系统设置

以下主题介绍如何配置一起划分到“系统设置”(System Settings) 页面的各种系统设置。这些设置涵盖整个系统功能。

配置管理访问

管理访问指能够登录到 Firewall Threat Defense 设备进行配置和监控。您可以配置以下项目：

- AAA 用于确定要用于用户访问身份验证的身份源。您可以使用本地用户数据库或外部 AAA 服务器。有关管理用户管理的详细信息，请参阅管理防火墙设备管理器和Firewall Threat Defense用户访问。
- 针对管理接口和数据接口的访问控制。对于这些接口有单独的访问列表。您可以决定允许哪些 IP 地址访问 HTTPS（用于 防火墙设备管理器）和 SSH（用于 CLI）。请参阅配置管理访问列表，第 2 页。

- 管理 Web 服务器证书，用户必须接受它们才能连接到防火墙设备管理器。通过上传网络浏览器已信任的证书，可以避免用户被要求信任未知的证书。请参阅配置 Firewall Threat Defense Web 服务器证书，第 4 页。

配置管理访问列表

默认情况下，您可以从任何 IP 地址的管理地址访问设备的 防火墙设备管理器 Web 或 CLI 界面。系统访问仅受用户名/密码的保护。但是，您可以配置访问列表以仅允许来自特定 IP 地址或子网的连接，以进一步加强保护。

您还可以开放数据接口以允许 防火墙设备管理器 或 SSH 连接至 CLI。然后，无需使用管理地址即可管理设备。例如，您可以允许对外部接口进行管理访问，这样就能远程配置设备。用户名/密码可防止不希望看到的连接。默认情况下，对数据接口的 HTTPS 管理访问会在内部接口上启用而在外部接口上禁用。对于配备默认“内部”桥接组的 Firepower 1010 或 Secure Firewall 1210/1220，这意味着可通过桥接组内任意数据接口将 防火墙设备管理器 连接至桥接组 IP 地址（默认为 192.168.95.1）。您可以只在进入设备所通过的接口上开放管理连接。

注意 如果只允许访问特定地址，那么您可能很容易将自己锁定在系统之外。如果删除对当前所用 IP 地址的访问，并且没有“任何”地址条目，则在部署策略时将丢失对系统的访问。如果决定配置访问列表，必须非常小心。

开始之前

不能在同一接口上为同一 TCP 端口同时配置 防火墙设备管理器 访问（HTTPS 访问）和远程访问 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。如果在同一接口上配置这两个功能，请确保至少更改其中一项服务的 HTTPS 端口，以避免冲突。

过程

步骤 1 点击 **设备**，然后点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

您还可以在此页面上配置 AAA，允许外部 AAA 服务器中定义的用户进行管理访问。有关详细信息，请参阅管理防火墙设备管理器和Firewall Threat Defense用户访问。

步骤 2 要为管理地址创建规则，请执行以下操作：

a) 选择**管理接口**选项卡。

规则列表定义允许访问专用端口的地址：443 用于 防火墙设备管理器 （HTTPS 网络接口），22 用于 SSH CLI。

规则不是一个有序列表。如果一个 IP 地址与请求的端口的任意规则匹配，则用户可以尝试登录设备。

注释

要删除规则，请点击该规则的垃圾桶图标( )。如果删除了某个协议的所有规则，则没有人可以使用该协议访问该接口上的设备。

b) 点击 + 并填写以下选项：

- **协议** - 选择规则是用于 HTTPS（端口 443）还是 SSH（端口 22）。
- **IP 地址** - 选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

c) 点击**确定**。

步骤 3 要为数据接口创建规则，请执行以下操作：

a) 选择**数据接口**选项卡。

规则列表定义允许访问接口上专用端口的地址：443 用于 防火墙设备管理器（HTTPS 网络接口），22 用于 SSH CLI。

规则不是一个有序列表。如果一个 IP 地址与请求的端口的任意规则匹配，则用户可以尝试登录设备。

注释

要删除规则，请点击该规则的垃圾桶图标( )。如果删除了某个协议的所有规则，则没有人可以使用该协议访问该接口上的设备。

b) 点击 + 并填写以下选项：

- **接口** - 选择要在其上允许管理访问的接口。
- **协议** - 选择规则是用于 HTTPS（端口 443）、SSH（端口 22）还是二者。不能为远程访问 VPN 连接配置文件中使用的外部接口配置 HTTPS 规则。
- **允许的网络** - 选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

c) （可选。）如果要更改 HTTPS 数据端口编号，请点击相应编号并输入新端口。请参阅在数据接口上配置用于管理访问的 HTTPS 端口，第 3 页。

d) 点击**确定**。

在数据接口上配置用于管理访问的 HTTPS 端口

默认情况下，出于管理目的进行的设备访问（对于 防火墙设备管理器 或 Firewall Threat Defense API）会通过端口 TCP/443 进行。您可以更改数据接口的管理访问端口。

如果更改端口，用户必须在 URL 中包含自定义端口才能访问系统。例如，如果数据接口是 ftd.example.com，并且您将端口更改为 4443，则用户必须将 URL 修改为 https://ftd.example.com:4443。

所有数据接口将使用同一端口。不得为每个接口配置不同的端口。

注释 不得更改管理接口的管理访问端口。管理接口始终使用端口 443。

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击**数据接口 (Data Interfaces)** 选项卡。

步骤 3 点击 **HTTPS 数据端口 (HTTPS Data Port)** 号。

步骤 4 在“数据接口设置”对话框中，将 **HTTPS 数据端口**更改为要使用的端口。

不得指定以下端口号：

- 22，该端口号用于 SSH 连接。
- 用于远程访问 VPN 的端口（如果您已为允许用于管理访问的任何接口配置了该端口）。远程访问 VPN 默认使用端口 443，但您可以为其配置自定义端口。
- 在身份策略中该端口用于主动身份验证，默认为 885。

步骤 5 点击**确定**。

配置 Firewall Threat Defense Web 服务器证书

当您登录到 Web 界面时，系统将使用数字证书来确保使用 HTTPS 的流量安全。默认证书不受您的浏览器信任，所以您会看到不受信任的颁发机构警告，并询问您是否要信任该证书。虽然用户可以将该证书保存到受信任的根证书存储区，但您也可以上传已配置为受浏览器信任的新证书。

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

如果您已位于“系统设置”(System Settings) 页面，只需点击目录中的**管理访问 (Management Access)**。

步骤 2 点击**管理 Web 服务器 (Management Web Server)** 选项卡。

步骤 3 在 **Web 服务器证书**中，选择要用于保护 防火墙设备管理器HTTPS 连接的内部证书.

如果尚未上传或创建证书，请点击列表底部的**新建内部证书 (Create New Internal Certificate)** 链接立即创建。

默认值为预定义的 DefaultWebserverCertificate 对象。

步骤 4 如果证书不是自签名证书，请将完全信任链中的所有中间证书和根证书添加到**受信任链**列表。

您最多可以向链中添加 10 个证书。点击 **+** 添加各个中间证书，最后添加根证书。点击**保存 (Save)**（然后在警告您 Web 服务器将重启的对话框中点击**继续 (Proceed)**）时，如果证书丢失，您将收到一条错误消息，其中包含链中缺少的下一个证书的通用名称。如果添加不在链中的证书，您也会收到错误消息。仔细检查消息，确定需要添加或删除的证书。

点击 **+** 后，点击**创建新的受信任 CA 证书 (Create New Trusted CA Certificate)**，即可在此处上传证书。

步骤 5 点击**保存 (Save)**。

更改将立即应用，且系统会重新启动 Web 服务器。您无需部署配置。

请等待几分钟，在重启完成后，刷新浏览器。

自定义登录屏幕

您可以在登录屏幕上添加自定义图片，如果组织需要，还可以选择添加免责声明等文字。通过浏览器登录时会显示该图像。文本既可在浏览器中显示，也可在 SSH 登录命令行界面时显示。

开始之前

这些自定义功能在每个设备上都是独一无二的。在高可用性对中，您对活动设备所做的更改不会自动复制到备用设备；您必须分别自定义每个设备。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **登录页面**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的**登录页面 (Login Page)**。

步骤 2 配置设置；点击**重置为默认值 (Reset to Default)** 可返回到禁用自定义的默认徽标。

- **登录屏幕图像** - 选择使用**默认图像 (Default Image)** 还是**无图像 (No Image)**，它会将图像显示在用户名/密码字段的左侧。
- **其他自定义徽标** - 自定义徽标是 HTTPS 登录屏幕的附加图像，位于用户名/密码字段上方。选择**无自定义徽标 (No Custom Logo)**，或选择**显示其他自定义徽标 (Show Additional Custom Logo)**，点击**浏览文件 (Browse a File)**，然后上传用户在登录时应看到的 SVG 或 PNG 格式的图像文件。如果您为登录屏幕图像选择“无图像”(No Image)，用户将只看到此自定义图像。

  图像文件必须小于 200KB。

- **显示用户文本** - 要同时向 HTTPS 和 SSH 登录屏幕添加文本，请选择此选项。然后，输入文字的标题和文字本身。例如，您可以添加警告和免责声明。用户在登录系统前必须确认已阅读并同意该文本。标题的最大大小为 64 个字符；文本的最大大小为 2048 个字符。

步骤 3 点击**预览 (Preview)** 并验证登录屏幕是否按预期显示。根据需要进行调整。

步骤 4 点击**保存**。

配置系统日志记录设置

您可以为 Firewall Threat Defense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。您可以为诊断日志记录和连接相关的日志记录（包括访问控制、入侵防御和文件及恶意软件日志记录）启用系统日志。

诊断日志记录可以为与连接不相关的事件（包括与设备和系统健康状况以及网络配置相关的事件）提供系统日志消息。可以在各个访问控制规则内配置连接日志记录。

诊断日志记录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。

有关这些消息的信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html中的 *Cisco Threat Defense* 系统日志消息 。

