使用受信任网络检测配置零信任网络访问

目录

简介

- 要求
- 使用的组件

背景信息

配置

- 步骤 1：创建受信任网络配置文件 — DNS服务器和域
- 步骤 2：EnableTND for Private orInternet Access
- 步骤 3：客户端配置

验证

- 从安全客户端
- 从DART套件 — ZTA日志

相关信息

简介

本文档介绍配置零信任网络访问受信任网络检测所需的步骤。

先决条件

- 安全客户端最低版本5.1.10
- 支持的平台 — Windows和MacOS
- 适用于Windows的受信任平台模块TPM
- 适用于Apple设备的安全群落协处理器
- 任何受信任网络配置文件中配置的受信任服务器都隐式排除在ZTA侦听之外。这些服务器也不能作为ZTA私有资源访问。
- TND配置会影响组织中的所有已注册客户端
- 管理员可以使用后续步骤为受信任服务器生成“证书公钥哈希”
  - 下载受信任服务器公共证书
  - 运行此shell命令以 generate the hash.

```
openssl x509 -in

      -pubkey -noout | openssl pkey -pubin -outform DER | openssl dgst -sha256
```

要求

Cisco 建议您了解以下主题：

- 思科安全访问
- 使用安全断言标记语言(SAML)或基于证书的身份验证以零信任访问注册设备。

使用的组件

- 安全客户端版本5.1.13
- 可信平台模块(TPM)
- 安全访问租户
- Windows设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

- TND使管理员能够配置安全客户端，以临时暂停受信任网络上的ZTA流量引导和实施。
- 安全客户端在终端离开受信任网络时恢复ZTA实施。
- 此功能不需要任何最终用户交互。
- ZTA TND配置可独立管理私有和互联网ZTA目标。



主要好处

- 提高网络性能和减少延迟，提供更流畅的用户体验。

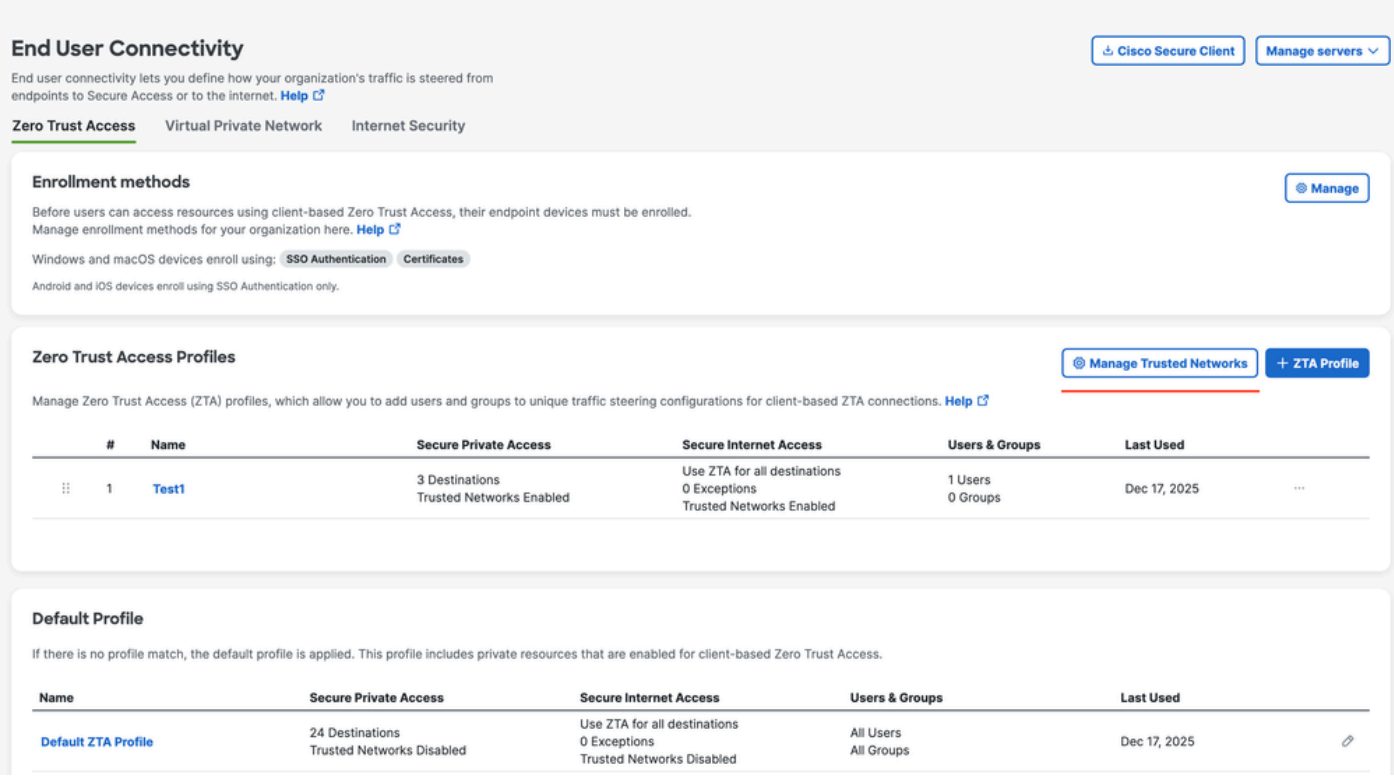
- 可信网络中的本地安全实施提供灵活且优化的资源利用率。
- 最终用户无需任何提示或操作即可利用优势。
- 对用于专用访问和互联网访问的TND进行独立控制，为管理员提供处理不同运营和安全问题的灵活性

