使用受信任網路檢測配置零信任網路訪問

目錄

簡介

本文檔介紹配置ZTNA可信網路檢測所需的步驟。

必要條件

- 安全客戶端最低版本5.1.10
- 支援的平台 — Windows和MacOS
- 適用於Windows的受信任平台模組(TPM)
- 適用於Apple裝置的安全群落協處理器
- 任何受信任網路配置檔案中配置的「受信任伺服器」將隱式排除在ZTA偵聽之外。這些伺服器也不能作為ZTA私有資源訪問。
- TND配置會影響組織中的所有已註冊客戶端
- 管理員可以使用後續步驟為受信任的伺服器生成「證書公鑰雜湊」
  - 下載受信任的伺服器公共證書
  - 運行此shell命令可以generate the hash:

```
openssl x509 -in

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

需求

思科建議您瞭解以下主題：

- Cisco Secure Access
- 使用SAML或基於證書的身份驗證將裝置註冊為零信任訪問。

採用元件

- 安全使用者端版本5.1.13
- TPM
- 安全訪問租戶
- Windows裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

- TND使管理員能夠配置安全客戶端，以臨時暫停受信任網路上的ZTA流量引導和實施。
- 當終端離開受信任網路時，安全客戶端恢復ZTA實施。
- 此功能不需要任何終端使用者互動。
- ZTA TND配置可以獨立管理專用和網際網路ZTA目標。

主要優勢

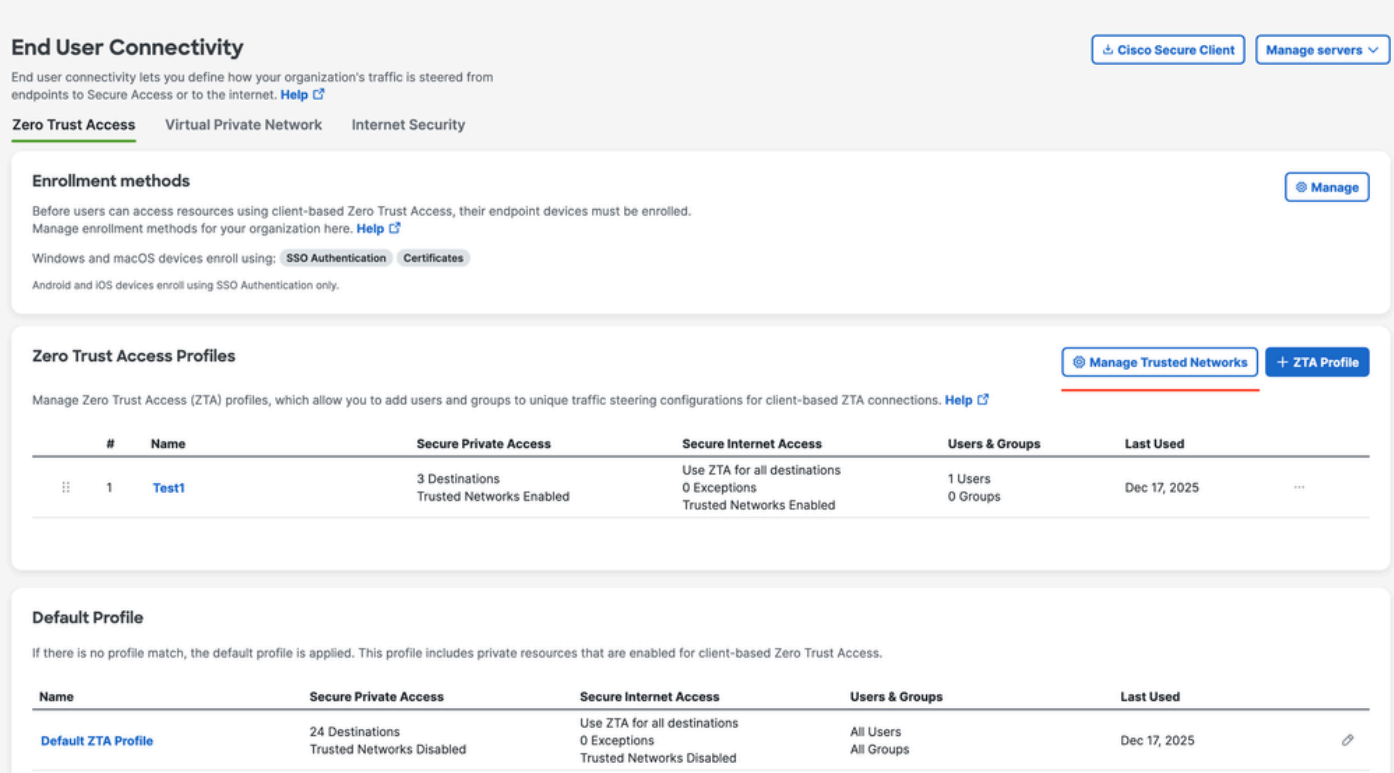
- 提高的網路效能和減少的延遲提供了更流暢的使用者體驗。
- 可信網路中的本地安全實施提供了靈活且最佳化的資源利用率。
- 終端使用者無需任何提示或操作即可利用這些優勢。
- 對專用接入和網際網路接入的TND進行獨立控制，為管理員提供處理不同運營和安全問題的靈活性

設定

步驟 1:建立受信任的網路配置檔案 — DNS伺服器和域

導航到Secure Access Dashboard:

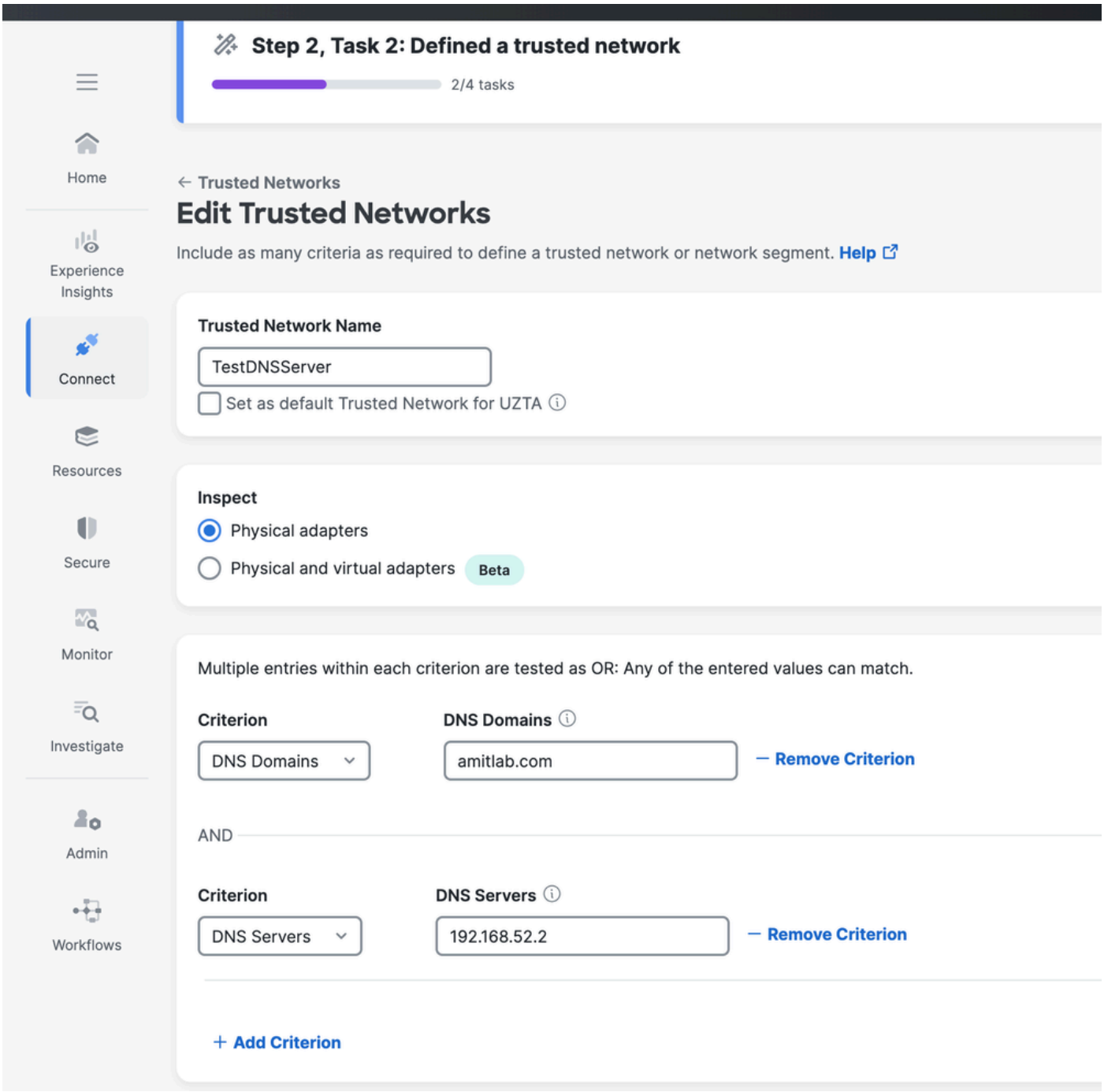
- 按一下Connect> End User Connectivity > Manage Trusted Networks > +Add



- 提供受信任網路配置檔案的名稱，並至少配置以下條件之一：
  - DNS Servers — 客戶端處於受信任網路時，網路介面必須擁有的所有DNS伺服器地址的逗號分隔值。任何輸入的伺服器都可以用於匹配此配置檔案。要匹配TND，任何DNS伺服器地址必須與本地介面匹配。
