Configuration de l'accès réseau sans confiance avec la détection de réseau sécurisé

Table des matières

Introduction

Ce document décrit les étapes requises pour configurer la détection de réseau sécurisé ZTNA.

Conditions préalables

- Client sécurisé version 5.1.10 minimum
- Plate-forme prise en charge - Windows et MacOS
- Module de plateforme sécurisée (TPM) pour Windows
- Coprocesseur Secure Enclave pour appareils Apple
- Les 'Serveurs approuvés' configurés dans un profil de réseau approuvé sont implicitement exclus de l'interception ZTA. Ces serveurs ne peuvent pas non plus être des accès en tant que ressources privées ZTA.
- La configuration TND affecte tous les clients inscrits dans l'organisation
- Les administrateurs peuvent utiliser les étapes suivantes pour générer un « hachage de clé publique de certificat » pour les serveurs approuvés
  - Télécharger le certificat public des serveurs approuvés
  - Exécutez cette commande shell pour generate the hash:

```
openssl x509 -in
```

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

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé Cisco
- Inscrivez les périphériques dans Zero Trust Access à l'aide de SAML ou de l'authentification basée sur certificat.

Composants utilisés

- Client sécurisé version 5.1.13
- TPM
- Locataire d'accès sécurisé
- Périphérique Windows

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

- TND permet aux administrateurs de configurer le client sécurisé pour suspendre temporairement la direction et l'application du trafic ZTA sur les réseaux sécurisés.
- Le client sécurisé reprend l'application ZTA lorsque le point d'extrémité quitte le réseau approuvé.
- Cette fonctionnalité ne nécessite aucune interaction de l'utilisateur final.
- Les configurations ZTA TND peuvent être gérées indépendamment pour les destinations ZTA privées et Internet.

Principaux avantages

- Des performances réseau améliorées et une latence réduite offrent une expérience utilisateur plus fluide.
- L'application de la sécurité locale dans le réseau sécurisé offre une utilisation flexible et

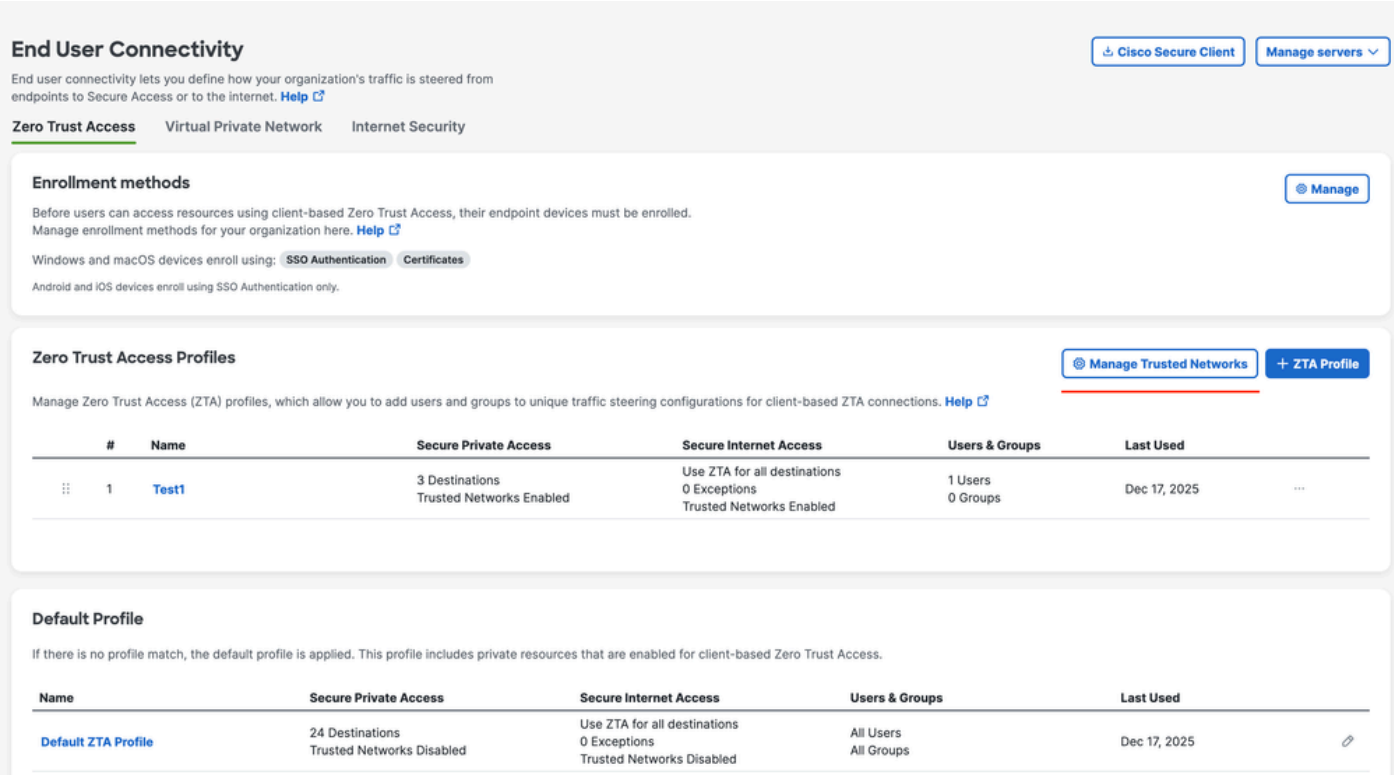
optimisée des ressources.
- Les utilisateurs finaux peuvent tirer parti de ces avantages sans aucune invite ni action.
- Le contrôle indépendant de TND pour l'accès privé et l'accès à Internet offre aux administrateurs la flexibilité nécessaire pour gérer les différents problèmes opérationnels et de sécurité

