零信任网络访问

以下主题提供有关 无客户端 Cisco Zero Trust 访问、通用零信任网络访问 的详细信息，以及如何配置和部署它们。

关于无客户端和通用 Zero Trust 网络访问

Zero Trust 访问 或 Zero Trust 网络访问 (ZTNA) 是指使用基于身份的访问来保护内部资源的进程，包括用户信任和终端安全评估。该流程先验证用户、设备和请求上下文，然后再允许访问内部资源和应用。仅在验证用户、了解请求上下文并评估任何风险后，它才会授予最低权限访问权限。

您可以在两个 ZTNA 部署模式之间进行选择：

- 无客户端 Cisco Zero Trust 访问
- 通用零信任网络访问

无客户端 Cisco Zero Trust 访问

无客户端零信任网络访问（无客户端 ZTNA）可对来自网络内部（本地）或外部（远程）的受保护的基于 Web 的资源和应用进行身份验证和授权访问。这是使用具有安全断言标记语言 (SAML) 身份验证的外部身份提供程序 (IdP) 来完成的。用户设备上不需要安装客户端软件。

无客户端 ZTNA 非常适合远程用户访问 Web 应用和非托管设备。

通用零信任网络访问

通用 Zero Trust 网络访问（通用 ZTNA）是一种基于客户端的解决方案，无论用户位于何处，它都可以提供对所有内部资源的基于身份的访问。它为每个应用和用户实施强认证、终端安全评估和流量检查。

通用 ZTNA 支持远程和本地用户。本地用户使用 Cisco Secure Firewall Threat Defense 设备访问受信任的网络。远程用户通过基于云的安全访问服务访问可信网络，该服务会在云中安全地评估策略并代理用户流量。

无客户端 Cisco Zero Trust 访问

无客户端 Cisco Zero Trust 访问 基于 Zero Trust 访问原则。Zero Trust 访问是一种消除隐式信任的 Zero Trust 安全模型。该模型在验证用户、请求的上下文以及分析风险（如果授予访问权限）后授予最低权限访问权限。

无客户端 Cisco Zero Trust 访问 允许您使用外部安全断言标记语言 (SAML) 身份提供程序 (IdP) 策略，从网络内部（本地）或外部（远程）对受保护的基于 Web 的资源和应用程序进行身份验证和授权访问。

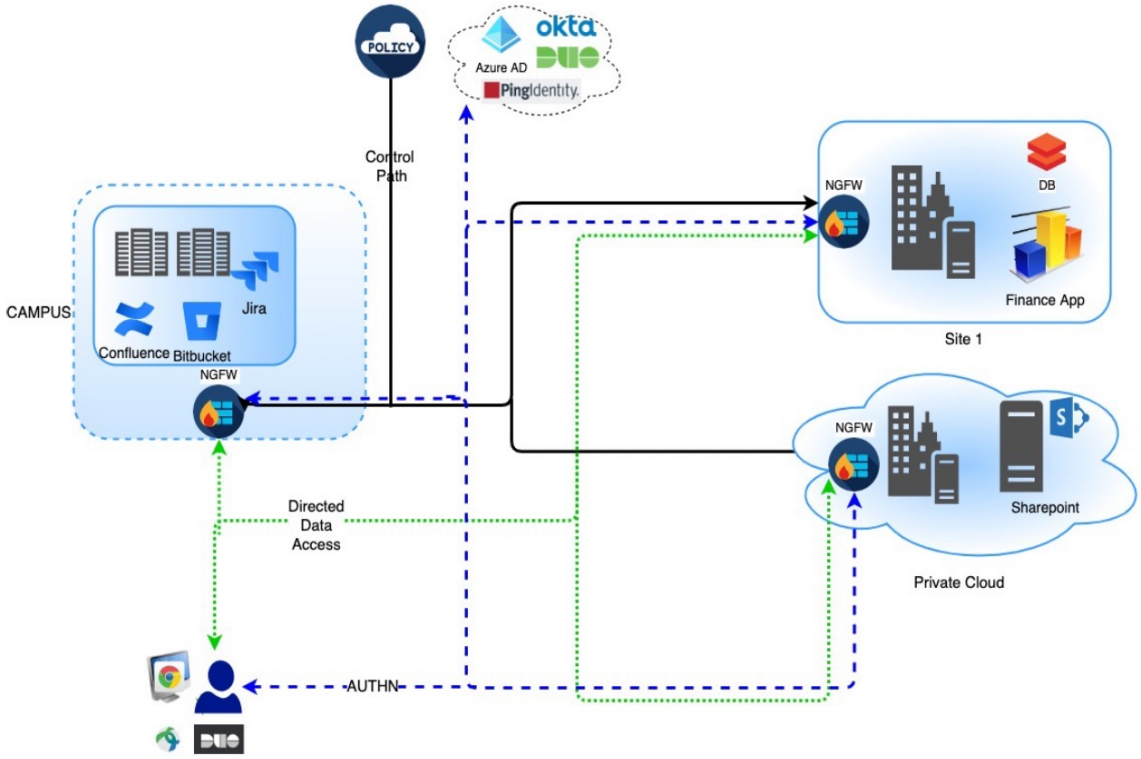
功能如下：

- 支持多个基于 SAML 的身份提供商，如 Duo、Azure Active Directory (Azure AD)、Okta 和其他身份提供商。
- 终端（客户端设备）上不需要思科 Cisco Secure 客户端 等客户端应用来进行安全访问。
- 通过浏览器进行访问和身份验证。
- 仅支持 TLS Web 应用。
- 通过代理（例如 Duo Health）支持客户端设备状态，使用该代理可以根据 Duo 中的策略评估设备的状态，并且可以基于相同的策略提供访问。可以与支持使用其代理（例如 Okta 或 PingID）进行安全评估的第三方身份提供程序一起执行相同的功能。
- 支持 HTTP 重定向 SAML 绑定。
- 支持应用组，便于在一组应用上启用 无客户端 Cisco Zero Trust 访问保护。
- 对 Zero Trust 应用流量利用威胁防御入侵和恶意软件防护。

您可以使用 Cisco Secure Firewall Management Center Web 界面创建 Zero Trust 应用策略，以便定义专用应用并向其分配威胁策略。该策略是应用特定的，其中管理员根据该应用的威胁感知来决定检测级别。

威胁防御如何与 Zero Trust 访问配合使用

图 *1:* 威胁防御部署



1. 远程或本地用户使用浏览器发送 HTTPS 请求，以从终端连接到应用。
2. HTTPS 请求被保护应用的防火墙拦截。
3. 防火墙将用户重定向到应用的已配置 IdP 进行身份验证。

注释 在图中，每个防火墙保护一组 Web 应用。用户可以在认证和授权后直接访问防火墙后面的应用。

4. 身份验证和授权过程完成后，防火墙允许用户访问应用。

为何使用 Zero Trust 网络访问？

Zero Trust 网络访问 (ZTNA) 通过要求每次连接都进行显式授权，提供安全、分段的访问。此方法减少了攻击面，并简化了安全迁移，无需增加设备。

ZTNA 利用您现有的威胁防御部署作为应用程序访问的实施点，实现分段和按应用程序授权。它为远程和本地用户建立独立的隧道。

此功能对用户隐藏网络，并确保他们只能访问已明确授权的应用程序。对网络中的一个应用进行授权不会为网络上的其他应用提供隐式授权，从而显着减少受攻击面。换句话说，对应用程序或资源的每次访问都必须经过明确授权。

通过在威胁防御中添加 Zero Trust 访问功能，您可以采纳更安全访问模型，而无需在网络中安装或管理额外设备。

无客户端 Cisco Zero Trust 访问 配置的组件

新的配置包括 Zero Trust 应用策略、应用组和应用。

- **Zero Trust 应用策略**-包括 Zero Trust 应用策略、应用组和应用。安全区域和安全控制设置在全局级别与所有未分组的应用和应用组关联。

  默认情况下，为策略分配全局端口池。从这个池中自动为配置的每个专用应用分配一个唯一的端口。

  Zero Trust 应用策略包括应用组、分组或未分组的应用。

- **应用组**- 由一组共享 SAML 身份验证设置的应用组成，可以选择性地共享安全区域和安全控制设置。

  应用组从全局策略继承安全区域和安全控制设置，并且可以覆盖这些值。

  创建应用组后，可以使用相同的 SAML IdP 配置对多个应用进行身份验证。属于应用组的应用继承应用组的 SAML 配置。这样就无需为每个应用配置 SAML 设置。创建应用组后，可以向其中添加新应用，而无需为其配置 IdP。

