

Universeller ZTNA für privaten Ressourcenzugriff bei sicherem Zugriff konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Über Universal ZTNA](#)

[Netzwerkerkennung](#)

[Typen für die Durchsetzung](#)

[Anwendungsfälle](#)

[Architekturkomponenten](#)

[Paketfluss](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Testfälle](#)

[Testfall 1: Remote-Benutzer - Cloud-Durchsetzung](#)

[Testfall 2 - Remote-Benutzer - Lokale Durchsetzung](#)

[Testfall 3 - Lokaler Benutzer - Lokale Durchsetzung](#)

[Testfall 4 - Lokaler und Remote-Benutzer - lokale oder Cloud-Durchsetzung mit TND](#)

[Fehlerbehebung](#)

[Nützliche Befehle:](#)

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

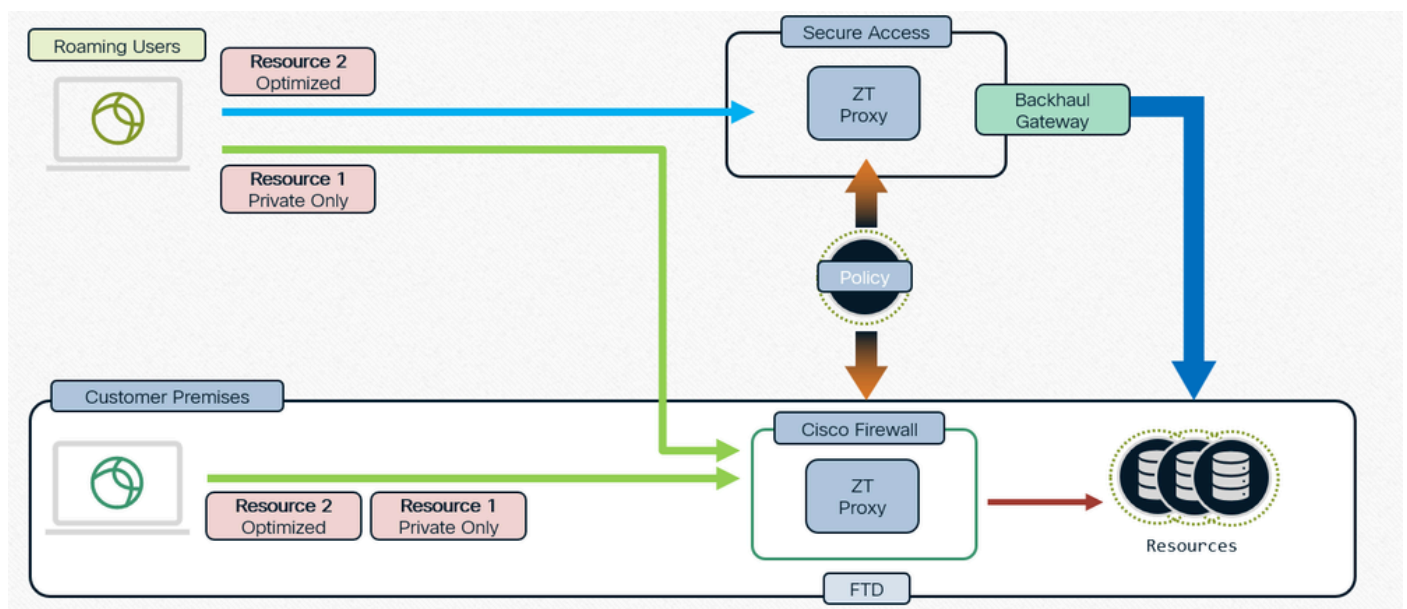
Universeller Zero Trust Network Access (uZTNA) ermöglicht es Administratoren, den Zugriff auf

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.

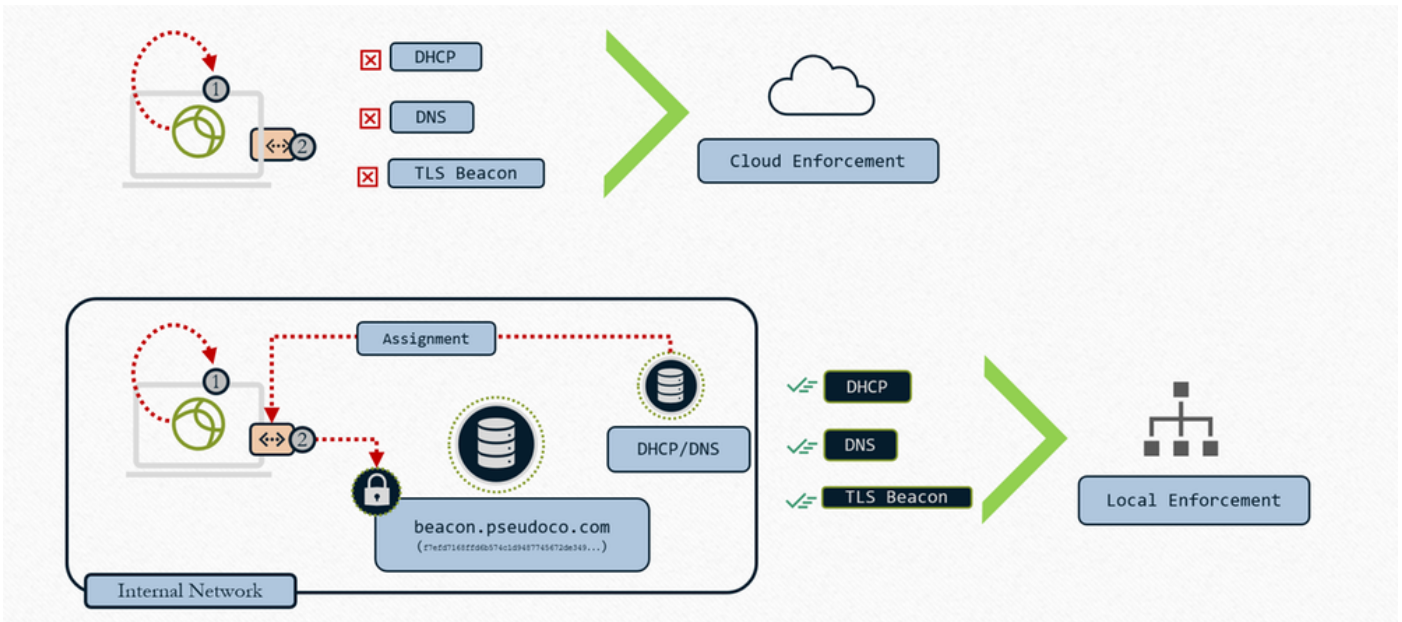
Datenverkehr-Proxys sowie die Durchsetzung von IPS-, Datei- und Malware-Richtlinien werden mit der Firepower Threat Defense (FTD) durchgeführt.



Zentrale Richtlinie, verteilte Durchsetzung

Netzwerkerkennung

Bestimmung der Cloud- oder lokalen Durchsetzung



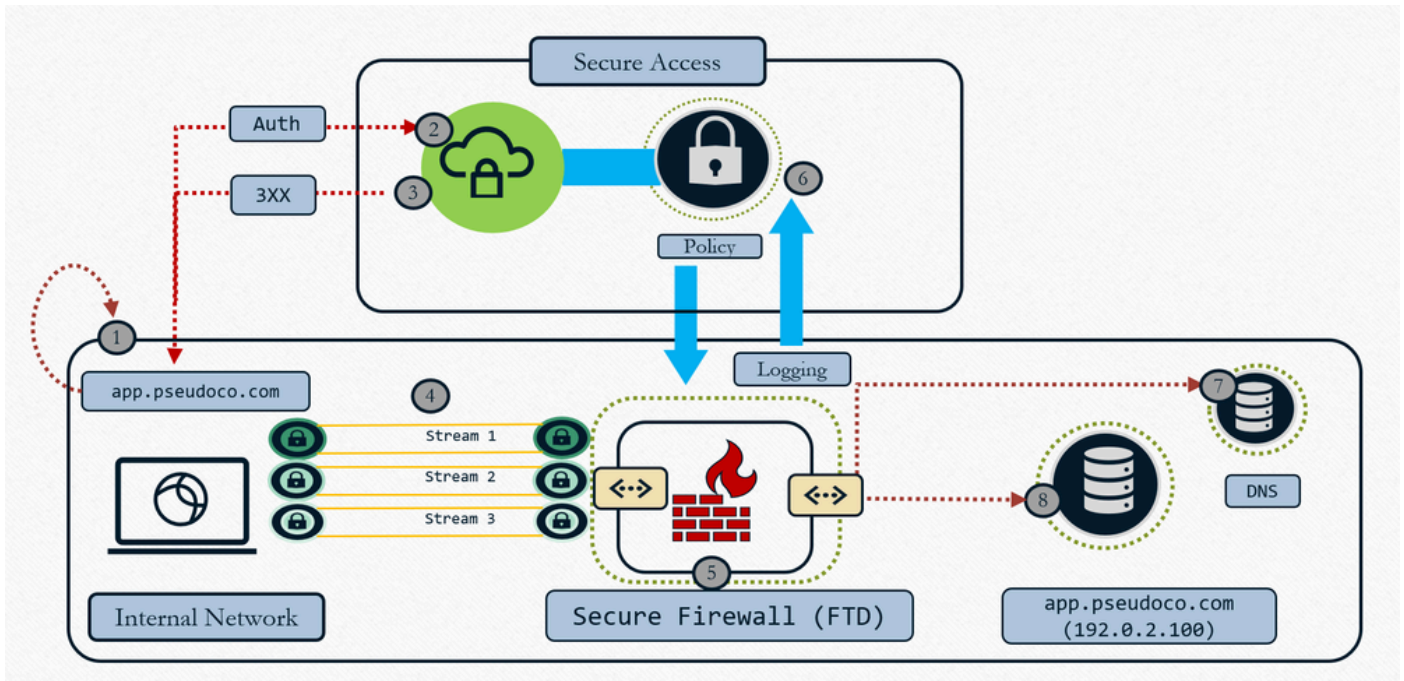
Universeller ZTNA: Festlegen der Cloud- oder lokalen Durchsetzung

- 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](#)

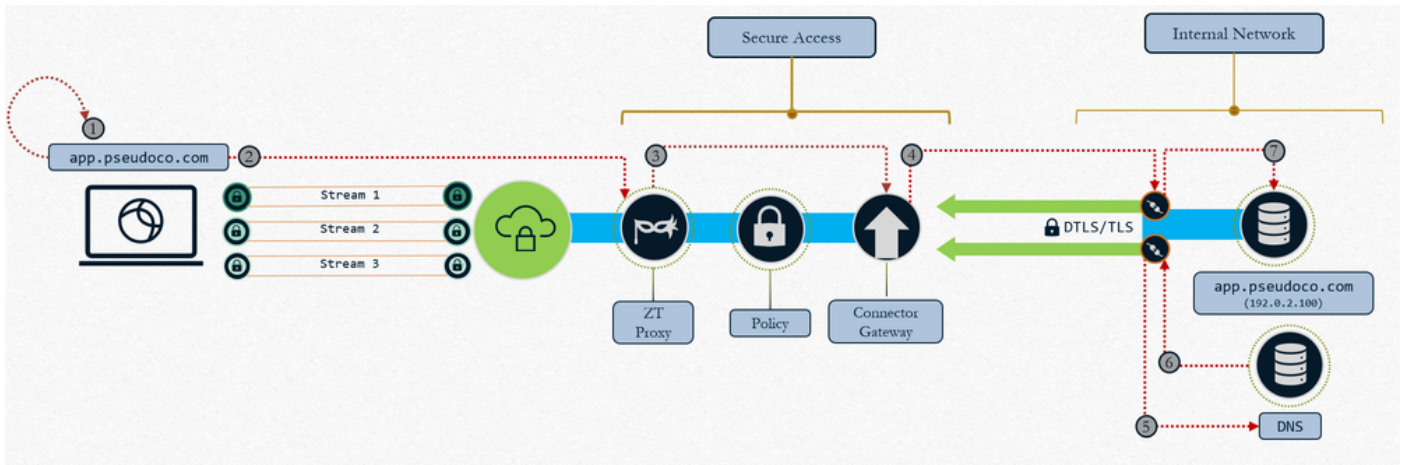
Typen für die Durchsetzung

- 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 Berichterstattung
 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

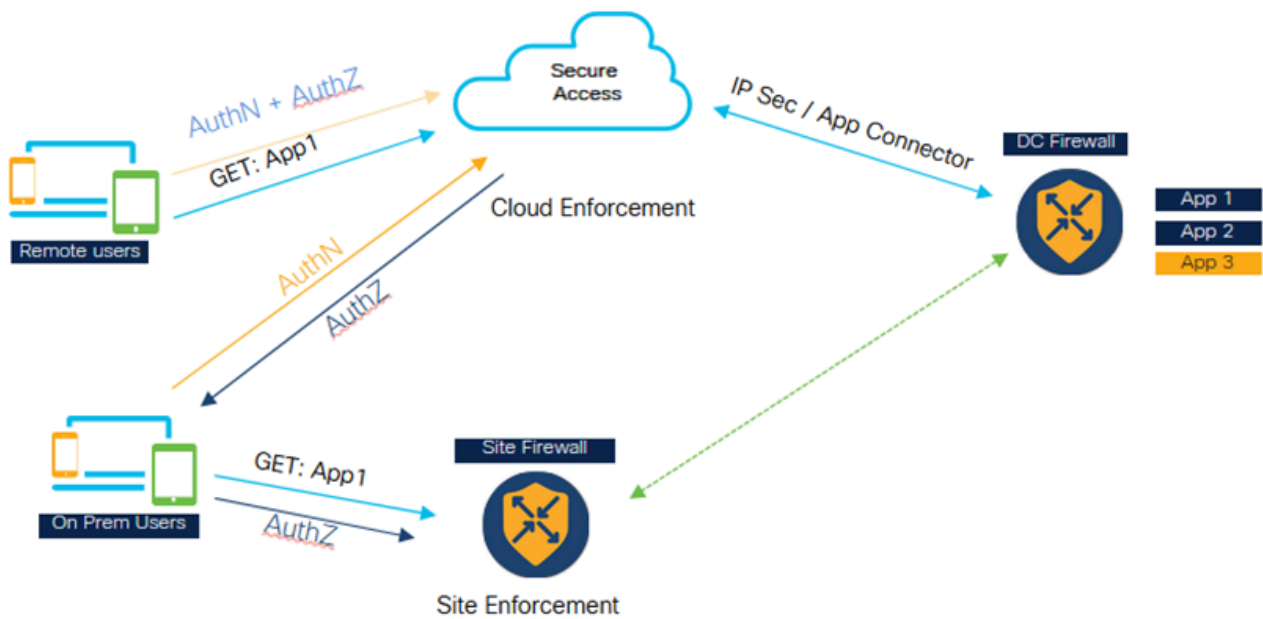


Universelles ZTNA: Durchsetzung der Cloud

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

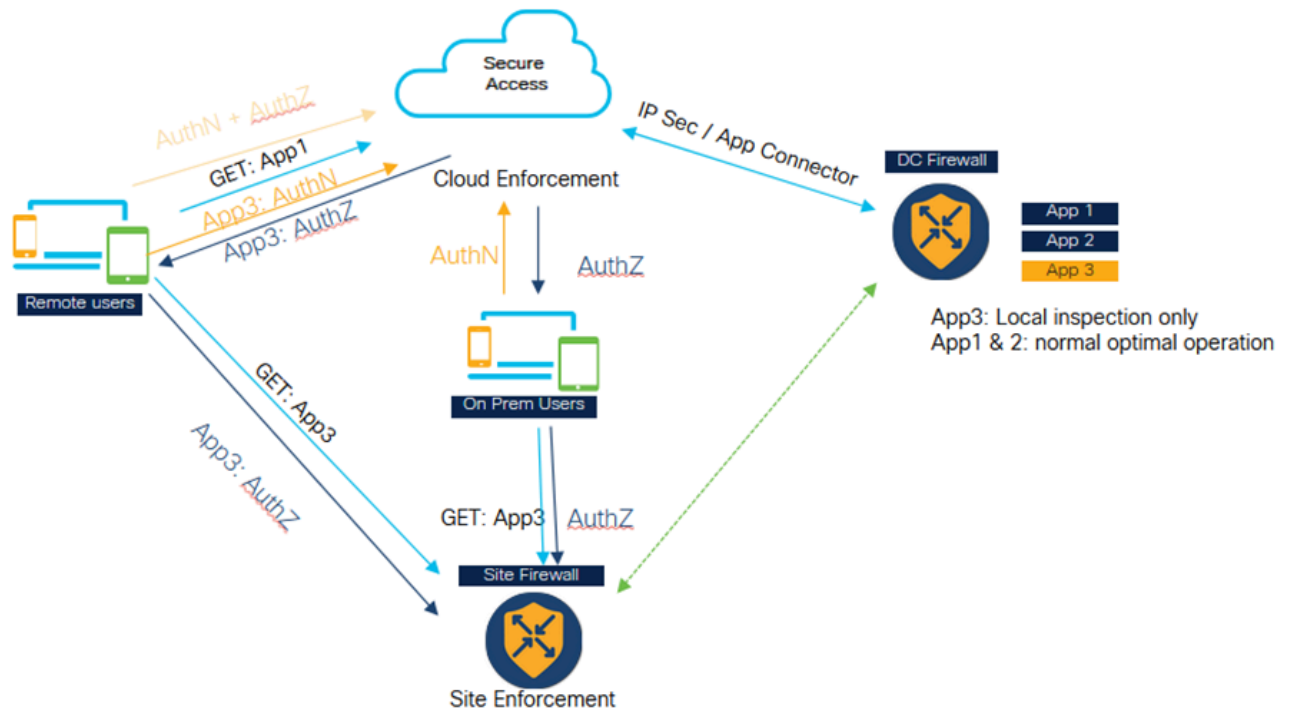
Fall 1: Konsistente und optimierte ZTNA für Benutzer vor Ort



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.

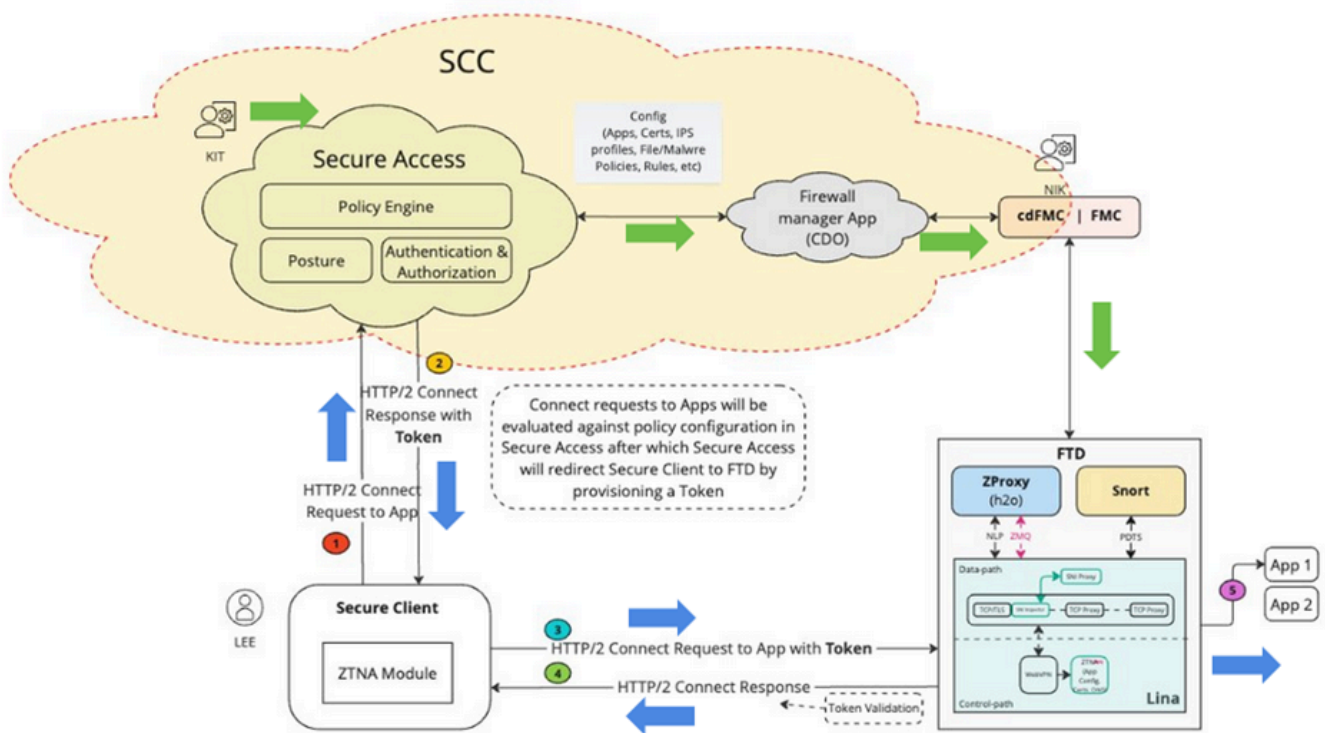
Fall 2: Private Inspektion für sensible Anwendungen



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.

