Configuración del acceso a la red sin confianza con la detección de redes de confianza

Contenido

Introducción

Este documento describe los pasos necesarios para configurar la Detección de redes de confianza de ZTNA.

Prerequisites

- Secure Client versión mínima 5.1.10
- Plataforma compatible: Windows y MacOS
- Módulo de plataforma segura (TPM) para Windows
- Coprocesador Secure Enclave para dispositivos Apple
- Los 'servidores de confianza' configurados en cualquier perfil de red de confianza se excluyen implícitamente de la interceptación ZTA. Esos servidores tampoco pueden ser accesos como recursos privados ZTA.
- La configuración de TND afecta a todos los clientes inscritos en la organización
- Los administradores pueden seguir estos pasos para generar un 'Hash de clave pública de certificado' para servidores de confianza
  - Descargue el certificado público de servidores de confianza
  - Ejecute este comando shell para generate the hash:

```
openssl x509 -in
```

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

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro de Cisco
- Inscriba dispositivos en acceso de confianza cero mediante autenticación SAML o basada en certificados.

Componentes Utilizados

- Secure Client versión 5.1.13
- TPM
- Arrendatario de acceso seguro
- Dispositivo Windows

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

- TND permite a los administradores configurar Secure Client para pausar temporalmente el direccionamiento y la aplicación del tráfico ZTA en redes de confianza.
- Secure Client reanudará la aplicación de ZTA cuando el terminal abandone la red de confianza.
- Esta función no requiere ninguna interacción por parte del usuario final.
- Las configuraciones ZTA TND se pueden gestionar de forma independiente para destinos ZTA privados e Internet.

Ventajas clave

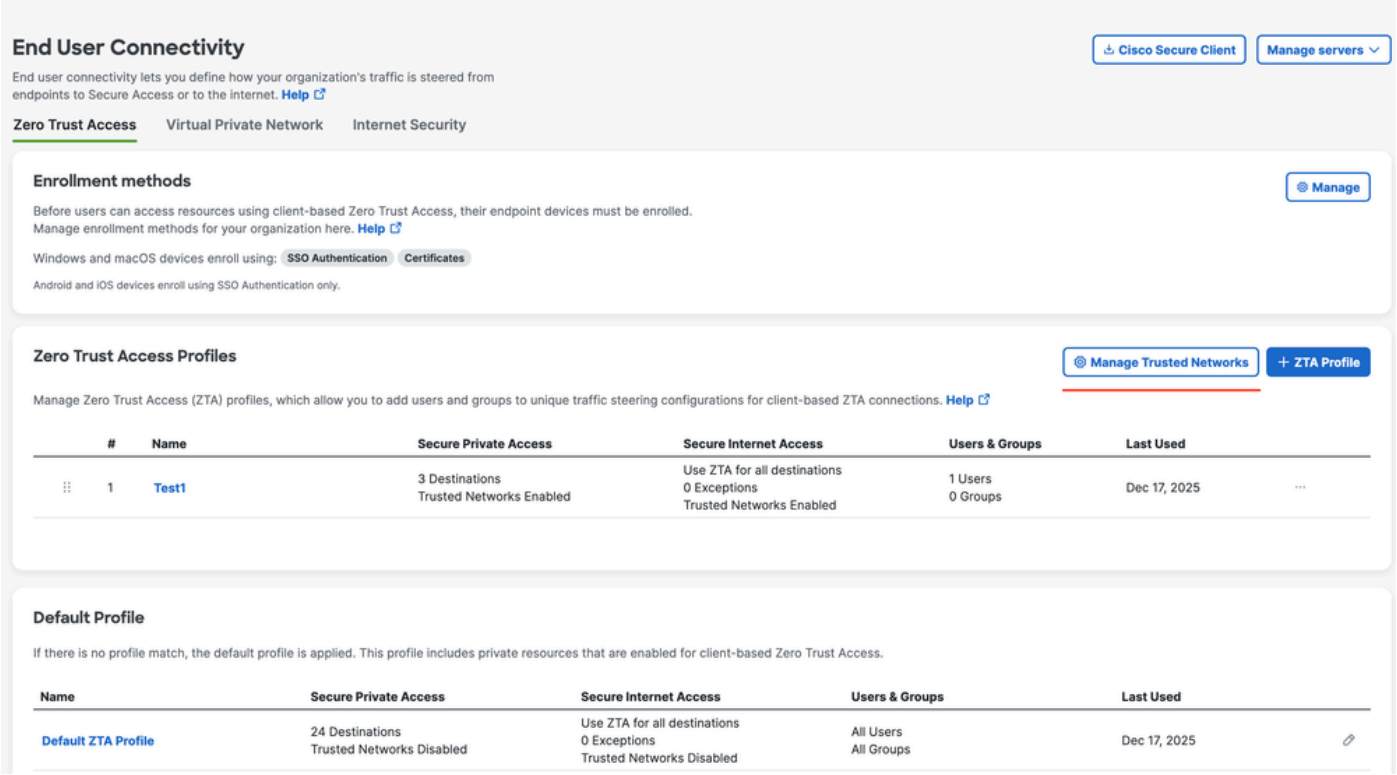
- Un rendimiento de red mejorado y una latencia reducida proporcionan una experiencia de usuario más fluida.
- La aplicación de seguridad local en la red de confianza ofrece una utilización de recursos flexible y optimizada.
- Los usuarios finales pueden aprovechar las ventajas sin ningún tipo de aviso o acción.
- El control independiente de TND para el acceso privado y el acceso a Internet proporciona flexibilidad administrativa para gestionar diferentes preocupaciones operativas y de seguridad

