

Configurazione di Universal ZTNA per l'accesso alle risorse private su accesso sicuro

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Informazioni sullo ZTNA universale](#)

[Rilevamento rete](#)

[Tipi di applicazione](#)

[Scenari d'uso](#)

[Componenti dell'architettura](#)

[Flusso dei pacchetti](#)

[Configurazione](#)

[Esempio di rete](#)

[Test case](#)

[Test case 1: Utente remoto - Applicazione cloud](#)

[Test case 2 - Utente remoto - Applicazione locale](#)

[Test case 3 - Utente locale - Applicazione locale](#)

[Test case 4 - Utente locale e remoto - Applicazione locale o cloud con TND](#)

[Risoluzione dei problemi](#)

[Comandi utili:](#)

Introduzione

In questo documento viene descritta la configurazione dell'accesso alle risorse private tramite Universal ZTNA con percorsi di traffico diversi.

Prerequisiti

Prima di configurare Universal ZTNA, è necessario completare la configurazione seguente

- [Provider di identità su Cisco Secure Access](#)
- [Registra dispositivi in accesso con attendibilità totale tramite certificati](#)
- [Configurazione dei tunnel con Cisco Secure Firewall](#)

- [Rete privata virtuale di accesso remoto](#)
- [Connettore risorse su accesso protetto](#)
- [Caricamento FTD su Security Cloud Control](#)
- È necessario abilitare il flag della funzionalità Hybrid ZTNA per il rispettivo tenant di accesso sicuro. Contattare Cisco TAC per abilitare il flag

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione VPN IPsec su Cisco Secure Access e Firewall Threat Defense
- Provider di identità (IdP) - Provisioning utente da Active Directory
- Configurazione VPN remota su Cisco Secure Access
- Distribuzione di Resource Connector su Cisco Secure Access
- Registrazione basata su certificato ZTA
- Certificato - OpenSSL, generazione CSR, modelli di certificato, ecc.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall Threat Defense (versione 7.7.10)
- Cisco Secure Firepower Management Center (versione 7.7.10)
- Cisco Secure Client (ZTA versione 5.1.10.1720)
- Windows 11
- Windows 2019 Server - Autorità di certificazione
- Resource Connector su ESXi

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Informazioni sullo ZTNA universale

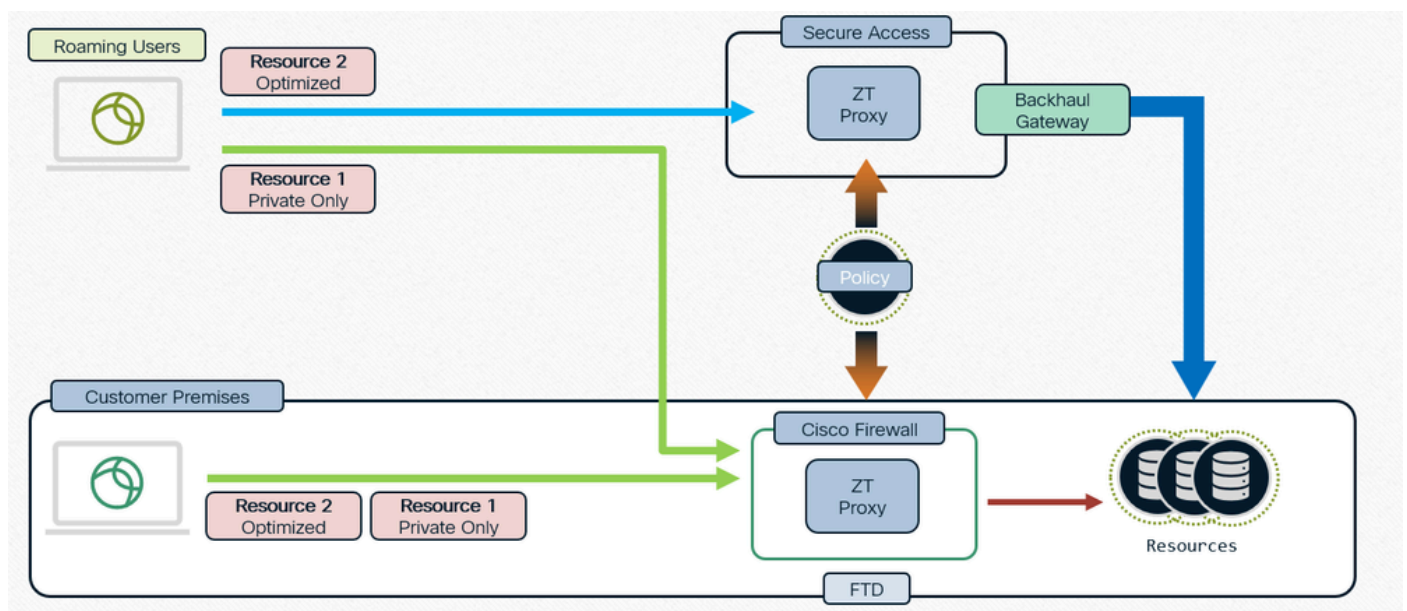
L'accesso universale alla rete senza attendibilità totale (uZTNA, Universal Zero Trust Network

Access) consente agli amministratori di consentire in modo specifico l'accesso alle risorse di rete interne in base all'identità dell'utente (compresa la fiducia e la postura dell'utente) e senza concedere l'accesso all'intera rete come con RA-VPN. uZTNA consente agli amministratori di proteggere le risorse e le applicazioni interne per gli utenti remoti e locali.

Poiché la Zutna non presuppone che l'accesso concesso a un'applicazione autorizzi implicitamente l'accesso ad altre applicazioni, la superficie di attacco della rete viene ridotta.

Secure Access valuta i criteri di accesso. Tutti i criteri di controllo di accesso distribuiti ai dispositivi da Centro gestione firewall protetto vengono ignorati.

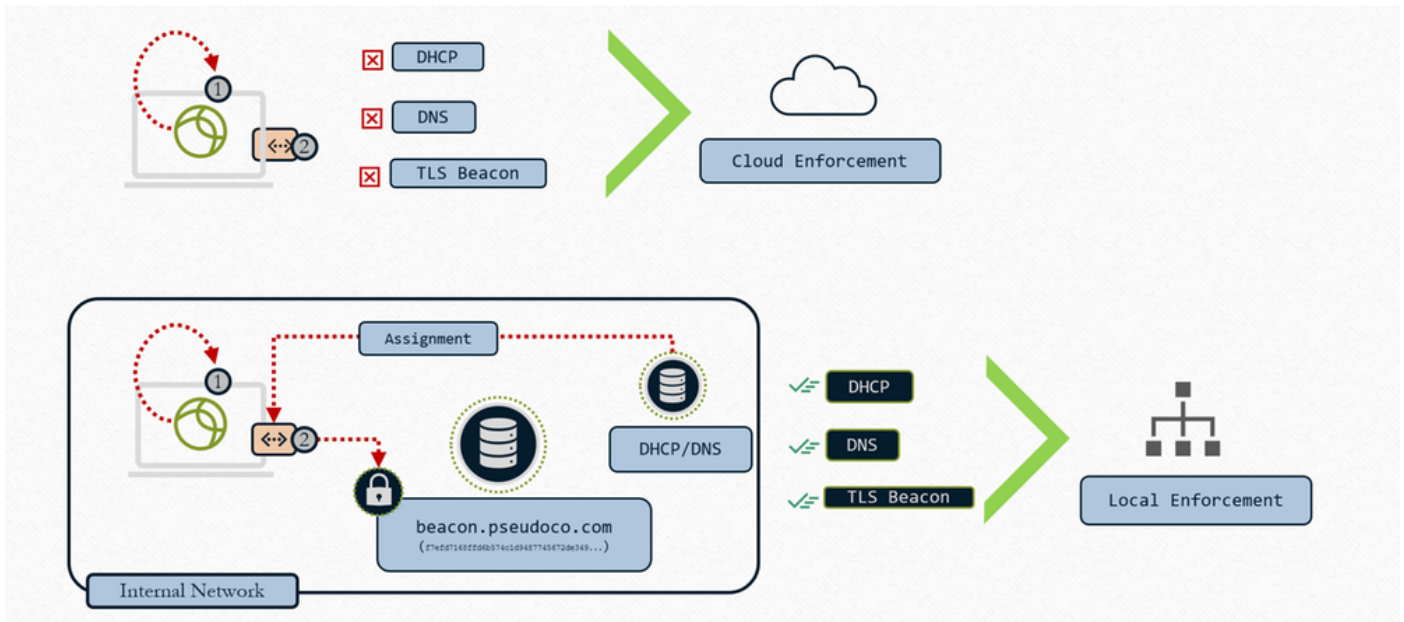
Il proxy del traffico, così come l'applicazione di IPS, file e policy antimalware, viene eseguito su Firepower Threat Defense (FTD).



Applicazione di un'unica policy distribuita

Rilevamento rete

Determinazione dell'applicazione cloud o locale



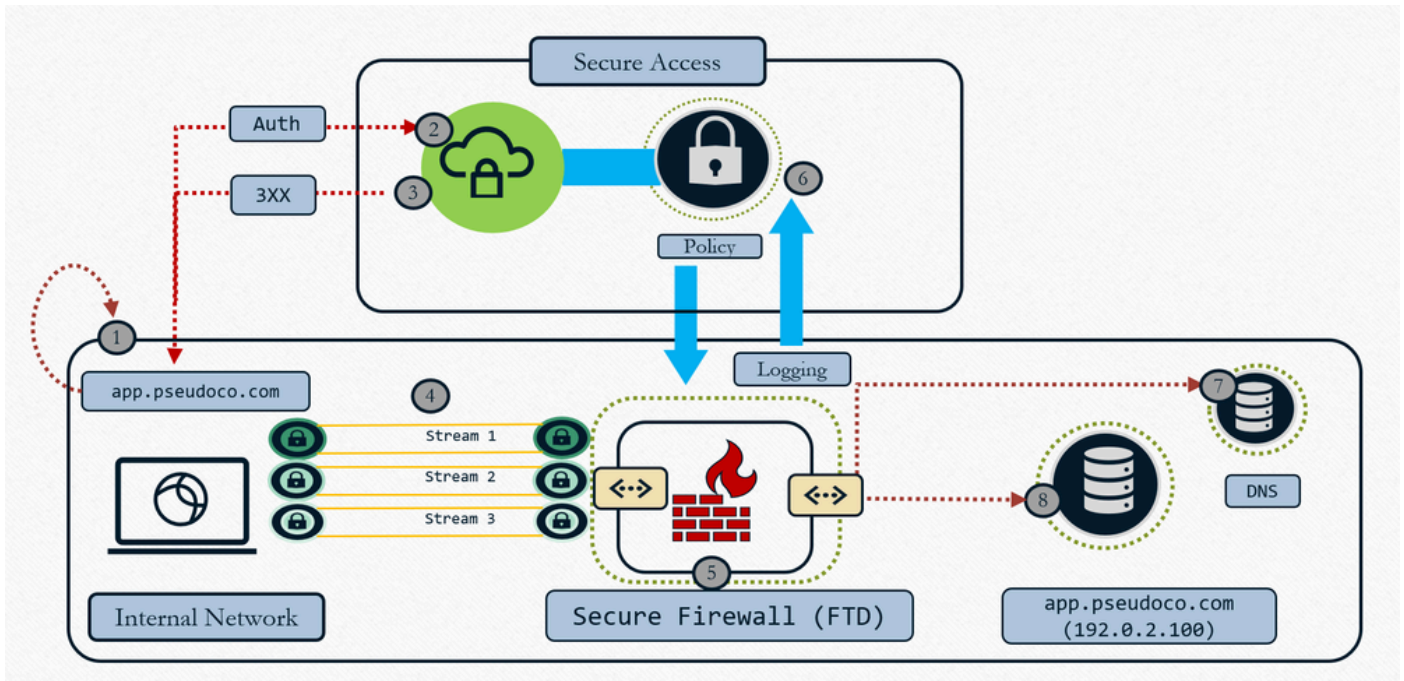
Universal ZTNA - Determinazione dell'applicazione cloud o locale

- 1- Il client interroga l'interfaccia locale per la configurazione della rete
- 2- Ricerche client per beacon TLS
- 3- Se la condizione corrisponde - Applicazione locale
- 4- Se la condizione non corrisponde - Applicazione cloud

Quando si configura la risorsa con "Applicazione cloud o locale" e si associa la regola TND con FTD , l'operazione effettivamente eseguita è l'insieme di regole di intercettazione che viene inviato al client includerà la valutazione della regola TND. Quindi, a quel client verrà detto dal cloud di valutare la regola TND. Quando inviamo la connessione, mettiamo il risultato di TND - valutazione impronta digitale di rete in intestazione HTTP in modo che dica al proxy se siamo in perm o su una rete non attendibile e poi il proxy utilizza quelle informazioni e reindirizza il traffico di conseguenza. Se l'impronta digitale corrisponde , Zproxy indica al client di reindirizzare il traffico a FTD e se l'impronta digitale non corrisponde reindirizza il traffico al cloud. Per ulteriori informazioni, fare riferimento al documento sulla [configurazione dell'accesso di rete con attendibilità totale con rilevamento reti attendibili](#)

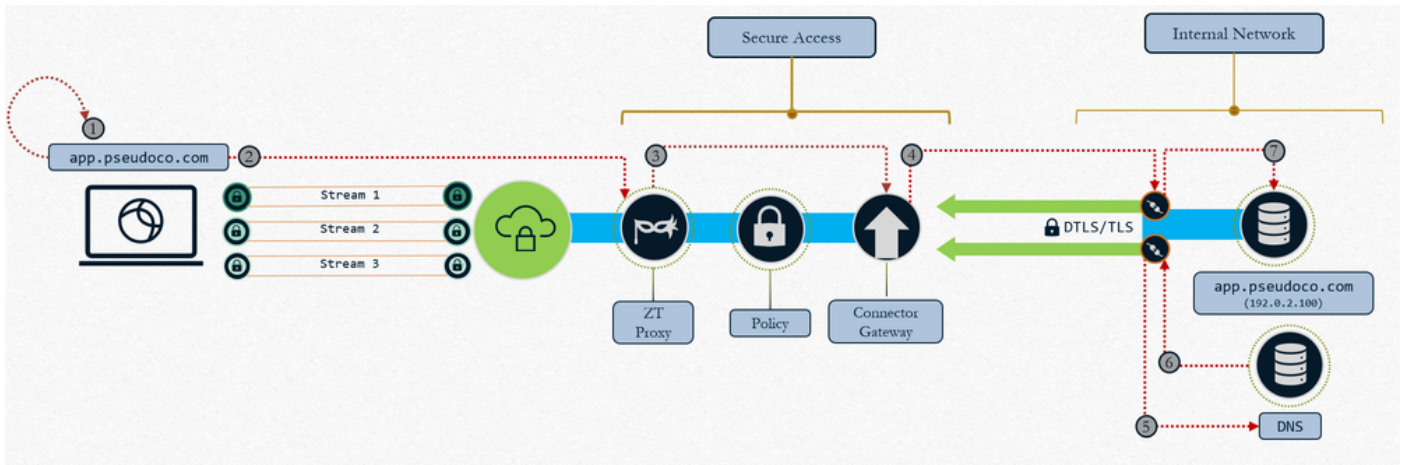
Tipi di applicazione

- Percorso di imposizione locale: Applicazione del firewall



Universal ZTNA - Applicazione locale

1. Richieste utente L'app, il client acquisisce e risolve la richiesta nell'IP temporaneo (intervallo localhost)
 2. Il traffico del controllo di autenticazione viene inviato a Secure Access Cloud per la valutazione dei criteri
 3. Il cloud restituisce il reindirizzamento a FTD per l'applicazione del piano dati (se il criterio lo consente)
 4. Traffico indirizzato all'headend configurato con firewall (interfaccia)
 5. I criteri definiti nel cloud sono imposti (IPS, malware, decrittografia) utilizzando il piano dati proxy locale
 6. Evento registrato e duplicato spedito nel cloud per la creazione di report coerenti
 7. Il firewall esegue la risoluzione DNS nella rete locale per instradare il traffico delle risorse (se consentito)
 8. Il firewall crea la connessione alla risorsa (nuova connessione basata sulla risorsa) in quanto il firewall si comporta come un proxy TCP
- Percorso imposizione cloud: OFF Network

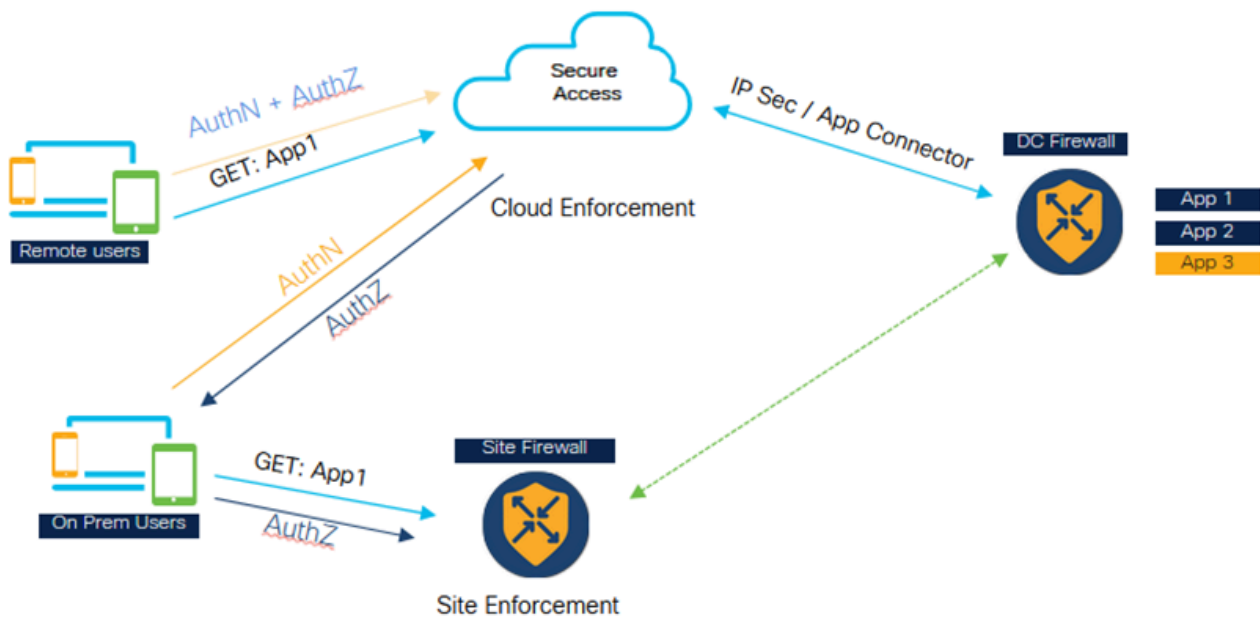


ZTNA universale : Applicazione tramite cloud

1. Richieste utente L'app, il client acquisisce e risolve la richiesta nell'IP temporaneo (intervallo localhost)
2. Il traffico viene trasportato al proxy Zero Trust in Secure Access
3. La connessione TCP viene inoltrata e costruita al connettore di risorse mappato. I criteri vengono imposti sul traffico
4. Il gateway stabilisce la connessione al connettore delle risorse
5. Il connettore di risorse risolve l'indirizzo IP della risorsa
6. Il DNS locale risponde con l'IP della risorsa
7. Connessione stabilita tra il connettore risorse e la risorsa

Scenari d'uso

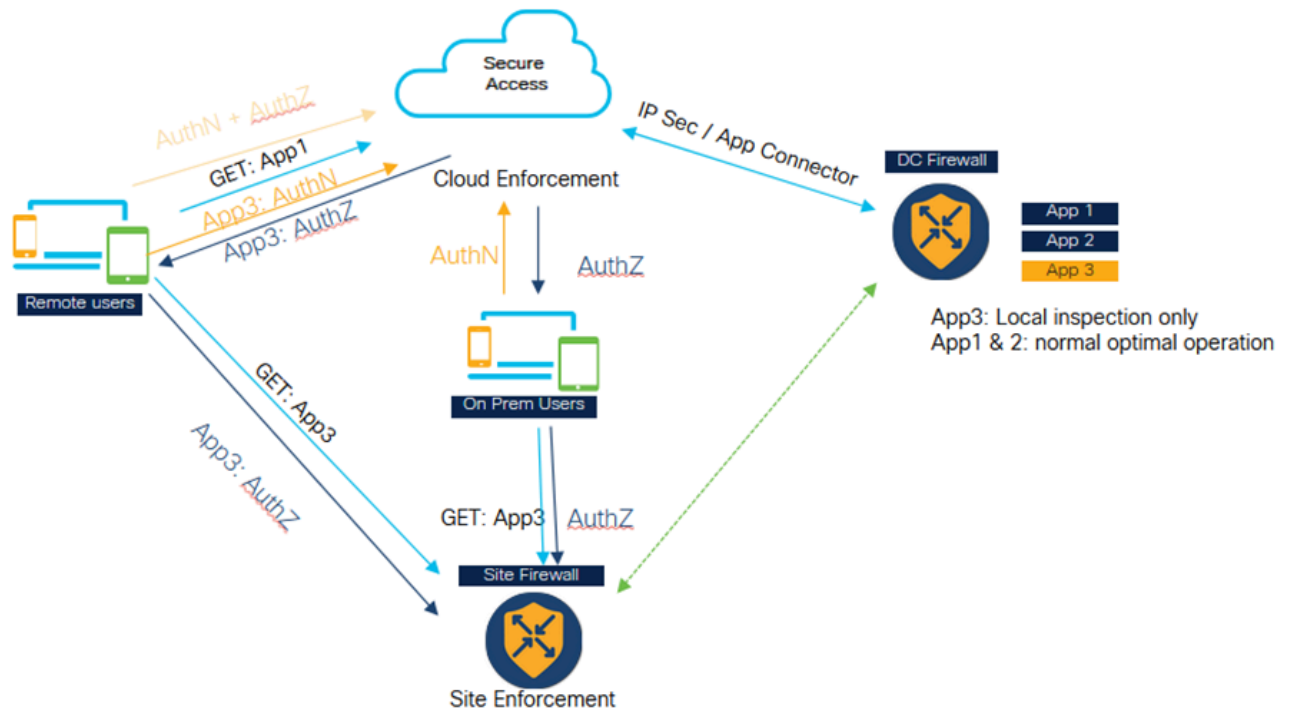
Caso 1: ZTNA coerente e ottimizzata per gli utenti in sede



ZTNA universale - ZTNA coerente e ottimizzata (utente in sede)

- Secure Access e Firewall sono entrambi configurati per proteggere l'applicazione.
- Se l'utente è remoto, accederà ad Accesso protetto per la valutazione e l'ispezione delle policy.
- Se l'utente è interno/locale, andrà al firewall per l'ispezione del traffico privato.
- L'utente locale può comunque accedere a Secure per l'autenticazione e la valutazione solo se il traffico Datapath raggiunge il firewall e viene ispezionato in base alla configurazione dei criteri.
- L'utente interno che accede all'applicazione attraverso il firewall ha un vantaggio in termini di prestazioni in quanto evita il traffico diretto al cloud e quindi il backhaul al centro dati

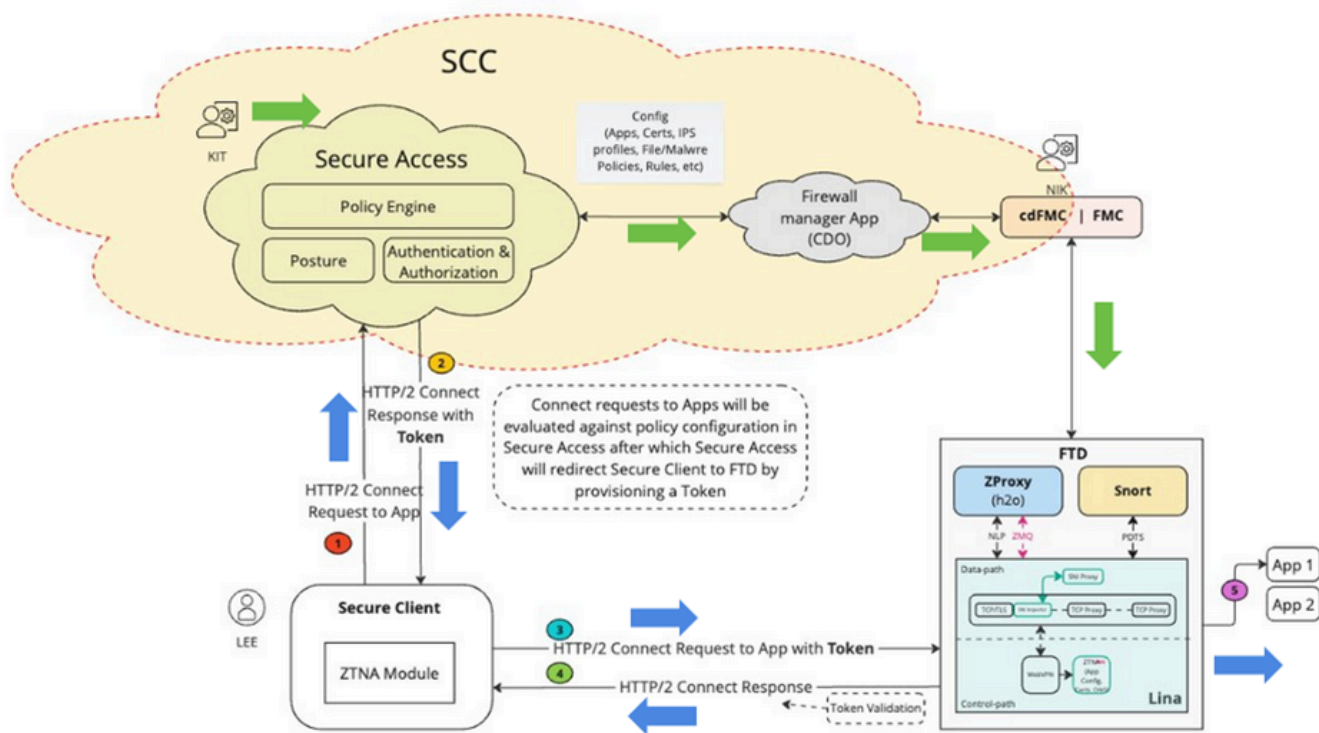
Caso 2: ispezione privata per applicazioni sensibili



Universal ZTNA - Ispezione privata per applicazioni sensibili

- Alcune applicazioni critiche possono essere configurate in modo da essere sempre accessibili attraverso il firewall.
- Il traffico di dati dell'app non deve necessariamente passare al cloud. Ad esempio, potrebbe essere presente un'applicazione di dati sensibili come il codice sorgente, che il cliente non desidera passare al cloud.
- In questi scenari, il traffico degli utenti sia remoto che permanente attraversa sempre il firewall e viene ispezionato. Anche in questo caso, tuttavia, l'autenticazione e la valutazione delle policy vengono sempre eseguite nel cloud, mentre solo il traffico dei componenti dati attraversa il firewall.