配置

步骤 1：创建受信任网络配置文件 — DNS服务器和域

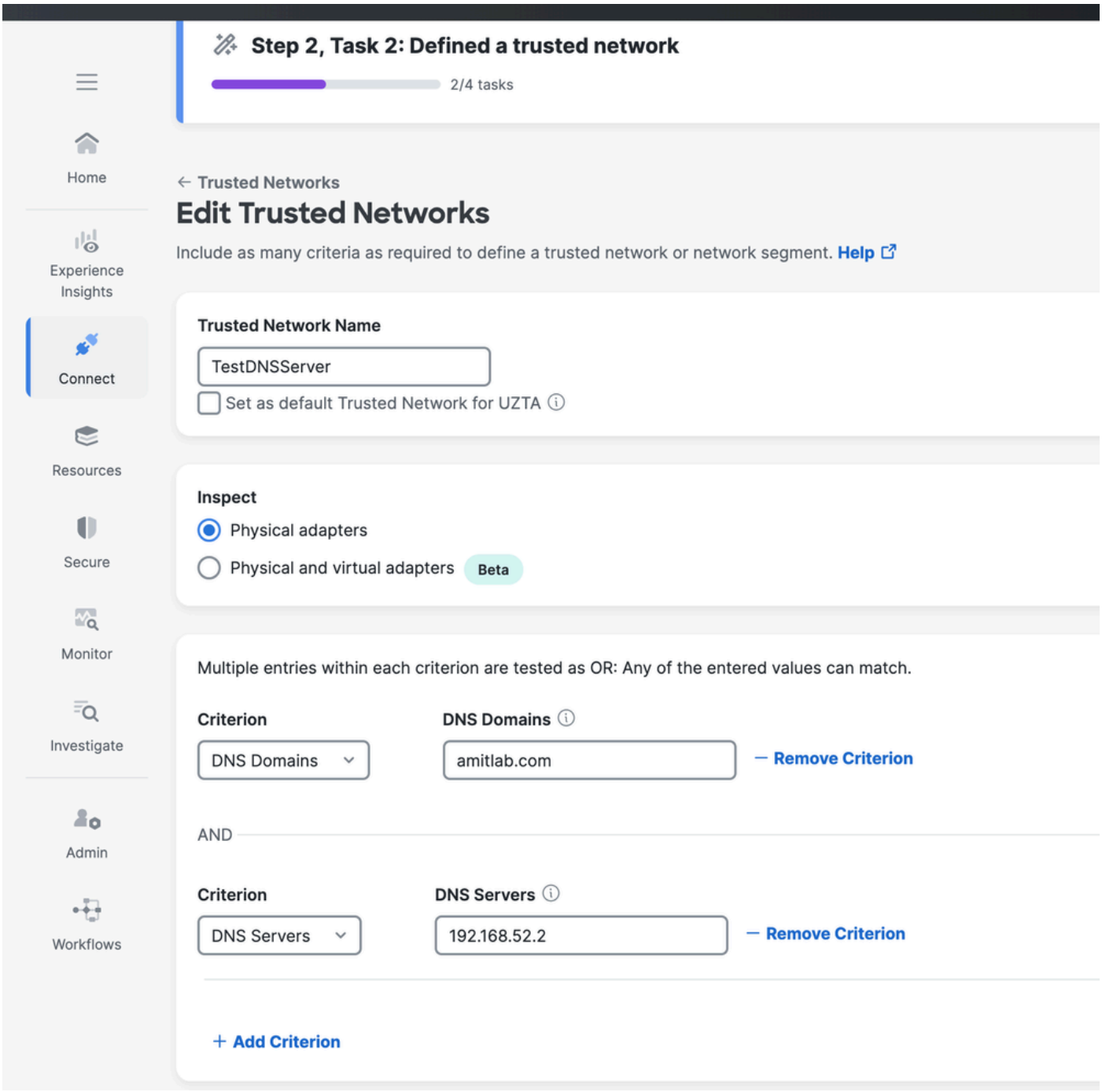
导航到安全访问控制面板:

