Universeller ZTNA für privaten Ressourcenzugriff bei sicherem Zugriff konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration für den Zugriff auf private Ressourcen über eine universelle ZTNA mit unterschiedlichen Datenverkehrspfaden erläutert.

Voraussetzungen

Die folgende Konfiguration muss vor der universellen ZTNA-Konfiguration abgeschlossen werden:

- Identitätsanbieter für sicheren Zugriff mit Cisco
- Registrieren von Geräten bei nicht vertrauenswürdigem Zugriff mithilfe von Zertifikaten
- Konfigurieren von Tunneln mit der Cisco Secure Firewall

- Virtual Private Network mit Remotezugriff
- Ressourcen-Connector für sicheren Zugriff
- FTD-Onboarding für Security Cloud Control
- Hybrid-ZTNA-Feature-Flag sollte für den jeweiligen Secure Access Tenant aktiviert werden. Wenden Sie sich an das Cisco TAC, um das Flag zu aktivieren.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IPsec-VPN-Konfiguration auf Cisco Secure Access und Firewall Threat Defense
- Identity Provide (IdP) - Benutzerbereitstellung über Active Directory
- Remote-VPN-Konfiguration auf Cisco Secure Access
- Bereitstellung von Resource Connectors auf Cisco Secure Access
- ZTA-zertifizierungsbasierte Registrierung
- Zertifikat - OpenSSL , CSR-Generierung , Zertifikatvorlagen usw.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall Threat Defense (Version 7.7.10)
- Cisco Secure FirePOWER Management Center (Version 7.7.10)
- Cisco Secure Client (ZTA Version 5.1.10.1720)
- Windows 11
- Windows 2019 Server - Zertifizierungsstelle
- Ressourcenanschluss auf ESXi

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Über Universal ZTNA

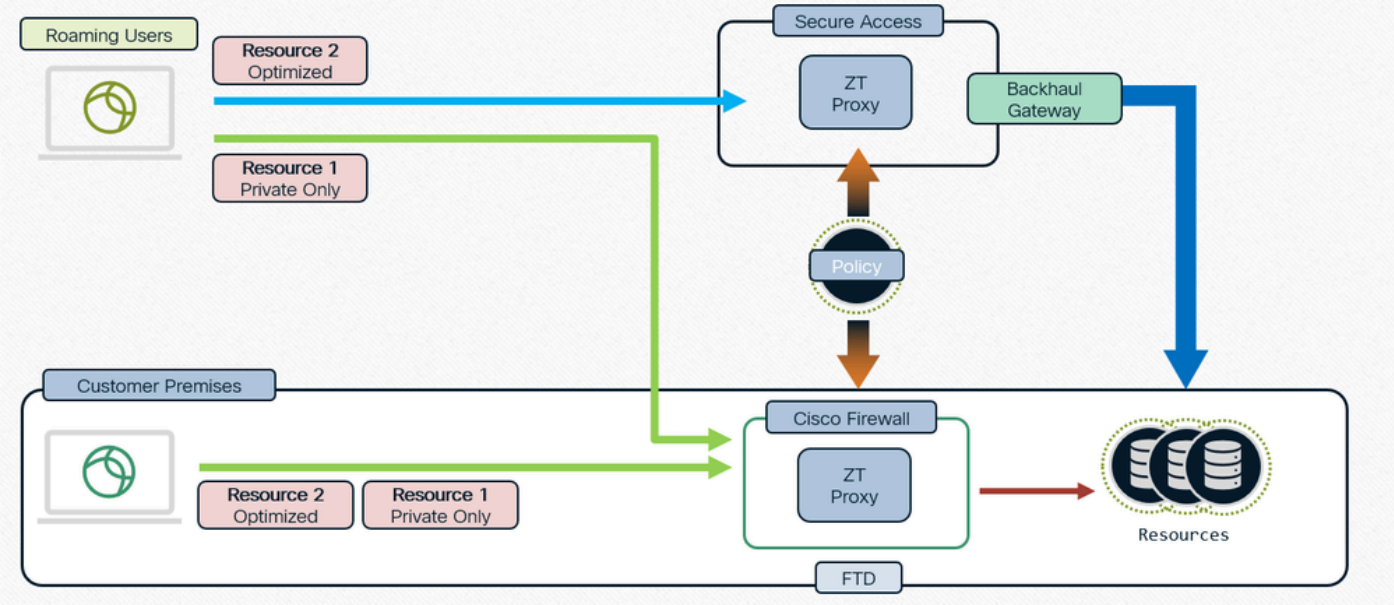
Universeller Zero Trust Network Access (uZTNA) ermöglicht es Administratoren, den Zugriff auf

interne Netzwerkressourcen je nach Benutzeridentität (einschließlich Benutzervertrauen und -status) zu erlauben, ohne den Zugriff auf das gesamte Netzwerk wie bei RA-VPN zu gewähren. uZTNA ermöglicht Administratoren die Sicherung interner Ressourcen und Anwendungen für Remote- und standortbasierte Benutzer.

Da uZTNA nicht davon ausgeht, dass der einer Anwendung gewährte Zugriff den Zugriff auf andere Anwendungen implizit autorisiert, wird die Angriffsfläche im Netzwerk verringert.

Secure Access bewertet die Zugriffsrichtlinie. Alle Zugriffskontrollrichtlinien, die auf Geräten vom Secure Firewall Management Center bereitgestellt werden, werden ignoriert.

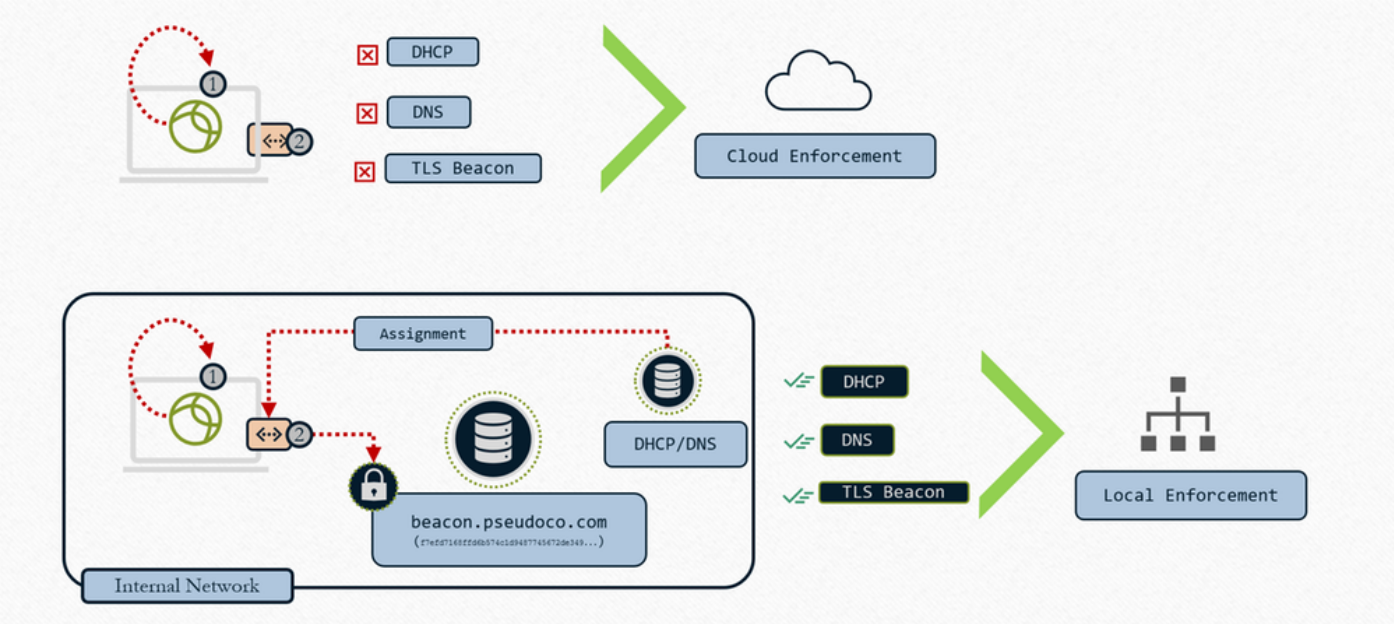
Datenverkehr-Proxys sowie die Durchsetzung von IPS-, Datei- und Malware-Richtlinien werden mit der Firepower Threat Defense (FTD) durchgeführt.



Zentrale Richtlinie, verteilte Durchsetzung

Netzwerkerkennung

Bestimmung der Cloud- oder lokalen Durchsetzung



Universeller ZTNA: Festlegen der Cloud- oder lokalen Durchsetzung

1- Client fragt lokale Schnittstelle zur Netzwerkkonfiguration ab

2- Client sucht nach TLS Beacon

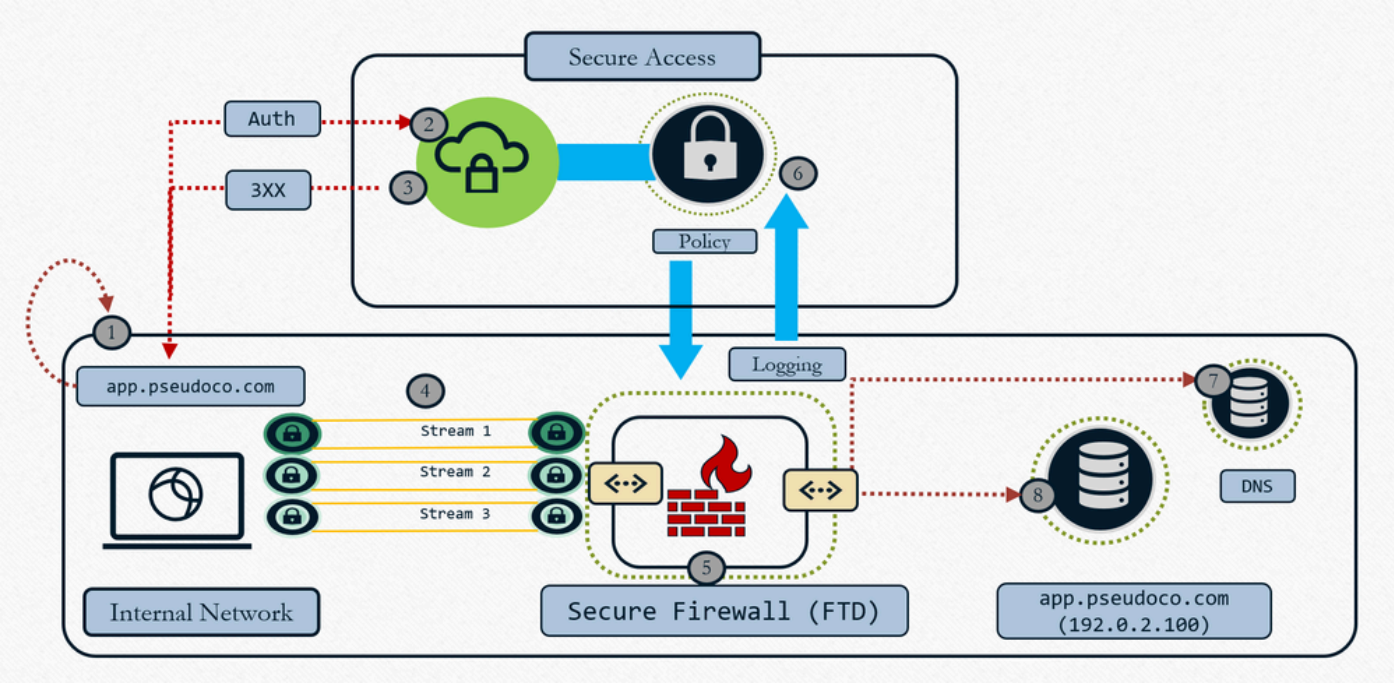
3 - Wenn Bedingung übereinstimmt - Lokale Durchsetzung

4- Wenn Bedingung nicht übereinstimmt - Cloud-Durchsetzung

Wenn wir die Ressource mit "Cloud oder Local Enforcement" konfigurieren und die TND-Regel mit FTD verknüpfen, führt dies tatsächlich dazu, dass der Satz von Abfangregeln, der an den Client gesendet wird, die TND-Regelauswertung beinhaltet. Der Kunde wird von der Cloud angewiesen, die TND-Regel zu evaluieren. Wenn wir die Verbindung senden, geben wir das Ergebnis dieser TND - Netzwerk-Fingerabdruck-Bewertung in den HTTP-Header ein, sodass der Proxy feststellen kann, ob wir uns dauerhaft oder in einem nicht vertrauenswürdigen Netzwerk befinden. Der Proxy verwendet diese Informationen und leitet den Datenverkehr entsprechend um. Wenn der Fingerabdruck übereinstimmt, weist Zproxy den Client an, den Datenverkehr an FTD umzuleiten, und wenn der Fingerabdruck nicht übereinstimmt, leitet er den Datenverkehr an die Cloud um. Weitere Informationen finden Sie unter Konfigurieren des Netzwerkzugriffs ohne Vertrauensstellung mit Erkennung vertrauenswürdiger Netzwerke

Typen für die Durchsetzung

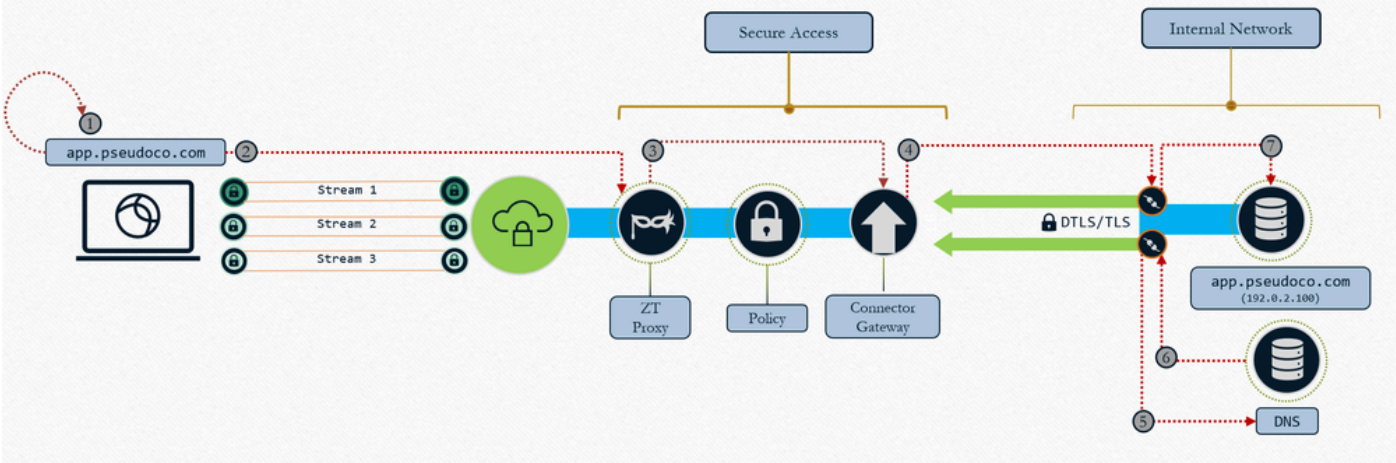
- Lokaler Durchsetzungspfad: Durchsetzung der Firewall



Universeller ZTNA - Lokale Durchsetzung

1. Benutzer fordert Anwendung an, Client erfasst und löst Anforderung an ephemere IP (localhost range) auf
2. Datenverkehr der Authentifizierungssteuerung wird zur Richtlinienauswertung an die Secure Access Cloud gesendet
3. Umleitung der Cloud-Rücksendungen an FTD zur Durchsetzung des Datentarifs (sofern die Richtlinie dies zulässt)
4. Datenverkehr an Firewall-konfiguriertes Headend (Schnittstelle)
5. In der Cloud definierte Richtlinien (IPS, Malware, Entschlüsselung) werden auf lokaler Proxydatenebene durchgesetzt
6. Ereignisprotokollierung und Versand von Duplikaten in die Cloud für konsistente Berichterstellung
7. Firewall führt DNS-Auflösung im lokalen Netzwerk durch, um Ressourcenverkehr weiterzuleiten (falls zulässig)
8. Die Firewall baut die Verbindung zur Ressource auf (neue Verbindung zur Ressource), da sich die Firewall wie ein TCP-Proxy verhält.

- Cloud-Durchsetzung: AUS-Netzwerk

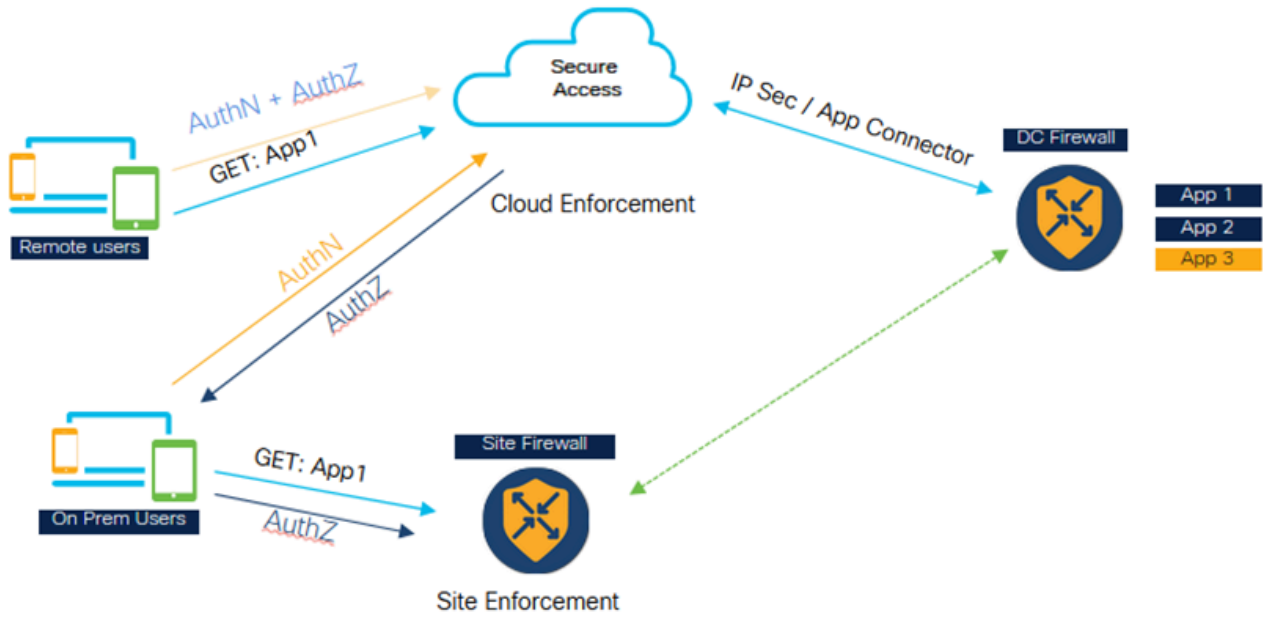


Universelles ZTNA: Durchsetzung der Cloud

1. Benutzer fordert Anwendung an, Client erfasst und löst Anforderung an ephemere IP (localhost range) auf
2. Datenverkehr wird in sicherem Zugriff an Zero Trust Proxy übertragen
3. Die TCP-Verbindung wird über einen Proxy mit dem zugeordneten Ressourcen-Connector hergestellt. Die Richtlinie wird für den Datenverkehr durchgesetzt.
4. Gateway stellt Verbindung zum Ressourcenanschluss her
5. Ressourcen-Connector löst Ressourcen-IP auf
6. Lokaler DNS antwortet mit Ressourcen-IP
7. Ressourcenkonnektor stellt Verbindung mit Ressource her

Anwendungsfälle

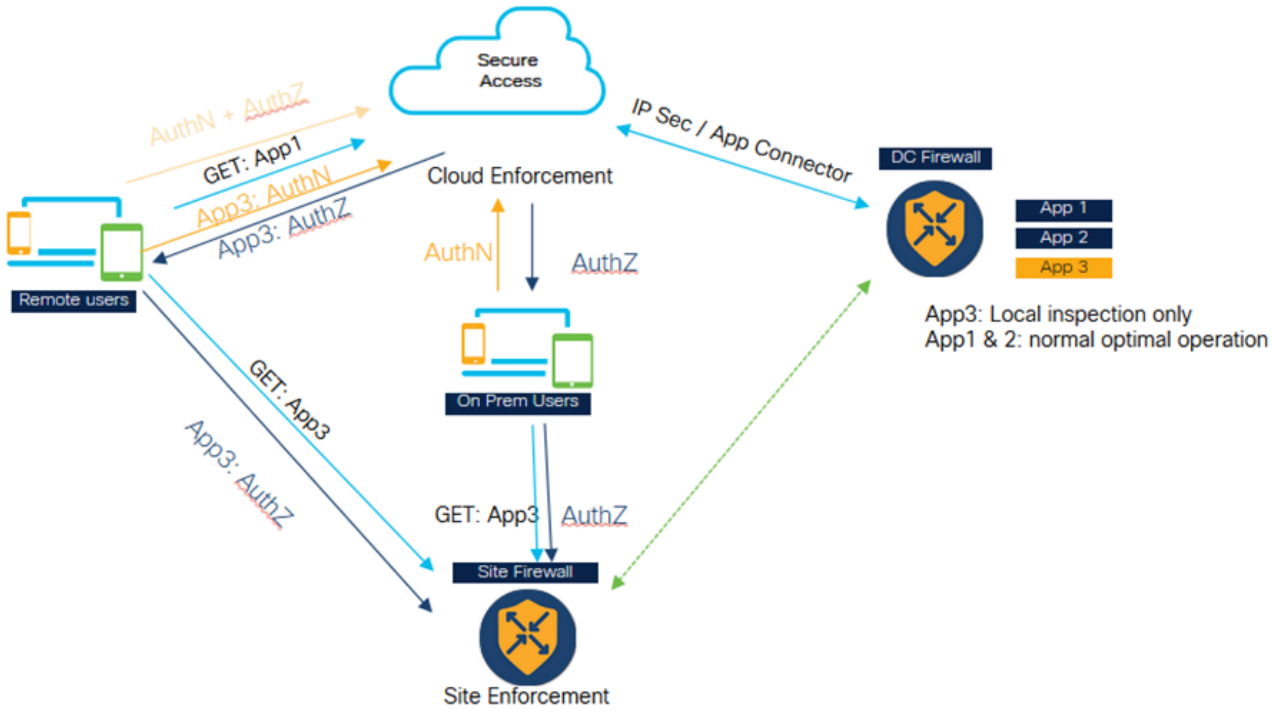
Fall 1: Konsistente und optimierte ZTNA für Benutzer vor Ort



Universal ZTNA - Consistent and Optimized ZTNA (On Premise User)

- Secure Access und Firewall sind beide für den Schutz der Anwendung konfiguriert.
- Wenn es sich um einen Remote-Benutzer handelt, wird dieser zur Richtlinienauswertung und -prüfung zum sicheren Zugriff weitergeleitet.
- Wenn der Benutzer intern/am Standort ist, wird er zur privaten Überprüfung des Datenverkehrs zur Firewall geleitet.
- Benutzer vor Ort können sich weiterhin zur Authentifizierung und Auswertung an Secure wenden, nur der Datenpfad geht zur Firewall und wird entsprechend der Richtlinienkonfiguration überprüft.
- Der interne Benutzer, der über die Firewall auf die Anwendung zugreift, hat einen Leistungsvorteil, da der Datenverkehr nicht in die Cloud und dann per Backhaul in das Rechenzentrum geleitet wird.

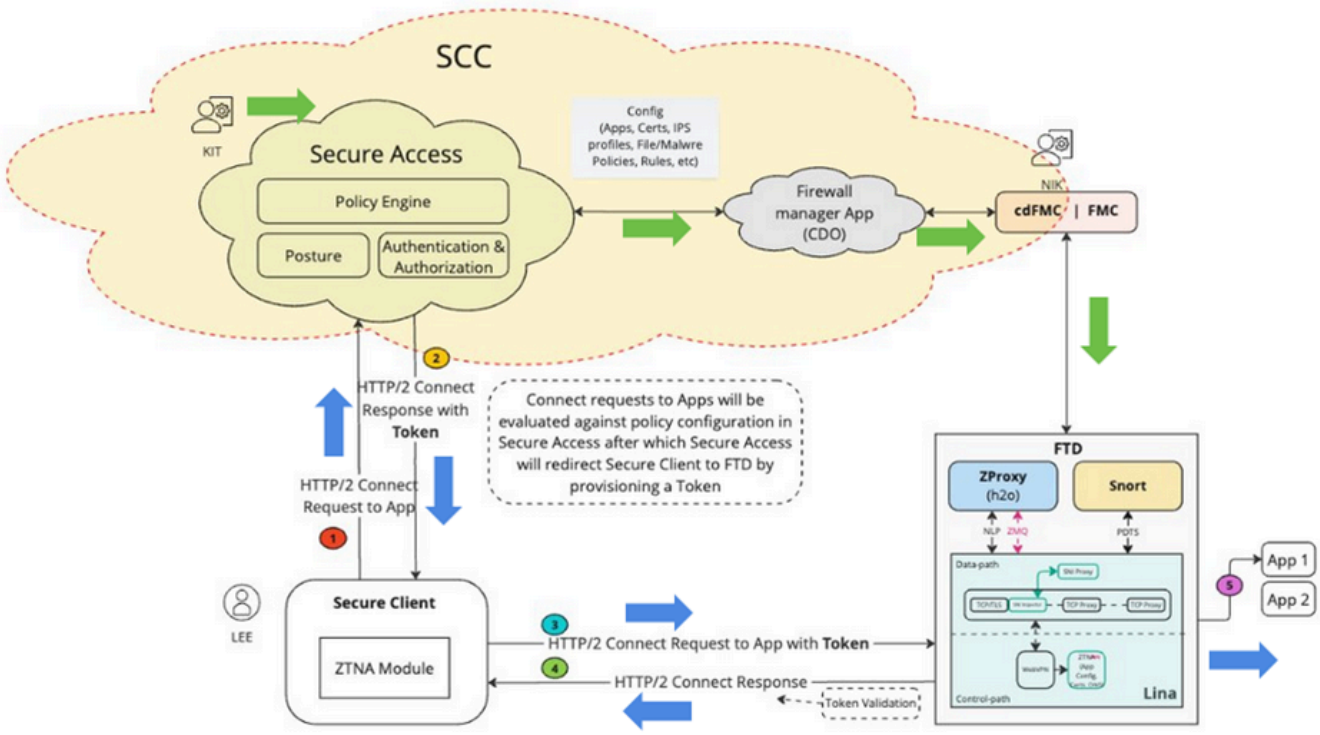
Fall 2: Private Inspektion für sensible Anwendungen



Universal ZTNA - Private Inspection für sensible Anwendungen

- Bestimmte kritische Anwendungen können so konfiguriert werden, dass der Zugriff immer über die Firewall erfolgt.
- Der Anwendungsdatenverkehr muss nicht in die Cloud verlagert werden. Es kann z. B. sensible Datenanwendungen wie Quellcode geben, die der Kunde nicht in die Cloud verlagern möchte.
- In solchen Szenarien durchläuft sowohl der Remote- als auch der permanente Benutzerdatenverkehr immer die Firewall und wird überprüft. In diesem Szenario finden Authentifizierung und Richtlinienauswertung jedoch immer in der Cloud statt, nur der Datenverkehr geht durch die Firewall.

Architekturkomponenten



Universal ZTA - Architekturkomponenten

Security Cloud Control (SCC) ist der primäre Manager für die ZTNA-Lösung. uZTNA ist die erste Funktion, die auf SCC aufbaut.

In SCC gibt es zwei Mikroanwendungen für sicheren Zugriff und Firewall. Nach der Bereitstellung von SCC und der Aktivierung der erforderlichen Feature-Flags werden diese Mikroanwendungen auf der linken Seite des SCC-Panels angezeigt.

Sicherer Client: In Secure Client müssen wir das Zero Trust Access Module (ZTNA) aktivieren, das wir beim ZTNA-Modul registrieren müssen, um auf die Anwendungen zugreifen zu können.

Schutz vor Firewall-Bedrohungen: FTD schützt diese Anwendungen. FTD führt einen ZT-Proxy aus, der auch als H2O bezeichnet wird (ebenso wie der Proxy in Secure Access Cloud).

Wenn ein Benutzer (z. B. ein KIT) eine private Ressource und eine Richtlinie für eine sichere Access-Mikroanwendung konfiguriert, wird diese Konfiguration in SCC an eine Firewall-Mikroanwendung weitergeleitet. Die Firewall-Anwendung versteht die internen Vorgänge der FTD-, FTD-Konfiguration, wie die Konfiguration auf FTD bereitgestellt und verwaltet wird. Die Firewall-App validiert diese Konfiguration und ruft die FMC-APIs auf, um die Konfiguration auf FMC zu übertragen und schließlich auf FTD bereitzustellen. FTD kann eine Option zur automatischen Bereitstellung aktivieren, sodass Administratoren (z. B. Nick) keine manuelle Bereitstellung durchführen müssen.

1. Wenn ein Benutzer (z. B. Lee) versucht, auf eine Anwendung zuzugreifen, stellt ein sicherer Client über den mTLS-Kanal eine Verbindung mit sicherem Zugriff her. Secure Access authentifiziert den Benutzer mithilfe des Zertifikats des Client-Geräts. Anschließend werden die Autorisierung, der Status und andere Richtlinien ausgewertet, die für diesen Benutzer und für diese Anwendung konfiguriert wurden.

2. Sicherer Zugriff: Wenn die Anwendung schließlich von der Firewall geschützt wird, generiert sie ein Authentifizierungstoken , das der Firewall mitteilt, dass diese bereits authentifiziert und autorisiert ist. Das Authentifizierungstoken ist verschlüsselt und von Secure Access signiert.

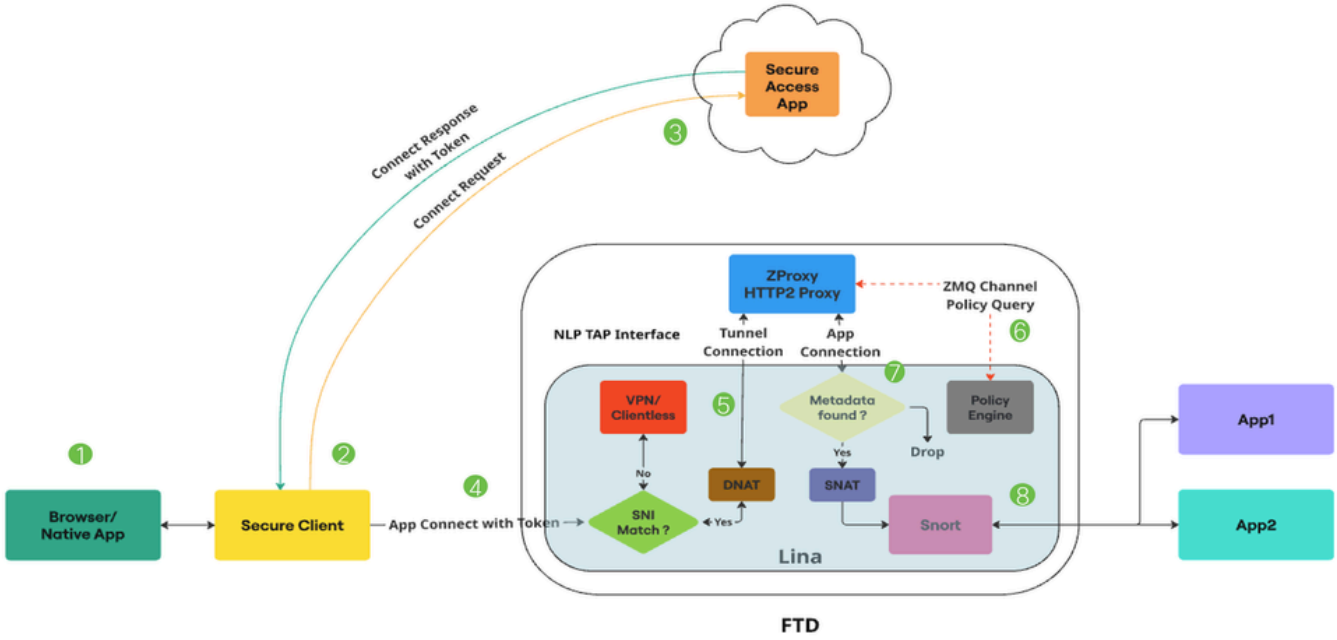
3. Secure Access leitet den Secure Client zusammen mit dem Authentifizierungstoken an FTD weiter.

4. Secure Client stellt eine weitere Verbindung zu FTD her, es handelt sich um eine HTTP2-Verbindung über den mTLS-Kanal. Er sendet eine CONNECT-Anforderung für die Anwendung, auf die zugegriffen wird, zusammen mit dem Token.

5. FTD validiert jetzt das Token. Wenn das Token erfolgreich validiert wird, kann der Benutzer auf die Anwendung zugreifen. FTD sendet die Bestätigung dann zurück an den Secure Client.

Paketfluss

Detaillierter Paketfluss mit Universal ZTNA



1. Der Benutzer versucht, über einen Webbrowser oder eine systemeigene Anwendung auf eine Anwendung zuzugreifen.

2. Der sichere Client fängt die Verbindung ab und identifiziert sie als einen Benutzer, der versucht, auf eine private Ressource zuzugreifen.

3. Der sichere Client stellt eine mTLS-Verbindung mit sicherem Zugriff her und fordert den Zugriff auf die Anwendung an.Der sichere Zugriff überprüft die allgemeinen ZTNA-Richtlinien und Statusprofile auf Konformität.Wenn alles in Ordnung ist, generiert der sichere Zugriff ein Zugriffstoken mit wesentlichen Informationen wie Benutzerdetails, Anwendungsdetails und IPS-/Dateirichtlinie.

4. Das Zugriffstoken wird verschlüsselt und von Secure Access signiert. Secure Access leitet dann den Secure Client zusammen mit dem Token an die FTD weiter.

5. Wenn das Paket den Lina-Datenpfad erreicht, fängt die SNI-Überprüfung die Verbindung ab und überprüft, ob der Servername (SNI-Erweiterung) im Client Hello mit dem auf dem Gerät konfigurierten Proxy-FQDN übereinstimmt.Wenn SNI übereinstimmt, wird die Verbindung an ZProxy weitergeleitet. Wenn SNI nicht übereinstimmt, wird die Verbindung zu anderen Funktionen weitergeleitet, die zusammen mit Universal GNA verwendet werden können.

Beispiele: VPN, Captive Portal oder Clientless ZTNA. ZProxy, das MASQUE über HTTP/2 unterstützt, wird auf dem FTD als Non-Lina-Prozess auf dedizierten Cores ausgeführt. Die Kommunikation zwischen Lina und ZProxy nutzt die NLP Tap Interface, um Datenverkehr zu verarbeiten.Die Ziel-IP der Verbindung wird vom SNI-Prüfer in die TAP-Schnittstellen-IP übersetzt.

6. Wenn der ZProxy die mTLS-Tunnelverbindung vom sicheren Client empfängt, überprüft er das Client-Gerätezertifikat, das vom sicheren Client gesendet wurde. Es verifiziert auch den mit der APP Connect gesendeten Zugriffs-Token. Zwischen Lina und ZProxy gibt es einen Zero-MQ-Kanal. ZProxy verwendet diesen Kanal für die FQDN Auflösung von privaten Ressourcen durch Kommunikation mit Lina.

Der Zero-MQ-Kanal wird auch verwendet, um Informationen, die im Zugriffstoken vorhanden sind, an Lina weiterzugeben. (Beispiel: Regel-ID, Richtlinien-ID usw.) Lina empfängt die Zugriffstoken-Informationen und speichert sie in einer Metadaten-Datenbank.

7. Nachdem die Steuernachrichten ausgetauscht wurden, initiiert ZProxy eine neue Verbindung zur privaten Ressource. Dies kann TCP oder UDP sein. Lina führt dann eine Metadaten-Datenbanksuche für diese App-Verbindung durch. Wenn die Metadaten nicht gefunden werden, wird die Verbindung gelöscht.

8. Da die App-Verbindung vom ZProxy stammt, hat sie eine interne IP (Beispiel:169.251.1.2) als

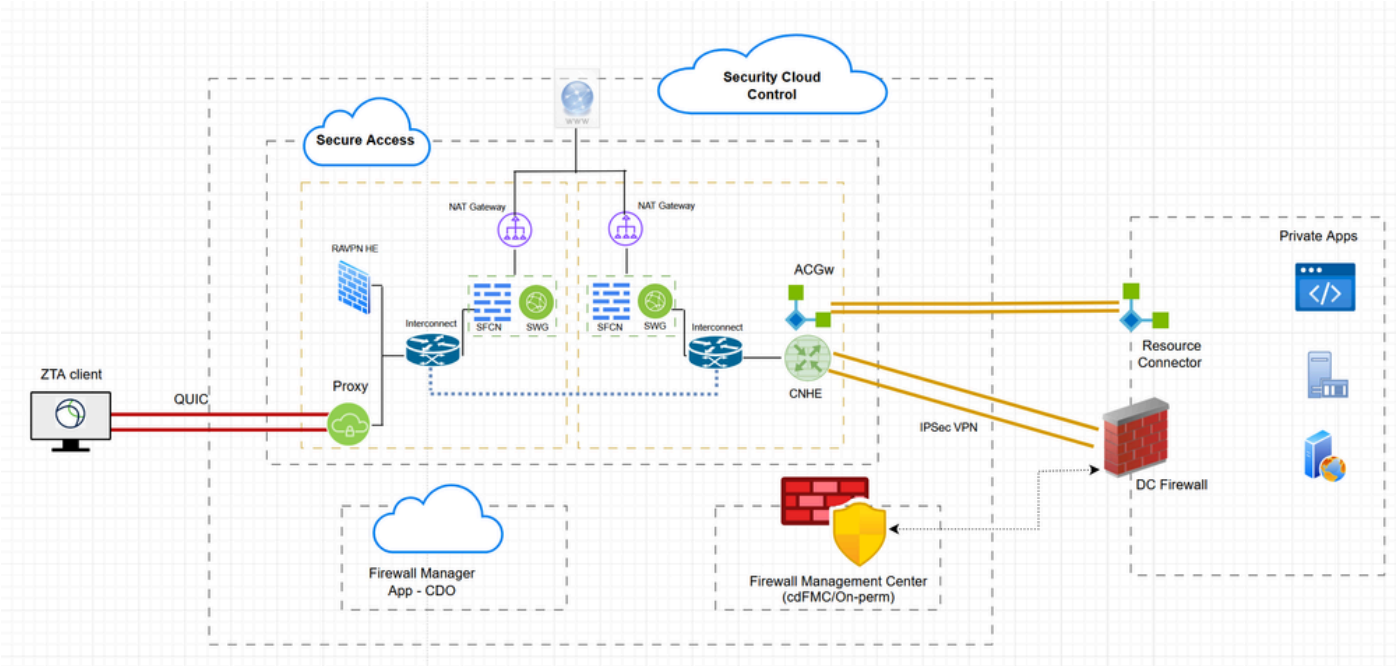
Quell-IP. Dies wird in die FTD-Ausgangsschnittstellen-IP übersetzt, bevor es versendet wird. Lina markiert Universal Zero Trust-Flows nur dann für die Snort-Prüfung, wenn im Zugriffstoken eine Datei- oder IPS-Richtlinie vorhanden ist.Die vom Zugriffstoken erhaltene Regel-ID wird in den Verbindungsmetadaten an Snort übergeben.

9. Universelle Zero Trust-Regeln und die entsprechenden Datei- und IPS-Richtlinienzuordnungen werden über das FMC an die FTD übermittelt. Das Zero Trust-Plug-In in Snort lädt diese Regeln während der Initialisierung.Lina markiert die Universal Zero Trust-Streams nur dann für die Snort-Prüfung, wenn im Zugriffstoken von Secure Access eine Datei- oder IPS-Richtlinie für den Zugriff auf diese private Ressource angegeben ist.

Die Regel-ID, die vom Zugriffstoken abgerufen wird, wird über Conn Meta an Snort übergeben. Für alle Streams mit Universeller Zero Trust führt das Plug-In Zero Trust in Snort eine Regelsuche für die Regel-ID durch, die vom Conn Meta abgerufen wird. Wenn eine Regelübereinstimmung gefunden wird, wird der Fluss zugelassen, und die spezifischen IPS- und Dateirichtlinien werden auf den Fluss angewendet. Wenn keine Regelübereinstimmung gefunden wird, wird das Plug-In Zero Trust Snort blockiert den Datenfluss.

Konfigurieren

Netzwerkdiagramm

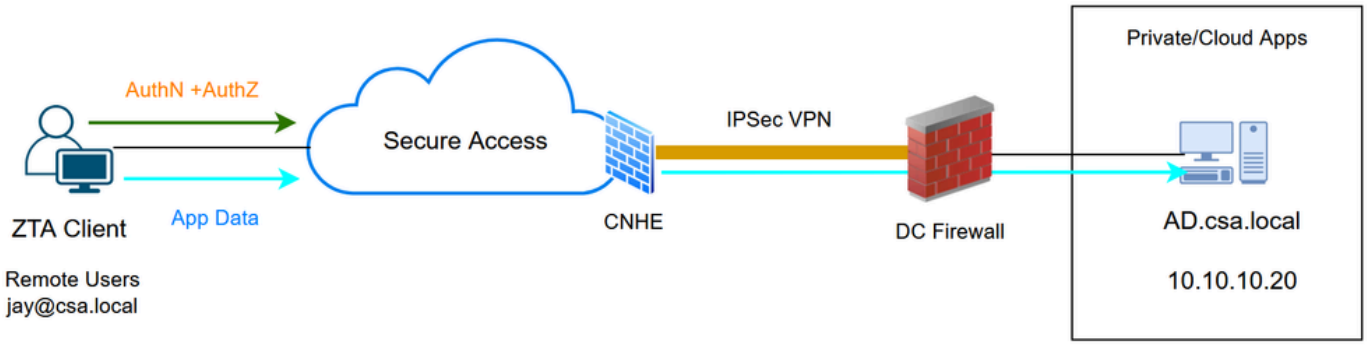


Hybrid-ZTNA - Netzwerkdiagramm

Testfälle

Testfall 1: Remote-Benutzer - Cloud-Durchsetzung

In diesem Testfall greifen wir per Cloud-Durchsetzung über die Netzwerk-Tunnelgruppe auf eine private Ressource zu. In diesem Fall werden sowohl die Richtlinienauswertung als auch die Anwendungsdaten von Secure Access über das ZTA-Modul abgefangen. Hierbei handelt es sich um einen herkömmlichen Datenstrom, bei dem der Zugriff auf eine private Anwendung über die Network Tunnel Group oder den Resource Connector vom registrierten ZTA-Client aus möglich ist.

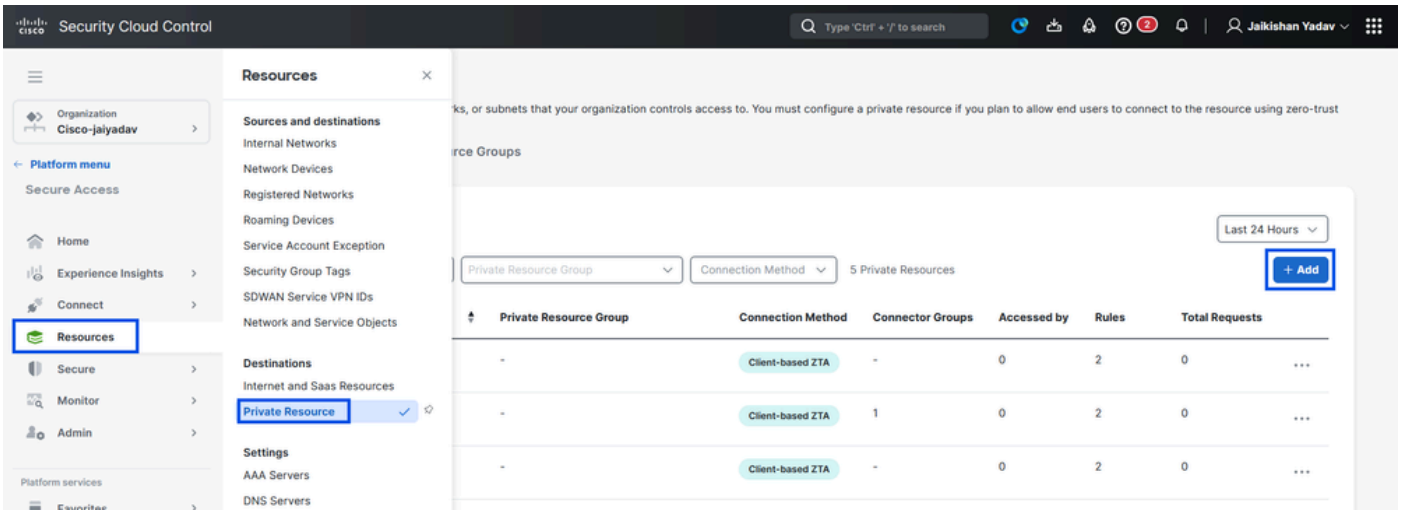


Universal ZTA - Testfall-Topologie

Schritt 1 - Definieren einer privaten Ressource für sicheren Zugriff

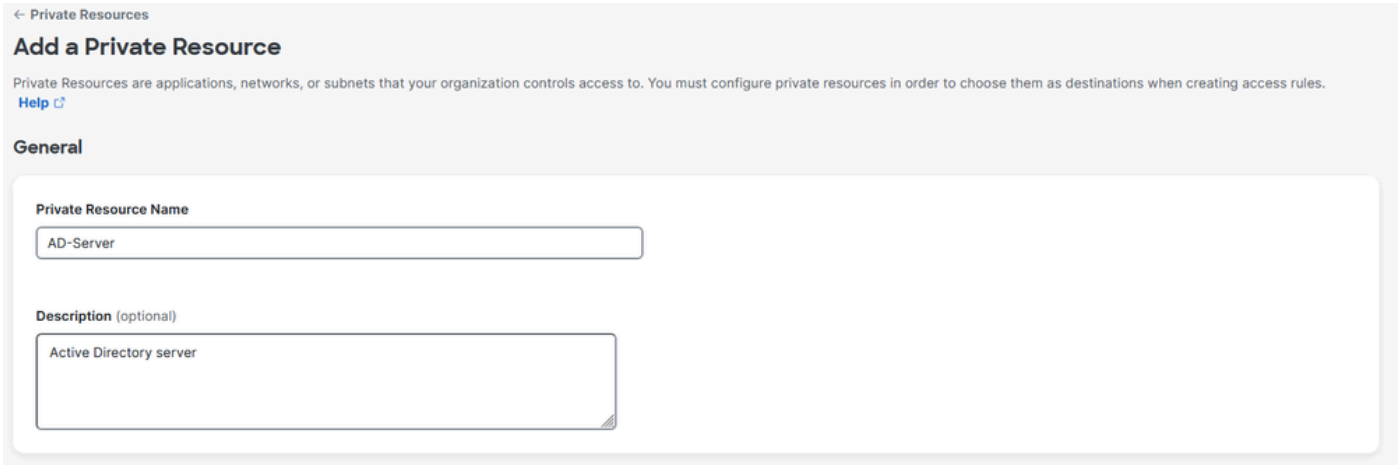
Konfigurieren einer privaten Ressource für den Zugriff über ein bei Zero Trust Access (ZTA) angemeldetes Gerät mit Cloud-Durchsetzung

1. Navigieren Sie zu Ressourcen > Ziele > Private Ressourcen > und klicken Sie auf +Hinzufügen.



Sicherer Zugriff - Konfiguration privater Ressourcen

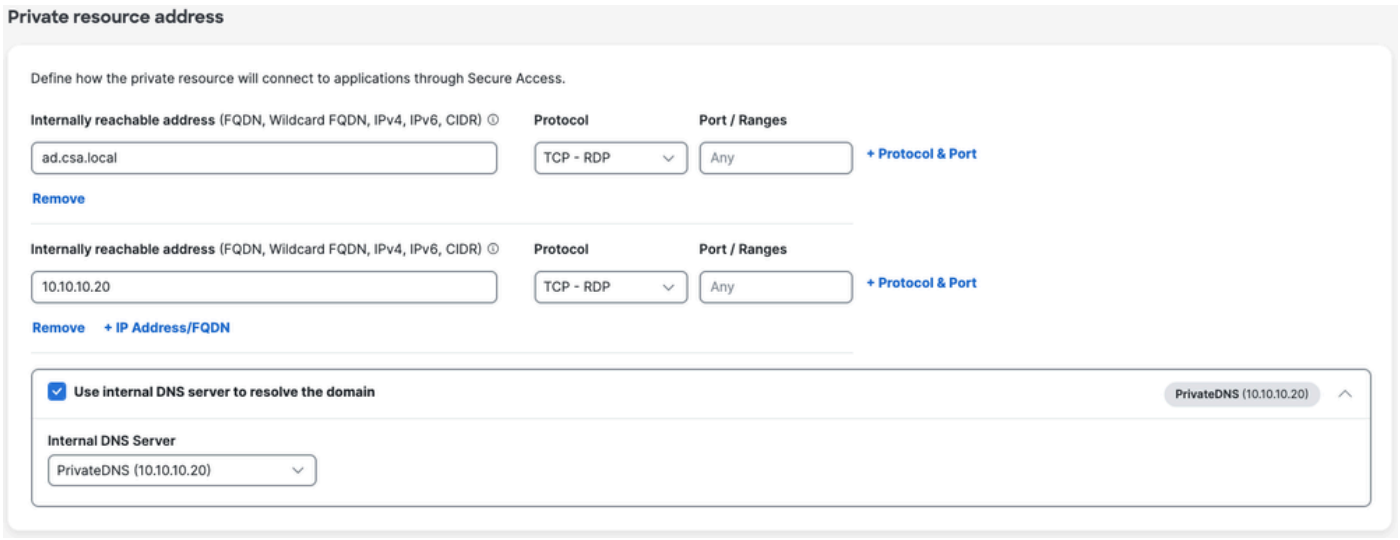
2. Geben Sie für Private Resource Name einen sinnvollen Namen für die Ressource ein. Für Description empfehlen wir, Informationen wie den Zweck der Ressource oder den Namen des Ressourcenbesitzers anzugeben.