Componenti dell'architettura



Universal ZTA - Componenti dell'architettura

Security Cloud Control (SCC) è il responsabile principale della soluzione uZTNA. La tecnologia uZTNA è la prima ad essere costruita su SCC.

In SCC sono disponibili due microapplicazioni Secure Access e Firewall. Una volta eseguito il provisioning della scheda SCC e abilitati i flag delle funzionalità richieste, queste microapplicazioni saranno visibili sul lato sinistro del pannello SCC.

Client protetto: In Secure Client dovremo abilitare Zero Trust Access Module (ZTNA) per poter accedere alle applicazioni, dovremo iscriverci al modulo ZTNA.

Difesa dalle minacce del firewall : FTD che protegge queste applicazioni. FTD esegue un proxy ZT noto anche come H2O (lo stesso del proxy eseguito in Secure Access Cloud)

Ora, quando un utente (ad esempio KIT) configura una risorsa privata e una policy su una microapplicazione Secure Access, questa configurazione verrà inviata alla microapplicazione Firewall in SCC. L'applicazione firewall comprende gli elementi interni della configurazione FTD e FTD, come distribuire e gestire la configurazione su FTD. Quindi, l'app Firewall convalida questa configurazione, e richiama le API FMC per inviare la configurazione al FMC e alla fine ottenerla distribuita sul FTD. FTD può avere un'opzione di distribuzione automatica abilitata in modo che gli amministratori (ad esempio Nick) non debbano eseguire la distribuzione manuale.

1. Quando un utente (ad esempio Lee) tenta di accedere a un'applicazione, un client sicuro si connette a Secure Access utilizzando il canale mTLS. Secure Access autentica l'utente utilizzando il certificato del dispositivo client. Valuta quindi l'autorizzazione, la postura e le altre policy configurate per l'utente e per l'applicazione.

2. Secure Access, se rileva che l'applicazione è protetta dal firewall, genera un token di autenticazione, che indica al firewall che l'applicazione è già autenticata e autorizzata. Il token di autenticazione è crittografato e firmato da Secure Access

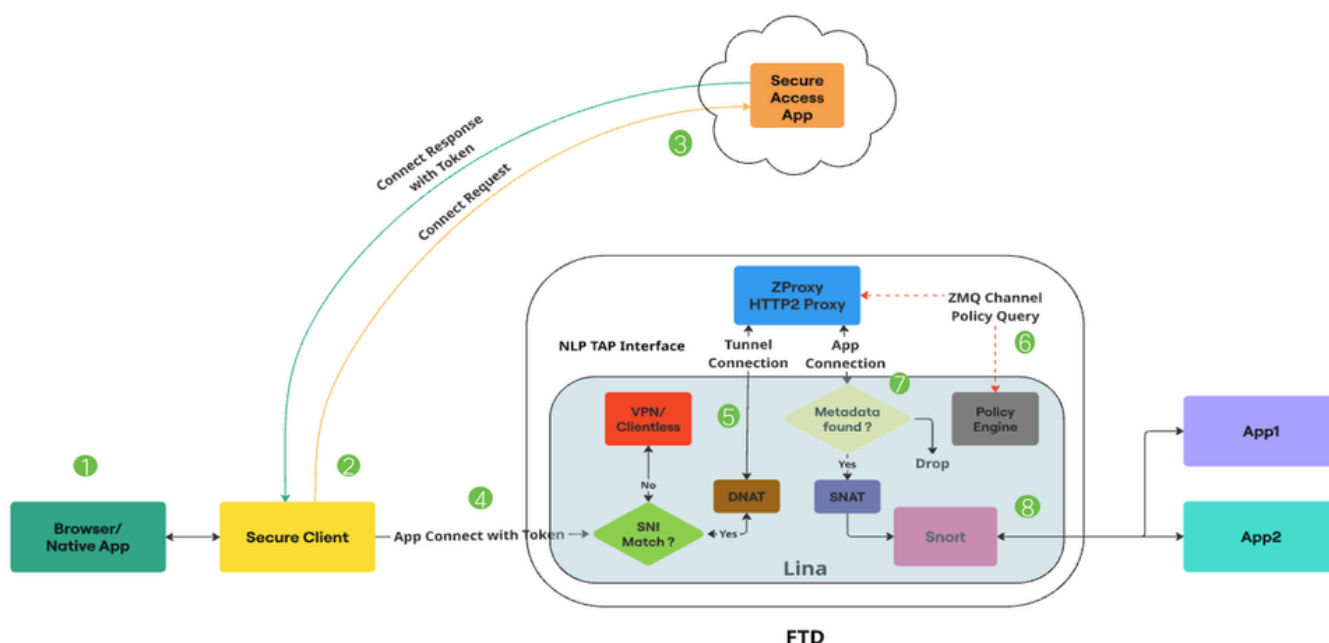
3. Secure Access reindirizza il client sicuro verso FTD insieme al token di autenticazione.

4. Secure Client stabilisce un'altra connessione con FTD, è una connessione HTTP2 su canale mTLS. Invia una richiesta CONNECT per l'applicazione a cui si sta accedendo insieme al Token.

5. FTD ora convalida il Token, se il Token viene convalidato correttamente, l'utente è autorizzato ad accedere a quell'applicazione. L'FTD invia quindi la conferma al client sicuro

Flusso dei pacchetti

Flusso di pacchetti dettagliato Universal ZTNA



Universal ZTA - Flusso pacchetto

1. L'utente tenta di accedere a un'applicazione tramite un browser Web o un'applicazione nativa.

2. Il client sicuro intercetta la connessione e la identifica come un utente che tenta di accedere a una risorsa privata.

3. Secure Client stabilisce una connessione mTLS per Secure Access, richiedendo l'accesso all'applicazione. Secure Access controlla la conformità ai criteri Universal ZTNA e ai profili di postura. Se tutto va bene, Secure Access genera un token di accesso contenente informazioni essenziali come i dettagli dell'utente, i dettagli dell'applicazione e i criteri IPS/File.

4. Il token di accesso è crittografato e firmato da Secure Access. Secure Access reindirizza quindi il client sicuro insieme al token al FTD.

5. Quando il pacchetto raggiunge il percorso dati Lina, il controllo SNI intercetta la connessione e verifica se il nome server (estensione SNI) nel client Hello corrisponde all'FQDN proxy configurato sul dispositivo. Se l'SNI corrisponde, la connessione viene indirizzata a ZProxy. Se SNI non corrisponde, la connessione viene indirizzata ad altre funzionalità che possono coesistere con Universal ZTNA.

Ad esempio: VPN, Captive Portal o ZTNA senza client. ZProxy, che supporta il protocollo MASQUE su HTTP/2, verrà eseguito sull'FTD come processo non Lina su core dedicati. La comunicazione tra Lina e ZProxy utilizza l'interfaccia Tap NLP per la gestione del traffico dati. L'IP di destinazione della connessione viene convertito nell'IP dell'interfaccia TAP dal controllo SNI.

6. Quando il proxy ZProxy riceve la connessione al tunnel mTLS dal client sicuro, verifica il certificato del dispositivo client inviato dal client sicuro. Verifica anche il token di accesso inviato con APP Connect. Tra Lina e ZProxy è presente un canale MQ zero. Viene utilizzato principalmente per scambiare messaggi di controllo. ZProxy utilizza questo canale per la risoluzione FQDN delle risorse private comunicando con Lina.

Zero MQ Channel è anche usato per propagare le informazioni presenti nel token di accesso a Lina. (Esempio: ID regola, ID criterio e così via) Lina riceve le informazioni sul token di accesso e le memorizza in un database di metadati.

7. Una volta scambiati i messaggi di controllo, ZProxy avvia una nuova connessione verso la risorsa privata. Può essere TCP o UDP. Lina quindi esegue una ricerca nel database dei metadati per questa connessione dell'app. Se i metadati non vengono trovati, la connessione viene interrotta.

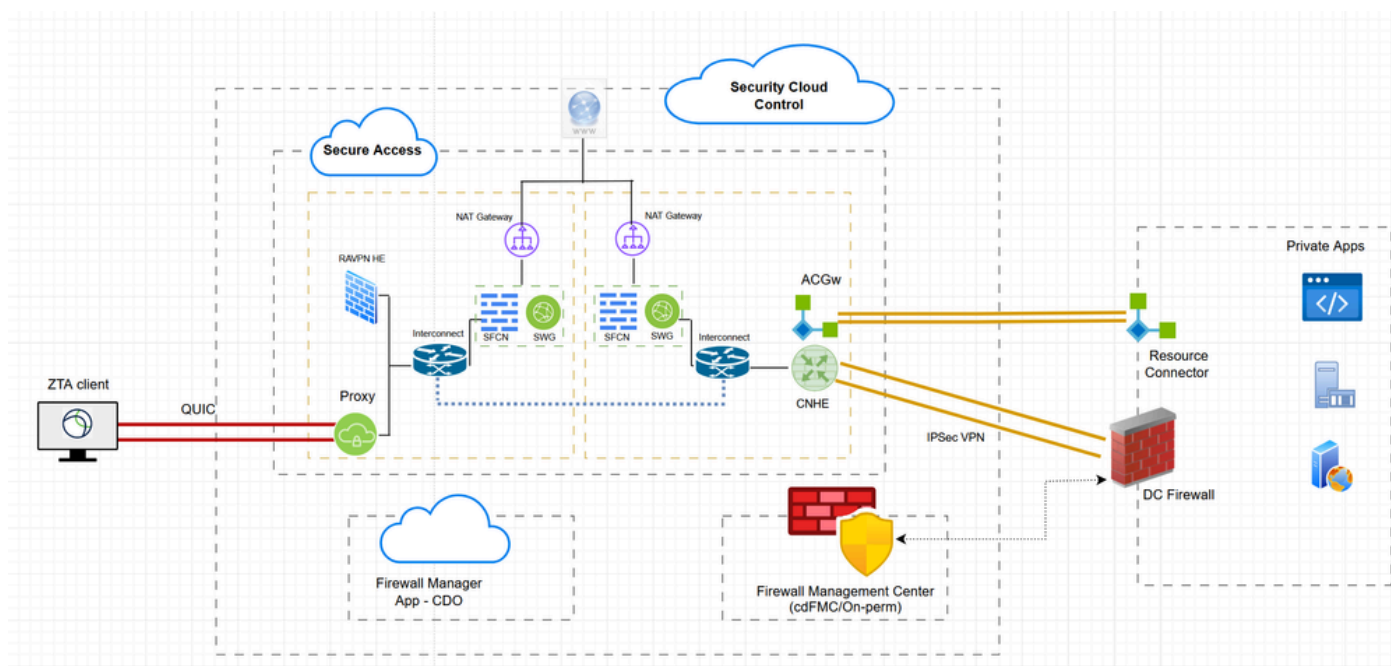
8. Poiché la connessione dell'app ha origine da ZProxy, avrà un IP interno (esempio: 169.251.1.2) come IP di origine. Il messaggio verrà convertito nell'indirizzo IP dell'interfaccia di uscita FTD prima dell'invio. Lina contrassegna quindi i flussi Universal Zero Trust per l'ispezione Snort solo se nel token di accesso è presente un criterio File o IPS. L'ID regola ottenuto dal token di accesso viene passato a Snort nei metadati di connessione.

9. Le regole Universal Zero Trust e i mapping dei criteri IPS e dei file corrispondenti vengono inviati all'FTD tramite il FMC. Il plug-in Zero Trust in Snort caricherà queste regole durante l'inizializzazione. Lina contrassegnerà i flussi di flusso Universal Zero Trust per l'ispezione dello Snort solo se nel token di accesso ottenuto da Secure Access per l'accesso a tale risorsa privata è indicato un criterio File o IPS.

L'ID regola ottenuto dal token di accesso viene passato a Snort tramite Conn Meta. Per tutti i flussi di flusso Universal Zero Trust, il plug-in Zero Trust in Snort eseguirà una ricerca di regole per l'ID regola ottenuto dal Conn Meta. Se viene trovata una corrispondenza di regole, il flusso verrà consentito e i criteri IPS e File specifici di tale regola verranno applicati al flusso. Se non viene trovata alcuna corrispondenza di regole, il plug-in Zero Trust in Snort bloccherà il flusso.

Configurazione

Esempio di rete



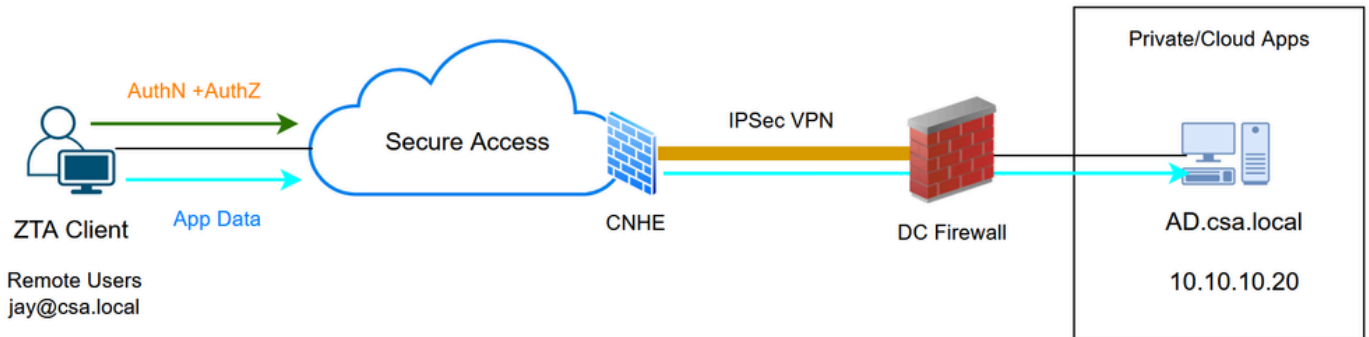
Hybrid ZTNA - Esempio di rete

Test case

Test case 1: Utente remoto - Applicazione cloud

In questo test case, verrà eseguito l'accesso a una risorsa privata su Network Tunnel Group

tramite l'imposizione del cloud. In questo caso sia la valutazione delle policy che i dati delle applicazioni verranno intercettati da Secure Access tramite il modulo ZTA . Si tratta di un flusso tradizionale a cui è possibile accedere tramite un'applicazione privata dal client registrato ZTA tramite Network Tunnel Group o Resource Connector



Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

1. Selezionare Risorse > Destinazioni > Risorse private > Fare clic su +Aggiungi

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has the **Resources** menu item highlighted. The main content area shows the **Resources** configuration page. It includes a search bar, a filter for **Private Resource Group**, and a table of existing private resources. The table has columns for **Private Resource Group**, **Connection Method**, **Connector Groups**, **Accessed by**, **Rules**, and **Total Requests**. There are three entries in the table, all using **Client-based ZTA** as the connection method.

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

Accesso sicuro - Configurazione risorse private

2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.

← Private Resources

Add a Private Resource

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

General

Private Resource Name
AD-Server

Description (optional)
Active Directory server

Accesso sicuro - Configurazione risorse private

3. Inserire il nome di dominio completo (FQDN) della risorsa privata a cui si desidera accedere. È inoltre possibile definire l'indirizzo IP della risorsa privata. Per ulteriori informazioni, vedere [Aggiungere una risorsa privata](#)

4. Selezionare il server DNS interno per risolvere il dominio

Private resource address

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

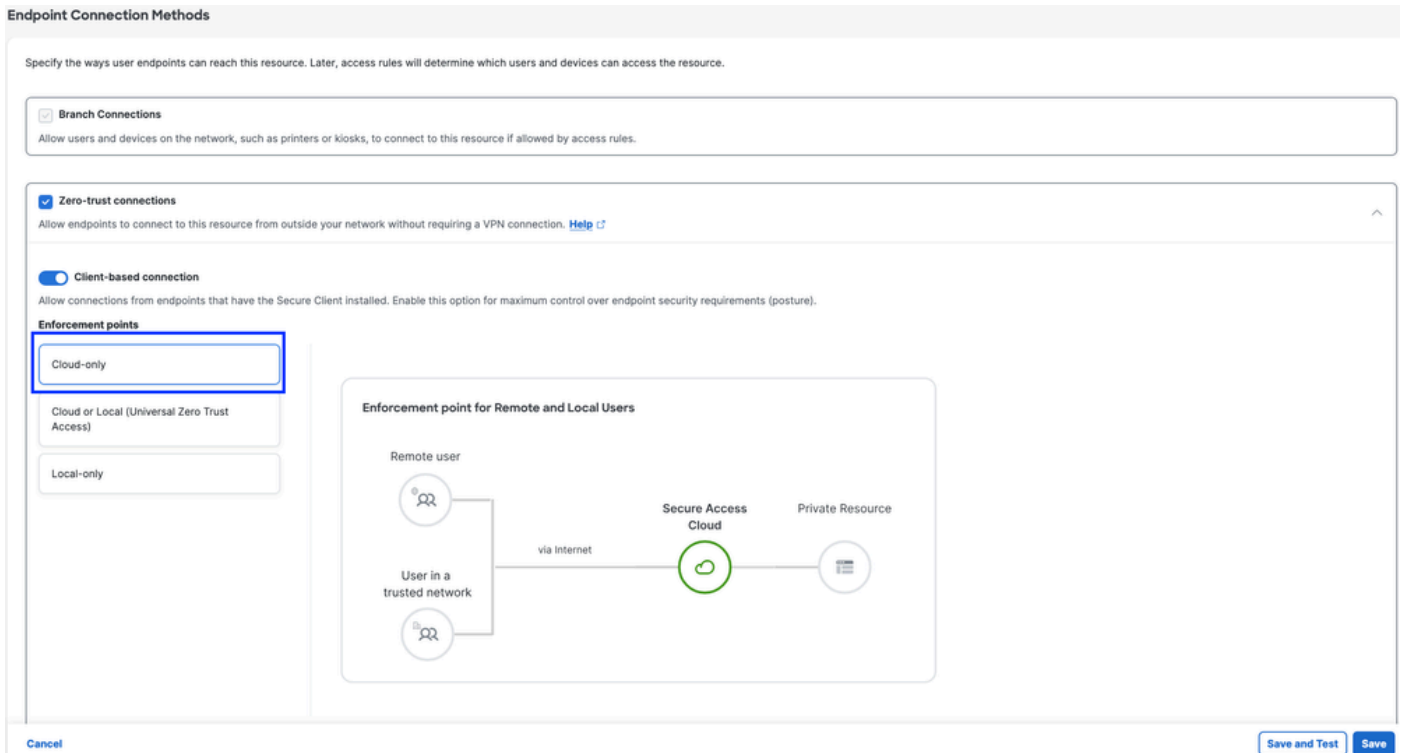
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
ad.csa.local	TCP - RDP	Any	+ Protocol & Port
Remove			
10.10.10.20	TCP - RDP	Any	+ Protocol & Port
Remove + IP Address/FQDN			

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

Internal DNS Server
PrivateDNS (10.10.10.20)

Accesso sicuro - Configurazione risorse private

5. Seleziona metodi di connessione degli endpoint



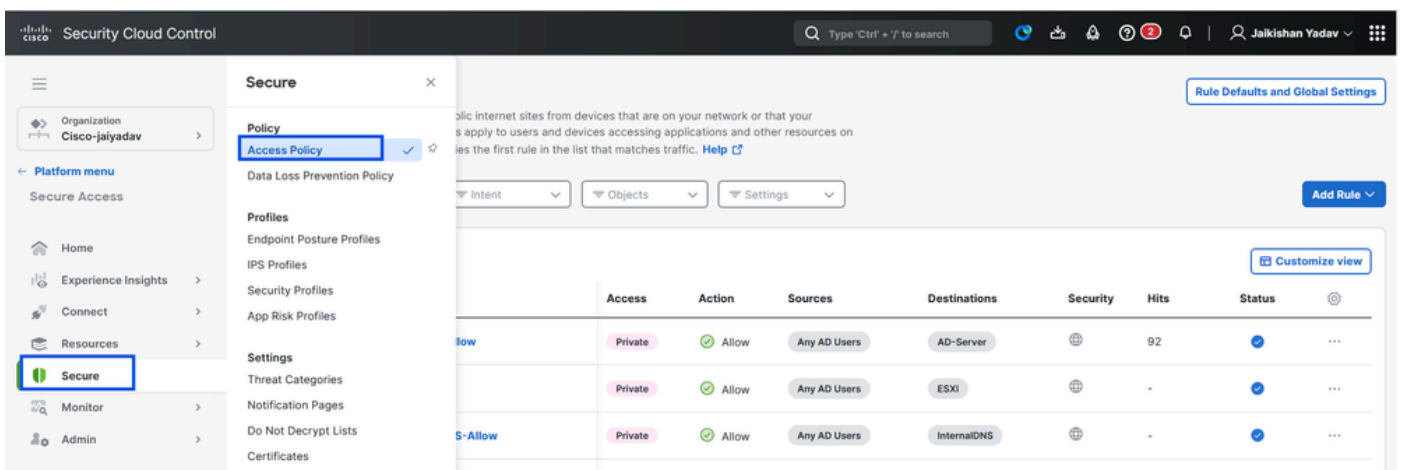
Accesso sicuro - Configurazione risorse private

6. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere [Regola di accesso privato](#)

1. Passare a Protezione > Criteri di accesso



Accesso sicuro - Configurazione criteri di accesso

2. Fare clic su Aggiungi regola, quindi scegliere Accesso privato.

Nella parte superiore della regola è disponibile un riepilogo che descrive i componenti configurati della regola.