  - DNS Domains — 客戶端處於受信任網路時，網路介面必須具有的DNS字尾的逗號分隔值。
  - Trusted Server — 在網路上新增一台或多台伺服器，這些伺服器提供一個TLS證書，該證書的雜湊與您提供的雜湊值匹配。要指定443以外的埠，請使用標準符號附加埠。您最多可以新增10個受信任的伺服器，其中只有一個需要通過驗證。
    - Certificate Public Key Hash:檢查步驟先決條件和系統限制，瞭解如何生成證書雜湊。

重複這些步驟以新增其他受信任網路配置檔案。

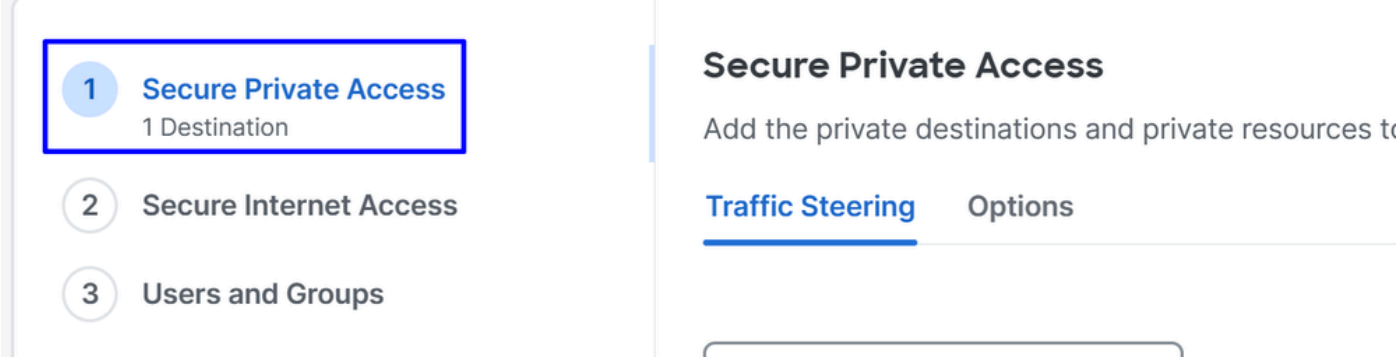
附註：同一標準內的多個選項是OR運算子。定義的不同條件是AND運算子。



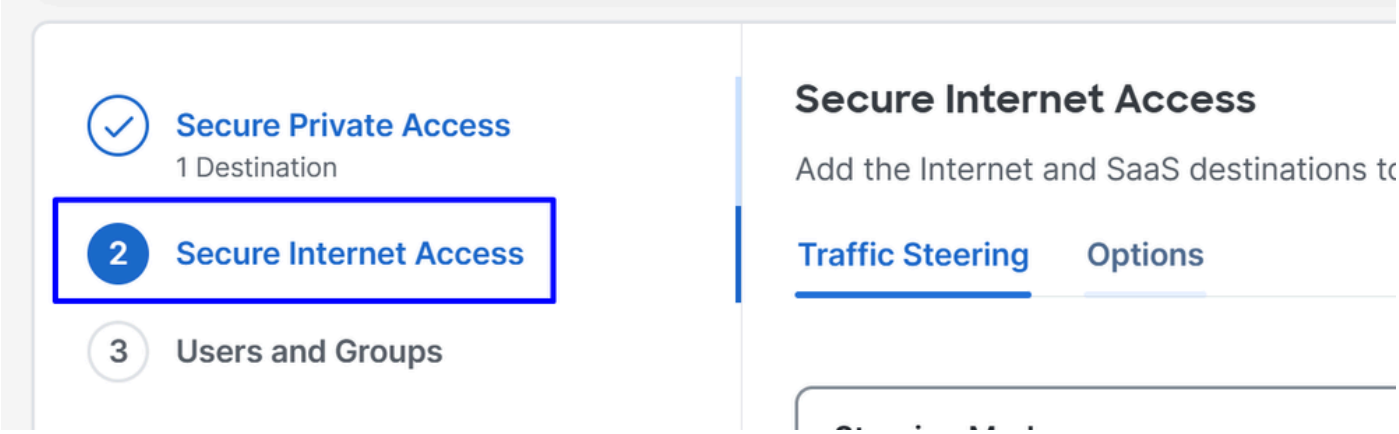
步驟 2:為專用或網際網路訪問啟用TND

- 導航至Connect> End User Connectivity
- 編輯ZTA配置檔案
- 對於Secure Private Destinations或 Secure Internet Access

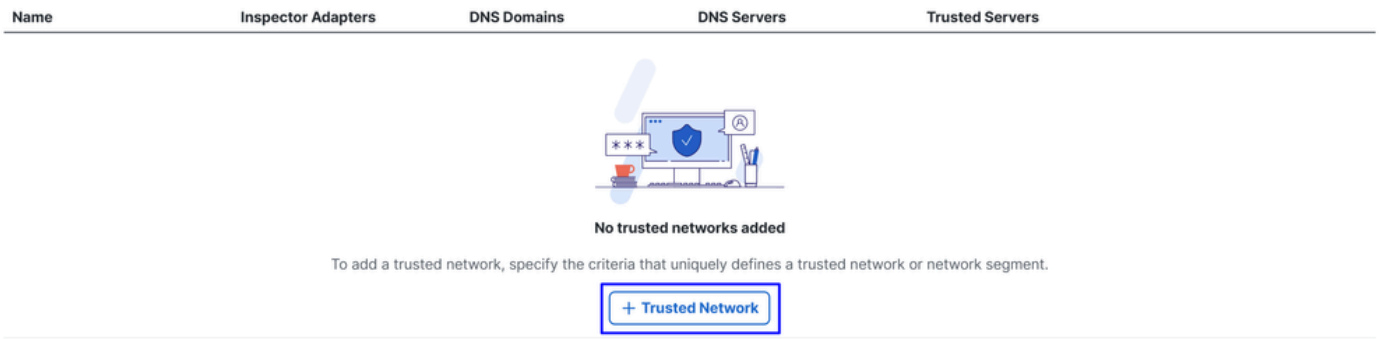
安全私人訪問



安全的網際網路訪問

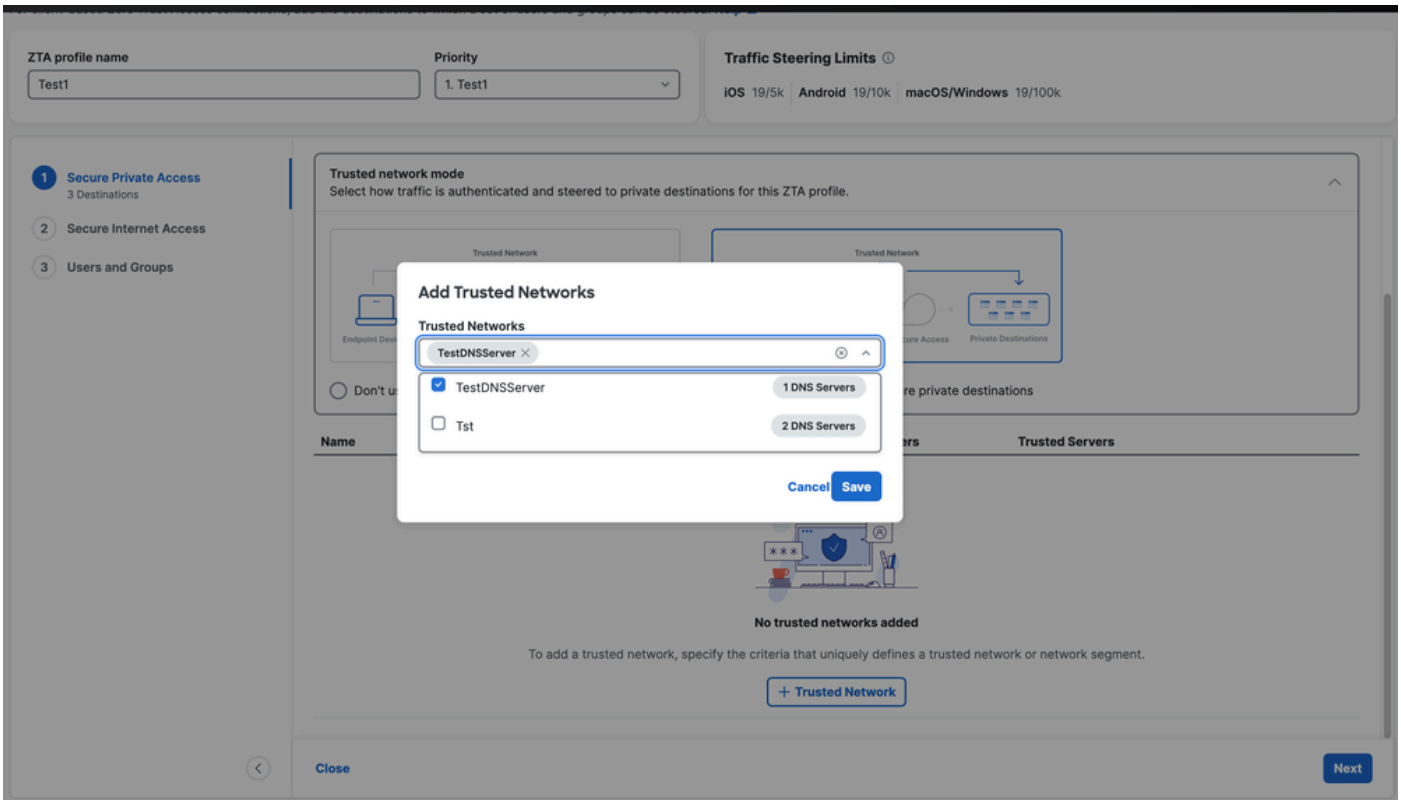