Sicherer Zugriff - Konfiguration privater Ressourcen

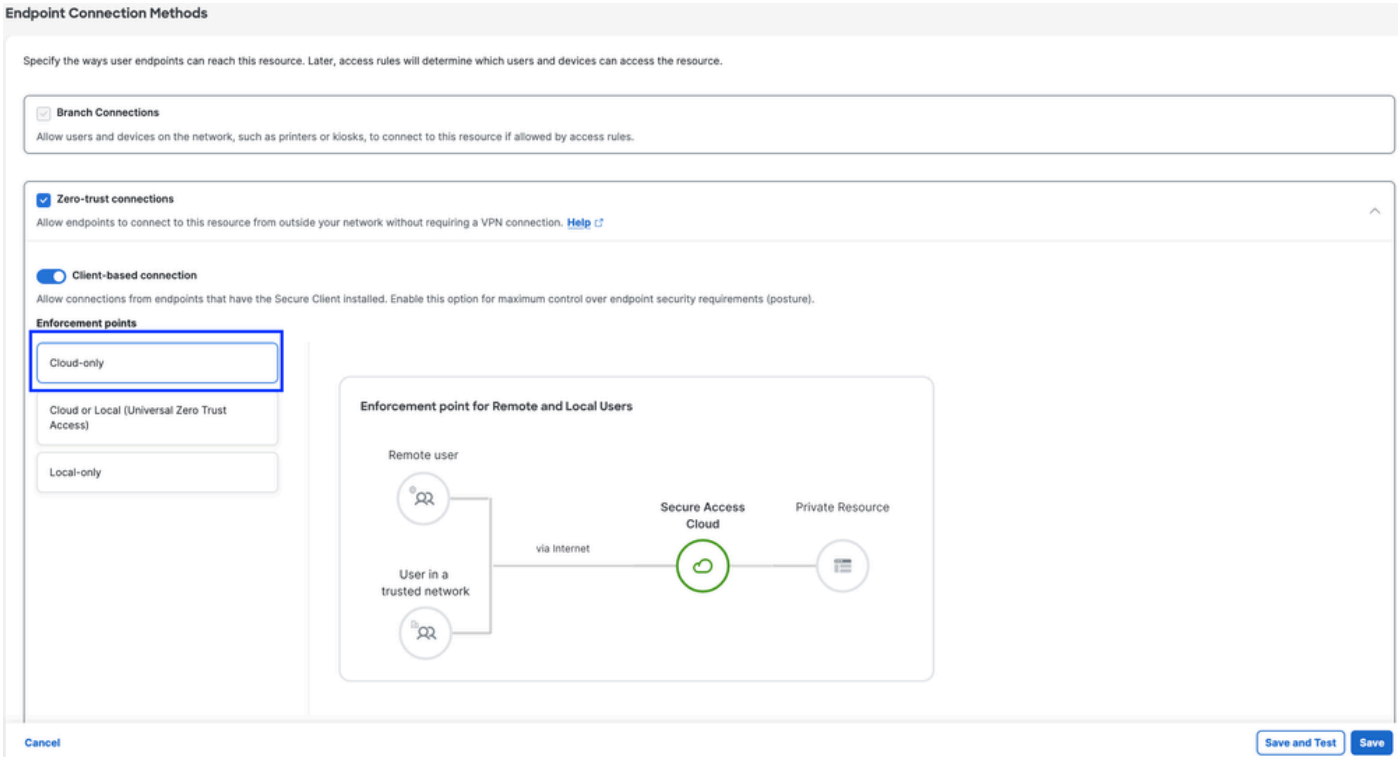
3. Geben Sie den FQDN der privaten Ressource ein, auf die Sie zugreifen möchten. Wir können auch die IP-Adresse der privaten Ressource definieren. Weitere Informationen finden Sie unter Hinzufügen einer privaten Ressource

4. Wählen Sie den internen DNS-Server, um die Domäne aufzulösen.



Sicherer Zugriff - Konfiguration privater Ressourcen

5. Endpunktverbindungsmethoden auswählen



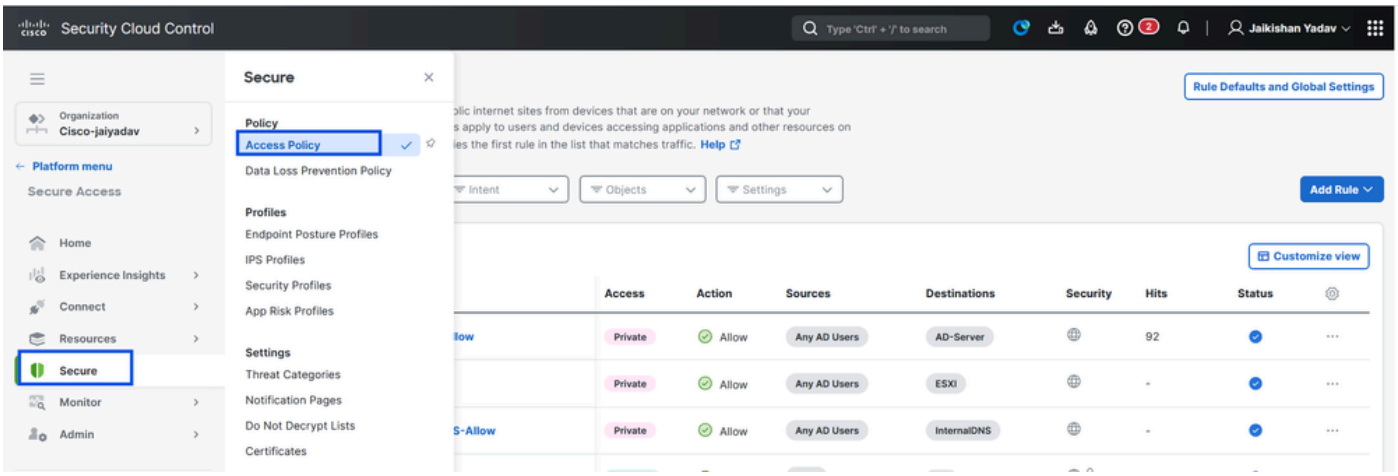
Sicherer Zugriff - Konfiguration privater Ressourcen

6. Klicken Sie auf Save (Speichern).

Schritt 2: Private Zugriffsregel erstellen

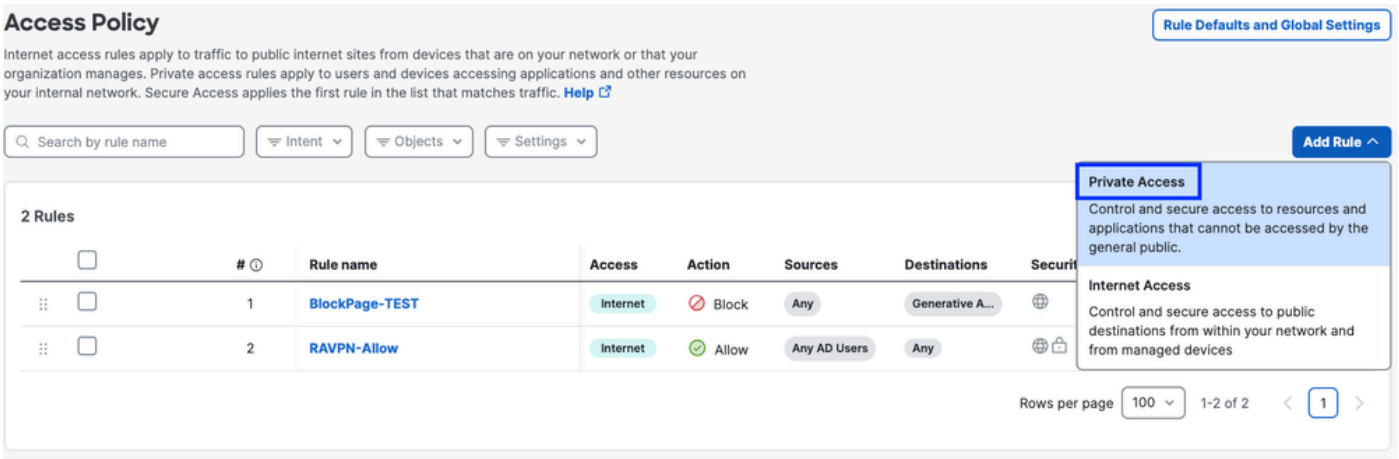
Konfigurieren Sie einen privaten Zugriff auf Secure Access, um Zugriff für Benutzer zu erhalten, die bei Universal ZTA registriert sind. Weitere Informationen finden Sie unter [Private Access Rule.]

1. Navigieren Sie zu Sicher > Zugriffsrichtlinie



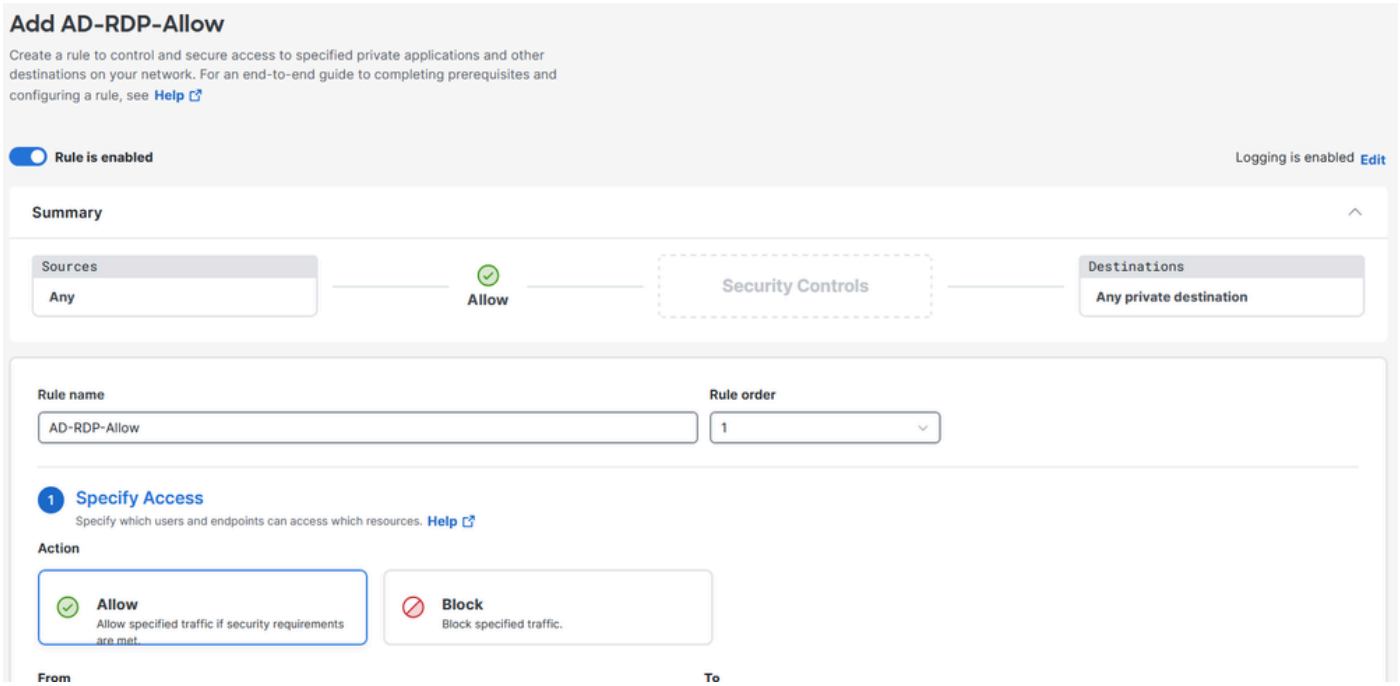
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

2. Klicken Sie auf Regel hinzufügen, und wählen Sie dann Privater Zugriff aus.
Oben auf der Regel befindet sich eine Zusammenfassung, die die konfigurierten Komponenten der Regel beschreibt.



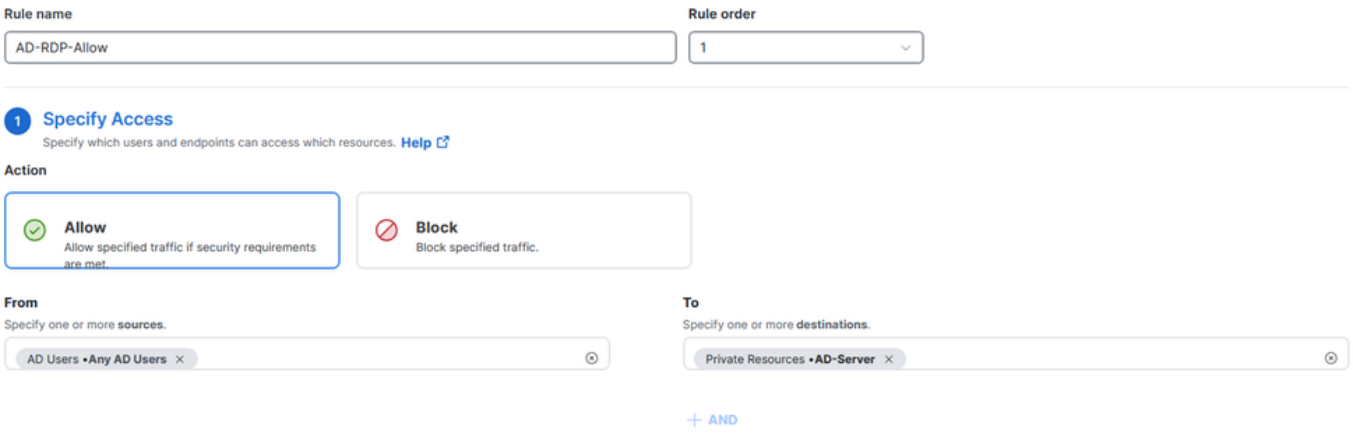
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

3. Hinzufügen eines Regelnamens



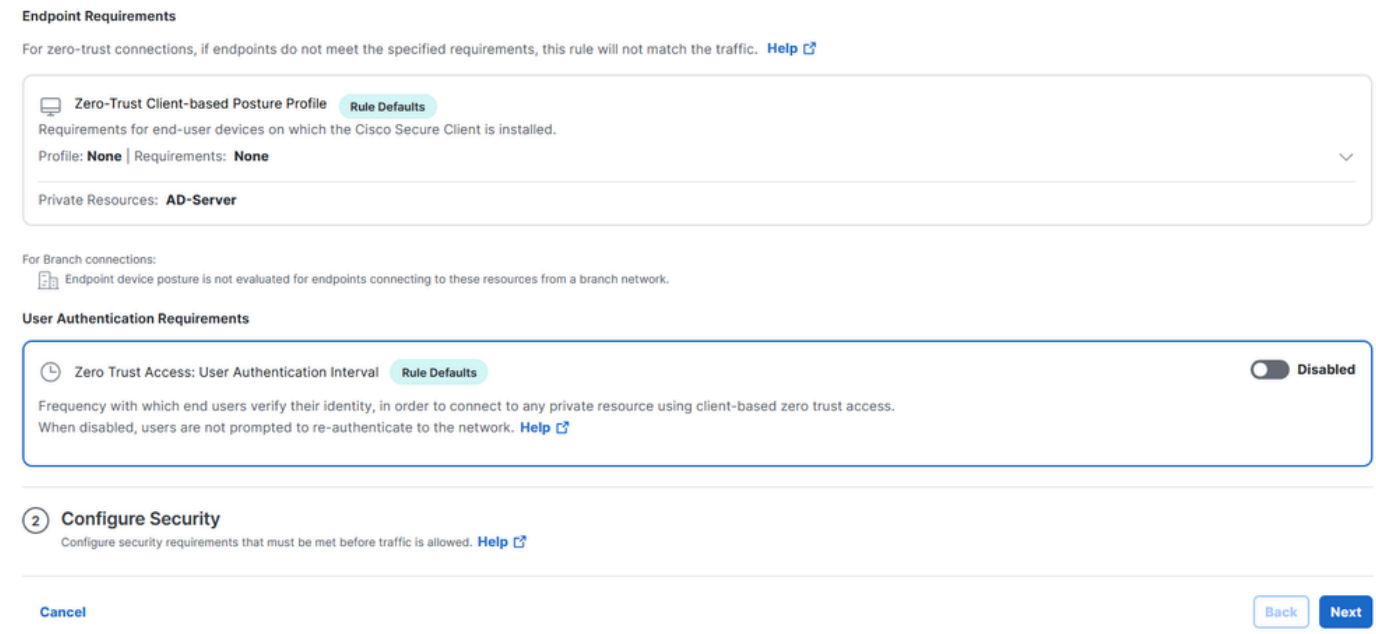
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

4. Wählen Sie die Regelaktion und dann Quelle und Ziel aus.



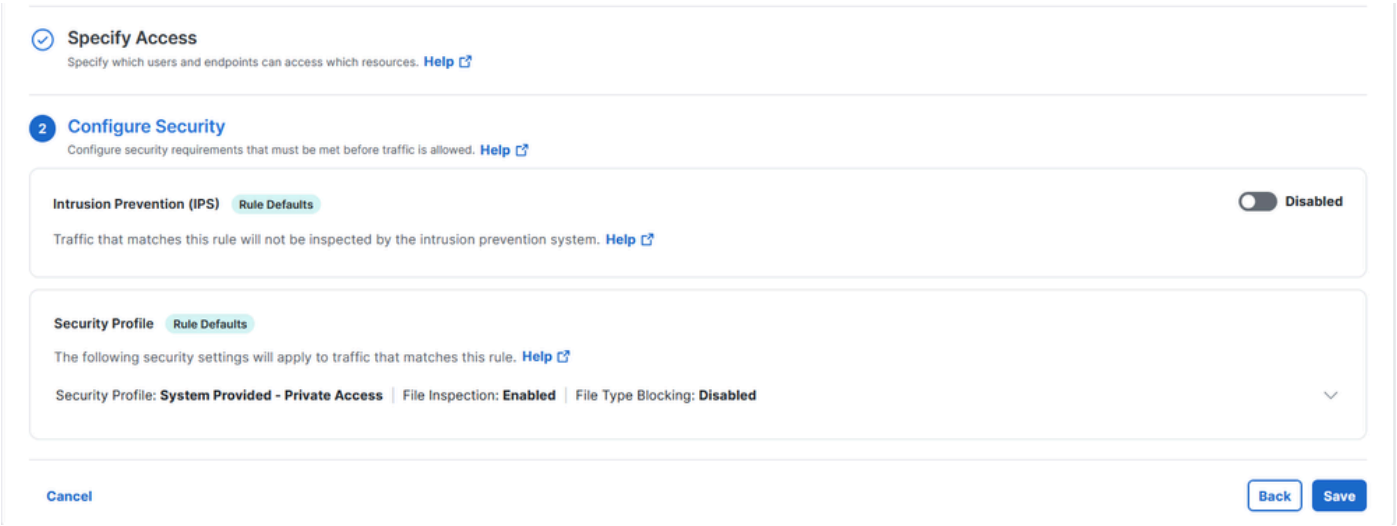
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen



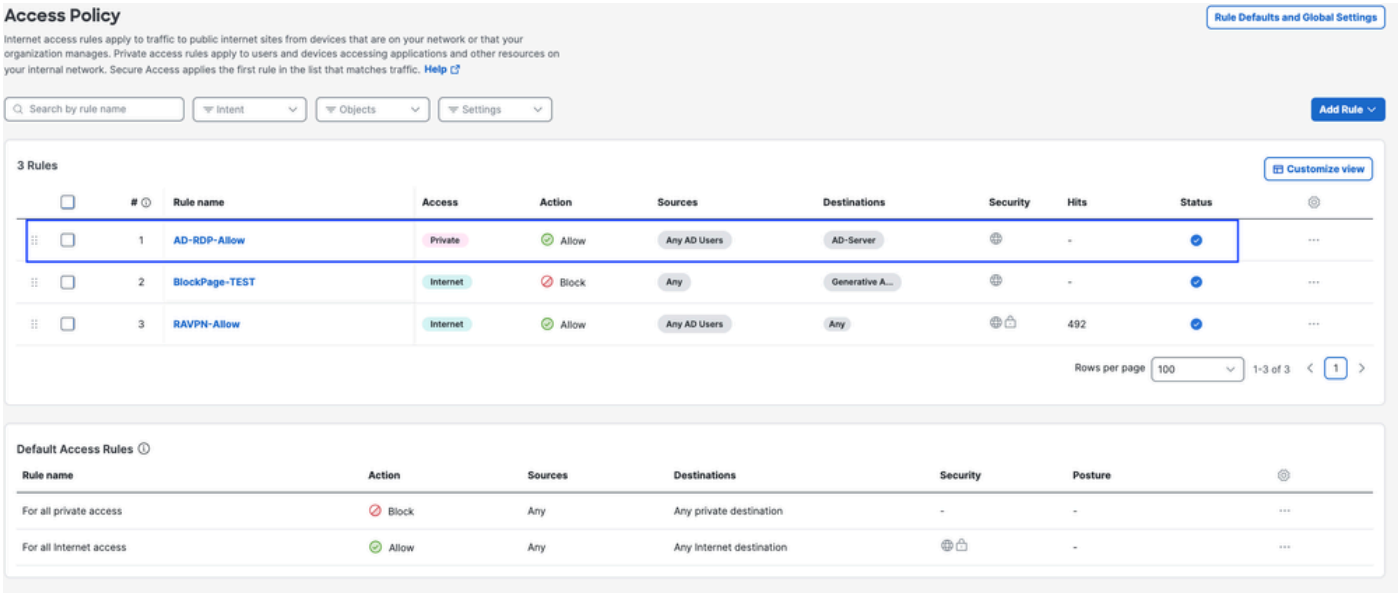
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

7. Klicken Sie auf Speichern

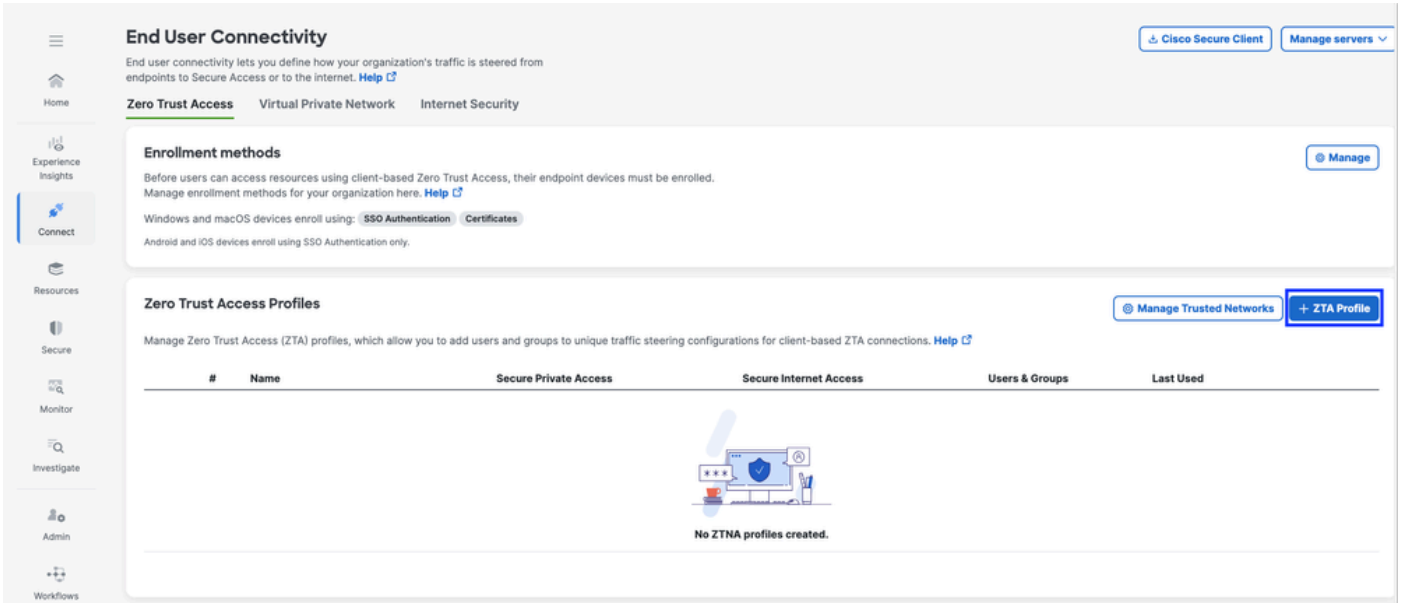


Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

Schritt - 3 Hinzufügen einer privaten Ressource zum ZTA-Profil

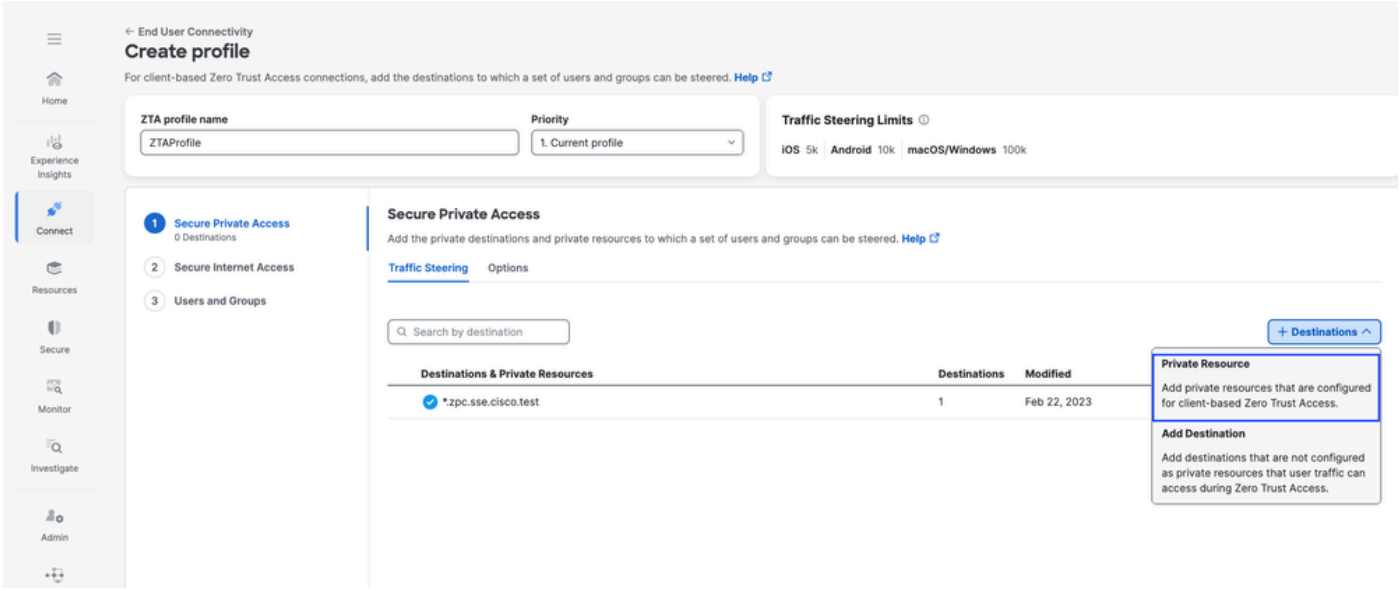
Wenn Sie ein benutzerdefiniertes ZTA-Profil verwenden, müssen Sie dem ZTA-Profil die entsprechende private Ressource hinzufügen.

1. Navigieren Sie zu Verbinden > Endbenutzerkonnektivität > Zugriff ohne Vertrauensstellung, und klicken Sie auf +ZTA-Profil

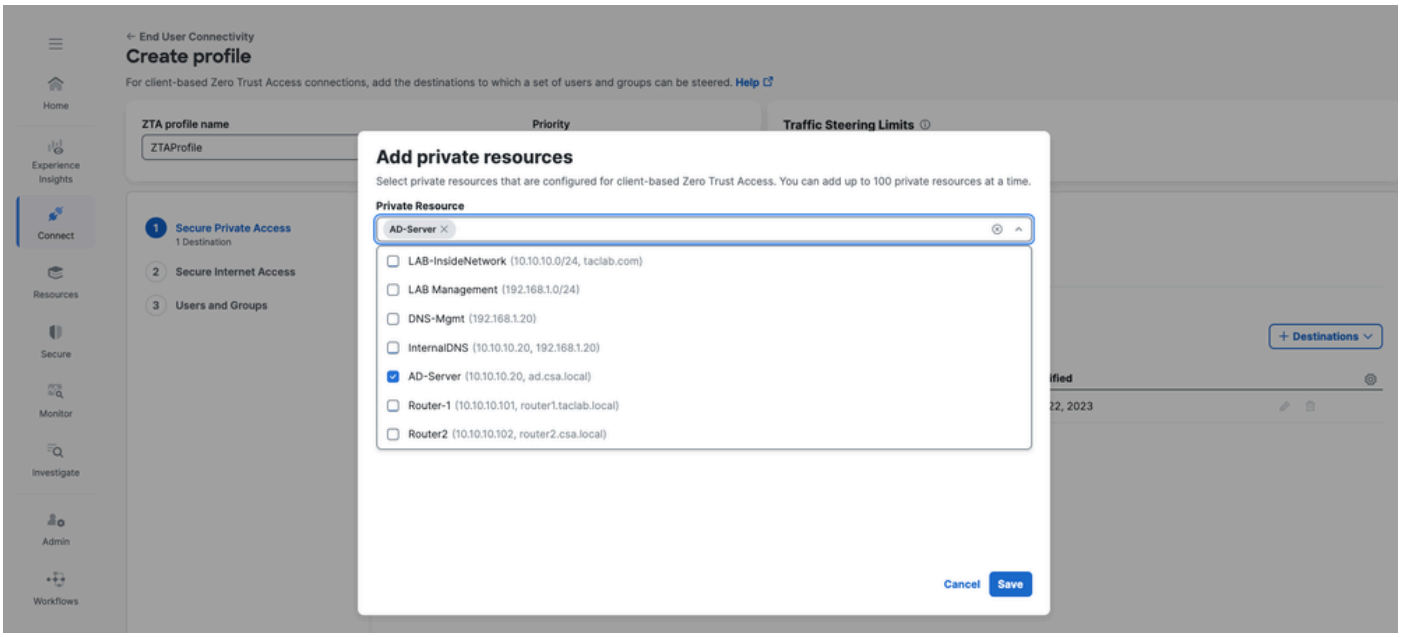


Sicherer Zugriff - ZTA-Profil

2. Fügen Sie die private Ressource hinzu

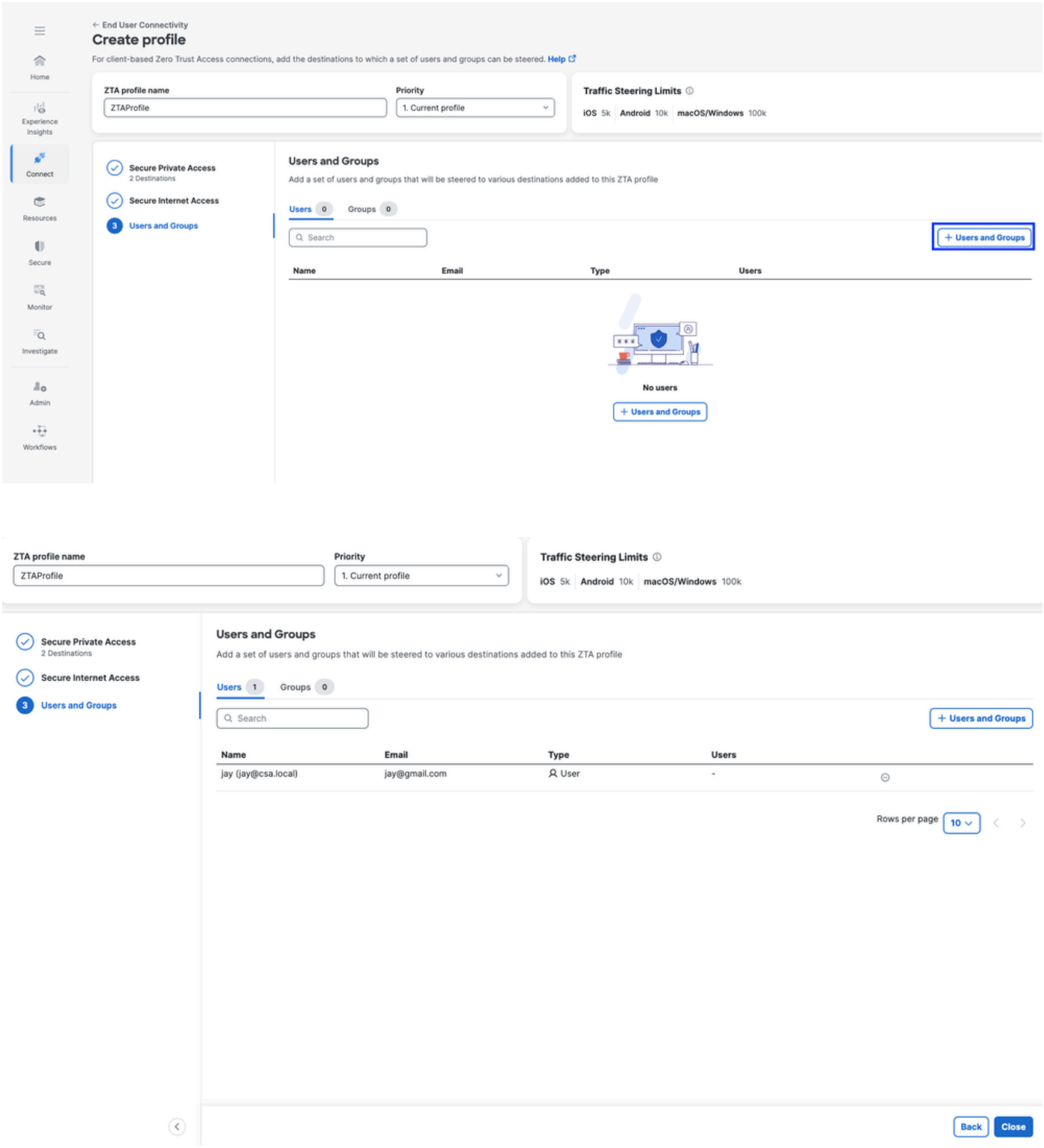


Sicherer Zugriff - ZTA-Profil



Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen



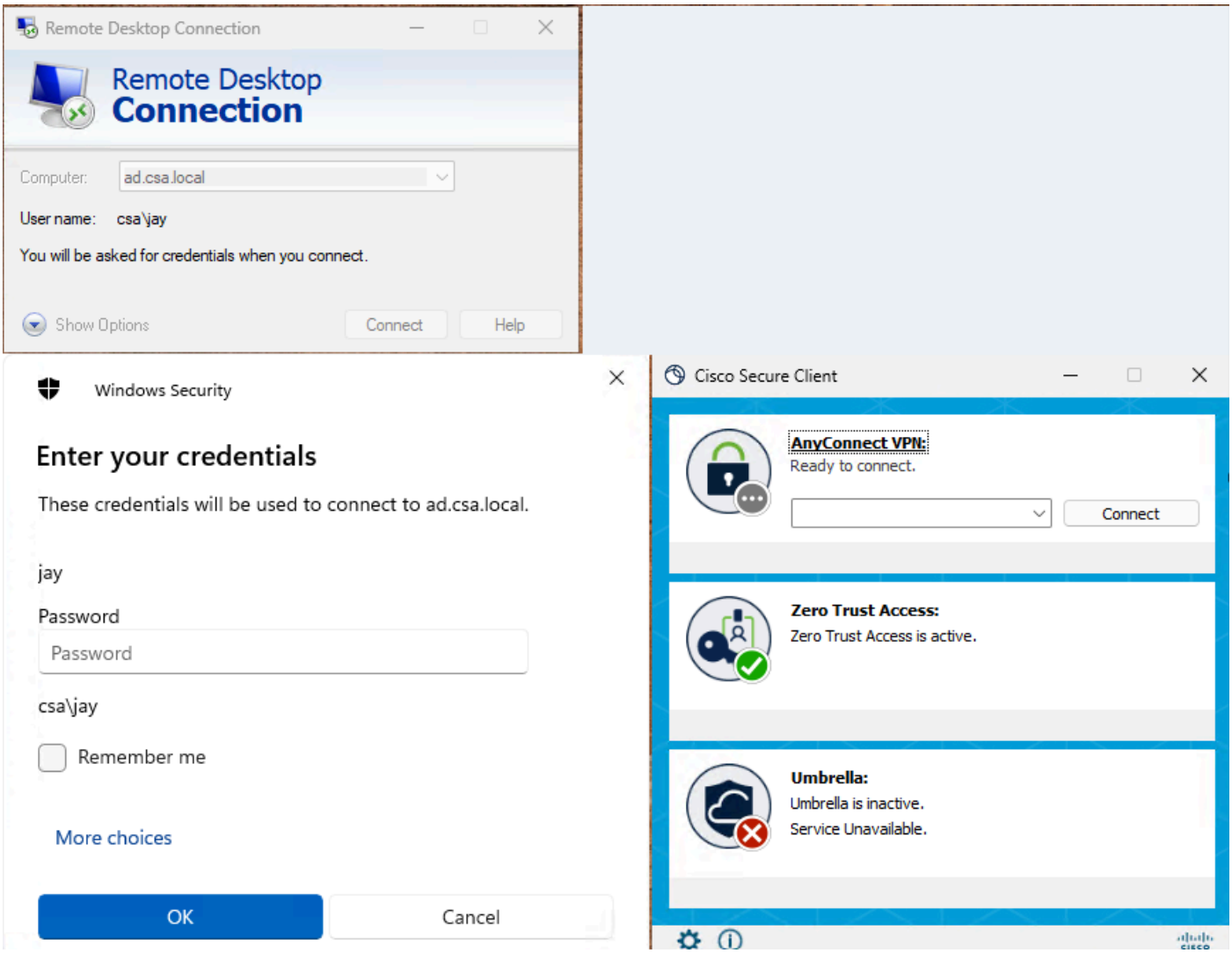
Sicherer Zugriff - ZTA-Profil

Anmerkung: Es kann bis zu 15-20 Minuten dauern, die Konfiguration für die zugewiesene private Ressource per Push und Synchronisierung mit dem Client zu übertragen.

