在安全訪問中配置專用資源訪問的通用ZTNA

目錄

簡介

在本文檔中，我們將介紹通過通用ZTNA使用不同流量路徑進行私有資源訪問的配置。

必要條件

在配置通用ZTNA之前，必須完成以下配置

- Cisco Secure Access上的身份提供程式
- 使用證書註冊零信任訪問中的裝置
- 使用思科安全防火牆配置隧道
- 遠端訪問虛擬專用網路
- 安全存取上的資源聯結器
- 安全雲控制上的FTD自註冊

- 應該為各自的安全訪問租戶啟用混合ZTNA功能標誌，請與思科TAC聯絡以啟用該標誌

需求

思科建議您瞭解以下主題：

- 思科安全訪問和防火牆威脅防禦上的IPsec VPN配置
- 身份提供(IdP) — 從Active Directory進行使用者設定
- 思科安全訪問上的遠端VPN配置
- Cisco Secure Access上的資源聯結器部署
- 基於ZTA證書的註冊
- 證書 — OpenSSL、CSR生成、證書模板等

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆威脅防禦（版本7.7.10）
- 思科安全Firepower管理中心（版本7.7.10）
- 思科安全使用者端（ZTA版本5.1.10.1720）
- Windows 11
- Windows 2019 Server — 證書頒發機構
- ESXi上的資源聯結器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

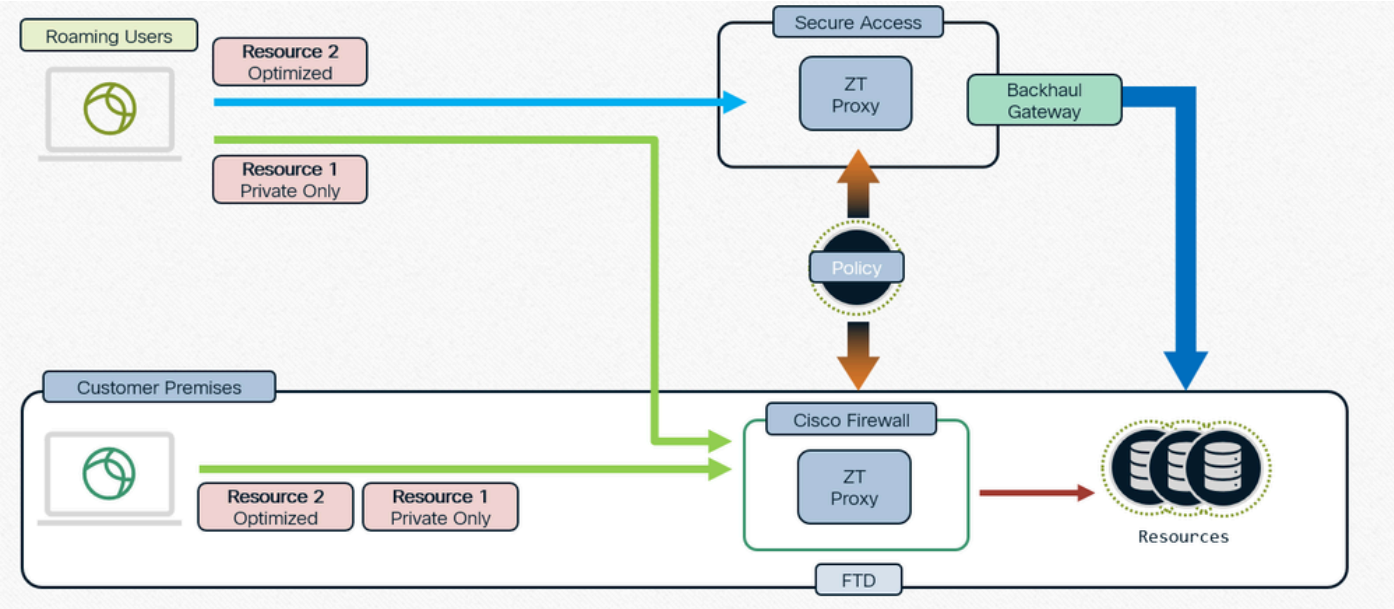
關於通用ZTNA

通用零信任網路訪問(uZTNA)使管理員能夠根據使用者身份（包括使用者信任和狀態）專門允許訪問內部網路資源，而不像RA-VPN那樣授予對整個網路的訪問許可權。uZTNA使管理員能夠保護遠端和本地使用者的內部資源和應用程式。

因為uZTNA不假設授予一個應用的訪問隱含地授權對其他應用的訪問，所以網路攻擊面減少了。

安全訪問評估訪問策略。將忽略從安全防火牆管理中心部署到裝置的所有訪問控制策略。

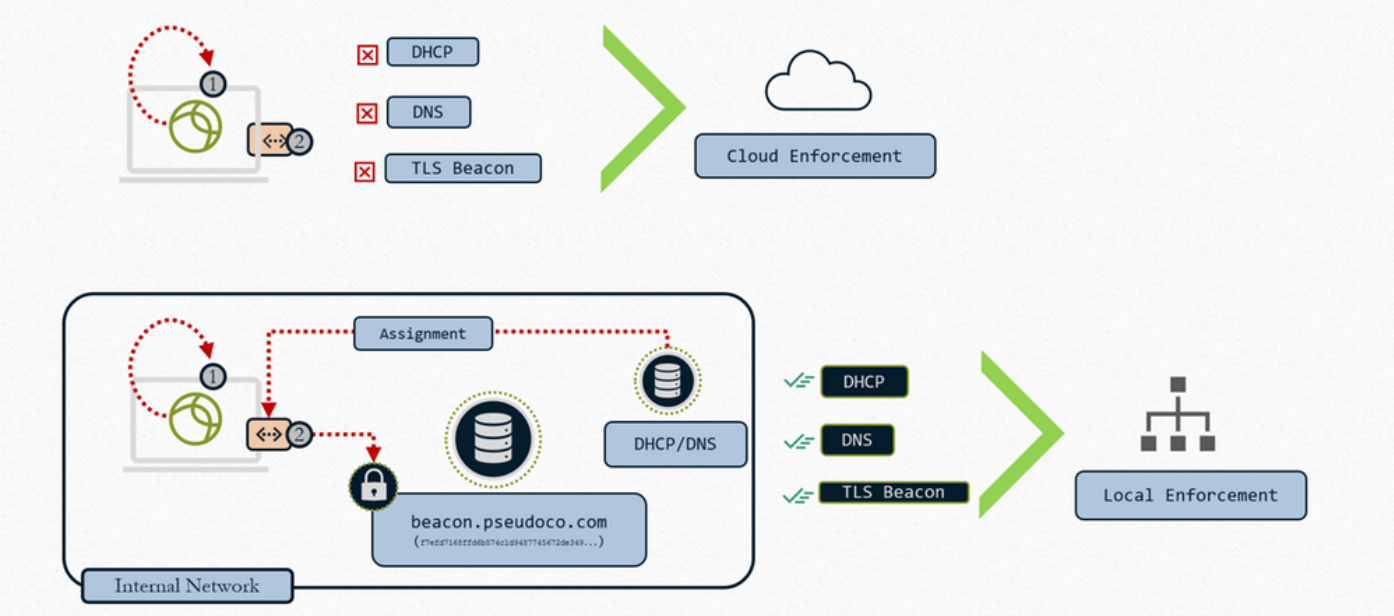
流量代理以及IPS、檔案和惡意軟體策略實施均在Firepower威脅防禦(FTD)上執行。



單一策略，分散式實施

網路偵測

確定雲或本地實施



通用ZTNA — 確定雲或本地實施

1 — 客戶端查詢本地介面以進行網路配置

2 — 客戶端搜尋TLS信標

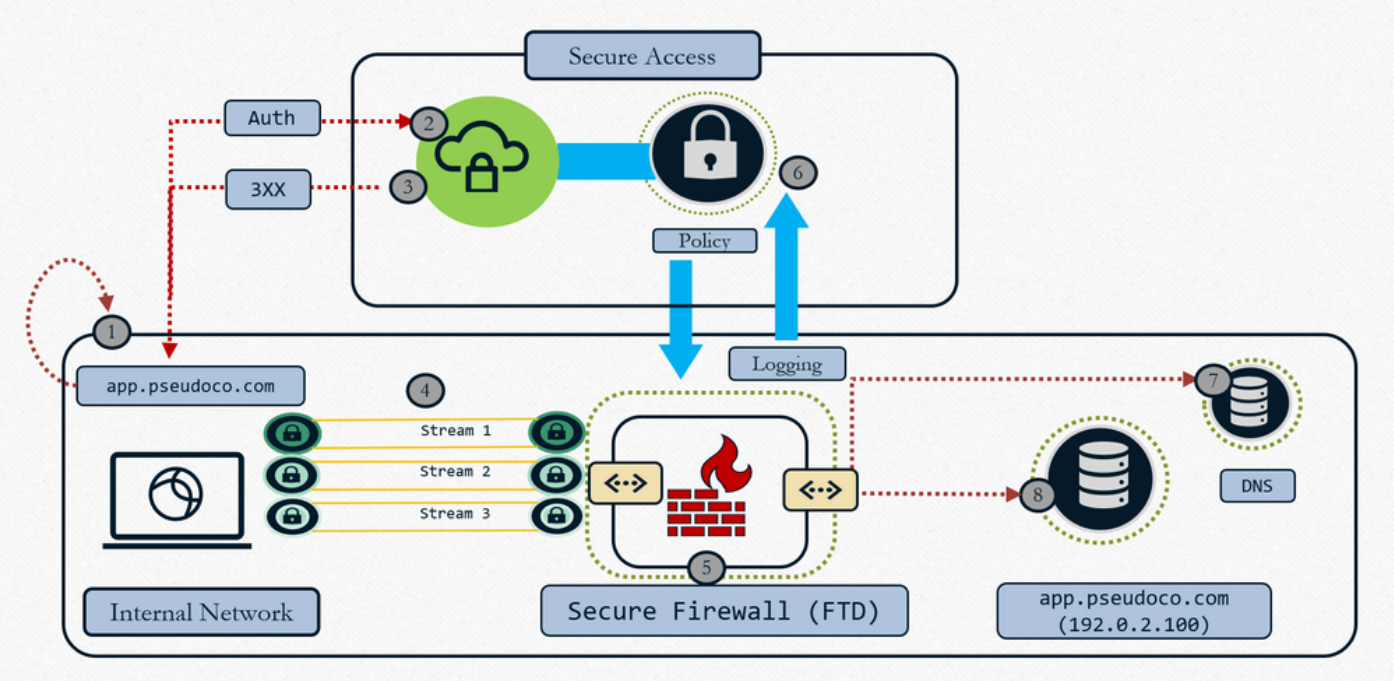
3 — 如果條件匹配 — 本地實施

4 — 如果條件不匹配 — 雲實施

當我們使用「雲或本地實施」配置資源並將TND規則與FTD關聯時，它實際所做的就是傳送到客戶端的一組攔截規則將包括TND規則評估。因此，雲端會告知使用者端評估TND規則。在傳送連線時，我們將網路指紋評估結果放在HTTP報頭中，這樣將告知Proxy我們是線上還是不可信網路，然後Proxy使用該資訊並相應地重定向流量。如果指紋匹配，Zproxy會告訴客戶端將流量重定向到FTD，如果指紋不匹配，則會將流量重定向到雲。請參閱使用受信任網路檢測配置零信任網路訪問

實施型別

- 本地實施路徑：防火牆執行

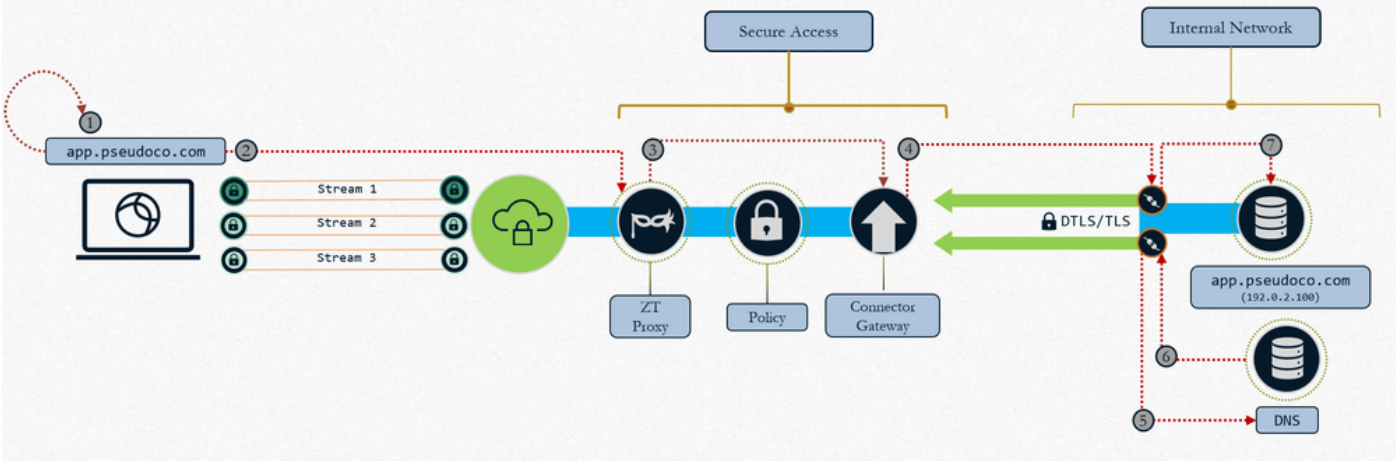


通用ZTNA — 本機執行

1. 使用者請求應用，客戶端捕獲並解析到短期IP（本地主機範圍）的請求
2. 將身份驗證控制流量傳送到安全訪問雲進行策略評估
3. 雲端傳回重新導向至FTD以進行資料計畫執行（如果原則允許）
4. 導向到防火牆配置的頭端（介面）的流量

5. 使用本地代理資料平面實施雲中定義的策略（IPS、惡意軟體、解密）
6. 事件已記錄並複製到雲以實現一致報告
7. Firewall在本地網路上執行DNS解析，以路由資源流量（如果允許）
8. 防火牆建立與資源的連線（與資源建立的新連線），因為防火牆的行為與TCP代理相同

- 雲實施路徑：關閉網路

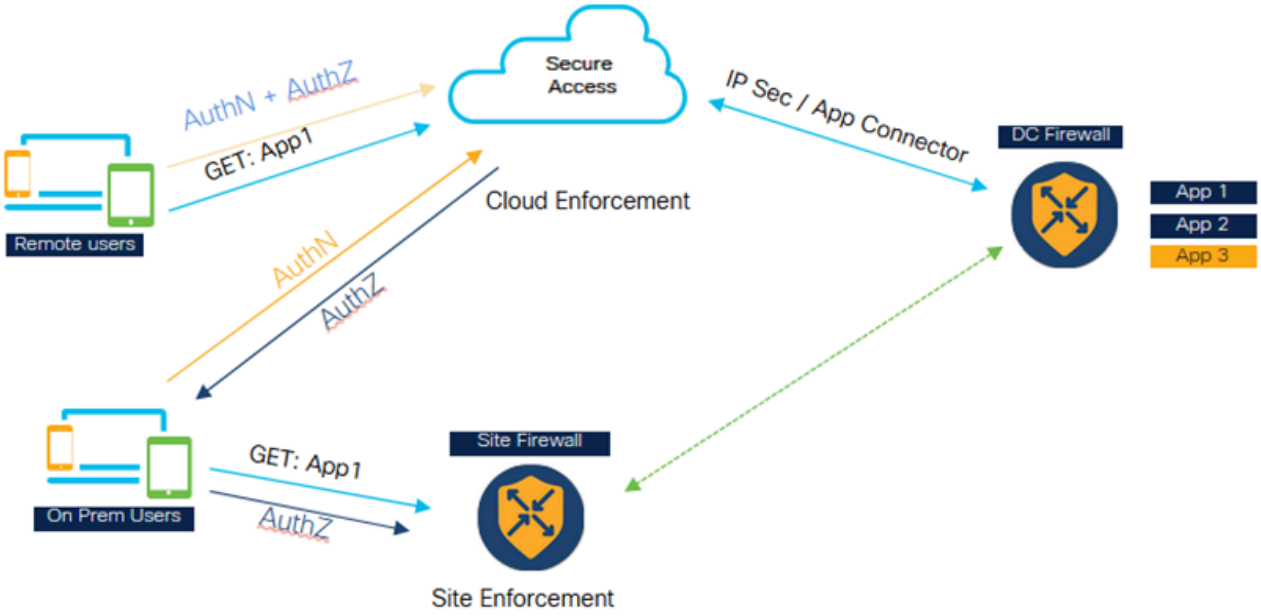


通用ZTNA:雲實施

1. 使用者請求應用，客戶端捕獲並解析到短期IP（本地主機範圍）的請求
2. 流量在安全訪問中傳輸到零信任代理
3. TCP連線被代理並構建到對映資源聯結器，策略在流量上實施
4. 網關建立與資源聯結器的連線
5. 資源聯結器解析資源IP
6. 本地DNS使用資源IP響應
7. 資源聯結器建立與資源的連線

使用案例

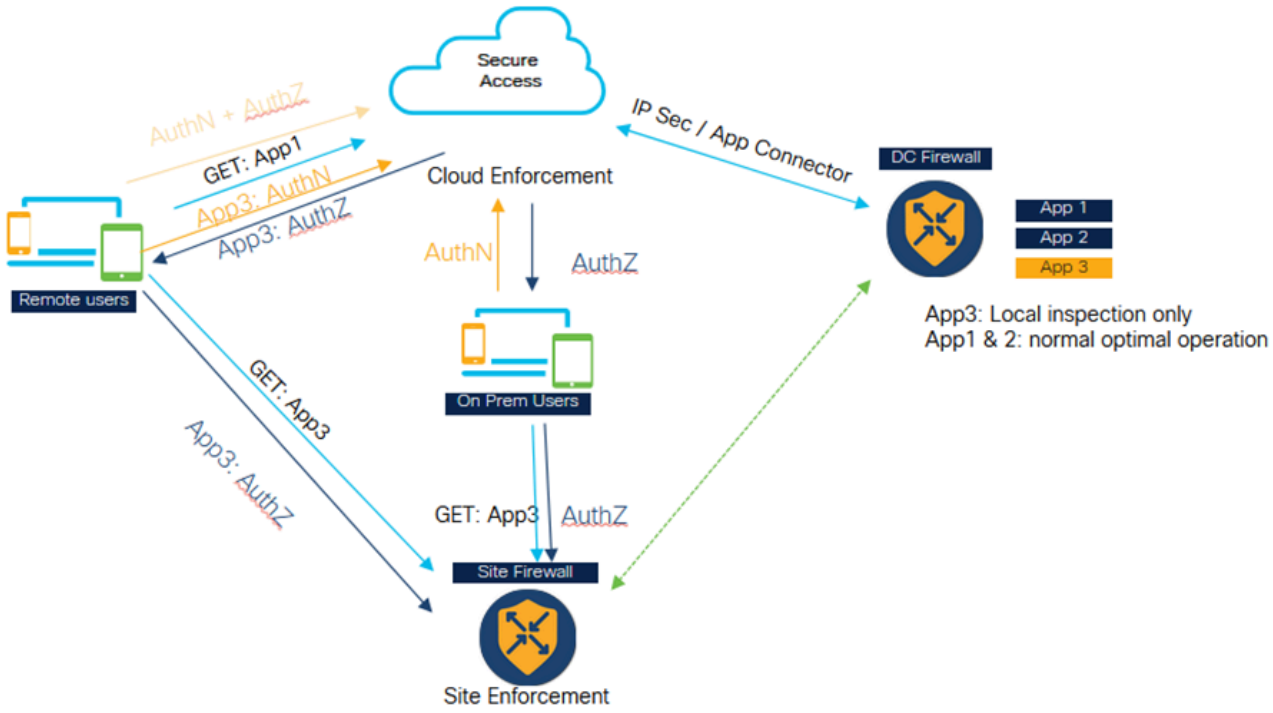
案例1：在現場為使用者提供一致且最佳化的ZTNA



通用ZTNA — 一致和最佳化的ZTNA（現場使用者）

- 安全訪問和防火牆都配置為保護應用程式。
- 如果使用者是遠端使用者，則他們將會轉到Secure Access進行策略評估和檢查。
- 如果使用者是內部/內部部署，則他們將前往防火牆進行專用流量檢測。
- 本地使用者仍然可以轉至Secure進行身份驗證和評估，只有資料路徑流量會轉到防火牆，並根據策略配置進行檢查。
- 通過防火牆訪問應用程式的內部使用者具有效能優勢，因為它避免了流量進入雲然後回遷到資料中心

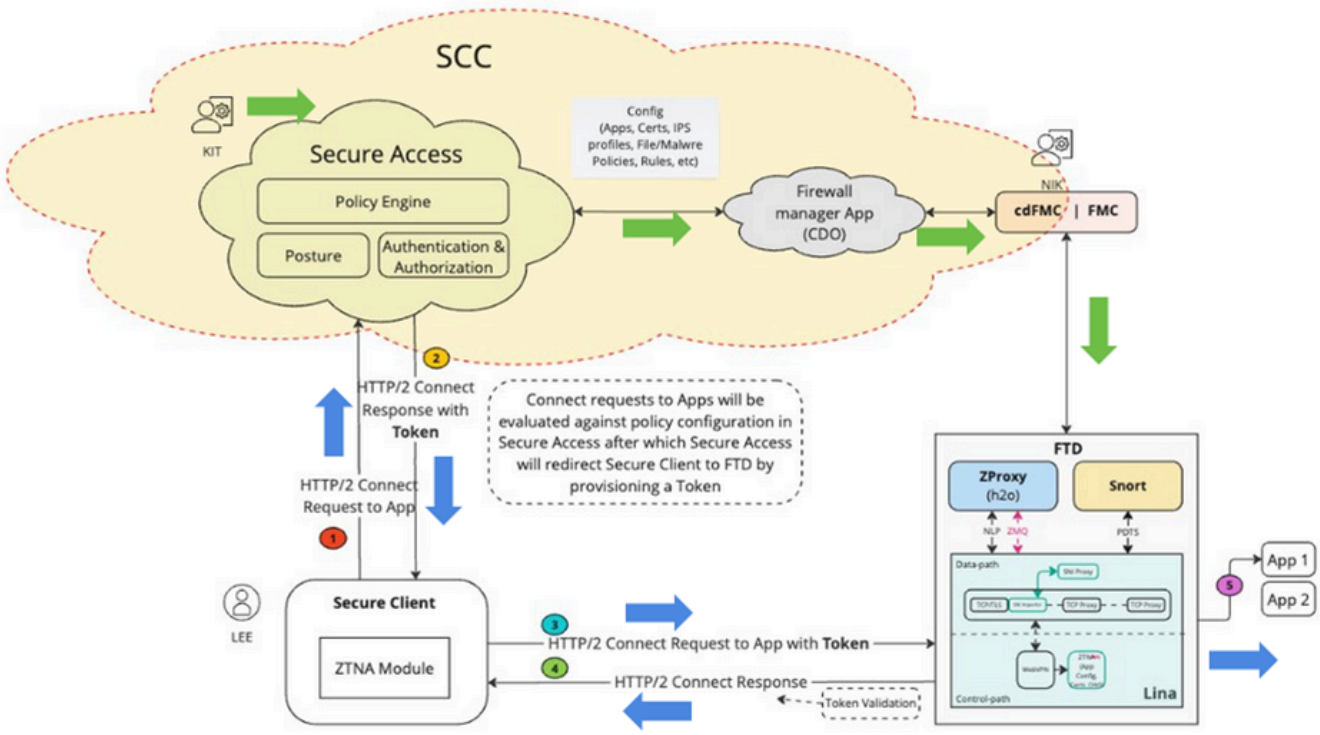
案例2：對敏感申請進行私人檢查



通用ZTNA — 敏感應用的專用檢測

- 可以將某些關鍵應用程式配置為始終通過防火牆進行訪問。
- 應用資料流量無需轉到雲。例如，可能存在原始碼等敏感資料應用程式，客戶不希望將其用於雲。
- 在此類情況下，遠端和永久使用者流量始終會通過防火牆並受到檢查。但是，在此場景中，身份驗證和策略評估始終在雲中進行，只有資料部分流量通過防火牆。

架構元件



通用ZTA — 架構元件

安全雲控制(SCC)是uZTNA解決方案的主要管理器。uZTNA是第一個在SCC之上構建的功能。

在SCC中，我們有兩個微應用安全訪問和防火牆。一旦設定了SCC並啟用了所需的功能標誌，我們將能夠在SCC面板的左側看到這些微應用。

安全客戶端：在安全客戶端中，我們必須啟用零信任訪問模組(ZTNA)，我們需要註冊到ZTNA模組才能訪問應用。

防火牆威脅防禦:FTD會保護這些應用程式。FTD執行也稱為H2O的ZT代理（與在Secure Access Cloud中執行的代理相同）

現在，當使用者（例如KIT）在Secure Access微應用上配置私有資源和策略時，此配置將被推送到SCC中的防火牆微應用。防火牆應用程式瞭解FTD、FTD組態的內部機制，以及如何在FTD上部署和管理組態。因此，Firewall應用會驗證此配置，並呼叫FMC API將配置推送到FMC，最終在FTD上部署它。FTD可以啟用自動部署選項，這樣管理員（例如Nick）就不必進行手動部署。

1.當使用者（例如Lee）嘗試訪問應用程式時，安全客戶端使用mTLS通道連線到Secure Access。安全訪問使用客戶端裝置證書對使用者進行身份驗證。然後，它評估為該使用者和該應用程式配置的授權、狀態和其他策略。

2.安全訪問，如果最終發現應用受到防火牆的保護，則生成身份驗證令牌，告知防火牆已經對其進

行身份驗證和授權。身份驗證權杖已加密，並由安全存取簽署

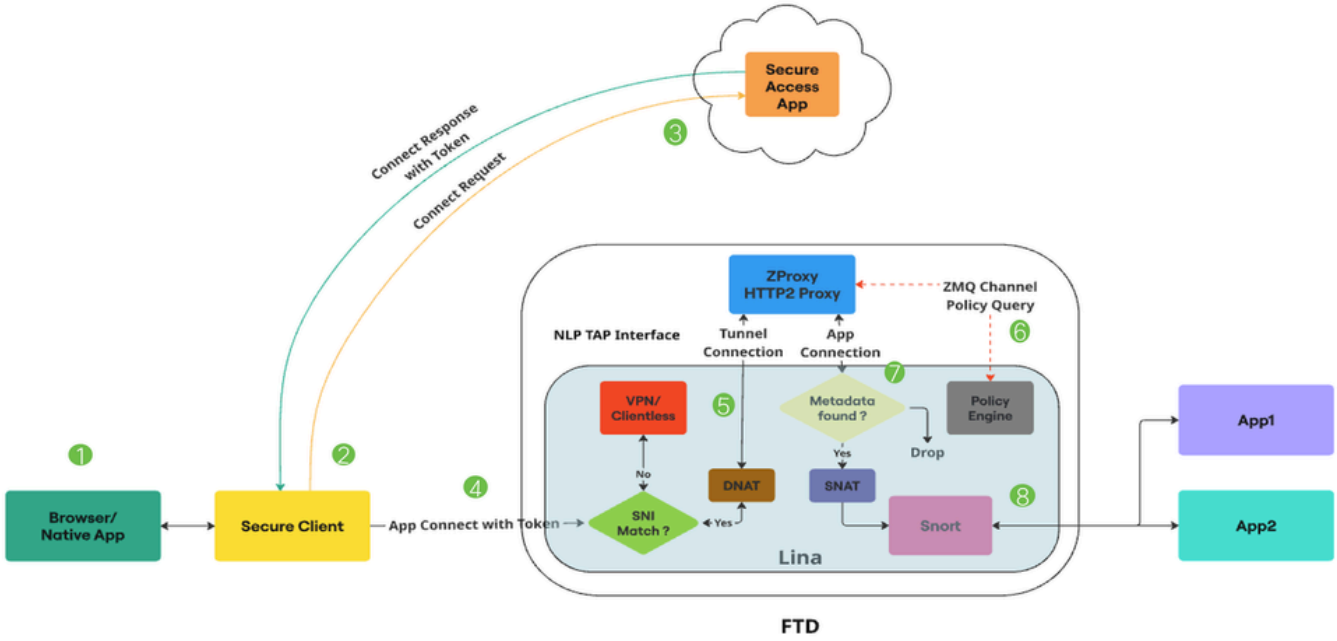
3.安全存取會將安全使用者端與驗證權杖一起重新導向至FTD。

4.安全客戶端與FTD建立另一個連線，它是通過mTLS通道的HTTP2連線。它會傳送與令牌一起訪問的應用程式的CONNECT請求。

5. FTD現在會驗證權杖，如果成功驗證權杖，則允許使用者訪問該應用程式。然後，FTD將確認傳回安全使用者端

封包流量

通用ZTNA詳細資料包流



通用ZTA — 封包流

1.使用者嘗試通過Web瀏覽器或本地應用程式訪問應用程式。

2.安全客戶端會攔截連線，並將其標識為嘗試訪問私有資源的使用者。

3.安全客戶端與安全訪問建立mTLS連線，請求訪問應用程式。安全訪問檢查通用ZTNA策略和狀態配置檔案是否合規。如果一切正常，安全訪問將生成包含基本資訊（如使用者詳細資訊、應用程式詳細資訊和IPS/檔案策略）的訪問令牌。

4.存取權杖經過加密，並由Secure Access簽署。然後，Secure Access會將安全使用者端連同權杖重新導向到FTD。

5.當資料包到達Lina資料路徑時，SNI檢查器會攔截連線，並驗證客戶端Hello中的伺服器名稱（SNI擴展）是否與裝置上配置的代理FQDN匹配。如果SNI匹配，則連線將定向到ZProxy。如果SNI不匹配，則連線將定向到可與Universal ZTNA共存的其他功能。

舉例來說：VPN、強制網路門戶或無客戶端ZTNA。ZProxy（支援HTTP/2上的MASQUE協定）將作為非Lina進程在專用核心上運行。Lina和ZProxy之間的通訊利用NLP分接頭介面處理資料流量。連線的目標IP由SNI檢查器轉換為TAP介面IP。

6.當ZProxy收到來自安全客戶端的mTLS隧道連線時，它驗證安全客戶端傳送的客戶端裝置證書。它也會驗證使用APP Connect傳送的訪問令牌。Lina和ZProxy之間有一個零MQ通道。它主要用於交換控制消息。ZProxy通過與Lina通訊來使用此通道進行專用資源的FQDN解析。

零MQ通道也用於將存取權杖中現有的資訊傳播到Lina。(範例：規則ID、策略ID等)Lina接收訪問令牌資訊並將其儲存在後設資料資料庫中。

7.交換控制消息後，ZProxy啟動與私有資源的新連線。這可以是TCP或UDP。然後，Lina為此應用連線執行後設資料資料庫查詢。如果未找到後設資料，則刪除連線

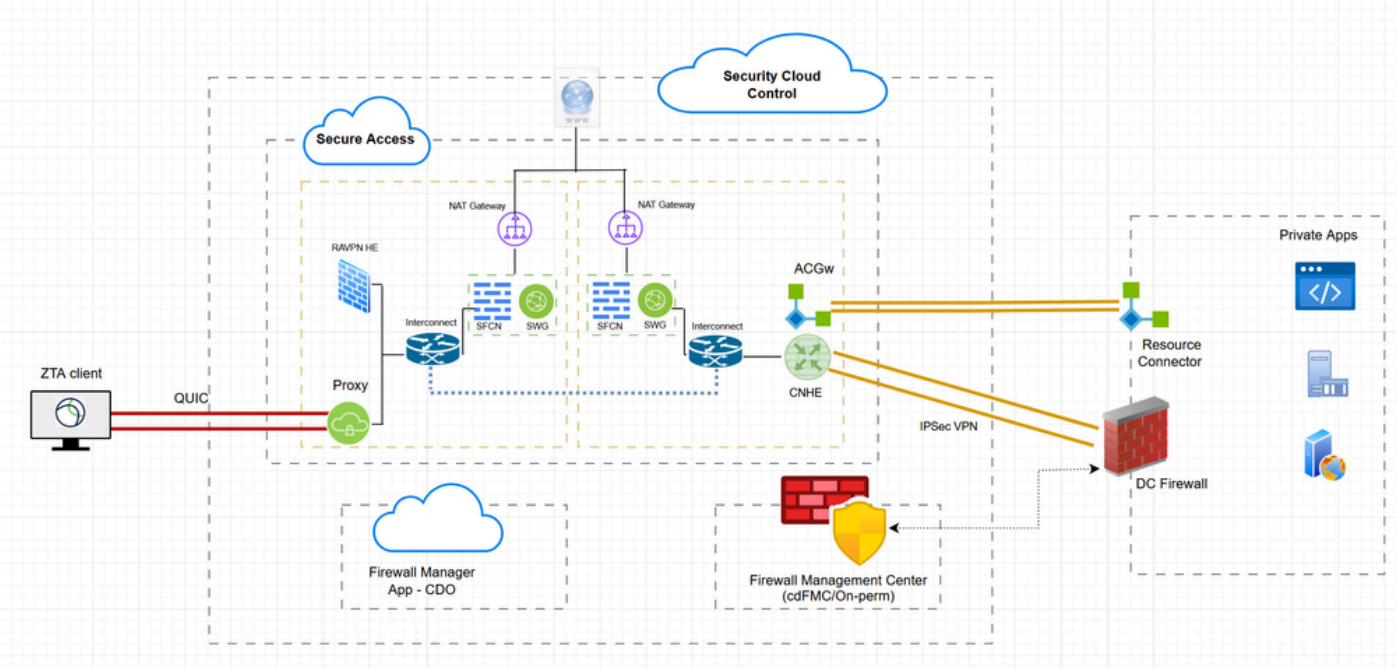
8.由於應用連線源自ZProxy，因此將具有內部IP（例如：169.251.1.2）作為源IP。在將此資訊傳送出去之前，此資訊將轉換為FTD輸出介面IP。然後，Lina僅在訪問令牌中存在檔案或IPS策略時標籤用於Snort檢查的通用零信任流。從訪問令牌獲得的規則ID在連線後設資料中傳遞到Snort。

9.通用零信任規則以及相應的檔案和IPS策略對映通過FMC推送到FTD。Snort中的零信任外掛將在初始化期間載入這些規則。僅當從安全訪問獲取用於訪問該私有資源的訪問令牌中提到檔案或IPS策略時，Lina才會標籤用於Snort檢查的通用零信任流流。

從訪問令牌獲得的規則ID通過Conn Meta傳遞到Snort。對於所有通用零信任流流，Snort中的零信任外掛將為從該Conn Meta獲得的規則ID執行規則查詢。如果找到規則匹配，將允許該流，並且特定於該規則的IPS和檔案策略將應用於該流。如果未找到規則匹配，Snort中的零信任外掛將阻止該流。

設定

網路圖表

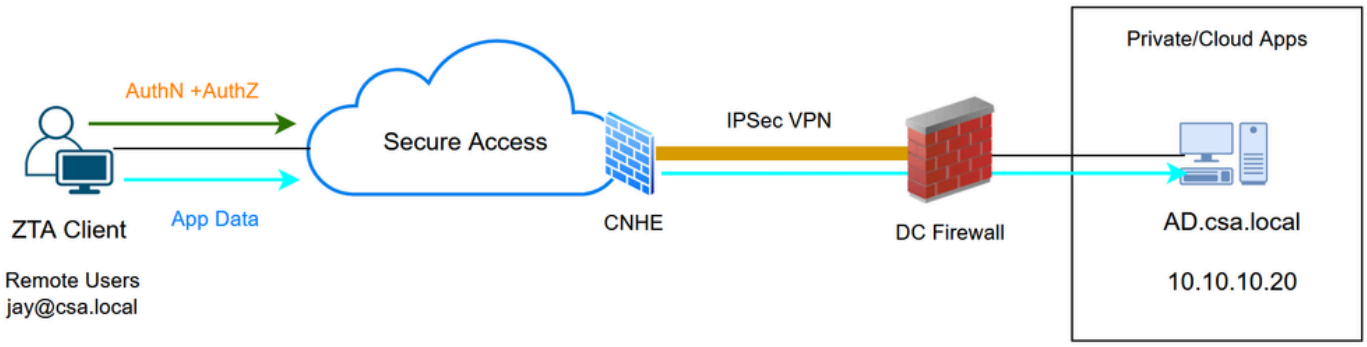


混合ZTNA — 網路圖表

測試案例

測試案例1： 遠端使用者 — 雲實施

在此測試案例中，我們將通過雲實施通過網路隧道組訪問私有資源。在這種情況下，策略評估和應用資料都將通過ZTA模組被安全訪問攔截。這是一個傳統流程，我們可以通過網路隧道組或資源聯結器從ZTA註冊客戶端訪問私有應用程式

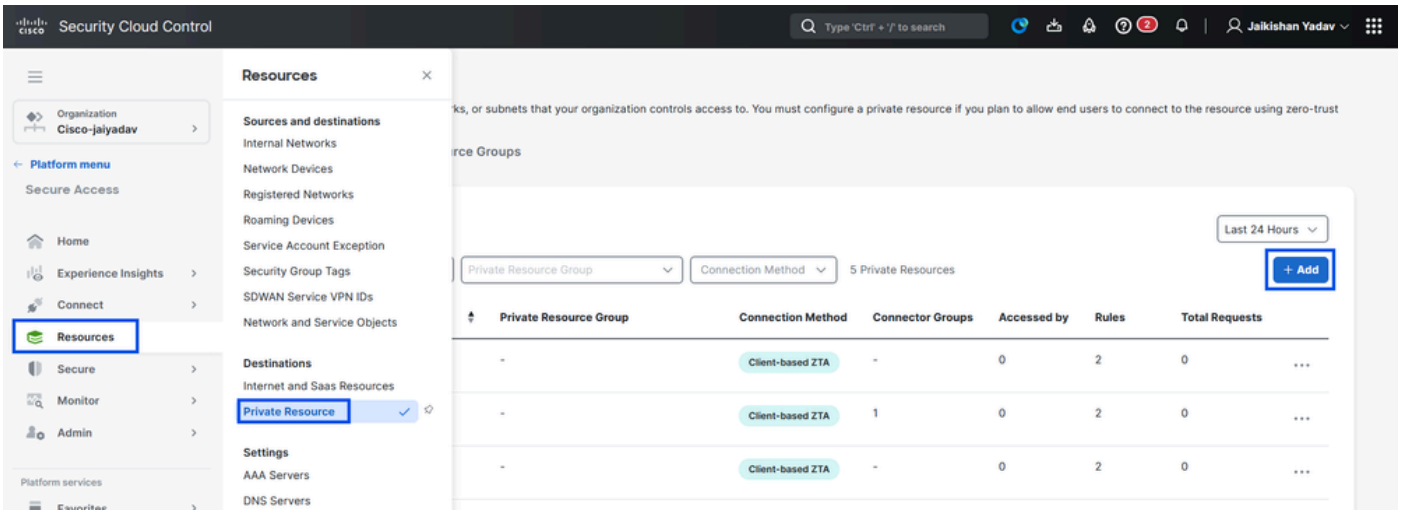


通用ZTA — 測試用例拓撲

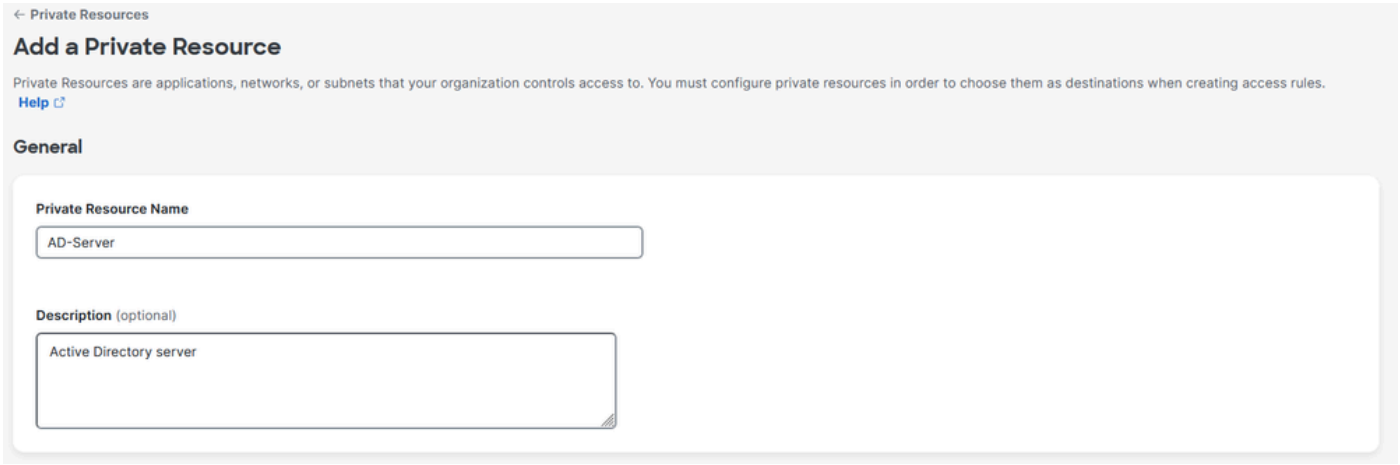
第1步 — 在安全訪問中定義專用資源

配置可通過零信任訪問(ZTA)註冊裝置訪問私有資源（具有雲實施）

1. 導覽至Resources > Destinations > Private Resources >按一下+Add

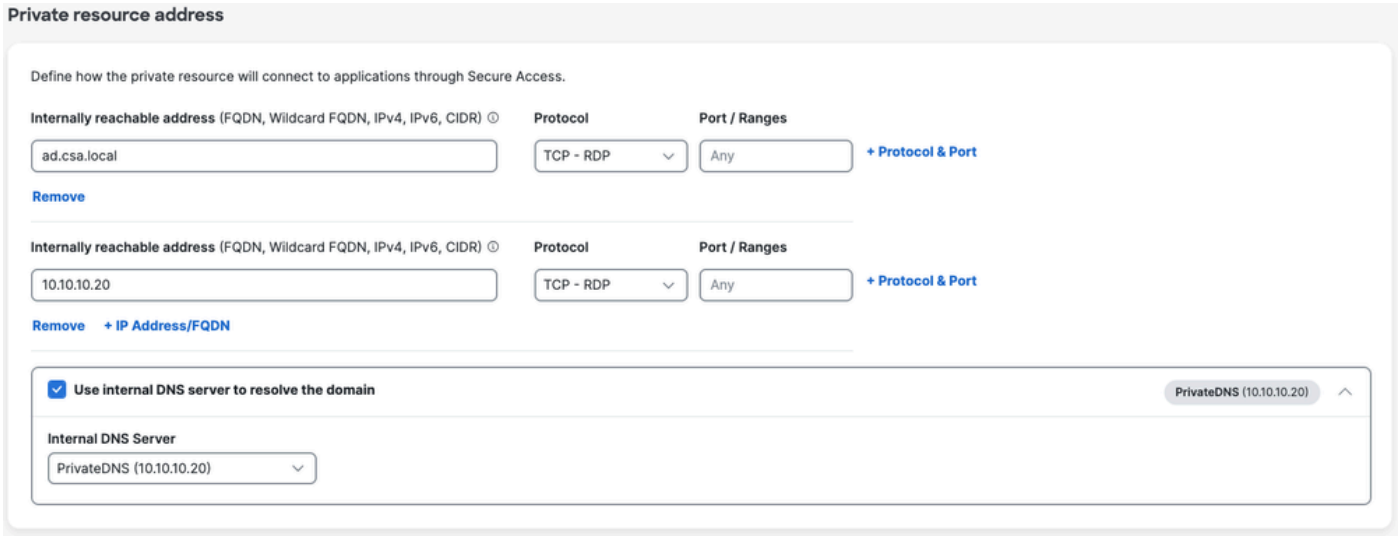


2.對於私有資源名稱，輸入資源有意義的名稱。對於Description，建議您提供諸如資源用途或資源擁有者名稱等資訊。

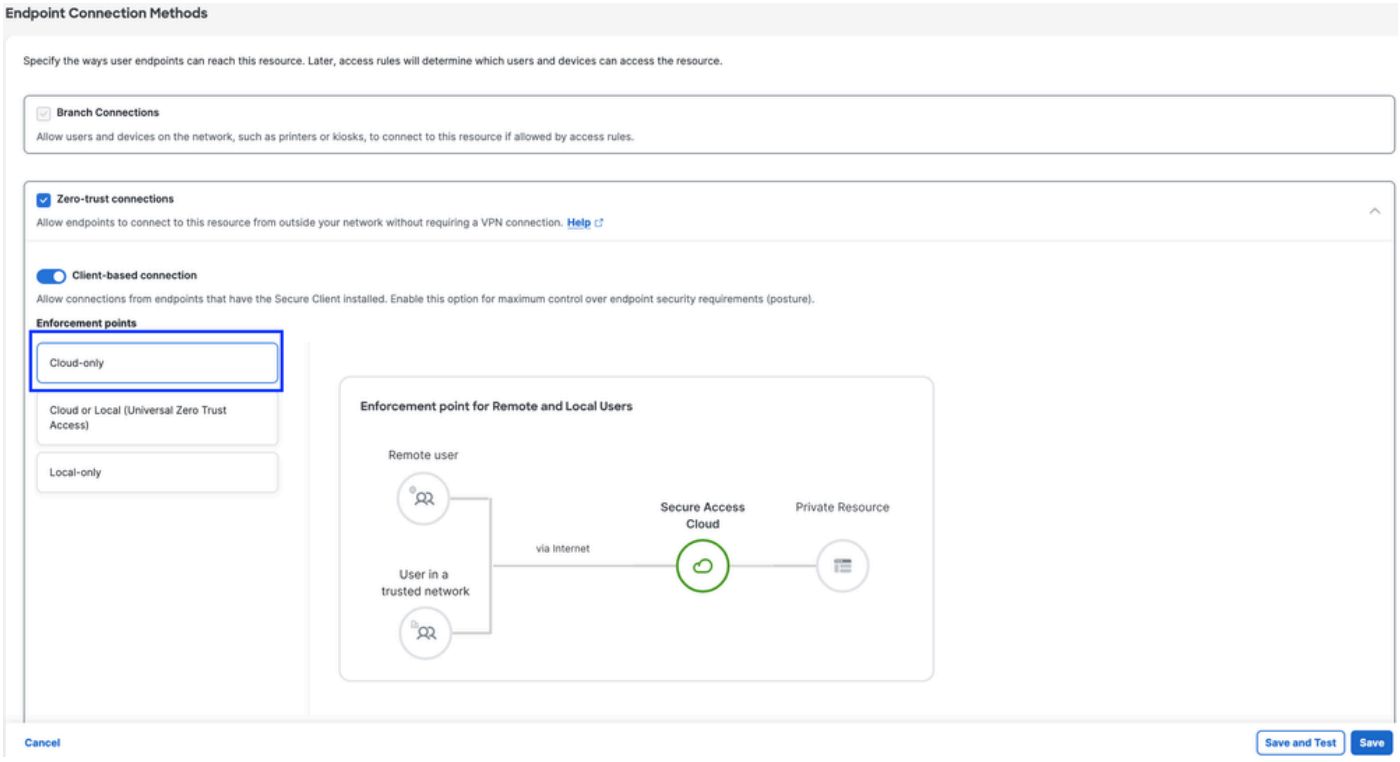


3.輸入要訪問的專用資源的FQDN。我們還可以定義專用資源的IP地址。有關詳細資訊，請參閱新增專用資源

4.選擇內部DNS伺服器以解析域



5. 選擇端點連線方法

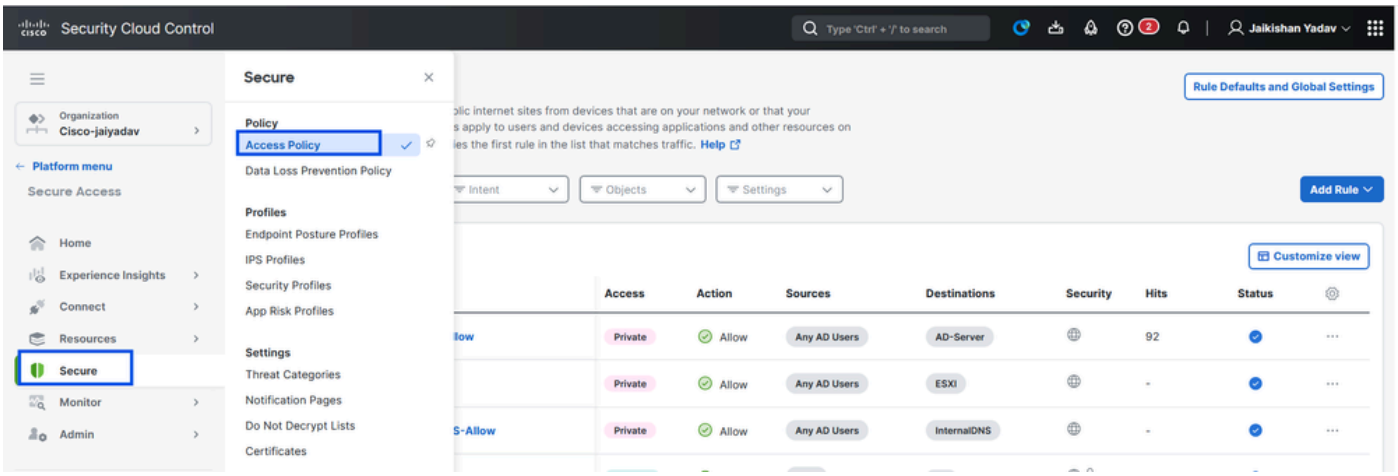


6. 按一下「Save」

第2步 — 建立專用訪問規則

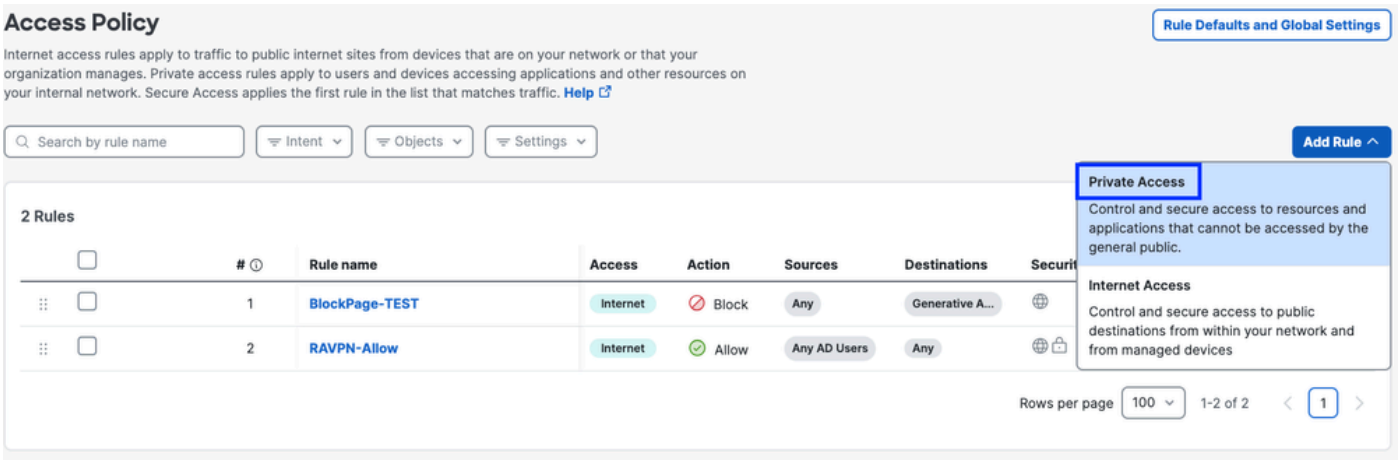
在Secure Access上配置專用訪問，以便由Universal ZTA註冊使用者訪問。有關詳細資訊，請參閱[專用訪問規則]

