在安全访问中配置用于私有资源访问的通用ZTNA

目录

简介

在本文档中，我们将介绍通过通用ZTNA使用不同流量路径进行私有资源访问的配置。

先决条件

以下配置必须在通用ZTNA配置之前完成

- 思科安全访问上的身份提供程序
- 使用证书以零信任访问注册设备
- 使用思科安全防火墙配置隧道
- 远程访问虚拟专用网络
- 安全访问上的资源连接器
- 安全云控制的FTD自注册

- 应该为各自的安全访问租户启用混合ZTNA功能标志，请联系思科TAC以启用该标志

要求

Cisco 建议您了解以下主题：

- 思科安全访问和防火墙威胁防御上的IPsec VPN配置
- 身份提供(IdP) — 从Active Directory进行用户调配
- 思科安全访问上的远程VPN配置
- 思科安全访问上的资源连接器部署
- 基于ZTA证书的注册
- 证书 — OpenSSL、CSR生成、证书模板等

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全防火墙威胁防御（版本7.7.10）
- 思科安全Firepower管理中心（版本7.7.10）
- 思科安全客户端（ZTA版本5.1.10.1720）
- Windows 11
- Windows 2019服务器 — 证书颁发机构
- ESXi上的资源连接器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

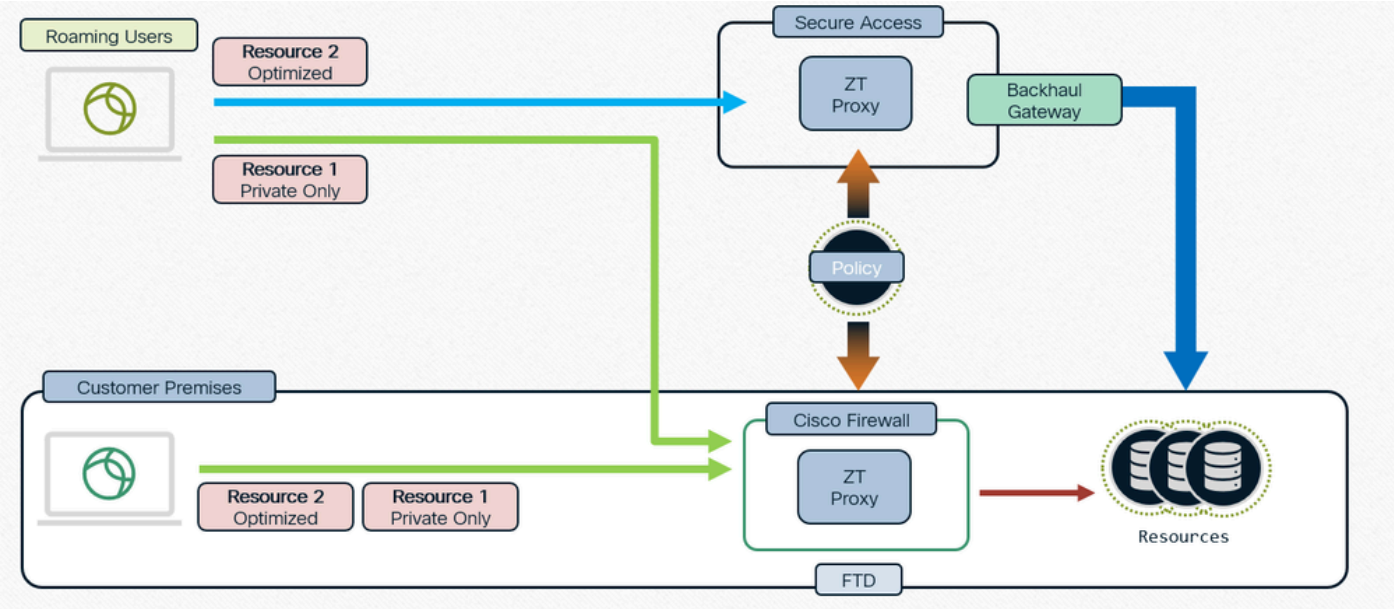
关于通用ZTNA

通用零信任网络访问(uZTNA)使管理员能够根据用户身份（包括用户信任和安全状态）专门允许访问内部网络资源，而不像RA-VPN那样授予对整个网络的访问权限。uZTNA使管理员能够保护远程和本地用户的内部资源和应用程序。

由于uZTNA不假设授予一个应用的访问隐式地授权对其他应用的访问，因此网络攻击面得以减少。

安全访问评估访问策略。将忽略从安全防火墙管理中心部署到设备的所有访问控制策略。

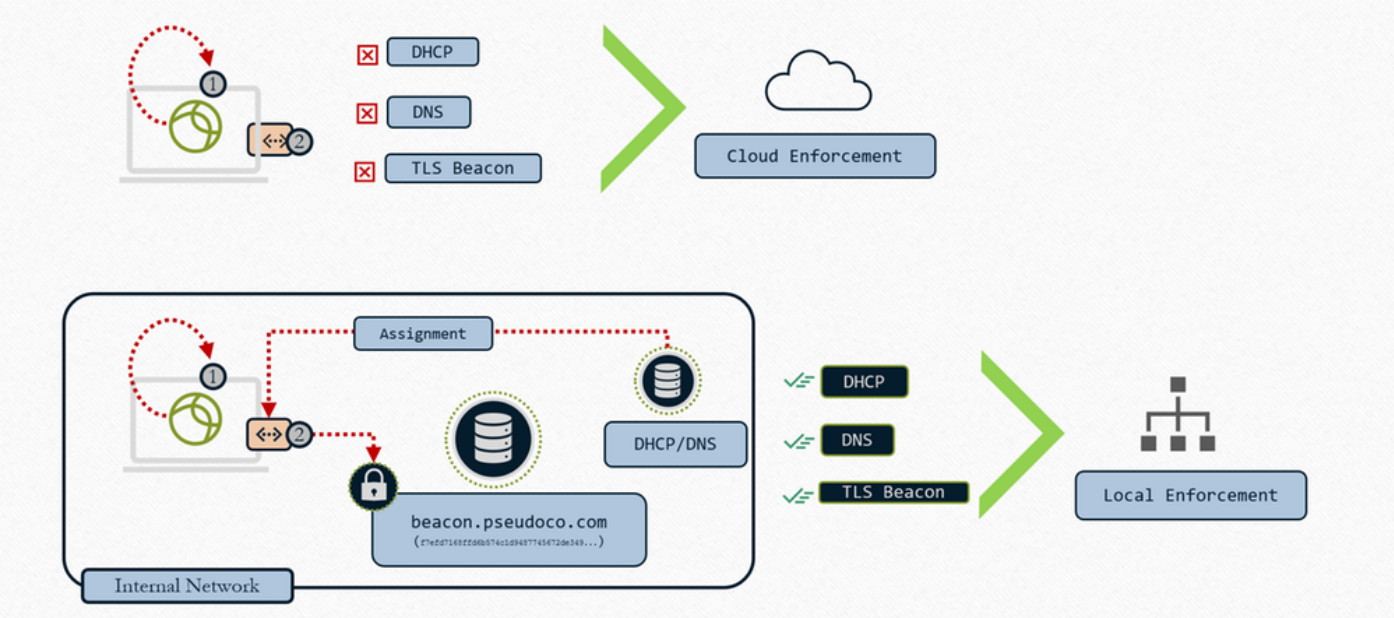
流量代理以及IPS、文件和恶意软件策略实施在Firepower威胁防御(FTD)上执行。



单一策略，分布式实施

网络检测

确定云或本地实施



通用ZTNA — 确定云或本地实施

1 — 客户端查询本地接口以进行网络配置

2 — 客户端搜索TLS信标

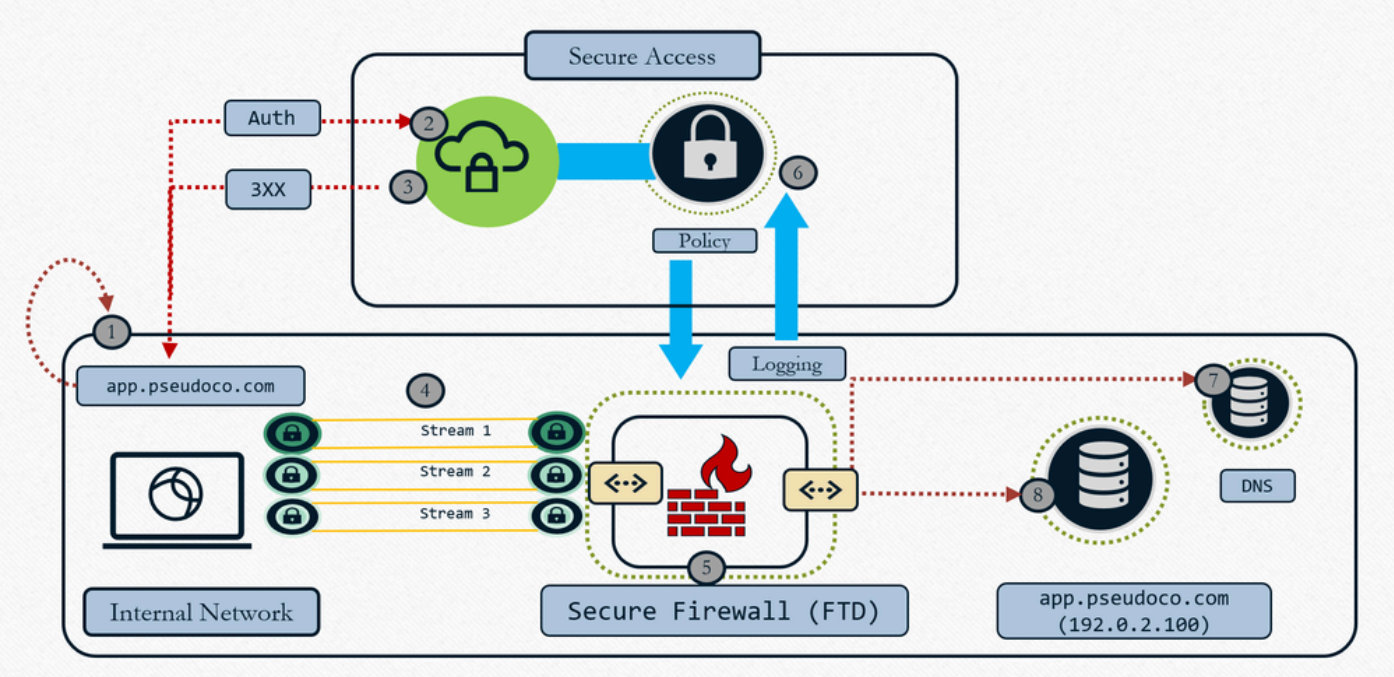
3 — 如果条件匹配 — 本地实施

4 — 如果条件不匹配 — 云实施

当我们使用“Cloud or Local Enforcement”配置资源并将TND规则与FTD关联时，它实际执行的操作是发送到客户端的一组拦截规则将包括TND规则评估。因此，云将通知客户端评估TND规则。在发送连接时，我们将网络指纹评估结果放入HTTP报头中，这样会告诉代理是处于正常状态还是处于不可信网络，然后代理会使用该信息并相应地重定向流量。如果指纹匹配，Zproxy会告知客户端将流量重定向至FTD，如果指纹不匹配，则会将流量重定向至云。请参阅使用受信任网络检测配置零信任网络访问

实施类型

- 本地实施路径：防火墙实施

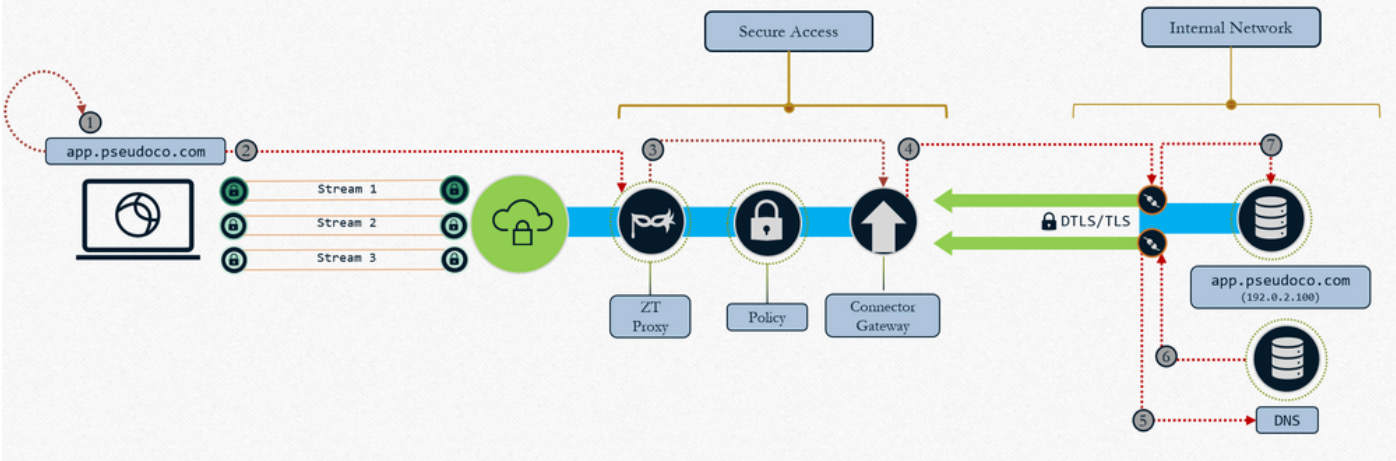


通用ZTNA — 本地实施

1. 用户请求应用、客户端捕获请求并将其解析为短暂IP（本地主机范围）
2. 身份验证控制流量发送到安全访问云进行策略评估
3. 云返回重定向至FTD以执行数据计划（如果策略允许）

4. 流向防火墙配置的头端（接口）的流量
5. 使用本地代理数据平面实施云中定义的策略（IPS、恶意软件、解密）
6. 事件已记录和复制已发送到云以实现一致报告
7. 防火墙在本地网络上执行DNS解析以路由资源流量（如果允许）
8. 防火墙建立与资源的连接（与资源建立的新连接），因为防火墙充当TCP代理

- 云实施路径：关闭网络

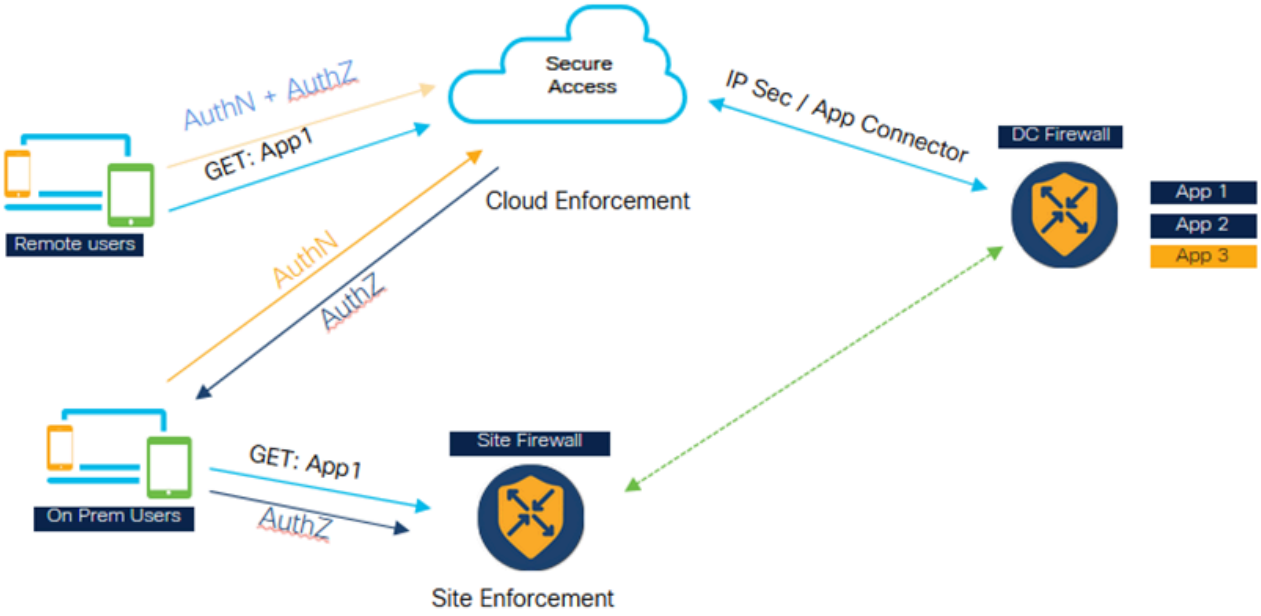


通用ZTNA:云实施

1. 用户请求应用、客户端捕获请求并将其解析为短暂IP（本地主机范围）
2. 流量在安全访问中传输到零信任代理
3. TCP连接被代理并构建到映射资源连接器，策略在流量上实施
4. 网关建立到资源连接器的连接
5. 资源连接器解析资源IP
6. 本地DNS使用资源IP进行响应
7. 资源连接器建立与资源的连接

使用案例

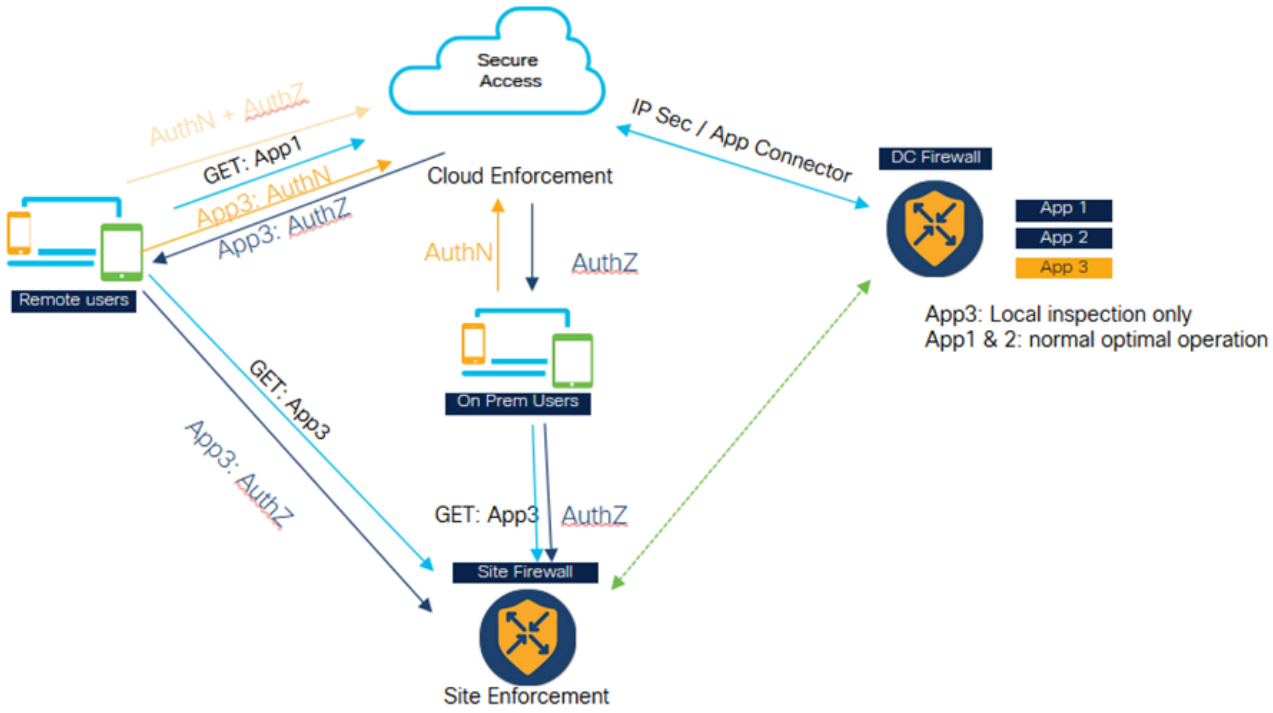
案例1：在内部部署时为用户提供一致且优化的ZTNA



通用ZTNA — 一致和优化的ZTNA（内部用户）

- 安全访问和防火墙均配置为保护应用。
- 如果用户是远程用户，则他们将转至Secure Access进行策略评估和检查。
- 如果用户为内部/内部用户，则他们将访问防火墙进行专用流量检测。
- 本地用户仍然可以转至Secure进行身份验证和评估，只有数据路径流量进入防火墙并根据策略配置进行检查。
- 通过防火墙访问应用的内部用户具有性能优势，因为它可避免流量进入云然后回传到数据中心

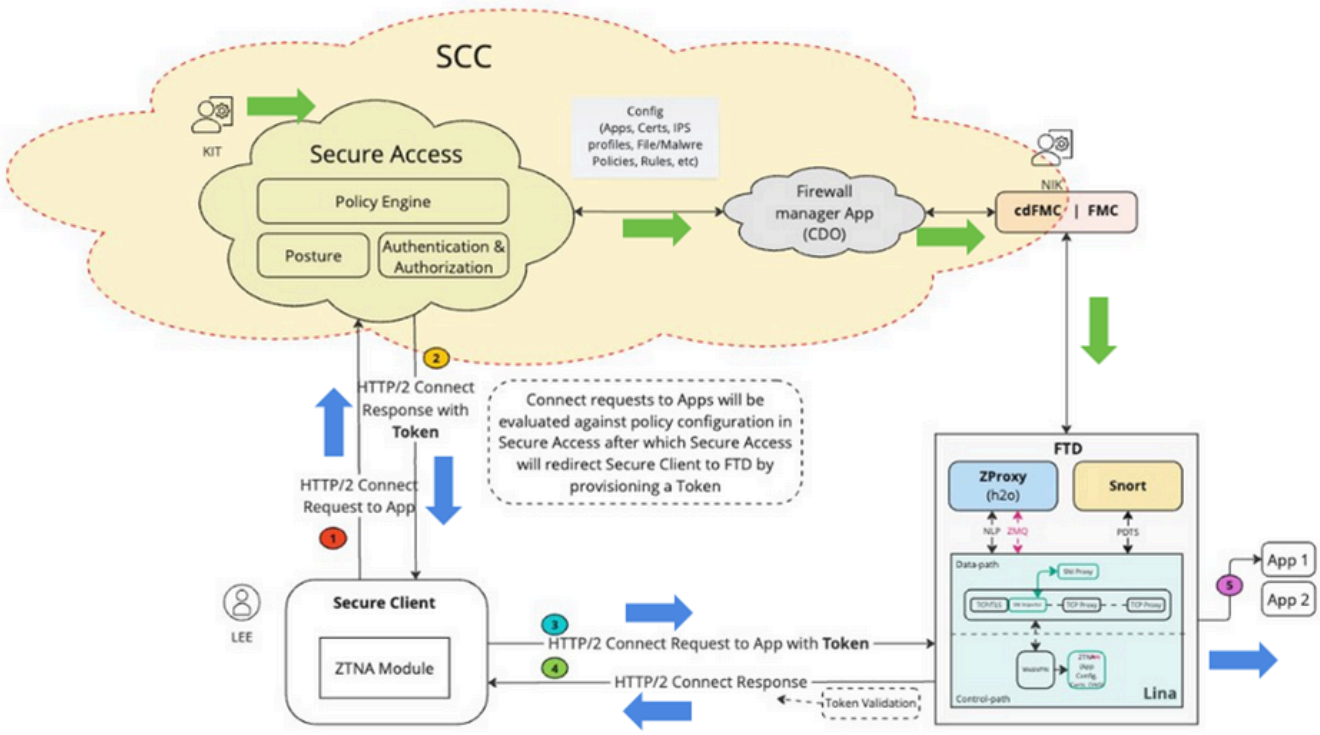
案例2：敏感应用的专用检测



通用ZTNA — 敏感应用的专用检测

- 某些关键应用可以配置为始终通过防火墙进行访问。
- 应用数据流量无需转至云。例如，可能存在诸如源代码之类的敏感数据应用，客户不希望将其迁移到云。
- 在这种情况下，远程和永久用户流量始终通过防火墙并受到检测。但是，在此场景中，身份验证和策略评估始终在云中进行，只有数据部分流量通过防火墙。

架构组件



通用ZTA — 架构组件

安全云控制(SCC)是uZTNA解决方案的主要管理器。uZTNA是第一个在SCC之上构建的功能。

在SCC中，我们有两个微应用安全访问和防火墙。一旦调配了SCC并启用了所需的功能标志，我们将能够在SCC面板的左侧看到这些微型应用。

安全客户端：在安全客户端中，我们必须启用零信任访问模块(ZTNA)，我们需要注册到ZTNA模块才能访问应用。

防火墙威胁防御:FTD保护这些应用。FTD运行也称为H2O的ZT代理（与在安全访问云中运行的代理相同）

现在，当用户（例如KIT）在Secure Access微应用上配置私有资源和策略时，此配置将被推送到SCC中的防火墙微应用。防火墙应用了解FTD、FTD配置的内部，以及如何在FTD上部署和管理配置。因此，防火墙应用验证此配置，并调用FMC API将配置推送到FMC，然后最终将其部署到FTD上。FTD可以启用自动部署选项，这样管理员（例如Nick）就不必进行手动部署。

1.当用户（例如Lee）尝试访问应用程序时，安全客户端使用mTLS通道连接到安全访问。安全访问使用客户端设备证书对用户进行身份验证。然后评估为该用户和该应用配置的授权、状态和其他策略。

2.安全访问，如果最终发现应用受到防火墙的保护，则生成身份验证令牌，告知防火墙已对其进行

身份验证和授权。身份验证令牌已加密，由安全访问签名

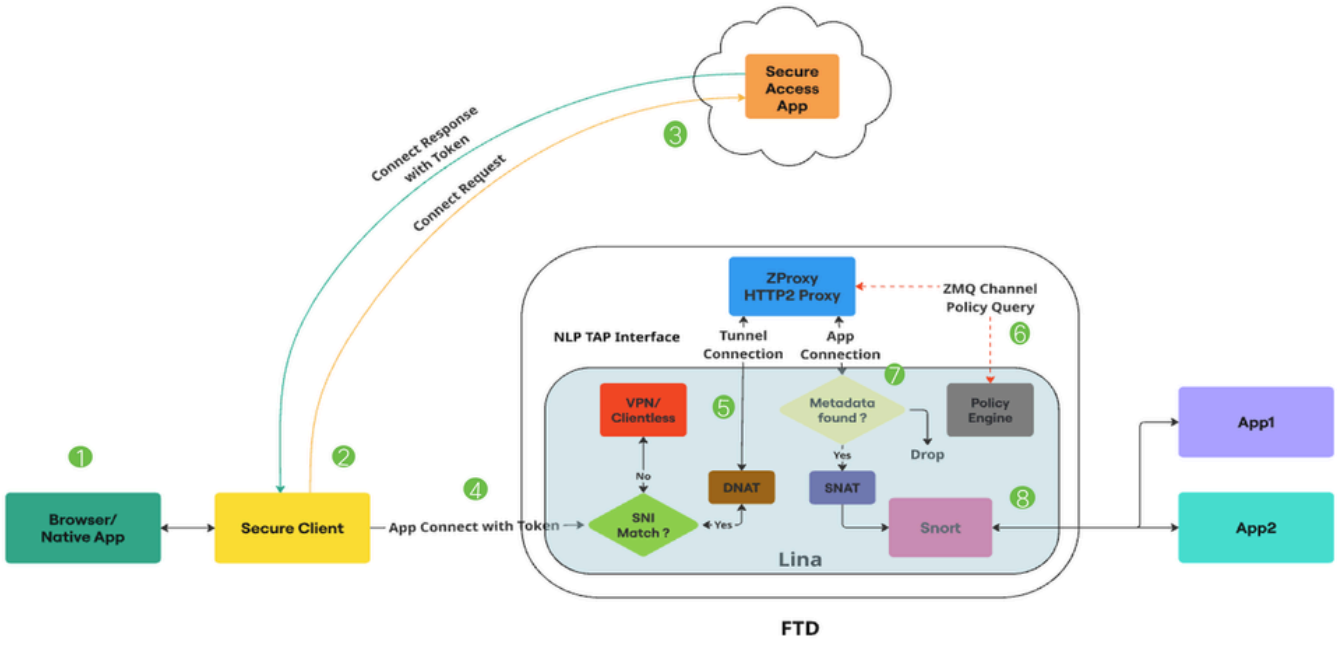
3.安全访问将安全客户端重定向至FTD以及身份验证令牌。

4.安全客户端与FTD建立另一个连接，它是通过mTLS信道的HTTP2连接。它会发送与令牌一起被访问的应用程序的CONNECT请求。

5. FTD现在验证令牌，如果令牌验证成功，则允许用户访问该应用。然后，FTD将确认消息发送回安全客户端

数据包流

通用ZTNA详细数据包流



通用ZTA — 数据包流

1.用户尝试通过Web浏览器或本地应用程序访问应用程序。

2.安全客户端拦截连接，并将其标识为尝试访问私有资源的用户。

3.安全客户端与安全访问建立mTLS连接，请求访问应用。安全访问检查通用ZTNA策略和状态配置文件是否合规。如果一切正常，安全访问将生成包含基本信息（如用户详细信息、应用详细信息和IPS/文件策略）的访问令牌。

4.访问令牌由安全访问加密并签名。然后，安全访问将安全客户端和令牌重定向到FTD。

5.当数据包到达Lina Datapath时，SNI检查器会拦截连接，并验证客户端Hello中的服务器名称（SNI扩展）是否与设备上配置的代理FQDN匹配。如果SNI匹配，则连接将定向到ZProxy。如果SNI不匹配，连接将定向到可与通用ZTNA共存的其他功能。

例如:VPN、强制网络门户或无客户端ZTNA。ZProxy（支持HTTP/2协议的MASQUE）将在FTD上作为专用核心上的非Lina进程运行。Lina和ZProxy之间的通信使用NLP分路接口，用于处理数据流量。连接的目标IP由SNI检查器转换为TAP接口IP。

6.当ZProxy从安全客户端收到mTLS隧道连接时，它会验证安全客户端发送的客户端设备证书。它还验证通过APP Connect发送的访问令牌。Lina和ZProxy之间有一个零MQ通道。它主要用于交换控制消息。ZProxy通过与Lina通信来使用此通道进行私有资源的FQDN解析。

零MQ信道还用于将访问令牌中存在的信息传播给Lina。(示例：规则ID、策略ID等)Lina接收访问令牌信息并将其存储在元数据数据库中。

7.一旦交换了控制消息，ZProxy就会向私有资源发起新的连接。这可以是TCP或UDP。然后，Lina为此应用连接执行元数据数据库查找。如果未找到元数据，则连接被丢弃

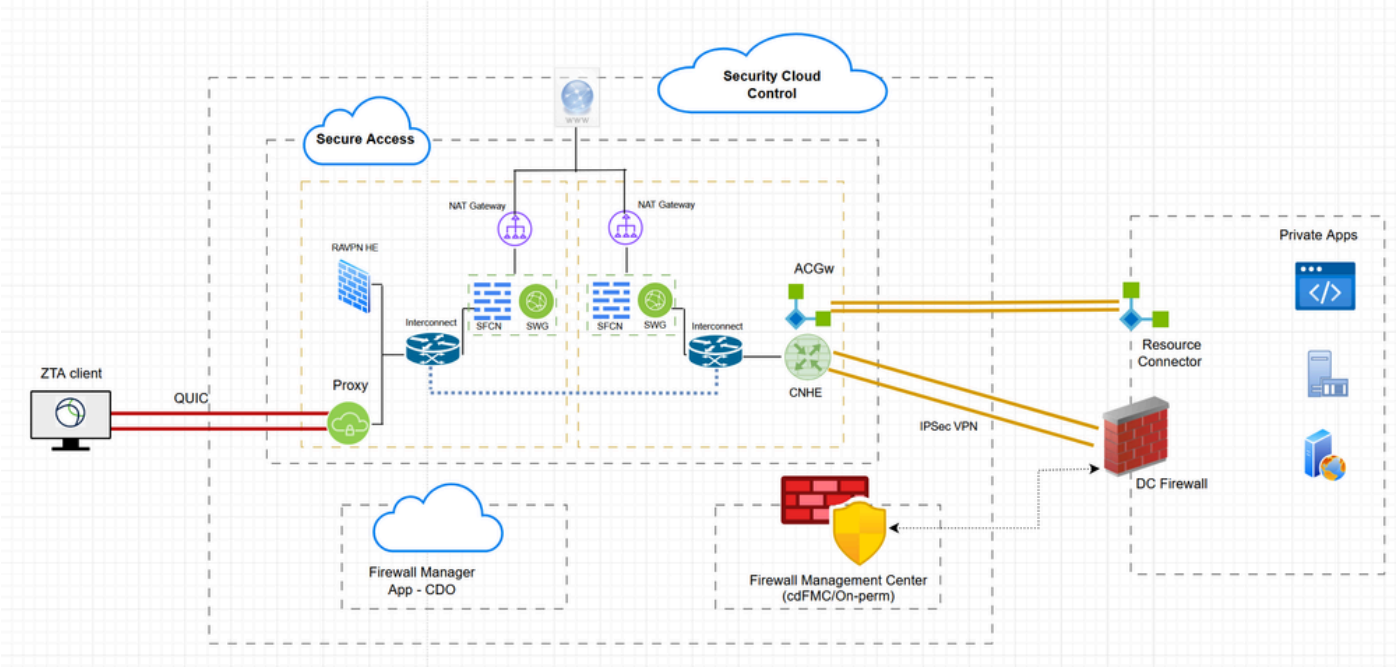
8.由于应用连接源自ZProxy，因此它将有一个内部IP（例如：169.251.1.2）作为源IP。在将其发送出去之前，此操作将转换为FTD出口接口IP。然后，仅当访问令牌中存在文件或IPS策略时，Lina才会为Snort检测标记通用零信任流。从访问令牌获取的规则ID将在连接元数据中传递到Snort。

9.通用零信任规则以及对应的文件和IPS策略映射通过FMC推送到FTD。Snort中的零信任插件将在初始化期间加载这些规则。仅当从安全访问获取用于访问该私有资源的访问令牌中提到文件或IPS策略时，Lina才会为Snort检测标记通用零信任流流。

从访问令牌获取的规则ID通过Conn Meta传递到Snort。对于所有通用零信任流流，Snort中的零信任插件将对从该Conn Meta获取的规则ID执行规则查找。如果找到规则匹配，则允许该流，并将该规则特定的IPS和文件策略应用于该流。如果未找到规则匹配，则Snort中的零信任插件将阻止该流。

配置

网络图

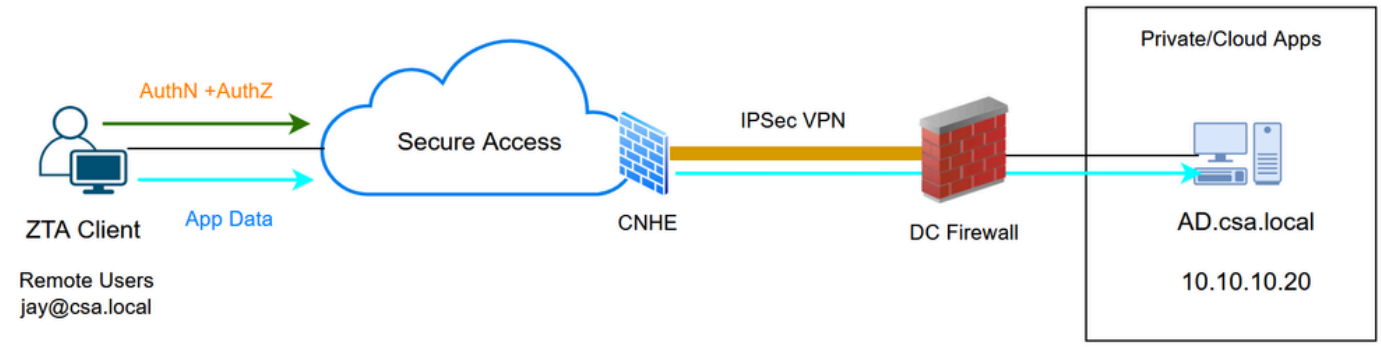


混合ZTNA — 网络图

测试案例

测试案例1: 远程用户 — 云实施

在本测试案例中，我们将通过云实施通过网络隧道组访问私有资源。在这种情况下，策略评估和应用数据都会被安全访问通过ZTA模块拦截。这是传统流程，我们可以通过网络隧道组或资源连接器从ZTA注册客户端访问私有应用

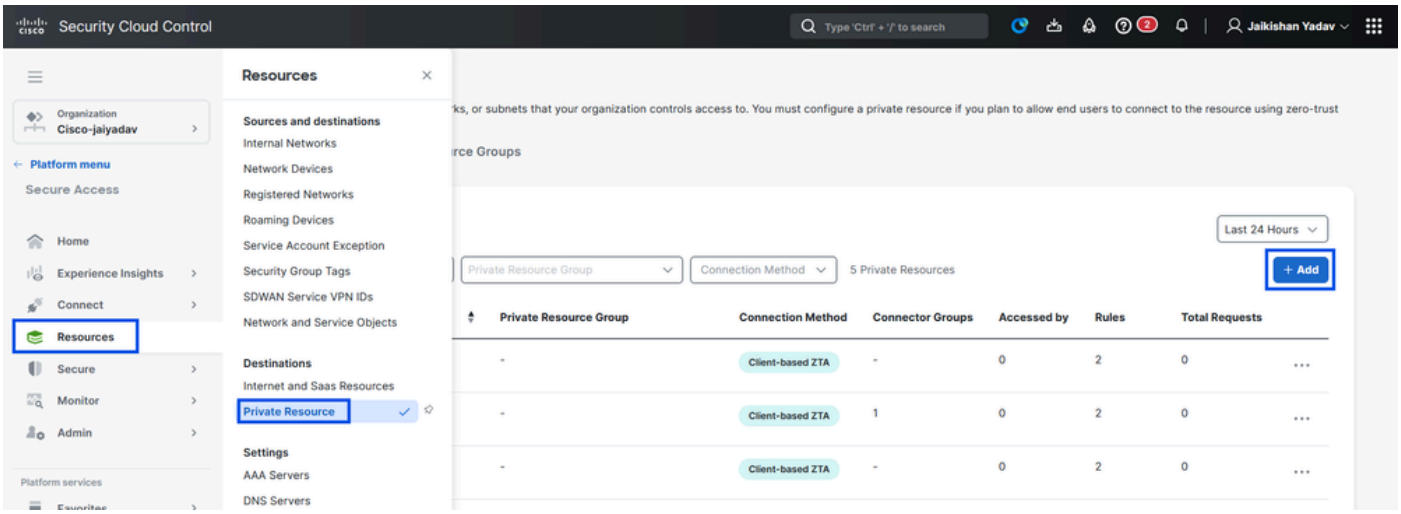


通用ZTA — 测试用例拓扑

第1步 — 在安全访问中定义私有资源

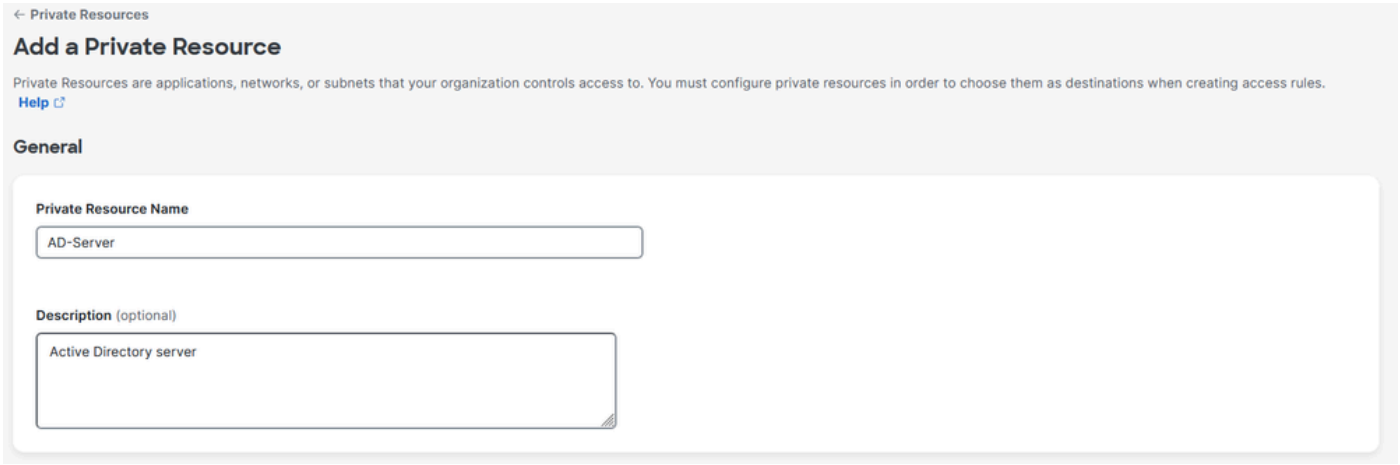
配置私有资源，使其可通过云实施的零信任访问(ZTA)注册设备访问

1. 导航到资源 > 目标 > 专用资源 >单击+添加



安全访问 — 私有资源配置

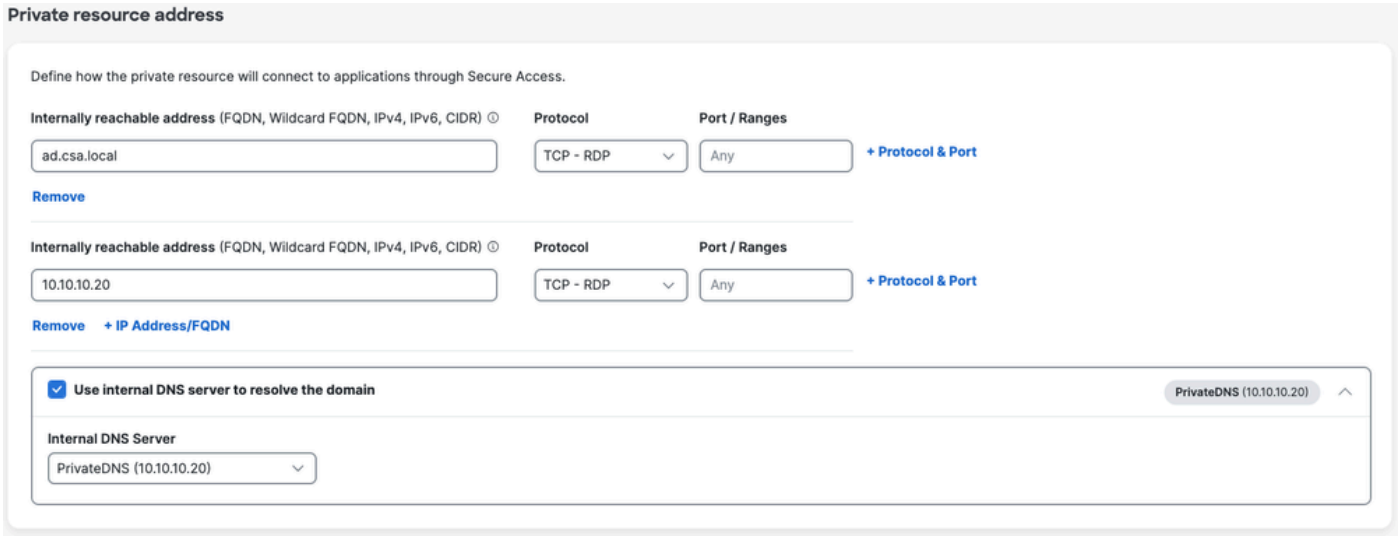
2.对于专用资源名称，输入资源有意义的名称。对于Description，建议您提供诸如资源用途或资源所有者名称等信息。