- 单击Connect> End User Connectivity> Manage Trusted Networks> +**Add**



重复上述步骤以添加其他受信任网络配置文件。

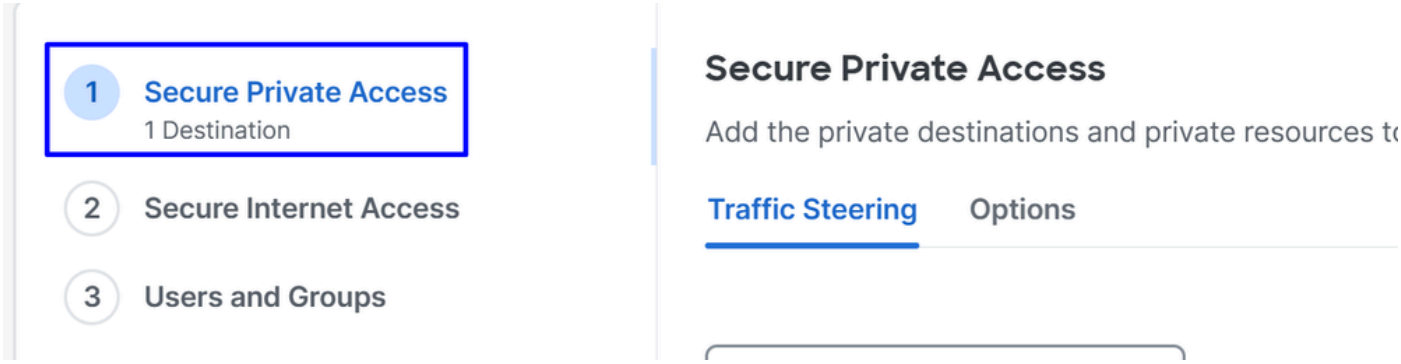
注意：同一条件内的多个选项为OR运算符。定义的不同条件为AND运算符。



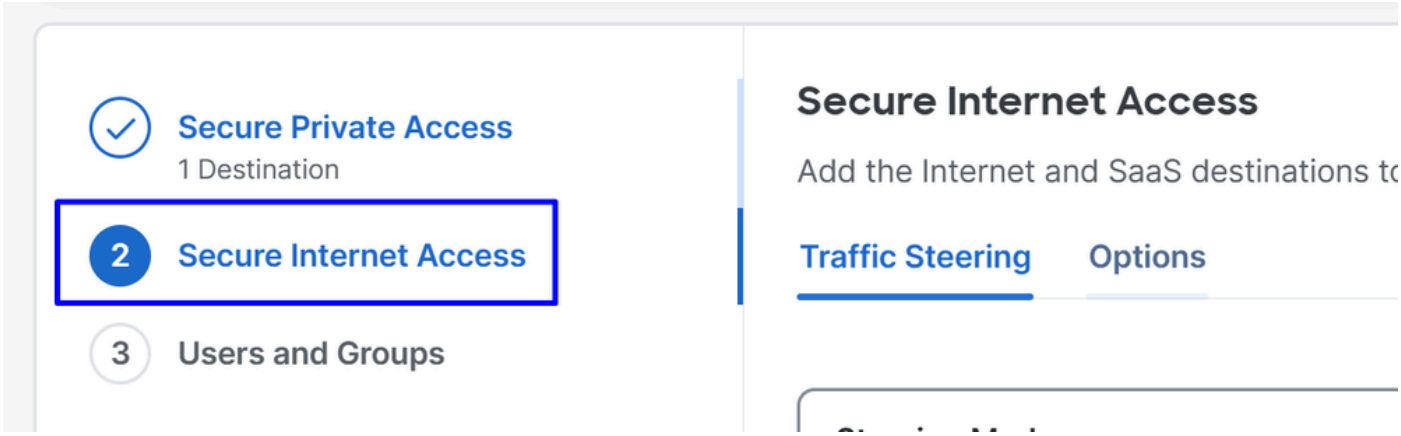
步骤 2：为专用或互联网访问启用TND

- 导航到Connect> End User Connectivity.
- 编辑ZTA配置文件。
- 对于Secure Private Destinations或 Secure Internet Access.

