

Universele ZTNA configureren voor toegang tot privébronnen op beveiligde toegang

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Over Universal ZTNA](#)

[Netwerkdetectie](#)

[Typen voor handhaving](#)

[Use cases](#)

[Architecturale componenten](#)

[Pakketstroom](#)

[Configureren](#)

[Netwerkdigram](#)

[Testcases](#)

[Testcase 1: externe gebruiker - handhaving van de cloud](#)

[Testcase 2 - Externe gebruiker - Lokale handhaving](#)

[Testcase 3 - Lokale gebruiker - Lokale handhaving](#)

[Testcase 4 - Lokale en externe gebruiker - Lokale of cloudhandhaving met TND](#)

[Problemen oplossen](#)

[Nuttige opdrachten:](#)

Inleiding

In dit document behandelen we de configuratie voor Private Resource Access via Universal ZTNA met verschillende verkeerspaden.

Voorwaarden

De volgende configuratie moet zijn voltooid voordat de Universal ZTNA-configuratie wordt uitgevoerd

- [Identiteitsprovider op Cisco Secure Access](#)
- [Apparaten inschrijven in Zero Trust Access met behulp van certificaten](#)

- [Tunnels configureren met Cisco Secure Firewall](#)
- [Virtual Private Network voor externe toegang](#)
- [Resource Connector voor beveiligde toegang](#)
- [FTD-onboarding voor Cloud Security Control](#)
- Hybride ZTNA-functievlag moet worden ingeschakeld voor de betreffende Secure Access-huurder, neem contact op met Cisco TAC om de vlag in te schakelen

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IPsec VPN-configuratie op Cisco Secure Access en Firewall Threat Defense
- Identiteitskeuze (IDP) - Gebruikersprovisioning vanuit Active Directory
- Externe VPN-configuratie op Cisco Secure Access
- Implementatie van Resource Connector op Cisco Secure Access
- Inschrijving op basis van ZTA-certificaat
- Certificaat - OpenSSL, CSR-generatie, Certificaatsjablonen enz.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall Threat Defense (versie 7.7.10)
- Cisco Secure Firepower Management Center (versie 7.7.10)
- Cisco Secure Client (ZTA-versie 5.1.10.1720)
- Windows 11
- Windows 2019 Server - Certificaatautoriteit
- Resource Connector op ESXi

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

Over Universal ZTNA

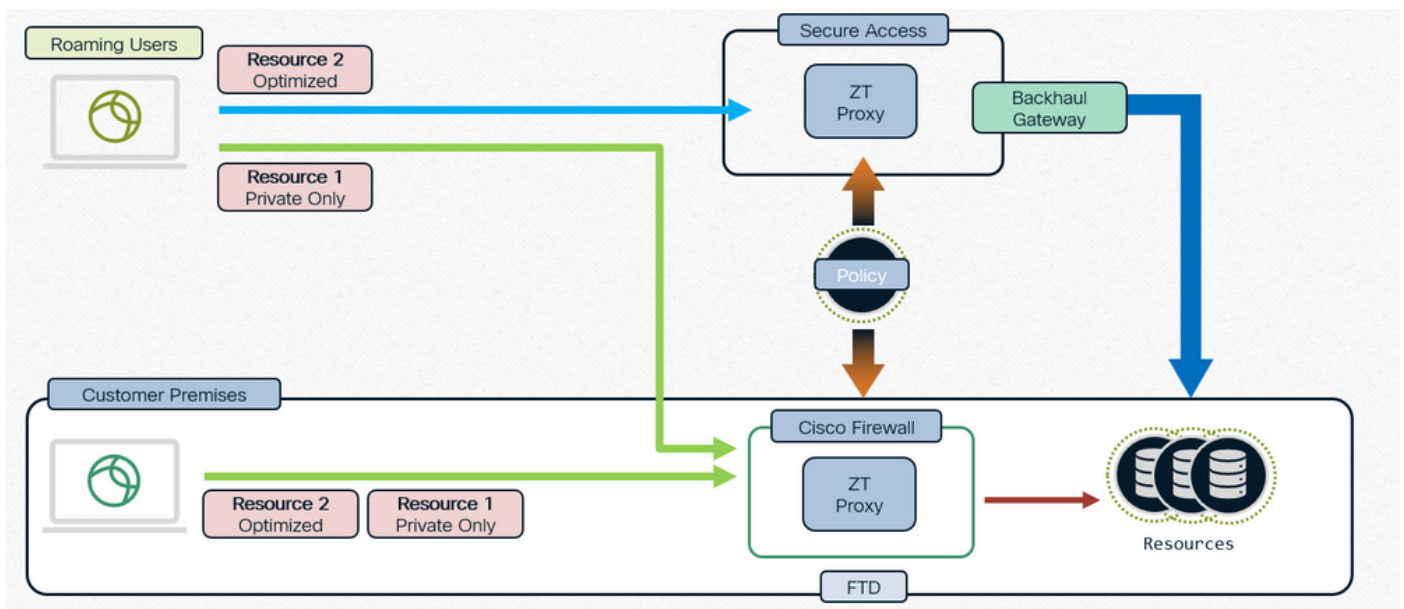
Universal Zero Trust Network Access (uZTNA) stelt beheerders in staat om specifiek toegang tot

interne netwerkbronnen toe te staan op basis van de identiteit van de gebruiker (inclusief het vertrouwen en de houding van de gebruiker) en zonder toegang te verlenen tot het hele netwerk, zoals bij RA-VPN. uZTNA stelt beheerders in staat om interne bronnen en toepassingen te beveiligen voor zowel externe als lokale gebruikers.

Omdat uZTNA er niet van uitgaat dat toegang tot één toepassing impliciet toegang tot andere toepassingen toestaat, wordt het oppervlak van de netwerkaanval vermindert.

Secure Access evalueert het toegangsbeleid. Alle toegangsbeheerbeleidsregels die vanuit het Secure Firewall Management Center op apparaten worden geïmplementeerd, worden genegeerd.

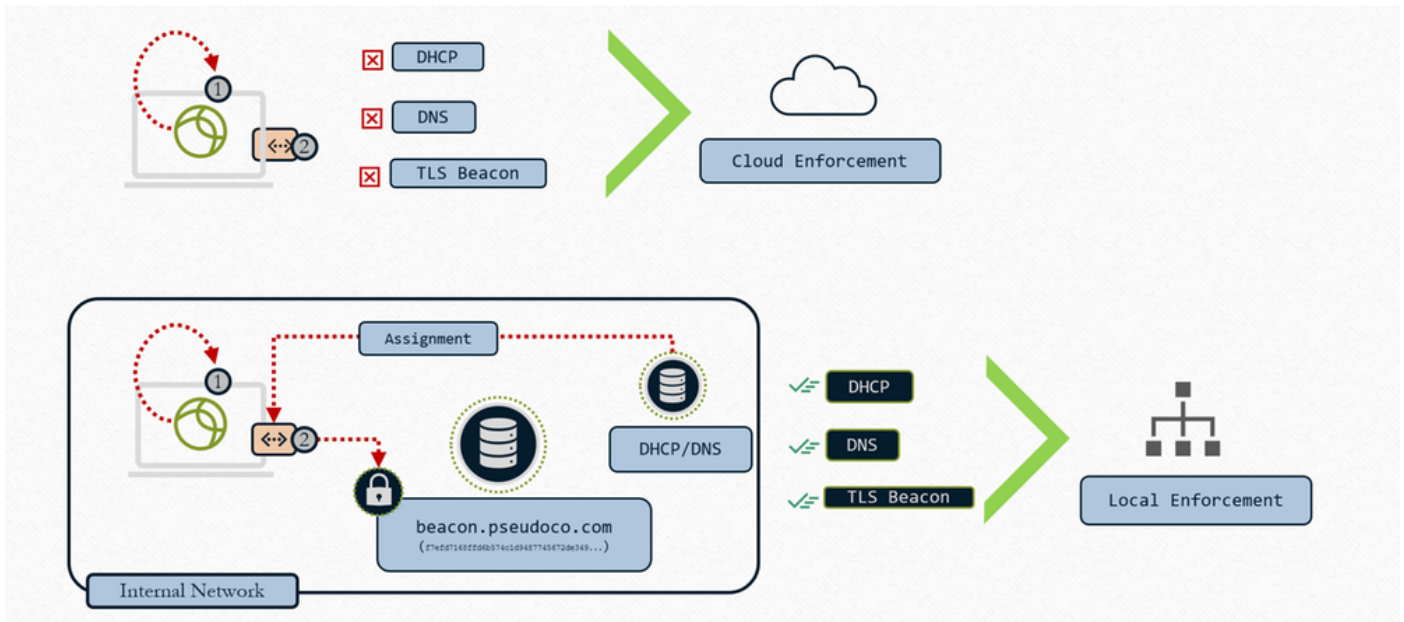
Verkeersproxy, evenals IPS-, bestands- en malwarebeleidshandhaving, wordt uitgevoerd op de Firepower Threat Defense (FTD).



één enkel beleid, gedistribueerde handhaving

Netwerkdetectie

Cloud- of lokale handhaving bepalen



Universal ZTNA - Bepaal de handhaving van de cloud of de lokale omgeving

1- Client ondervraagt lokale interface voor netwerkconfiguratie

2- Klant zoekt naar TLS Beacon

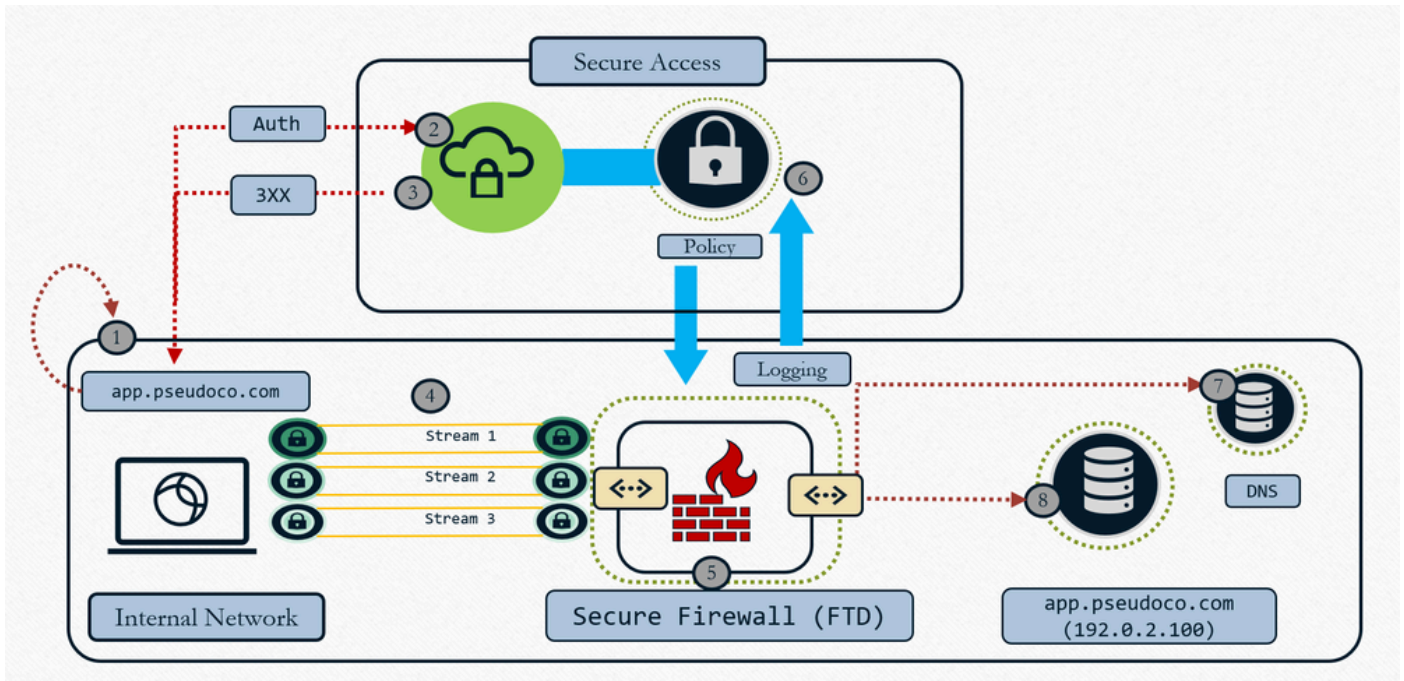
3- Als de voorwaarde overeenkomt – Lokale handhaving

4- Als de voorwaarde niet overeenkomt – Cloud Enforcement

Wanneer we de bron configureren met "Cloud of Local Enforcement" en de TND-regel koppelen aan FTD, is wat het feitelijk doet de set interceptregels die naar de klant wordt verzonden, inclusief de evaluatie van de TND-regel. Dus, die klant zal worden verteld door de cloud om de TND-regel te evalueren. Wanneer we de verbinding verzenden, zetten we het resultaat van die TND - network fingerprint evaluation in HTTP-header, zodat de proxy weet of we on-perm of op een niet-vertrouwd netwerk zijn en vervolgens gebruikt de proxy die informatie en stuurt het verkeer dienovereenkomstig. In het geval dat de vingerafdruk overeenkomt, vertelt Zproxy de client om het verkeer naar FTD om te leiden en als de vingerafdruk niet overeenkomt, wordt het verkeer naar de cloud omgeleid. Raadpleeg [Zero Trust Network Access configureren met Trusted Network Detection](#)

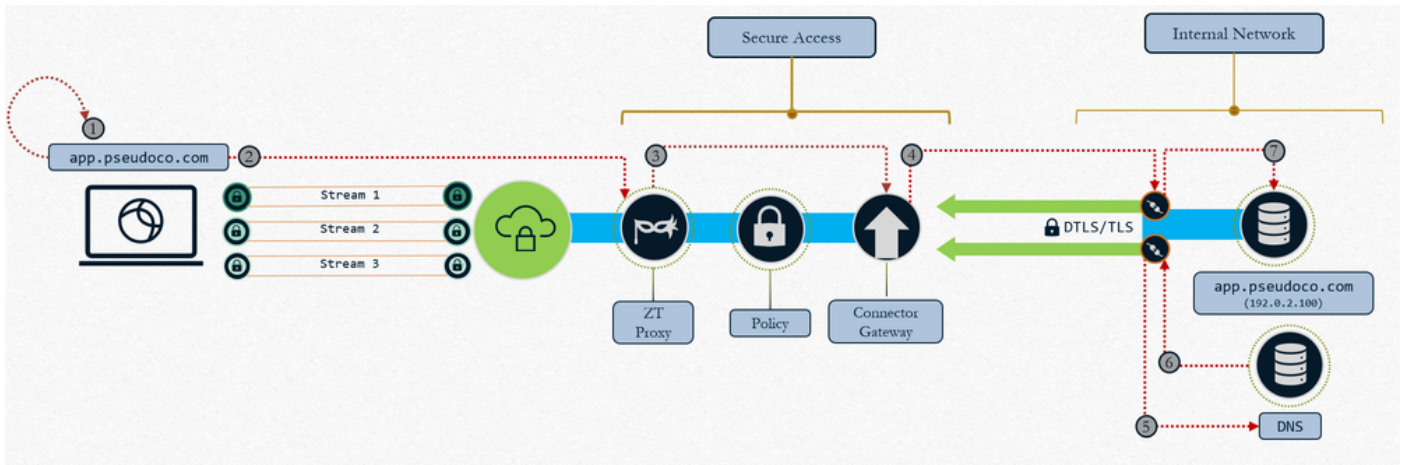
Typen voor handhaving

- Lokaal handhavingsspad: Firewall Enforcement



Universal ZTNA - Lokale handhaving

1. Gebruikersverzoeken App, client vangt en lost verzoek om efemere IP (localhost bereik)
 2. Verificatiecontroleverkeer wordt verzonden naar Secure Access Cloud voor beleidsevaluatie
 3. Cloud retourneert doorverwijzing naar FTD voor handhaving van gegevensplan (indien beleid dit toestaat)
 4. Verkeer gestuurd naar door firewall geconfigureerde kop (interface)
 5. Beleid dat in de cloud is gedefinieerd, wordt afgedwongen (IPS, Malware, Decryptie) met behulp van een lokaal proxy-gegevensvlak
 6. Gebeurtenisregistratie en duplicaat verzonden naar cloud voor consistente rapportage
 7. Firewall voert DNS-resolutie uit op lokaal netwerk om bronverkeer te routeren (indien toegestaan)
 8. Firewall maakt verbinding met resource (nieuwe verbinding gemaakt met resource) terwijl de firewall zich gedraagt als een TCP-proxy
- Cloud Enforcement-pad: OFF-netwerk

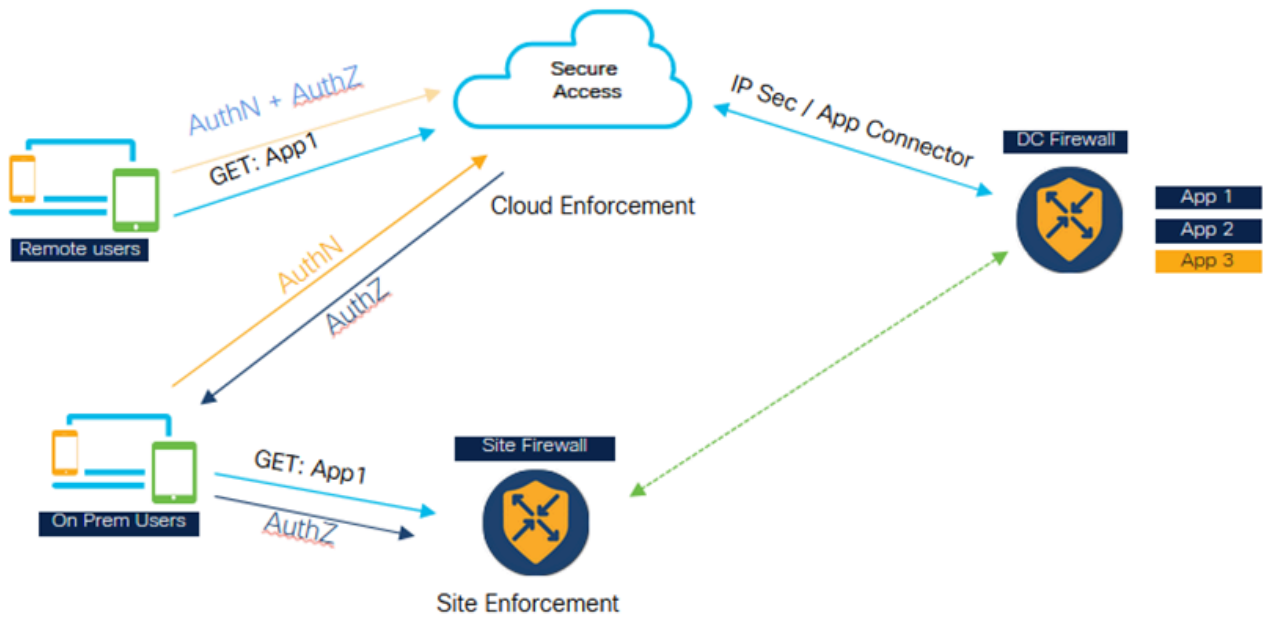


Universal ZTNA: Cloud Enforcement

1. Gebruikersverzoeken App, client vangt en lost verzoek om efemere IP (localhost bereik)
2. Verkeer wordt getransporteerd naar Zero Trust Proxy in Secure Access
3. TCP-verbinding is geproxydeerd en gebouwd op de toegewezen bronconnector, beleid wordt afgedwongen op verkeer
4. Gateway maakt verbinding met bronconnector
5. Resource-connector lost bron-IP op
6. Lokale DNS reageert met bron-IP
7. Bronconnector maakt verbinding met bron

Use cases

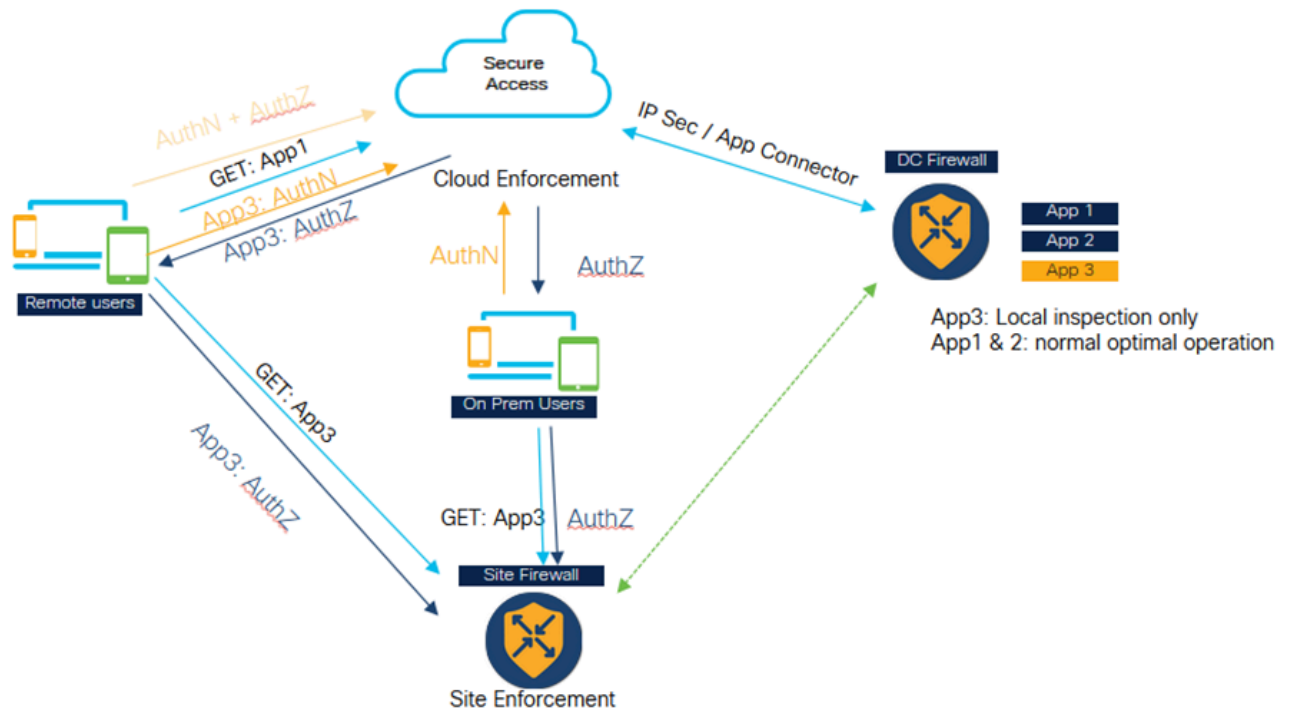
Geval 1: Consistente en geoptimaliseerde ZTNA voor gebruikers op locatie



Universele ZTNA - Consistente en geoptimaliseerde ZTNA (On-premise gebruiker)

- Secure Access en Firewall zijn beide geconfigureerd om de toepassing te beschermen.
- Als de gebruiker op afstand is, gaan ze naar Secure Access voor beleidsevaluatie en -inspectie.
- Als de gebruiker intern/on-premises is, gaat hij/zij naar de firewall voor privé-verkeersinspectie.
- De gebruiker op locatie kan nog steeds naar Beveiligd gaan voor verificatie en evaluatie, alleen het Datapath-verkeer gaat naar de Firewall en wordt geïnspecteerd volgens de beleidsconfiguratie.
- De interne gebruiker die toegang heeft tot de toepassing via de firewall heeft een prestatievoordeel omdat het voorkomt dat het verkeer naar de cloud gaat en vervolgens terugkeert naar het datacenter

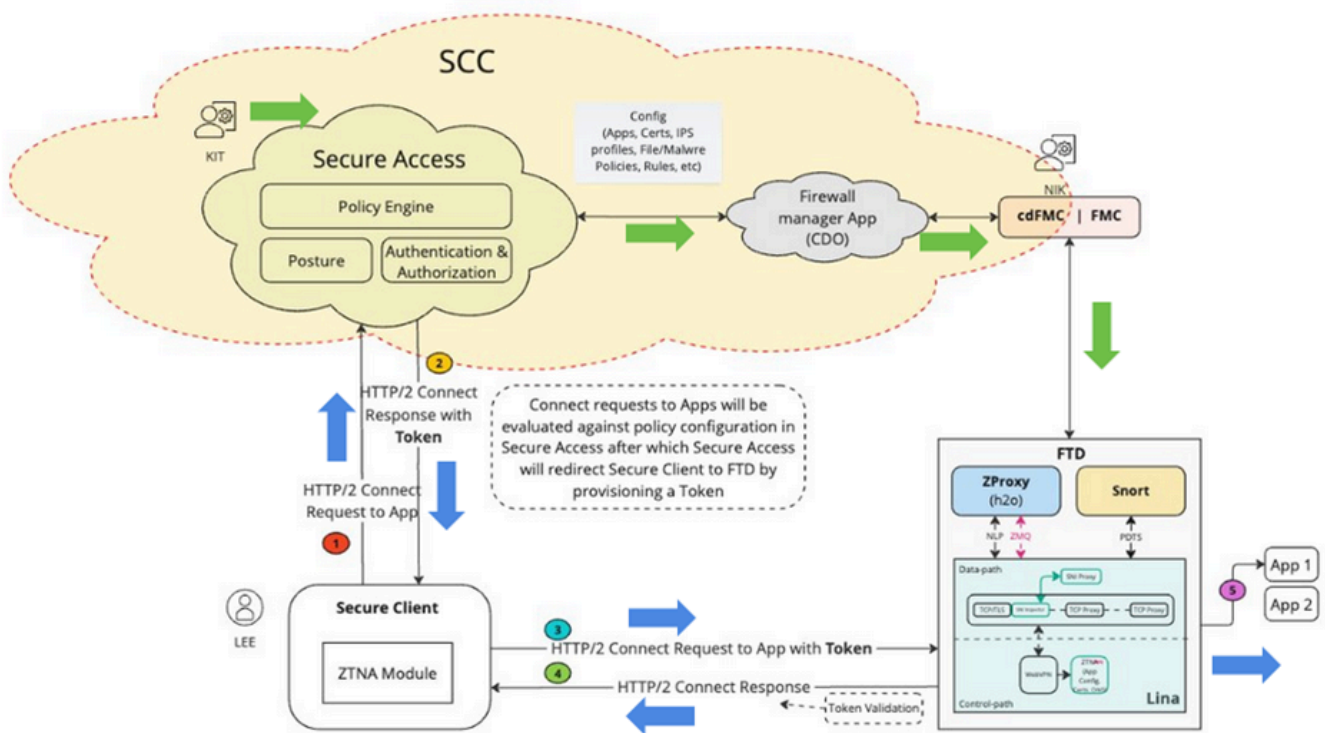
Geval 2: Particuliere inspectie voor gevoelige toepassingen



Universele ZTNA - Privé-inspectie voor gevoelige toepassingen

- Bepaalde kritieke toepassingen kunnen worden geconfigureerd om altijd toegankelijk te zijn via de firewall.
- Het dataverkeer van de app hoeft niet naar de cloud te gaan. Er kan bijvoorbeeld een gevoelige datatoepassing zijn, zoals broncode, die de klant niet naar de cloud wil gaan.
- In dergelijke scenario's gaat zowel extern als on-perm gebruikersverkeer altijd door de firewall en wordt geïnspecteerd. In dit scenario gebeurt authenticatie en beleidsevaluatie echter altijd in de cloud, alleen het dataverkeer gaat via de firewall.