Configurar

Paso 1: Crear perfil de red de confianza: servidor y dominio DNS

Vaya al Panel de Acceso Seguro:

- Haga clic en Connect > End User Connectivity > Manage Trusted Networks > +Add



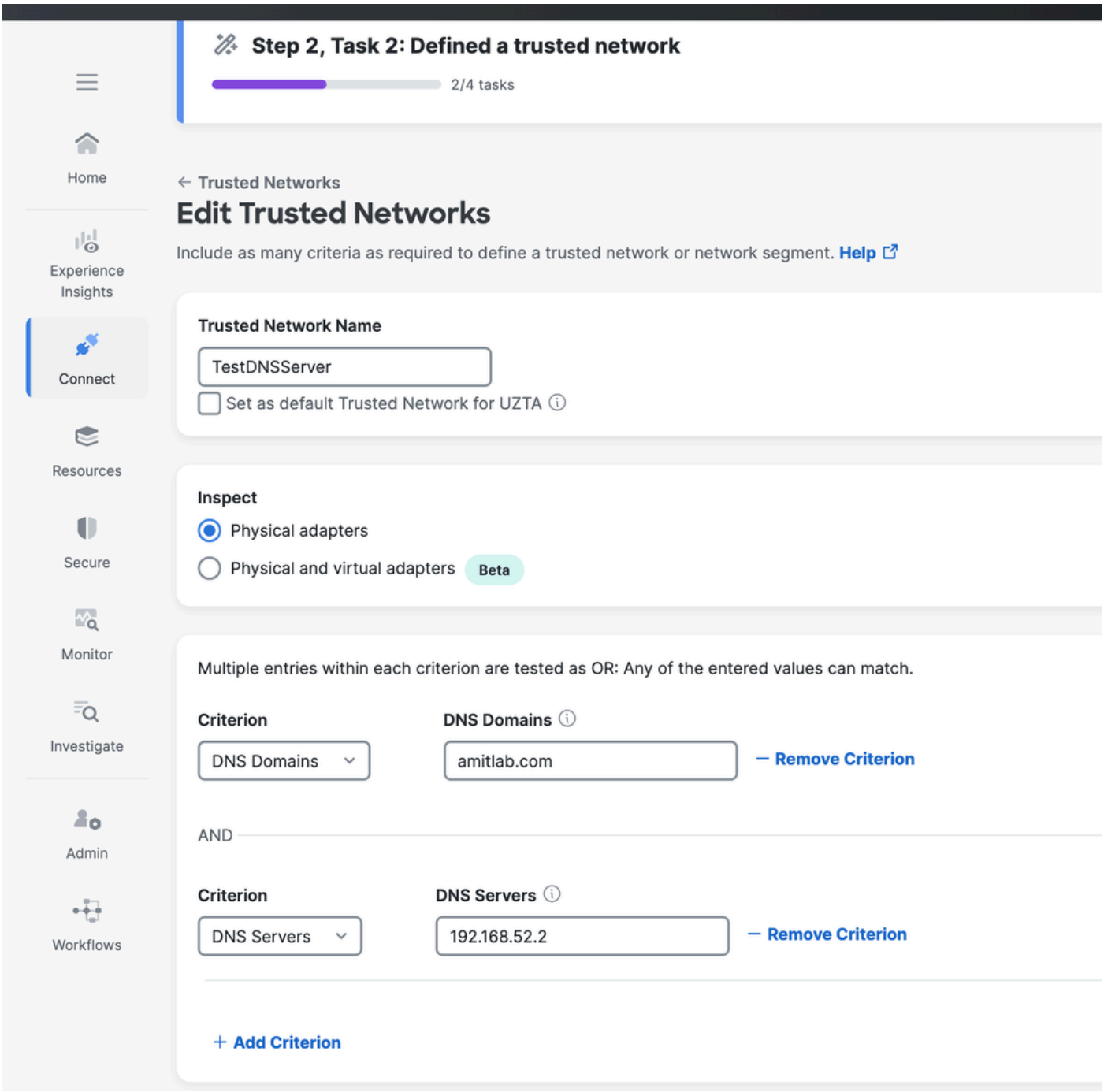
- Proporcione un nombre para el perfil de red de confianza y configure al menos uno de los siguientes criterios:
  - DNS Servers - Valores separados por comas de todas las direcciones de servidor DNS que debe tener una interfaz de red cuando el cliente está en una red de confianza. Cualquier servidor introducido se puede utilizar para coincidir con este perfil. Para que TND coincida, cualquier dirección del servidor DNS debe coincidir con la interfaz local.
  - DNS Domains - Valores separados por comas de sufijos DNS que debe tener una interfaz de red cuando el cliente está en una red de confianza.
  - Trusted

Server- Agregue uno o más servidores en la red que presenten un certificado TLS con un hash que coincida con el hash proporcionado. Para especificar un puerto que no sea 443, añada el puerto utilizando la notación estándar. Puede agregar hasta 10 servidores de confianza, de los cuales sólo uno debe pasar la validación.

- Certificate Public Key Hash: Verifique el paso Prerrequisitos y Límites del Sistema para saber cómo generar el hash del certificado.