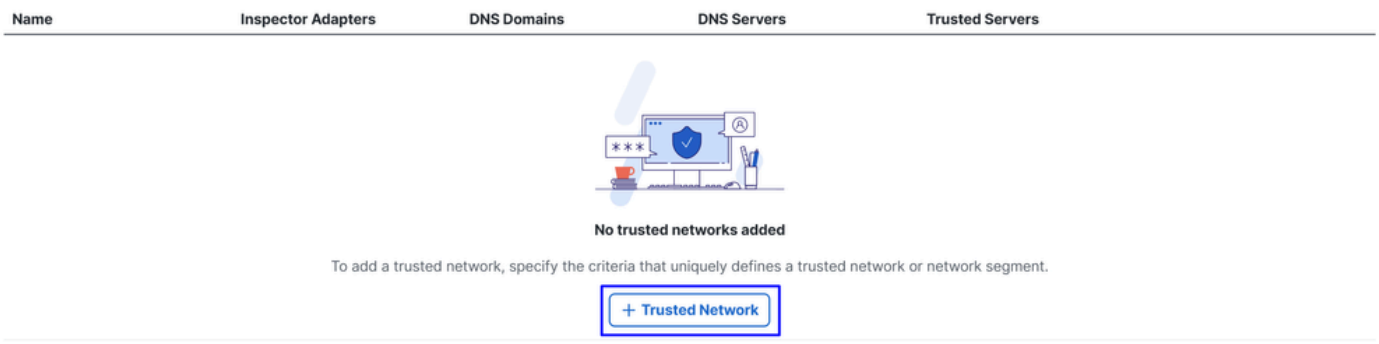
安全私有访问



安全的互联网访问

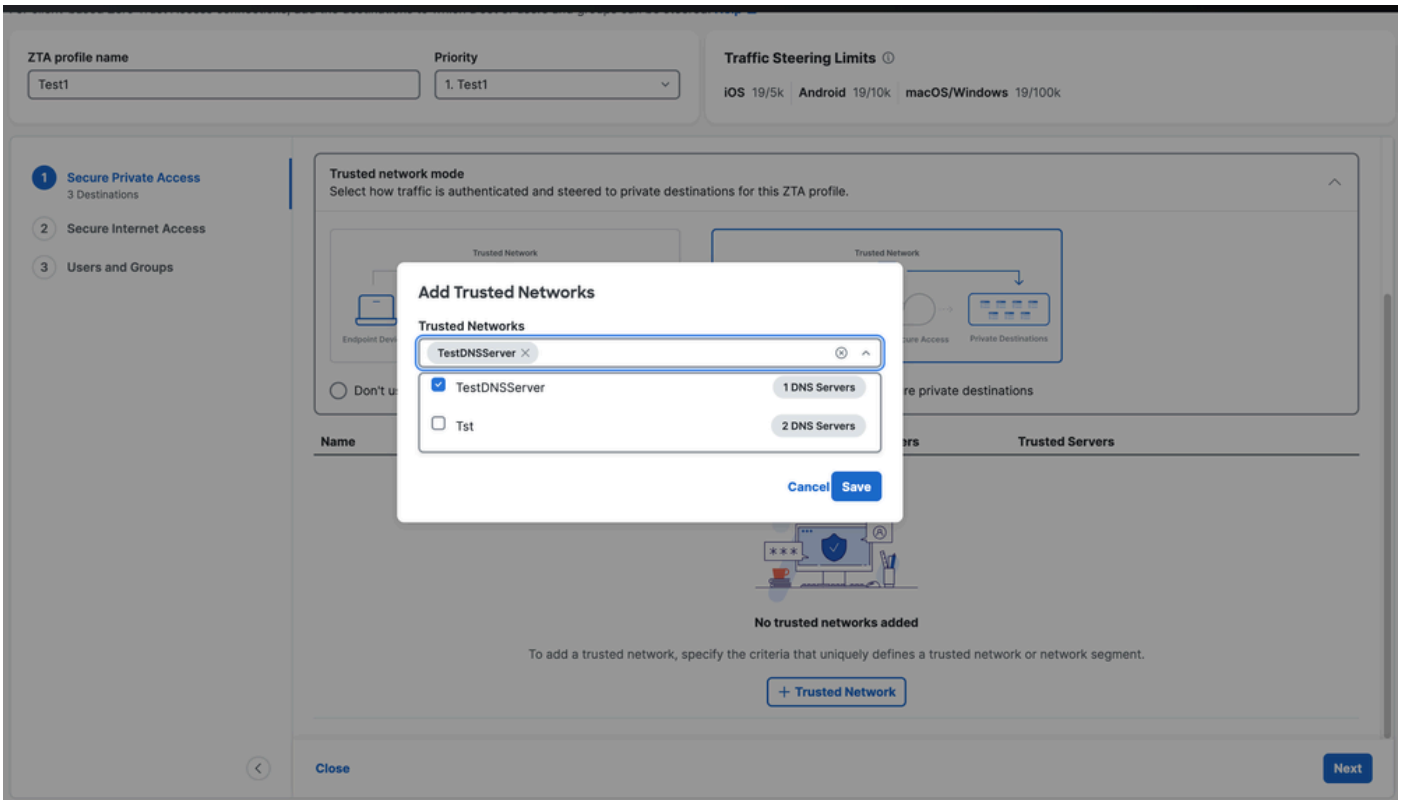


- 点击 Options.
  - 单击Use trusted networks to secure private destinationsUse trusted networks to secure internet destinations 或取决于之前选择的选项。
  - 点击 + Trusted Network.