Architecturale componenten



Universal ZTA - Architectural Components

Security Cloud Control (SCC) is de primaire manager voor uZTNA-oplossing. uZTNA is de eerste functie die bovenop SCC wordt gebouwd.

In SCC hebben we twee micro-applicaties, Secure Access en Firewall. Zodra SCC is geleverd en de vereiste functievlaggen zijn ingeschakeld, kunnen we deze micro-applicaties aan de linkerkant van het SCC-paneel zien.

Beveiligde client: in Beveiligde client moeten we Zero Trust Access Module (ZTNA) inschakelen als we ons moeten inschrijven voor de ZTNA-module om toegang te krijgen tot de toepassingen.

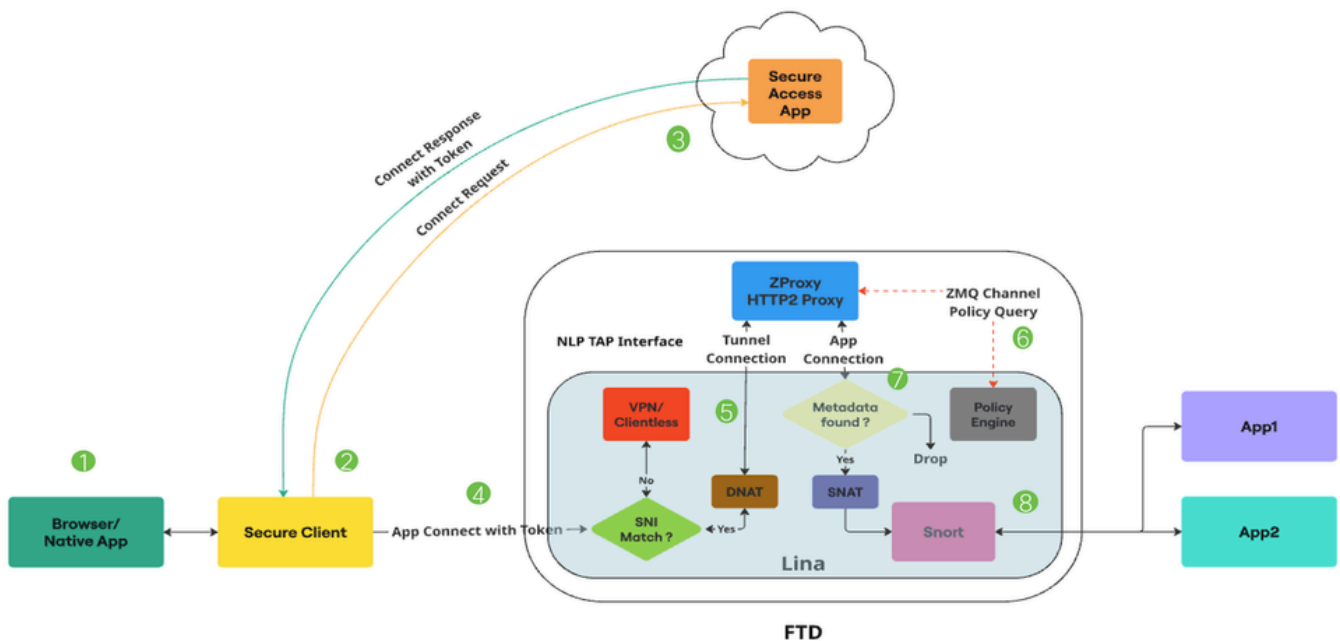
Firewall Threat Defense: FTD beschermt deze toepassingen. FTD voert een ZT-proxy uit die ook bekend staat als H2O (hetzelfde als de proxy in Secure Access Cloud)

Wanneer een gebruiker (bijv. KIT) een privébron en beleid voor Secure Access-microtoepassingen configureert, wordt deze configuratie naar de Firewall-microtoepassing in SCC gepusht. Firewalltoepassing begrijpt de interne FTD-, FTD-configuratie- en hoe u de configuratie op FTD kunt implementeren en beheren. Dus de Firewall-app valideert deze configuratie en roept de FMC-API's op om de configuratie naar FMC te duwen en deze uiteindelijk op FTD te laten implementeren. FTD kan een optie voor automatische implementatie hebben ingeschakeld, zodat beheerders (bijv. Nick) geen handmatige implementatie hoeven te doen.

1. Wanneer een gebruiker (bijv. Lee) probeert toegang te krijgen tot een toepassing, maakt een beveiligde client verbinding met Secure Access via het mTLS-kanaal. Secure Access verifieert de gebruiker met behulp van het clientapparaatcertificaat. Vervolgens worden de autorisatie, houding en andere beleidsregels geëvalueerd die voor die gebruiker en voor die toepassing zijn geconfigureerd.
2. Secure Access, als uiteindelijk wordt vastgesteld dat de toepassing wordt beschermd door Firewall, genereert het een authenticatie token, dat de firewall vertelt dat deze al is geverifieerd en geautoriseerd. De authenticatie token is versleuteld, ondertekend door Secure Access
3. Secure Access leidt de beveiligde client om naar FTD, samen met het auth-token.
4. Secure Client maakt een andere verbinding met FTD, het is een HTTP2-verbinding via mTLS-kanaal. Het stuurt een CONNECT-verzoek voor de applicatie die wordt geopend, samen met het Token.
5. FTD valideert nu het token, als het token met succes is gevalideerd, heeft de gebruiker toegang tot die toepassing. FTD stuurt de bevestiging vervolgens terug naar de beveiligde client

Pakketstroom

Universele ZTNA gedetailleerde pakketstroom



Universele ZTA - pakketstroom

1. De gebruiker probeert toegang te krijgen tot een toepassing via een webbrowser of een eigen toepassing.
2. De beveiligde client onderschept de verbinding en identificeert deze als een gebruiker die probeert toegang te krijgen tot een privébron.
3. De beveiligde client maakt een mTLS-verbinding met beveiligde toegang en vraagt om toegang tot de toepassing. beveiligde toegang controleert het universele ZTNA-beleid en de houdingsprofielen op naleving. als alles in orde is, genereert beveiligde toegang een toegangstoken met essentiële informatie zoals gebruikersgegevens, toepassingsgegevens en IPS / File-beleid.
4. Het toegangstoken wordt gecodeerd en ondertekend door Secure Access. Secure Access stuurt vervolgens de Secure Client samen met de token naar de FTD.
5. Wanneer het pakket de Lina-datapath bereikt, onderschept de SNI-checker de verbinding en controleert of de servernaam (SNI-extensie) in de client Hello overeenkomt met de proxy-FQDN die op het apparaat is geconfigureerd. Als SNI overeenkomt, wordt de verbinding naar ZProxy geleid. Als SNI niet overeenkomt, wordt de verbinding naar andere functies geleid die naast Universal ZTNA kunnen bestaan.

Bijvoorbeeld: VPN, Captive Portal of Clientless ZTNA. ZProxy, dat MASQUE over HTTP/2 protocol ondersteunt, wordt uitgevoerd op de FTD als een niet-Lina-proces op speciale kernen. De communicatie tussen Lina en ZProxy maakt gebruik van de NLP Tap Interface, voor het afhandelen van dataverkeer. De IP-bestemming van de verbinding wordt door de SNI-checker vertaald naar de IP-interface van de TAP.

6. Wanneer de ZProxy de mTLS-tunnelverbinding van de beveiligde client ontvangt, verifieert het het clientapparaatcertificaat dat door de beveiligde client is verzonden. Het verifieert ook het toegangstoken dat is verzonden met de APP Connect. Er is een Zero MQ-kanaal tussen Lina en ZProxy. Het wordt voornamelijk gebruikt om controleberichten uit te wisselen. ZProxy gebruikt dit kanaal voor FQDN-resolutie van privébronnen door te communiceren met Lina.

Zero MQ Channel wordt ook gebruikt om informatie in het toegangstoken naar Lina te propageren. (Voorbeeld: regel-ID, beleid-ID, enz.) Lina ontvangt de toegangstoken-informatie en slaat deze op in een metagegevensdatabase.

7. Zodra de controleberichten zijn uitgewisseld, initieert ZProxy een nieuwe verbinding met de privébron. Dit kan TCP of UDP zijn. Lina voert vervolgens een metadata-db-zoekopdracht uit voor deze app-verbinding. Als de metagegevens niet worden gevonden, wordt de verbinding verbroken
8. Aangezien de app-verbinding afkomstig is van ZProxy, heeft deze een intern IP (voorbeeld:

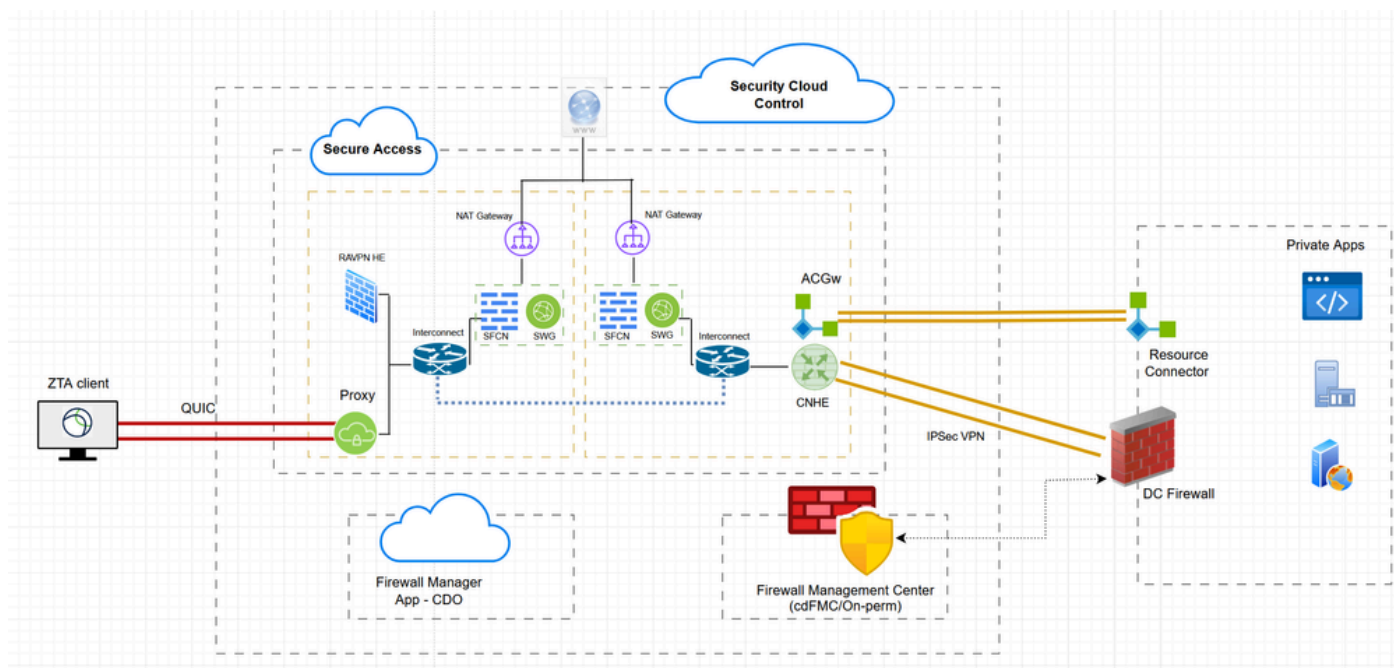
169.251.1.2) als bron-IP. Dit wordt vertaald naar de FTD-uitgang IP-interface, voordat deze wordt verzonden. Lina markeert vervolgens Universal Zero Trust-stromen voor Snort-inspectie alleen als een bestand of IPS-beleid aanwezig is in de toegangstoken. De regel-ID die is verkregen uit de toegangstoken wordt doorgegeven aan Snort in de metagegevens van de verbinding.

9. De Universal Zero Trust-regels en de bijbehorende bestands- en IPS-beleids mappings worden via het FMC naar het FTD gestuurd. De Zero Trust plugin in Snort laadt deze regels tijdens de initialisatie. Lina markeert de Universal Zero Trust stream stromen voor Snort inspectie alleen als een Bestand of IPS beleid wordt vermeld in de toegangstoken verkregen van Secure Access voor toegang tot die Private Resource.

Regel-ID verkregen uit het toegangstoken wordt doorgegeven aan Snort via Conn Meta. Voor alle Universal Zero Trust-stroomstromen voert de Zero Trust-plug-in in Snort een regel-opzoeking uit voor de regel-ID die is verkregen uit de Conn Meta. Als een overeenkomst tussen regels wordt gevonden, wordt de stroom toegestaan en worden de IPS- en bestandspolitiek die specifiek zijn voor die regel toegepast op de stroom. Als er geen overeenkomst tussen regels wordt gevonden, blokkeert de Zero Trust-plug-in in Snort de stroom.

Configureren

Netwerkdigram

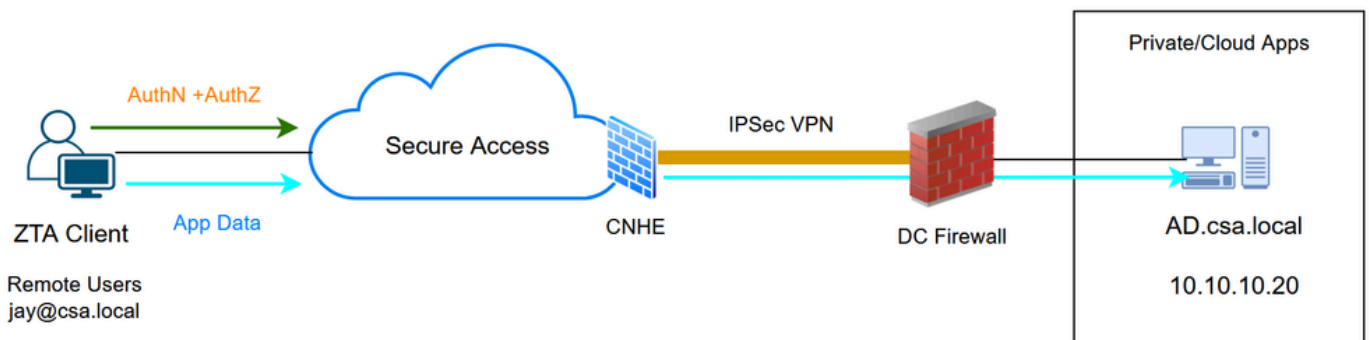


Hybride ZTNA - netwerkdigram

Testcases

Testcase 1: externe gebruiker - handhaving van de cloud

In dit testgeval zullen we via Cloud Enforcement toegang krijgen tot een privébron via Network Tunnel Group. In dit geval zullen zowel beleidsevaluatie- als toepassingsgegevens worden onderschept door Secure Access via de ZTA-module. Dit is een traditionele stroom waarbij privétoepassingen toegankelijk zijn vanaf een ZTA-geregistreerde client via Network Tunnel Group of Resource Connector



Universele ZTA - Test case topologie

Stap 1 - Een privébron definiëren voor beveiligde toegang

Configureer een privébron die toegankelijk is via een apparaat waarvoor Zero Trust Access (ZTA) is ingeschreven met cloudhandhaving

1. Navigeer naar Bronnen > Bestemmingen > Particuliere bronnen > Klik op +Toevoegen

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar contains a navigation menu with 'Resources' highlighted. The main content area displays the 'Resources' page, which includes a search bar, a filter for 'Private Resource Group', and a table of resources. The table has columns for Private Resource Group, Connection Method, Connector Groups, Accessed by, Rules, and Total Requests. Three resources are listed, all using 'Client-based ZTA' as the connection method.

Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules	Total Requests
-	Client-based ZTA	-	0	2	0
-	Client-based ZTA	1	0	2	0
-	Client-based ZTA	-	0	2	0

Veilige toegang - Configuratie van privébronnen

2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.

← Private Resources

Add a Private Resource

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure private resources in order to choose them as destinations when creating access rules. [Help](#)

General

Private Resource Name
AD-Server

Description (optional)
Active Directory server

Veilige toegang - Configuratie van privébronnen

3. Voer het FQDN in van de privébron die u wilt openen. We kunnen ook het IP-adres van de privébron definiëren. Zie [Een privébron toevoegen voor](#) meer informatie

4. Selecteer de interne DNS-server om het domein op te lossen

Private resource address

Define how the private resource will connect to applications through Secure Access.

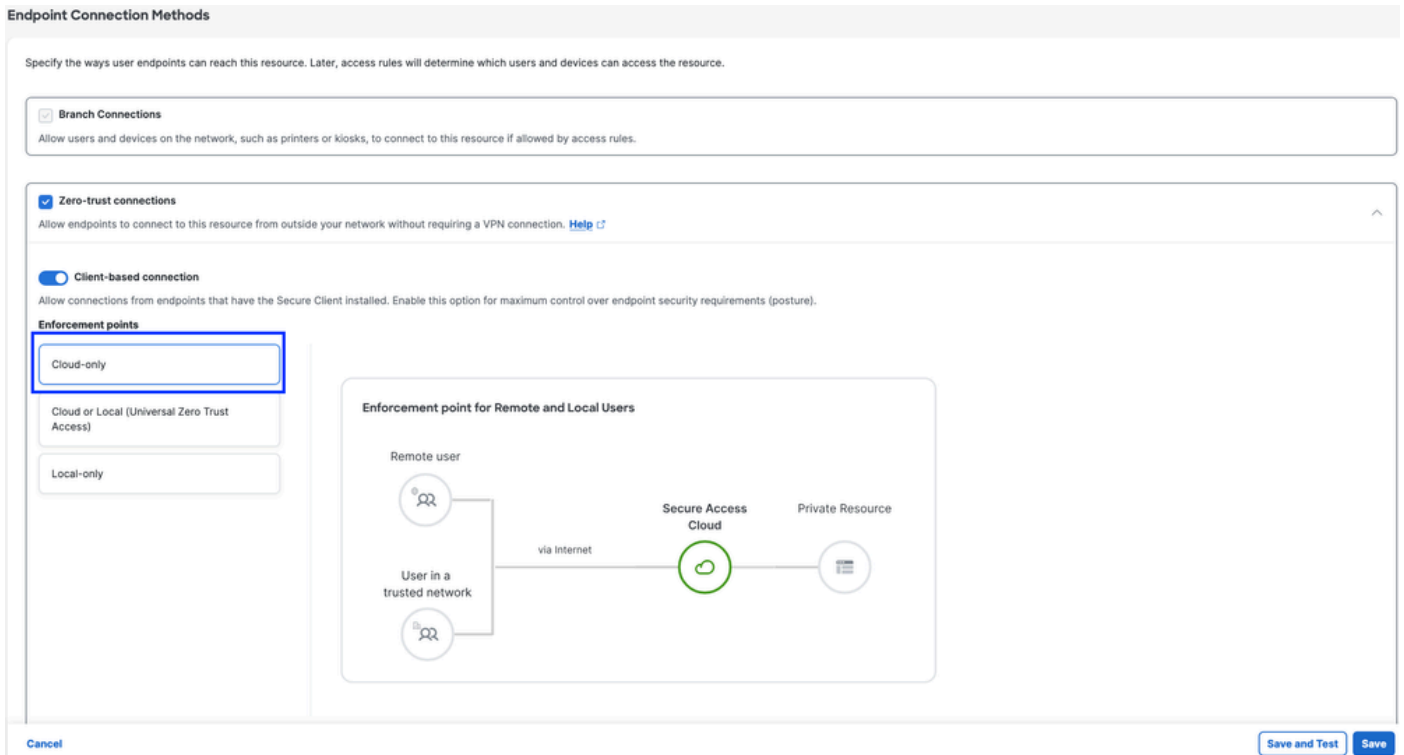
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
ad.csa.local	TCP - RDP	Any	+ Protocol & Port
Remove			
10.10.10.20	TCP - RDP	Any	+ Protocol & Port
Remove + IP Address/FQDN			

Use internal DNS server to resolve the domain PrivateDNS (10.10.10.20) ^

Internal DNS Server
PrivateDNS (10.10.10.20)

Veilige toegang - Configuratie van privébronnen

5. Selecteer methoden voor eindpuntverbinding



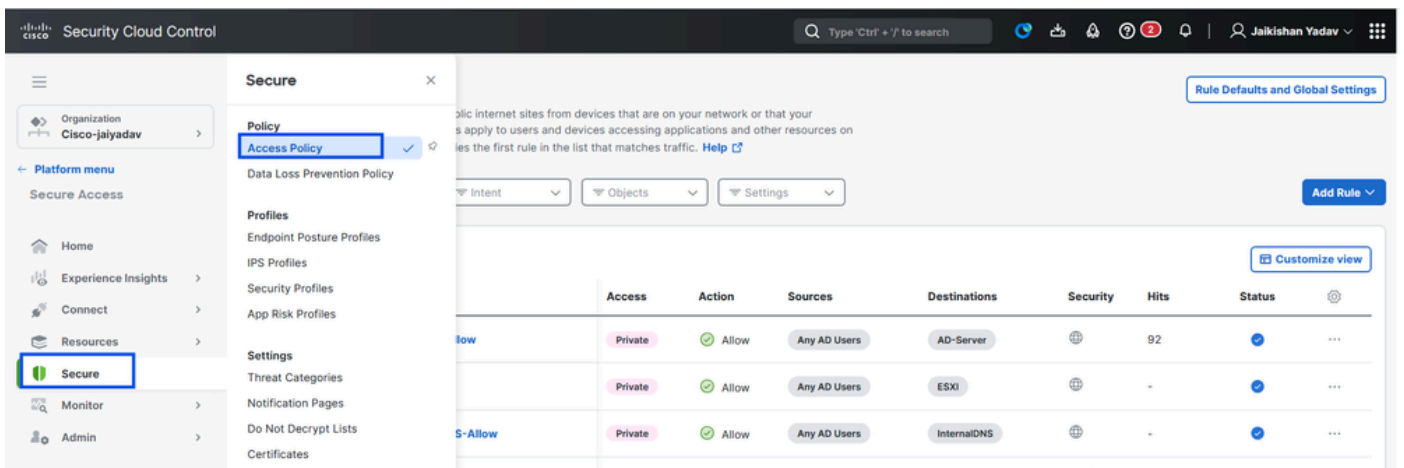
Veilige toegang - Configuratie van privébronnen

6. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie [Private Access Rule](#)

1. Navigeer naar Beveiligd > Toegangsbeleid



Beveiligde toegang - Configuratie toegangsbeleid

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.

Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.

Access Policy Rule Defaults and Global Settings

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name Intent Objects Settings Add Rule ^

	#	Rule name	Access	Action	Sources	Destinations	Security
<input type="checkbox"/>	1	BlockPage-TEST	Internet	Block	Any	Generative A...	🌐
<input type="checkbox"/>	2	RAVPN-Allow	Internet	Allow	Any AD Users	Any	🌐🔒

Rows per page 1-2 of 2 < 1 >

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen

Add AD-RDP-Allow

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled Logging is enabled [Edit](#)

Summary

Sources: Any — Allow — Security Controls — Destinations: Any private destination

Rule name: AD-RDP-Allow Rule order: 1

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action:

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From: To:

Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming

Rule name: Rule order:

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#)

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From
Specify one or more sources.

To
Specify one or more destinations.

+ AND

Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is installed.

Profile: **None** | Requirements: **None**

Private Resources: **AD-Server**

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval Rule Defaults Disabled

Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

[Cancel](#)

[Back](#)

[Next](#)

Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren

✓ **Specify Access**
Specify which users and endpoints can access which resources. [Help](#)

2 **Configure Security**
Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) [Rule Defaults](#) ⏻ Disabled

Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile [Rule Defaults](#)

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

[Cancel](#) [Back](#) [Save](#)

Beveiligde toegang - Configuratie toegangsbeleid

7. Klik op Opslaan

Access Policy [Rule Defaults and Global Settings](#)

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name Intent Objects Settings [Add Rule](#)

3 Rules [Customize view](#)

<input type="checkbox"/>	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	<input type="text"/>
<input type="checkbox"/>	1	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	🌐	-	🟢	⋮
<input type="checkbox"/>	2	BlockPage-TEST	Internet	Block	Any	Generative A...	🌐	-	🟢	⋮
<input type="checkbox"/>	3	RAVPN-Allow	Internet	Allow	Any AD Users	Any	🌐🔒	492	🟢	⋮

Rows per page: 100 1-3 of 3 1

Default Access Rules

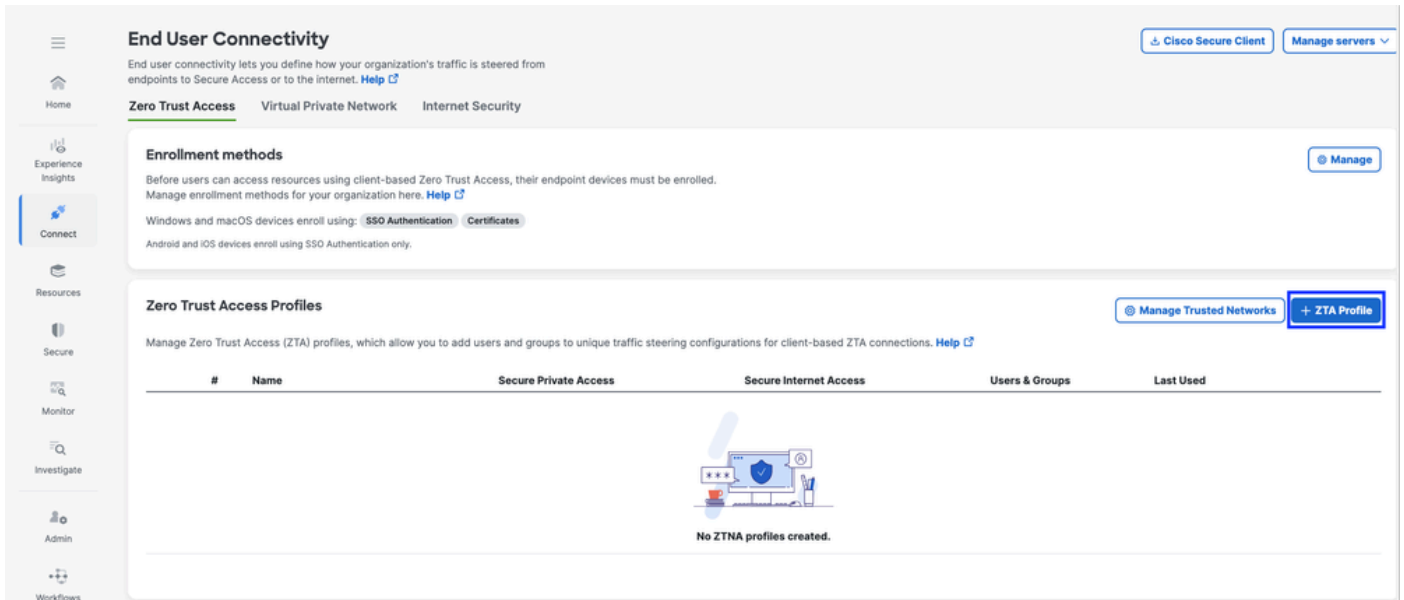
Rule name	Action	Sources	Destinations	Security	Posture	<input type="text"/>
For all private access	Block	Any	Any private destination	-	-	⋮
For all Internet access	Allow	Any	Any Internet destination	🌐🔒	-	⋮