以下主题介绍如何配置发送到各个输出位置的诊断和文件/恶意软件消息的日志记录。

严重性级别

下表列出系统日志消息严重性级别。

表 *1:* 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。
6	信息性	消息仅供参考。

级别号	严重性级别	说明
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 Firewall Threat Defense不会生成严重性级别为零（紧急）的系统日志消息。

配置系统将日志记录发送到远程系统日志服务器

您可以配置系统将系统日志消息发送到外部系统日志服务器。这是系统日志记录的最佳选项。通过使用外部服务器，您可以提供更多空间来暂存消息，并使用服务器的功能来查看、分析和存档消息。

此外，如果您在访问控制规则中对流量应用了文件策略，来控制文件访问或恶意软件，或同时控制两者，则您可以配置系统将文件事件消息发送到外部系统日志服务器。如果您未配置系统日志服务器，则仅可在 防火墙设备管理器 事件查看器中查看事件。

以下步骤介绍了如何为诊断（数据）日志记录和文件/恶意软件日志记录启用系统日志。您还可以为以下事件配置外部日志记录：

- 连接事件，通过在单个访问控制规则、SSL 解密规则或安全智能策略设置上选择系统日志服务器。
- 入侵事件，通过在入侵策略设置中选择系统日志服务器。

开始之前

仅当您应用需要 IPS 和 恶意软件防御许可证的文件或恶意软件策略时，文件/恶意软件事件的系统日志设置才具有相关性。

此外，您必须确保在应用这些策略的访问控制规则上选择了**文件事件** > **日志文件**选项。否则，系统不会生成任何事件，既不会为系统日志，也不会为事件查看器生成事件。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **日志记录设置**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的**日志记录设置 (Logging Settings)**

步骤 2 在**远程服务器**下，将**数据日志记录**滑块调为**启用**，以为诊断数据平面生成的消息启用将日志记录发送到外部系统日志服务器。然后，配置以下选项：

- **系统日志服务器** - 点击 + 并选择一个或多个系统日志服务器对象，然后点击**确定**。如果对象不存在，请点击**添加系统日志服务器**链接，并立即创建对象。有关详细信息，请参阅配置系统日志服务器。
- **过滤 FXOS 机箱系统日志的严重性级别** - 对于使用 FXOS 的特定设备型号，基础 FXOS 平台生成的系统日志消息的严重性级别。仅当其与您的设备相关时，系统才会显示此选项。选择严重性级别。此级别或更高级别的消息会发送到系统日志服务器。
- **消息过滤**- 选择以下选项之一来控制为 Firewall Threat Defense 操作系统生成的消息。
  - **用于过滤所有事件的严重性级别** - 选择严重性级别。此级别或更高级别的消息会发送到系统日志服务器。
  - **自定义日志记录过滤器** - 如果您想要执行其他消息过滤，以便仅获得您感兴趣的消息，请选择事件列表过滤器，定义您想要生成的消息。如果尚不存在过滤器，请点击**创建新的事件列表过滤器**，然后创建过滤器。有关详细信息，请参阅配置事件列表过滤器，第 9 页。

步骤 3 将**文件/恶意软件**滑块调为**启用**，以为文件和恶意软件事件启用将日志记录发送到外部系统日志服务器。然后，配置文件/恶意软件日志记录的选项：

- **系统日志服务器** - 选择系统日志服务器对象。如果对象不存在，请点击**添加系统日志服务器**链接，并立即创建对象。
- **日志严重性级别** - 选择应分配给文件/恶意软件事件的严重性级别。由于生成的所有文件/恶意软件事件都具有相同的严重性，因此不会执行任何过滤；无论选择哪种级别，您都会看到所有事件。这将是消息严重性字段中显示的级别（即，FTD-x-<message_ID> 中的 x）。文件事件的消息 ID 为 430004，恶意软件事件则为 430005。

步骤 4 点击**保存**。

配置系统将日志记录保存到内部缓冲区

您可以配置系统将系统日志消息保存到内部日志缓冲区。可在 CLI 或 CLI 控制台中使用 **show logging** 命令查看缓冲区的内容。

新消息将附加到缓冲区的末端。当缓冲区填充满时，系统将清除缓冲区并继续向其添加消息。当日志缓冲区已满时，系统将删除最早的消息，以释放缓冲区空间供新消息使用。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **日志记录设置**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的**日志记录设置 (Logging Settings)**

步骤 2 将**内部缓冲区**滑块调为**启用**，以将缓冲区设为日志记录目标。

步骤 3 配置内部缓冲区日志记录的选项：

- **用于过滤所有事件的严重性级别** - 选择严重性级别。此级别或更高级别的消息会发送到内部缓冲区。
- **自定义日志记录过滤器** -（可选。）如果您想要执行其他消息过滤，以便仅获得您感兴趣的消息，请选择事件列表过滤器，定义您想要生成的消息。如果尚不存在过滤器，请点击**创建新的事件列表过滤器**，然后创建过滤器。有关详细信息，请参阅配置事件列表过滤器，第 9 页。
- **缓冲区大小** - 用于保存系统日志消息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。Cisco Secure Firewall 200 的范围为 4096-5242880。

步骤 4 点击**保存**。

配置系统将日志记录发送到控制台

您可以配置系统将消息发送到控制台。当在控制台端口上登录 CLI 时会显示这些消息。使用 **show console-output** 命令也可以在其他界面（包括管理地址）的 SSH 会话中看到这些日志。此外，从主 CLI 中输入 **system support diagnostic-cli** 即可在诊断 CLI 中实时看到这些消息。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **日志记录设置**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的**日志记录设置 (Logging Settings)**

步骤 2 将**控制台过滤器**滑块调为**启用**，以将控制台设为日志记录目标。

步骤 3 选择**严重性**级别。此级别或更高级别的消息会发送到控制台。

步骤 4 点击**保存**。

配置事件列表过滤器

事件列表是一个自定义过滤器，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，只根据严重性来过滤目标消息，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。

仅当只按照严重性级别过滤消息不足以达到您的目的时，才会使用过滤器。

以下步骤介绍如何在**对象**页面创建过滤器。在配置可以使用过滤器的日志记录目标时，您还可以创建过滤器。

过程

步骤 1 选择**对象**，然后从目录中选择**事件列表过滤器**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置过滤器属性：

- **名称** - 过滤器对象的名称。
- **说明** - 对象的可选说明。
- **严重性和日志类** - 如果想要按消息类别进行过滤，请点击**+**，然后为类别过滤器选择一个严重性级别，并点击**确定**。然后，点击严重性级别内的下拉箭头，在此严重性级别上选择一个或多个类别进行过滤，并点击**确定**。

  仅当指定类别的消息的严重性级别处于或高于此级别时，系统才会发送其系统日志消息。您可以为每个严重性级别最多添加一行。

  如果对给定严重性级别上的所有类别进行过滤，请将严重性列表留空，并且在启用日志记录目标时，为此目标选择全局严重性级别。
- **系统日志范围/消息 ID** - 如果想要按系统日志消息 ID 过滤，请输入您要为其生成消息的单个消息 ID 或 ID 号码范围。使用连字符分隔开始 ID 号和结束 ID 号，例如 100000-200000。ID 是 6 位数号码。有关特定消息 ID 和相关消息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html中的 *Cisco Firepower Threat Defense* 系统日志消息 。

步骤 4 点击**保存**。

您现在可以在自定义过滤选项中选择此对象，用于允许此对象的日志记录目标。转至**设备** > **系统设置** > **日志记录设置**。

配置 DHCP

DHCP 服务器可为 DHCP 客户端提供网络配置参数，例如 IP 地址。您可以在接口上配置 DHCP 服务器，以便为连接网络中的 DHCP 客户端提供配置参数，也可以在接口上启用 DHCP 中继，以便将请求转发到在网络中的另一台设备上运行的外部 DHCP 服务器。

这两个功能只能二选其一：您可以配置其中一个功能或另一个功能，但不能同时配置这两个功能。

配置 DHCP 服务器

DHCP 服务器可为 DHCP 客户端提供网络配置参数，例如 IP 地址。您可以在接口上配置 DHCP 服务器，为连接的网络上的 DHCP 客户端提供配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。DHCP 服务器不支持 BOOTP 请求。

注释 不要在已经有 DHCP 服务器运行的网络上配置 DHCP 服务器。这两个服务器将发生冲突，结果不可预测。

开始之前

DHCP 客户端必须与启用了服务器的接口位于同一网络内。即服务器和客户端之间不能有干预路由器，但可以有交换机。

如果您必须支持多个网络，但不想在每个接口上配置 DHCP 服务器，您可以配置 DHCP 中继，将 DHCP 请求从一个网络转发到位于不同网络上的 DHCP 服务器。在这种情况下，DHCP 服务器必须位于网络中的不同设备上：不能在同一设备的一个接口上配置 DHCP 服务器，而在另一个接口上配置 DHCP 中继。使用 DHCP 中继时，请确保为 DHCP 服务器将管理的每个网络地址空间配置地址池。

要配置 DHCP 中继，请参阅配置 DHCP 中继 ，第 13 页。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DHCP 服务器/中继**链接。

如果已经位于“系统设置”(System Settings) 页面中，只需点击目录中的 **DHCP** > **DHCP 服务器 (DHCP Server)**。

