将陷阱事件发送到管理站。

注释 当 SNMP 主机 IP 地址是 IPv4 范围或 IPv4 子网时，您可以配置**轮询**或**陷阱**，而不是同时配置两者。

步骤 9 在**端口**字段中，输入 SNMP 主机的 UDP 端口号。默认值为 162。有效范围为 1 至 65535。

步骤 10 在**访问方式 (Reachable By)** 选项下，选择设备与 SNMP 管理站之间通信的接口类型。您可以选择设备的管理接口或可用的安全区域/命名接口。

- **设备管理接口 (Device Management Interface)** - 设备和 SNMP 管理站之间通过管理接口进行通信。

- 当您选择此接口进行 SNMPv3 轮询时，系统将允许所有已配置的 SNMPv3 用户进行轮询，而不限于步骤 步骤 6， 第 29 页中选择的用户。此处，SNMPv3 主机不允许 SNMPv1 和 SNMPv2c。
- 当您为 SNMPv1 和 SNMPv2c 轮询选择此接口时，轮询完全不受步骤 步骤 5， 第 29 页中所选版本的限制。

- **安全区域或命名接口 (Security Zones or Named Interface)** - 设备和 SNMP 管理站之间通过安全区域或接口进行通信。
  - 在**可用区域 (Available Zones)** 字段中搜索区域。
  - 添加包含设备可通过其与管理站通信的接口的区域至 **选择的区域/接口 (Selected Zone/Interface)** 字段中。对于不在区域中的接口，您可以在**所选区域/接口**列表下方的字段中键入接口名称，然后点击**添加**。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 11 点击**确定 (OK)**。

步骤 12 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SNMP 陷阱

使用“SNMP 陷阱”为 威胁防御 设备配置 SNMP 陷阱（事件通知）。 陷阱不同于浏览；它们是特定事件（例如上行链路、下行链路和系统日志事件）的从 威胁防御设备到管理站的未经请求的“注释"。该设备的 SNMP 对象 ID (OID) 显示在从设备发送的 SNMP 事件陷阱中。

某些陷阱不适用于某些硬件型号。如果将策略应用于其中某个型号，则这些陷阱将被忽略。例如，并非所有型号都有可现场更换的设备，因此不会在这些型号上配置**现场可更换的设备插入/删除**陷阱。

SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 威胁防御软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

从以下位置浏览思科 MIB、陷阱和 OID 的完整列表：

SNMP 对象导航器

此外，从以下位置通过 FTP 下载思科 OID：

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 使用 **SNMP** > **SNMP 陷阱** 为 威胁防御 设备配置 SNMP 陷阱（事件通知）。

步骤 3 选择适当的“启用陷阱”选项。您可以选择其中任一或两个选项。

a) 选中**启用所有 SNMP 陷阱**可在随后的四个部分中快速选择所有陷阱。

b) 选中**启用所有系统日志陷阱**以启用与陷阱相关的系统日志消息的传输。

注释 SNMP 陷阱预计近乎是实时的，因此优先级高于 威胁防御发出的其他通知消息。启用所有 SNMP 或系统日志陷阱时，SNMP 进程可能会消耗代理和网络中的过多资源，导致系统挂起。如果您发现系统延迟、未完成的请求或超，可以选择性地启用 SNMP 和系统日志陷阱。您也可以限制按严重性级别或消息 ID 生成系统日志消息的速率。例如，所有以数字 212 开头的系统日志消息 ID 都与 SNMP 类相关联。请参阅限制系统日志消息生成速率，第 44 页。

步骤 4 默认情况下，为现有策略启用**标准**部分中的事件通知陷阱：

- **身份验证** - 未经授权的 SNMP 访问。对于具有不正确的社区字符串的数据包，将会出现此身份验证失败。
- **上行链路 (Link Up)** - 设备的一个通信链路已变为可用（已“出现"），如通知中所示。
- **下行链路 (Link Down)** - 设备的一个通信链路已出现故障，如通知中所示。
- **冷启动 (Cold Start)** - 设备正在重新初始化自身，以使其配置或协议实体实现可能被更改。
- **热启动 (Warm Start)** - 设备正在重新初始化自身，以使其配置或协议实体实现不更改。

步骤 5 在**实体 MIB** 部分中选择所需的事件通知陷阱：

- **现场可更换设备插入** - 已插入现场可更换单元 (FRU)，如通知中所示。（FRU 包括电源、风扇、处理器模块、接口模块等组件）
- **现场可更换设备删除** - 已删除现场可更换单元 (FRU)，如通知中所示。
- **配置更改** - 已发生硬件更改，如通知中所示

步骤 6 在**资源**部分中选择所需的事件通知陷阱：

- **已达到连接限制** - 此陷阱指示连接尝试被拒绝，因为已达到配置的连接限制。

步骤 7 在**其他**部分中选择所需的事件通知陷阱：

- **NAT 数据包丢弃** - 此通知在 NAT 功能丢弃 IP 数据包时生成。可用的网络地址转换地址或端口已低于所配置的阈值。
- **CPU 上升阈值 (CPU Rising Threshold)** - 在配置的时间段内，当 CPU 使用率上升超过预定义阈值时，生成此通知。选中此选项可启用 CPU 上升阈值通知：

