

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Acerca de Universal ZTNA](#)

[Detección de red](#)

[Tipos de aplicación](#)

[Casos de uso](#)

[Componentes arquitectónicos](#)

[Flujo de paquetes](#)

[Configurar](#)

[Diagrama de la red](#)

[Casos de prueba](#)

[Caso de prueba 1: Usuario remoto - Aplicación en la nube](#)

[Caso de prueba 2: usuario remoto, aplicación local](#)

[Caso de prueba 3: usuario local, aplicación local](#)

[Caso de prueba 4: usuario local y remoto: aplicación local o en la nube con TND](#)

[Troubleshoot](#)

[Comandos útiles:](#)

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

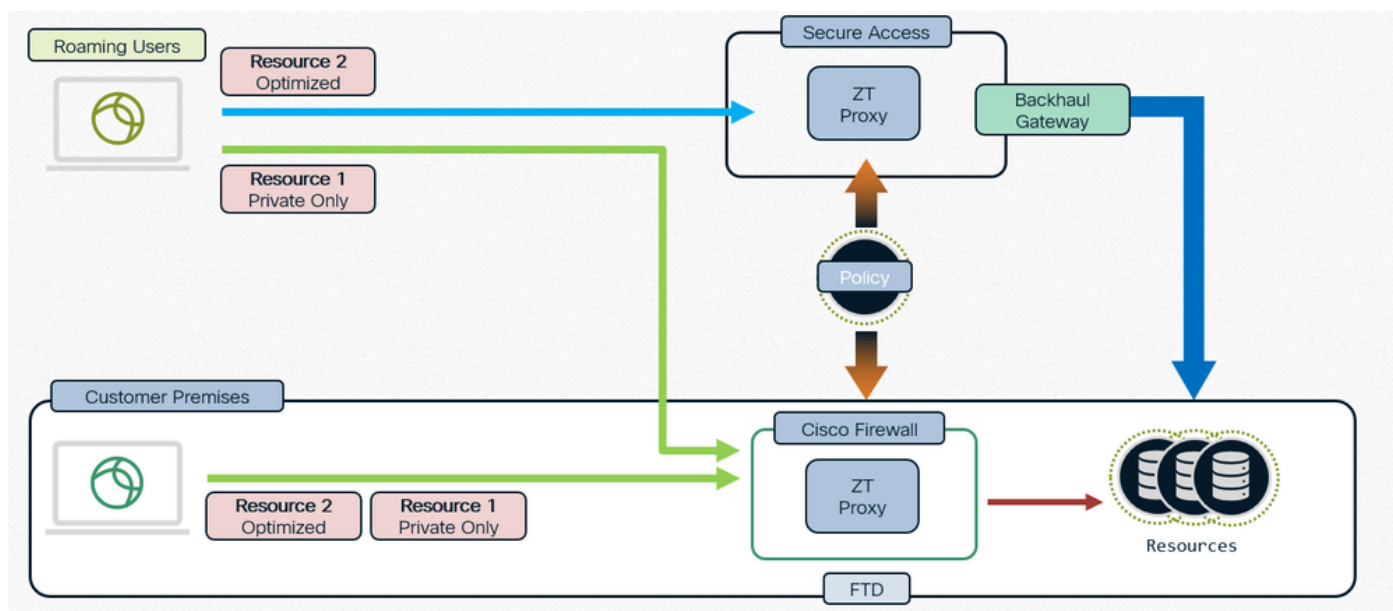
El acceso a la red universal de confianza cero (uZTNA) permite a los administradores permitir

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.

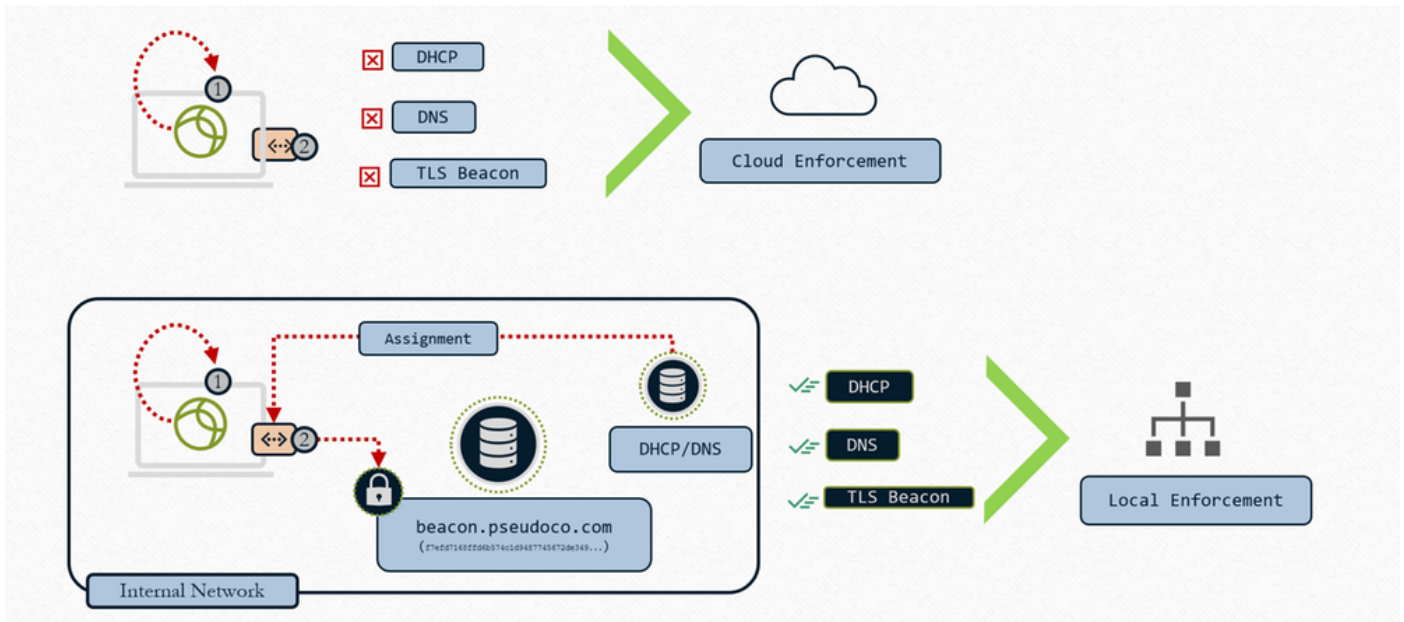
El proxy de tráfico, así como la aplicación de políticas de malware, archivos e IPS, se realiza en Firepower Threat Defence (FTD).



Política única, aplicación distribuida

Detección de red

Determinar la aplicación local o en la nube



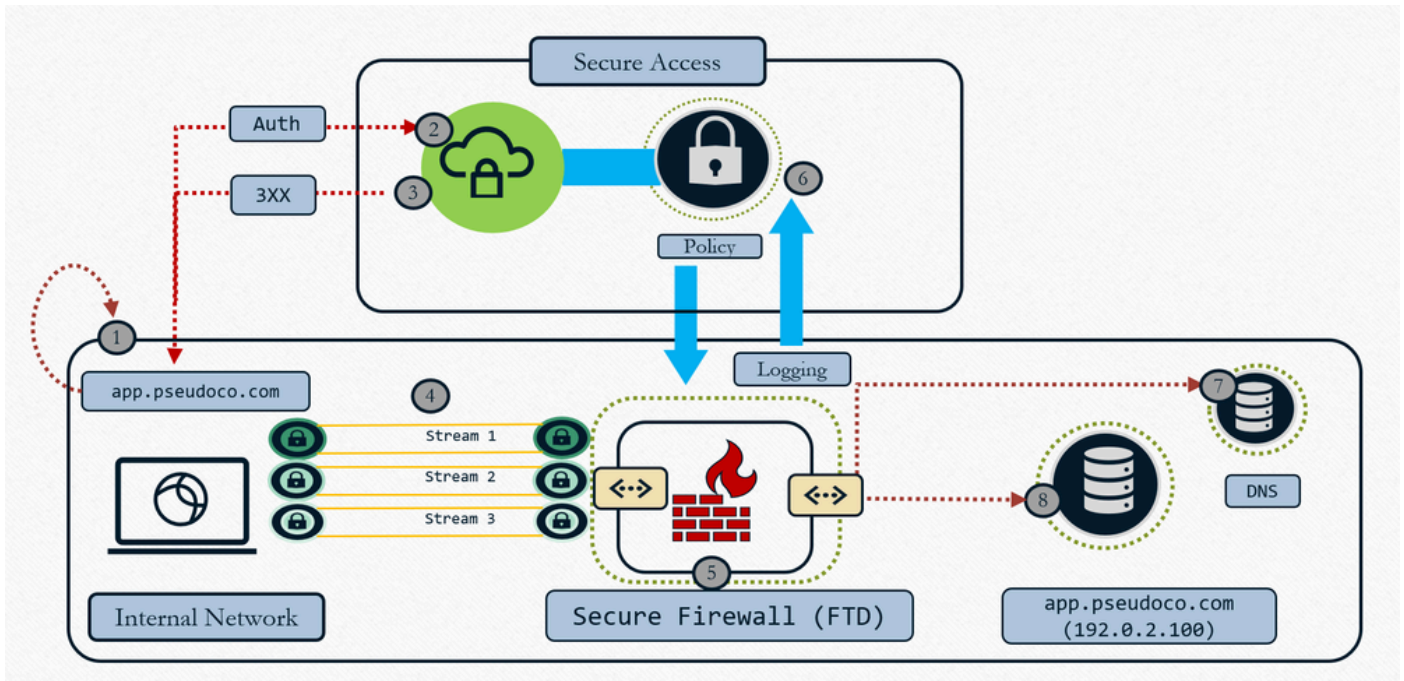
ZTNA universal: determinación de la aplicación local o en la nube

- 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 interceptación 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](#)

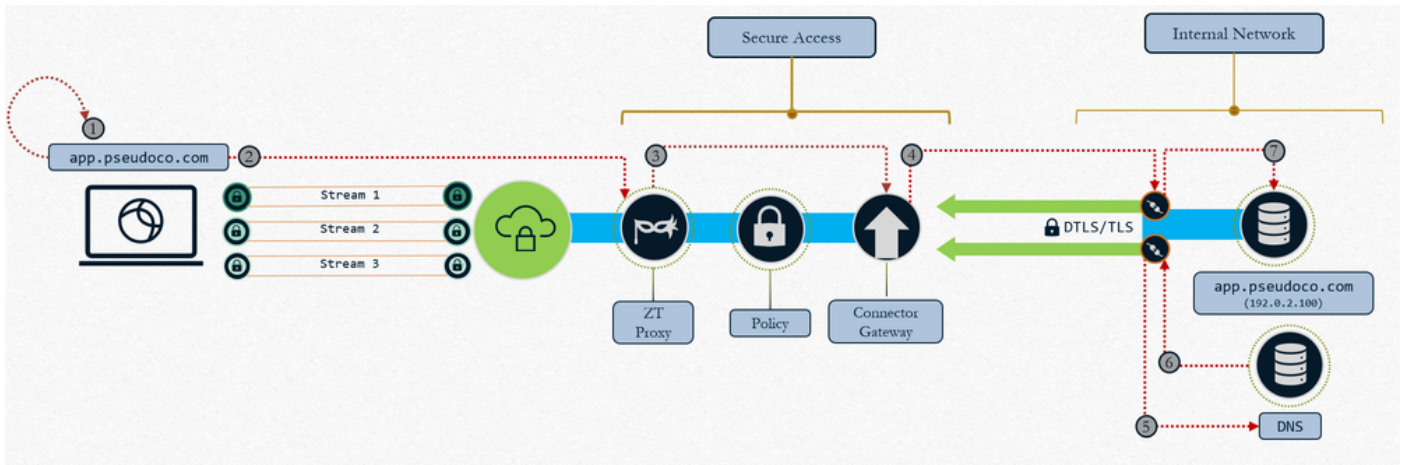
Tipos de aplicación

- 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

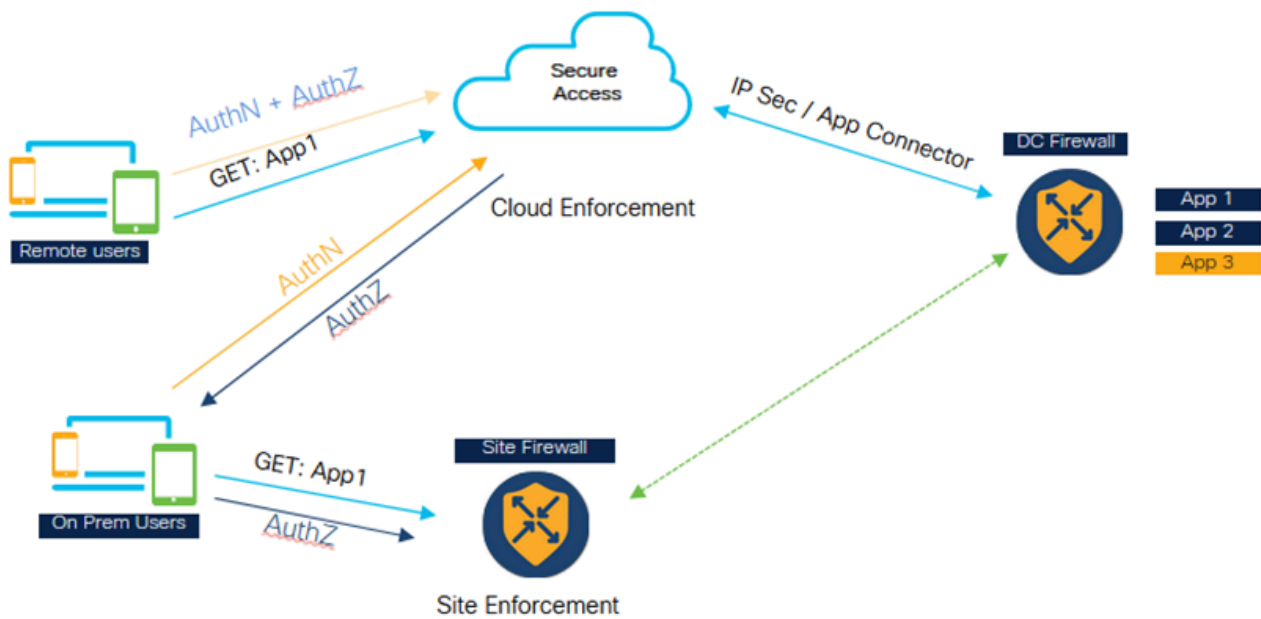


ZTNA universal: Aplicación en la nube

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

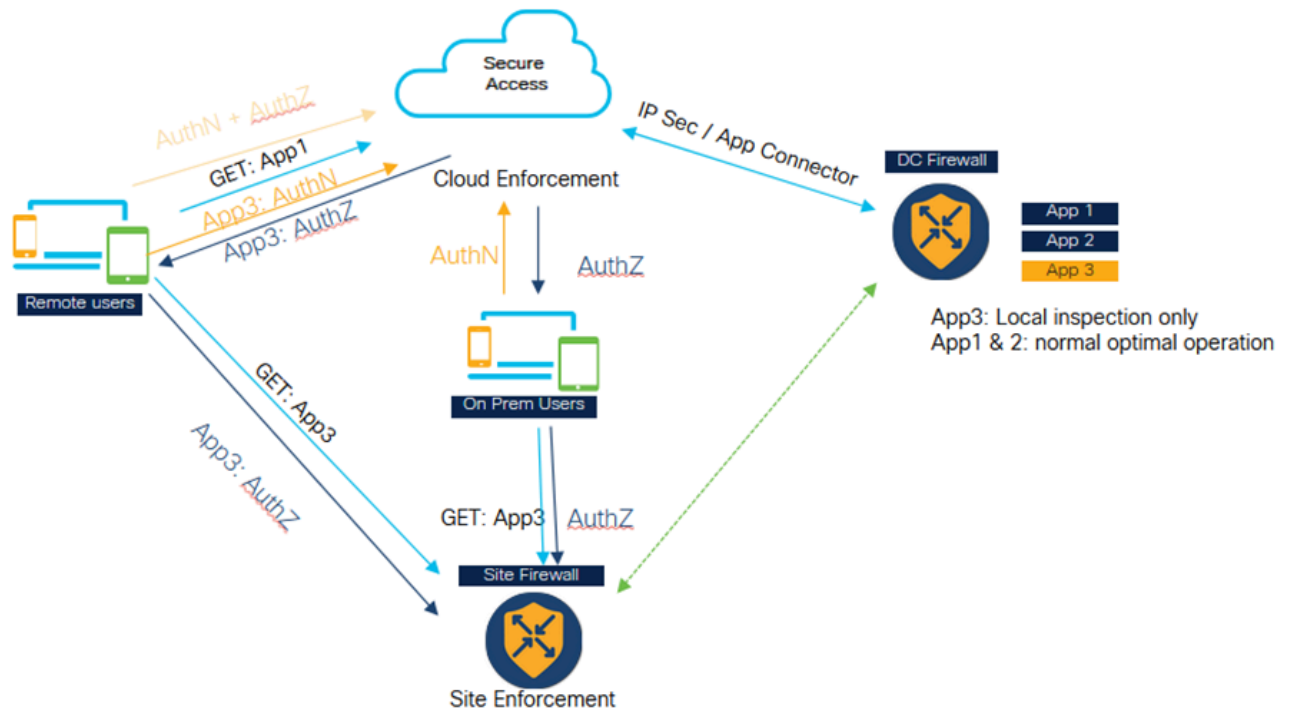
Caso 1: ZTNA coherente y optimizada para los usuarios cuando se encuentren en las instalaciones



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

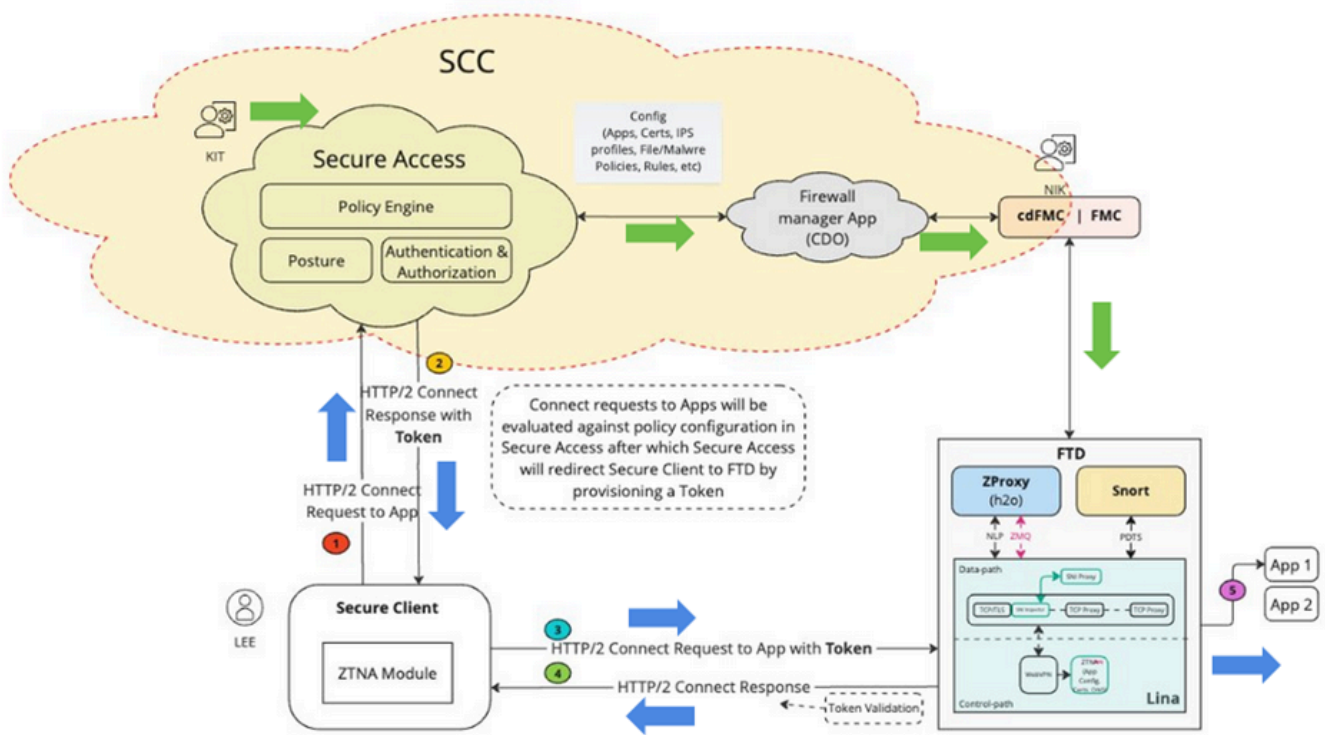
Caso 2: Inspección privada para aplicaciones sensibles



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 firewalls 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.

