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

- Netwerkdiagram
- 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

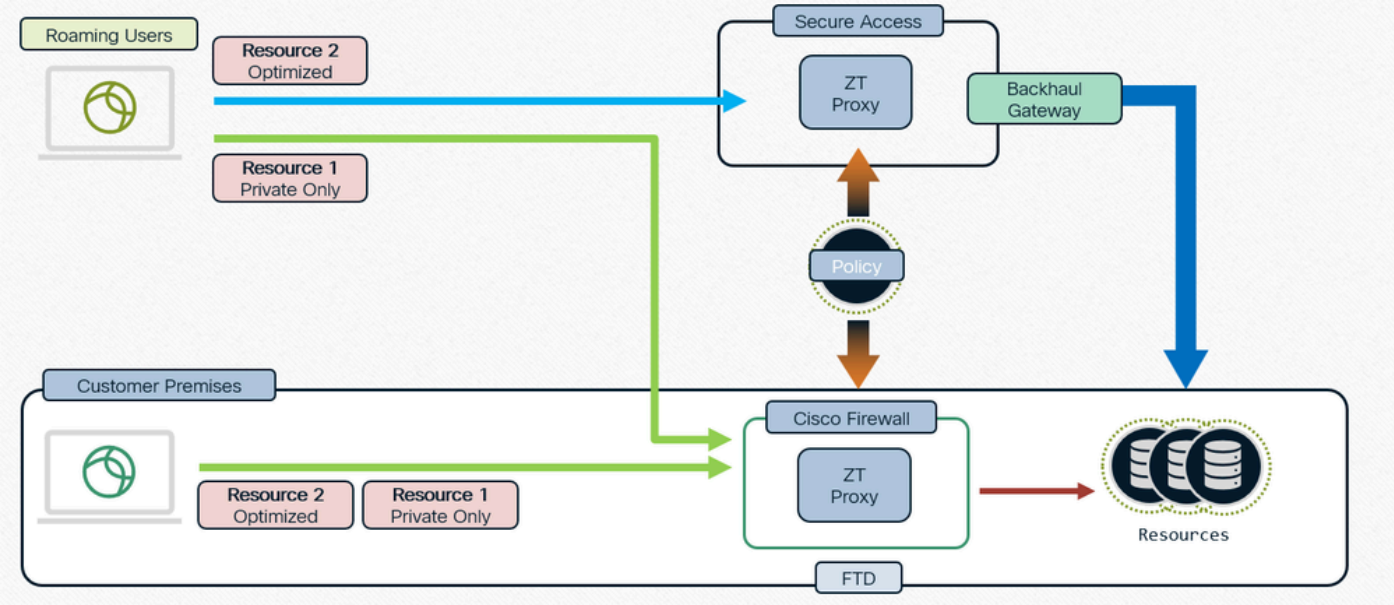
Universal Zero Trust Network Access (uZTNA) stelt beheerders in staat om specifiek toegang tot

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 verminderd.

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

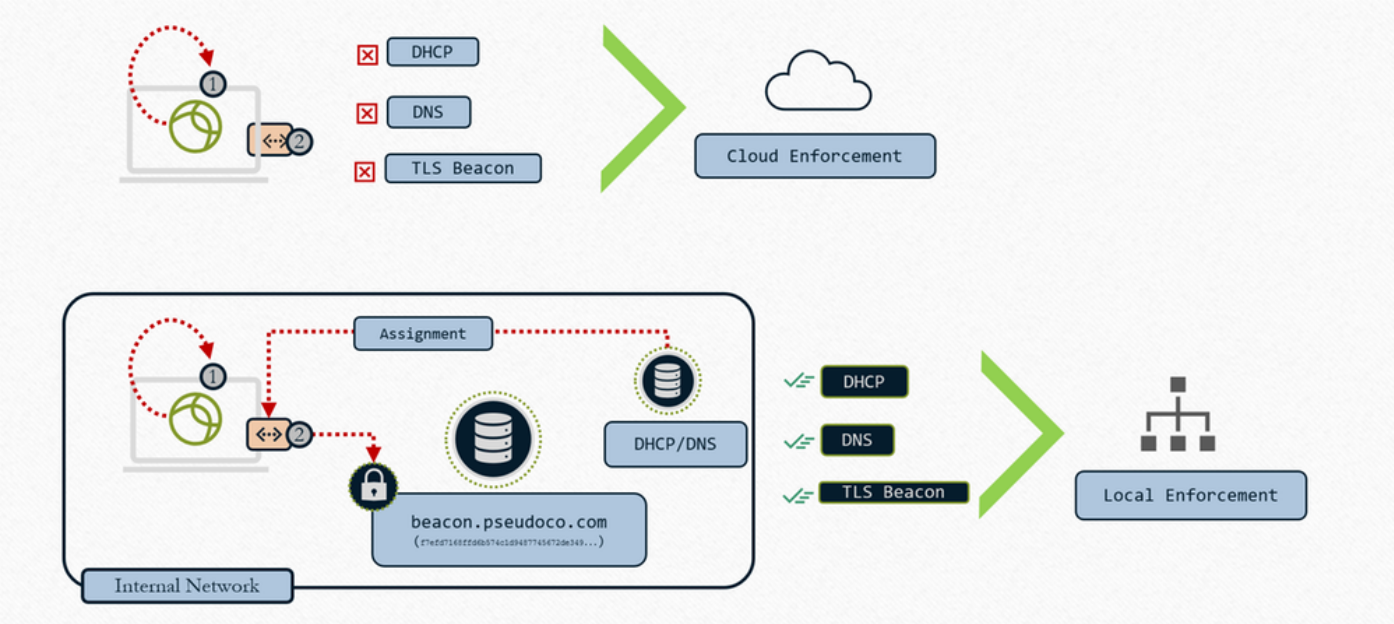
Verkeersproxy, evenals IPS-, bestands- en malwarebeleidshandhaving, wordt uitgevoerd op de Firepower Threat Defense (FTD).



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

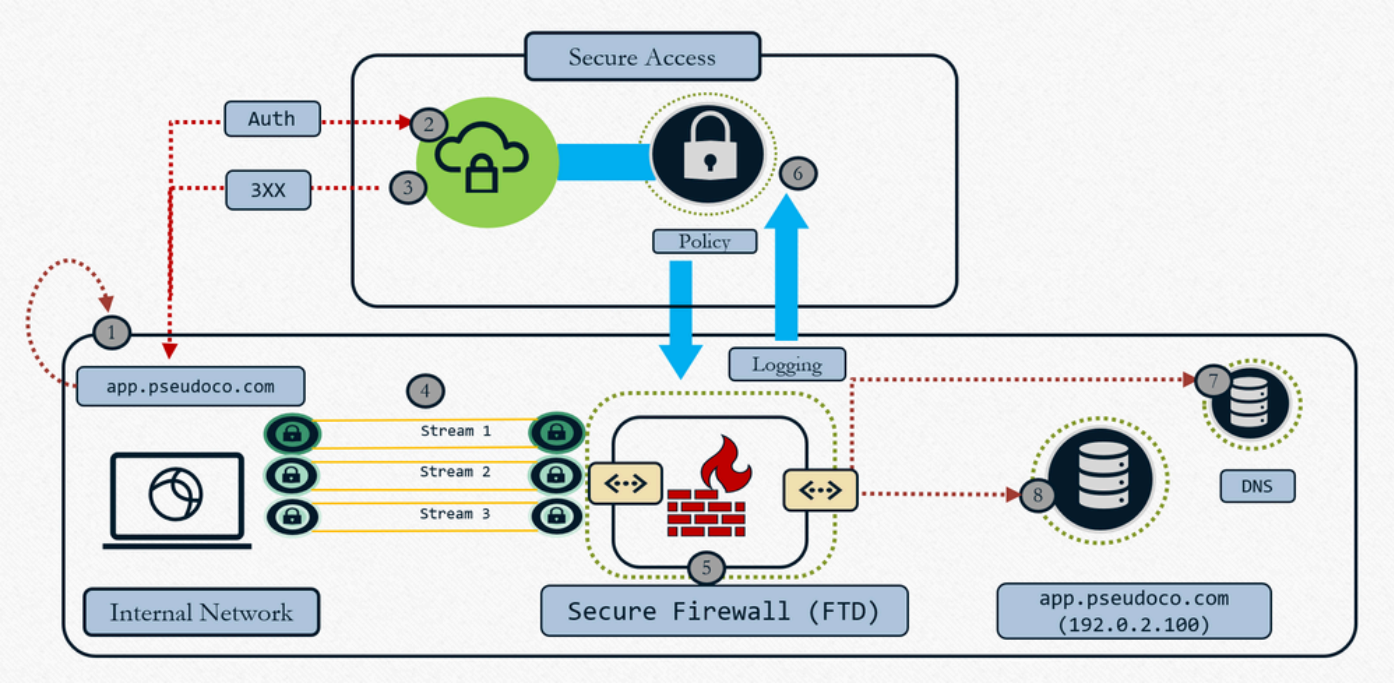
3- Als de voorwaarde overeenkomt – Lokale handhaving

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

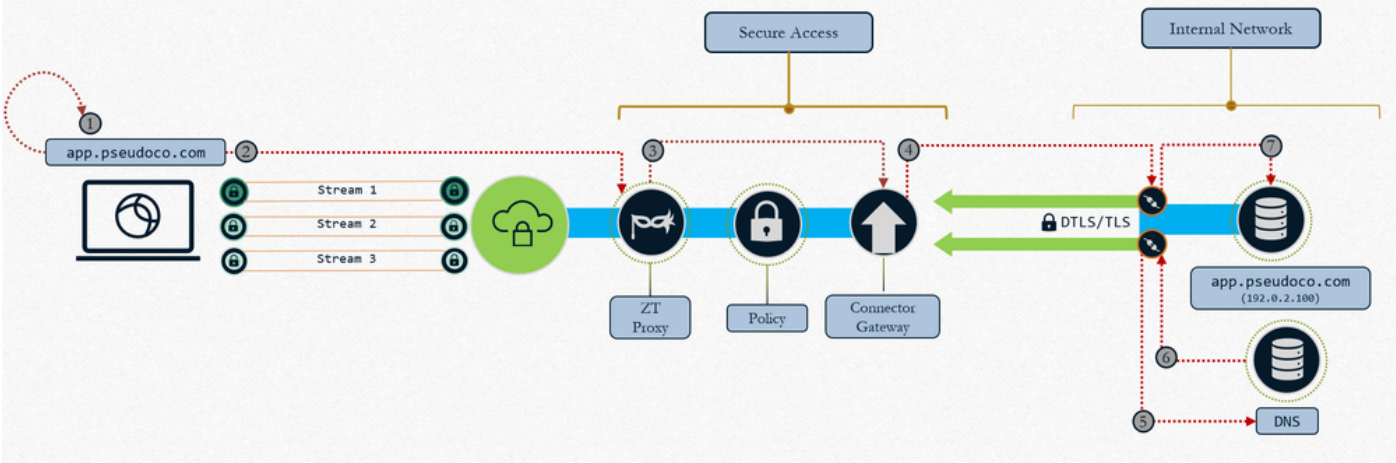
- Lokaal handhavingspad: Firewall Enforcement



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

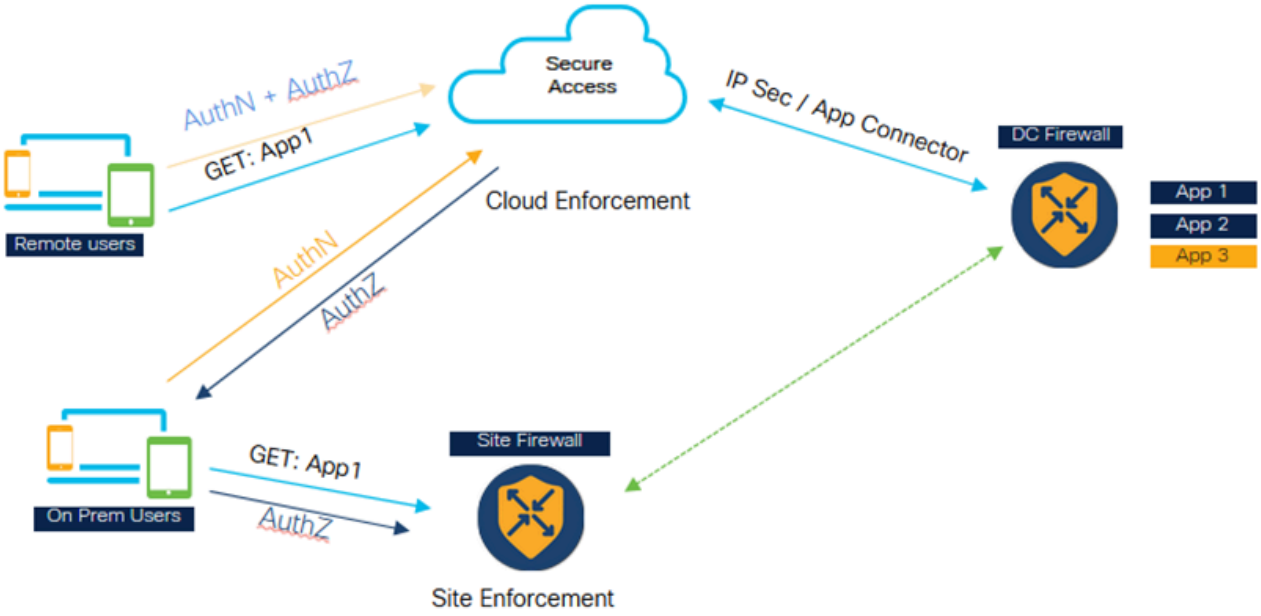


Universal ZTNA: Cloud Enforcement

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

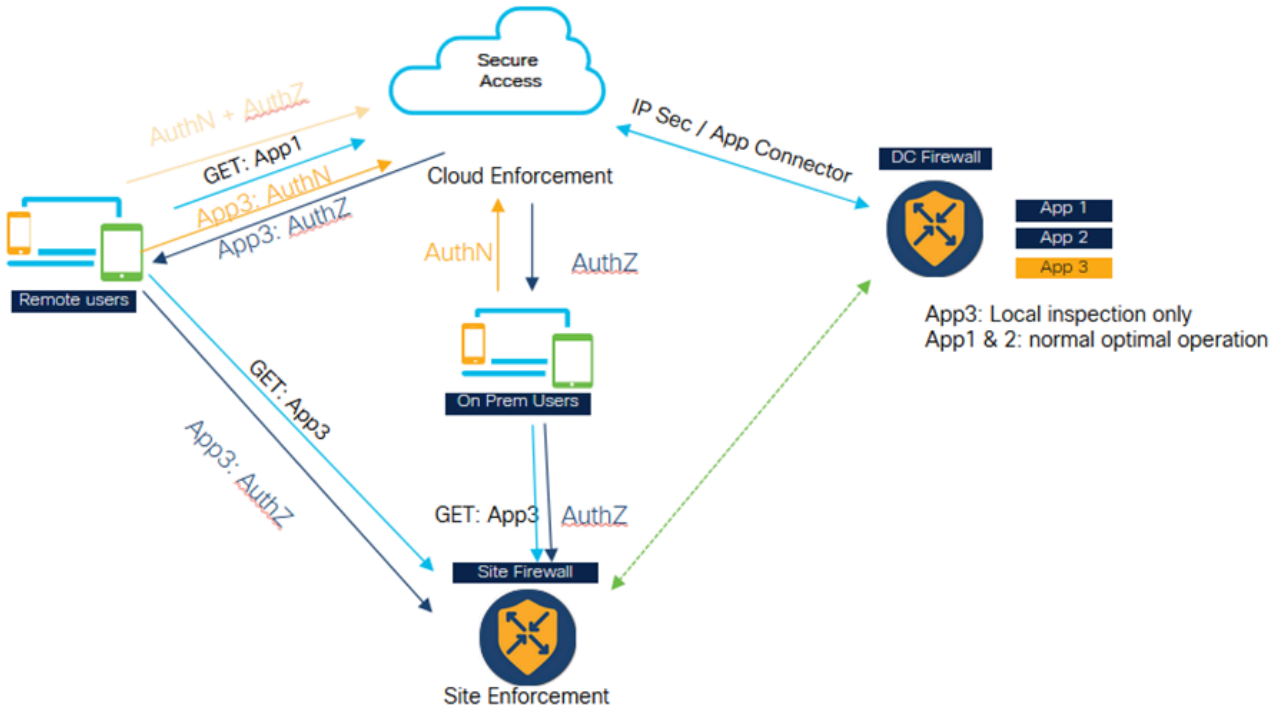
Geval 1: Consistente en geoptimaliseerde ZTNA voor gebruikers op locatie



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

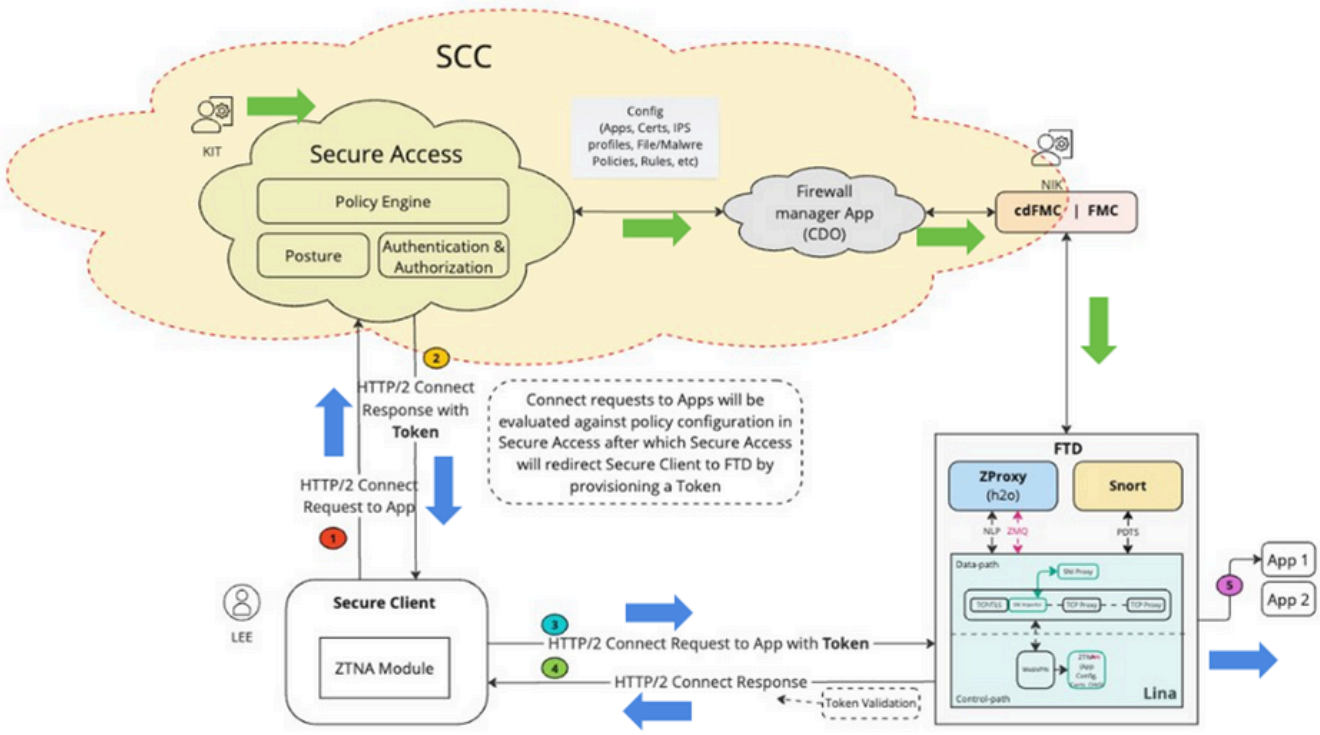
Geval 2: Particuliere inspectie voor gevoelige toepassingen



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 authentiken, dat de firewall vertelt dat deze al is geverifieerd en geautoriseerd. De authenticatie token is versleuteld, ondertekend door Secure Access

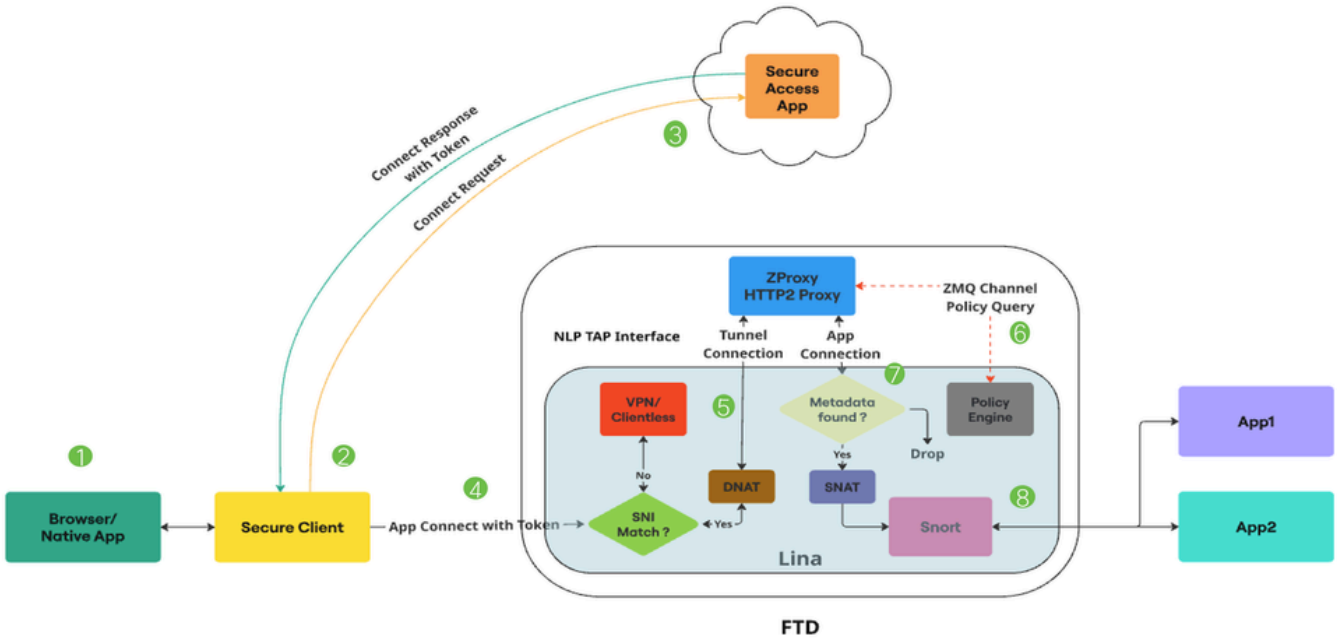
3. Secure Access leidt de beveiligde client om naar FTD, samen met het auth-token.

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 proporteren.(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:

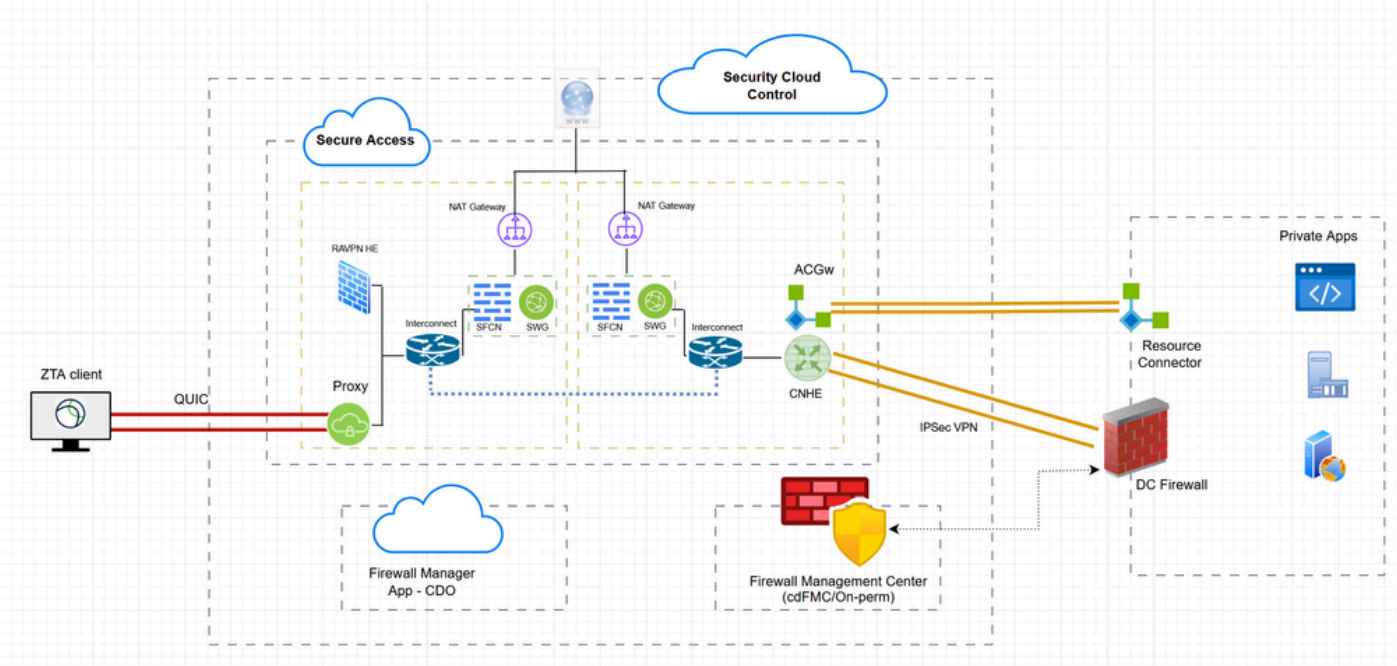
169.251.1.2) als bron-IP. Dit wordt vertaald naar de FTD-uitgang IP-interface, voordat deze wordt verzonden. Lina markeert vervolgens Universal Zero Trust-stromen voor Snort-inspectie alleen als een bestand of IPS-beleid aanwezig is in de toegangstoken.De regel-ID die is verkregen uit de toegangstoken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

9. De Universal Zero Trust-regels en de bijbehorende bestands- en IPS-beleidsmappings 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

Netwerkdiagram

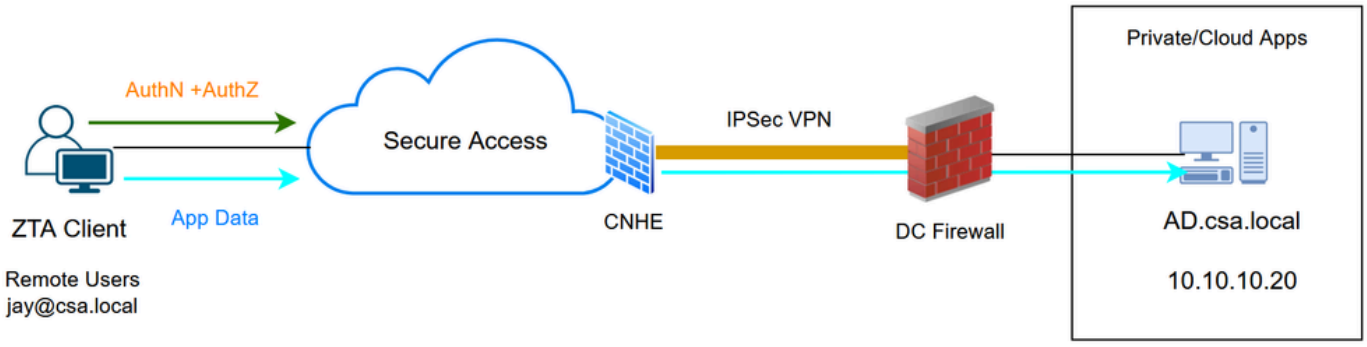


Hybride ZTNA - netwerkdiagram

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

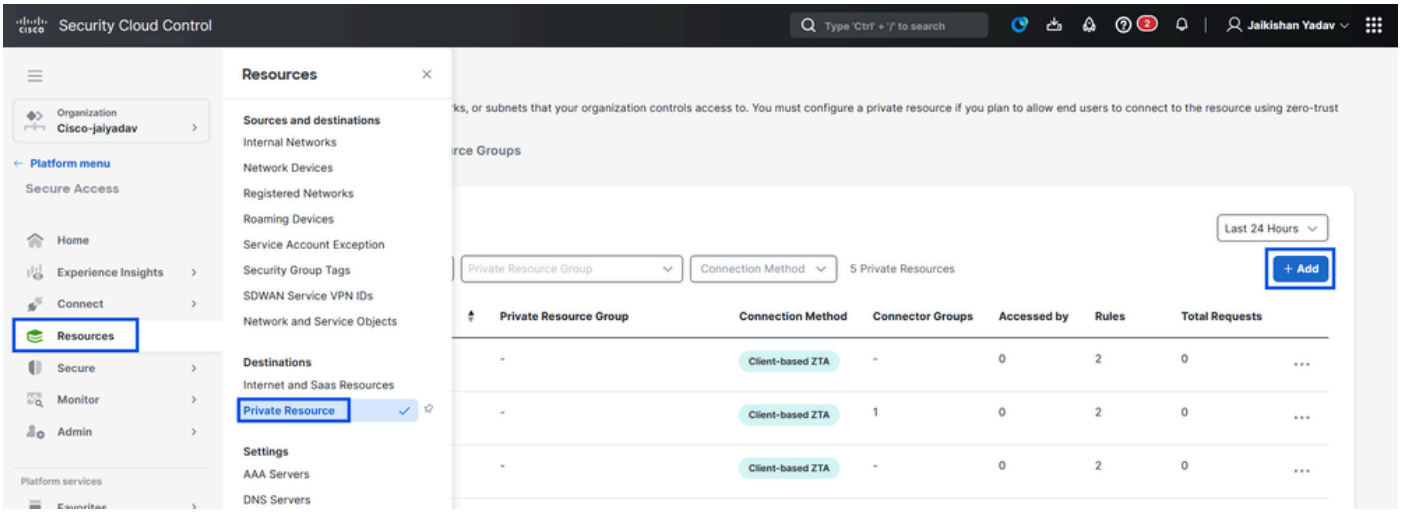


Universele ZTA - Test case topologie

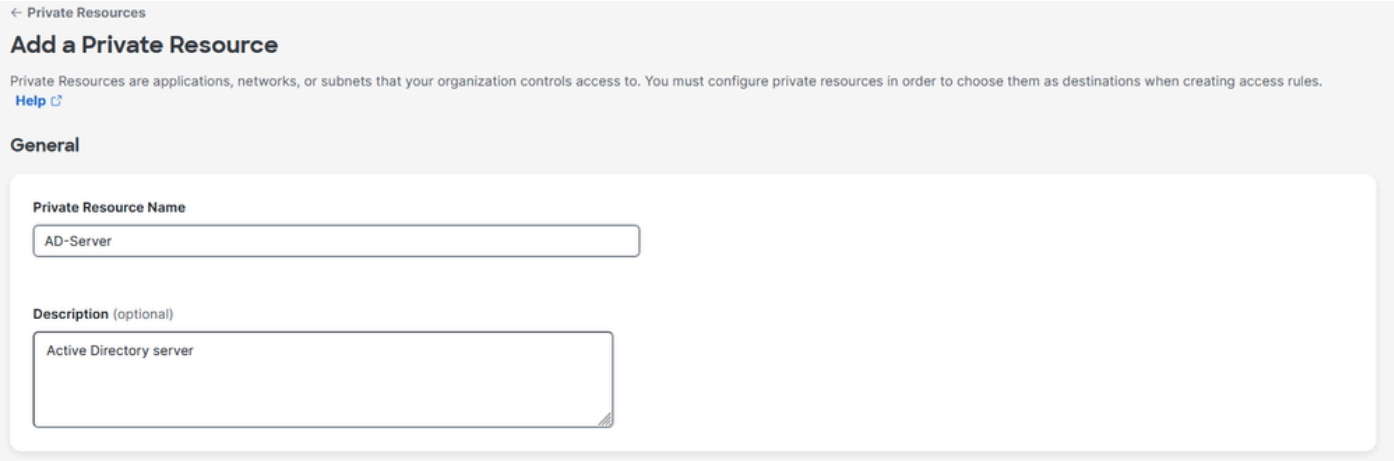
Stap 1 - Een privébron definiëren voor beveiligde toegang

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

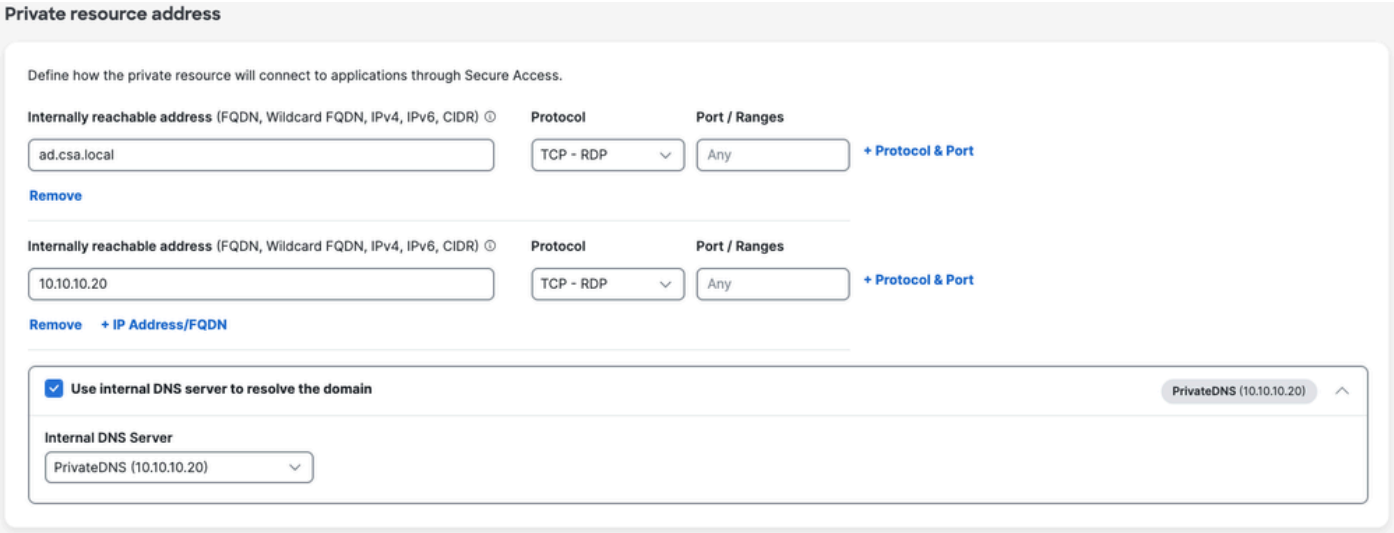


2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.

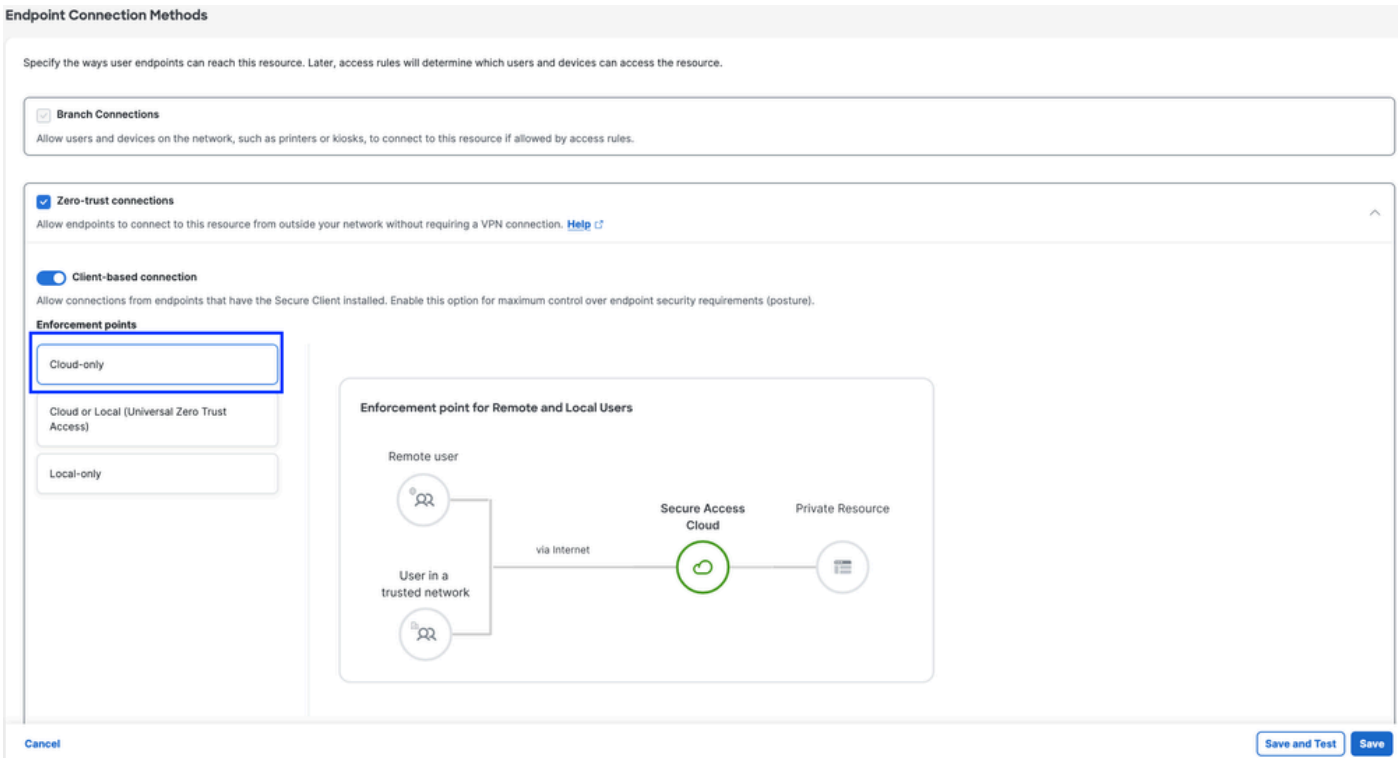


3. Voer het FQDN in van de privébron die u wilt openen. We kunnen ook het IP-adres van de privébron definiëren. Zie Een privébron toevoegen voor meer informatie

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



5. Selecteer methoden voor eindpuntverbinding



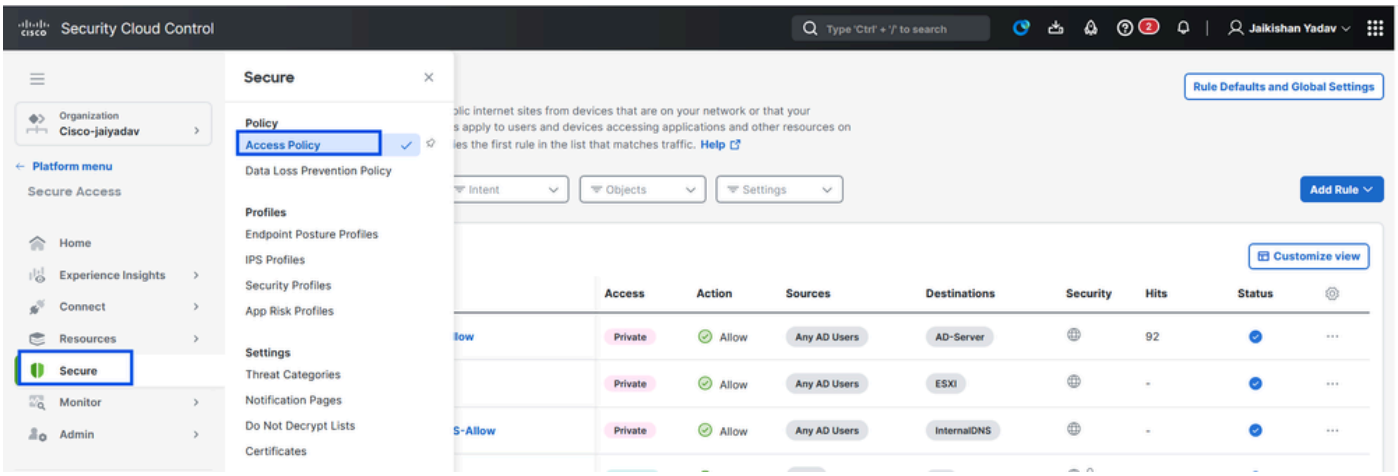
Veilige toegang - Configuratie van privébronnen

6. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

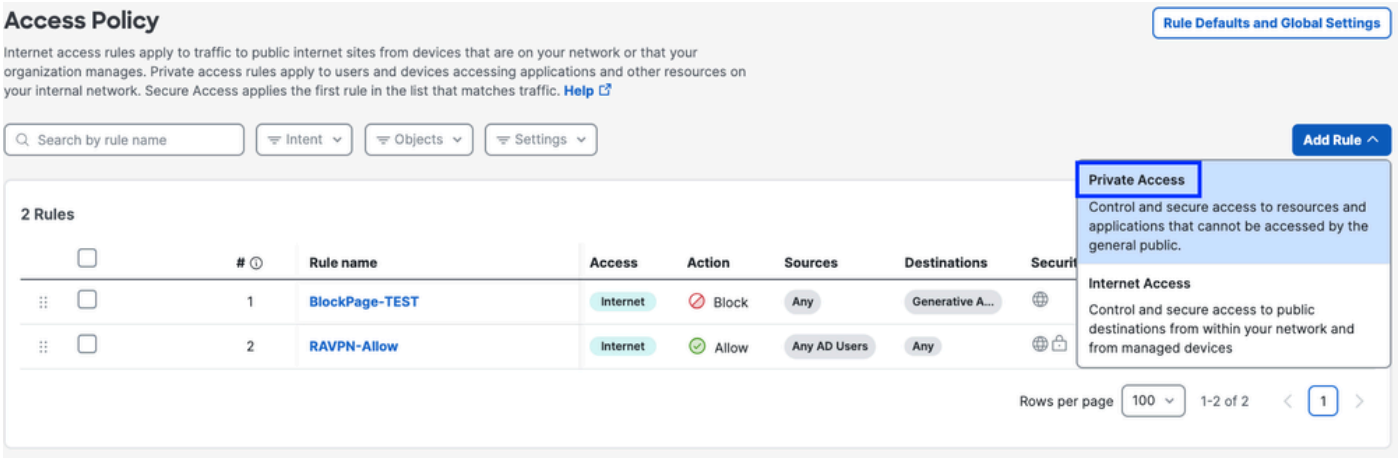
Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie Private Access Rule

1. Navigeer naar Beveiligd > Toegangsbeleid



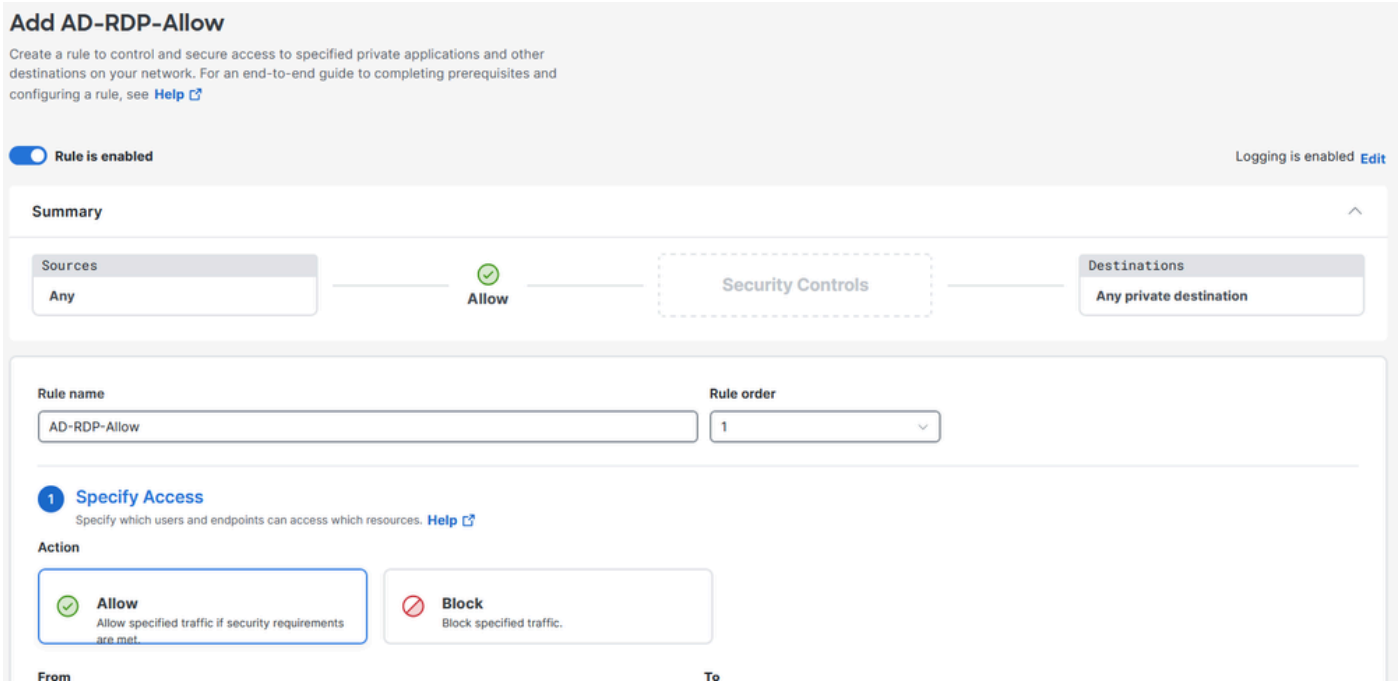
Beveiligde toegang - Configuratie toegangsbeleid

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.
Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.