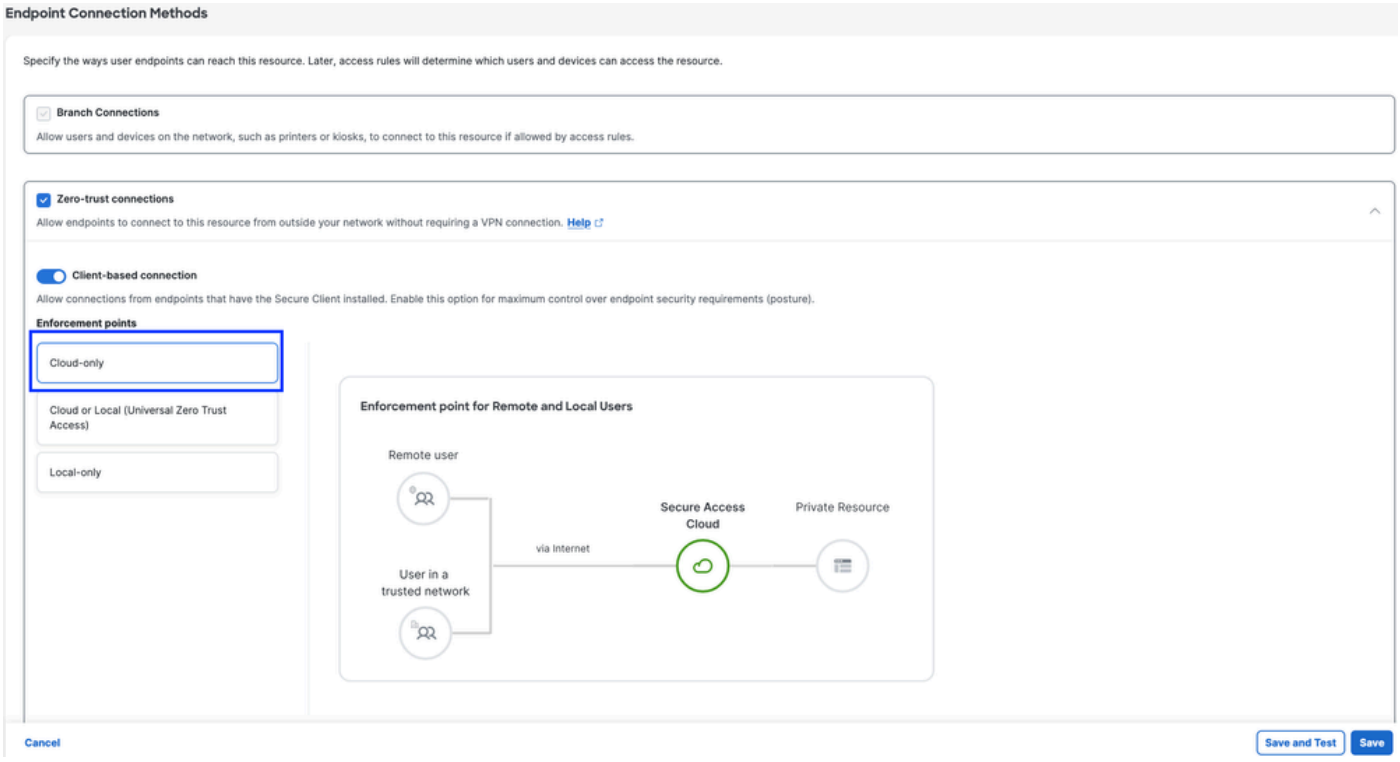
安全访问 — 私有资源配置

3.输入要访问的专用资源的FQDN。我们还可以定义私有资源的IP地址。有关详细信息，请参阅添加专用资源

4.选择要解析域的内部DNS服务器



5. 选择终端连接方法

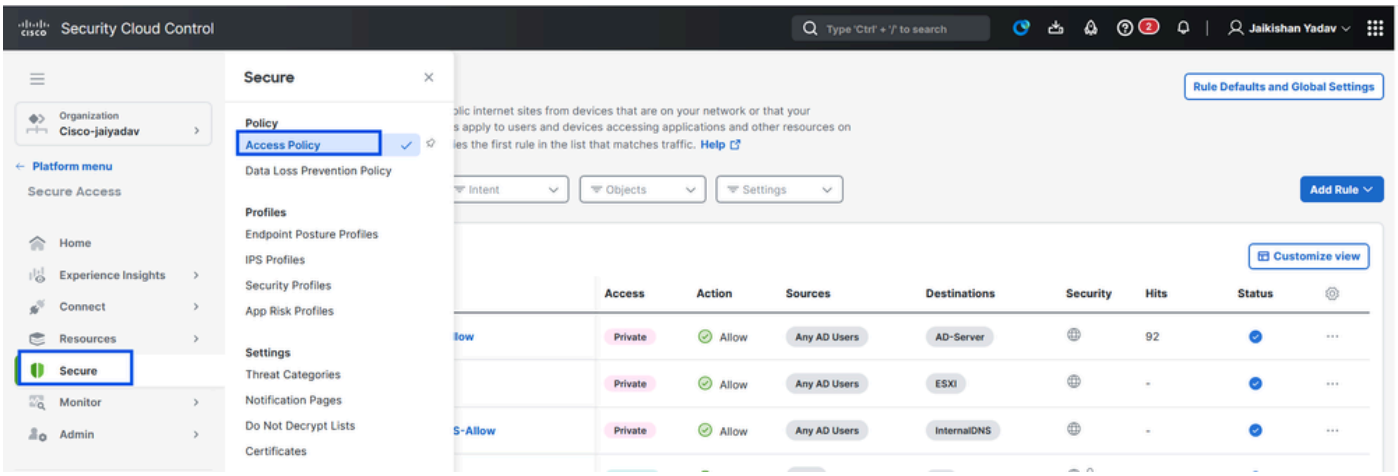


6. 点击保存

第2步 — 创建专用访问规则

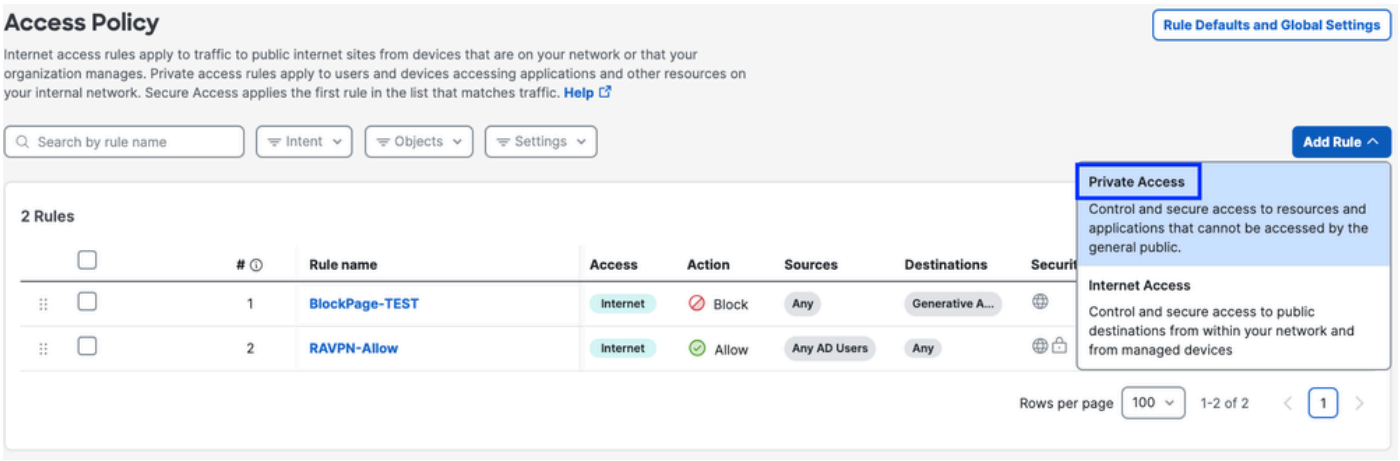
在Secure Access上配置私有访问，以便由通用ZTA注册用户访问。有关详细信息，请参阅[专用访问规则]

1. 导航到安全>访问策略



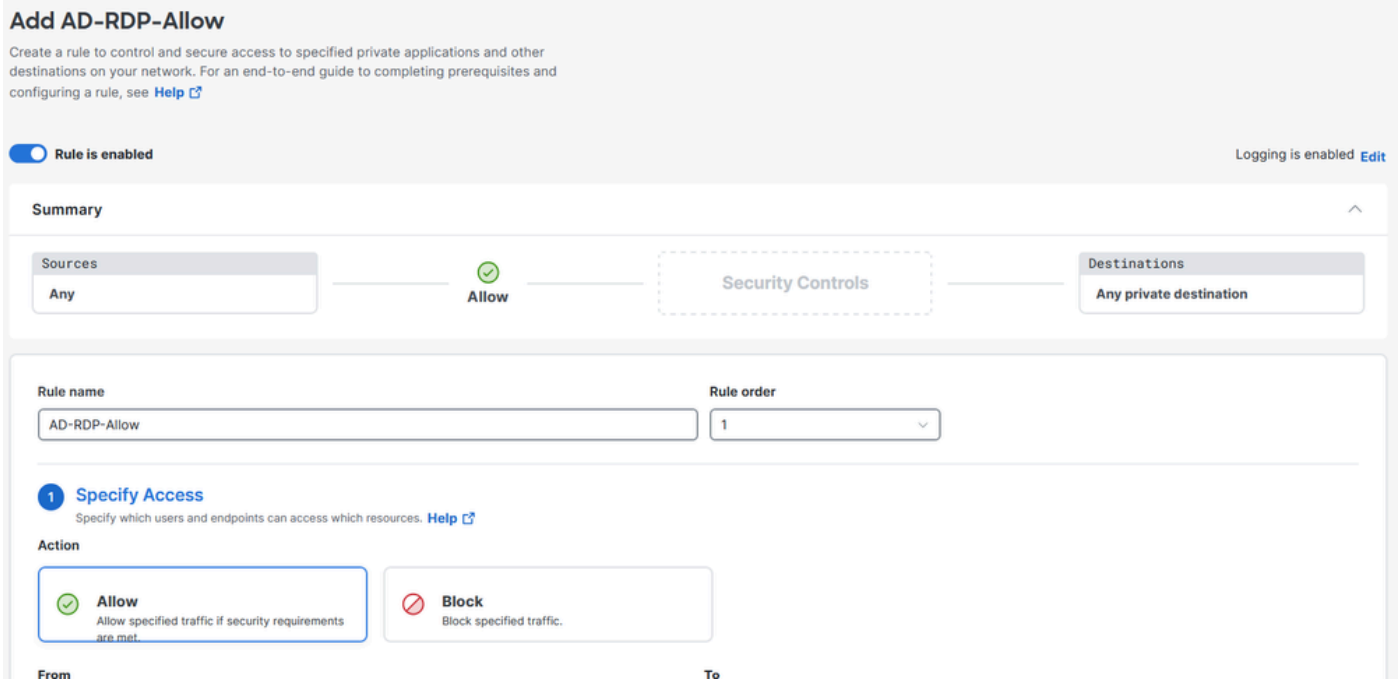
安全访问 — 访问策略配置

2.单击Add Rule，然后选择Private Access。
规则顶部是描述规则已配置组件的摘要。



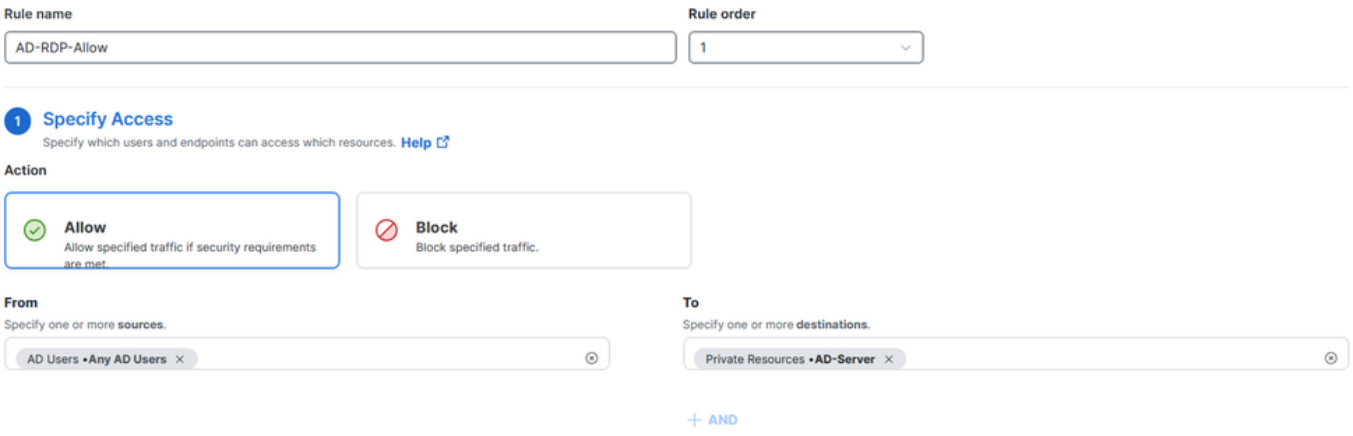
安全访问 — 访问策略配置

3.添加规则名称



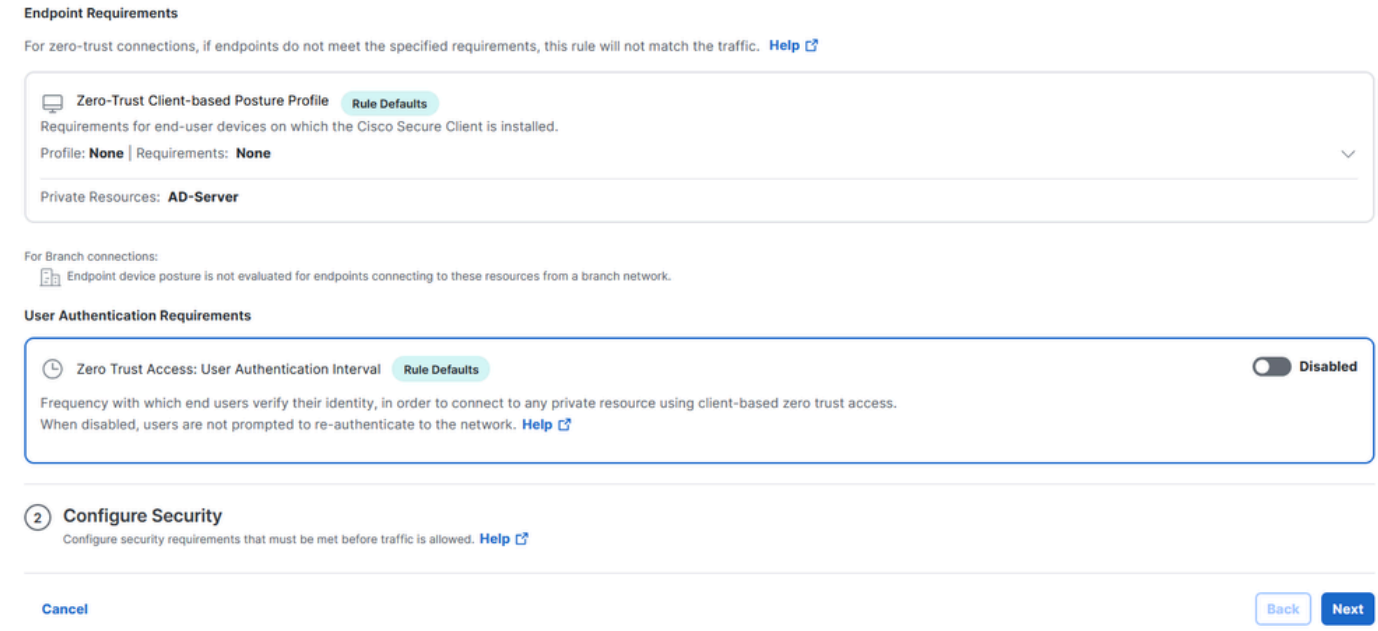
安全访问 — 访问策略配置

4.选择规则操作，然后选择来源和目标



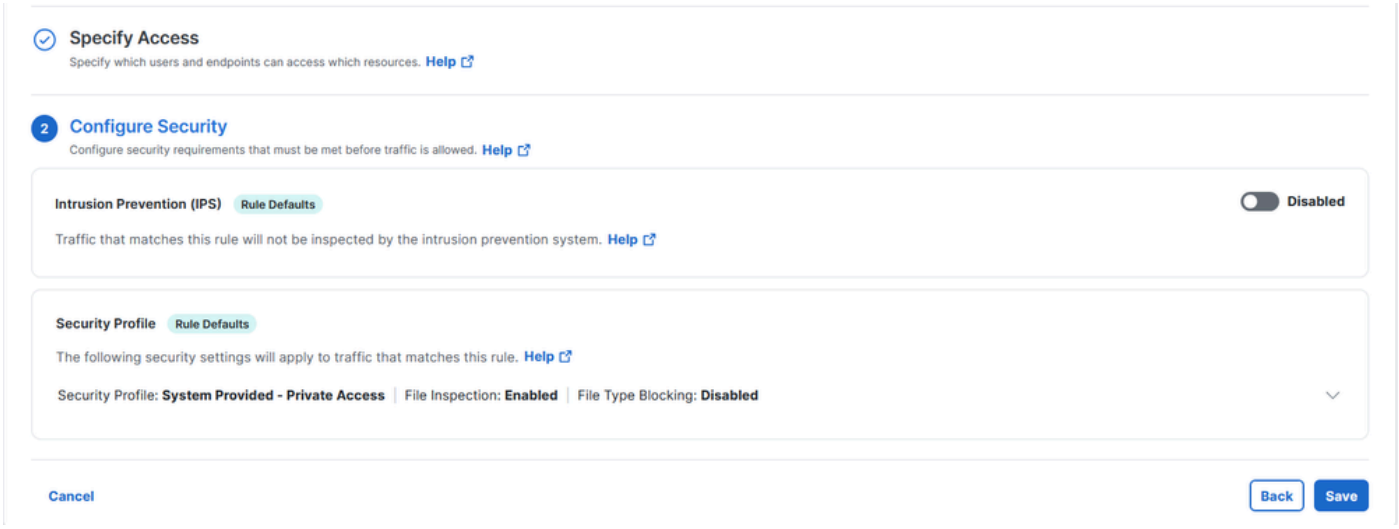
安全访问 — 访问策略配置

5.配置终端要求



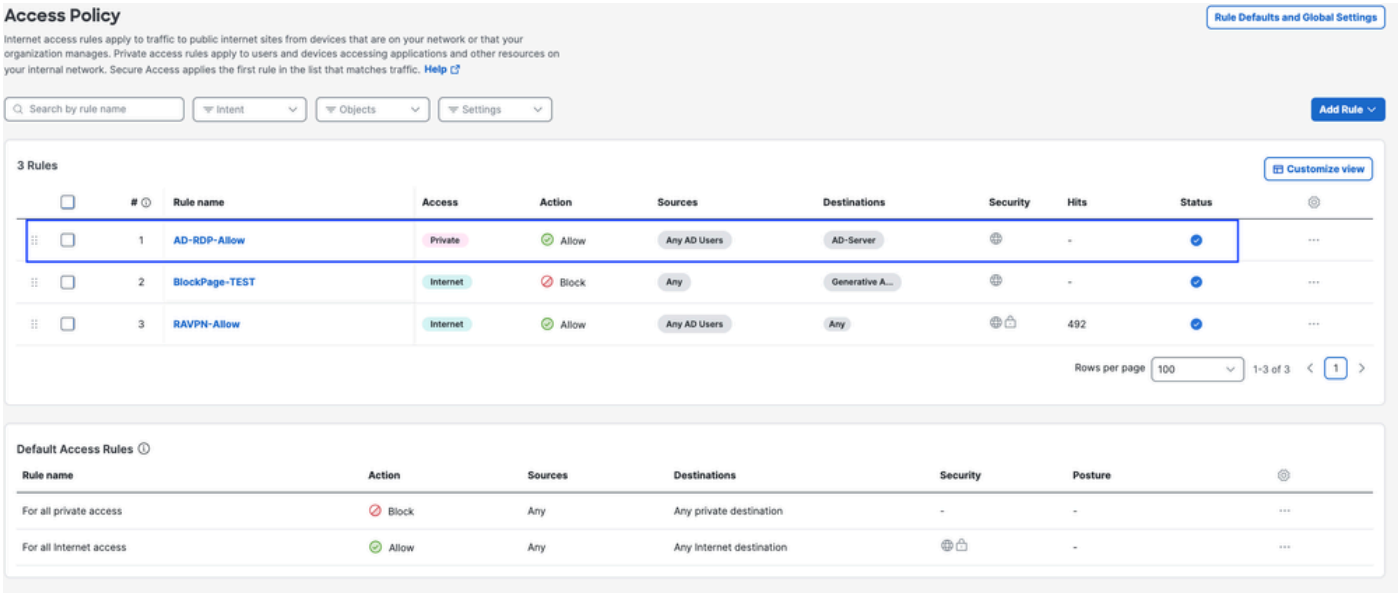
安全访问 — 访问策略配置

6. 配置安全性



安全访问 — 访问策略配置

7.单击Save

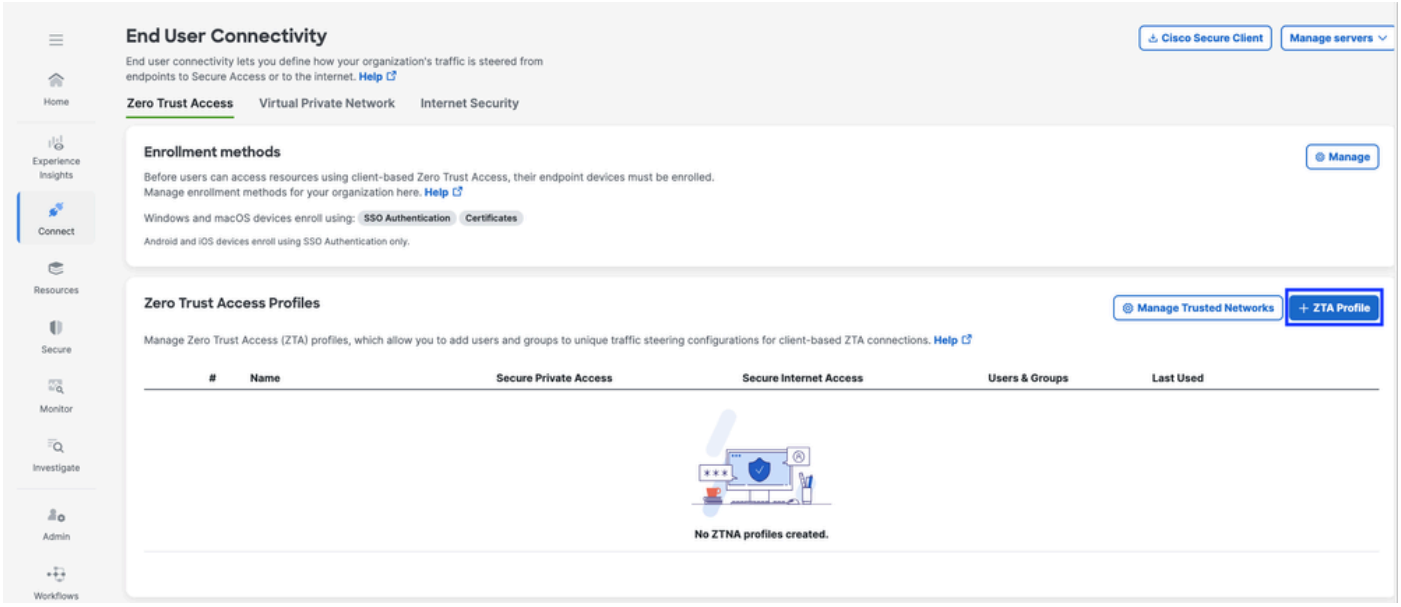


安全访问 — 访问策略配置

第3步 — 将私有资源添加到ZTA配置文件

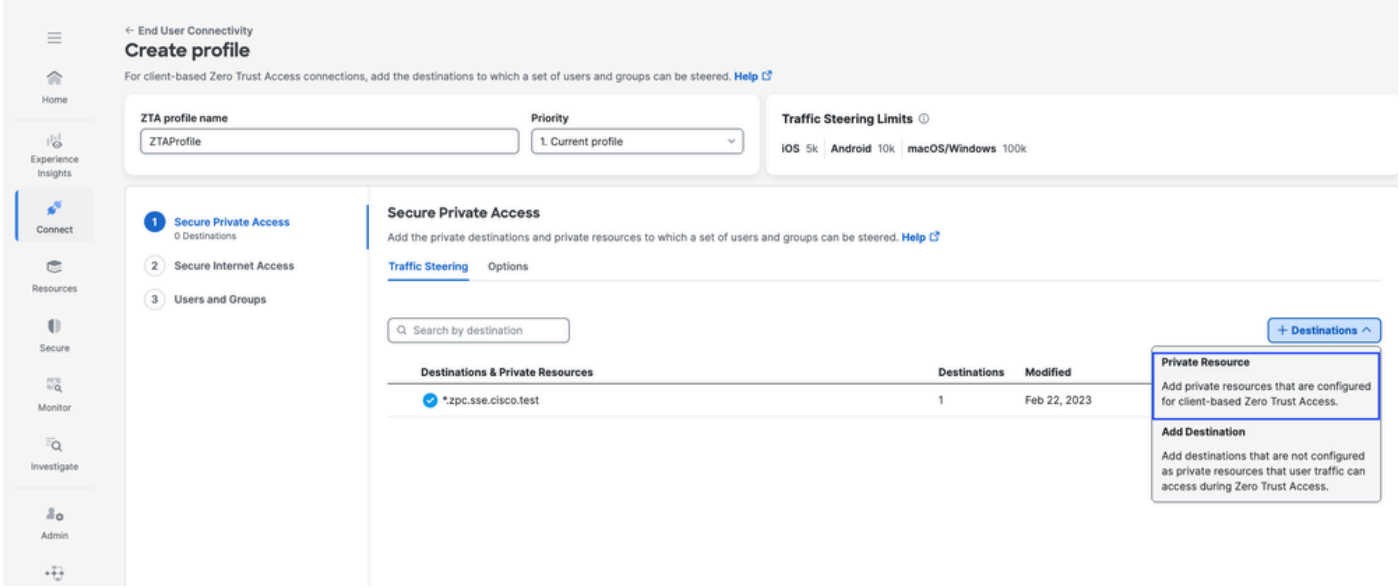
如果您使用的是自定义ZTA配置文件，则需要将相应的专用资源添加到ZTA配置文件中