Beveiligde toegang - Configuratie toegangsbeleid

Stap 3 Voeg privé-bronnen toe aan het ZTA-profiel

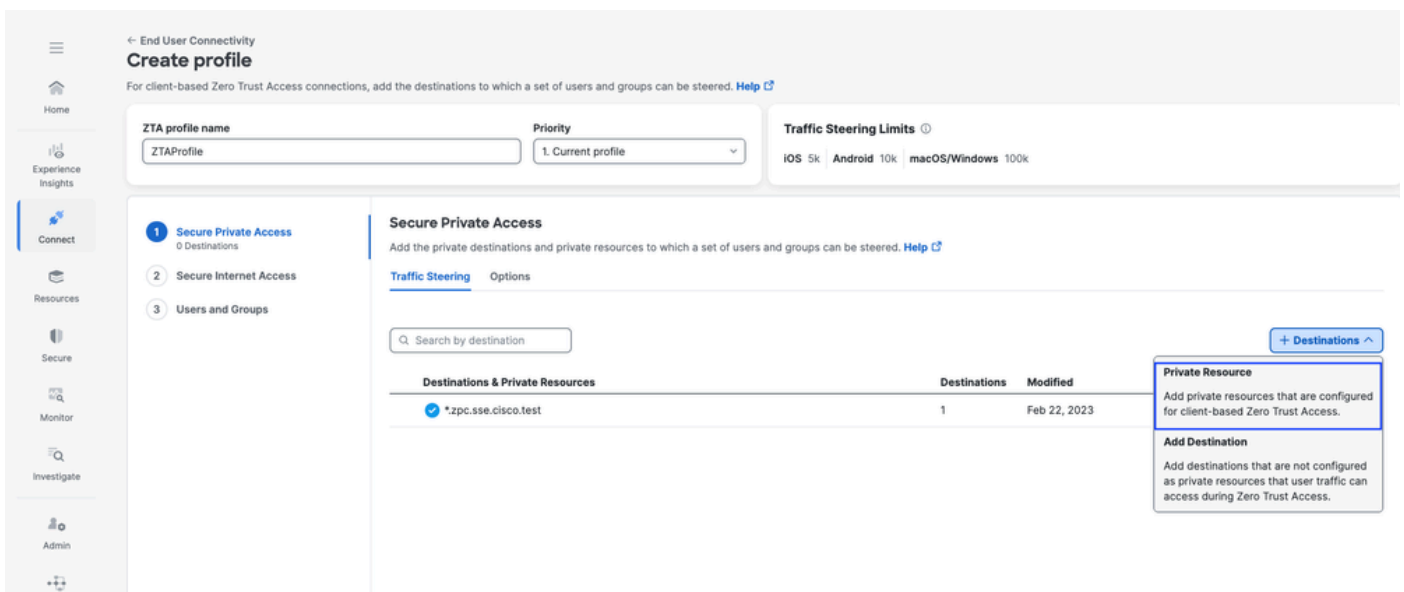
Als u een aangepast ZTA-profiel gebruikt, moet u de respectieve privébron toevoegen aan het ZTA-profiel

1. Navigeer naar Verbinden > Connectiviteit voor eindgebruikers > Toegang tot vertrouwensrelatie opheffen en klik op +ZTA-profiel

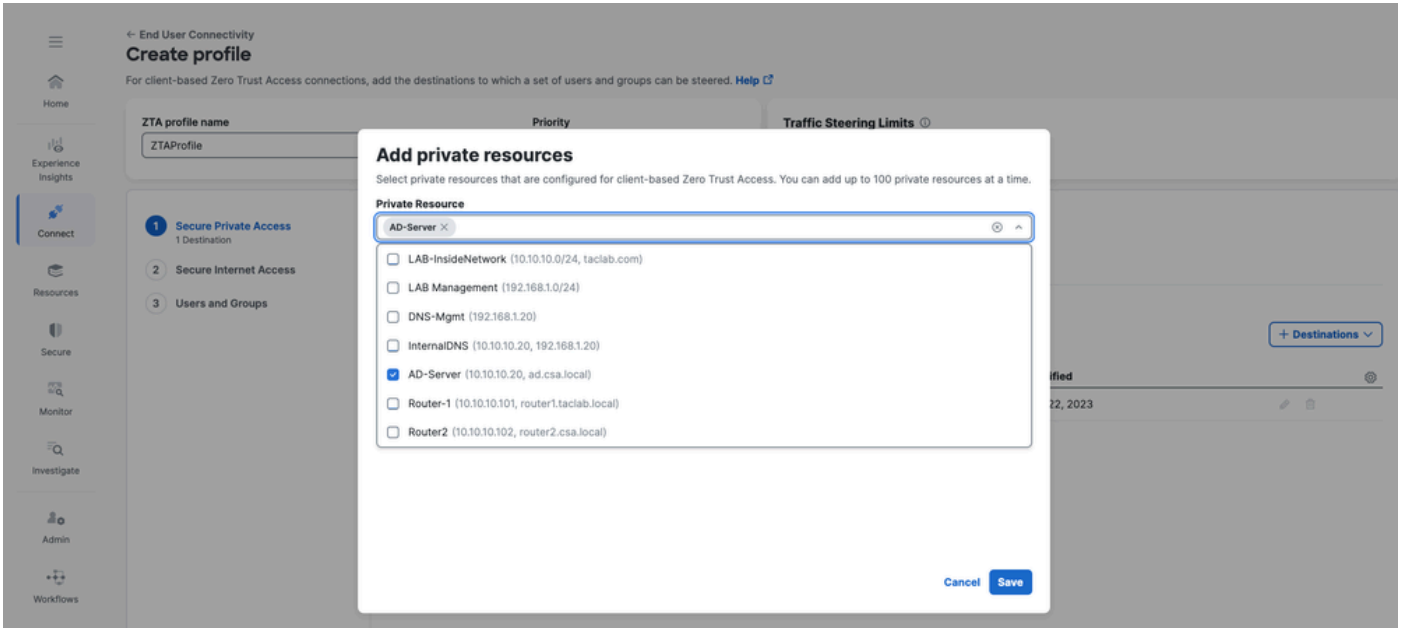


Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

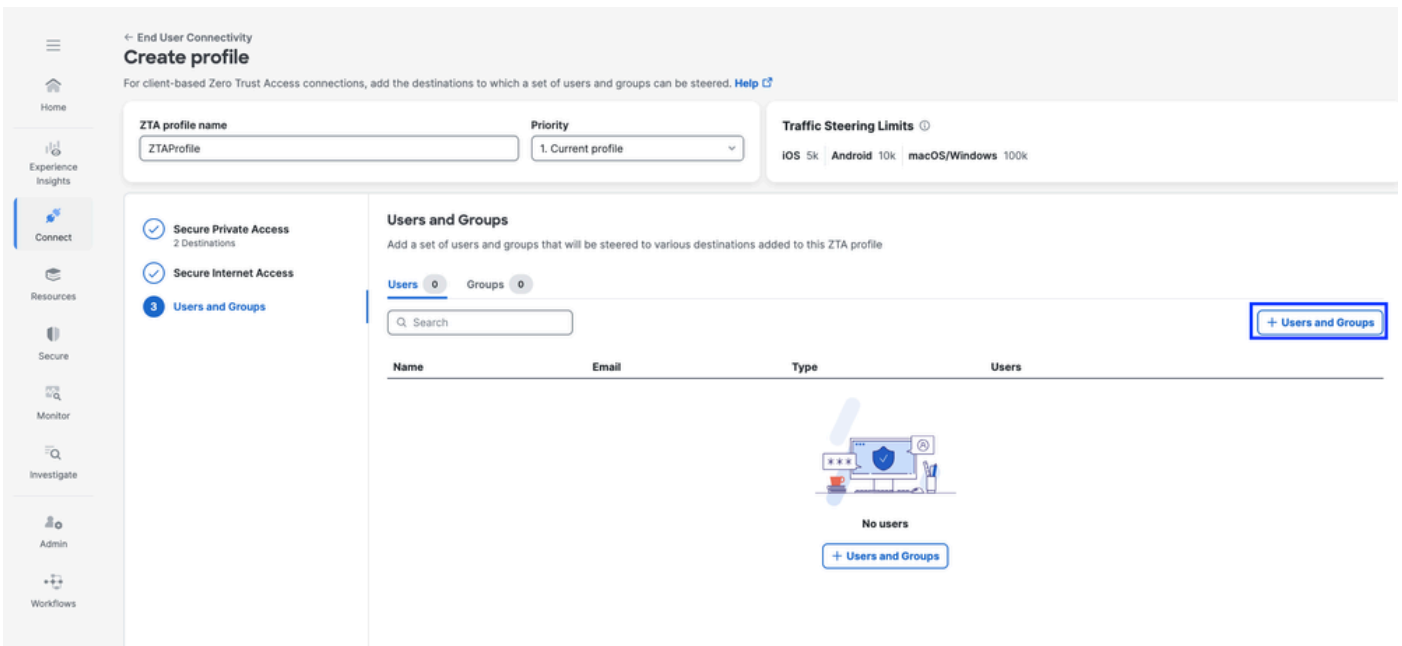


Veilige toegang - ZTA-profiel



Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen



ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

Secure Private Access (2 Destinations) | Secure Internet Access | **Users and Groups**

Users and Groups
Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users 1 | Groups 0

Q Search + Users and Groups

Name	Email	Type	Users
jay (jay@csa.local)	jay@gmail.com	User	-

Rows per page: 10

Back Close

Veilige toegang - ZTA-profiel

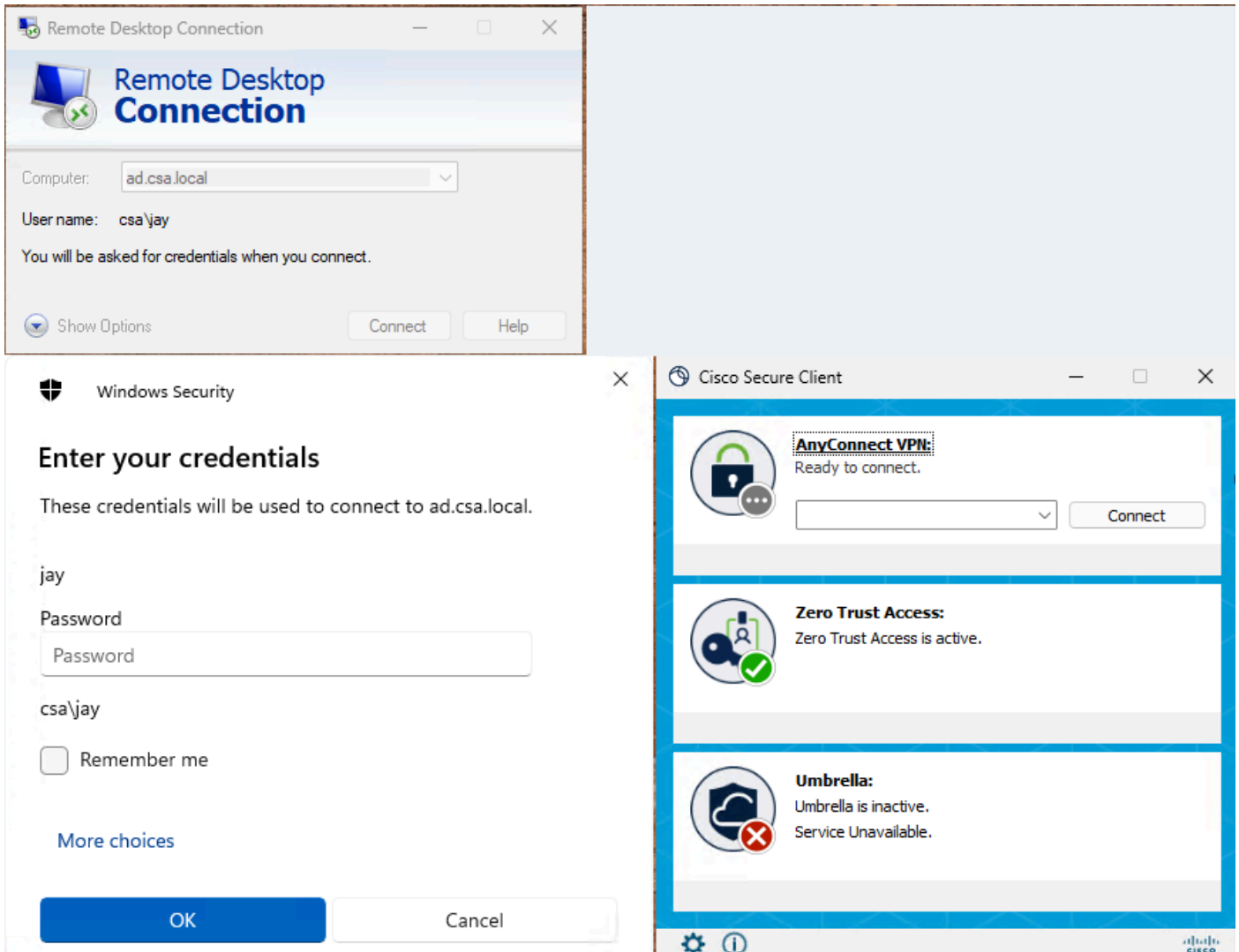


Opmerking: het kan tot 15-20 minuten duren om de configuratie te pushen en te synchroniseren met de client voor de toegewezen privébron

Stap 4: Controleer de toegang tot de privébron

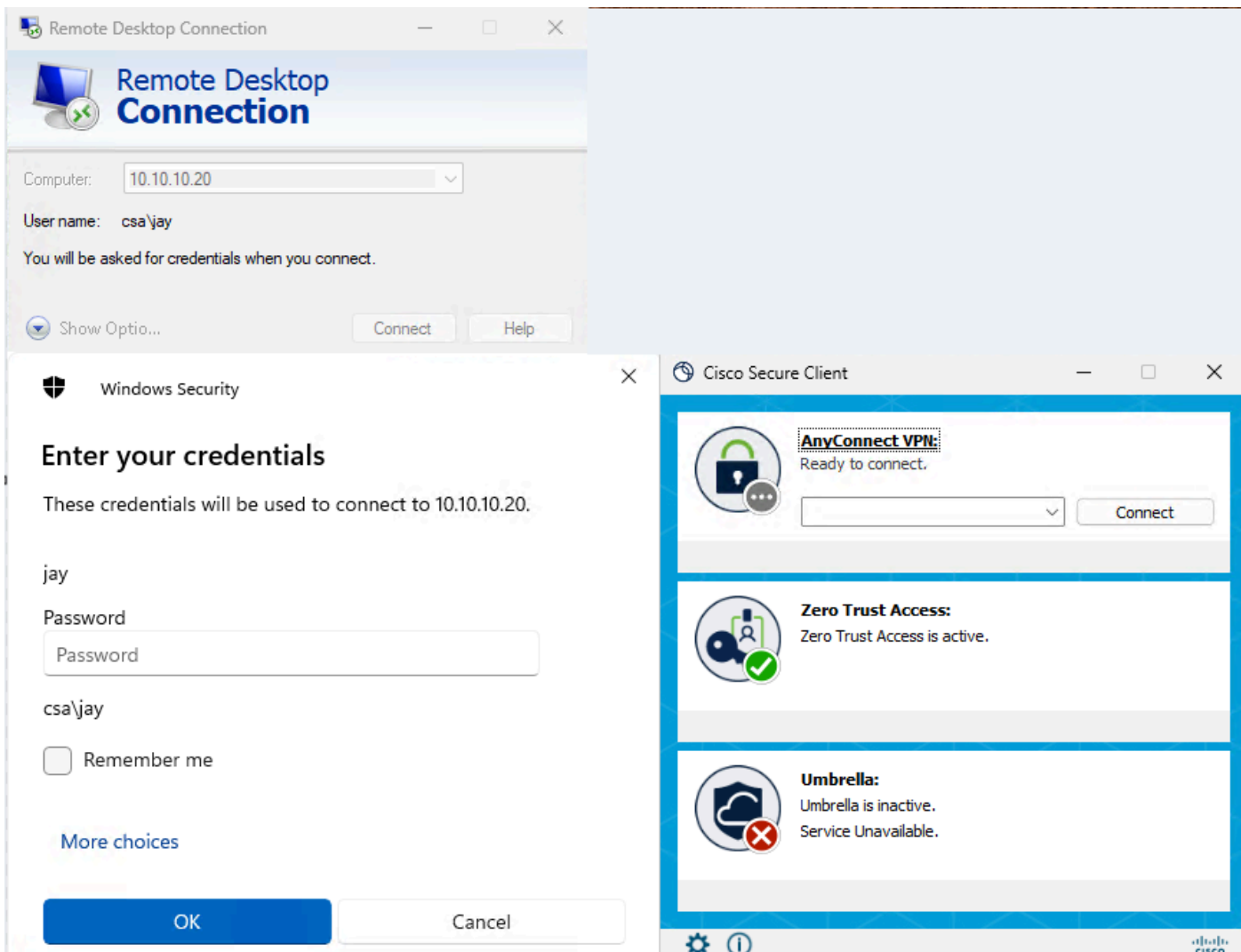
1. Toegang tot de particuliere middelen

Toegang tot de PR via FQDN



Veilige toegang - PR-testen

Toegang tot de PR via IP-adres



Veilige toegang - PR-testen

2. Verifiëren met de gebeurtenissen voor het zoeken naar activiteiten

Activity Search

Schedule Export CSV LAST 24 HOURS

FILTERS Search by domain, identity, or URL Advanced CLEAR Saved Searches Customize Columns ZTA Client-based

IP ADDRESS 10.10.10.20 RESPONSE Allowed Restore to default layout Save Search

3 Total Viewing activity from Jan 11, 2026 4:49 AM to Jan 12, 2026 4:49 AM Page: 1 Results per page: 50 1 - 3 of 3

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Applica
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server

Veilige toegang - zoeken naar activiteiten

Activity Search

Schedule Export CSV LAST 24 HOURS

Activity Search interface showing filters and event details.

Filters: IP ADDRESS 10.10.10.20, PORT 3389

Search filters: Response (Allowed, Blocked), Identity Type (AD Users, AD Groups, AD Devices, SAML Users), Enforced By (Secure Access Cloud, FTD, Umbrella Cloud)

Event Details:

- Identity: jay (jay@csa.local)
- Win1
- Rule Name: AD-RDP-Allow
- Resource/Application: AD-Server
- Zero Trust Access Profile: Default ZTA Profile
- Trusted Network: No Match
- Enforcement Point: Secure Access Cloud
- Destination: ad.csa.local
- Destination IP: 10.10.10.20

Request	Source	Action	Destination	Destination IP	Destination Port
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389

Veilige toegang - zoeken naar activiteiten

Activity Search interface showing a list of search results.

Filters: IP ADDRESS 10.10.10.20

Search filters: Response (Allowed, Blocked), Identity Type (AD Users, AD Groups)

9 Total Viewing activity from Jan 11, 2026 5:51 AM to Jan 12, 2026 5:51 AM

Request	Source	Action	Destination	Destination IP	Destination Port	Resource/Application	Zero Trust Access Profile	Rule Name	OS
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win

Veilige toegang - zoeken naar activiteiten

Activity Search

Schedule Export CSV LAST 24 HOURS

Search by domain, identity, or URL Advanced CLEAR

Filters: IP ADDRESS 10.10.10.20 X Saved Searches Customize Columns ZTA Client-based Save Search

9 Total Viewing activity from Jan 11, 2026 5:51 AM to Jan 12, 2026 5:51 AM Page: 1 Results per page: 50 1 - 9 of 9

Request	Source	Action	Destination	Destination IP	Destination Port	Resource/Application
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 12, 2026 5:51 AM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: AD-RDP-Allow

Resource/Application: AD-Server

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: 10.10.10.20

Destination IP

Veilige toegang - zoeken naar activiteiten

3. FMC-verbingsgebeurtenissen controleren

Events Troubleshooting

Destination Port / ICMP Code 3389

7 events Last 1 hour

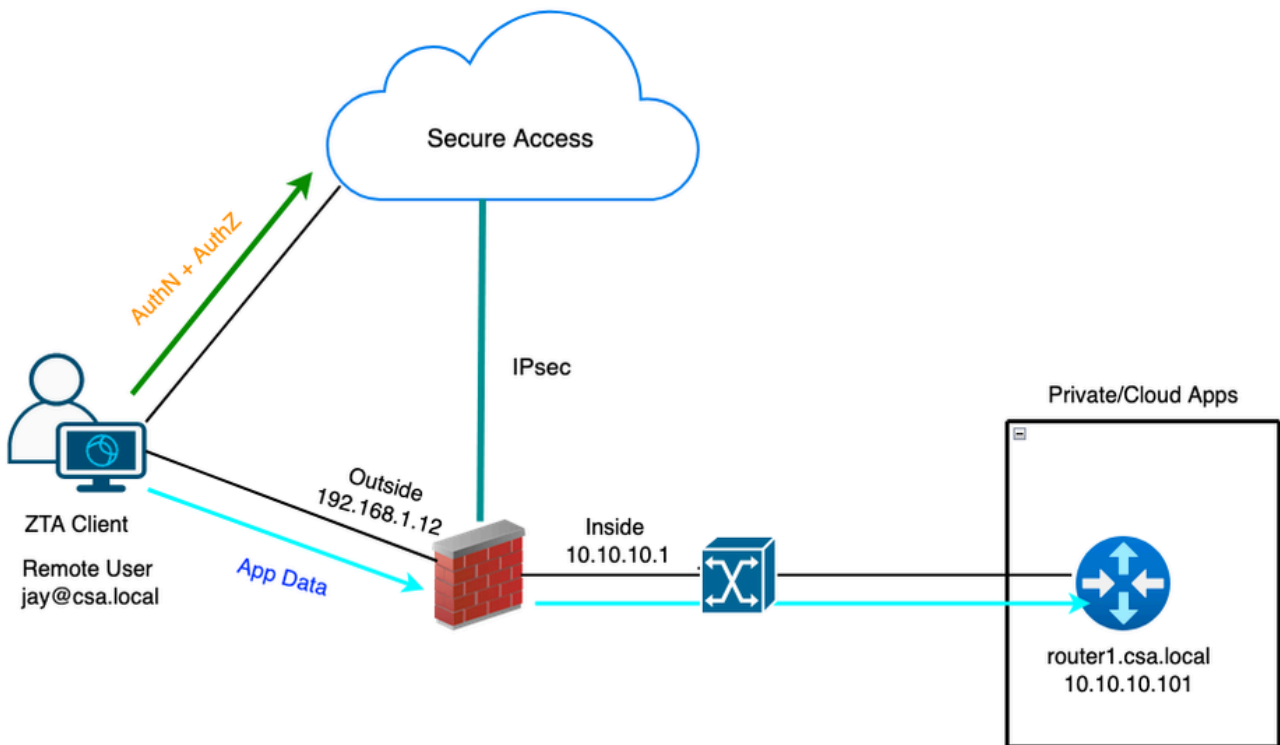
Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Web Application	Access Control Rule
2026-01-12 00:51:24	Connection	Fastpath		100.112.20.48	10.10.10.20	17674 / tcp	3389 / tcp		
2026-01-12 00:51:20	Connection	Fastpath		100.112.20.48	10.10.10.20	47021 / tcp	3389 / tcp		
2026-01-12 00:51:15	Connection	Fastpath		100.112.20.48	10.10.10.20	63712 / tcp	3389 / tcp		
2026-01-12 00:48:24	Connection	Fastpath		100.112.20.48	10.10.10.20	50756 / tcp	3389 / tcp		
2026-01-12 00:42:34	Connection	Fastpath		100.112.72.18	10.10.10.20	60548 / tcp	3389 / tcp		
2026-01-12 00:15:21	Connection	Fastpath		100.112.72.16	10.10.10.20	40660 / tcp	3389 / tcp		
2026-01-12 00:12:45	Connection	Fastpath		100.112.72.16	10.10.10.20	44262 / tcp	3389 / tcp		

FMC-verbingsgebeurtenissen

Testcase 2 - Externe gebruiker - Lokale handhaving

Toegang tot een Private Resource via lokale handhaving, in dit soort evaluatie van het handhavingsbeleid gebeurt op Secure Access, maar de toepassingsgegevens blijven lokaal voor FTD. Bijvoorbeeld een ZTA-geregistreerde client of gebruiker die is verbonden met het thuisnetwerk en probeert toegang te krijgen tot een privébron die zich achter de FTD-interface

bevindt.



Universele ZTA - Test case topologie

Stap 1 - Een privébron definiëren voor beveiligde toegang

Configureer een privébron die toegankelijk is via een apparaat waarvoor Zero Trust Access (ZTA) is ingeschreven met cloudhandhaving

1. Navigeer naar Bronnen > Bestemmingen > Particuliere bronnen > Klik op +Toevoegen

The screenshot shows the Cisco Security Cloud Control interface. The 'Resources' section is open, and the 'Private Resource' option is highlighted in the 'Destinations' list. The main area shows a table of Private Resources with columns for Private Resource Group, Connection Method, Connector Groups, Accessed by, Rules, and Total Requests.

Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules	Total Requests
-	Client-based ZTA	-	0	2	0
-	Client-based ZTA	1	0	2	0
-	Client-based ZTA	-	0	2	0

Veilige toegang - Configuratie van privébronnen

2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.

← Private Resources

Add a Private Resource

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure private resources in order to choose them as destinations when creating access rules. [Help](#)

General

Private Resource Name
Router1

Description (optional)
Router1 PR for UZTNA testing

Veilige toegang - Configuratie van privébronnen

3. Voer het FQDN in van de privébron die u wilt openen. We kunnen ook het IP-adres van de privébron definiëren. Zie [Een privébron toevoegen voor](#) meer informatie

4. Selecteer de interne DNS-server om het domein op te lossen

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR)	Protocol	Port / Ranges
router1.csa.local	Any TCP	22
10.10.10.101	Any TCP	22

Use internal DNS server to resolve the domain

Internal DNS Server: PrivateDNS (10.10.10.20)

Veilige toegang - Configuratie van privébronnen

5. Selecteer methoden voor eindpuntverbinding

6. Selecteer FTD als lokale handhavingpunten

Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

Branch Connections

Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by access rules.

Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... X Search by FTD na...

Traffic from users within a trusted network will get enforced at the selected Firewalls.

Enforcement point for Remote User



Enforcement point for Local user



Internal remote addresses are visible on end-user devices. If you want an address to be hidden, use an external address.