该页有两个选项卡。一开始，**配置**选项卡显示全局参数。

DHCP 服务器选项卡显示已在其上配置 DHCP 服务器的接口、服务器启用情况以及服务器的地址池。

步骤 2 在**配置**选项卡上，配置自动配置和全局设置。

DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。通常，如果您是在使用 DHCP 获取地址，则会使用自动配置，但您可以选择通过 DHCP 获取其地址的任何接口。如果无法使用自动配置，可以手动定义所需的选项。

a) 如果要使用自动配置，请点击**启用自动配置** > **开**（滑块应位于右侧），然后在**源接口**中选择正在通过 DHCP 获取其地址的接口。

如果要配置虚拟路由器，则只能在全局虚拟路由器中的接口上使用 DHCP 服务器自动配置。为用户定义的虚拟路由器分配的接口不支持自动配置功能。

b) 如果不启用自动配置，或者如果要覆盖任何一个自动配置的设置，请配置以下全局选项。这些设置将发送到托管 DHCP 服务器的所有接口上的 DHCP 客户端。

- **主 WINS IP 地址**、**辅助 WINS IP 地址** - Windows Internet Name Service (WINS) 服务器客户端应该用于 NetBIOS 域名解析的地址。
- **主 DNS IP 地址**、**辅助 DNS IP 地址** - 客户端应该用于域名解析的域名系统 (DNS) 服务器的地址。如果要配置 OpenDNS 公共 DNS 服务器，请点击**使用 OpenDNS**。点击该按钮会将正确的 IP 地址载入字段中。

c) 点击**保存**。

步骤 3 点击 **DHCP 服务器**选项卡并配置服务器。

a) 执行以下操作之一：

- 要为尚未列出的接口配置 DHCP 服务器，请点击 **+**。
- 要编辑现有的 DHCP 服务器，请点击该服务器的编辑图标 ( )。

要删除服务器，请点击该服务器的垃圾桶图标 ( )。

b) 配置服务器属性：

- **启用 DHCP 服务器** - 是否启用服务器。您可以配置服务器，但在做好准备开始使用之前，要一直将其禁用。
- **接口** - 选择您为客户端提供 DHCP 地址的接口。接口必须拥有静态 IP 地址；如果要在接口上运行 DHCP 服务器，则不能使用 DHCP 获取接口。对于网桥组，在网桥虚拟接口 (BVI) 上（而不是成员接口上）配置 DHCP 服务器，并且服务器在所有成员接口上运行。

  您不能在此屏幕中的管理接口上配置 DHCP 服务器，而应在上配置，它位于**设备** > **接口**页面。
- **地址池** - 允许服务器为请求地址的客户端提供的 IP 地址的范围（最低至最高）。指定该池的开始和结束地址，用连字符隔开。例如 10.100.10.12-10.100.10.250。

  该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。

  设备上地址池的大小限制为每个池 4096 个地址。Firewall Threat Defense 接口的网络掩码必须足够大，以包含该地址范围。例如，如果地址池范围大于 253 个地址，则接口的网络掩码不能为 C 类地址（例如 255.255.255.0 或 /24），而需要更大的掩码，例如 255.255.254.0。最大地址范围需要 /20 网络掩码。

c) 点击**确定**。

配置 DHCP 中继

您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。

DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 Firewall Threat Defense 设备进行转发，因为它不转发广播流量。DHCP 中继代理允许您配置接收广播的Firewall Threat Defense 设备的接口，以将 DHCP 请求转发到可通过另一个接口使用的 DHCP 服务器。

因此，子网中不托管 DHCP 服务器的客户端仍然可以从位于不同子网中的 DHCP 服务器获取 IP 地址租用。

开始之前

- 为要添加的每个子网配置具有地址池的 DHCP 服务器。例如，如果您在具有 192.168.1.1/24 地址的接口上启用 DHCP 中继客户端，要支持 192.168.1.0/24 网络上的客户端，DHCP 服务器必须能够提供 192.168.1.0/24 子网上的 IP 地址，例如 192.168.1.2-192.168.1.254。
- 为每个 DHCP 服务器创建主机网络对象，指定服务器的 IP 地址。
- 确保已删除或已禁用 **DHCP** > **DHCP 服务器 (DHCP Servers)** 页面上的所有服务器。如果在接口上启用了 DHCP 中继，则您不能在任何接口上托管 DHCP 服务器，即使它们是不同的接口。
- 接口限制 - 接口必须具有用于服务器或代理的名称。此外：
  - 接口不能是路由 ECMP 流量区域的成员。
  - 接口无法使用 DHCP 获取其地址。
  - 您可以在物理接口、子接口、VLAN 接口和 EtherChannel（但不是它们的成员）上配置 DHCP 服务器和 DHCP 中继。
  - 您还可以在虚拟隧道接口 (VTI) 上配置 DHCP 中继服务器。
  - 这两项服务都不支持管理接口，也不支持网桥组及其成员。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DHCP 服务器/中继**链接，然后点击目录中的 **DHCP** > **DHCP 中继**。

如果您已经在“系统设置”(System Settings) 页面中，只需点击目录中的 **DHCP** > **DHCP 中继 (DHCP Relay)**。

步骤 2 （可选。）根据需要调整 **IPv4 中继超时**和 **IPv6 中继超时**设置。

这些超时设置用于设置给定 IP 版本的 DHCP 中继地址协商所允许的秒数。默认值为 60 秒（1 分钟），但您可以设置介于 1-3600 秒的其他超时值。如果子网和 DHCP 服务器之间存在明显延迟，则可能需要更长的超时时间。

步骤 3 配置 **DHCP 中继服务器**。

DHCP 中继服务器是网络中应为 DHCP 中继请求提供服务的 DHCP 服务器。这些 DHCP 服务器与您正在配置的设备位于网络中的不同设备上。

a) 点击 +，选择具有 DHCP 服务器 IP 地址的主机网络对象，然后点击**确定**。

如果该对象尚不存在，请点击**创建新网络**并立即创建。如果您不想再使用已添加的 DHCP 服务器，请点击该服务器条目右侧的 **X** 将其删除。

b) 点击您添加的 DHCP 服务器条目，然后选择可以访问 DHCP 服务器的接口。

步骤 4 配置 DHCP 中继代理。

DHCP 中继代理在接口上运行。它们将来自其网段中客户端的 DHCP 请求转发到 DHCP 服务器，然后将响应返回给客户端。

a) 点击 +，选择应运行 DHCP 中继代理的接口，然后点击**确定**。

如果您不想再在接口上运行 DHCP 中继代理，请点击该服务器条目右侧的 **X** 将其删除。或者，您可以只禁用所有 DHCP 中继服务，而不从表中删除接口。

b) 点击您添加的接口条目，选择您希望代理提供的 DHCP 服务，然后点击**确定**。

- **启用 IPv4** - 将 IPv4 地址请求转发到 DHCP 服务器。如果不选择此选项，则会忽略任何 IPv4 地址请求，并且客户端无法获取 IPv4 地址。
- **设置路由** （仅限 IPv4）- 将从 DHCP 服务器发送的数据包中的第一个默认路由器地址更改为运行 DHCP 中继代理的 Firewall Threat Defense 设备接口的地址。通过此操作，客户端可以将其默认路由设置为指向 Firewall Threat Defense设备，即使 DHCP 服务器指定了另一个路由器也如此。如果数据包内无默认路由器选项，DHCP 中继代理会添加一个包含接口地址的选项。
- **启用 IPv6** - 将 IPv6 地址请求转发到 DHCP 服务器。如果不选择此选项，则会忽略任何 IPv6 地址请求，并且客户端无法获取 IPv6 地址。

步骤 5 点击**保存**。

配置动态 DNS

您可以将系统配置为使用 Web 更新方法将动态域名系统 (DDNS) 更改发送到动态 DNS 服务。这些服务随后会更新 DNS 服务器，以使用与完全限定域名 (FQDN) 关联的新 IP 地址。因此，当用户尝试使用主机名访问系统时，DNS 会将该名称解析为正确的 IP 地址。

使用 DDNS 有助于确保为系统中的接口定义的 FQDN 始终解析为正确的 IP 地址。当您将接口配置为使用 DHCP 获取地址时，这一点尤其重要。但使用它获取静态 IP 地址以确保 DNS 服务器具有正确的地址也是有价值的，并且在更改静态地址时可以很容易更新。

您可以将 DDNS 配置为使用一组选定的 DDNS 服务提供商，或者使用自定义选项将更新定向到支持 Web 更新的任何其他 DDNS 提供商。您为接口指定的 FQDN 应注册到这些服务提供商。

注释 您可以使用 防火墙设备管理器 仅配置 Web 更新 DDNS。您不能配置 DDNS 来实现 IETF RFC 2136 中定义的方法。

开始之前

系统必须拥有信任的 CA 证书，以验证提供商的证书，否则 DDNS 连接将不会成功。您可以从服务提供商的站点下载证书。请确保上传并部署适当的证书。还要确保您将上传的证书的**验证使用**设置为包括 **SSL 服务器**。请参阅上传受信任的 CA 证书。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DDNS 服务**链接。

如果已经位于“系统设置”页面中，只需点击目录中的 **DDNS 服务 (DDNS Service)**。

该页面显示 DDNS 更新方法的列表，包括服务提供商、接口、接口的完全限定域名 (FQDN)，以及 DNS 服务器因 FQDN IP 地址更改而更新的频率。您可以点击条目的**显示状态**链接来检查其是否正常工作。

步骤 2 执行以下操作之一：

- 要创建新的动态 DNS 更新方法，请点击 **+** 或**创建 DDNS 服务**按钮。
- 要编辑现有的动态 DNS 更新方法，请点击该方法的编辑图标 ( )。

要删除方法，请点击该方法的垃圾桶图标 ( )。

步骤 3 配置动态 DNS 服务属性：

- **名称** - 服务的名称。
- **Web 类型更新** - 根据您的 DDNS 服务提供商的支持情况选择要更新的地址类型。默认更新**所有地址**（IPv4 和 IPv6）。您可以更新 **IPv4 地址**、**IPv4 和一个 IPv6 地址**、**一个 IPv6 地址**、**所有 IPv6 地址**。

  对于 IPv6 地址，请注意以下几项：

  - 仅更新全局地址。从不更新本地链路地址。
  - 由于 防火墙设备管理器 允许您为每个接口配置一个 IPv6 地址，因此在实践中，只会更新一个 IPv6 地址。

- **服务提供商** - 选择将接收和处理动态 DNS 更新的服务提供商。您可以使用以下服务提供商。
  - **No-IP** - No-IP DDNS 服务提供商，https://www.noip.com/。
  - **动态 DNS** - Oracle Dynamic DNS 服务提供商，https://account.dyn.com/。