Configurer

Étape 1 : Créer un profil réseau approuvé - Serveur DNS et domaine

Accédez à Secure Access Dashboard :

- Cliquez sur Connect > End User Connectivity > Manage Trusted Networks > +Add



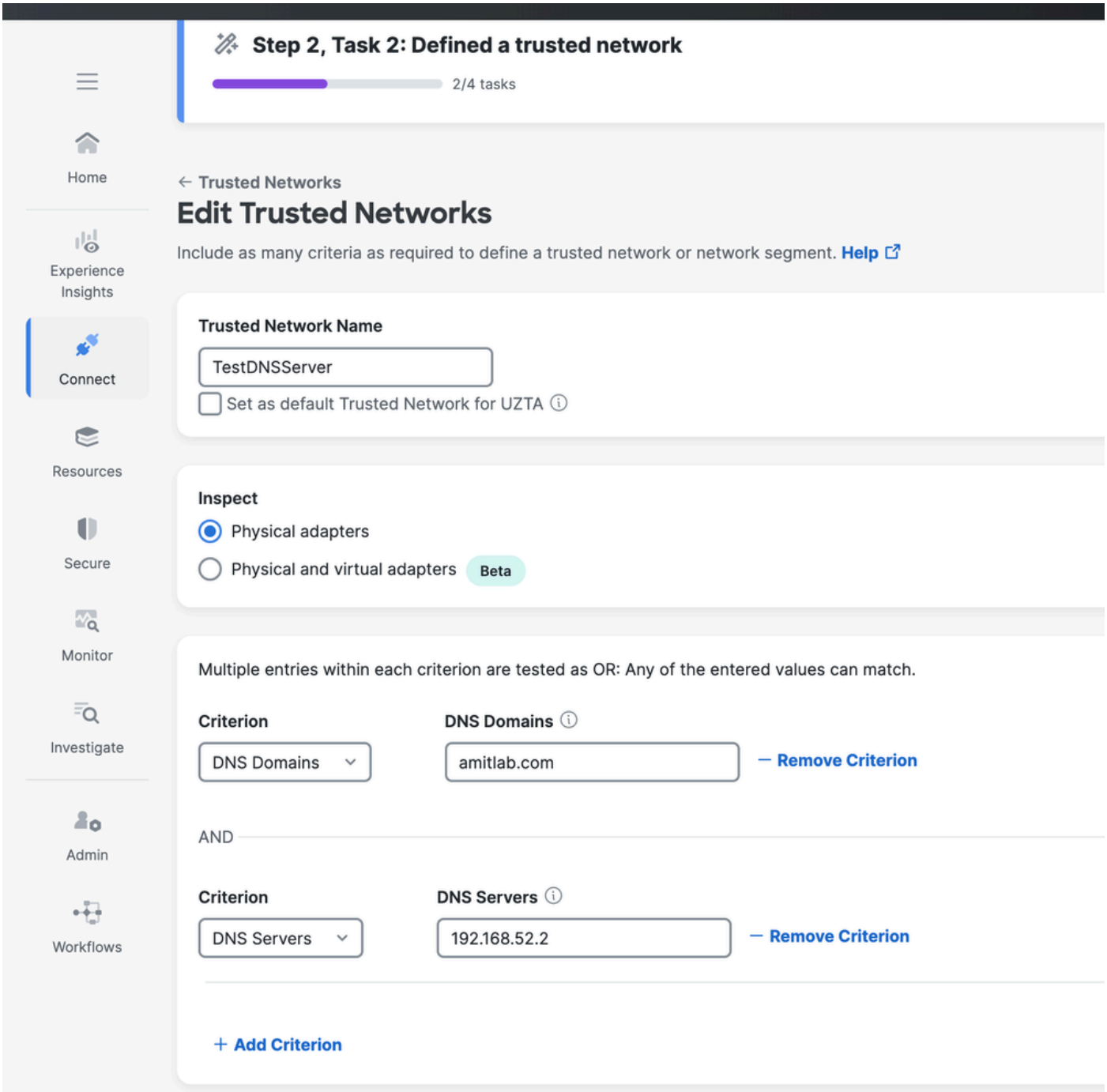
- Attribuez un nom au profil de réseau approuvé et configurez au moins l'un des critères suivants :
  - DNS Servers - Valeurs séparées par des virgules de toutes les adresses de serveur DNS qu'une interface réseau doit avoir lorsque le client se trouve dans un réseau approuvé. Tout serveur saisi peut être utilisé pour correspondre à ce profil. Pour que TND corresponde, l'une des adresses du serveur DNS doit correspondre à l'interface locale.
  - DNS Domains - Valeurs séparées par des virgules des suffixes DNS qu'une interface réseau doit avoir lorsque le client se trouve dans un réseau approuvé.
  - Trusted Server- Ajoutez un ou plusieurs serveurs sur le réseau qui présentent un certificat TLS avec un hachage qui correspond au hachage que vous fournissez. Pour spécifier un port autre que 443, ajoutez le port en notation standard. Vous pouvez ajouter

jusqu'à 10 serveurs approuvés, dont un seul doit passer la validation.

- Certificate Public Key Hash: Vérifiez les conditions préalables et les limites système pour savoir comment générer le hachage de certificat.

