

Configurar o ZTNA universal para acesso a recursos privados em acesso seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Sobre a Universal ZTNA](#)

[Detecção de rede](#)

[Tipos para Imposição](#)

[Casos de uso](#)

[Componentes da arquitetura](#)

[Fluxo de pacote](#)

[Configurar](#)

[Diagrama de Rede](#)

[Casos de teste](#)

[Caso de teste 1: Usuário remoto - Aplicação da nuvem](#)

[Caso de teste 2 - Usuário remoto - Aplicação local](#)

[Caso de teste 3 - Usuário local - Aplicação local](#)

[Caso de teste 4 - Usuário local e remoto - Aplicação local ou em nuvem com TND](#)

[Troubleshooting](#)

[Comandos úteis:](#)

Introdução

Neste documento, abordaremos a configuração para acesso de recurso privado via Universal ZTNA com diferentes caminhos de tráfego.

Pré-requisitos

A configuração a seguir deve ser concluída antes da configuração ZTNA universal

- [Provedor de identidade no Cisco Secure Access](#)
- [Registrar dispositivos no acesso de confiança zero usando certificados](#)
- [Configurar túneis com o Cisco Secure Firewall](#)

- [Rede Virtual Privada de Acesso Remoto](#)
- [Conector de recursos no acesso seguro](#)
- [Integração do FTD no Security Cloud Control](#)
- O sinalizador de recurso ZTNA híbrido deve ser habilitado para o respectivo Locatário de Acesso Seguro , entre em contato com o Cisco TAC para habilitar o sinalizador

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN IPsec no Cisco Secure Access e Firewall Threat Defense
- IdP (Provedor de Identidade) - Provisionamento de Usuário do Ative Directory
- Configuração de VPN remota no Cisco Secure Access
- Implantação do conector de recursos no Cisco Secure Access
- Inscrição baseada em certificado ZTA
- Certificado - OpenSSL , geração de CSR , modelos de certificado etc.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Threat Defense (Versão 7.7.10)
- Cisco Secure Firepower Management Center (Versão 7.7.10)
- Cisco Secure Client (ZTA versão 5.1.10.1720)
- Windows 11
- Windows 2019 Server - Autoridade de Certificação
- Conector de recursos no ESXi

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Sobre a Universal ZTNA

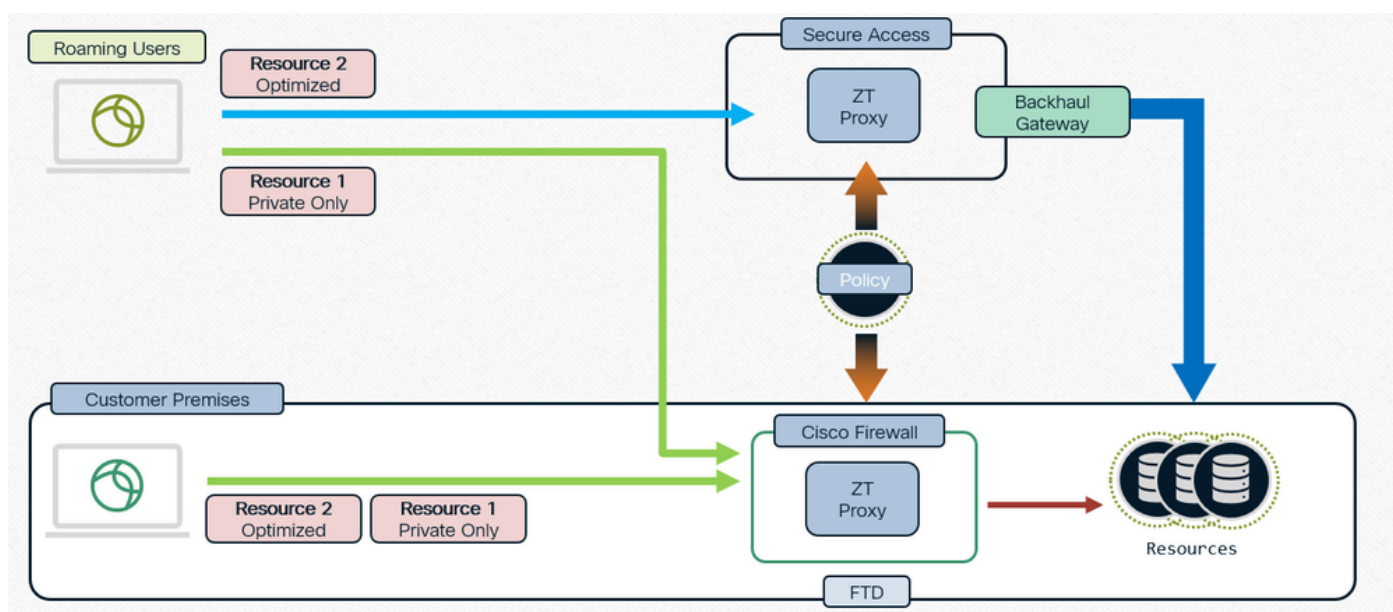
O acesso universal à rede de confiança zero (ZTNA) permite que os administradores permitam especificamente o acesso aos recursos da rede interna de acordo com a identidade do usuário

(incluindo confiança e postura do usuário) e sem conceder acesso a toda a rede, como com o RA-VPN. O ZTNA permite que os administradores protejam os recursos e aplicativos internos para usuários remotos e locais.

Como a ZTNA não presume que o acesso concedido a um aplicativo autoriza implicitamente o acesso a outros aplicativos, a superfície de ataque da rede é reduzida.

O Secure Access avalia a política de acesso. Todas as políticas de controle de acesso implantadas nos dispositivos do Secure Firewall Management Center são ignoradas.

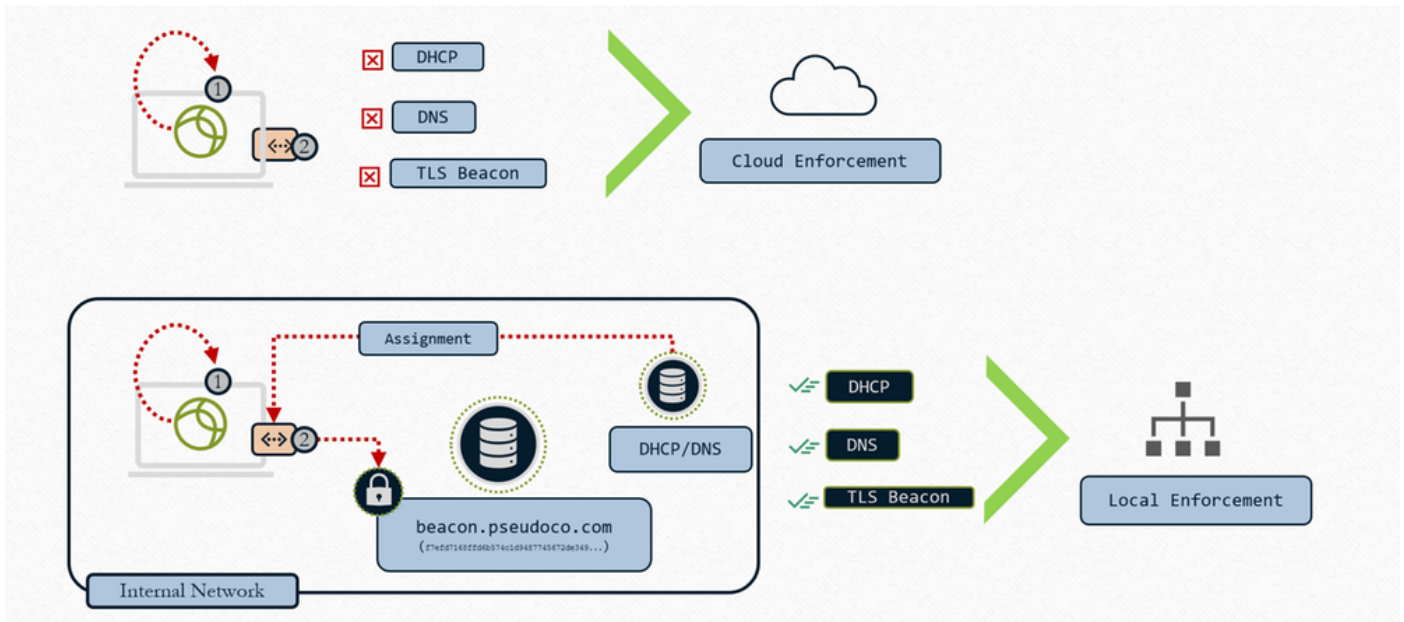
O proxy de tráfego, bem como a aplicação de políticas de IPS, arquivos e malware, é executado no Firepower Threat Defense (FTD).