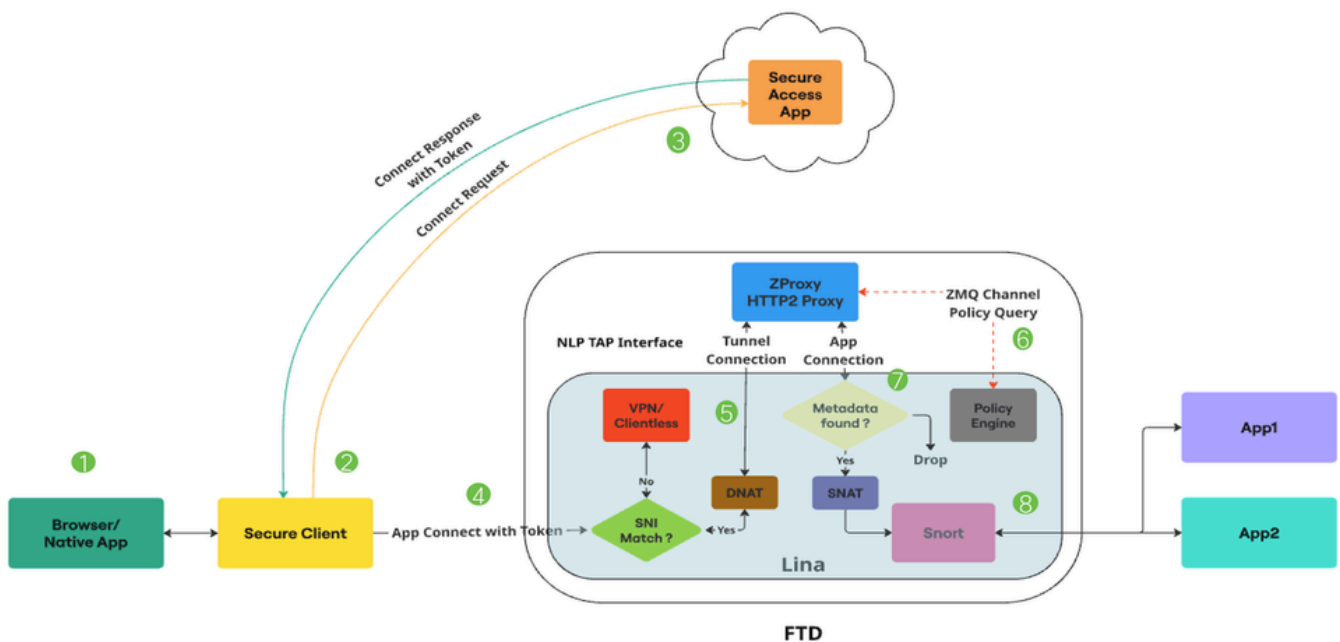
Schutz vor Firewall-Bedrohungen: FTD schützt diese Anwendungen. FTD führt einen ZT-Proxy aus, der auch als H2O bezeichnet wird (ebenso wie der Proxy in Secure Access Cloud).

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 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.

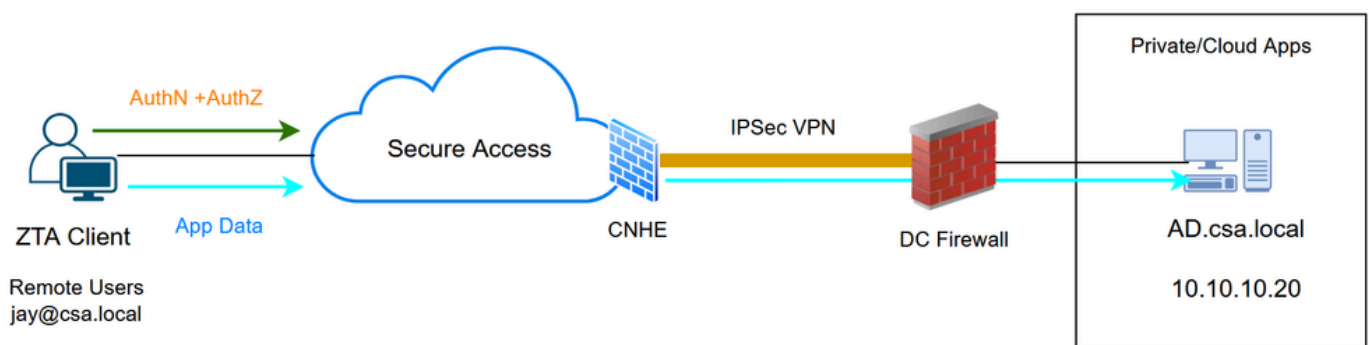
Der Zero-MQ-Kanal wird auch verwendet, um Informationen, die im Zugriffstoken vorhanden sind, an Lina weiterzugeben. (Beispiel: Regel-ID, Richtlinien-ID usw.) Lina empfängt die Zugriffstoken-Informationen und speichert sie in einer Metadaten-Datenbank.

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

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.

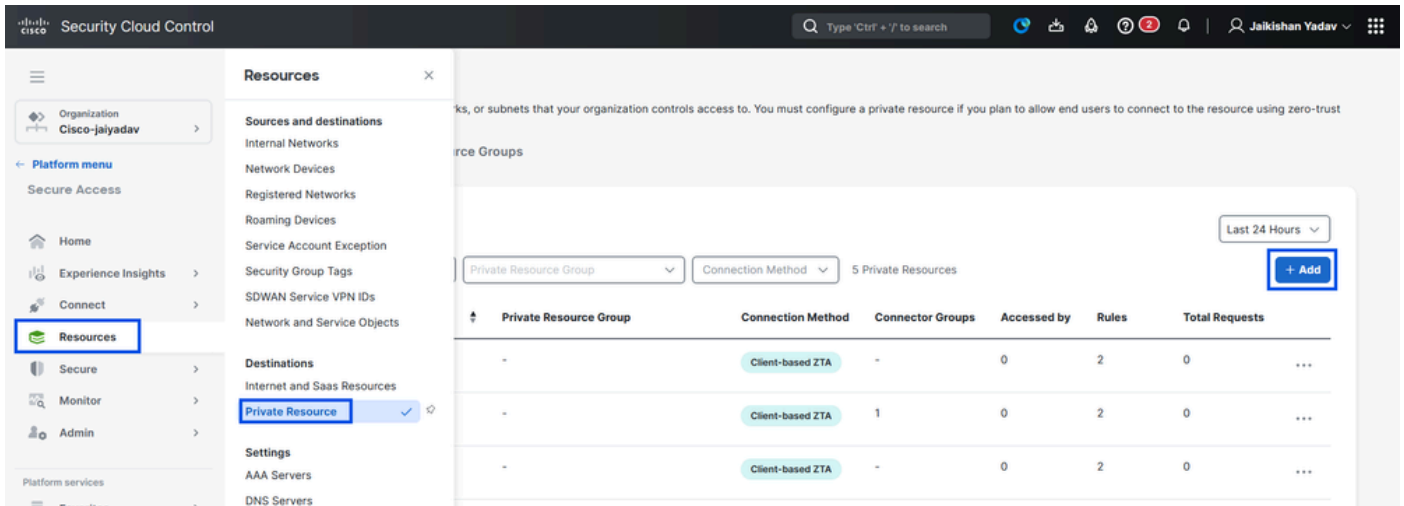


Universal ZTA - Testfall-Topologie

Schritt 1 - Definieren einer privaten Ressource für sicheren Zugriff

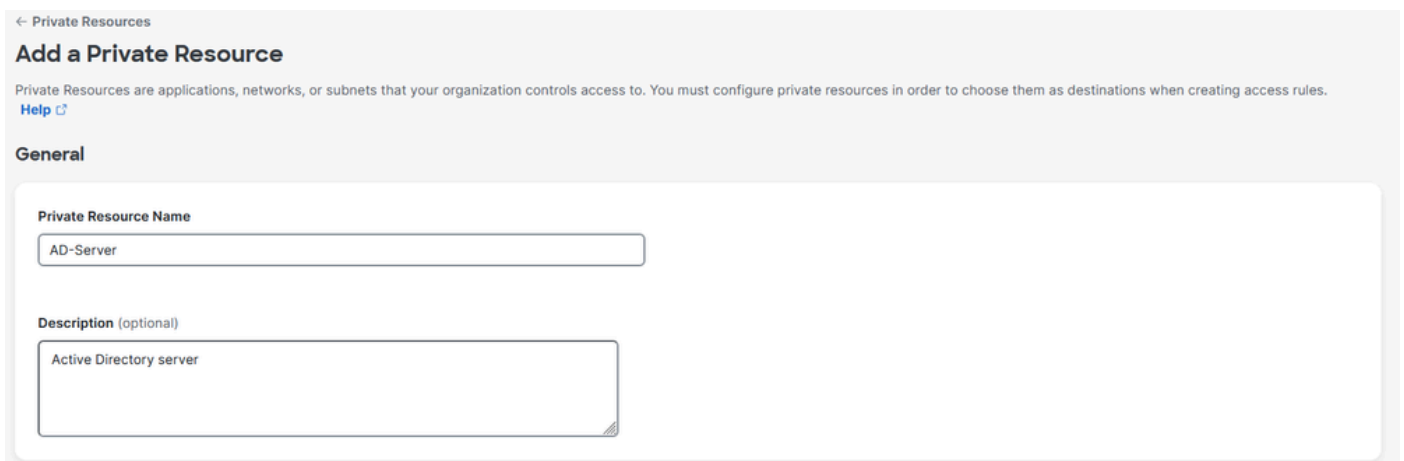
Konfigurieren einer privaten Ressource für den Zugriff über ein bei Zero Trust Access (ZTA) angemeldetes Gerät mit Cloud-Durchsetzung

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.

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ

ad.csa.local

Protocol

TCP - RDP

Port / Ranges

Any

+ Protocol & Port

Remove

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ

10.10.10.20

Protocol

TCP - RDP

Port / Ranges

Any

+ Protocol & Port

Remove + IP Address/FQDN

Use internal DNS server to resolve the domain

PrivateDNS (10.10.10.20) ^

Internal DNS Server

PrivateDNS (10.10.10.20)

Sicherer Zugriff - Konfiguration privater Ressourcen

5. Endpunktverbindungsmethoden auswählen

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Enforcement point for Remote and Local Users



Cancel

Save and Test

Save

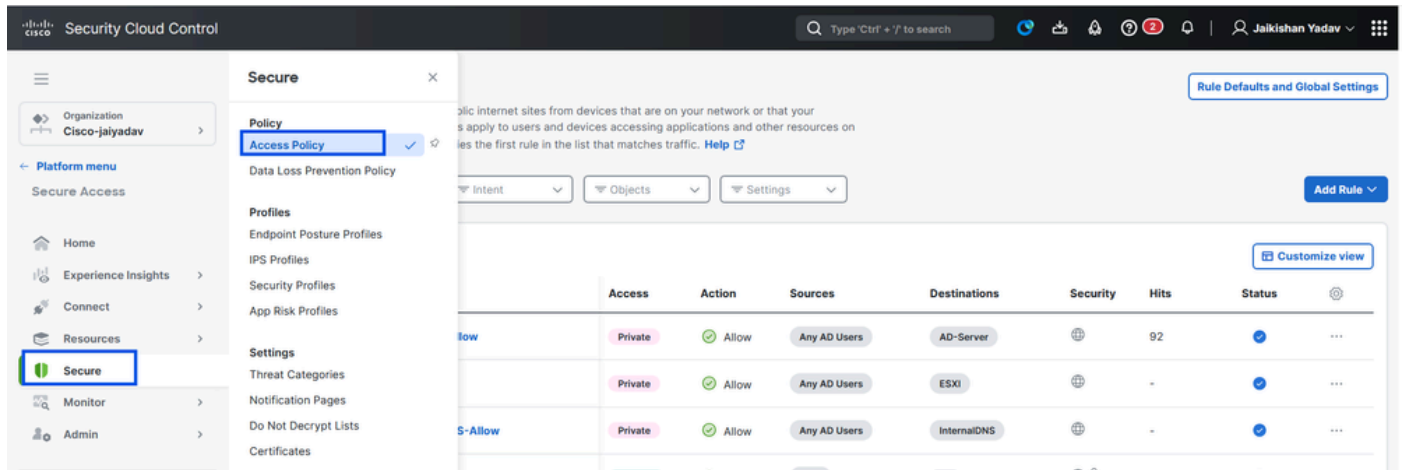
Sicherer Zugriff - Konfiguration privater Ressourcen

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](#).

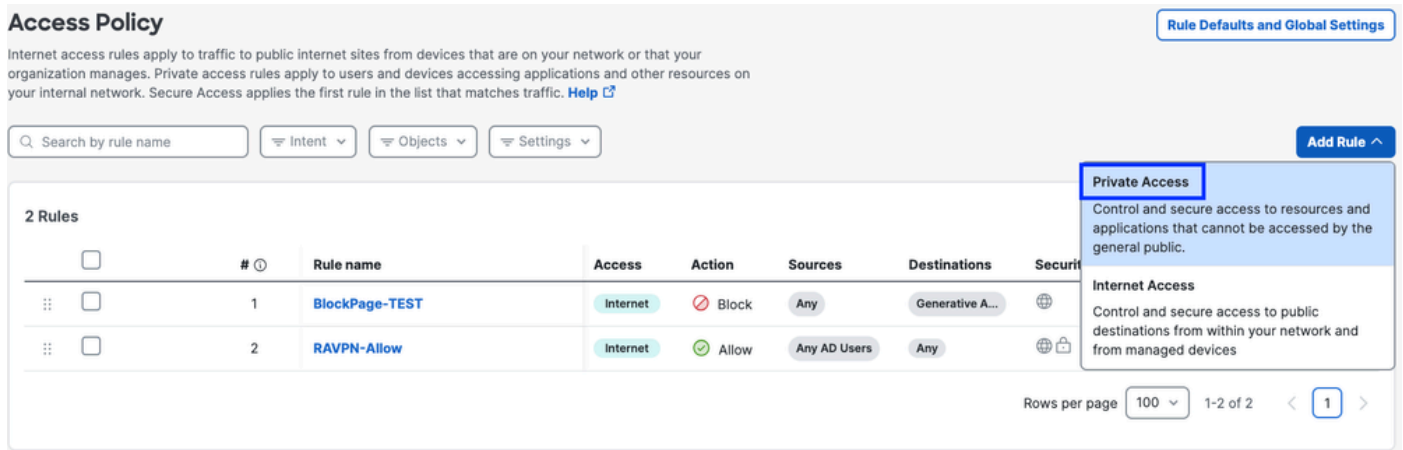
1. Navigieren Sie zu Sicher > Zugriffsrichtlinie



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

Add AD-RDP-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

AD-RDP-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

To

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

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

Rule name

AD-RDP-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources.

AD Users • Any AD Users

To

Specify one or more destinations.

Private Resources • AD-Server

+ AND

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen

Endpoint Requirements

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

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

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

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

Private Resources: **AD-Server**

For Branch connections:

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

User Authentication Requirements

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

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

2 Configure Security

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

[Cancel](#)

[Back](#)

[Next](#)

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren

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

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

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

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

Security Profile [Rule Defaults](#)

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

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

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

7. Klicken Sie auf Speichern

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

3 Rules Customize view

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		-	
2	BlockPage-TEST	Internet	Block	Any	Generative A...		-	
3	RAVPN-Allow	Internet	Allow	Any AD Users	Any		492	

Rows per page: 100 1-3 of 3

Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination		-

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

The screenshot shows the 'End User Connectivity' section of the Cisco Secure Cloud Manager. It includes tabs for 'Zero Trust Access', 'Virtual Private Network', and 'Internet Security'. Under 'Zero Trust Access', there are sections for 'Enrollment methods' and 'Zero Trust Access Profiles'. The 'Zero Trust Access Profiles' section shows a table with columns for '#', 'Name', 'Secure Private Access', 'Secure Internet Access', 'Users & Groups', and 'Last Used'. A message states 'No ZTNA profiles created.' and there is a '+ ZTA Profile' button.

Sicherer Zugriff - ZTA-Profil

2. Fügen Sie die private Ressource hinzu

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

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

Destinations & Private Resources

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

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

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

Sicherer Zugriff - ZTA-Profil

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

Private Resource

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

Cancel Save

Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen

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


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

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

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

Users 0 | Groups 0

Q Search + Users and Groups

Name	Email	Type	Users
 No users + Users and Groups			

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

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

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

Users 1 | Groups 0

Q Search + Users and Groups

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

Rows per page: 10 < >

Back Close

Sicherer Zugriff - ZTA-Profil

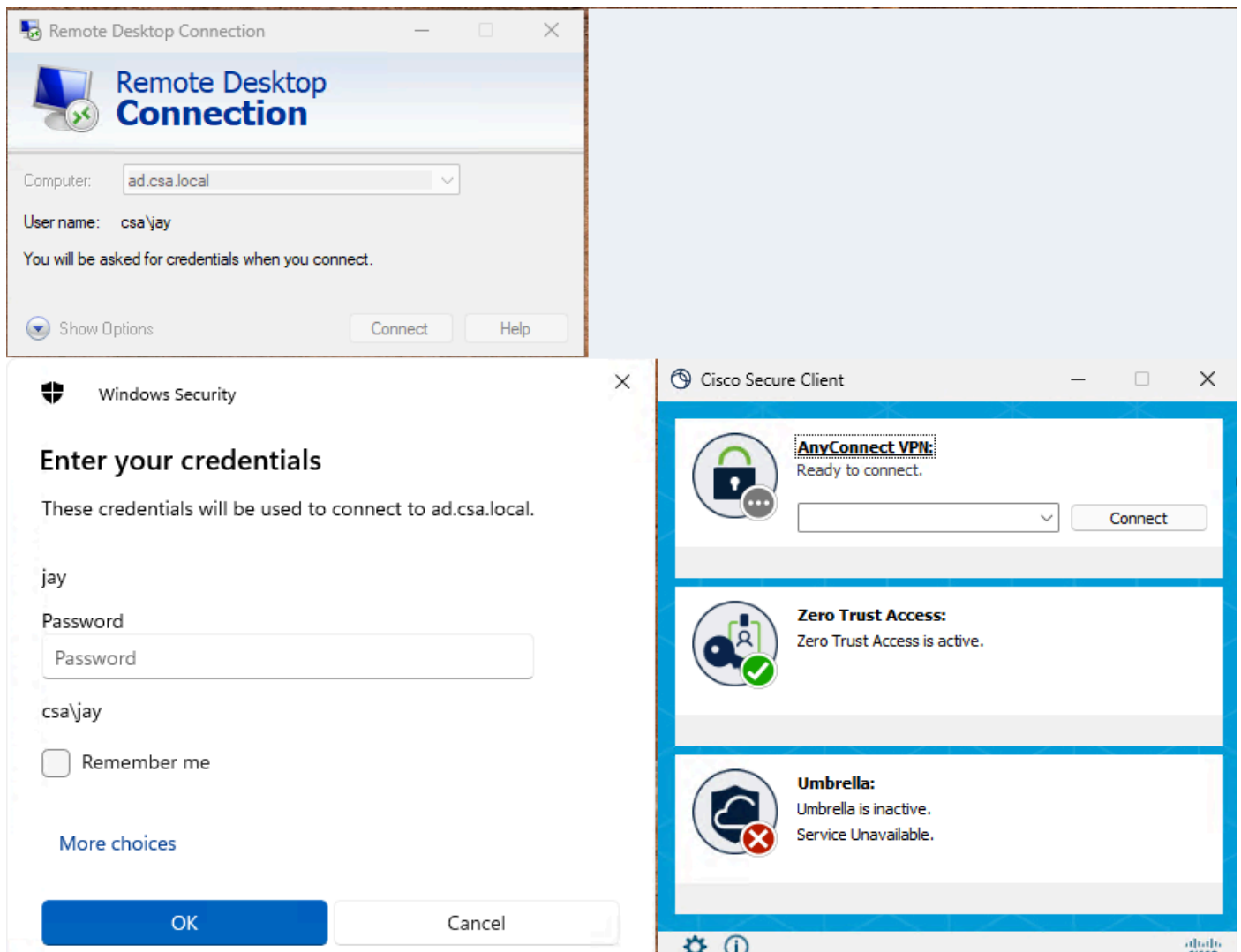


Anmerkung: Es kann bis zu 15-20 Minuten dauern, die Konfiguration für die zugewiesene private Ressource per Push und Synchronisierung mit dem Client zu übertragen.