Répétez les étapes pour ajouter d'autres profils de réseau sécurisé.

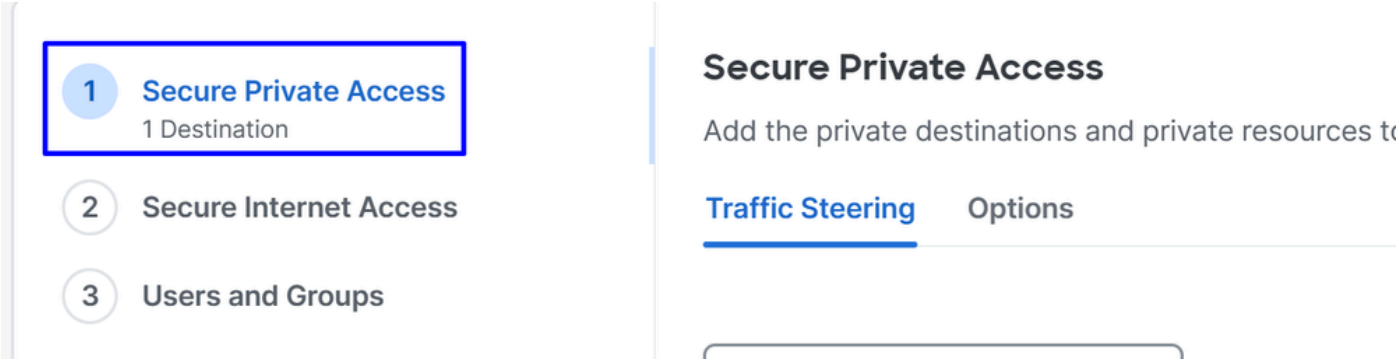
Remarque : Plusieurs options dans le même critère est un opérateur OU. Different Criteria Defined est un opérateur AND.



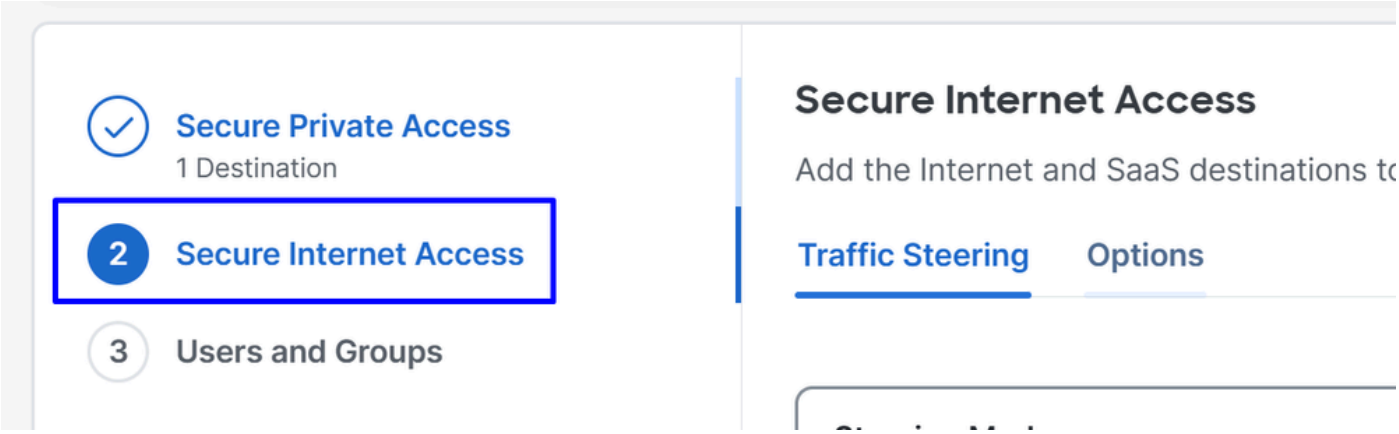
Étape 2 : Activer TND pour l'accès privé ou Internet

- Accédez à Connect > End User Connectivity
- Modifier le profil ZTA
- PourSecure Private DestinationsOU Secure Internet Access

