

# Configurar o acesso à rede com confiança zero com detecção de rede confiável

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Passo 1: Criar perfil de rede confiável - Servidor DNS e domínio](#)

[Passo 2: EnableTND para acesso privado ou à Internet](#)

[Passo 3: Configuração do lado do cliente](#)

[Verificar](#)

[Do cliente seguro](#)

[Do pacote DART - registros ZTA](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve as etapas necessárias para configurar o ZTNA Trusted Network Detection.

## Pré-requisitos

- Versão mínima do Secure Client 5.1.10
- Plataforma com suporte - Windows e MacOS
- Trusted Platform Module (TPM) para Windows
- Co-processador Secure Enclave para dispositivos Apple
- Os 'Servidores Confiáveis' configurados em qualquer perfil de Rede Confiável são implicitamente excluídos da interceptação ZTA. Esses servidores também não podem ser acessados como recursos privados ZTA.
- A configuração TND afeta todos os clientes inscritos na organização
- Os administradores podem usar as próximas etapas para gerar um 'Hash de chave pública de certificado' para servidores confiáveis
  - Baixar o certificado público de servidores confiáveis
  - Execute este comando shell para generate the hash:

```
openssl x509 -in
```

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

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro da Cisco
- Inscreva dispositivos no Zero Trust Access usando SAML ou autenticação baseada em certificado.

## Componentes Utilizados

- Secure Client Versão 5.1.13
- TPM
- Locatário de acesso seguro
- Dispositivo Windows

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

- A TND permite que os administradores configurem o Secure Client para pausar temporariamente a direção e a aplicação do tráfego ZTA em redes confiáveis.
- O Secure Client retoma a aplicação de ZTA quando o endpoint sai da rede confiável.
- Esse recurso não requer interação com o usuário final.
- As configurações ZTA TND podem ser gerenciadas de forma independente para destinos ZTA privados e de Internet.



## Principais benefícios

- O desempenho de rede aprimorado e a latência reduzida proporcionam uma experiência de

usuário mais tranquila.

- A aplicação de segurança local na rede confiável oferece utilização de recursos flexível e otimizada.
- Os usuários finais podem aproveitar os benefícios sem qualquer prompt ou ação.
- O controle independente da TND para acesso privado e acesso à Internet fornece flexibilidade administrativa para lidar com diferentes preocupações operacionais e de segurança

## Configurar

### Passo 1: Criar perfil de rede confiável - Servidor DNS e domínio

Navegue até [Secure Access Dashboard](#):

- Clique em Connect > End User Connectivity > Manage Trusted Networks > +Add

The screenshot shows the Cisco Secure Access Dashboard with the 'Manage Trusted Networks' page selected. The top navigation bar includes 'Cisco Secure Client' and 'Manage servers'. The main content area is divided into sections: 'Enrollment methods' (with a note about device enrollment and a 'Manage' button), 'Zero Trust Access Profiles' (with a table showing 'Test1' profile details), and 'Default Profile' (with a table showing the 'Default ZTA Profile' details). The 'Manage Trusted Networks' button is highlighted with a red box.

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

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

- Forneça um nome para o perfil de Rede Confiável e configure pelo menos um dos critérios a seguir:
  - DNS Servers - Valores separados por vírgula de todos os endereços de servidor DNS que uma interface de rede deve ter quando o cliente está em uma rede confiável. Qualquer servidor inserido pode ser usado para corresponder a esse perfil. Para que o TND corresponda, qualquer endereço de servidor DNS deve corresponder à interface local.
  - DNS Domains - Valores separados por vírgulas dos sufixos DNS que uma interface de rede deve ter quando o cliente está em uma rede confiável.
  - Trusted Server- Adicione um ou mais servidores na rede que apresentem um certificado

TLS com um hash que corresponda ao hash fornecido. Para especificar uma porta diferente de 443, anexe a porta usando a notação padrão. Você pode adicionar até 10 servidores confiáveis, dos quais apenas um precisa passar na validação.

- Certificate Public Key Hash: Verifique a etapa [Pré-requisitos e Limites do Sistema](#) para saber como gerar o hash de certificado.

Repita as etapas para adicionar outros perfis de rede confiável.