Schritt - 4 Überprüfen des Zugriffs auf die private Ressource

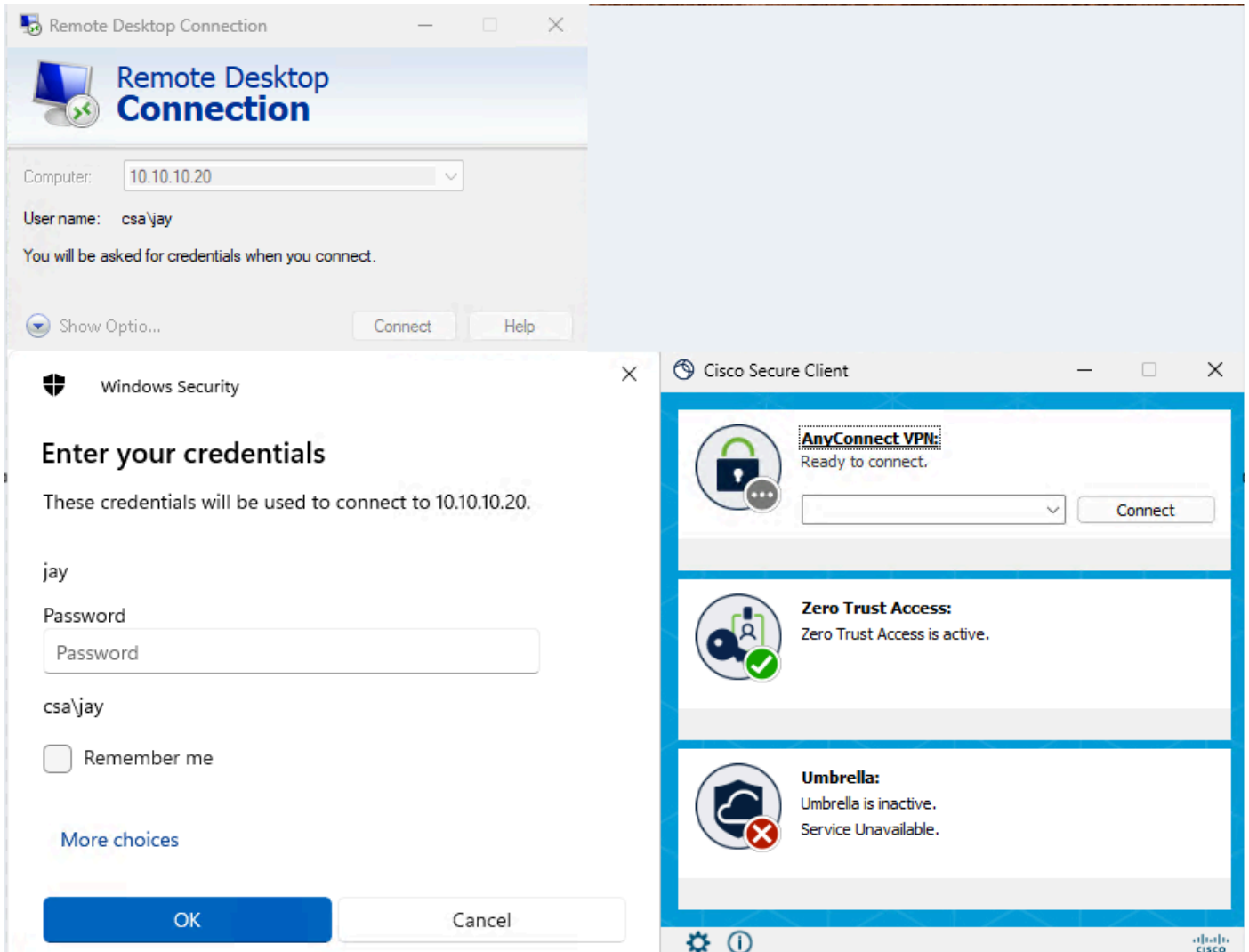
1. Zugriff auf die private Ressource

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

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 RESPONSE Allowed Restore to default layout Save Search

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

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

Sicherer Zugriff - Aktivitätssuche

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 **PORT** 3389 Restore to previous state Save Search

3 Total Viewing activity from Jan 11, 2026 4:53 AM to Jan 12, 2026 4:53 AM Page: 1 Results per page: 50 1 - 3 of 3

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

Event Details

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

Page: 1 Results per page: 50 1 - 3 of 3

Sicherer Zugriff - Aktivitätssuche

Activity Search Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 Restore to default layout Save Search

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

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

Sicherer Zugriff - Aktivitätssuche

Activity Search

Schedule Export CSV LAST 24 HOURS

Search by domain, identity, or URL Advanced CLEAR

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

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

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 12, 2026 5:51 AM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: AD-RDP-Allow

Resource/Application: AD-Server

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: 10.10.10.20

Destination IP

Sicherer Zugriff - Aktivitätssuche

3. FMC-Verbindungsereignisse überprüfen

Events Troubleshooting

Destination Port / ICMP Code 3389

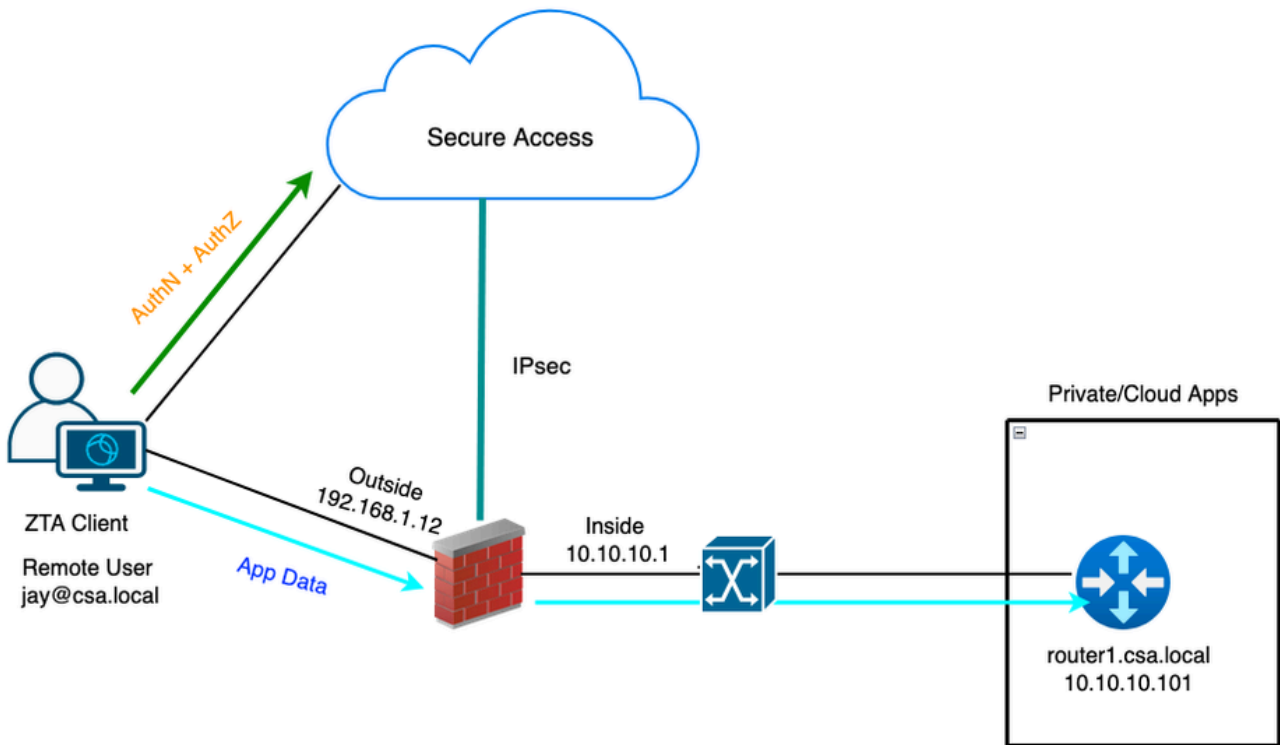
7 events Last 1 hour

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

FMC-Verbindungsereignisse

Testfall 2 - Remote-Benutzer - Lokale Durchsetzung

Der Zugriff auf eine private Ressource über lokale Durchsetzung erfolgt bei dieser Art von Richtlinienbewertung 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.

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

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.

← Private Resources

Add a Private Resource

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

General

Private Resource Name

Router1

Description (optional)

Router1 PR for UZTNA testing

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.

Private resource address

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

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

Use internal DNS server to resolve the domain

Internal DNS Server: PrivateDNS (10.10.10.20)

Sicherer Zugriff - Konfiguration privater Ressourcen

5. Endpunktverbindungsmethoden auswählen

6. Wählen Sie FTD als lokale Durchsetzungspunkte

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

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

Enforcement point for Remote User



Enforcement point for Local user



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

Change the remotely reachable addresses

Cancel

Save and Test Save

Sicherer Zugriff - Konfiguration privater Ressourcen



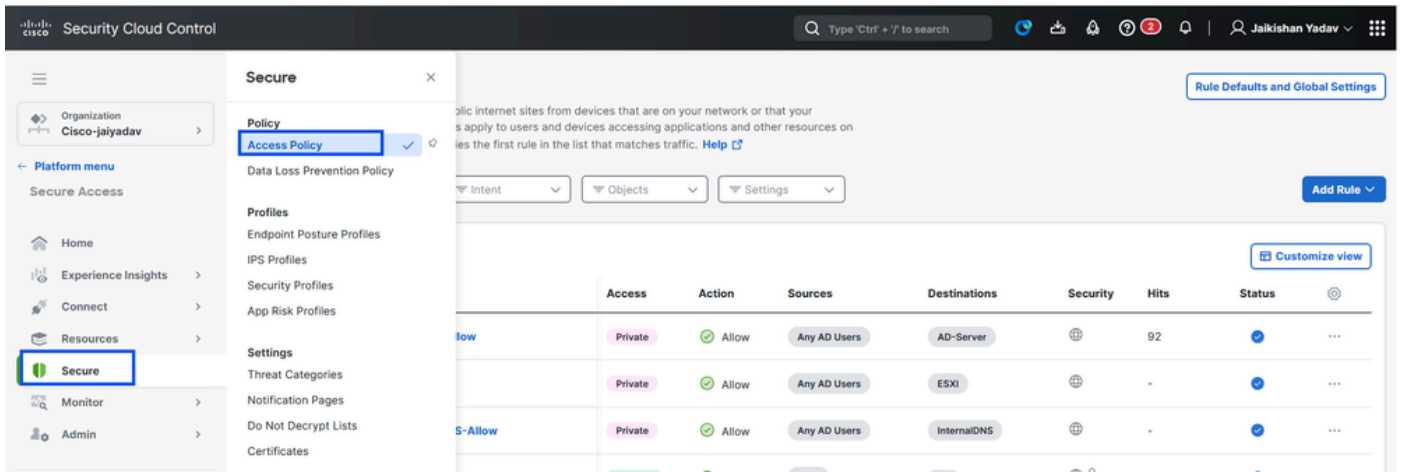
Anmerkung: Je nach gewählter Registrierungsart ordnet diese Änderung den PR automatisch dem FTD zu und löst eine Richtlinienbereitstellung aus.

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](#).

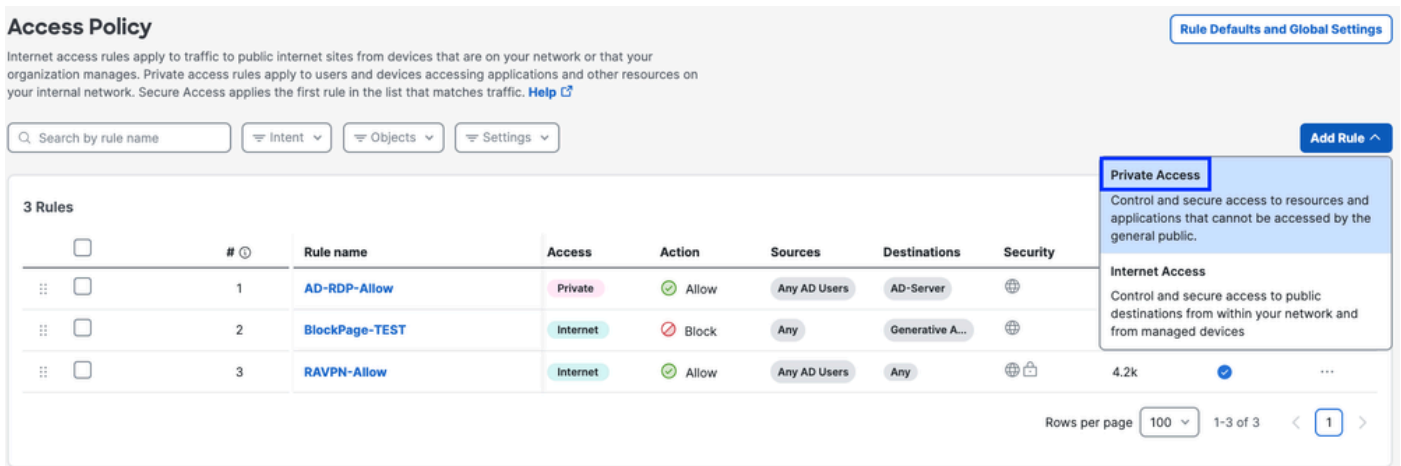
1. Navigieren Sie zu Sicher > Zugriffsrichtlinie



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

Add Router1-SSH

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

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

Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

From

Specify one or more sources.

AD Users - Any AD Users

To

Specify one or more destinations.

Private Resources - Router1

+ AND

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen

Endpoint Requirements

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

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

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

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

Private Resources: **Router-1**

For Branch connections:

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

User Authentication Requirements

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

Disabled

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

2 Configure Security

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

[Cancel](#)

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren

1 Specify Access

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

2 Configure Security

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

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

Disabled

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

Security Profile [Rule Defaults](#)

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

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

[Cancel](#)

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

7. Klicken Sie auf Speichern

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

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

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

Schritt 3 - Überprüfen der Zuordnung von PR auf dem FTD

1. Navigieren Sie zu Verbinden > Netzwerkverbindungen > FTDs

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' panel with 'Network Connections' selected under 'Essentials'. Below this, there are two status indicators: '0 Warning' and '1 Connected'. The 'FTDs' tab is active, showing a list of tunnel groups with filters for 'Region' and 'Status'. There are 2 Tunnel Groups listed. An '+ Add' button is visible at the bottom right.

Sicherer Zugriff - PR-Verifizierung

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

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

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

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status	
Synced	1

[View resources associated to this FTD](#)

[Associate Resources](#)

Sicherer Zugriff - PR-Verifizierung

Resources associated with FMC_FTD

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

Q Search by resource name

Configuration status

1 Resources

[Associate Resources](#)

Resource name

Status

Router1

Synced

[Close](#)

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.

The screenshot displays the 'Network Connections' section of the Palo Alto Networks management console. It shows a table of FTDs configured for Universal Zero Trust Access. The table has columns for FTD Name, Version, FMC, UZTA Configuration status, and Associated Resources. The 'FMC_FTD' entry is highlighted, showing a status of 'Synced'. To the right, a detailed view for 'FMC_FTD' is shown, including Firewall Details, UZTA Configuration status (Synced), and Assigned Trusted Network (LAN). The 'Associated Resources' section shows one resource associated with the FTD, also in a 'Synced' state.

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

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.

End User Connectivity

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

Zero Trust Access | Virtual Private Network | Internet Security

Enrollment methods Manage

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

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

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

Actions: Edit, Delete

Sicherer Zugriff - ZTA-Profil

2. Fügen Sie die private Ressource hinzu

Create profile

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

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

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

1 Secure Private Access (0 Destinations)

2 Secure Internet Access

3 Users and Groups

Search by destination:

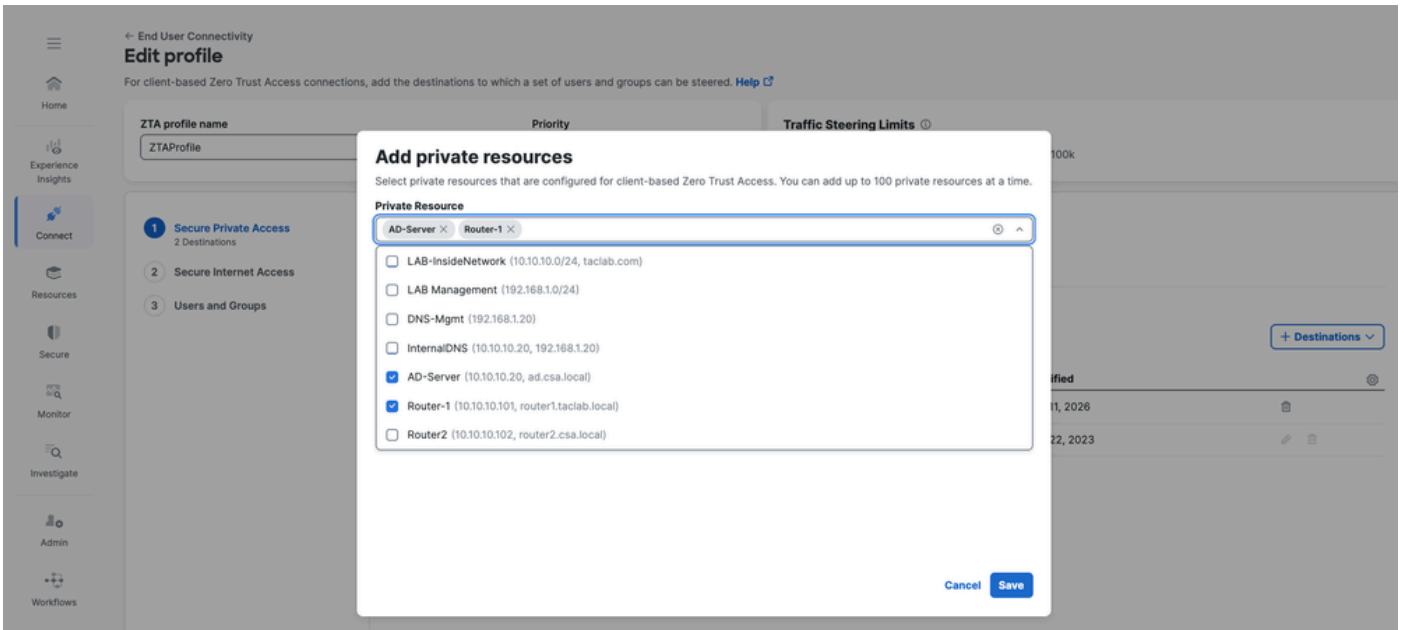
Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

Actions: + Destinations

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

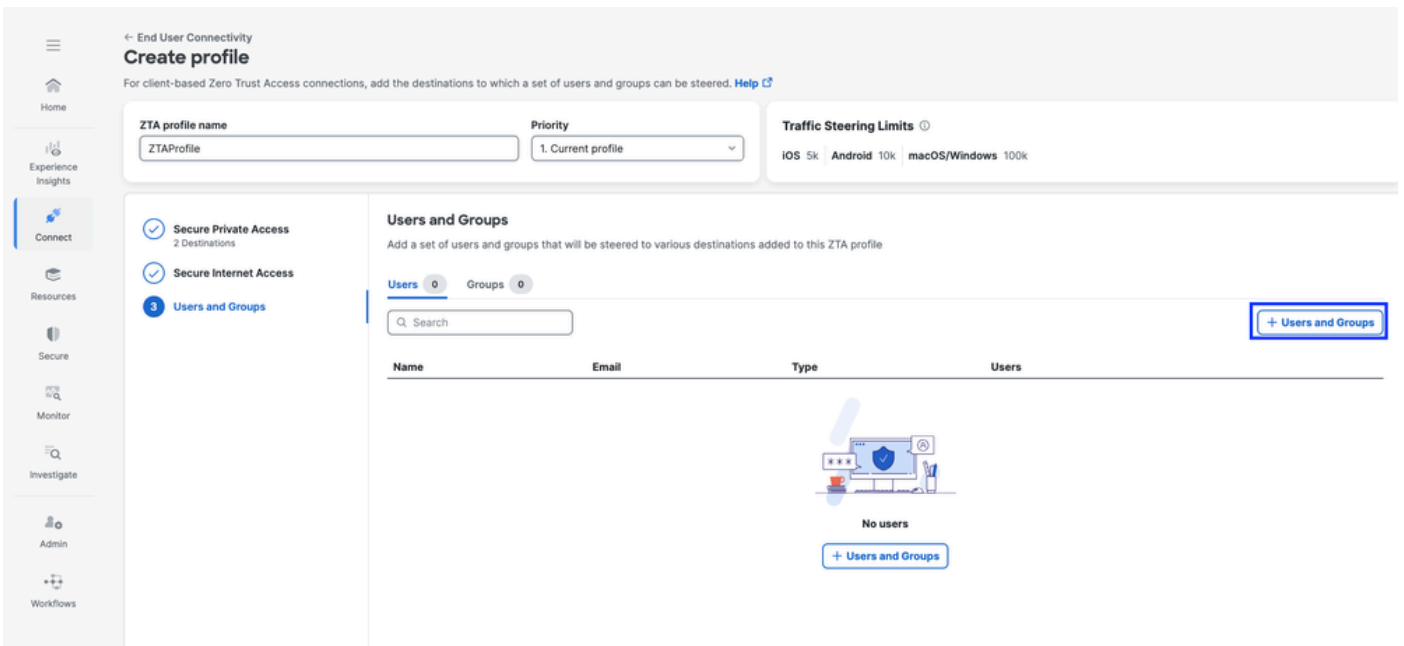
Add Destination
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Sicherer Zugriff - ZTA-Profil



Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen



Sicherer Zugriff - ZTA-Profil

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

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

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

Users: 1 | Groups: 0

Q Search + Users and Groups

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

Rows per page: 10

Back Close

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
```

Sicherer Zugriff - PR-Tests

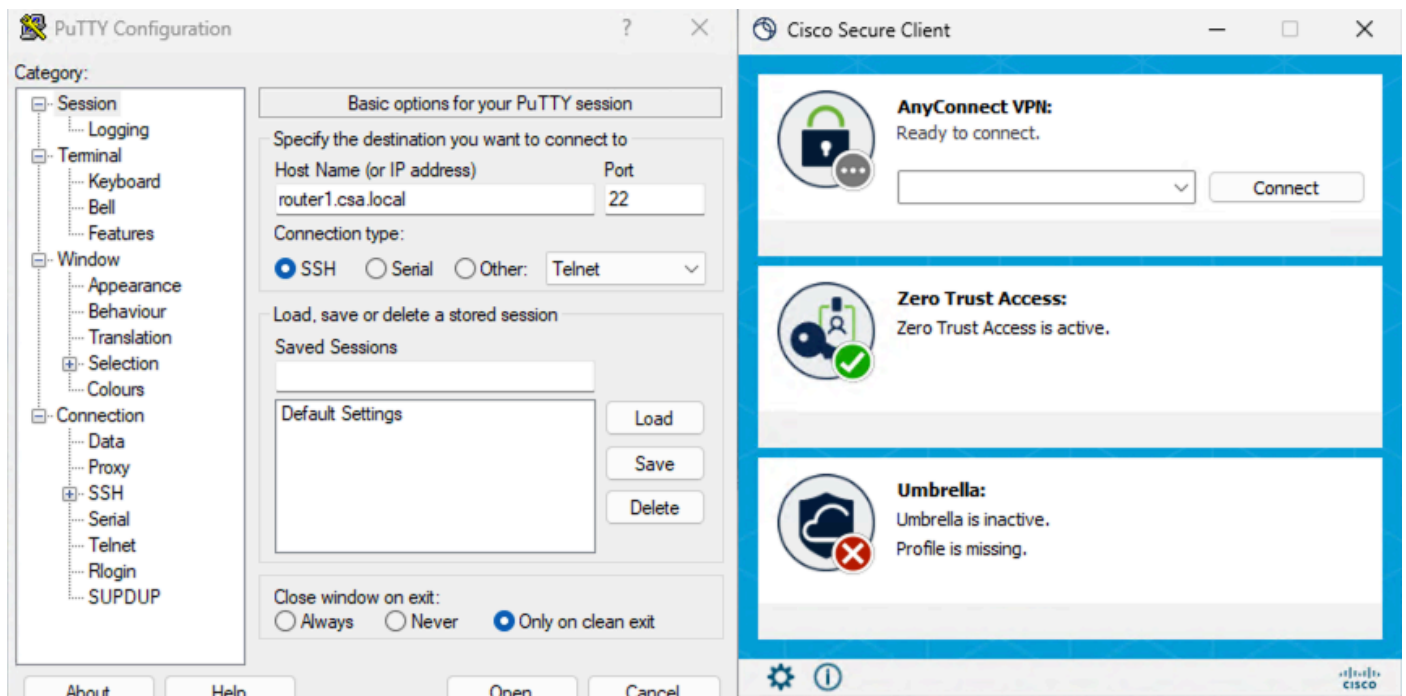
2. Überprüfen Sie, ob FTD über FQDN eine Verbindung zu privaten Ressourcen herstellen kann.

