Zero Trust 访问

以下主题概述了 Zero Trust 应用策略以及如何配置和部署这些策略。

关于零信任访问

零信任访问功能是基于零信任网络访问 (ZTNA) 原则。ZTNA 是一种消除隐式信任的零信任安全模型。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。

零信任访问允许您使用外部 SAML 身份提供商 (IdP) 策略从网络内部（本地）或外部（远程）对受保护的基于网络的资源和应用程序进行身份验证和授权访问。

功能如下：

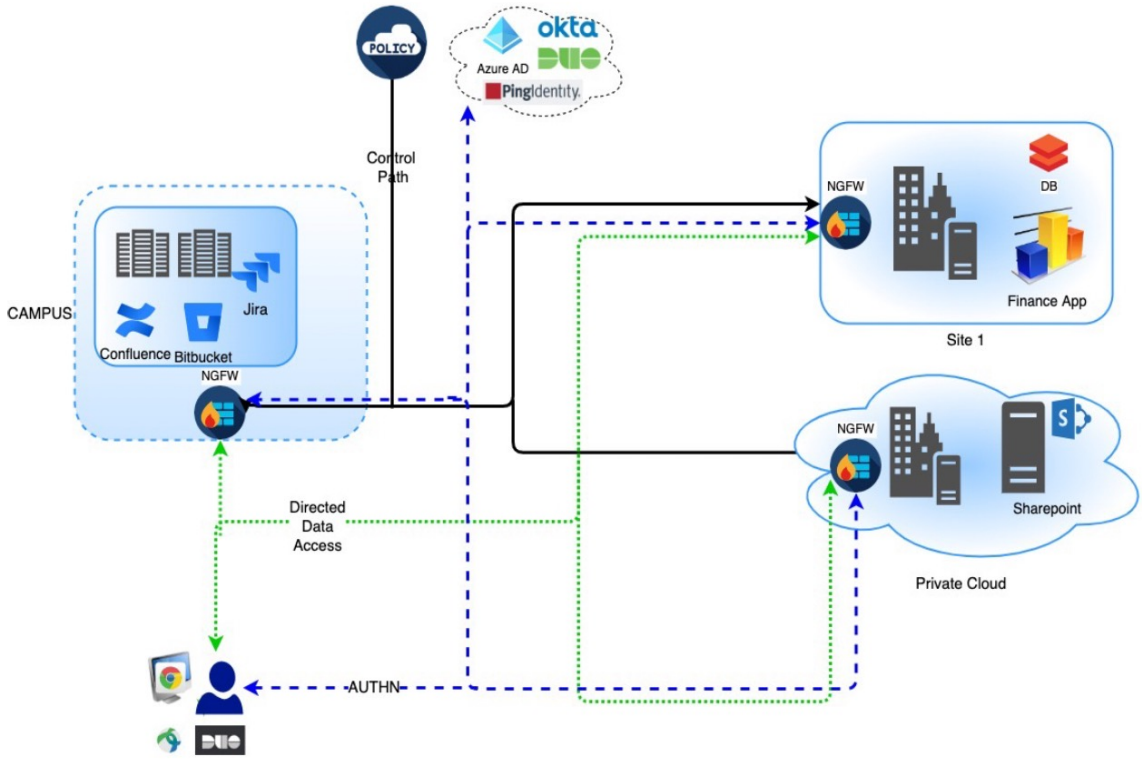
- 支持多个基于 SAML 的身份提供程序，例如 Duo、Azure AD、Okta 和其他身份提供程序。
- 终端（客户端设备）上不需要思科 Cisco Secure 客户端 等客户端应用来进行安全访问。

- 通过浏览器进行访问和身份验证。
- 仅支持 Web 应用 (HTTPS)。
- 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，以便更轻松地在一组应用上启用零信任保护。
- 对零信任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 界面创建零信任应用策略，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 访问？

Zero Trust访问利用现有的威胁防御部署作为应用访问的实施点。它允许远程和本地用户通过按应用授权和按应用隧道对专用应用进行分段访问。

该功能对用户隐藏网络，并仅允许用户访问其授权的应用。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，对应用的每次访问都必须经过明确授权。

将 Zero Trust 访问功能添加到威胁防御，可以迁移到更安全的访问模型，而无需在网络中安装或管理其他设备。

该功能易于管理，因为它不需要客户端，并且按应用访问。

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程序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**- 威胁防御 使用此证书伪装成应用。威胁防御 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 威胁防御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 威胁防御 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。