1. 導覽至Secure > Access Policy



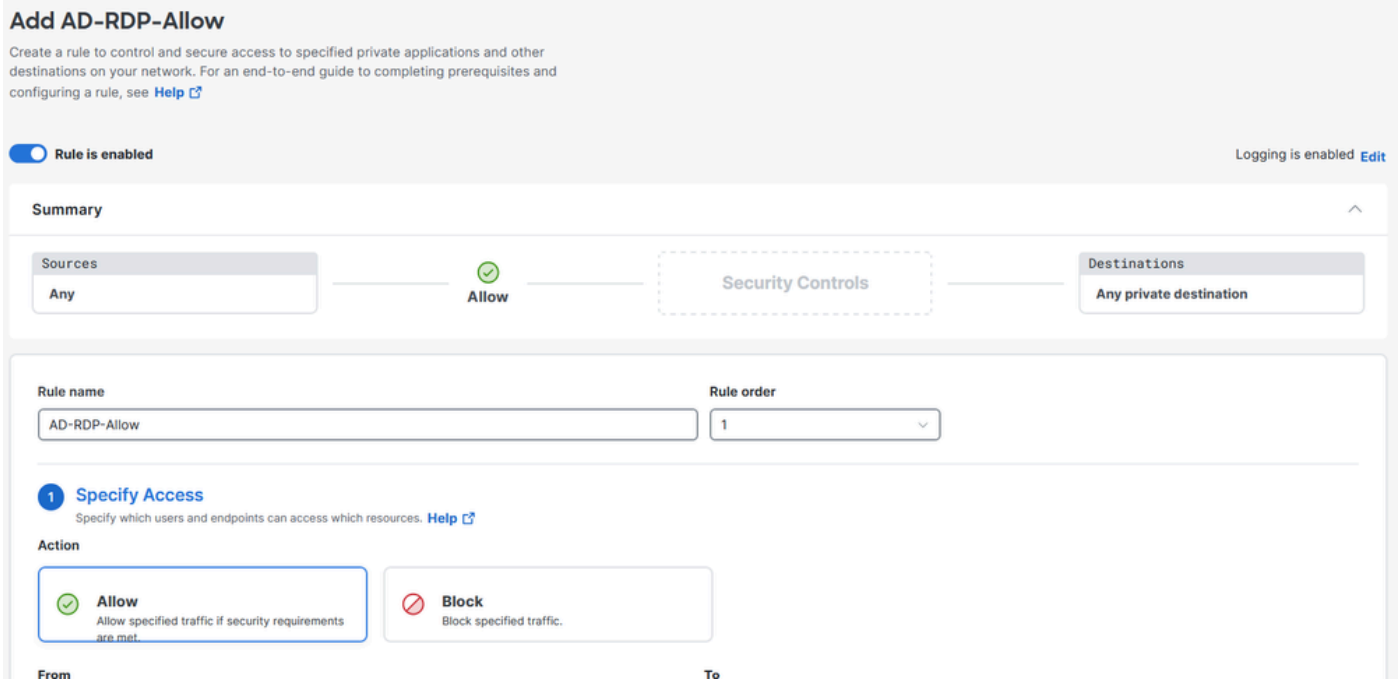
安全訪問 — 訪問策略配置

2.按一下Add Rule，然後選擇Private Access。
規則頂部是描述規則的已配置元件的摘要。



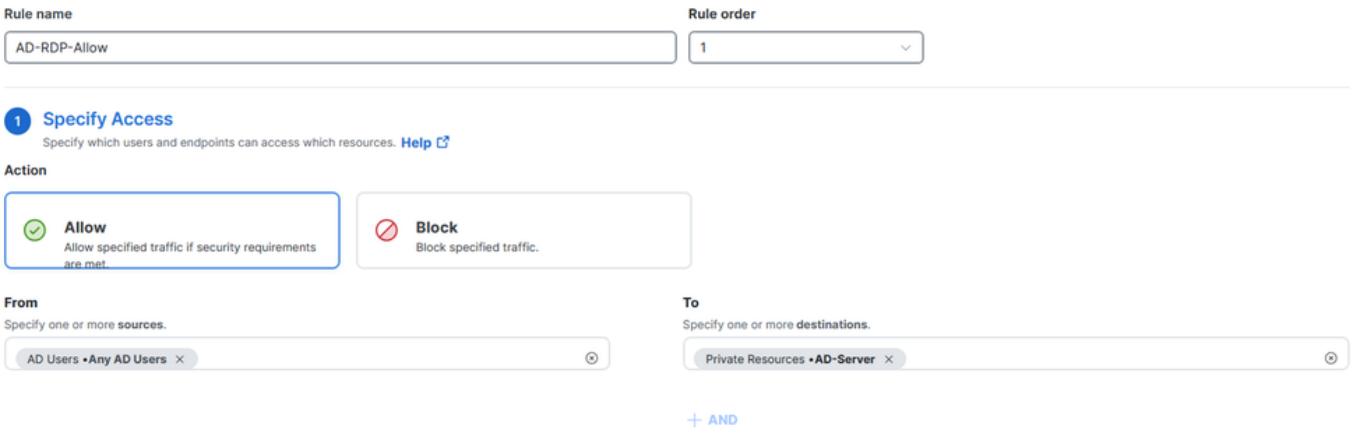
安全訪問 — 訪問策略配置

3.新增規則名稱



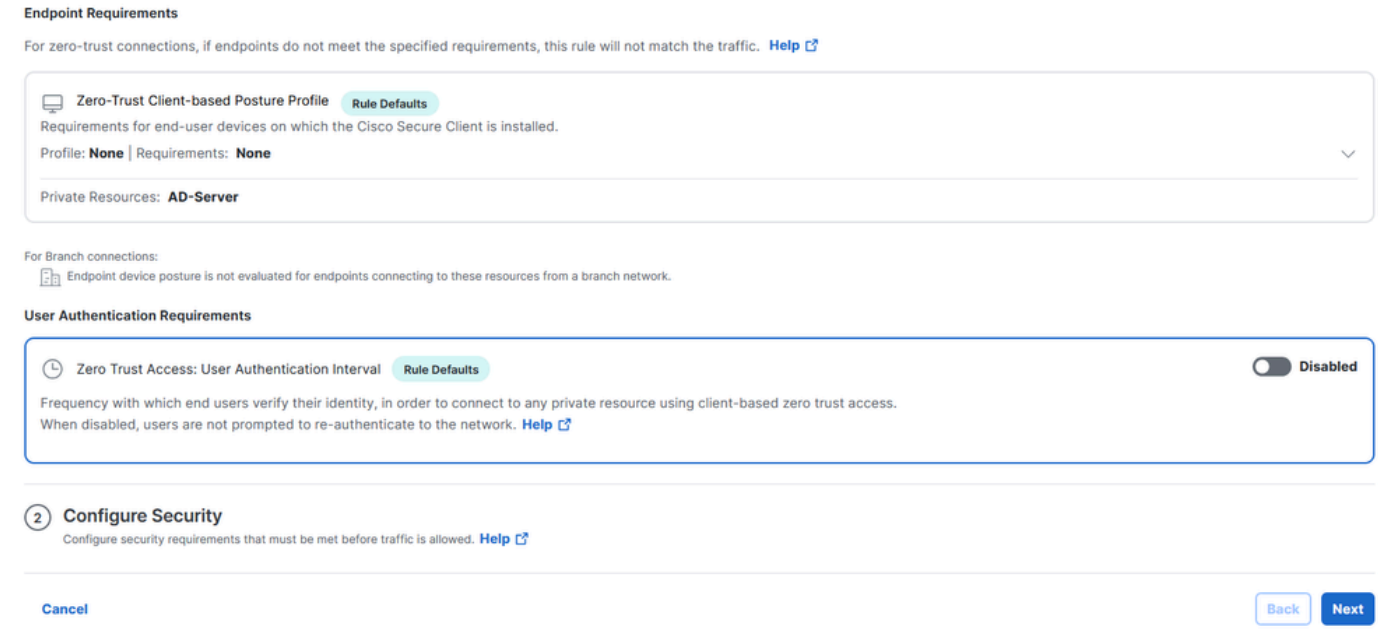
安全訪問 — 訪問策略配置

4.選擇規則操作，然後選擇來源和目標



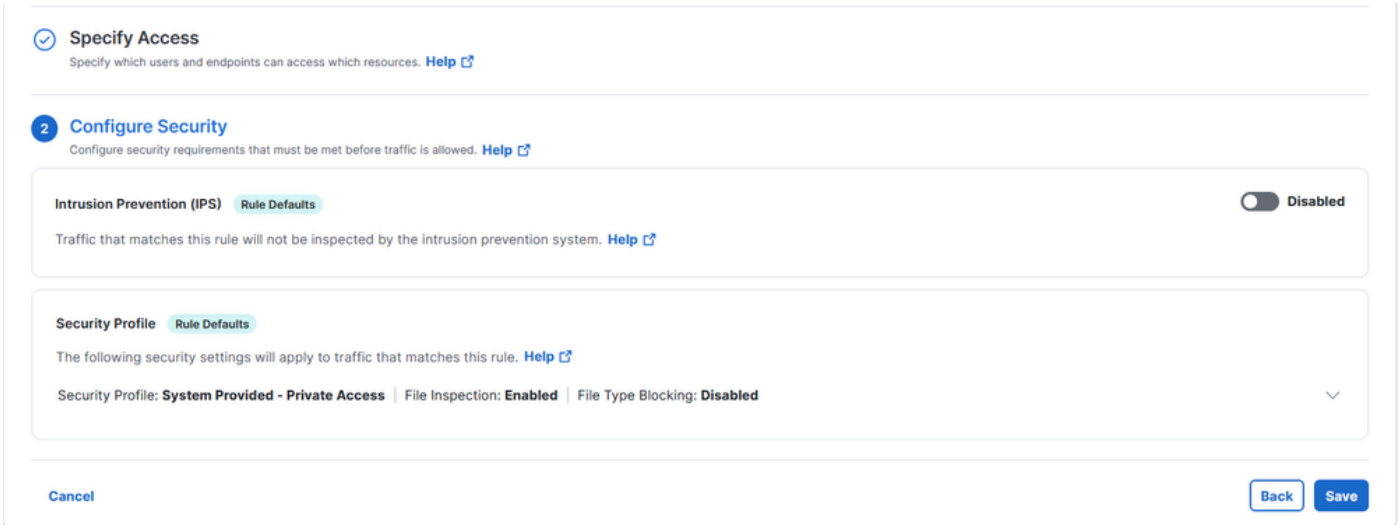
安全訪問 — 訪問策略配置

5.配置終端要求



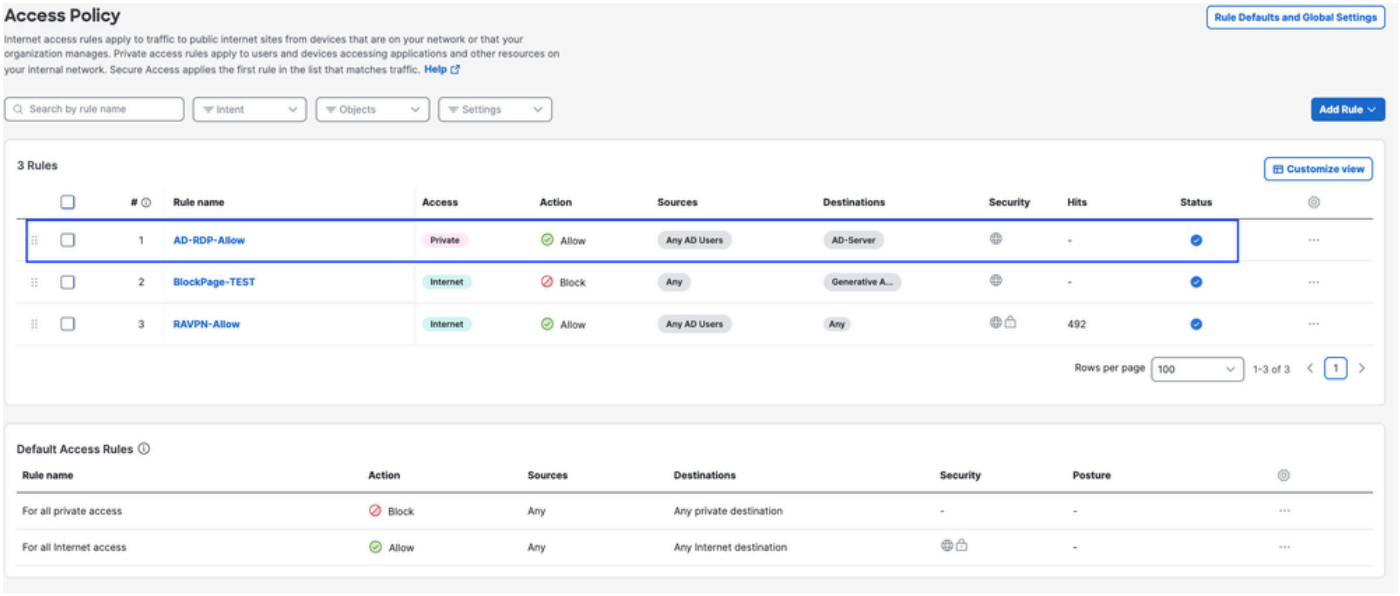
安全訪問 — 訪問策略配置

6. 配置安全性



安全訪問 — 訪問策略配置

7.按一下Save

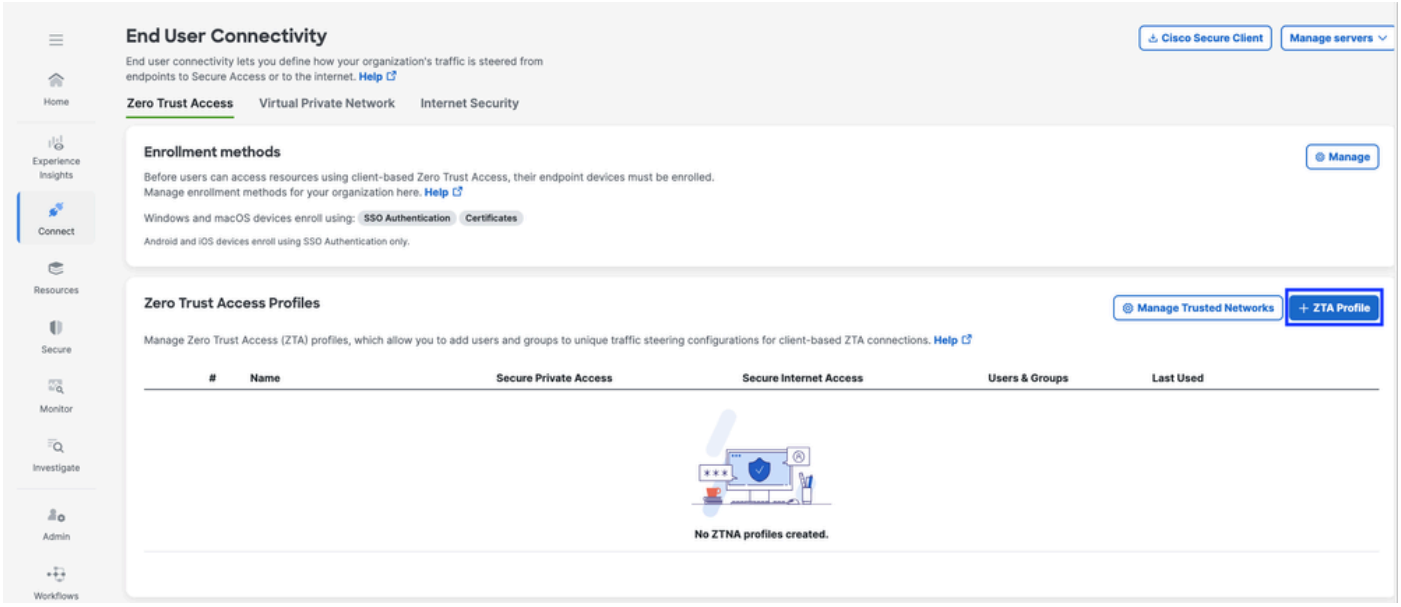


安全訪問 — 訪問策略配置

第3步向ZTA配置檔案中新增專用資源

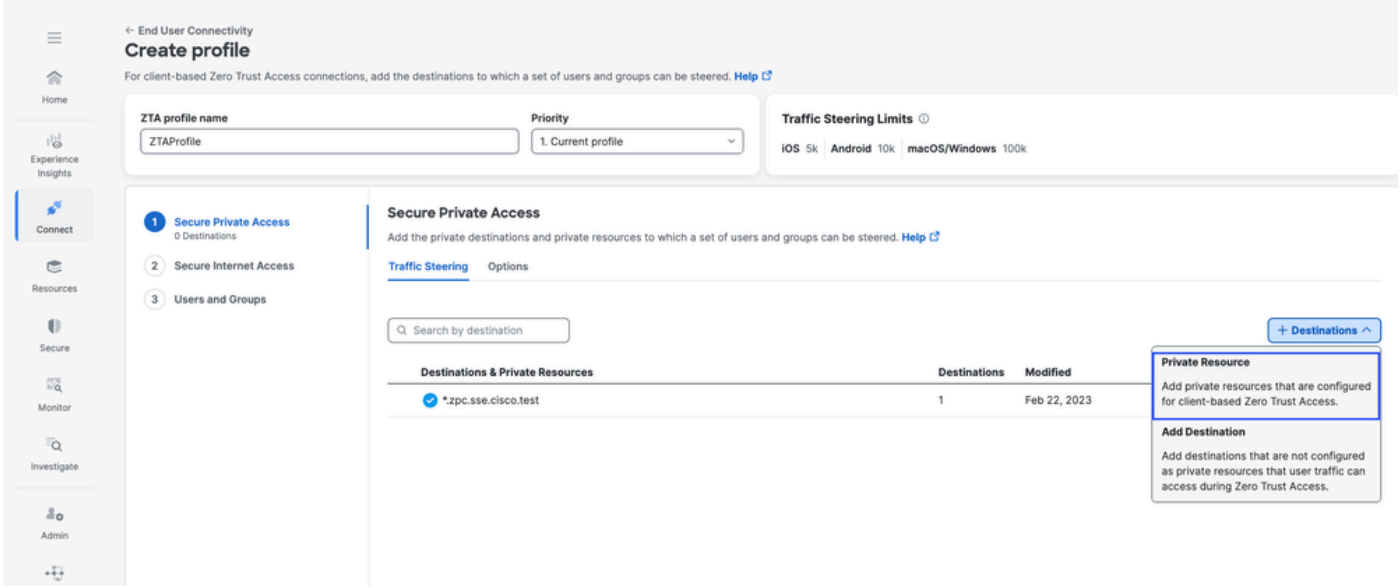
如果您使用的是自定義ZTA配置檔案，則需要將相應的專用資源新增到ZTA配置檔案中