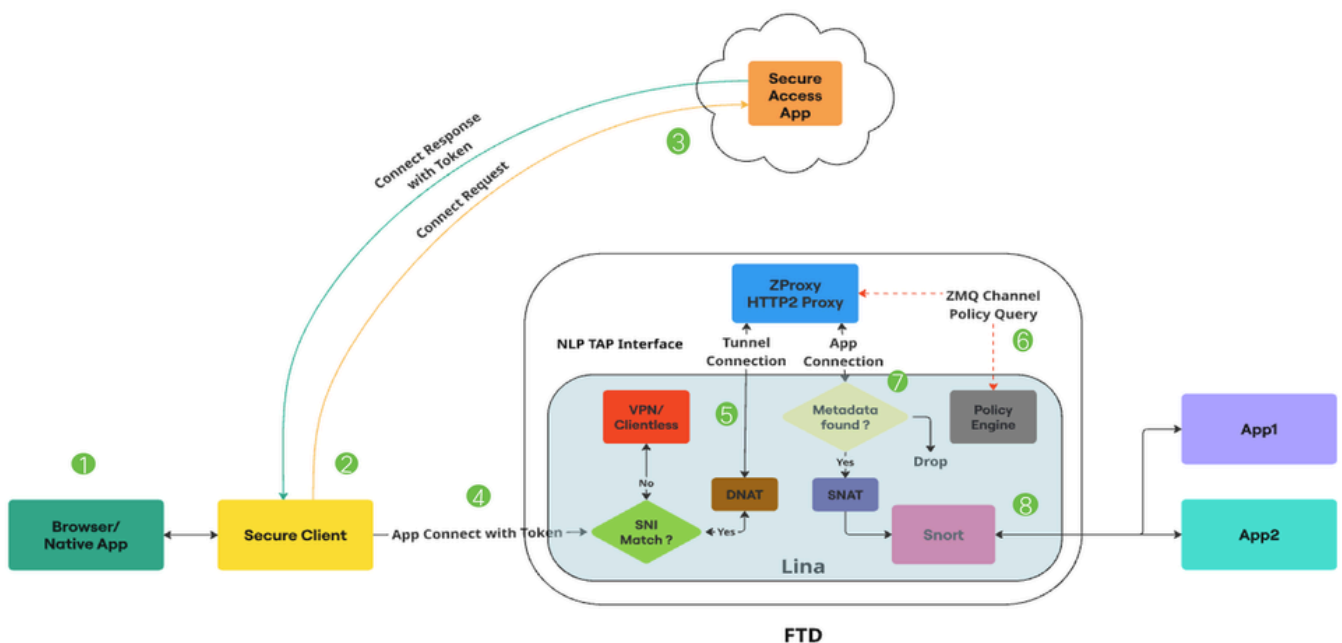
Defensa frente a amenazas de firewall: FTD que protege estas aplicaciones. FTD ejecuta un proxy ZT que también se conoce como H2O (igual que el proxy se ejecuta en la nube de acceso seguro)

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

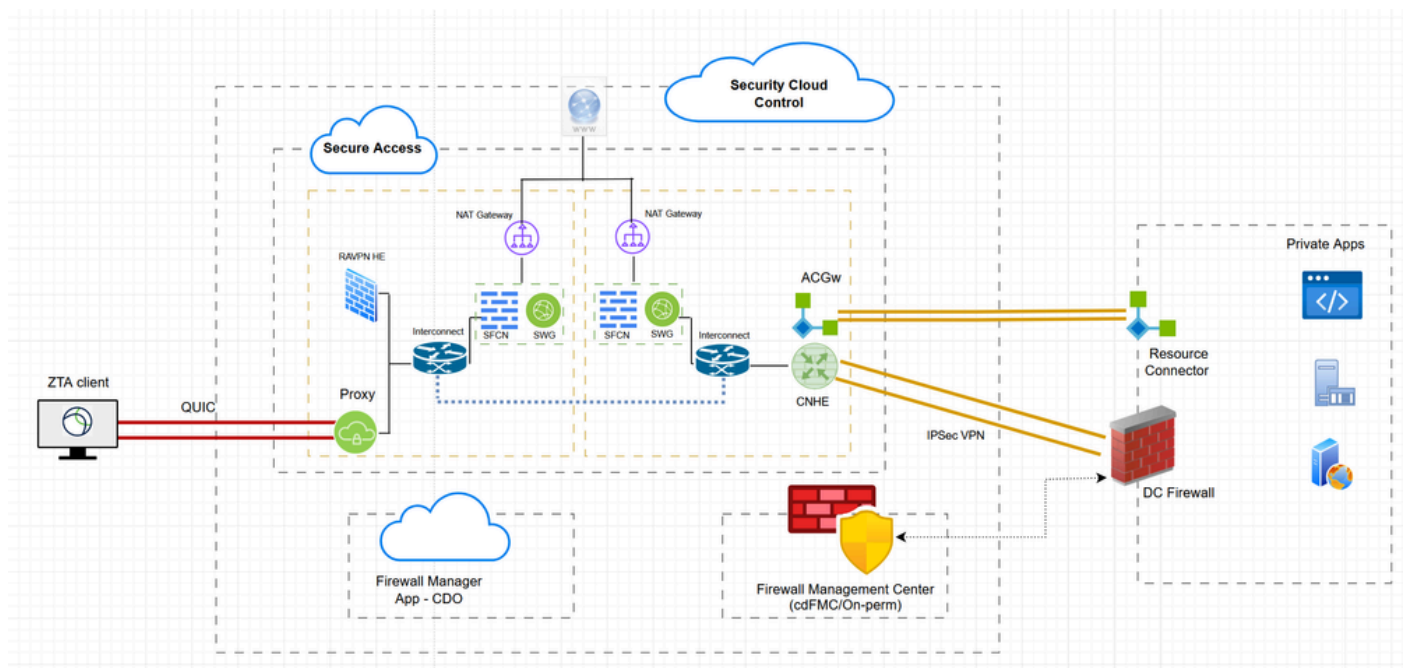
8. Dado que la conexión de la aplicación se origina desde ZProxy, tendrá una IP interna (ejemplo: 169.251.1.2) como IP de origen. Esto se traducirá a la IP de la interfaz de salida de FTD, antes de enviarla. Lina marca los flujos de confianza cero universal para la inspección de Snort solo si hay un 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

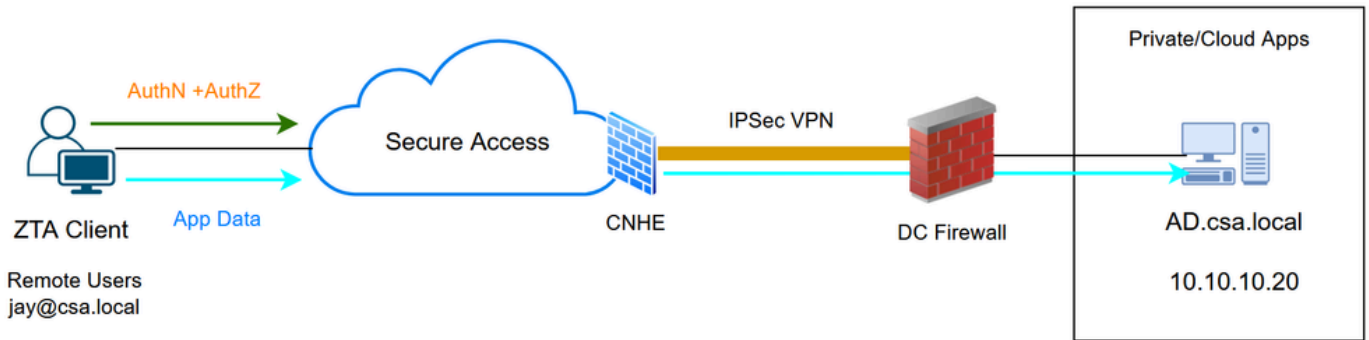


ZTNA híbrido: Diagrama de red

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

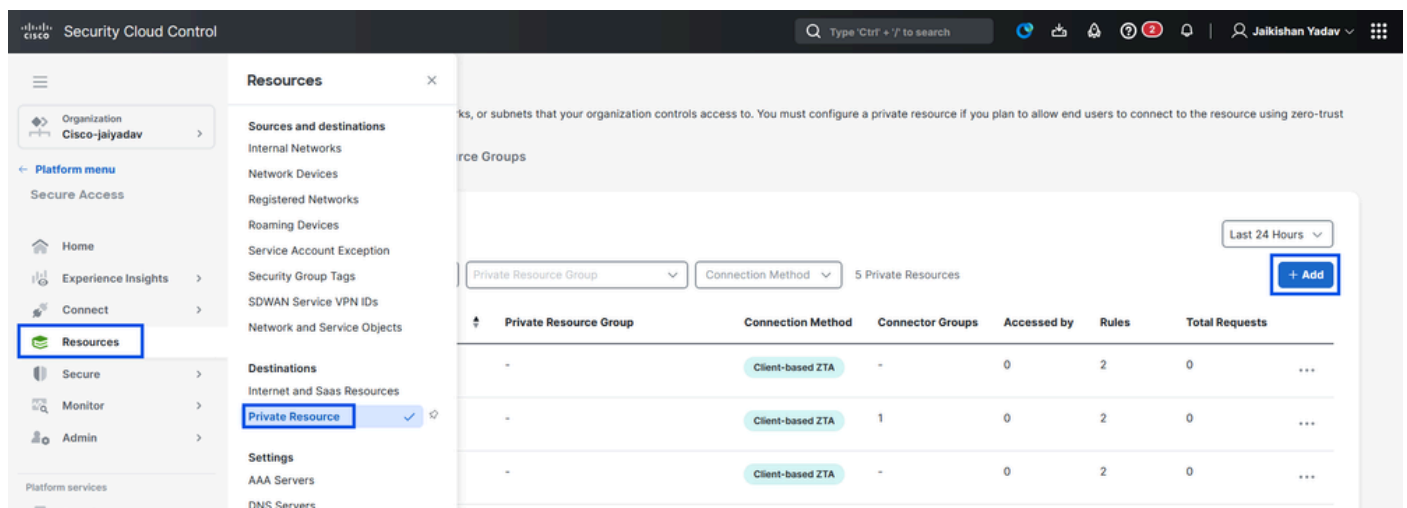


ZTA universal: topología de caso de prueba

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.

← Private Resources

Add a Private Resource

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

General

Private Resource Name

Description (optional)

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

Private resource address

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

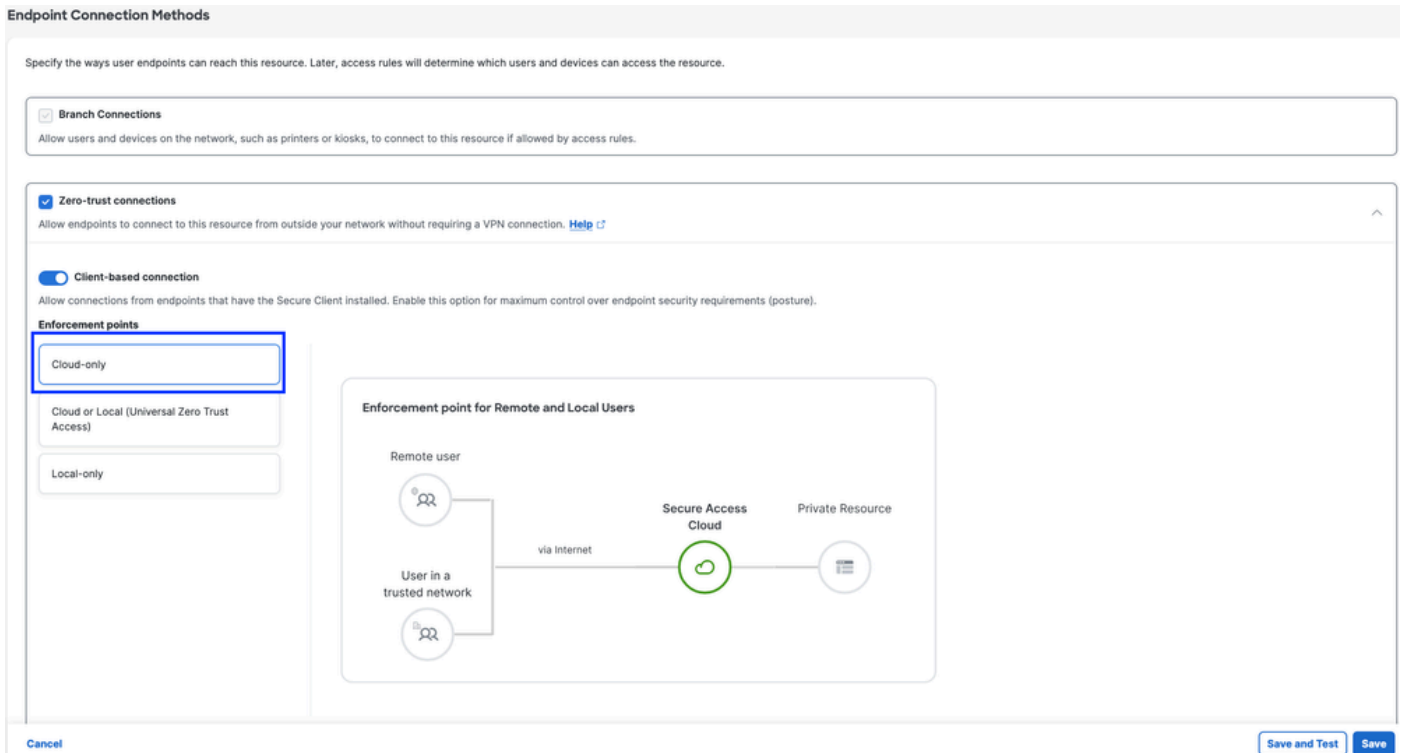
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
<input type="text" value="ad.csa.local"/>	TCP - RDP ▾	<input type="text" value="Any"/>	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.20"/>	TCP - RDP ▾	<input type="text" value="Any"/>	+ Protocol & Port
Remove	+ IP Address/FQDN		

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

Internal DNS Server

Acceso seguro - Configuración de recursos privados

5. Seleccionar métodos de conexión de terminales



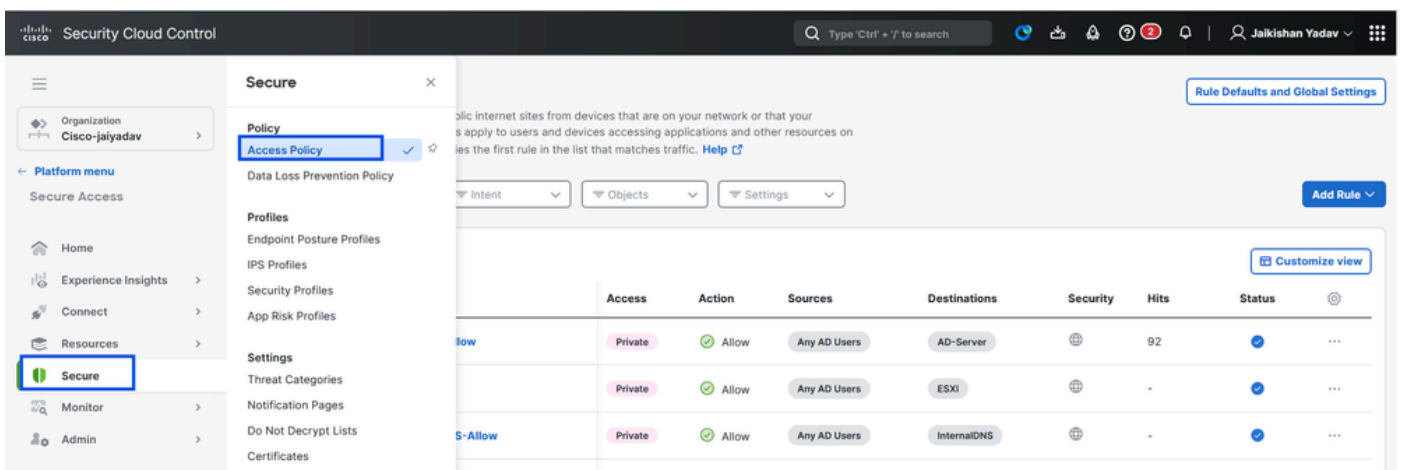
Acceso seguro - Configuración de recursos privados

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.

Access Policy Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings Add Rule ^

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

Rows per page: 100 1-2 of 2 < 1 >

Private Access

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

Internet Access

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

Acceso seguro - Configuración de la política de acceso

3. Agregar un nombre de regla

Add AD-RDP-Allow

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

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

Summary

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

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

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From: To:

Acceso seguro - Configuración de la política de acceso

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

Rule name: Rule order:

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From
Specify one or more sources.

To
Specify one or more destinations.

+ AND

Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is installed.

Profile: **None** | Requirements: **None**

Private Resources: **AD-Server**

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval Rule Defaults Disabled

Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

[Cancel](#)

[Back](#)

[Next](#)

Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad

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

2 **Configure Security**
Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) ⏻ Disabled

Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile ⏻

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

Cancel Back Save

Acceso seguro - Configuración de la política de acceso

7. Haga clic en Guardar

Access Policy Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings Add Rule

3 Rules										
#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status		
1	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	🌐	-	🟢	...	
2	BlockPage-TEST	Internet	Block	Any	Generative A...	🌐	-	🟢	...	
3	RAVPN-Allow	Internet	Allow	Any AD Users	Any	🌐🔒	492	🟢	...	

Rows per page 100 1-3 of 3 < 1 >

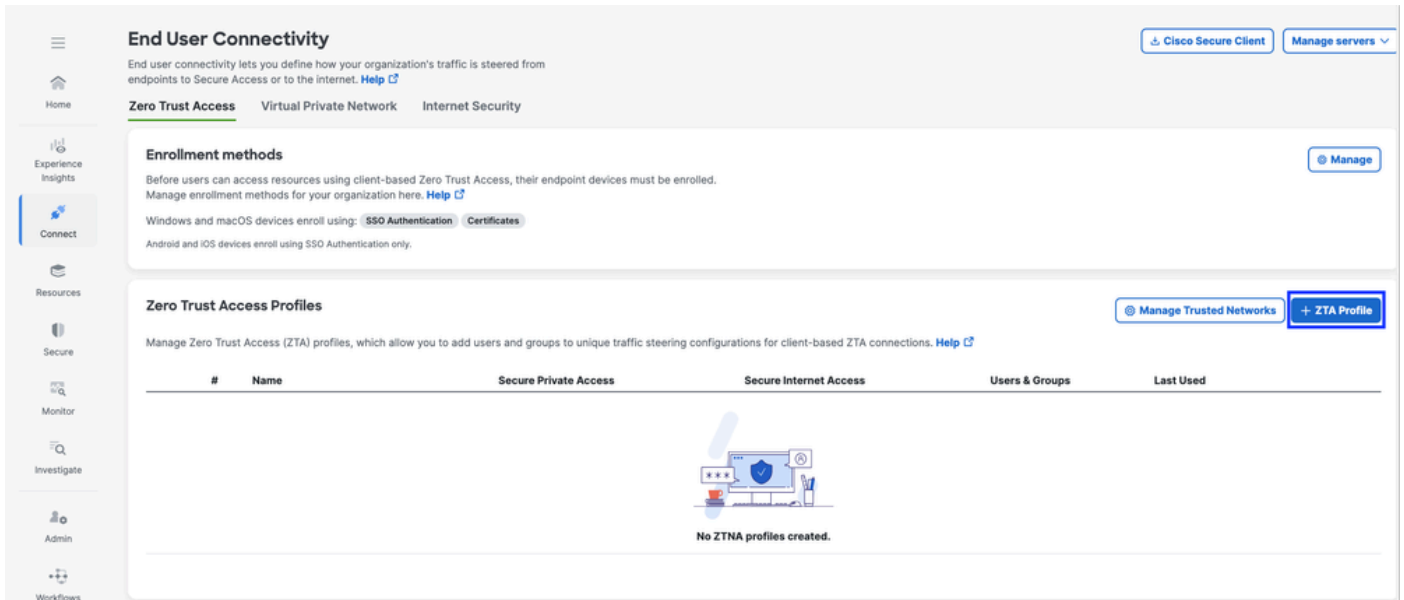
Default Access Rules						
Rule name	Action	Sources	Destinations	Security	Posture	
For all private access	Block	Any	Any private destination	-	-	...
For all Internet access	Allow	Any	Any Internet destination	🌐🔒	-	...

Acceso seguro - Configuración de la política de acceso

Paso - 3 Agregar un recurso privado al perfil ZTA

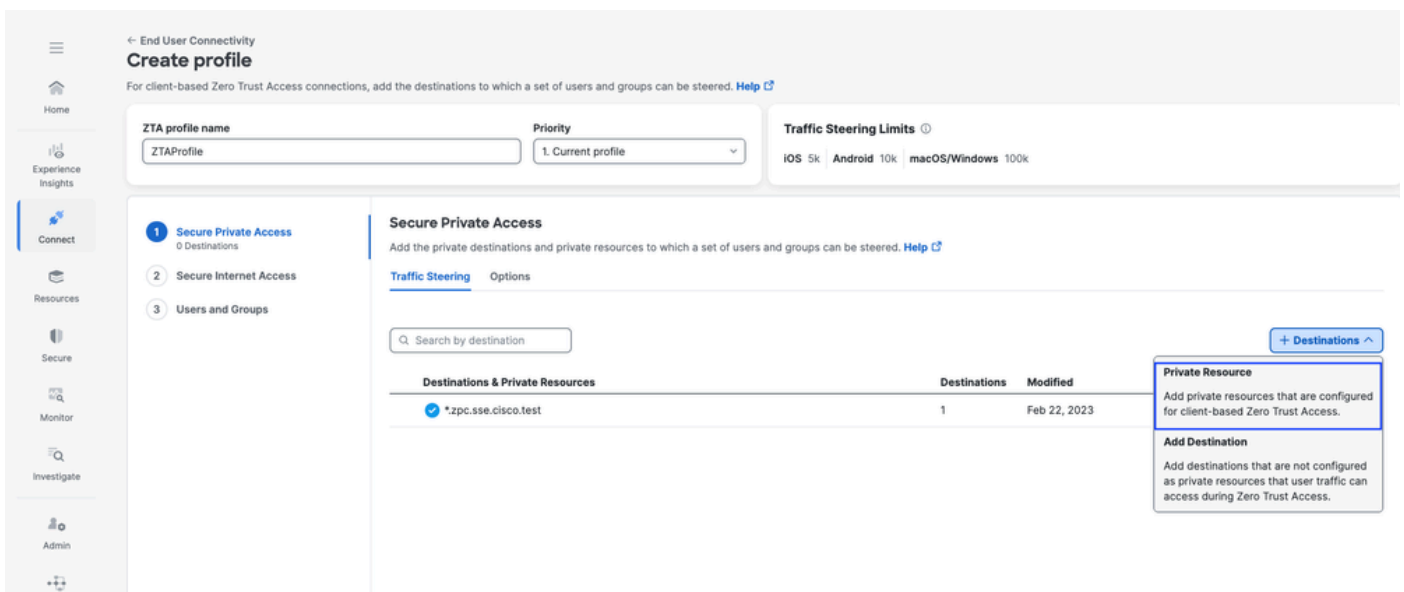
Si está utilizando un perfil ZTA personalizado, debe agregar el recurso privado correspondiente al perfil ZTA