  当最终用户尝试访问属于组的应用时，用户将首次通过应用组的身份验证。当用户尝试访问属于同一应用组的其他应用时，系统会为用户提供访问权限，而不会再次重定向到 IdP 进行身份验证。这可以防止应用访问请求使 IdP 过载，并在启用限制的情况下优化 IdP 的使用。

- **应用**- 有两种类型：
  - **未分组的应用**- 是独立的应用。必须为每个应用配置 SAML 设置。应用从全局策略继承安全区域和安全控制设置，并且可以由应用覆盖。
  - **分组应用**- 是指在应用组下分组的多个应用。SAML 设置继承自应用组，无法被覆盖。但是，可以为每个应用覆盖安全区域和安全控制设置。

配置需要以下证书：

- **身份证书**- Firewall Threat Defense 使用此证书伪装成应用。Firewall Threat Defense 充当 SAML 服务提供商 (SP)。此证书必须是与专用应用的 FQDN 匹配的通配符或使用者备用名称 (SAN) 证书。它是受 Firewall Threat Defense保护的所有应用的通用证书。
- **IdP 证书**- IdP 为每个定义的应用或应用组提供一个证书。必须配置此证书，以便 Firewall Threat Defense 可以验证 IDP 对传入 SAML 断言的签名。

注释 IdP 证书通常包含在元数据文件中；否则，用户需要在应用配置期间随时可用 IdP 证书。

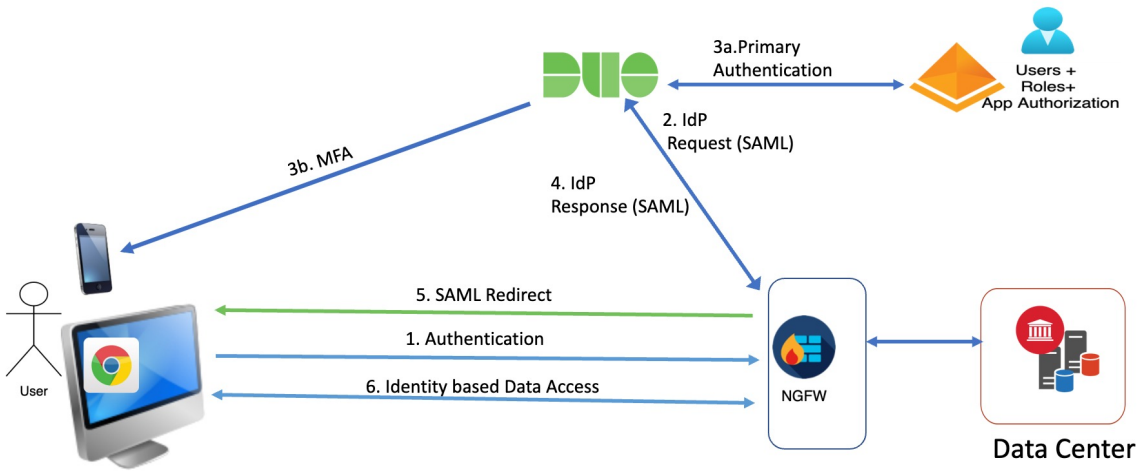
- **应用证书**- Firewall Threat Defense 使用此证书解密从用户到应用的加密流量，以进行检查。

注释 即使我们不执行 IPS/恶意软件检查，也需要此证书来验证信头中的 Cookie 以授权连接。

无客户端 Cisco Zero Trust 访问 工作流程

此图描绘了 Zero Trust 访问工作流程。

图 *2:* 无客户端 ***Zero Trust*** 网络访问工作流程



工作流程如下：

1. 用户在浏览器中键入应用 URL。
   - 如果 HTTPS 请求有效，则用户将被重定向到映射端口（步骤 6）。
   - 如果 HTTPS 请求无效，则发送用户进行身份验证（第 2 步）。
2. 用户被重定向到已配置的身份提供程序 (IdP)。
3. 1. 用户将被重定向到已配置的主身份验证源。
   2. 用户将使用已配置的辅助多因素身份验证（如果有）进行质询。
4. IdP 向威胁防御发送 SAML 响应。通过浏览器从 SAML 响应中检索用户 ID 和其他必要参数。

5. 用户被重定向到应用。
6. 验证成功后，允许用户访问应用。

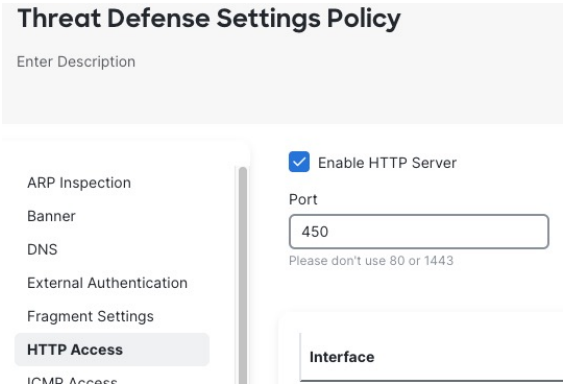
无客户端 Cisco Zero Trust 访问 的限制

- 仅支持启用了 TLS 的 Web 应用。所有流量都必须解密。
- 仅支持 SAML 身份提供程序。
- 支持 IPv6；但是，您只能使用同构网络地址转换 (NAT) 场景，例如 NAT66 和 NAT44。

  不支持 NAT64 和 NAT46 场景。
- 仅在启用了 Snort 3 时，才能对 Firewall Threat Defense 进行无客户端 Zero Trust 访问。
- 默认情况下，Firewall Threat Defense 设备会使用端口 443 进行安全通信。由于这与可能被配置为 Zero Trust 网络访问的启用 TLS 的应用使用的端口相同，因此，您必须更改设备的 HTTP 服务器端口。

  转至 **设备** > **平台设置**，然后编辑设备的威胁防御设置策略，点击 **HTTP 访问**，选中**启用 HTTP 服务器**复选框，并在该字段中输入 443 以外的端口。完成后，点击页面右上角的**保存**。

  下图显示了一个示例。



- 受保护的 Web 应用中的所有超链接都必须具有相对路径，并且在单个模式集群上不受支持。
- 在虚拟主机上或在内部负载均衡器后面运行的受保护 Web 应用必须使用相同的外部和内部 URL。
- 在启用了严格 HTTP 主机报头验证的应用上不受支持。
- 如果应用服务器托管多个应用并根据 TLS 客户端 Hello 中的服务器名称指示 (SNI) 报头提供内容，则 Zero Trust 应用配置的外部 URL 必须与该特定应用的 SNI 匹配。

Zero Trust 应用策略的前提条件

前提条件类型	说明
许可	• 具有出口管制功能的智能许可证账户 • （可选）IPS 和威胁许可证 - 如果使用安全控制，则为必填项。
配置	创建与专用应用的 FQDN 匹配的通配符或使用者备用名称 (SAN) 证书。有关详细信息，请参阅添加证书注册对象。
	通过监管对专用应用的访问来创建安全区域。有关详细信息，请参阅创建安全区域和接口组对象。

管理 Zero Trust 应用策略

您可以创建、编辑和删除 Zero Trust 应用策略。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 管理 Zero Trust 访问策略：

- 创建 - 点击 **新建策略**。请参阅 创建 Zero Trust 应用策略， 第 7 页
- 编辑 - 点击 **编辑** ()。请参阅 编辑 Zero Trust 应用策略， 第 13 页
- 报告 - 点击 **报告** ()。
- 删除 - 点击 **删除** ()。

步骤 3 点击**保存**。

下一步做什么

在将配置部署到威胁防御之前，请确保没有警告。要部署配置更改，请参阅 Cisco Secure Firewall Management Center 管理指南中的部署配置更改。