1.導航至Connect > End User Connectivity > Zero Trust Access，然後按一下+ZTA Profile

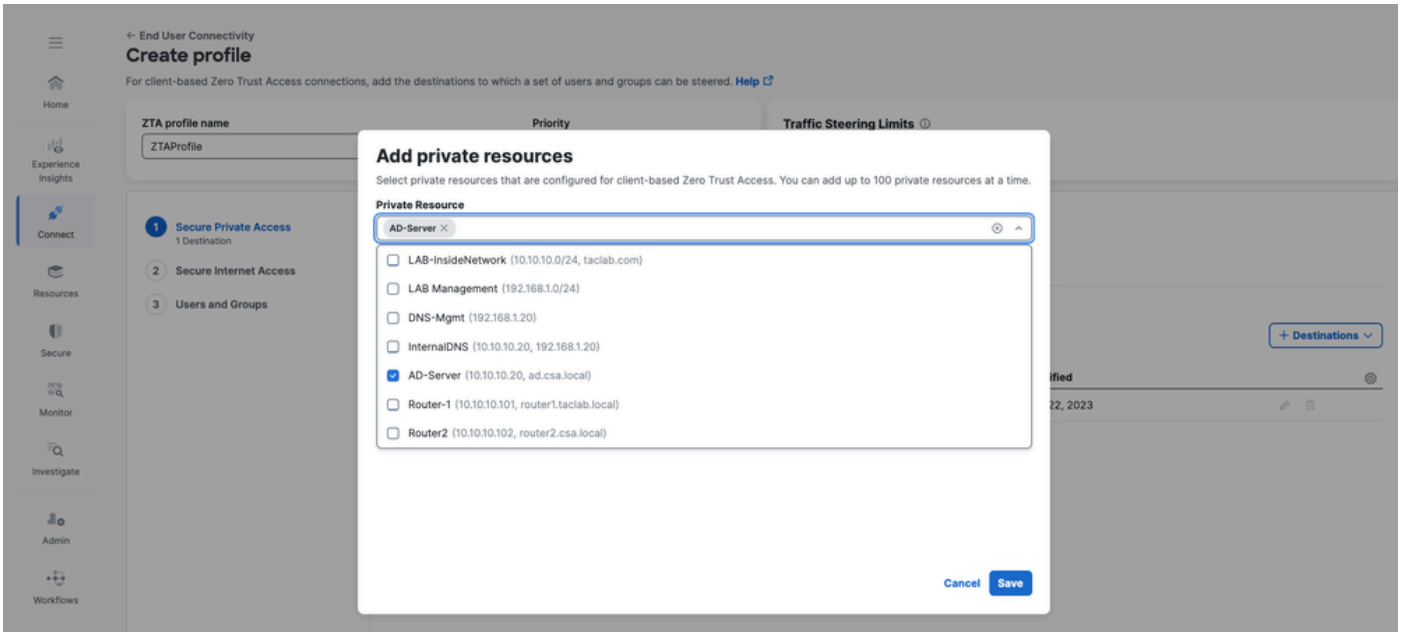


安全訪問 — ZTA配置檔案

2.新增專用資源

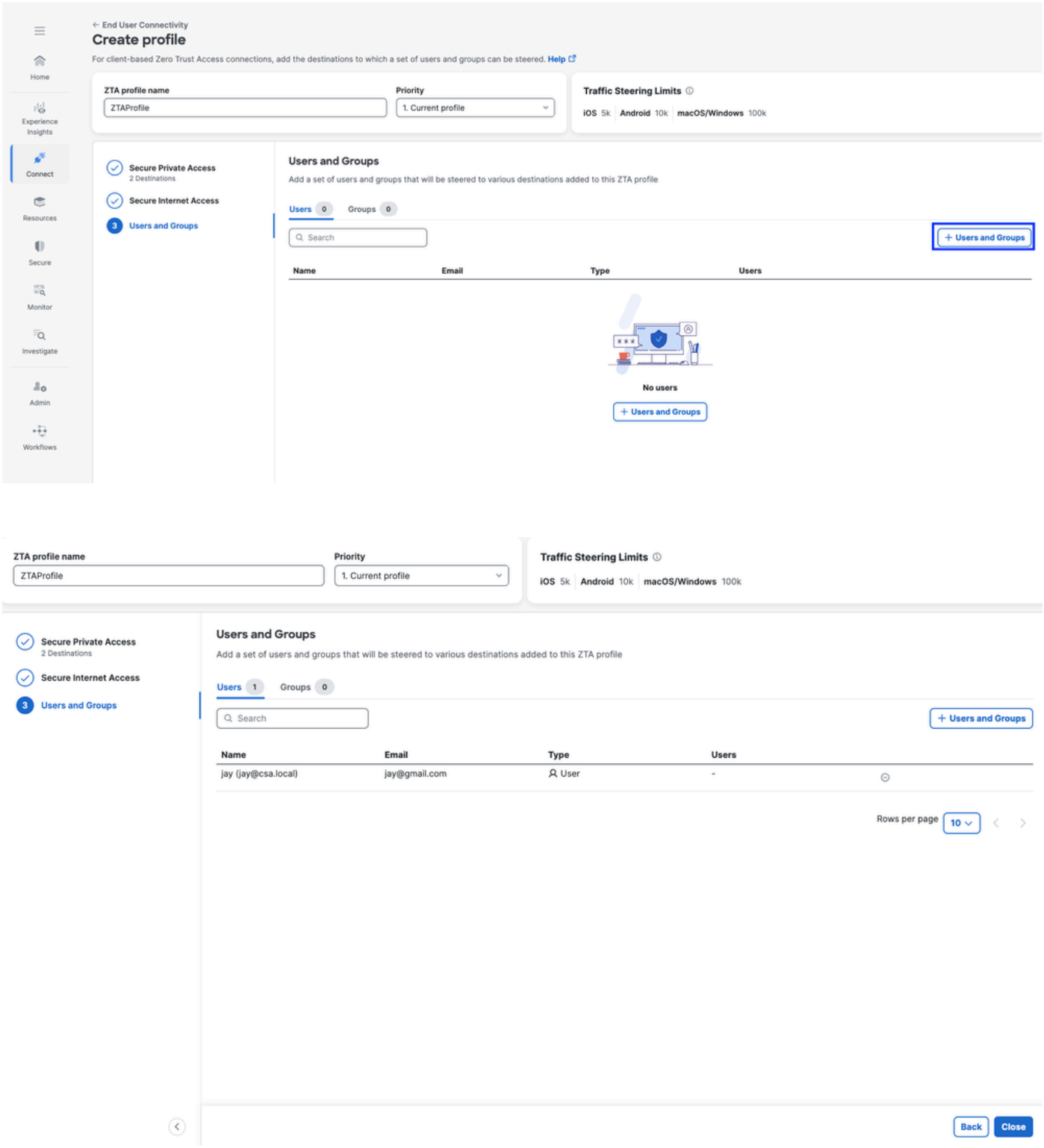


安全訪問 — ZTA配置檔案



安全訪問 — ZTA配置檔案

3.新增使用者和組



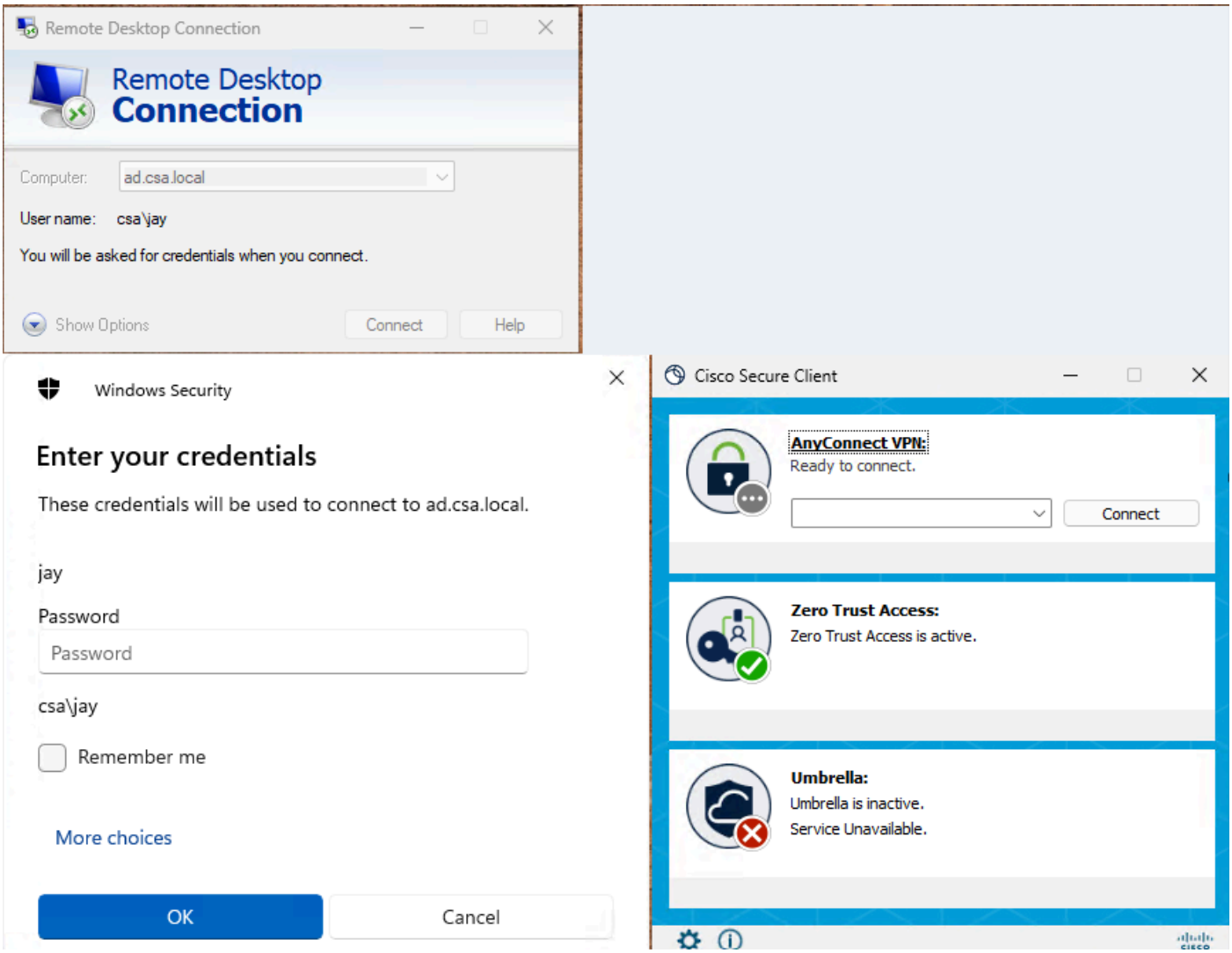
安全訪問 — ZTA配置檔案

附註：對於分配的專用資源，將配置推入並同步到客戶端可能需要15-20分鐘

步驟 — 4驗證對專用資源的訪問

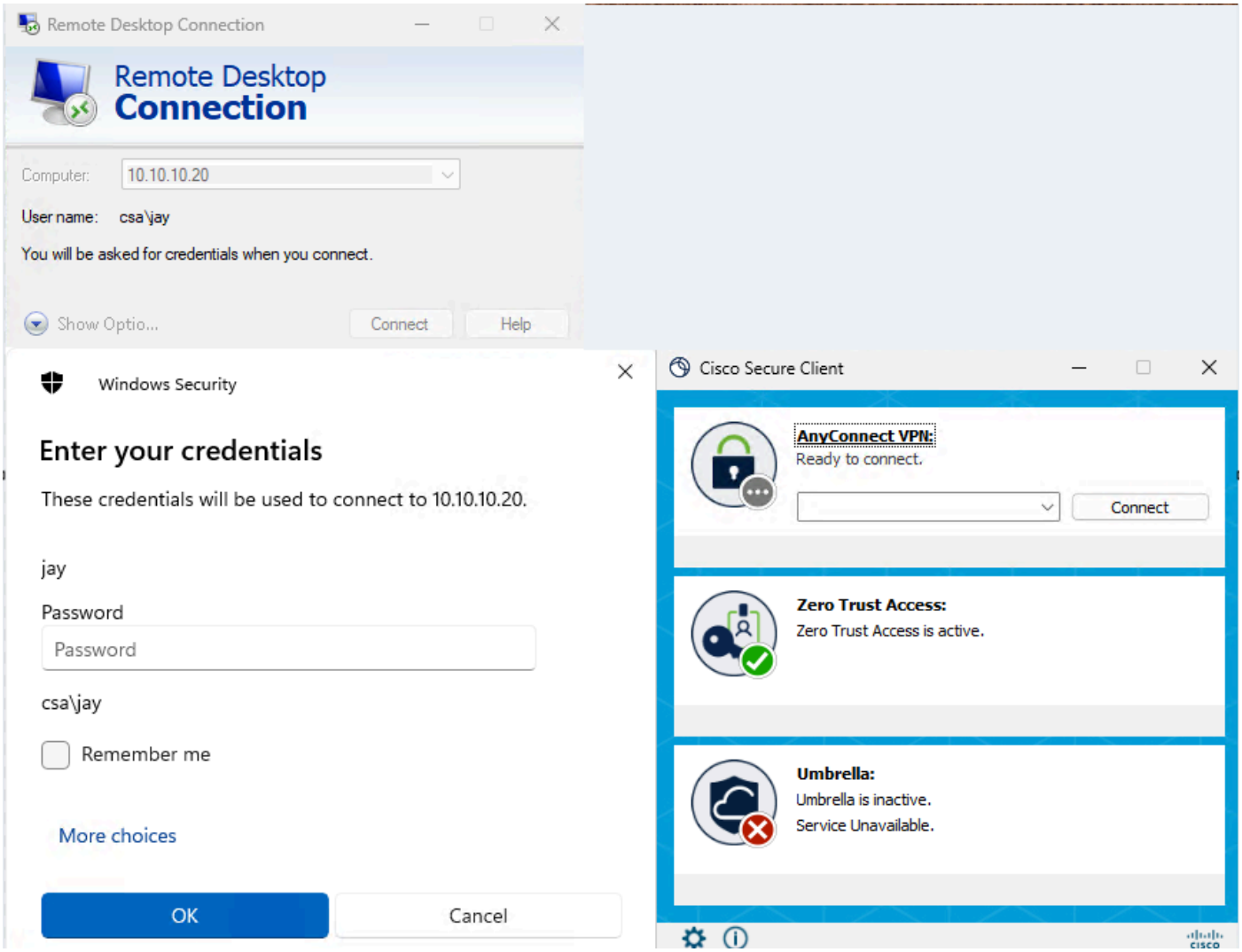
1.訪問專用資源

使用FQDN訪問PR



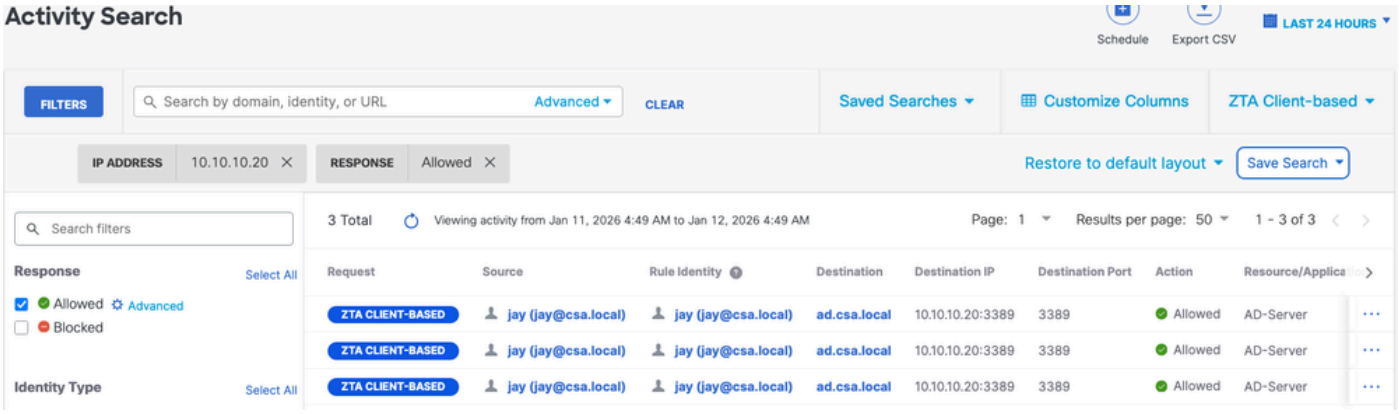
安全訪問 — PR測試

使用IP地址訪問PR

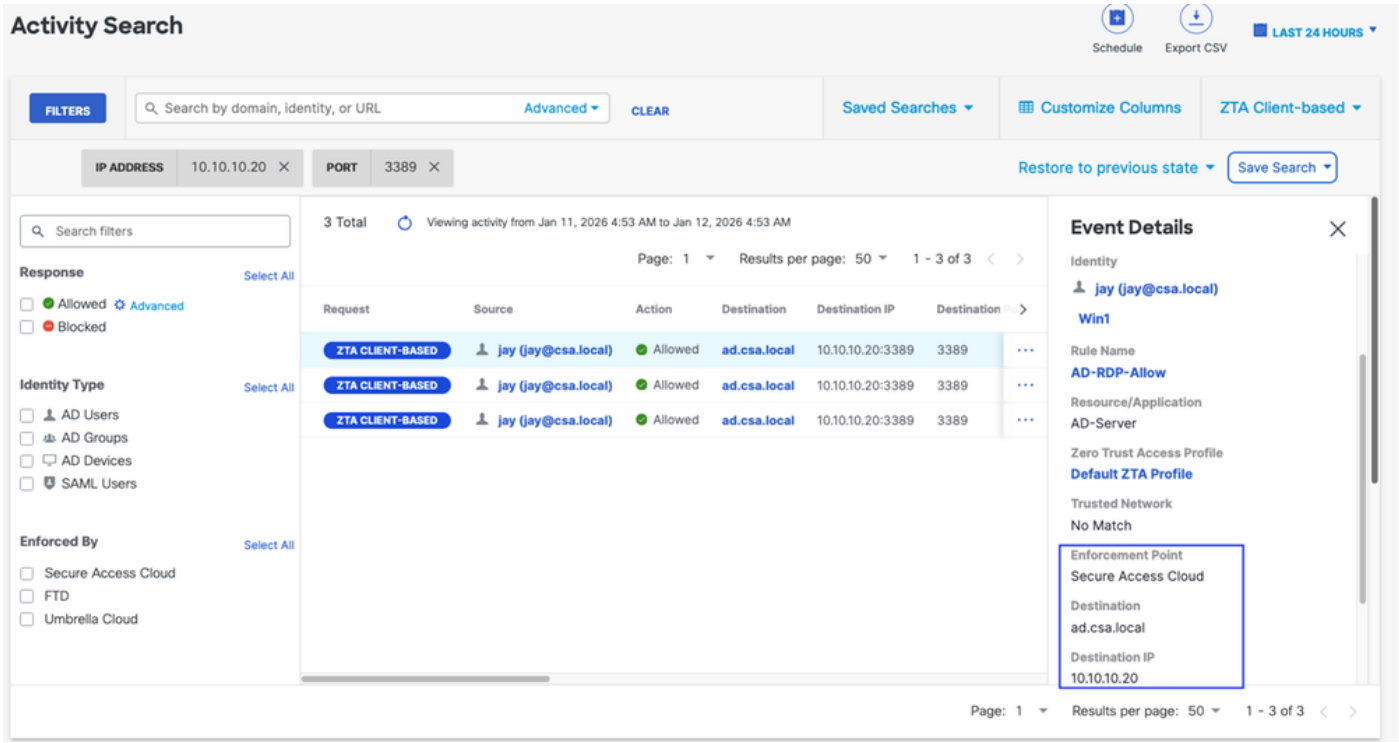


安全訪問 — PR測試

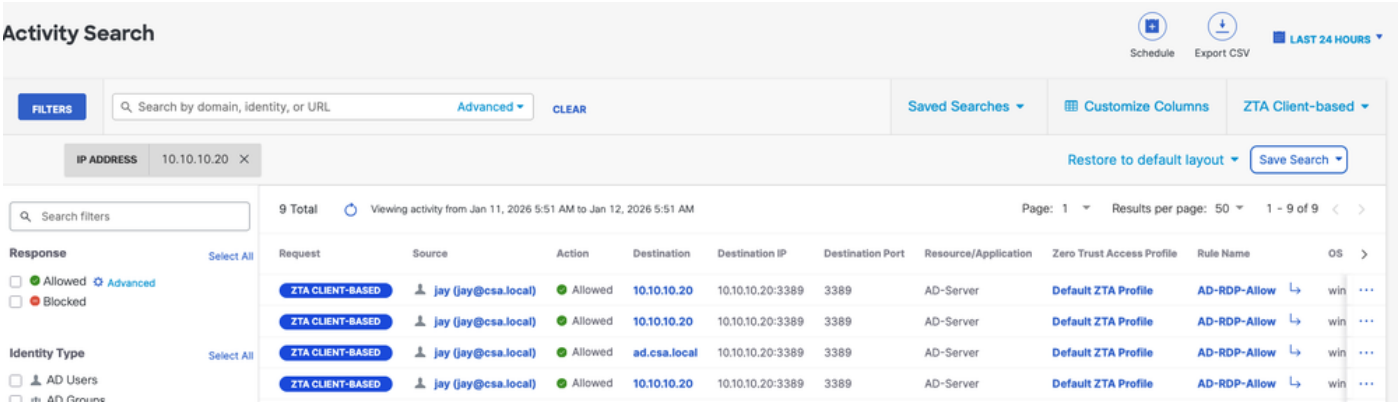
2.使用活動搜尋事件進行驗證



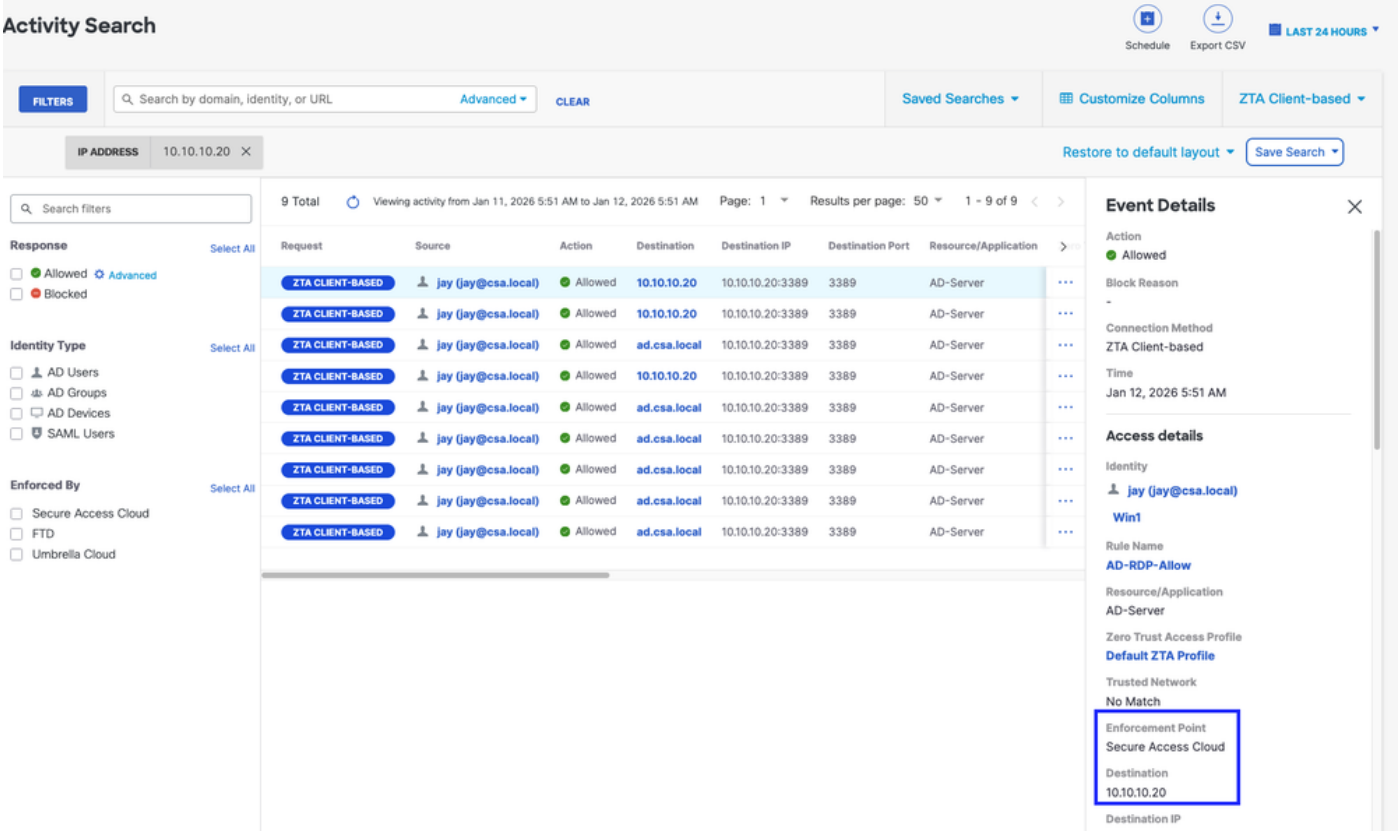
安全訪問 — 活動搜尋



安全訪問 — 活動搜尋

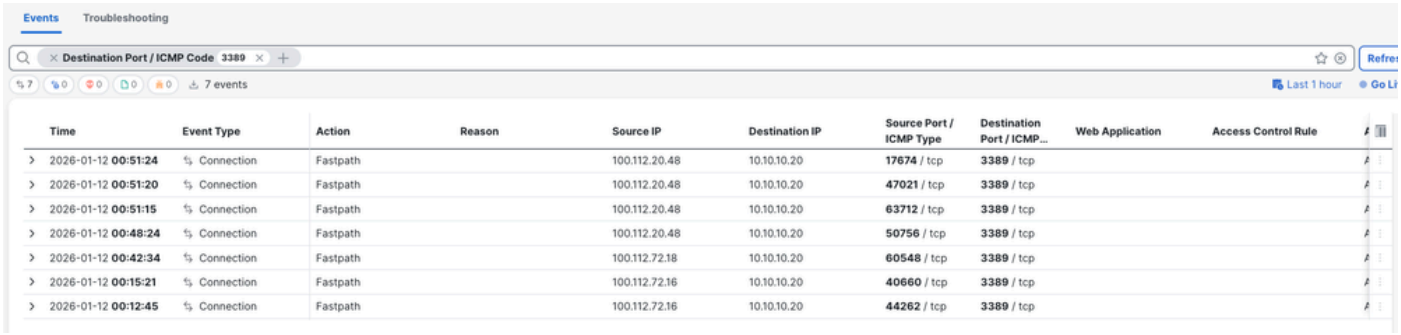


安全訪問 — 活動搜尋



安全訪問 — 活動搜尋

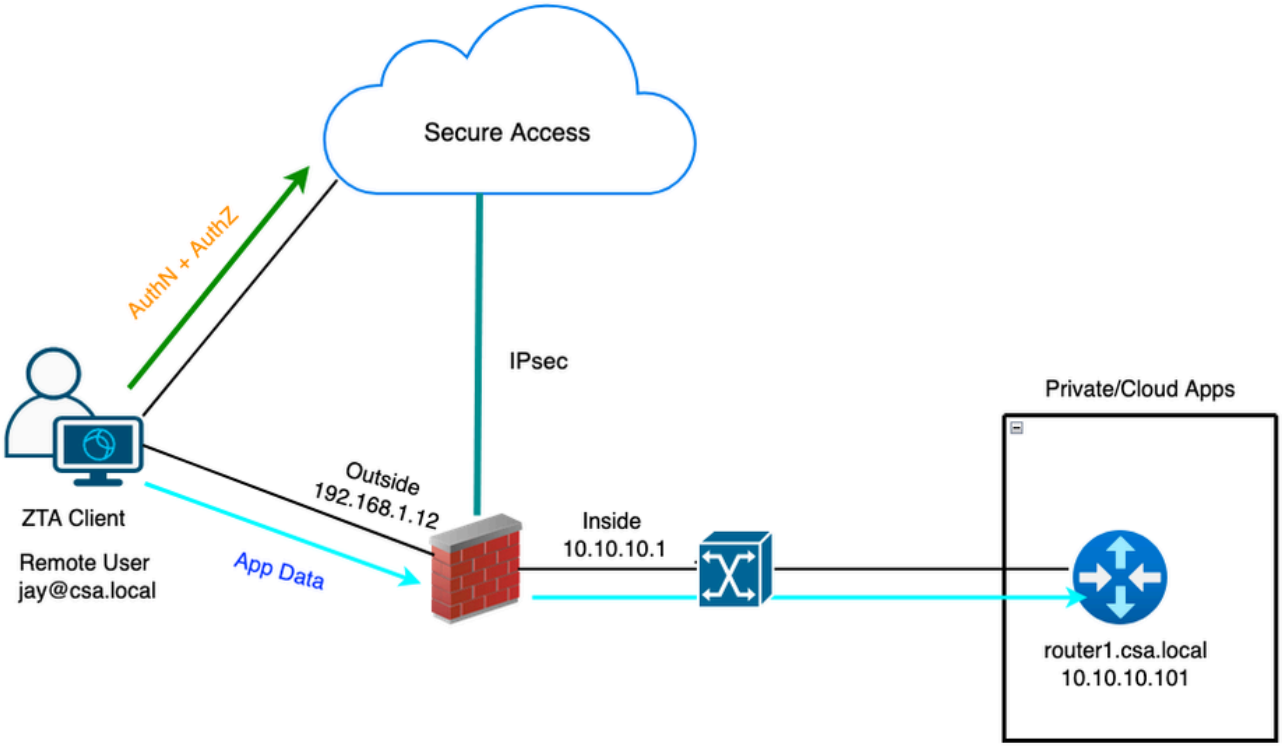
3.驗證FMC連線事件



FMC連線事件

測試案例2 — 遠端使用者 — 本地實施

通過本地實施訪問私有資源，這種型別的實施策略評估在安全訪問上進行，但應用程式資料對FTD保持本地。例如，ZTA註冊客戶端或連線到家庭網路的使用者，並嘗試訪問FTD內部介面後面的專用資源。

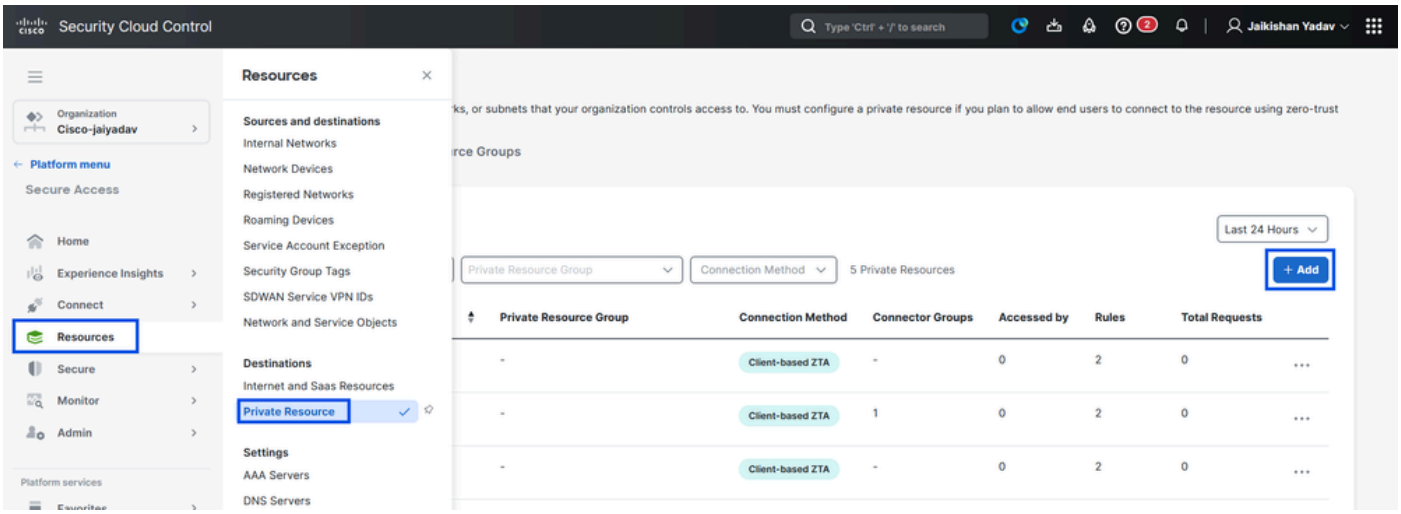


通用ZTA — 測試用例拓撲

第1步 — 在安全訪問中定義專用資源

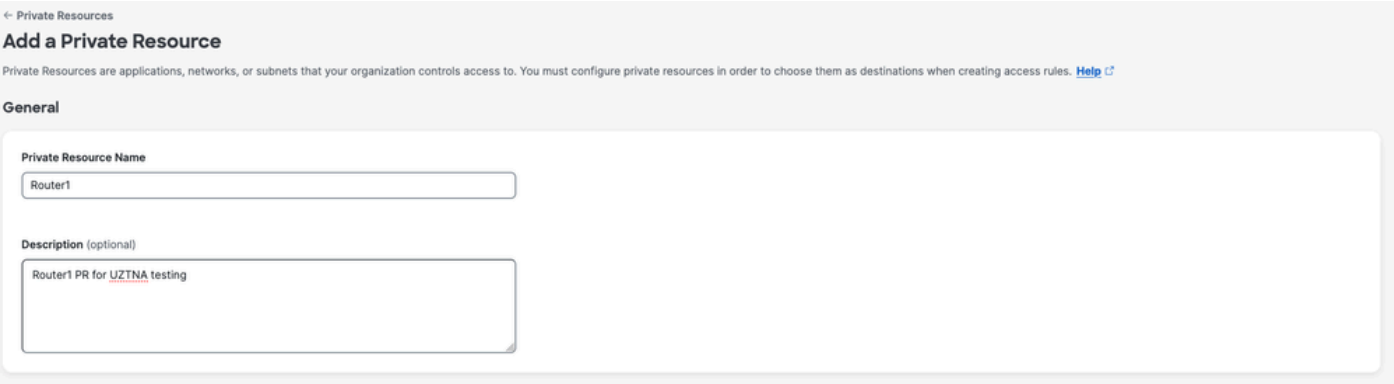
配置可通過零信任訪問(ZTA)註冊裝置訪問私有資源（具有雲實施）

1. 導覽至Resources > Destinations > Private Resources >按一下+Add



安全訪問 — 專用資源配置

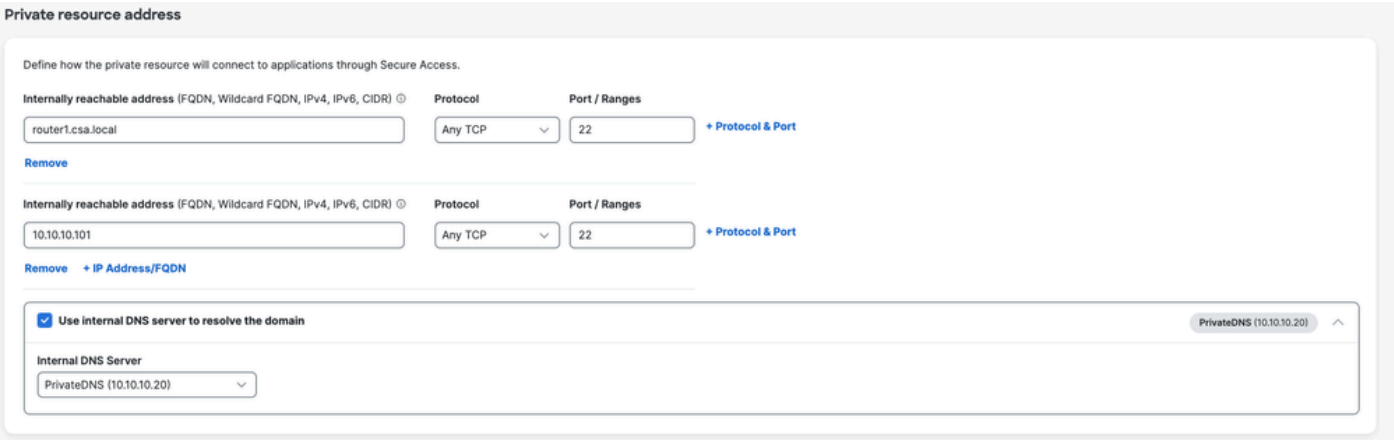
2.對於私有資源名稱，輸入資源有意義的名稱。對於Description，建議您提供諸如資源用途或資源擁有者名稱等資訊。



安全訪問 — 專用資源配置

3.輸入要訪問的專用資源的FQDN。我們還可以定義專用資源的IP地址。有關詳細資訊，請參閱新增專用資源

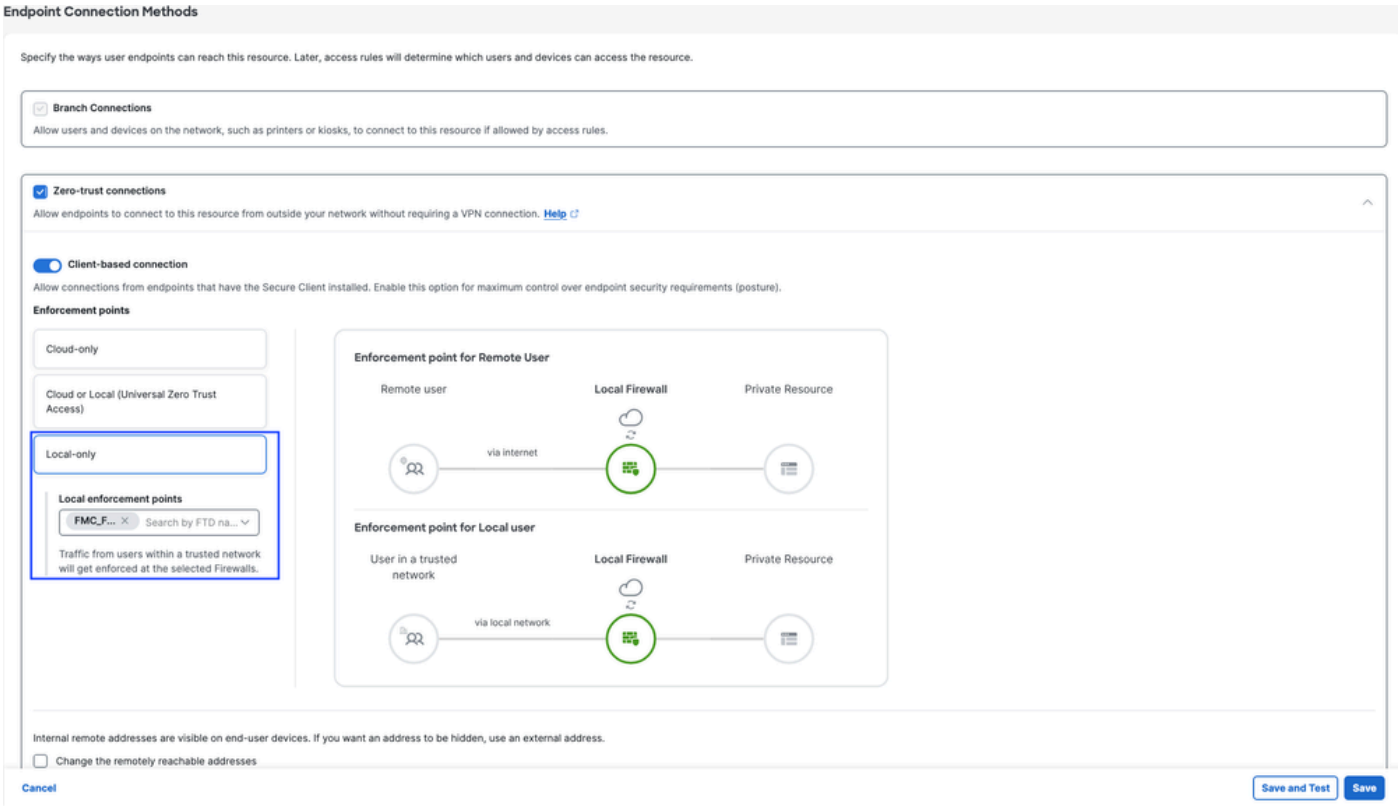
4.選擇內部DNS伺服器以解析域



安全訪問 — 專用資源配置

5. 選擇端點連線方法

6.選擇FTD作為本地實施點



安全訪問 — 專用資源配置

附註：根據您選擇的註冊型別，此更改將自動將PR與FTD關聯並觸發策略部署

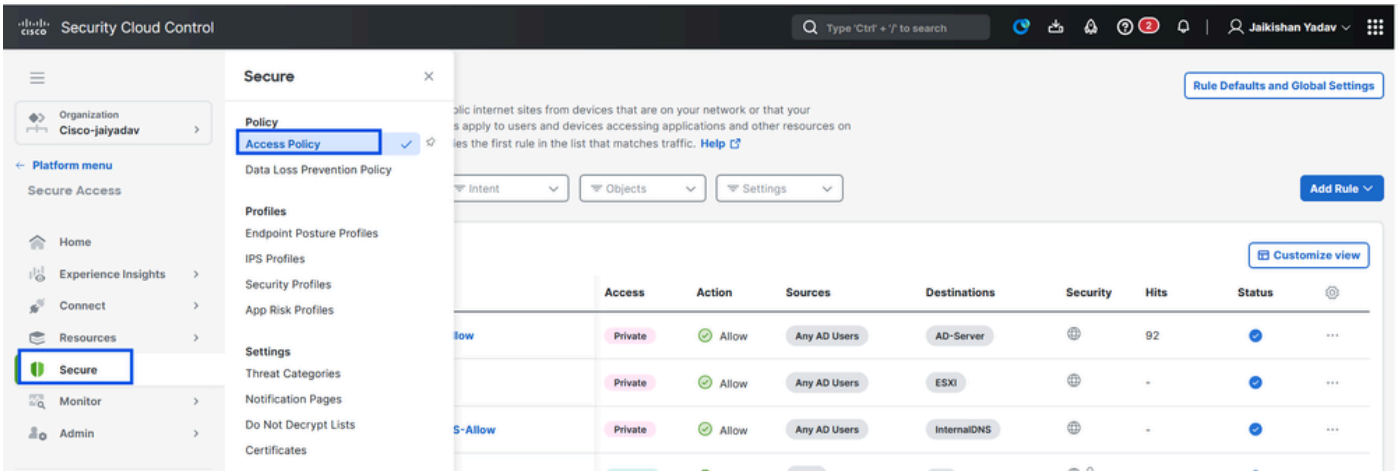
---

7. 按一下「Save」

第2步 — 建立專用訪問規則

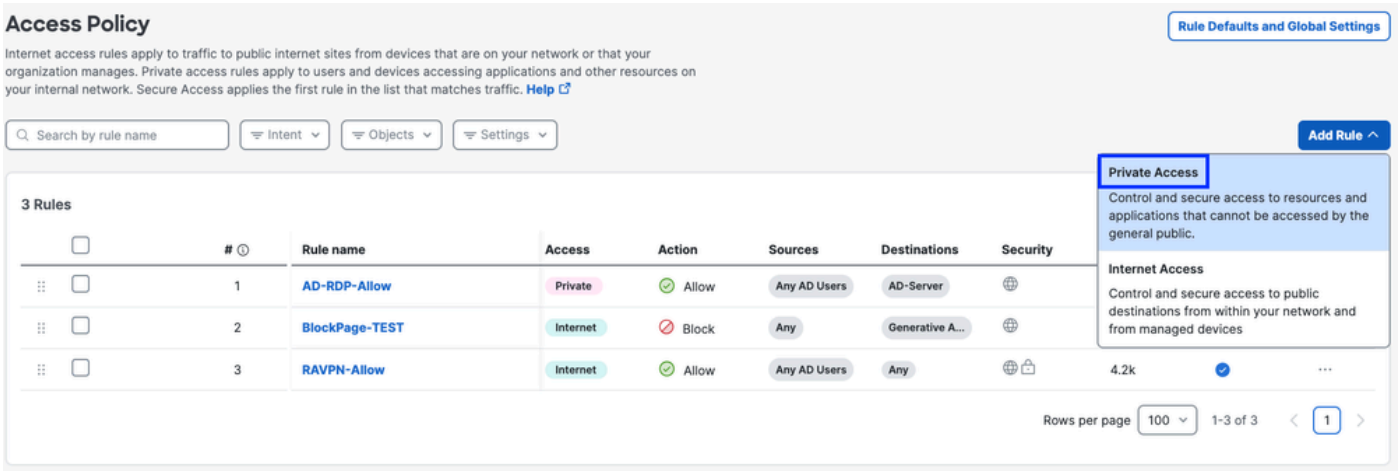
在Secure Access上配置專用訪問，以便由Universal ZTA註冊使用者訪問。有關詳細資訊，請參閱[專用訪問規則]