---



Note: Várias opções dentro do mesmo critério é um operador OU. Critérios Diferentes Definidos é um operador AND.

---

Step 2, Task 2: Defined a trusted network

2/4 tasks

Home

Experience Insights

Connect

Resources

Secure

Monitor

Investigate

Admin

Workflows

← 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 <span>i</span> | <a href="#">— Remove Criterion</a> |
|-------------|----------------------------|------------------------------------|
| DNS Domains | amitlab.com                | <a href="#">— Remove Criterion</a> |

AND

| Criterion   | DNS Servers <span>i</span> | <a href="#">— Remove Criterion</a> |
|-------------|----------------------------|------------------------------------|
| DNS Servers | 192.168.52.2               | <a href="#">— Remove Criterion</a> |

[+ Add Criterion](#)

## Passo 2: Habilitar TND para acesso privado ou à Internet

- Navegue até Connect > End User Connectivity
- Editar perfil ZTA
- Para **Secure Private Destinations** OU **Secure Internet Access**

Acesso privado seguro

## 1 Secure Private Access

1 Destination

## 2 Secure Internet Access

## 3 Users and Groups

## Secure Private Access

Add the private destinations and private resources to be secured.

### Traffic Steering

### Options

## Acesso seguro à Internet

## Secure Private Access

1 Destination

## 2 Secure Internet Access

## 3 Users and Groups

## Secure Internet Access

Add the Internet and SaaS destinations to be secured.

### Traffic Steering

### Options

- Clique em Options

- Clique em Use trusted networks to secure private destinations OU Use trusted networks to secure internet destinations depende da opção escolhida antes
- Clique em + Trusted Network

| Name | Inspector Adapters | DNS Domains | DNS Servers | Trusted Servers |
|------|--------------------|-------------|-------------|-----------------|
|      |                    |             |             |                 |