1.导航到Connect > End User Connectivity > Zero Trust Access，然后单击+ZTA Profile

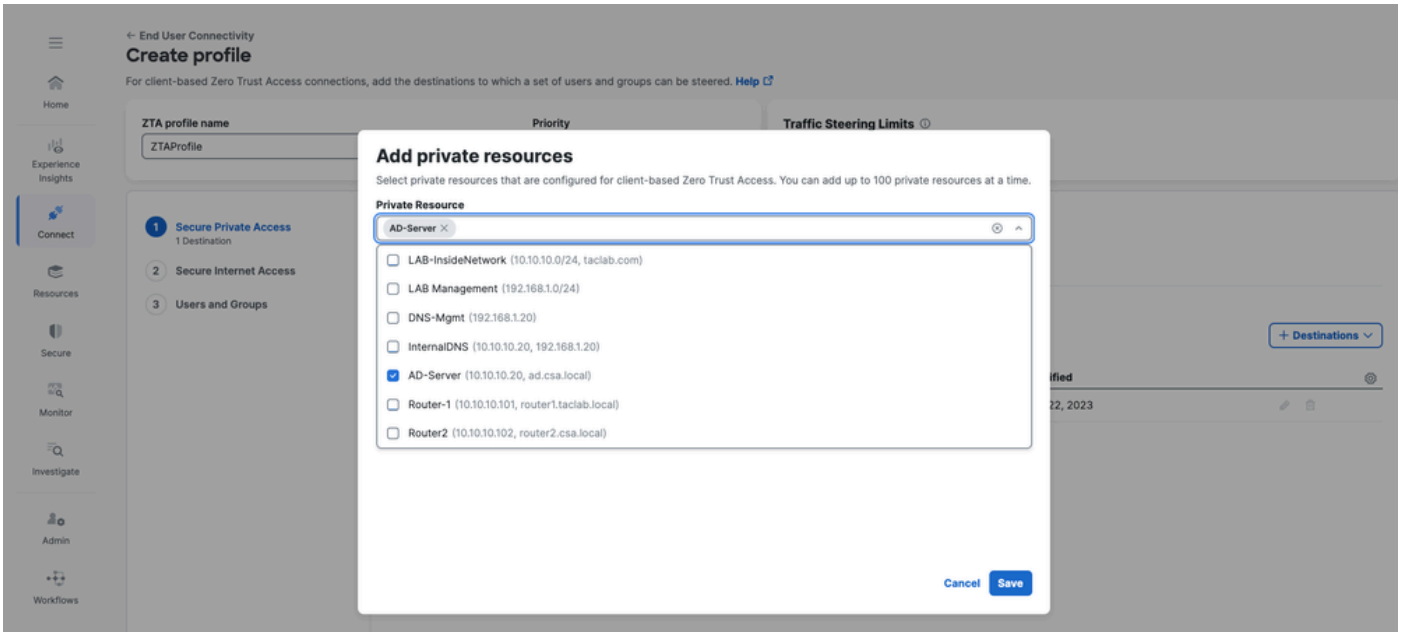


安全访问 — ZTA配置文件

2.添加专用资源

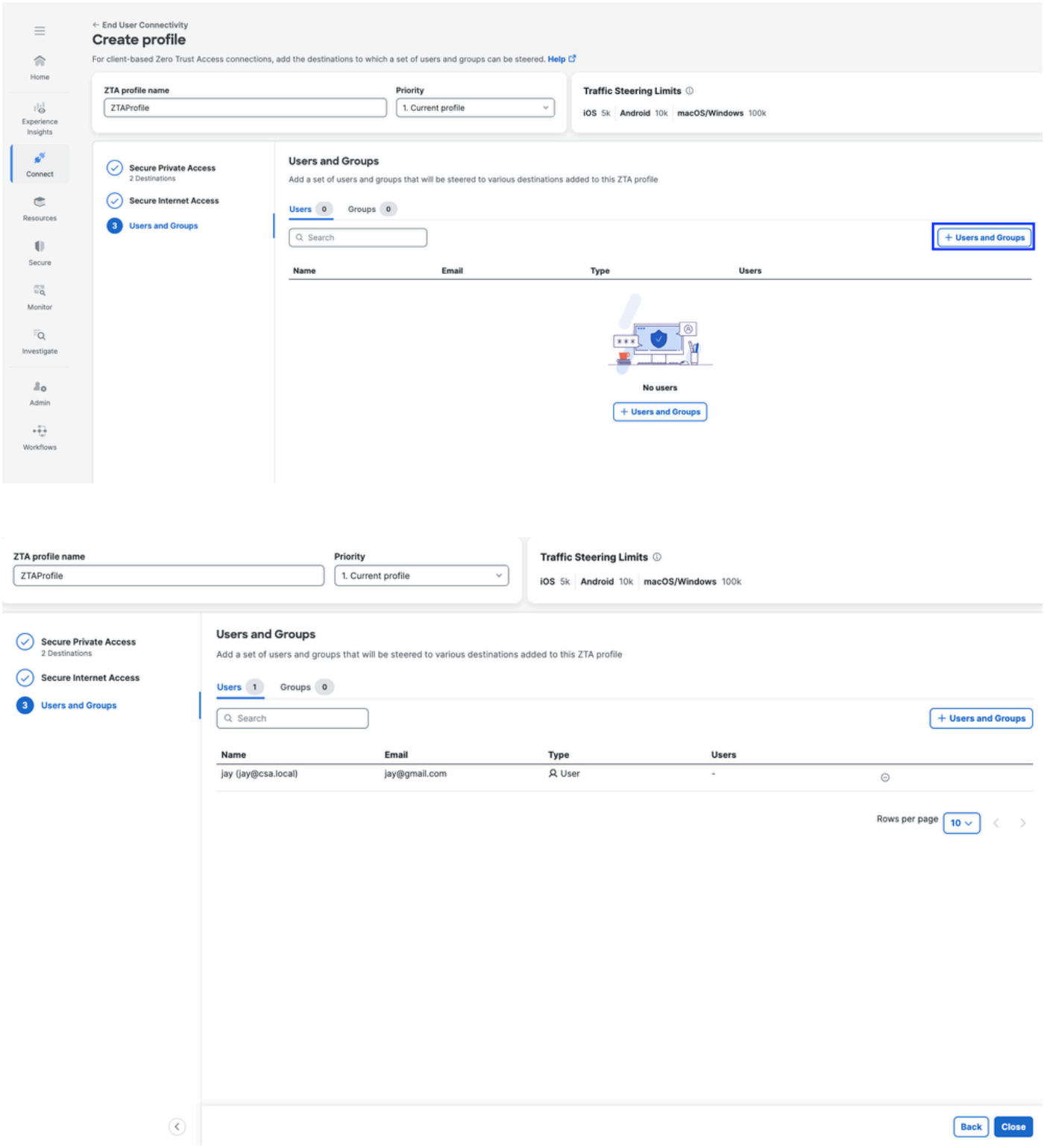


安全访问 — ZTA配置文件



安全访问 — ZTA配置文件

3.添加用户和组



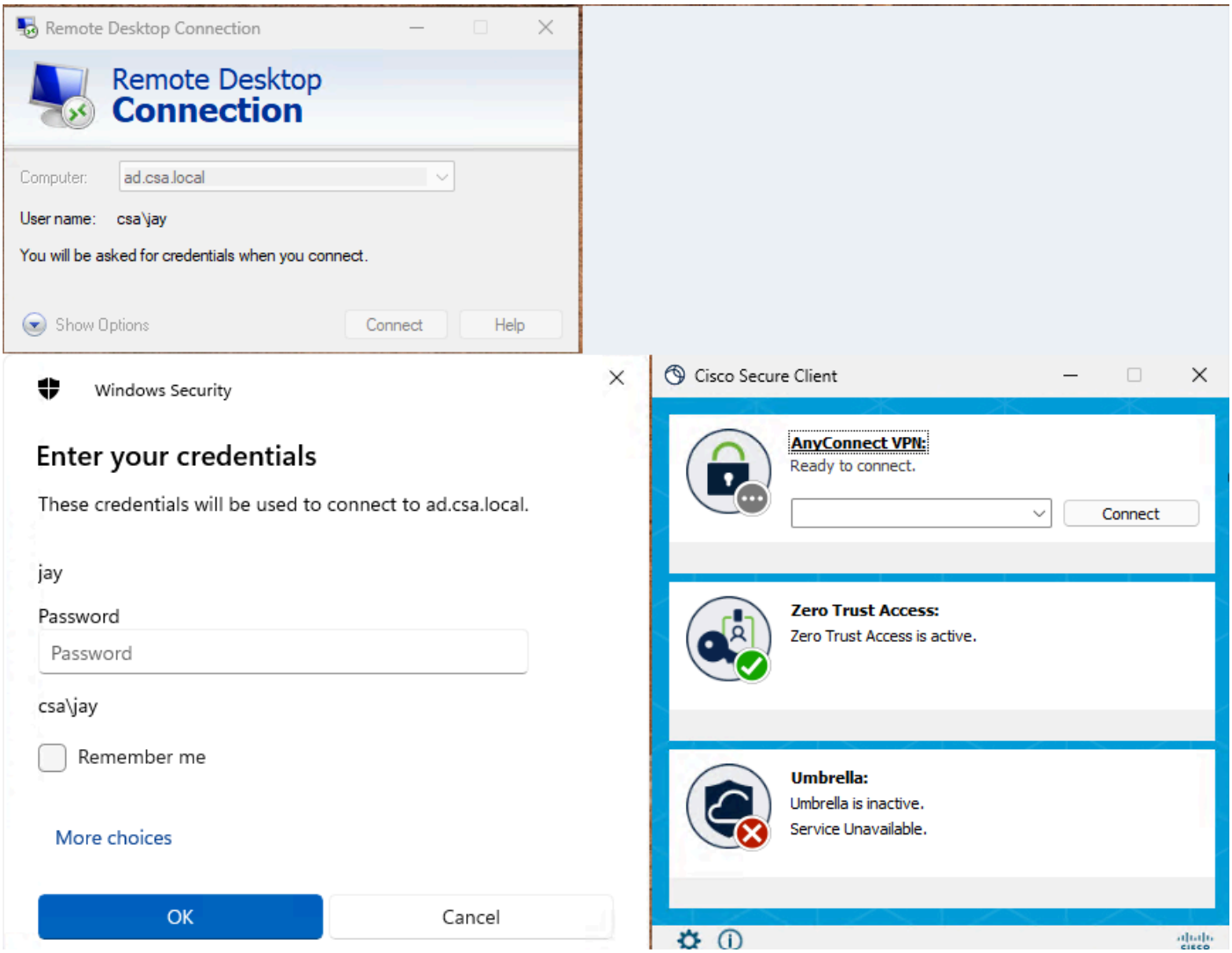
安全访问 — ZTA配置文件

注意：对于分配的专用资源，将配置推送到客户端并同步可能需要15-20分钟

步骤 — 4检验对专用资源的访问

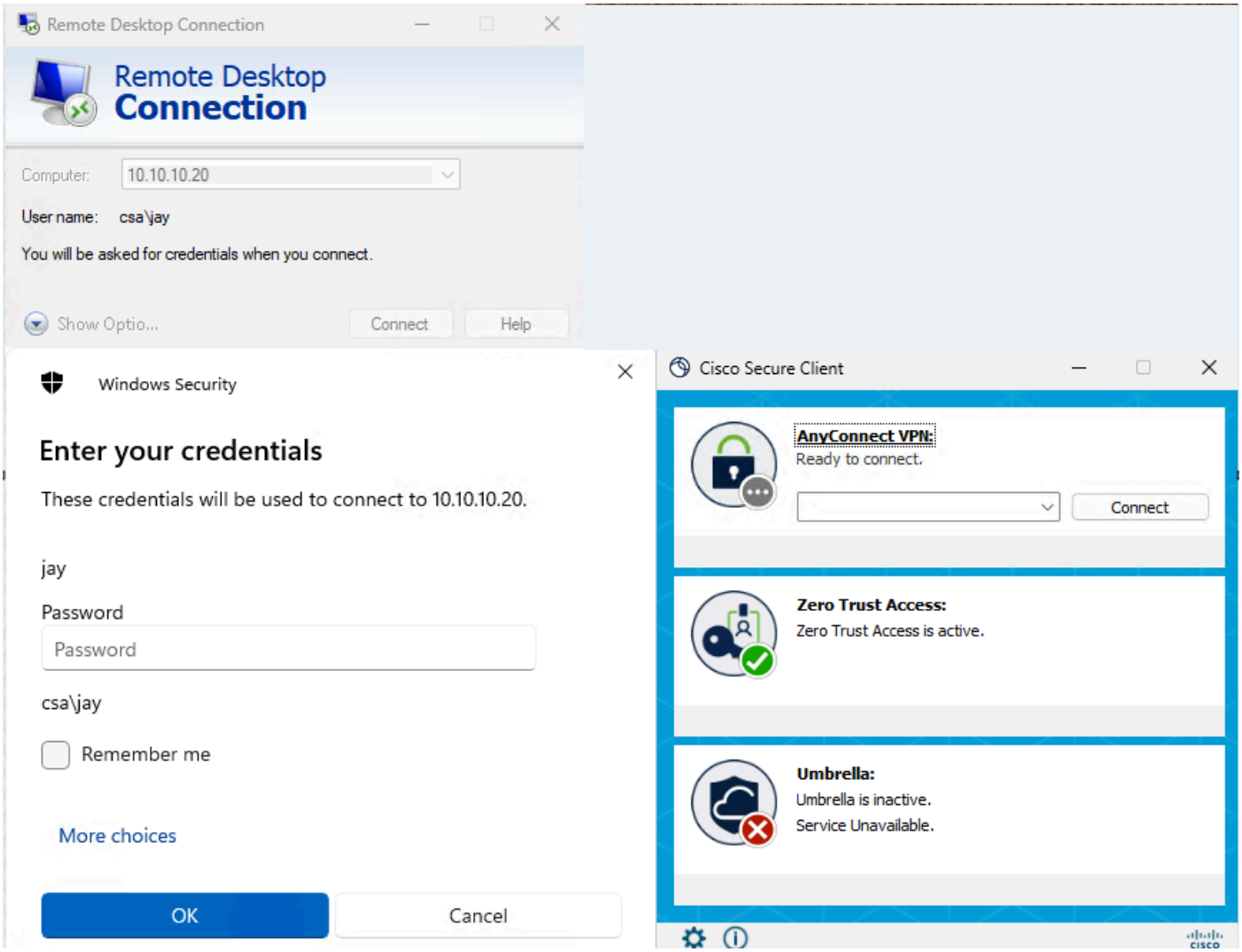
1.访问私有资源

使用FQDN访问PR



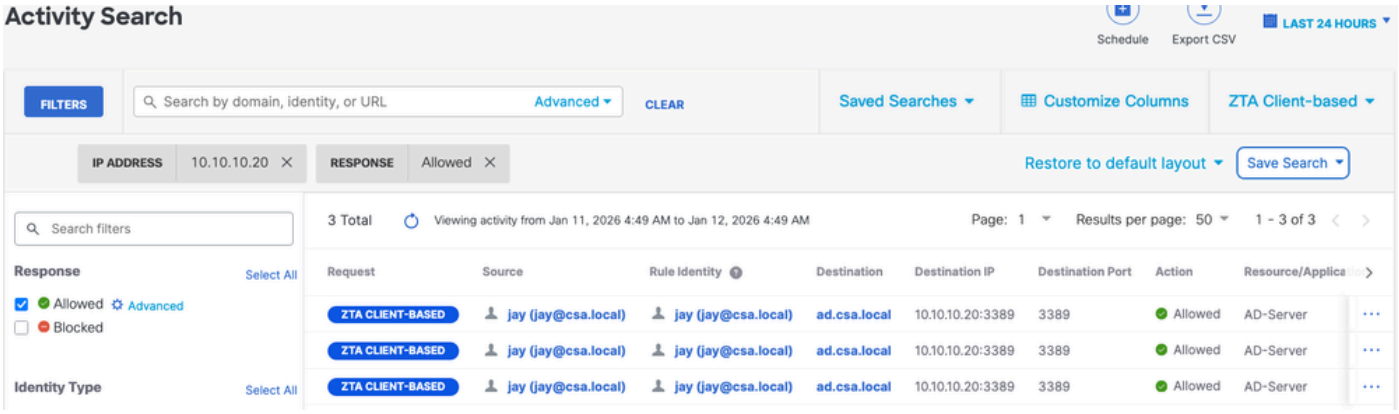
安全访问 — PR测试

使用IP地址访问PR

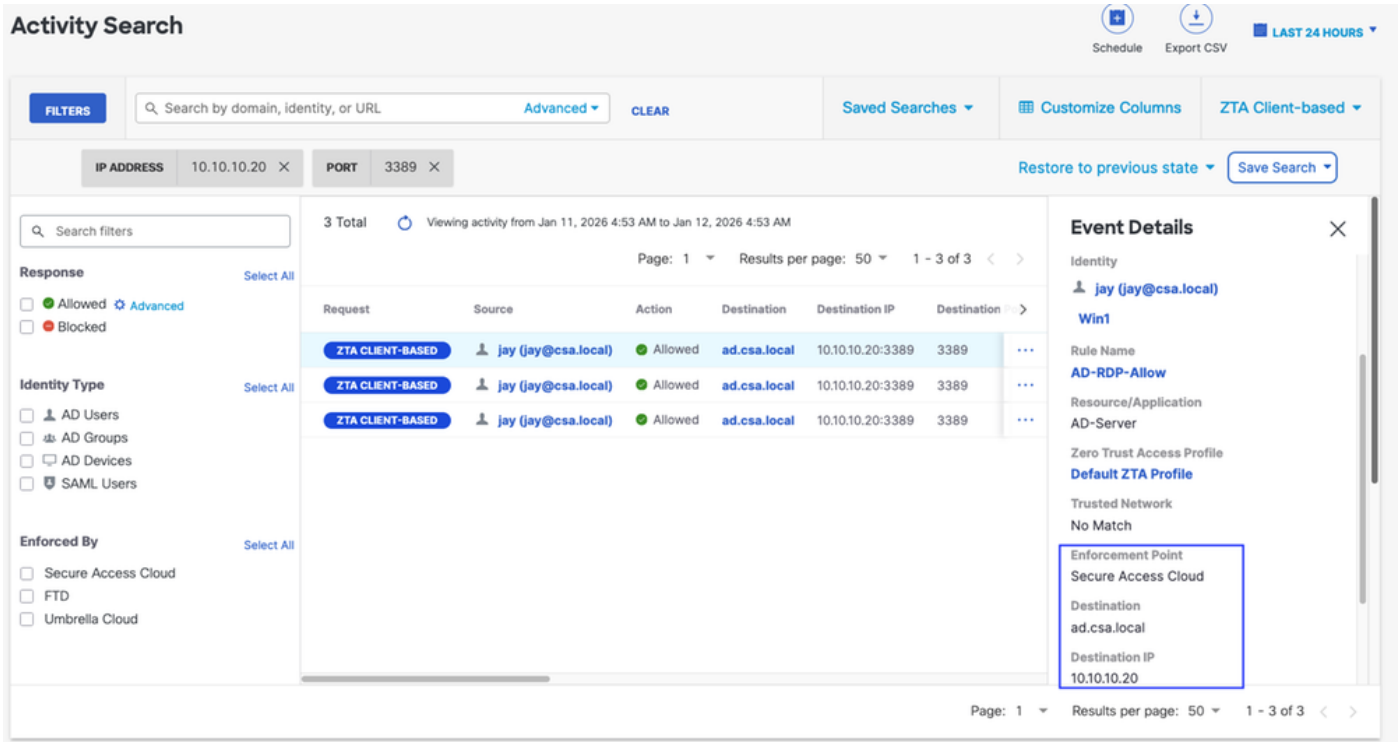


安全访问 — PR测试

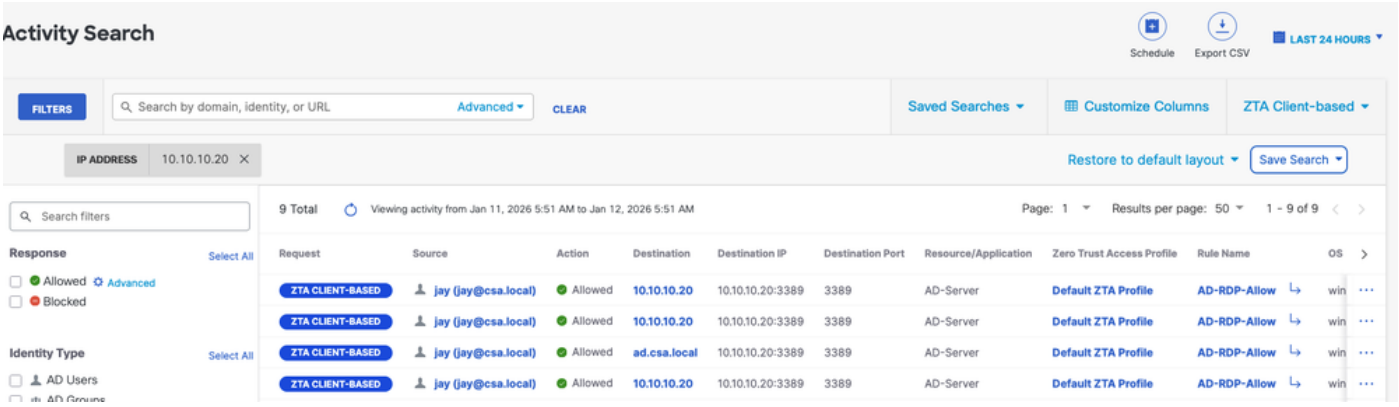
2.使用“活动搜索”事件进行验证



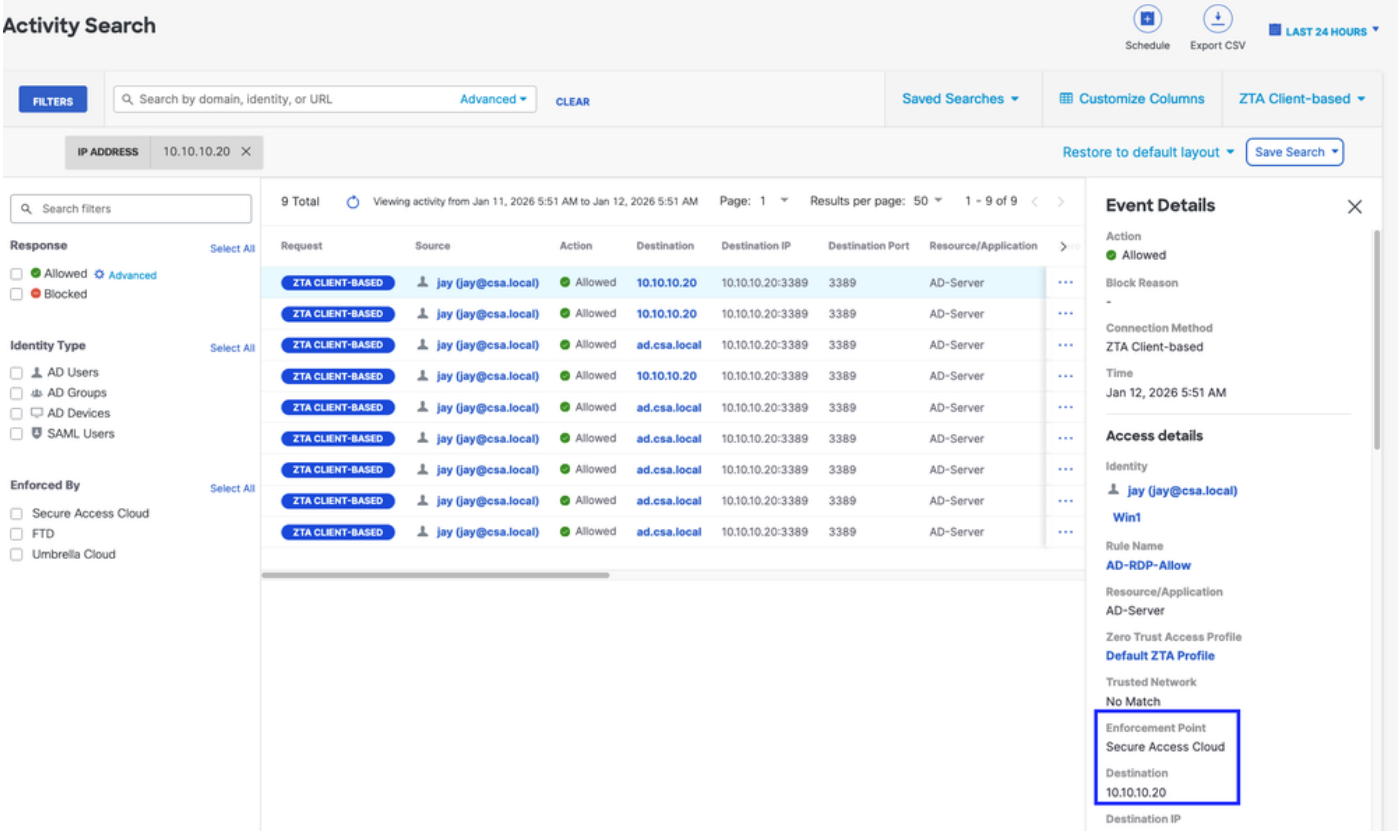
安全访问 — 活动搜索



安全访问 — 活动搜索

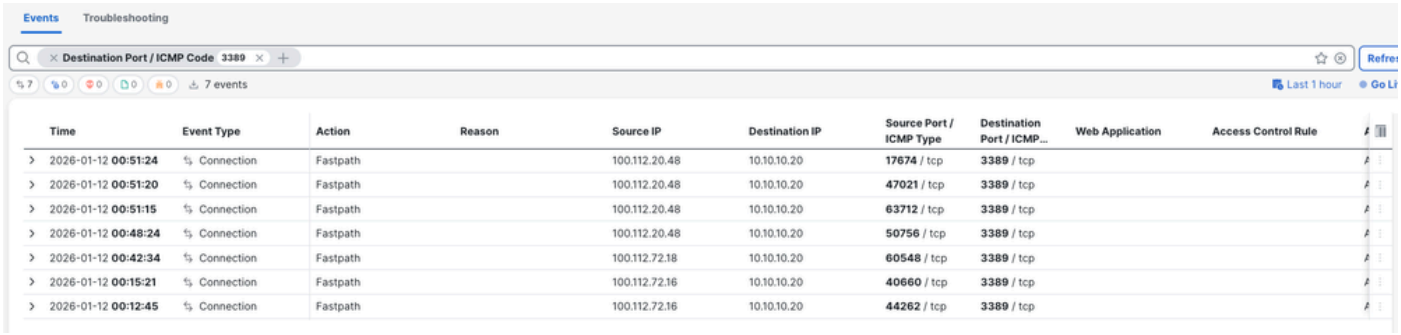


安全访问 — 活动搜索



安全访问 — 活动搜索

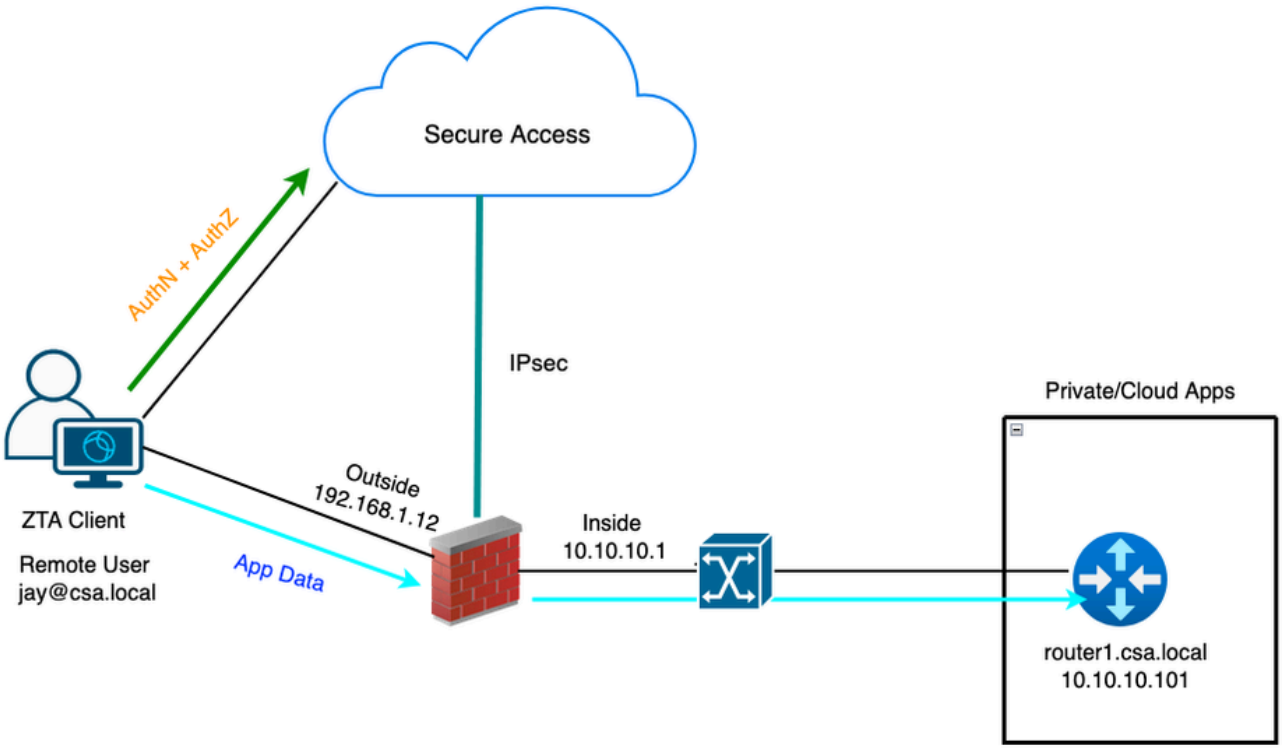
3.检验FMC连接事件



FMC连接事件

测试案例2 — 远程用户 — 本地实施

通过本地实施访问私有资源，这种类型的实施策略评估在安全访问上进行，但应用数据对FTD保持本地状态。例如，ZTA注册客户端或连接到家庭网络的用户，并尝试访问FTD内部接口后面的私有资源。

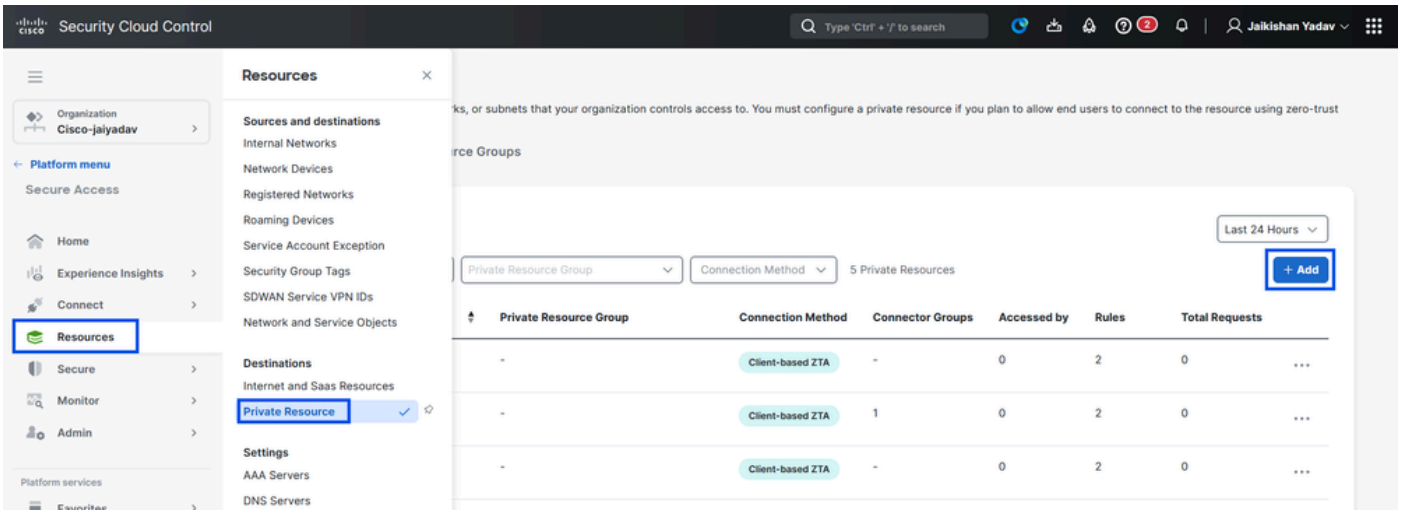


通用ZTA — 测试用例拓扑

第1步 — 在安全访问中定义私有资源

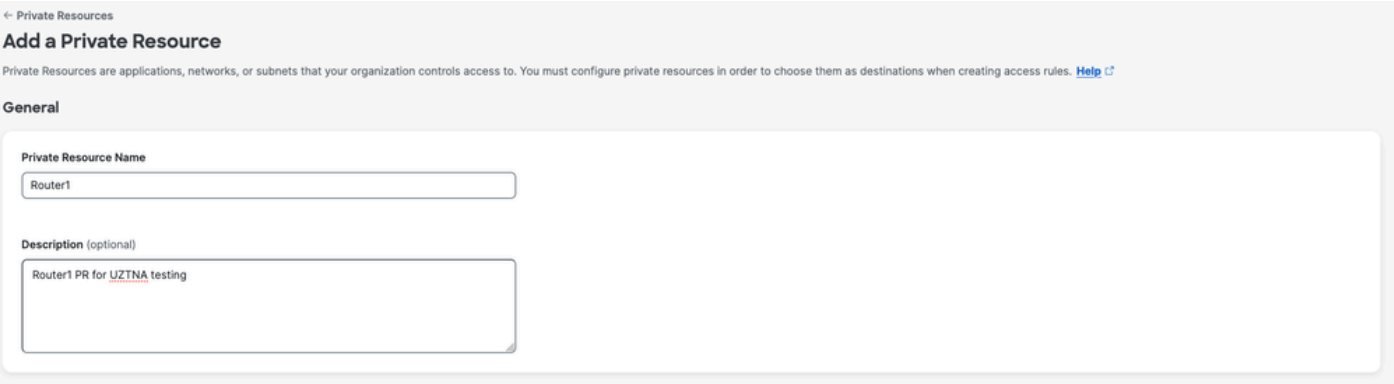
配置私有资源，使其可通过云实施的零信任访问(ZTA)注册设备访问

1. 导航到资源 > 目标 > 专用资源 >单击+添加



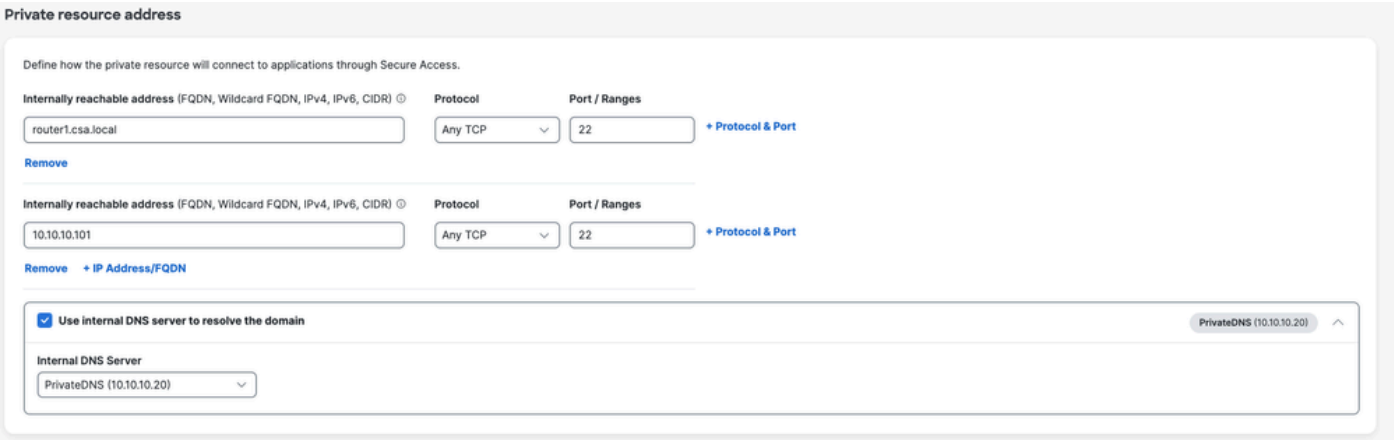
安全访问 — 私有资源配置

2.对于专用资源名称，输入资源有意义的名称。对于Description，建议您提供诸如资源用途或资源所有者名称等信息。



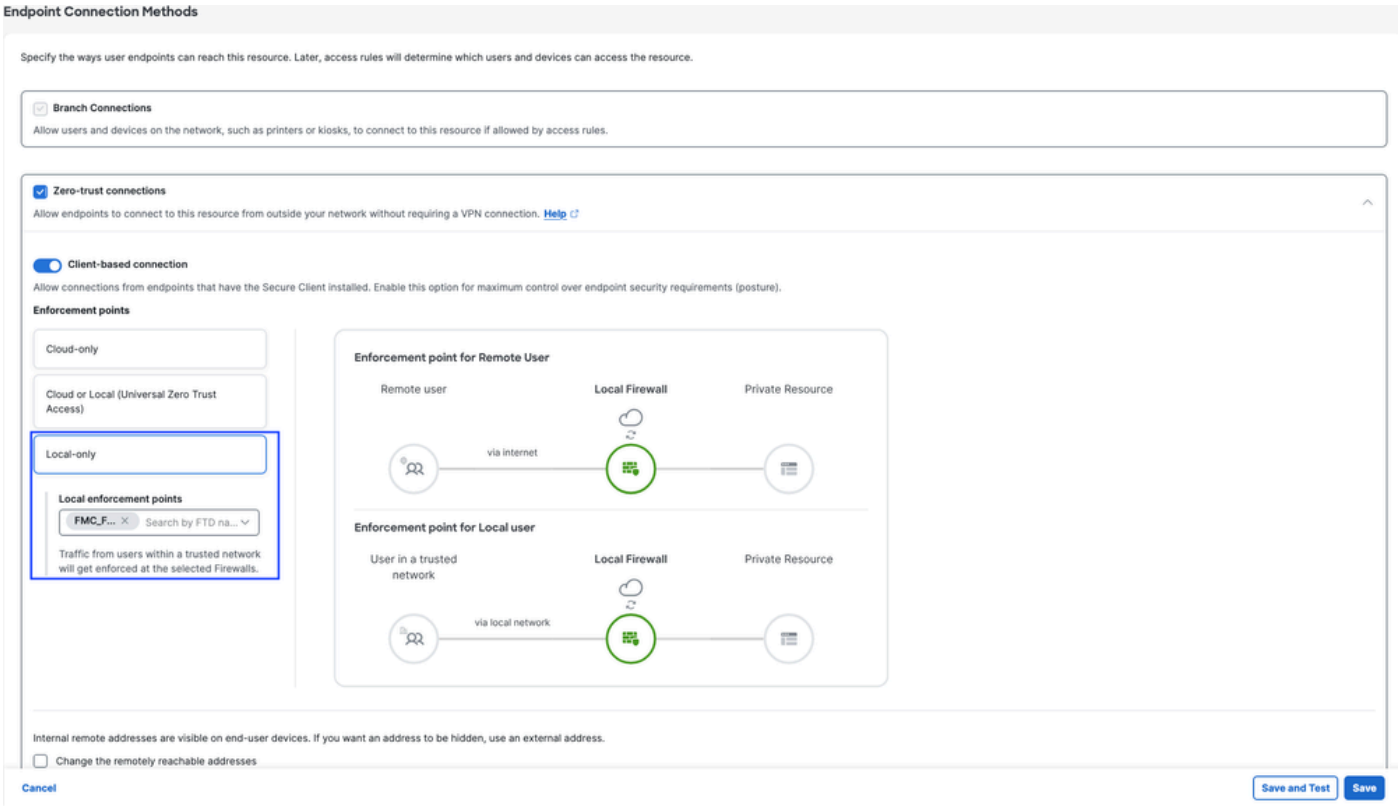
3.输入要访问的专用资源的FQDN。我们还可以定义私有资源的IP地址。有关详细信息，请参阅添加专用资源

4.选择要解析域的内部DNS服务器



5. 选择终端连接方法

6.选择FTD作为本地实施点



安全访问 — 私有资源配置

注意：根据您选择的注册类型，此更改将自动将PR与FTD关联并触发策略部署

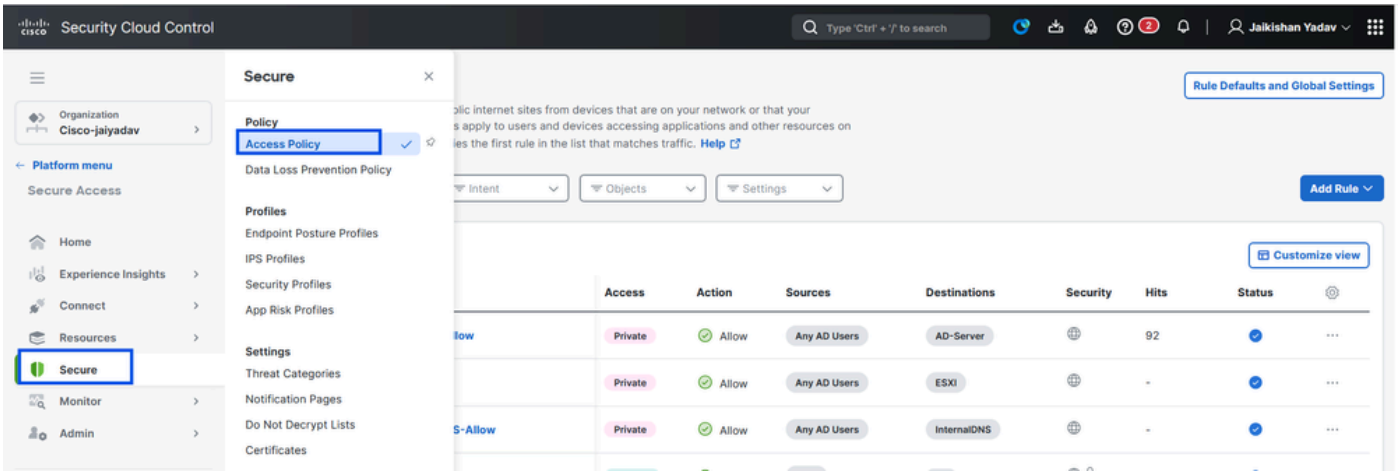
---

7. 点击保存

第2步 — 创建专用访问规则

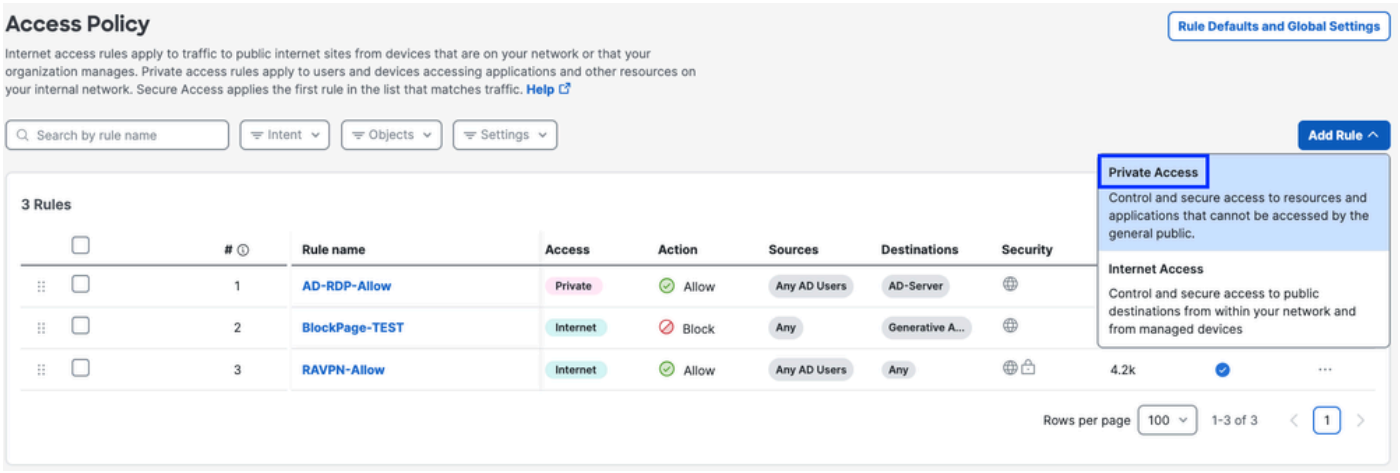
在Secure Access上配置私有访问，以便由通用ZTA注册用户访问。有关详细信息，请参阅专用访问规则