Política única, aplicação distribuída

Detecção de rede

Determine a aplicação na nuvem ou local



ZTNA universal - Determine a aplicação na nuvem ou local

1- O cliente interroga a interface local para a configuração da rede

2- O cliente procura o beacon TLS

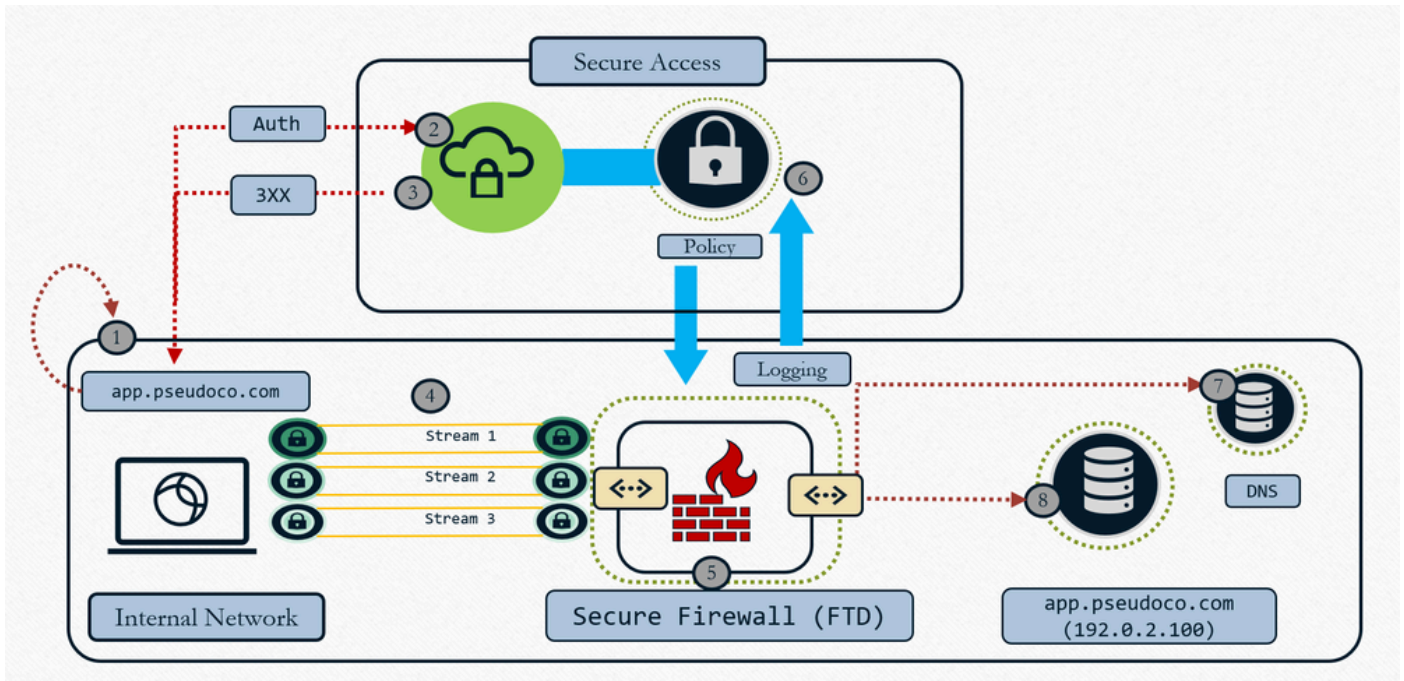
3- Se a condição corresponder - Aplicação Local

4- Se a condição não corresponder - Aplicação da nuvem

Quando configuramos o recurso com "Aplicação na nuvem ou local" e associamos a regra TND ao FTD, o que ele realmente faz é que o conjunto de regras de interceptação que é enviado ao cliente incluirá a avaliação da regra TND. Assim, o cliente será instruído pela nuvem a avaliar a regra TND. Quando enviamos a conexão, colocamos o resultado dessa TND - avaliação de impressão digital de rede no cabeçalho HTTP para que, que dirá ao proxy se estamos no local ou em uma rede não confiável e, em seguida, o proxy usa essas informações e redireciona o tráfego de acordo. Caso a impressão digital corresponda, Zproxy instrui o cliente a redirecionar o tráfego para FTD e, se a impressão digital não corresponder, redireciona o tráfego para a nuvem. Consulte [Configurar Acesso à Rede de Confiança Zero com Detecção de Rede Confiável](#)

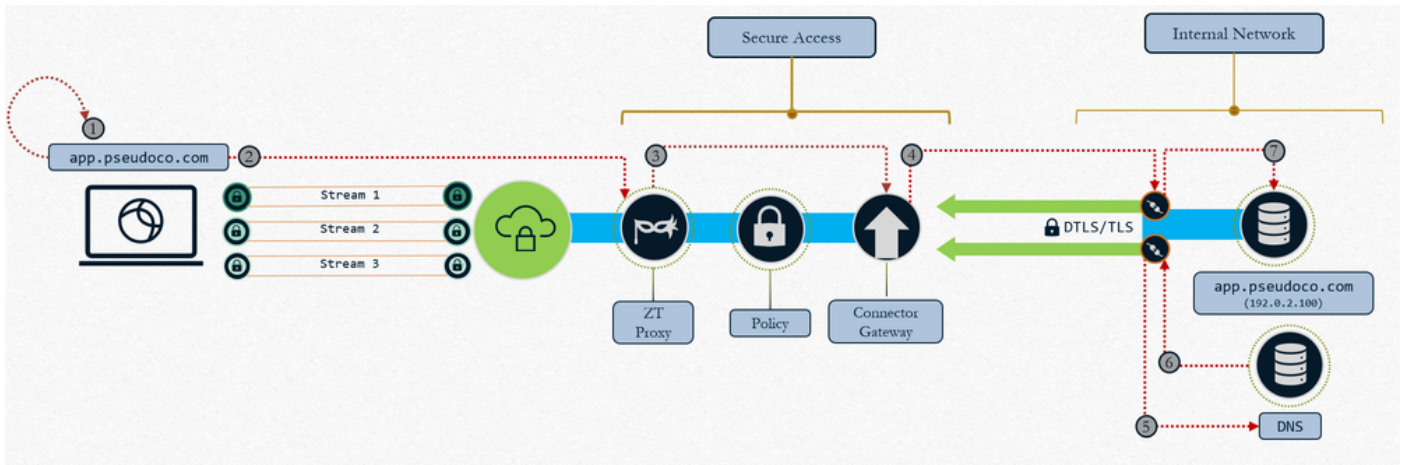
Tipos para Imposição

- Caminho de Imposição Local: Aplicação de firewall



ZTNA universal - Aplicação local

1. O usuário solicita o aplicativo, o cliente captura e resolve a solicitação para o IP efêmero (intervalo de localhost)
 2. O tráfego de controle de autenticação é enviado para a Secure Access Cloud para avaliação de política
 3. A nuvem retorna redirecionamento para o FTD para aplicação do plano de dados (se a política permitir)
 4. Tráfego direcionado para o headend configurado do firewall (interface)
 5. A política definida na nuvem é aplicada (IPS, malware, descriptografia) usando o plano de dados do proxy local
 6. Evento registrado e duplicado enviado para a nuvem para relatórios consistentes
 7. O firewall faz a resolução DNS na rede local para rotear o tráfego de recursos (se permitido)
 8. O firewall cria a conexão com o recurso (nova conexão criada para o recurso) à medida que o firewall se comporta como um proxy TCP
- Caminho de aplicação da nuvem: FORA da rede