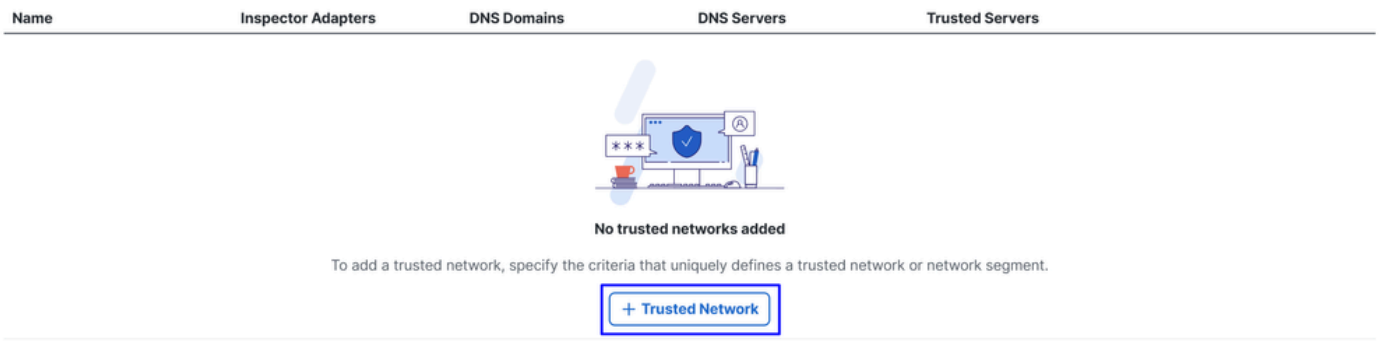
Accès privé sécurisé



Accès Internet sécurisé



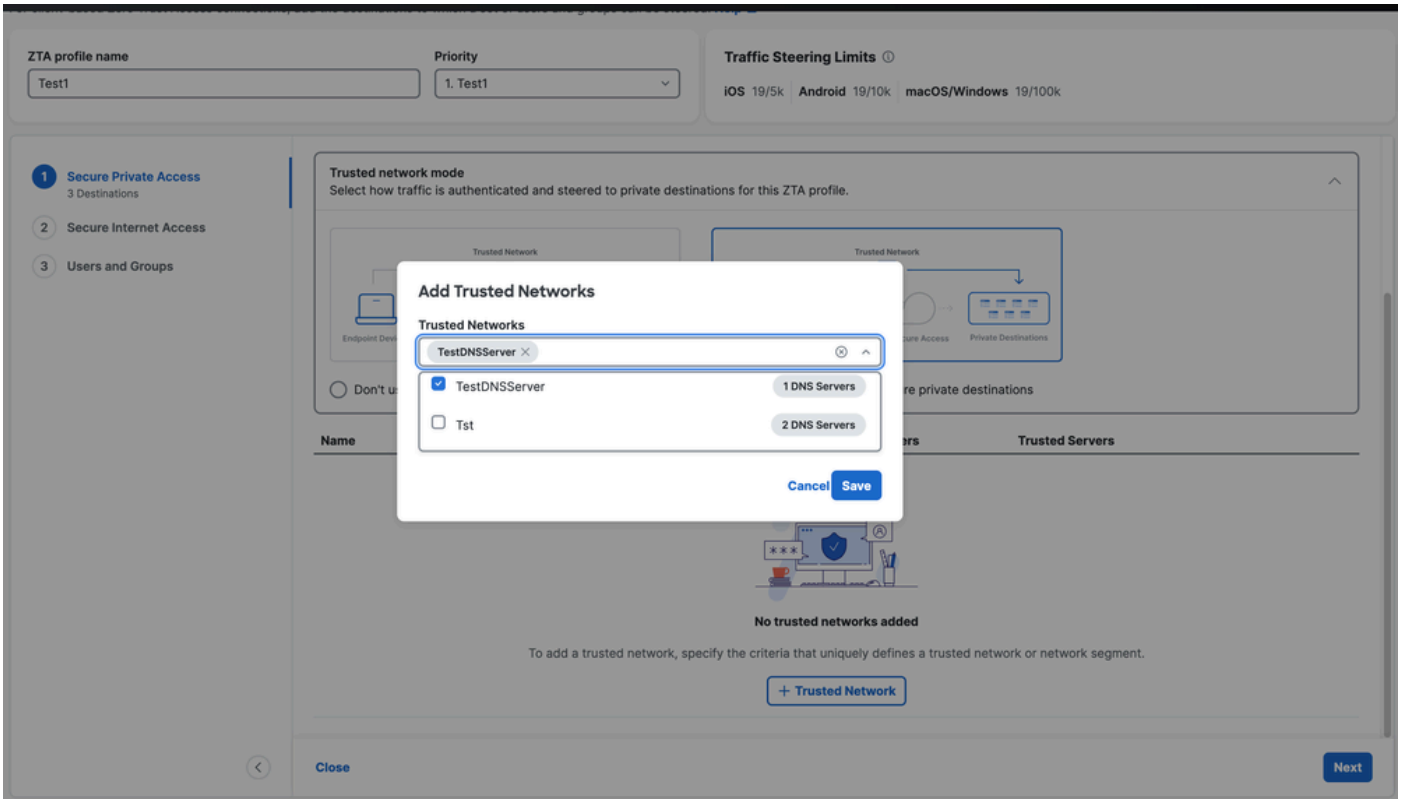
- Cliquez sur Options
  - Cliquez sur Use trusted networks to secure private destinations OU Use trusted networks to secure internet destinationsdépend de l'option choisie avant
  - Cliquez sur + Trusted Network