Change the remotely reachable addresses

Cancel

Save and Test

Save

Veilige toegang - Configuratie van privébronnen



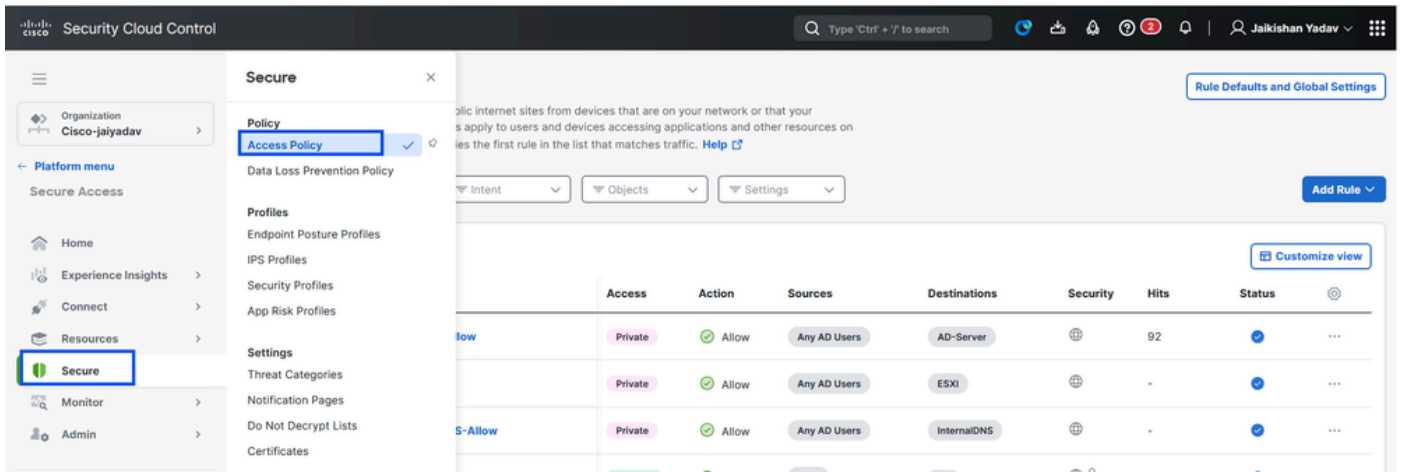
Opmerking: afhankelijk van het type inschrijving dat u selecteert, wordt de PR automatisch gekoppeld aan de FTD en wordt een beleidsimplementatie geactiveerd

7. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie [Private Access Rule](#)

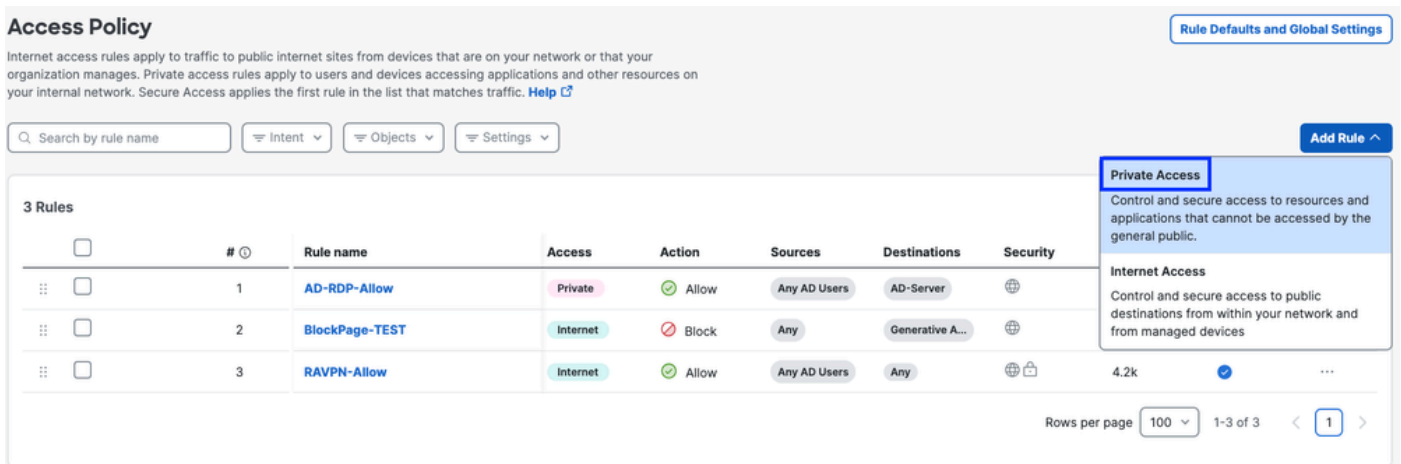
1. Navigeer naar Beveiligd > Toegangsbeleid



Veilige toegang - Configuratie van privébronnen

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.

Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.



Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen

Add Router1-SSH

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming

Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

From

Specify one or more sources.

AD Users - Any AD Users

To

Specify one or more destinations.

Private Resources - Router1

+ AND

Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile [Rule Defaults](#)

Requirements for end-user devices on which the Cisco Secure Client is installed.

Profile: **None** | Requirements: **None**

Private Resources: **Router-1**

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval [Rule Defaults](#)

Disabled

Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access.

When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

[Cancel](#)

[Back](#) [Next](#)

Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) [Rule Defaults](#)

Disabled

Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile [Rule Defaults](#)

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

[Cancel](#)

[Back](#) [Save](#)

Beveiligde toegang - Configuratie toegangsbeleid

7. Klik op Opslaan

Access Policy

Rule Defaults and Global Settings

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name Intent Objects Settings

Add Rule

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	Router1-SSH	Private	Allow	Any AD Users	Router1		-	✓
2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		-	✓
3	BlockPage-TEST	Internet	Block	Any	Generative A...		8.8k	✓
4	RAVPN-Allow	Internet	Allow	Any AD Users	Any		715	✓

Rows per page: 100 1-4 of 4 < 1 >

Beveiligde toegang - Configuratie toegangsbeleid

Stap 3 - Controleer de associatie van PR op de FTD

1. Navigeer naar Verbinden > Netwerkverbindingen > FTD's

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' panel with 'Essentials' and 'Network Connections' (checked) visible. Below this, there are statistics for 'FTDs' showing 0 Warning and 1 Connected. The interface also shows a 'Tunnel Groups' section with 'FTDs' highlighted and a '+ Add' button.

Veilige toegang - PR-verificatie

2. Klik op FTD > Bronnen weergeven die aan deze FTD zijn gekoppeld

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve end-user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Q Search by FTD name FMC Name Configuration status 1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associa
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced	1

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local
Auto deployment: Yes

UZTA Configuration status

Synced Last synced at 31 Dec 2025, at 2:51 AM UTC

Assigned Trusted Network

Trusted network	Networks
LAN (Default trusted network)	1 DNS Servers

[Edit assignment](#) + [Trusted network](#)

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status	
Synced	1

[View resources associated to this FTD](#)

[Associate Resources](#)

Veilige toegang - PR-verificatie

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

Q Search by resource name

Configuration status

1 Resources

[Associate Resources](#)

Resource name

Status

Router1

Synced

[Close](#)

Veilige toegang - PR-verificatie

3. Klik op sluiten

4. Controleer de status. De bijbehorende bron en configuratie moeten in gesynchroniseerde toestand zijn

The screenshot displays the 'Network Connections' section of the Palo Alto Networks management console. It shows a table of FTDs configured for Universal Zero Trust Access. The table has columns for FTD Name, Version, FMC, UZTA Configuration status, and Associated Resources. The 'FMC_FTD' entry is highlighted, showing it is 'Synced'. A right-hand sidebar provides details for the selected FTD, including Firewall Details, UZTA Configuration status (Synced), and Assigned Trusted Network (LAN).

FTD Name	Version	FMC	UZTA Configuration status	Associated Resources
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced	1

Veilige toegang - PR-verificatie

5. Controleer of de configuratie is ingesteld op FTD

Meld u aan bij FTD cli en navigeer naar de LINA-modus

Toon de toepassing Running-Config Object

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftd# sh run object application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
ftd#
```

FTD - PR-verificatie

Stap 4 Voeg privé-bronnen toe aan het ZTA-profiel

1. Navigeer naar Verbinden > Connectiviteit voor eindgebruikers > Toegang tot vertrouwensrelatie opheffen en klik op 3 punten om het ZTA-profiel te bewerken

End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust Access | Virtual Private Network | Internet Security

Enrollment methods Manage

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices enroll using: **SSO Authentication** | **Certificates**

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

Manage Zero Trust Access (ZTA) profiles, which allow you to add users and groups to unique traffic steering configurations for client-based ZTA connections. [Help](#)

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	ZTAProfile	2 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	1 Users 0 Groups	Jan 25, 2026

Edit
Delete

Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

Create profile

For client-based Zero Trust Access connections, add the destinations to which a set of users and groups can be steered. [Help](#)

ZTA profile name: ZTAProfile | Priority: 1. Current profile

Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

1 Secure Private Access (0 Destinations)

2 Secure Internet Access

3 Users and Groups

Secure Private Access

Add the private destinations and private resources to which a set of users and groups can be steered. [Help](#)

Traffic Steering | Options

Search by destination

Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

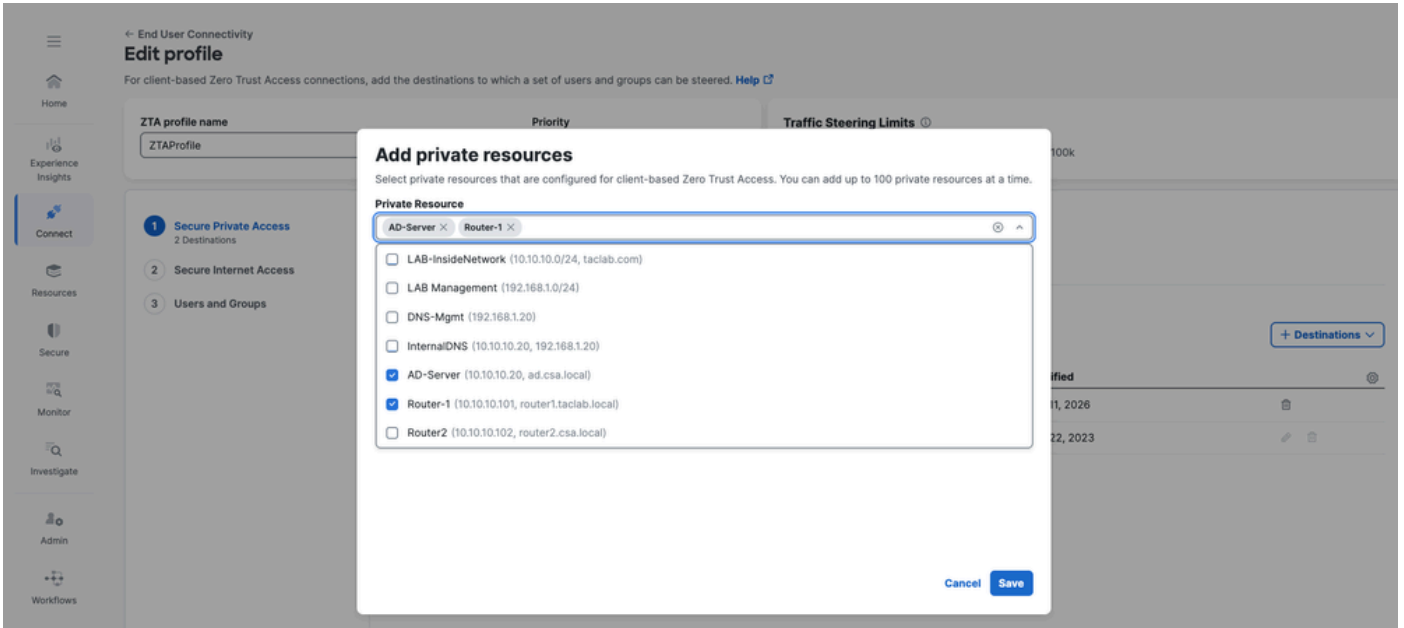
Private Resource

Add private resources that are configured for client-based Zero Trust Access.

Add Destination

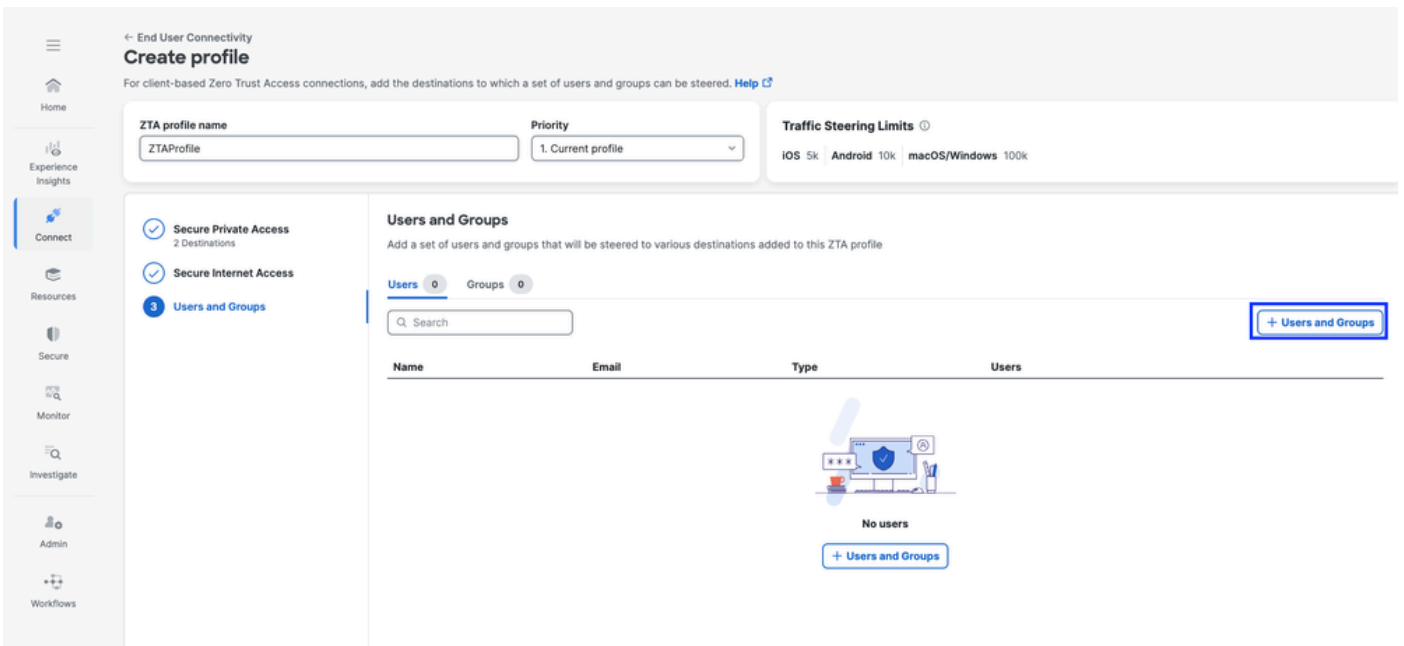
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Veilige toegang - ZTA-profiel



Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen



Veilige toegang - ZTA-profiel

ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

- Secure Private Access (2 Destinations)
- Secure Internet Access
- Users and Groups**

Users and Groups
Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users: 1 | Groups: 0

Search:

Name	Email	Type	Users
jay (jay@csa.local)	jay@gmail.com	User	-

Rows per page: 10

Back Close

Veilige toegang - ZTA-profiel

Stap 5: Controleer de toegang tot de privébron

1. Controleer of de externe gebruiker FTD FQDN kan oplossen

```
PS C:\Users\jay> ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
PS C:\Users\jay> nslookup ftd.csa.local
Server: UnKnown
Address: 192.168.1.20

Name: ftd.csa.local
Addresses: 192.168.1.12
```

Veilige toegang - PR-testen

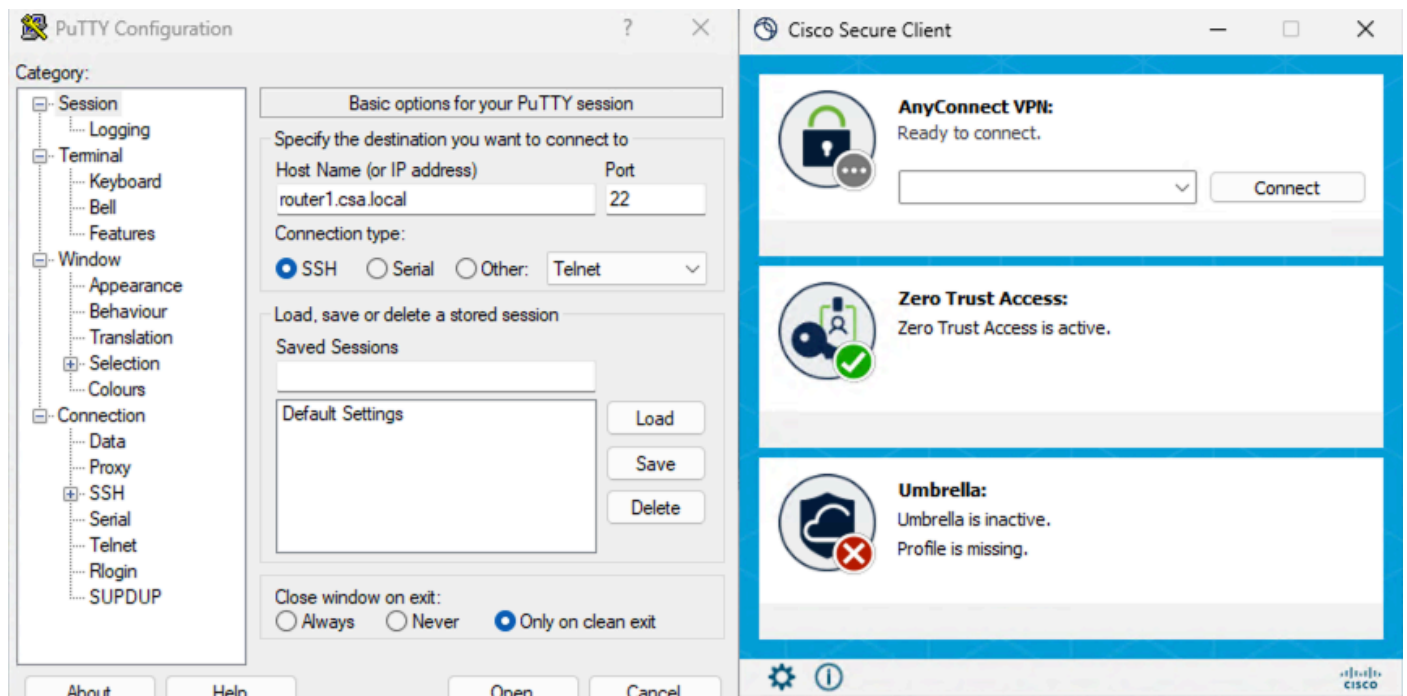
2. Controleren of FTD particuliere bronnen kan bereiken met behulp van FQDN

