

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Étape 1 : Créer un profil réseau approuvé - Serveur DNS et domaine](#)

[Étape 2 : EnableTND pour l'accès privé ou Internet](#)

[Étape 3 : Configuration côté client](#)

[Vérifier](#)

[À partir du client sécurisé](#)

[Offre groupée DART - Journaux ZTA](#)

[Informations connexes](#)

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.

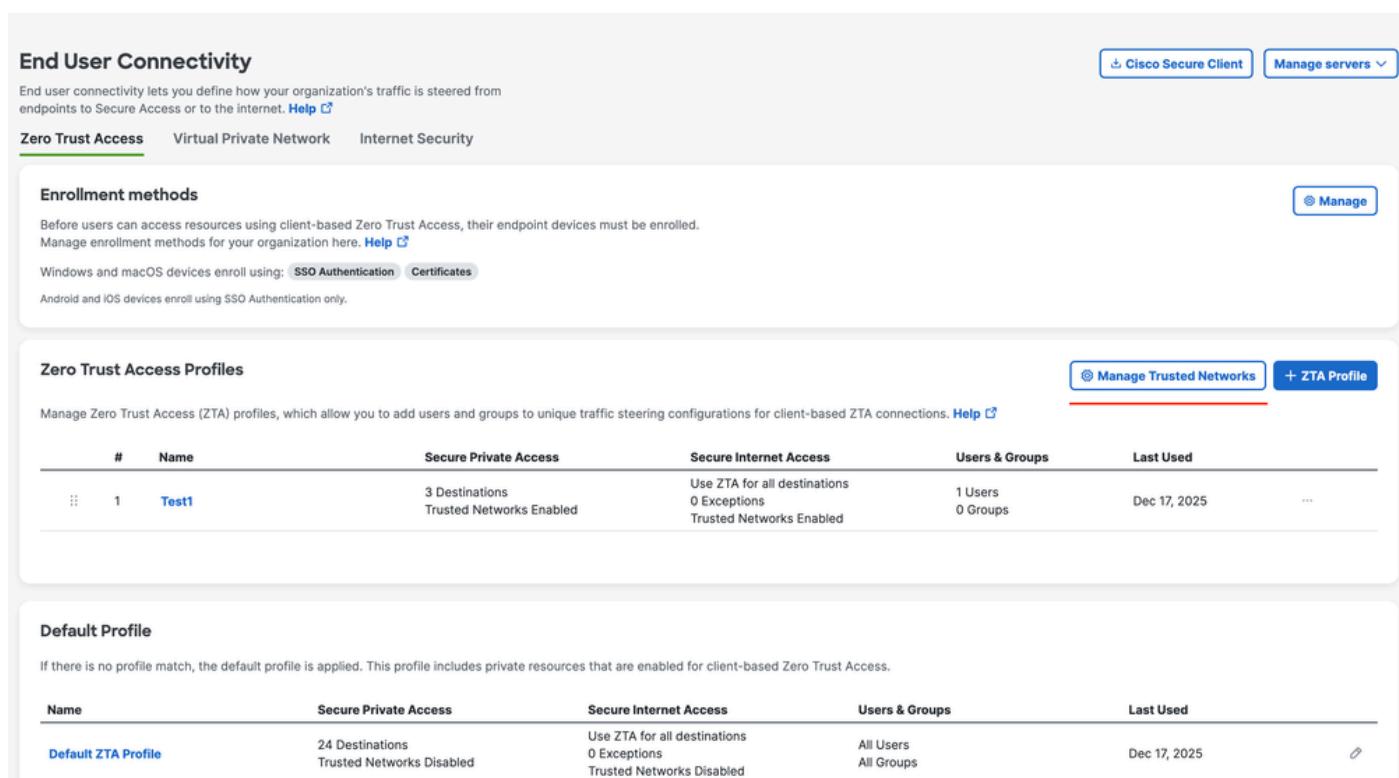
- Les utilisateurs finaux peuvent tirer parti de ces avantages sans aucune invite ni action.
- Le contrôle indépendant de TND pour l'accès privé et l'accès à Internet offre aux administrateurs la flexibilité nécessaire pour gérer les différents problèmes opérationnels et de sécurité

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



#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	Test1	3 Destinations Trusted Networks Enabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Enabled	1 Users 0 Groups	Dec 17, 2025

Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
Default ZTA Profile	24 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	All Users All Groups	Dec 17, 2025

- 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.

