Configuración de ZTNA universal para acceso a recursos privados en acceso seguro

Contenido

Introducción

En este documento trataremos la configuración para el Acceso a Recursos Privados a través de ZTNA Universal con diferentes trayectorias de tráfico.

Prerequisites

La siguiente configuración debe completarse antes de la configuración de ZTNA universal

- Proveedor de identidad en Cisco Secure Access
- Inscriba dispositivos sin acceso de confianza mediante certificados
- Configuración de túneles con Cisco Secure Firewall

- Red privada virtual de acceso remoto
- Conector de recursos en Secure Access
- Incorporación de FTD en el control de la nube de seguridad
- El indicador de la función ZTNA híbrida debe estar habilitado para el arrendatario de acceso seguro respectivo, póngase en contacto con el TAC de Cisco para habilitar el indicador

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de VPN IPsec en Cisco Secure Access y Firewall Threat Defence
- Proveedor de identidad (IdP): aprovisionamiento de usuarios desde Active Directory
- Configuración de VPN remota en Cisco Secure Access
- Implementación del conector de recursos en Cisco Secure Access
- Inscripción basada en certificados ZTA
- Certificado: OpenSSL , generación CSR , plantillas de certificado, etc.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Firewall Threat Defense (Versión 7.7.10)
- Cisco Secure Firepower Management Center (versión 7.7.10)
- Cisco Secure Client (versión 5.1.10.1720 de ZTA)
- Windows 11
- Windows 2019 Server: autoridad certificadora
- Conector de recursos en ESXi

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Acerca de Universal ZTNA

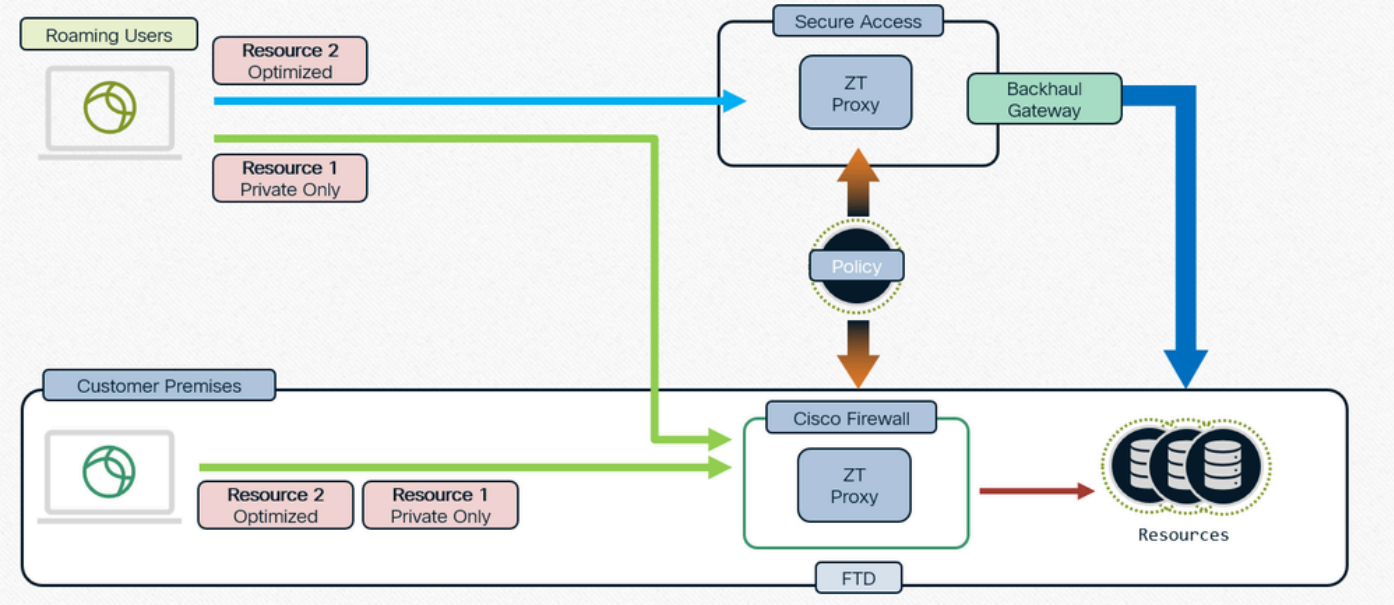
El acceso a la red universal de confianza cero (uZTNA) permite a los administradores permitir

específicamente el acceso a los recursos de la red interna en función de la identidad del usuario (incluida la confianza y el estado del usuario) y sin conceder acceso a toda la red como con RA-VPN. uZTNA permite a los administradores proteger los recursos internos y las aplicaciones tanto para usuarios remotos como locales.

Puesto que ZUTNA no supone que el acceso concedido a una aplicación autorice implícitamente el acceso a otras aplicaciones, se reduce la superficie de ataque a la red.

Secure Access evalúa la política de acceso. Se ignora cualquier política de control de acceso implementada en los dispositivos desde Secure Firewall Management Center.

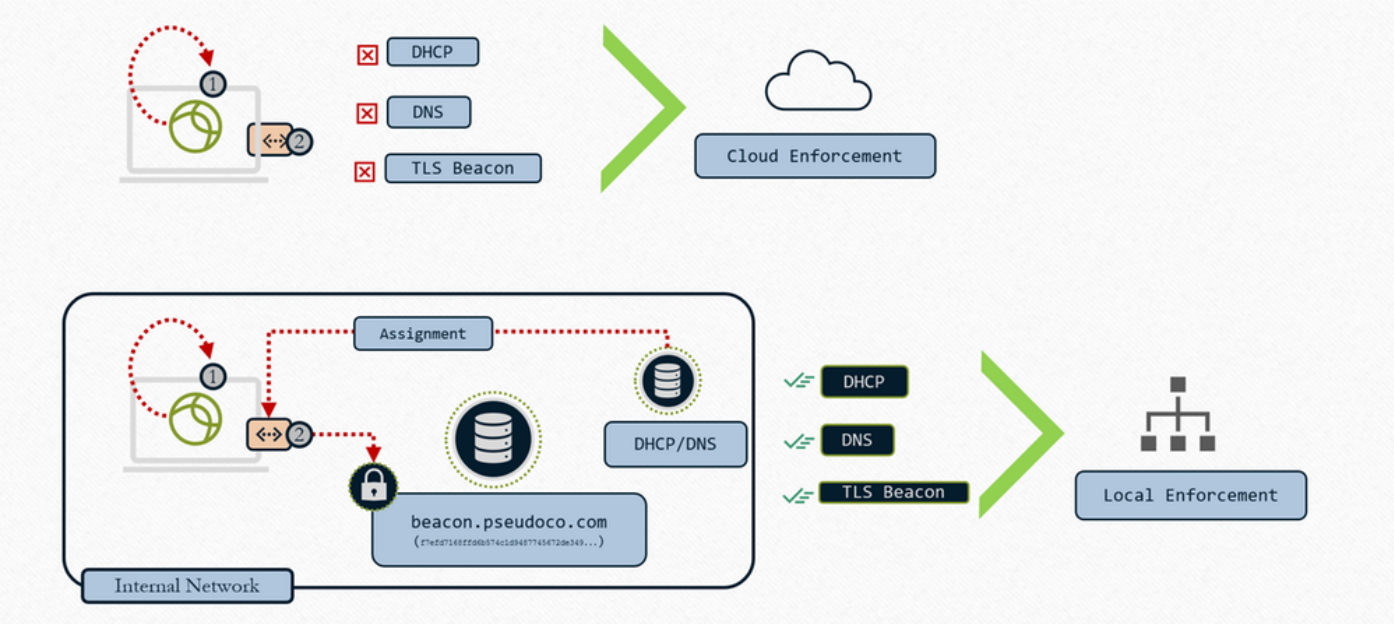
El proxy de tráfico, así como la aplicación de políticas de malware, archivos e IPS, se realiza en Firepower Threat Defence (FTD).



Política única, aplicación distribuida

Detección de red

Determinar la aplicación local o en la nube



ZTNA universal: determinación de la aplicación local o en la nube

1- El cliente interroga la interfaz local para la configuración de la red

2- El cliente busca la baliza TLS

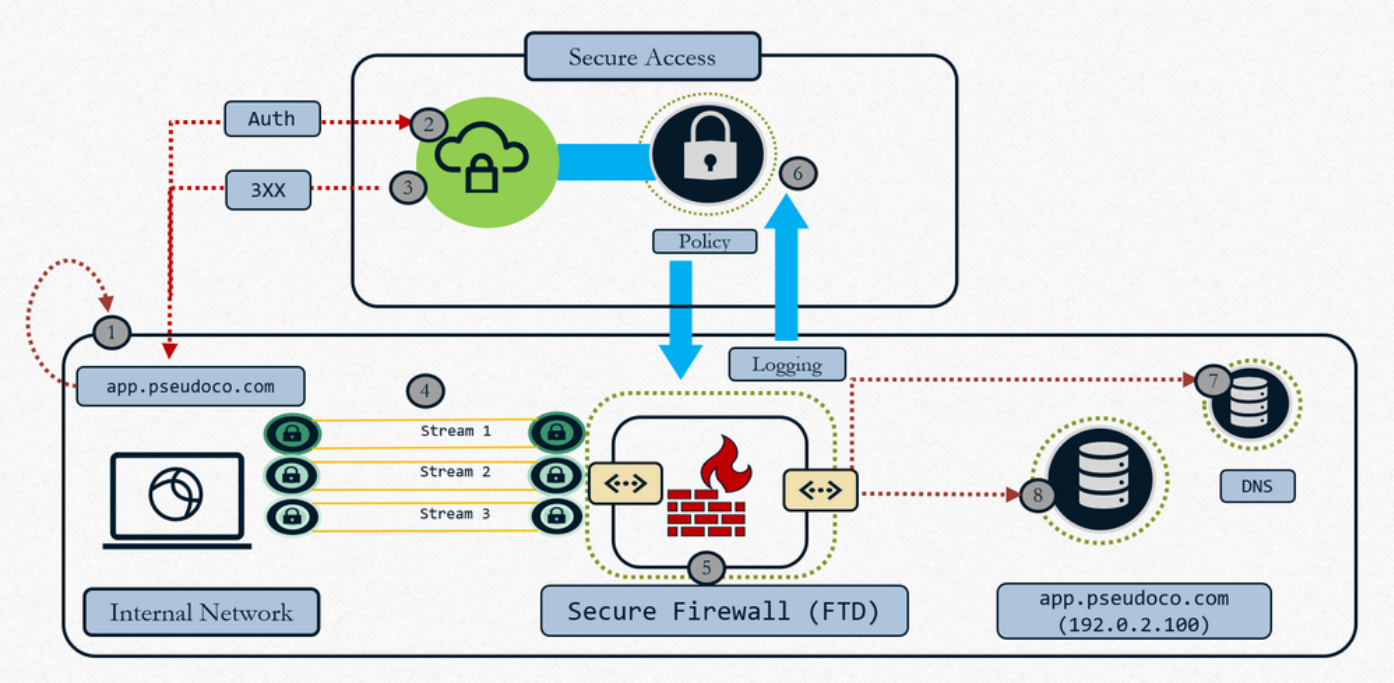
3- Si la condición coincide: aplicación local

4- Si la condición no coincide - Aplicación en la nube

Cuando configuramos el recurso con "Aplicación local o en la nube" y asociamos la regla TND con FTD , lo que realmente hace es que el conjunto de reglas de intercepción que se envía al cliente incluirá la evaluación de la regla TND. Por lo tanto, la nube indicará al cliente que evalúe la regla TND. Cuando enviamos la conexión, ponemos el resultado de esa evaluación de huella dactilar de red de TND en el encabezado HTTP para que indique al proxy si estamos en una red permanente o no fiable y, a continuación, el proxy utiliza esa información y redirige el tráfico en consecuencia. En caso de que la huella digital coincida , Zproxy le dice al cliente que redirija el tráfico a FTD y si la huella digital no coincide redirige el tráfico a la nube. Consulte [Configure Zero Trust Network Access with Trusted Network Detection]

Tipos de aplicación

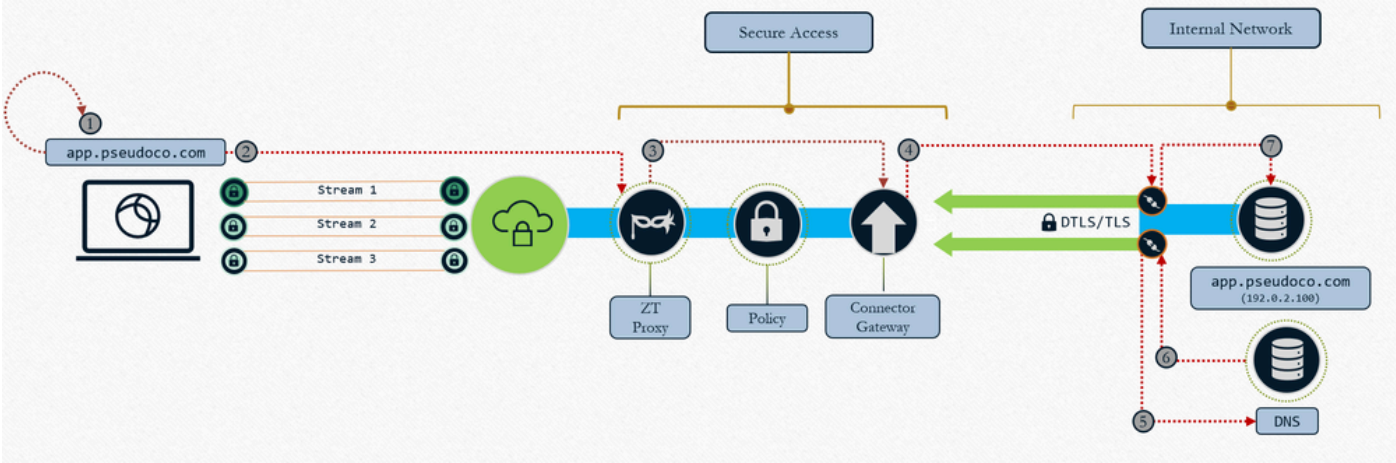
- Ruta de aplicación local: Aplicación de firewall



ZTNA universal: aplicación local

1. El cliente captura y resuelve la solicitud a una IP efímera (intervalo de host local)
2. El tráfico de control de autenticación se envía a la nube de acceso seguro para la evaluación de políticas
3. Las devoluciones en la nube redirigen a FTD para la aplicación del plan de datos (si la política lo permite)
4. Tráfico dirigido a la cabecera configurada como firewall (interfaz)
5. La política definida en la nube se aplica (IPS, malware y descifrado) mediante el plano de datos de proxy local
6. Evento registrado y duplicado enviado a la nube para informes coherentes
7. El firewall realiza la resolución DNS en la red local para enrutar el tráfico de recursos (si se permite)
8. El firewall crea una conexión con el recurso (nueva conexión creada con el recurso) a medida que se comporta como un proxy TCP

- Ruta de aplicación en la nube: RED APAGADA

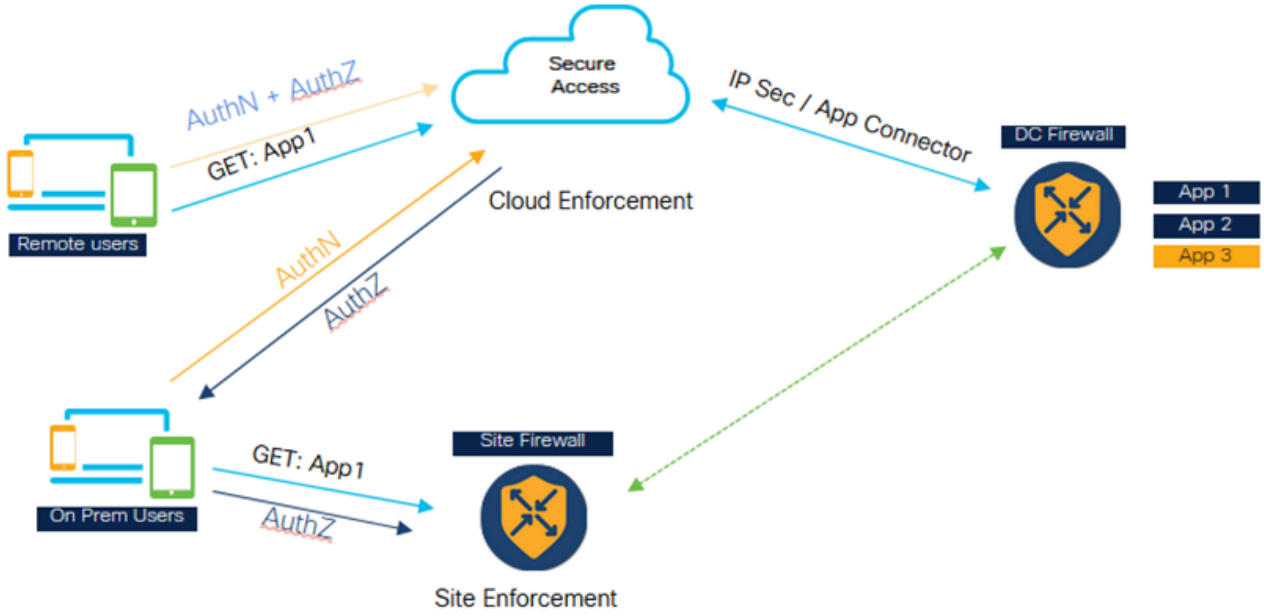


ZTNA universal: Aplicación en la nube

1. El cliente captura y resuelve la solicitud a una IP efímera (intervalo de host local)
2. El tráfico se transporta al proxy de confianza cero en Secure Access
3. La conexión TCP se proxy y se genera en el conector de recursos asignados. La directiva se aplica al tráfico
4. La puerta de enlace establece una conexión con el conector de recursos
5. El conector de recursos resuelve la IP de recursos
6. El DNS local responde con la IP de recurso
7. El conector de recursos establece la conexión con el recurso

Casos de uso

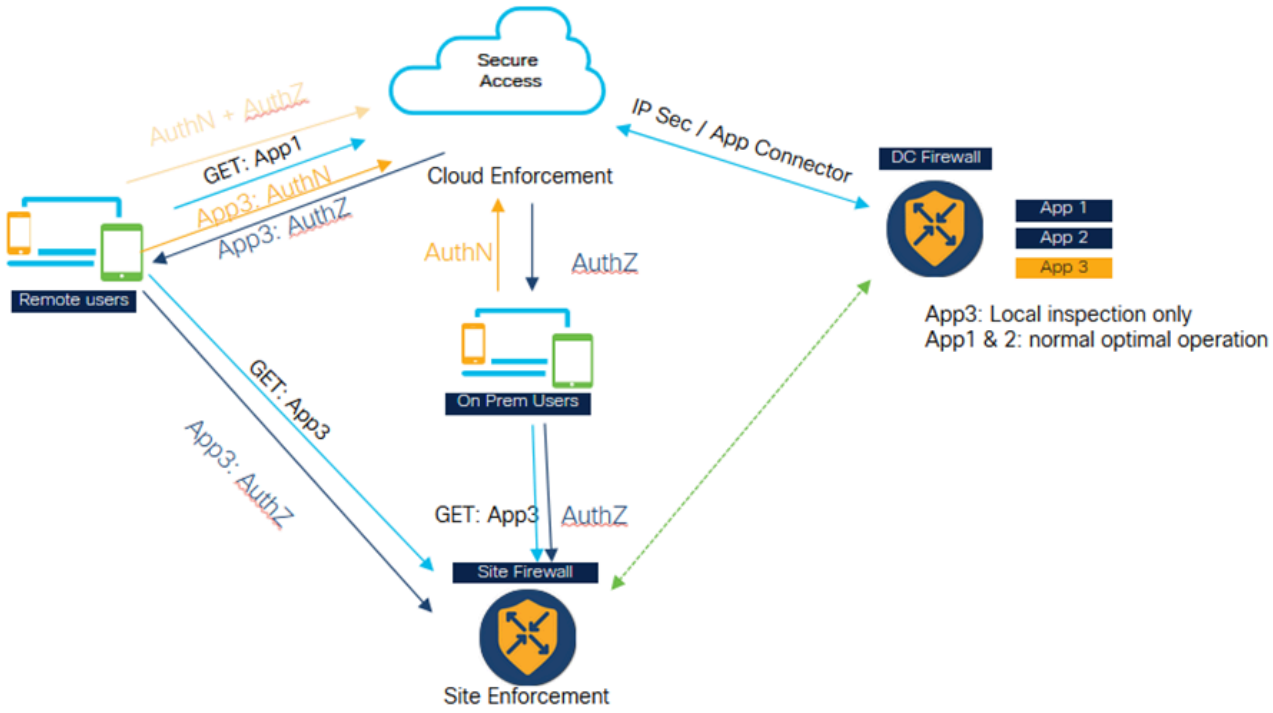
Caso 1: ZTNA coherente y optimizada para los usuarios cuando se encuentren en las instalaciones



ZTNA universal: ZTNA coherente y optimizada (usuario en las instalaciones)

- Secure Access y Firewall están configurados para proteger la aplicación.
- Si el usuario es un usuario remoto, pasará a Secure Access para la evaluación e inspección de políticas.
- Si el usuario es interno/in situ, se dirigirá al firewall para la inspección del tráfico privado.
- En las instalaciones, el usuario todavía puede ir a Secure para la autenticación y la evaluación, solo el tráfico de Datapath va al firewall y se inspecciona según la configuración de la política.
- El usuario interno que accede a la aplicación a través del firewall presenta una ventaja en cuanto a rendimiento, ya que evita que el tráfico se dirija a la nube y, a continuación, al Data Center

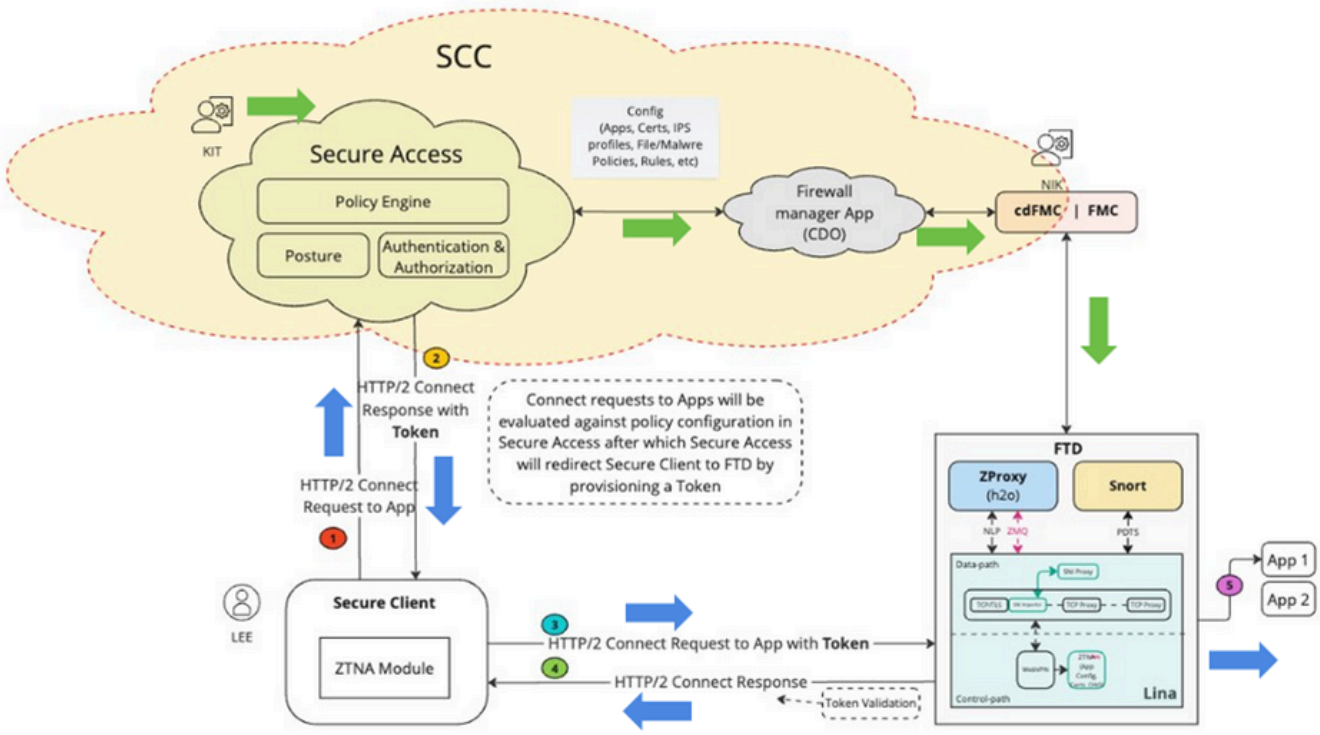
Caso 2: Inspección privada para aplicaciones sensibles



Universal ZTNA - Inspección privada para aplicaciones sensibles

- Determinadas aplicaciones críticas se pueden configurar para que siempre se pueda acceder a ellas a través del firewall.
- El tráfico de datos de la aplicación no necesita pasar a la nube. Por ejemplo, podría haber aplicaciones de datos confidenciales como el código fuente, que los clientes no desean migrar a la nube.
- En estos casos, el tráfico de usuarios tanto remoto como permanente siempre pasa a través del firewall y se inspecciona. Sin embargo, de nuevo, en esta situación, la autenticación y la evaluación de políticas siempre se llevan a cabo en la nube, solo el tráfico de la parte de datos pasa a través del firewall.

Componentes arquitectónicos



Universal ZTA - Componentes arquitectónicos

Security Cloud Control (SCC) es el gestor principal de la solución ZUTNA. ZUTNA es la primera función que se crea sobre SCC.

En SCC , contamos con dos firewall y acceso seguro para microaplicaciones. Una vez que se haya aprovisionado SCC y se hayan habilitado los indicadores de funciones requeridos, podremos ver estas microaplicaciones en el lado izquierdo del panel SCC.

Cliente seguro: En Secure Client tendremos que habilitar Zero Trust Access Module (ZTNA), tenemos que inscribirnos en el módulo ZTNA para poder acceder a las aplicaciones.

Defensa frente a amenazas de firewall: FTD que protege estas aplicaciones. FTD ejecuta un proxy ZT que también se conoce como H2O (igual que el proxy se ejecuta en la nube de acceso seguro)

Ahora, cuando un usuario (por ejemplo, KIT) configura un recurso privado y una política en una microaplicación de acceso seguro, esta configuración se envía a la microaplicación de firewall en SCC. La aplicación de firewall comprende los aspectos internos de FTD , la configuración de FTD, cómo implementar y administrar la configuración en FTD. Por lo tanto, la aplicación de firewall valida esta configuración e invoca las API de FMC para enviar la configuración a FMC y, finalmente, implementarla en FTD. FTD puede tener activada una opción de implementación automática para que los administradores (por ejemplo, Nick) no tengan que realizar la implementación manual.

1. Cuando un usuario (por ejemplo Lee) intenta acceder a una aplicación, el cliente seguro se conecta a Secure Access mediante el canal mTLS. Secure Access autentica al usuario mediante el certificado del dispositivo cliente. A continuación, evalúa la autorización, el estado y otras políticas que se configuran para ese usuario y para esa aplicación.

2. Secure Access , si finalmente encuentra que la aplicación está siendo protegida por Firewall, entonces genera un token de autenticación , que le dice al firewall que esto ya está autenticado y autorizado. El token de autenticación está cifrado y firmado por Secure Access

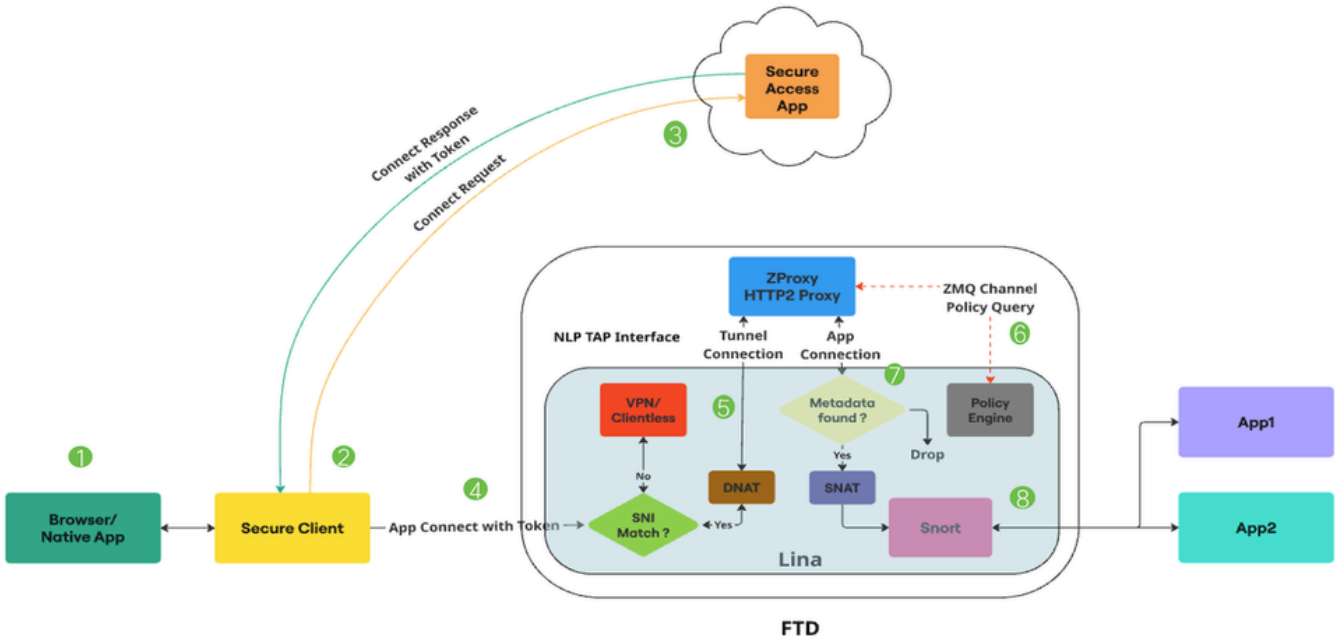
3. Secure Access redirige al cliente seguro hacia FTD junto con el token de autenticación.

4. Secure Client establece otra conexión a FTD , es una conexión HTTP2 sobre el canal mTLS. Envía una solicitud CONNECT para la aplicación a la que se está accediendo junto con el token.

5. El FTD ahora valida el token; si el token se valida correctamente, el usuario tiene permiso para acceder a esa aplicación. A continuación, FTD envía el reconocimiento de vuelta al cliente seguro

Flujo de paquetes

Flujo de paquetes detallado de ZTNA universal



ZTA universal: flujo de paquetes

1. El usuario intenta acceder a una aplicación a través de un navegador web o una aplicación nativa.

2. Secure Client intercepta la conexión y la identifica como un usuario que intenta acceder a un recurso privado.

3. Secure Client establece una conexión mTLS con Secure Access, solicitando acceso a la aplicación.Secure Access comprueba el cumplimiento de las políticas y los perfiles de estado de ZTNA universal.Si todo está bien, Secure Access genera un token de acceso que contiene información esencial como los detalles del usuario, los detalles de la aplicación y la política IPS/Archivo.

4. El token de acceso está cifrado y firmado por Secure Access. A continuación, Secure Access redirige el cliente seguro junto con el token al FTD.

5. Cuando el paquete alcanza la ruta de datos de línea, el verificador SNI intercepta la conexión y verifica si el nombre del servidor (extensión SNI) en el saludo del cliente coincide con el FQDN del proxy configurado en el dispositivo. Si SNI coincide, la conexión se dirige a ZProxy. Si SNI no coincide, la conexión se dirige a otras funciones que pueden coexistir con Universal ZTNA.

Por ejemplo: VPN, portal cautivo o ZTNA sin cliente. ZProxy, que admite el protocolo MASQUE sobre HTTP/2, se ejecutará en el FTD como un proceso no lineal en núcleos dedicados. La comunicación entre Lina y ZProxy utiliza la interfaz de NLP Tap para gestionar el tráfico de datos. El verificador SNI traduce la IP de destino de la conexión a la IP de interfaz TAP.

6. Cuando ZProxy recibe la conexión de túnel mTLS de Secure Client, verifica el certificado de dispositivo de cliente enviado por Secure Client. También verifica el token de acceso enviado con APP Connect. Hay un canal Zero MQ entre Lina y ZProxy. Se utiliza principalmente para intercambiar mensajes de control. ZProxy utiliza este canal para la resolución FQDN de recursos privados mediante la comunicación con Lina.

Zero MQ Channel también se utiliza para propagar la información presente en el token de acceso a Lina.(Ejemplo: ID de regla, ID de política, etc.) Lina recibe la información del token de acceso y la almacena en una base de datos de metadatos.

7. Una vez intercambiados los mensajes de control, ZProxy inicia una nueva conexión con el recurso privado. Puede ser TCP o UDP. Lina realiza una búsqueda en la base de datos de metadatos para esta conexión de aplicación. Si no se encuentran los metadatos, se descarta Connection

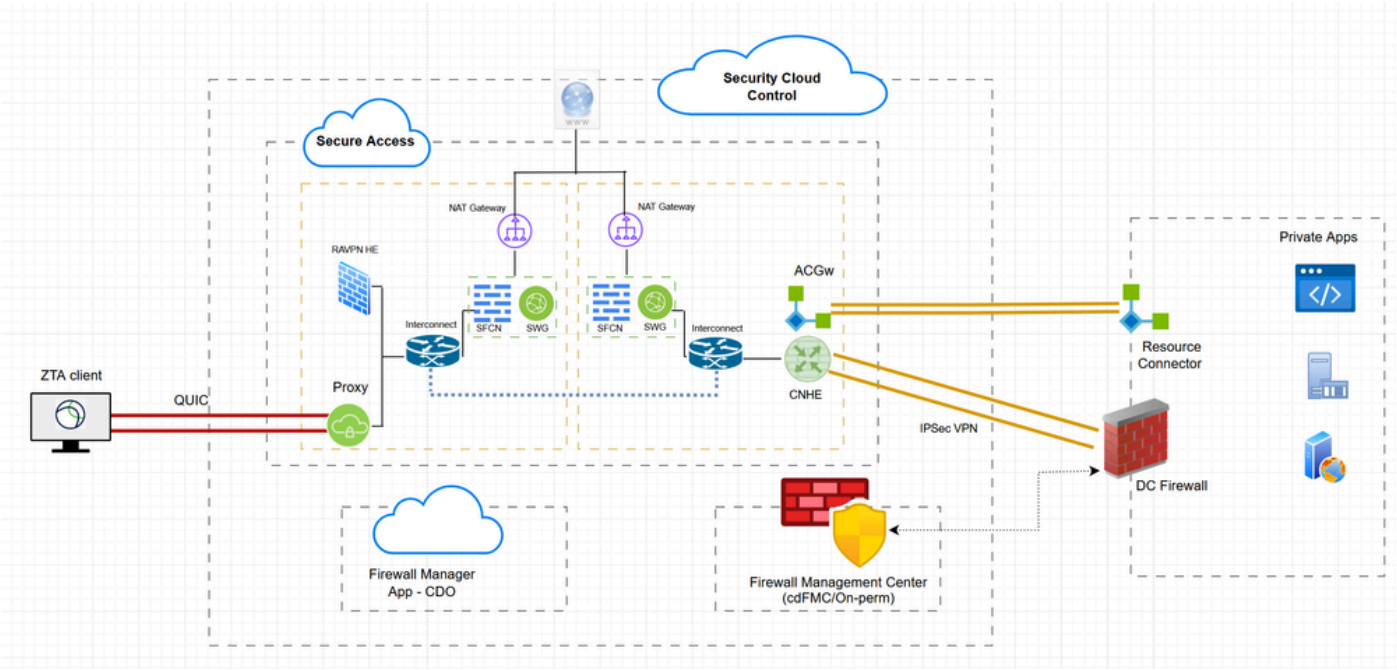
8. Dado que la conexión de la aplicación se origina desde ZProxy, tendrá una IP interna (ejemplo: 169.251.1.2) como IP de origen. Esto se traducirá a la IP de la interfaz de salida de FTD, antes de enviarla. Lina marca los flujos de confianza cero universal para la inspección de Snort solo si hay un archivo o una política IPS en el token de acceso. El ID de regla obtenido del token de acceso se pasa a Snort en los metadatos de conexión.

9. Las reglas de confianza cero universal y las asignaciones de políticas de IPS y archivos correspondientes se envían al FTD a través del FMC. El complemento Zero Trust de Snort cargará estas reglas durante la inicialización. Lina marcará los flujos de flujos de Zero Trust universal para la inspección de Snort solo si se menciona un archivo o una política IPS en el token de acceso obtenido de Secure Access para acceder a ese recurso privado.

El ID de regla obtenido del token de acceso se pasa a Snort a través de Conn Meta. Para todos los flujos de flujo de confianza cero universal, el complemento de confianza cero de Snort realizará una búsqueda de regla para el ID de regla obtenido de Conn Meta. Si se encuentra una coincidencia de regla, se permitirá el flujo y se aplicarán al flujo las políticas de IPS y de archivos específicas de esa regla. Si no se encuentra ninguna coincidencia de regla, el complemento de confianza cero de Snort bloqueará el flujo.

Configurar

Diagrama de la red

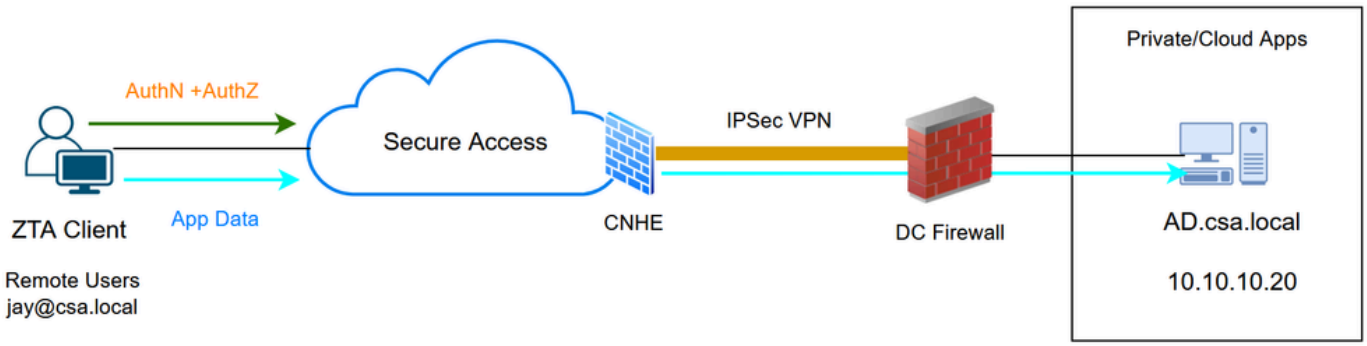


ZTNA híbrido: Diagrama de red

Casos de prueba

Caso de prueba 1: Usuario remoto - Aplicación en la nube

En este caso de prueba, accederemos a un recurso privado a través del grupo de túnel de red mediante la aplicación en la nube. En este caso, tanto la evaluación de políticas como los datos de aplicaciones serán interceptados por Secure Access a través del módulo ZTA . Se trata de un flujo tradicional en el que se puede acceder a una aplicación privada desde un cliente inscrito en ZTA a través del grupo de túnel de red o el conector de recursos

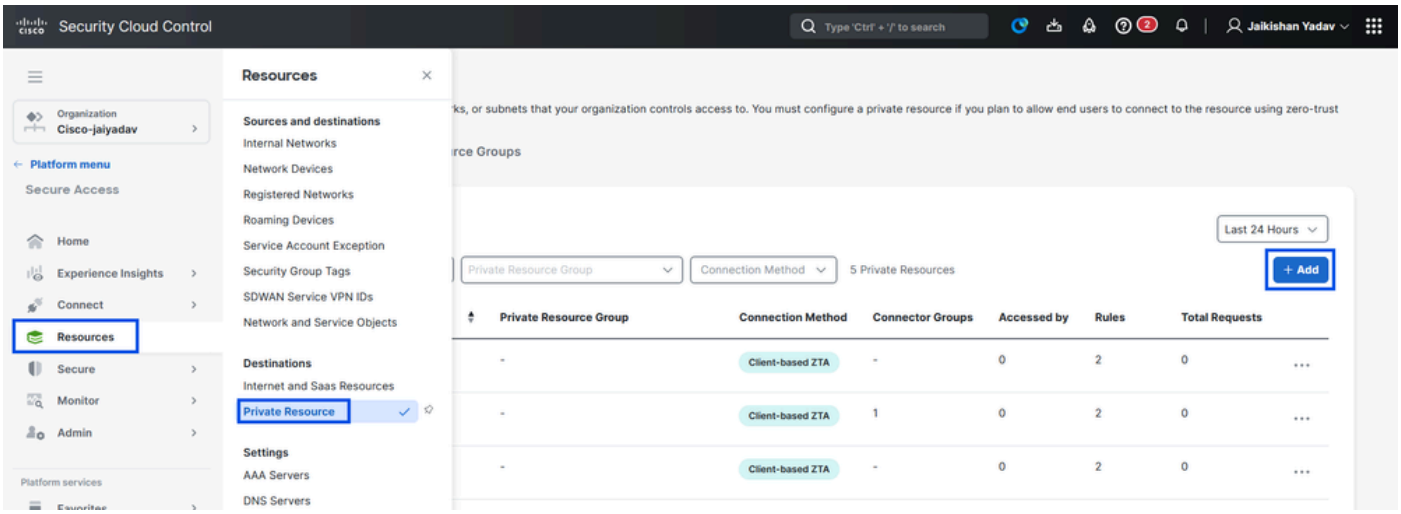


ZTA universal: topología de caso de prueba

Paso 1 - Definir un recurso privado en Secure Access

Configure un recurso privado al que se pueda acceder a través del dispositivo inscrito de acceso de confianza cero (ZTA) con aplicación en la nube

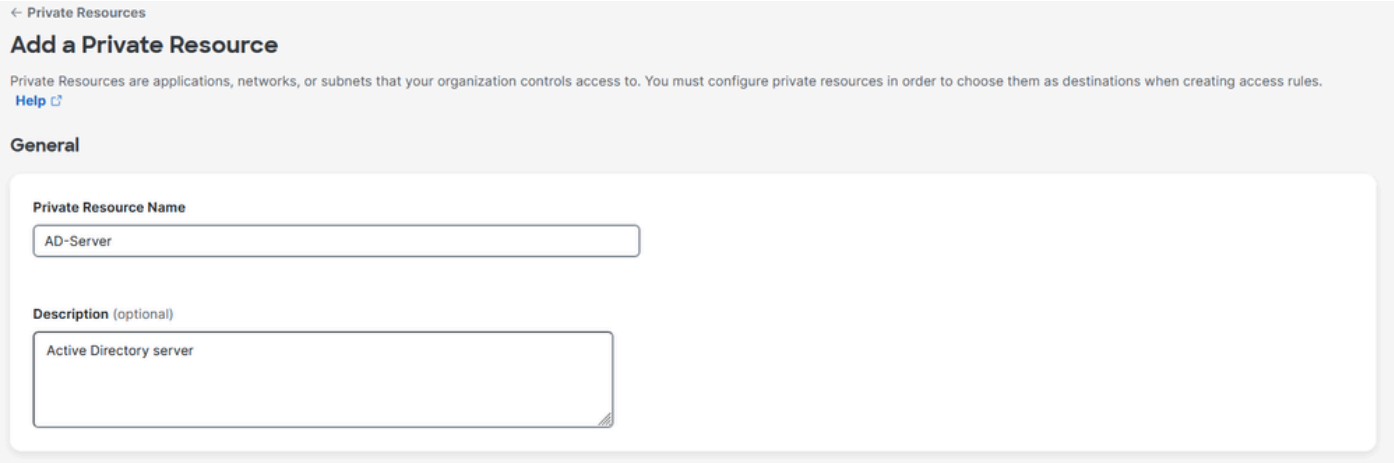
1. Navegue hasta Recursos > Destinos > Recursos privados > Haga clic en +Agregar



Acceso seguro - Configuración de recursos privados

2. En Nombre de Recurso Privado, introduzca un nombre significativo para el recurso. Para

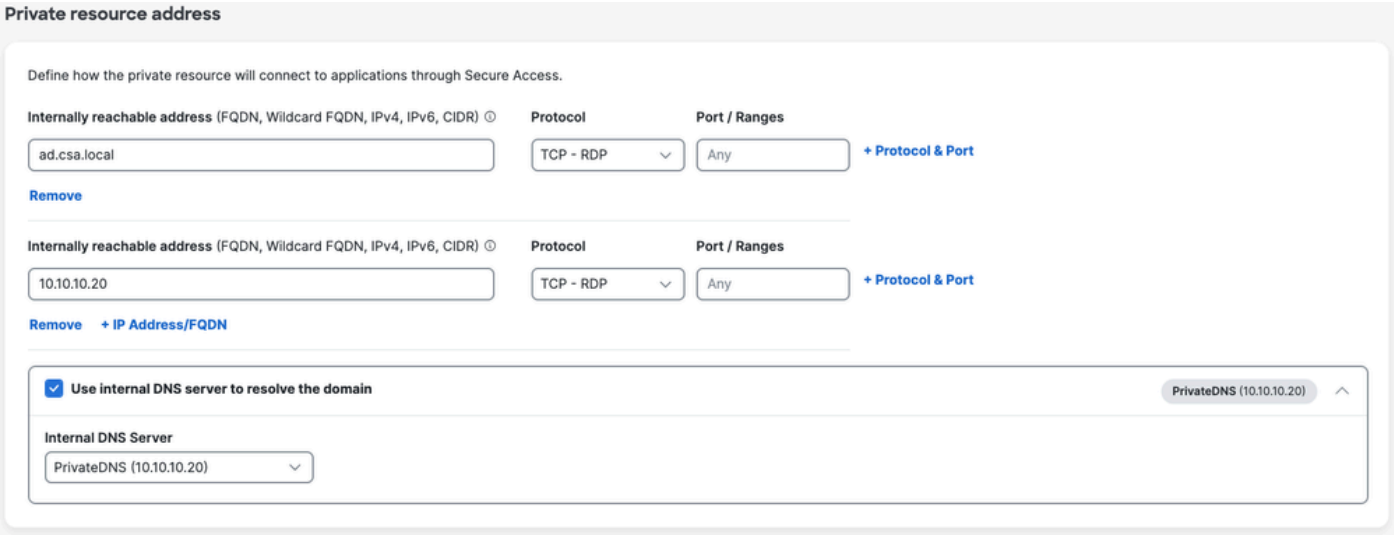
Descripción, se recomienda proporcionar información como el propósito del recurso o el nombre del propietario del recurso.