Schritt - 4 Überprüfen des Zugriffs auf die private Ressource

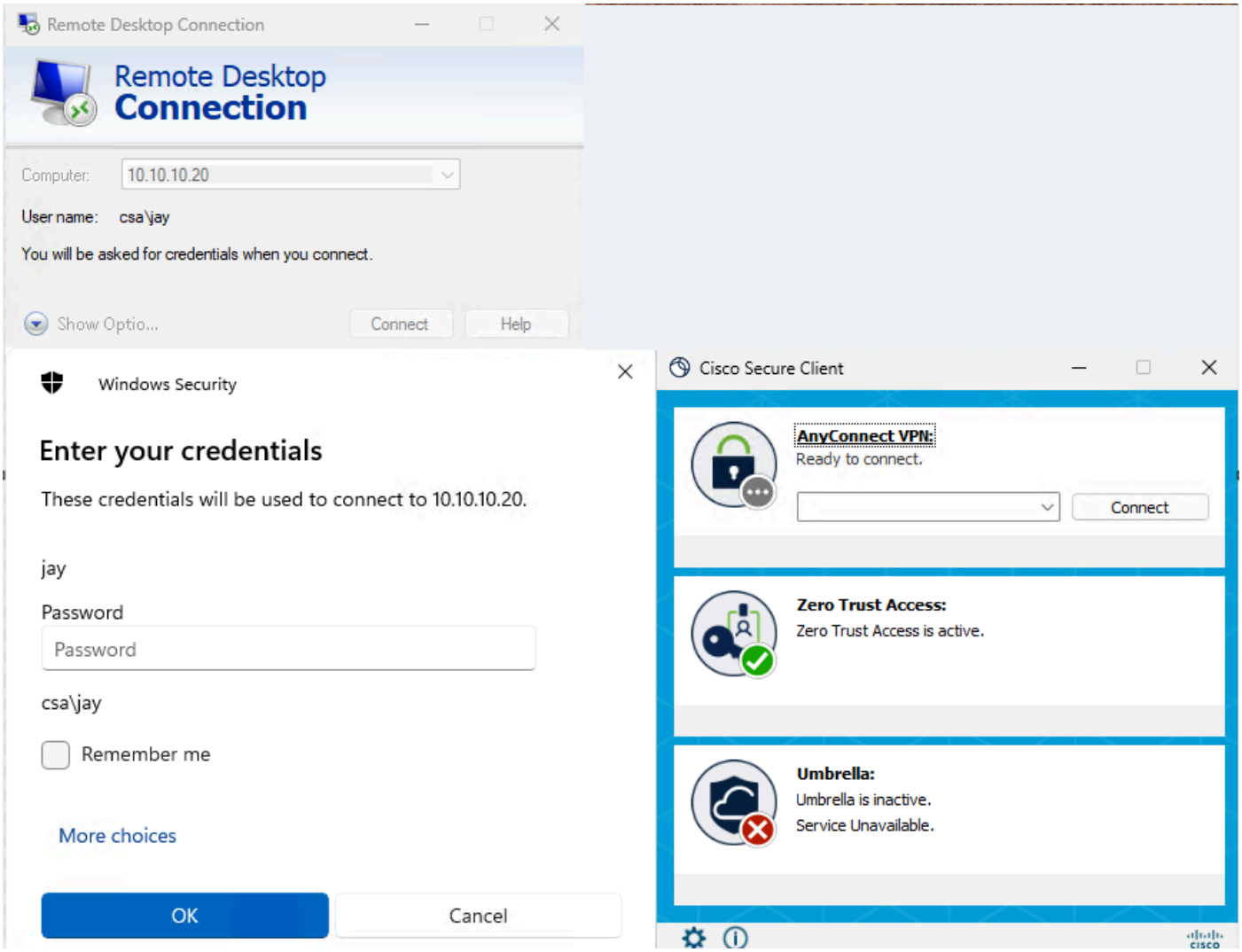
1. Zugriff auf die private Ressource

Zugriff auf den PR über FQDN



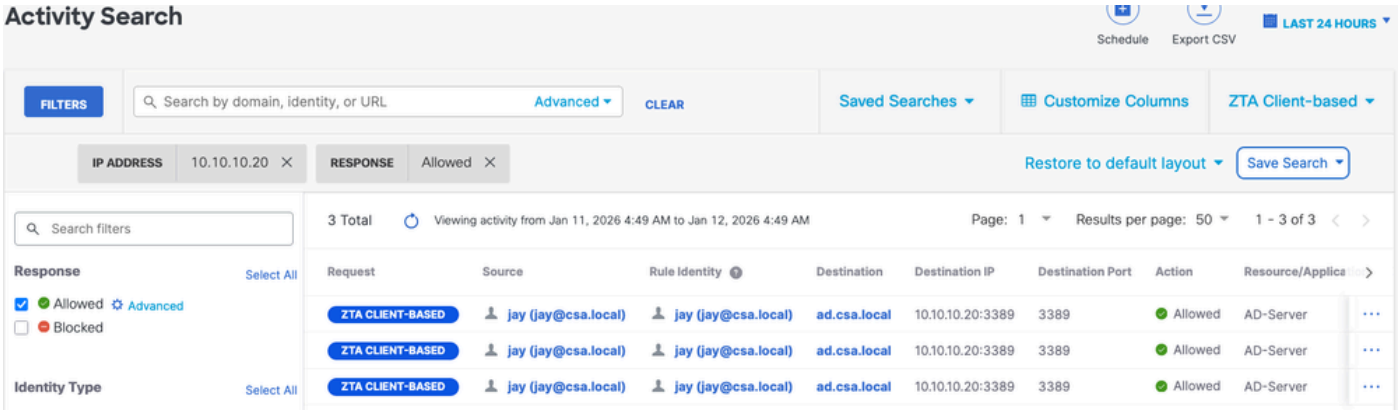
Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse

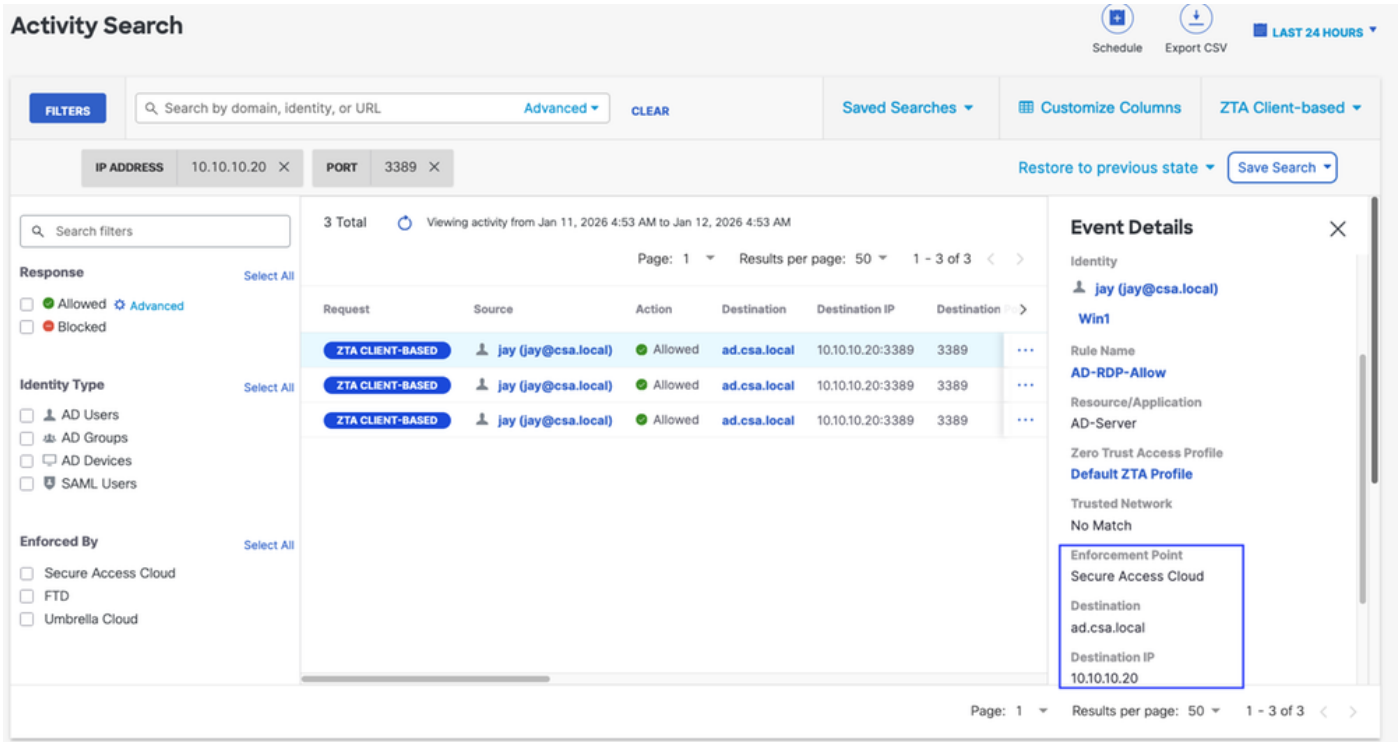


Sicherer Zugriff - PR-Tests

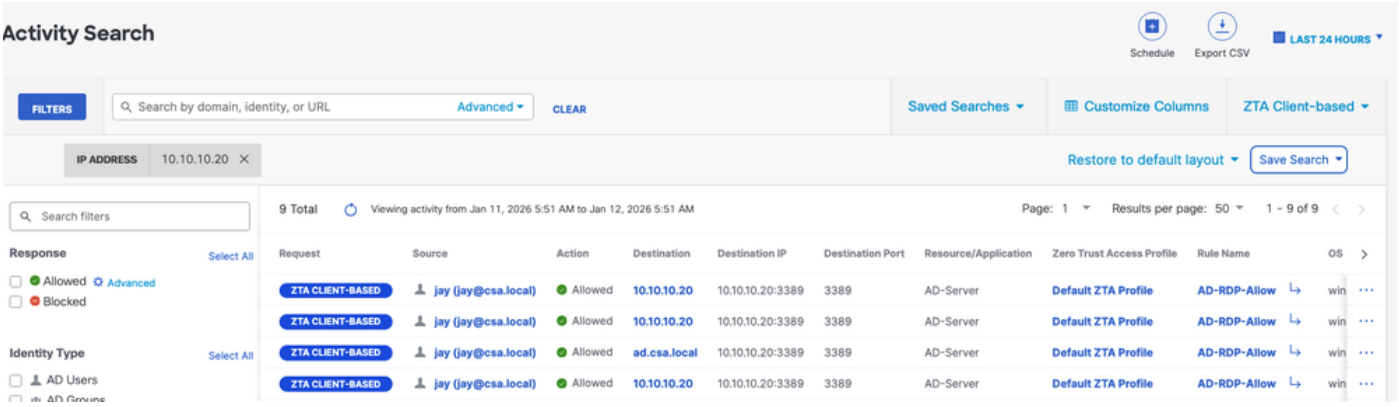
2. Überprüfen Sie dies mit den Ereignissen bei der Aktivitätssuche



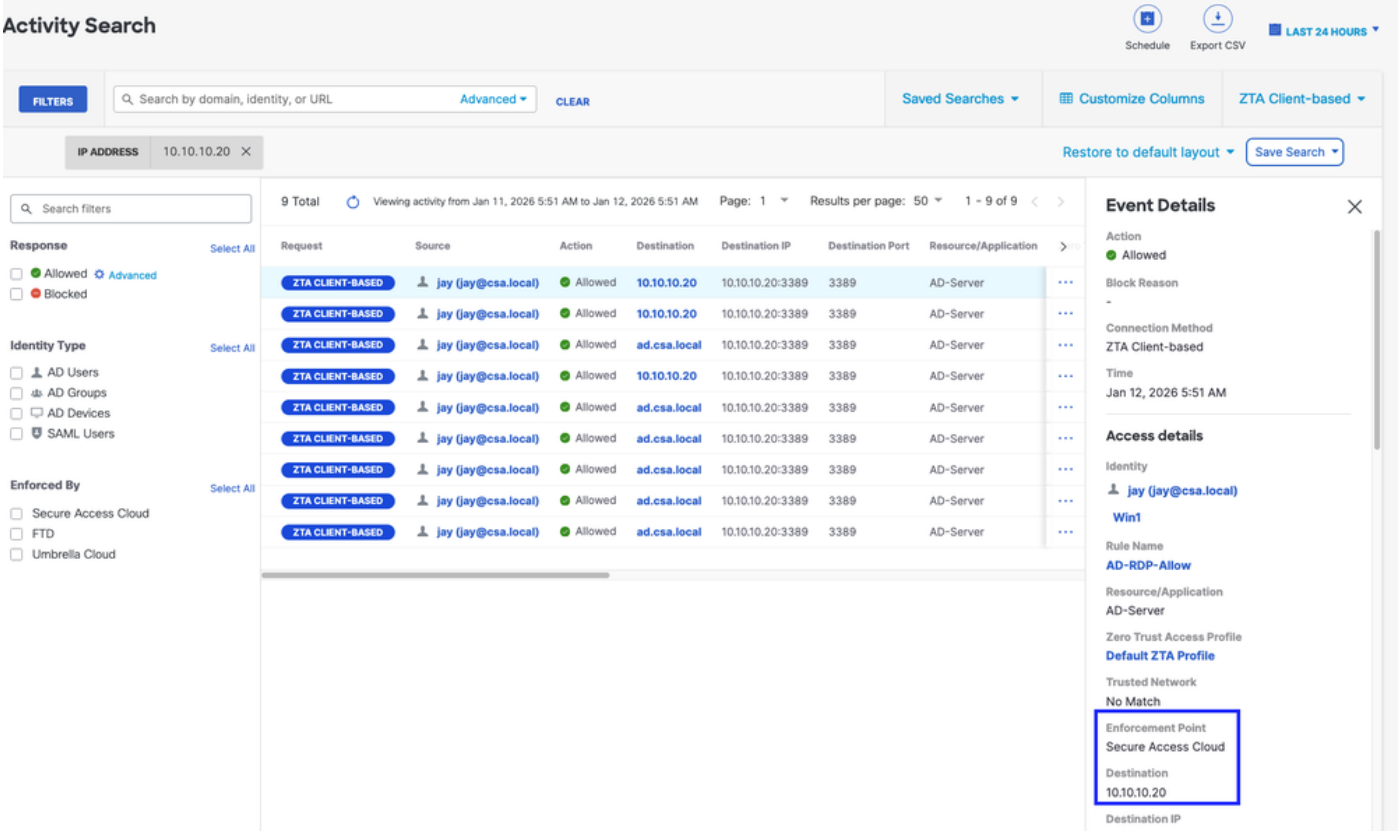
Sicherer Zugriff - Aktivitätssuche



Sicherer Zugriff - Aktivitätssuche

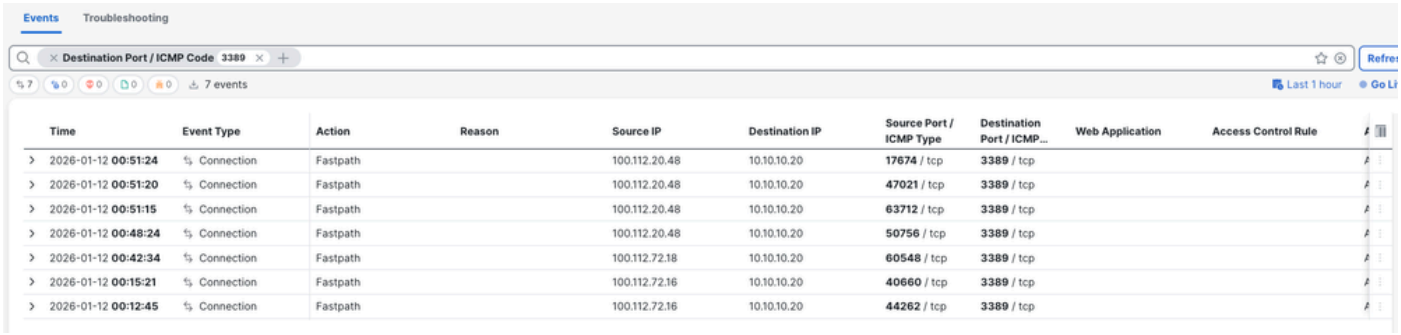


Sicherer Zugriff - Aktivitätssuche



Sicherer Zugriff - Aktivitätssuche

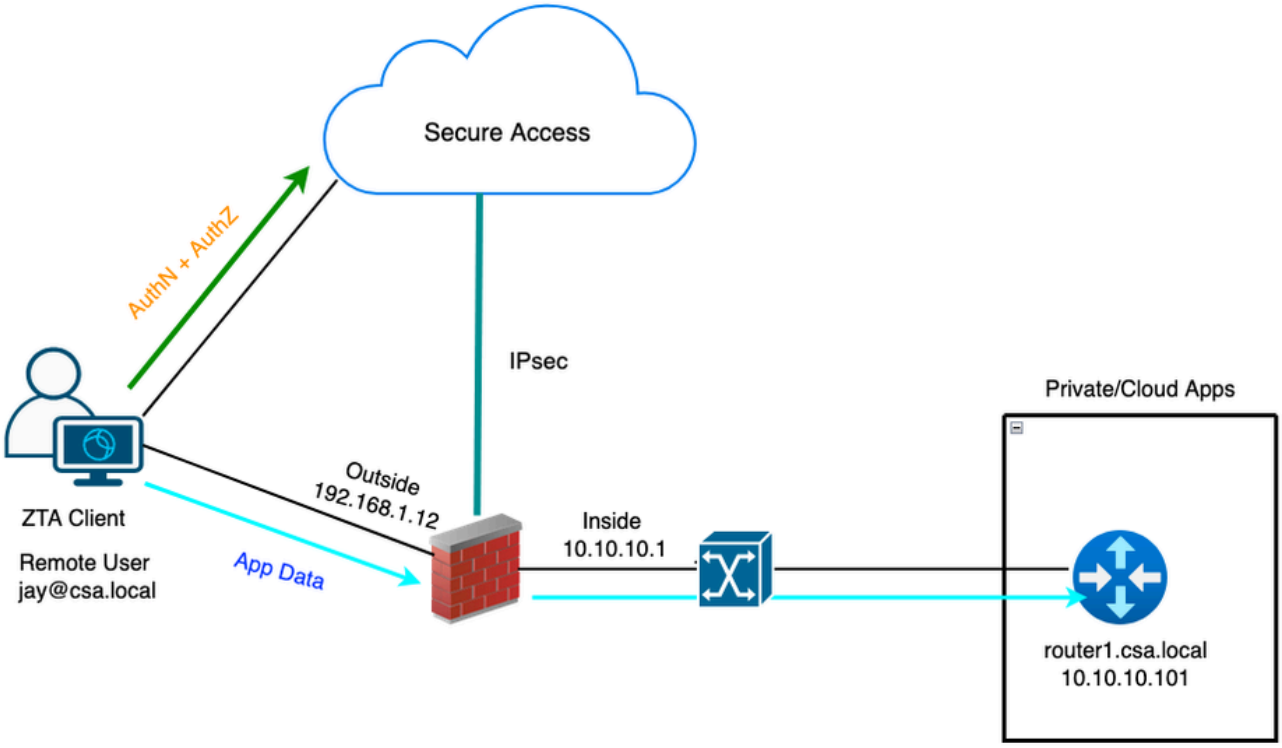
3. FMC-Verbindungsereignisse überprüfen



FMC-Verbindungsereignisse

Testfall 2 - Remote-Benutzer - Lokale Durchsetzung

Der Zugriff auf eine private Ressource über lokale Durchsetzung erfolgt bei dieser Art von Richtlinienauswertung über sicheren Zugriff, die Anwendungsdaten bleiben jedoch lokal bei FTD. Zum Beispiel, ein ZTA eingeschriebenen Client oder Benutzer mit Heimnetzwerk verbunden und versucht, eine private Ressource, die hinter FTD innerhalb Schnittstelle zugreifen .

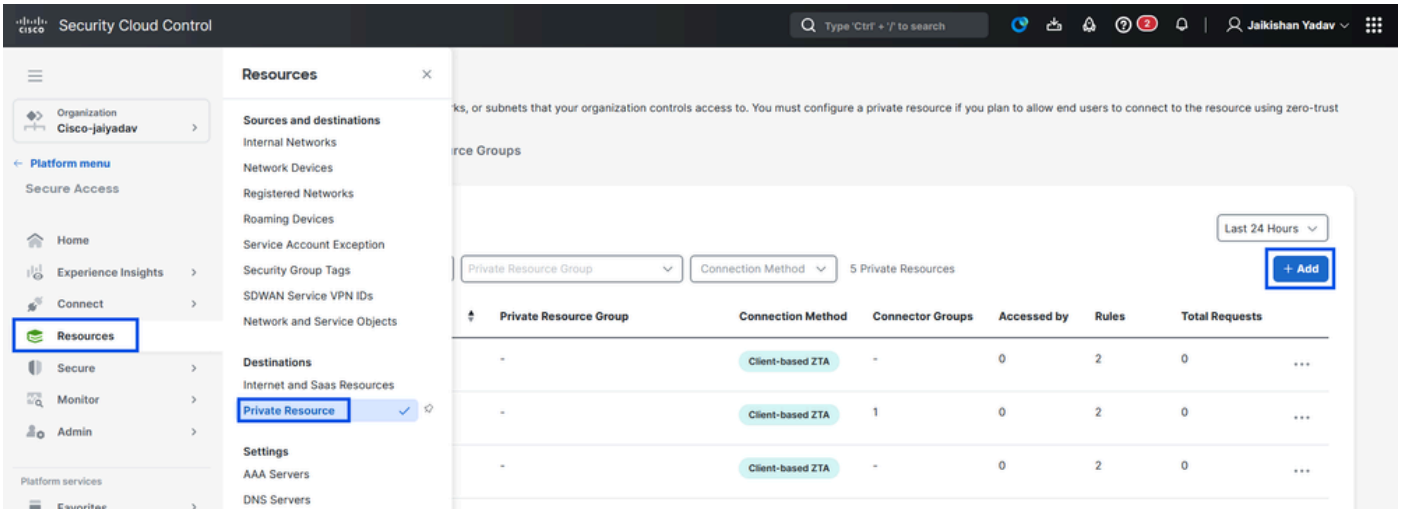


Universal ZTA - Testfall-Topologie

Schritt 1 - Definieren einer privaten Ressource für sicheren Zugriff

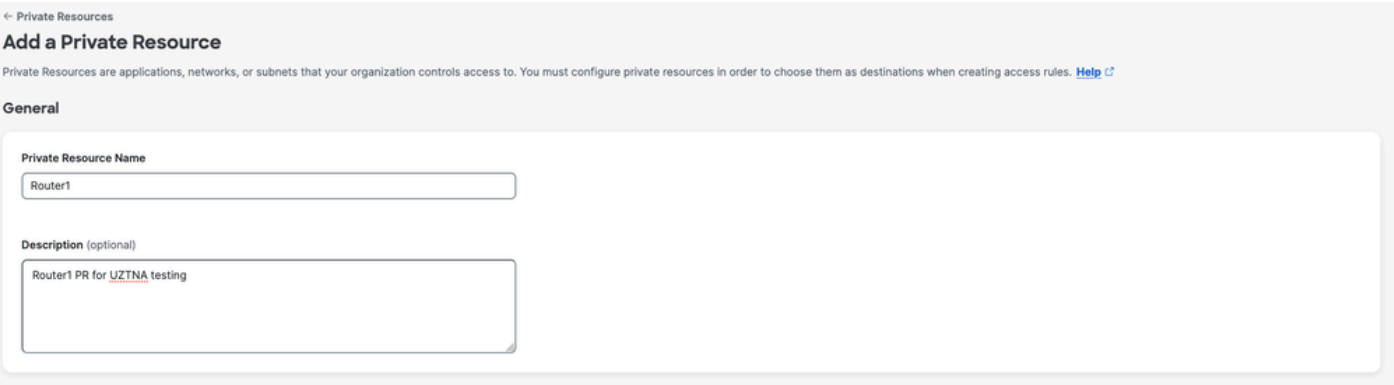
Konfigurieren einer privaten Ressource für den Zugriff über ein bei Zero Trust Access (ZTA) angemeldetes Gerät mit Cloud-Durchsetzung

1. Navigieren Sie zu Ressourcen > Ziele > Private Ressourcen > und klicken Sie auf +Hinzufügen.



Sicherer Zugriff - Konfiguration privater Ressourcen

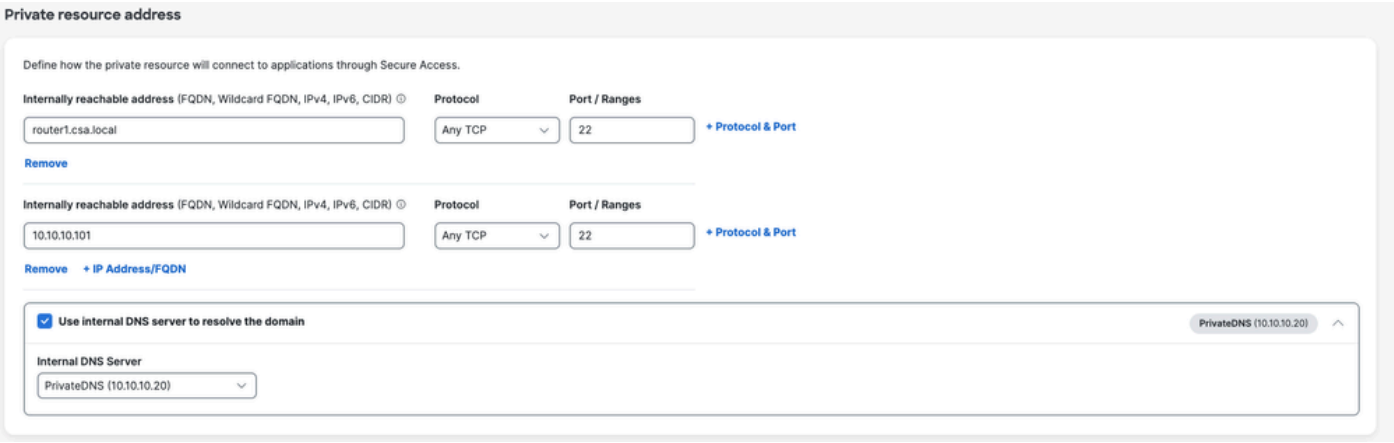
2. Geben Sie für Private Resource Name einen sinnvollen Namen für die Ressource ein. Für Description empfehlen wir, Informationen wie den Zweck der Ressource oder den Namen des Ressourcenbesitzers anzugeben.



Sicherer Zugriff - Konfiguration privater Ressourcen

3. Geben Sie den FQDN der privaten Ressource ein, auf die Sie zugreifen möchten. Wir können auch die IP-Adresse der privaten Ressource definieren. Weitere Informationen finden Sie unter [Hinzufügen einer privaten Ressource]

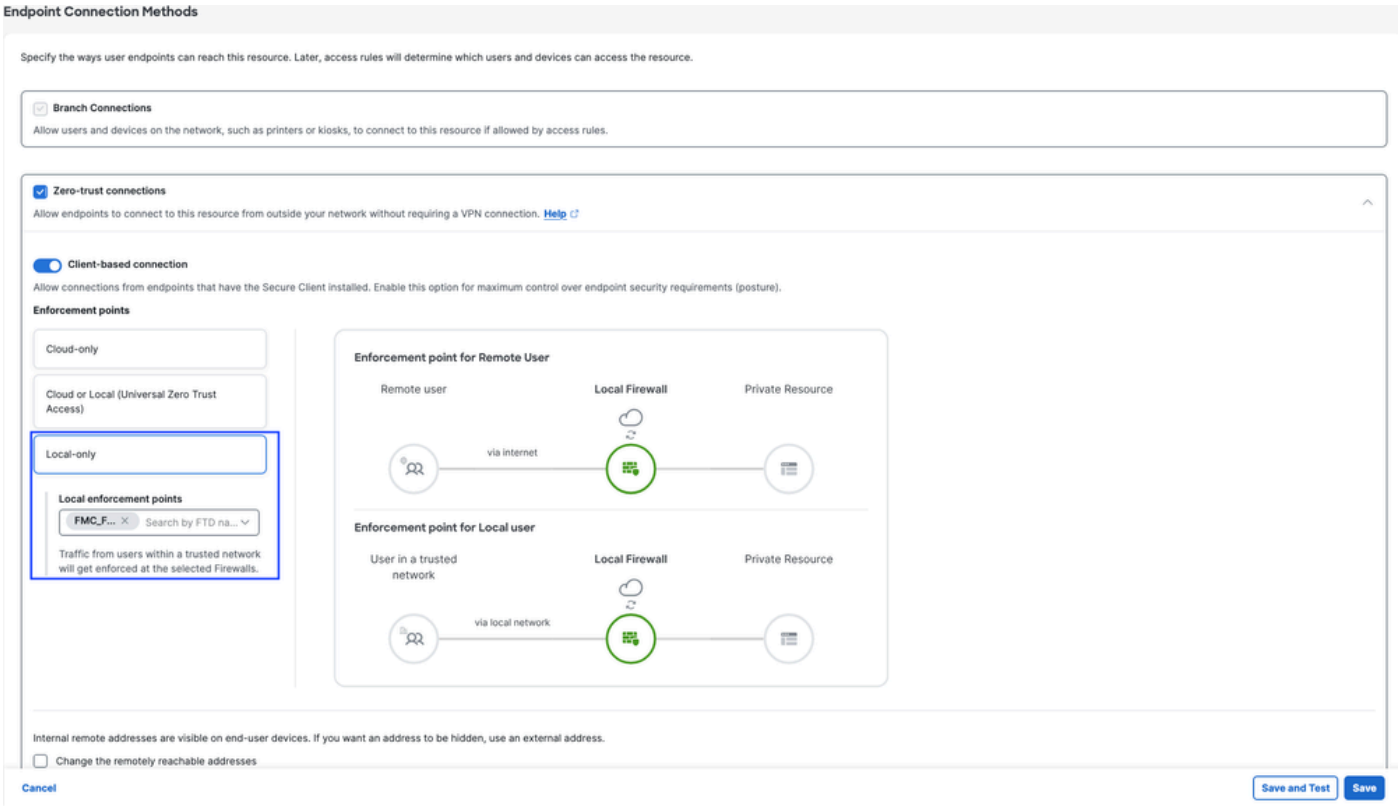
4. Wählen Sie den internen DNS-Server, um die Domäne aufzulösen.



Sicherer Zugriff - Konfiguration privater Ressourcen

5. Endpunktverbindungsmethoden auswählen

6. Wählen Sie FTD als lokale Durchsetzungspunkte



Sicherer Zugriff - Konfiguration privater Ressourcen

Anmerkung: Je nach gewählter Registrierungsart ordnet diese Änderung den PR automatisch dem FTD zu und löst eine Richtlinienbereitstellung aus.

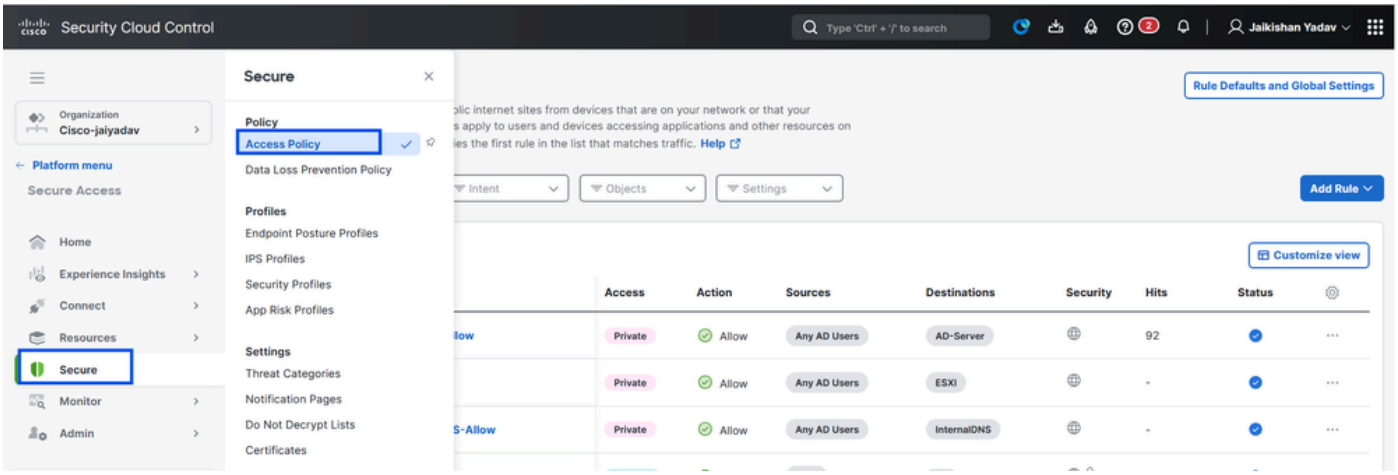
---

7. Klicken Sie auf Save (Speichern).

Schritt 2: Private Zugriffsregel erstellen

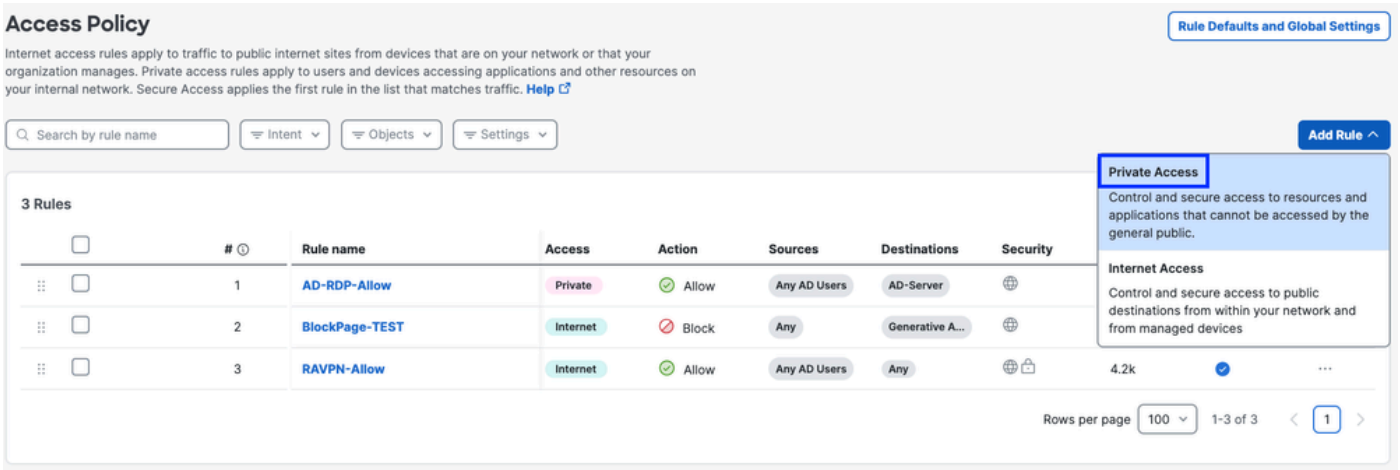
Konfigurieren Sie einen privaten Zugriff auf Secure Access, um Zugriff für Benutzer zu erhalten, die bei Universal ZTA registriert sind. Weitere Informationen finden Sie unter Private Access Rule.

1. Navigieren Sie zu Sicher > Zugriffsrichtlinie



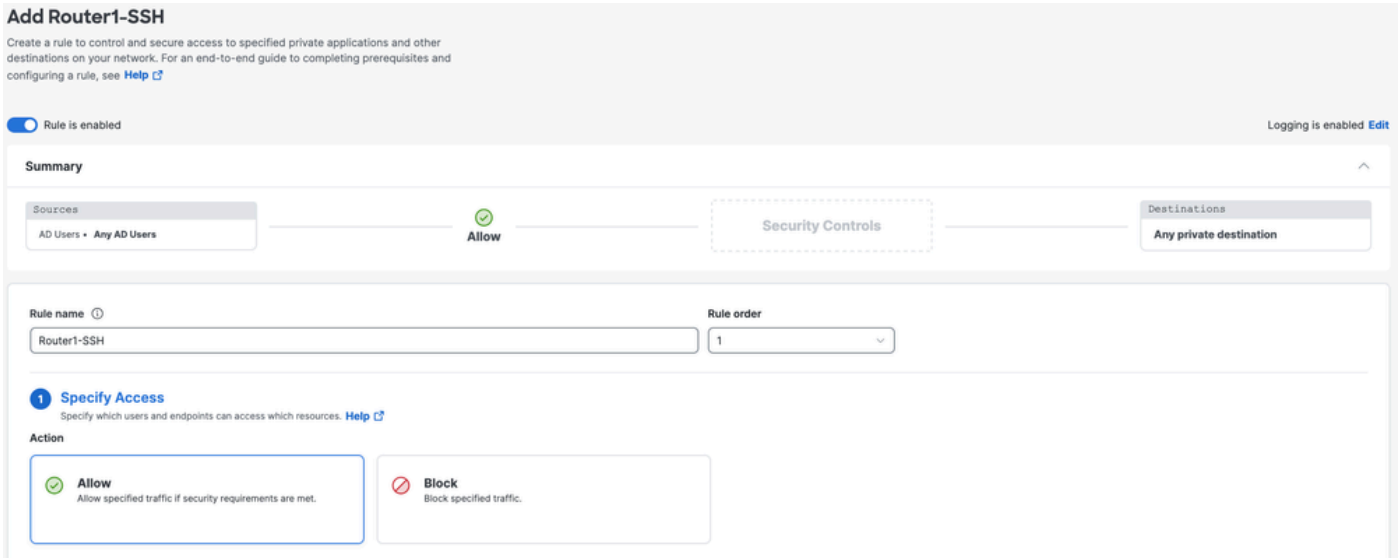
Sicherer Zugriff - Konfiguration privater Ressourcen

2. Klicken Sie auf Regel hinzufügen, und wählen Sie dann Privater Zugriff aus.
Oben auf der Regel befindet sich eine Zusammenfassung, die die konfigurierten Komponenten der Regel beschreibt.



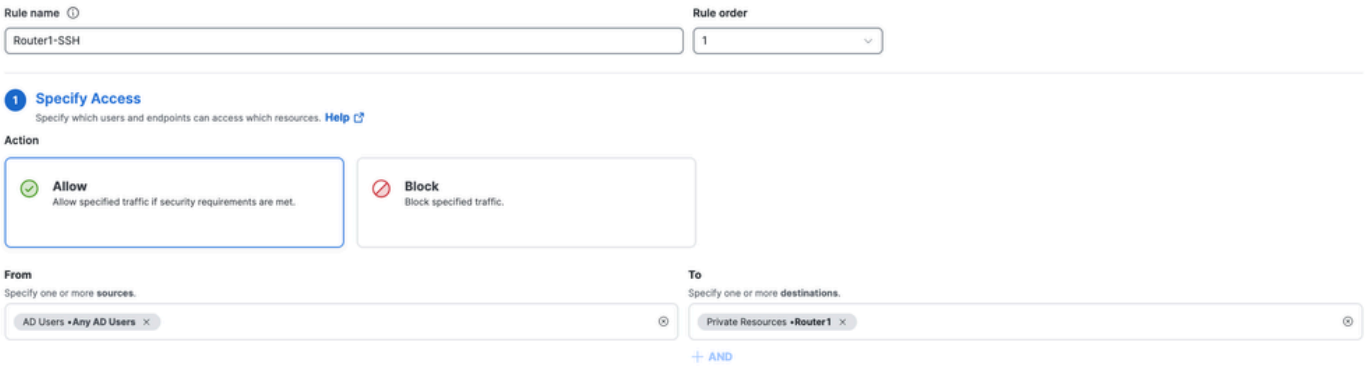
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

3. Hinzufügen eines Regelnamens



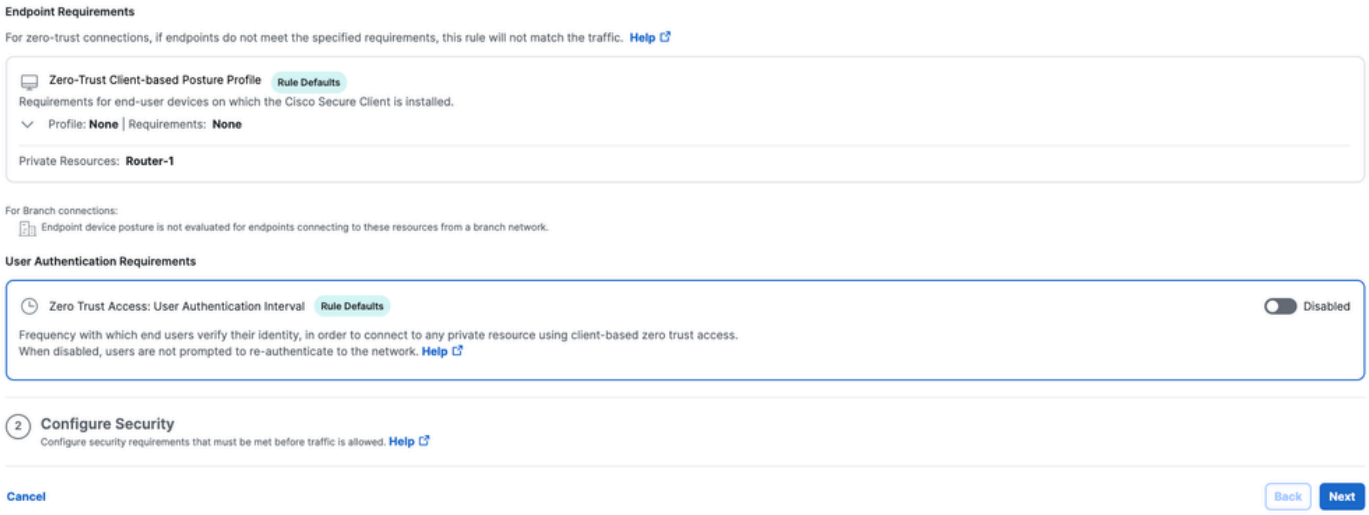
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

4. Wählen Sie die Regelaktion und dann Quelle und Ziel aus.



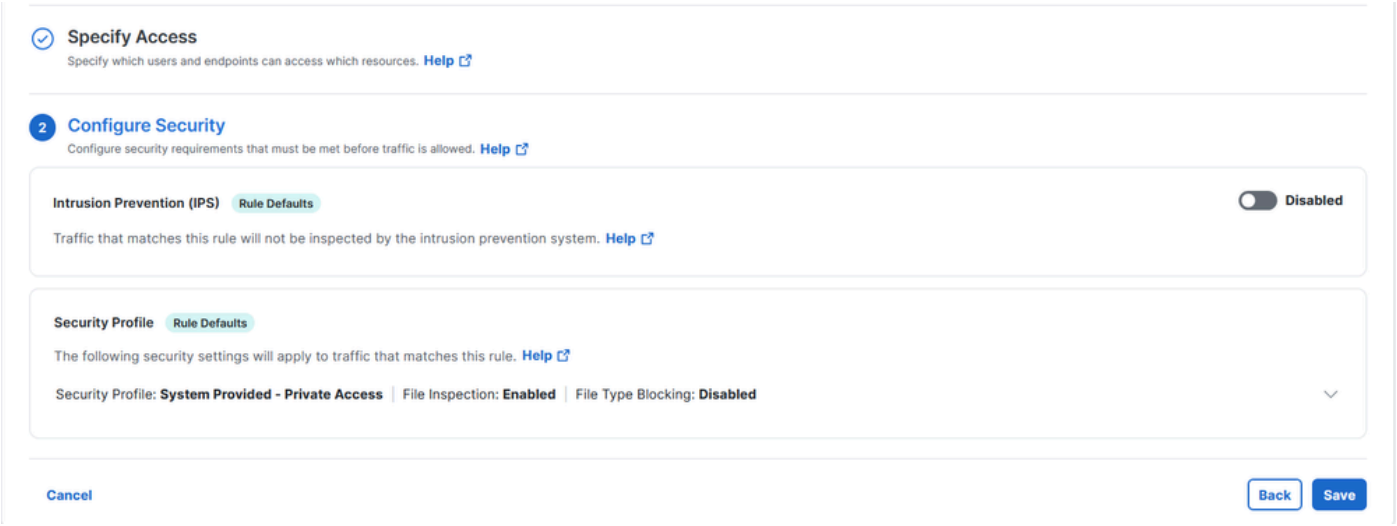
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen



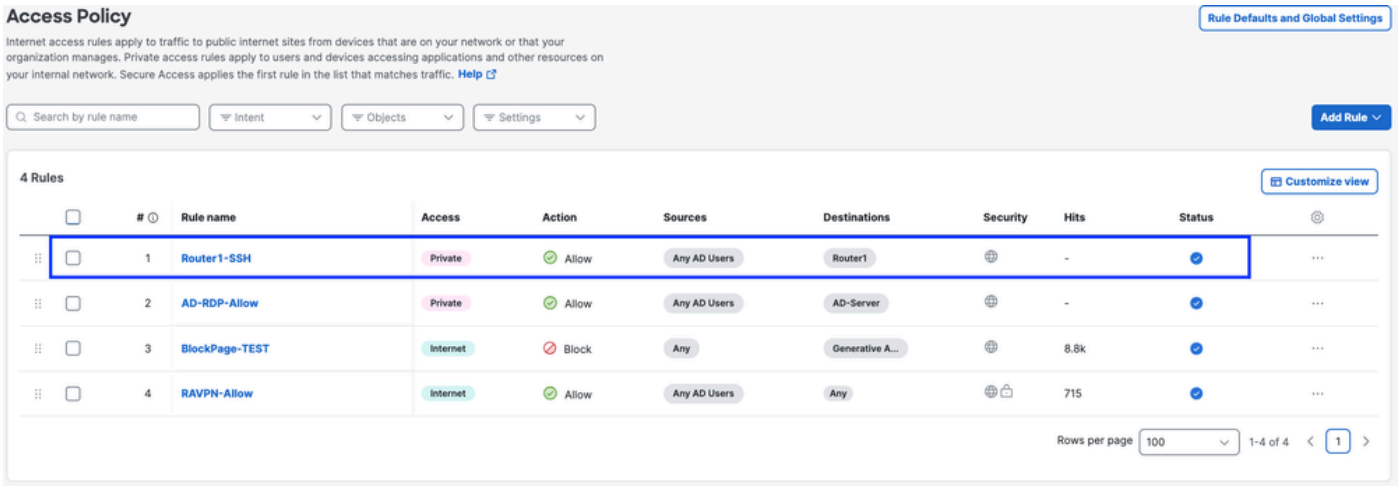
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

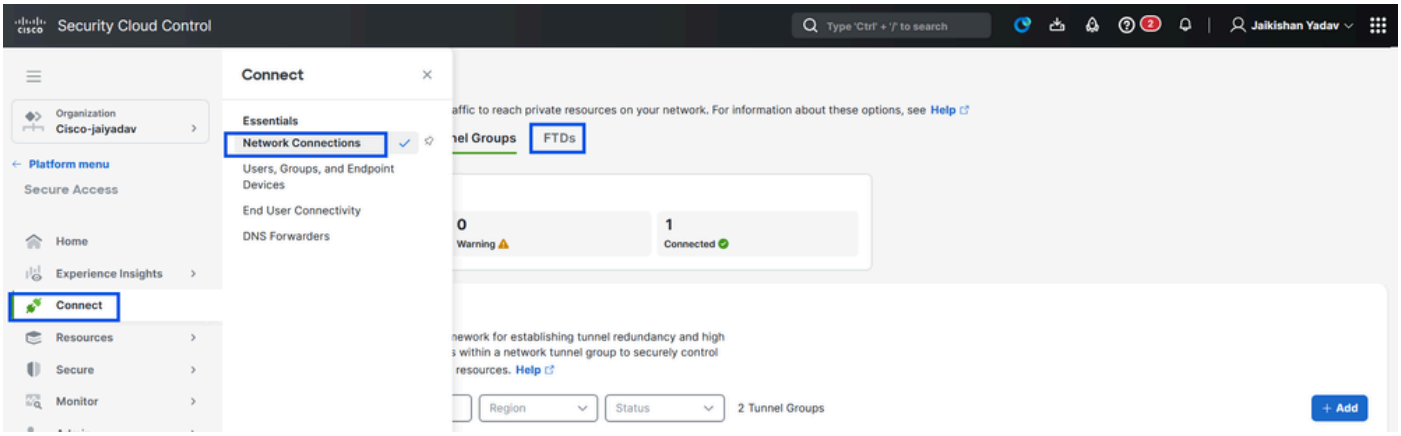
7. Klicken Sie auf Speichern



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

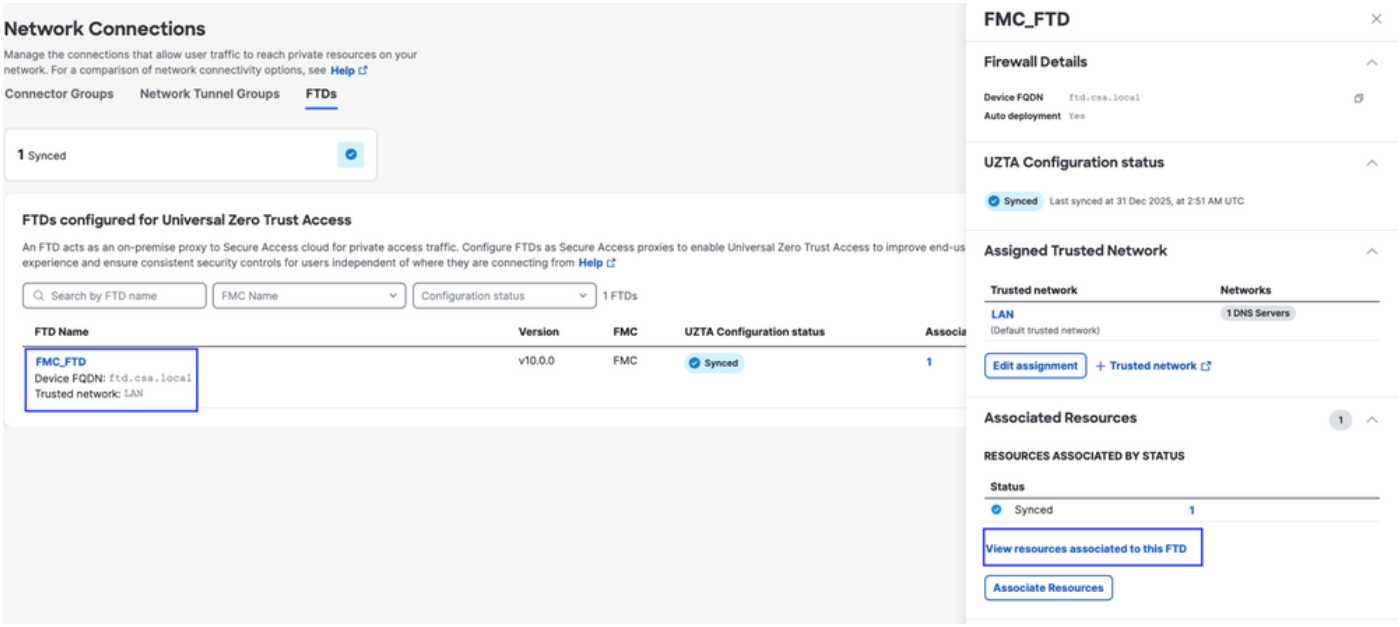
Schritt 3 - Überprüfen der Zuordnung von PR auf dem FTD

1. Navigieren Sie zu Verbinden > Netzwerkverbindungen > FTDs

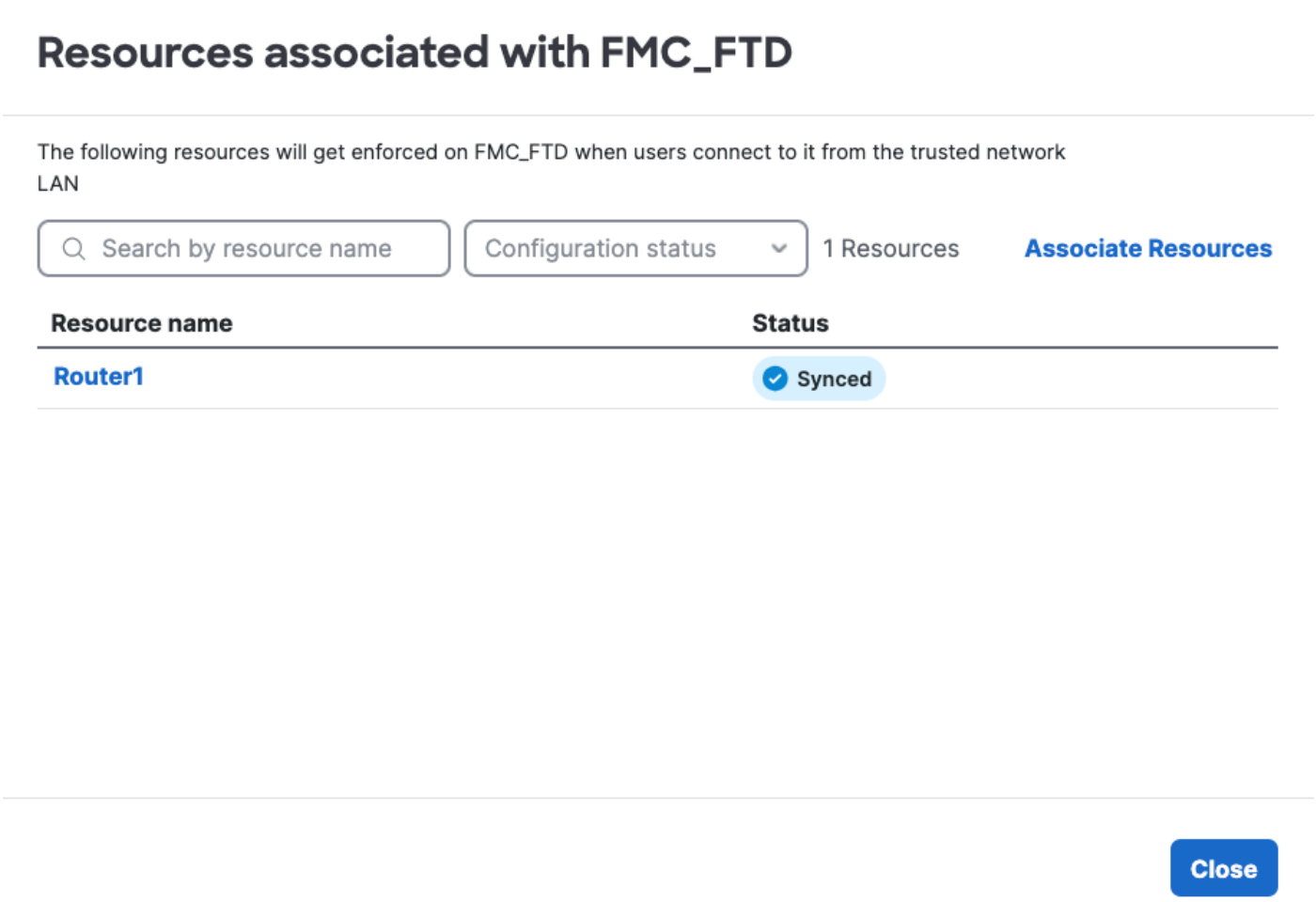


Sicherer Zugriff - PR-Verifizierung

2. Klicken Sie auf FTD > Ressourcen für diesen FTD anzeigen.



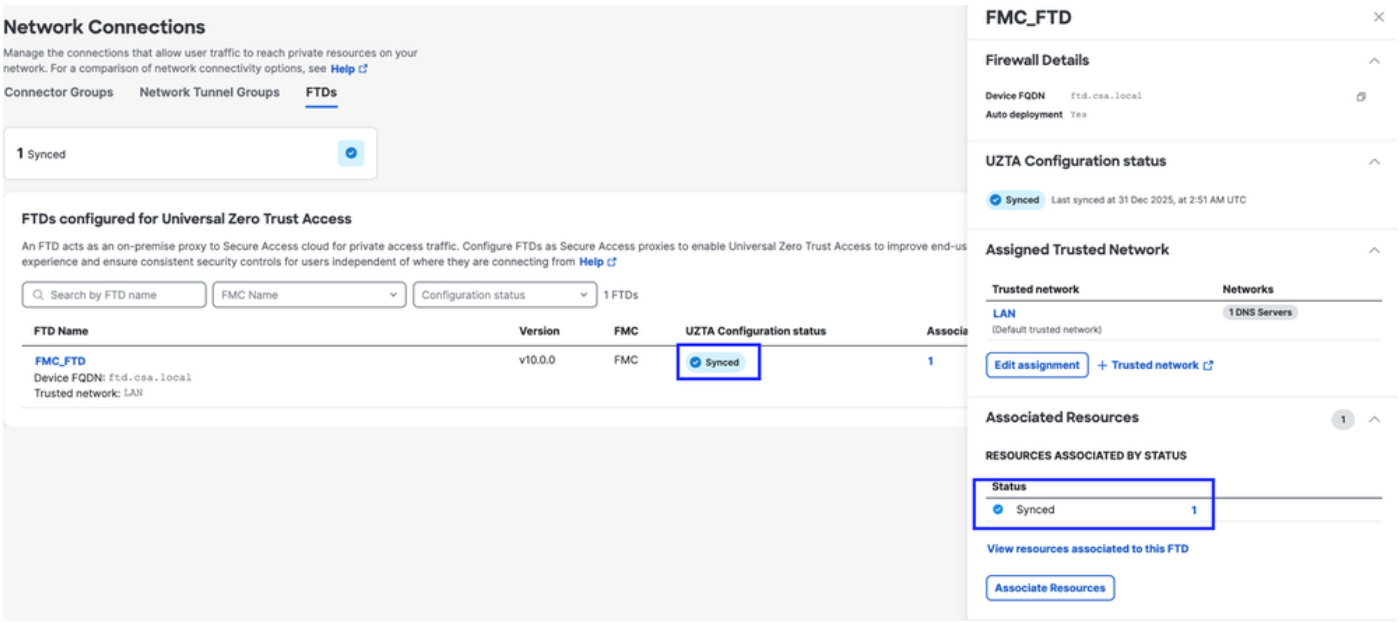
Sicherer Zugriff - PR-Verifizierung



Sicherer Zugriff - PR-Verifizierung

3. Klicken Sie auf Schließen

4. Vergewissern Sie sich, dass der Status , Associated Resource (Zugehörige Ressource) und Configuration (Konfiguration) den Status "Synchronisiert" aufweist.



