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

Sommario

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

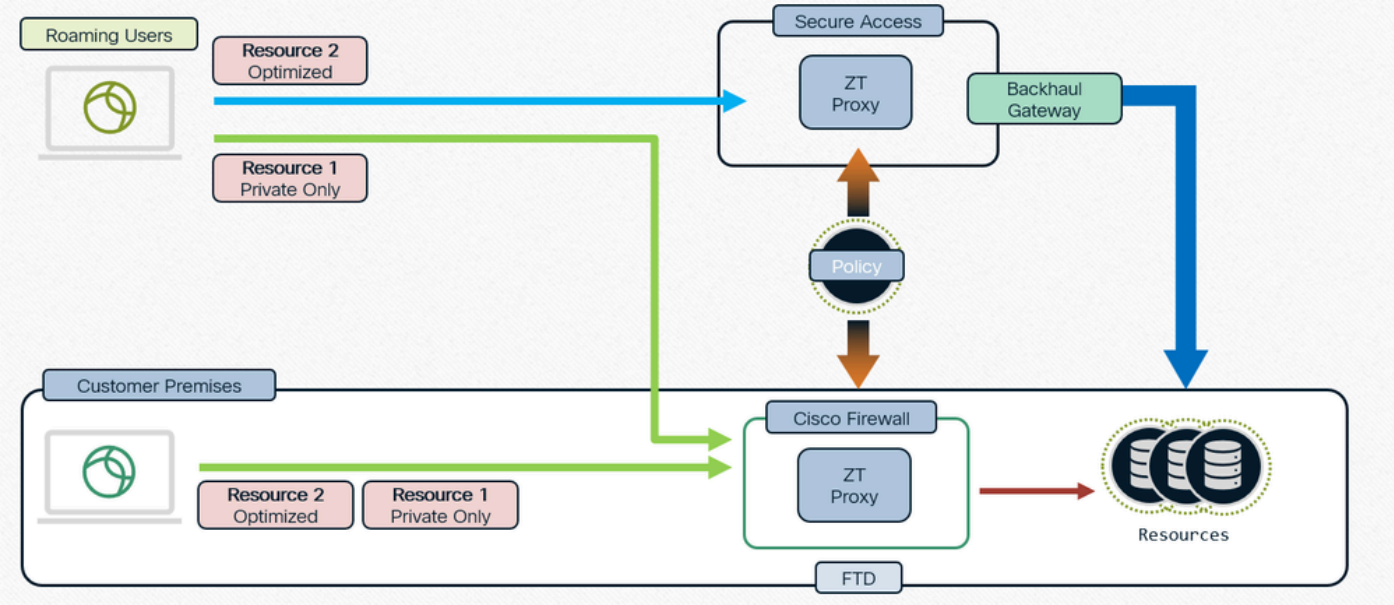
L'accesso universale alla rete senza attendibilità totale (uZTNA, Universal Zero Trust Network

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.

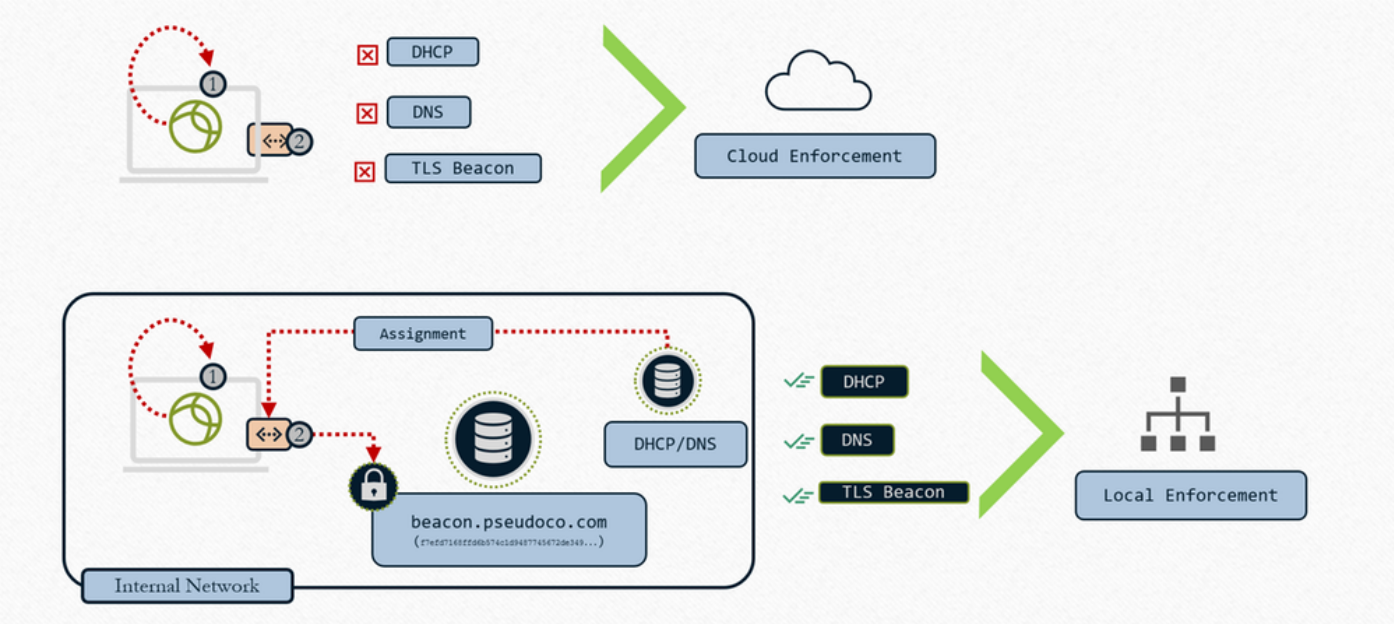
Il proxy del traffico, così come l'applicazione di IPS, file e policy antimalware, viene eseguito su Firepower Threat Defense (FTD).



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

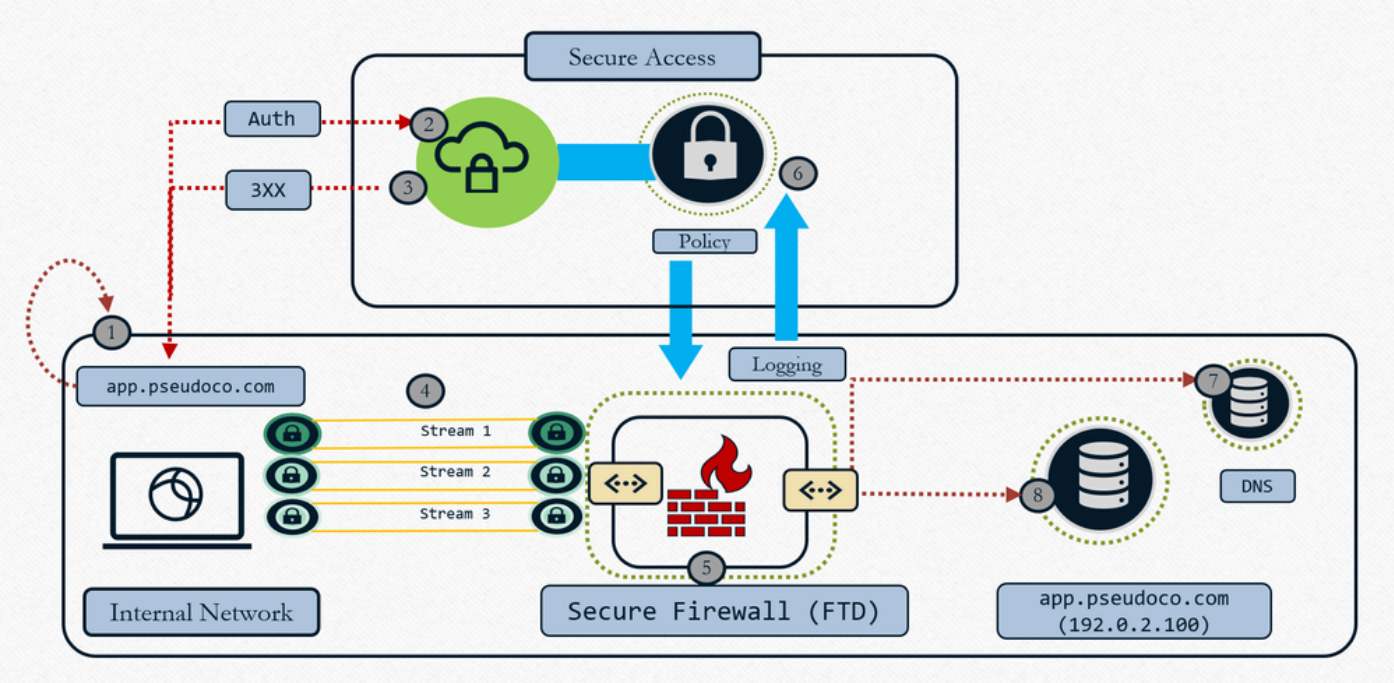
3- Se la condizione corrisponde - Applicazione locale

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

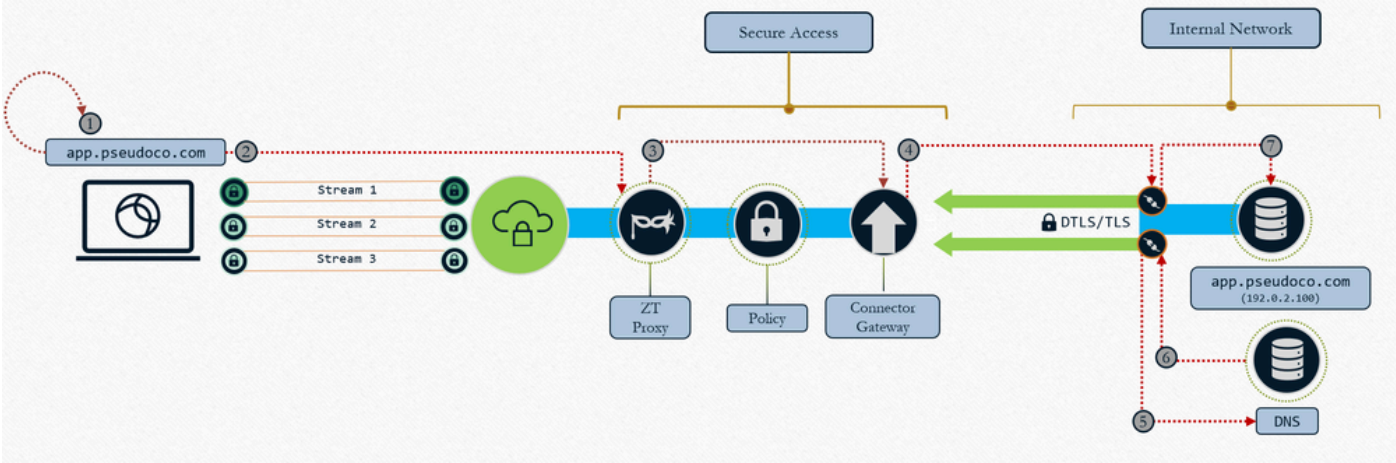
- Percorso di imposizione locale: Applicazione del firewall



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

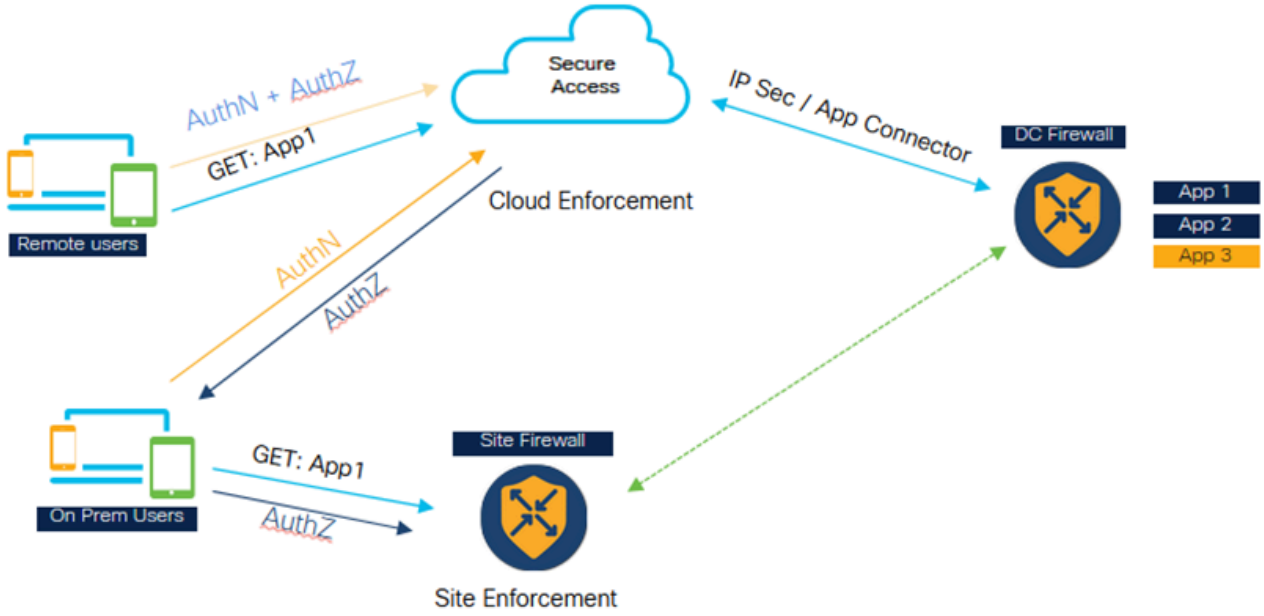


ZTNA universale : Applicazione tramite cloud

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

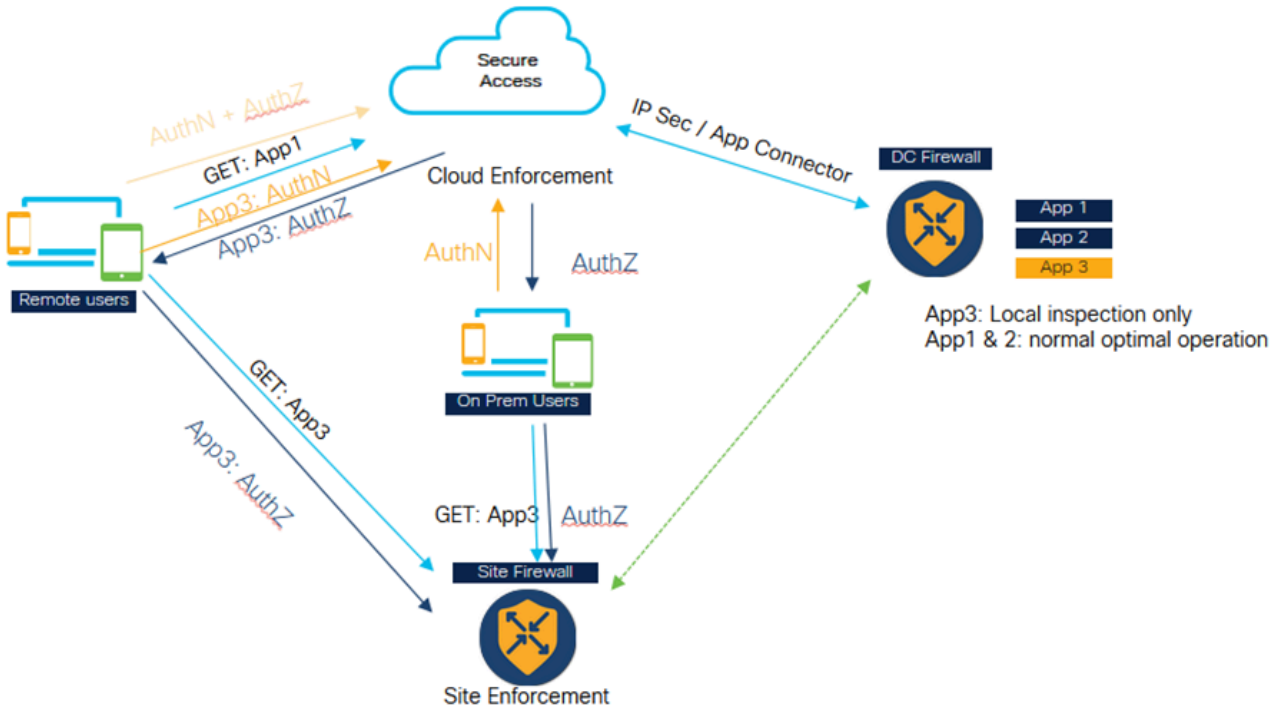
Caso 1: ZTNA coerente e ottimizzata per gli utenti in sede



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

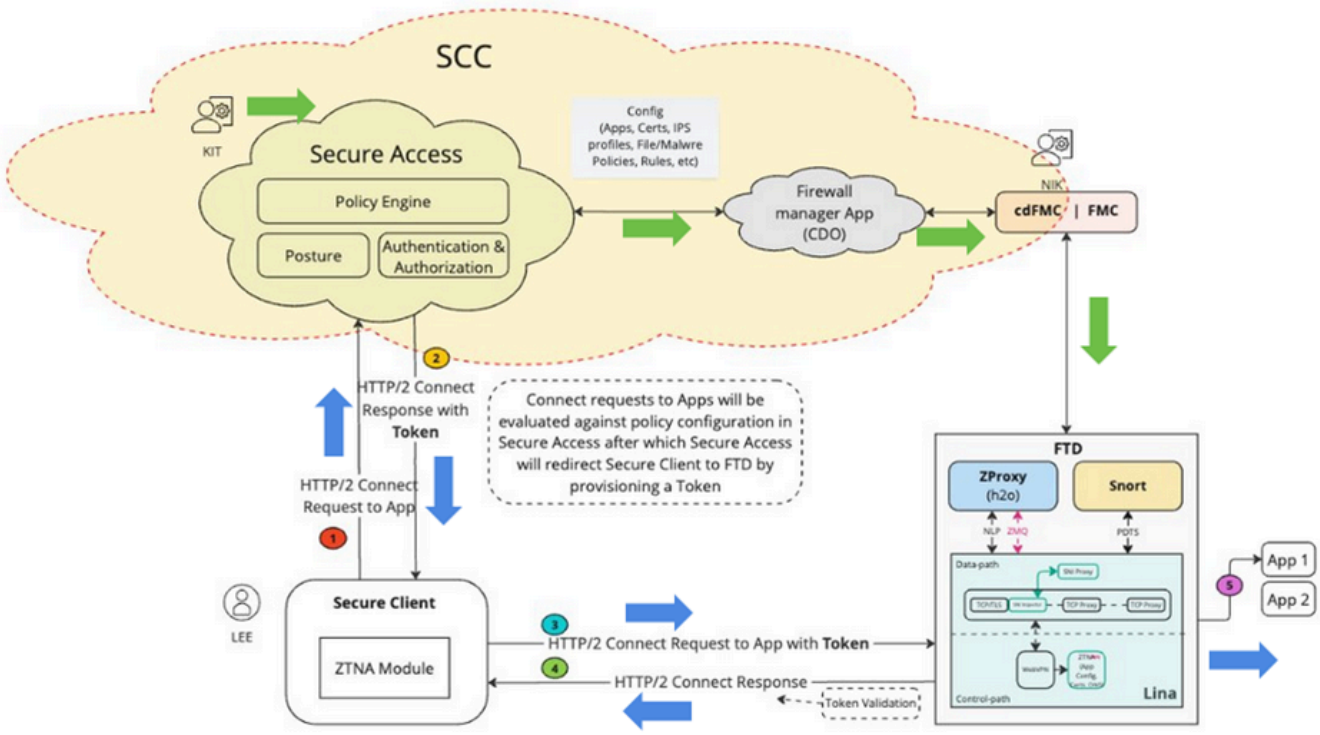
Caso 2: ispezione privata per applicazioni sensibili



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

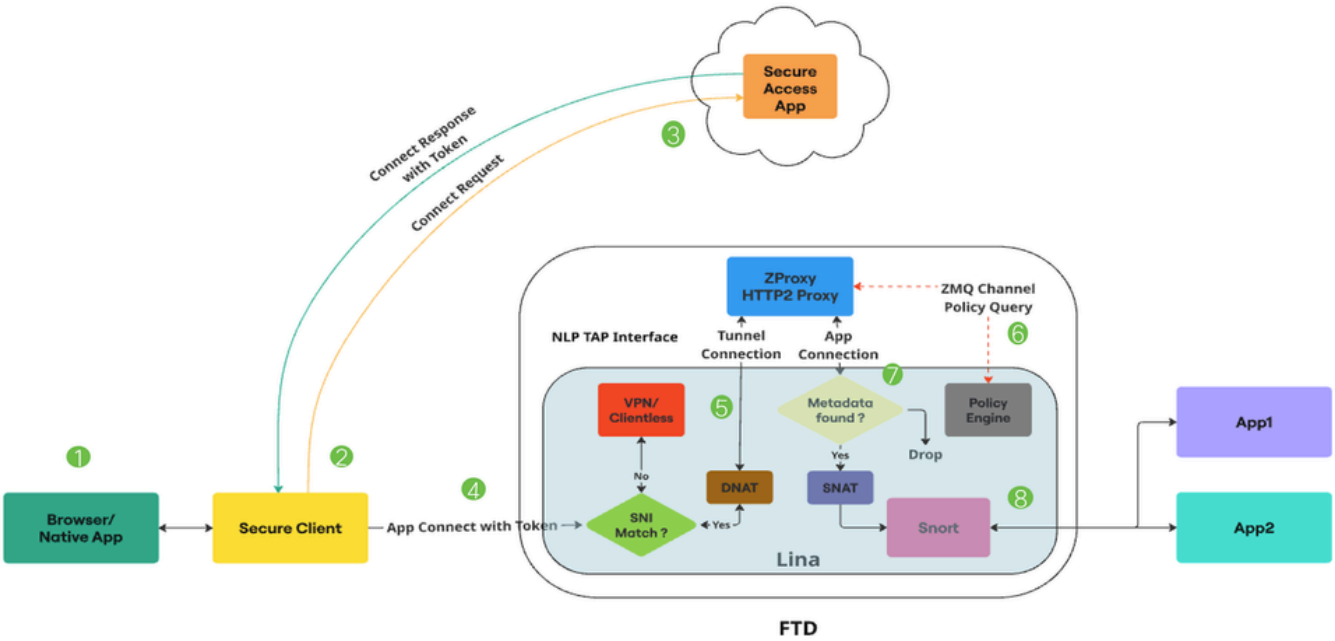
3. Secure Access reindirizza il client sicuro verso FTD insieme al token di autenticazione.

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

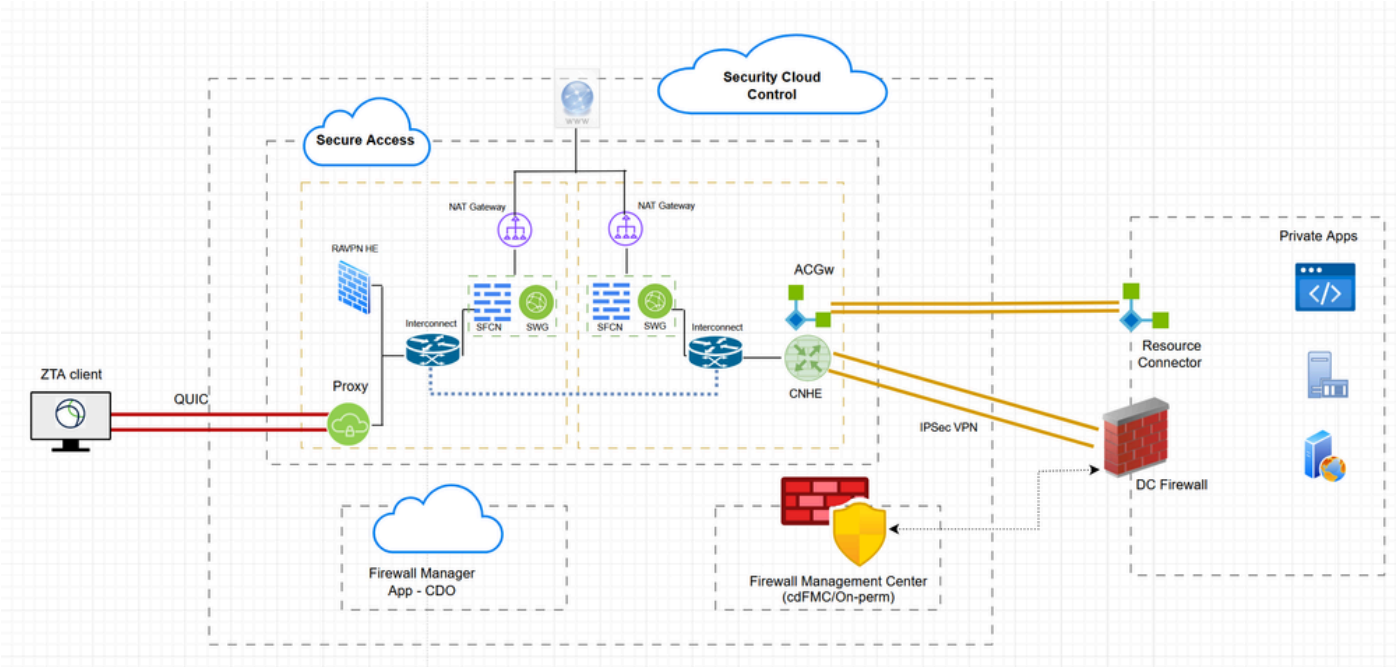
8. Poiché la connessione dell'app ha origine da ZProxy, avrà un IP interno (esempio:169.251.1.2) come IP di origine. Il messaggio verrà convertito nell'indirizzo IP dell'interfaccia di uscita FTD prima dell'invio. Lina contrassegna quindi i flussi Universal Zero Trust per l'ispezione Snort solo se nel 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



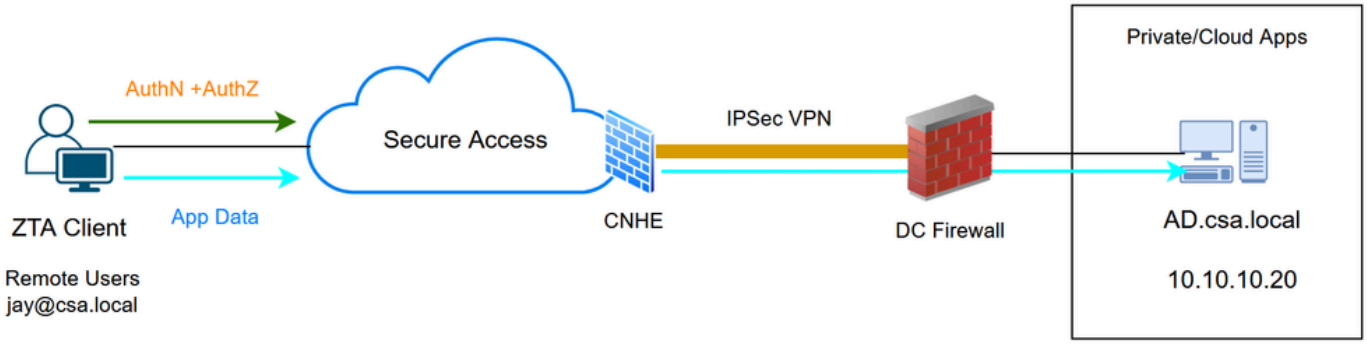
Hybrid ZTNA - Esempio di rete

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

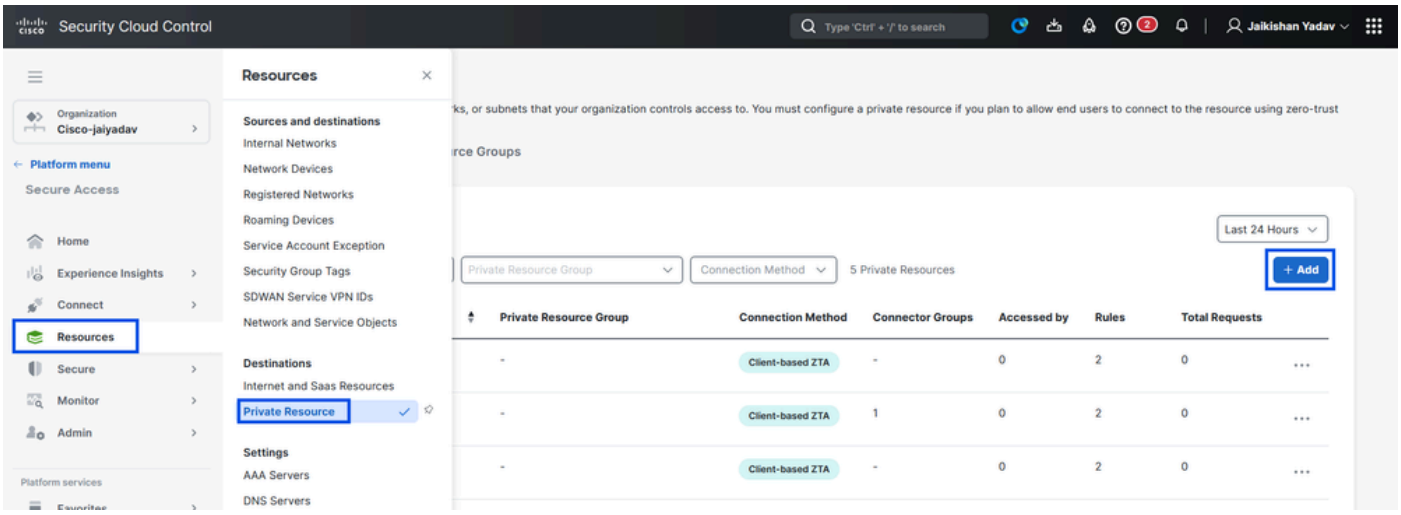


Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

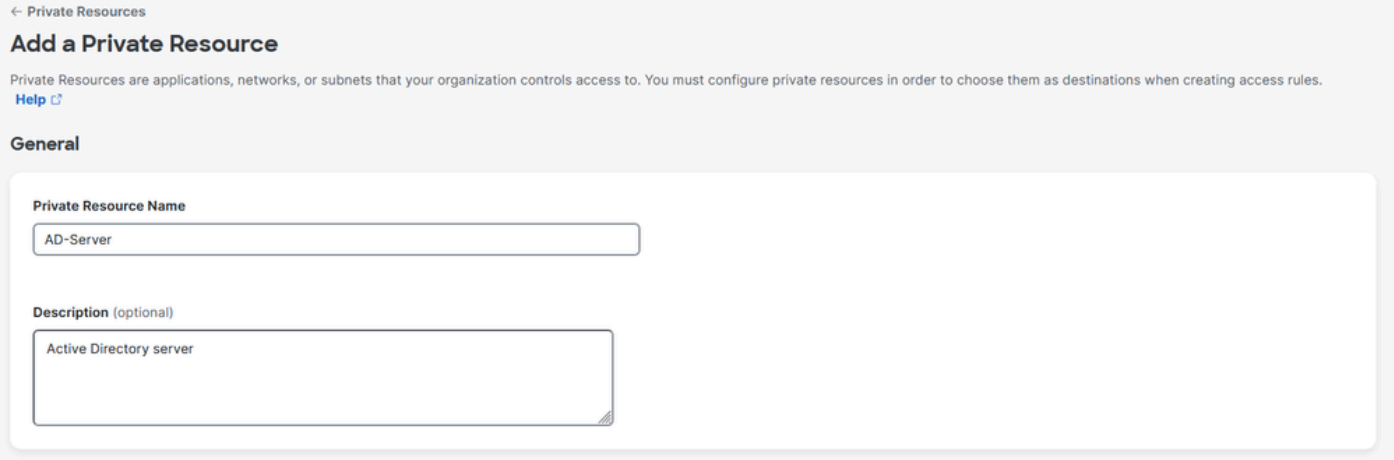
Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

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



Accesso sicuro - Configurazione risorse private

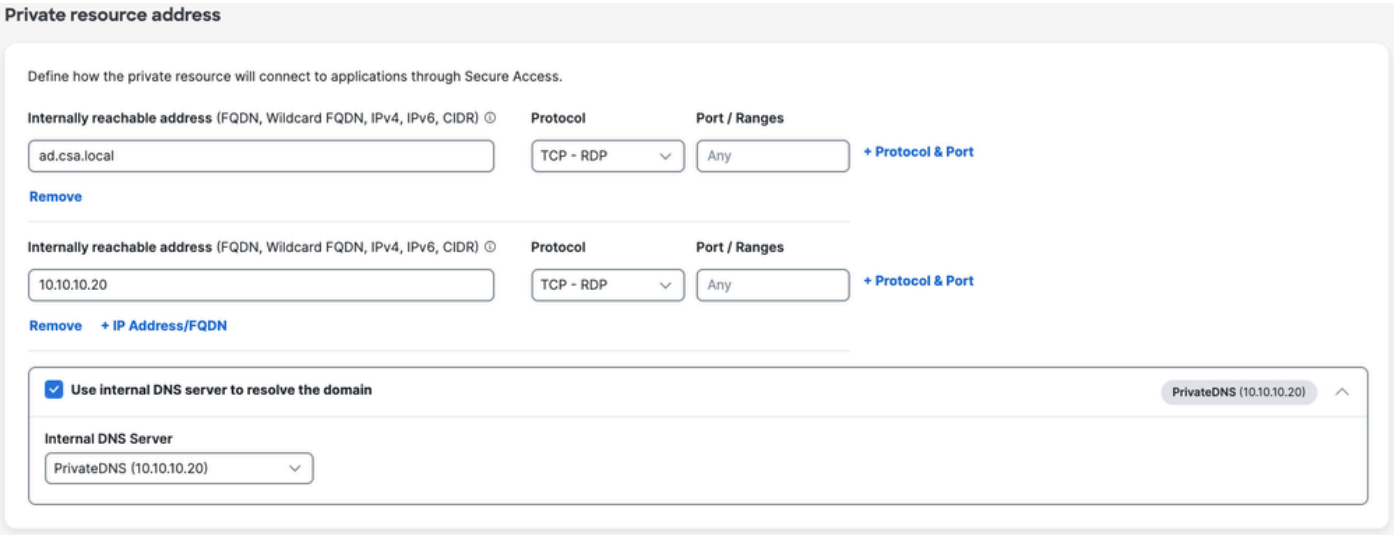
2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.



Accesso sicuro - Configurazione risorse private

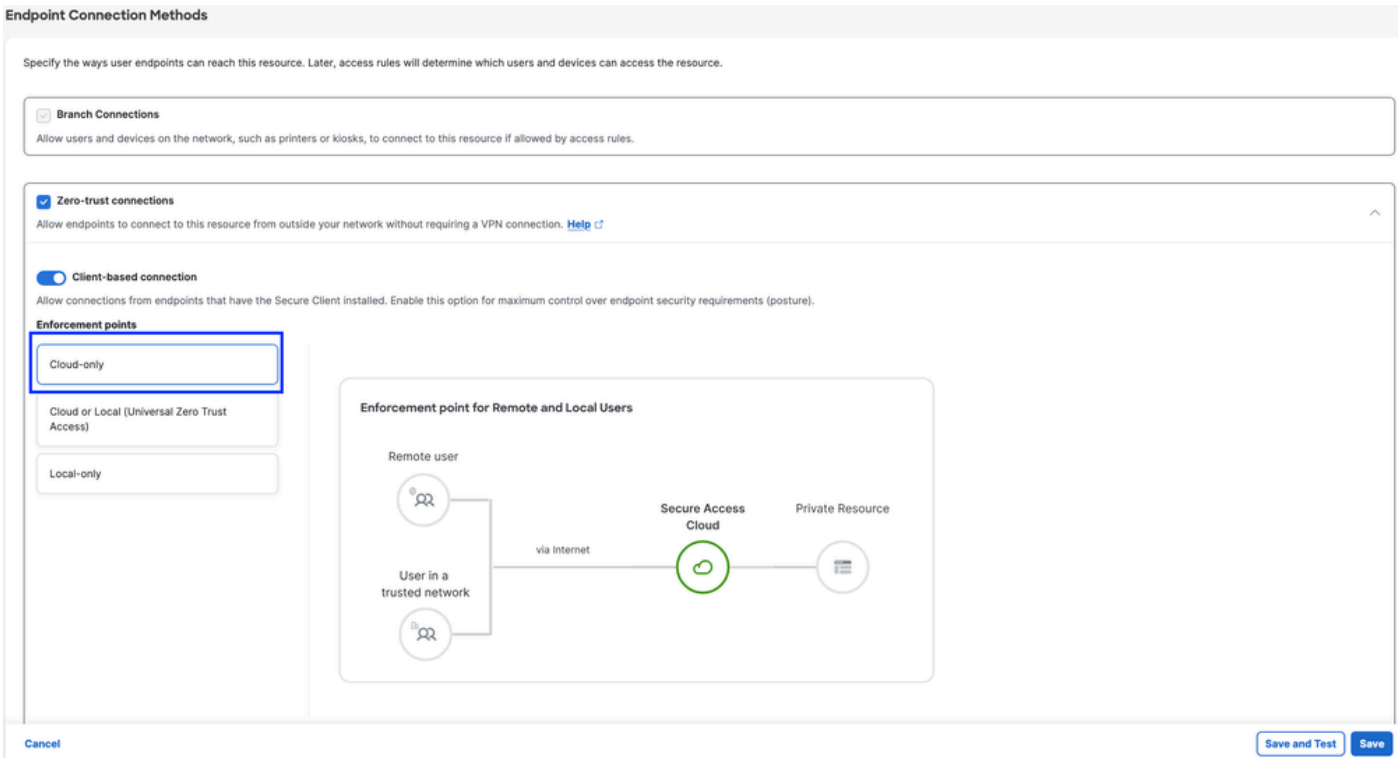
3. Inserire il nome di dominio completo (FQDN) della risorsa privata a cui si desidera accedere. È inoltre possibile definire l'indirizzo IP della risorsa privata. Per ulteriori informazioni, vedere [Aggiungere una risorsa privata]

4. Selezionare il server DNS interno per risolvere il dominio



Accesso sicuro - Configurazione risorse private

5. Seleziona metodi di connessione degli endpoint



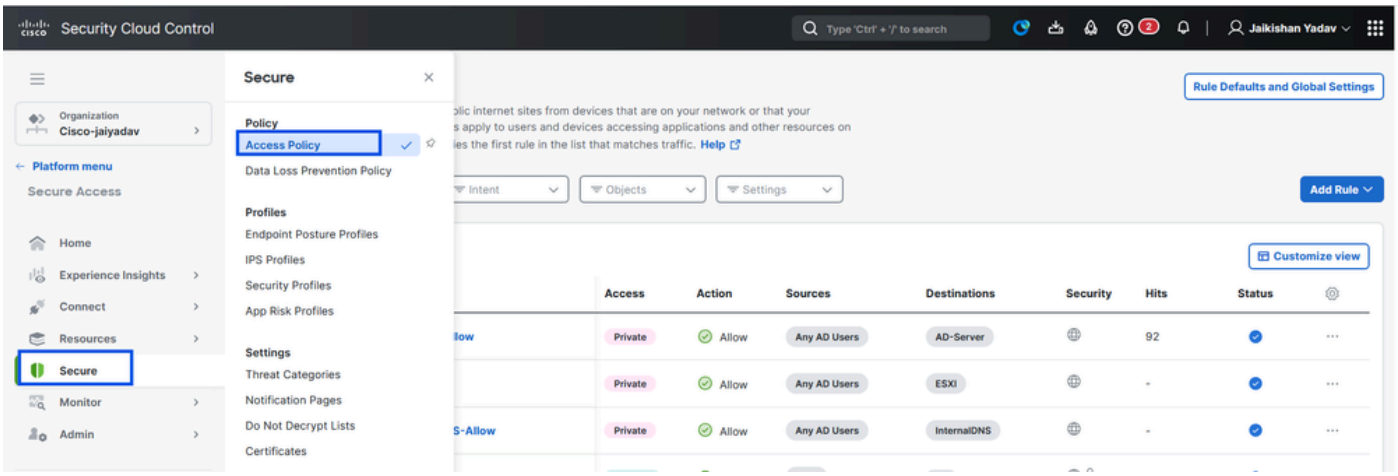
Accesso sicuro - Configurazione risorse private

6. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

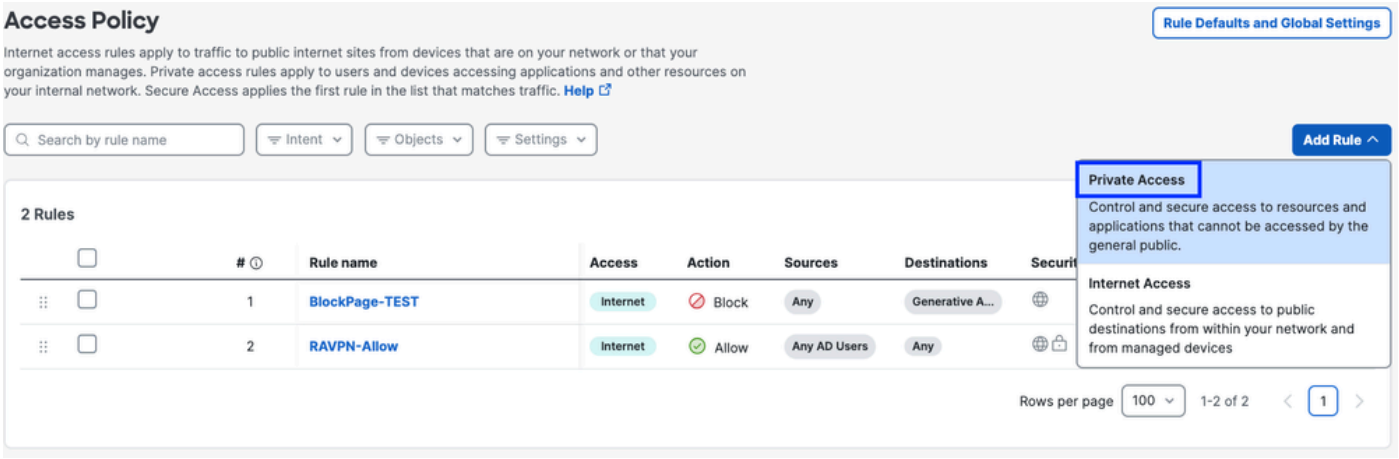
Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere Regola di accesso privato

1. Passare a Protezione > Criteri di accesso



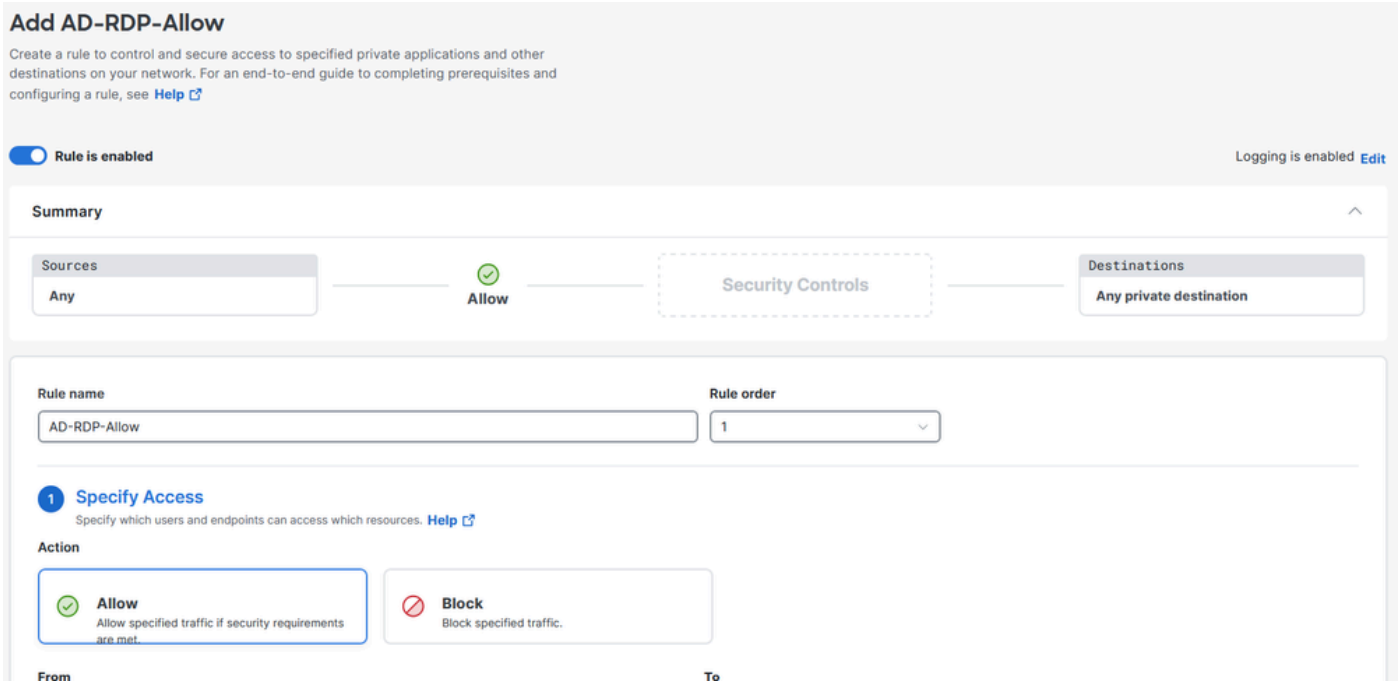
Accesso sicuro - Configurazione criteri di accesso

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.