Access Policy Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings Add Rule ^

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

Rows per page 1-2 of 2 < 1 >

Private Access

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

Internet Access

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

Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola

Add AD-RDP-Allow

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

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

Summary

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

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

1 Specify Access

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

Action:

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From: To:

Accesso sicuro - Configurazione criteri di accesso

4. Selezionare l'azione della regola e selezionare origine e destinazione

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

Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint

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

Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione

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](#)

Accesso sicuro - Configurazione criteri di accesso

7. Fare clic su Save (Salva)

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 1

Default Access Rules

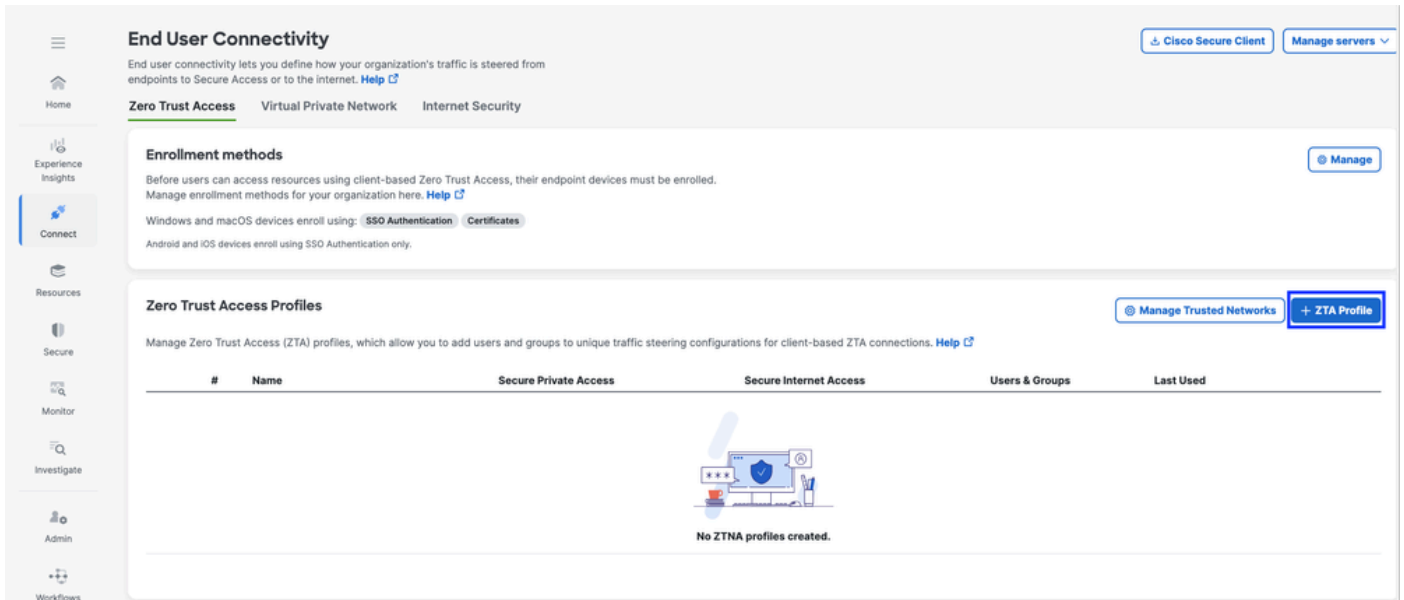
Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination	🌐🔒	-

Accesso sicuro - Configurazione criteri di accesso

Fase - 3 Aggiungere una risorsa privata al profilo ZTA

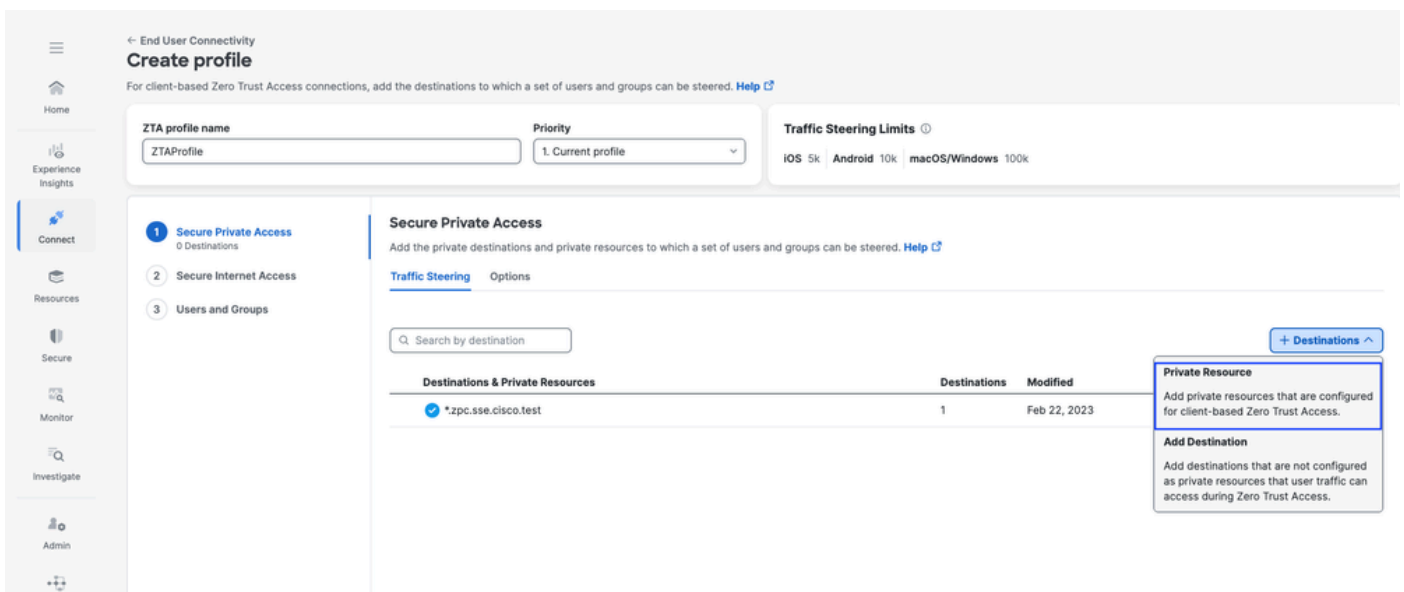
Se si utilizza un profilo ZTA personalizzato, è necessario aggiungere la rispettiva risorsa privata al profilo ZTA

1. Selezionare Connect > End User Connectivity > Zero Trust Access e fare clic su +ZTA Profile

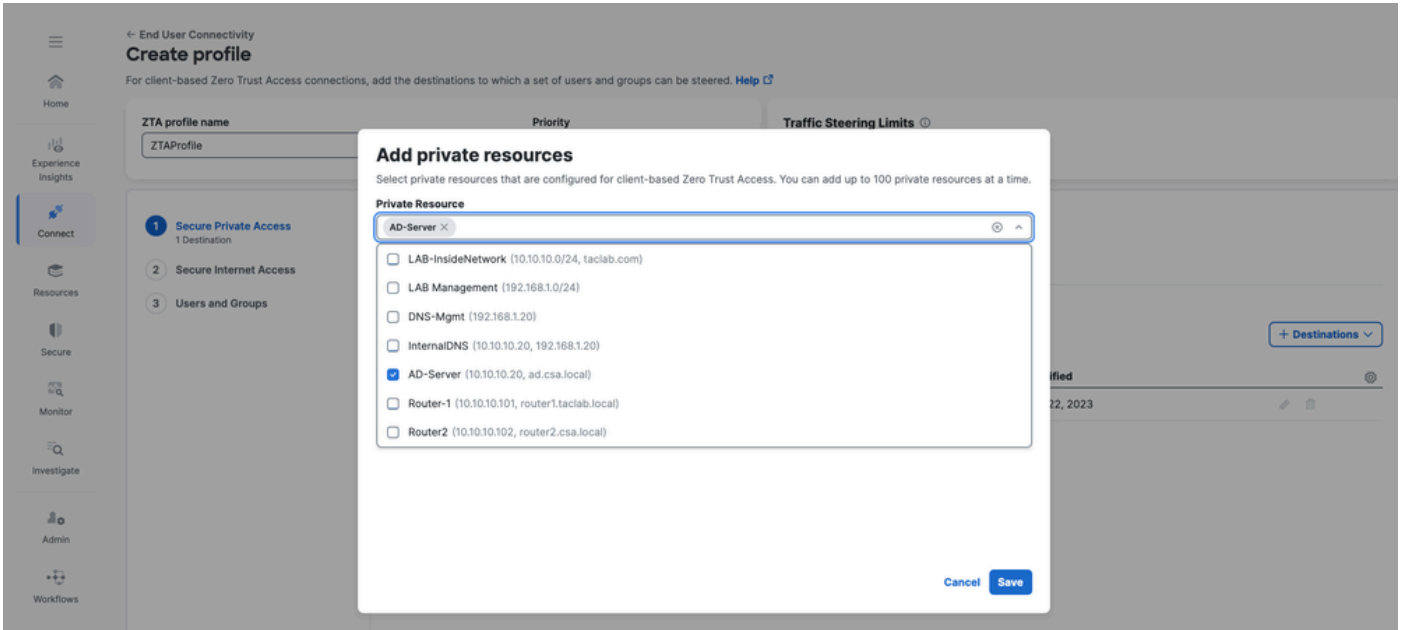


Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

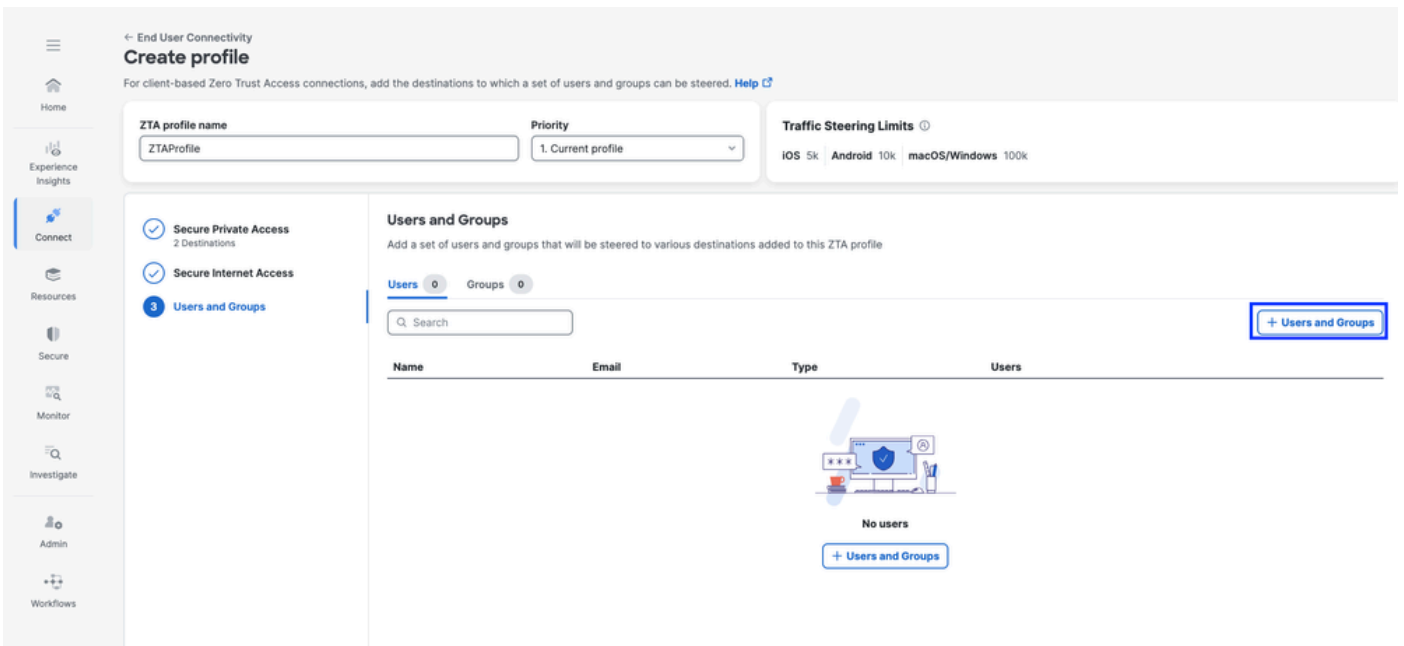


Accesso sicuro - Profilo ZTA



Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi



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

Accesso sicuro - Profilo ZTA

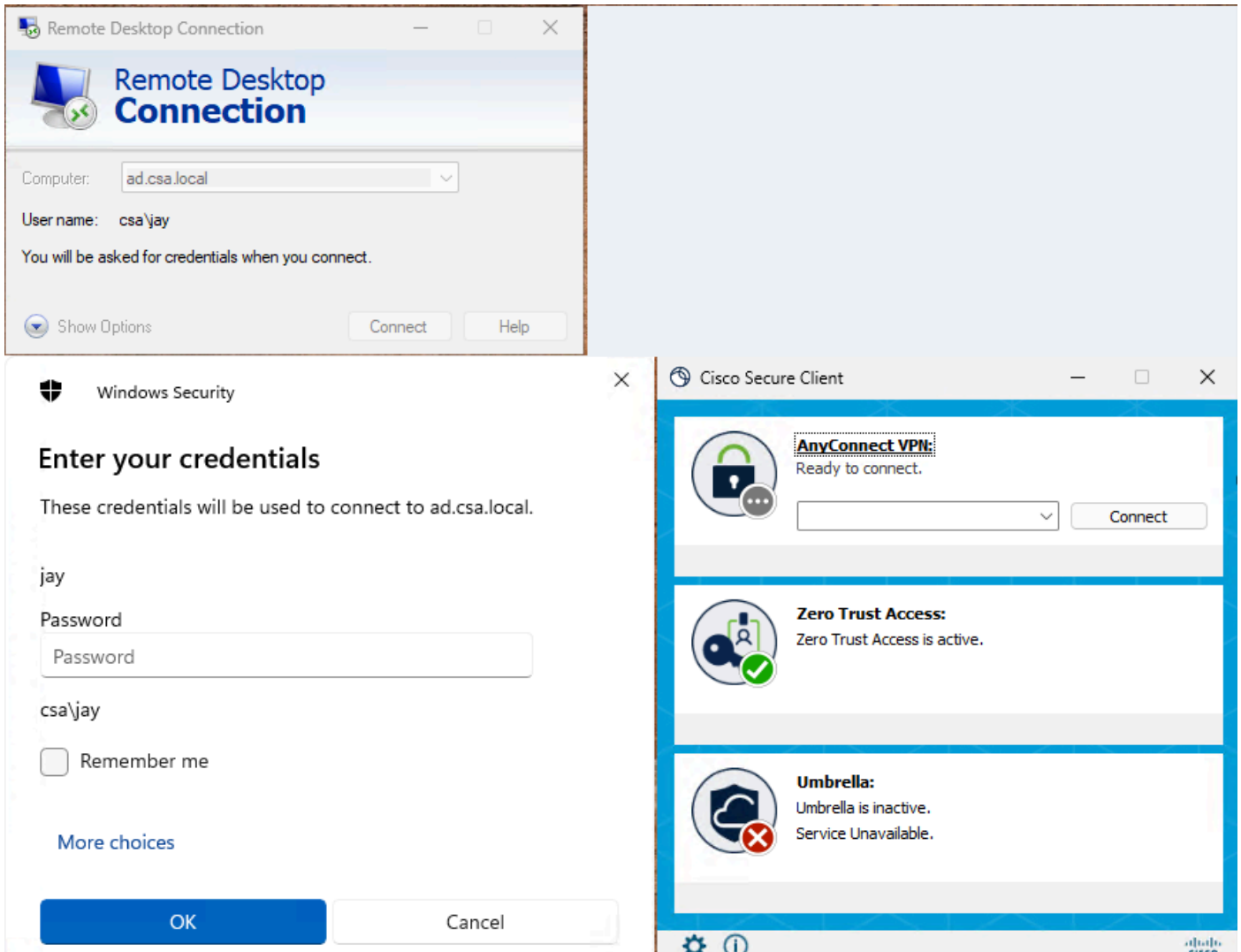


Nota: L'operazione di push e sincronizzazione della configurazione con il client per la risorsa privata assegnata può richiedere fino a 15-20 minuti

Fase - 4 Verifica dell'accesso alla risorsa privata

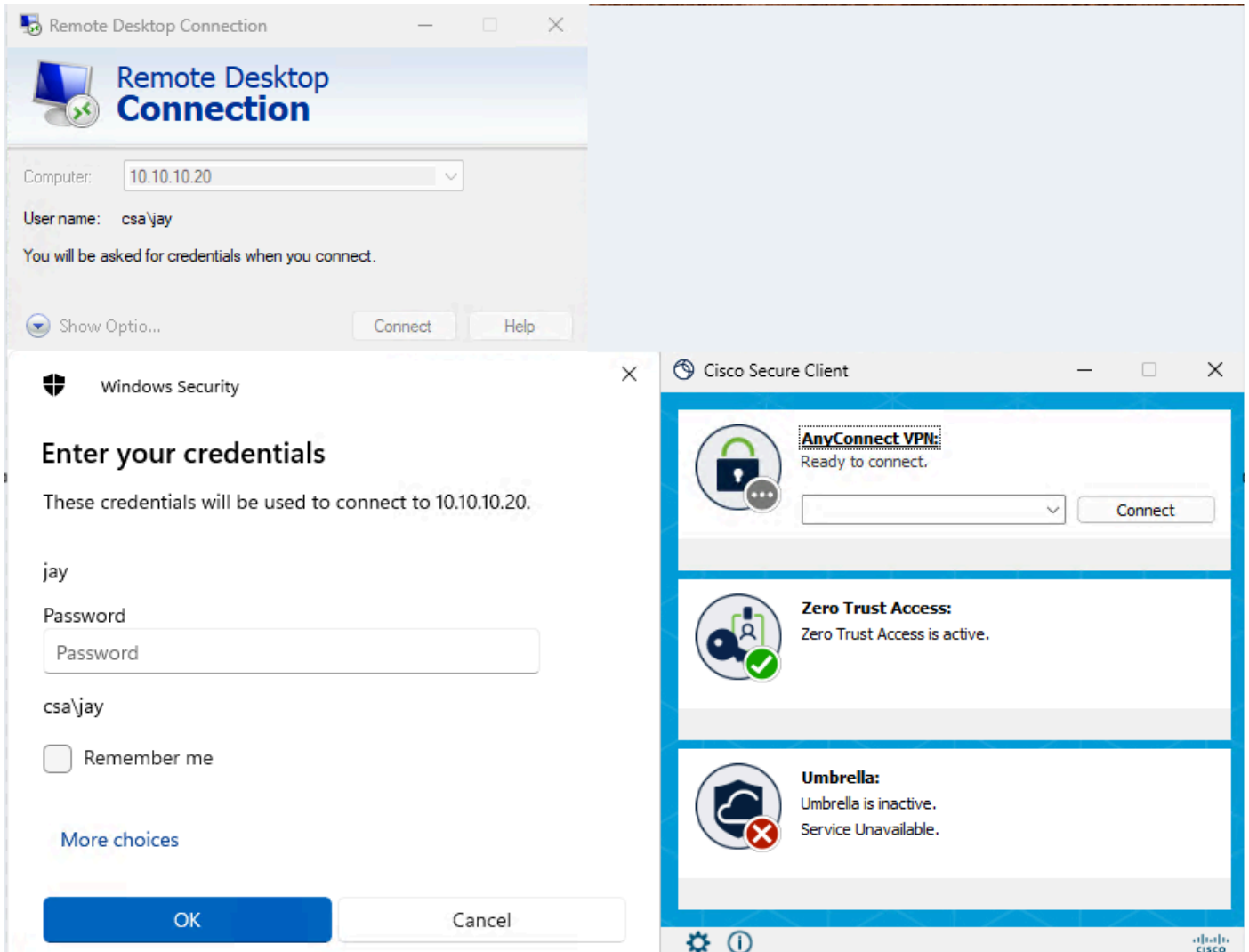
1. Accedere alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN



Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP



Accesso sicuro - Test PR

2. Verifica con gli eventi di Ricerca attività

Activity Search

Filters: IP ADDRESS 10.10.10.20, RESPONSE Allowed

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

Accesso sicuro - Ricerca attività

Activity Search

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

Accesso sicuro - Ricerca attività

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

Accesso sicuro - Ricerca attività

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

Accesso sicuro - Ricerca attività

3. Verificare gli eventi di connessione FMC

Events Troubleshooting

Destination Port / ICMP Code 3389

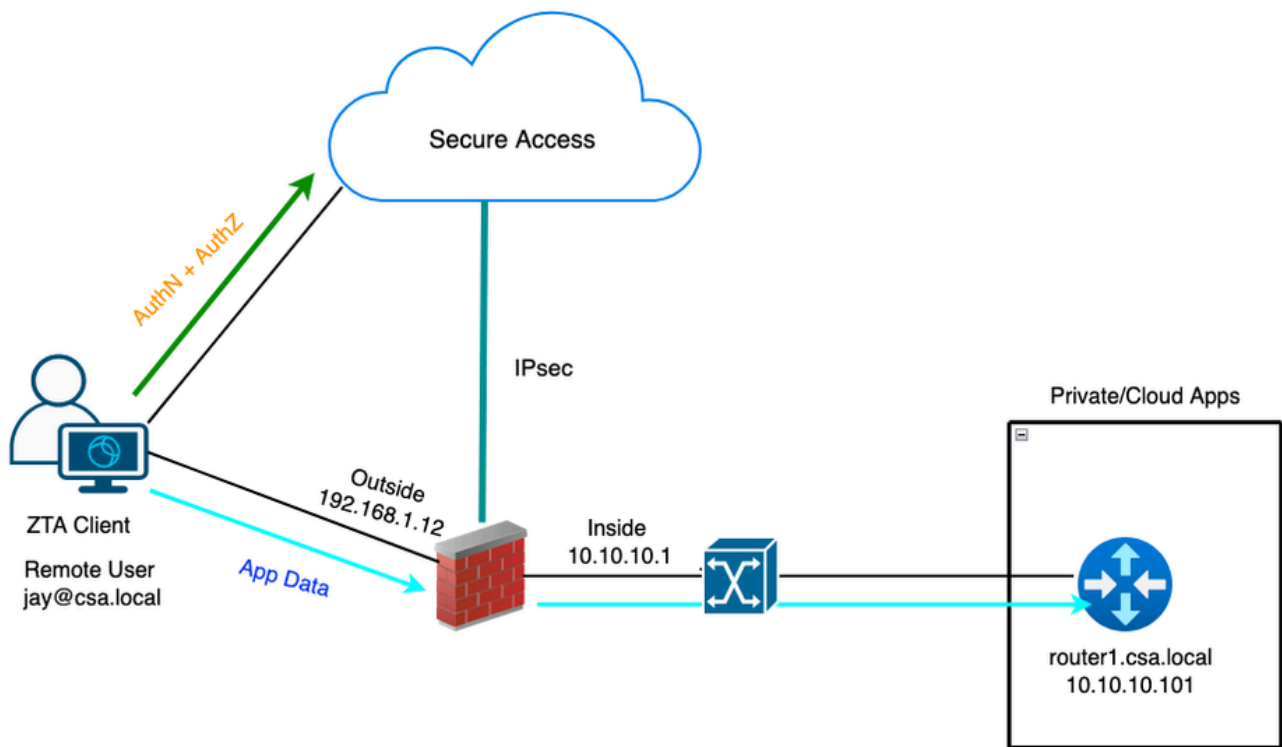
7 events Last 1 hour

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		

Eventi connessione FMC

Test case 2 - Utente remoto - Applicazione locale

L'accesso a una risorsa privata tramite l'imposizione locale, in questo tipo di valutazione dei criteri di imposizione avviene su Secure Access ma i dati dell'applicazione rimangono locali a FTD. Ad esempio, un client o un utente con registrazione ZTA si è connesso alla rete domestica e sta tentando di accedere a una risorsa privata che si trova dietro FTD all'interno dell'interfaccia.



Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

1. Selezionare Risorse > Destinazioni > Risorse private > Fare clic su +Aggiungi

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

Accesso sicuro - Configurazione risorse private

2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.