Step 2, Task 2: Defined a trusted network
2/4 tasks

← Trusted Networks

Edit Trusted Networks

Include as many criteria as required to define a trusted network or network segment. [Help](#)

Trusted Network Name

TestDNSServer

Set as default Trusted Network for UZTA

Inspect

Physical adapters

Physical and virtual adapters Beta

Multiple entries within each criterion are tested as OR: Any of the entered values can match.

Criterion	DNS Domains i	Remove Criterion
DNS Domains	amitlab.com	Remove Criterion

AND

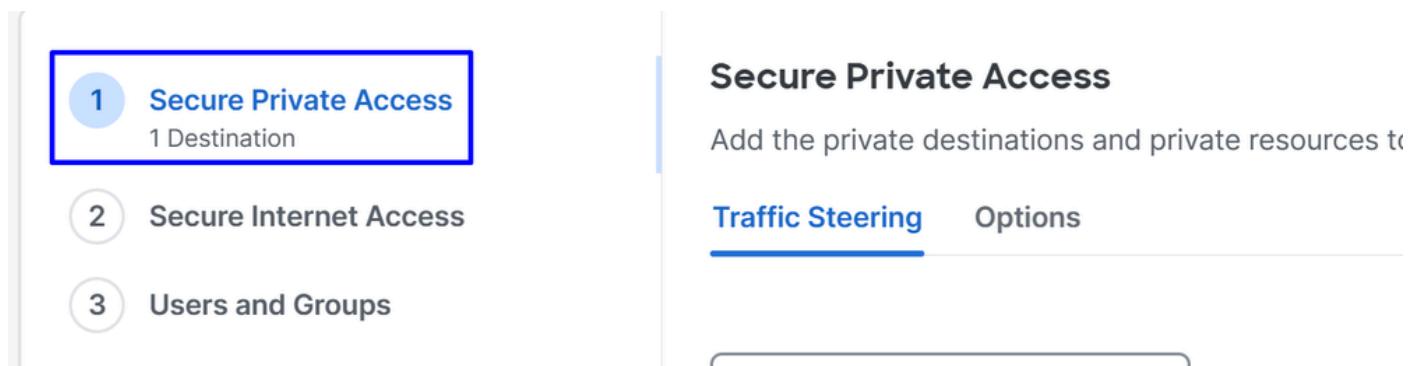
Criterion	DNS Servers i	Remove Criterion
DNS Servers	192.168.52.2	Remove Criterion

[+ Add Criterion](#)

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

- Accédez à Connect > End User Connectivity
- Modifier le profil ZTA
- Pour Secure Private Destinations OU Secure Internet Access

Accès privé sécurisé



Secure Private Access

Add the private destinations and private resources to be secured.