```
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# █
```

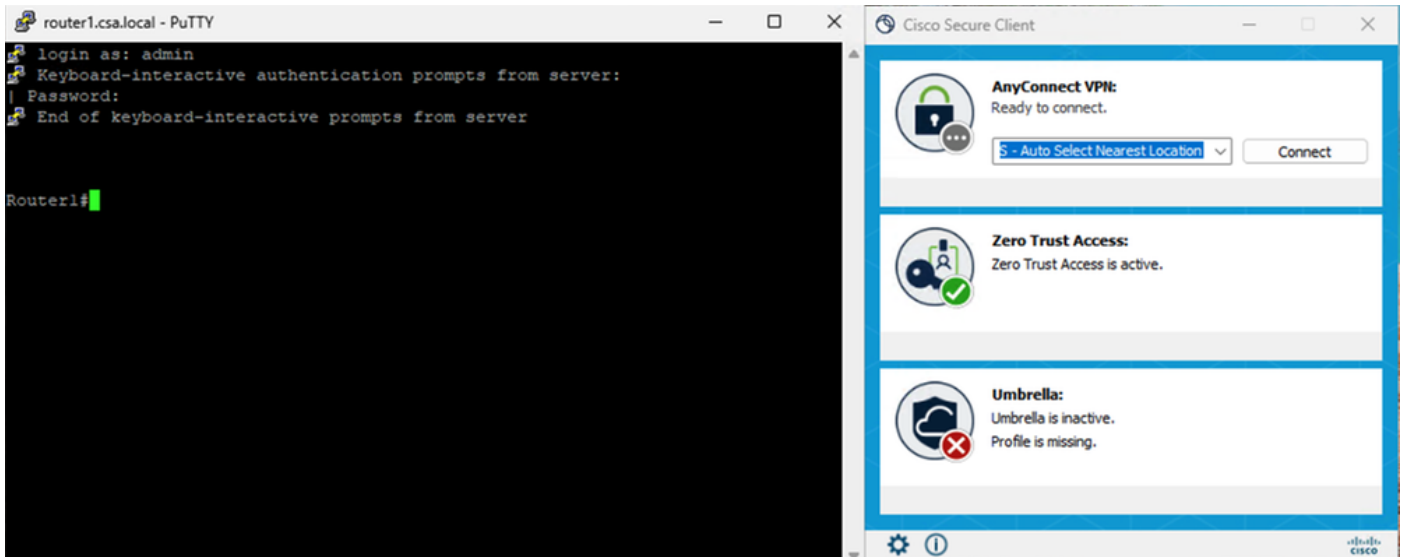
Sicherer Zugriff - PR-Tests

3. Testen der SSH-Verbindung mit der privaten Ressource

Zugriff auf den PR über FQDN

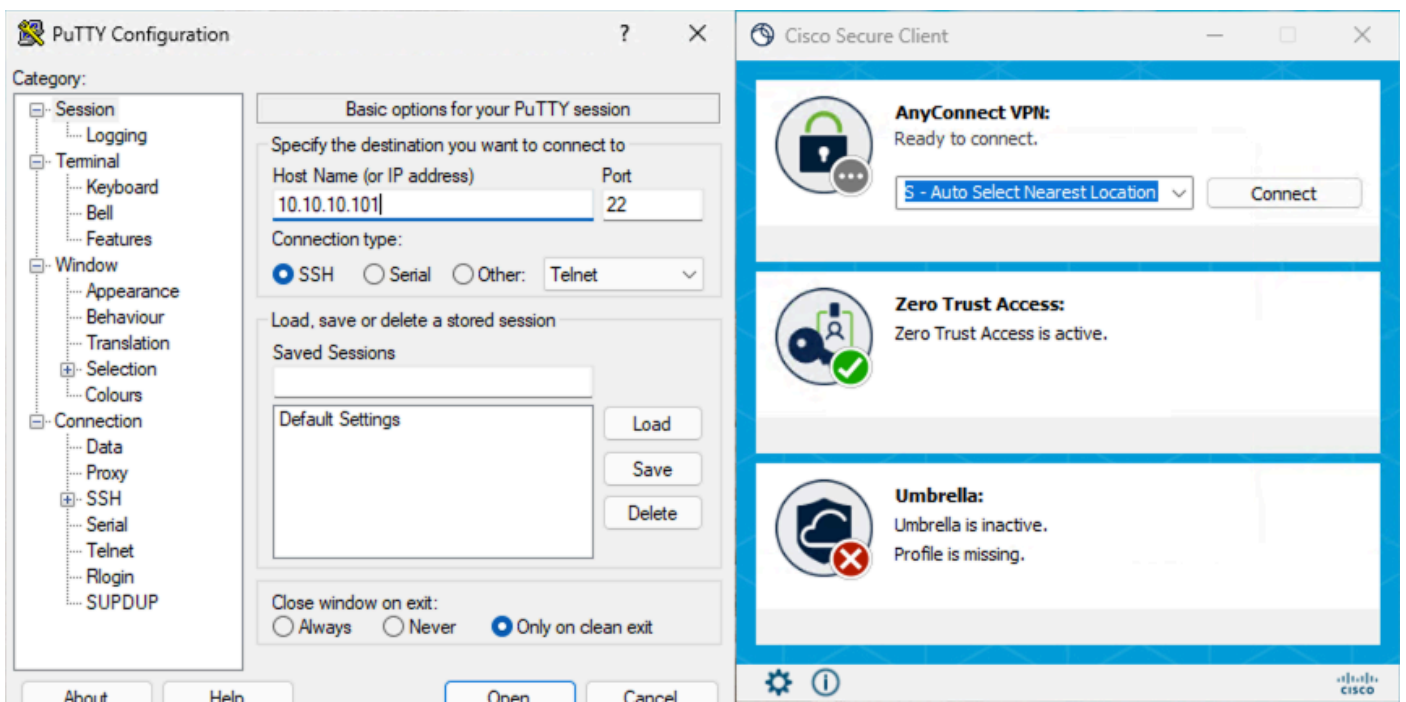


Sicherer Zugriff - PR-Tests

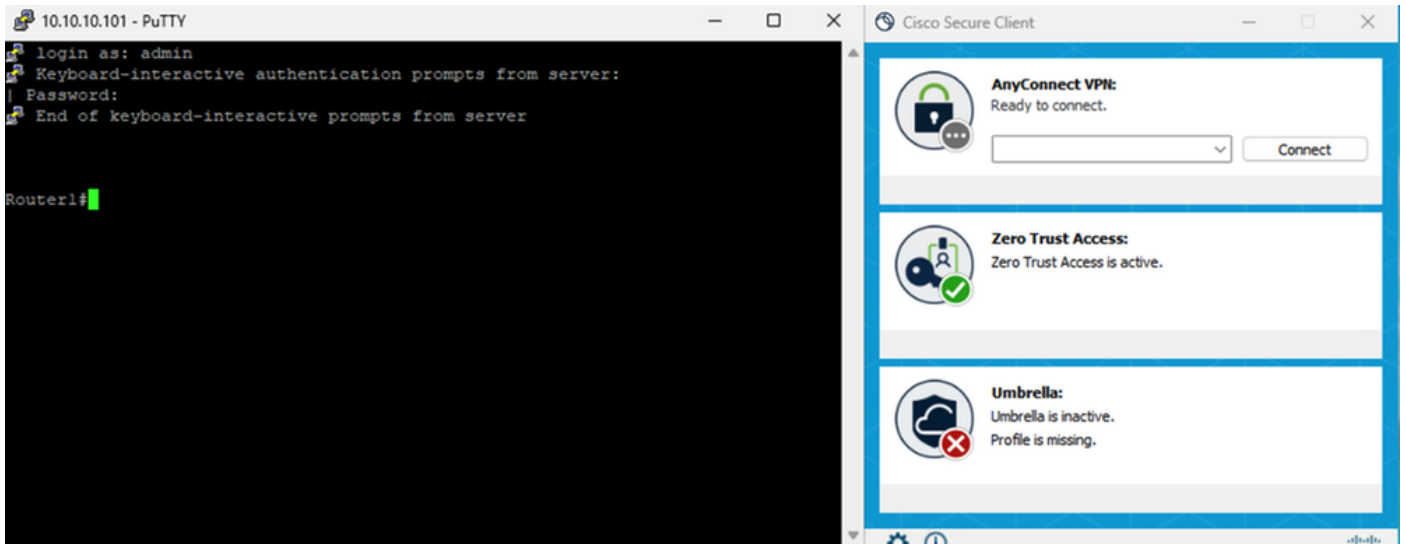


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse



Sicherer Zugriff - PR-Tests



Sicherer Zugriff - PR-Tests

4. Protokolle für die Suche nach sicheren Zugriffsaktivitäten überprüfen

Activity Search

Filters: Search by domain, identity, or URL. Domain: router1.csa.local. Response: Allowed.

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

Sicherer Zugriff - Aktivitätssuche

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:55 PM

Access details

Identity: jay (jay@csa.local)

Win: Win10

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

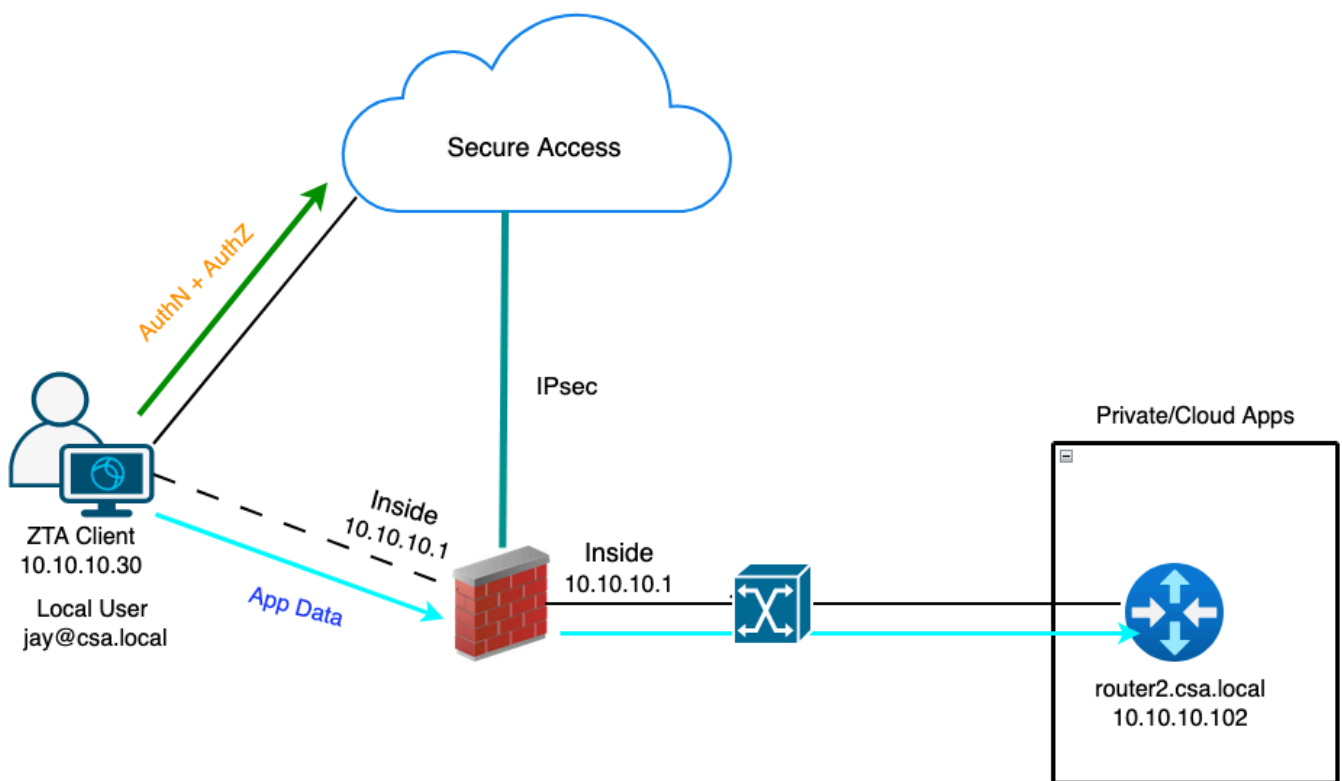
Enforcement Point: FTD > FMC_FTD

Destination: router1.csa.local

Destination IP: -

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.

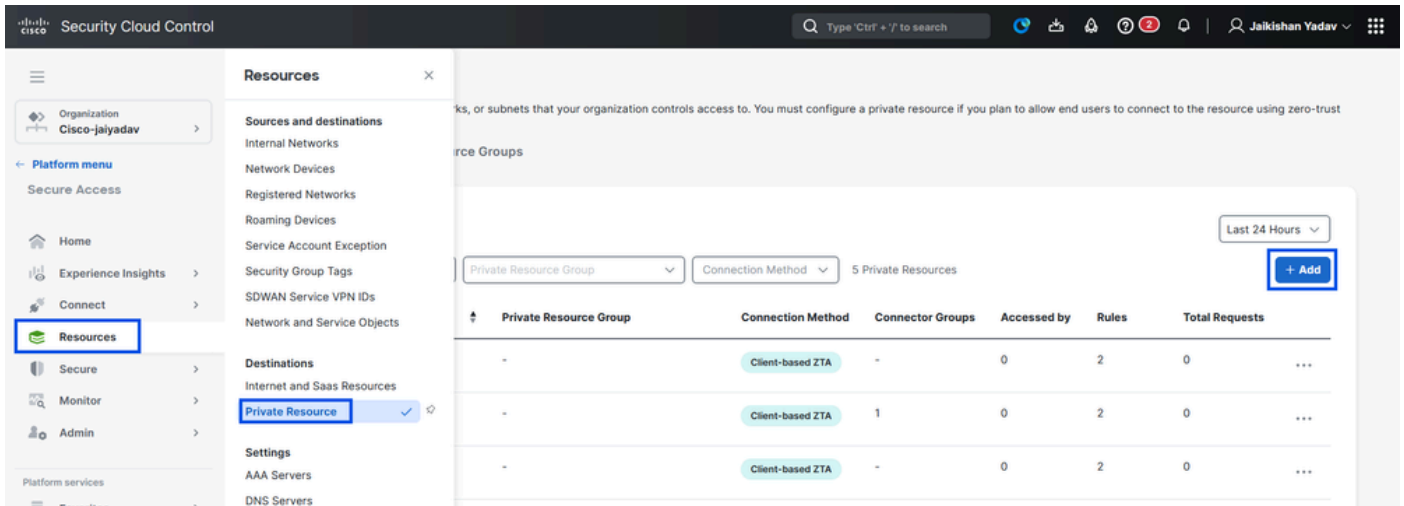


Universelle ZTA - Topologie der Testfälle

Schritt 1 - Definieren einer privaten Ressource für sicheren Zugriff

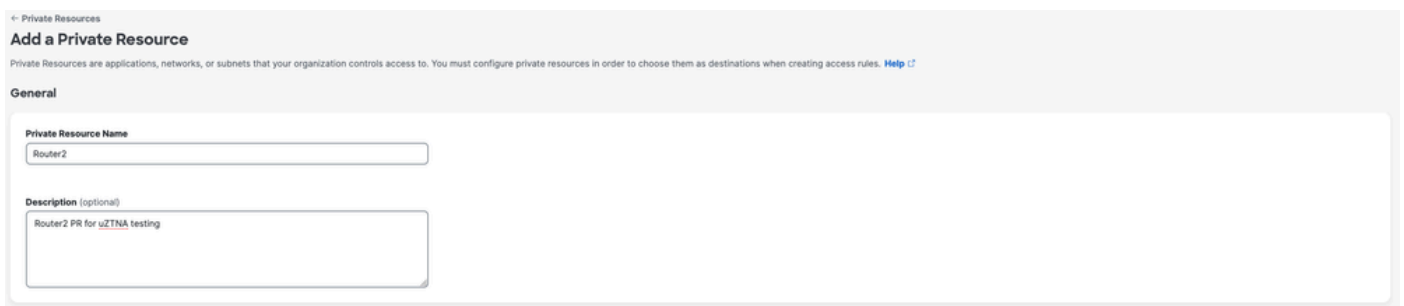
Konfigurieren einer privaten Ressource für den Zugriff über ein bei Zero Trust Access (ZTA) angemeldetes Gerät mit Cloud-Durchsetzung

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.

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) Protocol Port / Ranges + Protocol & Port

Remove

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) Protocol Port / Ranges + Protocol & Port

Remove + IP Address/FQDN

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

Internal DNS Server

Sicherer Zugriff - Konfiguration privater Ressourcen

5. Endpunktverbindungsmethoden auswählen

6. Wählen Sie FTD als lokale Durchsetzungspunkte

Endpoint Connection Methods

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

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

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

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

Search by FTD na...

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

Enforcement point for Remote User

Remote user Local Firewall

Enforcement point for Local user

User in a trusted network Local Firewall

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

Change the remotely reachable addresses

Cancel Save and Test Save

Sicherer Zugriff - Konfiguration privater Ressourcen



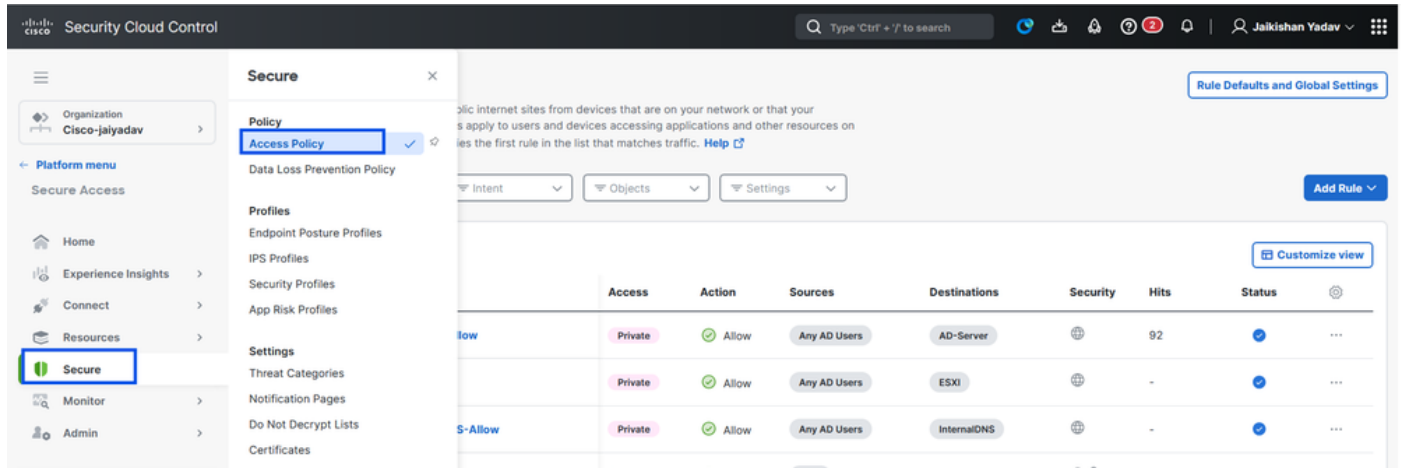
Anmerkung: Je nach gewählter Registrierungsart ordnet diese Änderung den PR automatisch dem FTD zu und löst eine Richtlinienbereitstellung aus.

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](#).

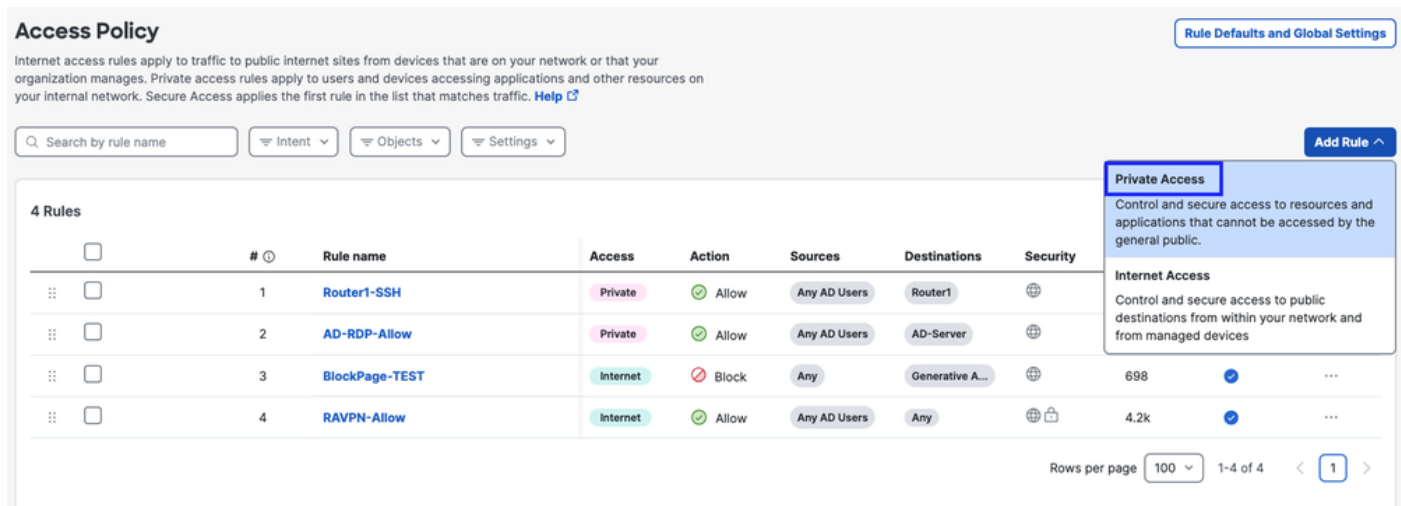
1. Navigieren Sie zu Sicher > Zugriffsrichtlinie



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

Add Router2-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

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

Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources

AD Users - Any AD Users

To

Specify one or more destinations

Private Resources - Router2

+ AND

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen

Endpoint Requirements

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

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

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

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

Private Resources: **Router2**

For Branch connections:

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

User Authentication Requirements

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

Disabled

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

2 Configure Security

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

[Cancel](#)

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren

1 Specify Access

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

2 Configure Security

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

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

Disabled

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

Security Profile [Rule Defaults](#)

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

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

▼

[Cancel](#)

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

7. Klicken Sie auf Speichern

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

5 Rules

Customize view

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

Rows per page 100 1-5 of 5 1

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

Schritt 3 - Überprüfen der Zuordnung von PR auf dem FTD

1. Navigieren Sie zu Verbinden > Netzwerkverbindungen > FTDs

The screenshot shows the Cisco Security Cloud Control interface. The 'Connect' section is active, with 'Network Connections' selected under 'Essentials'. The 'FTDs' tab is highlighted, showing a summary of 0 Warning and 1 Connected. The interface includes a search bar, navigation menu, and various status indicators.

Sicherer Zugriff - PR-Verifizierung

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

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

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

Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status
Synced 2

View resources associated to this FTD

Associate Resources

Sicherer Zugriff - PR-Verifizierung

Resources associated with FMC_FTD

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

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

Resource name	Status
Router1	Synced
Router2	Synced

Close

3. Klicken Sie auf Schließen

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

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

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

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