- 按一下 Options
  - 按一下Use trusted networks to secure private destinations或Use trusted networks to secure internet destinations視之前選擇的選項而定
  - 按一下 + Trusted Network

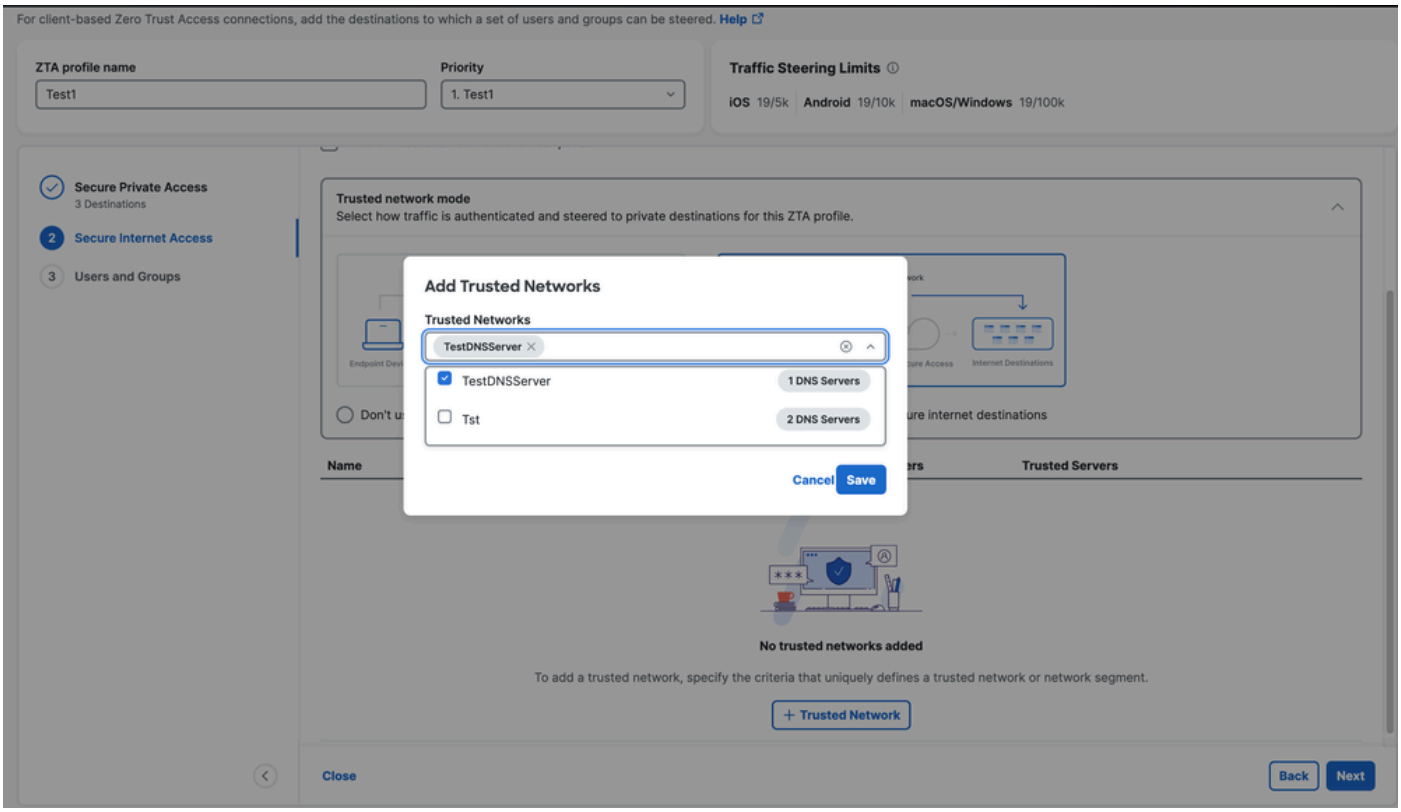


- 選擇您在上一頁中配置的受信任網路配置檔案，然後按一下 Save

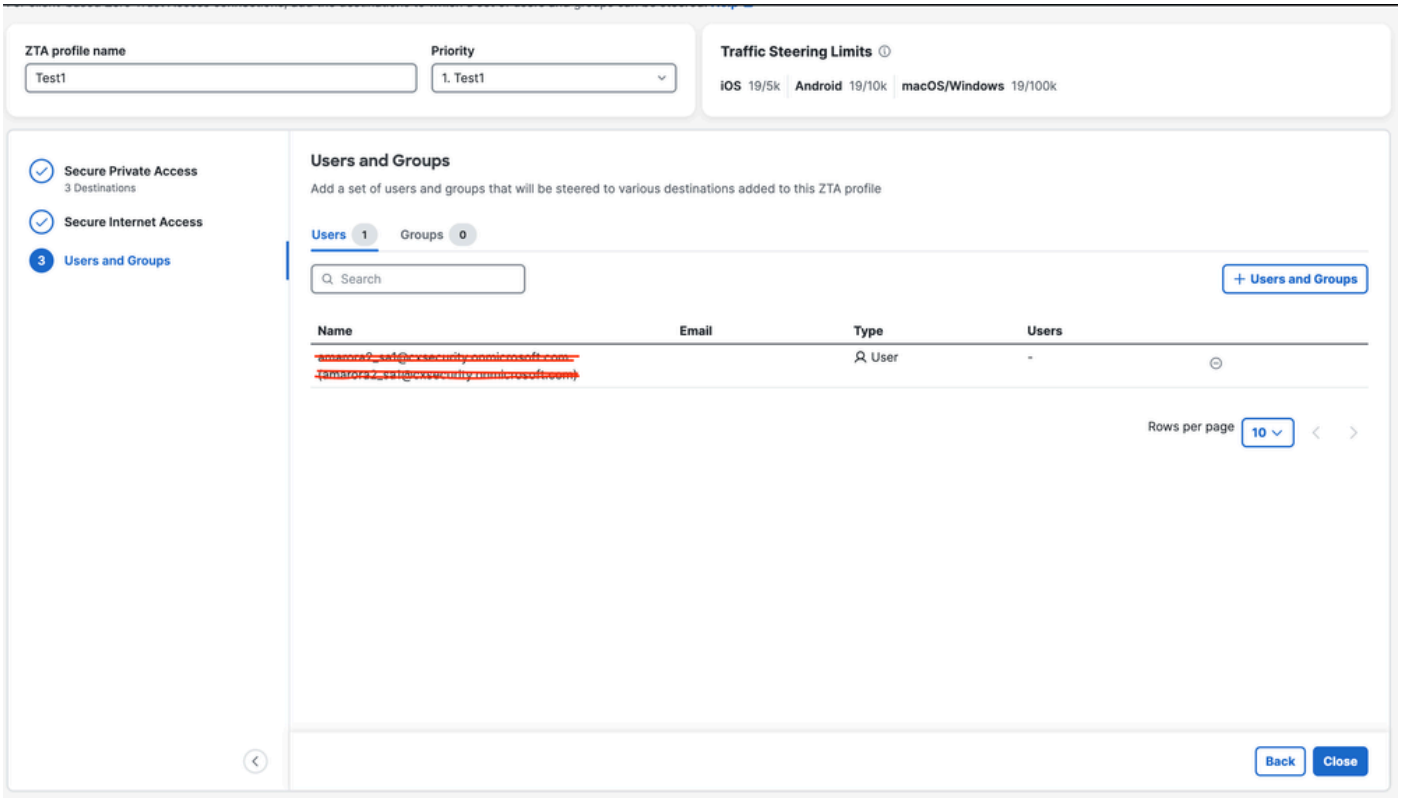
安全私人訪問



安全的網際網路訪問



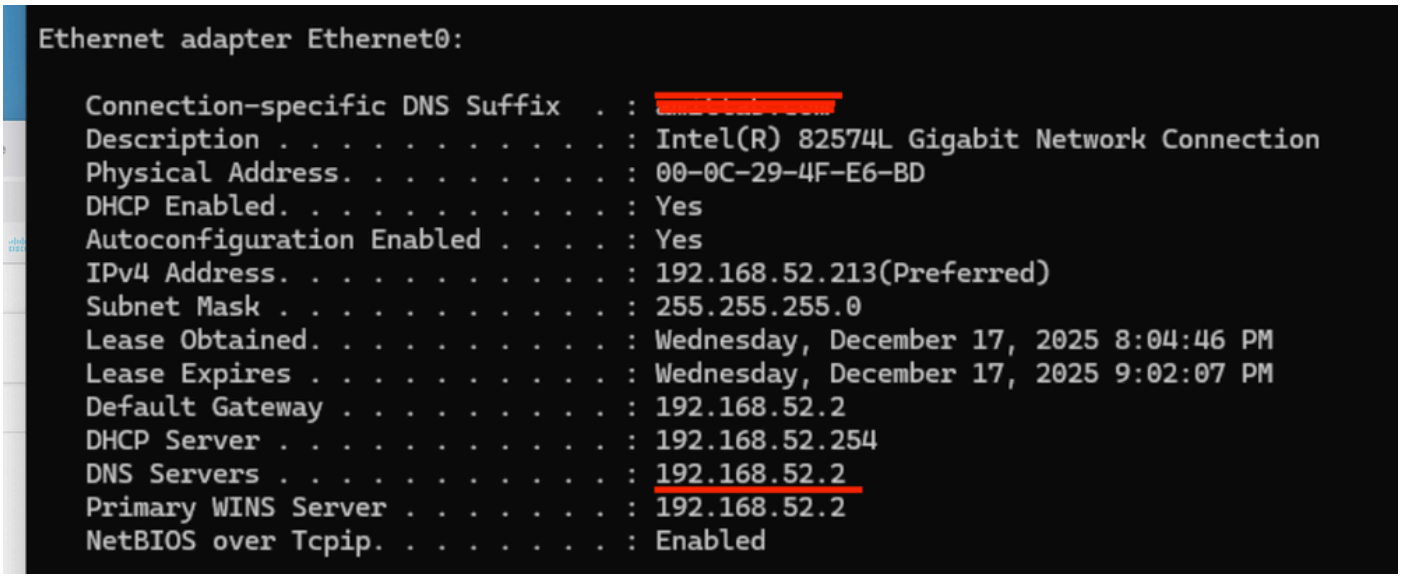
- 將分配給Users/GroupsZTA配置檔案，然後按一下Close。



步驟 3:客戶端配置

1.確保在乙太網介面卡下定義了正確的DNS伺服器，因為我們選擇了物理介面卡作為標準

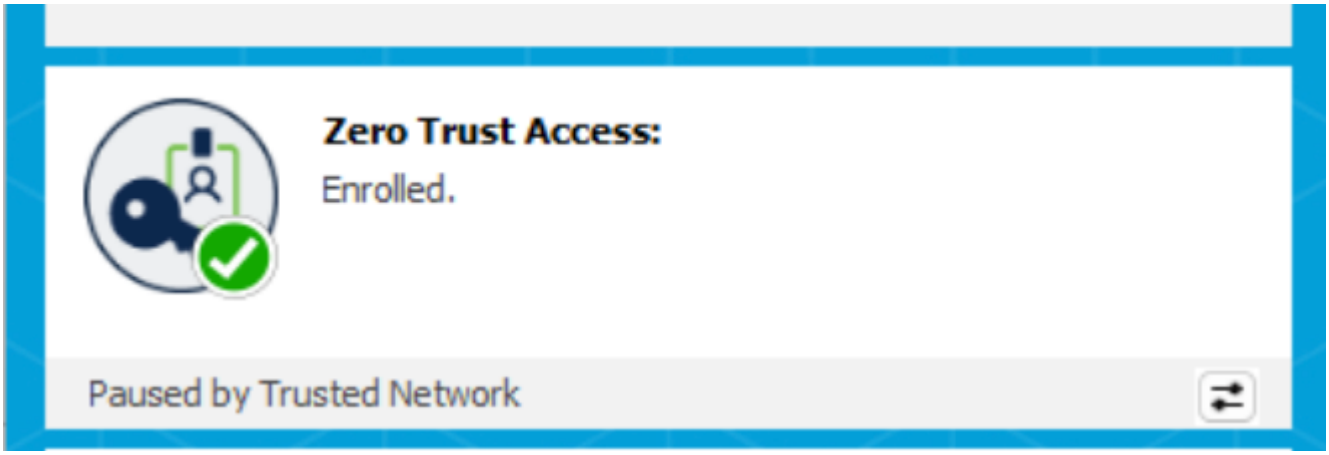
2.確保定義了連線特定的DNS字尾。

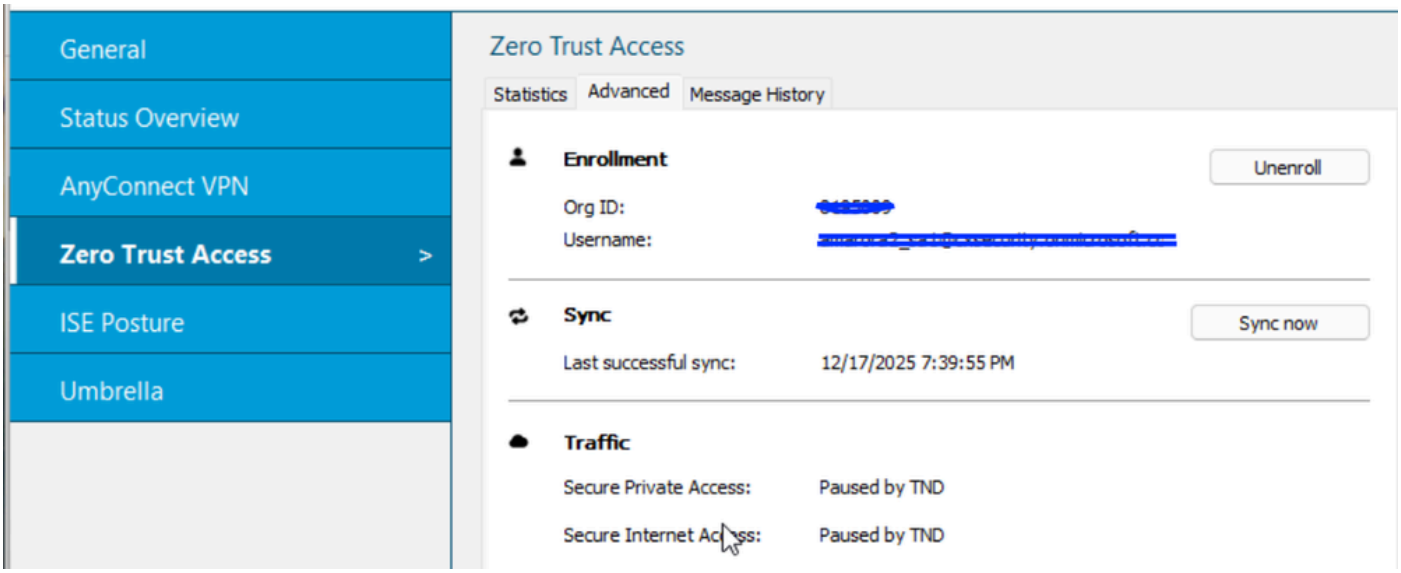


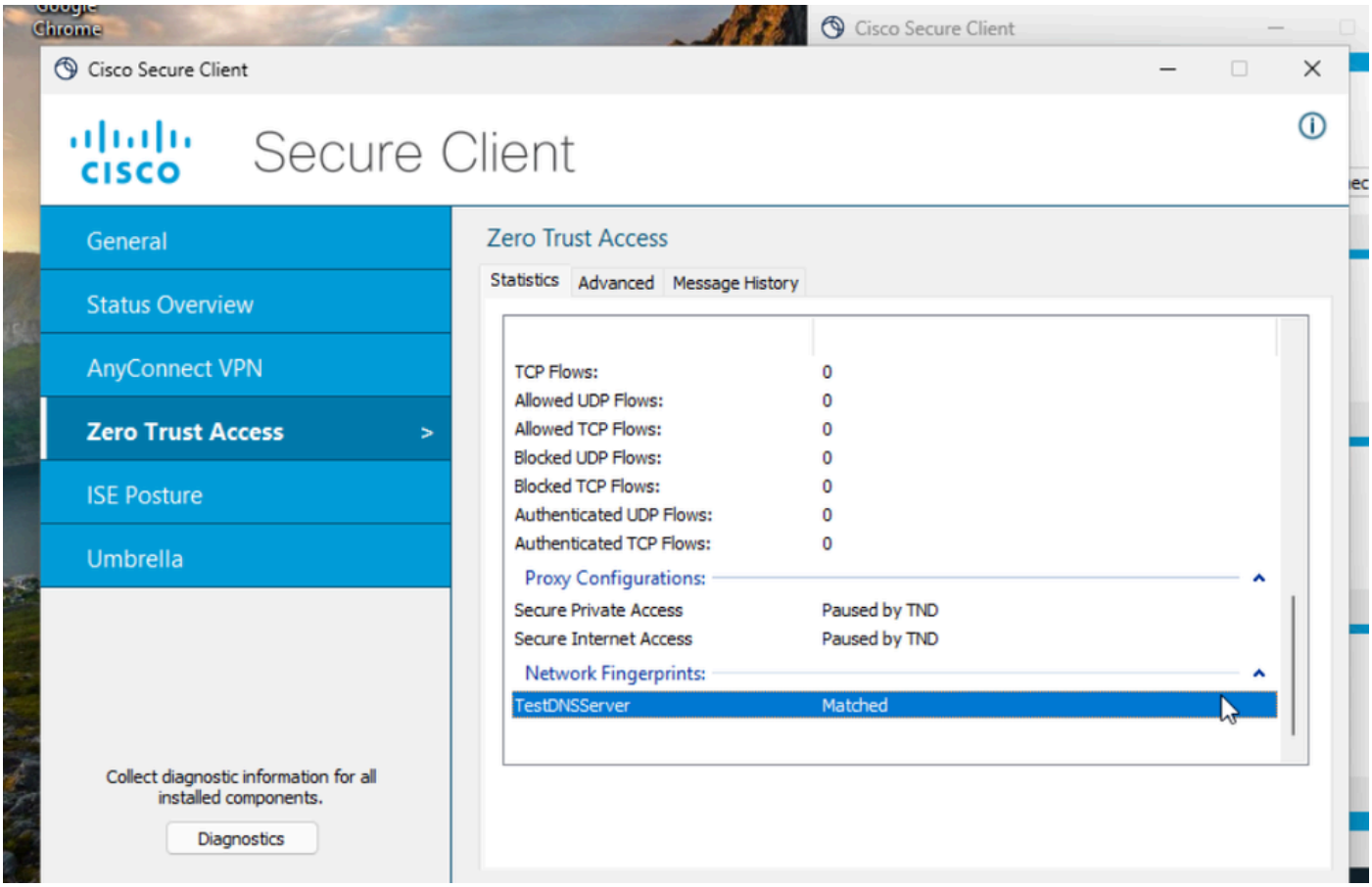