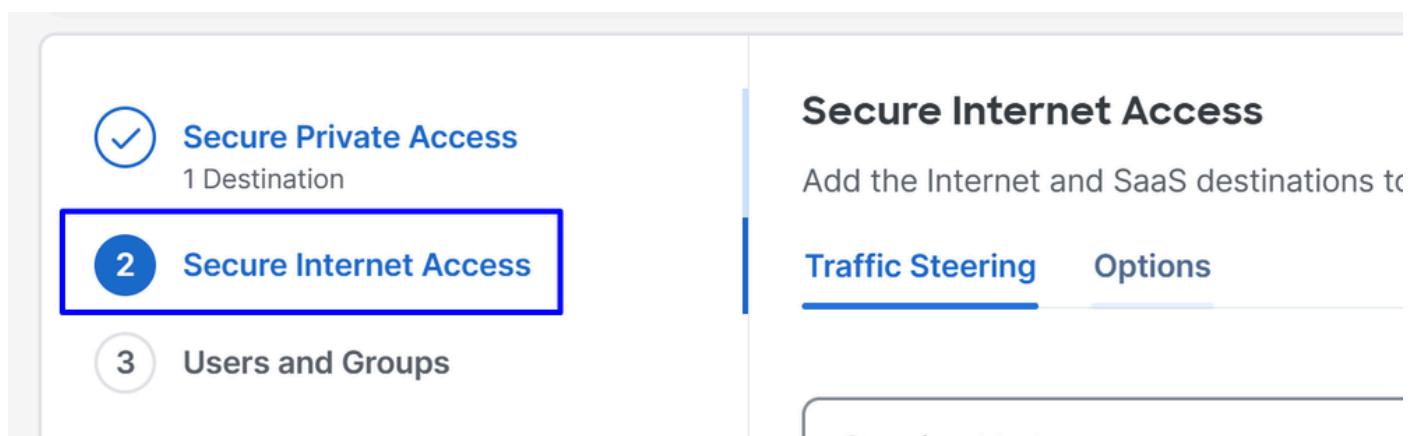
Traffic Steering **Options**

1 Secure Private Access
1 Destination

2 Secure Internet Access

3 Users and Groups

Accès Internet sécurisé



Secure Internet Access

Add the Internet and SaaS destinations to be secured.