- **Google** - Google Domains 服务提供商，https://domains.google.com。
- **自定义 URL** - 任何其他 DDNS 服务提供商。您将需要在 **Web URL** 字段中输入选定提供商所需的 URL（包括用户名和密码）。DDNS 服务应遵守 https://help.dyn.com/remote-access-api/ 中所述的标准。

- **用户名**、**密码**（非自定义 URL 方法）- 发送动态 DNS 更新时要使用的在服务提供商平台上定义的用户名和密码。

  注意：

  - 用户名不能包含空格，也不能包含 @ 和 : 字符，因为它们会被作为分隔符。
  - 密码不能包含空格或 @ 字符，因为它会被作为分隔符。第一个 : 之后和 @ 之前的任何 : 字符都被视为密码的一部分。

- **Web URL**（自定义 URL 方法）- 如果您选择自定义 URL 作为服务提供商，请输入您的动态 DNS 服务的 URL。URL 必须采用以下格式，限制为 511 个字符：

  http(s)://username:password@provider-domain/xyz?hostname=<h>&myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- **接口和完全限定域名** - 选择此服务提供商中要更新 DNS 记录的接口，然后输入每个接口的完全限定域名。例如，interface.example.com。接口受到以下限制：
  - 您只能选择指定的物理接口和子接口。
  - 您不能选择以下类型的接口：管理、BVI/EtherChannel 或其成员、VLAN、虚拟隧道接口 (VTI)。
  - 只能在一个 DDNS 更新方法中选择给定的接口。您可以选择应在同一 DDNS 更新对象中使用服务提供商的所有接口。

- **更新间隔** - 发送动态 DNS 更新的频率。默认值为**更改时**，只要接口的 IP 地址更改就发送更新。或者，您可以选择**每小时**、**每天**或**每月**。在每天和每月的设置中，还可以配置在每天的什么时间和每月的哪一天发送更新。

步骤 4 点击**确定**。

配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。DNS 服务器的配置在初始系统设置期间执行，并且这些服务器将应用于数据和管理接口。您可以在设置完成后对其进行更改，并对数据和管理接口使用单独的一组服务器。

至少，必须要为管理接口配置 DNS。如果您想要使用基于 FQDN 的访问控制规则，或想要在 CLI 命令（如 **ping**）中使用主机名，那么还必须要为数据接口配置 DNS。

DNS 的配置分两步完成：配置 DNS 组，然后在接口上配置 DNS。

以下主题更详细地介绍了这一过程。

配置 DNS 组

DNS 组定义 DNS 服务器列表和某些相关联的属性。您可以在管理和数据接口上单独配置 DNS。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。

完成设备设置向导后，您将有一个或两个系统定义的以下 DNS 组：

- CiscoUmbrellaDNSServerGroup - 此组包括思科 Umbrella 所搭配 DNS 服务器的 IP 地址。如果您在初始设置期间选择了这些服务器，此组便是系统定义的唯一组。您无法更改此组中的名称或服务器列表，但您可以编辑其他属性。
- CustomDNSServerGroup - 如果您不在设备设置期间选择 Umbrella 服务器，系统将使用您的服务器列表创建此组。您可以编辑此组中的任何属性。

过程

步骤 1 选择**对象**，然后从目录中选择 **DNS 组**。

步骤 2 执行以下操作之一：

- 要创建组，请点击**添加组** () 按钮。
- 要编辑组，请点击该组的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 配置以下属性：

- **名称** - DNS 服务器组的名称。保留 DefaultDNS 名称：不能使用该名称。
- **DNS IP 地址** - 输入 DNS 服务器的 IP 地址。点击**添加另一个 DNS IP 地址**配置多个服务器。如果您想要删除服务器地址，请点击该地址的删除图标 ()。

  列表采用优先顺序：始终使用列表中的第一个服务器，只有当从前面的服务器收不到响应时，才使用后面的服务器。最多可配置 3 台服务器。
- **域搜索名称** - 为您的网络输入域名，例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。名称必须不能超过 63 个字符以使用数据接口组。
- **重试次数** - 系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。此设置仅适用于数据接口上使用的 DNS 组。
- **超时** - 尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。此设置仅适用于数据接口上使用的 DNS 组。

步骤 4 点击**确定**。

为数据流量和管理流量配置 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，例如智能许可和数据库更新。

如果使用 CLI 安装向导，则在初始系统配置期间，配置管理 DNS 服务器。还可以在 防火墙设备管理器 安装向导中设置数据和管理 DNS 服务器。可使用以下过程更改 DNS 服务器默认设置。

您还可以在 CLI 中使用 **configure network dns servers** 和 **configure network dns searchdomains** 命令更改 DNS 配置。如果数据和管理接口使用相同的 DNS 组，组将更新，且所做的更改也会在下一个部署中应用到数据接口。

为了确定 DNS 服务器通信的正确接口， Firewall Threat Defense 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。

如果您无法进行 DNS 解析，请参阅：

- 常规 DNS 问题故障排除 ， 第 19 页
- 为管理接口排除 DNS 故障

开始之前

- 确保已创建 DNS 服务器组。有关说明，请参阅配置 DNS 组 ， 第 17 页。
- 确保 Firewall Threat Defense 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 点击**设备**，然后点击**系统设置** > **DNS 服务器**链接。

如果已经位于**系统设置 (System Settings)** 页面中，则点击目录中的 **DNS 服务器 (DNS Server)**。

步骤 2 为**数据接口**配置 DNS。

a) 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。设备始终使用路由查询来确定源接口。

- **任何**（不选择任何接口）- 在所有接口。设备 仅检查数据路由表。
- 已选择接口，但未选择管理接口或管理专用接口 - 在指定接口上启用 DNS 查找。设备仅检查数据路由表。

- 已选择接口，并且选择了管理接口或管理专用接口 - 在指定接口上启用 DNS 查找。设备检查数据路由表，如果未找到路由，则回退到管理专用路由表。
- 仅选择了管理接口或管理专用接口 - 在管理或管理专用接口上启用 DNS 查找。设备仅检查管理专用路由表。

b) 选择定义在数据接口上使用的服务器的 **DNS 组**。如果组尚不存在，请点击**创建新的 DNS 组 (Create New DNS Group)** 立即创建组。如果您想要阻止在数据接口上进行查找，请选择**无**。

c) （可选。）如果在访问控制规则中使用 FQDN 网络对象，配置 **FQDN DNS 设置**。

仅解析 FQDN 对象时使用这些选项，任何其他类型的 DNS 解析都将忽略这些选项。

- **轮询时间** - 将 FQDN 网络对象解析为 IP 地址的轮询周期，以分钟为单位。仅在访问控制策略中使用 FQDN 对象时，解析这些对象。计时器决定两次解析之间的最长时间；DNS 条目的生存时间 (TTL) 值也用于确定更新 IP 地址解析的时间，因此，解析单个 FQDN 的频率可能大于轮询周期。默认设置为 240（4 个小时）。范围为 1 至 65535 分钟。
- **过期** - DNS 条目过期（即，超出从 DNS 服务器获得的 TTL）后，从 DNS 查找表中删除该条目前等待的分钟数。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。默认设置为 1 分钟（即，TTL 过去后 1 分钟，会删除条目）。范围为 1 至 65535 分钟。

d) 点击**保存 (Save)**。您还必须部署配置，将更改应用到设备。

步骤 3 为**管理接口**配置 DNS。

a) 选择定义在管理接口上使用的服务器的 **DNS 组**。如果组尚不存在，请点击**创建新的 DNS 组 (Create New DNS Group)** 立即创建组。

b) 点击**保存 (Save)**。必须部署更改以更新管理 DNS 服务器。

常规 DNS 问题故障排除

必须为管理和数据接口单独配置DNS服务器。某些功能通过这两类接口中的其中一类接口，而不是这两类接口，解析域名。有时，给定的功能将使用不同的解析方法，具体取决于您如何使用该功能。

例如，**ping** *hostname* 和 **ping interface** *interface_name hostname* 命令使用数据接口 DNS 服务器解析域名，而 **ping system** *hostname* 命令使用管理接口 DNS 服务器。这使您可以通过特定接口和路由表测试连接。

排除主机名查找问题时，请记住这一点。

有关排除管理接口 DNS 故障的信息，另请参阅为管理接口排除 DNS 故障。

未发生域名解析

如果根本没有发生域名解析，可参照以下故障排除提示。

- 验证您是否已为管理和数据接口均配置 DNS 服务器。对于数据接口，对接口使用“任何”设置。仅当您不想在某些接口上允许 DNS 时，才明确指定接口。
- 您无法通过管理接口或管理专用接口访问DNS服务器。如果要使用管理接口，请确保该接口是选择的唯一接口。
- 执行 ping 操作，以验证是否可访问每个 DNS 服务器的 IP 地址。使用 **system** 和 **interface** 关键字测试特定接口。如果 ping 操作不成功，请检查您的静态路由和网关。您可能需要为服务器添加静态路由。
- 如果 ping 操作成功，但域名解析失败，请检查访问控制规则。验证您是否允许连接服务器的接口的 DNS 流量 (UDP/53)。此流量也可能被系统和 DNS 服务器之间的设备阻止，因此您可能需要使用不同的 DNS 服务器。
- 如果 ping 操作成功、路由充足，并且访问控制规则不是症结所在，请考虑 DNS 服务器是否存在 FQDN 映射。您可能需要使用不同的服务器。

域名解析错误

如果进行了域名解析，但名称的IP地址不是最新地址，可能存在缓存问题。此问题仅影响基于数据接口的功能，例如访问控制规则中使用的 FQDN 网络对象。

系统有从前期查找中获得的DNS信息的本地缓存。需要新的查询时，系统首先在本地缓存中查找。如果本地缓存中有该信息，则将返回生成的 IP 地址。如果本地缓存无法解析该请求，则将 DNS 查询发送至 DNS 服务器。如果外部 DNS 服务器解析请求，则生成的 IP 地址与其相应的主机名一起存储在本地缓存中。

每个查找都有一个生存时间值，该值由DNS服务器定义并自动从缓存到期。此外，系统会为访问控制规则中使用的 FQDN 定期刷新该值。至少，系统会按照轮询时间间隔（默认情况下，每 4 小时一次）刷新，不过可根据该条目的生存时间值，增加刷新频率。