Sicherer Zugriff - PR-Verifizierung

5. Überprüfen Sie, ob die Konfiguration auf FTD übertragen wurde.

Melden Sie sich bei der FTD-CLI an, und navigieren Sie zum LINA-Modus.

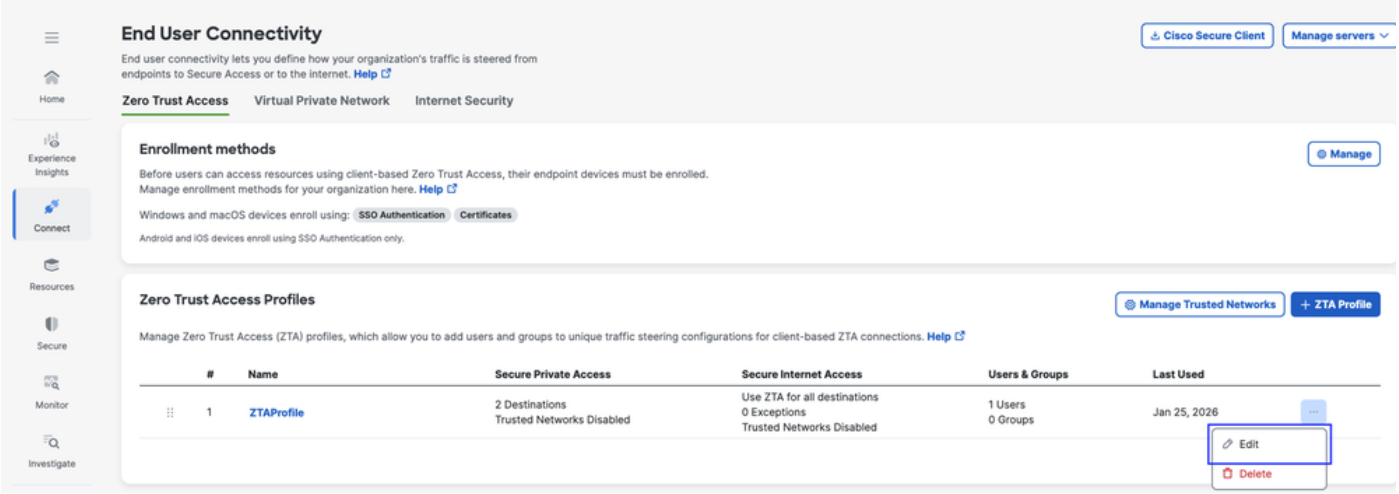
show running-config object application

```
> 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-Überprüfung

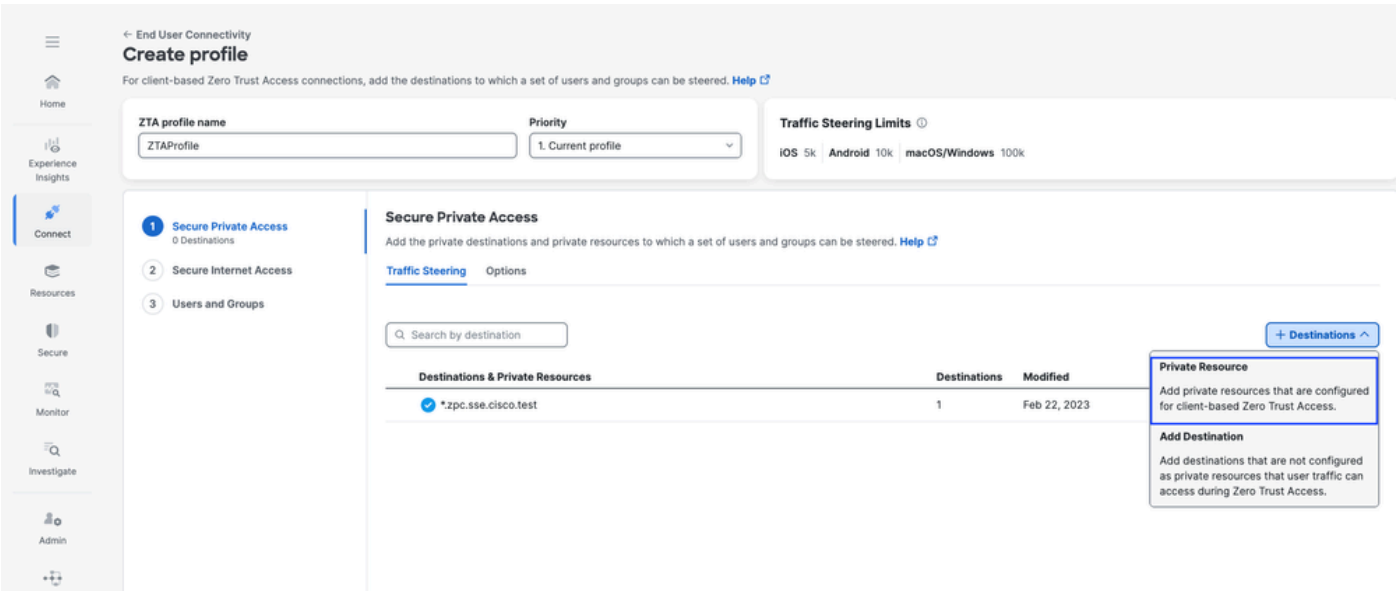
Schritt - 4 Hinzufügen einer privaten Ressource zum ZTA-Profil

1. Navigieren Sie zu Verbinden > Endbenutzerverbindung > Zugriff ohne Vertrauensstellung, und klicken Sie auf 3 Punkte, um das ZTA-Profil zu bearbeiten.

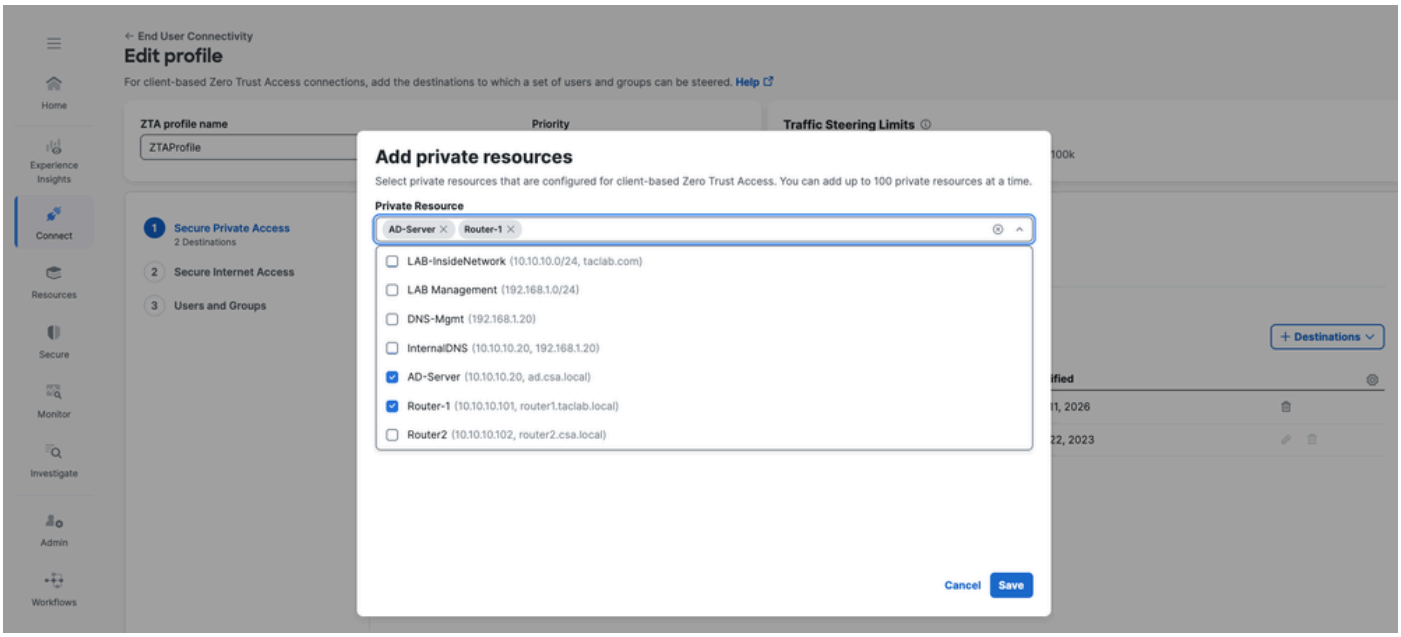


Sicherer Zugriff - ZTA-Profil

2. Fügen Sie die private Ressource hinzu

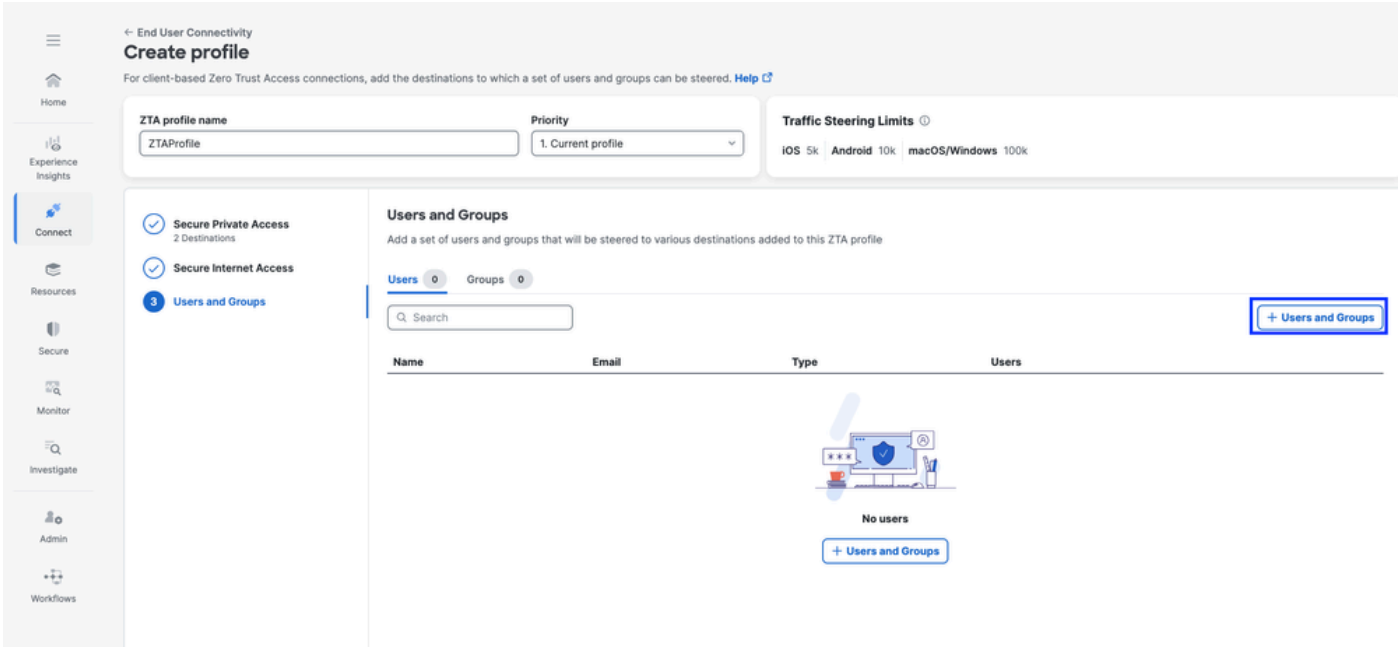


Sicherer Zugriff - ZTA-Profil

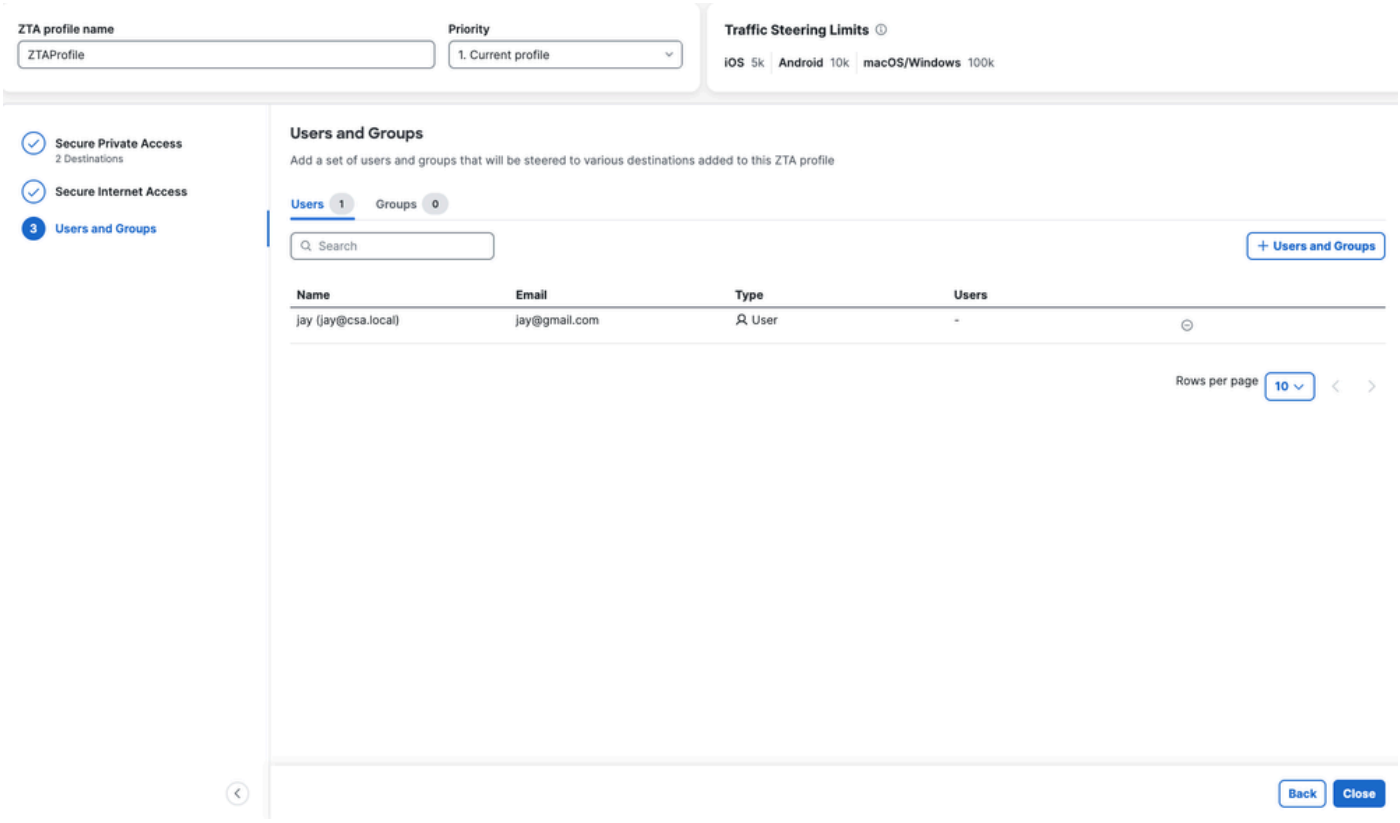


Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen



Sicherer Zugriff - ZTA-Profil



Sicherer Zugriff - ZTA-Profil

Schritt - 5 Überprüfen des Zugriffs auf die private Ressource

1. Überprüfen, ob der Remote-Benutzer den FTD FQDN auflösen kann

```
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
```

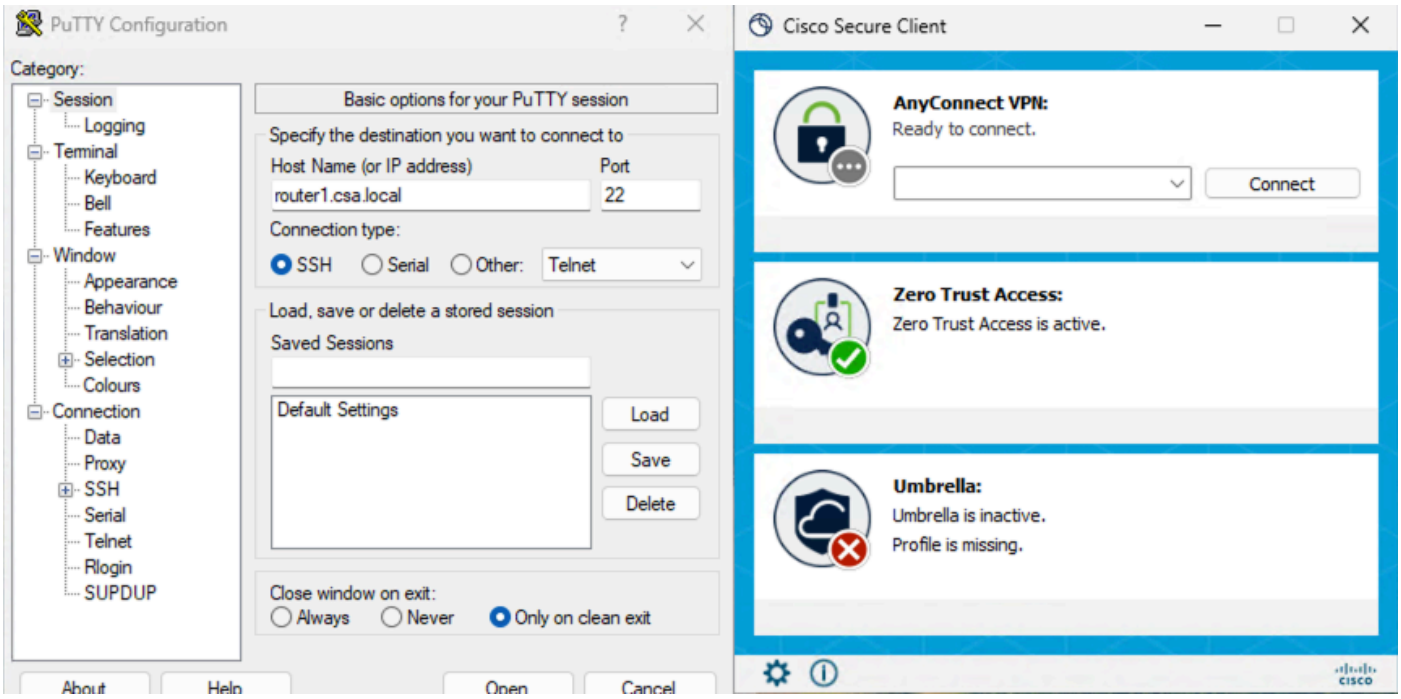
2. Überprüfen Sie, ob FTD über FQDN eine Verbindung zu privaten Ressourcen herstellen kann.