← 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

Description (optional)

Accesso sicuro - Configurazione risorse private

3. Inserire il nome di dominio completo (FQDN) della risorsa privata a cui si desidera accedere. È inoltre possibile definire l'indirizzo IP della risorsa privata. Per ulteriori informazioni, vedere [Aggiungere una risorsa privata](#)

4. Selezionare il server DNS interno per risolvere il dominio

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="router1.csa.local"/>	<input type="text" value="Any TCP"/>	<input type="text" value="22"/>	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.101"/>	<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 PrivateDNS (10.10.10.20) ^

Internal DNS Server

Accesso sicuro - Configurazione risorse private

5. Seleziona metodi di connessione degli endpoint

6. Selezionare FTD come punti di applicazione locale

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

Accesso sicuro - Configurazione risorse private



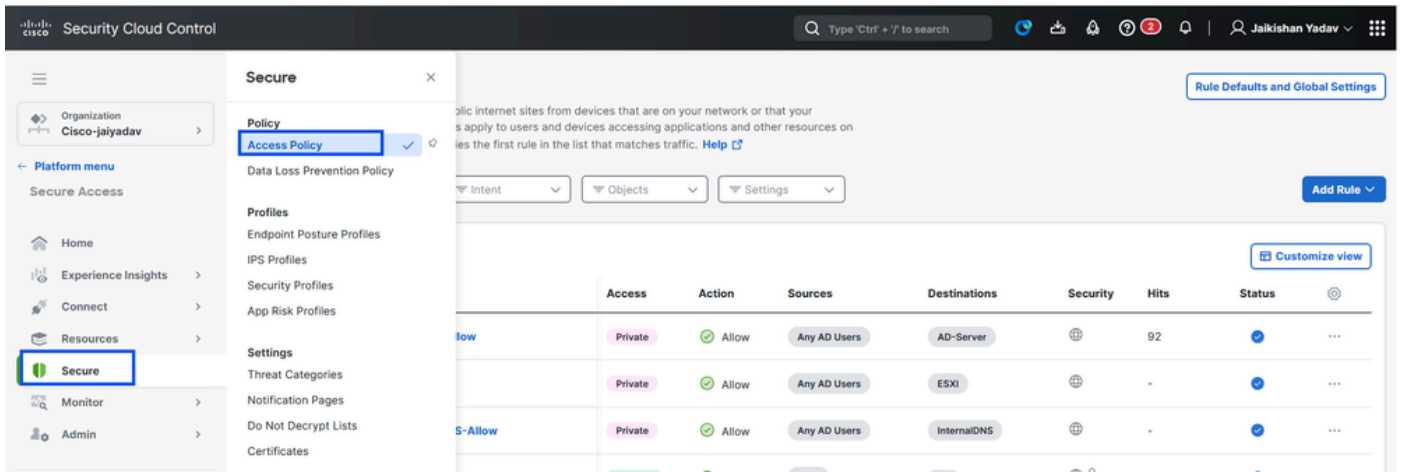
Nota: A seconda del tipo di iscrizione selezionato, questa modifica assocerà automaticamente la prenotazione permanente all'FTD e attiverà una distribuzione di criteri

7. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere [Regola di accesso privato](#)

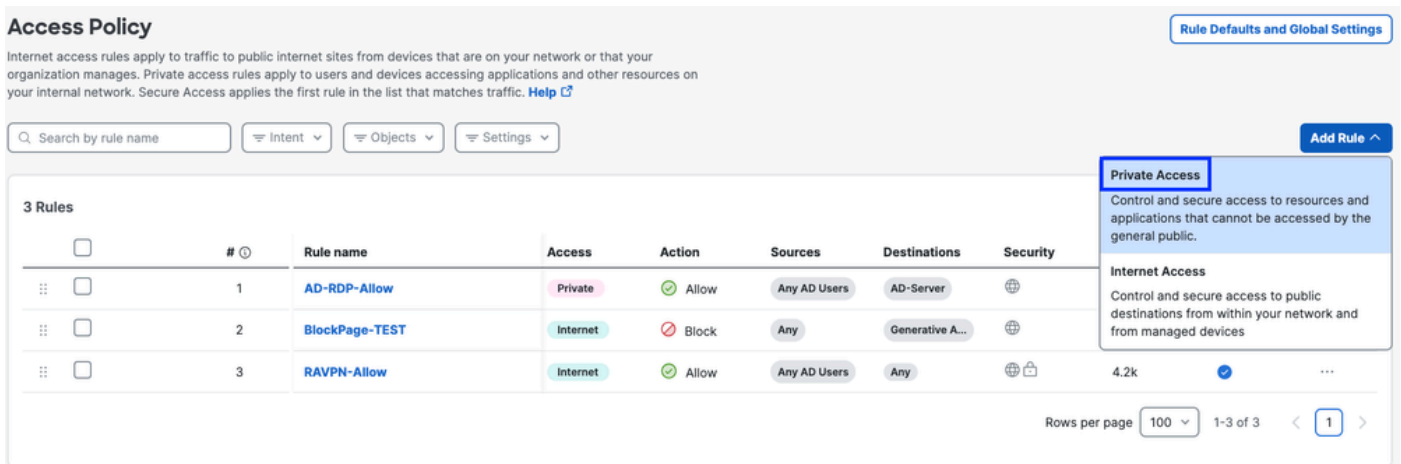
1. Passare a Protezione > Criteri di accesso



Accesso sicuro - Configurazione risorse private

2. Fare clic su Aggiungi regola, quindi scegliere Accesso privato.

Nella parte superiore della regola è disponibile un riepilogo che descrive i componenti configurati della regola.



Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola

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 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.

Accesso sicuro - Configurazione criteri di accesso

4. Selezionare l'azione della regola e selezionare origine e destinazione

Rule name Rule order

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

To

+ AND

Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint

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](#)

Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione

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](#)

Accesso sicuro - Configurazione criteri di accesso

7. Fare clic su Save (Salva)

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 >

Accesso sicuro - Configurazione criteri di accesso

Fase 3 - Verifica dell'associazione di PR sull'FTD

1. Passare a Connetti > Connessioni di rete > FTD

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' dialog box with 'Network Connections' selected under 'Essentials'. Below this, there are two status indicators: '0 Warning' and '1 Connected'. The 'FTDs' section is highlighted, showing a list of tunnel groups with filters for 'Region' and 'Status', and a '+ Add' button.

Accesso sicuro - Verifica PR

2. Fare clic su FTD > Visualizza risorse associate a questo FTD

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](#)

Accesso sicuro - Verifica PR

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](#)

Accesso sicuro - Verifica PR

3. Fare clic su chiudi

4. Verificare che lo stato , la risorsa associata e la configurazione siano sincronizzati

The screenshot displays the Palo Alto Networks management console. On the left, the 'Network Connections' page 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. One entry is visible: FMC_FTD (Device FQDN: ftd.csa.local, Trusted network: LAN, Version: v10.0.0, FMC: FMC, UZTA Configuration status: Synced, Associated Resources: 1). The 'UZTA Configuration status' cell is highlighted with a blue box. On 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 31 Dec 2025, at 2:51 AM UTC), Assigned Trusted Network (LAN, 1 DNS Servers), and Associated Resources (1). The 'Associated Resources' section shows a table with columns for Status and Count, with one entry: Synced (1). This entry is also highlighted with a blue box.

Accesso sicuro - Verifica PR

5. Verificare che la configurazione sia stata sottoposta a PUSH in FTD

Accedere alla cli FTD e passare alla modalità LINA

show running-config applicazione oggetto

```
> 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 - Verifica PR

Fase - 4 Aggiungere una risorsa privata al profilo ZTA

1. Selezionare Connect > End User Connectivity > Zero Trust Access e fare clic su 3 punti per modificare il profilo ZTA

The screenshot shows the 'End User Connectivity' dashboard. The 'Zero Trust Access Profiles' section is active, displaying a table with one profile named 'ZTAProfile'. A context menu is open over the profile, showing 'Edit' and 'Delete' options.

#	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

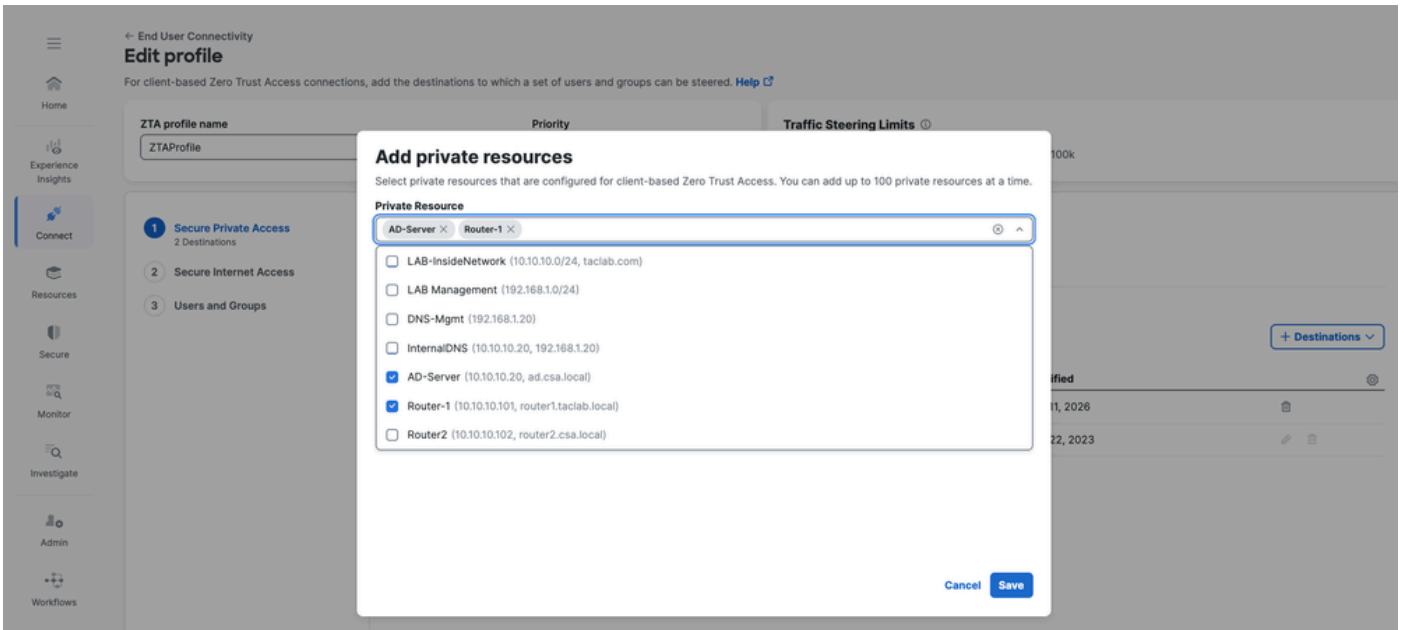
Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

The screenshot shows the 'Create profile' page for a Zero Trust Access profile. The 'Secure Private Access' step is active, showing a search for destinations. A table lists a private resource: '*zpc.sse.cisco.test'. A tooltip is visible over the table, explaining the 'Private Resource' and 'Add Destination' options.

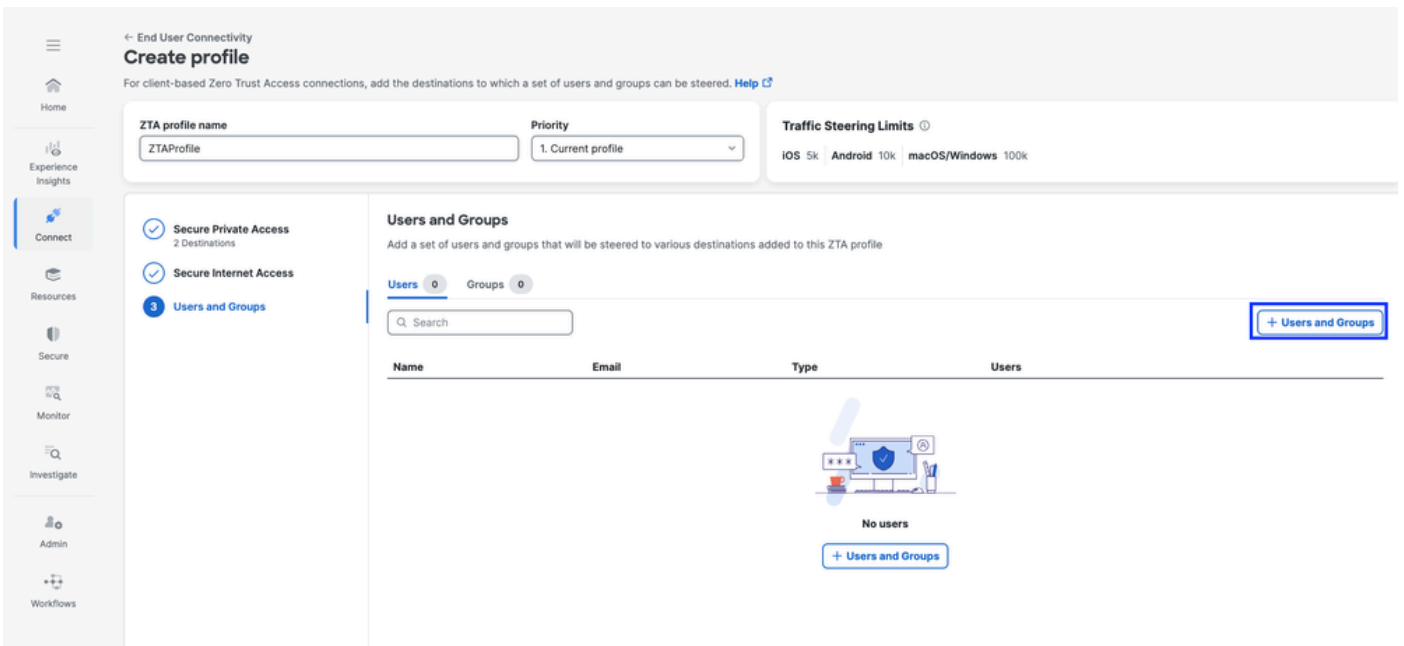
Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

Accesso sicuro - Profilo ZTA



Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi



Accesso sicuro - Profilo ZTA

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

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

Users and Groups

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

Users: 1 | Groups: 0

Search:

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

Rows per page: 10

Back Close

Accesso sicuro - Profilo ZTA

Fase - 5 Verifica dell'accesso alla risorsa privata

1. Verificare che l'utente remoto sia in grado di risolvere il nome di dominio completo FTD

```
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
```

Accesso sicuro - Test PR

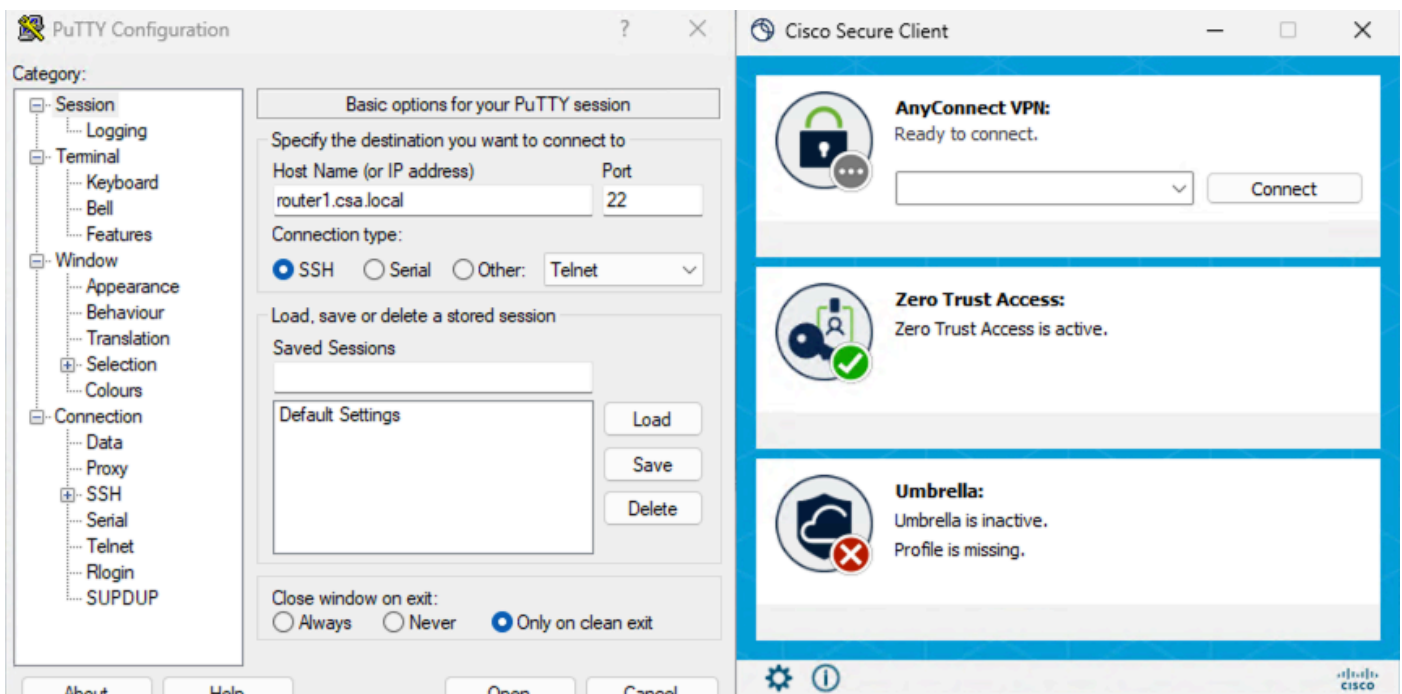
2. Verificare che l'FTD possa raggiungere la risorsa privata utilizzando il nome di dominio completo