使用 **show dns-hosts** 和 **show dns** 命令检查本地缓存。如果 FQDN 的 IP 地址错误，可以使用 **dns update** [**host** *hostname*] 命令强制系统刷新信息。如果在使用此命令时没有指定主机，系统会刷新所有主机名。

可以使用 **clear dns** [**host** *fqdn*] 和 **clear dns-hosts cache** 命令删除缓存的信息。

配置设备主机名

可以更改设备主机名。

您还可以在 CLI 中使用 **configure network hostname** 命令更改主机名。

⚠

注意 如果更改连接到系统所用的主机名，由于这些更改会立即应用，因此您将丢失对 防火墙设备管理器的访问。您需要重新连接到设备。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **主机名**链接。

如果已经位于“系统设置”页面中，只需点击目录中的**主机名 (Hostname)**

步骤 2 输入新主机名。

步骤 3 点击**保存**。

主机名更改随后立即应用到某些系统进程。但是，您必须部署更改以完成更新，以便所有系统进程都使用相同的名称。

配置网络时间协议 (NTP)

必须配置网络时间协议 (NTP) 服务器才能在系统上定义时间。NTP 服务器在初始系统设置期间配置，但您可以使用以下步骤程序对其进行更改。如果您无法连接到 NTP，请参阅 NTP 故障排除。

Firewall Threat Defense 设备支持 NTPv4。

注释 对于 Firepower 4100/9300，不通过 防火墙设备管理器 设置 NTP。在 FXOS 中配置 NTP。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **时间服务**链接。

如果已经在“系统设置”(System Settings) 页面中，则只需点击目录中的**时间服务 (Time Services)** 即可。

步骤 2 在 **NTP 服务器**下，点击 **+** 并选择要用于建立系统时间的 NTP 服务器对象。

最多可以选择 3 个服务器。点击创建新 NTP 服务器链接以新建 NTP 服务器对象。请参阅配置 NTP 服务器对象 ， 第 22 页。

点击**设置默认值**以恢复为系统默认 NTP 服务器。

步骤 3 点击**保存**。

配置 NTP 服务器对象

配置 NTP 服务器对象以定义网络时间协议服务器。然后，您可以使用这些对象来指定应由哪些服务器设置系统时间。

过程

步骤 1 选择**对象**，然后从目录中选择 **NTP 服务器**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的**名称**和说明（后者为可选项）。

步骤 4 在**服务器名称或 IP 地址**中，输入服务器的完全限定域名（例如 ntp.example.com）或服务器 IP 地址。

步骤 5 选择是否使用 **NTPv4 身份验证**。

NTPv4 身份验证使用加密密钥验证 NTP 服务器身份，确保时间同步数据来自可信源，并防止系统时钟被未授权篡改。配置以下选项：

- **密钥类型** — 密钥使用的加密密码。您可以选择以下选项之一：
  - MD5 — 这是一种弱密码，仅用于向后兼容。
  - SHA1 — 这是可用于传统支持的弱选项。不建议在新部署中使用。
  - SHA256 — 这是建议的基准标准。
  - SHA512 — 这是高安全性选项。
  - AES128CMAC — 这是符合 FIPS 的基于 AES 的选项。
- **密钥编号** — 范围为 1-65535 的唯一标识符。
- **密钥值** — 可从 NTP 服务器获取的有效十六进制字符串。该值具有算法特定的长度要求：
  - MD5 — 32 个十六进制字符（128 位）。
  - SHA1 — 40 个十六进制字符（160 位）。
  - SHA256 — 64 个十六进制字符（256 位）。
  - SHA512 — 128 个十六进制字符（512 位）。
  - AES128CMAC — 64 个十六进制字符（256 位）。

步骤 6 点击**确定**。

现在可以在**系统设置** > **时间服务**中选择该对象

配置精确时间协议 (ISA 3000)

精确时间协议 (PTP) 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。这些设备时钟通常具有不同的精度和稳定性。该协议专为工业联网测量和控制系统设计，而且最适合用于分布式系统，因为其需要极少的带宽和处理开销。

PTP 系统是一个分布式联网系统，包含 PTP 设备和非 PTP 设备的组合。PTP 设备包含常见的时钟、边界时钟和透明时钟。非 PTP 设备包含网络交换机、路由器和其他基础设施设备。

可以将 Firewall Threat Defense 设备配置为透明时钟。 Firewall Threat Defense 设备不会将其时钟与 PTP 时钟同步。 Firewall Threat Defense 设备将使用 PTP 默认配置文件，如 PTP 时钟上所定义。

配置 PTP 设备时，需要为要一起运行的设备定义一个域编号。因此，可以配置多个 PTP 域，然后将每个非 PTP 设备配置为特定域使用 PTP 时钟。

开始之前

确定设备应使用的 PTP 时钟上配置的域编号。另外，确定系统可通过哪些接口到达域中的 PTP 时钟。

以下是 PTP 配置准则：

- 此功能在思科 ISA 3000 设备上不可用。
- 思科 PTP 仅支持组播 PTP 消息。
- PTP 仅可用于 IPv4 网络，不可用于 IPv6 网络。
- 物理以太网数据接口支持 PTP 配置，无论是路由组还是网桥组成员。管理接口、子接口、Etherchannel 接口、桥接虚拟接口 (BVI) 或任何其他虚拟接口均不支持此版本。
- 假如父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。
- 必须确保允许 PTP 数据包通过设备。PTP 流量由 UDP 目标端口 319 和 320 以及目标 IP 地址 224.0.1.129 标识，因此允许此流量的任何访问控制规则均应有效。
- 当PTP数据包在路由接口之间传输时，您必须启用多路广播路由，并且每个接口应加入224.0.1.129 IGMP 多路组播组。当 PTP 数据包在同一网桥组中的接口之间流动时，您无需启用组播路由和配置 IGMP 组。

过程

步骤 1 验证面向 PTP 时钟的接口的配置。

默认配置将所有接口置于同一个网桥组中，但可以从网桥组中删除接口。必须确定接口是路由组成员还是网桥组成员，因为对于组播 IGMP 组而言这两种成员必须进行不同的配置。

以下操作步骤介绍如何确定哪些接口是网桥组成员。检查您为 PTP 配置的接口是否为网桥组成员。

a) 点击**设备** > **接口**中的**查看所有接口**。
b) 在列表中查找相应接口，并选中“模式”列。如果是 BridgeGroupMember，则意味着属于网桥组；否则应该属于路由组。

步骤 2 点击**设备**，然后点击**系统设置** > **时间服务**链接。

如果已经在**系统设置 (System Settings)** 页面中，则只需点击目录中的**时间服务 (Time Services)** 即可。

步骤 3 配置 PTP 设置：

- **域编号** - 在网络中的 PTP 设备上配置的域编号，范围为0-255。在其他域中接收的数据包将像正常组播数据包一样处理，不会进行任何 PTP 处理。
- **时钟模式**-选择 **EndToEndTransparent**。您只能将设备作为 PTP 透明时钟运行。

  或者，也可以选择**转发**，但这在本质上与不配置 PTP 时的情况相同。域编号将被忽略。PTP 数据包基于组播流量的路由表通过设备。这是默认的 PTP 配置。
- **接口** - 选择可由系统用于连接至网络中的 PTP 时钟的所有接口。仅在这些接口上启用 PTP。

步骤 4 点击**保存**。

步骤 5 如果您选择的任何接口是路由接口（即它们不是网桥组成员），则需要使用 FlexConfig 启用组播路由，并将路由接口加入正确的 IGMP 组。

如果所有选定的接口都是网桥组成员，则不用完成此步骤。如果您尝试在网桥组成员上配置IGMP，则会出现部署故障。

a) 在**设备** > **高级配置**中点击**查看配置**。
b) 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。
c) 创建启用组播路由和为路由接口配置 IGMP 加入所需的对象。

   以下将是对象的基本模板。在本示例中，GigabitEthernet1/2 是您在其中启用 PTP 的一个路由接口。根据需要更改接口硬件名称，并且如果您有多个路由接口，请对每个其他接口重复**interface** 和 **igmp** 命令。

   igmp 命令将会加入 224.0.1.129 IGMP 组。无论网络地址如何，这都是所有接口的正确 IP 地址。

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

   取消模板如下所示：

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) 点击目录中的 **FlexConfig 策略**，将此对象添加到 FlexConfig 策略中，然后点击**保存**。

验证预览内容是否会显示您对象中的预期命令。

下一步做什么

在部署更改后，您可以验证 PTP 设置。在 防火墙设备管理器 CLI 控制台或 SSH 或控制台会话中，发出各种 **show ptp** 命令。例如，如果仅为 GigabitEthernet1/2 配置了用于域 10 的 PTP，则输出内容可能如下所示：

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

配置管理连接的 HTTP 代理

如果系统和互联网之间没有直接连接，可以为管理接口设置 HTTP 代理。然后，系统将该代理用于所有管理连接，包括与 防火墙设备管理器 的连接以及为下载数据库更新而从系统到思科建立的连接。

您还可以使用 **configure network http-proxy** 命令在 Firewall Threat Defense CLI 中配置 HTTP 代理。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **HTTP 代理**链接。

如果已经位于**系统设置 (System Settings)** 页面中，只需点击目录中的 **HTTP 代理 (HTTP Proxy)**

步骤 2 点击此切换启用代理，然后配置代理设置：

- **HTTP 代理** - 代理服务器的 IP 地址。
- **端口** - 配置为侦听 HTTP 连接的代理服务器端口号。
- **使用代理身份验证** - 如果服务器配置为需要对代理连接进行身份验证，请选择此选项。如果选择此选项，还需输入可登录代理服务器的账户的**用户名**和**密码**。