```
ftd> en
Password:
ftd# ping router1.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ftd# █
```

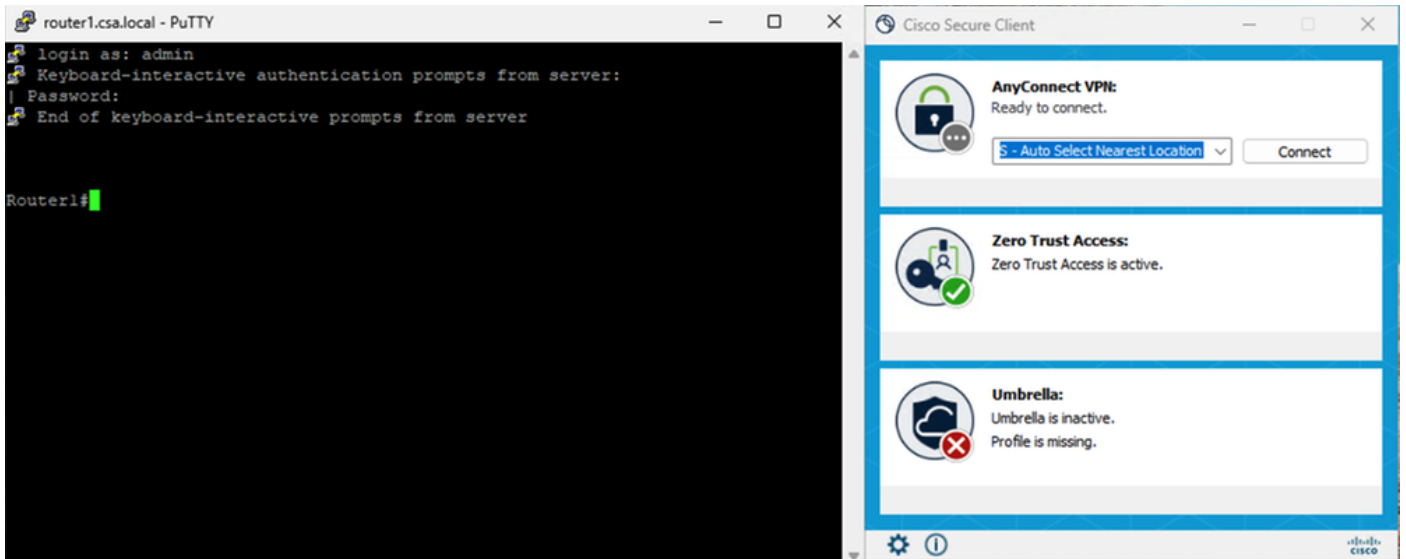
Veilige toegang - PR-testen

3. Test de SSH-verbinding met de Private Resource

Toegang tot de PR via FQDN

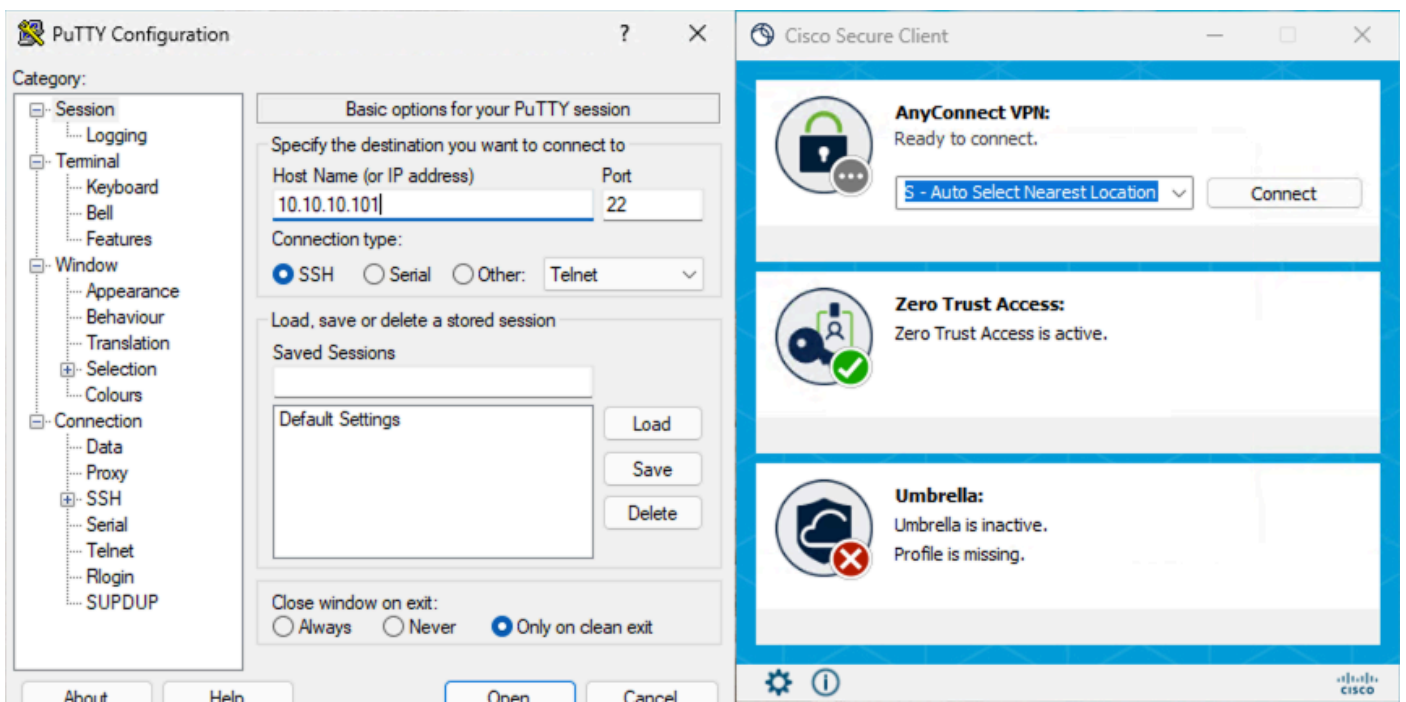


Veilige toegang - PR-testen

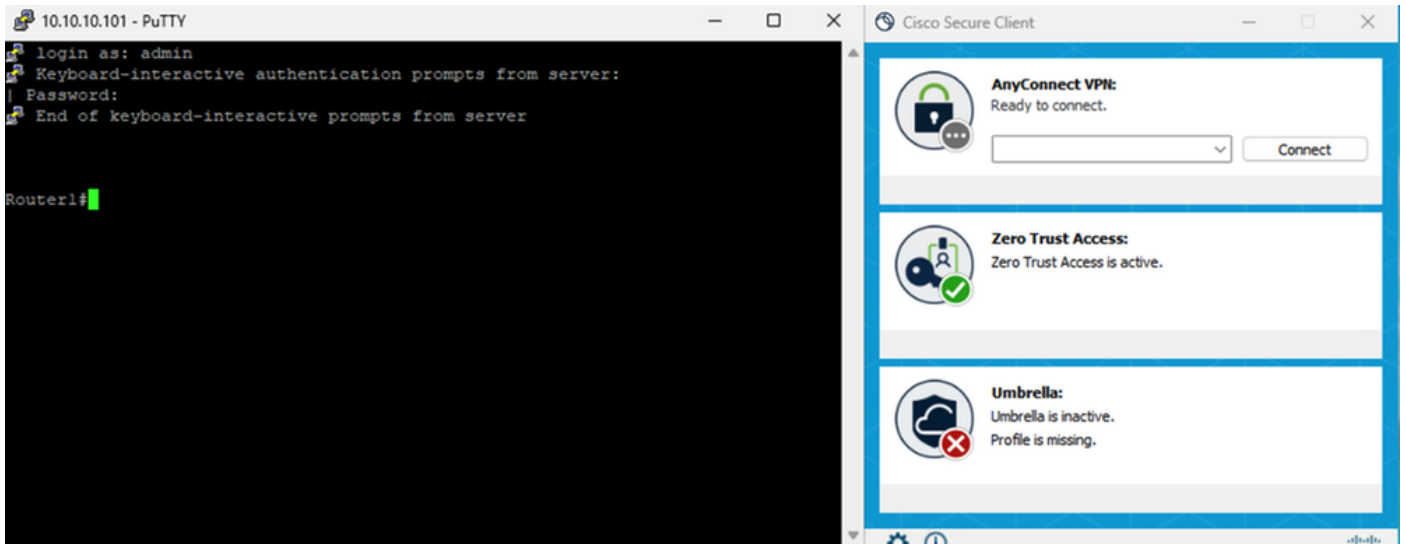


Veilige toegang - PR-testen

Toegang tot de PR via IP-adres



Veilige toegang - PR-testen



Veilige toegang - PR-testen

4. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten

Activity Search Schedule Export CSV LAST 24 HOURS

FILTERS Advanced CLEAR Saved Searches Customize Columns ZTA Client-based

DOMAIN router1.csa.local X **RESPONSE** Allowed X Restore to default layout Save Search

4 Total Viewing activity from Jan 9, 2026 5:57 PM to Jan 10, 2026 5:57 PM Page: 1 Results per page: 50 1 - 4 of 4

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location
<input checked="" type="checkbox"/> Allowed <input type="checkbox"/> Blocked	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76

Veilige toegang - zoeken naar activiteiten

4 Total Viewing activity from Jan 9, 2026 6:01 PM to Jan 10, 2026 6:01 PM Page: 1 Results per page: 50 1 - 4 of 4

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH

Event Details X

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:55 PM

Access details

Identity: jay (jay@csa.local)

Win: Win10

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD> FMC_FTD

Destination: router1.csa.local

Destination IP: -

Veilige toegang - zoeken naar activiteiten

Activity Search Schedule Export CSV LAST 24 HOURS

FILTERS Search by domain, identity, or URL Advanced CLEAR Saved Searches Customize Columns ZTA Client-based

IP ADDRESS 10.10.10.101 **RESPONSE** Allowed Restore to default layout Save Search

7 Total Viewing activity from Jan 9, 2026 6:01 PM to Jan 10, 2026 6:01 PM Page: 1 Results per page: 50 1 - 7 of 7

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location	Location IP
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.38.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.38.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.38.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.38.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.38.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.38.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.38.159.129

Response Select All
 Allowed Advanced
 Blocked

Identity Type Select All
 AD Users
 AD Groups
 AD Devices
 SAML Users

Enforced By Select All
 Secure Access Cloud
 FTD
 Umbrella Cloud

Veilige toegang - zoeken naar activiteiten

7 Total Viewing activity from Jan 9, 2026 6:09 PM to Jan 10, 2026 6:09 PM Page: 1 Results per page: 50 1 - 7 of 7

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Destination Country	Internal IP	External IP	Action	Categories
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	

Event Details ×

Action
Allowed

Block Reason
-

Connection Method
ZTA Client-based

Time
Jan 10, 2026 5:56 PM

Access details

Identity
jay (jay@csa.local)

Win1

Rule Name
Router1-SSH

Resource/Application
Router1

Zero Trust Access Profile
Default ZTA Profile

Trusted Network
No Match

Enforcement Point
FTD> FMC_FTD

Destination
10.10.10.101

Destination IP
10.10.10.101

Veilige toegang - zoeken naar activiteiten

5. FMC-verbindingsgebeurtenissen controleren

Firewall Management Center Events & Logs / Analysis / Unified Events Search Deploy admin

Events Troubleshooting

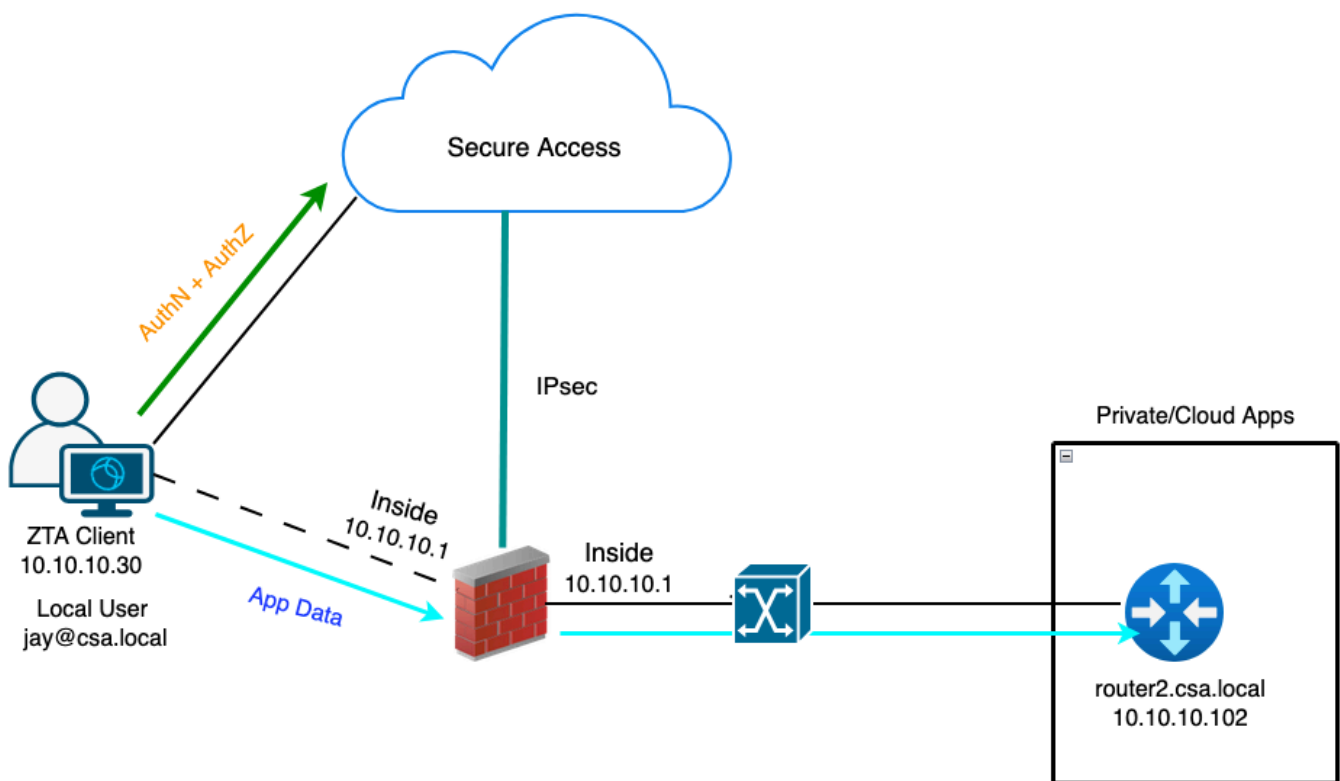
Monitor Destination IP: 10.10.10.101 Refresh

Insights & Reports 6 events Last 1 hour Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Web Application	Access Control Rule	Access Control Policy
2026-01-10 12:56:23	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.101	42217 / tcp	22 (ssh) / tcp			
2026-01-10 12:56:16	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.101	27221 / tcp	22 (ssh) / tcp			
2026-01-10 12:55:28	Connection	Allow	Zero Trust Flow	169.254.1186	10.10.10.101	50425 / tcp	22 (ssh) / tcp			
2026-01-10 12:54:46	Connection	Allow	Zero Trust Flow	169.254.1188	10.10.10.101	39499 / tcp	22 (ssh) / tcp			
2026-01-10 12:50:25	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.101	22631 / tcp	22 (ssh) / tcp			
2026-01-10 12:47:08	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.101	24739 / tcp	22 (ssh) / tcp			

Testcase 3 - Lokale gebruiker - Lokale handhaving

Toegang tot een Private Resource via lokale handhaving als een lokale gebruiker, in dit type van handhaving beleid evaluatie gebeurt op Secure Access, maar de applicatie gegevens blijft lokaal voor FTD. Bijvoorbeeld een ZTA-geregistreerde client of gebruiker die is verbonden met het thuisnetwerk en probeert toegang te krijgen tot een privébron die zich achter de FTD-interface bevindt. Als de private resource zich achter DMZ of een andere interface van de FTD bevindt, moeten we een toegangsregel op de FTD maken om het verkeer tussen Client IP of netwerk en Private Resource mogelijk te maken.

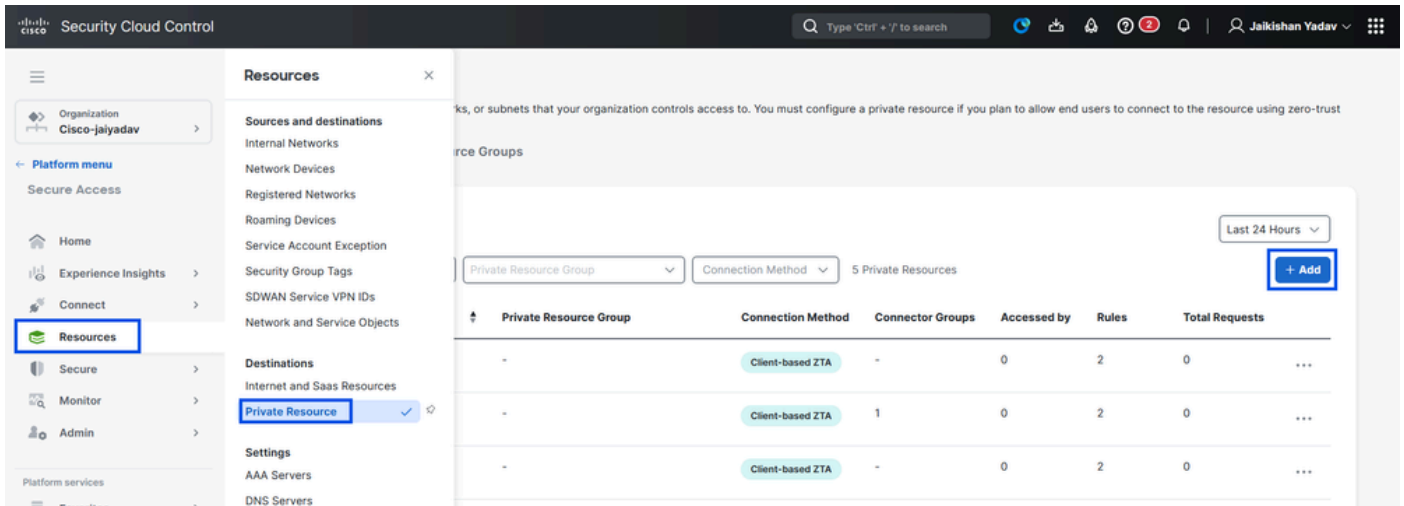


Universal ZTA - Test Case Topology

Stap 1 - Een privébron definiëren voor beveiligde toegang

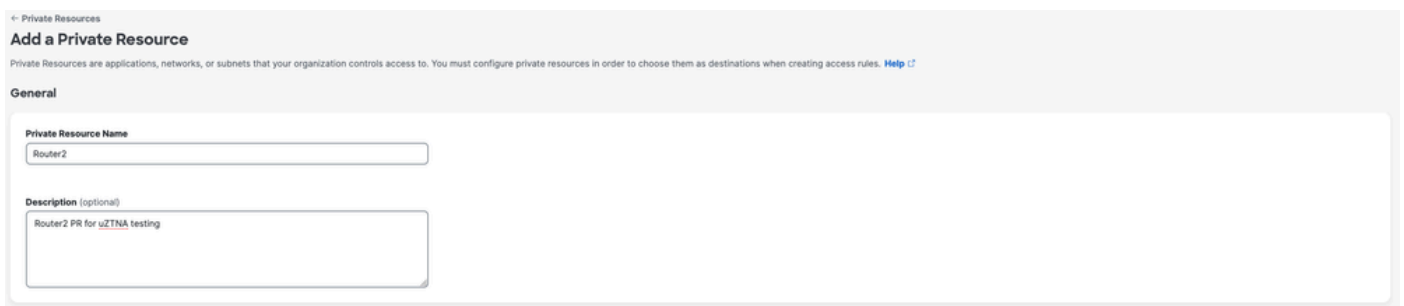
Configureer een privébron die toegankelijk is via een apparaat waarvoor Zero Trust Access (ZTA) is ingeschreven met cloudhandhaving

1. Navigeer naar Bronnen > Bestemmingen > Particuliere bronnen > Klik op +Toevoegen



Veilige toegang - Configuratie van privébronnen

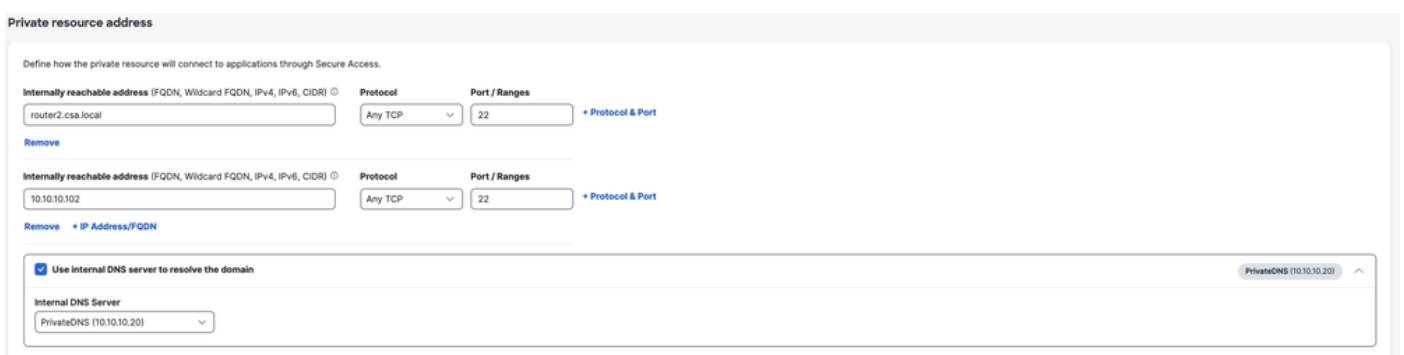
2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.



Veilige toegang - Configuratie van privébronnen

3. Voer het FQDN in van de privébron die u wilt openen. We kunnen ook het IP-adres van de privébron definiëren. Zie [Een privébron toevoegen voor](#) meer informatie

4. Selecteer de interne DNS-server om het domein op te lossen



5. Selecteer methoden voor eindpuntverbinding

6. Selecteer FTD als lokale handhavingpunten

Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

Branch Connections
Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by access rules.

Zero-trust connections
Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

Traffic from users within a trusted network will get enforced at the selected Firewalls.

Enforcement point for Remote User

Remote user — via internet — Local Firewall — Private Resource

Enforcement point for Local user

User in a trusted network — via local network — Local Firewall — Private Resource

Internal remote addresses are visible on end-user devices. If you want an address to be hidden, use an external address.

Change the remotely reachable addresses

Cancel Save and Test Save



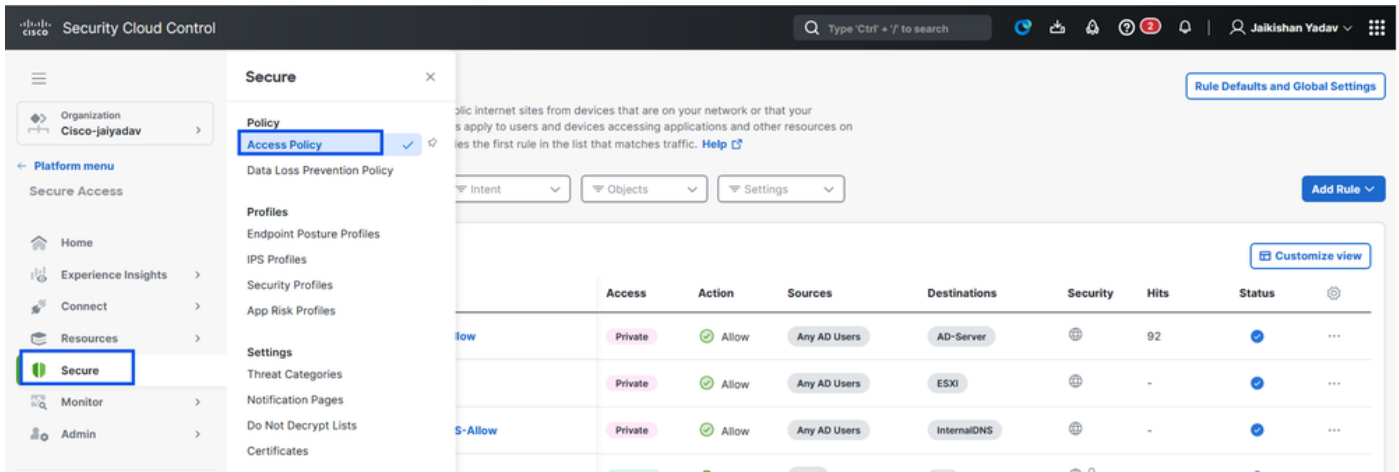
Opmerking: afhankelijk van het type inschrijving dat u selecteert, wordt de PR automatisch gekoppeld aan de FTD en wordt een beleidsimplementatie geactiveerd

7. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie [Private Access Rule](#)

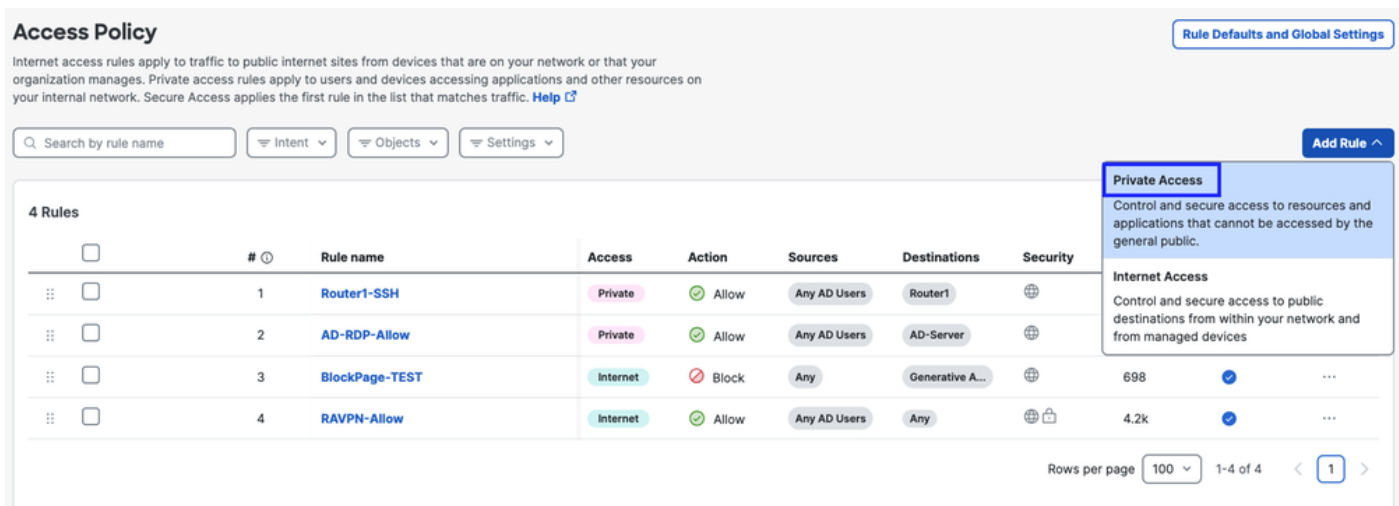
1. Navigeer naar Beveiligd > Toegangsbeleid



Beveiligde toegang - Configuratie toegangsbeleid

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.

Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.



Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen

Add Router2-SSH-Allow

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming

Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources

AD Users - Any AD Users

To

Specify one or more destinations

Private Resources - Router2

+ AND

Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is installed.

Profile: **None** | Requirements: **None**

Private Resources: **Router2**

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval Rule Defaults

Disabled

Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

[Cancel](#)

[Back](#) [Next](#)

Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) Rule Defaults

Disabled

Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile Rule Defaults

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

▼

[Cancel](#)

[Back](#) [Save](#)

Beveiligde toegang - Configuratie toegangsbeleid

7. Klik op Opslaan

Access Policy

Rule Defaults and Global Settings

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access rules applies the first rule in the list that matches traffic. [Help](#)

Search by rule name Intent Objects Settings

Add Rule

5 Rules

Customize view

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
<input type="checkbox"/>	1	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2		-	✓	...
<input type="checkbox"/>	2	Router1-SSH	Private	Allow	Any AD Users	Router1		-	✓	...
<input type="checkbox"/>	3	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		40	✓	...
<input type="checkbox"/>	4	BlockPage-TEST	Internet	Block	Any	Generative A...		698	✓	...
<input type="checkbox"/>	5	RAVPN-Allow	Internet	Allow	Any AD Users	Any		4.2k	✓	...

Rows per page 100 1-5 of 5 1

Beveiligde toegang - Configuratie toegangsbeleid

Stap 3 - Controleer de associatie van PR op de FTD

1. Navigeer naar Verbinding maken > Netwerkverbindingen > FTD's

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' dialog box with a 'Network Connections' tab selected. Under 'Essentials', there are four items: 'Users, Groups, and Endpoint Devices', 'End User Connectivity', 'DNS Forwarders', and 'Network Connections'. The 'Network Connections' item is checked. Below this, there is a summary card showing '0 Warning' and '1 Connected'. The main content area also shows a 'Tunnel Groups' section with a 'FTDs' tab selected. Below this, there is a table with columns for 'Region' and 'Status', and a '+ Add' button.

Veilige toegang - PR-verificatie

2. Klik op FTD > Bronnen weergeven die aan deze FTD zijn gekoppeld

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal to improve end-user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Q Search by FTD name FMC Name Configuration status 1 FTDs

FTD Name	Version	FMC	UZTA Configuration status
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local

Auto deployment: Yes

UZTA Configuration status

Synced | Last synced at 12 Jan 2026, at 6:29 AM UTC

Assigned Trusted Network

Trusted network: LAN (Default trusted network) Networks: 1 DNS Servers

Edit assignment + Trusted network

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status: Synced (2)

View resources associated to this FTD

Associate Resources

Veilige toegang - PR-verificatie

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

Q Search by resource name Configuration status 2 Resources [Associate Resources](#)

Resource name	Status
Router1	Synced
Router2	Synced

Close

3. Klik op sluiten

4. Controleer de status. De bijbehorende bron en configuratie moeten in gesynchroniseerde toestand zijn

The screenshot displays the 'Network Connections' page in the Palo Alto Networks management console. The 'FTDs' tab is active, showing a table of configured FTDs. The table has columns for 'FTD Name', 'Version', 'FMC', and 'UZTA Configuration status'. One FTD, 'FMC_FTD', is listed with version 'v10.0.0' and FMC 'FMC'. Its 'UZTA Configuration status' is 'Synced', which is highlighted with a blue box. To the right, a detailed view for 'FMC_FTD' is shown, including 'Firewall Details' (Device FQDN: ftd.csa.local, Auto deployment: Yes), 'UZTA Configuration status' (Synced, last synced at 12 Jan 2026, at 6:29 AM UTC), and 'Assigned Trusted Network' (LAN, 1 DNS Servers). Below this, 'Associated Resources' are listed with a status of 'Synced' and a count of 2, also highlighted with a blue box.

FTD Name	Version	FMC	UZTA Configuration status
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced

5. Controleer of de configuratie is ingesteld op FTD

Meld u aan bij FTD cli en navigeer naar de LINA-modus

Toon de toepassing Running-Config Object

```

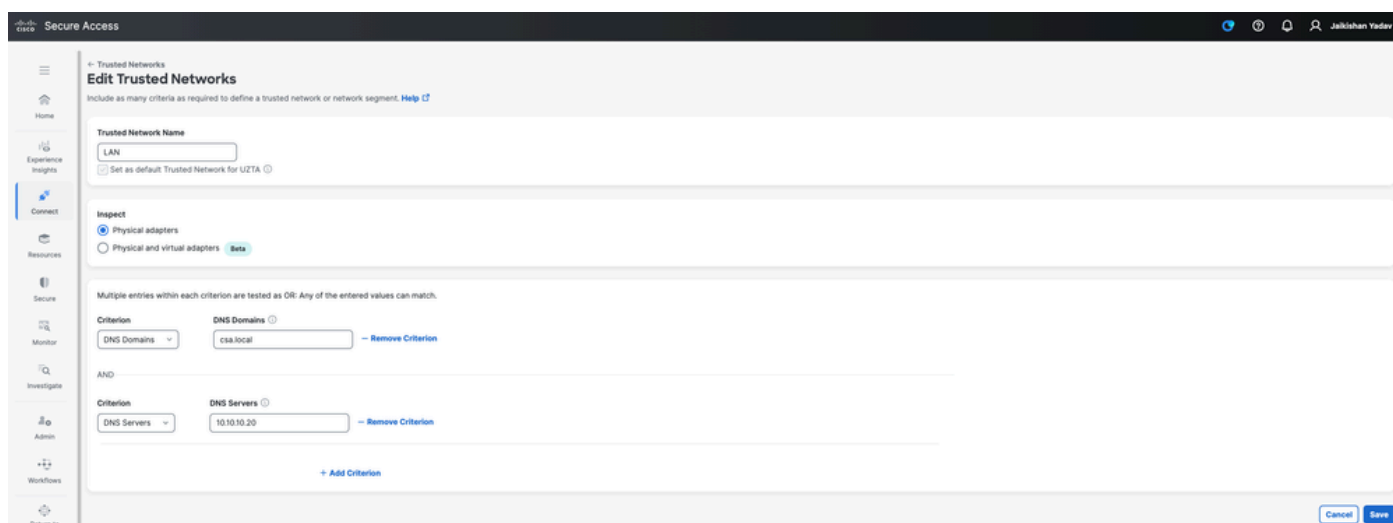
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal domain router2.csa.local tcp eq 22
  internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
  external domain router2.csa.local
  external subnet 10.10.10.102 255.255.255.255

```

Veilige toegang - PR-verificatie

Stap - 4 Configureren " Vertrouwde netwerken of ZTA-instellingen beheren"

Navigeer naar Verbinding maken > Eindgebruikersconnectiviteit > Toegang zonder vertrouwen > ZTA-instellingen en configureer vertrouwde netwerken



Veilige toegang - TND-configuratie

Stap -5 Voeg privé-bronnen toe aan het ZTA-profiel

1. Navigeer naar Verbinden > Connectiviteit voor eindgebruikers > Toegang tot vertrouwensrelatie opheffen en klik op 3 punten om het ZTA-profiel te bewerken

End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the Internet. [Help](#)

Zero Trust Access | Virtual Private Network | Internet Security

Enrollment methods Manage

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices enroll using: **SSO Authentication** | Certificates

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

Manage Zero Trust Access (ZTA) profiles, which allow you to add users and groups to unique traffic steering configurations for client-based ZTA connections. [Help](#)

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	ZTAProfile	2 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	1 Users 0 Groups	Jan 25, 2026

Actions: Edit, Delete

Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

Create profile

For client-based Zero Trust Access connections, add the destinations to which a set of users and groups can be steered. [Help](#)

ZTA profile name: ZTAProfile | Priority: 1. Current profile

Traffic Steering Limits

IOS 5k | Android 10k | macOS/Windows 100k

1 Secure Private Access (0 Destinations)

2 Secure Internet Access

3 Users and Groups

Secure Private Access

Add the private destinations and private resources to which a set of users and groups can be steered. [Help](#)

Traffic Steering | Options

Search by destination

Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

Actions: + Destinations

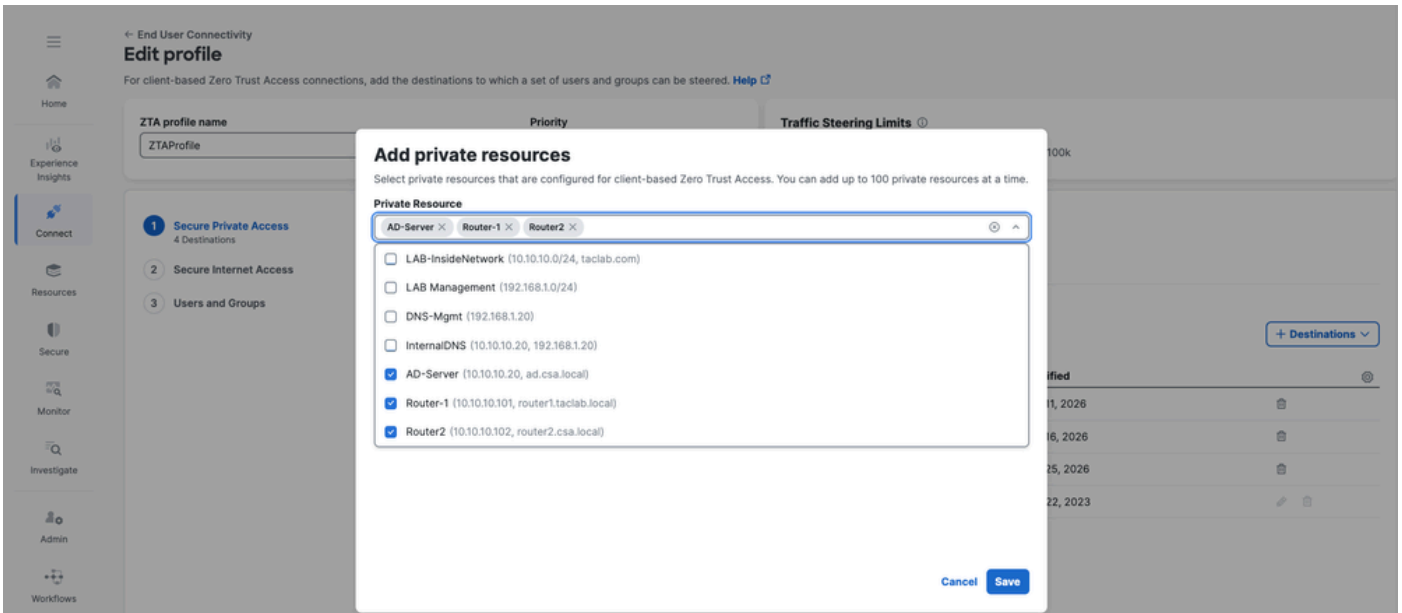
Private Resource

Add private resources that are configured for client-based Zero Trust Access.

Add Destination

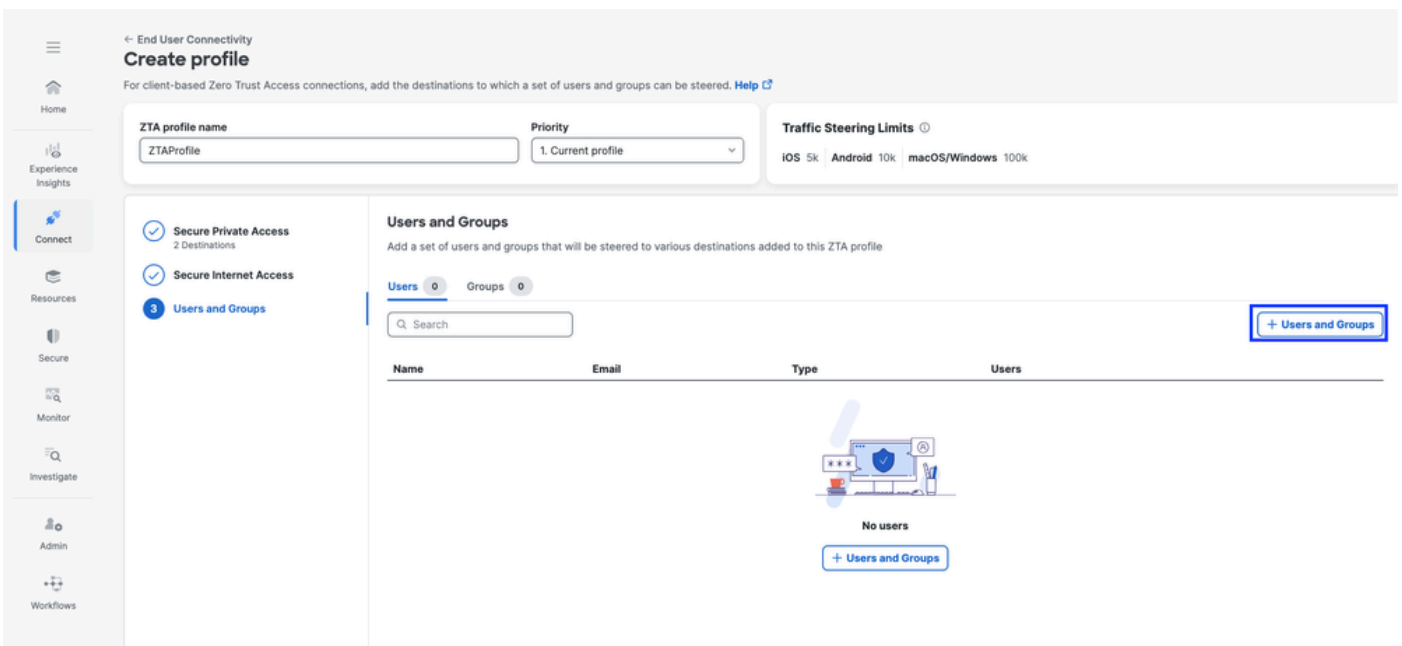
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Veilige toegang - ZTA-profiel



Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen



ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

Secure Private Access (2 Destinations)
Secure Internet Access
Users and Groups

Users and Groups

Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users 1 | Groups 0

Q Search + Users and Groups

Name	Email	Type	Users
jay (jay@csa.local)	jay@gmail.com	User	-

Rows per page: 10 < >

Back Close

Veilige toegang - ZTA-profiel

Stap 6: Controleer de toegang tot de privébron

1. Controleer de netwerkvingerafdruk voor ZTA TND

The screenshot displays the Cisco Secure Client application window. The title bar reads "Cisco Secure Client". The main header features the Cisco logo and the text "Secure Client". A left-hand navigation menu includes the following items: "General", "Status Overview", "AnyConnect VPN", "Zero Trust Access" (which is highlighted with a right-pointing arrow), and "Umbrella". Below the menu, there is a "Diagnostics" button with the text "Collect diagnostic information for all installed components." above it.

The main content area is titled "Zero Trust Access" and contains four tabs: "Statistics", "Advanced", "Configuration", and "Message History". The "Statistics" tab is active and displays the following data:

TCP Flows:	611
Allowed UDP Flows:	48
Allowed TCP Flows:	597
Blocked UDP Flows:	111
Blocked TCP Flows:	14
Authenticated UDP Flows:	0
Authenticated TCP Flows:	0

Below the statistics, there are two expandable sections:

- Proxy Configurations:**
 - Secure Private Access: Active
 - Secure Internet Access: Active
- Network Fingerprints:**
 - LAN: Matched

A vertical scrollbar is visible on the right side of the statistics area.

Veilige toegang - PR-testen

2. Controleer of de externe gebruiker FTD FQDN kan oplossen