1. 导航到安全>访问策略



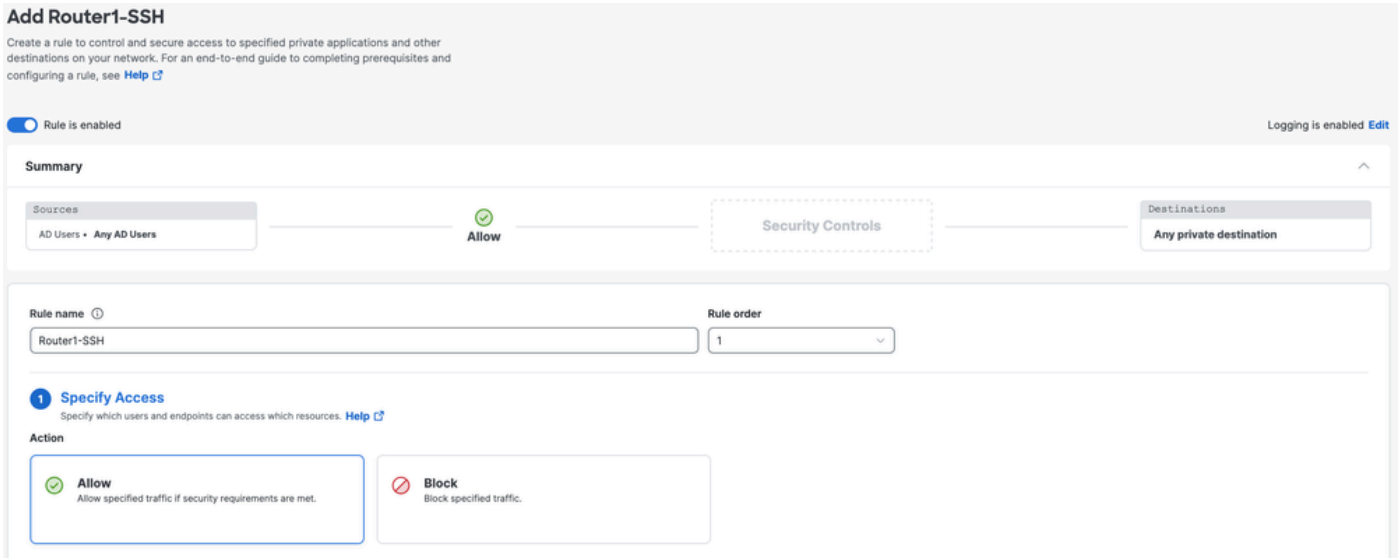
安全访问 — 私有资源配置

2.单击Add Rule，然后选择Private Access。
规则顶部是描述规则已配置组件的摘要。



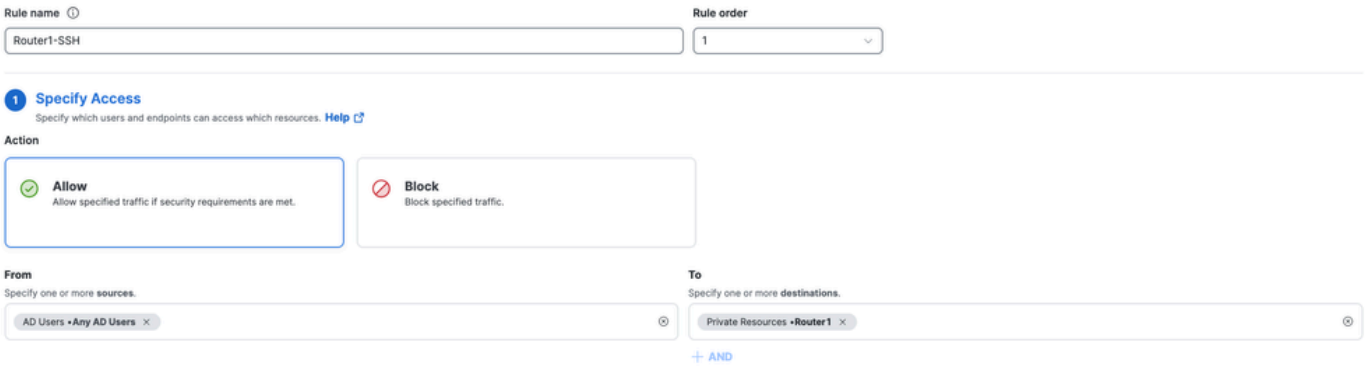
安全访问 — 访问策略配置

3.添加规则名称



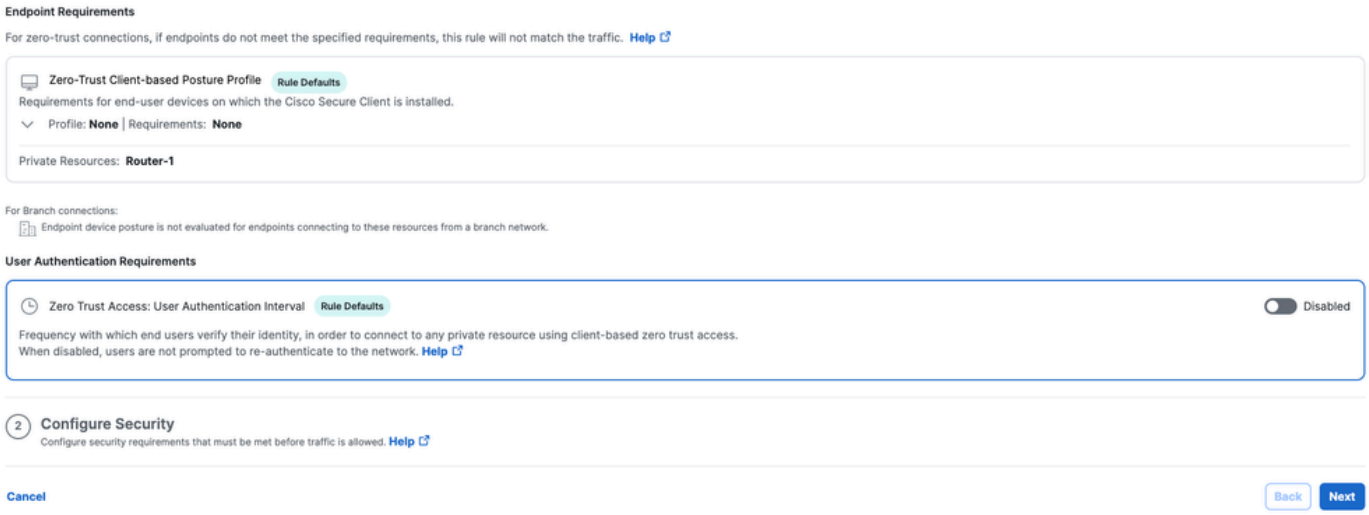
安全访问 — 访问策略配置

4.选择规则操作，然后选择来源和目标



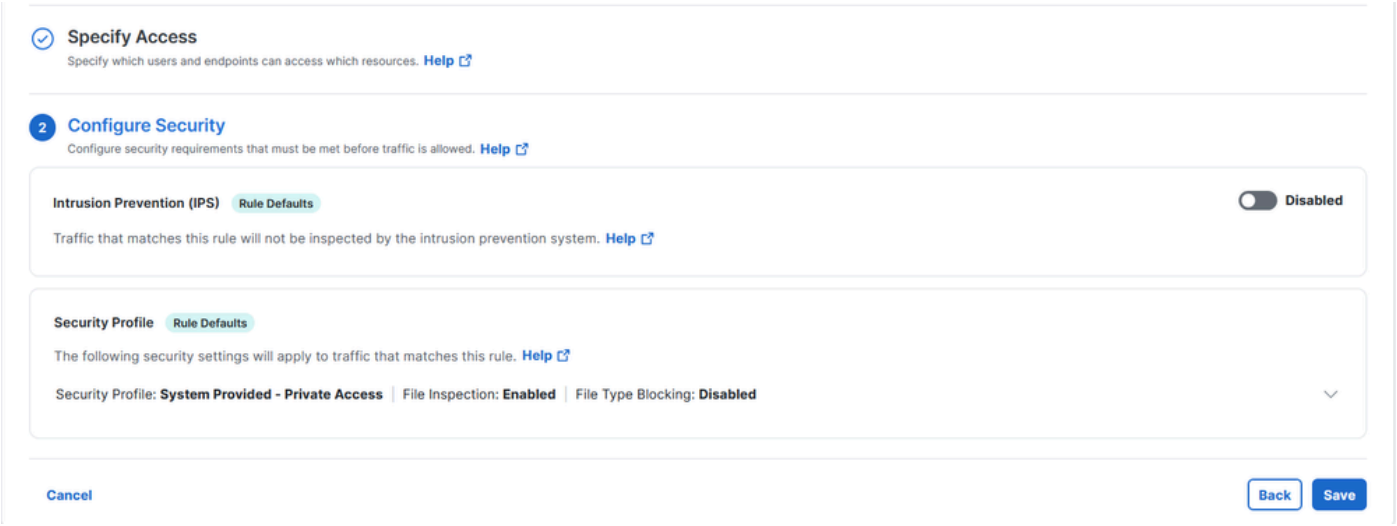
安全访问 — 访问策略配置

5.配置终端要求



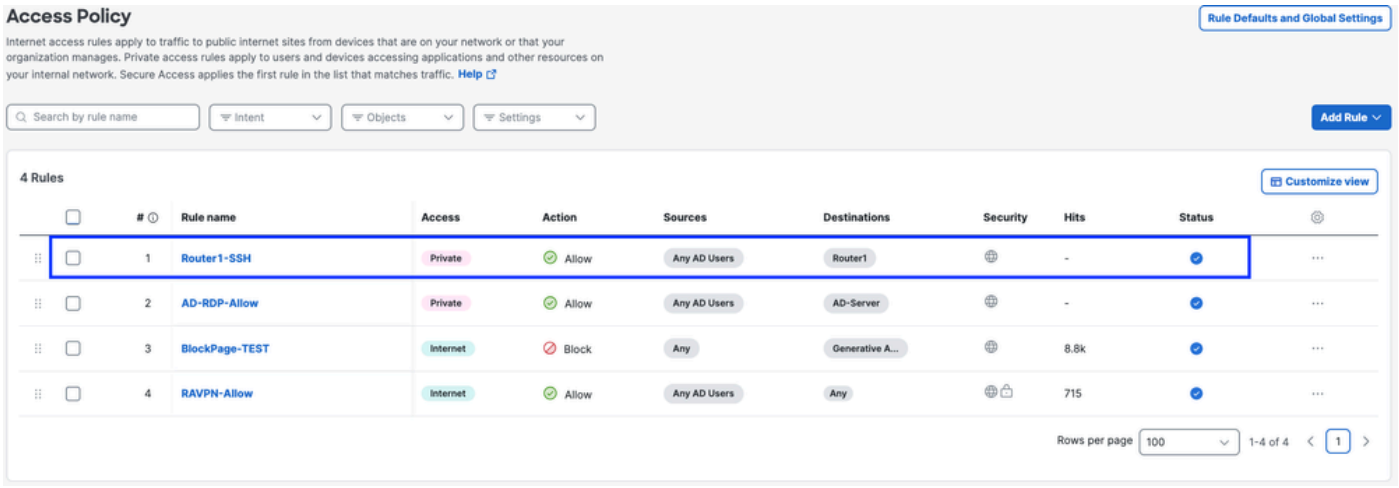
安全访问 — 访问策略配置

6. 配置安全性



安全访问 — 访问策略配置

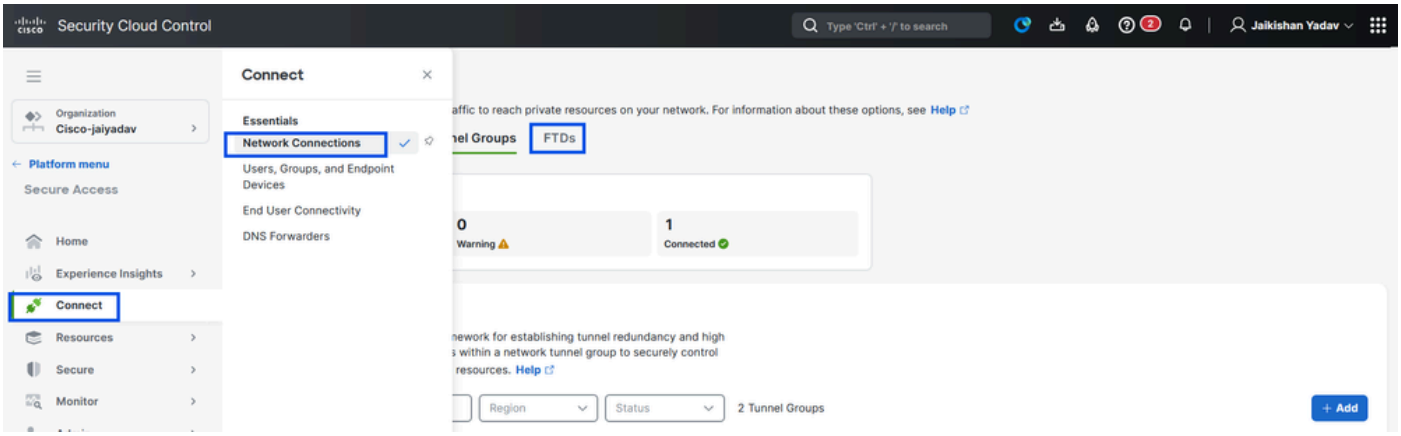
7.单击Save



安全访问 — 访问策略配置

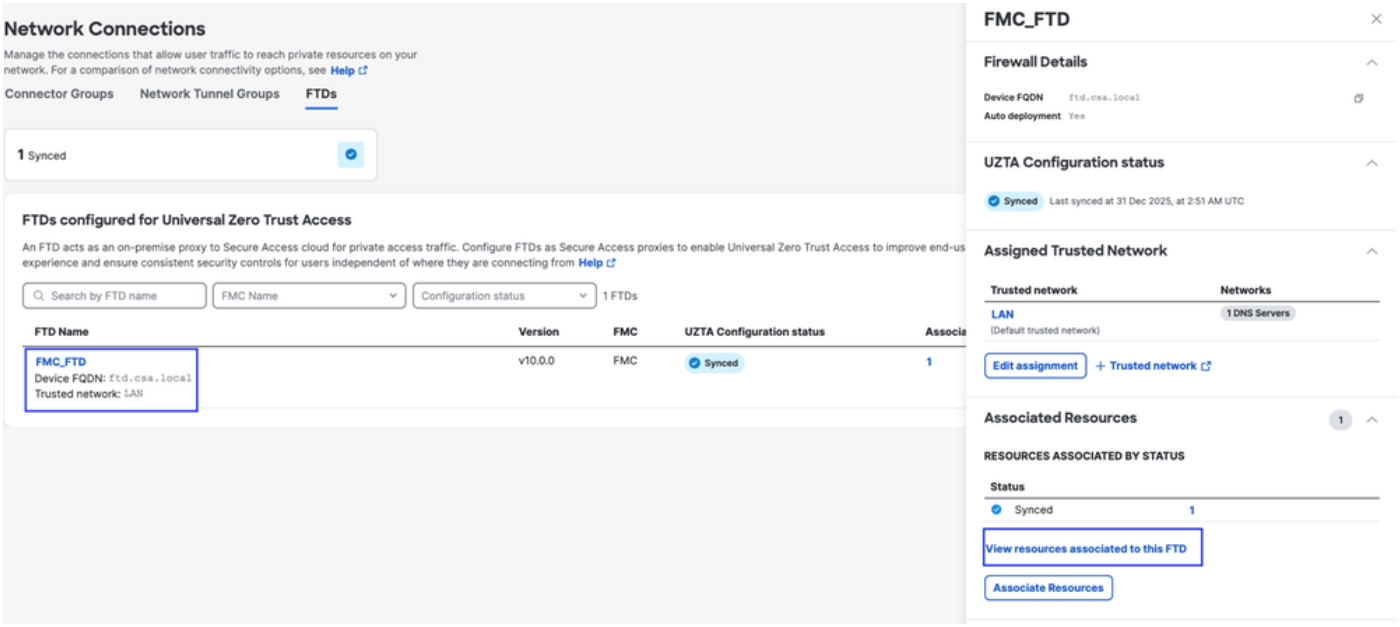
第3步 — 检验FTD上PR的关联

1.导航到连接>网络连接> FTD



安全访问 — PR验证

2. 单击FTD > View resources associated to this FTD



安全访问 — PR验证

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

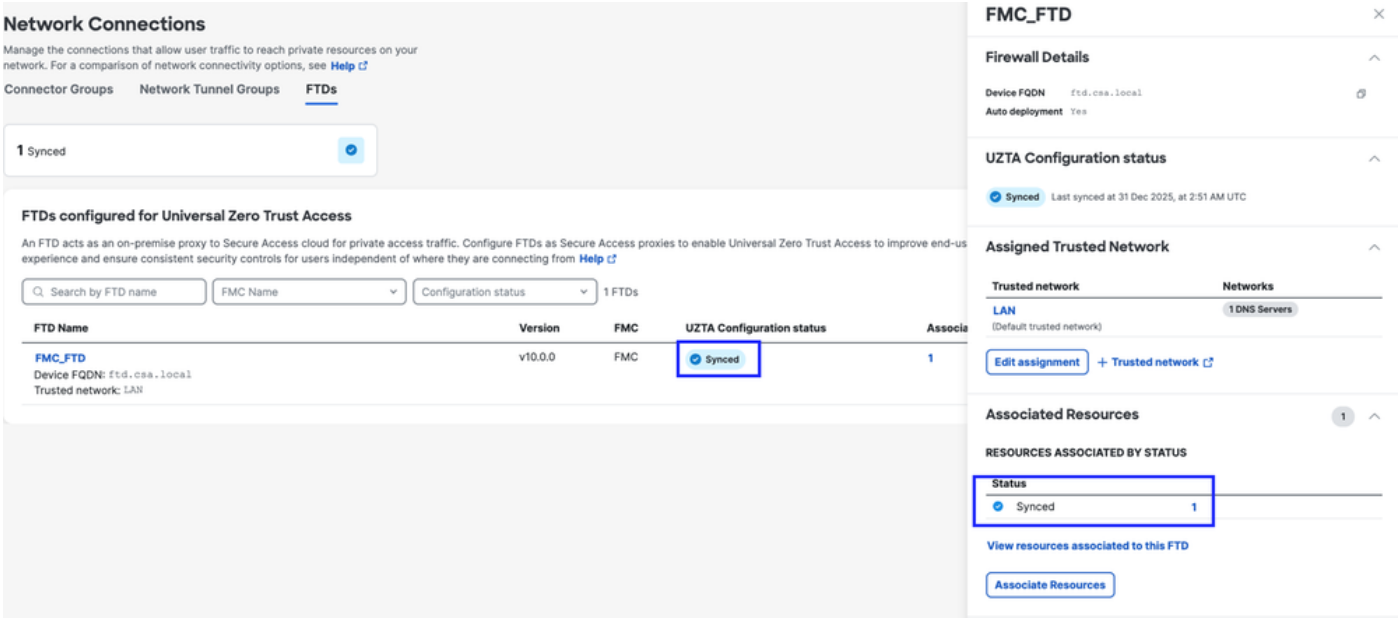
Resource name	Status
Router1	Synced

Close

安全访问 — PR验证

3. 单击close

4.验证状态、关联的资源和配置是否应该处于“同步”状态



安全访问 — PR验证

5.检验配置是否已推送到FTD

登录到FTD cli并导航到LINA模式

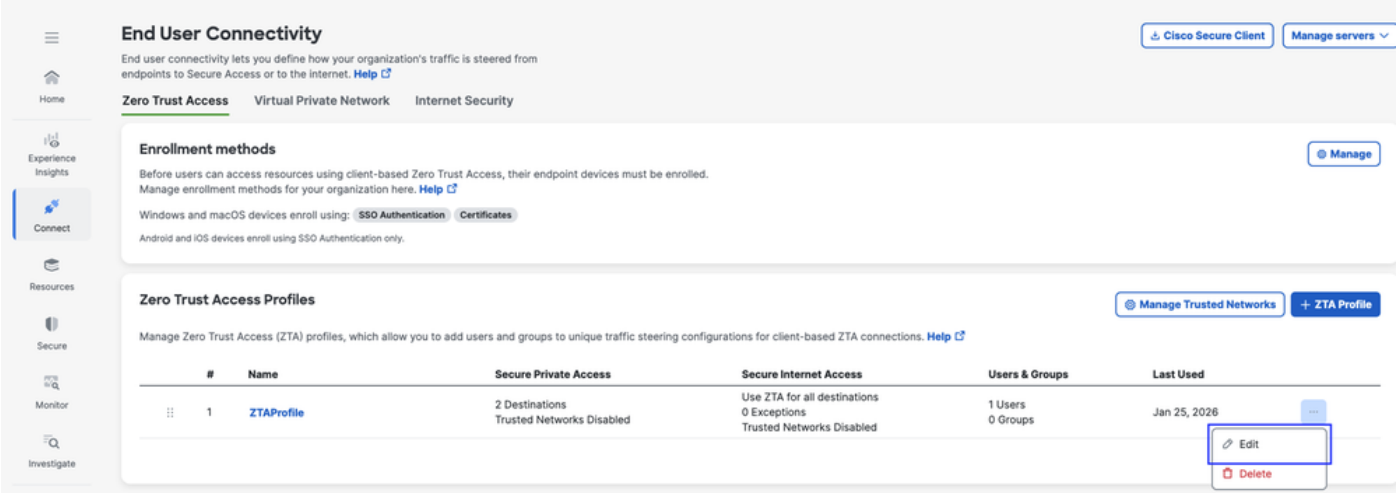
show running-config object application

```
> 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验证

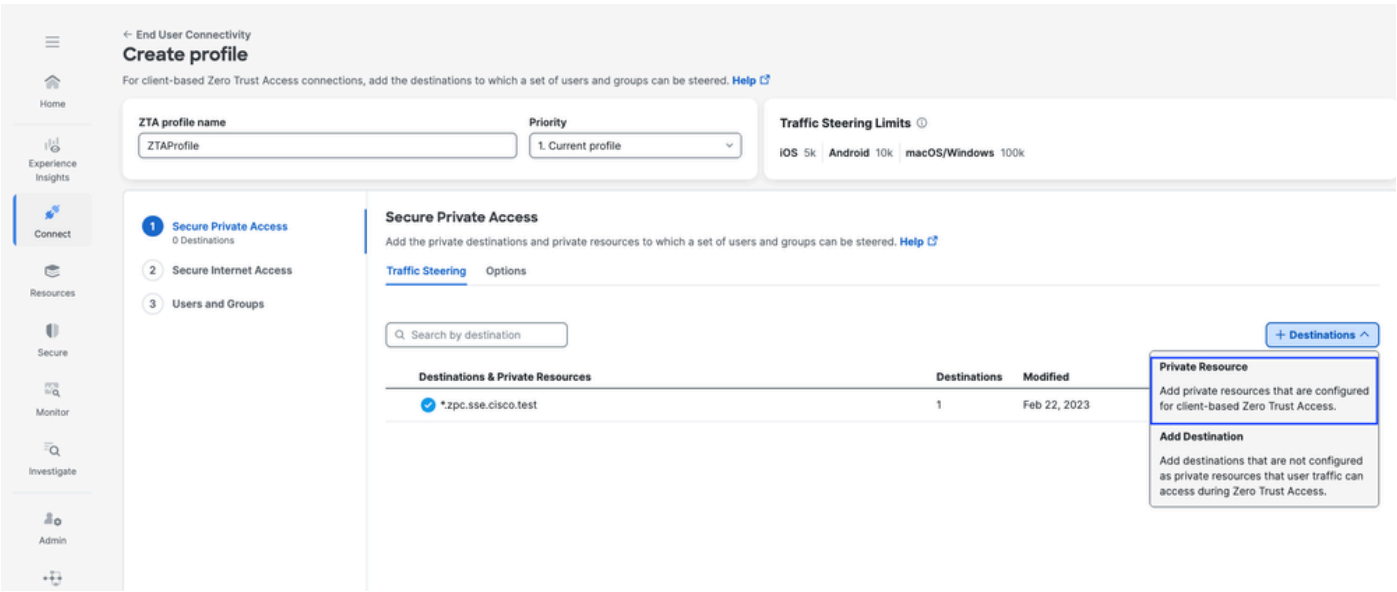
第4步 — 将私有资源添加到ZTA配置文件

1.导航到Connect > End User Connectivity > Zero Trust Access，然后单击3个点以编辑ZTA配置文件

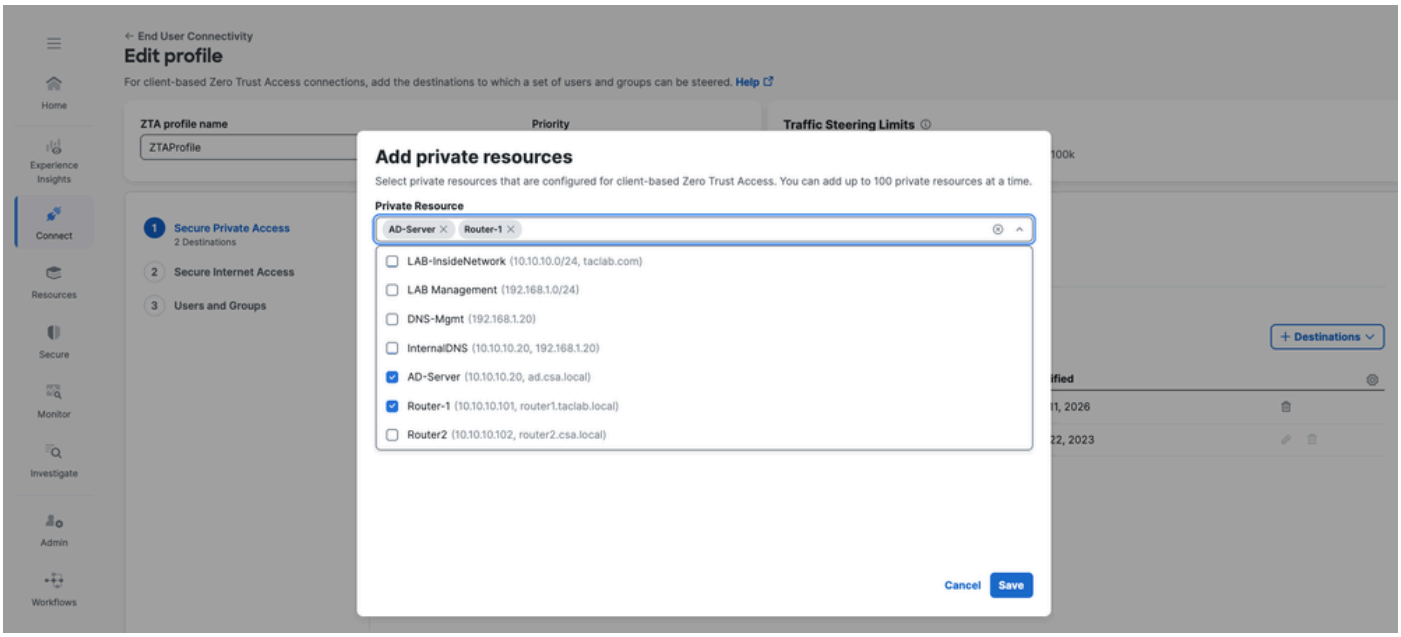


安全访问 — ZTA配置文件

2.添加专用资源

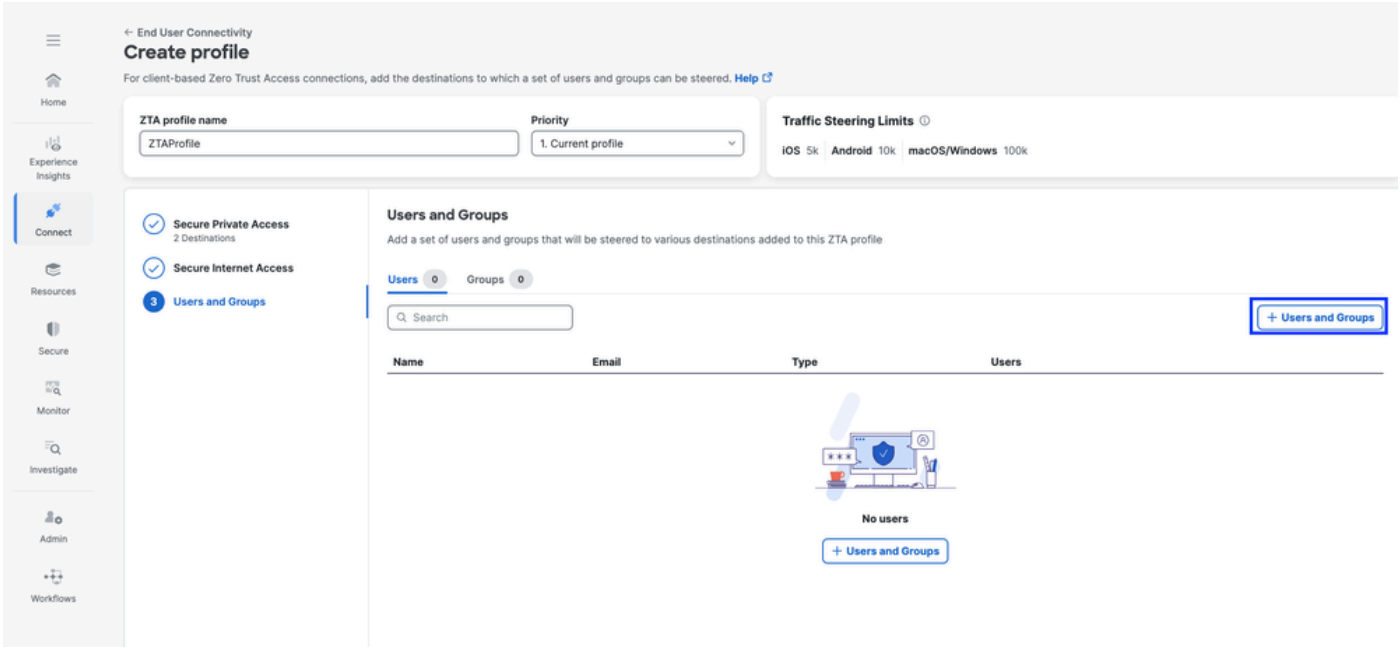


安全访问 — ZTA配置文件

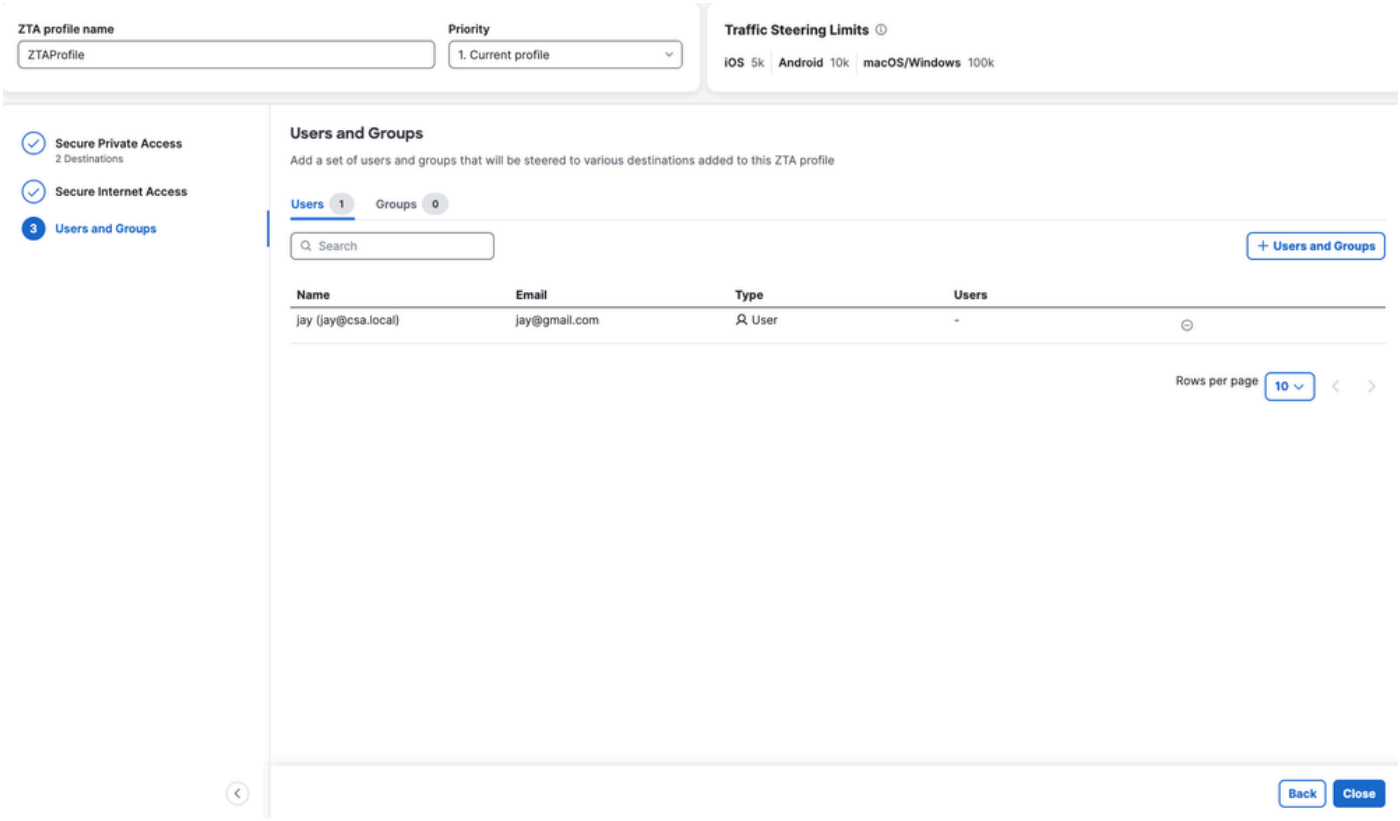


安全访问 — ZTA配置文件

3.添加用户和组



安全访问 — ZTA配置文件



安全访问 — ZTA配置文件

步骤 — 5检验对专用资源的访问

1. 验证远程用户可以解析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
```

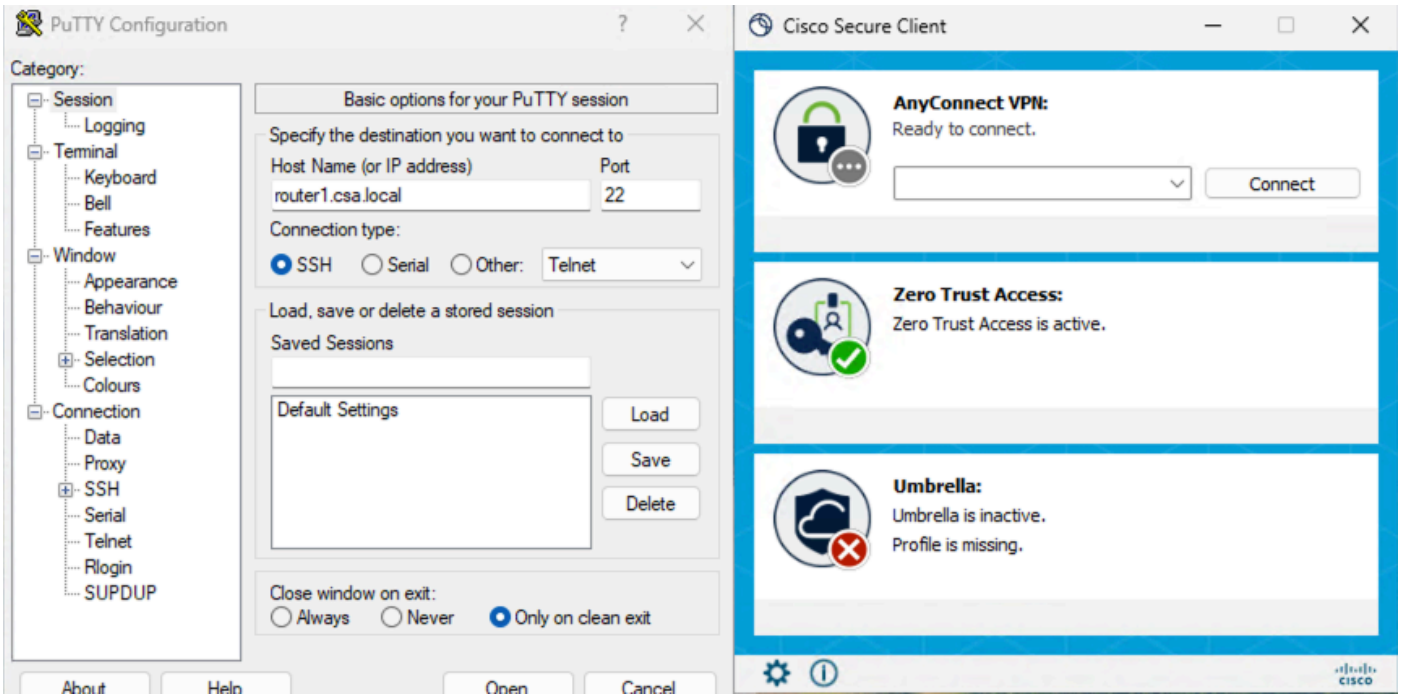
2.验证FTD是否可以使用FQDN访问私有资源

```
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#
```

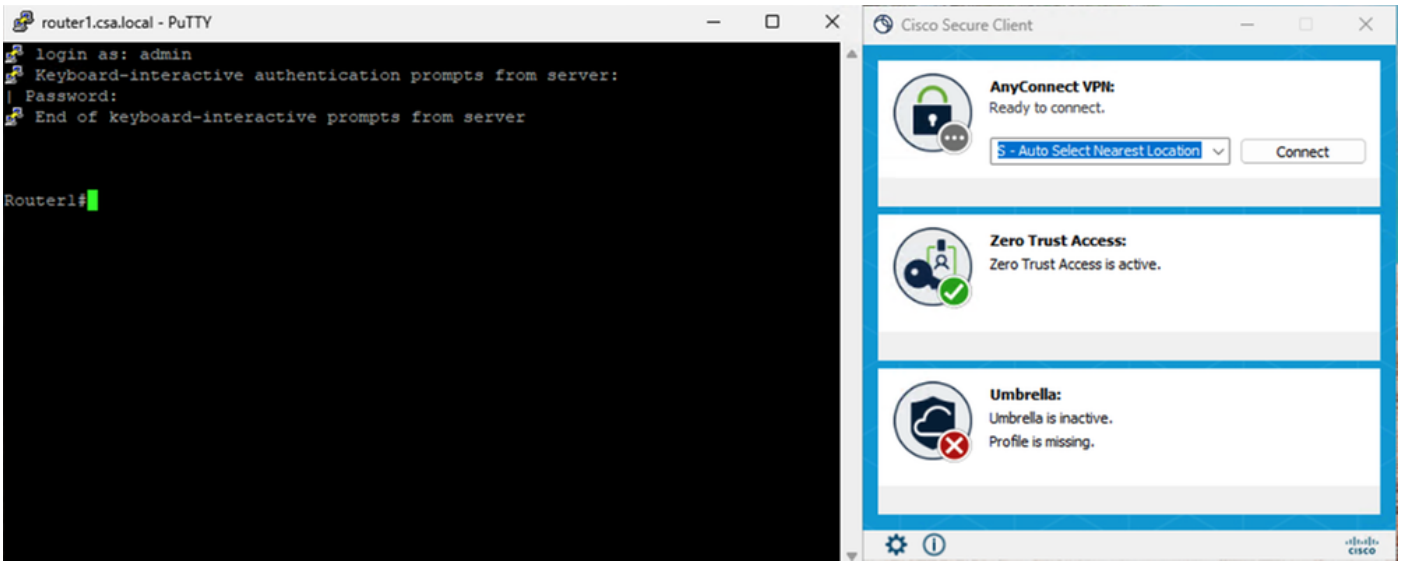
安全访问 — PR测试

3. 测试与专用资源的SSH连接

使用FQDN访问PR

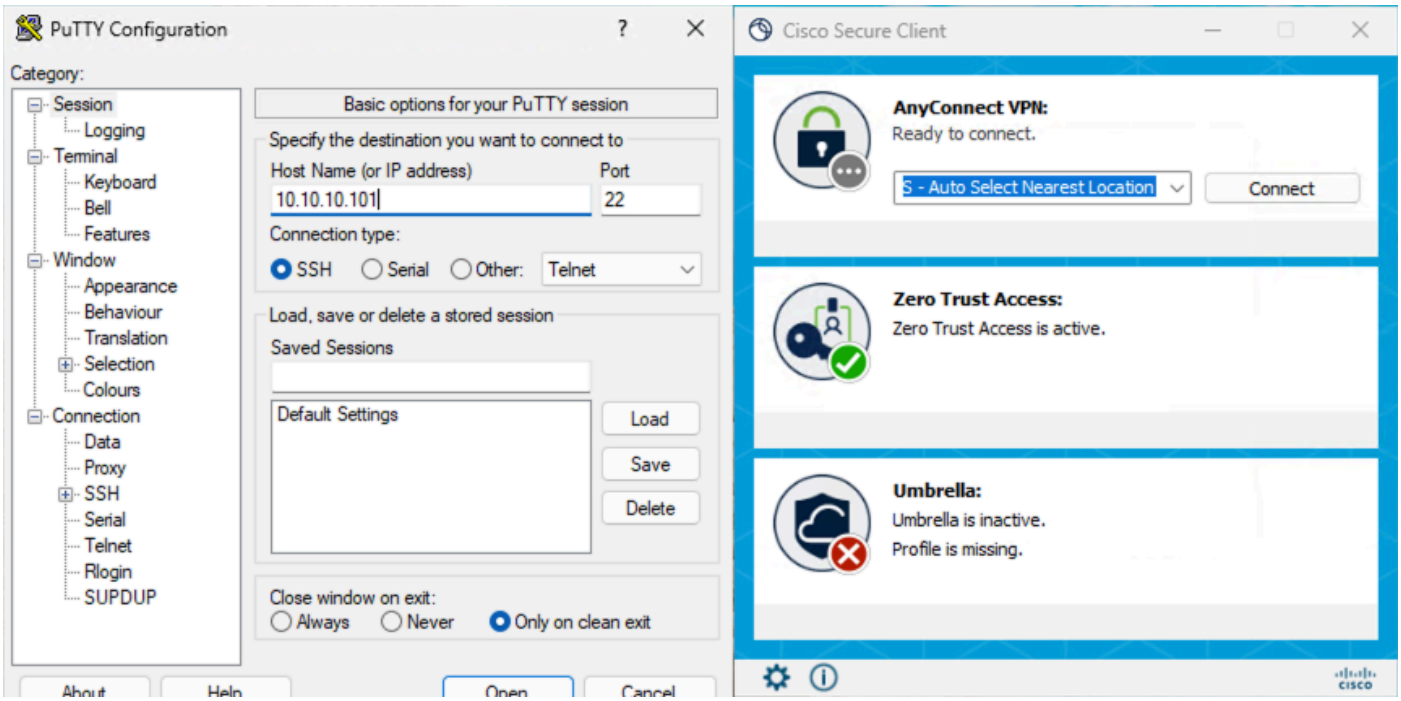


安全访问 — PR测试

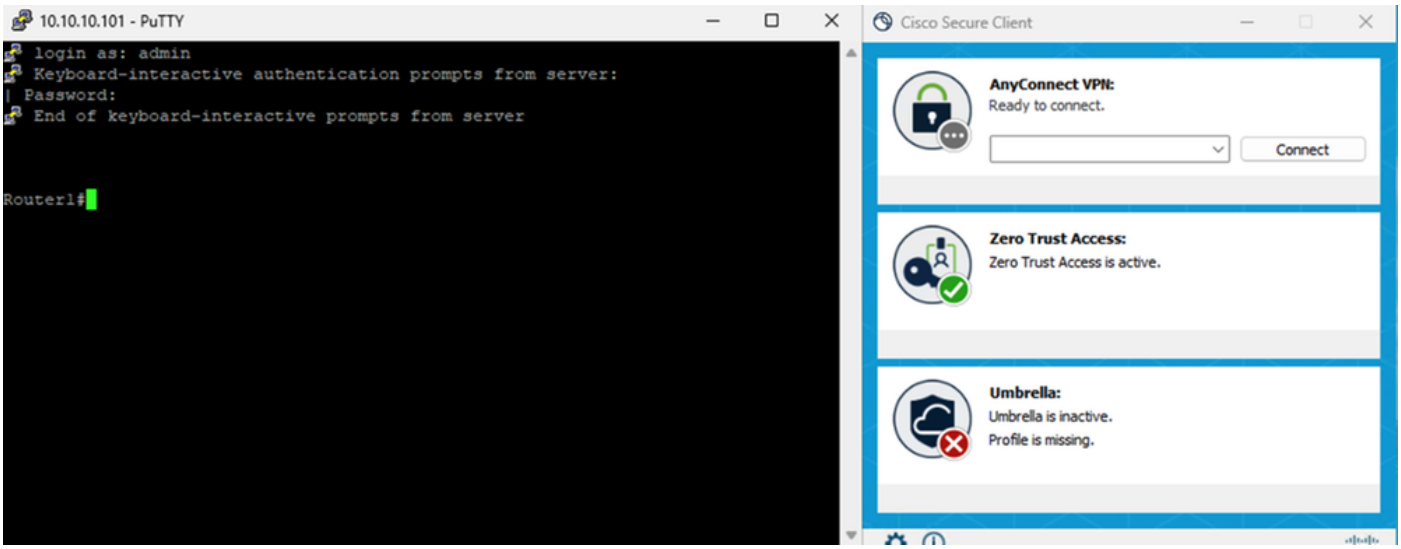


安全访问 — PR测试

使用IP地址访问PR

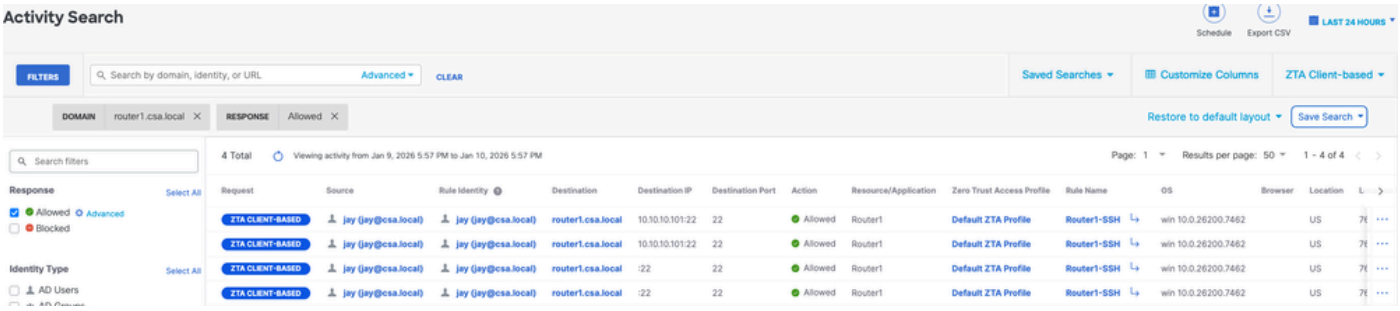


安全访问 — PR测试

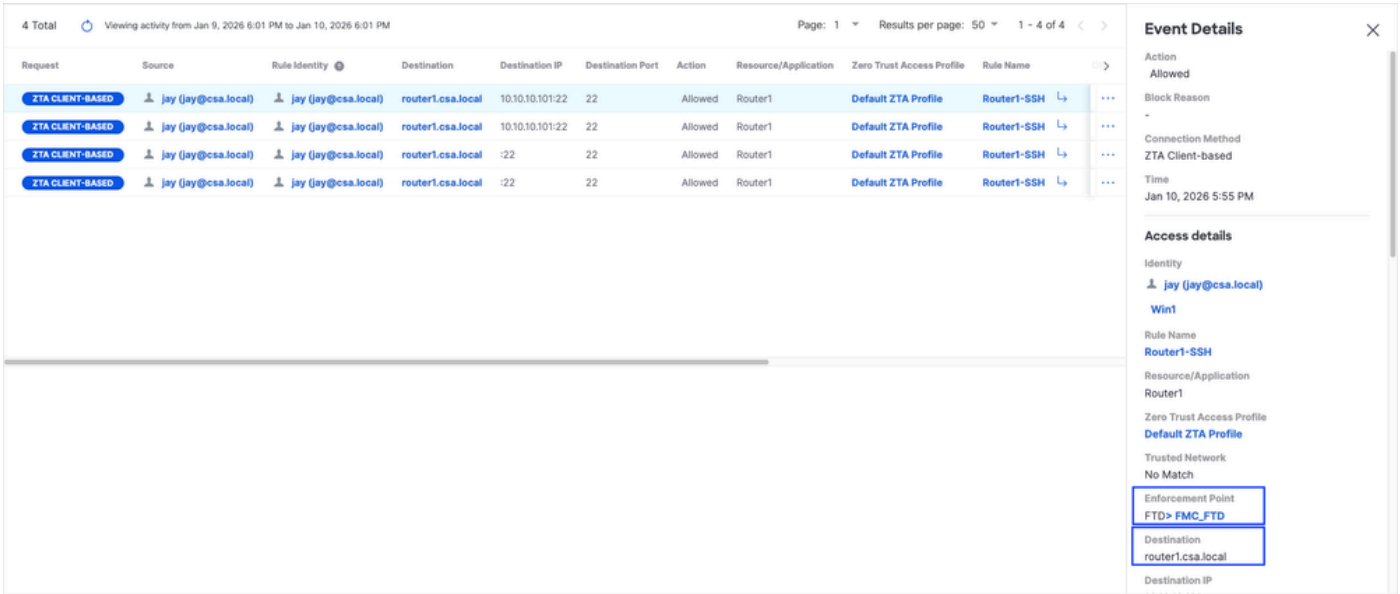


安全访问 — PR测试

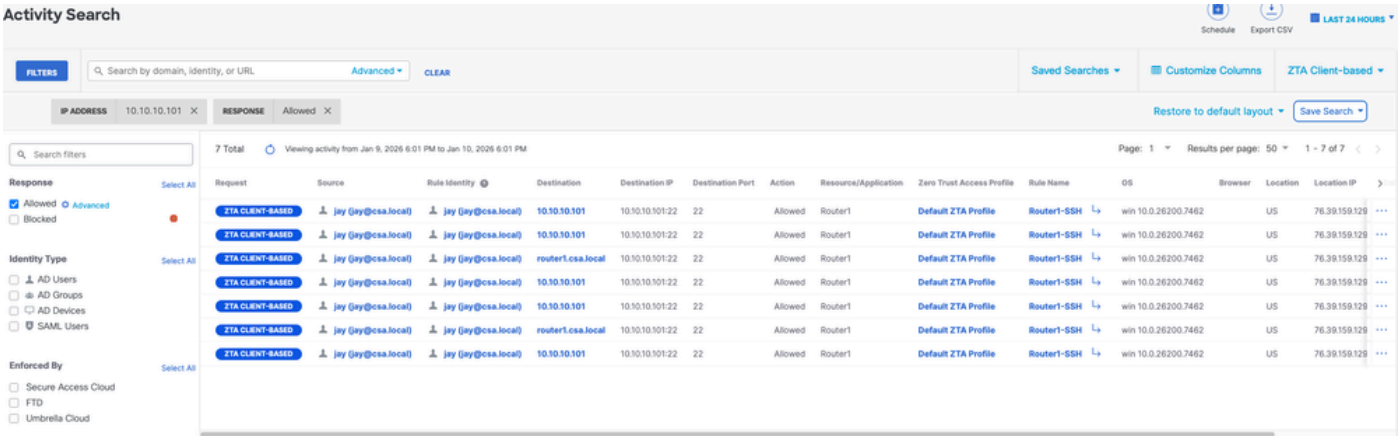
4. 验证安全访问活动搜索日志



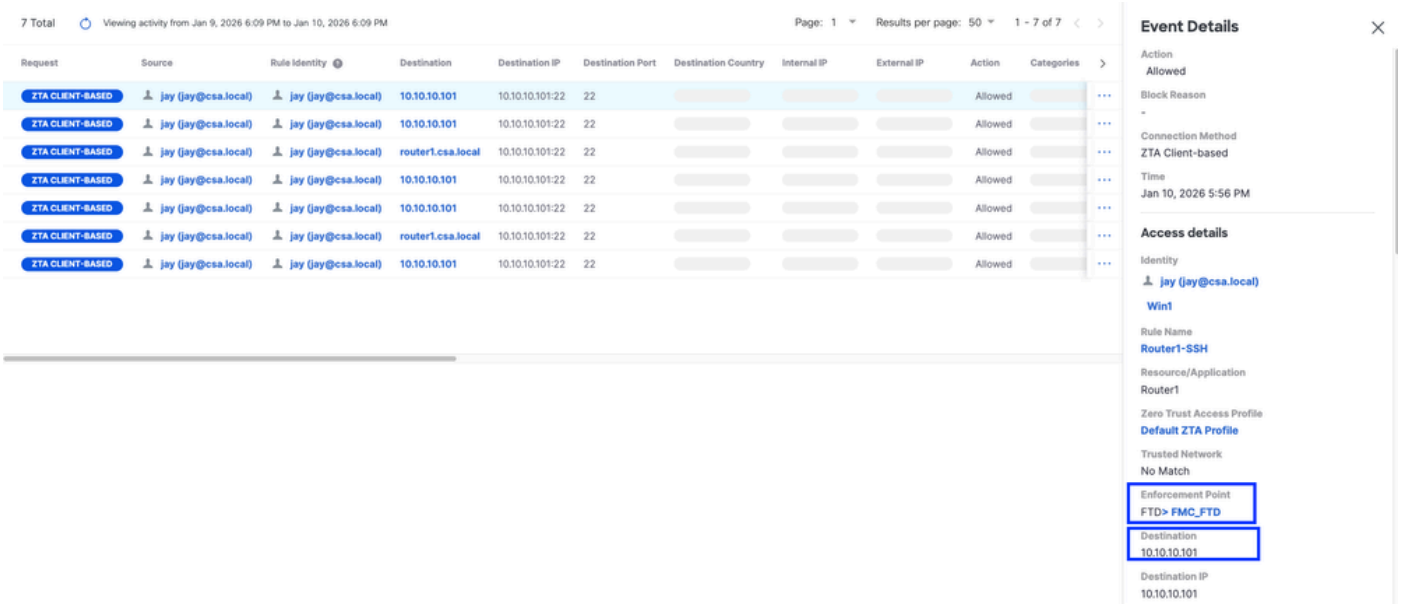
安全访问 — 活动搜索



安全访问 — 活动搜索

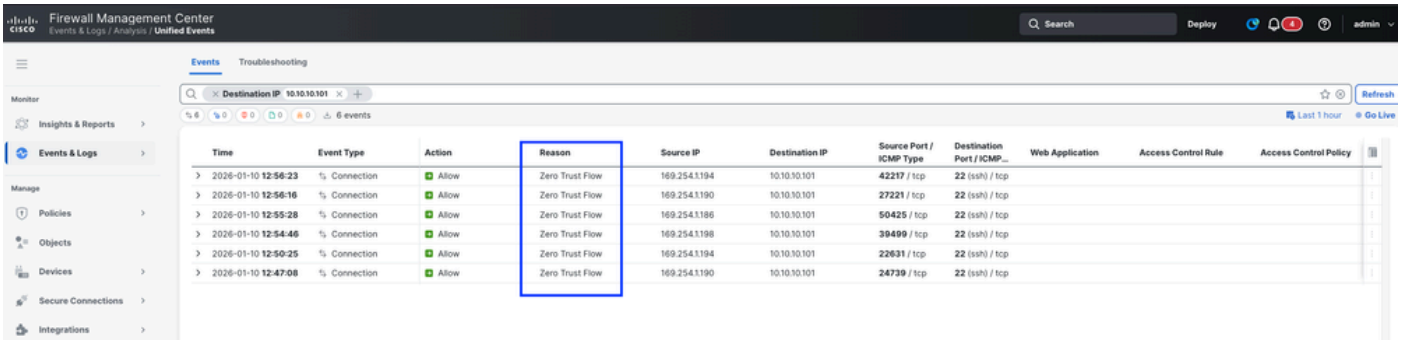


安全访问 — 活动搜索



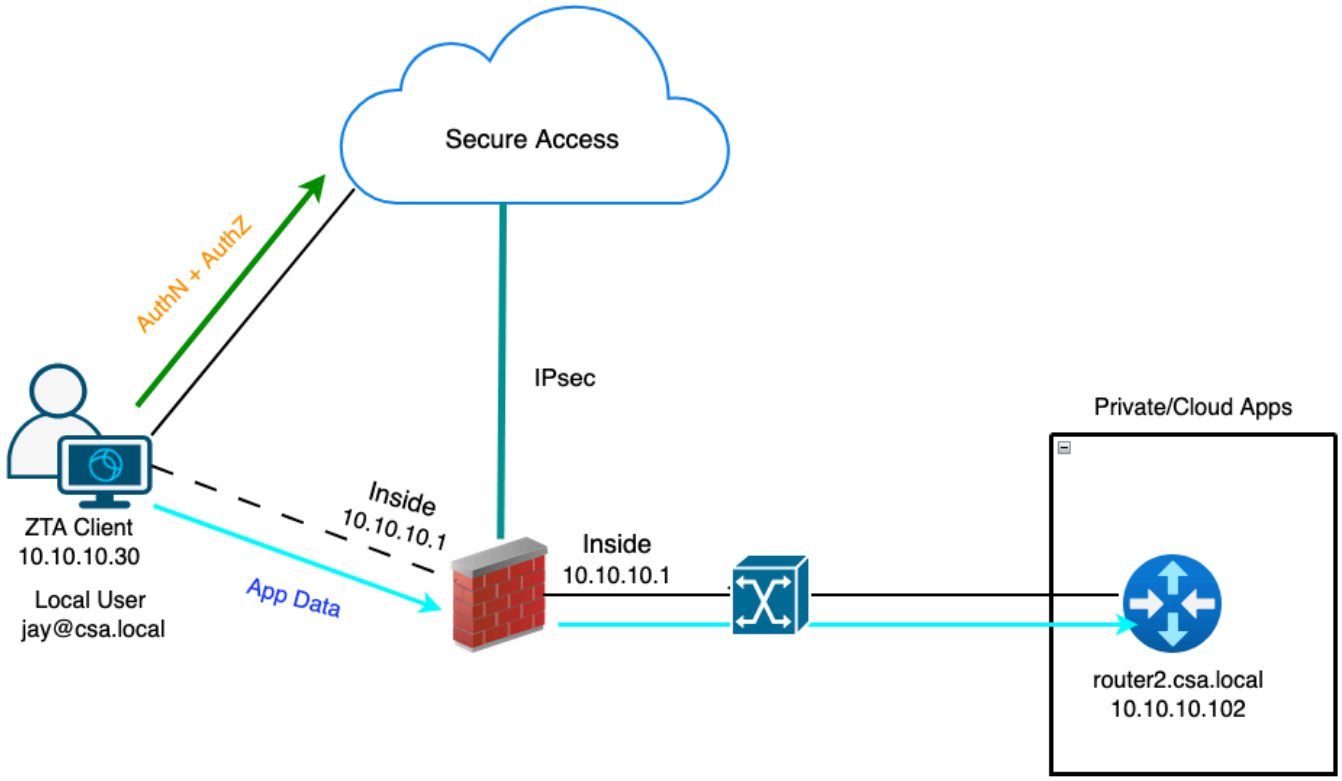
安全访问 — 活动搜索

5. 验证FMC连接事件



测试案例3 — 本地用户 — 本地实施

通过本地实施作为本地用户访问私有资源，这种类型的实施策略评估在安全访问上进行，但应用数据对FTD保持本地状态。例如，ZTA注册客户端或连接到家庭网络的用户，并尝试访问FTD内部接口后面的私有资源。如果私有资源位于DMZ或FTD的任何其他接口之后，则我们必须在FTD上创建访问规则以允许客户端IP或网络和私有资源之间的流量。

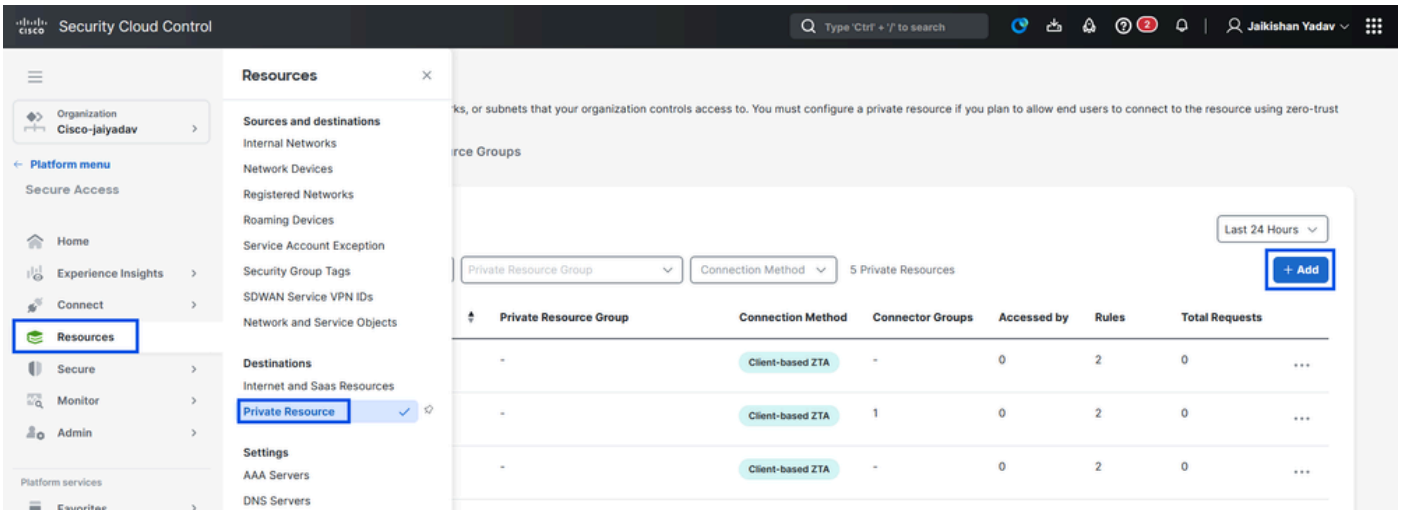


通用ZTA — 测试用例拓扑

第1步 — 在安全访问中定义私有资源

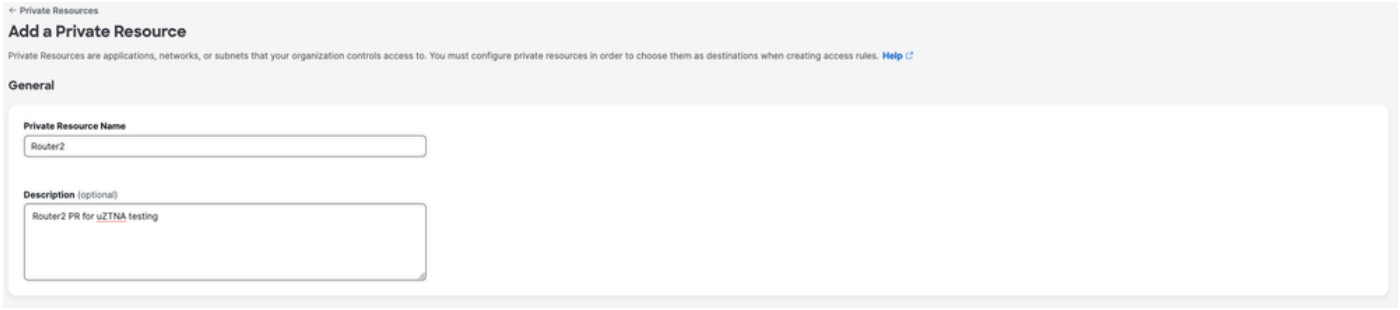
配置私有资源，使其可通过云实施的零信任访问(ZTA)注册设备访问

1. 导航到资源 > 目标 > 专用资源 >单击+添加



安全访问 — 私有资源配置

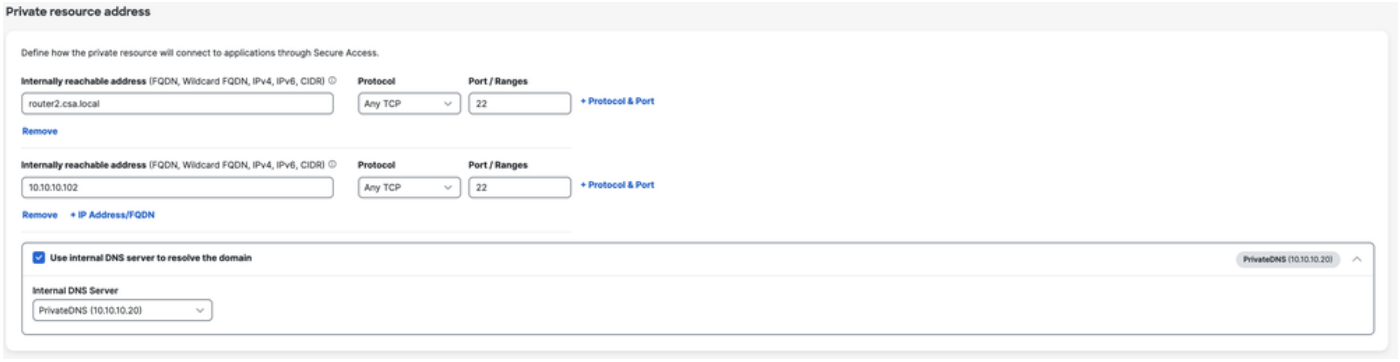
2.对于专用资源名称，输入资源有意义的名称。对于Description，建议您提供诸如资源用途或资源所有者名称等信息。