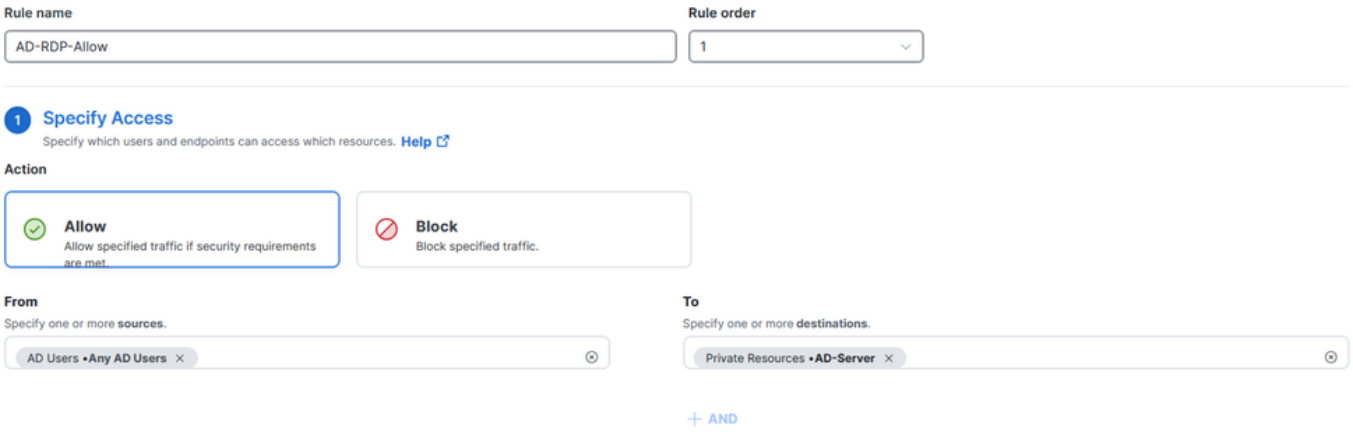
Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen



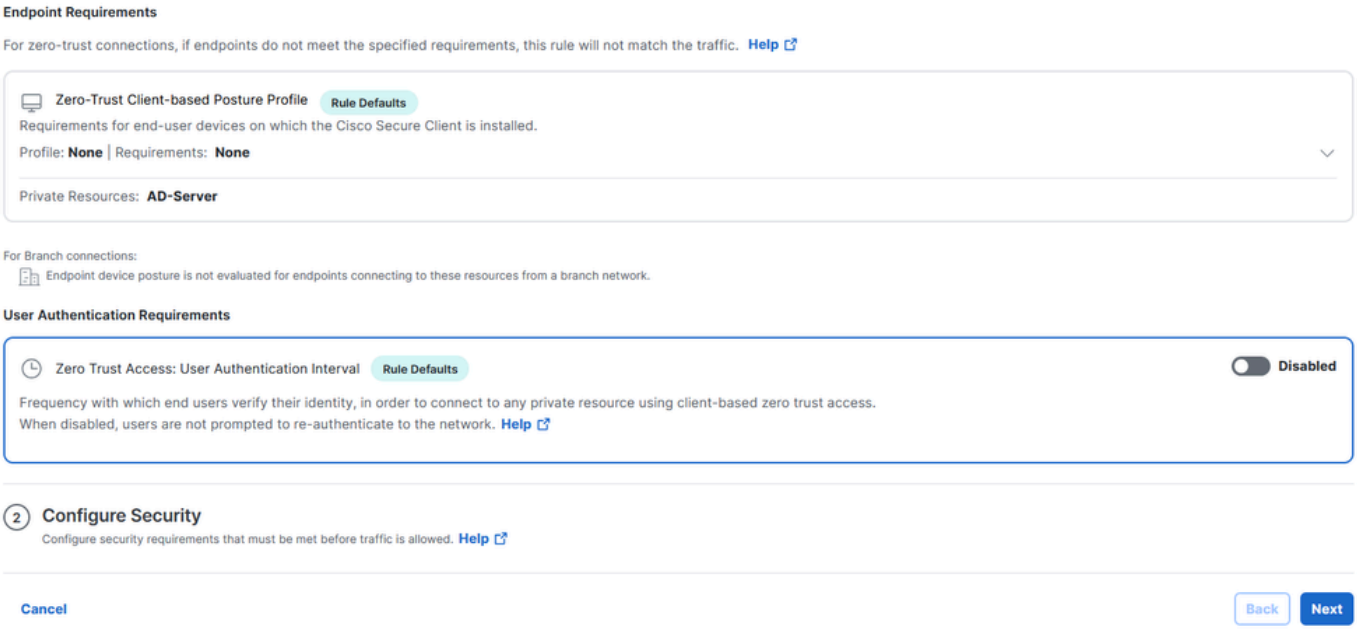
Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming



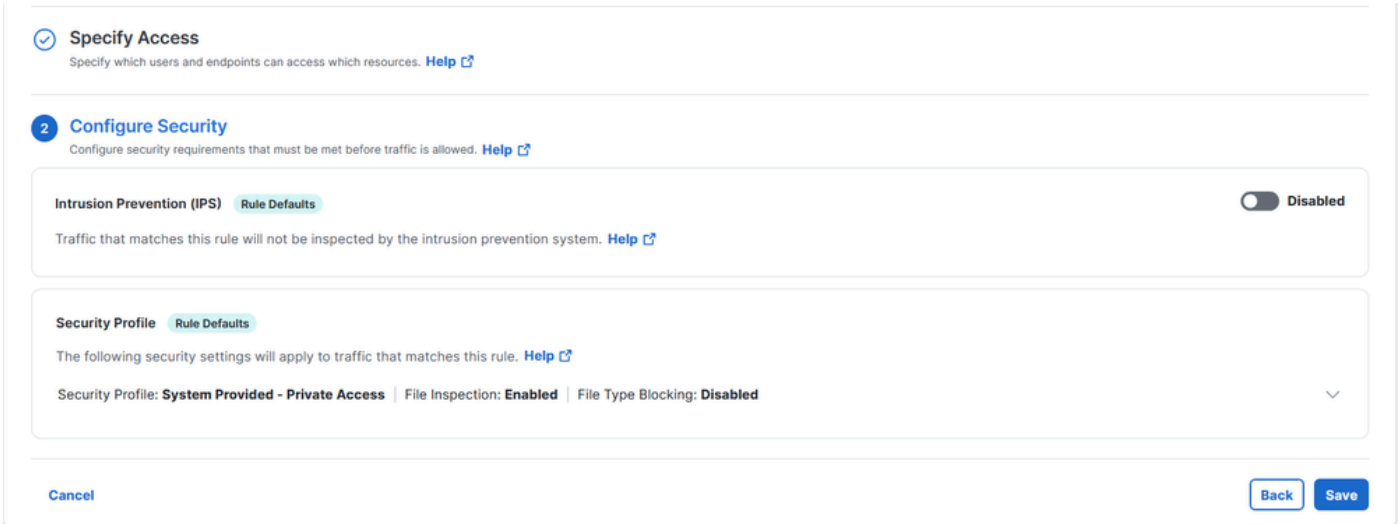
Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren



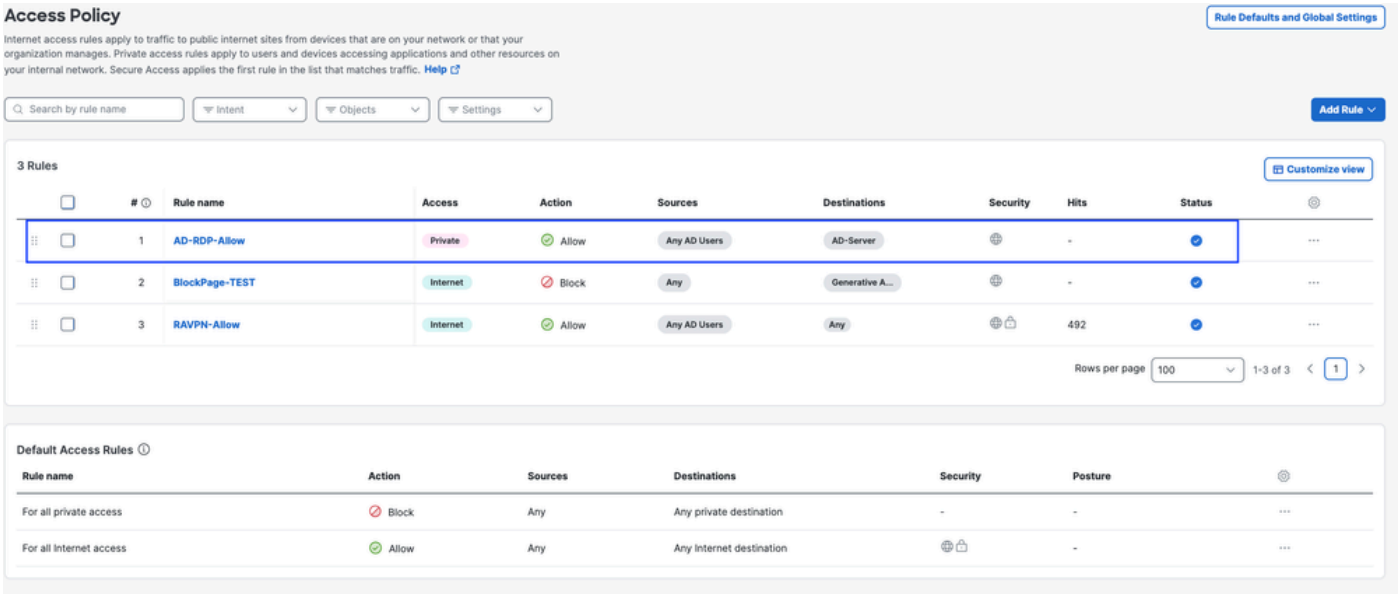
Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren



Beveiligde toegang - Configuratie toegangsbeleid

7. Klik op Opslaan

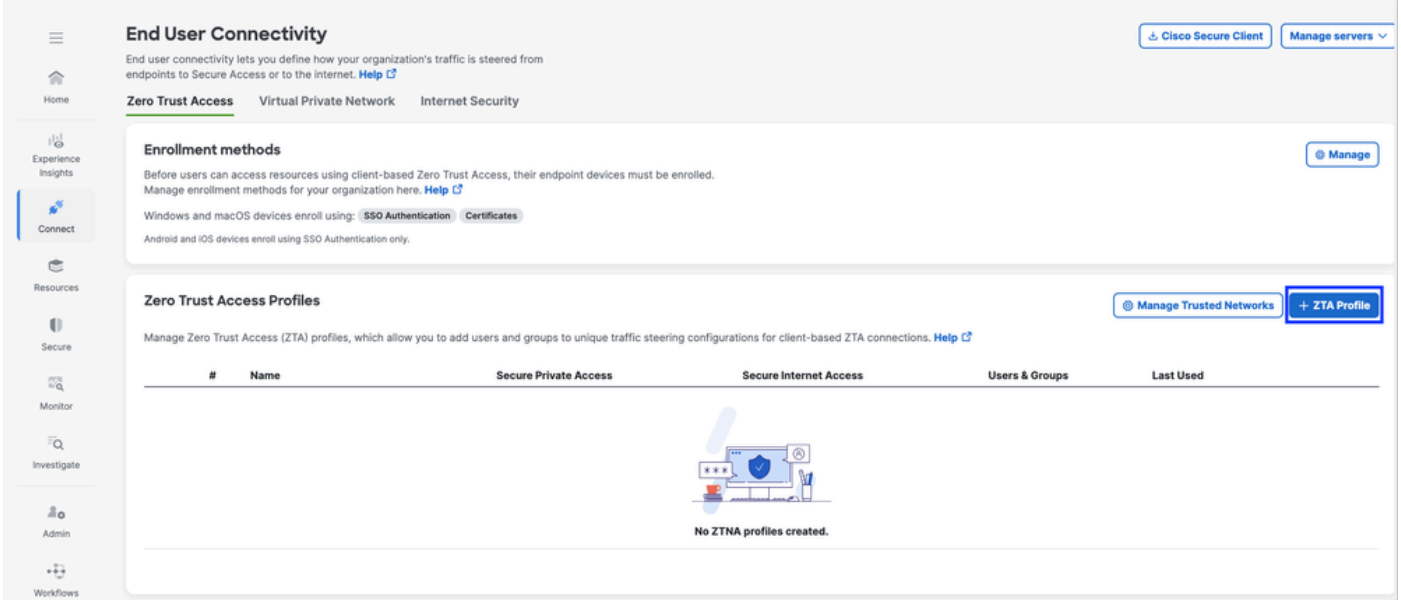


Beveiligde toegang - Configuratie toegangsbeleid

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

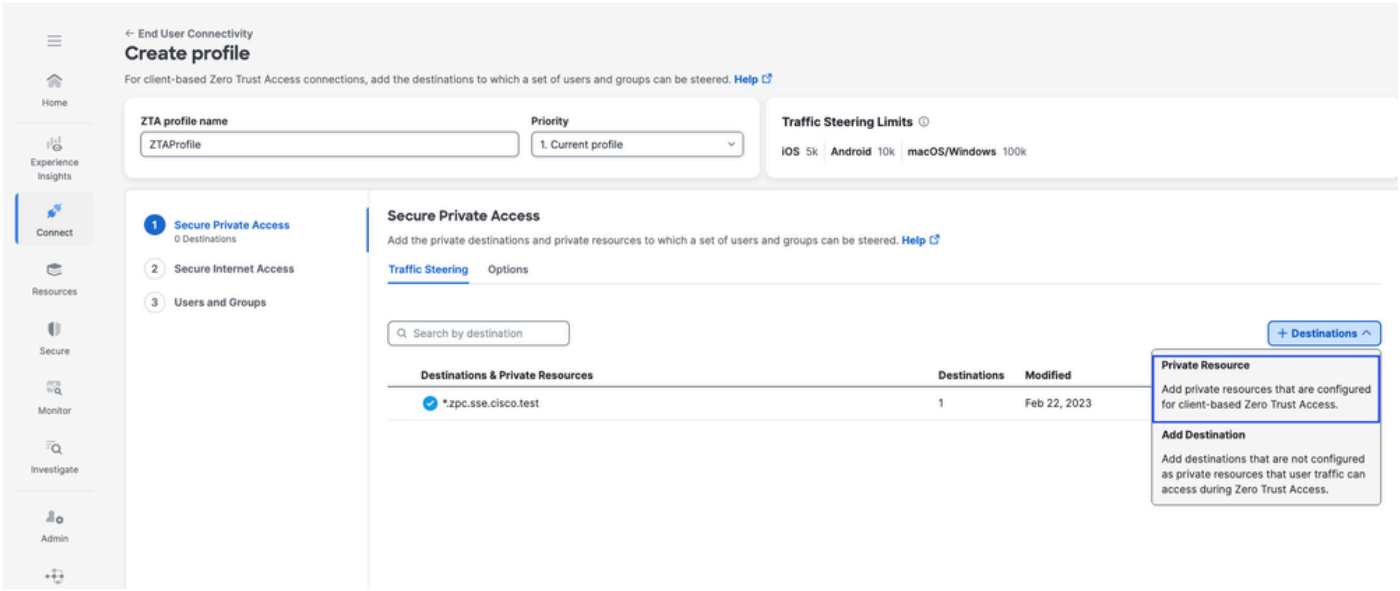
Als u een aangepast ZTA-profiel gebruikt, moet u de respectieve privébron toevoegen aan het ZTA-profiel

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

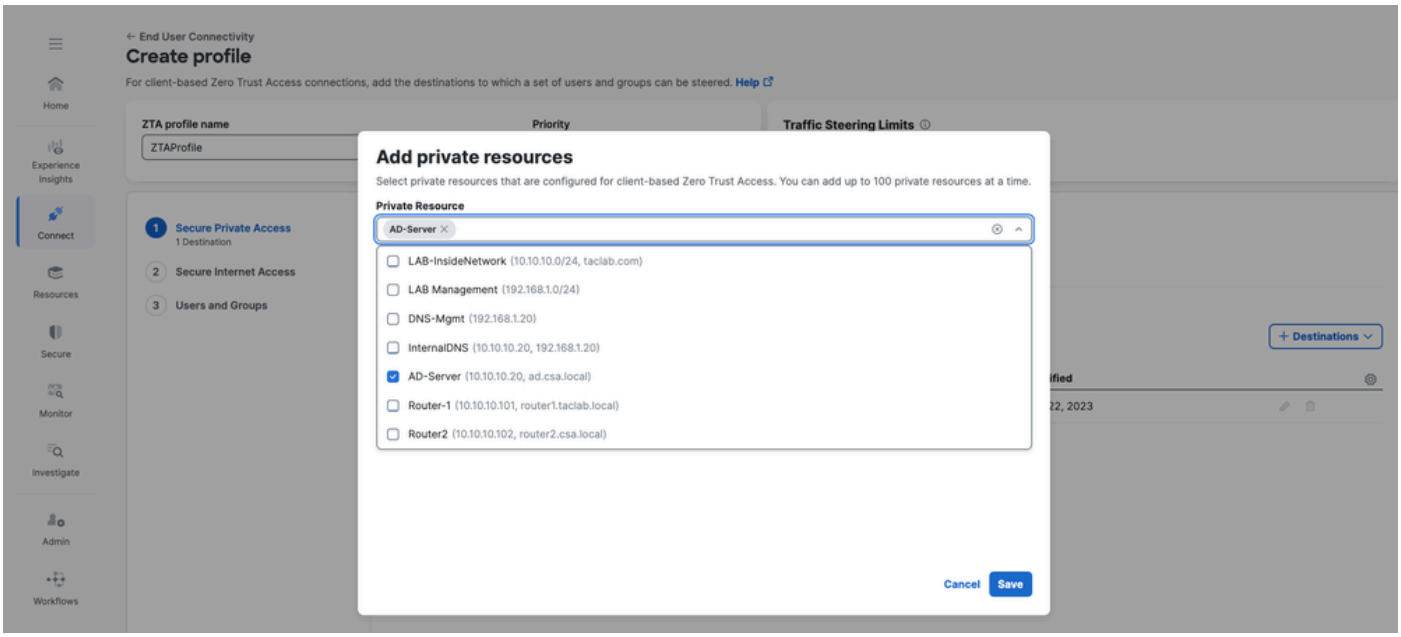


Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

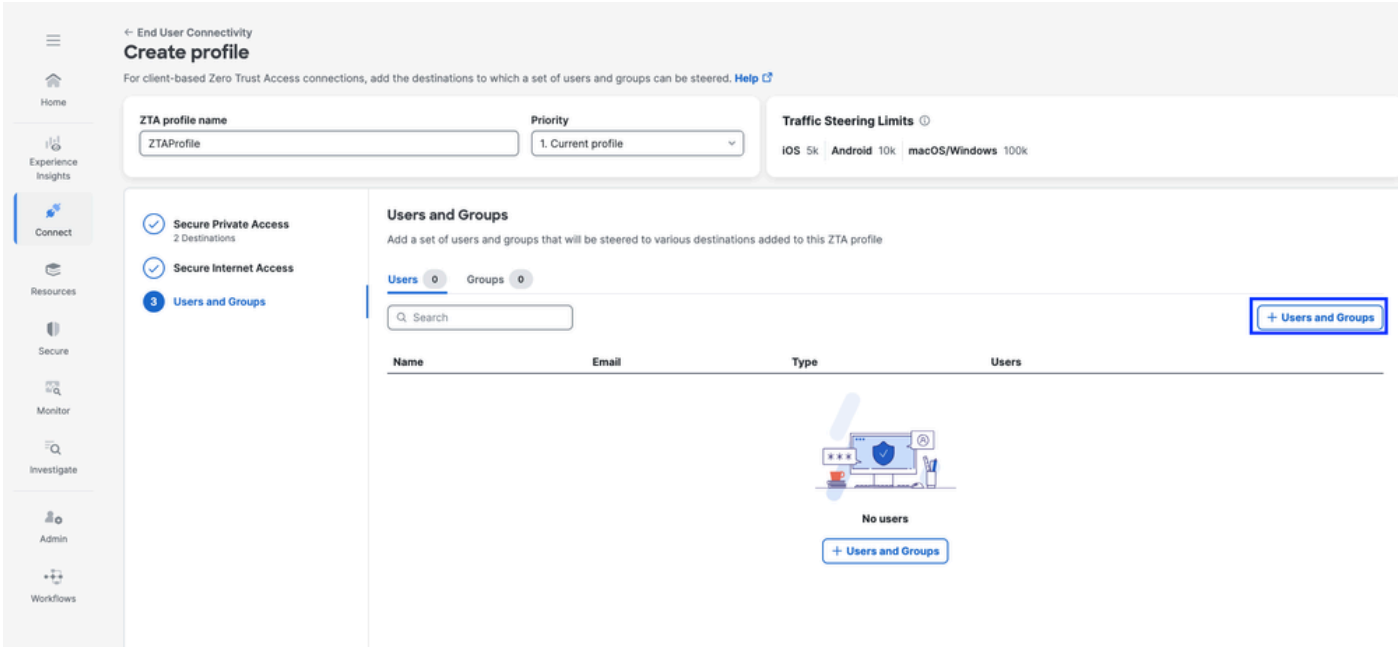


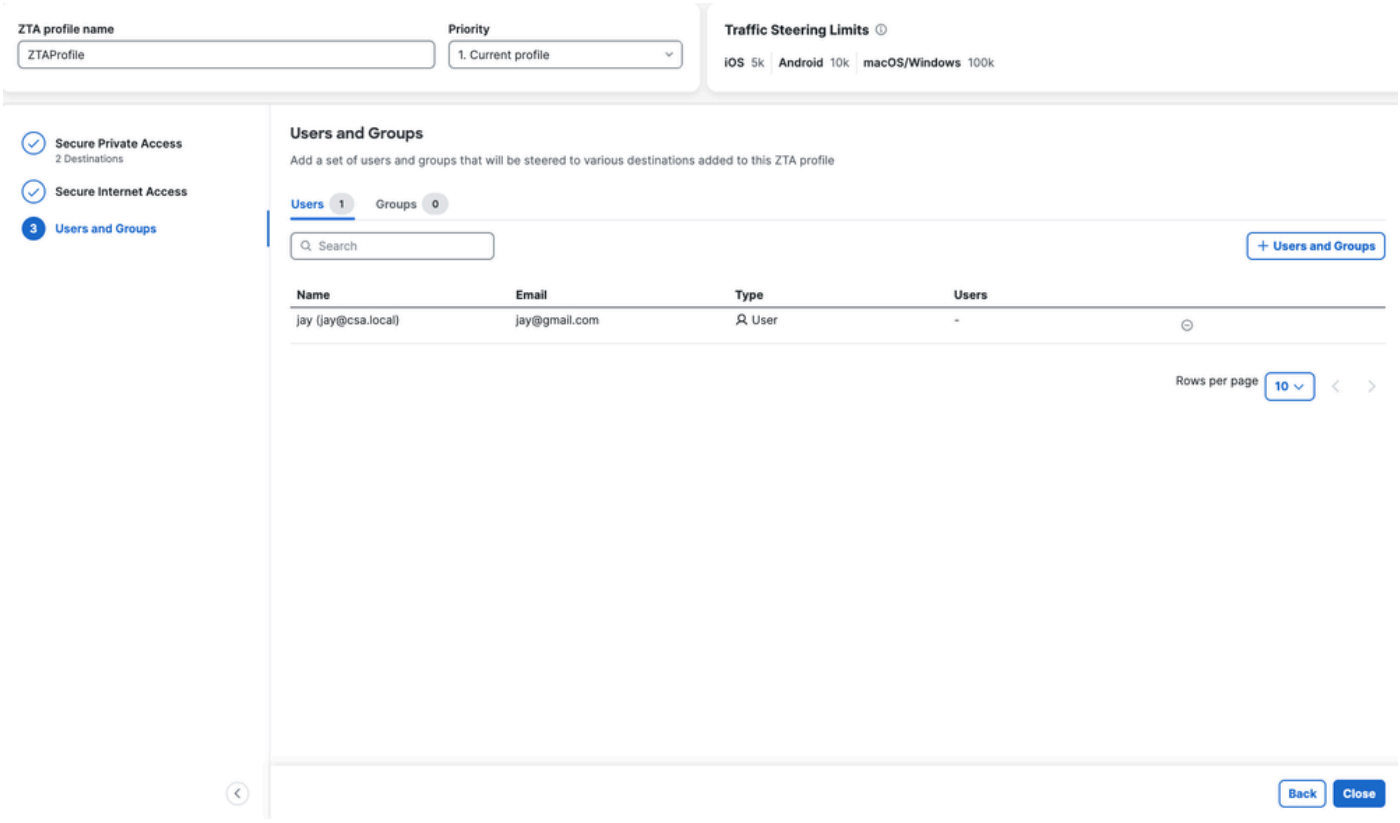
Veilige toegang - ZTA-profiel



Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen





Veilige toegang - ZTA-profiel

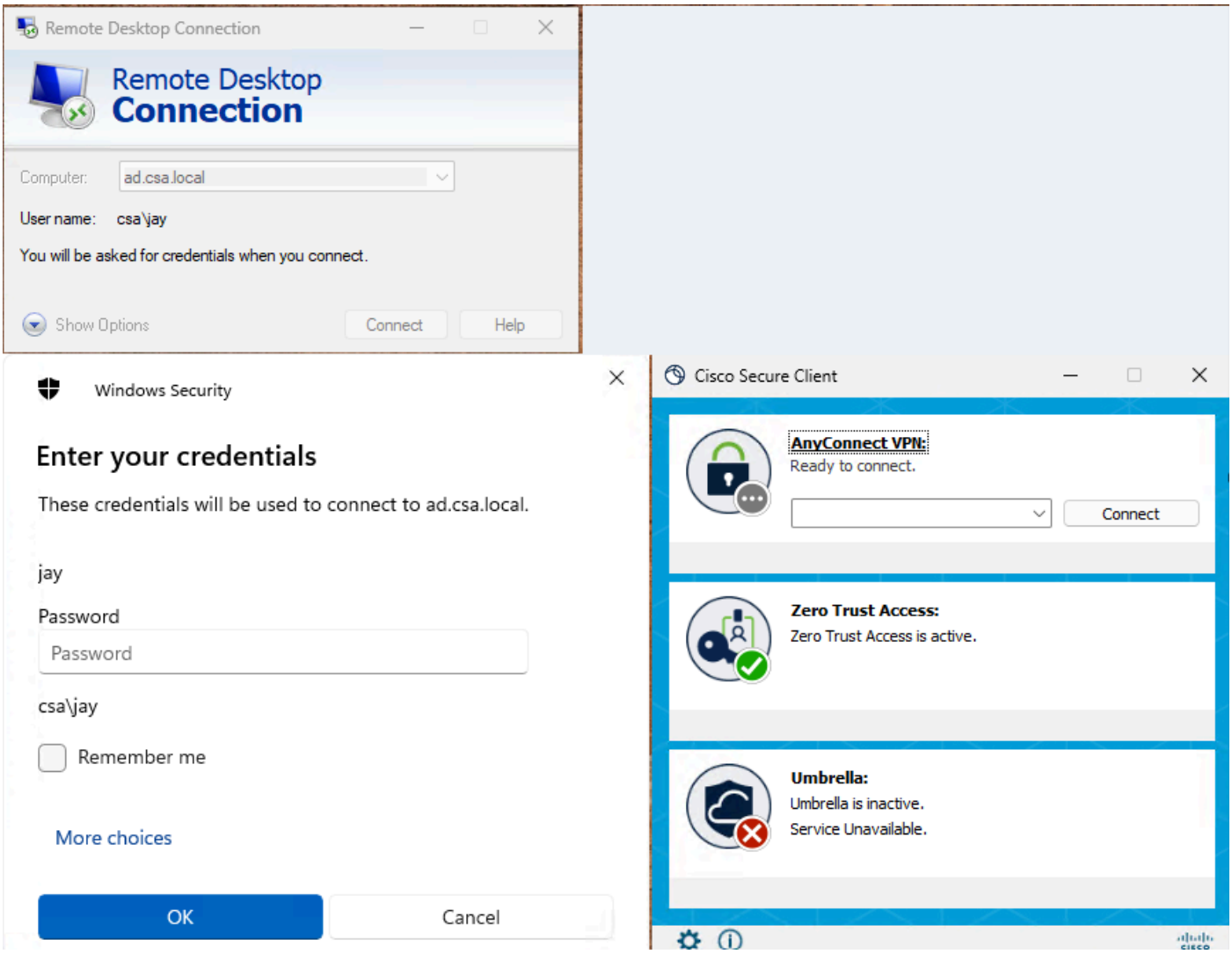
Opmerking: het kan tot 15-20 minuten duren om de configuratie te pushen en te synchroniseren met de client voor de toegewezen privébron

---

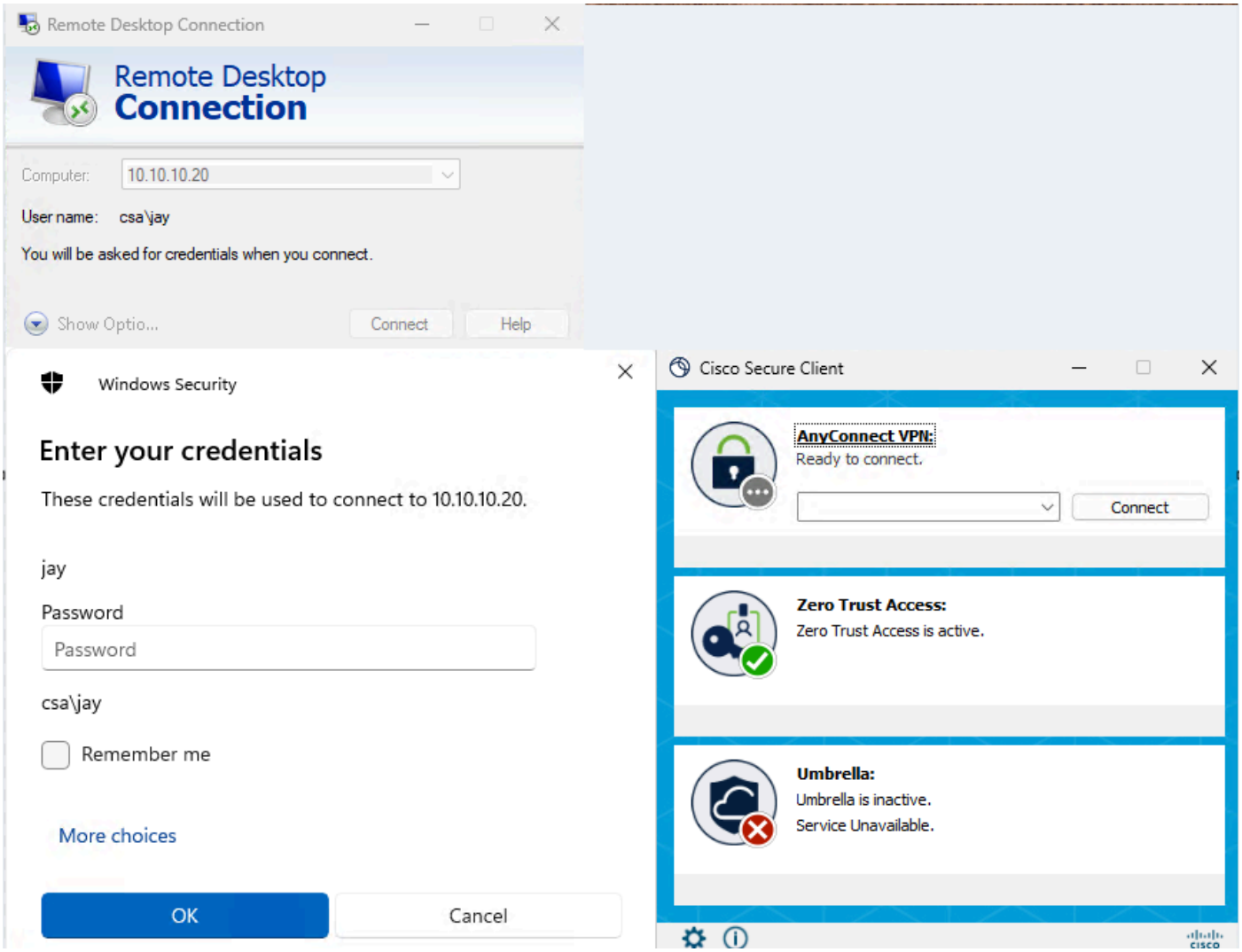
Stap 4: Controleer de toegang tot de privébron

1. Toegang tot de particuliere middelen

Toegang tot de PR via FQDN

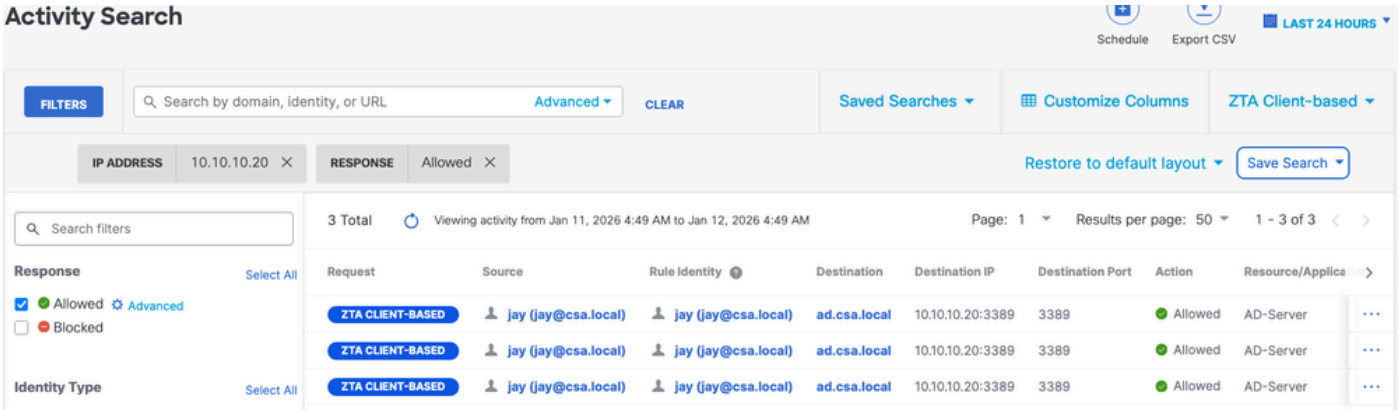


Toegang tot de PR via IP-adres

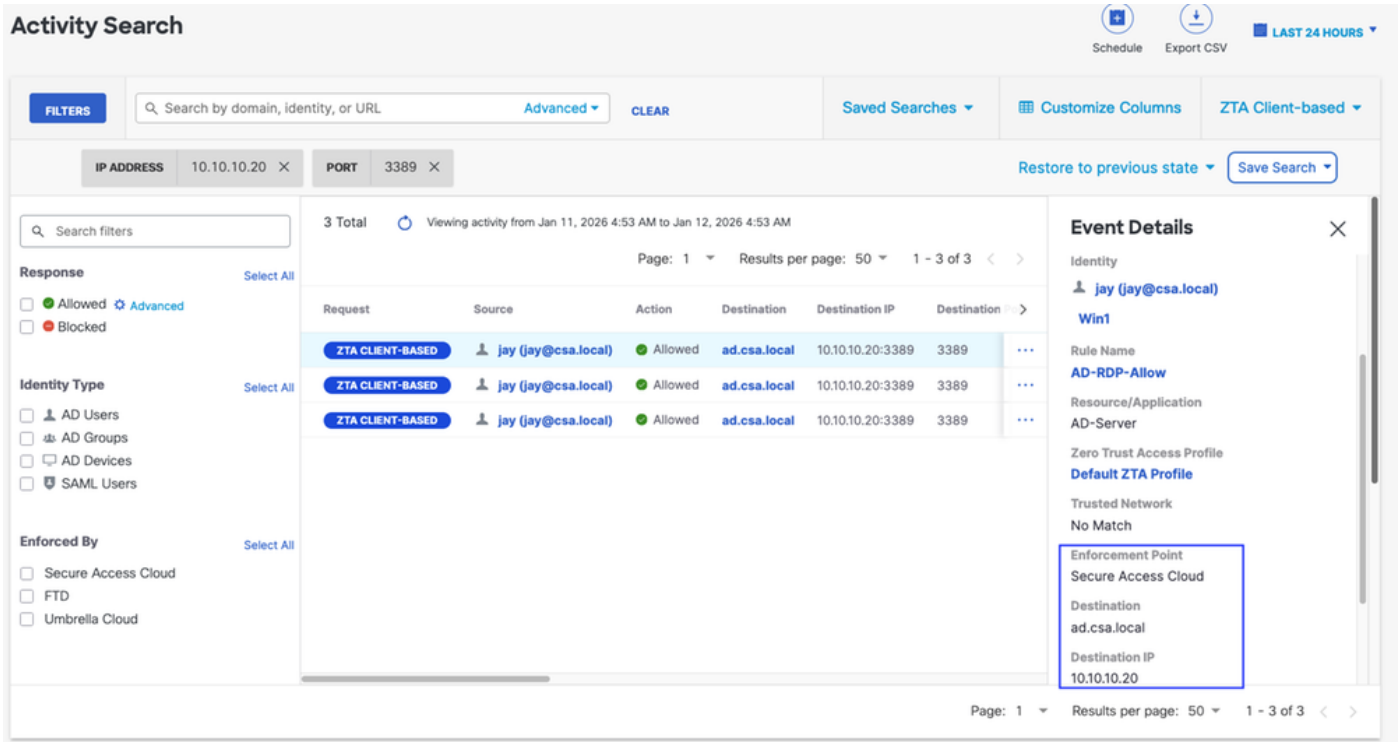


Veilige toegang - PR-testen

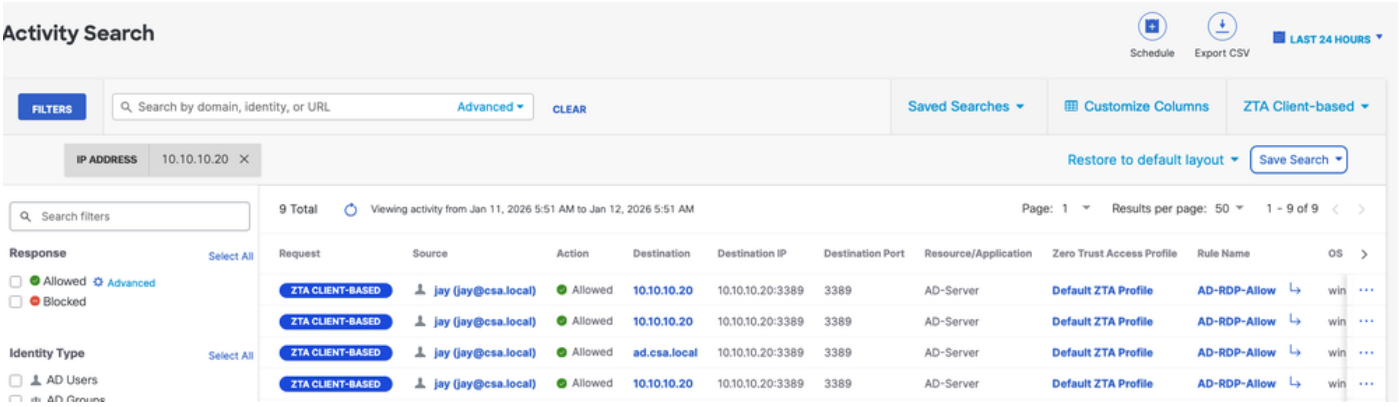
2. Verifiëren met de gebeurtenissen voor het zoeken naar activiteiten



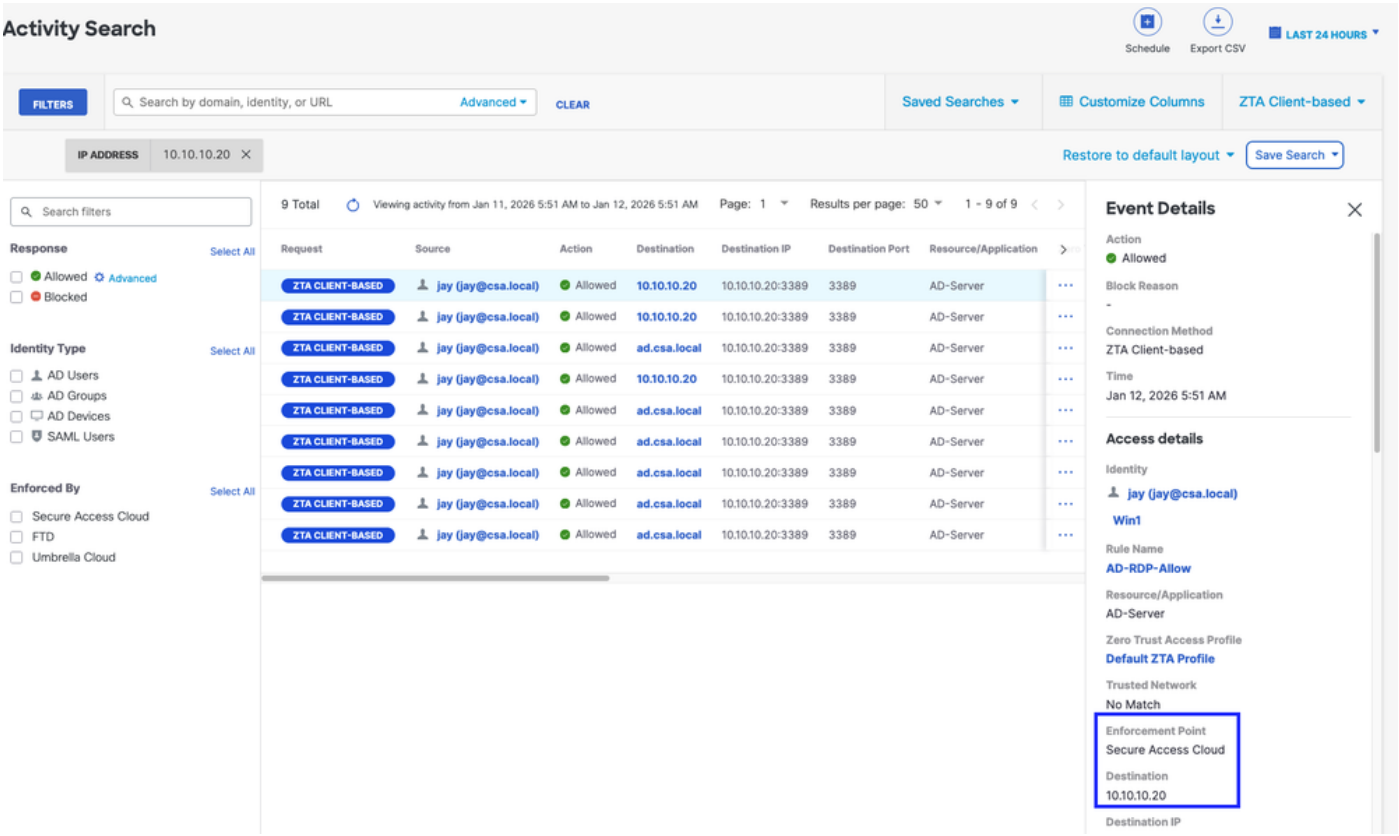
Veilige toegang - zoeken naar activiteiten



Veilige toegang - zoeken naar activiteiten

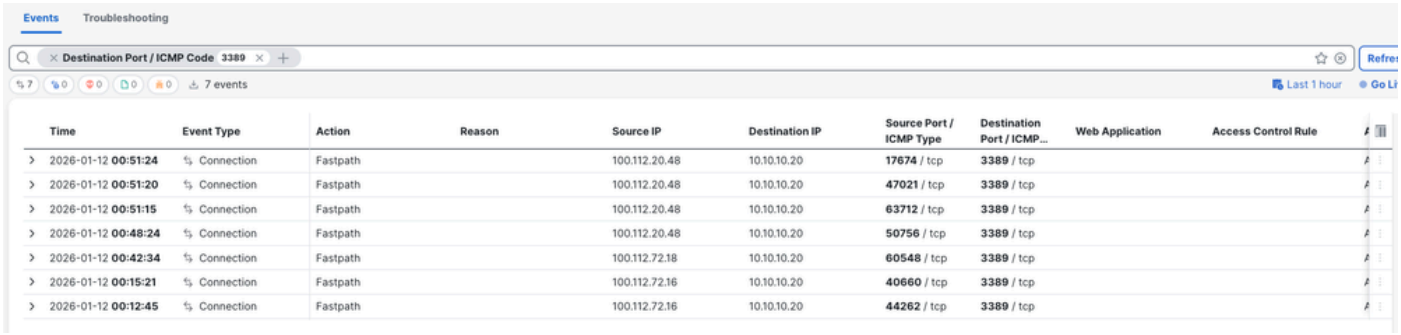


Veilige toegang - zoeken naar activiteiten



Veilige toegang - zoeken naar activiteiten

3. FMC-verbindingsgebeurtenissen controleren

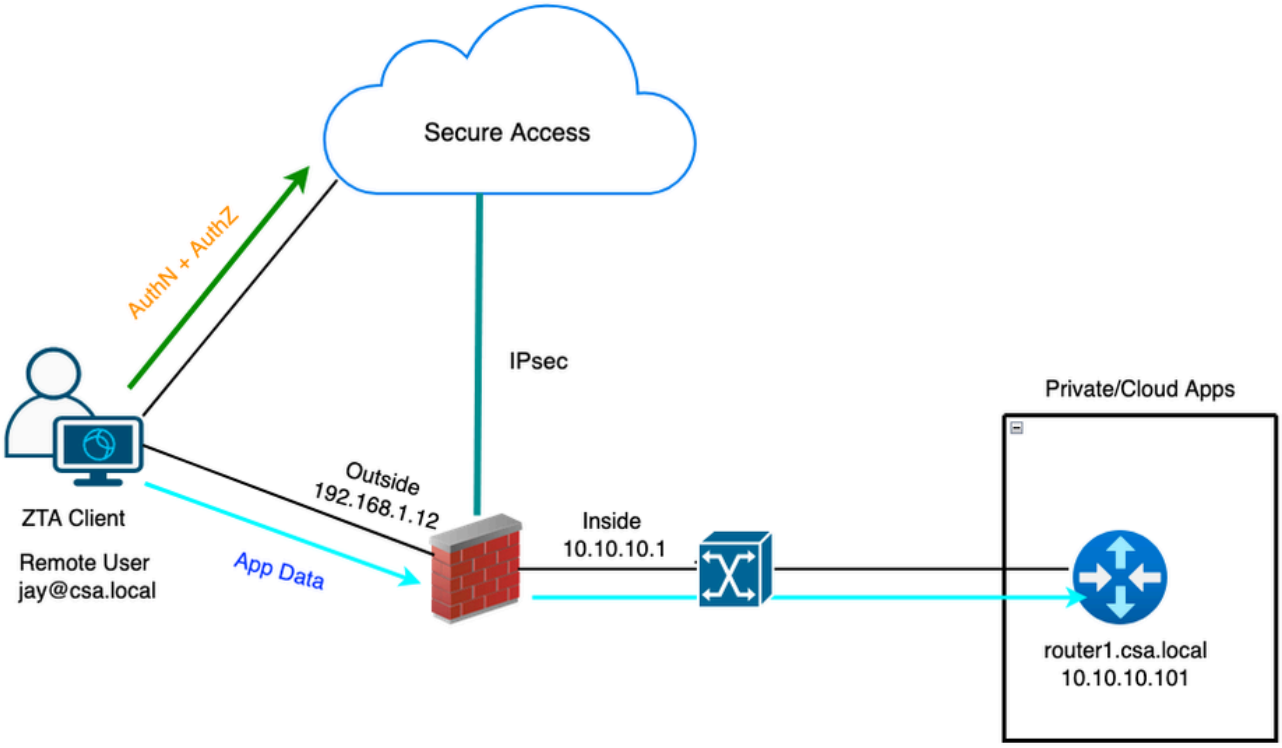


FMC-verbindingsgebeurtenissen

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.