```
C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [10.10.10.1] with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 10.10.10.20

Name: ftd.csa.local
Addresses: 10.10.10.1
```

Veilige toegang - PR-testen

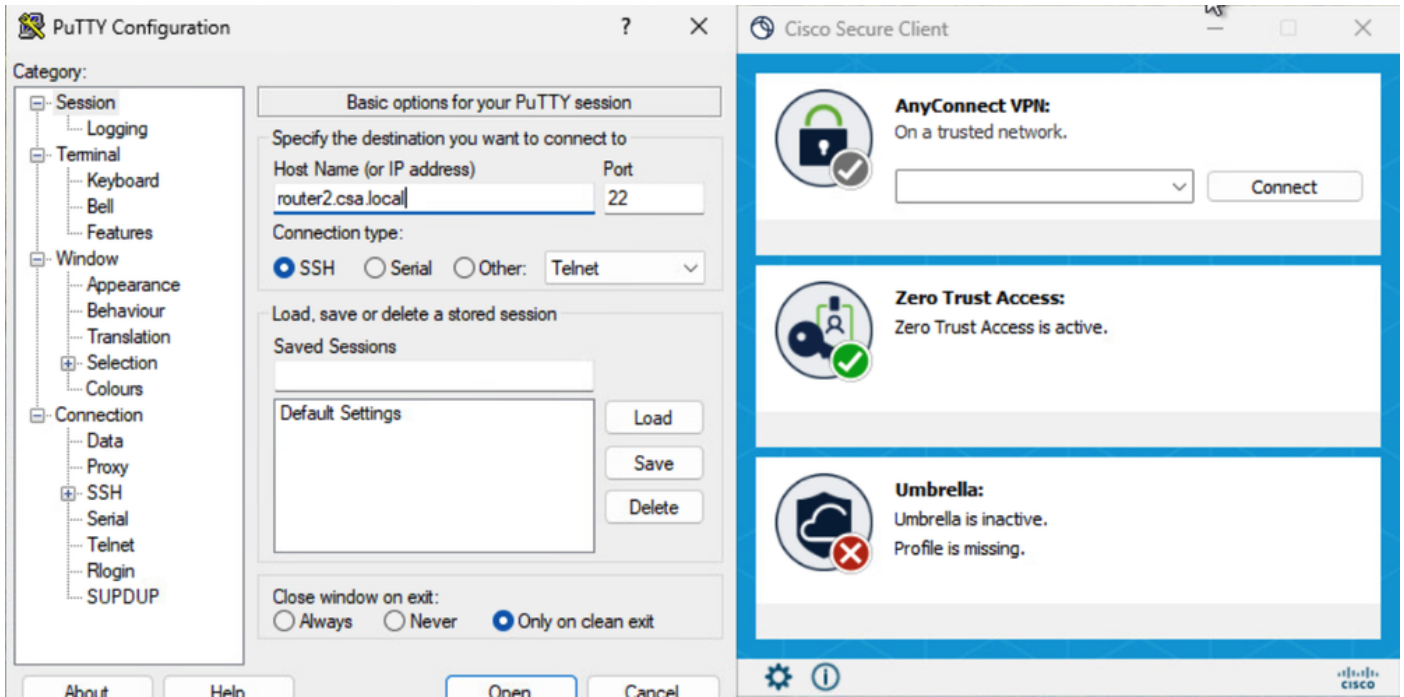
3. Controleren of FTD particuliere bronnen kan bereiken met behulp van FQDN

```
ftd# ping router2.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/60 ms
ftd# █
```

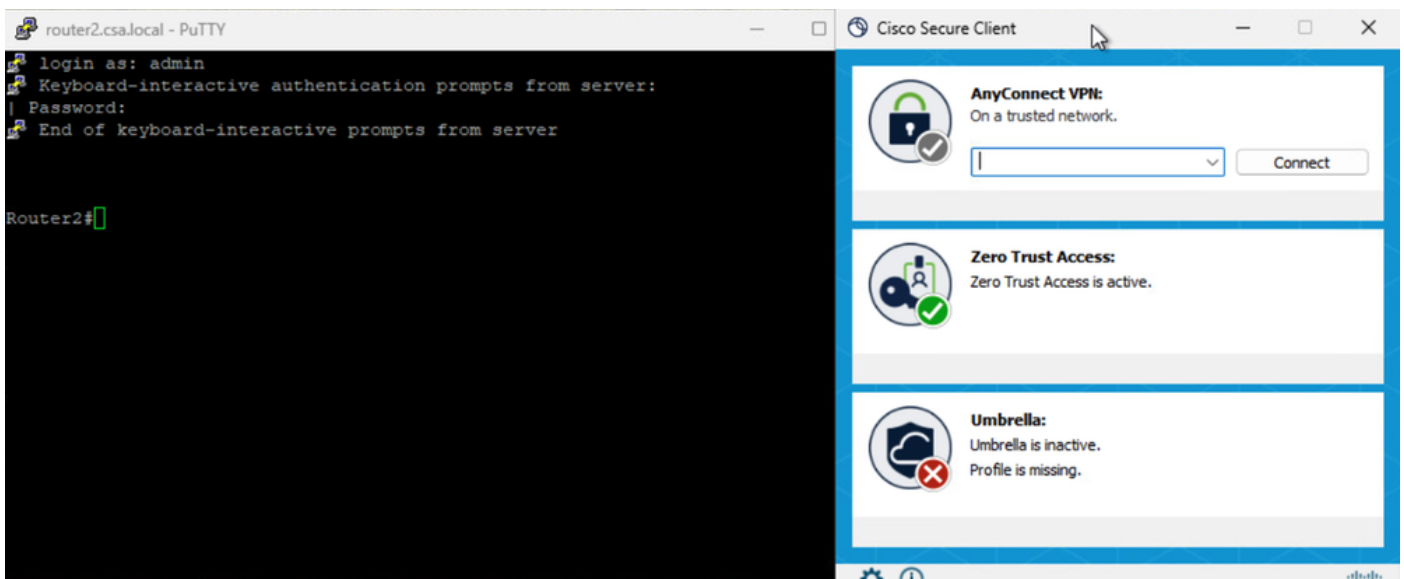
Veilige toegang - PR-testen

4. Test de SSH-verbinding met de Private Resource

Toegang tot de PR via FQDN

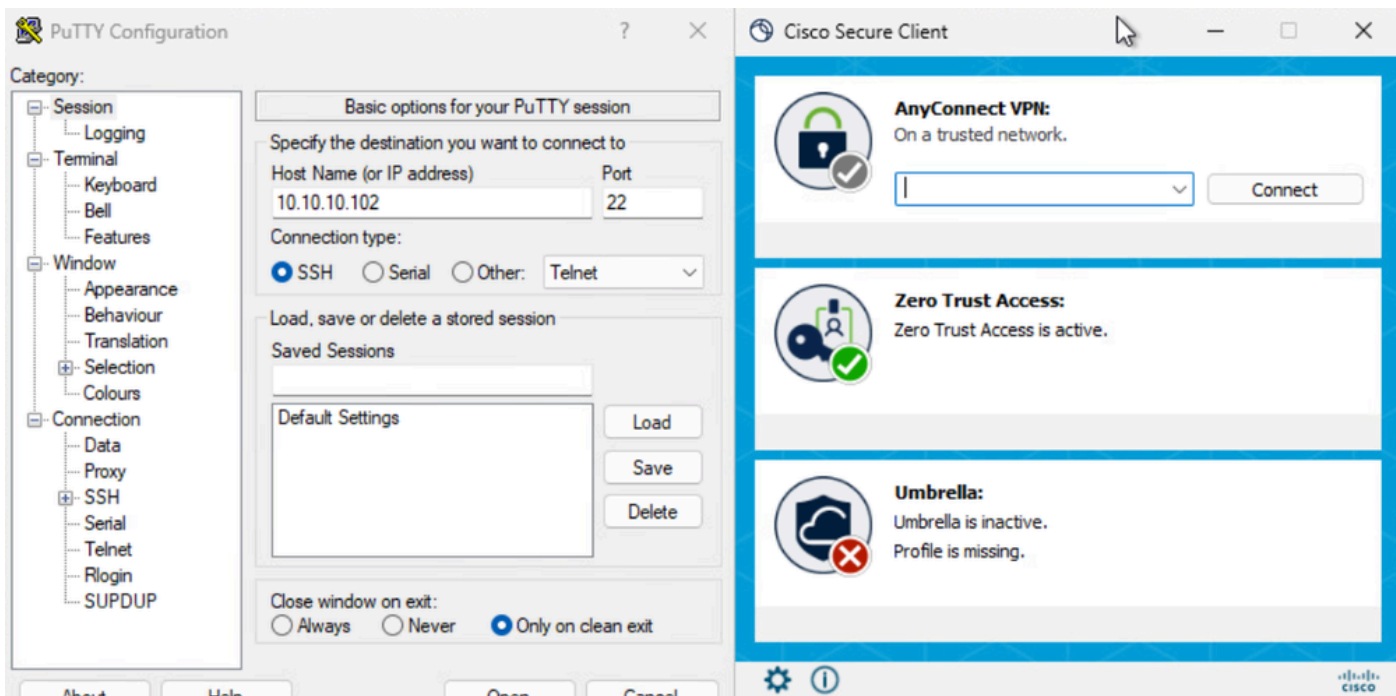


Veilige toegang - PR-testen

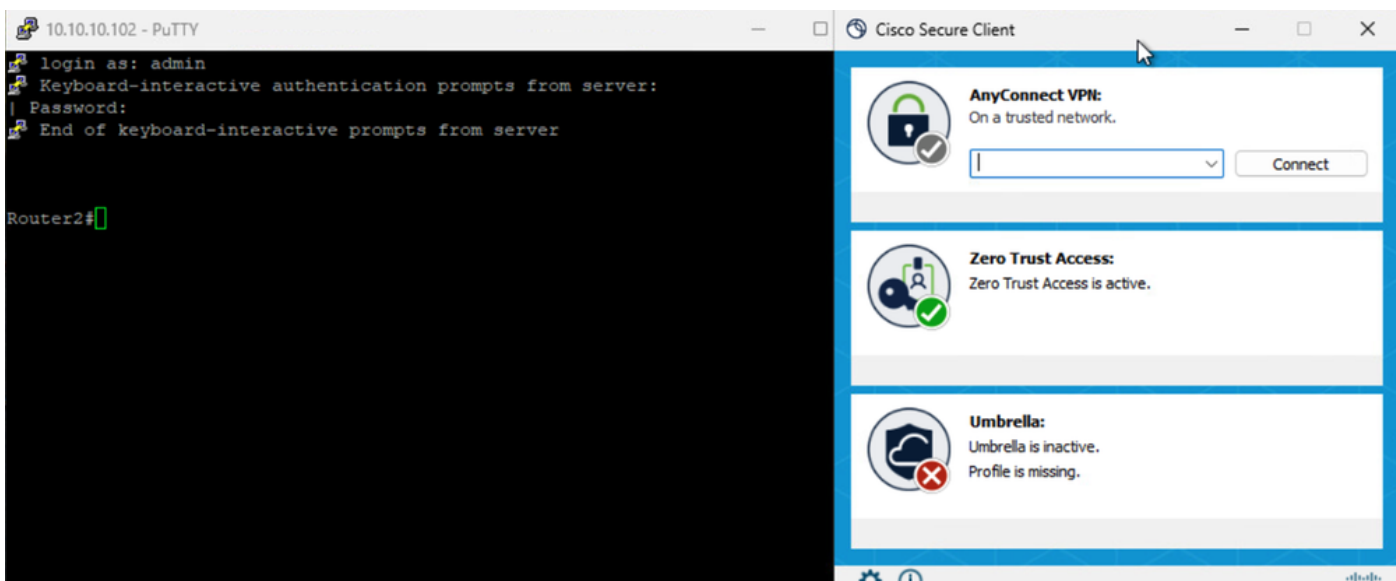


Veilige toegang - PR-testen

Toegang tot de PR via IP-adres



Veilige toegang - PR-testen



Veilige toegang - PR-testen

5. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten

Activity Search

Activity Search interface showing search filters and results for domain 'router2.csa.local'. The search criteria include 'DOMAIN: router2.csa.local'. The results table shows 8 total results, all with a response of 'Allowed'. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, OS, and Bro. The 'Request' column for all entries is 'ZTA CLIENT-BASED'. The 'Source' column shows 'jey (jey@csa.local)'. The 'Destination' column shows 'router2.csa.local'. The 'Destination IP' column shows '10.10.10.102'. The 'Destination Port' column shows '22'. The 'Action' column shows 'Allowed'. The 'Resource/Application' column shows 'Router2'. The 'Zero Trust Access Profile' column shows 'ZTAProfile'. The 'Rule Name' column shows 'Router2-SSH-Allow'. The 'OS' column shows 'win 10.0.26200.7840'.

Veilige toegang - zoeken naar activiteiten

Activity Search

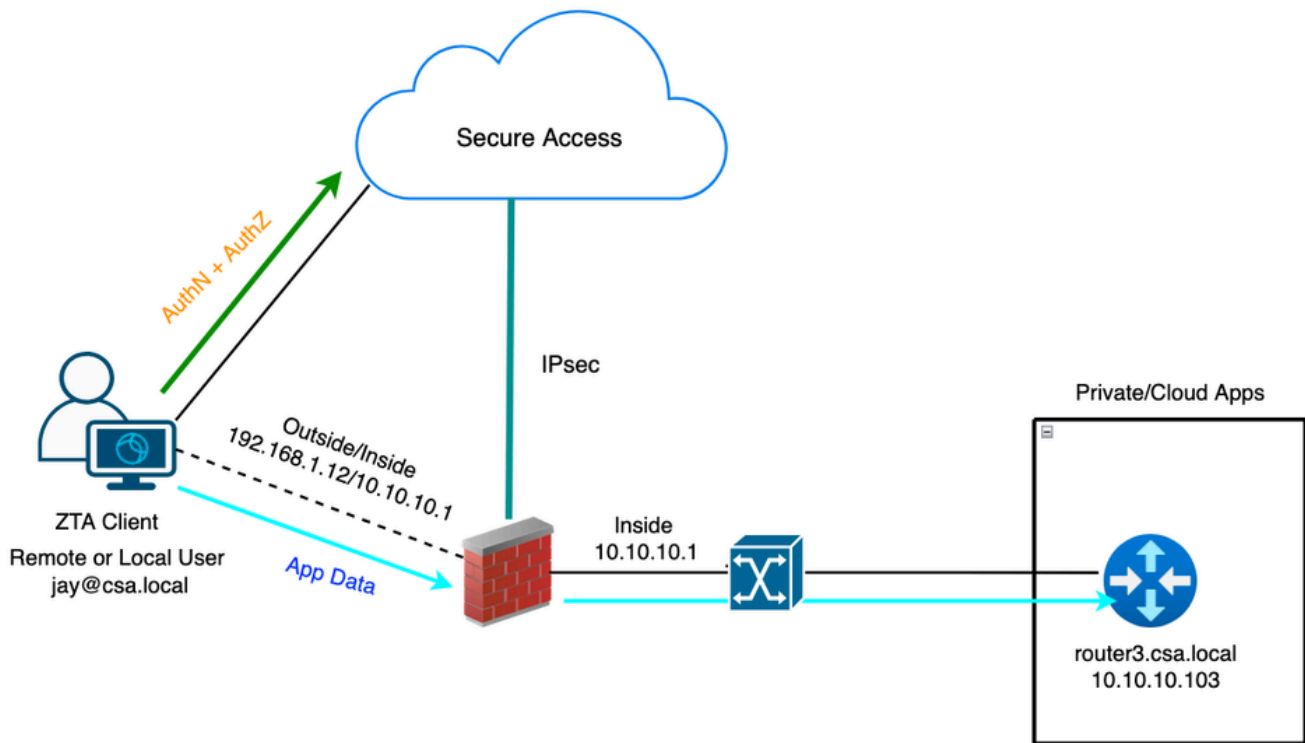
Activity Search interface showing search filters and results for response 'Allowed'. The search criteria include 'RESPONSE: Allowed'. The results table shows 17 total results, all with a response of 'Allowed'. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/App, and Event Details. The 'Request' column for all entries is 'ZTA CLIENT-BASED'. The 'Source' column shows 'jey (jey@csa.local)' and 'jalayadv1 (jalayadv1@cxsecurity.onmicrosoft.com)'. The 'Destination' column shows 'router2.csa.local' and '10.10.10.102'. The 'Destination IP' column shows '10.10.10.102' and '192.168.1.64'. The 'Destination Port' column shows '22' and '7680'. The 'Action' column shows 'Allowed'. The 'Resource/App' column shows 'Router2' and 'LAB Manager'. The 'Event Details' panel on the right shows 'Action: Allowed', 'Block Reason: -', 'Connection Method: ZTA Client-based', 'Time: Feb 23, 2026 3:33 AM', 'Access details: Identity: jey (jey@csa.local), ZTNA Client: Router2-SSH-Allow, Resource/Application: Router2, Zero Trust Access Profile: ZTAProfile, Trusted Network: No Match, Enforcement Point: FTD > FMC_FTD, Destination: router2.csa.local'.

Veilige toegang - zoeken naar activiteiten

Activity Search

Activity Search interface showing search filters and results for IP address '10.10.10.102'. The search criteria include 'IP ADDRESS: 10.10.10.102' and 'RESPONSE: Allowed'. The results table shows 19 total results, all with a response of 'Allowed'. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, and OS. The 'Request' column for all entries is 'ZTA CLIENT-BASED'. The 'Source' column shows 'jey (jey@csa.local)'. The 'Destination' column shows '10.10.10.102'. The 'Destination IP' column shows '10.10.10.102'. The 'Destination Port' column shows '22'. The 'Action' column shows 'Allowed'. The 'Resource/Application' column shows 'Router2'. The 'Zero Trust Access Profile' column shows 'ZTAProfile'. The 'Rule Name' column shows 'Router2-SSH-Allow'.

Veilige toegang - zoeken naar activiteiten



Universal ZTA - Test Case Topology

Stap 1 - Een privébron definiëren voor beveiligde toegang

Configureer een privébron die toegankelijk is via een apparaat waarvoor Zero Trust Access (ZTA) is ingeschreven met cloudhandhaving

1. Navigeer naar Bronnen > Bestemmingen > Particuliere bronnen > Klik op +Toevoegen

Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules	Total Requests
-	Client-based ZTA	-	0	2	0
-	Client-based ZTA	1	0	2	0
-	Client-based ZTA	-	0	2	0

Veilige toegang - Configuratie van privébronnen

2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.

← Private Resources

Add a Private Resource

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure private resources in order to choose them as destinations when creating access rules. [Help](#)

General

Private Resource Name
Router3

Description (optional)
Router 3 for uZTNA Testing

Veilige toegang - Configuratie van privébronnen

3. Voer het FQDN in van de privébron die u wilt openen. We kunnen ook het IP-adres van de privébron definiëren. Zie [Een privébron toevoegen voor](#) meer informatie

4. Selecteer de DNS-server om het domein op te lossen

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
router3.csa.local	Any TCP	22	+ Protocol & Port
Remove			
192.168.1.103	Any TCP	22	+ Protocol & Port
Remove			
10.10.10.103	Any TCP	22	+ Protocol & Port
Remove + IP Address/FQDN			

Use internal DNS server to resolve the domain LabDNS (192.168.1.20, 10.10.10.20) ▼

Veilige toegang - Configuratie van privébronnen

5. Selecteer methoden voor eindpuntverbinding

6. Selecteer FTD als lokale handhavingpunten

Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

Branch Connections
Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by access rules.

Zero-trust connections
Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

FMC_F... x Search by FTD na... ^

FMC_FTD (ftd.csa.local) ✓
Will get enforced at the selected firewalls.

Local-only

Enforcement point for Remote User

Remote user — via Internet — Secure Access Cloud — Private Resource

Enforcement point for Local user

User in a trusted network — via local network — Local Firewall — Private Resource

Cancel Save and Test Save

Veilige toegang - Configuratie van privébronnen

Selecteer RC als de Private Resource toegankelijk is via RC, anders leeg laten als de Private Resource toegankelijk is via Network Tunnel Group (IPsec Tunnel).

Resource Connector Groups

Secure Access can forward Zero Trust Access traffic to this private resource using resource connectors. ⓘ

For more information, see [Help](#)

Resource Connector Groups (optional) ⓘ

RC-ESXI x e.g. My Server Group v

Choose a connector group in the same data center, branch office, or security zone as the resource. ⓘ

Veilige toegang - Configuratie van privébronnen



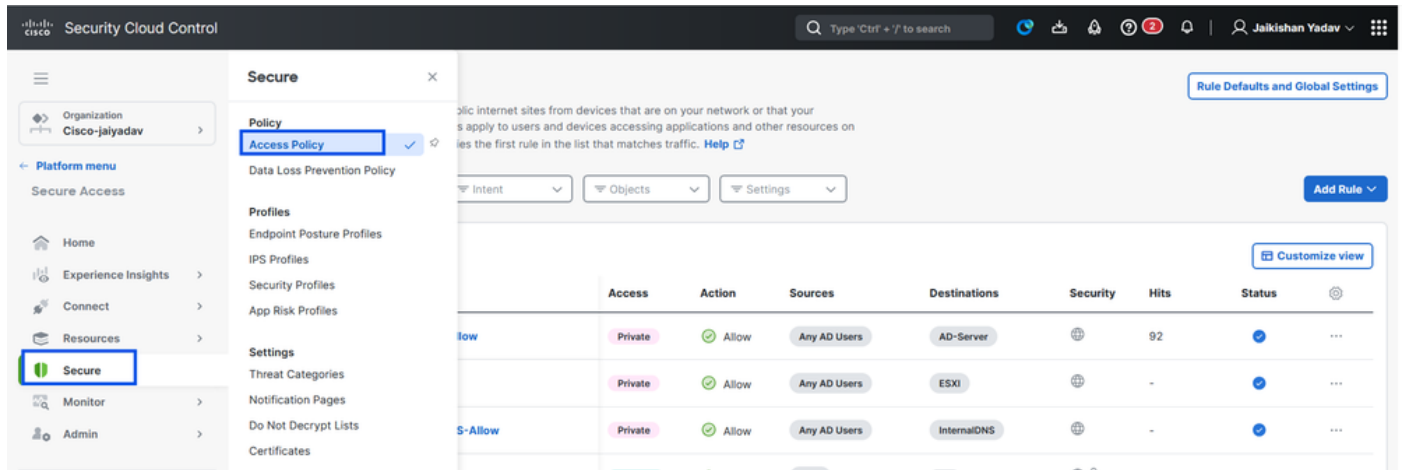
Opmerking: afhankelijk van het type inschrijving dat u selecteert, wordt de PR automatisch gekoppeld aan de FTD en wordt een beleidsimplementatie geactiveerd

7. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie [Private Access Rule](#)

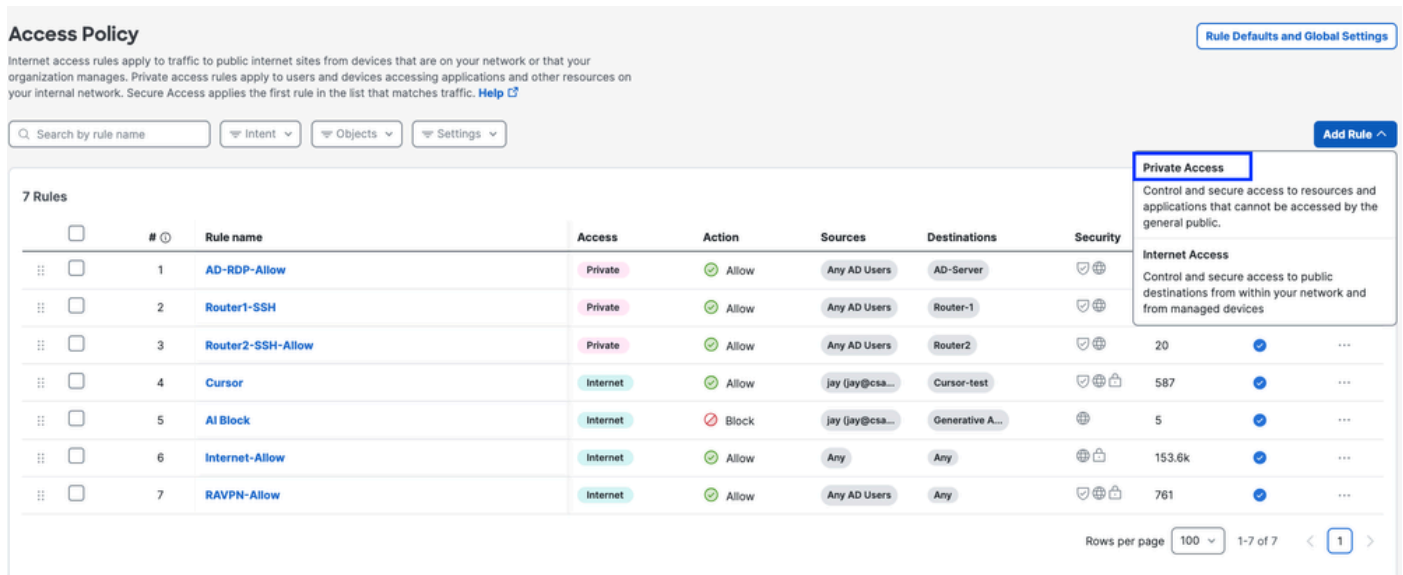
1. Navigeer naar Beveiligd > Toegangsbeleid



Beveiligde toegang - Configuratie toegangsbeleid

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.

Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.



Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen

Add Router3-SSH-Allow

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming

Rule name Rule order

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#)

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

To

+ AND

Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile [Rule Defaults](#)
Requirements for end-user devices on which the Cisco Secure Client is installed.
Profile: **None** | Requirements: **None**
Private Resources: **Router3**

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval [Rule Defaults](#) Disabled
Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Cancel

[Back](#) [Next](#)

Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren

Specify Access

Specify which users and endpoints can access which resources. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) [Rule Defaults](#) Disabled
Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile

[Rule Defaults](#)

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

Cancel

[Back](#) [Save](#)

Beveiligde toegang - Configuratie toegangsbeleid

7. Klik op Opslaan

Access Policy Rule Defaults and Global Settings

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name Intent Objects Settings Add Rule

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	Router3-SSH-Allow	Private	Allow	Any AD Users	Router3	Shield	-	On
2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	Shield	-	On
3	Router1-SSH	Private	Allow	Any AD Users	Router-1	Shield	-	On
4	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2	Shield	20	On
5	Cursor	Internet	Allow	jay (jay@csa...	Cursor-test	Shield	587	On
6	AI Block	Internet	Block	jay (jay@csa...	Generative A...	Shield	5	On
7	Internet-Allow	Internet	Allow	Any	Any	Shield	154.8k	On
8	RAVPN-Allow	Internet	Allow	Any AD Users	Any	Shield	761	On

Rows per page: 100 | 1-8 of 8 | Page 1

Beveiligde toegang - Configuratie toegangsbeleid

Stap 3 - Controleer de associatie van PR op de FTD

1. Navigeer naar Verbinding maken > Netwerkverbindingen > FTD's

The screenshot shows the Cisco Security Cloud Control interface. On the left, the 'Connect' menu is expanded, highlighting 'Network Connections'. The main content area shows a 'Connect' dialog box with 'Essentials' selected. Under 'Essentials', 'Network Connections' is checked. Below this, there are two status indicators: '0 Warning' and '1 Connected'. The 'FTDs' section is also visible, showing a list of tunnel groups with filters for 'Region' and 'Status'.

Veilige toegang - PR-verificatie

2. Klik op FTD > Bronnen weergeven die aan deze FTD zijn gekoppeld

