Zero Trust Network Access configureren met Trusted Network Detection

Inhoud

Inleiding

In dit document worden de vereiste stappen beschreven voor het configureren van de ZTNA Trusted Network Detection.

Voorwaarden

- Minimale versie van Secure Client 5.1.10
- Ondersteund platform - Windows en MacOS
- Trusted Platform Module (TPM) voor Windows
- Secure Enclave-coprocessor voor Apple apparaten
- 'Vertrouwde servers' die in een Trusted Network-profiel zijn geconfigureerd, zijn impliciet uitgesloten van ZTA-interceptie. Deze servers kunnen ook niet worden gebruikt als ZTA-privébronnen.
- De TND-configuratie is van invloed op alle geregistreerde clients in de organisatie
- Beheerders kunnen de volgende stappen gebruiken om een 'Certificate Public Key Hash' voor vertrouwde servers te genereren
  - Download de vertrouwde servers public cert
  - Voer deze opdracht shell uit op generate the hash:

```
openssl x509 -in
```

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

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Access
- Meld apparaten aan bij Zero Trust Access met SAML- of CERT-gebaseerde verificatie.

Gebruikte componenten

- Beveiligde clientversie 5.1.13
- TPM
- Secure Access-huurder
- Windows-apparaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

- Met TND kunnen beheerders Secure Client configureren om de besturing en handhaving van ZTA-verkeer op Trusted Networks tijdelijk te onderbreken.
- Beveiligde client hervat ZTA-handhaving wanneer het eindpunt het vertrouwde netwerk verlaat.
- Voor deze functie is geen interactie met de eindgebruiker vereist.
- ZTA TND-configuraties kunnen onafhankelijk worden beheerd voor privé- en internetZTA-bestemmingen.

Belangrijkste voordelen

- Verbeterde netwerkprestaties en verminderde latentie zorgen voor een soepelere

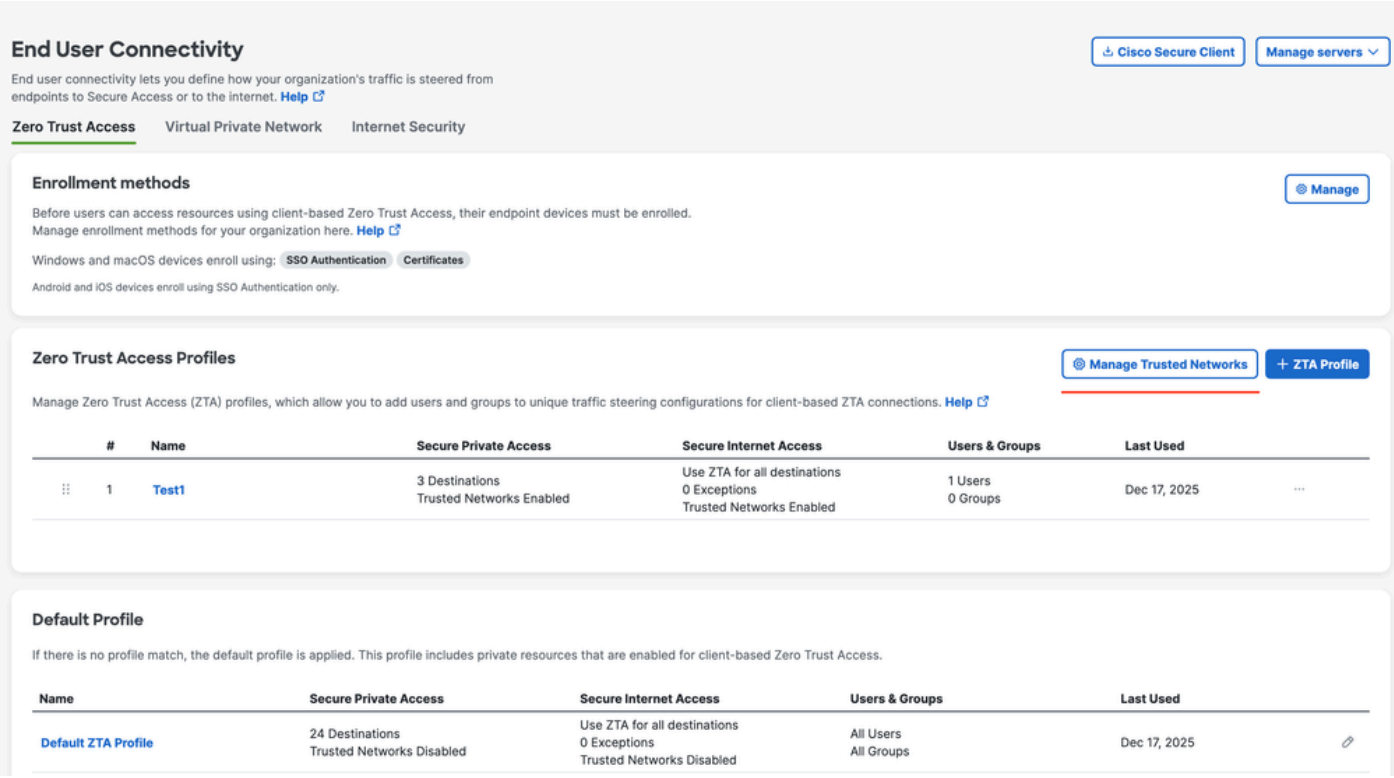
gebruikerservaring.
- Lokale handhaving van de beveiliging in het vertrouwde netwerk biedt een flexibel en geoptimaliseerd gebruik van bronnen.
- Eindgebruikers kunnen profiteren van de voordelen zonder aanwijzingen of acties.
- Onafhankelijke controle van TND voor privétoegang en internettoegang biedt beheerdersflexibiliteit om verschillende operationele en beveiligingsproblemen aan te pakken