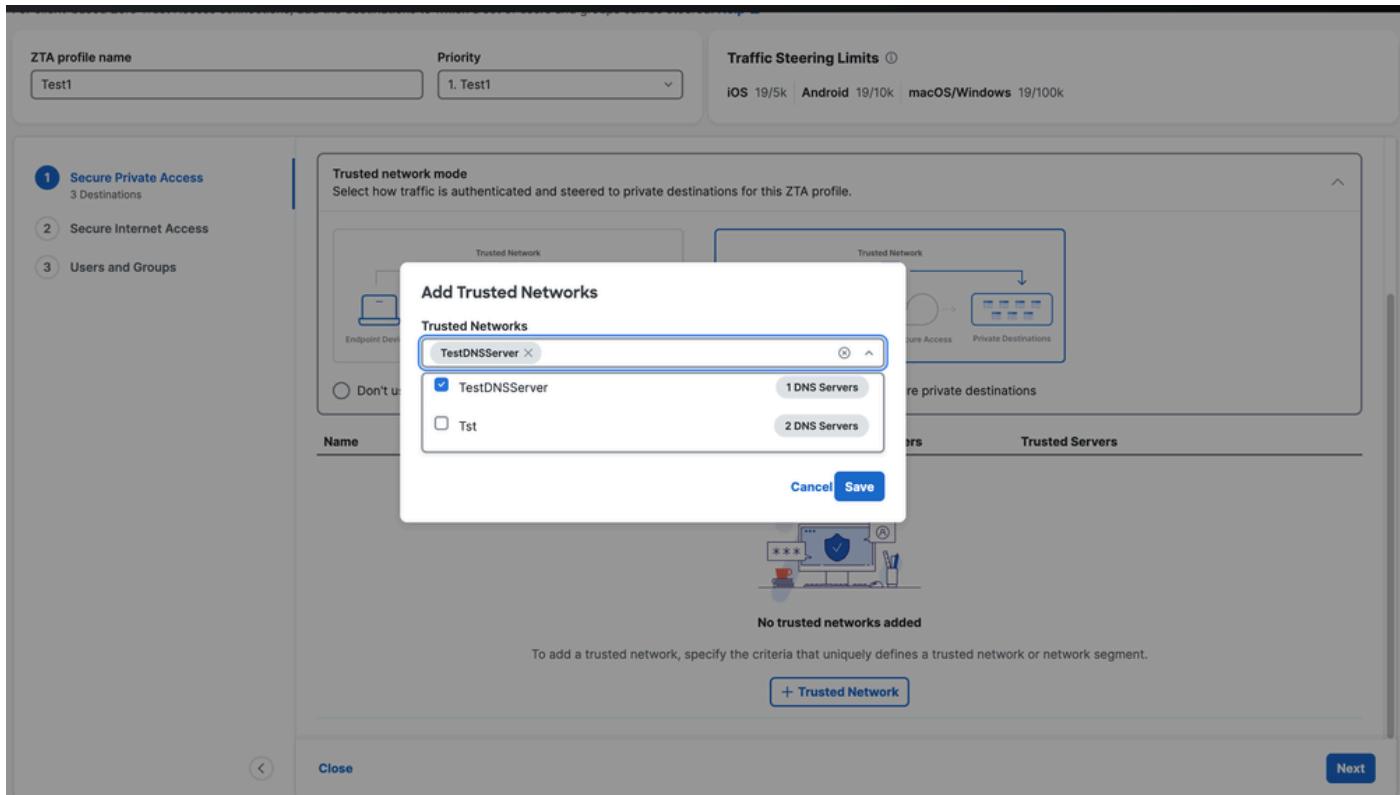
No trusted networks added