Repita los pasos para agregar perfiles de red de confianza adicionales.

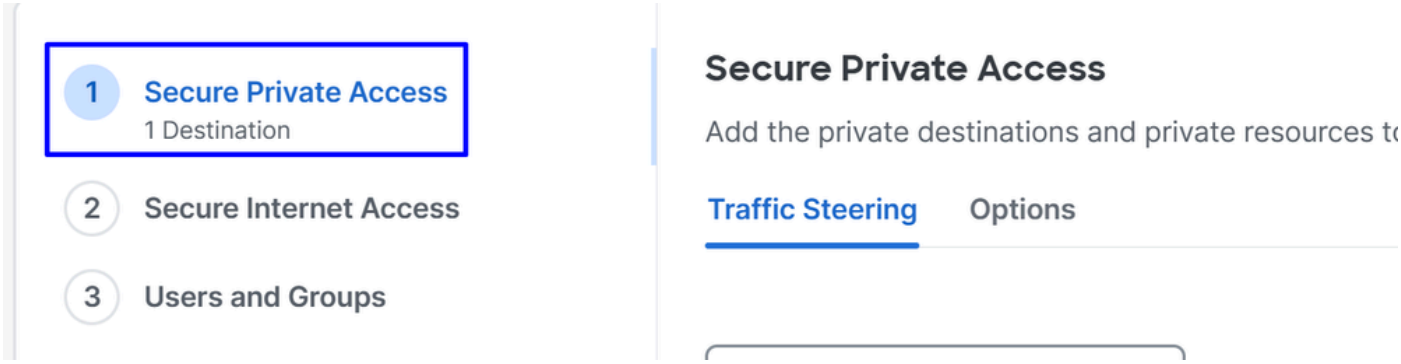
Nota: Varias opciones dentro de los mismos criterios es un operador OR. Distintos criterios definidos es un operador AND.



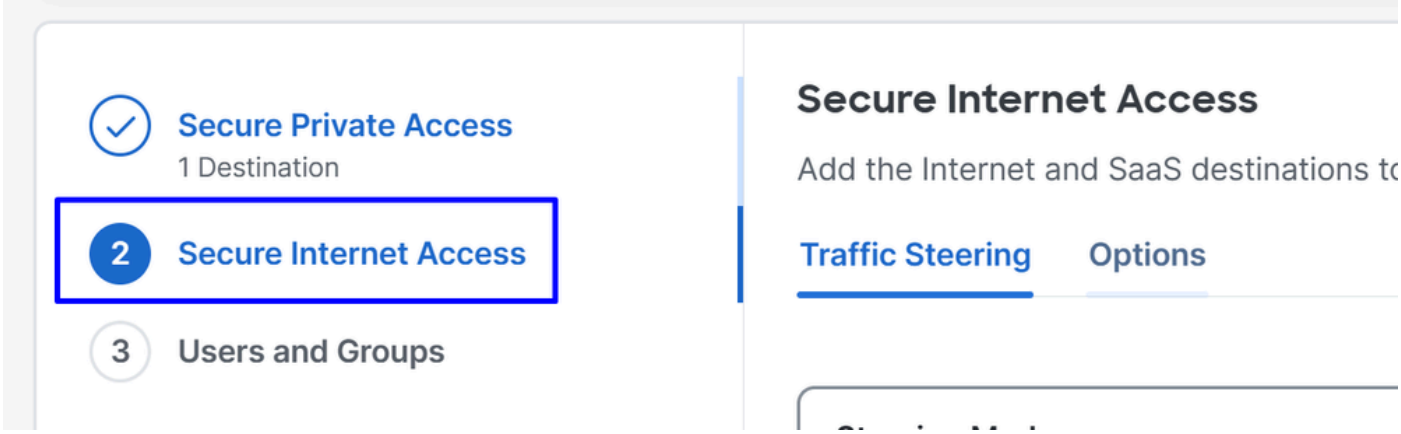
Paso 2: Activar TND para acceso privado o a Internet

- Vaya a Connect > End User Connectivity
- Editar perfil ZTA
- ParaSecure Private DestinationsO Secure Internet Access