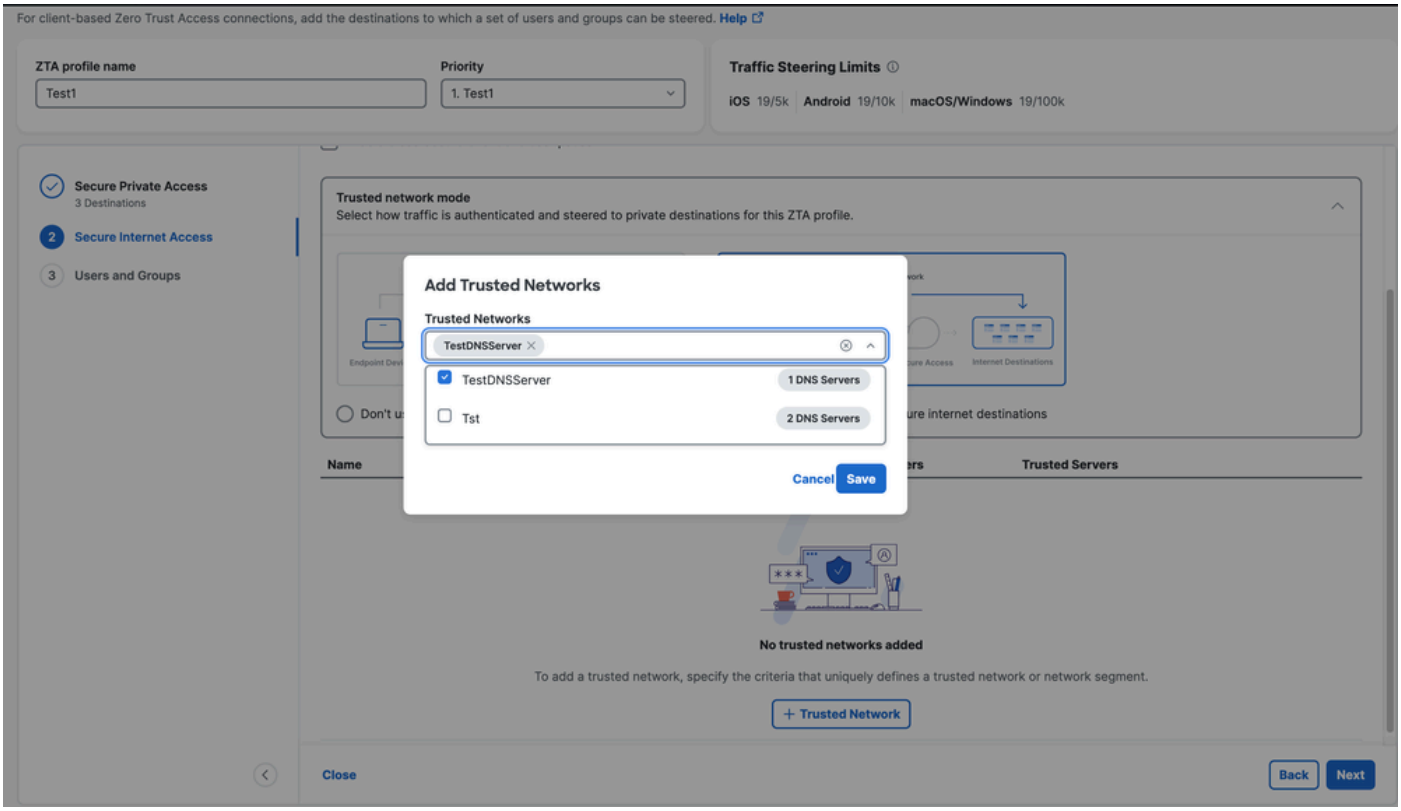


- 选择您在上一页中配置的受信任网络配置文件，然后点击 Save.