Acceso seguro - Configuración de recursos privados

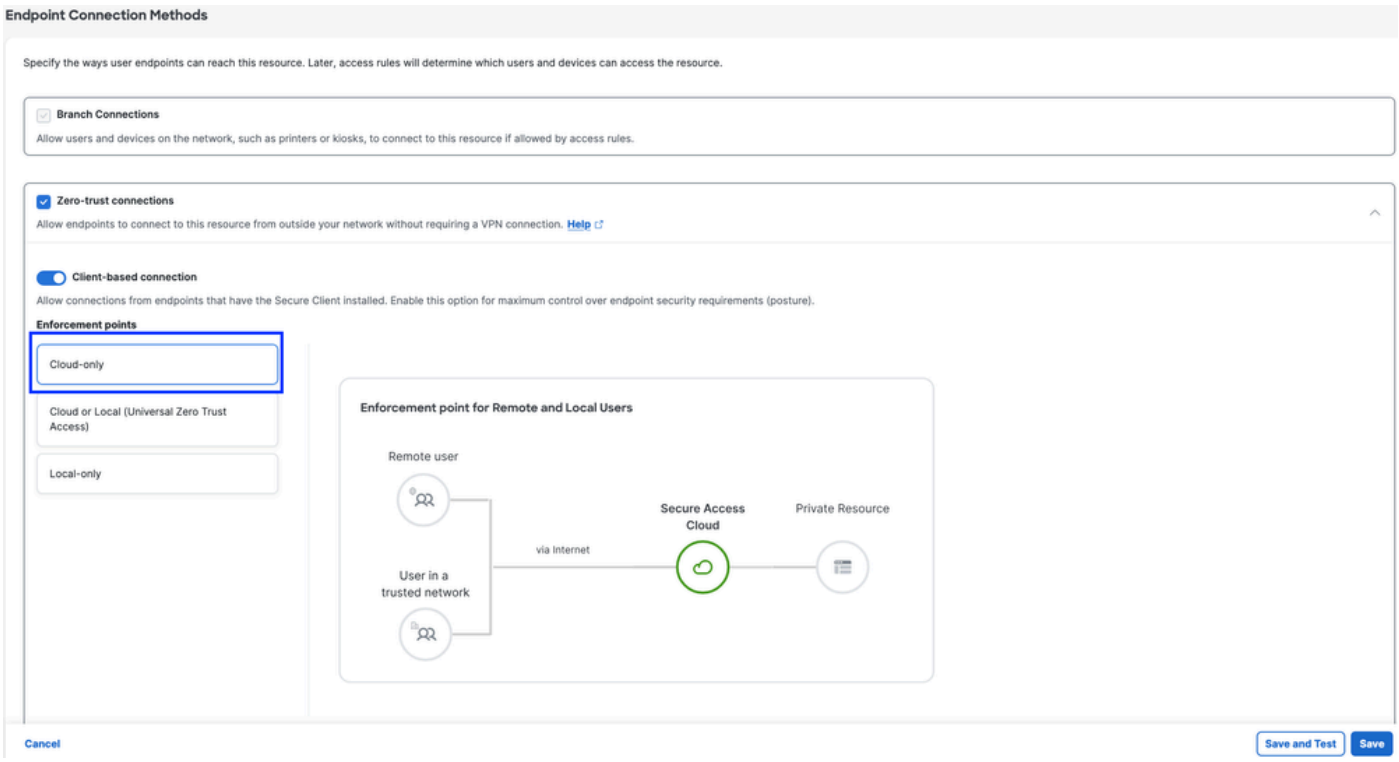
3. Introduzca el FQDN del recurso privado al que desea acceder . También podemos definir la dirección IP del recurso privado . Para obtener más información, vea Agregar un recurso privado

4. Seleccione el servidor DNS interno para resolver el dominio



Acceso seguro - Configuración de recursos privados

5. Seleccionar métodos de conexión de terminales



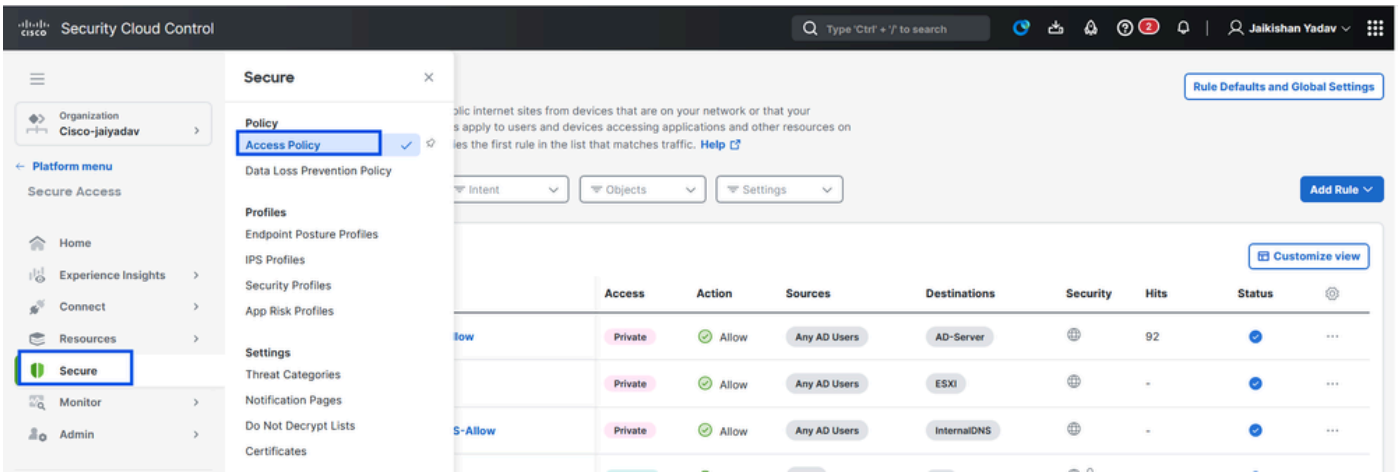
Acceso seguro - Configuración de recursos privados

6. Haga clic en Save (Guardar).

Paso 2: Crear regla de acceso privado

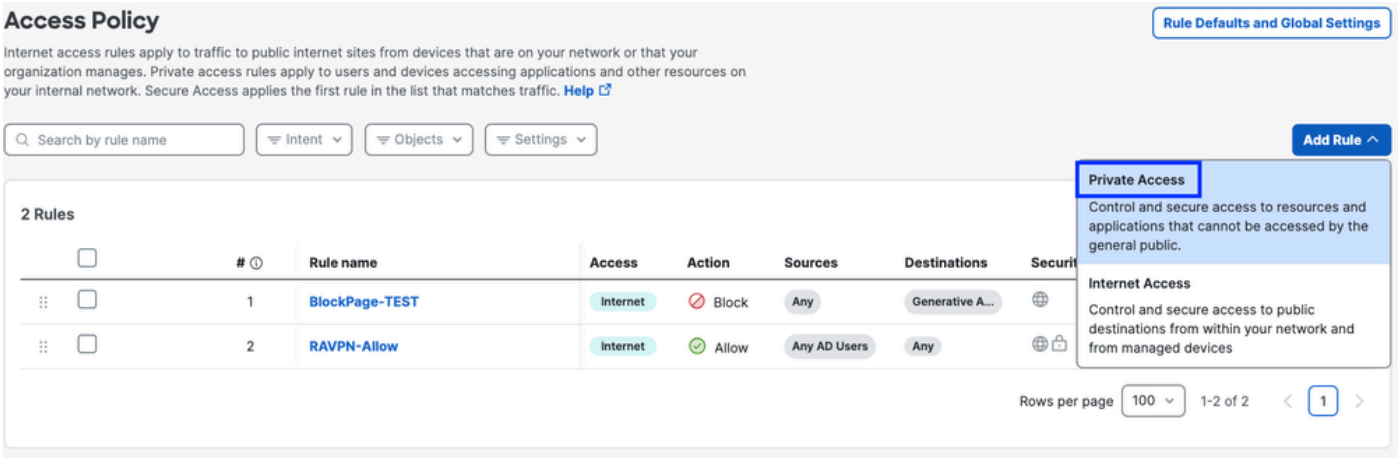
Configure un acceso privado en Secure Access para que los usuarios inscritos en Universal ZTA puedan acceder . Para obtener más información, vea Regla de acceso privado

1. Vaya a Seguro > Política de acceso



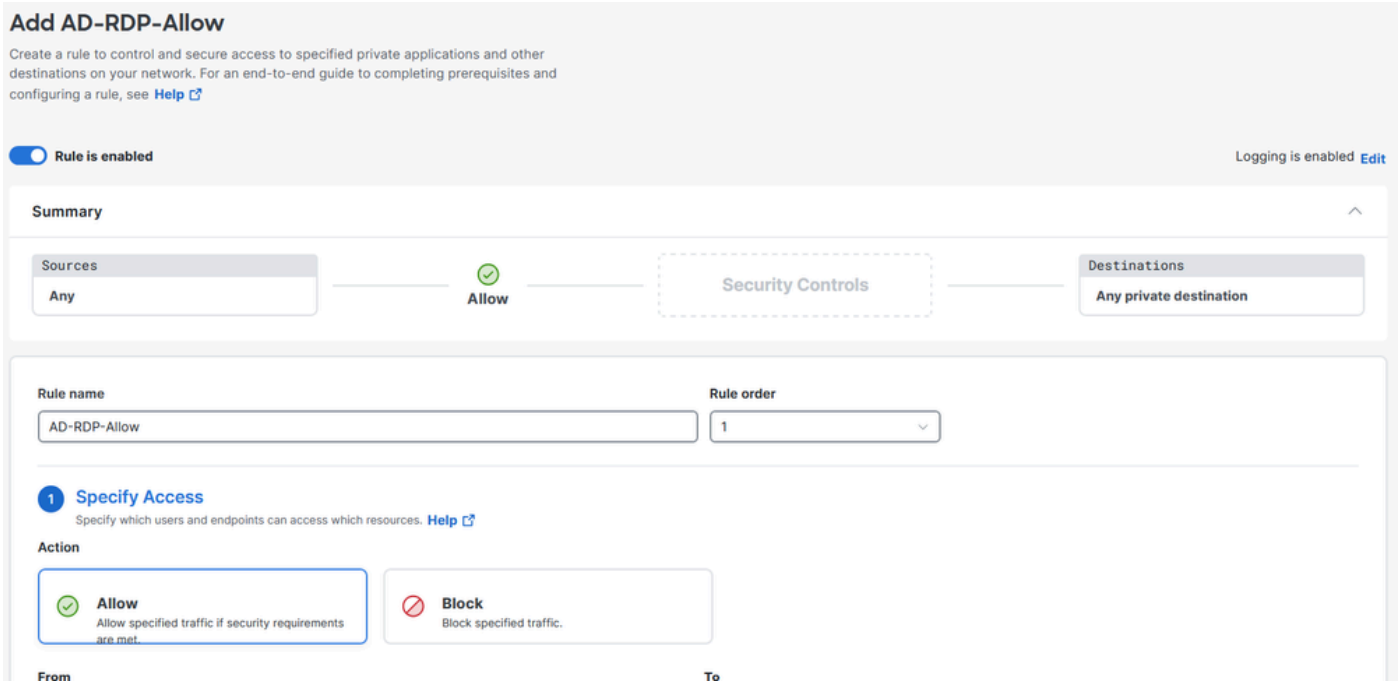
Acceso seguro - Configuración de la política de acceso

2. Haga clic en Agregar regla, y luego elija Acceso privado.
   En la parte superior de la regla hay un resumen que describe los componentes configurados de la regla.



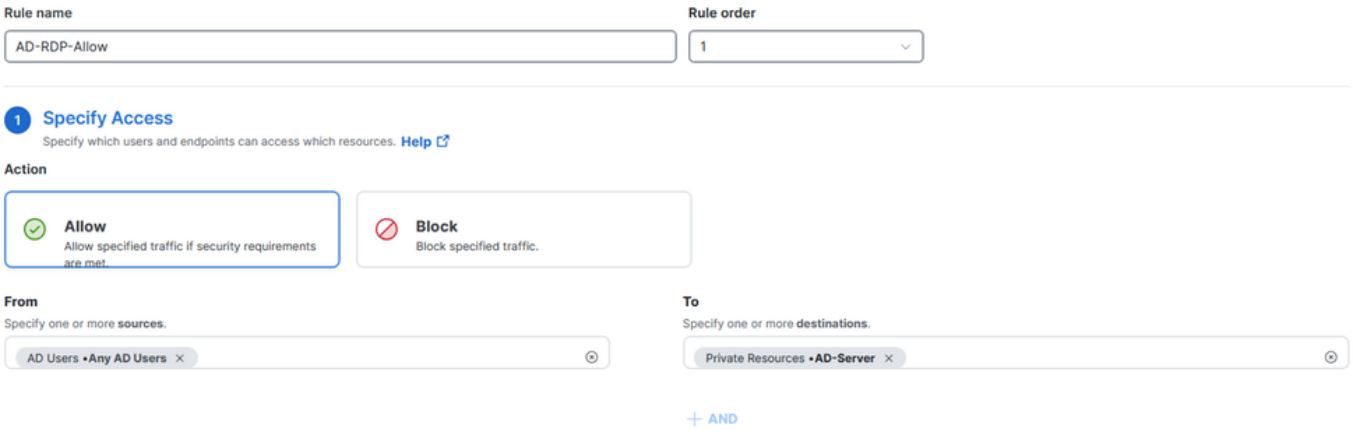
Acceso seguro - Configuración de la política de acceso

3. Agregar un nombre de regla



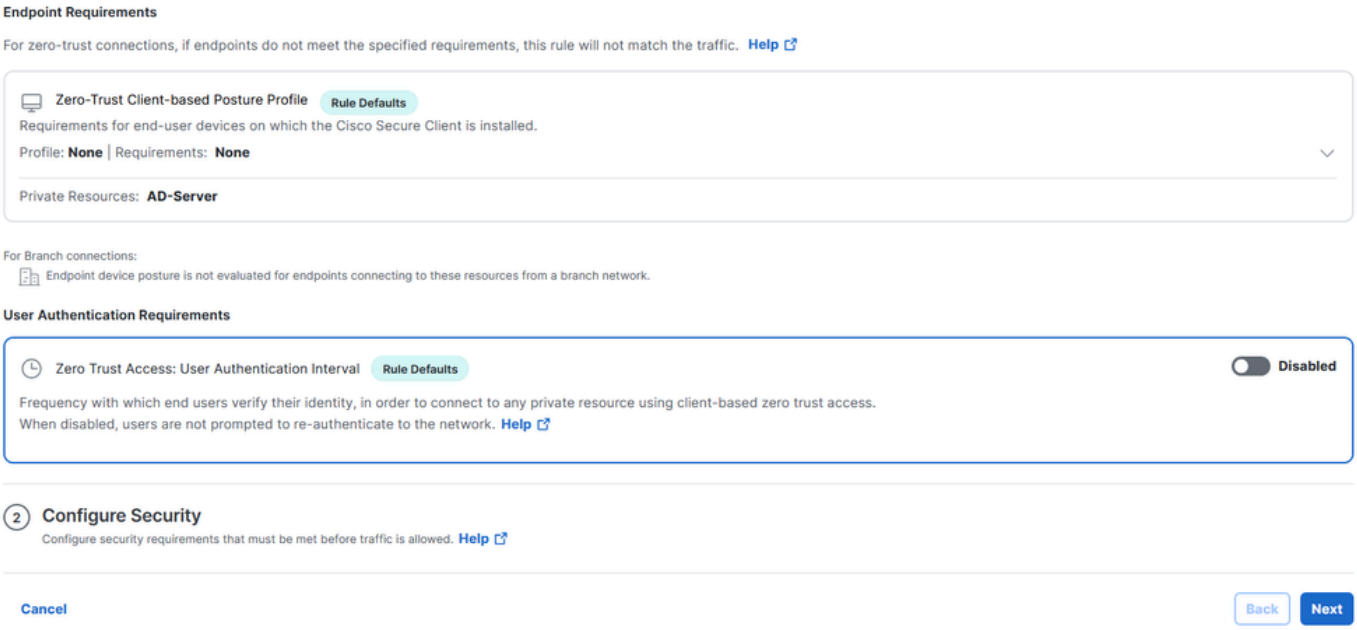
Acceso seguro - Configuración de la política de acceso

4. Seleccione la acción de regla y seleccione origen y destino



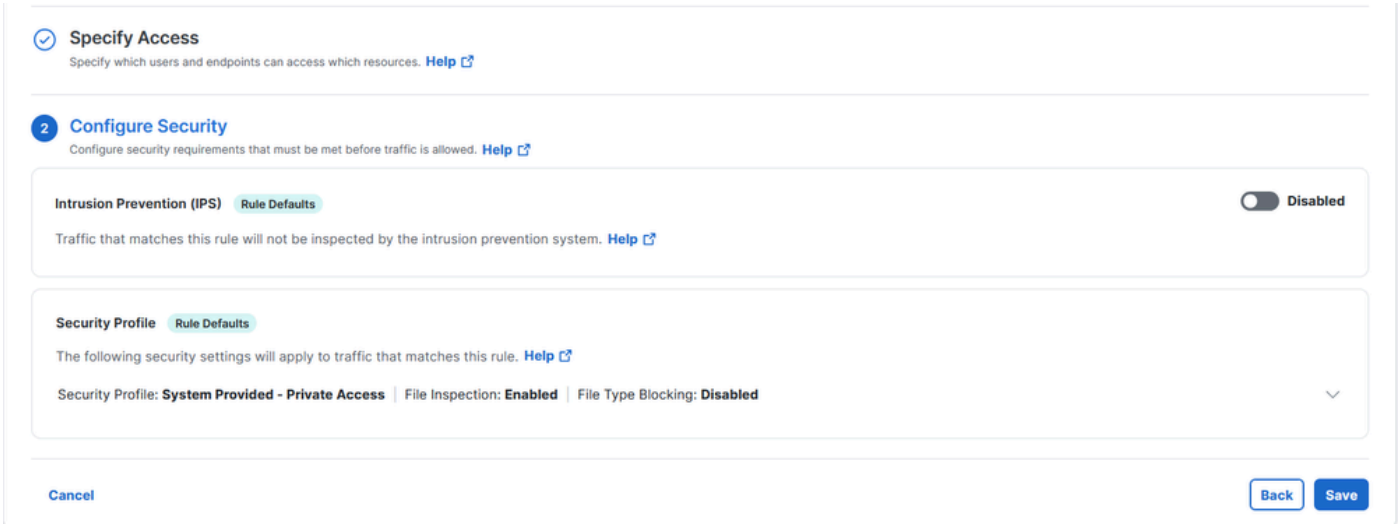
Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales



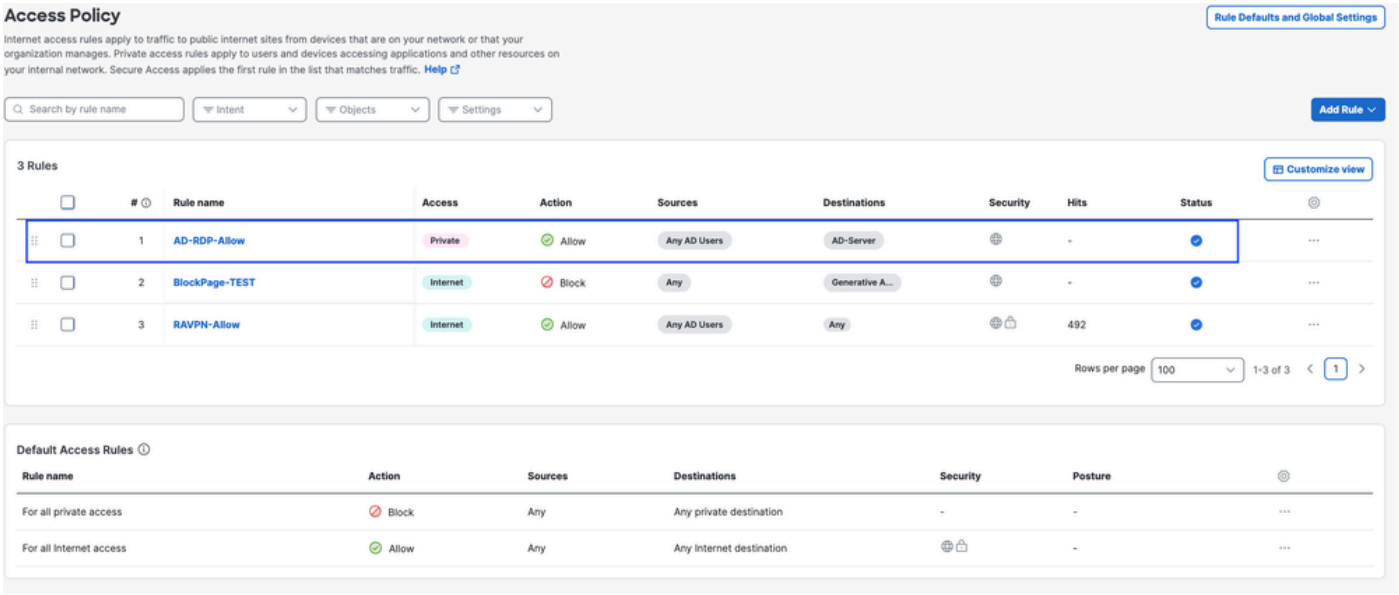
Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad



Acceso seguro - Configuración de la política de acceso

7. Haga clic en Guardar

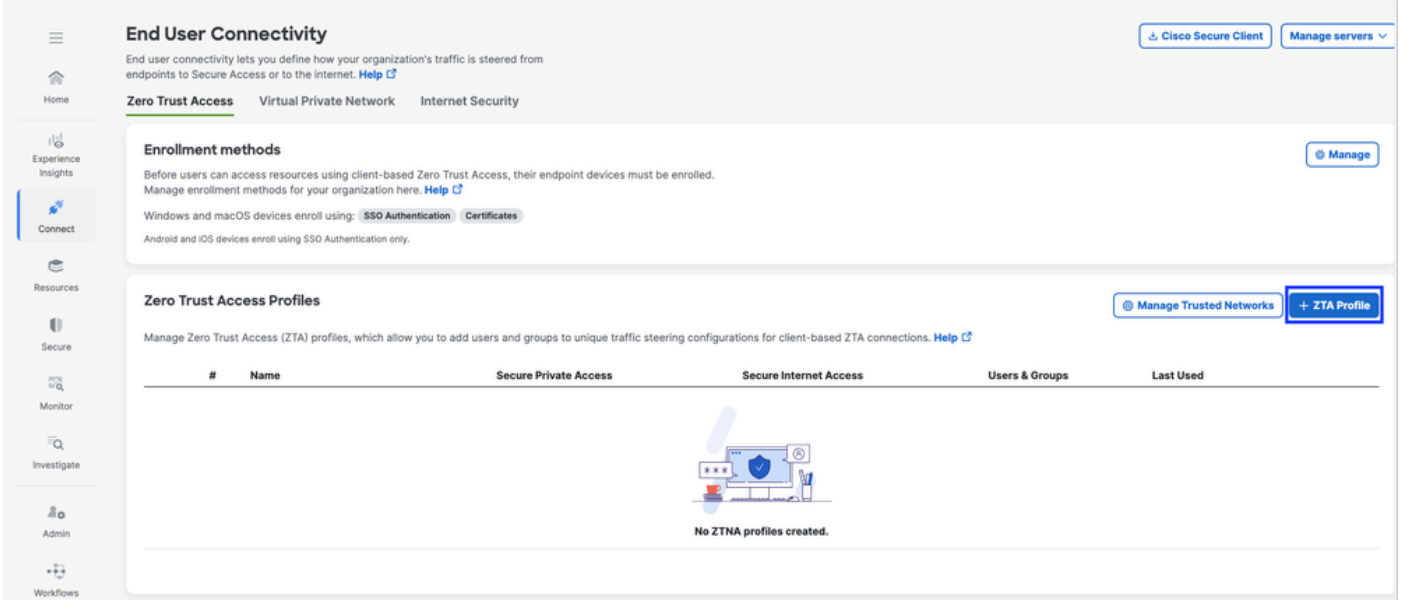


Acceso seguro - Configuración de la política de acceso

Paso - 3 Agregar un recurso privado al perfil ZTA

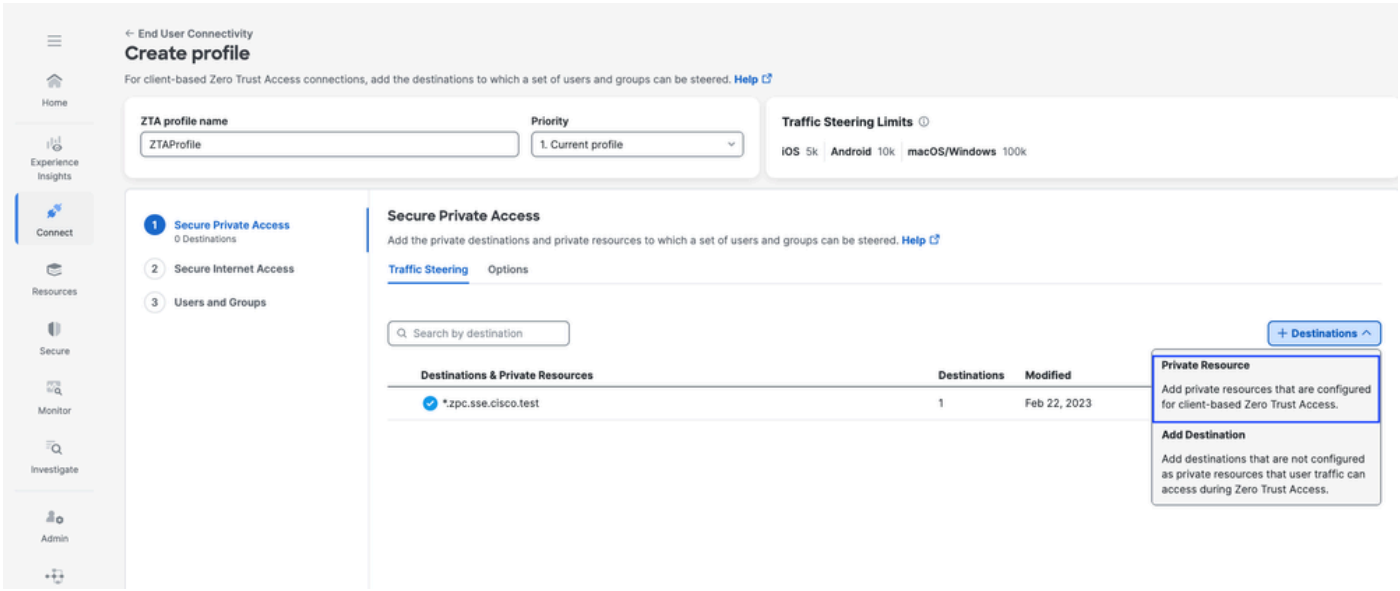
Si está utilizando un perfil ZTA personalizado, debe agregar el recurso privado correspondiente al perfil ZTA

1. Navegue hasta Conexión > Conectividad del usuario final > Acceso de confianza cero y haga clic en +Perfil ZTA

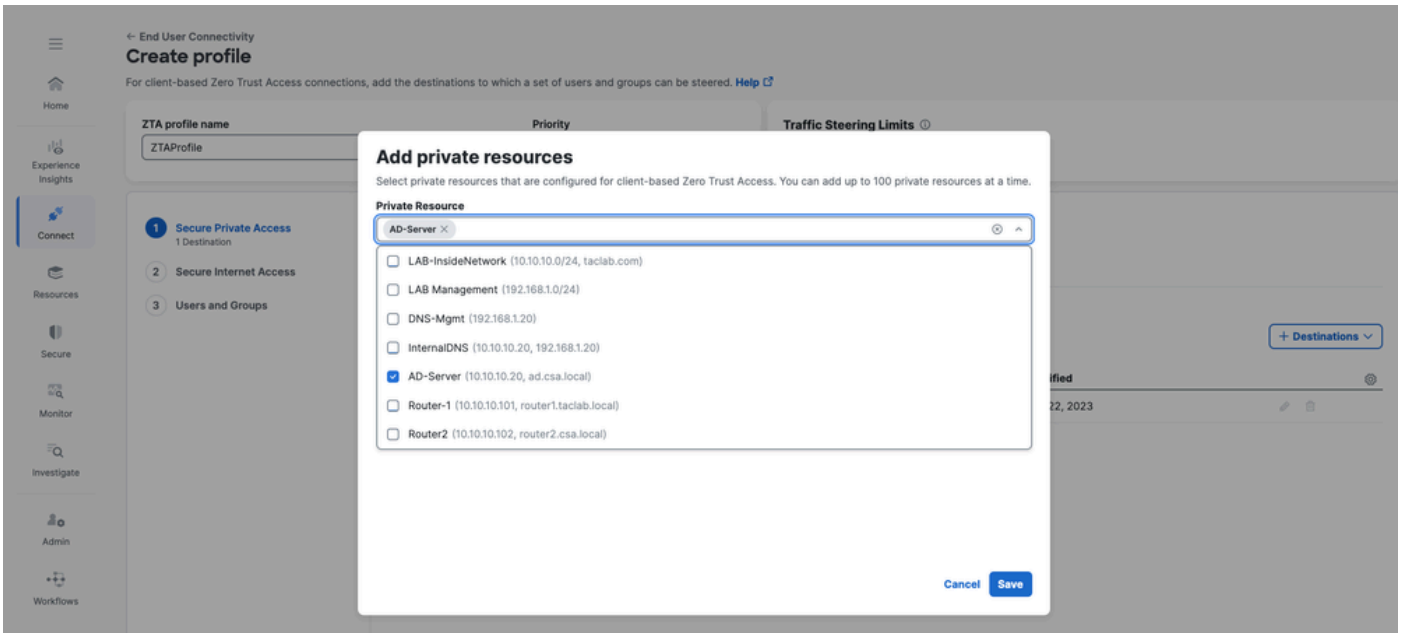


Acceso seguro - Perfil ZTA

2. Añada el recurso privado

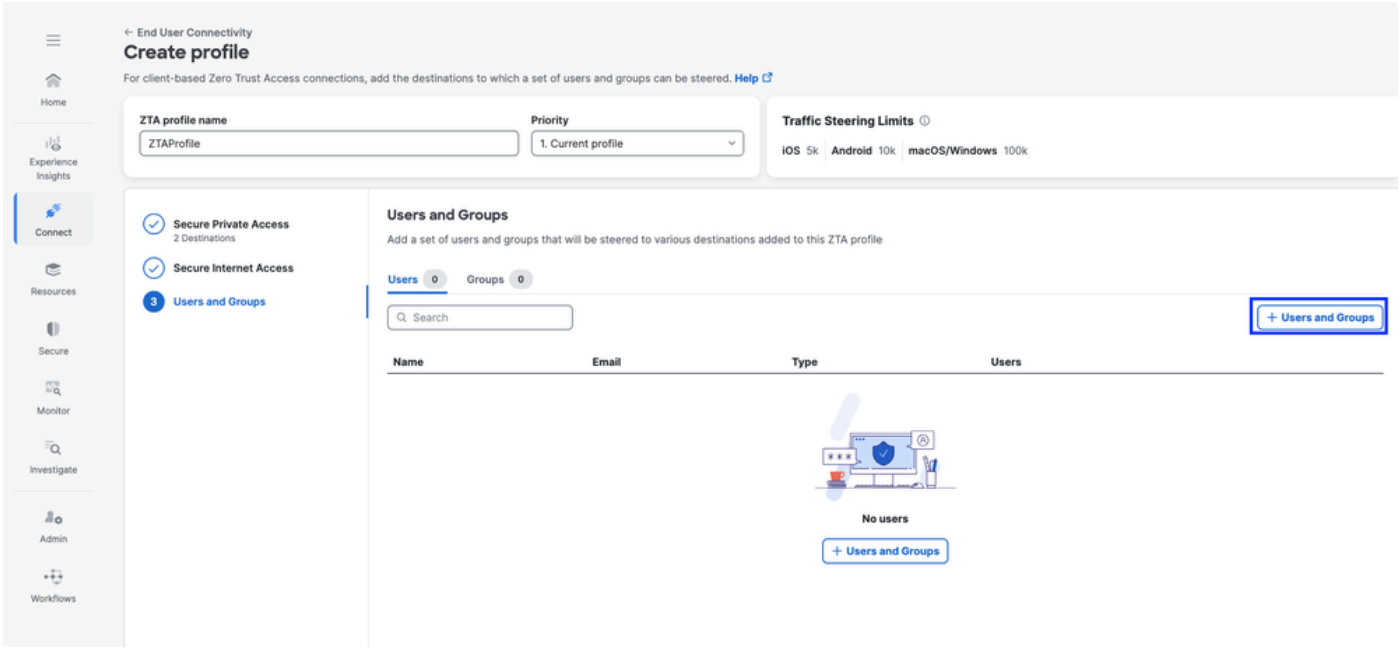


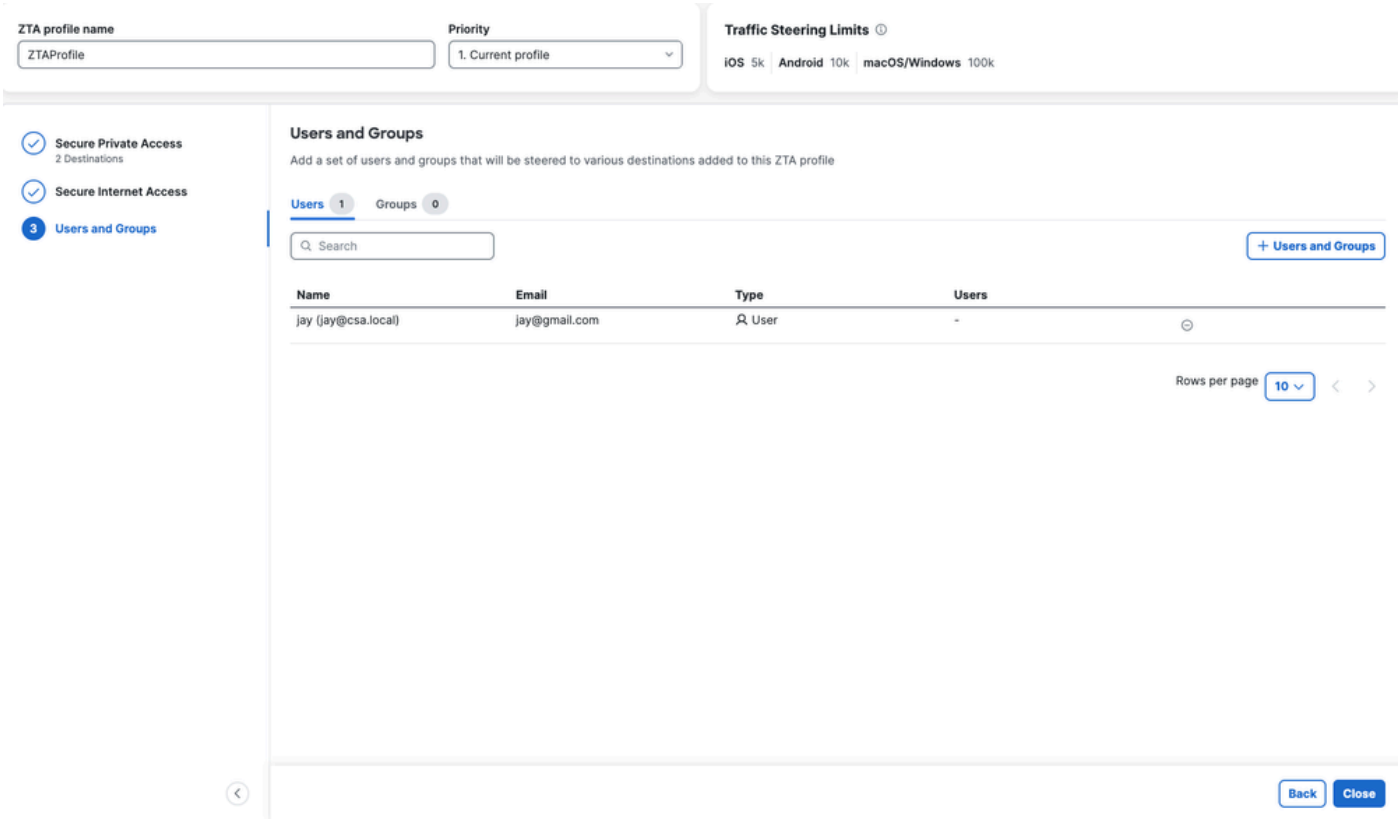
Acceso seguro - Perfil ZTA



Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos





Acceso seguro - Perfil ZTA

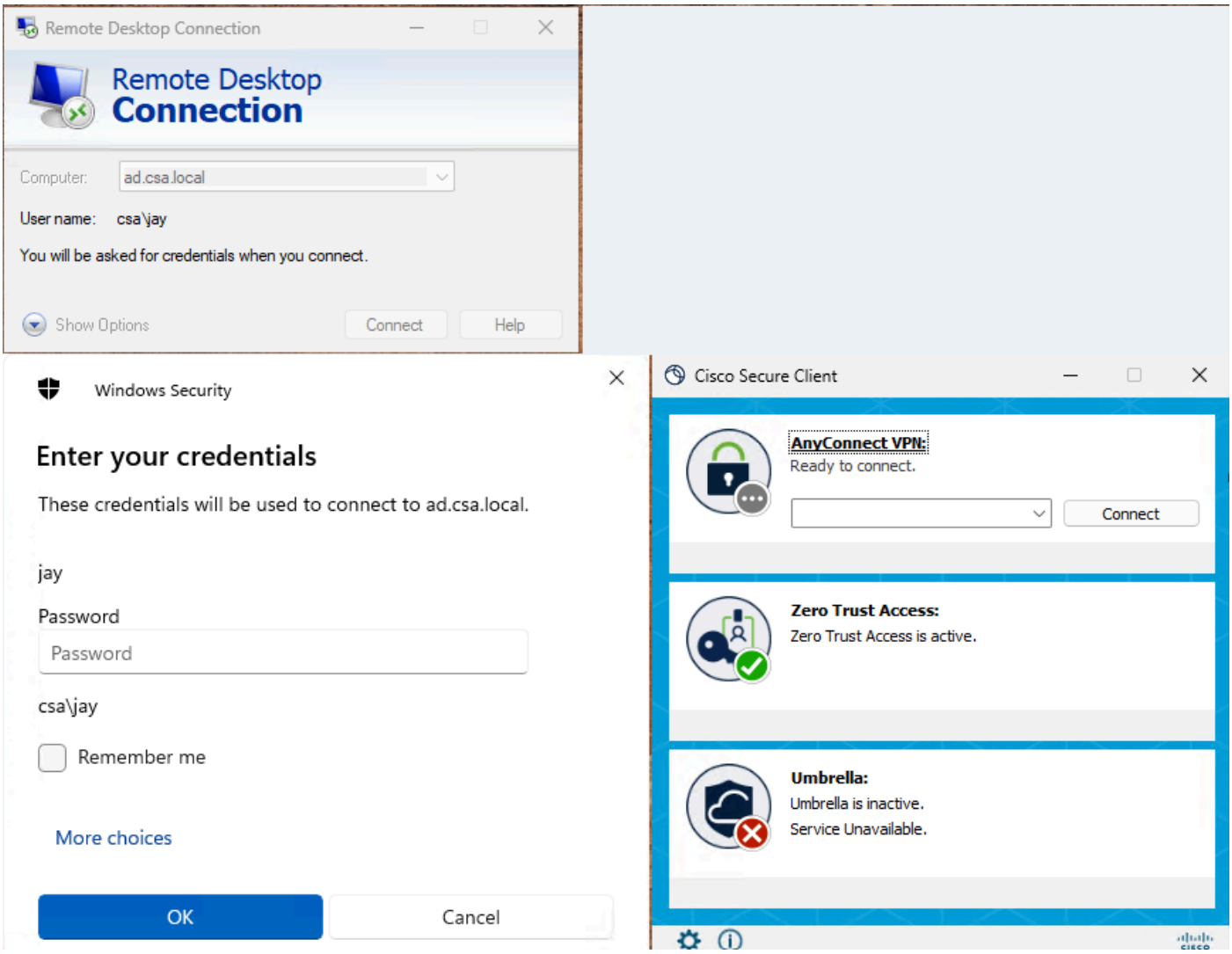
Nota: Puede tardar hasta 15-20 minutos en insertar y sincronizar la configuración con el cliente para el recurso privado asignado

---

Paso - 4 Verificar el acceso al recurso privado

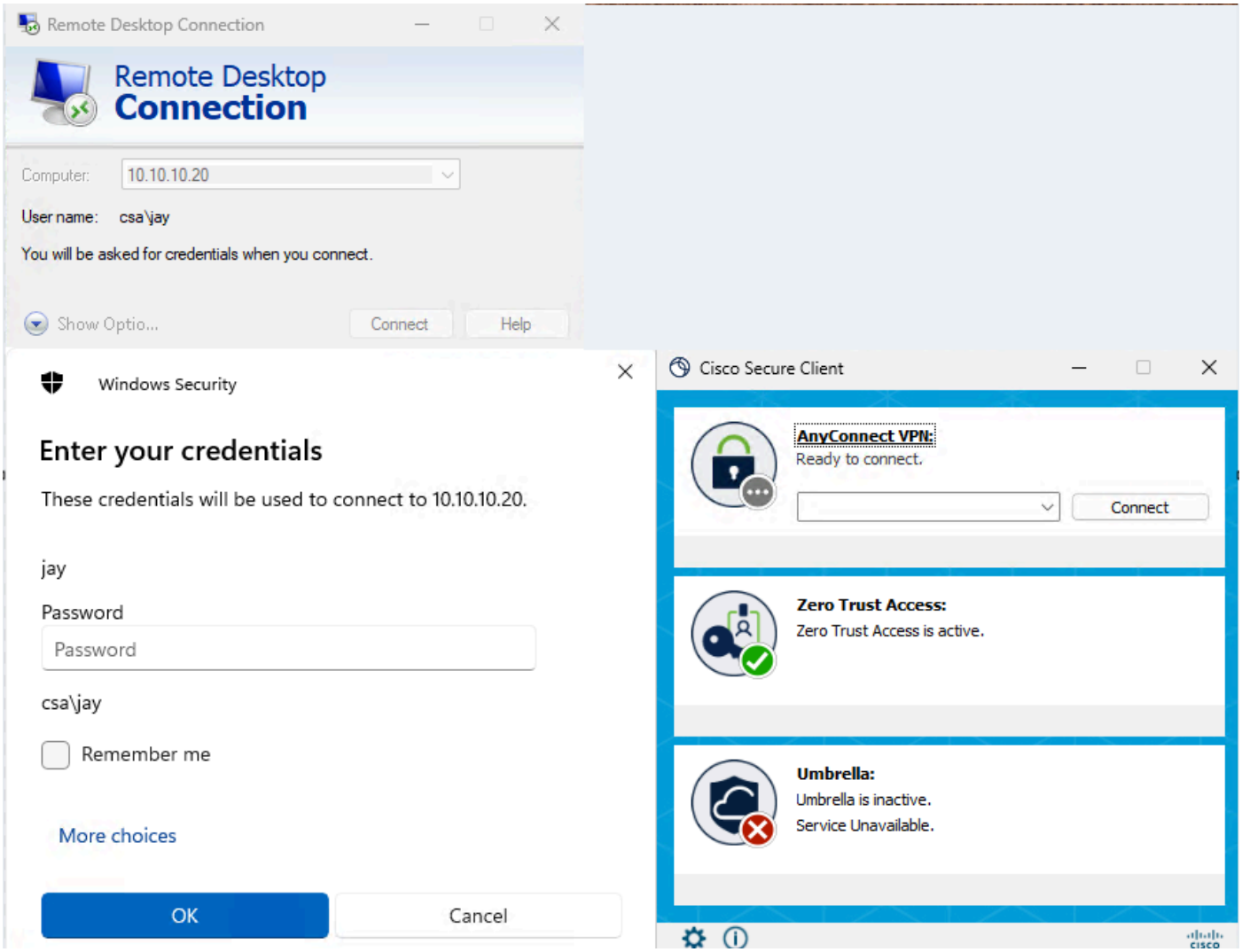
1. Acceso al recurso privado

Acceso al PR mediante FQDN



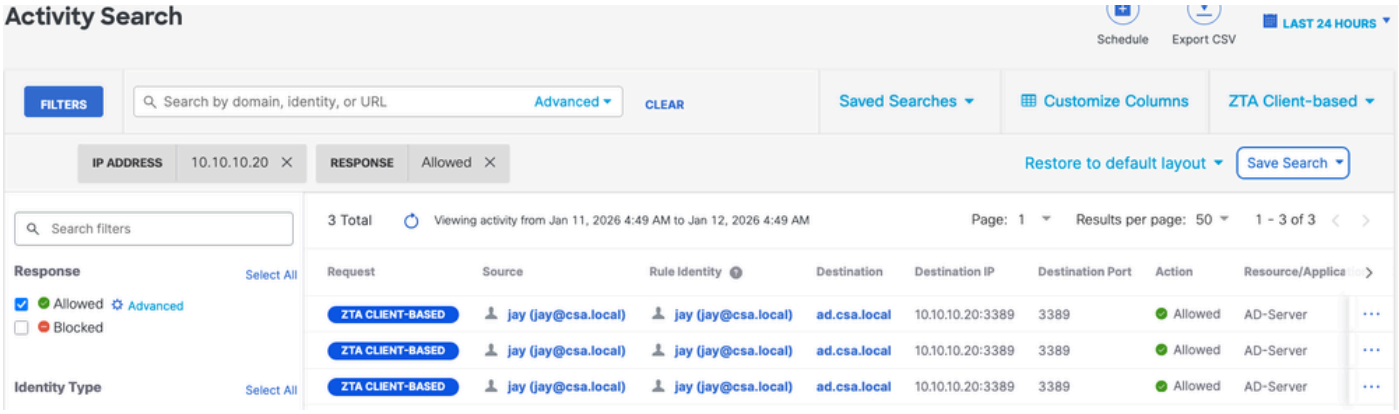
Secure Access - Prueba de relaciones públicas