创建 Zero Trust 应用策略

此任务配置 Zero Trust 应用策略。

开始之前

确保满足Zero Trust 应用策略的前提条件，第 7 页中列出的所有前提条件。

过程

步骤 1 选择**策略** > **安全策略** > **Zero Trust 应用**。

步骤 2 点击**添加策略 (Add Policy)**。

步骤 3 在 **常规** 部分中，在 **名称** 字段中输入策略名称。说明字段是可选的。

步骤 4 在 **域名** 字段中输入域名。

确保域名已添加到 DNS。域名解析为访问应用的Firewall Threat Defense网关接口。域名用于为应用组中的所有专用应用生成 ACS URL。

如果在下一步中选择 ACME 证书作为策略的身份证书，则域名必须与 ACME 证书的公用名 (CN) 匹配。

注释
更改域名后，SAML 服务提供商 (SP) 元数据将随之更新。必须重新配置以下设置：

- 使用新 SAML SP 元数据的 IdP
- 使用新域名的 DNS 服务器

如果在更改域名后进行部署，系统将移除并重新添加所有应用，这会导致应用访问中断。

步骤 5 从 **身份证书** 下拉列表中选择现有证书。

点击 **添加** (+) 图标以配置证书注册对象。有关详细信息，请参阅 添加证书注册对象。

可以选择 ACME 证书，将 Firewall Threat Defense 设备作为 SAML SP 进行身份验证，以用于 Zero Trust 应用策略。ACME 证书可自动执行 SSL 和 TLS 证书的生命周期管理，包括自动续约。

步骤 6 从 **安全区域** 下拉列表中选择安全区域。

点击 **添加** (+) 图标以添加新的安全区域。

要添加安全区域，请参阅 创建安全区域和接口组对象。

步骤 7 在 **全局端口池** 部分，显示默认端口范围。如果需要，请修改。端口值范围为 1024 到 65535。此池中的唯一端口分配给每个专用应用。

注释
此端口范围应避免与现有 NAT 范围发生任何冲突。

步骤 8 （可选）在 **安全控制** 部分，您可以添加入侵或恶意软件和文件策略：

- **入侵策略**- 从下拉列表中选择默认策略，或点击 **添加** (+) 图标以创建新的自定义入侵策略。有关详细信息，请参阅最新版本的 Cisco Secure Firewall Management Center Snort 3 配置指南中的创建自定义 Snort 3 入侵策略主题。

- **变量集**- 从下拉列表中选择默认变量集，或点击 **添加** (+) 图标以创建新的变量集。有关详细信息，请参阅 创建变量集。

  注释
  要使用变量集，必须拥有托管设备的 Cisco Secure Firewall Threat Defense IPS 许可证。

- **恶意软件和文件策略**- 从下拉列表中选择现有策略。点击 **添加** (+) 图标来创建新的恶意软件和文件策略。有关详细信息，请参阅管理文件策略。

步骤 9 点击**保存**保存策略。

下一步做什么

1. 创建应用组。请参阅创建应用组， 第 9 页。
2. 创建应用。请参阅创建应用， 第 10 页。
3. 将 Zero Trust 应用策略与设备关联。请参阅 为目标设备设置 Zero Trust 访问策略， 第 12 页
4. 部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

创建应用组

开始之前

创建 Zero Trust 应用策略， 第 7 页

过程

步骤 1 点击 **添加应用组**。

步骤 2 在 **应用组** 部分，在 **名称** 字段中键入名称，然后点击 **下一步**。

步骤 3 在 **SAML 服务提供商 (SP) 元数据** 部分，数据是动态生成的。复制 **实体 ID** 和 **断言使用者服务 (ACS) URL** 字段的值，或点击 **下载 SP 元** 数据以 XML 格式下载此数据，以便将其添加到 IdP。点击**下一步 (Next)**。

步骤 4 在 **SAML 身份提供程序 (IdP) 元数据** 部分，使用以下任一方法添加元数据：

- **XML 文件上传**- 选择文件或拖放 XML 文件。

  系统将显示 **实体 ID**、 **单点登录 URL**和 **IdP 证书** 的详细信息。

- **手动配置**- 执行以下步骤：
  - **实体 ID** - 输入在 SAML IdP 中定义的用于唯一标识服务提供商的 URL。
  - **单点登录 URL** - 输入用于登录到 SAML 身份提供程序服务器的 URL。

- **IdP 证书** - 选择注册到威胁防御以验证由 IdP 签名的消息的 IdP 的证书。

  点击 **添加** (+) 图标来配置新的认证登记对象。有关详细信息，请参阅添加证书注册。

- **稍后配置**- 如果没有 IdP 元数据，可以稍后配置。

点击**下一步 (Next)**。

步骤 5 在 **重新身份验证间隔** 部分中，在 **超时间隔** 字段中输入值，然后点击 **下一步**。

重新身份验证间隔允许您提供一个值，以确定用户何时必须再次进行身份验证。

步骤 6 在 **安全区域和安全控制** 部分，从父策略继承安全区域和威胁设置。您可以覆盖这些设置。点击**下一步 (Next)**。

步骤 7 检查配置摘要。在任何区域，点击 **编辑** 以修改详细信息。点击 **Finish**。

步骤 8 点击**保存**。

应用组已创建，并显示在“Zero Trust 应用”页面上。

下一步做什么

1. 创建应用， 第 10 页。
2. 部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

创建应用

使用此任务可创建已分组或未分组的应用。

开始之前

1. 创建 Zero Trust 应用策略， 第 7 页。
2. 创建应用组， 第 9 页 （仅分组应用需要）。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 选择策略。

步骤 3 点击**添加应用 (Add Application)**。

步骤 4 在 **应用设置** 部分中，填写以下字段：

- **应用名称**-输入应用名称。
- **外部 URL**- 输入用户用于访问应用的 URL。

- **应用 URL**-默认情况下，外部 URL 用作应用 URL。取消选中 **使用外部 URL 作为应用 URL** 复选框来指定不同 URL。

  如果威胁防御使用内部 DNS，则应用程序 URL 必须与该 DNS 中的条目匹配，以确保它解析到应用程序。此外，如果输入的完全限定域名 (FQDN) 既可以是 IPv4，也可以是 IPv6 地址，则 FQDN 必须同时解析为 IPv4 和 IPv6。威胁防御不在这些类型的地址之间进行转换。

- **应用证书**- 选择专用应用的证书。点击 **添加** (+) 图标可配置内部证书对象。有关详细信息，请参阅 添加内部证书对象。

- **源网络地址转换** — 源网络地址转换 (source NAT) 将数据包中的源 IP 地址转换为指定范围内的地址。

  启用**源网络地址转换**以指定 IP 地址范围。传入请求的源 IP 地址将转换为指定范围内的 IP 地址。源 NAT 同时适用于 IPv4 和 IPv6 地址。

  - **IPv4** — 从列表中选择 NAT 的源网络。点击 **添加** (+) 以创建网络对象。有关详细信息，请参阅 网络。
  - **IPv6** — 从列表中选择 NAT 的源网络。点击 **添加** (+) 以创建网络对象。有关详细信息，请参阅 网络。

  源 NAT 将传入请求的源 IP 地址转换为网络对象或对象组中指定的可路由 IP 地址。

  注释
  仅支持类型为“主机”或“范围”的对象或对象组。

- **应用组** - 从下拉列表中选择应用组。请参阅创建应用组，第 9 页。

  注释
  此字段不适用于未分组的应用。

步骤 5 点击**下一步 (Next)**。

步骤 6 根据应用类型：

- 对于分组应用，**SAML 服务提供程序 (SP) 元数据**、**SAML 身份提供程序 (IdP) 元数据** 和 **重新身份验证间隔** 继承自应用组，不需要由用户配置。
- 对于未分组的应用，请执行以下步骤：
  1. 在 **SAML 服务提供商 (SP) 元数据** 部分，数据是动态生成的。复制 IdP 的**实体 ID**、**断言使用者服务 (ACS) URL**，或点击**下载 SP 元数据**以 XML 格式下载此数据，以便将其添加到 IdP。点击**下一步 (Next)**。
  2. 在 **SAML 身份提供程序 (IdP) 元数据** 部分，使用以下任一方法添加元数据：
     - **XML 文件上传**- 选择文件或拖放 XML 文件。

       系统将显示 **实体 ID**、**单点登录 URL**和 **IdP 证书** 的详细信息。

     - **手动配置**- 执行以下步骤：
       - **实体 ID** - 输入在 SAML IdP 中定义的用于唯一标识服务提供商的 URL。

- **单点登录 URL** - 输入用于登录到 SAML 身份提供程序服务器的 URL。
- **IdP 证书** - 选择注册到威胁防御以验证由 IdP 签名的消息的 IdP 的证书。