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

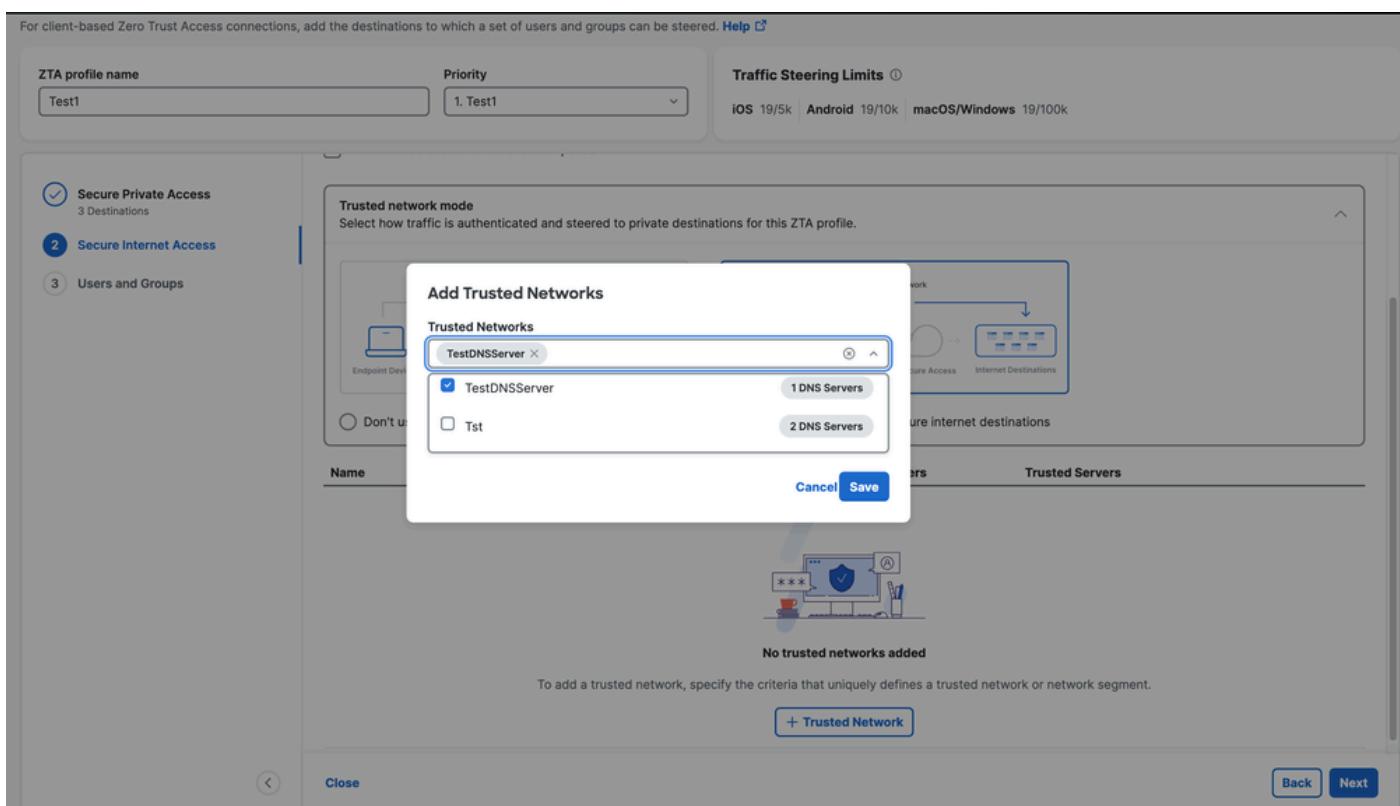
[+ Trusted Network](#)