Acceso al PR mediante la dirección IP

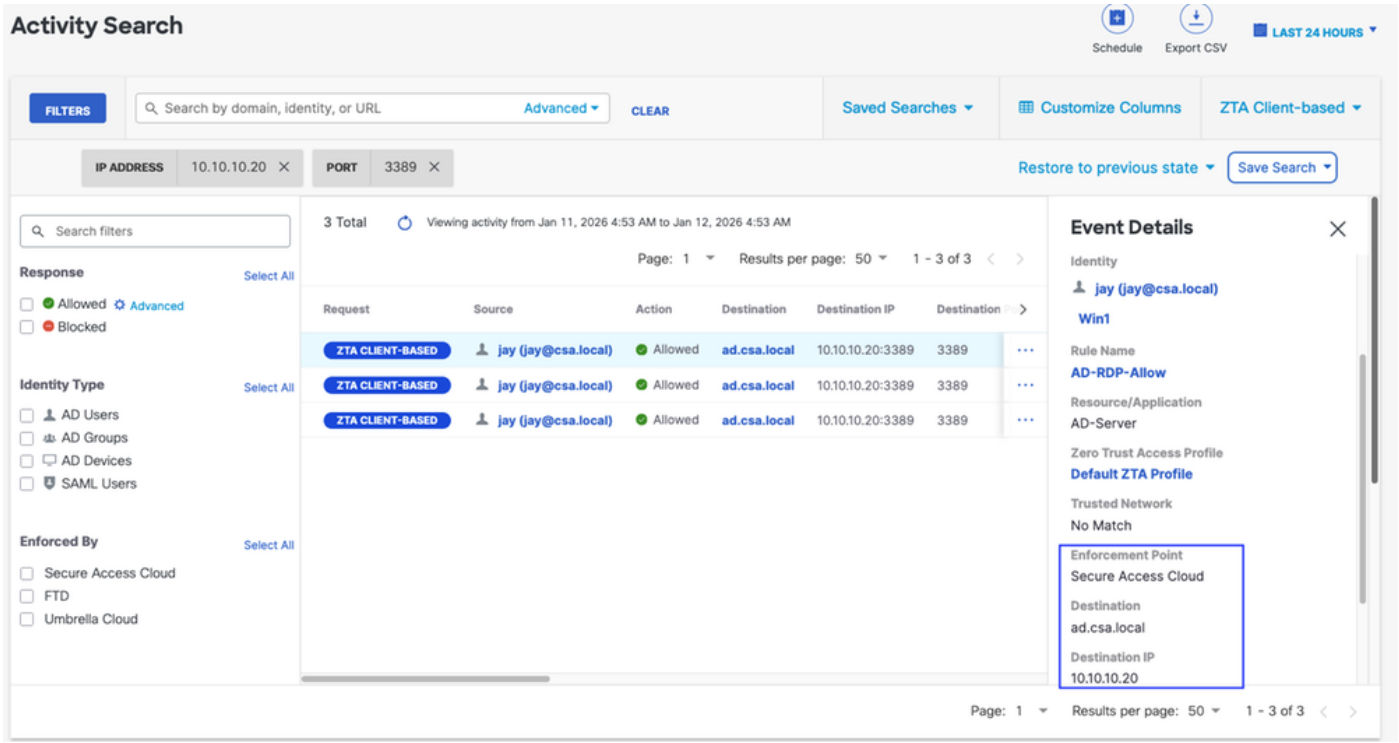


Secure Access - Prueba de relaciones públicas

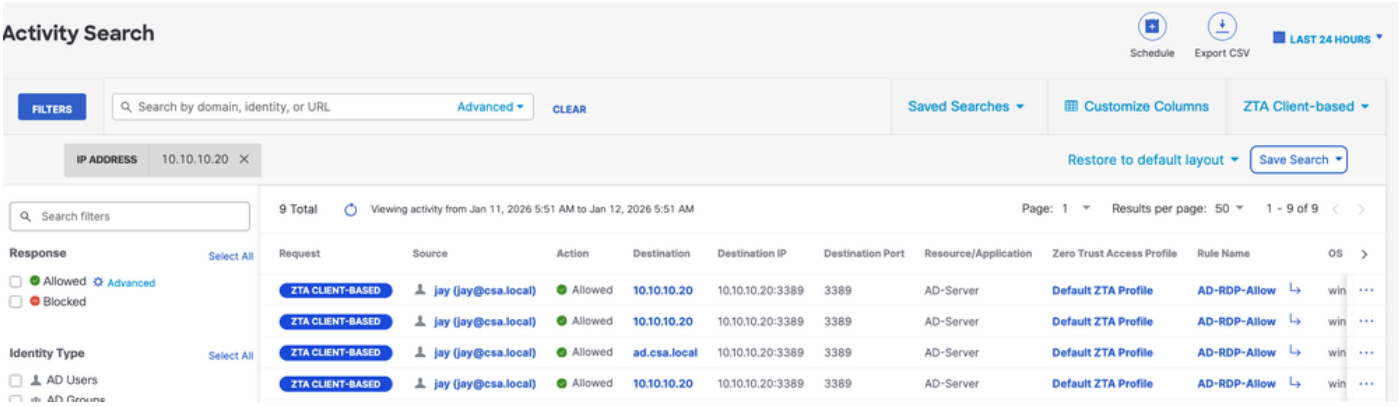
2. Verifíquelo con los eventos de búsqueda de actividad



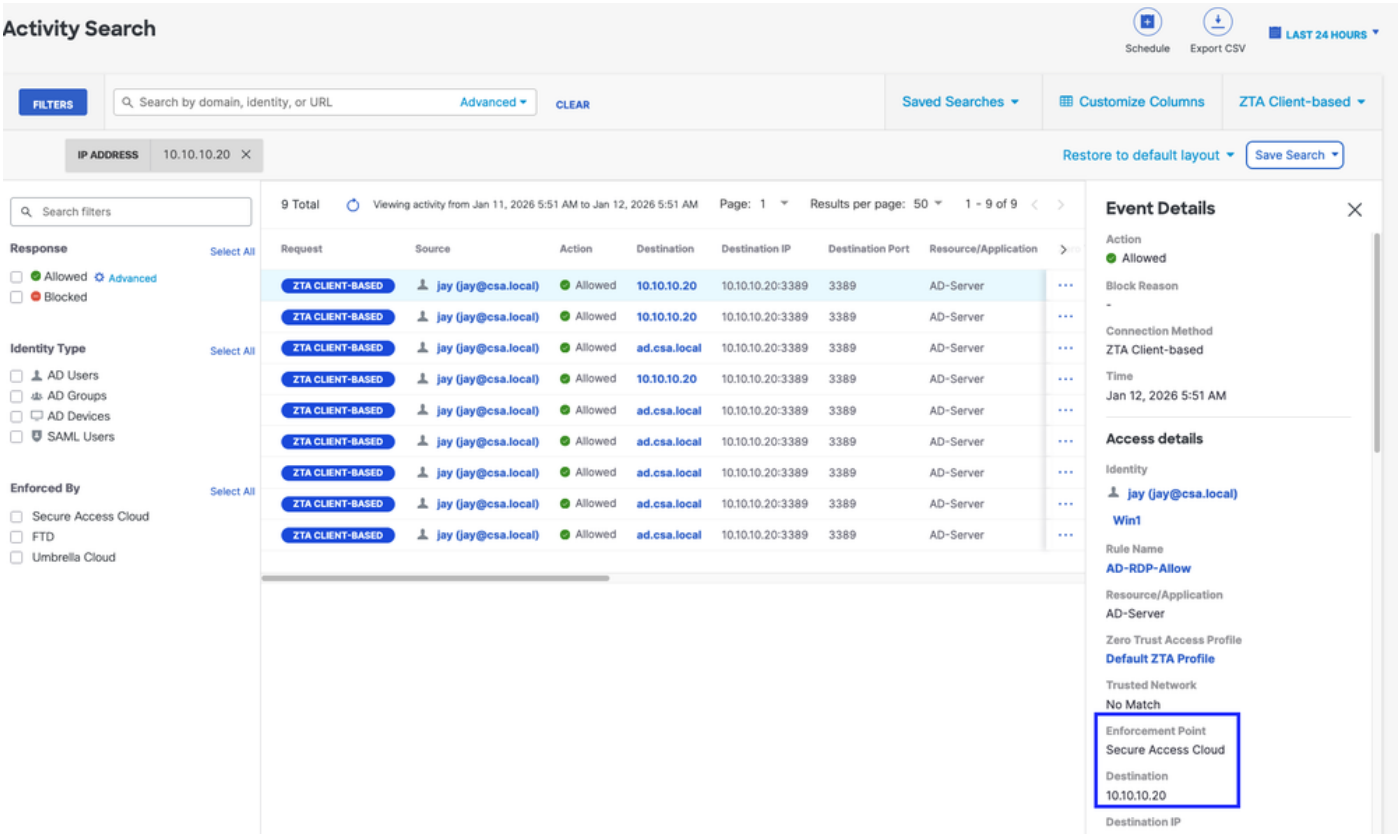
Acceso seguro - Búsqueda de actividad



Acceso seguro - Búsqueda de actividad

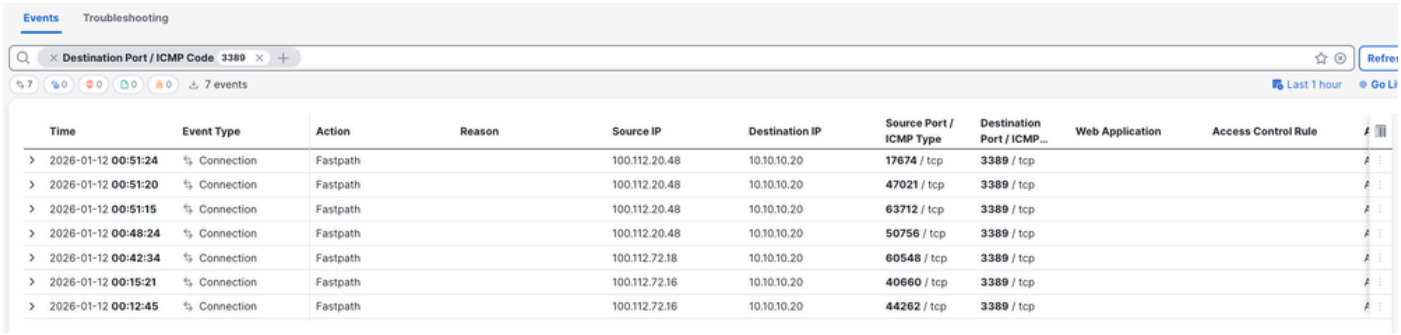


Acceso seguro - Búsqueda de actividad



Acceso seguro - Búsqueda de actividad

3. Verifique los eventos de conexión FMC

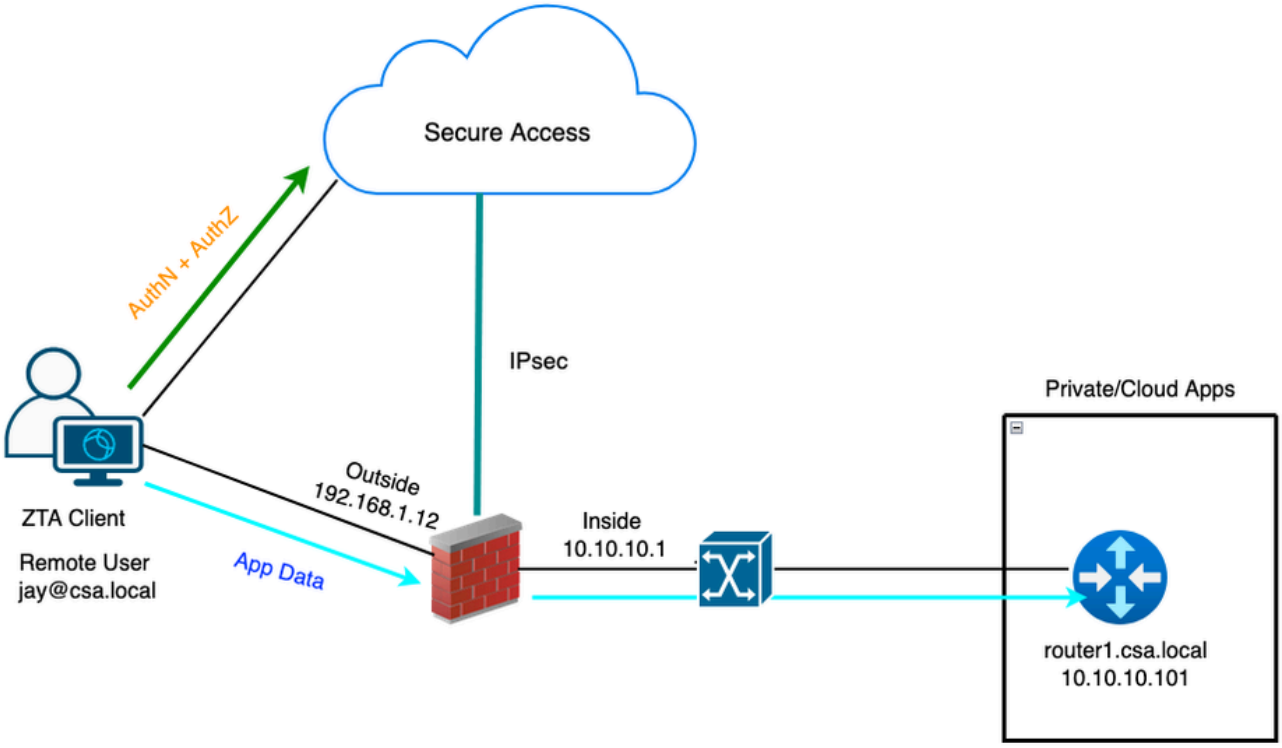


Eventos de conexión FMC

Caso de prueba 2: usuario remoto, aplicación local

El acceso a un recurso privado a través de la aplicación local , en este tipo de aplicación, la evaluación de la política tiene lugar en Secure Access pero los datos de la aplicación permanecen locales en FTD. Por ejemplo , un cliente o usuario registrado de ZTA conectado a la red doméstica e intentando acceder a un recurso privado que está detrás de la interfaz interna de

FTD .

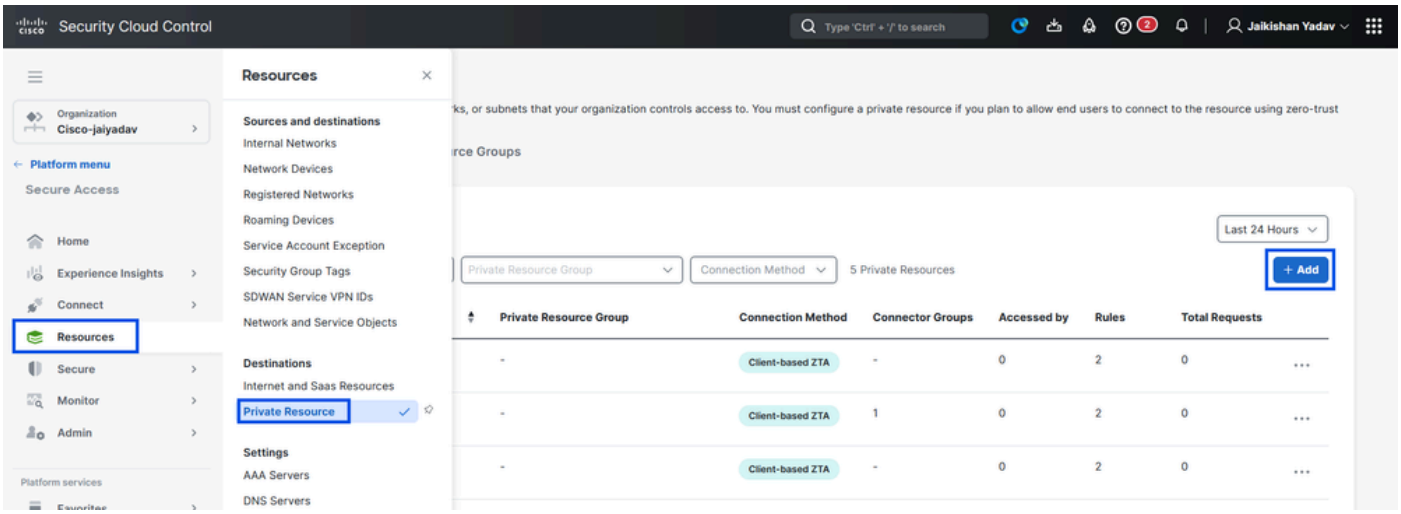


ZTA universal: topología de caso de prueba

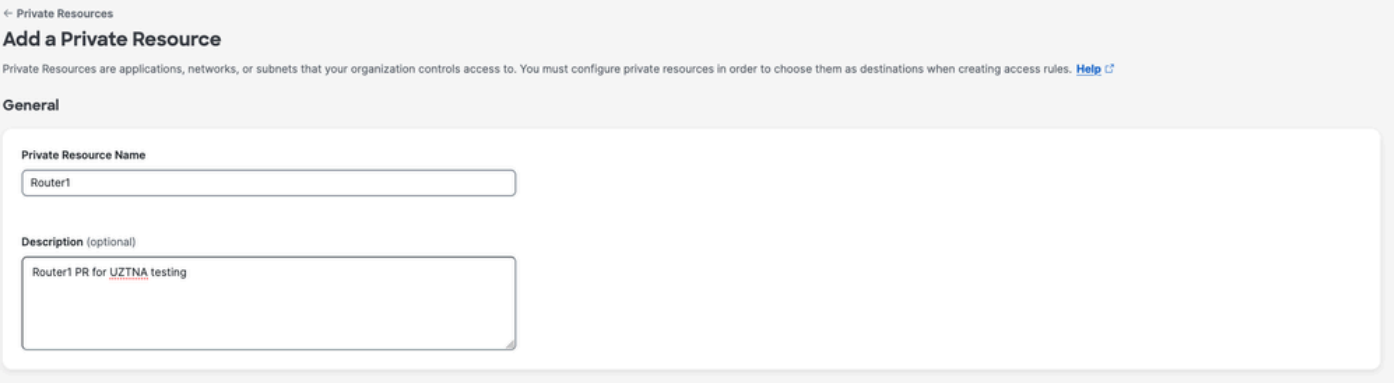
Paso 1 - Definir un recurso privado en Secure Access

Configure un recurso privado al que se pueda acceder a través del dispositivo inscrito de acceso de confianza cero (ZTA) con aplicación en la nube

1. Navegue hasta Recursos > Destinos > Recursos privados > Haga clic en +Agregar

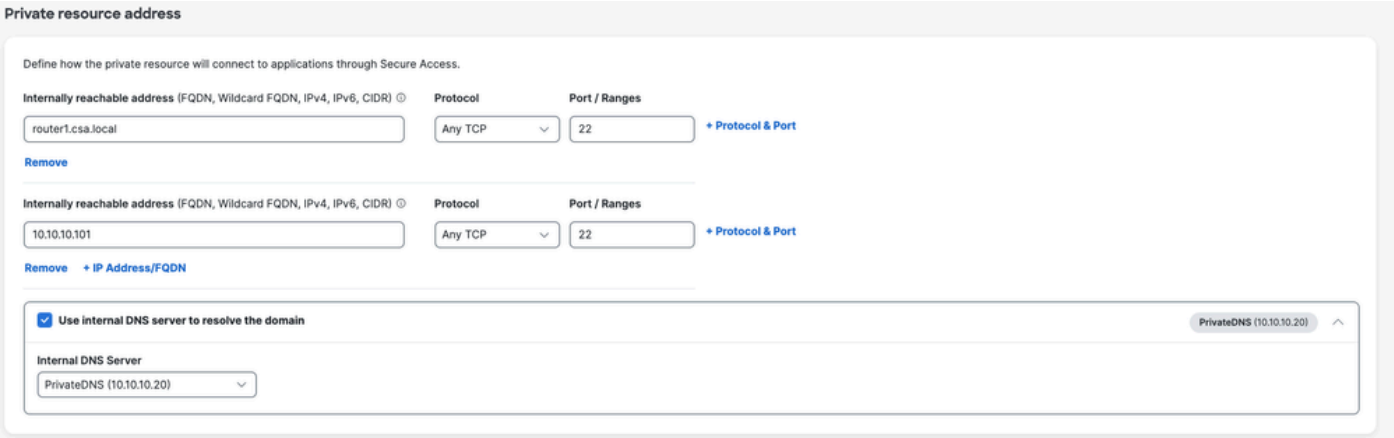


2. En Nombre de Recurso Privado, introduzca un nombre significativo para el recurso. Para Descripción, se recomienda proporcionar información como el propósito del recurso o el nombre del propietario del recurso.



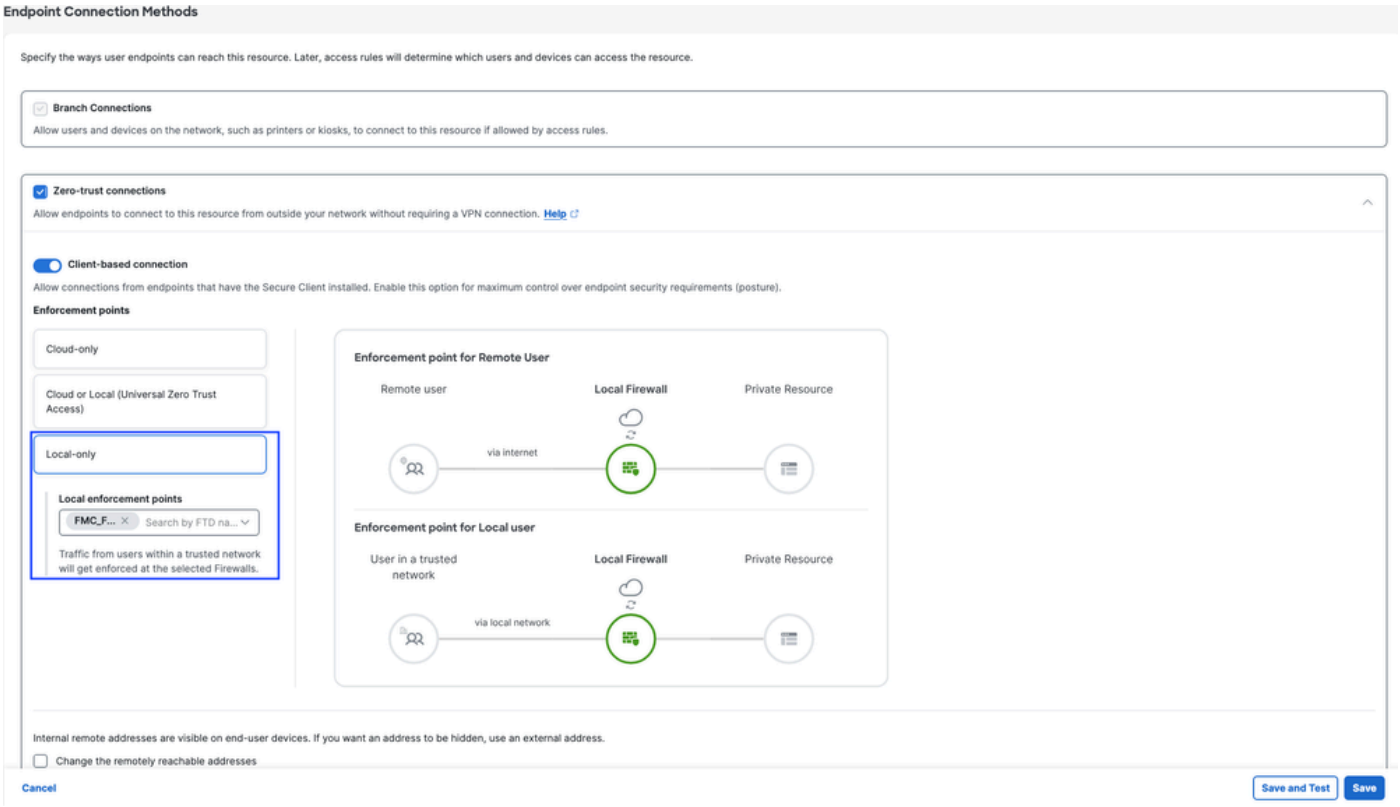
3. Introduzca el FQDN del recurso privado al que desea acceder . También podemos definir la dirección IP del recurso privado . Para obtener más información, vea Agregar un recurso privado

4. Seleccione el servidor DNS interno para resolver el dominio



5. Seleccionar métodos de conexión de terminales

6. Seleccione FTD como puntos de aplicación locales



Acceso seguro - Configuración de recursos privados

Nota: En función del tipo de inscripción que seleccione, este cambio asociará automáticamente el PR al FTD y activará una implementación de políticas

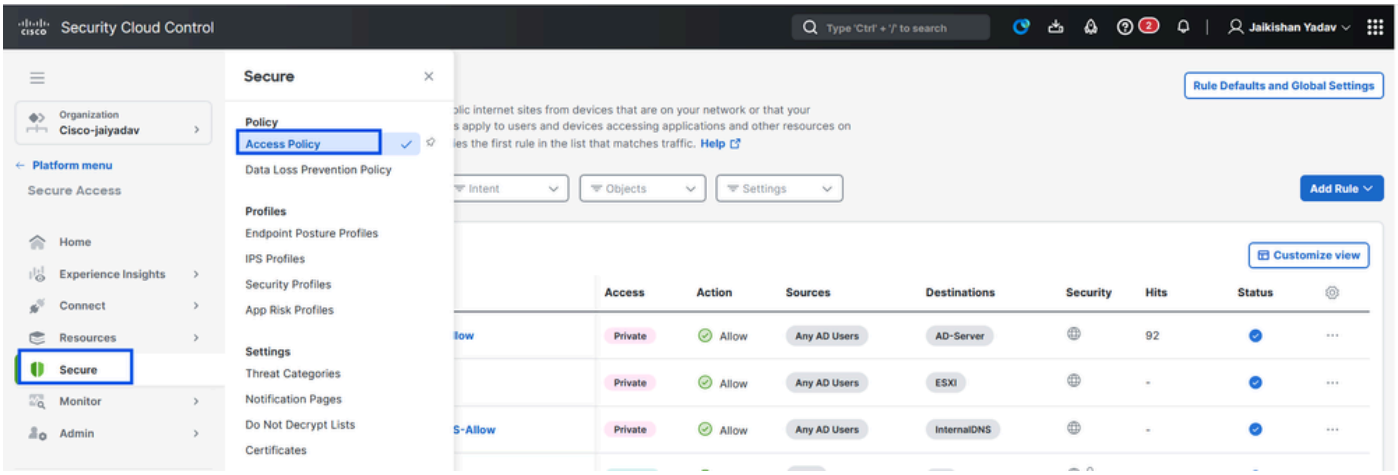
---

7. Haga clic en Save (Guardar).

Paso 2: Crear regla de acceso privado

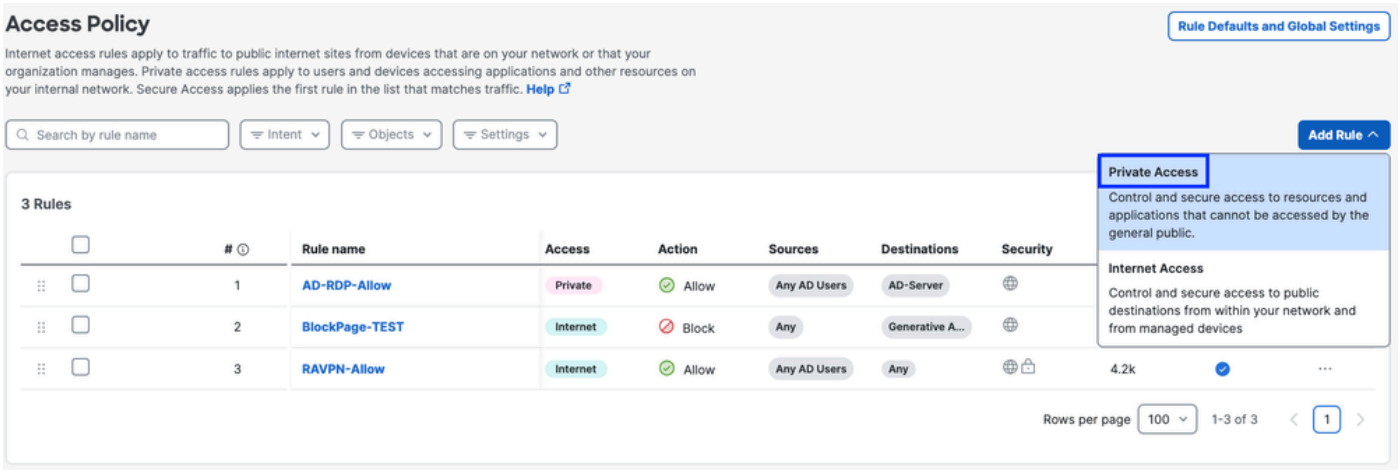
Configure un acceso privado en Secure Access para que los usuarios inscritos en Universal ZTA puedan acceder . Para obtener más información, vea Regla de acceso privado

1. Vaya a Seguro > Política de acceso



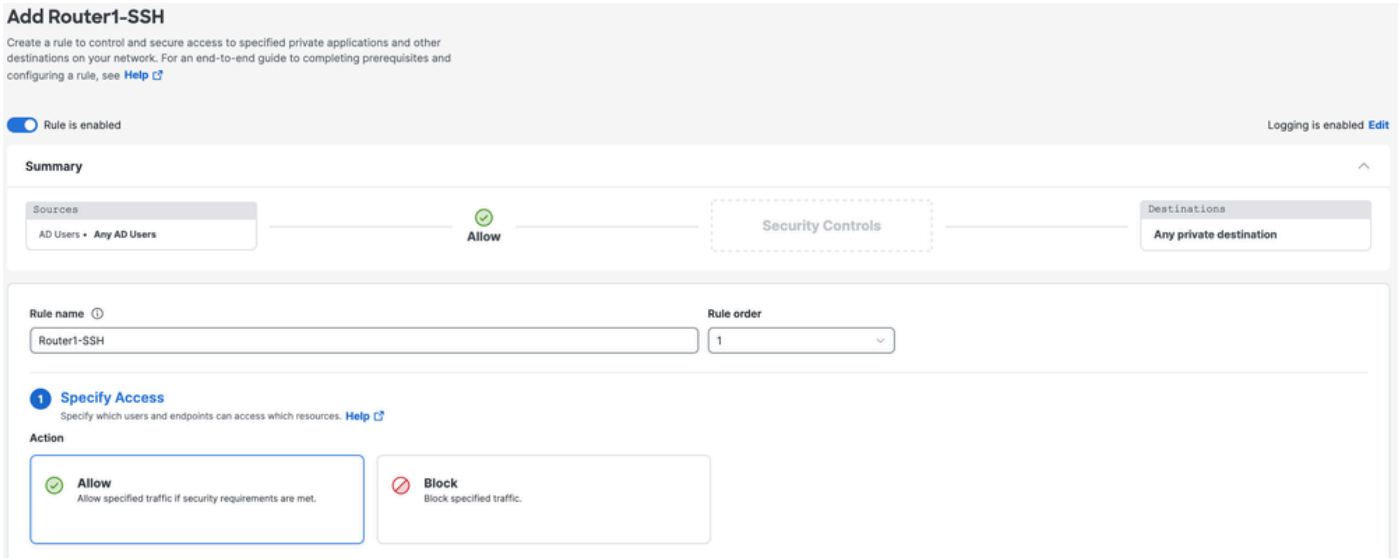
Acceso seguro - Configuración de recursos privados

2. Haga clic en Agregar regla, y luego elija Acceso privado.
   En la parte superior de la regla hay un resumen que describe los componentes configurados de la regla.



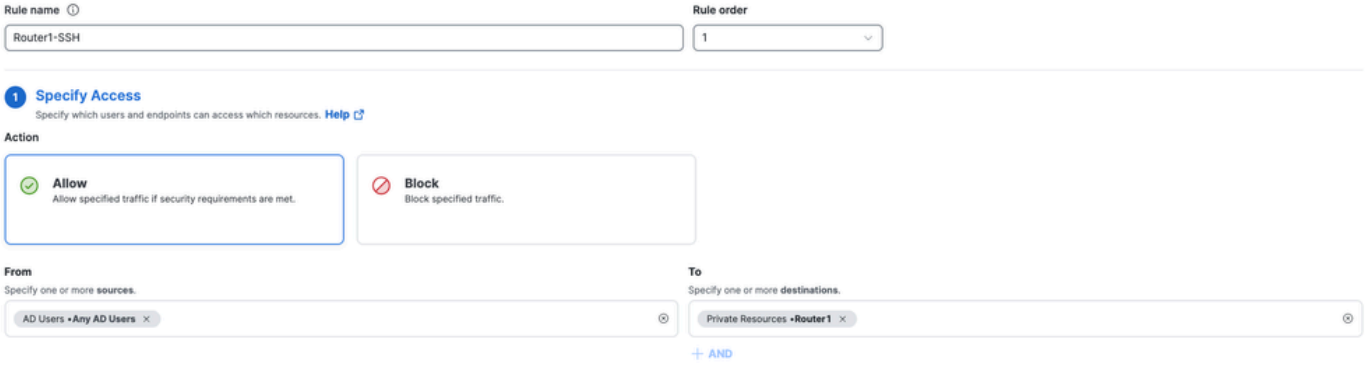
Acceso seguro - Configuración de la política de acceso

3. Agregar un nombre de regla



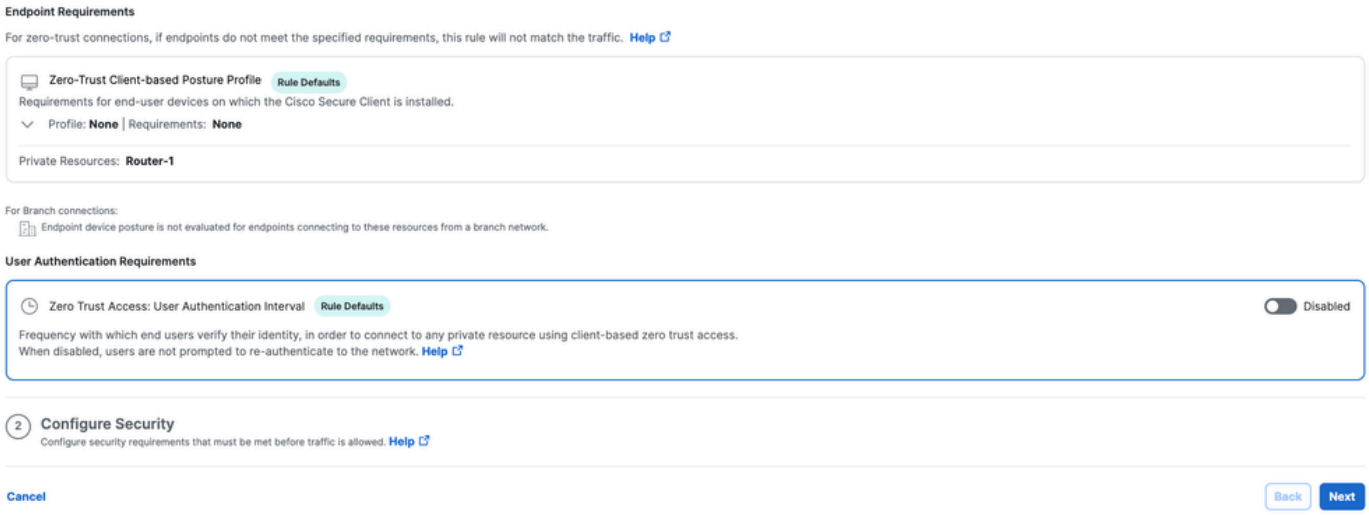
Acceso seguro - Configuración de la política de acceso

4. Seleccione la acción de regla y seleccione origen y destino



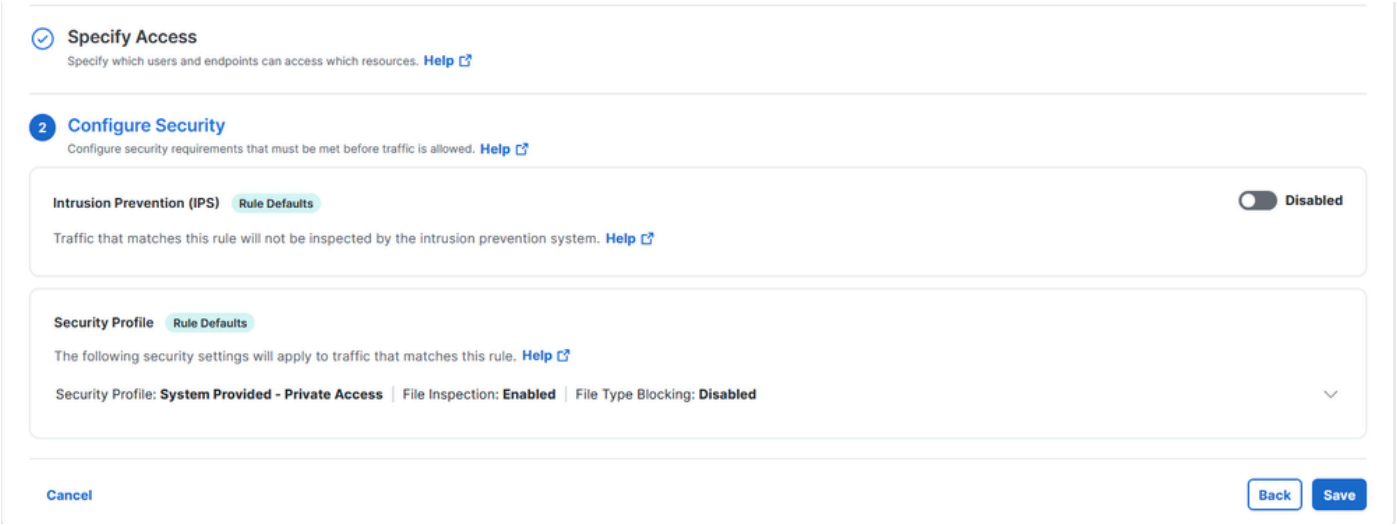
Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales



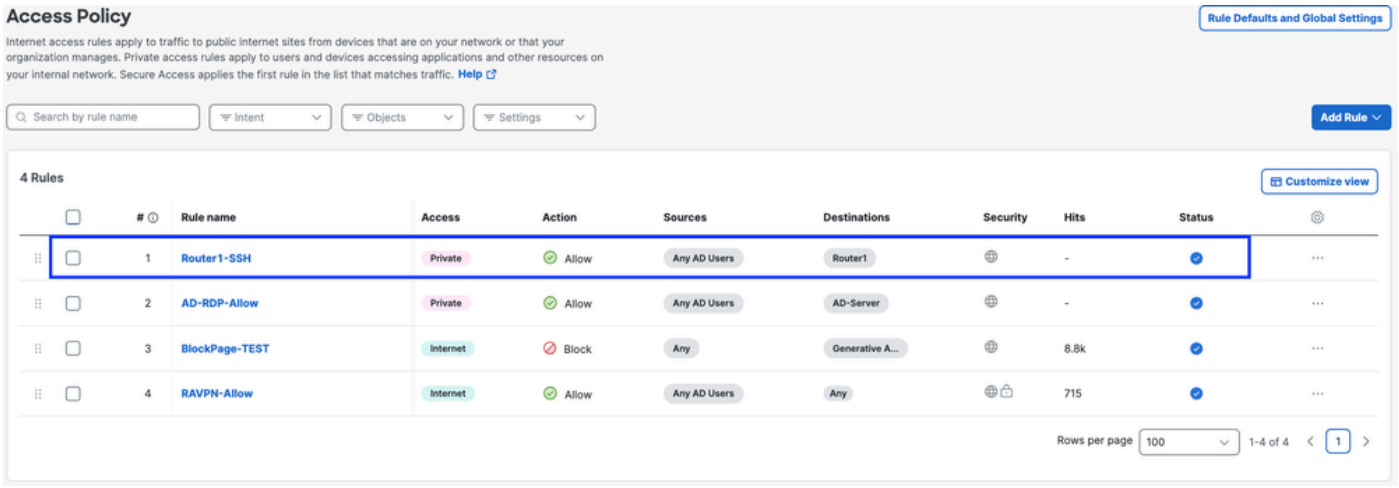
Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad



Acceso seguro - Configuración de la política de acceso

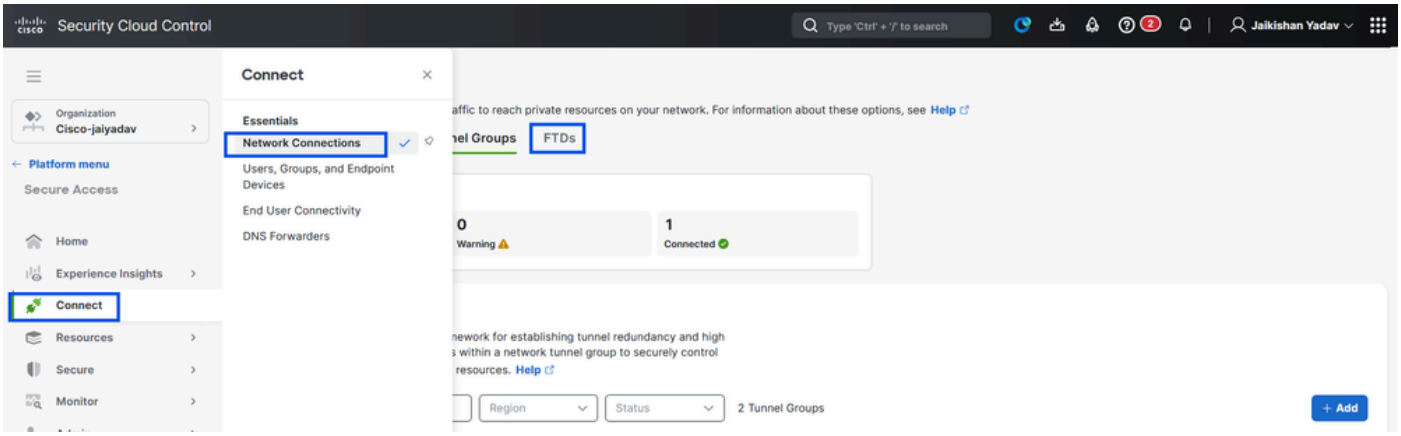
7. Haga clic en Guardar



Acceso seguro - Configuración de la política de acceso

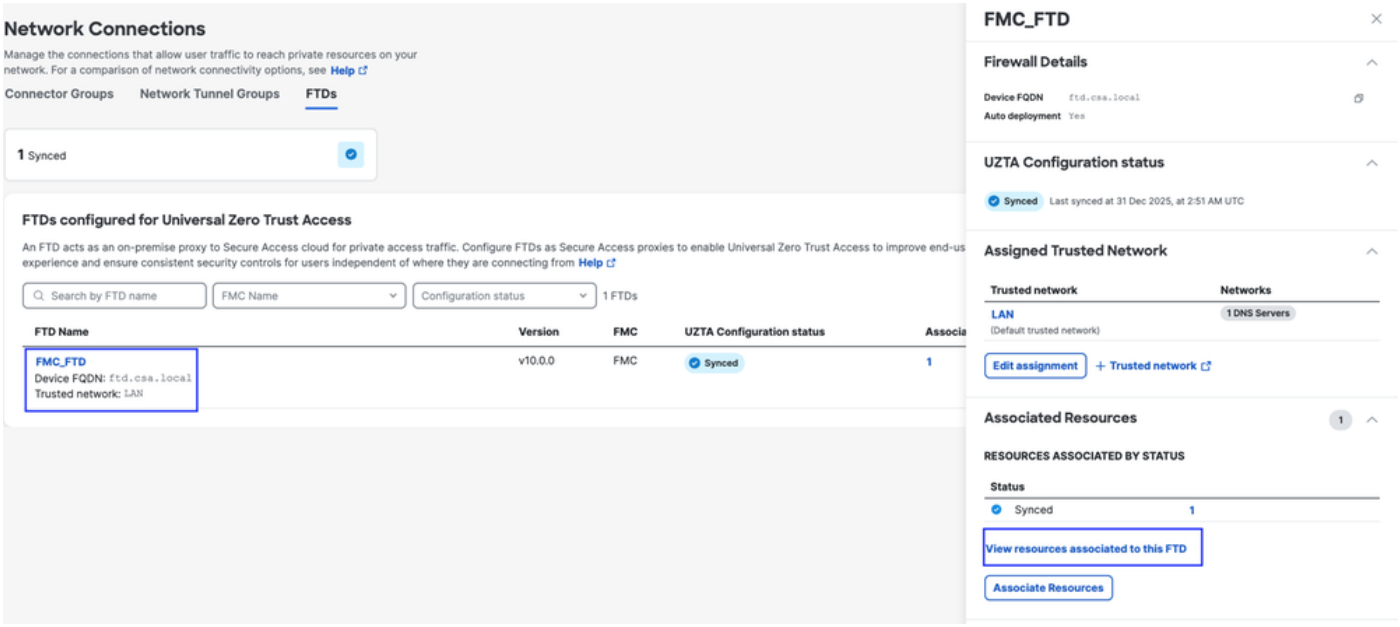
Paso 3 - Verificar la asociación de RP en el FTD

1. Vaya a Conexión > Conexiones de red > FTD

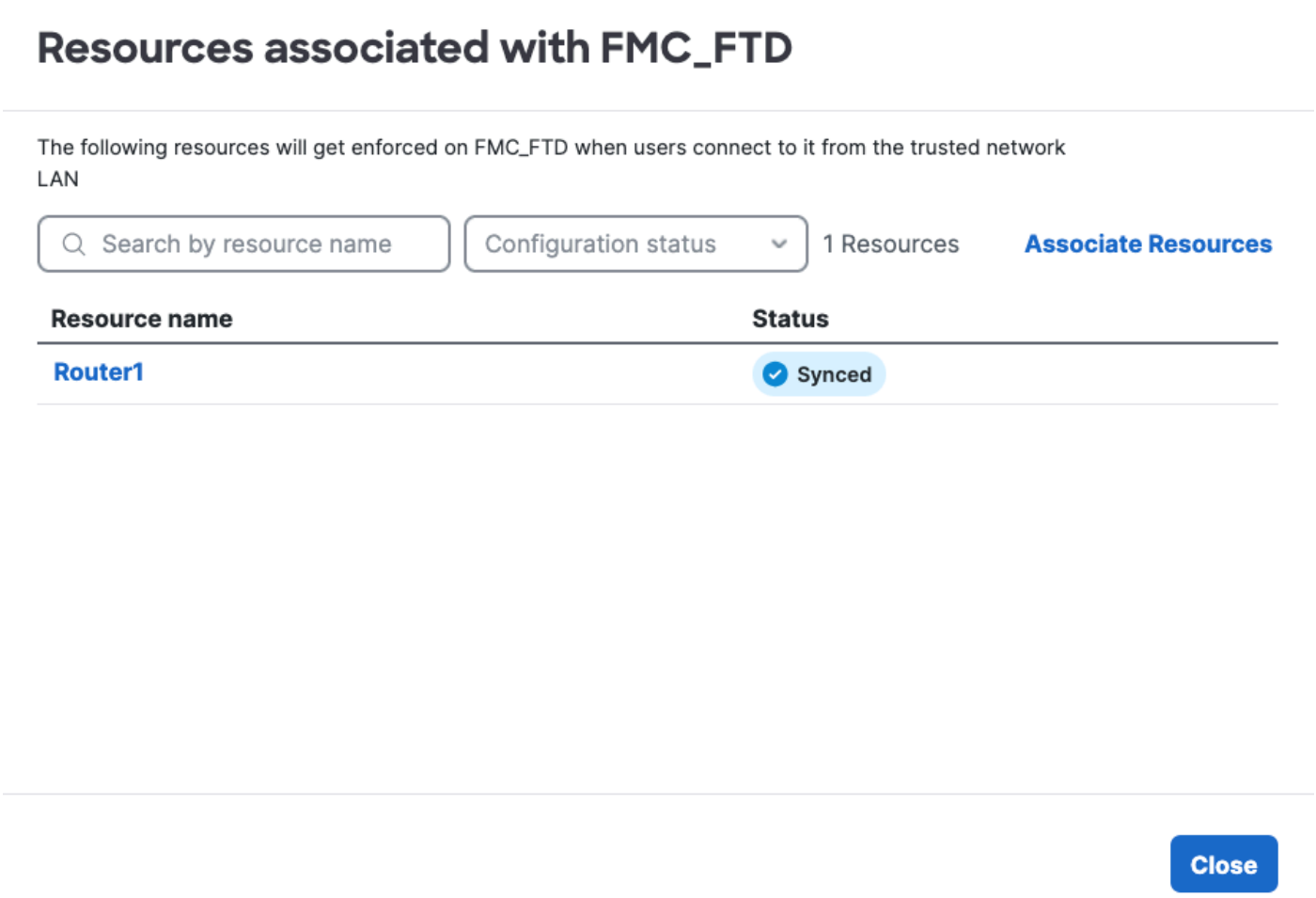


Acceso seguro - Verificación de relaciones públicas

2. Haga clic en FTD > Ver recursos asociados a este FTD



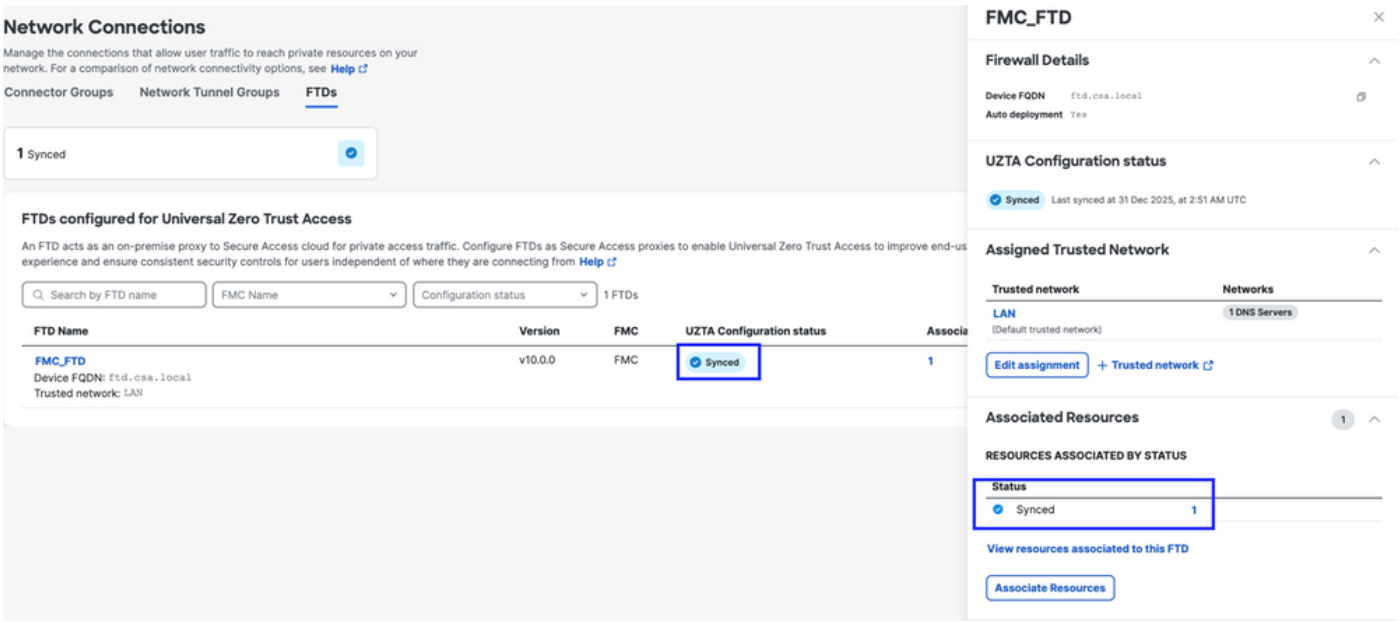
Acceso seguro - Verificación de relaciones públicas