- **百分比 (Percentage)** - 对于高阈值通知，默认值为 70%；范围介于 10% 和 94% 之间。临界阈值硬编码为 95%。
- **期间 (Period)** - 默认监控周期为 1 分钟；范围介于 1 到 60 分钟之间。

- **内存上升阈值 (Memory Rising Threshold)** - 当内存利用率上升超过预定义阈值时，会生成此通知，从而减少可用内存。选中此选项可启用内存上升阈值通知：
  - **百分比 (Percentage)** - 对于高阈值通知，默认值为 70%；范围介于 50% 和 95% 之间。
- **故障转移 (Failover)** - 当 CISCO-UNIFIED-FIREWALL-MIB 报告的故障切换状态发生变化时，生成此通知。
- **集群 (Cluster)** - 当 CISCO-UNIFIED-FIREWALL-MIB 报告集群运行状况发生变化时，生成此通知。
- **对等体摆动** - 当存在 BGP 路由摆动（即 BGP 系统发送过多的更新消息来通告网络可访问性信息）时，生成此通知。

步骤 8 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置系统日志

您可以为 威胁防御设备启用系统日志记录（系统日志）。日志记录信息可以帮助您发现并隔离网络或设备配置问题。您还可以将一些安全事件发送到系统日志服务器。以下主题介绍日志记录以及如何配置日志记录。

关于系统日志

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

表 *10: ...*的系统日志 *Cisco Secure Firewall Threat Defense*

与以下各项相关的日志	详细信息	配置位置
设备和系统运行状况、网络配置	此系统日志配置可为在数据平面上运行的功能（即在 CLI 配置中定义的功能，可以使用 **show running-config** 命令查看这些功能）生成消息。这包括诸如路由、VPN、数据接口、DHCP 服务器、NAT 等功能。数据平面系统日志消息将被编号，并且这些消息与运行 ASA 软件的设备所生成的那些消息相同。但是，Cisco Secure Firewall Threat Defense不一定会生成每种可用于 ASA 软件的消息类型。有关这些消息的信息，请参阅思科 *Cisco Secure Firewall Threat Defense*系统日志消息，网址为：https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html。此配置将在以下主题中加以说明。	**平台设置**
安全事件	此系统日志配置会生成文件和恶意软件、连接、安全情报和入侵事件的警报。	访问控制策略中的**平台设置**和 **日志记录**
（所有设备） 策略、规则和事件	此系统日志配置将为访问控制规则、入侵规则和中所述的其他高级服务生成警报，如 《Cisco Secure Firewall Management Center 管理指南》中的配置支持警报响应。这些消息不会被编号。有关配置这种类型的系统日志的信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 创建系统日志警报响应 。	访问控制策略中的**警报响应**和 **日志记录**

可以配置多个系统日志服务器，并可控制发送到每个服务器的消息和事件。还可配置不同目标，如控制台、邮件、内部缓冲区等。

严重性级别

下表列出系统日志消息严重性级别。

表 *11:* 系统日志消息严重级别

级别号	严重性级别	说明
0	**应急**	系统不可用。
1	**警报**	需要立即采取措施。
2	**严重**	严重情况。
3	**错误**	错误情况。
4	**警告**	警告情况。
5	**通知**	正常但重大的情况。

级别号	严重性级别	说明
6	**信息性**	消息仅供参考。
7	**调试**	消息仅供调试。 调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。

注释 ASA 和 威胁防御 不会生成严重性级别为零 (emergencies) 的系统日志消息。

系统日志消息过滤

您可以过滤生成的系统日志消息，以便仅将某些系统日志消息发送到特定输出目标。例如，您可以将 威胁防御设备 配置为将所有系统日志消息发送至一个输出目标，而将这些系统日志消息中的一部分发送至其他输出目标。

具体而言，您可以根据以下条件将系统日志消息定向到输出目标：

- 系统日志消息 ID 号

  （这不适用于连接和入侵事件等安全事件的系统日志消息。）

- 系统日志消息严重性级别
- 系统日志消息类（相当于一个功能区）

  （这不适用于连接和入侵事件等安全事件的系统日志消息。）

通过创建一个在设置输出目标时可以指定的消息列表来自定义这些条件。或者，可以将 威胁防御设备 配置为将一个特定的消息类发送至每种类型的输出目标，而不管消息列表是什么。

（消息列表不适用于连接和入侵事件等安全事件的系统日志消息。）

系统日志消息类

注释 此主题不适用于安全事件（连接、入侵等）的消息。

可以通过两种方法使用系统日志消息类：

- 指定整个类别的系统日志消息的输出位置。使用 **logging class** 命令。
- 创建指定消息类的消息列表。使用 **logging list** 命令。