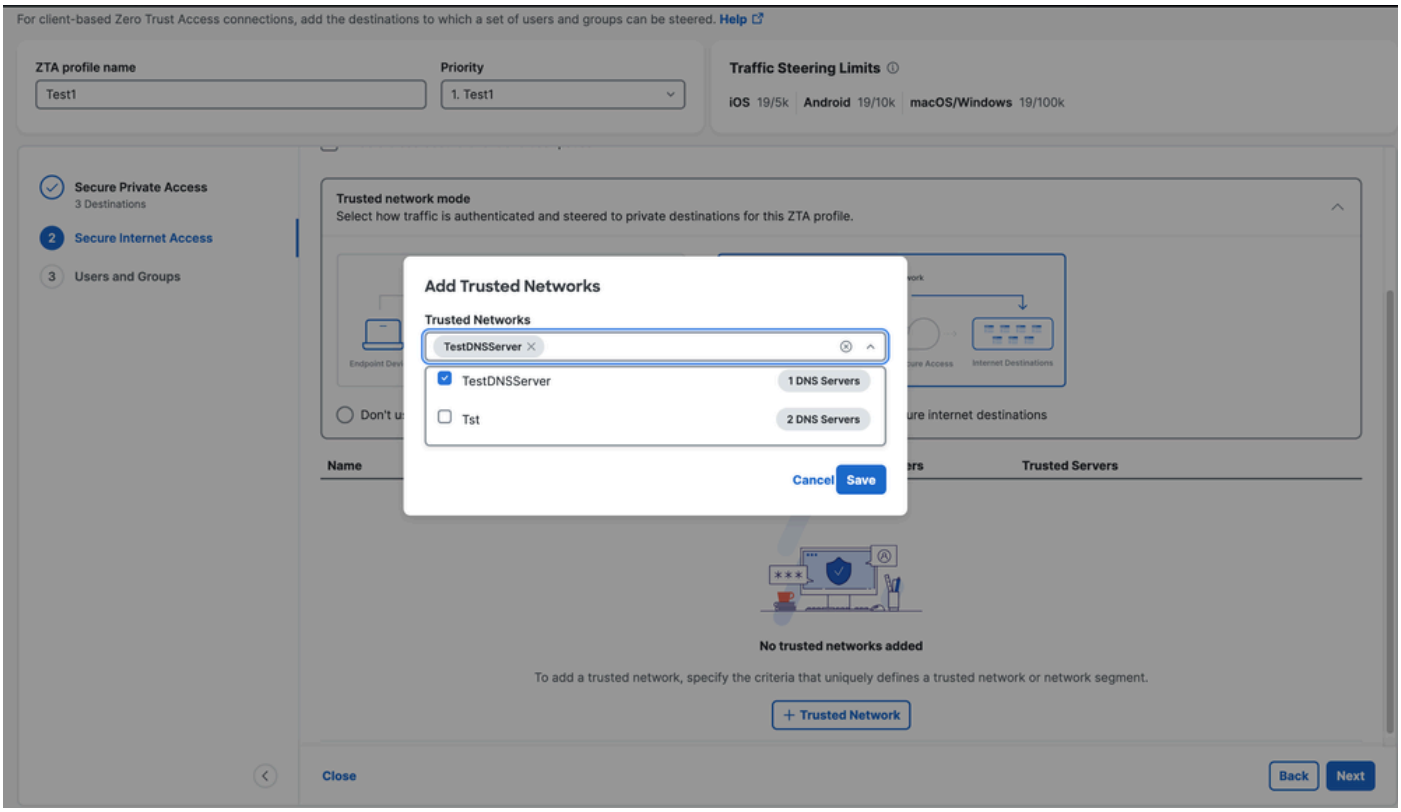
- Sélectionnez le ou les profils de réseau sécurisé que vous avez configurés à la page