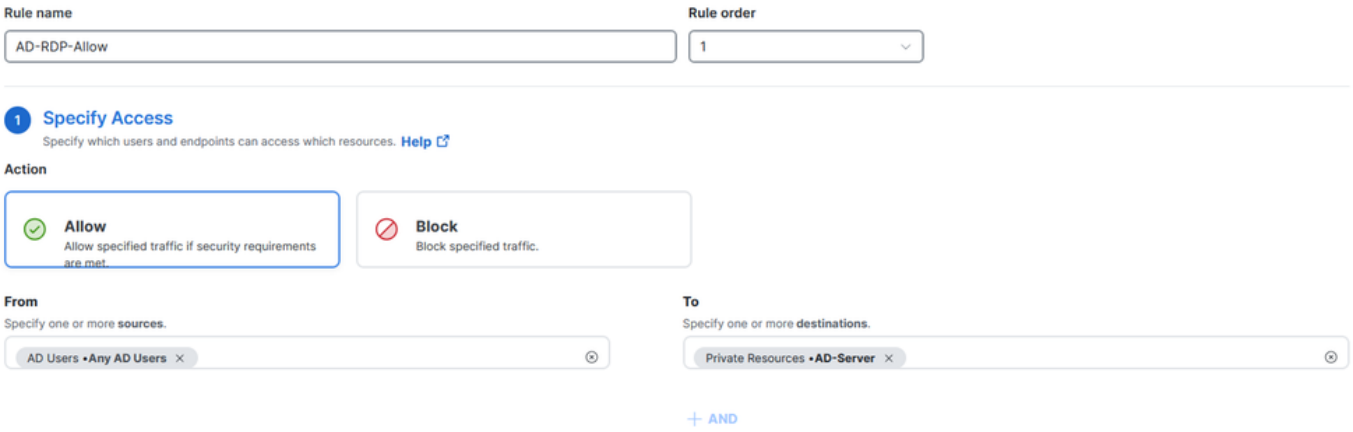
Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola



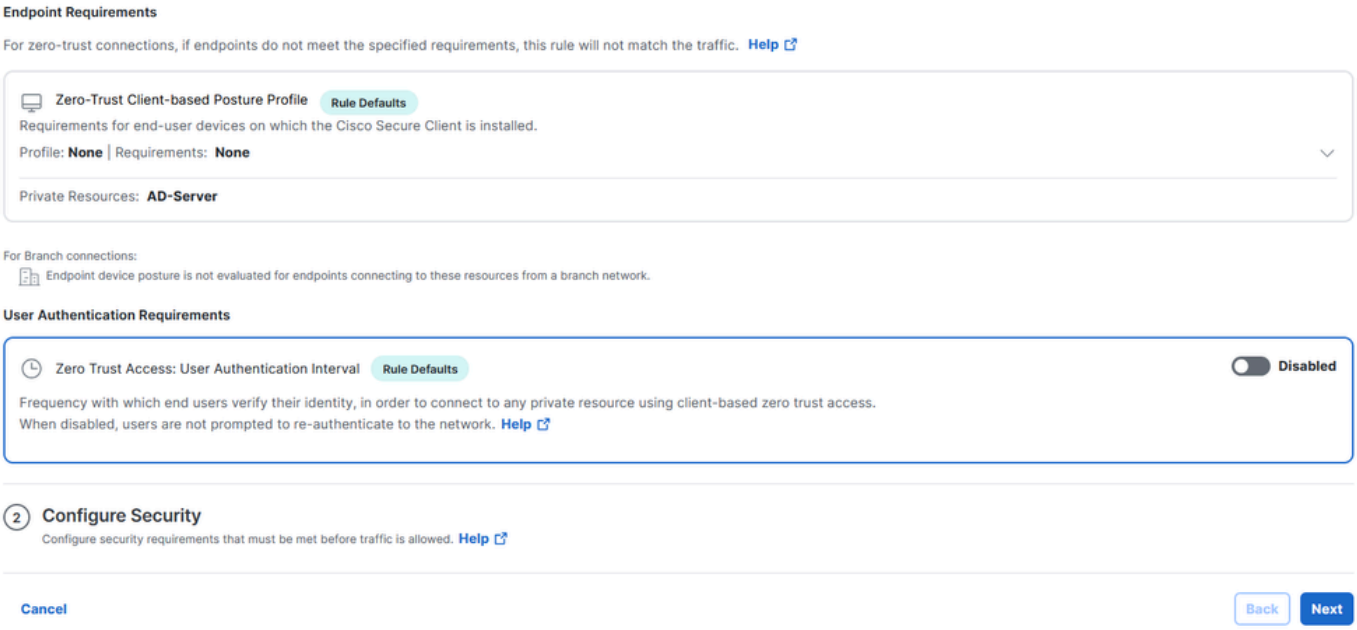
Accesso sicuro - Configurazione criteri di accesso

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



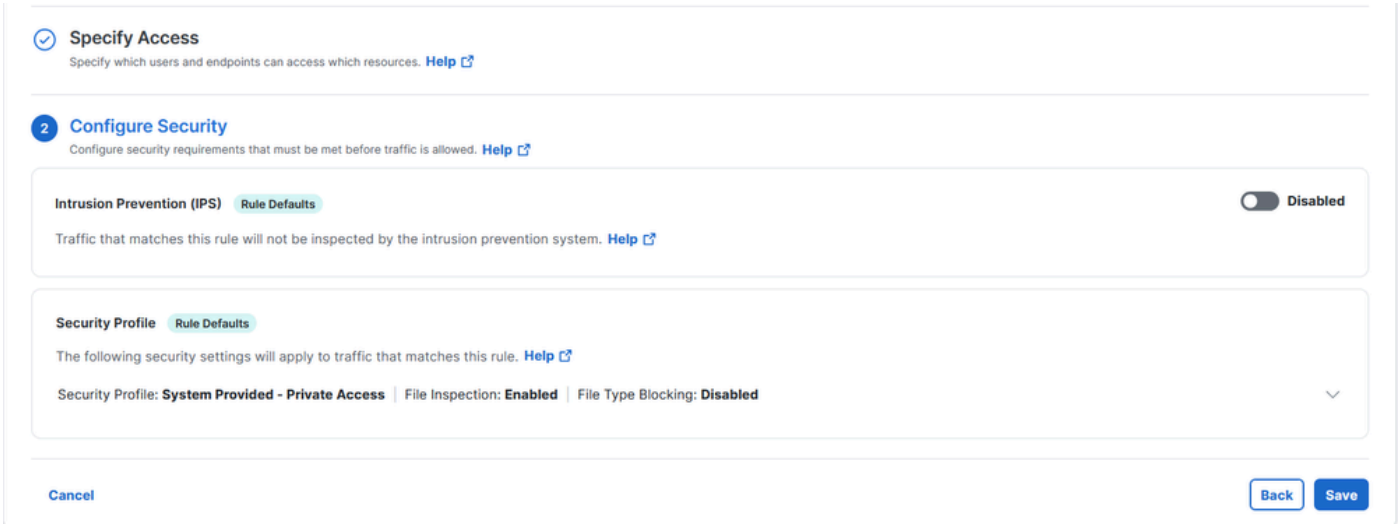
Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint



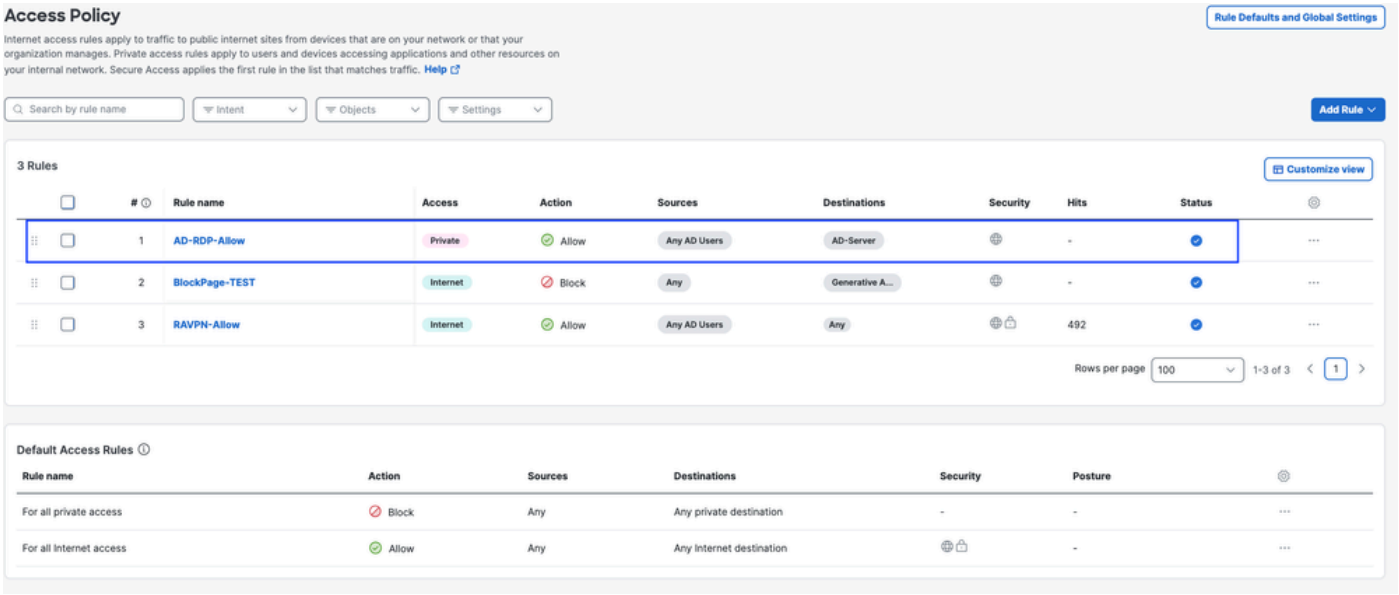
Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione



Accesso sicuro - Configurazione criteri di accesso

7. Fare clic su Save (Salva)

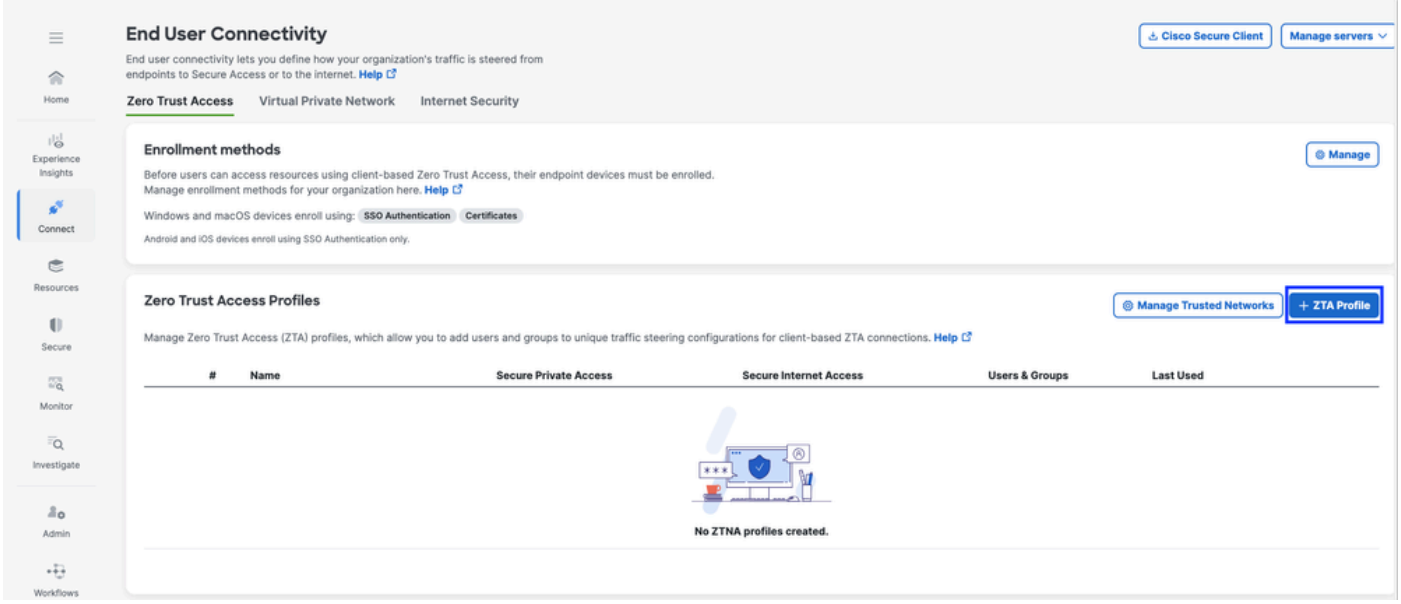


Accesso sicuro - Configurazione criteri di accesso

Fase - 3 Aggiungere una risorsa privata al profilo ZTA

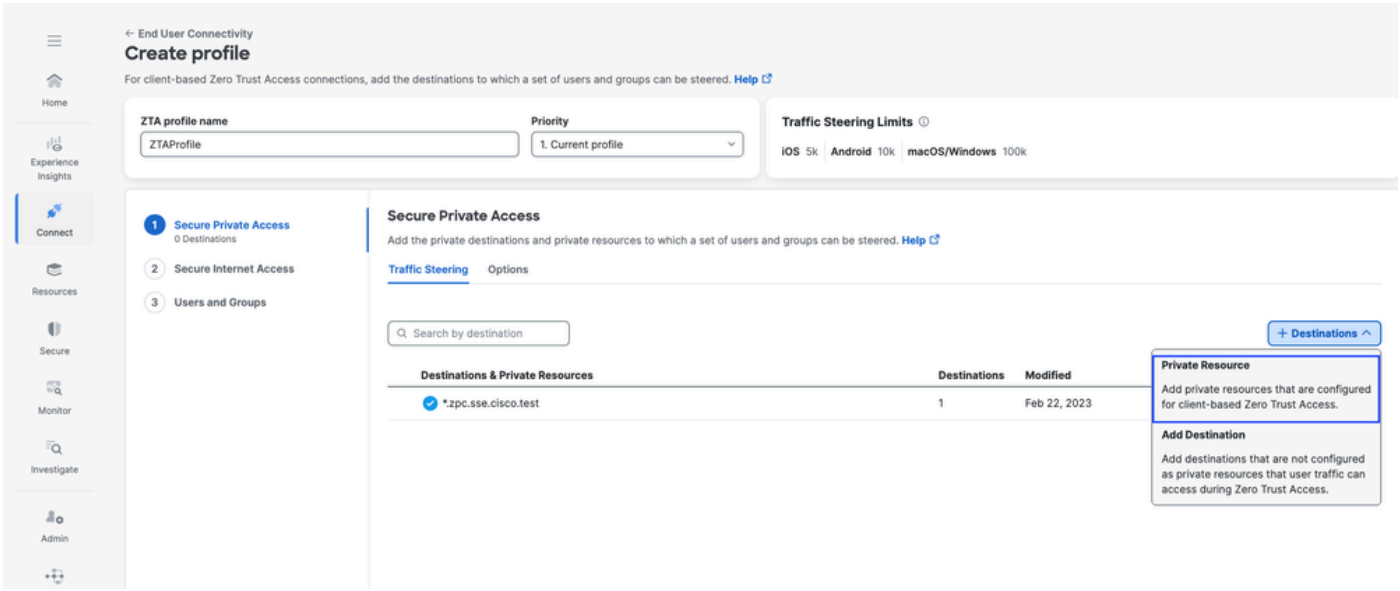
Se si utilizza un profilo ZTA personalizzato, è necessario aggiungere la rispettiva risorsa privata al profilo ZTA

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

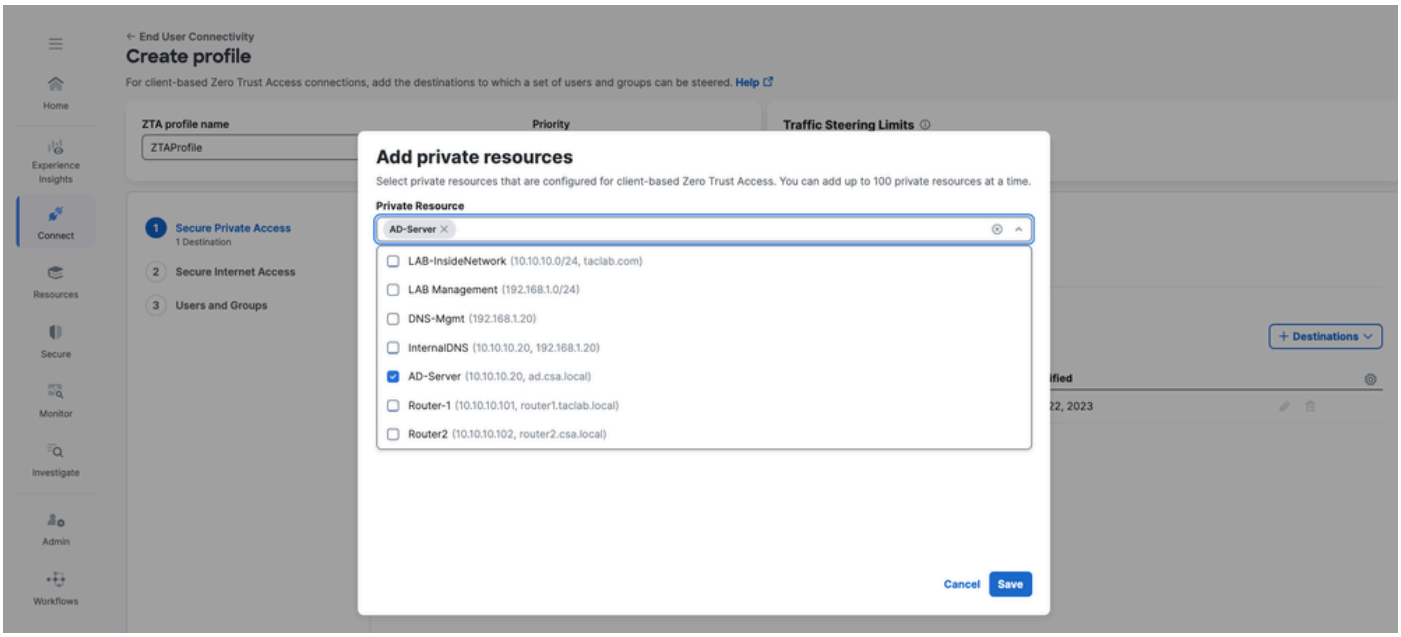


Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

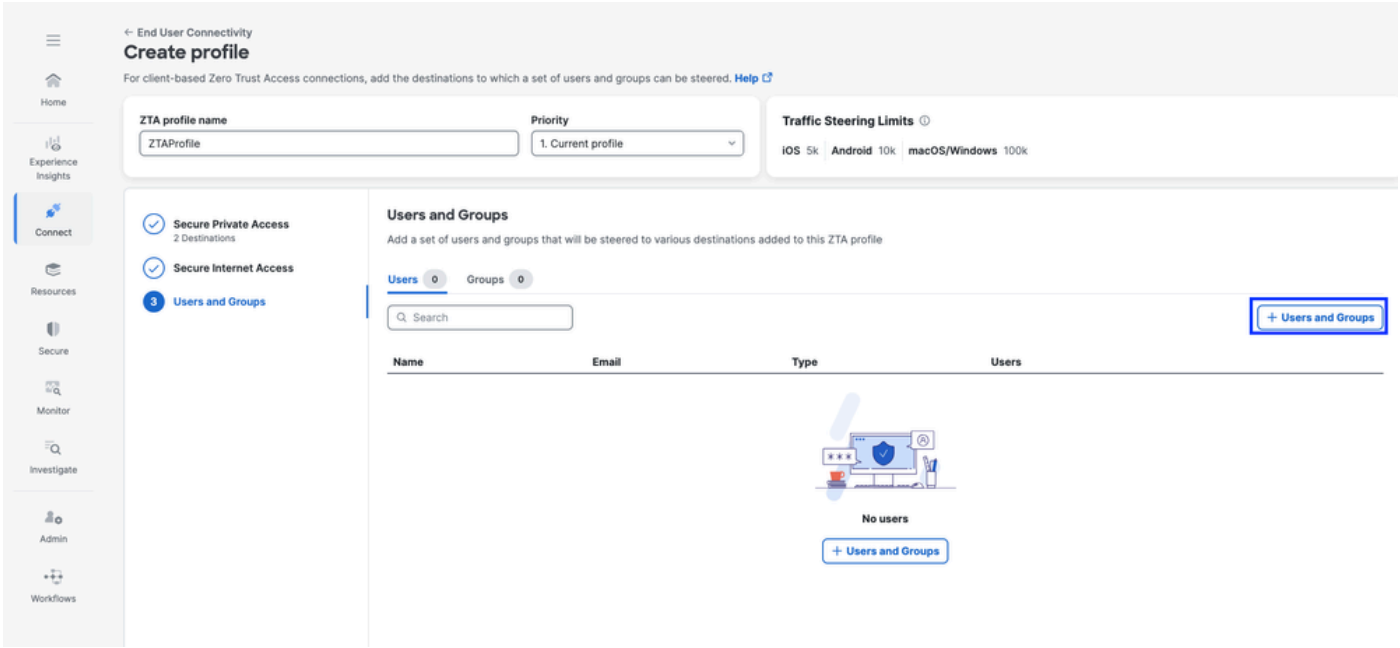


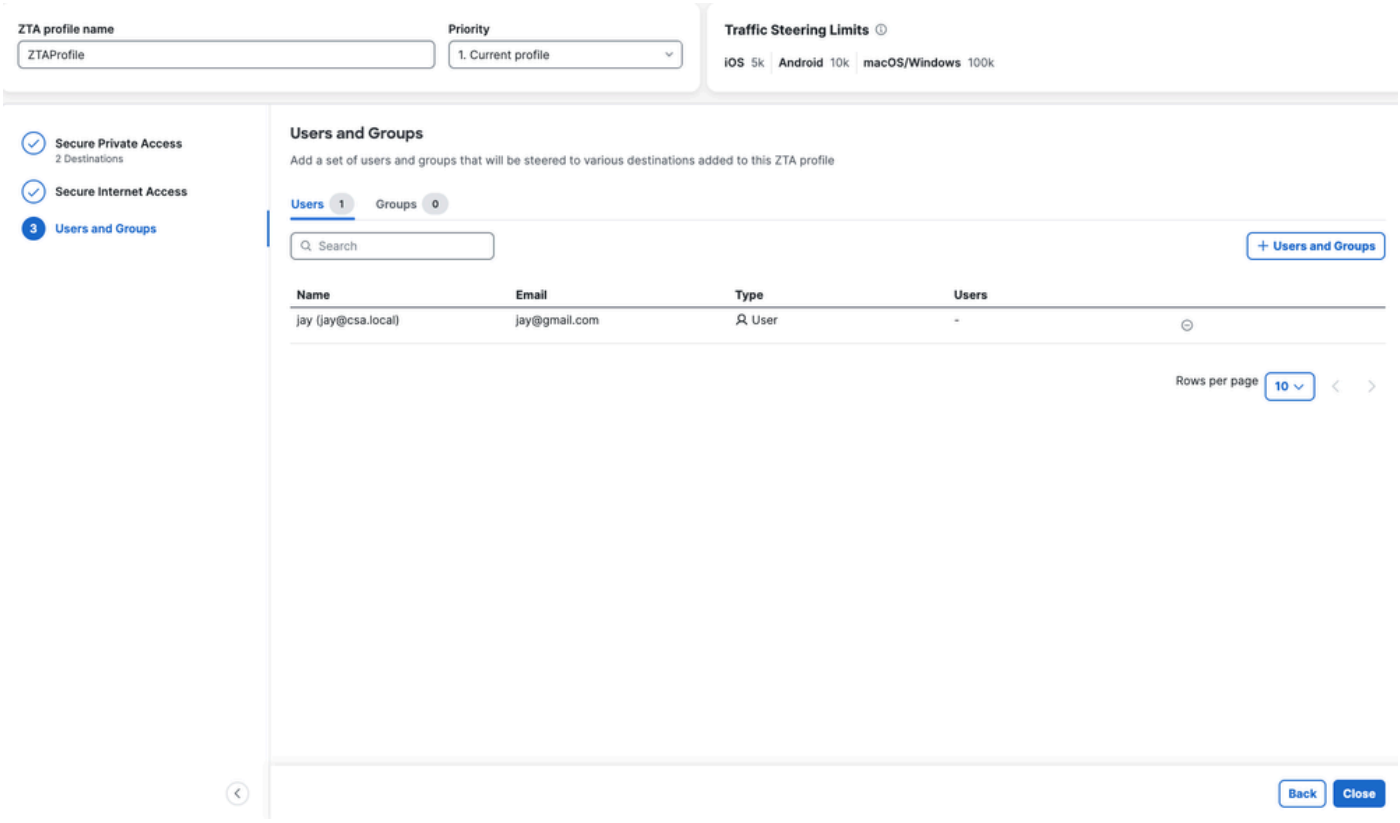
Accesso sicuro - Profilo ZTA



Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi





Accesso sicuro - Profilo ZTA

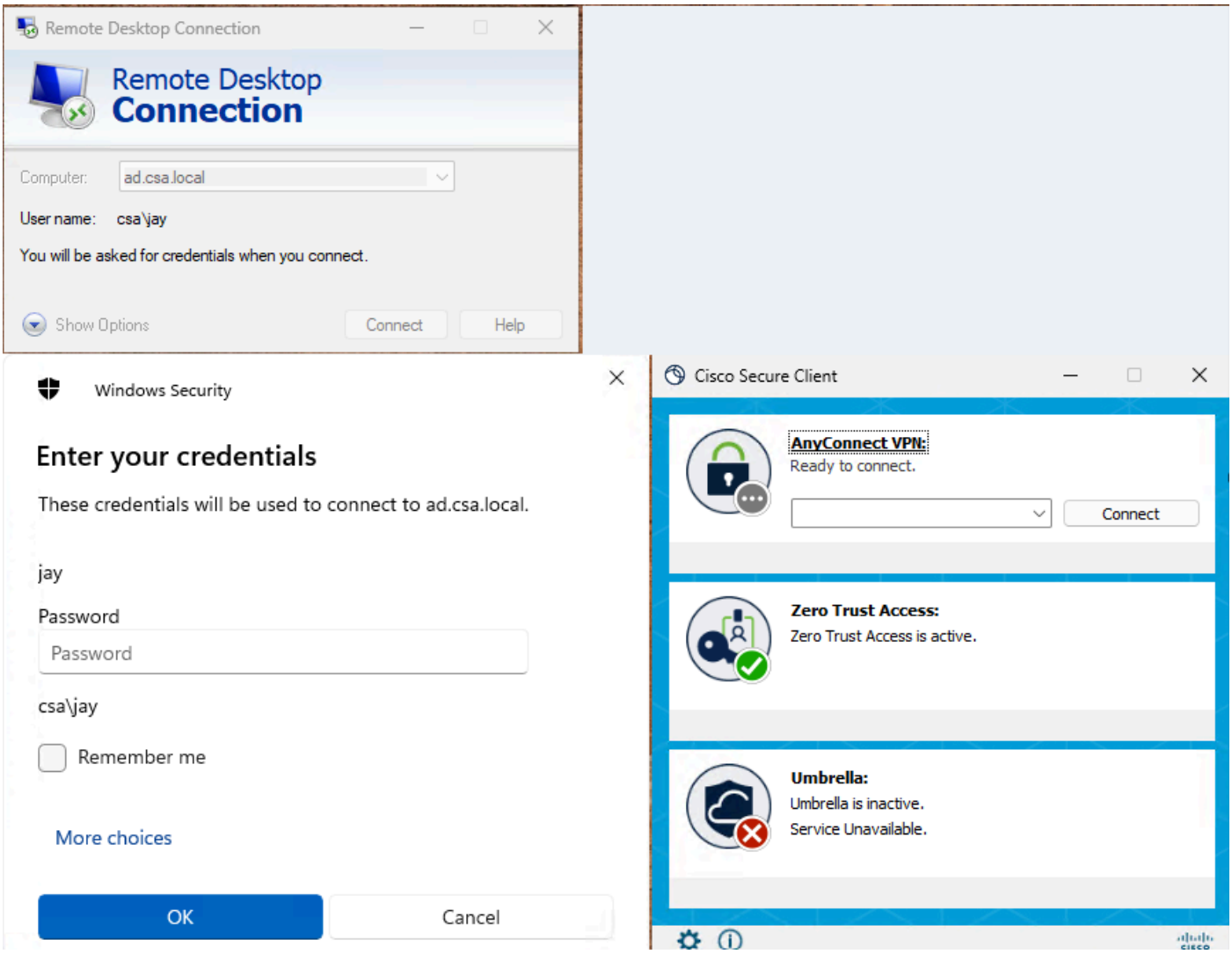
Nota: L'operazione di push e sincronizzazione della configurazione con il client per la risorsa privata assegnata può richiedere fino a 15-20 minuti

---

Fase - 4 Verifica dell'accesso alla risorsa privata

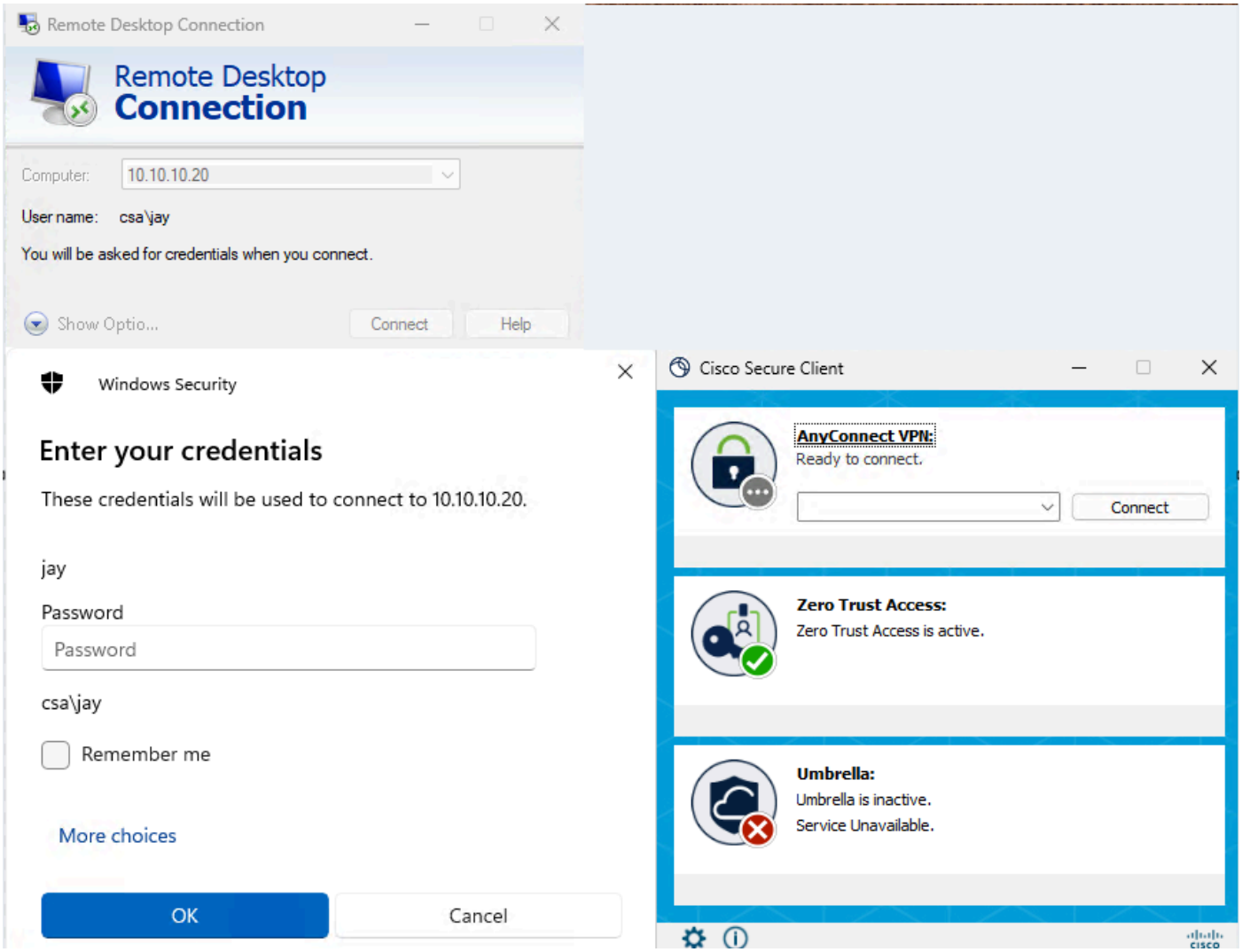
1. Accedere alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN



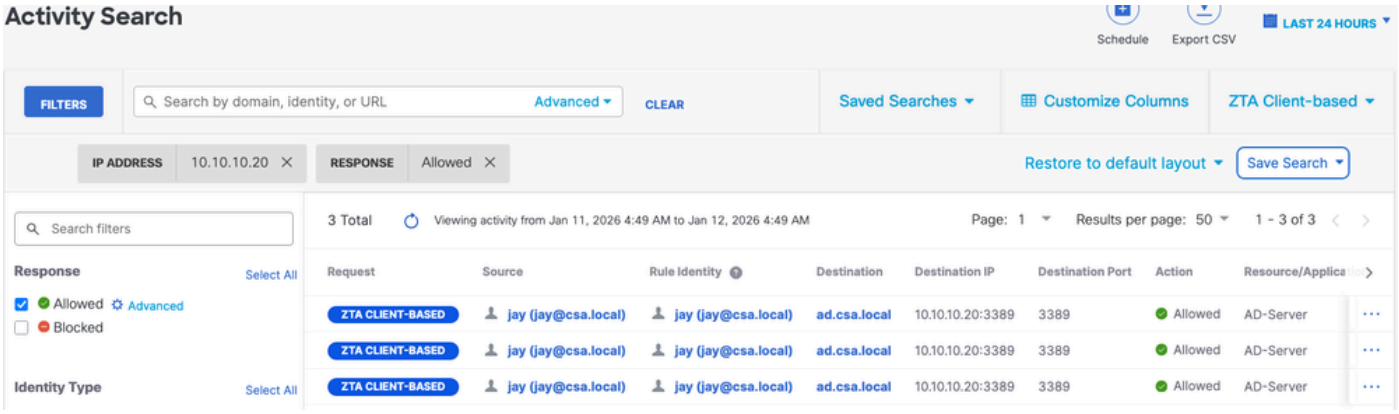
Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP

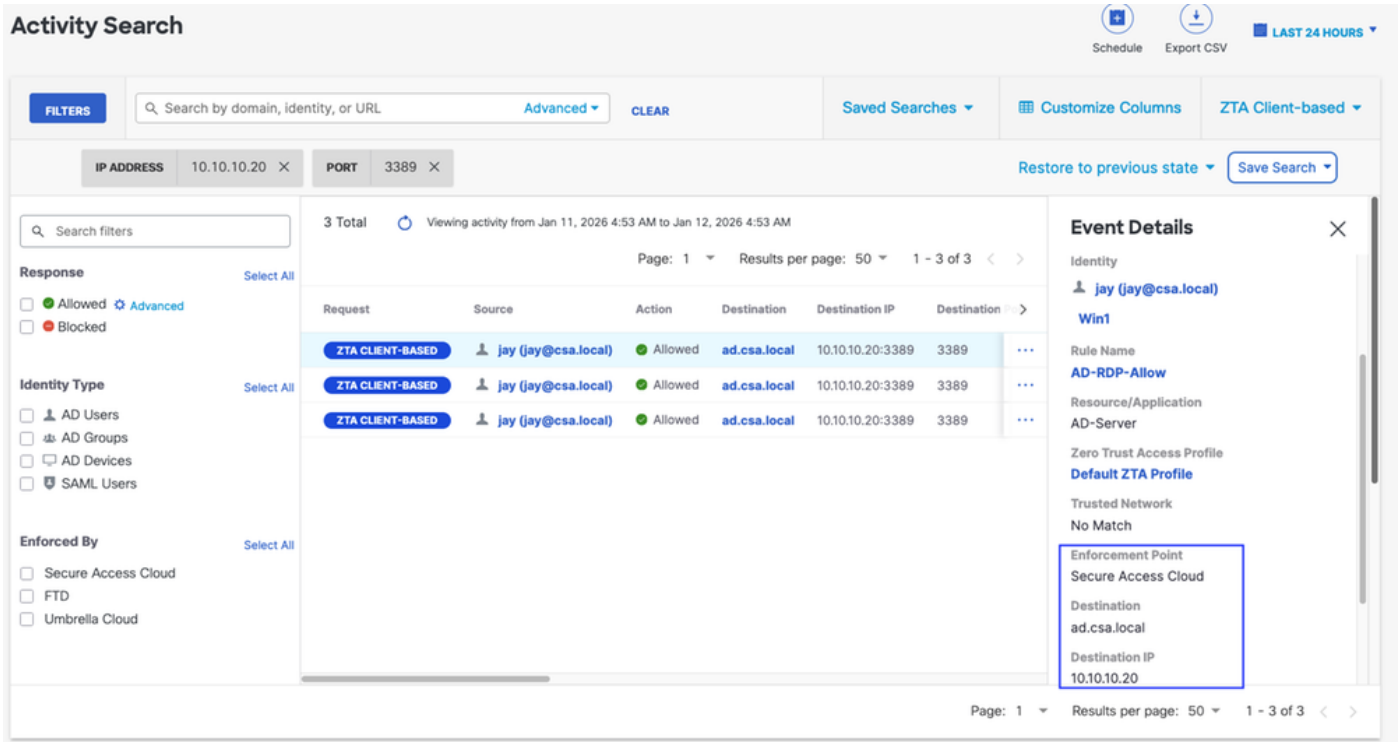


Accesso sicuro - Test PR

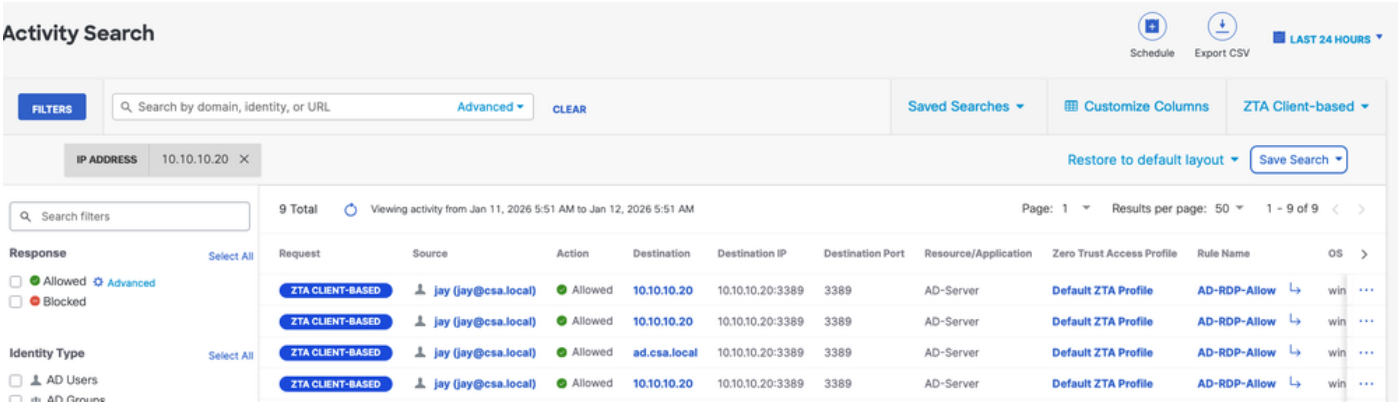
2. Verifica con gli eventi di Ricerca attività



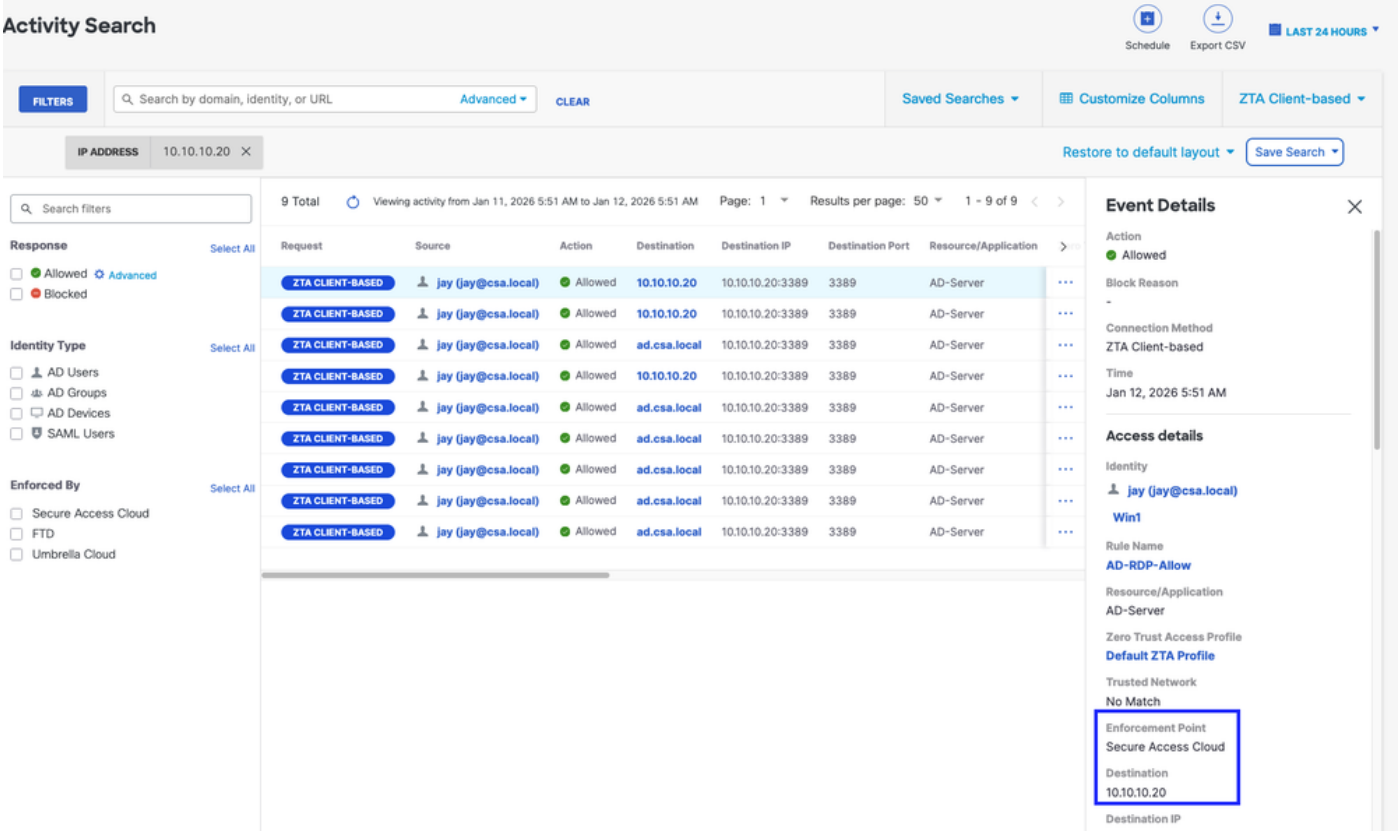
Accesso sicuro - Ricerca attività



Accesso sicuro - Ricerca attività

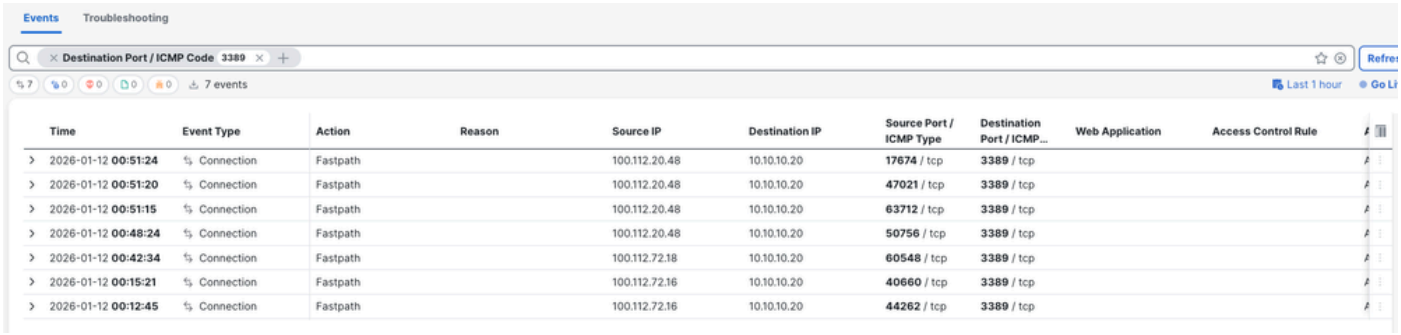


Accesso sicuro - Ricerca attività



Accesso sicuro - Ricerca attività

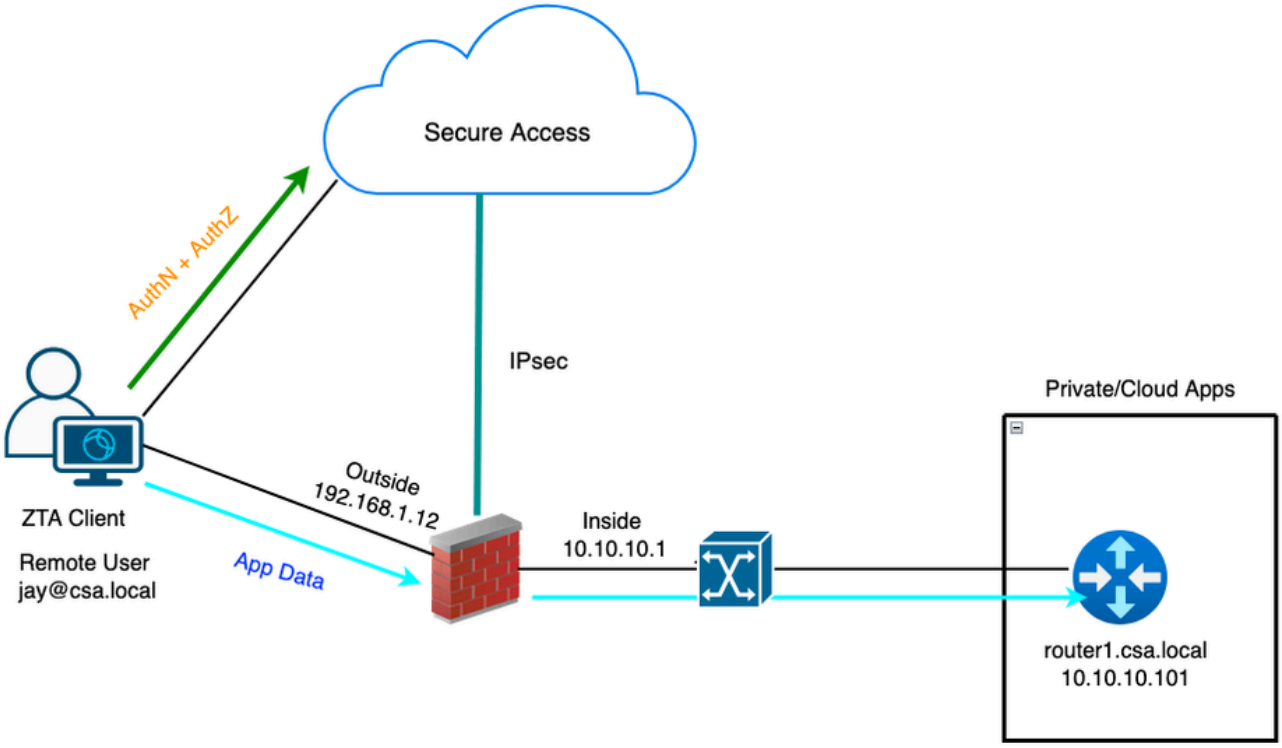
3. Verificare gli eventi di connessione FMC



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.