```

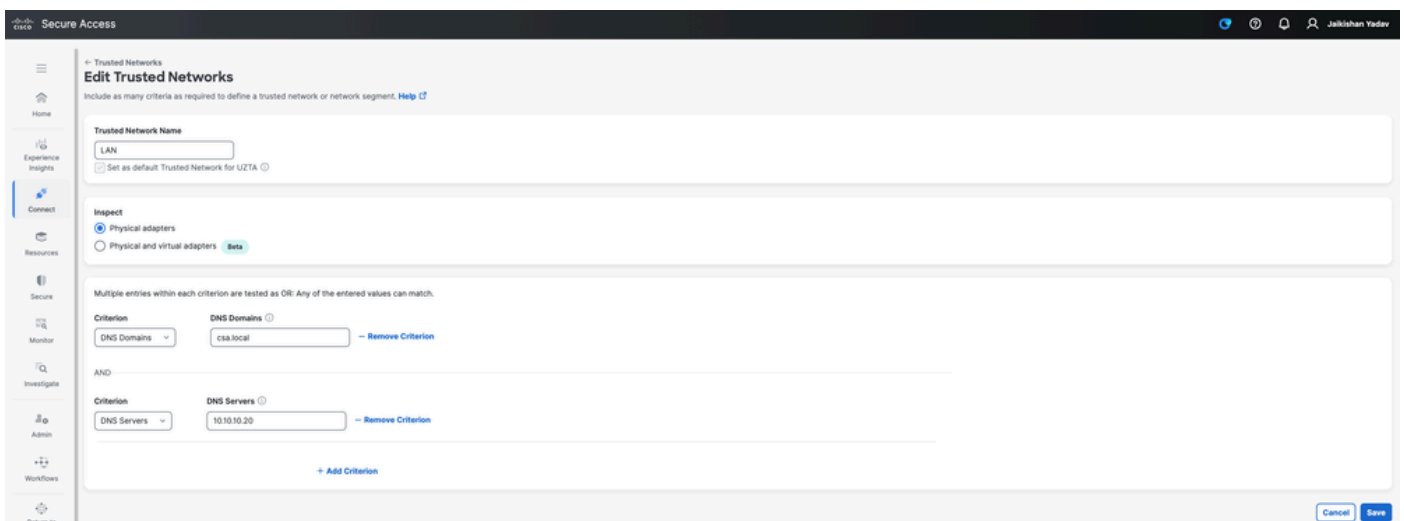
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal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

End User Connectivity

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

Zero Trust Access | Virtual Private Network | Internet Security

Enrollment methods Manage

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

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

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

Buttons: Edit, Delete

Sicherer Zugriff - ZTA-Profil

2. Fügen Sie die private Ressource hinzu

Create profile

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

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

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

1 Secure Private Access (0 Destinations)

2 Secure Internet Access

3 Users and Groups

Secure Private Access

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

Traffic Steering | Options

Search by destination

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

Buttons: + Destinations

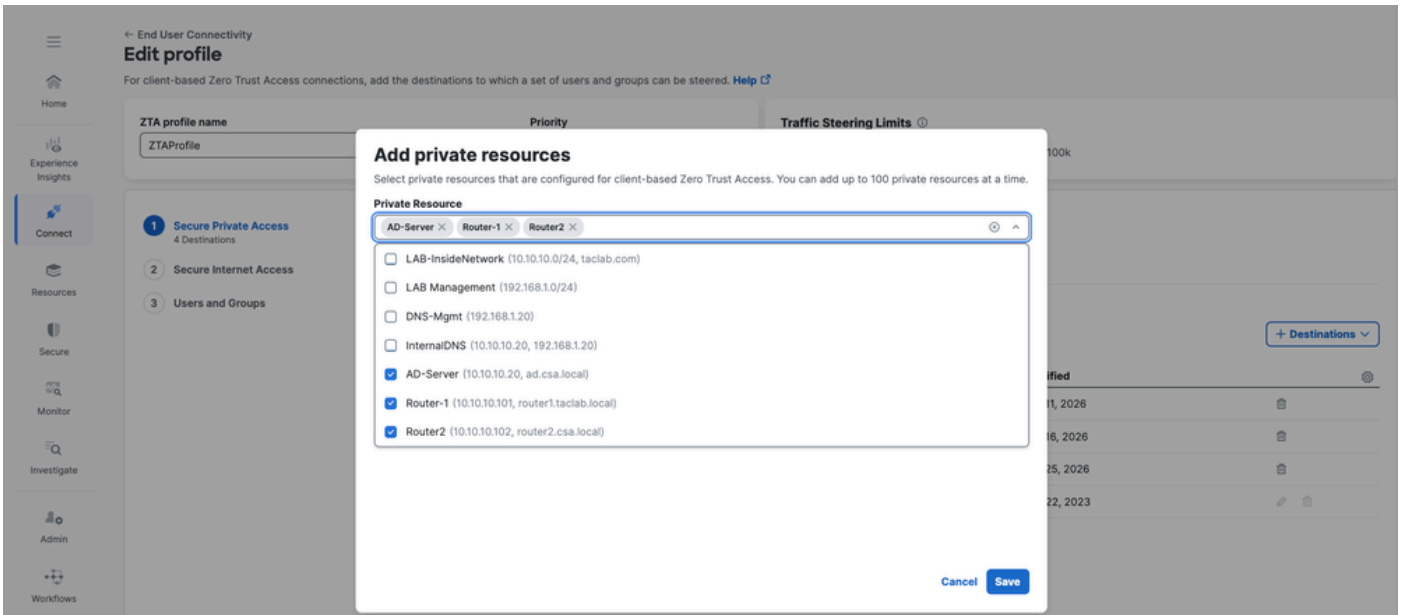
Private Resource

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

Add Destination

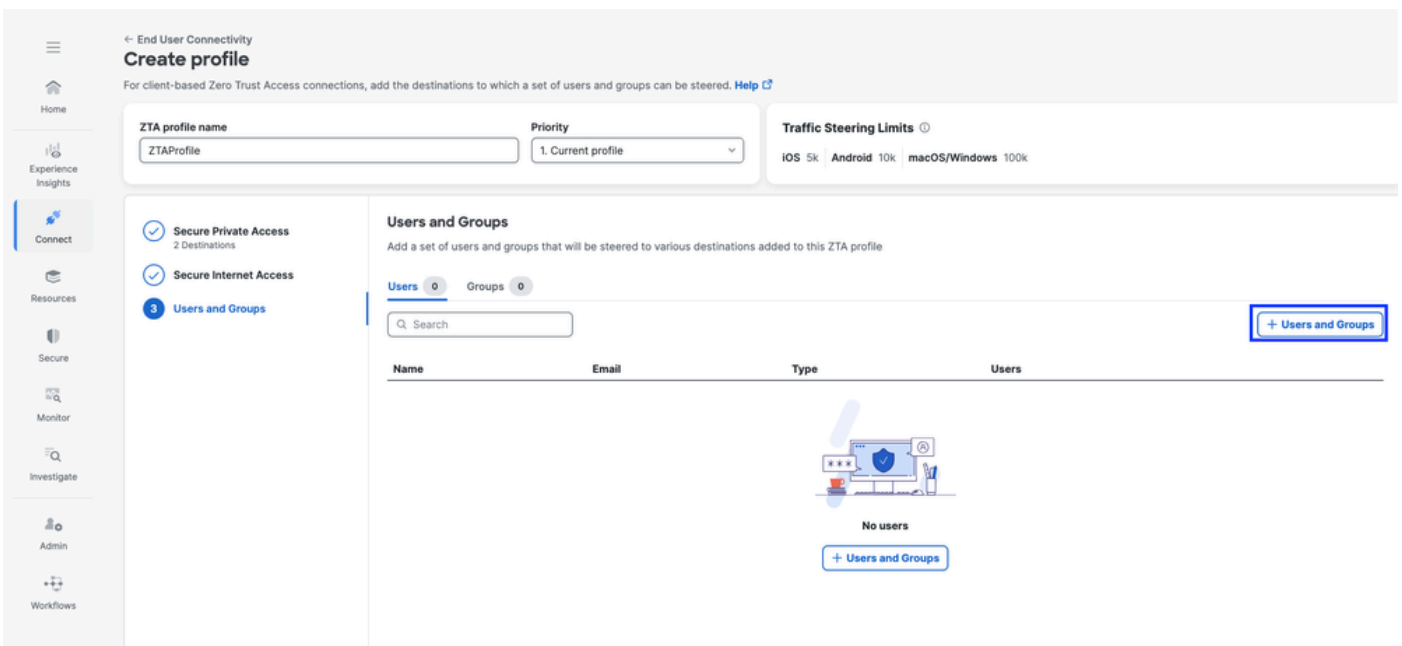
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Sicherer Zugriff - ZTA-Profil



Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen



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

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

Users and Groups

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

Users 1 | Groups 0

Q Search + Users and Groups

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

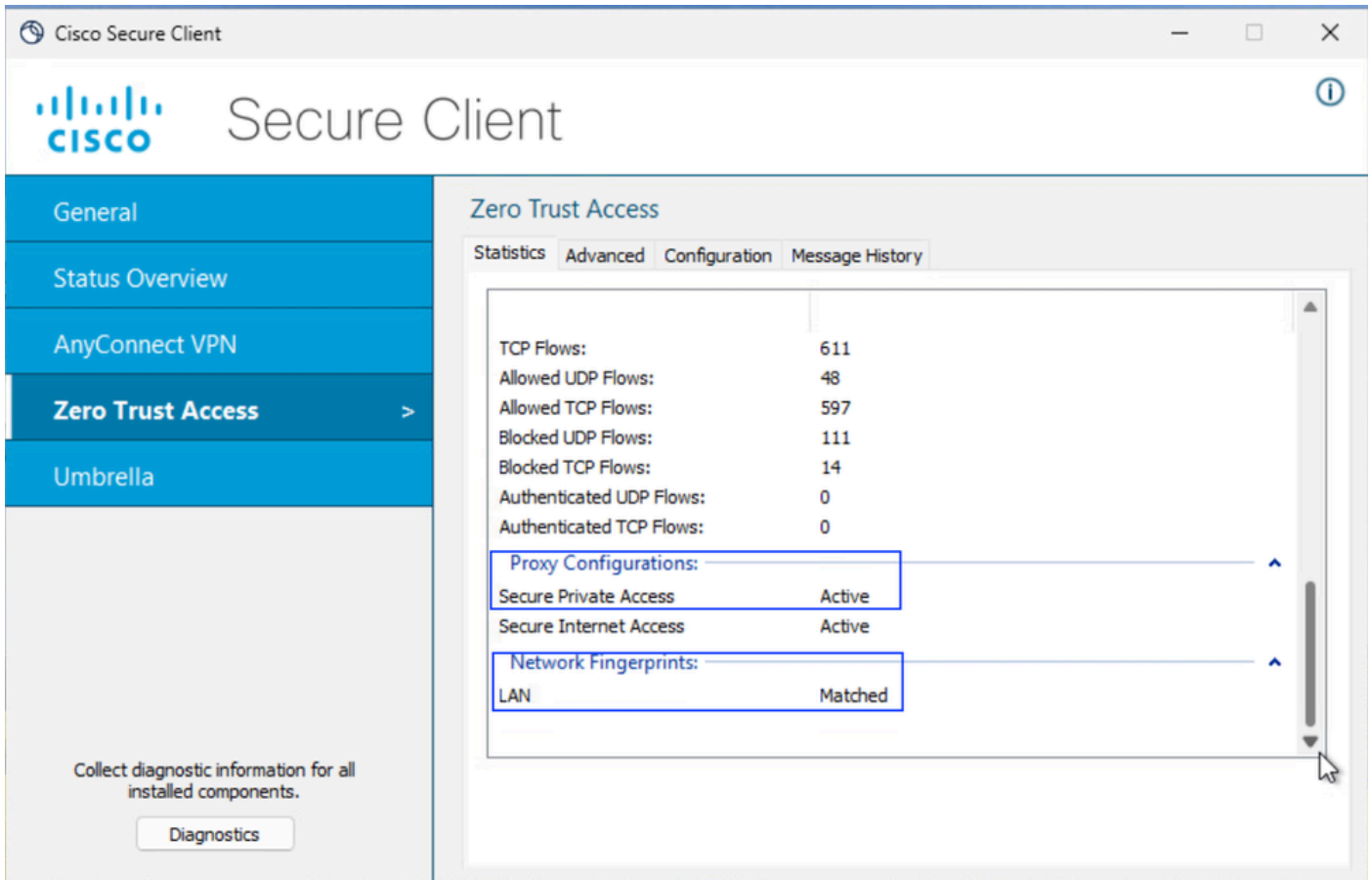
Rows per page: 10 < >

Back Close

Sicherer Zugriff - ZTA-Profil

Schritt - 6 Überprüfen des Zugriffs auf die private Ressource

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



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

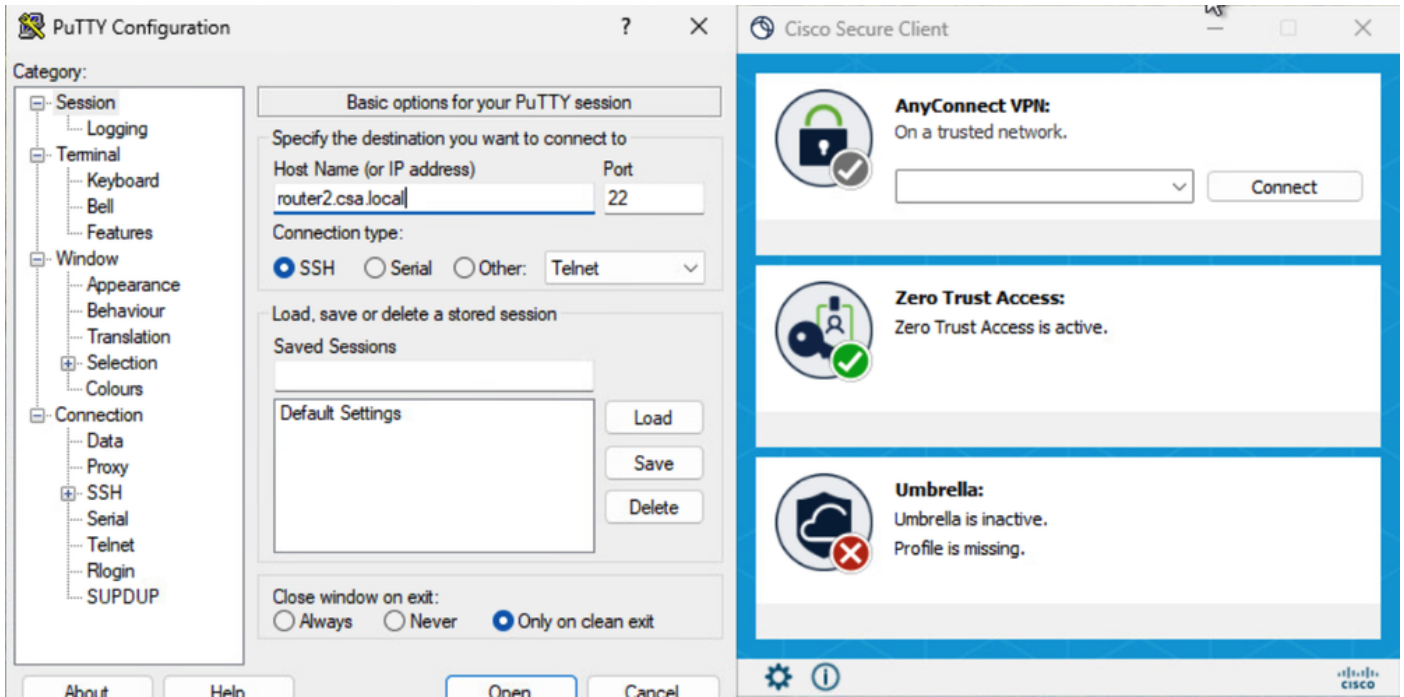
3. Überprüfen Sie, ob FTD über FQDN eine Verbindung zu einer privaten Ressource herstellen kann.

```
ftd# ping 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# █
```