précédente, puis cliquez sur Save

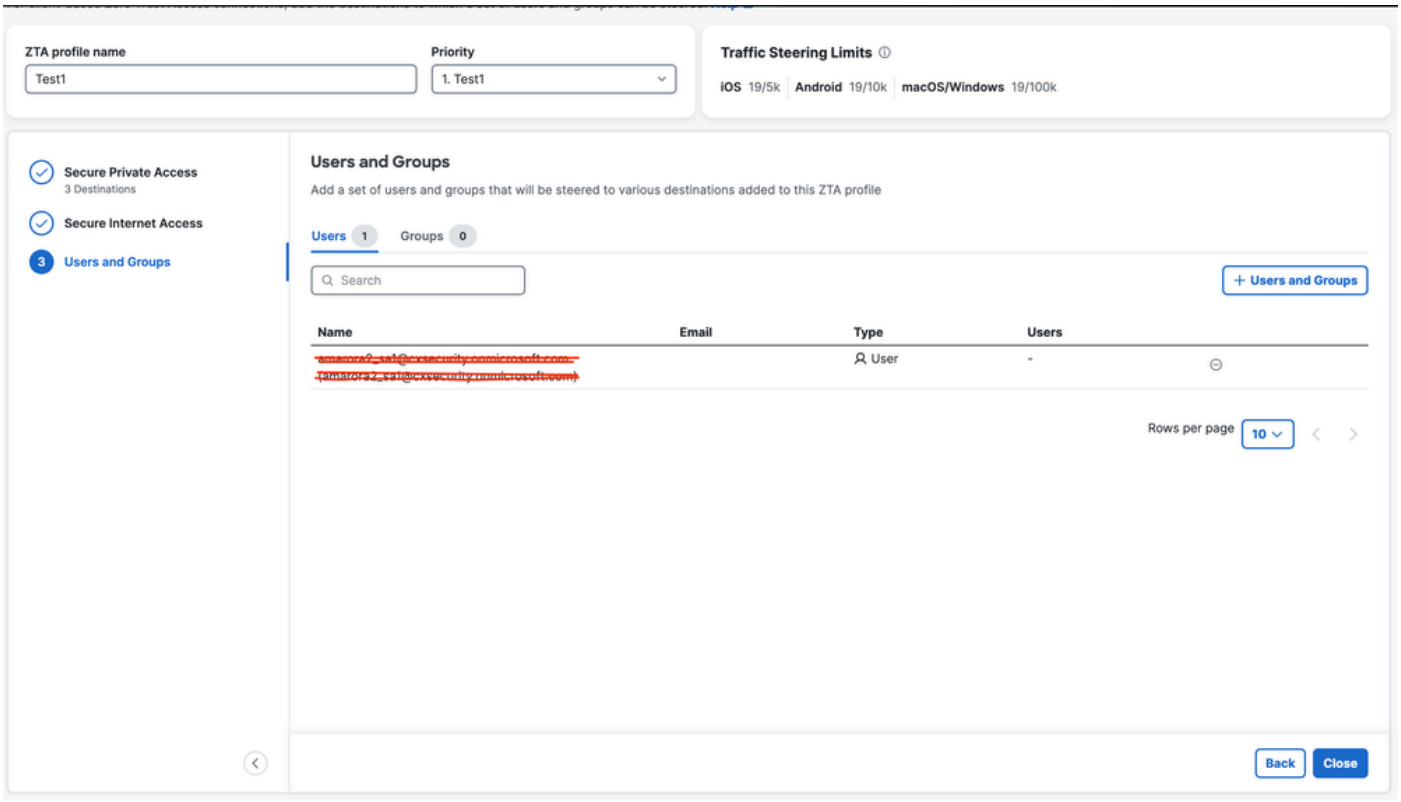
Accès privé sécurisé



Accès Internet sécurisé



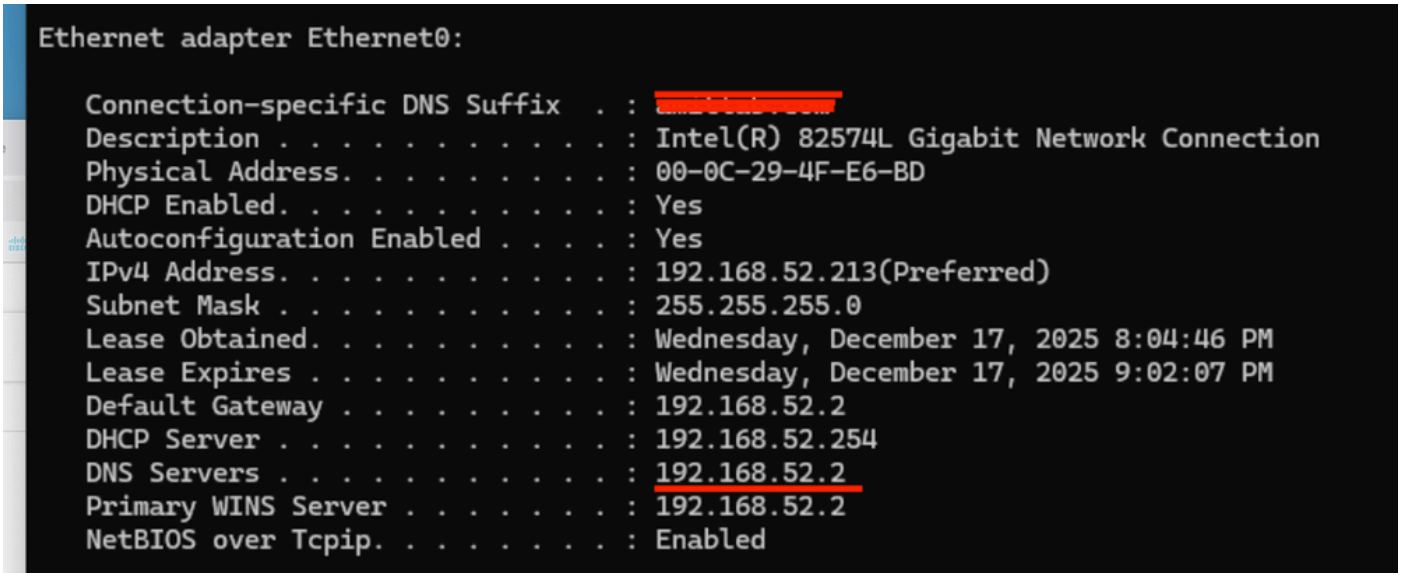
- Attribuez le Users/Groups au profil ZTA et cliquez sur Close.



Étape 3 : Configuration côté client

1. Assurez-vous que vous disposez du bon serveur DNS défini sous Adaptateur Ethernet, car nous avons choisi Adaptateur physique comme critère