- Escolha o(s) perfil(is) de rede confiável(is) configurado(s) na página anterior e clique em Save

## Acesso privado seguro



## Acesso seguro à Internet



- Atribua o Users/Groups ao perfil ZTA e clique em Close.

The screenshot shows the 'Users and Groups' section of a ZTA profile configuration. On the left, there are checkboxes for 'Secure Private Access' (3 Destinations) and 'Secure Internet Access'. A 'Users and Groups' section is highlighted with a blue border, showing 1 user and 0 groups. The user listed is 'marcelo.zaf@cesc-city.com.br'. The interface includes a search bar, a table with columns for Name, Email, Type, and Users, and buttons for 'Back' and 'Close'.

### Passo 3: Configuração do lado do cliente

1. Certifique-se de que o servidor DNS correto esteja definido no adaptador Ethernet, pois escolhemos o adaptador físico como critério
2. Verifique se você tem um Sufixo DNS Específico da Conexão definido.

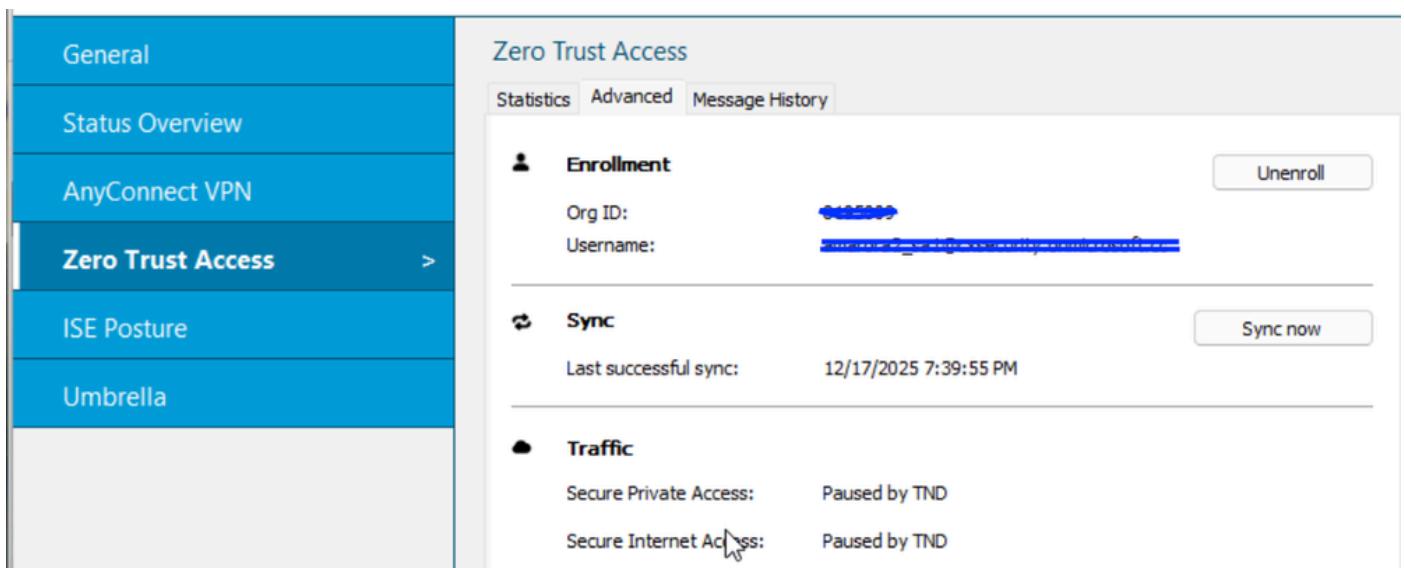
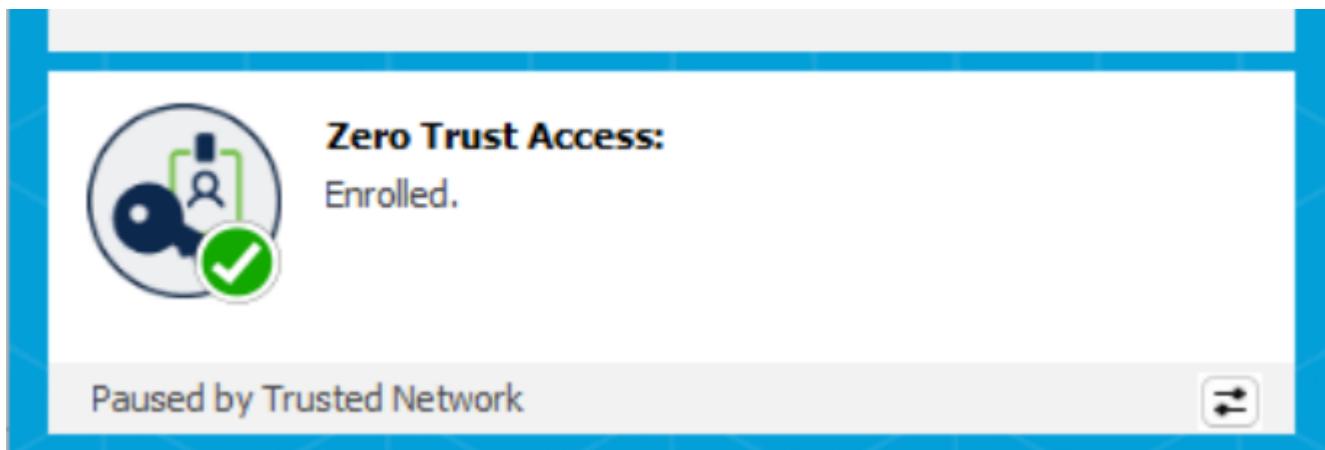
```
Ethernet adapter Ethernet0:

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
```