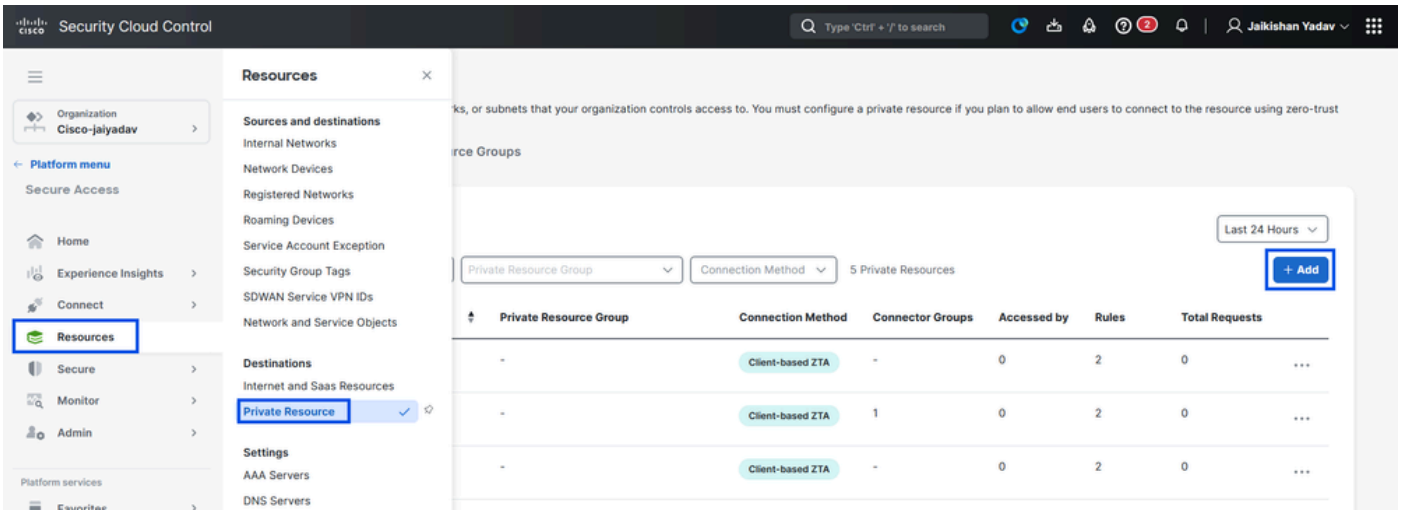


Universele ZTA - Test case topologie

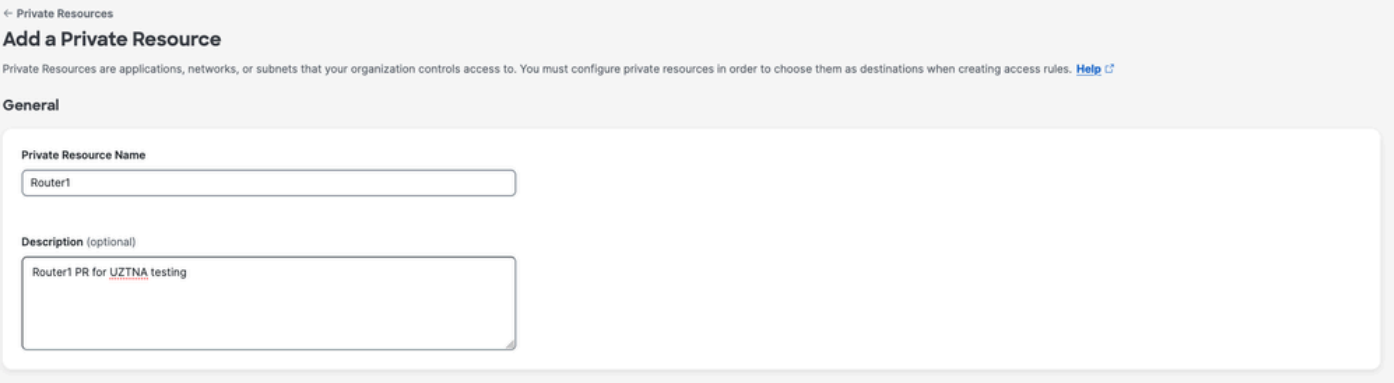
Stap 1 - Een privébron definiëren voor beveiligde toegang

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

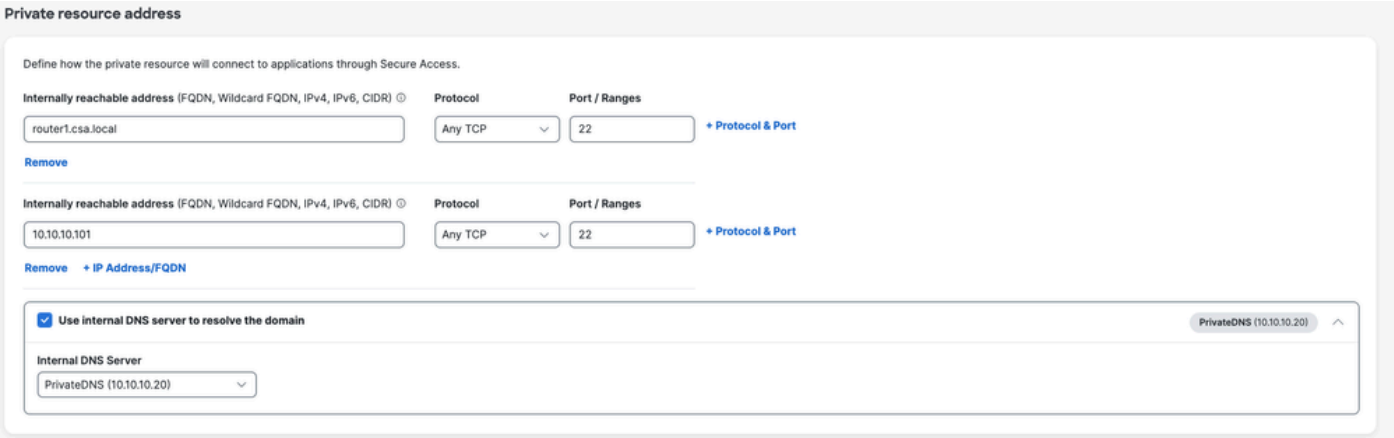


2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.



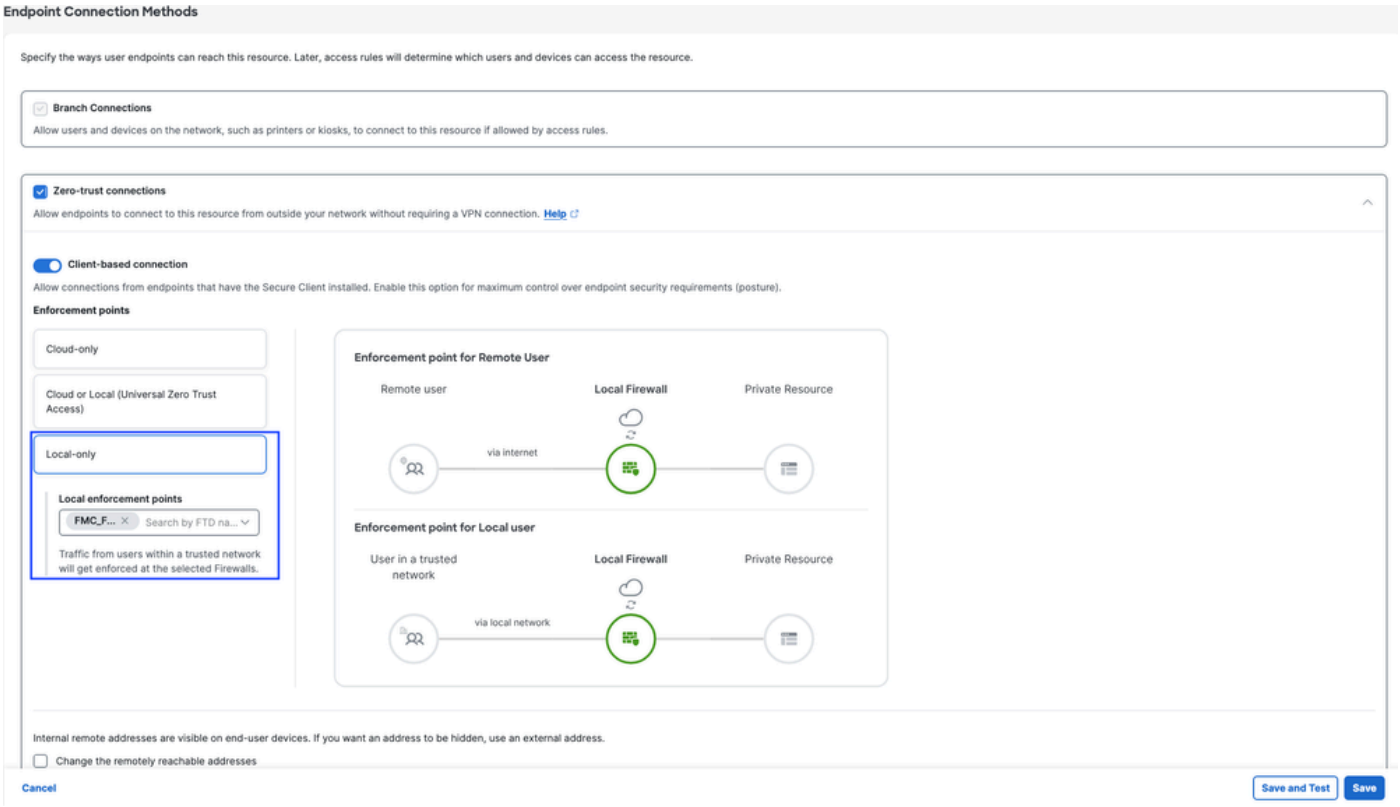
3. Voer het FQDN in van de privébron die u wilt openen. We kunnen ook het IP-adres van de privébron definiëren. Zie Een privébron toevoegen voor meer informatie

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



5. Selecteer methoden voor eindpuntverbinding

6. Selecteer FTD als lokale handhavingspunten



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

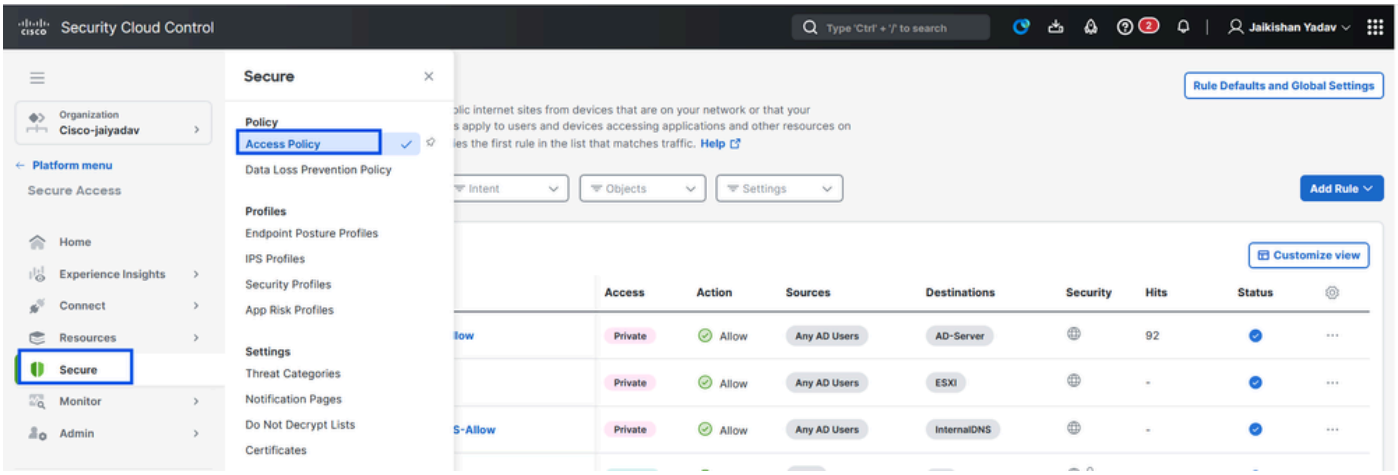
---

7. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

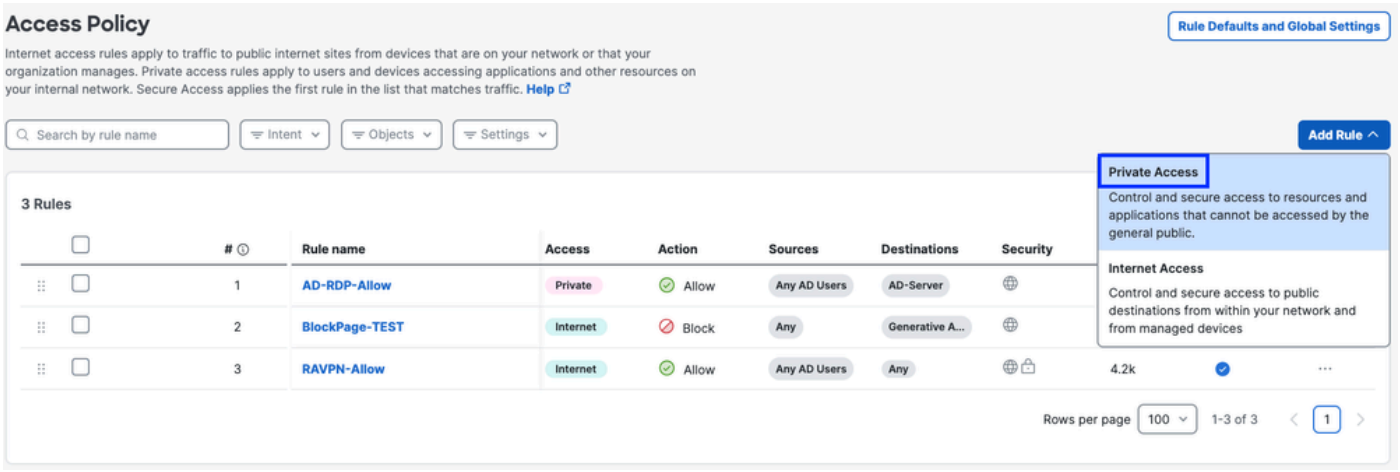
Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie Private Access Rule

1. Navigeer naar Beveiligd > Toegangsbeleid



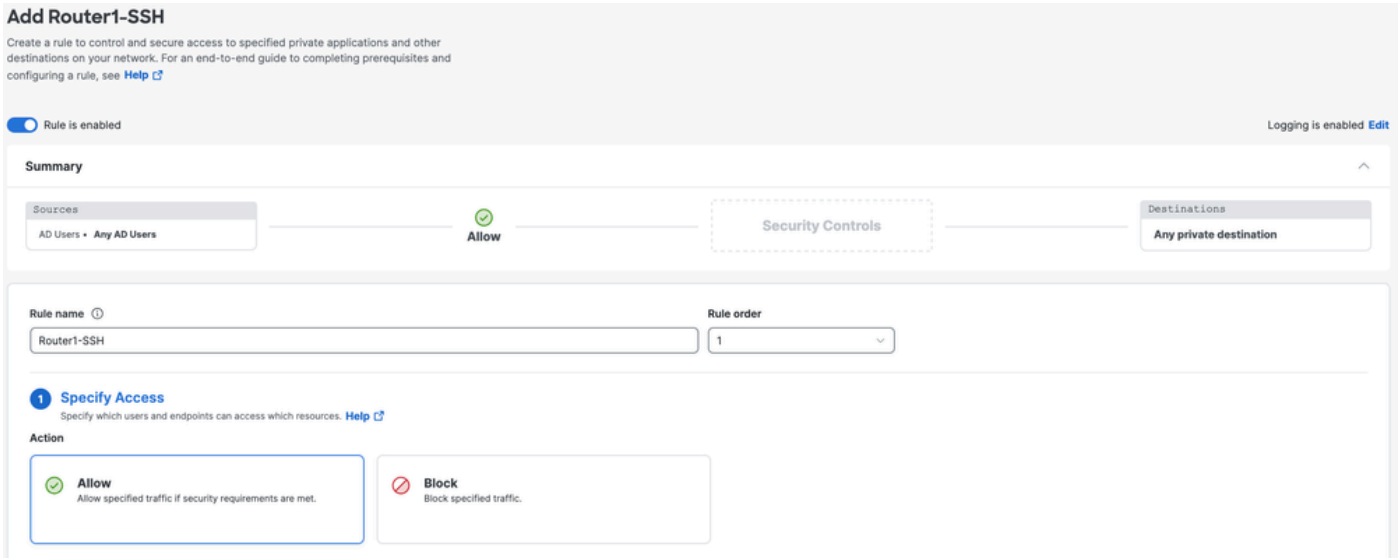
Veilige toegang - Configuratie van privébronnen

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.
Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.



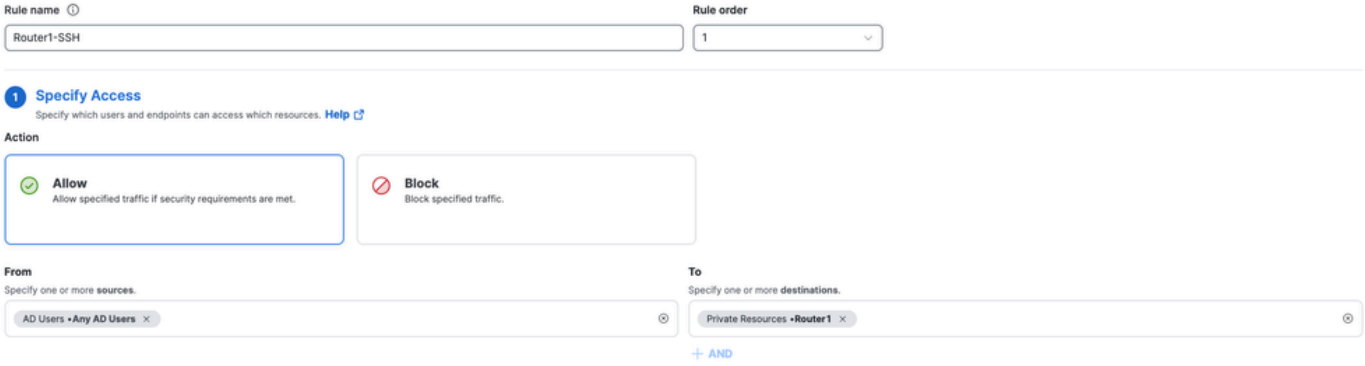
Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen



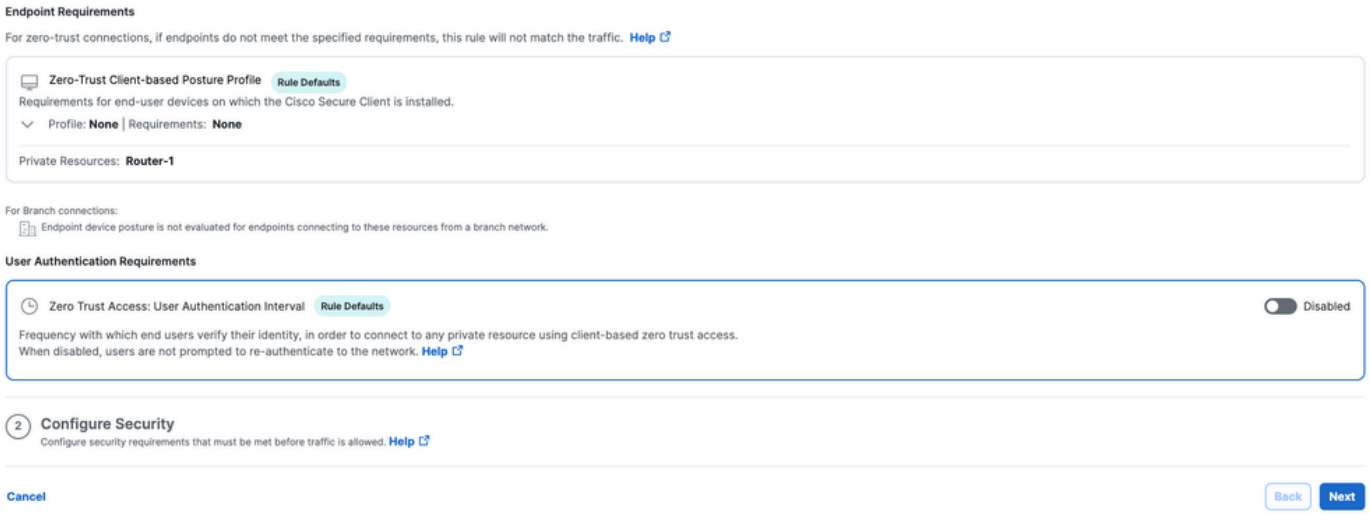
Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming



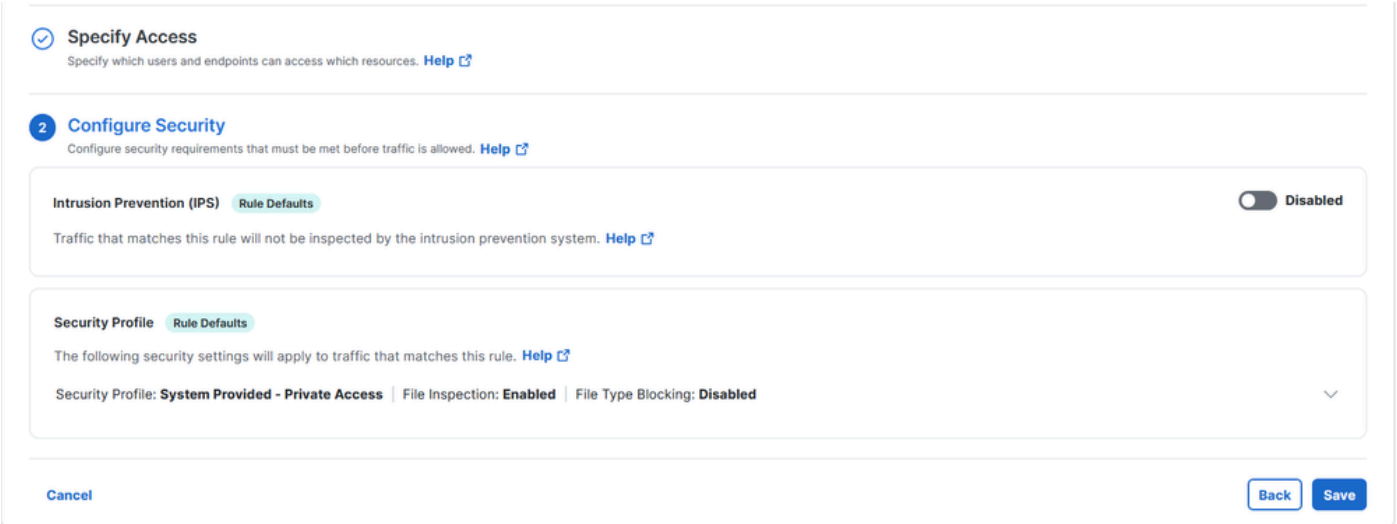
Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren



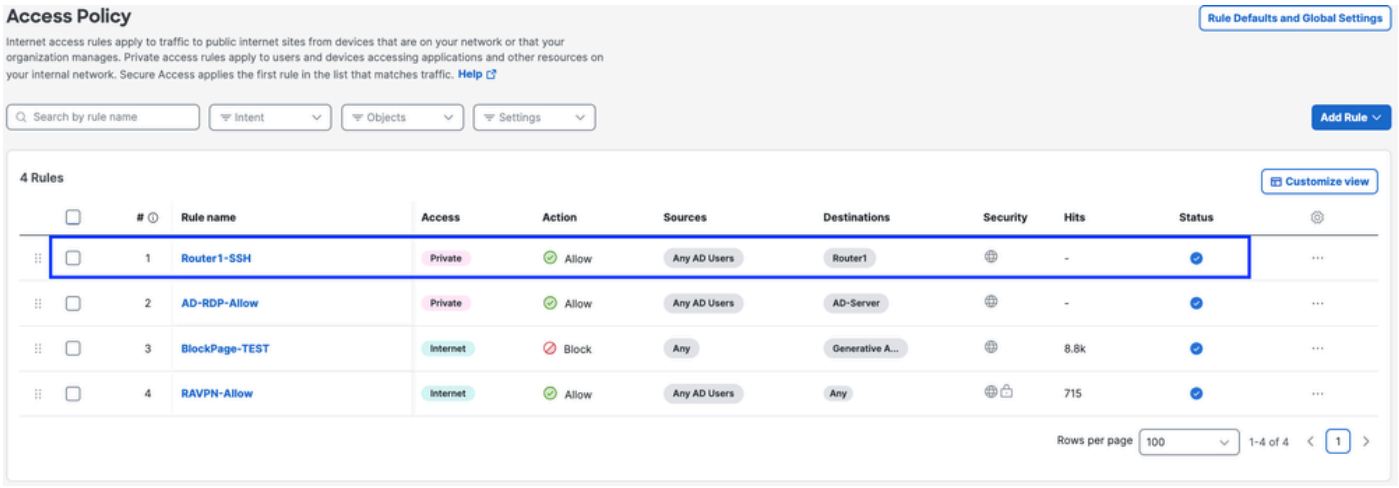
Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren



Beveiligde toegang - Configuratie toegangsbeleid

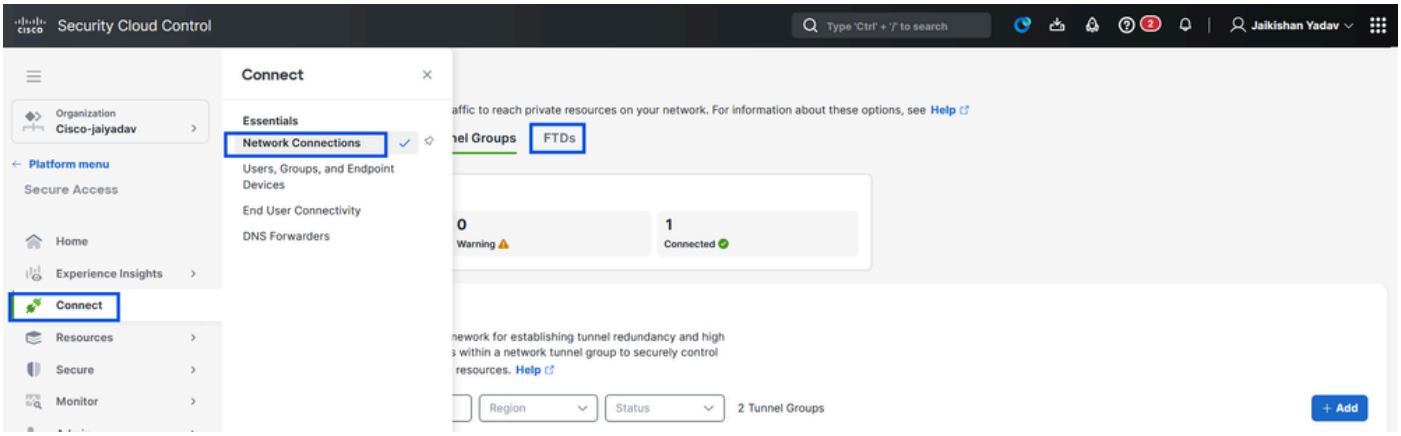
7. Klik op Opslaan



Beveiligde toegang - Configuratie toegangsbeleid

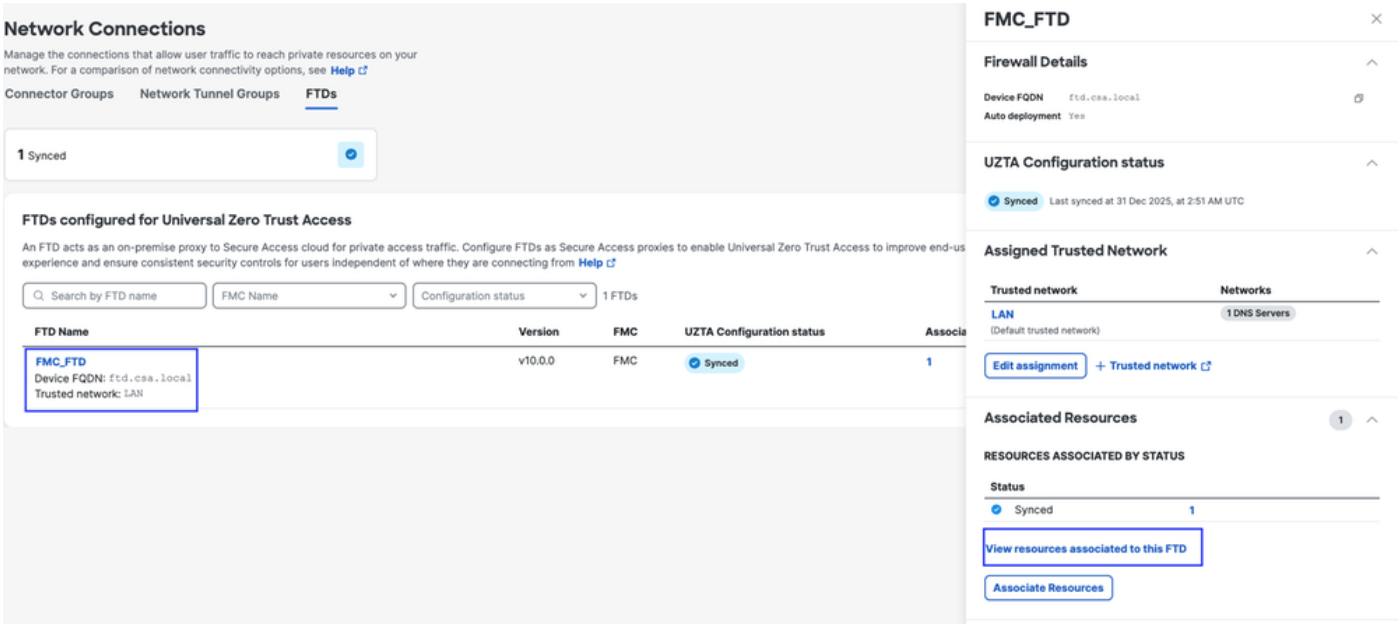
Stap 3 - Controleer de associatie van PR op de FTD