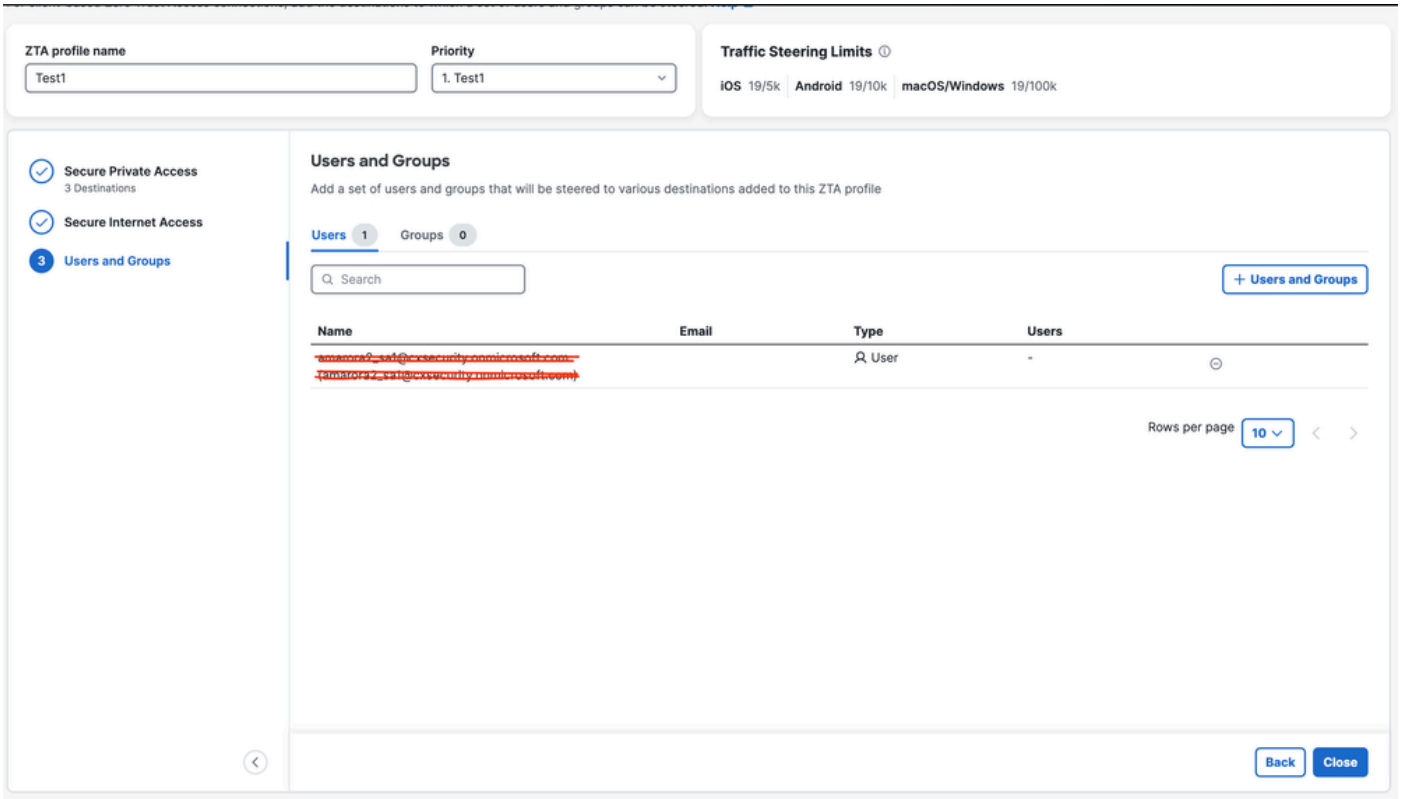
安全私有访问



安全的互联网访问



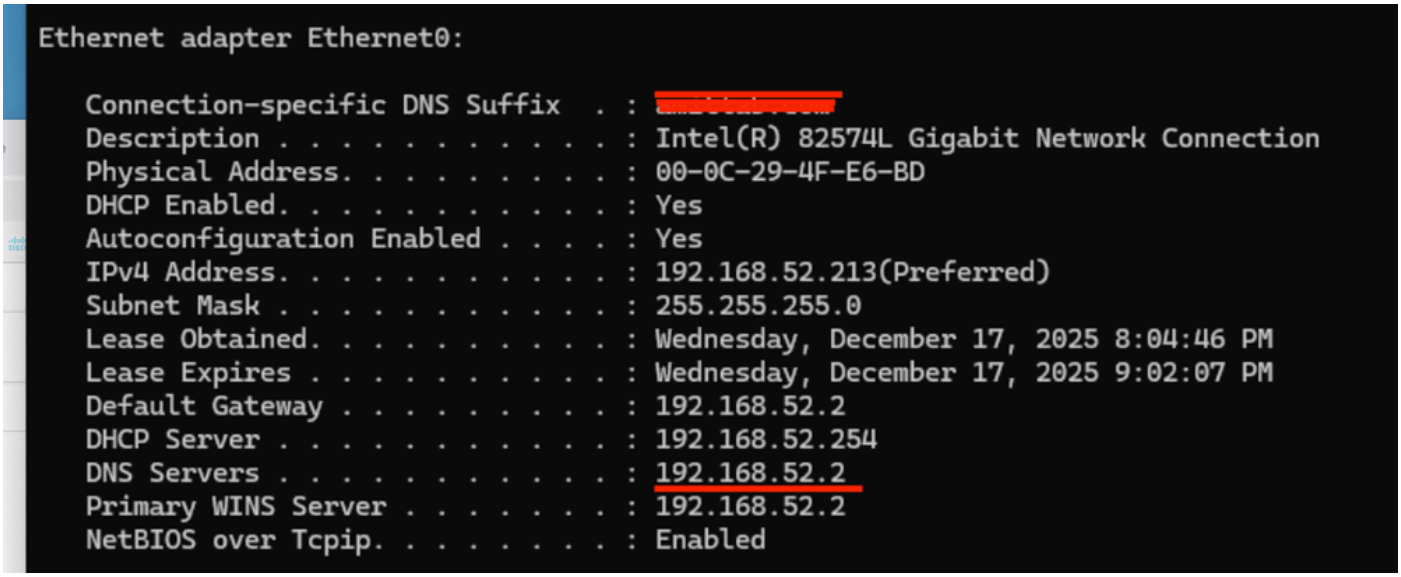
- 将分配给Users/GroupsZTA配置文件，然后点击Close。



步骤 3：客户端配置

1.确保在以太网适配器下定义了正确的DNS服务器，因为您已选择物理适配器作为标准。