系统日志消息类提供一个按类型将系统日志消息分类的方法，相当于设备的特性或功能。例如，RIP 类表示 RIP 路由。

特定类中的所有系统日志消息共享其系统日志消息 ID 号中相同的前三位数字。例如，所有以数字 611 开头的系统日志消息 ID 都与 vpnc（VPN 客户端）类相关联。与 VPN 客户端功能相关联的系统日志消息范围从 611101 至 611323。

此外，大多数 ISAKMP 系统日志消息都具有公用预置对象集来帮助识别隧道。这些对象在适用时前置于系统日志消息的描述性文本。如果在生成系统日志消息时对象未知，则不显示特定的 heading = value 组合。

对象的前缀如下：

Group = *groupname*, Username = *user*, IP = *IP_address*

其中组是隧道组，用户名是来自本地数据库或 AAA 服务器的用户名，IP 地址是远程访问客户端或第 2 层对等体的公用 IP 地址。

下表列出消息类以及每个类中的消息 ID 范围。

表 *12:* 系统日志消息类和关联的消息 *ID* 号

类别	定义	系统日志消息 ID 号
auth	用户身份验证	109、113
-	访问列表	106
-	应用防火墙	415
bridge	透明防火墙	110、220
ca	PKI 证书颁发机构	717
citrix	Citrix Client	723
-	集群	747
-	卡管理	323
config	命令界面	111、112、208、308
csd	安全桌面	724
cts	Cisco TrustSec	776
dap	动态访问策略	734
eap, eapoudp	用于网络准入控制的 EAP 或 EAPoUDP	333、334
eigrp	EIGRP 路由	336
电子邮件	邮件代理	719
-	环境监控	735
ha	故障切换	101、102、103、104、105、210、311、709

类别	定义	系统日志消息 ID 号
-	基于身份认证的防火墙	746
ids	入侵检测系统	400、733
-	IKEv2 工具包	750、751、752
ip	IP 堆栈	209、215、313、317、408
ipaa	IP 地址分配	735
ips	入侵保护系统	400、401、420
-	IPv6	325
-	僵尸网络流量过滤。	338
-	许可	444
mdm-proxy	MDM 代理	802
nac	网络准入控制	731、732
nacpolicy	NAC 策略	731
nacsettings	配置 NAC 设置，以应用 NAC 策略	732
-	网络无线接入点	713
np	网络处理器	319
-	NP SSL	725
ospf	OSPF 路由	318、409、503、613
-	密码加密	742
-	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
-	Smart Call Home	120
session	用户会话	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
-	ScanSafe	775

类别	定义	系统日志消息 ID 号
ssl	SSL 堆栈	725
svc	SSL VPN 客户端	722
sys	System	199、211、214、216、306、307、315、414、604、605，606、610、612、614、615、701、711、741
-	威胁检测	733
tre	事务规则引擎	780
-	UC-IME	339
标记交换	服务标记交换	779
vm	VLAN 映射	730
vpdn	PPTP 和 L2TP 会话	213、403、603
vpn	IKE 和 IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN 客户端	611
vpnfo	VPN 故障切换	720
vpnlb	VPN 负载均衡	718
-	VXLAN	778
webfo	WebVPN 故障切换	721
webvpn	WebVPN 和 AnyConnect 客户端	716
-	NAT 与 PAT	305

日志记录准则

本节介绍您在配置日志记录之前应审阅的准则和限制。

IPv6 准则

- 支持 IPv6。可以使用 TCP 或 UDP 发送系统日志。
- 确保配置用于发送系统日志的接口已经启用，支持 IPv6，并且可以通过指定接口到达系统日志服务器。
- 不支持通过 IPv6 进行安全登录。

其他准则

- 请勿配置 管理中心 为主系统日志服务器。 管理中心 可以记录一些系统日志。但是，它没有足够的存储调配来容纳来自每个传感器的连接事件的大量信息，尤其是在使用多个传感器并且都发送系统日志时。
- 系统日志服务器必须运行一个名为 syslogd 的服务器程序。Windows 提供了一个系统日志服务器，作为其操作系统的组成部分。
- 要查看由 威胁防御设备 生成的日志，必须指定日志记录输出目标。如果启用日志记录而未指定日志记录输出目标，则 威胁防御设备 会生成消息，但不会将其保存到可对其进行查看的位置。必须单独指定每个不同的日志记录输出目标。
- 如果您使用 TCP 作为传输协议，系统会打开与系统日志服务器的 4 个连接，以确保消息不会丢失。如果您使用系统日志服务器从大量设备收集消息，并且合并的连接开销对该服务器来说太大，请改用 UDP。
- 不能将两个不同的列表或类分配给不同的系统日志服务器或相同位置。
- 您最多可以配置 16 个系统日志服务器。
- 应该可以通过 威胁防御设备 到达系统日志服务器。应将该设备配置为拒绝可以从其到达系统日志服务器的接口上的 ICMP 不可达消息，并将系统日志发送到同一服务器。请确保已对所有严重性级别启用日志记录。要防止系统日志服务器崩溃，请抑制系统日志 313001、313004 和 313005 的生成。
- 用于系统日志的 UDP 连接数与硬件平台上的 CPU 数量和您配置的系统日志服务器数量直接相关。在任何时刻，UDP 系统日志连接的数量都等于 CPU 数量乘以已配置的系统日志服务器数量的积。这是预期行为。请注意，全局 UDP 连接空闲超时适用于这些会话，默认值为 2 分钟。如果您想更快关闭这些会话，可以调整该设置，但超时适用于所有 UDP 连接，而不仅是系统日志。
- 当 威胁防御设备 通过 TCP 发送系统日志时，在系统日志服务重新启动后，需要大约一分钟来启动连接。