Configureren

Stap 1: Vertrouwd netwerkprofiel maken - DNS-server en -domein

Navigeer naar Secure Access Dashboard:

- Klik op Connect > End User Connectivity > Manage Trusted Networks > +Add



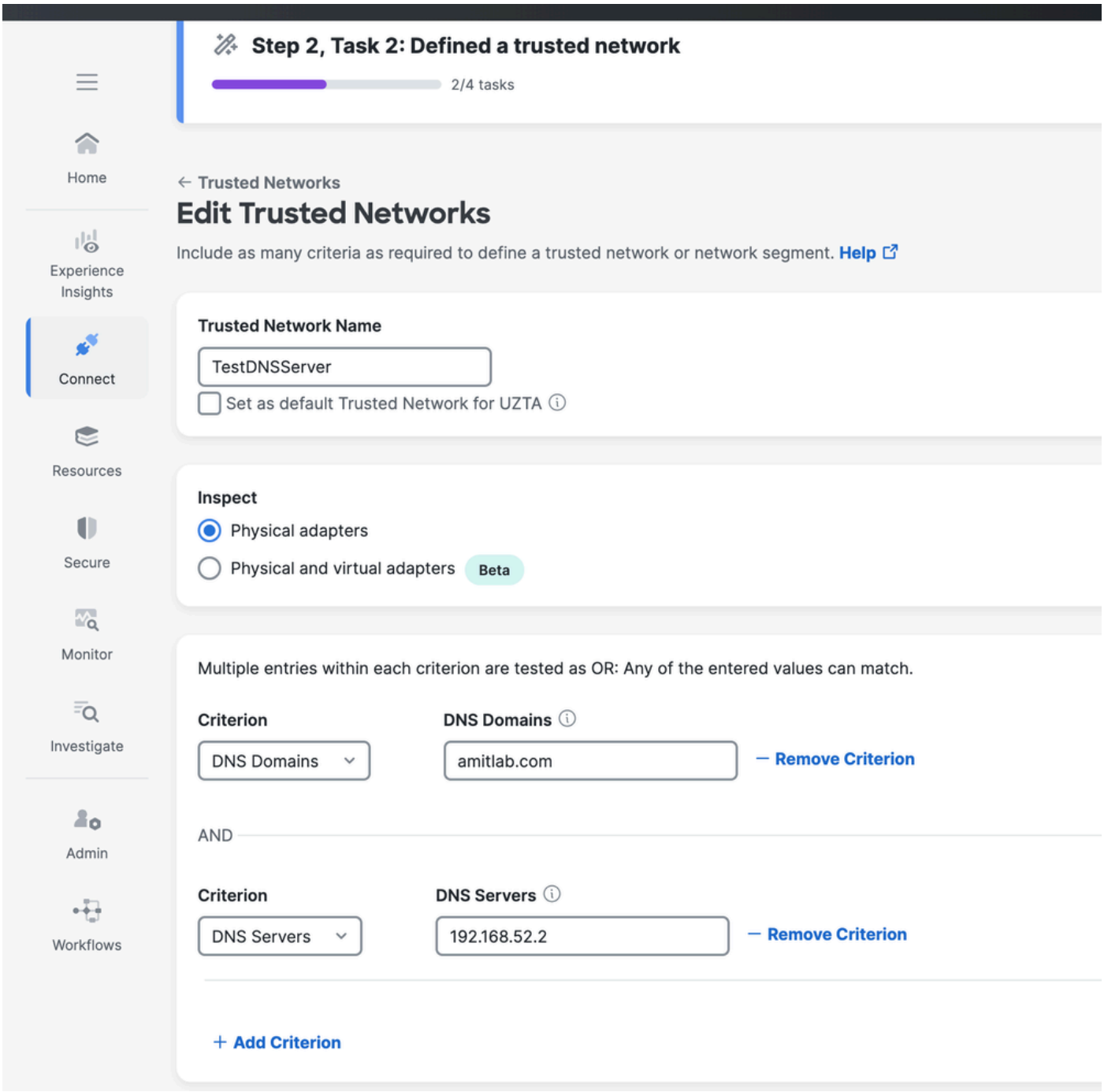
- Geef een naam op voor het Trusted Network-profiel en configureer ten minste een van de volgende criteria:
  - DNS Servers – Kommagescheiden waarden van alle DNS-serveradressen die een netwerkinterface moet hebben wanneer de client zich in een vertrouwd netwerk bevindt. Elke ingevoerde server kan worden gebruikt om aan dit profiel te voldoen. Om TND te laten overeenkomen, moet elk adres van de DNS-server overeenkomen met de lokale interface.
  - DNS Domains – Kommagescheiden waarden van DNS-achtervoegsels die een netwerkinterface moet hebben wanneer de client zich in een vertrouwd netwerk

bevindt.

- Trusted Server- Voeg een of meer servers op het netwerk toe die een TLS-certificaat presenteren met een hash die overeenkomt met de hash die u opgeeft. Als u een andere poort dan 443 wilt opgeven, voegt u de poort toe met standaardnotatie. U kunt maximaal 10 vertrouwde servers toevoegen, waarvan er slechts één moet worden gevalideerd.
  - Certificate Public Key Hash: Controleer stap Vereisten en systeemlimieten om te weten hoe u de hash van het certificaat kunt genereren.