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

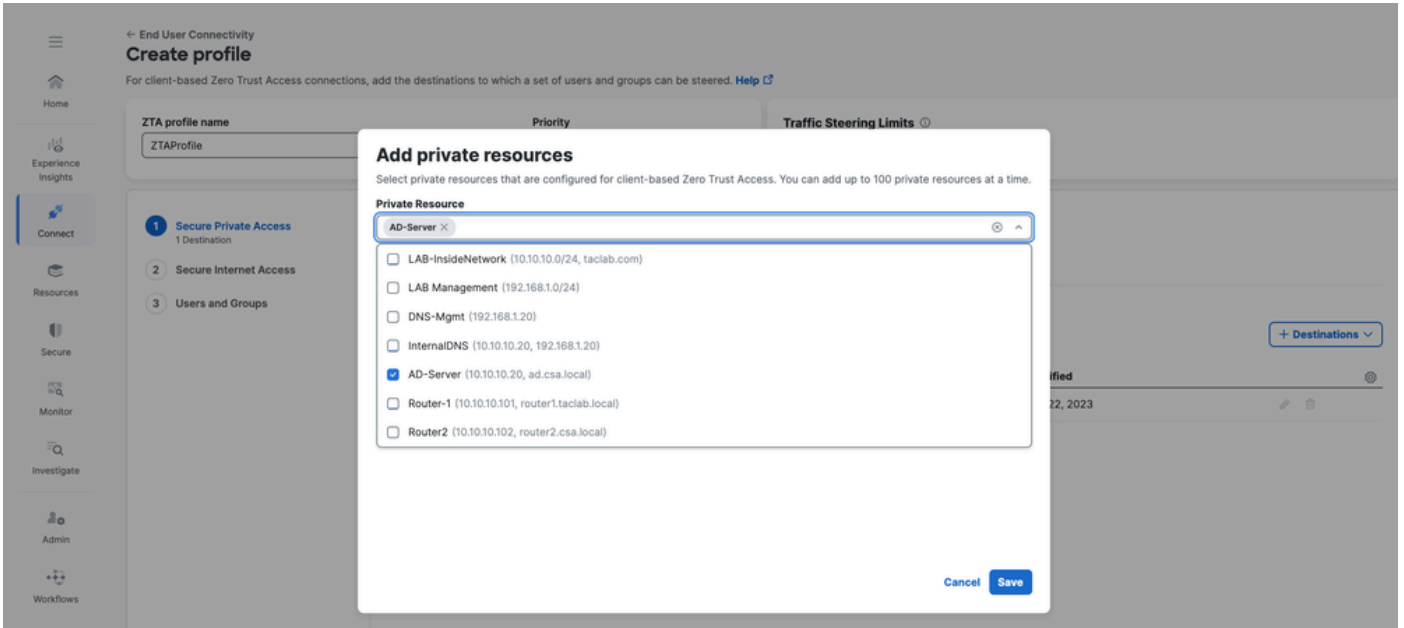


Acceso seguro - Perfil ZTA

2. Añada el recurso privado

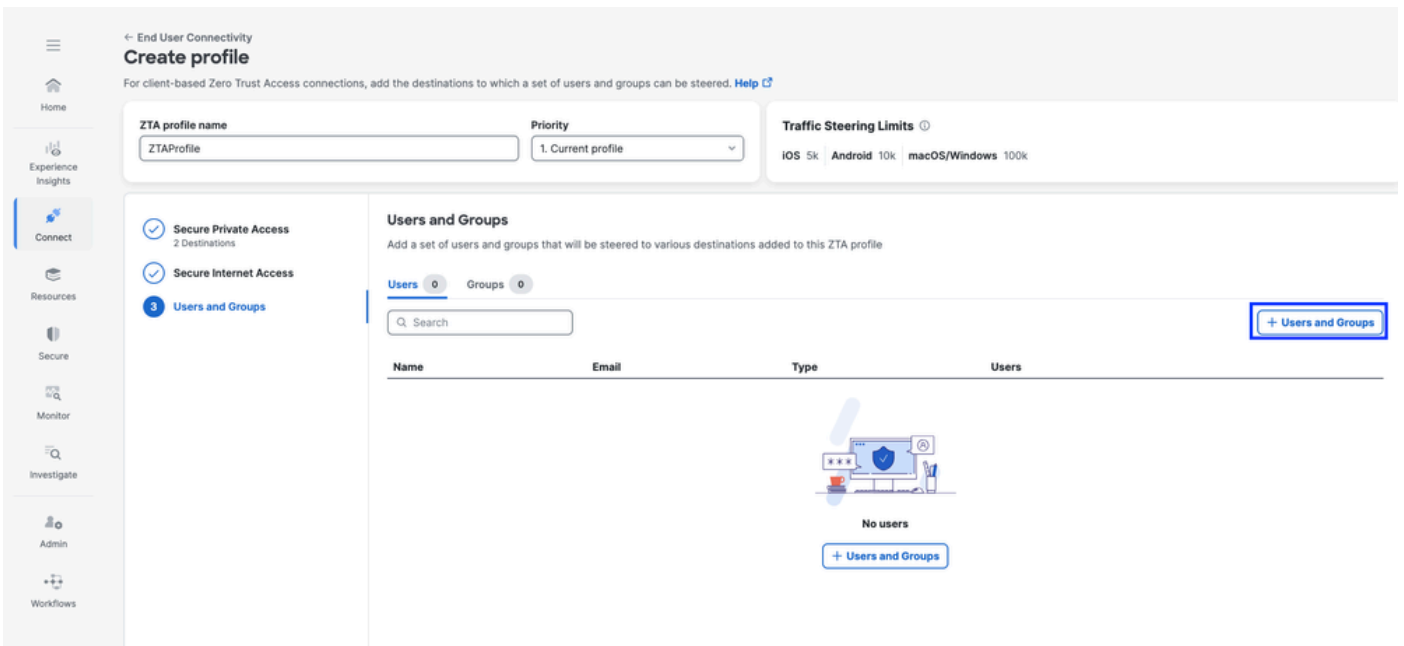


Acceso seguro - Perfil ZTA



Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos



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

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

Users and Groups

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

Users 1 | Groups 0

Q Search + Users and Groups

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

Rows per page: 10 < >

Back Close

Acceso seguro - Perfil ZTA

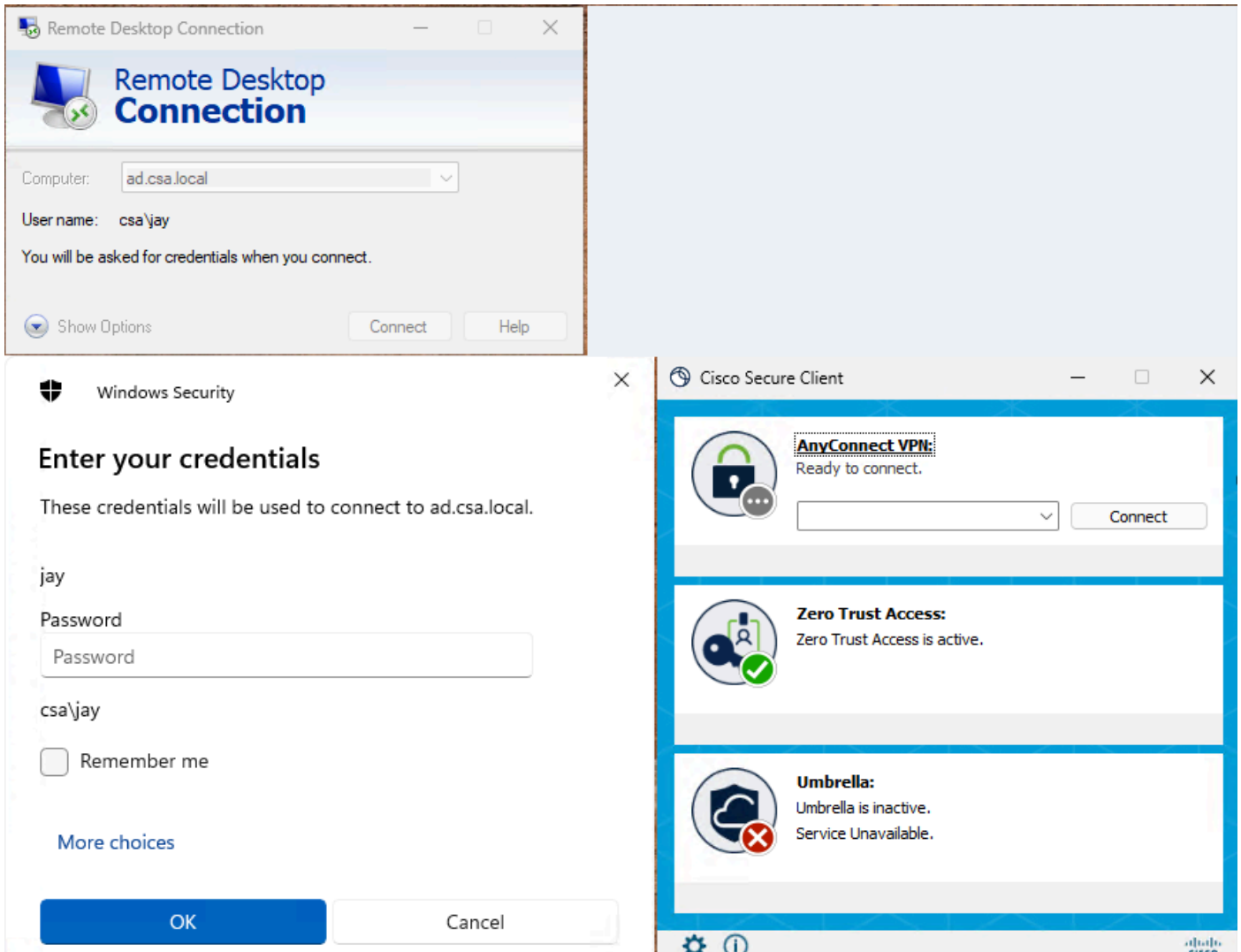


Nota: Puede tardar hasta 15-20 minutos en insertar y sincronizar la configuración con el cliente para el recurso privado asignado

Paso - 4 Verificar el acceso al recurso privado

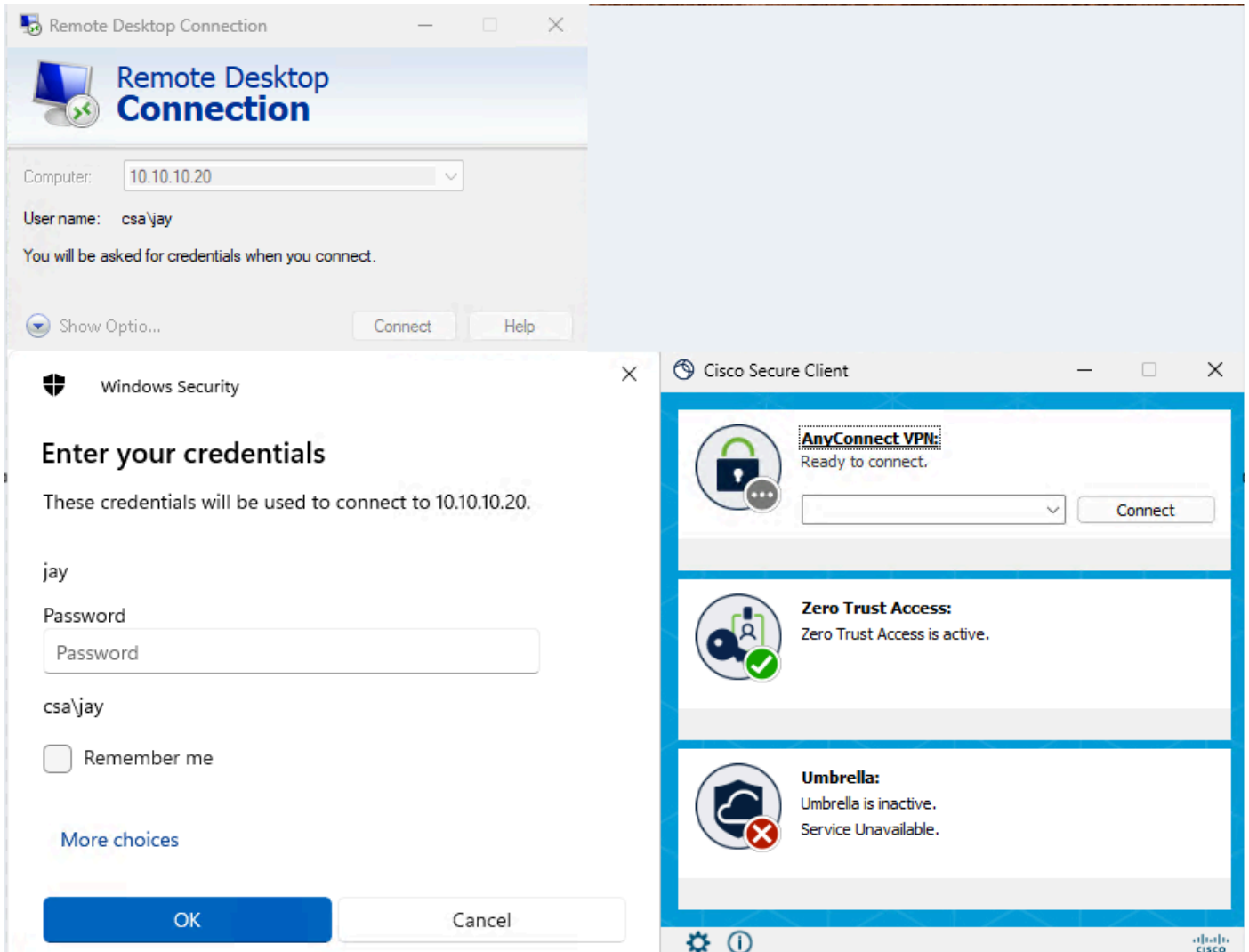
1. Acceso al recurso privado

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

Activity Search

Schedule Export CSV LAST 24 HOURS

FILTERS Search by domain, identity, or URL Advanced CLEAR Saved Searches Customize Columns ZTA Client-based

IP ADDRESS 10.10.10.20 RESPONSE Allowed Restore to default layout Save Search

3 Total Viewing activity from Jan 11, 2026 4:49 AM to Jan 12, 2026 4:49 AM Page: 1 Results per page: 50 1 - 3 of 3

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Applica
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server

Acceso seguro - Búsqueda de actividad

Activity Search

Schedule Export CSV LAST 24 HOURS

FILTERS Search by domain, identity, or URL **Advanced** CLEAR Saved Searches Customize Columns ZTA Client-based

IP ADDRESS 10.10.10.20 PORT 3389 Restore to previous state Save Search

3 Total Viewing activity from Jan 11, 2026 4:53 AM to Jan 12, 2026 4:53 AM Page: 1 Results per page: 50 1 - 3 of 3

Response Select All
 Allowed Advanced
 Blocked

Identity Type Select All
 AD Users
 AD Groups
 AD Devices
 SAML Users

Enforced By Select All
 Secure Access Cloud
 FTD
 Umbrella Cloud

Request	Source	Action	Destination	Destination IP	Destination Port
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389

Event Details

Identity: jay (jay@csa.local)
Win1
Rule Name: AD-RDP-Allow
Resource/Application: AD-Server
Zero Trust Access Profile: Default ZTA Profile
Trusted Network: No Match
Enforcement Point: Secure Access Cloud
Destination: ad.csa.local
Destination IP: 10.10.10.20

Page: 1 Results per page: 50 1 - 3 of 3

Acceso seguro - Búsqueda de actividad

Activity Search Schedule Export CSV LAST 24 HOURS

FILTERS Search by domain, identity, or URL **Advanced** CLEAR Saved Searches Customize Columns ZTA Client-based

IP ADDRESS 10.10.10.20 Restore to default layout Save Search

9 Total Viewing activity from Jan 11, 2026 5:51 AM to Jan 12, 2026 5:51 AM Page: 1 Results per page: 50 1 - 9 of 9

Response Select All
 Allowed Advanced
 Blocked

Identity Type Select All
 AD Users
 AD Groups

Request	Source	Action	Destination	Destination IP	Destination Port	Resource/Application	Zero Trust Access Profile	Rule Name	OS
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win

Acceso seguro - Búsqueda de actividad

Activity Search

Schedule Export CSV LAST 24 HOURS

Search by domain, identity, or URL Advanced CLEAR

Filters: IP ADDRESS 10.10.10.20 X Saved Searches Customize Columns ZTA Client-based Save Search

9 Total Viewing activity from Jan 11, 2026 5:51 AM to Jan 12, 2026 5:51 AM Page: 1 Results per page: 50 1 - 9 of 9

Request	Source	Action	Destination	Destination IP	Destination Port	Resource/Application
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 12, 2026 5:51 AM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: AD-RDP-Allow

Resource/Application: AD-Server

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: 10.10.10.20

Destination IP

Acceso seguro - Búsqueda de actividad

3. Verifique los eventos de conexión FMC

Events Troubleshooting

Destination Port / ICMP Code 3389

7 events Last 1 hour

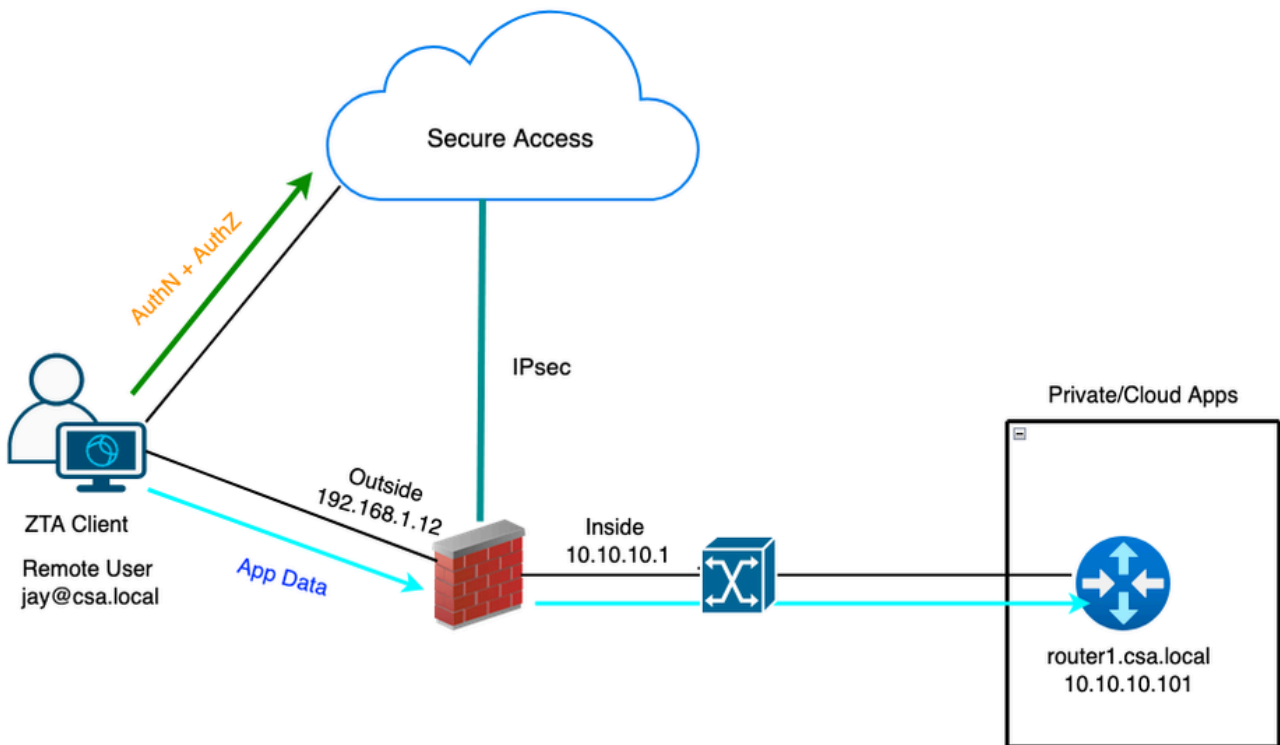
Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Web Application	Access Control Rule
2026-01-12 00:51:24	Connection	Fastpath		100.112.20.48	10.10.10.20	17674 / tcp	3389 / tcp		
2026-01-12 00:51:20	Connection	Fastpath		100.112.20.48	10.10.10.20	47021 / tcp	3389 / tcp		
2026-01-12 00:51:15	Connection	Fastpath		100.112.20.48	10.10.10.20	63712 / tcp	3389 / tcp		
2026-01-12 00:48:24	Connection	Fastpath		100.112.20.48	10.10.10.20	50756 / tcp	3389 / tcp		
2026-01-12 00:42:34	Connection	Fastpath		100.112.72.18	10.10.10.20	60548 / tcp	3389 / tcp		
2026-01-12 00:15:21	Connection	Fastpath		100.112.72.16	10.10.10.20	40660 / tcp	3389 / tcp		
2026-01-12 00:12:45	Connection	Fastpath		100.112.72.16	10.10.10.20	44262 / tcp	3389 / tcp		

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

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has 'Resources' highlighted. The main content area shows a table of Private Resource Groups. The table has the following columns: Private Resource Group, Connection Method, Connector Groups, Accessed by, Rules, and Total Requests. There are three rows of data, all with 'Client-based ZTA' as the connection method.

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

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.

← Private Resources

Add a Private Resource

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

General

Private Resource Name
Router1

Description (optional)
Router1 PR for UZTNA testing

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

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR)	Protocol	Port / Ranges
router1.csa.local	Any TCP	22
10.10.10.101	Any TCP	22

Use internal DNS server to resolve the domain

Internal DNS Server
PrivateDNS (10.10.10.20)

Acceso seguro - Configuración de recursos privados

5. Seleccionar métodos de conexión de terminales

6. Seleccione FTD como puntos de aplicación locales

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

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

Enforcement point for Remote User



Enforcement point for Local user



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

Change the remotely reachable addresses

Cancel

Save and Test

Save

Acceso seguro - Configuración de recursos privados



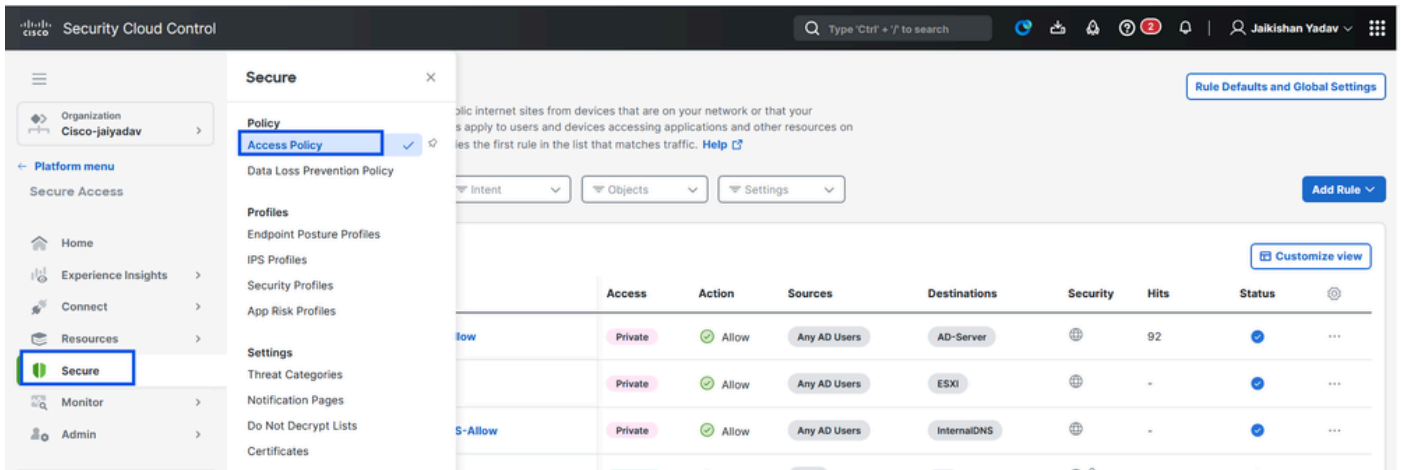
Nota: En función del tipo de inscripción que seleccione, este cambio asociará automáticamente el PR al FTD y activará una implementación de políticas

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](#)

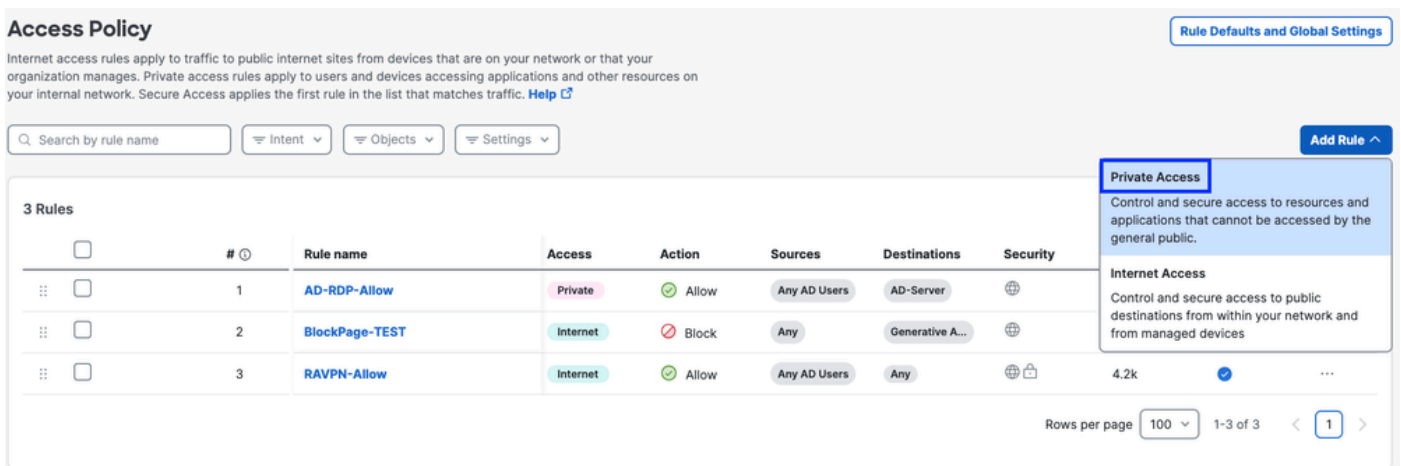
1. Vaya a Seguro > Política de acceso



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

Add Router1-SSH

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

Acceso seguro - Configuración de la política de acceso

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

Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

From

Specify one or more sources.

AD Users - Any AD Users

To

Specify one or more destinations.

Private Resources - Router1

+ AND

Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile [Rule Defaults](#)

Requirements for end-user devices on which the Cisco Secure Client is installed.

Profile: **None** | Requirements: **None**

Private Resources: **Router-1**

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval [Rule Defaults](#)

Disabled

Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

[Cancel](#)

[Back](#) [Next](#)

Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad

1 Specify Access

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

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) [Rule Defaults](#)

Disabled

Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile [Rule Defaults](#)

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

[Cancel](#)

[Back](#) [Save](#)

Acceso seguro - Configuración de la política de acceso

7. Haga clic en Guardar

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	Router1-SSH	Private	Allow	Any AD Users	Router1		-	✓
2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		-	✓
3	BlockPage-TEST	Internet	Block	Any	Generative A...		8.8k	✓
4	RAVPN-Allow	Internet	Allow	Any AD Users	Any		715	✓

Rows per page: 100 1-4 of 4 < 1 >

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

The screenshot shows the Cisco Security Cloud Control interface. On the left, the 'Connect' menu is expanded, with 'Network Connections' selected. The main content area shows a 'Connect' dialog box with a 'Network Connections' tab. Under this tab, there are two status indicators: '0 Warning' and '1 Connected'. Below this, there is a section for 'Tunnel Groups' with a dropdown for 'Region' and a dropdown for 'Status', showing '2 Tunnel Groups'. An '+ Add' button is visible at the bottom right.