步骤 3 点击**保存**，然后确认进行更改。

所做更改会立即应用。不需要部署作业。

由于您要更改系统完成管理连接的方式，因此将失去与 防火墙设备管理器的连接。请等待几分钟以完成更改，然后刷新浏览器窗口并重新登录。

配置云服务

您可以注册云服务，以便使用各种基于云的应用，例如 Security Cloud Control、Cisco 威胁响应和 Cisco Success Network。

在云中注册后，该页面将显示注册状态和租用类型，以及注册设备所使用的账户名称。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于**系统设置 (System Settings)** 页面，只需点击目录中的**云服务 (Cloud Services)**。

如果您的设备未注册，此页面会显示注册思科云的注册方法。注册云后，您将能够启用或禁用单个云服务。

步骤 2 要注册思科云（在评估模式下或从云服务取消注册后），请选择以下选项之一：

- Security Cloud Control**安全/SCC 帐户** - 您可以使用以下方法之一：
  - **从 Security Cloud Control自动注册租用**（仅限 Firepower 1000、Cisco Secure Firewall 3100）。您可以使用自动注册而不是获取注册密钥。首先，转到 Security Cloud Control，使用设备的序列号添加设备。然后，在 防火墙设备管理器中，选中此复选框并启动注册。从设备机箱或装箱单上获取序列号。对于 FXOS，您可以进入 FXOS CLI 并使用 **show chassis detail** 命令检索标记为“Serial (SN)”的正确序列号。请注意， Firewall Threat Defense 命令 **show serial-number** 提供不同的序列号，不建议用于 Security Cloud Control 注册。此方法适用于 Security Cloud Control 中的云交付 以及 Security Cloud Control 中的传统设备管理器模式。

    注释

传统设备管理器模式仅适用于已经使用该模式管理 Firewall Threat Defense 设备的现有用户。

- 登录 Security Cloud Control 或其他安全账户并生成注册密钥。然后返回此页面，选择**云服务区域 (Cloud Services Region)**并粘贴**注册密钥 (Registration Key)**。此方法仅适用于 Security Cloud Control 中的传统设备管理器模式。有关 Security Cloud Control 中的云交付管理中心，请参阅从设备管理器切换到管理中心或 Security Cloud Control。

  注释
  传统设备管理器模式仅适用于已经使用该模式管理 Firewall Threat Defense 设备的现有用户。

  此时，您还可以启用**Security Cloud Control**和 **Cisco Success Network**。默认情况下，这些功能处于启用状态。

- **智能许可证**-（仅当您不使用 Security Cloud Control时。）点击链接转到“智能许可”(Smart Licensing) 页面并注册 CSSM。向 CSSM 注册也会将设备注册到云服务。

  注释
  若已从 Cloud Services 取消注册，则智能许可注册可能需要额外步骤。在这种情况下，请选择**云服务区域 (Cloud Services Region)**，然后点击**注册 (Register)**。阅读披露内容并点击**接受 (Accept)**。

步骤 3 注册云服务后，您可以根据需要启用或禁用功能。请参阅以下主题：

- 启用或禁用 Security Cloud Control（传统设备管理器模式）
- 连接到 Cisco Success Network， 第 28 页
- 将事件发送至思科云， 第 29 页
- 取消注册云服务， 第 30 页

启用或禁用 Security Cloud Control（传统设备管理器模式）

注释 本部分仅适用于 Security Cloud Control 中的传统设备管理器模式，而不适用于云交付的管理中心。

如果您从 Security Cloud Control 中使用注册密钥注册了云服务（如配置云服务， 第 26 页中推荐），则设备已向 Security Cloud Control 注册。此后，您可以根据需要禁用或重新启用连接。

如果使用智能许可将设备注册到云服务，则在启用 Security Cloud Control 时会出现问题：设备不会显示在 Security Cloud Control 清单中。强烈建议您先从云服务取消注册设备；从齿轮 (⚙) 下拉列表中选择**取消注册云服务**。取消注册后，从 Security Cloud Control 获取注册令牌，然后使用该令牌和您的安全账户重新注册，如配置云服务， 第 26 页中所述。

有关云管理原理的更多信息，请参阅 Security Cloud Control 门户 (http://www.cisco.com/go/cdo) 或咨询您的经销商或合作伙伴。

开始之前

如果您想要配置高可用性，则必须注册您要在高可用性组中使用的两台设备。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 点击 Security Cloud Control 功能的 **启用/禁用** 按钮，根据需要更改设置。

连接到 Cisco Success Network

注册设备时，需决定是否启用与 Cisco Success Network 之间的连接。请参阅注册设备。

通过启用 Cisco Success Network，可以向思科提供使用信息和统计信息，这对思科为您提供技术支持至关重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。

启用连接时，设备将与思科云建立安全连接，以确保设备可以参与思科提供的其他服务（例如技术支持服务、云管理和监控服务）。您的设备将随时建立并维护此安全连接。有关完全断开与云的连接的信息，请参阅取消注册云服务，第 30 页。

注册设备后，可以更改 Cisco Success Network 设置。

注释 系统向思科发送数据时，任务列表会显示一项遥测作业。

开始之前

要启用 Cisco Success Network，必须向云注册设备。要注册设备，请使用 Cisco 智能软件管理器（在“智能许可”(Smart Licensing) 页面上）注册该设备，在注册过程中选择 “Cisco Success Network” 选项，或者通过输入注册密钥使用 Security Cloud Control 进行注册（仅限 Security Cloud Control 中的传统设备管理器模式）。

注释 如果您在高可用性组的主用设备上启用 Cisco Success Network，也会在备用设备上启用该连接。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 点击 Cisco Success Network 功能的**启用**/**禁用**控件，可以根据需要更改设置。

可以点击**样本数据**链接，查看发送给思科的信息类型。

启用该连接时，请阅读披露的信息并点击**接受**。

将事件发送至思科云

可以将事件发送至思科云服务器。各种思科云服务均可从这里访问事件。然后，可以使用这些云应用来分析事件并评估设备可能遇到的威胁。

云工具确定是否使用您发送的事件。请查阅工具的文档，或检查事件数据，以确保您不会将未使用的事件发送到云（这会浪费带宽和存储空间）。请记住，这些工具从同一来源提取事件，因此您的选择应反映您使用的所有工具，而不仅仅是限制性最强的工具。例如：

- Security Cloud Control 中的安全分析和日志记录工具可以利用所有连接事件。
- 威胁响应仅使用高优先级连接事件，因此无需将所有连接事件都发送到云端。此外，它将仅使用安全智能高优先级事件。

开始之前

必须先向云服务注册设备，然后才能启用此服务。

在美国地区通过 https://visibility.amp.cisco.com/，在欧盟地区通过 https://visibility.eu.amp.cisco.com，以及在 APJC 地区通过 https://visibility.apjc.amp.cisco.com 可以连接至威胁响应。您可以在 YouTube 上观看视频 (http://cs.co/CTRvideos)，了解此应用的使用方法和优点。有关详细信息，请参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html 处提供的 *Cisco Secure Firewall Threat Defense* 和 *SecureX* 威胁响应集成指南。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 点击用于**将事件发送至思科云**选项的**启用**/**禁用**控件，可以根据需要更改设置。

步骤 3 当您启用该服务时，系统会提示您选择要发送到云的事件。稍后，您可以点击所选事件列表旁边的**编辑**以更改这些选项。选择要发送的事件类型并点击**确定**。

- **文件/恶意软件** - 适用于在任何访问控制规则中应用的任何文件策略。
- **入侵** - 适用于在任何访问控制规则中应用的任何入侵策略。

- **连接** - 适用于已启用日志记录的访问控制规则。选择此选项后，您还可以选择发送所有连接事件，或者只发送高优先级连接事件。高优先级连接事件是指与触发入侵、文件或恶意软件事件的连接相关，或与匹配安全智能阻止策略的连接相关。

取消注册云服务

如果不想再使用任何云服务，则可以从云中取消注册设备。您可能希望在从服务中删除设备或以其他方式处理设备时取消注册。如果需要更改云服务区域，请先取消注册，然后在重新注册时选择新区域。

使用此程序从云中取消注册不会影响智能许可注册。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”(System Settings) 页面，只需点击目录中的**云服务 (Cloud Services)**。

步骤 2 从齿轮 (⚙) 下拉列表中选择**取消注册云服务**。

步骤 3 阅读警告并点击**取消注册**。

已启用的任何云服务都将自动禁用，并且您将无法再启用这些服务。但现在会显示注册云的控件，您可以重新注册。

启用或禁用网络分析

启用网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。

默认启用网络分析。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **网络分析**链接。

如果已经位于“系统设置”页面中，只需点击目录中的**网络分析 (Web Analytics)**。

步骤 2 点击**网络分析 (Web Analytics)** 功能的**启用/禁用 (Enable/Disable)** 控件，根据需要更改设置。

配置 URL 过滤首选项

系统从思科 综合安全智能（CSI、思科 Talos 智能小组 (Talos)）获取 URL 类别和信誉数据库。这些首选项控制数据库更新和系统如何处理类别或信誉未知的 URL。必须启用 URL 过滤许可证，才能设置这些首选项。

开始之前

Cisco Secure Firewall 200 不维护本地 URL 数据库。因此，对于此类设备，以下选项不可用或不支持：**启用自动更新**、**仅限本地数据库**的URL查询源，以及**本地数据库和思科云**选项。**思科云查找**是唯一允许的选项，且无法取消选择。