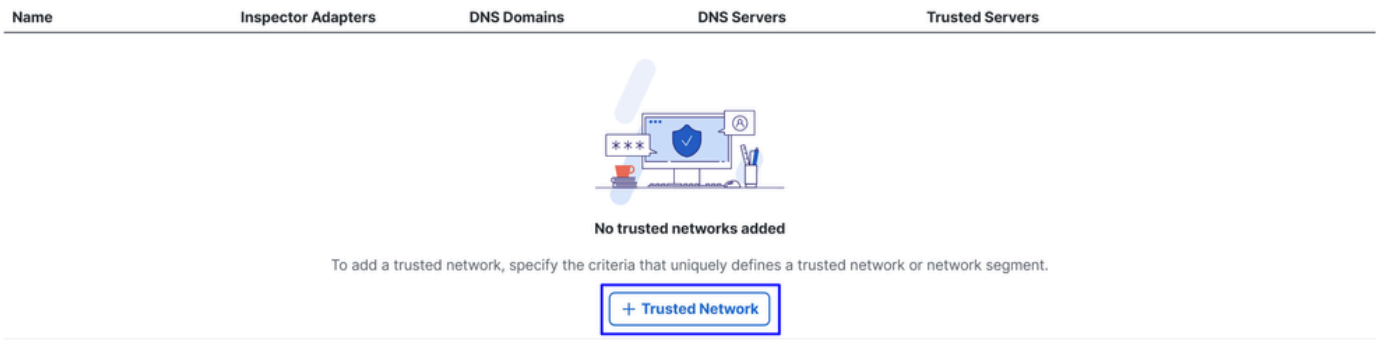
Acceso privado seguro



Acceso seguro a Internet

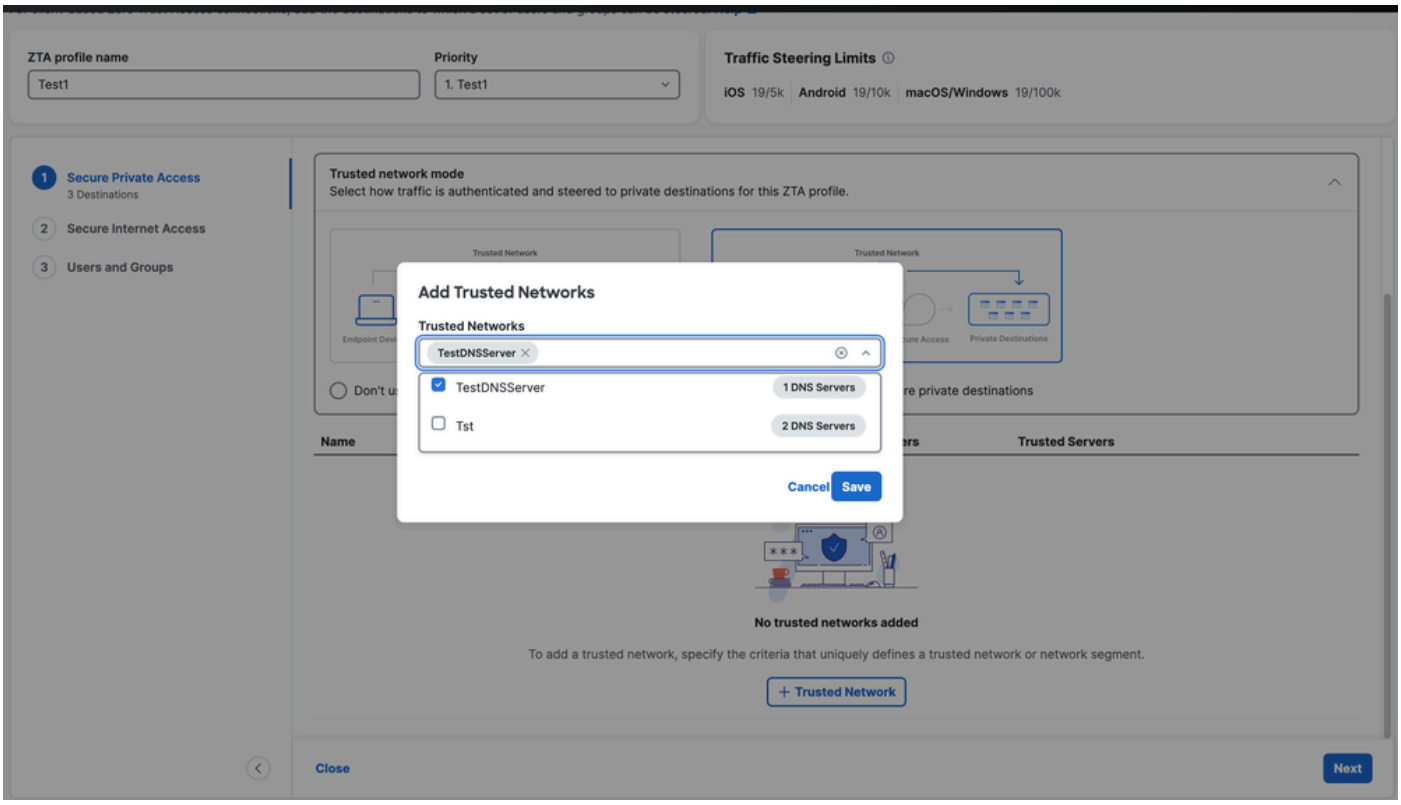


- Haga clic en Options
  - Haga clic en Use trusted networks to secure private destinations o Use trusted networks to secure internet destinationsdepende de la opción elegida antes de
  - Haga clic en + Trusted Network