1. Navigeer naar Verbinden > Netwerkverbindingen > FTD's

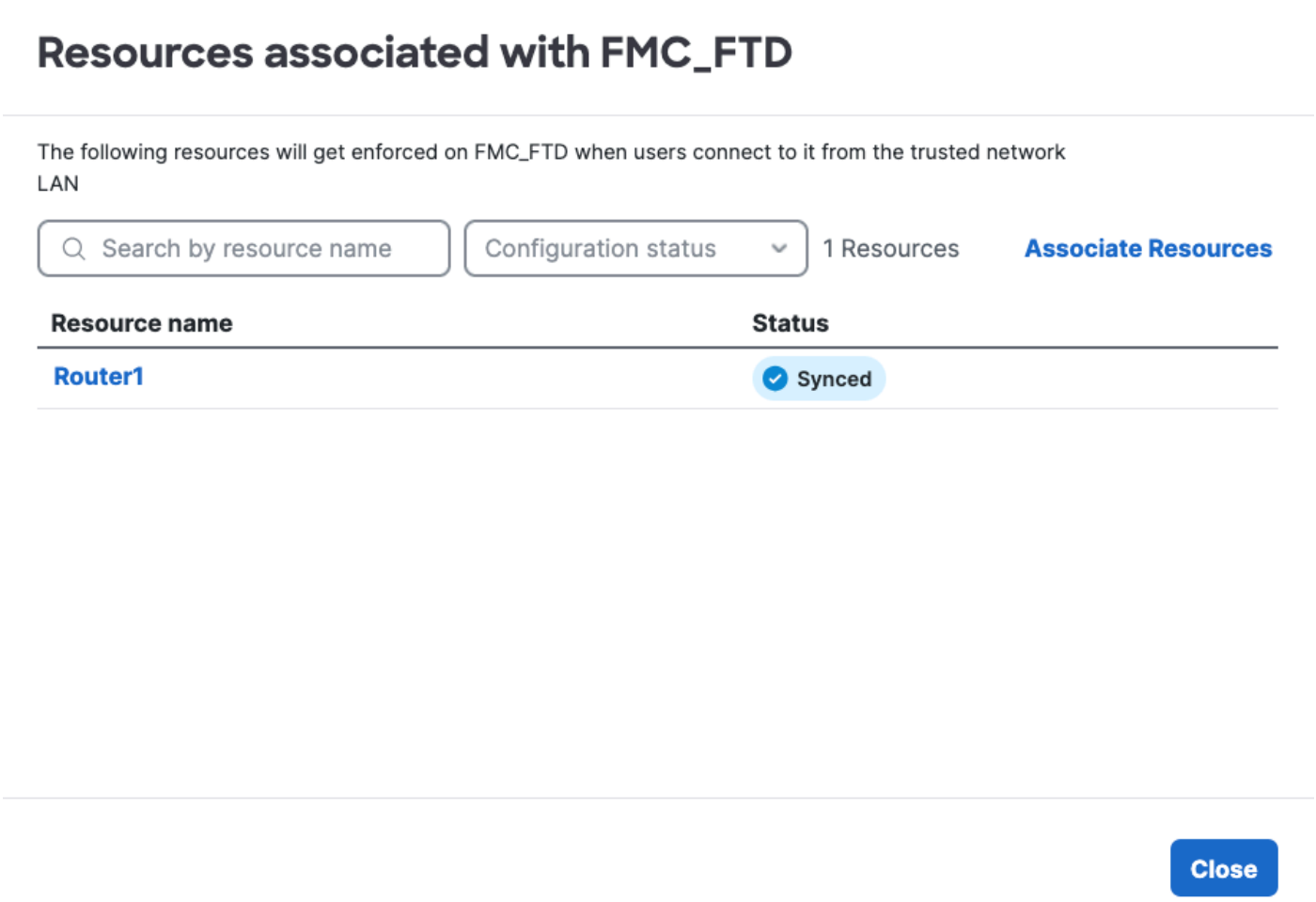


Veilige toegang - PR-verificatie

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



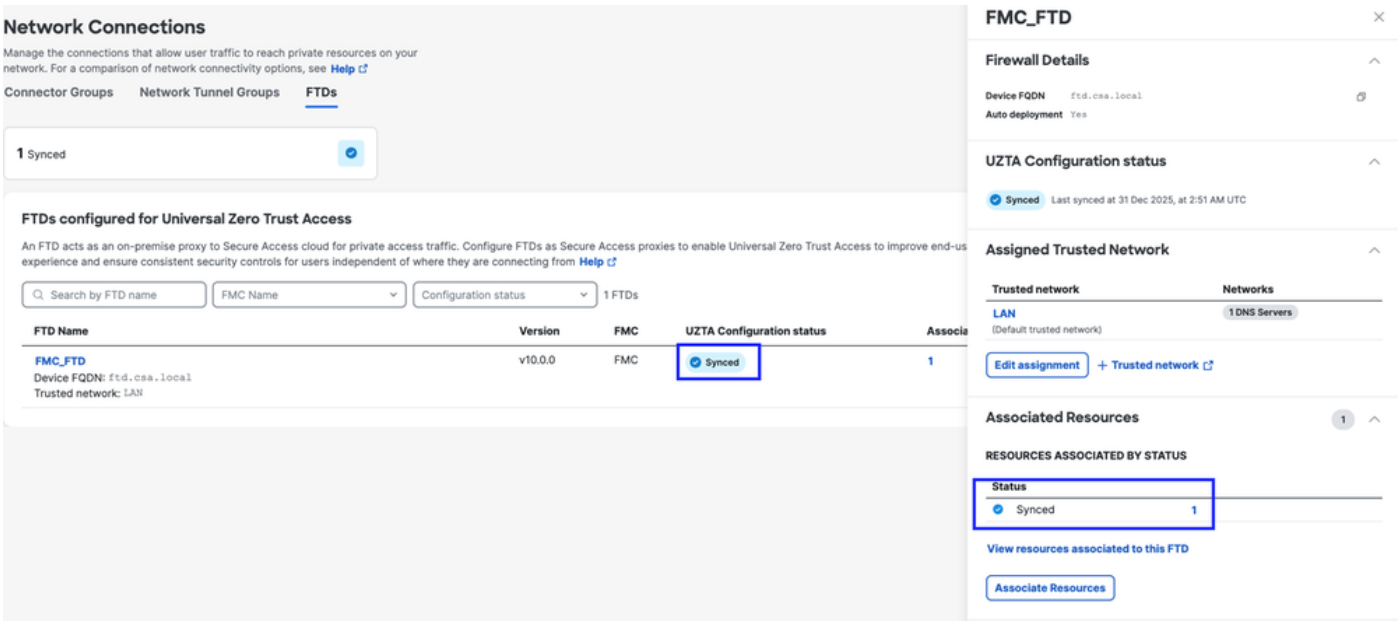
Veilige toegang - PR-verificatie



Veilige toegang - PR-verificatie

3. Klik op sluiten

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



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

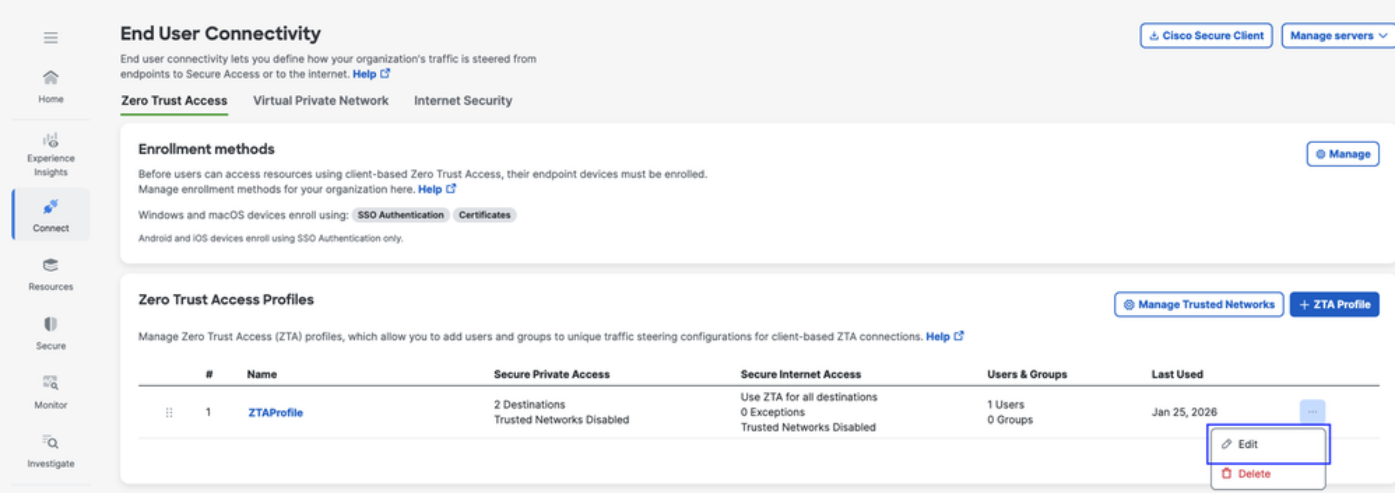
Toon de toepassing Running-Config Object

```
> 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

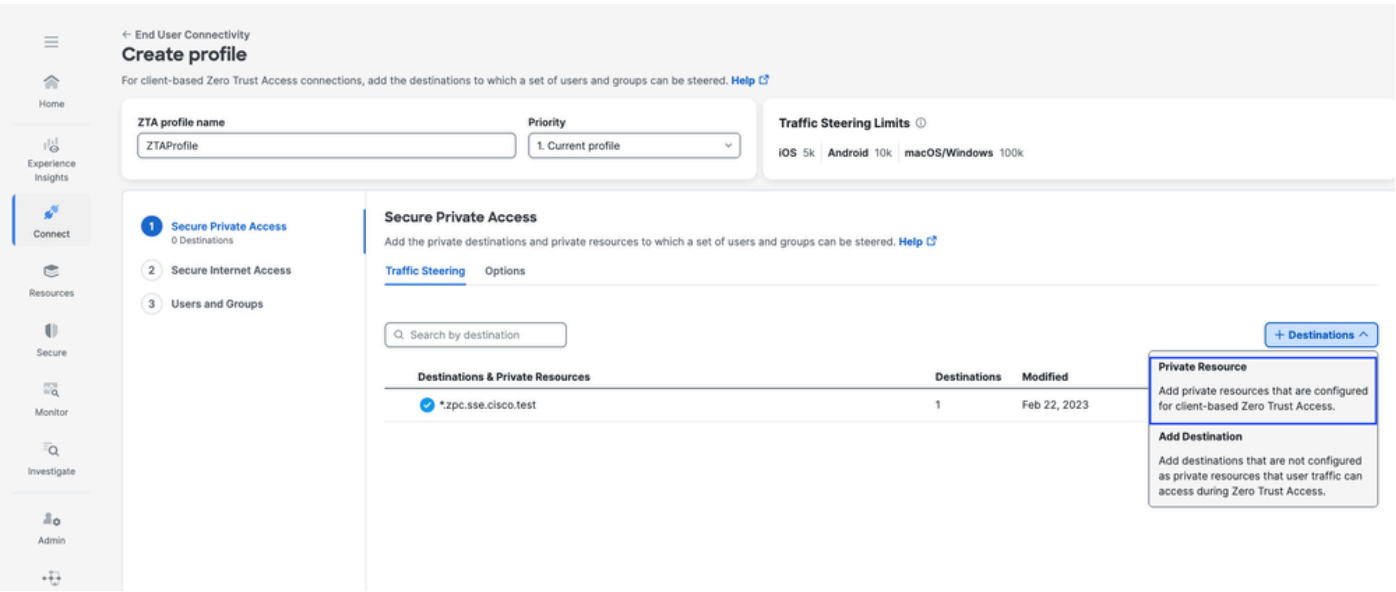
Stap 4 Voeg privé-bronnen toe aan het ZTA-profiel

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

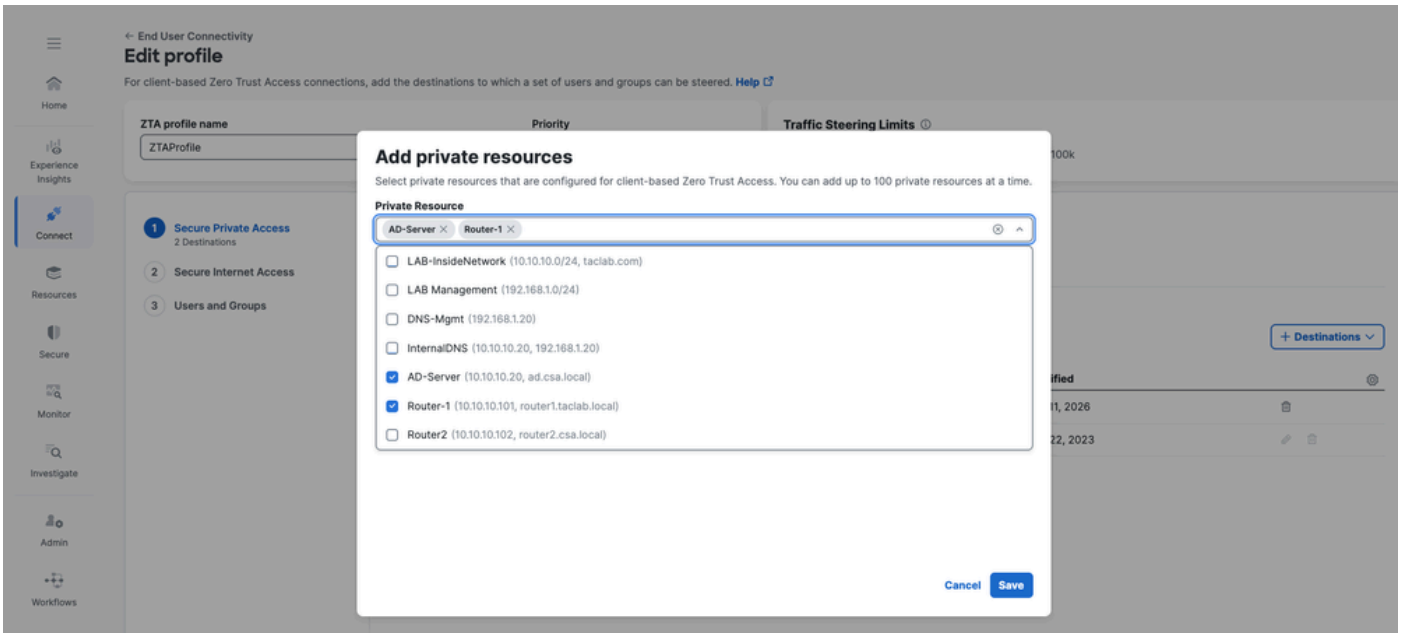


Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

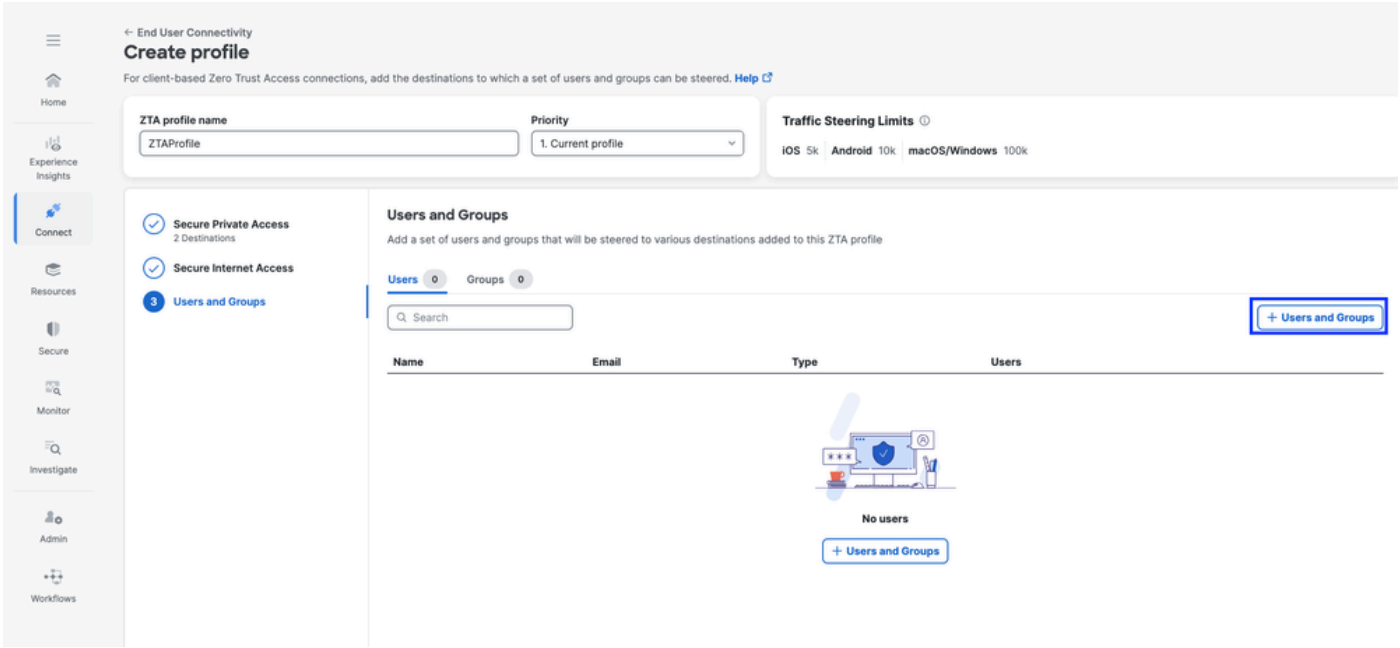


Veilige toegang - ZTA-profiel

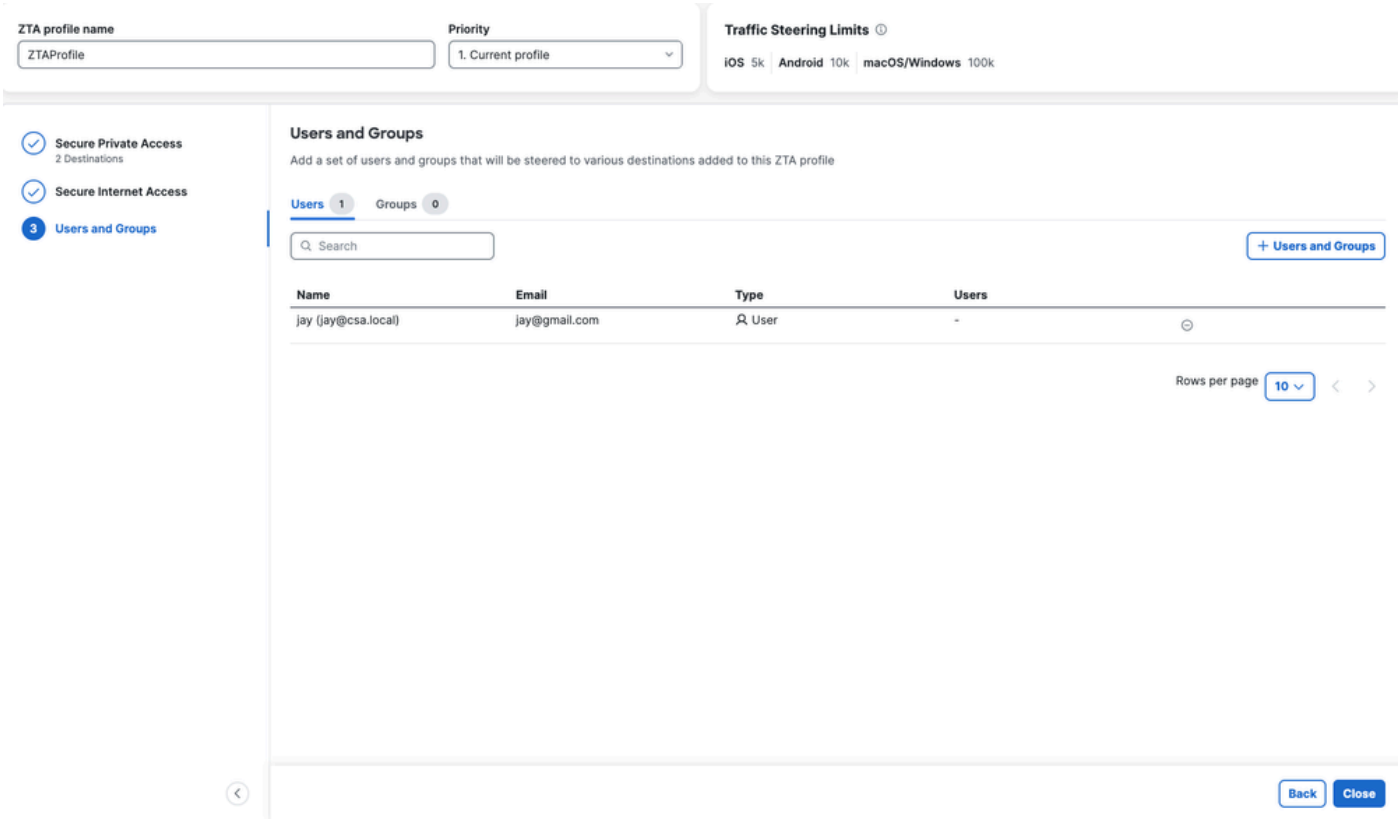


Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen



Veilige toegang - ZTA-profiel



Veilige toegang - ZTA-profiel

Stap 5: Controleer de toegang tot de privébron

1. Controleer of de externe gebruiker FTD FQDN kan oplossen

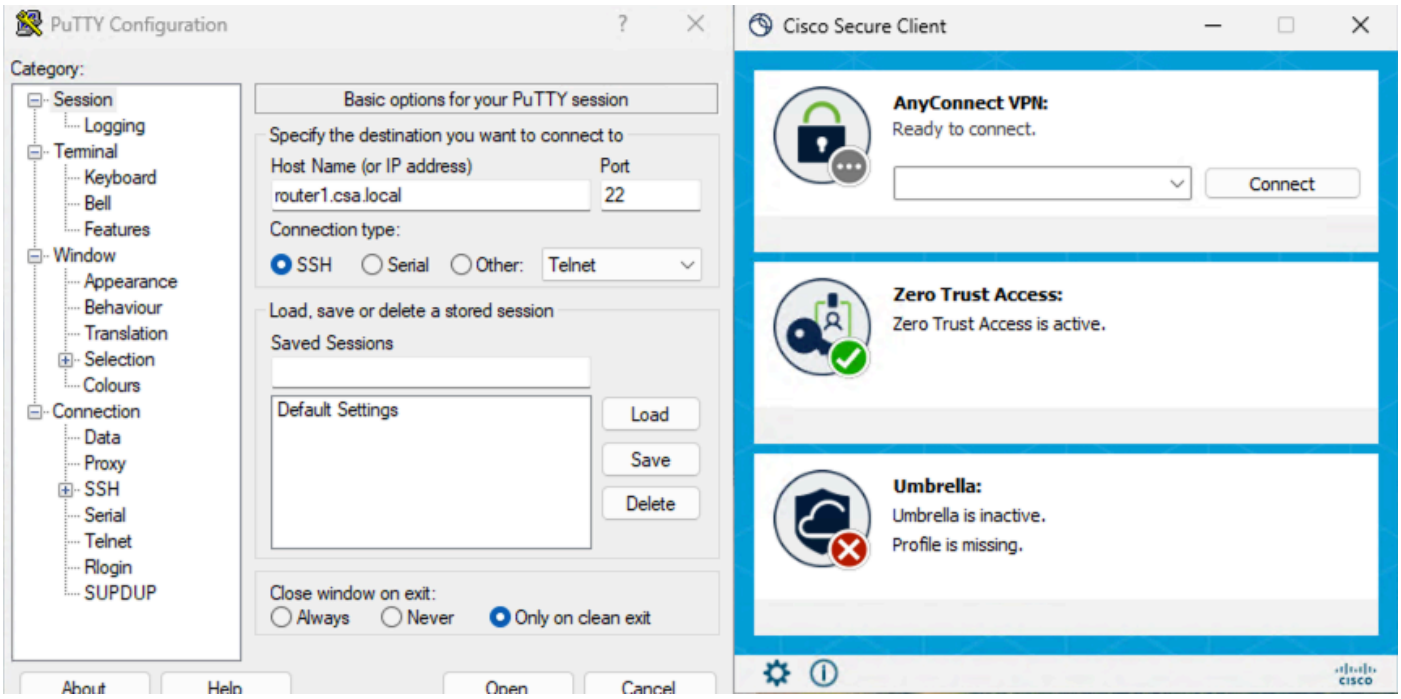
```
PS C:\Users\jay> ping ftd.csa.local

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
```

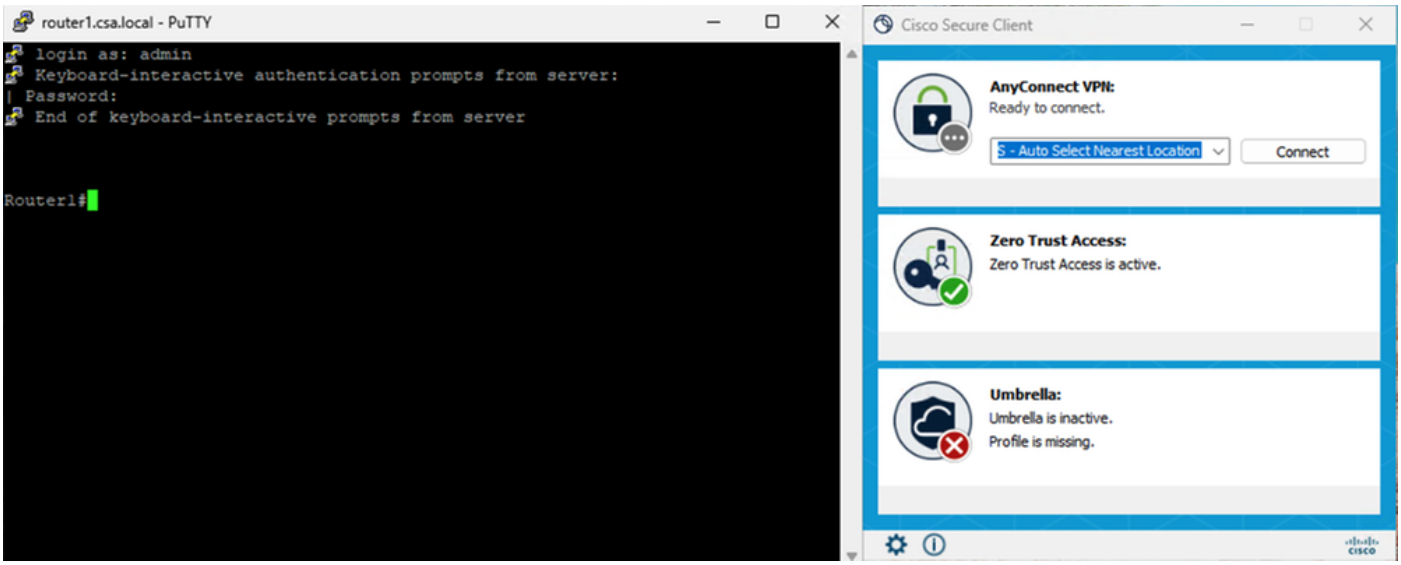
2. Controleren of FTD particuliere bronnen kan bereiken met behulp van FQDN