```
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# █
```

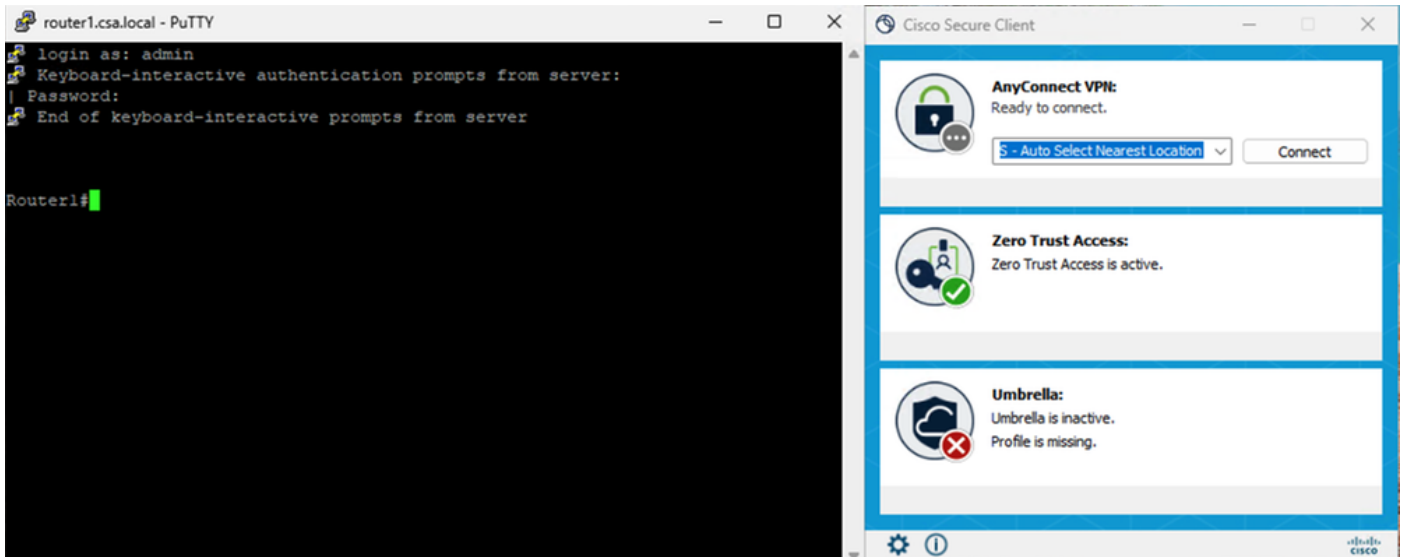
Accesso sicuro - Test PR

3. Eseguire il test della connessione SSH alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN

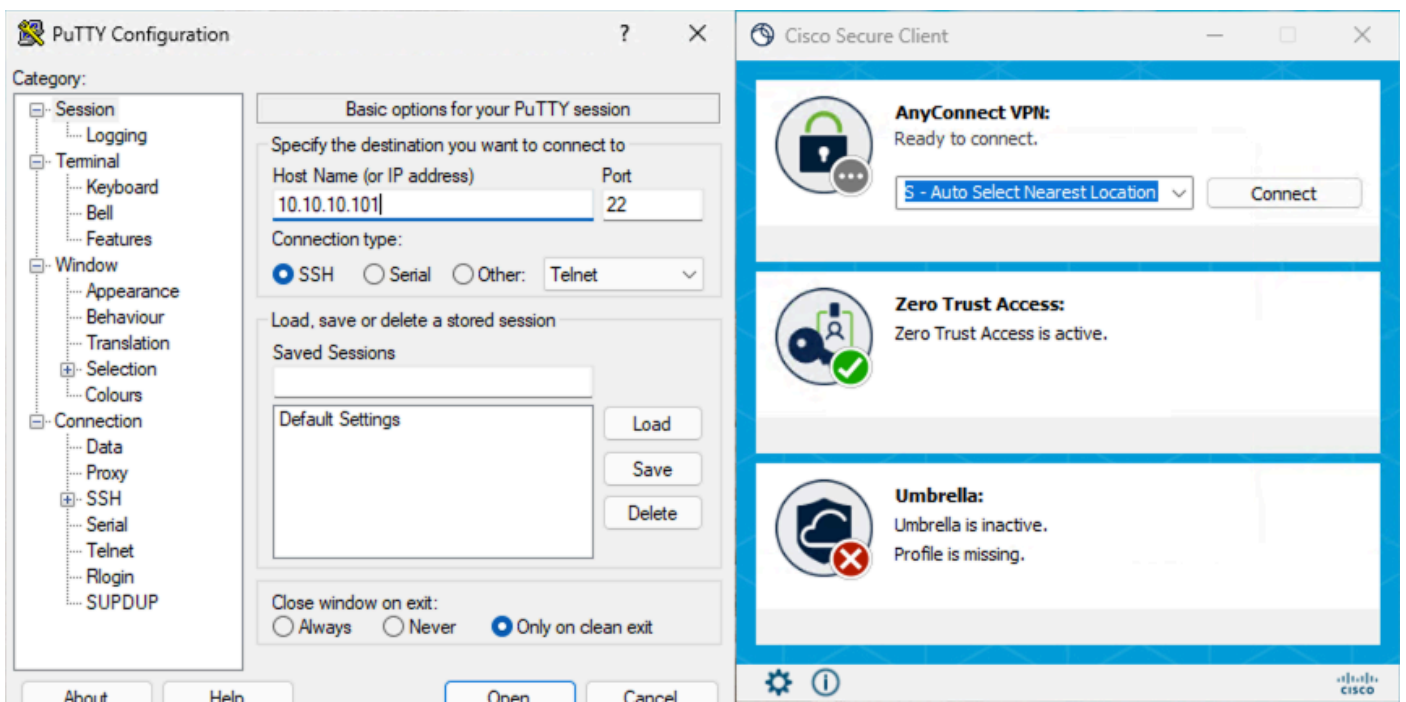


Accesso sicuro - Test PR

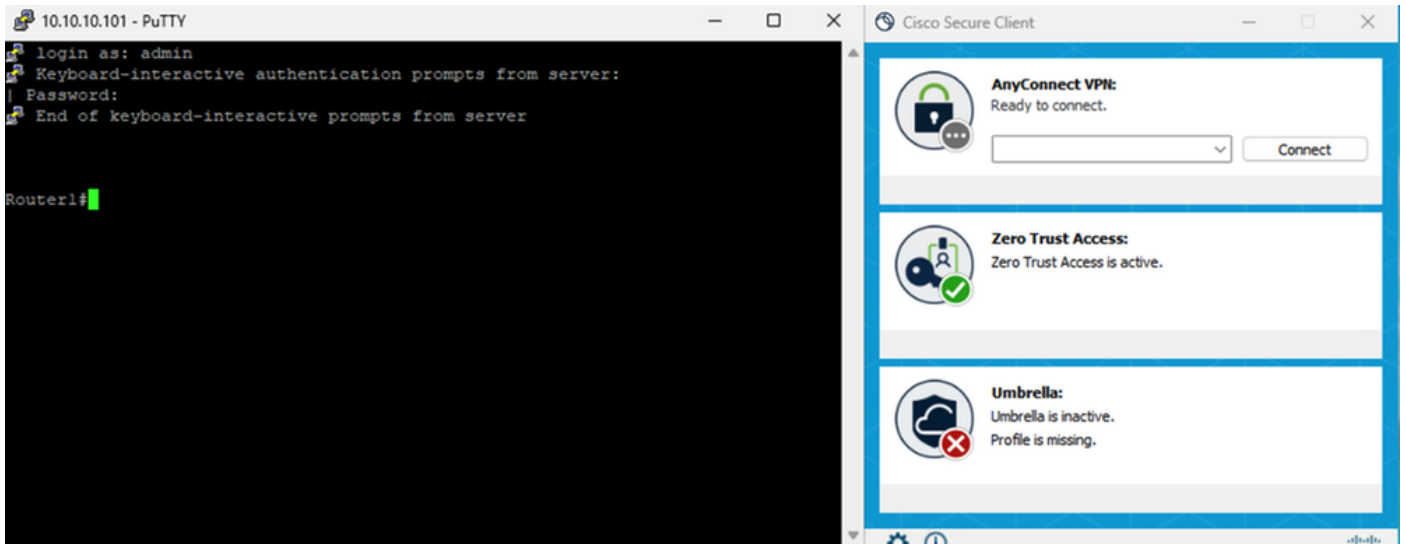


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP



Accesso sicuro - Test PR



Accesso sicuro - Test PR

4. Verifica registri di ricerca attività accesso sicuro

Activity Search Schedule Export CSV LAST 24 HOURS

FILTERS Advanced CLEAR Saved Searches Customize Columns ZTA Client-based

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

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

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location
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

Accesso sicuro - Ricerca attività

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

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

Event Details X

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:55 PM

Access details

Identity: jay (jay@csa.local)

Win: Win10

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

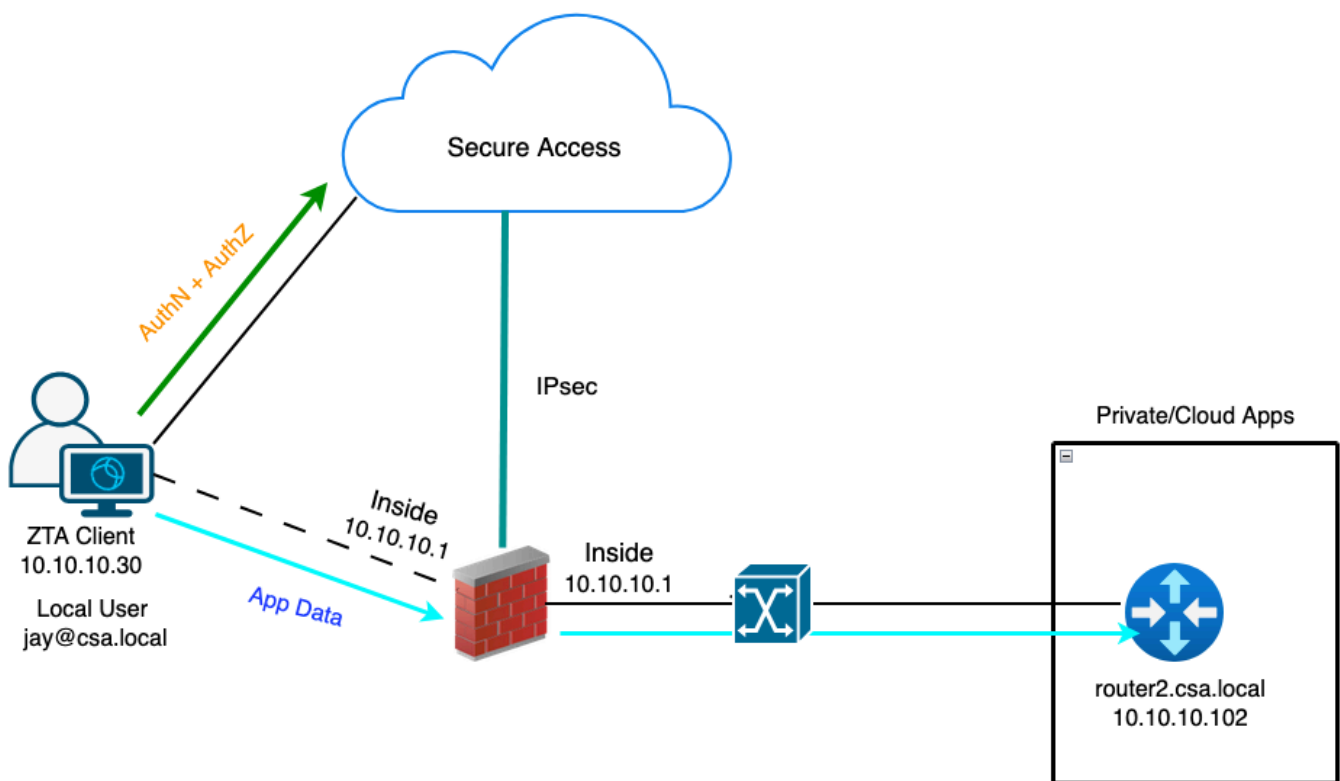
Enforcement Point: FTD > FMC_FTD

Destination: router1.csa.local

Destination IP: -

Test case 3 - Utente locale - Applicazione locale

L'accesso a una risorsa privata tramite l'imposizione locale come utente locale, in questo tipo di valutazione dei criteri di imposizione avviene su Secure Access ma i dati dell'applicazione rimangono locali a FTD. Ad esempio, un client o un utente con registrazione ZTA si è connesso alla rete domestica e sta tentando di accedere a una risorsa privata che si trova dietro FTD all'interno dell'interfaccia. Se la risorsa privata si trova dietro la DMZ o qualsiasi altra interfaccia dell'FTD, dovremo creare una regola di accesso sull'FTD per autorizzare il traffico tra l'IP o la rete del client e la risorsa privata.

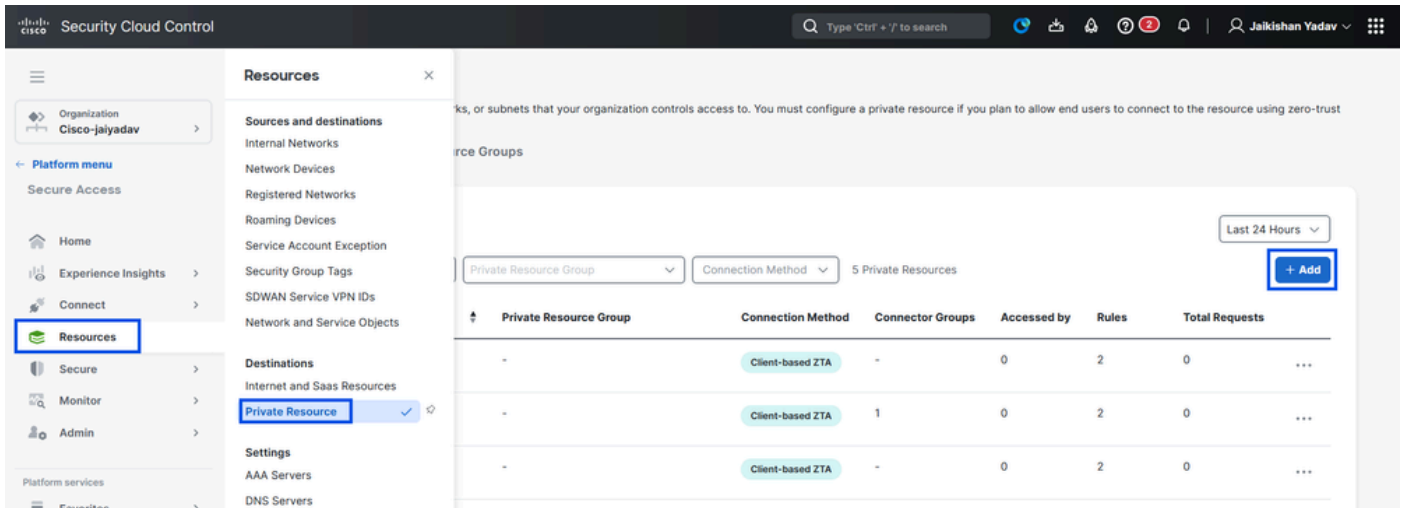


Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

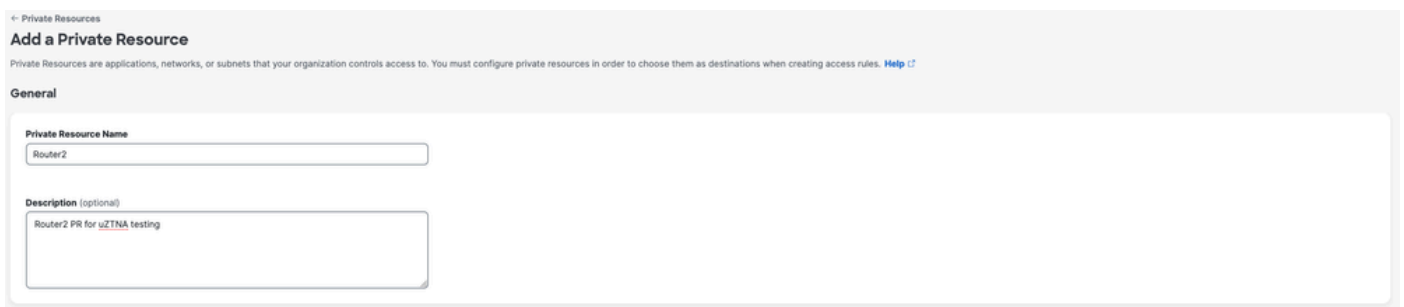
Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

1. Selezionare Risorse > Destinazioni > Risorse private > Fare clic su +Aggiungi



Accesso sicuro - Configurazione risorse private

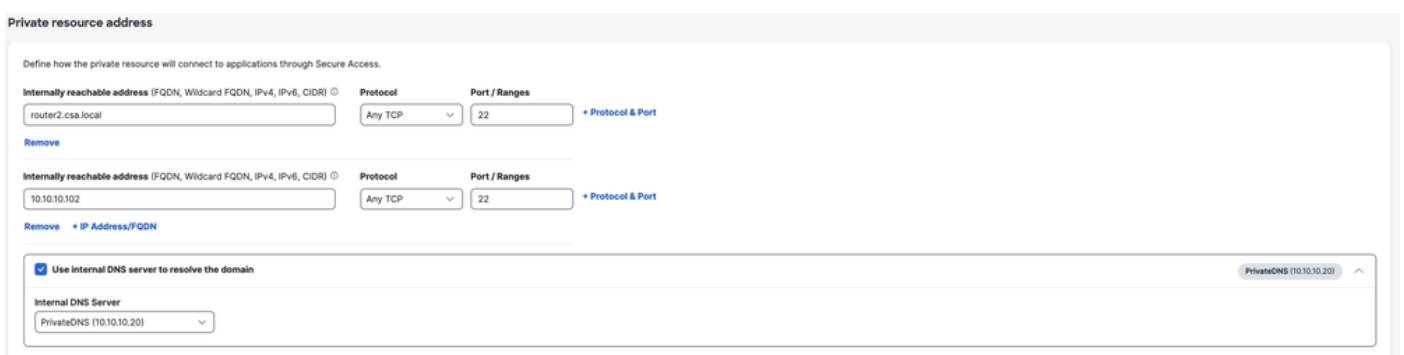
2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.



Accesso sicuro - Configurazione risorse private

3. Inserire il nome di dominio completo (FQDN) della risorsa privata a cui si desidera accedere. È inoltre possibile definire l'indirizzo IP della risorsa privata. Per ulteriori informazioni, vedere [Aggiungere una risorsa privata](#)

4. Selezionare il server DNS interno per risolvere il dominio



5. Seleziona metodi di connessione degli endpoint

6. Selezionare FTD come punti di applicazione locale

Endpoint Connection Methods

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

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

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

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

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

Enforcement point for Remote User

Remote user via internet Local Firewall Private Resource

Enforcement point for Local user

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

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

Change the remotely reachable addresses

Cancel Save and Test Save



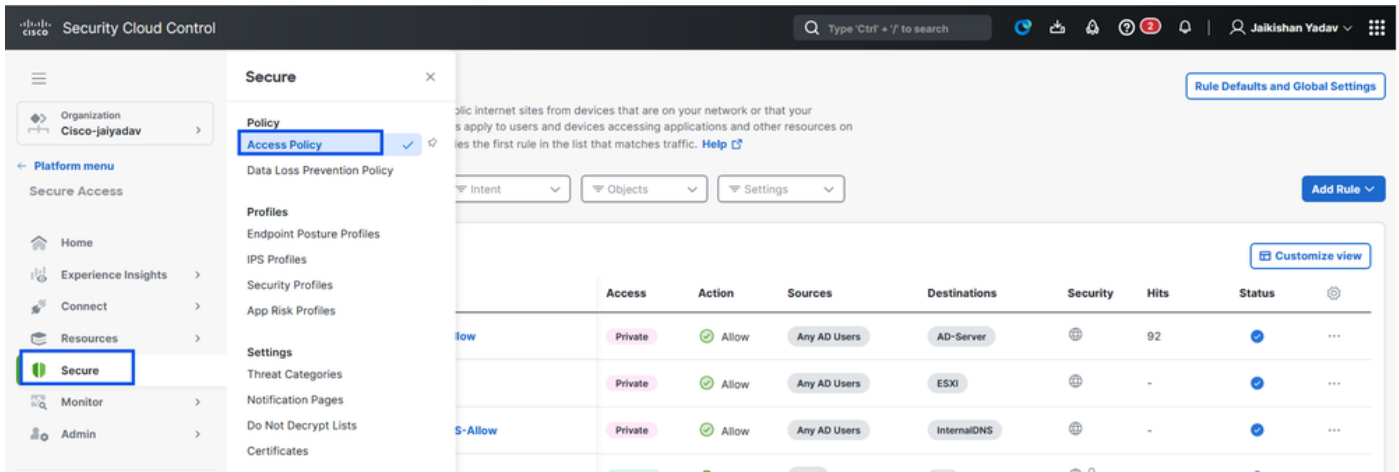
Nota: A seconda del tipo di iscrizione selezionato, questa modifica assocerà automaticamente la prenotazione permanente all'FTD e attiverà una distribuzione di criteri

7. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere [Regola di accesso privato](#)

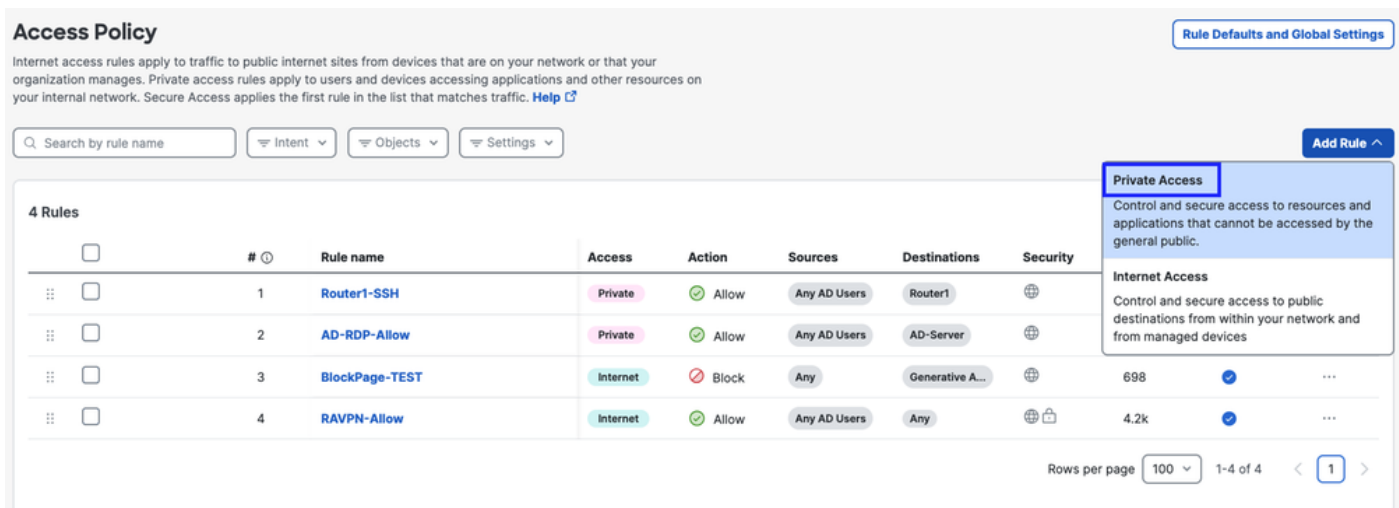
1. Passare a Protezione > Criteri di accesso



Accesso sicuro - Configurazione criteri di accesso

2. Fare clic su Aggiungi regola, quindi scegliere Accesso privato.

Nella parte superiore della regola è disponibile un riepilogo che descrive i componenti configurati della regola.



Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola

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.

Accesso sicuro - Configurazione criteri di accesso

4. Selezionare l'azione della regola e selezionare origine e destinazione

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

Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint

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](#)

Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione

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](#)

Accesso sicuro - Configurazione criteri di accesso

7. Fare clic su Save (Salva)

Access Policy

Rule Defaults and Global Settings

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access rules apply 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

Accesso sicuro - Configurazione criteri di accesso

Fase 3 - Verifica dell'associazione di PR sull'FTD

1. Passare a connessione > Connessioni di rete > FTD

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' dialog box with 'Essentials' and 'Network Connections' selected. Below this, there are 'Network Groups' and 'FTDs' sections. A summary card shows '0 Warning' and '1 Connected'. At the bottom, there are filters for 'Region' and 'Status' and an '+ Add' button.

Accesso sicuro - Verifica PR

2. Fare clic su FTD > Visualizza risorse associate a questo FTD

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

Accesso sicuro - Verifica PR

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

Accesso sicuro - Verifica PR

3. Fare clic su chiudi

4. Verificare che lo stato , la risorsa associata e la configurazione siano sincronizzati

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', FMC 'FMC', and a 'Synced' status, 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).

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

Accesso sicuro - Verifica PR

5. Verificare che la configurazione sia stata sottoposta a PUSH in FTD

Accedere alla cli FTD e passare alla modalità LINA

show running-config applicazione oggetto

```

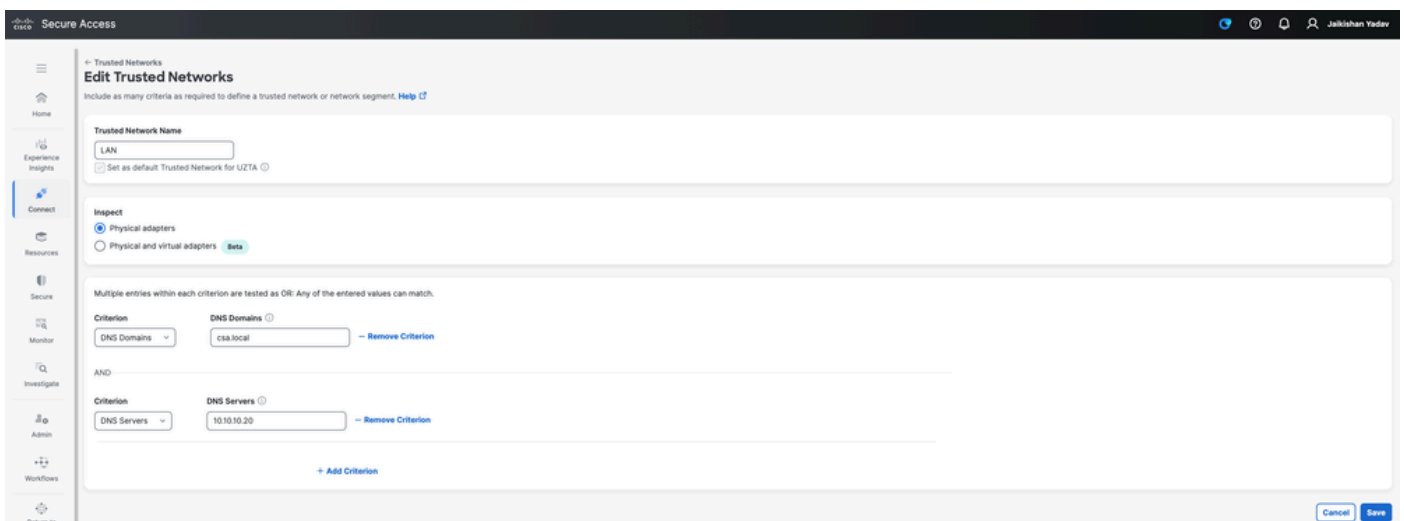
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal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

```

Accesso sicuro - Verifica PR

Passaggio 4: Configurare " Gestire le reti attendibili o le impostazioni ZTA"

Selezionare Connetti > Connettività utente finale > Accesso con attendibilità totale > Impostazioni ZTA e configurare Reti attendibili



Accesso sicuro - Configurazione TND

Fase -5 Aggiungere una risorsa privata al profilo ZTA

1. Selezionare Connetti > End User Connectivity > Zero Trust Access e fare clic su 3 punti per modificare il profilo ZTA

End User Connectivity

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

Zero Trust Access | Virtual Private Network | Internet Security

Enrollment methods Manage

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

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

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

Edit Delete

Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

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

+ Destinations

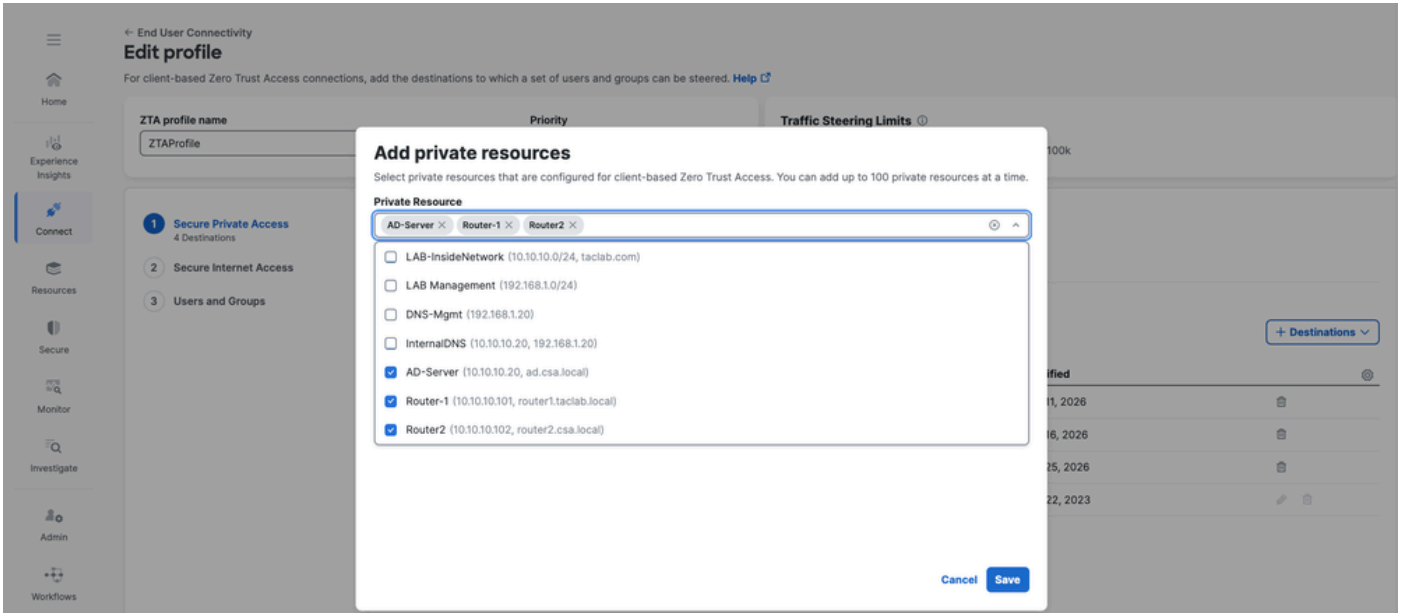
Private Resource

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

Add Destination

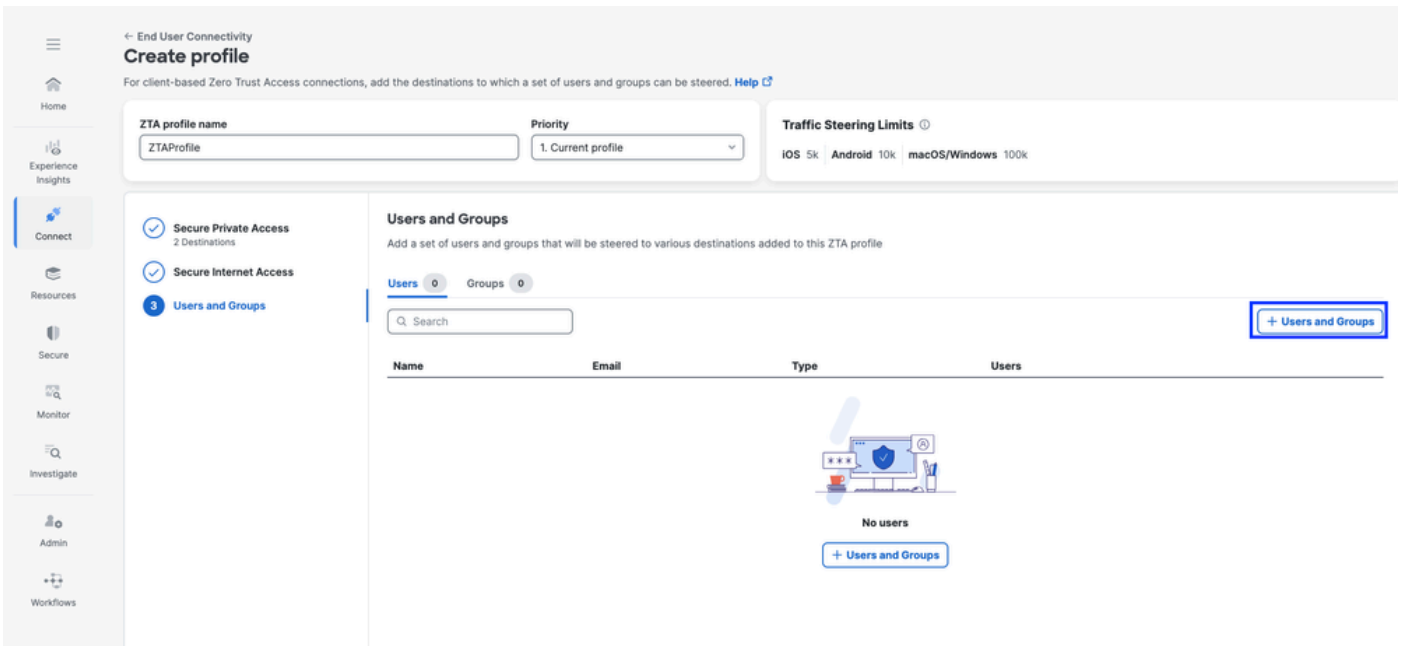
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Accesso sicuro - Profilo ZTA



Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi



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

Accesso sicuro - Profilo ZTA

Fase - 6 Verifica dell'accesso alla risorsa privata

1. Verificare l'impronta digitale di rete per ZTA TND

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

The main content area is titled "Zero Trust Access" and contains four tabs: "Statistics", "Advanced", "Configuration", and "Message History". The "Statistics" tab is active, showing a list of network flow statistics:

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

Below the statistics, there are two expandable sections:

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

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

Accesso sicuro - Test PR

2. Verificare che l'utente remoto sia in grado di risolvere il nome di dominio completo FTD