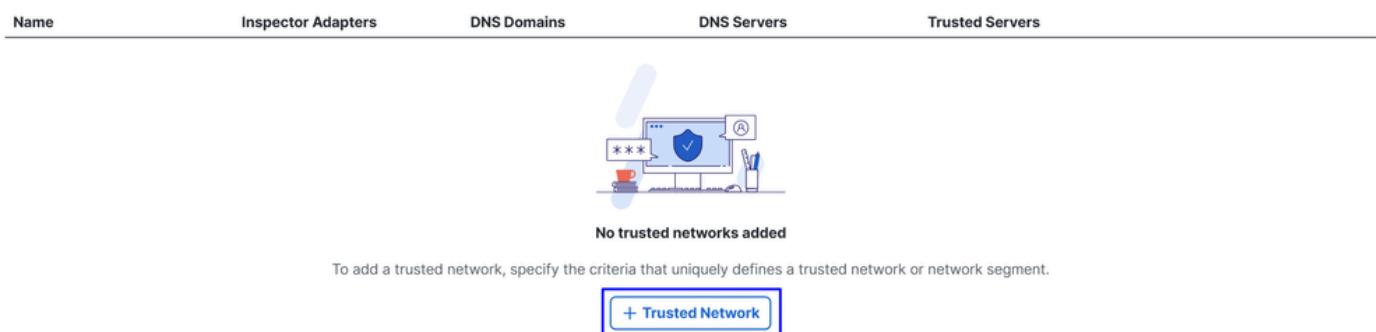
Traffic Steering **Options**

Secure Private Access
1 Destination

2 Secure Internet Access

3 Users and Groups

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



Name	Inspector Adapters	DNS Domains	DNS Servers	Trusted Servers

No trusted networks added

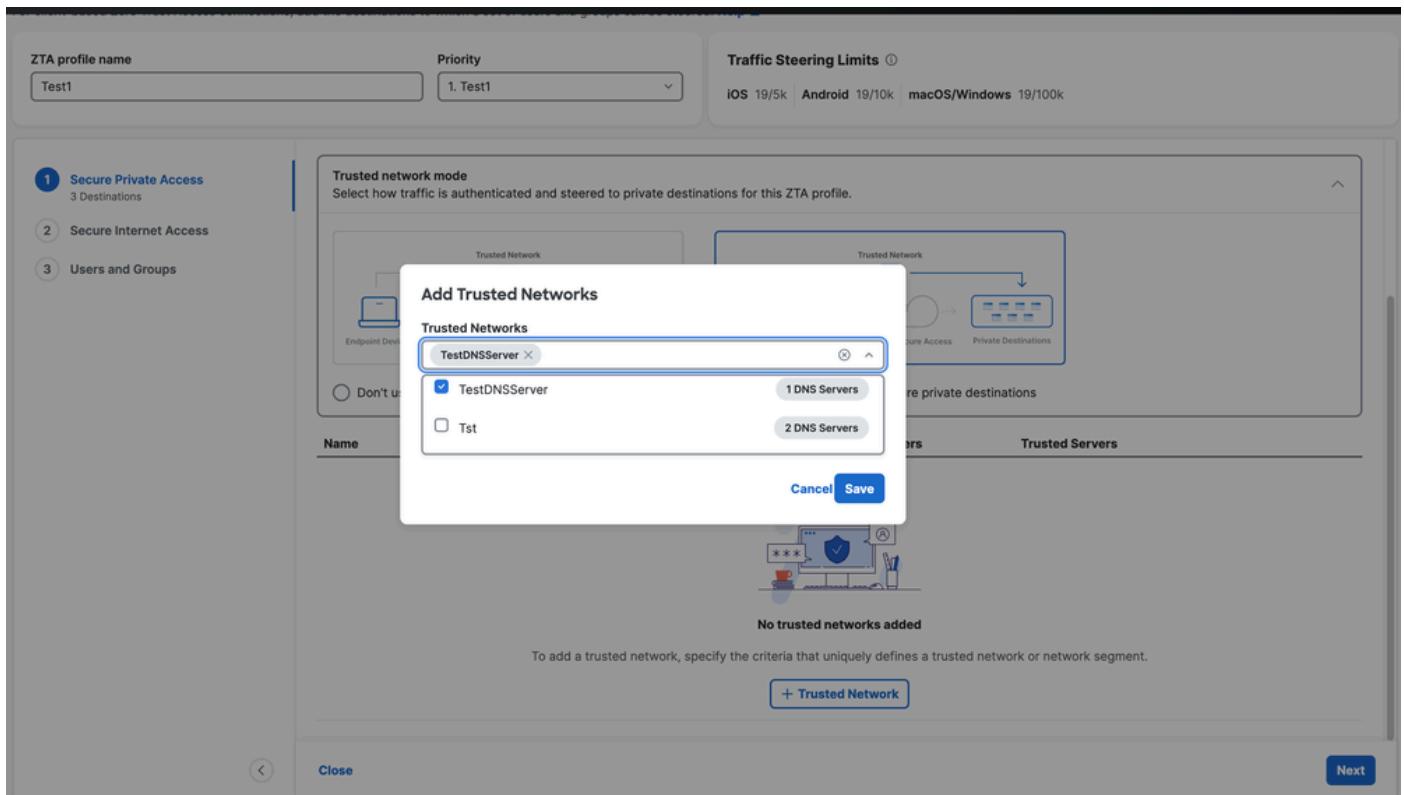
To add a trusted network, specify the criteria that uniquely defines a trusted network or network segment.