安全访问 — 私有资源配置

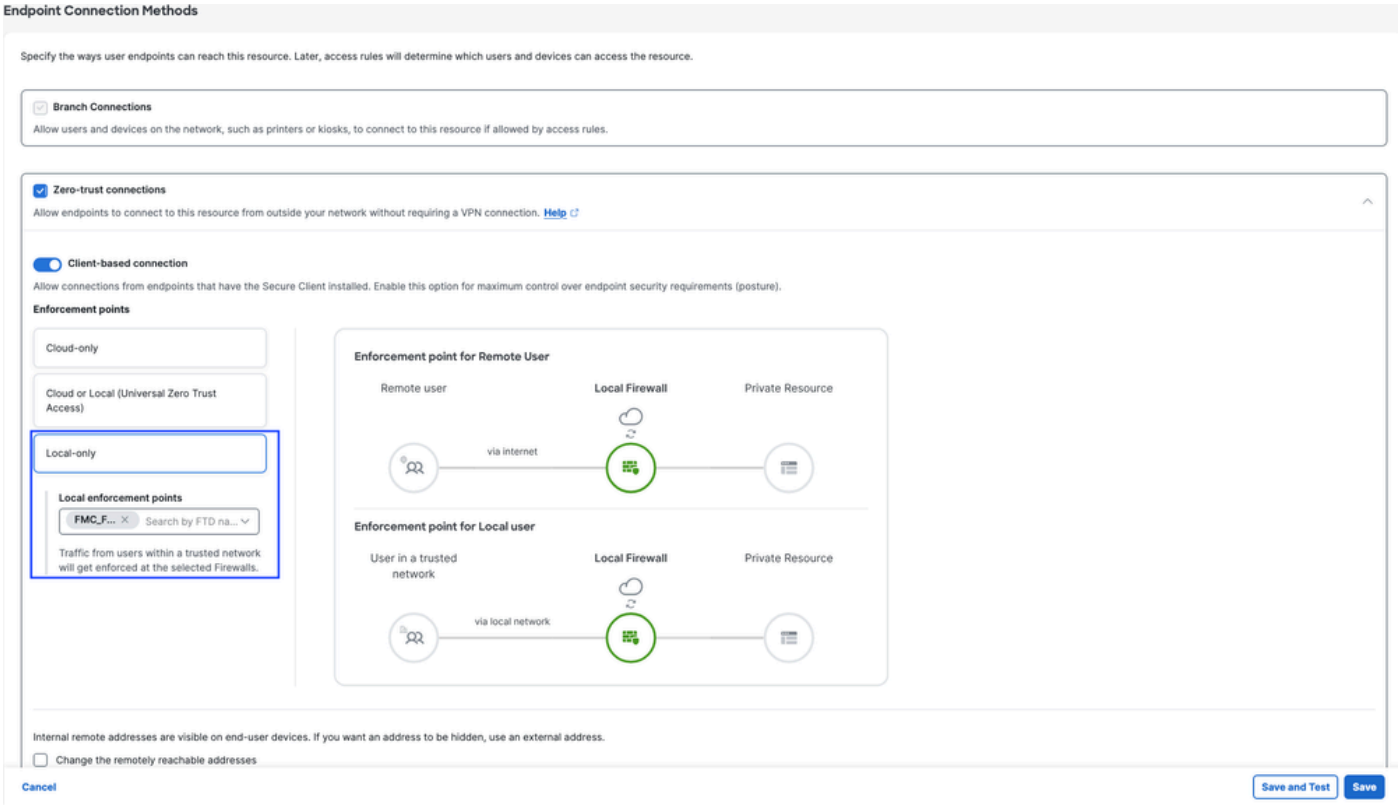
3.输入要访问的专用资源的FQDN。我们还可以定义私有资源的IP地址。有关详细信息，请参阅[添加专用资源]

4.选择要解析域的内部DNS服务器



5. 选择终端连接方法

6.选择FTD作为本地实施点



安全访问 — 私有资源配置

注意：根据您选择的注册类型，此更改将自动将PR与FTD关联并触发策略部署

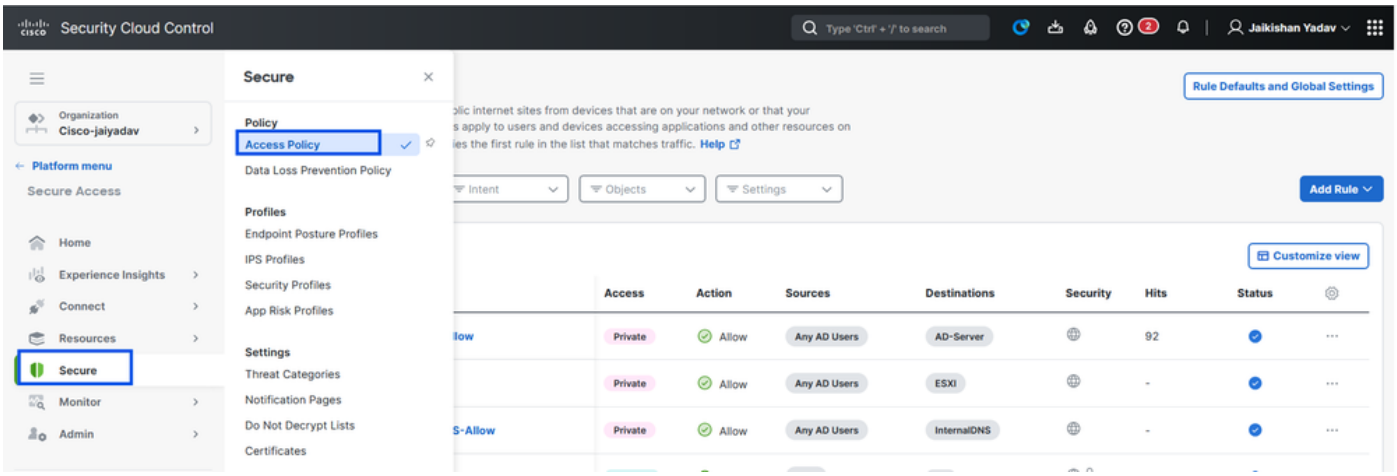
---

7. 点击保存

第2步 — 创建专用访问规则

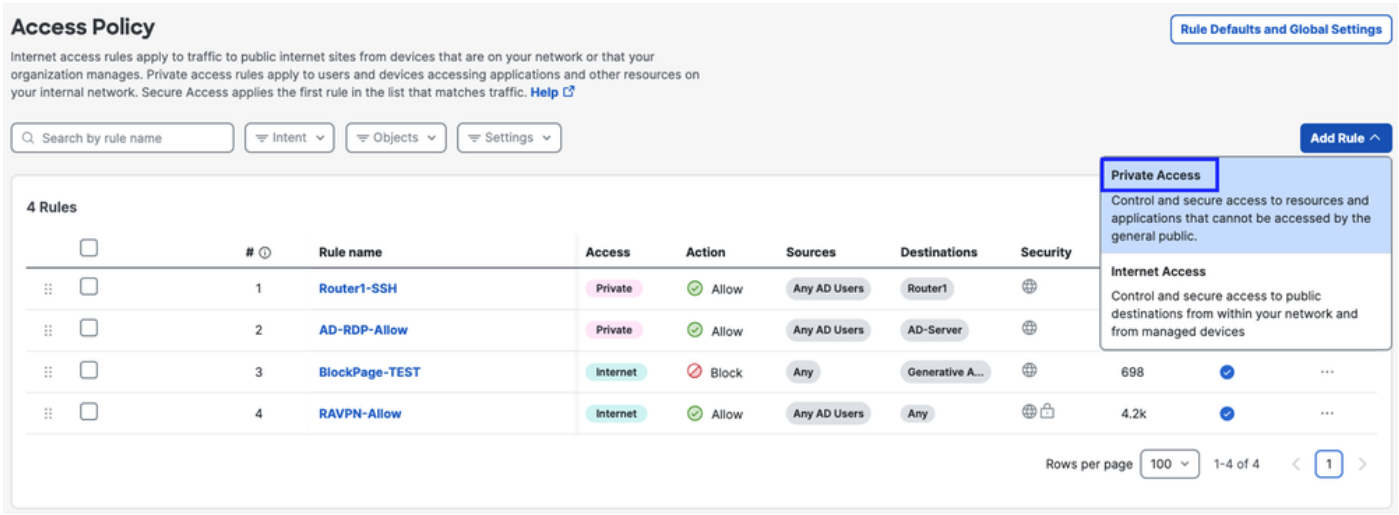
在Secure Access上配置私有访问，以便由通用ZTA注册用户访问。有关详细信息，请参阅专用访问规则

1. 导航到安全>访问策略



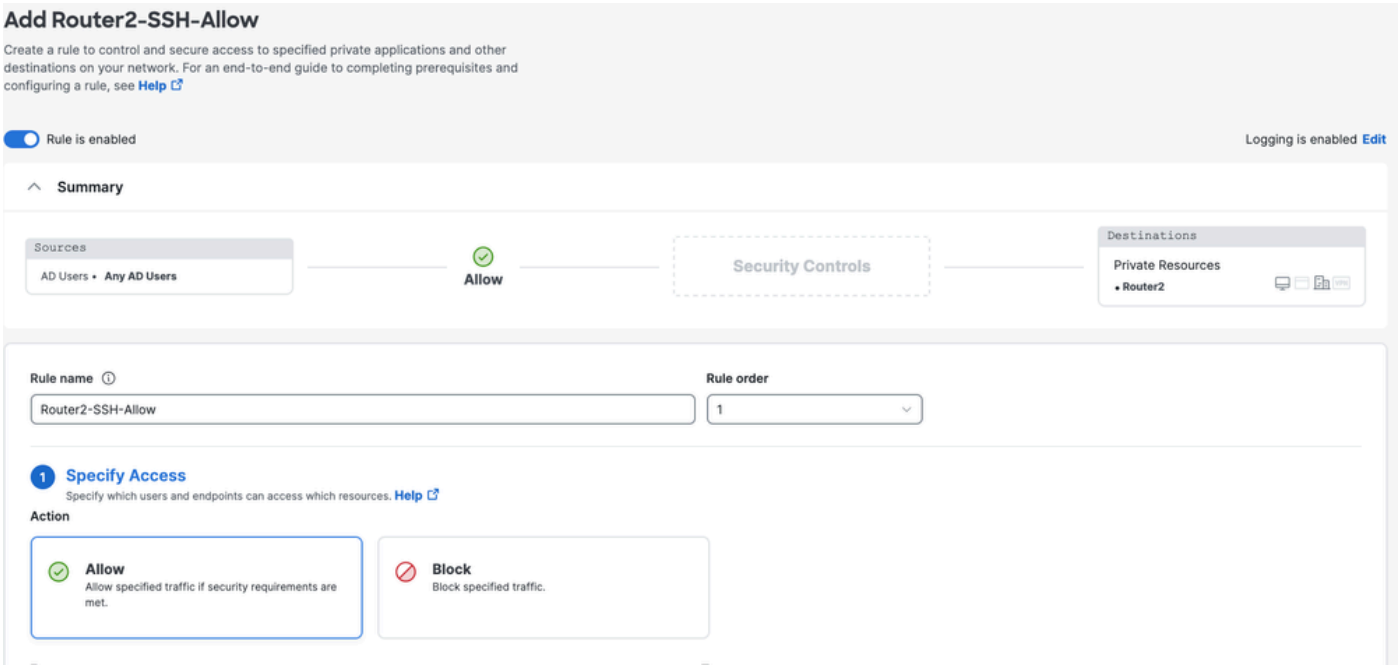
安全访问 — 访问策略配置

2.单击Add Rule，然后选择Private Access。
规则顶部是描述规则已配置组件的摘要。



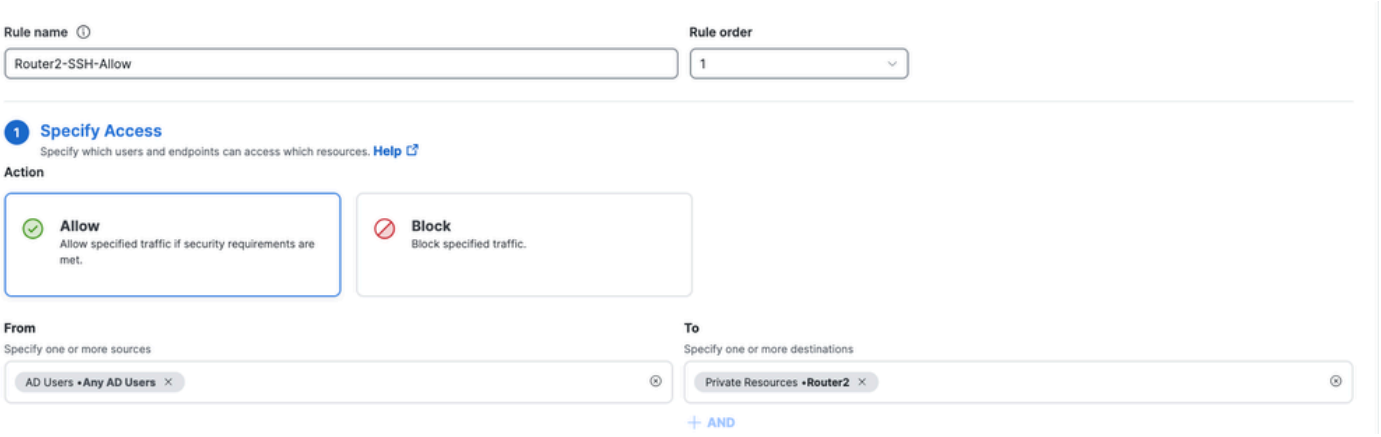
安全访问 — 访问策略配置

3.添加规则名称



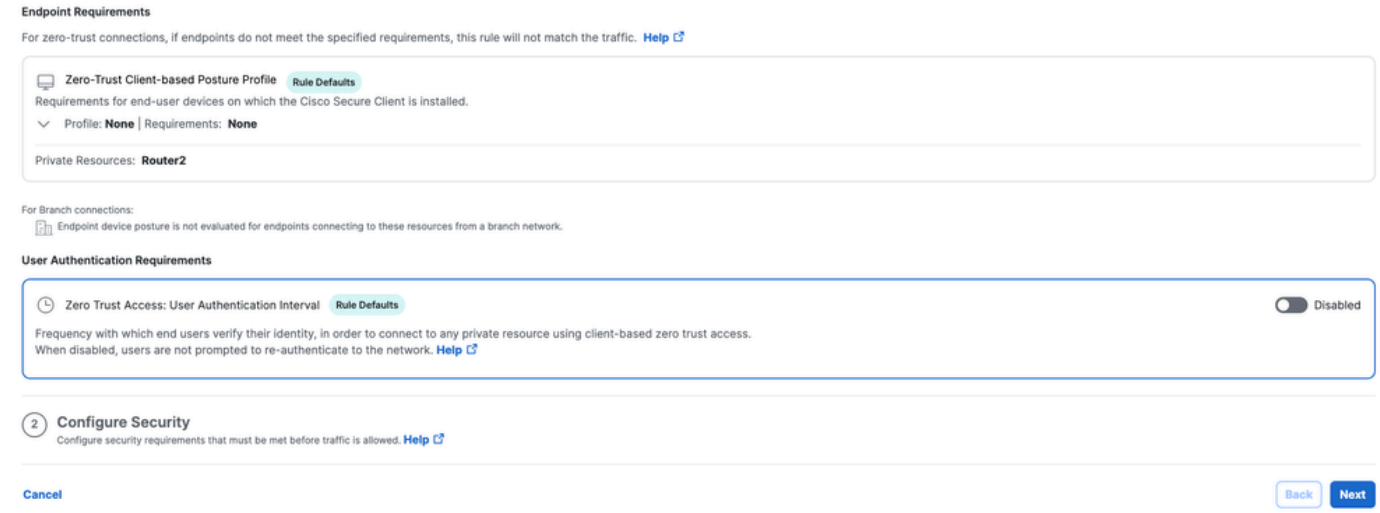
安全访问 — 访问策略配置

4.选择规则操作，然后选择来源和目标



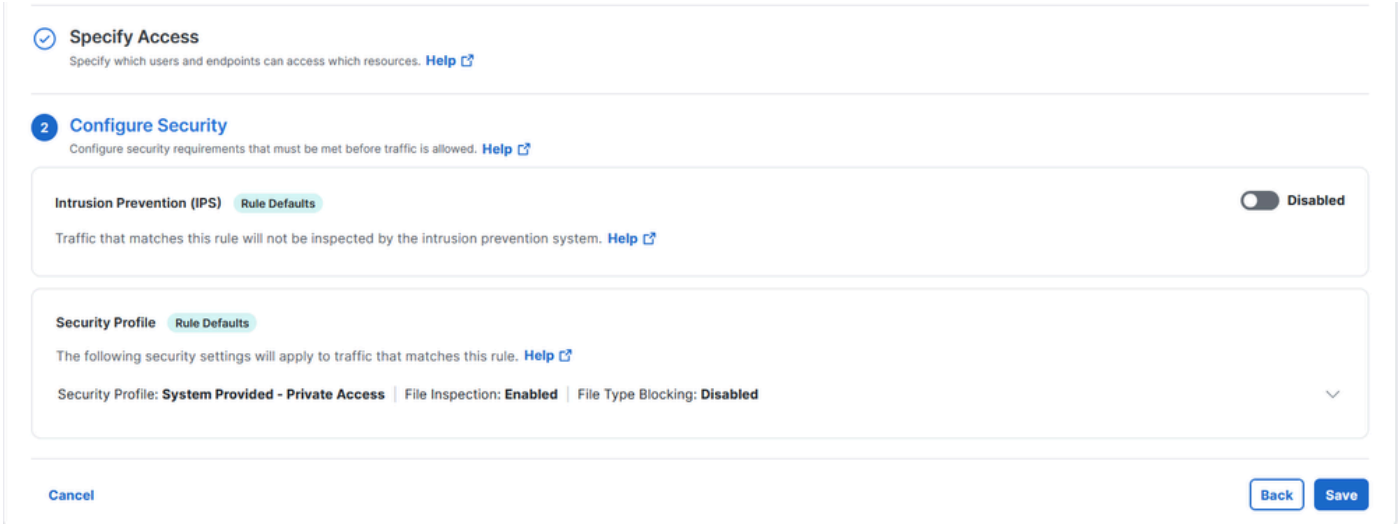
安全访问 — 访问策略配置

5.配置终端要求



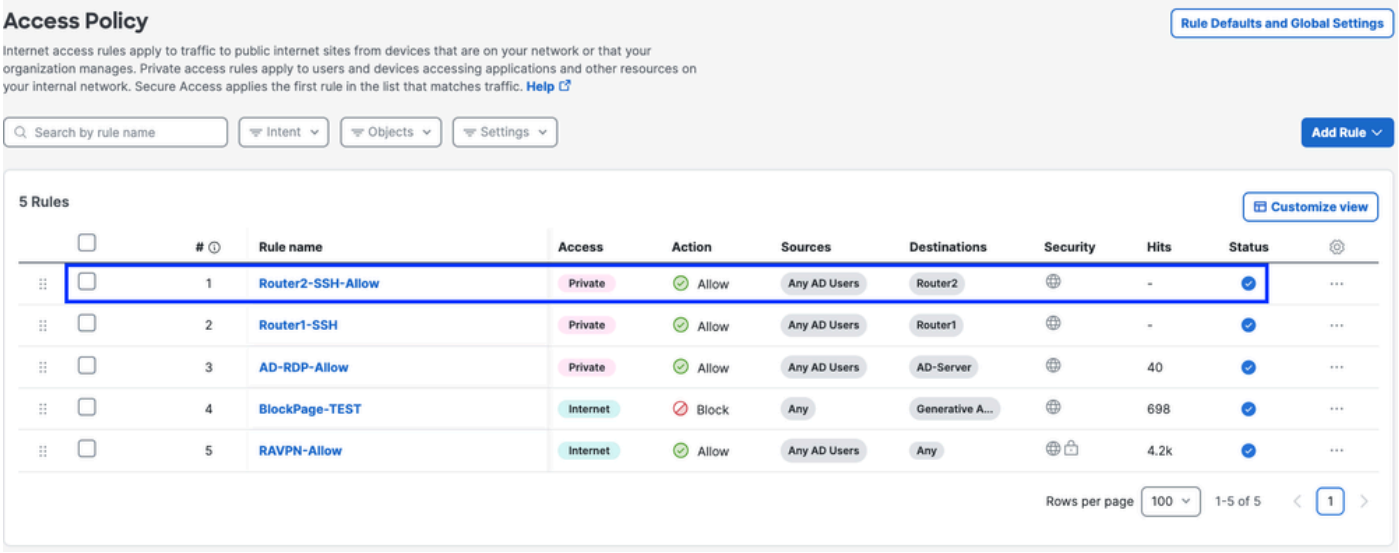
安全访问 — 访问策略配置

6. 配置安全性



安全访问 — 访问策略配置

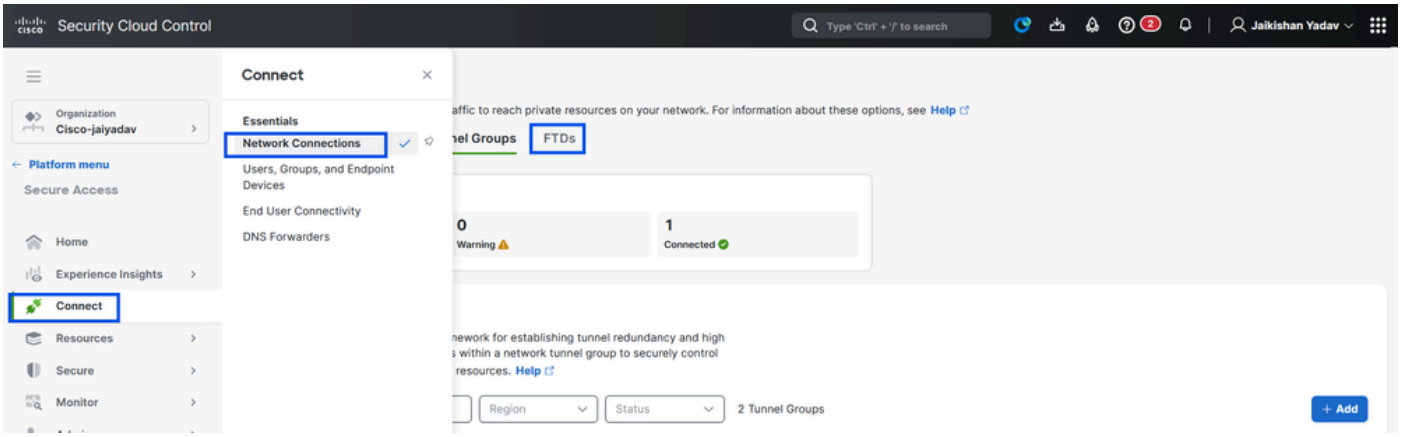
7.单击Save



安全访问 — 访问策略配置

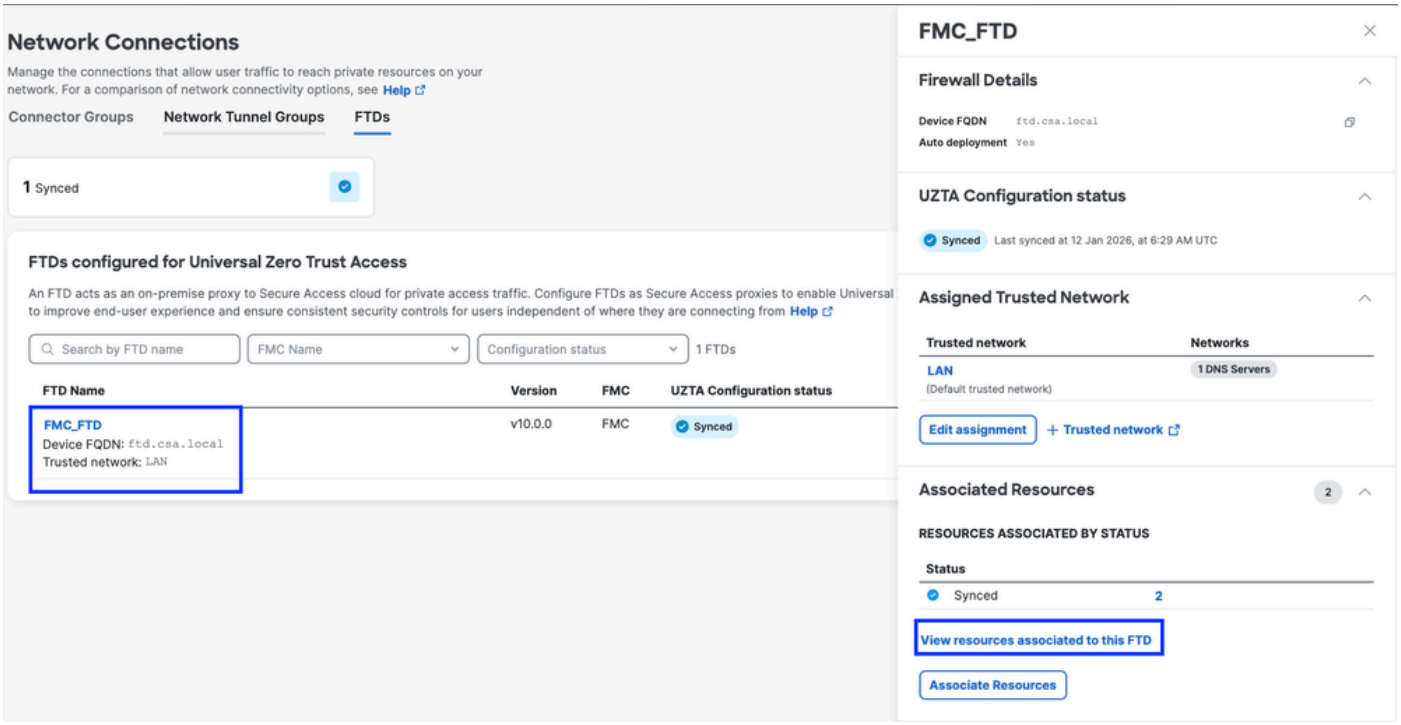
第3步 — 检验FTD上PR的关联

1.导航至connect > Network Connections > FTDs

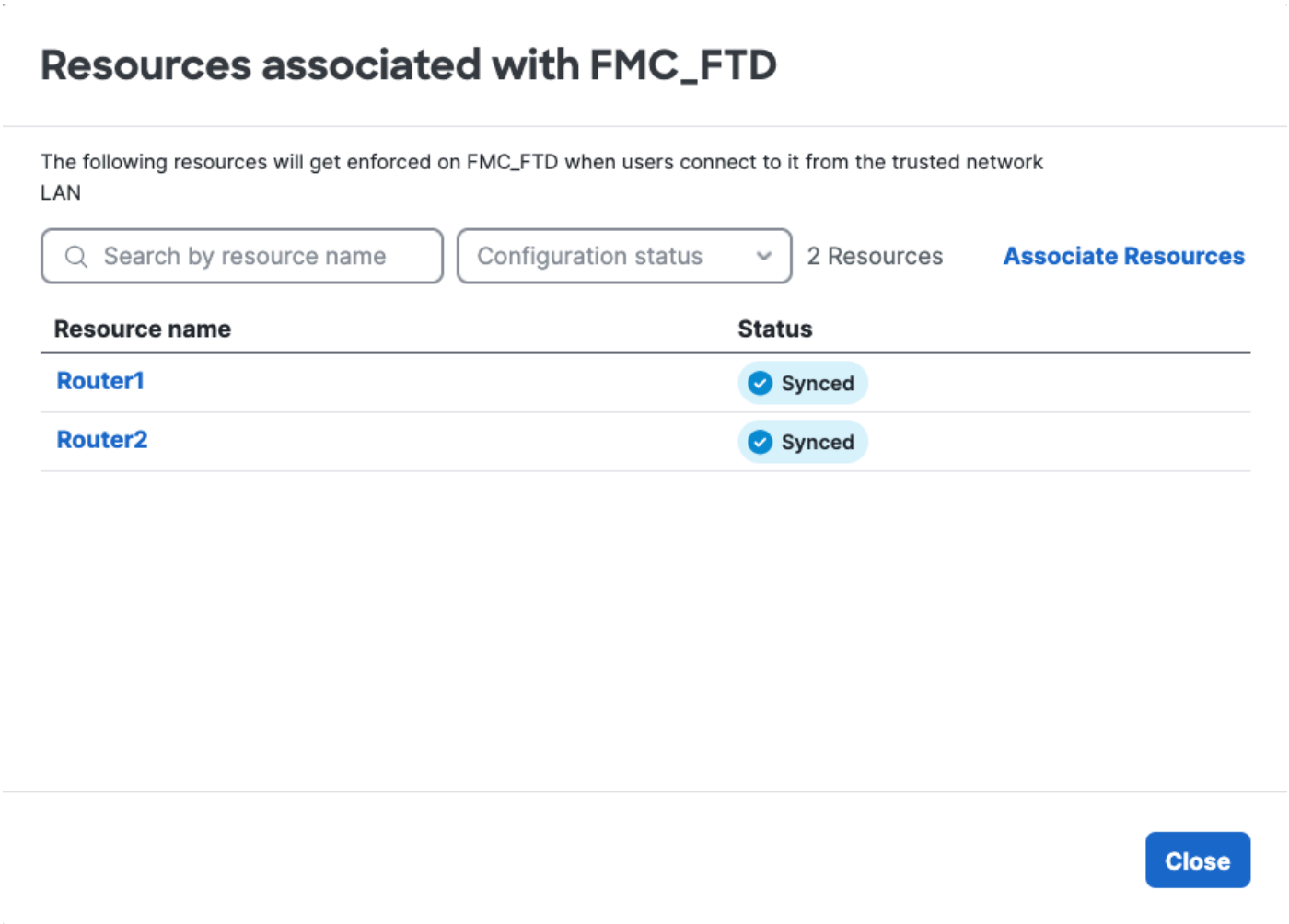


安全访问 — PR验证

2. 点击FTD >查看与此FTD关联的资源

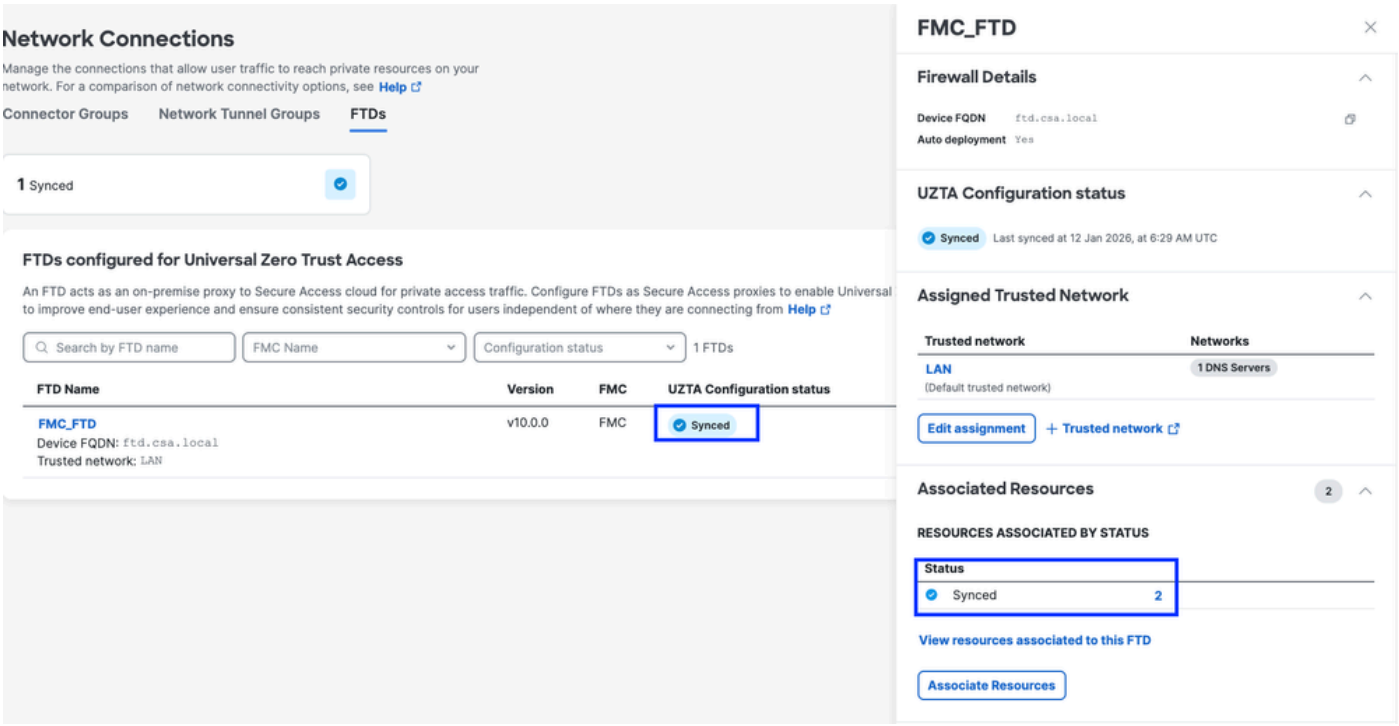

Network Connections
Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help
Connector Groups
Network Tunnel Groups
FTDs
1 Synced
FTDs configured for Universal Zero Trust Access
An FTD acts as an on-premise proxy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

安全访问 — PR验证


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. 单击close

4.验证状态、关联的资源和配置是否应该处于“同步”状态



安全访问 — PR验证

5.检验配置是否已推送到FTD

登录到FTD cli并导航到LINA模式

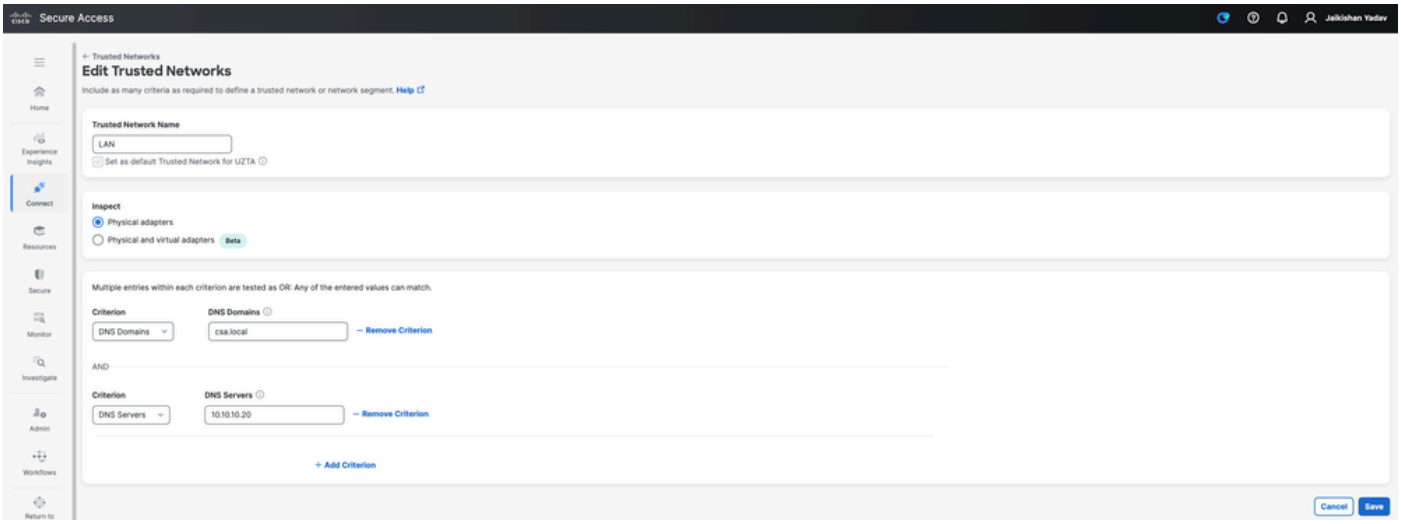
show running-config object application

```
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
```

安全访问 — PR验证

第–4步配置“管理受信任网络或ZTA设置”

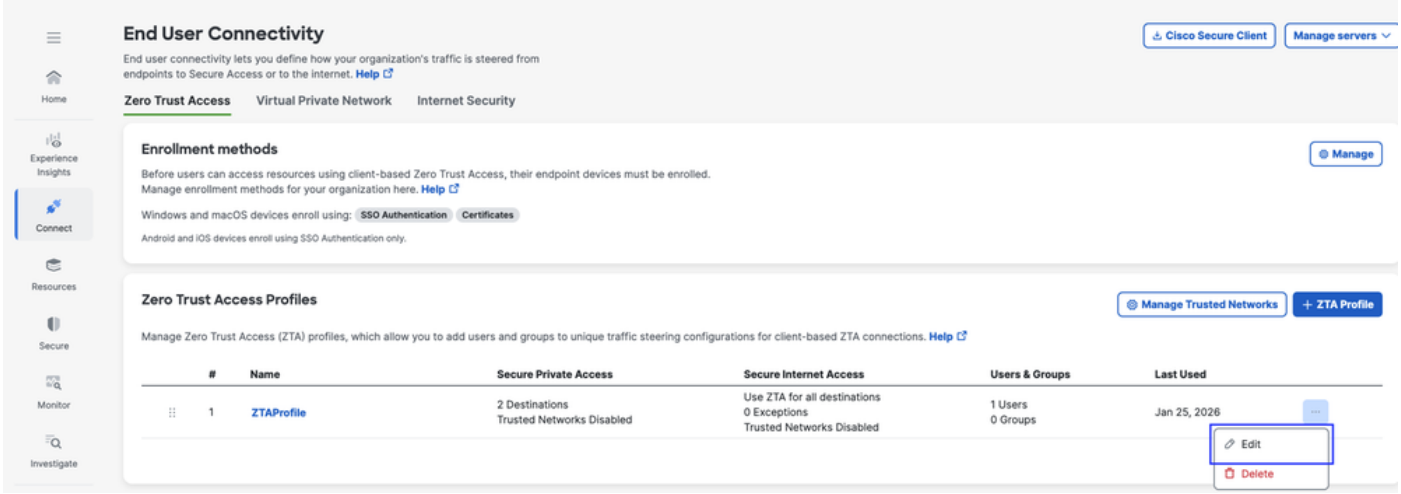
导航到Connect > End User Connectivity > Zero Trust Access > ZTA Settings并配置受信任网络