Herhaal de stappen om extra vertrouwde netwerkprofielen toe te voegen.

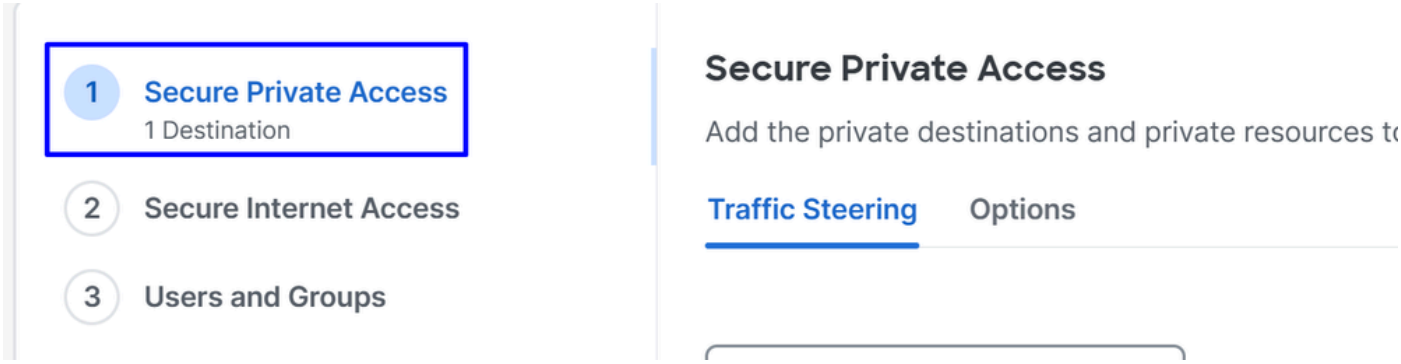
Opmerking: Meerdere opties binnen dezelfde criteria is een OR-operator. Different Criteria Defined is een AND-operator.



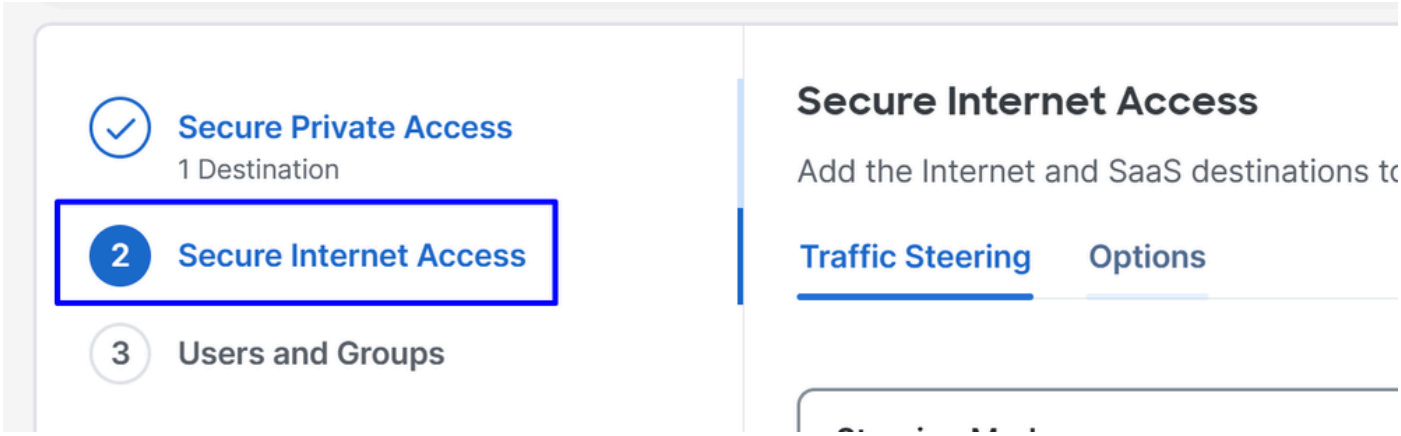
Stap 2: TND inschakelen voor privé- of internettoegang

- Navigeer naar Connect > End User Connectivity
- ZTA-profiel bewerken
- VoorSecure Private Destinationsof Secure Internet Access