  点击 **添加** (+) 图标来配置新的认证登记对象。有关详细信息，请参阅添加证书注册。

- **稍后配置** — 如果您没有 IdP 元数据，可以稍后配置。

点击**下一步 (Next)**。

3. 在 **重新身份验证间隔** 部分中，在 **超时间隔** 字段中输入值，然后点击 **下一步**。重新身份验证间隔允许您提供一个值，以确定用户何时必须再次进行身份验证。

步骤 7 在**安全区域和安全控制**部分，从策略或应用组继承安全区域和威胁设置。您可以覆盖这些设置。点击**下一步 (Next)**。

步骤 8 检查配置摘要。在任何区域，点击 **编辑** 以修改详细信息。点击 **Finish**。

步骤 9 点击**保存**。

该应用程序列在 Zero Trust 应用程序页面上，并默认启用。

下一步做什么

1. 为目标设备设置 Zero Trust 访问策略， 第 12 页。
2. 部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

为目标设备设置 Zero Trust 访问策略

每项 Zero Trust 策略可以多台设备为目标；每天设备每次只能部署一项策略。

开始之前

1. 创建 Zero Trust 应用策略， 第 7 页。
2. 创建应用组， 第 9 页。
3. 创建应用， 第 10 页。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 选择策略。

步骤 3 点击 **目标设备**。

步骤 4 使用以下任何方法之一，选择要部署策略的设备：

- 从 **可用设备** 列表中选择一个设备，然后点击 >> 或 **添加** (⊕) 图标。
- 要从 **所选设备** 列表中删除设备，请选择一个设备，然后点击 << 或 **删除** (🗑) 图标。

步骤 5 点击 **应用** 以保存策略分配。

步骤 6 点击**保存**保存策略。

下一步做什么

部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

编辑 Zero Trust 应用策略

您可以编辑 Zero Trust 应用策略、应用组或应用的设置。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 点击要编辑的 Zero Trust 应用策略旁边的 **编辑** (✎) 。

步骤 3 编辑 Zero Trust 应用策略。

您可以更改以下设置或执行以下操作：

- 名称和说明 - 点击策略名称旁边的 **编辑** (✎)，进行更改，然后点击 **应用**。
- 要修改策略设置，请执行以下操作：
  - 点击**设置**
  - 根据需要修改设置。

    重要事项
    编辑 SAML ACS URL 的域名会中断应用访问。

  - 点击**保存**。
- 要修改应用组设置，请执行以下操作：
  - 点击 **应用**。
  - 点击要编辑的应用组旁边的 **编辑** (✎) 。
  - 在每个部分中，根据需要点击 **编辑** 以修改设置

    重要事项

编辑应用组名称会中断应用访问。

- 修改部分中的设置后，点击 **应用** 。
- 点击 **完成**。
- 点击**保存**。

- 要修改应用设置，请执行以下操作：
  - 点击 **应用**。
  - 点击要编辑的应用旁边的 **编辑** ( ) 。
  - 在每个部分中，点击 **编辑** 以根据需要修改设置。

    重要事项
    编辑应用名称会中断应用访问。

  - 修改部分中的设置后，点击 **应用** 。
  - 点击 **完成**。
  - 点击**保存**。
- 要启用、禁用或删除多个应用，请选择应用，点击所需的批量操作，然后点击 **保存**。

  注释
  这些操作也可通过右键点击菜单来执行。

  - 要启用所有应用，请点击 **批量操作** > **启用**。
  - 要禁用所有应用，请点击 **批量操作** > **禁用**。
  - 要删除所有应用，请点击 **批量操作** > **删除**。
- 点击 **返回 Zero Trust 应用 (Return to Zero Trust Application)** 以返回到策略页面。

下一步做什么

部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

监控 Zero Trust 会话

连接事件

部署 Zero Trust 应用策略后，新字段可用。要将字段添加到表视图：

1. 选择**事件和日志** > **+ 显示更多** > **连接** > **事件**。

2. 点击**连接事件的表视图 (Table View of Connection Events)** 选项卡。
3. 事件表视图中的多个字段在默认情况下处于隐藏状态。要更改显示的字段，请点击任何列名称中的 **x** 图标以显示字段选择器。
4. 选择以下字段：
   - **身份验证源**
   - **Zero Trust 应用**
   - **Zero Trust 应用组**
   - **Zero Trust 应用主机**
   - **Zero Trust 应用策略**
   - **Zero Trust 源用户**
   - **Zero Trust 代理**
   - **Zero Trust 规则**
   - **Zero Trust 状态**
   - **Zero Trust 隧道 ID**
5. 点击**应用 (Apply)**。

有关连接事件的详细信息，请参阅 Cisco Secure Firewall Management Center 管理指南 中的连接和安全相关的连接事件 。

Zero Trust 控制面板

通过 Zero Trust 控制面板，您可以监控设备上活动 Zero Trust 会话的实时数据。

Zero Trust 控制面板提供由管理中心管理的排名靠前的 Zero Trust 应用和 Zero Trust 用户的摘要。选择 **洞察和报告** > **控制面板**，然后点击 **Zero Trust** 选项卡以访问控制面板。

控制面板具有以下构件：

- 热门 Zero Trust 应用
- 热门 Zero Trust 用户

CLI 命令

请登录设备 CLI 并使用以下命令：

CLI 命令	说明
show running-config zero-trust	查看 Zero Trust 配置的运行配置。
show running-config zero-trust-hybrid	查看通用 Zero Trust 配置的运行配置。

CLI 命令	说明
show zero-trust	显示运行时 Zero Trust 统计信息和会话信息。
show cluster zero-trust	显示集群中各节点的 Zero Trust 统计信息摘要。
clear zero-trust	清除 Zero Trust 会话和统计信息。
show counters protocol zero_trust	查看 Zero Trust 流命中的计数器。

诊断工具

诊断工具通过检测 Zero Trust 配置可能存在的问题来促进故障排除过程。诊断可以分为两种类型：

- **特定于应用的诊断**用于检测以下问题：
  - DNS 相关问题
  - 错误配置（例如套接字未打开）以及分类和 NAT 规则问题。
  - Zero Trust 策略或 SSL 规则的部署问题
  - 源 NAT 问题和 PAT 池耗尽问题
- **常规诊断** 用于检测以下问题：
  - 未启用强密码许可证
  - 无效应用证书
  - SAML 相关问题
  - 本地代理和集群批量同步问题

要运行诊断工具，请执行以下操作：

1. 点击要进行故障排除的 Zero Trust 应用旁边的诊断 ( )。系统将显示 **诊断** 对话框。
2. 从 **选择设备** 下拉列表中选择设备并点击 **运行**。诊断过程完成后，系统会在“报告”选项卡中生成 **报告** 。
3. 要查看、复制或下载日志，请点击 **日志** 选项卡。

通用零信任网络访问

通用零信任网络访问 (通用 ZTNA) 使管理员能够根据用户身份（包括用户信任和终端安全评估）专门允许访问内部网络资源，而无需像远程访问 VPN 那样授予对整个网络的访问权限。通用 ZTNA 是基于客户端的 ZTNA 解决方案，无论用户位于何处（远程或本地部署），都能让用户安全访问内部资源和应用。

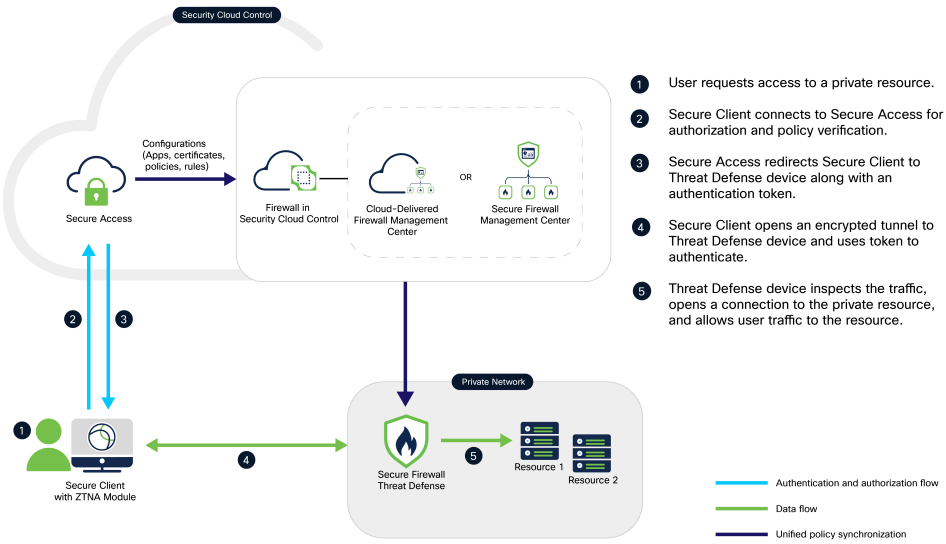
由于 通用 ZTNA 不假定授予一个应用的访问权限会隐式授权访问其他应用，因此网络攻击面得以减少。