幾分鐘後，下一個ZTA配置同步到安全客戶端，ZTA模組檢測到它位於一個已配置的可信網路時，會自動暫停。

驗證

- 從安全客戶端


Zero Trust Access:
Enrolled.
Paused by Trusted Network


General
Status Overview
AnyConnect VPN
Zero Trust Access
ISE Posture
Umbrella
Zero Trust Access
Statistics
Advanced
Message History
Enrollment
Unenroll
Org ID:
Username:
Sync
Sync now
Last successful sync:
12/17/2025 7:39:55 PM
Traffic
Secure Private Access:
Paused by TND
Secure Internet Access:
Paused by TND



- 從DART捆綁包 — ZTA日誌

未配置TND規則。

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons()TND將連線ProxyConfig 'default_spa_config'（無規則）

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons()TND將連線ProxyConfig 'default_tia_config'（無規則）

配置的TND規則 — DNS伺服器 — 客戶端接收配置

25-12-17 20:33:15.987956 csc_zta_agent[0x00000f80, 0x00000ed4]帶CaptivePortalDetectionService.cpp:308 CaptivePortalDetectionService::getProbeUrl()無最後一個網路快照，使用第一個探測url

2025-12-17 20:33:15.992042 csc_zta_agent[0x00000f80, 0x00000ed4] I/NetworkChangeService.cpp:144 NetworkChangeService::**Start()初始網路快照：Ethernet0: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"告訴TND已在ZTA配置檔案中配置。

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":"connect"},"id" ","label":"Secure Private