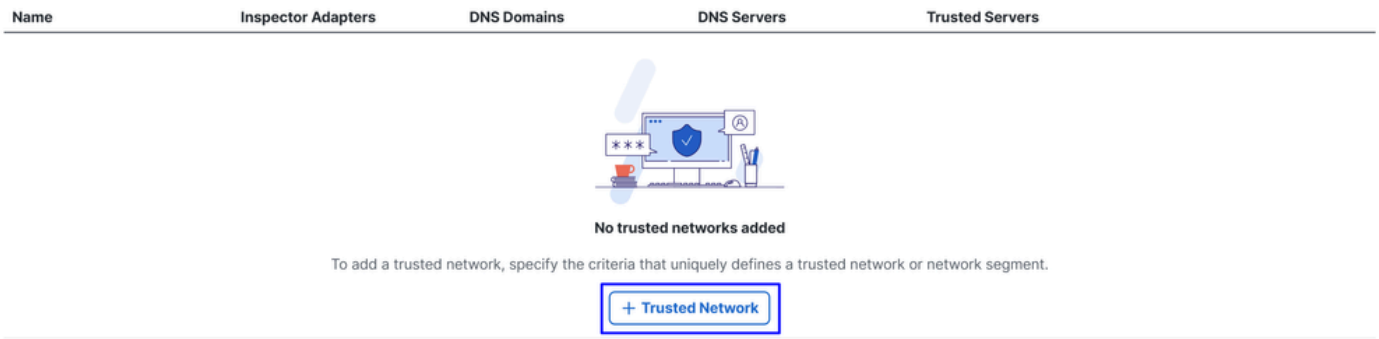
Beveiligde privétoegang



Veilige internettoegang

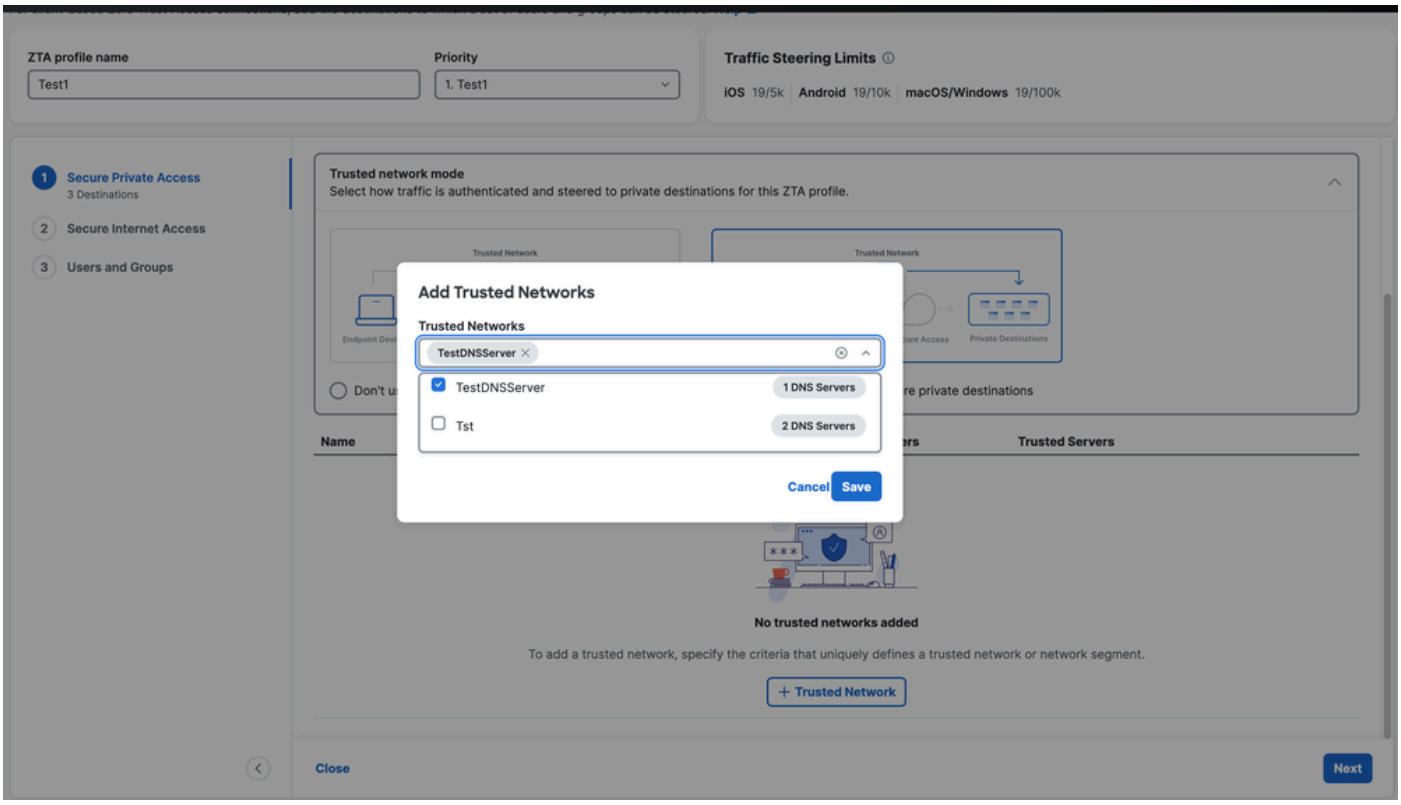


- Klik op Options
  - Klik op Use trusted networks to secure private destinations of Use trusted networks to secure internet destinationshangt af van de gekozen optie
  - Klik op + Trusted Network