配置 FTD 设备的系统日志日志记录

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 39 页。

要配置系统日志设置，请执行以下步骤：

开始之前

请参阅日志记录准则，第 37 页中的要求。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 从目录中选择**系统日志**。

步骤 3 点击**日志记录设置 (Logging Setup)** 以启用日志记录，指定 FTP 服务器设置，并指定闪存用法。有关详细信息，请参阅启用日志记录并配置基本设置，第 40 页

步骤 4 点击**日志记录目标 (Logging Destinations)** 可以启用对特定目标的日志记录，并指定对邮件严重性级别、事件类或自定义事件列表的过滤。有关详细信息，请参阅启用日志记录目标，第 41 页

必须启用日志记录目标才能查看该目标的消息。

步骤 5 点击**邮件设置 (E-mail Setup)** 以指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。有关详细信息，请参阅将系统日志消息发送给邮件消息，第 42 页

步骤 6 点击**事件列表 (Events List)** 可定义包括事件类、严重性级别和事件 ID 的自定义事件列表。有关详细信息，请参阅创建自定义事件列表，第 43 页

步骤 7 点击**速率限制 (Rate Limit)** 可指定发送到所有配置的目标的邮件数量，并定义要为其分配速率限制的邮件严重性级别。有关详细信息，请参阅限制系统日志消息生成速率，第 44 页

步骤 8 点击**系统日志设置 (Syslog Settings)** 以指定日志记录设施，启用时间戳包含，并启用其他设置以将服务器设置为一个系统日志目标。有关详细信息，请参阅配置系统日志设置，第 44 页

步骤 9 点击**系统日志服务器 (Syslog Servers)** 以便为指定为日志记录目标的系统日志服务器指定 IP 地址、使用的协议、格式和安全区域。有关详细信息，请参阅配置系统日志服务器，第 46 页

适用于安全事件系统日志消息的 威胁防御 平台设置

“安全事件”包括连接、安全情报、入侵以及文件和恶意软件事件。

设备 > 平台设置 > 威胁防御设置 > 系统日志 页面及其选项卡上的某些系统日志设置适用于安全事件的系统日志消息，但大多数只适用于与系统运行状况和网络有关的事件的信息。

以下设置适用于安全事件的系统日志消息：

- **日志记录设置**选项卡：
  - **发送 EMBLEM 格式的系统日志**
- **系统日志设置**选项卡：
  - **在系统日志消息中启用时间戳**
  - **时间戳格式**
  - **启用系统日志设备 ID**
- **系统日志服务器**选项卡：
  - **添加系统日志服务器**表单 （以及已配置的服务器列表） 上的所有选项。

启用日志记录并配置基本设置

您必须为系统启用日志记录，才能为数据平面事件生成系统日志消息。

您还可以将闪存或 FTP 服务器上的存档设置为本地缓冲区已满时使用的存储位置。您可以在保存日志记录数据后对其进行操作。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

下面的过程介绍了一些基本系统日志设置。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 威胁防御 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 39 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **日志记录设置**。

步骤 3 启用日志记录并配置基本日志记录设置。

- **启用日志记录** - 为 威胁防御设备启用数据平面系统日志记录。
- **在故障切换备用设备上启用日志记录** - 为 威胁防御设备的备用设备（如果有）启用日志记录。
- **以 EMBLEM 格式发送系统日志** - 为每个日志记录目标启用 EMBLEM 格式日志记录。如果启用 EMBLEM，必须使用 UDP 协议来发布系统日志消息，EMBLEM 与 TCP 不兼容。

  注释 RFC5424 格式的系统日志消息通常显示优先级值（PRI）。但是，在 管理中心中，只有当您启用 Cisco EMBLEM 格式的日志记录时，才会显示受管 威胁防御的系统日志消息中的 PRI 值。有关 PRI 的详细信息，请参阅 RFC5424。

- **发送调试消息作为系统日志** - 将所有调试跟踪输出重定向到系统日志。如果启用了此选项，则控制台中不会显示系统日志消息。因此，要查看调试消息，必须在控制台上启用日志记录并将其配置为调试系统日志消息编号和日志记录级别的目标。使用的系统日志消息编号是 711001。此系统日志的默认日志记录级别为调试。
- **内部缓冲区的内存大小** - 指定在启用了日志记录缓冲区的情况下，将系统日志消息保存到的内部缓冲区的大小。当缓冲区填满时，它将被覆盖。默认值为 4096 字节。范围为 4096 到 52428800。