1. 導覽至Secure > Access Policy



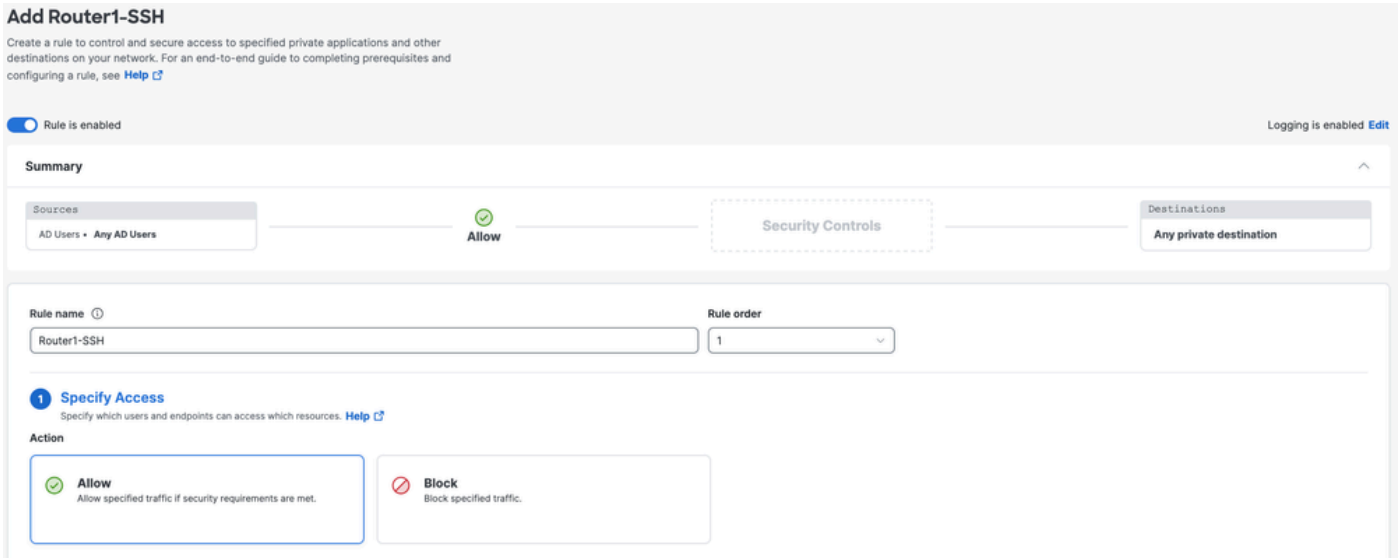
安全訪問 — 專用資源配置

2.按一下Add Rule，然後選擇Private Access。
規則頂部是描述規則的已配置元件的摘要。



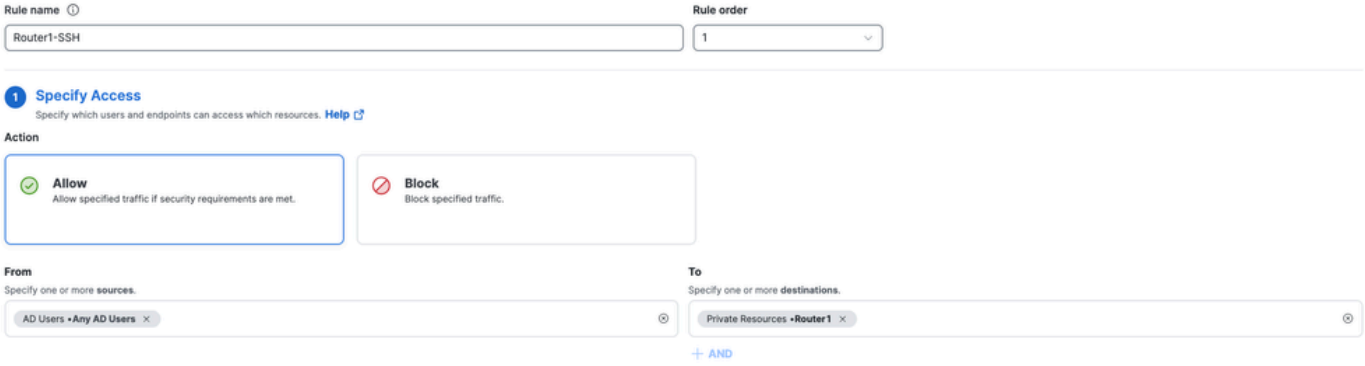
安全訪問 — 訪問策略配置

3.新增規則名稱



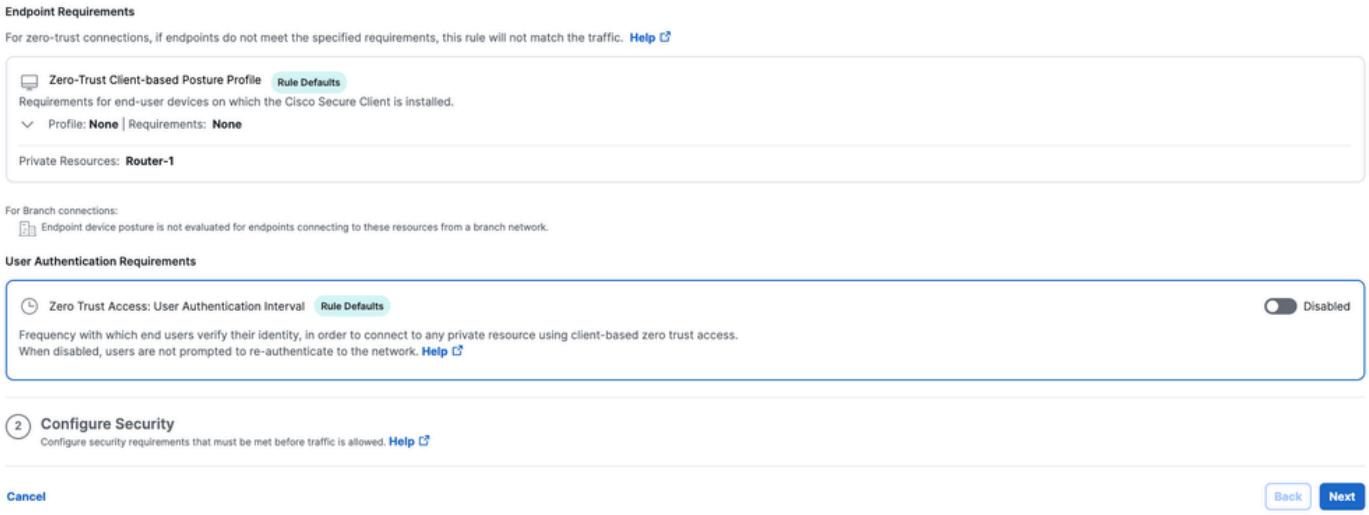
安全訪問 — 訪問策略配置

4.選擇規則操作，然後選擇來源和目標



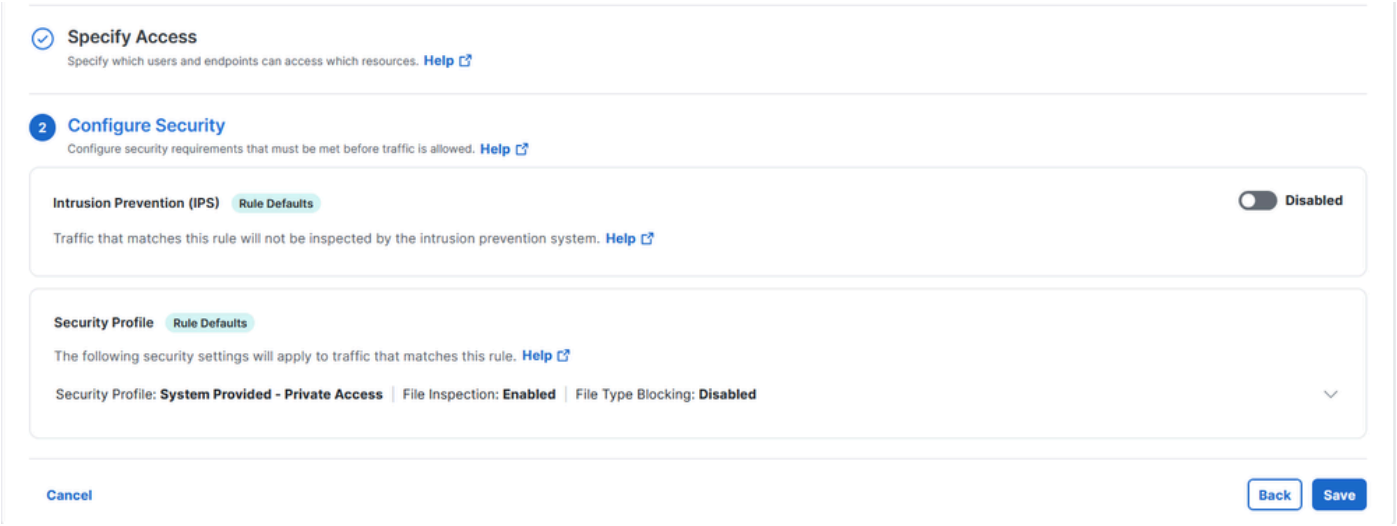
安全訪問 — 訪問策略配置

5.配置終端要求



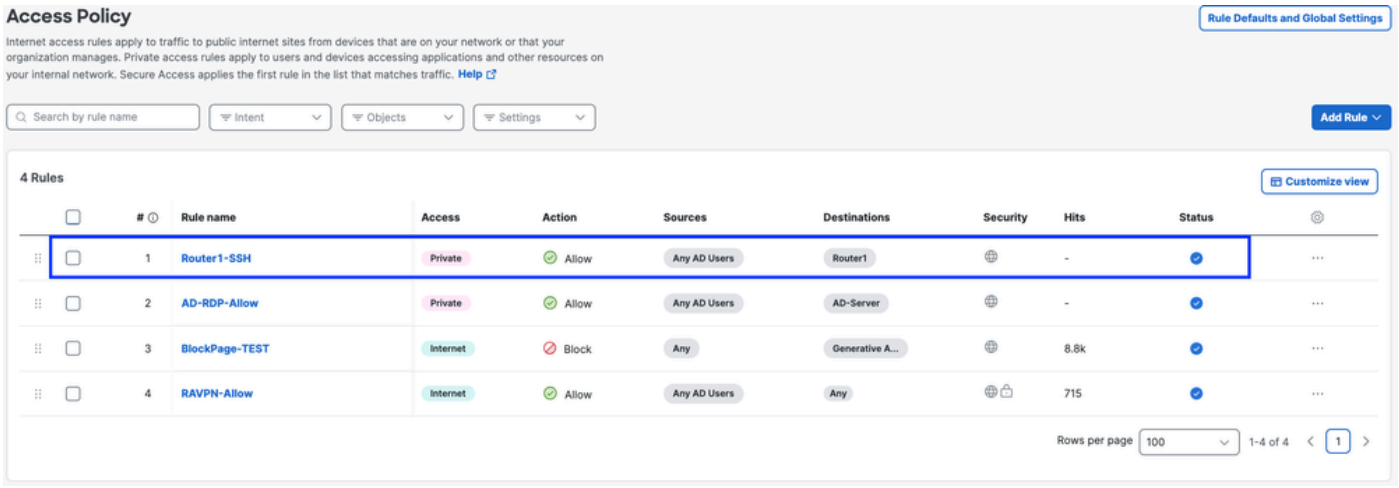
安全訪問 — 訪問策略配置

6. 配置安全性



安全訪問 — 訪問策略配置

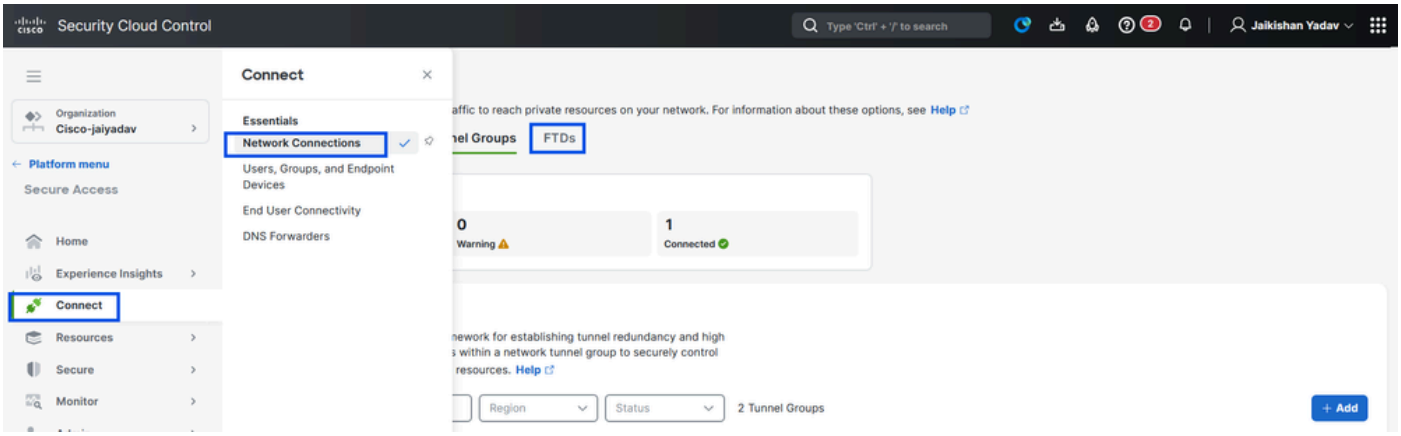
7.按一下Save



安全訪問 — 訪問策略配置

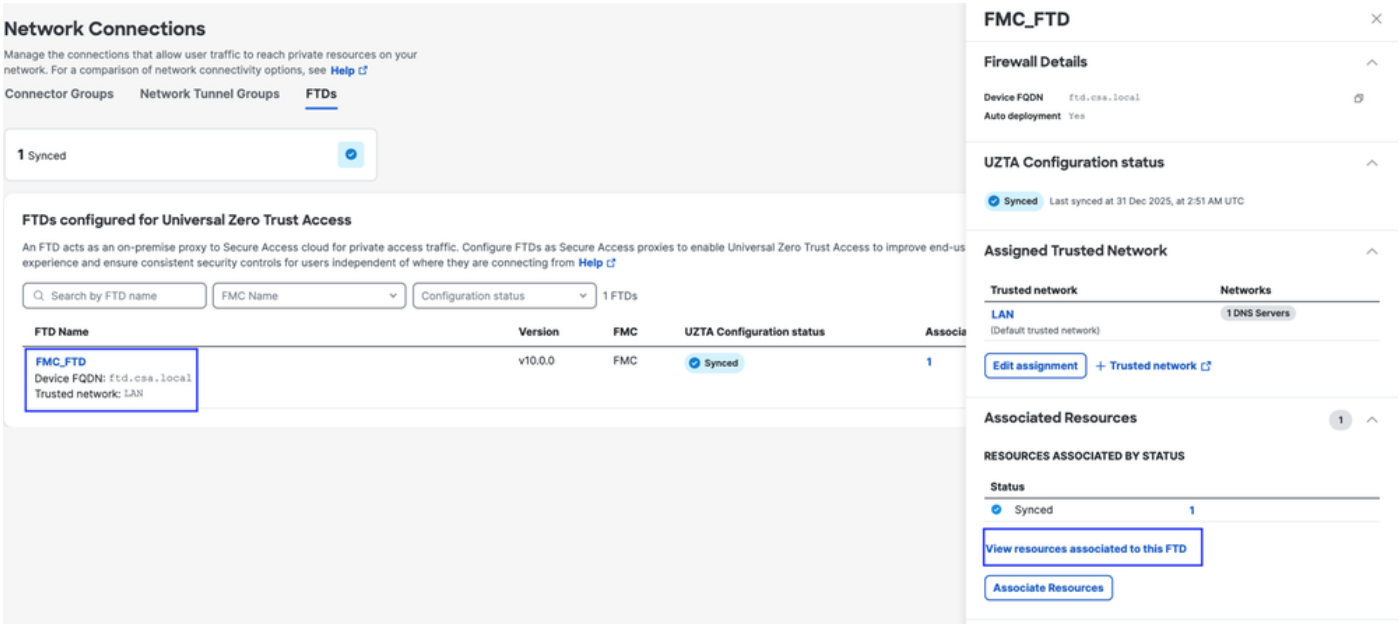
步驟3 — 驗證FTD上PR的關聯

1.導覽至Connect > Network Connections > FTD

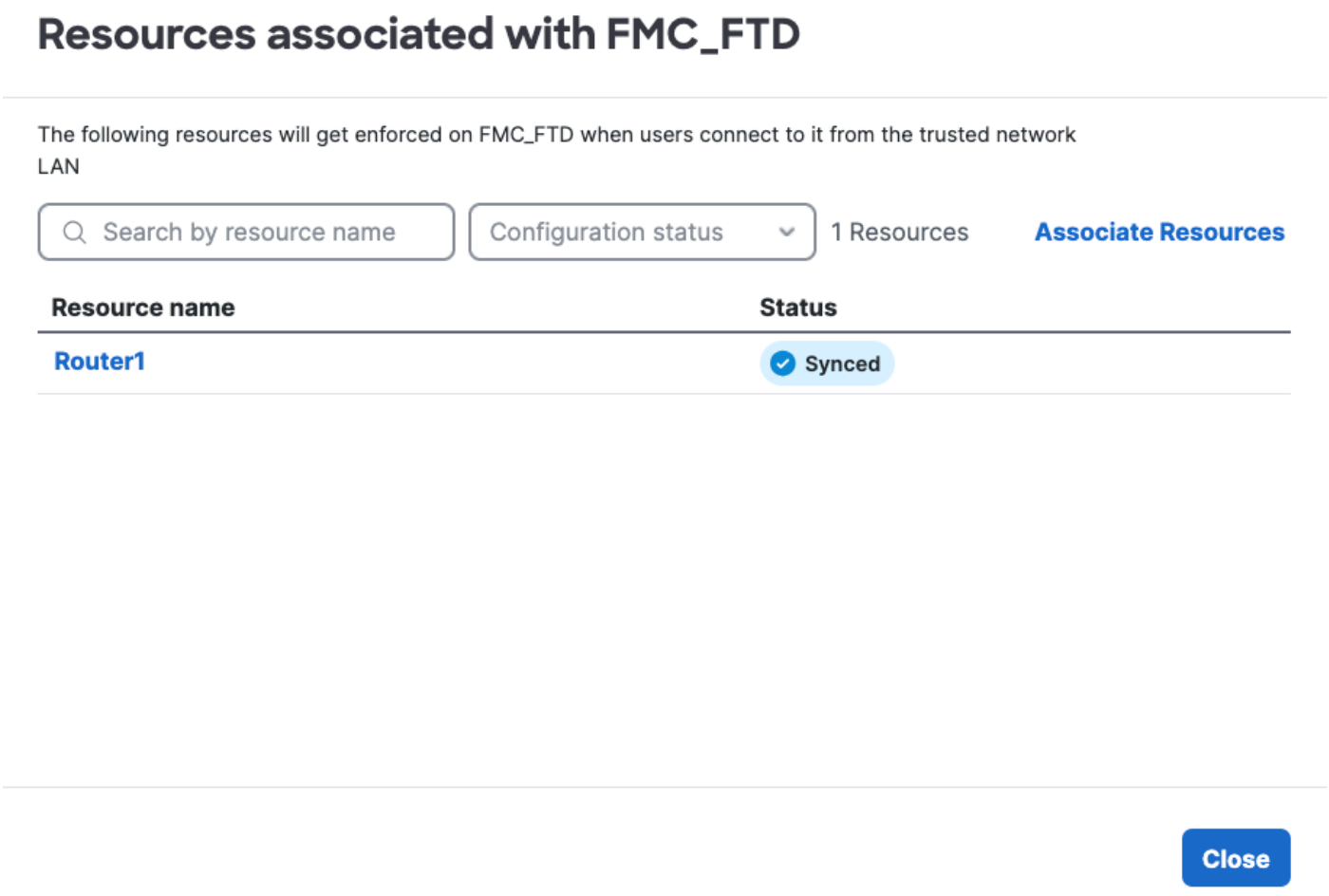


安全訪問 — PR驗證

2. 按一下FTD >檢視與此FTD相關聯的資源



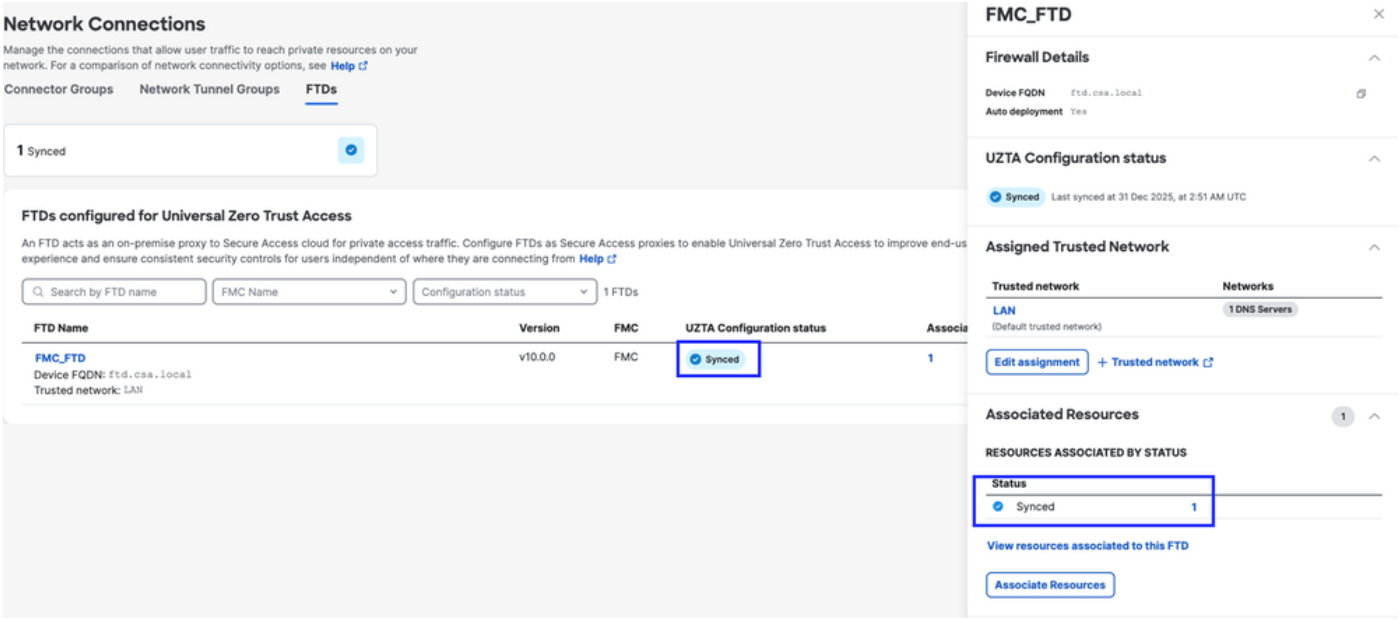
安全訪問 — PR驗證



安全訪問 — PR驗證

3. 按一下「close」

4.驗證狀態、關聯的資源和配置是否應該處於「已同步」狀態



安全訪問 — PR驗證

5.驗證組態是否已推送到FTD

登入FTD CLI並導覽至LINA模式

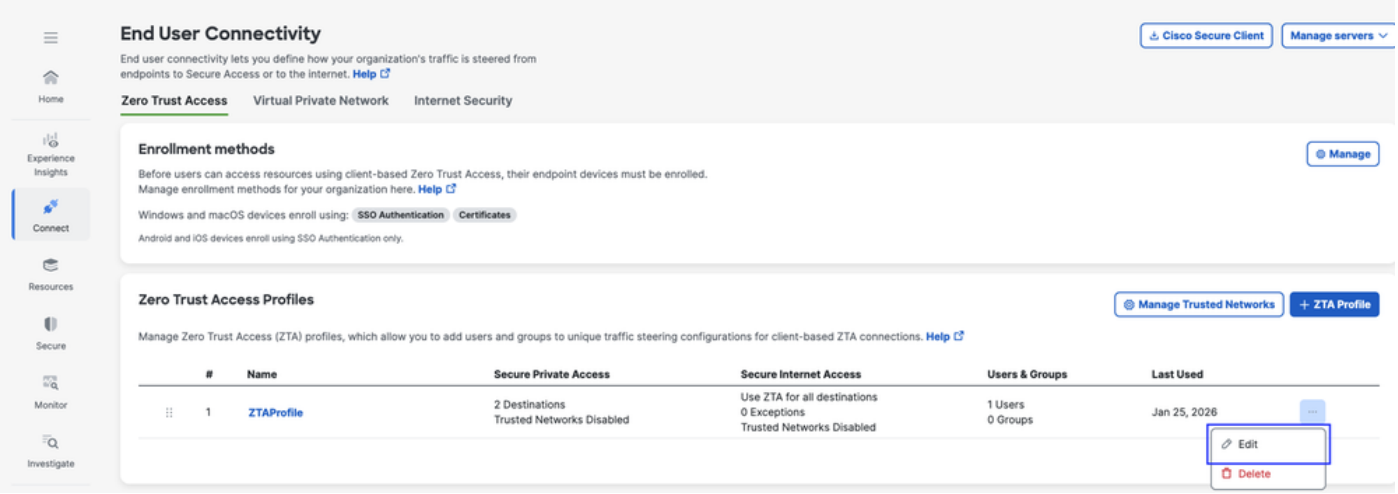
show running-config object application

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

FTD - PR驗證

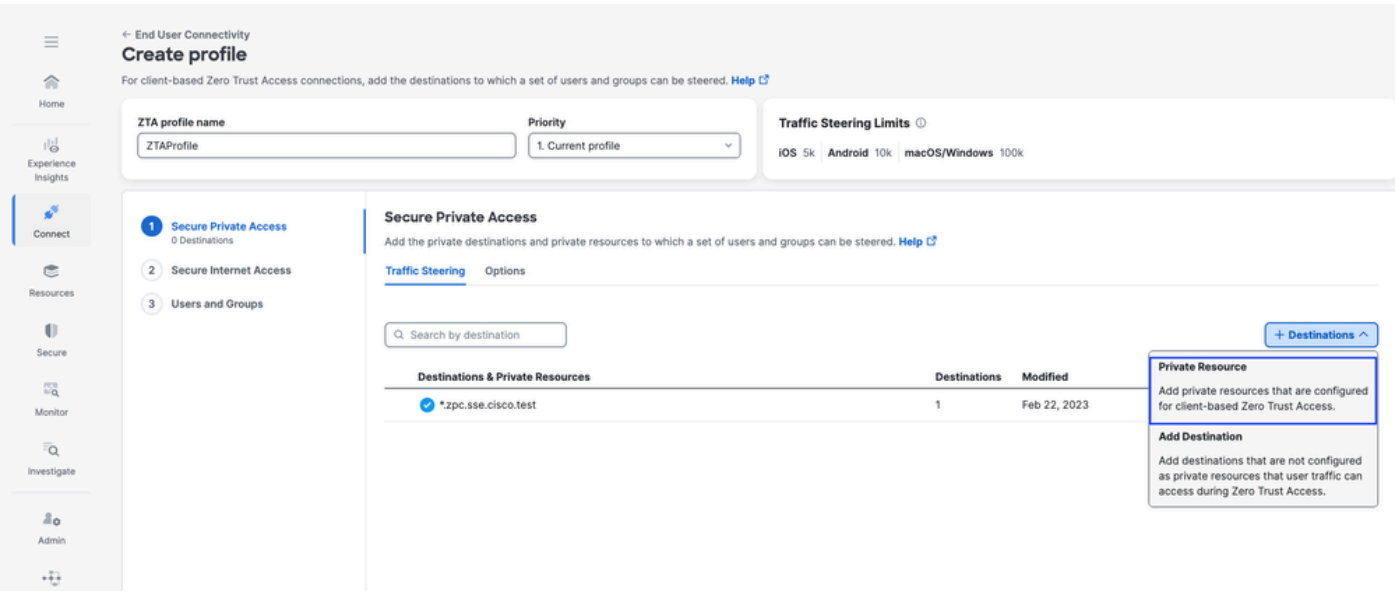
第4步向ZTA配置檔案中新增專用資源

1.導航至Connect > End User Connectivity > Zero Trust Access，然後按一下3個點以編輯ZTA配置檔案

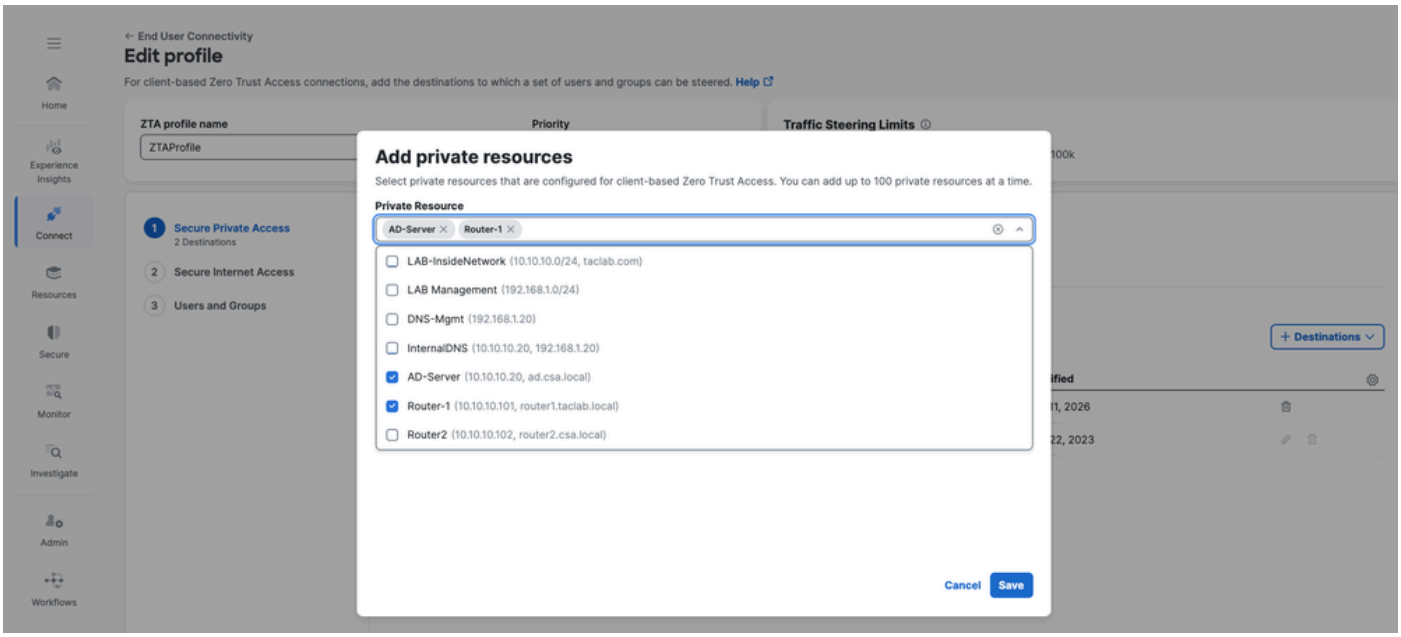


安全訪問 — ZTA配置檔案

2.新增專用資源

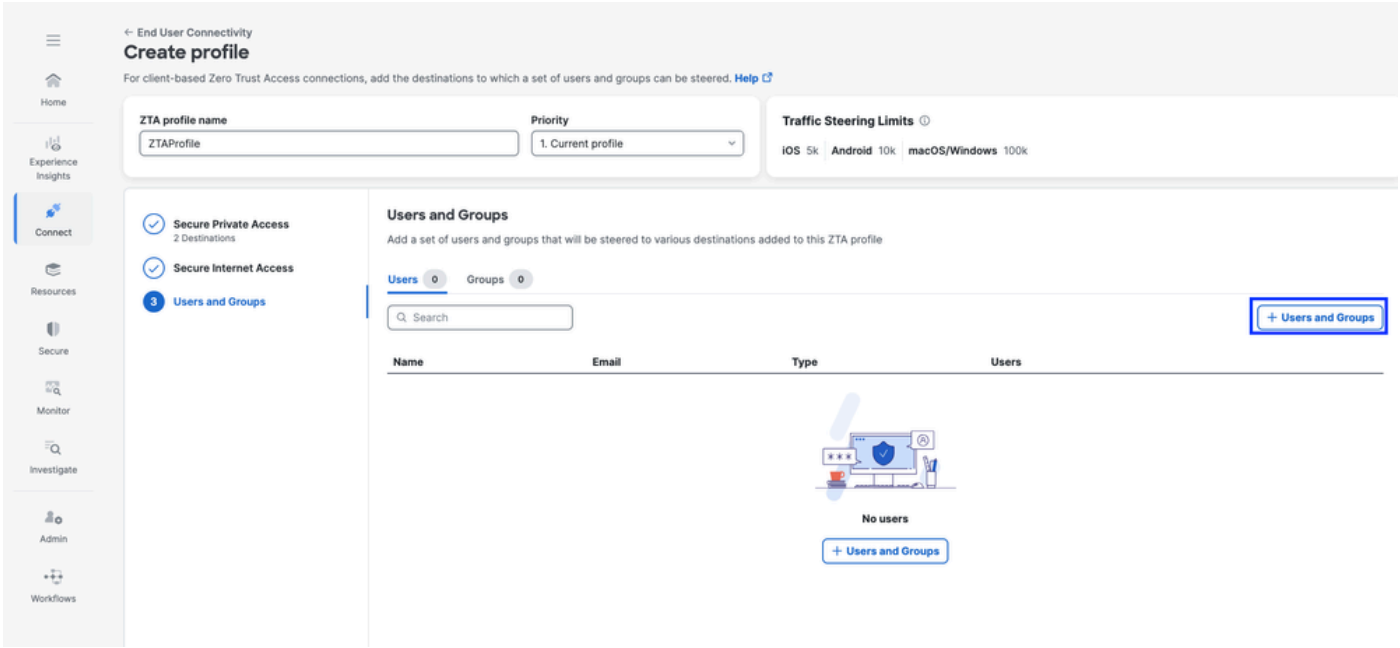


安全訪問 — ZTA配置檔案

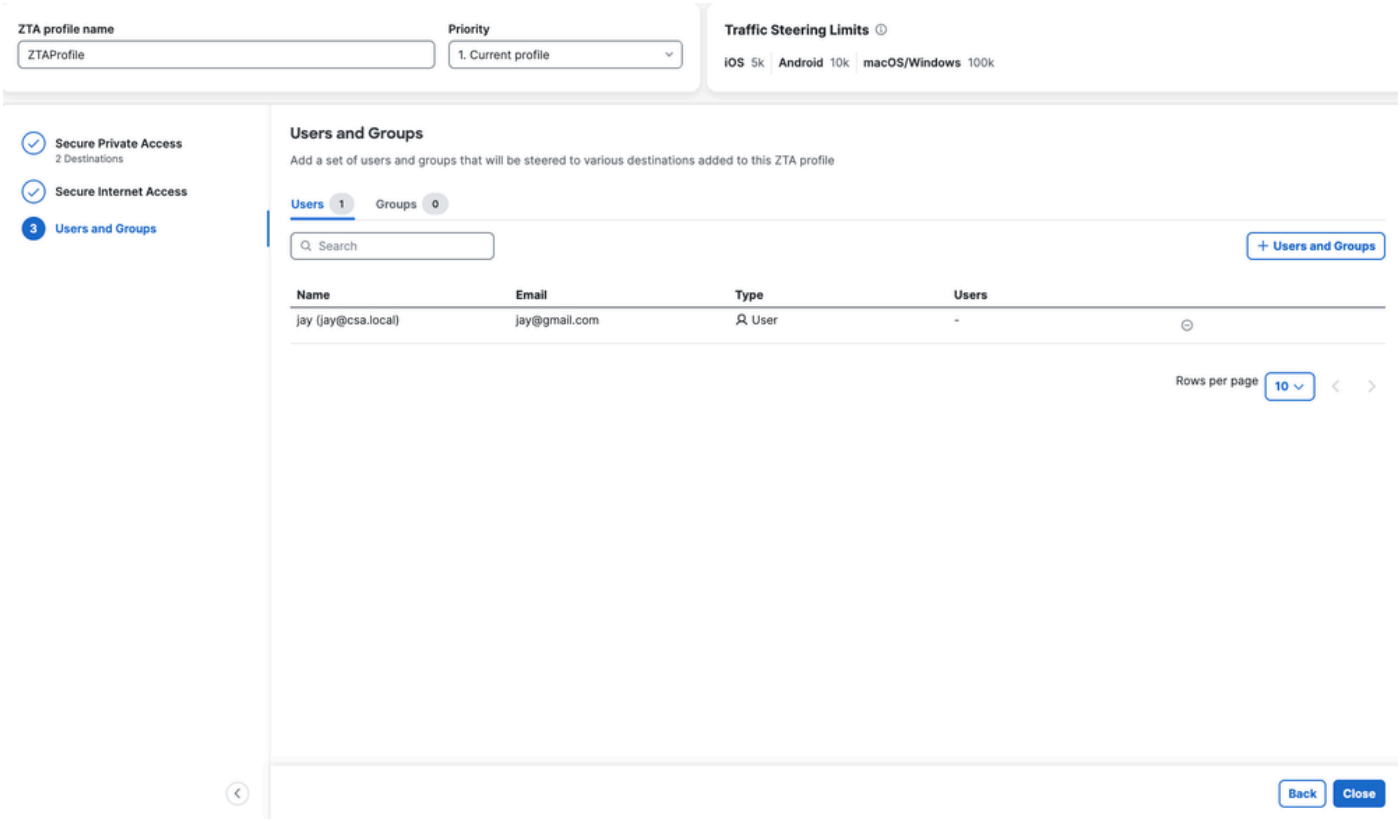


安全訪問 — ZTA配置檔案

3.新增使用者和組



安全訪問 — ZTA配置檔案



安全訪問 — ZTA配置檔案

步驟 — 5驗證對專用資源的訪問

1. 驗證遠端使用者是否可解析FTD FQDN

```
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
```

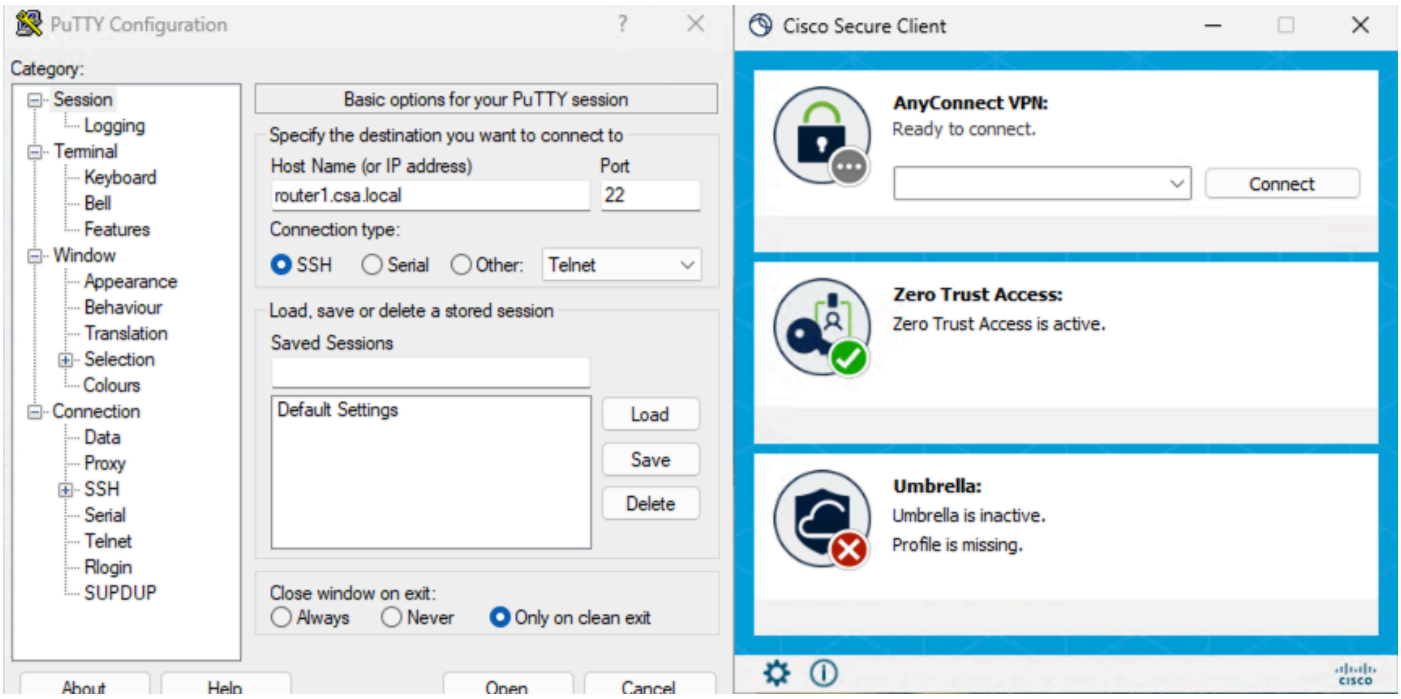
2.驗證FTD是否可以使用FQDN訪問私有資源

```
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#
```

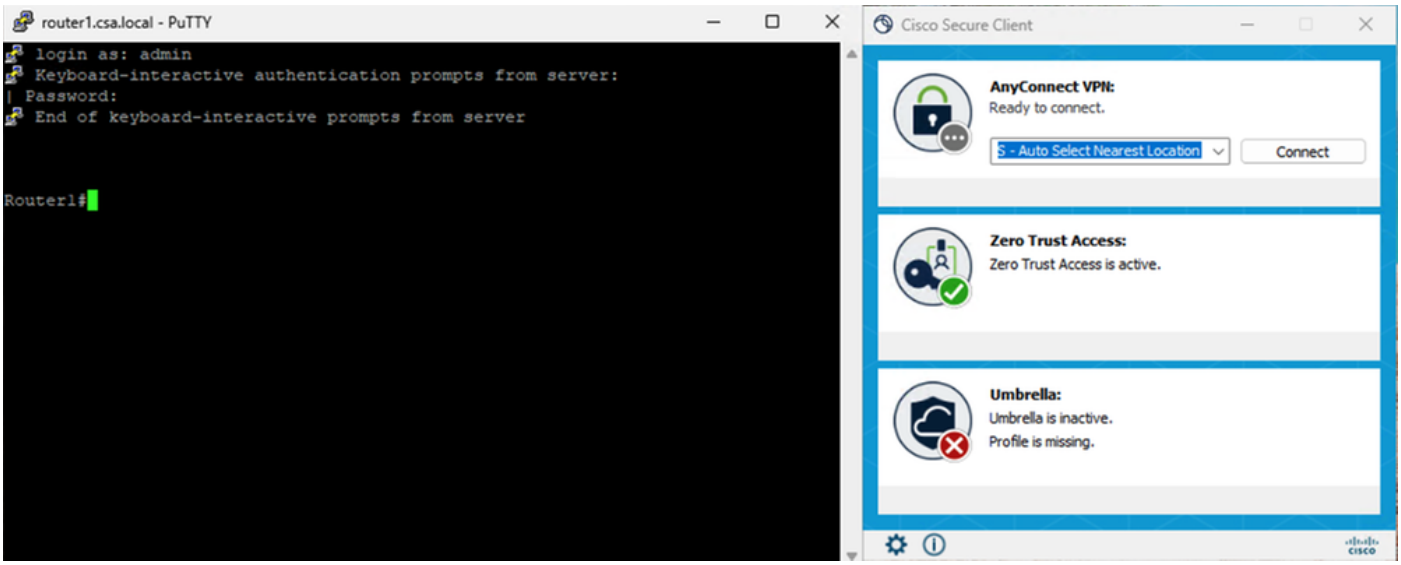
安全訪問 — PR測試

3. 測試到專用資源的SSH連線

使用FQDN訪問PR

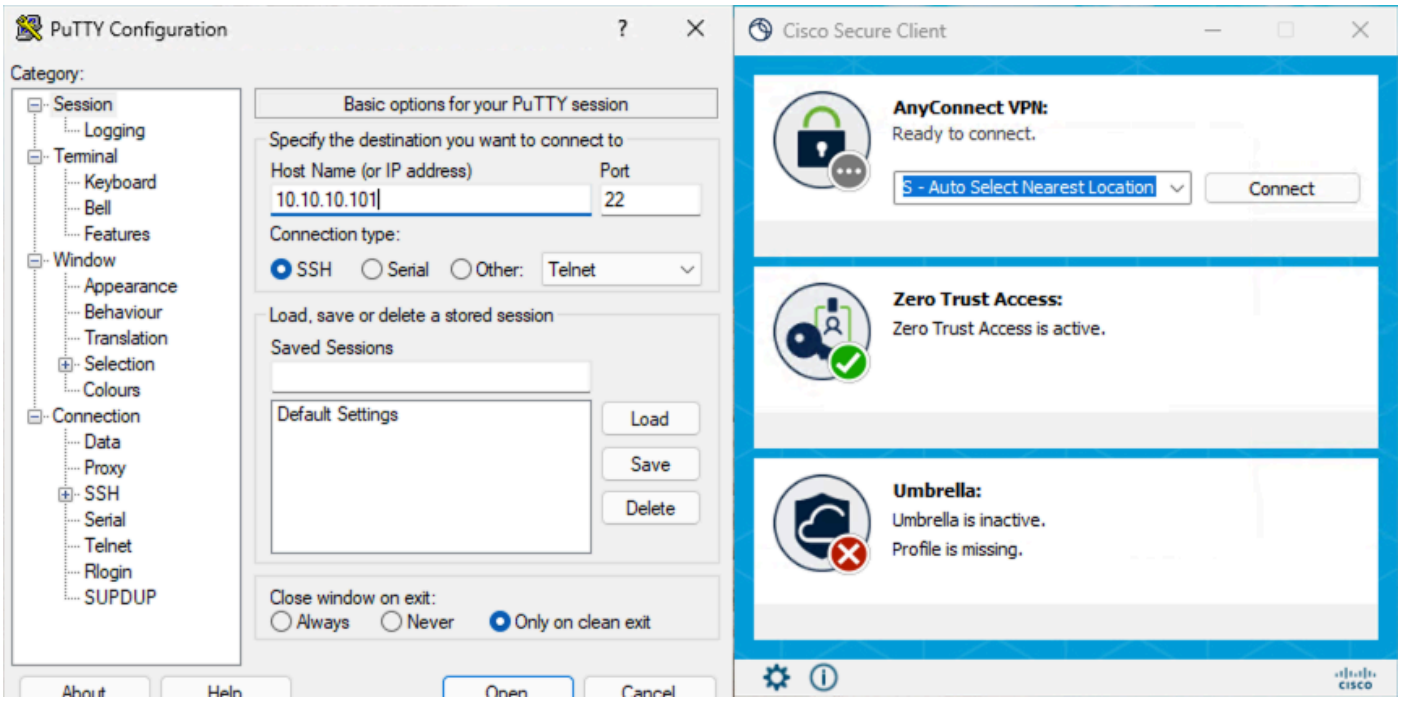


安全訪問 — PR測試

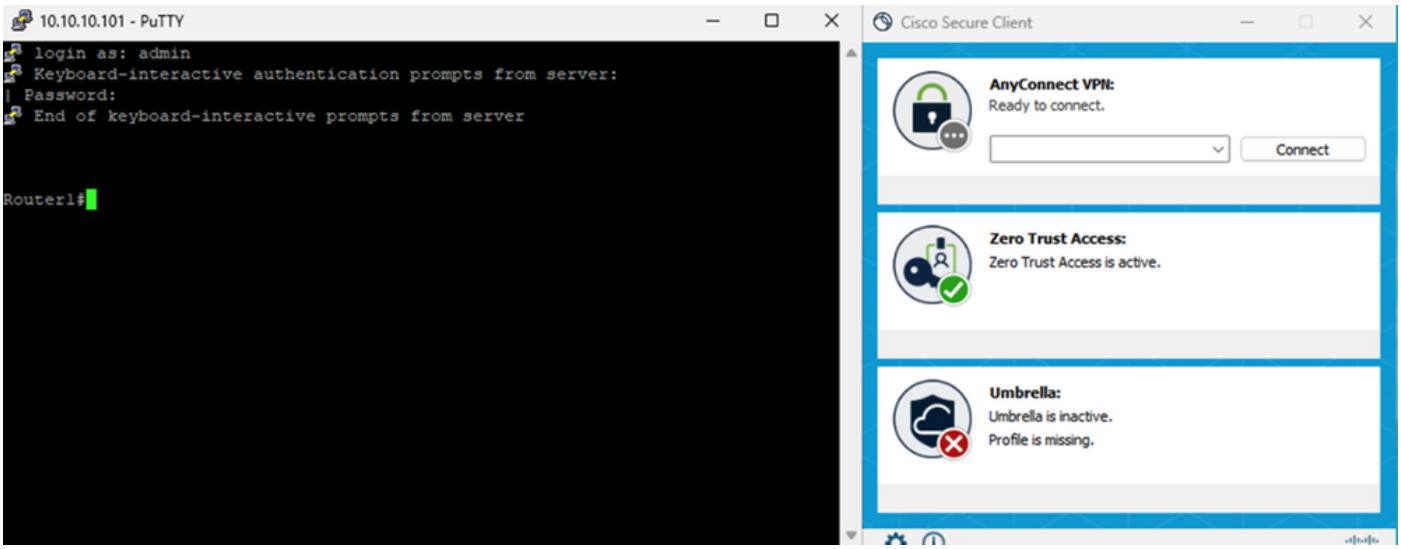


安全訪問 — PR測試

使用IP地址訪問PR

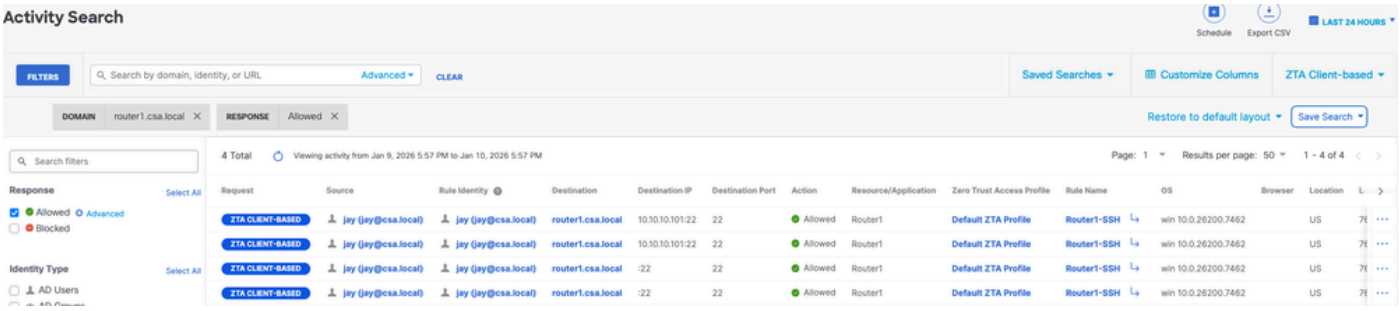


安全訪問 — PR測試

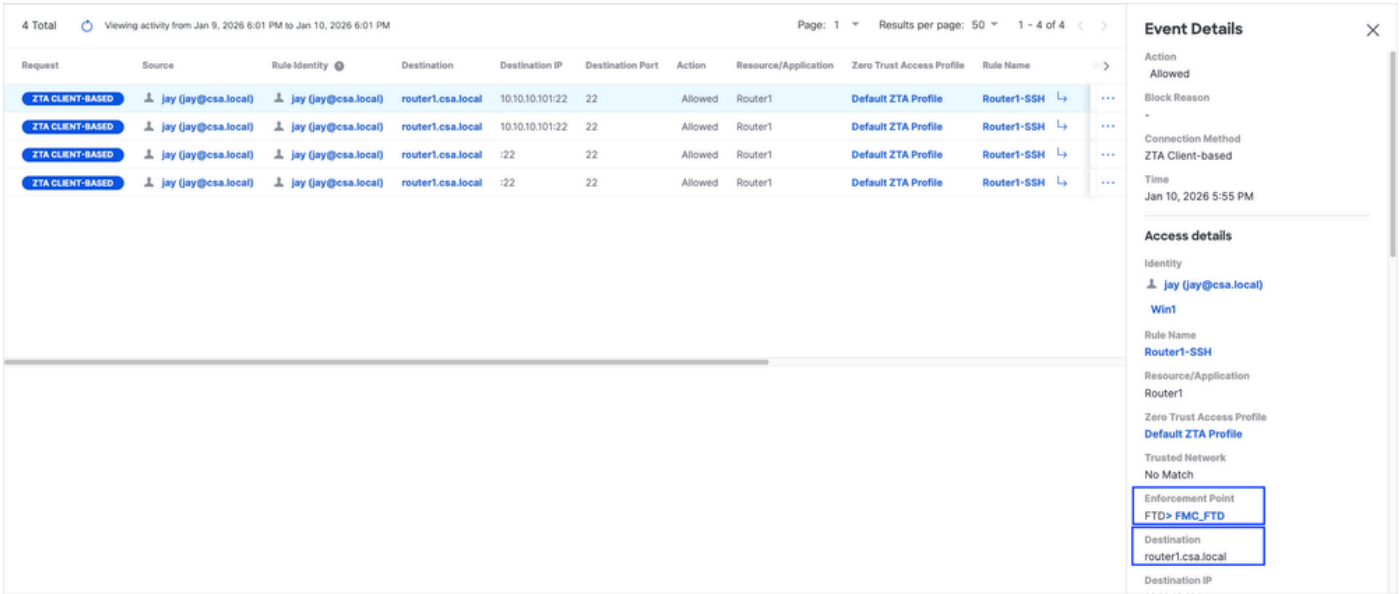


安全訪問 — PR測試

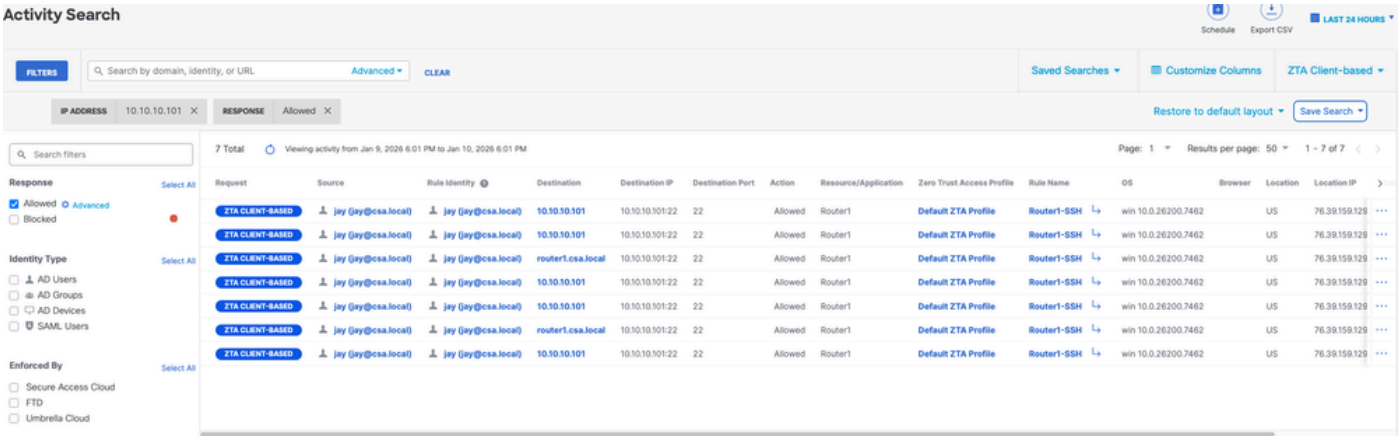
4. 驗證安全訪問活動搜尋日誌



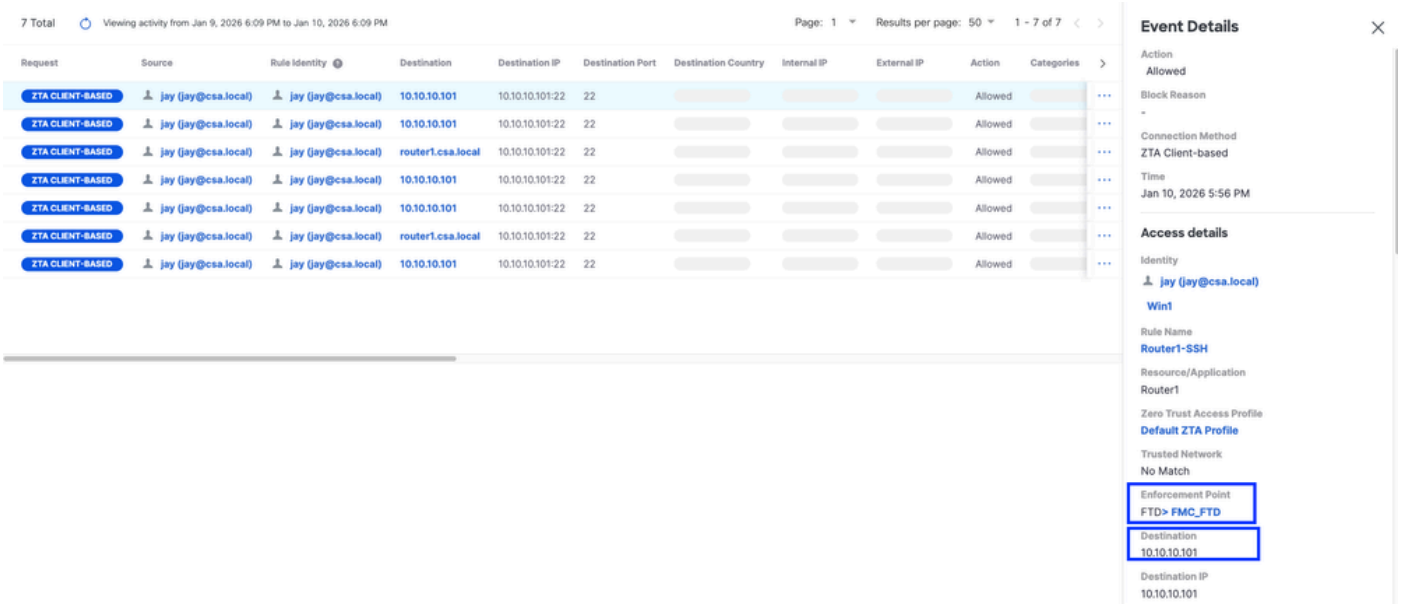
安全訪問 — 活動搜尋



安全訪問 — 活動搜尋

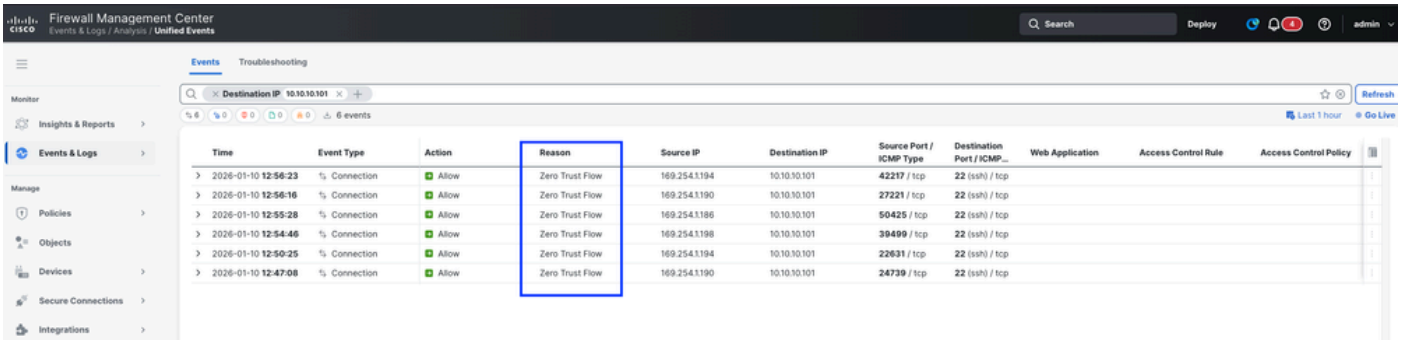


安全訪問 — 活動搜尋



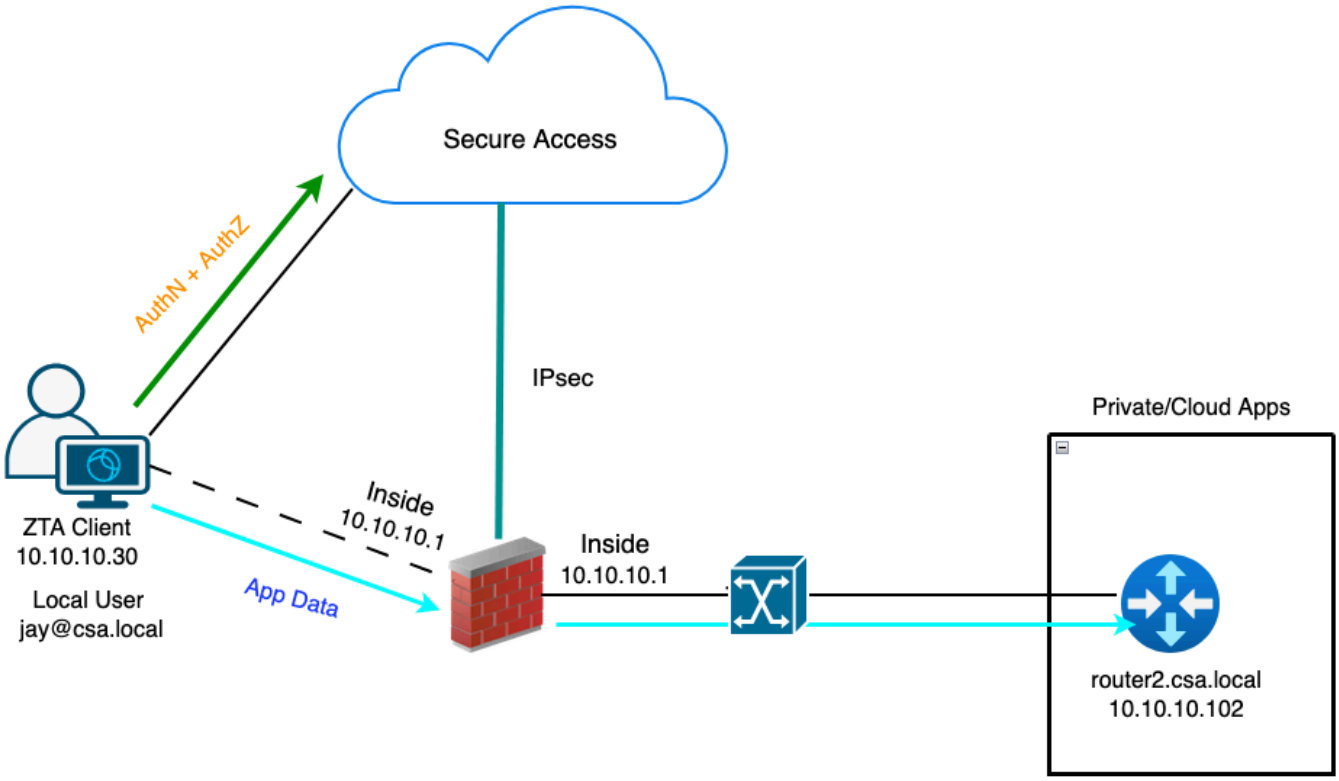
安全訪問 — 活動搜尋

5. 驗證FMC連線事件



測試案例3 — 本地使用者 — 本地實施

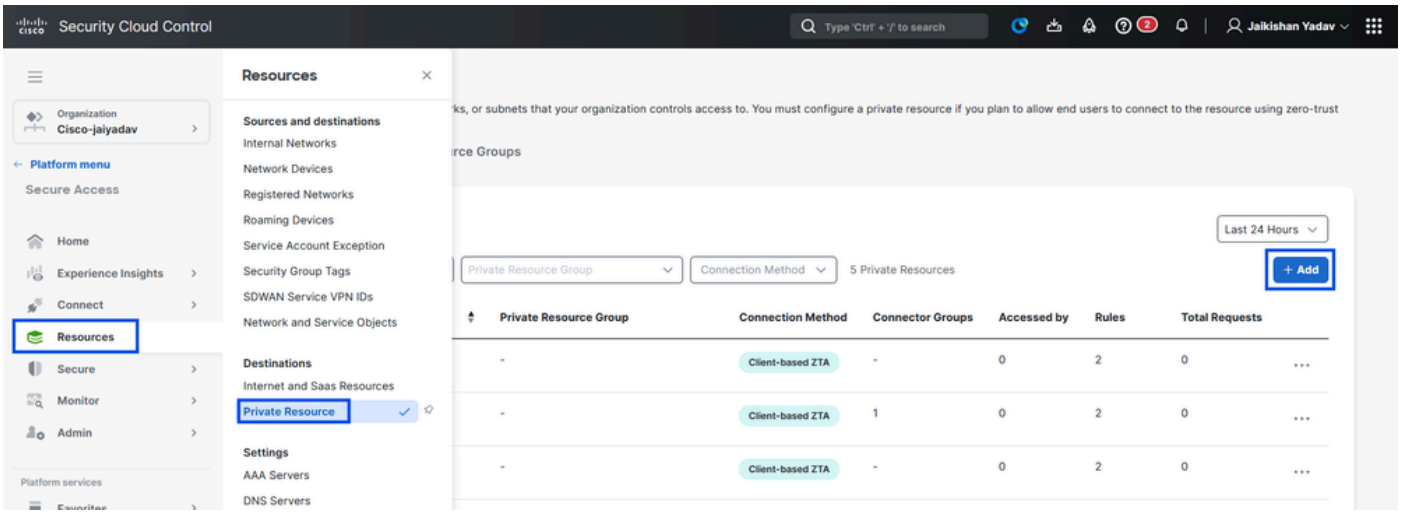
以本地使用者身份通過本地實施訪問私有資源，這種型別的實施策略評估發生在Secure Access上，但應用程式資料對FTD保持本地。例如，ZTA註冊客戶端或連線到家庭網路的使用者，並嘗試訪問FTD內部介面後面的專用資源。如果私人資源位於DMZ或FTD的任何其他介面之後，則我們將不得不在FTD上建立存取規則，以允許使用者端IP或網路與私人資源之間的流量。



第1步 — 在安全訪問中定義專用資源

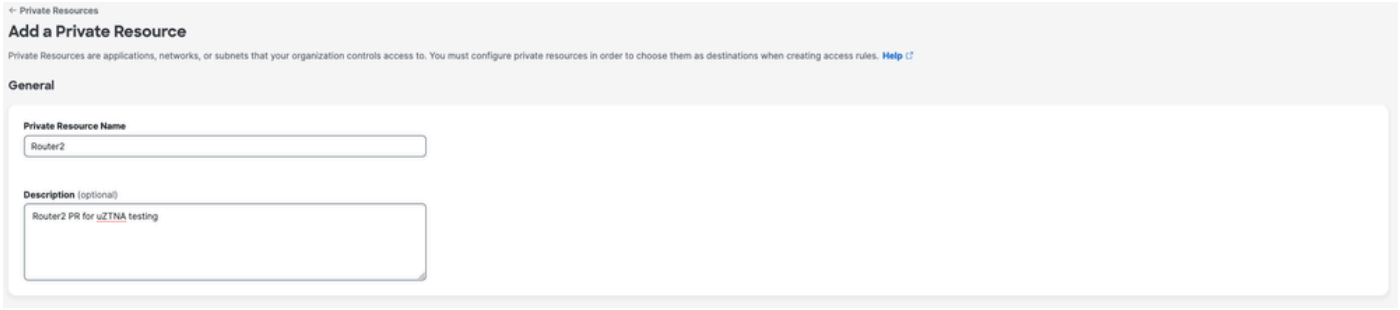
配置可通過零信任訪問(ZTA)註冊裝置訪問私有資源（具有雲實施）

1. 導覽至Resources > Destinations > Private Resources >按一下+Add



安全訪問 — 專用資源配置

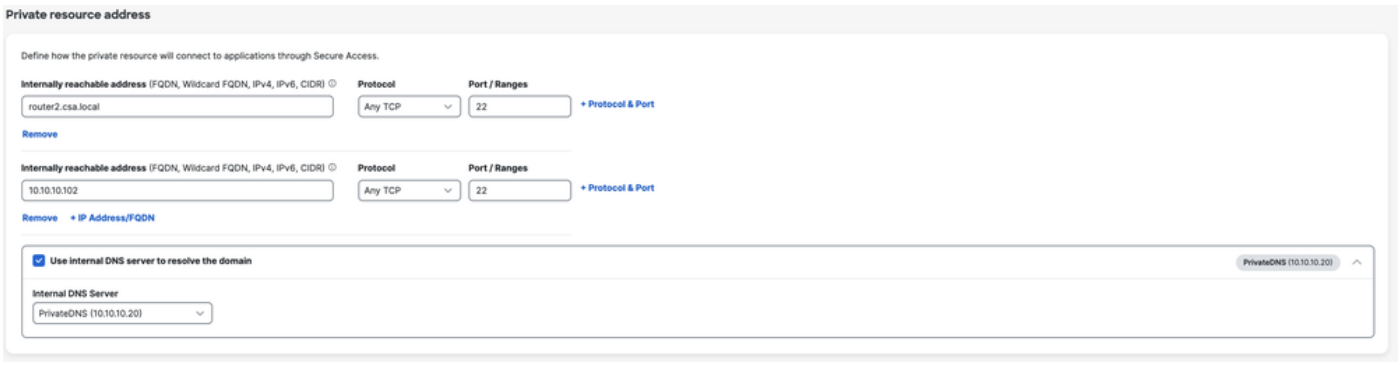
2.對於私有資源名稱，輸入資源有意義的名稱。對於Description，建議您提供諸如資源用途或資源擁有者名稱等資訊。