Com a próxima sincronização de configuração ZTA para Secure Client em alguns minutos, o módulo ZTA faz automaticamente uma pausa quando detecta que está em uma das redes confiáveis configuradas.

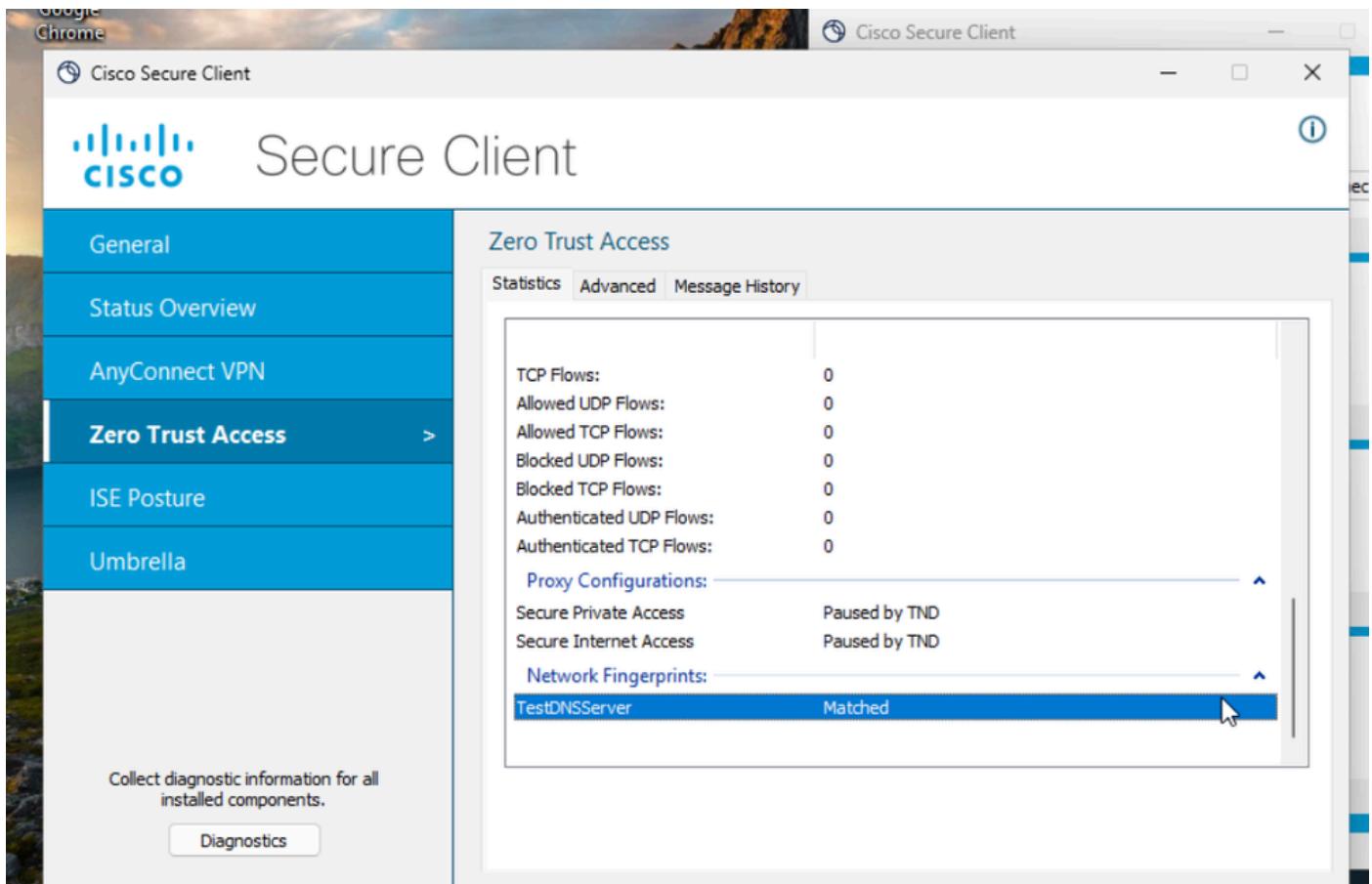
# Verificar

- Do cliente seguro



A screenshot of a web-based dashboard for 'Zero Trust Access'. On the left is a vertical sidebar with the following menu items: General, Status Overview, AnyConnect VPN, Zero Trust Access (which is highlighted with a blue background and a dropdown arrow), ISE Posture, and Umbrella. The main content area is titled 'Zero Trust Access' and contains three sections: 'Enrollment', 'Sync', and 'Traffic'. The 'Enrollment' section shows 'Org ID:' and 'Username:' both redacted with blue bars. There is a 'Unenroll' button. The 'Sync' section shows 'Last successful sync: 12/17/2025 7:39:55 PM' and a 'Sync now' button. The 'Traffic' section shows 'Secure Private Access: Paused by TND' and 'Secure Internet Access: Paused by TND'.

| Section                | Status        |
|------------------------|---------------|
| Secure Private Access  | Paused by TND |
| Secure Internet Access | Paused by TND |



- Do pacote DART - Logs ZTA

Nenhuma regra TND configurada.

2025-12-17 17:53:40.711938 csc\_zta\_agent[0x0000206c/config\_enforcer, 0x0000343c] |/ AtiveSteeringPolicy.cpp:316  
AtiveSteeringPolicy::collectProxyConfigPauseReasons() TND conectará ProxyConfig 'default\_spa\_config' (sem regras)

2025-12-17 17:53:40.711938 csc\_zta\_agent[0x0000206c/config\_enforcer, 0x0000343c] |/ AtiveSteeringPolicy.cpp:316  
AtiveSteeringPolicy::collectProxyConfigPauseReasons() TND conectará ProxyConfig 'default\_tia\_config' (sem regras)

Regra TND configurada - Servidor DNS - Configuração recebida do cliente

25-12-17 20:33:15.987956 csc\_zta\_agent[0x00000f80, 0x00000ed4] W/ CaptivePortalDetectionService.cpp:308  
CaptivePortalDetectionService::getProbeUrl() no último instantâneo de rede, usando a primeira url de investigação

2025-12-17 20:33:15.992042 csc\_zta\_agent[0x00000f80, 0x00000ed4] |/ NetworkChangeService.cpp:144 NetworkChangeService::Start() Instantâneo inicial da rede:

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=Desconhecido

Conditional\_actions": [{"action": "disconnect"}] informa que o TND está configurado no perfil ZTA.