通过强身份验证、终端安全评估验证和全面的流量检测，通用 ZTNA 确保实现最小权限、按应用、按用户的访问。它能有效保护混合环境中的应用。

通用 ZTNA 的组件

通用 ZTNA 的新配置包括安全云控制防火墙管理（以前称为 Cisco Defense Orchestrator）和“安全访问”，两者均在安全云控制平台上配置。安全云控制防火墙管理通过 Cisco Secure Firewall Management Center 来管理防火墙威胁防御设备。

图 *3:* 通用 *ZTNA* 的组件



- **安全云控制防火墙管理：**管理 Firewall Threat Defense 设备的 通用 ZTNA 策略配置和部署。威胁防御设备通过实施 通用 ZTNA 策略来保护 本地部署 资源。威胁防御会检测流量，并对流量实施入侵防御系统 (IPS)、文件和恶意软件策略。
- **安全访问：**安全访问定义用户的访问策略、终端安全评估和安全配置文件。它通过云对用户流量实施策略。
- **安全云控制平台：**安全云控制为安全访问和防火墙提供统一的安全管理平面，简化了跨两者的通用 ZTNA 策略管理。
- **安全客户端：**安全客户端安装在最终用户的设备上。它作为实施点拦截对受保护内部资源的连接请求，从而实现基于身份的安全访问。

以下部分介绍如何在威胁防御设备上启用通用 ZTNA。有关 通用 ZTNA 的完整配置，请参阅《通用 *Zero Trust* 网络访问配置指南》。

威胁防御如何与 通用 ZTNA 配合使用

启用 通用 ZTNA 的防火墙威胁防御设备是关键的实施点，通过将 Zero Trust 原则与防火墙功能相结合来保护私有资源。它通过以下方式保护私有资源：

- **实施访问并验证策略**：威胁防御设备拦截所有对私有资源的访问请求。它实施精细的、基于上下文的访问策略，在授予访问权限前验证用户身份、设备状态和上下文因素。仅允许满足最小权限标准的请求，阻止未经授权的资源访问尝试。
- **建立到资源的安全隧道**：验证访问策略后，威胁防御设备在用户设备和私有资源之间建立安全的加密隧道。此隧道确保私有资源不会直接暴露在网络中。
- **检测流量**：威胁防御设备持续检测流量，在威胁到达资源前将其阻止。设备应用入侵防御系统、文件和恶意软件检测功能来检测和阻止威胁。
- **微分段并防止横向移动**：设备通过将流量流限制为仅授权资源来实施微分段。这种隔离可防止网络内的横向移动，从而限制任何潜在漏洞的影响。

通用零信任网络访问 的前提条件

本主题讨论 通用零信任网络访问 (通用 ZTNA) 的要求和准则。

许可要求

- Cisco Secure Firewall Management Center 需要具有受控出口功能的智能许可证账户。它在 通用 ZTNA 的评估模式下无法运行。

  如果配置了入侵策略，Cisco Secure Firewall Threat Defense 设备需要 IPS 许可证。如果配置了恶意软件策略，设备需要 IPS 和恶意软件防御许可证。有关详细信息，请参阅《*Cisco Secure Firewall Management Center* 管理指南》中的“许可证”部分。
- 安全访问需要 Cisco Secure 专用访问 Essentials 或 Advantage 订用。

设备要求

- 所有 Secure Firewall Management Center 和 Cisco Secure Firewall Threat Defense 设备必须运行 7.7.10 及更高版本。
- 所有 Cisco Secure Firewall Threat Defense 设备必须配置为路由模式；不支持透明模式。
- 在安全云控制中为设备配置通用 Zero Trust 访问时，确保设备身份证书的注册类型是使用 PKCS12 文件格式创建的对象。不支持其他证书类型。如有必要，也可以从安全云控制创建新的证书对象，该对象支持 PKCS12 格式。请参阅配置安全设备。
- 配置域名系统 (DNS) 以解析私有资源的完全限定域名 (FQDN)。使用 Cisco Secure Firewall 上的平台设置 (Platform Settings) 菜单配置 DNS。请参阅接口和设备设置。
- 支持高可用性 (HA) 设备；它们显示为一个实体。
- 支持安全客户端（已启用 ZTNA 模块）5.1.10 及更高版本。

客户端必须在支持可信平台模块 (TPM) 的平台（如 Windows 11）上运行。

证书类型准则

- **用户身份证书**：启用了 Zero Trust 访问的 Secure Client 在与 Secure Access 和 Firewall Threat Defense 进行双向传输层安全 (mTLS) 会话时出示用户身份证书，以请求访问私有资源。
- **防火墙威胁防御设备证书**：已启用通用 ZTNA 的 威胁防御设备使用设备证书与安全客户端和安全访问建立安全的 mTLS 连接。确保设备身份证书为 PKCS12 类型。

  如果已为设备注册手动证书，请先在防火墙管理中心上使用 **Devices** > **Certificates** > **Export Certificate** 菜单将其导出为 PKCS12 格式。使用导出的 PKCS12 文件创建新的 PKCS12 证书注册对象。
- **解密证书**：（可选）要解密发送到私有资源的流量，请在安全访问中为资源启用**解密**，并提供服务器证书和密钥。我们建议您使用由公开认可的证书颁发机构 (CA) 签名的证书。

支持的设备

本地防火墙管理中心和云交付型防火墙管理中心均可配置为管理设备。

仅支持具有 16 个或更多内核的设备。此类 Cisco Secure Firewall Threat Defense 型号包括：

- 1150
- 3105、3110、3120、3130、3140
- 4115、4125、4145、4112
- 4215、4225、4245
- FTDv

注释 您可以在 16 核 FTDv 上配置 通用 ZTNA。FTDv 的其他部署配置均不支持通用 ZTNA。

通用零信任网络访问 的限制

- 通用 ZTNA 不支持 IPv6。
- 启用 通用 ZTNA 的设备不会对通过站点间隧道的流量实施策略。
- 通用 ZTNA 不支持集群设备。
- 通用 ZTNA 不支持多实例模式下的设备。
- 通用 ZTNA 会话不支持巨型帧。
- 通用 ZTNA 仅支持全局 VRF。

- 通用 ZTNA 不支持 FTP 或 TFP 等由服务器发起数据连接或次要连接的协议。

  例如，主动模式 FTP 连接使用持久控制连接传输命令，并创建临时数据连接传输文件。通用 ZTNA 不支持此类由服务器发起的数据连接。

将防火墙管理中心与安全云控制集成

注释 此任务仅适用于本地防火墙管理中心。

将本地部署的 Secure Firewall Management Center 与 Security Cloud Control 集成使您能够配置您的 Secure Firewall Management Center 及其关联的 Cisco Secure Firewall Threat Defense 设备。这些设备随后可使用配置和管理 通用 ZTNA 所需的网络、专用资源和策略。

注释 通用 ZTNA 仅使用 安全接入 定义的访问策略。从 Secure Firewall Management Center 部署到威胁防御设备的任何其他访问控制策略和规则，在 通用 ZTNA 中都会被忽略。