步骤 4 （可选）通过选中**为 FMC 启用日志记录**复选框启用 VPN 日志记录。从**日志记录级别**下拉列表中选择 VPN 消息的系统日志严重性级别。

有关级别的信息，请参阅严重性级别，第 33 页。

步骤 5 （可选）如果要在覆盖缓冲区之前将日志缓冲区内容保存到 FTP 服务器，请配置该服务器。指定 FTP 服务器信息。

- **FTP 服务器缓冲区回绕** - 要在缓冲区内容被覆盖之前将其保存到 FTP 服务器，请选中此框并在以下字段中输入必要的目标信息。要删除 FTP 配置，请取消选择此选项。

- **IP 地址** - 选择包含 FTP 服务器 IP 地址的主机网络对象。
- **用户名** - 输入连接到 FTP 服务器时要使用的用户名。
- **路径** - 输入相对于 FTP 根目录的路径，缓冲区内容应保存在此处。
- **密码/确认** - 输入并确认用于对访问 FTP 服务器的用户名进行身份验证的密码。

步骤 6 （可选）如果要在覆盖缓冲区之前将日志缓冲区内容保存到闪存，请指定闪存大小。

- **闪存** - 要在缓冲区内容被覆盖之前将其保存到闪存，请选中此框。
- **日志记录所使用的最大闪存大小 (KB)** - 指定用于日志记录的闪存所使用的最大空间（以 KB 为单位）。范围为 4 至 8044176 千字节。
- **要保留的最小可用空间 (KB)** - 指定要在闪存中保留的最小可用空间（以 KB 为单位）。范围为 0 至 8044176 千字节。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

启用日志记录目标

必须启用日志记录目标才能查看该目标的消息。启用目标时，还必须为该目标指定消息过滤器。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数FTD平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 39 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **日志记录目标**。

步骤 3 点击**添加**以启用目标并应用日志记录过滤器，或编辑现有目标。

步骤 4 在**日志记录目标**对话框中，选择目标并配置用于目标的过滤器：

a) 在**日志记录目标**下拉列表中，选择要启用的目标。您可以为每个目标创建一个过滤器：控制台、邮件、内部缓冲区、SNMP 陷阱、SSH 会话和系统日志服务器。

注释 控制台和 SSH 会话日志记录只有在诊断 CLI 中工作。输入 **system support diagnostic-cli**。

b) 在**事件类**中，选择将应用于表中未列出的所有类的过滤器。

您可以配置这些过滤器：

- **基于严重性过滤** - 选择严重性级别。此级别或更高级别的消息将会发送到目标
- **使用事件列表** - 选择定义过滤器的事件列表。在**事件列表 (Event Lists)** 页面上创建这些列表。

- **禁用日志记录** - 阻止消息发送到此目标。

c) 如果要为每个事件类创建过滤器，请点击**添加**以创建新过滤器，或编辑现有过滤器，然后选择事件类和严重性级别以限制该类中的消息。点击**确定**以保存过滤器。

有关事件类的说明，请参阅系统日志消息类，第 34 页。

d) 点击**确定**。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

将系统日志消息发送给邮件消息

您可以设置以邮件形式发送的系统日志消息收件人列表。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 39 页。

开始之前

- 在 SMTP 服务器平台设置页面上配置 SMTP 服务器
- 启用日志记录并配置基本设置，第 40 页
- 启用日志记录目标

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **邮件设置**。

步骤 3 指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。

步骤 4 点击 **Add** 以输入指定的系统日志消息的新邮件地址收件人。

步骤 5 从下拉列表中选择发送给收件人的系统日志消息的严重性级别。

用于目标邮件地址的系统日志消息严重性过滤器会导致发送指定严重性级别和更高严重性级别的消息。有关级别的信息，请参阅严重性级别，第 33 页。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

创建自定义事件列表

事件列表是一个自定义筛选器，您可以将其应用于日志记录目标，以控制将哪些消息发送到目标。通常，只根据严重性来筛选目标消息，但可以使用事件列表根据事件类、严重性和消息标识符 (ID) 组合进一步控制要发送的消息。

创建自定义事件列表分为两步。在**事件列表 (Event Lists)** 中创建自定义列表，然后使用事件列表在**日志记录目标 (Logging Destinations)** 中为各种类型的目标定义日志记录筛选。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 39 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **事件列表**。