2025-12-17 17:55:36.430233 csc\_zta\_agent[0x00000c90/config\_service, 0x0000343c] |/ ConfigSync.cpp:309  
ConfigSync::HandleRequestComplete() **recebeu nova configuração:**

{"ztnaConfig": {"global\_settings": {"exclude\_local\_lan": true}, "network\_fingerprints": [{"id": "28f629ee-7618-44cd-852d-6ae1674e3cac", "label": "TestDNSServer"}, {"action": "connect"}], "id": "default\_spa\_config", "label": "Secure Private Access", "match\_resource\_configs": [{"spa\_steering\_config": "spa\_proxy\_server"}, {"proxy\_server": "spa\_proxy\_server"}], "condition\_actions": [{"action": "disconnect", "check\_type": "on\_error"}]}]

["192.168.52.2"], "interval\_repetição": 300}], "configs\_proxy": [{"ações\_condicionais": [{"ação": "desconectar", "tipo\_de\_verificação": "na\_rede", "combinar\_im": 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"}], "condition\_actions": [{"action": "disconnect", "check\_type": "on\_error"}]}

44cd-852d-6ae1674e3cac"]},{"action":"access"

2025-12-17 17:55:36.472435 csc\_zta\_agent[0x000039a8/main, 0x0000343c] I/ NetworkFingerprintService.cpp:196  
NetworkFingerprintService::handleStatusUpdate() transmitindo o status de impressão digital da rede: **Impressão digital: 28f629ee-7618-44cd-852d-6ae1674e3cac** Interfaces: Ethernet0

#### Desconexão TND em uma Condição DNS

2025-12-17 17:55:36.729130 csc\_zta\_agent[0x0000206c/config\_enforcer, 0x0000343c] I/ AтивSteeringPolicy.cpp:378  
AтивSteeringPolicy::UpdateActiveProxyConfigs() atualizando a configuração do proxy ativo

2025-12-17 17:55:36.729130 csc\_zta\_agent[0x0000206c/config\_enforcer, 0x0000343c] I/ AтивSteeringPolicy.cpp:287

AтивSteeringPolicy::collectProxyConfigPauseReasons() TND desconectará ProxyConfig "Acesso Seguro à Internet" devido à condição: na\_rede:

**28f629ee-7618-44cd-852d-6ae1674e3cac** ação=Desconectar

2025-12-17 17:55:36.729130 csc\_zta\_agent[0x0000206c/config\_enforcer, 0x0000343c] I/ AтивSteeringPolicy.cpp:366

AтивSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Private Access' está desconectando devido a: Tendêncialnativa

2025-12-17 17:55:36.729130 csc\_zta\_agent[0x0000206c/config\_enforcer, 0x0000343c] I/ AтивSteeringPolicy.cpp:366

AтивSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Internet Access' está desconectando devido a: Tendêncialnativa

#### Corresponder DNS de tipo de regra

2025-12-17 17:55:36.731286 csc\_zta\_agent[0x000039a8/main, 0x0000343c] I/ ZtnaTransportManager.cpp:1251

ZtnaTransportManager::closeObsoleteAppFlows() forçam o fechamento do fluxo do aplicativo devido a ProxyConfig obsoleto  
enrollmentId=7b35249c-64e1-4f55-b12b-58875a806969 proxyConfigId=default\_tia\_config destino TCP [safebrowsing.googleapis.com]:443  
srcPort=61049 realDestIpAddr=172.253.122.95 processo=<chrome.exe|PID 11904|user amit\amita> parentProcess=<Rule5.exe

## Informações Relacionadas

- [Supporte técnico e downloads da Cisco](#)
- [Central de ajuda do Cisco Secure Access](#)
- [Guia de design do Cisco SASE](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.