Acceso seguro - Verificación de relaciones públicas

3. Haga clic en Close (Cerrar)

4. Verifique el estado , el recurso asociado y la configuración deben estar en el estado Sincronizado



Acceso seguro - Verificación de relaciones públicas

5. Compruebe que la configuración se ha enviado al FTD

Inicie sesión en FTD cli y navegue hasta el modo LINA

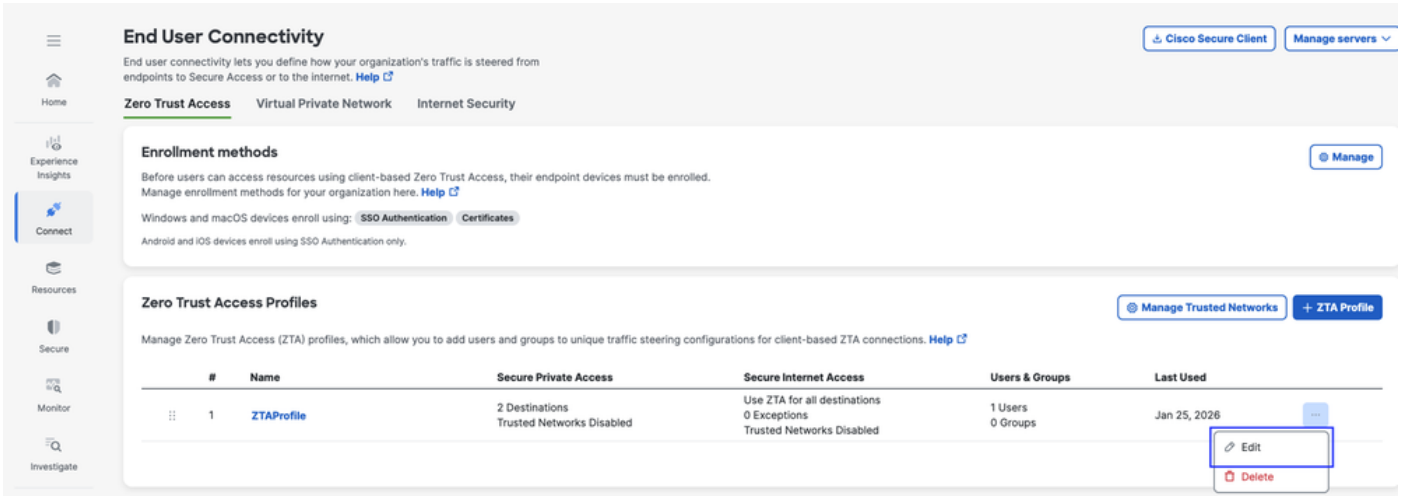
show running-config object application

```
> 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 - Verificación PR

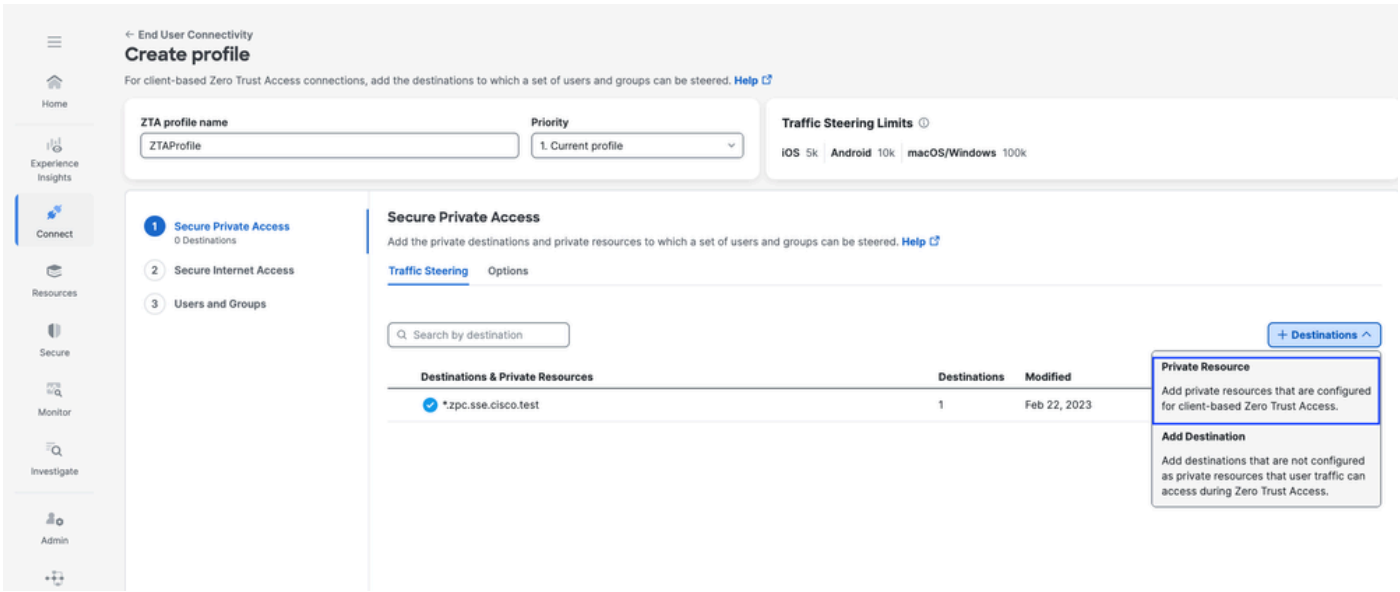
Paso 4: Agregar un recurso privado al perfil ZTA

1. Navegue hasta Conexión > Conectividad del usuario final > Acceso de confianza cero y haga clic en 3 puntos para editar el perfil ZTA

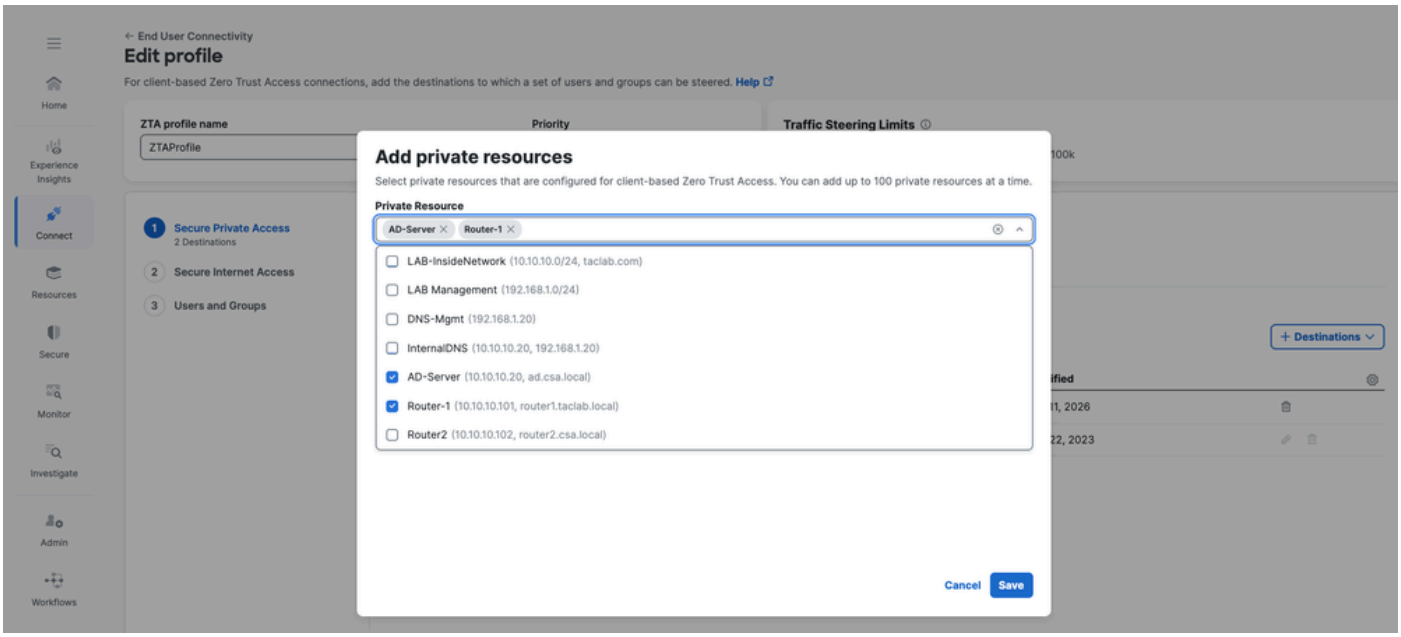


Acceso seguro - Perfil ZTA

2. Añada el recurso privado

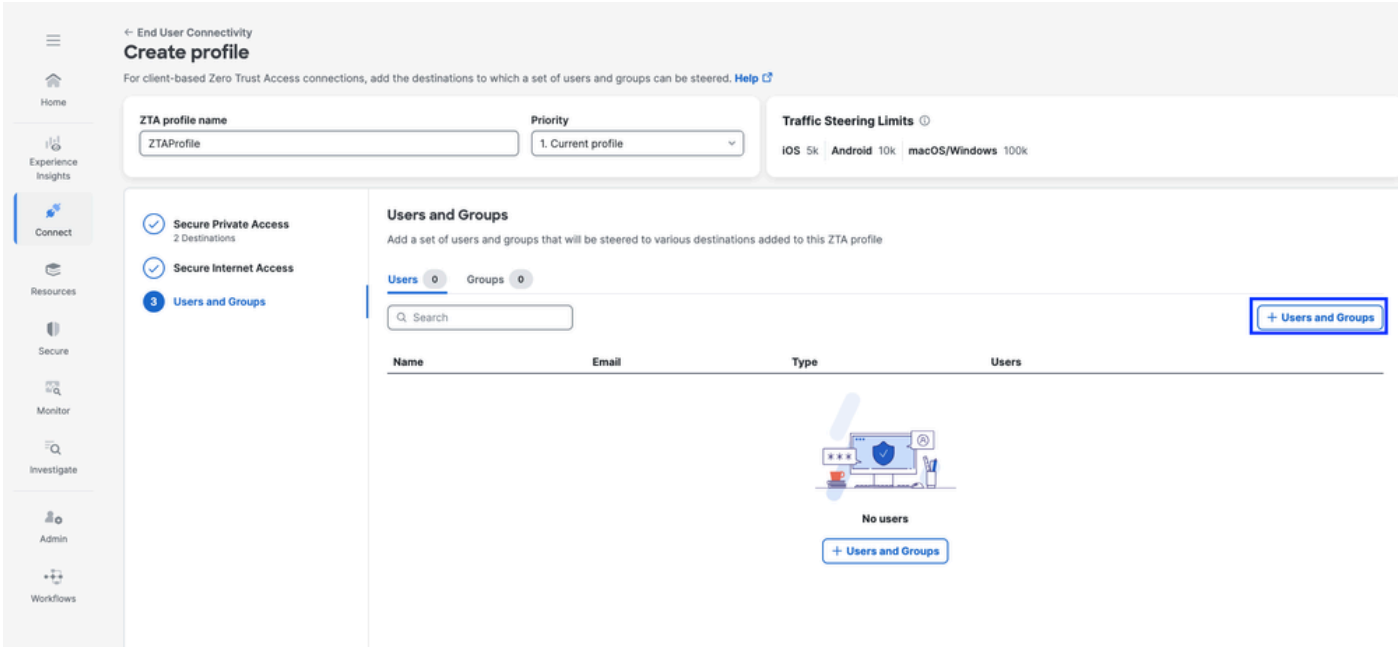


Acceso seguro - Perfil ZTA

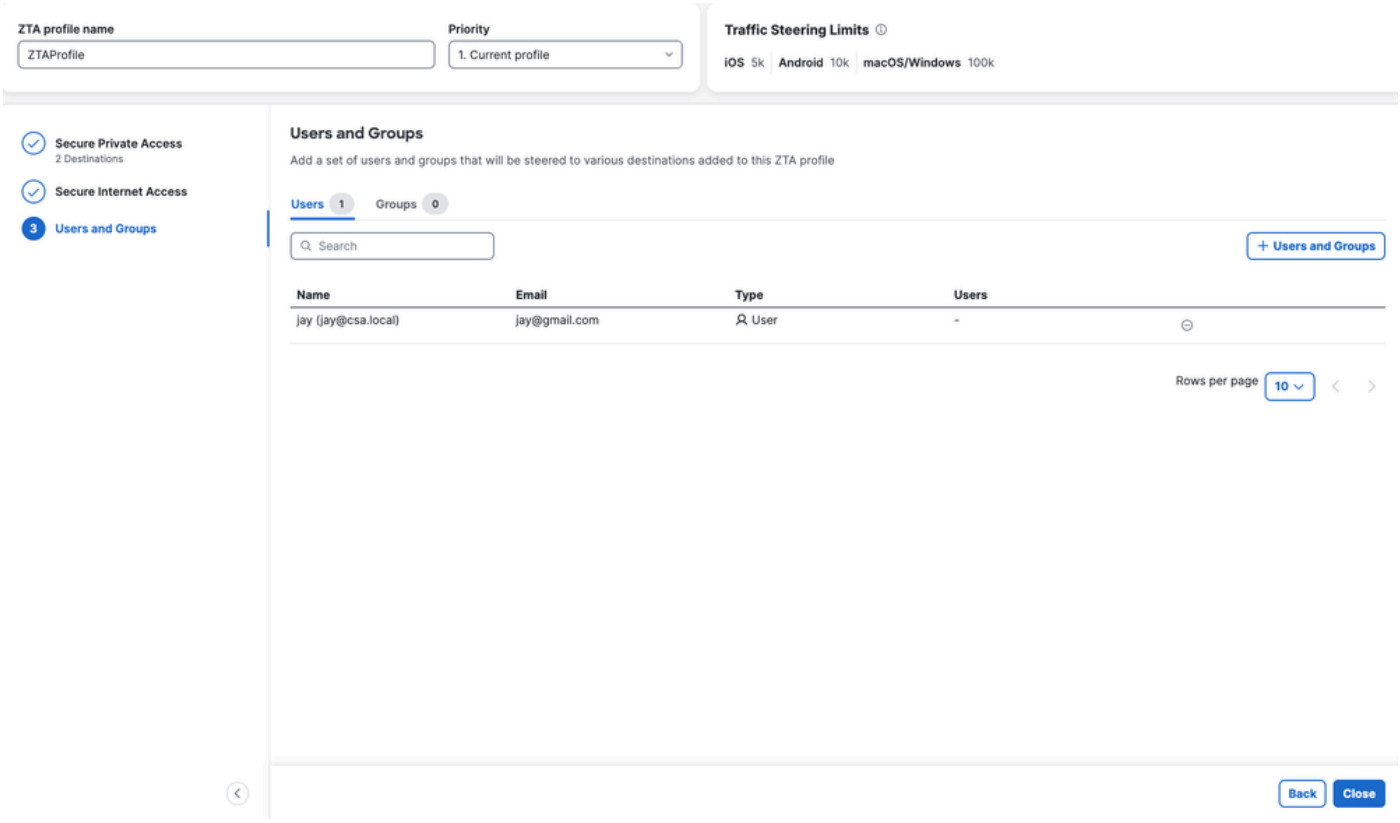


Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos



Acceso seguro - Perfil ZTA



Acceso seguro - Perfil ZTA

Paso - 5 Verificar el acceso al recurso privado

1. Compruebe que el usuario remoto puede resolver el FQDN del FTD

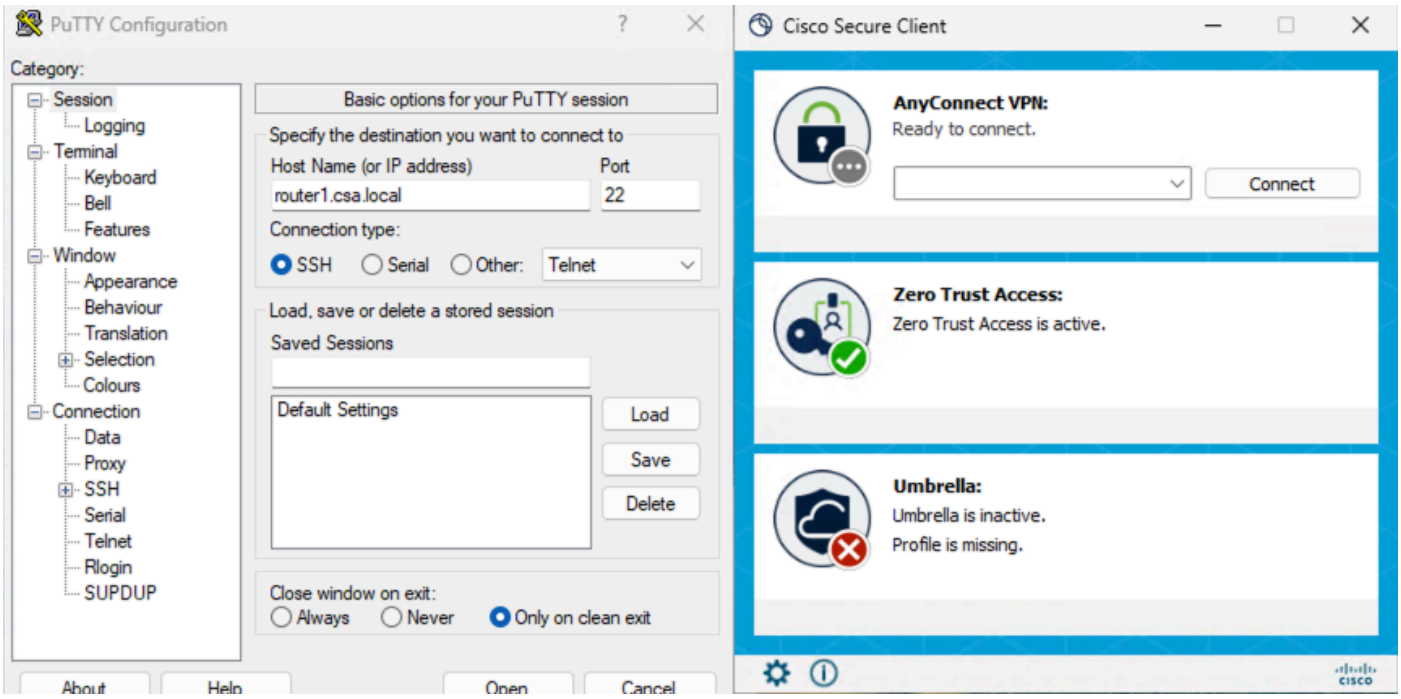
```
PS C:\Users\jay> ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
PS C:\Users\jay> nslookup ftd.csa.local
Server:  UnKnown
Address:  192.168.1.20

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

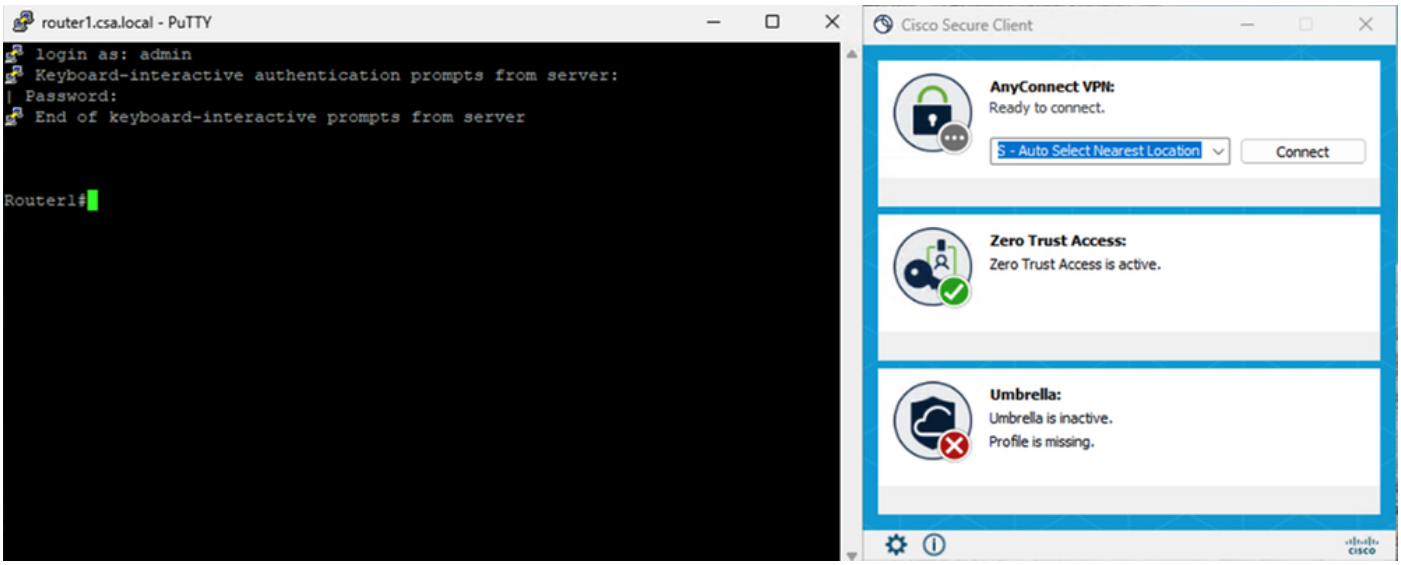
2. Compruebe que FTD puede llegar a un recurso privado mediante FQDN

```
ftd> en
Password:
ftd# ping router1.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ftd#
```


3. Pruebe la conexión SSH al recurso privado

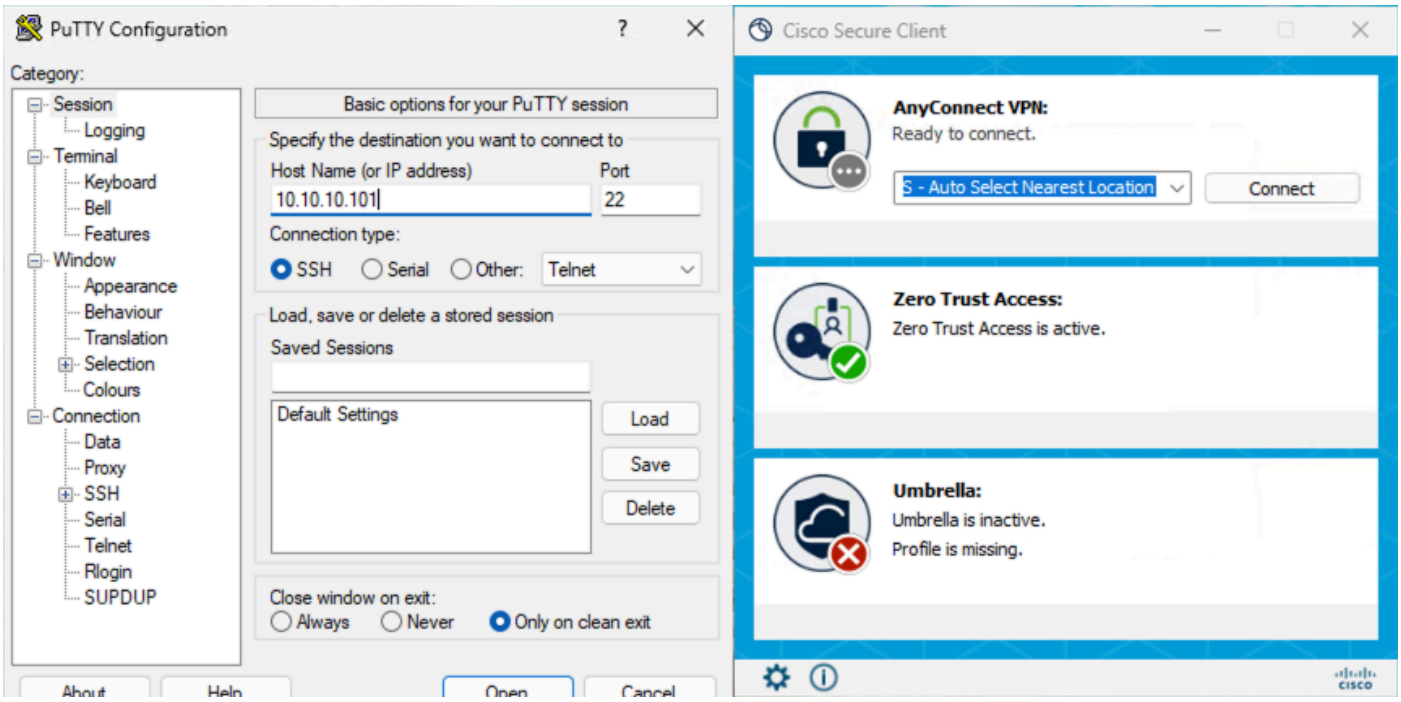
Acceso al PR mediante FQDN



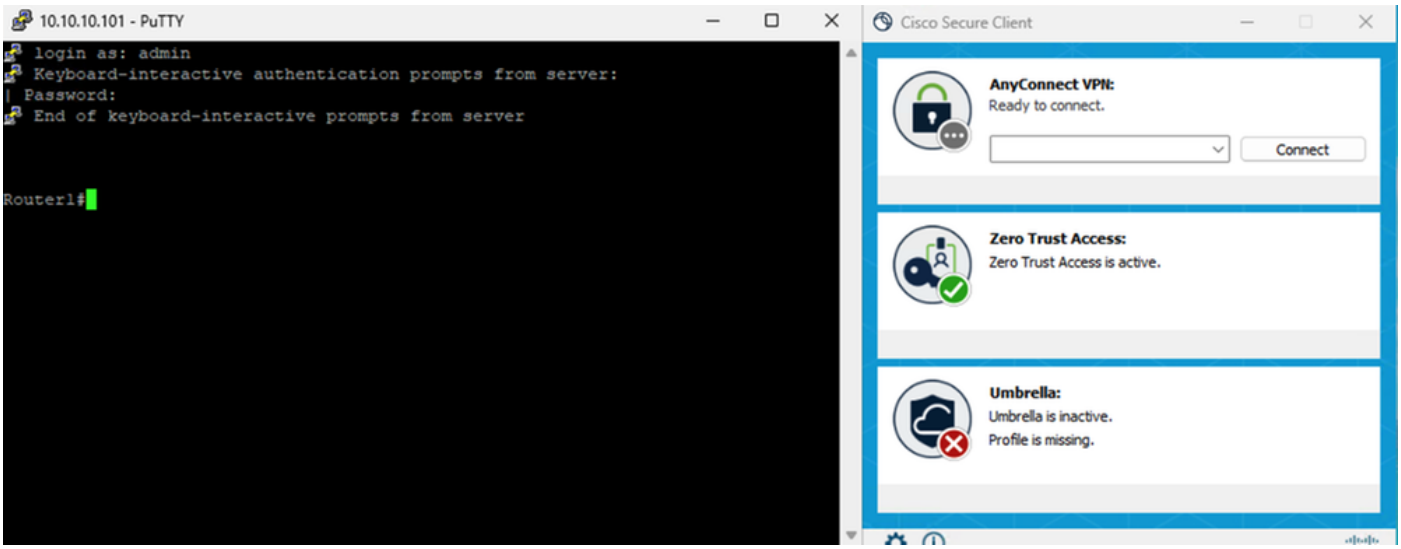


Secure Access - Prueba de relaciones públicas

Acceso al PR mediante la dirección IP

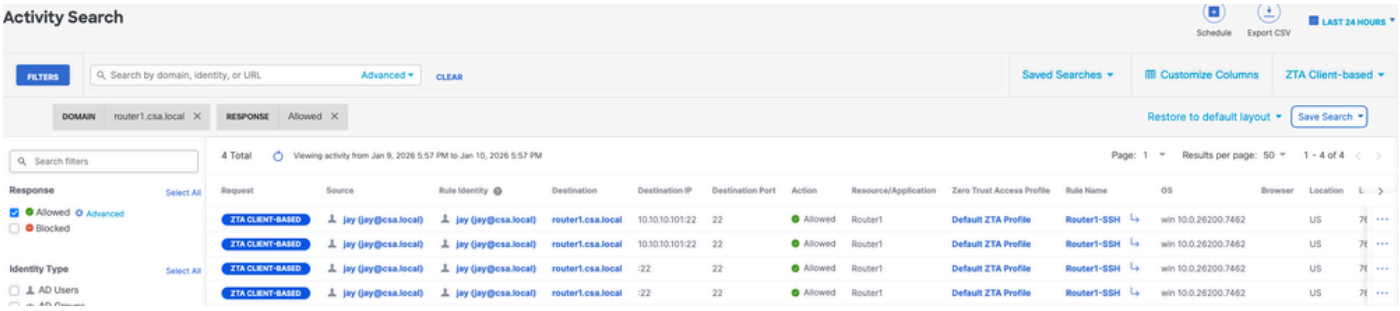


Secure Access - Prueba de relaciones públicas

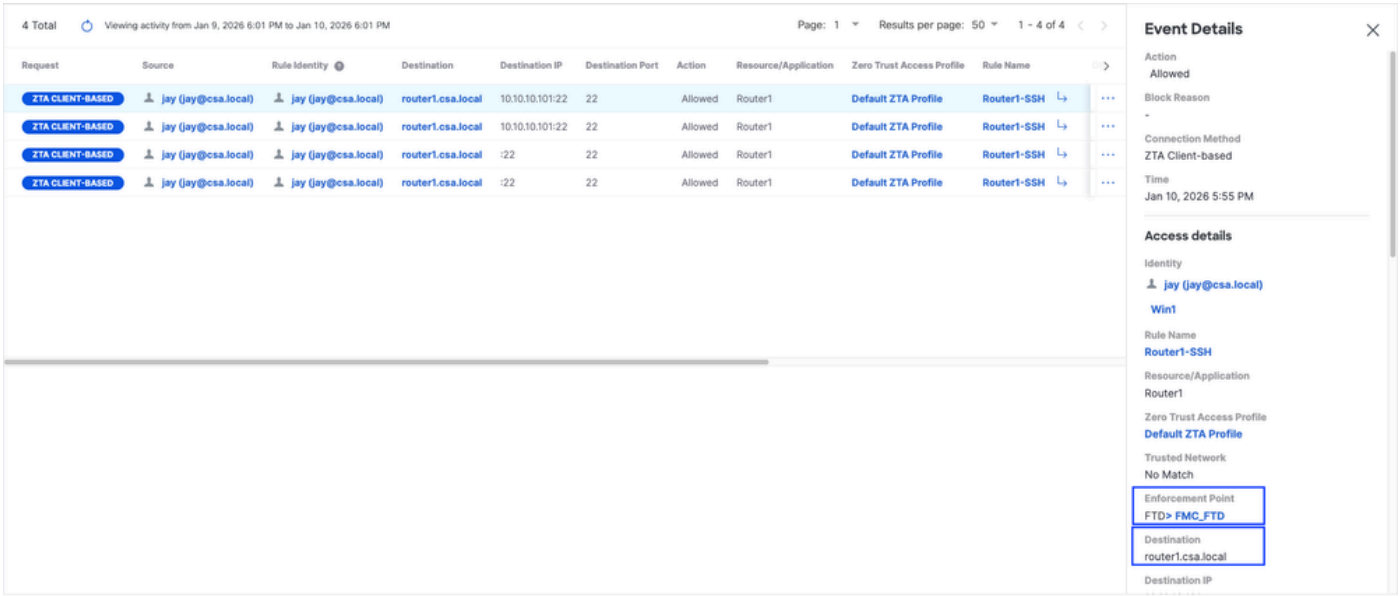


Secure Access - Prueba de relaciones públicas

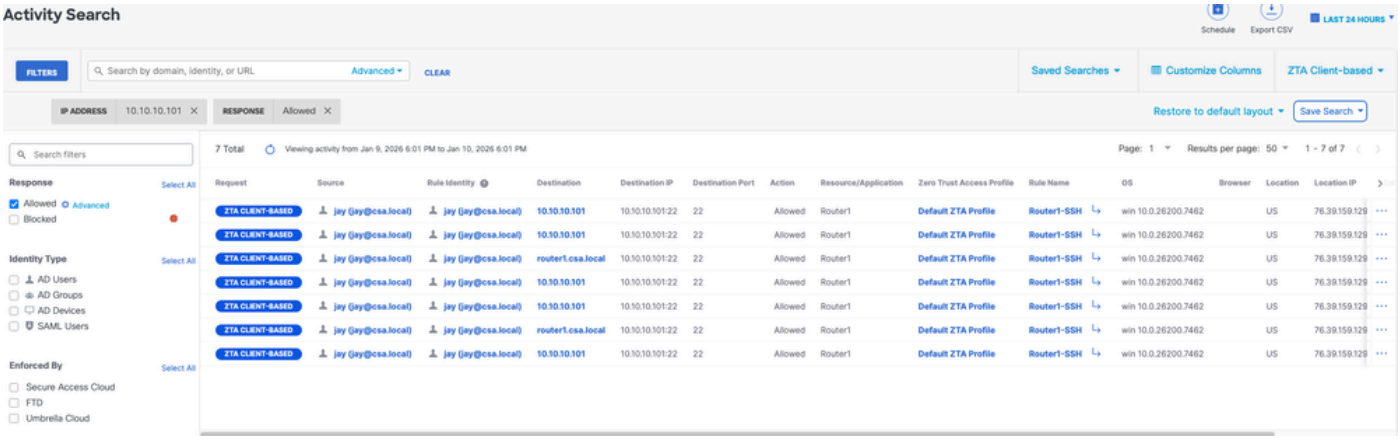
4. Verificar registros de búsqueda de actividad de acceso seguro



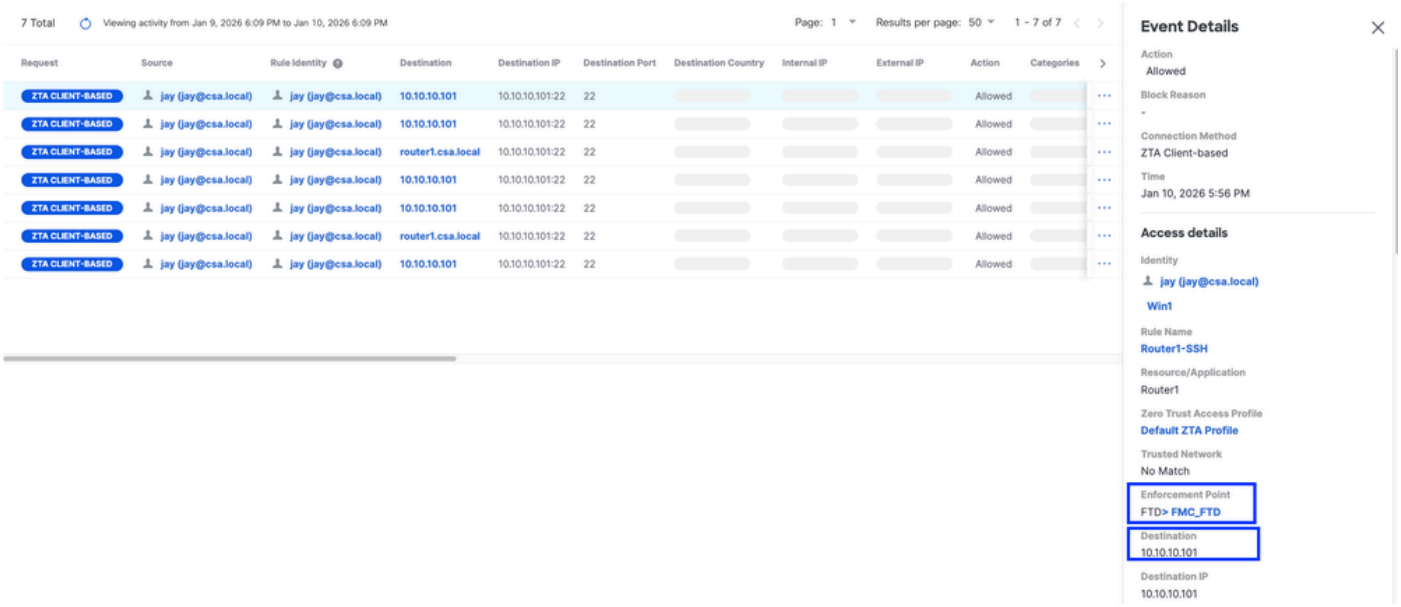
Acceso seguro - Búsqueda de actividad



Acceso seguro - Búsqueda de actividad

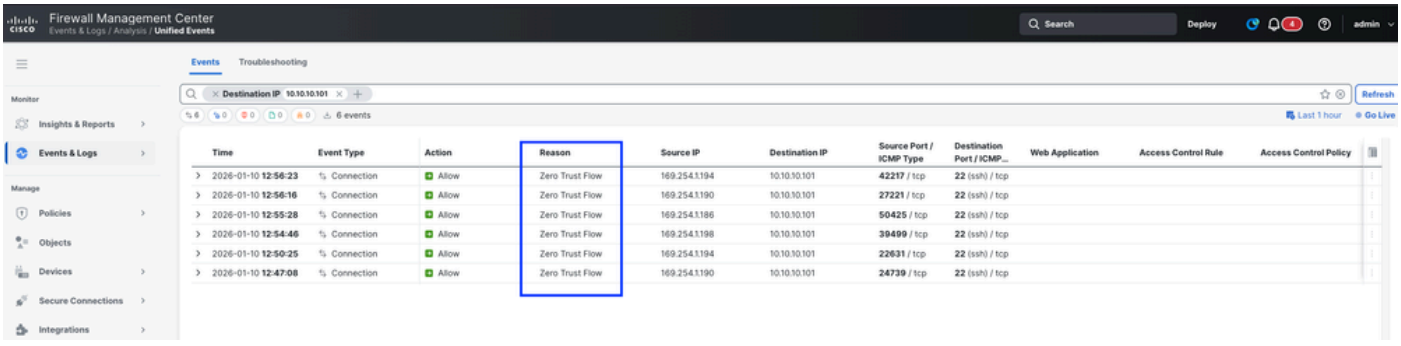


Acceso seguro - Búsqueda de actividad



Acceso seguro - Búsqueda de actividad

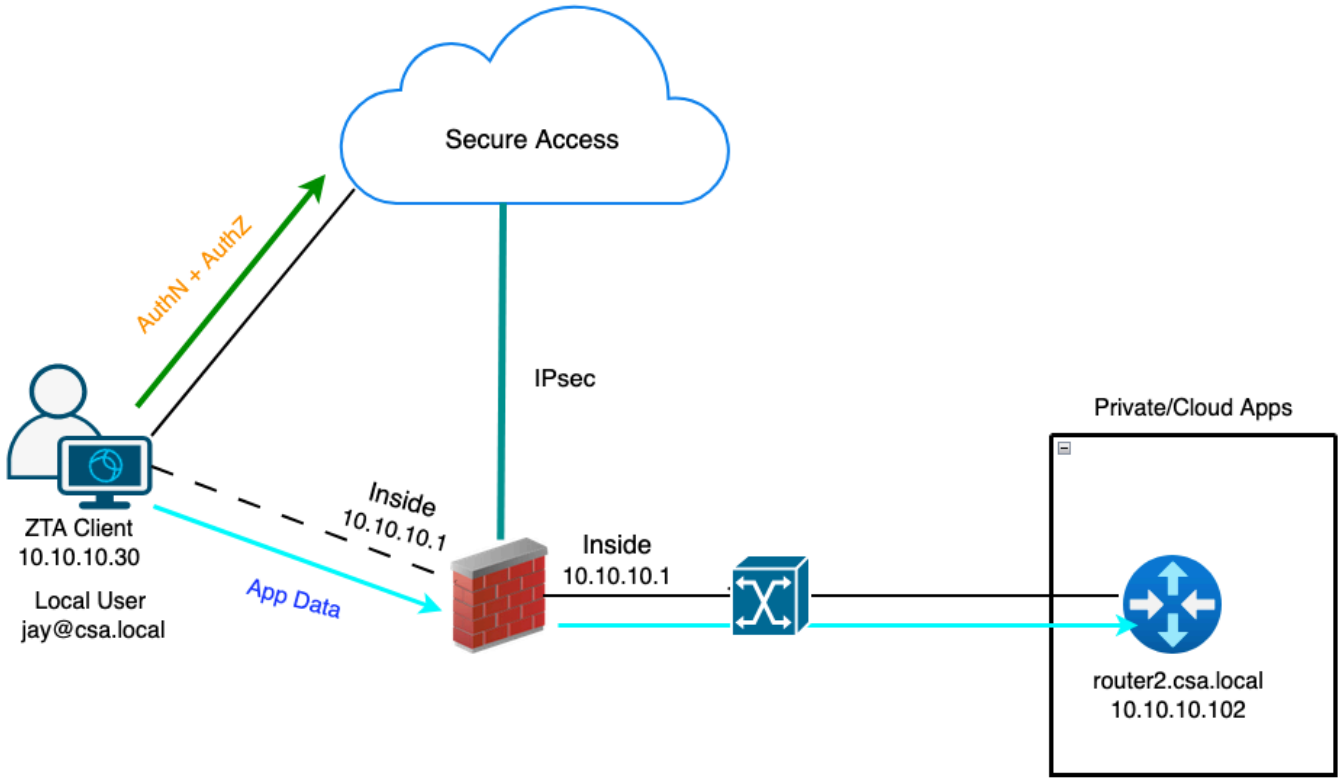
5. Verificar eventos de conexión FMC



Eventos de conexión FMC

Caso de prueba 3: usuario local, aplicación local

Al acceder a un recurso privado a través de la aplicación local como usuario local, en este tipo de aplicación, la evaluación de la política se realiza en Secure Access, pero los datos de la aplicación permanecen locales en FTD. Por ejemplo , un cliente o usuario registrado de ZTA conectado a la red doméstica e intentando acceder a un recurso privado que está detrás de la interfaz interna de FTD . Si el recurso privado está detrás de DMZ o cualquier otra interfaz del FTD, entonces tendríamos que crear una regla de acceso en el FTD para permitir el tráfico entre la IP del cliente o la red y el recurso privado.