安全訪問 — 專用資源配置

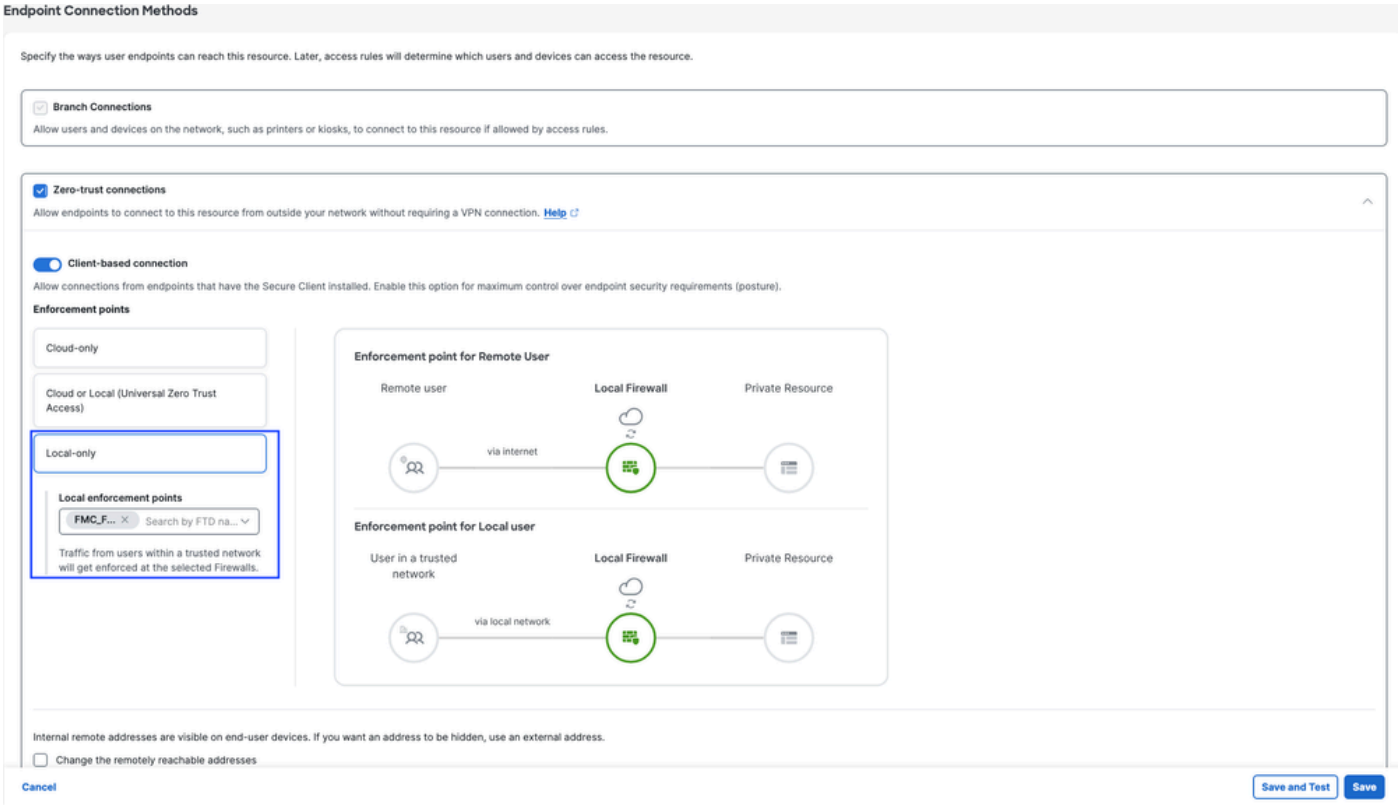
3.輸入要訪問的專用資源的FQDN。我們還可以定義專用資源的IP地址。有關詳細資訊，請參閱新增專用資源

4.選擇內部DNS伺服器以解析域



5. 選擇端點連線方法

6.選擇FTD作為本地實施點



安全訪問 — 專用資源配置

附註：根據您選擇的註冊型別，此更改將自動將PR與FTD關聯並觸發策略部署

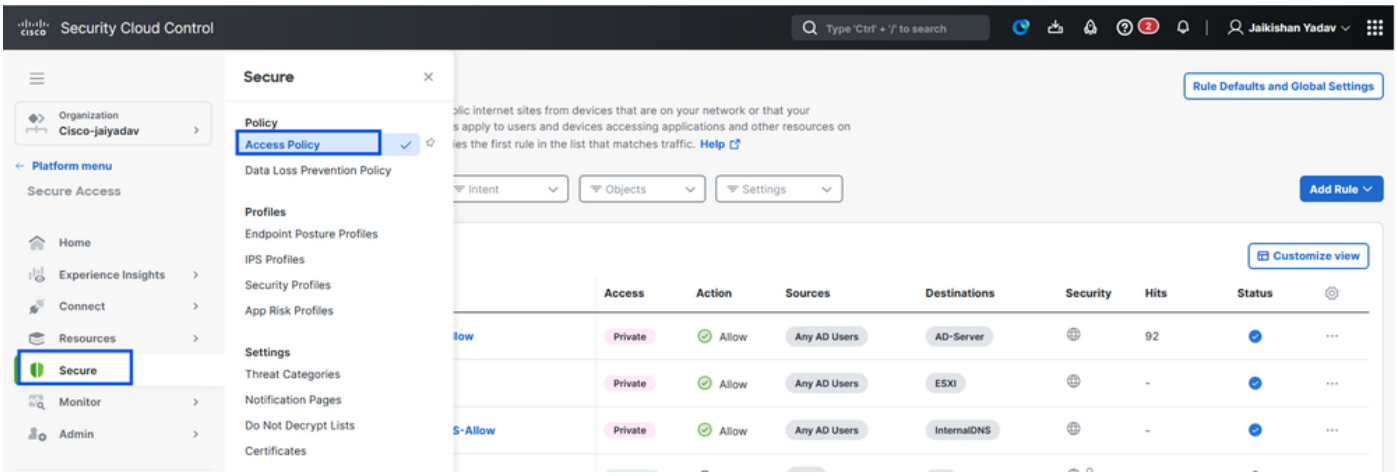
---

7. 按一下「Save」

第2步 — 建立專用訪問規則

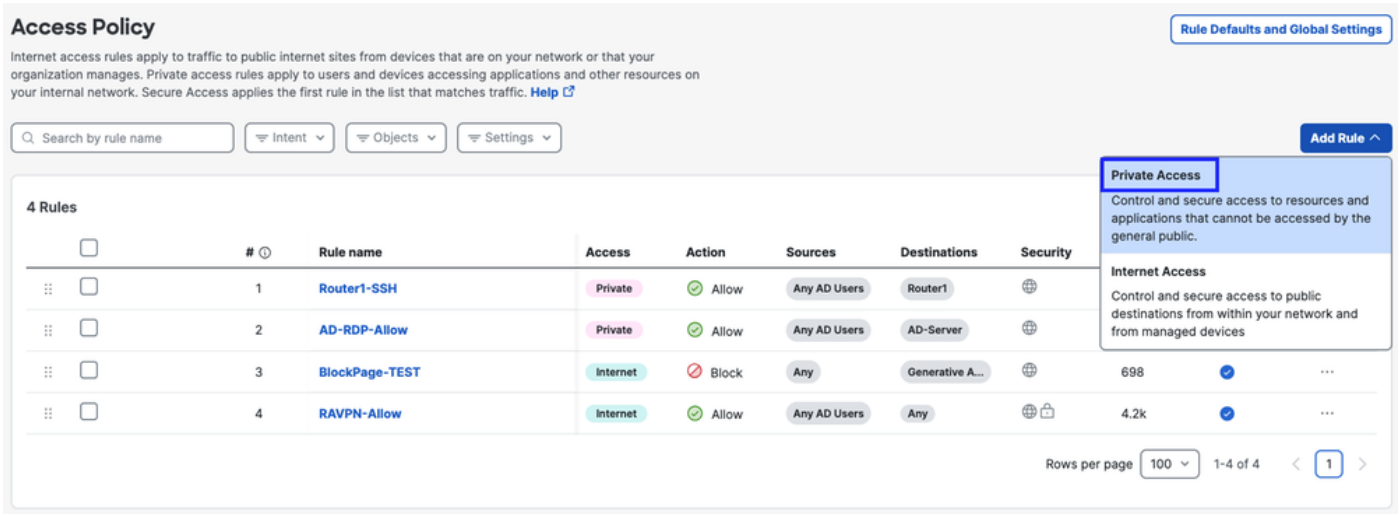
在Secure Access上配置專用訪問，以便由Universal ZTA註冊使用者訪問。有關詳細資訊，請參閱[專用訪問規則]

1. 導覽至Secure > Access Policy



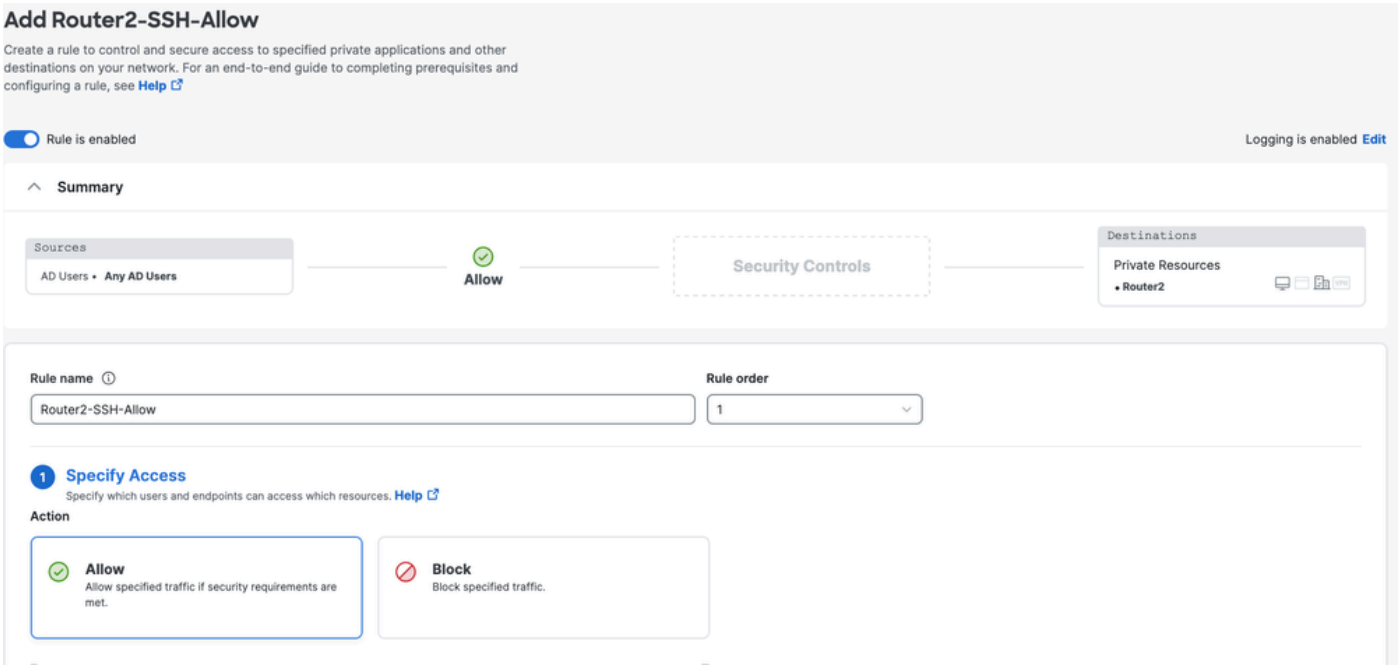
安全訪問 — 訪問策略配置

2.按一下Add Rule，然後選擇Private Access。
規則頂部是描述規則的已配置元件的摘要。



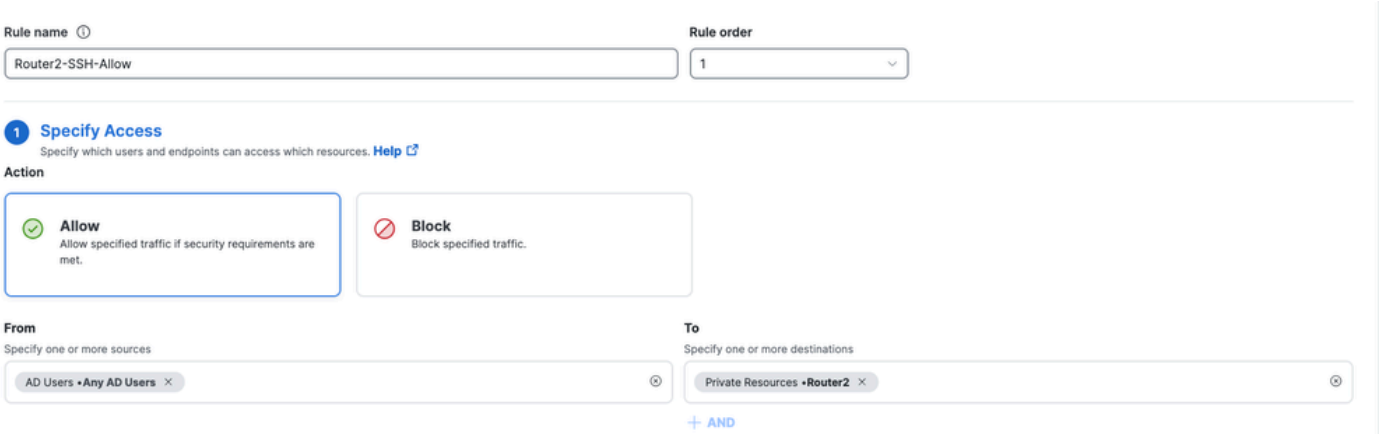
安全訪問 — 訪問策略配置

3.新增規則名稱



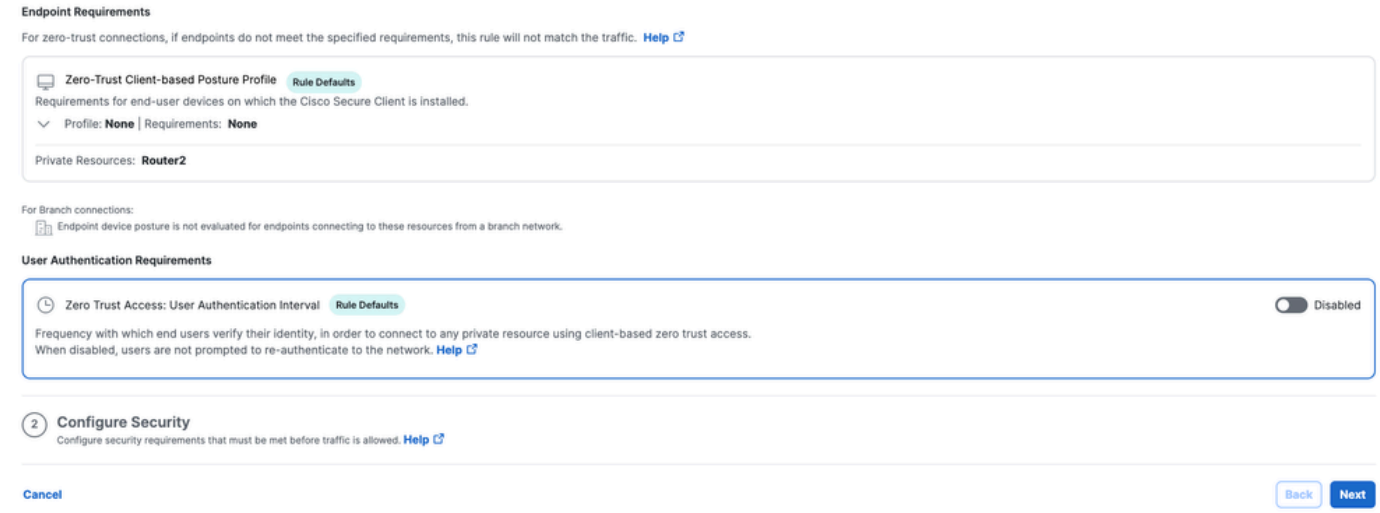
安全訪問 — 訪問策略配置

4.選擇規則操作，然後選擇來源和目標



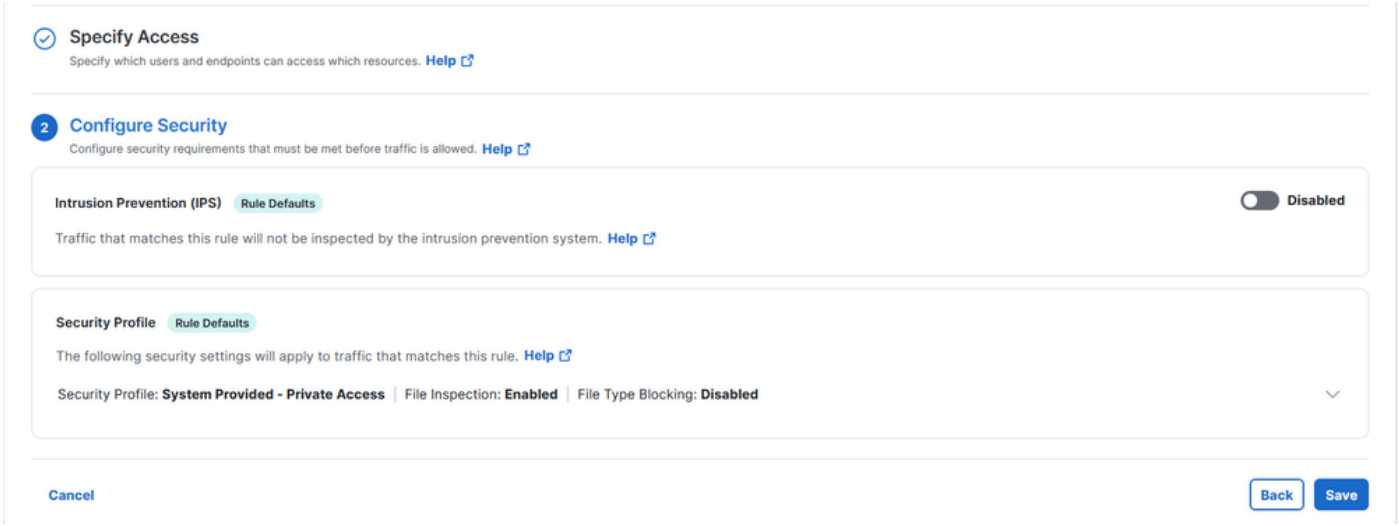
安全訪問 — 訪問策略配置

5.配置終端要求



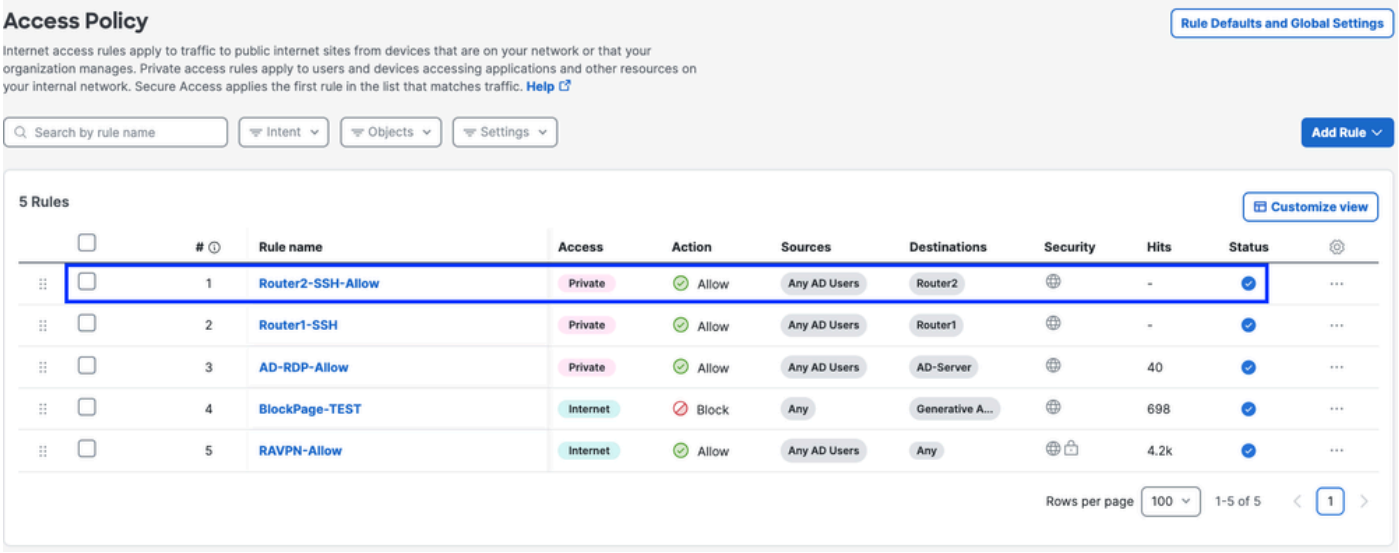
安全訪問 — 訪問策略配置

6. 配置安全性



安全訪問 — 訪問策略配置

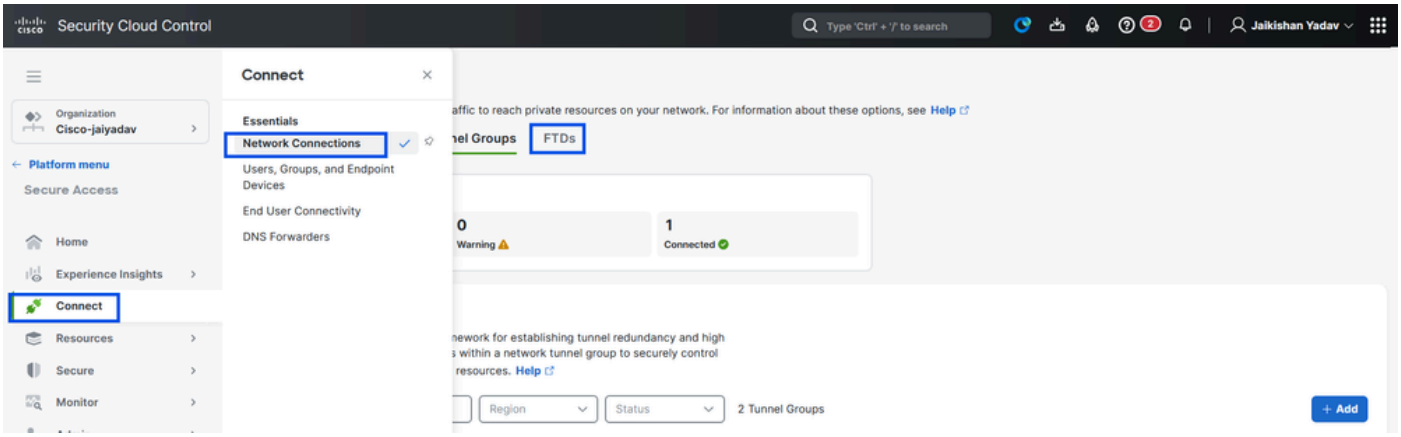
7.按一下Save



安全訪問 — 訪問策略配置

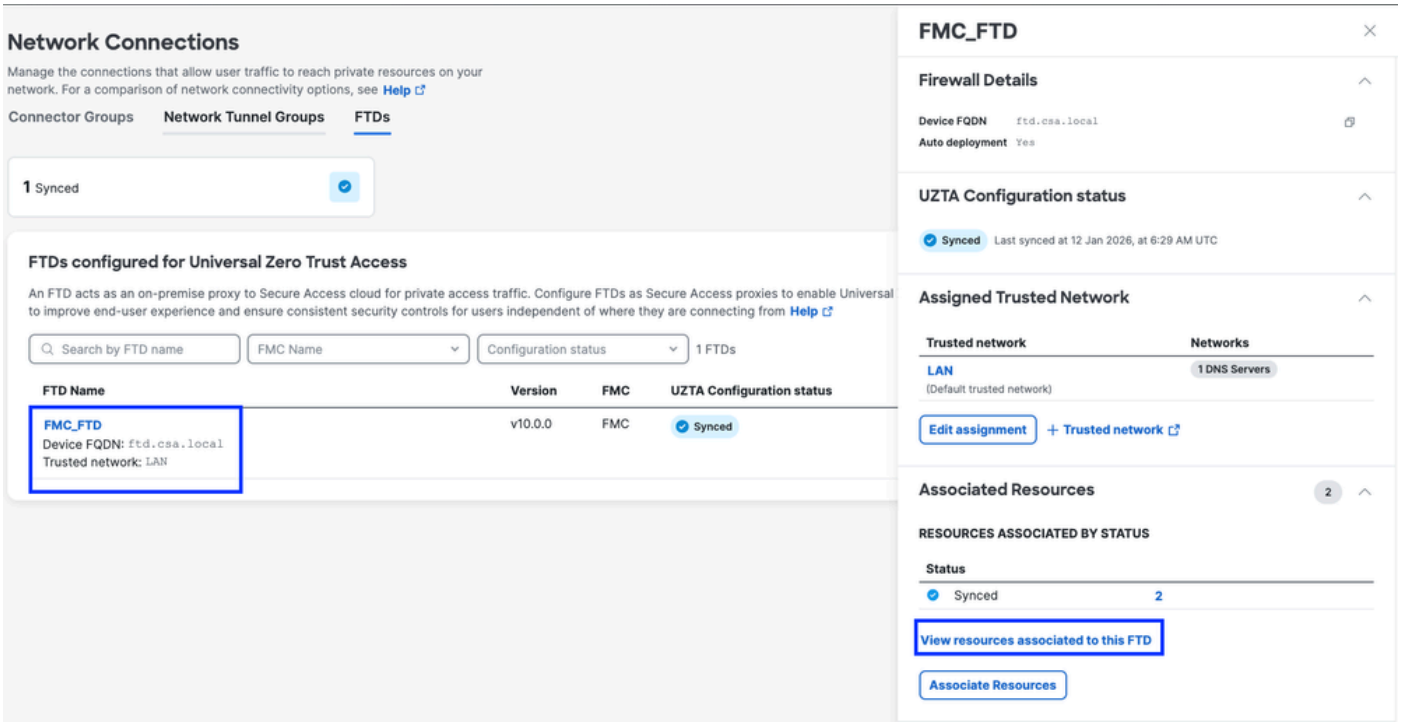
步驟3 — 驗證FTD上PR的關聯

1.定位至「連線」>「網路連線」>「FTD」

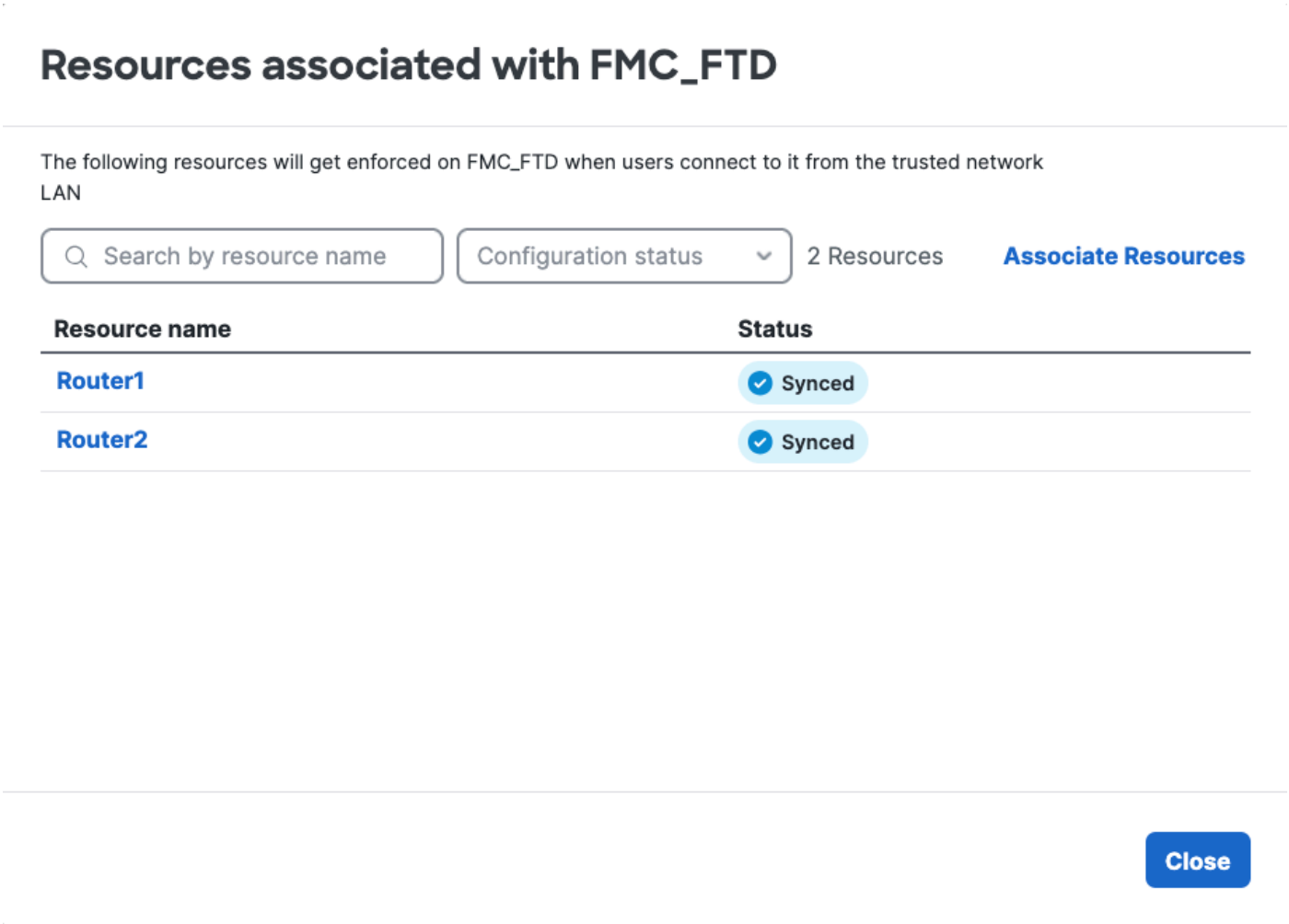


安全訪問 — PR驗證

2. 按一下FTD >檢視與此FTD相關聯的資源

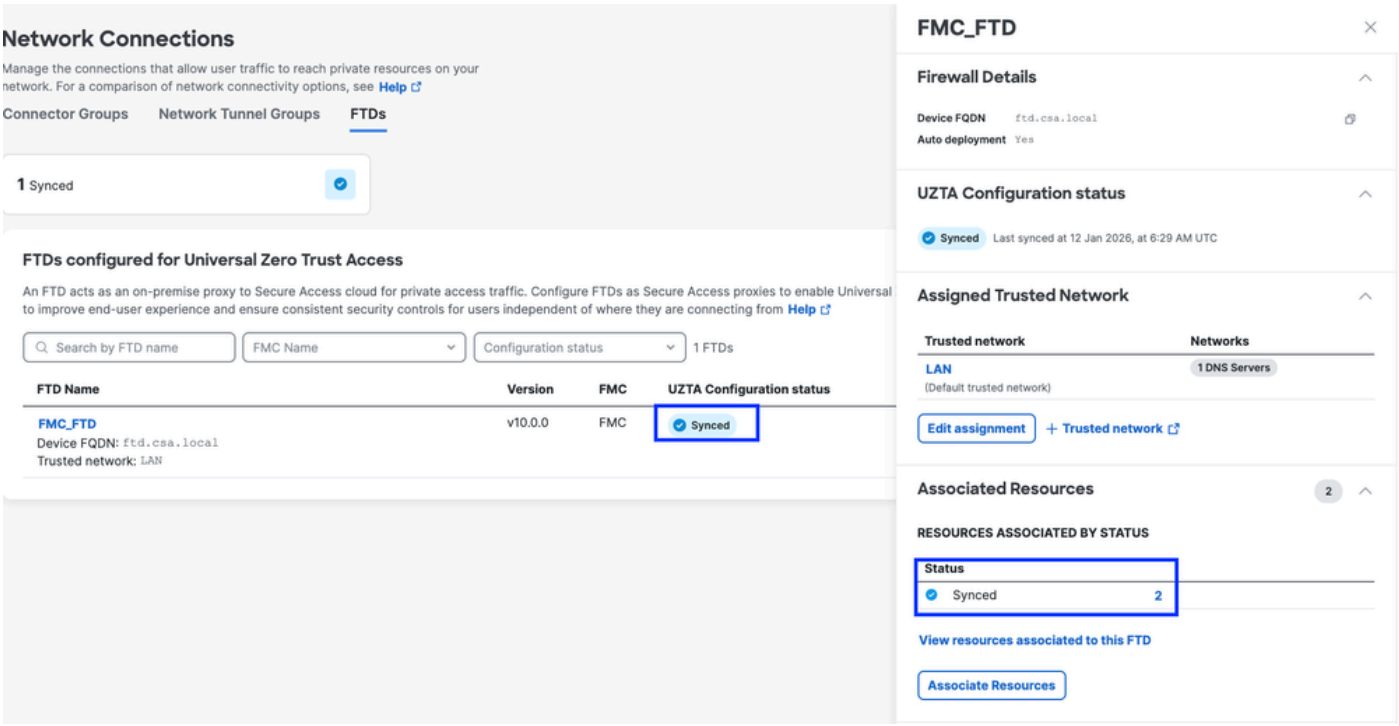

Network Connections
Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help
Connector Groups
Network Tunnel Groups
FTDs
1 Synced
FTDs configured for Universal Zero Trust Access
An FTD acts as an on-premise proxy 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
2
RESOURCES ASSOCIATED BY STATUS
Status
Synced
2
View resources associated to this FTD
Associate Resources

安全訪問 — PR驗證


Resources associated with FMC_FTD
The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN
Search by resource name
Configuration status
2 Resources
Associate Resources
Resource name
Status
Router1
Synced
Router2
Synced
Close

3. 按一下「close」

4.驗證狀態、關聯的資源和配置是否應該處於「已同步」狀態



安全訪問 — PR驗證

5.驗證組態是否已推送到FTD

登入FTD CLI並導覽至LINA模式

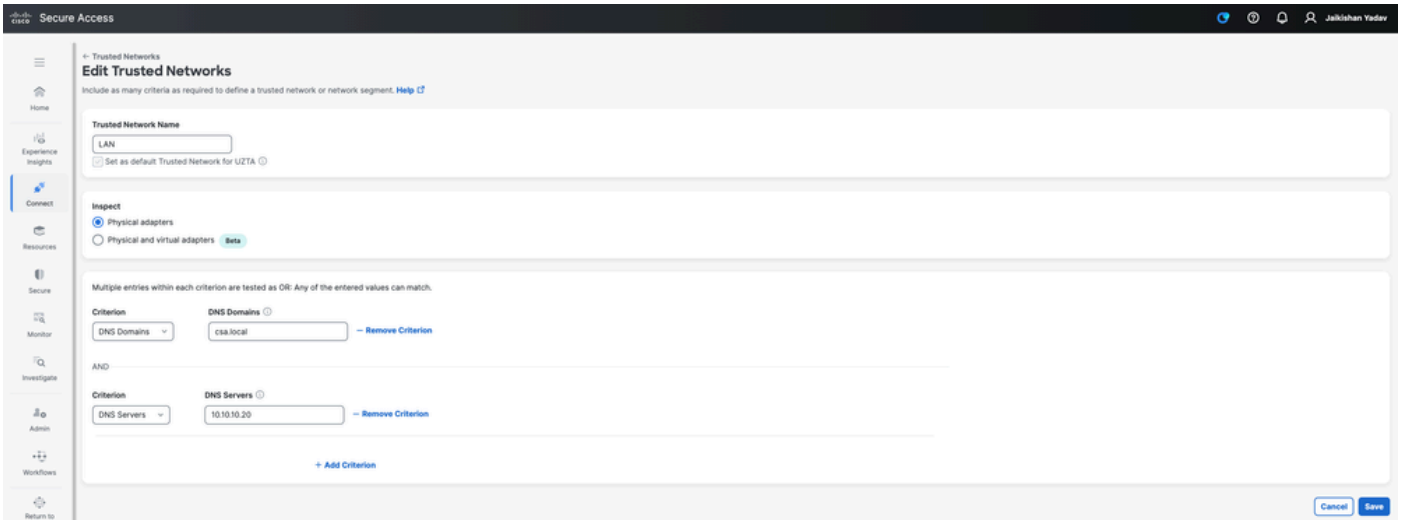
show running-config object application

```
ftd# sh run ob application
object application PR_Router1
 id 427221
 internal domain router1.csa.local tcp eq 22
 internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
 external domain router1.csa.local
 external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
 id 434482
 internal domain router2.csa.local tcp eq 22
 internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
 external domain router2.csa.local
 external subnet 10.10.10.102 255.255.255.255
```

安全訪問 — PR驗證

步驟 — 4 Configure" Manage Trusted Networks or ZTA Settings"

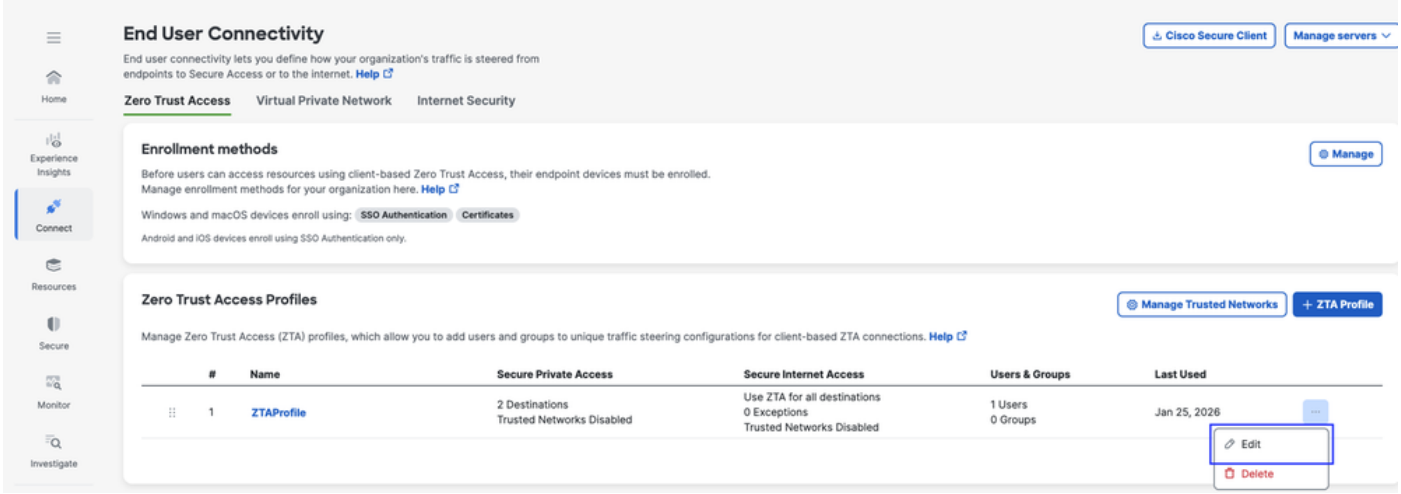
導航到Connect > End User Connectivity > Zero Trust Access > ZTA Settings並配置受信任網路