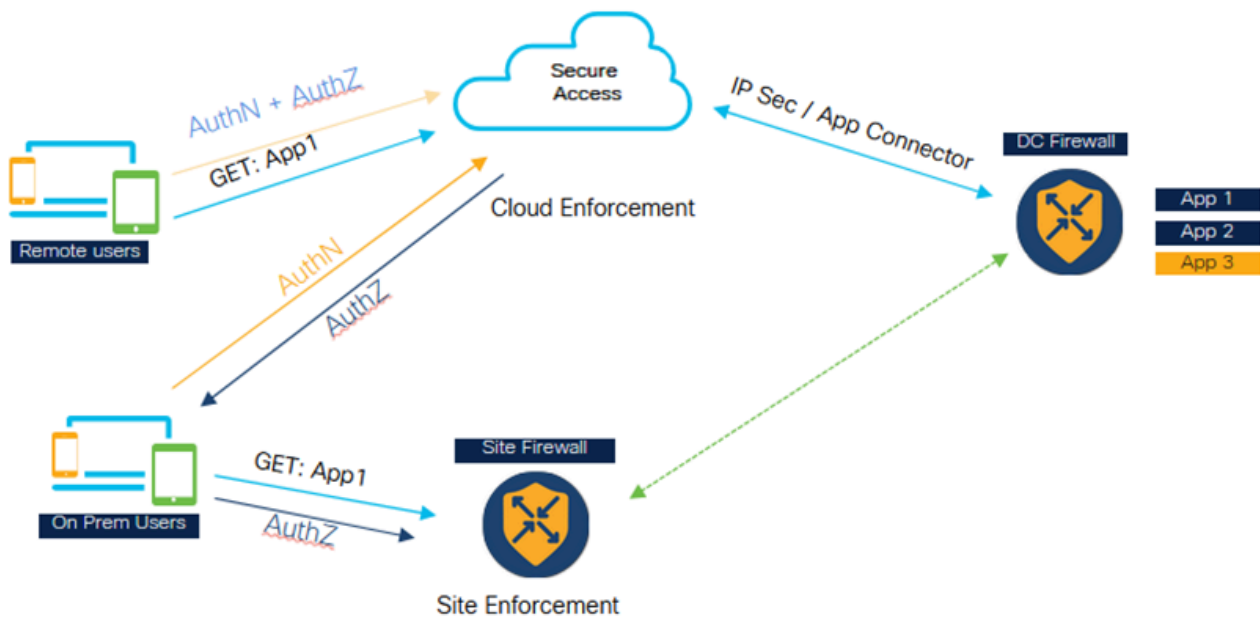


ZTNA universal: Aplicação da nuvem

1. O usuário solicita o aplicativo, o cliente captura e resolve a solicitação para o IP efêmero (intervalo de localhost)
2. O tráfego é transportado para o proxy de confiança zero no acesso seguro
3. A conexão TCP é submetida a proxy e criada para o conector de recurso mapeado, a política é aplicada no tráfego
4. O gateway estabelece a conexão com o conector de recursos
5. O conector de recursos resolve o IP do recurso
6. O DNS local responde com o IP do recurso
7. O conector de recurso estabelece a conexão com o recurso

Casos de uso

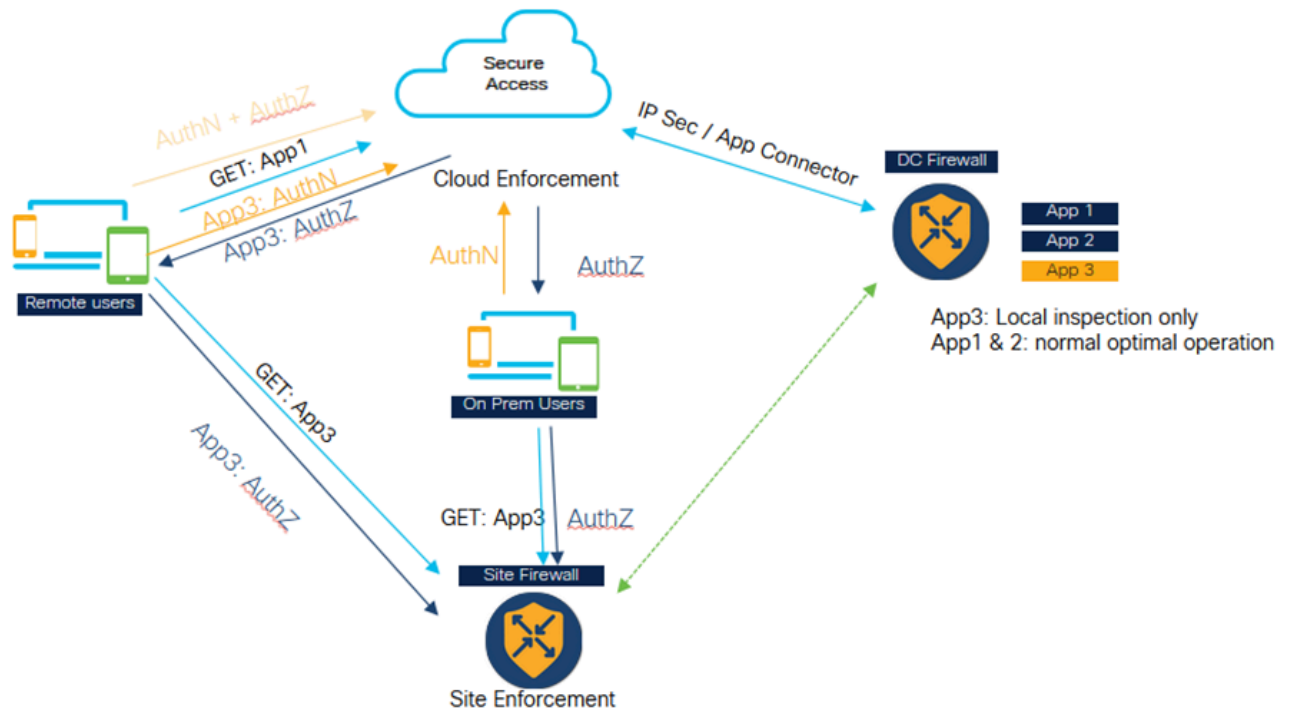
Caso 1: ZTNA consistente e otimizada para usuários no local



ZTNA universal - ZTNA consistente e otimizado (usuário no local)

- O Secure Access e o Firewall são configurados para proteger o aplicativo.
- Se o usuário for remoto, ele irá para Acesso seguro para avaliação e inspeção de políticas.
- Se o usuário for Interno/Local, ele irá para o firewall para inspeção de tráfego privado.
- O usuário local ainda pode acessar o Secure para obter autenticação e avaliação, apenas o tráfego do caminho de dados vai para o Firewall e é inspecionado de acordo com a configuração da política.
- O usuário interno que acessa o aplicativo por meio do firewall tem uma vantagem de desempenho, pois evita que o tráfego vá para a nuvem e, em seguida, faça o backhaul para o data center