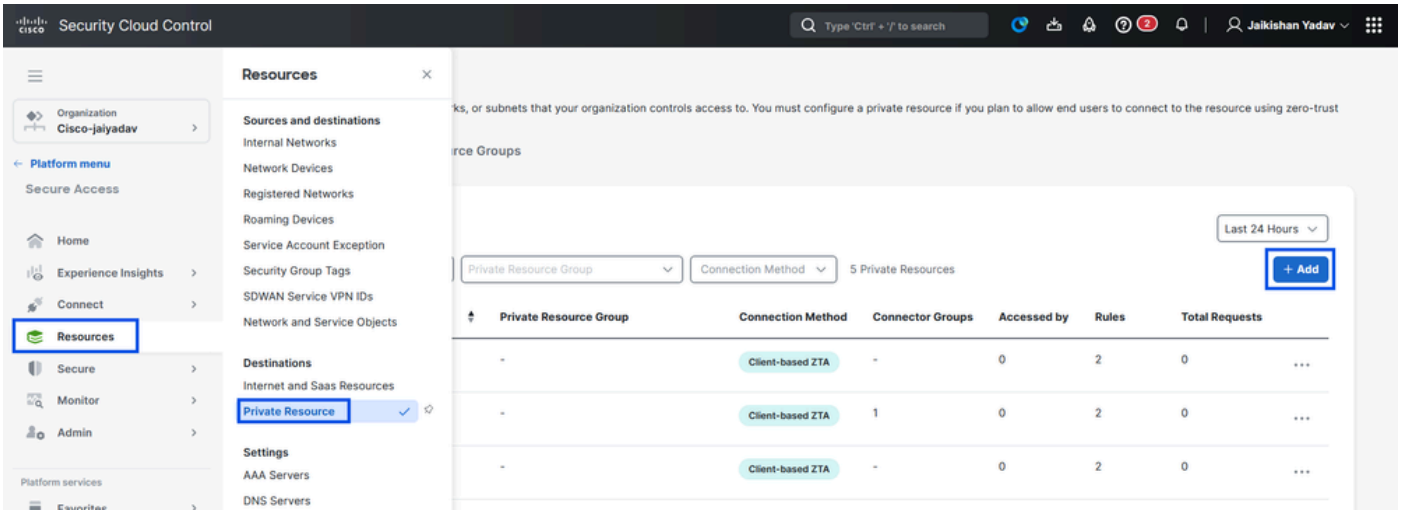


Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

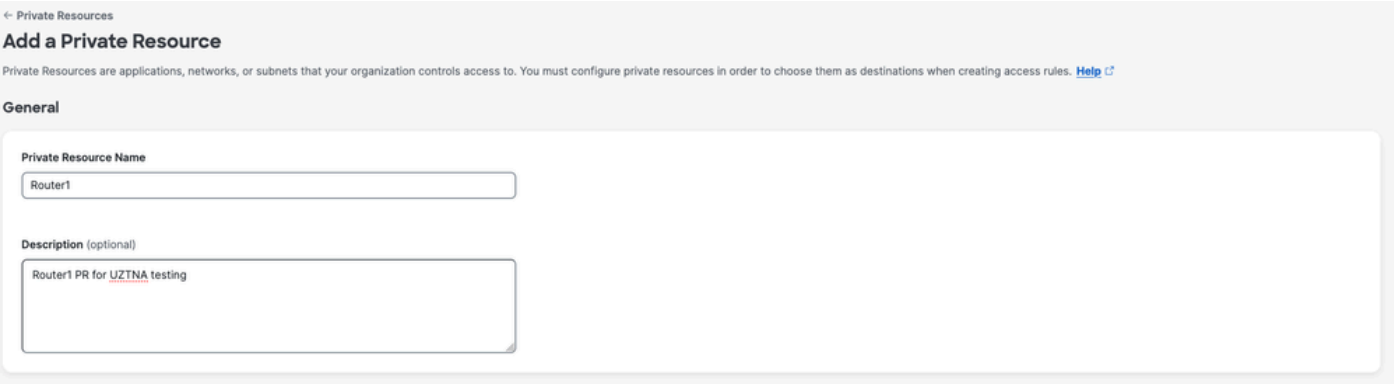
Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

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



Accesso sicuro - Configurazione risorse private

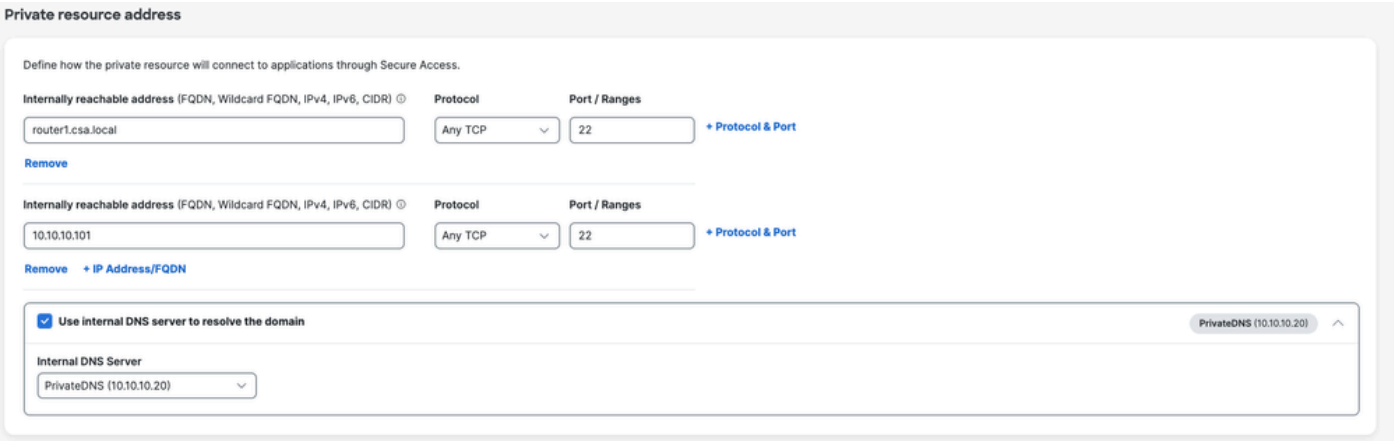
2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.



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

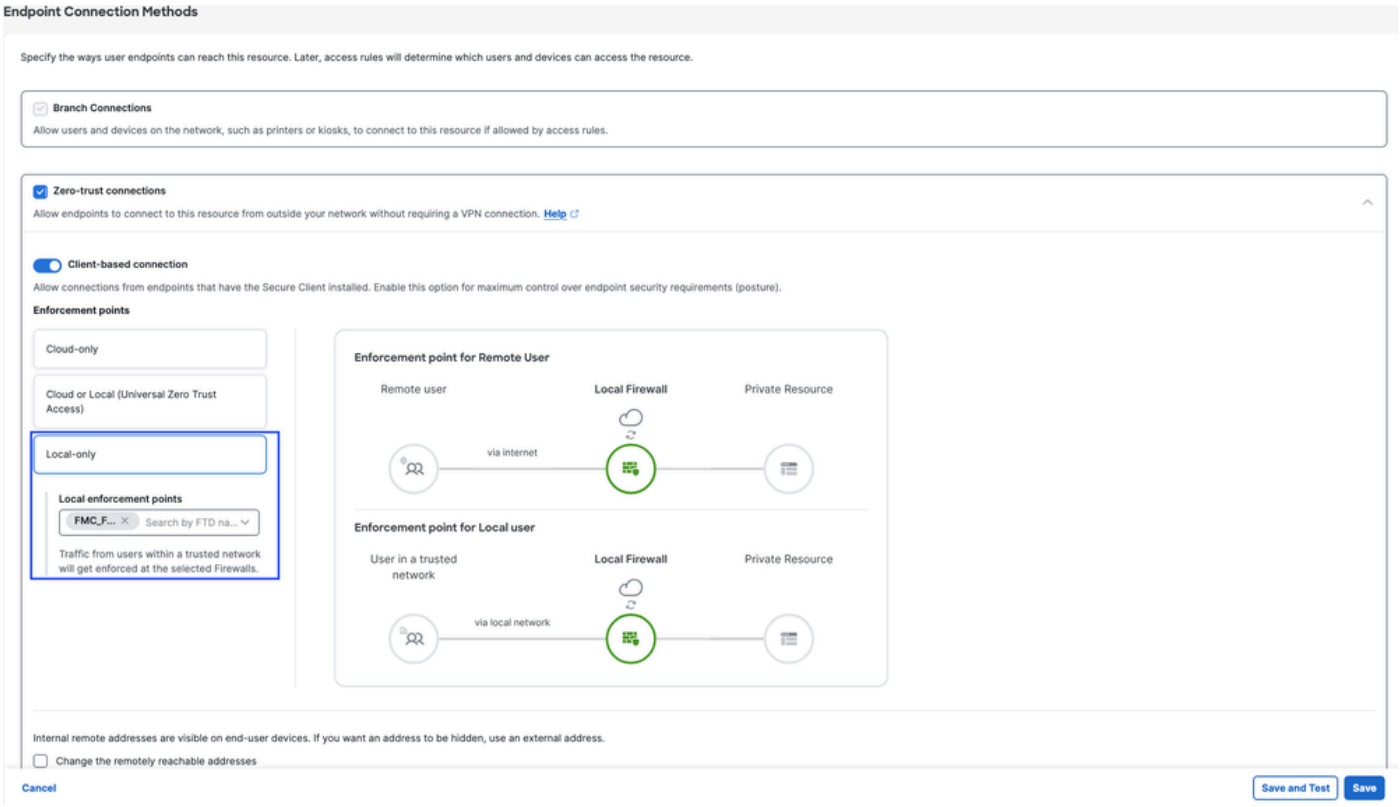
4. Selezionare il server DNS interno per risolvere il dominio



Accesso sicuro - Configurazione risorse private

5. Seleziona metodi di connessione degli endpoint

6. Selezionare FTD come punti di applicazione locale



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

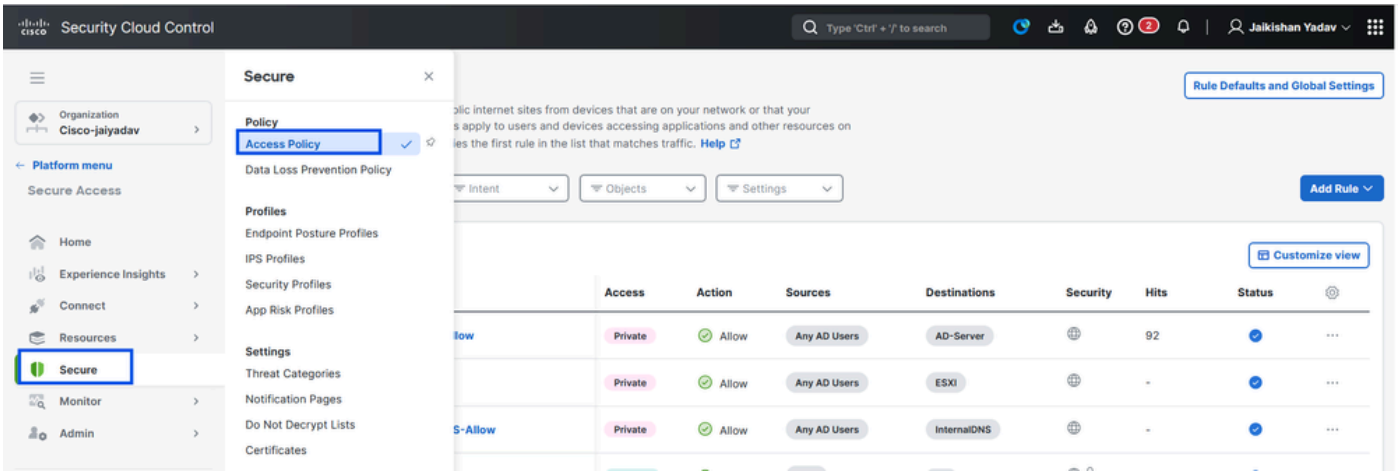
---

7. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

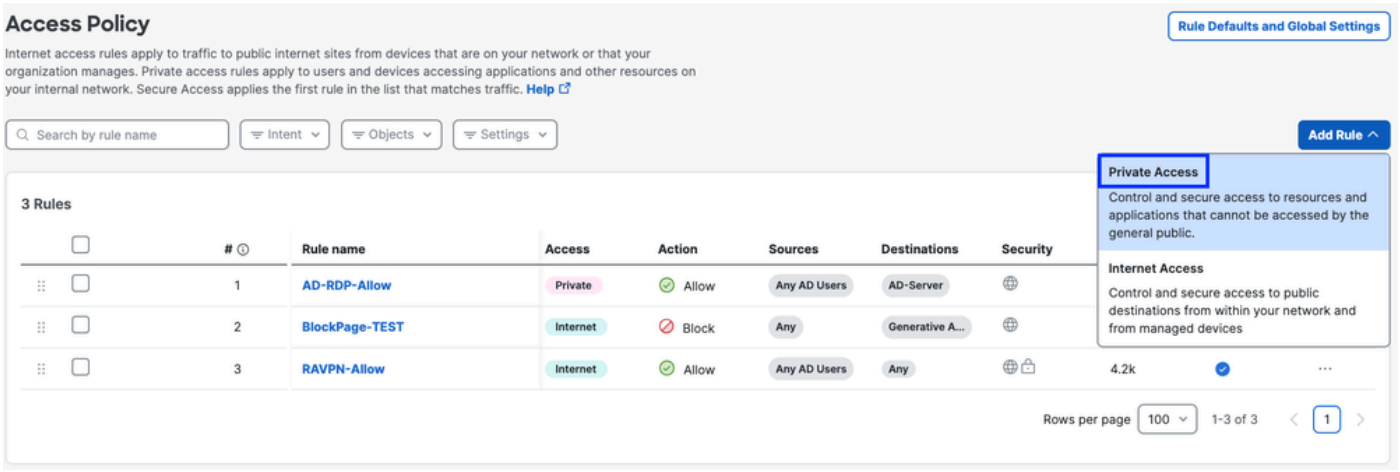
Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere Regola di accesso privato

1. Passare a Protezione > Criteri di accesso



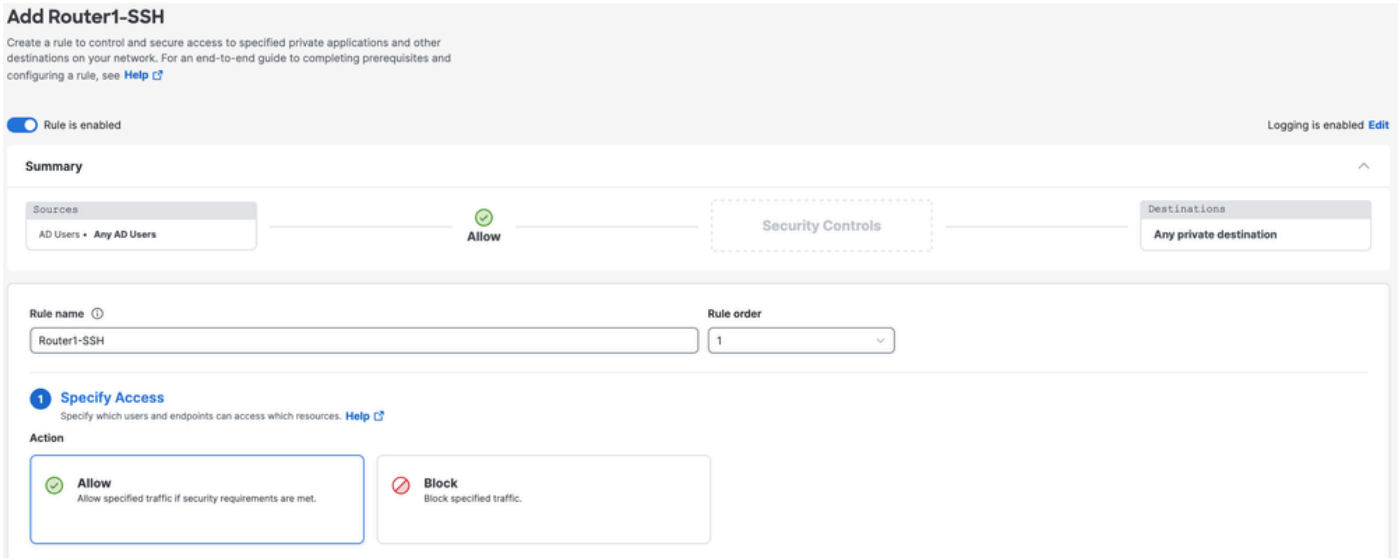
Accesso sicuro - Configurazione risorse private

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.



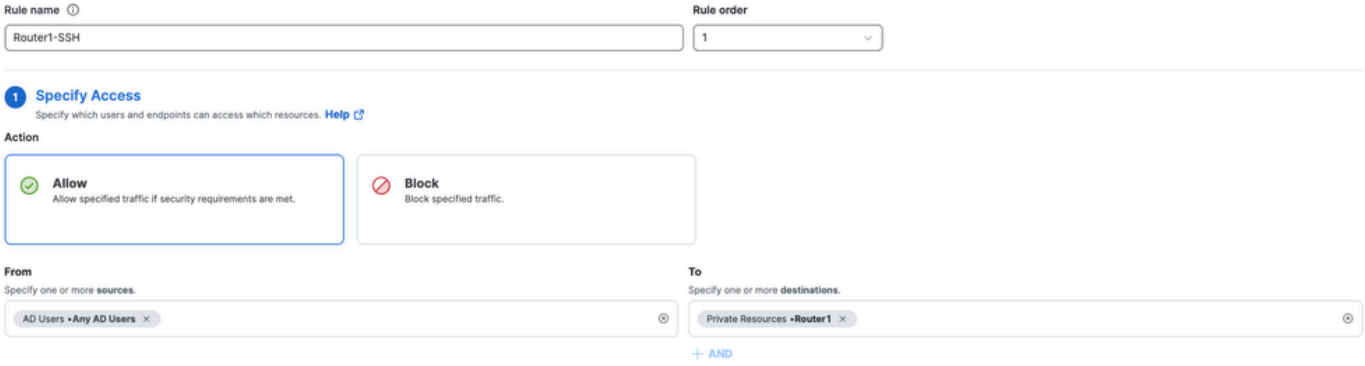
Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola



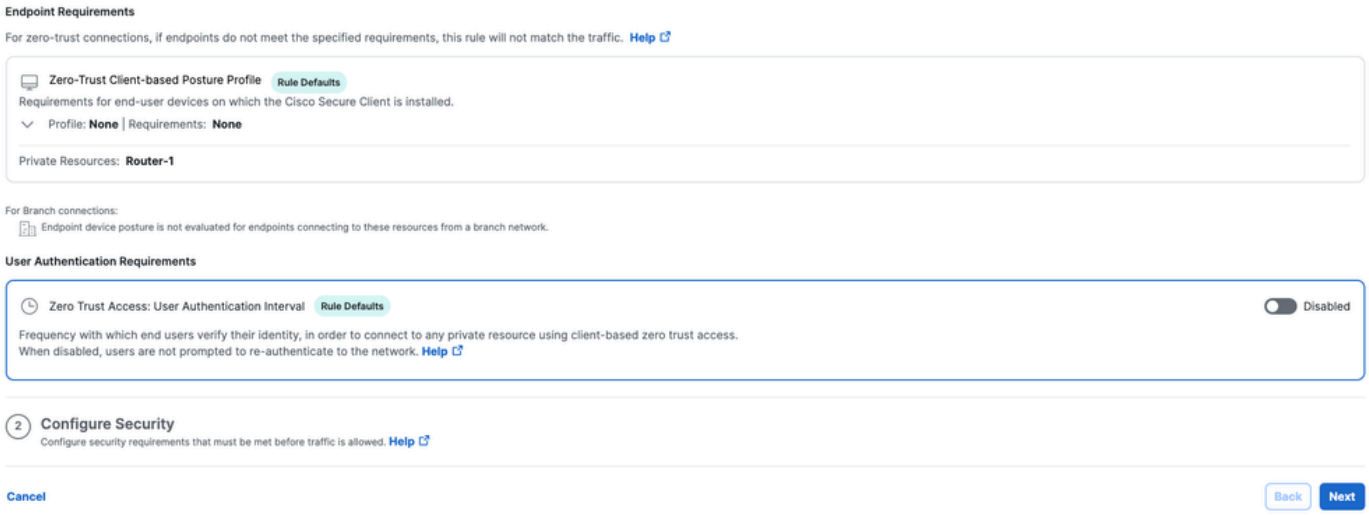
Accesso sicuro - Configurazione criteri di accesso

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



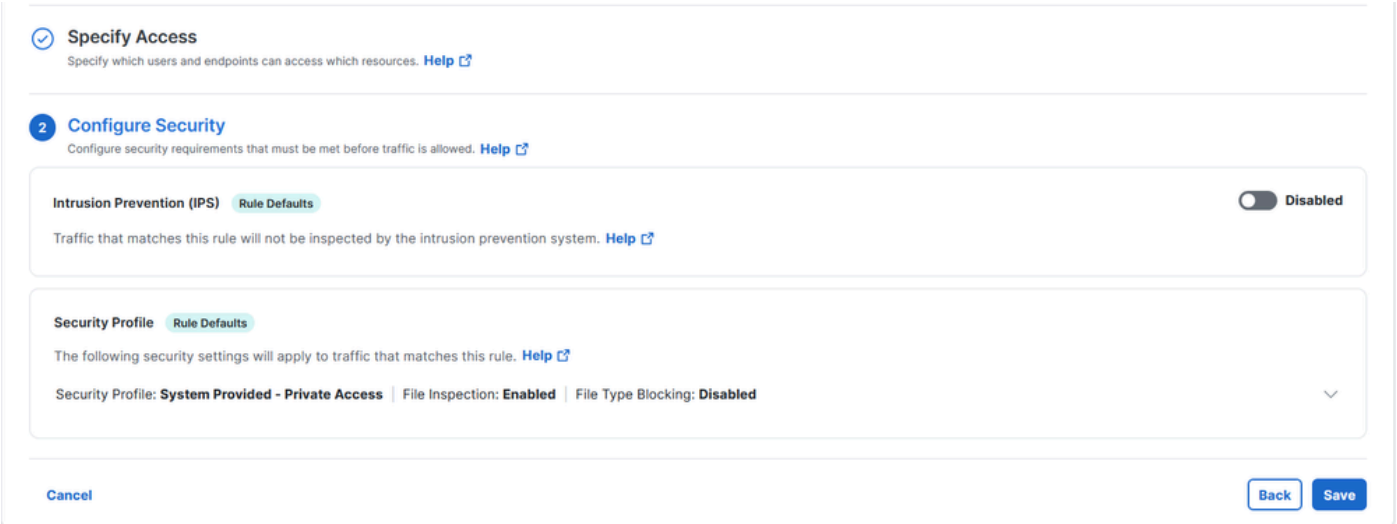
Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint



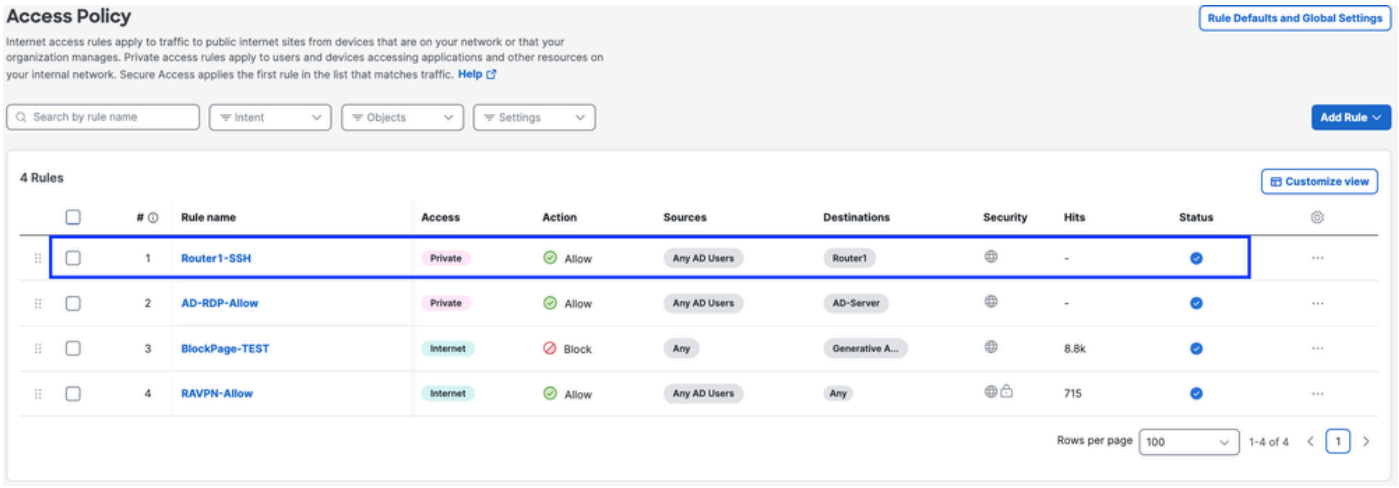
Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione



Accesso sicuro - Configurazione criteri di accesso

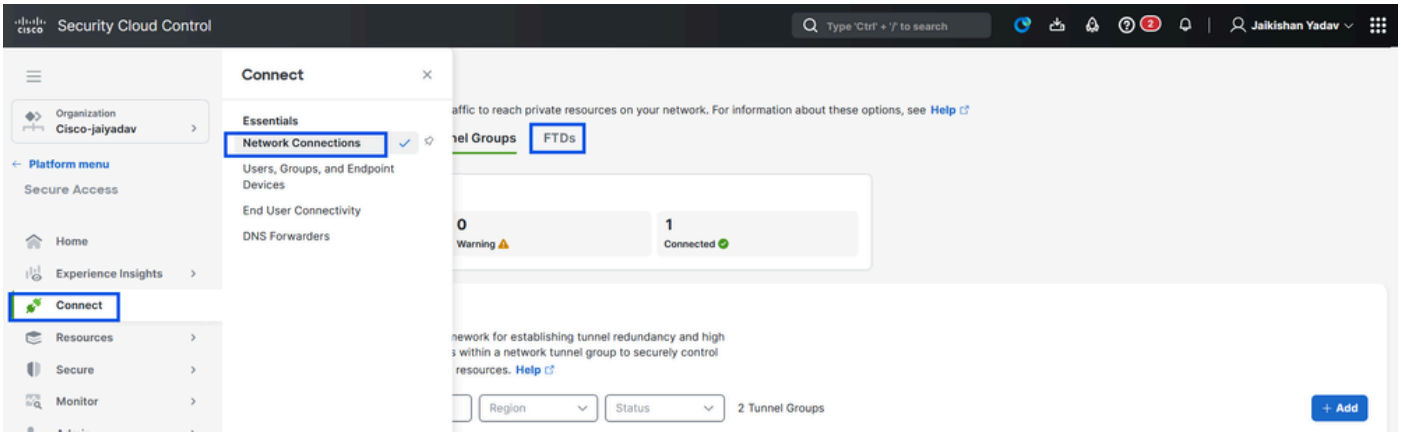
7. Fare clic su Save (Salva)



Accesso sicuro - Configurazione criteri di accesso

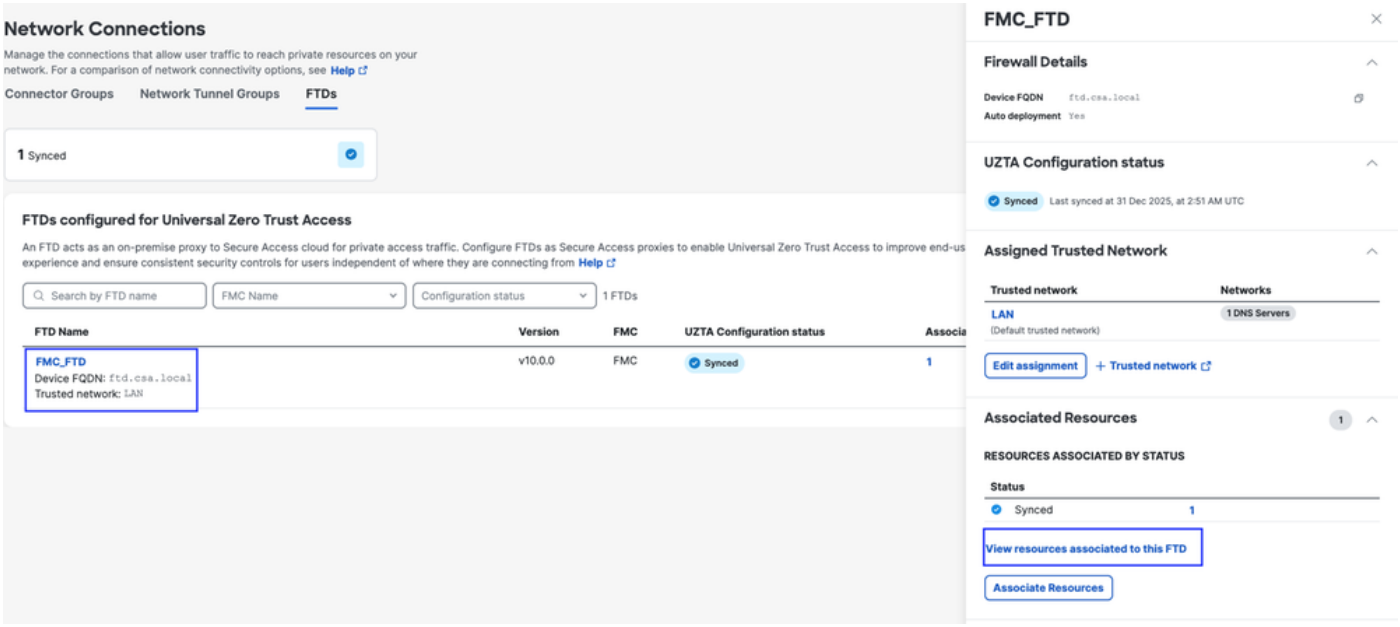
Fase 3 - Verifica dell'associazione di PR sull'FTD

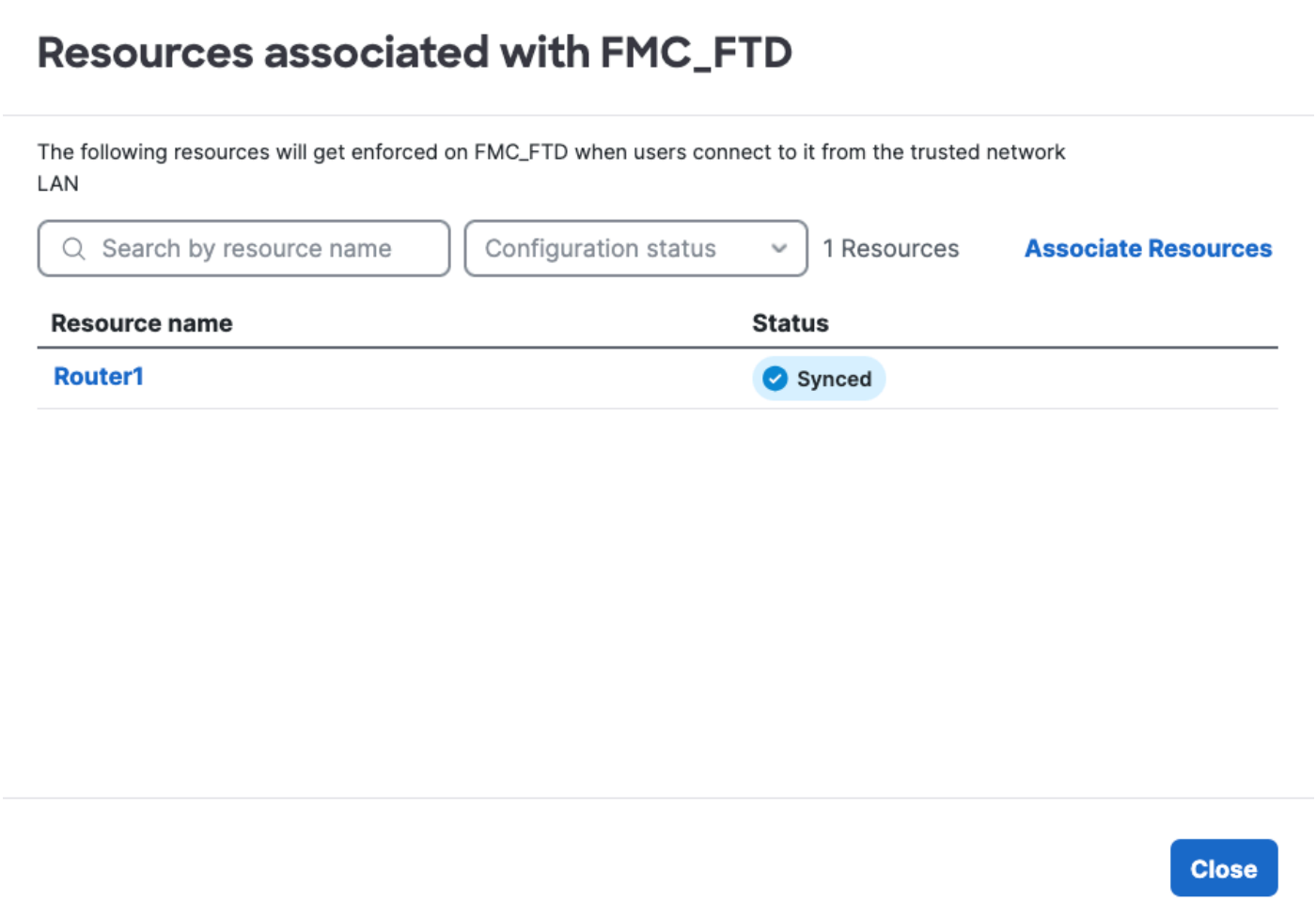
1. Passare a Connetti > Connessioni di rete > FTD



Accesso sicuro - Verifica PR

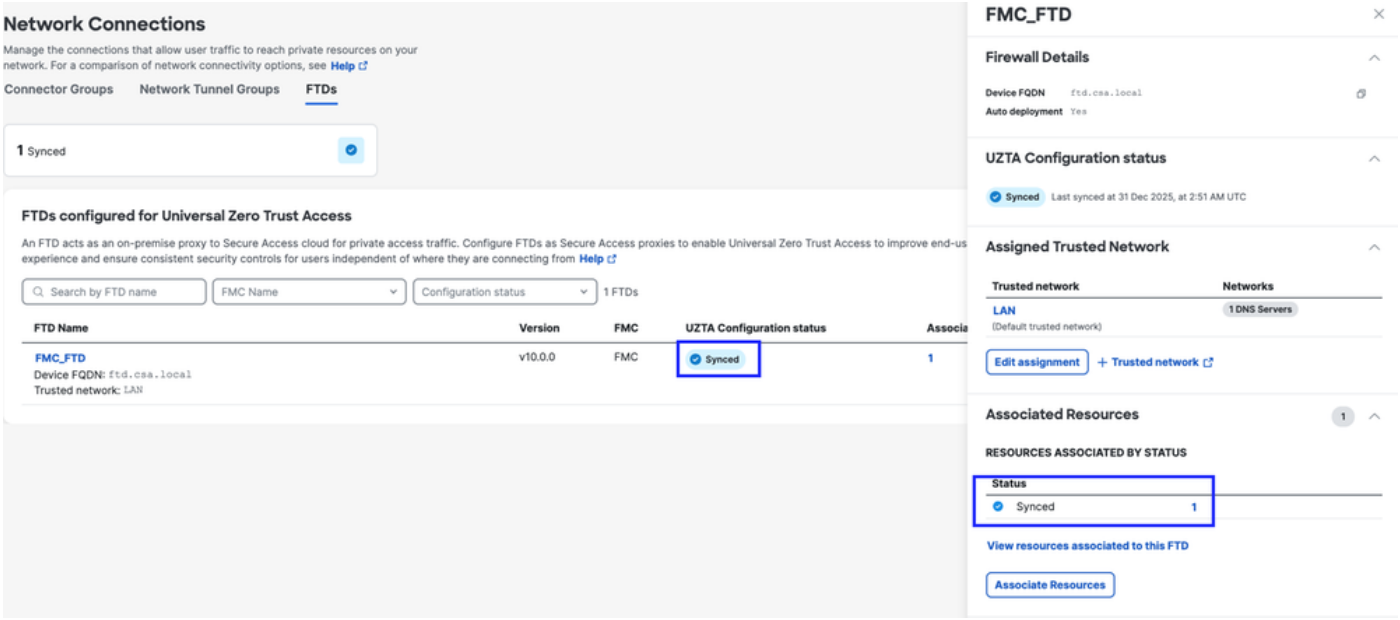
2. Fare clic su FTD > Visualizza risorse associate a questo FTD


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-us 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
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
1
RESOURCES ASSOCIATED BY STATUS
Status
Synced 1
View resources associated to this FTD
Associate Resources


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
1 Resources
Associate Resources
Resource name
Status
Router1
Synced
Close