```
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
```

Accesso sicuro - Test PR

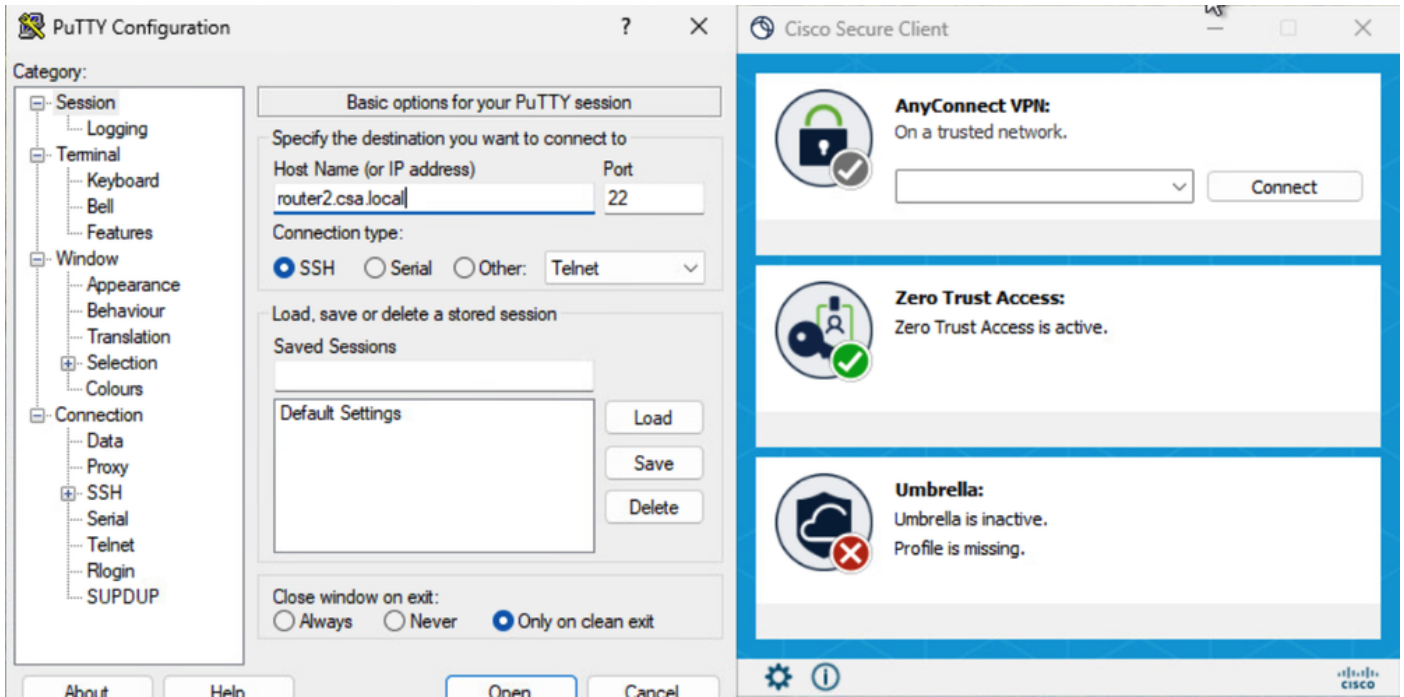
3. Verificare che l'FTD possa raggiungere la risorsa privata utilizzando l'FQDN

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

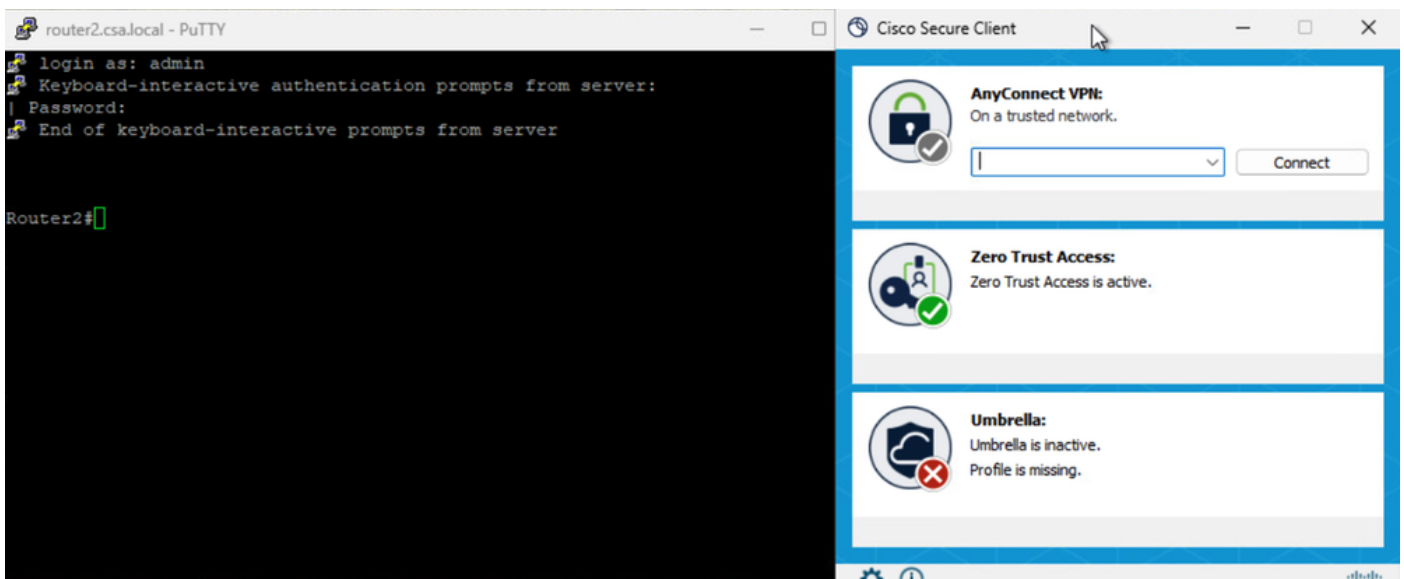
Accesso sicuro - Test PR

4. Eseguire il test della connessione SSH alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN

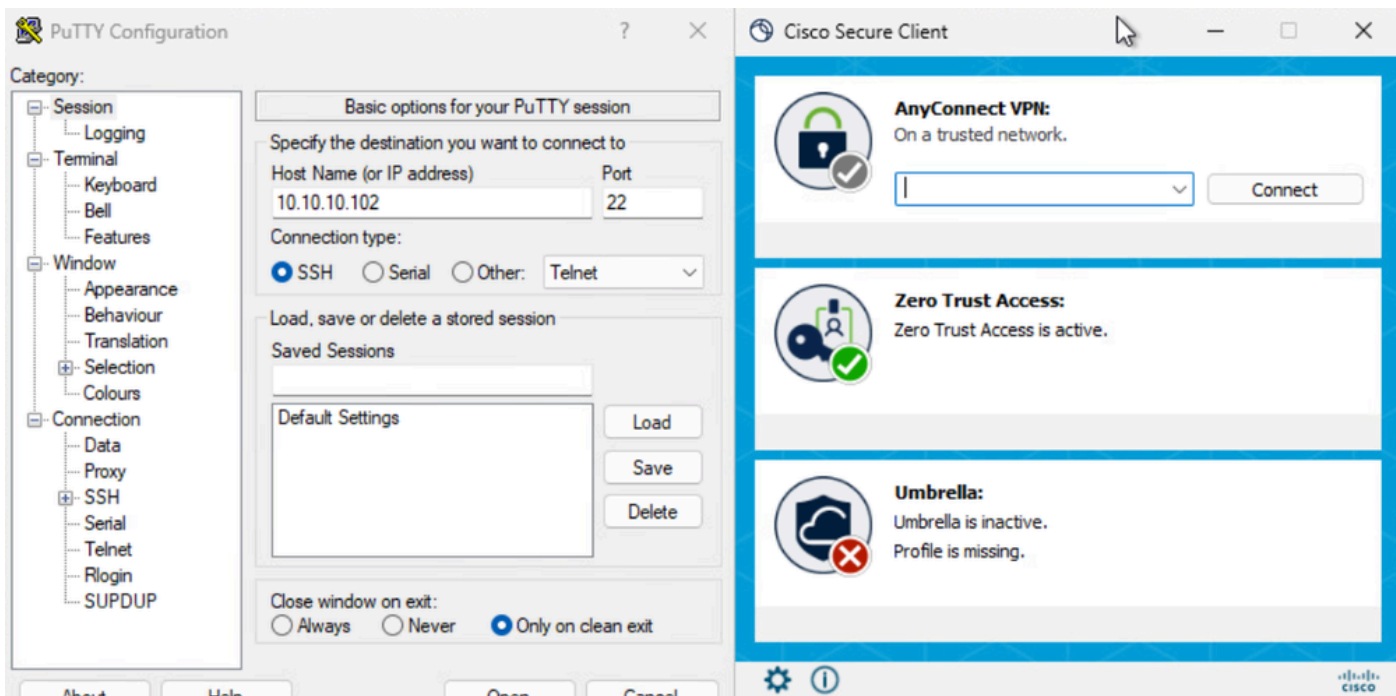


Accesso sicuro - Test PR

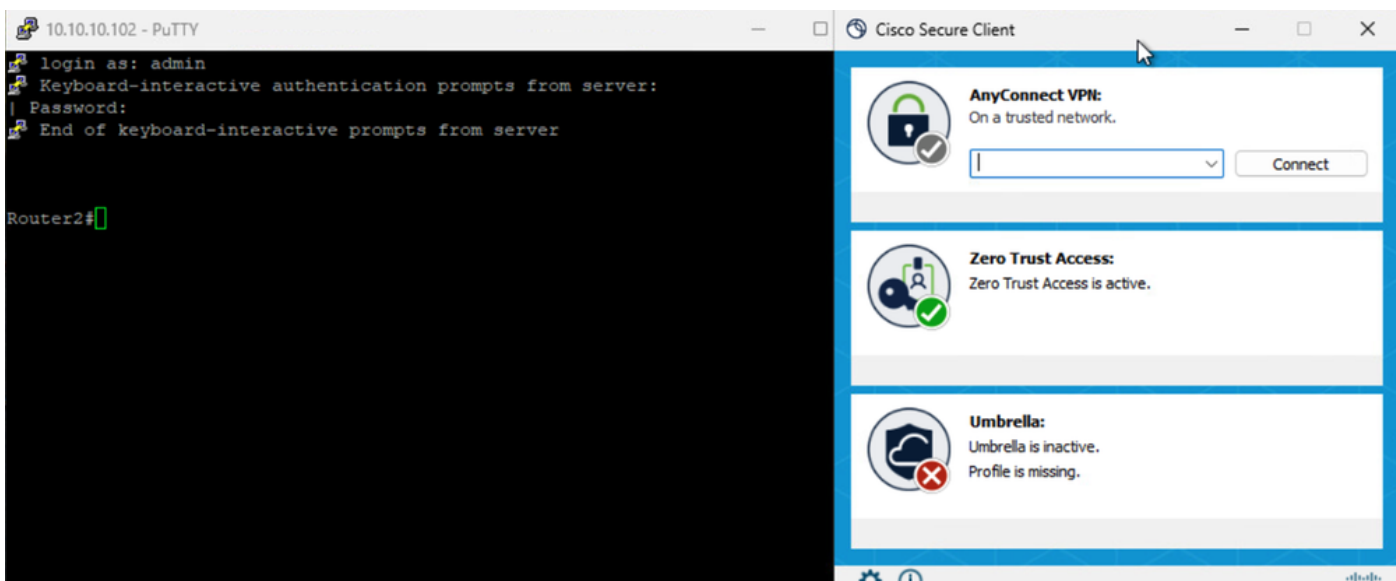


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP



Accesso sicuro - Test PR



Accesso sicuro - Test PR

5. Verifica registri di ricerca attività accesso sicuro

Activity Search

Activity Search interface showing search filters and results for domain router2.csa.local. The interface includes a search bar, filters, and a table of activity records.

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser
Allowed	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	...
Allowed	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	...
Allowed	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	...
Allowed	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	...
Allowed	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	...

Accesso sicuro - Ricerca attività

Activity Search

Activity Search interface showing search filters and results for response Allowed. The interface includes a search bar, filters, and a table of activity records. An event details panel is open on the right.

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)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.64	192.168.1.64	7680	Allowed	LAB Manager
Allowed	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

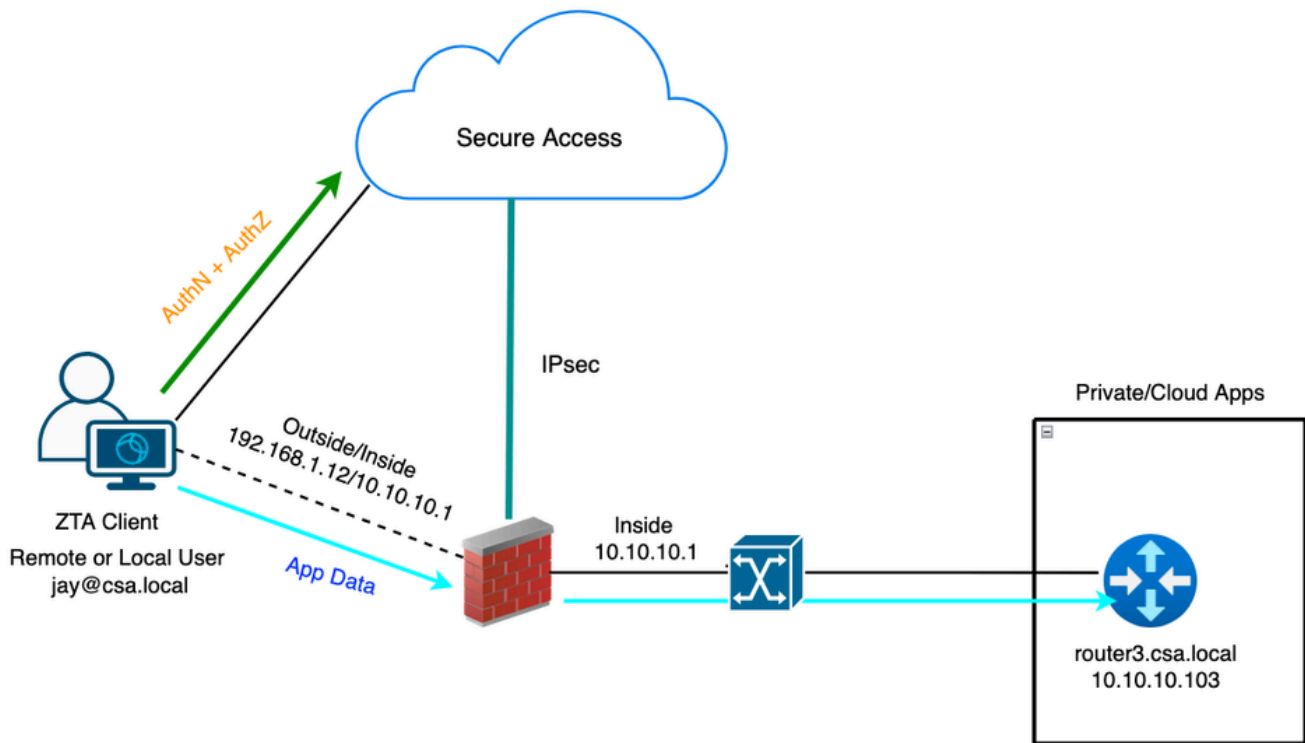
Accesso sicuro - Ricerca attività

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, and a table of activity records.

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)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow
Allowed	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
Allowed	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
Allowed	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

Accesso sicuro - Ricerca attività



Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

1. Selezionare Risorse > Destinazioni > Risorse private > Fare clic su +Aggiungi

The screenshot shows the Cisco Security Cloud Control interface. The 'Resources' section is expanded to show 'Private Resource' under 'Destinations'. A table lists 5 Private Resources with columns for Private Resource Group, Connection Method, Connector Groups, Accessed by, Rules, and Total Requests.

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

Accesso sicuro - Configurazione risorse private

2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.

← Private Resources

Add a Private Resource

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

General

Private Resource Name

Router3

Description (optional)

Router 3 for uZTNA Testing

Accesso sicuro - Configurazione risorse private

3. Inserire il nome di dominio completo (FQDN) della risorsa privata a cui si desidera accedere. È inoltre possibile definire l'indirizzo IP della risorsa privata. Per ulteriori informazioni, vedere [Aggiungere una risorsa privata](#)

4. Selezionare il server DNS per risolvere il dominio

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) ▾

Accesso sicuro - Configurazione risorse private

5. Seleziona metodi di connessione degli endpoint

6. Selezionare FTD come punti di applicazione locale

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

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

FMC_FTD (ftd.csa.local) ✓

Will get enforced at the selected firewalls.

Local-only

Enforcement point for Remote User

Remote user Secure Access Cloud Private Resource



Enforcement point for Local user

User in a trusted network Local Firewall Private Resource



Cancel

Save and Test

Save

Accesso sicuro - Configurazione risorse private

Selezionare RC se la risorsa privata è accessibile tramite RC, altrimenti lasciare vuoto se la risorsa privata è accessibile tramite gruppo di tunnel di rete (tunnel IPsec).

Resource Connector Groups

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

For more information, see [Help](#)

Resource Connector Groups (optional) ⓘ

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

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

Accesso sicuro - Configurazione risorse private



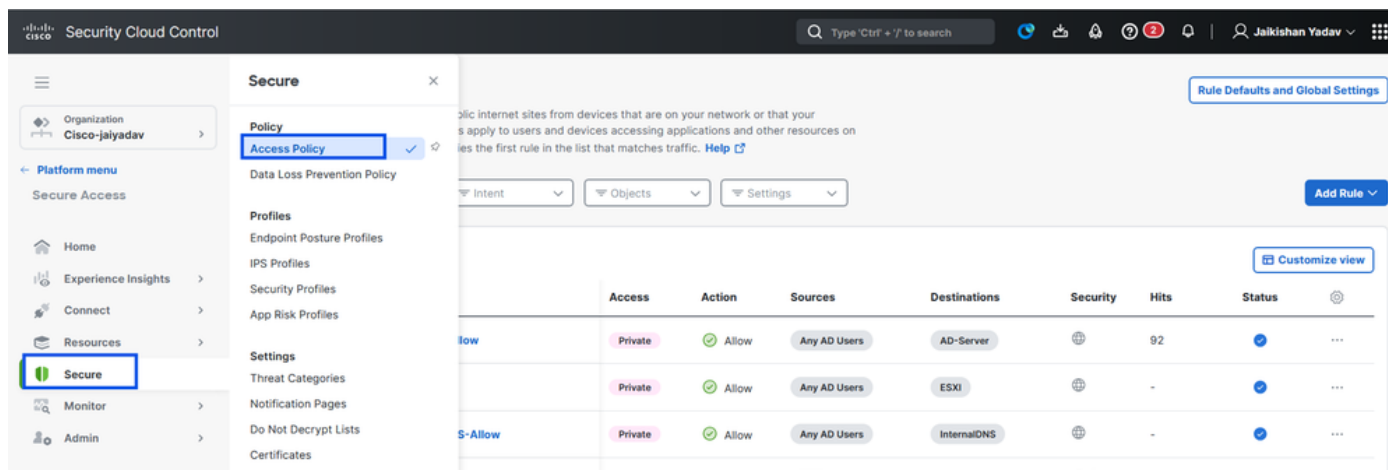
Nota: A seconda del tipo di iscrizione selezionato, questa modifica assocerà automaticamente la prenotazione permanente all'FTD e attiverà una distribuzione di criteri

7. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere [Regola di accesso privato](#)

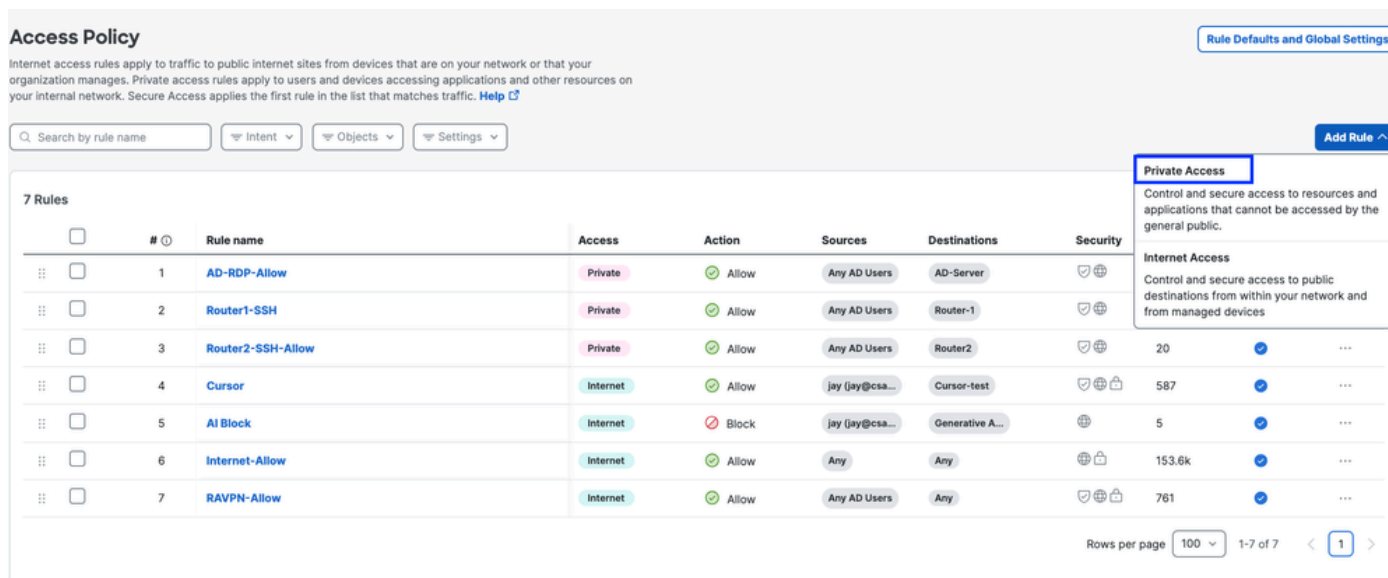
1. Passare a Protezione > Criteri di accesso



Accesso sicuro - Configurazione criteri di accesso

2. Fare clic su Aggiungi regola, quindi scegliere Accesso privato.

Nella parte superiore della regola è disponibile un riepilogo che descrive i componenti configurati della regola.



Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola

Add Router3-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Accesso sicuro - Configurazione criteri di accesso

4. Selezionare l'azione della regola e selezionare origine e destinazione

Rule name Rule order

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From To

+ AND

Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint

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](#)

Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione

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](#)

Accesso sicuro - Configurazione criteri di accesso

7. Fare clic su Save (Salva)

Access Policy Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings Add Rule

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

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

Accesso sicuro - Configurazione criteri di accesso

Fase 3 - Verifica dell'associazione di PR sull'FTD

1. Passare a connessione > Connessioni di rete > FTD

The screenshot shows the Cisco Security Cloud Control interface. On the left, the 'Connect' menu is expanded, highlighting 'Network Connections'. The main content area shows a 'Network Connections' section with a 'FTDs' tab selected. A summary card displays '0 Warning' and '1 Connected'. Below this, there are filters for 'Region' and 'Status', and a '+ Add' button.

Accesso sicuro - Verifica PR

2. Fare clic su FTD > Visualizza risorse associate a questo FTD

```

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

```

Accesso sicuro - Verifica PR

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Syncing
●

0 Synced
●

FTDs configured for Universal Zero Trust Access

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

Configuration changes are being processed

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

FMC Name

Configuration status

1 FTDs

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

FMC_FTD ✕

Firewall Details ^

Device FQDN: ftd.csa.local 🔗

Auto deployment: Yes

UZTA Configuration status ^

● Syncing

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

Assigned Trusted Network ^

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

Edit assignment
+ Trusted network

Associated Resources 3 ^

RESOURCES ASSOCIATED BY STATUS

Status	Count
● Synced	3

View resources associated to this FTD

Associate Resources

Accesso sicuro - Verifica PR