```
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#
```

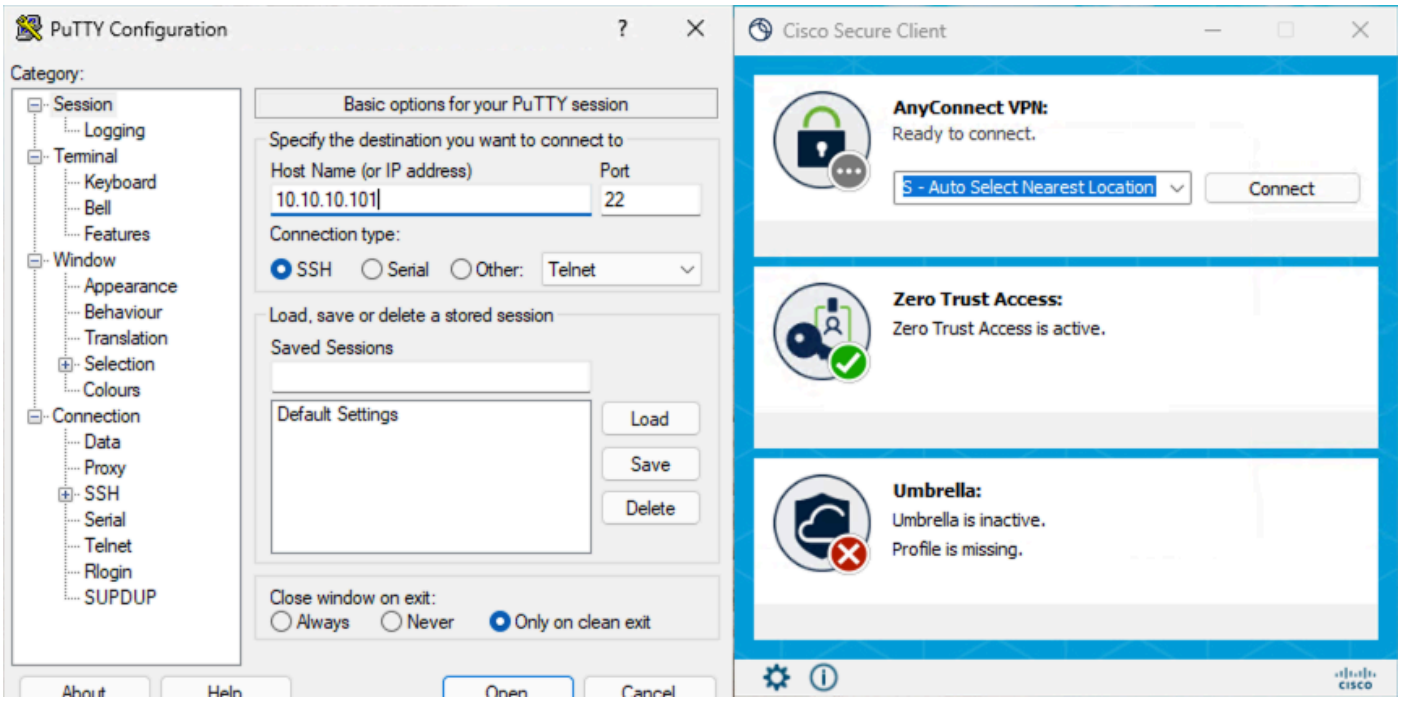

3. Test de SSH-verbinding met de Private Resource

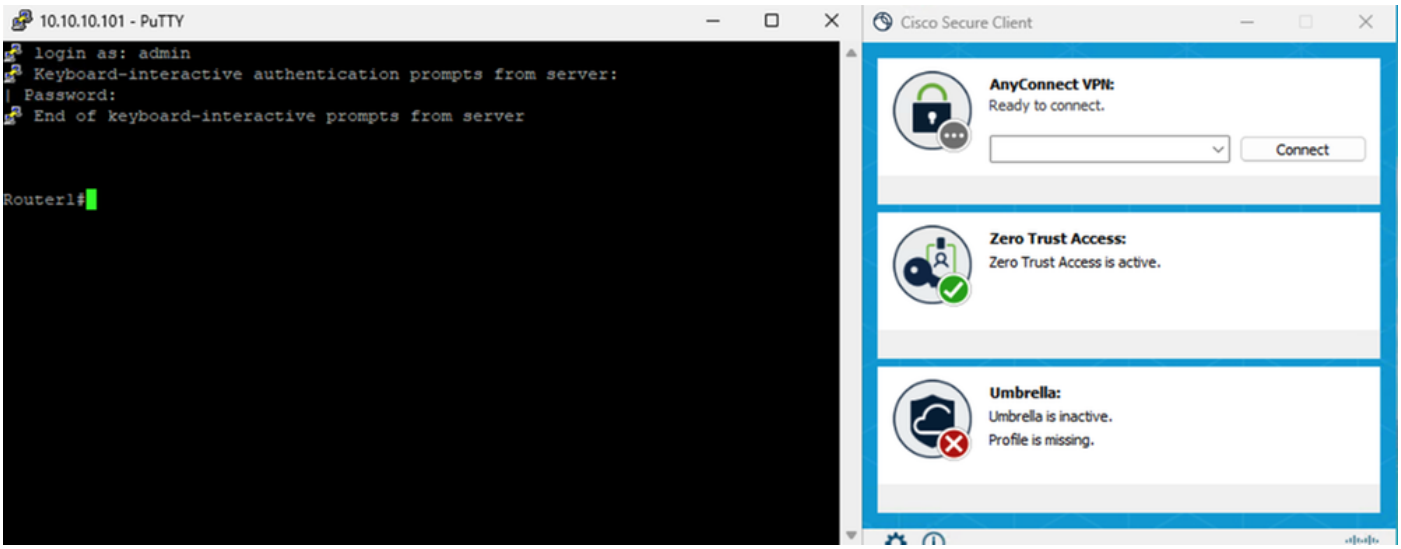
Toegang tot de PR via FQDN





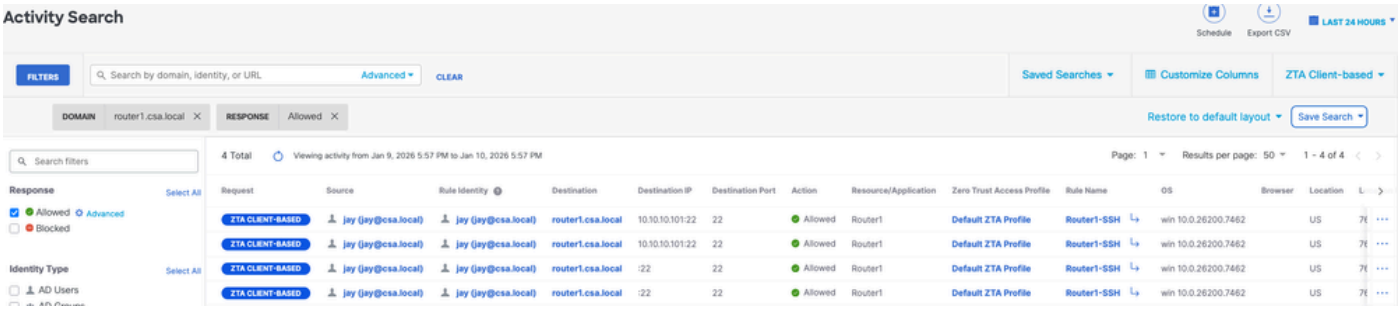
Toegang tot de PR via IP-adres



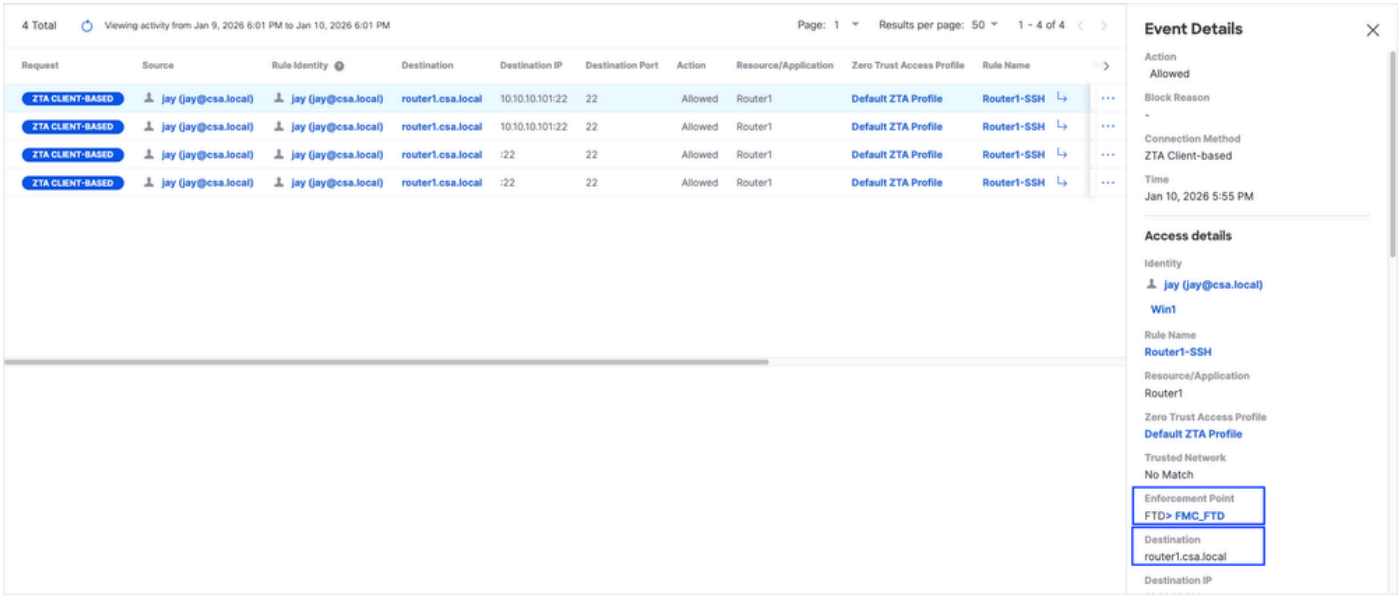


Veilige toegang - PR-testen

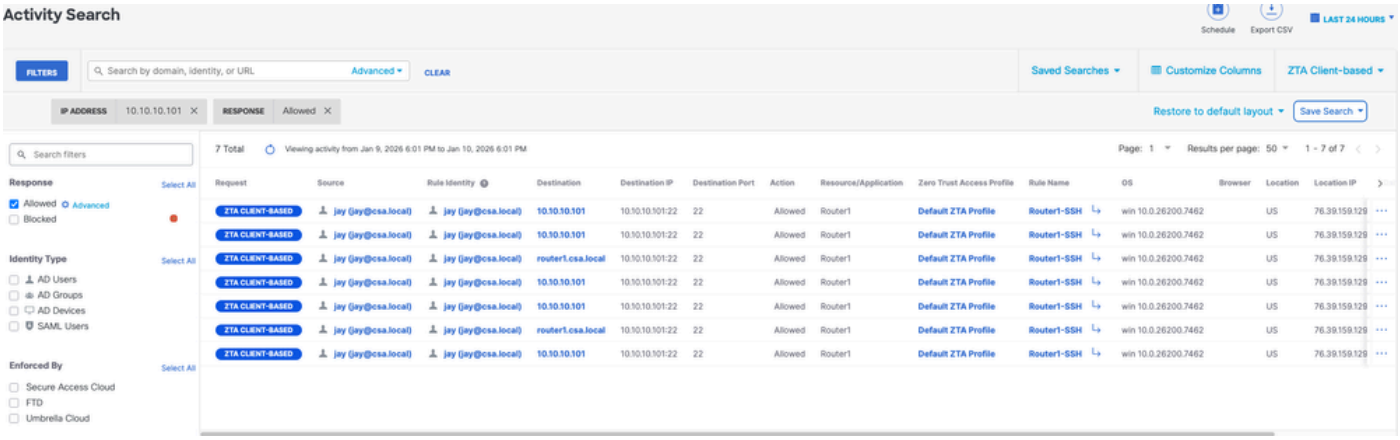
4. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten



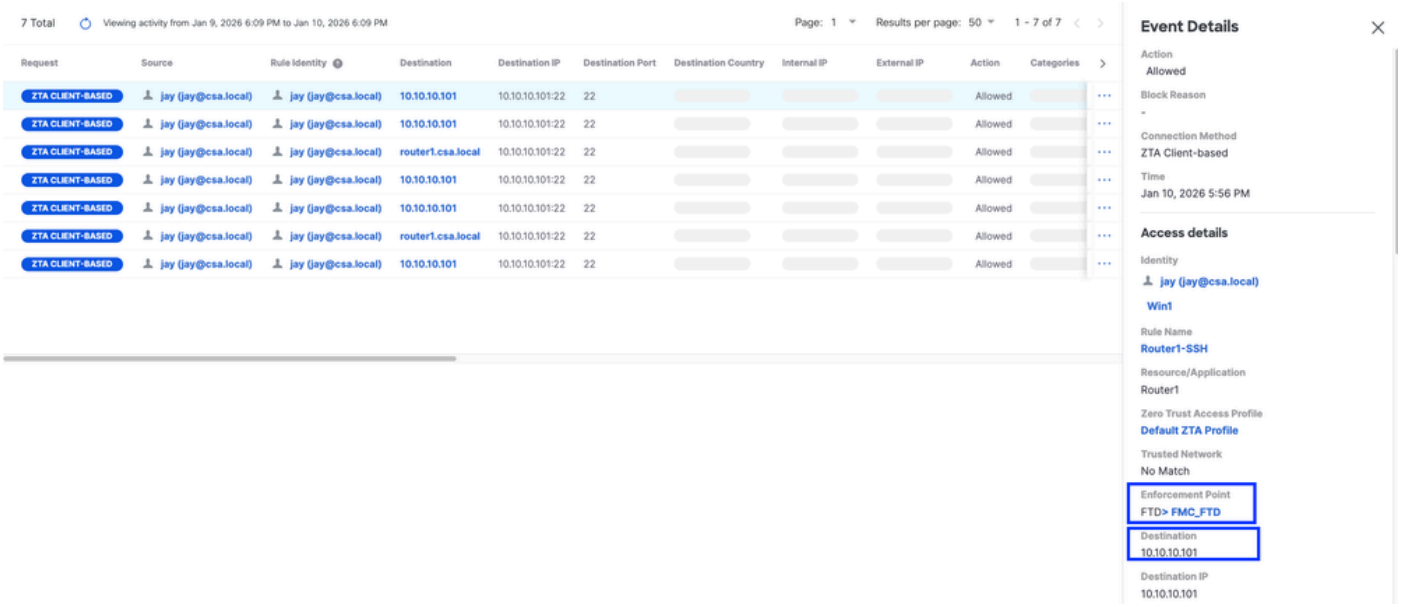
Veilige toegang - zoeken naar activiteiten



Veilige toegang - zoeken naar activiteiten

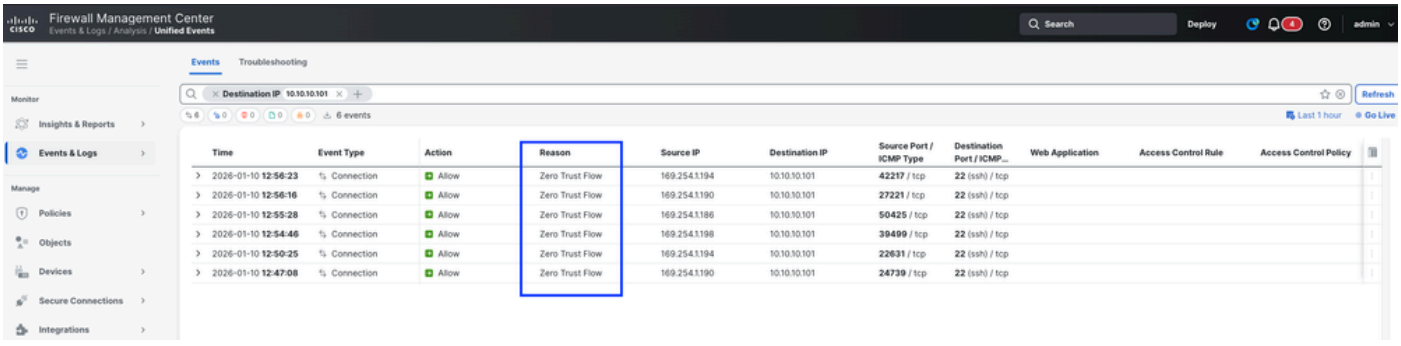


Veilige toegang - zoeken naar activiteiten



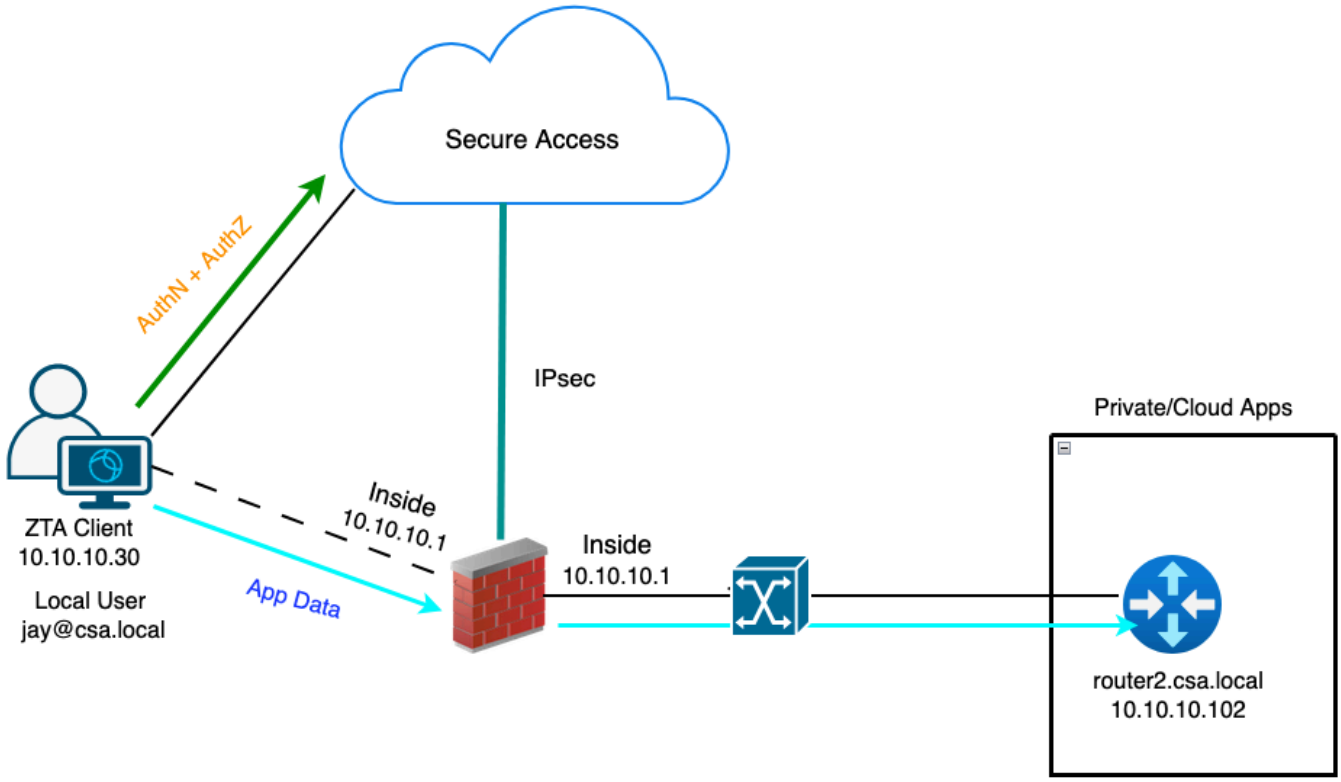
Veilige toegang - zoeken naar activiteiten

5. FMC-verbindingsgebeurtenissen controleren



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.

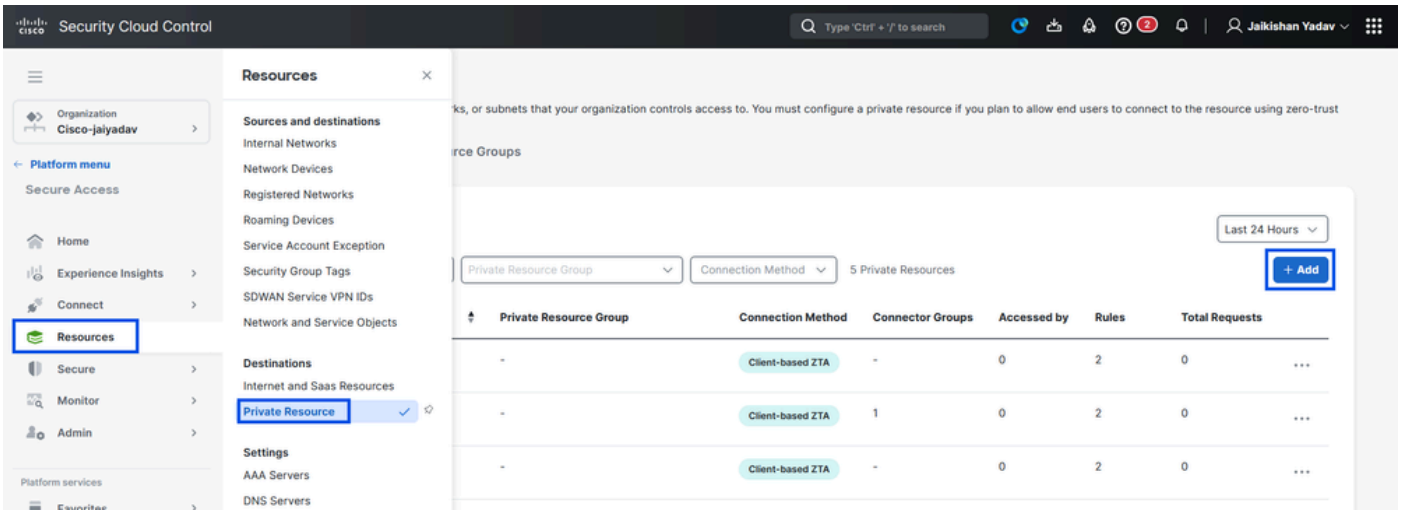


Universal ZTA - Test Case Topology

Stap 1 - Een privébron definiëren voor beveiligde toegang

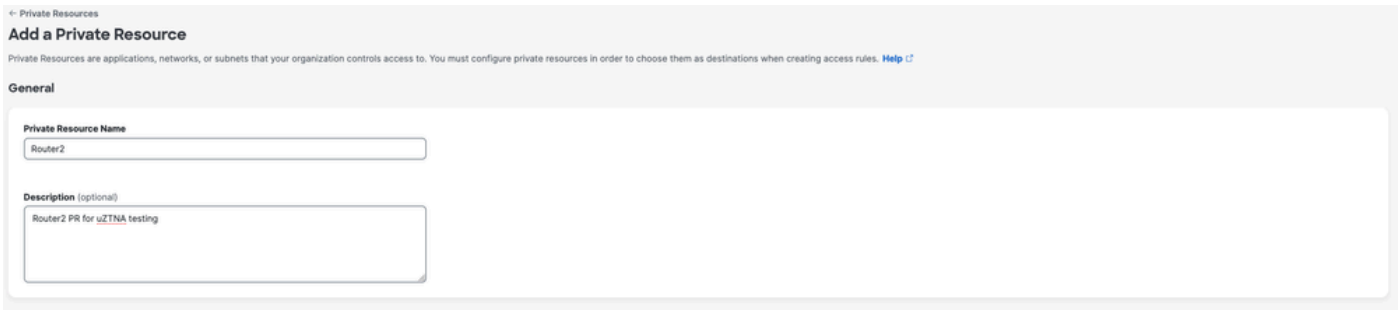
Configureer een privébron die toegankelijk is via een apparaat waarvoor Zero Trust Access (ZTA) is ingeschreven met cloudhandhaving

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



Veilige toegang - Configuratie van privébronnen

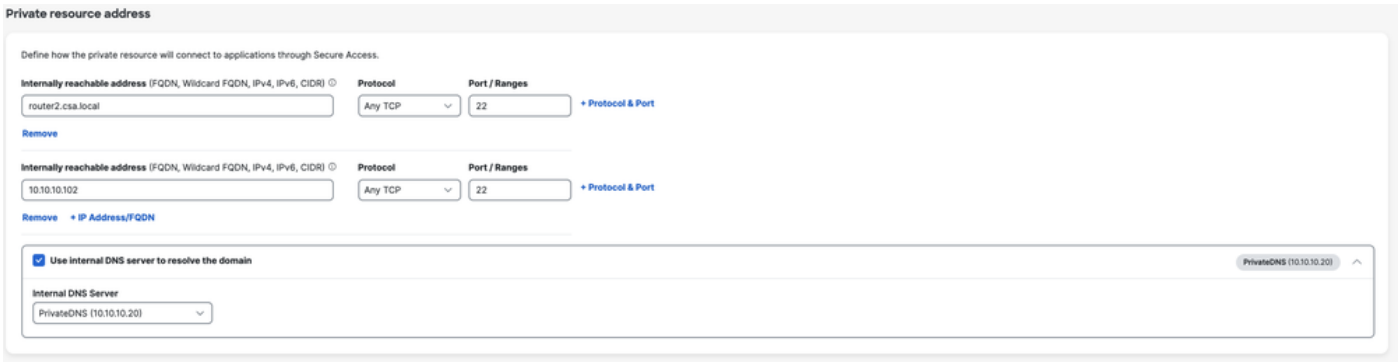
2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.



Veilige toegang - Configuratie van privébronnen

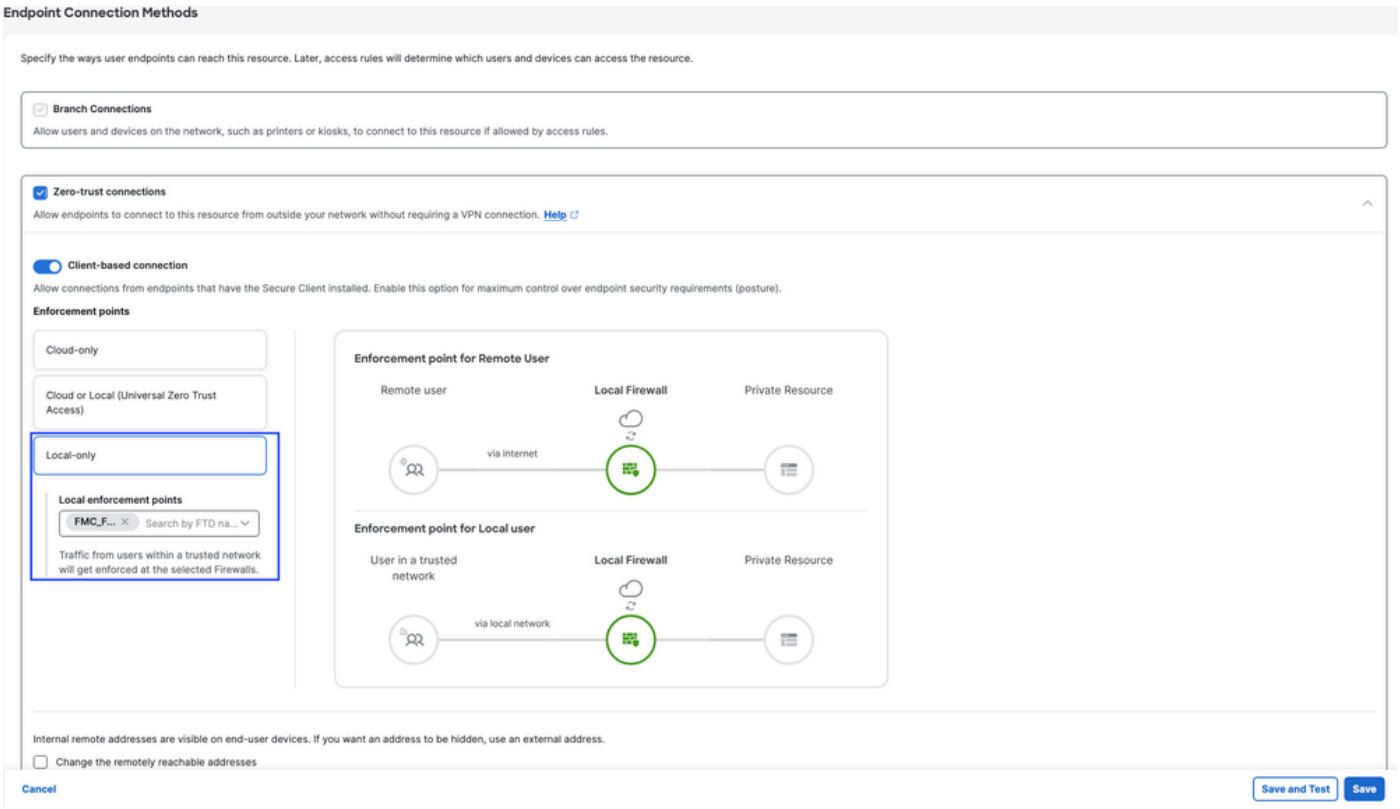
3. Voer het FQDN in van de privébron die u wilt openen. We kunnen ook het IP-adres van de privébron definiëren. Zie Een privébron toevoegen voor meer informatie

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



5. Selecteer methoden voor eindpuntverbinding

6. Selecteer FTD als lokale handhavingspunten



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

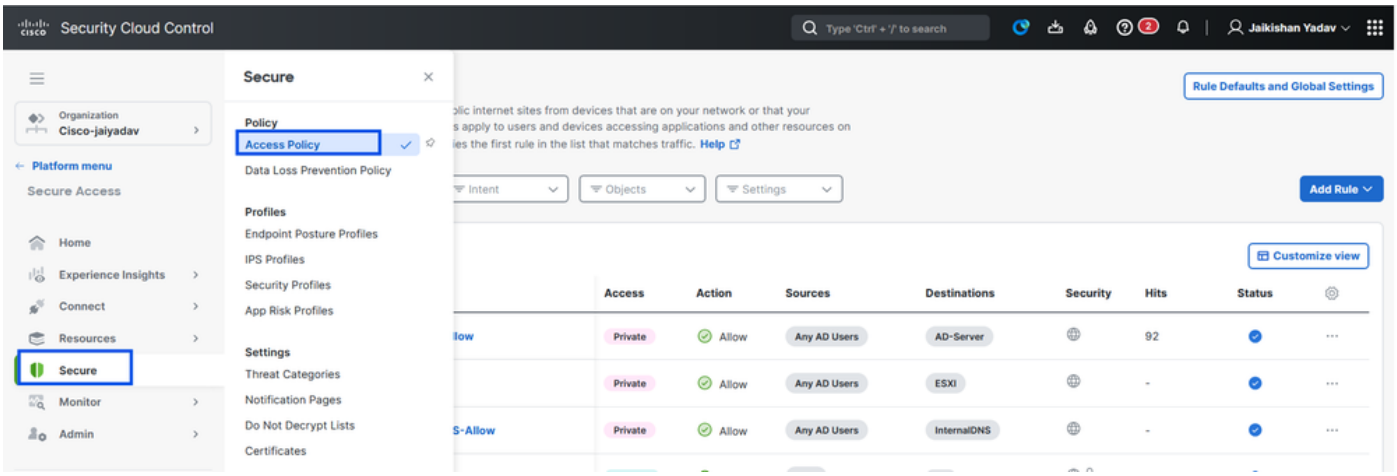
---

7. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

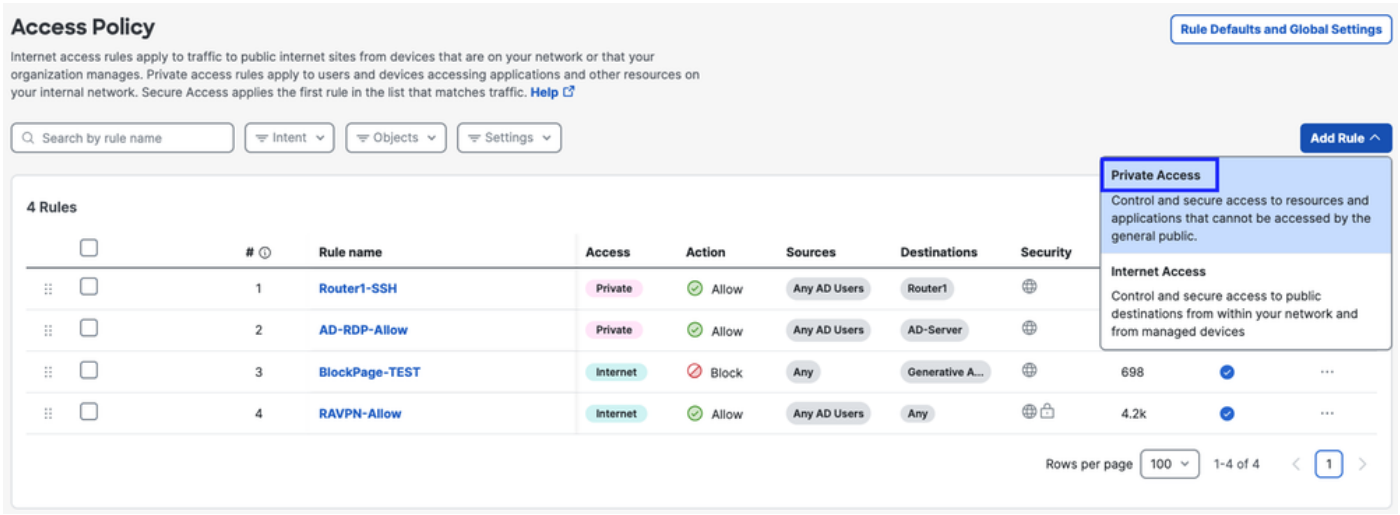
Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie Private Access Rule

1. Navigeer naar Beveiligd > Toegangsbeleid



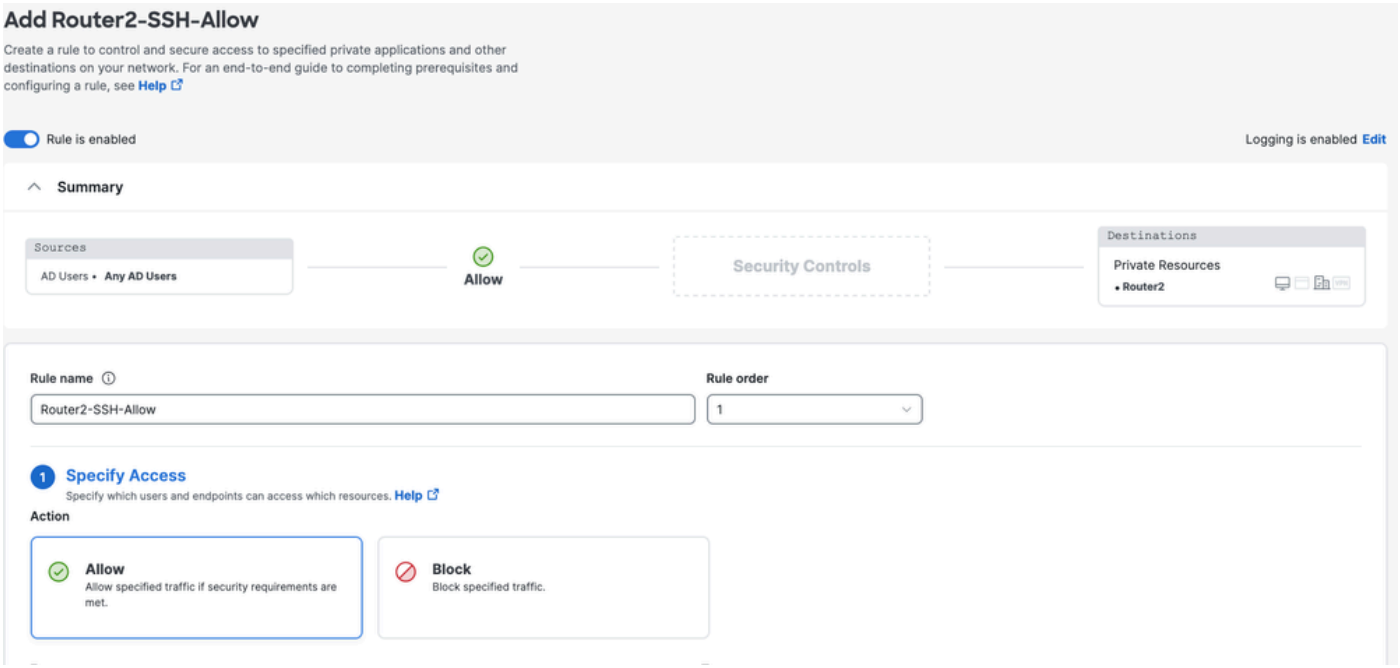
Beveiligde toegang - Configuratie toegangsbeleid

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.
Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.



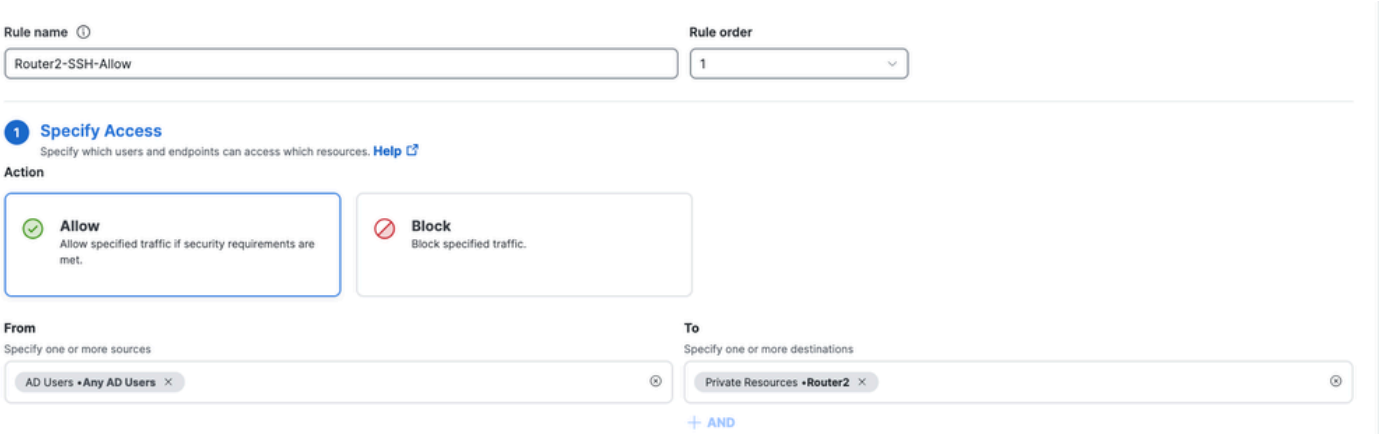
Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen



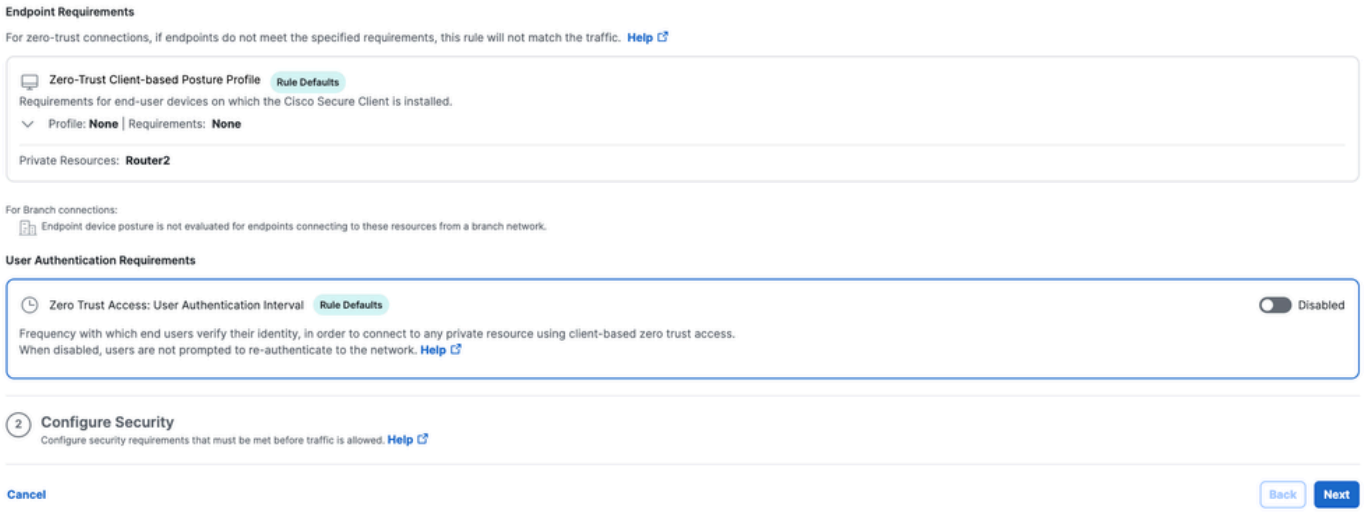
Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming



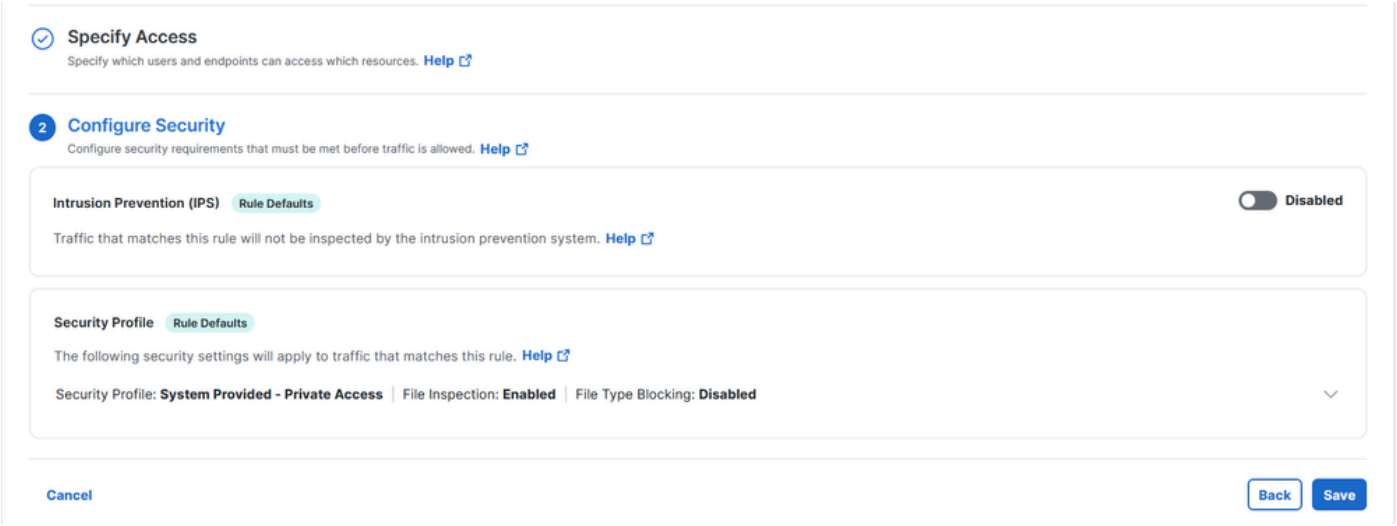
Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren



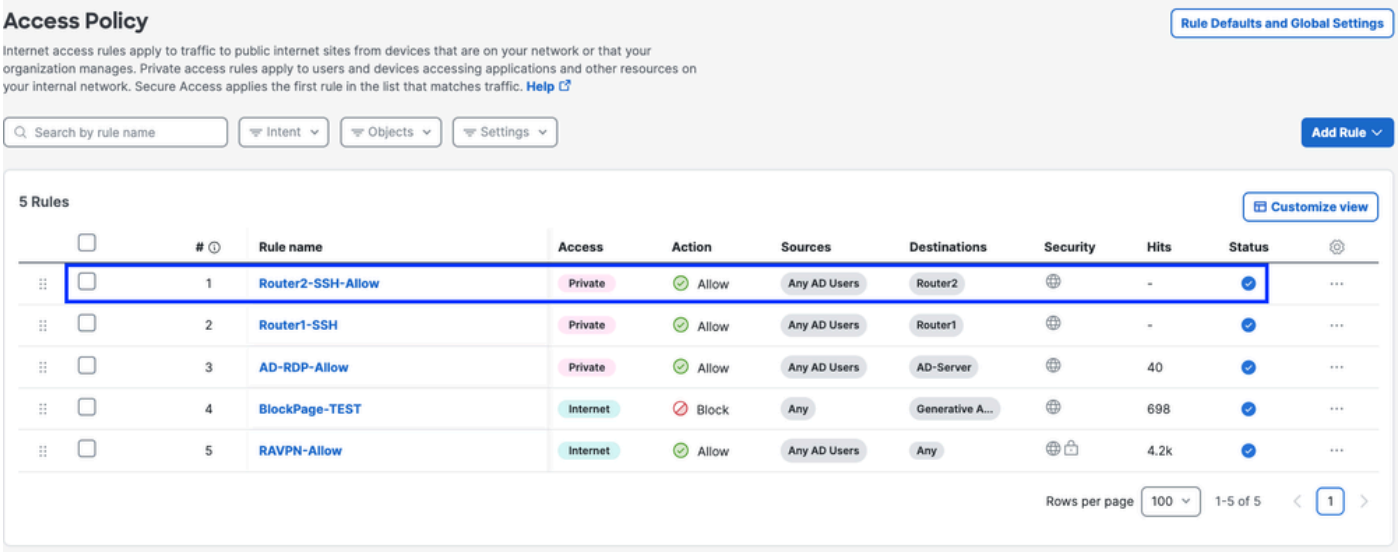
Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren



Beveiligde toegang - Configuratie toegangsbeleid

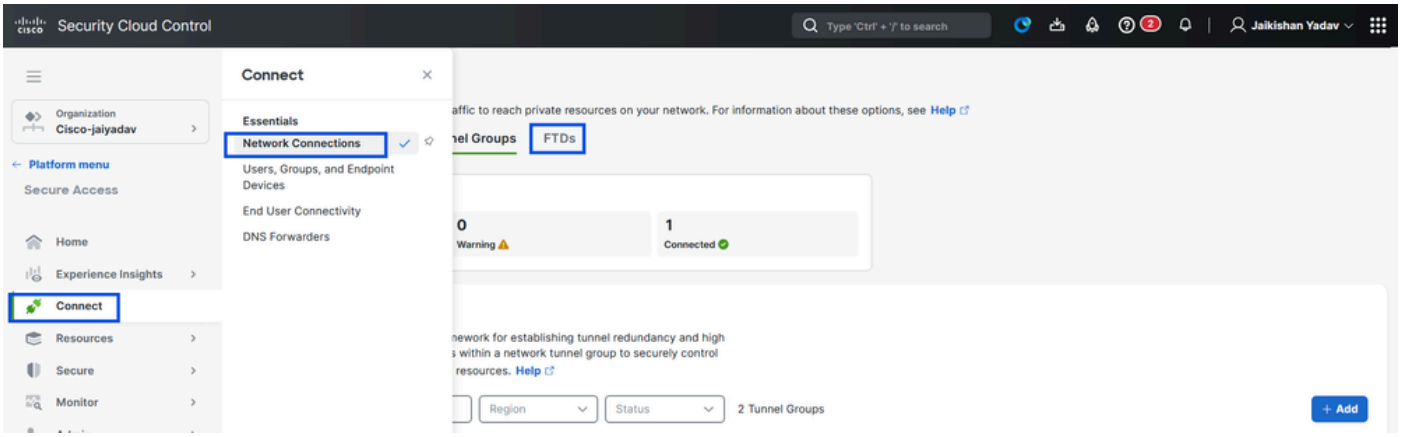
7. Klik op Opslaan



Beveiligde toegang - Configuratie toegangsbeleid

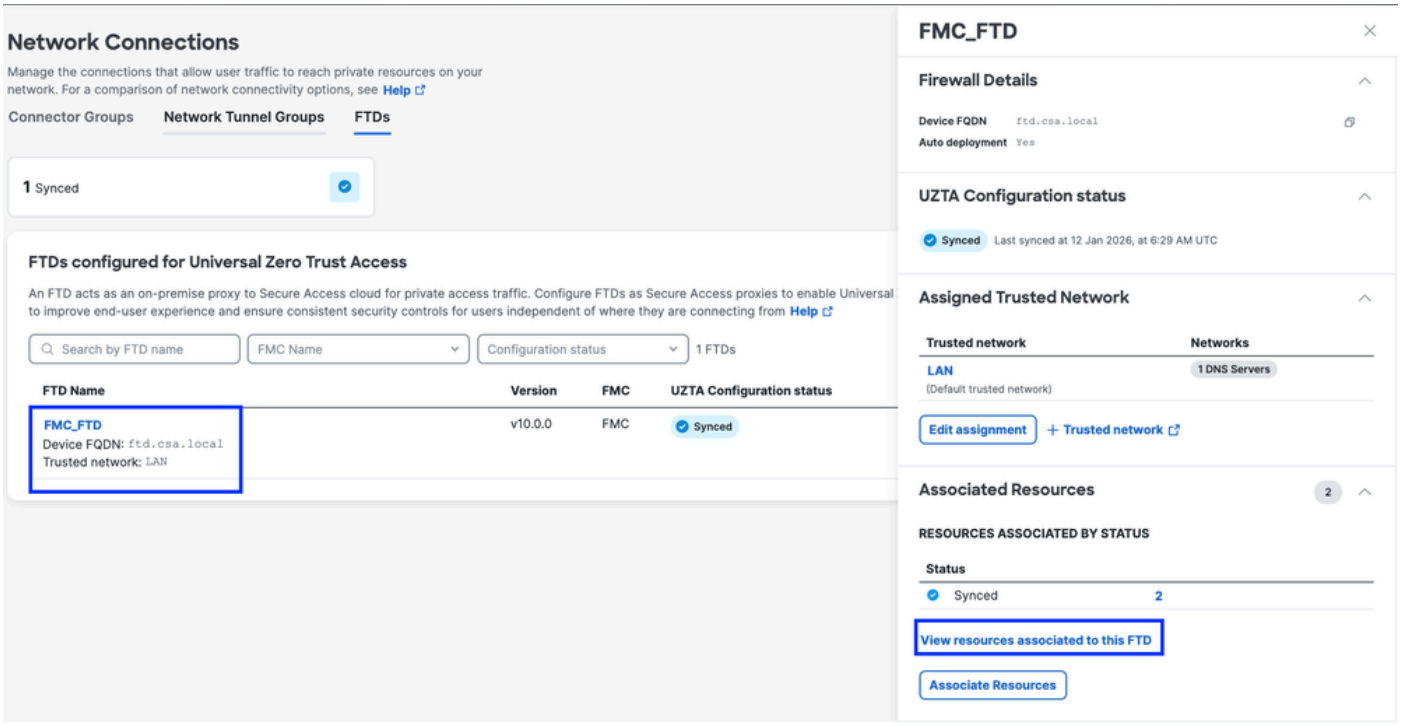
Stap 3 - Controleer de associatie van PR op de FTD

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

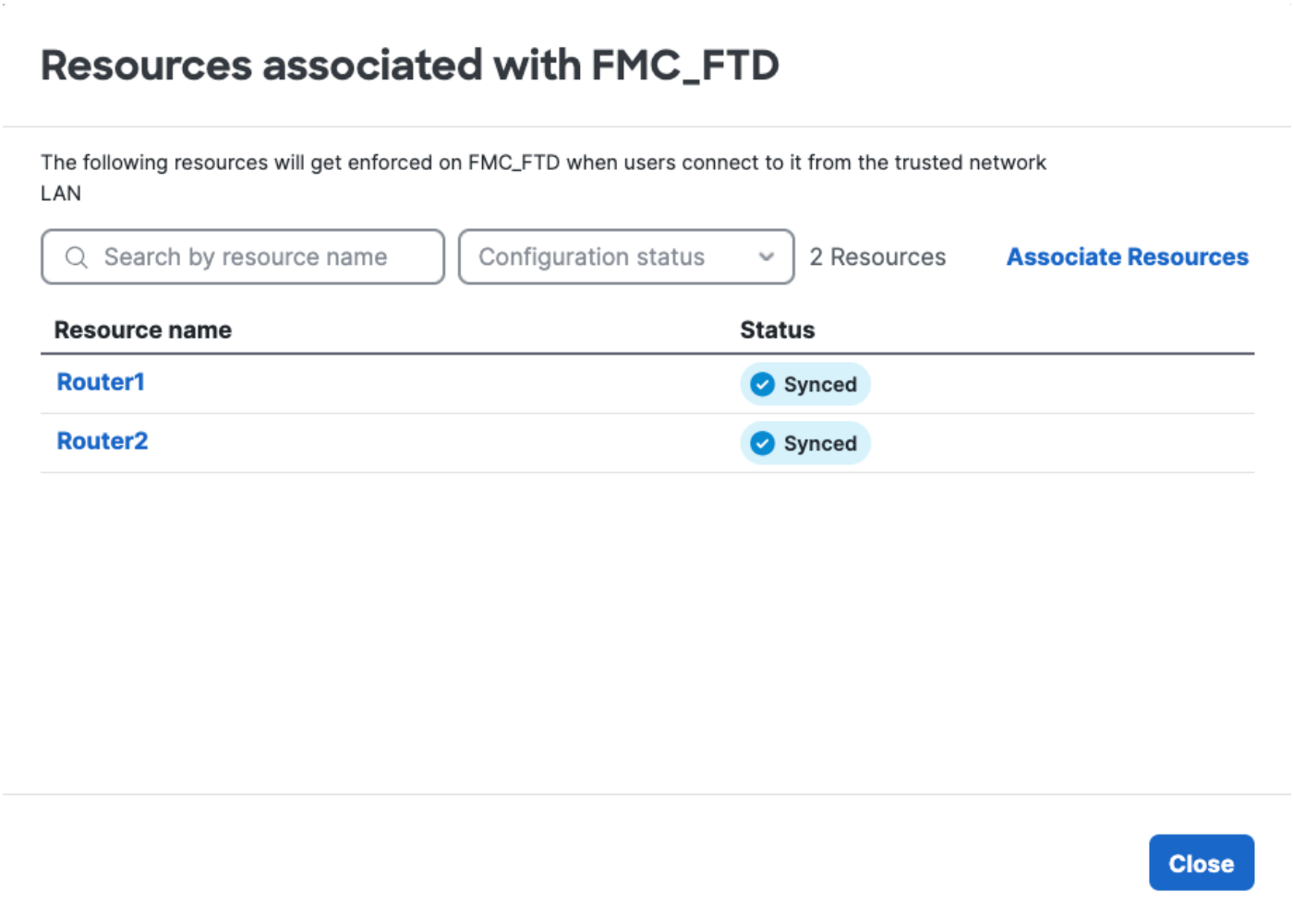


Veilige toegang - PR-verificatie

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

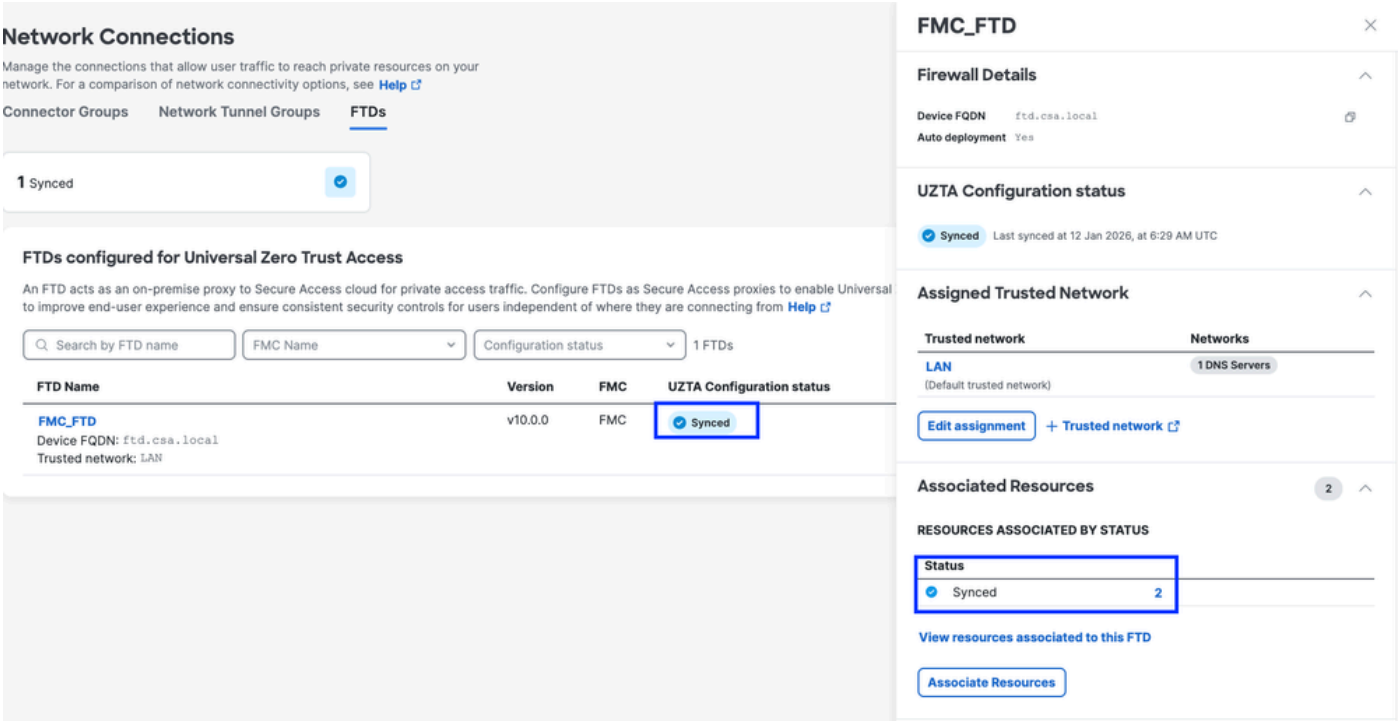


Veilige toegang - PR-verificatie



3. Klik op sluiten

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



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

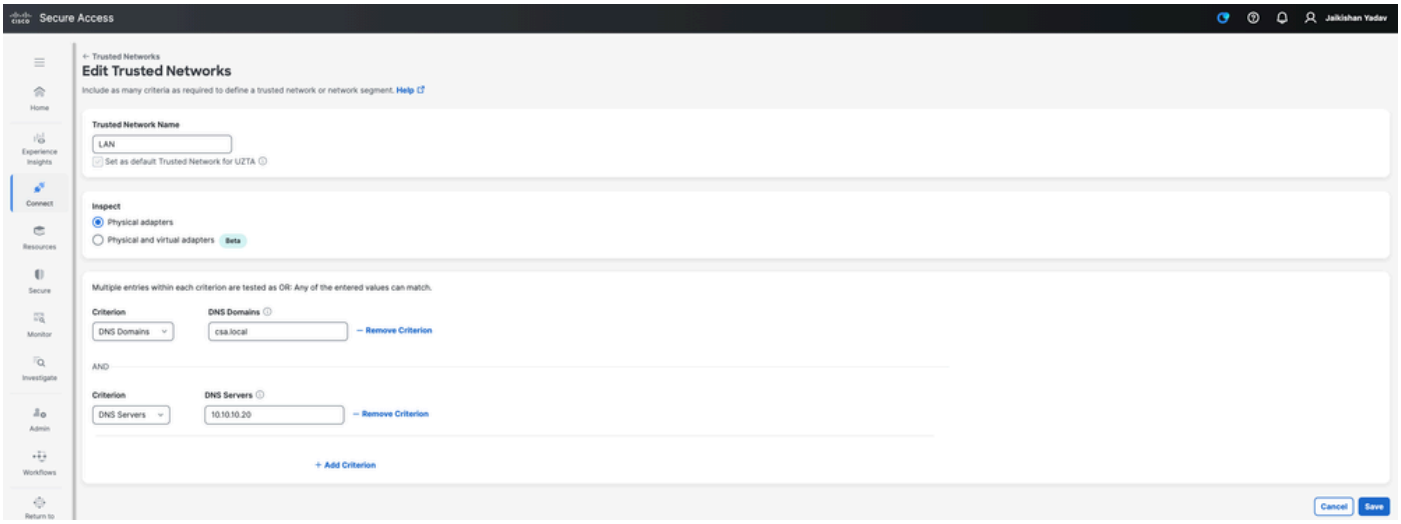
Toon de toepassing Running-Config Object

```
ftd# sh run 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"

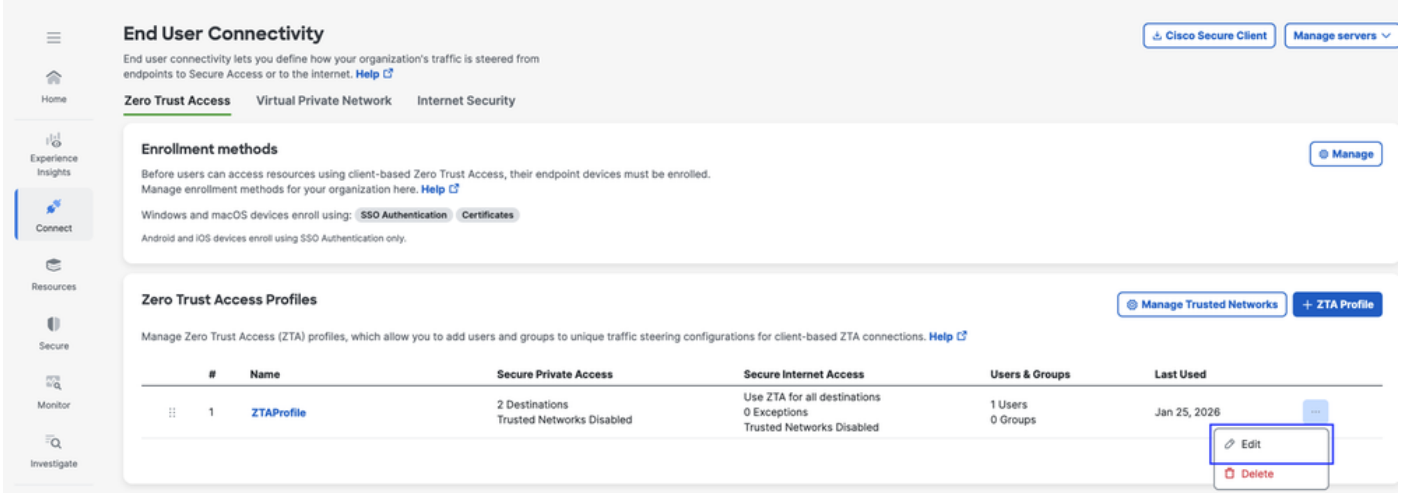
Navigeer naar Verbinding maken > Eindgebruikersconnectiviteit > Toegang zonder vertrouwen > ZTA-instellingen en configureer vertrouwde netwerken



Veilige toegang - TND-configuratie

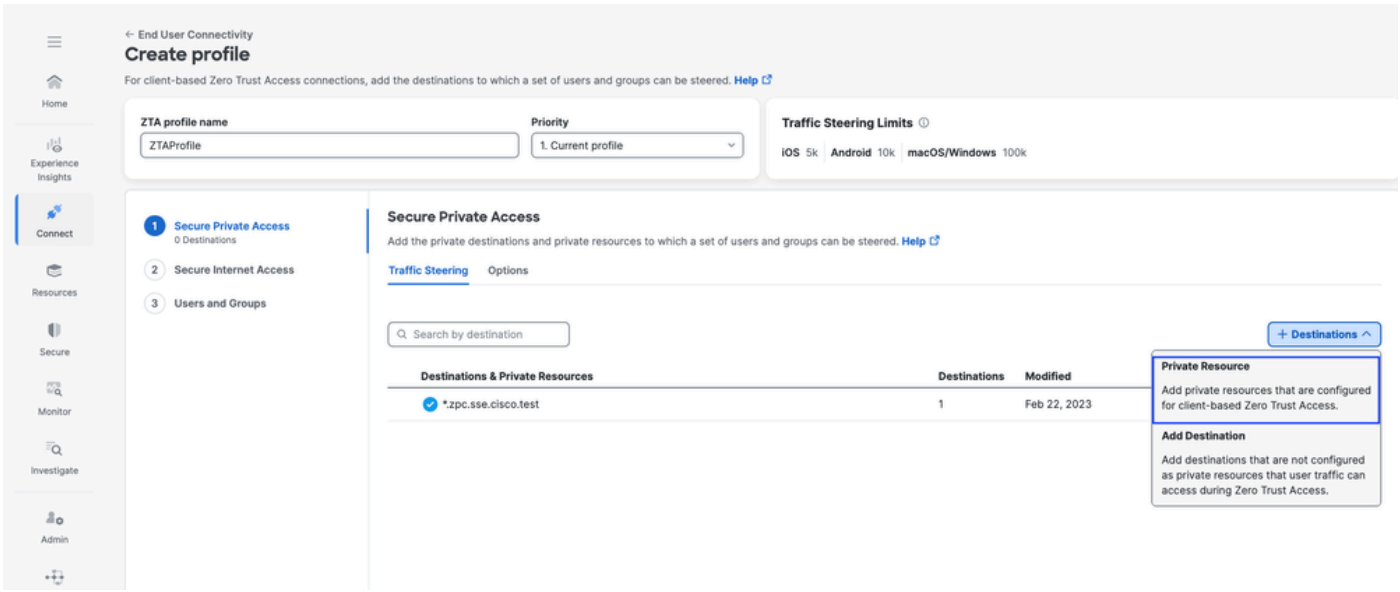
Stap -5 Voeg privé-bronnen toe aan het ZTA-profiel