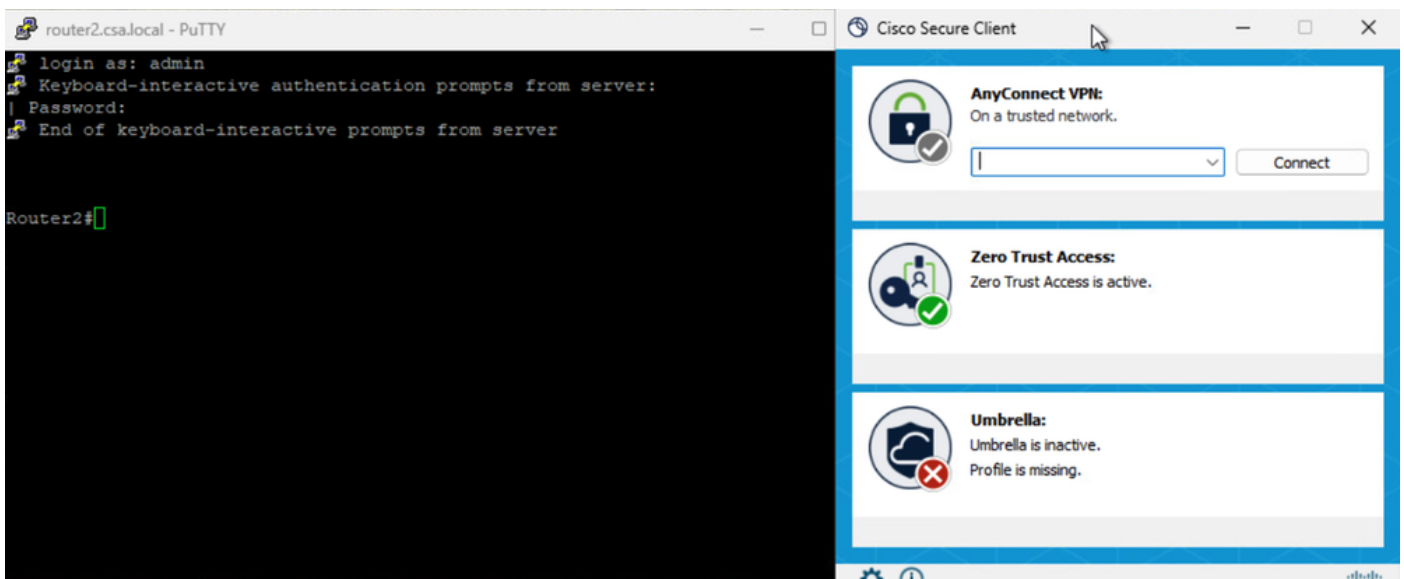
Sicherer Zugriff - PR-Tests

4. Testen der SSH-Verbindung mit der privaten Ressource

Zugriff auf den PR über FQDN

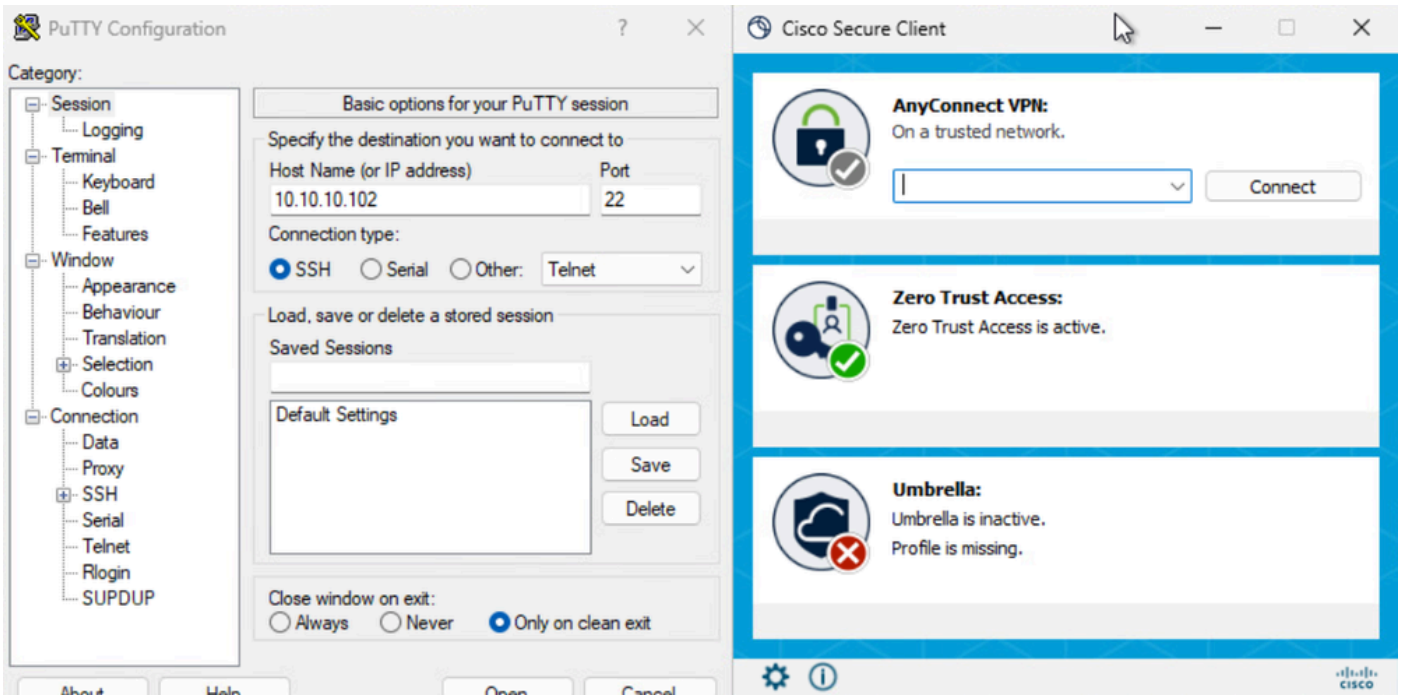


Sicherer Zugriff - PR-Tests

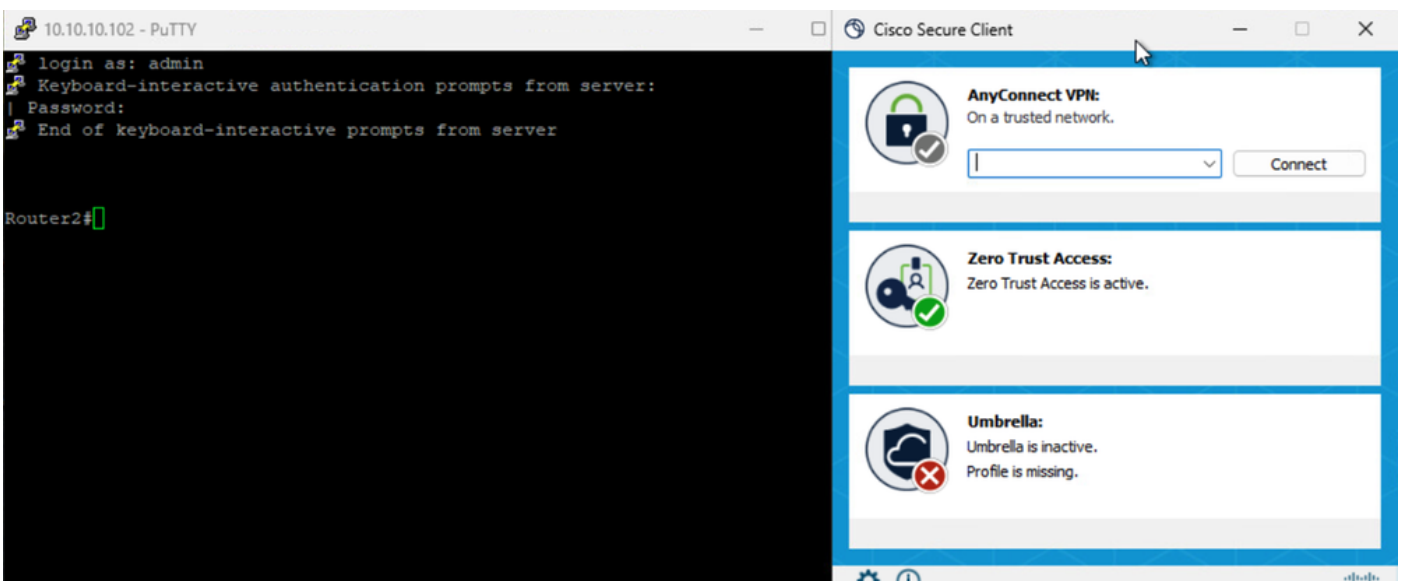


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse



Sicherer Zugriff - PR-Tests



Sicherer Zugriff - PR-Tests

5. Überprüfen der Suchprotokolle für Aktivitäten mit sicherem Zugriff

Activity Search

Activity Search interface showing search filters and results for domain router2.csa.local. The interface includes a search bar, filters for Response (Allowed, Blocked), Identity Type (AD Users, AD Groups, AD Devices, SAML Users), and Enforced By (Secure Access Cloud, FTD, Umbrella Cloud). The results table shows 8 total results for the period from Feb 22, 2026 3:28 AM to Feb 23, 2026 3:38 AM. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, OS, and Bro.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Bro
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...

Sicherer Zugriff - Aktivitätssuche

Activity Search

Activity Search interface showing search filters and results for response Allowed. The interface includes a search bar, filters for Response (Allowed, Blocked), Identity Type (AD Users, AD Groups, AD Devices, SAML Users), and Enforced By (Secure Access Cloud, FTD, Umbrella Cloud). The results table shows 17 total results for the period from Feb 22, 2026 3:33 AM to Feb 23, 2026 3:33 AM. An Event Details panel is open on the right, showing details for a blocked connection from router2.csa.local to 10.10.10.102 on port 22, blocked by the Router2-SSH-Allow rule.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/App
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.64	192.168.1.64	7680	Allowed	LAB Manager
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.23	192.168.1.23	7680	Allowed	LAB Manager

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 3:33 AM

Access details

Identity: jay (jay@csa.local)

ZTNA Client

Rule Name: Router2-SSH-Allow

Resource/Application: Router2

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: FTD > FMC_FTD

Destination: router2.csa.local

Sicherer Zugriff - Aktivitätssuche

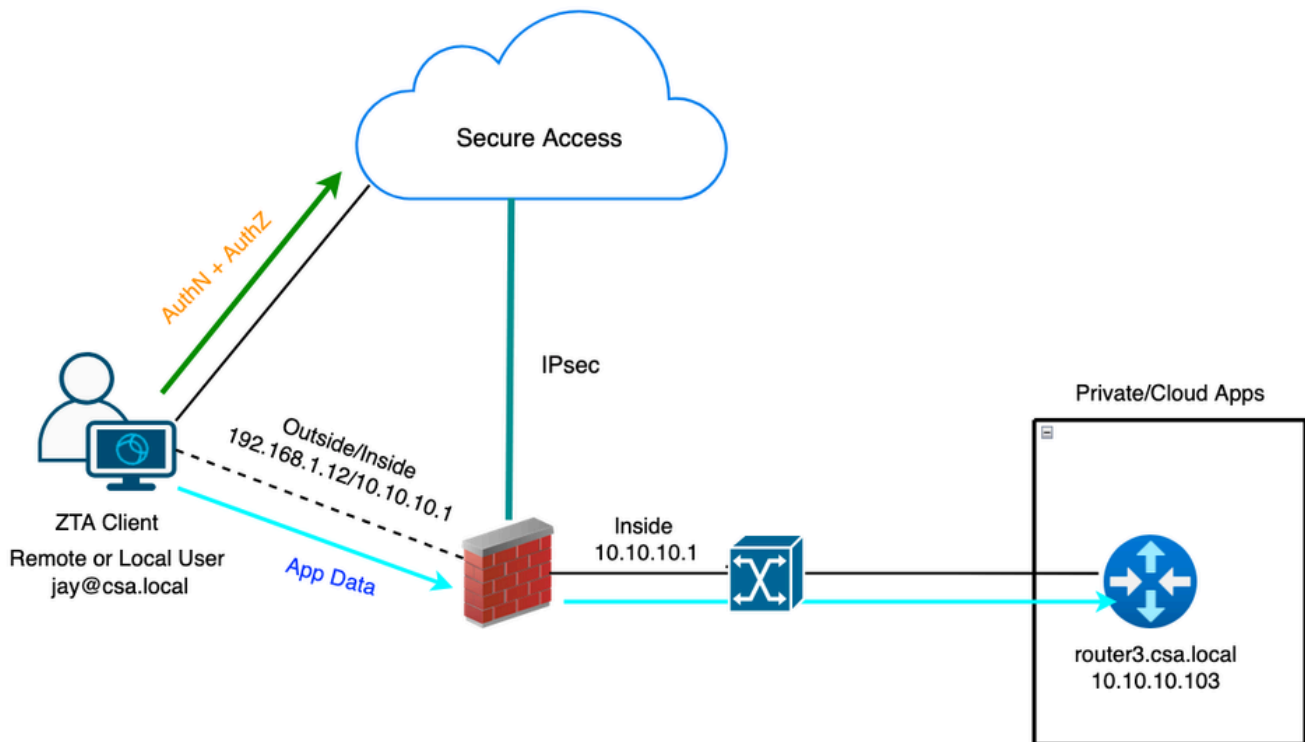
Activity Search

Activity Search interface showing search filters and results for IP address 10.10.10.102 and response Allowed. The interface includes a search bar, filters for Response (Allowed, Blocked), Identity Type (AD Users, AD Groups, AD Devices, SAML Users), and Enforced By (Secure Access Cloud, FTD, Umbrella Cloud). The results table shows 19 total results for the period from Feb 22, 2026 3:38 AM to Feb 23, 2026 3:38 AM. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, and Bro.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	Bro
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...

Sicherer Zugriff - Aktivitätssuche

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

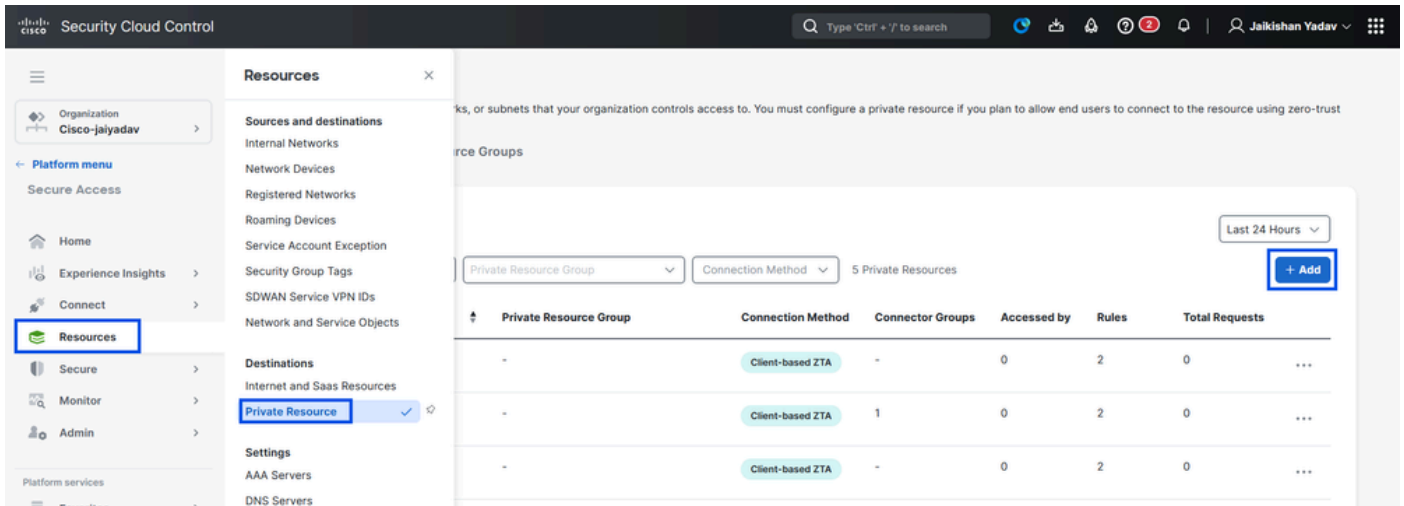


Universelle ZTA - Topologie der Testfälle

Schritt 1 - Definieren einer privaten Ressource für sicheren Zugriff

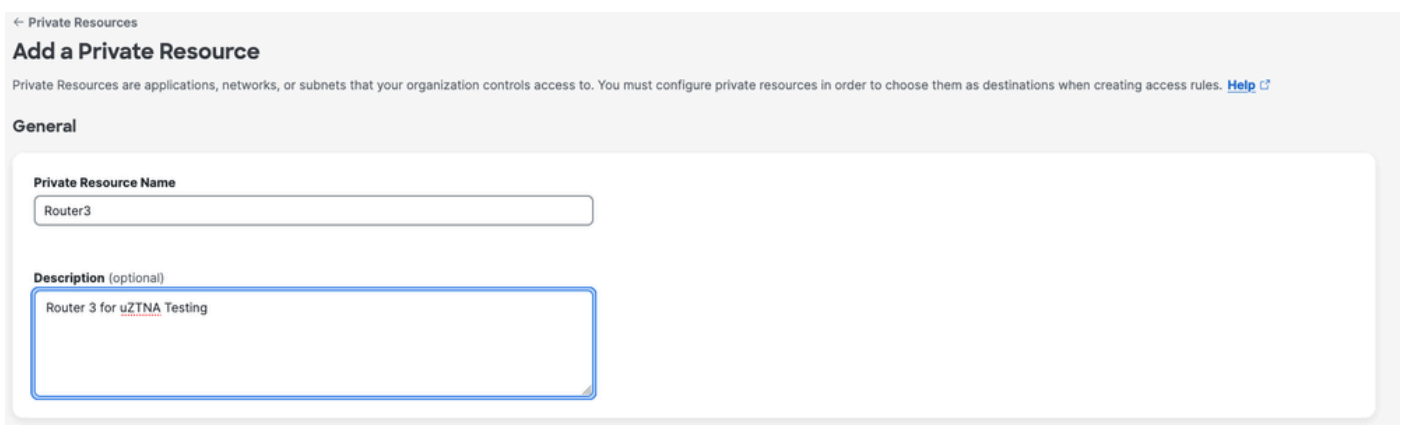
Konfigurieren einer privaten Ressource für den Zugriff über ein bei Zero Trust Access (ZTA) angemeldetes Gerät mit Cloud-Durchsetzung

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

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
<input type="text" value="router3.csa.local"/>	<input type="text" value="Any TCP"/>	<input type="text" value="22"/>	+ Protocol & Port
Remove			
<input type="text" value="192.168.1.103"/>	<input type="text" value="Any TCP"/>	<input type="text" value="22"/>	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.103"/>	<input type="text" value="Any TCP"/>	<input type="text" value="22"/>	+ Protocol & Port
Remove + IP Address/FQDN			

Use internal DNS server to resolve the domain

LabDNS (192.168.1.20, 10.10.10.20) ▼

Sicherer Zugriff - Konfiguration privater Ressourcen

5. Endpunktverbindungsmethoden auswählen

6. Wählen Sie FTD als lokale Durchsetzungspunkte

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

FMC_F... x Search by FTD na... ^
FMC_FTD (ftd.csa.local) ✓
Will get enforced at the selected firewalls.

Local-only

Enforcement point for Remote User



Enforcement point for Local user



Cancel

Save and Test Save

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.

Resource Connector Groups

Secure Access can forward Zero Trust Access traffic to this private resource using resource connectors. [Help](#)

For more information, see [Help](#)

Resource Connector Groups (optional) [Help](#)

RC-ESXI X e.g. My Server Group

Choose a connector group in the same data center, branch office, or security zone as the resource. [Help](#)

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

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar is expanded to 'Secure', and the 'Access Policy' is selected. The main content area displays a table of rules. The table has columns for Access, Action, Sources, Destinations, Security, Hits, and Status. Three rules are visible:

Access	Action	Sources	Destinations	Security	Hits	Status
low	Private	Allow	Any AD Users	AD-Server	92	On
	Private	Allow	Any AD Users	ESXI	-	On
S-Allow	Private	Allow	Any AD Users	InternalDNS	-	On

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.