安全訪問 — TND配置

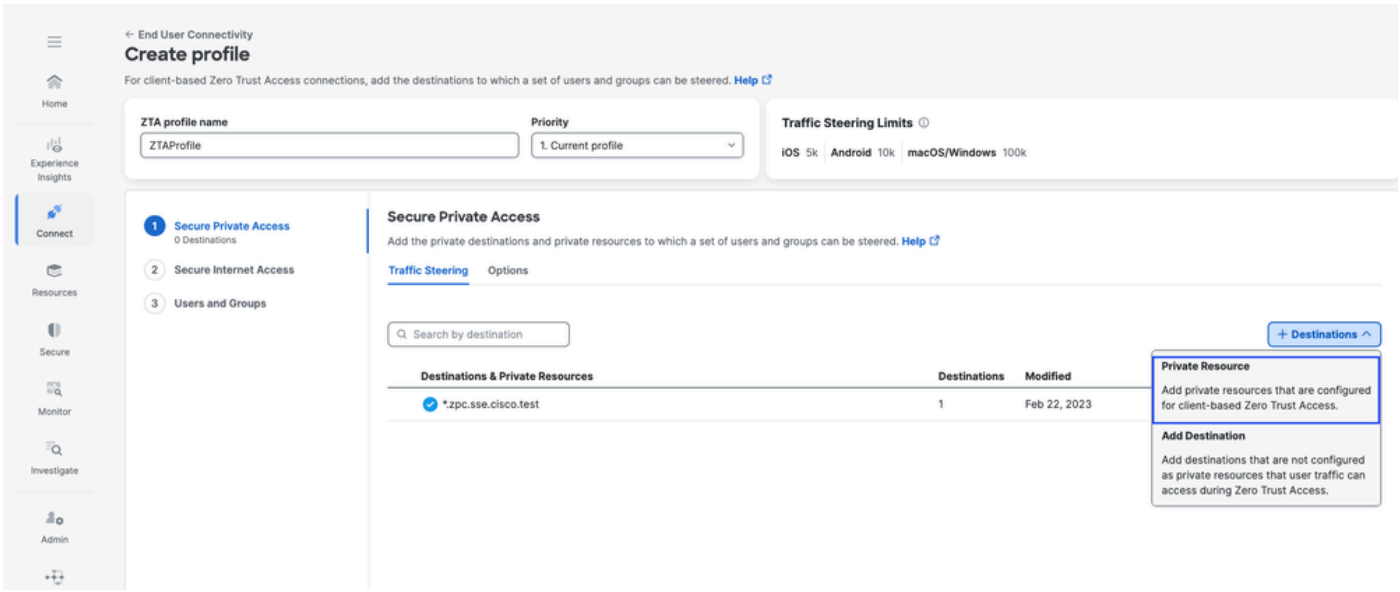
第–5步向ZTA配置檔案中新增專用資源

1.導航至Connect > End User Connectivity > Zero Trust Access，然後按一下3個點以編輯ZTA配置檔案

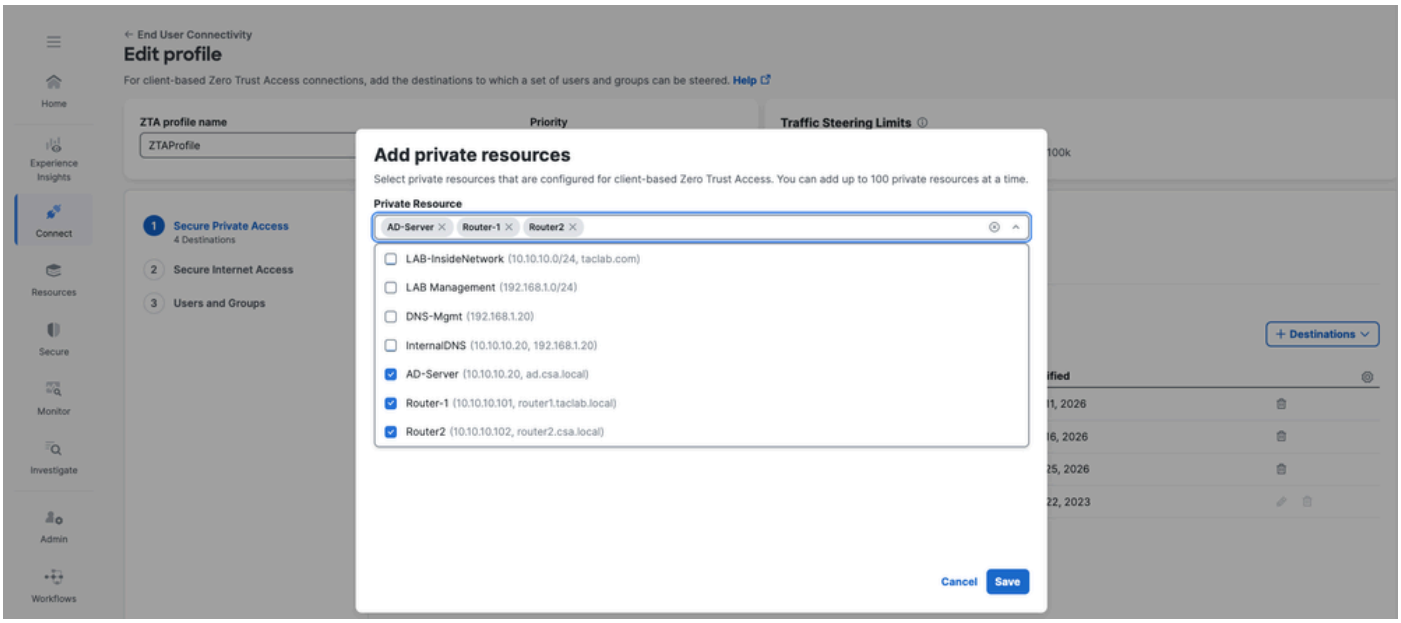


安全訪問 — ZTA配置檔案

2.新增專用資源

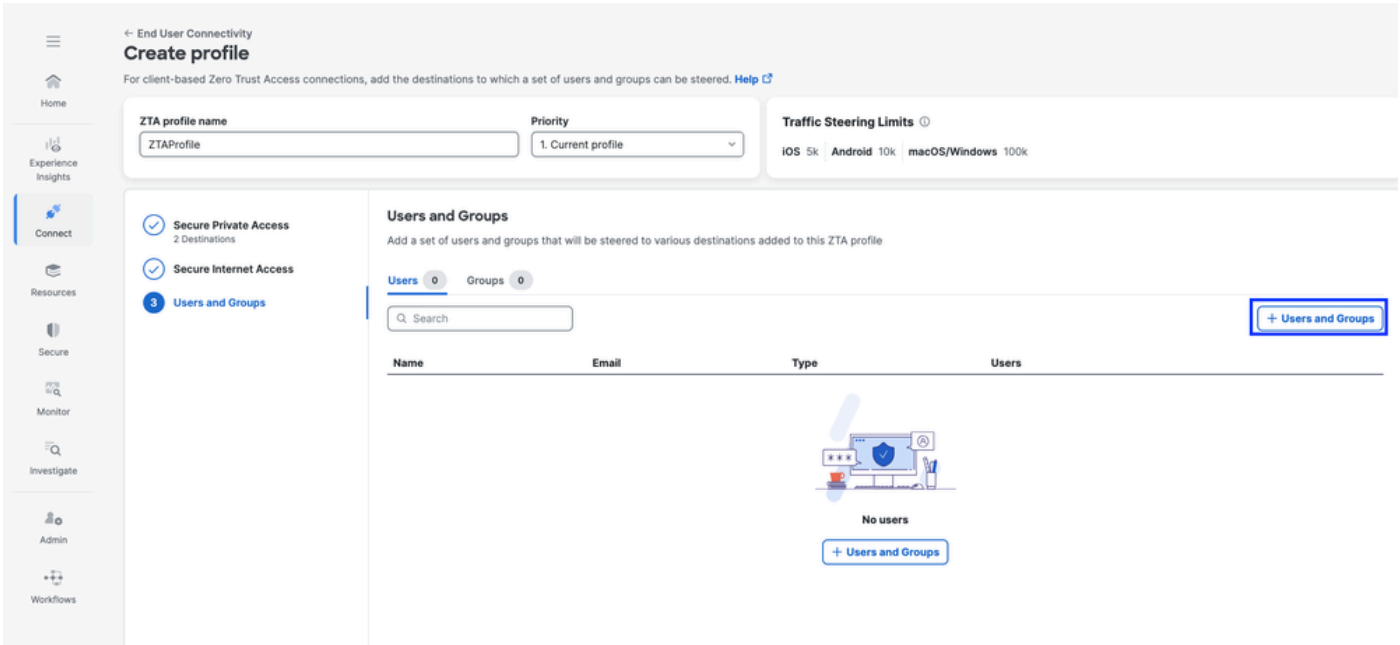


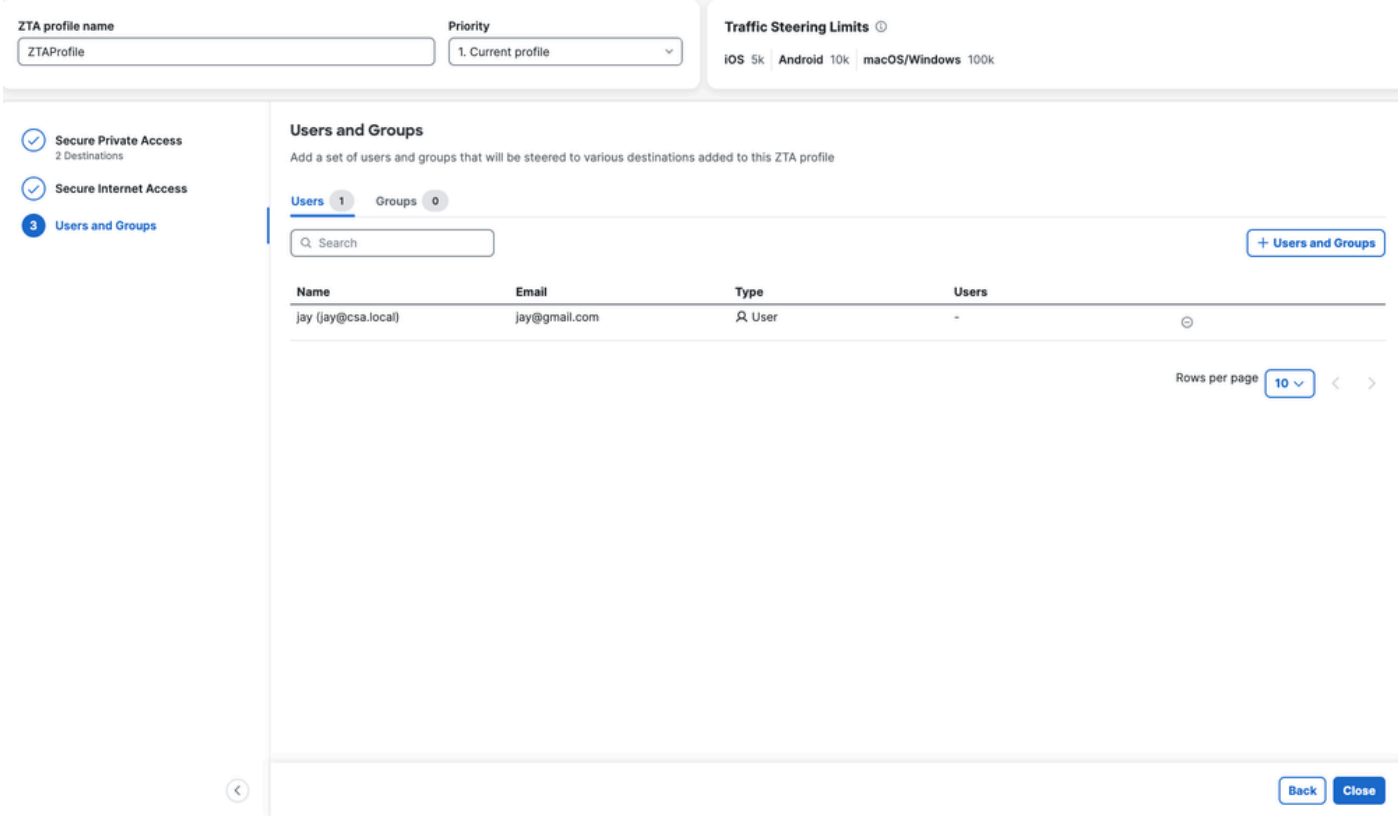
安全訪問 — ZTA配置檔案



安全訪問 — ZTA配置檔案

3.新增使用者和組

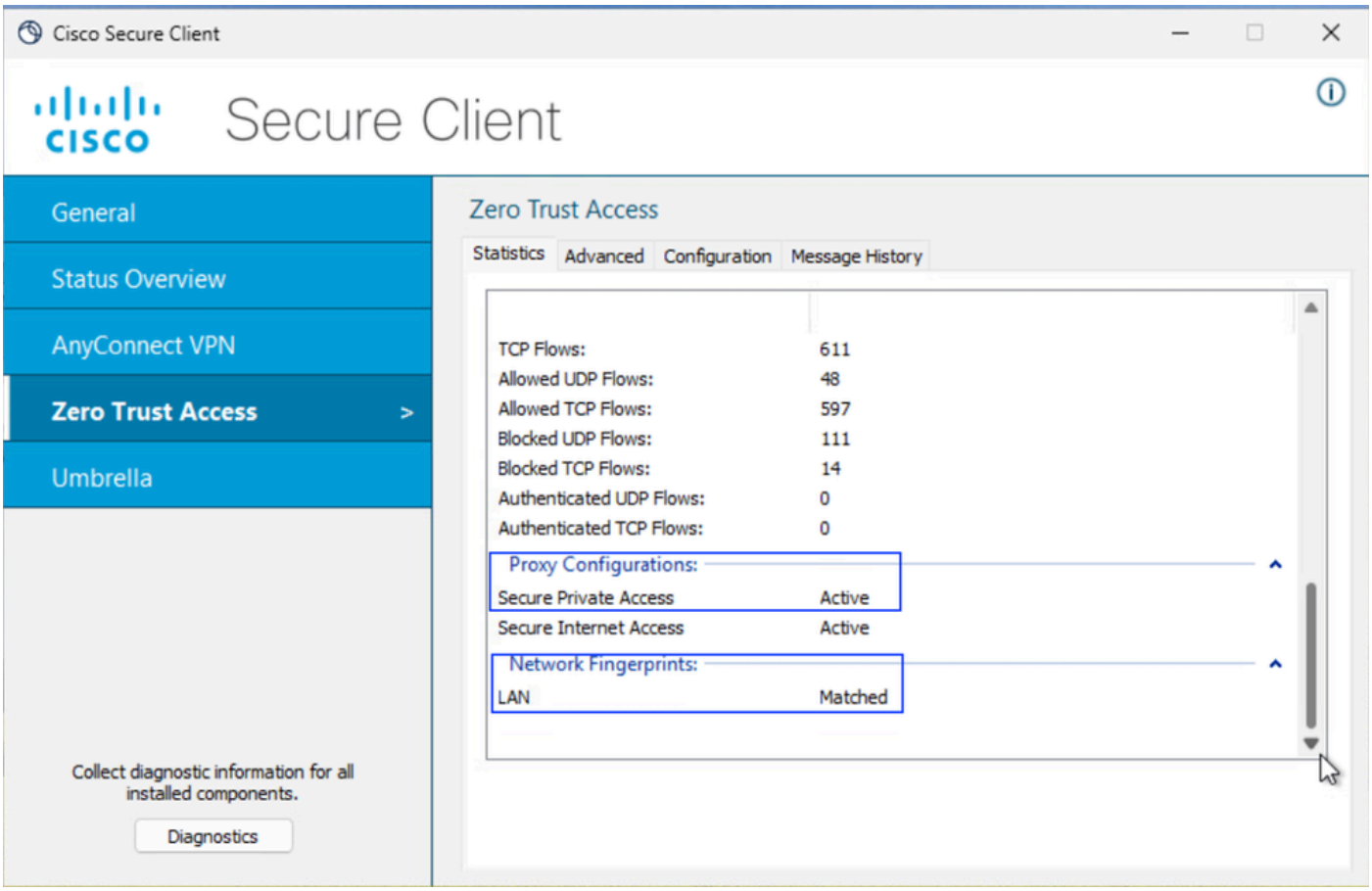




安全訪問 — ZTA配置檔案

步驟 — 6驗證對專用資源的訪問

1.驗證ZTA TND的網路指紋



安全訪問 — PR測試

2. 驗證遠端使用者是否可解析FTD FQDN

```
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
```

安全訪問 — PR測試

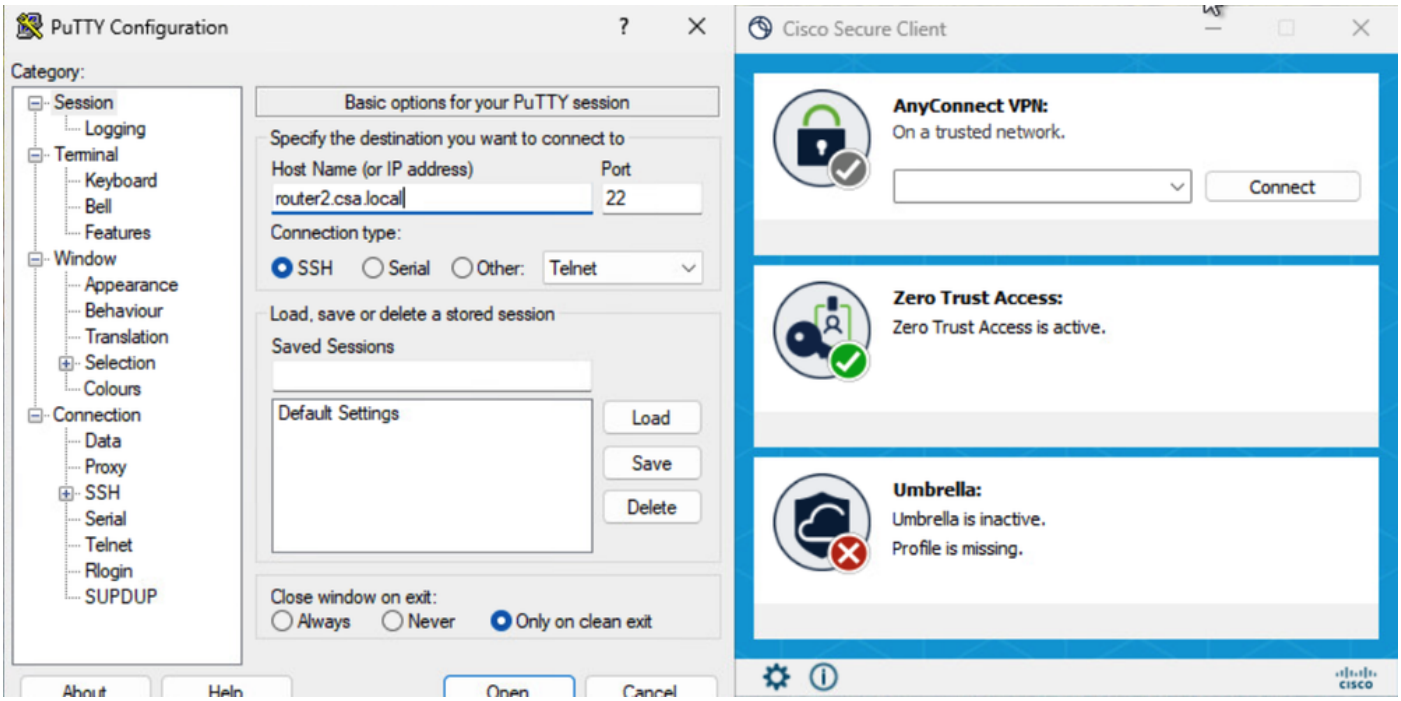
3.驗證FTD是否可以使用FQDN訪問私有資源

```
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#
```

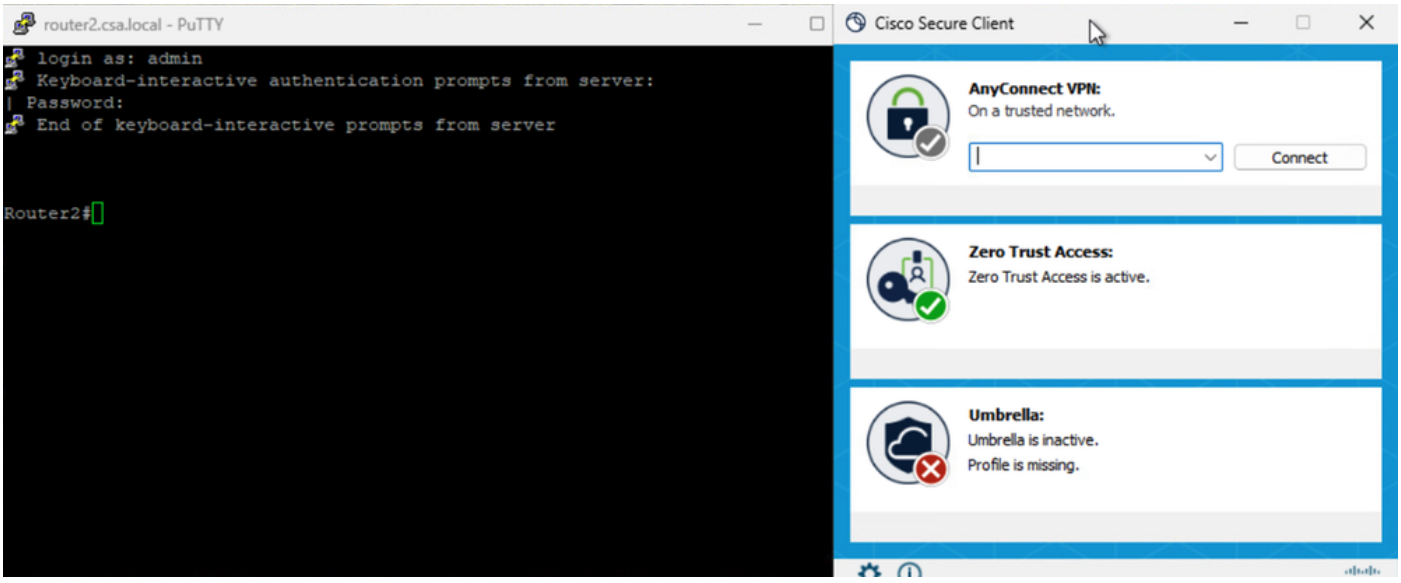
安全訪問 — PR測試

4. 測試到專用資源的SSH連線

使用FQDN訪問PR

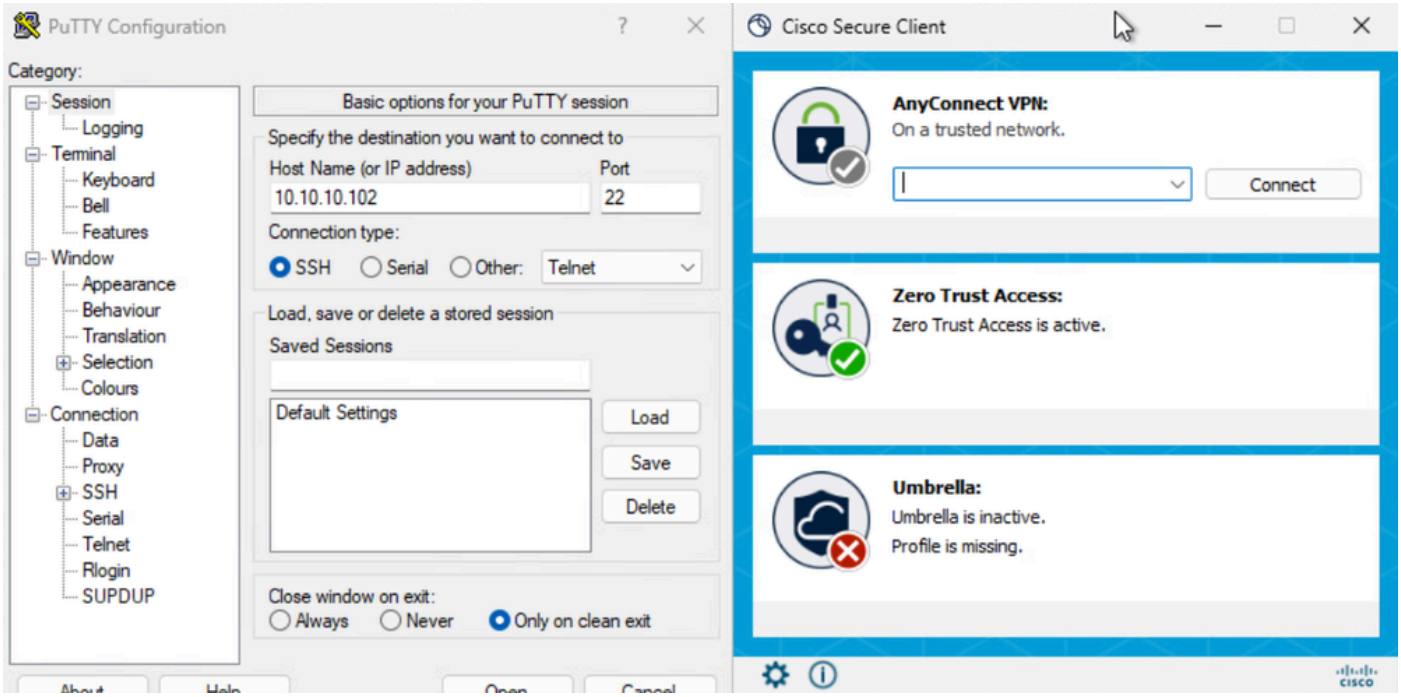


安全訪問 — PR測試

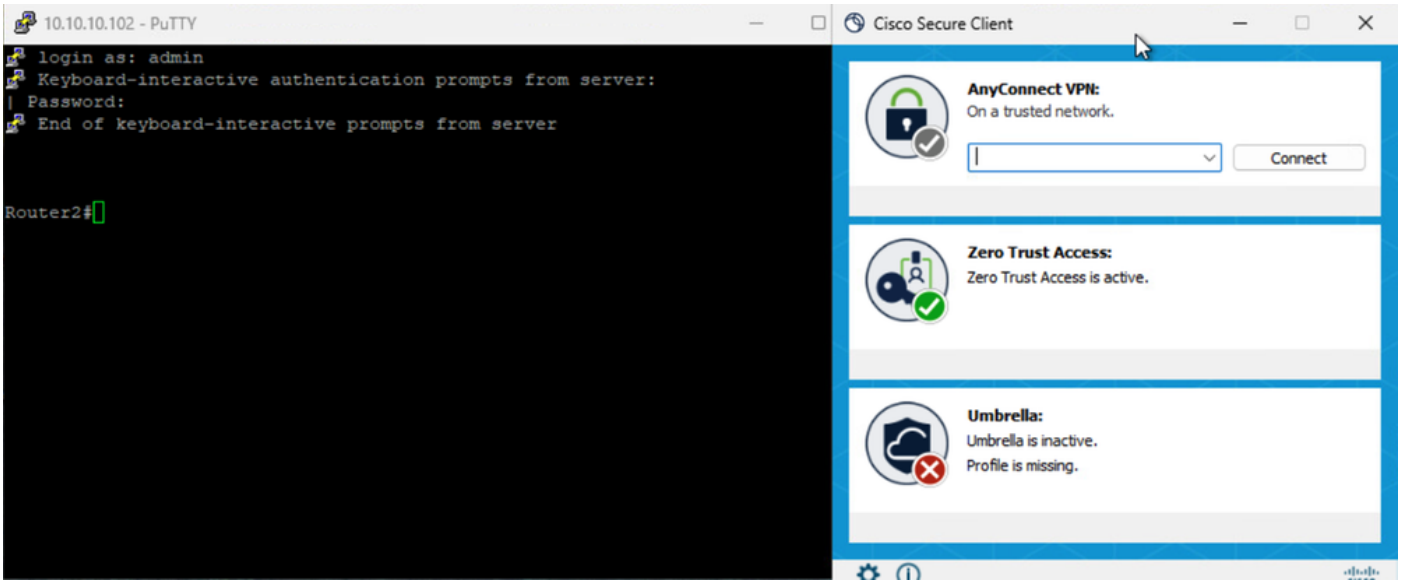


安全訪問 — PR測試

使用IP地址訪問PR

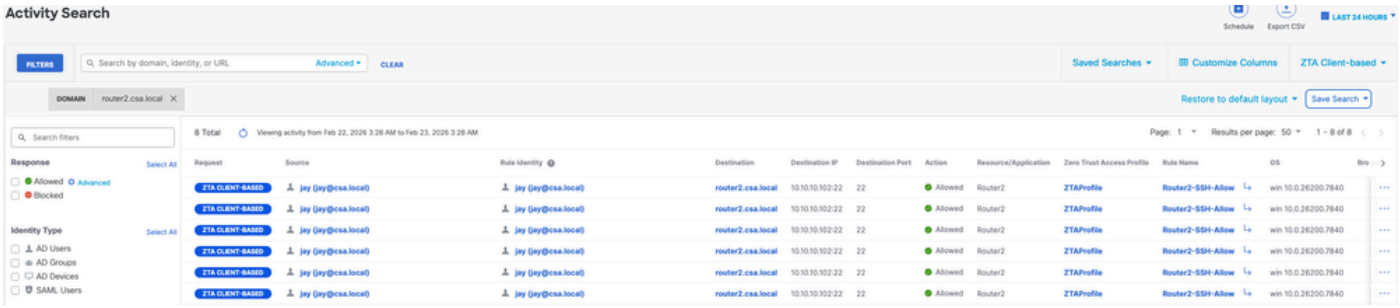


安全訪問 — PR測試

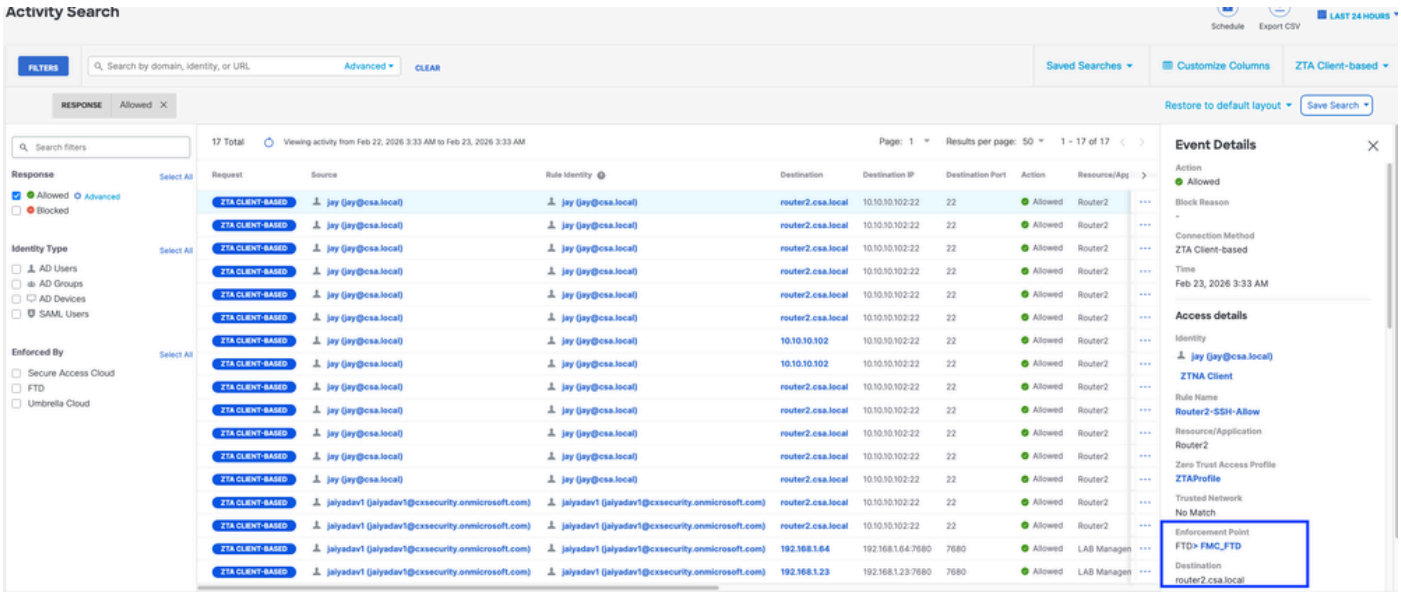


安全訪問 — PR測試

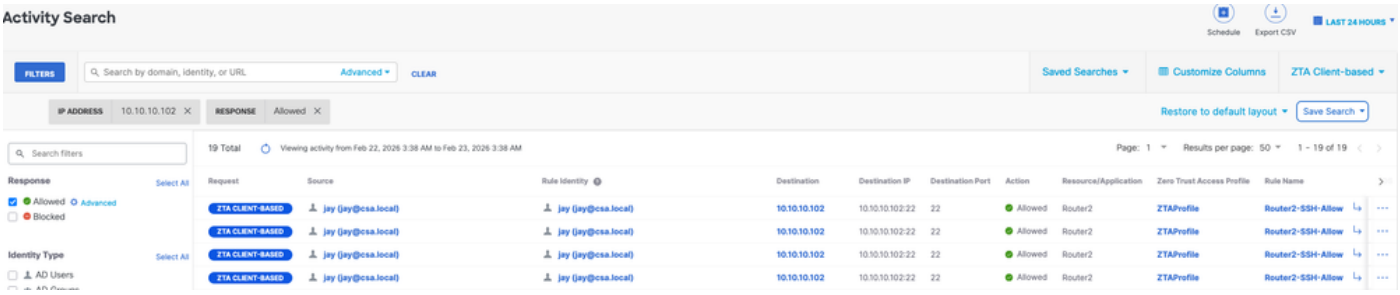
5. 驗證安全訪問活動搜尋日誌



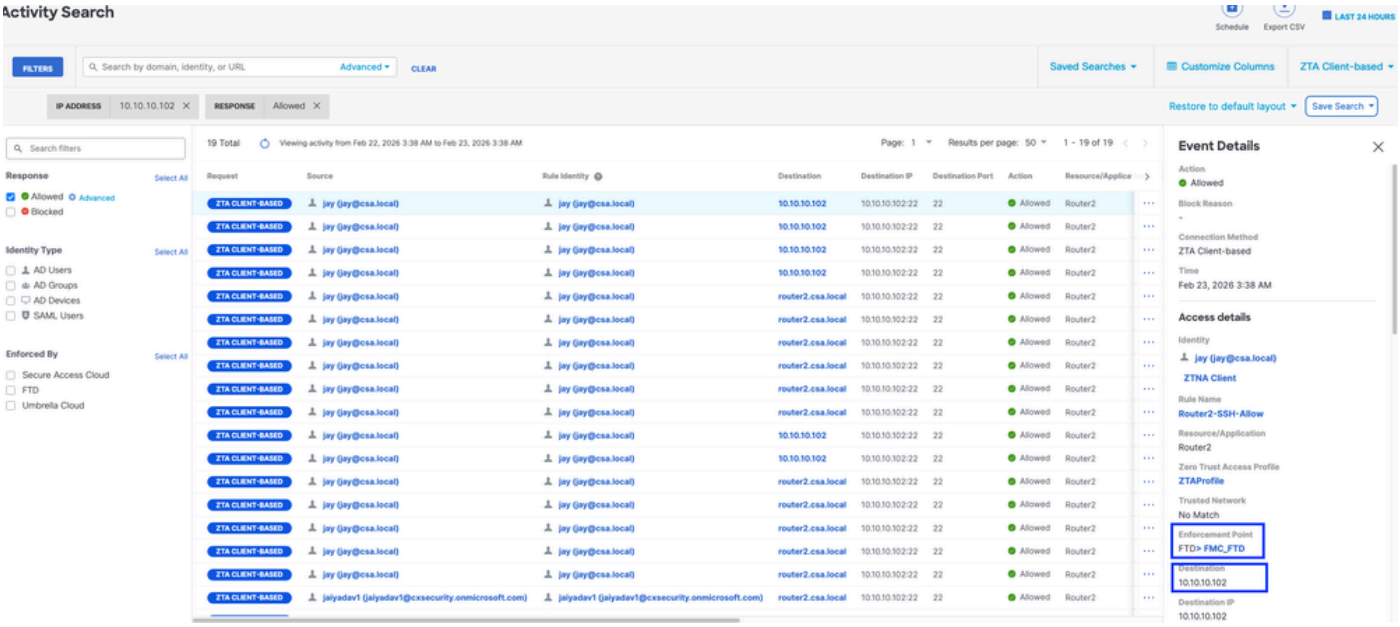
安全訪問 — 活動搜尋



安全訪問 — 活動搜尋

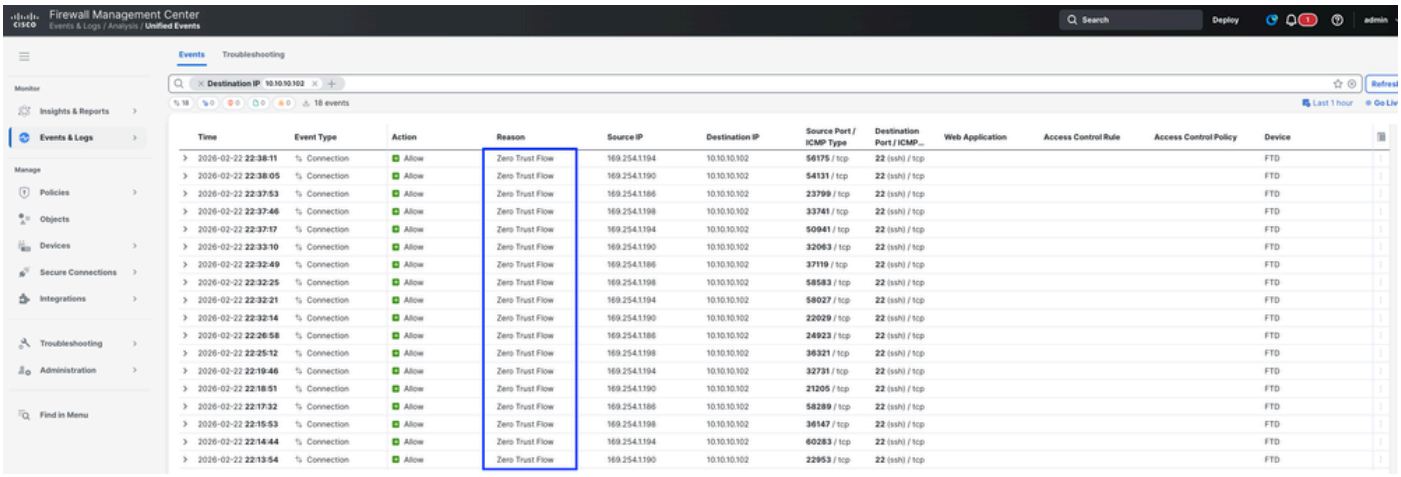


安全訪問 — 活動搜尋



安全訪問 — 活動搜尋

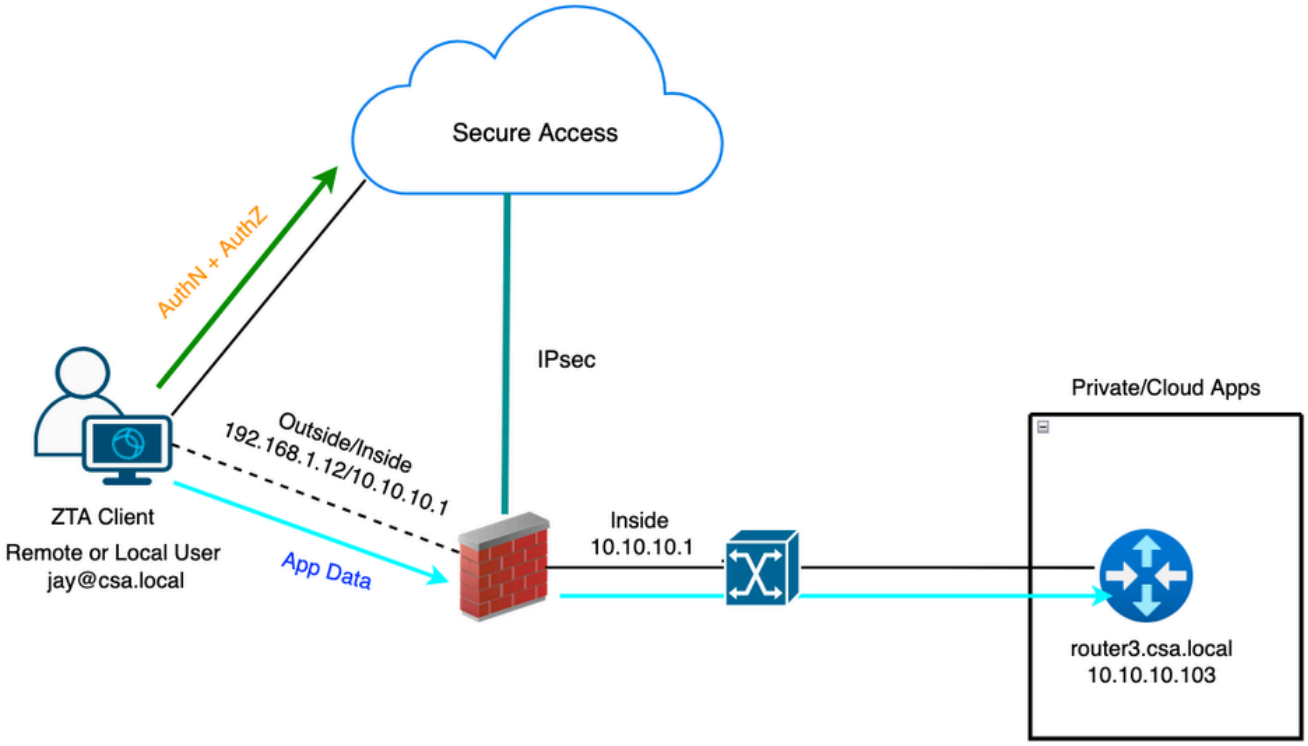
6. 驗證FMC連線事件



FMC連線事件

測試案例4 — 本地和遠端使用者 — 使用TND的本地或雲實施

在本例中，實施的型別取決於使用者位置，如果使用者是本地或受信任FTD區域（內部、DMZ等）之後，則實施的型別將是本地（測試案例3）。同樣，如果使用者是遠端使用者，則實施方式為雲（測試案例1）。 使用者位置將根據網路指紋或TND設定確定，如果網路指紋匹配，則使用者的本地為Local，如果不匹配，則使用者本地為Remote。