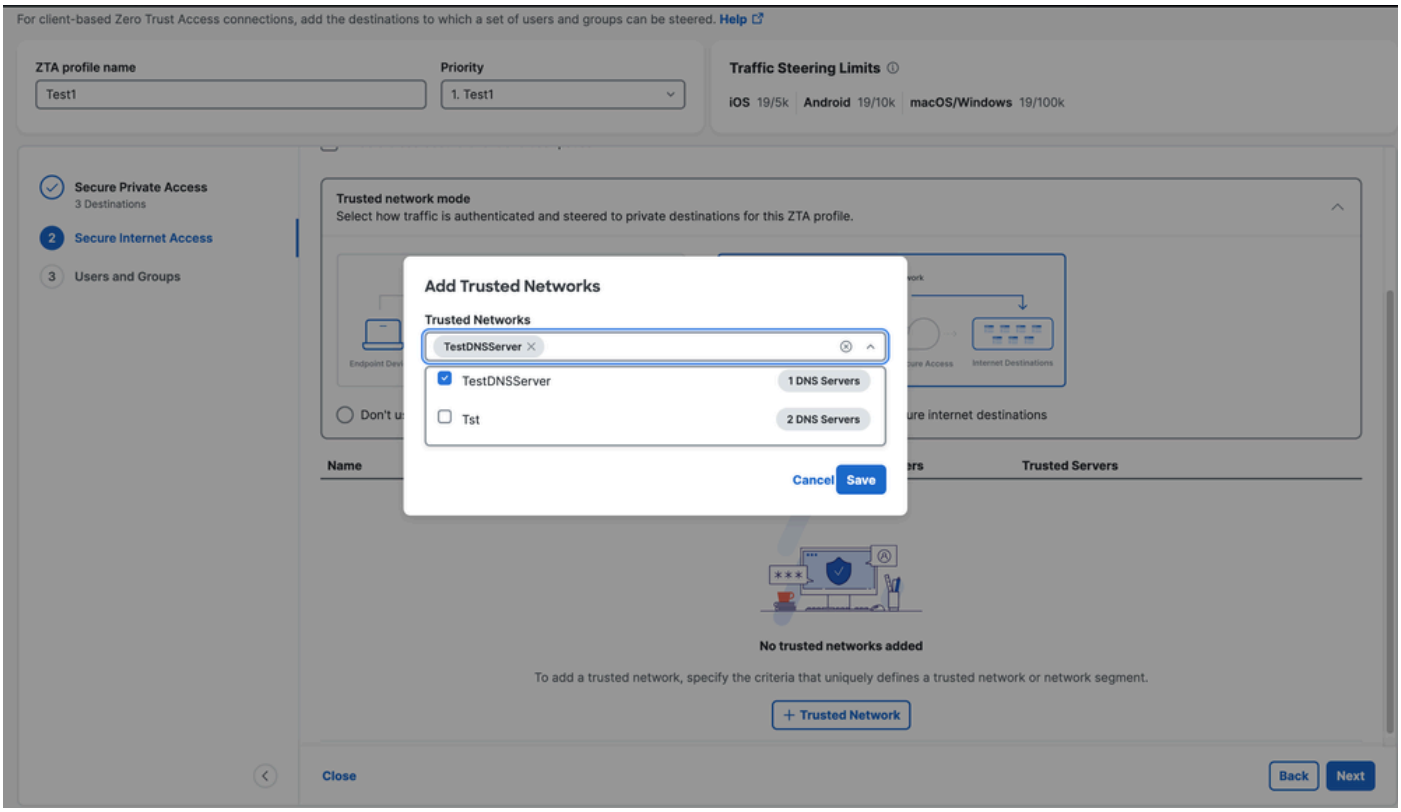


- Elija los perfiles de redes de confianza que ha configurado en la página anterior y haga clic en Save