Acceso seguro - Verificación de relaciones públicas

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

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associa
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced	1

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local
Auto deployment: Yes

UZTA Configuration status

Synced Last synced at 31 Dec 2025, at 2:51 AM UTC

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status: Synced 1

View resources associated to this FTD

Associate Resources

Acceso seguro - Verificación de relaciones públicas

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

Q Search by resource name Configuration status 1 Resources [Associate Resources](#)

Resource name	Status
Router1	Synced

Close

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

The screenshot displays the 'Network Connections' section of the Palo Alto Networks management console. It features a table of FTDs configured for Universal Zero Trust Access. The table has columns for FTD Name, Version, FMC, UZTA Configuration status, and Associated Resources. One FTD, 'FMC_FTD', is listed with version v10.0.0, FMC as the management point, and a 'Synced' status. A right-hand sidebar provides detailed information for the selected 'FMC_FTD', including Firewall Details (Device FQDN: ftd.csa.local, Auto deployment: Yes), UZTA Configuration status (Synced, last synced at 31 Dec 2025, 2:51 AM UTC), Assigned Trusted Network (LAN), and Associated Resources (1 resource associated).

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

The screenshot shows the 'End User Connectivity' dashboard. The 'Zero Trust Access Profiles' section contains a table with the following data:

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

Buttons for 'Edit' and 'Delete' are visible next to the profile entry.

Acceso seguro - Perfil ZTA

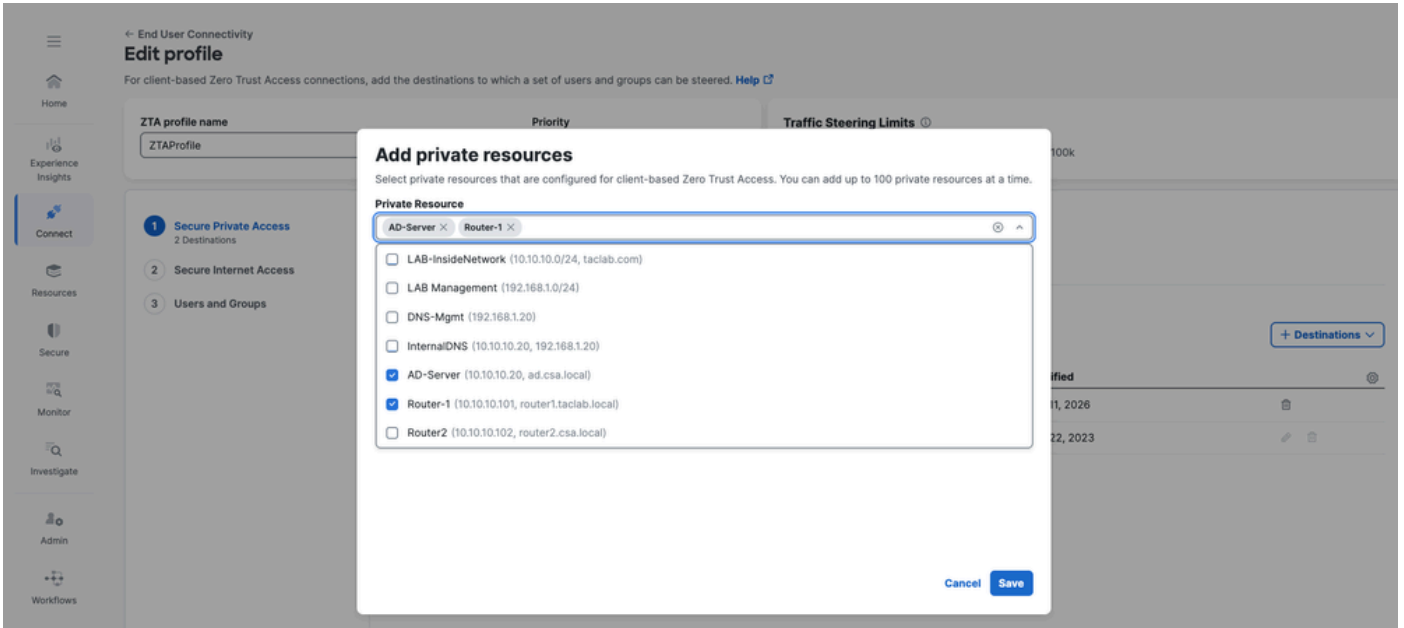
2. Añada el recurso privado

The screenshot shows the 'Create profile' page. The 'Secure Private Access' section is active, showing a search for destinations. The table below lists the destinations and private resources:

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

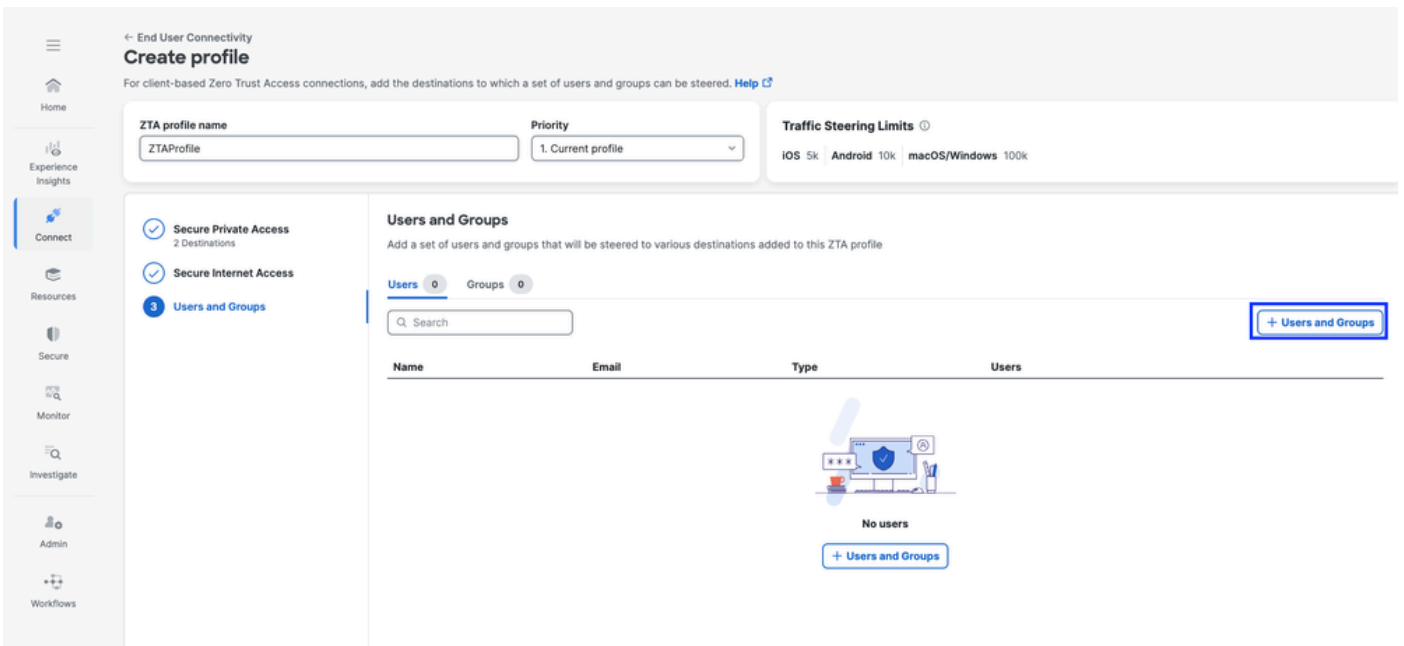
A 'Private Resource' tooltip is visible, explaining that it adds private resources configured for client-based Zero Trust Access.

Acceso seguro - Perfil ZTA



Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos



Acceso seguro - Perfil ZTA

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

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

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

Users: 1 | Groups: 0

Q Search + Users and Groups

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

Rows per page: 10

Back Close

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
```

Secure Access - Prueba de relaciones públicas

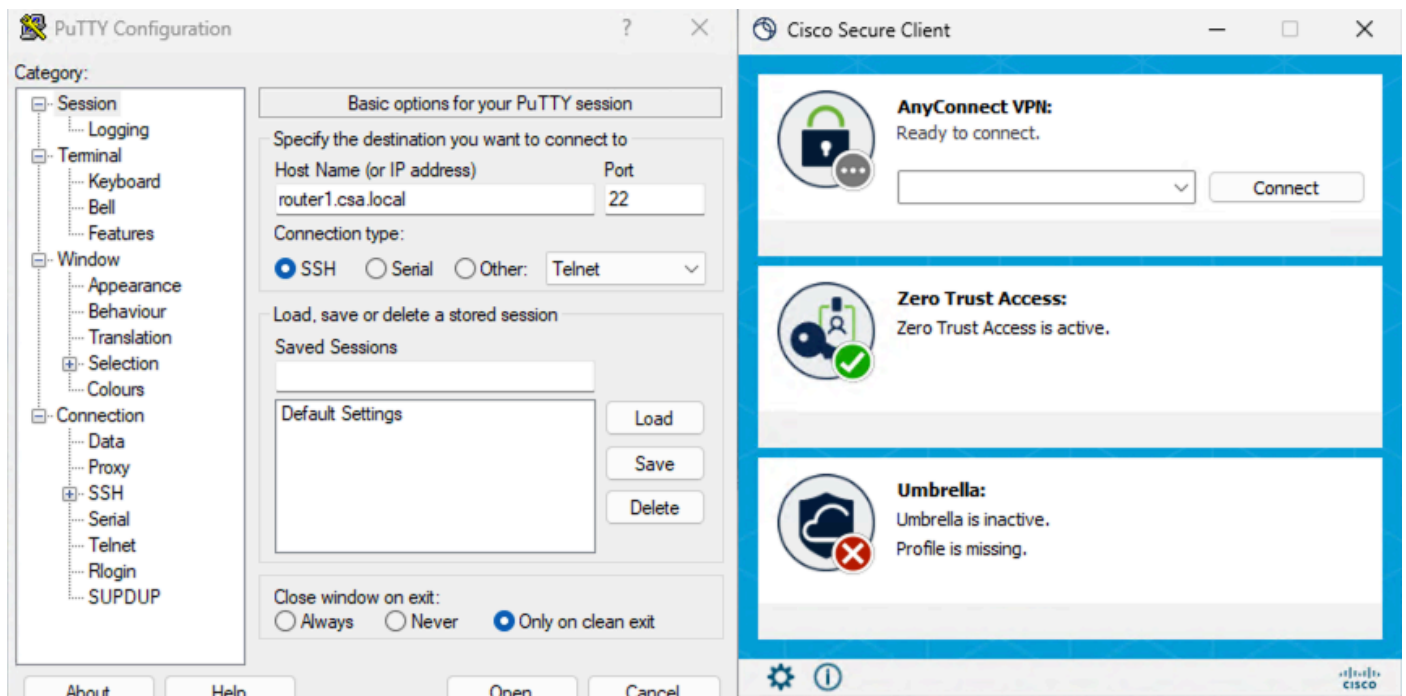
2. Compruebe que FTD puede llegar a un recurso privado mediante FQDN