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

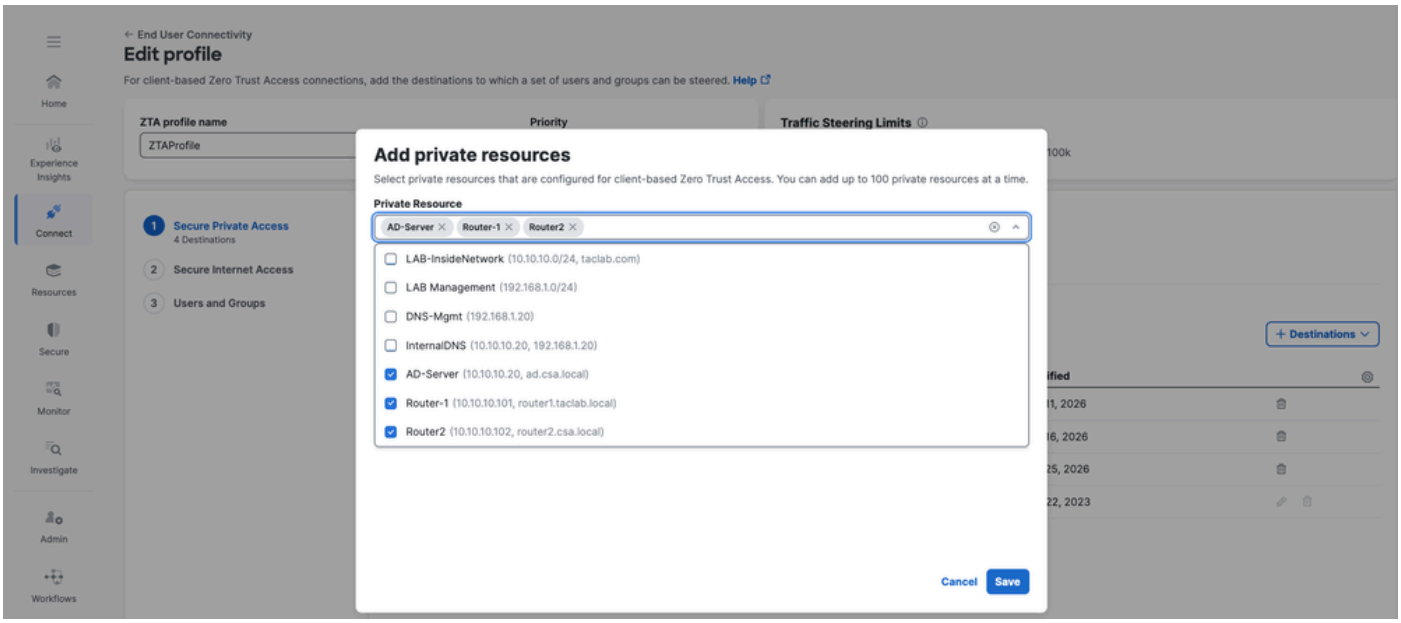


Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

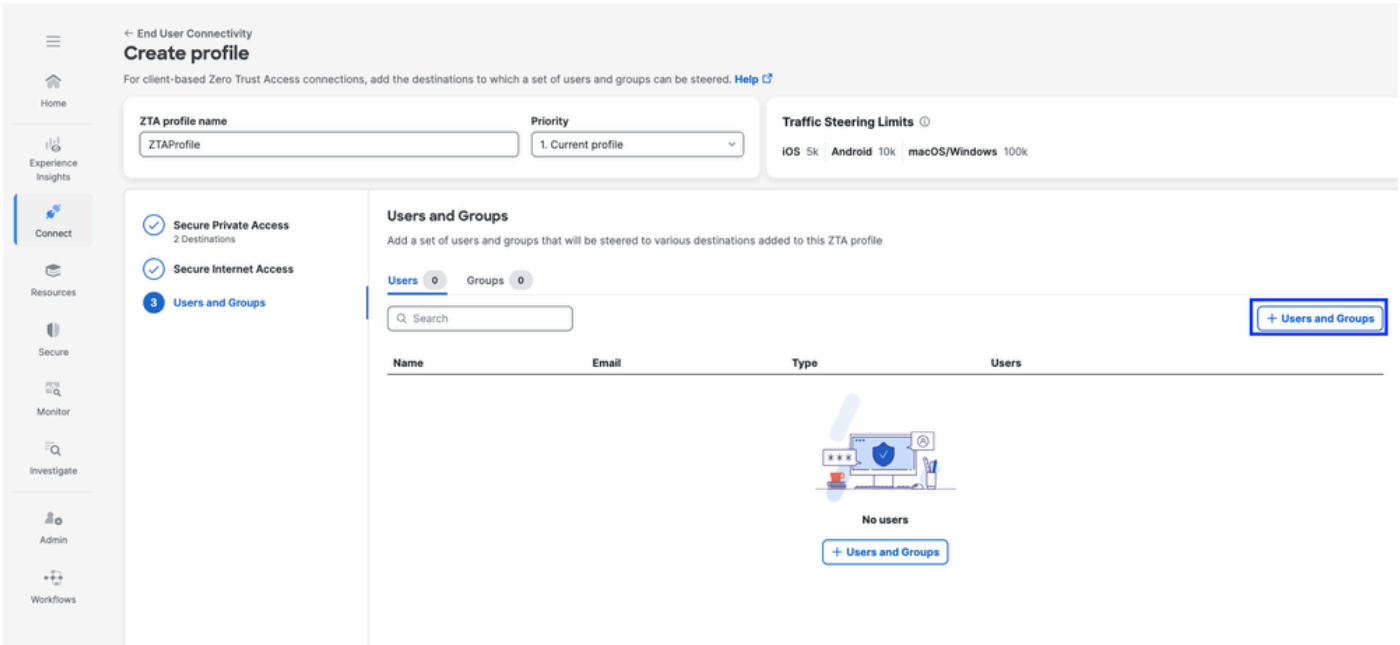


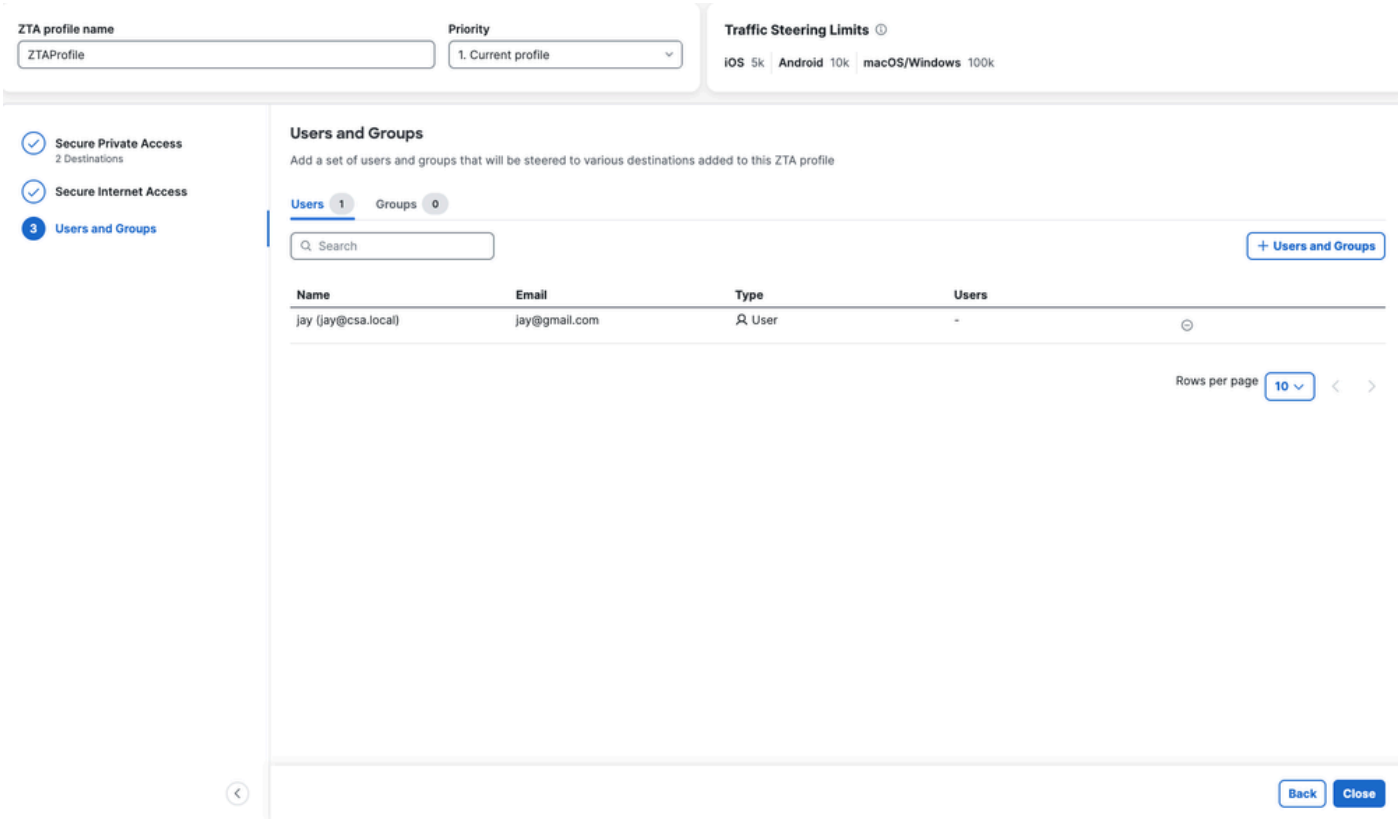
Veilige toegang - ZTA-profiel



Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen

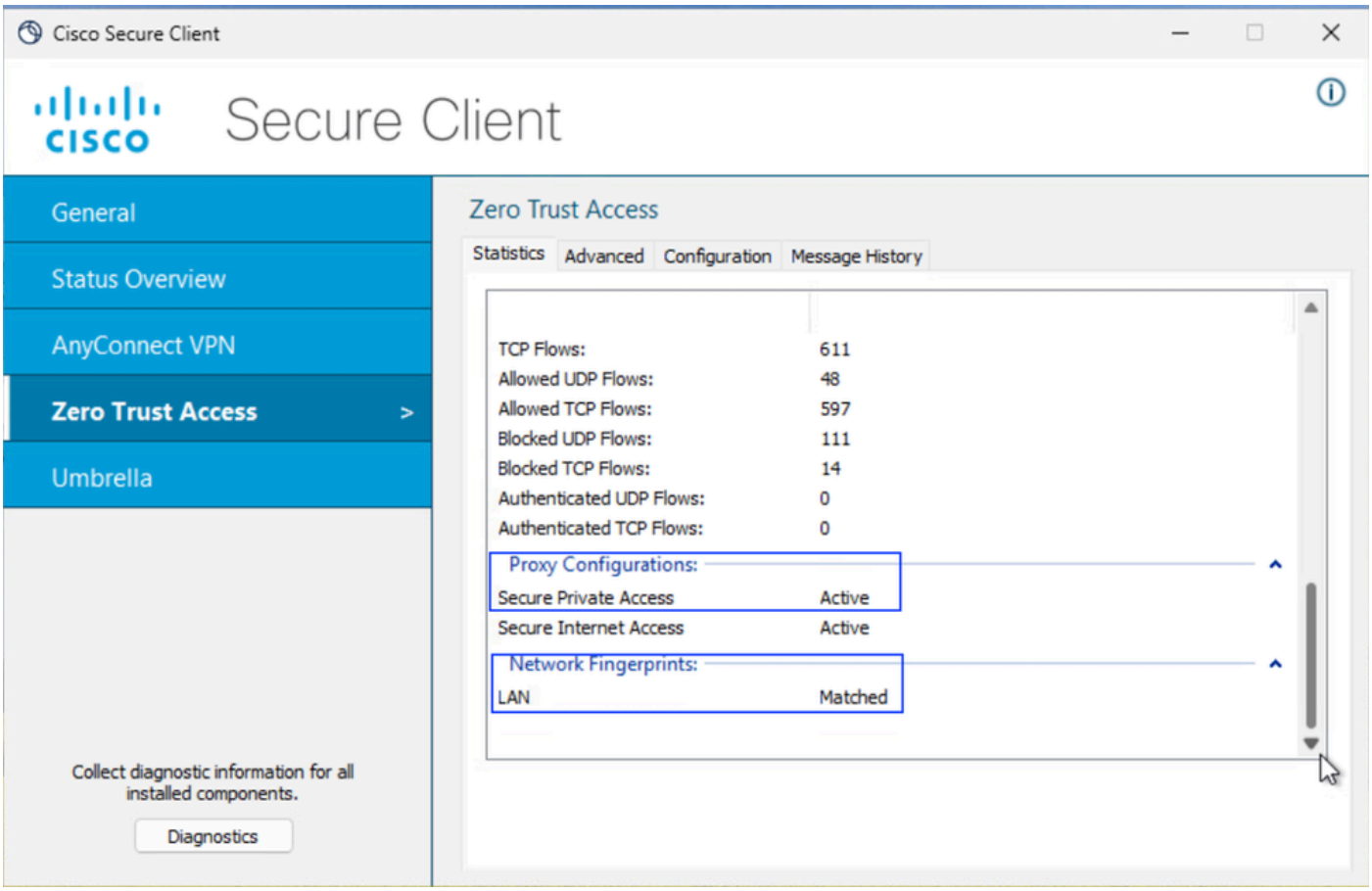




Veilige toegang - ZTA-profiel

Stap 6: Controleer de toegang tot de privébron

1. Controleer de netwerkvingerafdruk voor ZTA TND



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

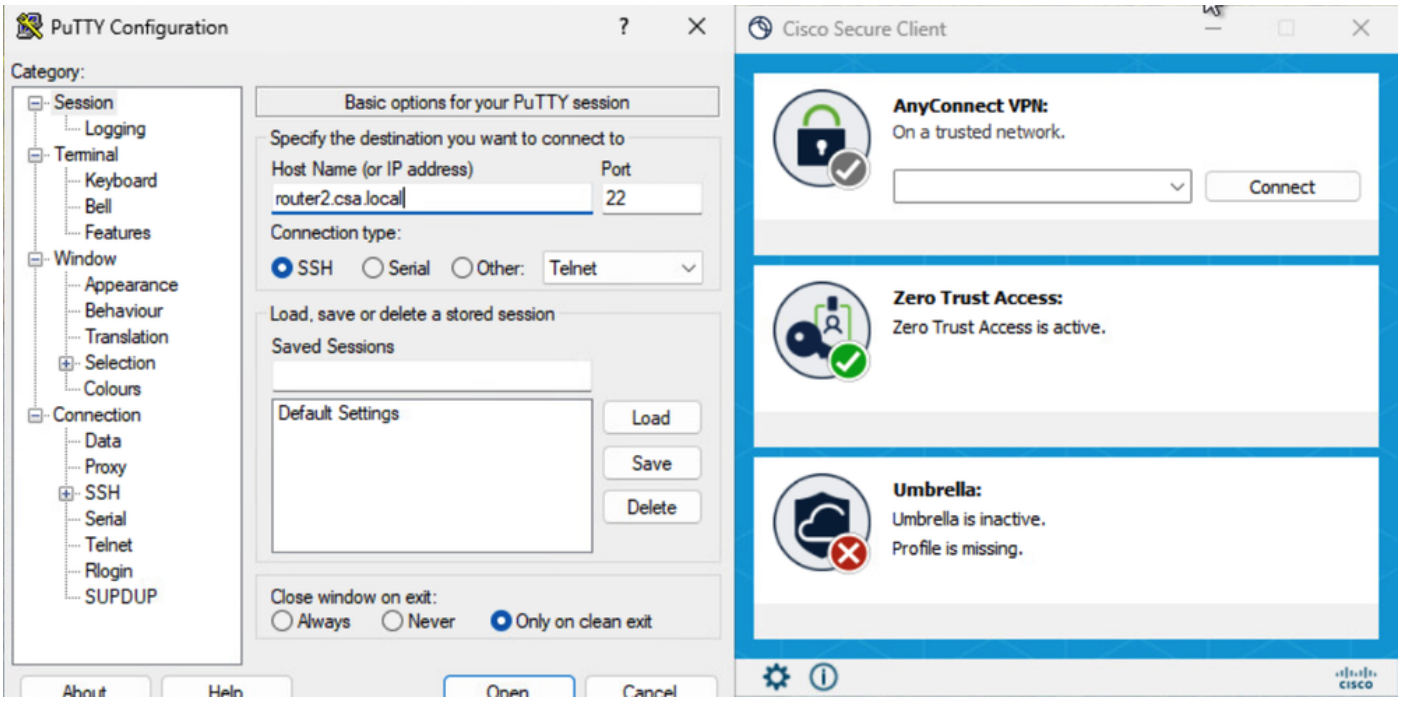
3. Controleren of FTD particuliere bronnen kan bereiken met behulp van FQDN

```
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#
```

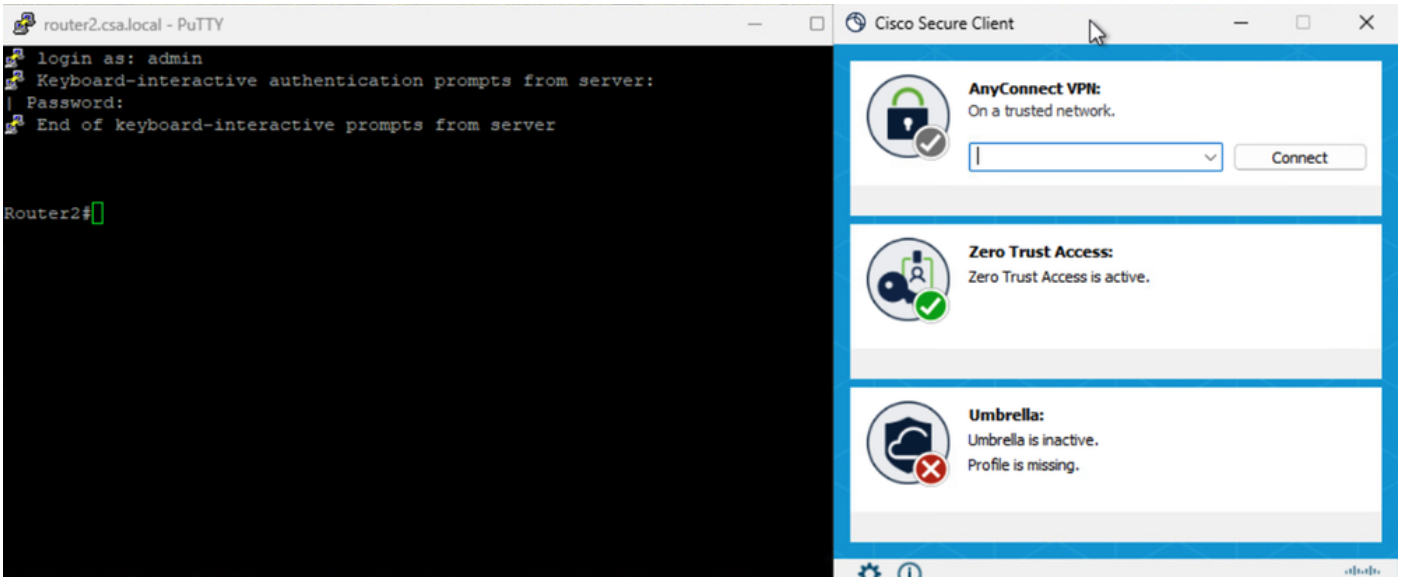
Veilige toegang - PR-testen

4. Test de SSH-verbinding met de Private Resource

Toegang tot de PR via FQDN

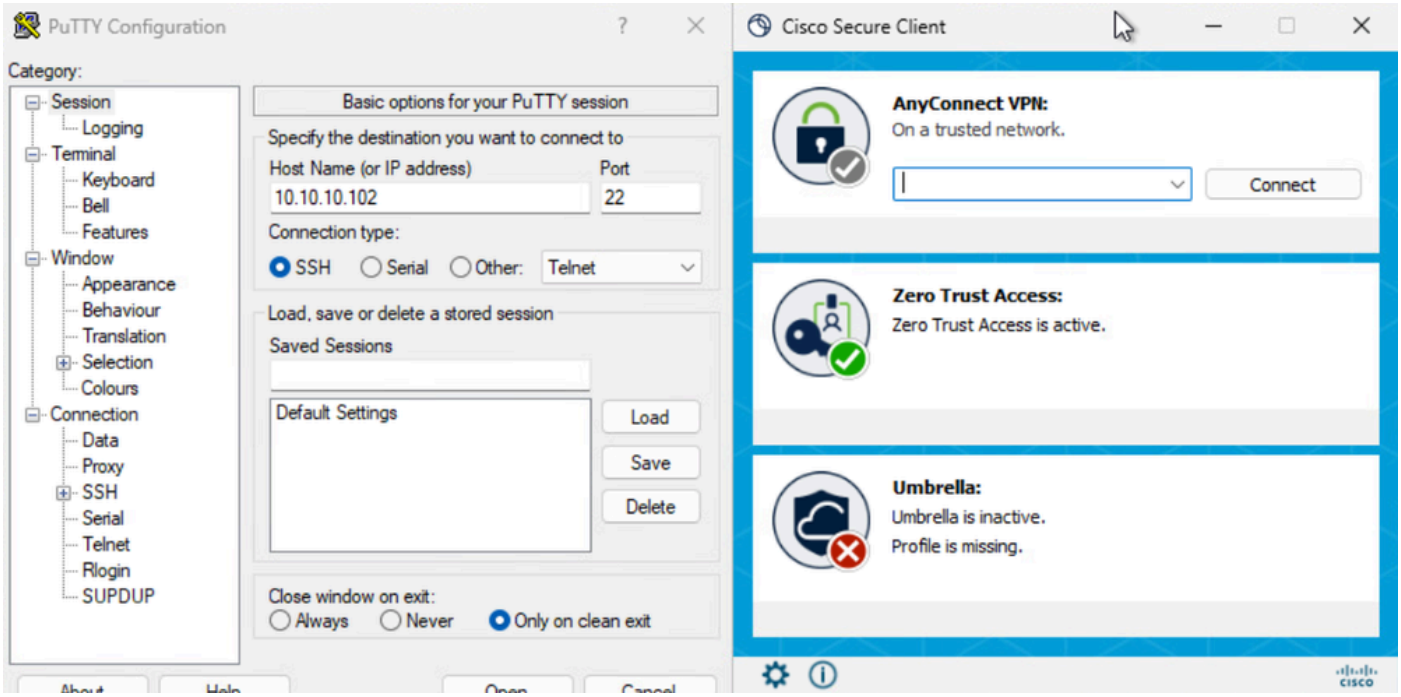


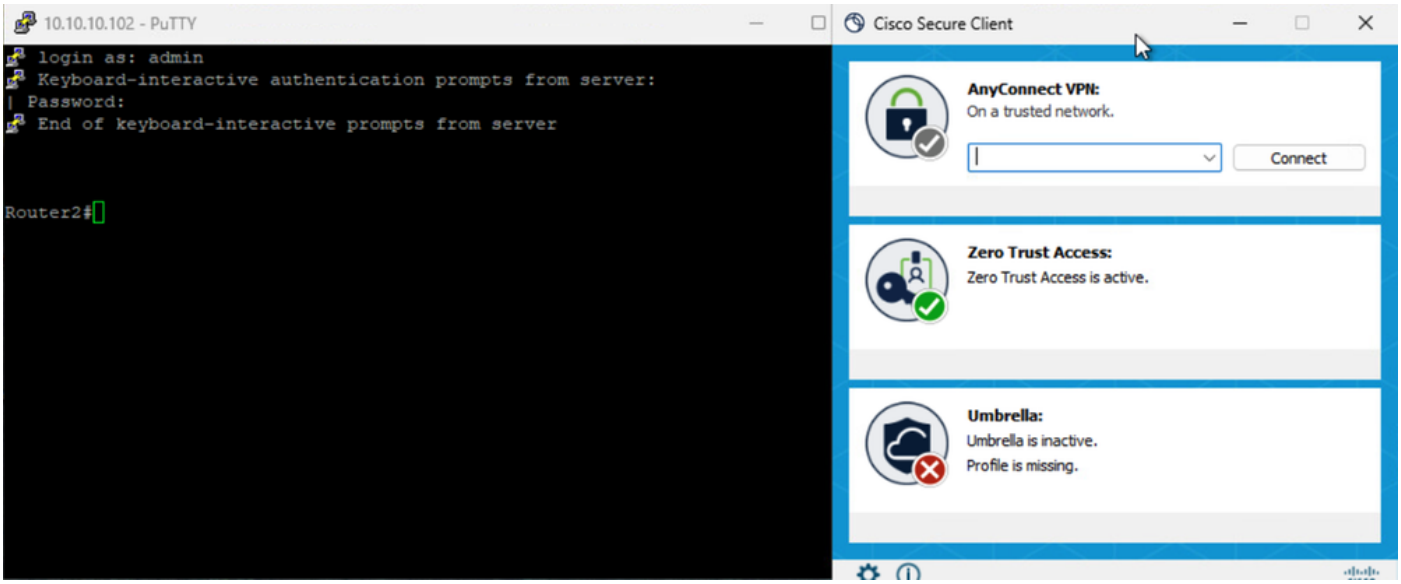
Veilige toegang - PR-testen



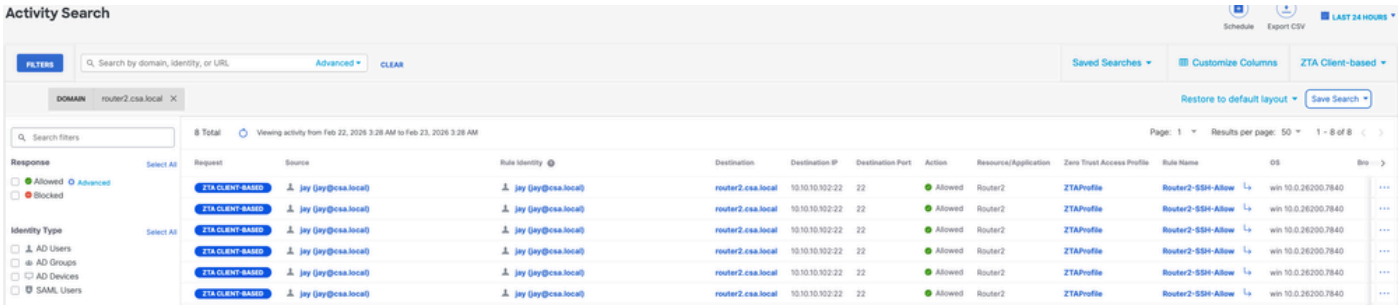
Veilige toegang - PR-testen

Toegang tot de PR via IP-adres

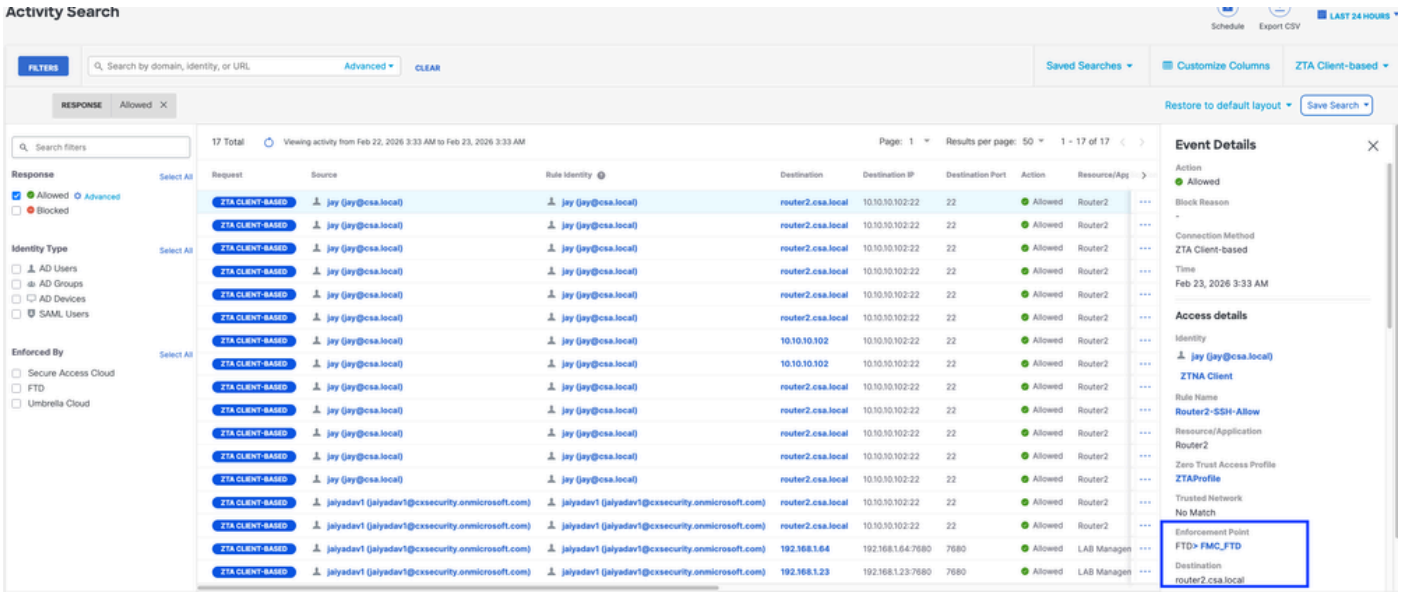




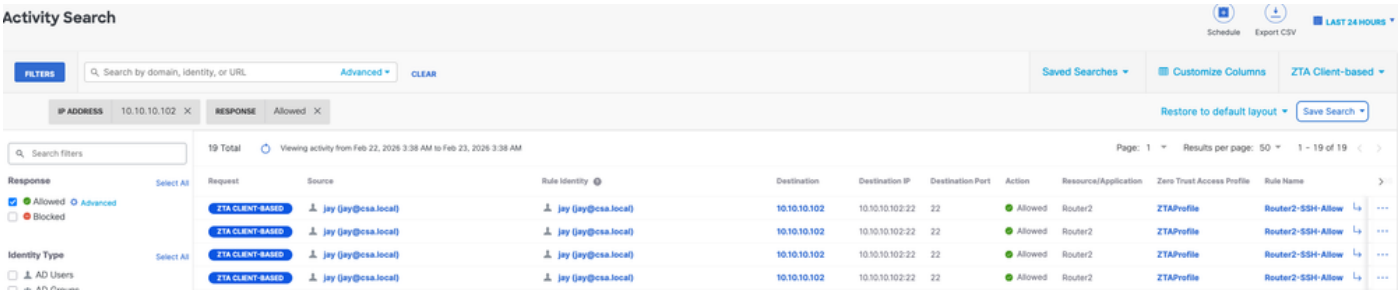
5. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten



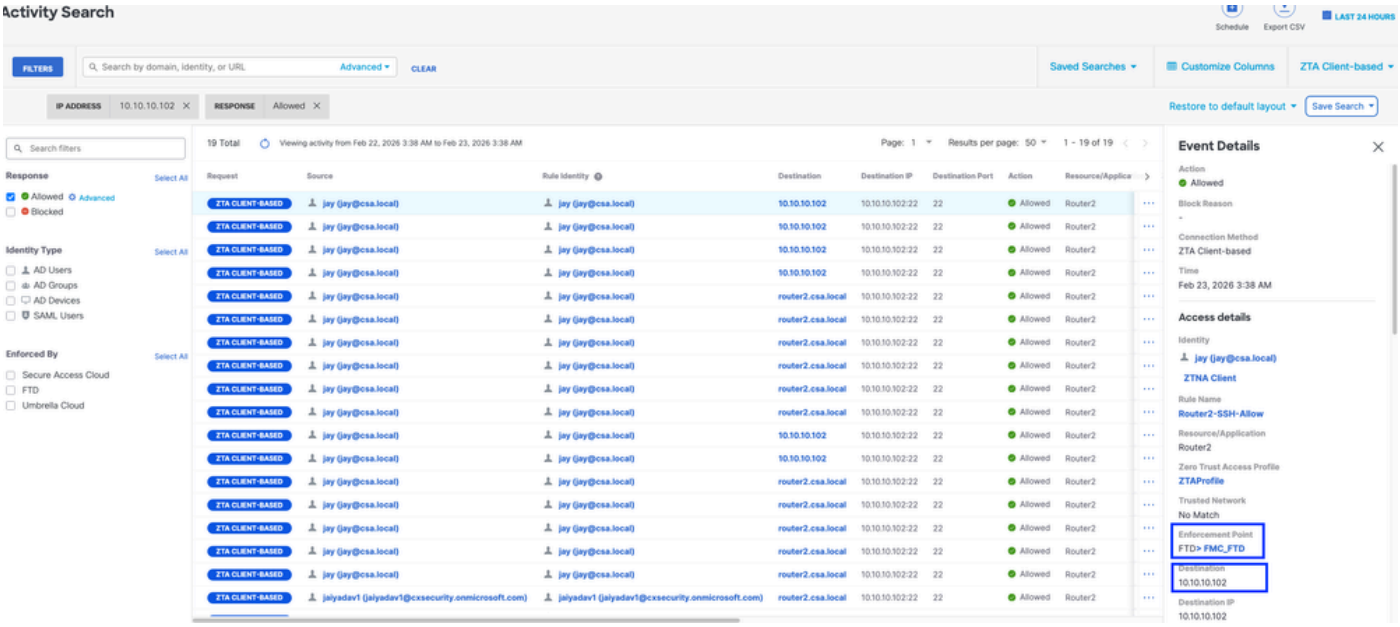
Veilige toegang - zoeken naar activiteiten



Veilige toegang - zoeken naar activiteiten

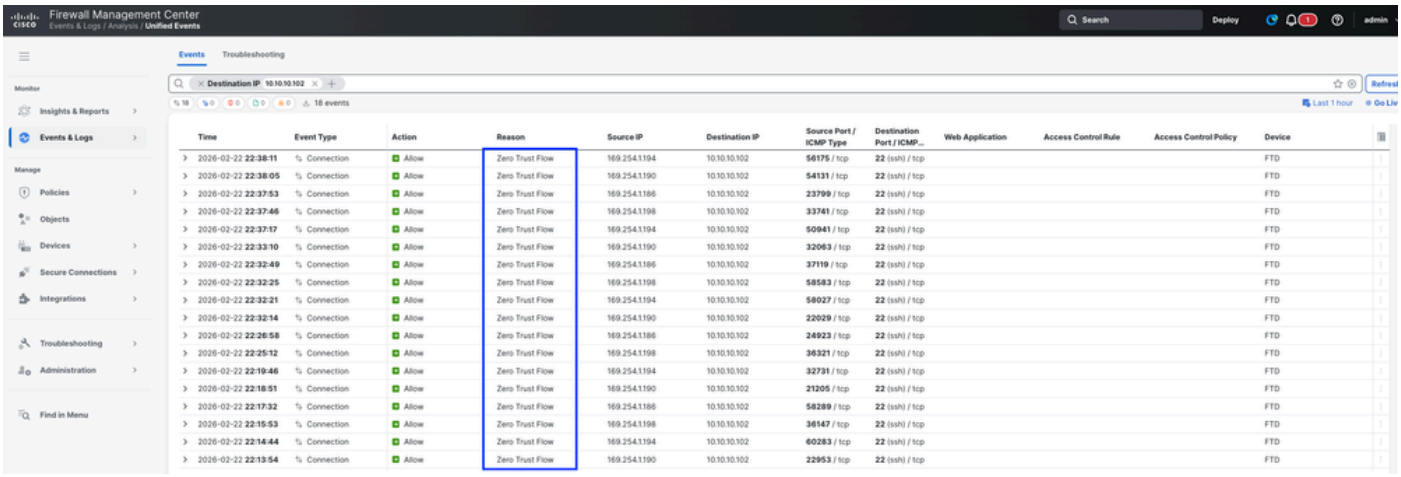


Veilige toegang - zoeken naar activiteiten



Veilige toegang - zoeken naar activiteiten

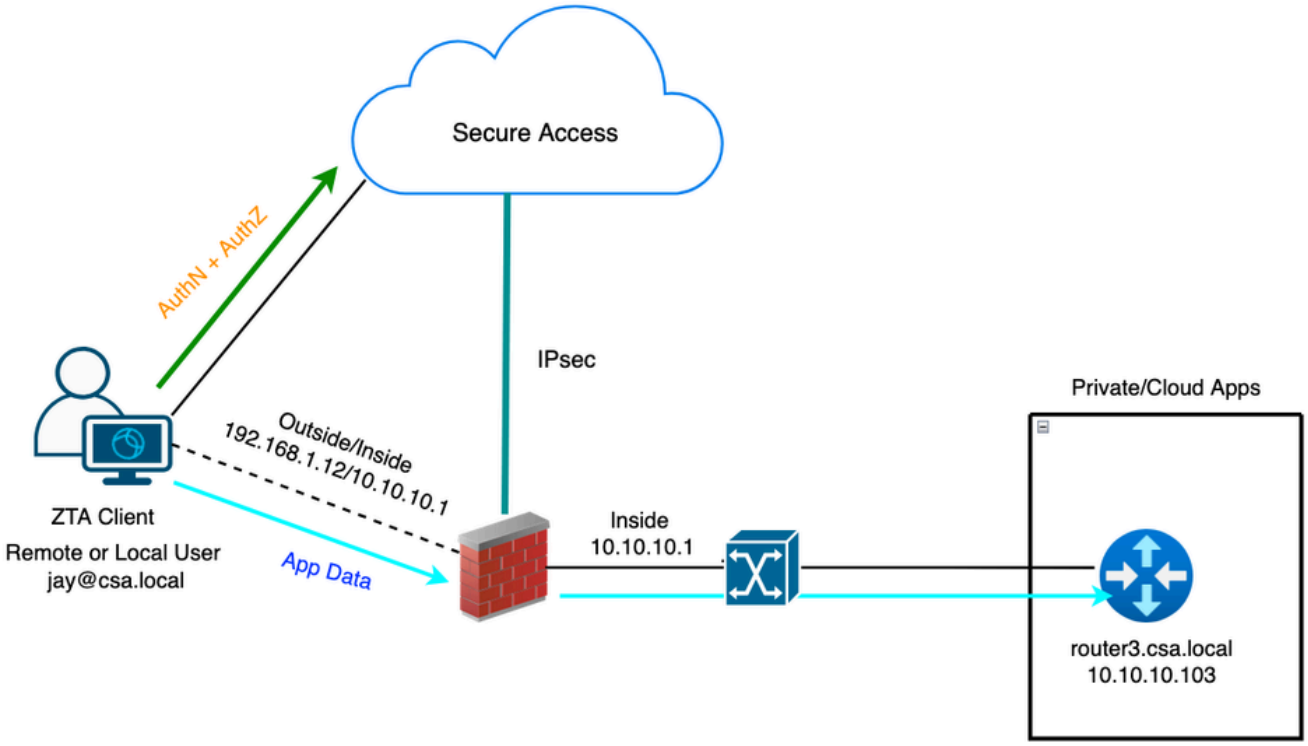
6. FMC-verbindingsgebeurtenissen controleren



FMC-verbindingsgebeurtenissen

Testcase 4 - Lokale en externe gebruiker - Lokale of cloudhandhaving met TND

In dit geval hangt het type handhaving af van de locatie van de gebruiker, als de gebruiker Lokaal is of achter een vertrouwde FTD-zone (binnen, DMZ enz.), dan zou de handhaving Lokaal zijn (Test case 3). Evenzo, als de gebruiker op afstand is, zou de handhaving cloud zijn (testcase 1). De locatie van de gebruiker wordt bepaald op basis van de Network Fingerprint- of TND-instelling. Als de netwerkvingerafdruk overeenkomt, is de lokale locatie van de gebruiker Lokaal en als deze niet overeenkomt, wordt de lokale gebruiker als Extern beschouwd.

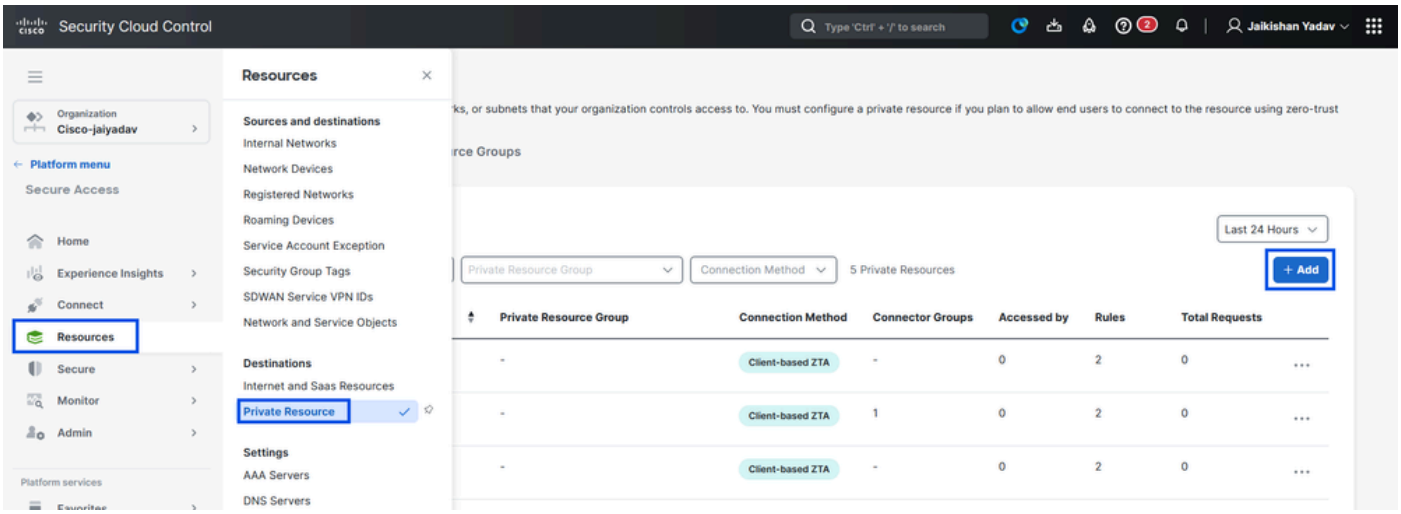


Universal ZTA - Test Case Topology

Stap 1 - Een privébron definiëren voor beveiligde toegang

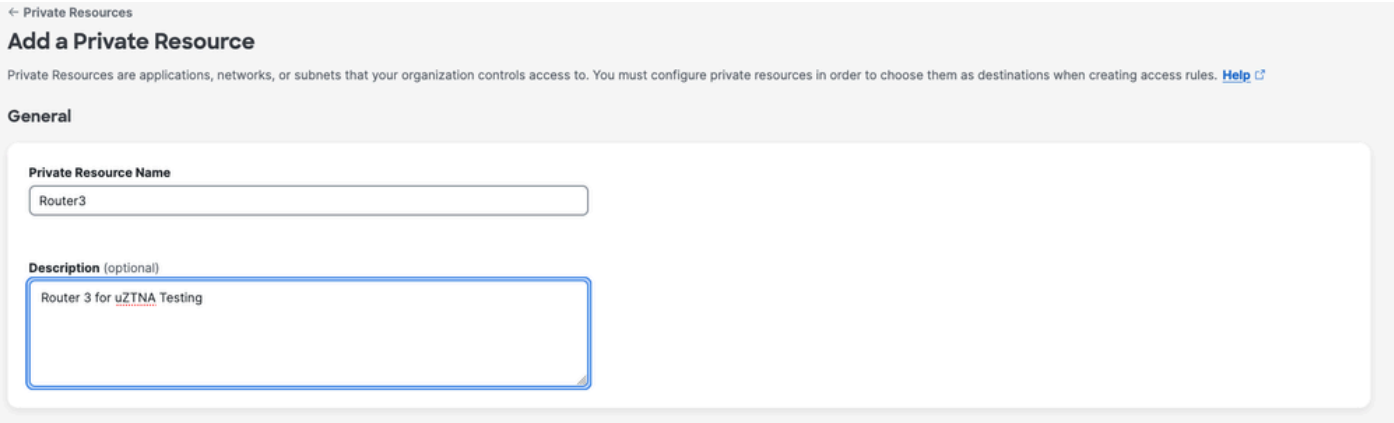
Configureer een privébron die toegankelijk is via een apparaat waarvoor Zero Trust Access (ZTA) is ingeschreven met cloudhandhaving

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



Veilige toegang - Configuratie van privébronnen

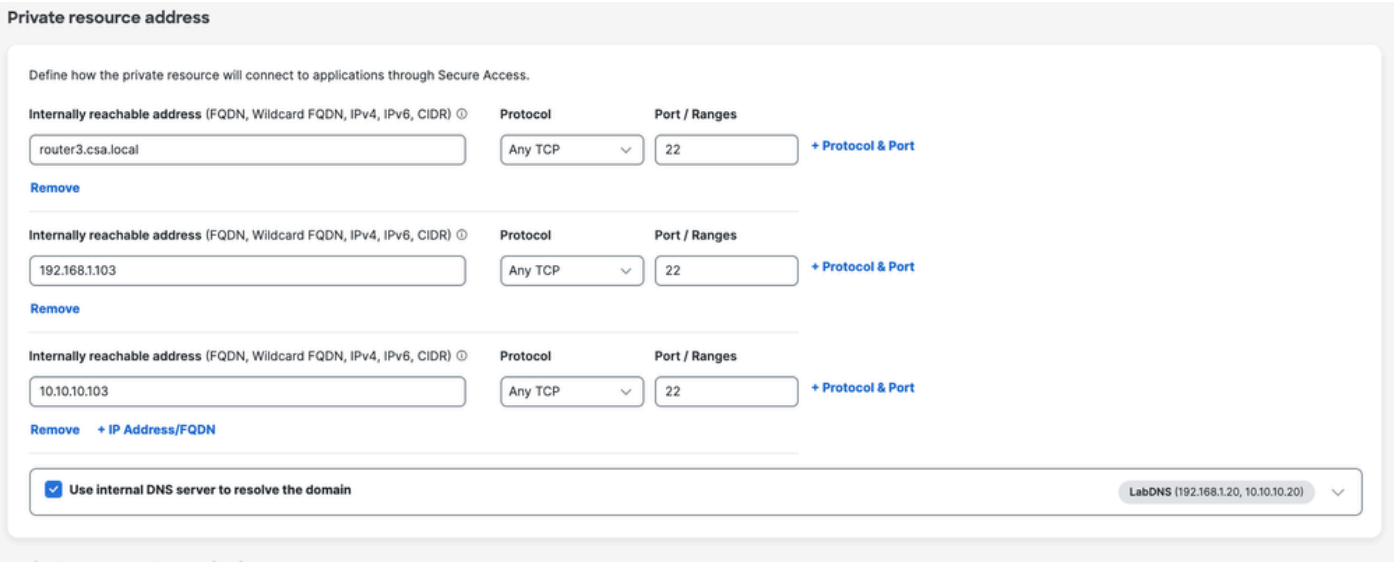
2. Voer voor de naam van de private resource een betekenisvolle naam in voor de resource. Voor de beschrijving raden we u aan informatie te verstrekken, zoals het doel van de bron of de naam van de eigenaar van de bron.



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

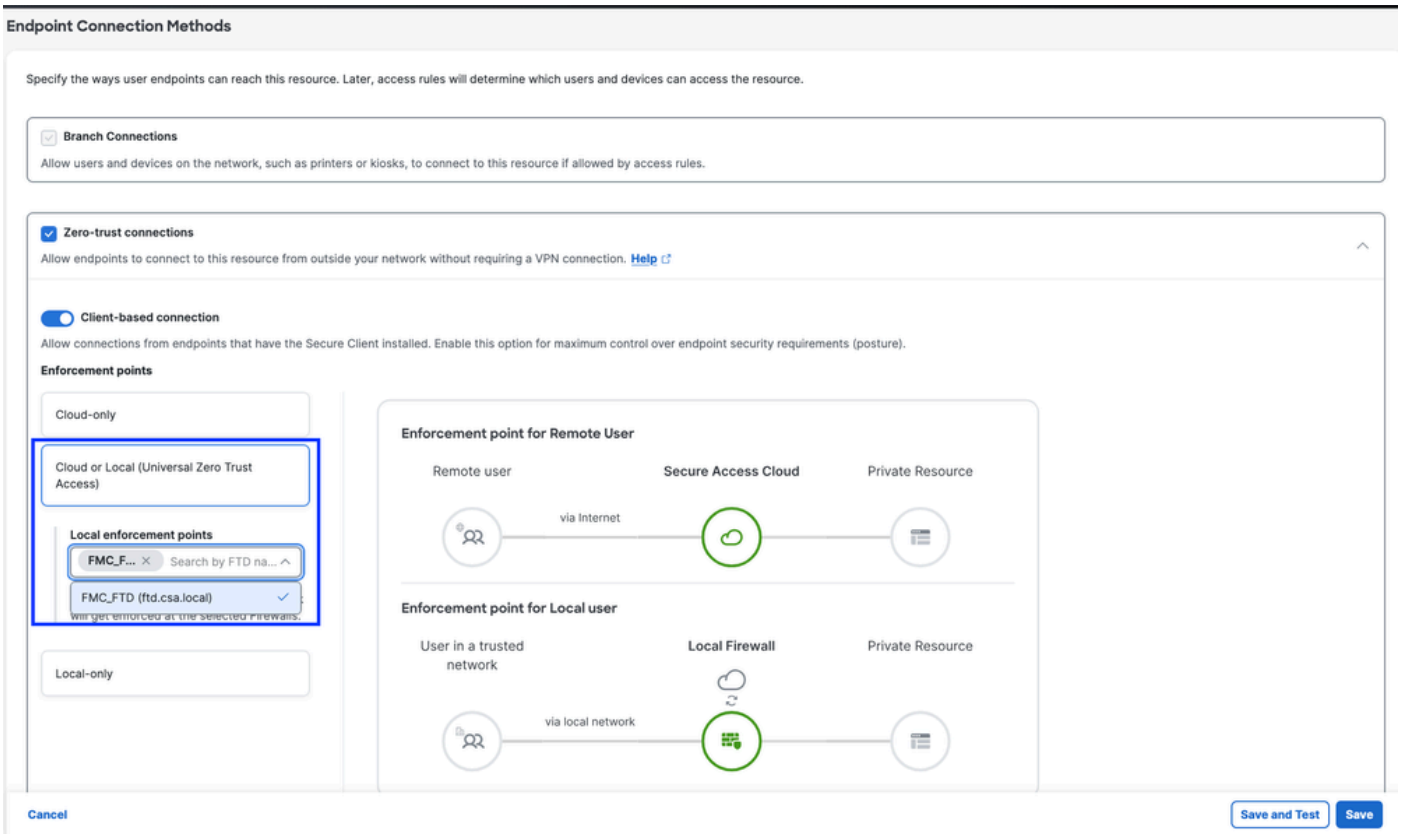
4. Selecteer de DNS-server om het domein op te lossen



Veilige toegang - Configuratie van privébronnen

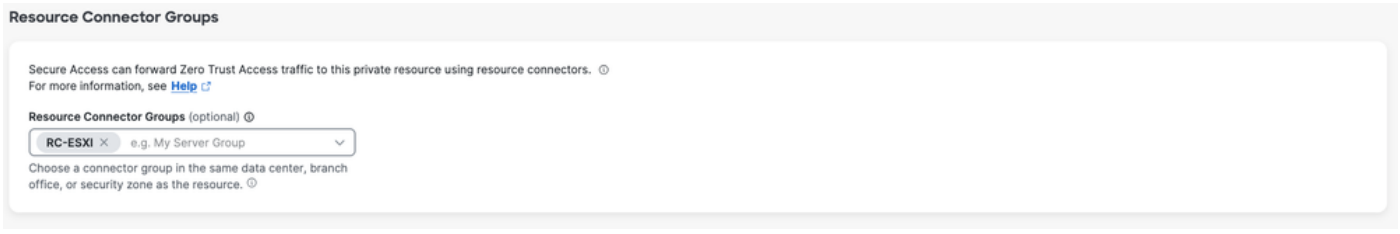
5. Selecteer methoden voor eindpuntverbinding

6. Selecteer FTD als lokale handhavingspunten



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).