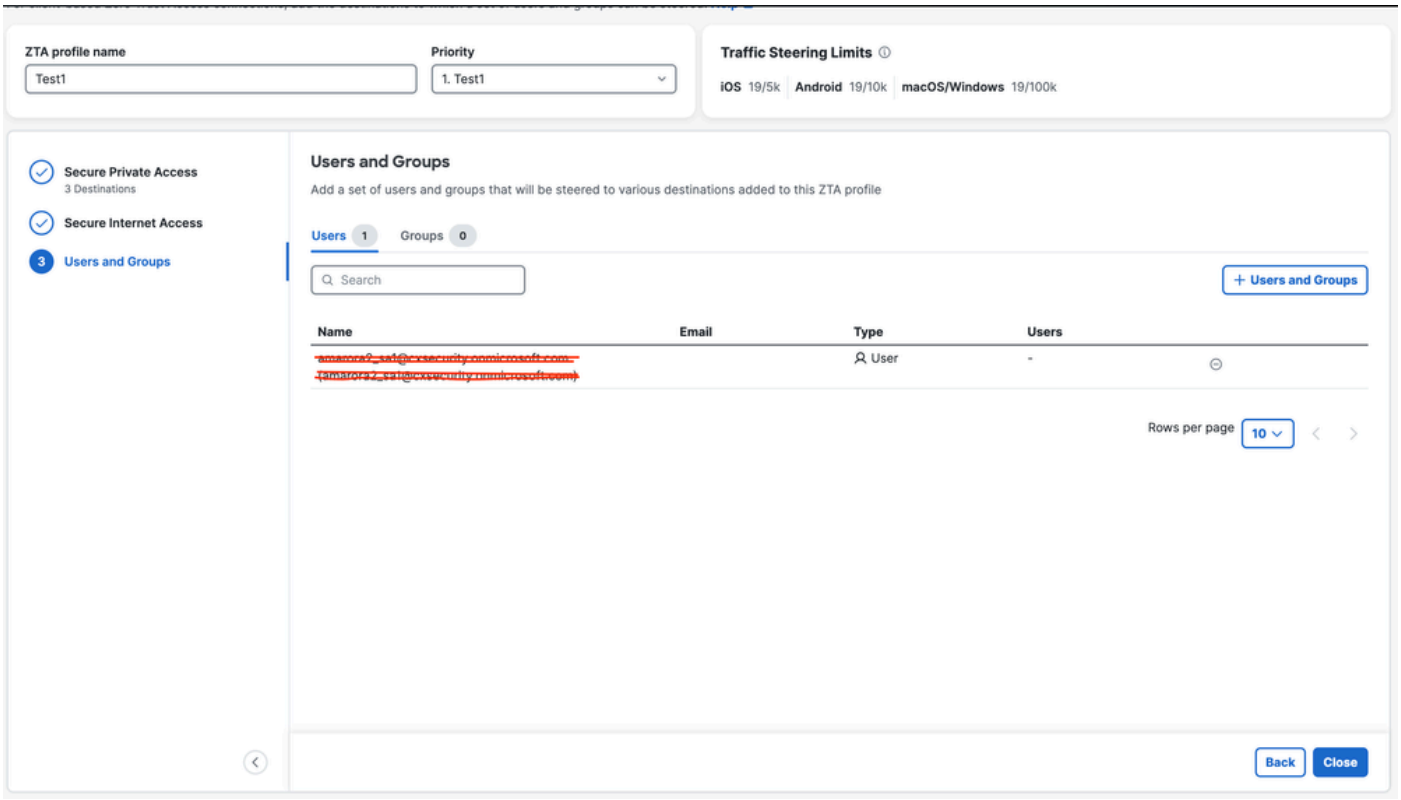
Acceso privado seguro



Acceso seguro a Internet



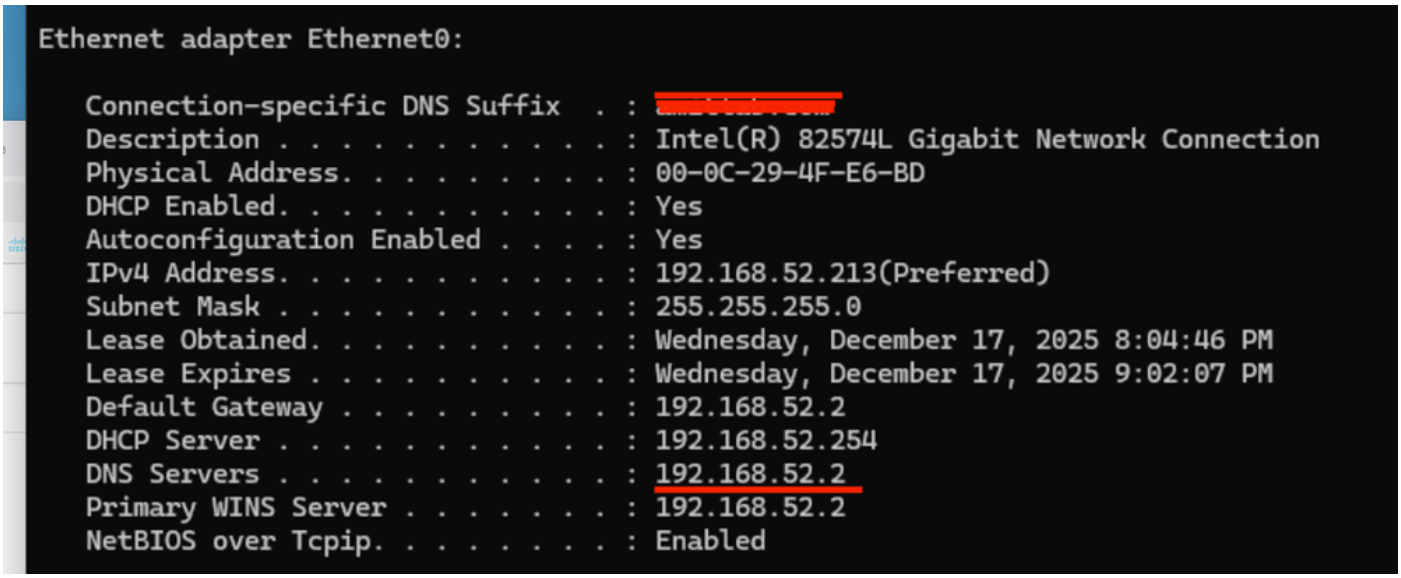
- Asigne el Users/Groups a Perfil ZTA y haga clic en Close.



Paso 3: Configuración del lado del cliente

1. Asegúrese de que tiene el servidor DNS correcto definido en Adaptador Ethernet, ya que hemos elegido Adaptador físico como criterio

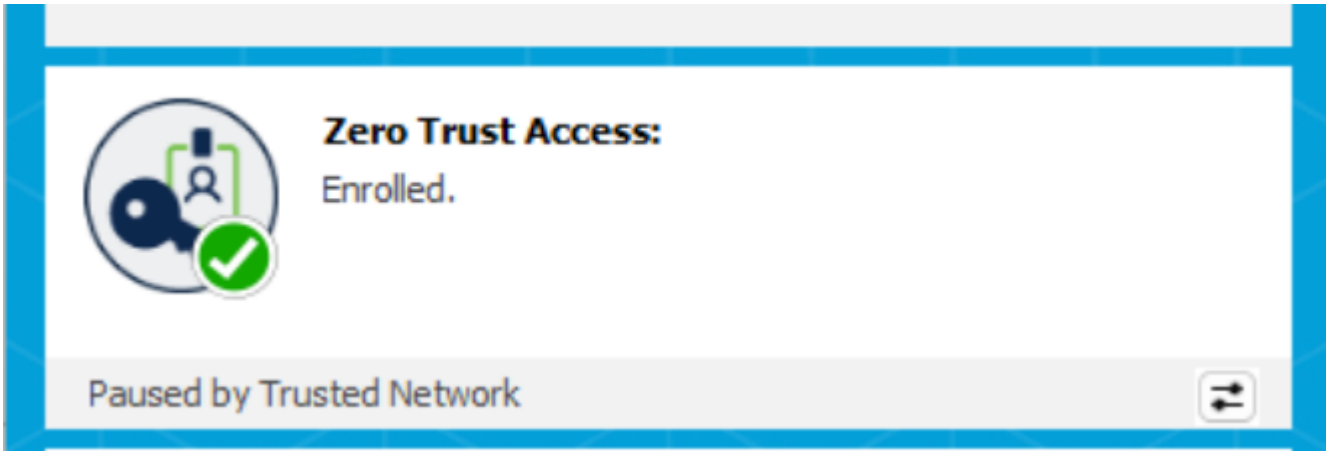
2. Asegúrese de que ha definido el sufijo DNS específico de la conexión.