步骤 3 配置事件列表。

a) 点击**添加**以添加新列表或编辑现有列表。

b) 在**名称**字段中输入事件列表的名称。不允许使用空格。

c) 要根据严重性或事件类来标识消息，请选择**严重性/事件类**选项卡，并添加或编辑条目。

有关可用类的信息，请参阅系统日志消息类，第 34 页。

有关级别的信息，请参阅严重性级别，第 33 页。

某些事件类在透明模式下不适用于该设备。如果配置了此类选项，将绕过这些选项，不予以部署。

d) 若要通过消息 ID 明确标识消息，请选择**消息 ID (Message ID)**，并添加或编辑 ID。

您可以使用连字符输入 ID 范围，例如 100000-200000。ID 是六位数字。有关初始三位数字如何映射到功能的信息，请参阅系统日志消息类，第 34 页。

有关特定的消息编号，请参阅 Cisco ASA 系列日志消息。

e) 点击**确定**保存事件列表。

步骤 4 点击**日志记录目标 (Logging Destinations)**，然后添加或编辑应使用过滤器的目标。

请参阅启用日志记录目标，第 41 页。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

限制系统日志消息生成速率

您可以限制按严重性级别或消息ID生成系统日志消息的速率。您可以为每个日志记录级别和每个系统日志消息 ID 指定单独的限制。如果设置冲突，则会优先考虑系统日志消息 ID 限制。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数FTD平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 39 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **速率限制**。

步骤 3 要按严重性级别限制邮件生成，请点击**日志记录级别 (Logging Level)** > **添加 (Add)**，然后配置以下选项：

- **日志记录级别** - 您要限制速率的严重性级别。有关级别的信息，请参阅严重性级别，第 33 页。
- **消息数** - 在指定时间段内允许的指定类型的最大消息数。
- **间隔** - 在速率限制计数器重置之前的秒数。

步骤 4 点击**确定**。

步骤 5 要按系统日志消息 ID 限制邮件生成，请点击**系统日志级别 (Syslog Level)** > **添加 (Add)**，然后配置以下选项：

- **系统日志 ID** - 您要限制速率的系统日志消息 ID。有关特定消息编号，请参阅思科 ASA 系列系统日志消息。
- **消息数** - 在指定时间段内允许的指定类型的最大消息数。
- **间隔** - 在速率限制计数器重置之前的秒数。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置系统日志设置

可以配置一般系统日志设置，以设置要包括在将被发送到系统日志服务器的系统日志消息中的设备代码；指定是否在每条消息中包括时间戳；指定是否将设备ID包括在消息中；查看和修改消息的严重性级别；以及禁用特定消息的生成。

如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则此页面上的某些设置不适用于这些消息。另请参阅《Cisco Secure Firewall Management Center 管理指南》中的适用于安全事件系统日志消息的威胁防御平台设置。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 依次选择**系统日志** > **系统日志设置**。

步骤 3 在**设备**下拉列表中为系统日志服务器选择要用作文件消息基础的系统日志设备。

默认值为大多数 UNIX 系统期望的 LOCAL4(20)。但是，由于网络设备共享可用设备，因此可能需要为系统日志更改此值。

设施值通常与安全事件无关。

步骤 4 选中**在每个系统日志消息上启用时间戳**复选框, 以包括在系统日志消息中生成消息的日期和时间。

步骤 5 选择系统日志消息的**时间戳格式**：

- 传统 (MMM dd yyyy HH:mm:ss) 格式为系统日志消息的默认格式。

  选择此时间戳格式时，消息不会指示时区，该时区始终为 UTC。

- RFC 5424 (yyyy-MM-ddTHH:mm:ssZ) 使用 RFC 5424 系统日志格式中指定的 ISO 8601 时间戳格式。

  如果选择RFC 5424格式，则会在每个时间戳的末尾附加“Z”，以指示时间戳使用UTC时区。

步骤 6 如果希望向系统日志消息添加设备标识符（它将被放置在消息的开头），则请选中**启用系统日志设备 ID** 复选框，然后选择 ID 的类型。

- **接口** - 使用所选接口的 IP 地址，无论设备通过哪个接口发送消息。选择标识接口的安全区。该区域必须映射到某一接口。
- **用户定义的 ID** - 使用所选的文本字符串（最多 16 个字符）。
- **主机名** - 使用设备的主机名。

步骤 7 使用“系统日志消息”表来更改特定系统日志消息的默认设置。仅当希望更改默认设置时，才需要此表中的配置规则。可以更改分配给消息的严重性，或者可以禁用消息的生成。

默认情况下，将启用 Netflow，并在表中显示条目。

a) 要抑制因 Netflow 而冗余的系统日志消息，请选择 **Netflow 等效系统日志**。

这会将消息作为受抑制的消息添加到该表中。

注释 如果其中任何等效系统日志已经位于该表中，则不会覆盖现有规则。

b) 要添加新规则，请点击**添加 (Add)**。

c) 如果希望更改所选消息编号的配置，则请进入**系统日志 ID** 下拉列表，然后从**日志记录级别**下拉列表中选择新的严重性级别，或者选择**已抑制**以禁用消息的生成。通常不会更改严重性级别并禁用消息，但如果需要，可以对这两个字段进行更改。

d) 点击**确定**以将规则添加到该表中。

步骤 8 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

- 部署配置更改。

配置系统日志服务器

要配置系统日志服务器，以处理您的系统生成的消息，请执行以下步骤。

如果您希望此系统日志服务器接收连接和入侵事件等安全事件，另请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 39 页。

开始之前

- 请参阅日志记录准则，第 37 页中的要求。
- 请确保您的设备可以通过网络访问您的系统日志收集器。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 依次选择**系统日志** > **系统日志服务器**。