开始之前

您的思科联系人必须将您的 Security Cloud Control 和 安全接入 系统纳入管理，并创建用户和租户。

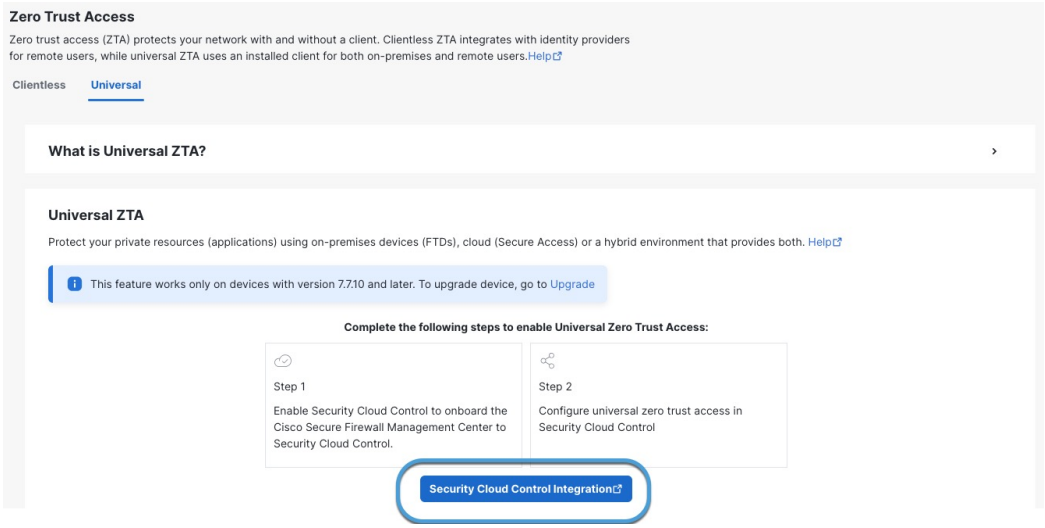
过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **Zero Trust 应用**。

步骤 3 点击**通用**选项卡。

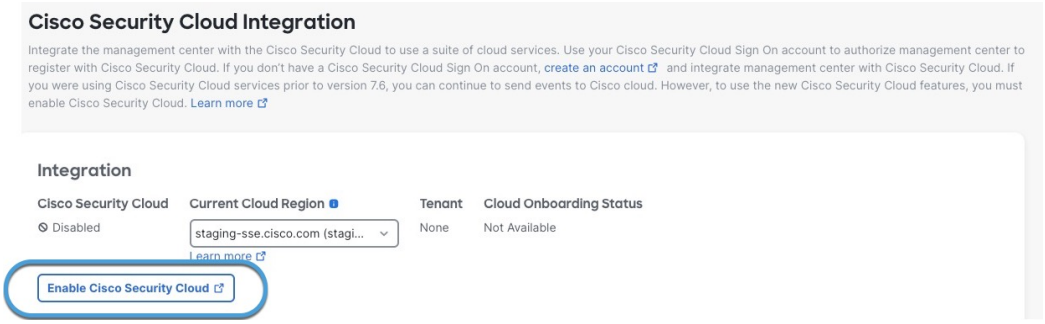
系统将显示“Zero Trust 访问”页面。



步骤 4 点击**安全云控制集成**。

步骤 5 在**当前云区域**列表中，点击您的 Security Cloud Control 区域的名称。

步骤 6 点击 **启用思科安全云**。

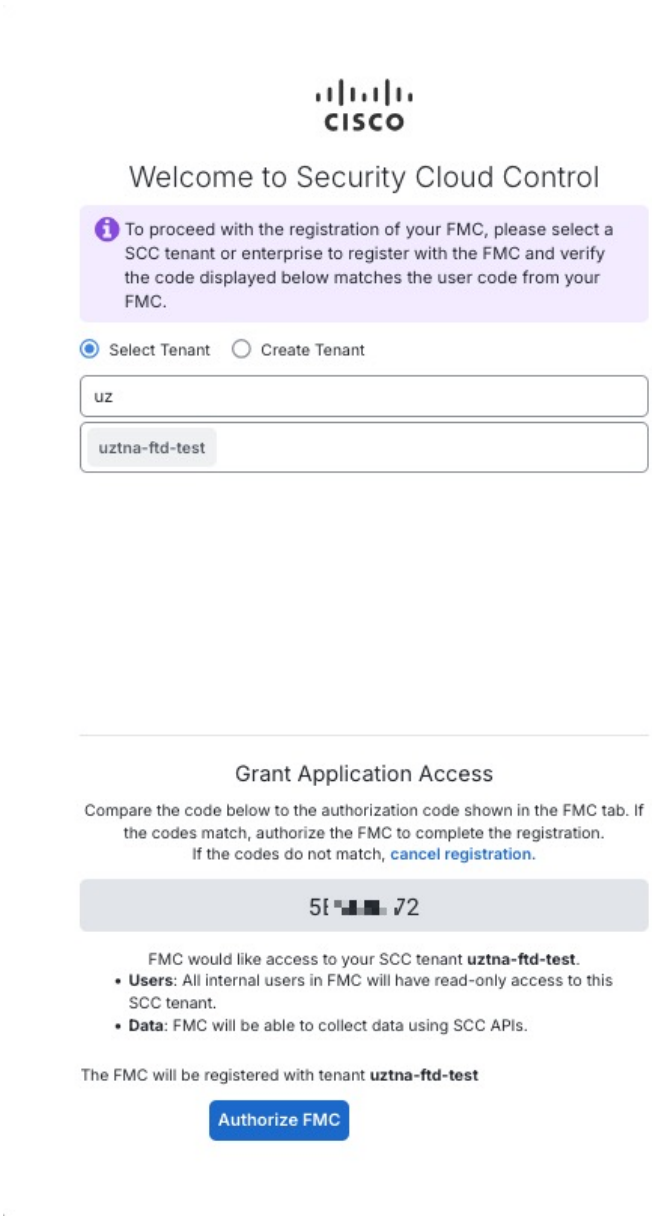


步骤 7 出现提示时，点击**继续使用思科 SSO**。

步骤 8 登录 Security Cloud Control。

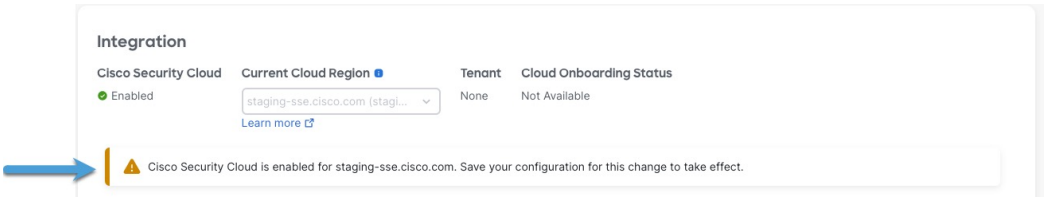
步骤 9 在**选择租户**列表中，点击租户名称。

步骤 10 在随后显示的页面上，点击**授权 FMC**。



步骤 11 出现提示时，关闭选项卡页面。

步骤 12 系统将显示一条确认消息，表明载入操作已成功。



步骤 13 点击页面底部的**保存**。

保存配置可能需要几分钟时间。配置保存后，页面会显示载入状态和租户名称。

步骤 14 有关此页面上其他选项的详细信息，请参阅安全云控制设置，第 23 页。

安全云控制设置

以下主题讨论“Cisco Security Cloud 集成”页面上的设置，可通过在 Secure Firewall Management Center 上选择 **集成** > **安全云控制** 来访问该页面。

事件配置

在Security Cloud Control中监控选定的事件：

- **向云发送事件**：选中此复选框以在 Security Cloud Control 中监控事件；清除此复选框以不监控任何事件。

  您可以在 Security Cloud Control 中通过**防火墙** > **事件和日志**查看事件。

- **入侵事件**：如果您使用 IPS 策略，请选中此复选框以监控这些策略。
- **文件和恶意软件事件**：如果您使用文件或恶意软件策略，请选中此复选框以监控这些策略。
- **连接事件**：选中要监控的事件旁的复选框，**安全**（用于文件和 IPS 事件）或**全部**。

有关事件的详细信息，请参阅安全云控制中的事件类型。

思科安全云支持（可选）

（可选）选中复选框以启用以下功能：

- **启用 Cisco Success Network**：选中此复选框以启用《*Cisco Success Network 从 Cisco Secure Firewall Management Center*收集的遥测数据，版本 *7.7*》中讨论的统计信息收集。
- **启用思科支持诊断**：选中此复选框以启用*Cisco Secure Firewall Management Center* 管理指南中讨论的统计信息收集。