2. Assurez-vous que le suffixe DNS spécifique à la connexion est défini.

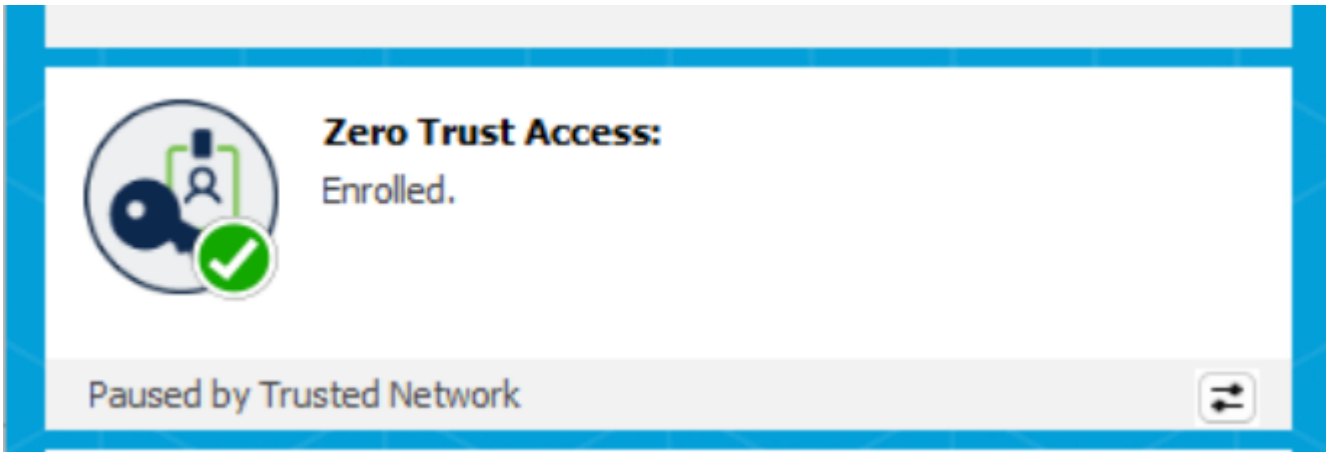


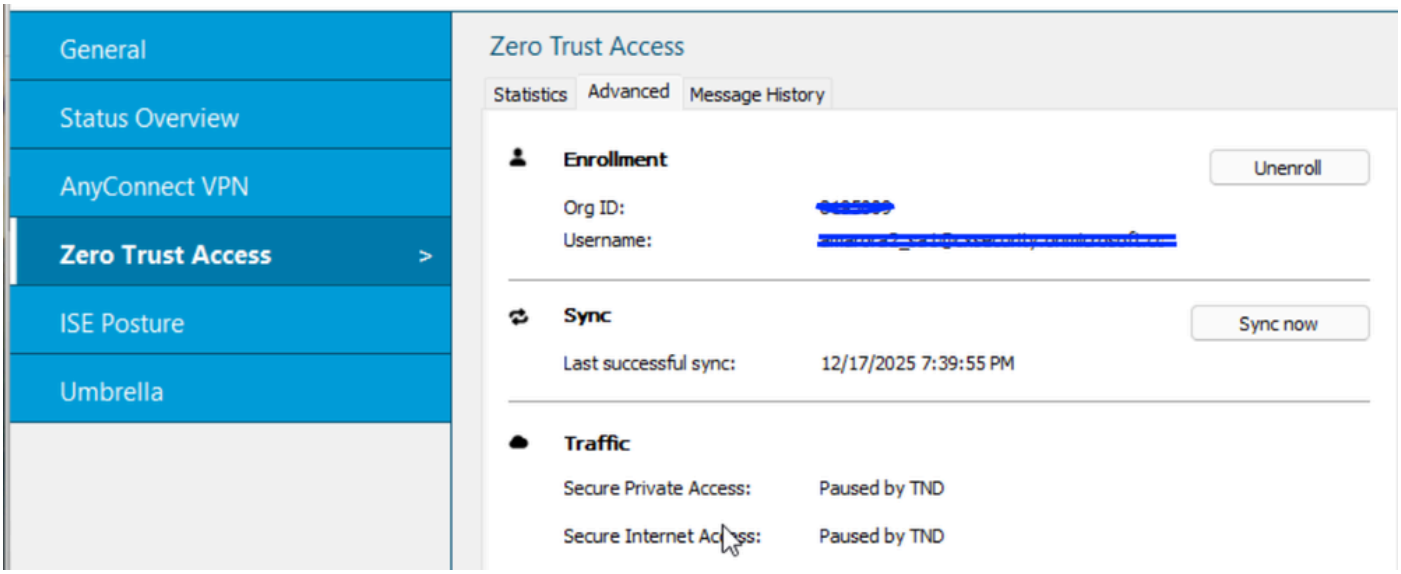
Lors de la prochaine synchronisation de la configuration ZTA avec le client sécurisé dans quelques minutes, le module ZTA s'interrompt automatiquement lorsqu'il détecte qu'il se trouve

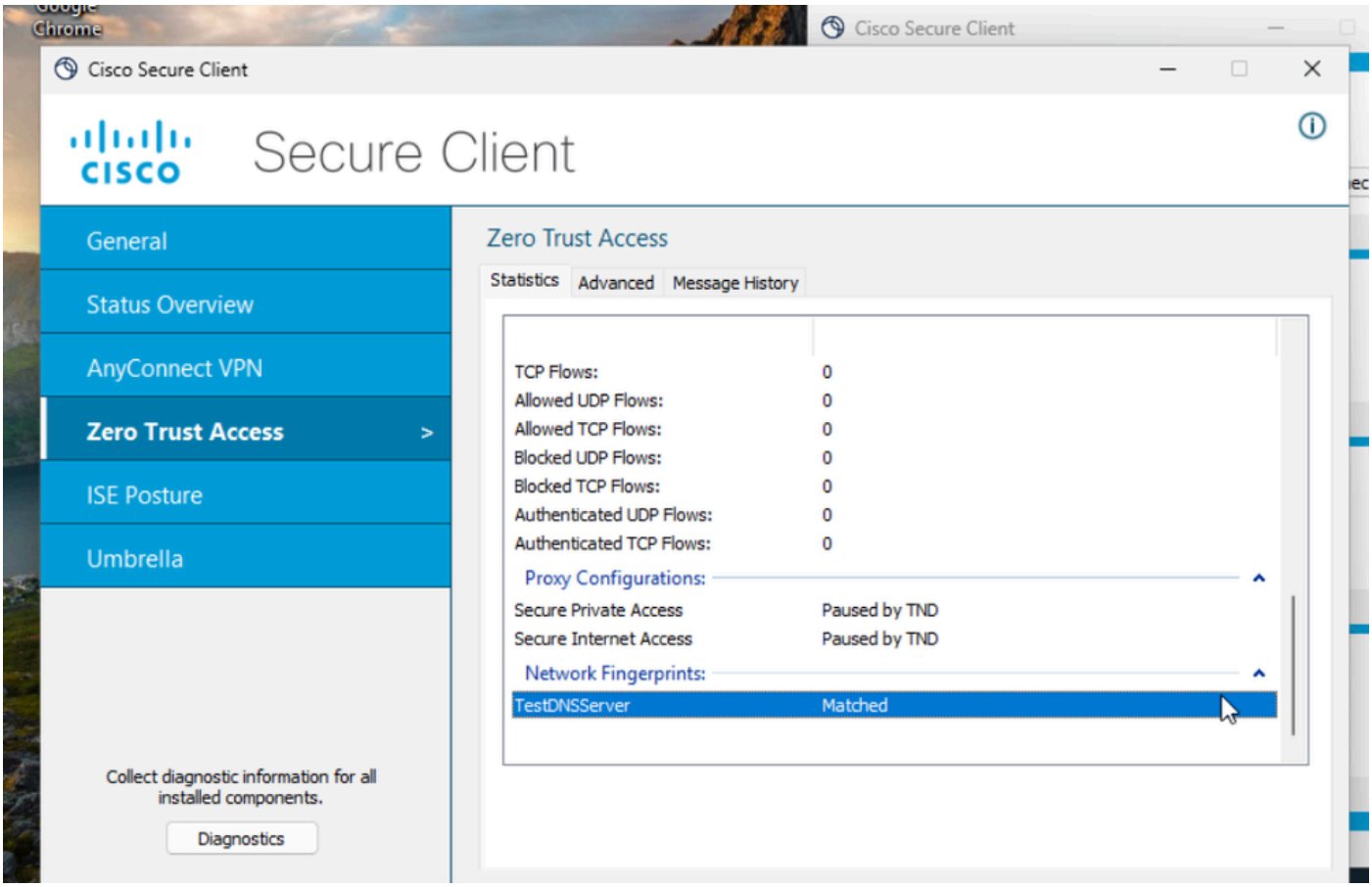
sur l'un des réseaux sécurisés configurés.