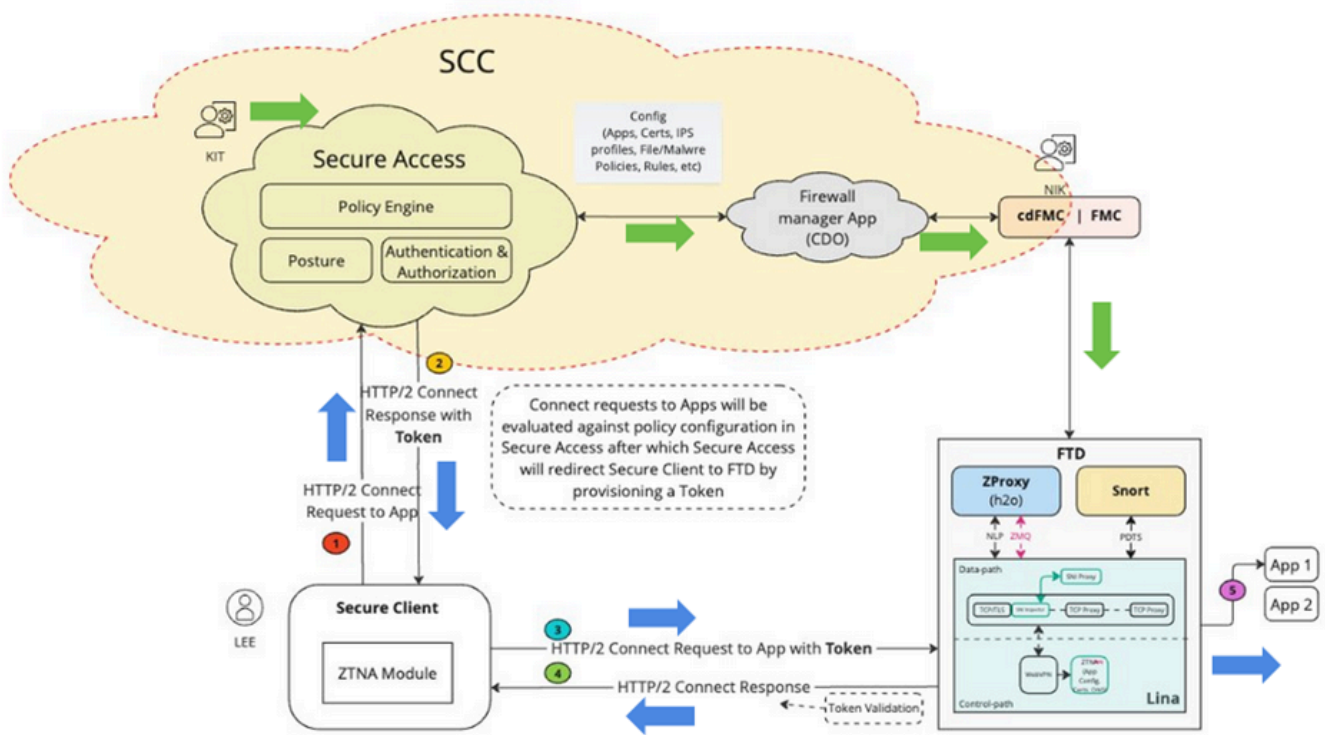
Caso 2: Inspeção Privada para Aplicações Sensíveis



ZTNA Universal - Inspeção Privada para Aplicações Sensíveis

- Determinados aplicativos críticos podem ser configurados para sempre serem acessados através do firewall.
- O tráfego de dados do aplicativo não precisa ir para a nuvem. Por exemplo, pode haver um aplicativo de dados confidenciais, como o código-fonte, que o cliente não quer ir para a nuvem.
- Nesses cenários, o tráfego do usuário remoto e no local sempre passa pelo firewall e é inspecionado. No entanto, novamente, nesse cenário, a avaliação de autenticação e política está sempre acontecendo na nuvem, apenas o tráfego da parte de dados passa pelo firewall.

Componentes da arquitetura



ZTA universal - Componentes arquitetônicos

O Security Cloud Control (SCC) é o principal gerenciador da solução da ZTNA. A ZTNA é o primeiro recurso a ser construído sobre o SCC.

No SCC, temos dois microaplicativos Secure Access e Firewall. Depois que o SCC for provisionado e os sinalizadores de recursos necessários forem habilitados, poderemos ver esses microaplicativos no lado esquerdo do painel SCC.

Cliente seguro: No Secure Client, precisaremos habilitar o ZTNA (Zero Trust Access Module, módulo de acesso zero confiável) para que possamos acessar os aplicativos.

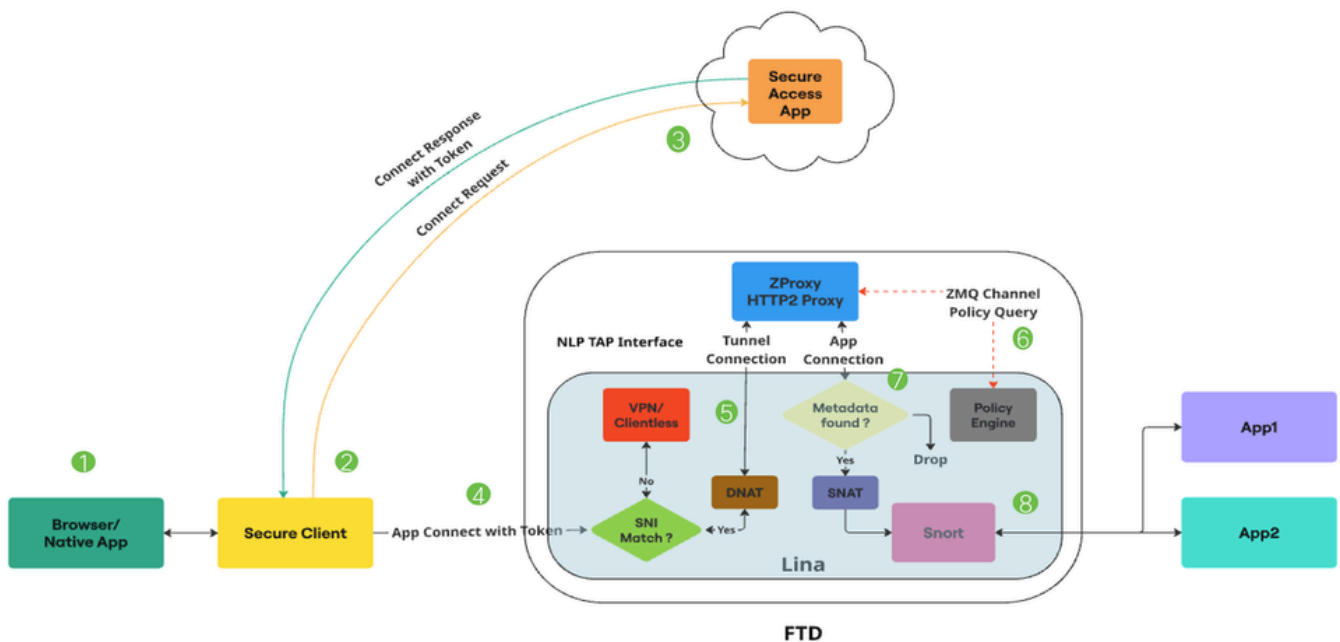
Firewall Threat Defense: FTD protegendo esses aplicativos. O FTD executa um proxy ZT que também é conhecido como H2O (o mesmo que o proxy é executado na Secure Access Cloud)

Agora, quando um usuário (por exemplo, KIT) configurar um recurso privado e uma política no microaplicativo Secure Access, essa configuração será enviada para o microaplicativo Firewall no SCC. O aplicativo de firewall compreende os internos do FTD, a configuração do FTD, como implantar e gerenciar a configuração no FTD. Portanto, o aplicativo de firewall valida essa configuração e chama as APIs do FMC para enviar a configuração para o FMC e, em seguida, implantá-la no FTD. O FTD pode ter uma opção de implantação automática habilitada para que os administradores (por exemplo, Nick) não precisem fazer a implantação manual.

1. Quando um usuário (por exemplo, Lee) tenta acessar um aplicativo, o cliente seguro se conecta ao Secure Access usando o canal mTLS. O Secure Access autentica o usuário usando o certificado do dispositivo cliente. Em seguida, ele avalia a autorização, a postura e outras políticas configuradas para esse usuário e para esse aplicativo.
2. Acesso Seguro: se ele finalmente descobrir que o aplicativo está sendo protegido pelo Firewall, ele gerará um token de autenticação, que informará ao firewall que ele já está autenticado e autorizado. O token de autenticação está criptografado, assinado pelo Secure Access
3. O Secure Access redireciona o cliente Secure para o FTD junto com o token de autenticação.
4. O Cliente Seguro estabelece outra conexão com o FTD, é uma conexão HTTP2 no canal mTLS. Ele envia uma solicitação CONNECT para o aplicativo que está sendo acessado junto com o Token.
5. O FTD agora valida o Token. Se o Token for validado com êxito, o usuário poderá acessar esse aplicativo. Em seguida, o FTD envia a confirmação de volta ao Cliente seguro

Fluxo de pacote

Fluxo de pacote detalhado ZTNA universal



ZTA universal - Fluxo de pacotes

1. O usuário tenta acessar um aplicativo através de um navegador da Web ou de um aplicativo

nativo.