Access Policy

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

Search by rule name Intent Objects Settings Add Rule ^

	#	Rule name	Access	Action	Sources	Destinations	Security			
<input type="checkbox"/>	1	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server				
<input type="checkbox"/>	2	Router1-SSH	Private	Allow	Any AD Users	Router-1				
<input type="checkbox"/>	3	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2		20		
<input type="checkbox"/>	4	Cursor	Internet	Allow	jay (jay@csa...)	Cursor-test		587		
<input type="checkbox"/>	5	AI Block	Internet	Block	jay (jay@csa...)	Generative A...		5		
<input type="checkbox"/>	6	Internet-Allow	Internet	Allow	Any	Any		153.6k		
<input type="checkbox"/>	7	RAVPN-Allow	Internet	Allow	Any AD Users	Any		761		

Rows per page 1-7 of 7 < >

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

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

3. Hinzufügen eines Regelnamens

Add Router3-SSH-Allow

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

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

Summary

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

Rule name Rule order

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

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

Rule name 📄 Rule order

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From
Specify one or more sources

To
Specify one or more destinations

+ AND

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

5. Konfigurieren der Endpunktanforderungen

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

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

Private Resources: **Router3**

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

User Authentication Requirements

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

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

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

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

6. Sicherheit konfigurieren

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

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

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

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

Security Profile [Rule Defaults](#)

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

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

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

Sicherer Zugriff - Konfiguration der Zugriffsrichtlinie

7. Klicken Sie auf Speichern

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

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

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

8 Rules [Customize view](#)

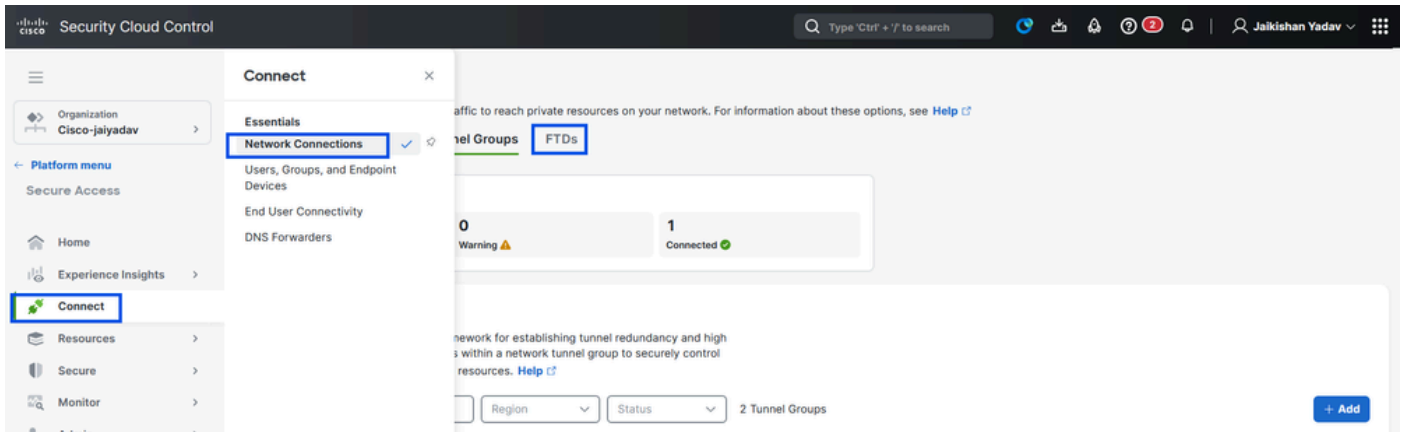
<input type="checkbox"/>	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	<input type="checkbox"/>
<input type="checkbox"/>	1	Router3-SSH-Allow	Private	Allow	Any AD Users	Router3	🛡️🌐	-	🟢	⋮
<input type="checkbox"/>	2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	🛡️🌐	-	🟢	⋮
<input type="checkbox"/>	3	Router1-SSH	Private	Allow	Any AD Users	Router-1	🛡️🌐	-	🟢	⋮
<input type="checkbox"/>	4	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2	🛡️🌐	20	🟢	⋮
<input type="checkbox"/>	5	Cursor	Internet	Allow	jay (jay@c...)	Cursor-test	🛡️🌐🔒	587	🟢	⋮
<input type="checkbox"/>	6	AI Block	Internet	Block	jay (jay@c...)	Generative A...	🌐	5	🟢	⋮
<input type="checkbox"/>	7	Internet-Allow	Internet	Allow	Any	Any	🌐🔒	154.8k	🟢	⋮
<input type="checkbox"/>	8	RAVPN-Allow	Internet	Allow	Any AD Users	Any	🛡️🌐🔒	761	🟢	⋮

Rows per page 100 1-8 of 8 < 1 >

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

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

Connector Groups Network Tunnel Groups **FTDs**

1 Syncing 0 Synced

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

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

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

UZTA Configuration status
 Syncing Last synced at 23 Feb 2026, at 5:02 AM UTC

Assigned Trusted Network
 Trusted network: LAN (Default trusted network)
 Networks: 1 DNS Domains, 1 DNS Servers
[Edit assignment](#) [+ Trusted network](#)

Associated Resources
 3

RESOURCES ASSOCIATED BY STATUS
 Status: Synced (3)
[View resources associated to this FTD](#)
[Associate Resources](#)

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

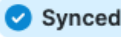
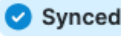
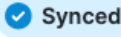
Name: ftd.csa.local
Addresses: 192.168.1.12
```

Sicherer Zugriff - PR-Verifizierung

Resources associated with FMC_FTD

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

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

Resource name	Status
Router-1	 Synced
Router2	 Synced
Router3	 Synced

[Close](#)

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.

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources (3)

RESOURCES ASSOCIATED BY STATUS

Status: **Synced** (3)

View resources associated to this FTD

Associate Resources

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.

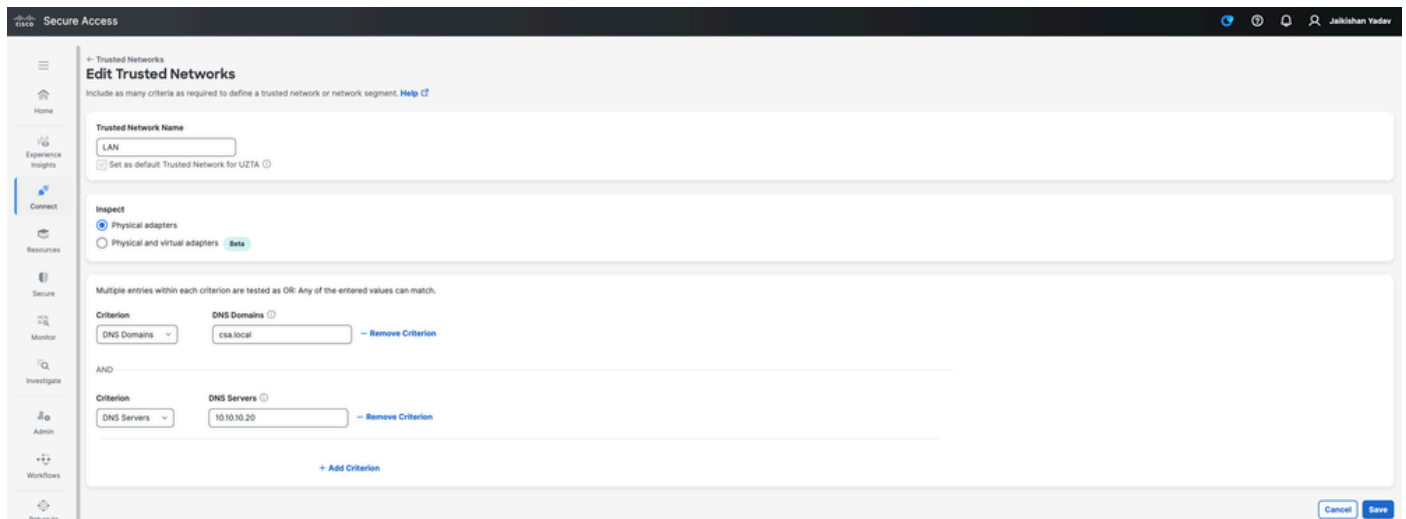
show running-config object application

```
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"

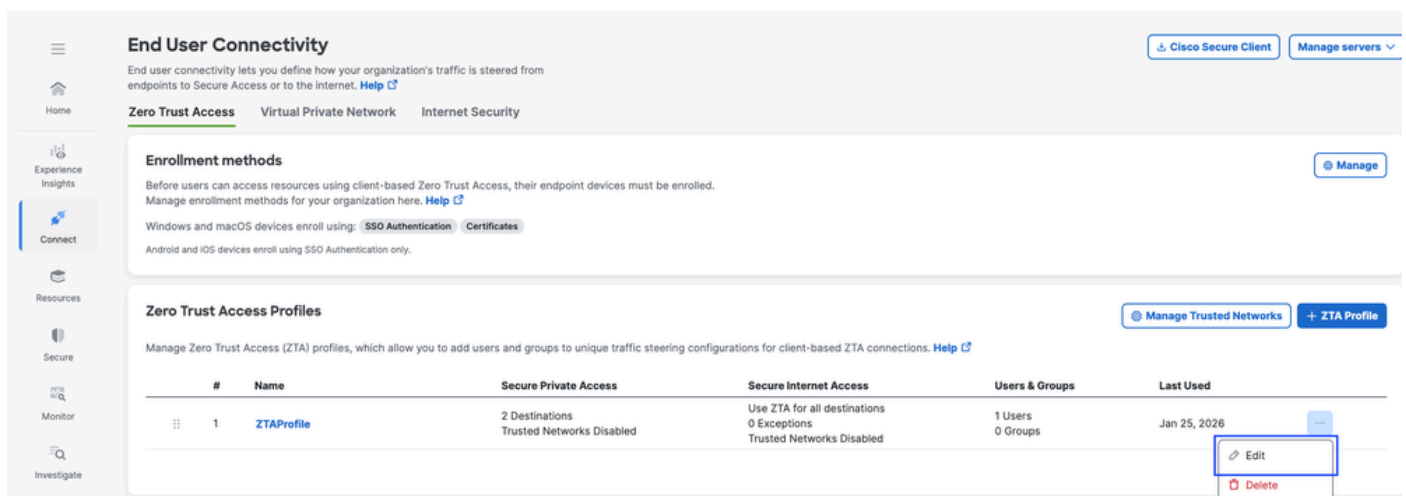
Navigieren Sie zu Verbinden > Endbenutzerverbindungen > Zugriff ohne Vertrauensstellung > ZTA-Einstellungen, und konfigurieren Sie vertrauenswürdige Netzwerke.



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

The screenshot shows the 'Create profile' page for End User Connectivity. The page is titled 'Create profile' and includes a sub-header 'Secure Private Access'. The main content area is divided into three steps: 1. Secure Private Access (0 Destinations), 2. Secure Internet Access, and 3. Users and Groups. The 'Secure Private Access' section is active, showing a search bar and a table of destinations and private resources. The table has columns for 'Destinations & Private Resources', 'Destinations', and 'Modified'. A single entry is visible: '*zpc.sse.cisco.test' with 1 destination and a modification date of Feb 22, 2023. A tooltip is visible over the table, defining 'Private Resource' as resources configured for client-based Zero Trust Access and 'Add Destination' as destinations that can be accessed during Zero Trust Access.

Sicherer Zugriff - ZTA-Profil

The screenshot shows the 'Edit profile' page for End User Connectivity. The page is titled 'Edit profile' and includes a sub-header 'Secure Private Access'. The main content area is divided into three steps: 1. Secure Private Access (5 Destinations), 2. Secure Internet Access, and 3. Users and Groups. The 'Secure Private Access' section is active, showing a search bar and a table of destinations and private resources. A modal window titled 'Add private resources' is open, showing a list of private resources to be added to the profile. The modal window has a search bar and a list of resources with checkboxes. The resources are: LAB-InsideNetwork (10.10.10.0/24, taclab.com), InternalDNS (10.10.10.20, 192.168.1.20), AD-Server (10.10.10.20, ad.csa.local), LAB Management (192.168.1.0/24), DNS-Mgmt (192.168.1.20/32), Router2 (10.10.10.102, router2.csa.local), Router-1 (10.10.10.101, router1.csa.local), and Router3 (10.10.10.103, 192.168.1.103, router3.csa.local). The 'AD-Server', 'DNS-Mgmt', 'Router-1', and 'Router3' resources are selected. The modal window also has 'Cancel' and 'Save' buttons.

Sicherer Zugriff - ZTA-Profil

3. Hinzufügen von Benutzern und Gruppen

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


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

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

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

Users 0 | Groups 0

Q Search + Users and Groups

Name	Email	Type	Users
 No users + Users and Groups			

Sicherer Zugriff - ZTA-Profil

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

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

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

Users 1 | Groups 0

Q Search + Users and Groups

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

Rows per page: 10 < >

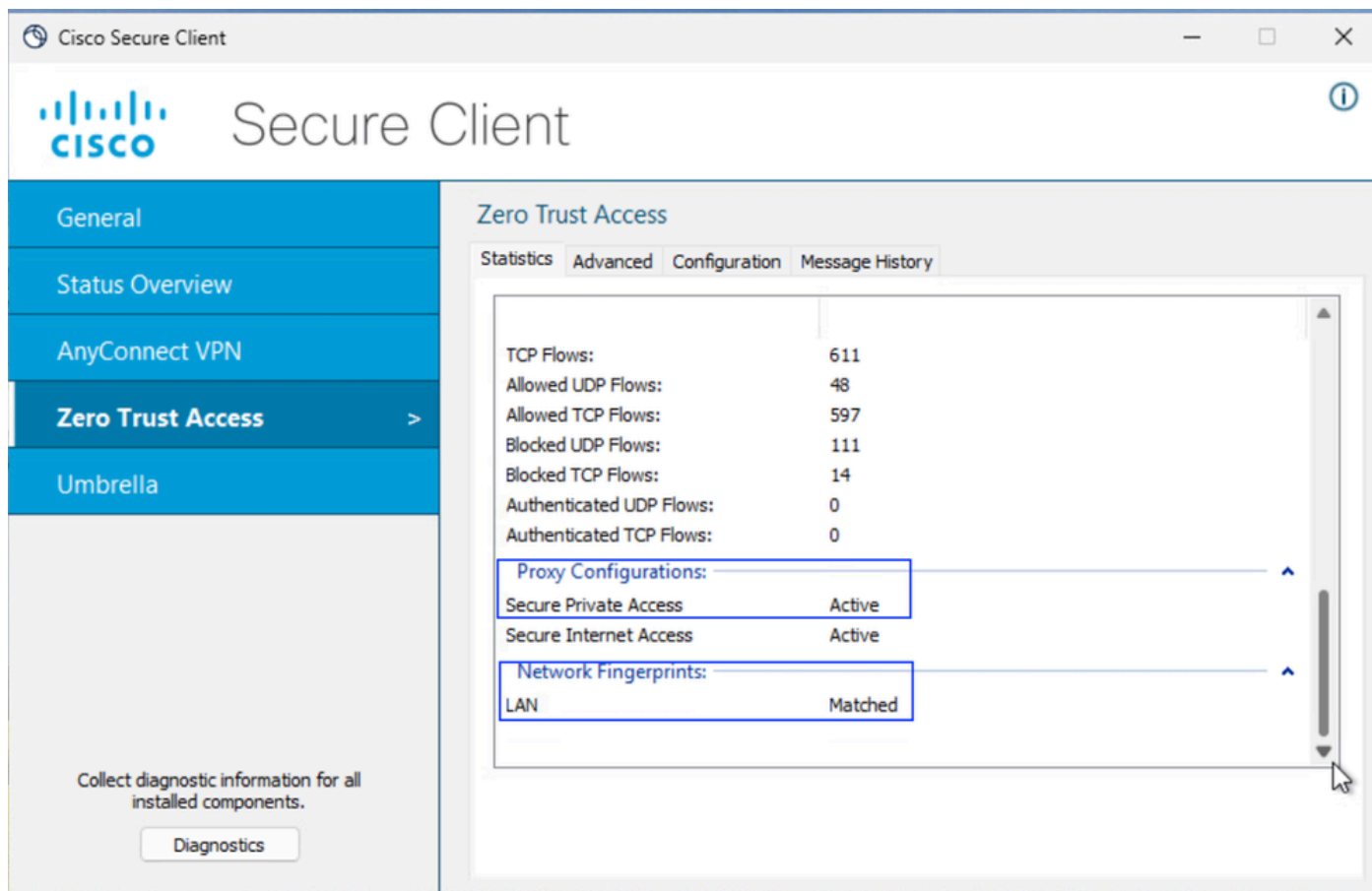
Back Close

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

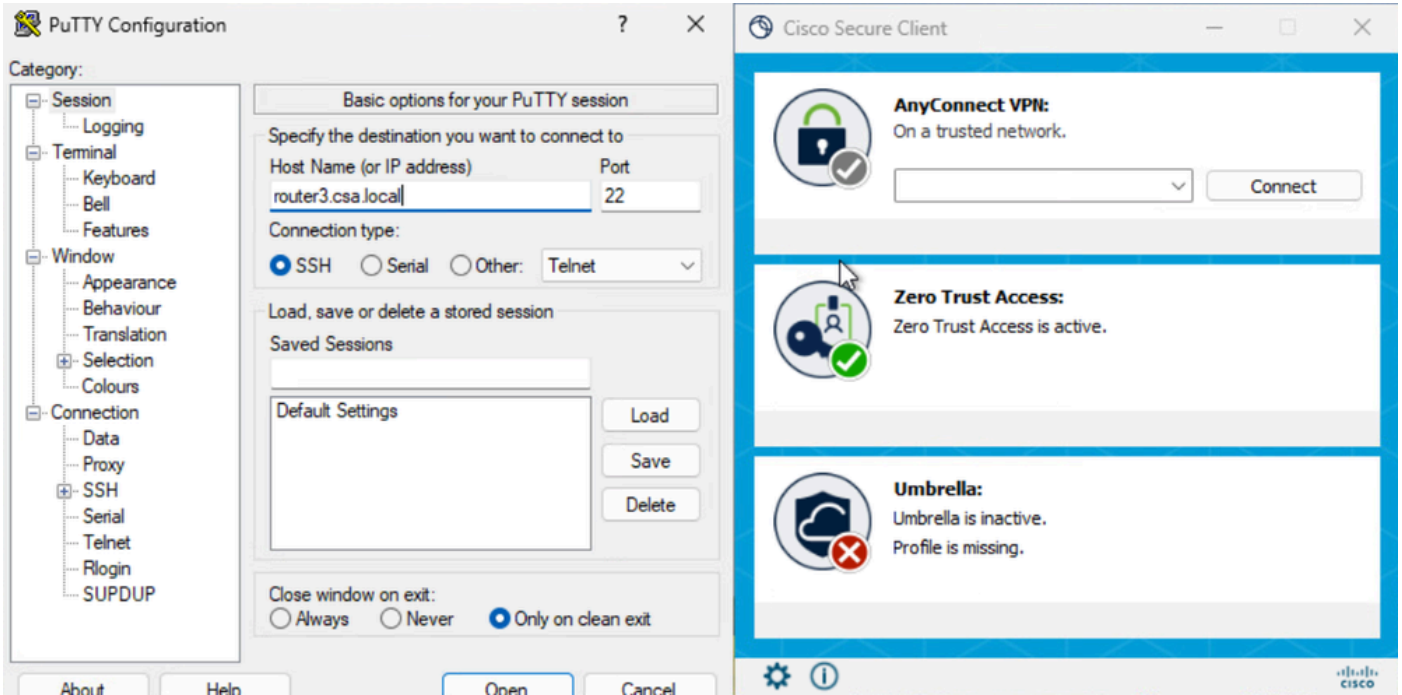
3. Überprüfen Sie, ob FTD über FQDN eine Verbindung zu einer privaten Ressource herstellen kann.

```
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# █
```