```
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#
```

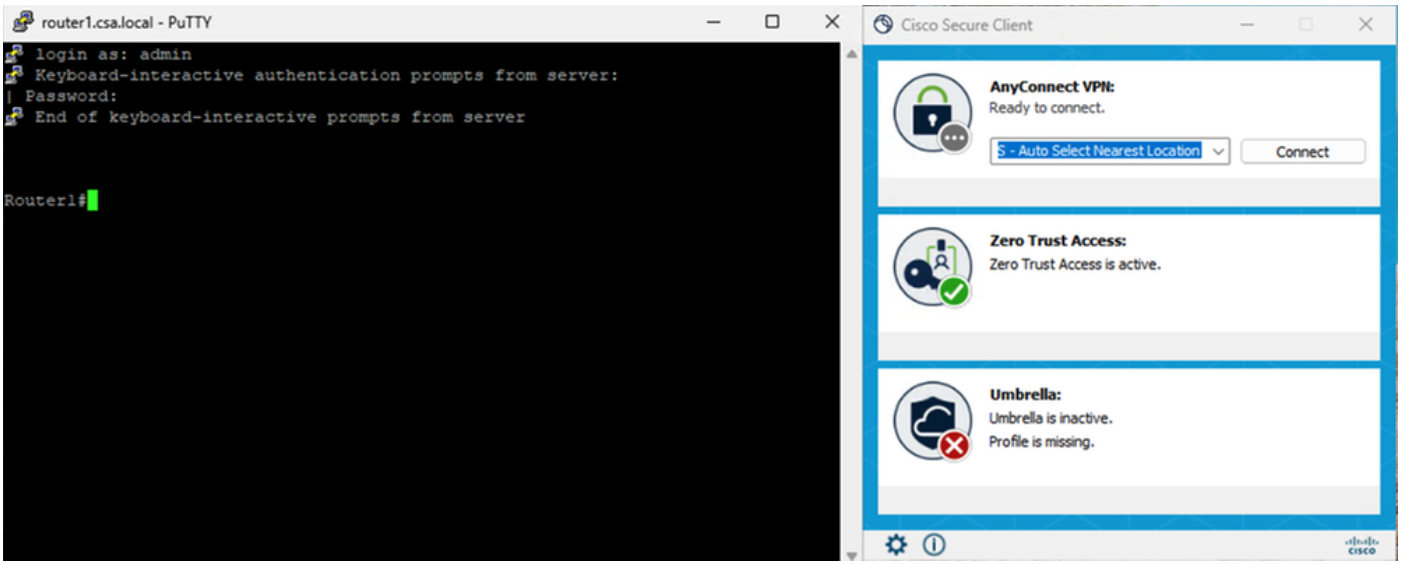
Sicherer Zugriff - PR-Tests

3. Testen der SSH-Verbindung mit der privaten Ressource

Zugriff auf den PR über FQDN

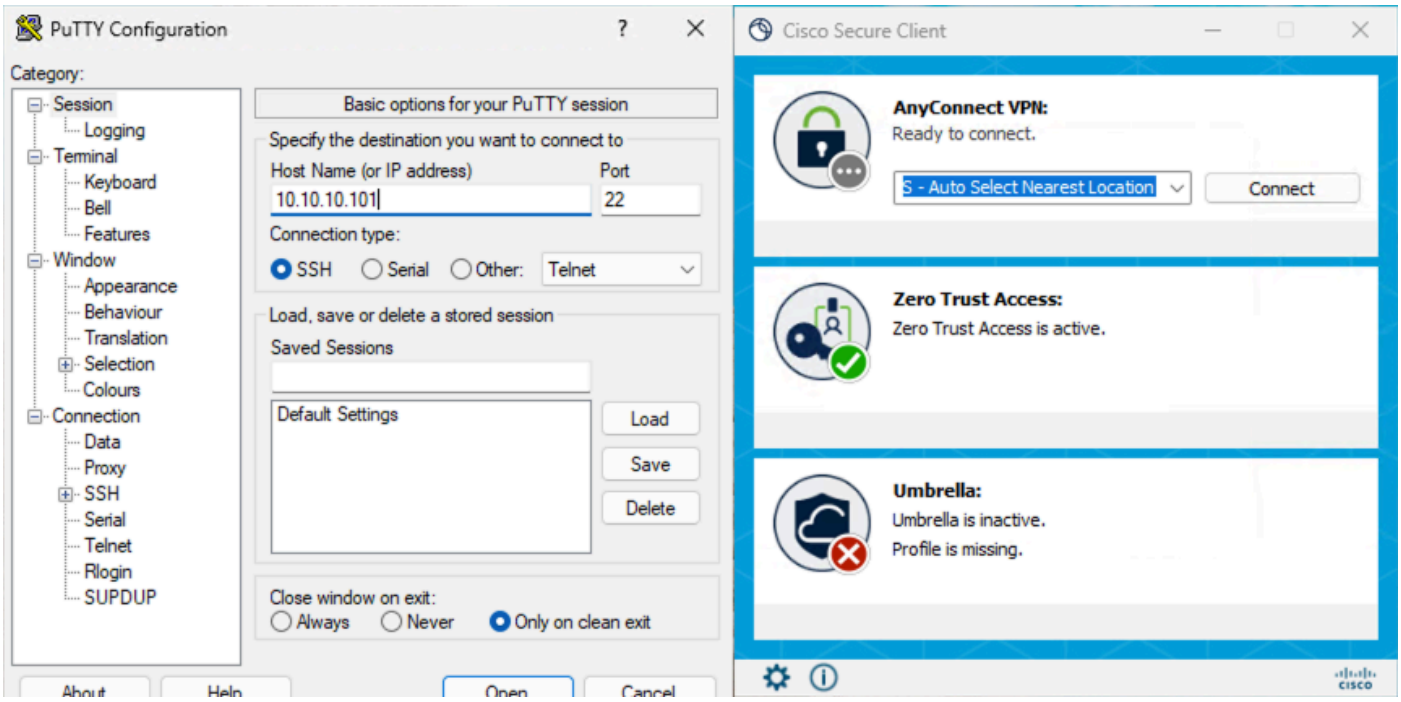


Sicherer Zugriff - PR-Tests

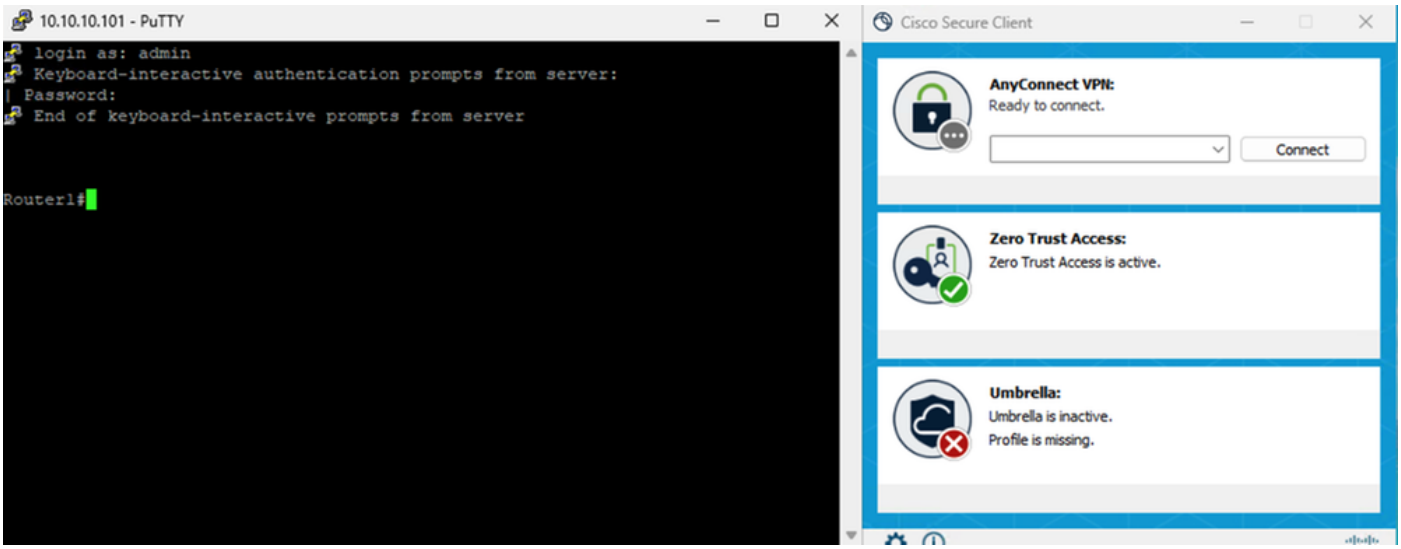


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse

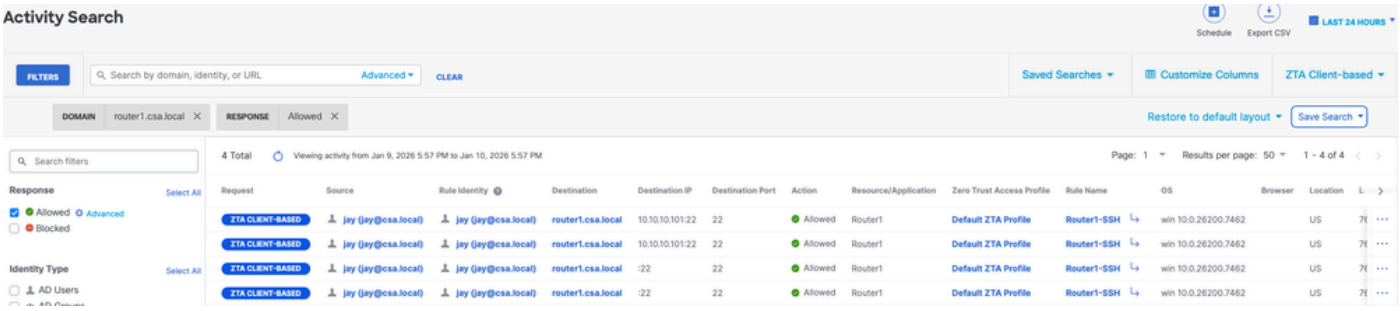


Sicherer Zugriff - PR-Tests

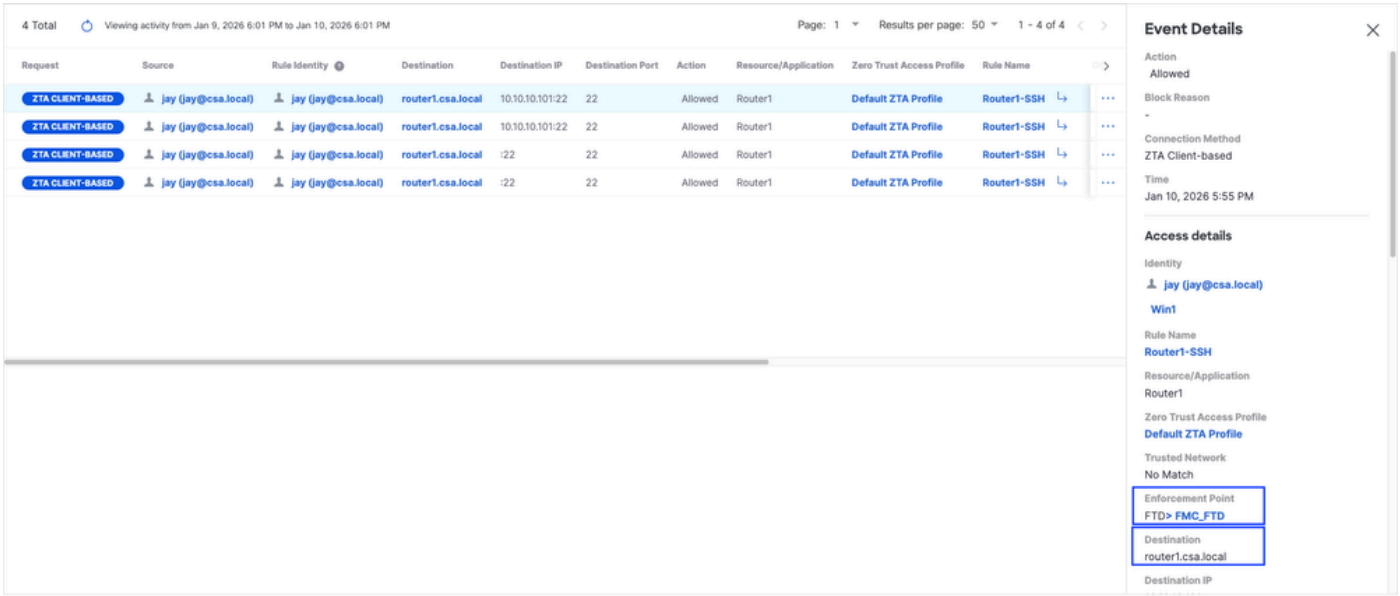


Sicherer Zugriff - PR-Tests

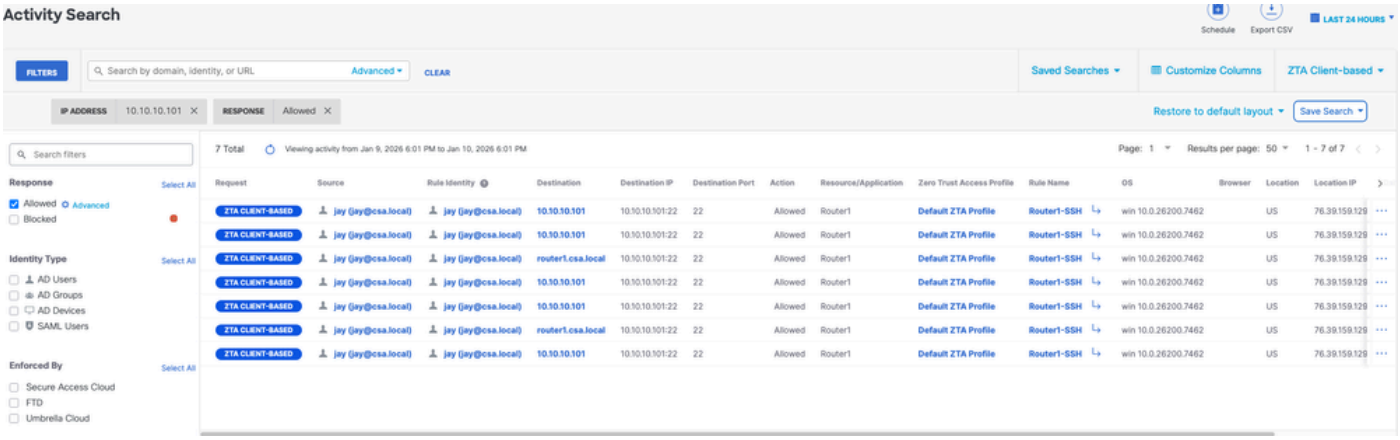
4. Protokolle für die Suche nach sicheren Zugriffsaktivitäten überprüfen



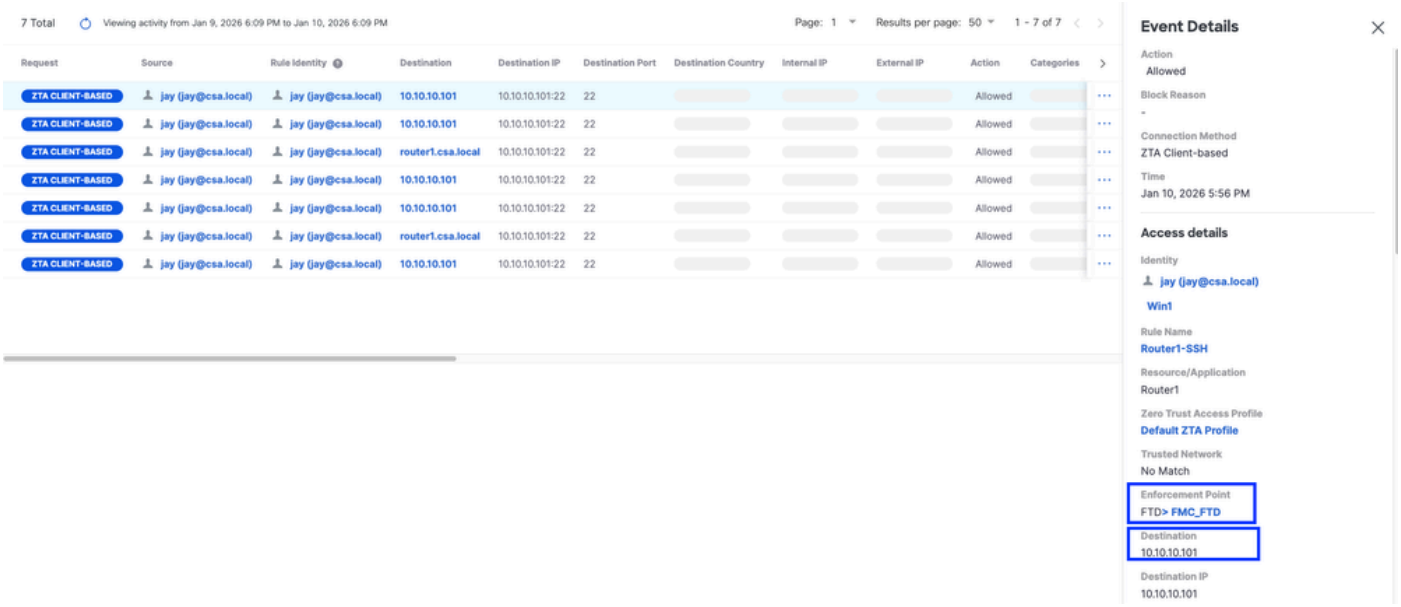
Sicherer Zugriff - Aktivitätssuche



Sicherer Zugriff - Aktivitätssuche

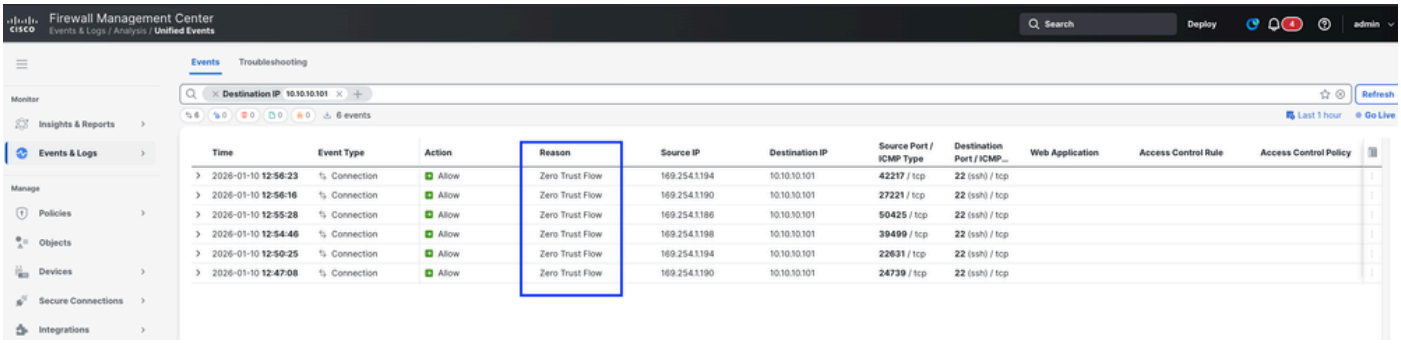


Sicherer Zugriff - Aktivitätssuche



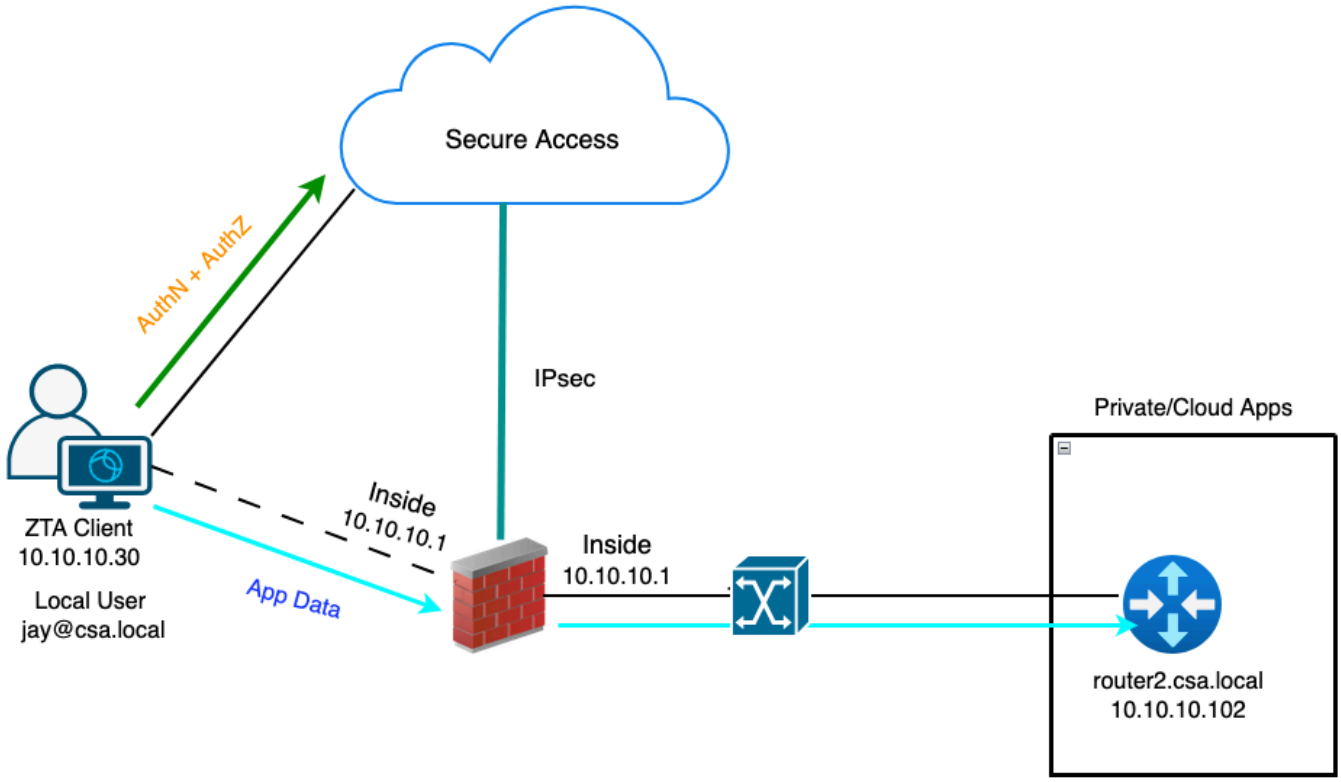
Sicherer Zugriff - Aktivitätssuche

5. Überprüfen von FMC-Verbindungsereignissen



Testfall 3 - Lokaler Benutzer - Lokale Durchsetzung

Der Zugriff auf eine private Ressource über die lokale Durchsetzung als lokaler Benutzer erfolgt bei dieser Art der Richtlinienauswertung für den sicheren Zugriff, die Anwendungsdaten bleiben jedoch für FTD lokal. Zum Beispiel, ein ZTA eingeschriebenen Client oder Benutzer mit Heimnetzwerk verbunden und versucht, eine private Ressource, die hinter FTD innerhalb Schnittstelle zugreifen . Wenn sich die private Ressource hinter der DMZ oder einer anderen FTD-Schnittstelle befindet, müssen wir eine Zugriffsregel auf der FTD erstellen, um den Datenverkehr zwischen der Client-IP oder dem Netzwerk und der privaten Ressource zuzulassen.

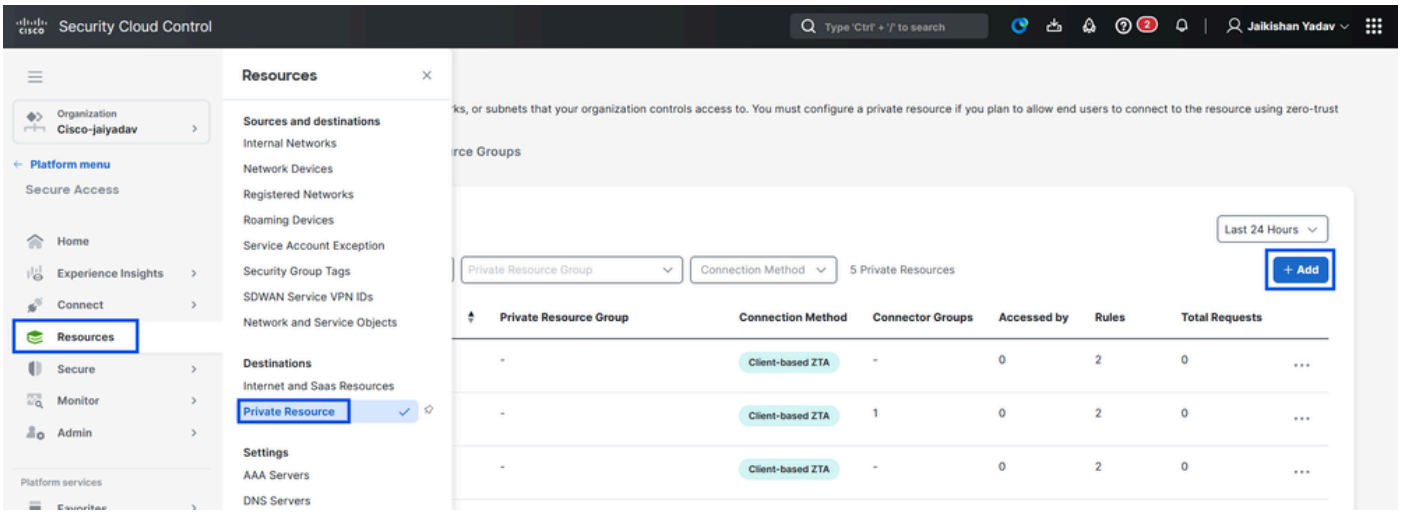


Universelle ZTA - Topologie der Testfälle

Schritt 1 - Definieren einer privaten Ressource für sicheren Zugriff

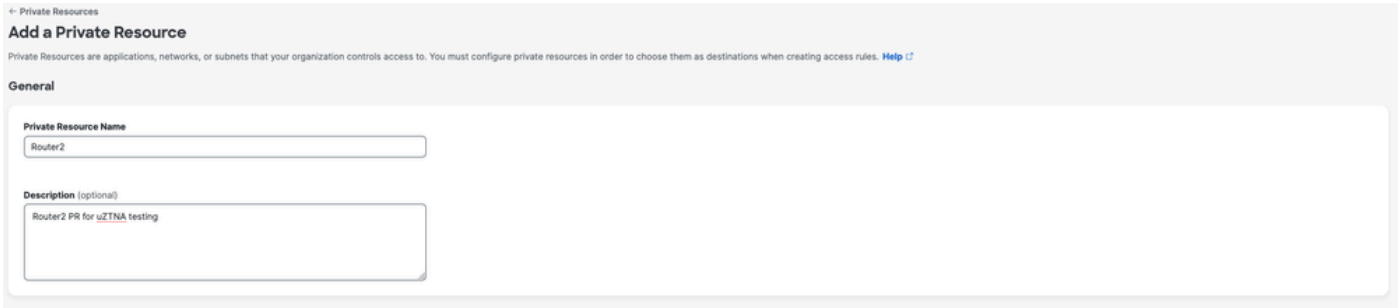
Konfigurieren einer privaten Ressource für den Zugriff über ein bei Zero Trust Access (ZTA) angemeldetes Gerät mit Cloud-Durchsetzung

1. Navigieren Sie zu Ressourcen > Ziele > Private Ressourcen > und klicken Sie auf +Hinzufügen.



Sicherer Zugriff - Konfiguration privater Ressourcen

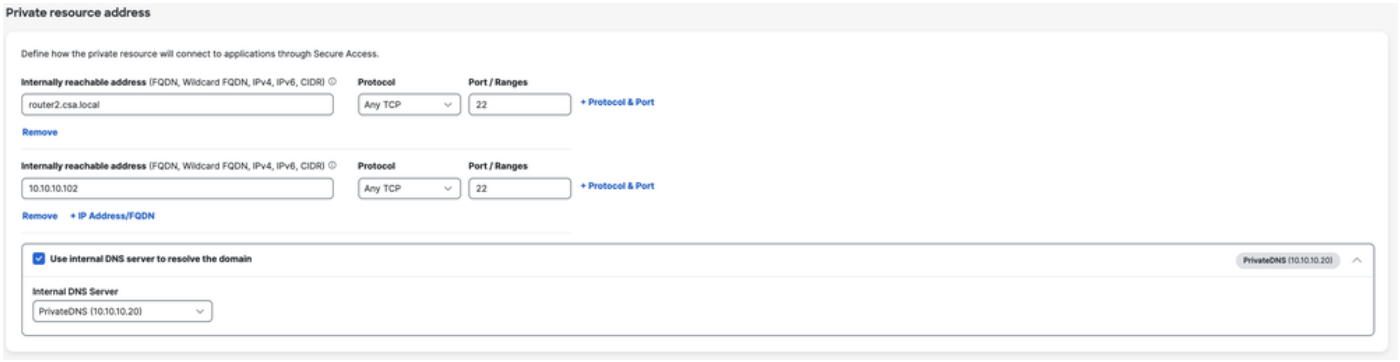
2. Geben Sie für Private Resource Name einen sinnvollen Namen für die Ressource ein. Für Description empfehlen wir, Informationen wie den Zweck der Ressource oder den Namen des Ressourcenbesitzers anzugeben.



Sicherer Zugriff - Konfiguration privater Ressourcen

3. Geben Sie den FQDN der privaten Ressource ein, auf die Sie zugreifen möchten. Wir können auch die IP-Adresse der privaten Ressource definieren. Weitere Informationen finden Sie unter [Hinzufügen einer privaten Ressource]

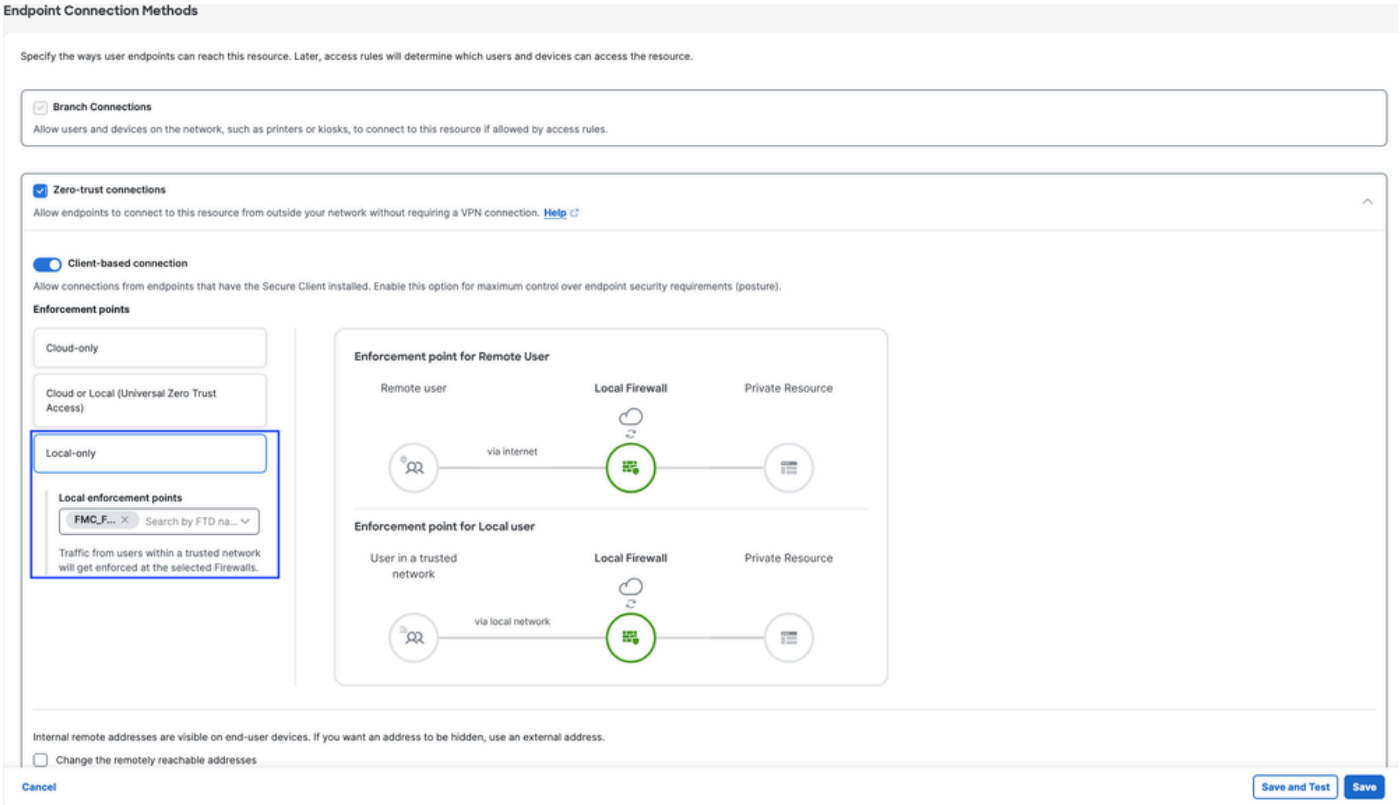
4. Wählen Sie den internen DNS-Server, um die Domäne aufzulösen.



Sicherer Zugriff - Konfiguration privater Ressourcen

5. Endpunktverbindungsmethoden auswählen

6. Wählen Sie FTD als lokale Durchsetzungspunkte



Sicherer Zugriff - Konfiguration privater Ressourcen

Anmerkung: Je nach gewählter Registrierungsart ordnet diese Änderung den PR automatisch dem FTD zu und löst eine Richtlinienbereitstellung aus.

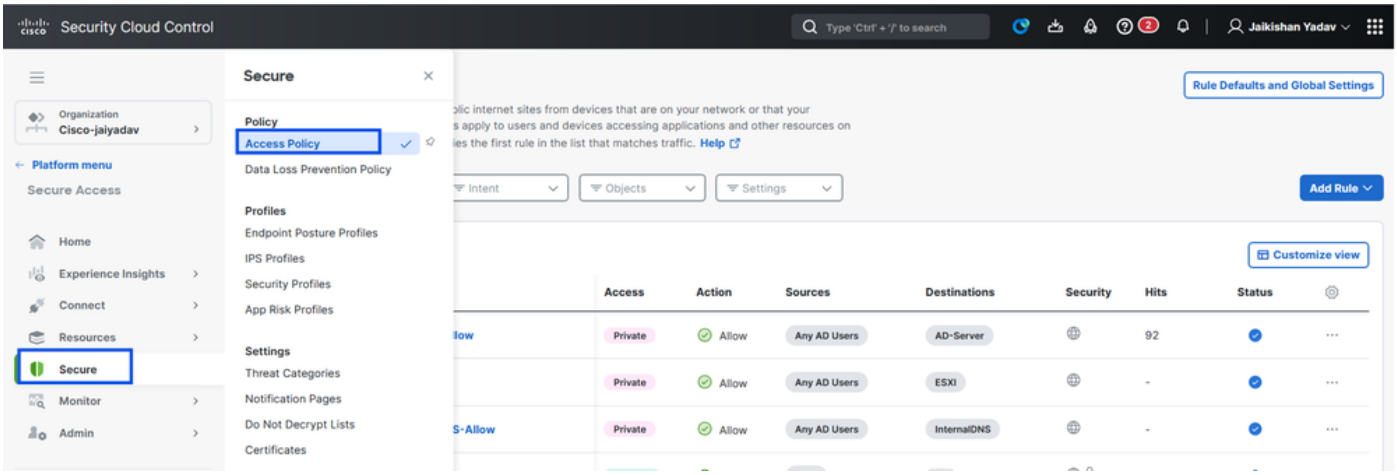
---

7. Klicken Sie auf Save (Speichern).

Schritt 2: Private Zugriffsregel erstellen

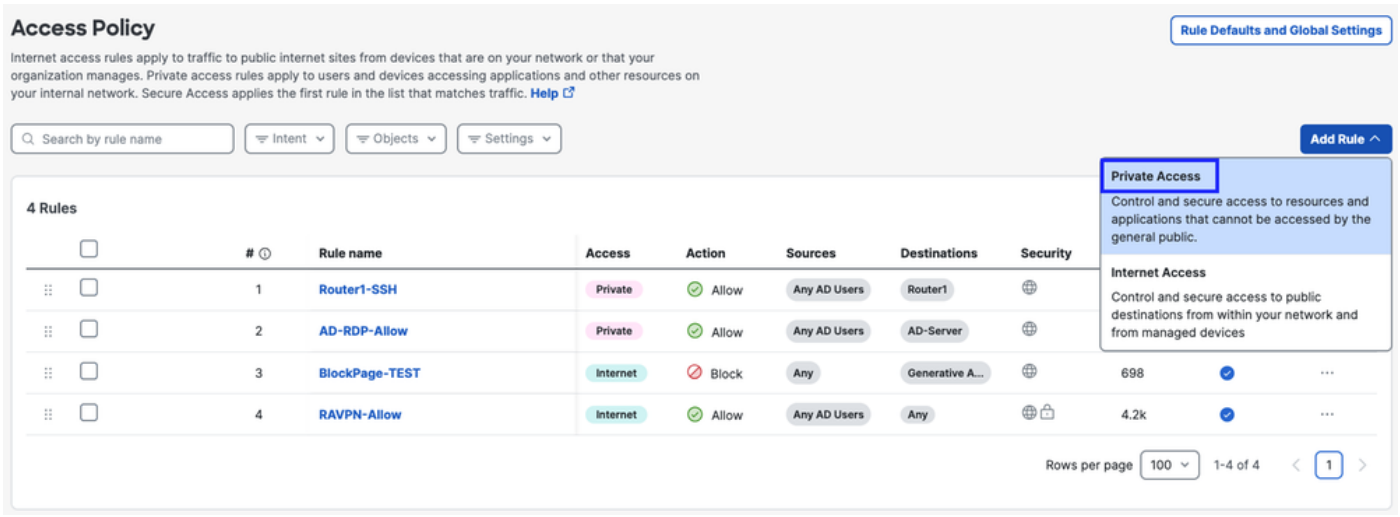
Konfigurieren Sie einen privaten Zugriff auf Secure Access, um Zugriff für Benutzer zu erhalten, die bei Universal ZTA registriert sind. Weitere Informationen finden Sie unter Private Access Rule.

1. Navigieren Sie zu Sicher > Zugriffsrichtlinie



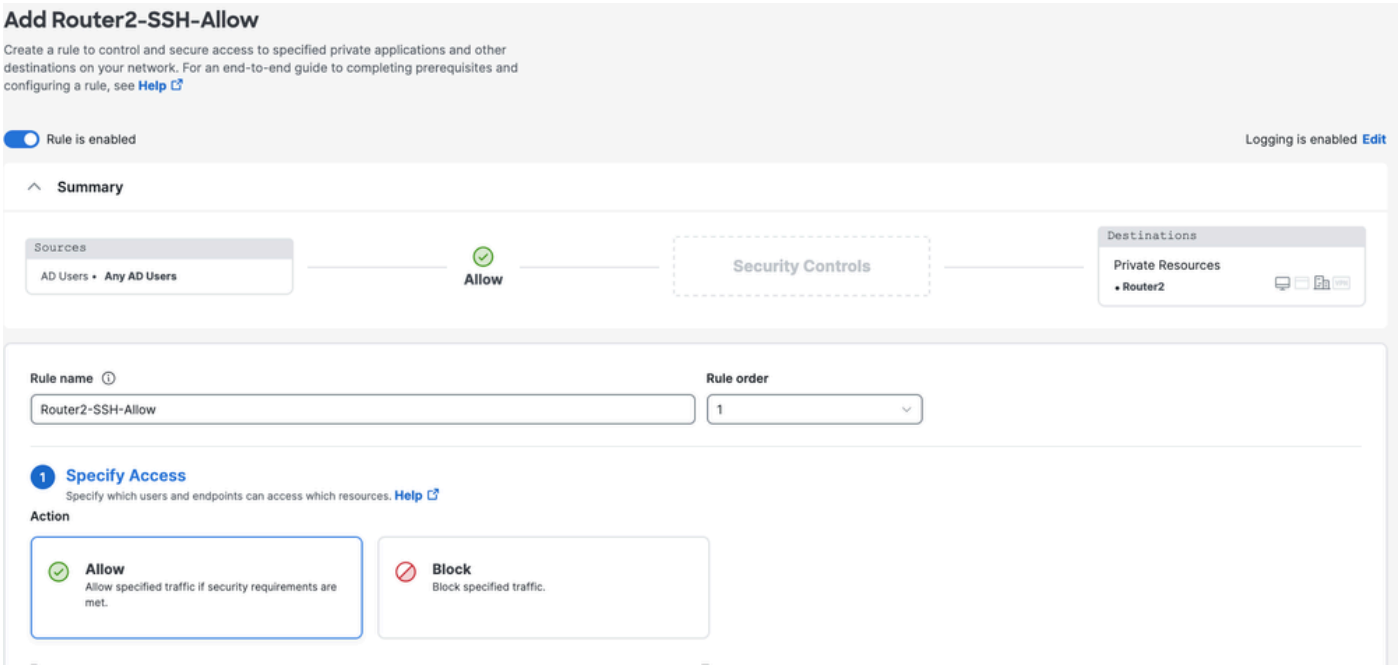
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

2. Klicken Sie auf Regel hinzufügen, und wählen Sie dann Privater Zugriff aus.
Oben auf der Regel befindet sich eine Zusammenfassung, die die konfigurierten Komponenten der Regel beschreibt.



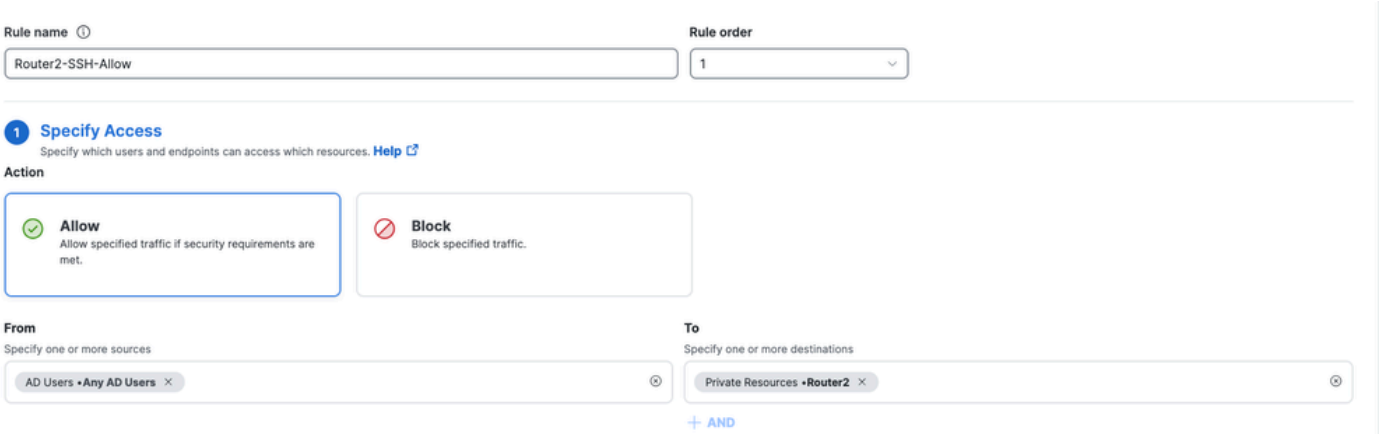
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

3. Hinzufügen eines Regelnamens



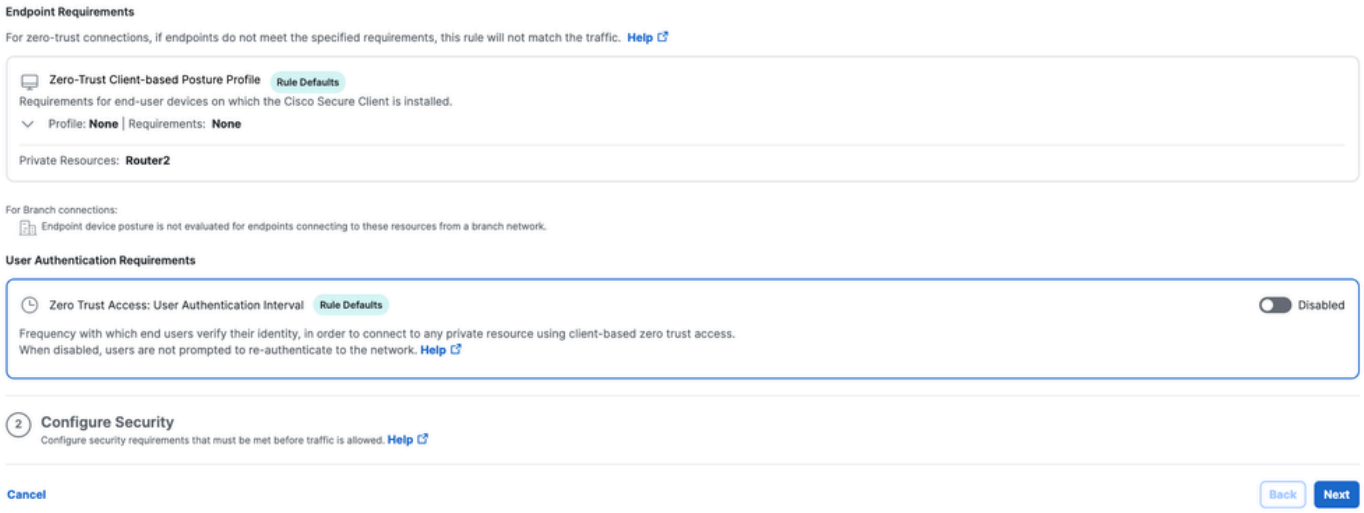
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

4. Wählen Sie die Regelaktion und dann Quelle und Ziel aus.



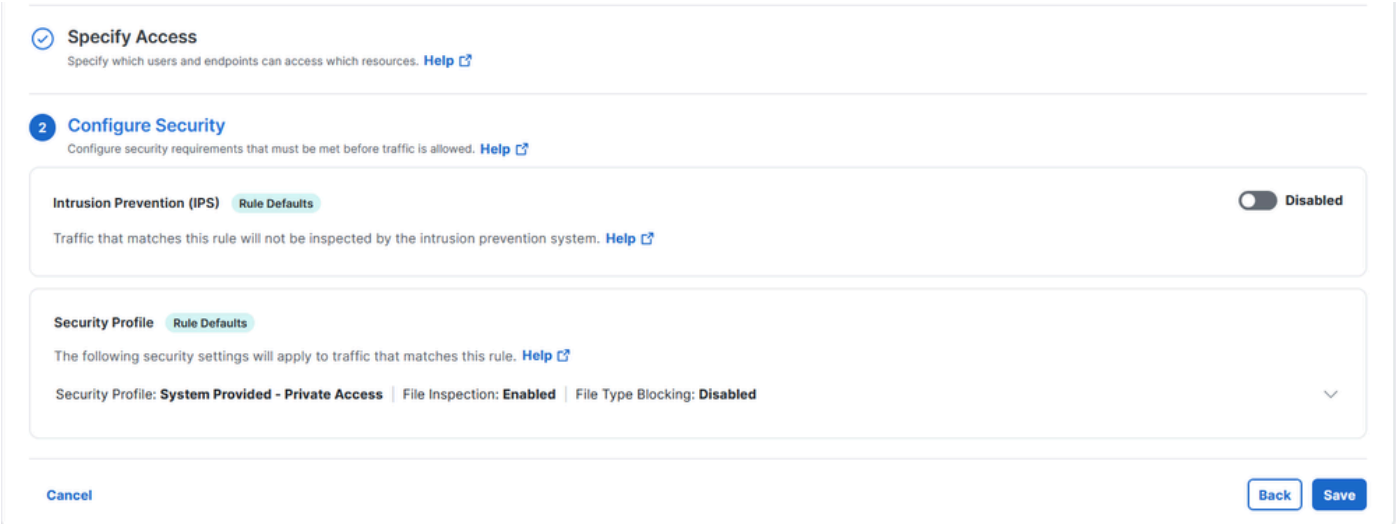
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen



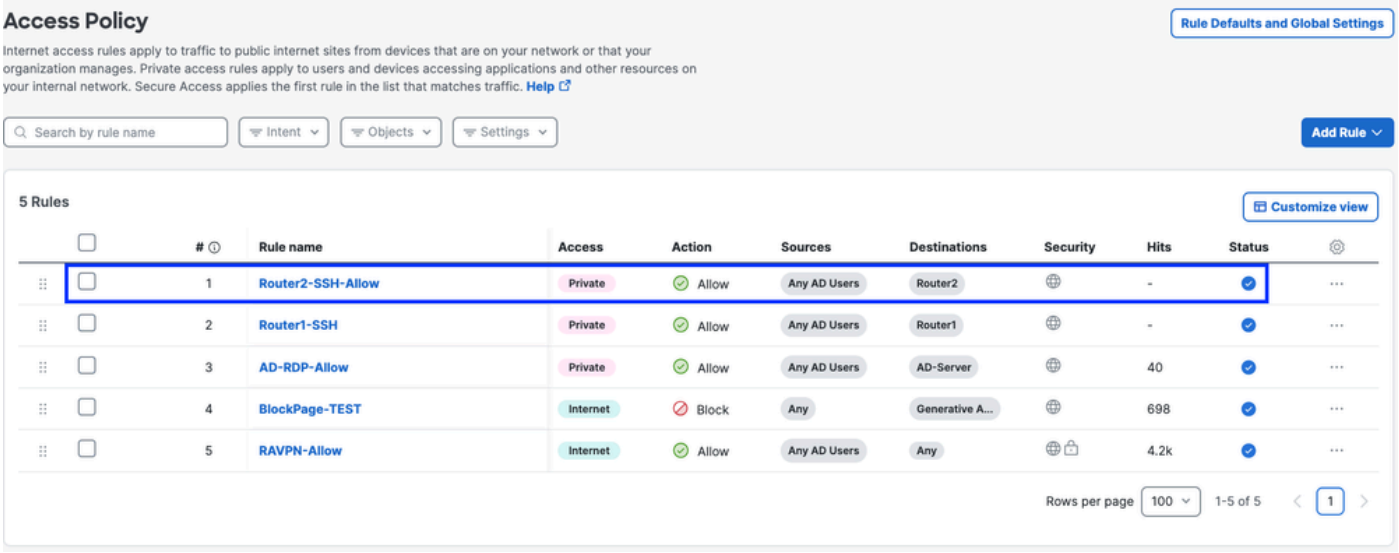
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

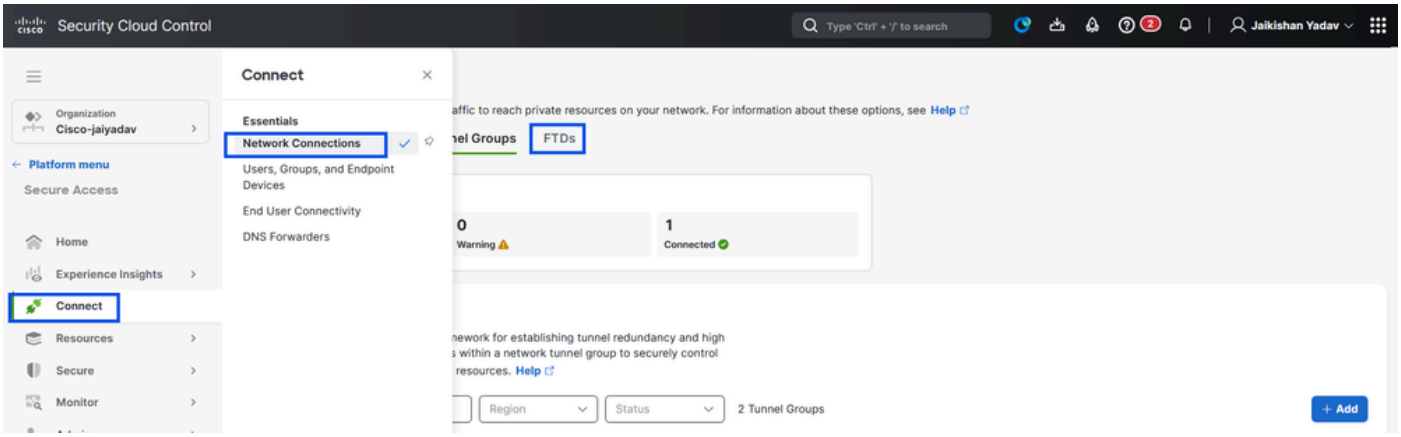
7. Klicken Sie auf Speichern



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

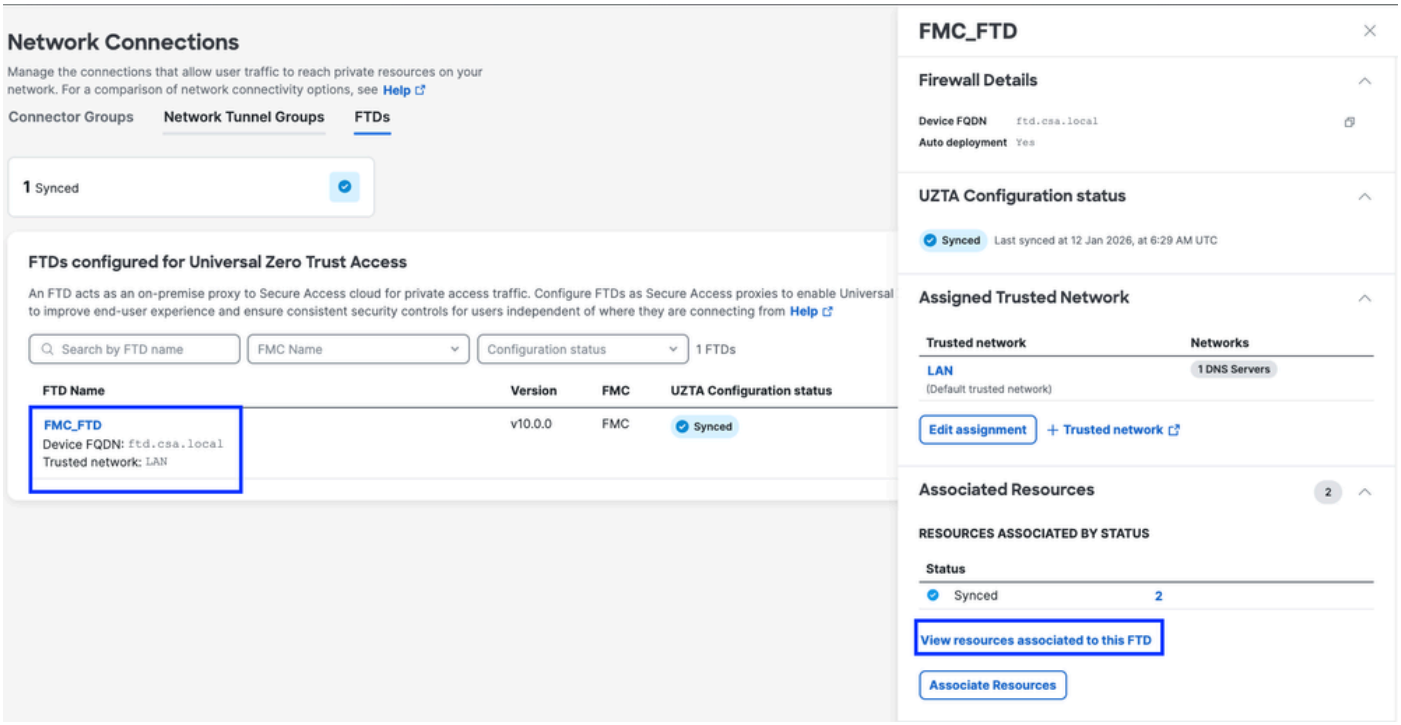
Schritt 3 - Überprüfen der Zuordnung von PR auf dem FTD

1. Navigieren Sie zu Verbinden > Netzwerkverbindungen > FTDs

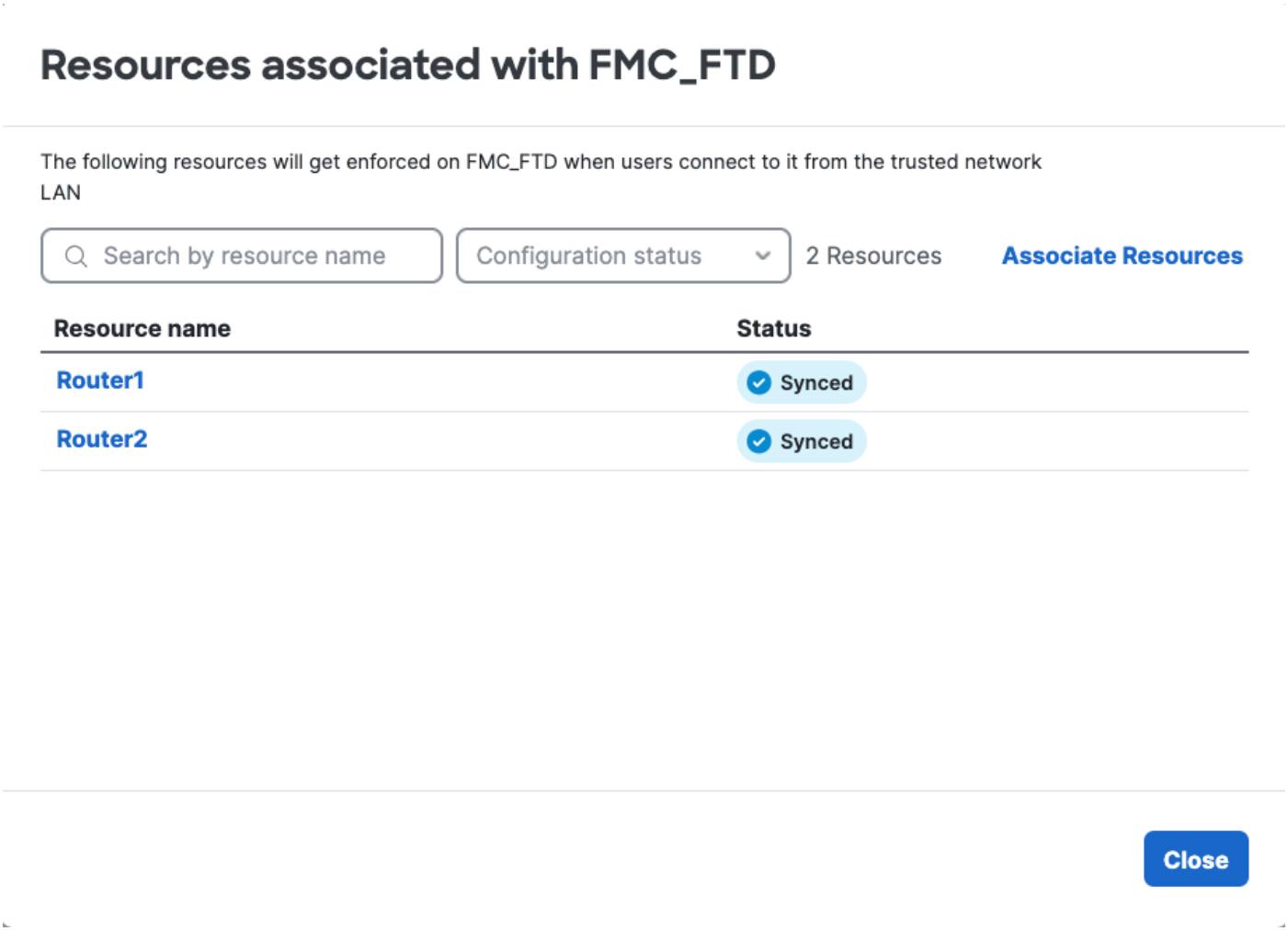


Sicherer Zugriff - PR-Verifizierung

2. Klicken Sie auf FTD > Ressourcen anzeigen, die diesem FTD zugeordnet sind.

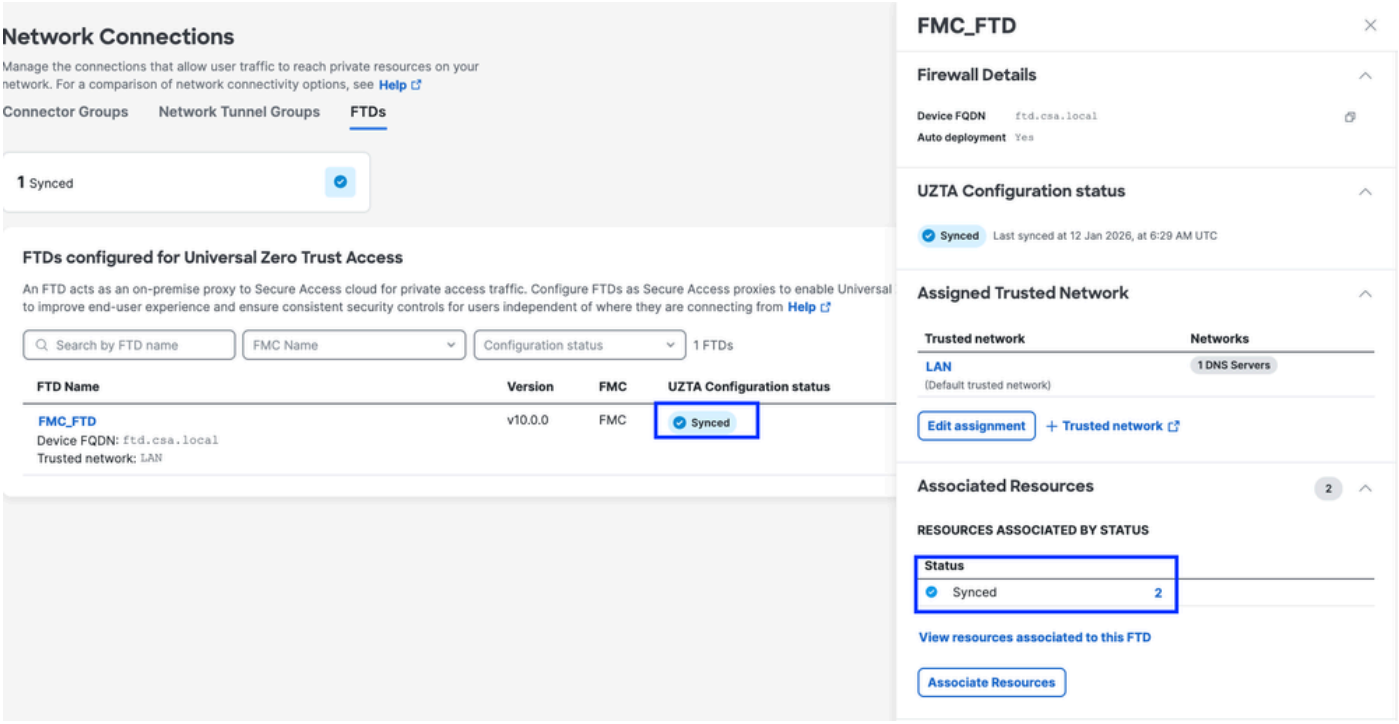


Sicherer Zugriff - PR-Verifizierung



3. Klicken Sie auf Schließen

4. Vergewissern Sie sich, dass der Status , Associated Resource (Zugehörige Ressource) und Configuration (Konfiguration) den Status "Synchronisiert" aufweist.



Sicherer Zugriff - PR-Verifizierung

5. Überprüfen Sie, ob die Konfiguration auf FTD übertragen wurde.

Melden Sie sich bei der FTD-CLI an, und navigieren Sie zum LINA-Modus.

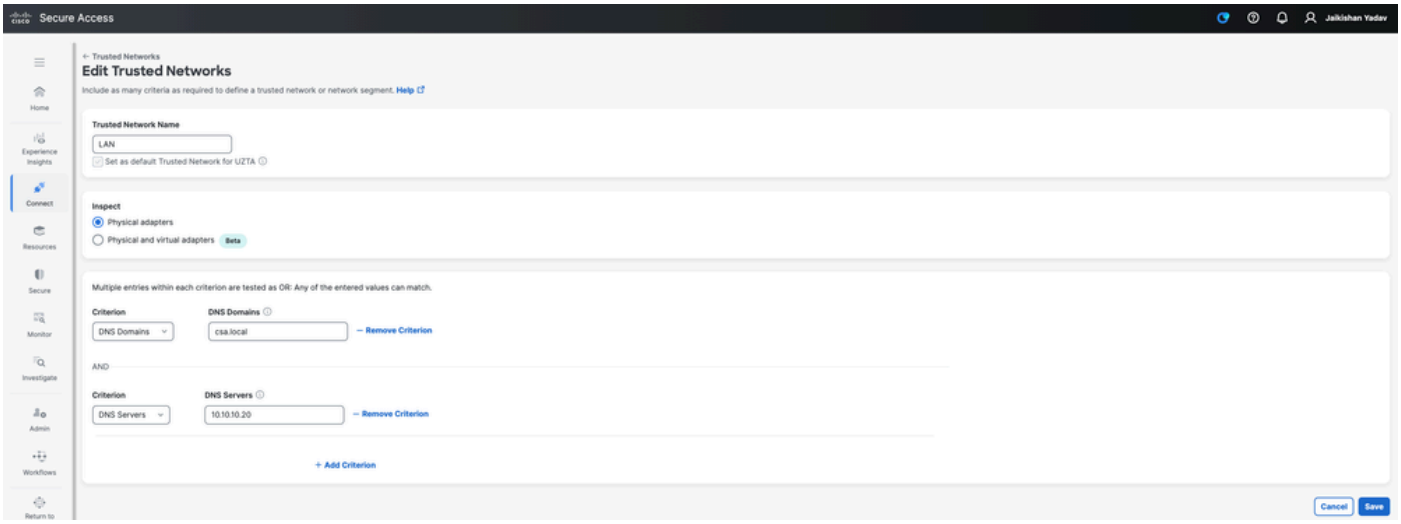
show running-config object application