安全访问 — TND配置

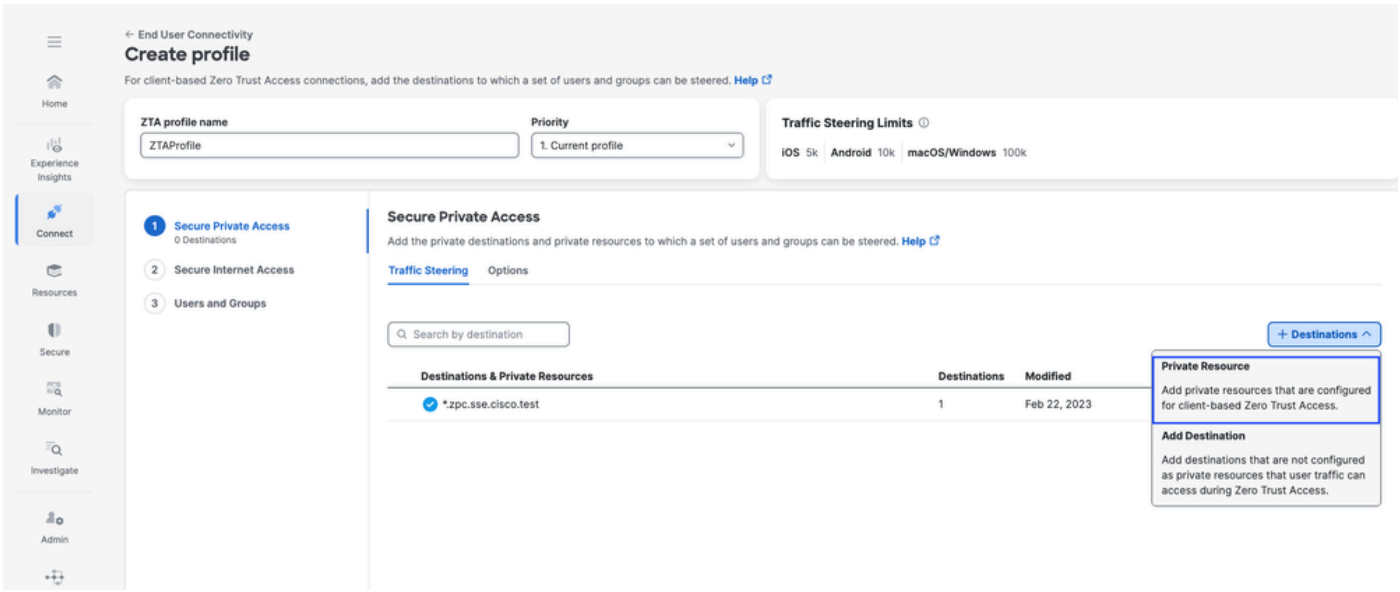
第–5步将私有资源添加到ZTA配置文件

1.导航到Connect > End User Connectivity > Zero Trust Access，然后单击3个点以编辑ZTA配置文件

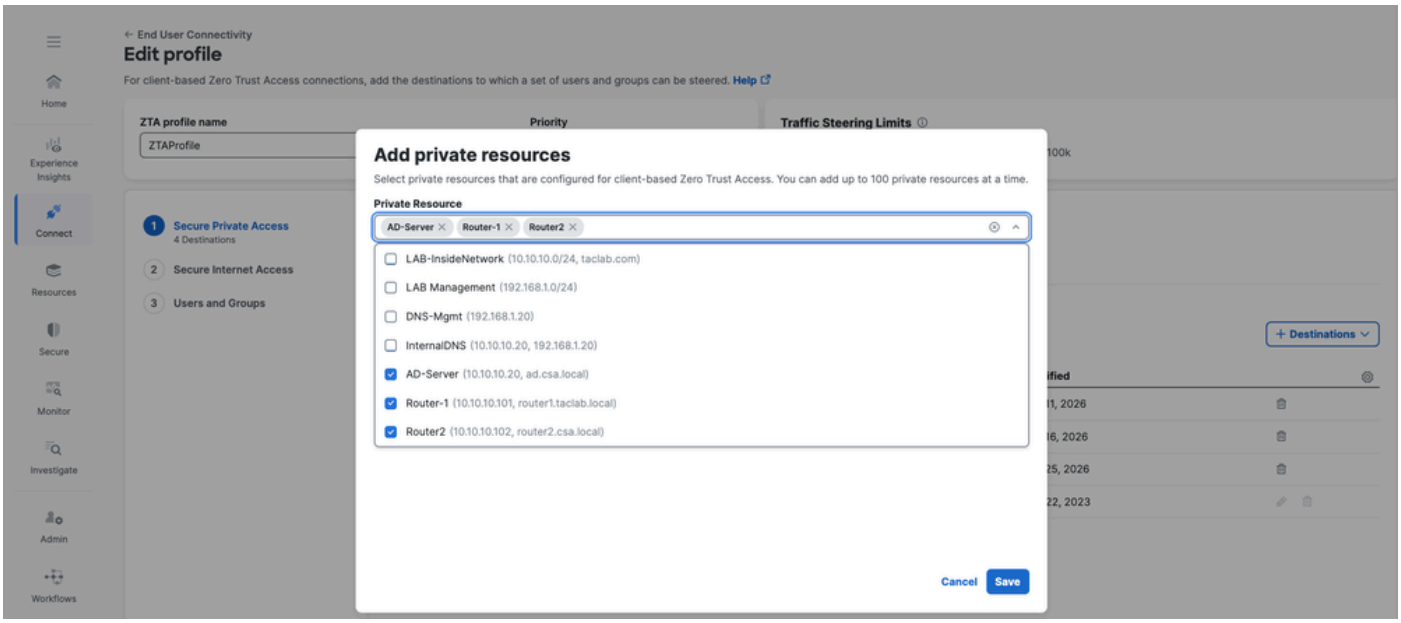


安全访问 — ZTA配置文件

2.添加专用资源

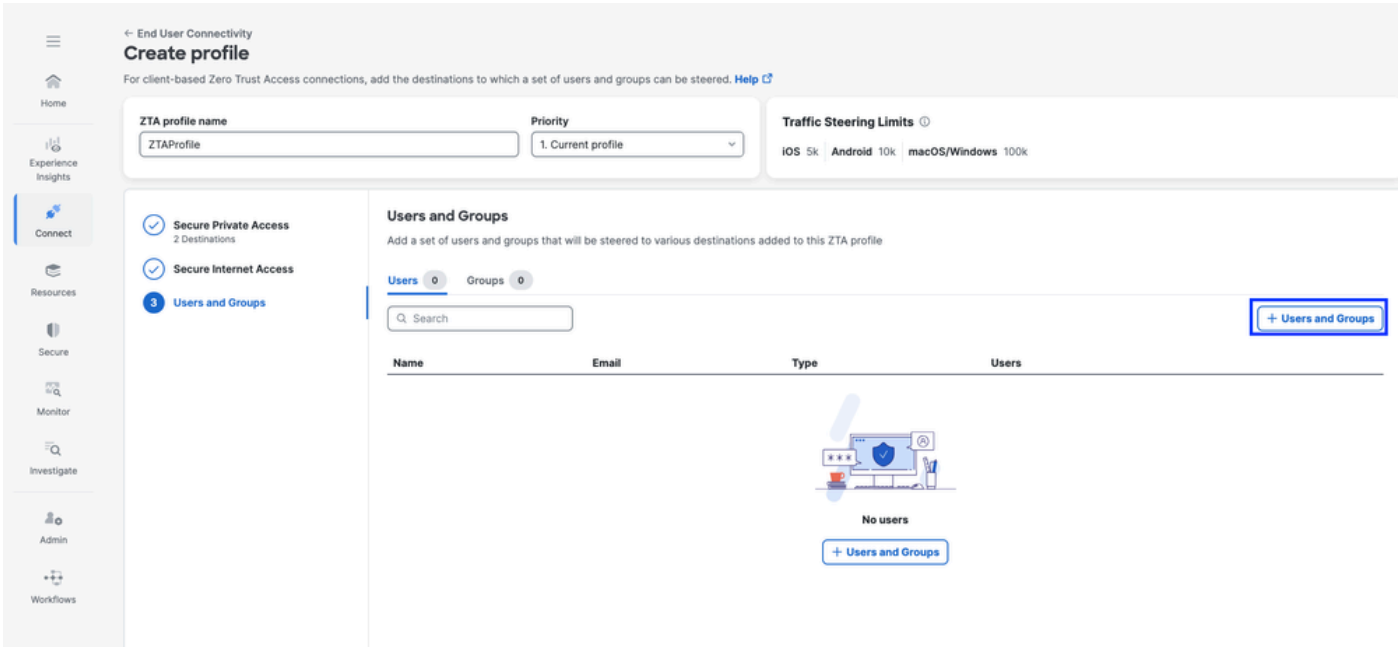


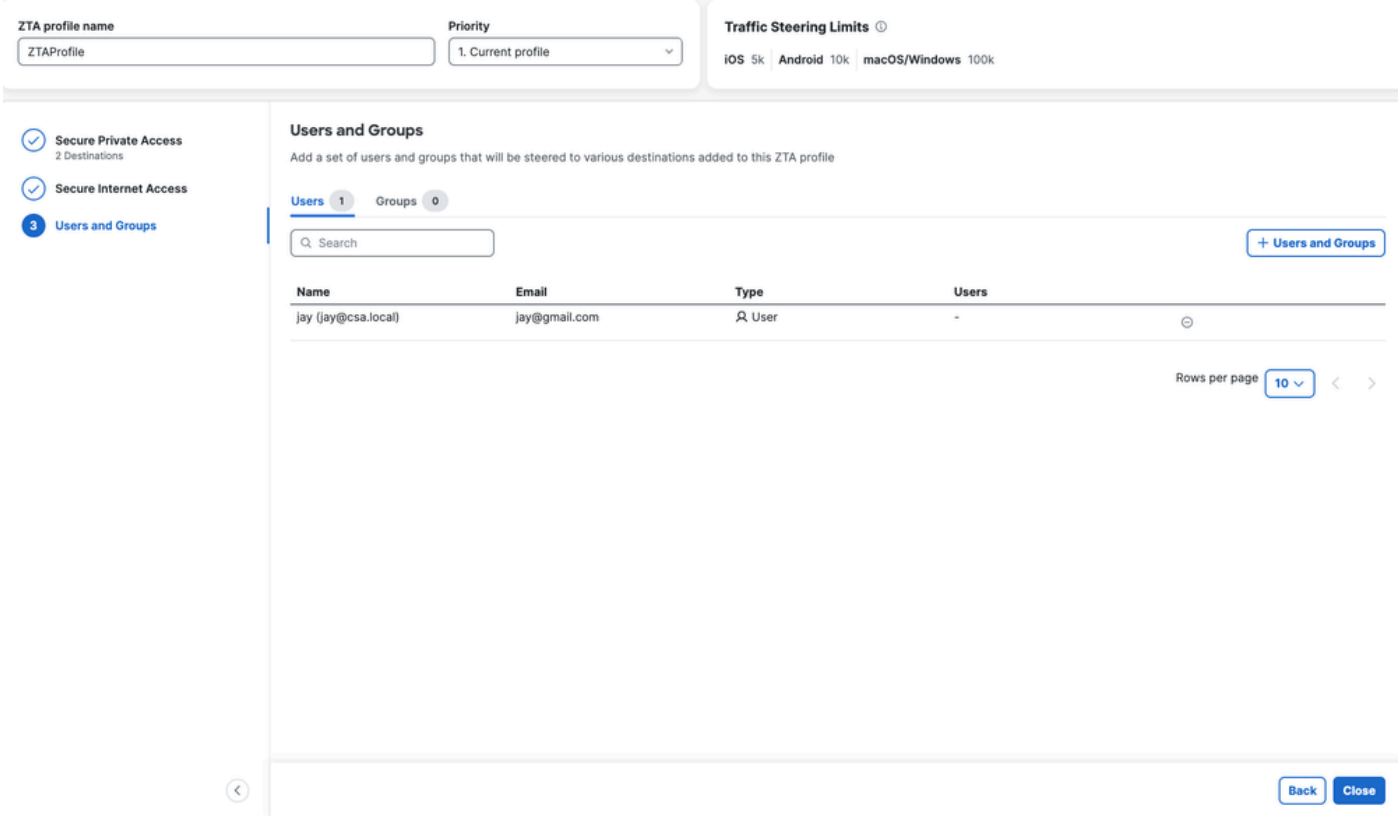
安全访问 — ZTA配置文件



安全访问 — ZTA配置文件

3.添加用户和组

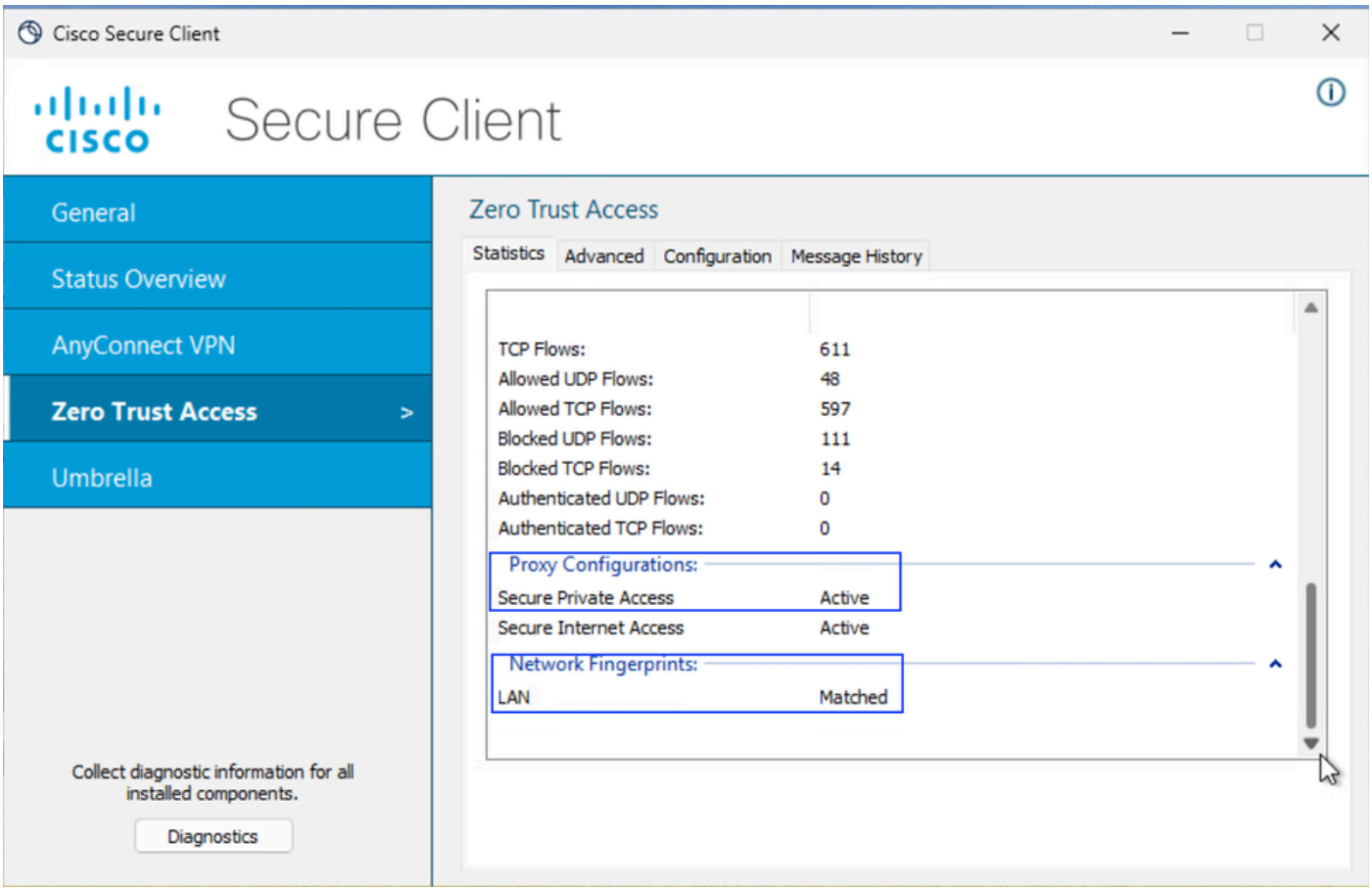




安全访问 — ZTA配置文件

第–6步检验对专用资源的访问

1.验证ZTA TND的网络指纹



安全访问 — PR测试

2. 验证远程用户可以解析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
```

安全访问 — PR测试

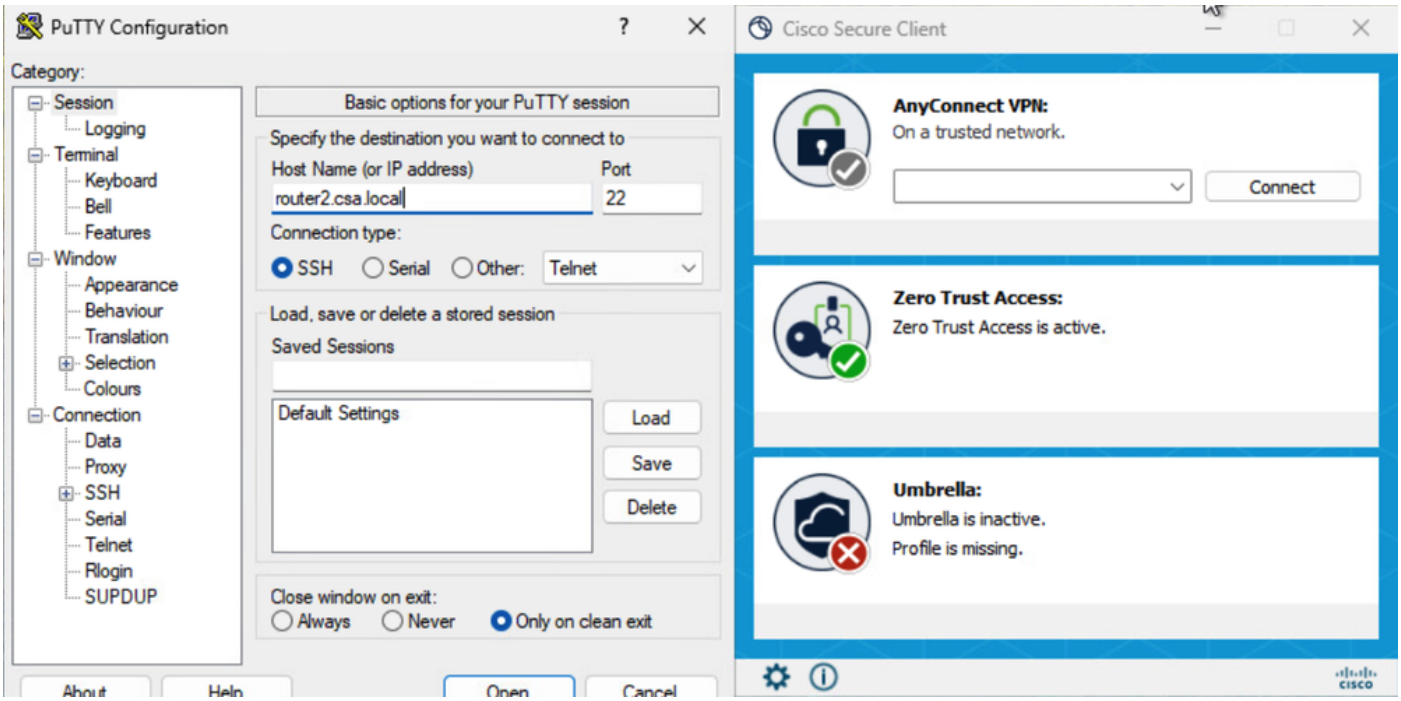
3.验证FTD是否可以使用FQDN访问私有资源

```
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#
```

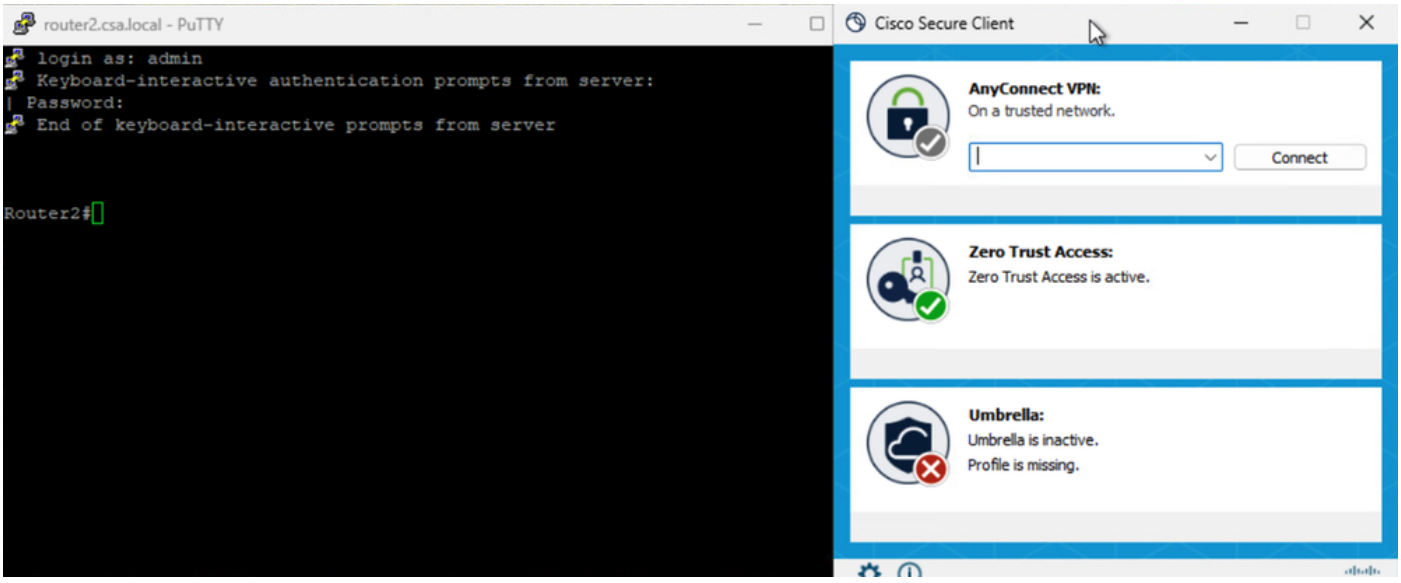
安全访问 — PR测试

4. 测试与专用资源的SSH连接

使用FQDN访问PR

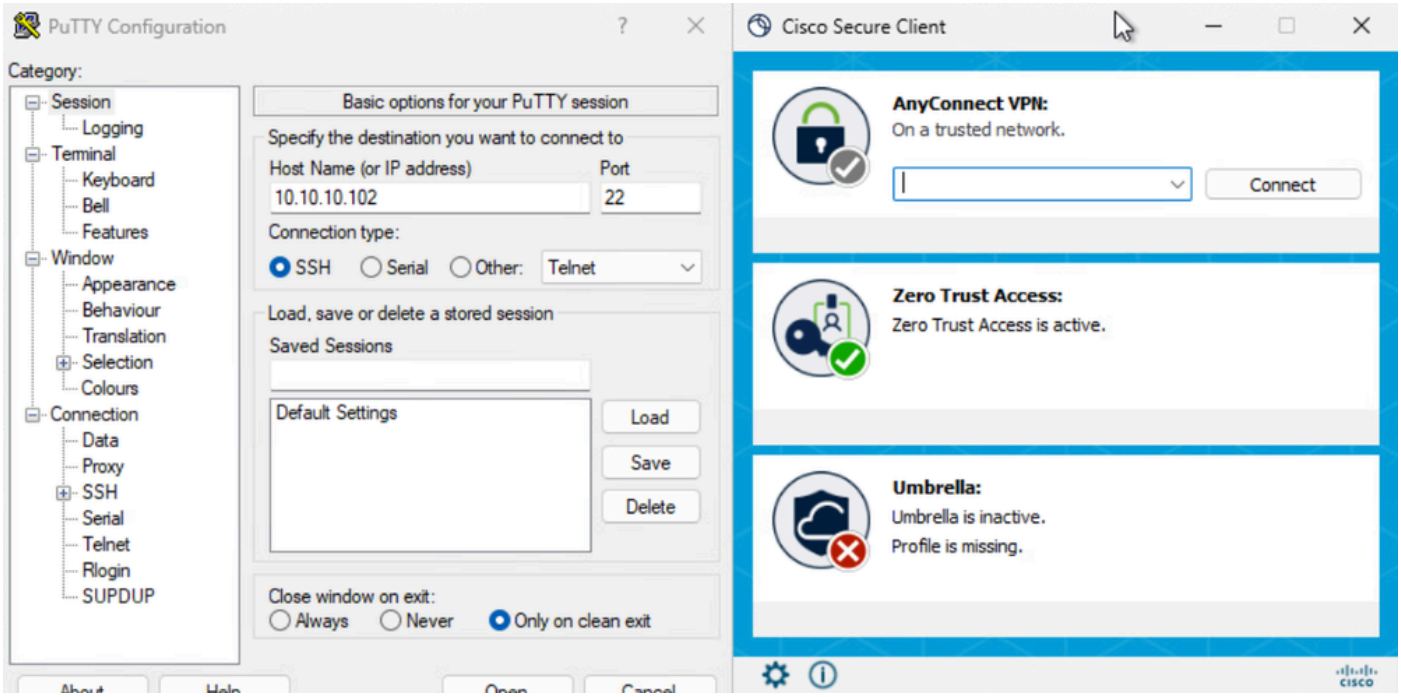


安全访问 — PR测试

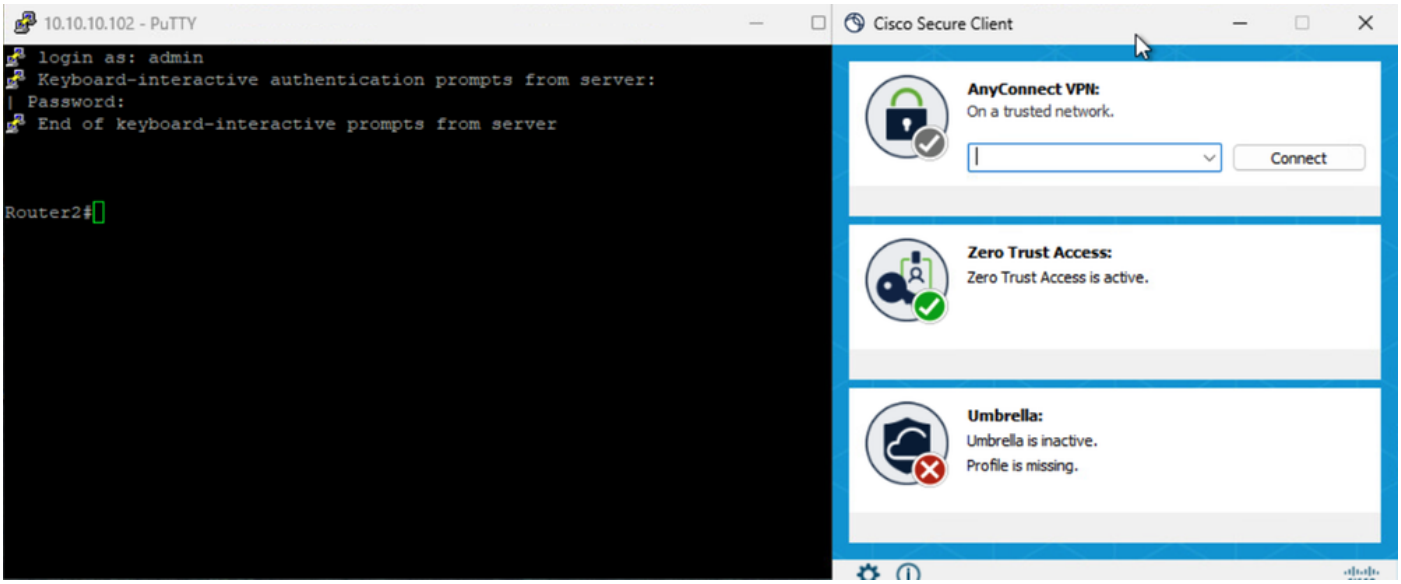


安全访问 — PR测试

使用IP地址访问PR

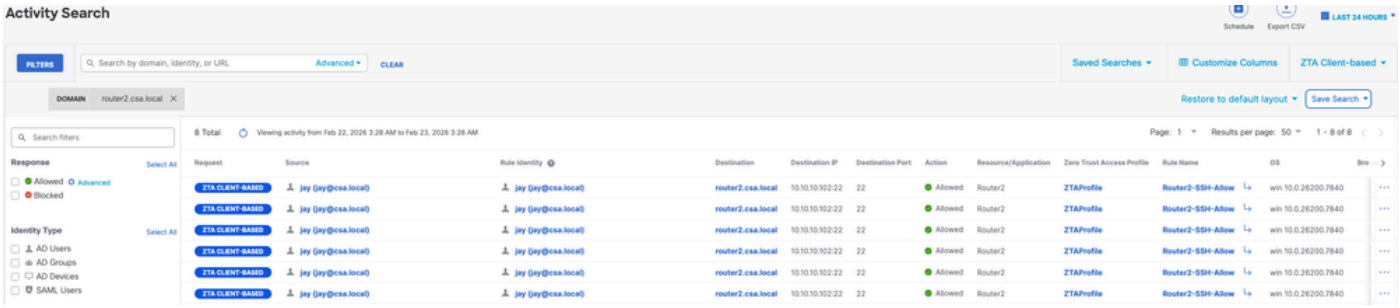


安全访问 — PR测试

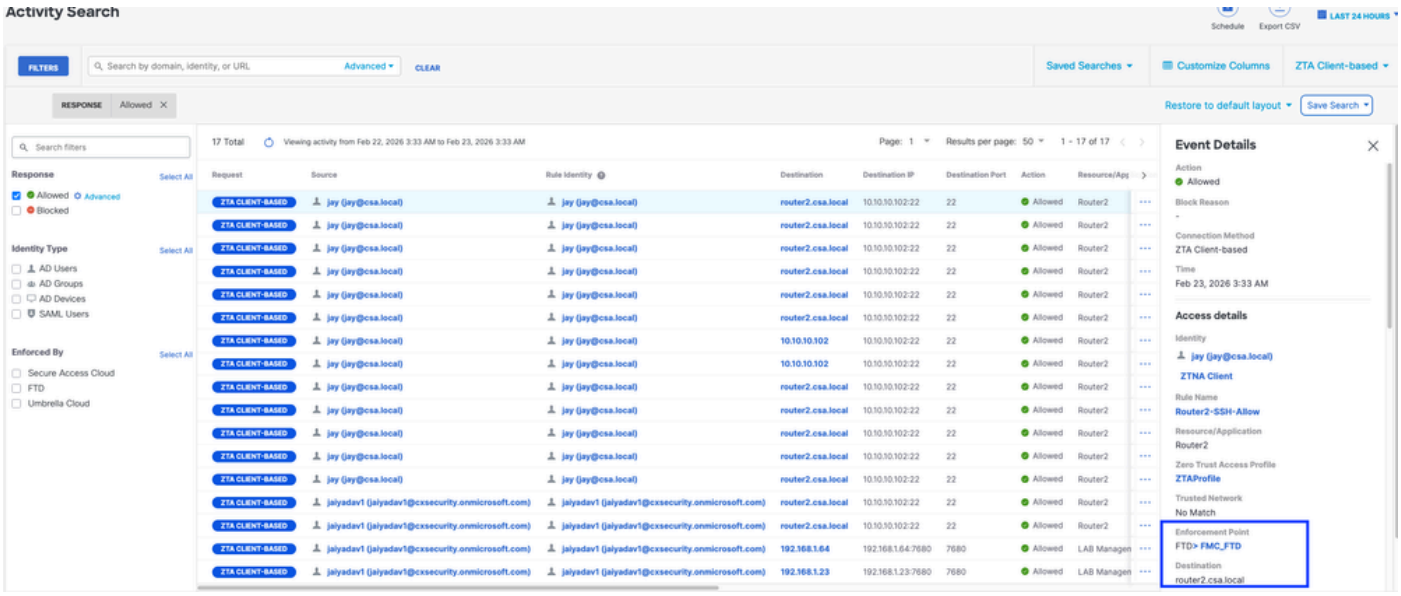


安全访问 — PR测试

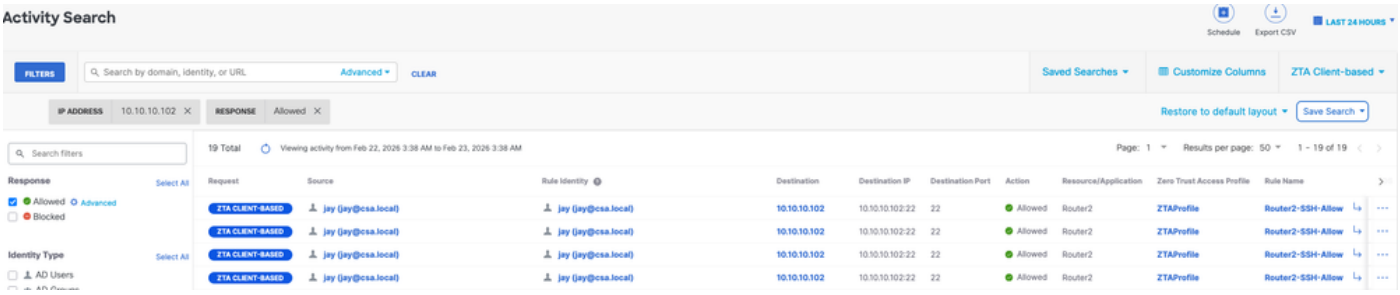
5. 验证安全访问活动搜索日志



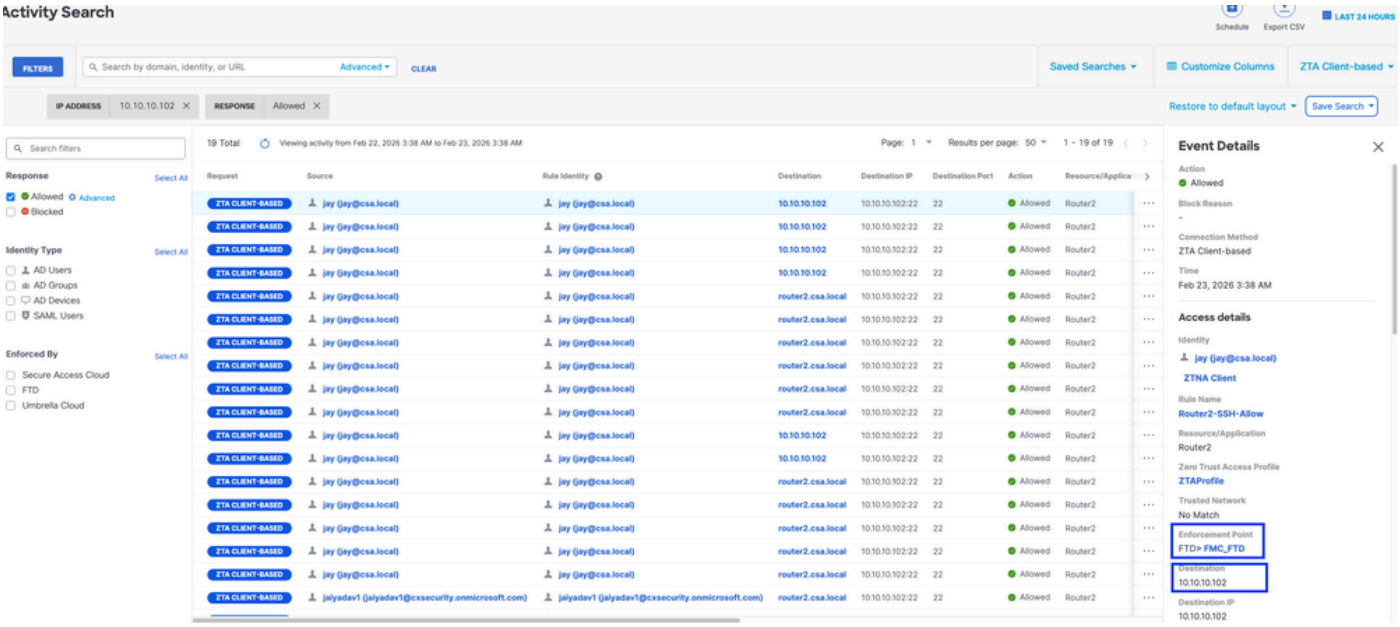
安全访问 — 活动搜索



安全访问 — 活动搜索

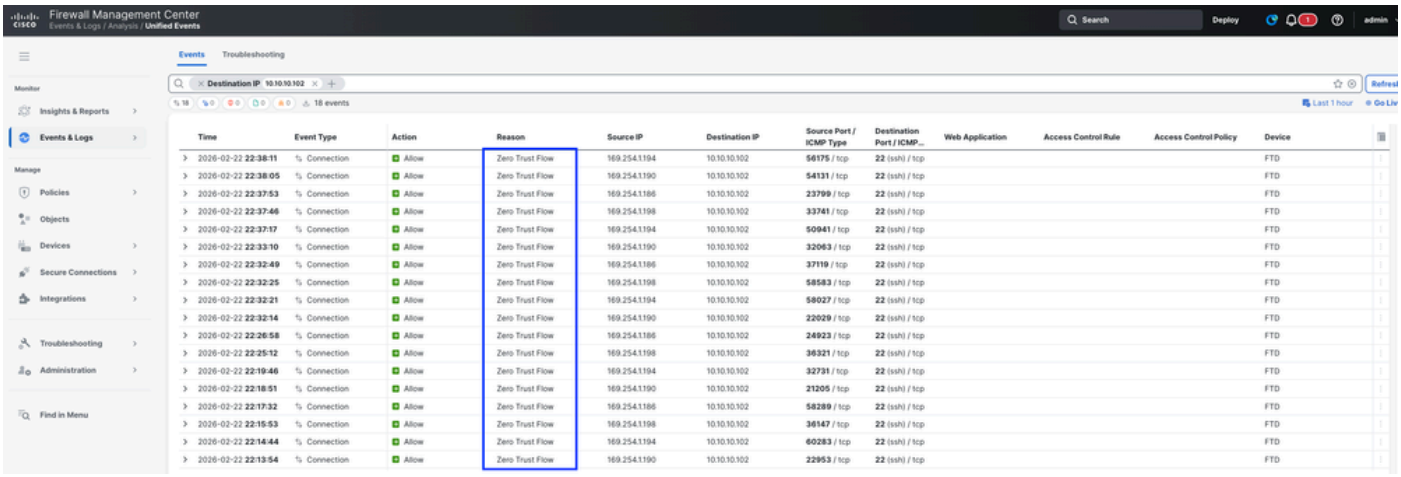


安全访问 — 活动搜索



安全访问 — 活动搜索

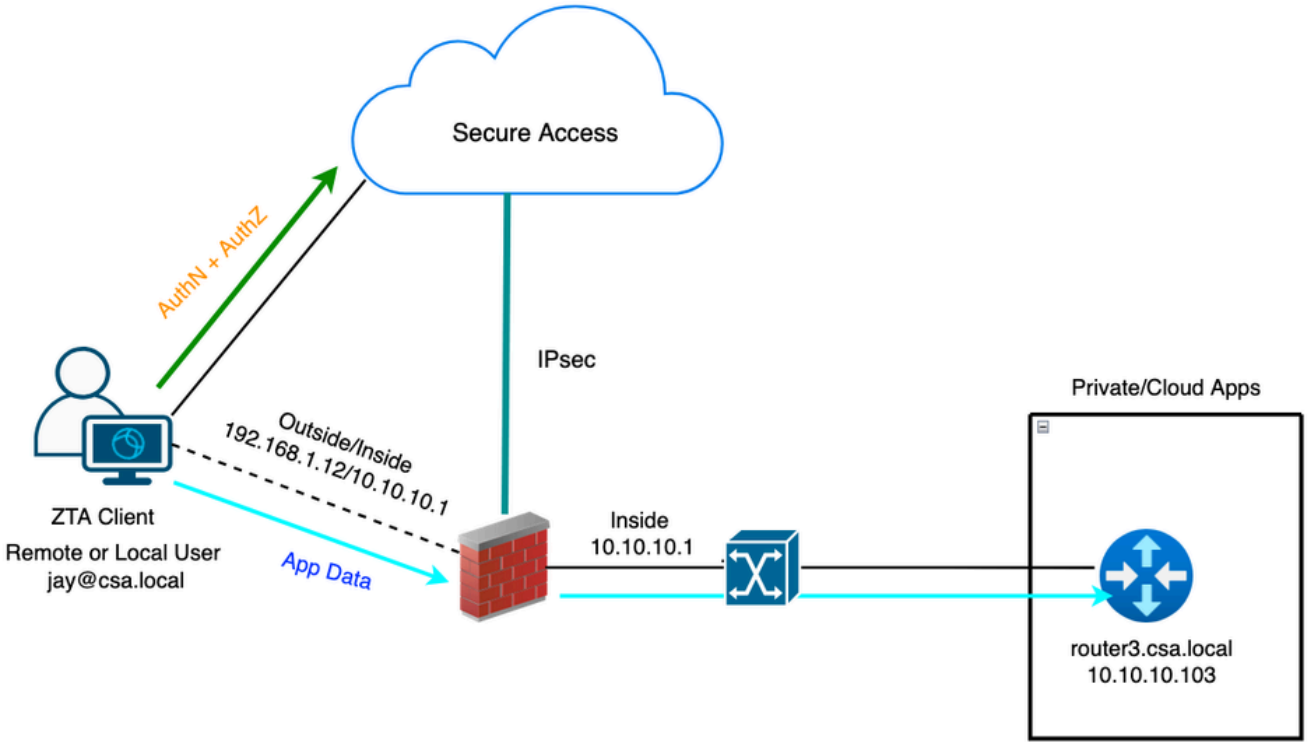
6. 验证FMC连接事件



FMC连接事件

测试案例4 — 本地和远程用户 — 使用TND实施本地或云

在这种情况下，实施类型取决于用户位置，如果用户为Local或受信任FTD区域（内部、DMZ等）之后，则实施为Local（测试案例3）。同样，如果用户是远程用户，则实施方式为云（测试案例1）。用户位置将根据网络指纹或TND设置确定，如果网络指纹匹配，则用户的本地将为Local，如果不匹配，则用户本地将被视为Remote。

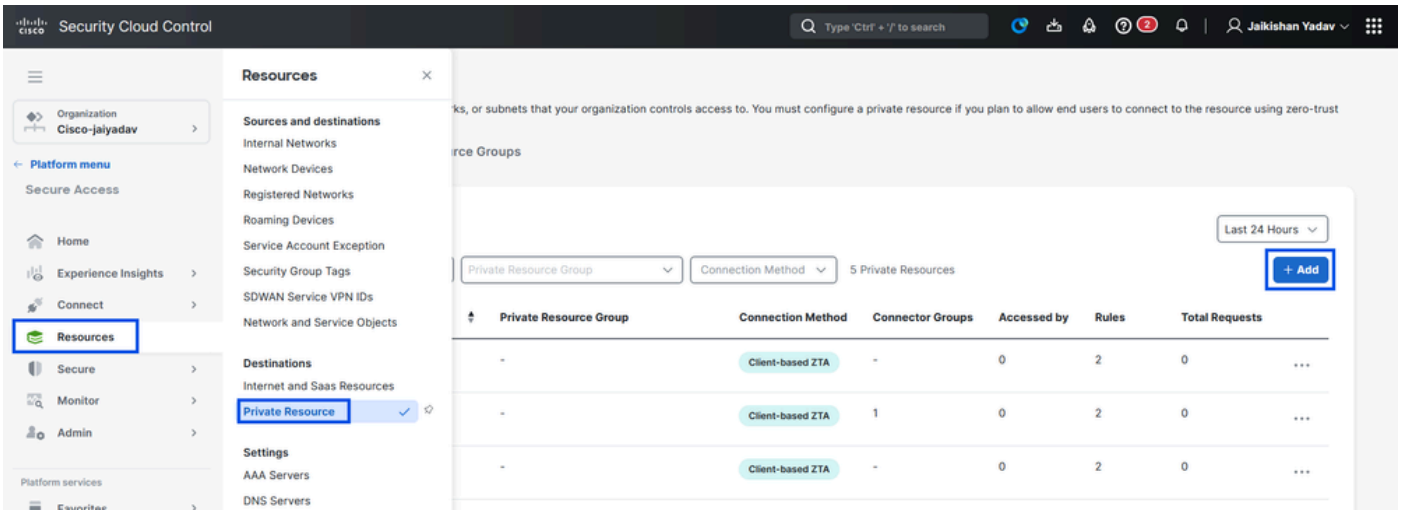


通用ZTA — 测试用例拓扑

第1步 — 在安全访问中定义私有资源

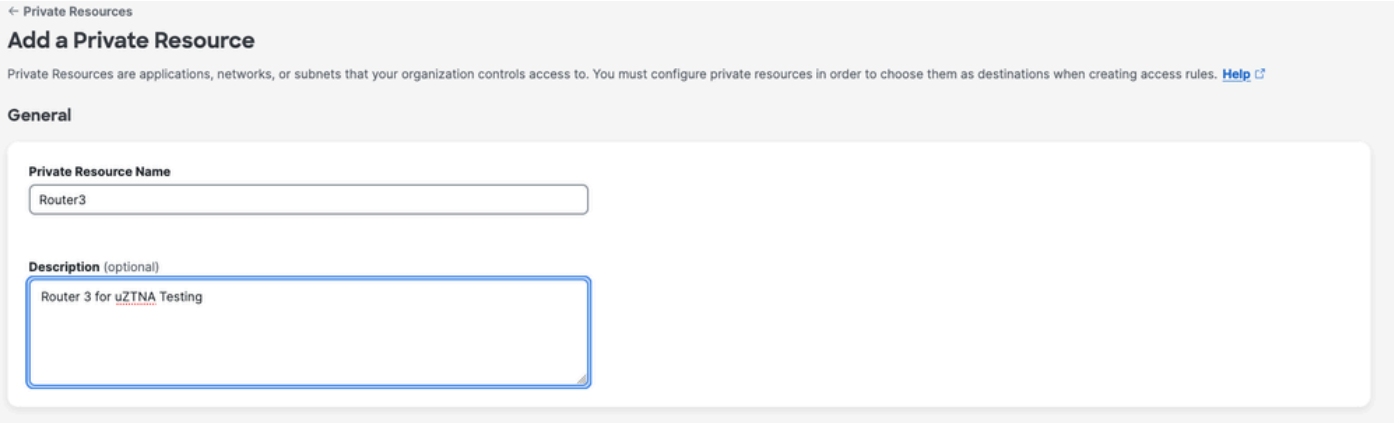
配置私有资源，使其可通过云实施的零信任访问(ZTA)注册设备访问

1. 导航到资源 > 目标 > 专用资源 >单击+添加



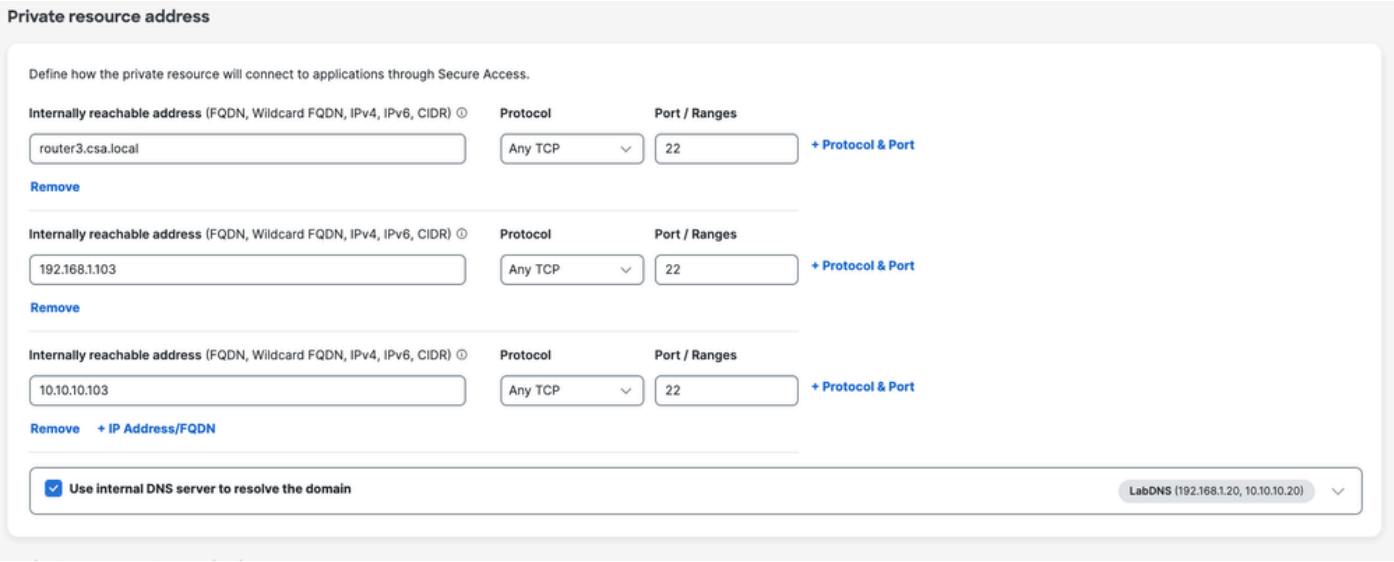
安全访问 — 私有资源配置

2.对于专用资源名称，输入资源有意义的名称。对于Description，建议您提供诸如资源用途或资源所有者名称等信息。



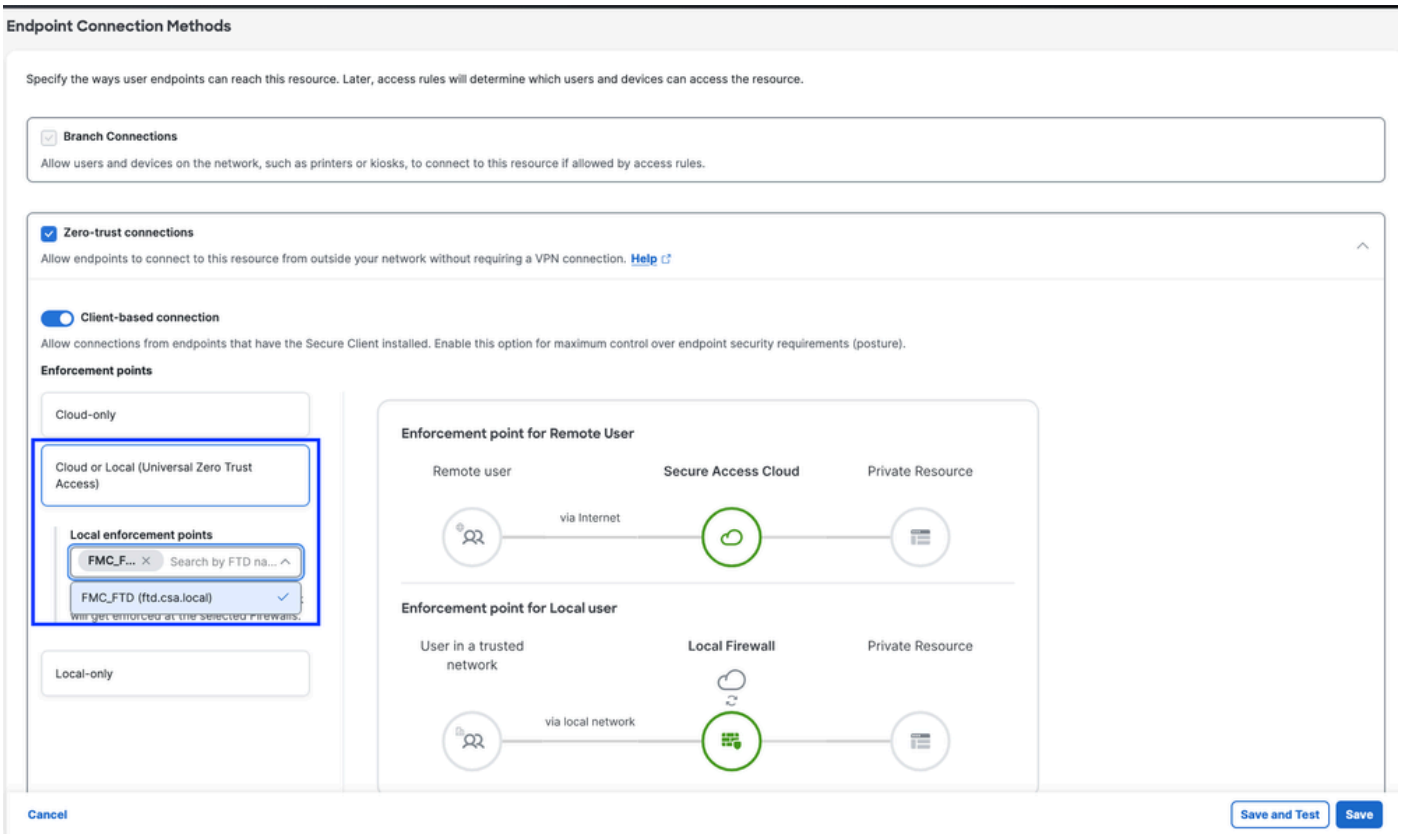
3.输入要访问的专用资源的FQDN。我们还可以定义私有资源的IP地址。有关详细信息，请参阅添加专用资源

4.选择要解析域的DNS服务器



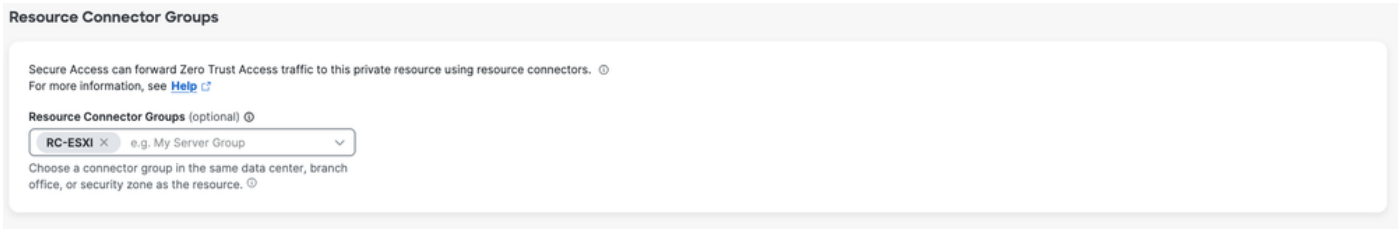
5. 选择终端连接方法

6.选择FTD作为本地实施点



安全访问 — 私有资源配置

如果私有资源可以通过RC访问，请选择RC ，否则如果私有资源可以通过网络隧道组（IPsec隧道）访问，请将其留空。



安全访问 — 私有资源配置

注意：根据您选择的注册类型，此更改将自动将PR与FTD关联并触发策略部署

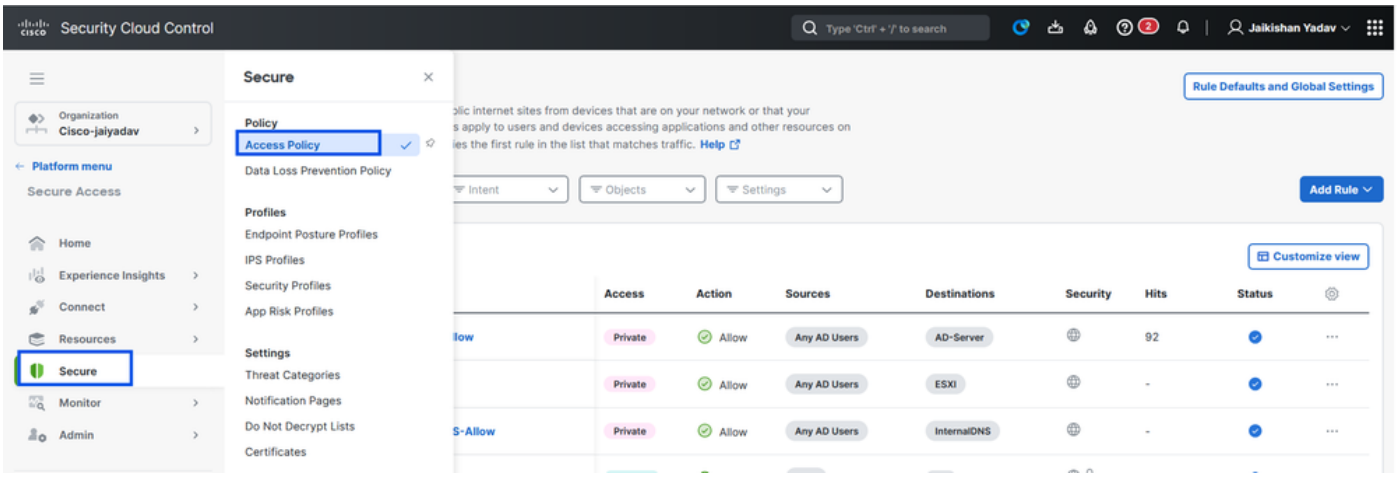
7. 点击保存

第2步 — 创建专用访问规则

在Secure Access上配置私有访问，以便由通用ZTA注册用户访问。有关详细信息，请参阅专用访问

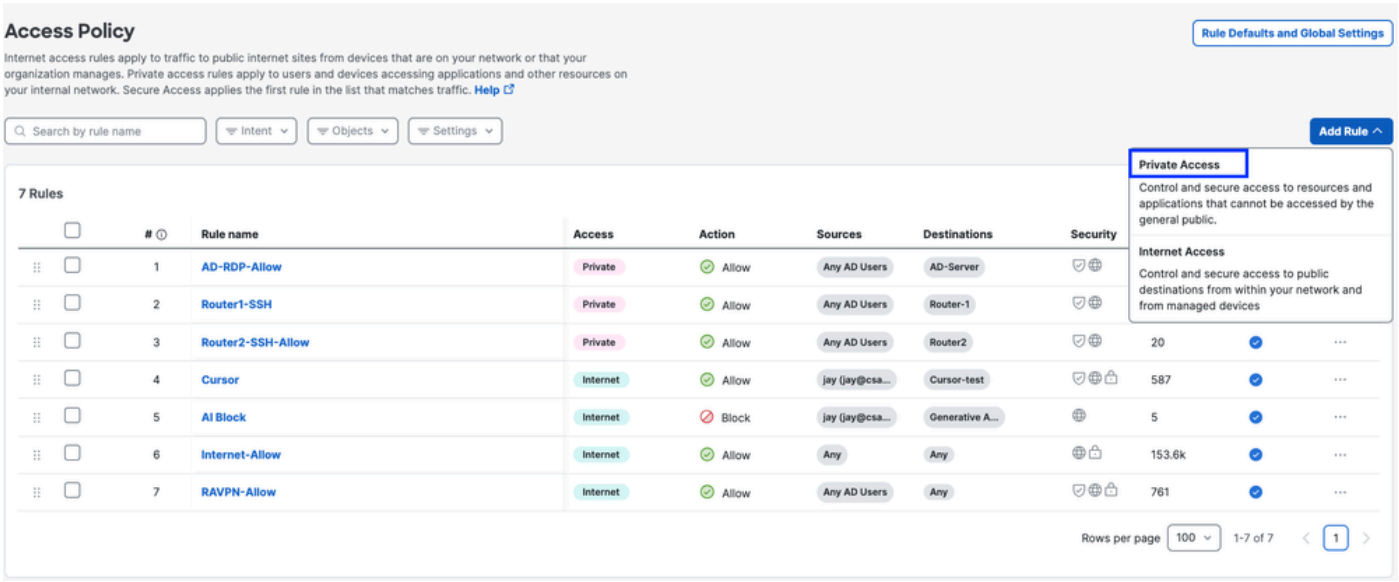
规则

1. 导航到安全>访问策略



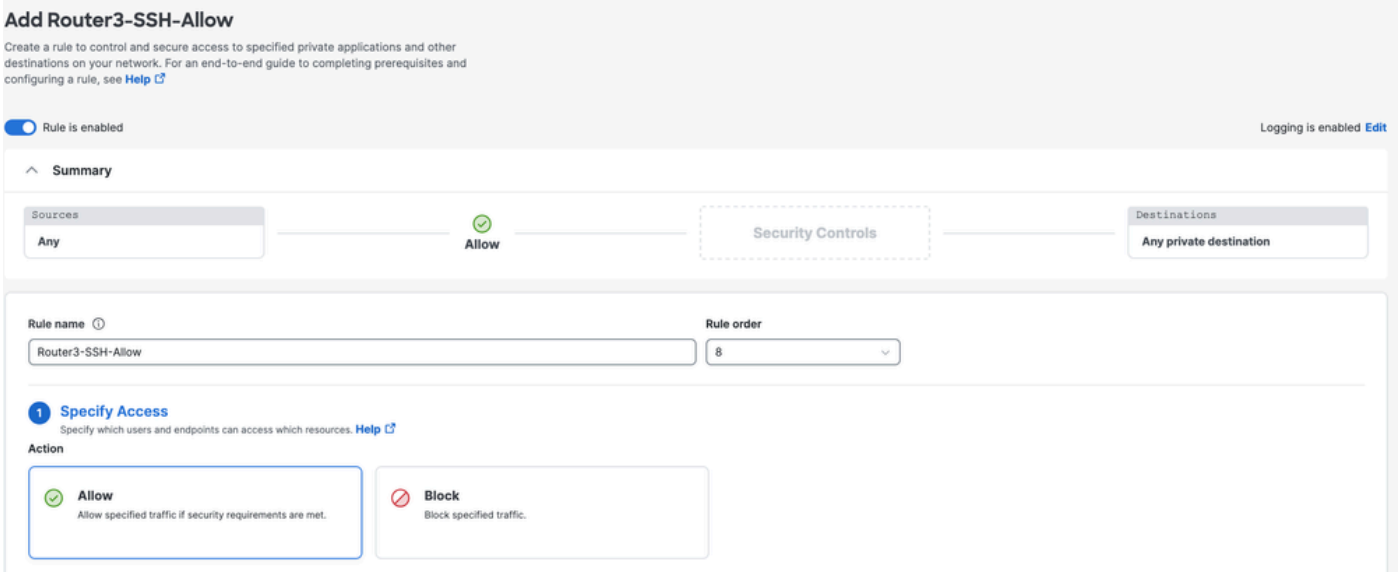
安全访问 — 访问策略配置

2.单击Add Rule，然后选择Private Access。
规则顶部是描述规则已配置组件的摘要。



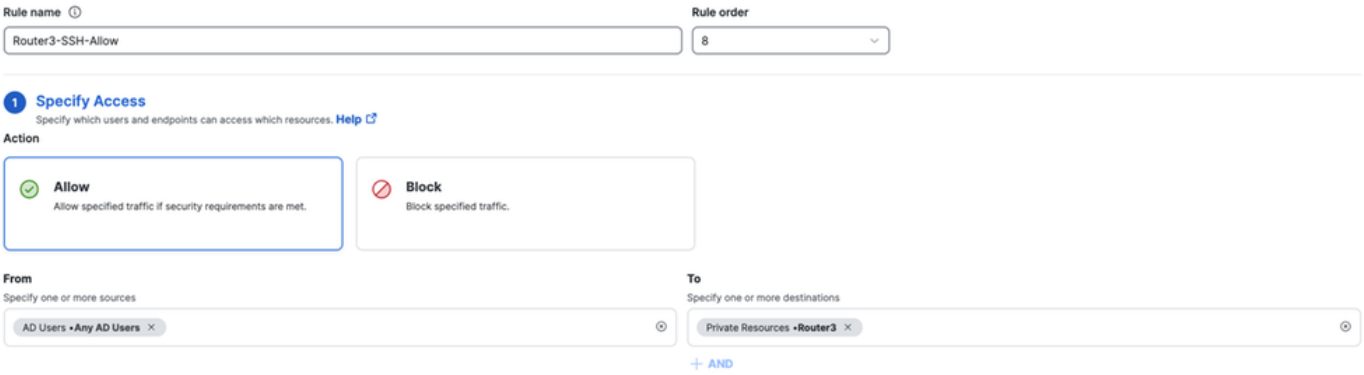
安全访问 — 访问策略配置

3.添加规则名称



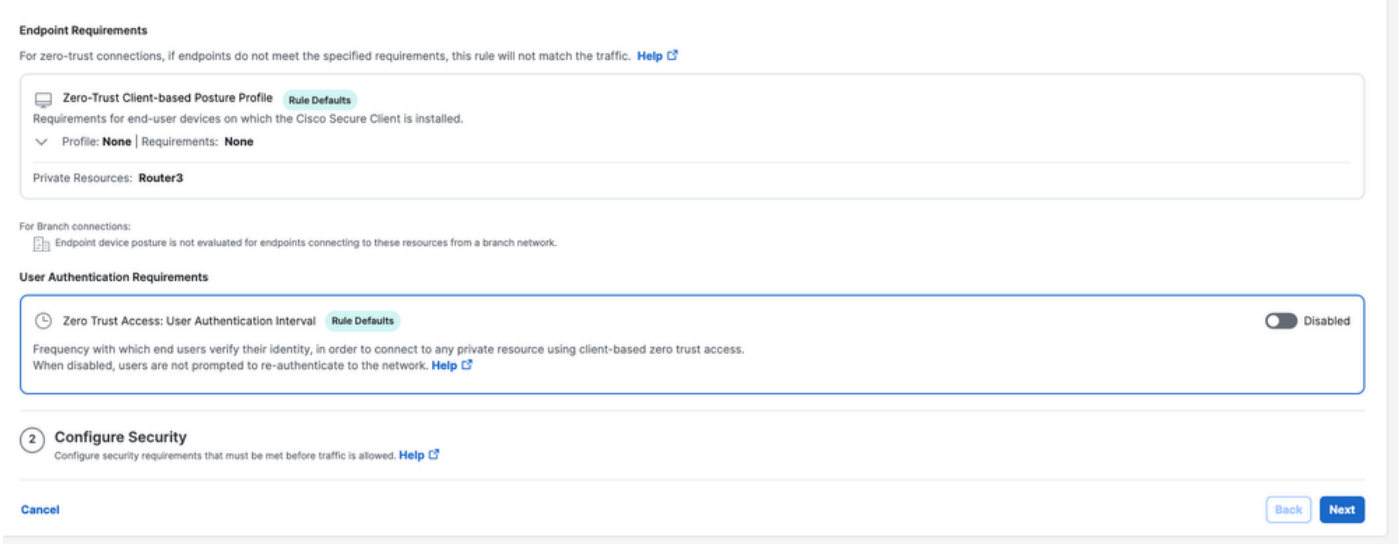
安全访问 — 访问策略配置

4.选择规则操作，然后选择来源和目标



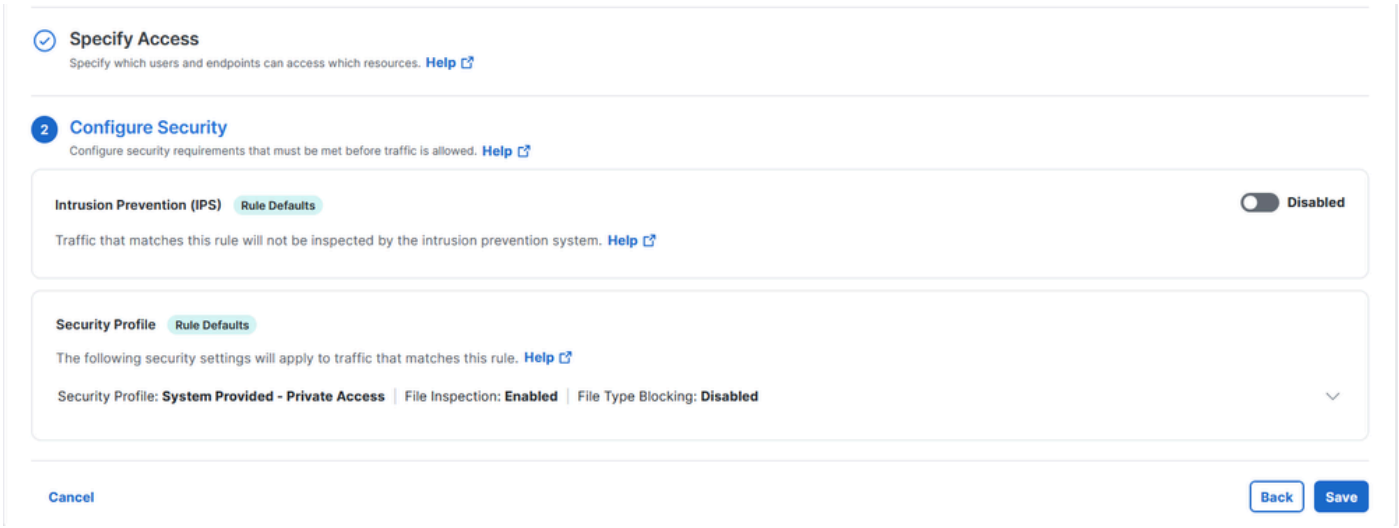
安全访问 — 访问策略配置

5.配置终端要求



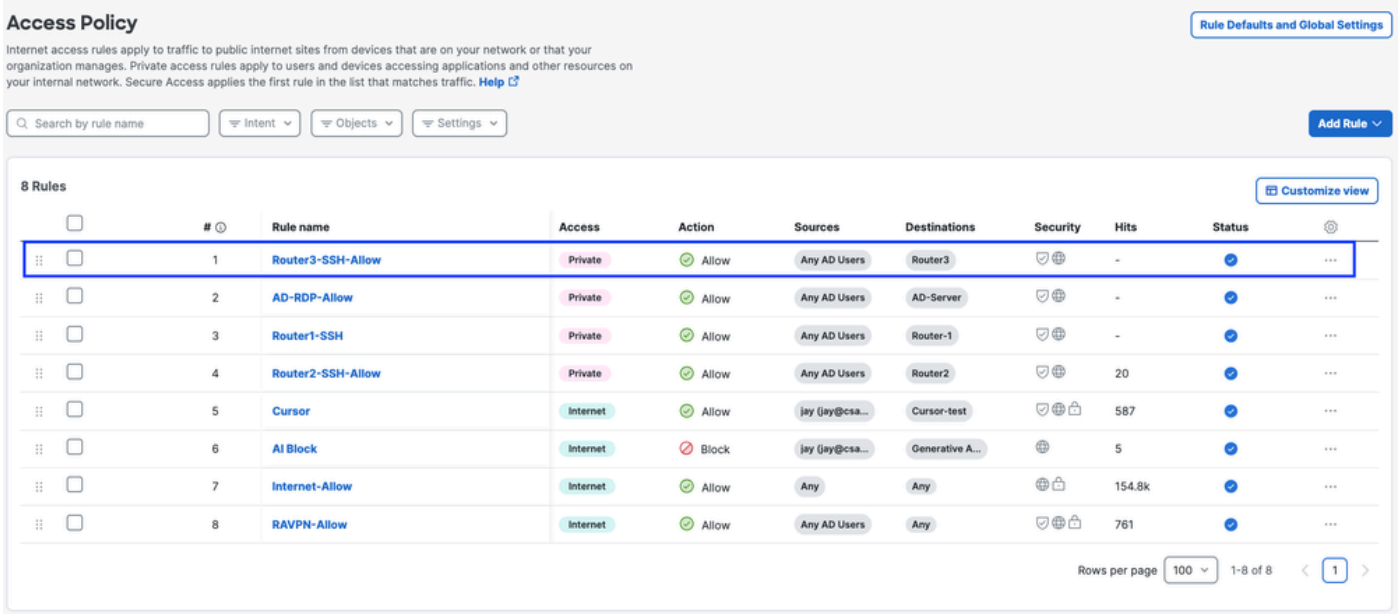
安全访问 — 访问策略配置

6. 配置安全性



安全访问 — 访问策略配置

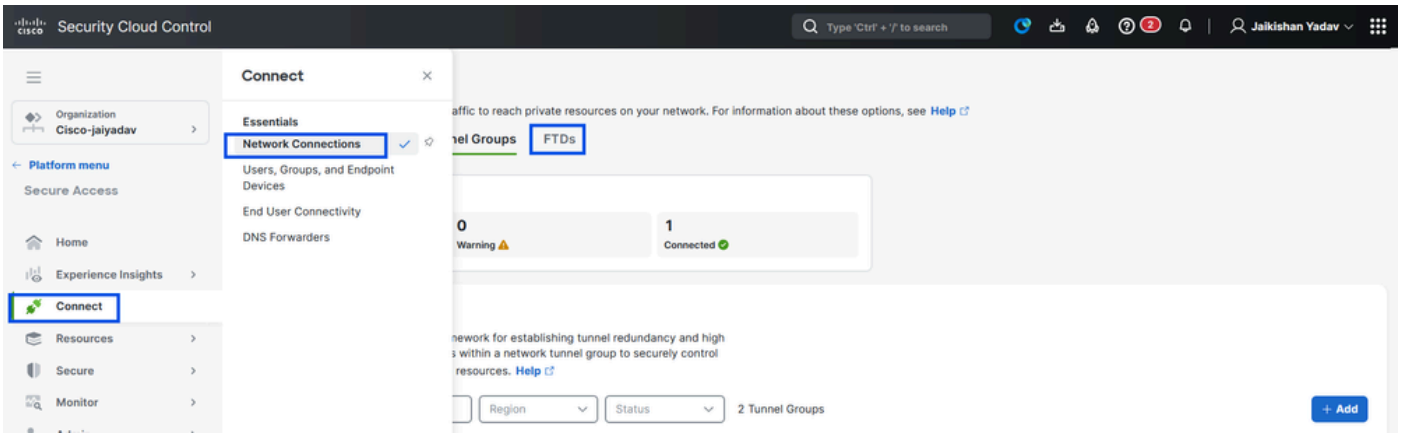
7.单击Save



安全访问 — 访问策略配置

第3步 — 检验FTD上PR的关联

1.导航至connect > Network Connections > FTDs

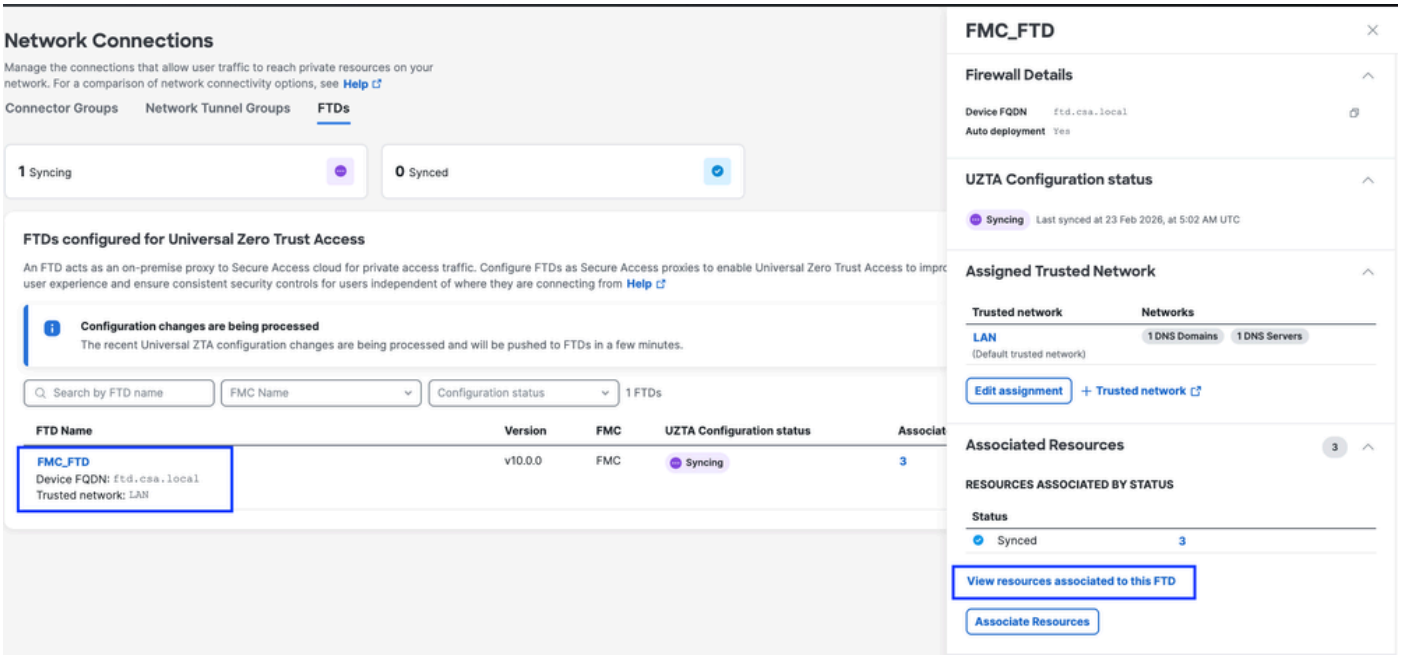


安全访问 — PR验证

2. 点击FTD >查看与此FTD关联的资源