3. Fare clic su chiudi

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



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

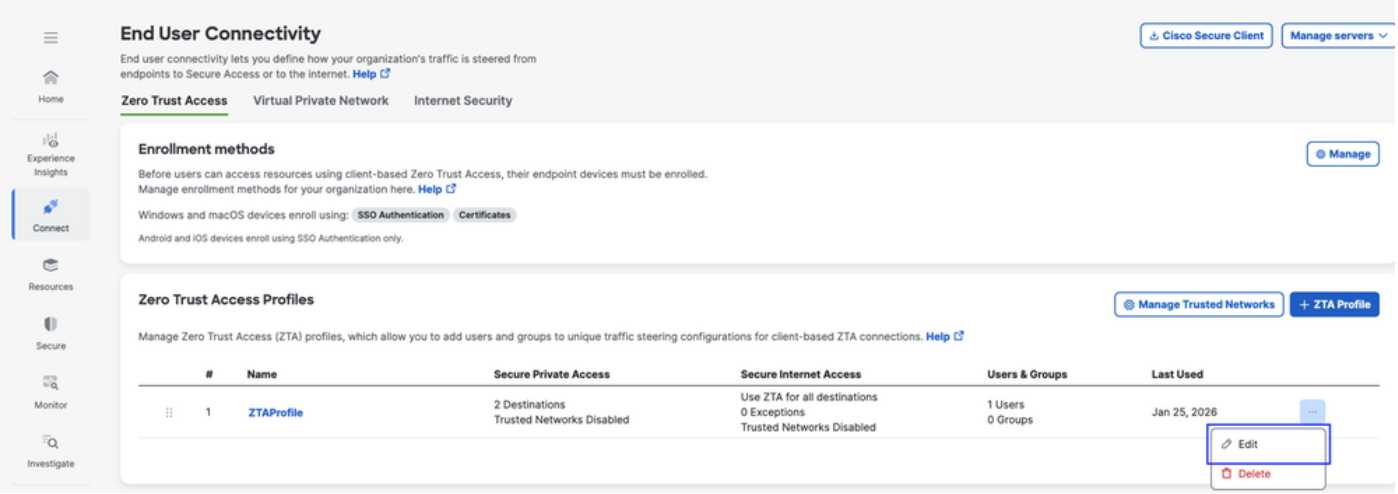
show running-config applicazione oggetto

```
> 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

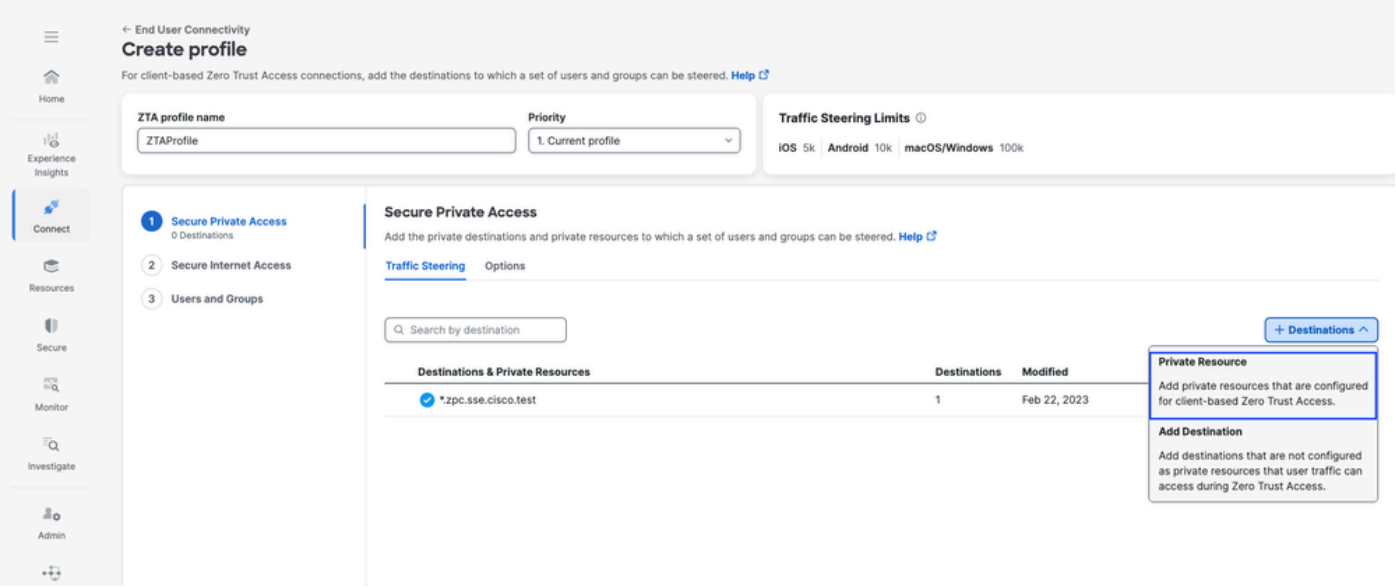
Fase - 4 Aggiungere una risorsa privata al profilo ZTA

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

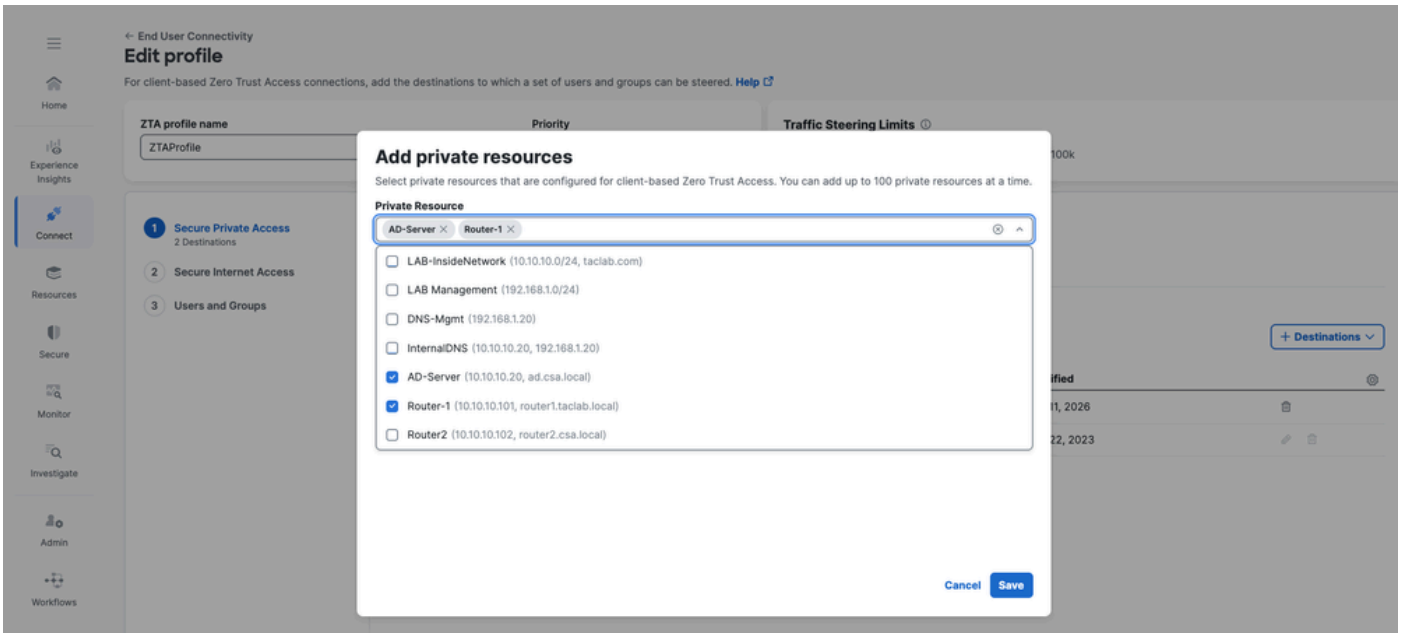


Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

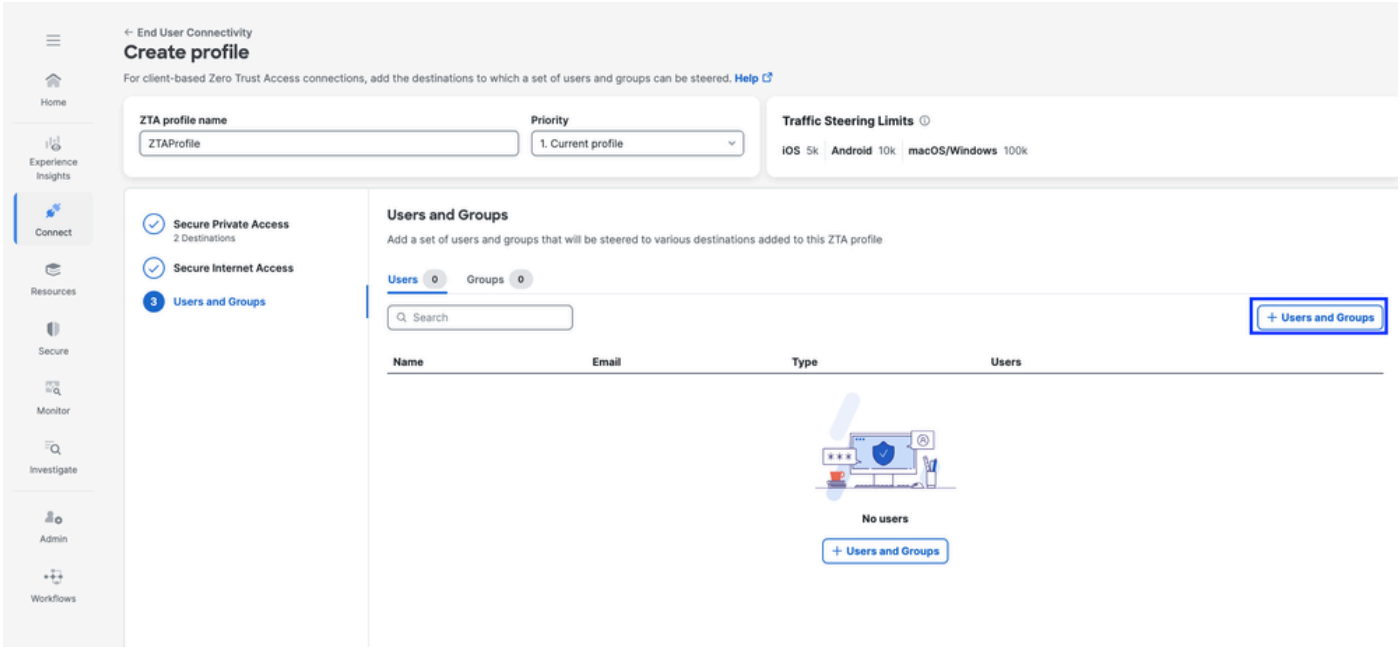


Accesso sicuro - Profilo ZTA

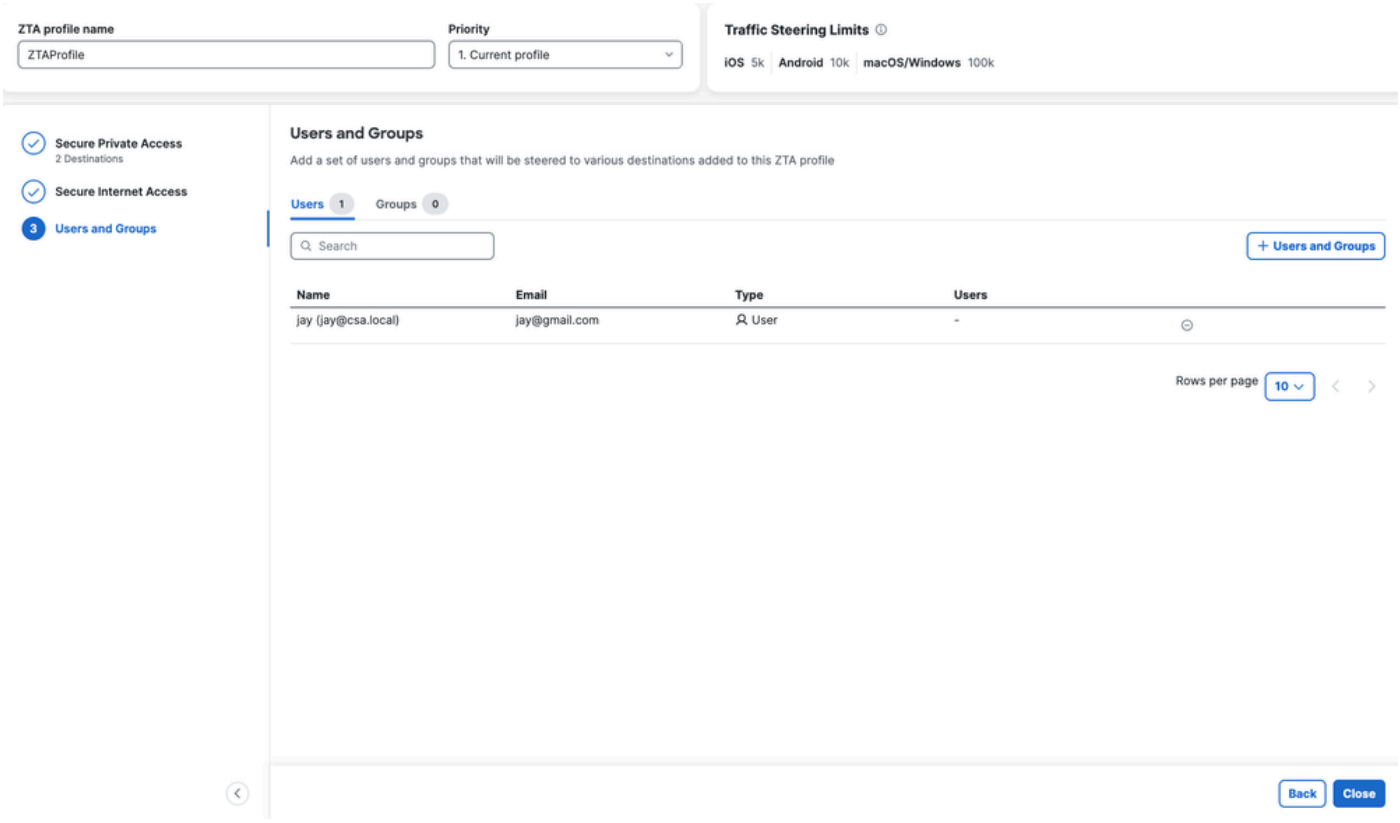


Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi



Accesso sicuro - Profilo ZTA



Accesso sicuro - Profilo ZTA

Fase - 5 Verifica dell'accesso alla risorsa privata

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

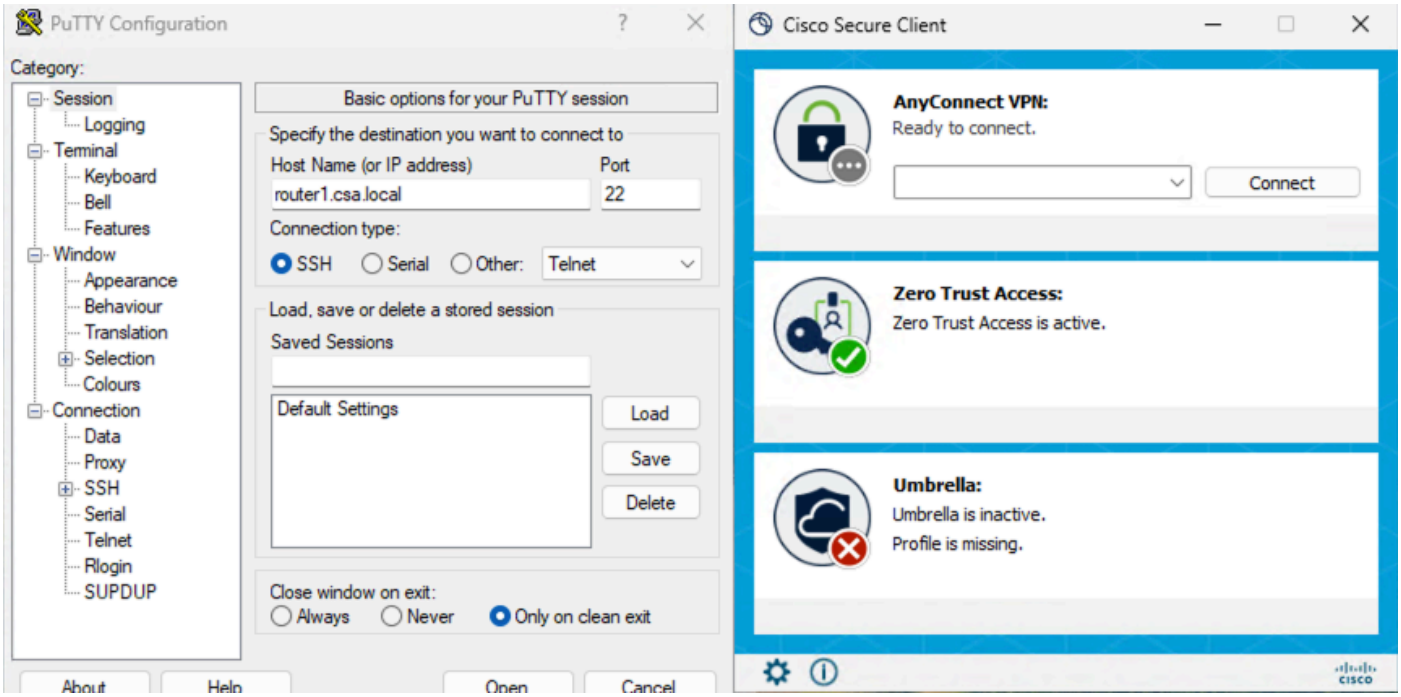
```
PS C:\Users\jay> ping ftd.csa.local

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
```

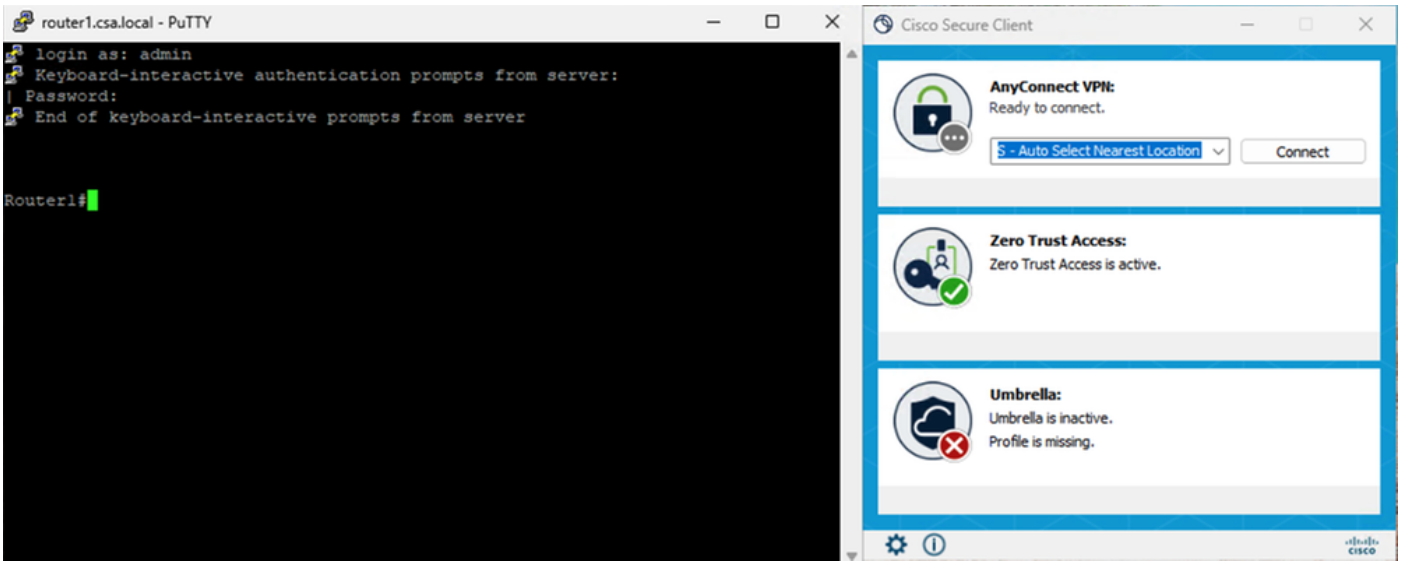
2. Verificare che l'FTD possa raggiungere la risorsa privata utilizzando il nome di dominio completo