2. O Cliente Seguro intercepta a conexão e a identifica como um usuário tentando acessar um Recurso Privado.
3. O Cliente Seguro estabelece uma conexão mTLS com o Acesso Seguro, solicitando acesso ao aplicativo. O Acesso Seguro verifica a conformidade das políticas ZTNA Universal e dos perfis de postura. Se tudo estiver bem, o Acesso Seguro gera um Token de Acesso que contém informações essenciais, como detalhes do usuário, detalhes do aplicativo e política de IPS/Arquivo.
4. O Token de Acesso é criptografado e assinado pelo Acesso Seguro. Em seguida, o Acesso Seguro redireciona o Cliente Seguro junto com o token para o FTD.
5. Quando o pacote alcança o caminho de dados Lina, o verificador SNI intercepta a conexão e verifica se o nome do servidor (extensão SNI) no Hello do cliente corresponde ao FQDN do proxy configurado no dispositivo. Se o SNI coincidir, a conexão será direcionada ao ZProxy. Se o SNI não coincidir, a conexão é direcionada para outros recursos que podem coexistir com a Universal ZTNA.

Por exemplo: VPN, Portal cativo ou ZTNA sem cliente. O ZProxy, que oferece suporte ao protocolo MASQUE sobre HTTP/2, será executado no FTD como um Processo Não Lina em núcleos dedicados. A comunicação entre Lina e ZProxy utiliza a Interface Tap NLP para manipular o tráfego de dados. O IP de destino da conexão é convertido para o IP da interface TAP pelo verificador SNI.

6. Quando o ZProxy recebe a conexão de túnel mTLS do Secure Client, ele verifica o certificado do dispositivo do cliente enviado pelo Secure Client. Ele também verifica o Token de Acesso enviado com o APP Connect. Há um canal Zero MQ entre Lina e ZProxy. Ele é usado principalmente para trocar mensagens de controle. O ZProxy usa esse canal para resolução FQDN de recursos Privados ao se comunicar com Lina.

O canal Zero MQ também é usado para propagar informações presentes no token de acesso para Lina. (Exemplo: ID da regra, ID da política, etc.) Lina recebe as informações do token de acesso e as armazena em um banco de dados de metadados.

7. Quando as mensagens de controle forem trocadas, o ZProxy iniciará uma nova conexão com o recurso privado. Pode ser TCP ou UDP. Lina então executa uma pesquisa de banco de dados de metadados para esta conexão de aplicativo. Se os metadados não forem encontrados, o Connection será descartado

8. Como a conexão do aplicativo é originária do ZProxy, ela terá um IP Interno

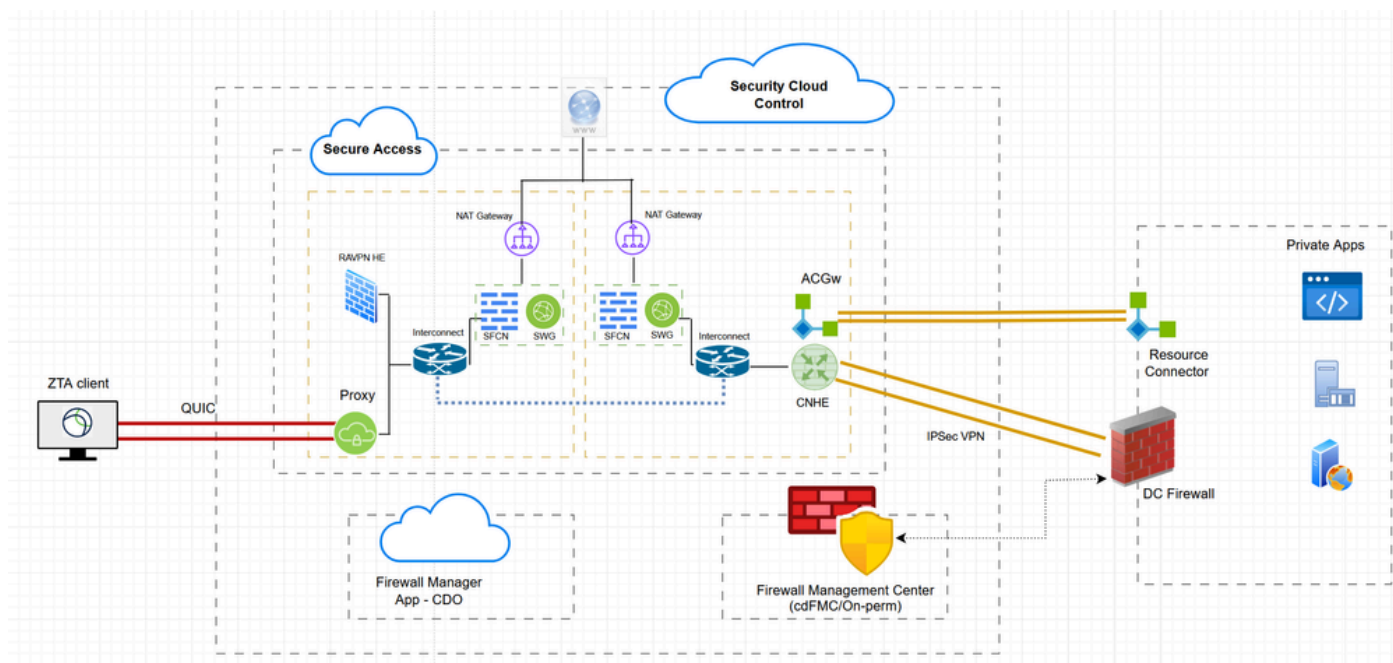
(exemplo:169.251.1.2) como IP de Origem. Isso será traduzido para o IP da interface de saída do FTD, antes de enviá-lo. Em seguida, Lina marca os fluxos de Confiança Zero Universal para inspeção do Snort somente se uma política de Arquivo ou IPS estiver presente no token de acesso. A ID da Regra obtida do token de acesso é passada para o Snort nos metadados da conexão.

9. As regras universais de confiança zero e os correspondentes mapeamentos de políticas de ficheiro e de SPI são transmitidos ao DTF através do CVP. O plug-in Confiança Zero no Snort carregará essas regras durante a inicialização. Lina marcará os fluxos de fluxo Confiança Zero Universal para inspeção do Snort somente se uma política de Arquivo ou IPS for mencionada no token de acesso obtido do Acesso Seguro para acessar esse Recurso Privado.

A ID de regra obtida do token de acesso é passada para o Snort via Conn Meta. Para todos os fluxos de fluxo de Confiança Zero Universal, o plug-in Confiança Zero no Snort executará uma pesquisa de regra para a ID de regra obtida da Conn Meta. Se uma correspondência de regra for encontrada, o fluxo será permitido e as políticas de IPS e Arquivo específicas para essa regra serão aplicadas ao fluxo. Se nenhuma correspondência de regra for encontrada, o plug-in Confiança Zero no Snort bloqueará o fluxo.

Configurar

Diagrama de Rede

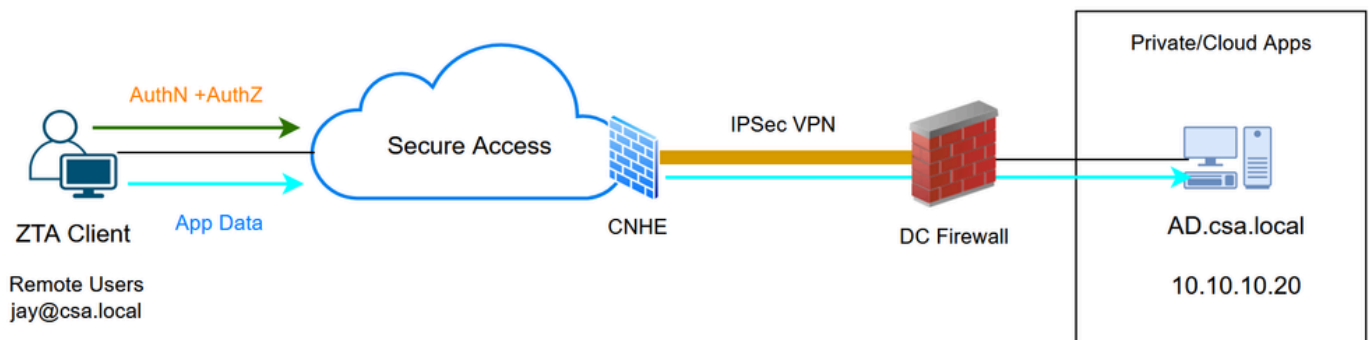


ZTNA híbrido - Diagrama de rede

Casos de teste

Caso de teste 1: Usuário remoto - Aplicação da nuvem

Neste caso de teste, acessaremos um recurso privado pelo Network Tunnel Group por meio da aplicação da nuvem. Nesse caso, os dados de avaliação de política e de aplicação serão interceptados pelo acesso seguro através do módulo ZTA. Este é um fluxo tradicional onde a aplicação privada pode ser acessada do cliente registrado ZTA através do Network Tunnel Group ou do Resource Connector



ZTA universal - Topologia de caso de teste

Etapa 1 - Definir um recurso privado no acesso seguro

Configurar um recurso privado para ser acessível por meio do dispositivo registrado ZTA (Zero Trust Access) com aplicação de nuvem

1. Navegue até Recursos > Destinos > Recursos particulares > Clique em +Adicionar

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	...