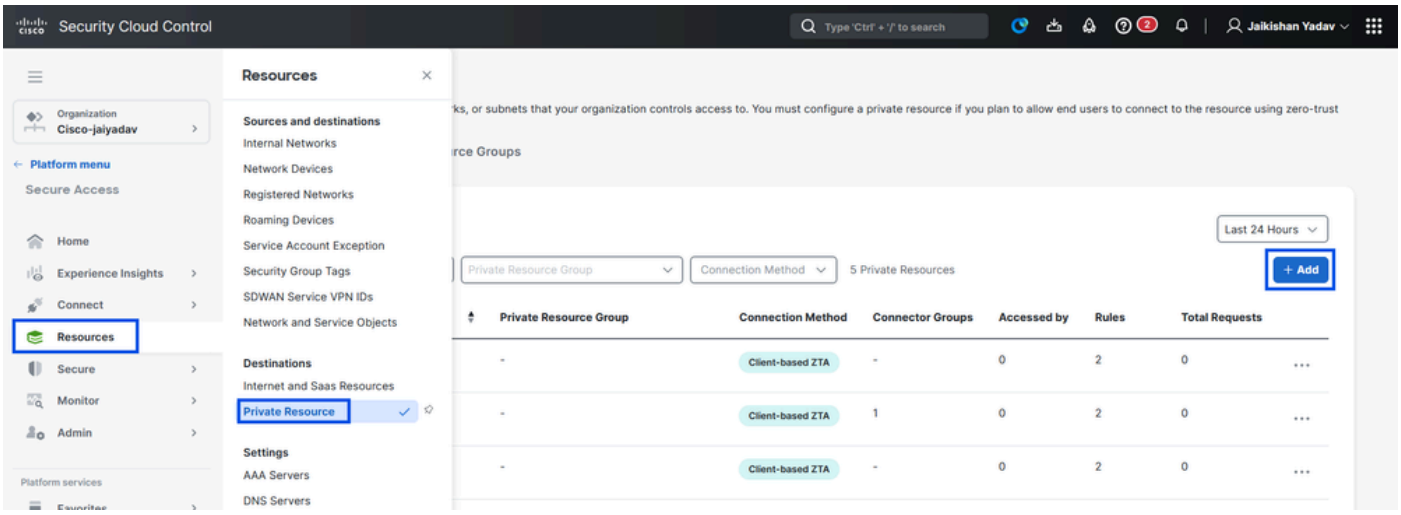


通用ZTA — 測試用例拓撲

第1步 — 在安全訪問中定義專用資源

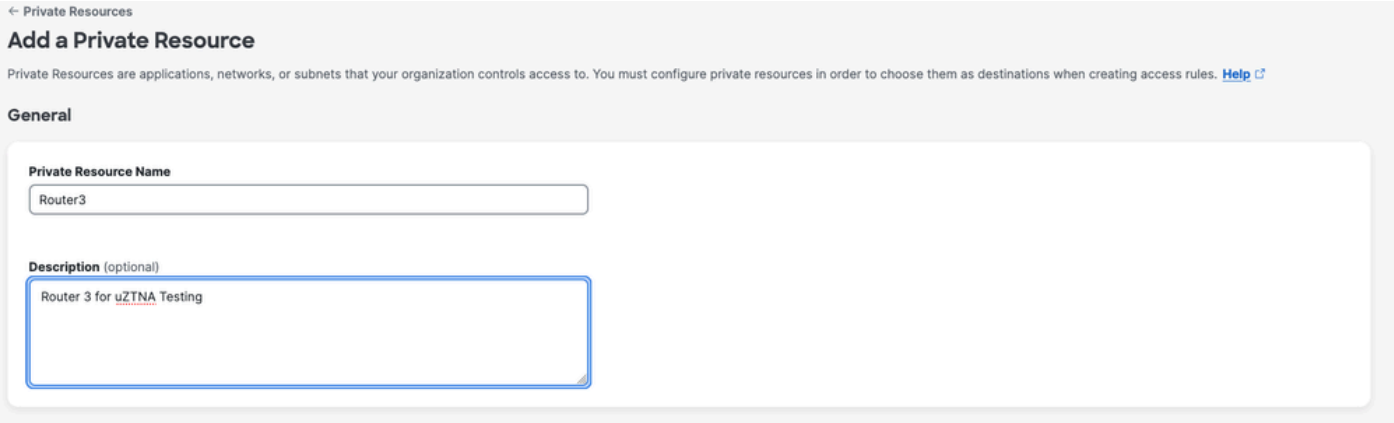
配置可通過零信任訪問(ZTA)註冊裝置訪問私有資源（具有雲實施）

1. 導覽至Resources > Destinations > Private Resources >按一下+Add



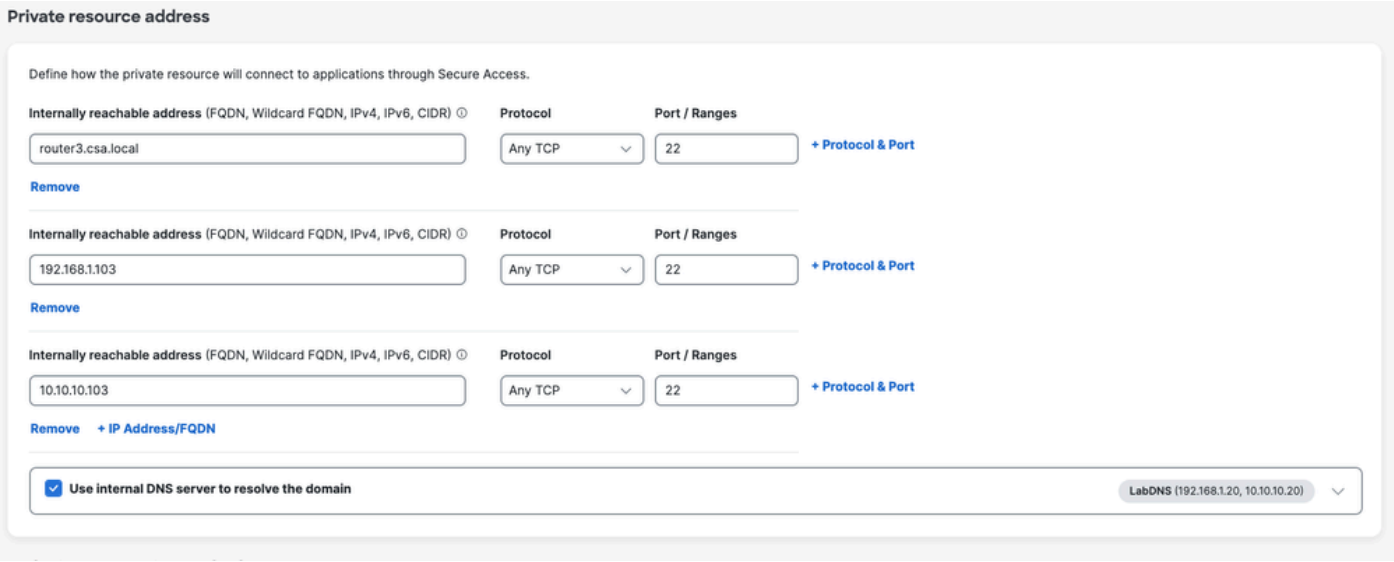
安全訪問 — 專用資源配置

2.對於私有資源名稱，輸入資源有意義的名稱。對於Description，建議您提供諸如資源用途或資源擁有者名稱等資訊。



3.輸入要訪問的專用資源的FQDN。我們還可以定義專用資源的IP地址。有關詳細資訊，請參閱新增專用資源

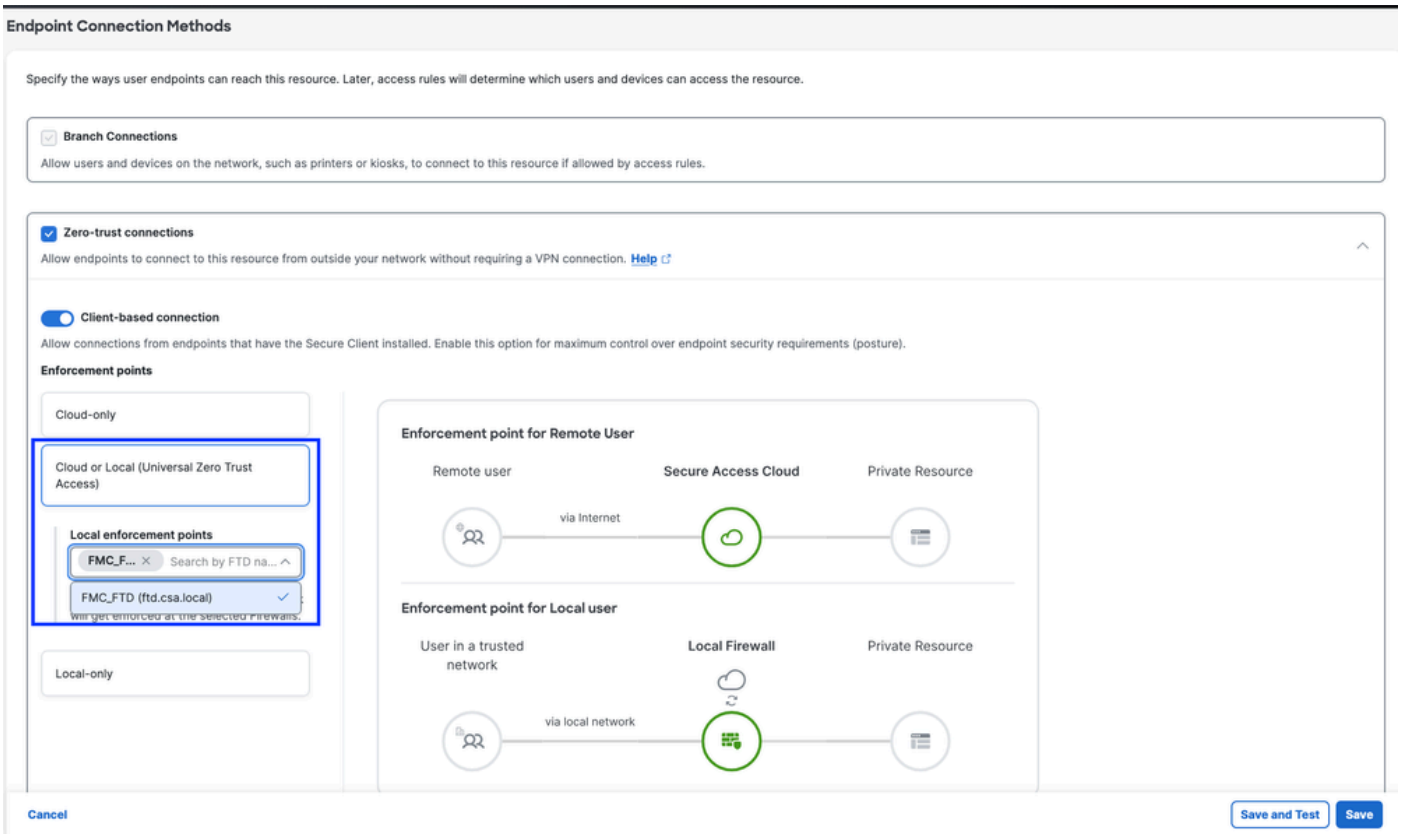
4.選擇要解析域的DNS伺服器



安全訪問 — 專用資源配置

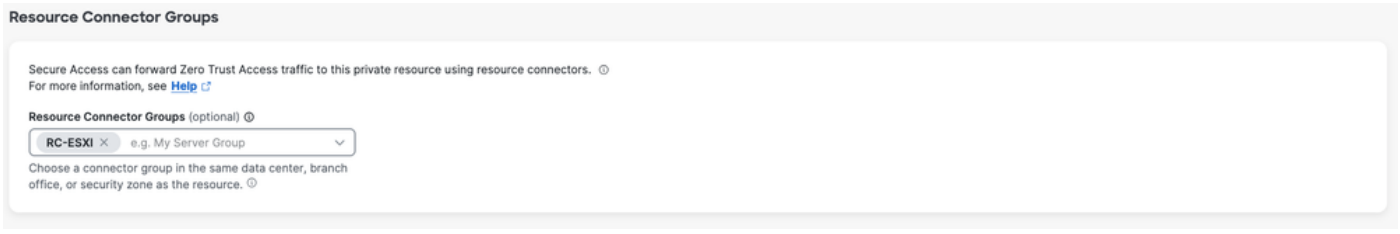
5. 選擇端點連線方法

6.選擇FTD作為本地實施點



安全訪問 — 專用資源配置

如果可通過RC訪問私有資源，則選擇RC；否則，如果可通過網路隧道組（IPsec隧道）訪問私有資源，請將其留空。



安全訪問 — 專用資源配置

附註：根據您選擇的註冊型別，此更改將自動將PR與FTD關聯並觸發策略部署

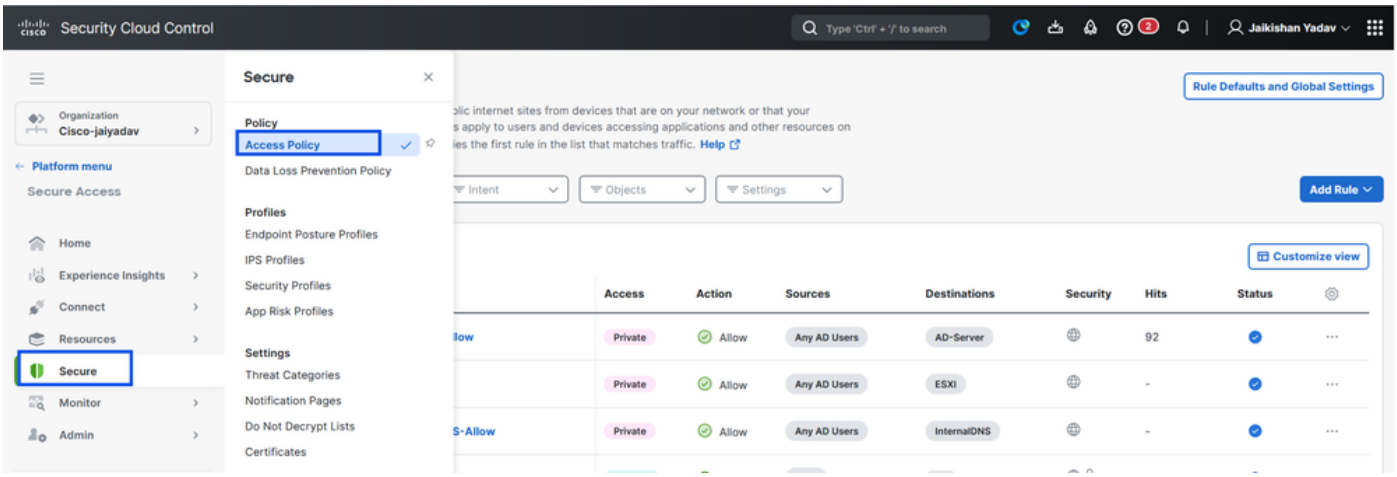
7. 按一下「Save」

第2步 — 建立專用訪問規則

在Secure Access上配置專用訪問，以便由Universal ZTA註冊使用者訪問。有關詳細資訊，請參閱

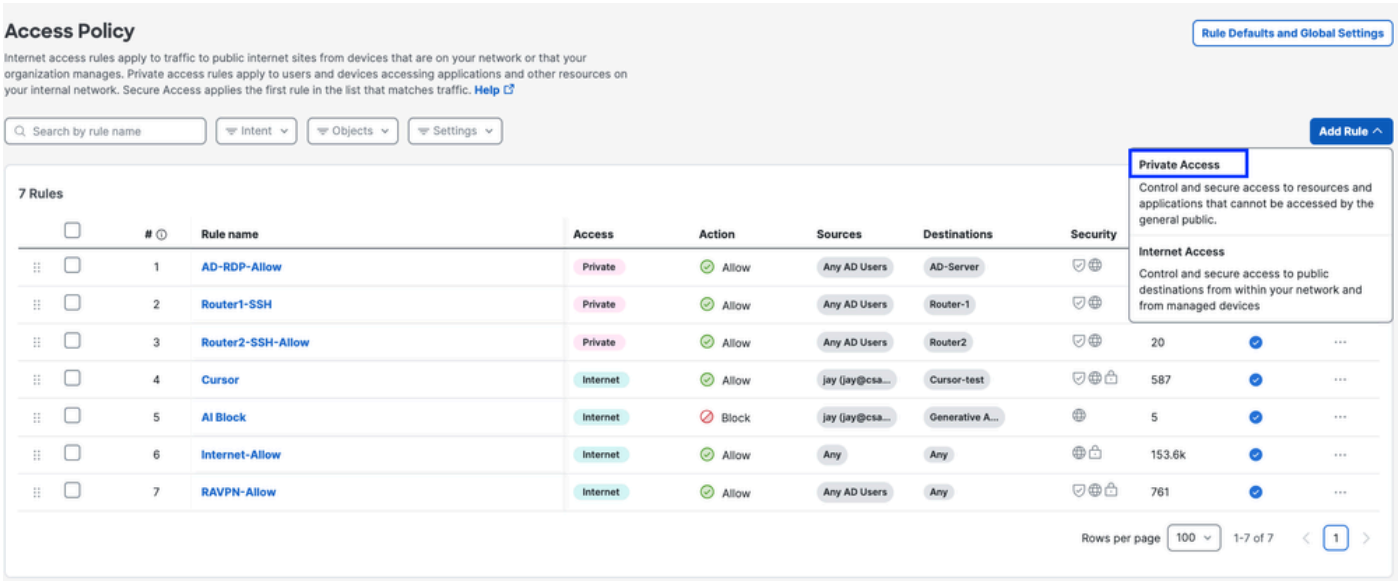
[專用訪問規則]

1. 導覽至Secure > Access Policy



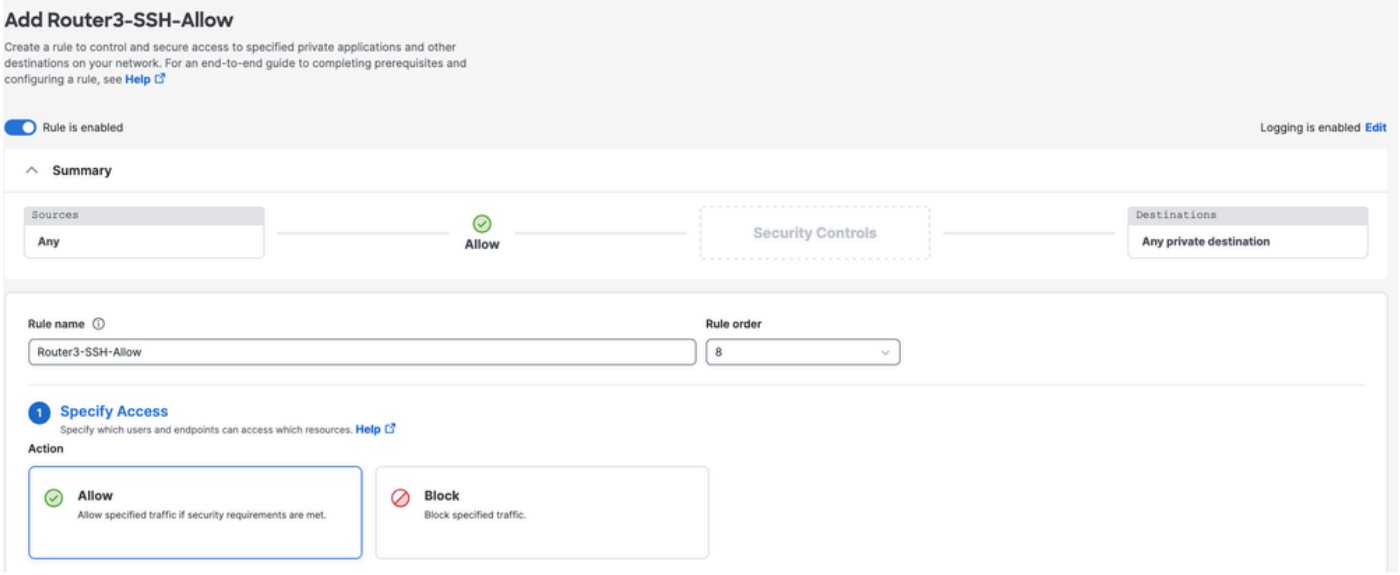
安全訪問 — 訪問策略配置

2.按一下Add Rule，然後選擇Private Access。
規則頂部是描述規則的已配置元件的摘要。



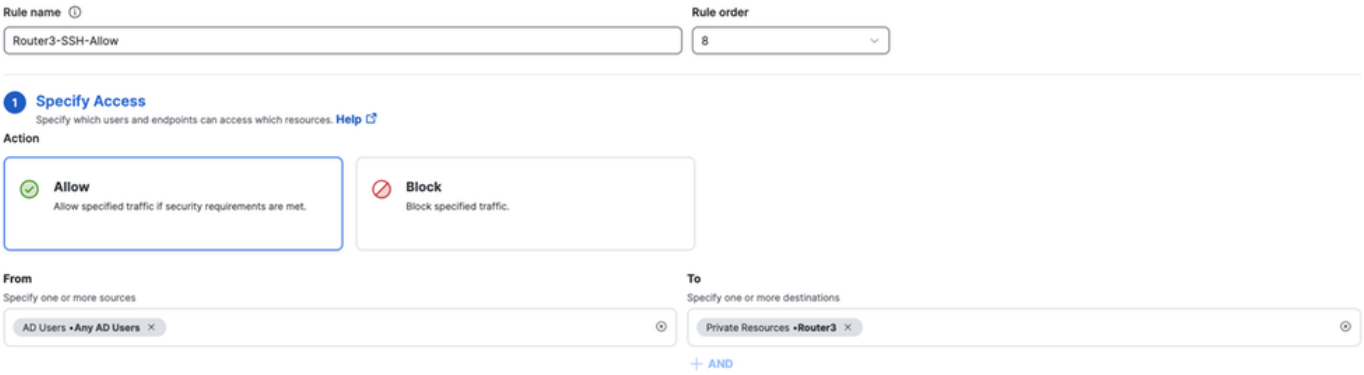
安全訪問 — 訪問策略配置

3.新增規則名稱



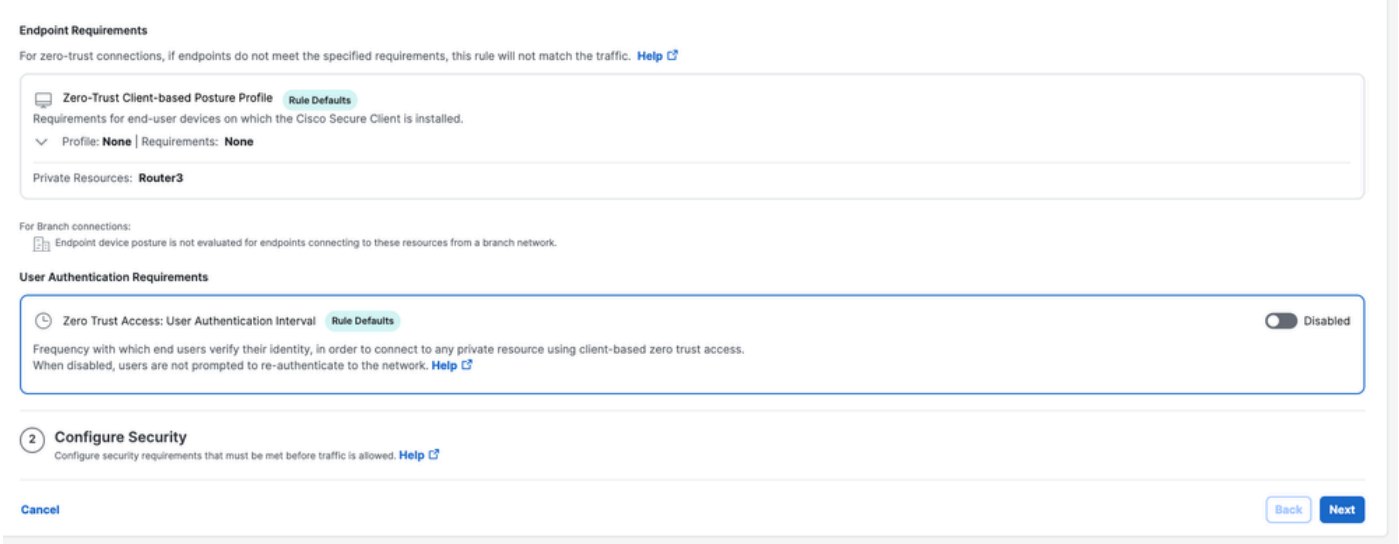
安全訪問 — 訪問策略配置

4.選擇規則操作，然後選擇來源和目標



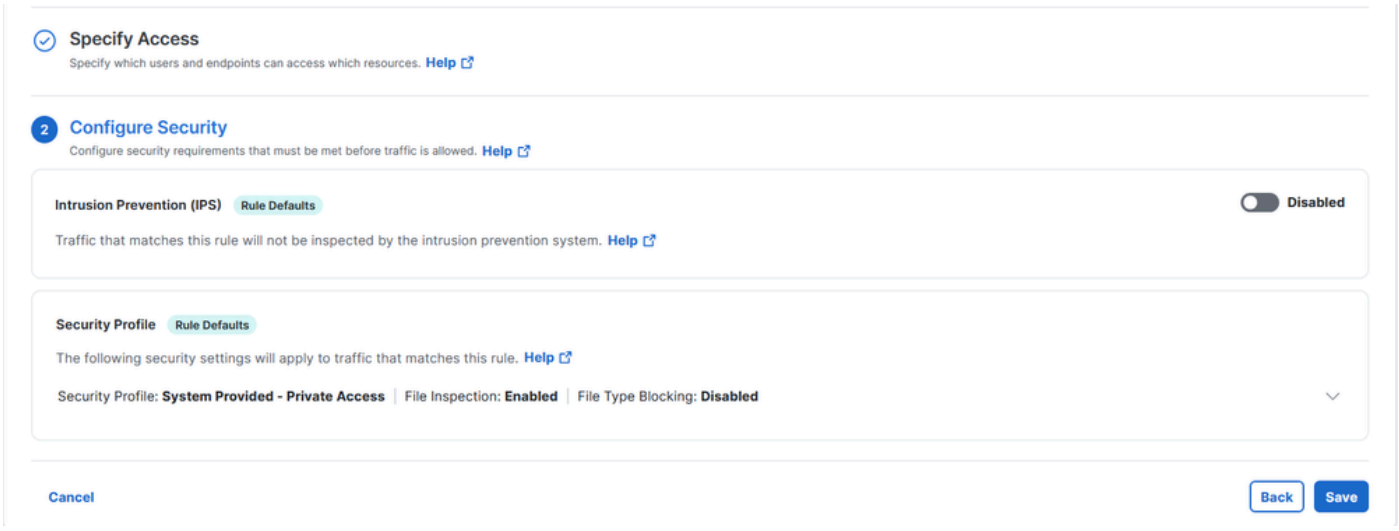
安全訪問 — 訪問策略配置

5.配置終端要求



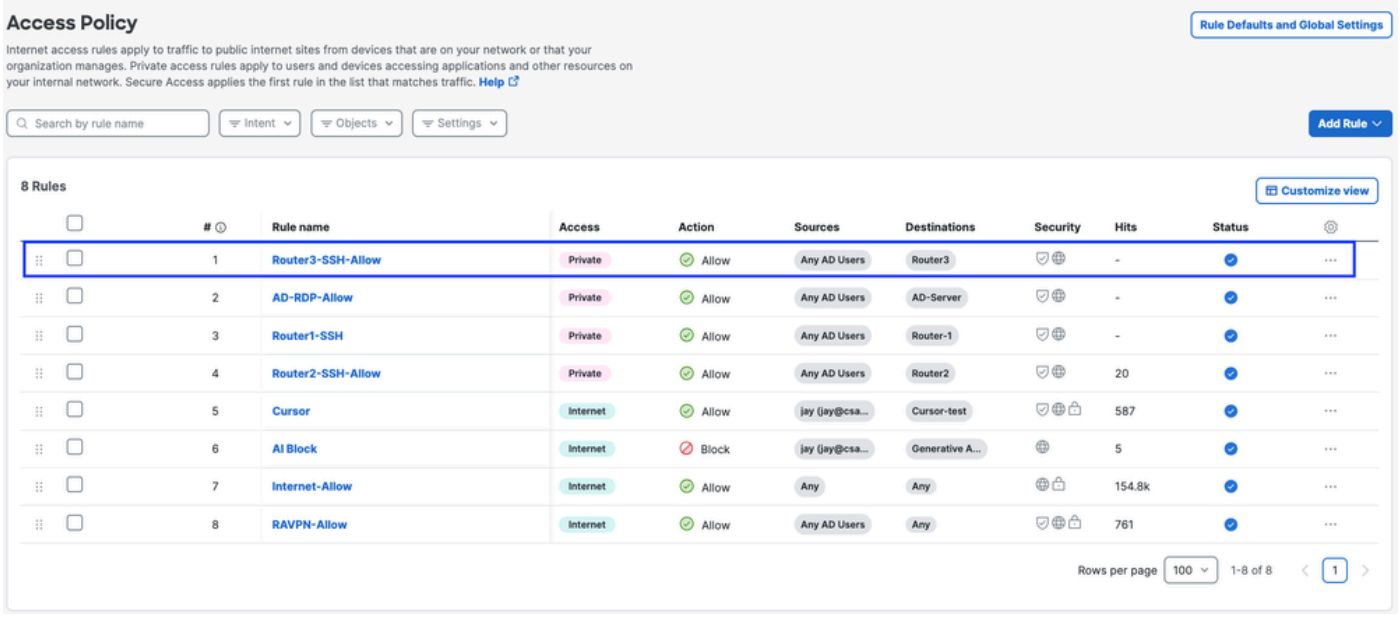
安全訪問 — 訪問策略配置

6. 配置安全性



安全訪問 — 訪問策略配置

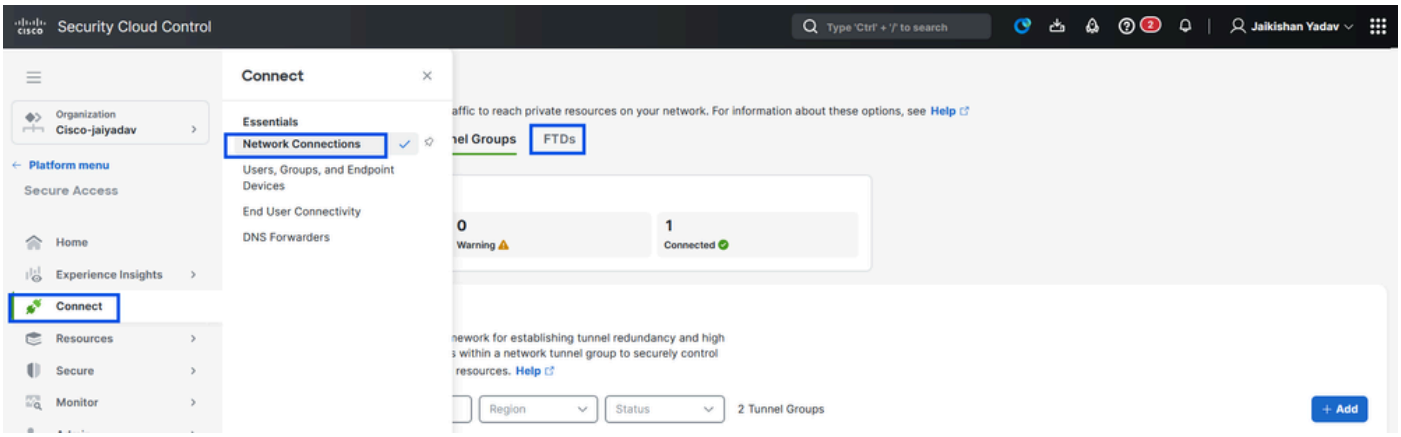
7.按一下Save



安全訪問 — 訪問策略配置

步驟3 — 驗證FTD上PR的關聯

1.定位至「連線」>「網路連線」>「FTD」

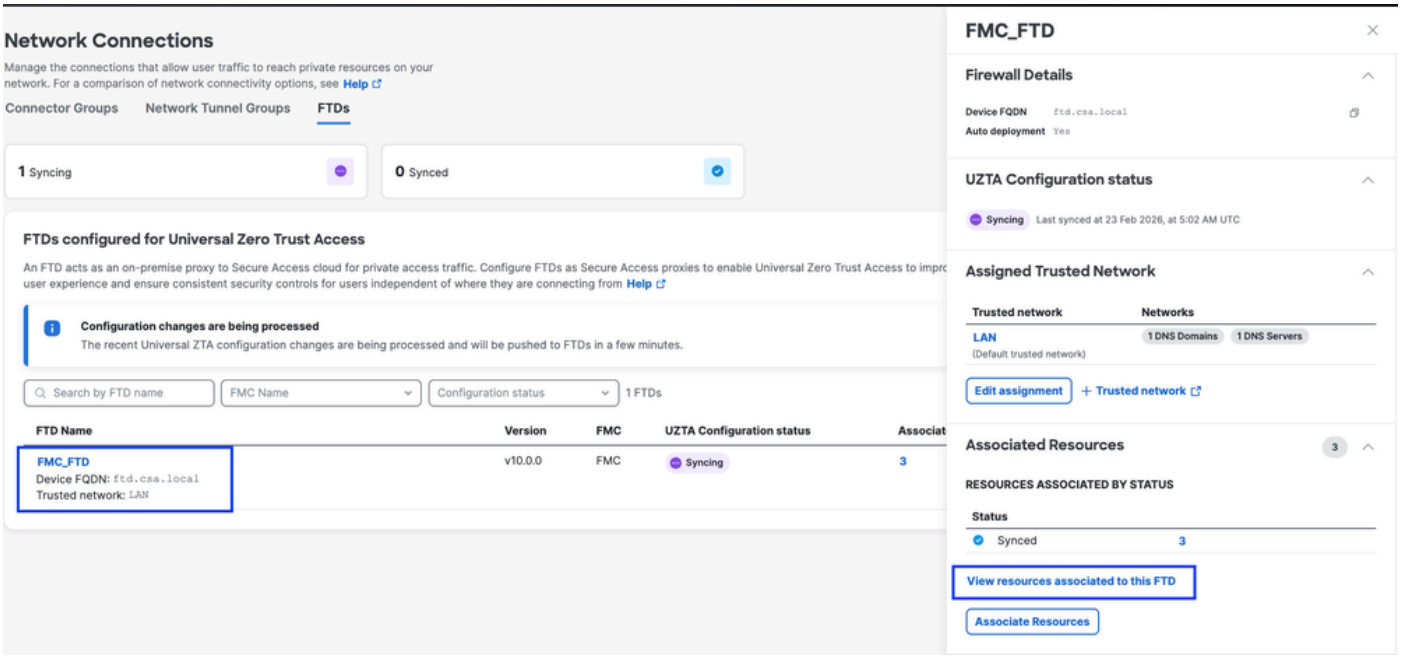


安全訪問 — PR驗證

2. 按一下FTD >檢視與此FTD相關聯的資源

```
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
```

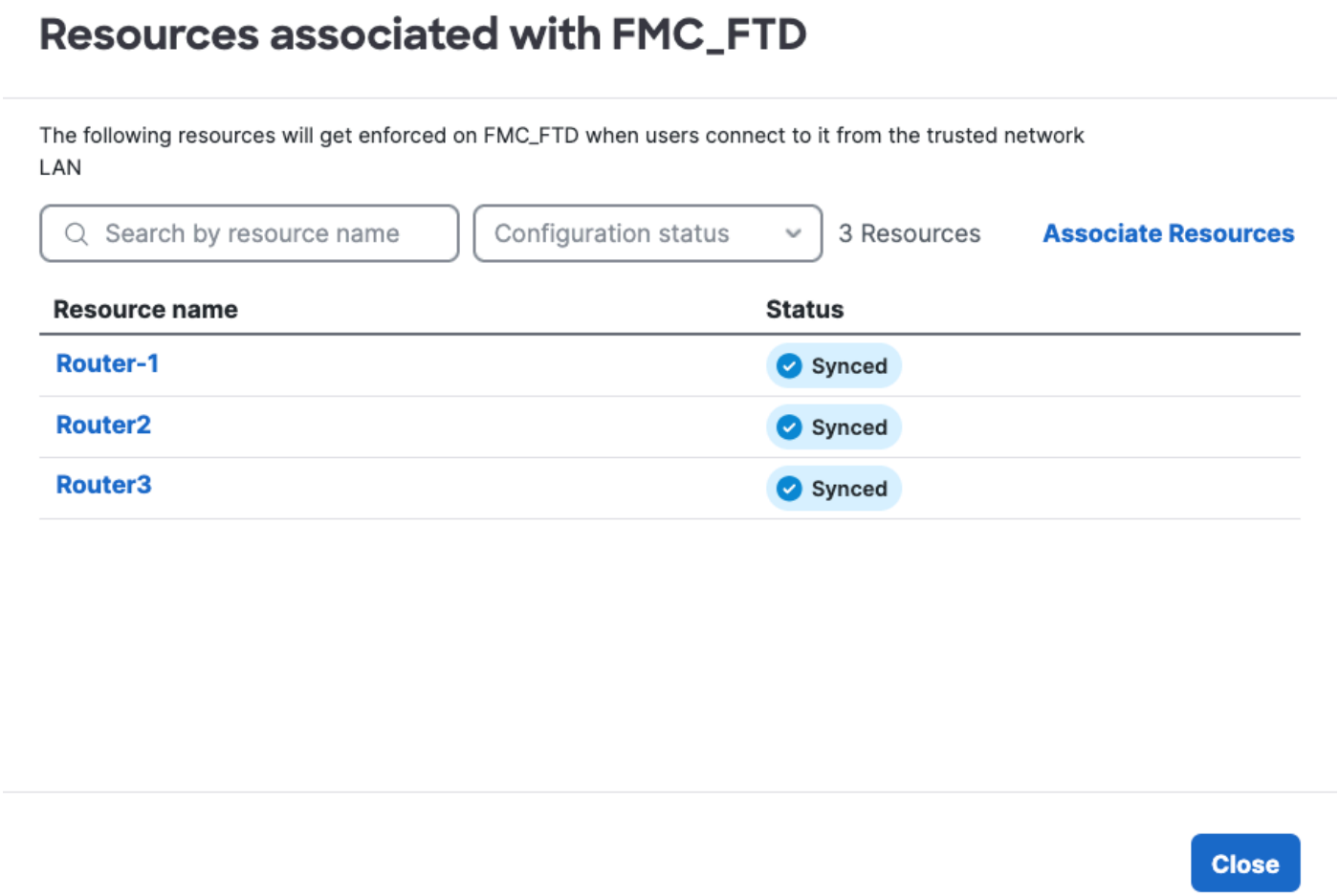
安全訪問 — PR驗證



安全訪問 — PR驗證

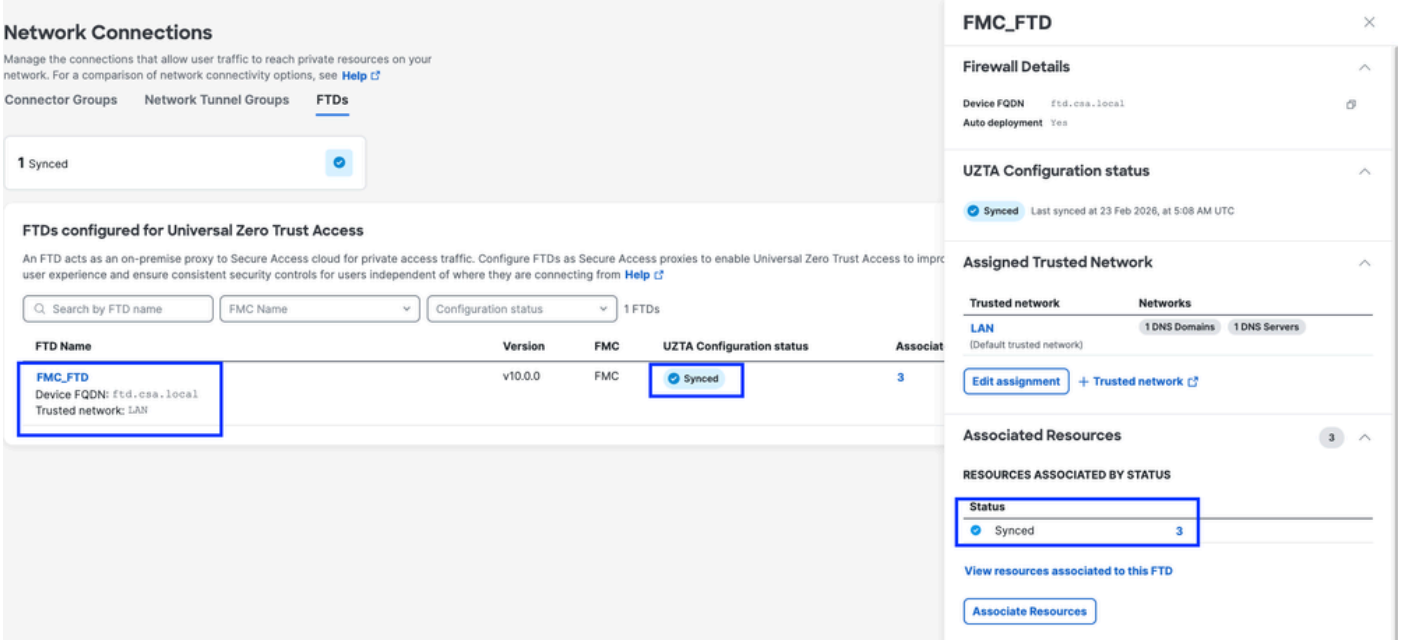
```
C:\Users\jay>ping ftd.csa.local

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
```

安全訪問 — PR驗證



3. 按一下「close」

4.驗證狀態、關聯的資源和配置是否應該處於「已同步」狀態



安全訪問 — PR驗證

5.驗證組態是否已推送到FTD

登入FTD CLI並導覽至LINA模式

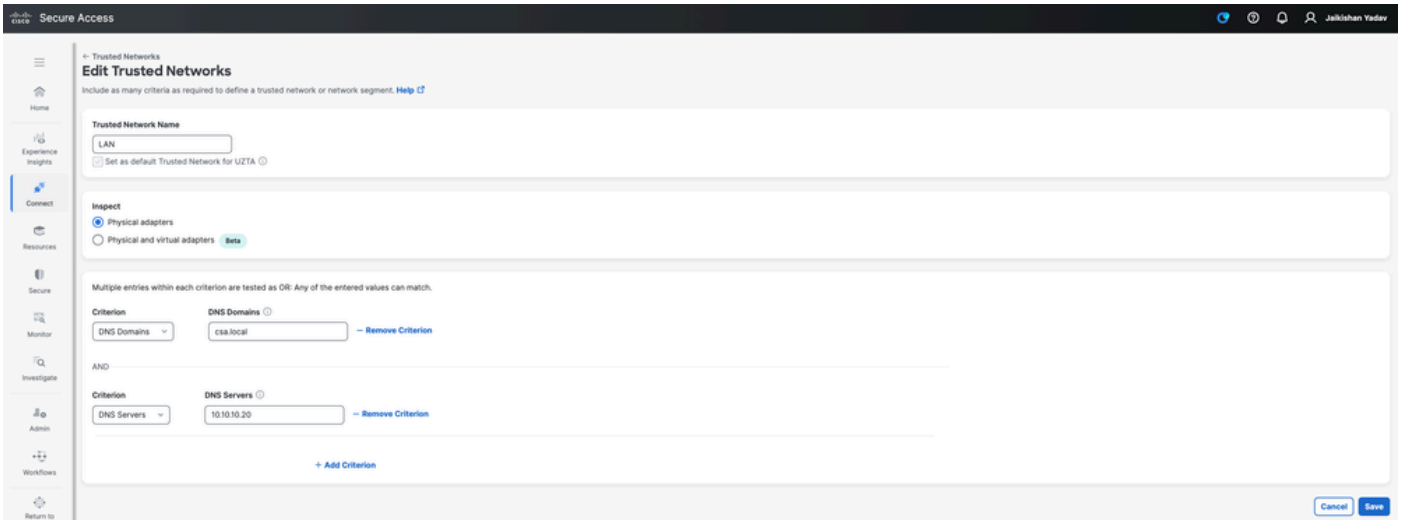
show running-config object application

```
ftd# sh run object application
object application PR_Router2
 id 443200
 internal domain router2.csa.local tcp eq 22
 internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
 external domain router2.csa.local
 external subnet 10.10.10.102 255.255.255.255
object application PR_Router-1
 id 438025
 internal domain router1.csa.local tcp range 1 65535
 internal subnet 10.10.10.101 255.255.255.255 tcp range 1 65535
 external domain router1.csa.local
 external subnet 10.10.10.101 255.255.255.255
object application PR_Router3
 id 468677
 internal domain router3.csa.local tcp eq 22
 internal subnet 192.168.1.103 255.255.255.255 tcp eq 22
 internal subnet 10.10.10.103 255.255.255.255 tcp eq 22
 external domain router3.csa.local
 external subnet 10.10.10.103 255.255.255.255
 external subnet 192.168.1.103 255.255.255.255
```

安全訪問 — PR驗證

步驟 — 4 配置或驗證「管理受信任網路或ZTA設定」

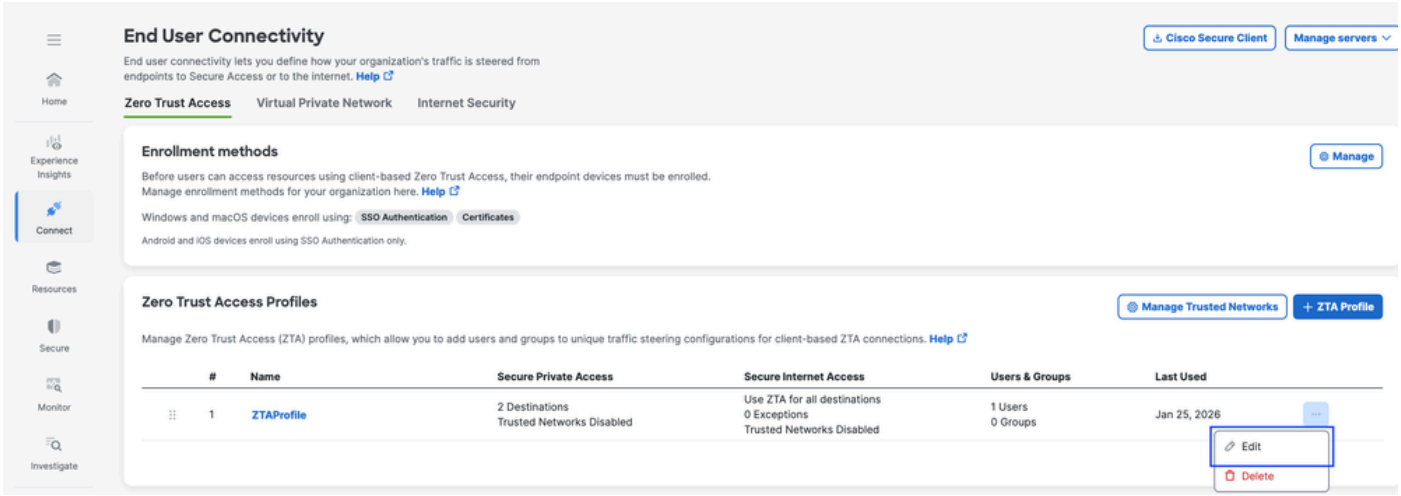
導航到Connect > End User Connectivity > Zero Trust Access > ZTA Settings並配置受信任網路