```
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#
```


3. Eseguire il test della connessione SSH alla risorsa privata

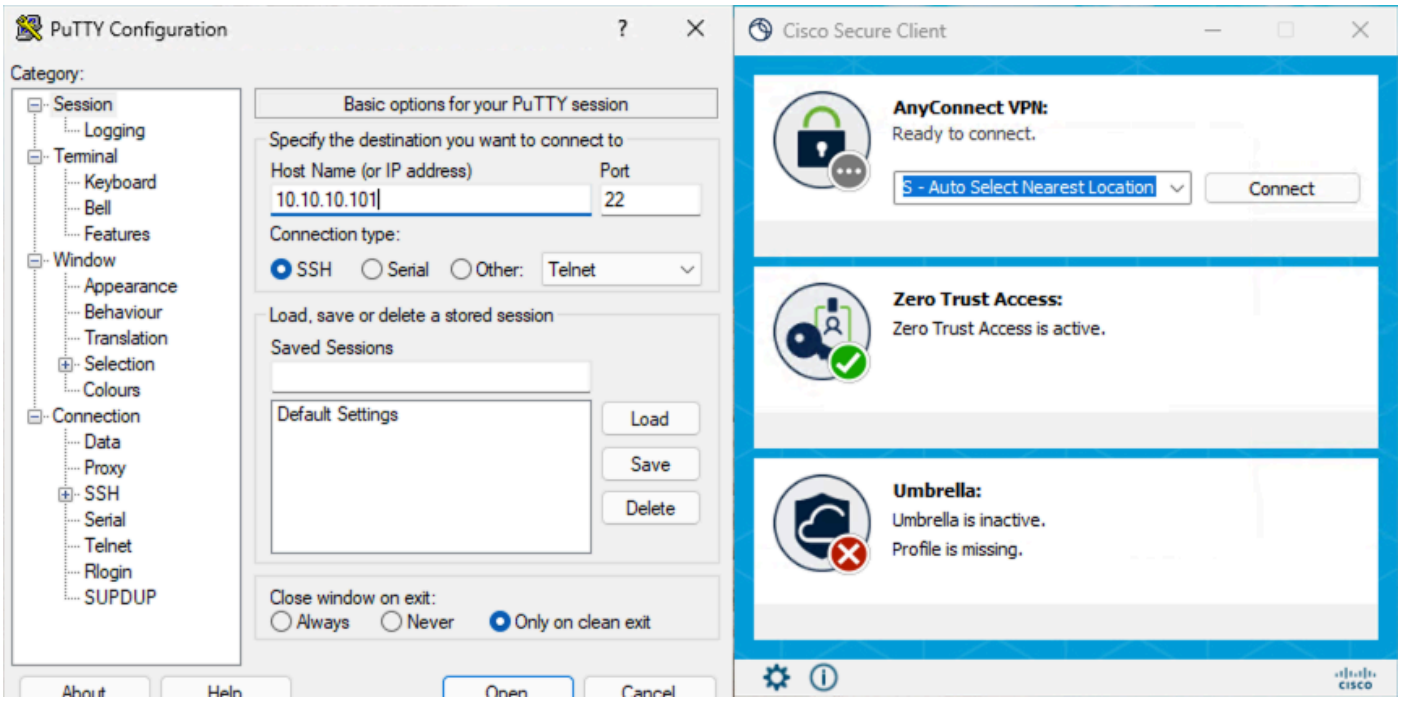
Accedere alla prenotazione permanente utilizzando FQDN



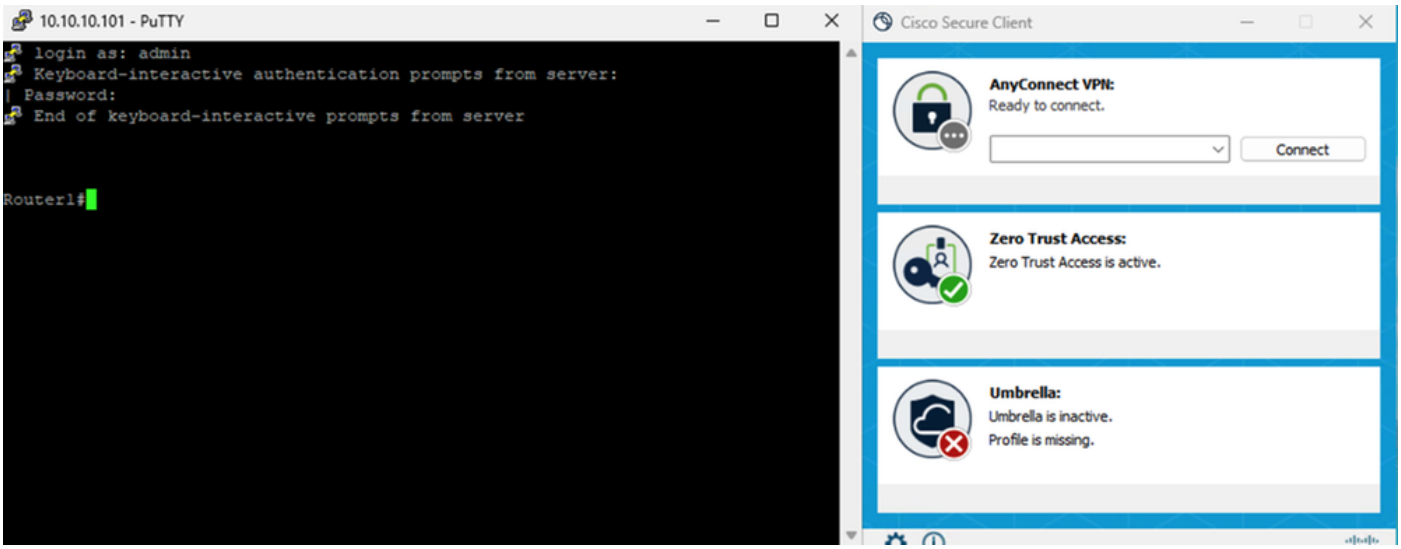


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP

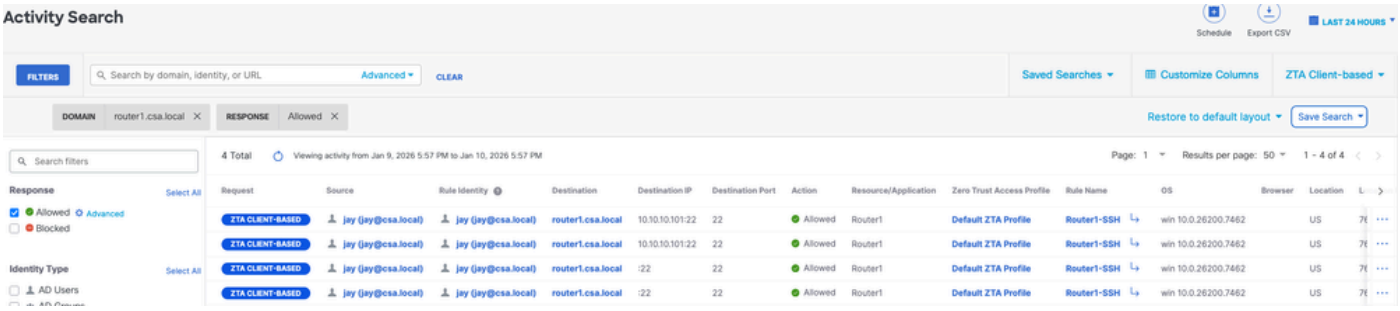


Accesso sicuro - Test PR

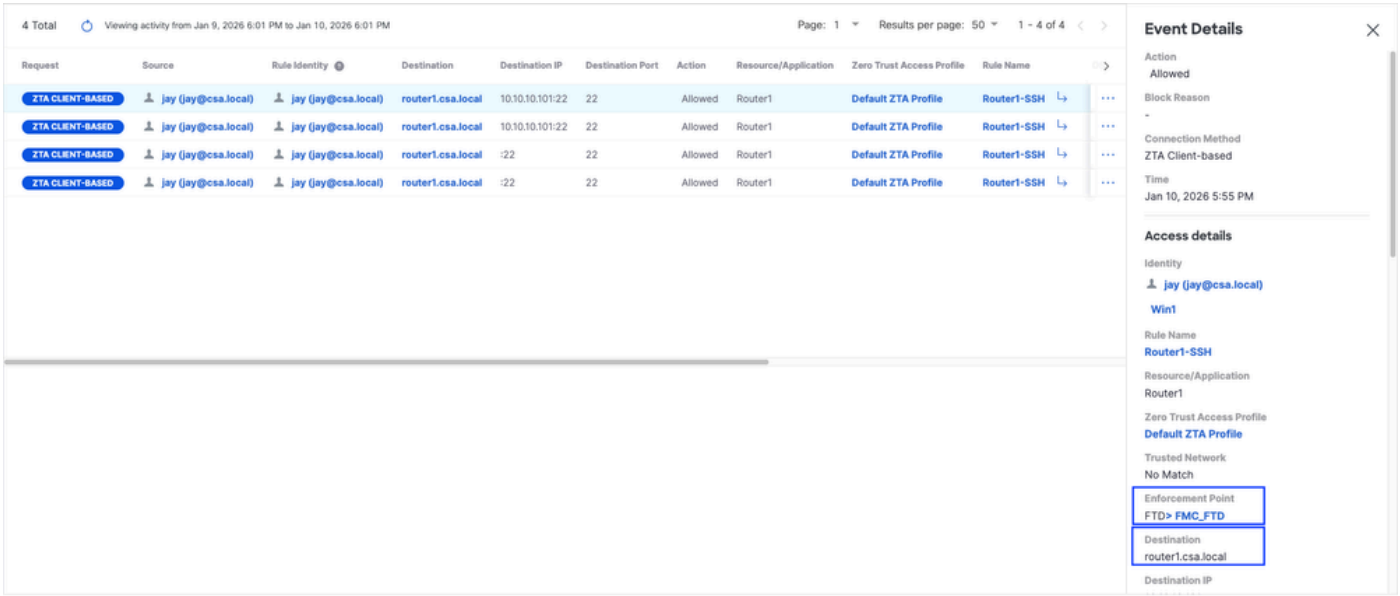


Accesso sicuro - Test PR

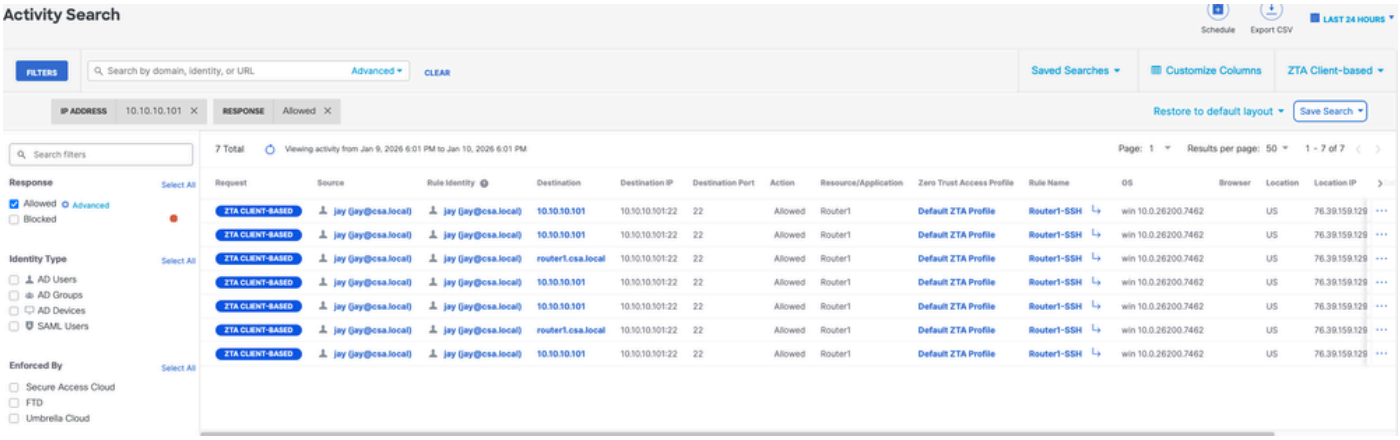
4. Verifica registri di ricerca attività accesso sicuro



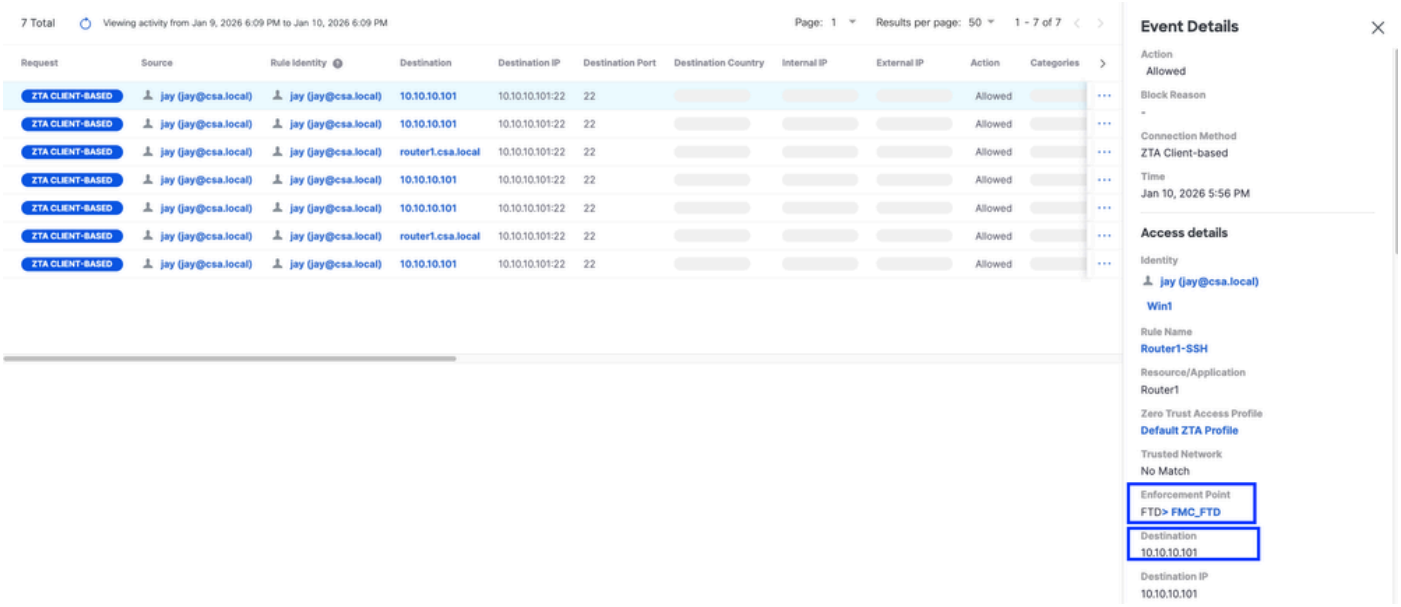
Accesso sicuro - Ricerca attività



Accesso sicuro - Ricerca attività

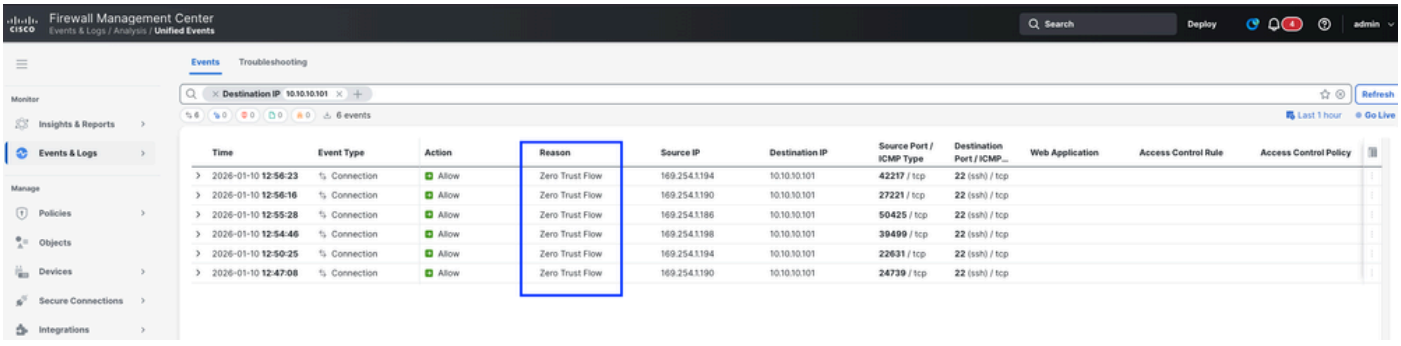


Accesso sicuro - Ricerca attività



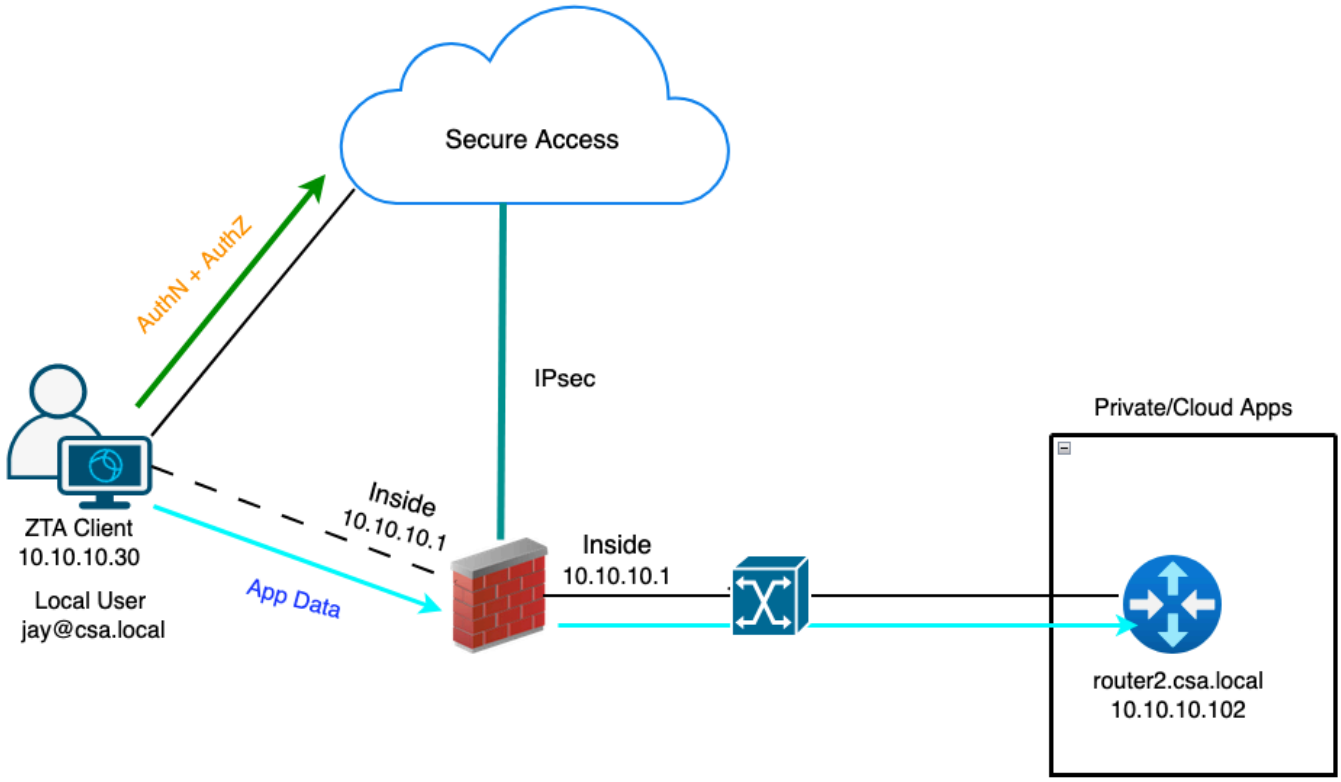
Accesso sicuro - Ricerca attività

5. Verificare gli eventi di connessione FMC



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.

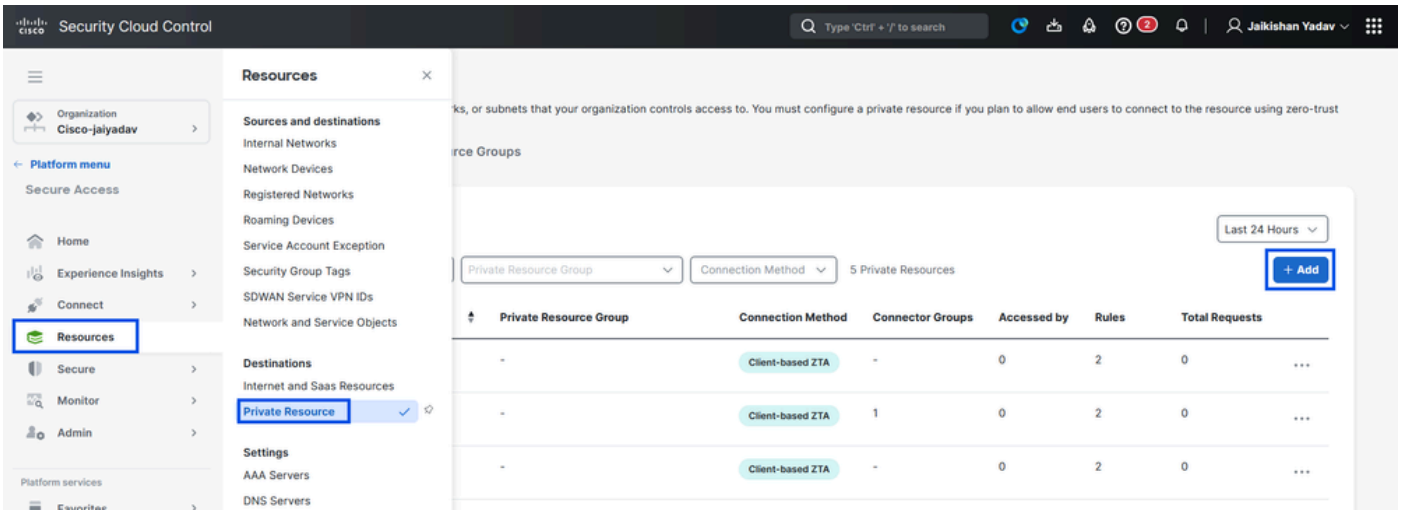


Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

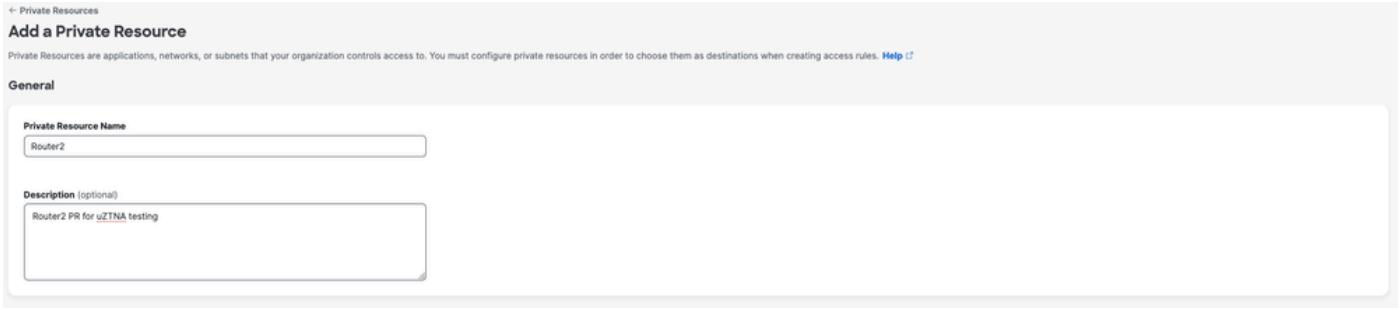
Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

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



Accesso sicuro - Configurazione risorse private

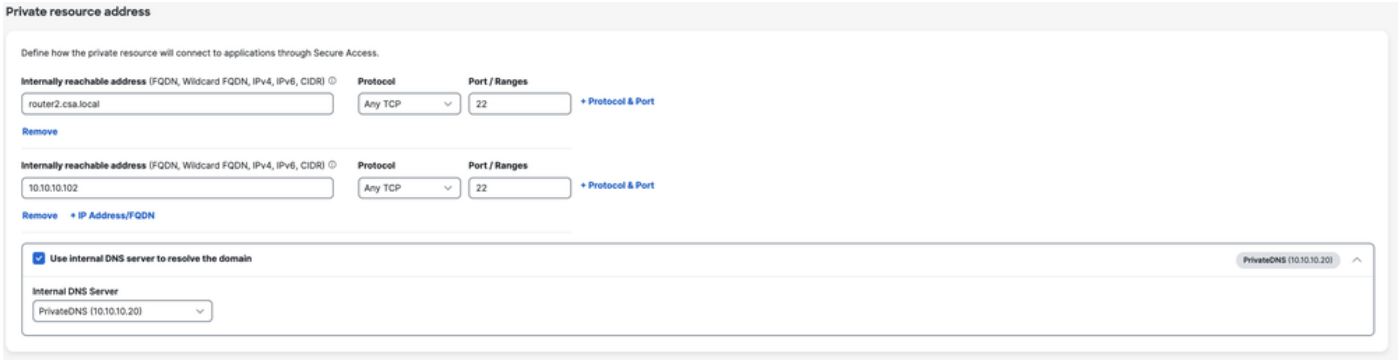
2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.



Accesso sicuro - Configurazione risorse private

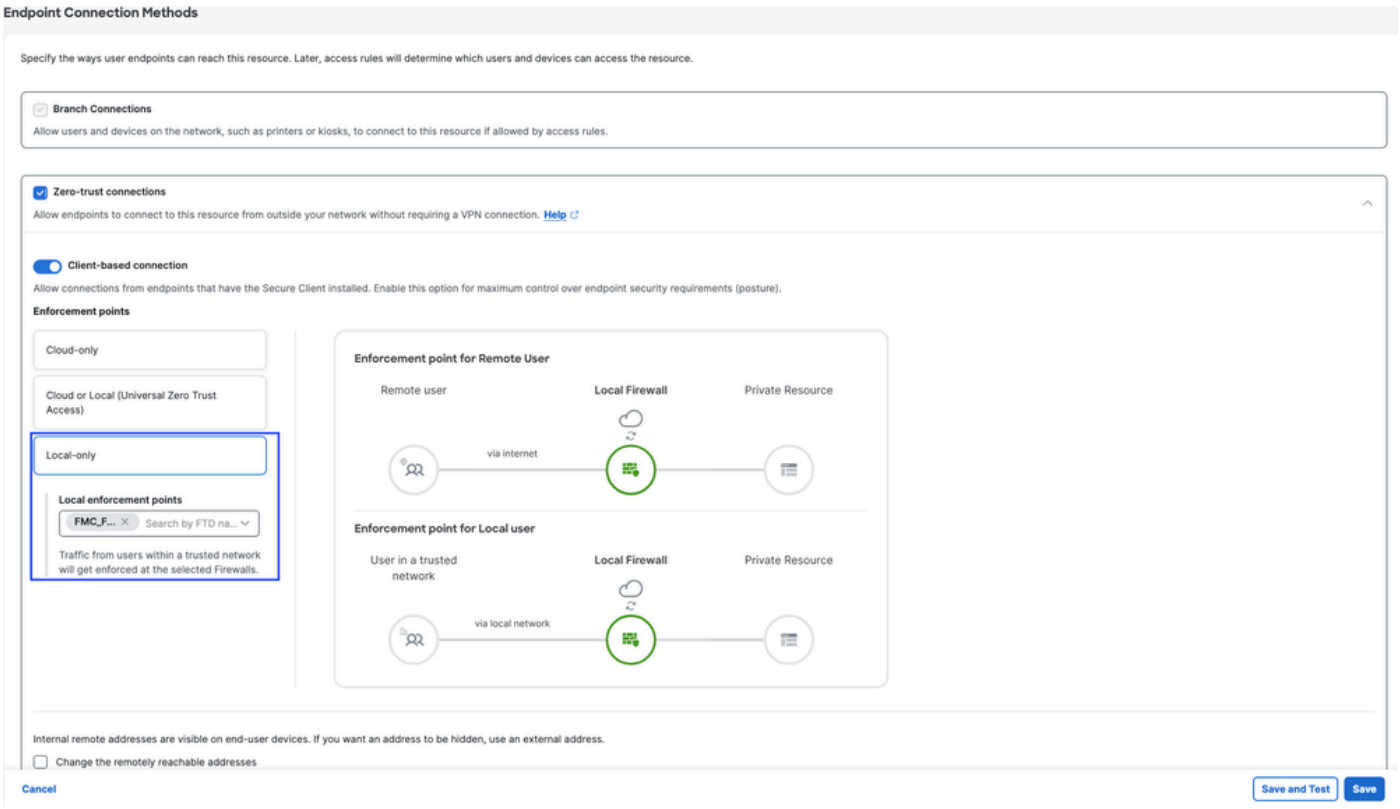
3. Inserire il nome di dominio completo (FQDN) della risorsa privata a cui si desidera accedere. È inoltre possibile definire l'indirizzo IP della risorsa privata. Per ulteriori informazioni, vedere [Aggiungere una risorsa privata]

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



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

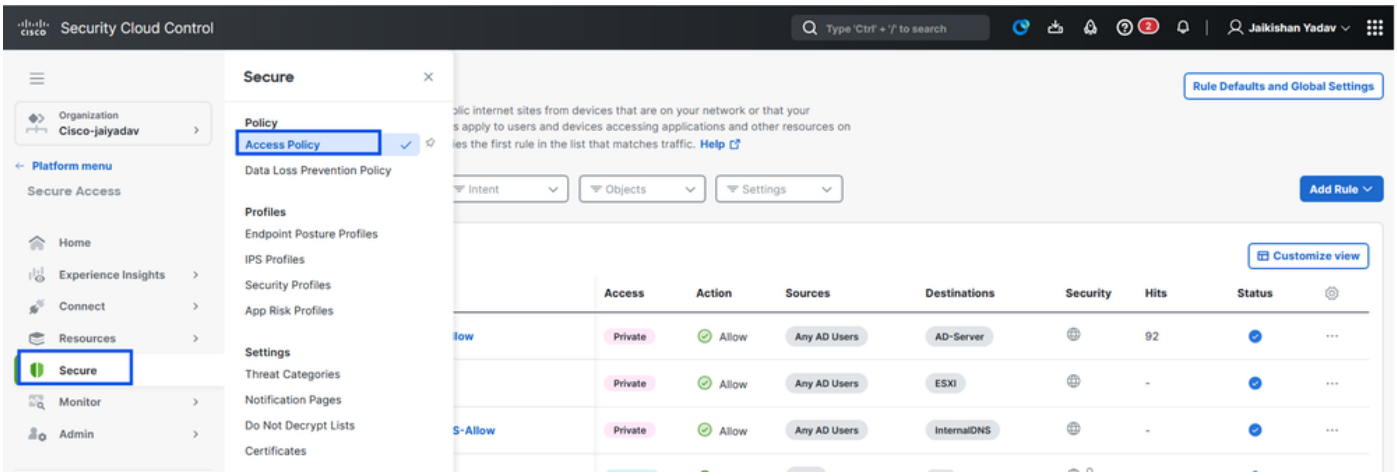
---

7. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

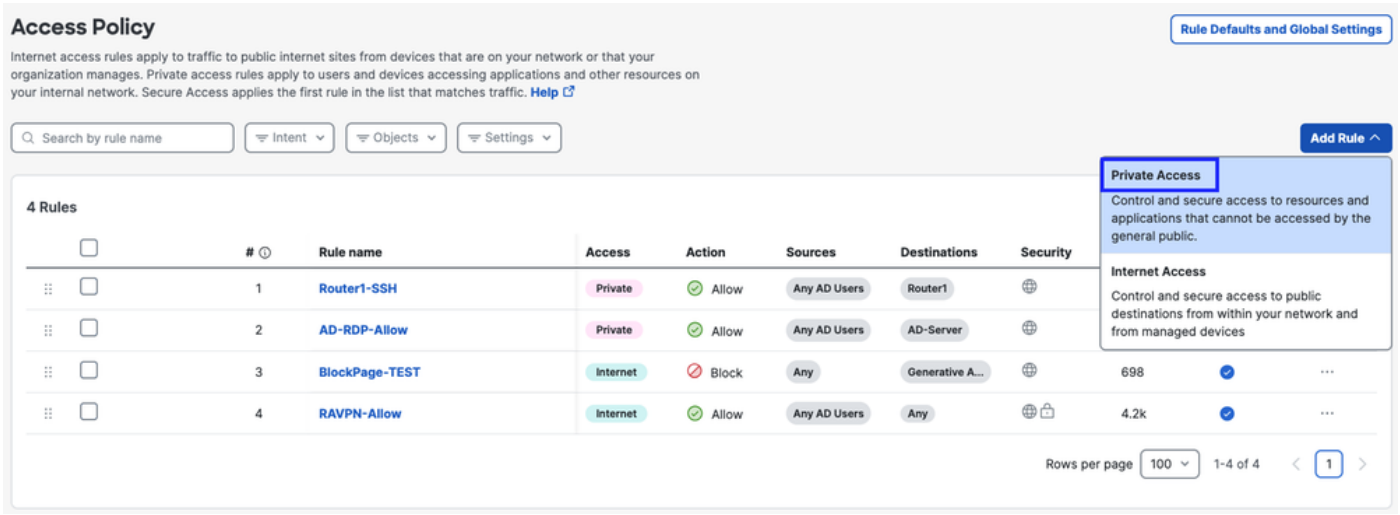
Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere Regola di accesso privato

1. Passare a Protezione > Criteri di accesso



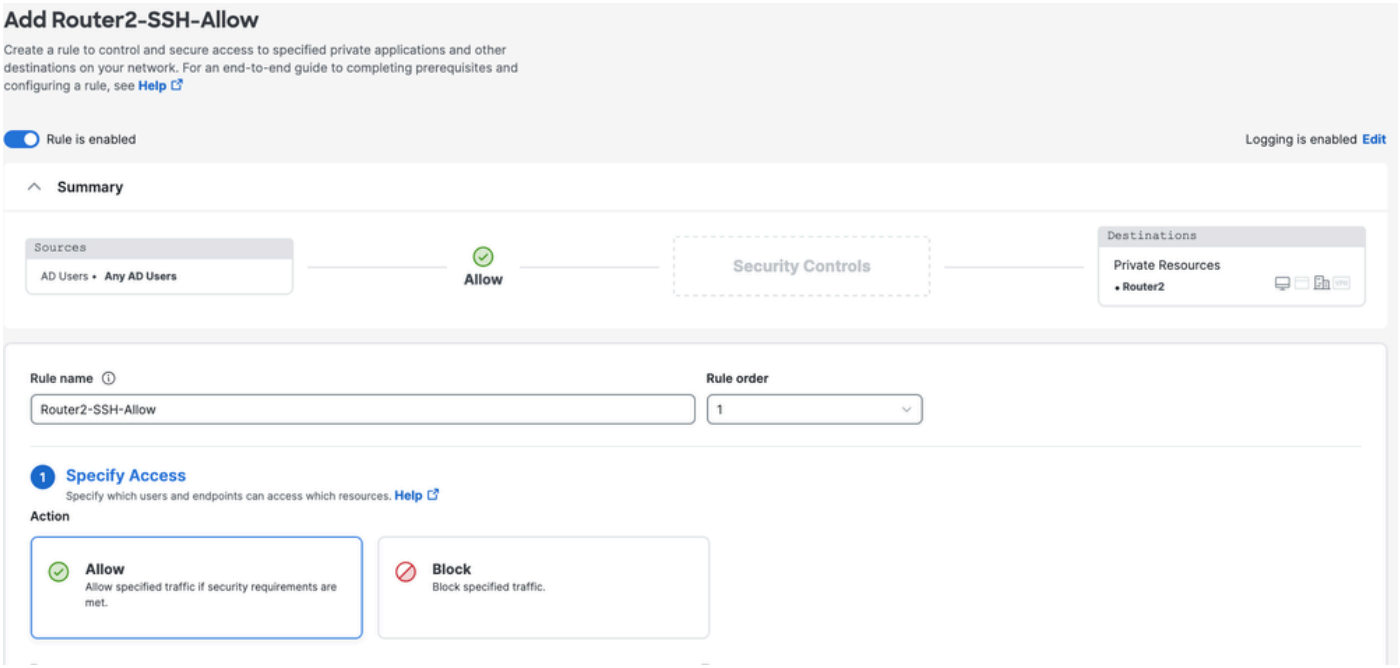
Accesso sicuro - Configurazione criteri di accesso

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.



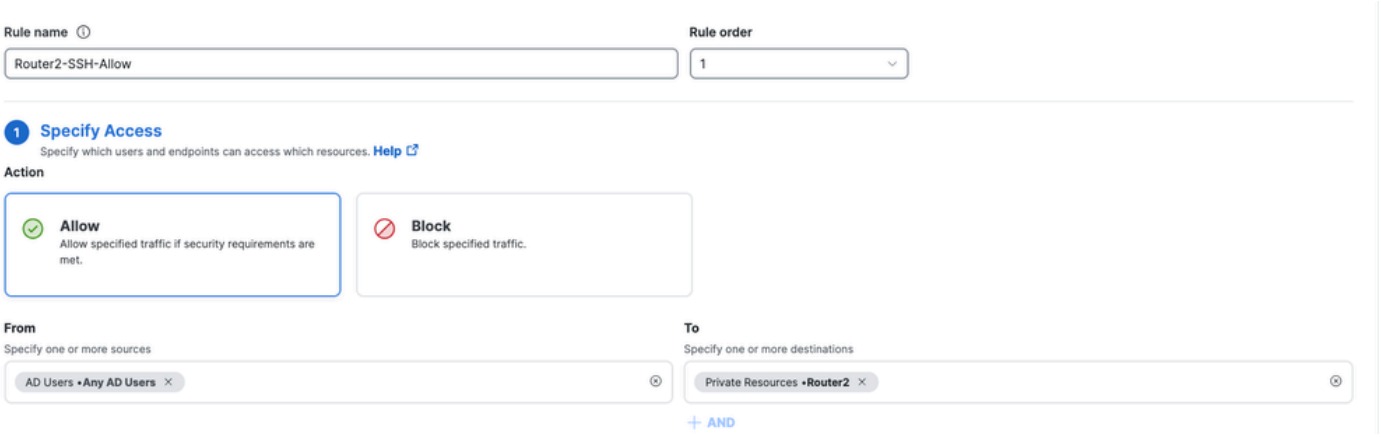
Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola



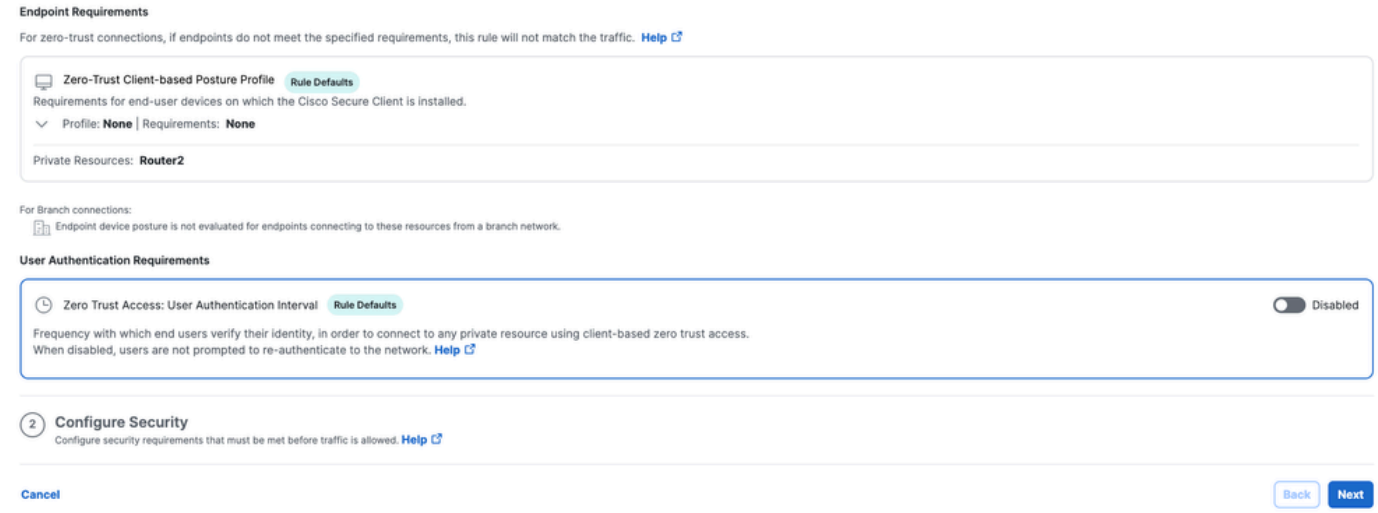
Accesso sicuro - Configurazione criteri di accesso

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



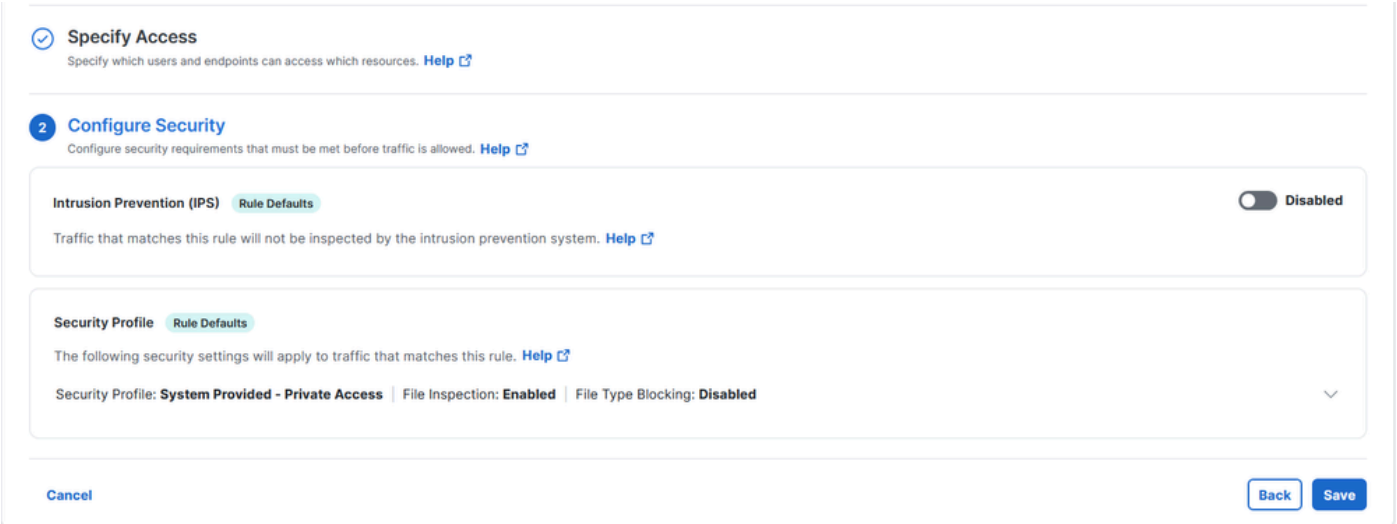
Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint



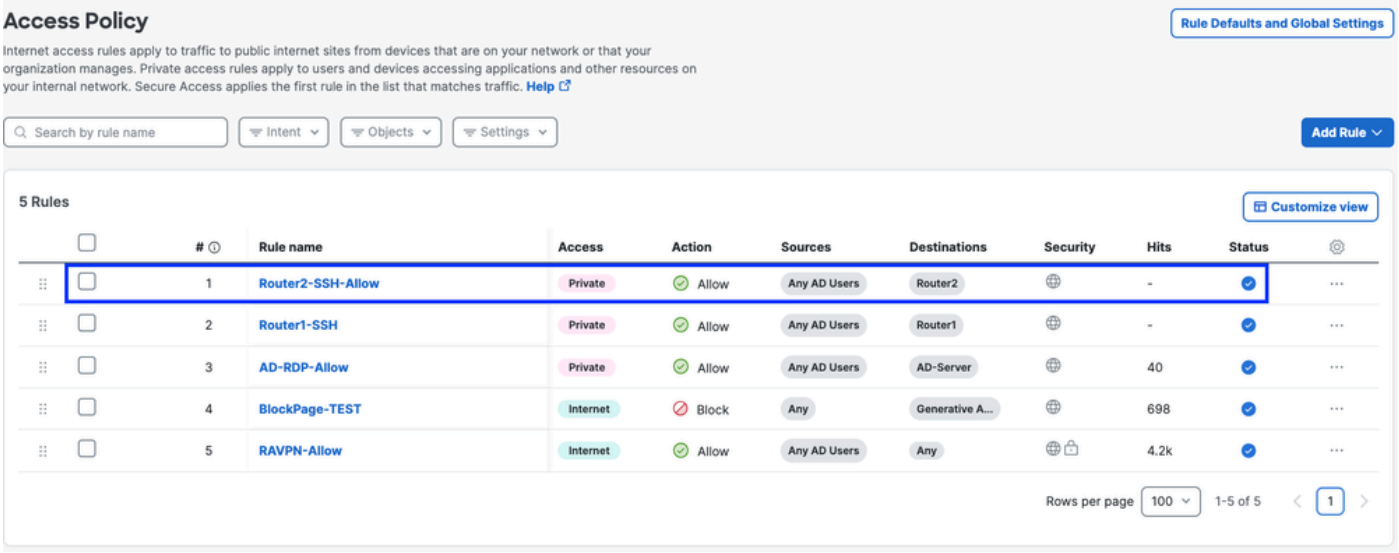
Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione



Accesso sicuro - Configurazione criteri di accesso

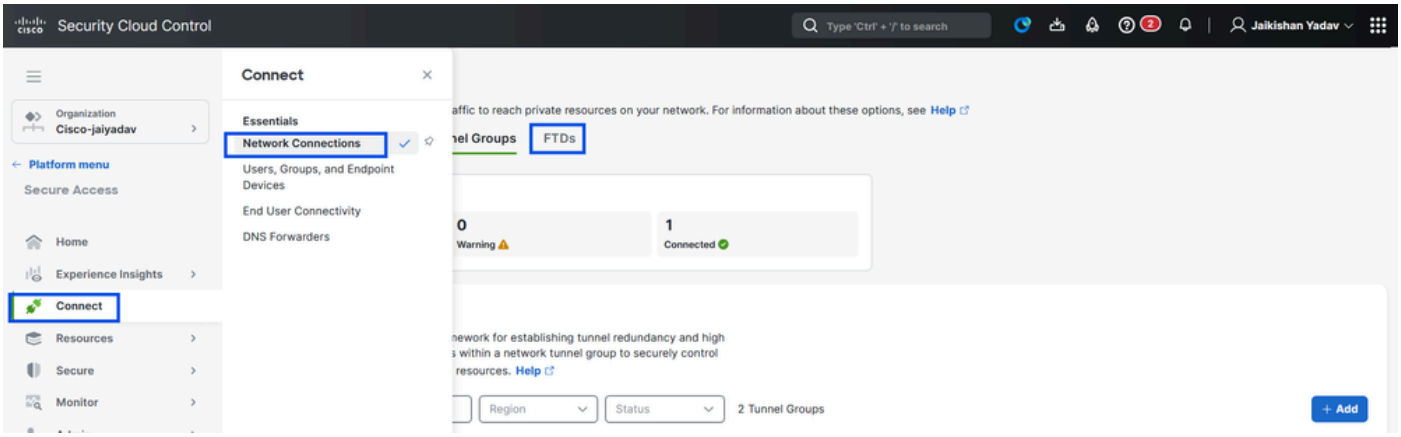
7. Fare clic su Save (Salva)



Accesso sicuro - Configurazione criteri di accesso

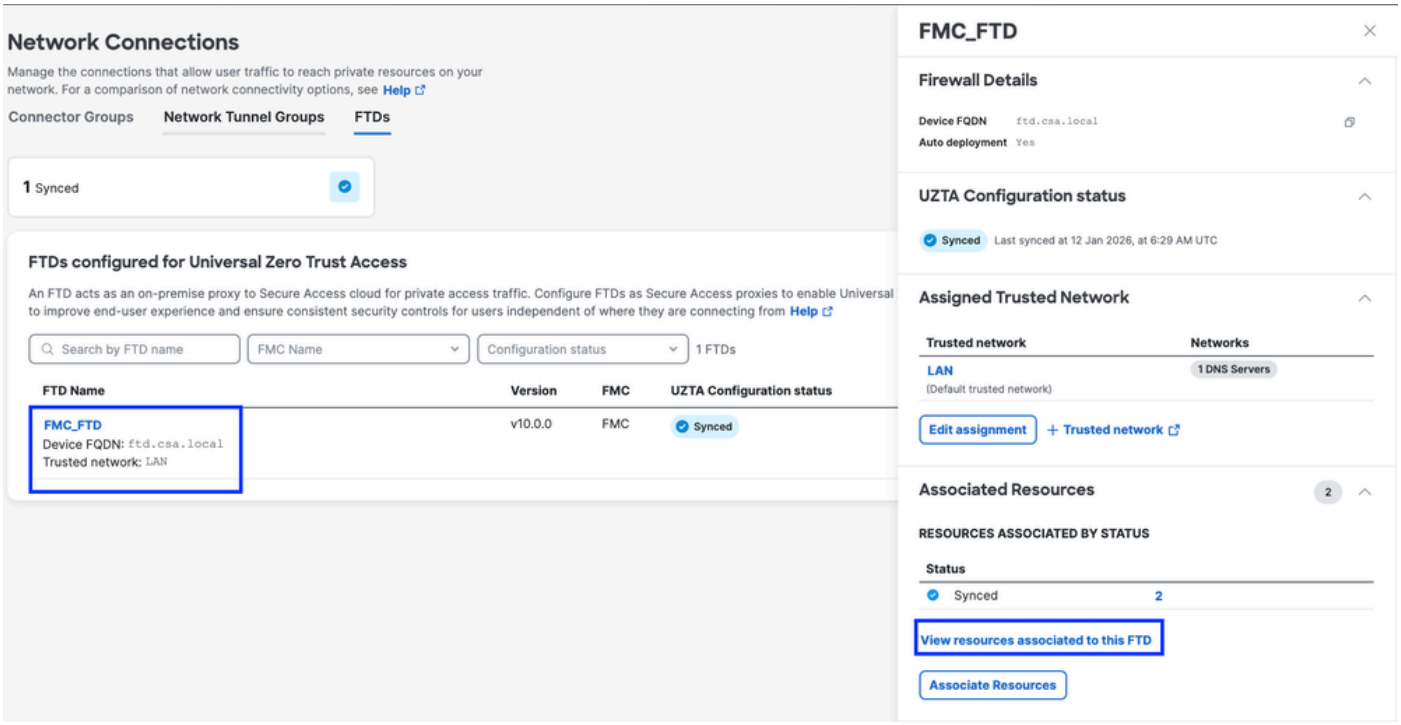
Fase 3 - Verifica dell'associazione di PR sull'FTD

1. Passare a connessione > Connessioni di rete > FTD

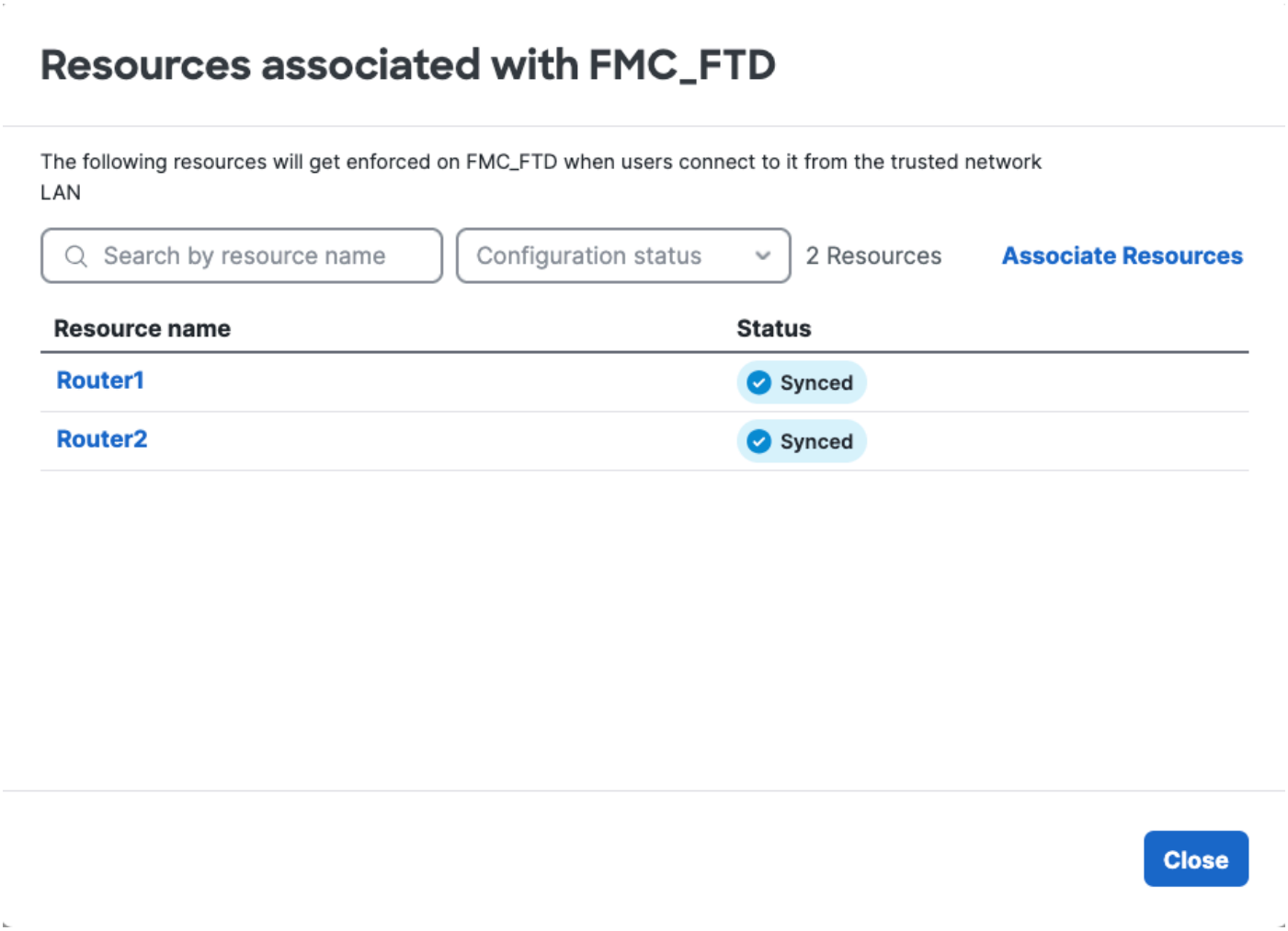


Accesso sicuro - Verifica PR

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

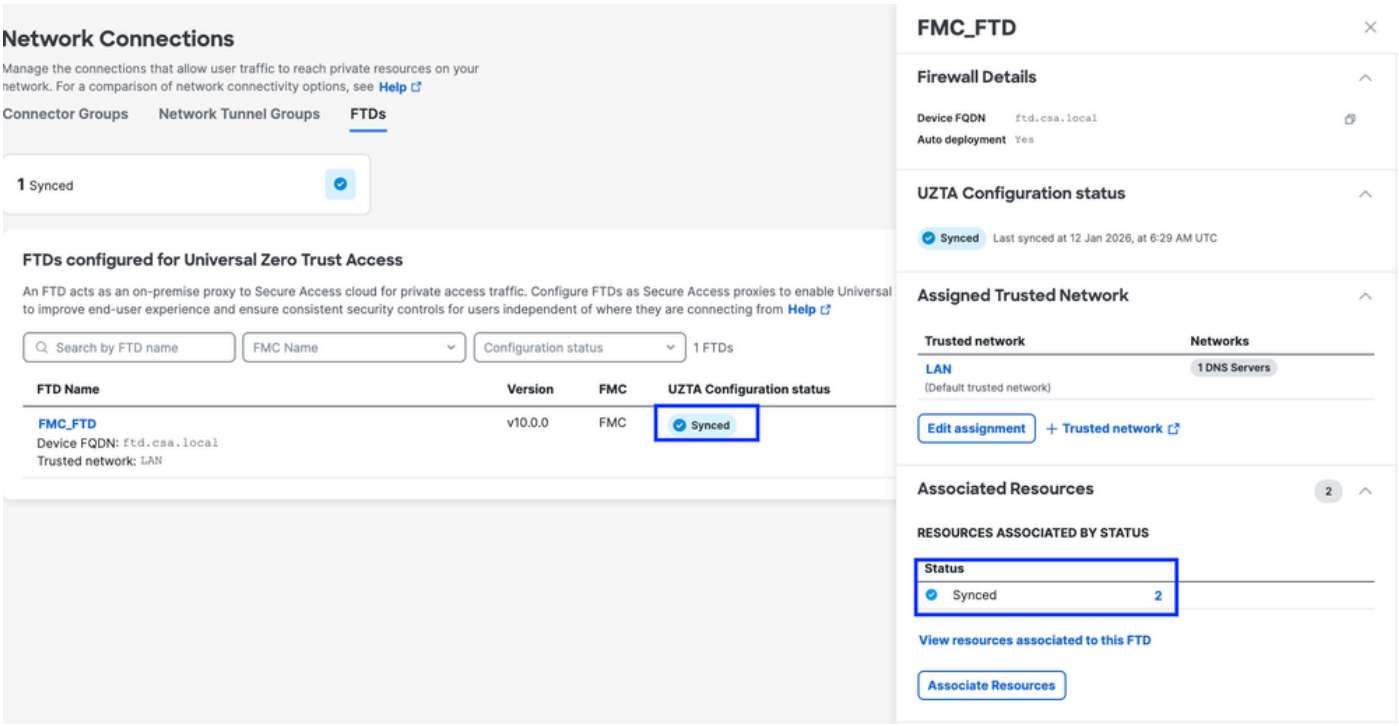


Accesso sicuro - Verifica PR



3. Fare clic su chiudi

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



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

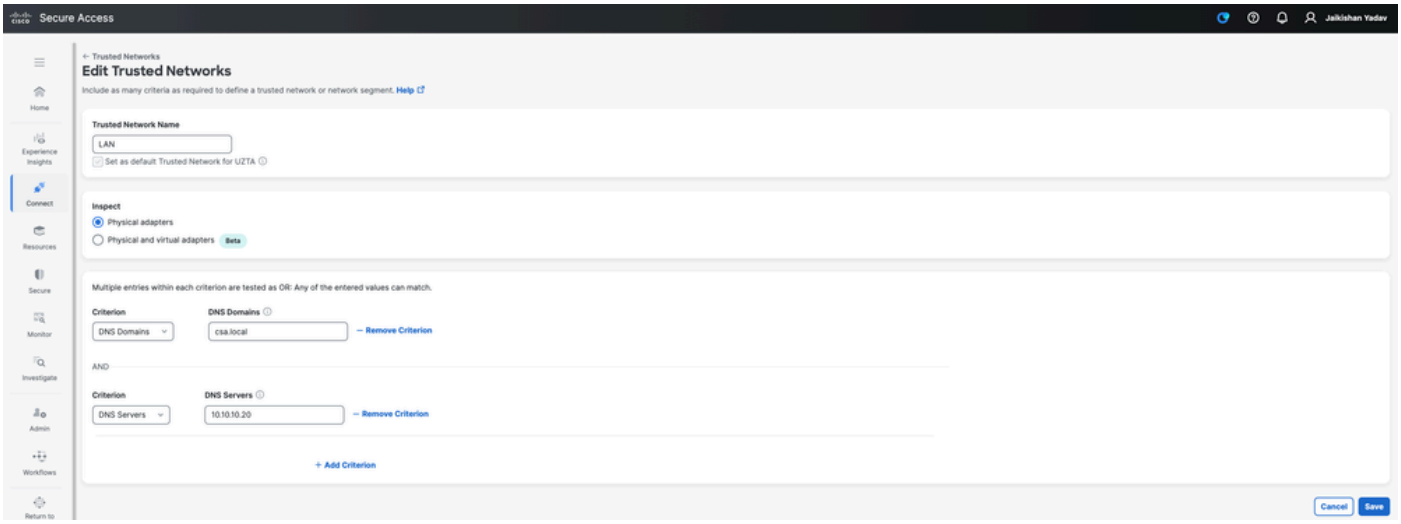
show running-config applicazione oggetto

```
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"

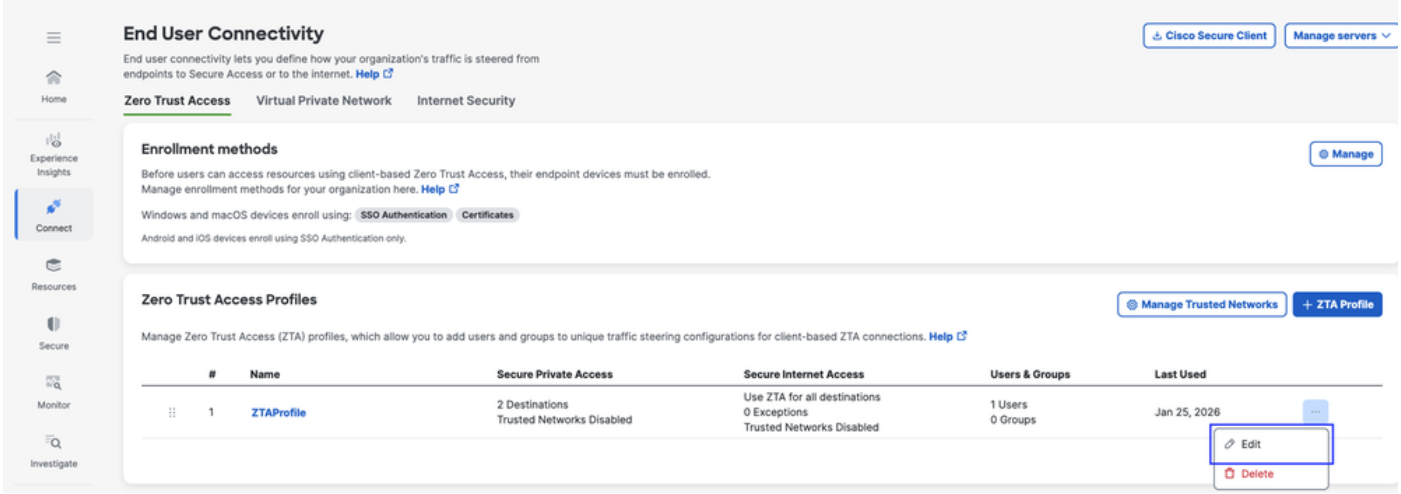
Selezionare Connetti > Connettività utente finale > Accesso con attendibilità totale > Impostazioni ZTA e configurare Reti attendibili



Accesso sicuro - Configurazione TND

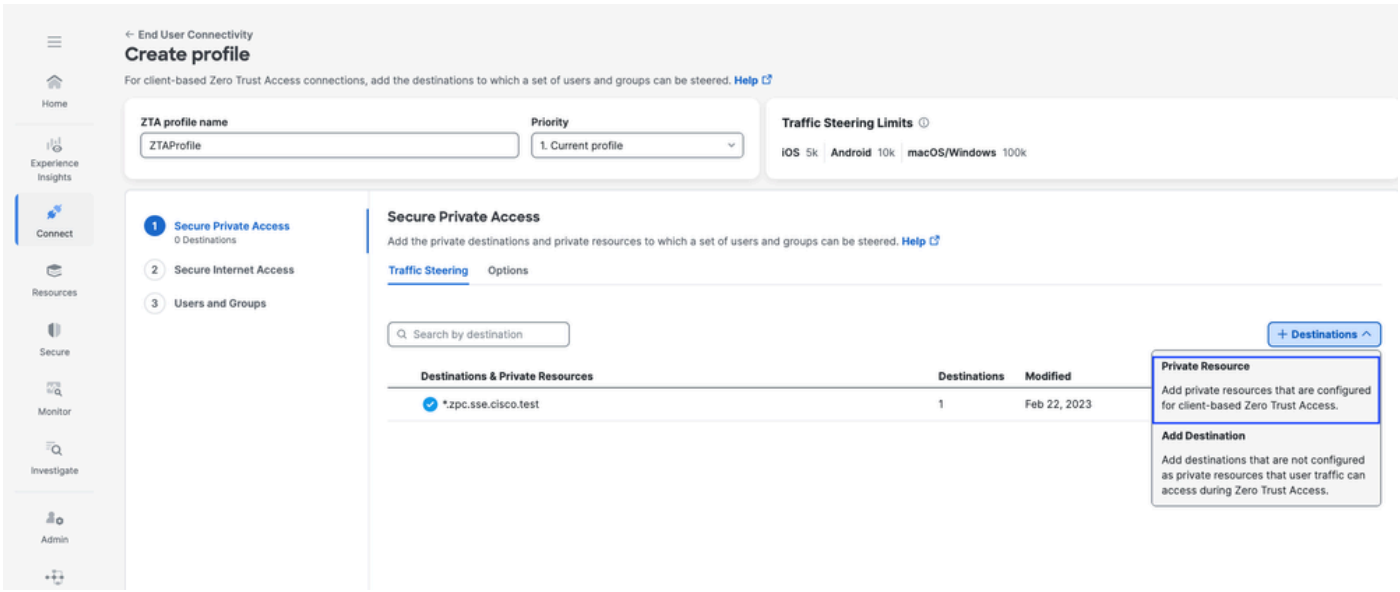
Fase -5 Aggiungere una risorsa privata al profilo ZTA