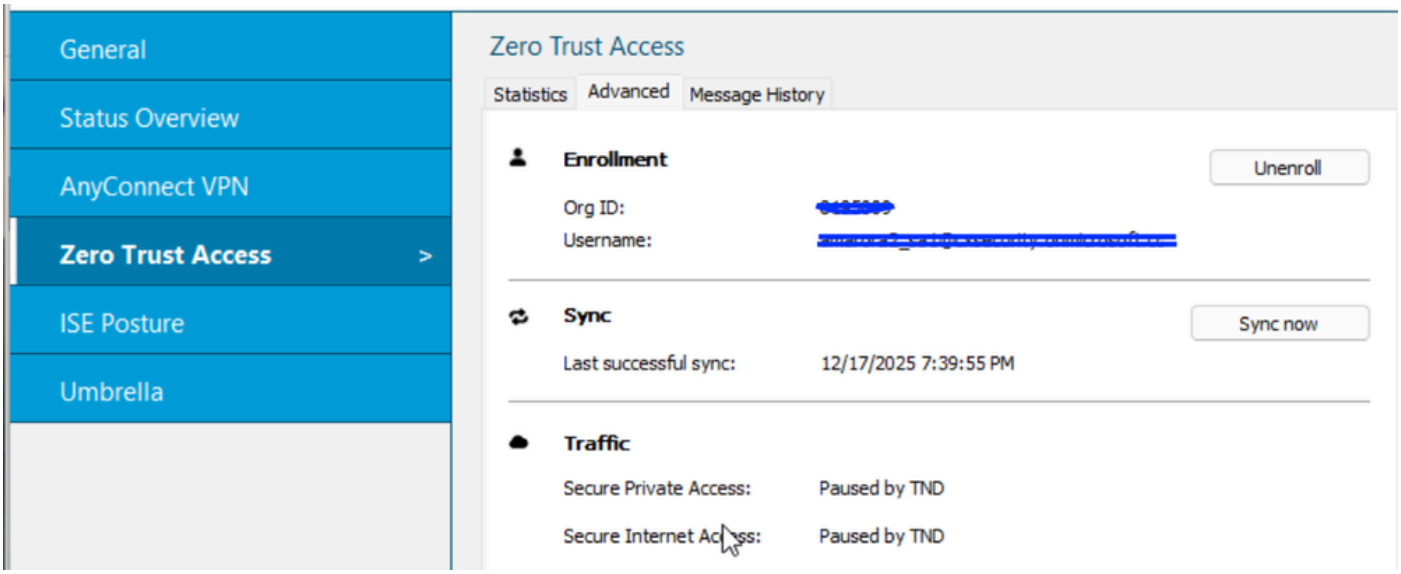


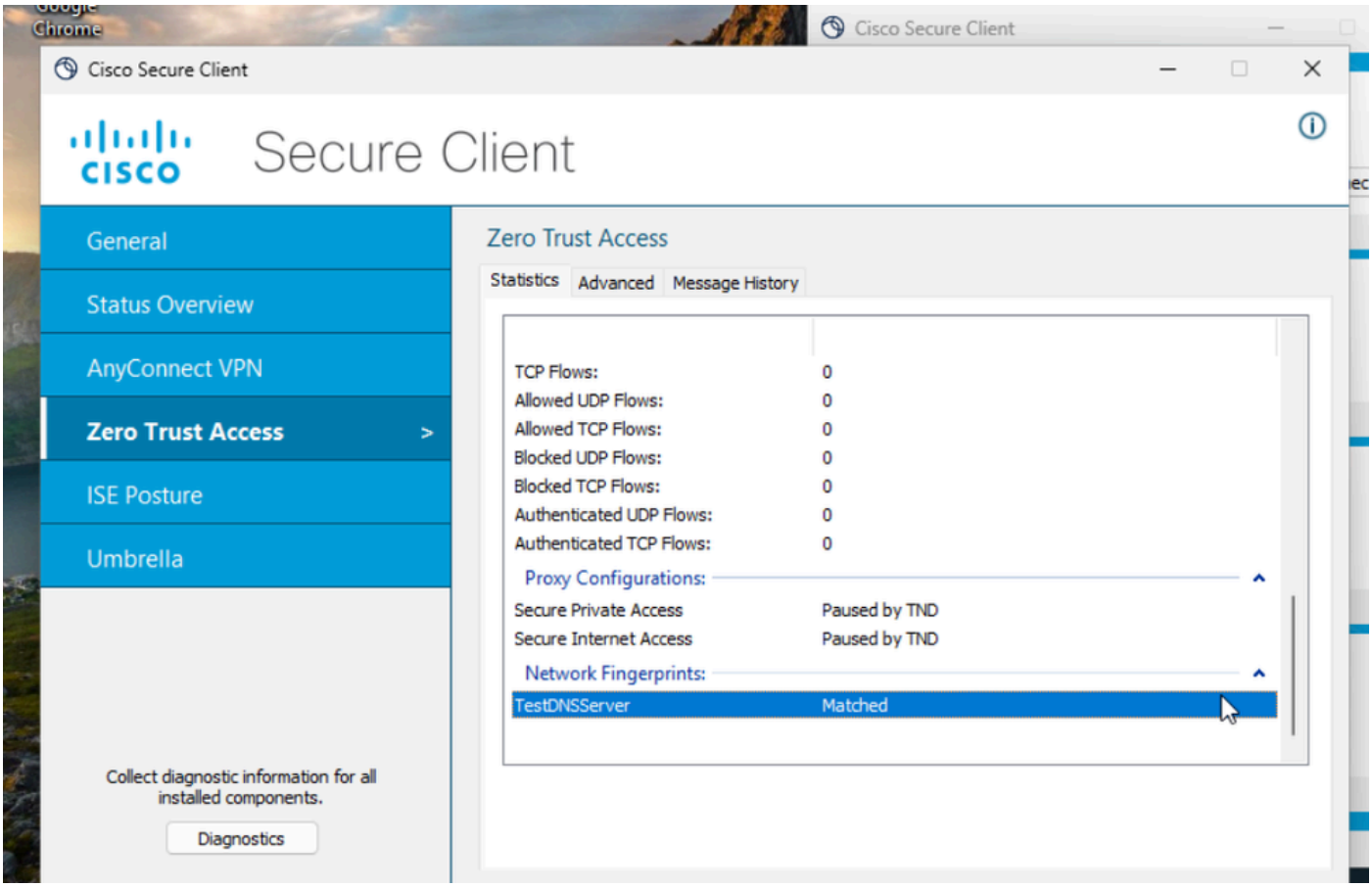
Con la siguiente sincronización de configuración ZTA a Secure Client en unos minutos, el módulo ZTA se detiene automáticamente cuando detecta que está en una de las redes de confianza configuradas.

Verificación

- Desde Secure Client







- Desde el paquete DART: registros ZTA

No hay reglas TND configuradas.

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

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

Regla TND configurada - Servidor DNS - Configuración recibida por el cliente

25-12-17 20:33:15.987956 csc_zta_agent[0x00000f80, 0x00000ed4] W/ CaptivePortalDetectionService.cpp:308 CaptivePortalDetectionService::getProbeUrl() ninguna última instantánea de red, utilizando la primera url de sondeo

2025-12-17 20:33:15.992042 csc_zta_agent[0x00000f80, 0x00000ed4] I/ NetworkChangeService.cpp:144 NetworkChangeService::**Start() Instantánea de red inicial:**
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=Desconocido

acciones_condicionales":[{"action":"disconnect" indica que TND está configurado en el perfil ZTA.

2025-12-17 17:55:36.430233 csc_zta_agent[0x00000c90/config_service, 0x0000343c] I/ ConfigSync.cpp:309 ConfigSync::HandleRequestComplete() **recibió nueva configuración:**

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

["192.168.52.2"],"retry_interval":300}],"proxy_configs":[{**"condition_actions":[{"action":"disconnect"**,"check_type":"on_network","match_network_fingerprin
7618-44cd-852d-6ae1674e3cac"]} ,{"action":"connect"}],"id":"default_spa_config","label":"Secure Private Access","match_resource_configs":["spa_direction_config"],"proxy_server":"spa_proxy_server"},{"condition_actions":[{"action":"disconnect","check_type":"on_n