+ Trusted Network

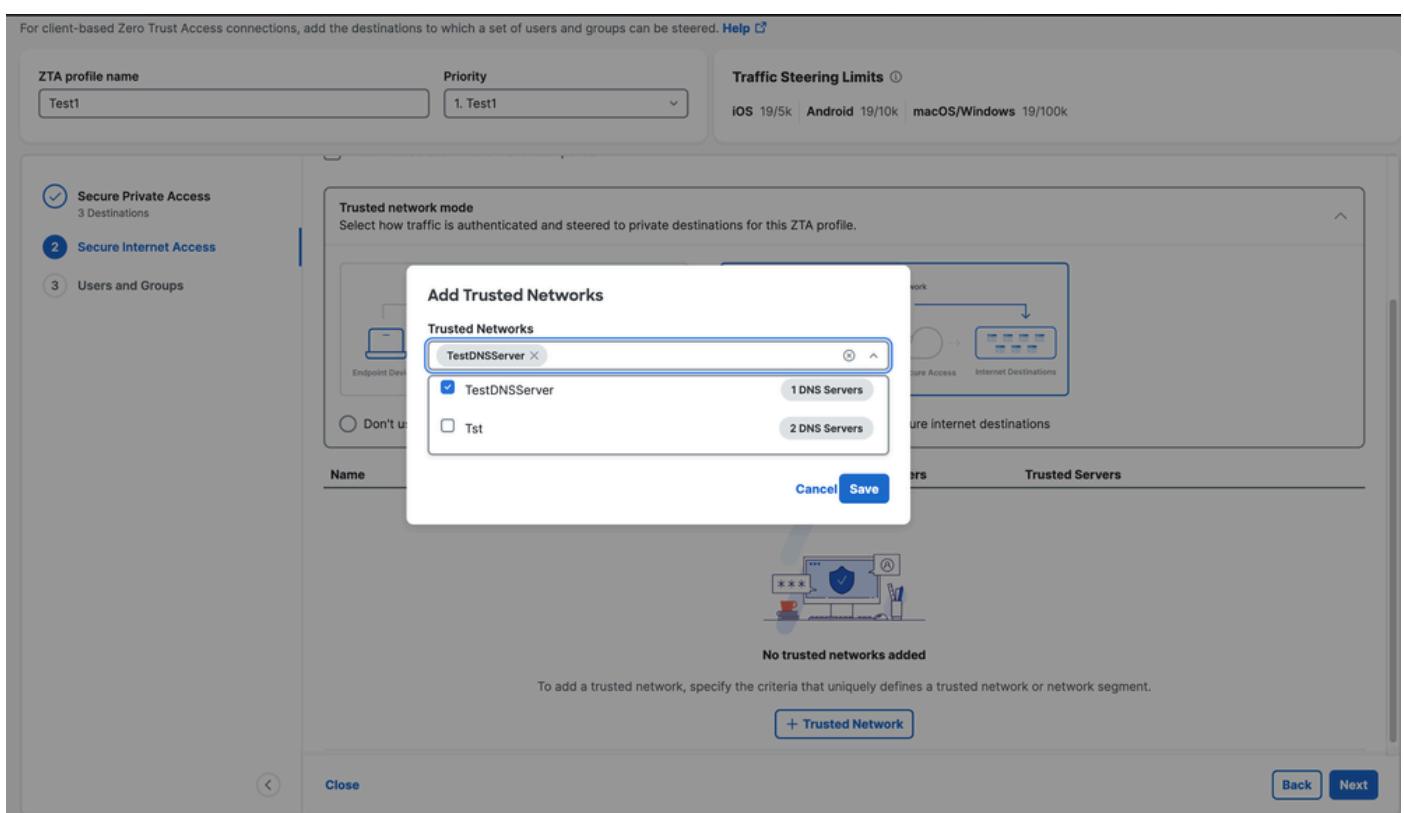
- Sélectionnez le ou les profils de réseau sécurisé que vous avez configurés à la page

précédente, puis cliquez sur Save

Accès privé sécurisé



Accès Internet sécurisé



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

The screenshot shows the ZTA profile configuration interface. At the top, there are fields for 'ZTA profile name' (Test1) and 'Priority' (1. Test1). Below this is a 'Traffic Steering Limits' section with options for iOS 19/5k, Android 19/10k, and macOS/Windows 19/100k. On the left, a sidebar shows 'Secure Private Access' (3 Destinations), 'Secure Internet Access', and a selected 'Users and Groups' item. The main content area is titled 'Users and Groups' and contains a table with one user entry. The table columns are Name, Email, Type, and Users. The user listed is 'testuser2-sec@secURITY.onmicrosoft.com' (Type: User). Below the table are buttons for 'Rows per page' (10), 'Back', and 'Close'.