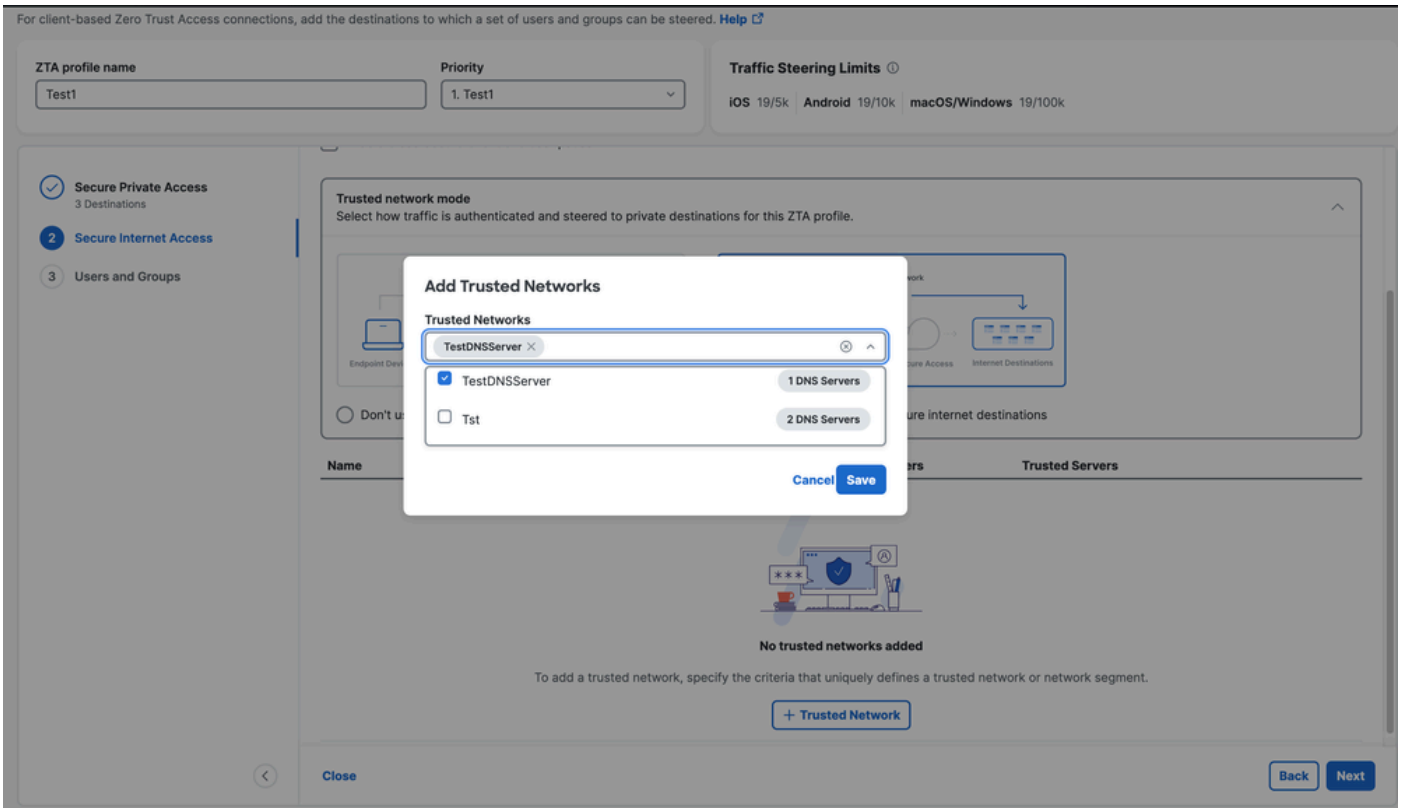


- Kies de vertrouwde netwerkprofielen die u op de vorige pagina hebt geconfigureerd en klik op Save