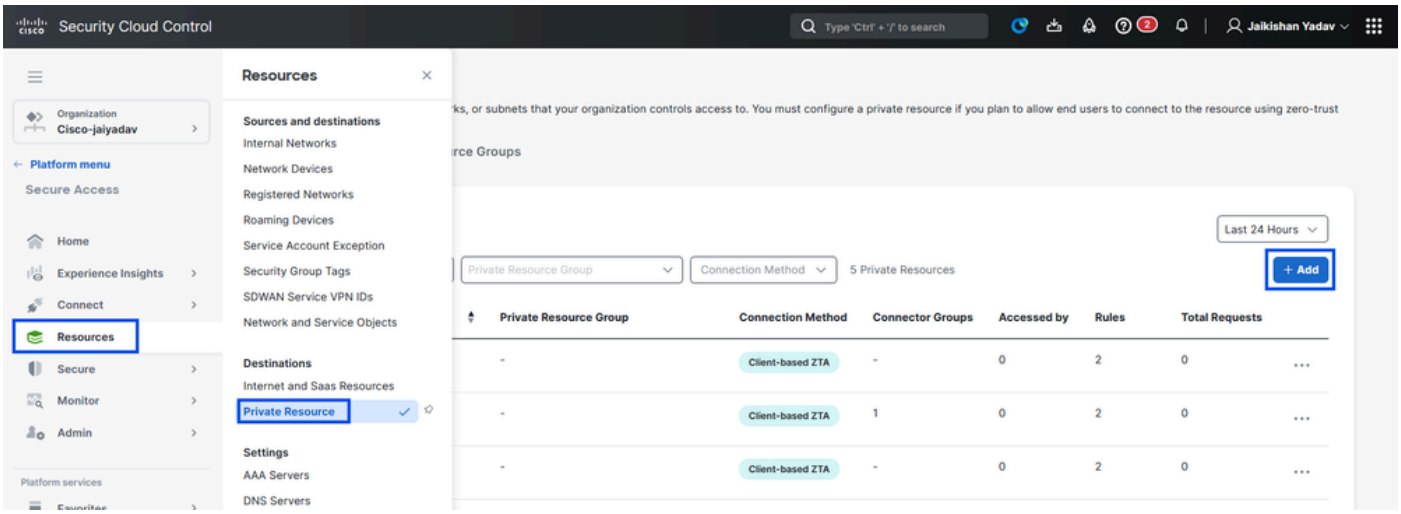


Universal ZTA - Topología de casos de prueba

Paso 1 - Definir un recurso privado en Secure Access

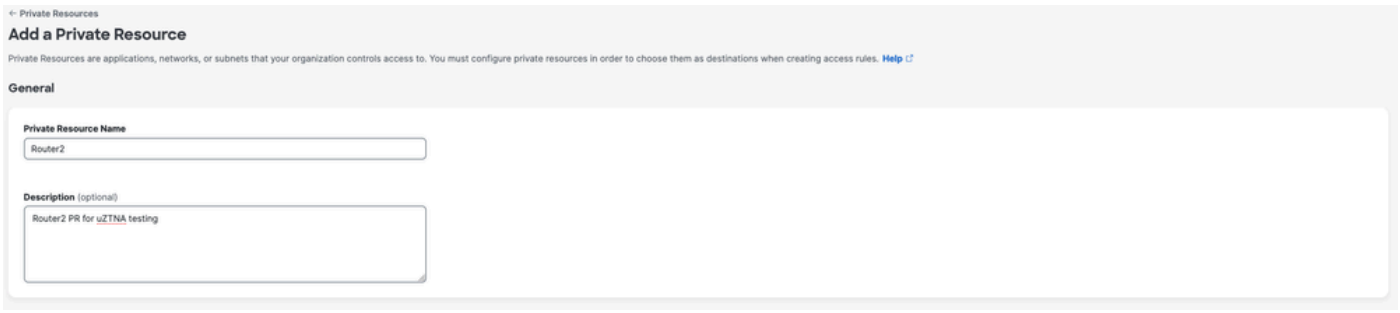
Configure un recurso privado al que se pueda acceder a través del dispositivo inscrito de acceso de confianza cero (ZTA) con aplicación en la nube

1. Navegue hasta Recursos > Destinos > Recursos privados > Haga clic en +Agregar



Acceso seguro - Configuración de recursos privados

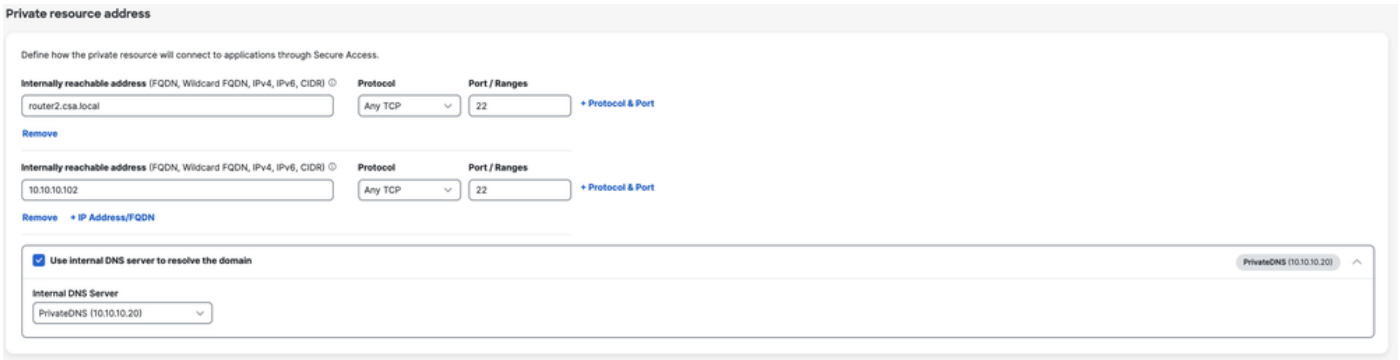
2. En Nombre de Recurso Privado, introduzca un nombre significativo para el recurso. Para Descripción, se recomienda proporcionar información como el propósito del recurso o el nombre del propietario del recurso.



Acceso seguro - Configuración de recursos privados

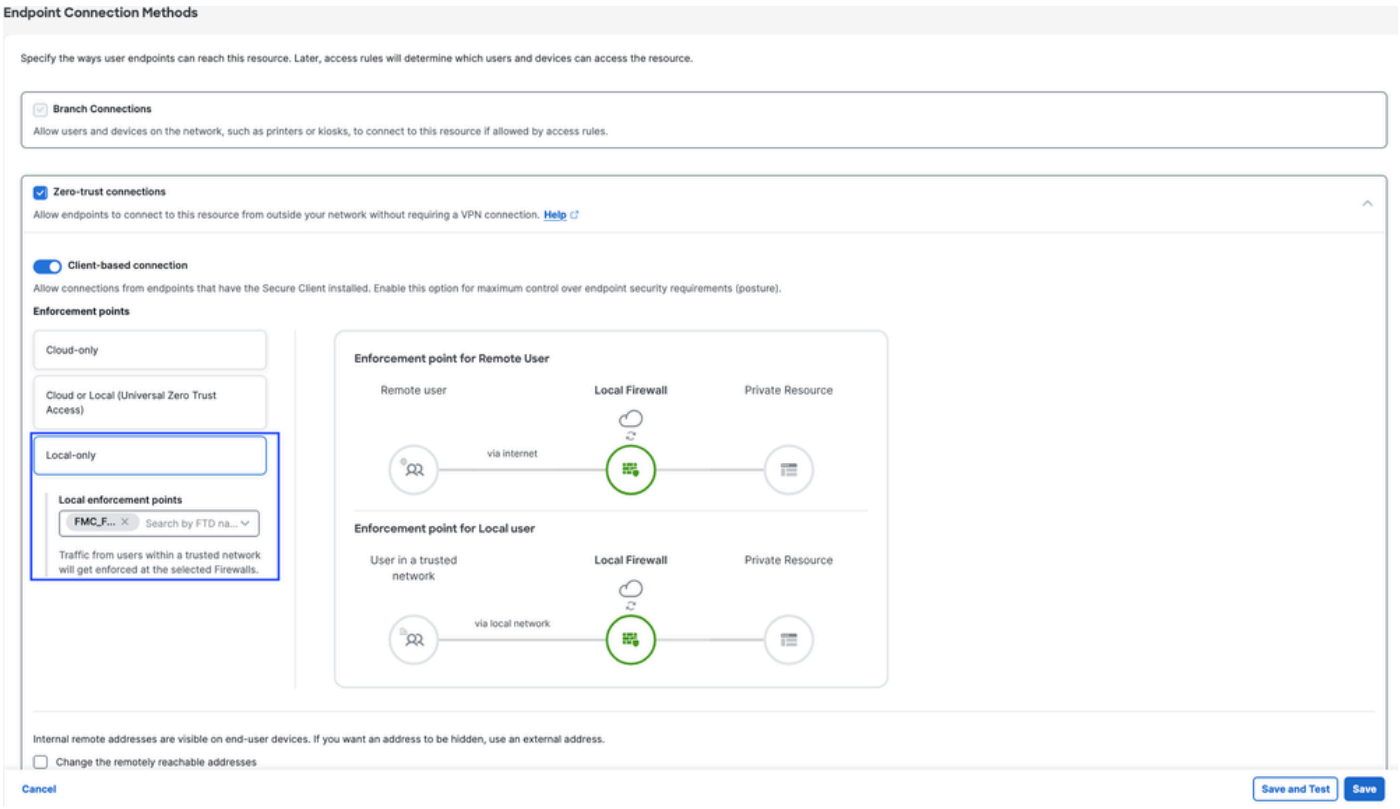
3. Introduzca el FQDN del recurso privado al que desea acceder . También podemos definir la dirección IP del recurso privado . Para obtener más información, vea [Agregar un recurso privado]

4. Seleccione el servidor DNS interno para resolver el dominio



5. Seleccionar métodos de conexión de terminales

6. Seleccione FTD como puntos de aplicación locales



Acceso seguro - Configuración de recursos privados

Nota: En función del tipo de inscripción que seleccione, este cambio asociará automáticamente el PR al FTD y activará una implementación de políticas

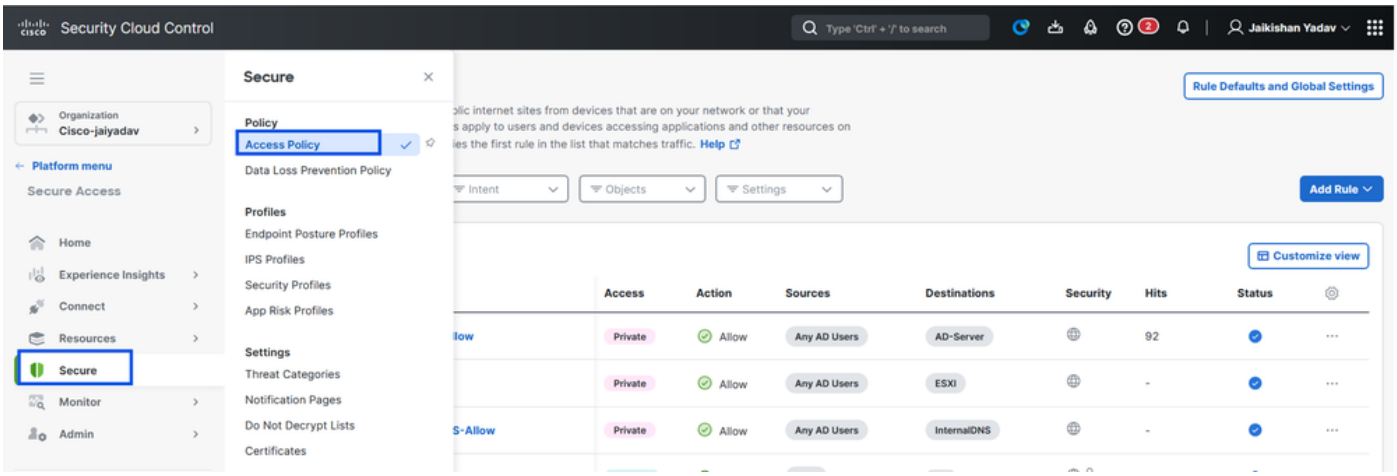
---

7. Haga clic en Save (Guardar).

Paso 2: Crear regla de acceso privado

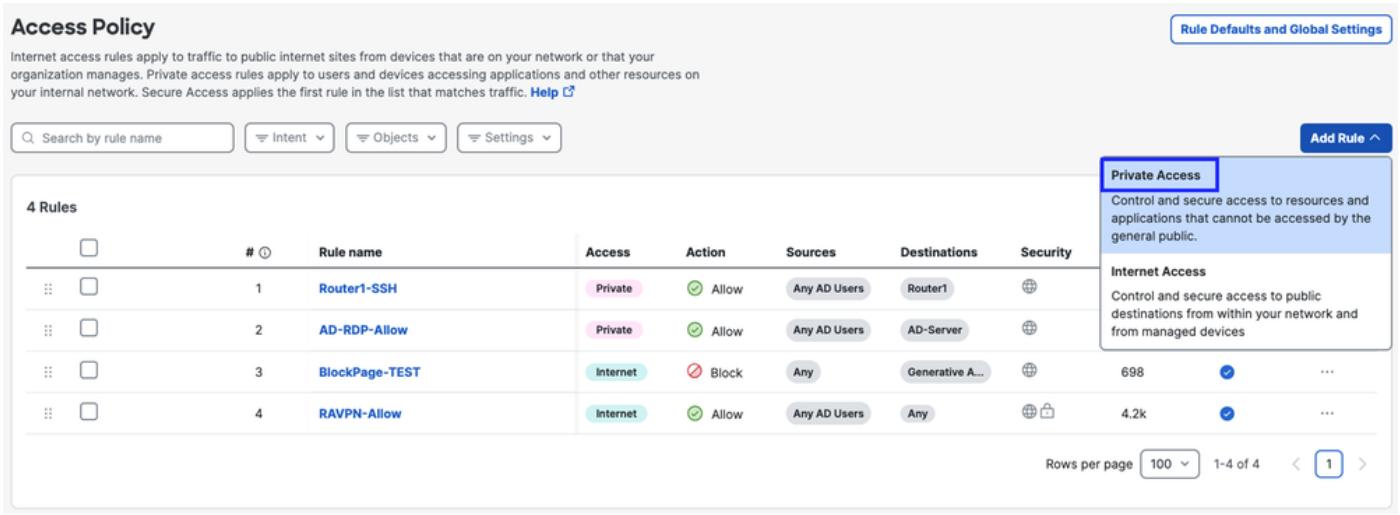
Configure un acceso privado en Secure Access para que los usuarios inscritos en Universal ZTA puedan acceder . Para obtener más información, vea Regla de acceso privado

1. Vaya a Seguro > Política de acceso



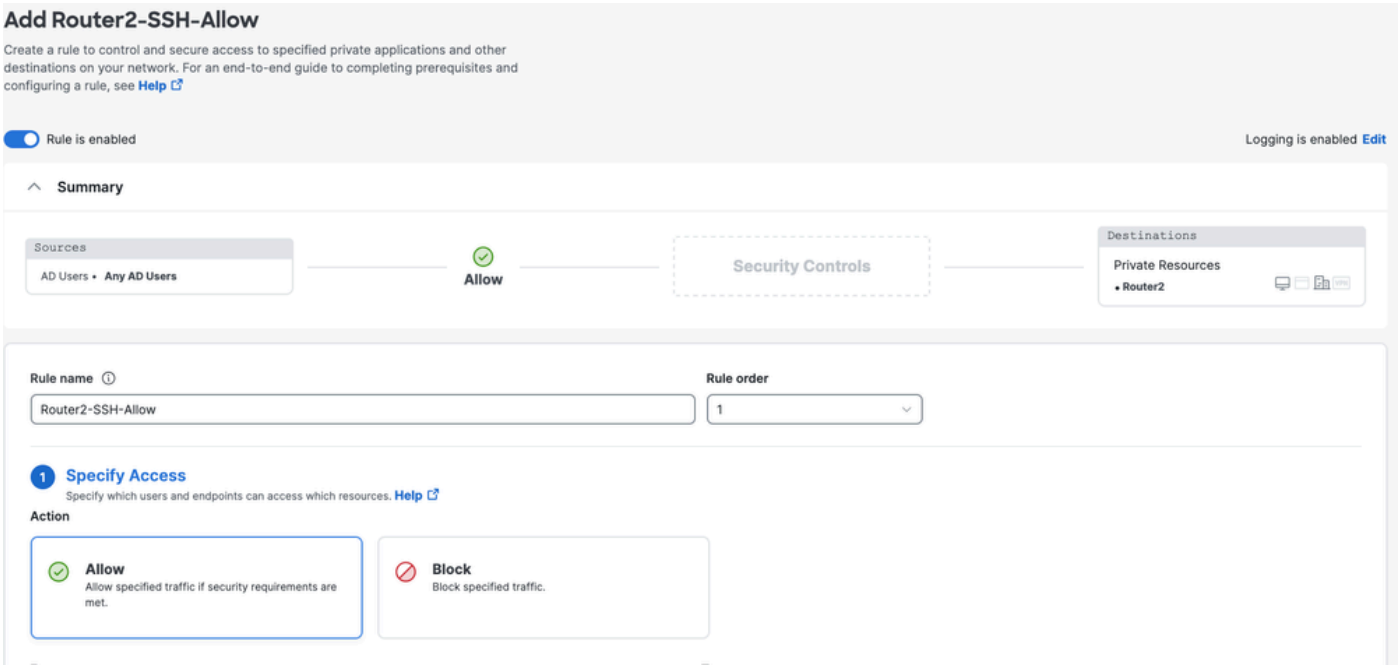
Acceso seguro - Configuración de la política de acceso

2. Haga clic en Agregar regla, y luego elija Acceso privado.
En la parte superior de la regla hay un resumen que describe los componentes configurados de la regla.



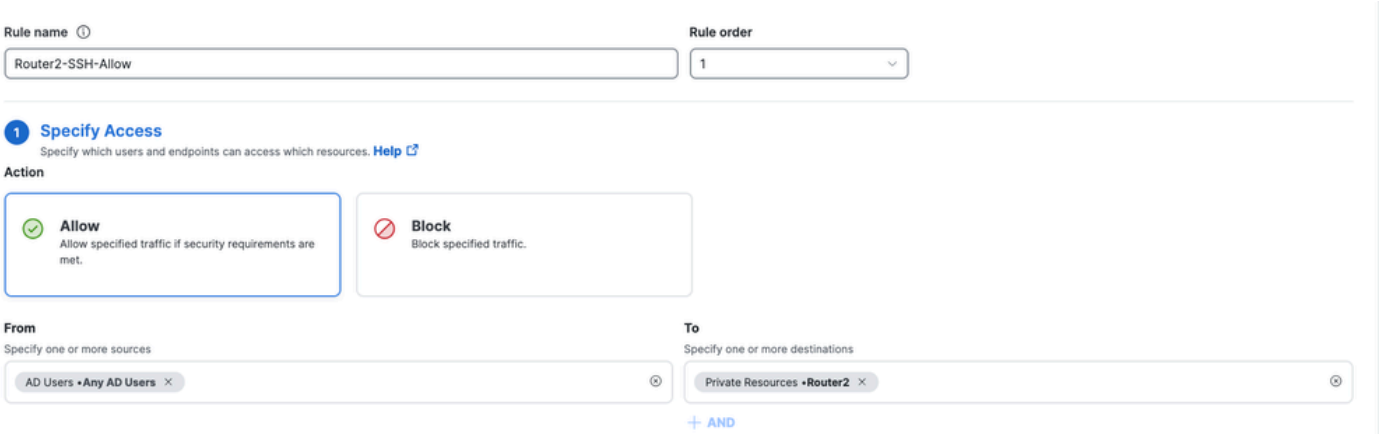
Acceso seguro - Configuración de la política de acceso

3. Agregar un nombre de regla



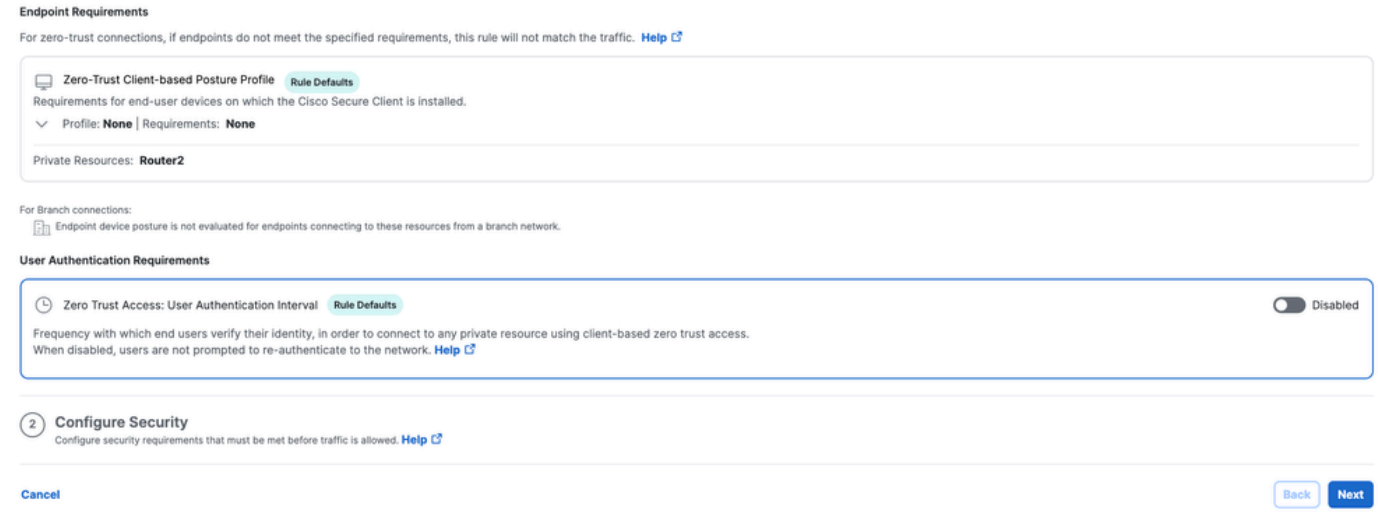
Acceso seguro - Configuración de la política de acceso

4. Seleccione la acción de regla y seleccione origen y destino



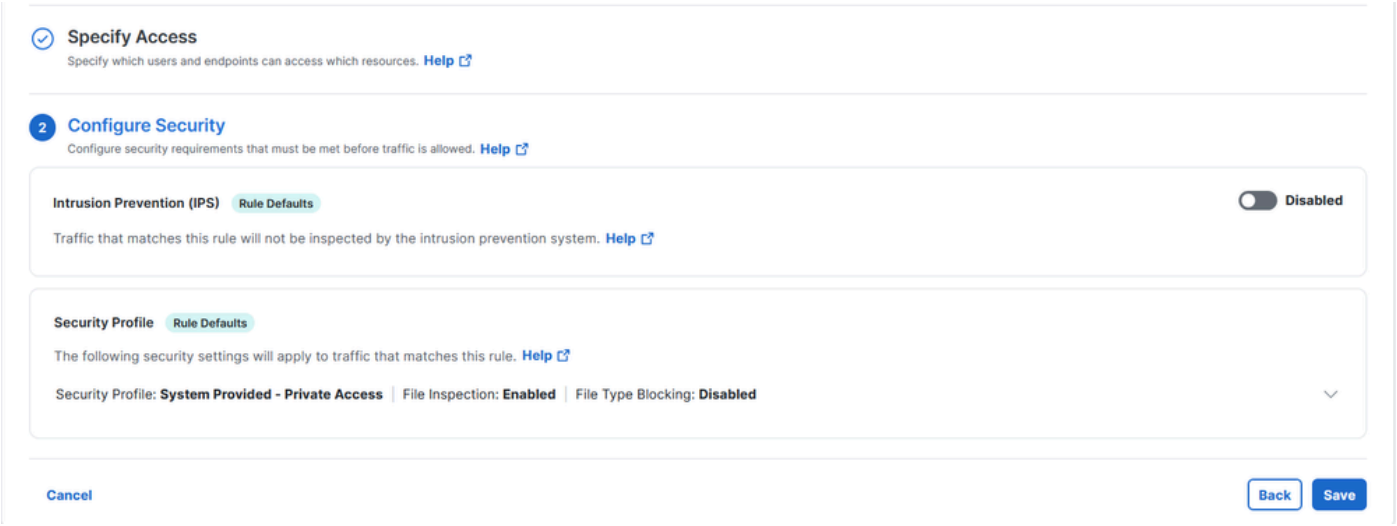
Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales



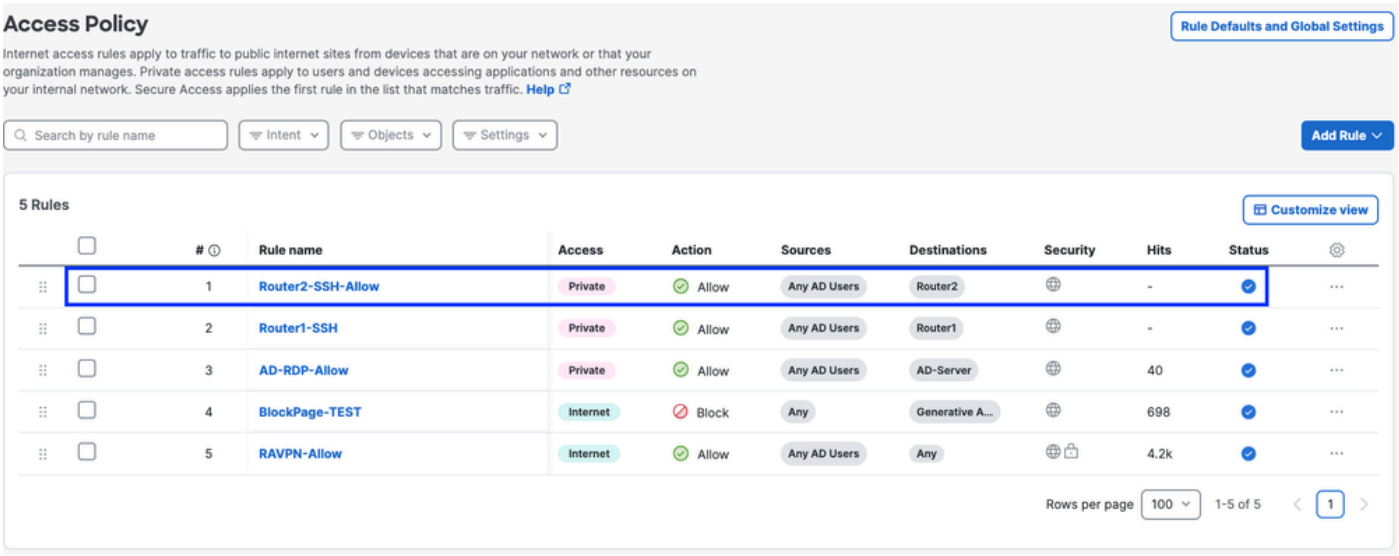
Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad



Acceso seguro - Configuración de la política de acceso

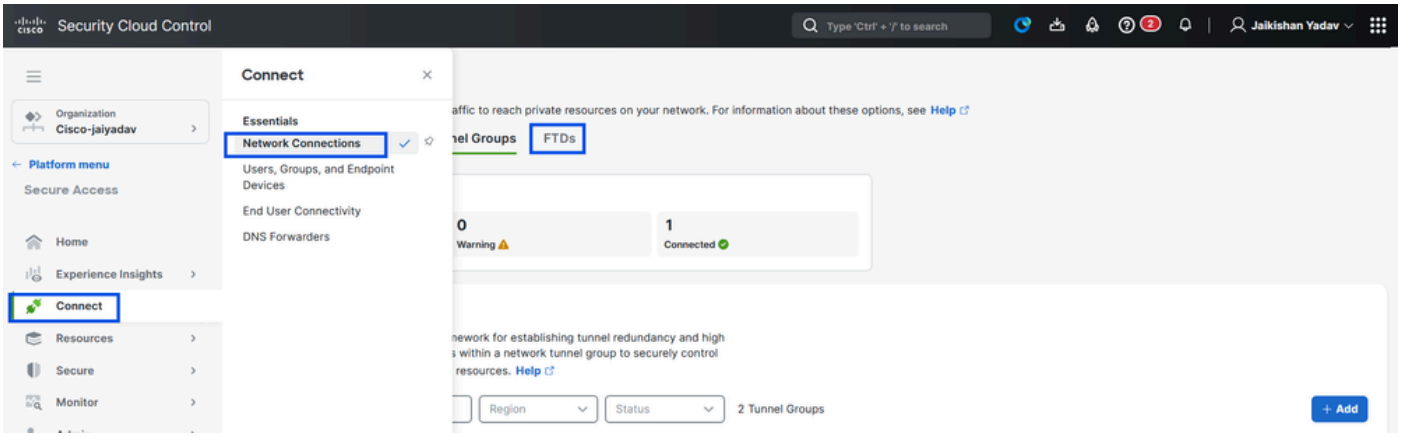
7. Haga clic en Guardar



Acceso seguro - Configuración de la política de acceso

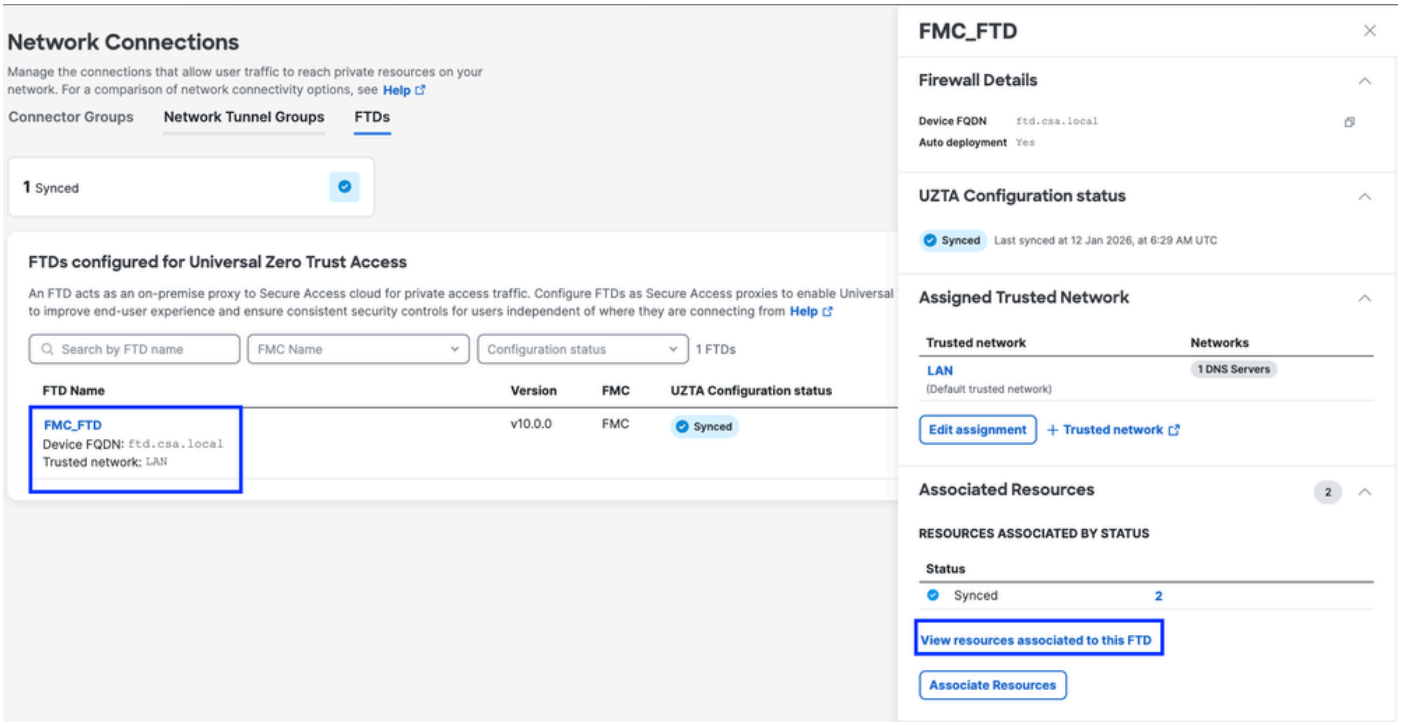
Paso 3 - Verificar la asociación de RP en el FTD

1. Vaya a connect > Network Connections > FTDs

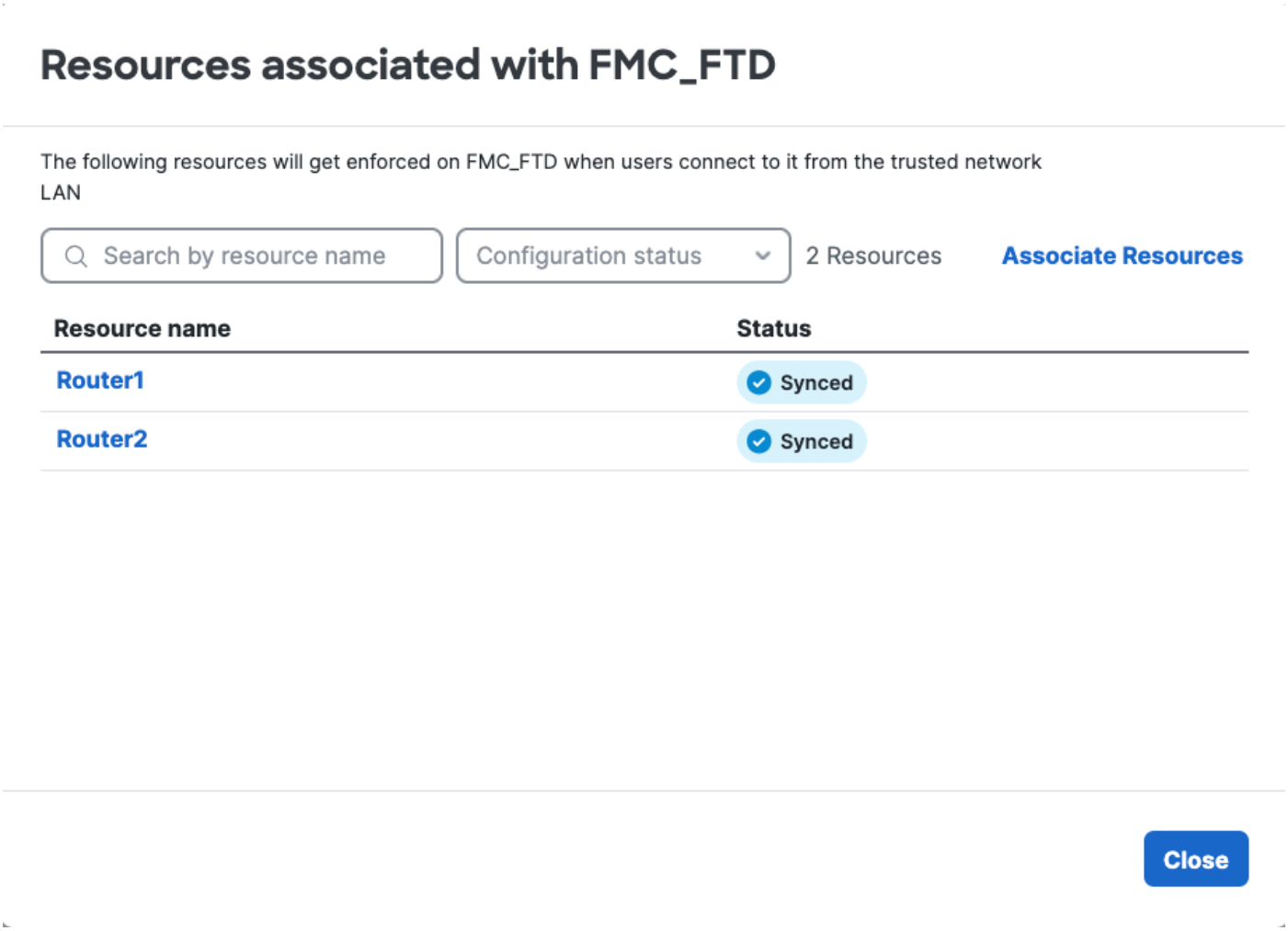


Acceso seguro - Verificación de relaciones públicas

2. Haga clic en el FTD > Ver recursos asociados a este FTD

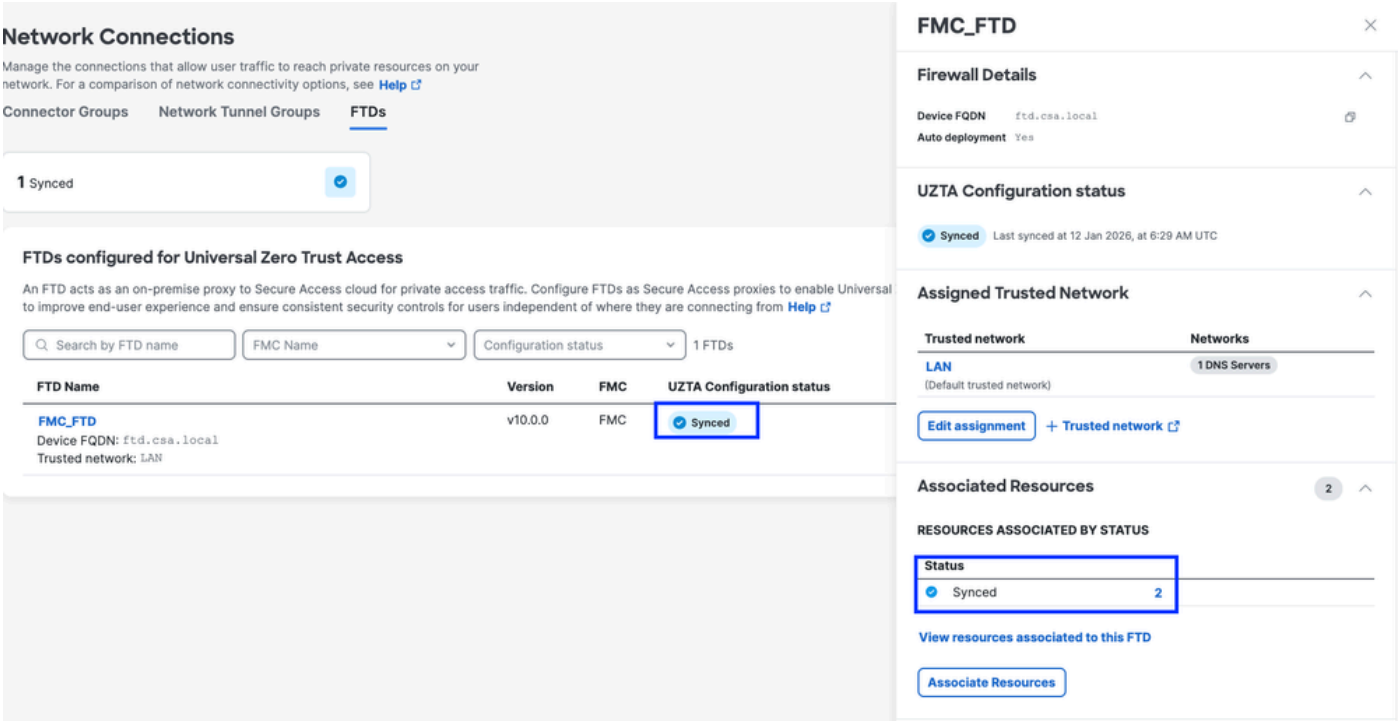


Acceso seguro - Verificación de relaciones públicas



3. Haga clic en Close (Cerrar)

4. Verifique el estado , el recurso asociado y la configuración deben estar en el estado Sincronizado



Acceso seguro - Verificación de relaciones públicas

5. Compruebe que la configuración se ha enviado al FTD

Inicie sesión en FTD cli y navegue hasta el modo LINA

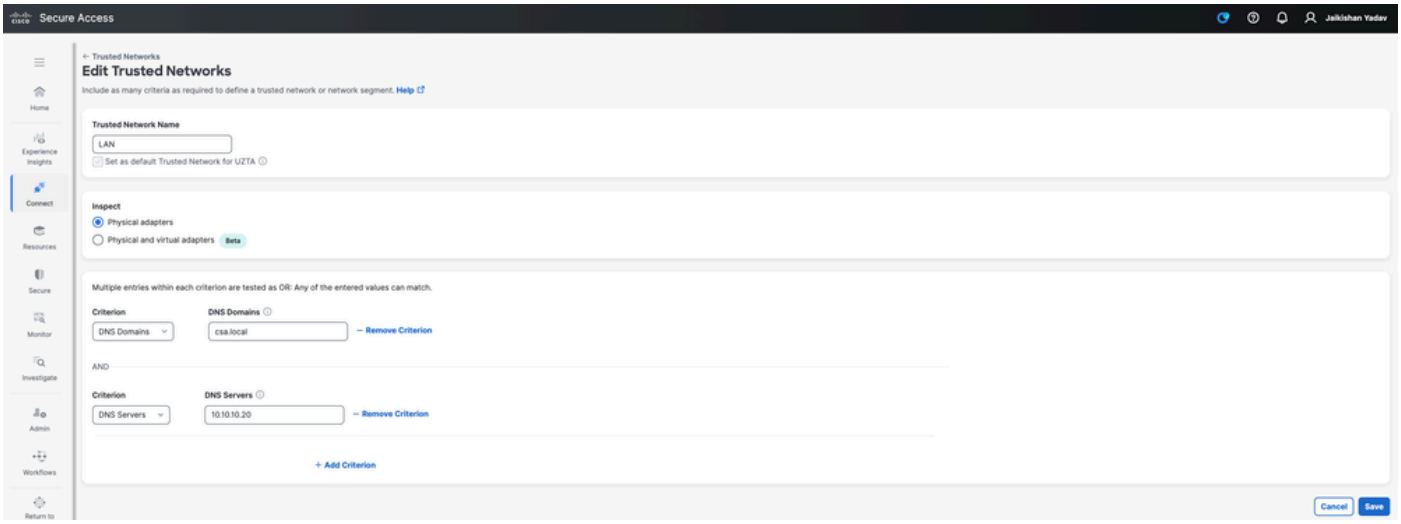
show running-config object application

```
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
```

Acceso seguro - Verificación de relaciones públicas

Paso - 4 Configurar " Administrar redes de confianza o configuración ZTA"

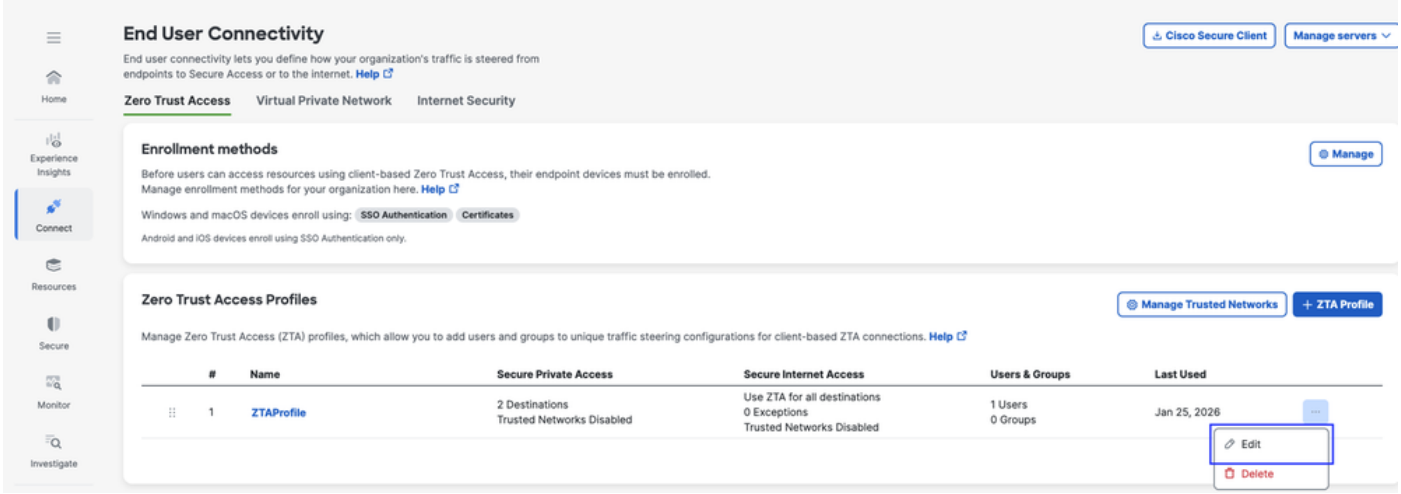
Vaya a Connect > End User Connectivity > Zero Trust Access > ZTA Settings y configure Trusted Networks



Acceso seguro - Configuración de TND

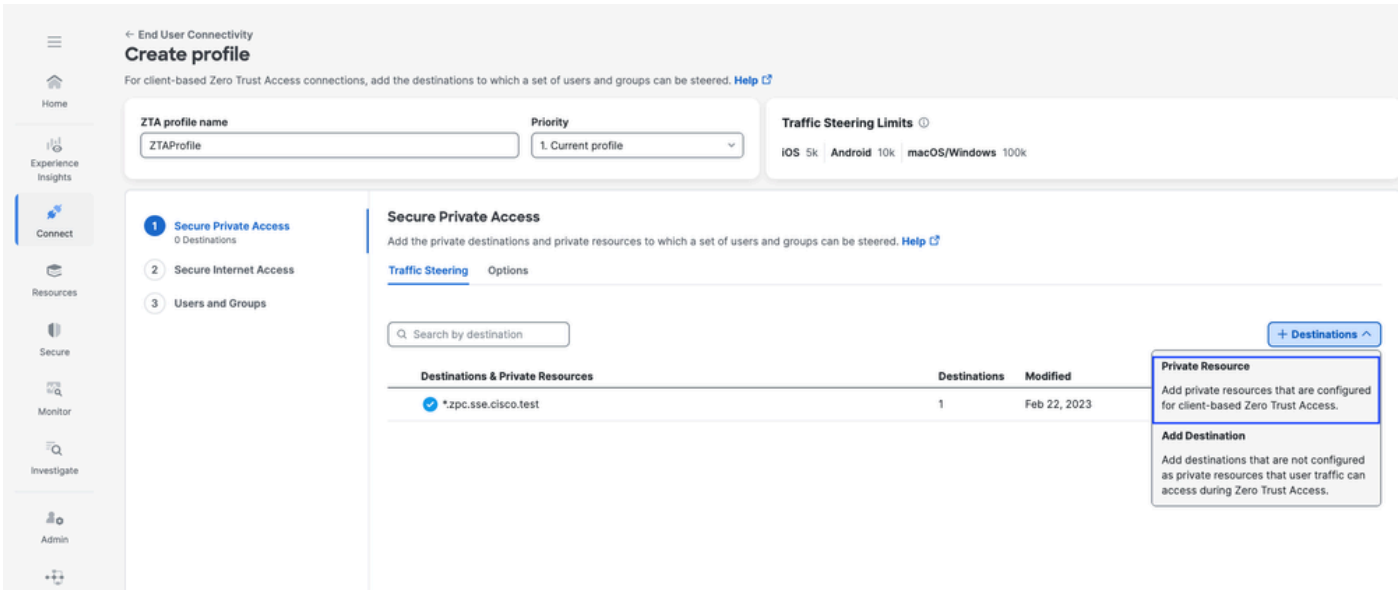
Paso -5 Agregar recurso privado al perfil ZTA

1. Navegue hasta Conexión > Conectividad del usuario final > Acceso de confianza cero y haga clic en 3 puntos para editar el perfil ZTA