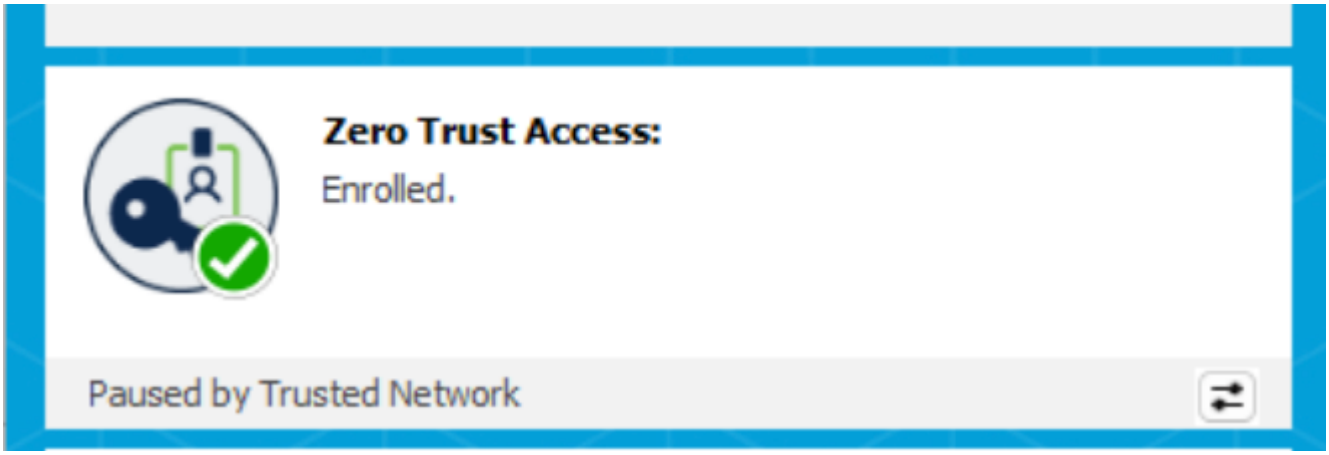
2.确保定义了连接特定的DNS后缀。

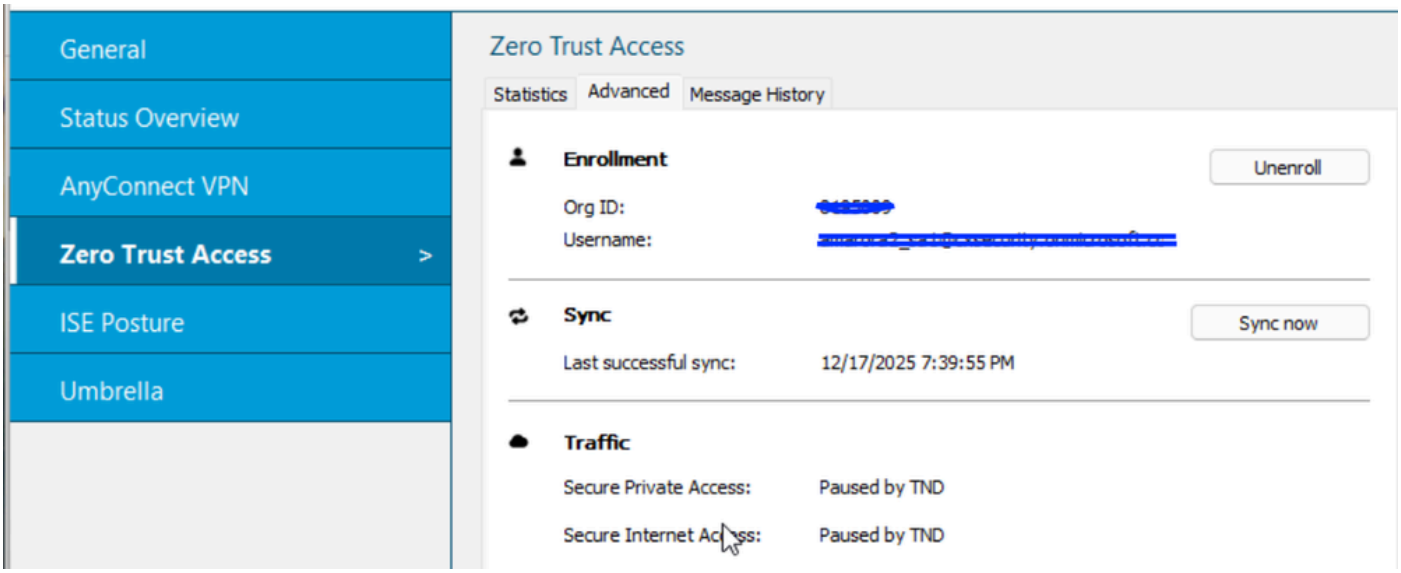


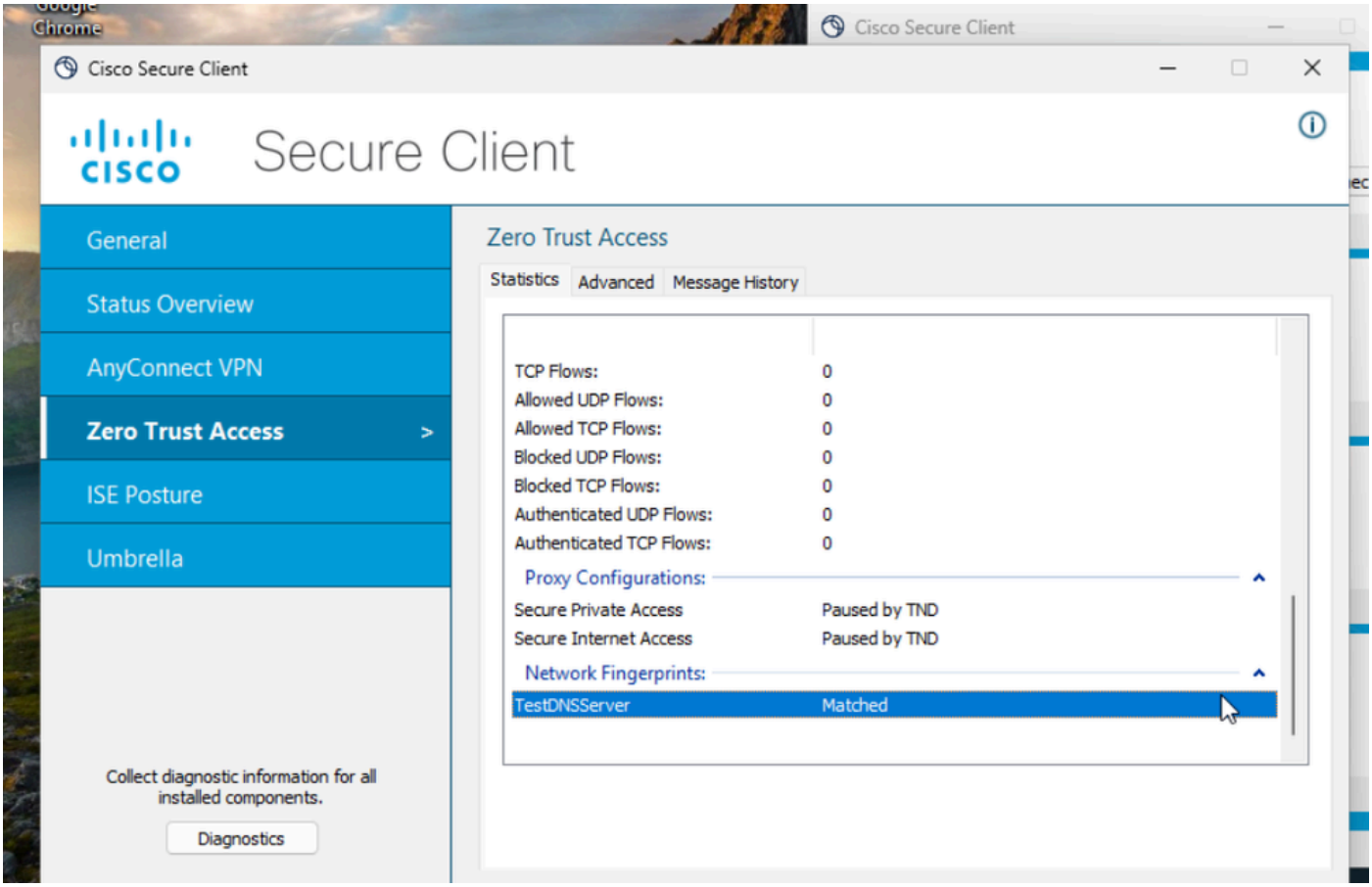
在几分钟内将下一个ZTA配置同步到安全客户端后，ZTA模块检测到它位于其中一个已配置受信任网络时自动暂停。