```
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
```

Sicherer Zugriff - PR-Verifizierung

Schritt - 4 Konfigurieren " Vertrauenswürdige Netzwerke oder ZTA-Einstellungen verwalten"

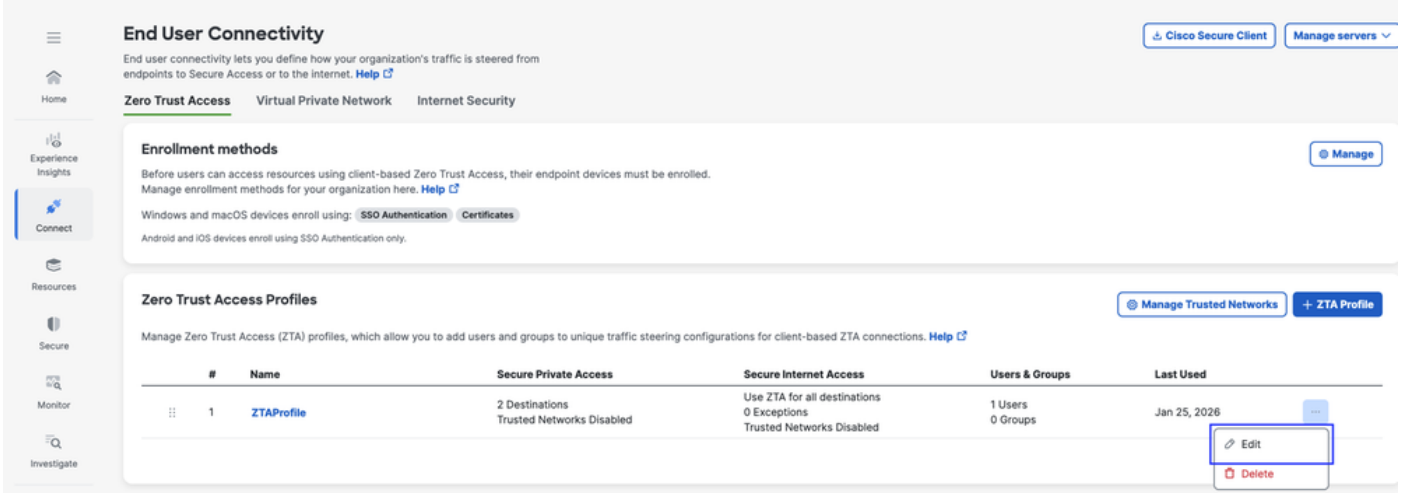
Navigieren Sie zu Verbinden > Endbenutzerverbindungen > Zugriff ohne Vertrauensstellung > ZTA-Einstellungen, und konfigurieren Sie vertrauenswürdige Netzwerke.



Sicherer Zugriff - TND-Konfiguration

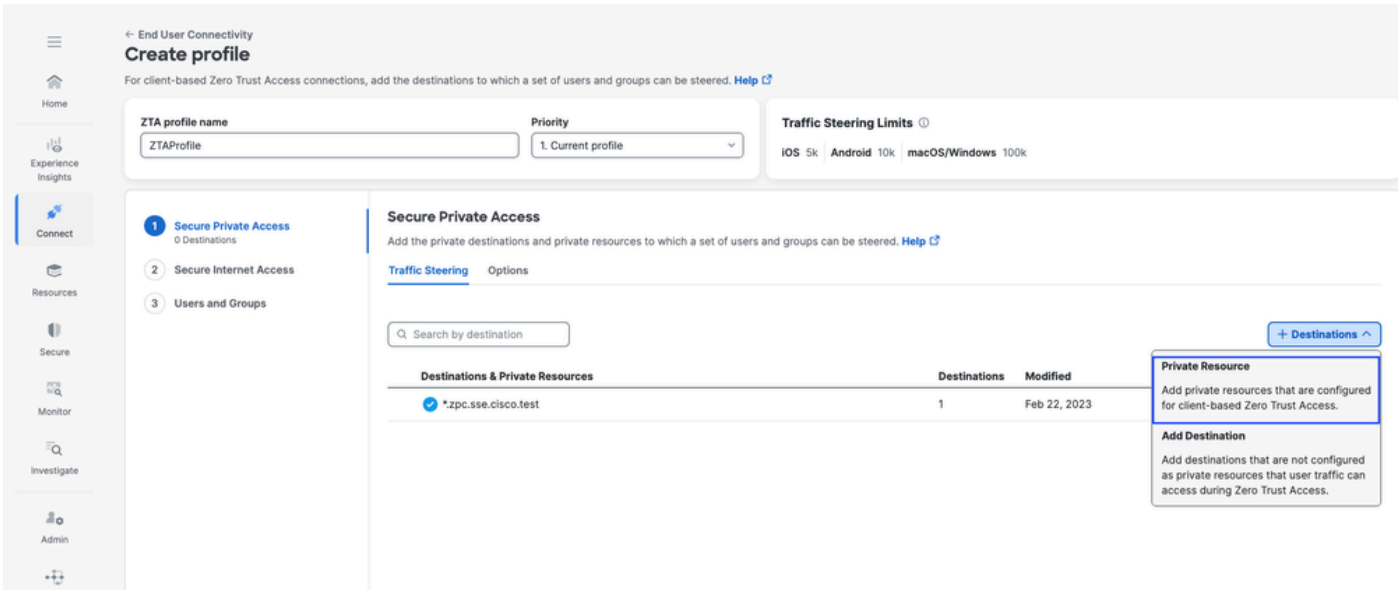
Schritt -5 Hinzufügen einer privaten Ressource zum ZTA-Profil

1. Navigieren Sie zu Verbinden > Endbenutzerverbindung > Zugriff ohne Vertrauensstellung, und klicken Sie auf 3 Punkte, um das ZTA-Profil zu bearbeiten.

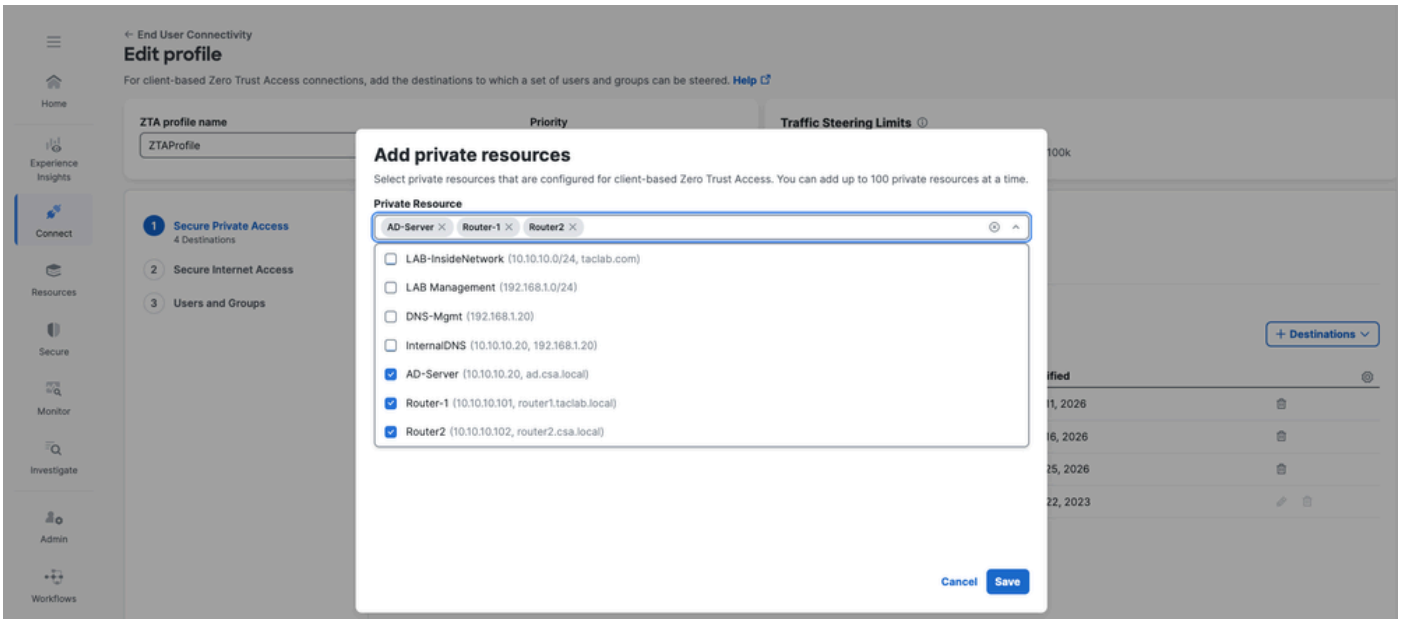


Sicherer Zugriff - ZTA-Profil

2. Fügen Sie die private Ressource hinzu

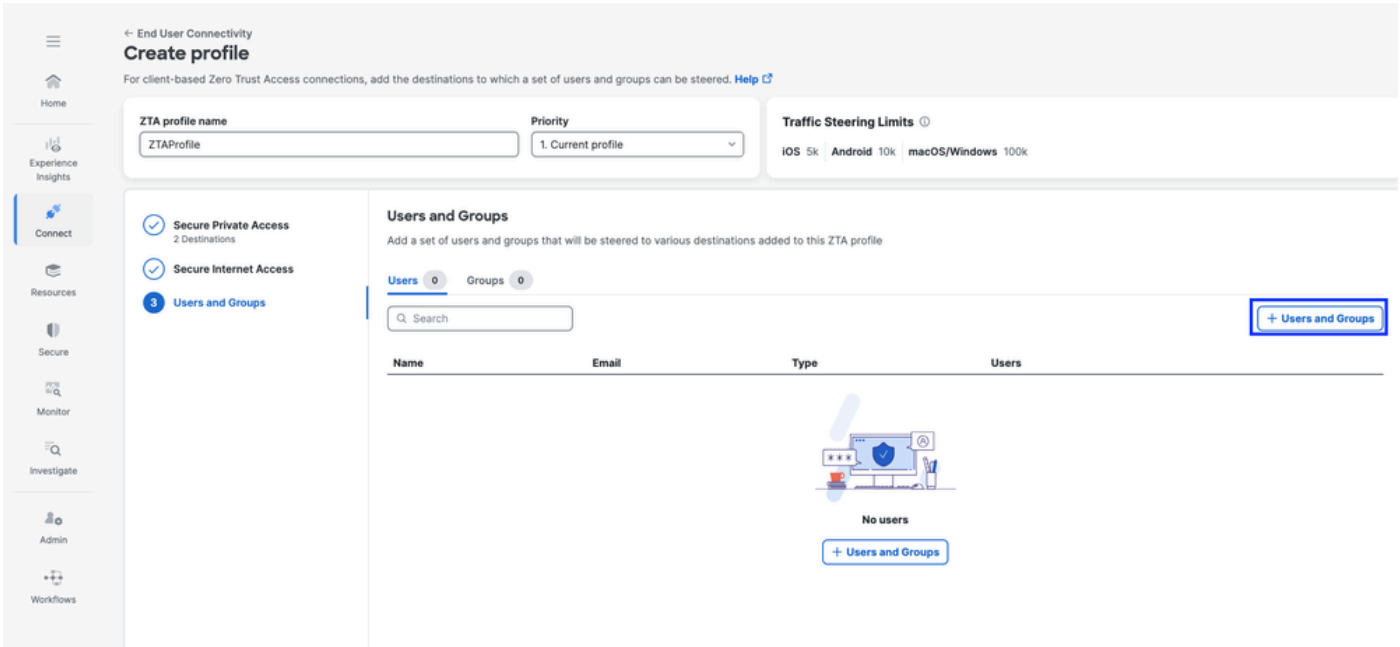


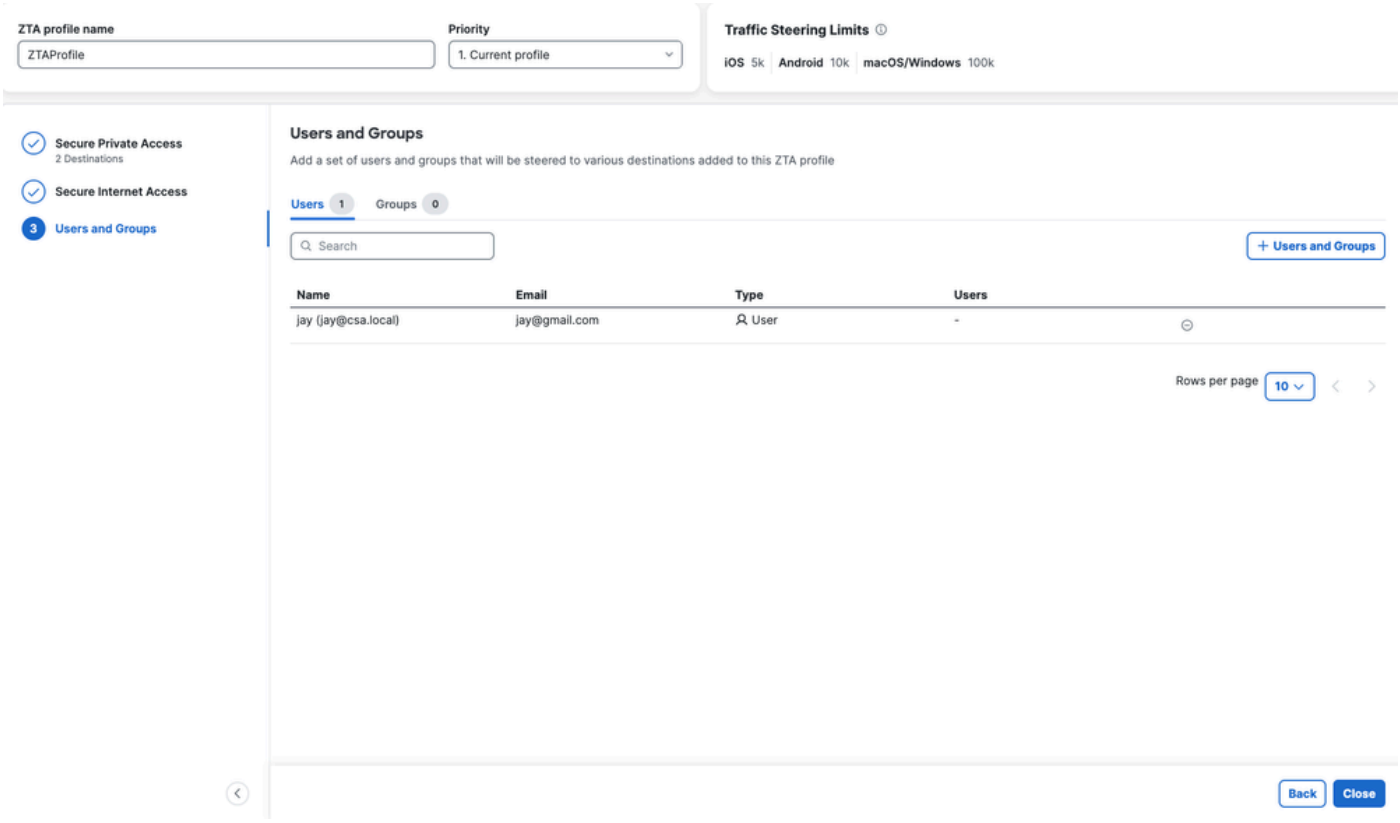
Sicherer Zugriff - ZTA-Profil



Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen

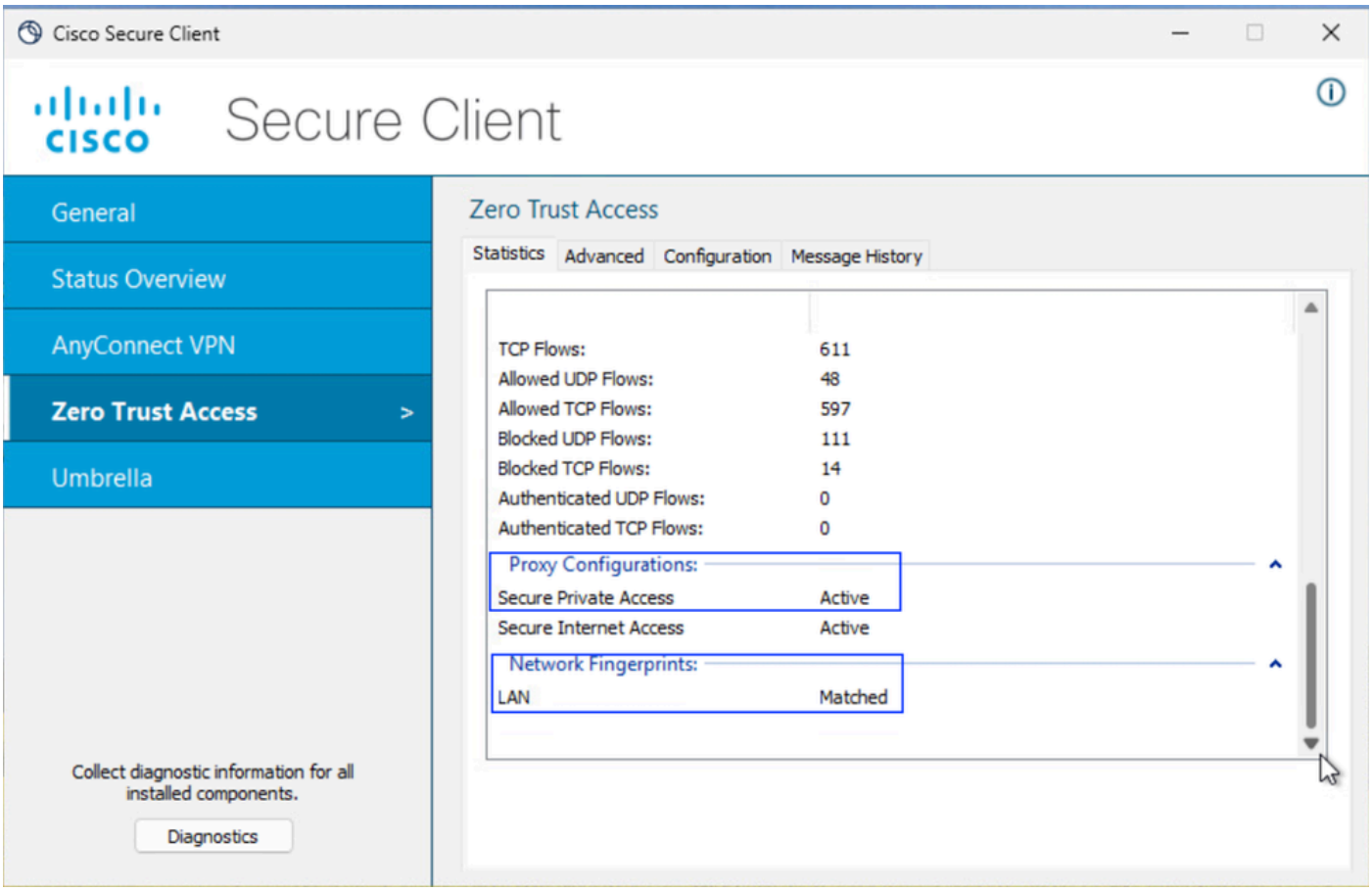




Sicherer Zugriff - ZTA-Profil

Schritt - 6 Überprüfen des Zugriffs auf die private Ressource

1. Überprüfen Sie den Netzwerk-Fingerprint für ZTA TND.



2. Überprüfen, ob der Remote-Benutzer den FTD FQDN auflösen kann

```
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
```

Sicherer Zugriff - PR-Tests

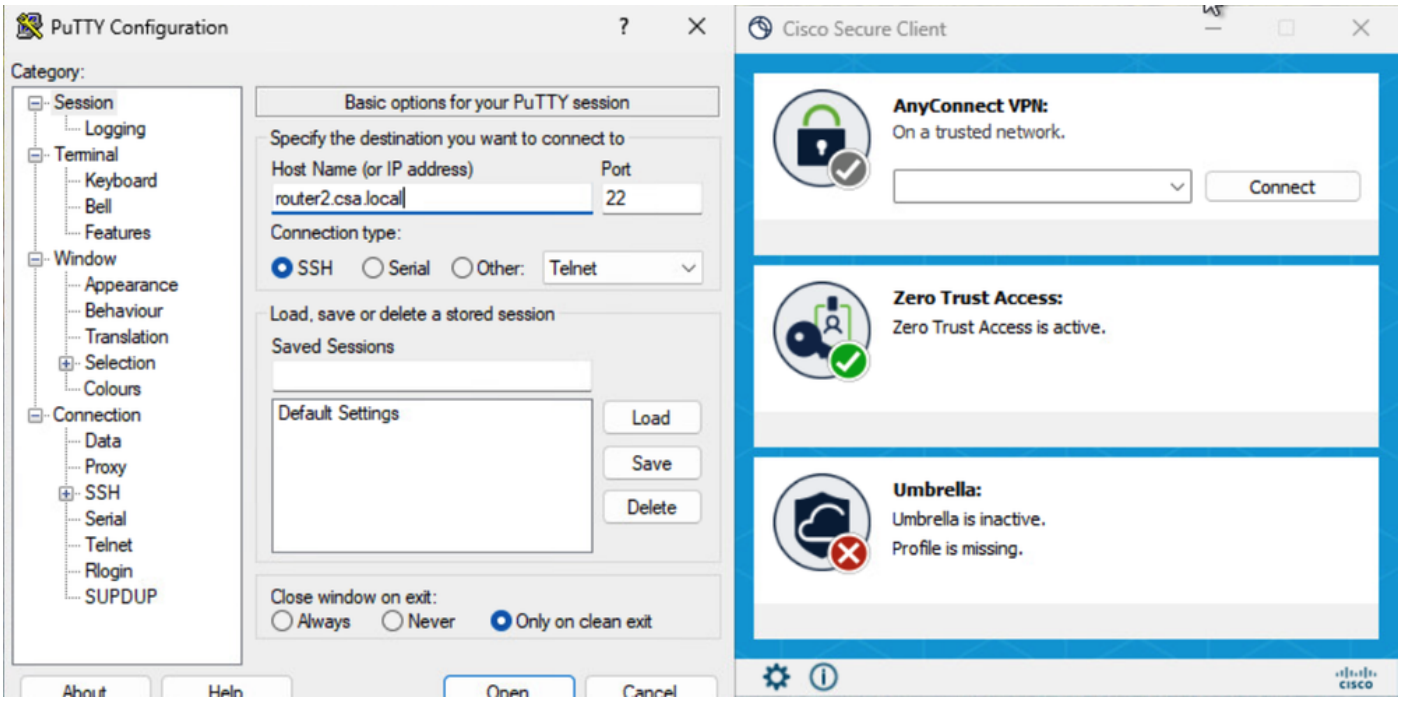
3. Überprüfen Sie, ob FTD über FQDN eine Verbindung zu einer privaten Ressource herstellen kann.

```
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#
```

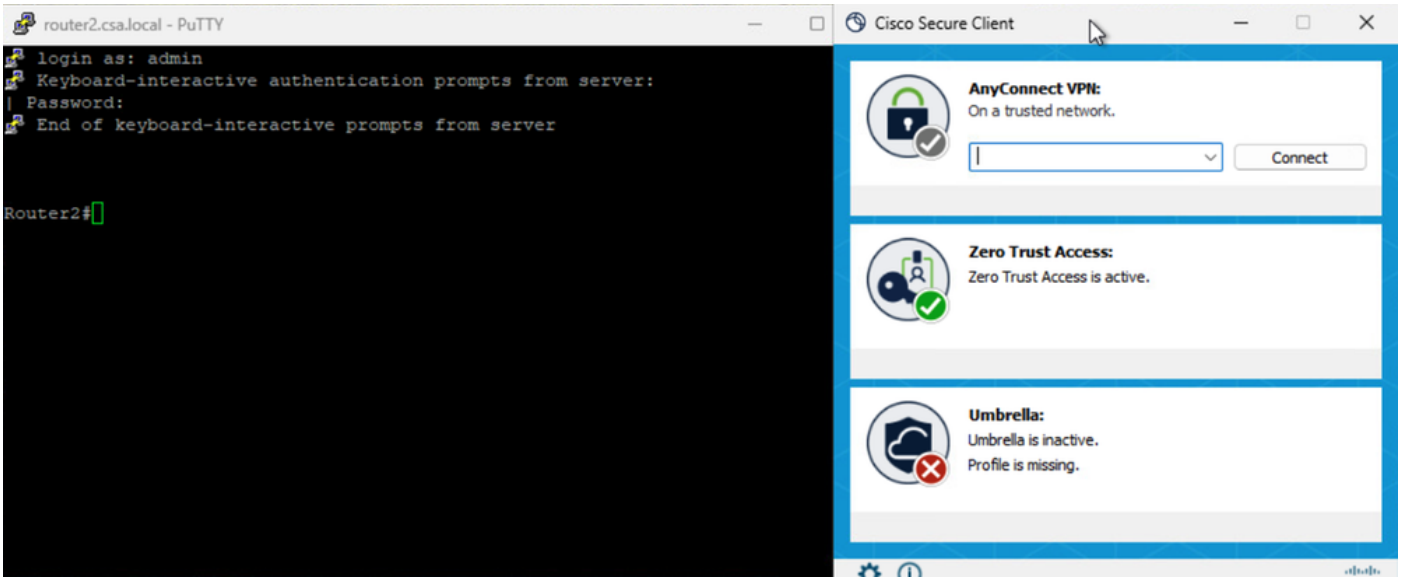
Sicherer Zugriff - PR-Tests

4. Testen der SSH-Verbindung mit der privaten Ressource

Zugriff auf den PR über FQDN

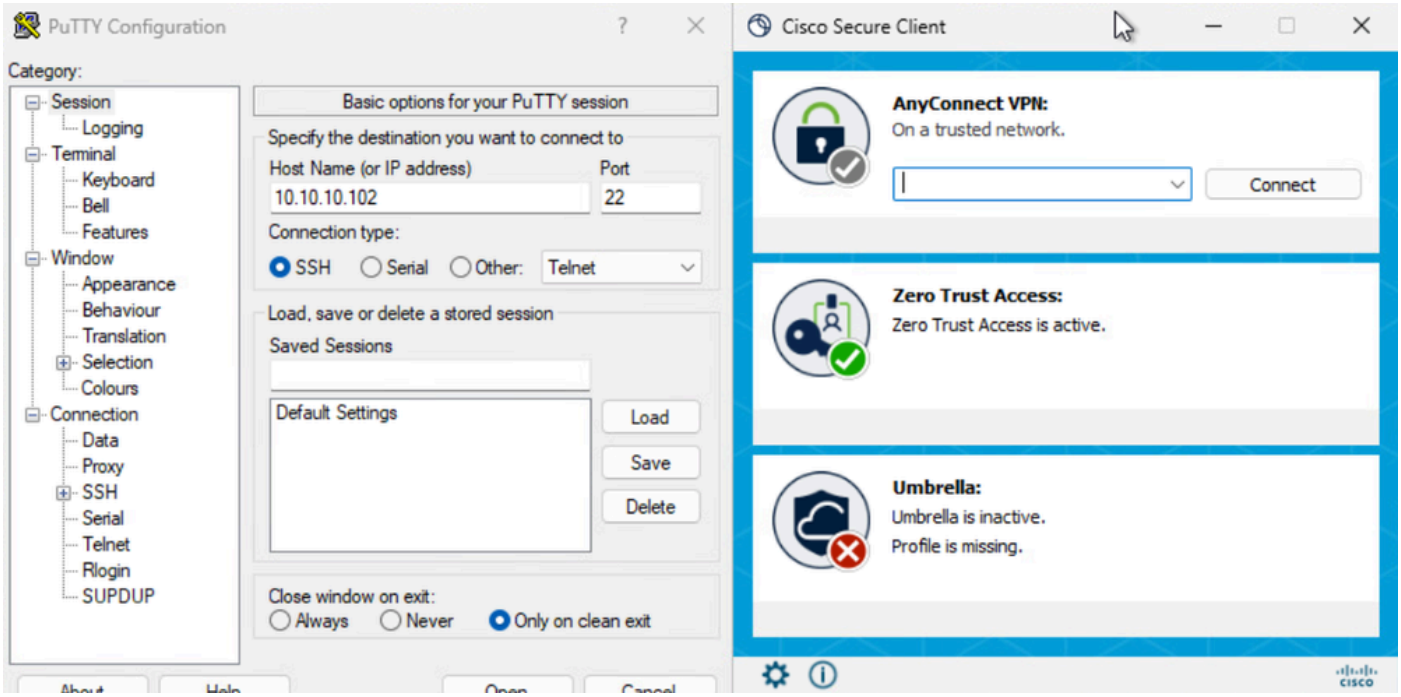


Sicherer Zugriff - PR-Tests

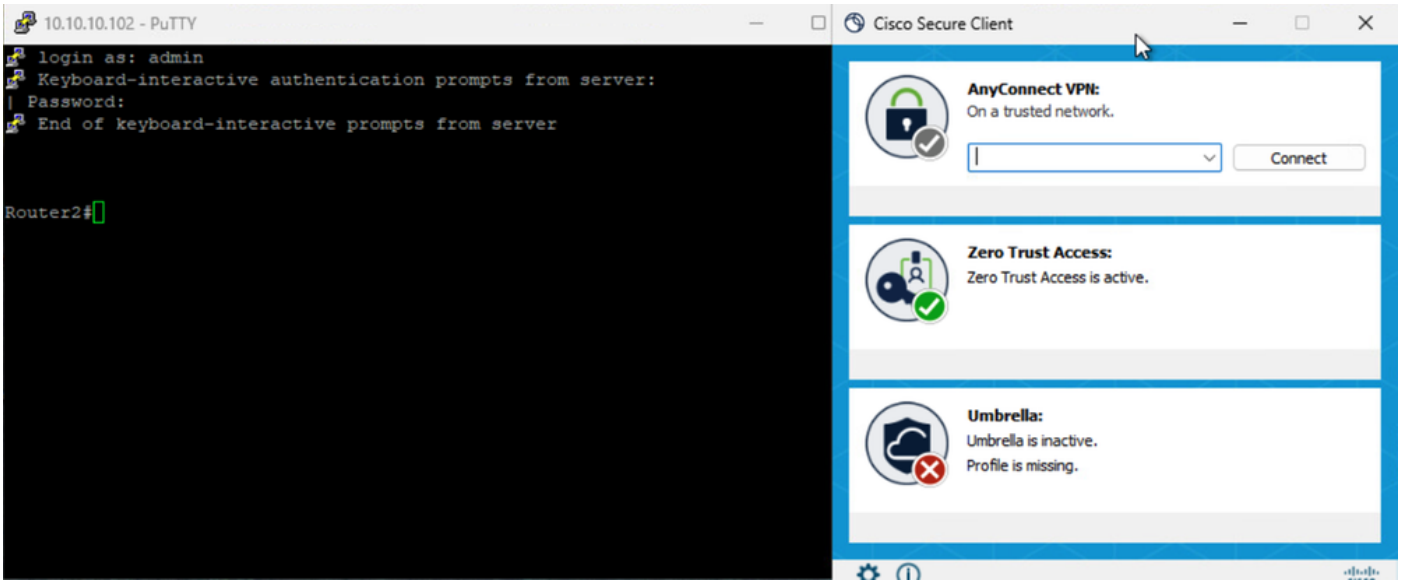


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse

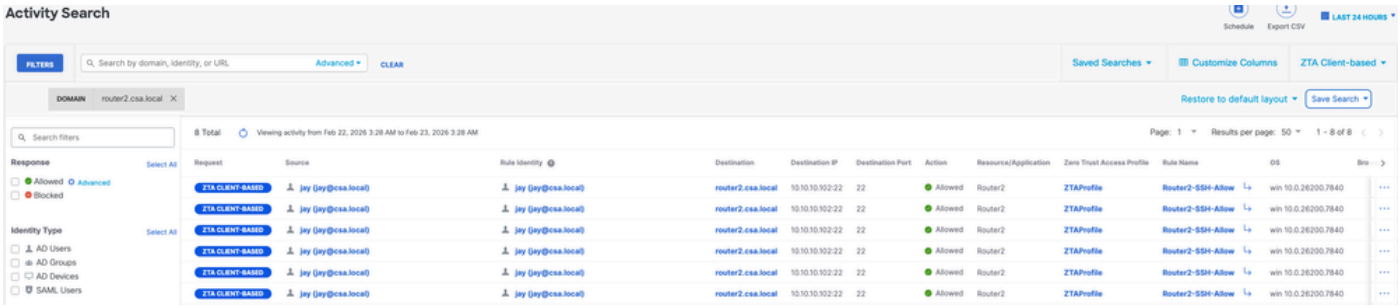


Sicherer Zugriff - PR-Tests

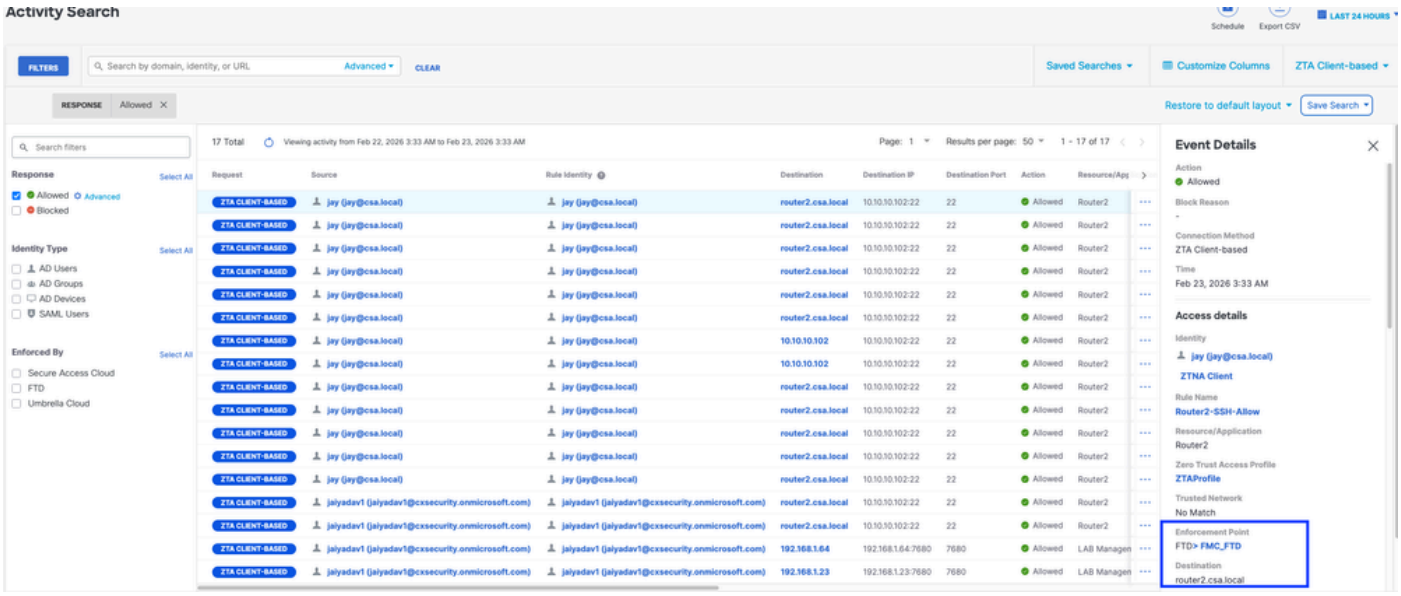


Sicherer Zugriff - PR-Tests

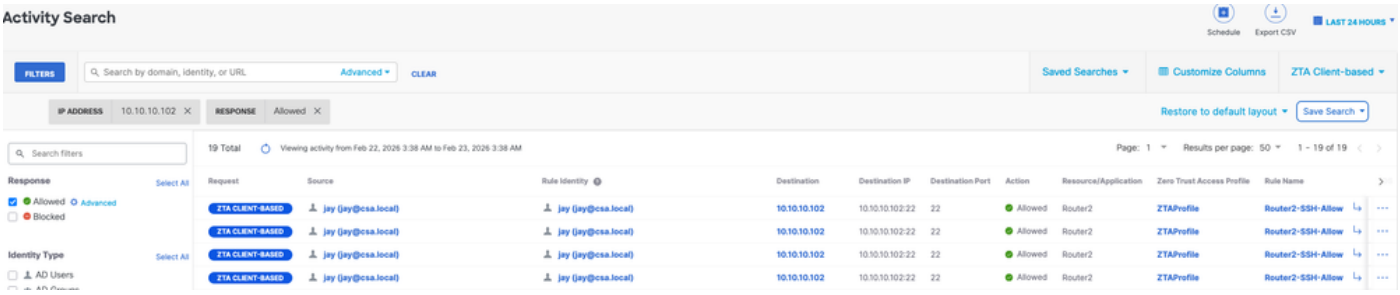
5. Überprüfen der Suchprotokolle für Aktivitäten mit sicherem Zugriff



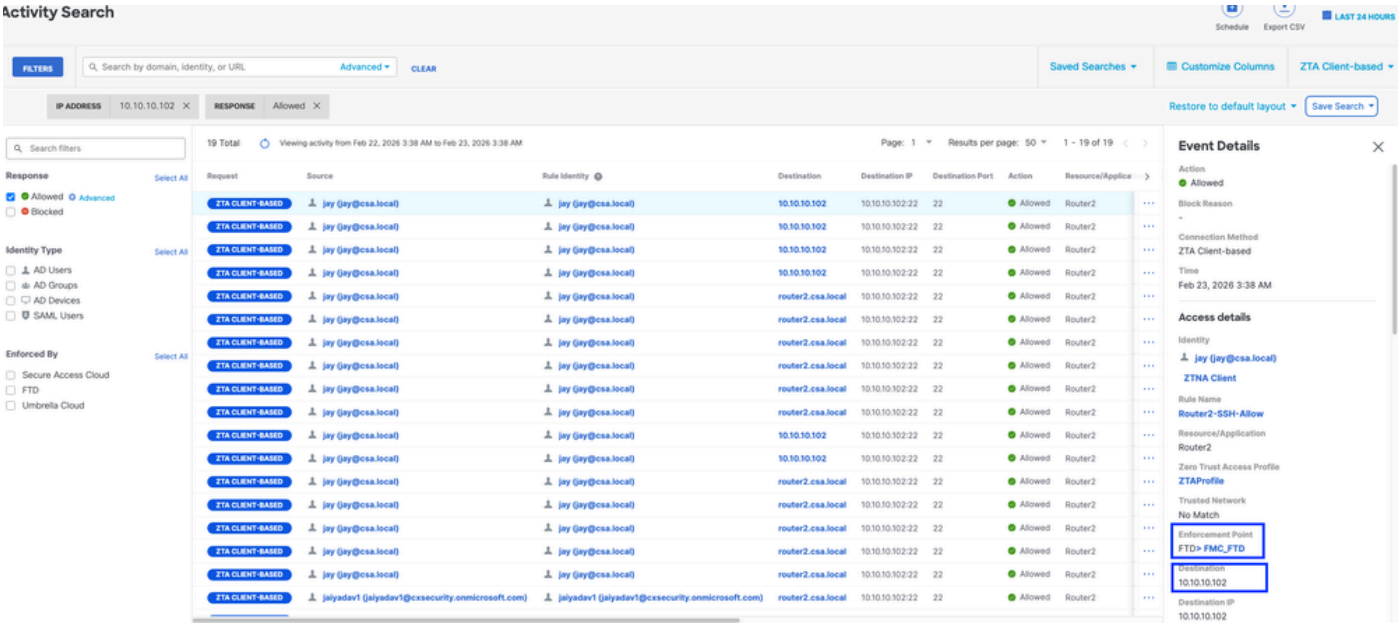
Sicherer Zugriff - Aktivitätssuche



Sicherer Zugriff - Aktivitätssuche

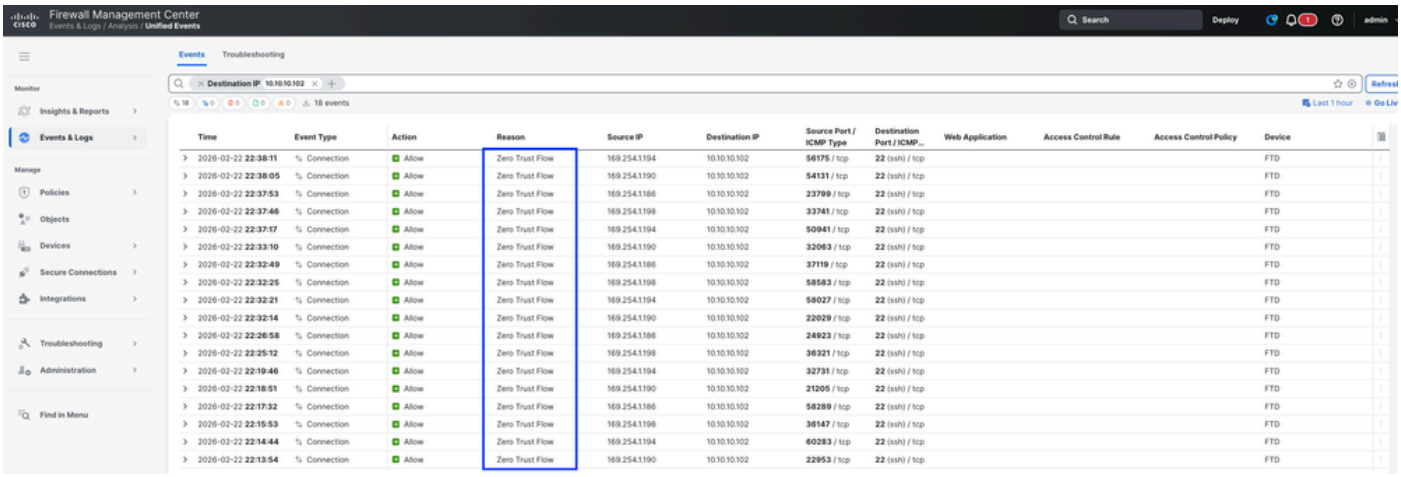


Sicherer Zugriff - Aktivitätssuche



Sicherer Zugriff - Aktivitätssuche

6. Überprüfen von FMC-Verbindungsereignissen

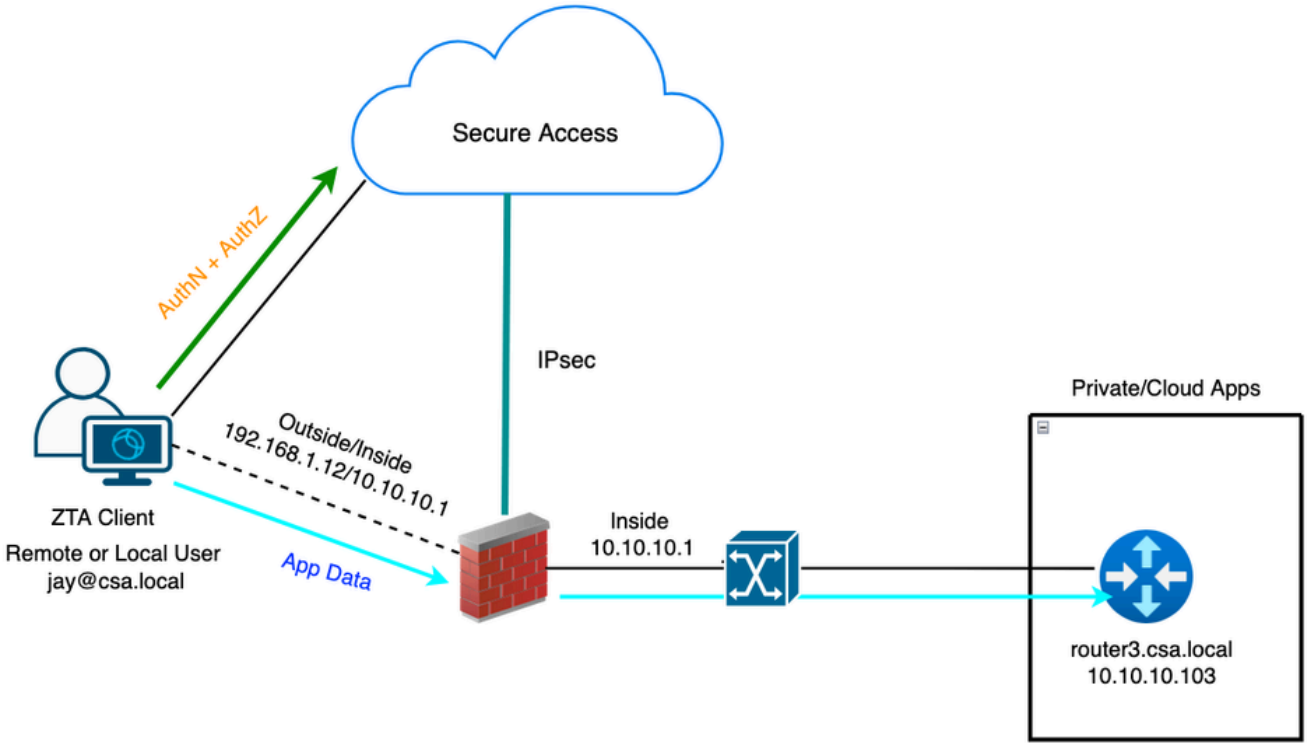


FMC-Verbindungsereignisse

Testfall 4 - Lokaler und Remote-Benutzer - lokale oder Cloud-Durchsetzung mit TND

In diesem Fall hängt die Art der Durchsetzung vom Standort des Benutzers ab. Wenn der Benutzer "Local" (Lokal) ist oder sich hinter einer vertrauenswürdigen FTD-Zone (Innen, DMZ usw.) befindet, ist die Durchsetzung "Local" (Testfall 3). Wenn der Benutzer ein Remote-Benutzer ist, wird die Cloud-Durchsetzung entsprechend durchgeführt (Testfall 1). Der Benutzerstandort wird anhand der Einstellungen für den Netzwerk-Fingerabdruck oder den TND festgelegt. Wenn der Netzwerk-Fingerabdruck übereinstimmt, ist der lokale Benutzer "Lokal", und wenn keine

Übereinstimmung besteht, wird der lokale Benutzer als "Remote" angesehen.

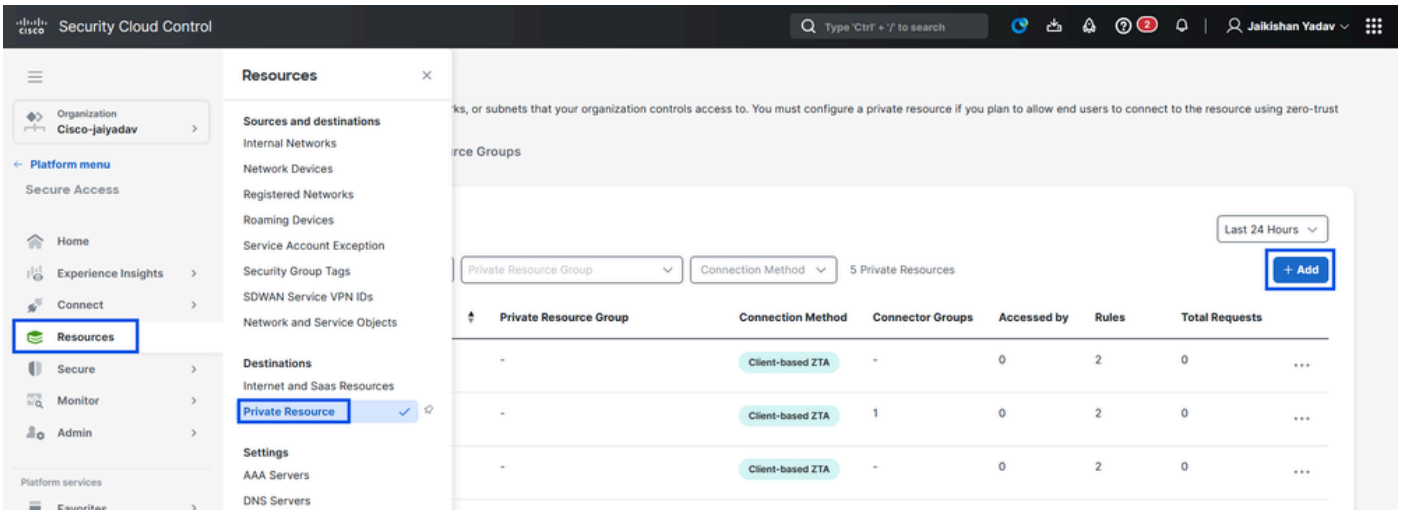


Universelle ZTA - Topologie der Testfälle

Schritt 1 - Definieren einer privaten Ressource für sicheren Zugriff

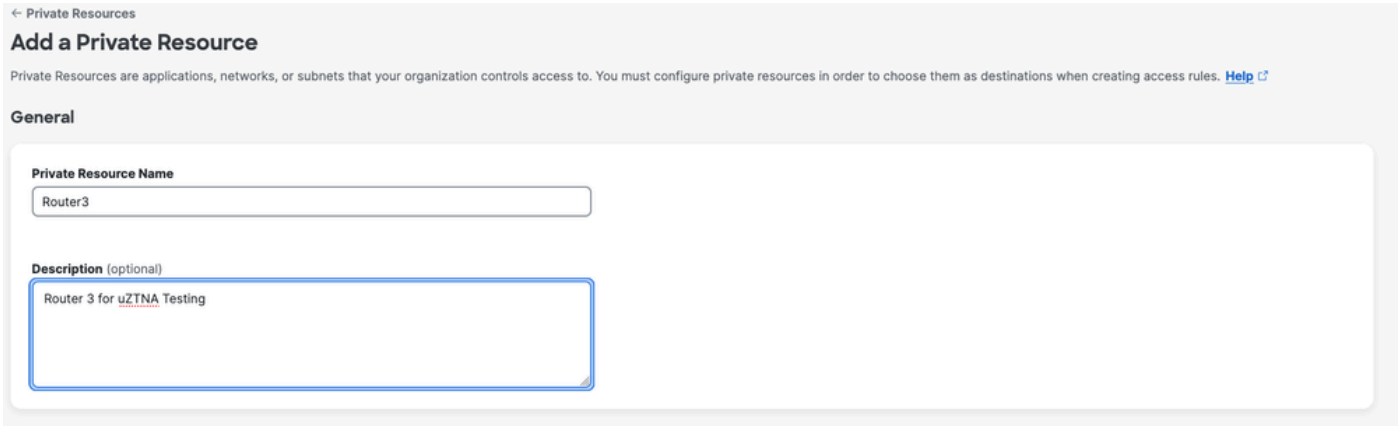
Konfigurieren einer privaten Ressource für den Zugriff über ein bei Zero Trust Access (ZTA) angemeldetes Gerät mit Cloud-Durchsetzung

1. Navigieren Sie zu Ressourcen > Ziele > Private Ressourcen > und klicken Sie auf +Hinzufügen.



Sicherer Zugriff - Konfiguration privater Ressourcen

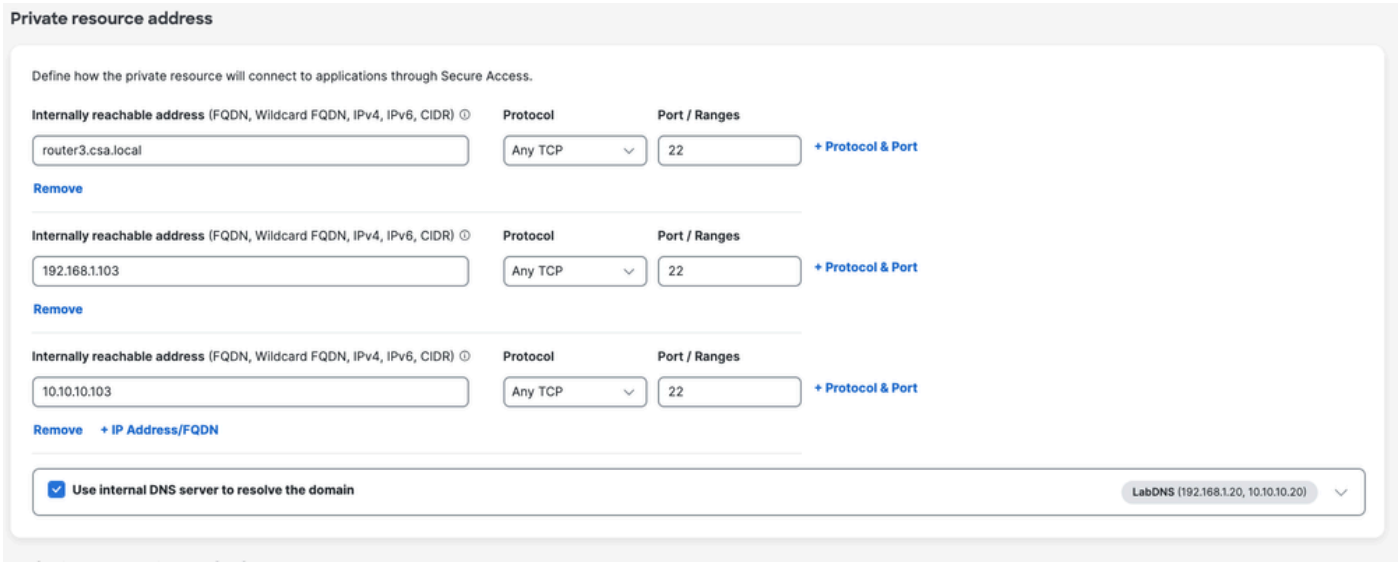
2. Geben Sie für Private Resource Name einen sinnvollen Namen für die Ressource ein. Für Description empfehlen wir, Informationen wie den Zweck der Ressource oder den Namen des Ressourcenbesitzers anzugeben.



Sicherer Zugriff - Konfiguration privater Ressourcen

3. Geben Sie den FQDN der privaten Ressource ein, auf die Sie zugreifen möchten. Wir können auch die IP-Adresse der privaten Ressource definieren. Weitere Informationen finden Sie unter Hinzufügen einer privaten Ressource

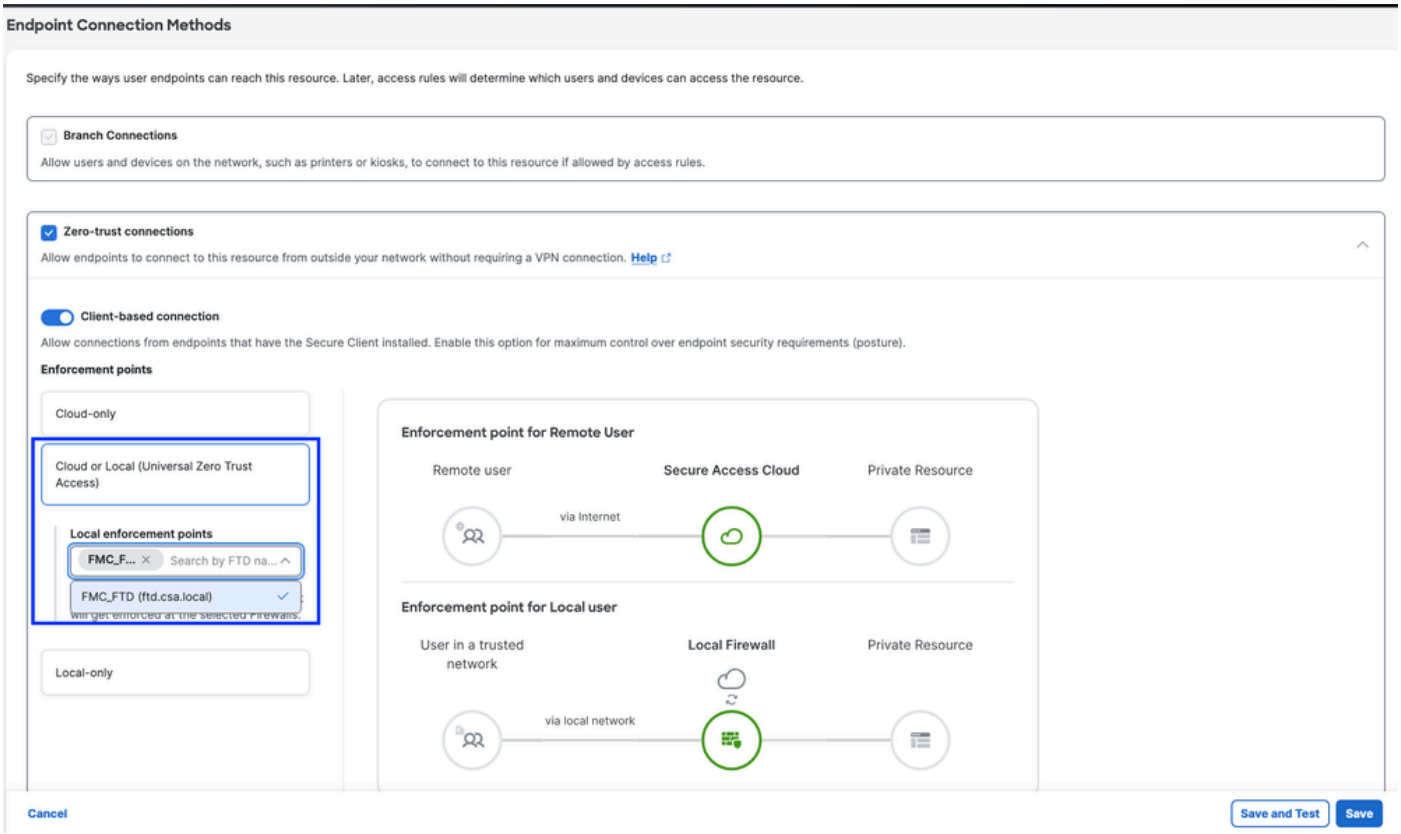
4. Wählen Sie den DNS-Server, um die Domäne aufzulösen



Sicherer Zugriff - Konfiguration privater Ressourcen

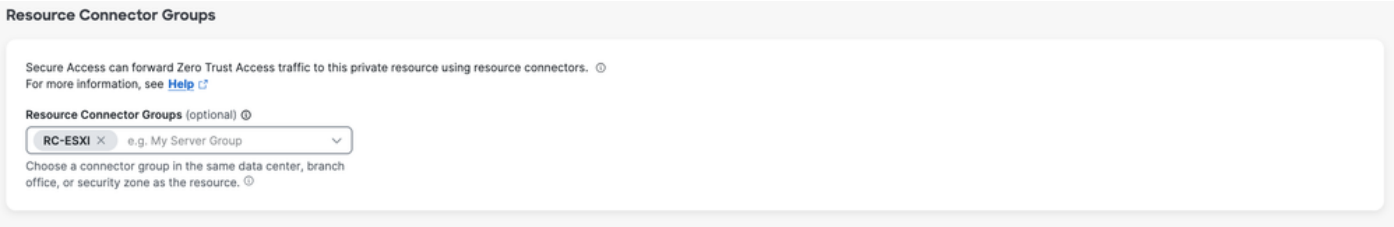
5. Endpunktverbindungsmethoden auswählen

6. Wählen Sie FTD als lokale Durchsetzungspunkte



Sicherer Zugriff - Konfiguration privater Ressourcen

Wählen Sie RC, wenn die private Ressource über RC zugänglich ist, andernfalls lassen Sie sie leer, wenn die private Ressource über die Netzwerk-Tunnelgruppe (IPsec-Tunnel) zugänglich ist.



Sicherer Zugriff - Konfiguration privater Ressourcen

Anmerkung: Je nach gewählter Registrierungsart ordnet diese Änderung den PR automatisch dem FTD zu und löst eine Richtlinienbereitstellung aus.

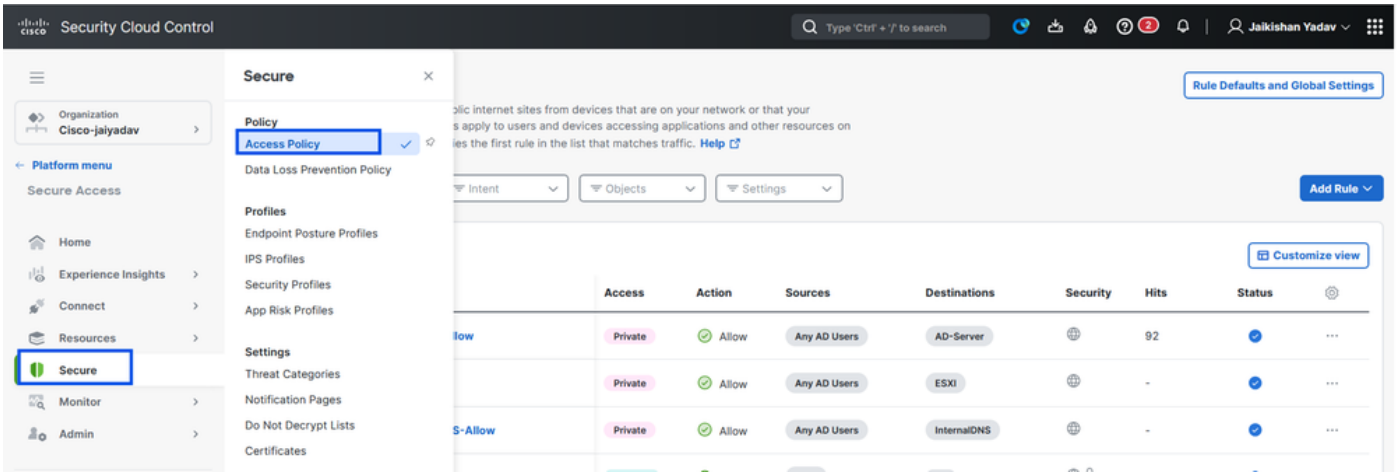
---

7. Klicken Sie auf Save (Speichern).

Schritt 2: Private Zugriffsregel erstellen

Konfigurieren Sie einen privaten Zugriff auf Secure Access, um Zugriff für Benutzer zu erhalten, die bei Universal ZTA registriert sind. Weitere Informationen finden Sie unter Private Access Rule.

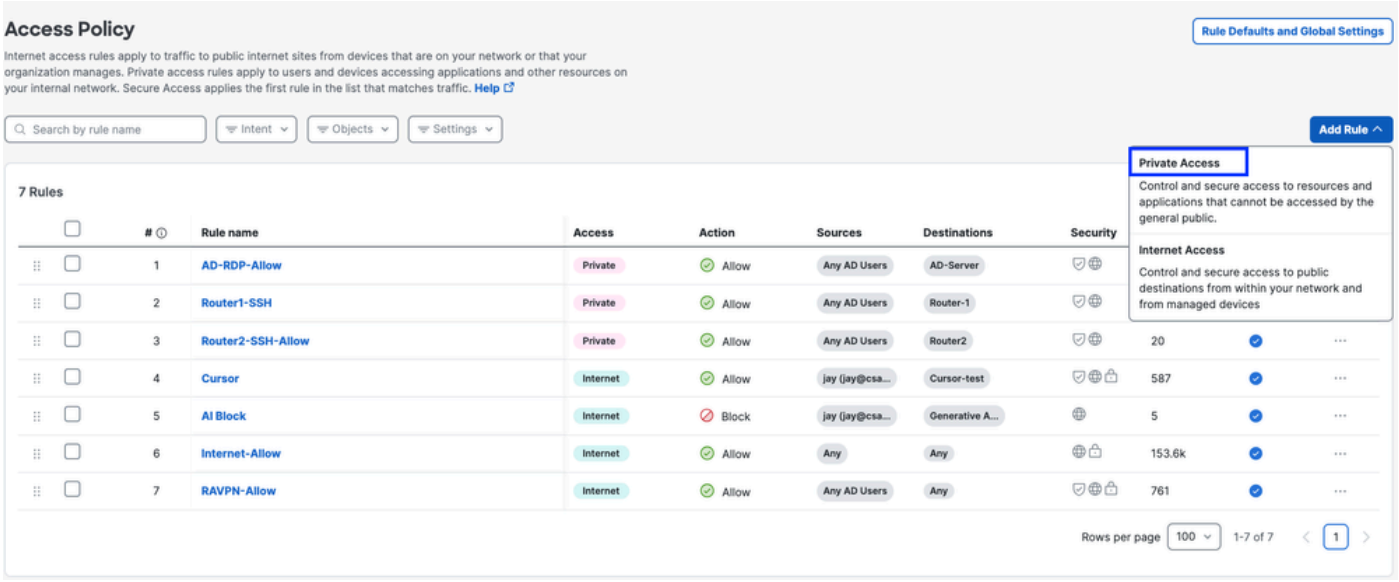
1. Navigieren Sie zu Sicher > Zugriffsrichtlinie



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

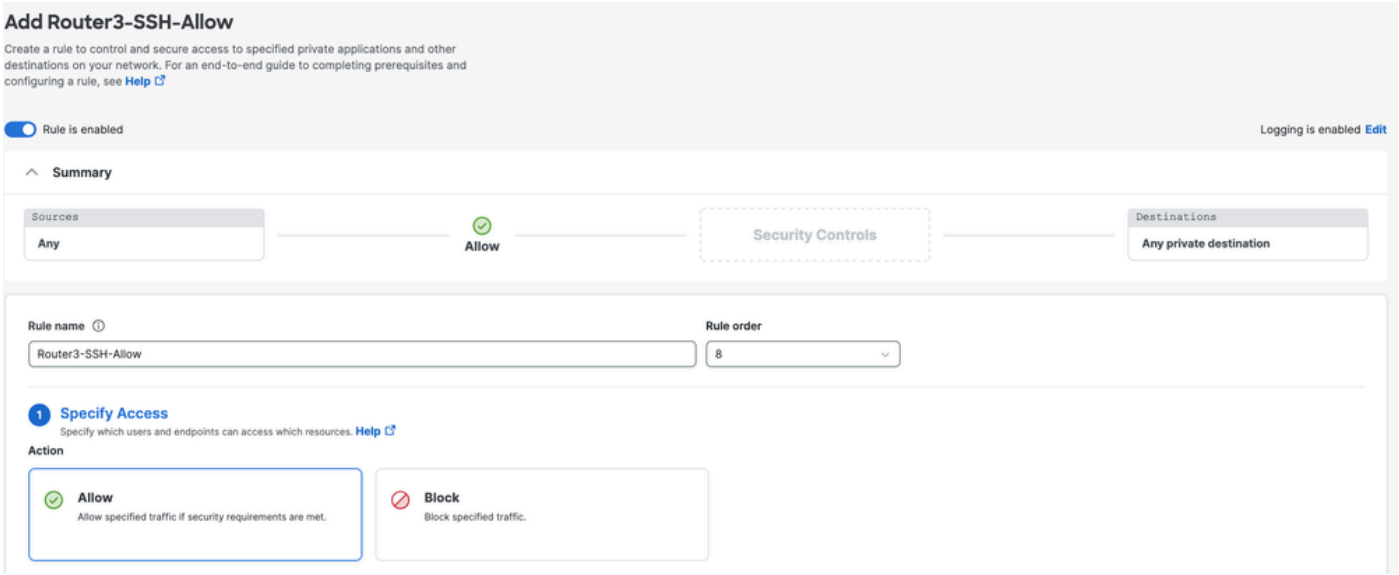
2. Klicken Sie auf Regel hinzufügen, und wählen Sie dann Privater Zugriff aus.
Oben auf der Regel befindet sich eine Zusammenfassung, die die konfigurierten Komponenten

der Regel beschreibt.



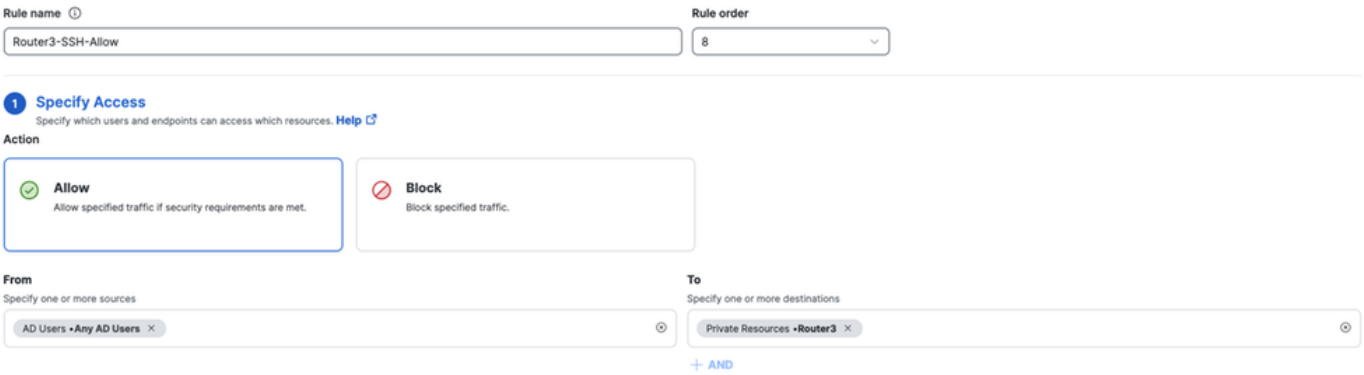
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

3. Hinzufügen eines Regelnamens



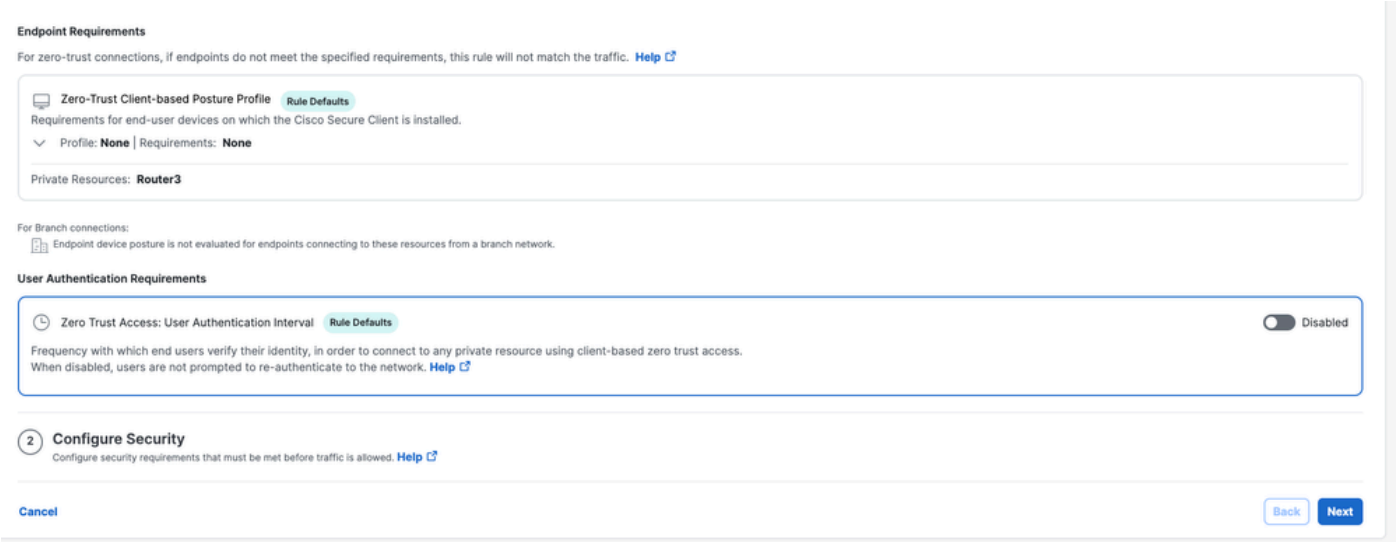
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

4. Wählen Sie die Regelaktion und dann Quelle und Ziel aus.



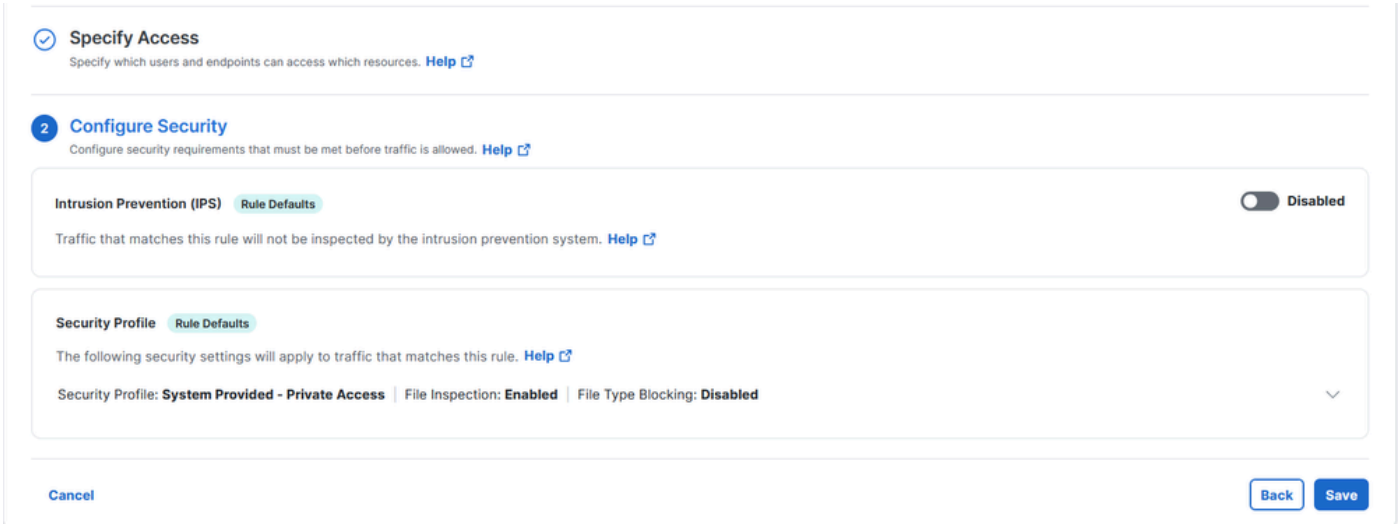
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen



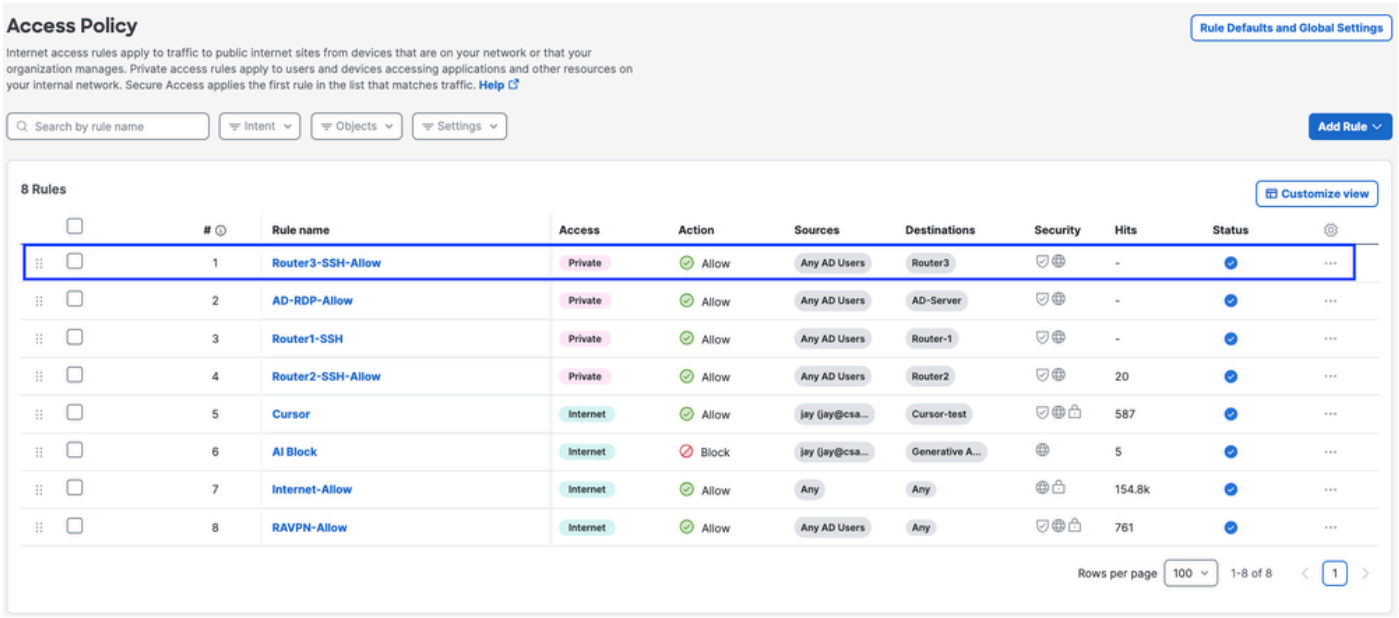
Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

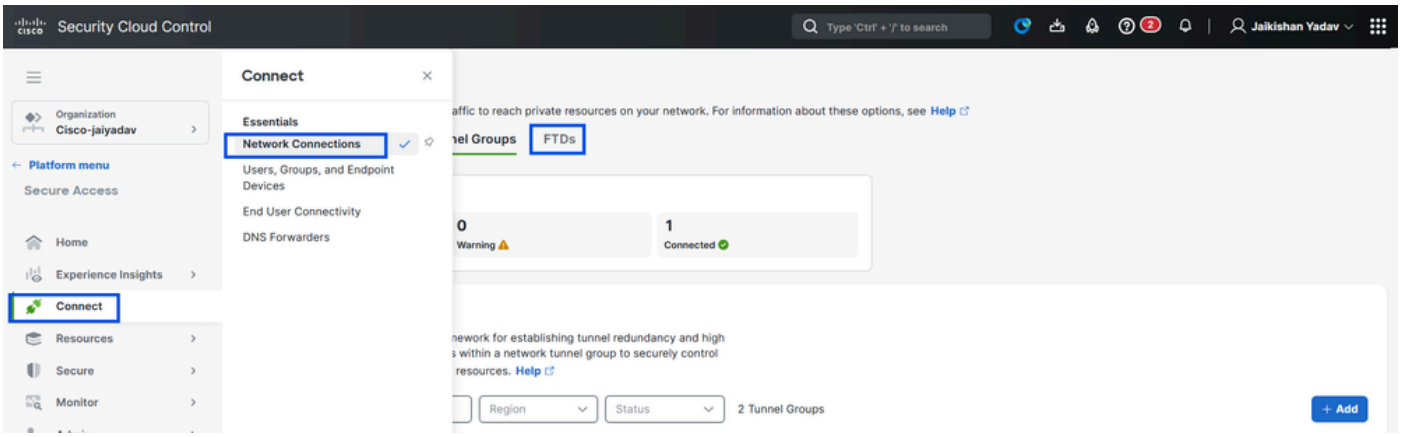
7. Klicken Sie auf Speichern



Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

Schritt 3 - Überprüfen der Zuordnung von PR auf dem FTD

1. Navigieren Sie zu Verbinden > Netzwerkverbindungen > FTDs

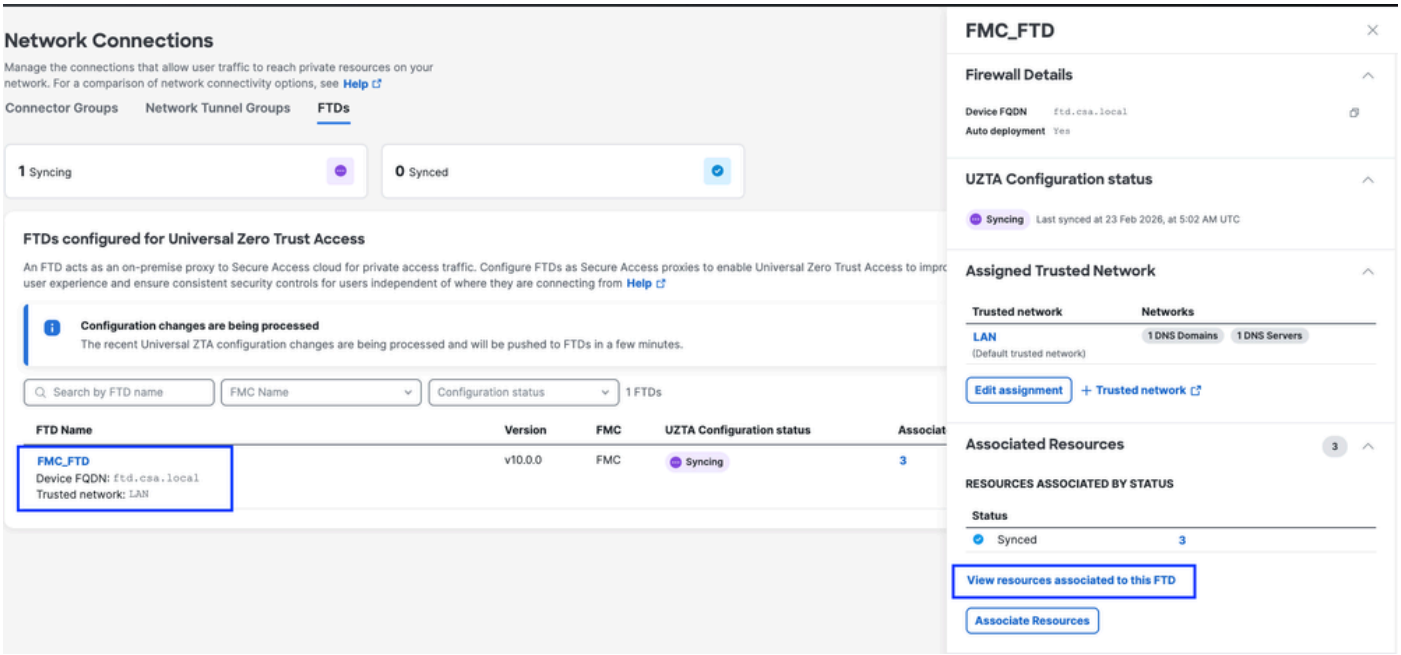


Sicherer Zugriff - PR-Verifizierung

2. Klicken Sie auf FTD > Ressourcen anzeigen, die diesem FTD zugeordnet sind.