Acesso seguro - Configuração de recursos privados

2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do 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
AD-Server

Description (optional)
Active Directory server

Acesso seguro - Configuração de recursos privados

3. Informe o FQDN do recurso privado que deseja acessar. Também podemos definir o endereço IP do recurso privado. Para obter mais informações, consulte [Adicionar um recurso privado](#)

4. Selecione o servidor DNS interno para resolver o problema do domínio

Private resource address

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

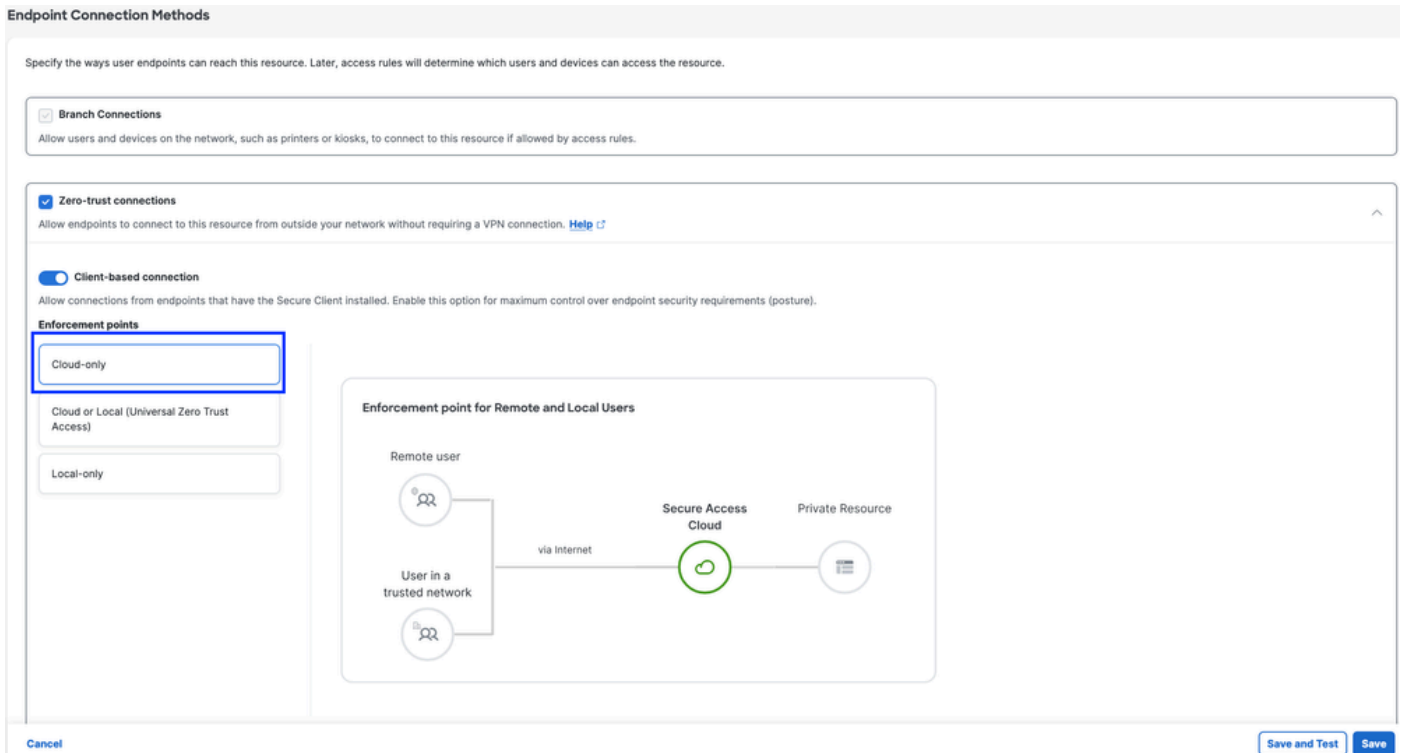
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
ad.csa.local	TCP - RDP	Any	+ Protocol & Port
Remove			
10.10.10.20	TCP - RDP	Any	+ Protocol & Port
Remove + IP Address/FQDN			

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

Internal DNS Server
PrivateDNS (10.10.10.20)

Acesso seguro - Configuração de recursos privados

5. Selecionar Métodos de Conexão de Ponto de Extremidade



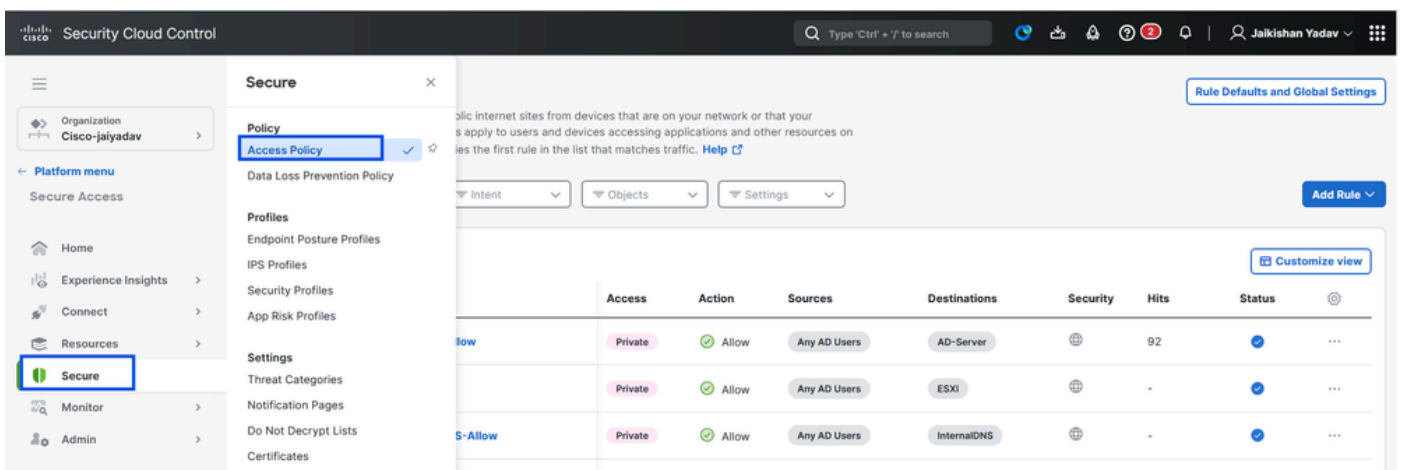
Acesso seguro - Configuração de recursos privados

6. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA . Para obter mais informações, consulte [Regra de acesso privado](#)

1. Navegue até Proteger > Política de acesso



Acesso seguro - Configuração da política de acesso

2. Clique em Adicionar Regra e escolha Acesso Particular.

Na parte superior da regra há um resumo que descreve os componentes configurados da regra.