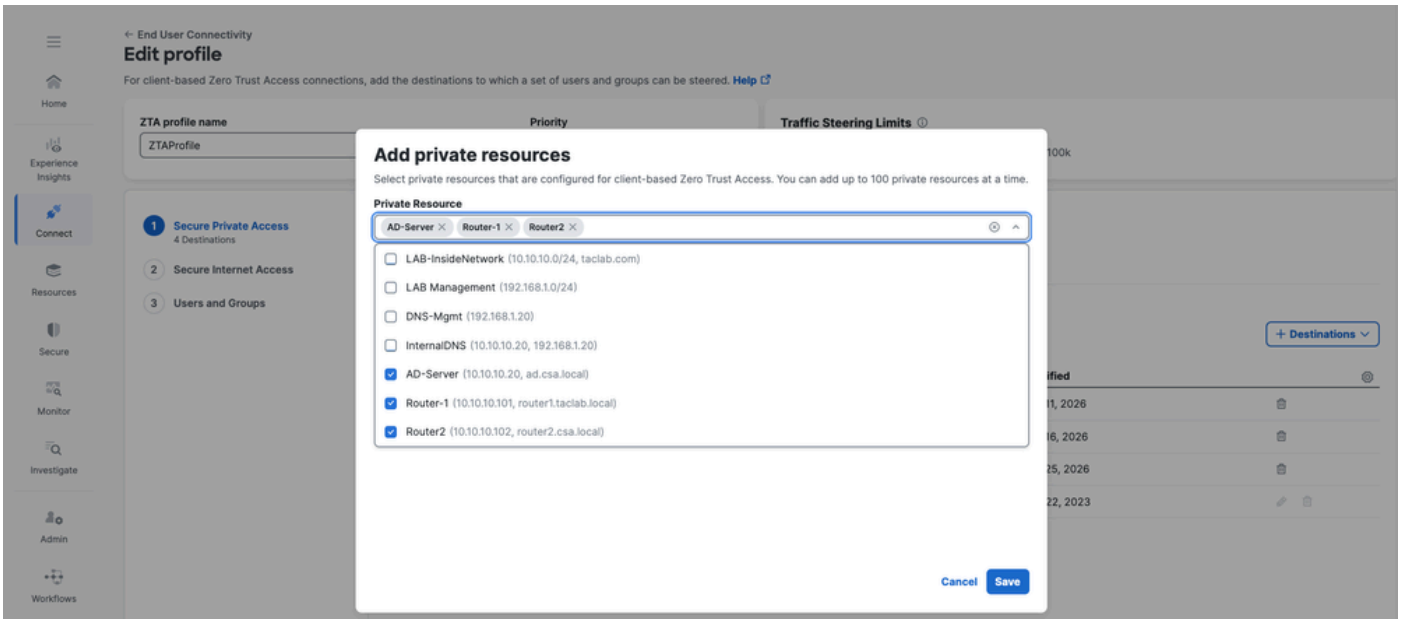


Acceso seguro - Perfil ZTA

2. Añada el recurso privado

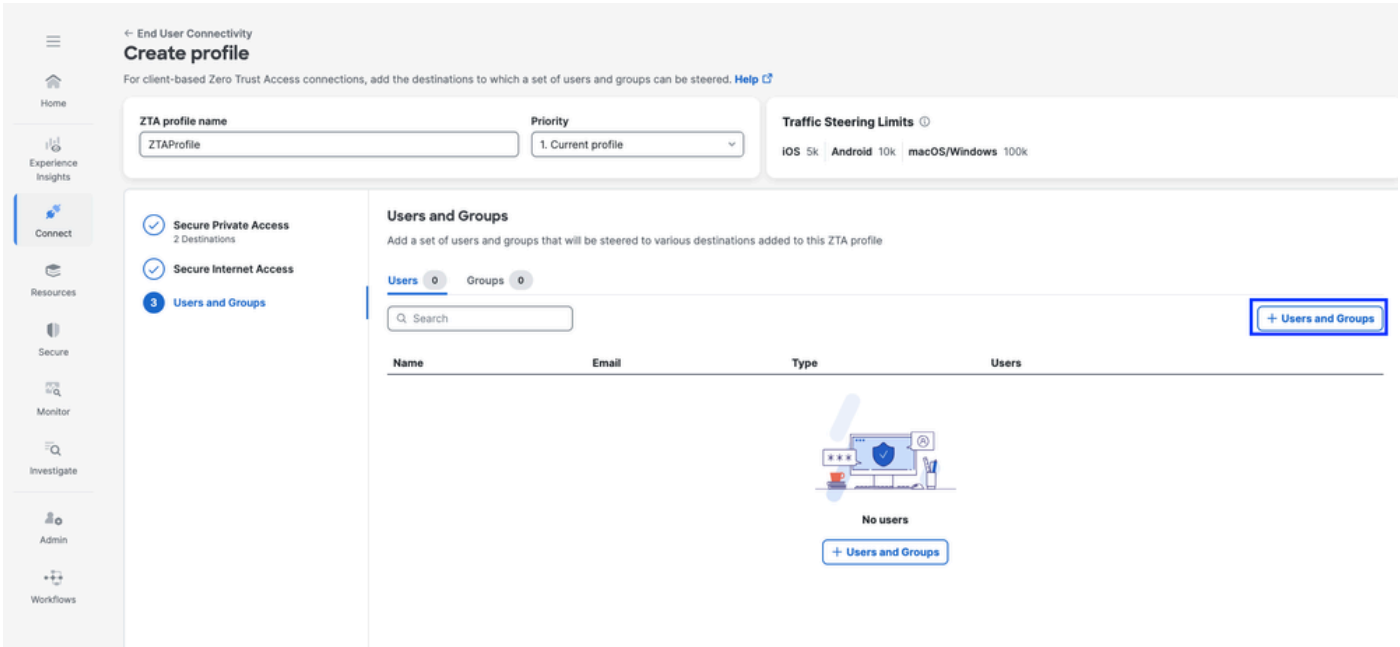


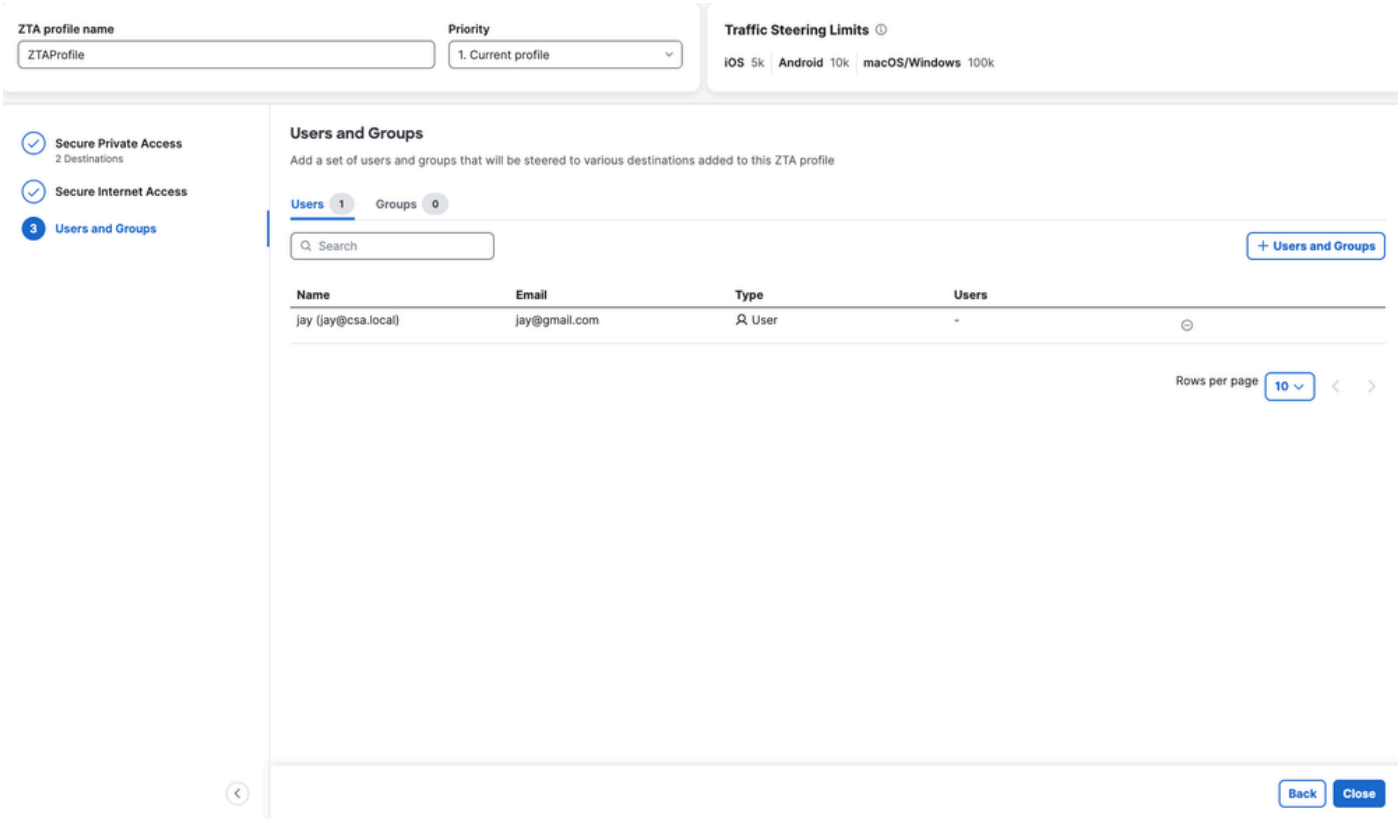
Acceso seguro - Perfil ZTA



Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos

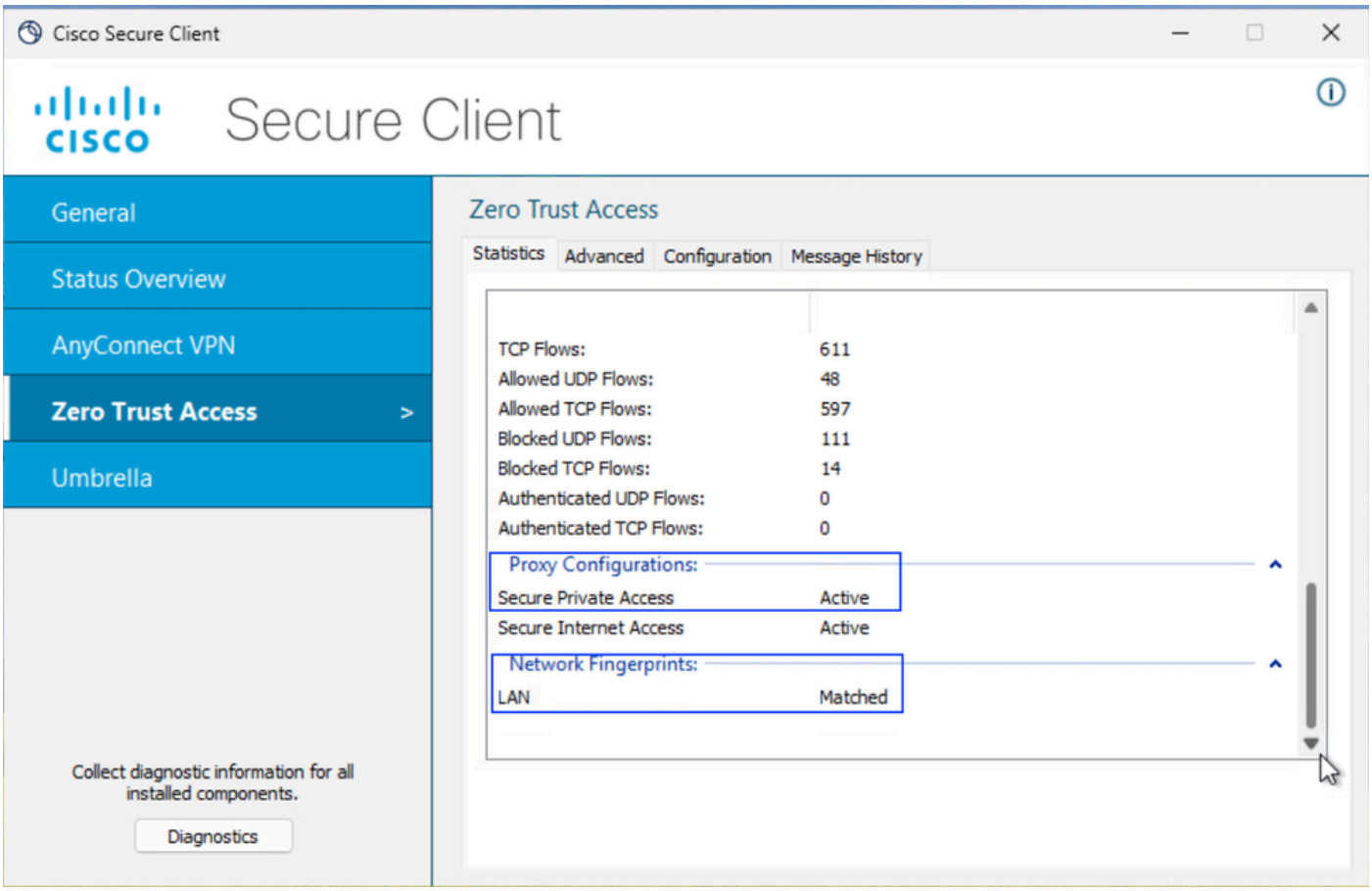




Acceso seguro - Perfil ZTA

Paso - 6 Verificar el acceso al recurso privado

1. Verifique la huella digital de la red para ZTA TND



Secure Access - Prueba de relaciones públicas

2. Compruebe que el usuario remoto puede resolver el FQDN del FTD

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

Pinging ftd.csa.local [10.10.10.1] with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\jay>nslookup ftd.csa.local
Server:  AD.csa.local
Address:  10.10.10.20

Name:    ftd.csa.local
Addresses:  10.10.10.1
```

Secure Access - Prueba de relaciones públicas

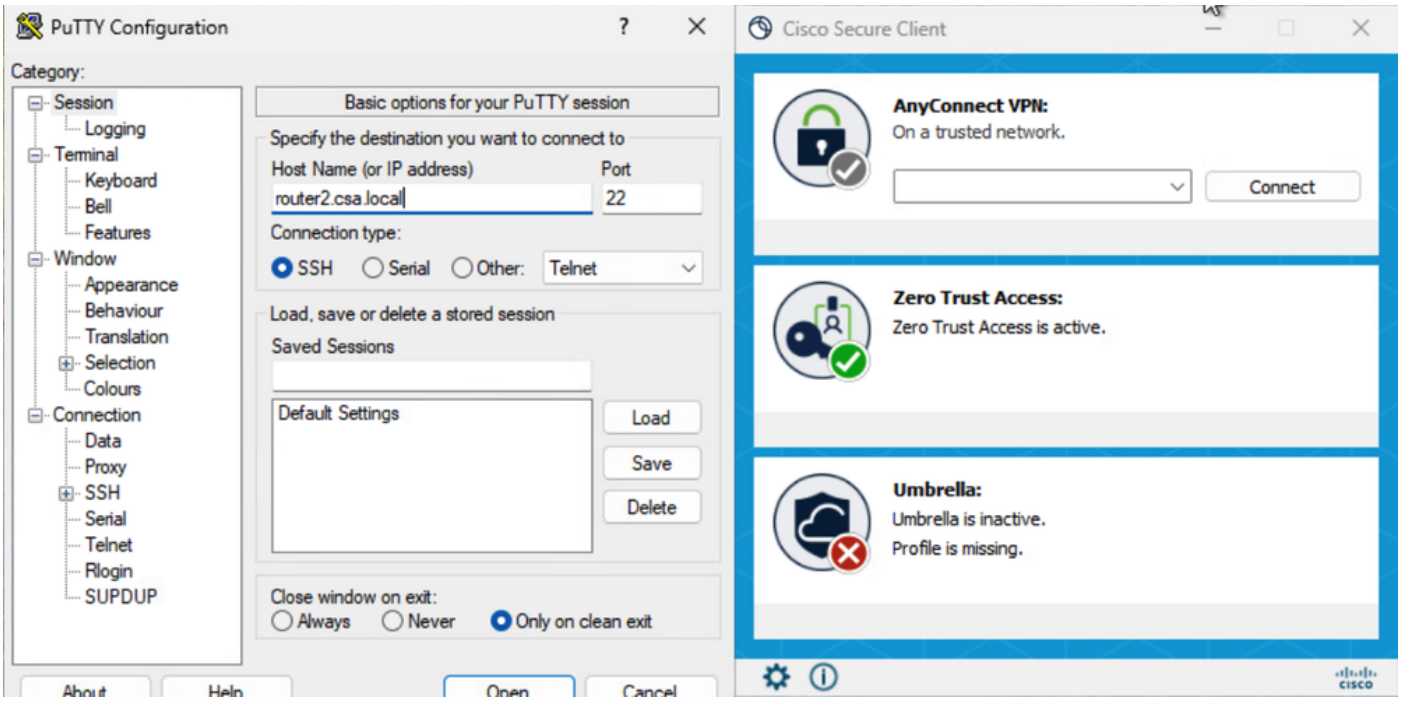
3. Compruebe que FTD puede alcanzar un recurso privado mediante FQDN

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

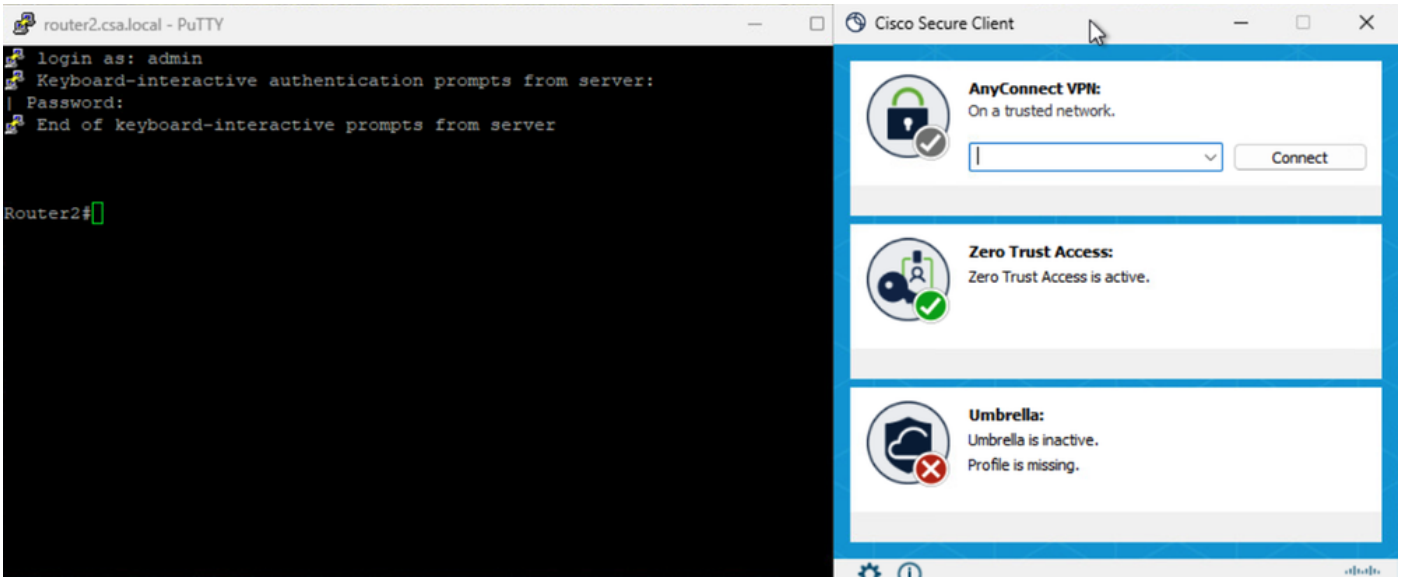
Secure Access - Prueba de relaciones públicas

4. Pruebe la conexión SSH al recurso privado

Acceso al PR mediante FQDN

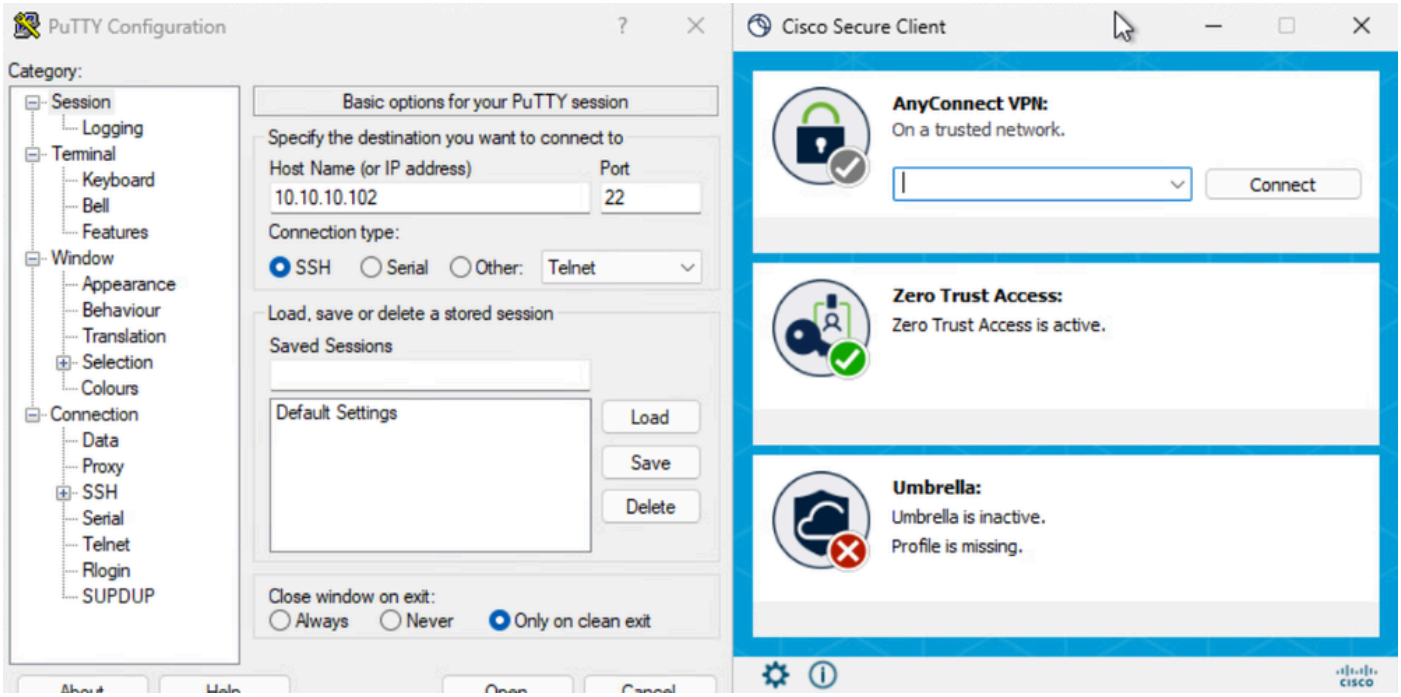


Secure Access - Prueba de relaciones públicas

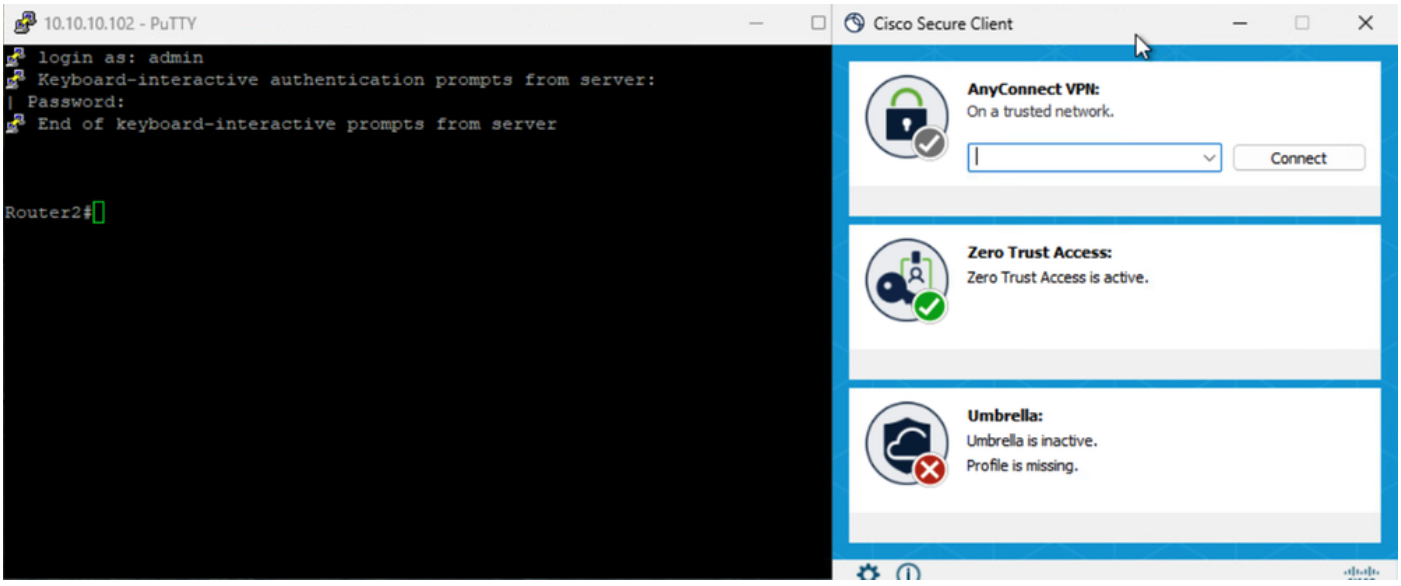


Secure Access - Prueba de relaciones públicas

Acceso al PR mediante la dirección IP

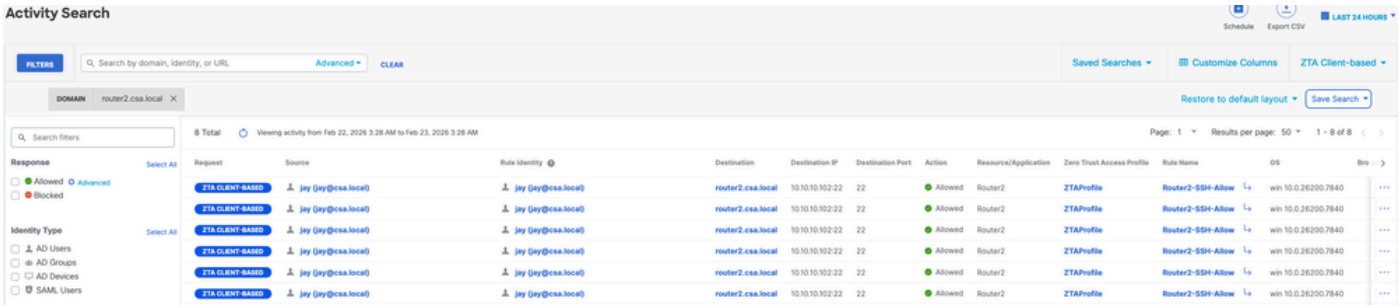


Secure Access - Prueba de relaciones públicas

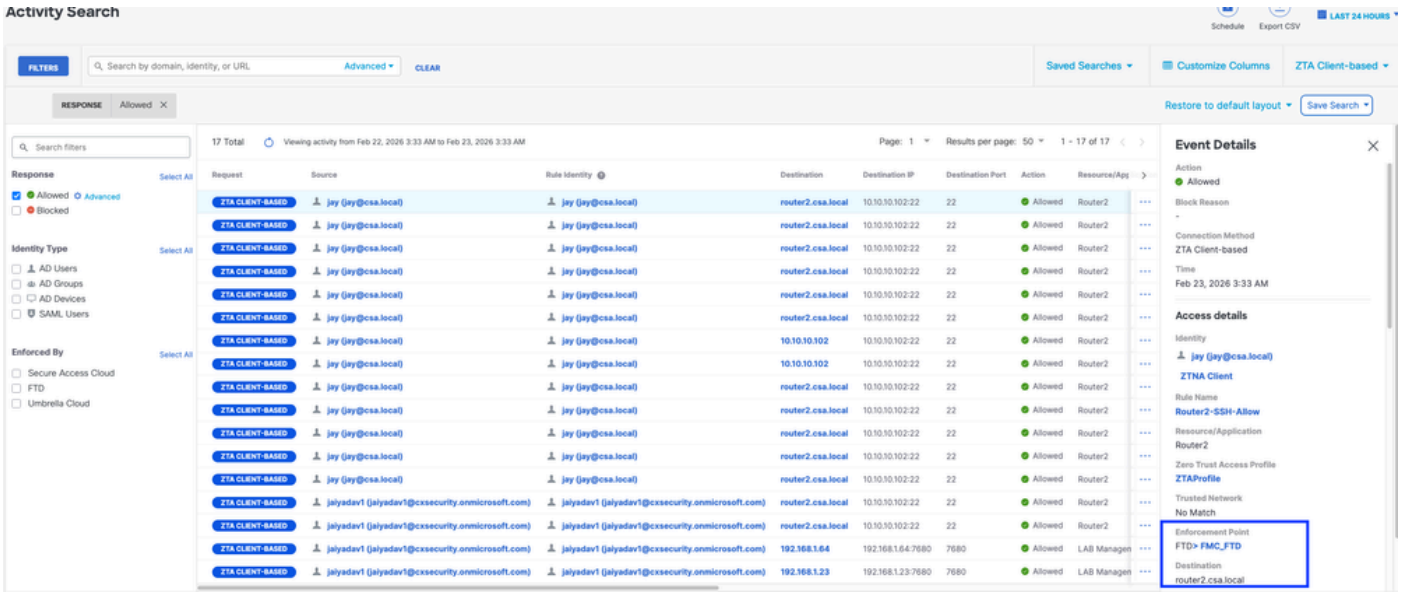


Secure Access - Prueba de relaciones públicas

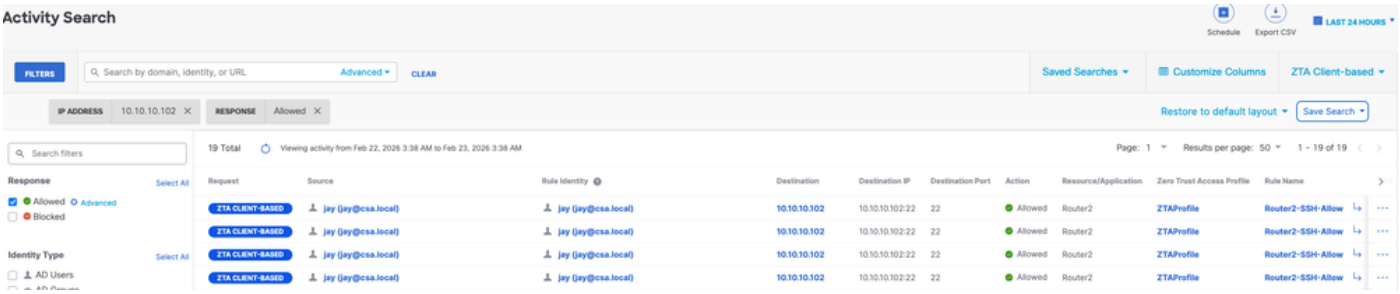
5. Verificar registros de búsqueda de actividad de acceso seguro



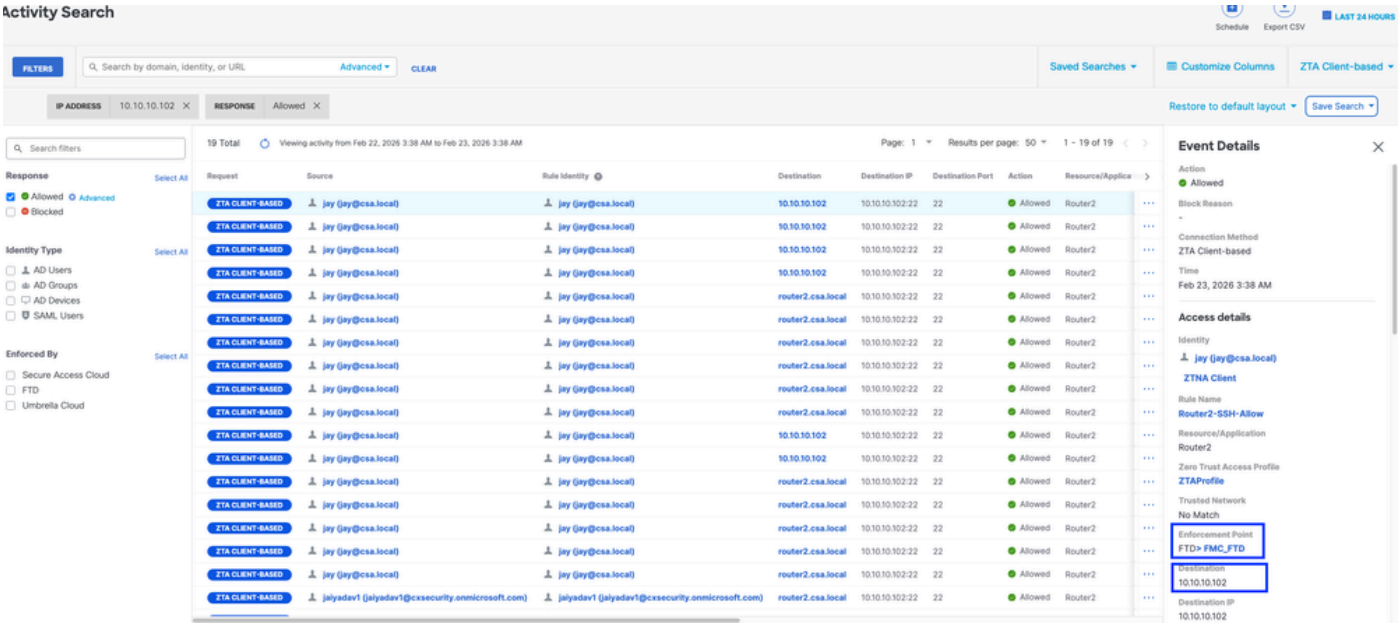
Acceso seguro - Búsqueda de actividad



Acceso seguro - Búsqueda de actividad

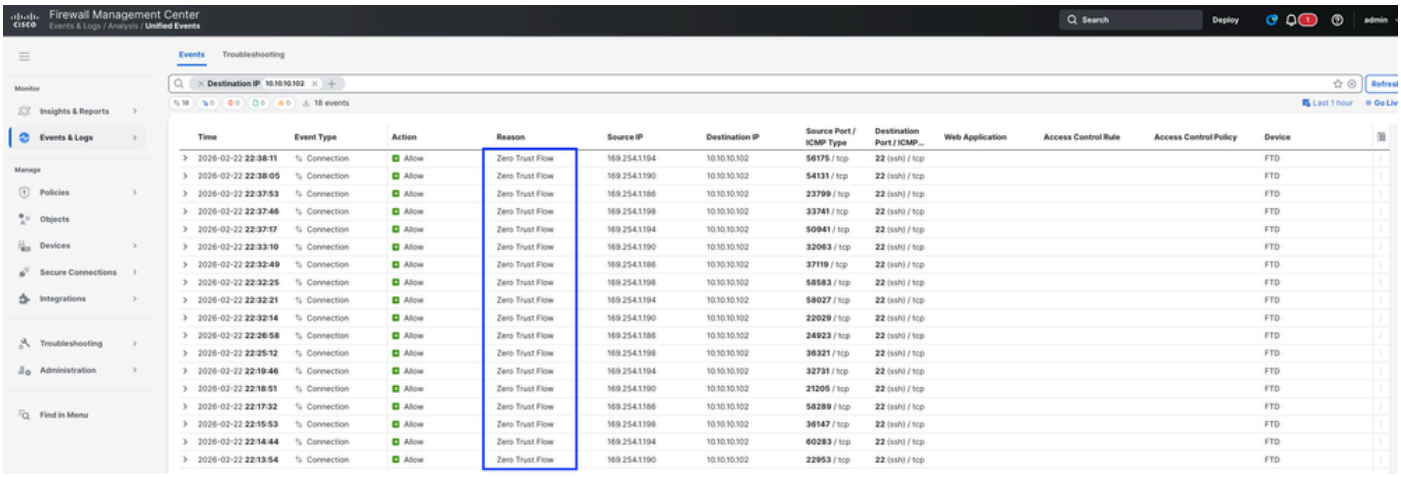


Acceso seguro - Búsqueda de actividad



Acceso seguro - Búsqueda de actividad

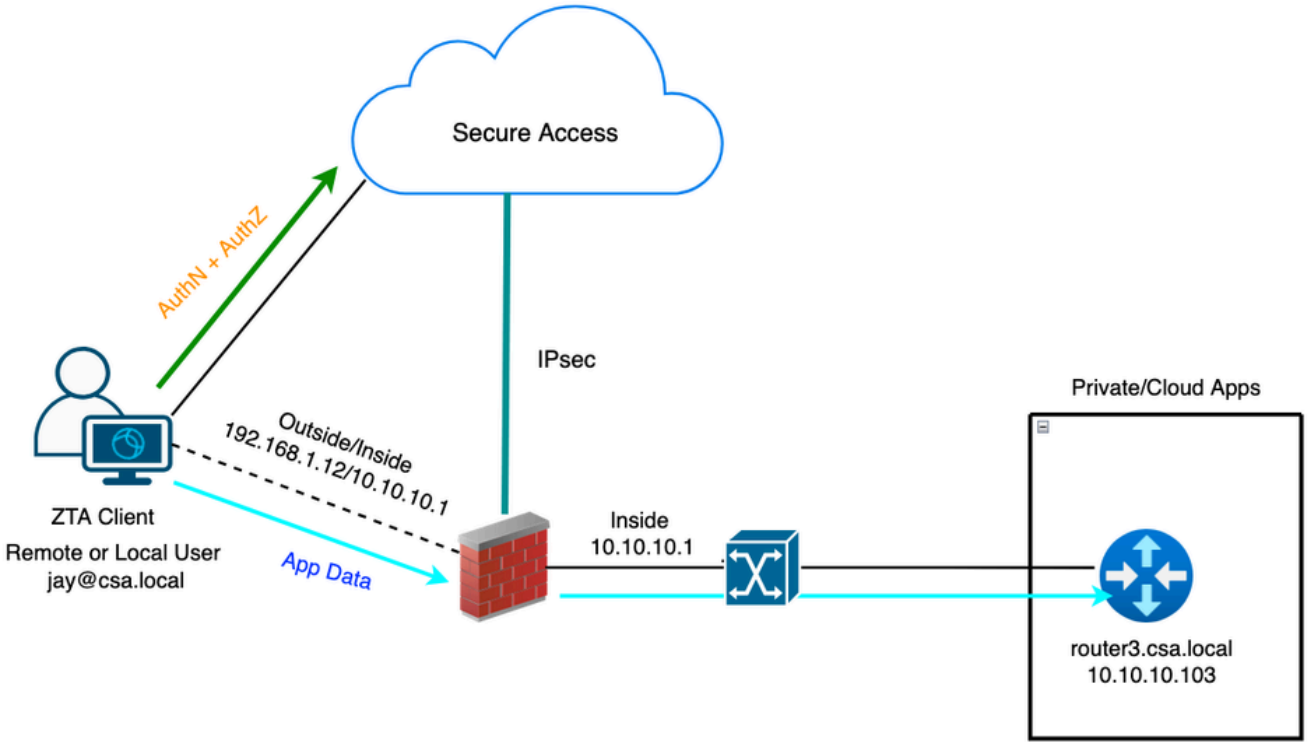
6. Verificar eventos de conexión FMC



Eventos de conexión FMC

Caso de prueba 4: usuario local y remoto; aplicación local o en la nube con TND

En este caso, el tipo de aplicación depende de la ubicación del usuario, si el usuario es local o está detrás de una zona FTD de confianza (dentro, DMZ, etc.), la aplicación sería local (caso de prueba 3). Del mismo modo, si el usuario es remoto, la aplicación sería en la nube (caso de prueba 1). La ubicación del usuario se decidirá en función de la huella dactilar de la red o de la configuración de TND, si la huella dactilar de la red coincide, el nombre local del usuario será Local y si no coincide, el nombre local del usuario se considerará Remoto .

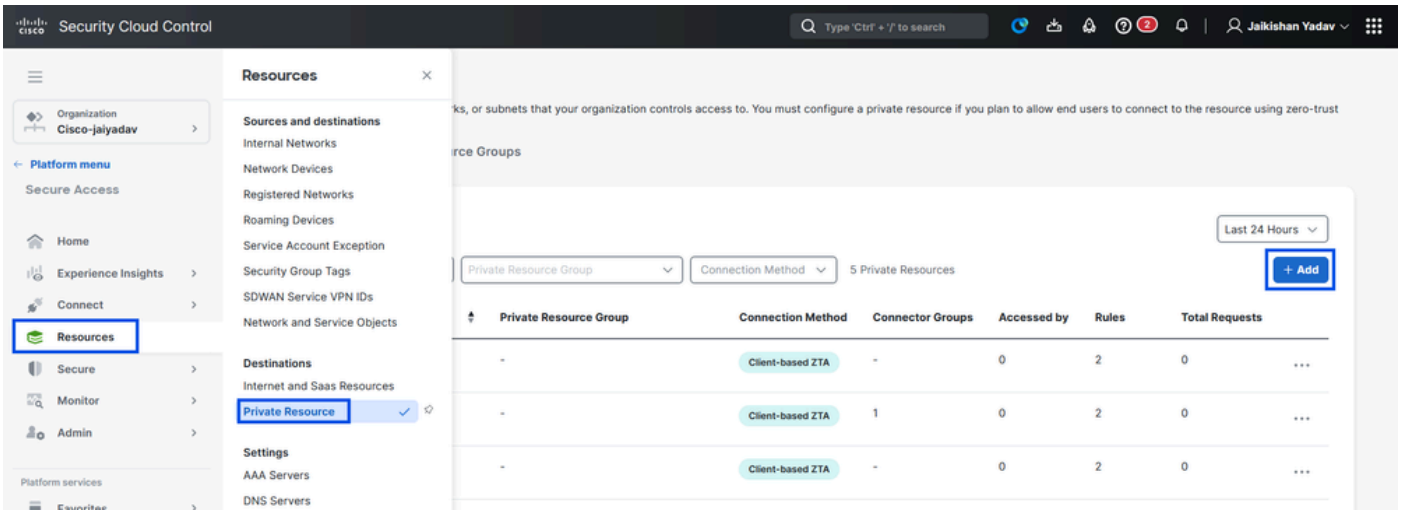


Universal ZTA - Topología de casos de prueba

Paso 1 - Definir un recurso privado en Secure Access

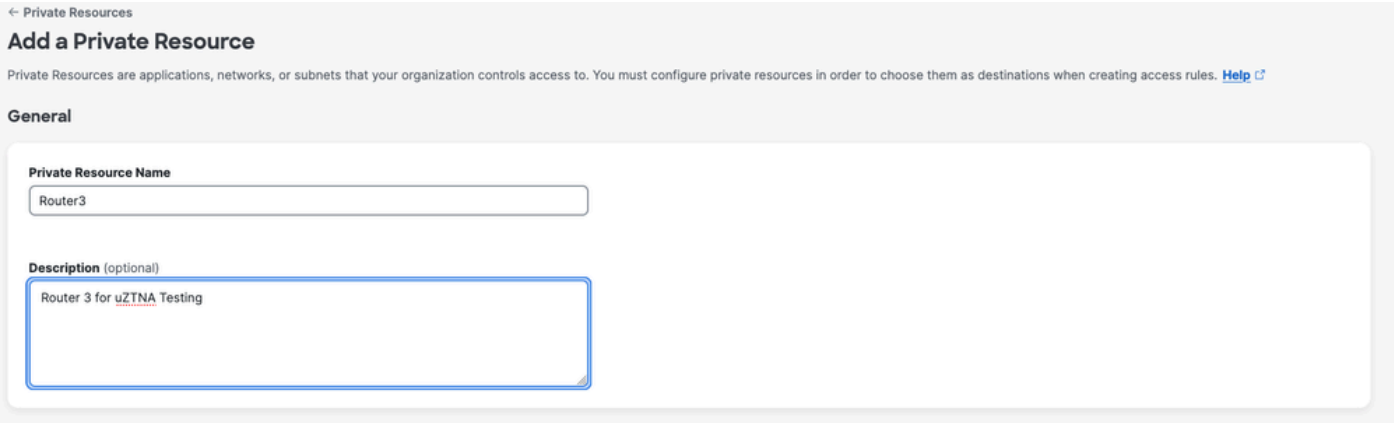
Configure un recurso privado al que se pueda acceder a través del dispositivo inscrito de acceso de confianza cero (ZTA) con aplicación en la nube

1. Navegue hasta Recursos > Destinos > Recursos privados > Haga clic en +Agregar



Acceso seguro - Configuración de recursos privados

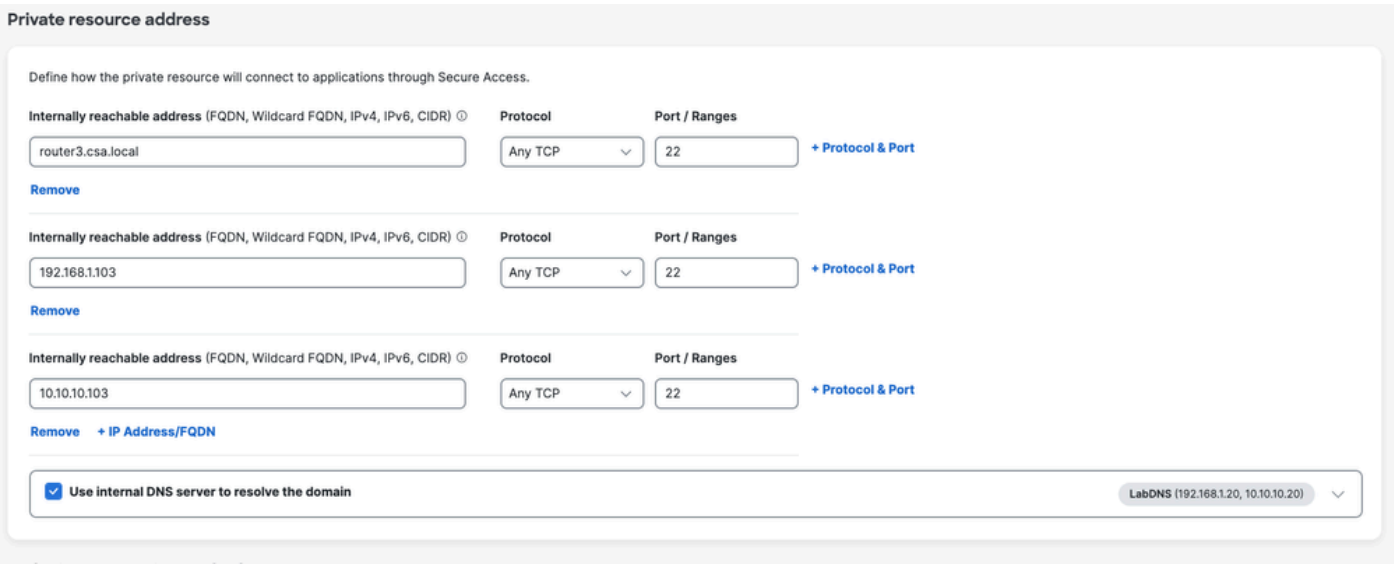
2. En Nombre de Recurso Privado, introduzca un nombre significativo para el recurso. Para Descripción, se recomienda proporcionar información como el propósito del recurso o el nombre del propietario del recurso.



Acceso seguro - Configuración de recursos privados

3. Introduzca el FQDN del recurso privado al que desea acceder . También podemos definir la dirección IP del recurso privado . Para obtener más información, vea Agregar un recurso privado

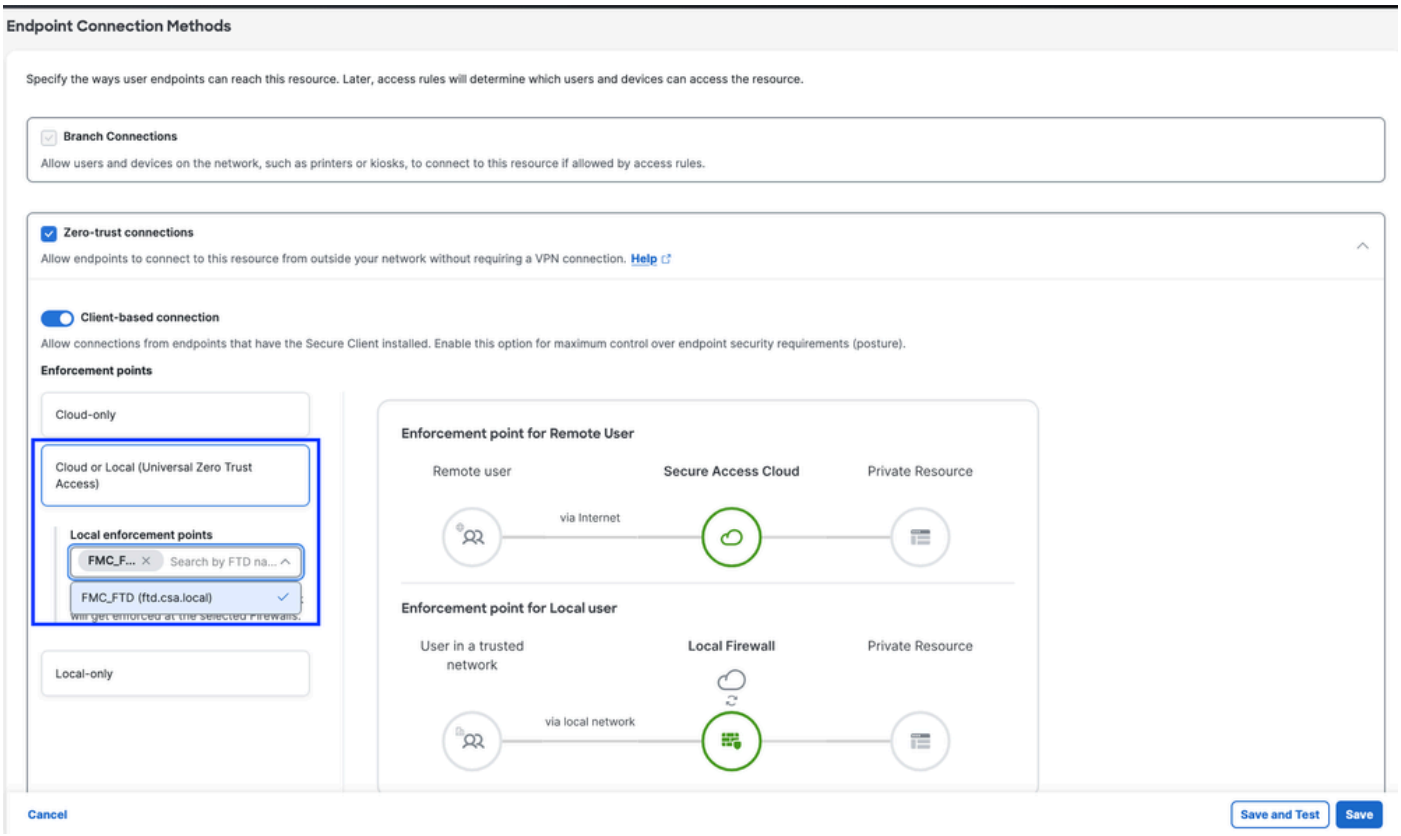
4. Seleccione el servidor DNS para resolver el dominio



Acceso seguro - Configuración de recursos privados

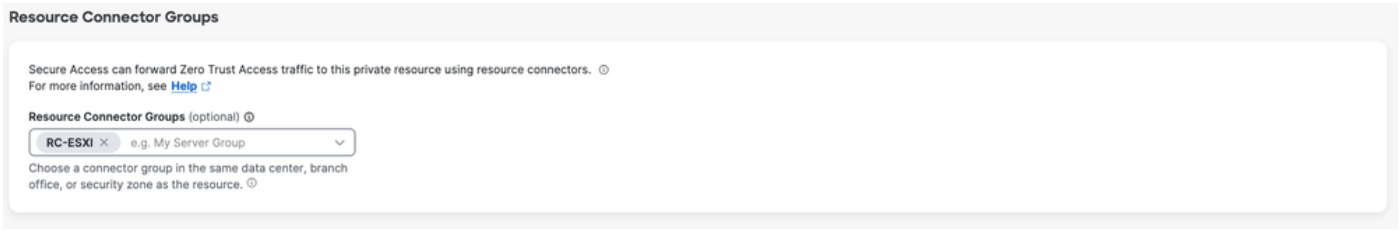
5. Seleccionar métodos de conexión de terminales

6. Seleccione FTD como puntos de aplicación locales



Acceso seguro - Configuración de recursos privados

Seleccione RC si se puede acceder al recurso privado a través de RC; de lo contrario, déjelo en blanco si se puede acceder al recurso privado a través del grupo de túnel de red (túnel IPsec).



Acceso seguro - Configuración de recursos privados

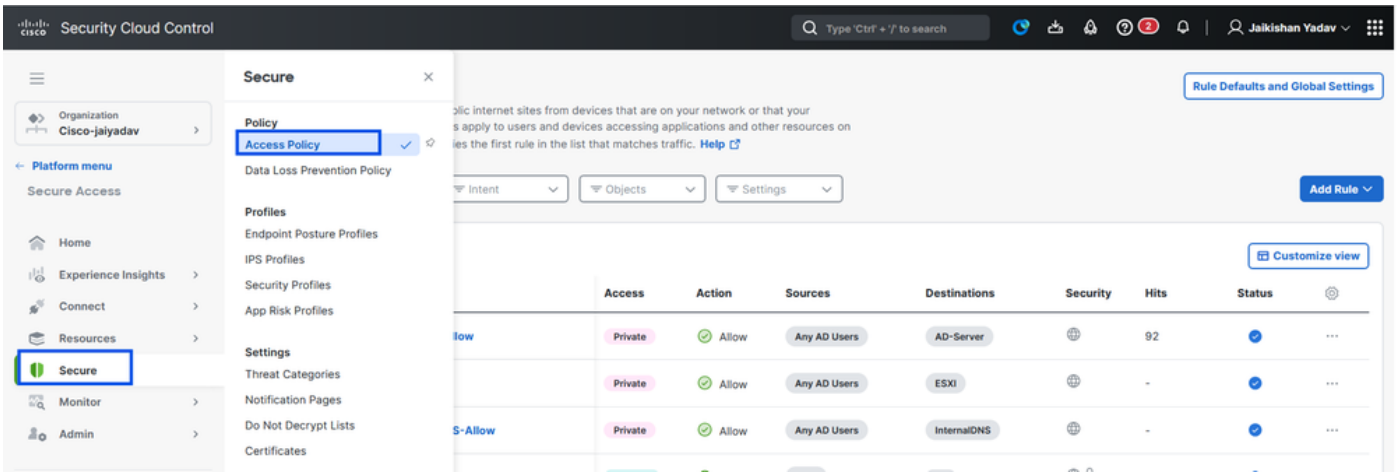
Nota: En función del tipo de inscripción que seleccione, este cambio asociará automáticamente el PR al FTD y activará una implementación de políticas

7. Haga clic en Save (Guardar).

Paso 2: Crear regla de acceso privado

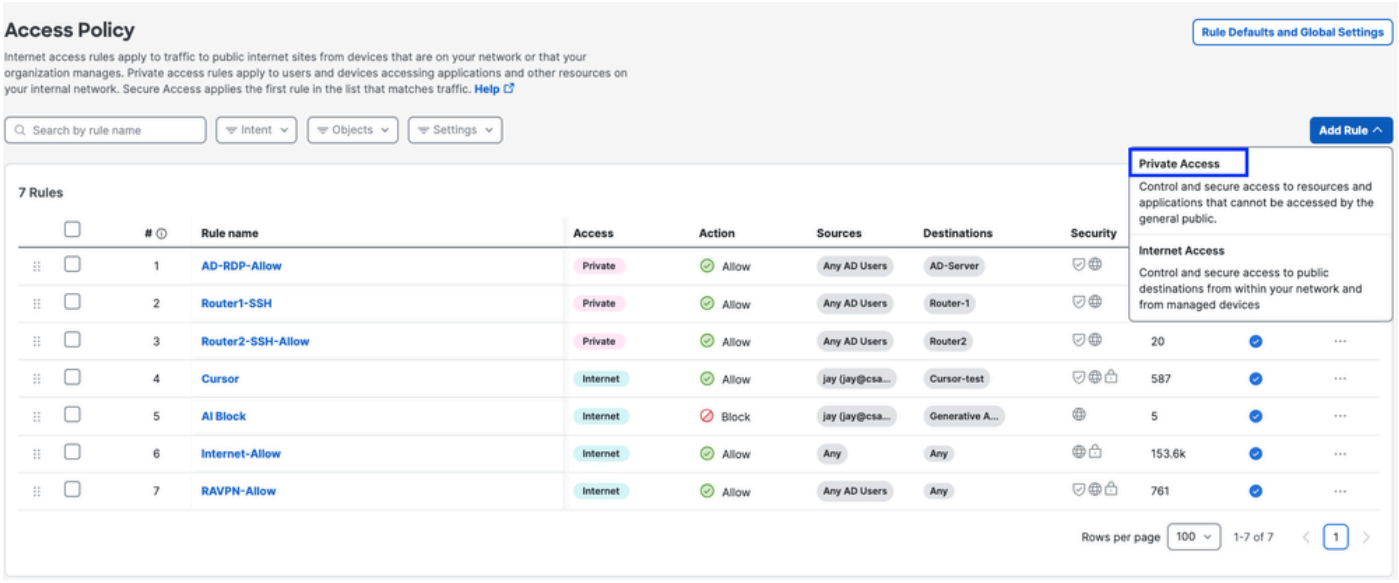
Configure un acceso privado en Secure Access para que los usuarios inscritos en Universal ZTA puedan acceder . Para obtener más información, vea Regla de acceso privado

1. Vaya a Seguro > Política de acceso



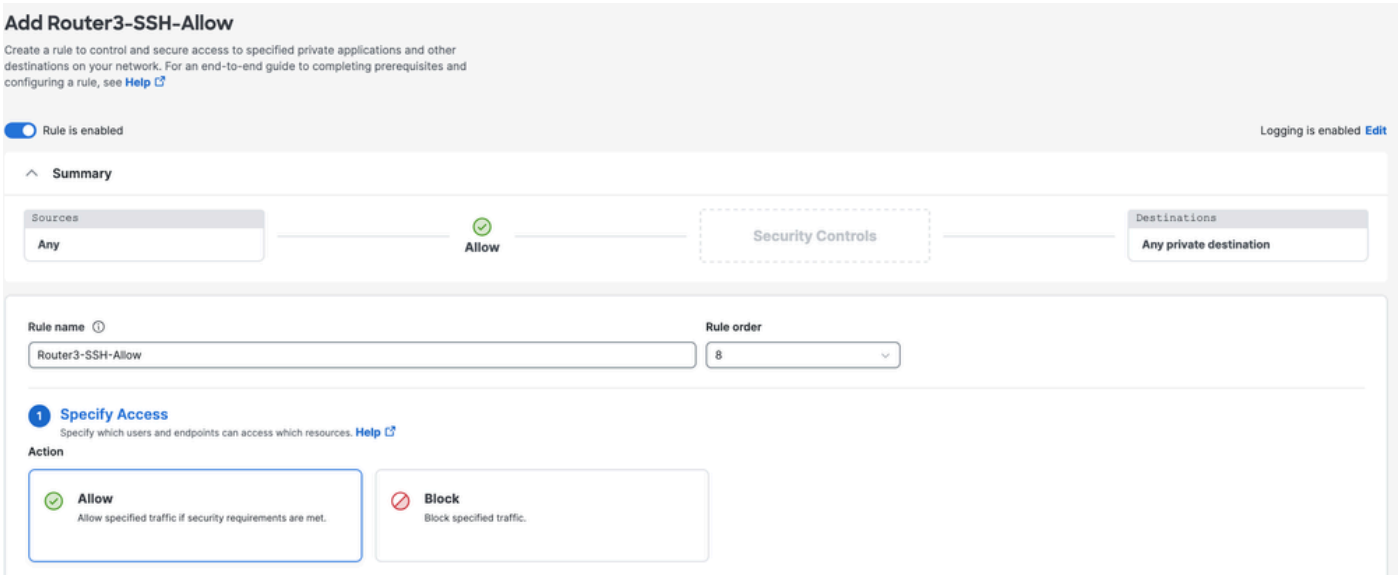
Acceso seguro - Configuración de la política de acceso

2. Haga clic en Agregar regla, y luego elija Acceso privado.
En la parte superior de la regla hay un resumen que describe los componentes configurados de la regla.



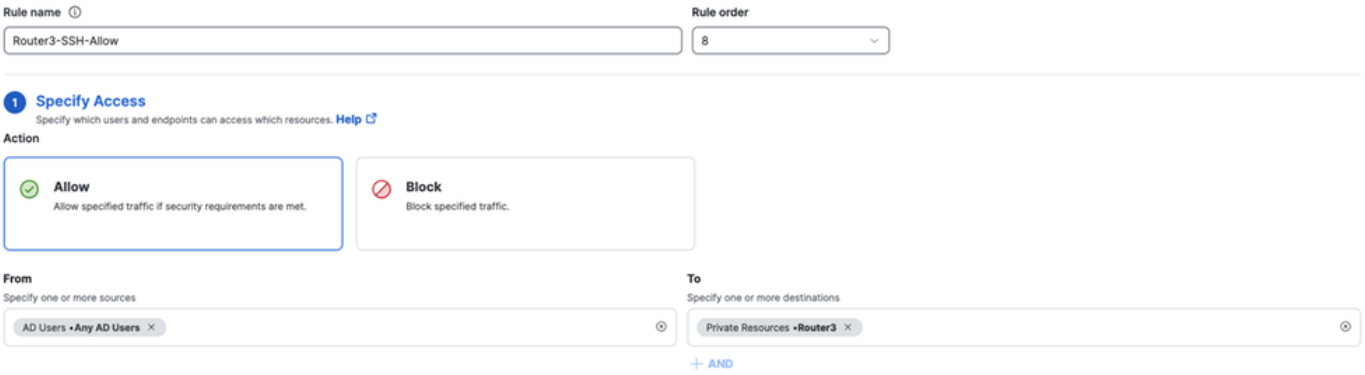
Acceso seguro - Configuración de la política de acceso

3. Agregar un nombre de regla



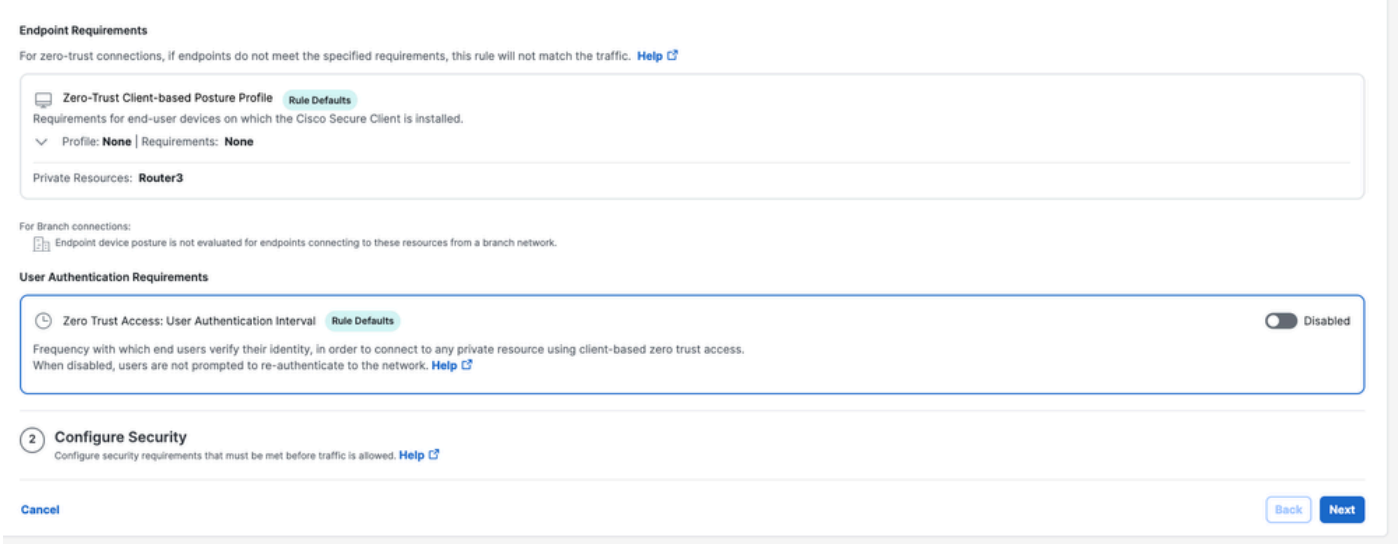
Acceso seguro - Configuración de la política de acceso

4. Seleccione la acción de regla y seleccione origen y destino



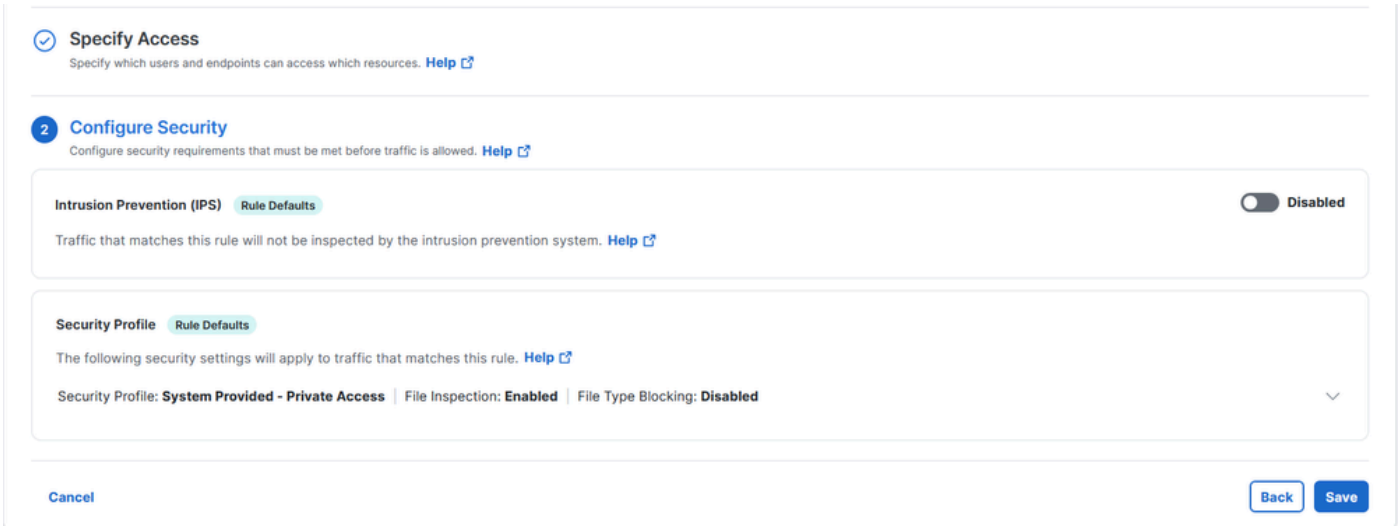
Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales



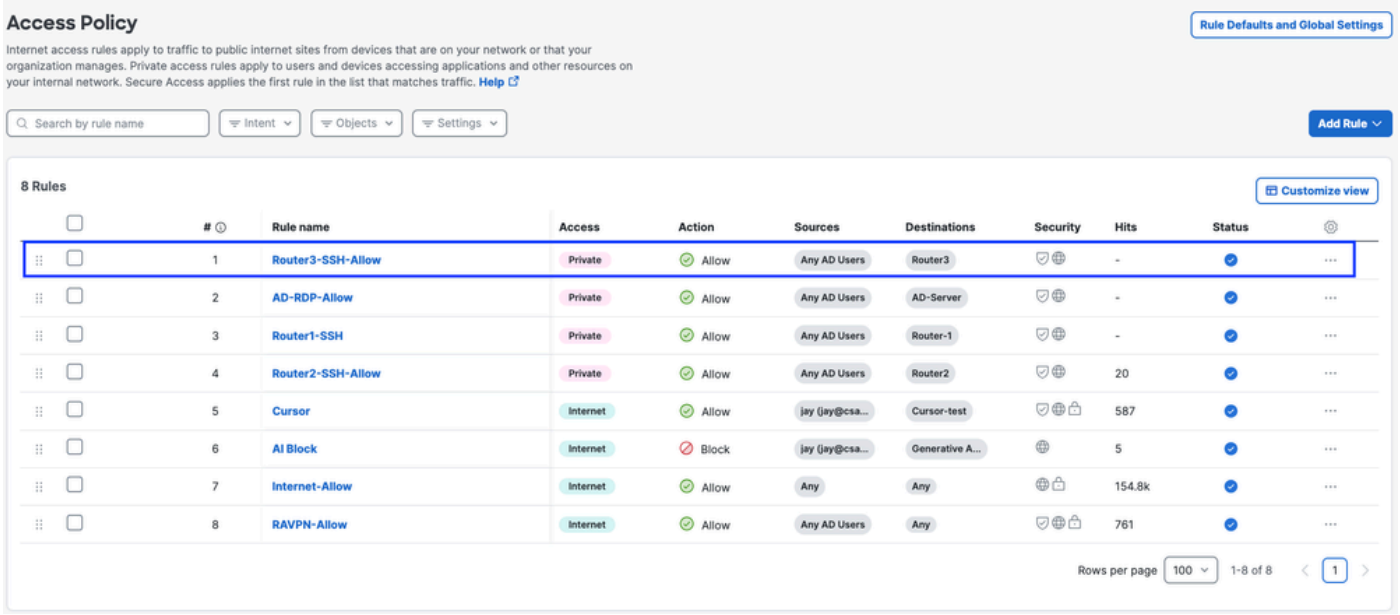
Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad



Acceso seguro - Configuración de la política de acceso

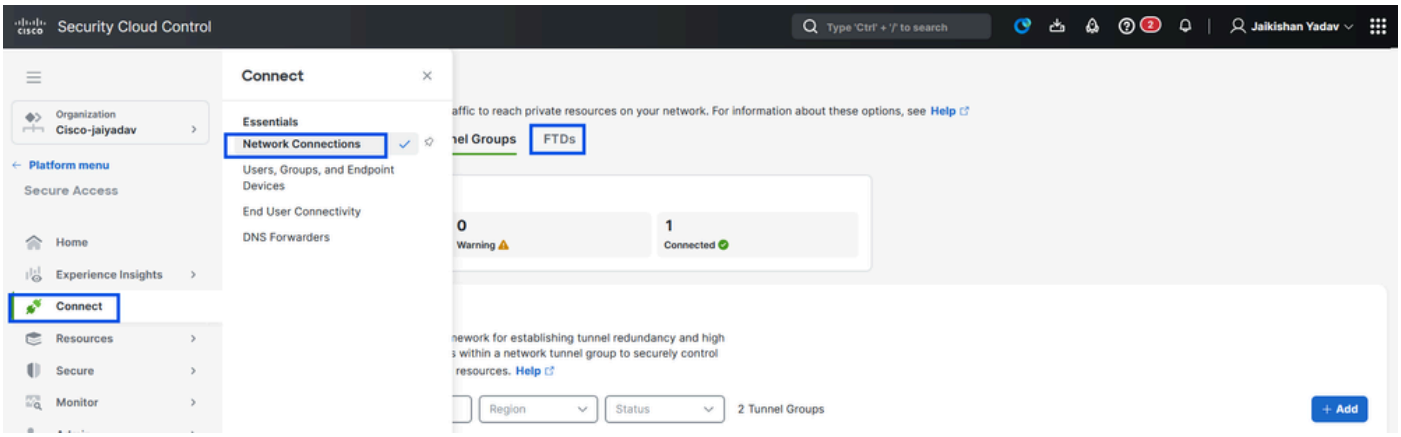
7. Haga clic en Guardar



Acceso seguro - Configuración de la política de acceso

Paso 3 - Verificar la asociación de RP en el FTD

1. Vaya a connect > Network Connections > FTDs

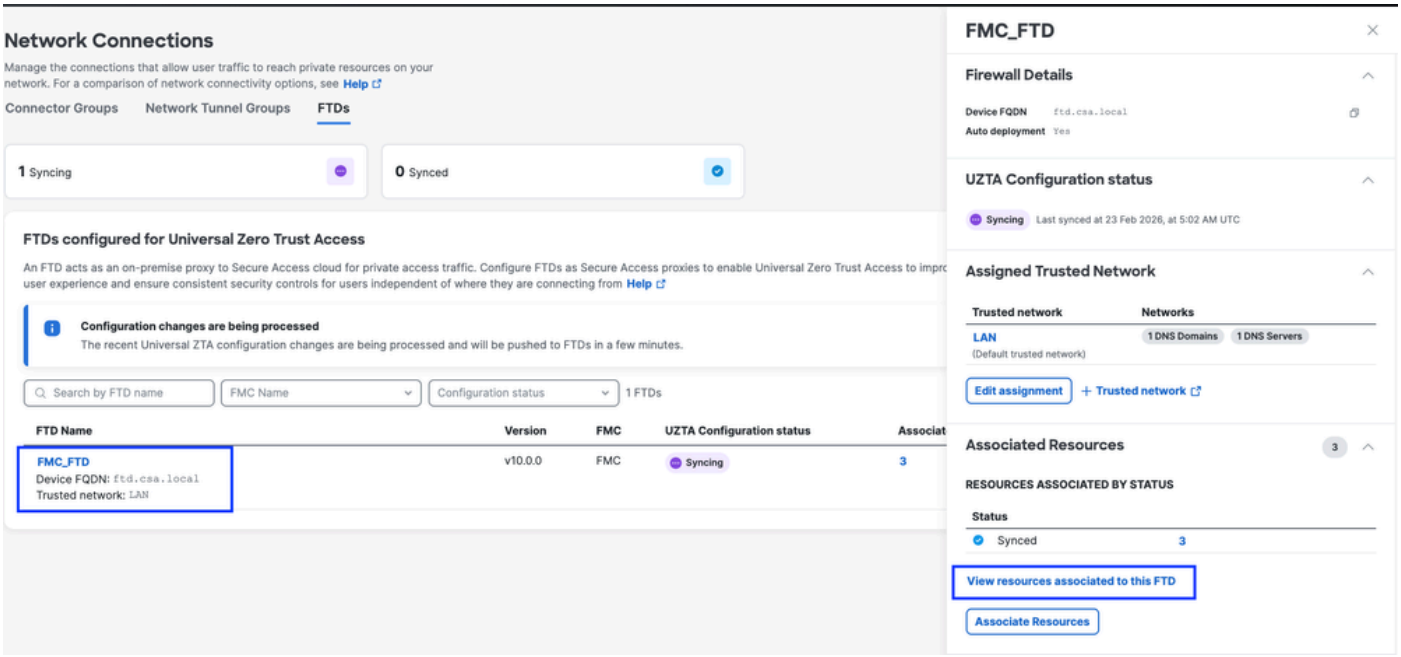


Acceso seguro - Verificación de relaciones públicas

2. Haga clic en el FTD > Ver recursos asociados a este FTD

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

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server:  AD.csa.local
Address:  192.168.1.20

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

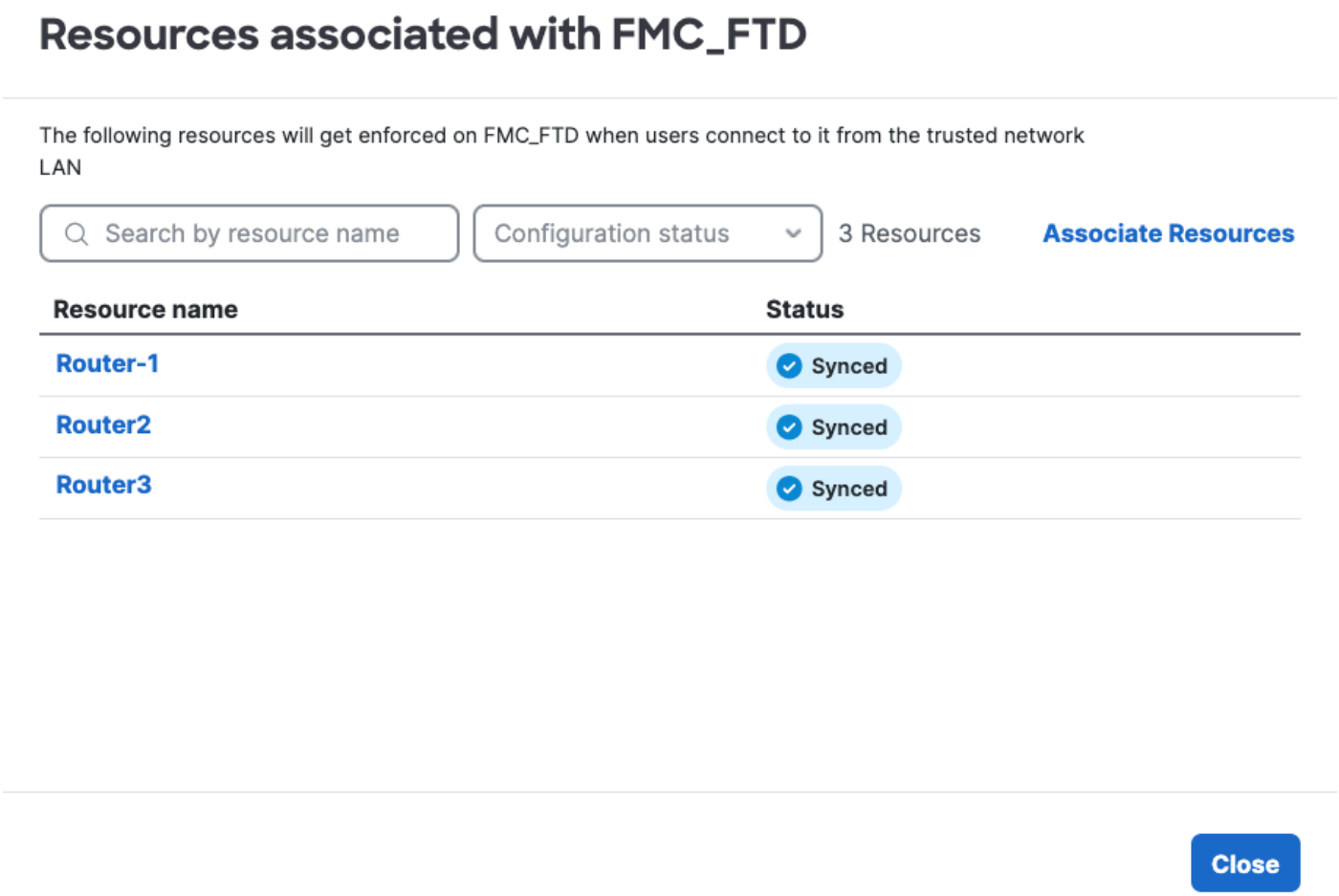
Acceso seguro - Verificación de relaciones públicas



Acceso seguro - Verificación de relaciones públicas

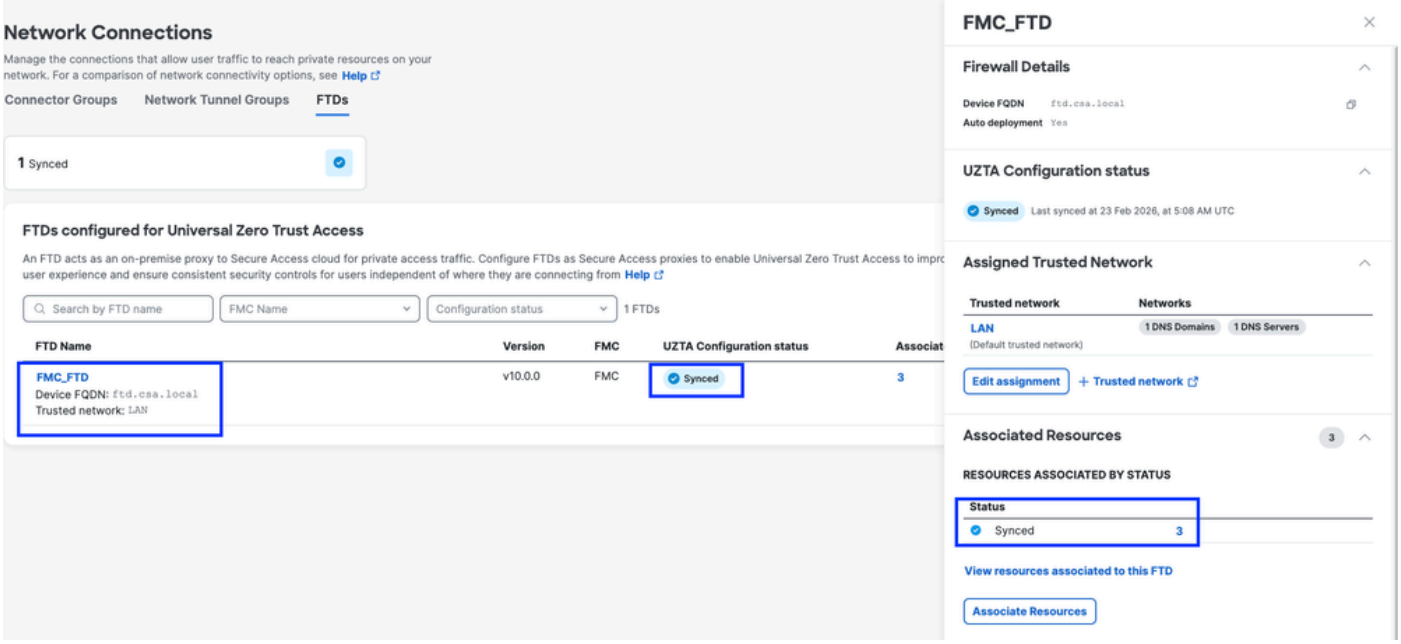
```
C:\Users\jay>ping ftd.csa.local