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

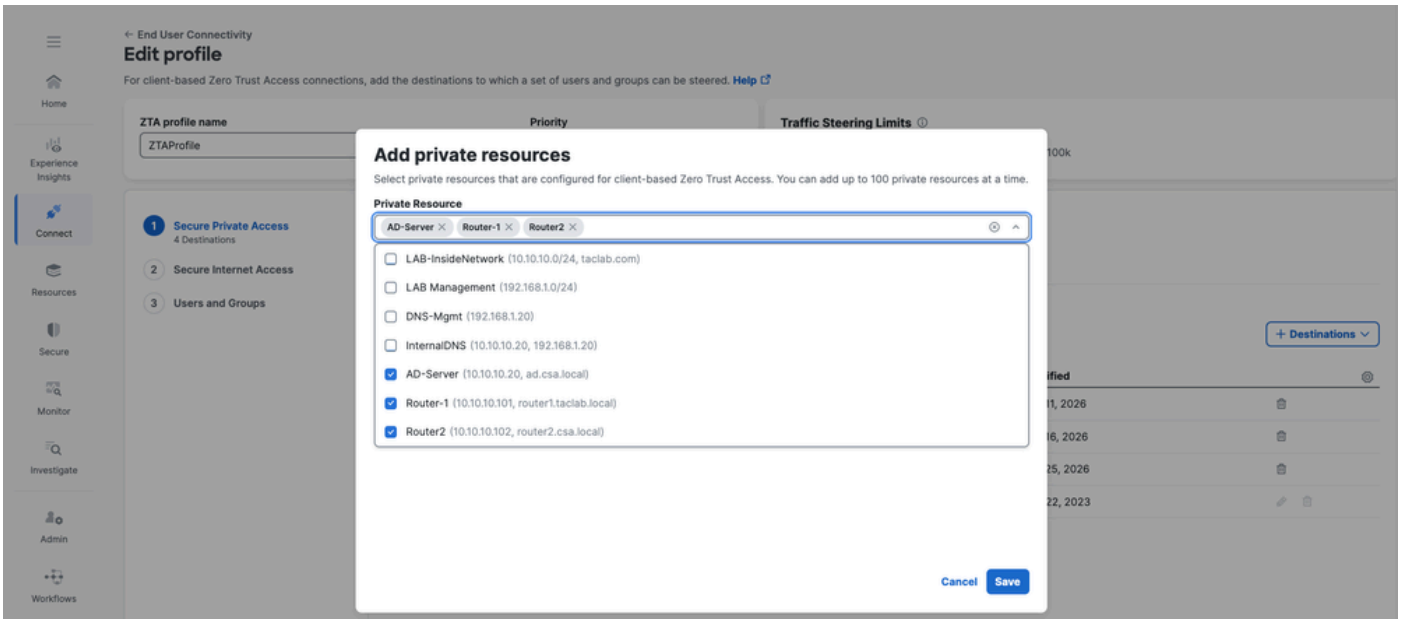


Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

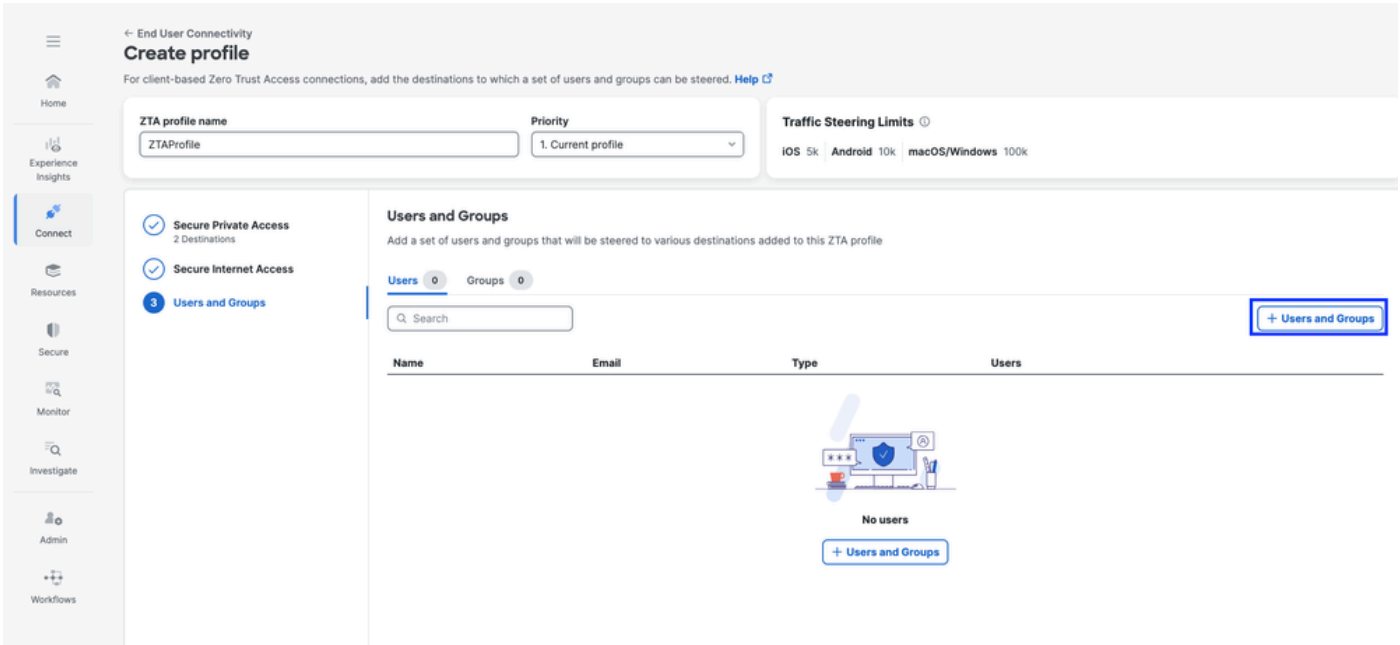


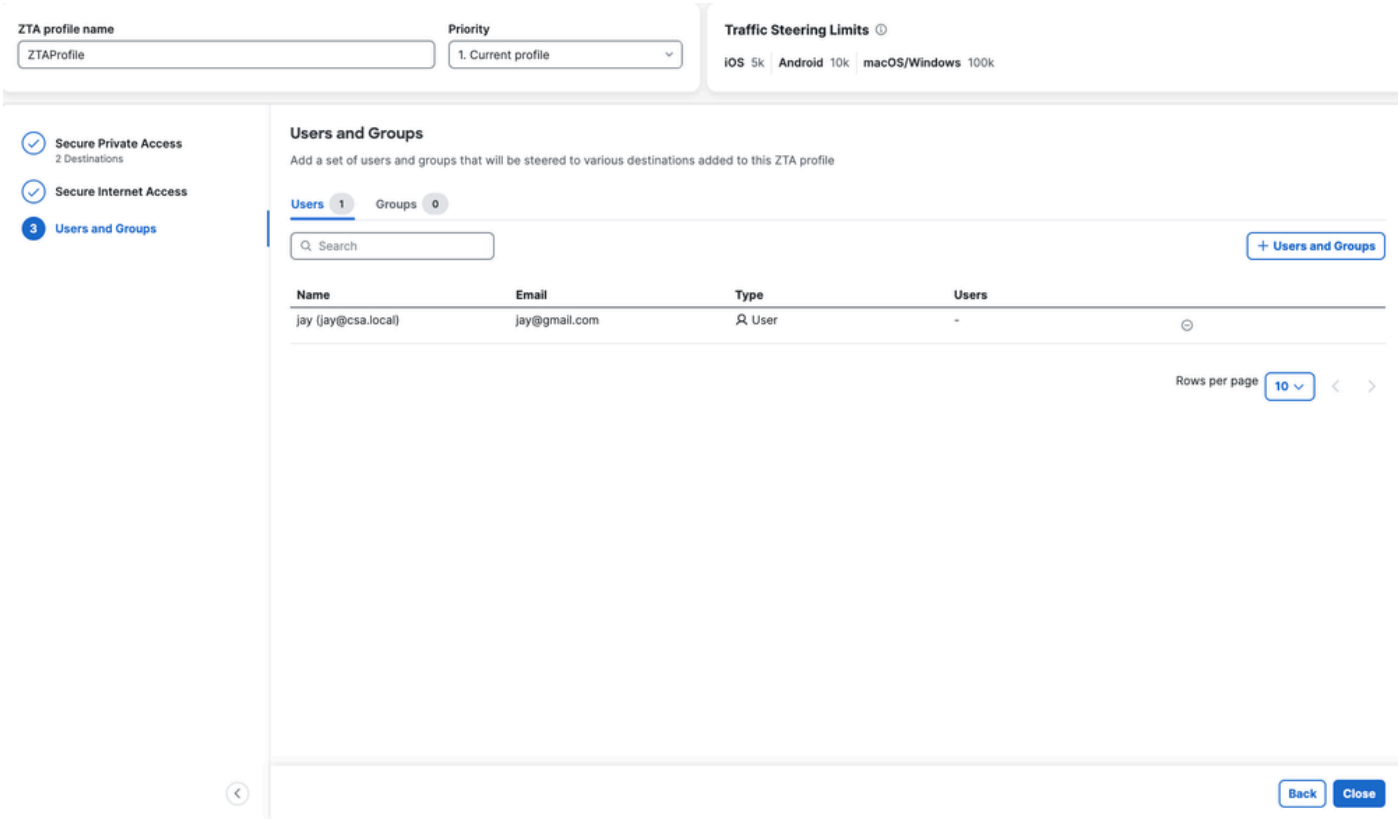
Accesso sicuro - Profilo ZTA



Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi

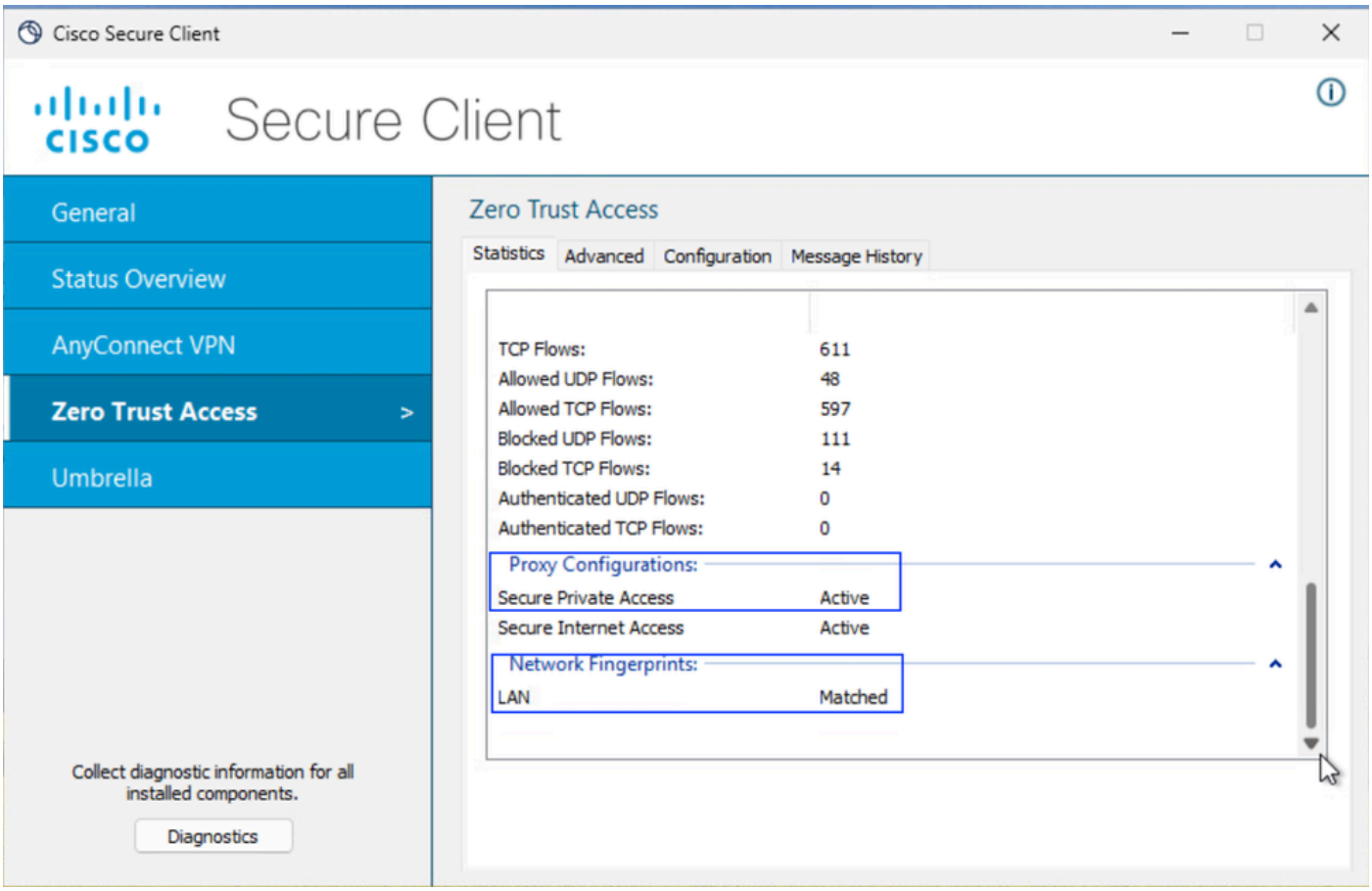




Accesso sicuro - Profilo ZTA

Fase - 6 Verifica dell'accesso alla risorsa privata

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



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

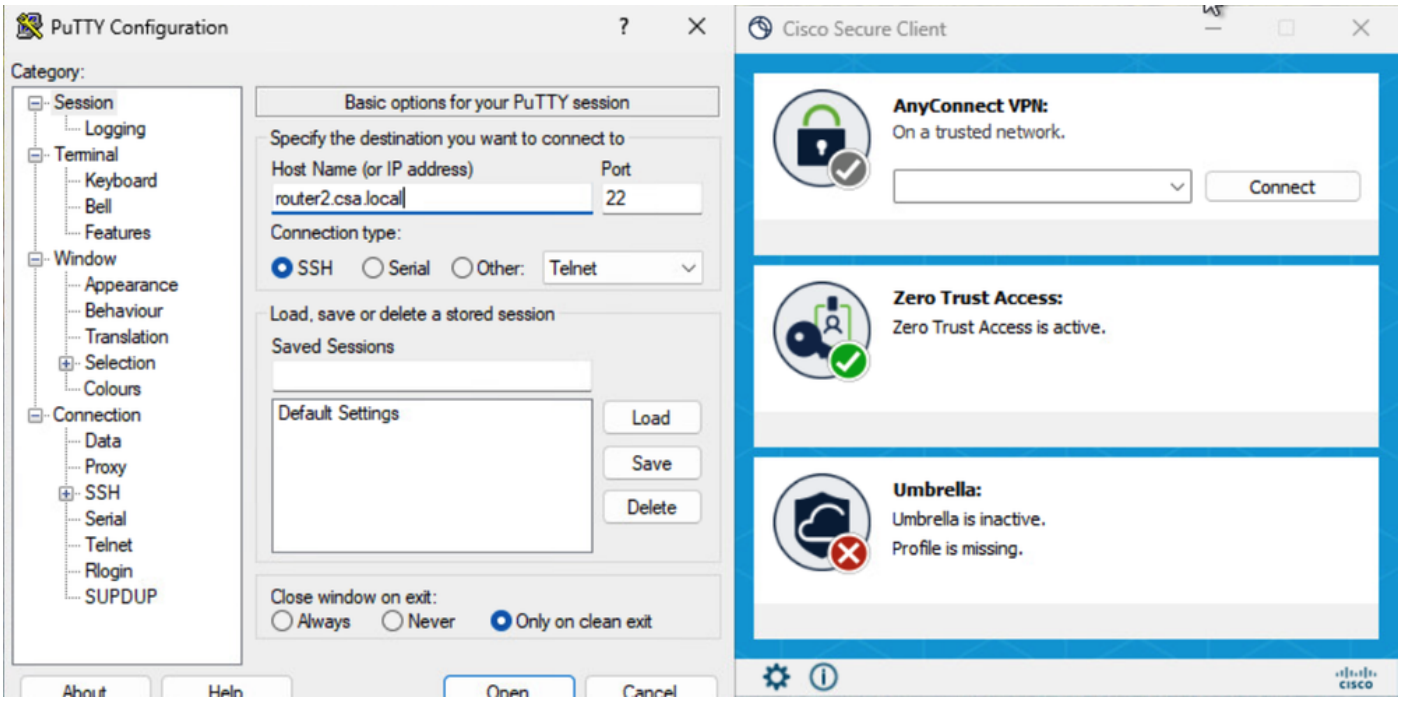
3. Verificare che l'FTD possa raggiungere la risorsa privata utilizzando l'FQDN

```
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#
```

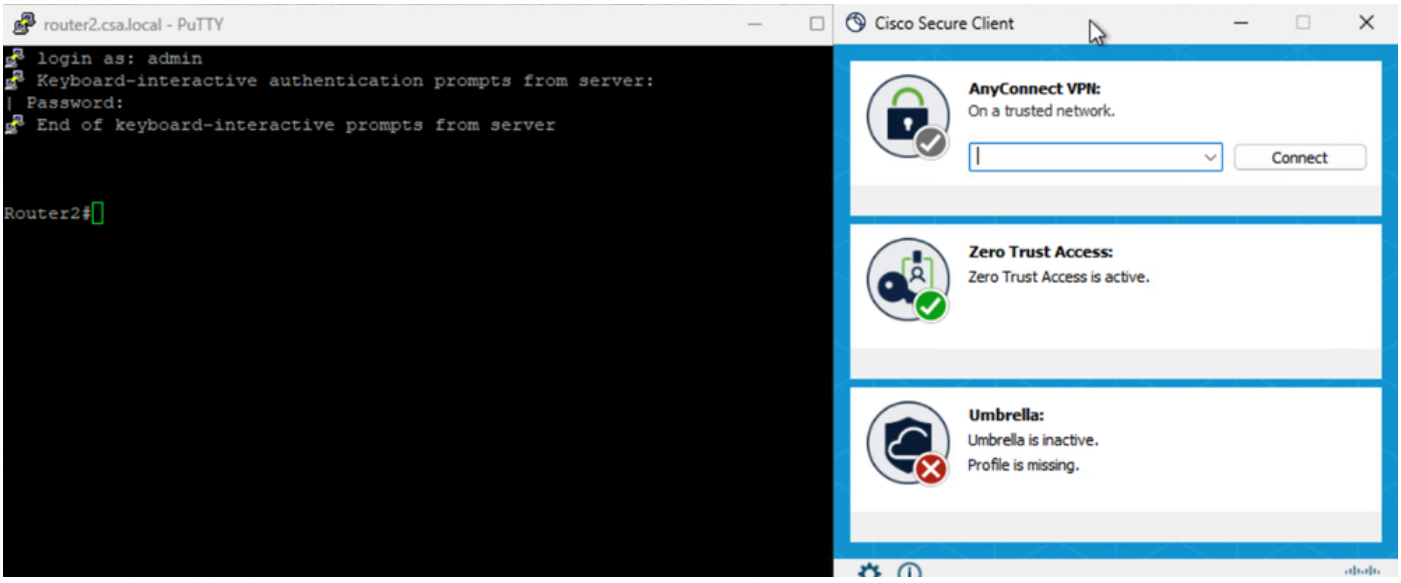
Accesso sicuro - Test PR

4. Eseguire il test della connessione SSH alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN

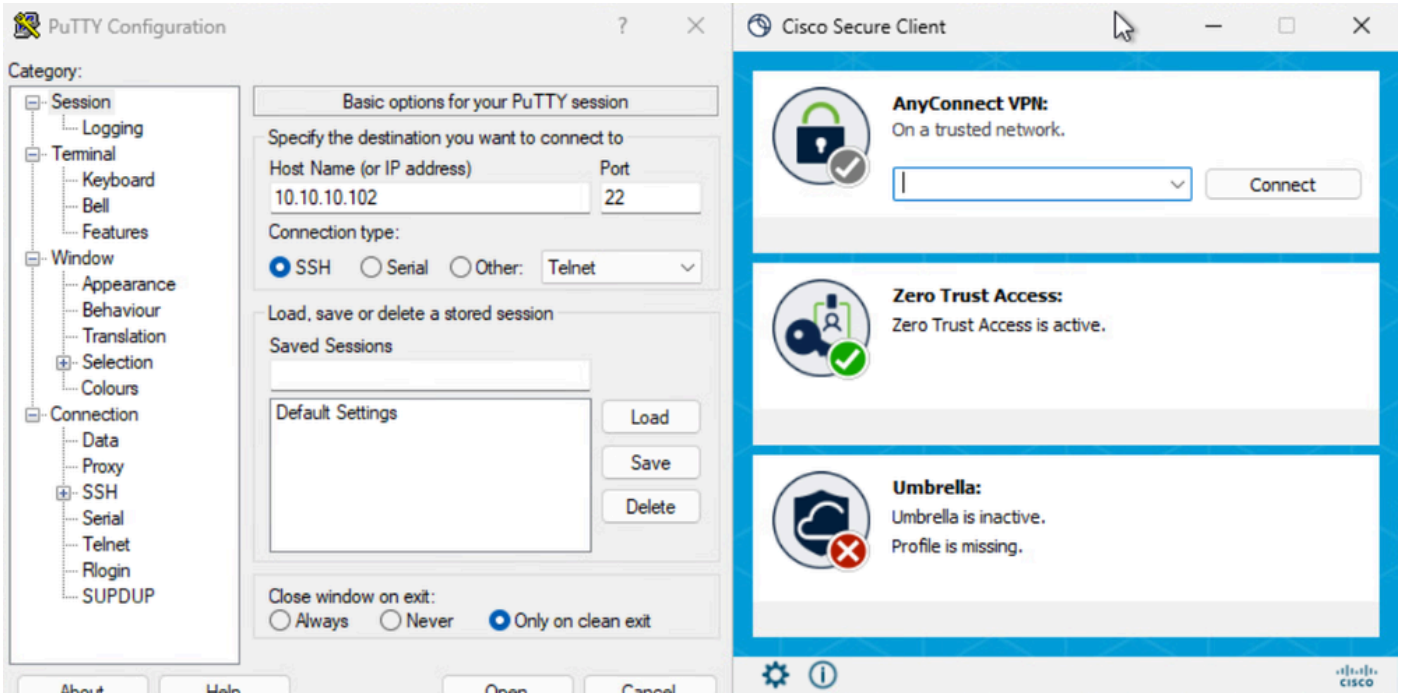


Accesso sicuro - Test PR

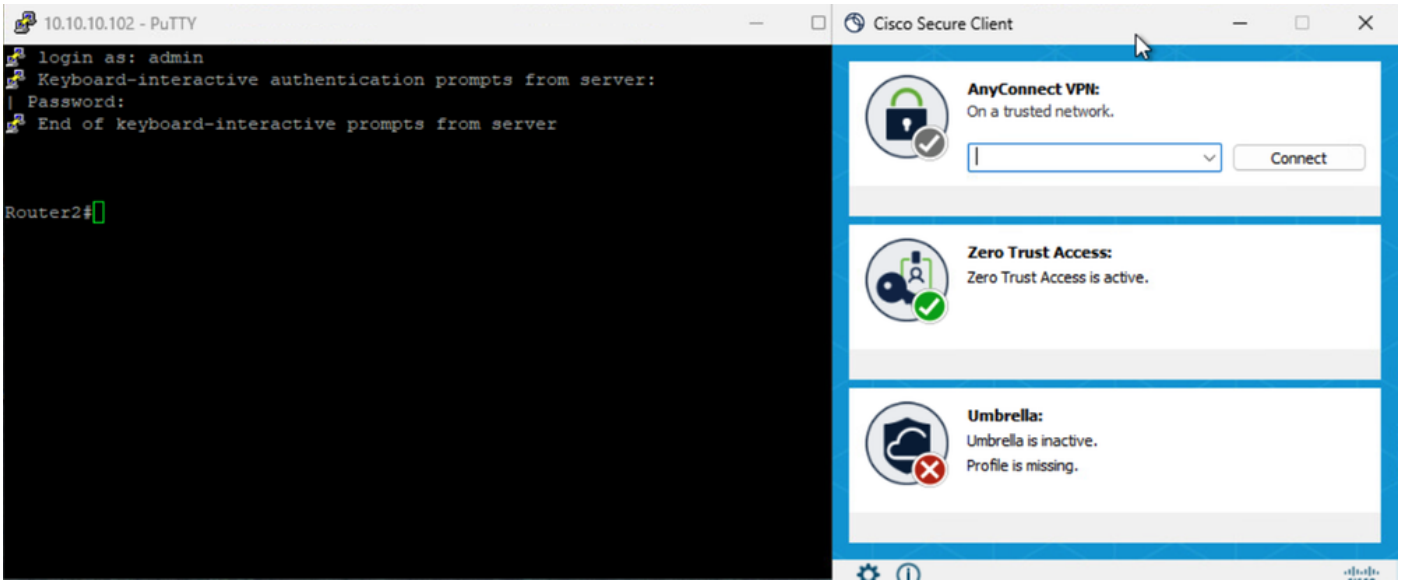


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP

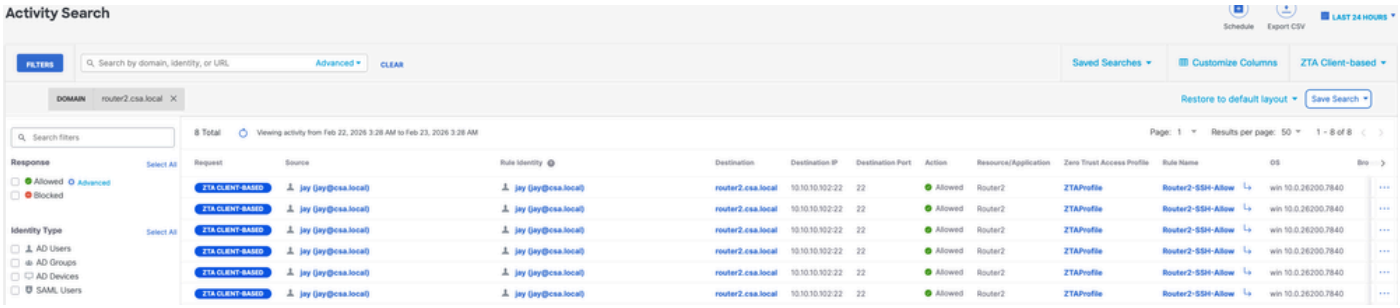


Accesso sicuro - Test PR

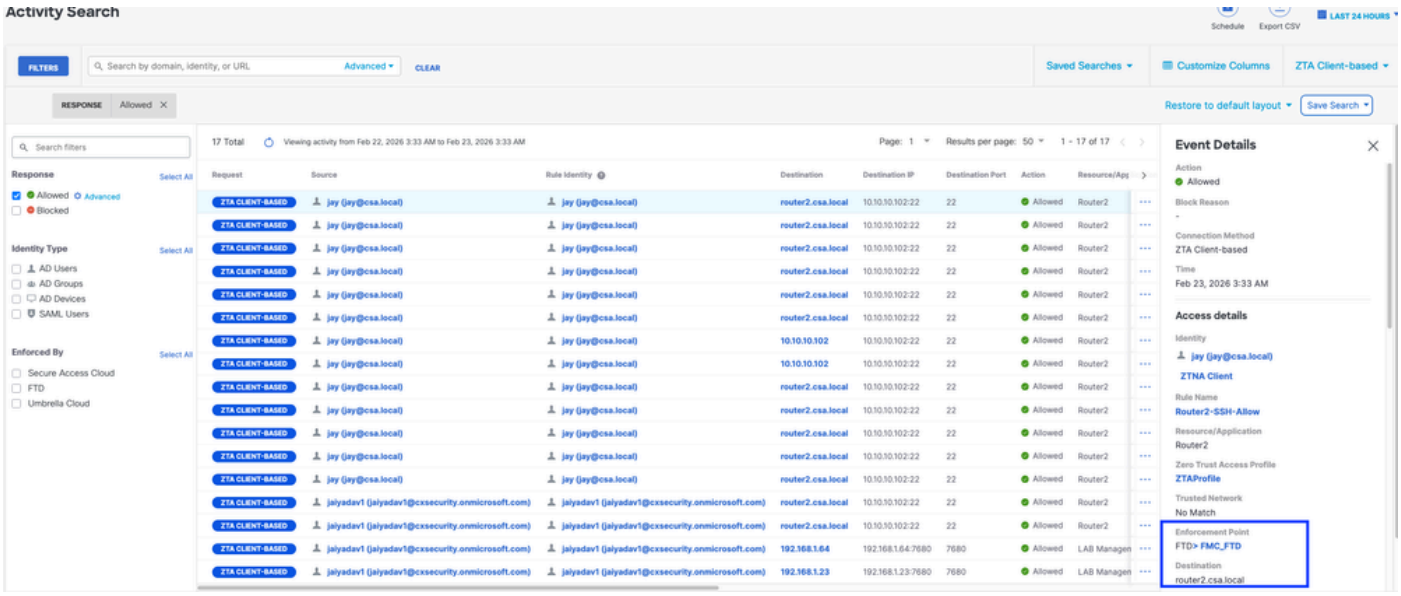


Accesso sicuro - Test PR

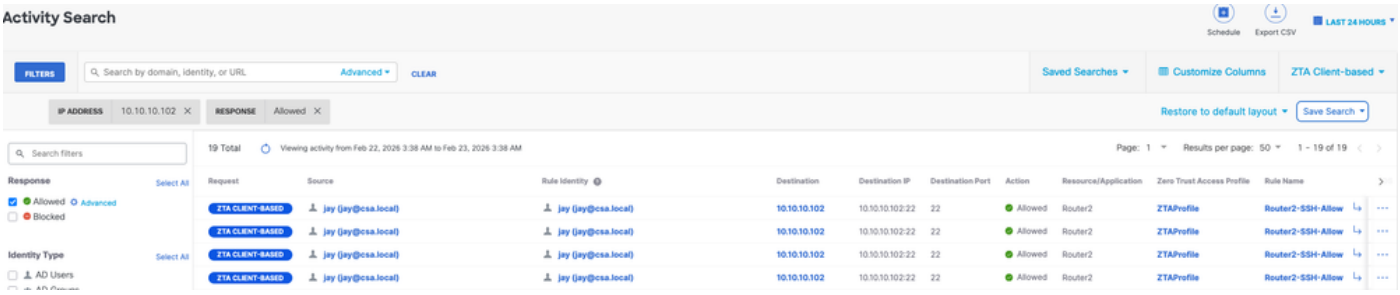
5. Verifica registri di ricerca attività accesso sicuro



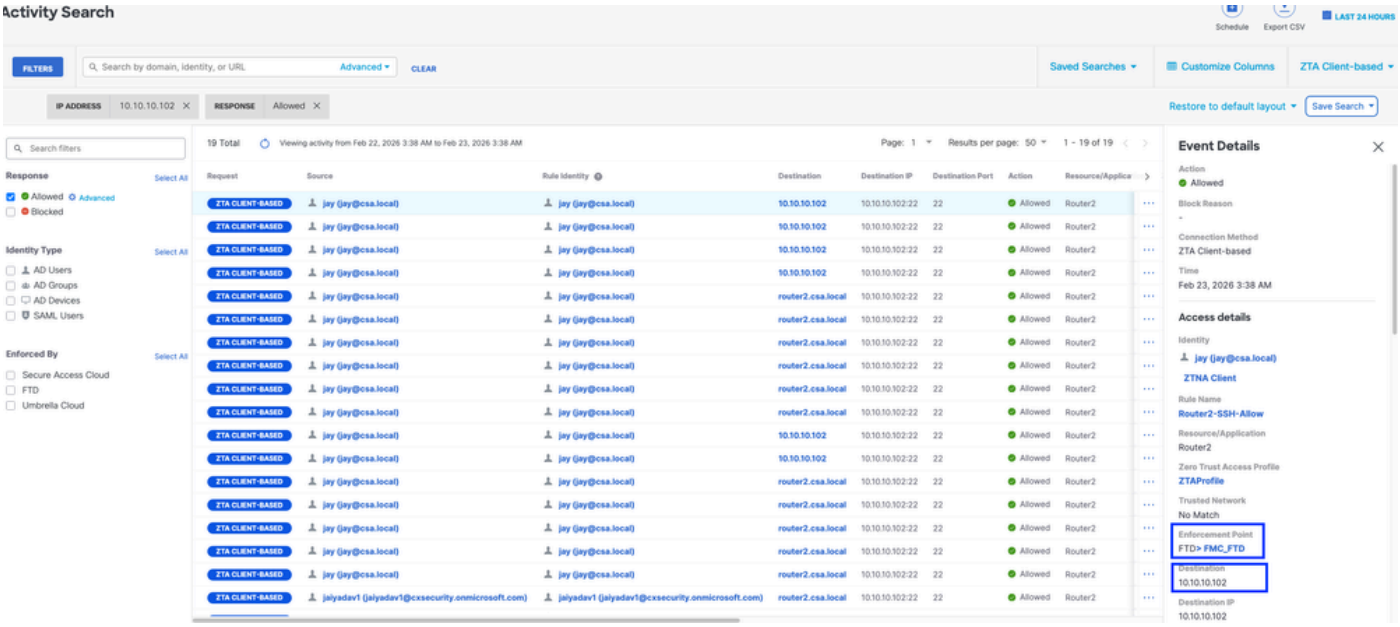
Accesso sicuro - Ricerca attività



Accesso sicuro - Ricerca attività

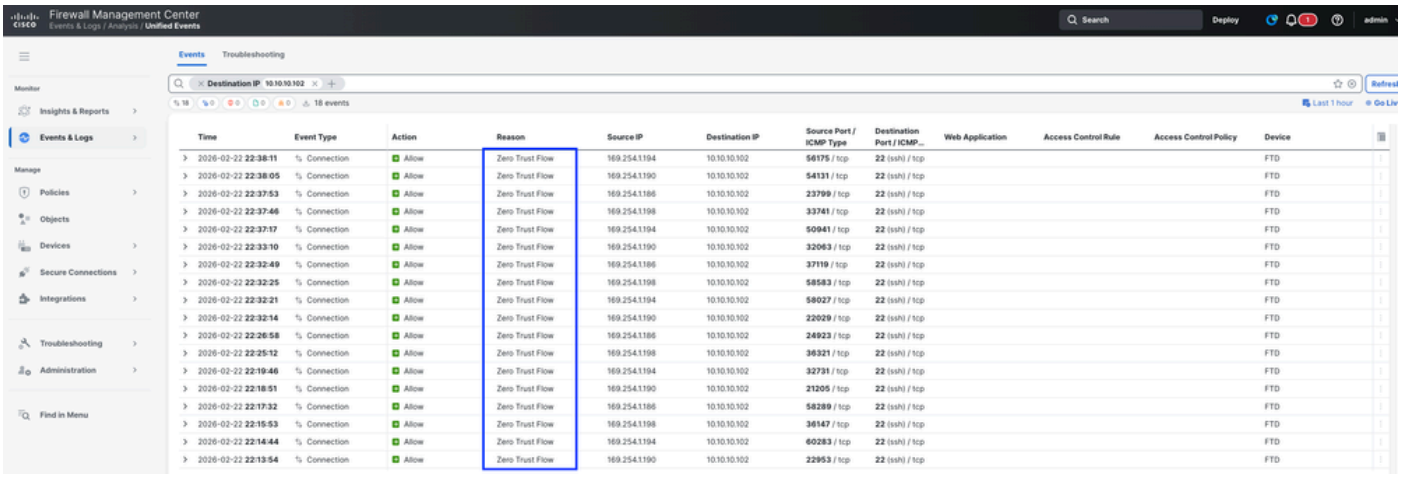


Accesso sicuro - Ricerca attività



Accesso sicuro - Ricerca attività

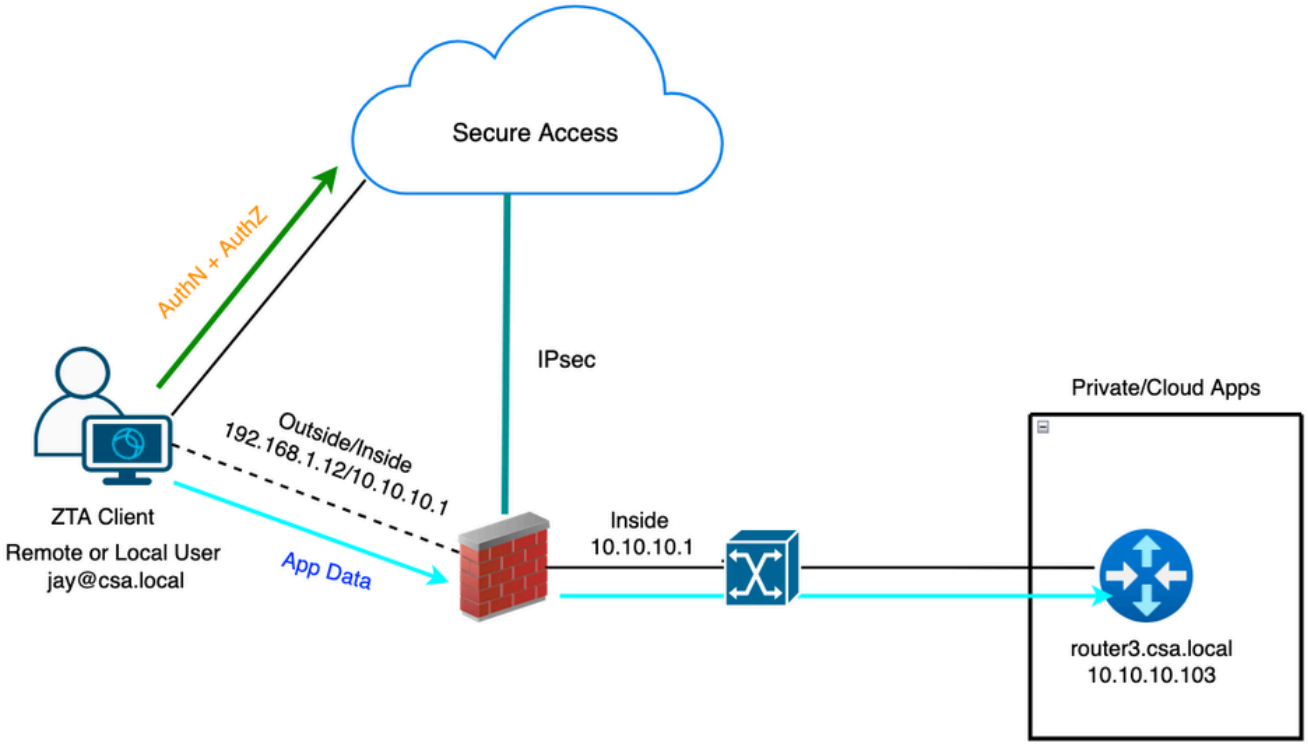
6. Verificare gli eventi di connessione FMC



Eventi connessione FMC

Test case 4 - Utente locale e remoto - Applicazione locale o cloud con TND

In questo caso il tipo di imposizione dipende dalla posizione dell'utente, se l'utente è Locale o dietro una zona FTD attendibile (all'interno, DMZ e così via) l'imposizione sarà Locale (Test case 3). Se l'utente è remoto, l'imposizione sarà cloud (Test case 1). La posizione dell'utente viene decisa in base all'impostazione di Network Fingerprint o TND, se l'impronta digitale di rete corrisponde allora la posizione locale dell'utente sarà Locale e se non corrisponde allora la posizione locale dell'utente sarà considerata Remota.

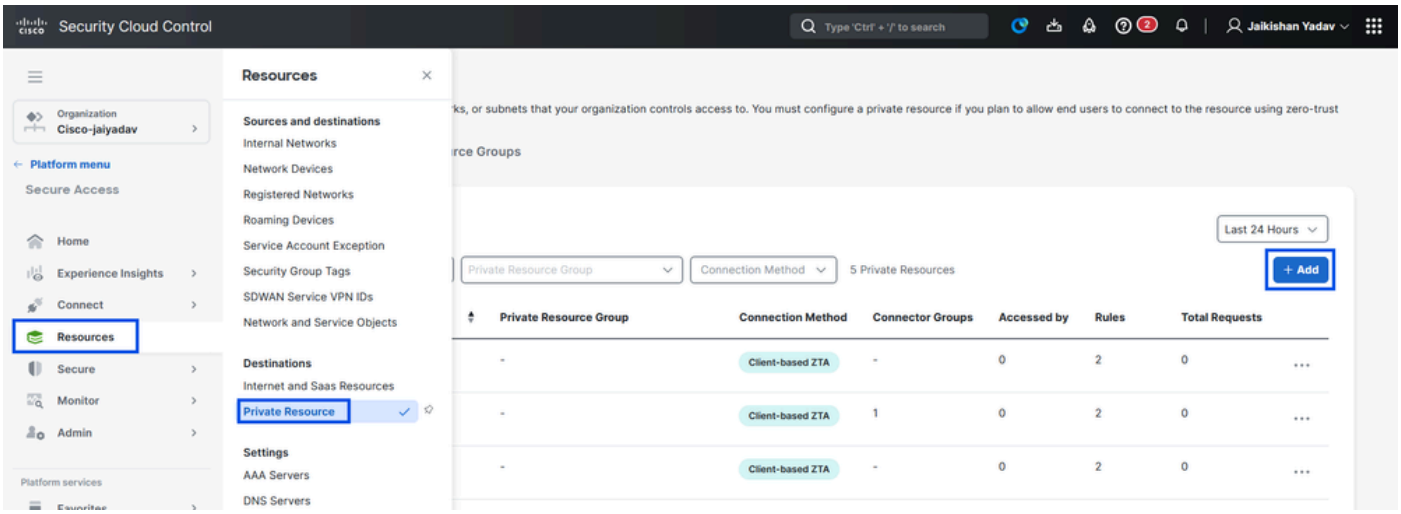


Universal ZTA - Topologia test case

Passaggio 1 - Definizione di una risorsa privata su accesso sicuro

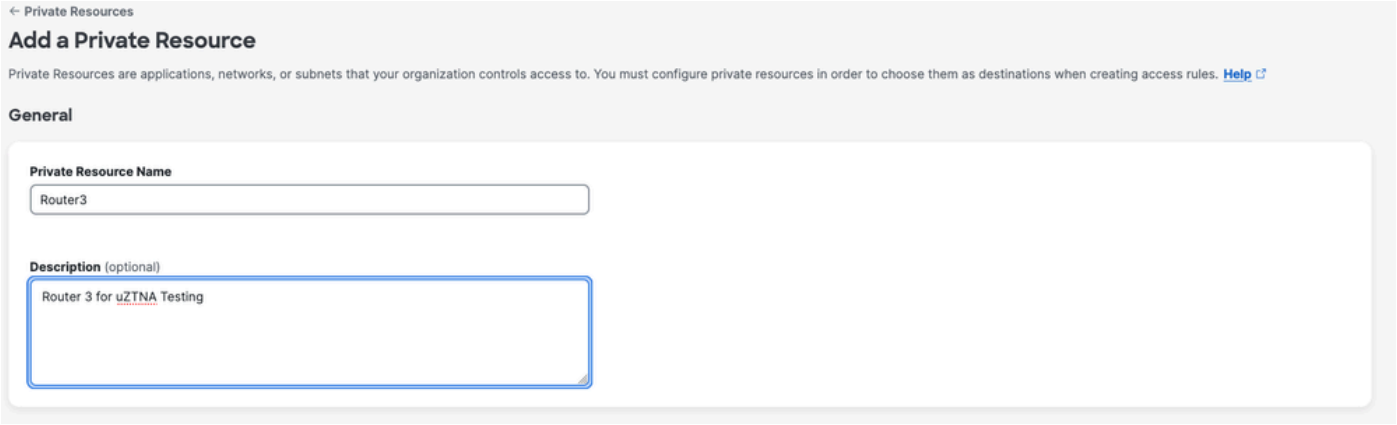
Configurare una risorsa privata in modo che sia accessibile tramite un dispositivo con registrazione ZTA (Zero Trust Access) con imposizione cloud

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



Accesso sicuro - Configurazione risorse private

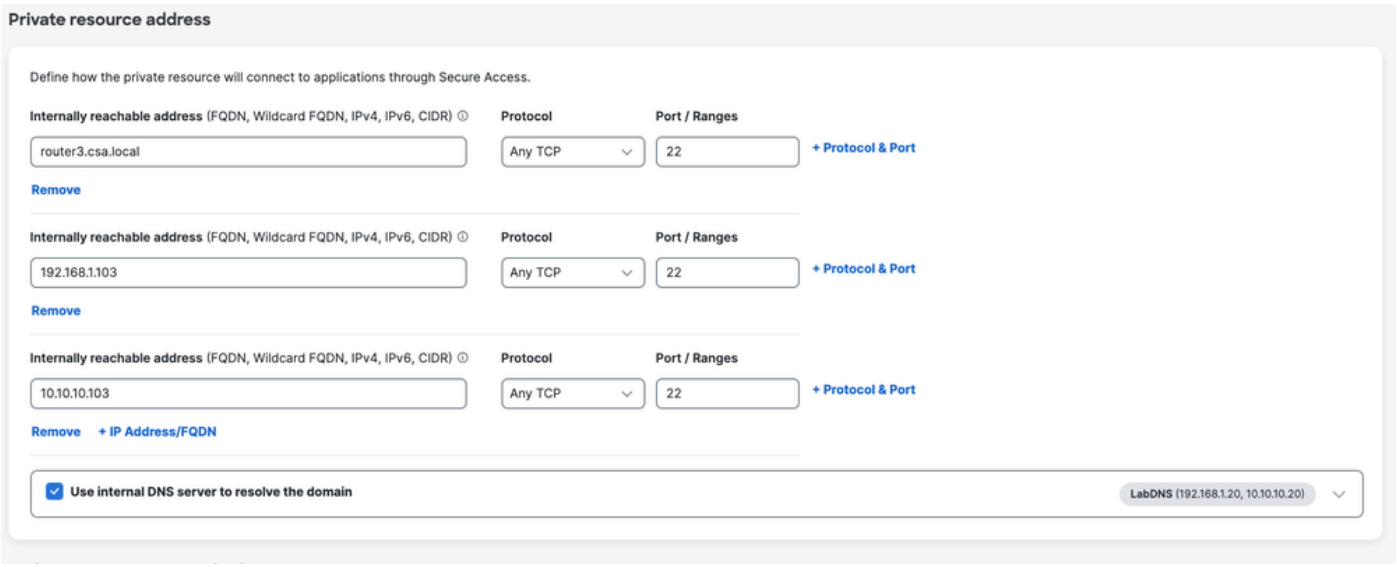
2. In Nome risorsa privata, inserire un nome significativo per la risorsa. Per Descrizione, è consigliabile fornire informazioni quali lo scopo della risorsa o il nome del proprietario della risorsa.



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]

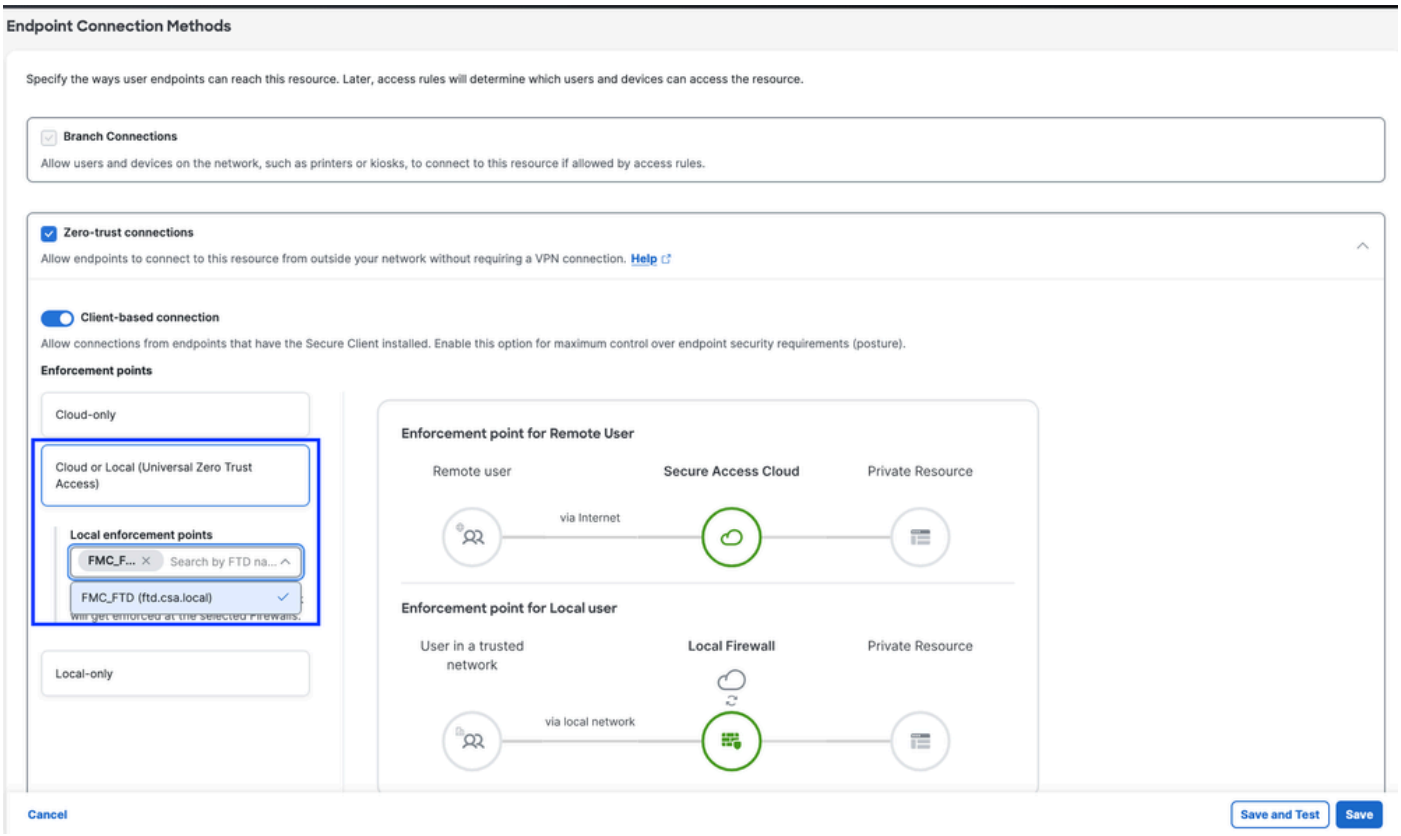
4. Selezionare il server DNS per risolvere il dominio



Accesso sicuro - Configurazione risorse private

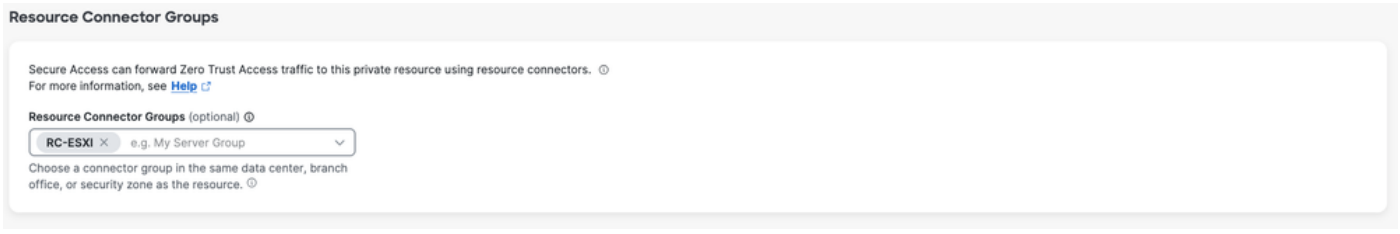
5. Seleziona metodi di connessione degli endpoint

6. Selezionare FTD come punti di applicazione locale



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).