Access","match_resource_configs":["spa_steering_config"],"proxy_server":"spa_proxy_server"},{"conditional_actions":[{"action":"disconnect","check_type":"on_
7618-44cd-852d-6ae1674e3cac"]},{"action":

2025-12-17 17:55:36.472435 csc_zta_agent[0x000039a8/main，0x0000343c] I/網路指紋服務.cpp:196 NetworkFingerprintService::handleStatusUpdate()廣播網路指紋狀態：**指紋:28f629ee-7618-44cd-852d-6ae1674e3cac介面：Ethernet0**

DNS條件上的TND斷開連線

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

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer， 0x0000343c] I/ ActiveSteeringPolicy.cpp:287 ActiveSteeringPolicy::collectProxyConfigPauseReasons()TND由於以下情況將斷開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'正在斷開連線，原因是：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'正在斷開連線，原因是：InactiveTn

匹配規則型別DNS

2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main，0x0000343c] I/ZtnaTransportManager.cpp:1251 ZtnaTransportManager::closeObsoleteAppFlows()由於過時的ProxyConfig註冊Id=7b35249c-64e1-4f55-b12b-58875a806969 proxyConfigConfigConfigId id=default_tia_config TCP destination [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**

相關資訊

- 思科技術支援與下載
- Cisco Secure Access幫助中心
- Cisco SASE設計手冊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。