步骤 3 如果任何使用 TCP 协议的系统日志服务器关闭，则请选中**在系统日志服务器关闭时允许用户流量传递**复选框，以允许流量。

步骤 4 在**消息队列大小（消息）(Message queue size [messages])** 字段中输入当系统日志服务器繁忙时安全应用上用于存储系统日志消息的队列的大小。最小值为 1 条消息。默认值为 512。指定 0 可允许不限数量的消息排队（受可用块内存约束）。

当消息超过配置的队列大小时，它们会被丢弃并导致系统日志丢失。要确定理想的队列大小，您需要确定可用的块内存。使用 **show blocks** 命令了解当前内存使用率。有关命令及其属性的详细信息，请参阅《*Cisco Secure Firewall ASA* 系列命令参考指南》。如需进一步帮助，请与思科 TAC 联系。

步骤 5 点击 **Add** 以添加新系统日志服务器。

a) 在 **IP 地址**下拉列表中，选择包含系统日志服务器 IP 地址的网络主机对象。

b) 选择协议（TCP 或 UDP），然后输入用于 威胁防御设备与系统日志服务器之间通信的端口号。

UDP 比 TCP 更快，并且在设备上使用的资源更少。

默认 UDP 端口为 514。您必须为 TCP 手动配置端口 1470。任一协议的有效非默认端口值为 1025 至 65535。

c) 选中 **Log messages in Cisco EMBLEM format (UDP only)** 复选框以指定是否记录思科 EMBLEM 格式的消息（仅在选择 UDP 作为协议的情况下才可用）。

注释 RFC5424格式的系统日志消息通常显示优先级值（PRI）。但是，在管理中心中，只有当您启用Cisco EMBLEM格式的日志记录时，才会显示受管 威胁防御 的系统日志消息中的PRI值。有关PRI的详细信息，请参阅RFC5424。

d) 选中**启用安全系统日志**复选框，以使用SSL/TLS over TCP对设备与服务器之间的连接进行加密。

注释 必须选择TCP作为协议才能使用此选项。还必须在 **设备** > **证书** 页面上上传与系统日志服务器通信所需的证书。最后，将该证书从威胁防御设备上传到系统日志服务器，以完成安全关系，并允许其对流量进行解密。设备管理界面不支持 **启用安全系统日志** 选项。

e) 选择**设备管理接口**或**安全区域或指定接口**，以与系统日志服务器通信。

- **设备管理接口**：从管理接口发送系统日志。 我们建议您在配置Snort事件的系统日志时使用此选项。

  注释 **设备管理界面** 选项不支持 **启用安全系统日志** 选项。

- **安全区域或指定接口**：从**可用区域**列表中选择接口，然后点击**添加**。

f) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

- 部署配置更改。

配置全局超时

可以设置各种协议的连接和转换插槽的全局空闲超时持续时间。如果插槽在指定的空闲时间内未使用，资源将返回到空闲池。

还可以为设备的控制台会话设置超时。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**超时**。

步骤 3 配置要更改的超时。

对于任何给定的设置，请选择**自定义**来定义您自己的值，选择**默认**将恢复系统默认值。在大多数情况下，最大超时为1193小时。

您可以通过选择**禁用**来禁用某些超时。

- **控制台超时** - 关闭到控制台的连接之前的空闲时间，范围为0 或 5 到 1440 分钟。默认超时时间为 0，表示会话不会超时。如果更改该值，现有的控制台会话将使用原来的超时值。新值仅适用于新连接。
- **转换插槽** - NAT 转换插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 3 小时。
- **连接** - 连接插槽释放前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 1 小时。
- **半封闭** - TCP 半闭合连接关闭前的空闲时间。如果同时收到 FIN 和 FIN-ACK，则连接会被认为是半关闭的。如果只看到了 FIN，则常规连接超时适用。最小值为 30 秒。默认值为 10 分钟。
- **UDP** - UDP 连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。
- **ICMP** - 通用 ICMP 状态关闭前的空闲时间。默认值（及最小值）是 2 秒。
- **RPC/Sun RPC** - SunRPC 插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 10 分钟。