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

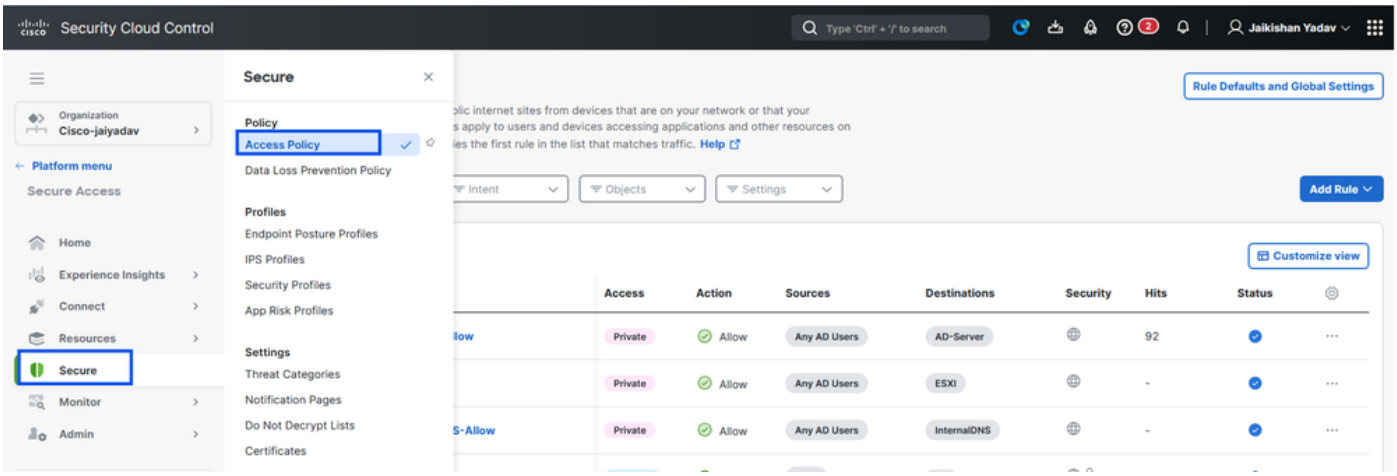
---

7. Klik op Opslaan

Stap 2 - Maak een regel voor privétoegang

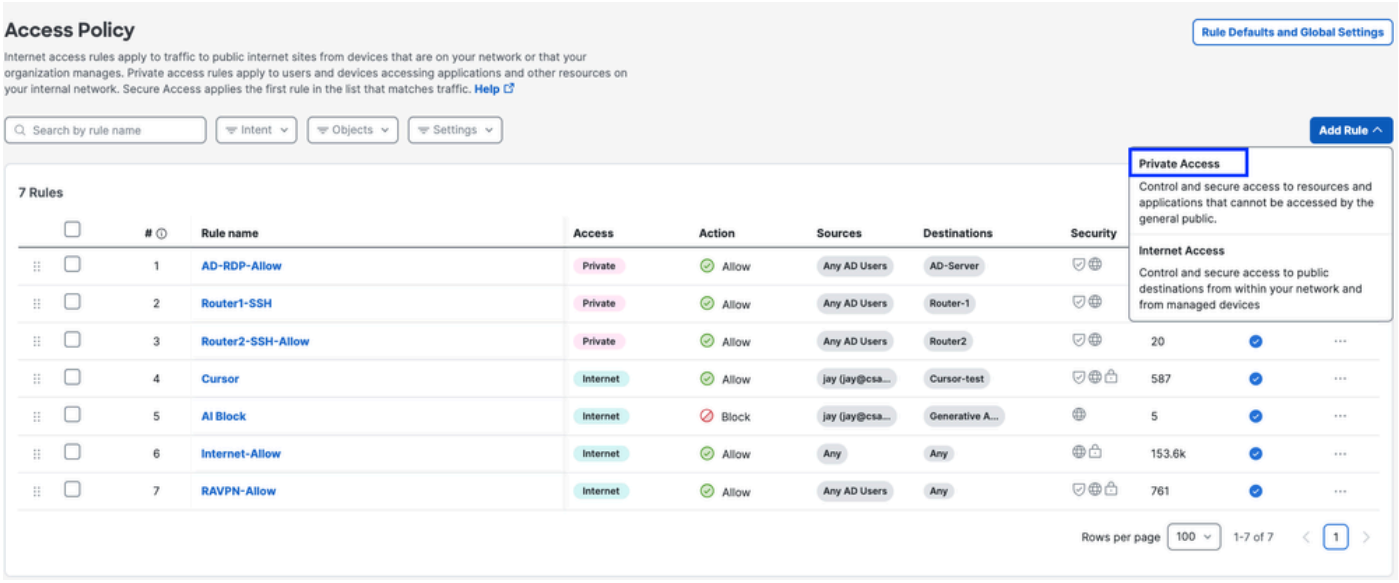
Configureer een privé-toegang op Secure Access om toegang te krijgen door Universal ZTA-geregistreerde gebruikers. Zie voor meer informatie Private Access Rule

1. Navigeer naar Beveiligd > Toegangsbeleid



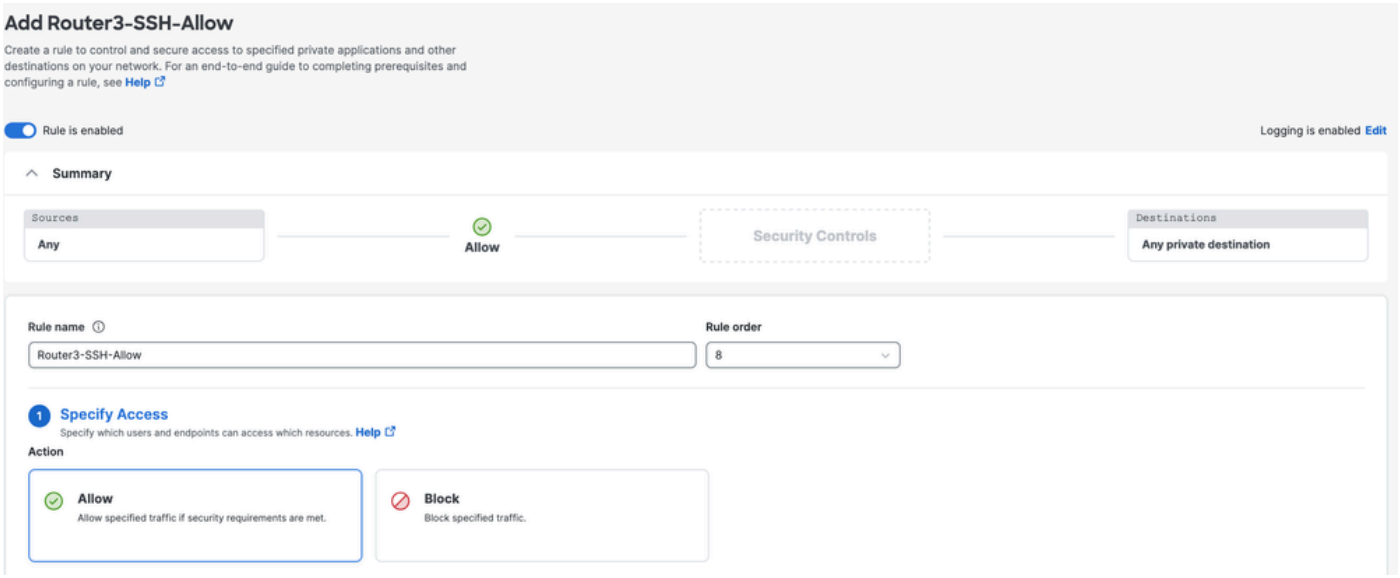
Beveiligde toegang - Configuratie toegangsbeleid

2. Klik op Regel toevoegen en kies vervolgens Particuliere toegang.
Bovenaan de regel staat een samenvatting die de geconfigureerde componenten van uw regel beschrijft.



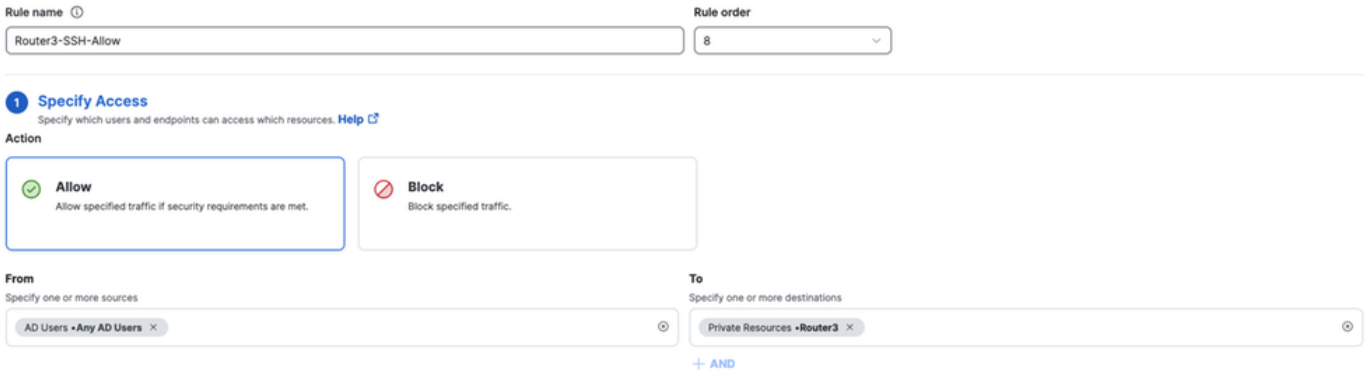
Beveiligde toegang - Configuratie toegangsbeleid

3. Een regelnaam toevoegen



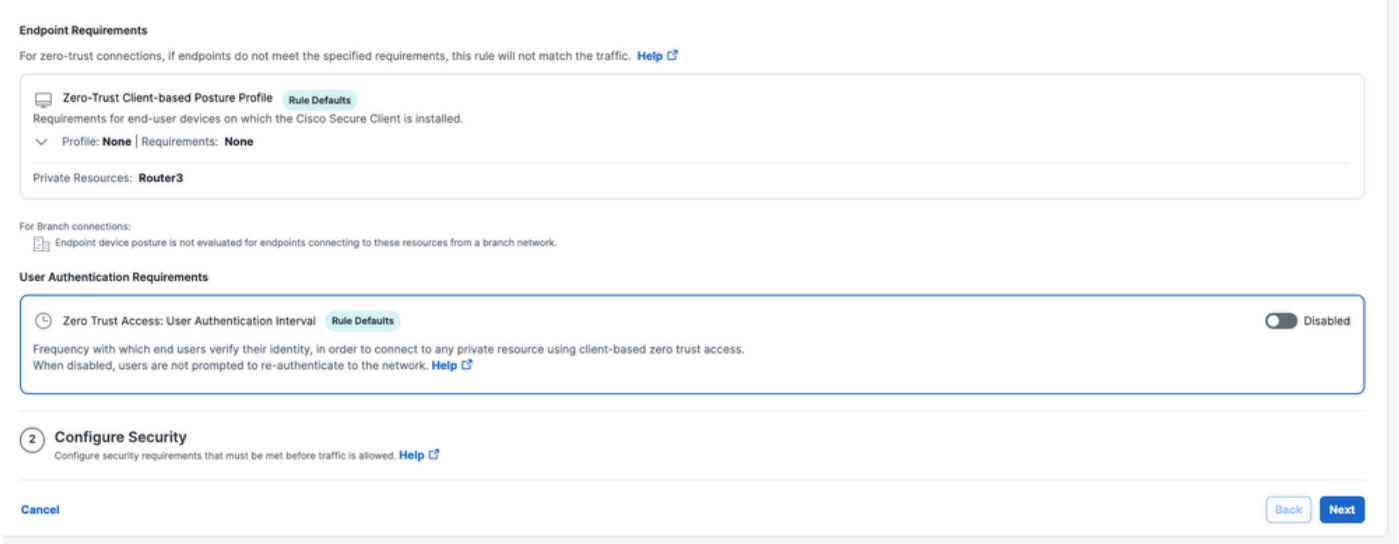
Beveiligde toegang - Configuratie toegangsbeleid

4. Selecteer de actie regel en selecteer bron en bestemming



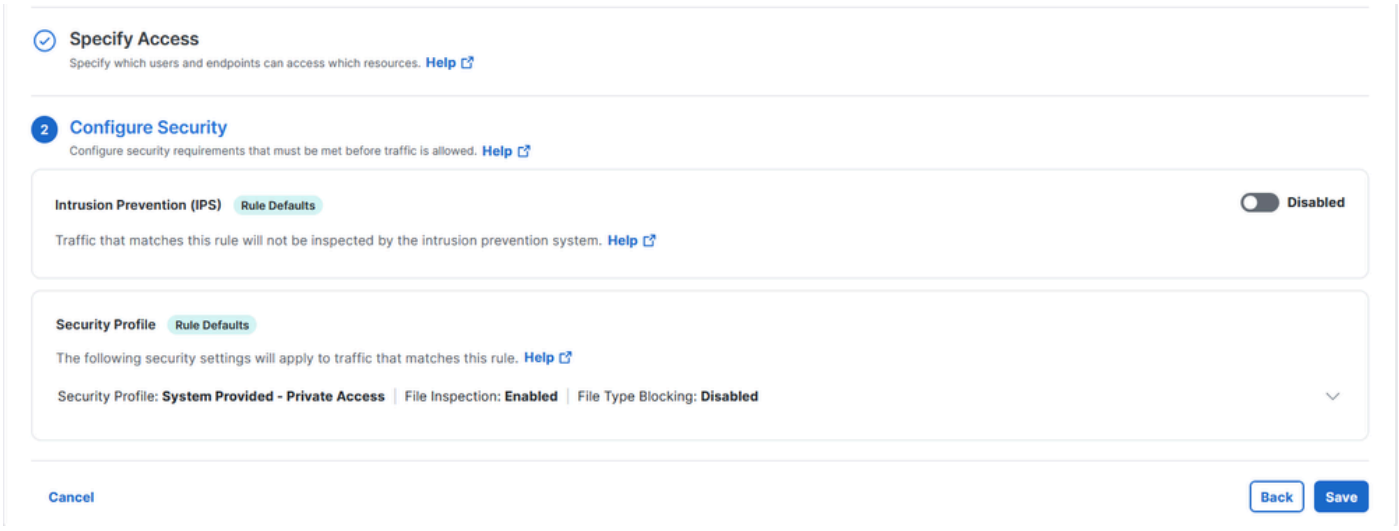
Beveiligde toegang - Configuratie toegangsbeleid

5. Eindpuntvereisten configureren



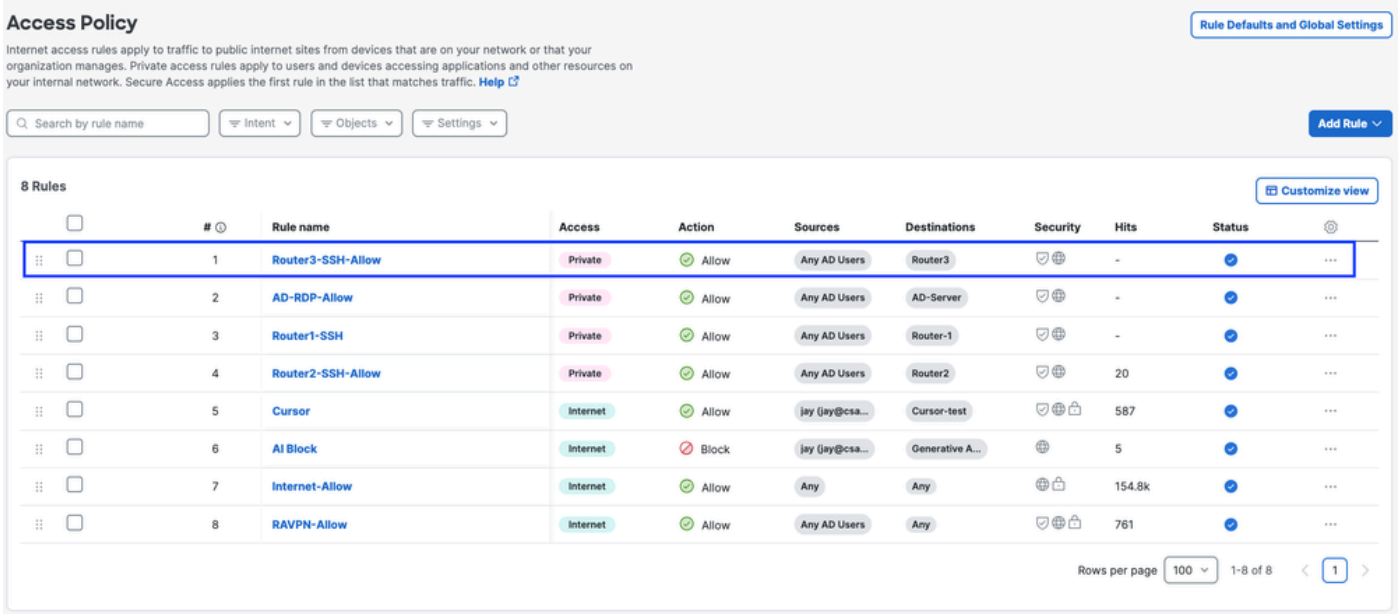
Beveiligde toegang - Configuratie toegangsbeleid

6. Beveiliging configureren



Beveiligde toegang - Configuratie toegangsbeleid

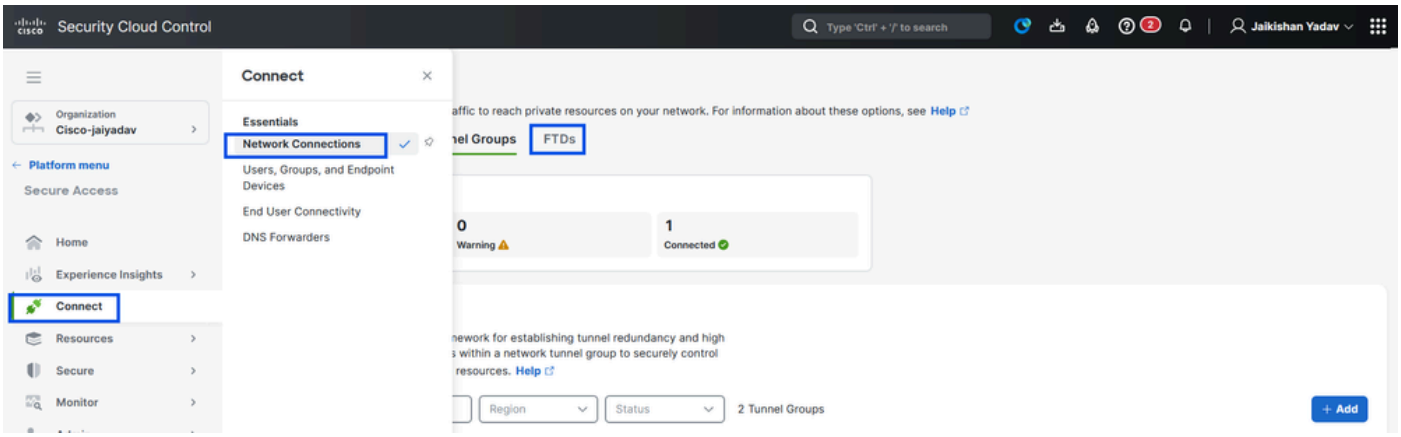
7. Klik op Opslaan



Beveiligde toegang - Configuratie toegangsbeleid

Stap 3 - Controleer de associatie van PR op de FTD

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

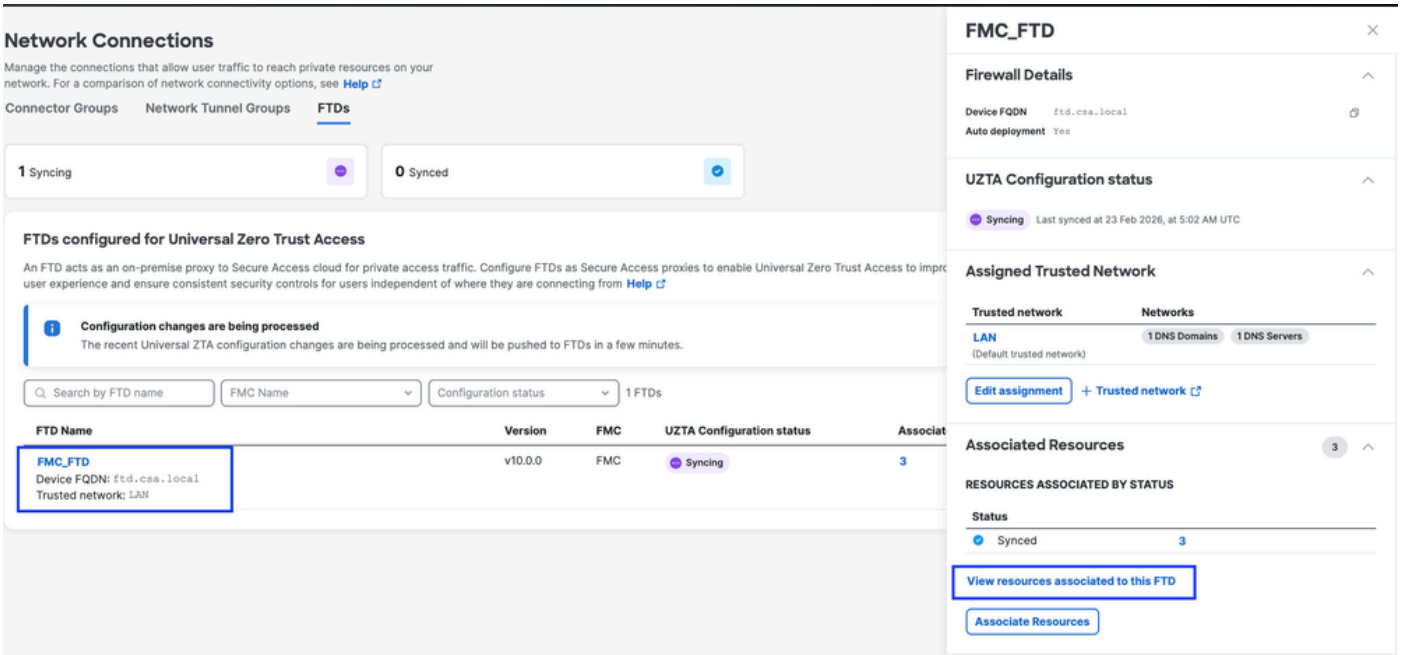


Veilige toegang - PR-verificatie

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
```

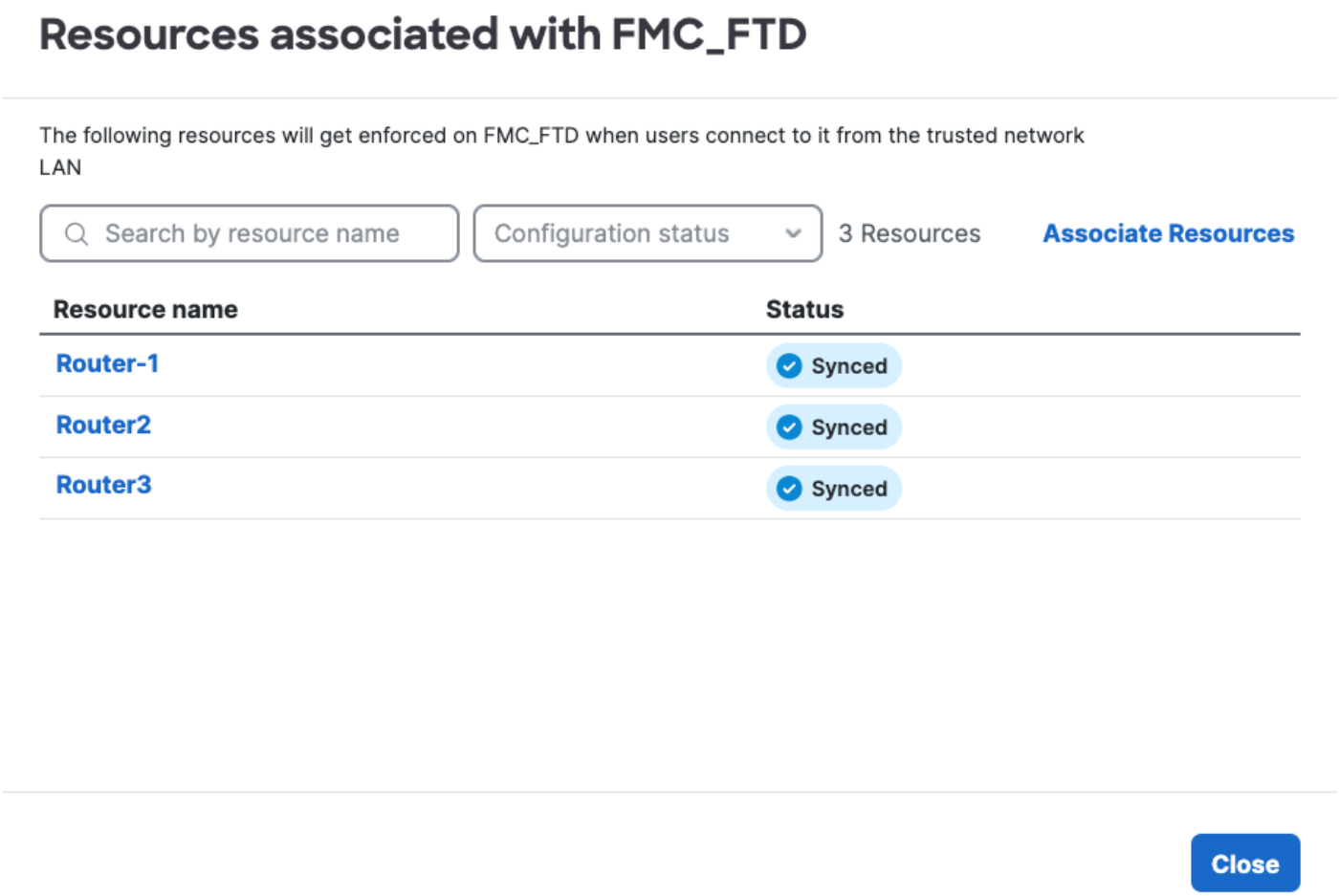
Veilige toegang - PR-verificatie



Veilige toegang - PR-verificatie

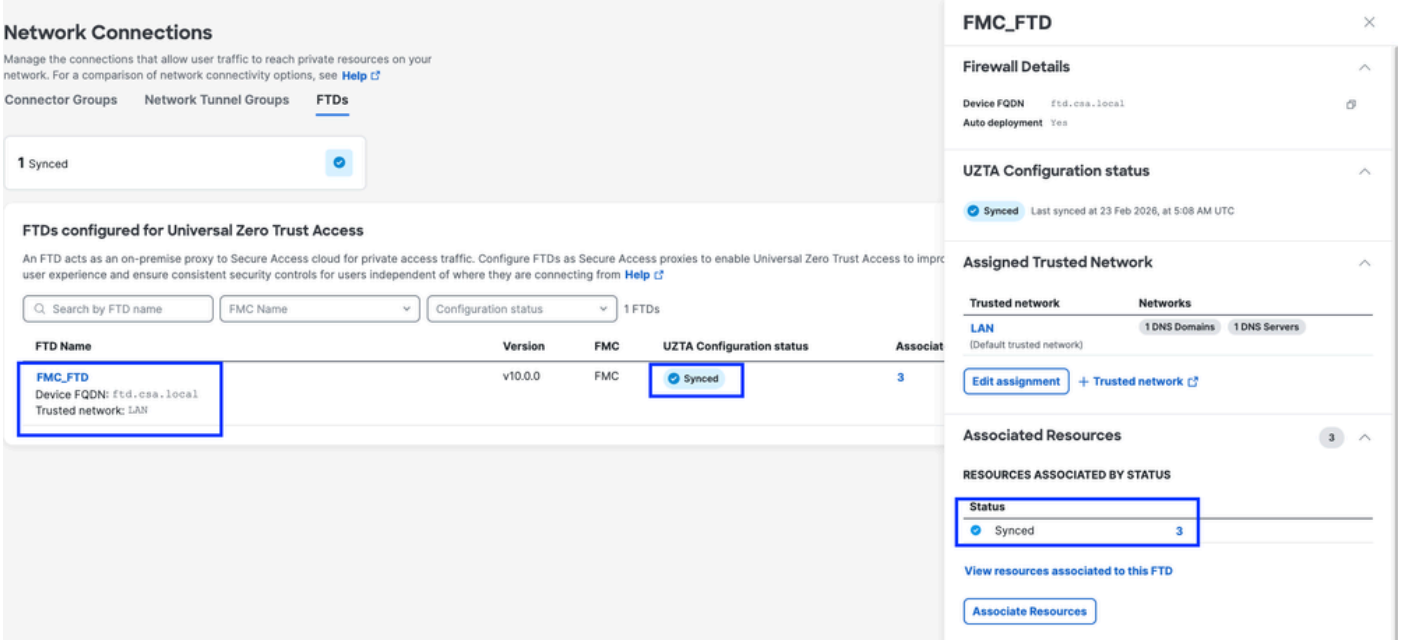
```
C:\Users\jay>ping ftd.csa.local