```
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# █
```

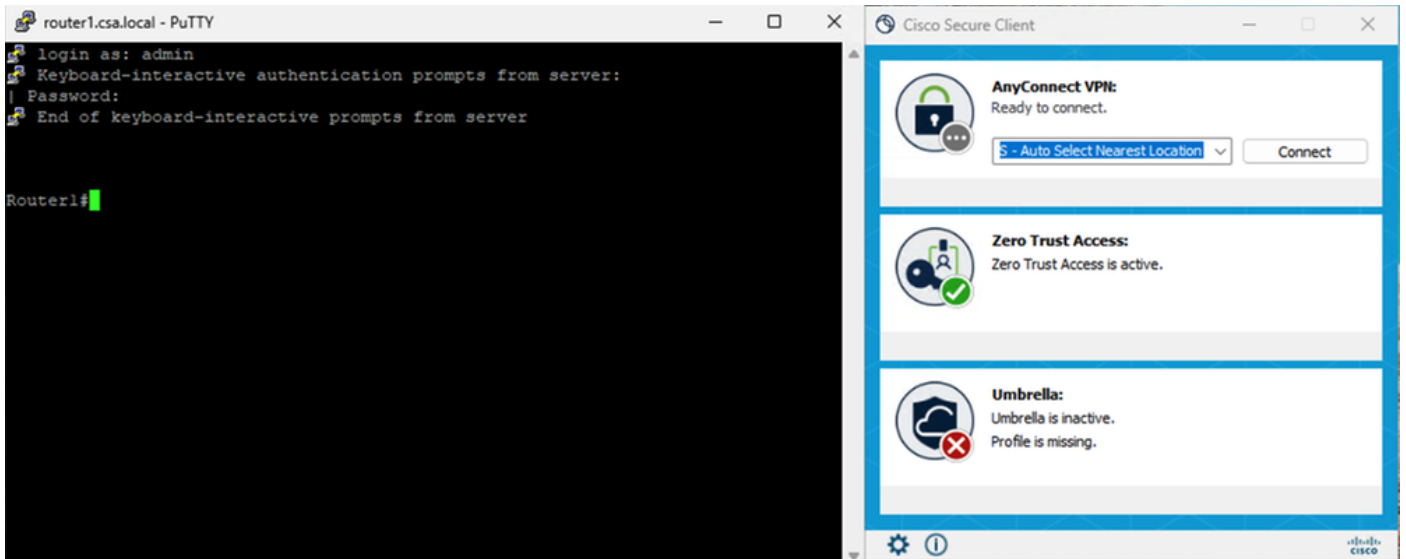
Secure Access - Prueba de relaciones públicas

3. Pruebe la conexión SSH al recurso privado

Acceso al PR mediante FQDN

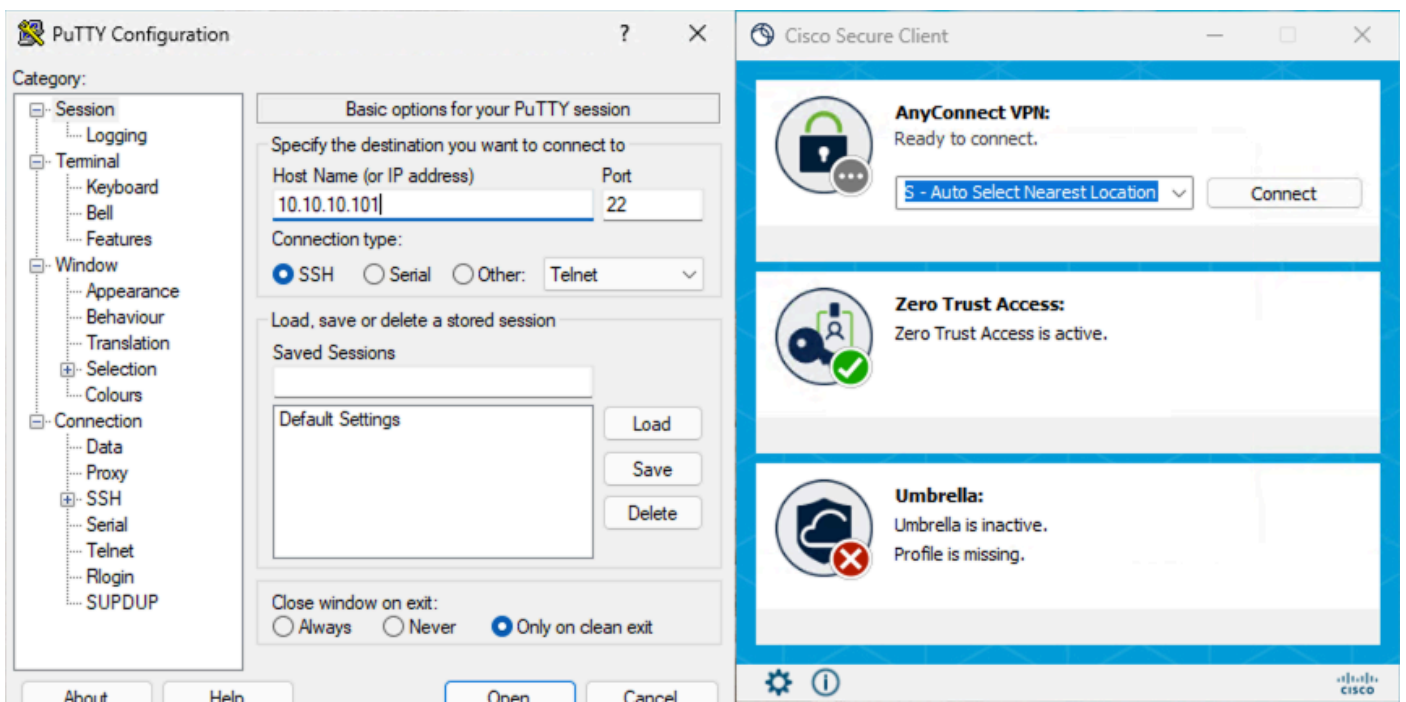


Secure Access - Prueba de relaciones públicas

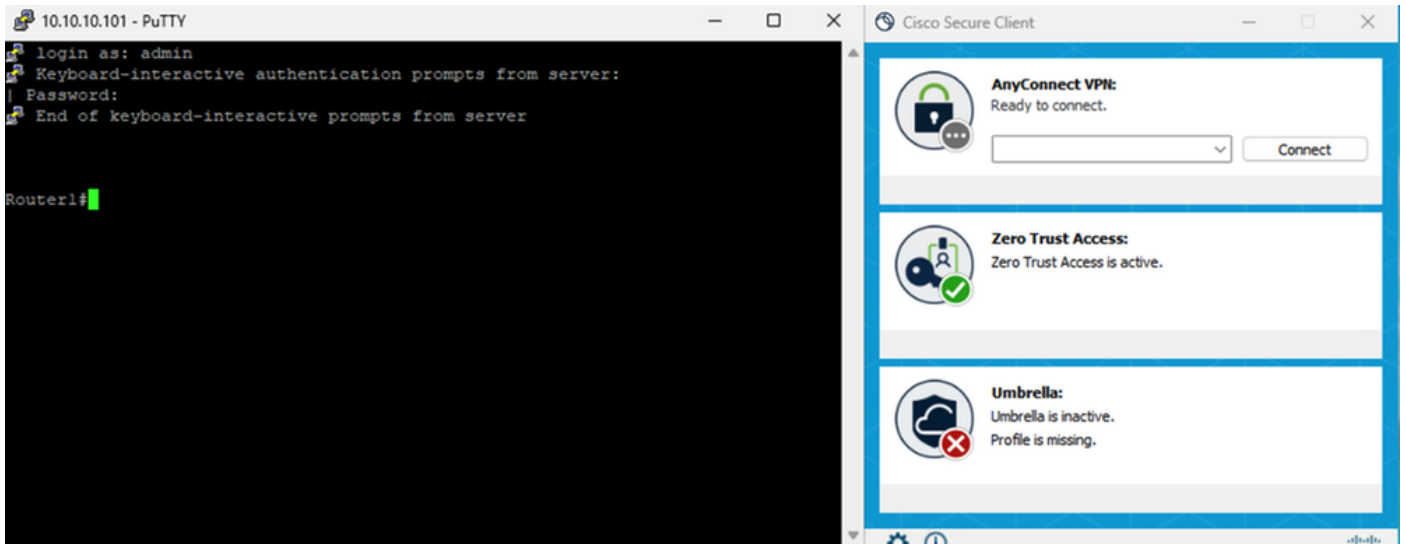


Secure Access - Prueba de relaciones públicas

Acceso al PR mediante la dirección IP



Secure Access - Prueba de relaciones públicas



Secure Access - Prueba de relaciones públicas

4. Verificar registros de búsqueda de actividad de acceso seguro

Activity Search

Filters: Search by domain, identity, or URL. Domain: router1.csa.local, Response: Allowed.

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76

Acceso seguro - Búsqueda de actividad

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

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:55 PM

Access details

Identity: jay (jay@csa.local)

Win: Win10

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD > FMC_FTD

Destination: router1.csa.local

Destination IP: -

Acceso seguro - Búsqueda de actividad

Activity Search

Filters: Search by domain, identity, or URL. Advanced. CLEAR

IP ADDRESS: 10.10.10.101 X RESPONSE: Allowed X

7 Total. Viewing activity from Jan 9, 2026 6:01 PM to Jan 10, 2026 6:01 PM. Page: 1. Results per page: 50. 1 - 7 of 7

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location	Location IP
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...

Acceso seguro - Búsqueda de actividad

7 Total. Viewing activity from Jan 9, 2026 6:09 PM to Jan 10, 2026 6:09 PM. Page: 1. Results per page: 50. 1 - 7 of 7

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Destination Country	Internal IP	External IP	Action	Categories
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22				Allowed	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22				Allowed	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22				Allowed	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22				Allowed	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22				Allowed	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22				Allowed	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101:22	22				Allowed	...

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:56 PM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD> FMC_FTD

Destination: 10.10.10.101

Destination IP: 10.10.10.101

Acceso seguro - Búsqueda de actividad

5. Verificar eventos de conexión FMC

Firewall Management Center - Events & Logs / Analysis / Unified Events

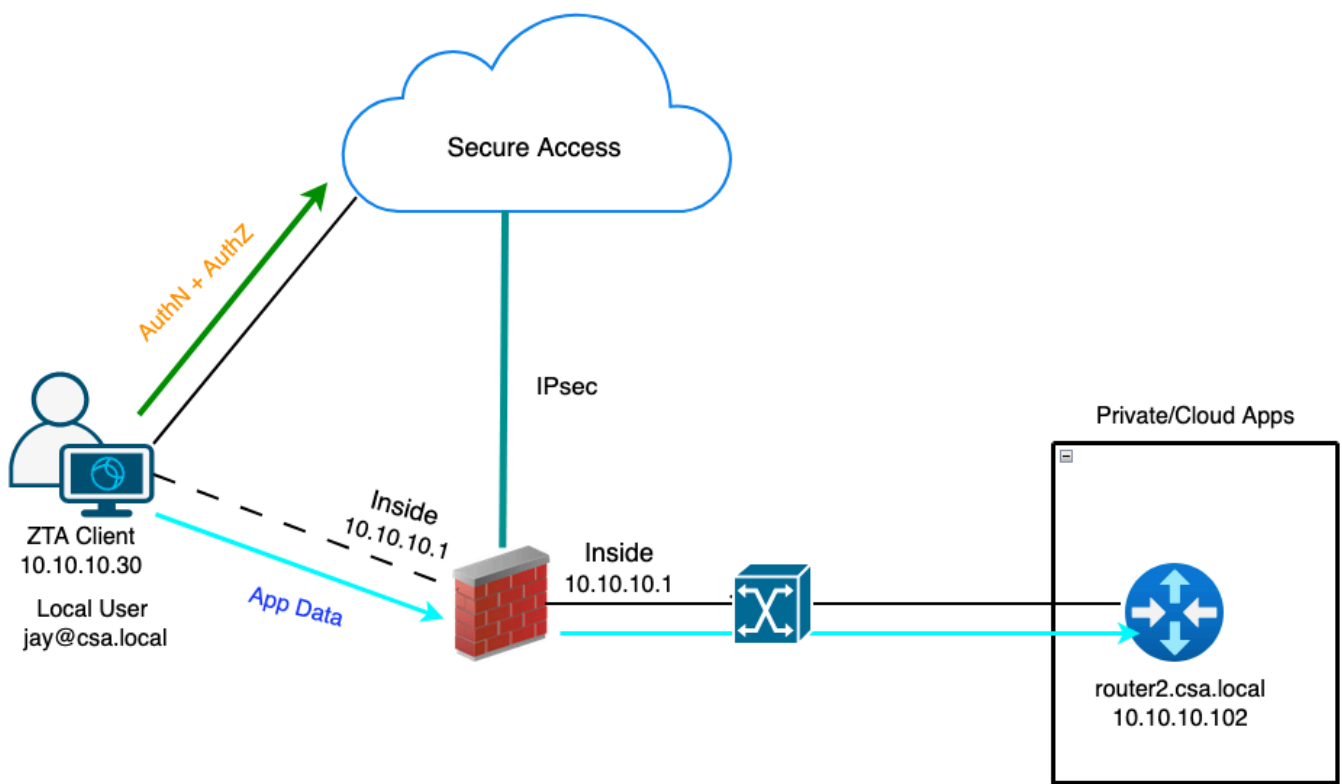
Search: [Destination IP: 10.10.10.101] Refresh

6 events

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Web Application	Access Control Rule	Access Control Policy
2026-01-10 12:56:23	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.101	42217 / tcp	22 (ssh) / tcp			
2026-01-10 12:56:16	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.101	27221 / tcp	22 (ssh) / tcp			
2026-01-10 12:55:28	Connection	Allow	Zero Trust Flow	169.254.1186	10.10.10.101	50425 / tcp	22 (ssh) / tcp			
2026-01-10 12:54:46	Connection	Allow	Zero Trust Flow	169.254.1188	10.10.10.101	39499 / tcp	22 (ssh) / tcp			
2026-01-10 12:50:25	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.101	22631 / tcp	22 (ssh) / tcp			
2026-01-10 12:47:08	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.101	24739 / tcp	22 (ssh) / tcp			

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.

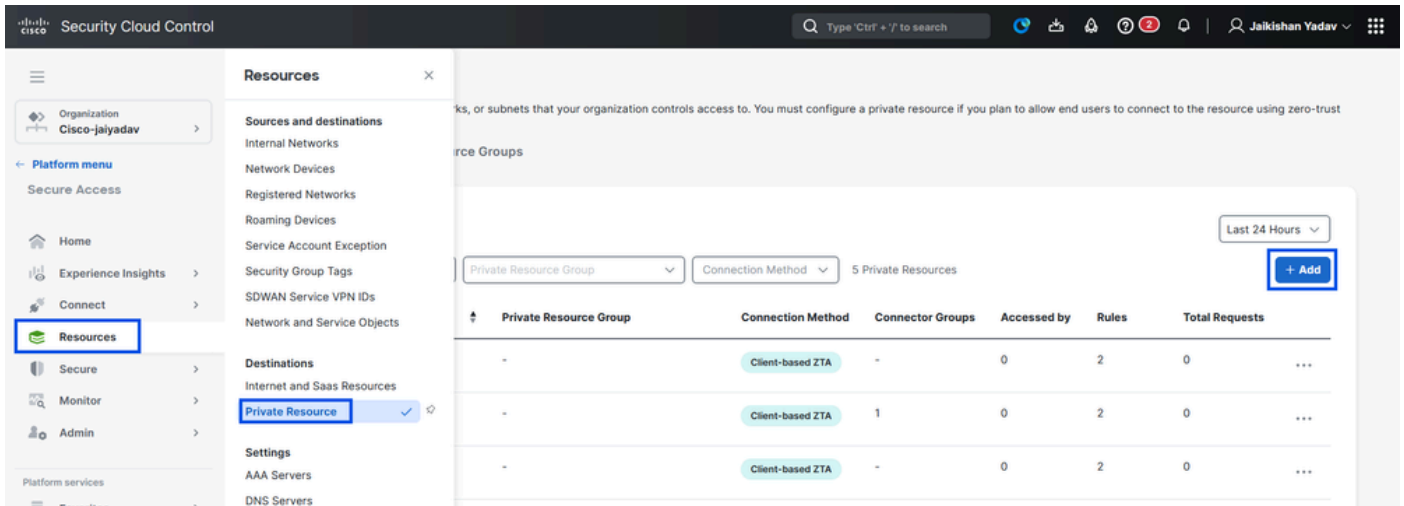


Universal ZTA - Topología de casos de prueba

Paso 1 - Definir un recurso privado en Secure Access

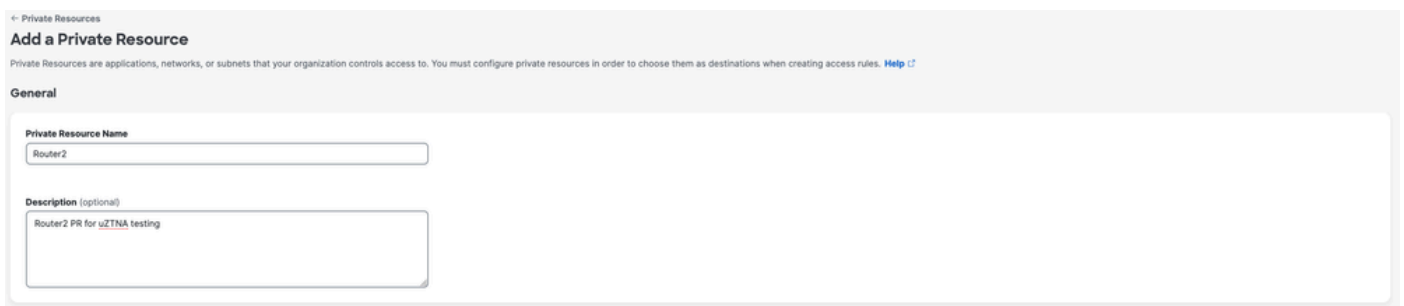
Configure un recurso privado al que se pueda acceder a través del dispositivo inscrito de acceso de confianza cero (ZTA) con aplicación en la nube

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



Acceso seguro - Configuración de recursos privados

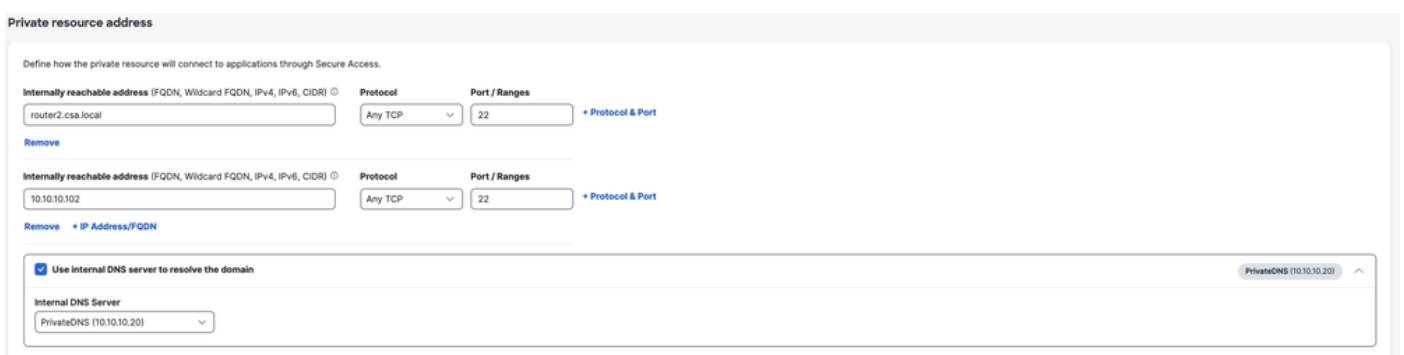
2. En Nombre de Recurso Privado, introduzca un nombre significativo para el recurso. Para Descripción, se recomienda proporcionar información como el propósito del recurso o el nombre del propietario del recurso.



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



Acceso seguro - Configuración de recursos privados

5. Seleccionar métodos de conexión de terminales

6. Seleccione FTD como puntos de aplicación locales

Endpoint Connection Methods

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

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

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

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD ná...
Traffic from users within a trusted network will get enforced at the selected Firewalls.

Enforcement point for Remote User

Remote user — via internet — Local Firewall — Private Resource

Enforcement point for Local user

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

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

Change the remotely reachable addresses

Cancel Save and Test Save

Acceso seguro - Configuración de recursos privados



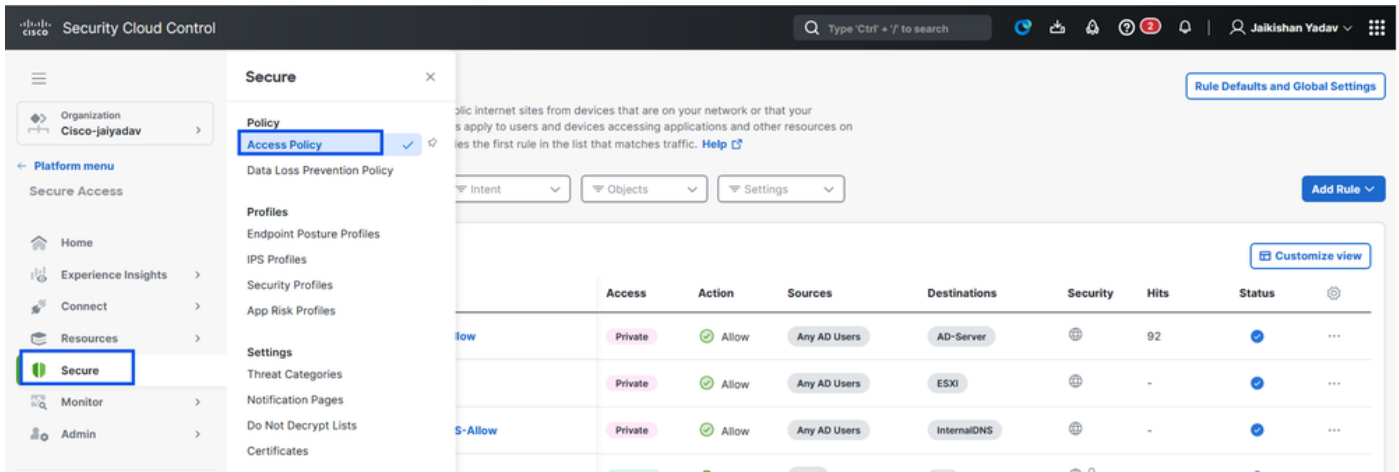
Nota: En función del tipo de inscripción que seleccione, este cambio asociará automáticamente el PR al FTD y activará una implementación de políticas

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](#)

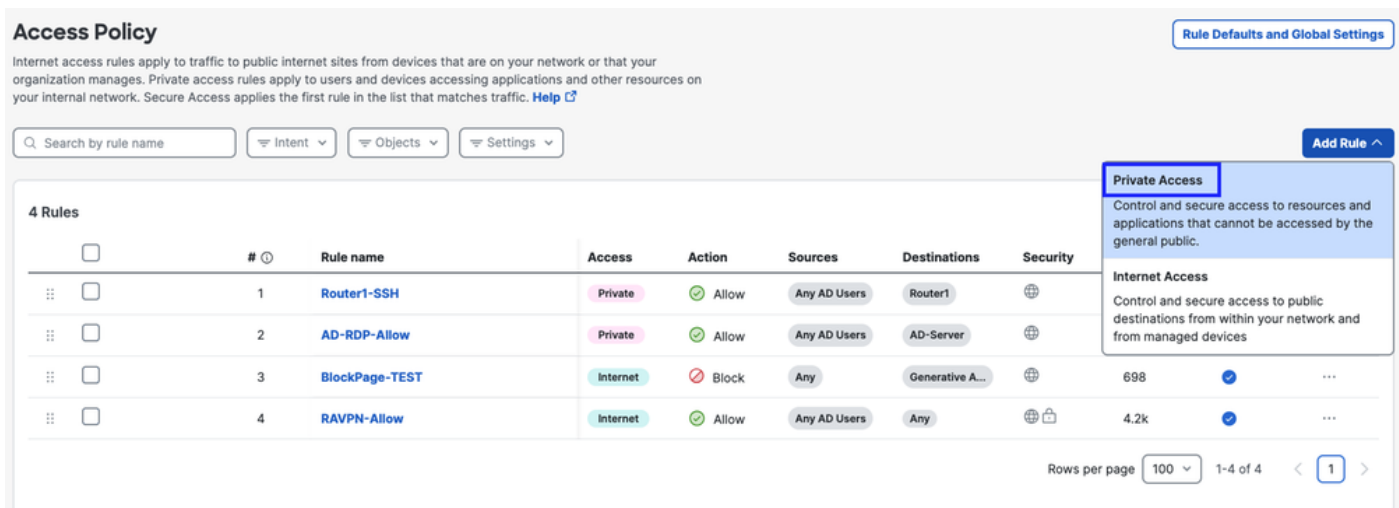
1. Vaya a Seguro > Política de acceso



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

Add Router2-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Acceso seguro - Configuración de la política de acceso

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

Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources

AD Users - Any AD Users

To

Specify one or more destinations

Private Resources - Router2

+ AND

Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile [Rule Defaults](#)
Requirements for end-user devices on which the Cisco Secure Client is installed.
Profile: **None** | Requirements: **None**
Private Resources: **Router2**

For Branch connections:
Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval [Rule Defaults](#) Disabled
Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access.
When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

[Cancel](#) [Back](#) [Next](#)

Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad

1 Specify Access

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

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) [Rule Defaults](#) Disabled
Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile [Rule Defaults](#)
The following security settings will apply to traffic that matches this rule. [Help](#)
Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

[Cancel](#) [Back](#) [Save](#)

Acceso seguro - Configuración de la política de acceso

7. Haga clic en Guardar

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

5 Rules

Customize view

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
<input type="checkbox"/>	1	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2		-	✓	...
<input type="checkbox"/>	2	Router1-SSH	Private	Allow	Any AD Users	Router1		-	✓	...
<input type="checkbox"/>	3	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		40	✓	...
<input type="checkbox"/>	4	BlockPage-TEST	Internet	Block	Any	Generative A...		698	✓	...
<input type="checkbox"/>	5	RAVPN-Allow	Internet	Allow	Any AD Users	Any		4.2k	✓	...

Rows per page 100 1-5 of 5 1

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

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. A 'Connect' dialog box is open, showing 'Essentials' with 'Network Connections' selected. The main content area shows 'FTDs' with a status indicator of '1 Connected' and a 'Warning' icon. Below this, there are filters for 'Region' and 'Status' and a '+ Add' button.

Acceso seguro - Verificación de relaciones públicas

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

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

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

Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local

Auto deployment: Yes

UZTA Configuration status

Synced | Last synced at 12 Jan 2026, at 6:29 AM UTC

Assigned Trusted Network

Trusted network: LAN (Default trusted network) Networks: 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

Acceso seguro - Verificación de relaciones públicas

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. Haga clic en Close (Cerrar)

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

The screenshot displays the 'Network Connections' management interface. On the left, under 'FTDs', a summary shows '1 Synced'. Below this, a table lists 'FTDs configured for Universal Zero Trust Access'. The table has columns for 'FTD Name', 'Version', 'FMC', and 'UZTA Configuration status'. One entry is shown: 'FMC_FTD' with version 'v10.0.0', FMC 'FMC', and a 'Synced' status. A search bar and filters for 'FMC Name' and 'Configuration status' are visible above the table. On the right, a detailed view for 'FMC_FTD' is shown. It includes 'Firewall Details' (Device FQDN: ftd.csa.local, Auto deployment: Yes), 'UZTA Configuration status' (Synced, last synced at 12 Jan 2026, 6:29 AM UTC), 'Assigned Trusted Network' (LAN, 1 DNS Servers), and 'Associated Resources' (2 resources associated by status: Synced).

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

```

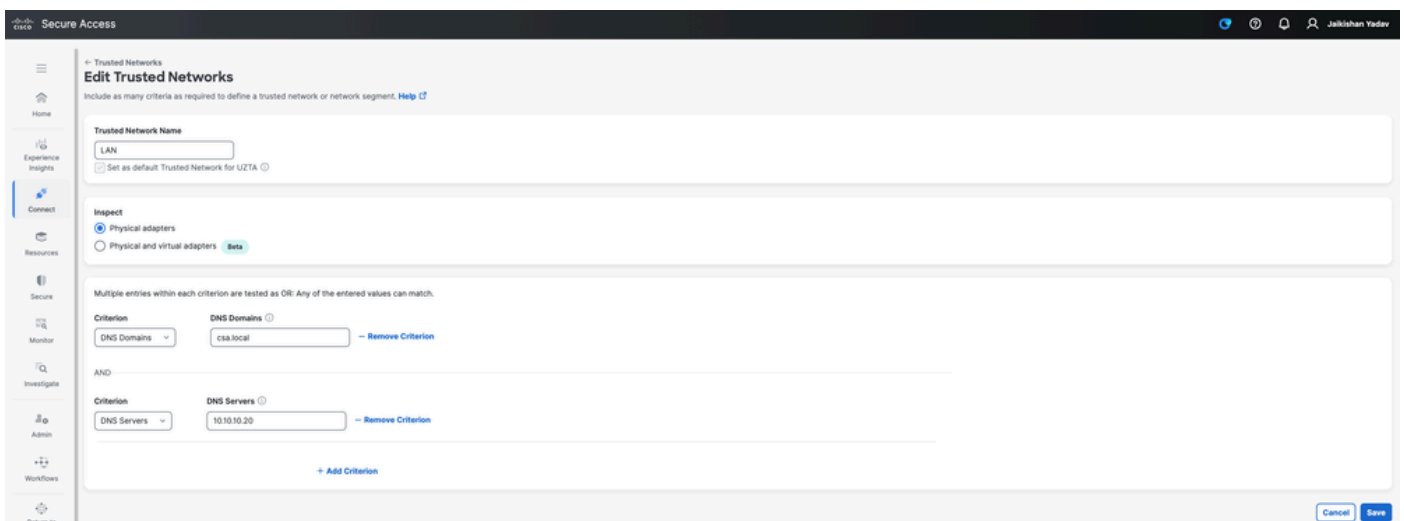
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal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

End User Connectivity

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

Enrollment methods Manage

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

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

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

Edit Delete

Acceso seguro - Perfil ZTA

2. Añada el recurso privado

Create profile

For client-based Zero Trust Access connections, add the destinations to which a set of users and groups can be steered. [Help](#)

ZTA profile name: Priority:

Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

1 Secure Private Access 0 Destinations

2 Secure Internet Access

3 Users and Groups

Secure Private Access

Add the private destinations and private resources to which a set of users and groups can be steered. [Help](#)

[Traffic Steering](#) [Options](#)

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

+ Destinations

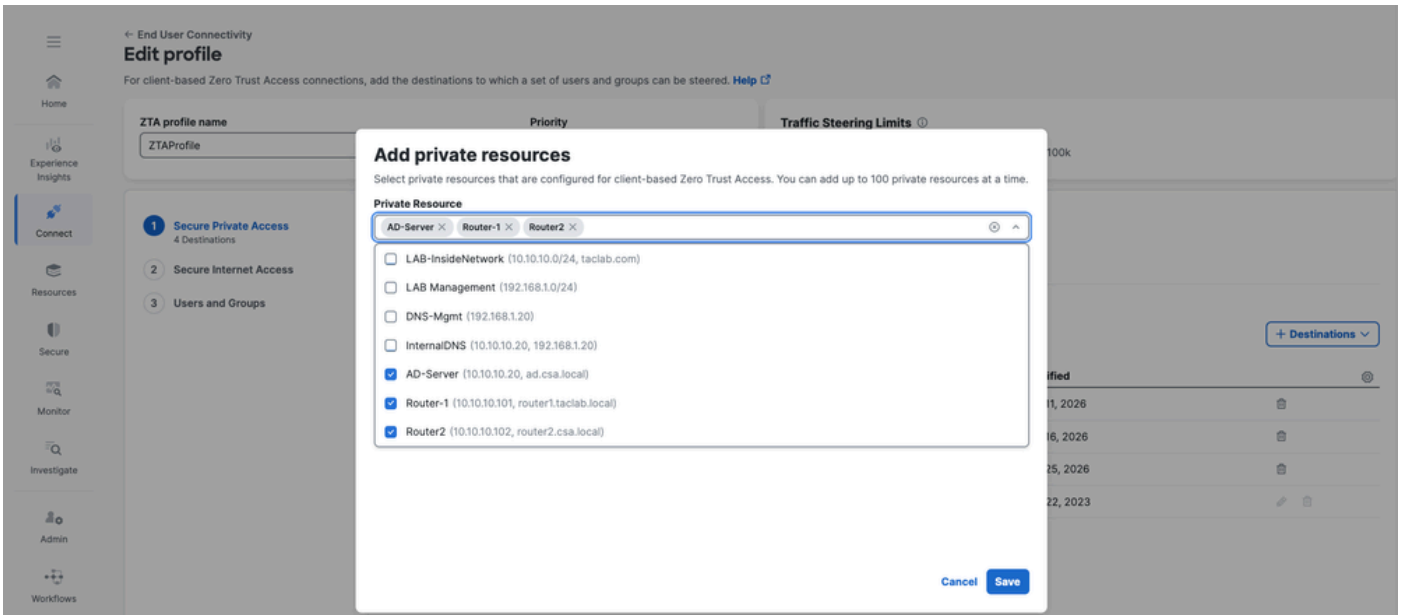
Private Resource

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

Add Destination

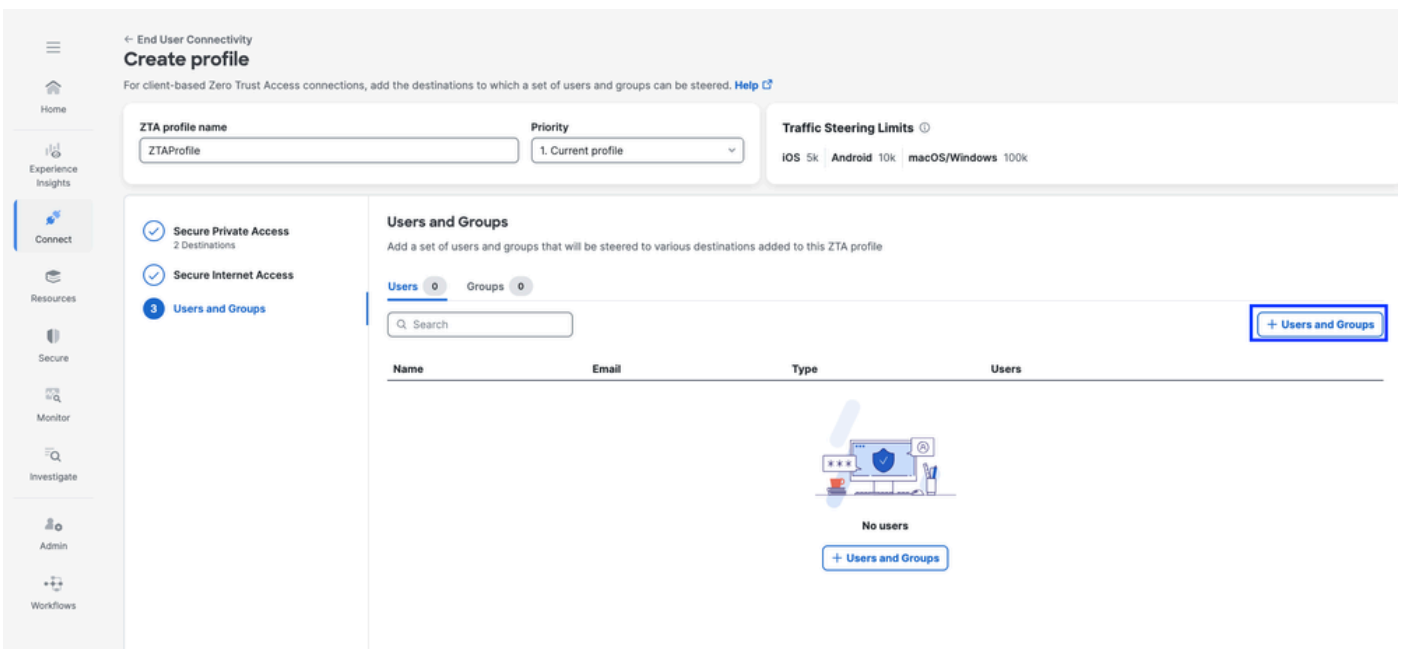
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Acceso seguro - Perfil ZTA



Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos



ZTA profile name: ZTAProfile

Priority: 1. Current profile

Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

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

Users and Groups

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

Users 1 | Groups 0

Q Search + Users and Groups

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

Rows per page: 10 < >

Back Close

Acceso seguro - Perfil ZTA

Paso - 6 Verificar el acceso al recurso privado

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

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

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

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

Below the statistics, there are two expandable sections:

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

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

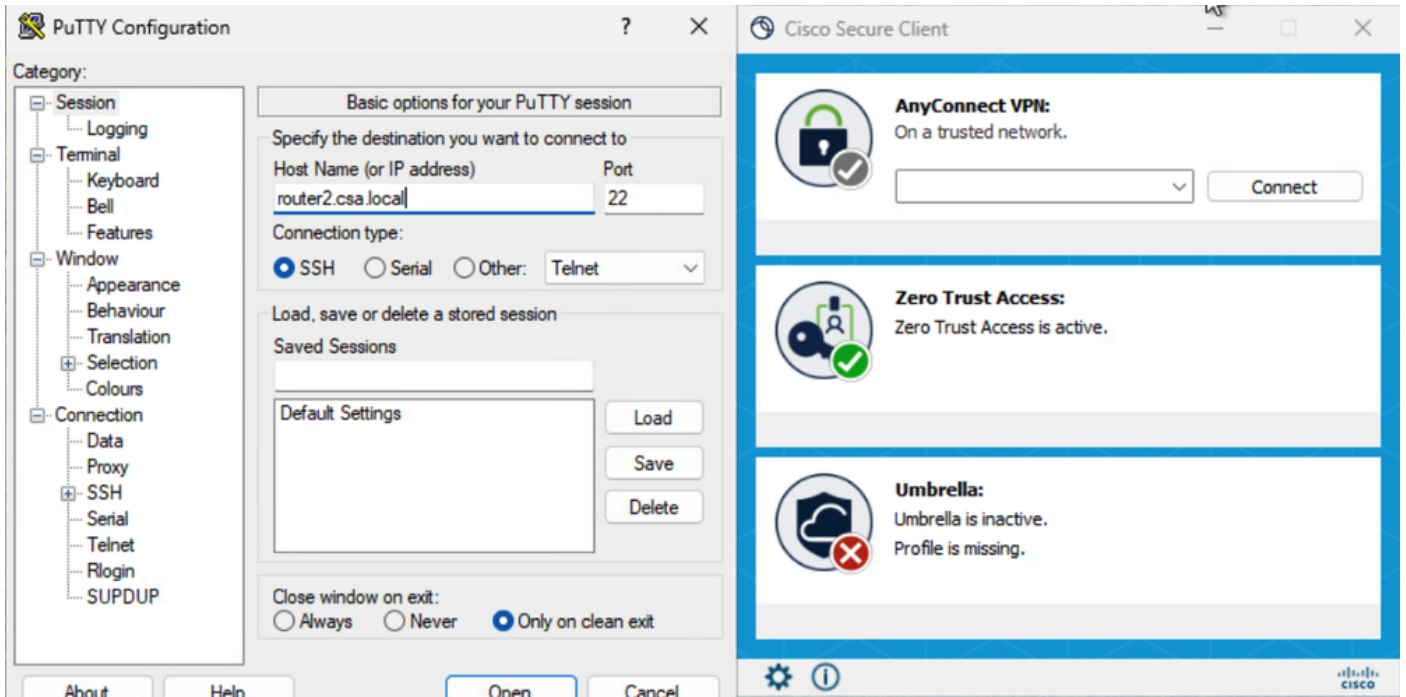
3. Compruebe que FTD puede alcanzar un recurso privado mediante FQDN

```
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# █
```

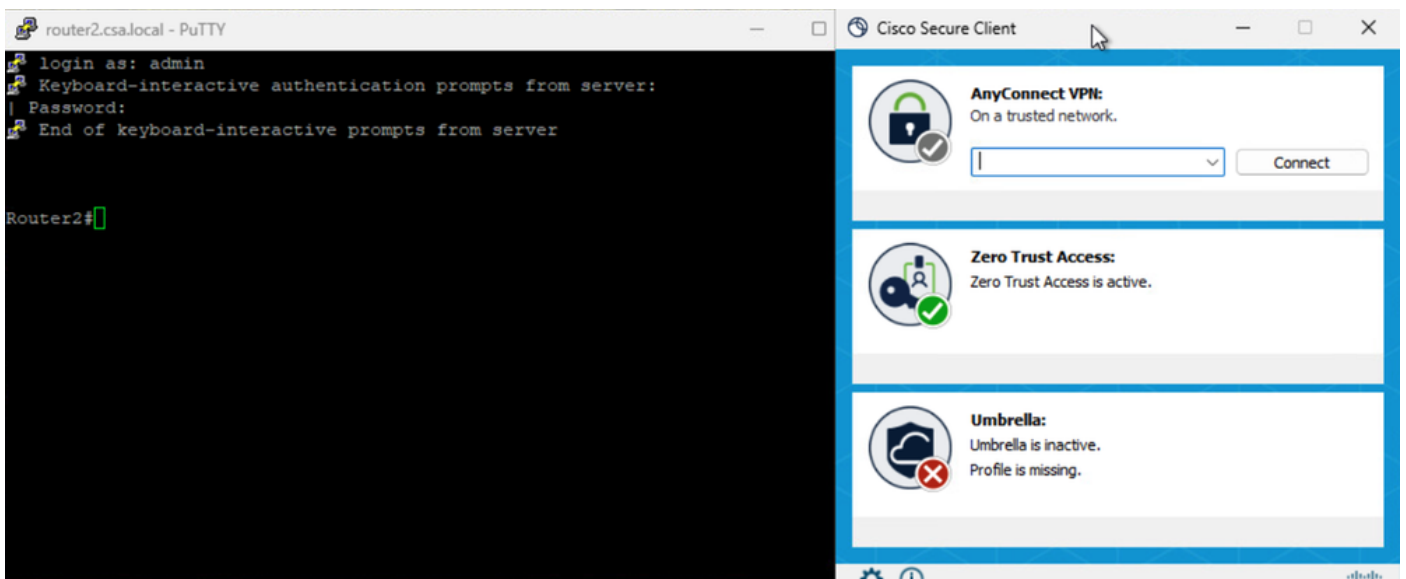
Secure Access - Prueba de relaciones públicas

4. Pruebe la conexión SSH al recurso privado

Acceso al PR mediante FQDN

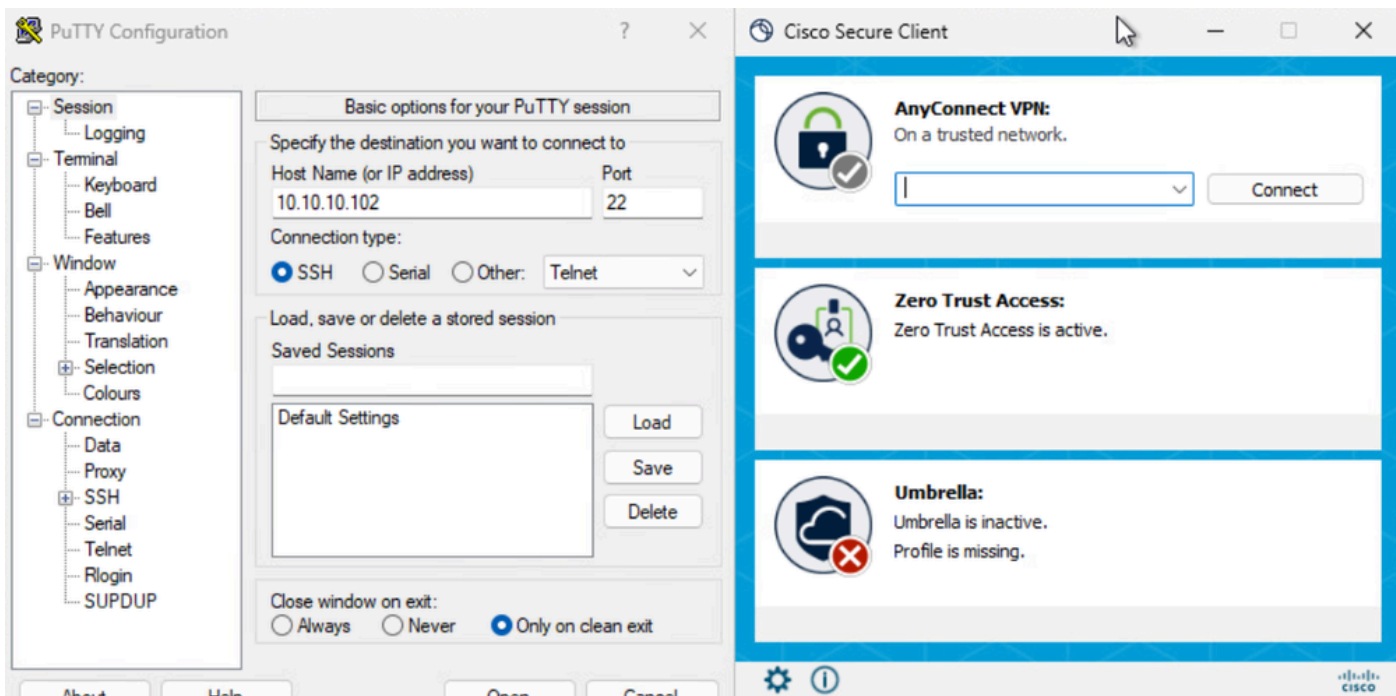


Secure Access - Prueba de relaciones públicas

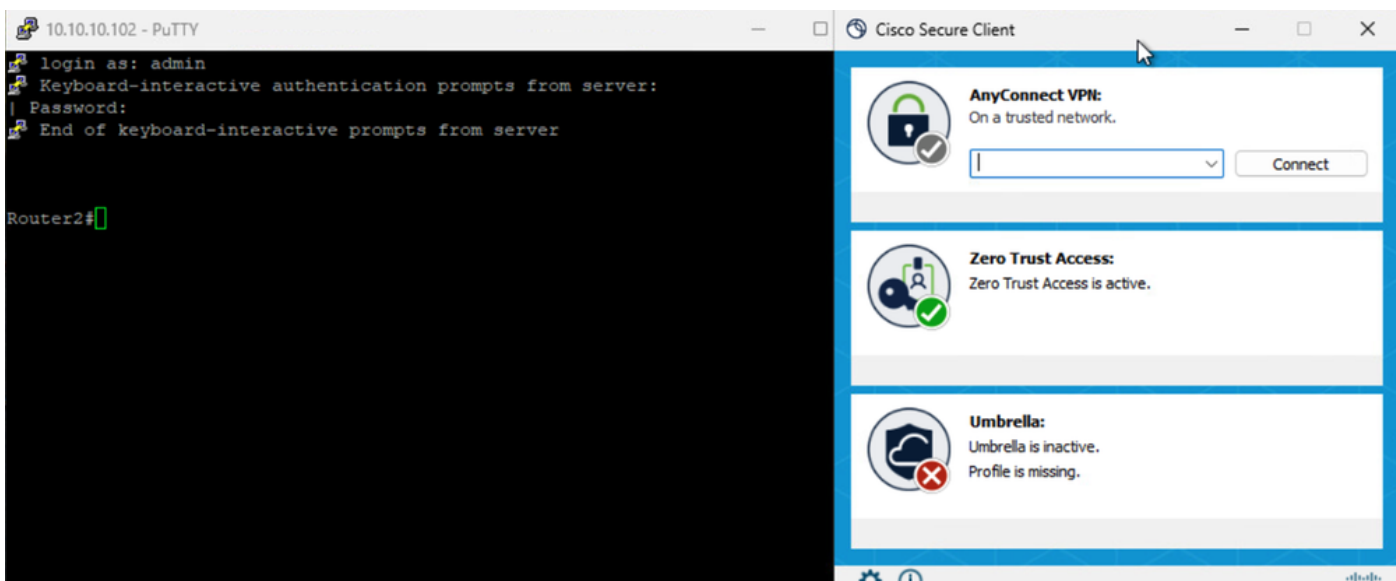


Secure Access - Prueba de relaciones públicas

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

Activity Search

Activity Search interface showing search filters and results for domain router2.csa.local. The search criteria include filters for Response (Allowed, Blocked) and Identity Type (AD Users, AD Groups, AD Devices, SAML Users). The results table displays columns for Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, OS, and Bro.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Bro
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...

Acceso seguro - Búsqueda de actividad

Activity Search

Activity Search interface showing search filters and results for response Allowed. The search criteria include filters for Response (Allowed, Blocked) and Identity Type (AD Users, AD Groups, AD Devices, SAML Users). The results table displays columns for Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/App, and Event Details. The Event Details panel shows information such as Action (Allowed), Block Reason, Connection Method (ZTA Client-based), Time (Feb 23, 2026 3:33 AM), Access details (Identity: jay (jay@csa.local), Rule Name: Router2-SSH-Allow, Resource/Application: Router2, Zero Trust Access Profile: ZTAProfile, Trusted Network: No Match), and Enforcement Point (FTD > FMC_FTD).

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/App	Event Details
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.64	192.168.1.64	7680	Allowed	LAB Manager	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.23	192.168.1.23	7680	Allowed	LAB Manager	...

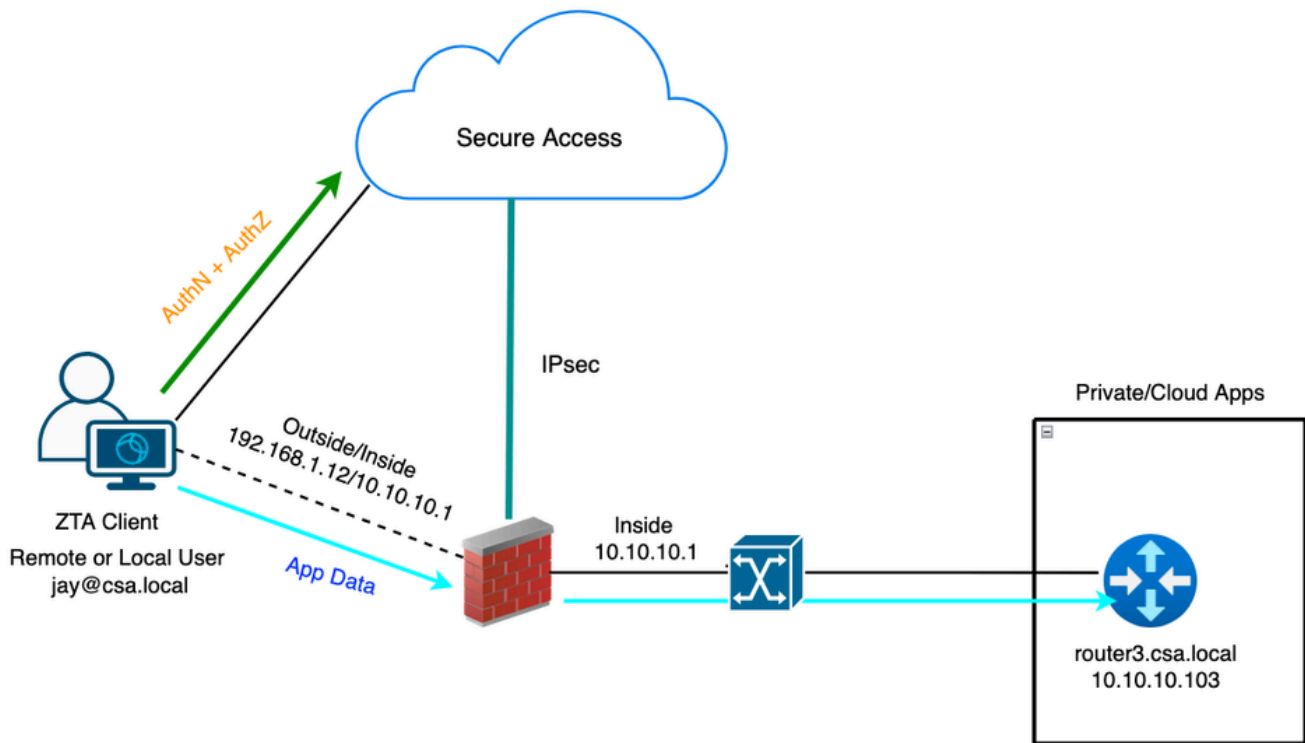
Acceso seguro - Búsqueda de actividad

Activity Search

Activity Search interface showing search filters and results for IP address 10.10.10.102 and response Allowed. The search criteria include filters for IP Address (10.10.10.102) and Response (Allowed, Blocked). The results table displays columns for Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, and Bro.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	Bro
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...

Acceso seguro - Búsqueda de actividad



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

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

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

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.

← Private Resources

Add a Private Resource

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

General

Private Resource Name
Router3

Description (optional)
Router 3 for uZTNA Testing

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

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
router3.csa.local	Any TCP	22	+ Protocol & Port
Remove			
192.168.1.103	Any TCP	22	+ Protocol & Port
Remove			
10.10.10.103	Any TCP	22	+ Protocol & Port
Remove + IP Address/FQDN			

Use internal DNS server to resolve the domain LabDNS (192.168.1.20, 10.10.10.20) ▼

Acceso seguro - Configuración de recursos privados

5. Seleccionar métodos de conexión de terminales

6. Seleccione FTD como puntos de aplicación locales

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

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

FMC_FTD (ftd.csa.local) ✓

Will get enforced at the selected firewalls.

Local-only

Enforcement point for Remote User

Remote user

Secure Access Cloud

Private Resource



via Internet



Enforcement point for Local user

User in a trusted network

Local Firewall

Private Resource



via local network



Cancel

Save and Test

Save

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).

Resource Connector Groups

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

For more information, see [Help](#)

Resource Connector Groups (optional) ⓘ

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

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

Acceso seguro - Configuración de recursos privados



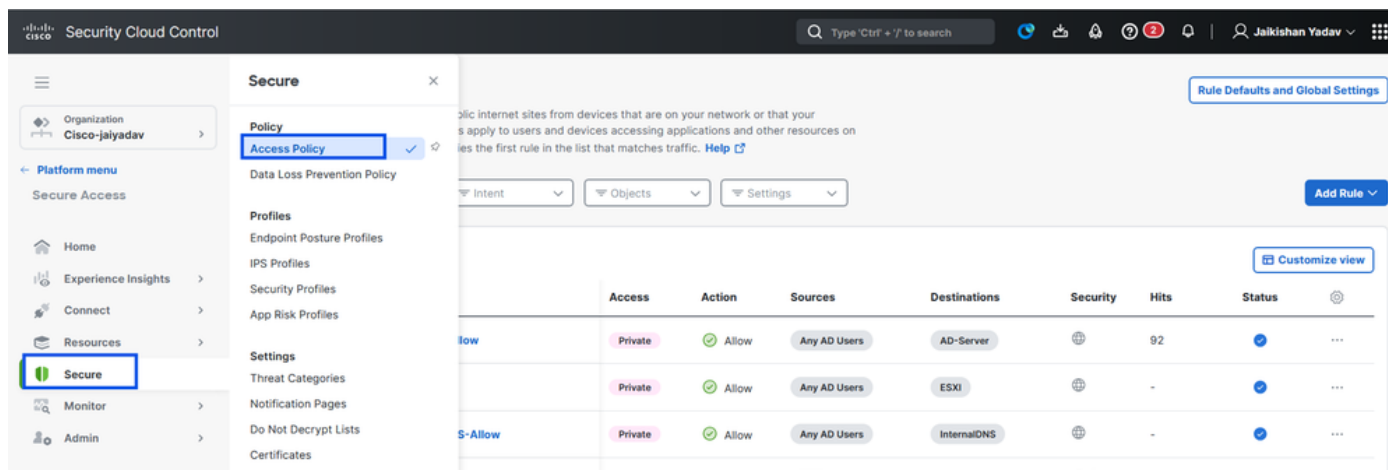
Nota: En función del tipo de inscripción que seleccione, este cambio asociará automáticamente el PR al FTD y activará una implementación de políticas

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](#)

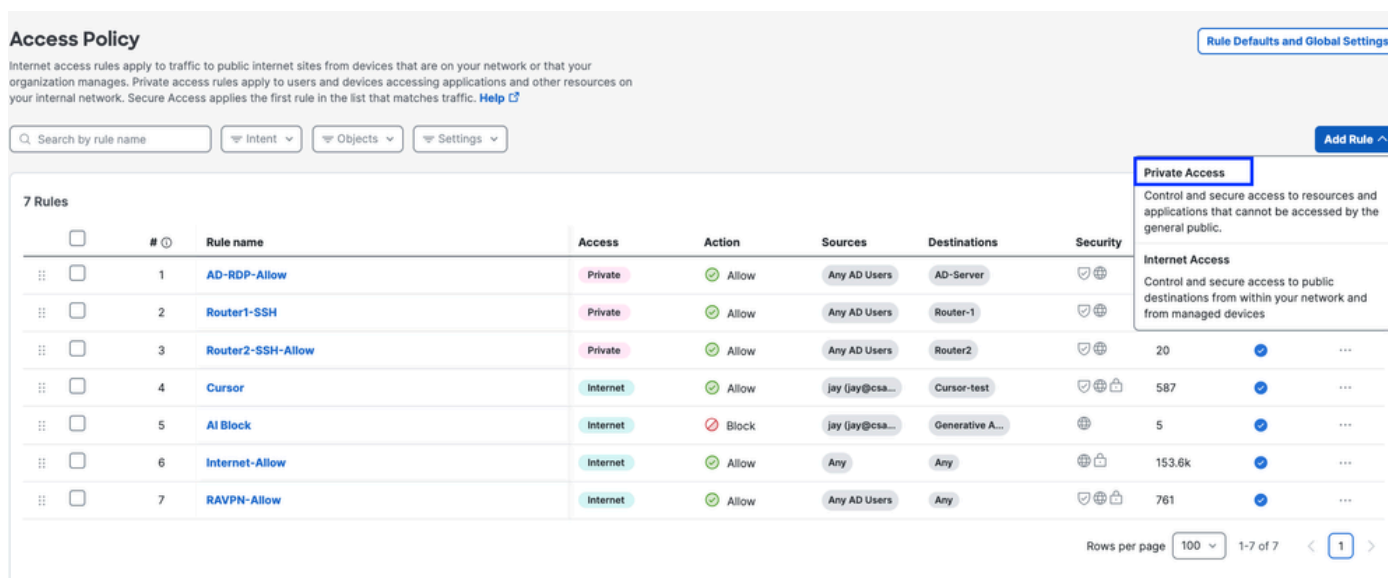
1. Vaya a Seguro > Política de acceso



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

Add Router3-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Acceso seguro - Configuración de la política de acceso

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

Rule name Rule order

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From To

+ AND

Acceso seguro - Configuración de la política de acceso

5. Configurar requisitos de terminales

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile [Rule Defaults](#)
Requirements for end-user devices on which the Cisco Secure Client is installed.
Profile: **None** | Requirements: **None**
Private Resources: **Router3**

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

User Authentication Requirements

Zero Trust Access: User Authentication Interval [Rule Defaults](#) Disabled
Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. [Help](#)

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Cancel

[Back](#) [Next](#)

Acceso seguro - Configuración de la política de acceso

6. Configurar seguridad

Specify Access

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

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) [Rule Defaults](#) Disabled
Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile

[Rule Defaults](#)

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

Cancel

[Back](#) [Save](#)

Acceso seguro - Configuración de la política de acceso

7. Haga clic en Guardar

Access Policy Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings Add Rule

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

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

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

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

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

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Syncing

0 Synced

FTDs configured for Universal Zero Trust Access

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

Configuration changes are being processed

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

1 FTDs

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

FMC_FTD ✕

Firewall Details ^

Device FQDN: ftd.csa.local 🔗

Auto deployment: Yes

UZTA Configuration status ^

Syncing

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

Assigned Trusted Network ^

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

[Edit assignment](#)
+ Trusted network

Associated Resources 3 ^

RESOURCES ASSOCIATED BY STATUS

Status	Count
Synced	3

[View resources associated to this FTD](#)

[Associate Resources](#)