```
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
```

Accesso sicuro - Verifica PR

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

Accesso sicuro - Verifica PR

- 3. Fare clic su chiudi
- 4. Verificare che lo stato , la risorsa associata e la configurazione siano sincronizzati

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)
 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

Accesso sicuro - Verifica PR

5. Verificare che la configurazione sia stata sottoposta a PUSH in FTD

Accedere alla cli FTD e passare alla modalità LINA

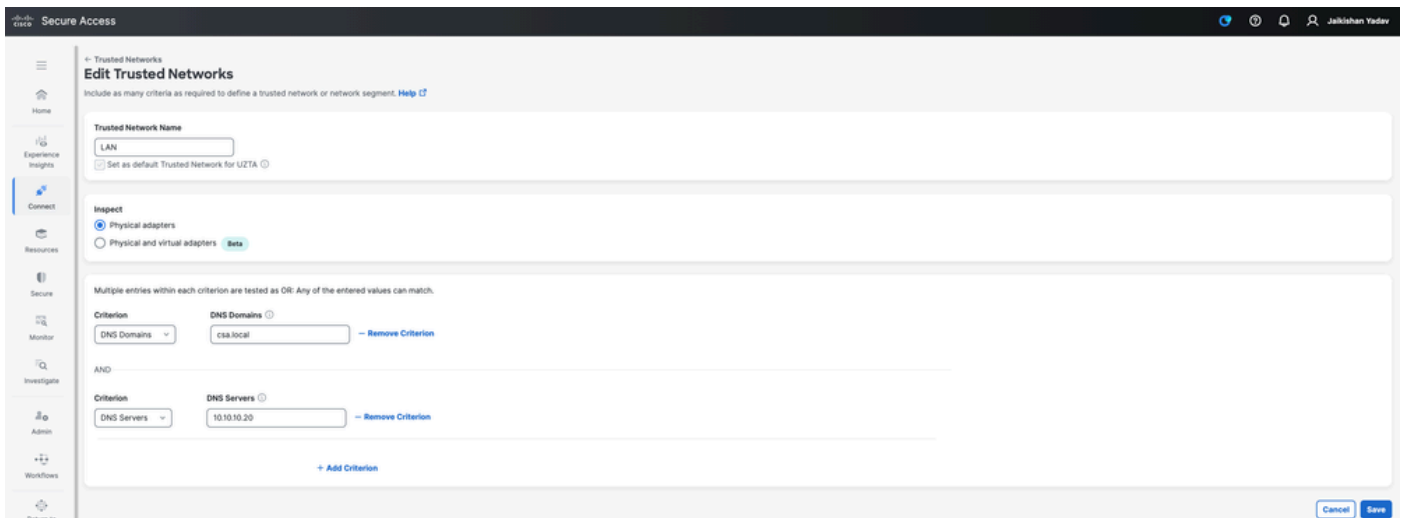
show running-config applicazione oggetto

```
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
```

Accesso sicuro - Verifica PR

Passaggio 4: Configurare o verificare " Gestire reti attendibili o impostazioni ZTA"

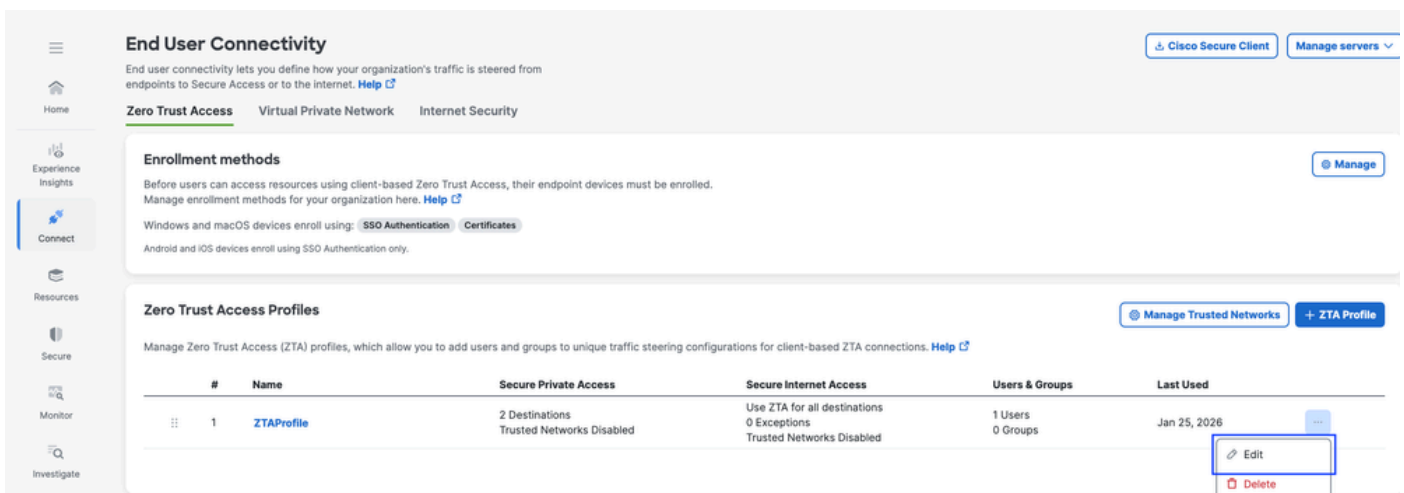
Selezionare Connetti > Connettività utente finale > Accesso con attendibilità totale > Impostazioni ZTA e configurare Reti attendibili



Accesso sicuro - Configurazione TND ZTA

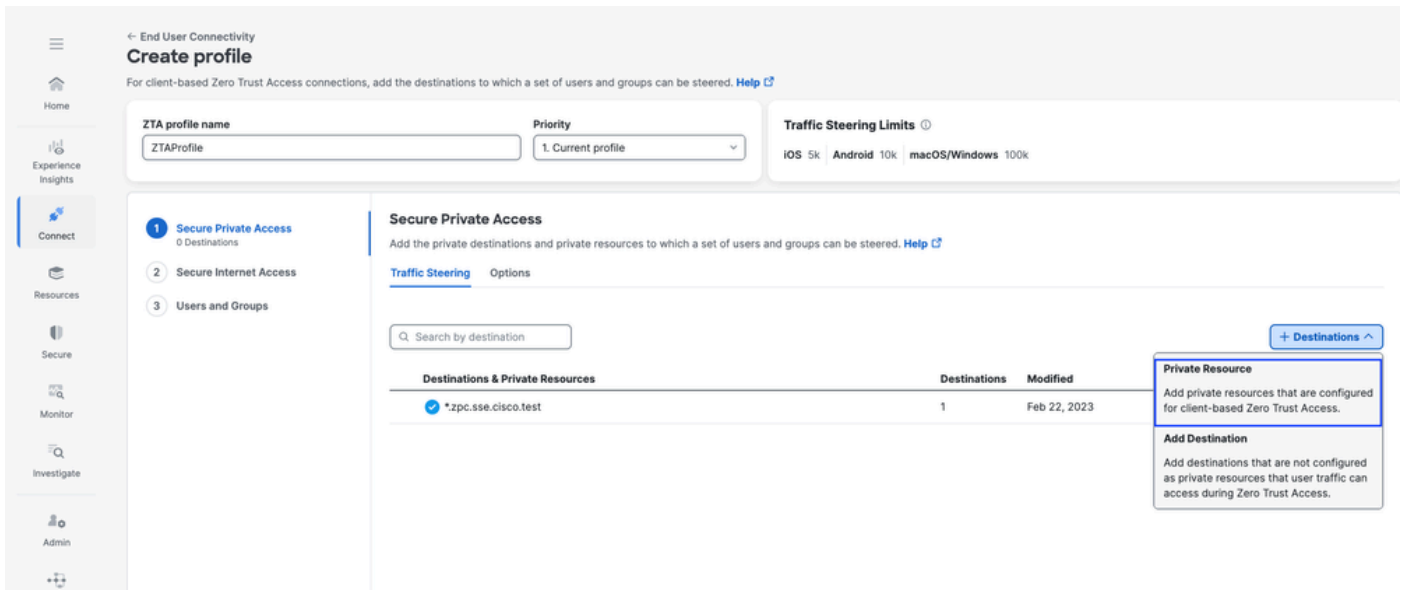
Fase - 5 Aggiungere una risorsa privata al profilo ZTA

1. Selezionare Connetti > End User Connectivity > Zero Trust Access e fare clic su 3 punti per modificare il profilo ZTA

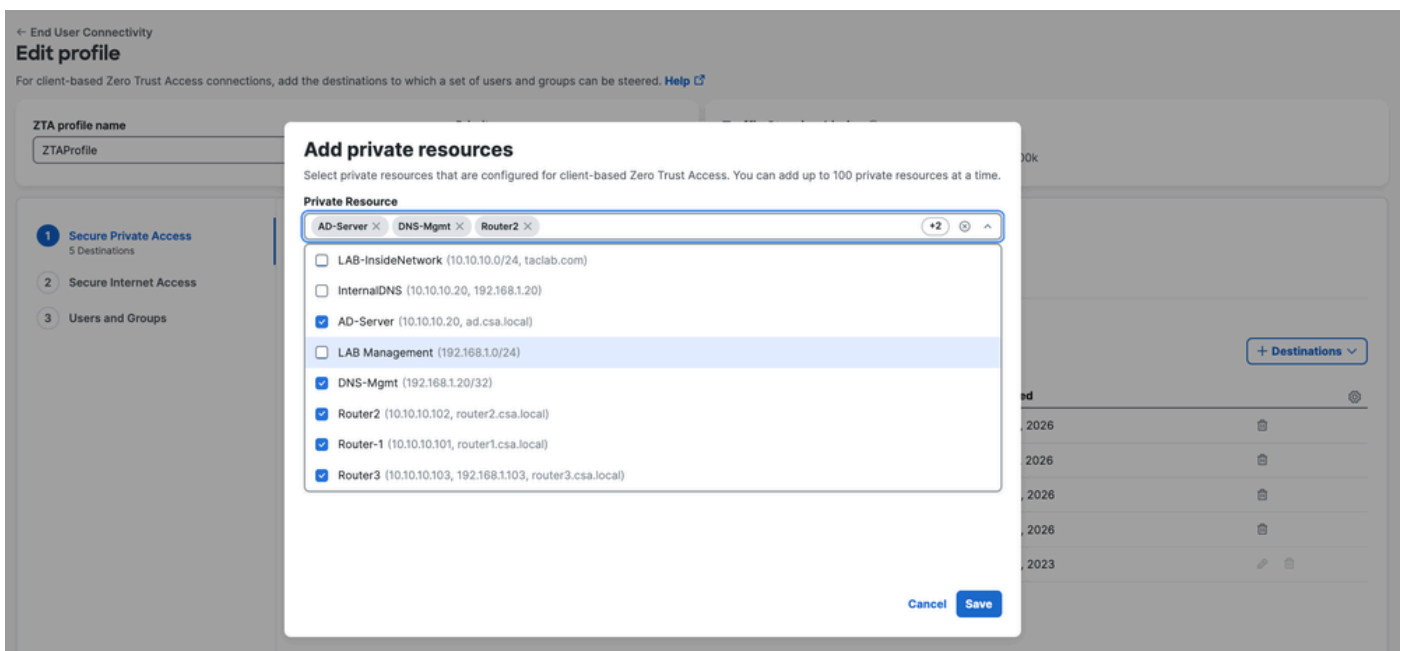


Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

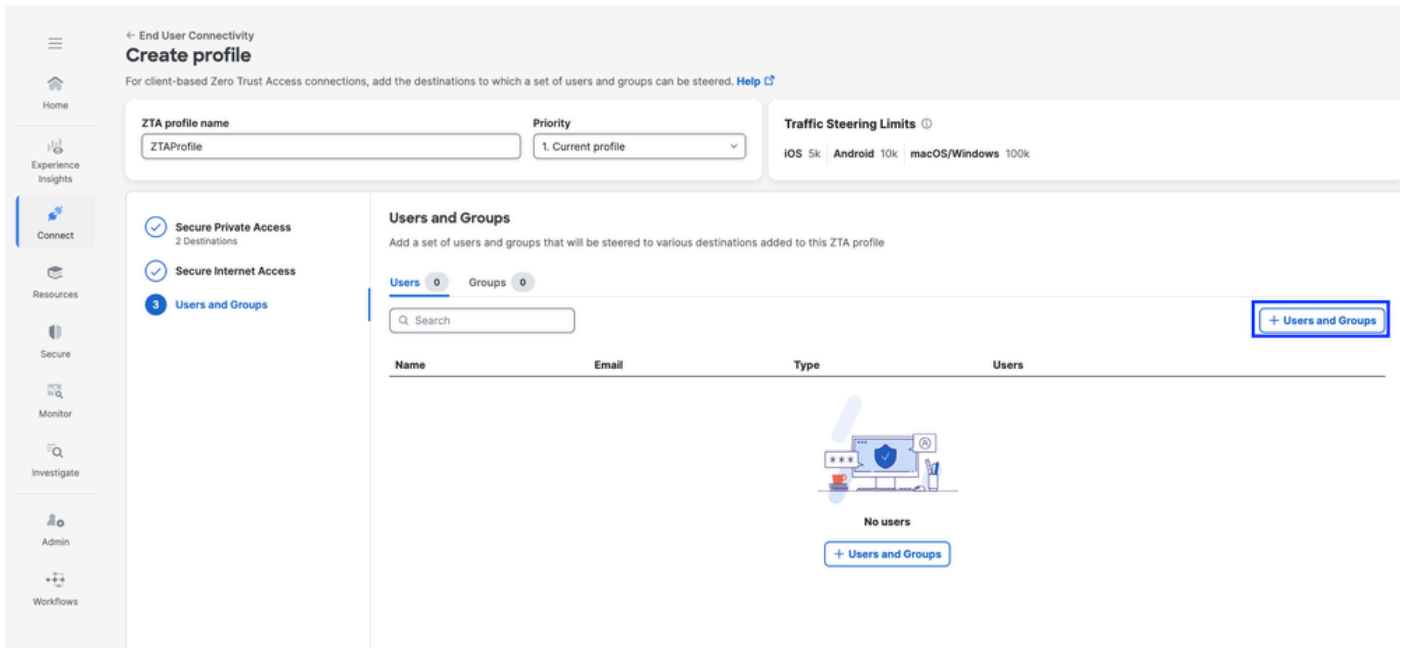


Accesso sicuro - Profilo ZTA

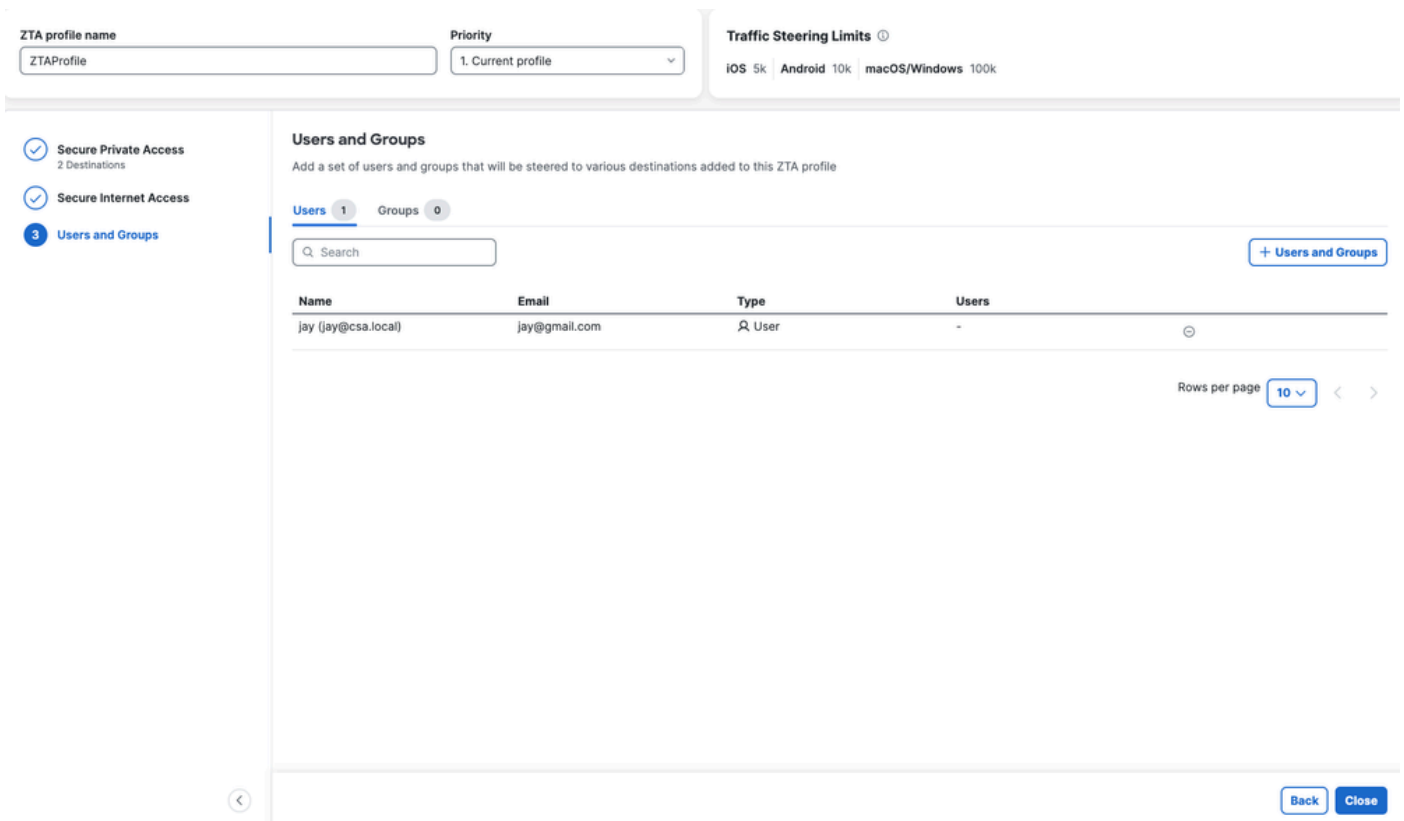


Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi



Accesso sicuro - Profilo ZTA

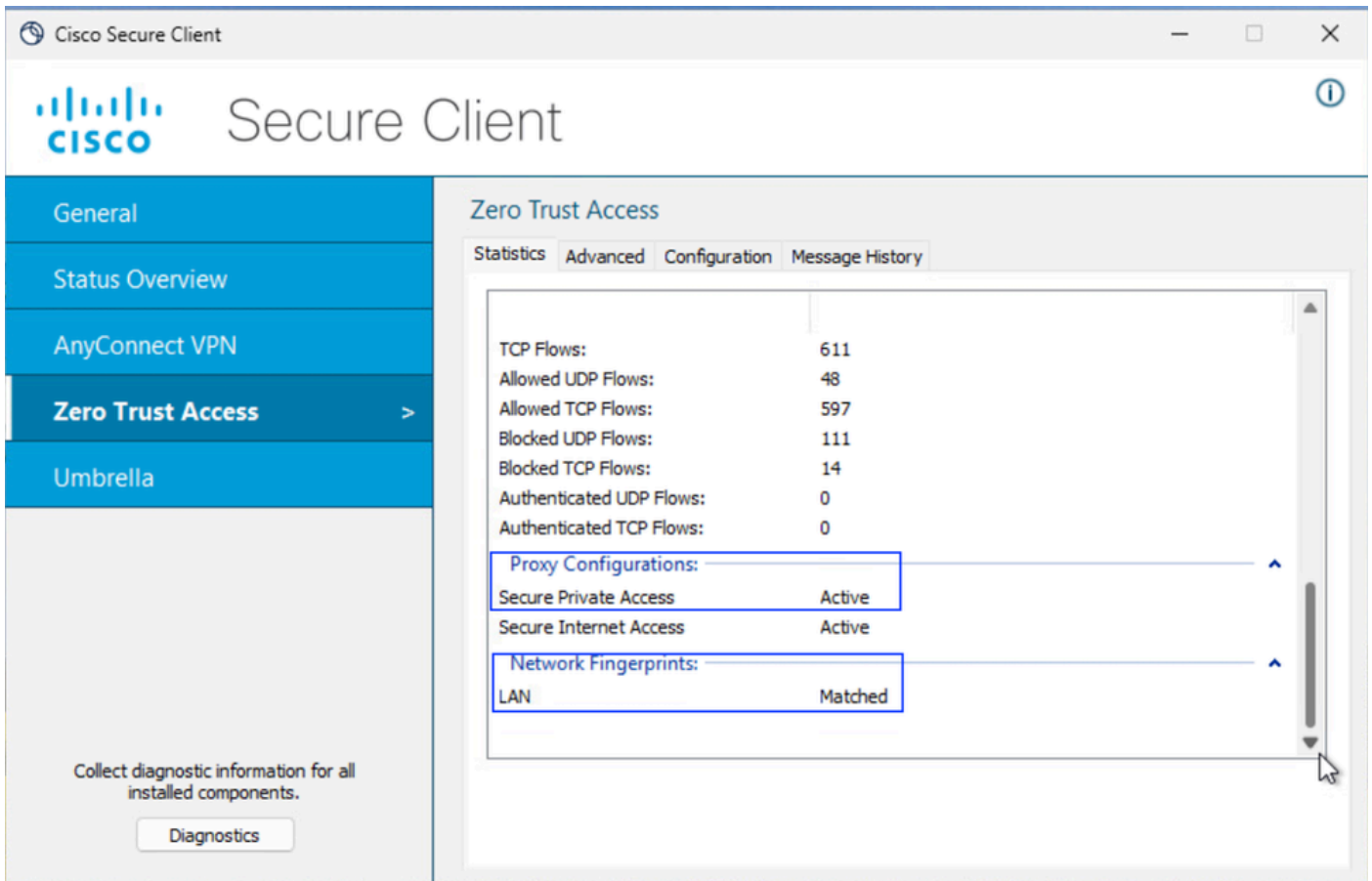


Accesso sicuro - Profilo ZTA

Fase - 6 Verifica dell'accesso alla risorsa privata

Quando l'utente è locale

1. Verificare l'impronta digitale di rete per ZTA TND. Deve corrispondere se l'utente è locale e se Accesso privato sicuro deve essere attivo



Accesso sicuro - Test PR

2. Verificare che l'utente remoto sia in grado di risolvere il nome di dominio completo FTD