```

C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

Name:     ftd.csa.local
Addresses: 192.168.1.12

```

Veilige toegang - PR-verificatie

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Syncing
●

0 Synced
●

FTDs configured for Universal Zero Trust Access

An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Configuration changes are being processed

The recent Universal ZTA configuration changes are being processed and will be pushed to FTDs in a few minutes.

FMC Name
▼

Configuration status
▼

1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associat
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	● Syncing	3

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local

Auto deployment: Yes

UZTA Configuration status

● Syncing Last synced at 23 Feb 2026, at 5:02 AM UTC

Assigned Trusted Network

Trusted network	Networks
LAN <small>(Default trusted network)</small>	1 DNS Domains 1 DNS Servers

Edit assignment
+ Trusted network

Associated Resources 3

RESOURCES ASSOCIATED BY STATUS

Status	
● Synced	3

View resources associated to this FTD

Associate Resources

Veilige toegang - PR-verificatie

```
C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

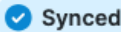
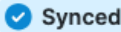
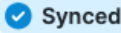
Name: ftd.csa.local
Addresses: 192.168.1.12
```

Veilige toegang - PR-verificatie

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

Search by resource name Configuration status 3 Resources [Associate Resources](#)

Resource name	Status
Router-1	 Synced
Router2	 Synced
Router3	 Synced

Close

Veilige toegang - PR-verificatie

3. Klik op sluiten

4. Controleer de status. De bijbehorende bron en configuratie moeten in gesynchroniseerde toestand zijn

Network Connections
 Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access
 An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Q Search by FTD name FMC Name Configuration status 1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associated
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced	3

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local
Auto deployment: Yes

UZTA Configuration status

Synced Last synced at 23 Feb 2026, at 5:08 AM UTC

Assigned Trusted Network

Trusted network: **LAN** (Default trusted network) 1 DNS Domains 1 DNS Servers

Edit assignment + Trusted network

Associated Resources 3

RESOURCES ASSOCIATED BY STATUS

Status: **Synced** 3

View resources associated to this FTD

Associate Resources

Veilige toegang - PR-verificatie

5. Controleer of de configuratie is ingesteld op FTD

Meld u aan bij FTD cli en navigeer naar de LINA-modus

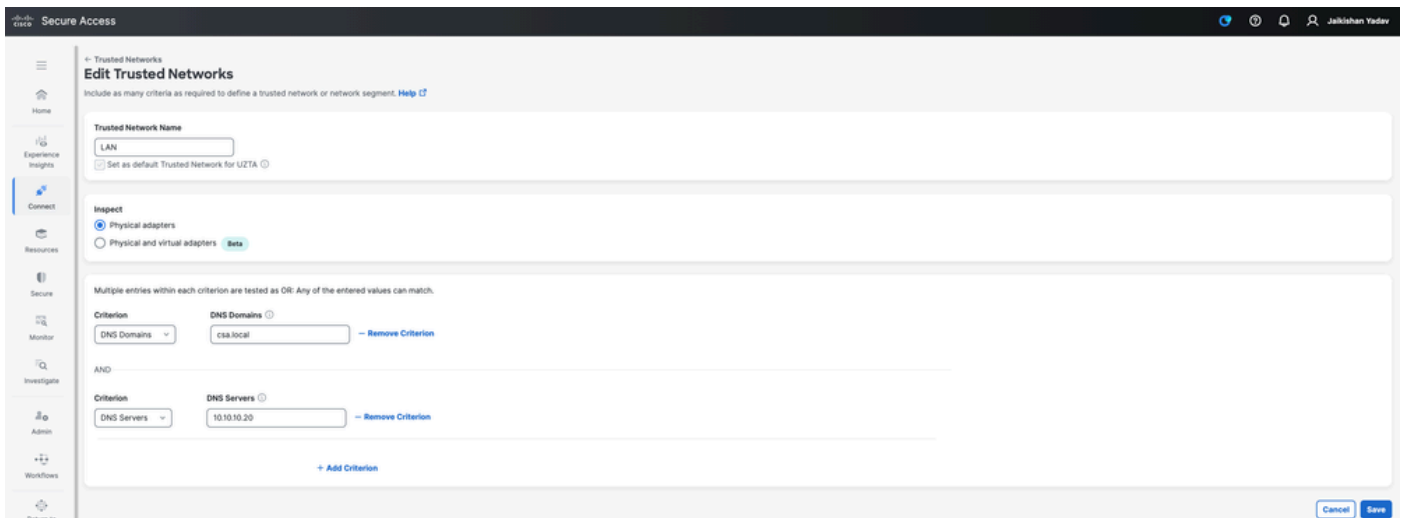
Toon de toepassing Running-Config Object

```
ftd# sh run object application
object application PR_Router2
id 443200
internal domain router2.csa.local tcp eq 22
internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
external domain router2.csa.local
external subnet 10.10.10.102 255.255.255.255
object application PR_Router-1
id 438025
internal domain router1.csa.local tcp range 1 65535
internal subnet 10.10.10.101 255.255.255.255 tcp range 1 65535
external domain router1.csa.local
external subnet 10.10.10.101 255.255.255.255
object application PR_Router3
id 468677
internal domain router3.csa.local tcp eq 22
internal subnet 192.168.1.103 255.255.255.255 tcp eq 22
internal subnet 10.10.10.103 255.255.255.255 tcp eq 22
external domain router3.csa.local
external subnet 10.10.10.103 255.255.255.255
external subnet 192.168.1.103 255.255.255.255
```

Veilige toegang - PR-verificatie

Stap - 4 Configureren of verifiëren " Vertrouwde netwerken of ZTA-instellingen beheren"

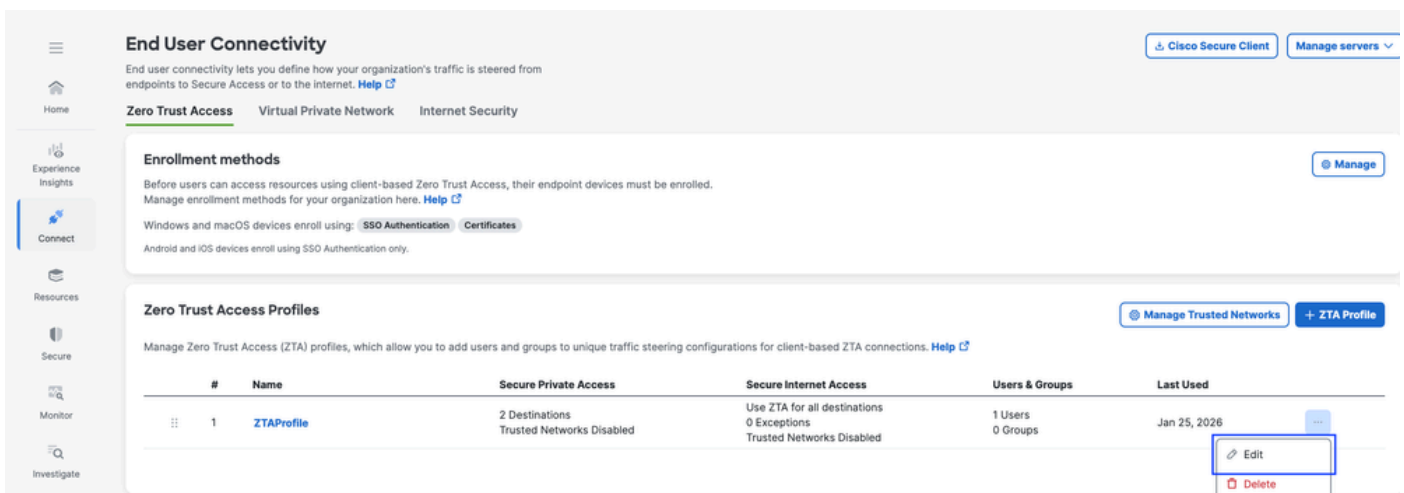
Navigeer naar **Verbinding maken > Eindgebruikersconnectiviteit > Toegang zonder vertrouwen > ZTA-instellingen** en configureer vertrouwde netwerken



Veilige toegang - ZTA TND-configuratie

Stap 5 Voeg privé-bronnen toe aan het ZTA-profiel

1. Navigeer naar **Verbinden > Connectiviteit voor eindgebruikers > Toegang tot vertrouwensrelatie opheffen** en klik op 3 punten om het ZTA-profiel te bewerken



Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

The screenshot shows the 'Create profile' page for a Zero Trust Access profile. The profile name is 'ZTAProfile' and the priority is '1. Current profile'. The traffic steering limits are set to 5k for iOS, 10k for Android, and 100k for macOS/Windows. The 'Secure Private Access' section is active, showing a table of destinations and private resources. A tooltip is visible over the 'Destinations' column, explaining the difference between 'Private Resource' and 'Add Destination'.

Destinations & Private Resources	Destinations	Modified
<input checked="" type="checkbox"/> *.zpc.sse.cisco.test	1	Feb 22, 2023

Private Resource
Add private resources that are configured for client-based Zero Trust Access.

Add Destination
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Veilige toegang - ZTA-profiel

The screenshot shows the 'Edit profile' page for a Zero Trust Access profile. A modal window titled 'Add private resources' is open, allowing the user to select private resources for the profile. The modal lists several resources, including 'AD-Server', 'DNS-Mgmt', 'Router2', 'Router-1', and 'Router3', each with a checkbox and a description.

Add private resources
Select private resources that are configured for client-based Zero Trust Access. You can add up to 100 private resources at a time.

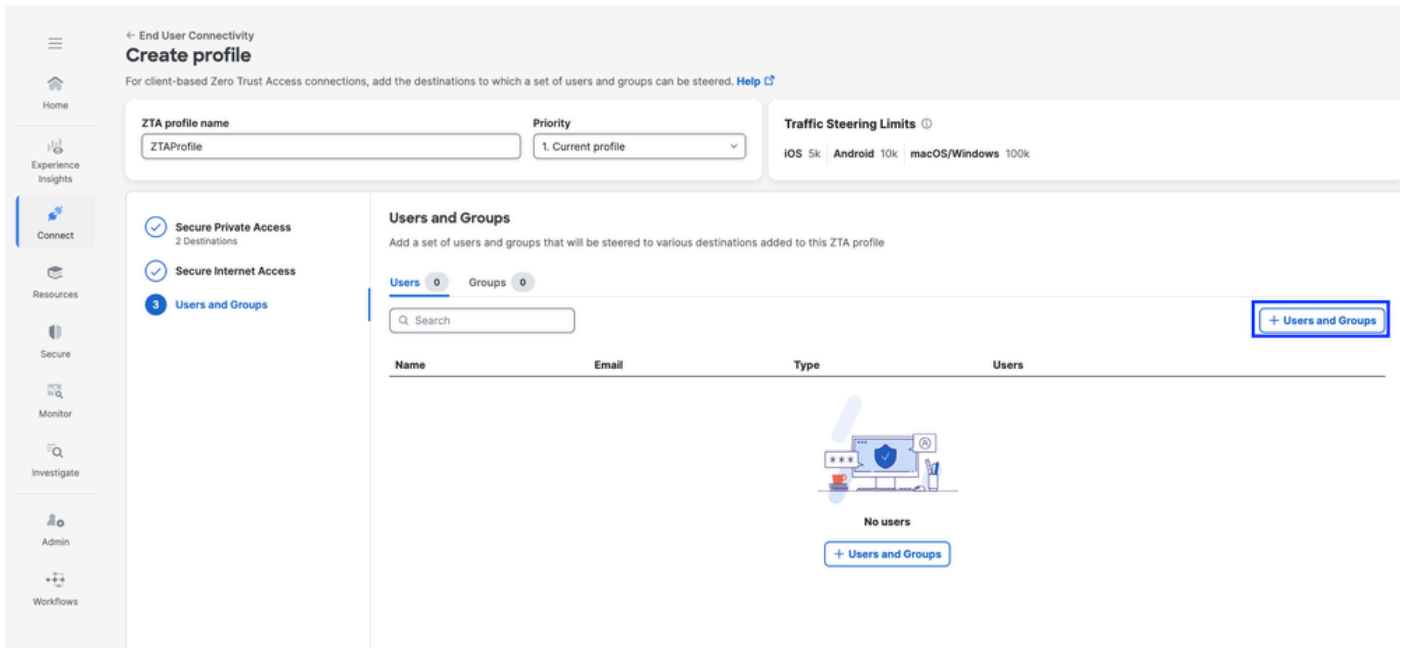
Private Resource

- LAB-InsideNetwork (10.10.10.0/24, taclab.com)
- InternalDNS (10.10.10.20, 192.168.1.20)
- AD-Server (10.10.10.20, ad.csa.local)
- LAB Management (192.168.1.0/24)
- DNS-Mgmt (192.168.1.20/32)
- Router2 (10.10.10.102, router2.csa.local)
- Router-1 (10.10.10.101, router1.csa.local)
- Router3 (10.10.10.103, 192.168.1.103, router3.csa.local)

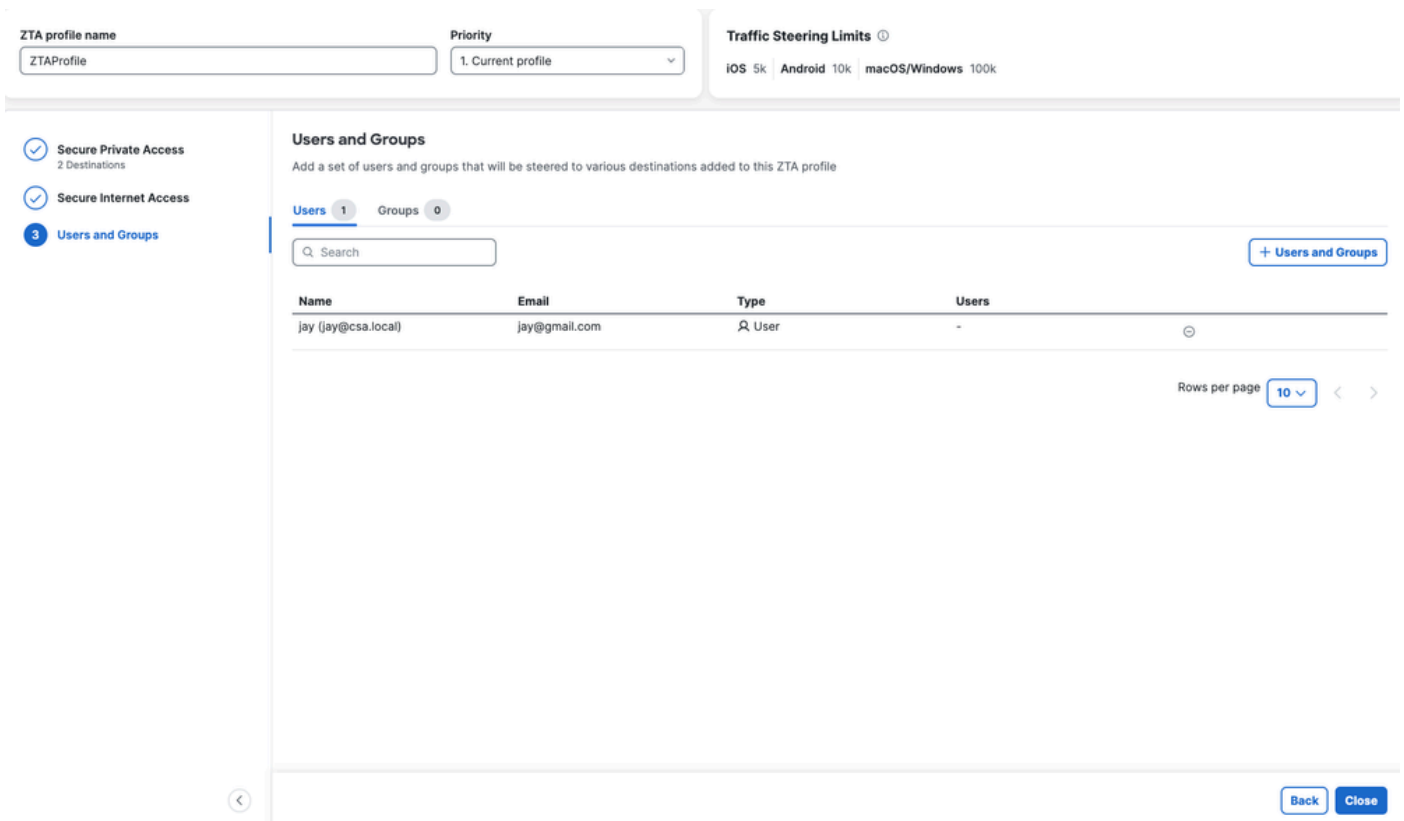
Cancel Save

Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen



Veilige toegang - ZTA-profiel

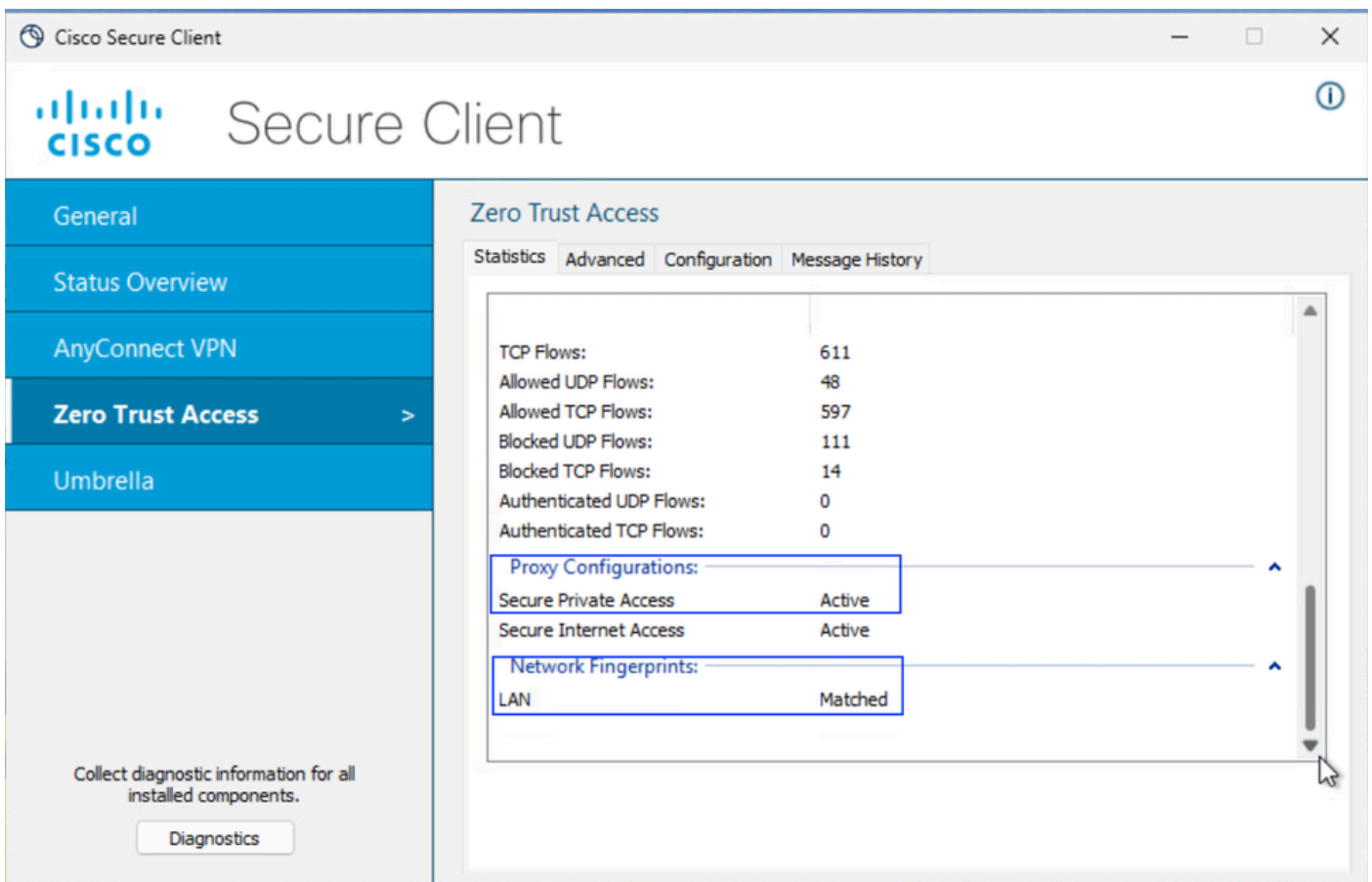


Veilige toegang - ZTA-profiel

Stap 6: Controleer de toegang tot de privébron

Wanneer de gebruiker lokaal is

1. Controleer de netwerkvingerafdruk voor ZTA TND, deze moet overeenkomen als de gebruiker Lokaal is en Secure Private Access moet actief zijn



Veilige toegang - PR-testen

2. Controleer of de externe gebruiker FTD FQDN kan oplossen

```
C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [10.10.10.1] with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 10.10.10.20