Étape 3 : Configuration côté client

- Assurez-vous que vous disposez du bon serveur DNS défini sous Adaptateur Ethernet, car nous avons choisi Adaptateur physique comme critère
- Assurez-vous que le suffixe DNS spécifique à la connexion est défini.

```
Ethernet adapter Ethernet0:

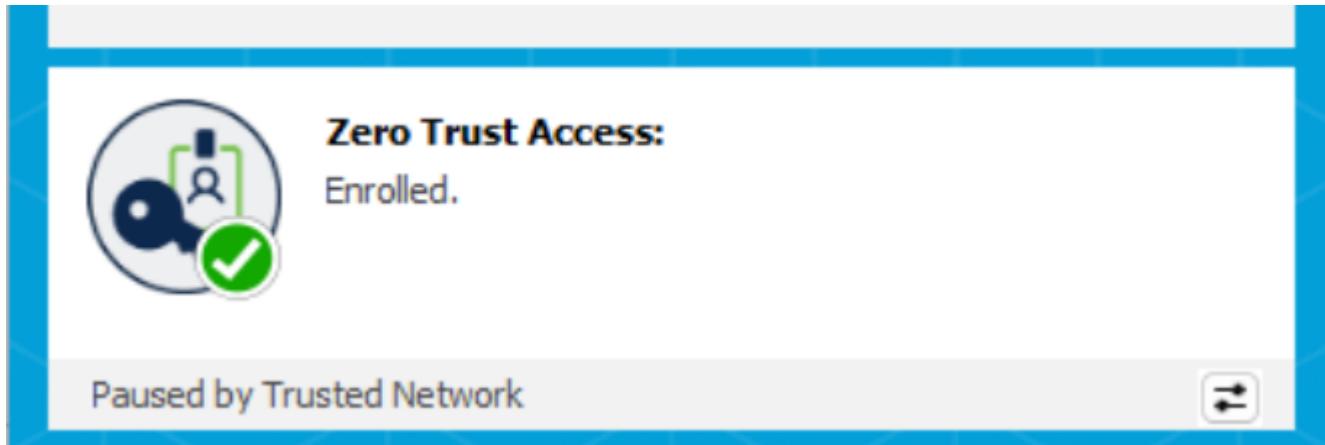
Connection-specific DNS Suffix . . . . . : [REDACTED]
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-4F-E6-BD
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.52.213(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, December 17, 2025 8:04:46 PM
Lease Expires . . . . . : Wednesday, December 17, 2025 9:02:07 PM
Default Gateway . . . . . : 192.168.52.2
DHCP Server . . . . . : 192.168.52.254
DNS Servers . . . . . : 192.168.52.2
Primary WINS Server . . . . . : 192.168.52.2
NetBIOS over Tcpip. . . . . : Enabled
```

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

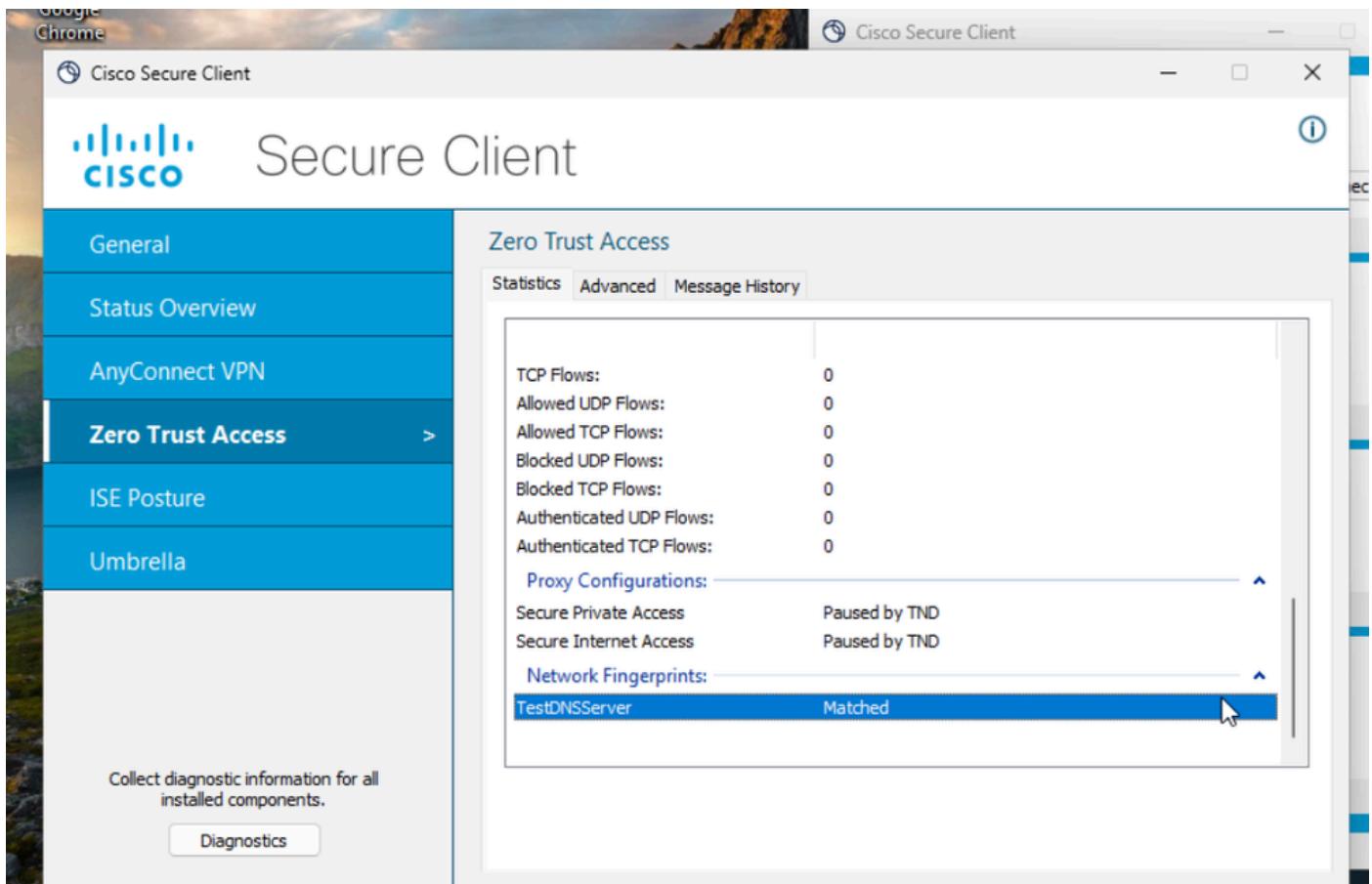
sur l'un des réseaux sécurisés configurés.