安全訪問 — ZTA TND配置

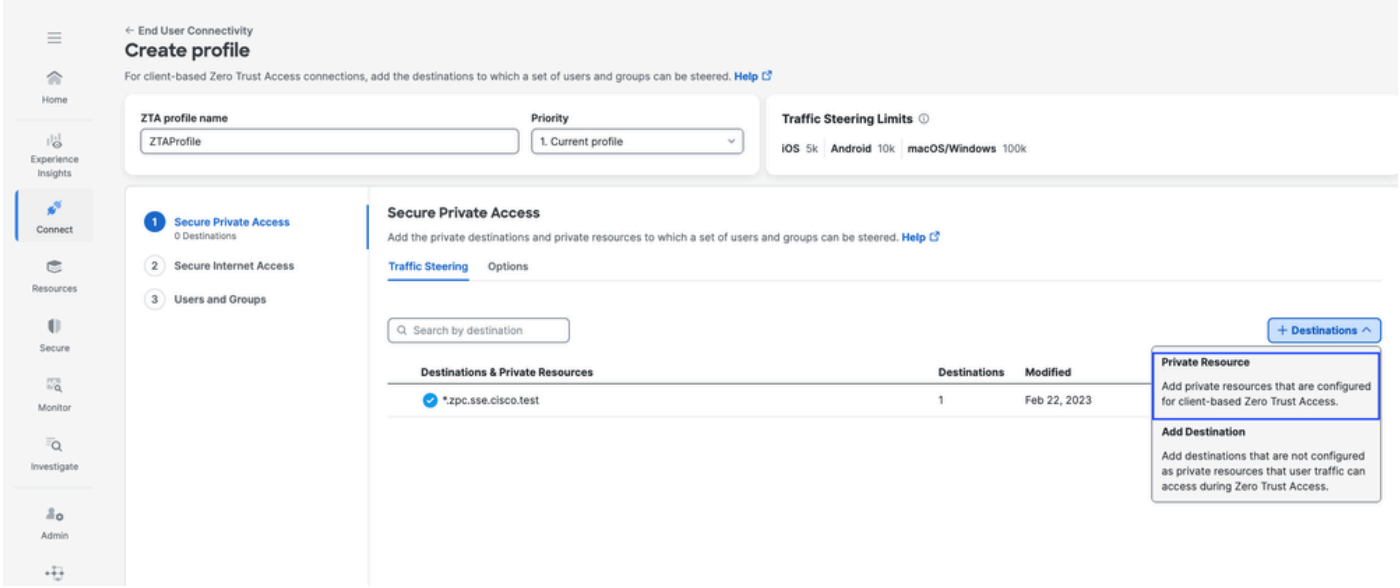
第5步向ZTA配置檔案中新增專用資源

1.導航至Connect > End User Connectivity > Zero Trust Access，然後按一下3個點以編輯ZTA配置檔案

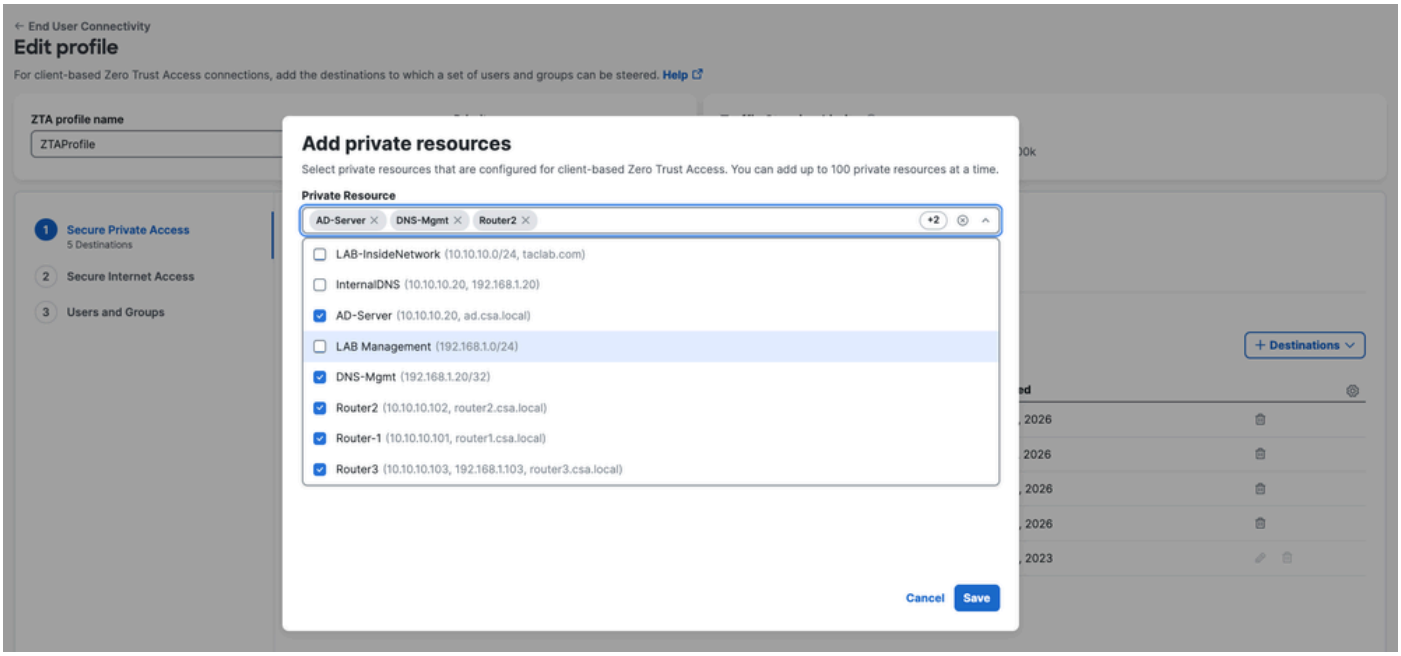


安全訪問 — ZTA配置檔案

2.新增專用資源

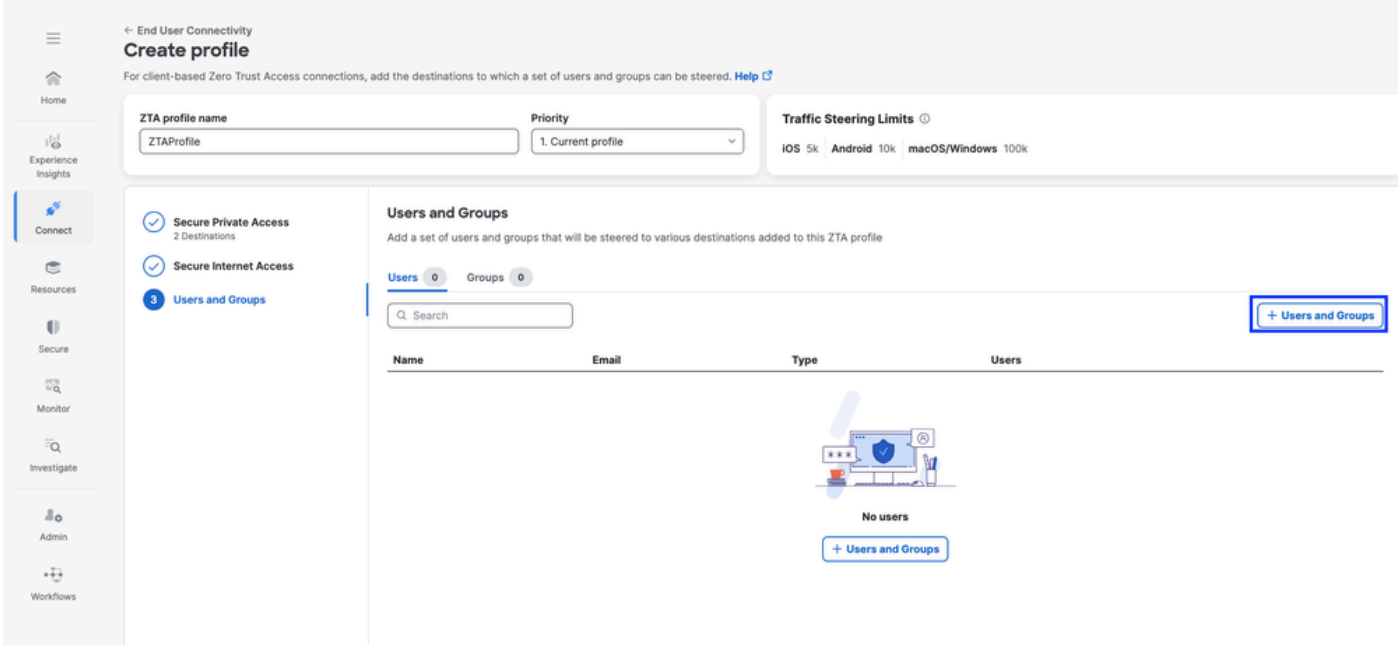


安全訪問 — ZTA配置檔案

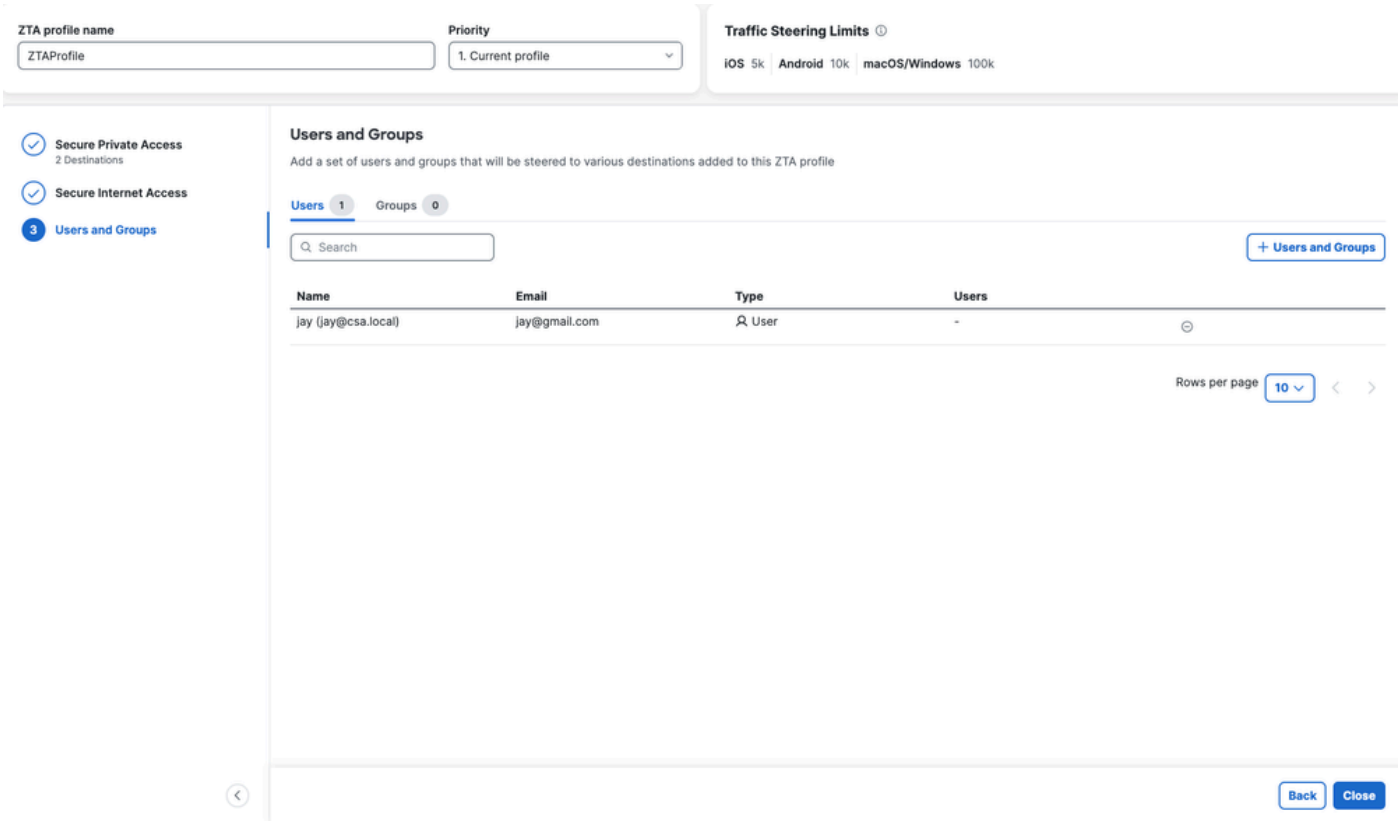


安全訪問 — ZTA配置檔案

3.新增使用者和組



安全訪問 — ZTA配置檔案

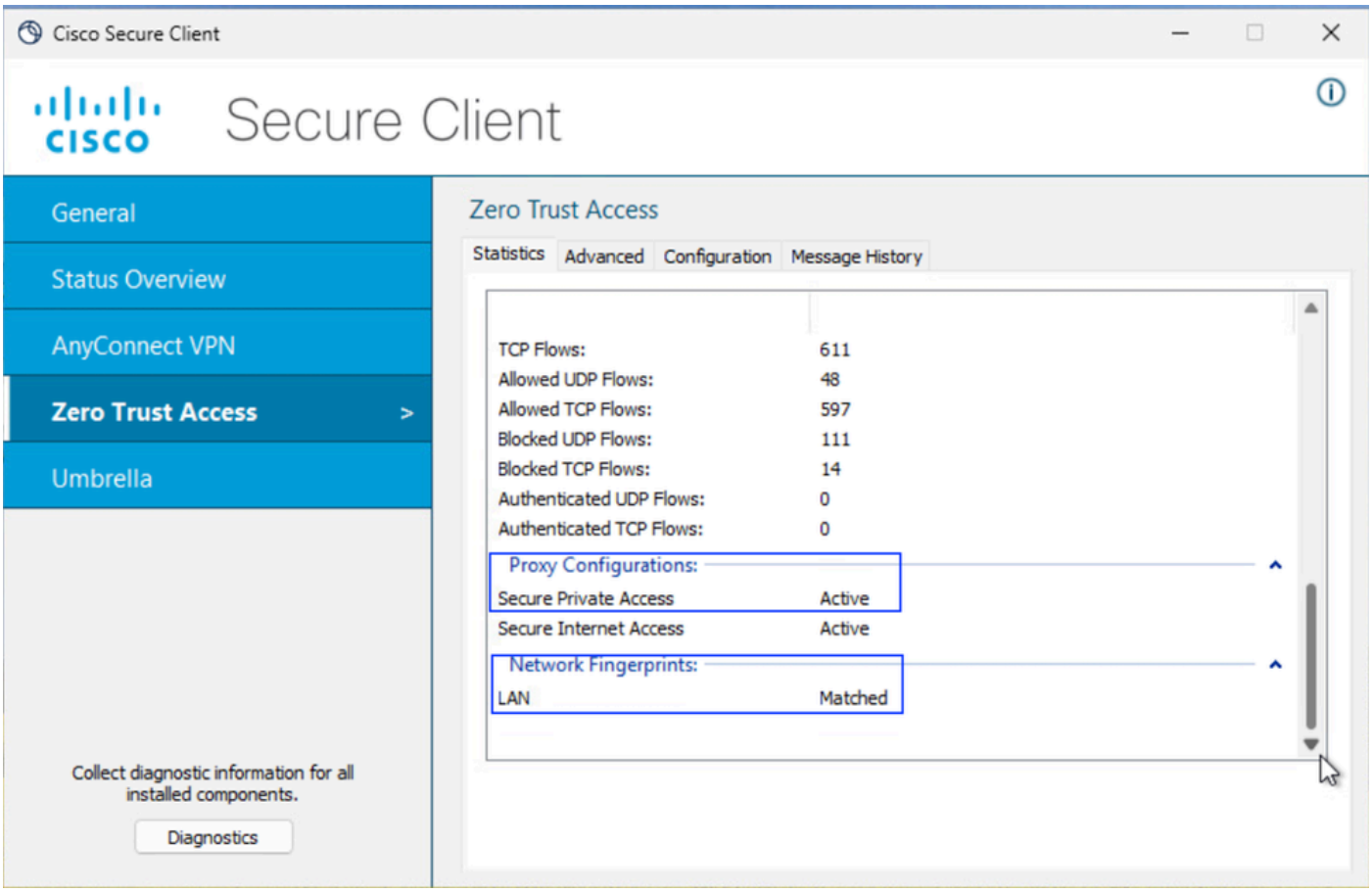


安全訪問 — ZTA配置檔案

步驟 — 6驗證對專用資源的訪問

使用者是本地使用者時

1.驗證ZTA TND的網路指紋，如果使用者為本地且安全專用訪問應處於活動狀態，則該指紋應匹配



安全訪問 — PR測試

2. 驗證遠端使用者是否可解析FTD FQDN

```
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
```

安全訪問 — PR測試

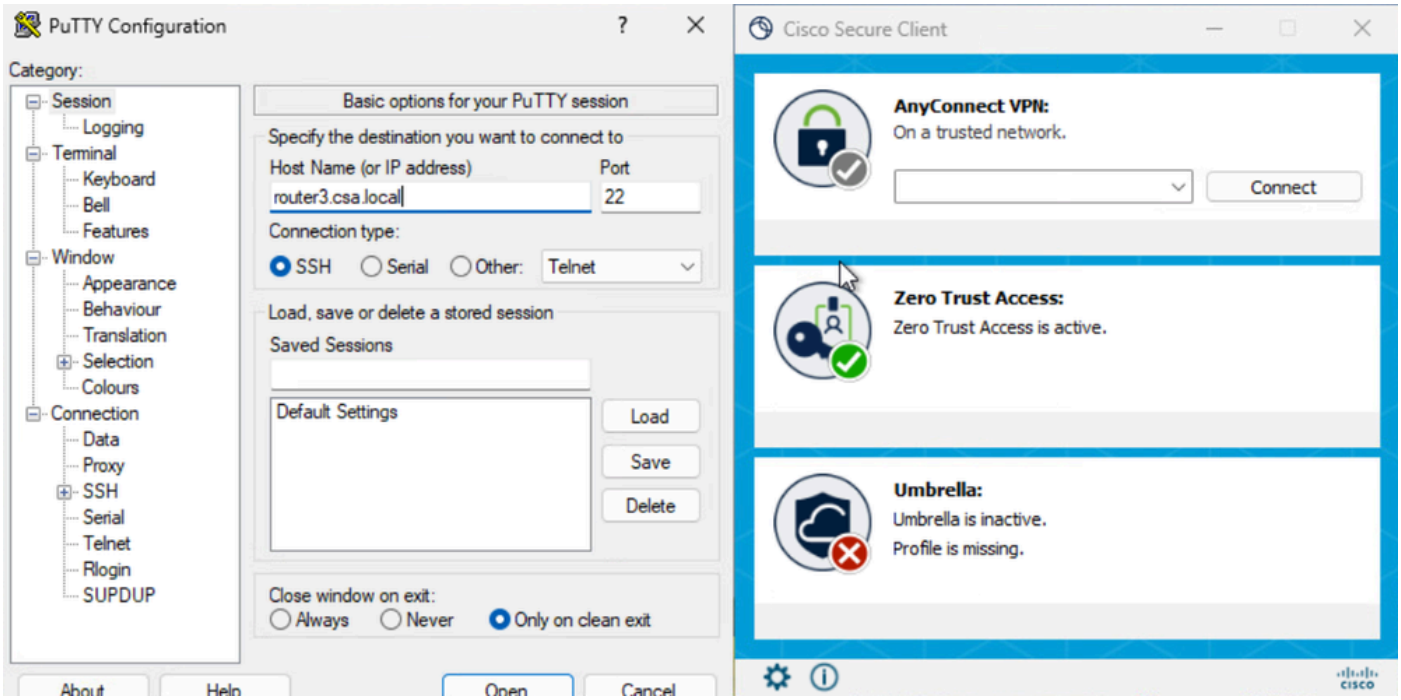
3.驗證FTD是否可以使用FQDN訪問私有資源

```
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#
```

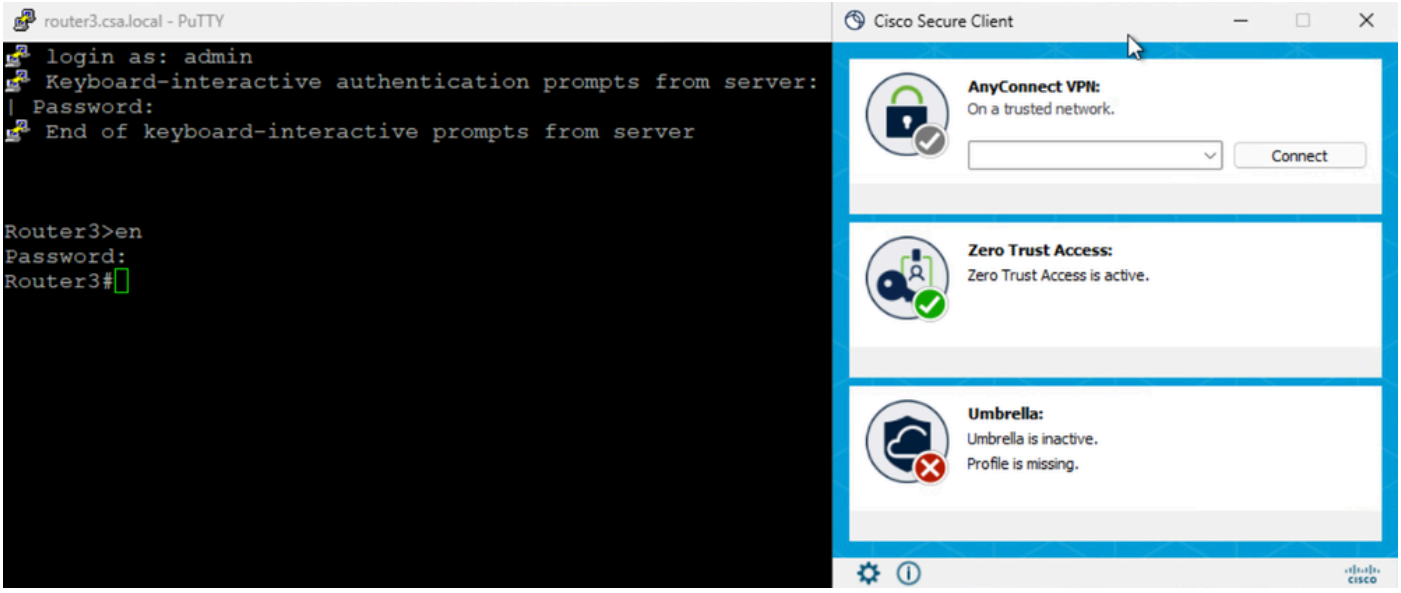
安全訪問 — PR測試

4. 測試到專用資源的SSH連線

使用FQDN訪問PR

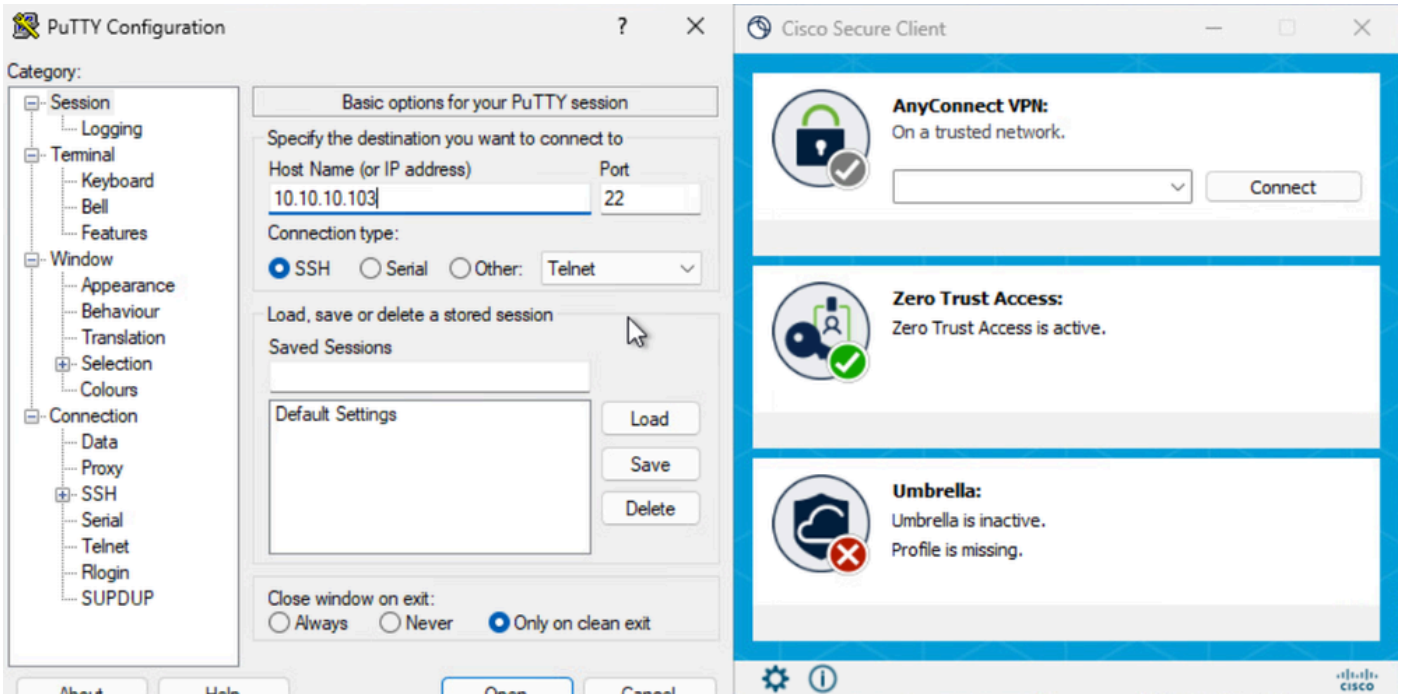


安全訪問 — PR測試

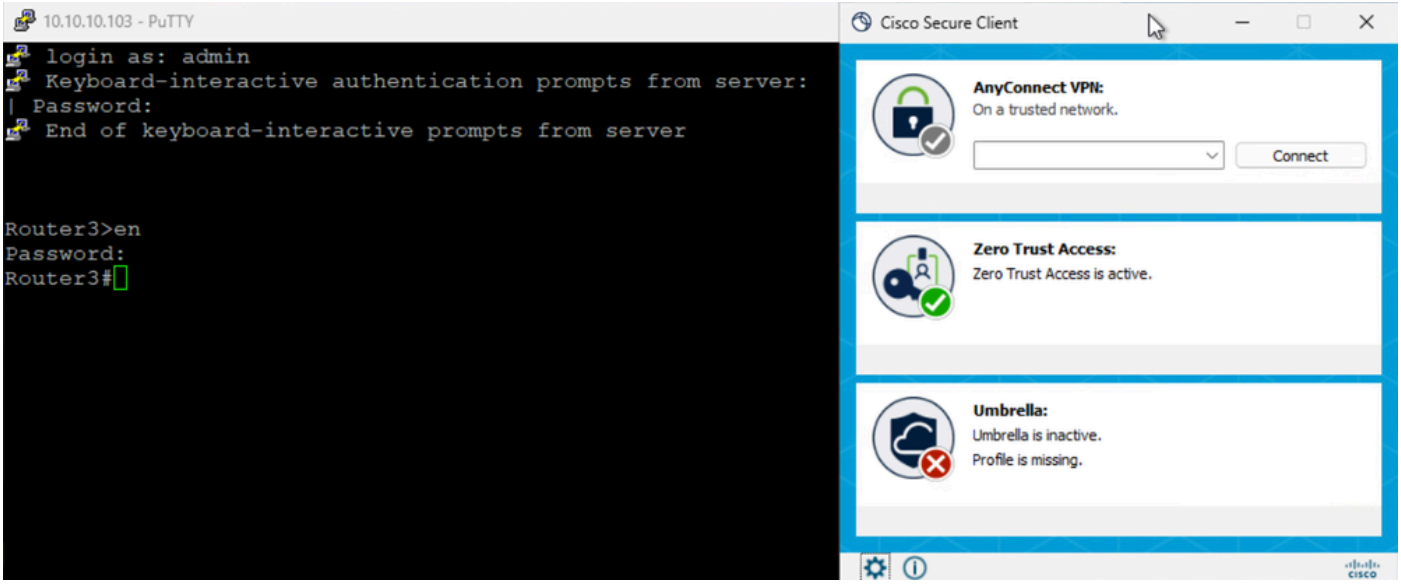


安全訪問 — PR測試

使用IP地址訪問PR

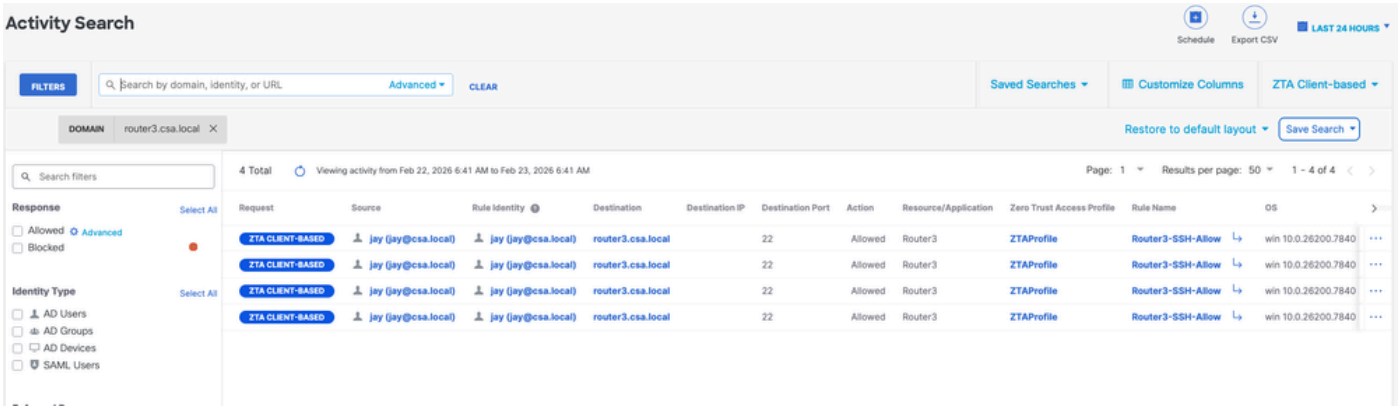


安全訪問 — PR測試

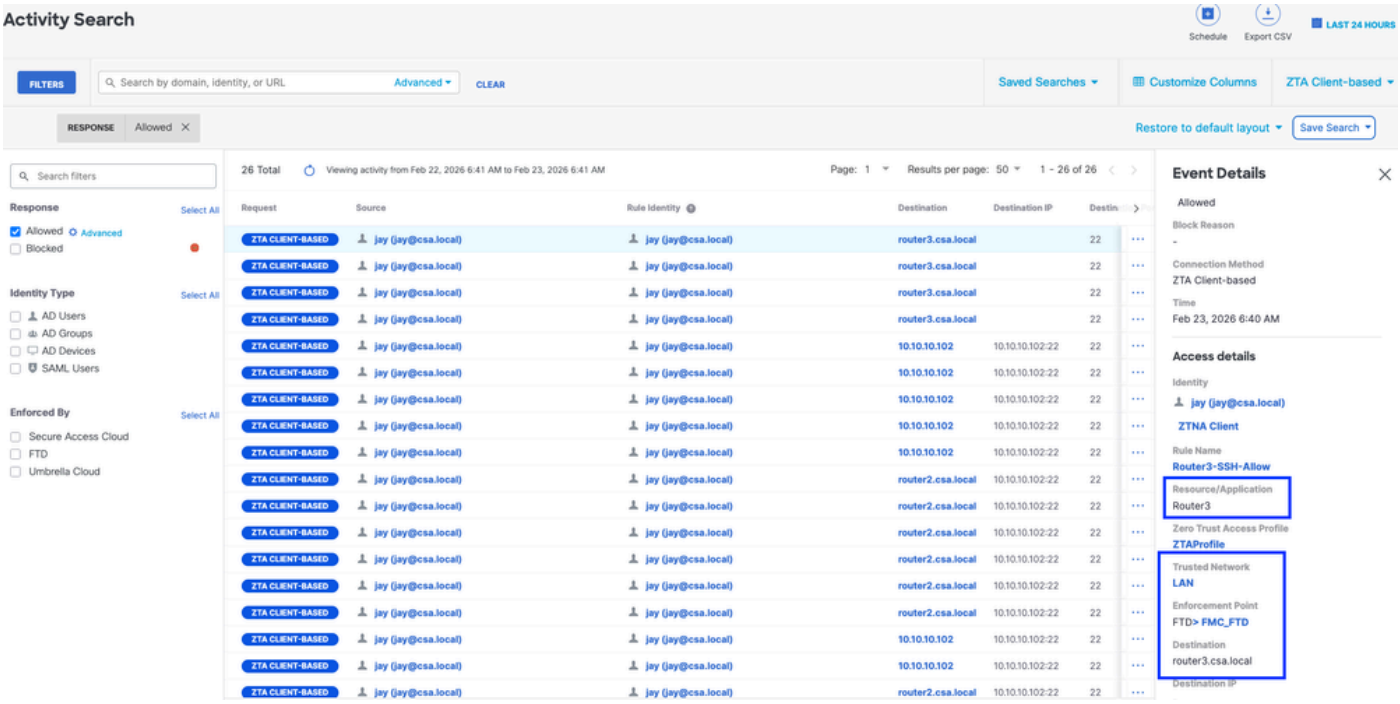


安全訪問 — PR測試

5. 驗證安全訪問活動搜尋日誌

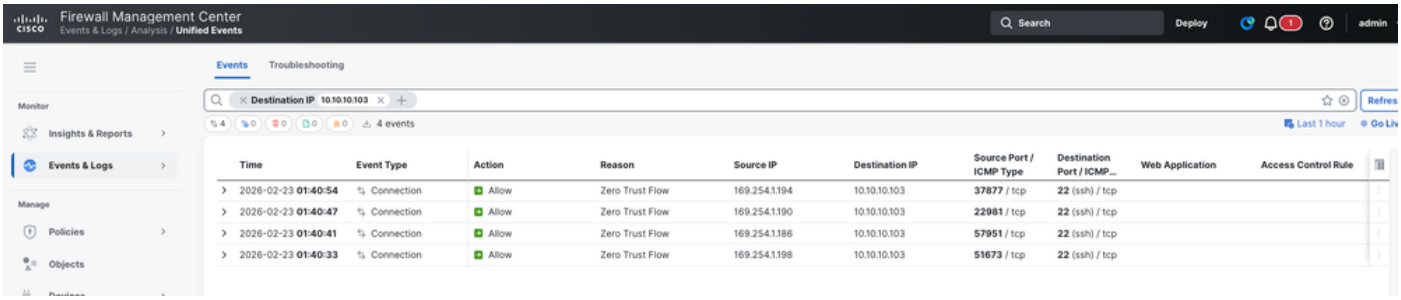


安全訪問 — 活動搜尋



安全訪問 — 活動搜尋

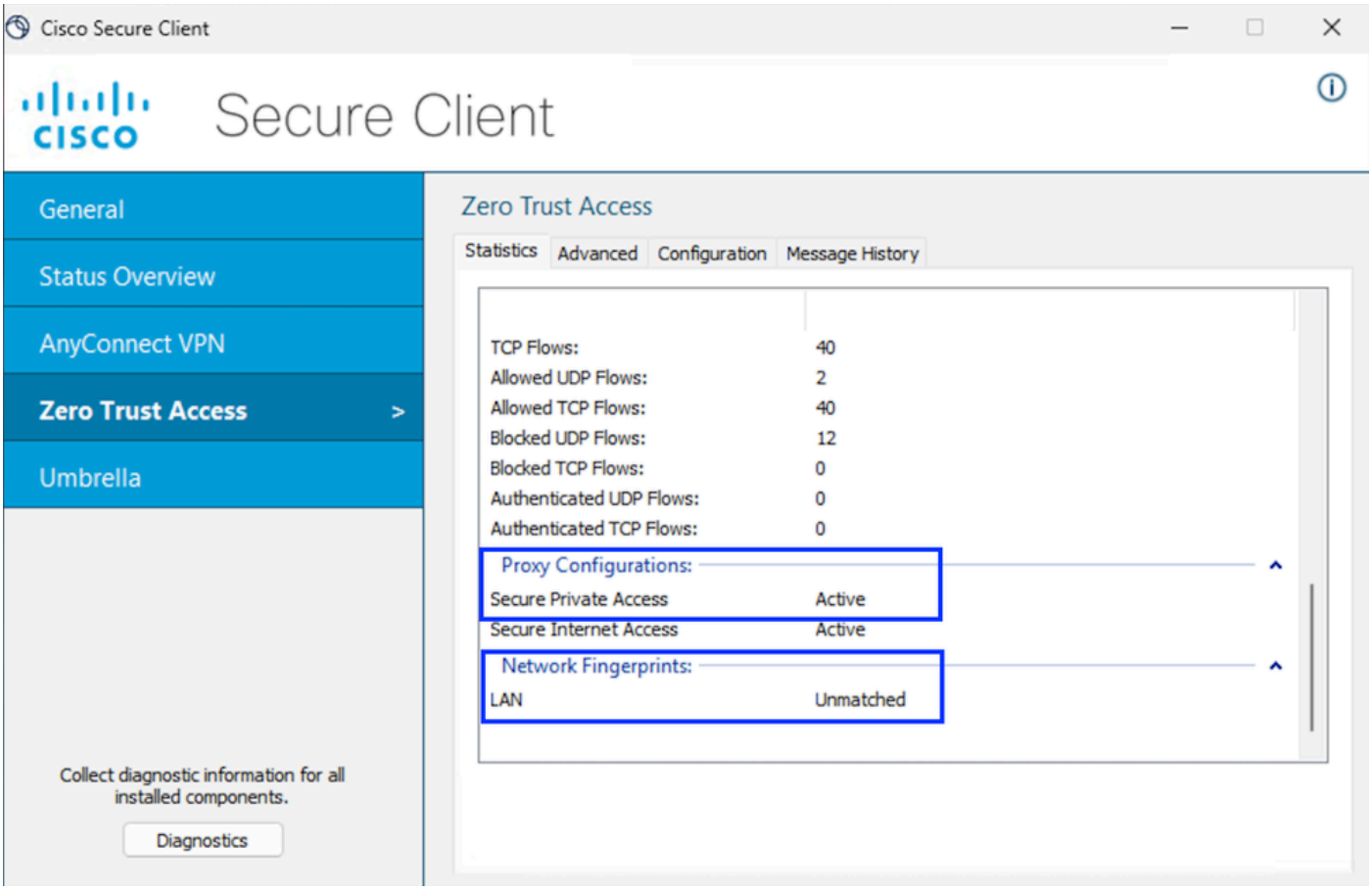
6. 驗證FMC連線事件



FMC連線事件

使用者為「遠端」時

1.驗證ZTA TND的網路指紋，如果使用者是遠端使用者，則此指紋應取消匹配



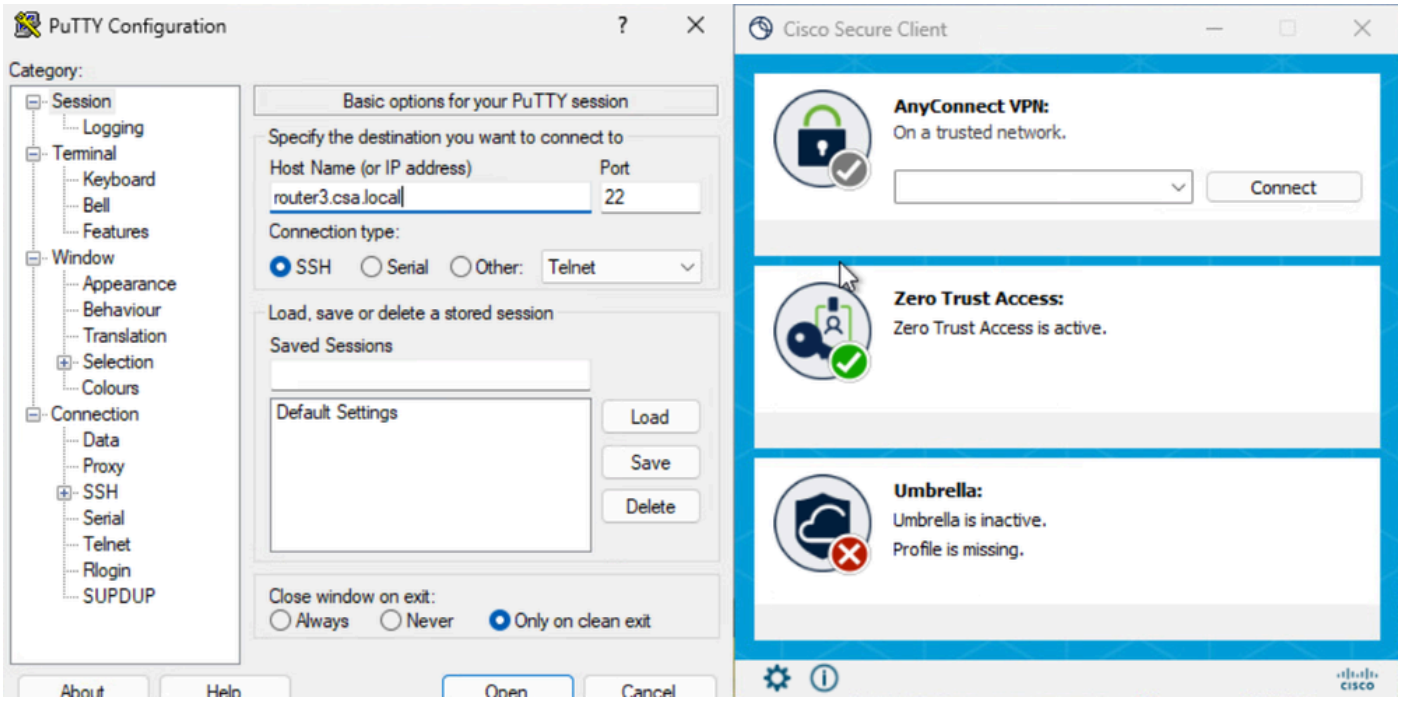
安全訪問 — PR測試

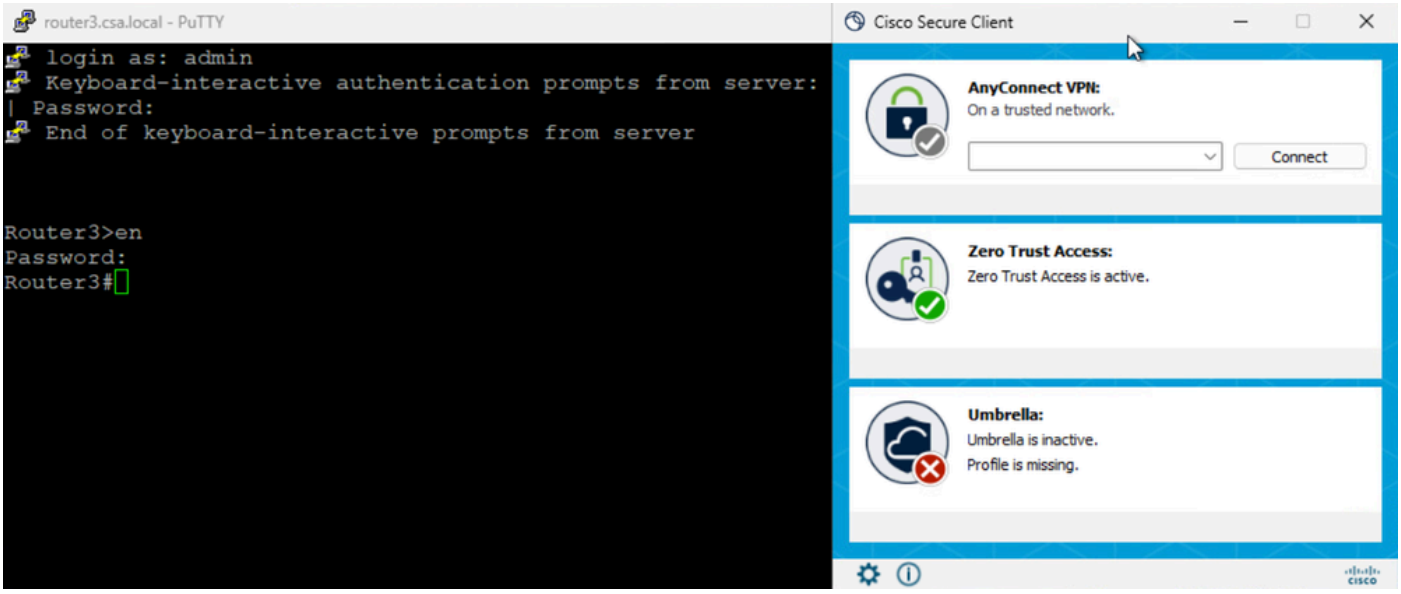
2. 驗證遠端使用者是否可解析FTD FQDN

```
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. 測試到專用資源的SSH連線

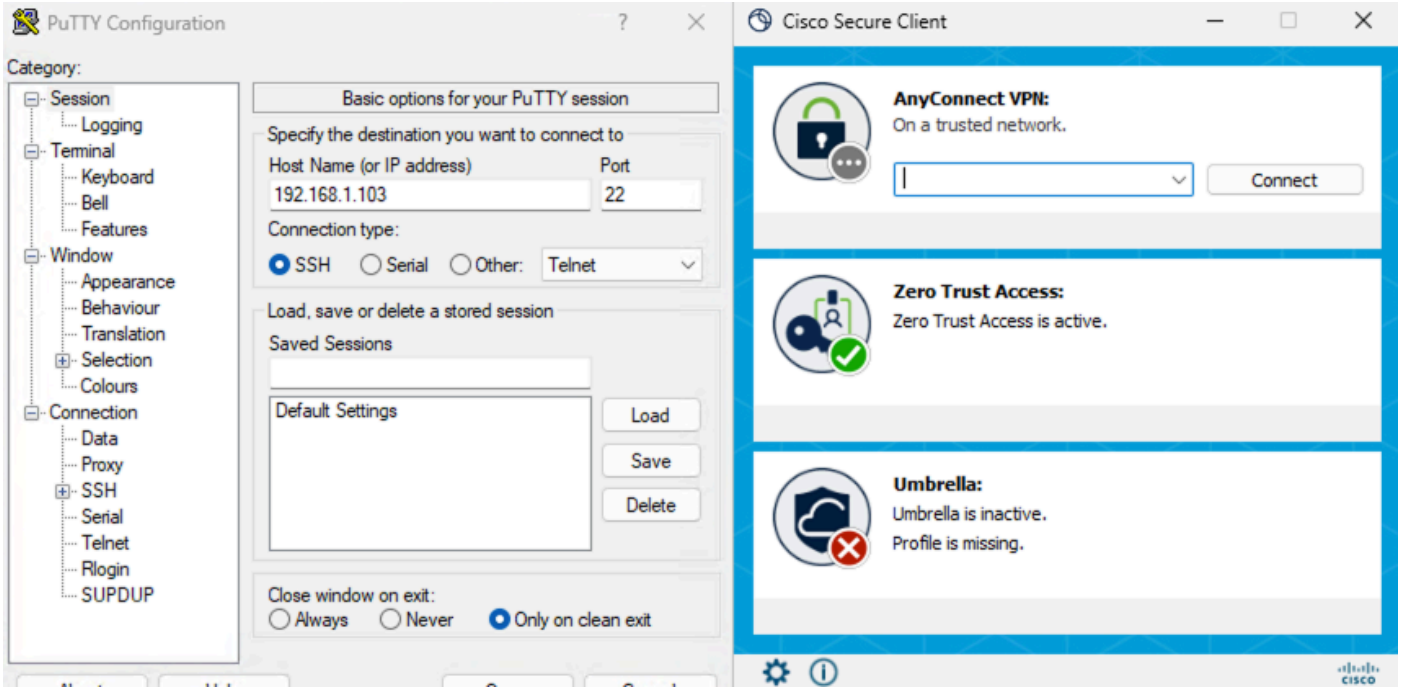
使用FQDN訪問PR



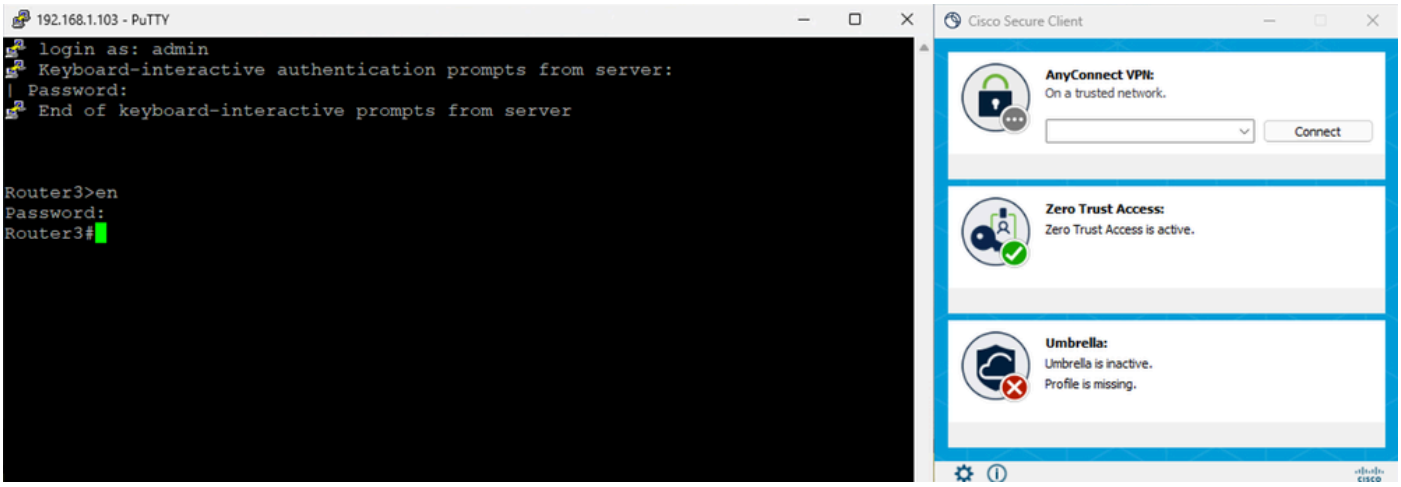


安全訪問 — PR測試

使用IP地址訪問PR

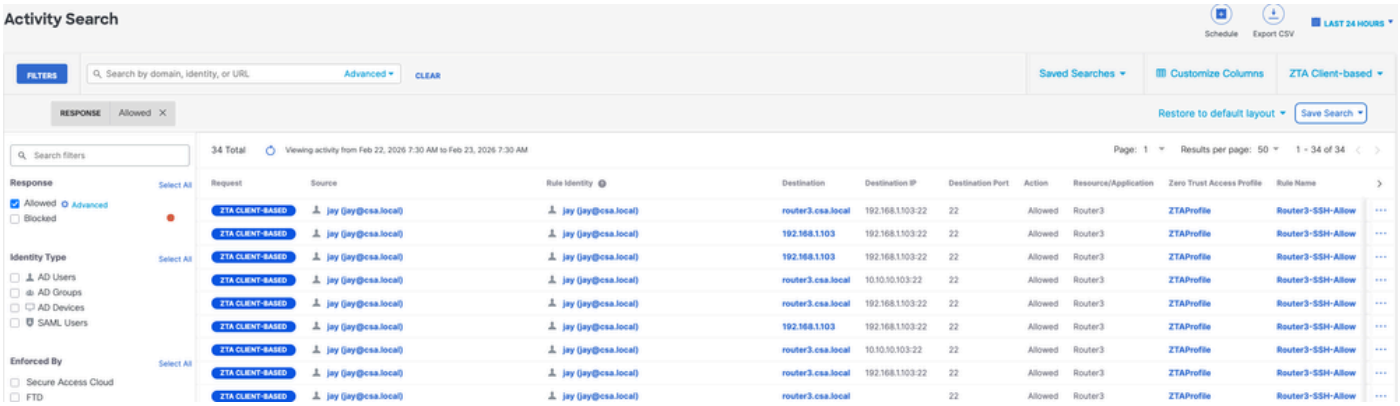


安全訪問 — PR測試

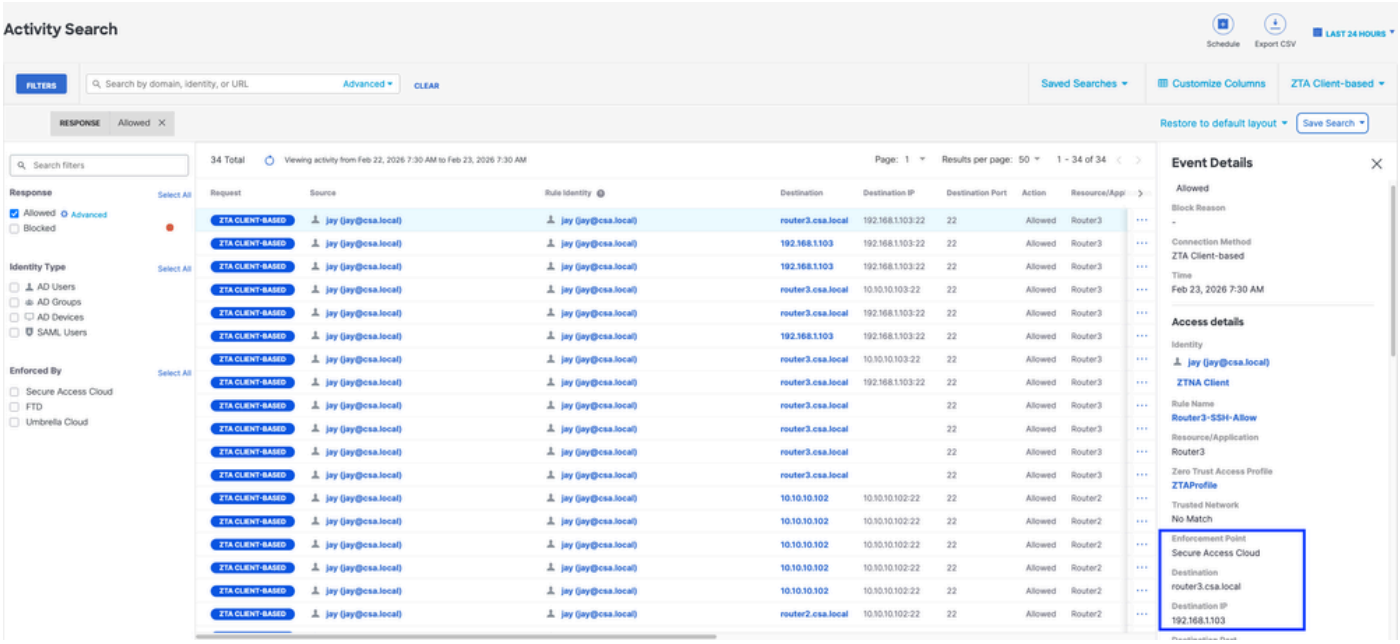


安全訪問 — PR測試

5. 驗證安全訪問活動搜尋日誌



安全訪問 — 活動搜尋



疑難排解

有用的命令：

> 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

!然後進入專家模式

tail -f /ngfw/var/log/messages

show conn all

show nat detail

show asp table socket

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。