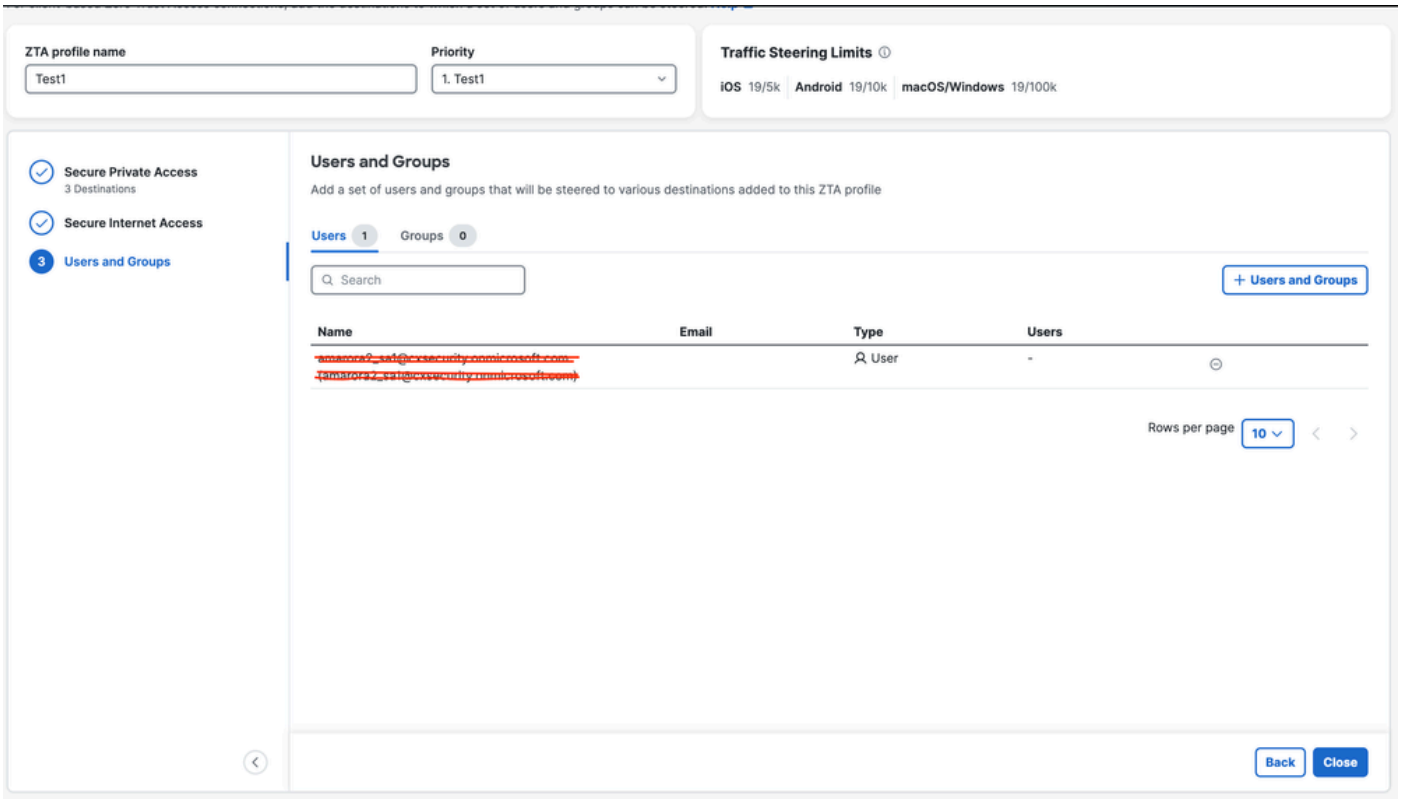
Beveiligde privétoegang



Veilige internettoegang



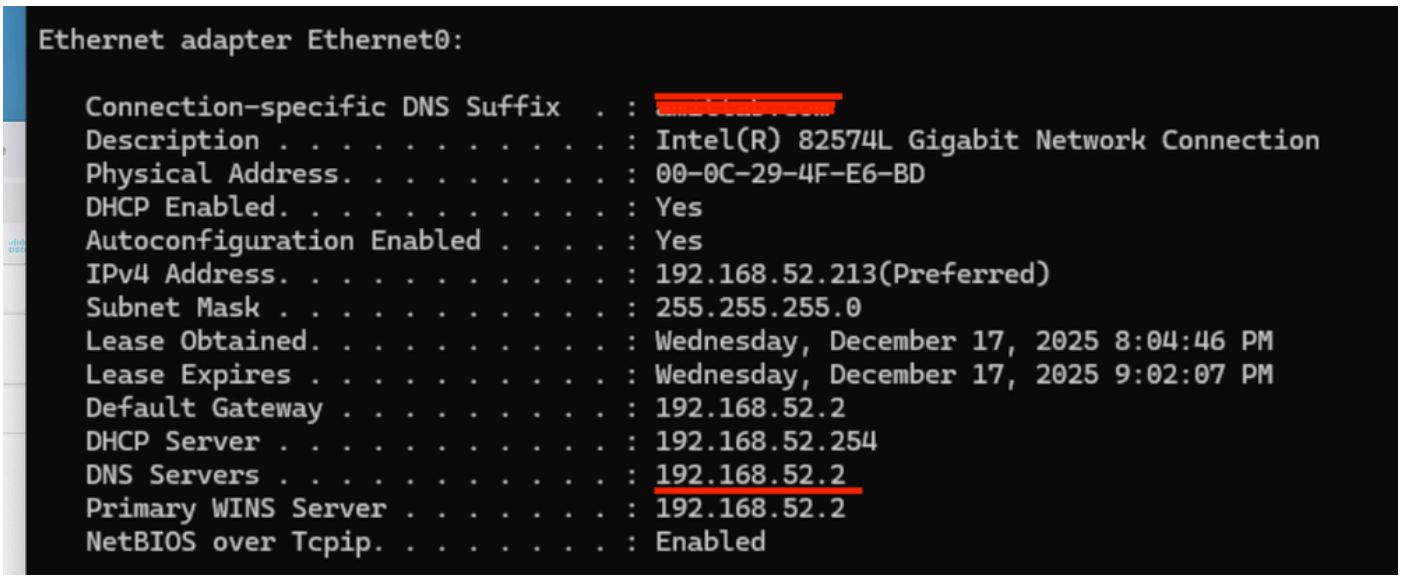
- Wijs het Users/Groups profiel toe aan ZTA Profile en klik op Close.



Stap 3: Configuratie aan clientzijde

1. Zorg ervoor dat u de juiste DNS-server hebt gedefinieerd onder Ethernet-adapter, omdat we de fysieke adapter als criterium hebben gekozen

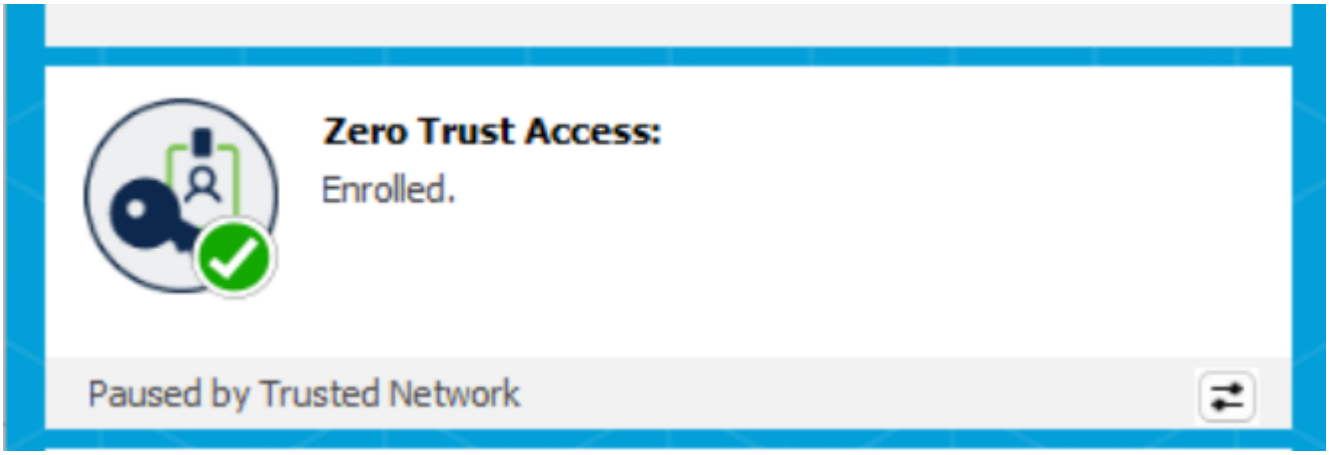
2. Zorg ervoor dat u Connection Specific DNS Suffix (Verbindingsspecifiek DNS-suffix) hebt gedefinieerd.