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

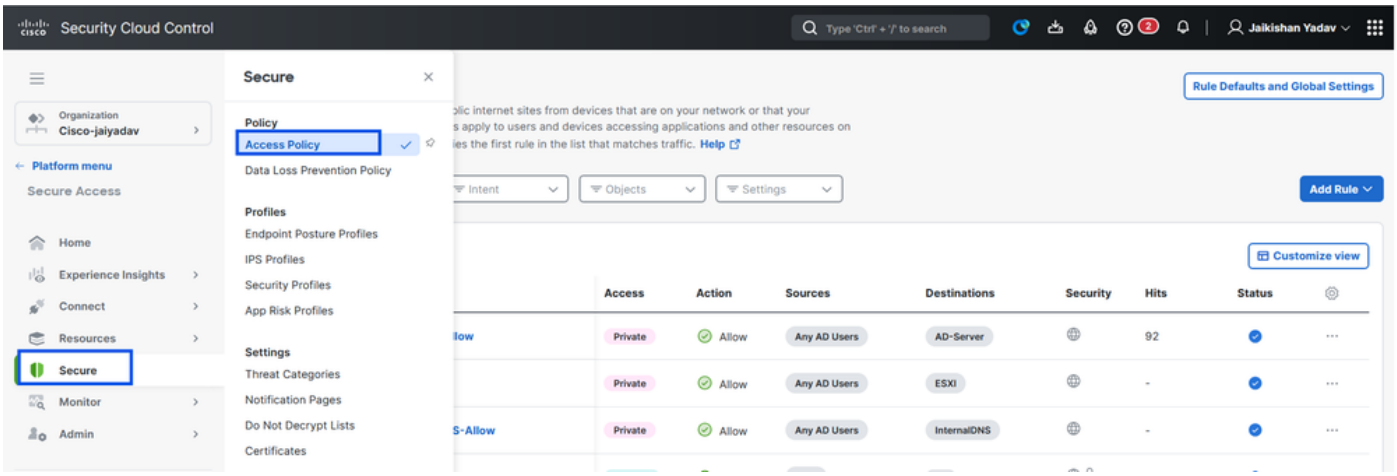
---

7. Fare clic su Salva.

Passaggio 2 - Creazione della regola di accesso privato

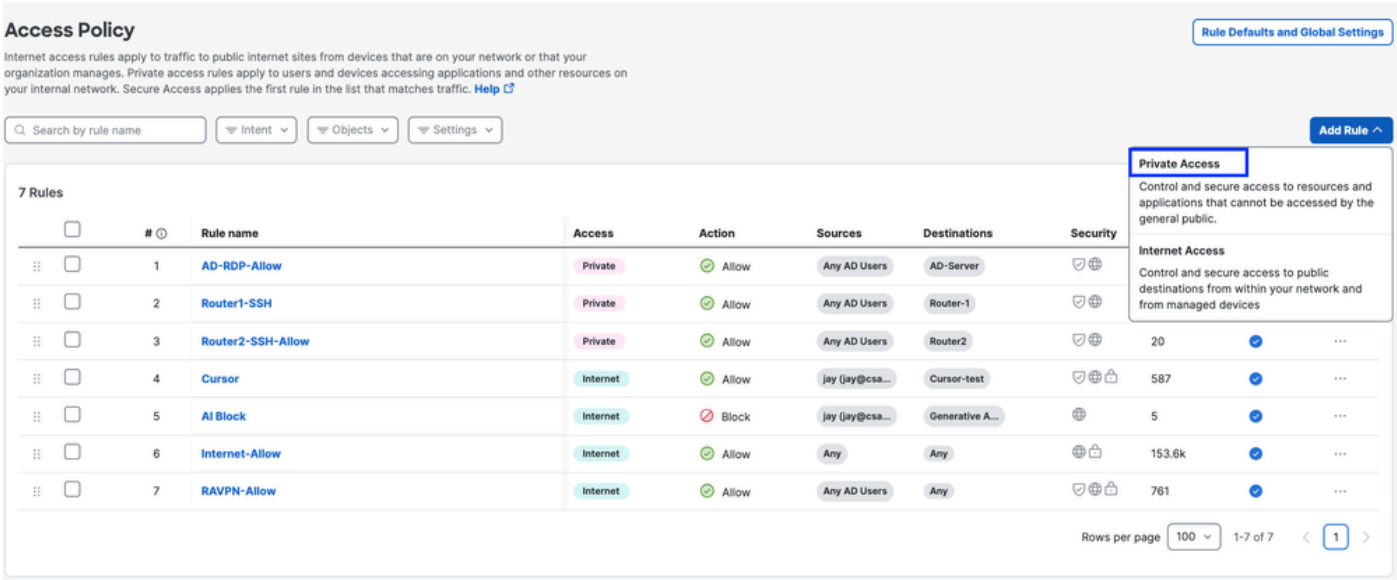
Configurare un accesso privato su Secure Access in modo che gli utenti con registrazione ZTA universale possano accedervi. Per ulteriori informazioni, vedere Regola di accesso privato

1. Passare a Protezione > Criteri di accesso



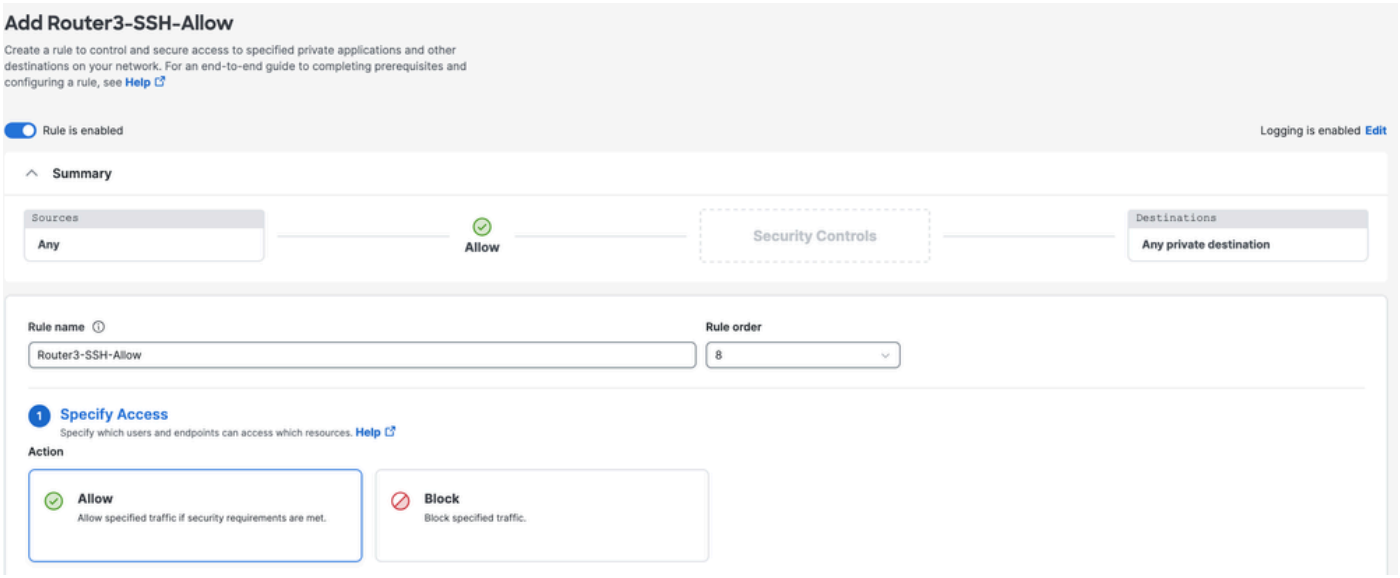
Accesso sicuro - Configurazione criteri di accesso

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.



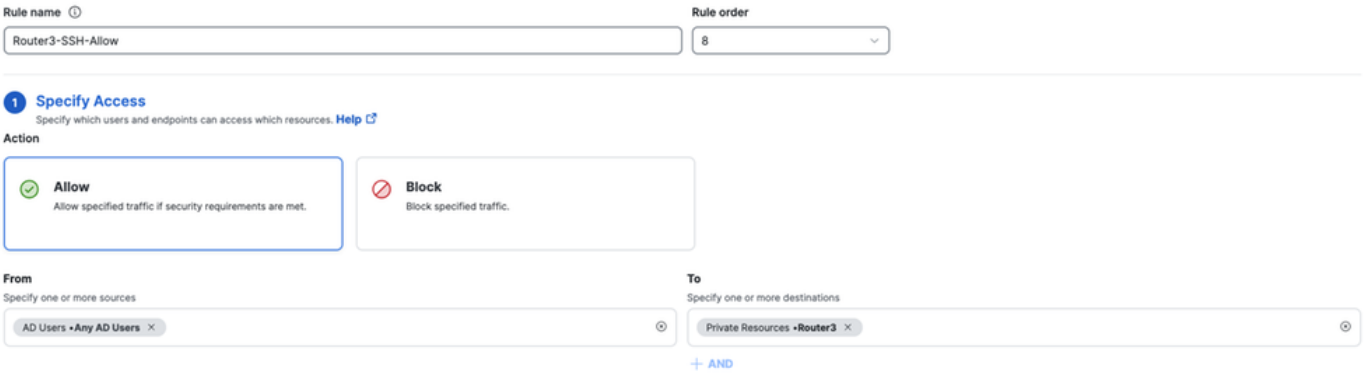
Accesso sicuro - Configurazione criteri di accesso

3. Aggiungere un nome di regola



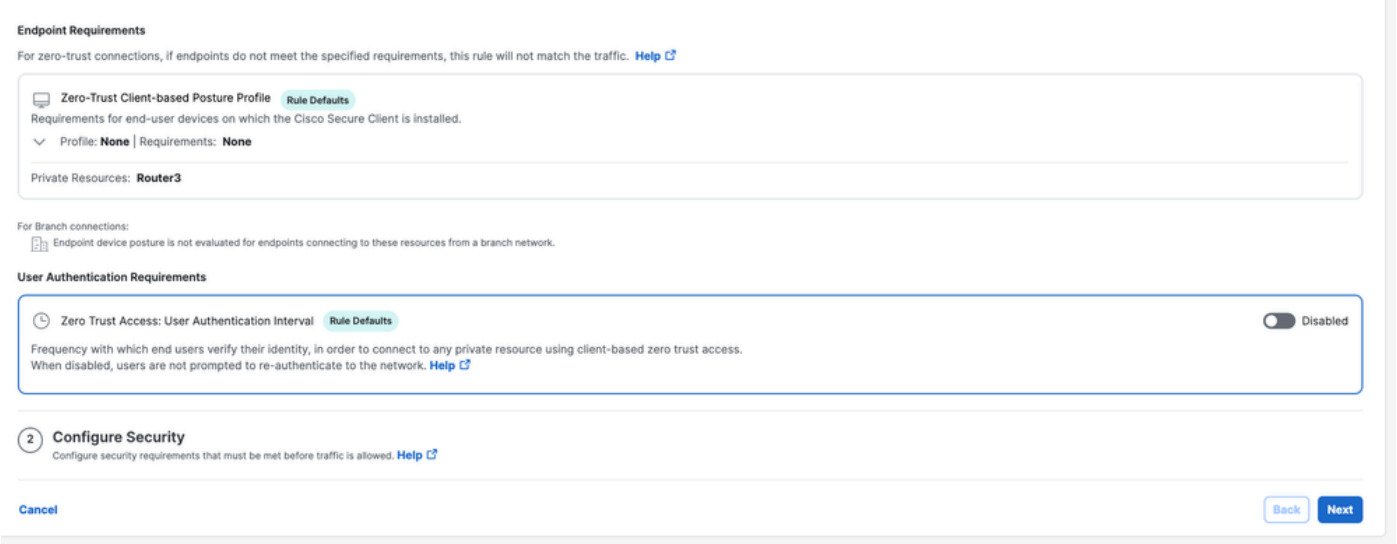
Accesso sicuro - Configurazione criteri di accesso

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



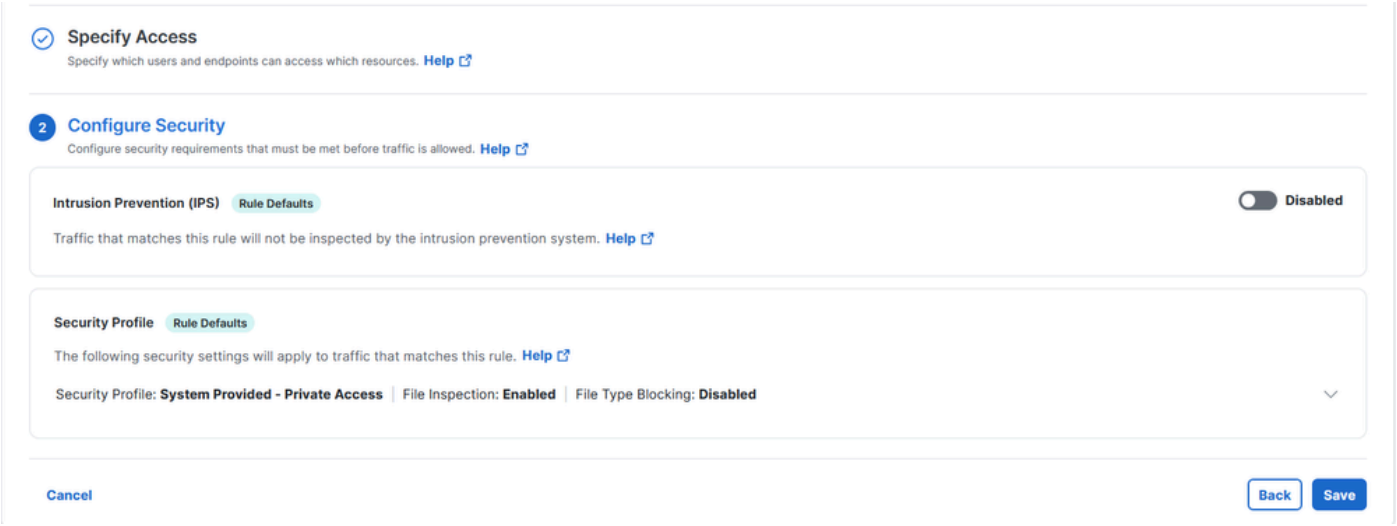
Accesso sicuro - Configurazione criteri di accesso

5. Configurare i requisiti degli endpoint



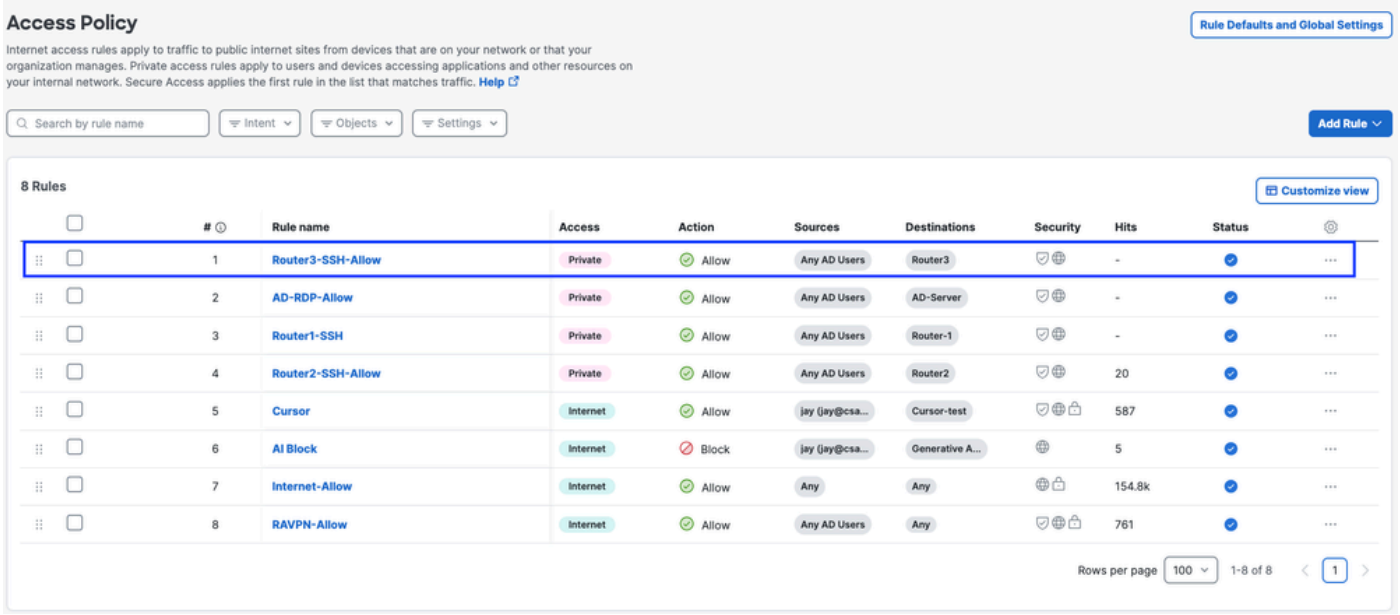
Accesso sicuro - Configurazione criteri di accesso

6. Configura protezione



Accesso sicuro - Configurazione criteri di accesso

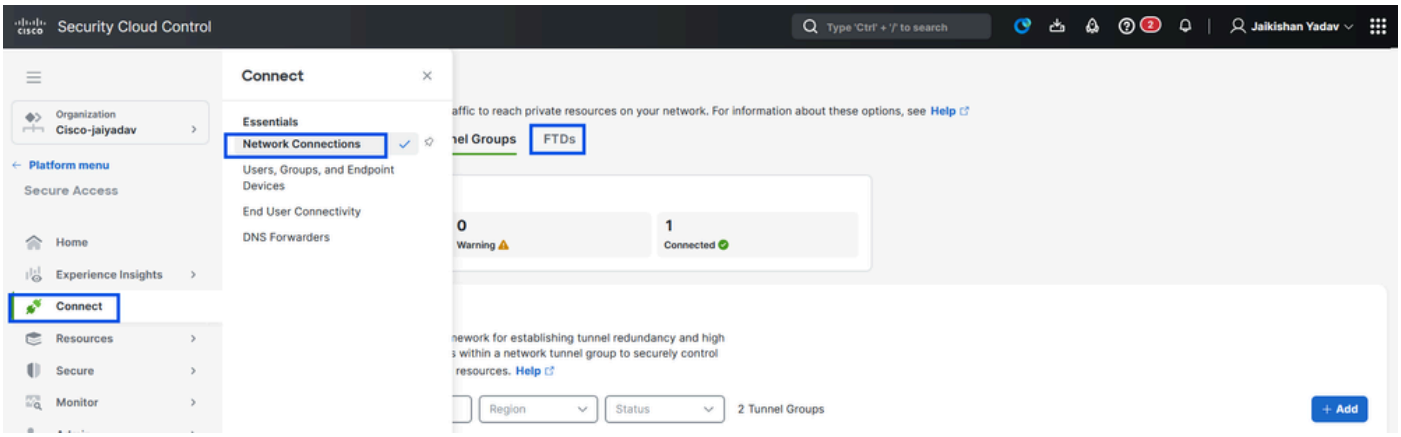
7. Fare clic su Save (Salva)



Accesso sicuro - Configurazione criteri di accesso

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

1. Passare a connessione > Connessioni di rete > FTD

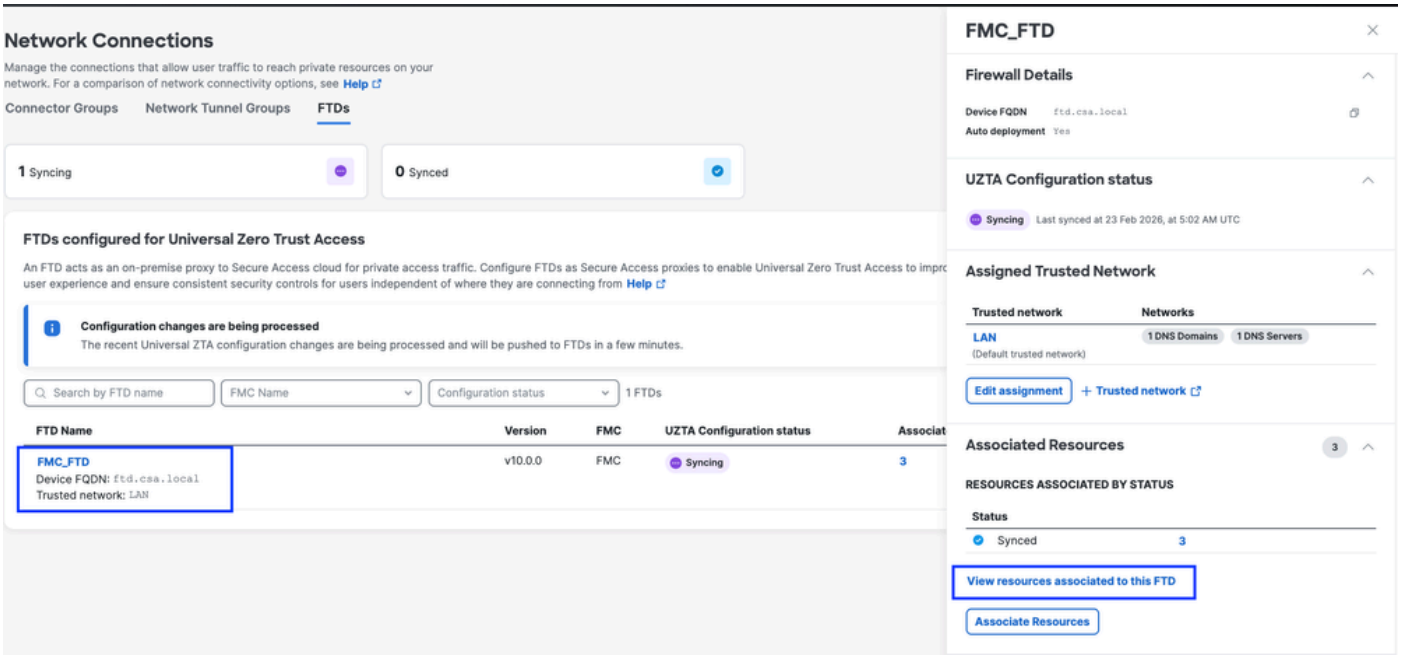


Accesso sicuro - Verifica PR

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

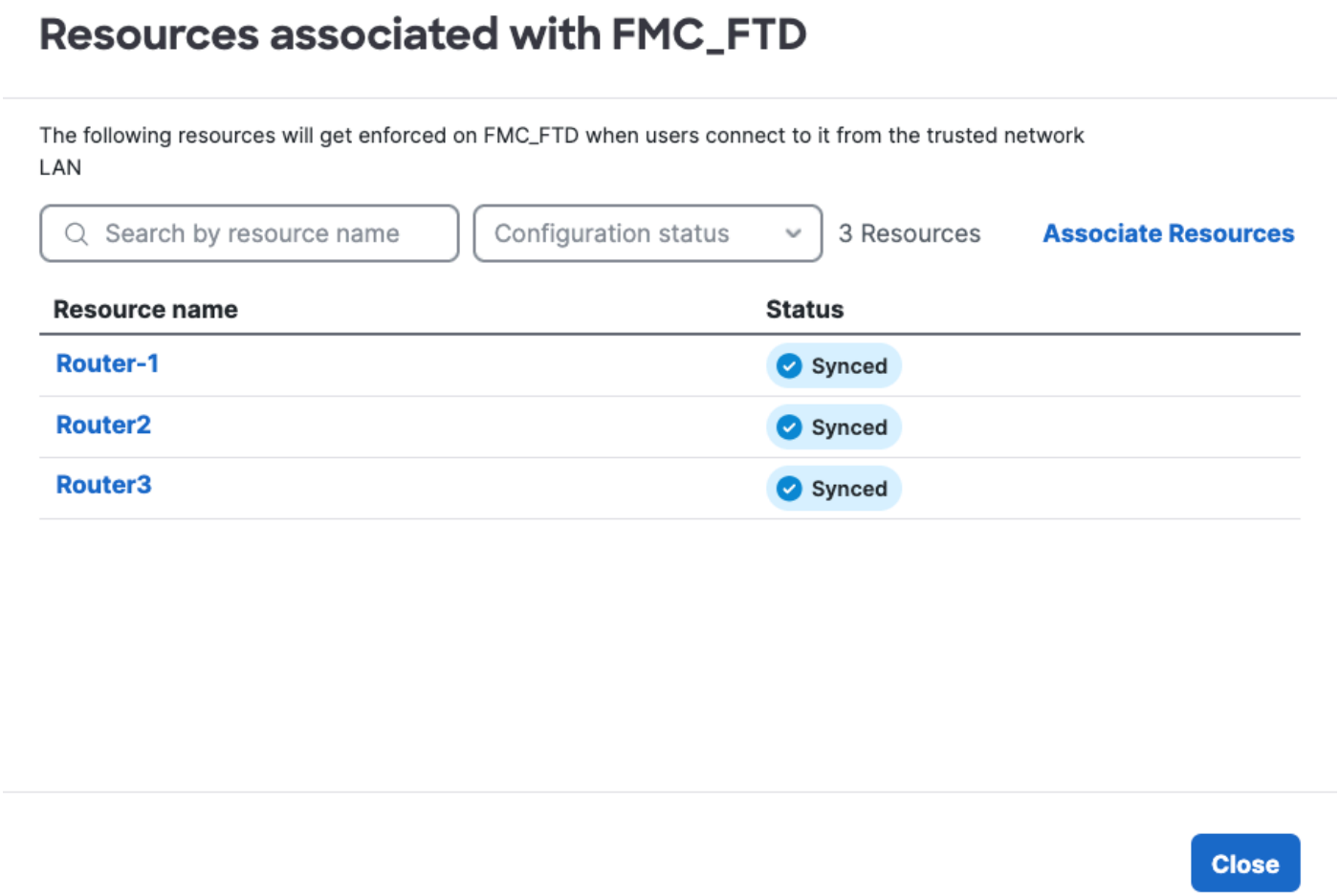
```
C:\Users\jay>ping ftd.csa.local

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



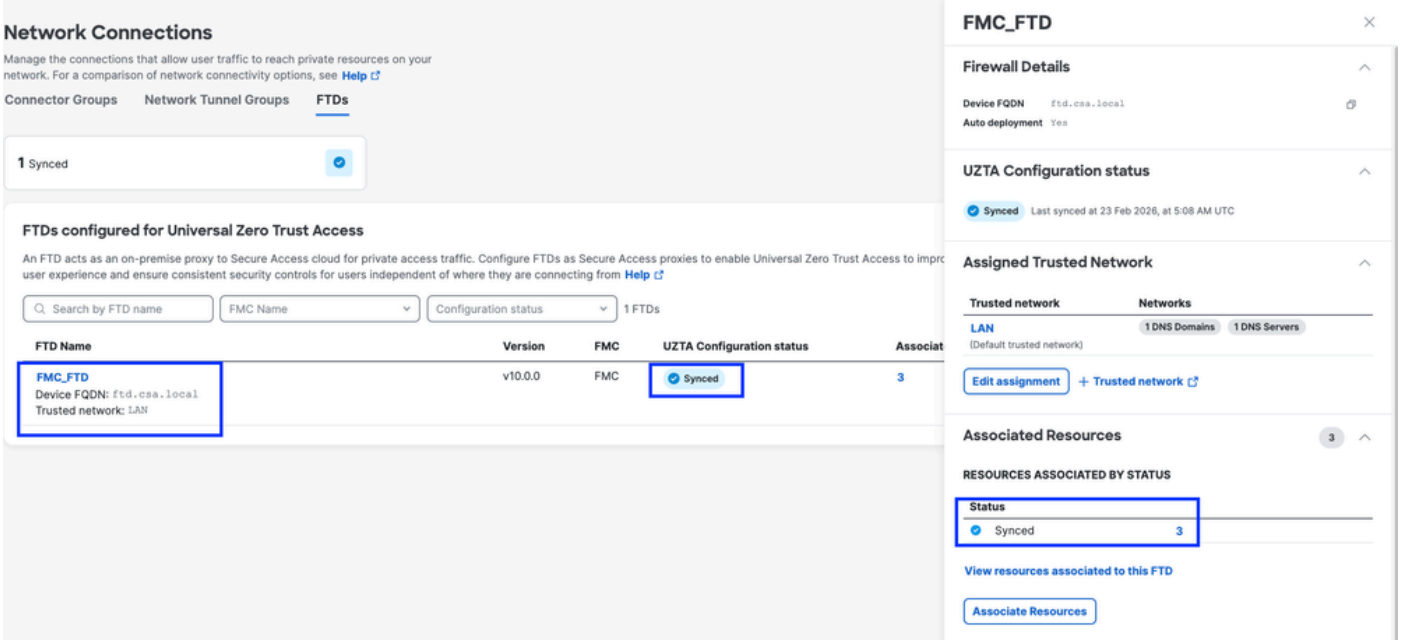
Accesso sicuro - Verifica PR

```
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
```



3. Fare clic su chiudi

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



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

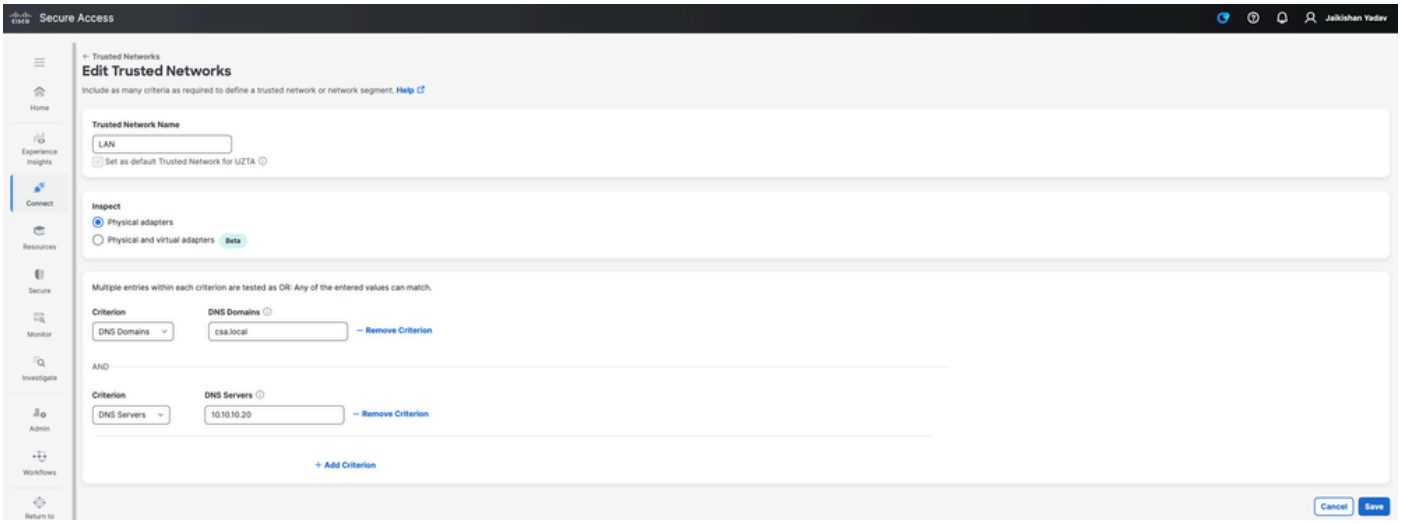
show running-config applicazione oggetto

```
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"

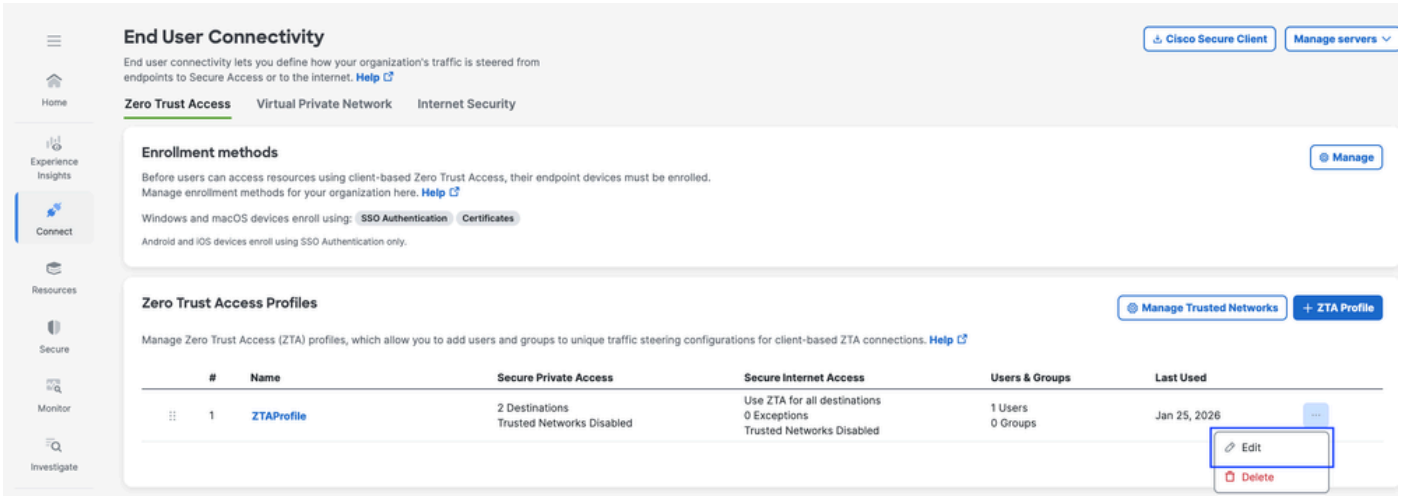
Selezionare Connetti > Connettività utente finale > Accesso con attendibilità totale > Impostazioni ZTA e configurare Reti attendibili



Accesso sicuro - Configurazione TND ZTA

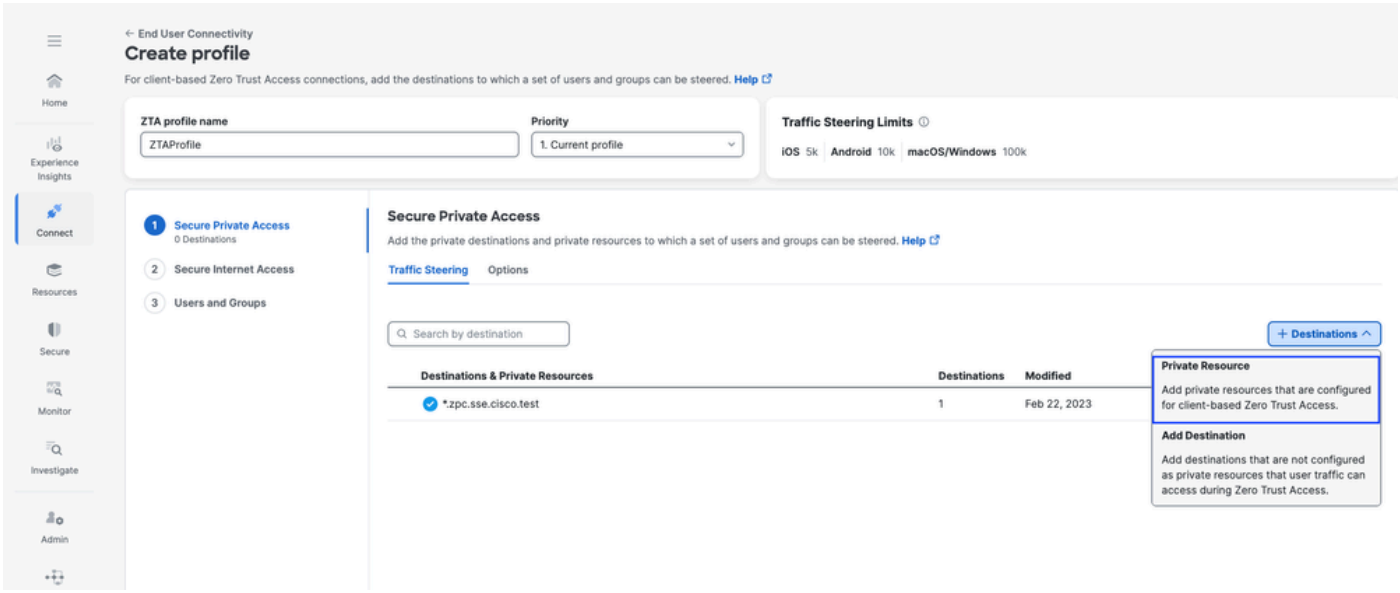
Fase - 5 Aggiungere una risorsa privata al profilo ZTA