Vérifier

- À partir du client sécurisé



The screenshot shows a web-based management interface for Zero Trust Access. On the left, a sidebar menu lists several options: General, Status Overview, AnyConnect VPN, Zero Trust Access (which is currently selected and highlighted in blue), ISE Posture, and Umbrella. The main content area is titled "Zero Trust Access" and contains three tabs: Statistics, Advanced, and Message History. The "Advanced" tab is selected. The page is divided into sections: "Enrollment" (Org ID: [REDACTED], Username: [REDACTED], Unenroll button), "Sync" (Last successful sync: 12/17/2025 7:39:55 PM, Sync now button), and "Traffic" (Secure Private Access: Paused by TND, Secure Internet Access: Paused by TND).



- 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"]}], "proxy_configs": [{"conditionnelle_actions": [{"action": "disconnect", "check_type": "on_network", "match_network_fingerprints": ["7618-44cd-852d-6ae1674e3cac"]}], "action": "connect", "id": "default_spa_config", "label": "Secure Private Access", "match_resource_configs": [{"spa_Steering_config": "spa_Proxy_Server", "proxy_server": "spa_Proxy_Server"}]}], "conditionnel_actions": [{"action": "disconnect", "check_type": "on_network", "match_network_fingerprints": ["7618-44cd-852d-6ae1674e3cac"]}], "action": "connect", "id": "default_spa_config", "label": "Secure Private Access", "match_resource_configs": [{"spa_Steering_config": "spa_Proxy_Server", "proxy_server": "spa_Proxy_Server"}]}]

["192.168.52.2"], "retry_interval": 300}], "proxy_configs": [{"conditionnelle_actions": [{"action": "disconnect", "check_type": "on_network", "match_network_fingerprints": ["7618-44cd-852d-6ae1674e3cac"]}], "action": "connect", "id": "default_spa_config", "label": "Secure Private Access", "match_resource_configs": [{"spa_Steering_config": "spa_Proxy_Server", "proxy_server": "spa_Proxy_Server"}]}], "conditionnel_actions": [{"action": "disconnect", "check_type": "on_network", "match_network_fingerprints": ["7618-44cd-852d-6ae1674e3cac"]}], "action": "connect", "id": "default_spa_config", "label": "Secure Private Access", "match_resource_configs": [{"spa_Steering_config": "spa_Proxy_Server", "proxy_server": "spa_Proxy_Server"}]}]

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

2025-12-17 17:55:36.472435 csc_zta_agent[0x000039a8/main, 0x0000343c] l/ 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] l/ 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] l/ 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] l/ 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] l/ 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] l/ 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.