```
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
```

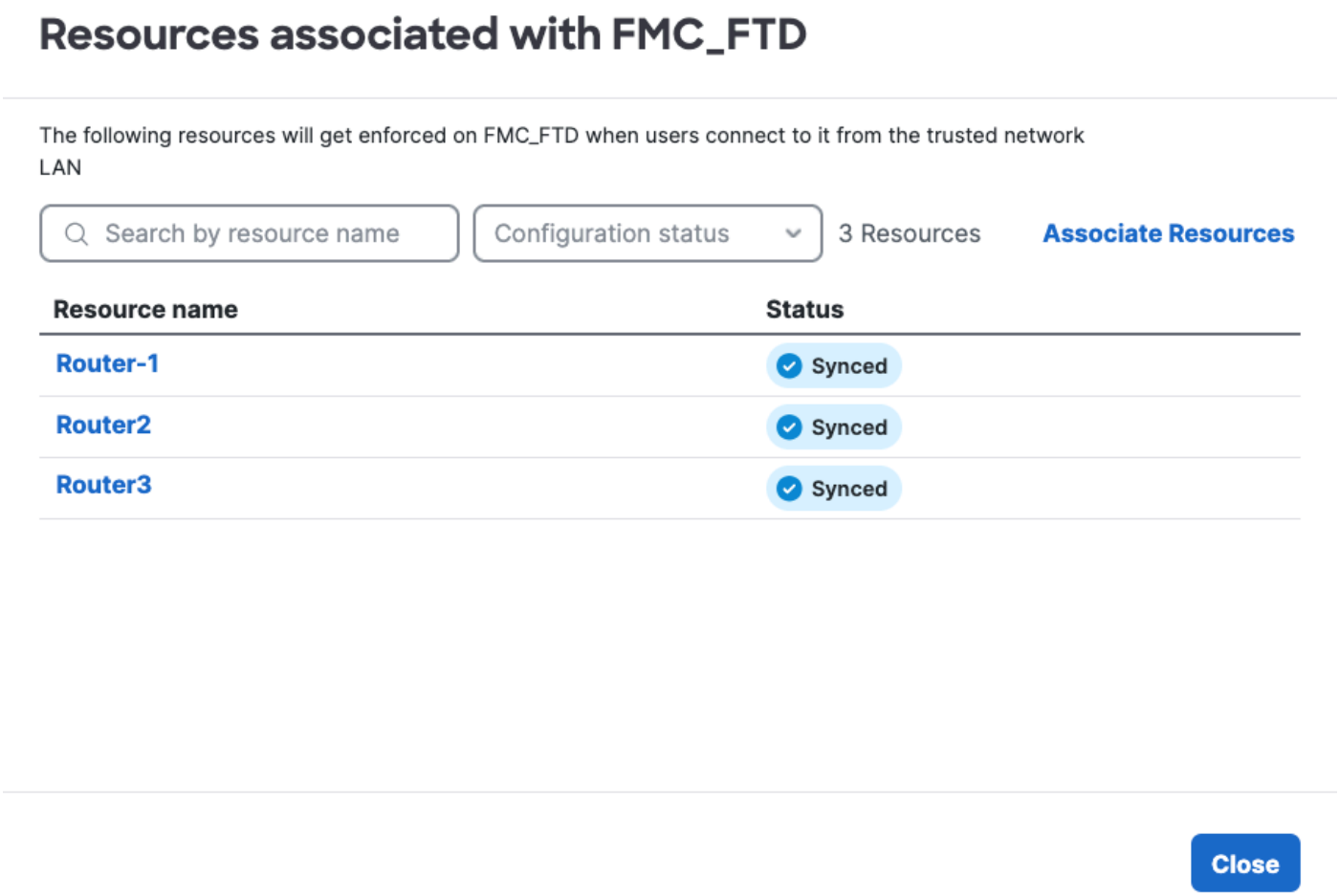
安全访问 — PR验证



安全访问 — PR验证

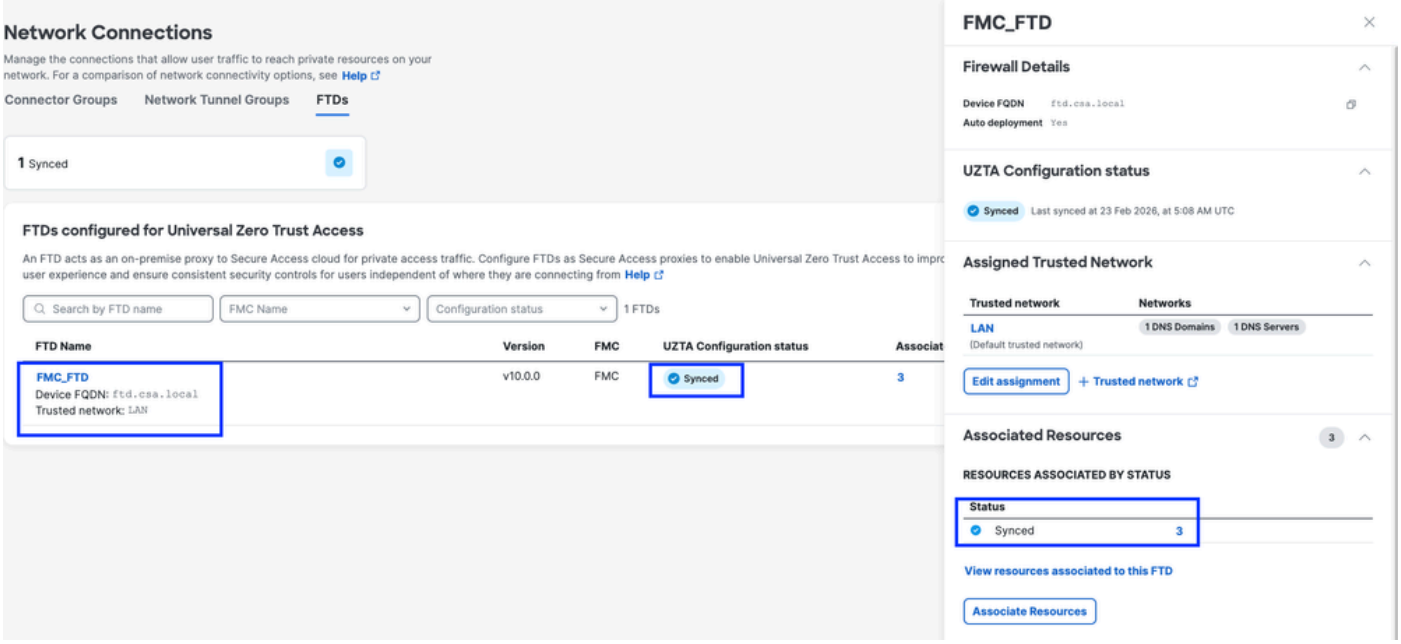
```
C:\Users\jay>ping ftd.csa.local

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
```

安全访问 — PR验证



3. 单击close

4.验证状态、关联的资源和配置是否应该处于“同步”状态



安全访问 — PR验证

5.检验配置是否已推送到FTD

登录到FTD cli并导航到LINA模式

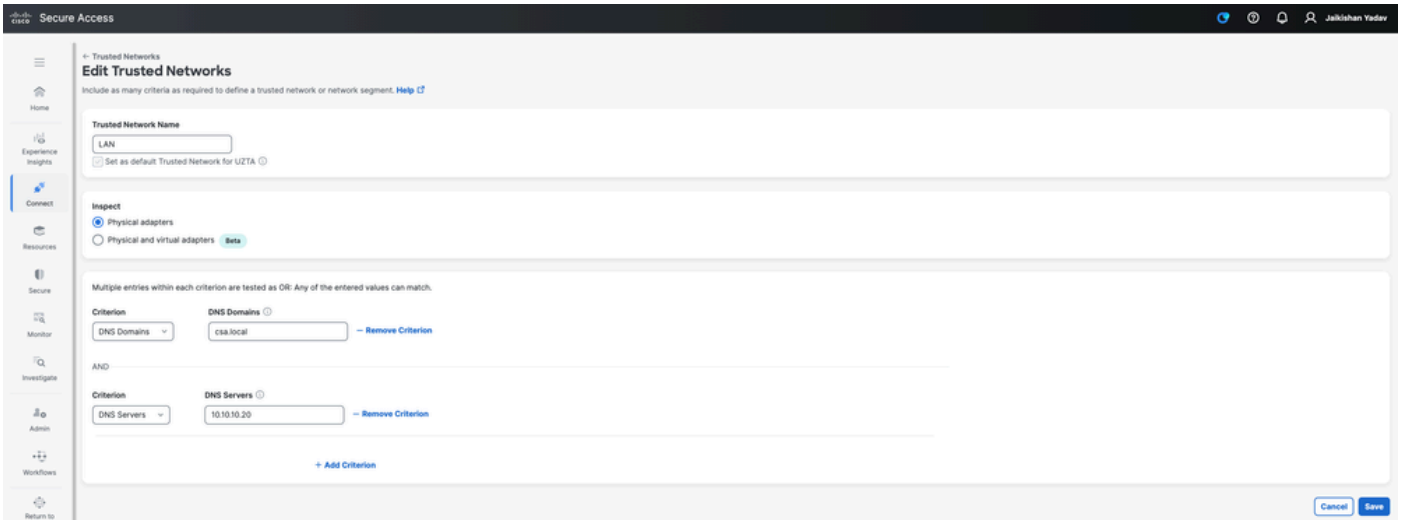
show running-config object application

```
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
```

安全访问 — PR验证

第–4步配置或验证“管理受信任网络或ZTA设置”

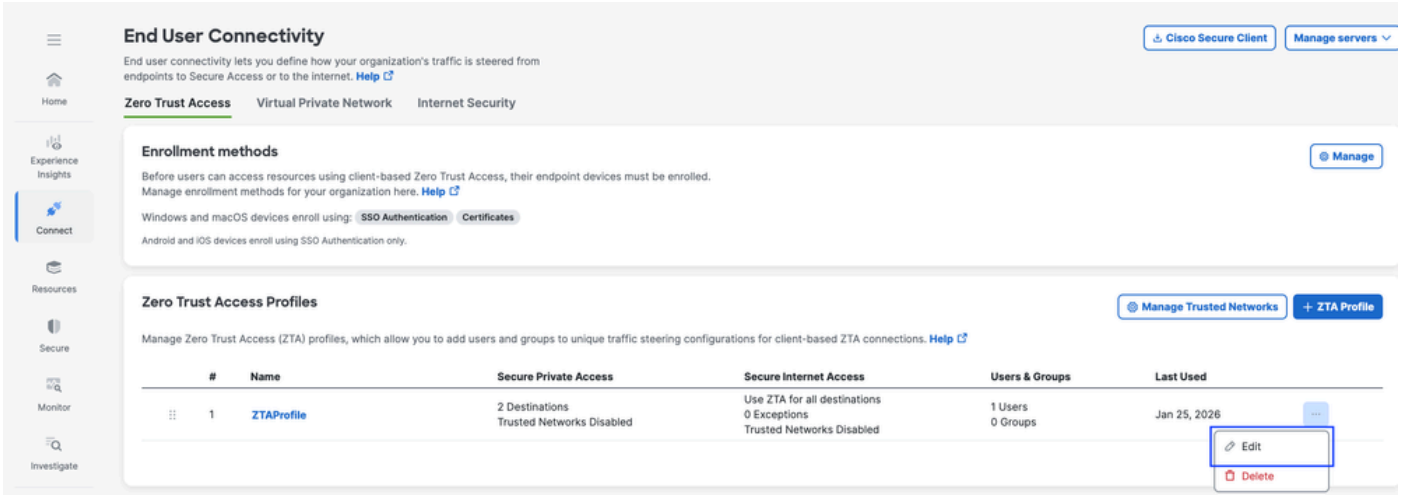
导航到Connect > End User Connectivity > Zero Trust Access > ZTA Settings并配置受信任网络



安全访问 — ZTA TND配置

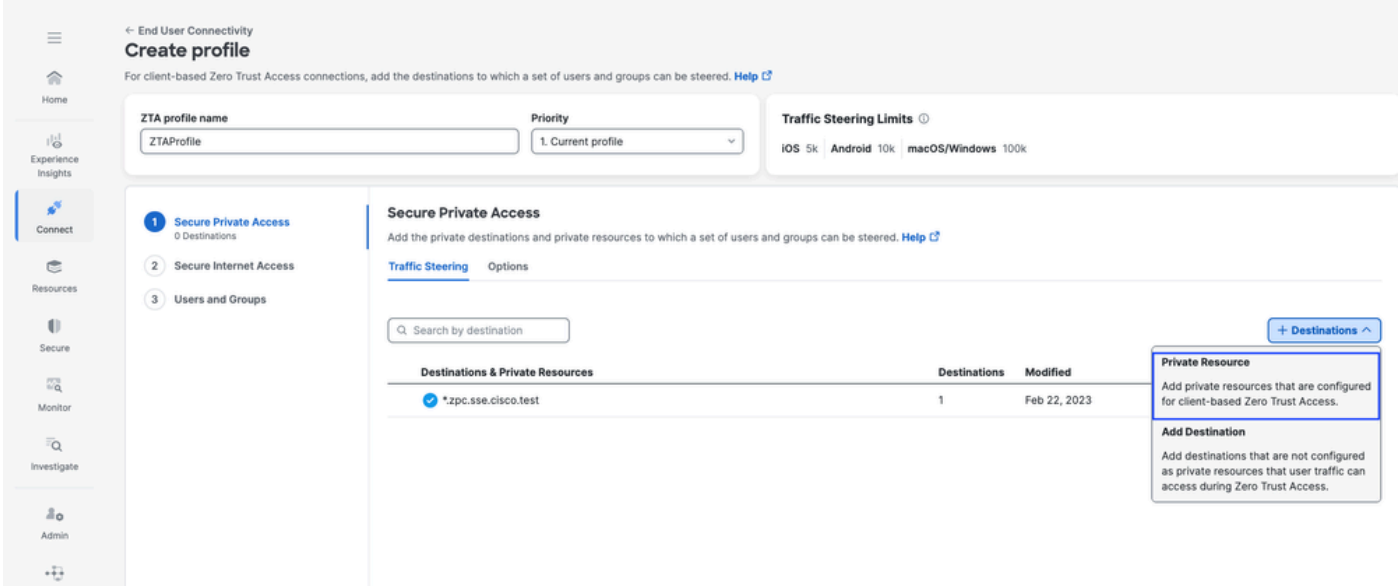
第5步 — 将私有资源添加到ZTA配置文件

1.导航到Connect > End User Connectivity > Zero Trust Access，然后单击3个点以编辑ZTA配置文件

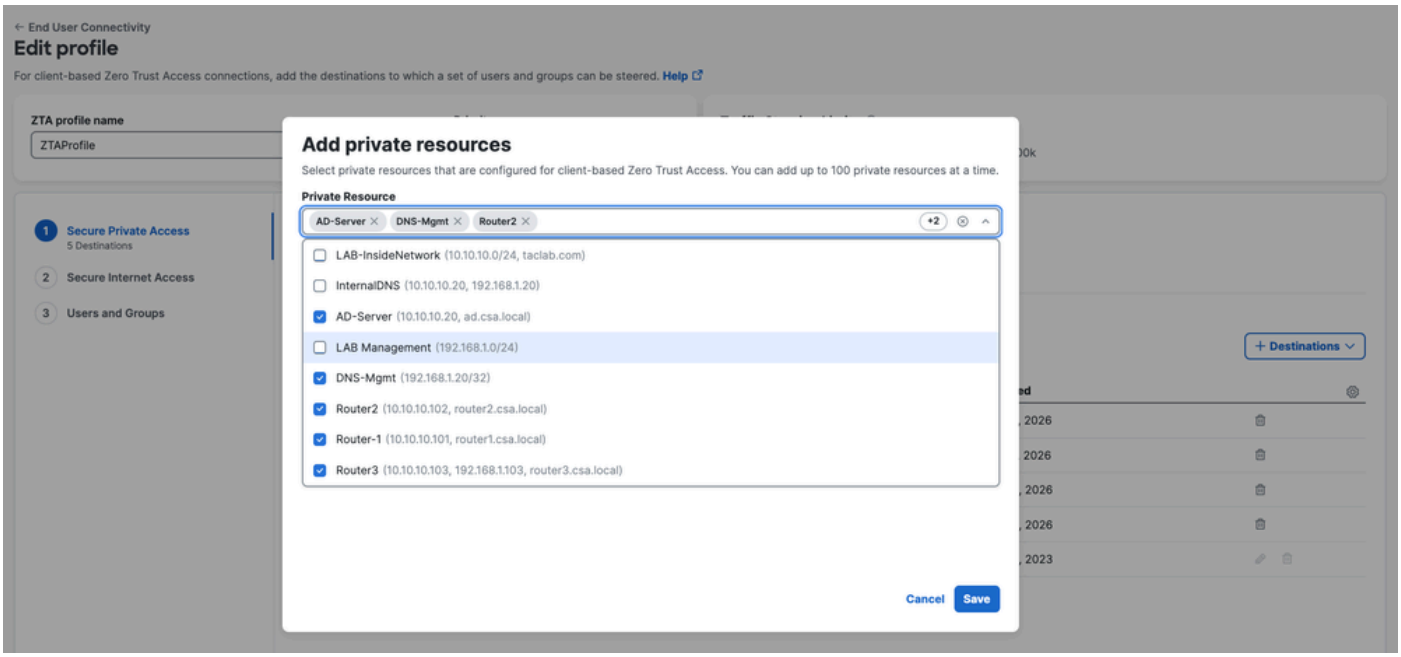


安全访问 — ZTA配置文件

2.添加专用资源

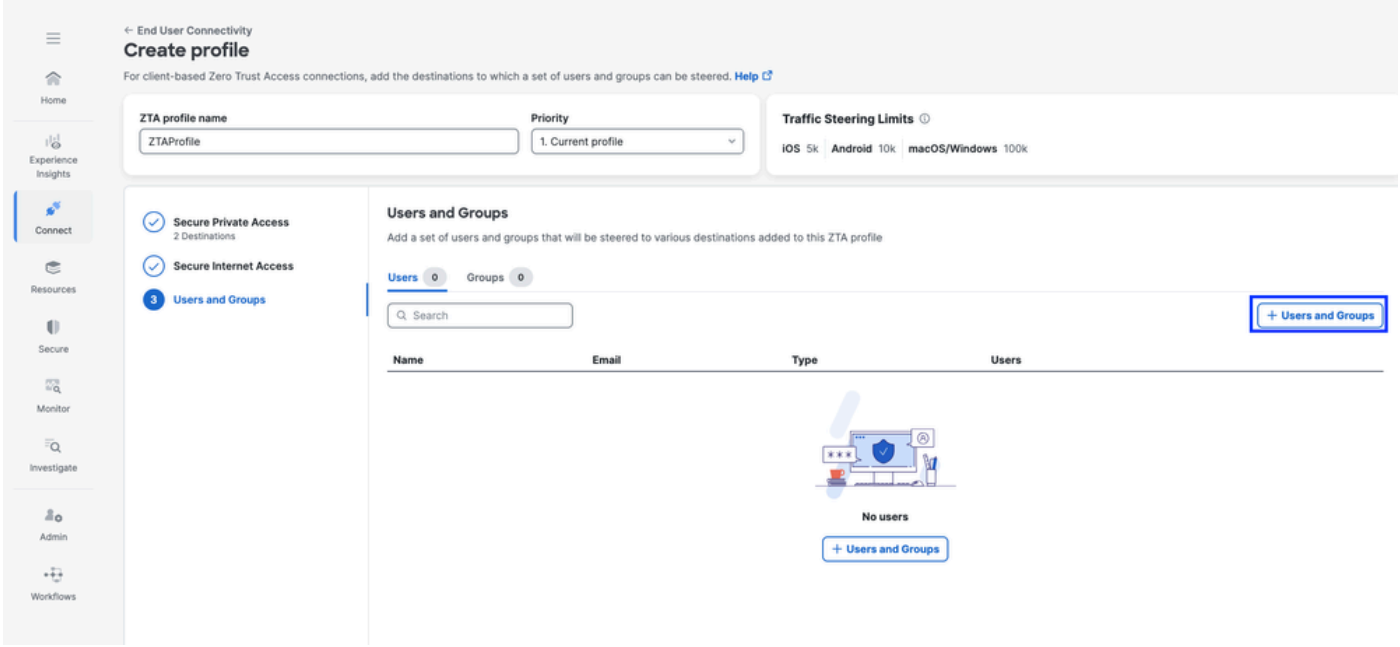


安全访问 — ZTA配置文件

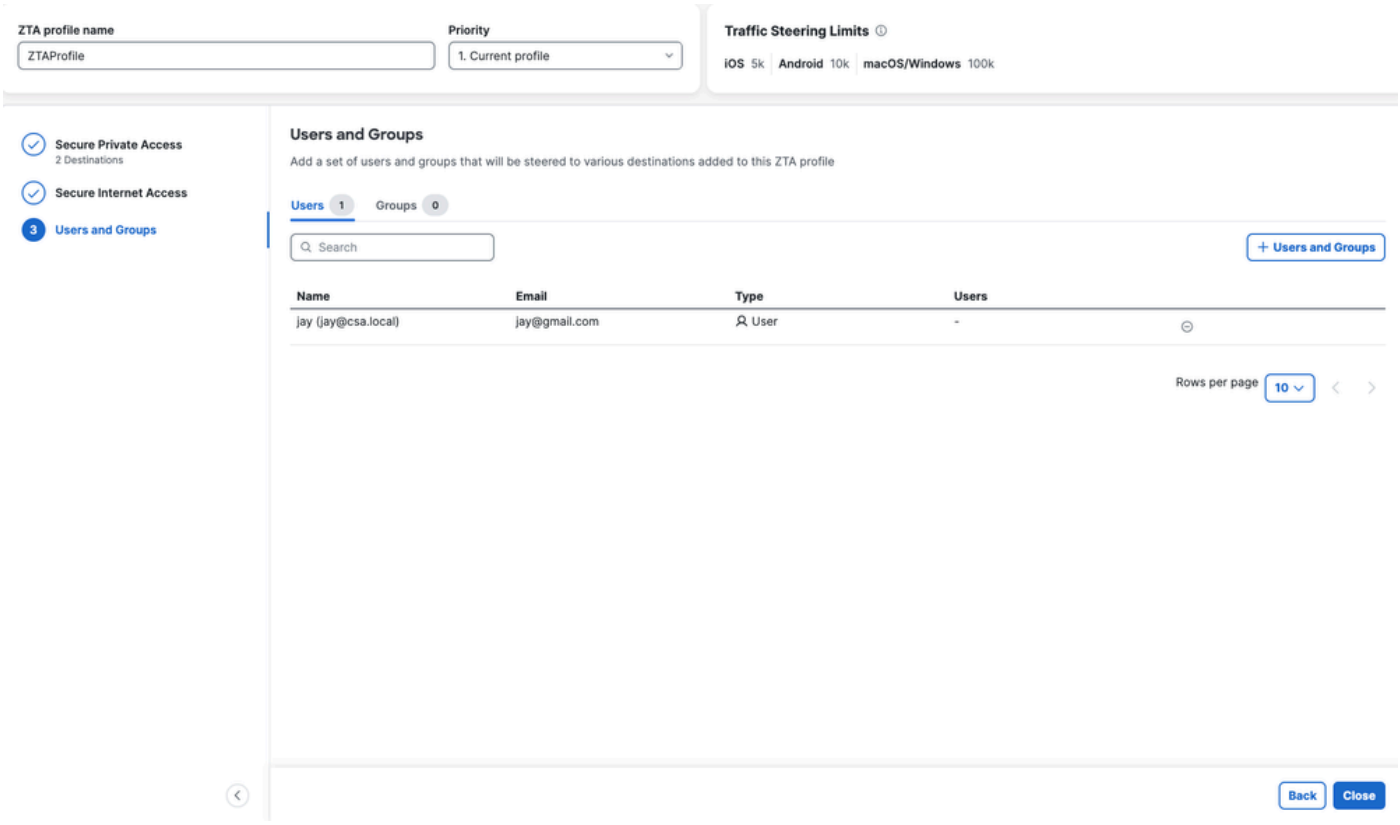


安全访问 — ZTA配置文件

3.添加用户和组



安全访问 — ZTA配置文件

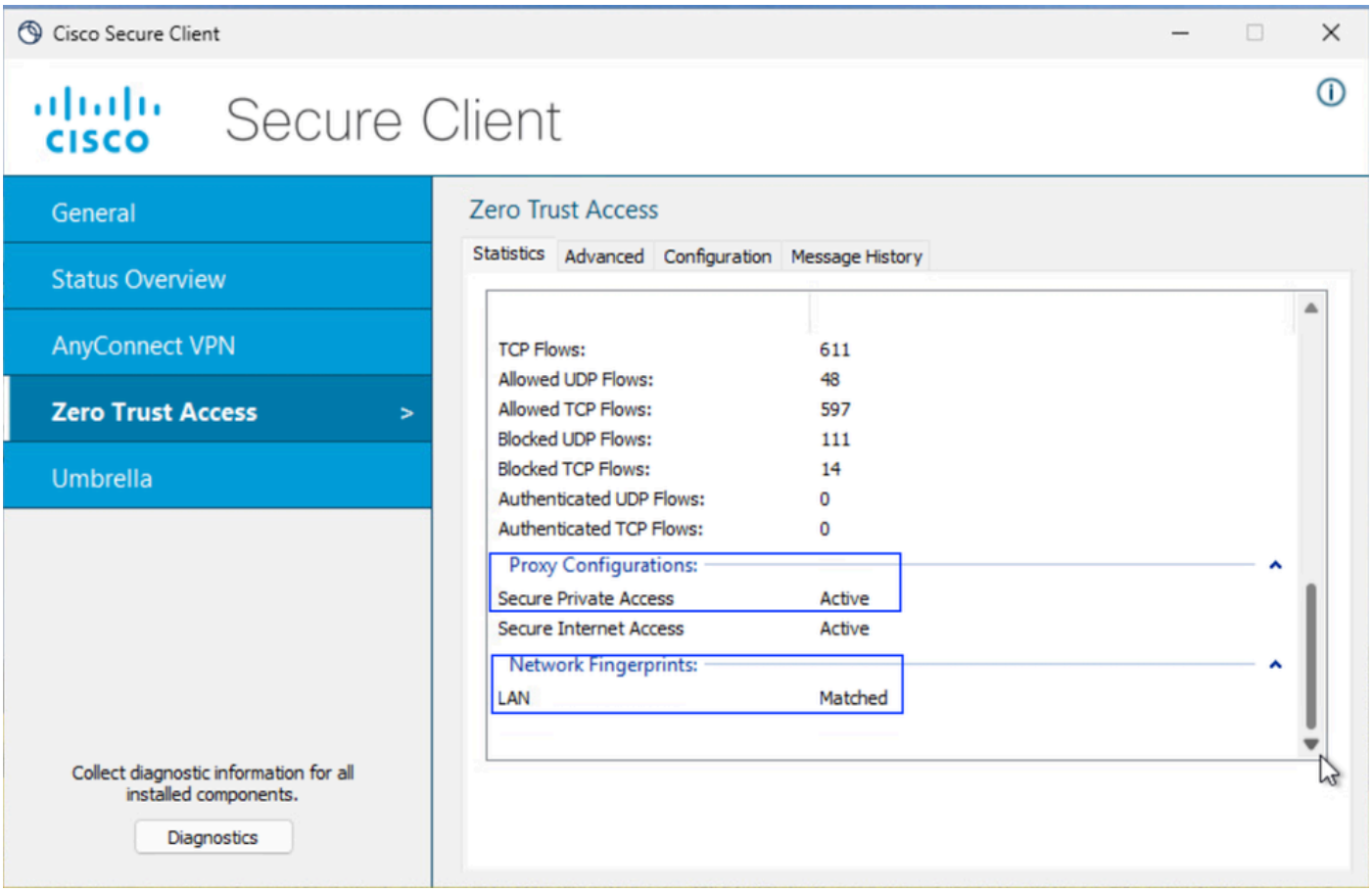


安全访问 — ZTA配置文件

第–6步检验对专用资源的访问

用户为Local时

1.验证ZTA TND的网络指纹，如果用户为本地且安全专用访问应处于活动状态，则该指纹应匹配



安全访问 — PR测试

2. 验证远程用户可以解析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
```