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



3. Klik op sluiten

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



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

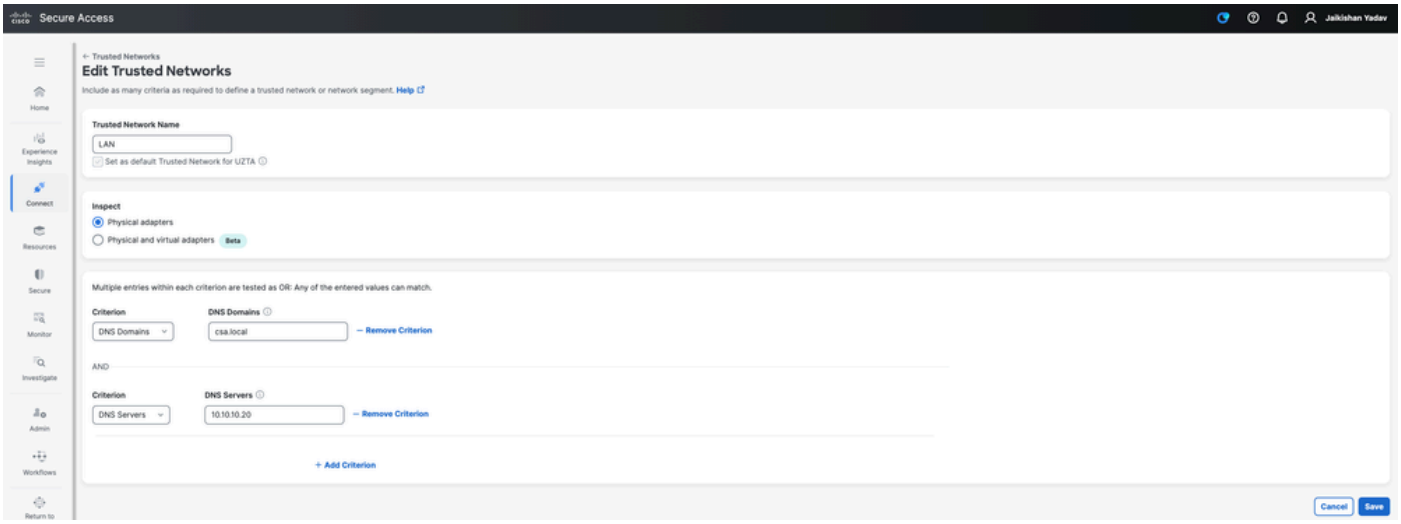
Toon de toepassing Running-Config Object

```
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"

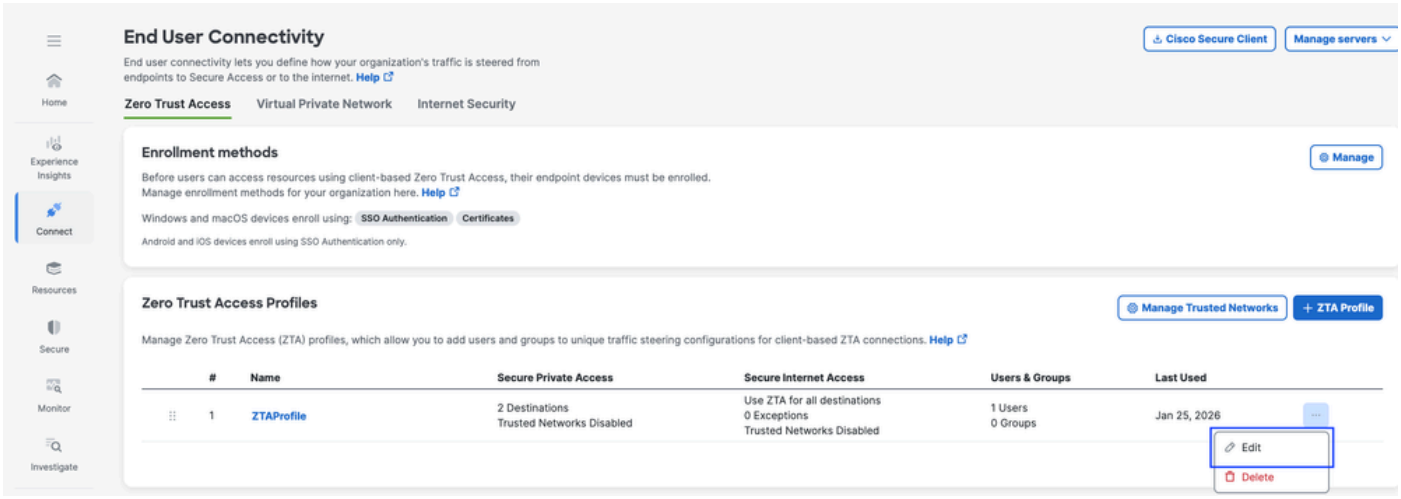
Navigeer naar Verbinding maken > Eindgebruikersconnectiviteit > Toegang zonder vertrouwen > ZTA-instellingen en configureer vertrouwde netwerken



Veilige toegang - ZTA TND-configuratie

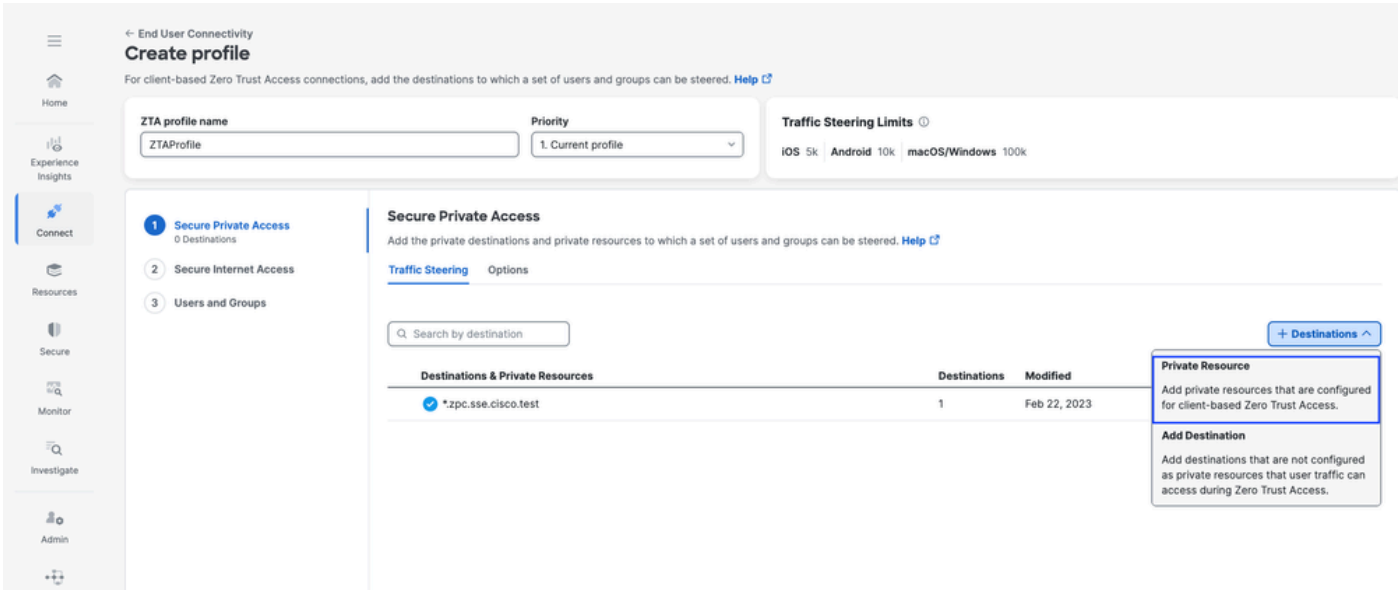
Stap 5 Voeg privé-bronnen toe aan het ZTA-profiel

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

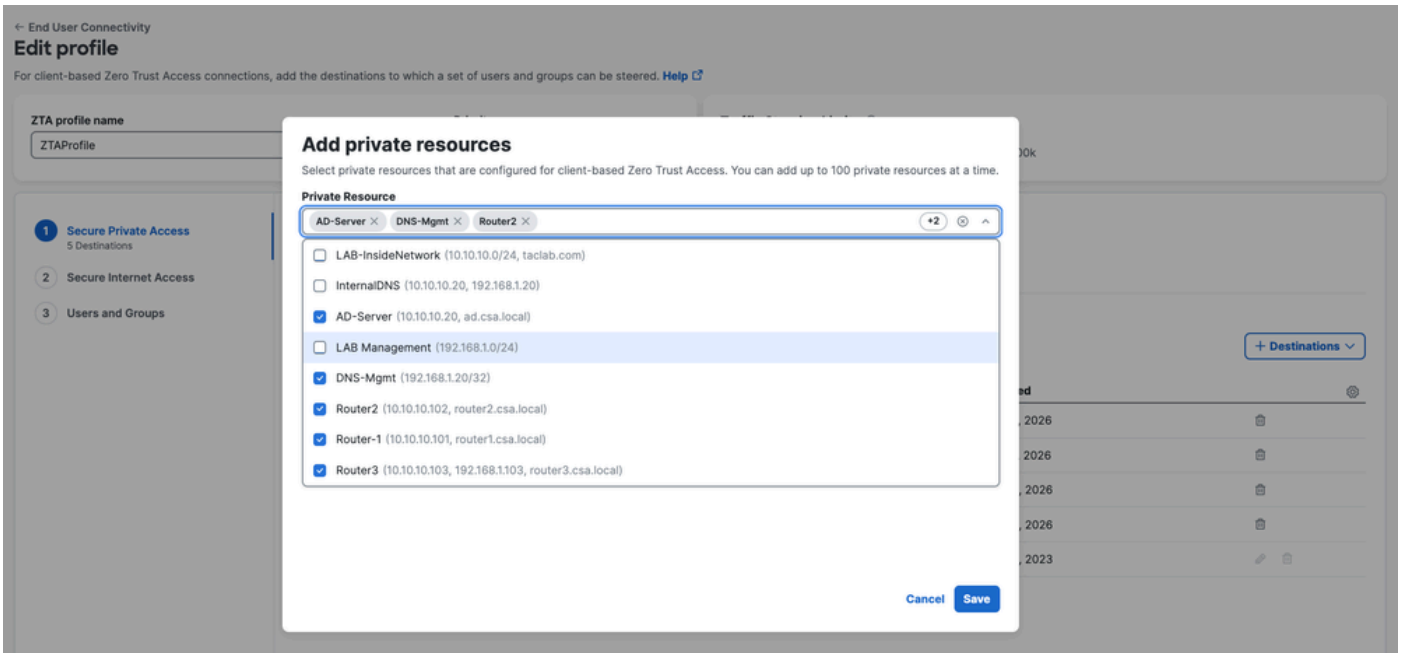


Veilige toegang - ZTA-profiel

2. Voeg de persoonlijke middelen toe

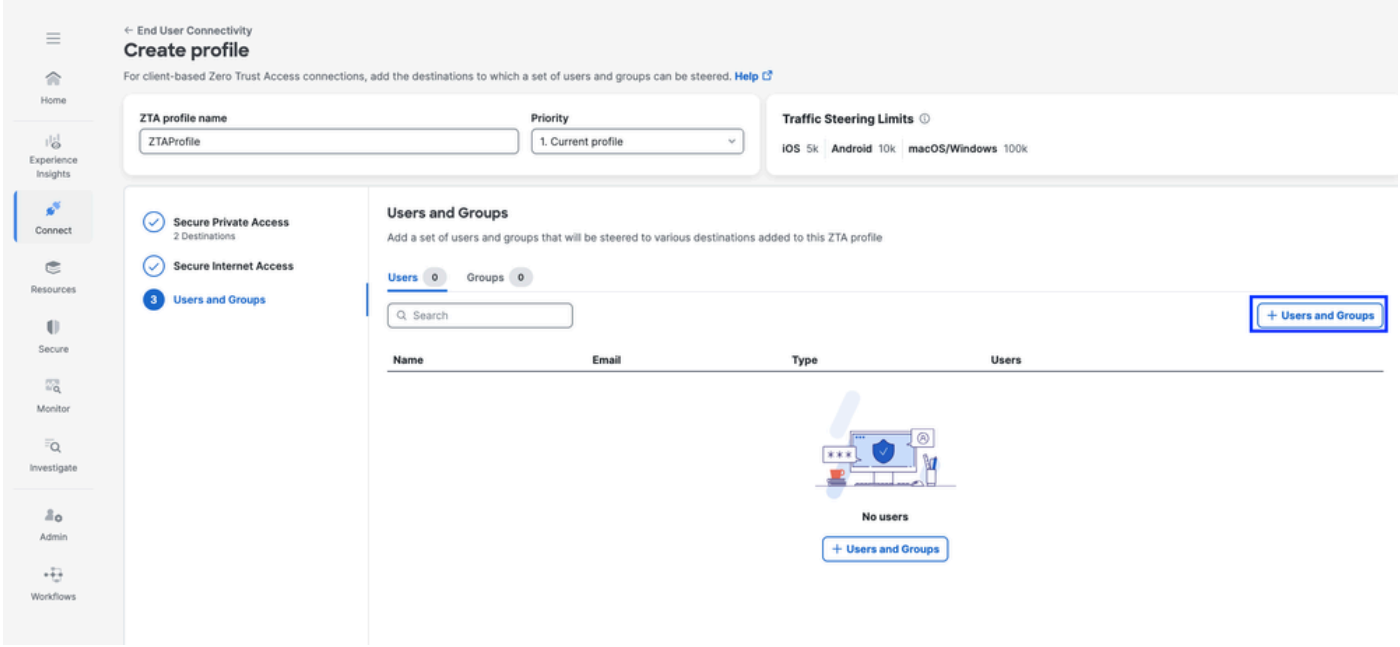


Veilige toegang - ZTA-profiel

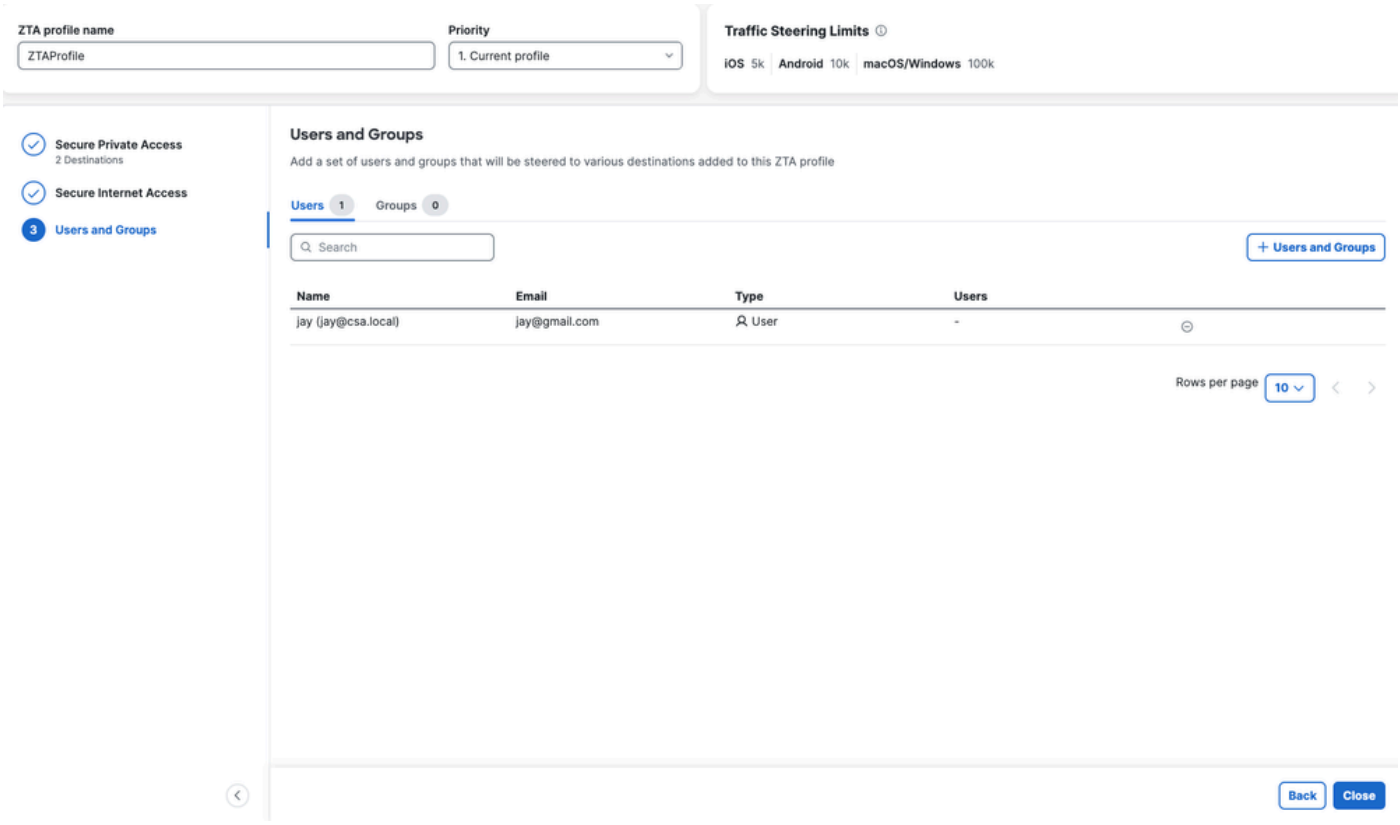


Veilige toegang - ZTA-profiel

3. Gebruikers en groepen toevoegen



Veilige toegang - ZTA-profiel

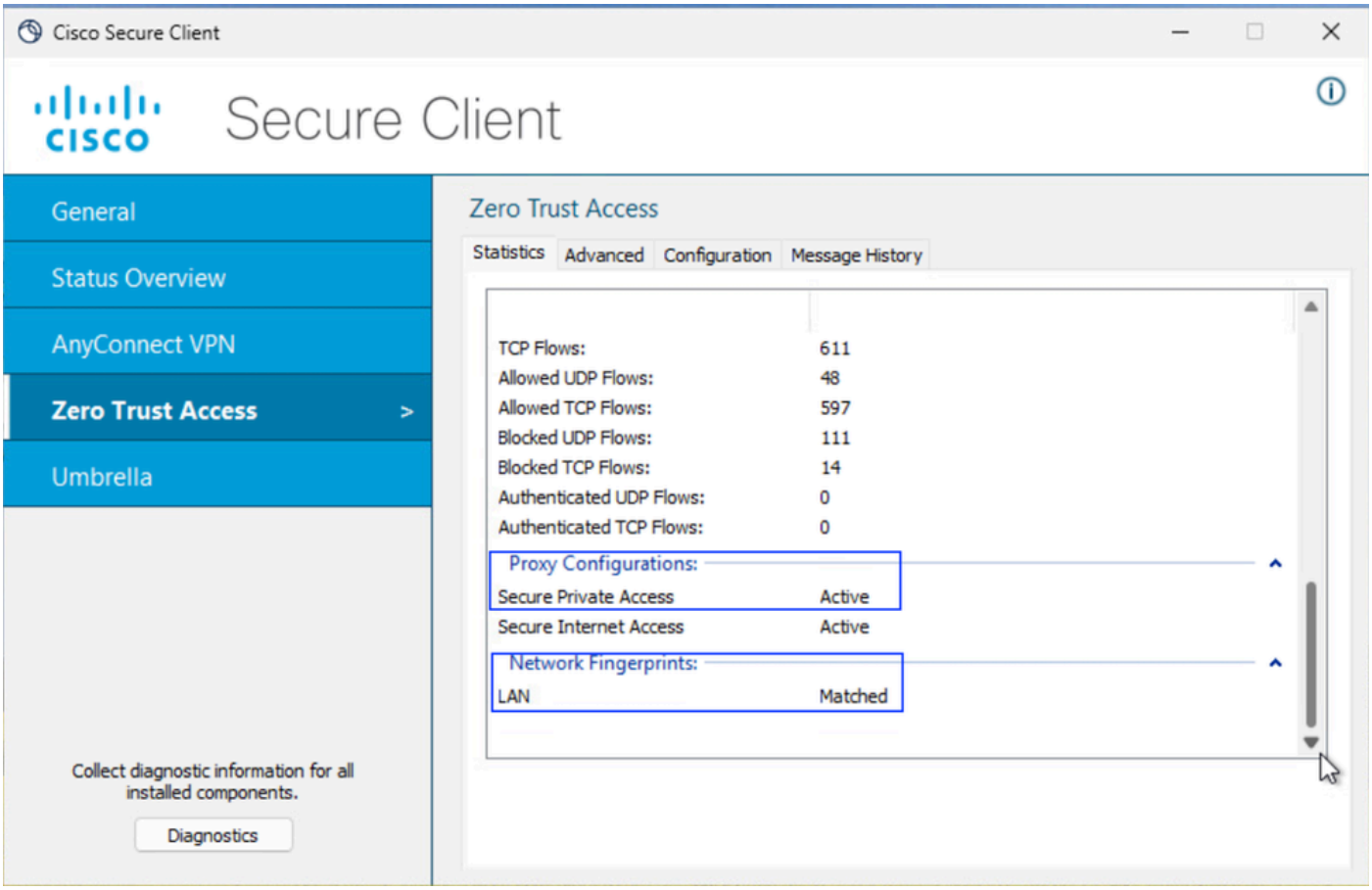


Veilige toegang - ZTA-profiel

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



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

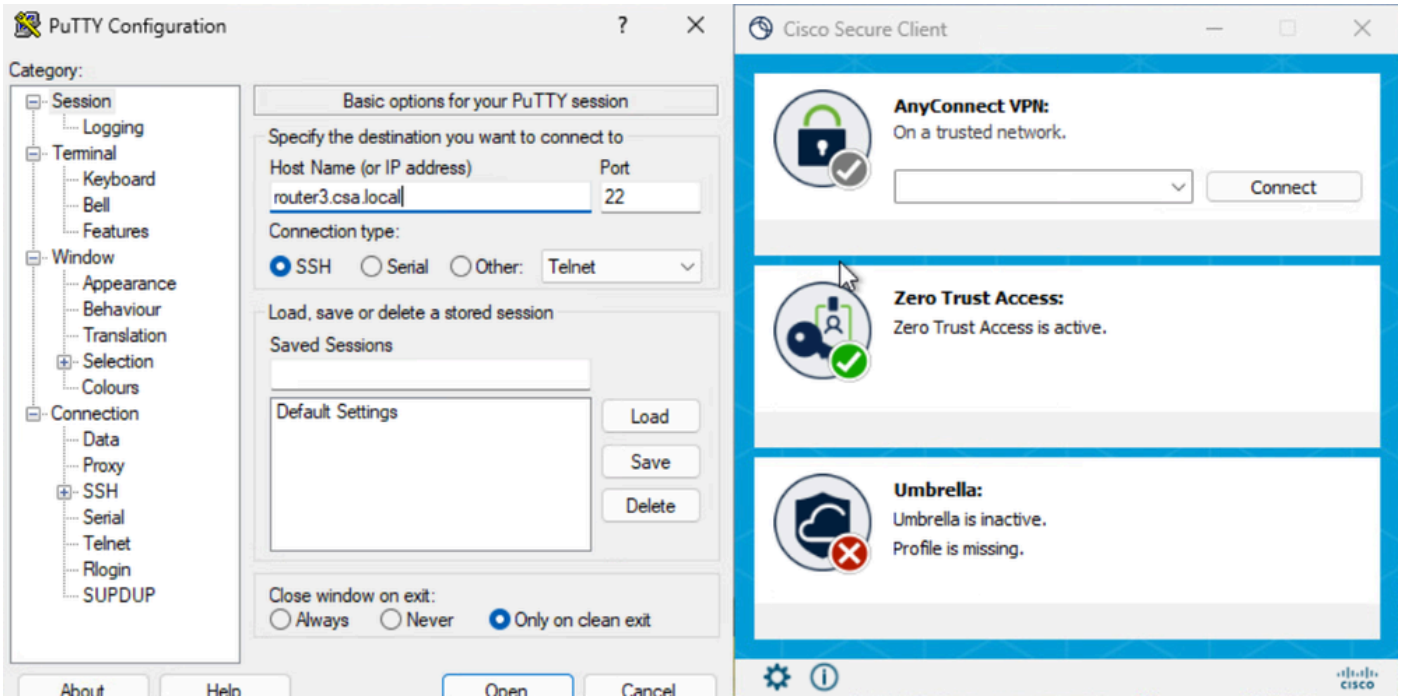
3. Controleren of FTD particuliere bronnen kan bereiken met behulp van FQDN

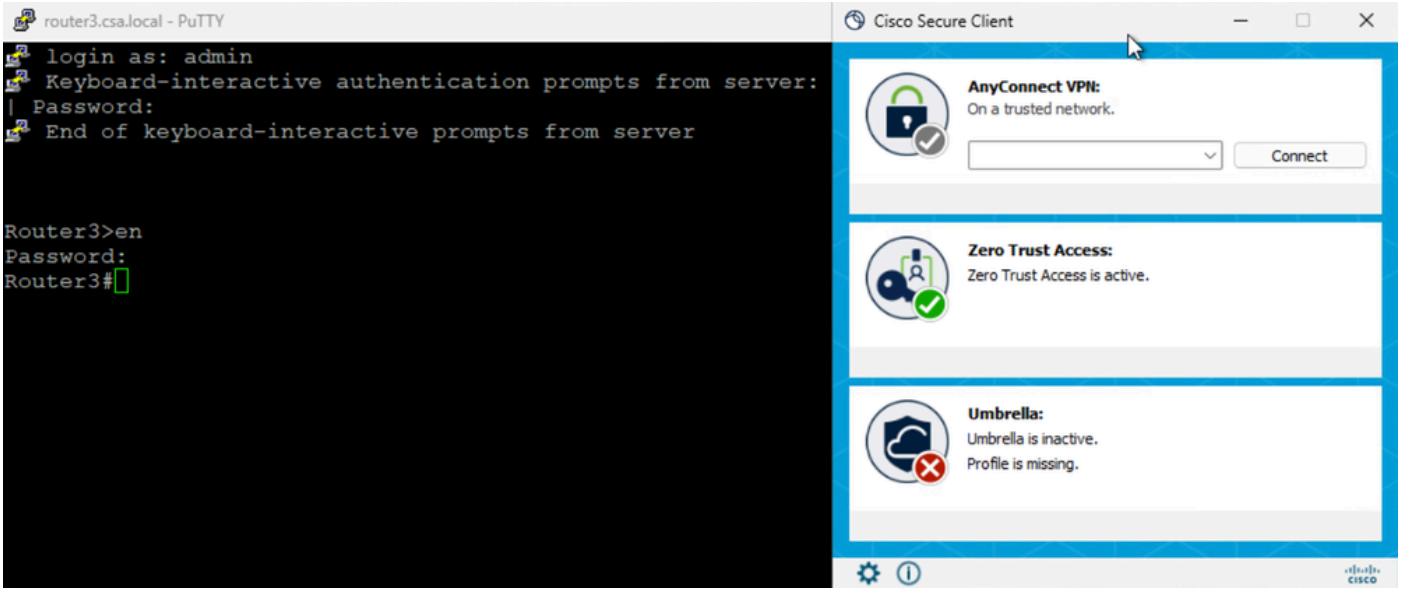
```
ftd# ping router3.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.103, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd#
```

Veilige toegang - PR-testen

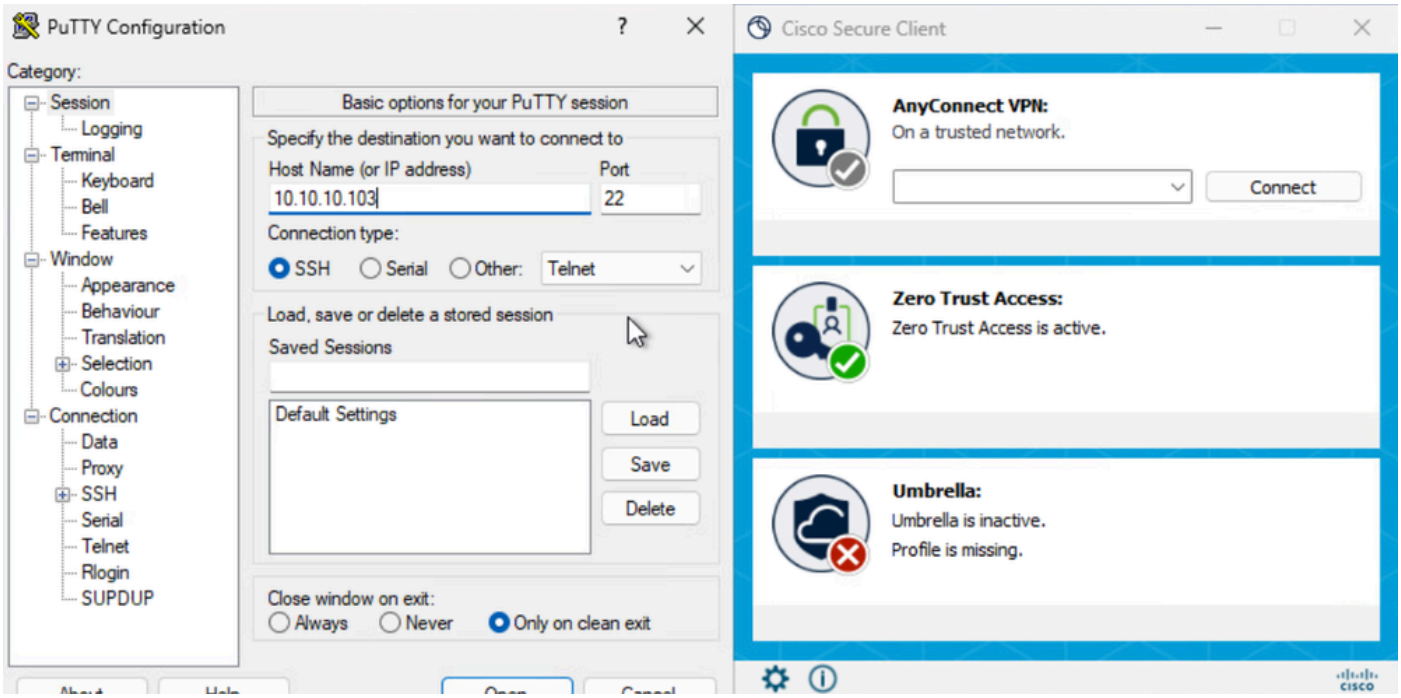
4. Test de SSH-verbinding met de Private Resource

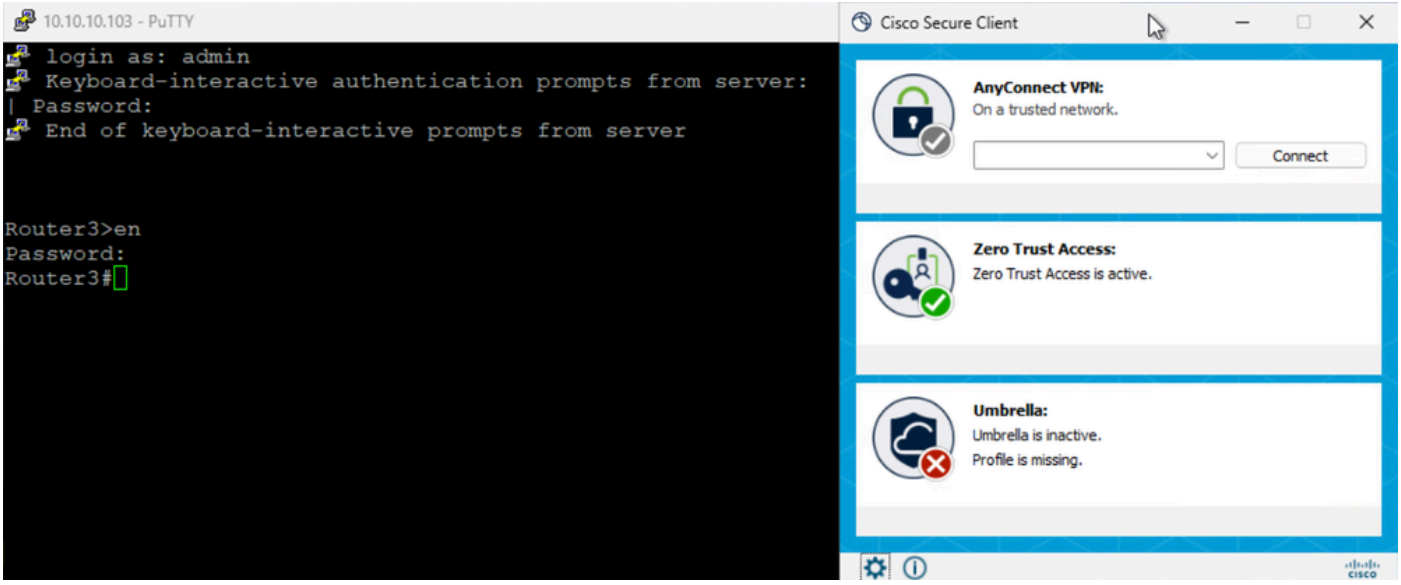
Toegang tot de PR via FQDN



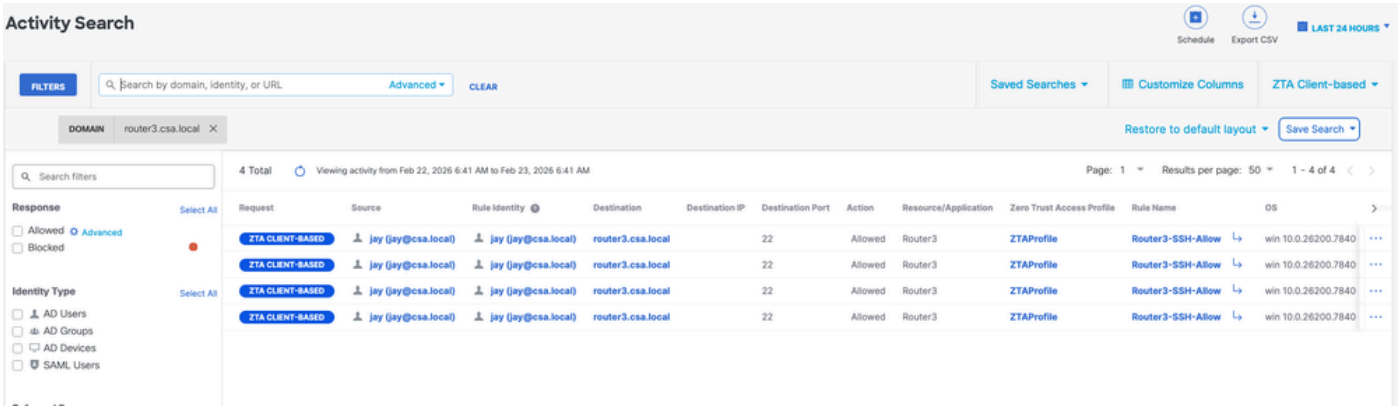


Toegang tot de PR via IP-adres

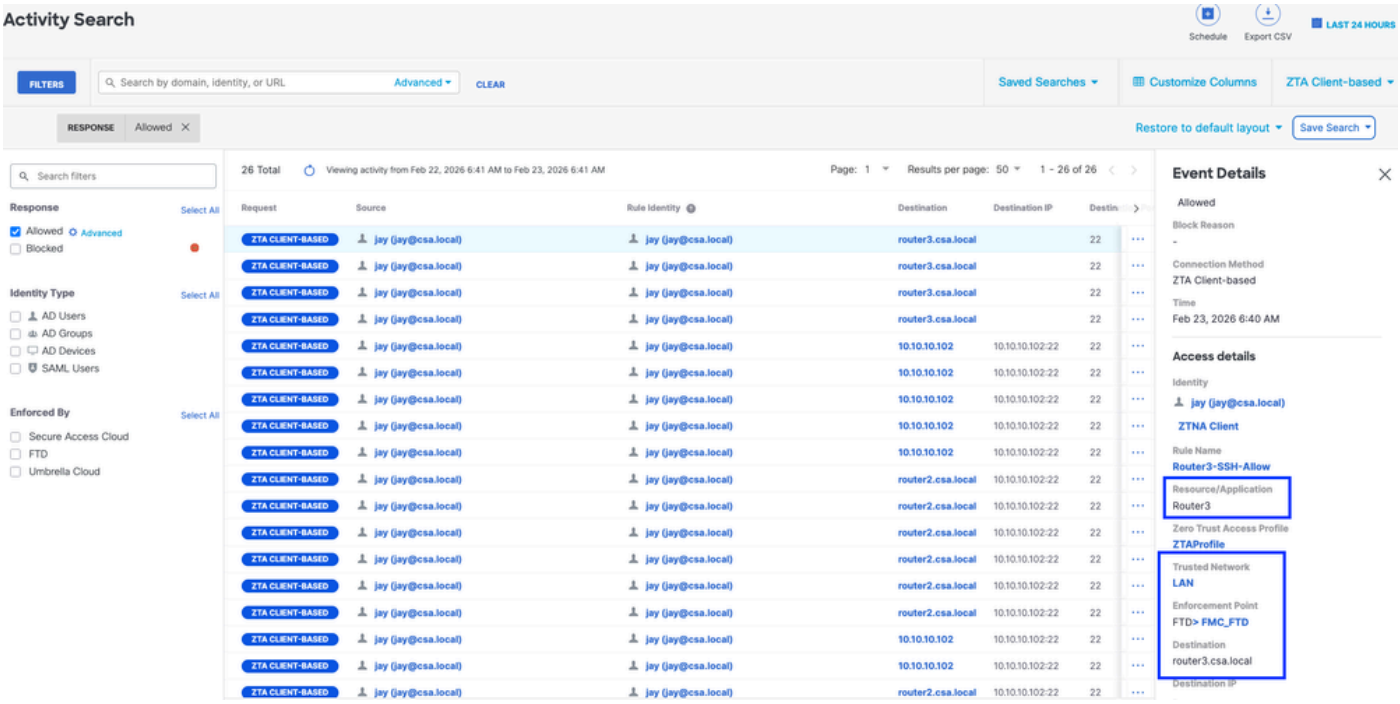




5. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten

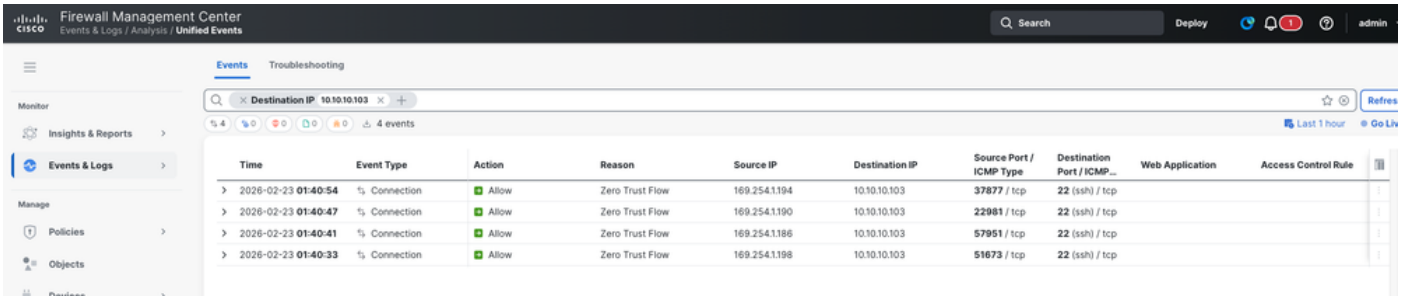


Veilige toegang - zoeken naar activiteiten



Veilige toegang - zoeken naar activiteiten

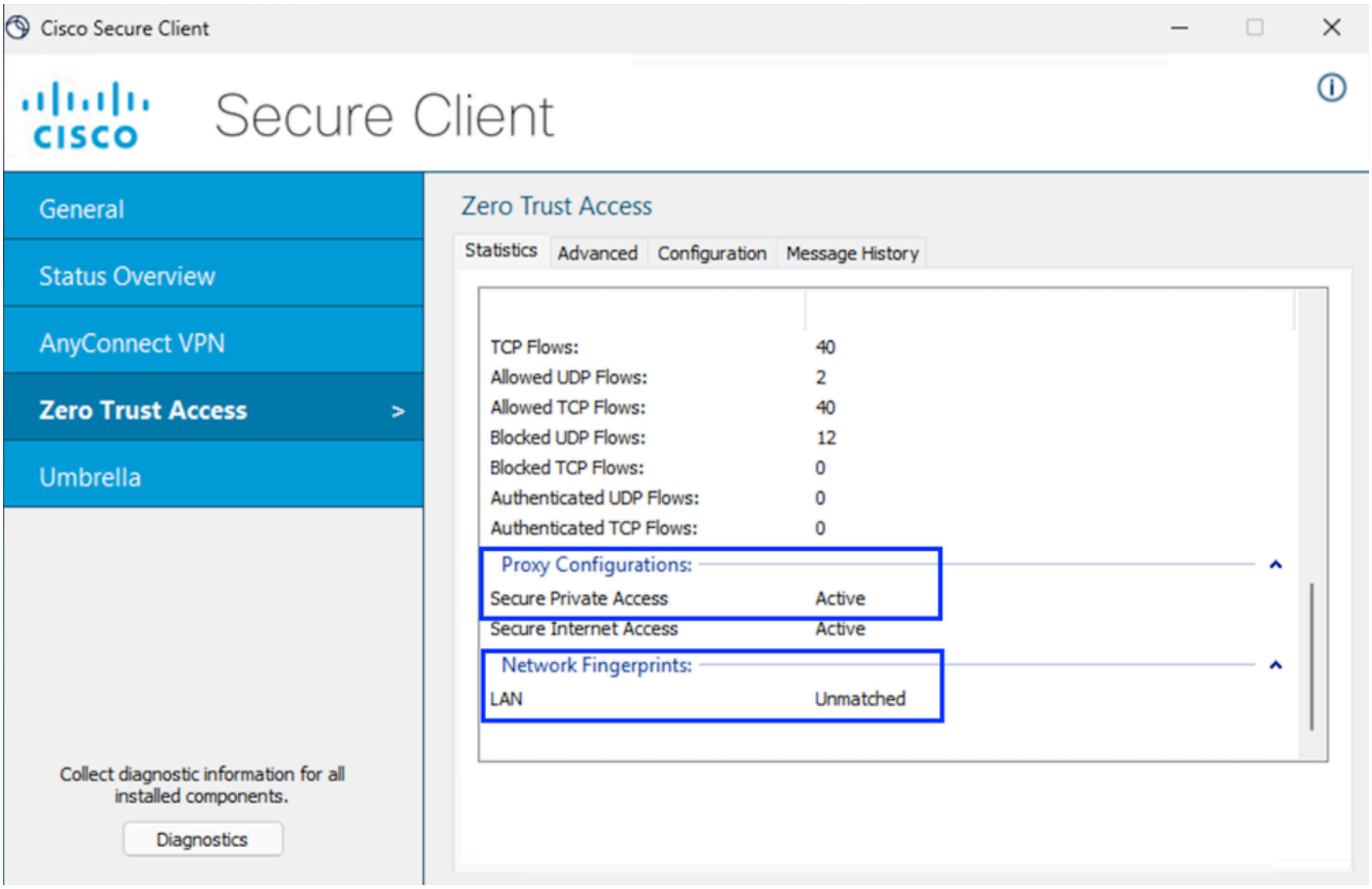
6. FMC-verbindingsgebeurtenissen controleren



FMC-verbindingsgebeurtenissen

Wanneer de gebruiker op afstand is

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

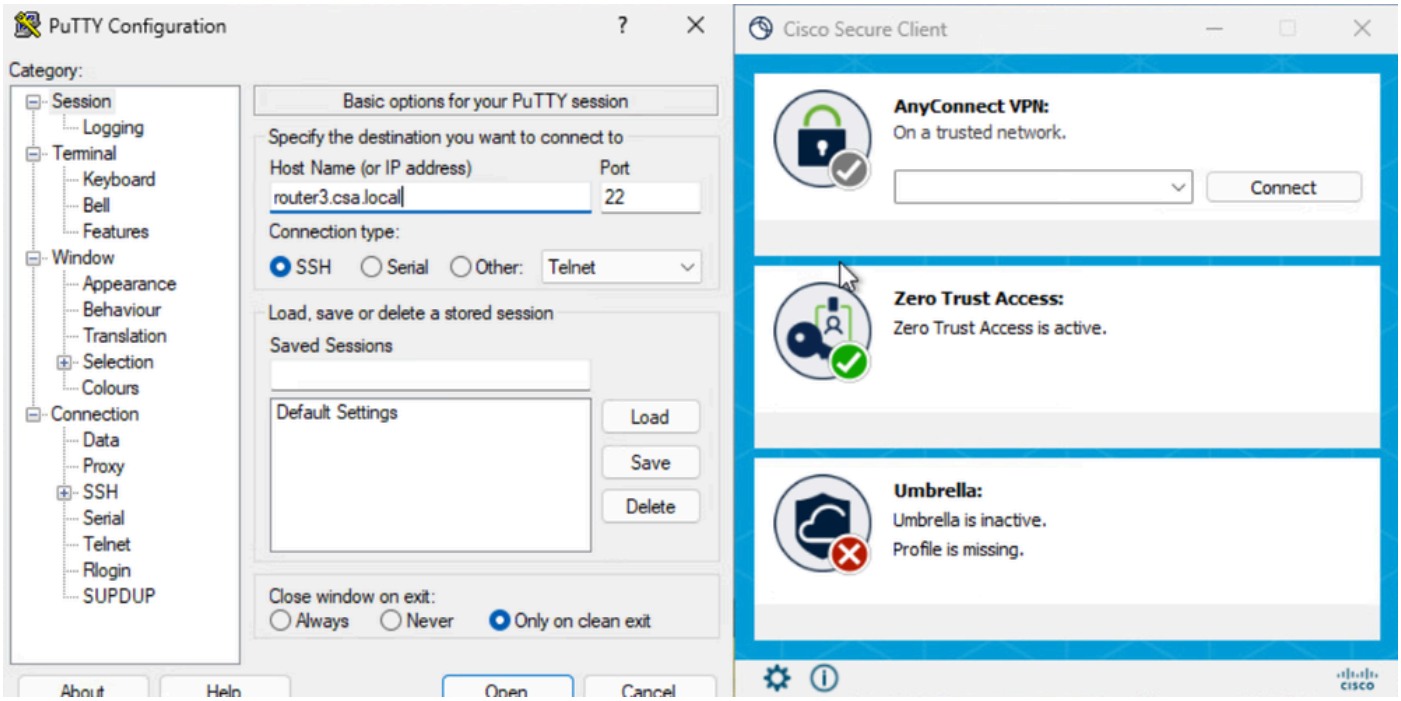


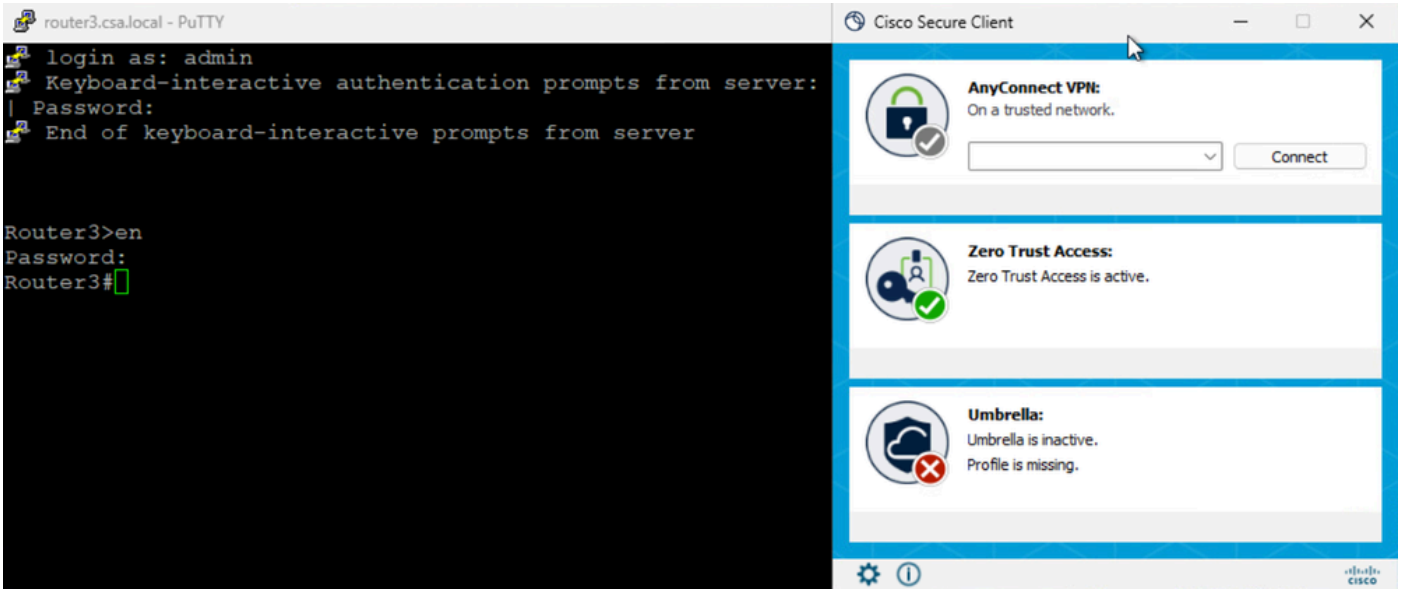
2. Controleer of de externe gebruiker FTD FQDN kan oplossen

```
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
```

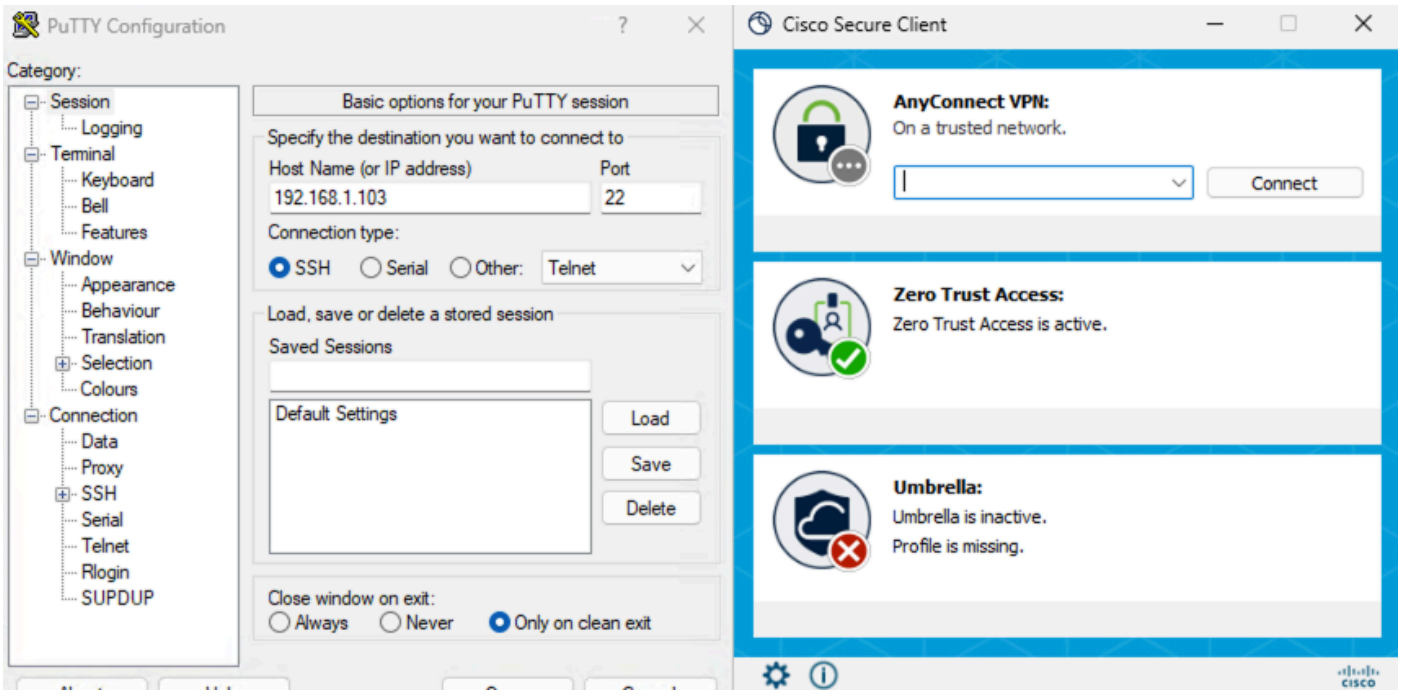

3. Test de SSH-verbinding met de Private Resource

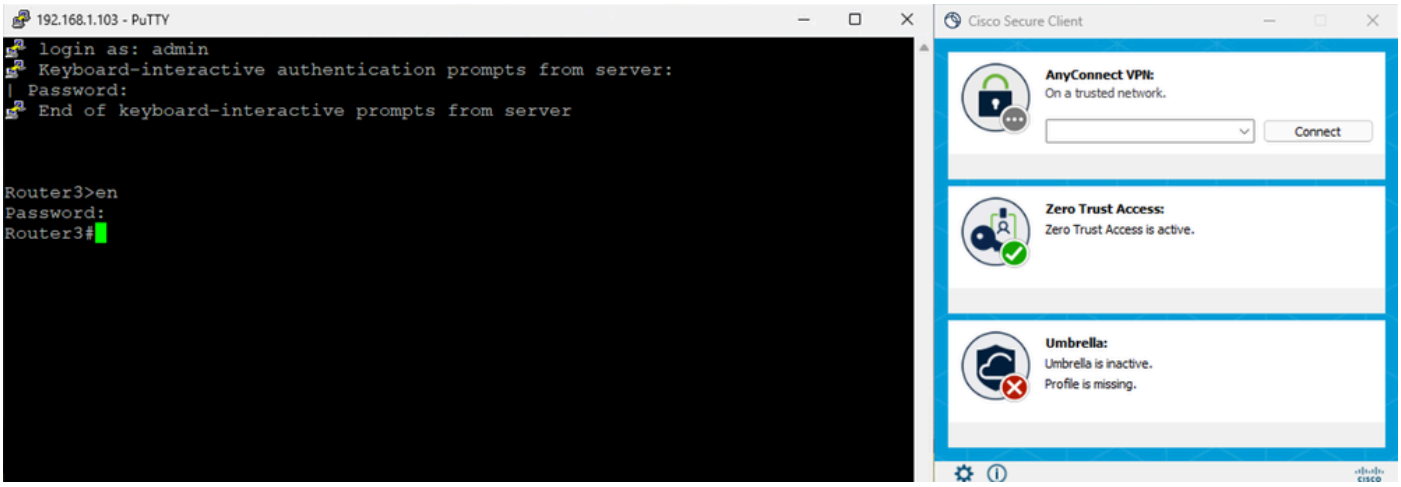
Toegang tot de PR via FQDN





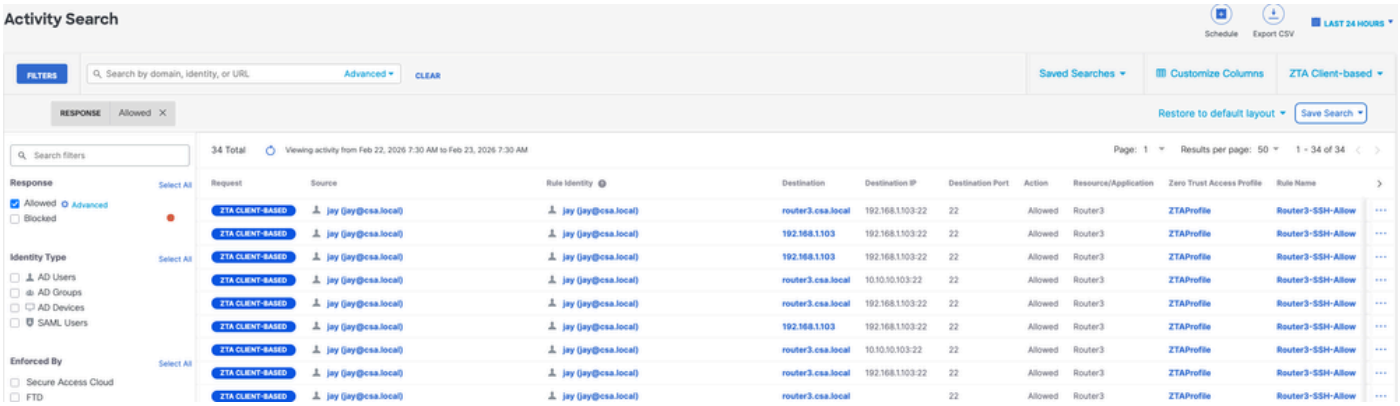
Toegang tot de PR via IP-adres



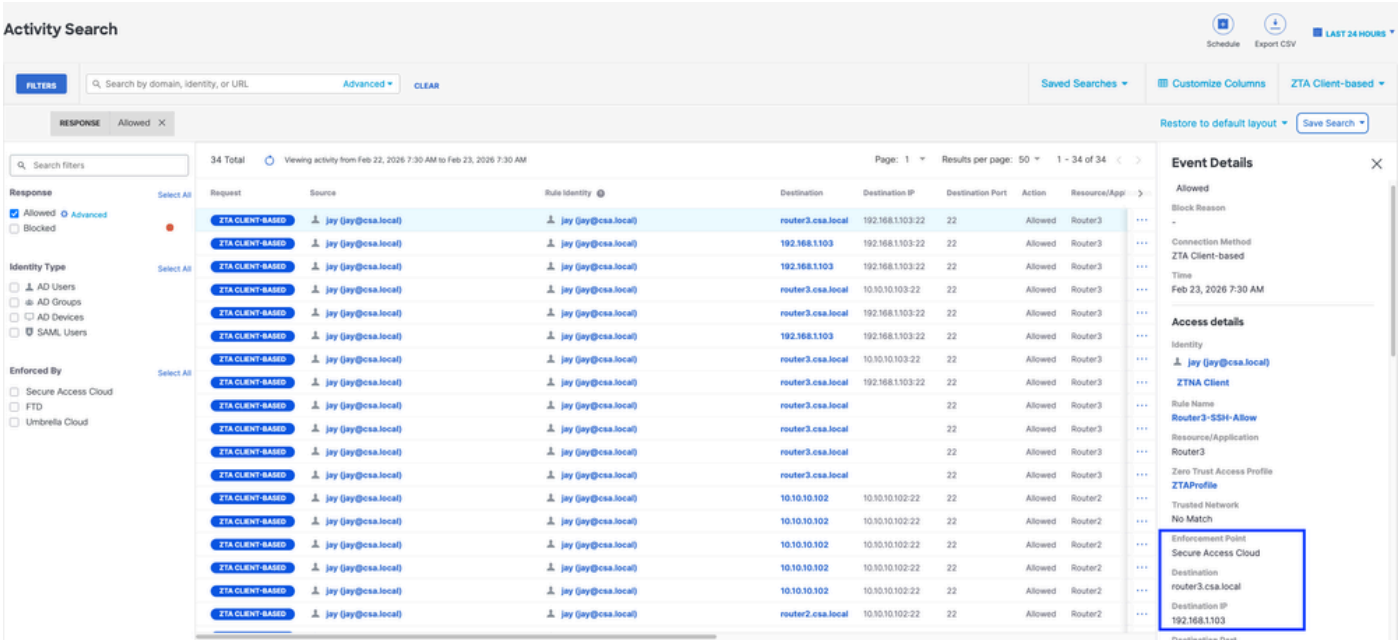


Veilige toegang - PR-testen

5. Verifieer de logboeken voor het zoeken naar beveiligde toegangsactiviteiten



Veilige toegang - zoeken naar activiteiten



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.