Name: ftd.csa.local
Addresses: 10.10.10.1
```

Veilige toegang - PR-testen

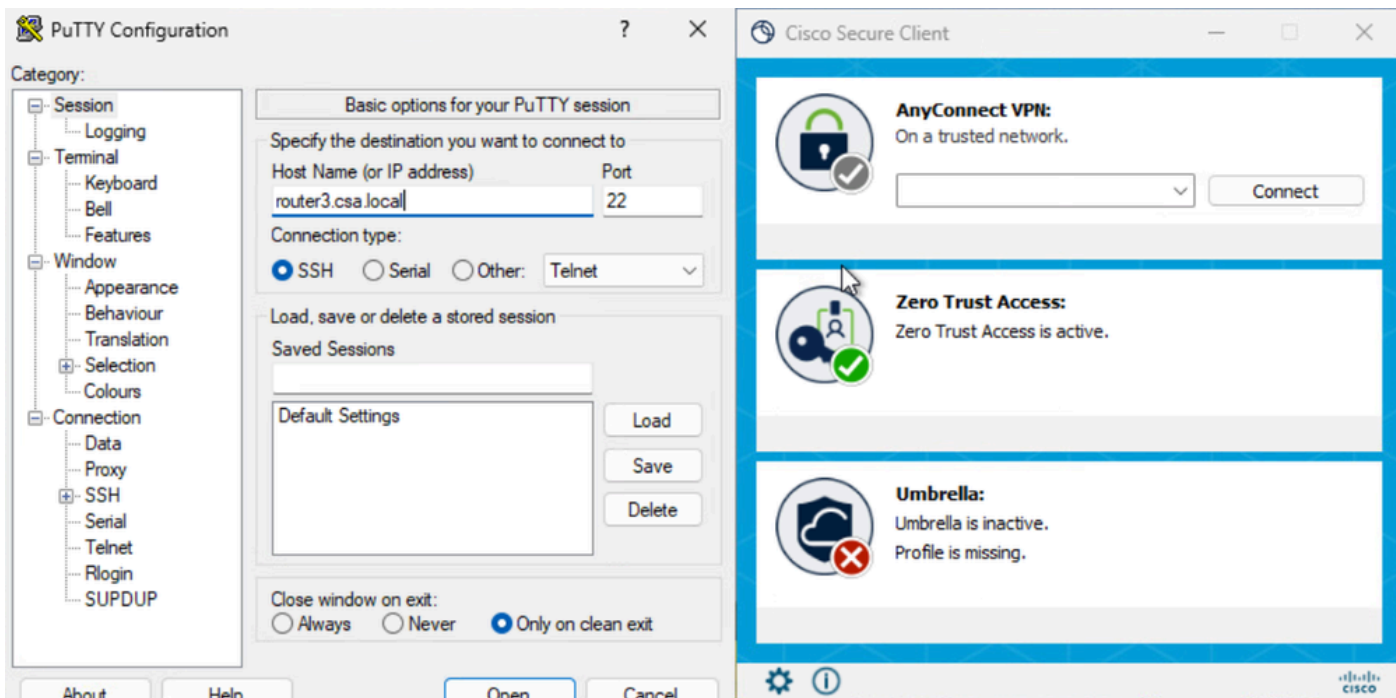
3. Controleren of FTD particuliere bronnen kan bereiken met behulp van FQDN

```
ftd# ping router3.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.103, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd# █
```

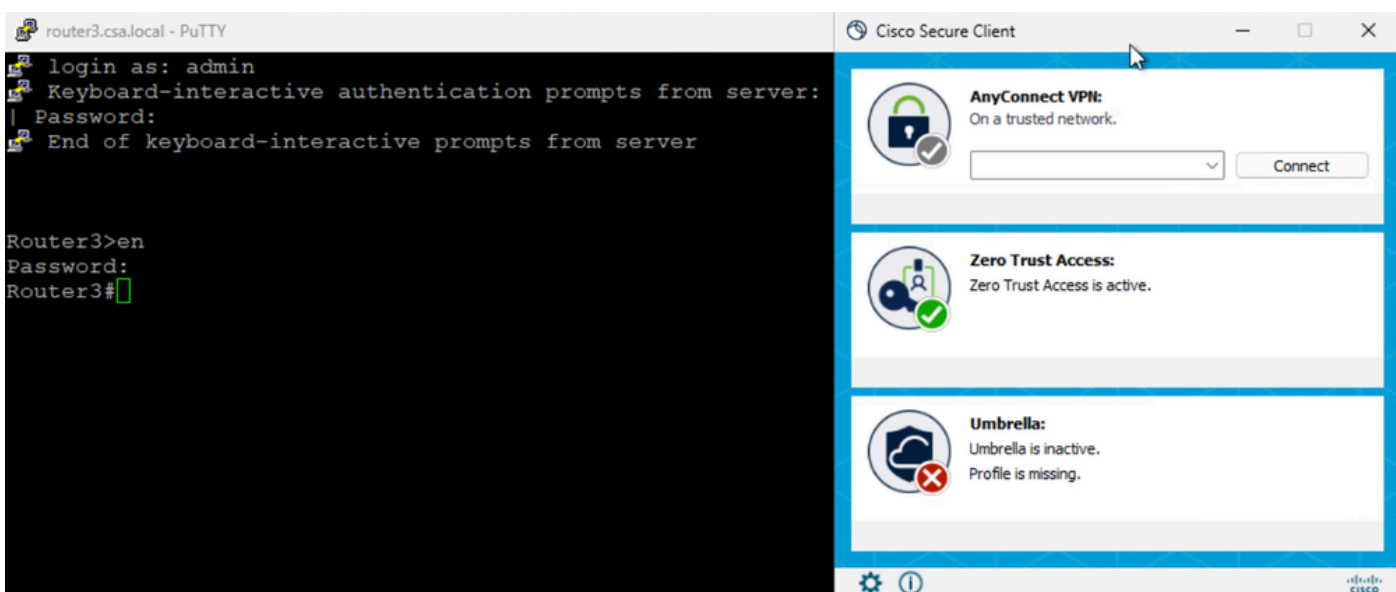
Veilige toegang - PR-testen

4. Test de SSH-verbinding met de Private Resource

Toegang tot de PR via FQDN

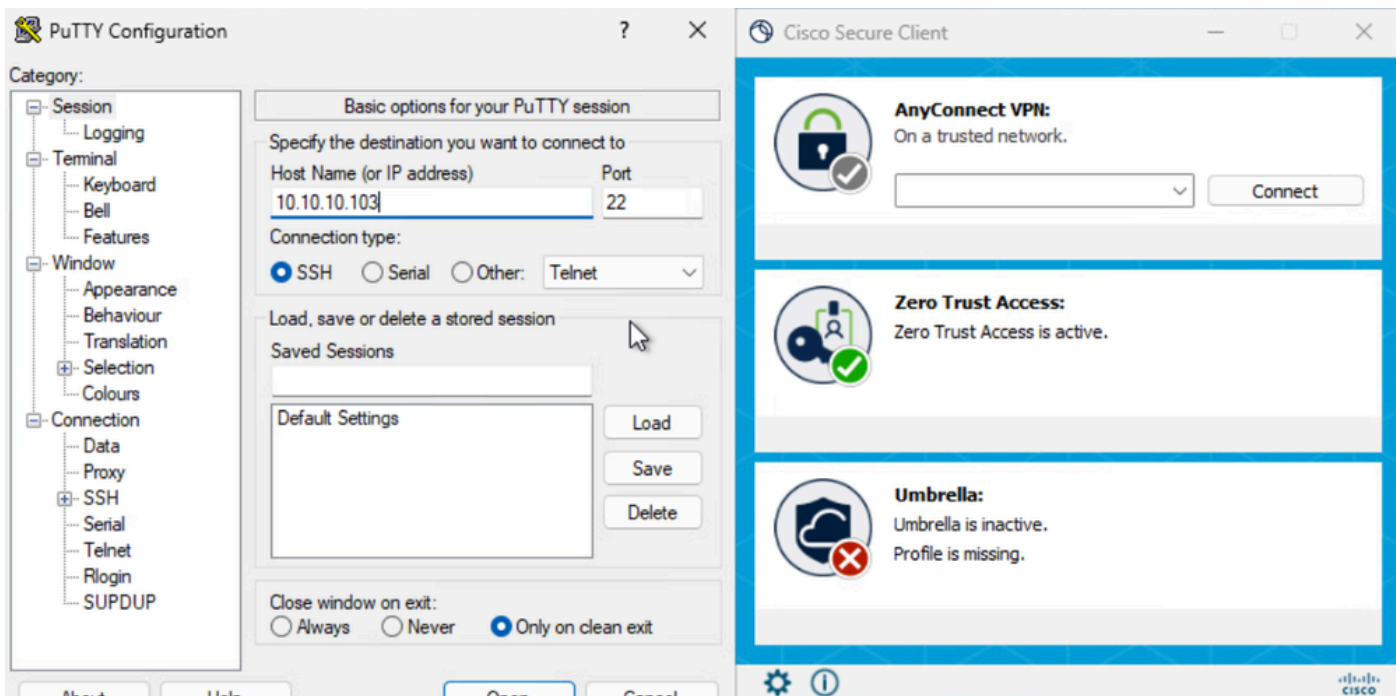


Veilige toegang - PR-testen

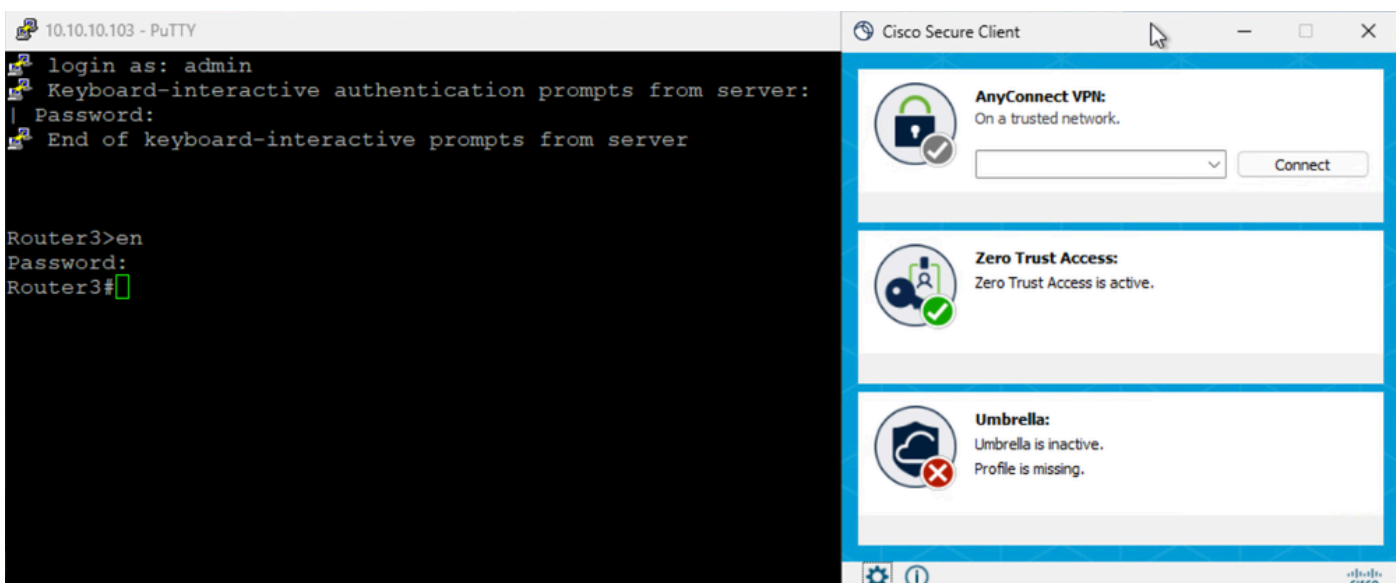


Veilige toegang - PR-testen

Toegang tot de PR via IP-adres



Veilige toegang - PR-testen

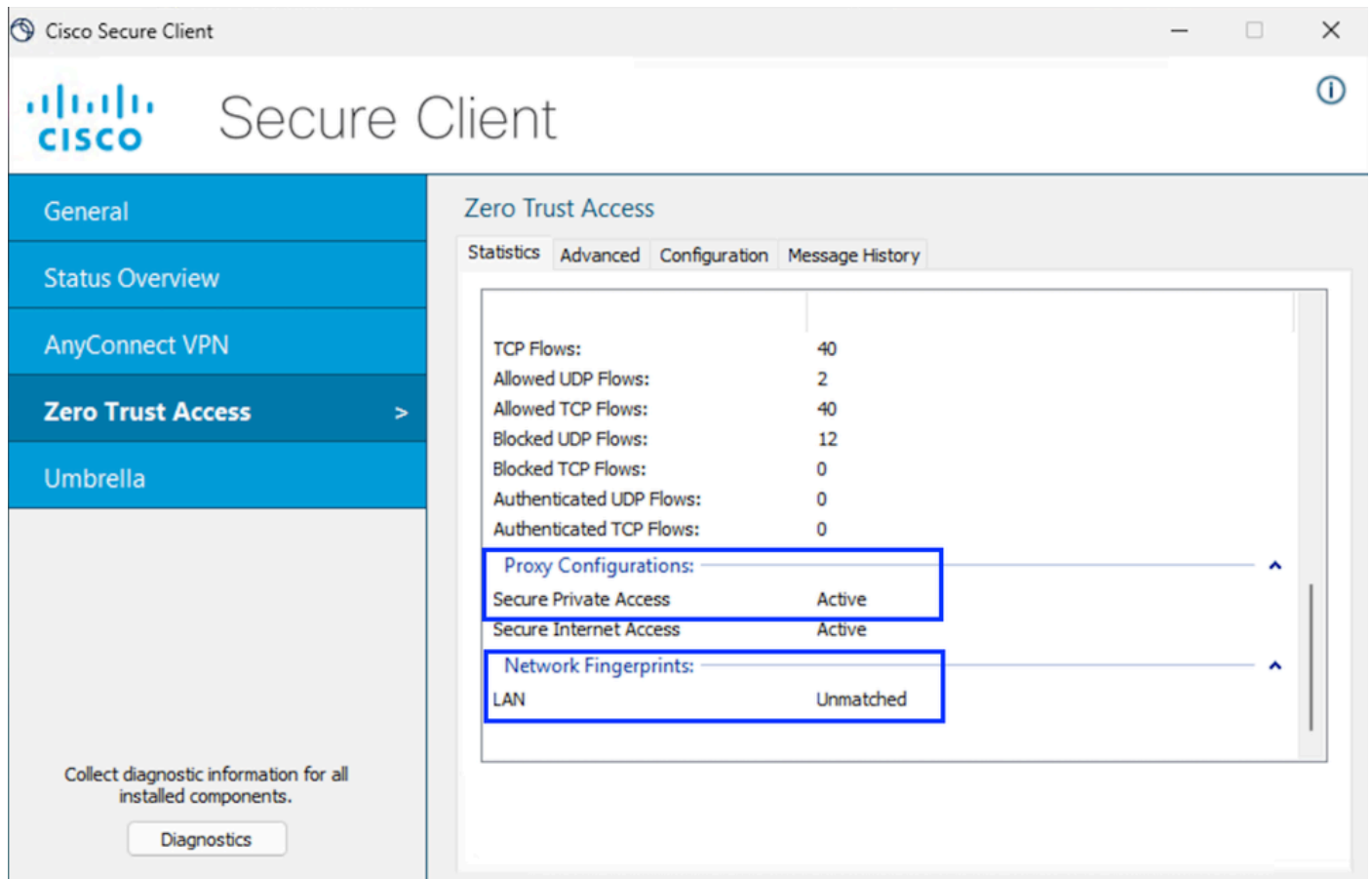


Veilige toegang - PR-testen

5. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten

Wanneer de gebruiker op afstand is

1. Controleer de netwerkvingerafdruk voor ZTA TND, deze moet niet overeenkomen als de gebruiker extern is



Veilige toegang - PR-testen

2. Controleer of de externe gebruiker FTD FQDN kan oplossen

```

C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

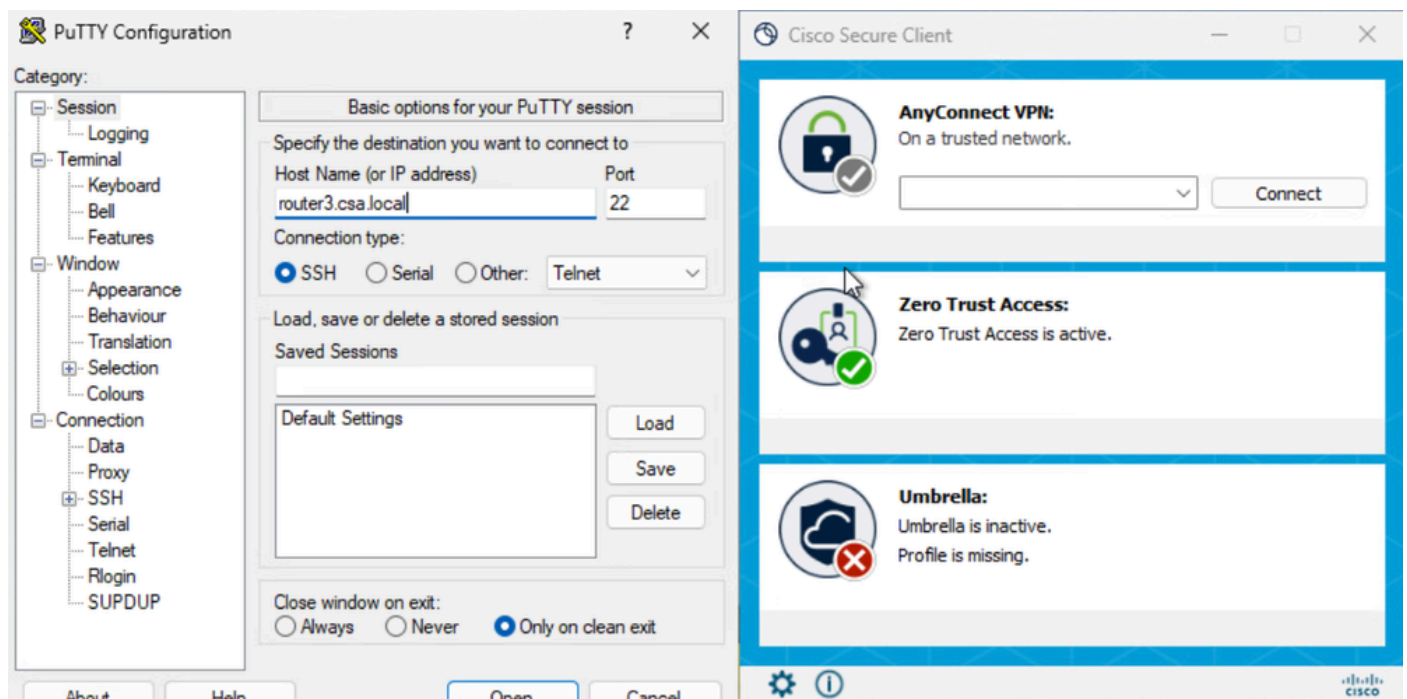
Name: ftd.csa.local
Addresses: 192.168.1.12

```

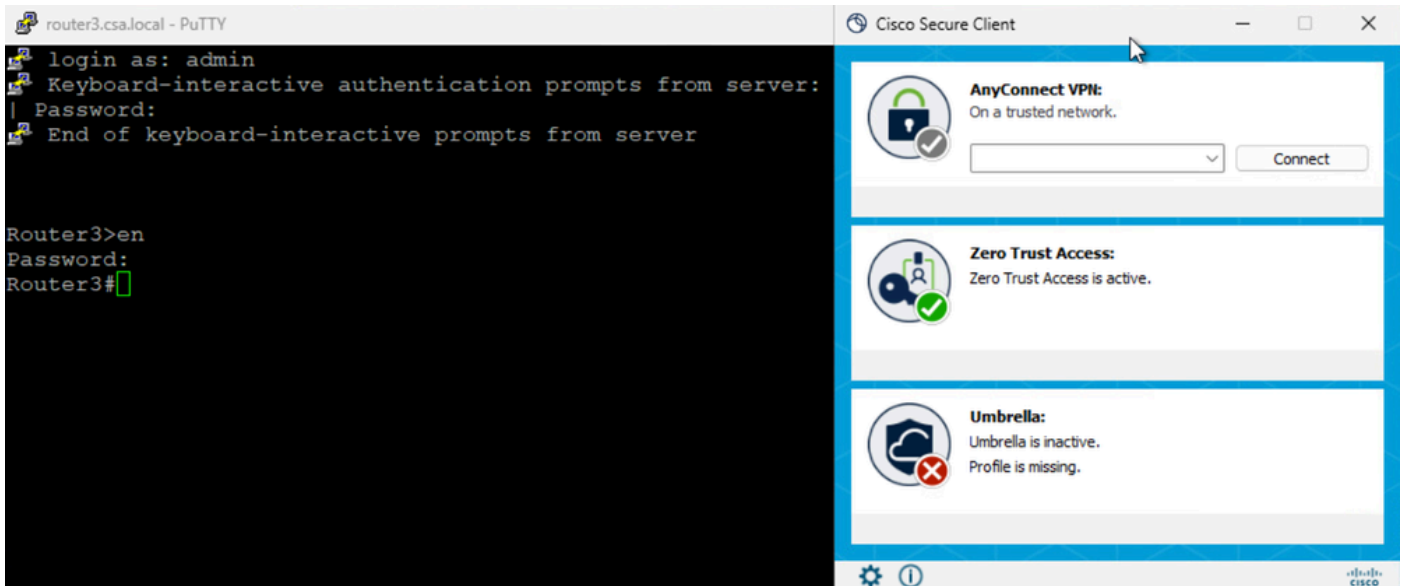
Veilige toegang - PR-testen

3. Test de SSH-verbinding met de Private Resource

Toegang tot de PR via FQDN

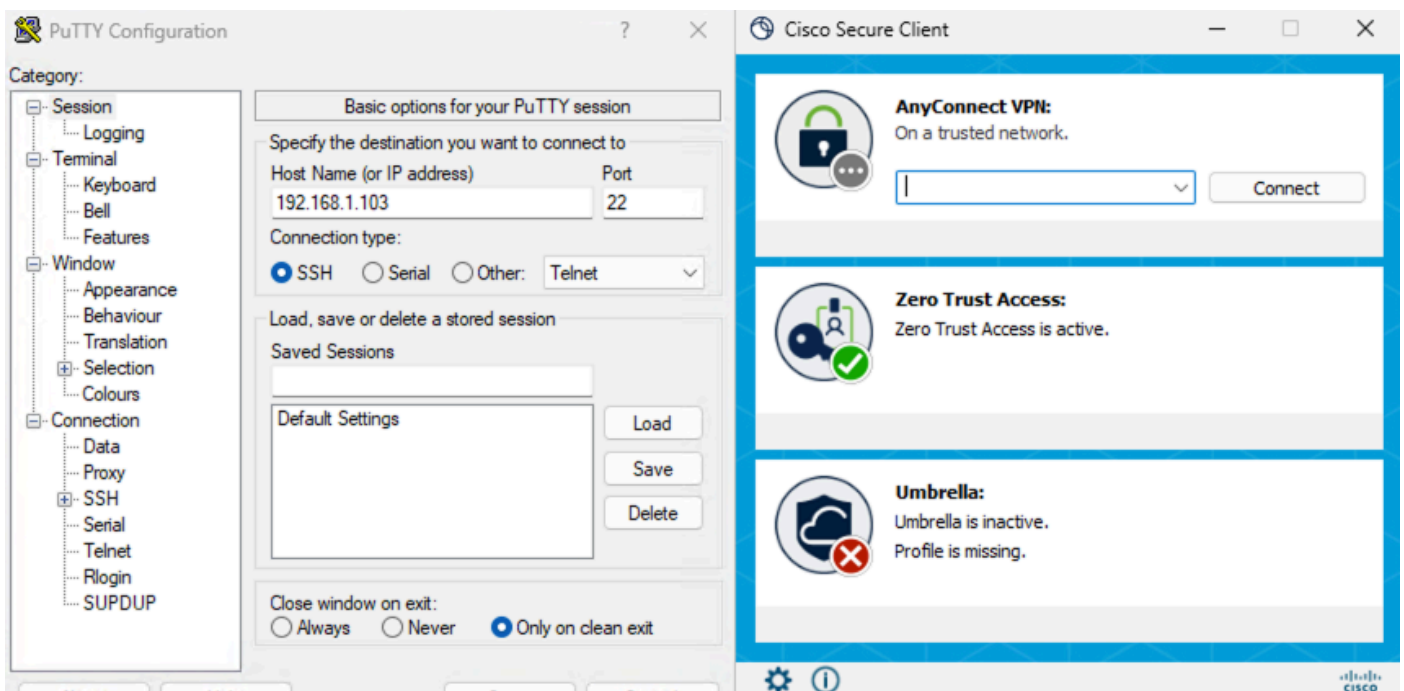


Veilige toegang - PR-testen

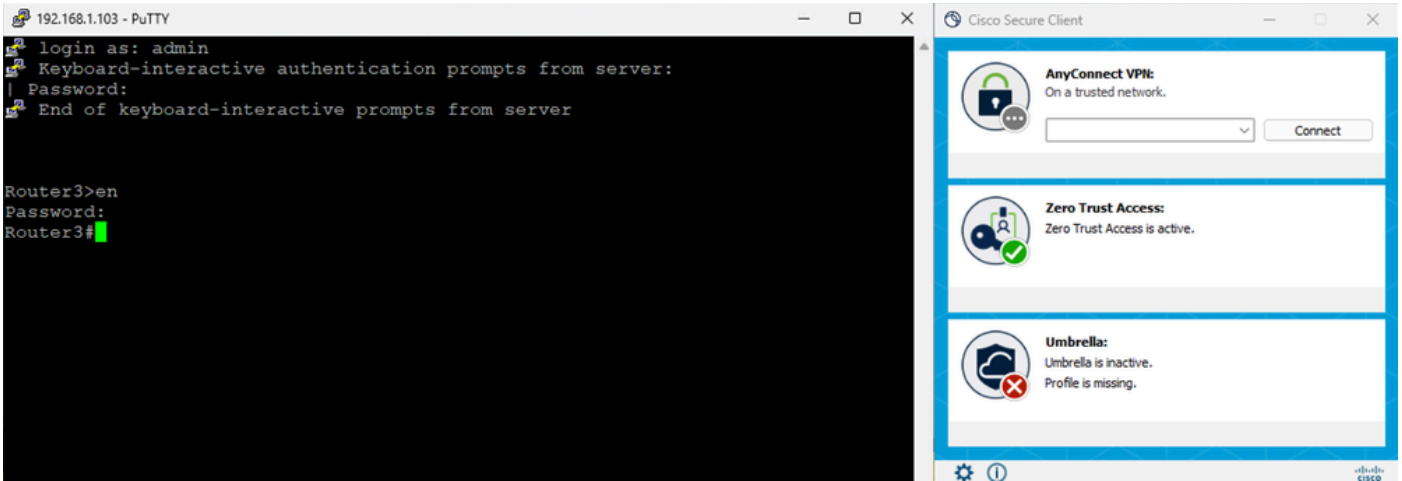


Veilige toegang - PR-testen

Toegang tot de PR via IP-adres



Veilige toegang - PR-testen



Veilige toegang - PR-testen

5. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten

Activity Search

Filters: Search by domain, identity, or URL. Advanced. CLEAR

Response: Allowed

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM. Page: 1. Results per page: 50. 1 - 34 of 34

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow

Veilige toegang - zoeken naar activiteiten

Activity Search

Filters: Search by domain, identity, or URL. Advanced. CLEAR

Response: Allowed

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM. Page: 1. Results per page: 50. 1 - 34 of 34

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/App
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 7:30 AM

Access details

Identity: Jay (jay@csa.local)

ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: router3.csa.local

Destination IP: 192.168.1.103

Problemen oplossen

Nuttige opdrachten:

- > Toegewezen-kernprofiel tonen
- > ASP Inspect-DP-snort tonen
- > SH Running-Config Universal-Zero-Trust
- > Interface IP-samenvatting tonen

> Debug Universal-Zero-Trust Zproxy 7

Ja, en ga dan naar Expert Mode

```
# tail -f /ngfw/var/log/messages
```

```
# Toon alle
```

```
# NAT-details weergeven
```

```
# ASP-tabelsocket tonen
```

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.