安全访问 — PR测试

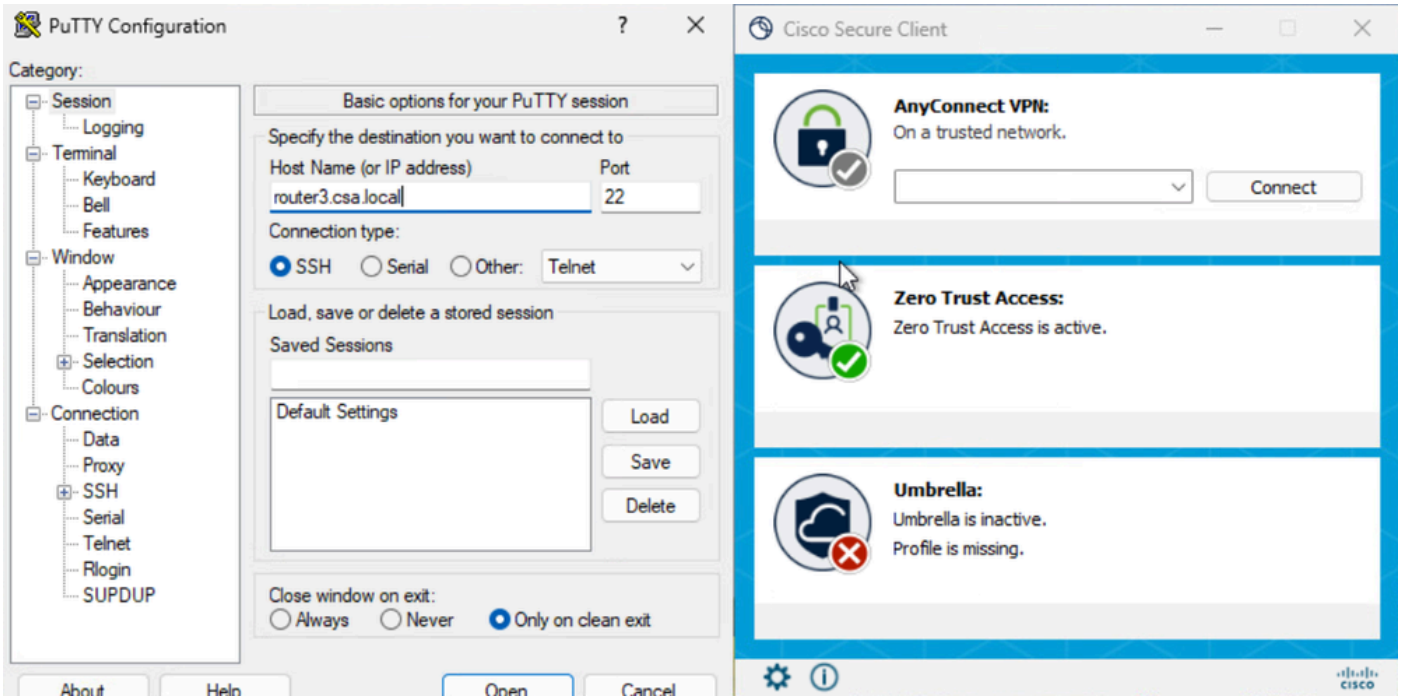
3.验证FTD是否可以使用FQDN访问私有资源

```
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#
```

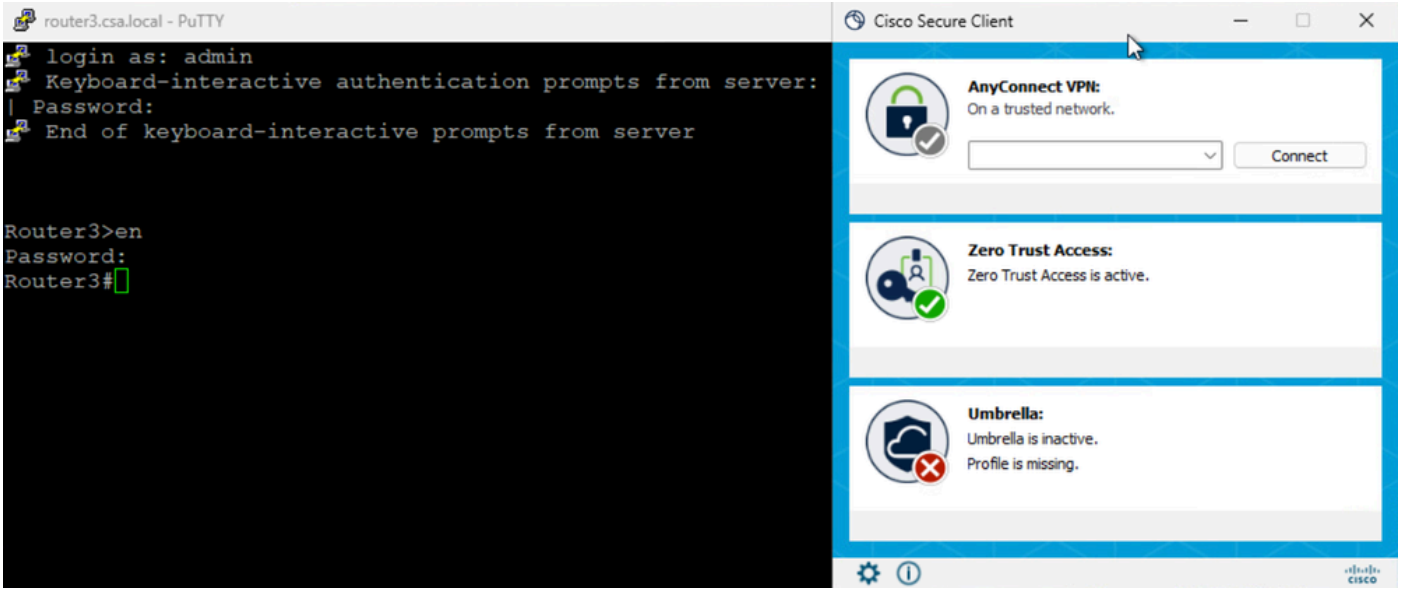
安全访问 — PR测试

4. 测试与专用资源的SSH连接

使用FQDN访问PR

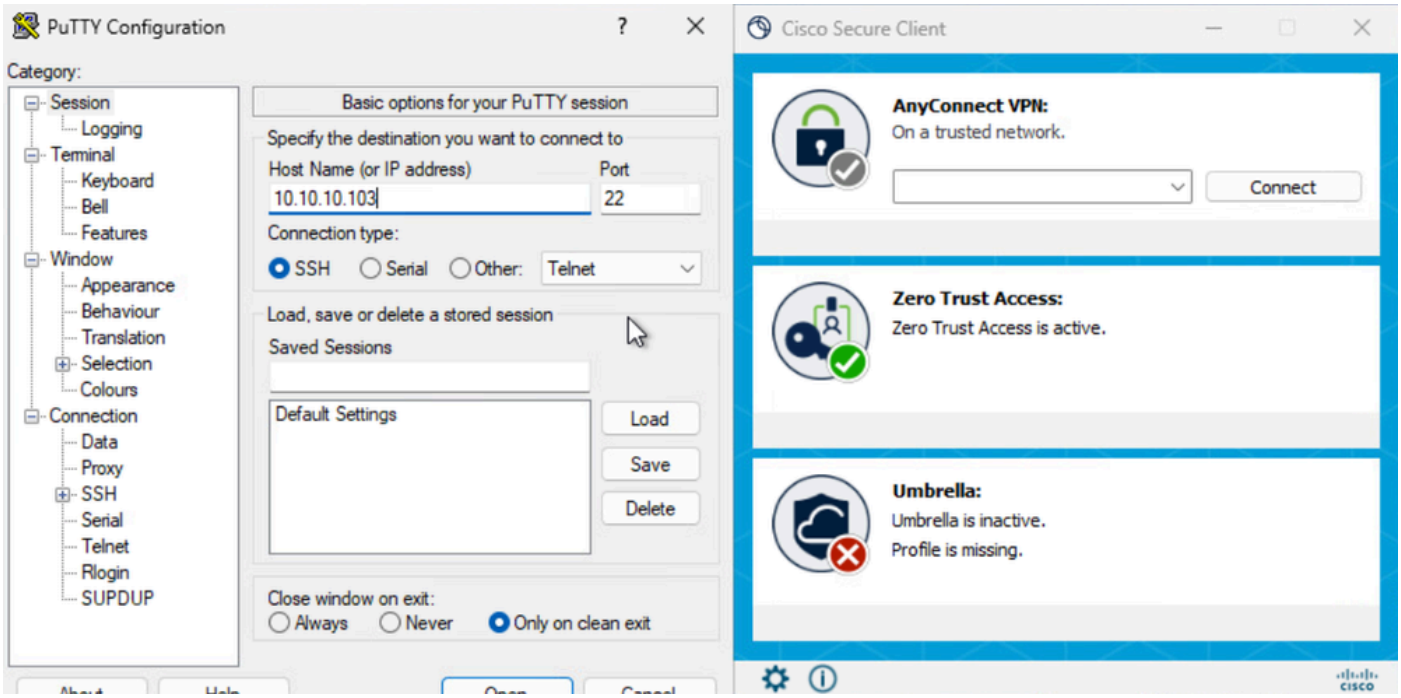


安全访问 — PR测试

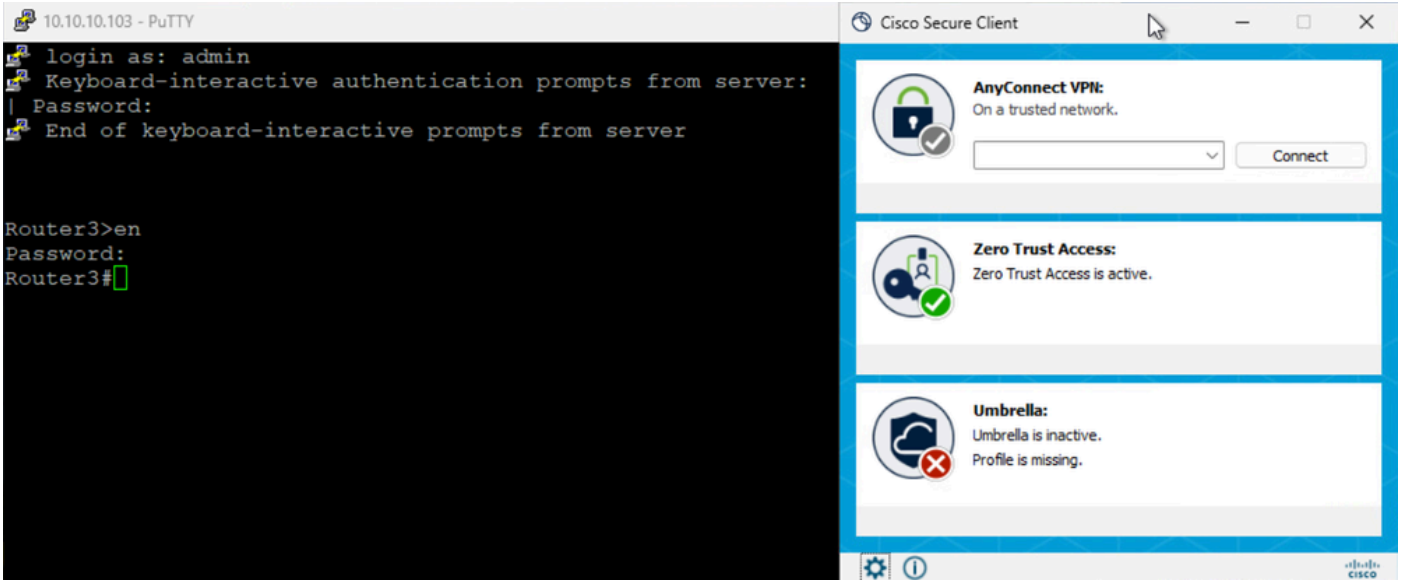


安全访问 — PR测试

使用IP地址访问PR

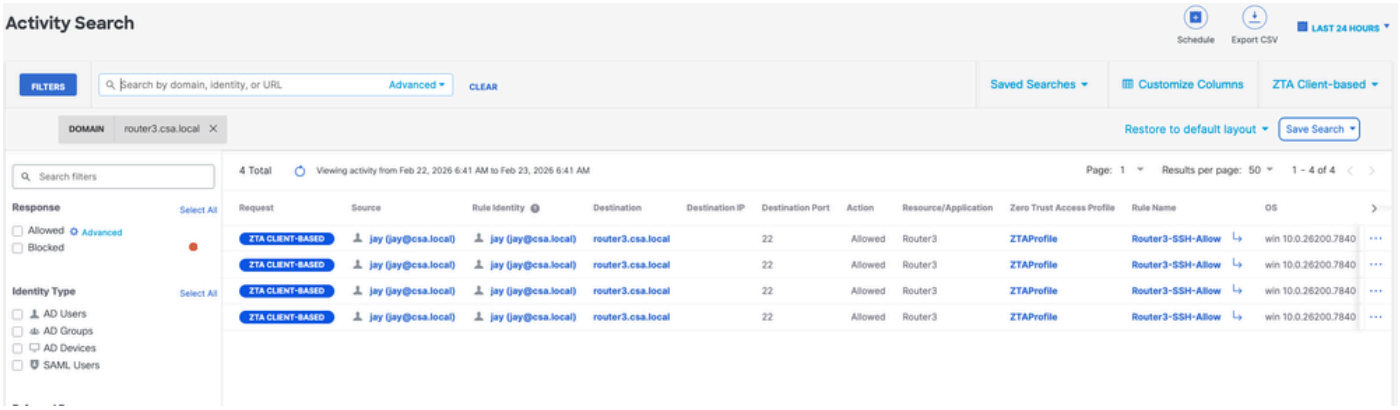


安全访问 — PR测试

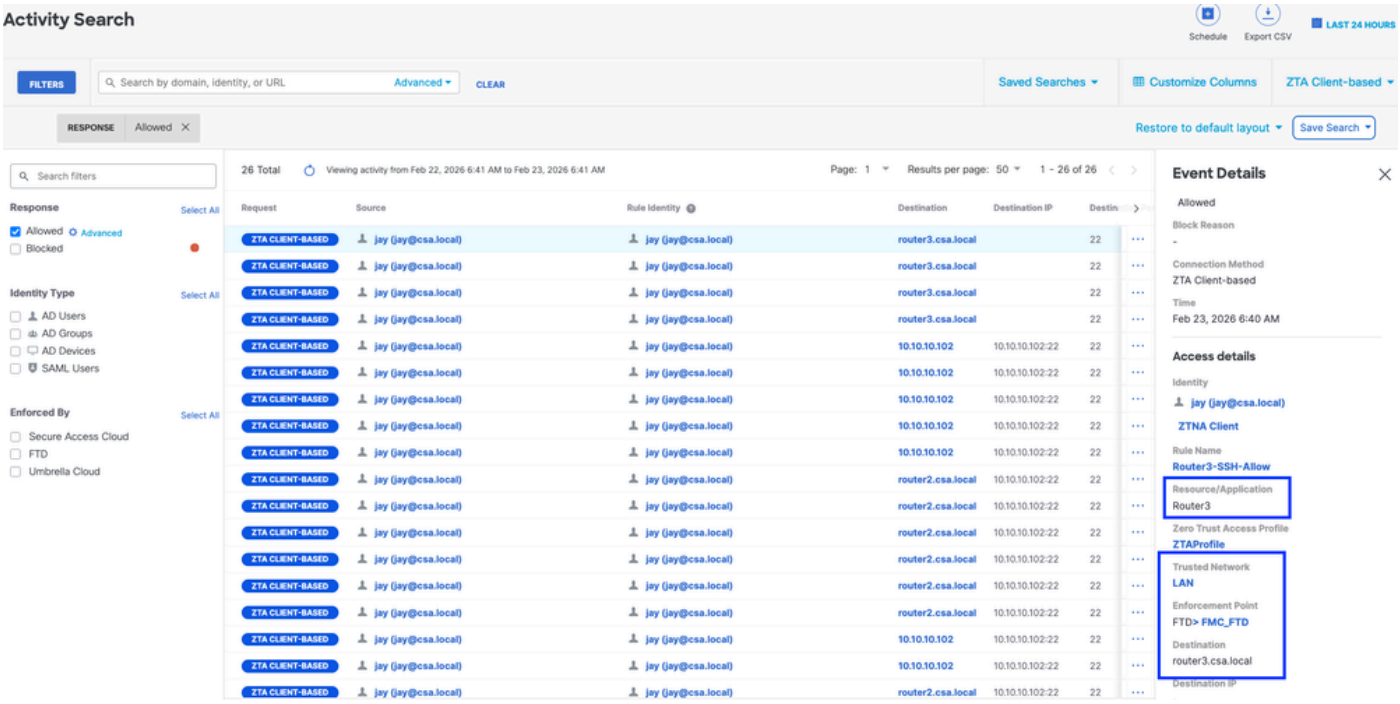


安全访问 — PR测试

5. 验证安全访问活动搜索日志

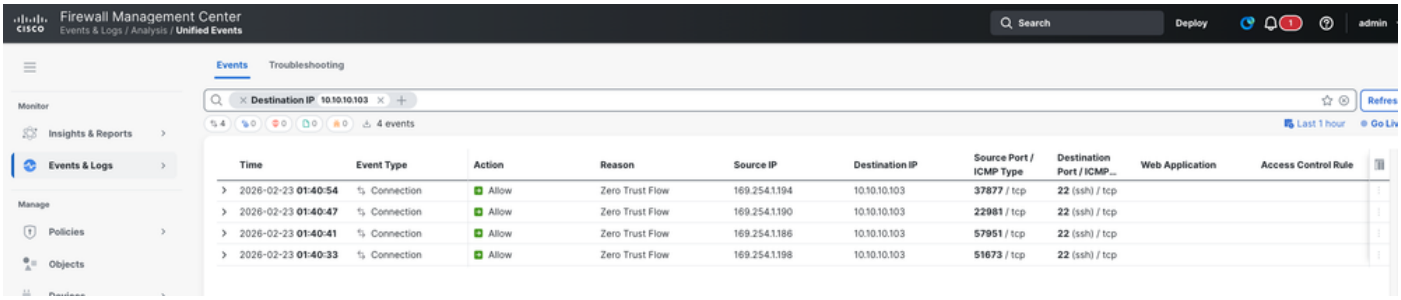


安全访问 — 活动搜索



安全访问 — 活动搜索

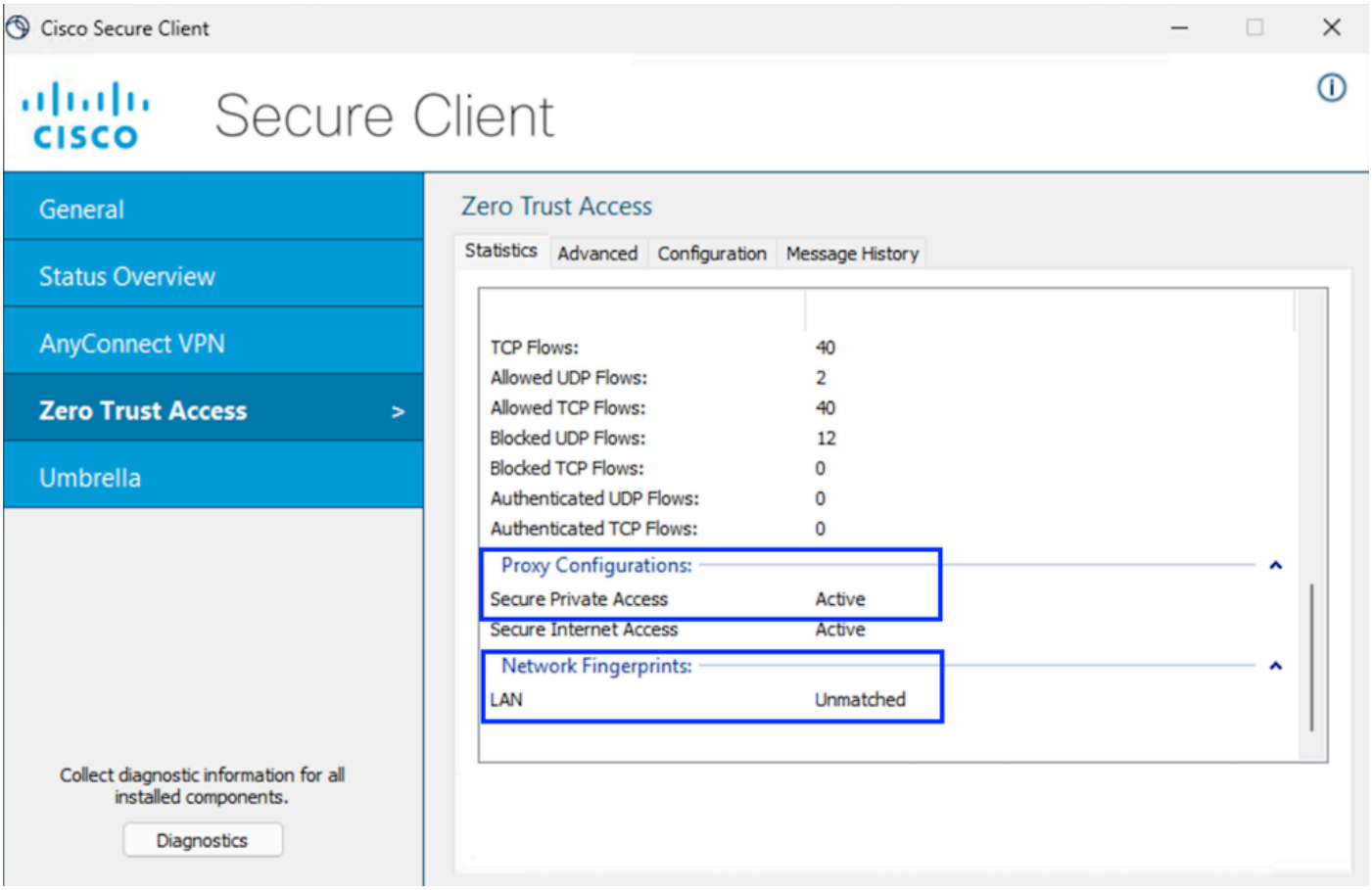
6. 验证FMC连接事件



FMC连接事件

用户处于远程状态时

1.验证ZTA TND的网络指纹，如果用户是远程用户，则应该取消匹配



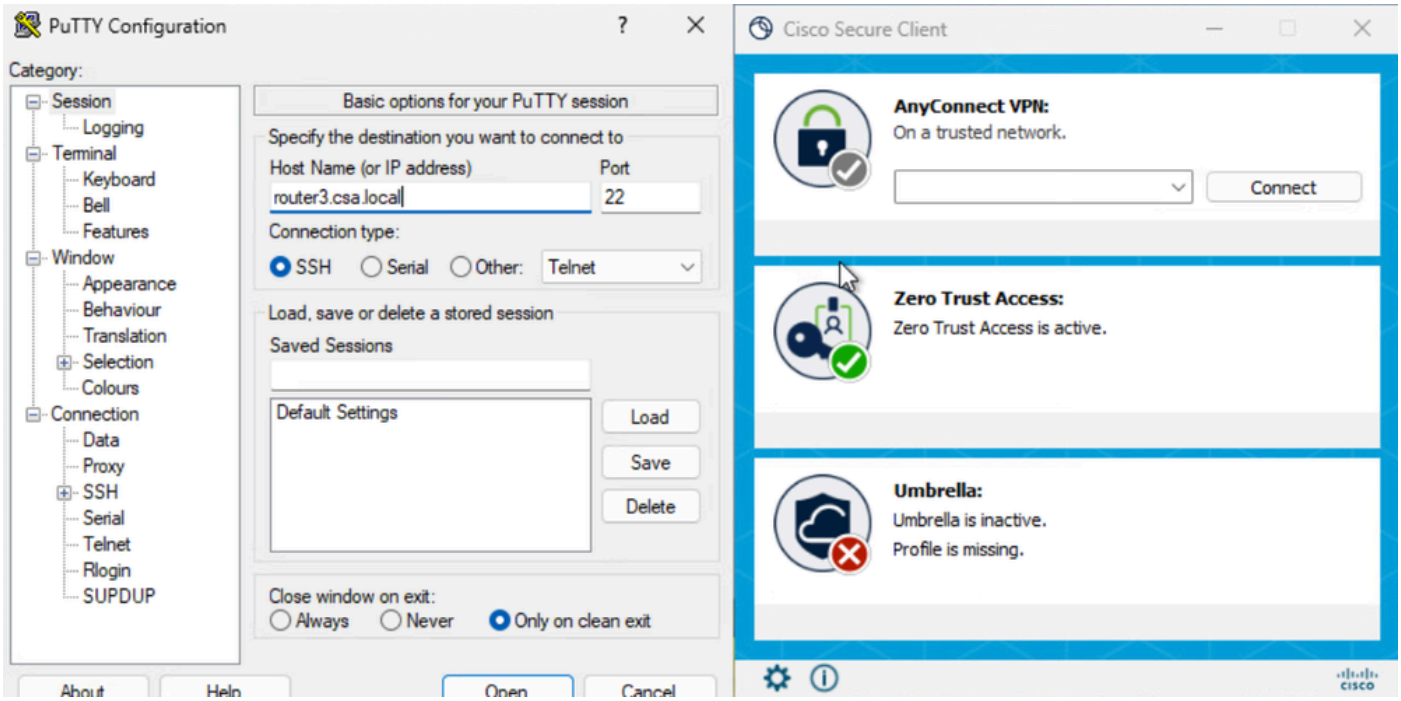
安全访问 — PR测试

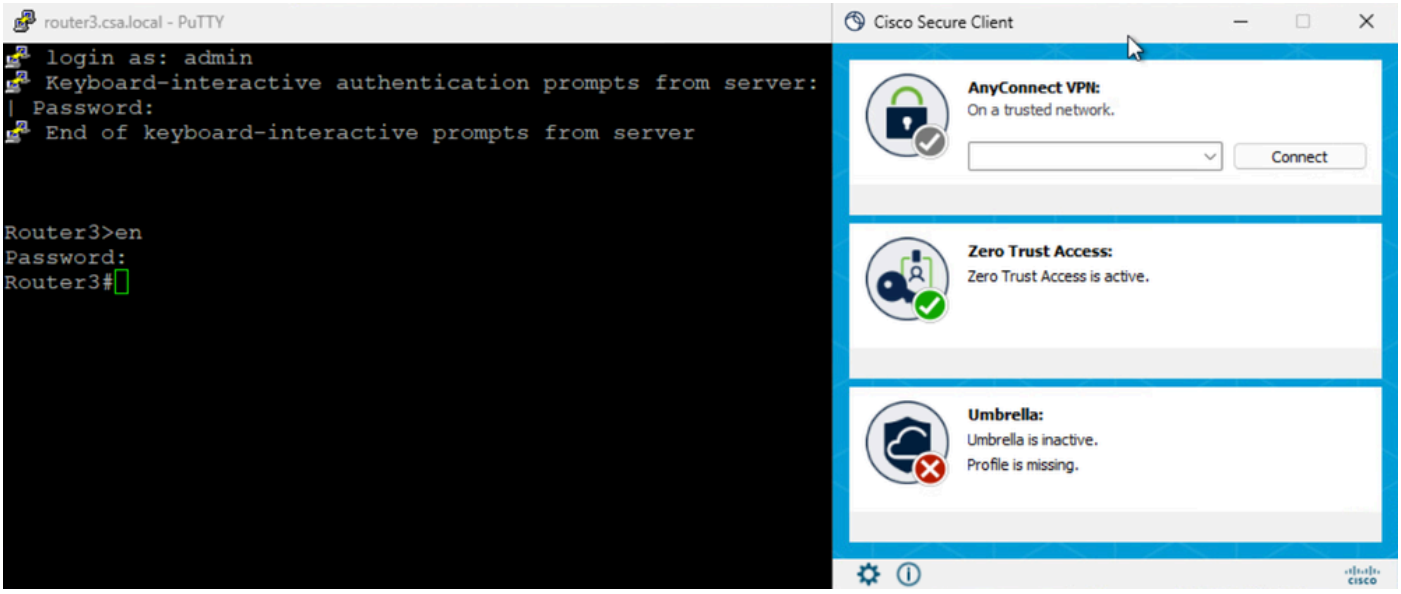
2. 验证远程用户可以解析FTD FQDN

```
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. 测试与专用资源的SSH连接

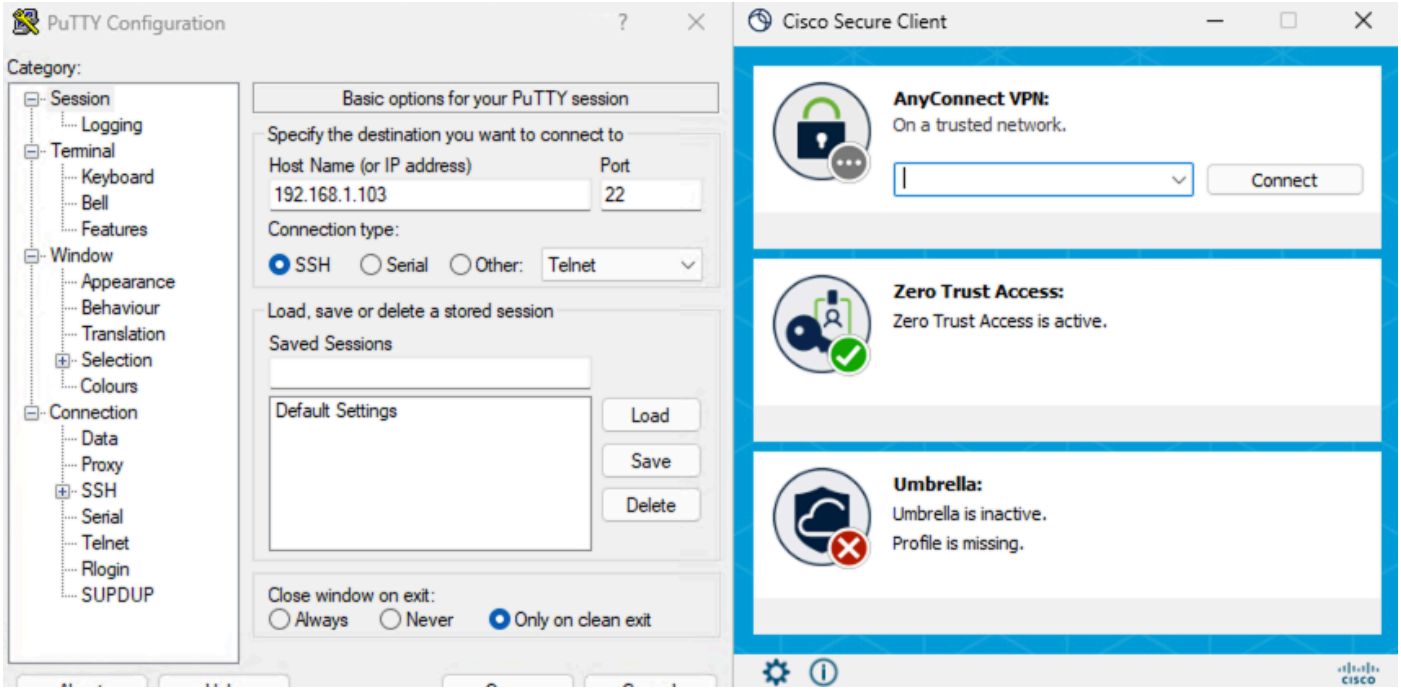
使用FQDN访问PR



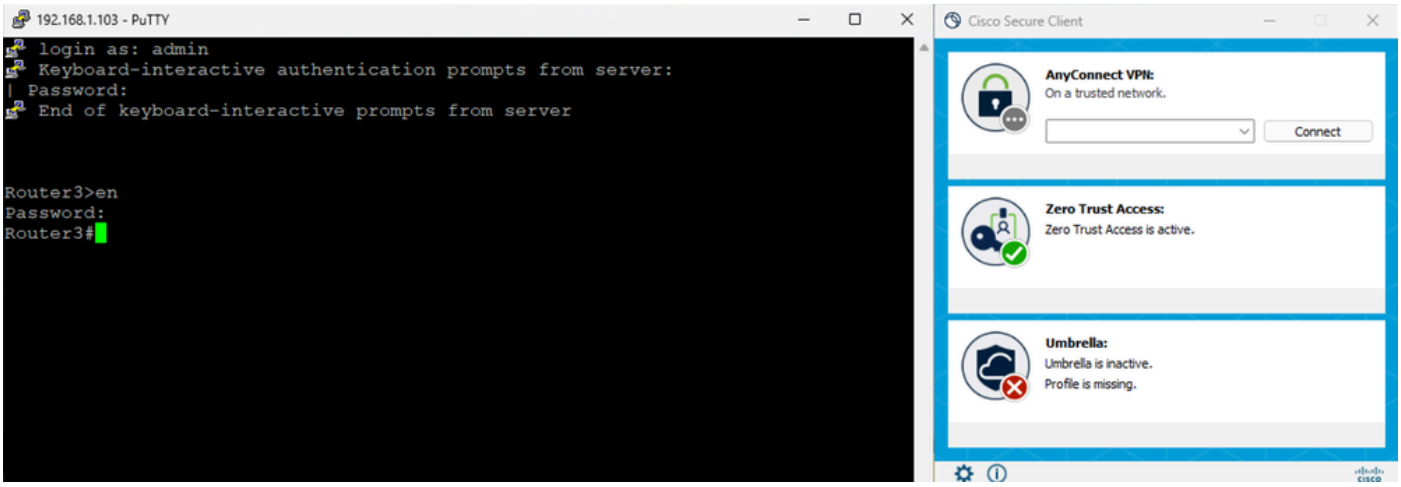


安全访问 — PR测试

使用IP地址访问PR

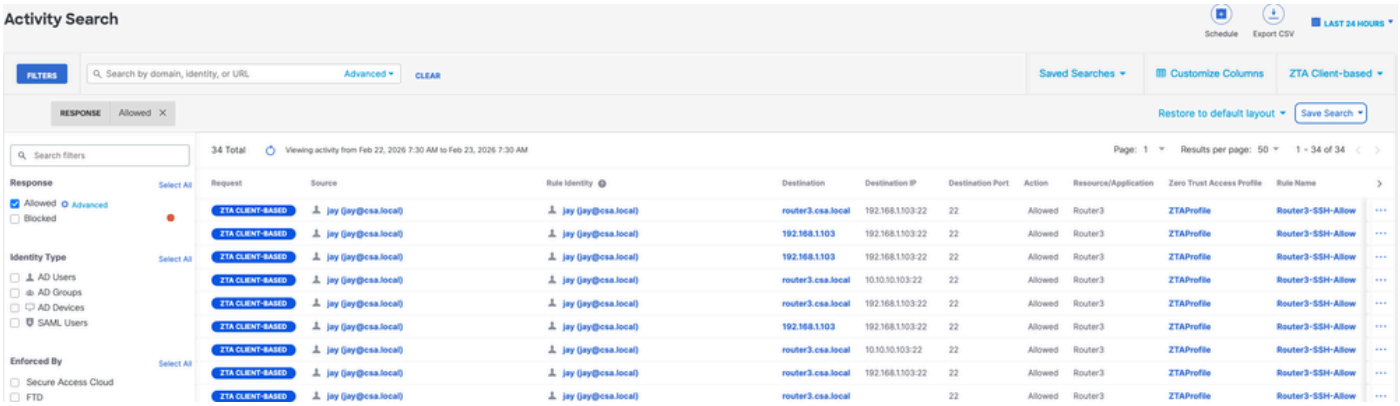


安全访问 — PR测试

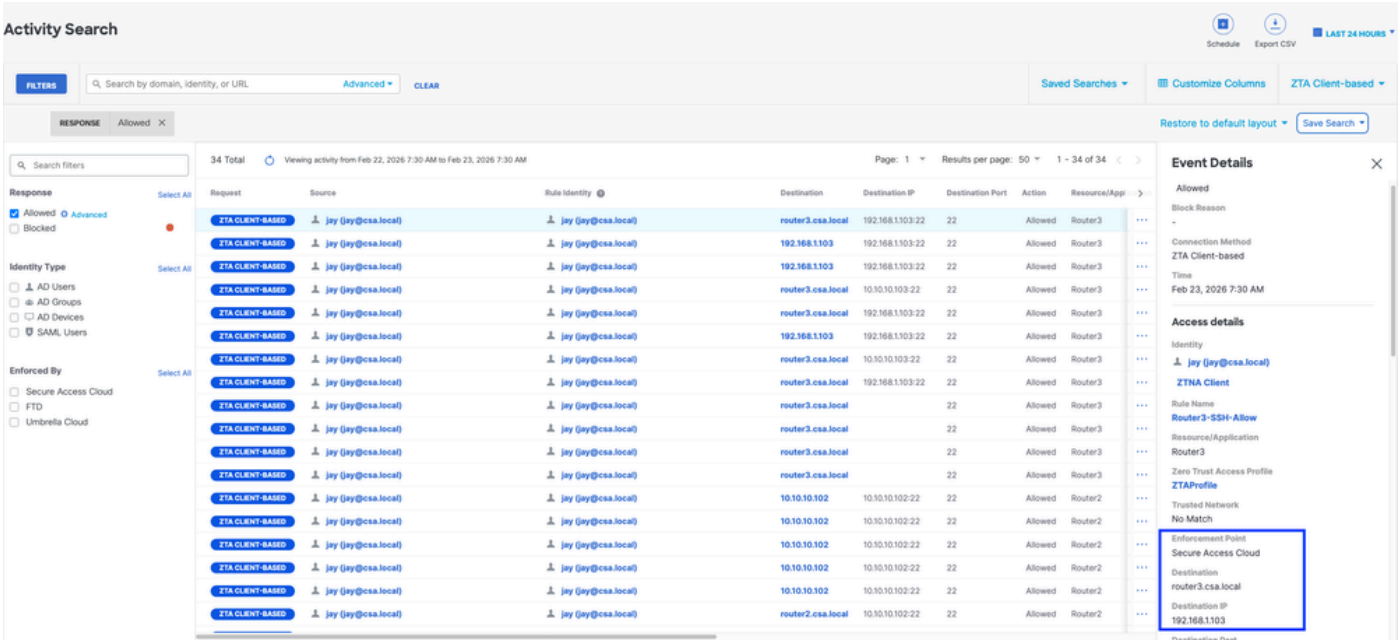


安全访问 — PR测试

5. 验证安全访问活动搜索日志



安全访问 — 活动搜索



故障排除

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

!然后进入专家模式

tail -f /ngfw/var/log/messages

show conn all

show nat detail

show asp table socket

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。