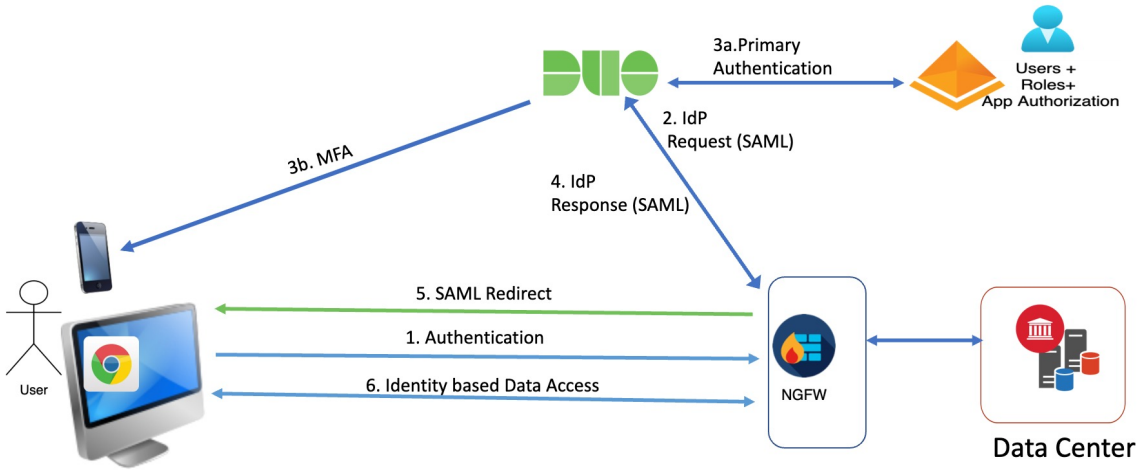
- **应用证书**- 威胁防御 使用此证书解密从用户到应用的加密流量，以进行检查。

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。

Zero Trust 访问工作流程

此图描绘了 Zero Trust 访问工作流程。

图 *2: Zero Trust* 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。

Zero Trust 访问的限制

- 仅支持 Web 应用 (HTTPS)。不支持需要解密豁免的场景。
- 仅支持 SAML IdP。
- 不支持 IPv6。不支持 NAT66、NAT64 和 NAT46 场景。
- 仅当启用 Snort 3 时，此功能才可用于威胁防御。
- 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。

- 独立模式集群中不支持。
- 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，则零信任应用配置的外部 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** > **访问控制** > **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 创建零信任应用策略， 第 7 页
- 编辑 - 点击 **编辑**（）。请参阅 编辑 Zero Trust 应用策略， 第 12 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。

创建零信任应用策略

此任务配置零信任应用策略。

开始之前

确保满足Zero Trust 应用策略的前提条件 ， 第 6 页中列出的所有前提条件。

过程

步骤 1 选择 **策略** > **访问控制** > **零信任应用**。

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 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。

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。

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，必须拥有受管设备的 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 **Save** 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 8 页。
2. 创建应用。请参阅创建应用，第 9 页。
3. 将零信任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 11 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

创建零信任应用策略，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 **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 **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 **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“零信任应用”页面上。

下一步做什么

1. 创建应用，第 9 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. 创建零信任应用策略，第 7 页。
2. 创建应用组，第 8 页（仅分组应用需要）。

过程

步骤 1 选择 **策略** > **访问控制** > **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 URL 必须与该 DNS 中的条目保持一致，以确保对应用进行解析。

- **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。
- **IPv4 源转换**- 从下拉列表中选择 NAT 的源网络。点击 **添加**（+） 图标以创建新的网络对象。有关详细信息，请参阅 网络。

  该网络对象或对象组用于将传入请求的公共网络源IP地址转换为企业网络内的可路由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 8 页。

  注释 此字段不适用于未分组的应用。

步骤 5 点击 **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** 或 **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 **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**- 如果没有 IdP 元数据，可以稍后配置。

     点击 **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 **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**。

该应用在“零信任应用”页面上列出，默认情况下处于启用状态。

下一步做什么

1. 为目标设备设置 Zero Trust 访问策略， 第 11 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. 创建零信任应用策略， 第 7 页。
2. 创建应用组， 第 8 页。
3. 创建应用， 第 9 页。

过程

步骤 1 选择 **策略** > **访问控制** > **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 (Save)** 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** > **访问控制** > **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 **返回零信任应用** 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

部署零信任应用策略后，新字段可用。要将字段添加到表视图：

1. 选择 **分析** > **连接** > **事件** 。
2. 转到 **连接事件的表视图** 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
   - 零信任应用
   - 零信任应用组
   - 零信任应用策略
5. 点击 **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 。

零信任控制面板

通过零信任控制面板，您可以监控设备上活动零信任会话的实时数据。

零信任控制面板提供由管理中心管理的排名靠前的零信任应用和零信任用户的摘要。选择 **概述 > 控制面板 > 零信任** 以访问控制面板。

控制面板具有以下构件：

- 热门零信任应用
- 热门零信任用户

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	查看零信任配置的运行配置
show zero-trust	显示运行时零信任统计信息和会话信息
show cluster zero-trust	显示集群中各节点的零信任统计信息摘要
clear zero-trust	清除零信任会话和统计信息
show counters protocol zero_trust	查看零信任流命中的计数器

诊断工具

诊断工具通过检测零信任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。
  - 零信任策略或 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零信任应用旁边的诊断 ( )。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。

Zero Trust 访问的历史记录

功能	最低 管理中心	最低 威胁防御	详情
Zero Trust 访问的增强功能	7.4.1	7.4.1	• 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。 • 现在还提供了一个诊断工具，以方便故障排除过程。该工具可检测 Zero Trust 配置可能存在的问题。
Zero Trust 访问	7.4.0	7.4.0	您可以允许用户访问私人应用，而无需在其个人设备上安装额外的软件。该功能利用基于 SAML 的身份验证，支持 Duo 以及所有其他主要身份提供程序。

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。