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 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

Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra

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

Acesso seguro - Configuração da política de acesso

4. Selecione a ação da regra e selecione origem e 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

Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint

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](#)

Acesso seguro - Configuração da política de acesso

6. Configurar segurança

✓ **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](#)

Acesso seguro - Configuração da política de acesso

7. Clique em Salvar

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 [Add Rule](#)

3 Rules [Customize view](#)

<input type="checkbox"/>	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	<input type="checkbox"/>
<input type="checkbox"/>	1	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	🌐	-	🟢	⋮
<input type="checkbox"/>	2	BlockPage-TEST	Internet	Block	Any	Generative A...	🌐	-	🟢	⋮
<input type="checkbox"/>	3	RAVPN-Allow	Internet	Allow	Any AD Users	Any	🌐🔒	492	🟢	⋮

Rows per page: 1-3 of 3

Default Access Rules

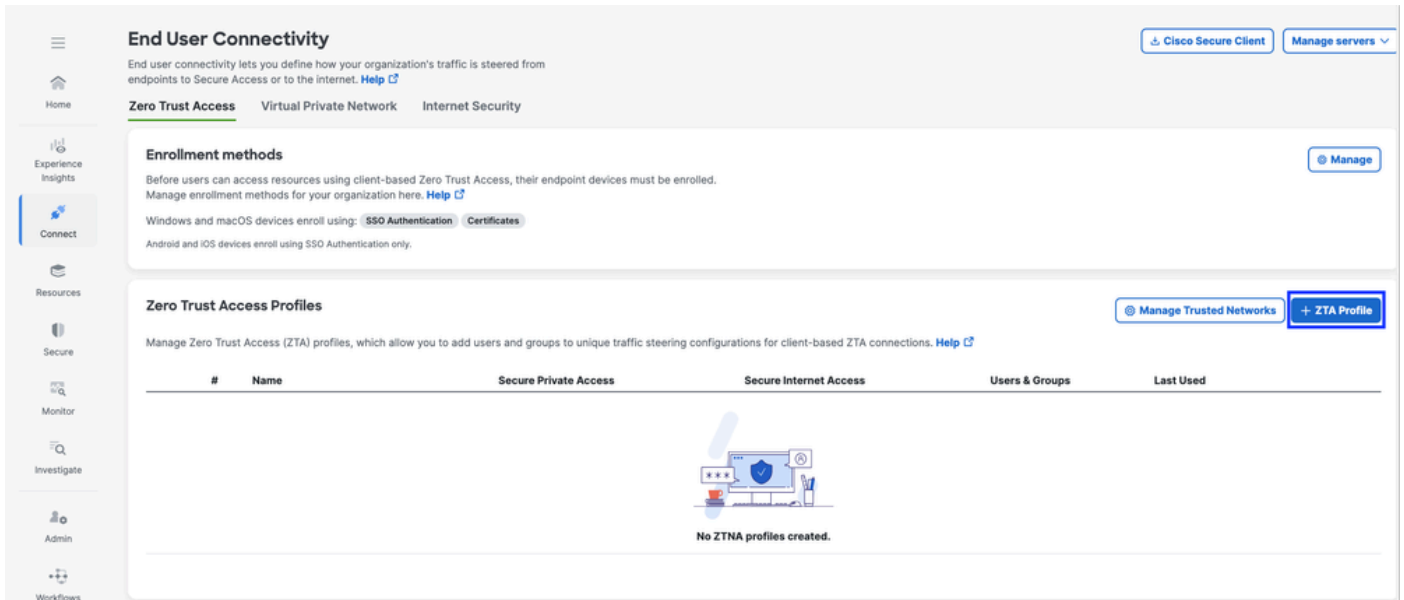
Rule name	Action	Sources	Destinations	Security	Posture	<input type="checkbox"/>
For all private access	Block	Any	Any private destination	-	-	⋮
For all Internet access	Allow	Any	Any Internet destination	🌐🔒	-	⋮

Acesso seguro - Configuração da política de acesso

Etapa - 3 Adicionar recurso privado ao perfil ZTA

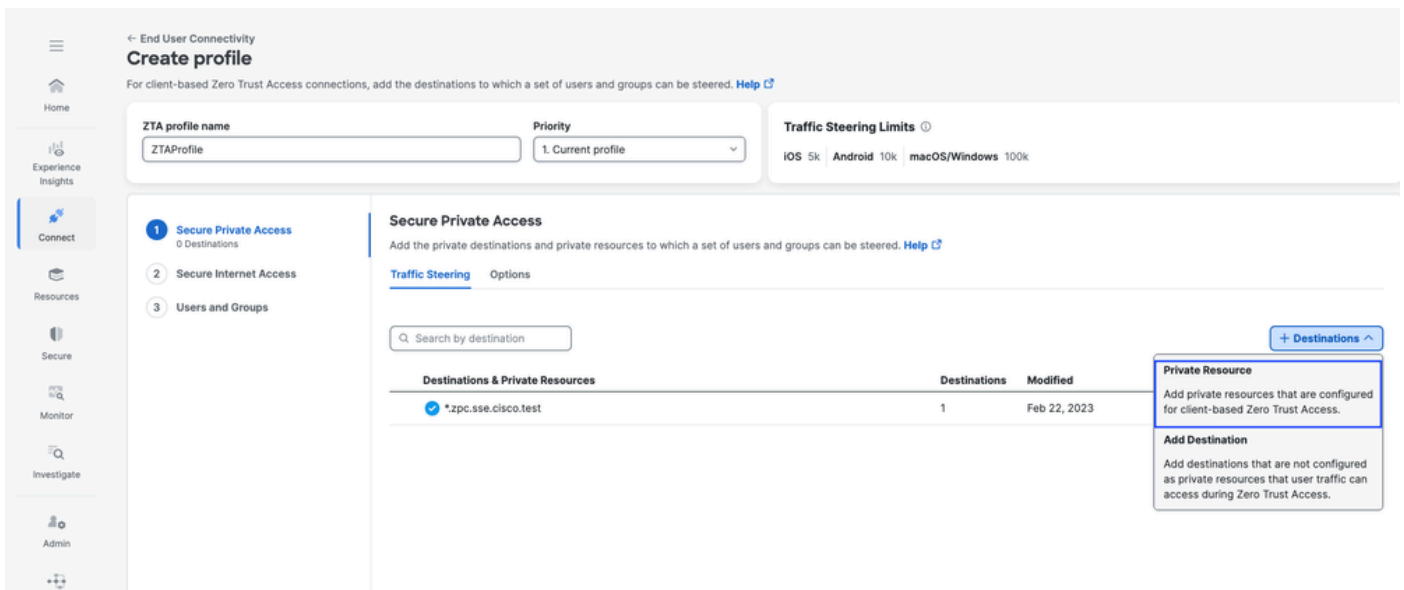
Se estiver usando um perfil ZTA personalizado, você precisará adicionar o respectivo recurso privado ao perfil ZTA