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() estado de la huella digital de la red de radiodifusión: **Huella digital**: **28f629ee-7618-44cd-852d-6ae1674e3cac Interfaces: Ethernet0**

Desconexión de TND en una condición DNS

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:378 ActiveSteeringPolicy::UpdateActiveProxyConfigs() actualizar la configuración de proxy activo

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:287 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND desconectará ProxyConfig "Secure Internet Access" debido a la condición: on_network: **28f629ee-7618-44cd-852d-6ae1674e3cac action=Desconectar**

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Private Access' se está desconectando debido a: InactiveTnd

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Internet Access' se está desconectando debido a: InactiveTnd

Tipo de regla de coincidencia DNS

2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main, 0x0000343c] I/ ZtnaTransportManager.cpp:1251 ZtnaTransportManager::closeObsoleteAppFlows() fuerza el cierre del flujo de la aplicación debido a una configuración ProxyConfig obsoleta enrollmentId=7b35249c-64e1-4f55-b12b-58875a806969 proxyConfigId=default_tia_config TCP destination [safebrowsing.googleapis.com]:443 srcPort=61049 realDestIpAddr=172.253.122.95 process=<chrome.exe|PID 11904|user amita\amita> parentProcess=<chromeID>|**amita_user**

Información Relacionada

- Soporte técnico y descargas de Cisco
- Centro de ayuda de Cisco Secure Access
- Guía de diseño de Cisco SASE

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).