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
```

Acceso seguro - Verificación de relaciones públicas



3. Haga clic en Close (Cerrar)

4. Verifique el estado , el recurso asociado y la configuración deben estar en el estado Sincronizado



Acceso seguro - Verificación de relaciones públicas

5. Compruebe que la configuración se ha enviado al FTD

Inicie sesión en FTD cli y navegue hasta el modo LINA

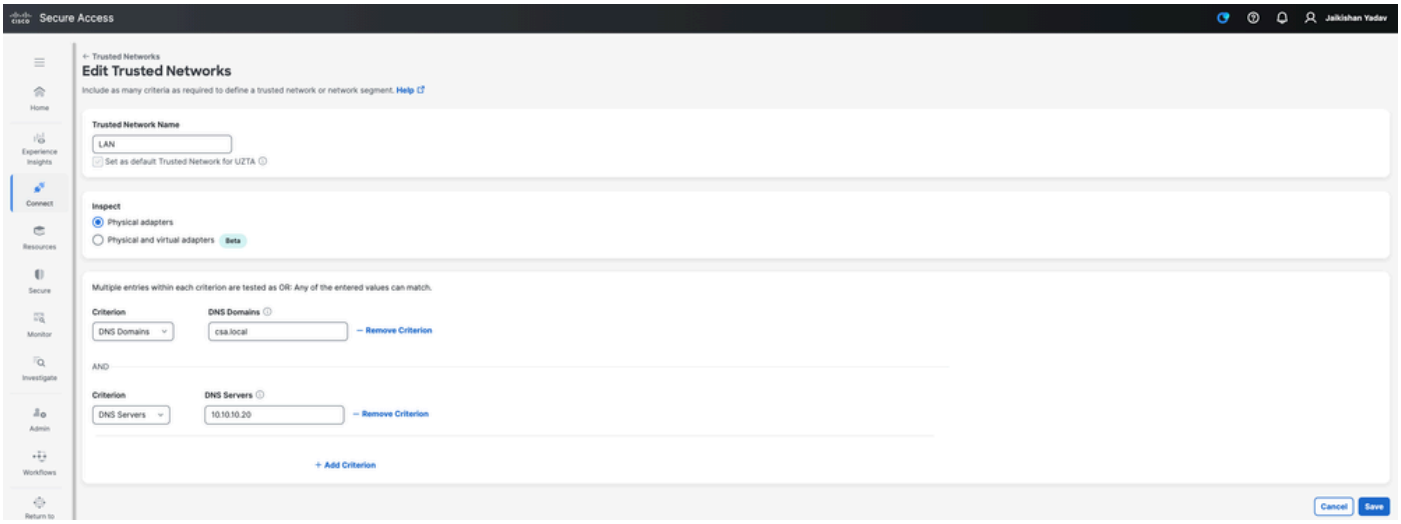
show running-config object application

```
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
```

Acceso seguro - Verificación de relaciones públicas

Paso - 4 Configurar o verificar " Administrar redes de confianza o configuración ZTA"

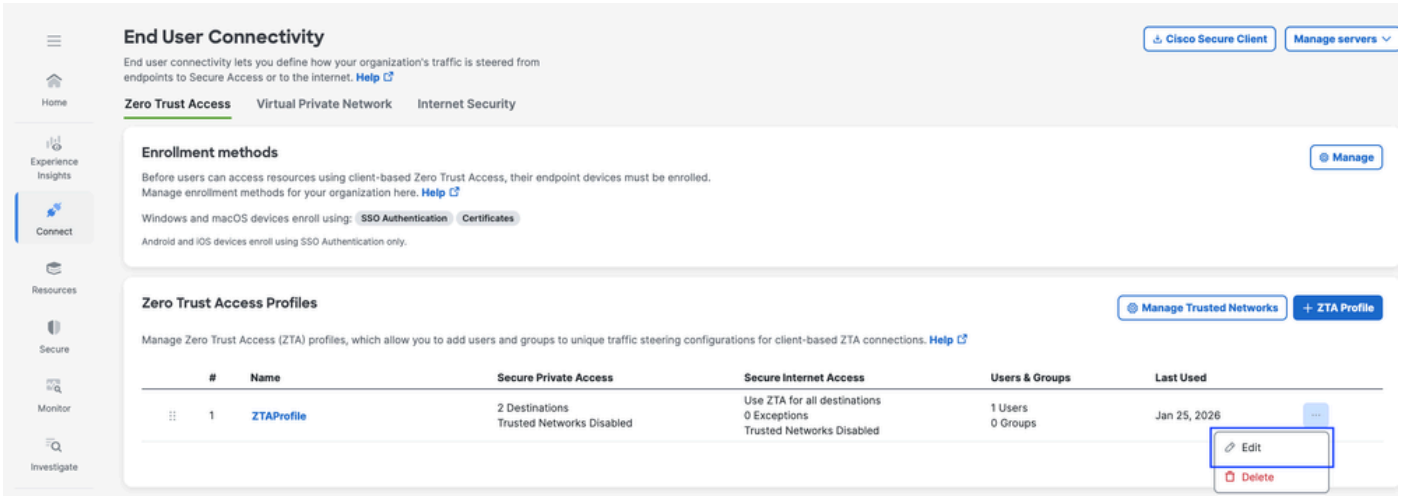
Vaya a Connect > End User Connectivity > Zero Trust Access > ZTA Settings y configure Trusted Networks



Acceso seguro - Configuración de ZTA TND

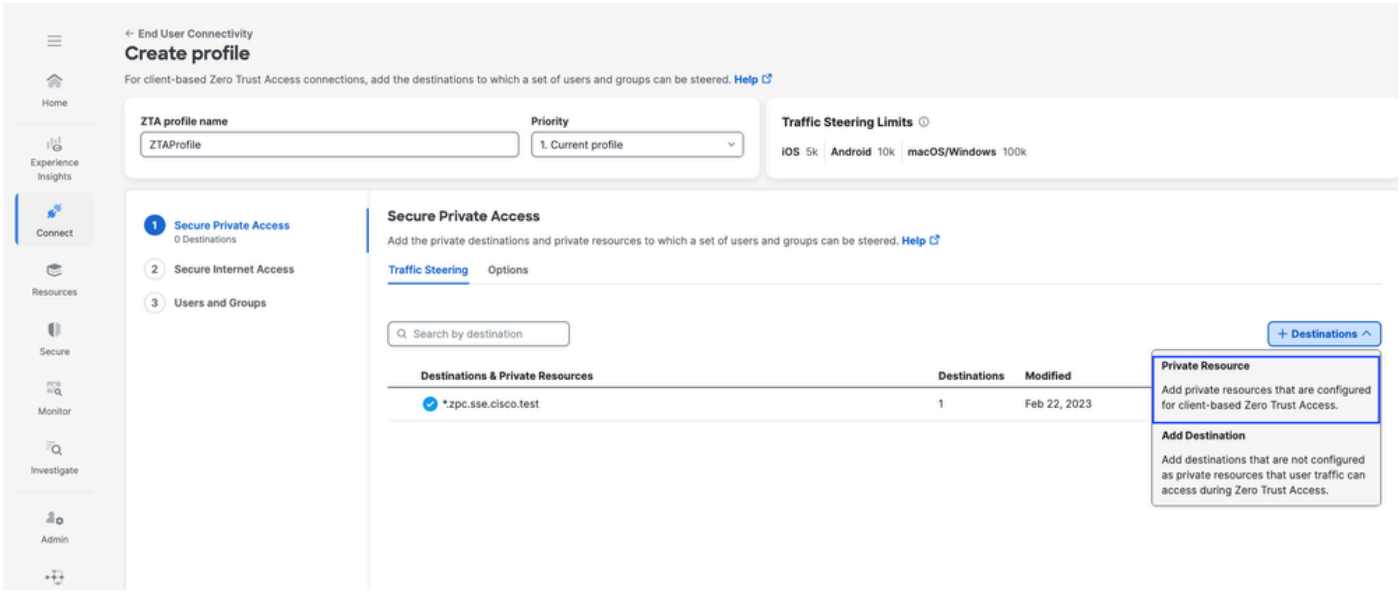
Paso - 5 Agregar un recurso privado al perfil ZTA

1. Navegue hasta Conexión > Conectividad del usuario final > Acceso de confianza cero y haga clic en 3 puntos para editar el perfil ZTA

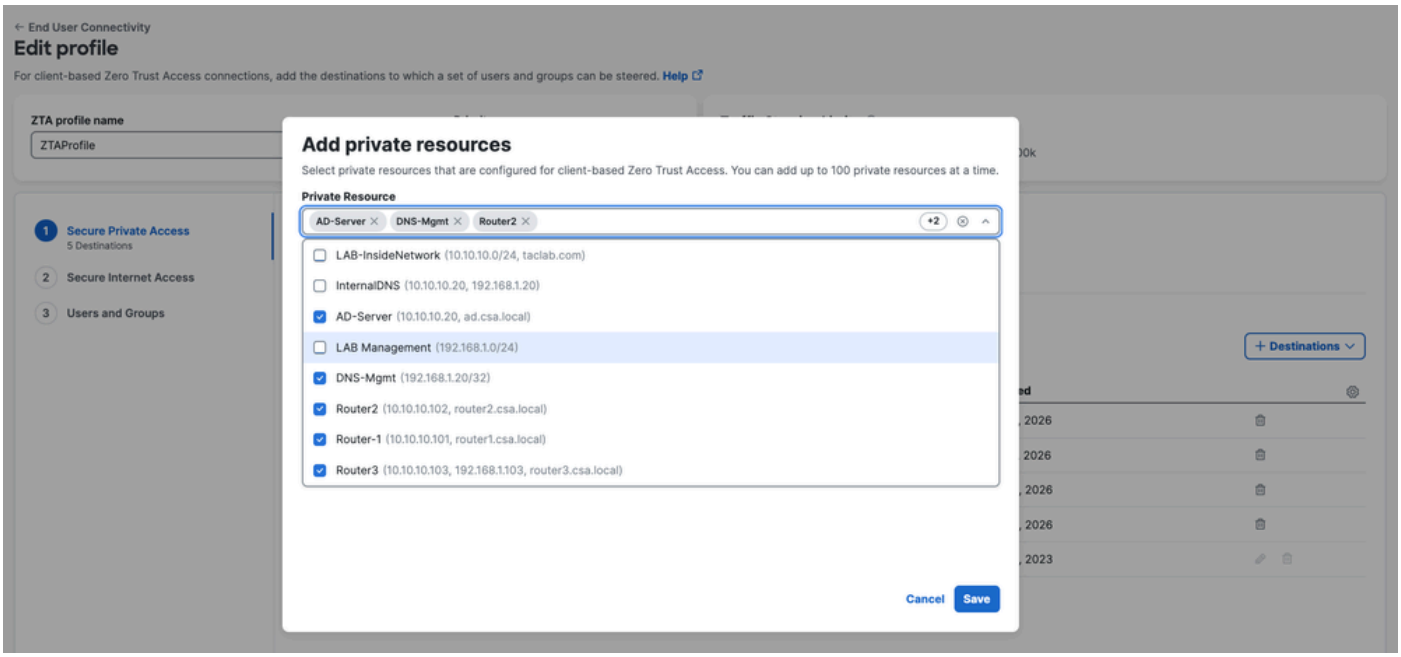


Acceso seguro - Perfil ZTA

2. Añada el recurso privado

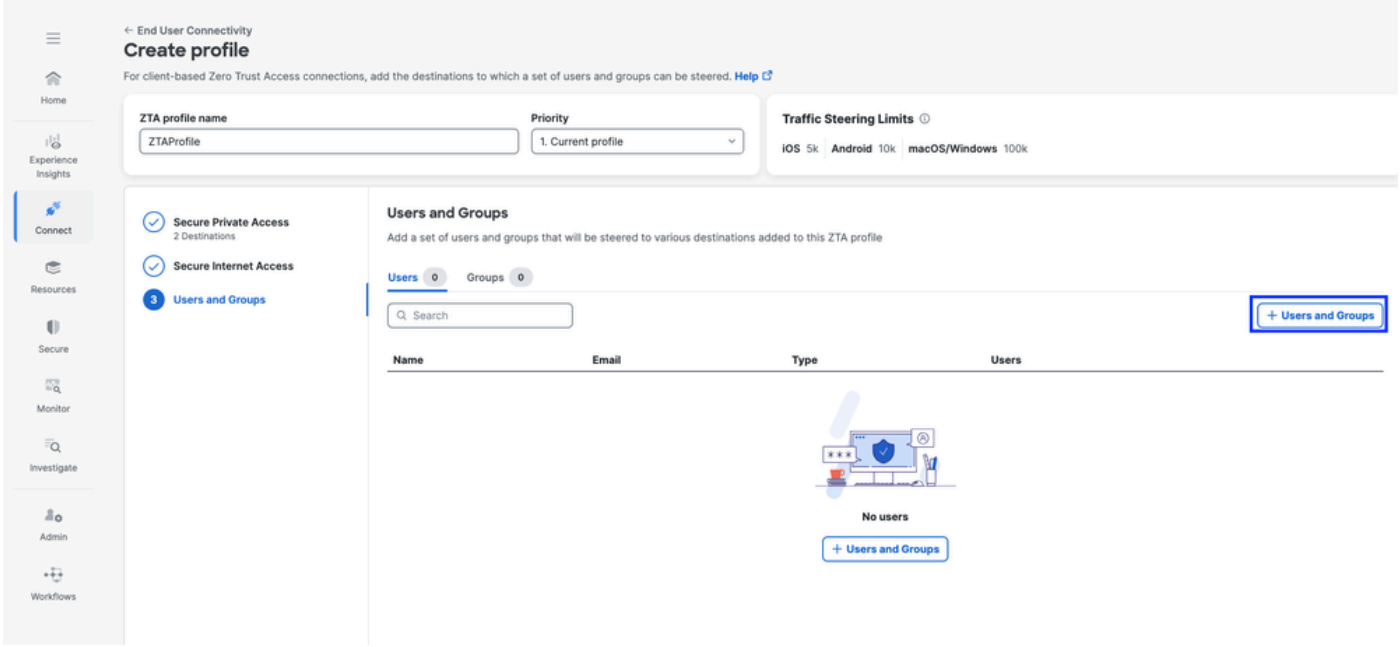


Acceso seguro - Perfil ZTA

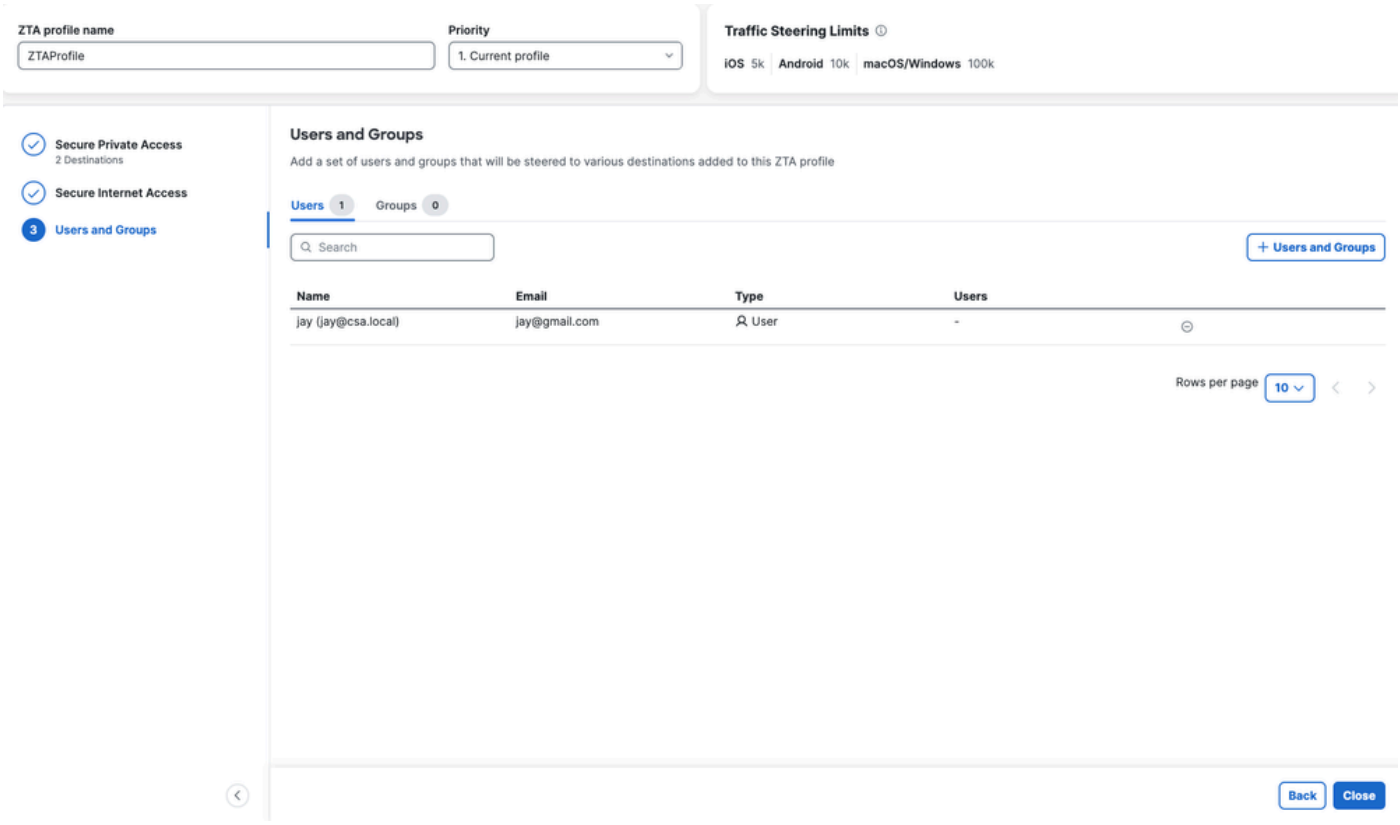


Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos



Acceso seguro - Perfil ZTA

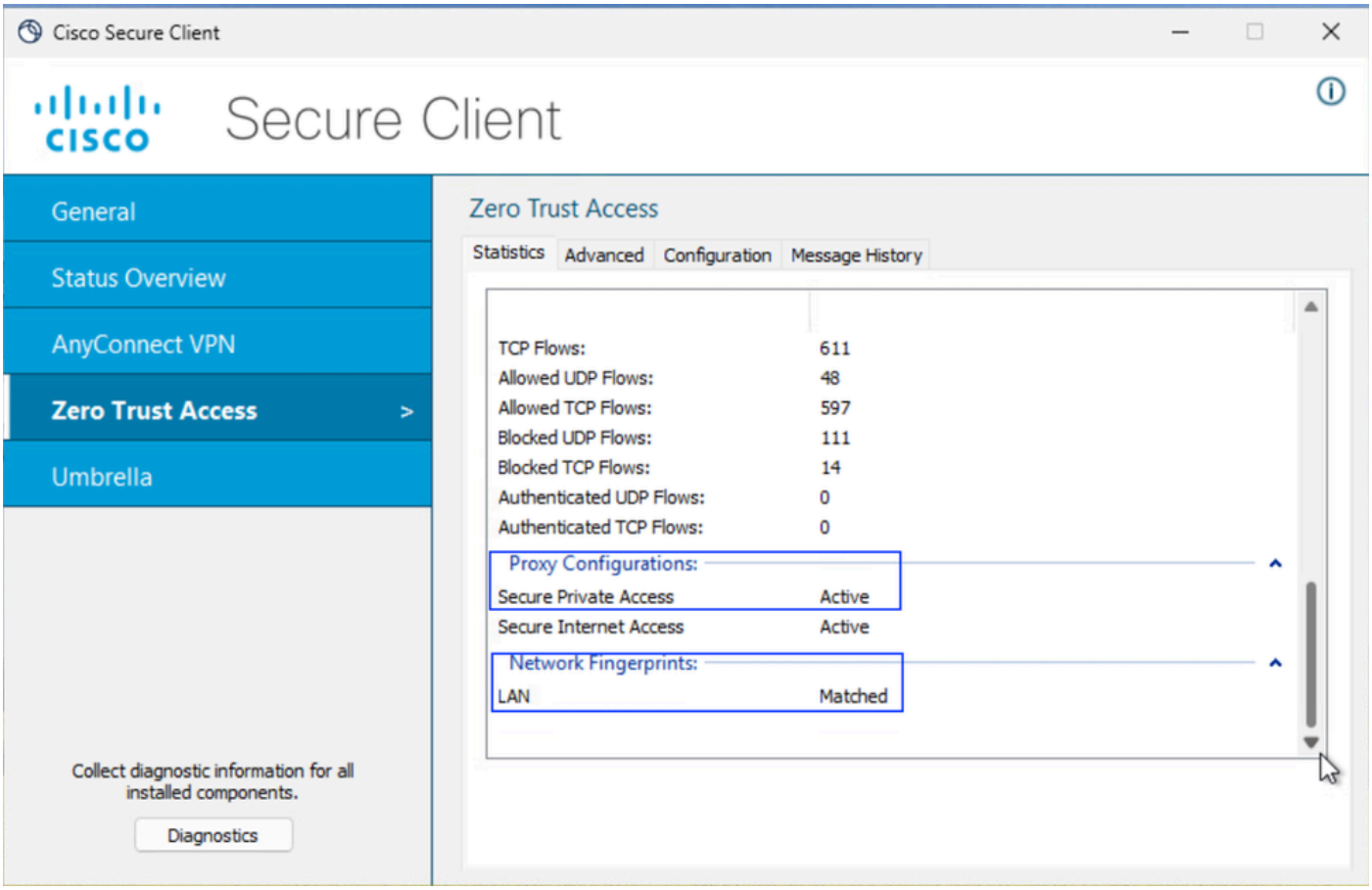


Acceso seguro - Perfil ZTA

Paso - 6 Verificar el acceso al recurso privado

Cuando el usuario es local

1. Verifique la huella dactilar de la red para ZTA TND, debe coincidir si el usuario es local y el acceso privado seguro debe estar activo



Secure Access - Prueba de relaciones públicas

2. Compruebe que el usuario remoto puede resolver el FQDN del FTD

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

Pinging ftd.csa.local [10.10.10.1] with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\jay>nslookup ftd.csa.local
Server:  AD.csa.local
Address:  10.10.10.20

Name:    ftd.csa.local
Addresses:  10.10.10.1
```