```
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
```

Accesso sicuro - Test PR

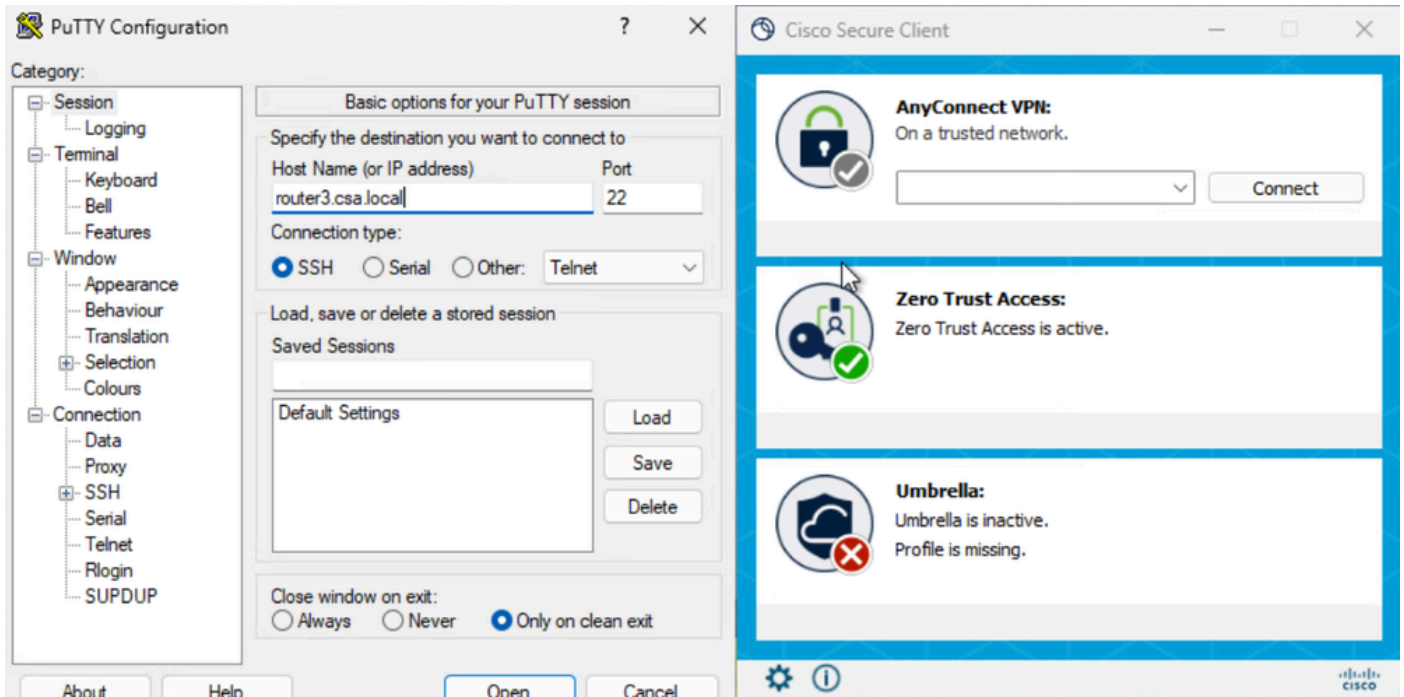
3. Verificare che l'FTD possa raggiungere la risorsa privata utilizzando l'FQDN

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

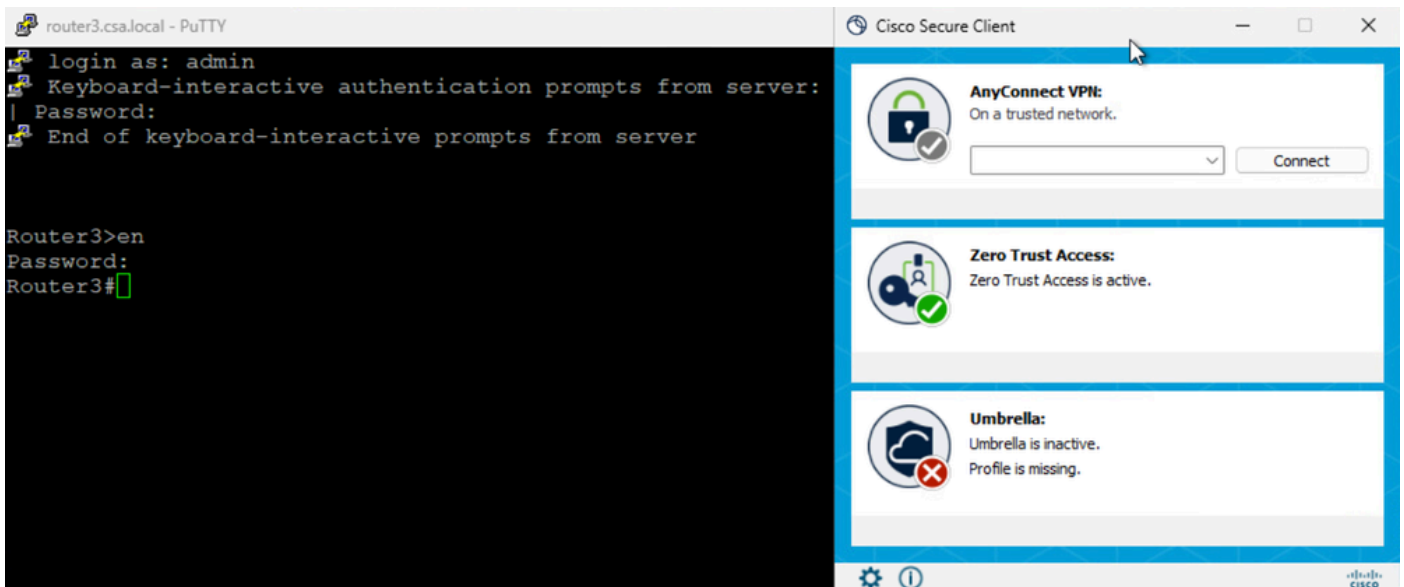
Accesso sicuro - Test PR

4. Eseguire il test della connessione SSH alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN

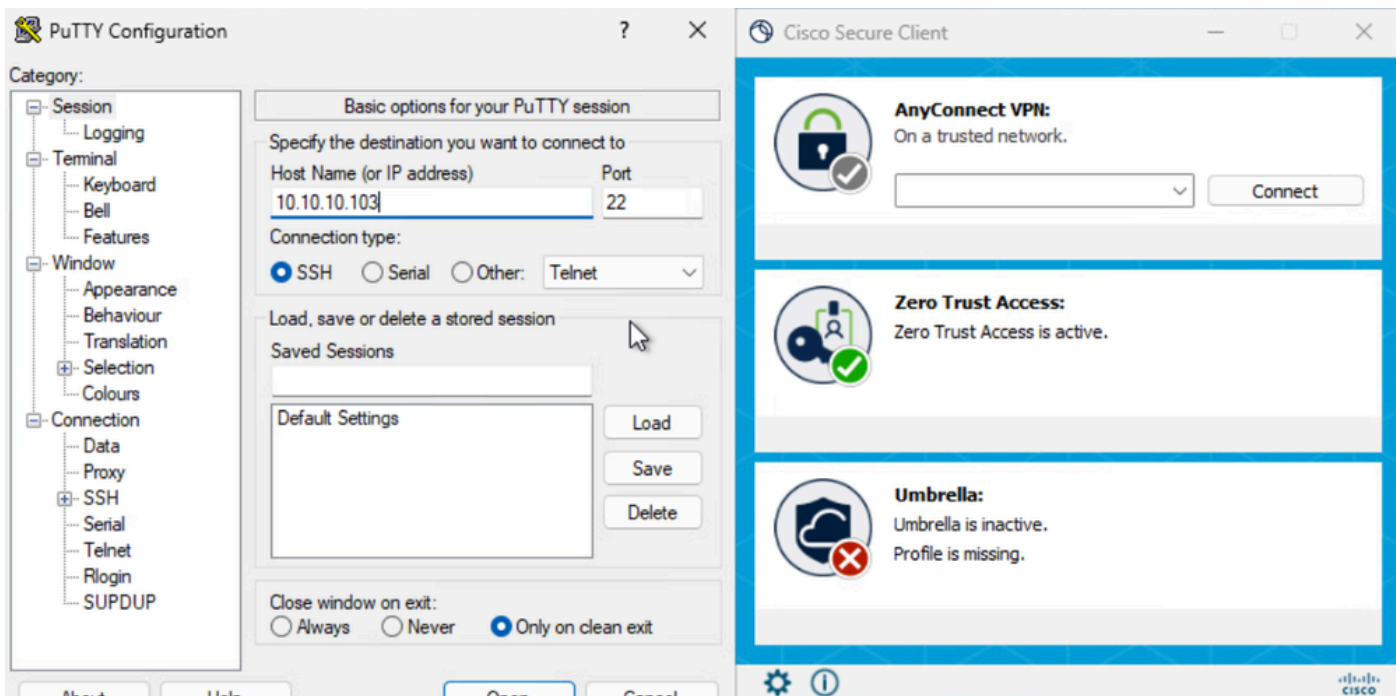


Accesso sicuro - Test PR

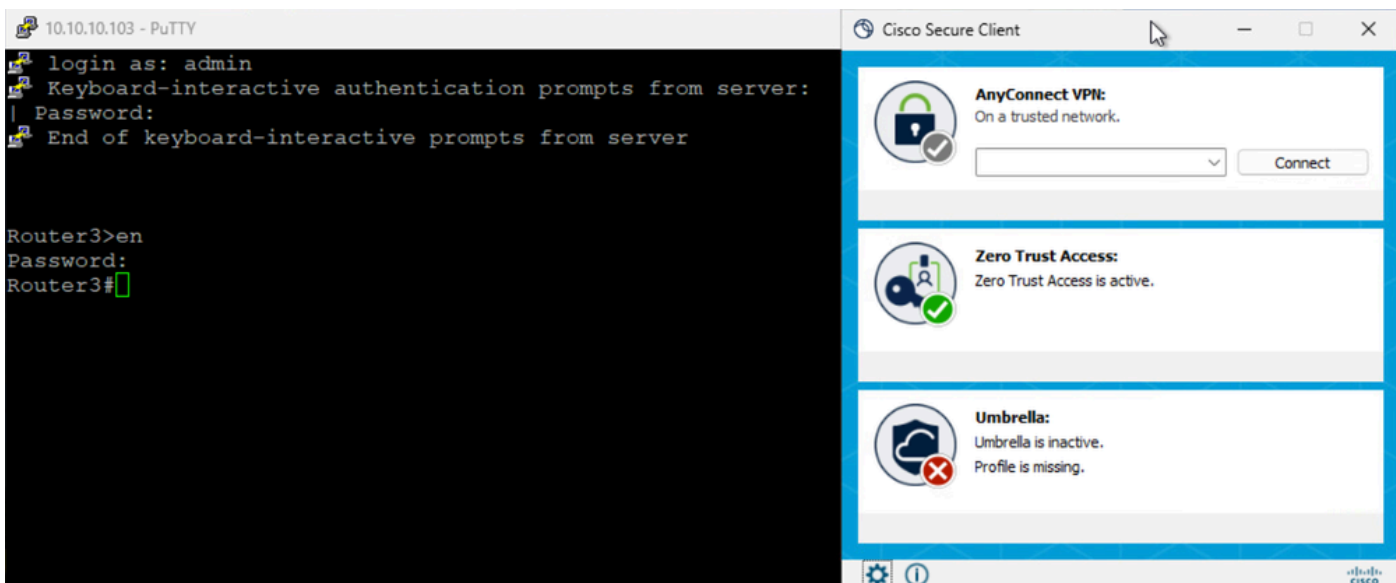


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP



Accesso sicuro - Test PR



Accesso sicuro - Test PR

5. Verifica registri di ricerca attività accesso sicuro

Activity Search

Search by domain, identity, or URL Advanced CLEAR

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

Accesso sicuro - Ricerca attività

Activity Search

Search by domain, identity, or URL Advanced CLEAR

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
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

Accesso sicuro - Ricerca attività

6. Verificare gli eventi di connessione FMC

Firewall Management Center

Events & Logs / Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Destination IP: 10.10.10.103

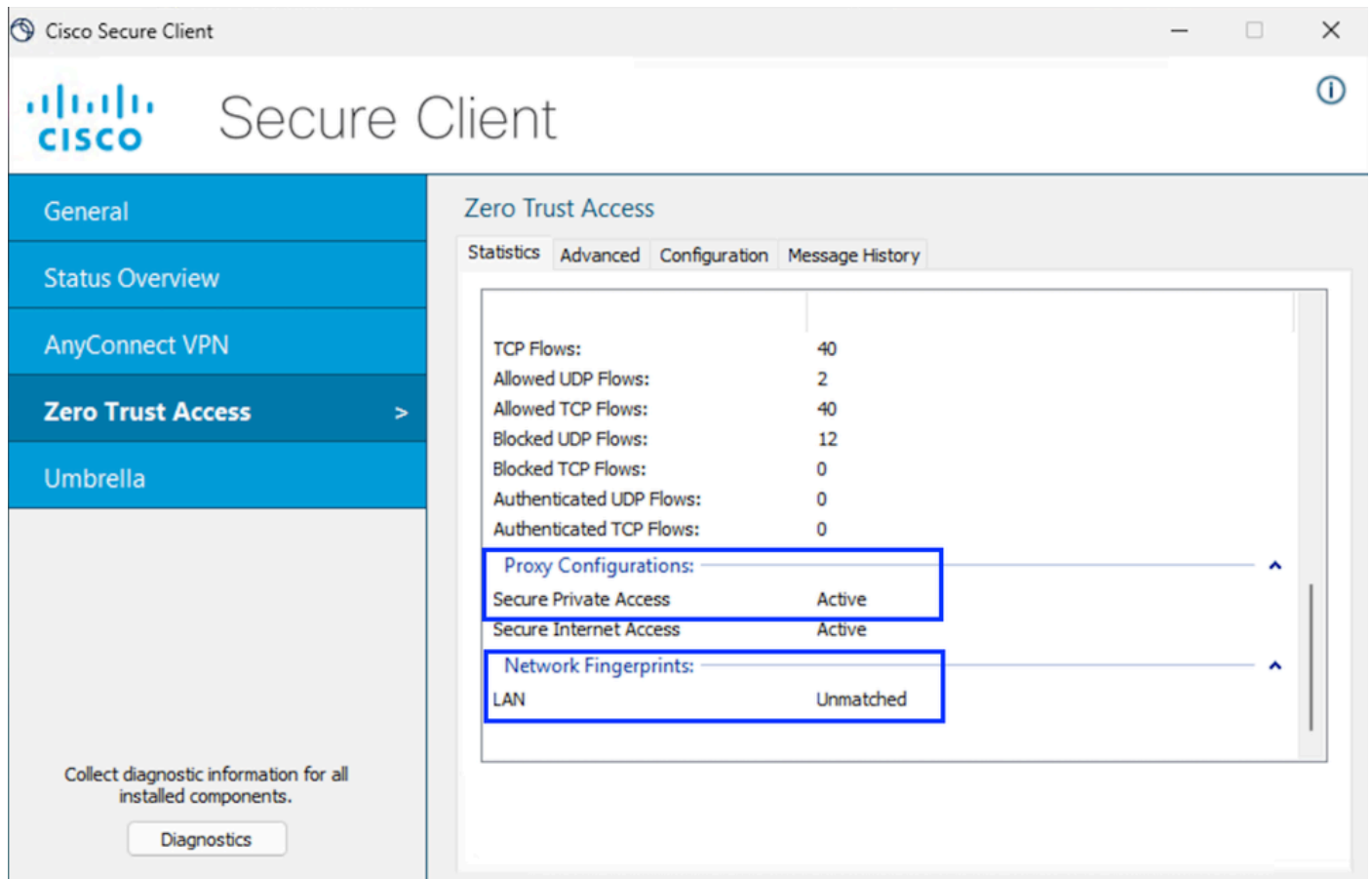
4 events

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		

Eventi connessione FMC

Quando l'utente è remoto

1. Verificare l'impronta digitale di rete per ZTA TND, dovrebbe non corrispondere se l'utente è remoto



Accesso sicuro - Test PR

2. Verificare che l'utente remoto sia in grado di risolvere il nome di dominio completo FTD

```

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

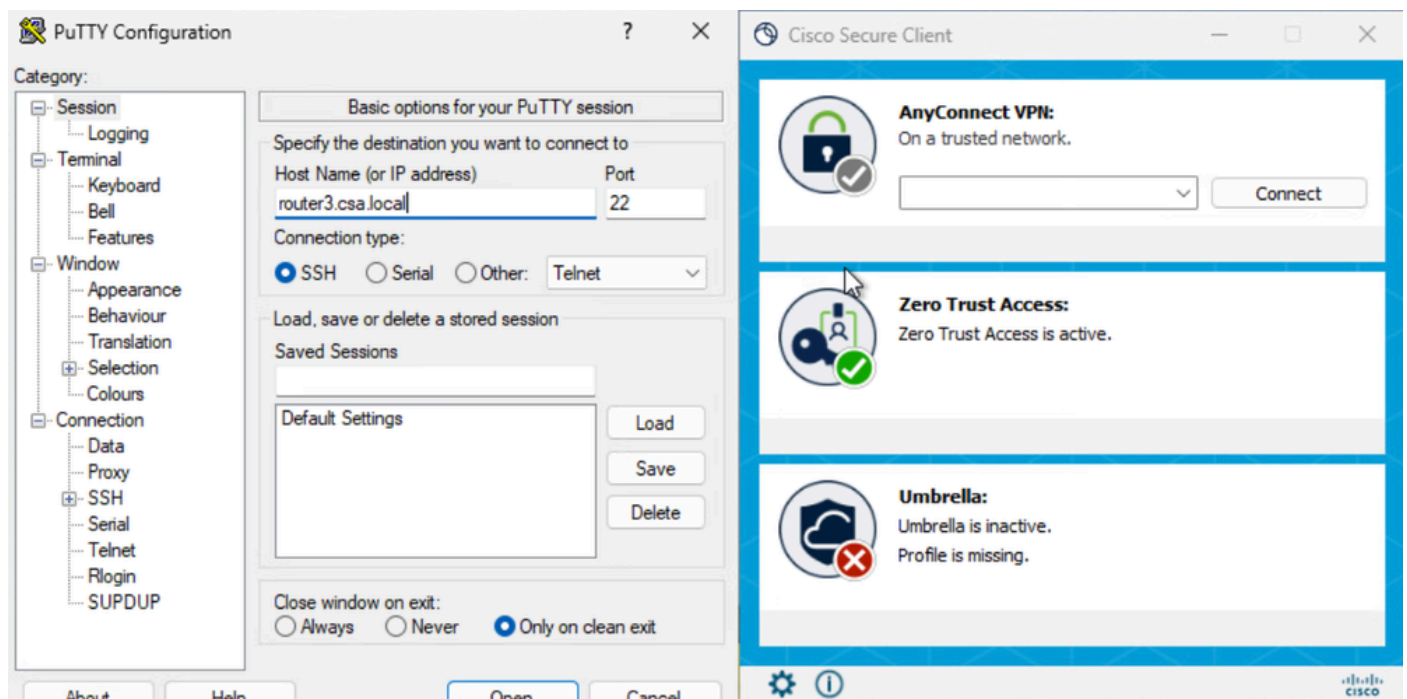
Name: ftd.csa.local
Addresses: 192.168.1.12

```

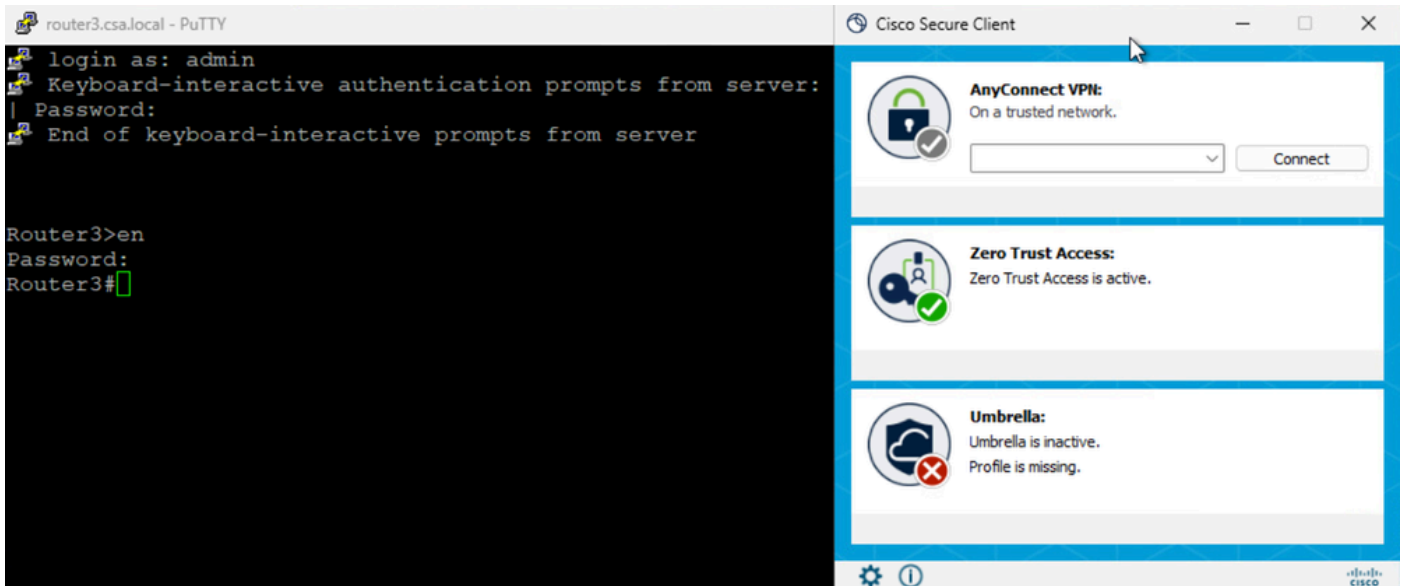
Accesso sicuro - Test PR

3. Eseguire il test della connessione SSH alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN

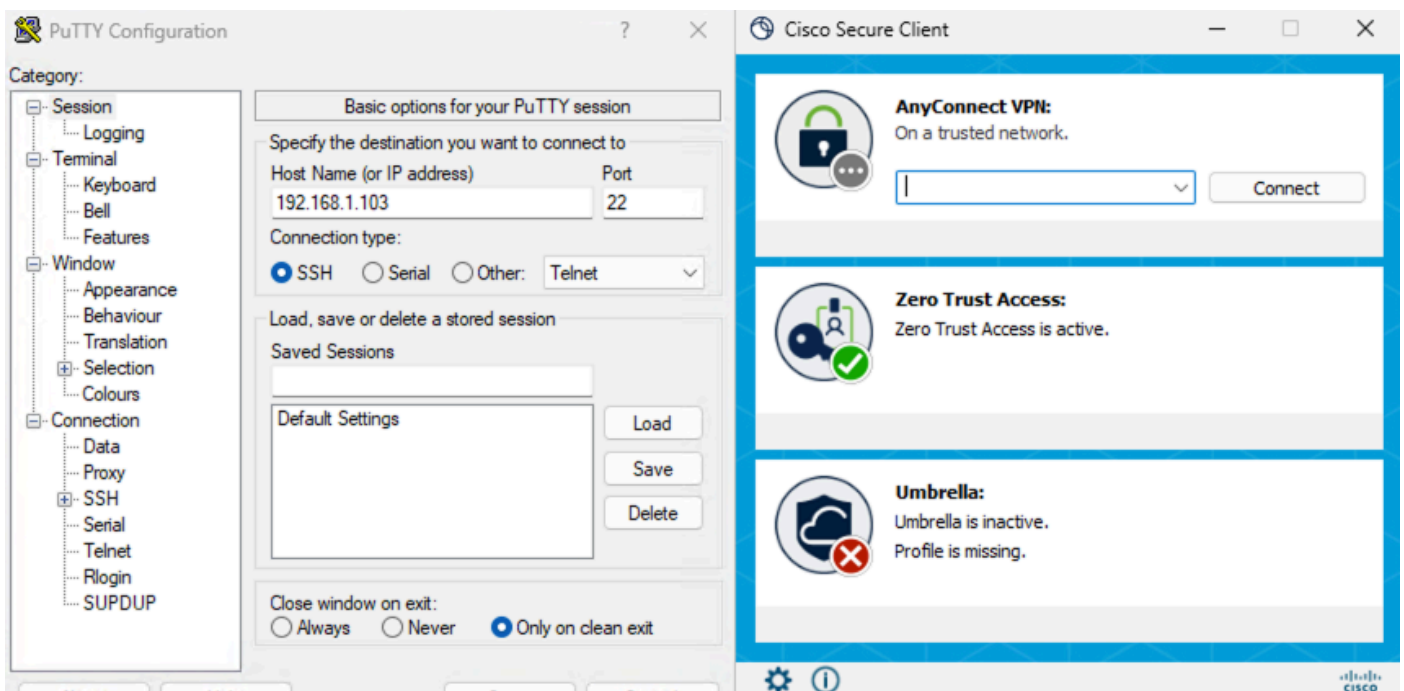


Accesso sicuro - Test PR

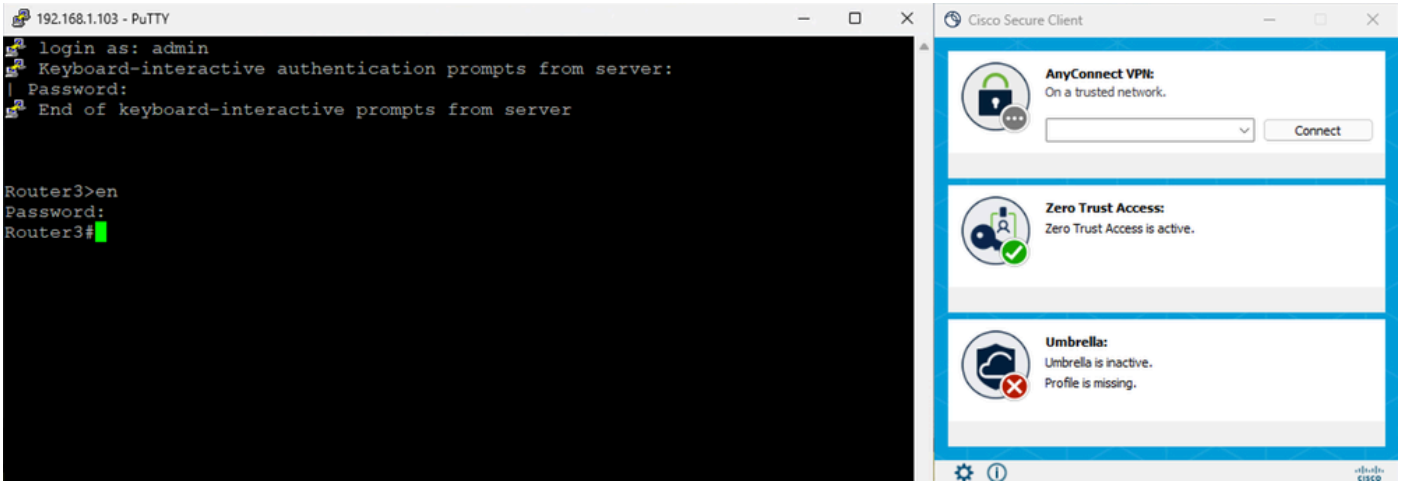


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP



Accesso sicuro - Test PR



Accesso sicuro - Test PR

5. Verifica registri di ricerca attività accesso sicuro

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

Accesso sicuro - Ricerca attività

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

Risoluzione dei problemi

Comandi utili:

```
> show allocate-core profile
> show asp inspect-dp snort
> sh running-config universal-zero-trust
> show interface ip brief
```

```
> debug universal-zero-trust zproxy 7
```

! quindi passare alla modalità esperto

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

```
# show conn all
```

```
# show nat detail
```

```
# show asp table socket
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).