过程

步骤 1 点击 **设备**，然后点击**系统设置** > **URL 过滤首选项**链接。

如果已在“系统设置”页面，只需点击目录中的 **URL 过滤首选项**。

步骤 2 配置以下选项：

- **启用自动更新** - 允许系统自动检查和下载更新的 URL 数据，这些数据中包括类别和信誉信息。系统每30分钟检查一次更新，不过数据通常每天更新一次。默认会启用更新。如果取消选中该选项，并且在使用类别和信誉过滤，请定期启用该功能以获得新的 URL 数据。
- **URL 查询源**- 要获取 URL 的类别和信誉的查询源。
  - **Local Database Only**- 仅在本地URL过滤数据库中查找类别和信誉。如果没有匹配项，URL将被取消分类，没有信誉。此方法可能会受到限制，特别是在存储有限的低端系统上，因此 URL 过滤数据库较小。
  - **本地数据库和 Cisco Cloud** — 如果本地数据库中无匹配项，将查询 Cisco Cloud 以获取更新的类别/信誉信息。如果及时收到响应，则将其用于匹配目的。否则，如果没有匹配项，URL 将被取消分类，没有信誉。
  - **仅 Cisco 云**- 始终向 Cisco 云查询类别和信誉信息。请勿使用本地 URL 数据库。
- **URL 生存时间**（选择**对未知 URL 查询 Cisco CSI** 时可用）- 特定 URL 的类别和信誉查找值的缓存时间。生存时间到期时，下一个 URL 访问尝试将导致新的类别/信誉查找。更短的时间会产生更准确的 URL 过滤，较长的时间会给未知 URL 带来更好的表现。您可以将 TTL 设置为 2、4、8、12、24 或 48 小时、一周或从不（默认）。

步骤 3 您可以根据需要**检查 URL 的类别**。

您可以检查特定 URL 的类别和信誉。在**待检查的 URL** 框中输入 URL，然后点击**前往**。系统会将您转至外部网站以查看结果。如果您对分类持有不同意见，请点击**提交 URL 类别争议**链接，将您的想法反馈给我们。

步骤 4 点击保存。

从 防火墙设备管理器 切换到 或 Security Cloud Control

如果要从 防火墙设备管理器进行切换，您可以将 Firewall Threat Defense 设备配置连接到 或 Security Cloud Control 进行管理。

注释 Security Cloud Control可以使用云交付的管理中心来管理 Firewall Threat Defense 设备。Security Cloud Control 中的简化设备管理器功能仅适用于已经在此模式下管理 Firewall Threat Defense的现有用户。此程序仅适用于云交付的管理中心。

当您使用 防火墙设备管理器执行 /Security Cloud Control 设置时， 在您切换到 /Security Cloud Control 进行管理时，除管理接口和管理器访问设置外，会保留在 防火墙设备管理器 中完成的所有接口配置。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 Firewall Threat Defense CLI 为 /Security Cloud Control执行初始设置时，仅保留管理接口和管理器访问设置（例如，不保留默认的内部接口配置）。

切换到 /Security Cloud Control后，您将无法再使用 防火墙设备管理器 管理 Firewall Threat Defense 设备。

开始之前

如果防火墙已配置为高可用性，您必须首先使用 防火墙设备管理器 （如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 如果您将防火墙注册到思科智能软件管理器，则必须在切换管理器之前取消注册防火墙。请参阅取消注册设备。

取消注册防火墙会释放基本许可证和所有功能许可证。如果不取消注册防火墙，这些许可证将保持分配给思科智能软件管理器中的防火墙。

步骤 2 （可能需要）配置管理接口。请参阅配置管理接口。

您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用 防火墙设备管理器 连接的管理接口，则必须重新连接到 防火墙设备管理器 。

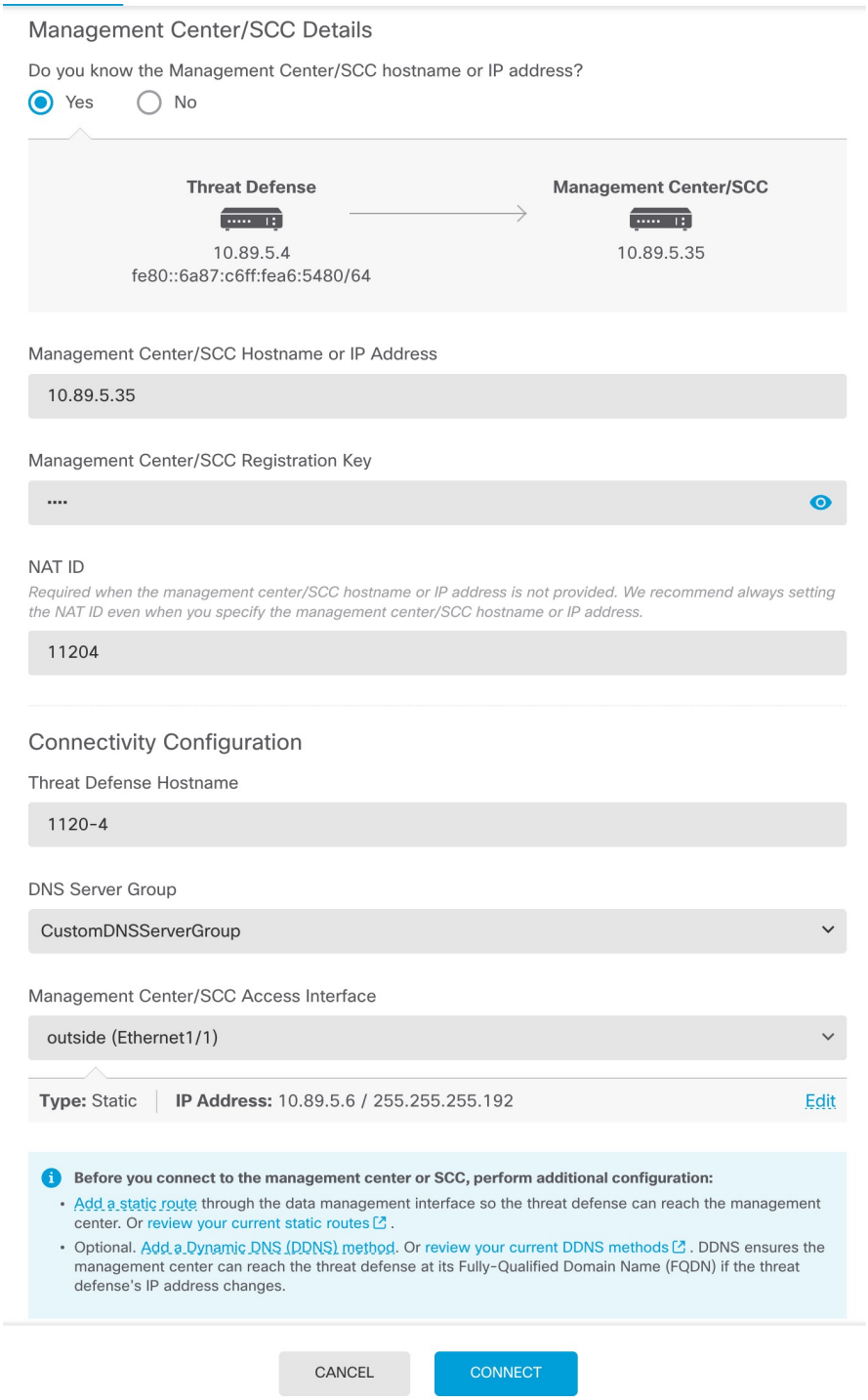
- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。

- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

步骤 3 选择**设备** > **系统设置** > **集中管理**，然后点击**继续**以设置 /Security Cloud Control 管理。

步骤 4 配置**管理中心/SCC 详细信息**。

图 *1:* 管理中心/*SCC* 详细信息



a) 对于**是否知道管理中心/SCC 主机名或 IP 地址？**，如果您可以使用 IP 地址或主机名访问 /Security Cloud Control，请点击**是**，如果 Security Cloud Control 位于 NAT 之后或没有公共 IP 地址或主机名，请点击**否**。

必须至少有一个设备（ /Security Cloud Control 或 Firewall Threat Defense 设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。

b) 如果您选择**是 (Yes)**，则输入**管理中心/SCC 主机名或 IP 地址**。

c) 指定**管理中心/SCC 注册密钥**。

此密钥是您选择的一次性注册密钥，注册Firewall Threat Defense设备时也要在 /Security Cloud Control上指定它。注册密钥必须为2到36个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 可用于将多台设备注册到 /Security Cloud Control。

a) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在 /Security Cloud Control上指定它。NAT ID 必须介于 2 到 36 个字符之间。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能 用于将任何其他设备注册到 /Security Cloud Control。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。我们建议您始终使用 NAT ID，即使它是可选的，但在以下情况下必须使用：

- 您将 IP 地址设置为 **DONTRESOLVE**。
- 在 上添加设备时，您没有指定可访问的设备 IP 地址或主机名。
- 即使双方都指定了 IP 地址，也只能使用数据接口进行管理。
- 使用多个管理接口。

步骤 5 配置**连接配置**。

a) 指定 **FTD 主机名**。

如果您使用数据接口进行**管理中心/SCC 访问接口**访问，则此 FQDN 将用于此接口。

b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

如果要为**管理中心/SCC访问接口**选择数据接口，则此设置会设置数据接口DNS服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在 /Security Cloud Control上，数据接口 DNS 服务器在您分配给此 Firewall Threat Defense 的平台设置策略中配置。当您将Firewall Threat Defense设备添加到/Security Cloud Control时，本地设置将保留，并且DNS服务器 不会 添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 Firewall Threat Defense 设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 /Security Cloud Control 和 Firewall Threat Defense 设备同步。

此外，仅当在初始注册时发现 DNS 服务器， /Security Cloud Control 才会保留本地 DNS 服务器。

如果要为 管理中心/ **访问接口**访问接口选择管理接口，则此设置会配置管理 DNS 服务器。

c) 对于**管理中心/SCC访问接口**，请选择任何已配置的接口。

将Firewall Threat Defense设备注册到/Security Cloud Control后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 6 （可选） 如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到 /Security Cloud Control之前手动配置默认路由。 有关配置静态路由的更多信息，请参阅配置静态路由。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。请参阅配置管理接口。

步骤 7 （可选） 如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保 /Security Cloud Control 可接通完全限定域名 (FQDN) 的 Firewall Threat Defense 设备。参阅**设备** > **系统设置** > **DDNS 服务**配置动态 DNS。

如果您在将Firewall Threat Defense设备添加到/Security Cloud Control之前配置 DDNS，则Firewall Threat Defense设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便Firewall Threat Defense设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。 Firewall Threat Defense支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (https://help.dyn.com/remote-access-api/)。