Secure Access - Prueba de relaciones públicas

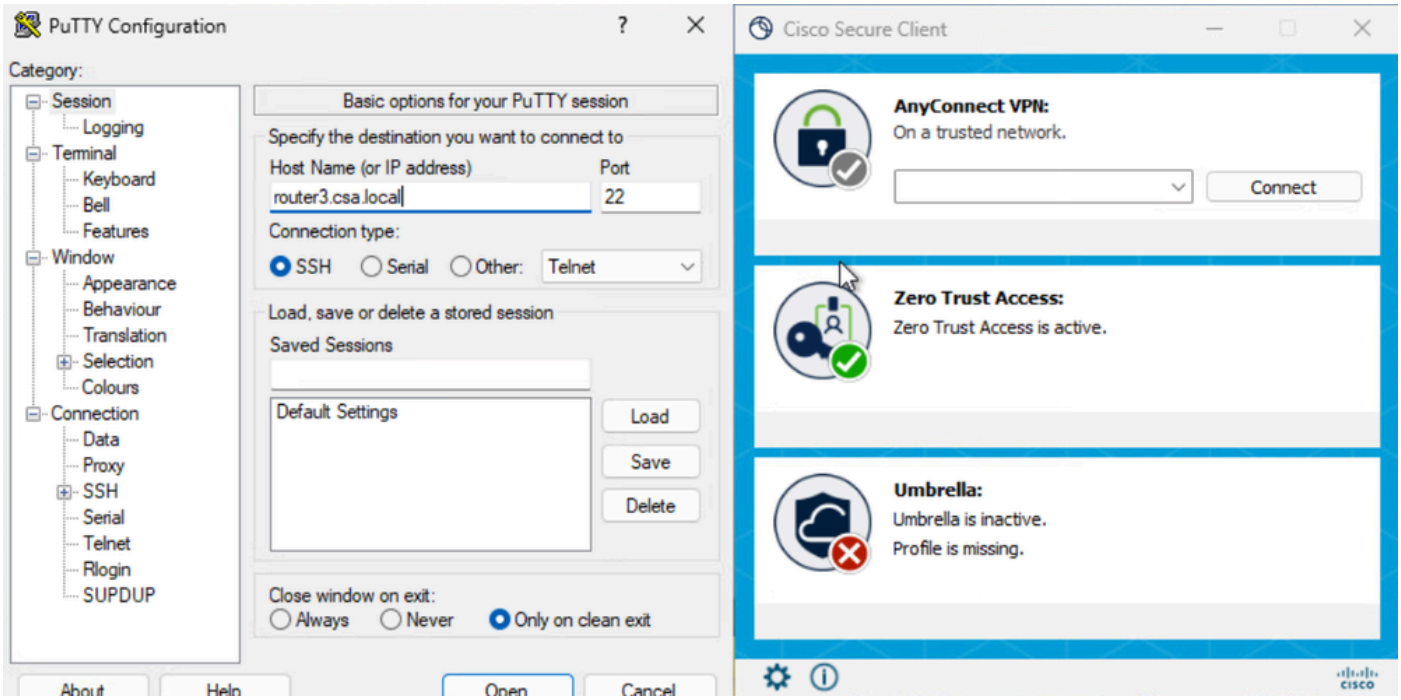
3. Compruebe que FTD puede alcanzar un recurso privado mediante FQDN

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

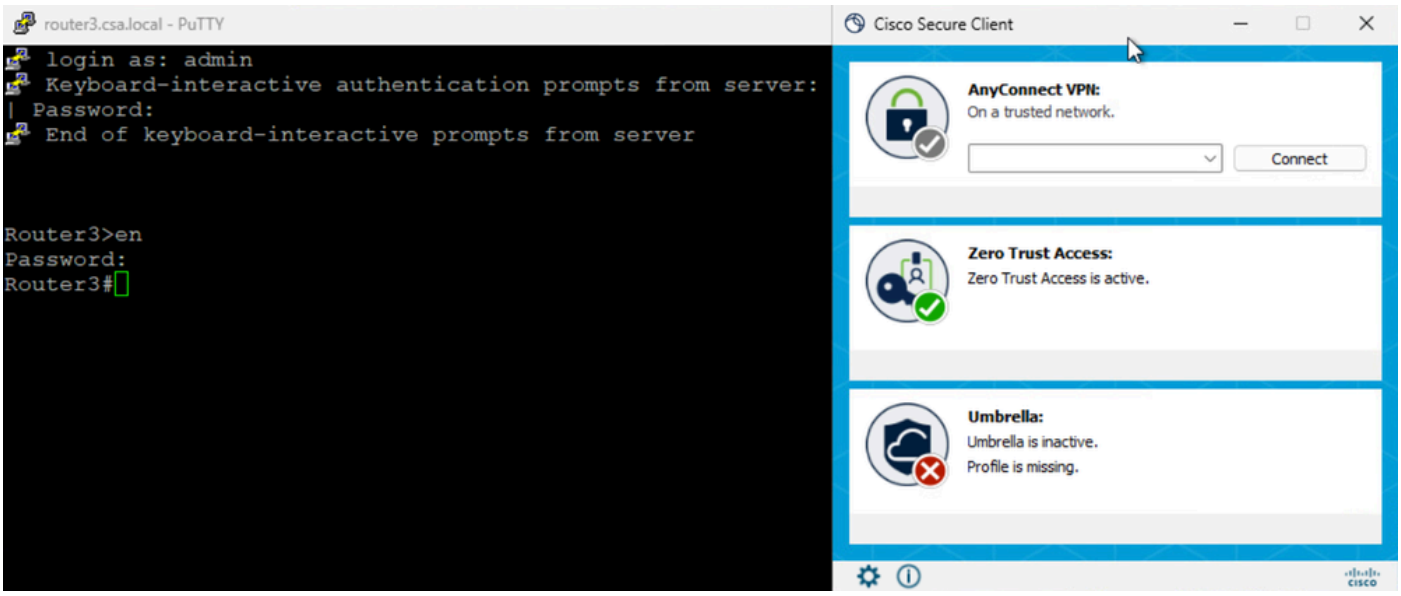
Secure Access - Prueba de relaciones públicas

4. Pruebe la conexión SSH al recurso privado

Acceso al PR mediante FQDN

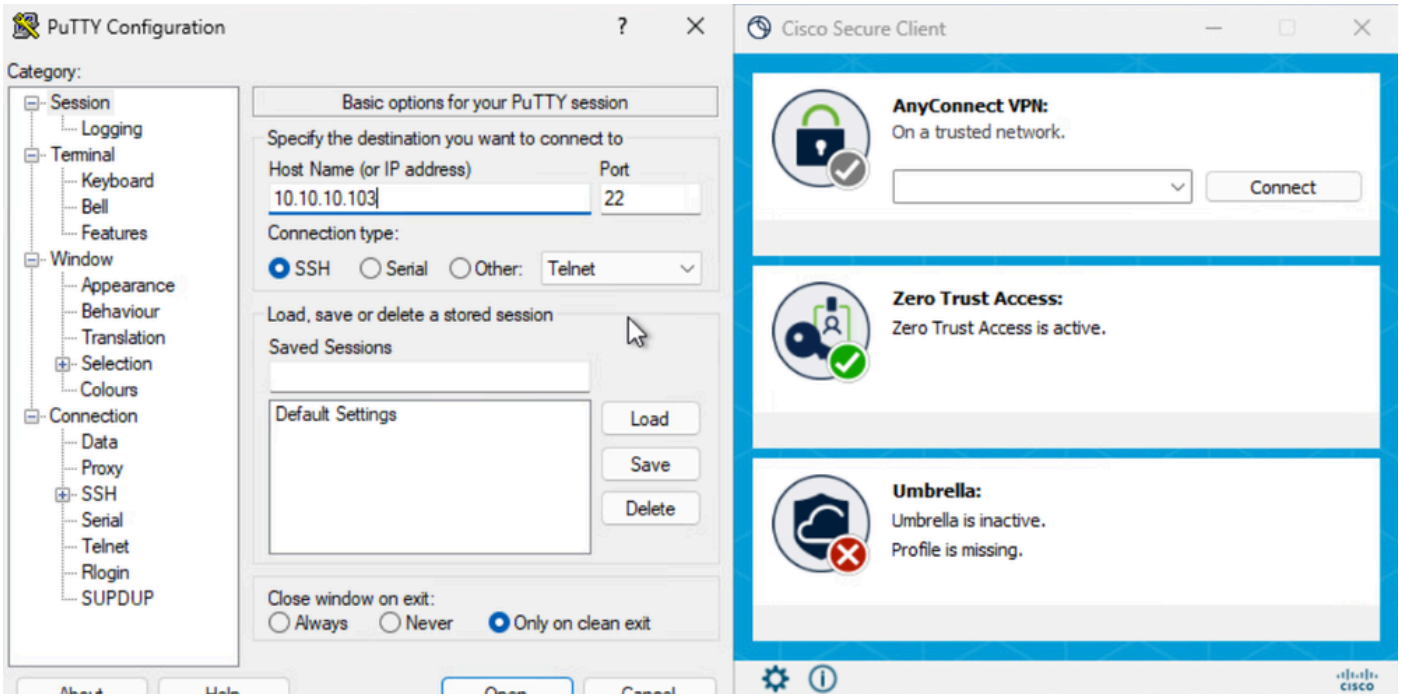


Secure Access - Prueba de relaciones públicas

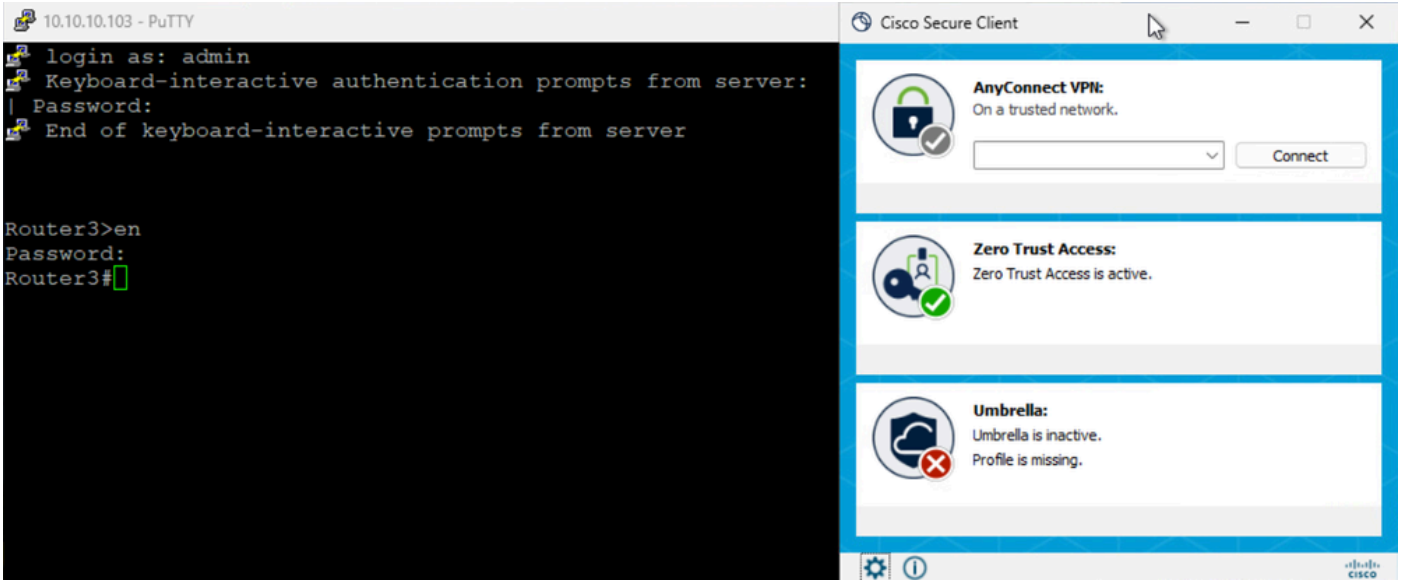


Secure Access - Prueba de relaciones públicas

Acceso al PR mediante la dirección IP

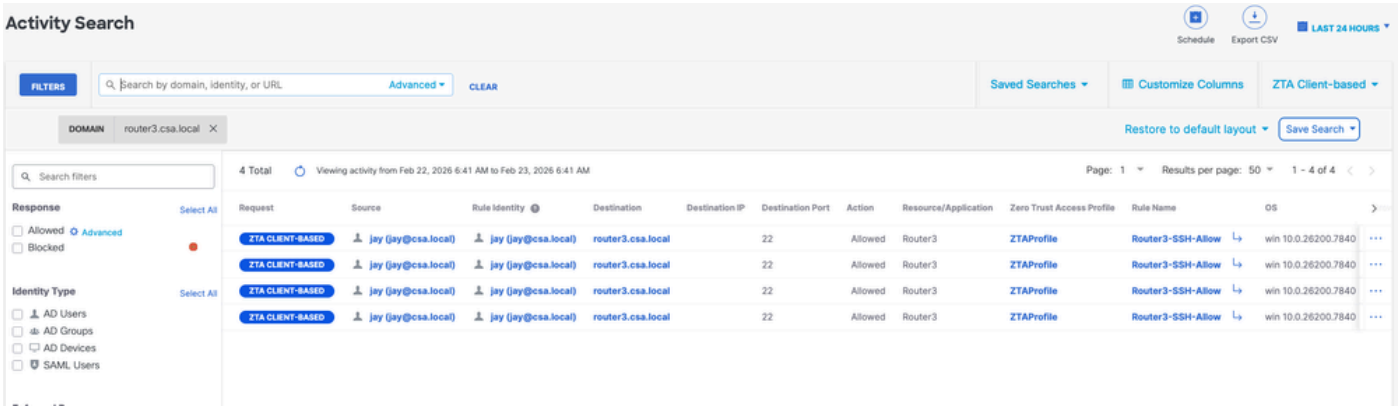


Secure Access - Prueba de relaciones públicas

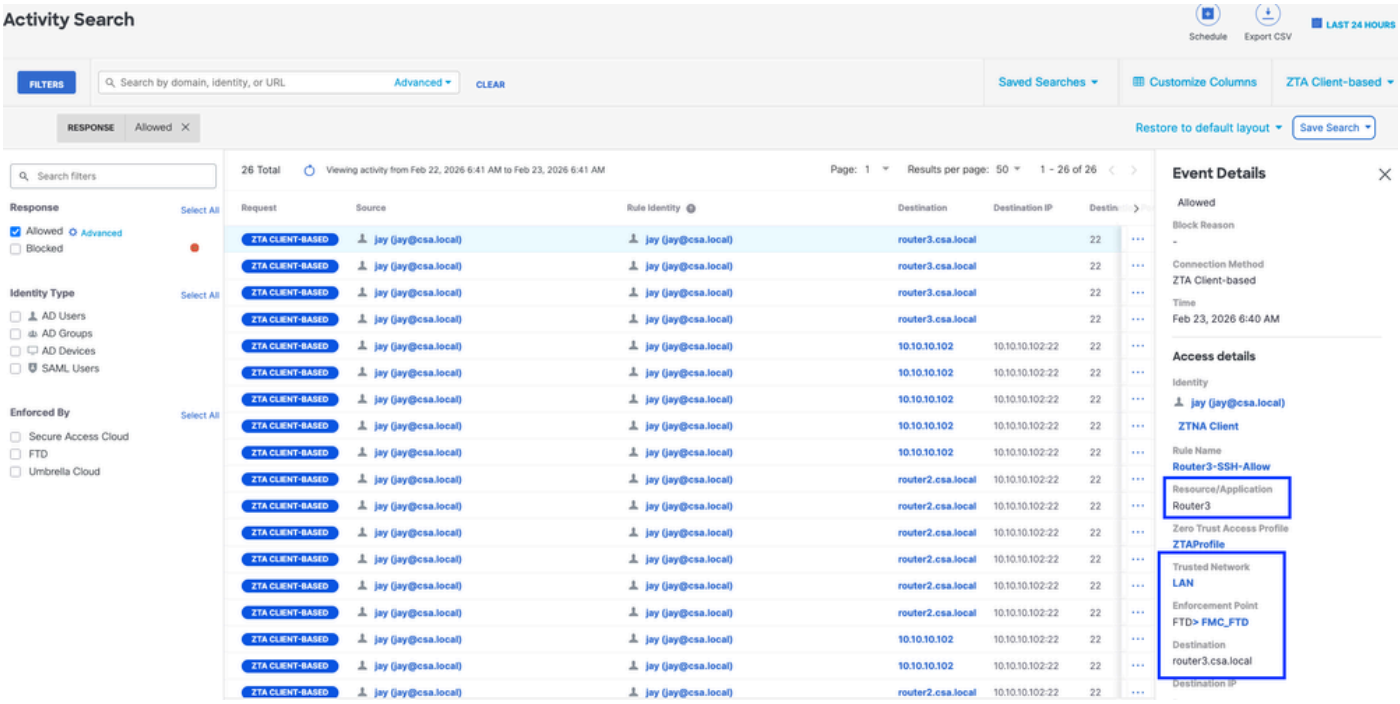


Secure Access - Prueba de relaciones públicas

5. Verificar registros de búsqueda de actividad de acceso seguro

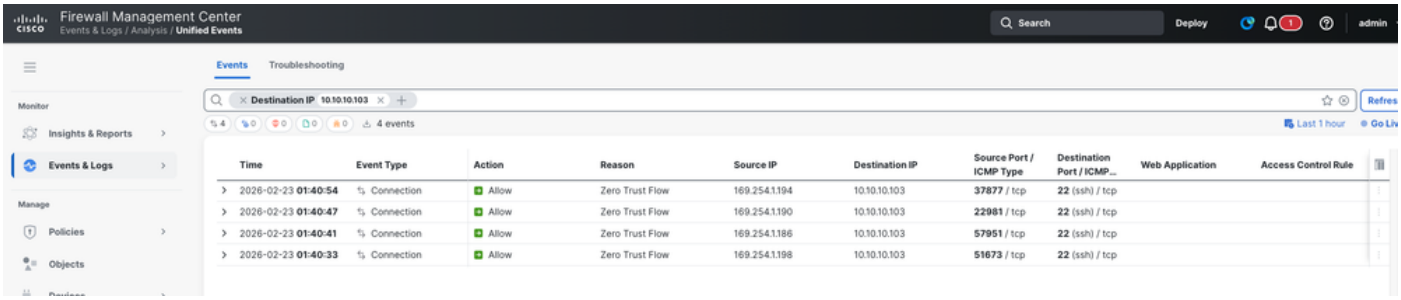


Acceso seguro - Búsqueda de actividad



Acceso seguro - Búsqueda de actividad

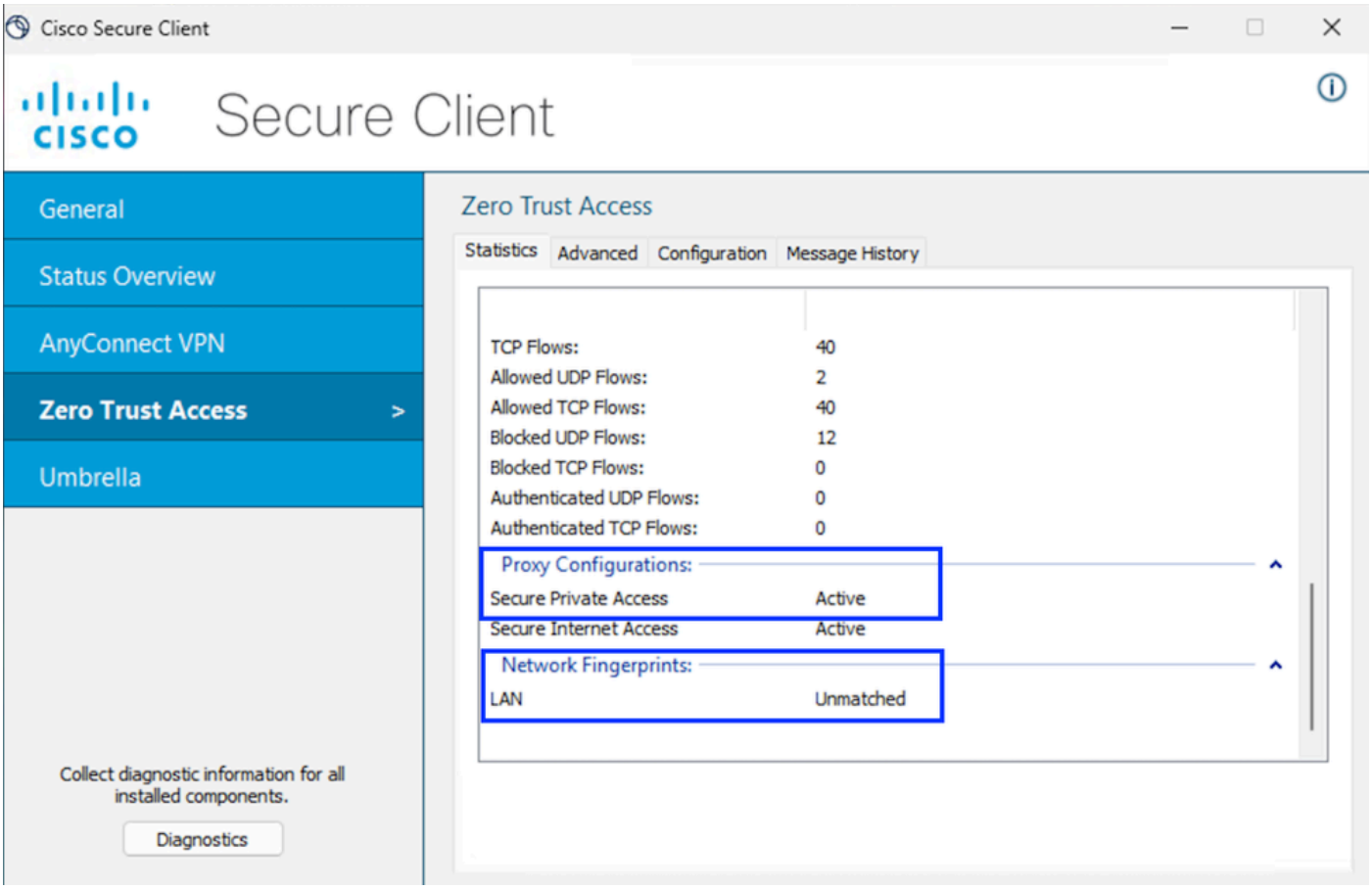
6. Verificar eventos de conexión FMC



Eventos de conexión FMC

Cuando el usuario es remoto

1. Verifique la huella dactilar de la red para ZTA TND, debe dejar de coincidir si el usuario es remoto



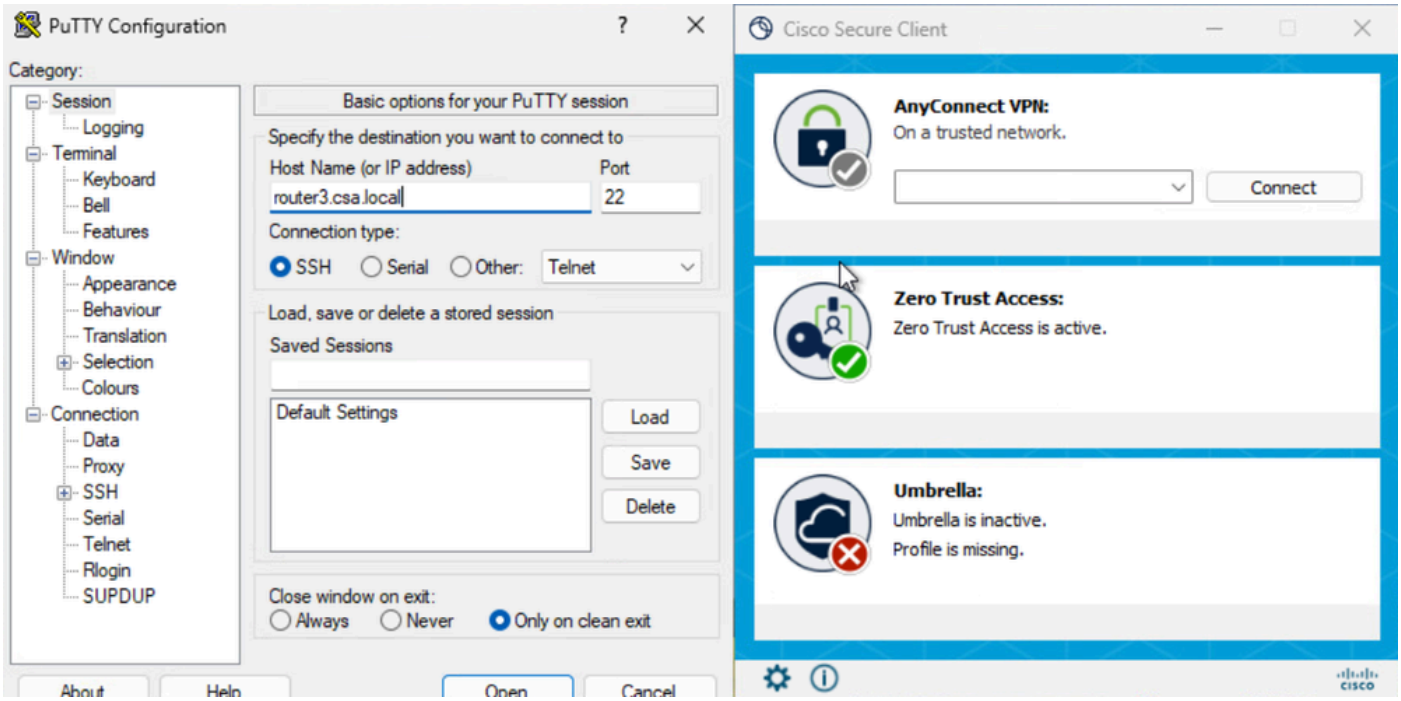
Secure Access - Prueba de relaciones públicas

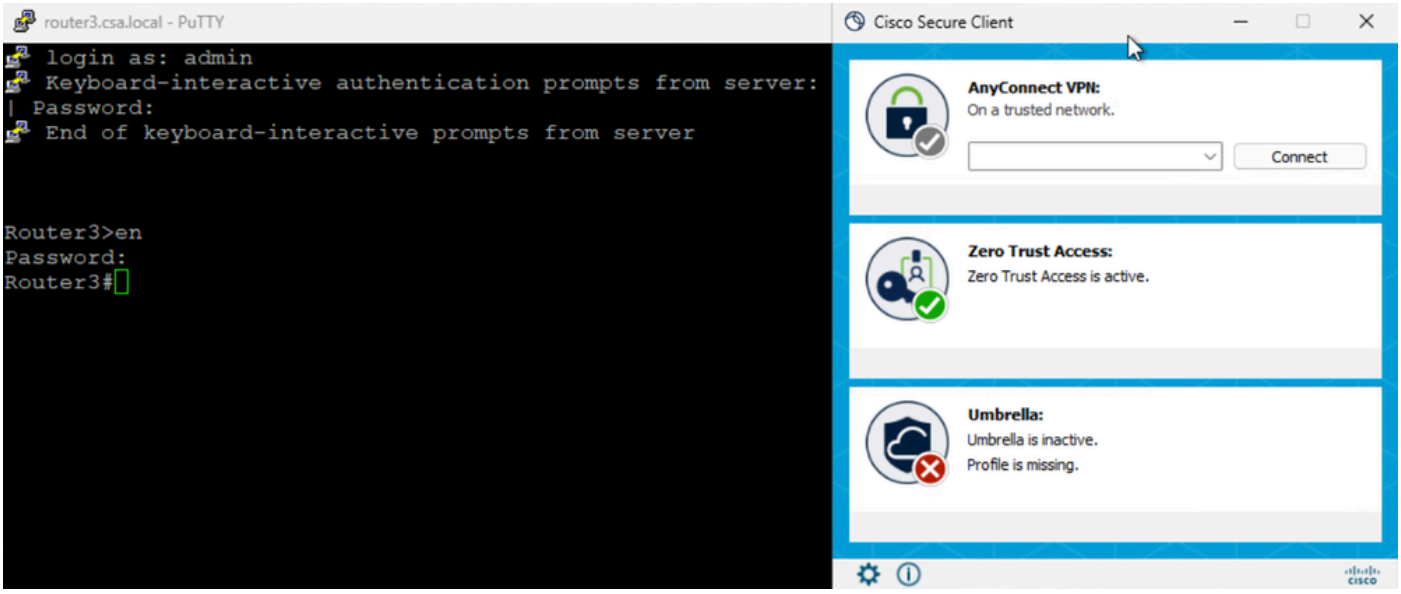
2. Compruebe que el usuario remoto puede resolver el FQDN del FTD

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

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server:  AD.csa.local
Address:  192.168.1.20

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


3. Pruebe la conexión SSH al recurso privado

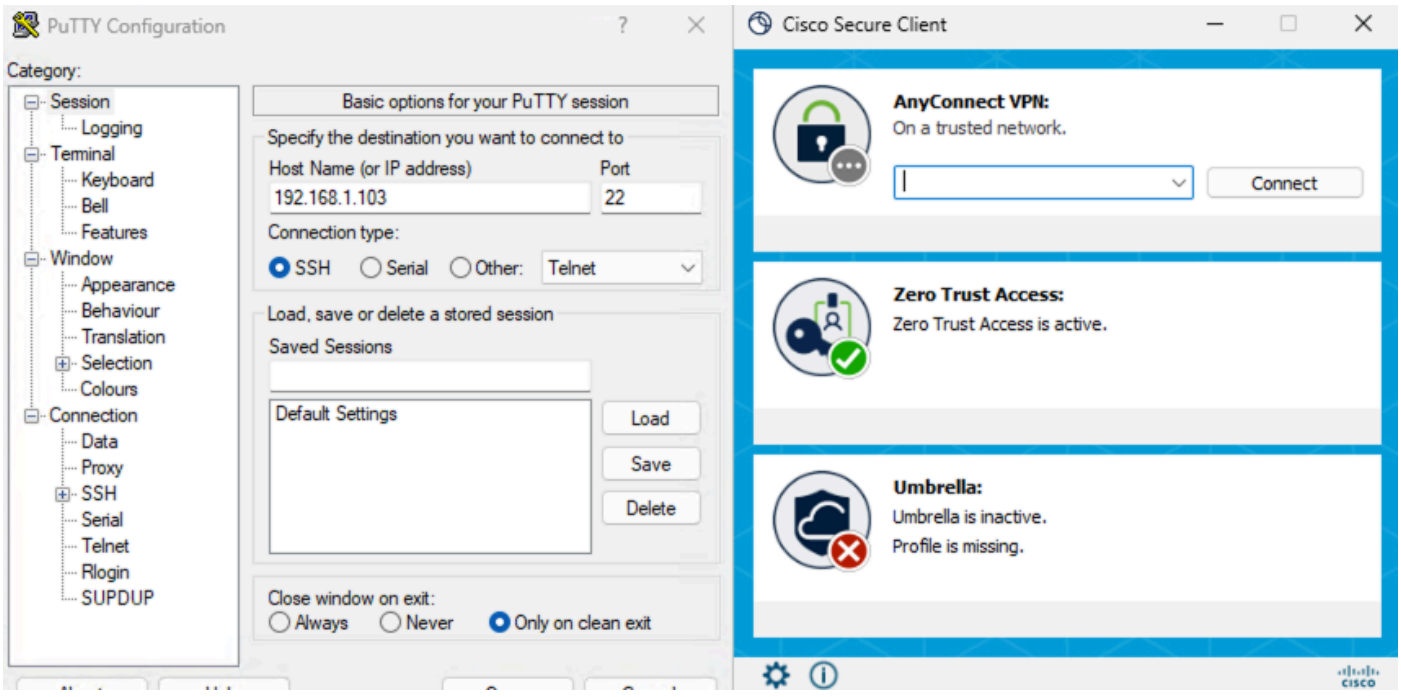
Acceso al PR mediante FQDN



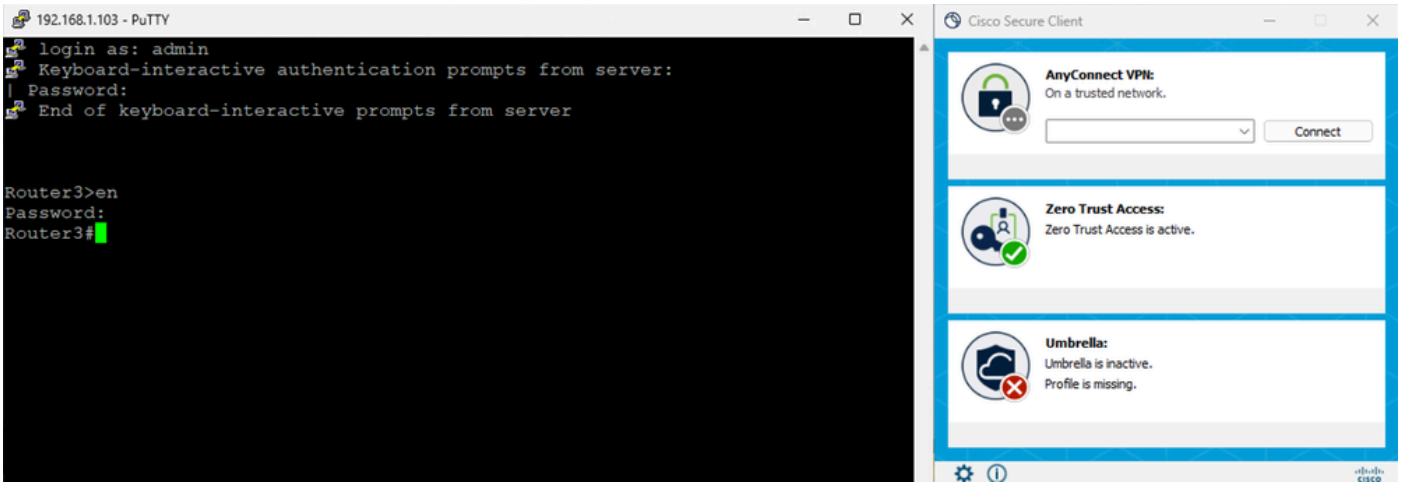


Secure Access - Prueba de relaciones públicas

Acceso al PR mediante la dirección IP

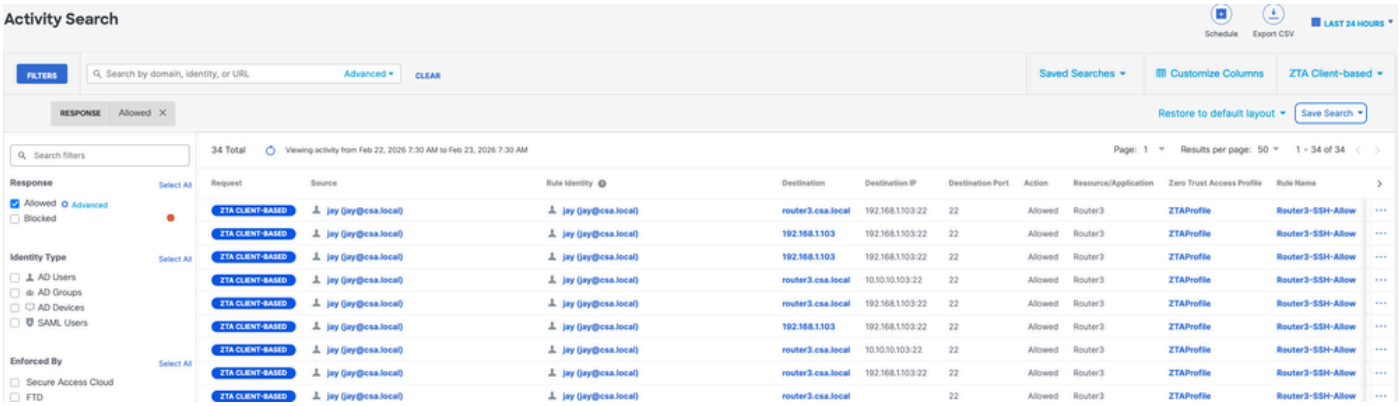


Secure Access - Prueba de relaciones públicas

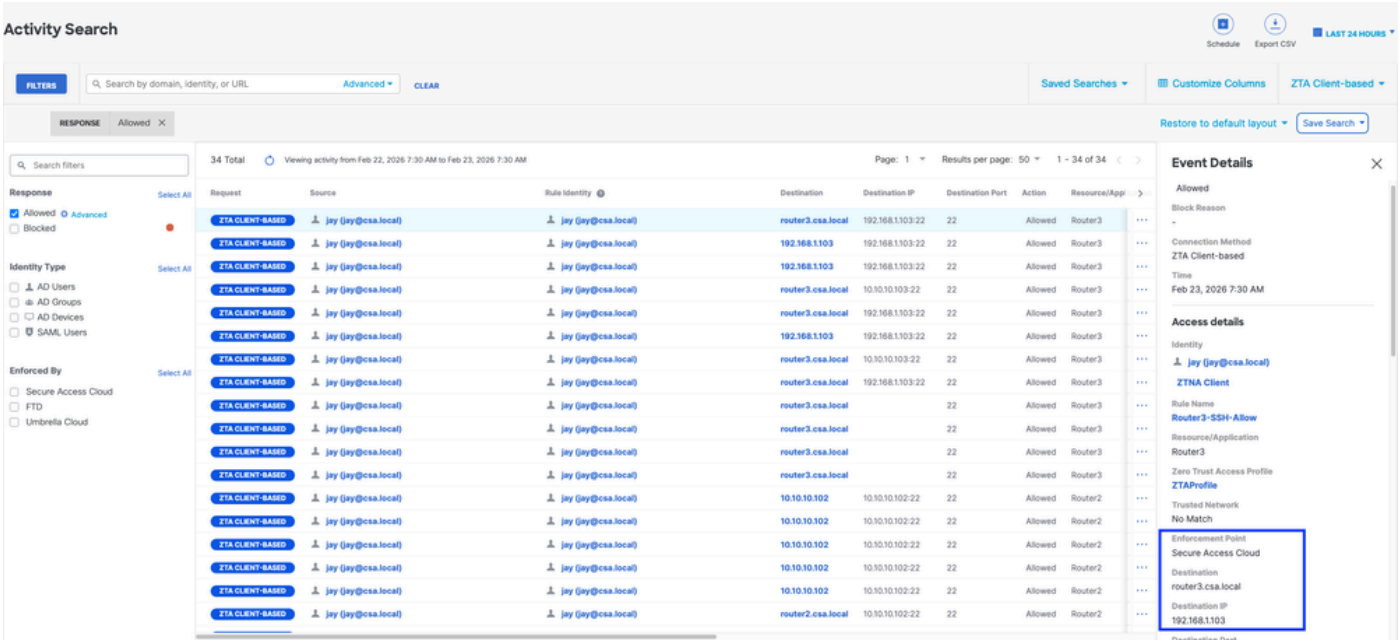


Secure Access - Prueba de relaciones públicas

5. Verificar registros de búsqueda de actividad de acceso seguro



Acceso seguro - Búsqueda de actividad



Troubleshoot

Comandos útiles:

> 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

! y, a continuación, vaya al modo experto

tail -f /ngfw/var/log/messages

show conn all

show nat detail

show asp table socket

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).