```
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
```

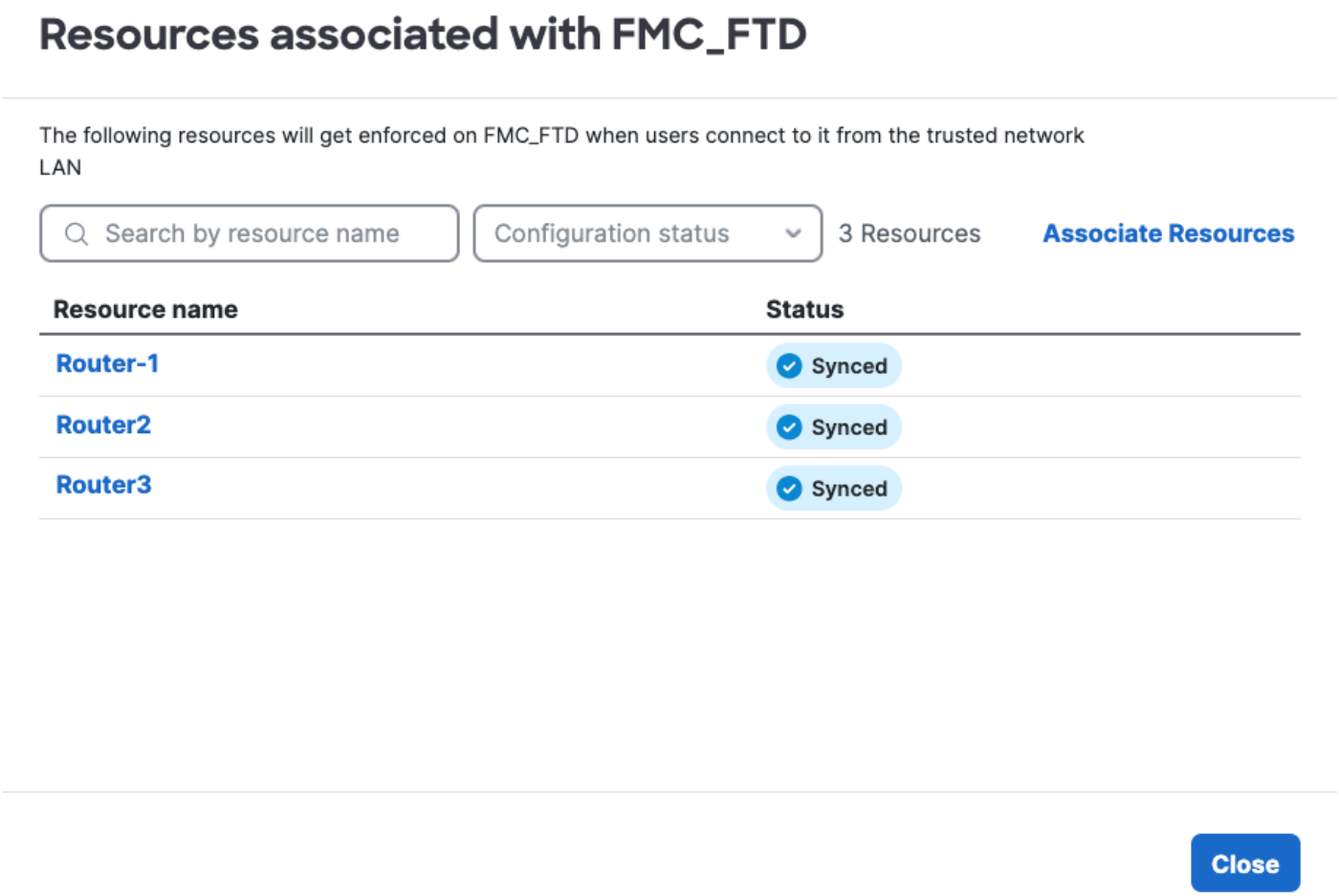
Sicherer Zugriff - PR-Verifizierung



Sicherer Zugriff - PR-Verifizierung

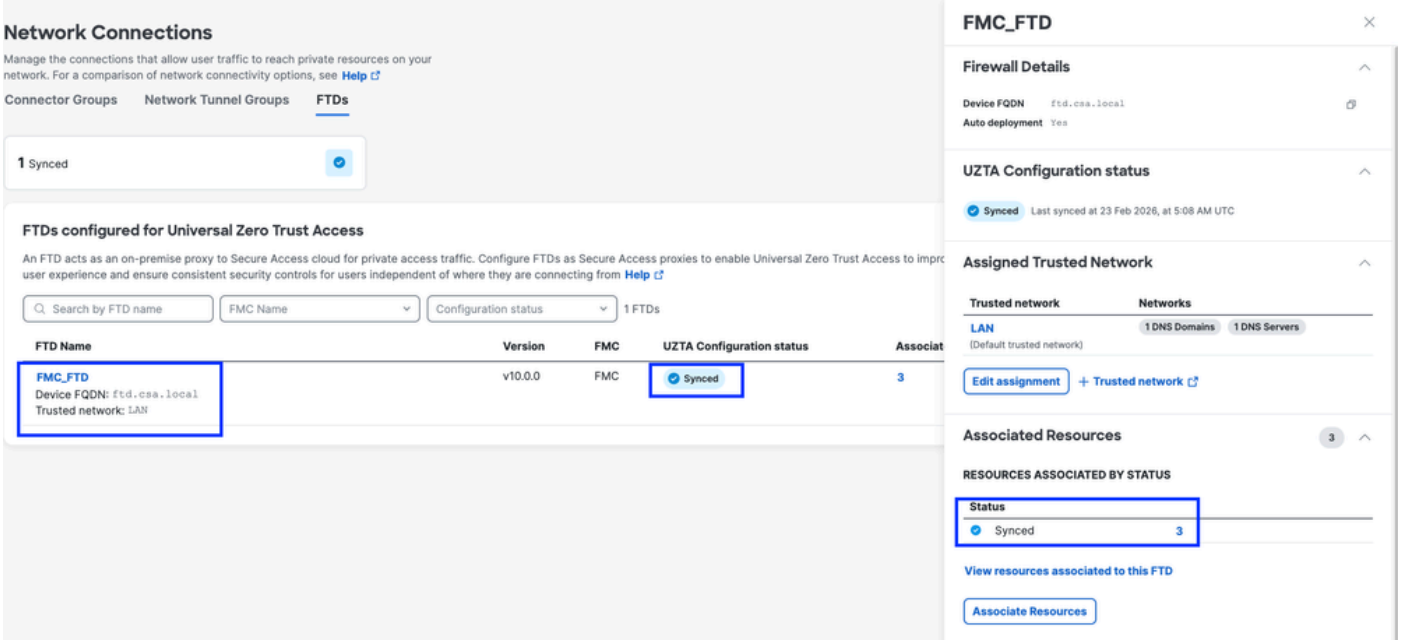
```
C:\Users\jay>ping ftd.csa.local

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
```

Sicherer Zugriff - PR-Verifizierung



3. Klicken Sie auf Schließen

4. Vergewissern Sie sich, dass der Status , Associated Resource (Zugehörige Ressource) und Configuration (Konfiguration) den Status "Synchronisiert" aufweist.



Sicherer Zugriff - PR-Verifizierung

5. Überprüfen Sie, ob die Konfiguration auf FTD übertragen wurde.

Melden Sie sich bei der FTD-CLI an, und navigieren Sie zum LINA-Modus.

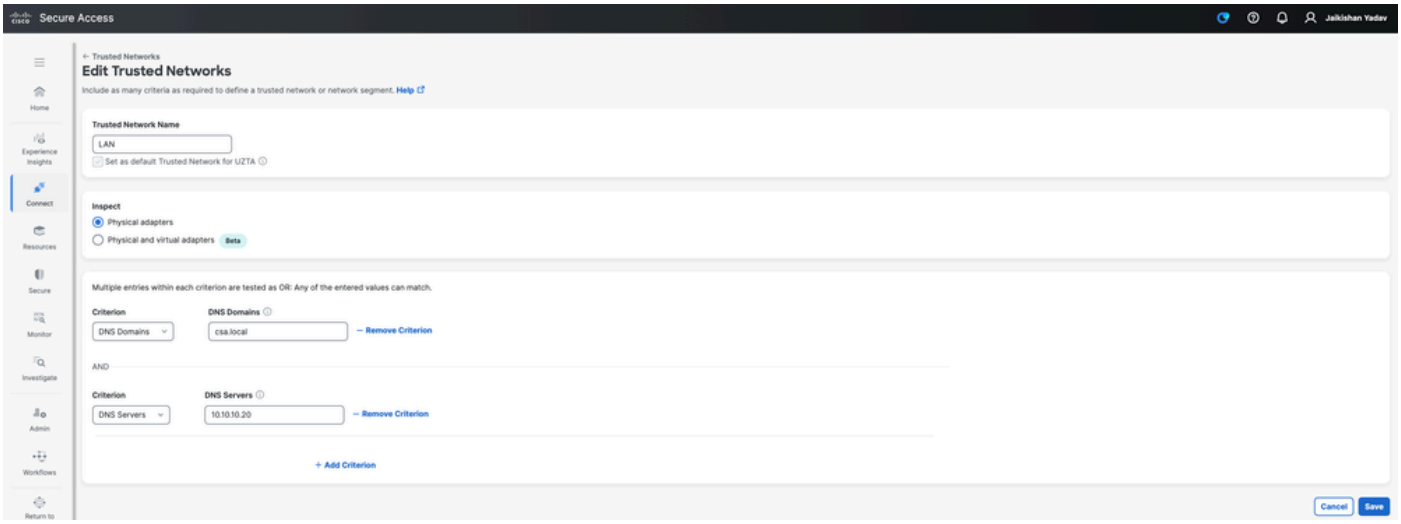
show running-config object application

```
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
```

Sicherer Zugriff - PR-Verifizierung

Schritt - 4 Konfigurieren oder Überprüfen "Vertrauenswürdige Netzwerke oder ZTA-Einstellungen verwalten"

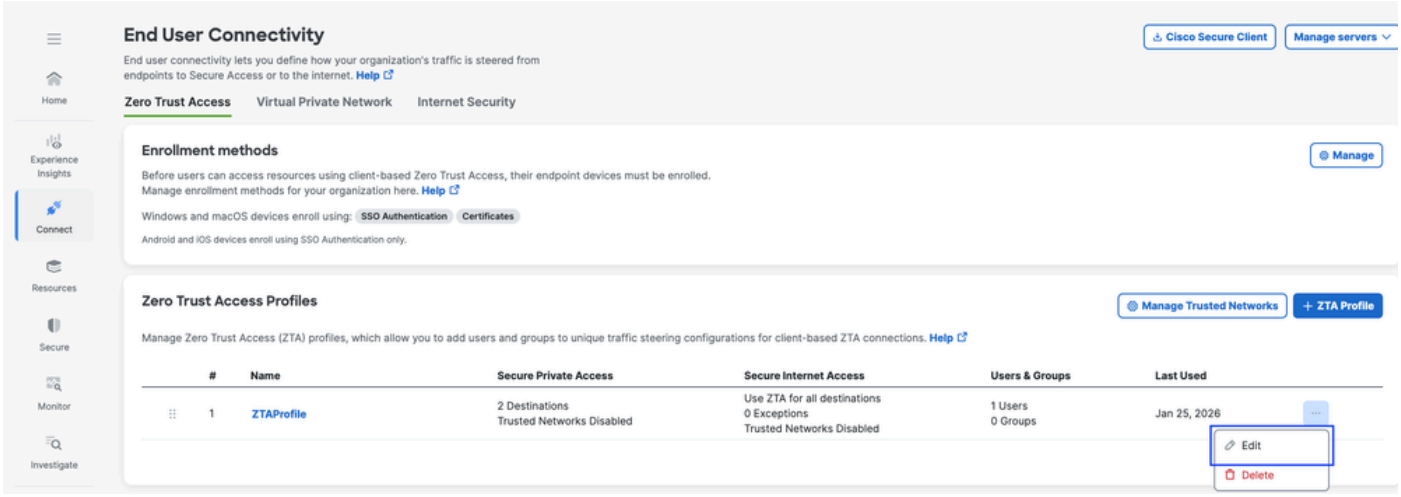
Navigieren Sie zu Verbinden > Endbenutzerverbindungen > Zugriff ohne Vertrauensstellung > ZTA-Einstellungen, und konfigurieren Sie vertrauenswürdige Netzwerke.



Sicherer Zugriff - ZTA TND-Konfiguration

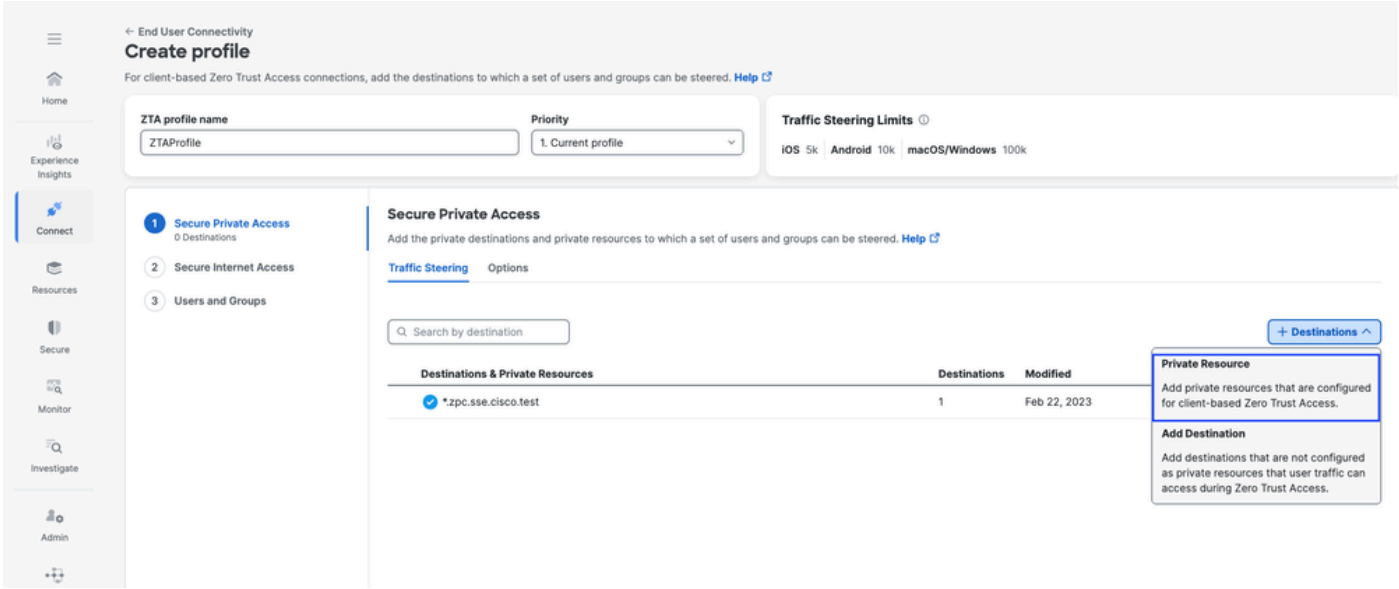
Schritt - 5 Hinzufügen einer privaten Ressource zum ZTA-Profil

1. Navigieren Sie zu Verbinden > Endbenutzerverbindung > Zugriff ohne Vertrauensstellung, und klicken Sie auf 3 Punkte, um das ZTA-Profil zu bearbeiten.

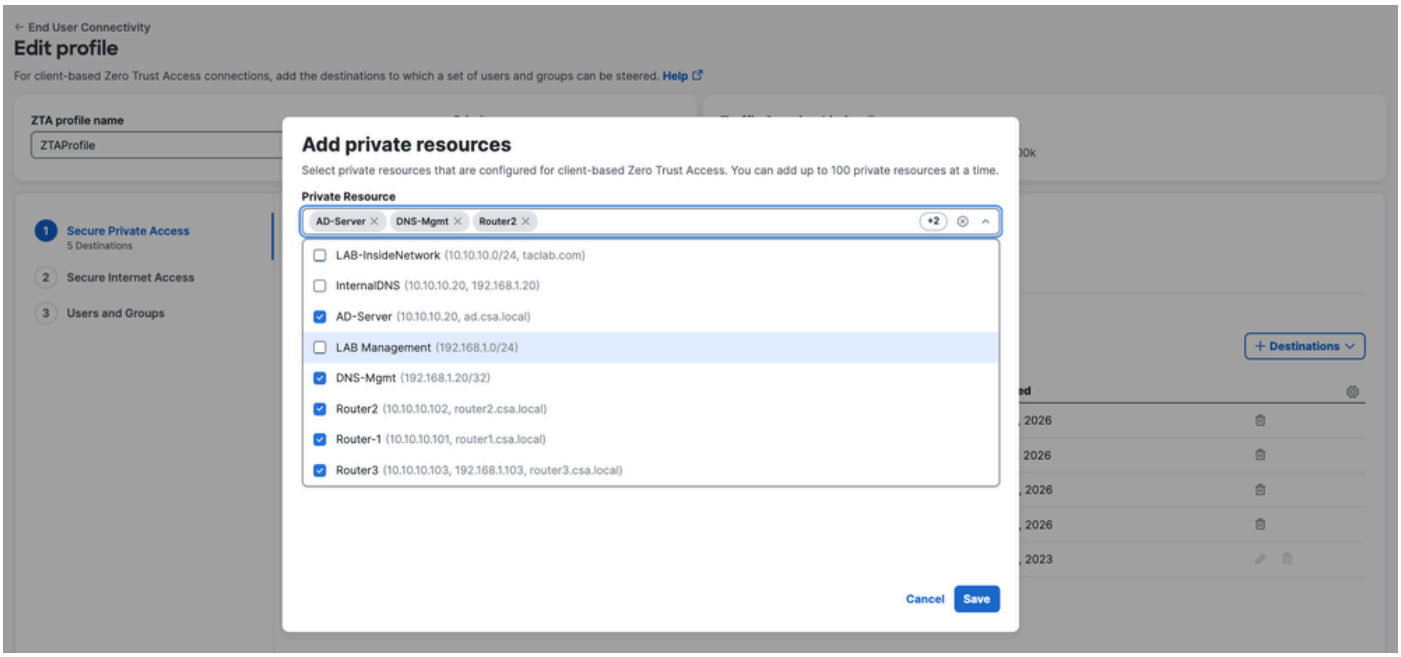


Sicherer Zugriff - ZTA-Profil

2. Fügen Sie die private Ressource hinzu

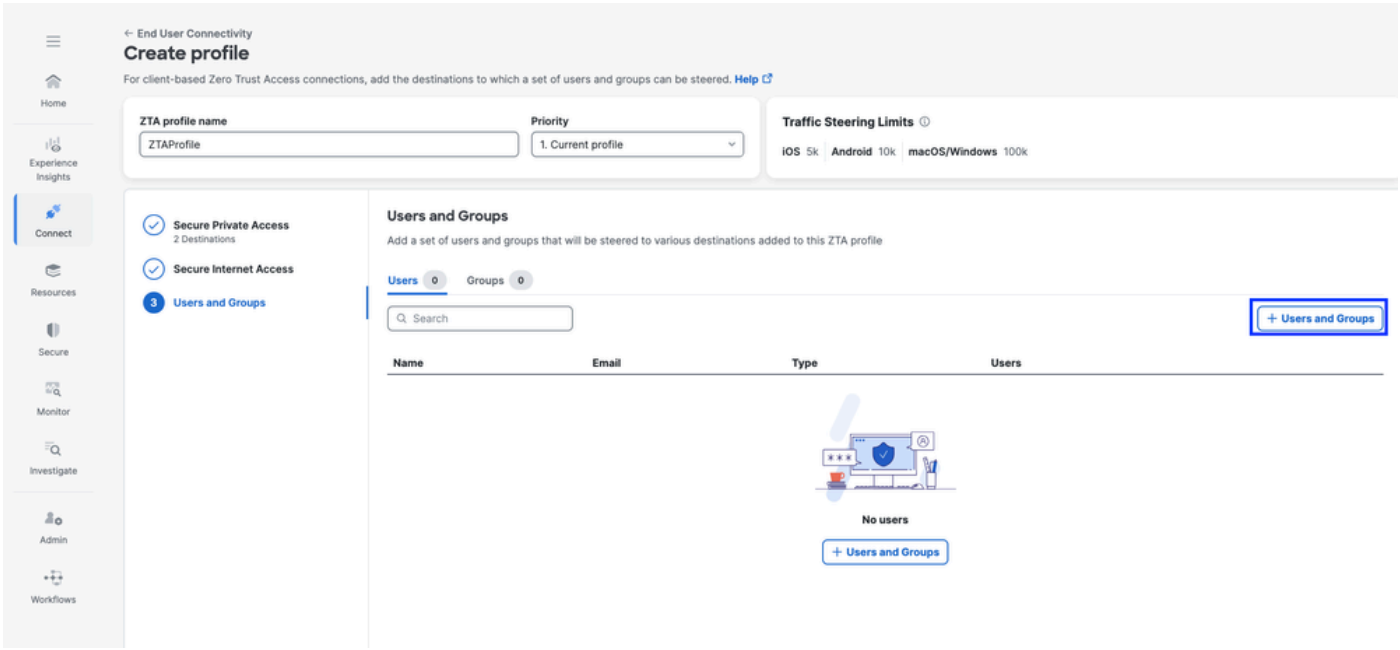


Sicherer Zugriff - ZTA-Profil

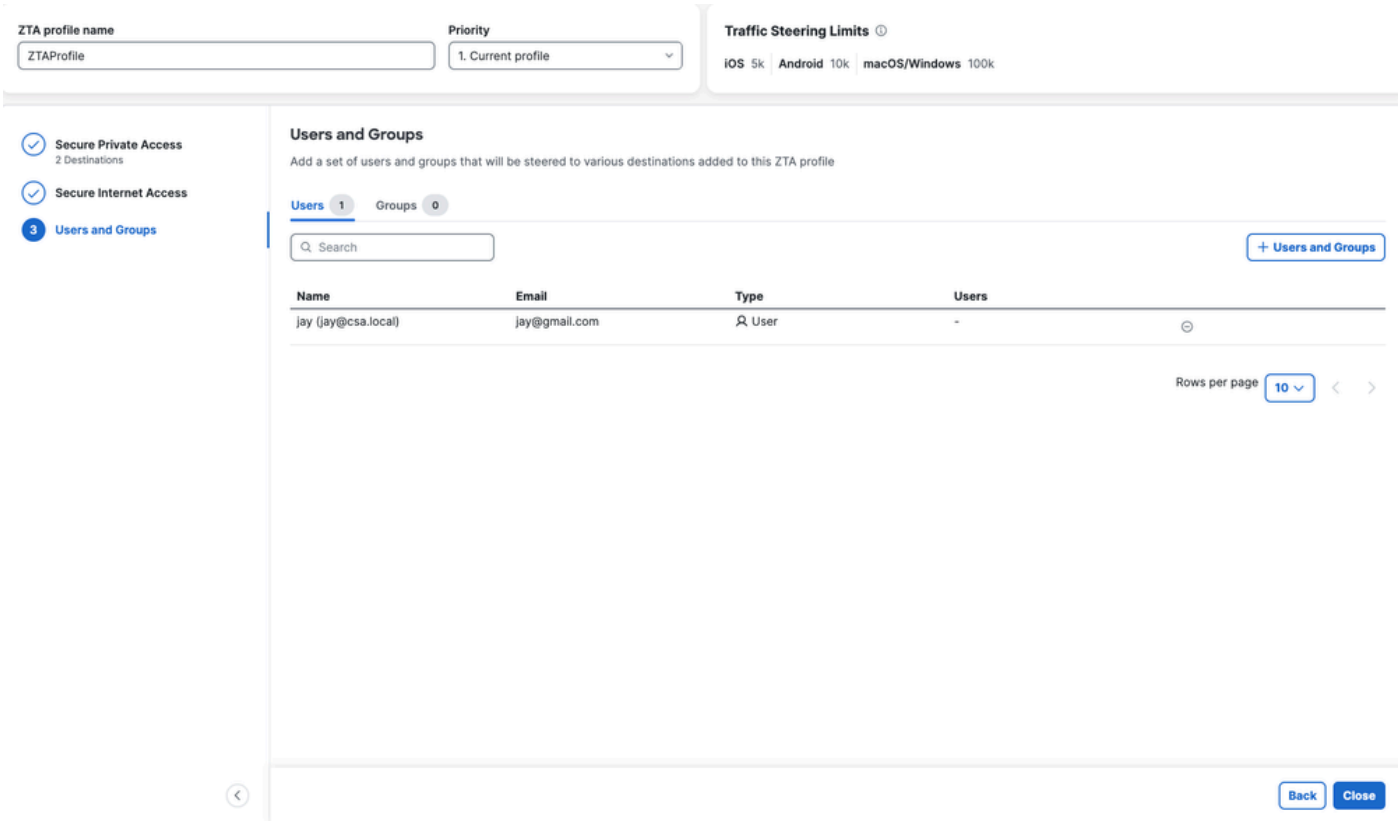


Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen



Sicherer Zugriff - ZTA-Profil

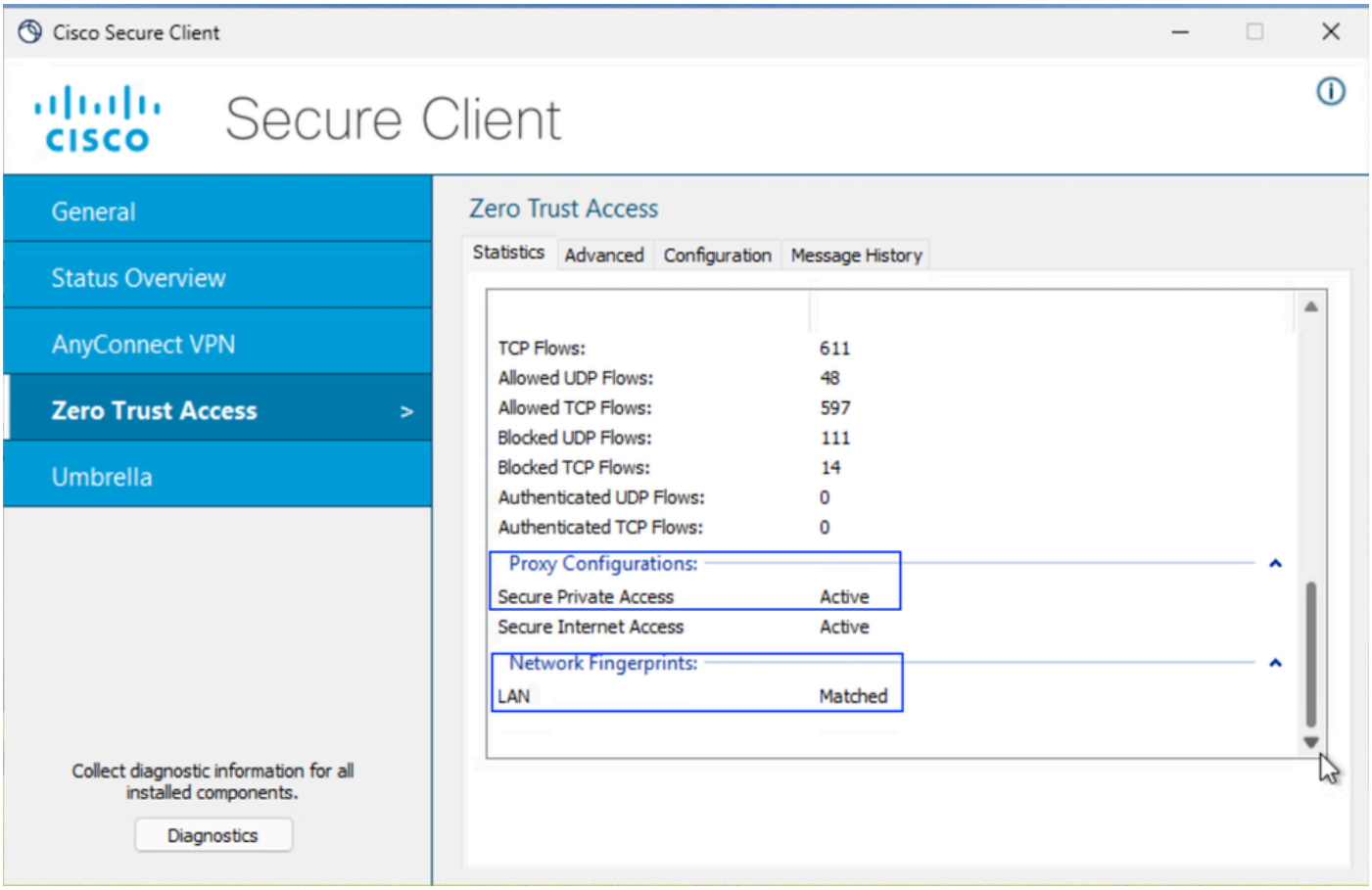


Sicherer Zugriff - ZTA-Profil

Schritt - 6 Überprüfen des Zugriffs auf die private Ressource

Wenn der Benutzer "Lokal" ist

1. Überprüfen Sie den Netzwerk-Fingerprint für ZTA TND. Er sollte übereinstimmen, wenn der Benutzer "Lokal" ist und "Sicherer privater Zugriff" aktiv sein sollte.



Sicherer Zugriff - PR-Tests

2. Überprüfen, ob der Remote-Benutzer den FTD FQDN auflösen kann