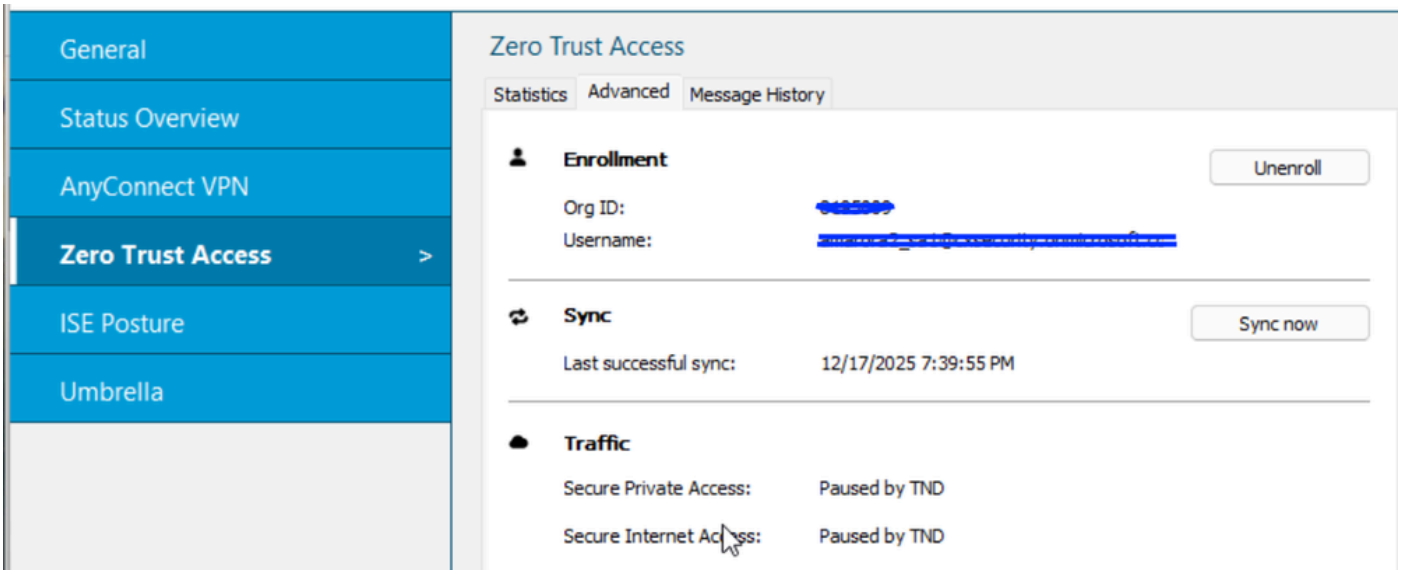


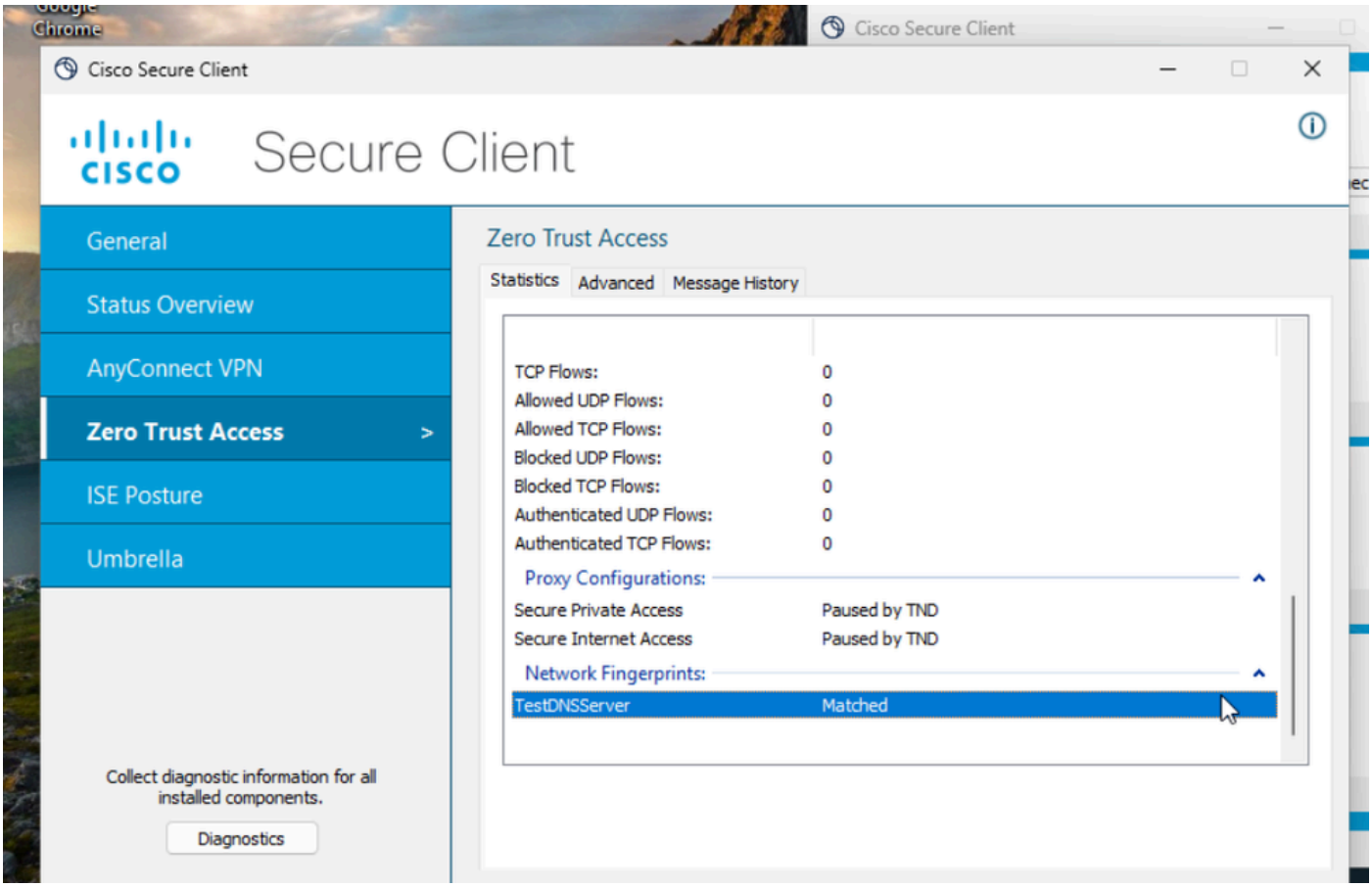
Wanneer de volgende ZTA-configuratie binnen enkele minuten wordt gesynchroniseerd met de Secure Client, wordt de ZTA-module automatisch onderbroken wanneer deze wordt gedetecteerd op een van de geconfigureerde Trusted Networks.