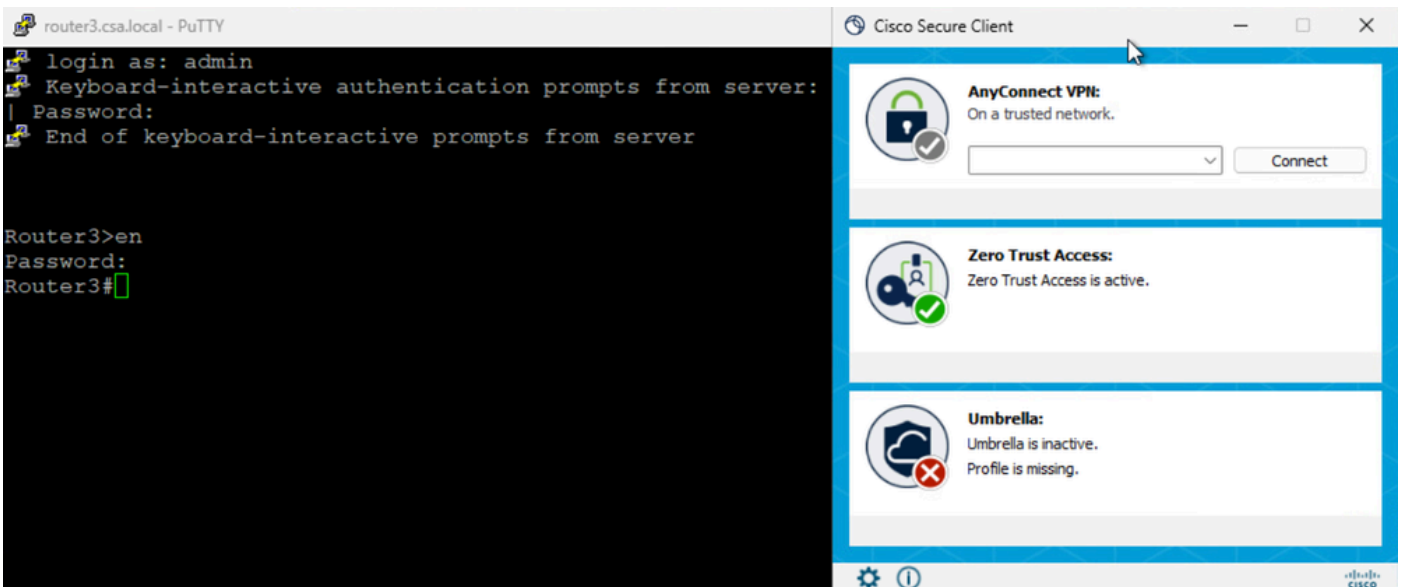
Sicherer Zugriff - PR-Tests

4. Testen der SSH-Verbindung mit der privaten Ressource

Zugriff auf den PR über FQDN

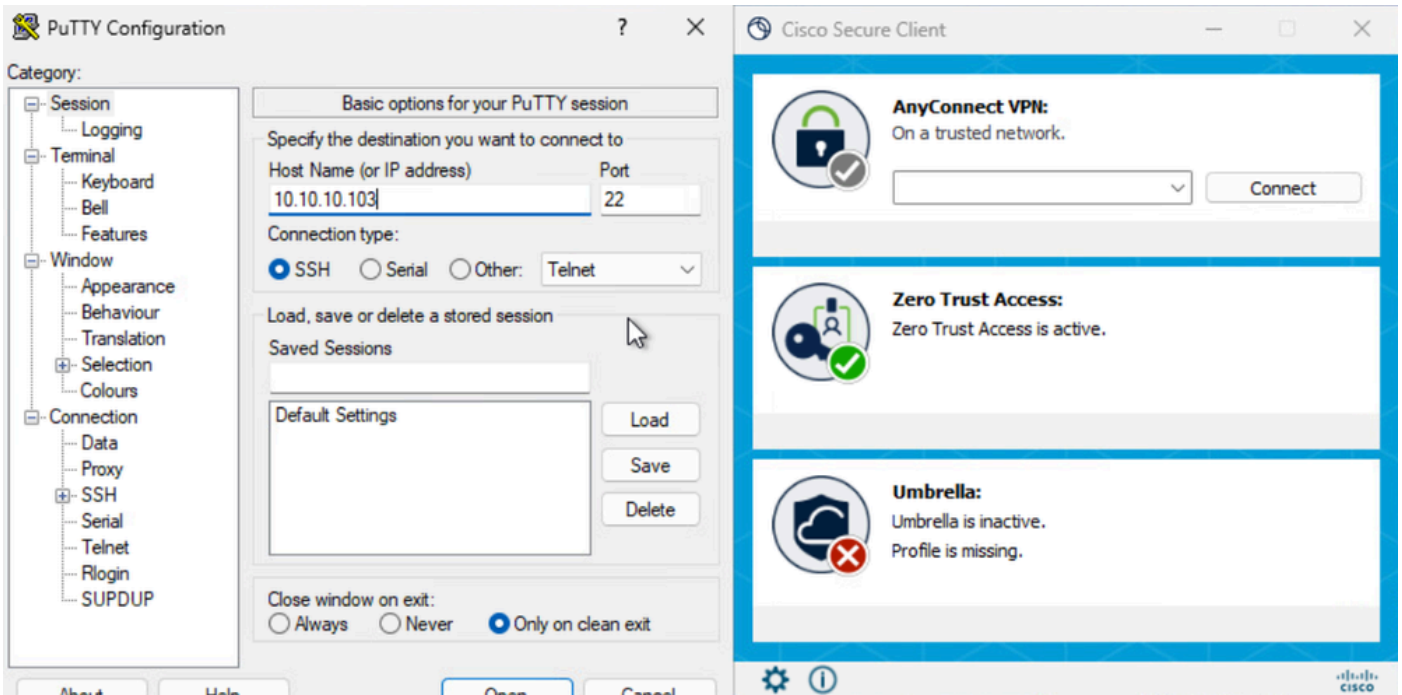


Sicherer Zugriff - PR-Tests

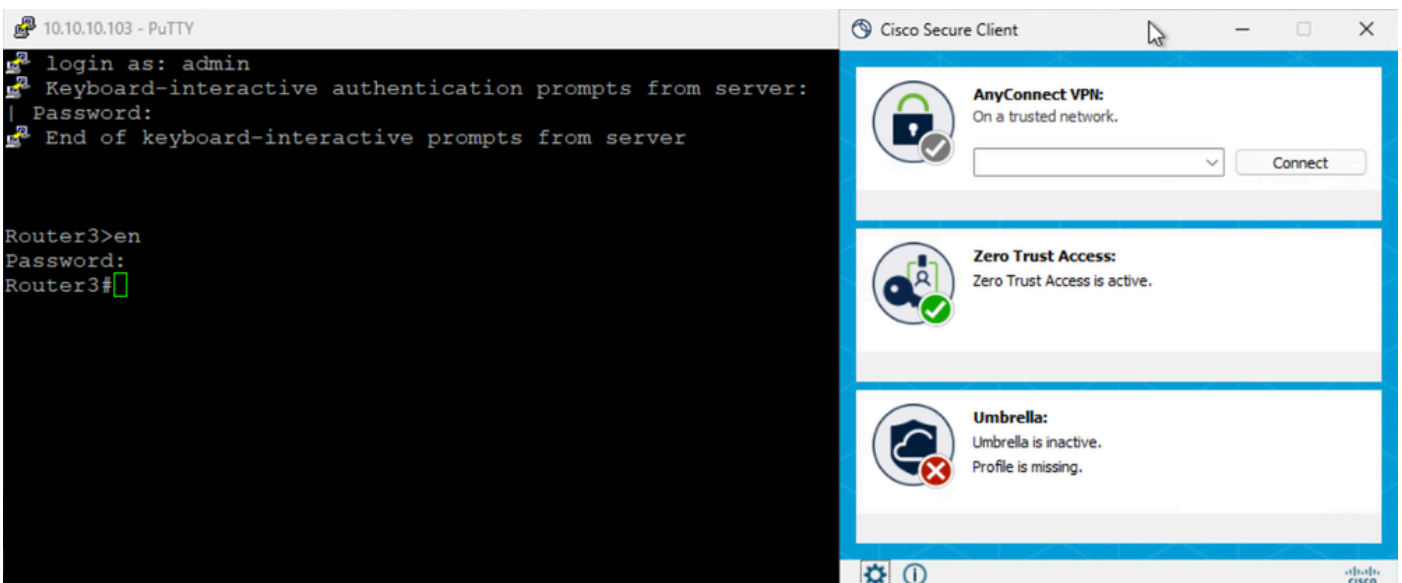


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse



Sicherer Zugriff - PR-Tests



Sicherer Zugriff - PR-Tests

5. Überprüfen der Suchprotokolle für Aktivitäten mit sicherem Zugriff

Activity Search

Search by domain, identity, or URL

Filters: **DOMAIN** router3.csa.local

4 Total | Viewing activity from Feb 22, 2026 6:41 AM to Feb 23, 2026 6:41 AM

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840

Sicherer Zugriff - Aktivitätssuche

Activity Search

Search by domain, identity, or URL

Filters: **RESPONSE** Allowed

26 Total | Viewing activity from Feb 22, 2026 6:41 AM to Feb 23, 2026 6:41 AM

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 6:40 AM

Access details

Identity: jay (jay@csa.local)

ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: LAN

Enforcement Point: FTD> FMC_FTD

Destination: router3.csa.local

Destination IP: 10.10.10.102

Sicherer Zugriff - Aktivitätssuche

6. Überprüfen von FMC-Verbindungsereignissen

Firewall Management Center

Events & Logs / Analysis / Unified Events

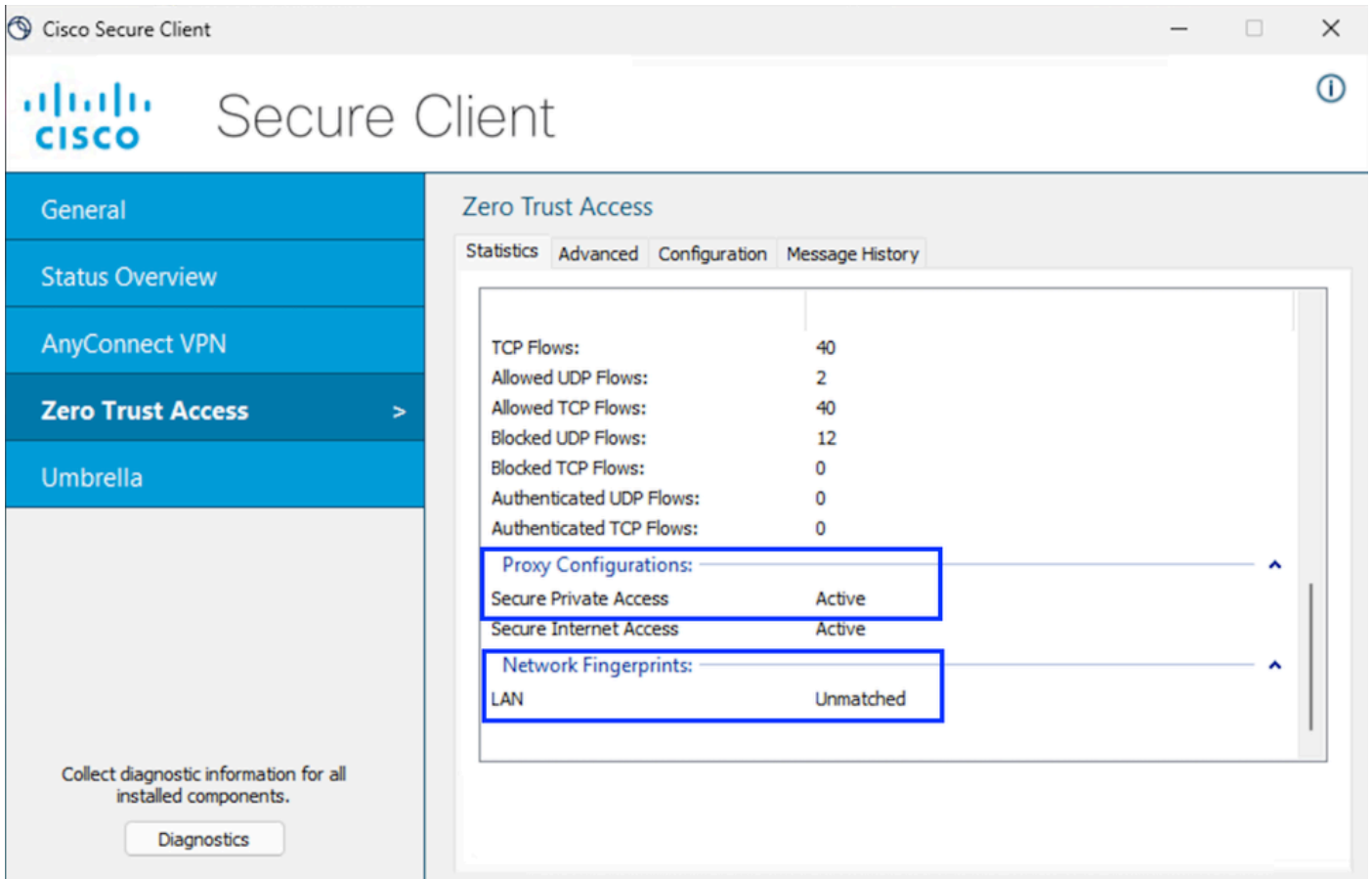
Search: [Destination IP: 10.10.10.103] 4 events

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Type	Web Application	Access Control Rule
2026-02-23 01:40:54	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.103	37877 / tcp	22 (ssh) / tcp		
2026-02-23 01:40:47	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.103	22981 / tcp	22 (ssh) / tcp		
2026-02-23 01:40:41	Connection	Allow	Zero Trust Flow	169.254.1186	10.10.10.103	57951 / tcp	22 (ssh) / tcp		
2026-02-23 01:40:33	Connection	Allow	Zero Trust Flow	169.254.1198	10.10.10.103	51673 / tcp	22 (ssh) / tcp		

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.



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 [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

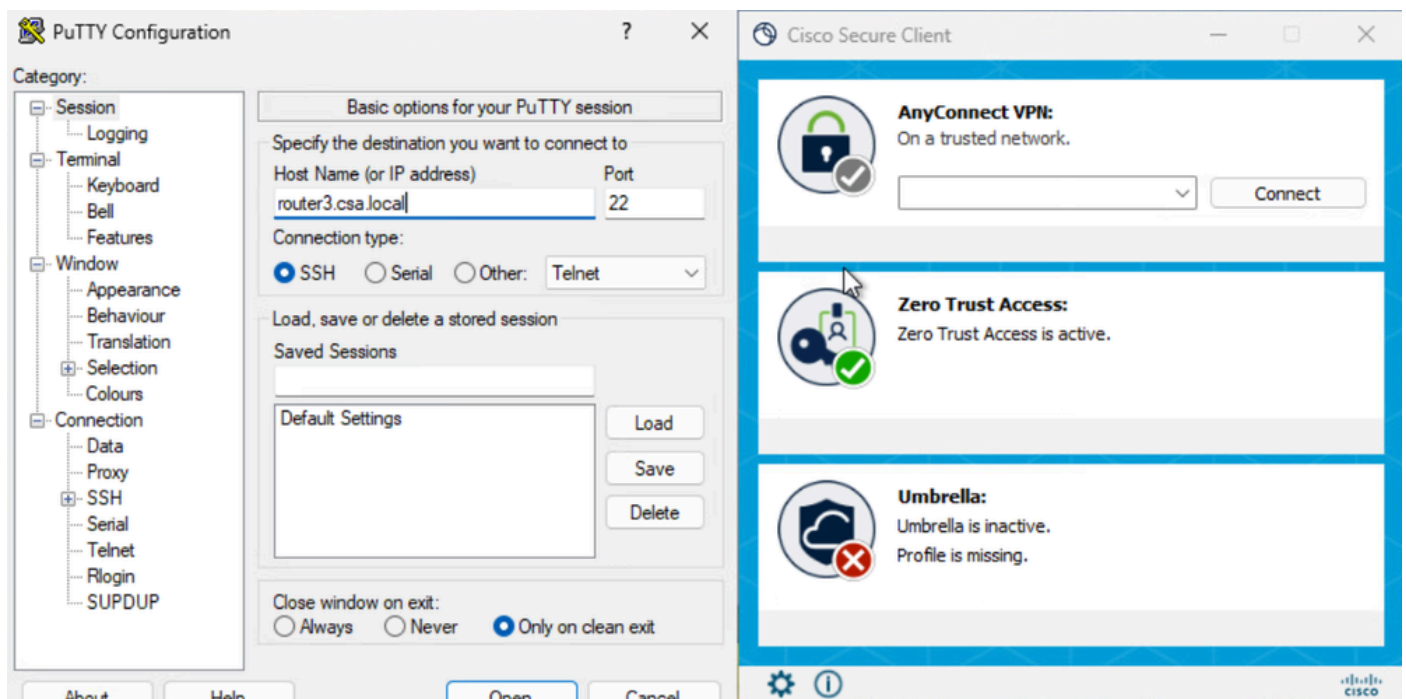
Name: ftd.csa.local
Addresses: 192.168.1.12

```

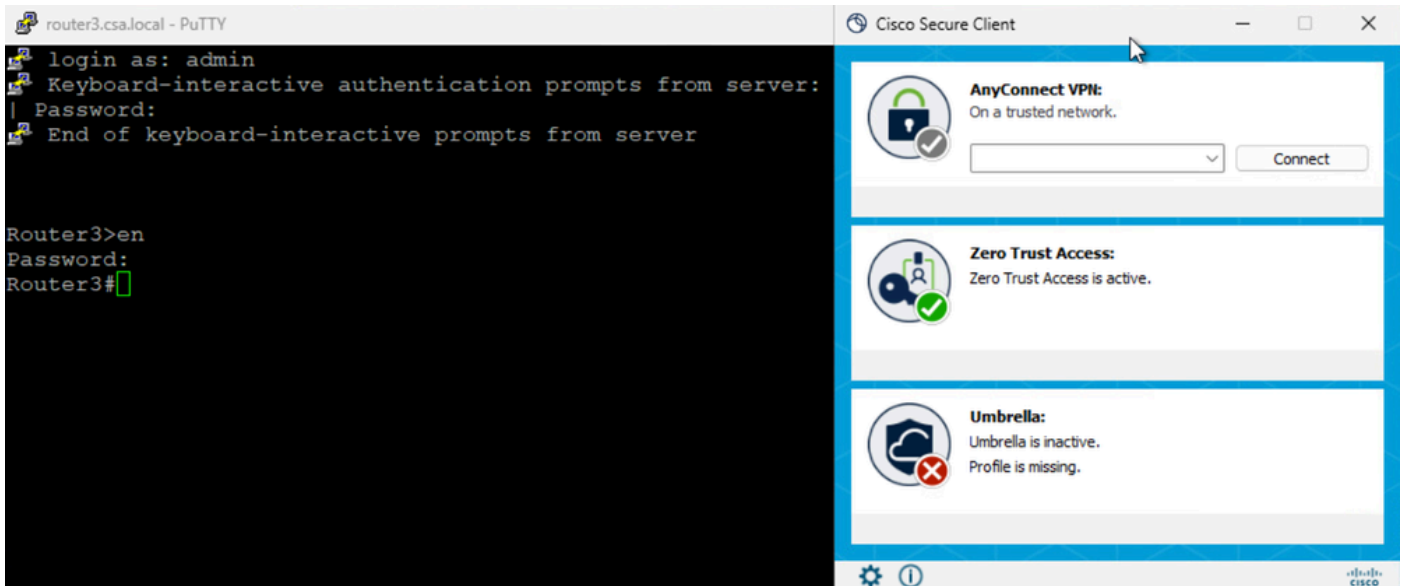
Sicherer Zugriff - PR-Tests

3. Testen der SSH-Verbindung mit der privaten Ressource

Zugriff auf den PR über FQDN

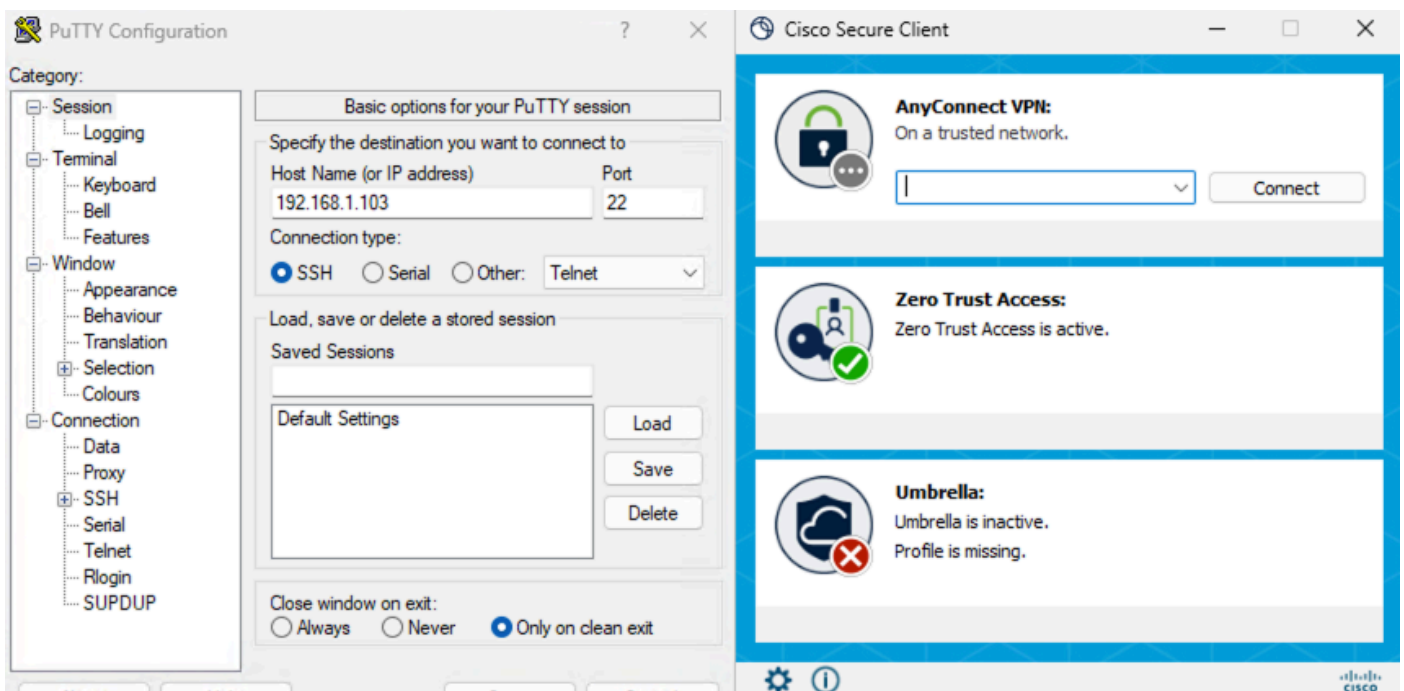


Sicherer Zugriff - PR-Tests

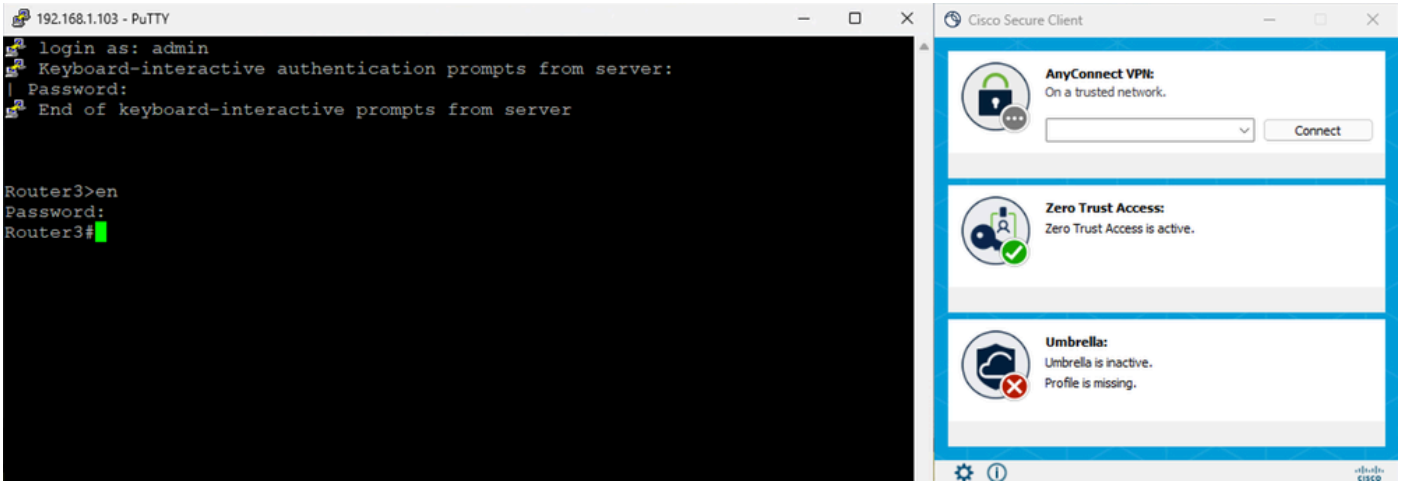


Sicherer Zugriff - PR-Tests

Zugriff auf PR über IP-Adresse



Sicherer Zugriff - PR-Tests



Sicherer Zugriff - PR-Tests

5. Überprüfen der Suchprotokolle für Aktivitäten mit sicherem Zugriff

Activity Search

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

Response: Allowed X

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

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

Sicherer Zugriff - Aktivitätssuche

Activity Search

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

Response: Allowed X

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

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

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 7:30 AM

Access details

Identity: Jay (Jay@csa.local)

ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: router3.csa.local

Destination IP: 192.168.1.103

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.