思科安全 AI 助手

选中复选框以启用《有效使用 Cisco AI Assistant for Security 管理您的威胁防御设备》中讨论的 AI 助手。

思科 XDR 自动化

选中复选框以启用思科 XDR 帮助中心中讨论的 XDR 工作流程自动化。

策略分析器和优化器

选中复选框以启用策略分析器；点击**了解更多**获取详情。

零接触调配 (ZTP)

选中复选框以启用*Cisco Secure Firewall Management Center* 管理指南中讨论的零接触配置。

配置安全设备

与您载入 Security Cloud Control 的 Secure Firewall Management Center 相关联的所有防火墙威胁防御设备都是安全设备，您可以：

- 将私有资源（即您希望通过基于身份的访问控制、IPS、恶意软件和其他保护措施进行保护的内部应用）与这些设备相关联。
- 部署 安全接入 访问规则。安全设备负责为 本地部署 用户、远程用户或两者实施访问规则。

执行以下步骤，在 威胁防御设备上启用**通用 Zero Trust 网络访问设置**。这些步骤包括配置设备 FQDN、内部接口、外部接口和 PKCS12 证书，以在设备上启用通用 ZTNA。

开始之前

完成将防火墙管理中心与安全云控制集成，第 20 页中讨论的所有任务。

您必须知道每个设备的内部和外部网络接口名称：

- 内部接口（也称为 *DMZ* 接口）用于对本地用户应用访问规则。
- 外部接口用于对远程用户应用访问规则。

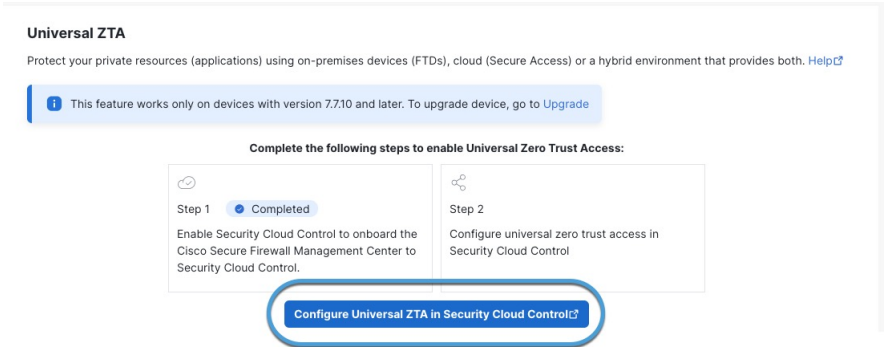
您可以为每个安全设备选择内部接口、外部接口或两种类型的接口。

过程

步骤 1 在 Secure Firewall Management Center 中，点击 **策略** > **安全策略** > **Zero Trust 应用**。

步骤 2 点击**在安全云控制中配置通用 ZTA**。

下图显示了一个示例。

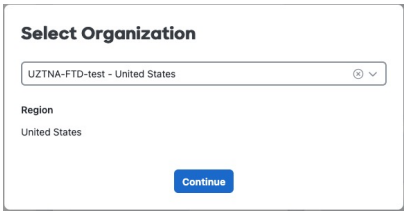


步骤 3 出现提示时，登录到 Security Cloud Control。

步骤 4 出现提示时，从下拉列表中选择您的组织，然后点击**继续**。

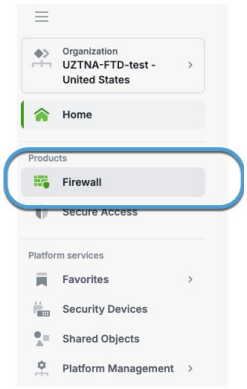
选择已配置安全访问和 Cisco Secure Firewall 微应用的组织。

下图显示了一个示例。



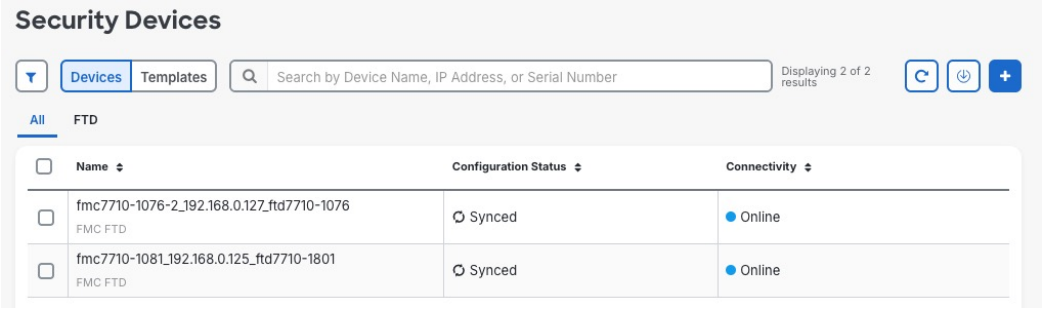
步骤 5 在 Security Cloud Control 中，在“产品”部分，点击**防火墙**。

下图显示了一个示例。



步骤 6 在“管理”部分，点击**安全设备**。

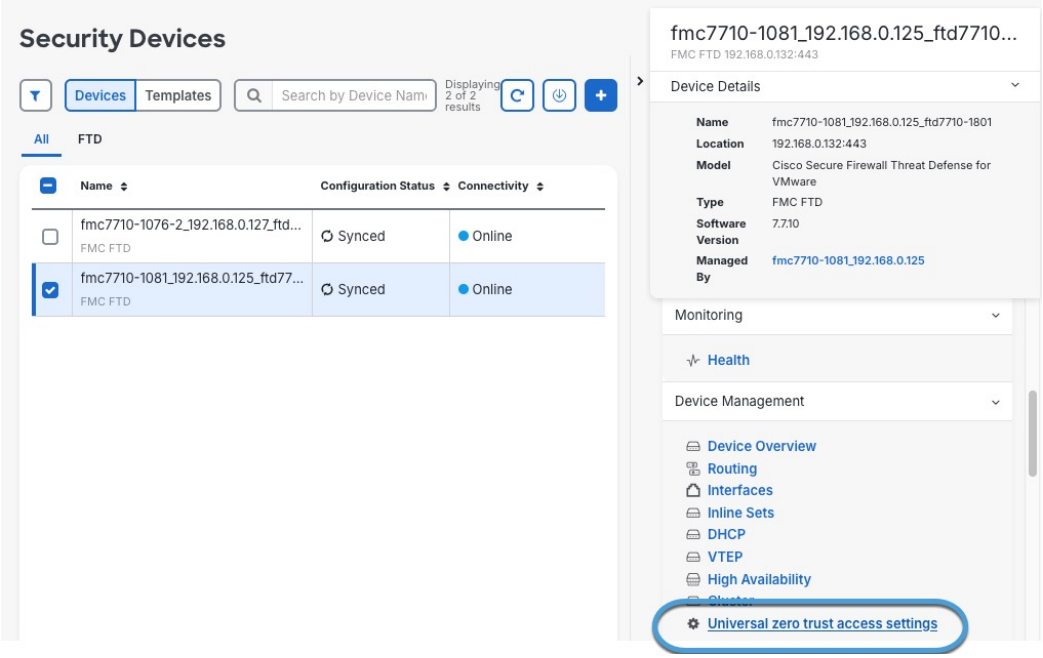
安全设备页面显示可用的安全设备。



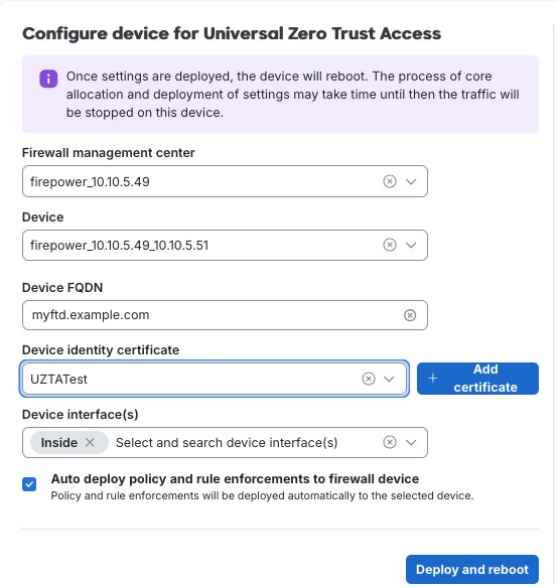
步骤 7 选中要添加到 通用零信任网络访问 配置中的设备旁边的复选框。

步骤 8 在右侧窗格中，点击**设备管理** > **通用 Zero Trust 访问设置**。

下图显示了一个示例。



步骤 9 在**为通用 Zero Trust 访问配置设备**页面上输入或编辑以下信息。



下表描述了要在设备上启用 通用 ZTNA 的配置。

项目	说明
防火墙管理中心	从下拉列表中，点击要用于策略部署、监控和其他任务的 Secure Firewall Management Center 的名称。
设备	从下拉列表中，点击要用于规则部署和实施的设备的名称。
设备 FQDN	输入安全设备的完全限定域名 (FQDN)。FQDN 也称为 TLS/SSL 证书的公用名。 Secure Access 将客户端重定向到此 FQDN 所代表的资源。 确保设备 FQDN 与设备身份证书的通用名称 (CN) 完全匹配，并且还必须匹配证书中的主题备用名称 (SAN)。