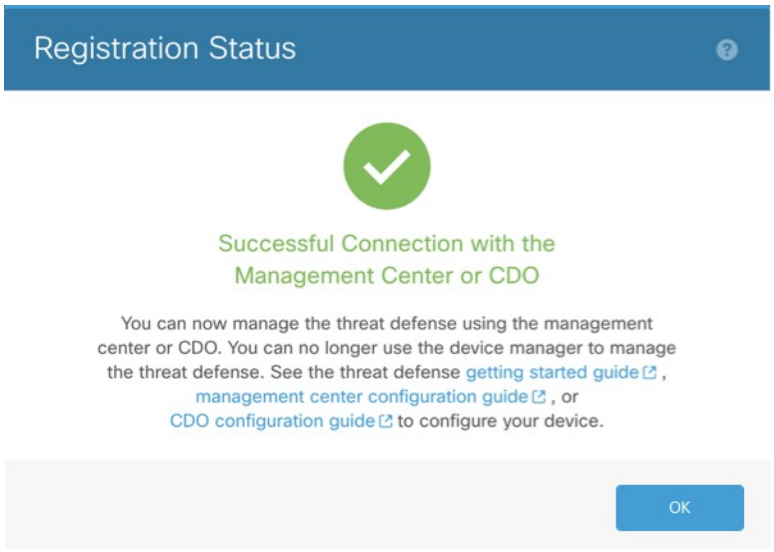
使用管理接口访问管理器时，不支持 DDNS。

步骤 8 点击**连接 (Connect)**。**注册状态** 对话框显示切换到 /Security Cloud Control的当前状态。在**保存管理中心/SCC 注册设置**步骤后，转到 /Security Cloud Control，并添加防火墙。

如果要取消切换到 /Security Cloud Control，请点击 **取消注册**。否则，请在**保存管理中心/SCC 注册设置**步骤之后关闭防火墙设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到 防火墙设备管理器时才会恢复。

如果您在**保存管理中心/SCC 注册设置**步骤后保持连接到 防火墙设备管理器，您最终将看到**与管理中心/SCC** 成功连接对话框。您将断开与 防火墙设备管理器 的连接。

图 2: 成功连接



从 或 Security Cloud Control 切换到 防火墙设备管理器

您可以将当前由本地部署或云交付的管理的Firewall Threat Defense设备配置为使用防火墙设备管理器设备。

您可以从切换到防火墙设备管理器，而无需重新安装软件。在从切换到防火墙设备管理器之前，请确认防火墙设备管理器 满足您的所有配置要求。如果要从 防火墙设备管理器 切换到 ，请参阅从 防火墙设备管理器 切换到 或 Security Cloud Control ， 第 32 页。

⚠

注意 切换到 防火墙设备管理器 会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

过程

步骤 1 在 中，从**设备 (Devices)** > **设备管理 (Device Management)** 页面删除防火墙。

步骤 2 使用 SSH 或控制台端口连接到 Firewall Threat Defense CLI。如果使用 SSH，请打开与 **管理 IP 地址** 的连接，并使用 **admin** 用户名（或具有管理员权限的任何其他用户）登录 Firewall Threat Defense CLI。

控制台端口默认为 FXOS CLI。使用 **connect ftd** 命令连接到 Firewall Threat Defense CLI。SSH 会话直接连接到 Firewall Threat Defense CLI。

如果无法连接到管理 IP 地址，请执行以下操作之一：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。使用 **configure network ipv4/ipv6 manual** 命令。

步骤 3 验证您当前处于远程管理模式之下。

show managers

示例：

```
> show managers
Type                    : Manager
Host                    : 10.89.5.35
Display name            : 10.89.5.35
Identifier              : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration            : Completed
```

步骤 4 删除远程管理器，进入无管理器模式。

configure manager delete *uuid*

无法直接从远程管理转至本地管理。 如果定义了多个管理器，则需要指定标识符（也称为 UUID；请参阅 **show managers** 命令）。单独删除每个管理器条目。

示例：

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

步骤 5 配置本地管理器。

configure manager local

现在，您可以使用 Web 浏览器在 **https://***management-IP-address* 位置打开本地管理器。

示例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

配置 TLS/SSL 密码设置

SSL 密码设置控制允许使用哪些 TLS 版本和加密密码套件来建立与设备的 TLS/SSL 连接。

通常，您配置的密码套件应具有多个可用的加密密码套件。系统将确定客户端和 Firewall Threat Defense 设备都支持的最高 TLS 版本，然后选择两者都支持且与该 TLS 版本兼容的密码套件。系统将选择两个终端都支持的最强 TLS 版本和密码套件，以确保在您允许的密码中建立最安全的连接。

开始之前

默认情况下，系统使用 DefaultSSLCipher 对象定义允许的密码套件。您也可以选择其他预定义加密套件对象，或创建自定义对象。理想的情况是，创建一个对象，其中包括所有且仅包括您希望允许的 TLS 版本和密码。如需创建自定义对象，请参阅配置 TLS/SSL 密码对象，第 40 页。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **SSL 设置**链接。

步骤 2 配置 **SSL 设置**：

这些设置控制在建立远程访问 VPN 连接时，允许客户端使用的加密套件。

- **密码** - 选择定义允许的 TLS 版本和加密算法的 SSL 密码对象。

  如果需要立即创建对象，请点击列表底部的**创建新密码**。

- **临时 Diffie-Hellman 组** - 用于临时加密算法的 DH 组。有关 DH 组的说明，请参阅决定要使用的 Diffie-Hellman 模数组。默认值为 14。

- **椭圆曲线 DH 组** - 用于椭圆曲线加密算法的 DH 组。默认值为 19。

步骤 3 配置**防火墙设备管理器 Web 服务器**。

使用“Web 服务器 SSL 设置”限制可用于连接 防火墙设备管理器 的加密套件。

点击**设为与 SSL 设置相同**，可配置与 RA VPN 连接定义相同的加密套件。

否则，请选择定义允许使用的 TLS 版本和加密算法的 SSL 加密套件对象。

步骤 4 配置**身份 Web 服务器**。

使用身份 Web 服务器 SSL 设置，限制可用于连接强制网络门户的加密套件，以执行主动身份验证身份规则。确保用户终端支持这些加密套件；否则，将无法完成主动身份验证，其身份也无法用于访问控制。

点击**设为与 SSL 设置相同**，可配置与 RA VPN 连接定义相同的加密套件。

否则，请选择定义允许使用的 TLS 版本和加密算法的 SSL 加密套件对象。

步骤 5 点击**保存**。

配置 TLS/SSL 密码对象

SSL 密码对象定义在建立与 Firewall Threat Defense 设备的 SSL 连接时可以使用的安全级别、TLS/DTLS 协议版本和加密算法的组合。在**设备** > **系统设置** > **SSL 设置**中使用这些对象为与设备建立 SSL 连接的用户定义安全要求。

您可以选择的 TLS 版本和密码由您的智能许可证账户控制。如果满足出口合规性要求，则可以选择选任意组合选项。如果您的许可证不符合出口要求，则只能使用最低安全选项 TLSv1.0 和 DES-CDC-SHA。评估模式被视为不合规模式，因此在许可系统之前，您的选项会受到限制。

系统中包括多个预定义对象。仅当预定义对象不符合安全要求时，才需要创建新对象。这些对象为：

- DefaultSSLCipher—这是一个自定义级别组，提供合理的安全性。它是 SSL 设置中使用的默认值。
- CiscoRecommendedCipher - 这是一个安全级别较高的组，仅包括最安全的密码和 TLS 版本。此组具有最高的安全性，但您需要确保您的客户端可以使用匹配的密码。由于密码不匹配问题，某些客户端无法完成连接的可能性更大。
- FIPSCipher — 此自定义组包含符合联邦信息处理标准 (FIPS) 的密码，该标准由美国国家标准与技术研究院 (NIST) 制定，供美国联邦政府机构及其承包商使用。使用此密码对象可提供 FIPS 兼容性，但不会将系统切换为运行完全符合 FIPS 规范的加密模块。

过程

步骤 1 选择**对象**，然后从目录中选择 **SSL 密码**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的**名称**和说明（后者为可选项）。

步骤 4 配置以下选项：

- **安全级别** - 对象的相对安全级别。请注意，如果在选择安全级别后编辑协议版本或密码套件列表，则对象提供的实际安全级别可能与选择的安全级别不匹配。选择以下其中一个选项：
  - **全部** - 在对象中包括从低安全性到高安全性的所有 TLS 级别和密码套件。
  - **低** - 包括所有 TLS 版本和密码，允许用户使用安全性最低的密码完成连接。对于非出口合规许可证，这包括 TLSv1.0 和 DES-CBC-SHA。
  - **中** - 包括所有 TLS 版本，但会删除一些相对不安全的密码。此选项与“低”/“全部”选项之间的差异极小。不能将此选项用于非出口合规许可证。

- **高** - 仅允许最新的 DTLS 和 TLS 版本，以及适用于这些版本的密码。此选项将连接限制为当前可用的最安全密码。不能将此选项用于非出口合规许可证。
- **自定义** - 想要单独选择 TLS 版本和密码时选择此选项。您选择的选项将决定您是定义高安全加密设置还是低安全加密设置。虽然自定义对象没有默认设置，但如果您在选择自定义之前选择了另一个级别，则为方便起见，之前显示的选项将保持选中状态。

- **协议版本**- 允许客户端在与 Firewall Threat Defense 设备建立 TLS/SSL 连接时使用的 TLS/DTLS 版本。对于自定义对象，请选择要支持的版本。对于其他安全级别，最好不要编辑列表，但您可以根据需要添加或删除版本。
- **适用的密码套件** - 客户端可以使用的加密算法。点击 **+** 可添加新套件；点击某个套件上的 **x** 可将其删除。

  您选择的协议版本控制此列表中可用的套件。如果更改协议版本，系统将标记不再适用于所选版本的所选套件：您必须删除这些版本或重新添加所需的协议版本。

步骤 5 点击**确定**。

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。