```
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
```

Sicherer Zugriff - PR-Tests

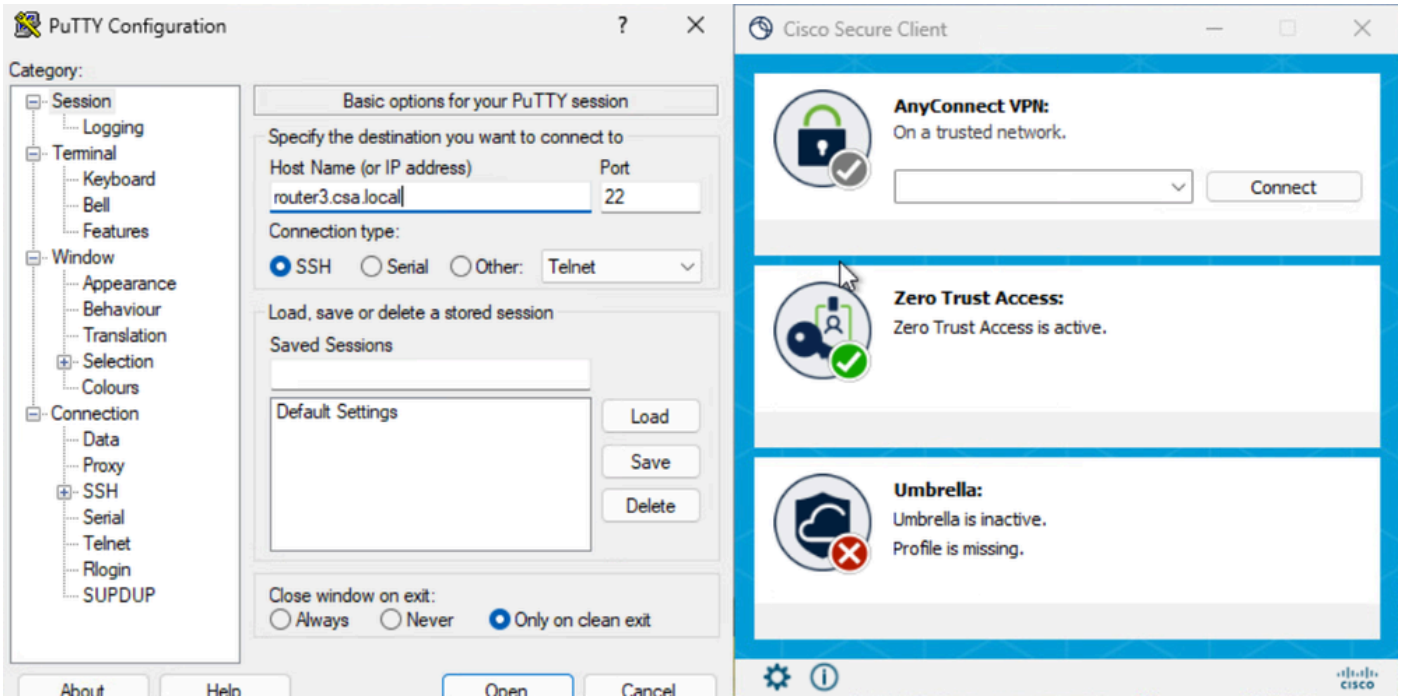
3. Überprüfen Sie, ob FTD über FQDN eine Verbindung zu einer privaten Ressource herstellen kann.

```
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#
```

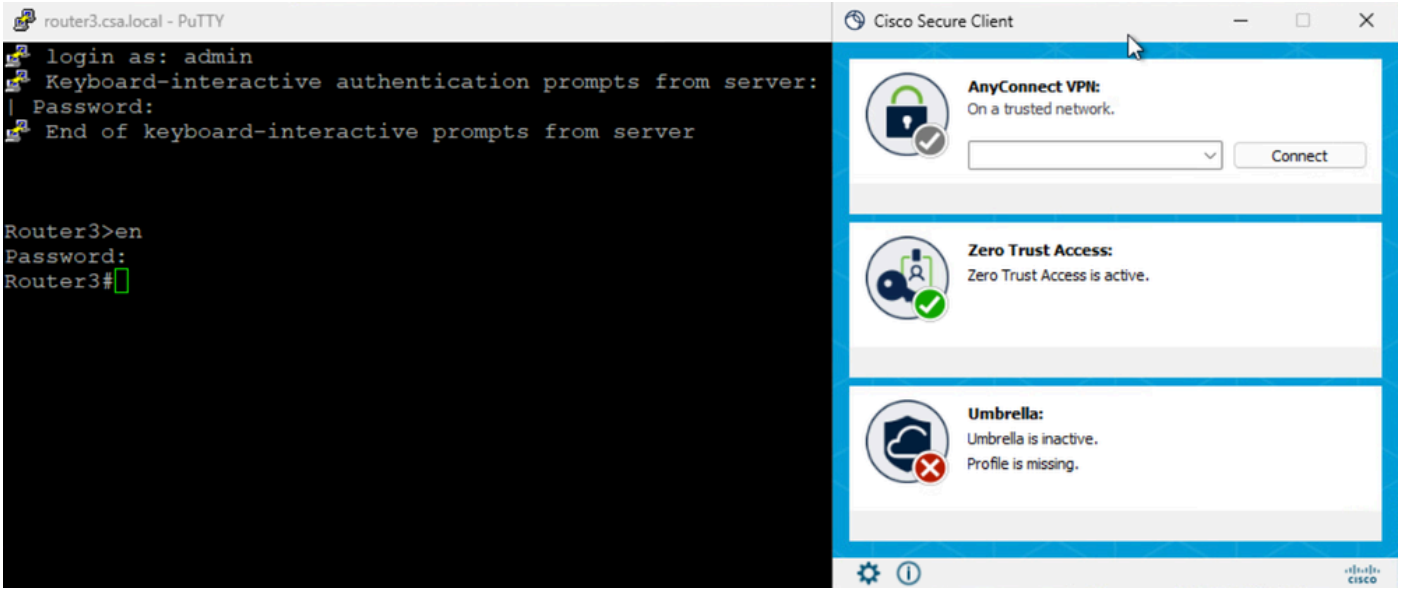
Sicherer Zugriff - PR-Tests

4. Testen der SSH-Verbindung mit der privaten Ressource

Zugriff auf den PR über FQDN

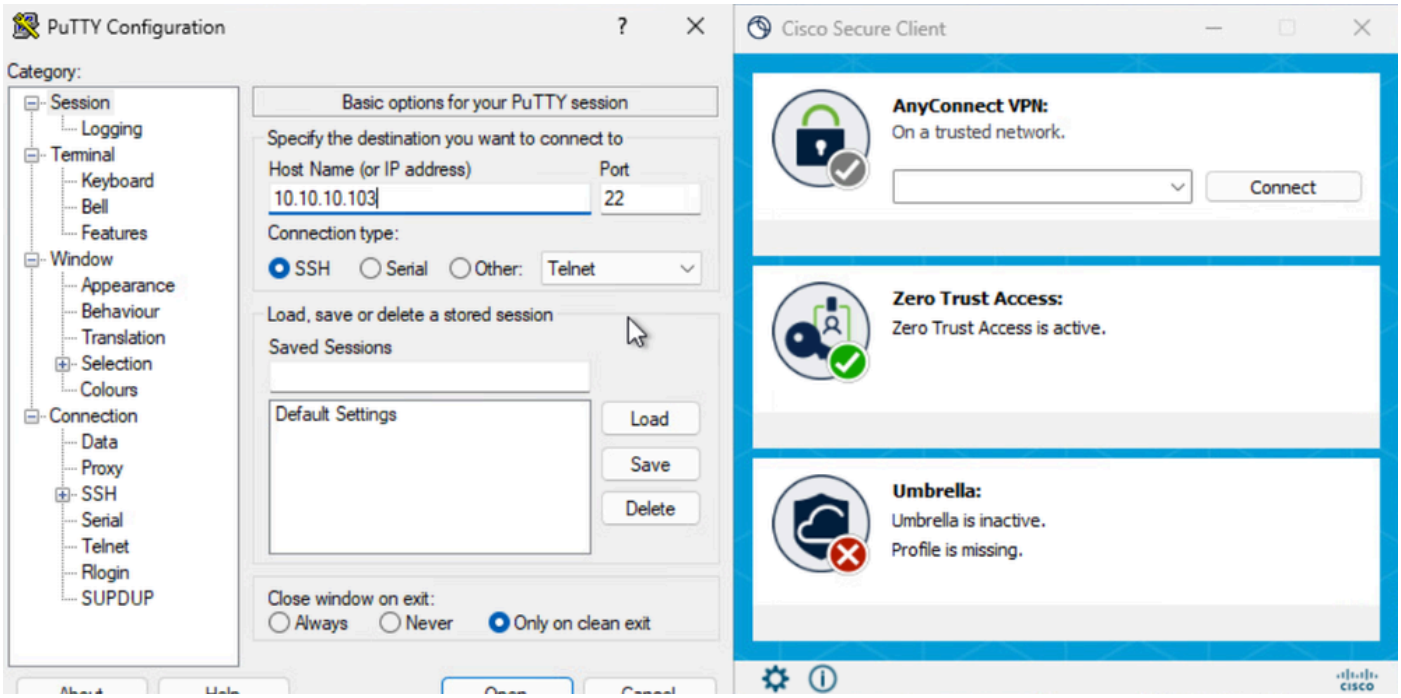


Sicherer Zugriff - PR-Tests

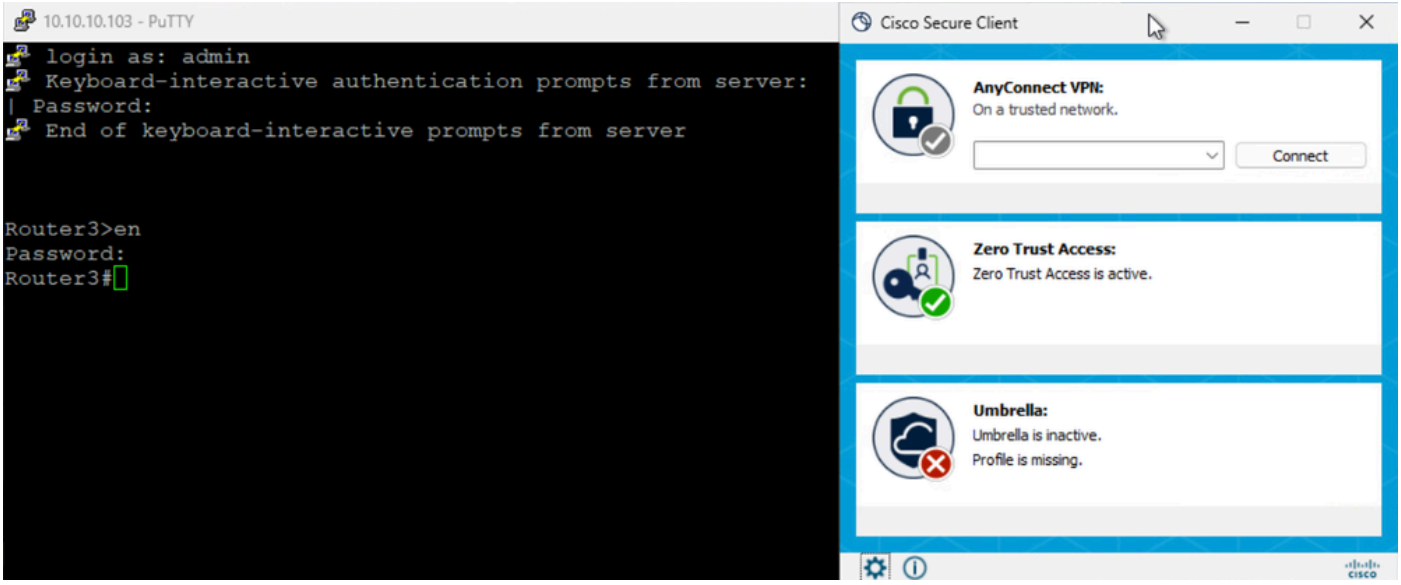


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse

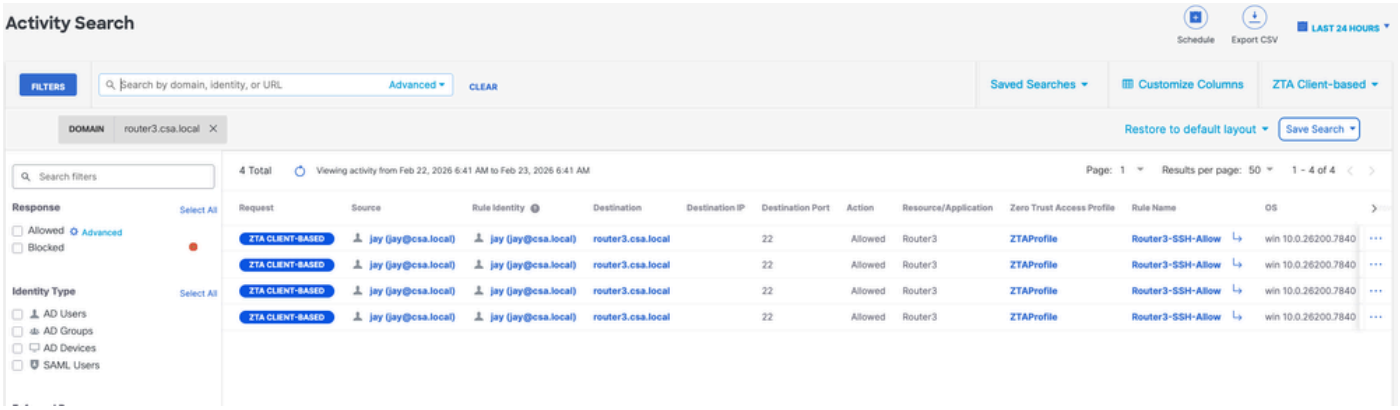


Sicherer Zugriff - PR-Tests

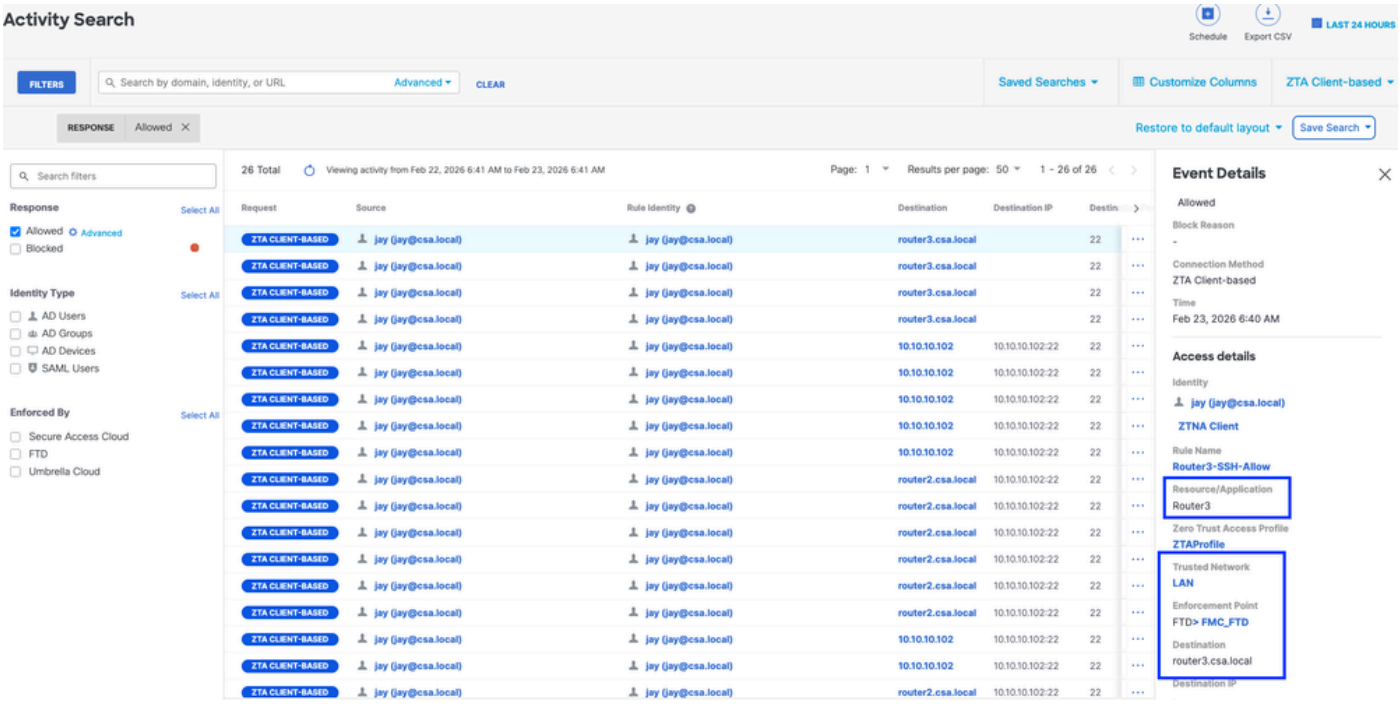


Sicherer Zugriff - PR-Tests

5. Überprüfen der Suchprotokolle für Aktivitäten mit sicherem Zugriff

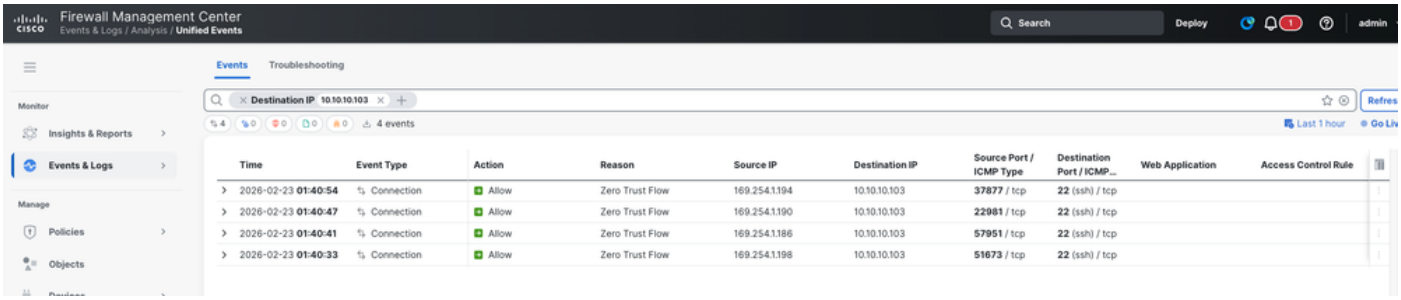


Sicherer Zugriff - Aktivitätssuche



Sicherer Zugriff - Aktivitätssuche

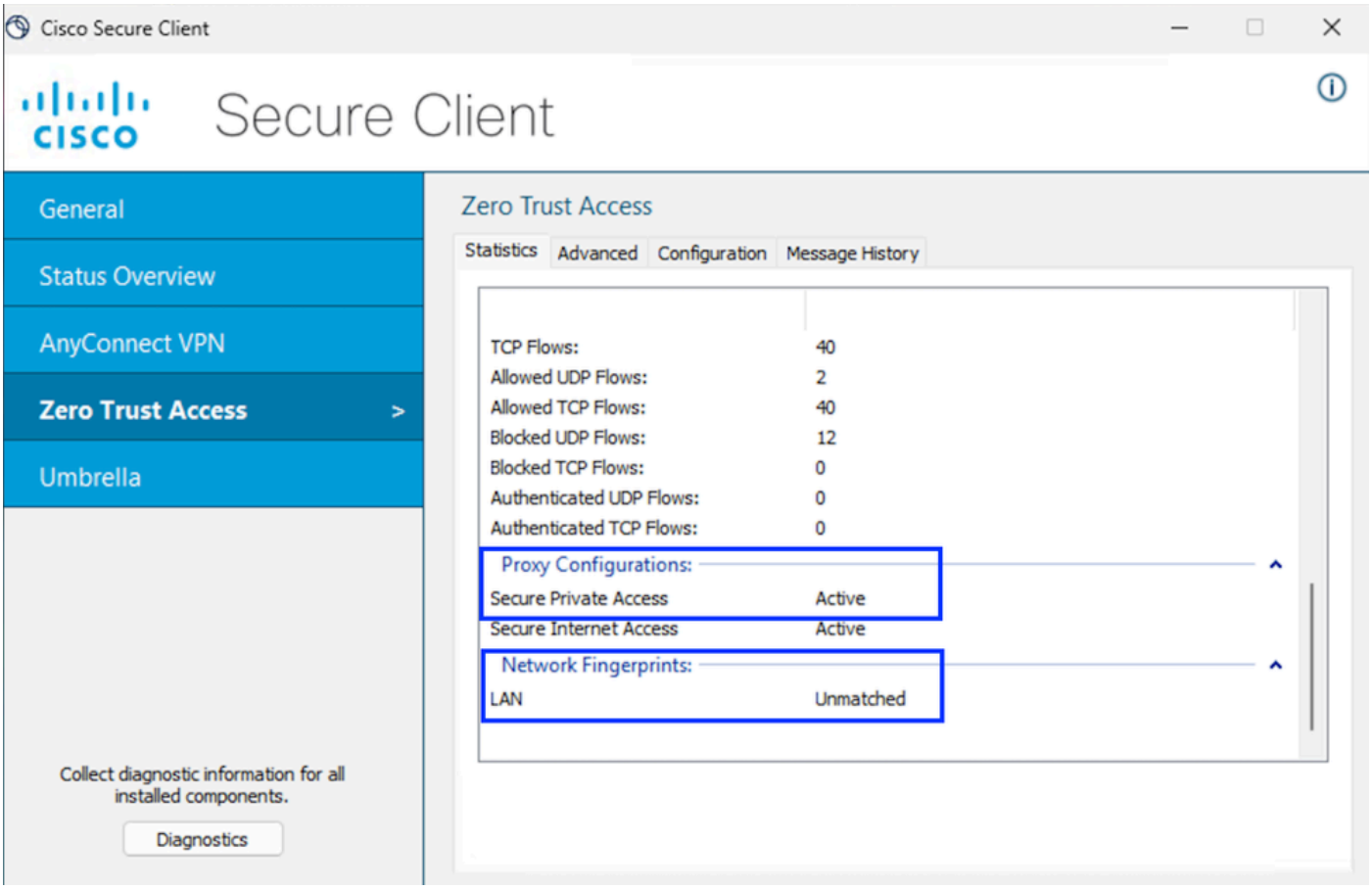
6. Überprüfen von FMC-Verbindungsereignissen



FMC-Verbindungsereignisse

Wenn der Benutzer Remote ist

1. Überprüfen Sie den Netzwerk-Fingerprint für ZTA TND. Die Übereinstimmung sollte aufgehoben werden, wenn der Benutzer ein Remote-Benutzer ist.

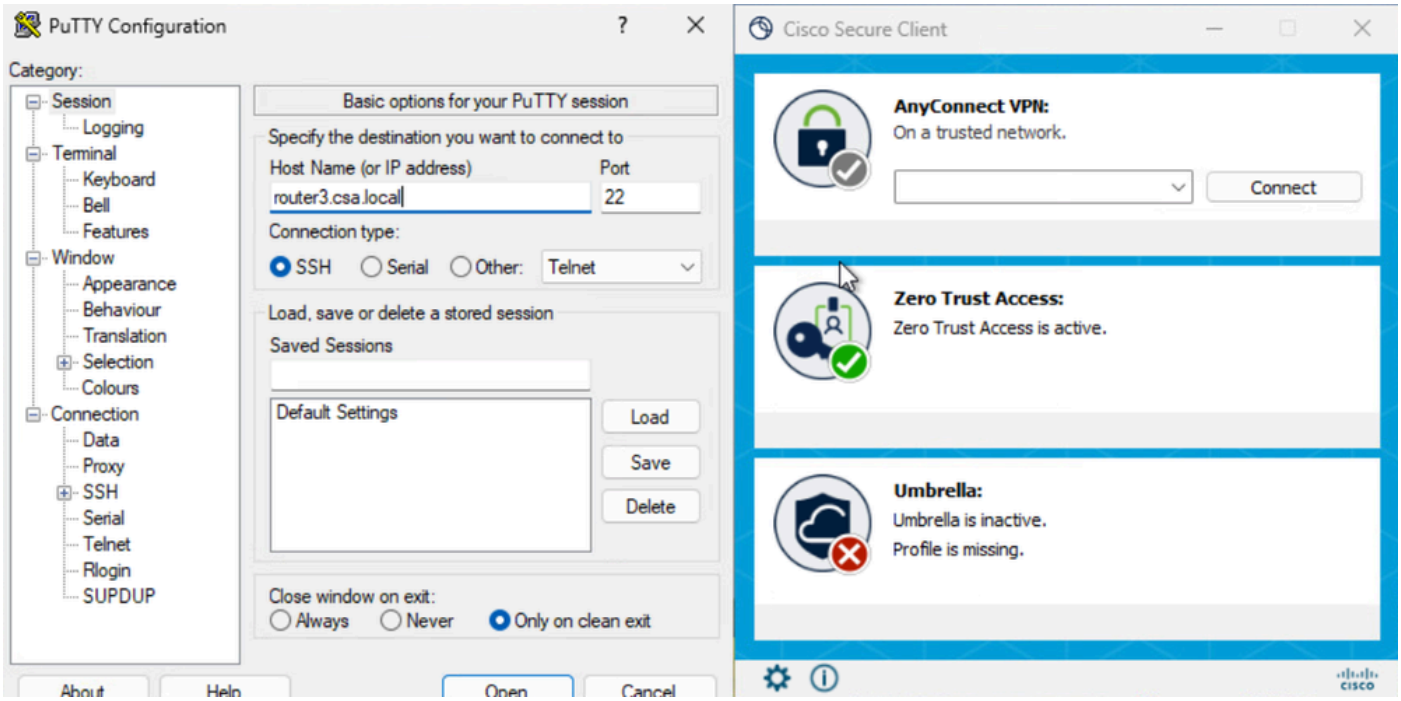


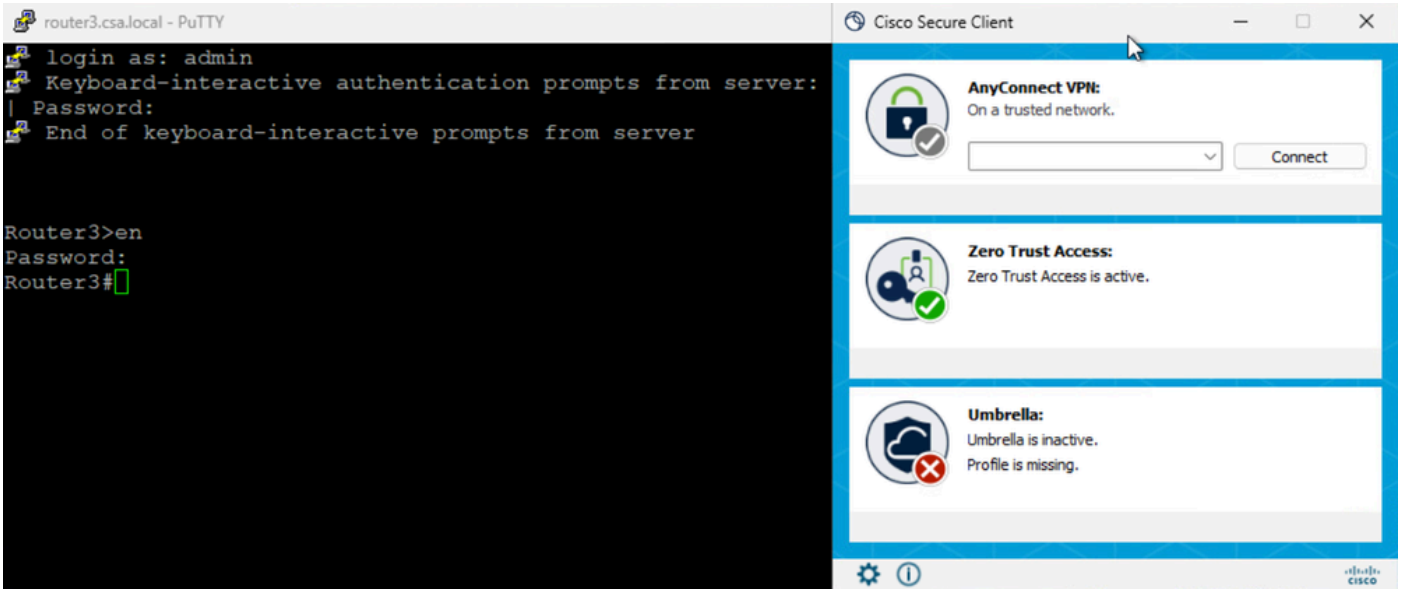
2. Überprüfen, ob der Remote-Benutzer den FTD FQDN auflösen kann

```
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. Testen der SSH-Verbindung mit der privaten Ressource

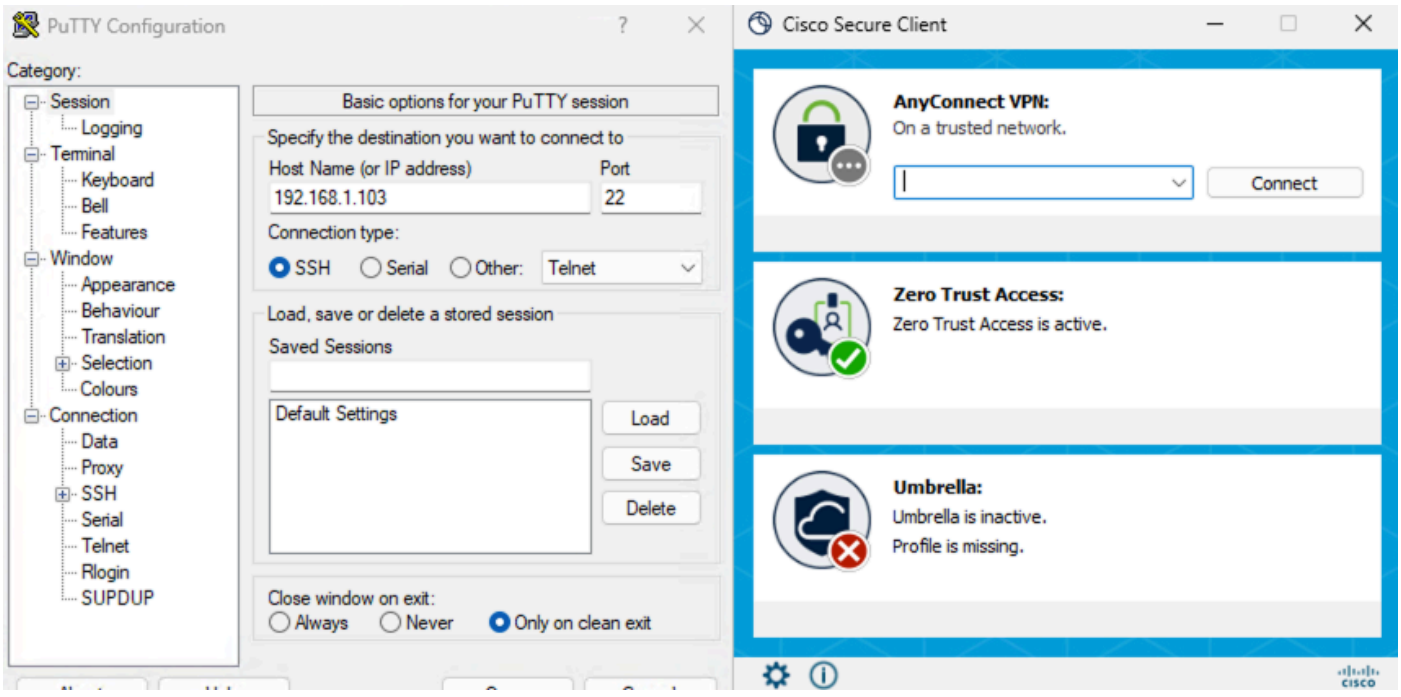
Zugriff auf den PR über FQDN



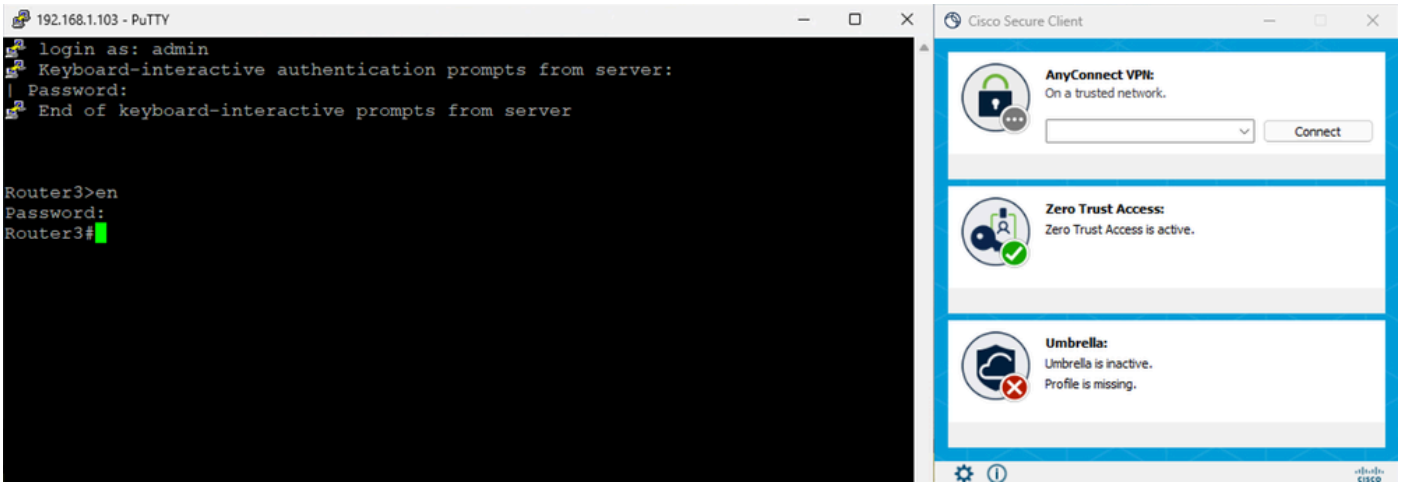


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse

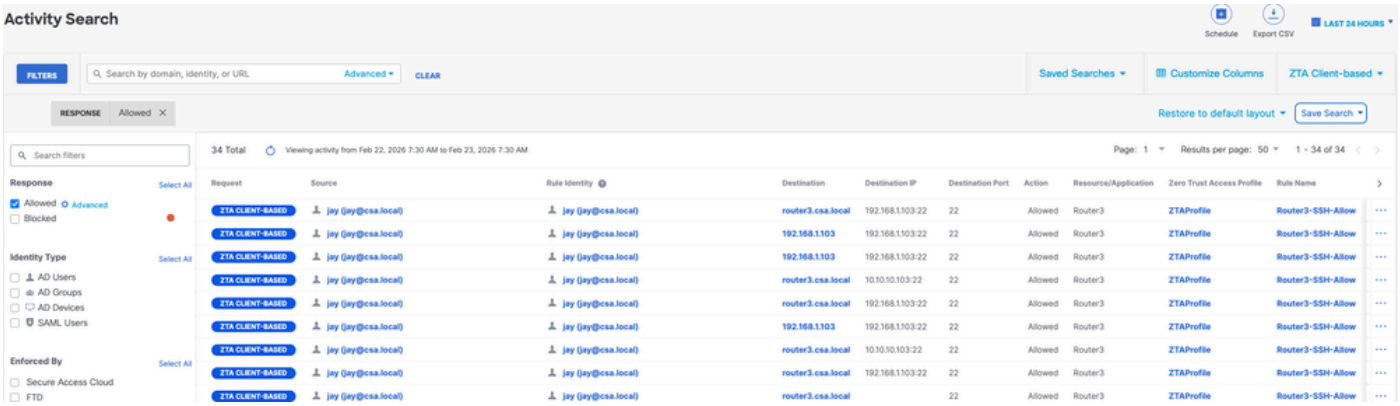


Sicherer Zugriff - PR-Tests

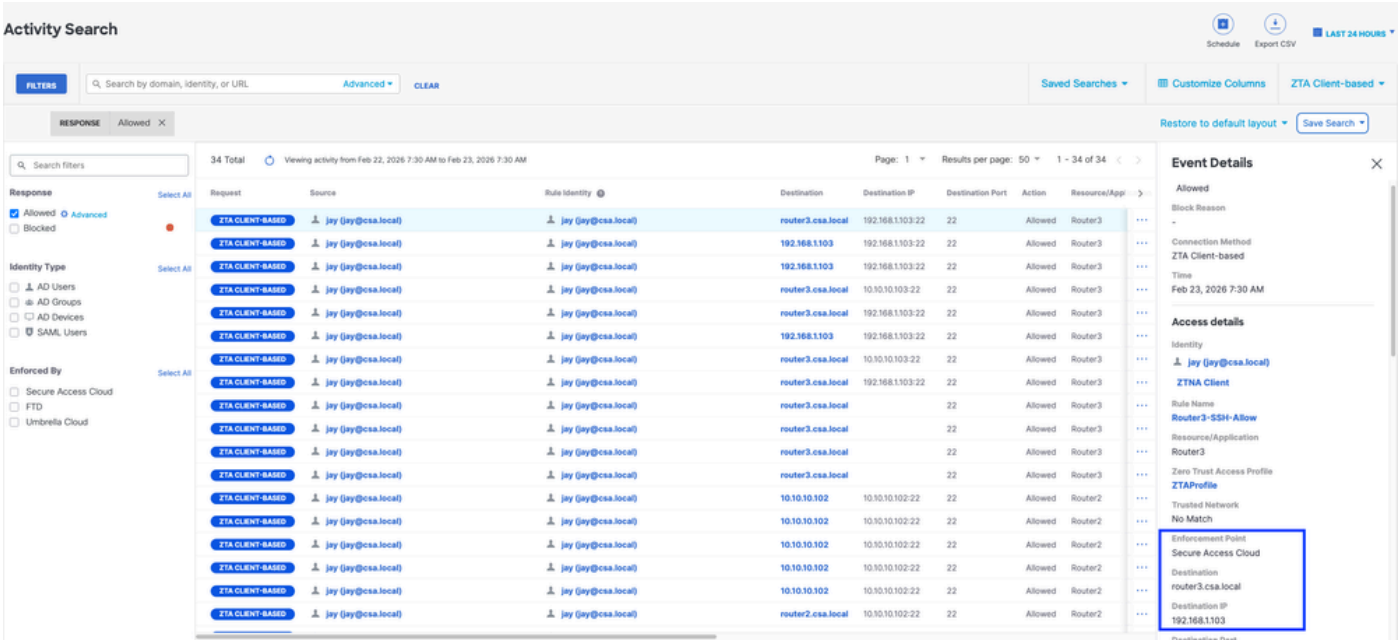


Sicherer Zugriff - PR-Tests

5. Überprüfen der Suchprotokolle für Aktivitäten mit sicherem Zugriff



Sicherer Zugriff - Aktivitätssuche



Fehlerbehebung

Nützliche Befehle:

> Zuordnungs-Core-Profil anzeigen
> asp inspect-dp snort anzeigen
> sh running-config universal-zero trust
> show interface ip brief

> debug universal-zero trust zproxy 7

! und dann in den Expertenmodus wechseln.

tail -f /ngfw/var/log/messages

Alle anzeigen

nat detail anzeigen

asp table socket anzeigen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.