验证

- 从安全客户端







- 从DART套件 — ZTA日志

未配置TND规则。

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons()TND将连接ProxyConfig 'default_spa_config'（无规则）

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons()TND将连接ProxyConfig 'default_tia_config'（无规则）

已配置的TND规则 — DNS服务器 — 客户端已接收配置

25-12-17 20:33:15.987956 csc_zta_agent[0x00000f80, 0x00000ed4]带CaptivePortalDetectionService.cpp:308 CaptivePortalDetectionService::getProbeUrl()无最后一个网络快照，使用第一个探测url

2025-12-17 20:33:15.992042 csc_zta_agent[0x00000f80, 0x00000ed4] I/ NetworkChangeService.cpp:144 NetworkChangeService::**Start()初始网络快照：以太网接口0:subnets=192.168.52.213/24 dns_servers=192.168.52.2 dns_domain=amitlab.com dns_suffixes=amitlab.com isPhysical=true default_gateways=192.168.52.2**
captivePortalState=未知

conditional_actions":[{"action":"disconnect"告诉TND已在ZTA配置文件中配置。

2025-12-17 17:55:36.430233 csc_zta_agent[0x00000c90/config_service， 0x0000343c] I/ ConfigSync.cpp:309 ConfigSync::HandleRequestComplete()已收到新配置：

{"ztnaConfig":{"global_settings":{"exclude_local_lan":true},"**network_fingerprint":[{"id":"28f629ee-7618-44cd-852d-6ae1674e3cac","label":"TestDNSServer","match_dns_domains":["amitlab.com"],"match_dns_servers":**

["192.168.52.2"],"retry_interval":300}],"proxy_configs":[{"**conditional_actions":[{"action":"disconnect"**,"check_type":"on_network","match_network_fingerprint":["28f629ee-7618-44cd-852d-6ae1674e3cac"]},{"action":"connect"},"id" ","label":"安全专用访问","match_resource_configs":["spa_steering_config"],"proxy_server":"spa_proxy_server"},{"conditional_actions":[{"action":"disconnect","check_type":"on_networ
7618-44cd-852d-6ae1674e3cac"]},{"action":"connect"

2025-12-17 17:55:36.472435 csc_zta_agent[0x000039a8/main，0x0000343c] I/ NetworkFingerprintService.cpp:196 NetworkFingerprintService::handleStatusUpdate()广播网络指纹状态：**指纹:28f629ee-7618-44cd-852d-6ae1674e3cac接口：以太网接口0**

DNS条件上的TND断开连接

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:378 ActiveSteeringPolicy::UpdateActiveProxyConfigs()更新活动代理配置

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:287 ActiveSteeringPolicy::collectProxyConfigPauseReasons()TND由于以下情况将断开ProxyConfig "Secure Internet Access":on_network:**28f629ee-7618-44cd-852d-6ae1674e3cac action=Disconnect**
2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus()ProxyConfig 'Secure Private Access'正在断开连接，原因如下：InactiveTn
2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus()ProxyConfig 'Secure Internet Access'正在断开连接，原因如下：InactiveTn

匹配规则类型DNS

2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main， 0x0000343c] I/ ZtnaTransportManager.cpp:1251 ZtnaTransportManager::closeObsoleteAppFlows()强制关闭应用流，因为过时的ProxyConfig enrollmentId=7b35249c-64e1-4f55-b12b-58875a806969 proxyConfigConfigConfigProxyConfigConfigFlow id=default_tia_config TCP目标[safebrowsing.googleapis.com]:443 srcPort=61049 realDestIpAddr=172.253.122.95 process=<chrome.exe|PID 11904|user amit\amita> parentProcess=<chrome.exe|PID 5220|user amit\amita> **matchRuleType=DNS**

相关信息

- 思科技术支持和下载
- 思科安全访问帮助中心
- Cisco SASE设计指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。