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
```

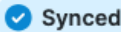
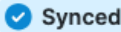
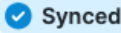
```
Addresses: 192.168.1.12
```

Acceso seguro - Verificación de relaciones públicas

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

Search by resource name Configuration status 3 Resources [Associate Resources](#)

Resource name	Status
Router-1	 Synced
Router2	 Synced
Router3	 Synced

Close

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

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local
Auto deployment: Yes

UZTA Configuration status

Synced Last synced at 23 Feb 2026, at 5:08 AM UTC

Assigned Trusted Network

Trusted network: **LAN** (Default trusted network)
1 DNS Domains 1 DNS Servers

Edit assignment + Trusted network

Associated Resources (3)

RESOURCES ASSOCIATED BY STATUS

Status

Synced 3

View resources associated to this FTD

Associate Resources

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

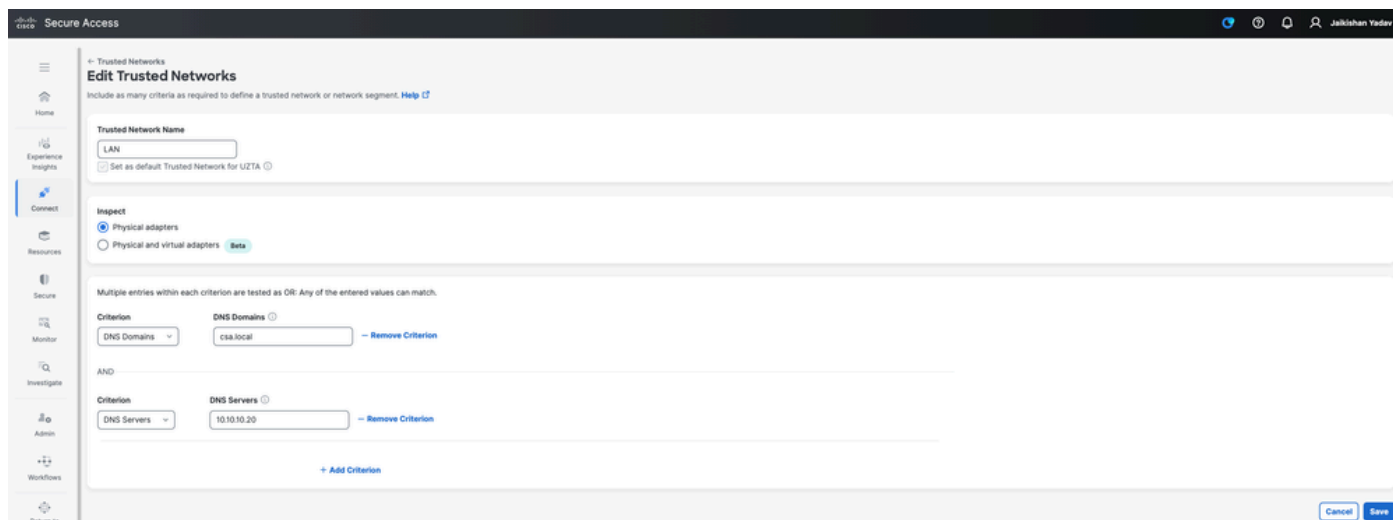
show running-config object application

```
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"

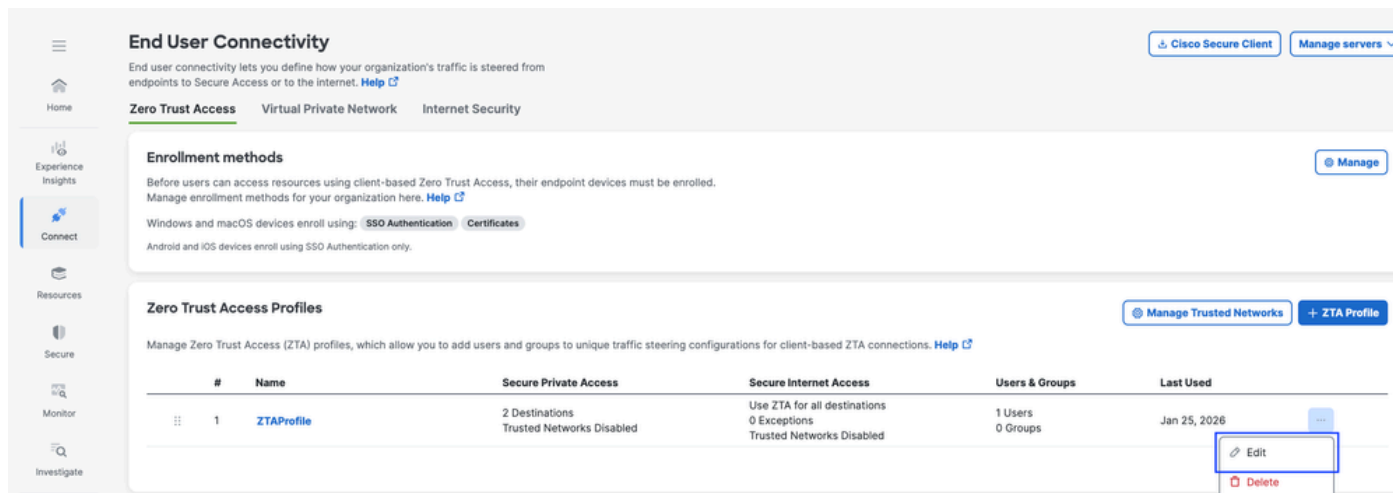
Vaya a Connect > End User Connectivity > Zero Trust Access > ZTA Settings y configure Trusted Networks



Acceso seguro - Configuración de ZTA TND

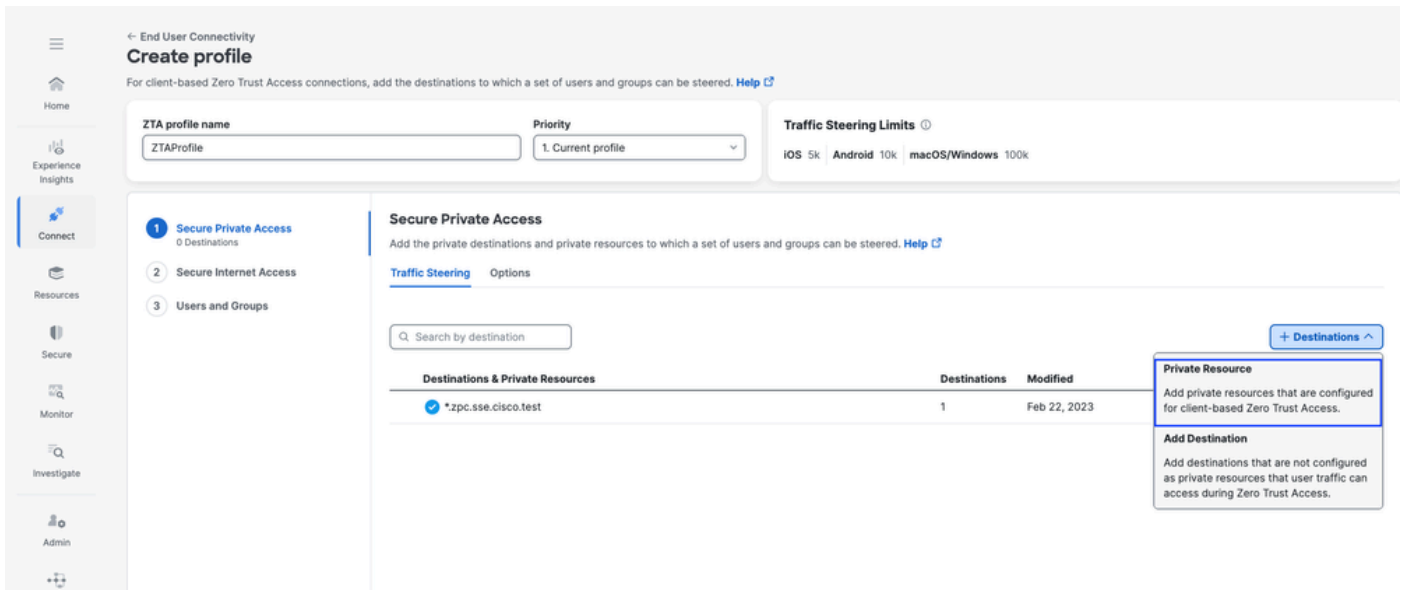
Paso - 5 Agregar un recurso privado al perfil ZTA

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

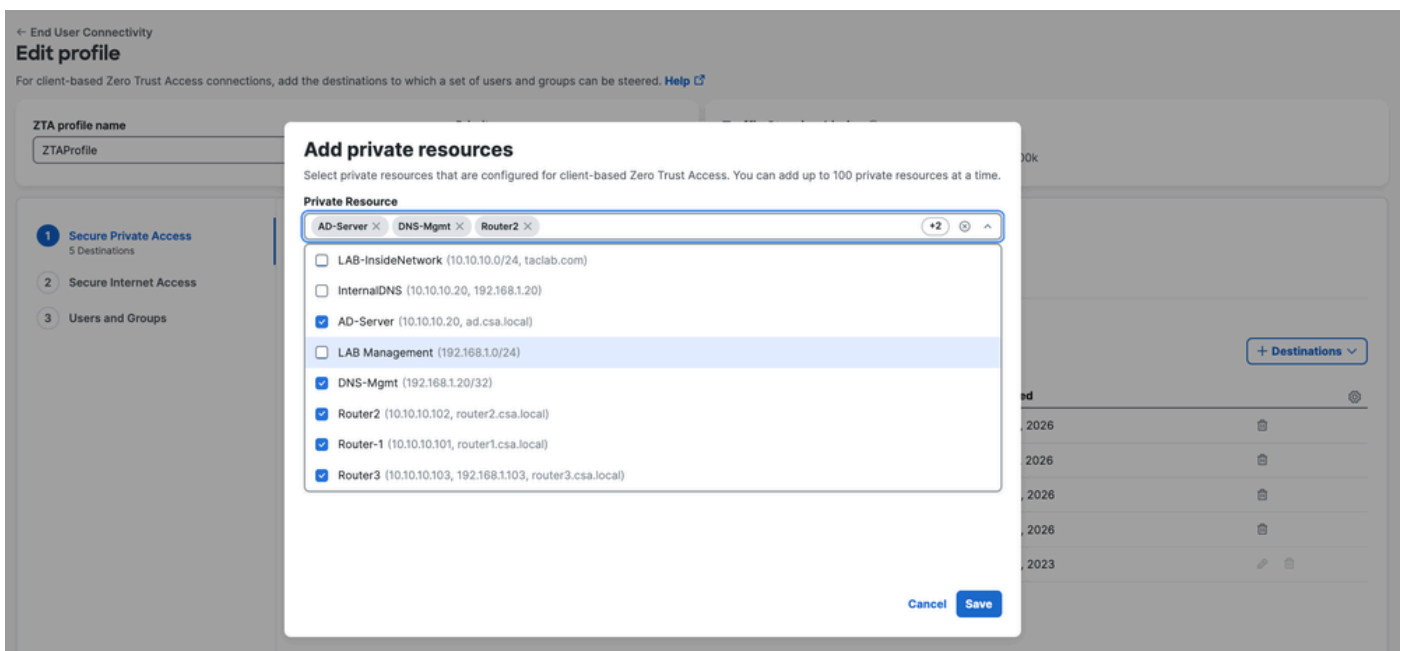


Acceso seguro - Perfil ZTA

2. Añada el recurso privado

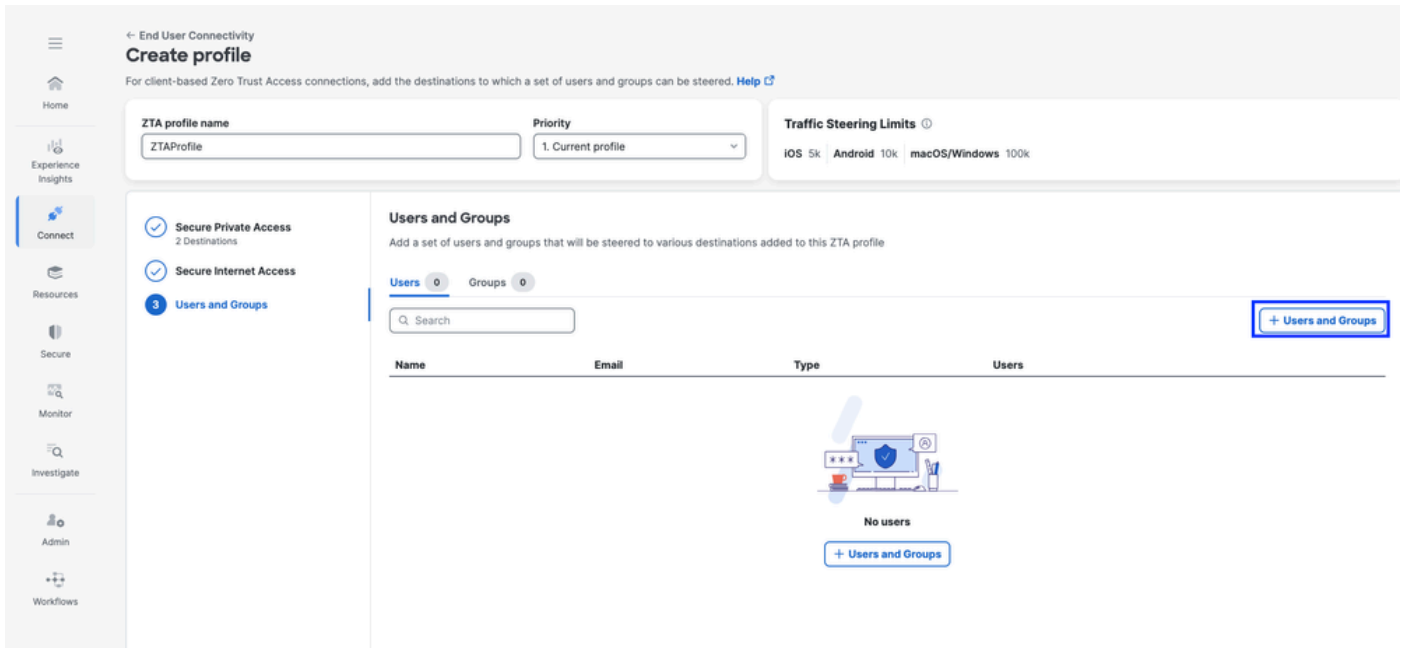


Acceso seguro - Perfil ZTA

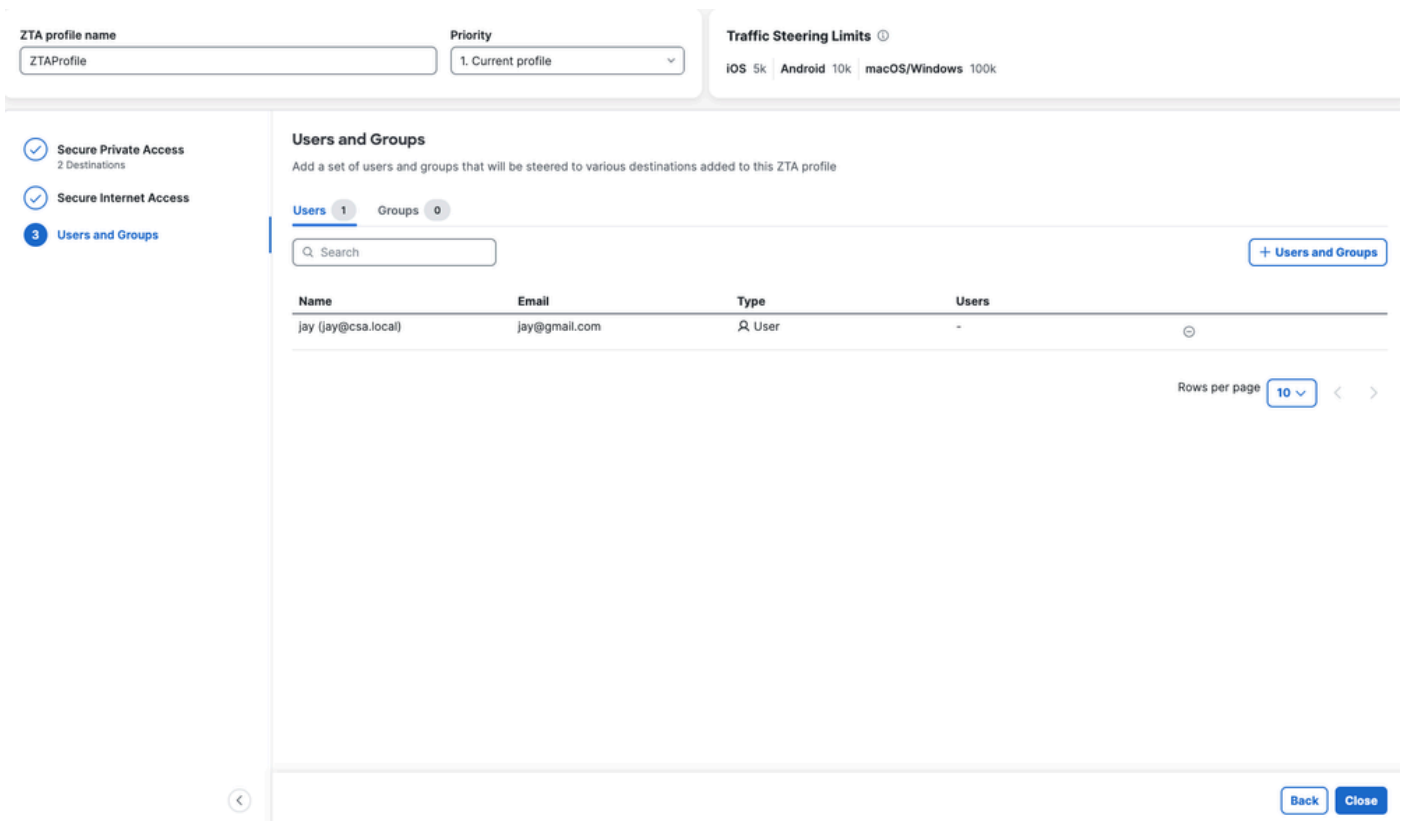


Acceso seguro - Perfil ZTA

3. Agregar usuarios y grupos



Acceso seguro - Perfil ZTA

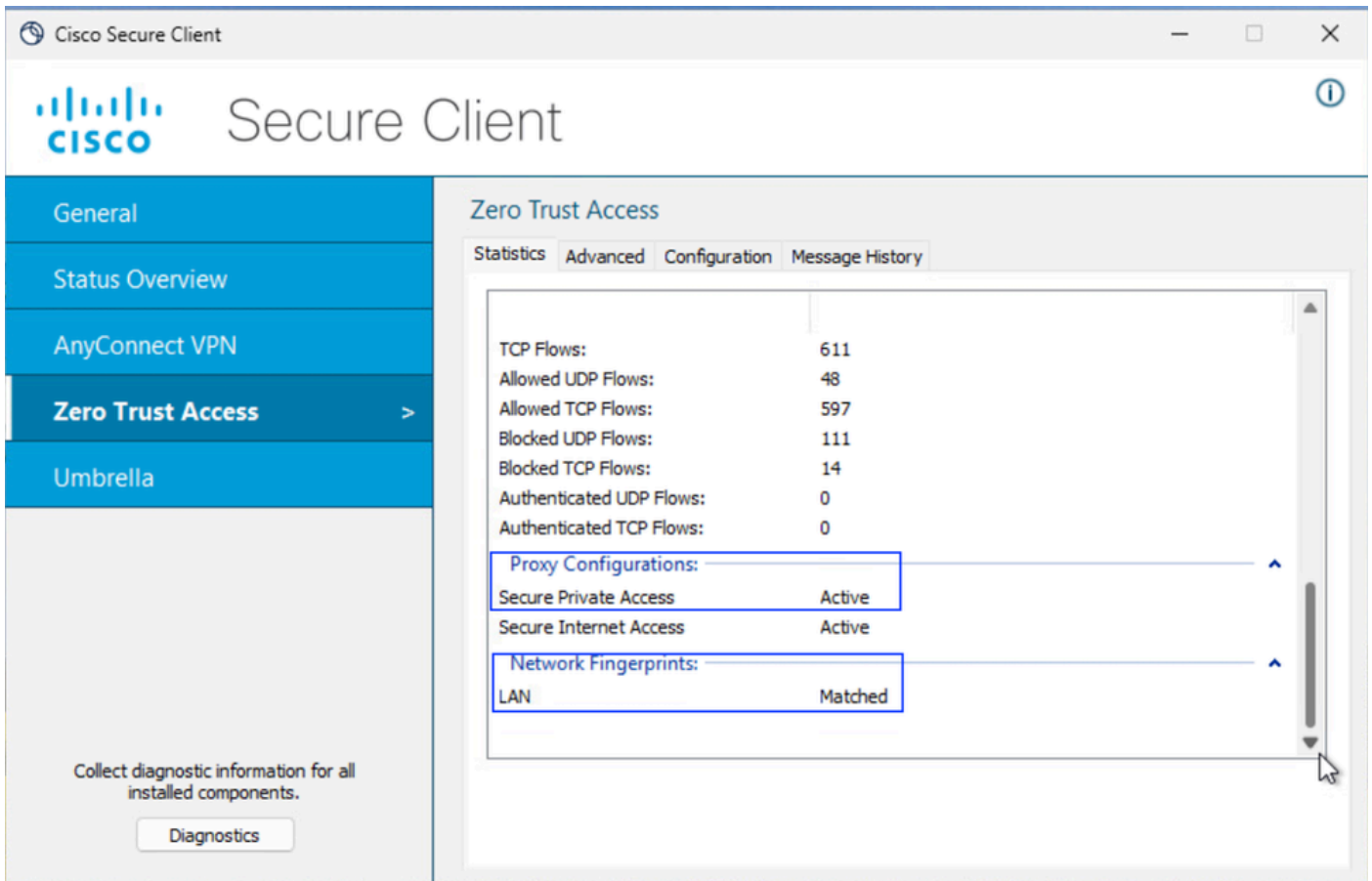


Acceso seguro - Perfil ZTA

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

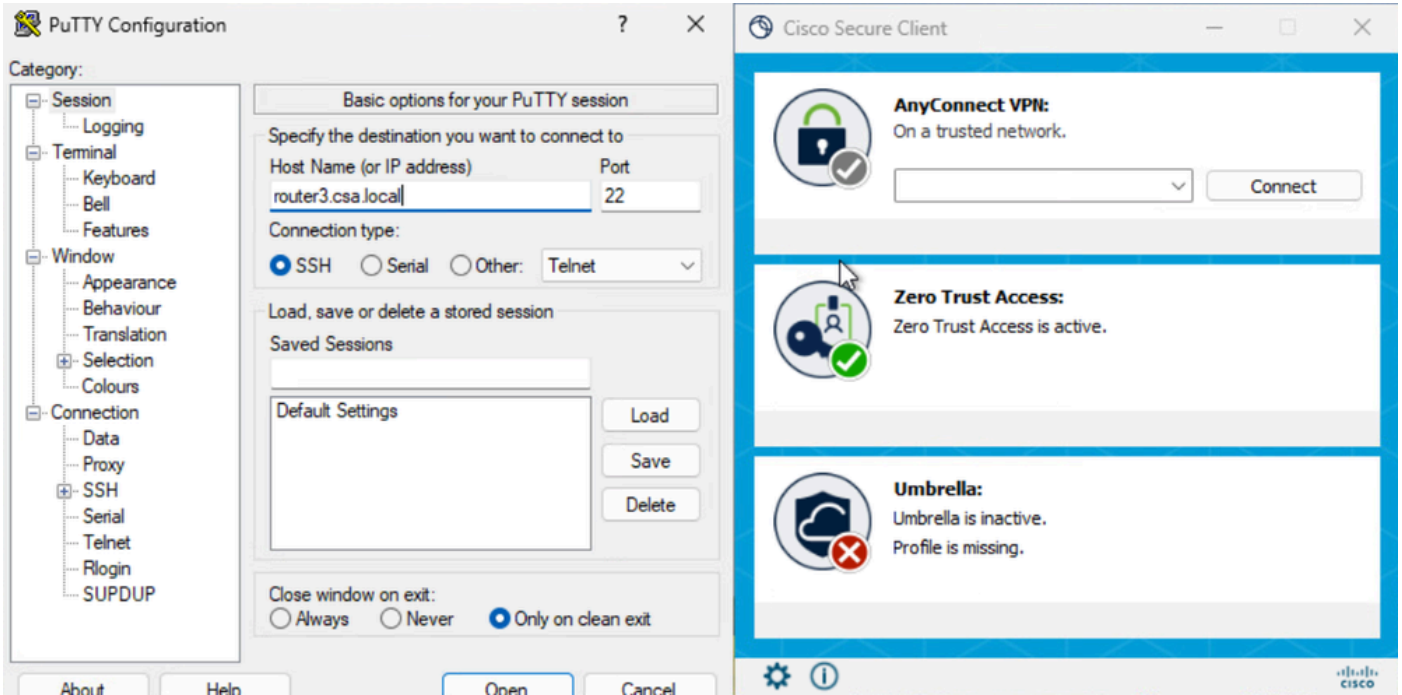
3. Compruebe que FTD puede alcanzar un recurso privado mediante FQDN

```
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# █
```