项目	说明
设备身份证书	**设备身份证书**的通用名称必须： • 与您在**设备 FQDN** 字段中输入的值完全匹配。 • 与证书中的使用者备用名称 (SAN) 匹配。 从下拉列表中，点击列表中现有身份证书的名称。 点击**添加证书**，以 **.p12** 格式（也称为 PKCS#12；请参阅 ssl.com 上的此文章）添加身份证书。 **注释** 通用 ZTNA 仅支持 PKCS#12 格式的证书注册。 在提供的字段中，输入用于标识证书的**名称**。然后复制粘贴、拖放或上传证书和私钥。如果证书已加密，请在提供的字段中输入其密码。 您也可以按照 ssl.com 上的什么是通配符证书？中的说明使用通配符证书。
设备接口	从下拉列表中，选中以下任一类型接口旁边的复选框。 • 内部网络接口（或 DMZ）：仅对本地用户部署访问规则。 • 外部网络接口：仅对远程用户部署访问规则。 • 两种类型的接口：对本地用户或远程用户部署访问规则。
自动将策略和规则实施部署到防火墙设备	选中此复选框，以便在 安全接入 上更新访问规则后，自动将其部署到设备。 在设备上，“自动部署”功能仅选择性地部署 通用 ZTNA 访问策略。它不会影响防火墙管理中心上的其他更改或配置。 **注释** 如果设备上存在与 通用 ZTNA 访问策略相互关联的其他依赖策略，防火墙配置状态会显示错误消息。然后部署会停止。在这种情况下，您应从防火墙管理中心手动部署 通用 ZTNA 访问策略。

步骤 10 点击**部署并重启**。

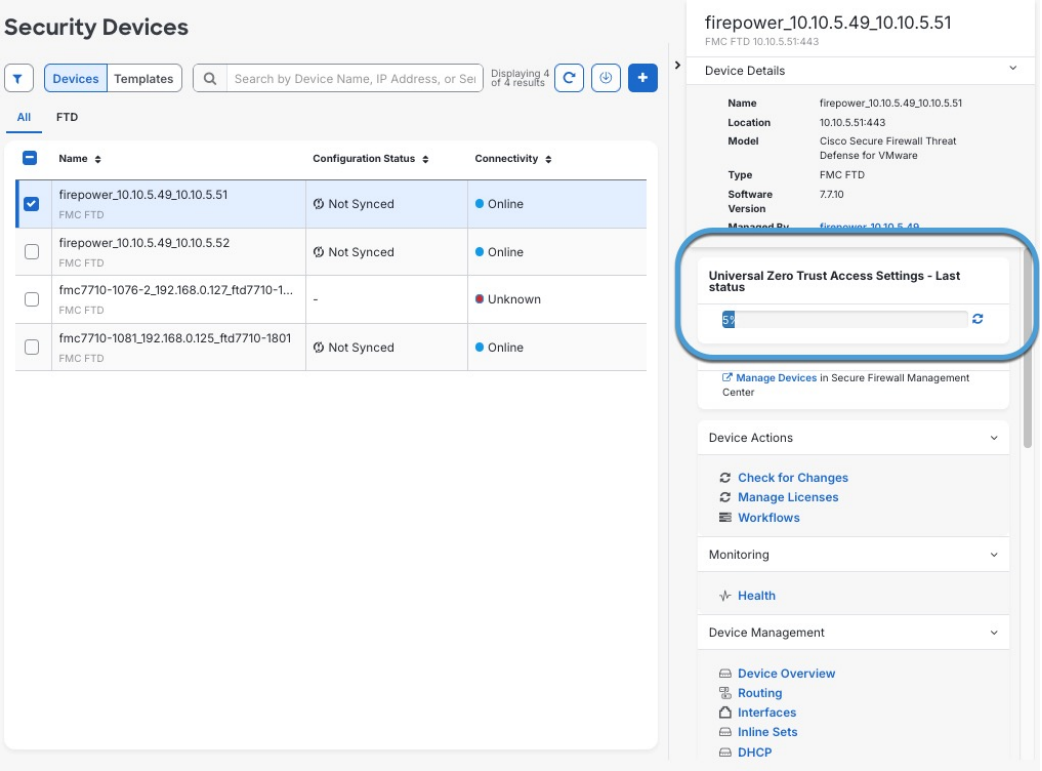
设备会重启以重新为 通用 ZTNA 组件分配系统资源。

注释
设备重启需要几分钟时间，在此期间，设备处理的所有流量都会中断。

如果您部署高可用性 (HA) 对设备，两台设备会同时重启。

步骤 11 在**安全设备**页面上，选中您刚刚部署 通用 ZTNA 配置的设备旁边的复选框。

右侧窗格显示部署状态，如下图所示。



有关详细信息，请在右侧窗格中点击**设备操作** > **工作流程**。

部署完成后，您可以在设备的**通用 Zero Trust 访问设置 - 最后状态**选项卡中查看完成状态。

已启用通用 ZTNA 的防火墙威胁防御设备已连接到安全访问。

下一步做什么

通过点击**安全云控制** > **安全访问** > **连接** > **网络连接** > **FTD**，检查安全访问下威胁防御设备的可用性。

Zero Trust 网络访问历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
通用 Zero Trust 网络访问（通用 ZTNA）。	7.7.10	7.7.10	通用 Zero Trust 网络访问（通用 ZTNA）是一种全面的解决方案，基于用户身份、信任和状态提供对内部网络资源的安全访问。它确保对一个应用的访问不会像远程访问 VPN 那样隐式授予对整个网络的访问权限。 新增/修改的屏幕： **策略** > **安全策略** > **Zero Trust 应用** 需要 Cisco 安全接入 和 Security Cloud Control。 部署限制：不支持集群设备、容器实例或透明模式。 支持的平台：Cisco Secure Firewall 1150、3100、4100、4200 和 Firewall Threat Defense Virtual。
Zero Trust 访问增强功能。	7.4.1	带有 Snort 3 的 7.4.1	防火墙管理中心 管理中心现在包括以下 Zero Trust 访问增强功能： • 现在，您可以为应用配置 NAT 的源网络。配置的网络对象或对象组用于将传入请求的公共网络源 IP 地址转换为应用网络内的可路由 IP 地址。 • 您可以使用诊断工具对 Zero Trust 配置问题进行故障排除。 新增/修改的屏幕： **策略** > **访问控制** > **Zero Trust 应用** 新增/修改的 CLI 命令：**show running-config zero-trust**、**show zero-trust statistics**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
无客户端 Zero Trust 访问。	7.4.0	带有 Snort 3 的 7.4.0	Zero Trust 访问允许使用外部 SAML 身份提供程序 (IdP) 策略对来自网络内部（本地）或外部（远程）的受保护基于 Web 的资源、应用或数据的访问进行身份验证和授权。 配置包括 Zero Trust 应用策略 (ZTAP)、应用组和应用。 新增/修改的菜单项： • **策略 (Policies)** > **Zero Trust 应用 (Zero Trust Application)** • **分析** > **连接** > **事件** • **概述 (Overview)** > **控制面板 (Dashboard)** > **Zero Trust** 新增/修改的 CLI 命令： • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics**

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。