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

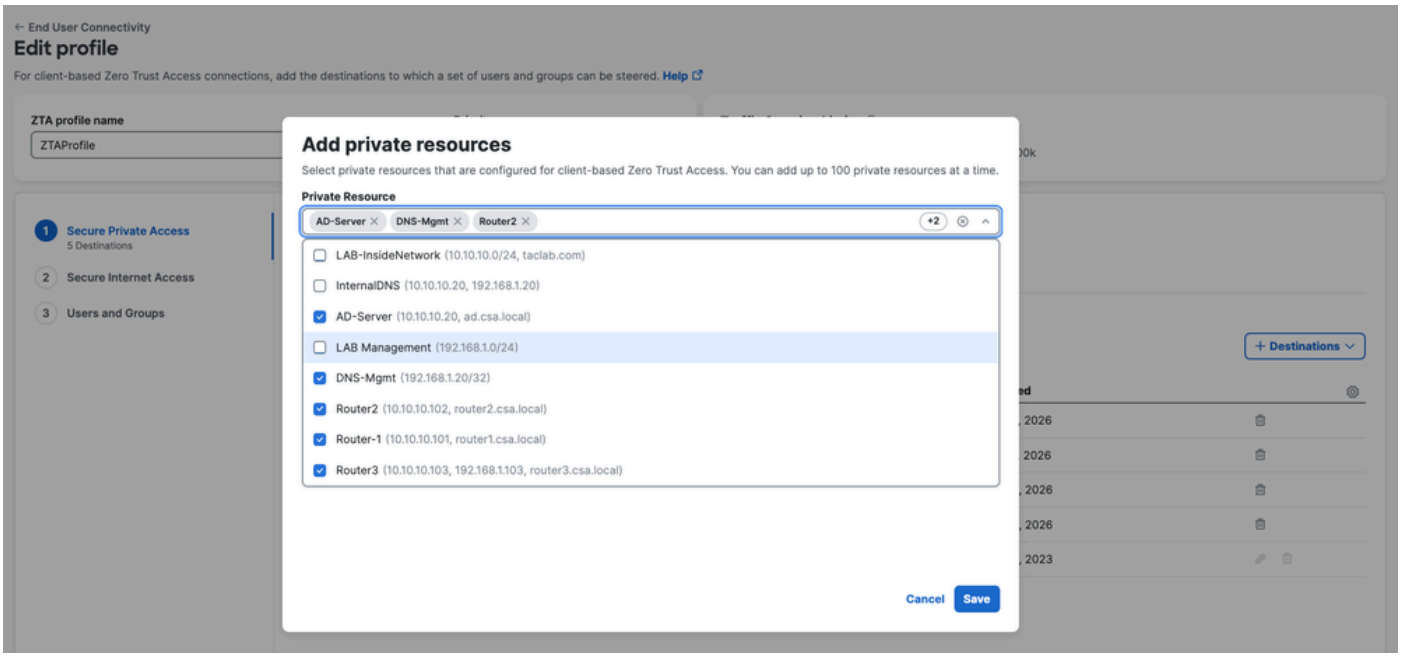


Accesso sicuro - Profilo ZTA

2. Aggiungere la risorsa privata

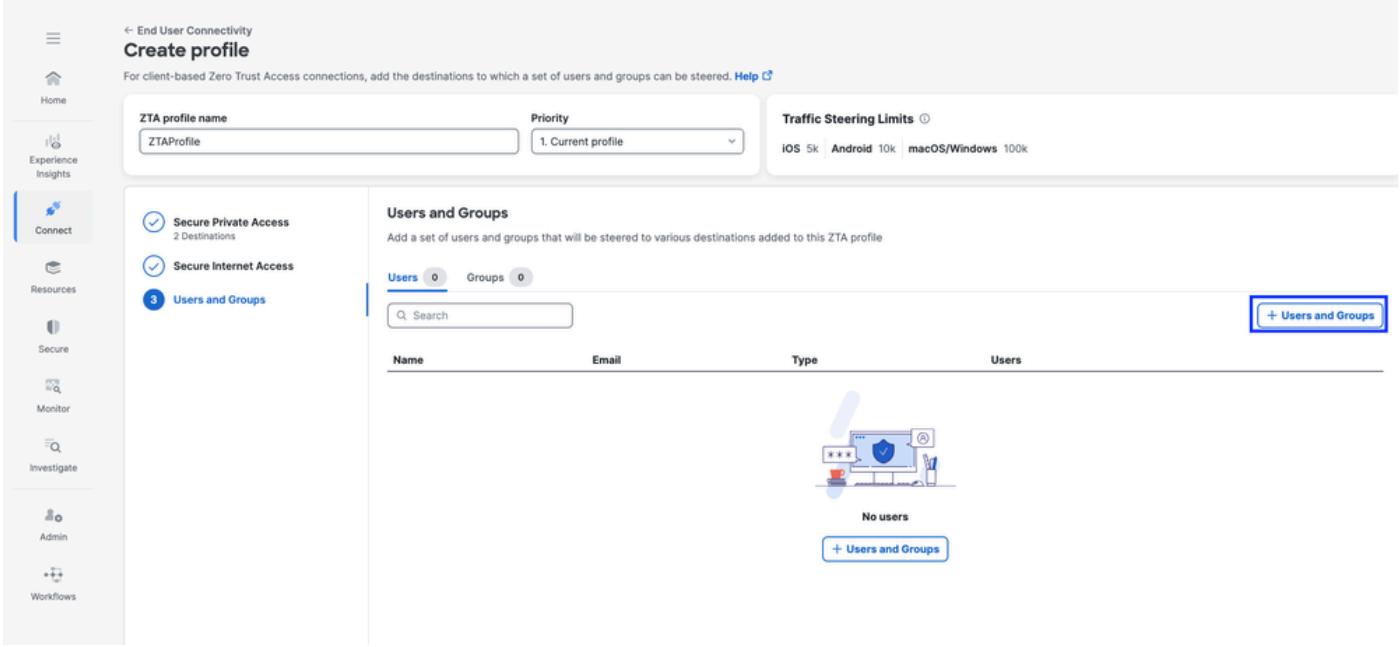


Accesso sicuro - Profilo ZTA

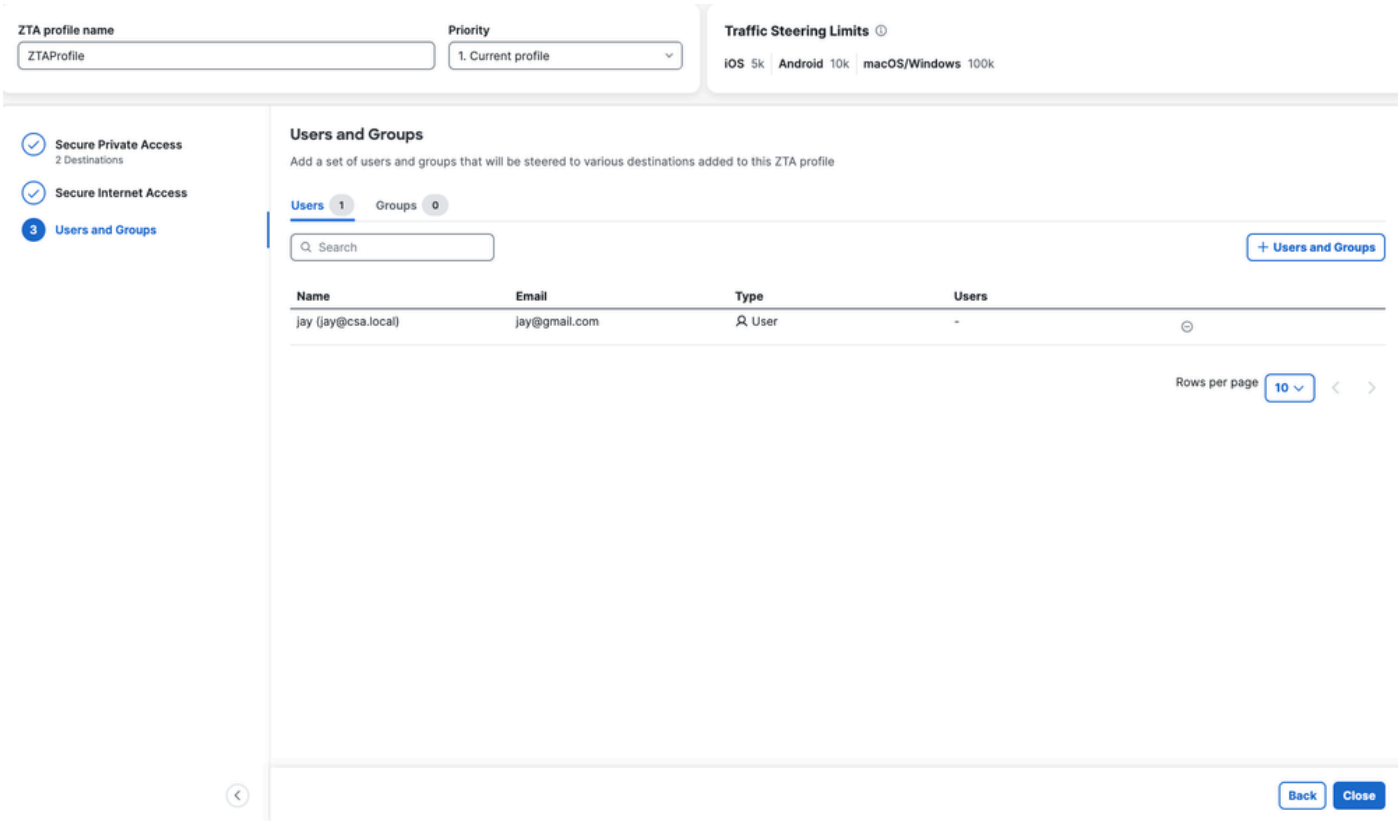


Accesso sicuro - Profilo ZTA

3. Aggiungi utenti e gruppi



Accesso sicuro - Profilo ZTA

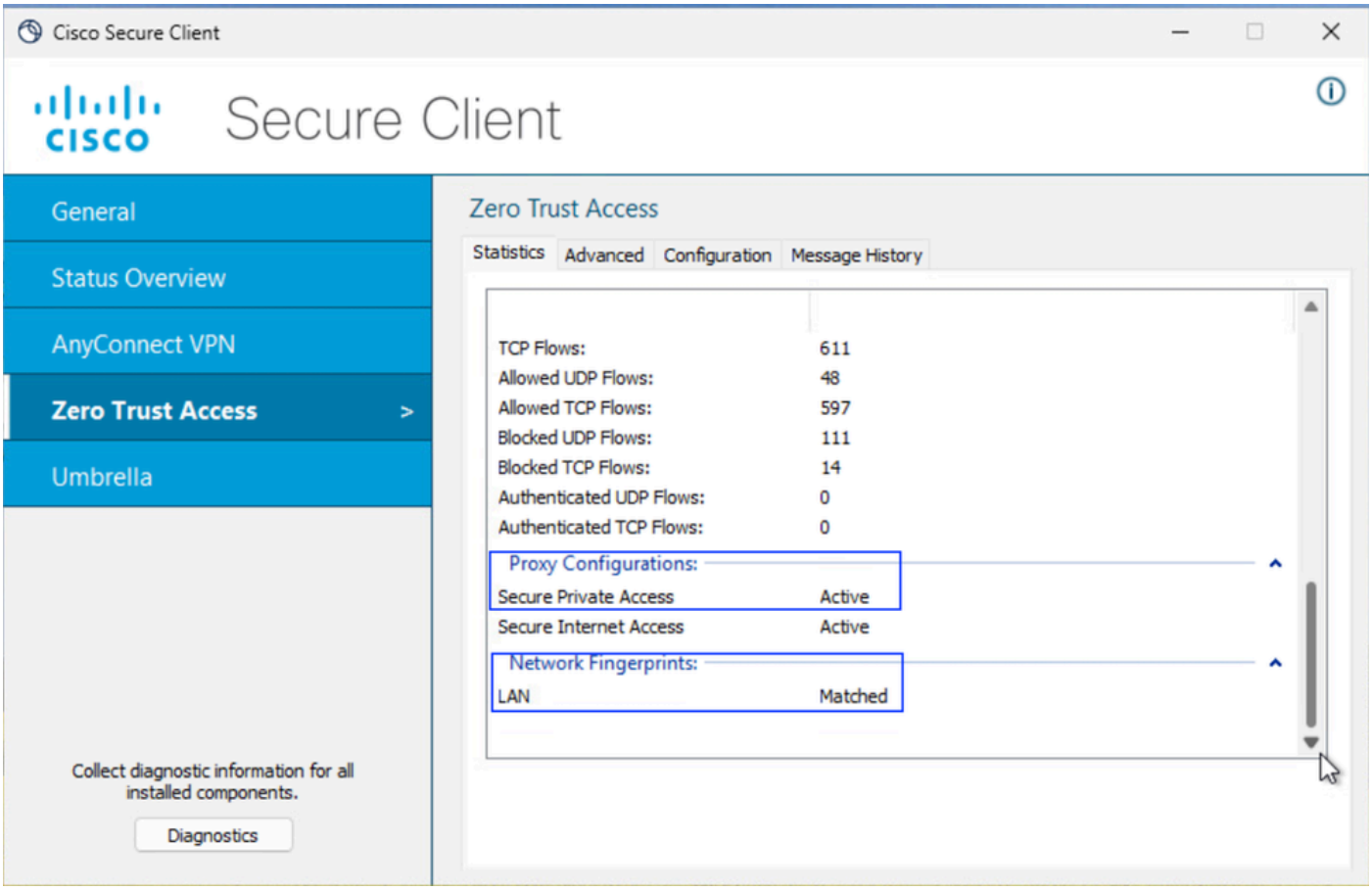


Accesso sicuro - Profilo ZTA

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

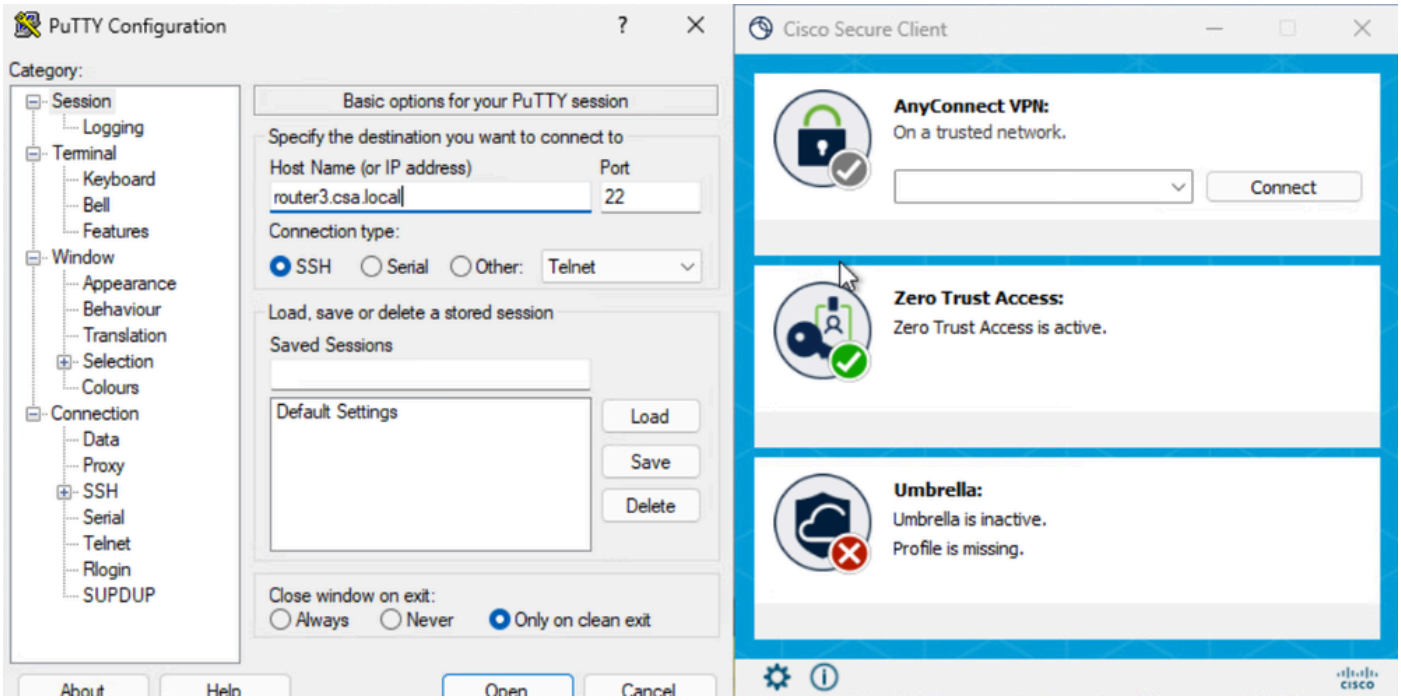
3. Verificare che l'FTD possa raggiungere la risorsa privata utilizzando l'FQDN

```
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#
```

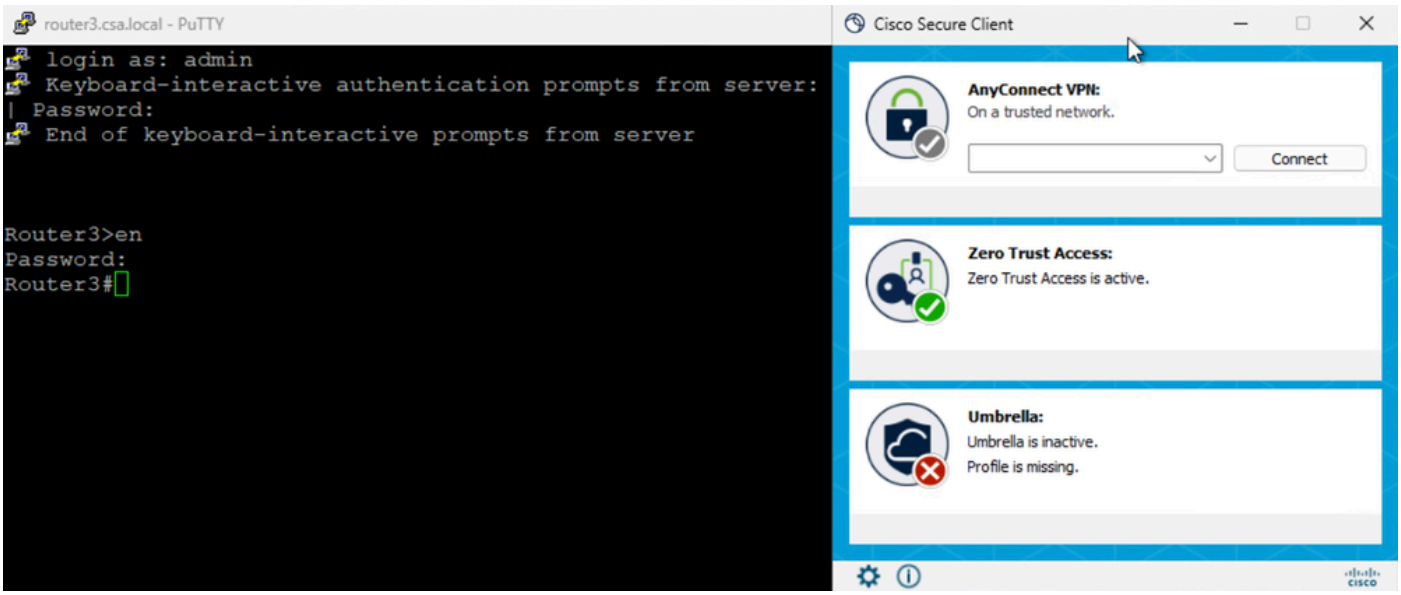
Accesso sicuro - Test PR

4. Eseguire il test della connessione SSH alla risorsa privata

Accedere alla prenotazione permanente utilizzando FQDN

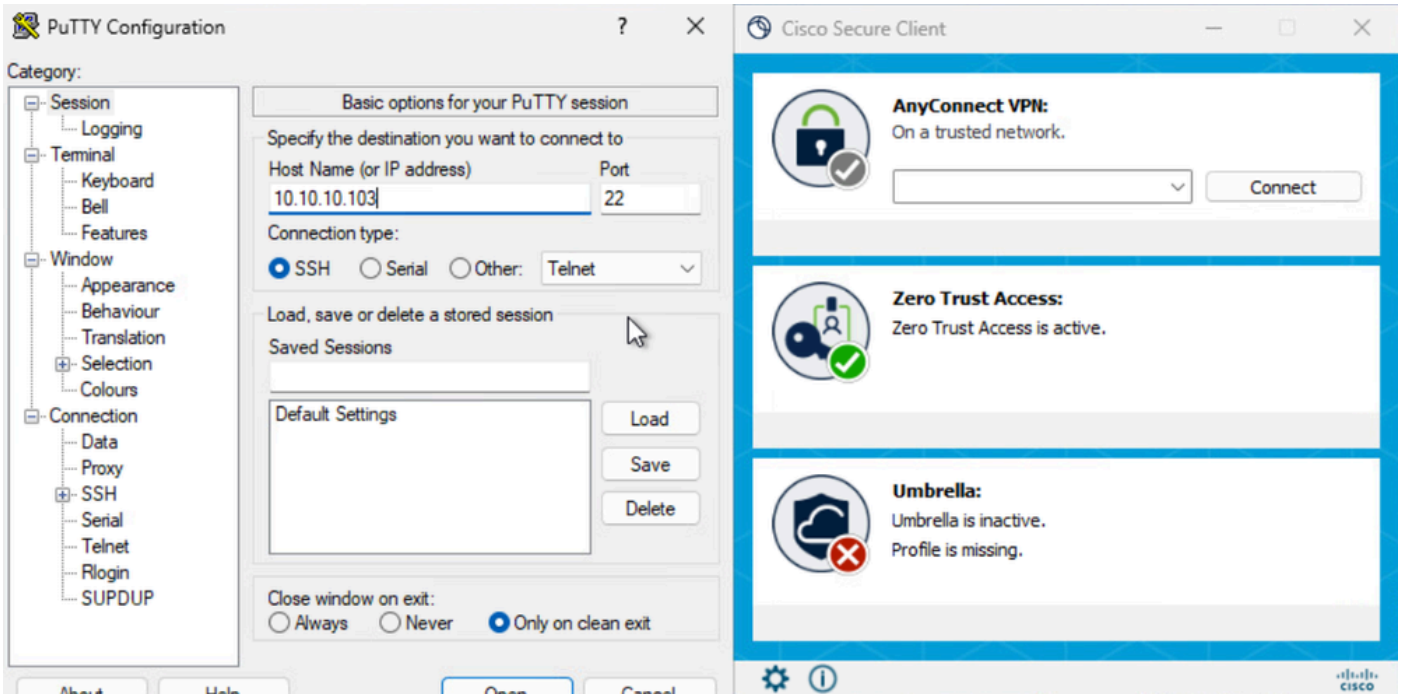


Accesso sicuro - Test PR

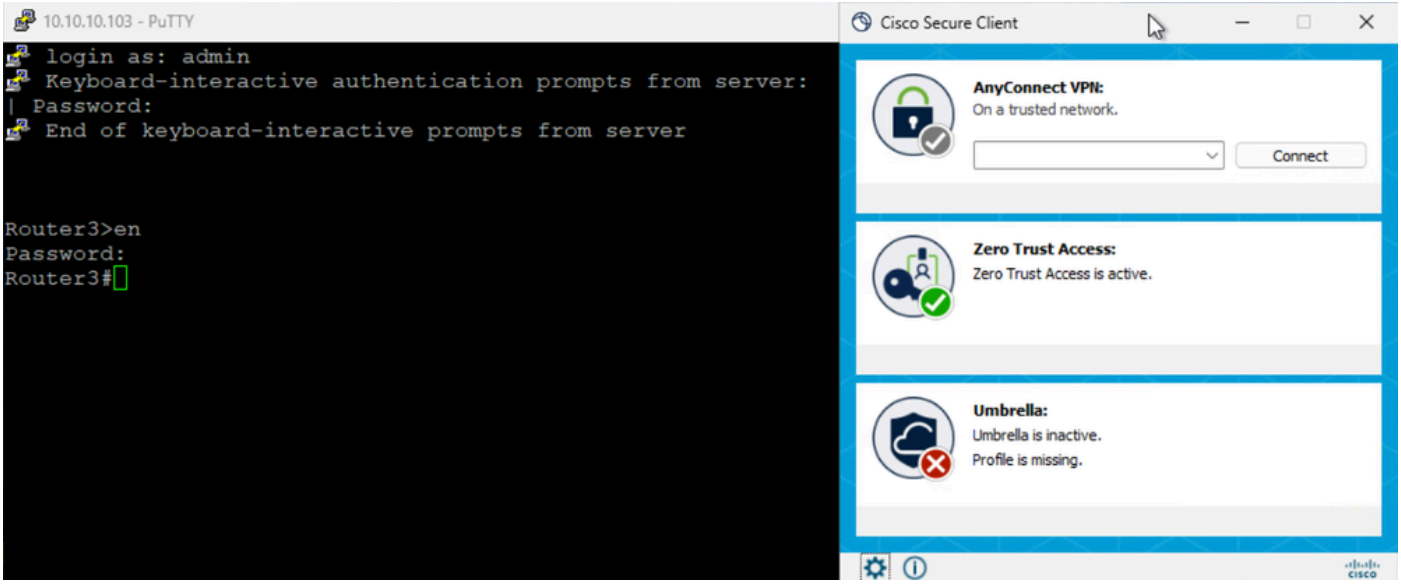


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP

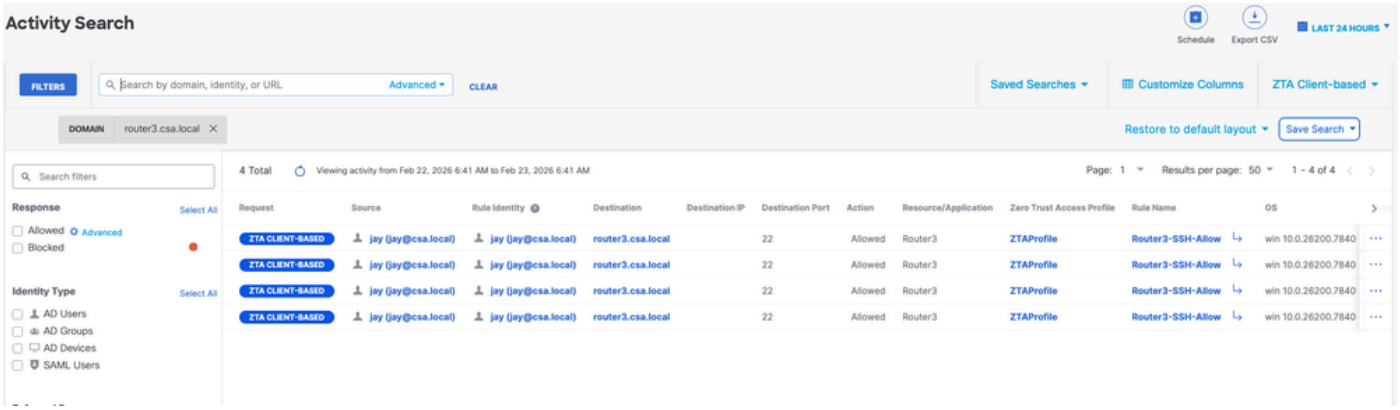


Accesso sicuro - Test PR

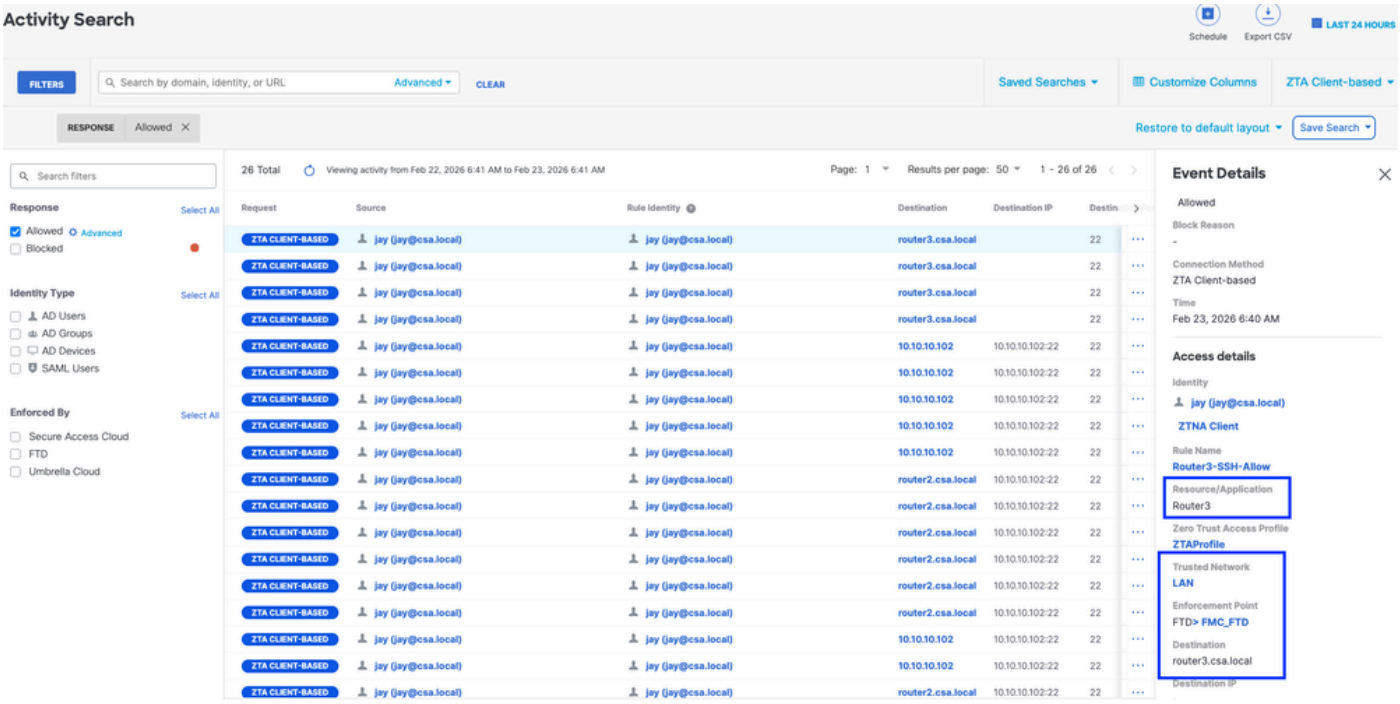


Accesso sicuro - Test PR

5. Verifica registri di ricerca attività accesso sicuro

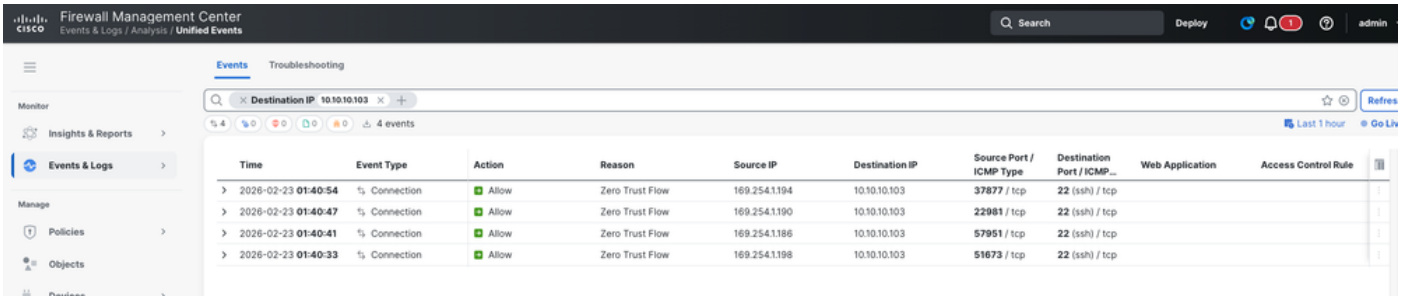


Accesso sicuro - Ricerca attività



Accesso sicuro - Ricerca attività

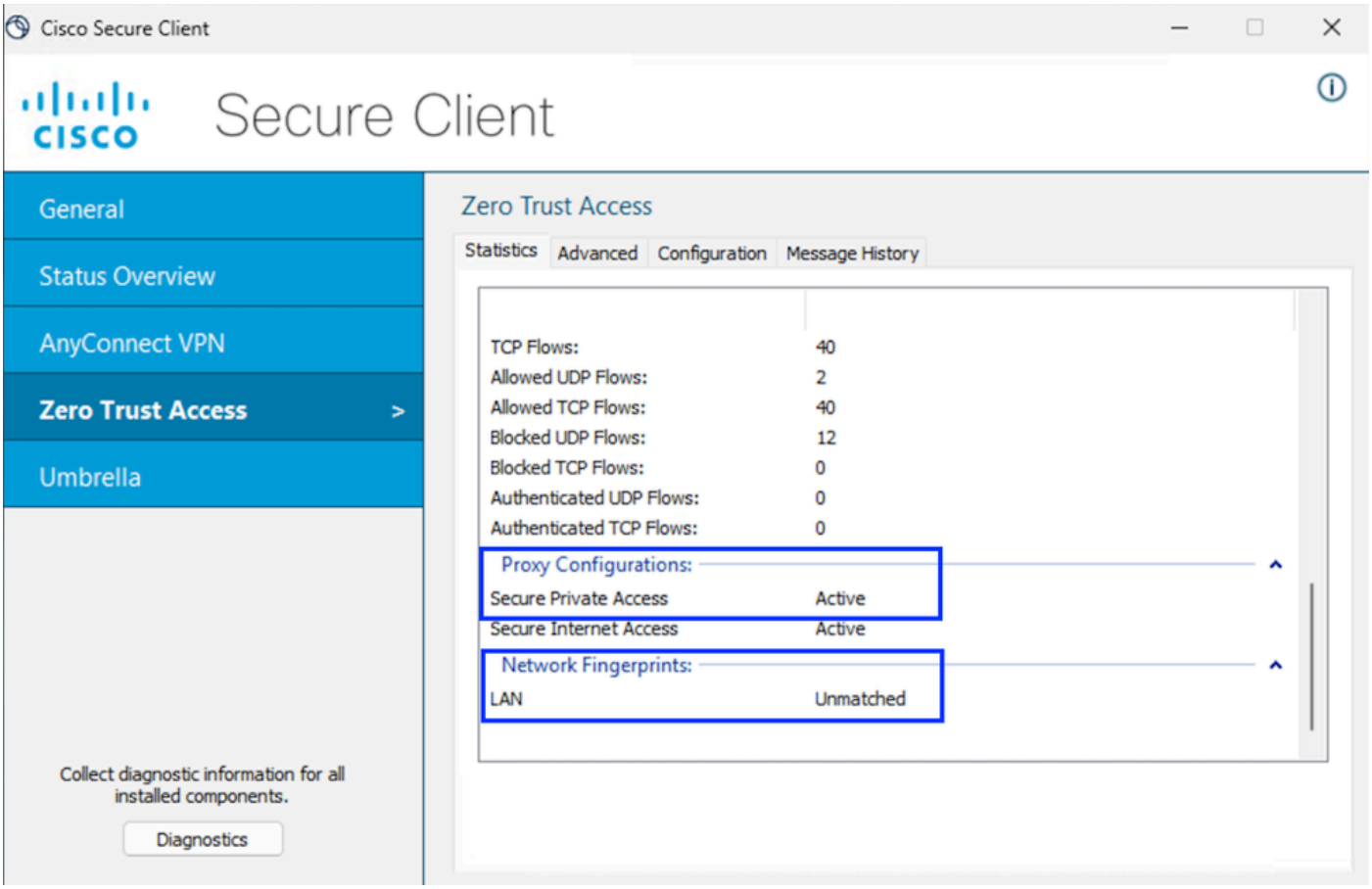
6. Verificare gli eventi di connessione FMC



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



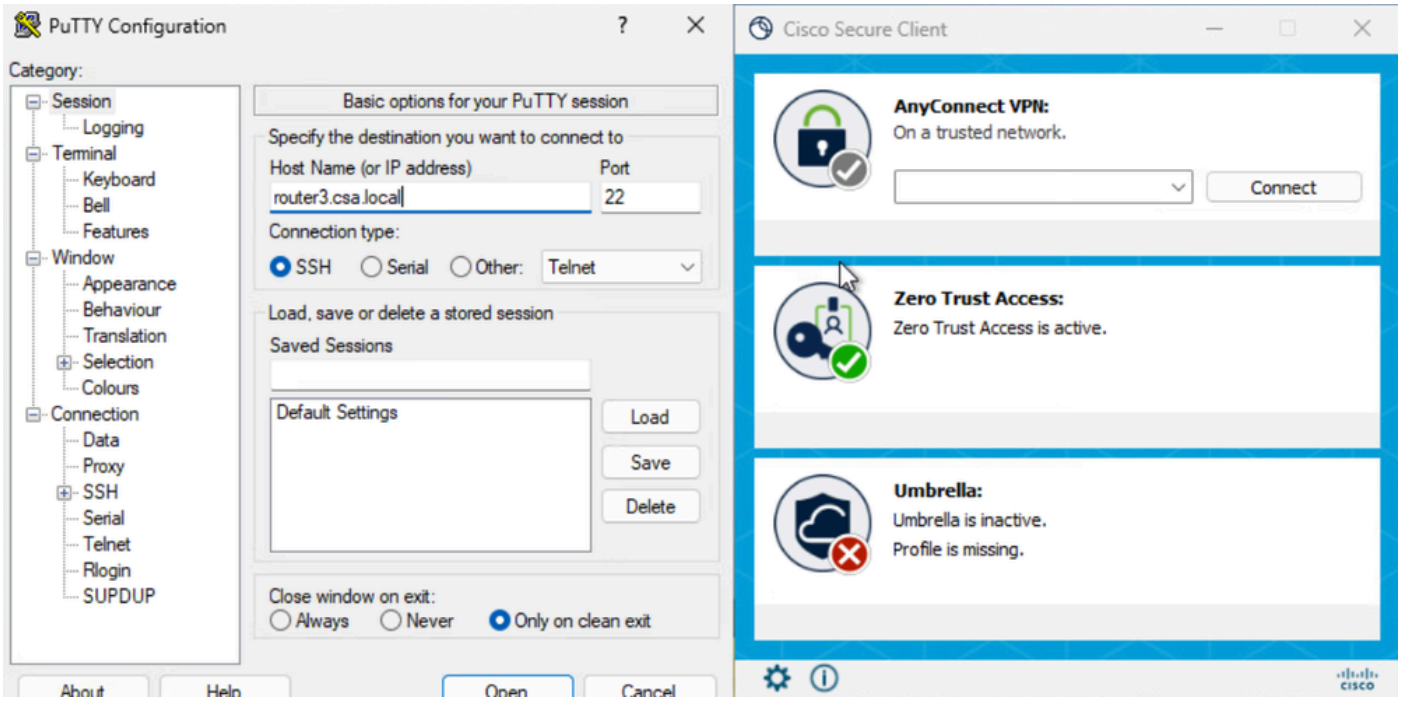
Accesso sicuro - Test PR

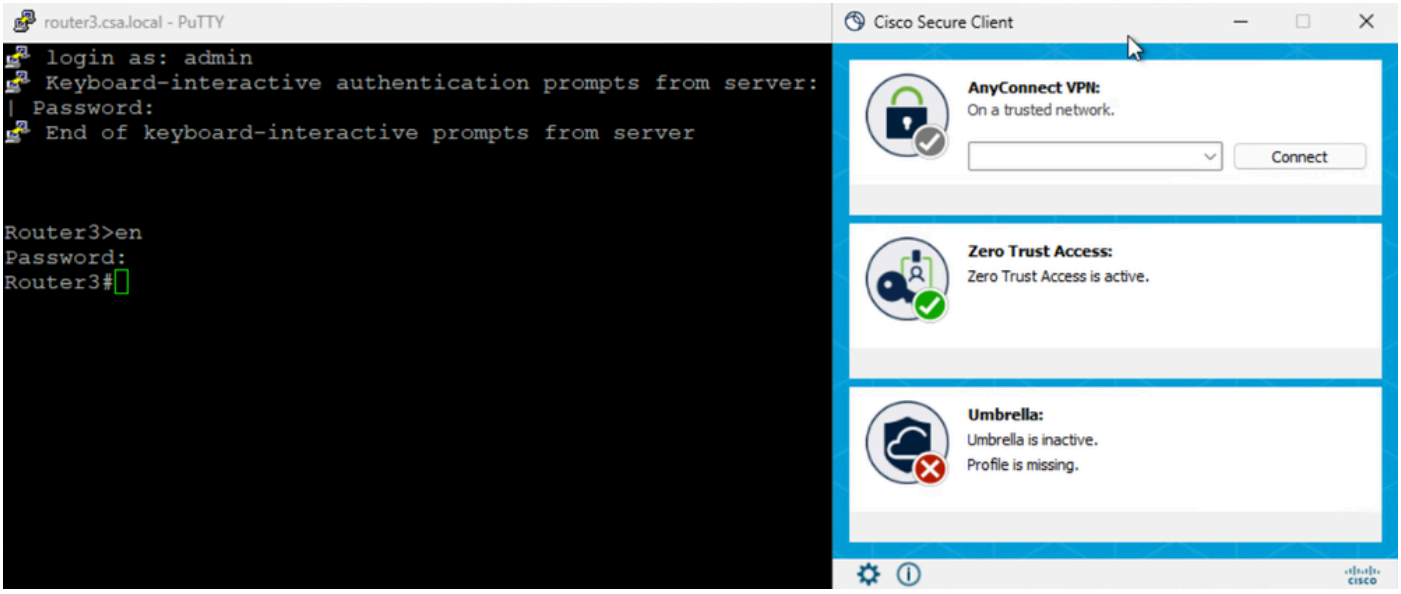
2. Verificare che l'utente remoto sia in grado di risolvere il nome di dominio completo FTD

```
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
```


3. Eseguire il test della connessione SSH alla risorsa privata

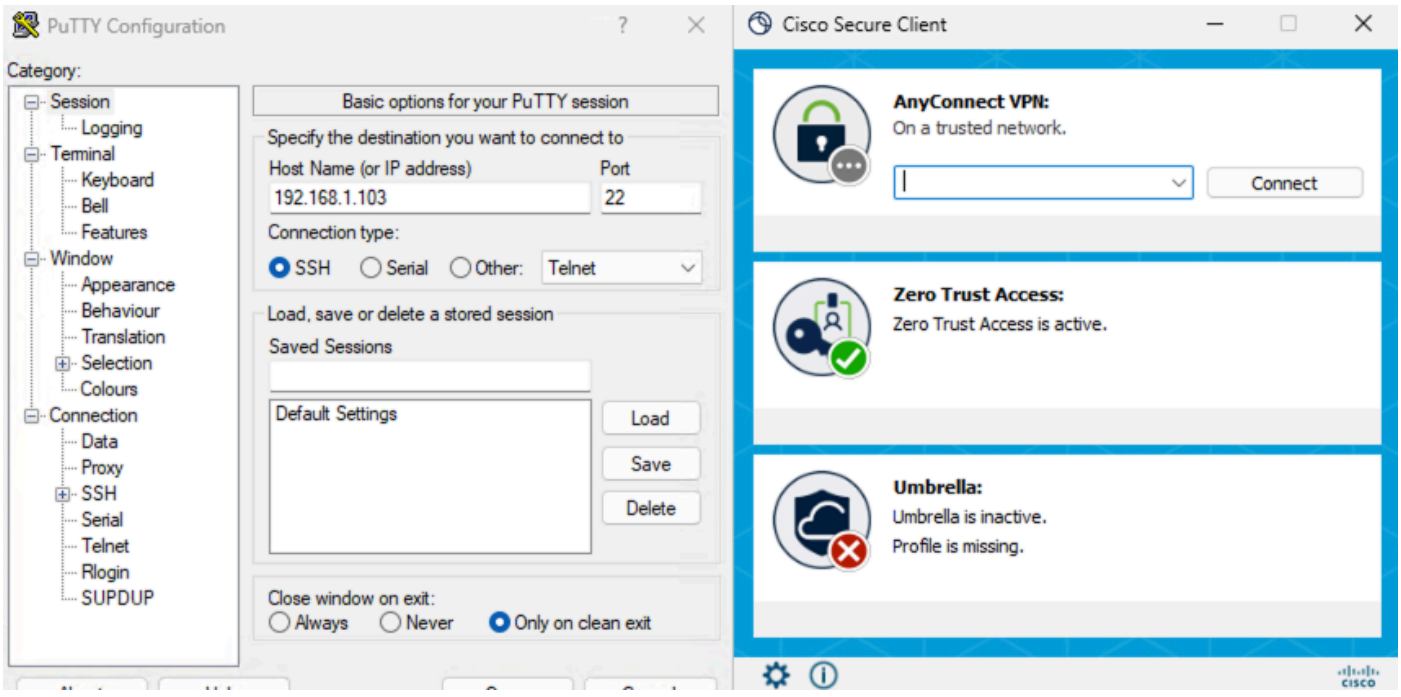
Accedere alla prenotazione permanente utilizzando FQDN



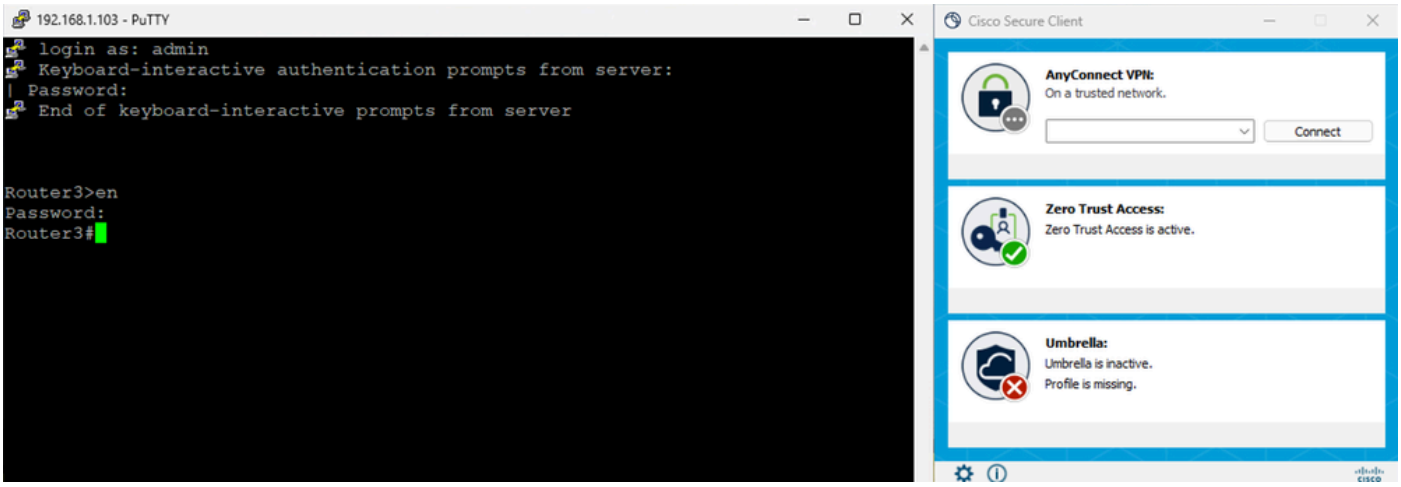


Accesso sicuro - Test PR

Accedere alla prenotazione permanente utilizzando l'indirizzo IP

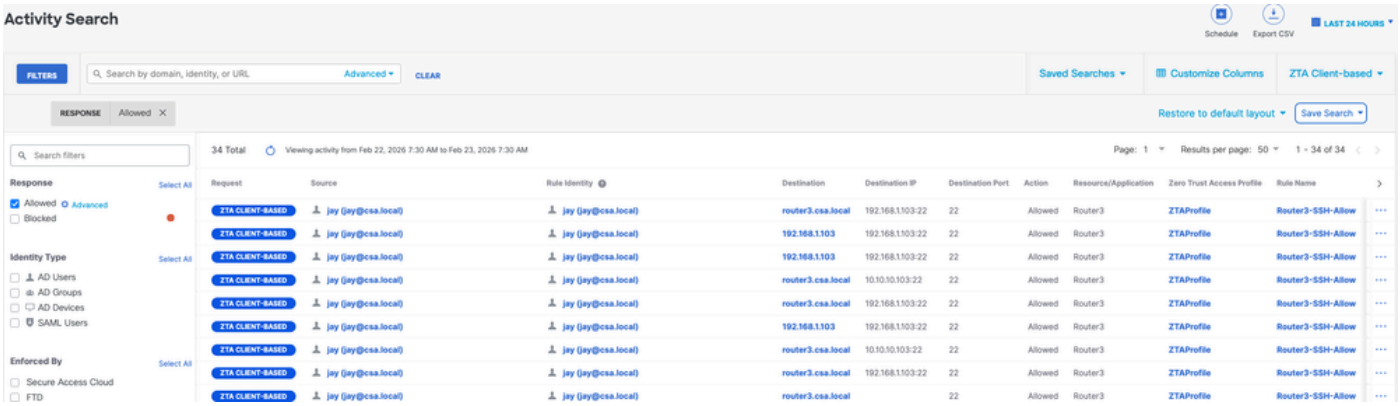


Accesso sicuro - Test PR

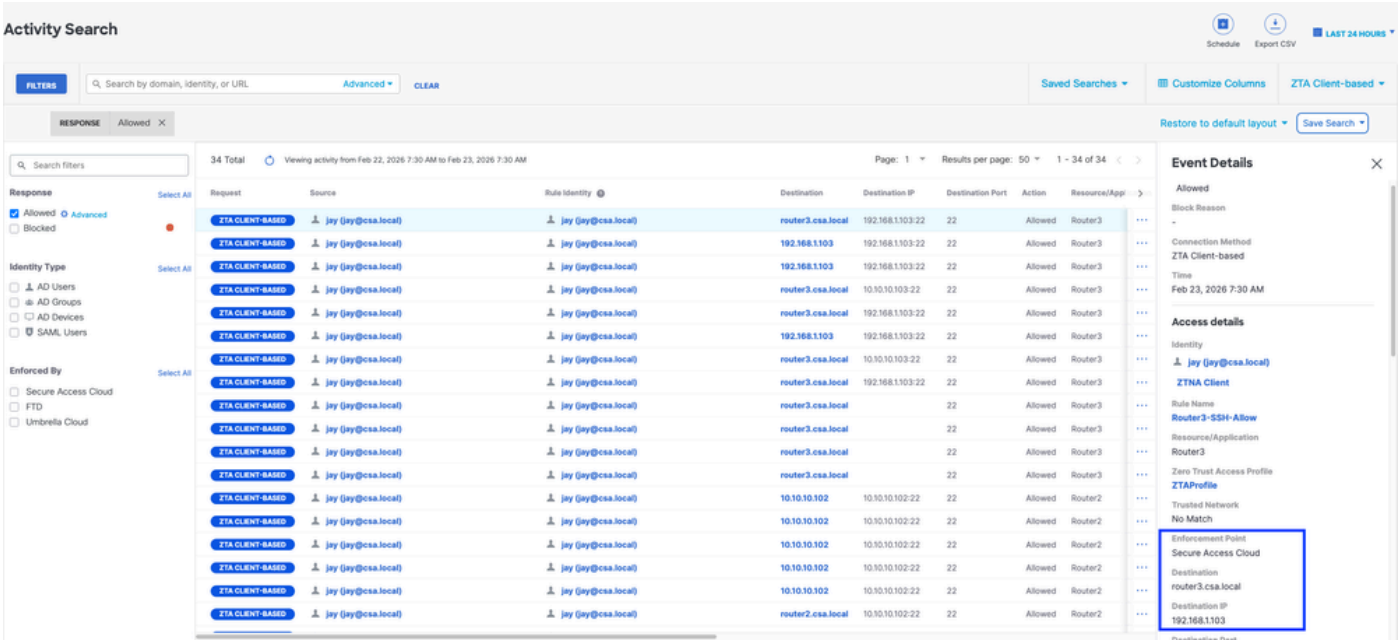


Accesso sicuro - Test PR

5. Verifica registri di ricerca attività accesso sicuro



Accesso sicuro - Ricerca attività



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).