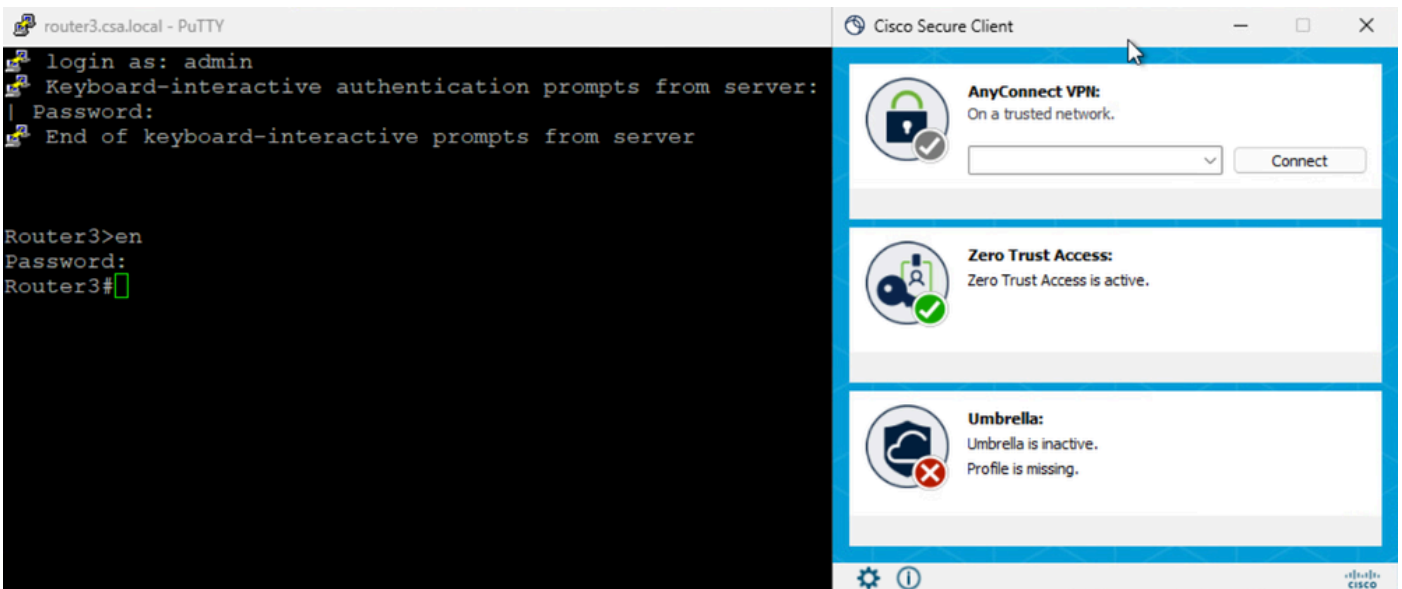
Secure Access - Prueba de relaciones públicas

4. Pruebe la conexión SSH al recurso privado

Acceso al PR mediante FQDN

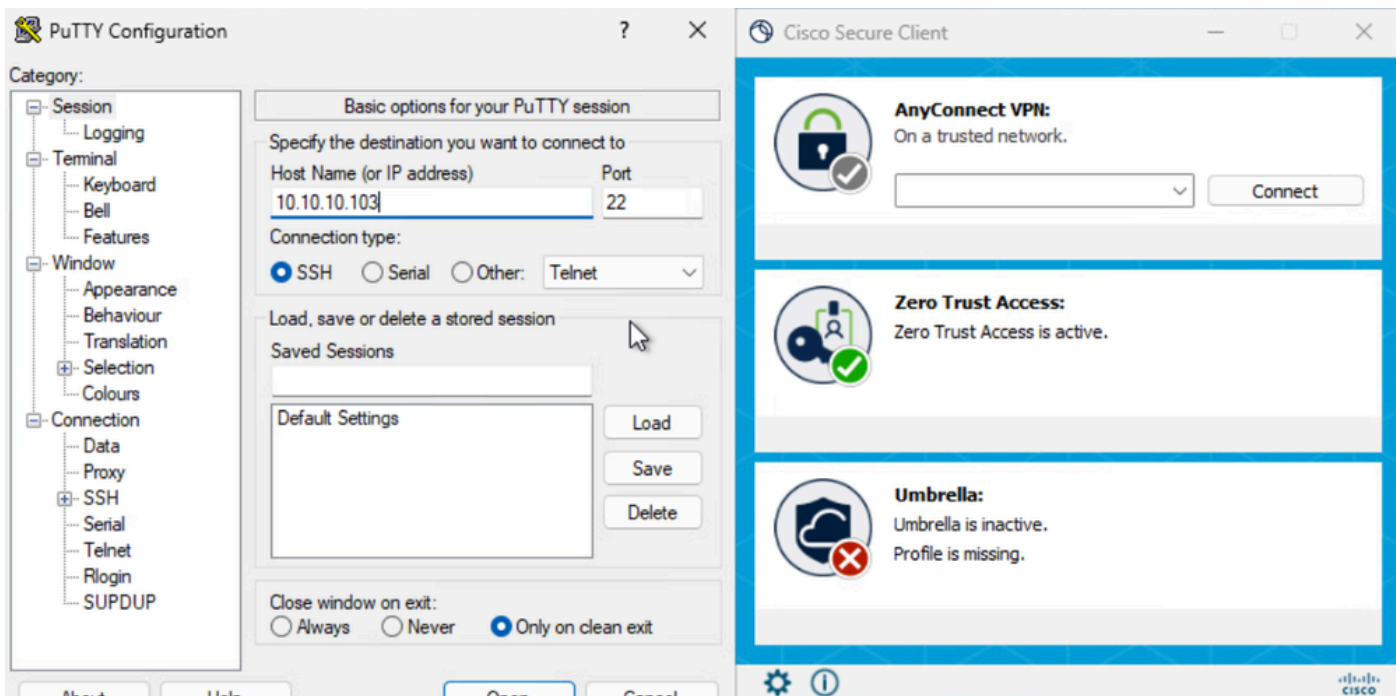


Secure Access - Prueba de relaciones públicas

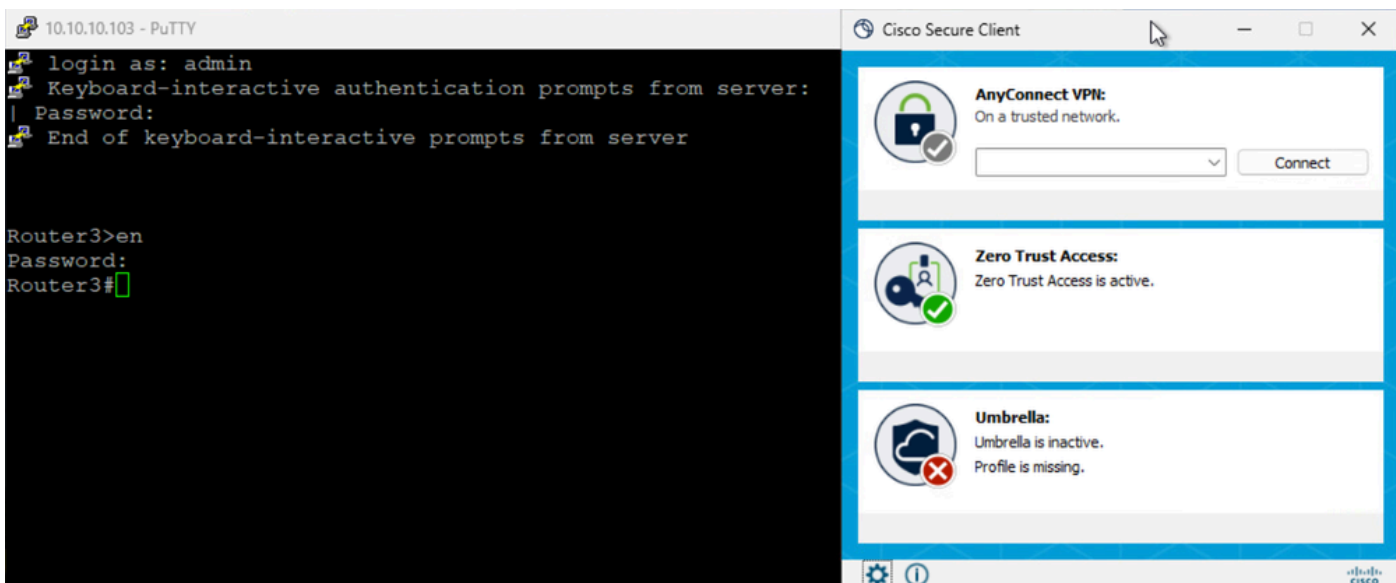


Secure Access - Prueba de relaciones públicas

Acceso al PR mediante la dirección IP



Secure Access - Prueba de relaciones públicas

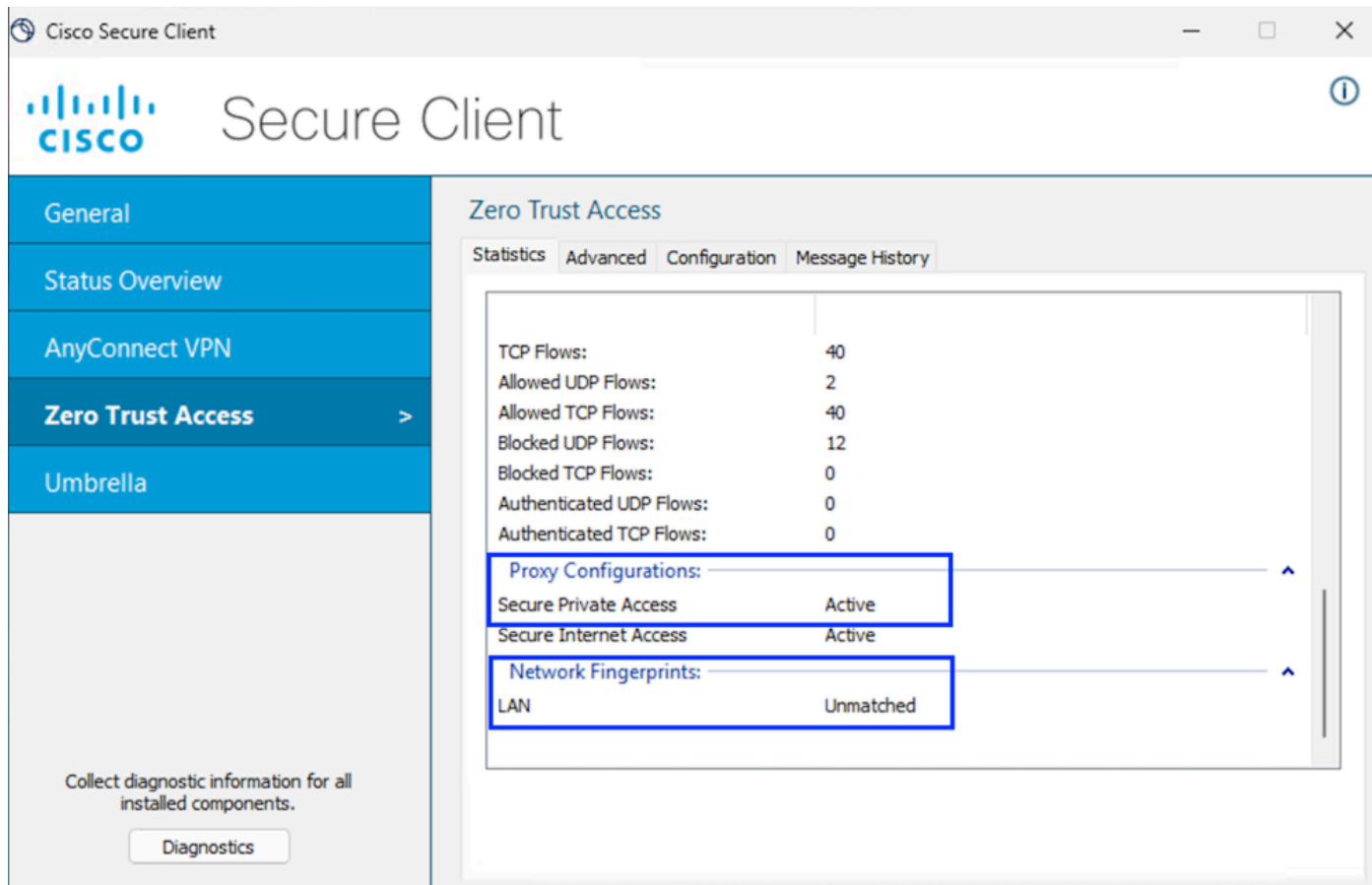


Secure Access - Prueba de relaciones públicas

5. Verificar registros de búsqueda de actividad de acceso seguro

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

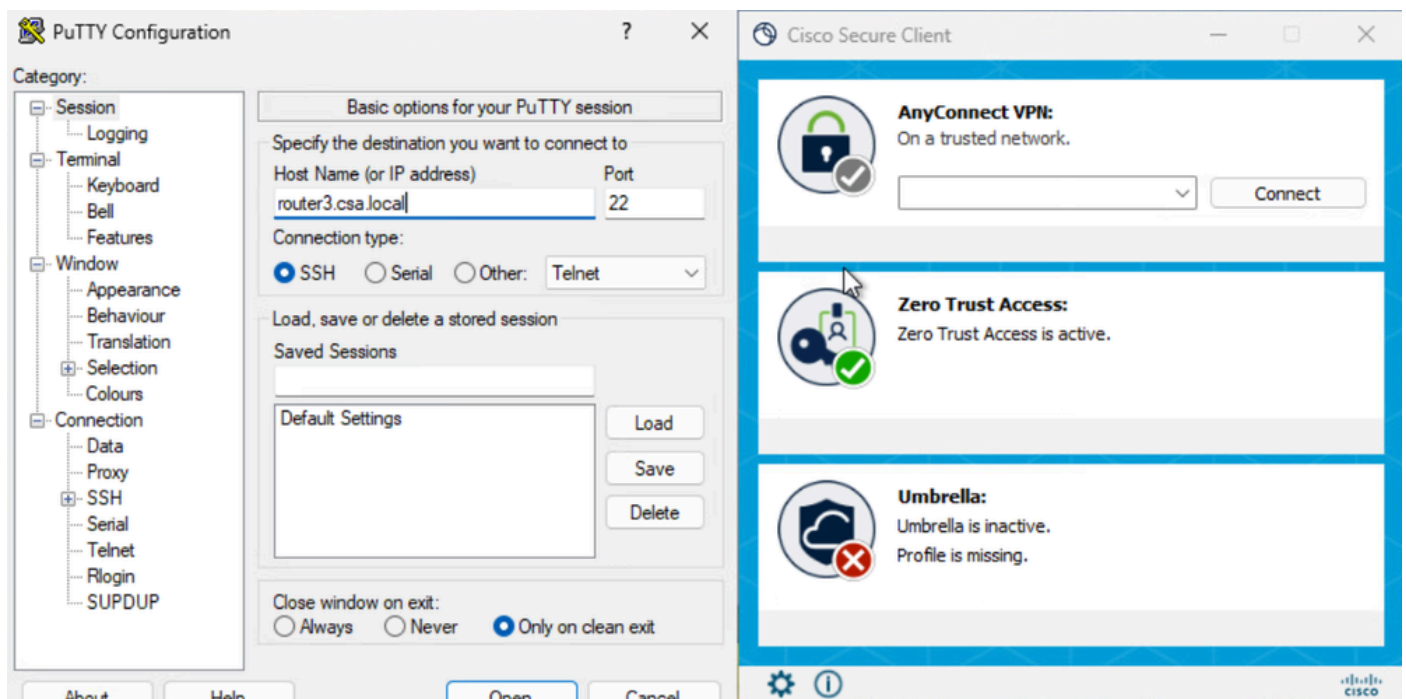
Name: ftd.csa.local
Addresses: 192.168.1.12

```

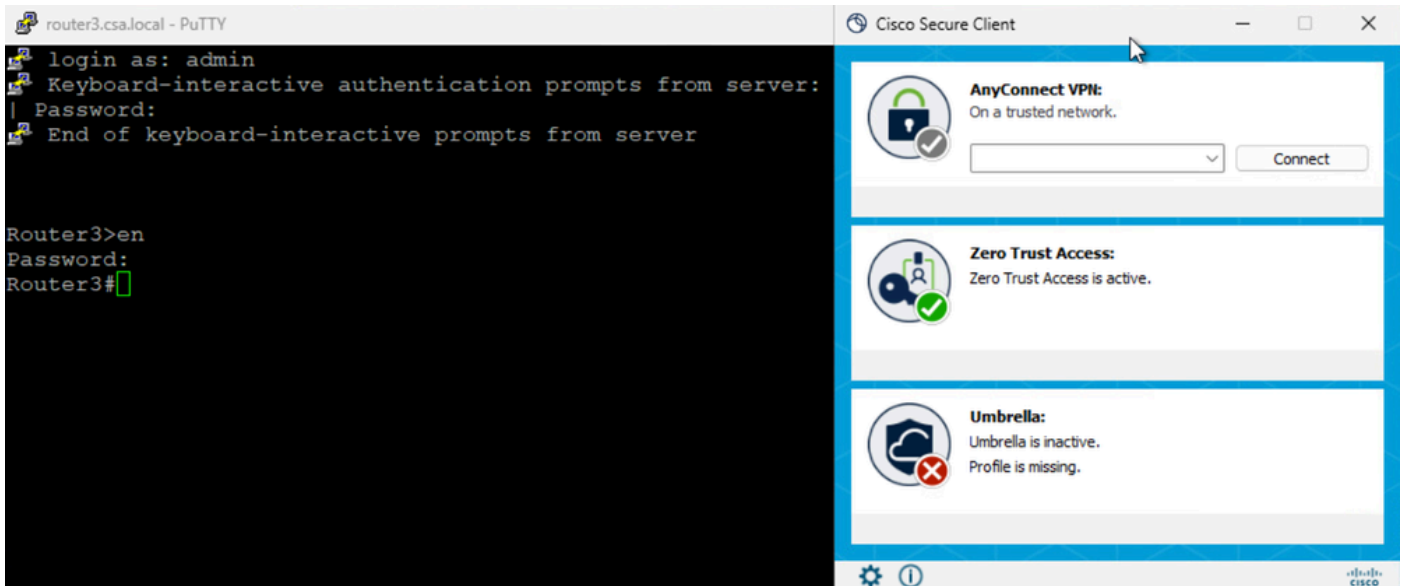
Secure Access - Prueba de relaciones públicas

3. Pruebe la conexión SSH al recurso privado

Acceso al PR mediante FQDN

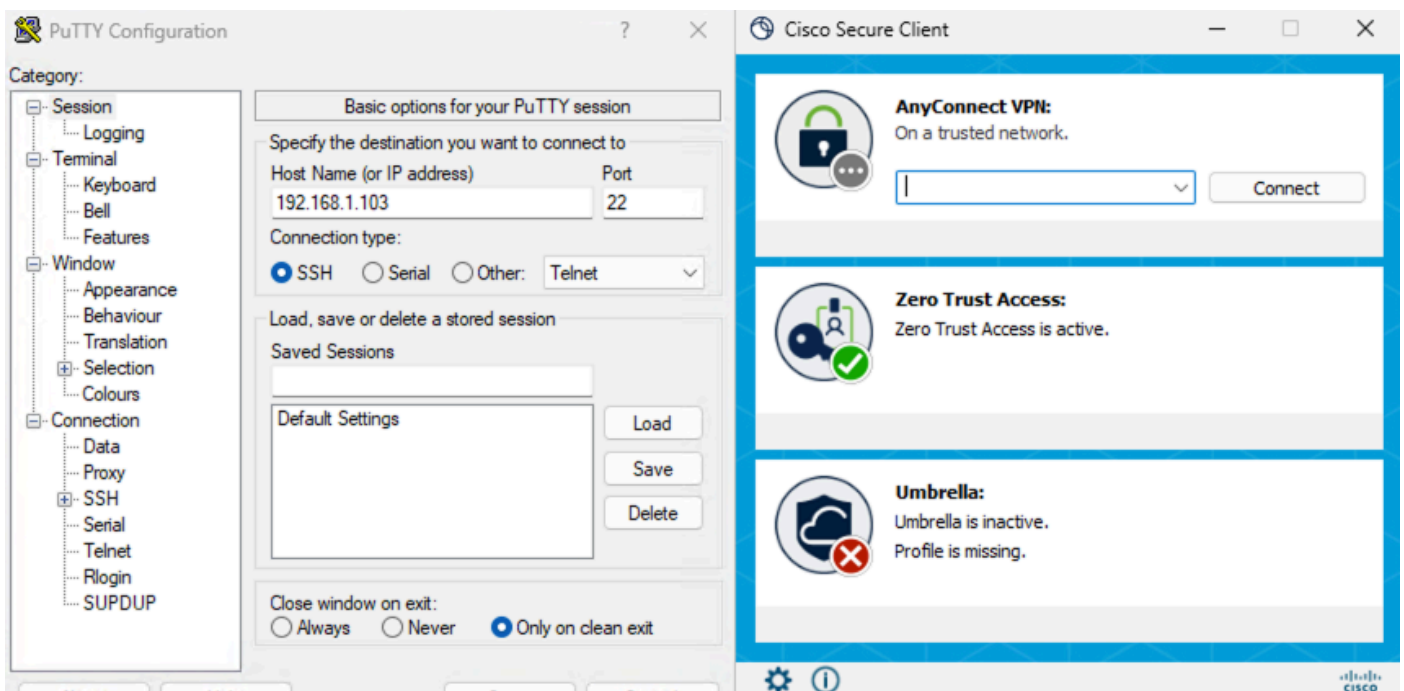


Secure Access - Prueba de relaciones públicas

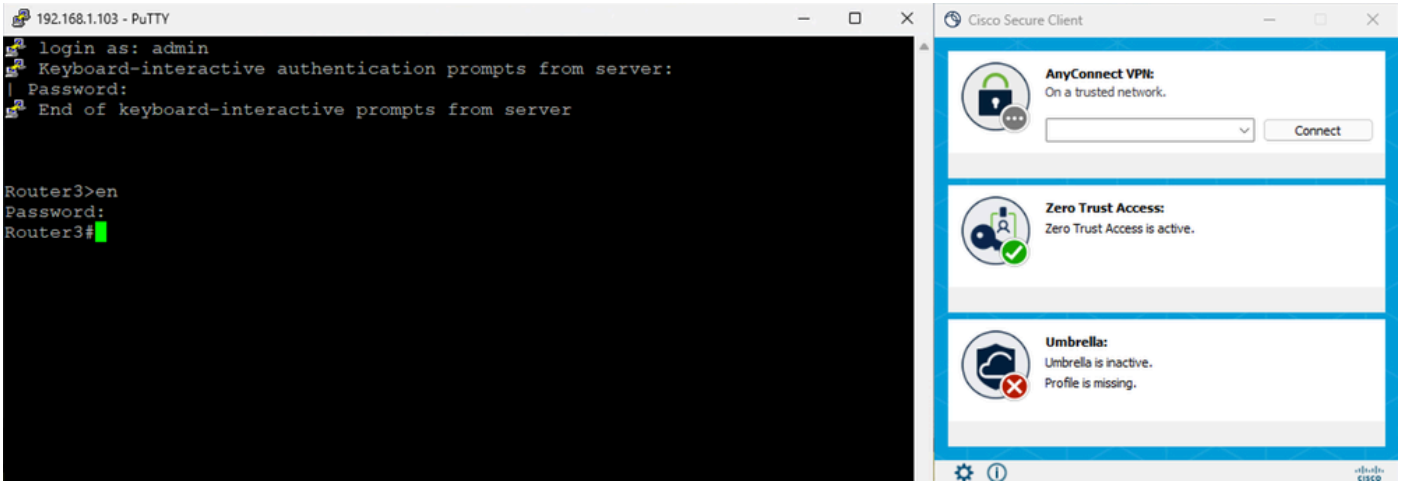


Secure Access - Prueba de relaciones públicas

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

Activity Search

Filters: Search by domain, identity, or URL. Advanced. CLEAR

RESPONSE: Allowed X

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM. Page: 1. Results per page: 50. 1 - 34 of 34

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow

Acceso seguro - Búsqueda de actividad

Activity Search

Filters: Search by domain, identity, or URL. Advanced. CLEAR

RESPONSE: Allowed X

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM. Page: 1. Results per page: 50. 1 - 34 of 34

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/App
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 7:30 AM

Access details

Identity: Jay (jay@csa.local)

ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: router3.csa.local

Destination IP: 192.168.1.103

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).