Vérifier

- À partir du client sécurisé







- De l'offre groupée DART - Journaux ZTA

Aucune règle TND configurée.

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcement, 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND va connecter ProxyConfig 'default_spa_config' (pas de règles)

2025-12-17 17:53:40.711938 csc_tia_agent[0x0000206c/config_enforcement, 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND va connecter ProxyConfig 'default_tia_config' (pas de règles)

Règle TND configurée - Serveur DNS - Configuration reçue par le client

25-12-17 20:33:15.987956 csc_zta_agent[0x00000f80, 0x00000ed4] Avec CaptivePortalDetectionService.cpp:308 CaptivePortalDetectionService::getProbeUrl() pas de dernier snapshot réseau, utilisation de la première URL de sonde

2025-12-17 20:33:15.992042 csc_zta_agent[0x00000f80, 0x00000ed4] I/ NetworkChangeService.cpp:144 NetworkChangeService::**Start() Instantané réseau initial :**
Ethernet0 : subnets=192.168.52.213/24 dns_servers=192.168.52.2 dns_domain=amitlab.com dns_suffixes=amitlab.com isPhysical=true default_gateway=192.168.52.2
captivePortalState=Inconnu

conditionnelle_actions":[{"action":"disconnect" indique que TND est configuré dans le profil ZTA.

2025-12-17 17:55:36.430233 csc_zta_agent[0x00000c90/config_service, 0x0000343c] I/ ConfigSync.cpp:309 ConfigSync::HandleRequestComplete() **a reçu une nouvelle configuration :**

{"ztnaConfig":{"global_settings":{"exclude_local_lan":true},**"network_fingerprints":[{"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":[{**"conditionnelle_actions":[{"action":"disconnect"**,"check_type":"on_network","match_network_finge
7618-44cd-852d-6ae1674e3cac"]},{"action": "connect"}],"id":"default_spa_config","label":"Secure Private Access","match_resource_configs":["spa_Steering_config"],"proxy_server":"spa_proxy_server"},{"conditionnel_actions":[{"action":"disconnect","check_type":"or

7618-44cd-852d-6ae1674e3cac"]},{"action":"connect"}],"id":

2025-12-17 17:55:36.472435 csc_zta_agent[0x000039a8/main, 0x0000343c] I/ NetworkFingerprintService.cpp:196 NetworkFingerprintService::handleStatusUpdate() diffusion de l'état des empreintes du réseau : **Empreinte digitale** : **28f629ee-7618-44cd-852d-6ae1674e3cac Interfaces : Ethernet0**

Déconnexion TND sur une condition DNS

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcement, 0x0000343c] I/ ActiveSteeringPolicy.cpp:378 ActiveSteeringPolicy::UpdateActiveProxyConfigs() mise à jour de la configuration du proxy actif

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcement, 0x0000343c] I/ ActiveSteeringPolicy.cpp:287 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND va déconnecter ProxyConfig "Secure Internet Access" en raison de la condition suivante : sur_réseau : **28f629ee-7618-44cd-852d-6ae1674e3cac action=Déconnecter**

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig « Accès privé sécurisé » se déconnecte en raison de : TndInactif

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Accès Internet sécurisé' se déconnecte en raison de : TndInactif

Correspondance du type de règle DNS

2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main, 0x0000343c] I/ ZtnaTransportManager.cpp:1251 ZtnaTransportManager::closeObsoleteAppFlows() force la fermeture du flux d'applications en raison de l'ID d'inscription ProxyConfig obsolète=7b35249c-64e1-4f55-b12b-58875a806969 proxyConfigId=default_tia_config Destination TCP [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**

Informations connexes

- Assistance technique de Cisco et téléchargements
- Centre d'aide Cisco Secure Access
- Guide de conception Cisco SASE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.