  在基于 Sun RPC 的连接中，当父连接被删除或出现超时时，新的子连接可能不会被视为父-子连接的一部分，因此可以根据策略或系统中设置的规则来评估新的连接。父连接超时后，现有的子连接仅在达到超时值集之前有效。
- **H.225** - H.225 信令连接关闭前的空闲时间。默认值为 1 小时。若要在清除所有调用后立即关闭连接，建议使用超时值 1 秒 (0:0:1)。
- **H.323** - TH.245 (TCP) 和 H.323 (UDP) 媒体连接关闭前的空闲时间。默认值（和最小值）为 5 分钟。由于 H.245 和 H.323 媒体连接上设置的连接标志相同，因此 H.245 (TCP) 连接与 H.323（RTP 和 RTCP）媒体连接共享空闲超时。
- **SIP** - SIP 信令端口连接关闭前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 30 分钟。
- **SIP 媒体** - SIP 媒体端口连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。SIP 媒体计时器用于具有 SIP UDP 媒体数据包的 SIP RTP/RTCP，而不是 UDP 非活动超时。
- **SIP 断开连接** - 在 CANCEL 或 BYE 消息未收到 200 OK 的情况下，SIP 会话删除之前的空闲时间，该值介于 0:0:1 至 00:10:0 之间。默认值为 2 分钟 (0:2:0)。
- **SIP 邀请** - PROVISIONAL 响应和媒体转换的针孔关闭前的空闲时间，该值介于 0:1:0 至 00:30:0 之间。默认值为 3 分钟 (0:3:0)。
- **SIP 临时媒体** - SIP 临时媒体连接的超时值，该值介于 1 至 30 分钟之间。默认值为 2 分钟。
- **Floating Connection** - 当某个网络存在具有不同指标的多个路由时，系统会使用连接创建时指标最佳的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。为了可以使用更好的路由，请将超时设置为 0:0:30 至 1193:0:0 之间的值。
- **Xlate PAT** - PAT 转换插槽释放前的空闲时间，该值介于 0:0:30 至 0:5:0 之间。默认值为 30 秒。如果上游路由器拒绝使用释放的 PAT 端口的新连接，您可能会想要增加超时，因为以前的连接在上游设备中可能仍处于开放状态。

- **TCP 代理重组** - 等待重组的缓冲数据包丢弃前的空闲时间，该值介于 0:0:10 到 1193:0:0 之间。默认值为 1 分钟 (0:1:0)。
- **ARP 超时** - ARP 表重建之间的秒数，从 60 到 4294967。默认值为 14,400 秒（4 小时）。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

为威胁防御配置 NTP 时间同步

使用网络时间协议 (NTP) 服务器同步设备上的时钟设置。建议您将 管理中心 托管的所有 威胁防御 配置为使用同一台 NTP 服务器作为 管理中心。威胁防御 直接从配置的NTP服务器获取时间。如果 威胁防御 配置的NTP服务器由于任何原因无法访问，则会与 管理中心 同步时间。

设备支持 NTPv4。

注释 如果要在 Firepower 4100/9300 机箱上部署 威胁防御，则必须在 Firepower 4100/9300 机箱上配置 NTP，以便智能许可正常运行，并确保设备注册采用正确的时间戳。对于 Firepower 4100/9300 机箱和 管理中心，应使用相同的 NTP 服务器。

开始之前

- 如果您的组织有 威胁防御 可以访问的一个或多个NTP服务器，请在 管理中心 上的**系统 (System)** > **配置 (Configuration)** 页面上为已为时间同步配置的设备使用相同的 NTP 服务器。
- 如果您选择了**仅当为配置 NTP 服务器**管理中心时使用仅通过身份验证的NTP服务器管理中心，则对于您的设备，仅使用配置为通过进行身份验证的NTP服务器。（托管设备将使用与管理中心 相同的 NTP 服务器，但其 NTP 连接将不使用身份验证。）
- 如果您的设备无法访问 NTP 服务器或您的组织没有 NTP 服务器，则必须使用以下程序中讨论的**通过防御中心通过 NTP** 选项。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**时间同步 (Time Synchronization)**。

步骤 3 配置以下时钟选项之一：

- **通过 NTP 从防御中心** -（默认）。托管设备从为 管理中心 配置的 NTP 服务器（经过身份验证的 NTP 服务器除外）获取时间，并直接与这些服务器同步时间。但是，如果满足以下任一条件，则托管设备将从 管理中心 同步时间：

- 设备无法访问 管理中心 的 NTP 服务器。
- 管理中心 没有未经身份验证的服务器。

- **通过网络上的 NTP (Via NTP from)**：如果您的 管理中心使用的是网络上的 NTP 服务器，请选择此选项，并输入您在**系统 (System) > 配置 (Configuration) > 时间同步 (Time Synchronization)** 中指定的同一 NTP 服务器的完全限定 DNS 名称（例如 ntp.example.com）或 IPv4 或 IPv6 地址。如果无法访问 NTP 服务器，则 管理中心将充当 NTP 服务器。

步骤 4 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

为策略应用配置设备时区

默认情况下，系统使用 UTC 时区。要为设备指定不同的时区，请使用此程序。

您指定的时区将仅用于支持此功能的策略中基于时间的策略应用。

注释 从 FMC 7.0 开始，Snort 3 也支持基于时间的 ACL。

过程

步骤 1 依次选择**设备 (Devices)** > **平台设置 (Platform Settings)**，并创建或编辑 威胁防御 策略。

您还可以从 **对象 >对象管理 > 时区** 页面创建时区对象。

步骤 2 通过点击 +创建新的时区对象。

步骤 3 选择时区。

步骤 4 点击**保存**。

下一步做什么

- 创建时间范围对象，在访问控制和预过滤器规则中选择适用的时间范围，并将父策略分配给与正确时区关联的设备。
- 部署配置更改。

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。