Verifiëren

- Van beveiligde client







- Van DART-bundel - ZTA-logs

Er zijn geen TND-regels geconfigureerd.

2025-12-17 17:53:40.711938 csc_zta_agent[0x000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND zal ProxyConfig 'default_spa_config' verbinden (geen regels)

2025-12-17 17:53:40.711938 csc_zta_agent[0x000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND zal ProxyConfig 'default_tia_config' verbinden (geen regels)

Geconfigureerde TND-regel - DNS-server - Configuratie client ontvangen

25-12-17 20:33:15.987956 csc_zta_agent[0x00000f80, 0x00000ed4] W/ CaptivePortalDetectionService.cpp:308 CaptivePortalDetectionService::getProbeUrl() geen laatste netwerkmomentopname, eerste probe-URL gebruiken

2025-12-17 20:33:15.992042 csc_zta_agent[0x00000f80, 0x00000ed4] I/ NetworkChangeService.cpp:144 NetworkChangeService::**Start() Eerste netwerkmomentopname:**
Ethernet0: subnetten=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=onbekend

conditional_actions":[{"action":"disconnect" vertelt dat TND is geconfigureerd in het ZTA-profiel.

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

{"ztnaConfig":{"global_settings":{"exclude_local_lan":true},**"network_fingerprints":[{"id":"28f629ee-7618-44cd-852d-6ae1674e3cac","label":"TestDNServer","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_fingerpr
7618-44CD-852D-6AE1674E3CAC"]},{"action":"connect"}],"ID": default_spa_config","label":"Beveiligd privé
Access","match_resource_configs":["spa_steering_config"],"proxy_server":"spa_proxy_server"},{"conditional_actions":[{"action":"disconnect","check_type":"on_

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() zendernetwerk-vingerafdrukstatus: **Vingerafdruk**: **28f629ee-7618-44cd-852d-6ae1674e3cac-interfaces: Ethernet0**

TND verbreekt verbinding onder DNS-voorwaarde

2025-12-17 17:55:36.729130 csc_zta_agent[0x000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:378 ActiveSteeringPolicy::UpdateActiveProxyConfigs() bijwerken van actieve proxyconfiguratie

2025-12-17 17:55:36.729130 csc_zta_agent[0x000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:287 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND verbreekt de verbinding met ProxyConfig "Secure Internet Access" vanwege voorwaarde: on_network: 28f629ee-7618-44cd-852d-6ae1674e3cac actie=**loskoppelen**

2025-12-17 17:55:36.729130 csc_zta_agent[0x000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Private Access' verbreekt verbinding vanwege: InactiveTnd

2025-12-17 17:55:36.729130 csc_zta_agent[0x000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Internet Access' verbreekt de verbinding vanwege: InactiveTnd

Type overeenkomende regel DNS

2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main, 0x0000343c] I/ ZtnaTransportManager.cpp:1251 ZtnaTransportManager::closeObsoleteAppFlows() forceren van sluiten van app flow door verouderde ProxyConfig enrollmentId=7b35249c-64e1-4f55-b12b-58875a806969 proxyConfigId=default_tia_config TCP-bestemming [safebrowsing.googleapis.com]:443 srcPort=61049 realDestIpAdr=172.253.122.95|process=<chrome.exe4 parentProcess=<chrome.exe|PID 5220|user amit\amita> **matchRuleType=DNS**

Gerelateerde informatie

- Cisco Technical Support en downloads
- Cisco Secure Access Help Center
- Cisco SASE-ontwerphandleiding

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.