1. Navegue até Connect > End User Connectivity > Zero Trust Access e clique em +ZTA Profile

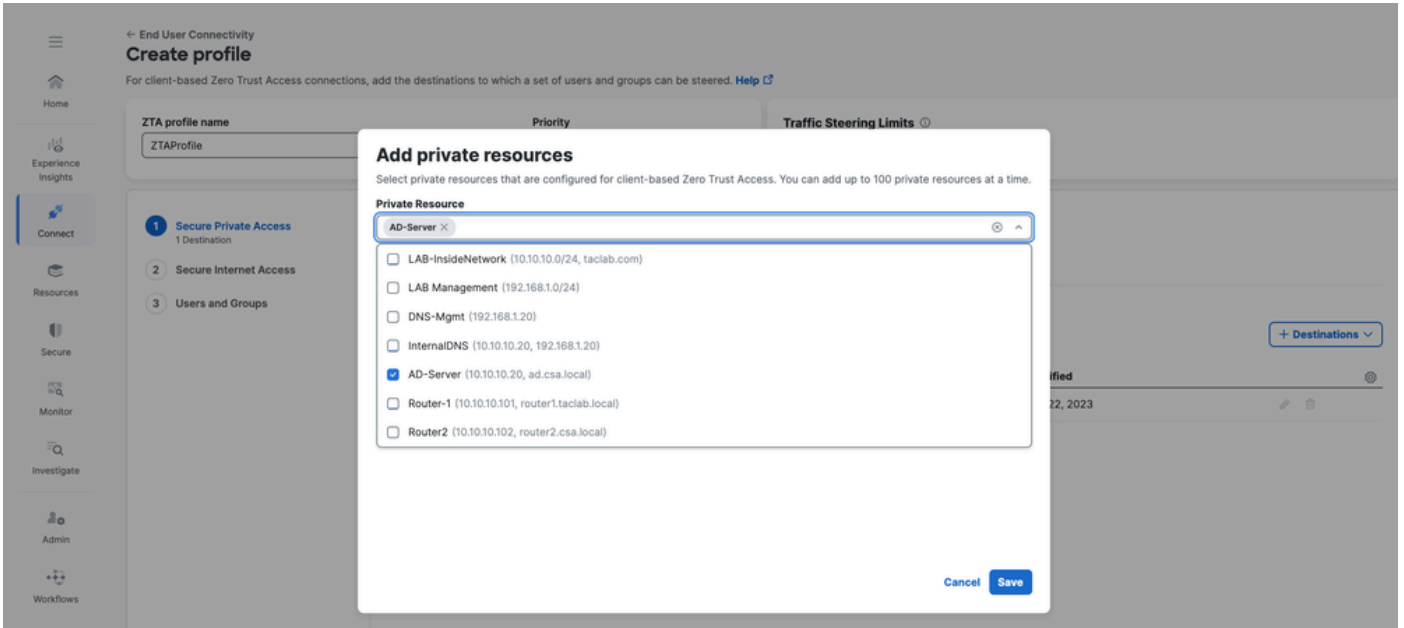


Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

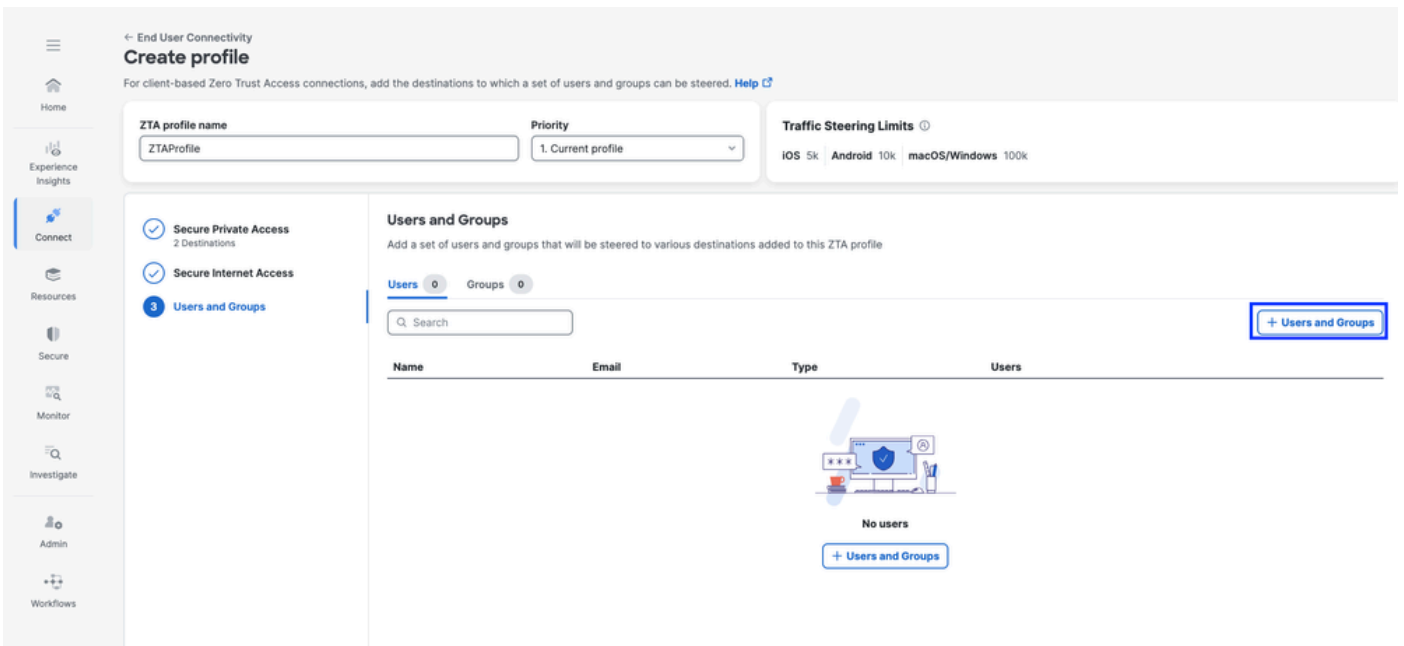


Acesso seguro - perfil ZTA



Acesso seguro - perfil ZTA

3. Adicionar usuários e 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

Acesso seguro - perfil ZTA

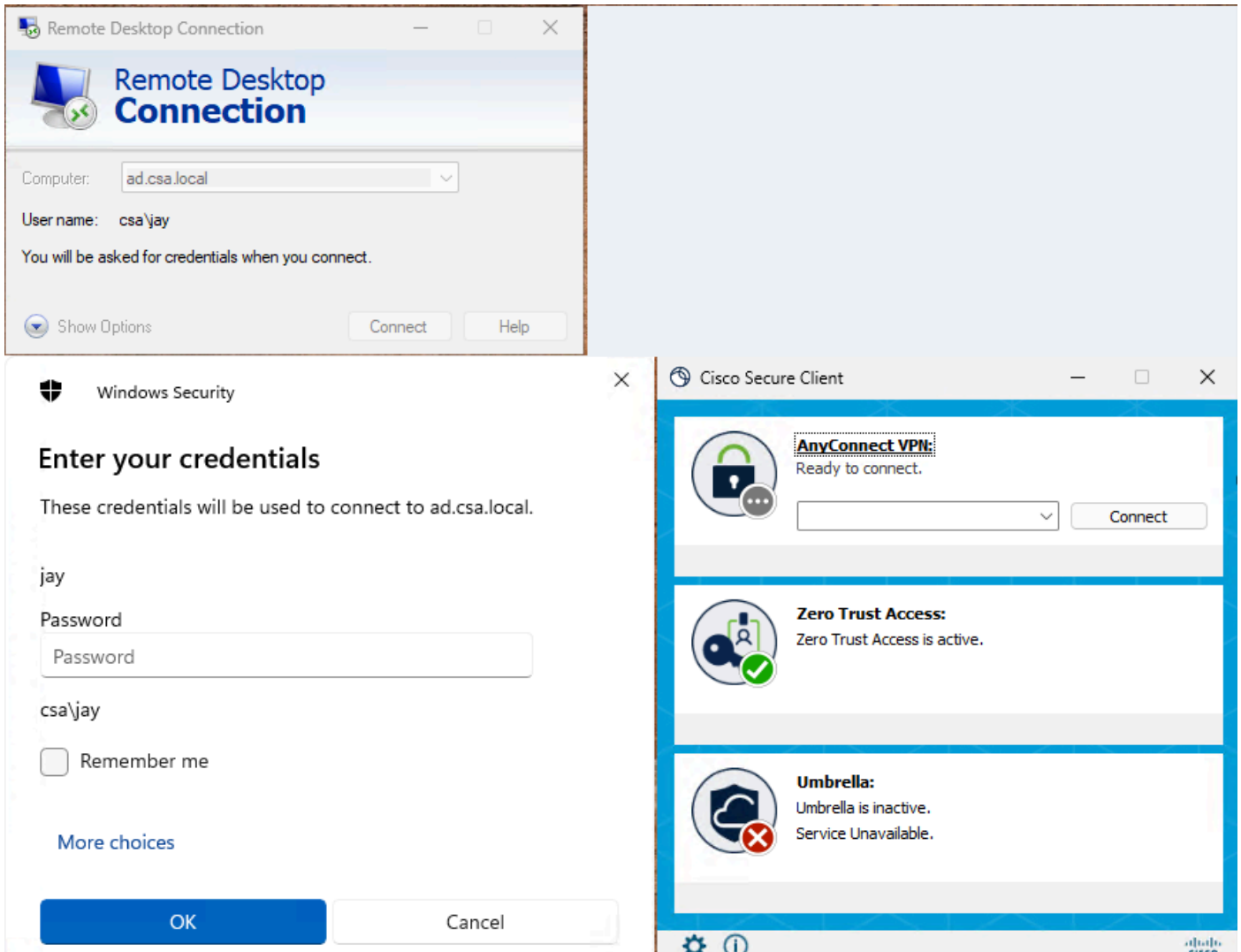


Note: Pode levar de 15 a 20 minutos para enviar e sincronizar a configuração para o cliente para o recurso privado atribuído

Etapa - 4 Verificar o acesso ao recurso privado

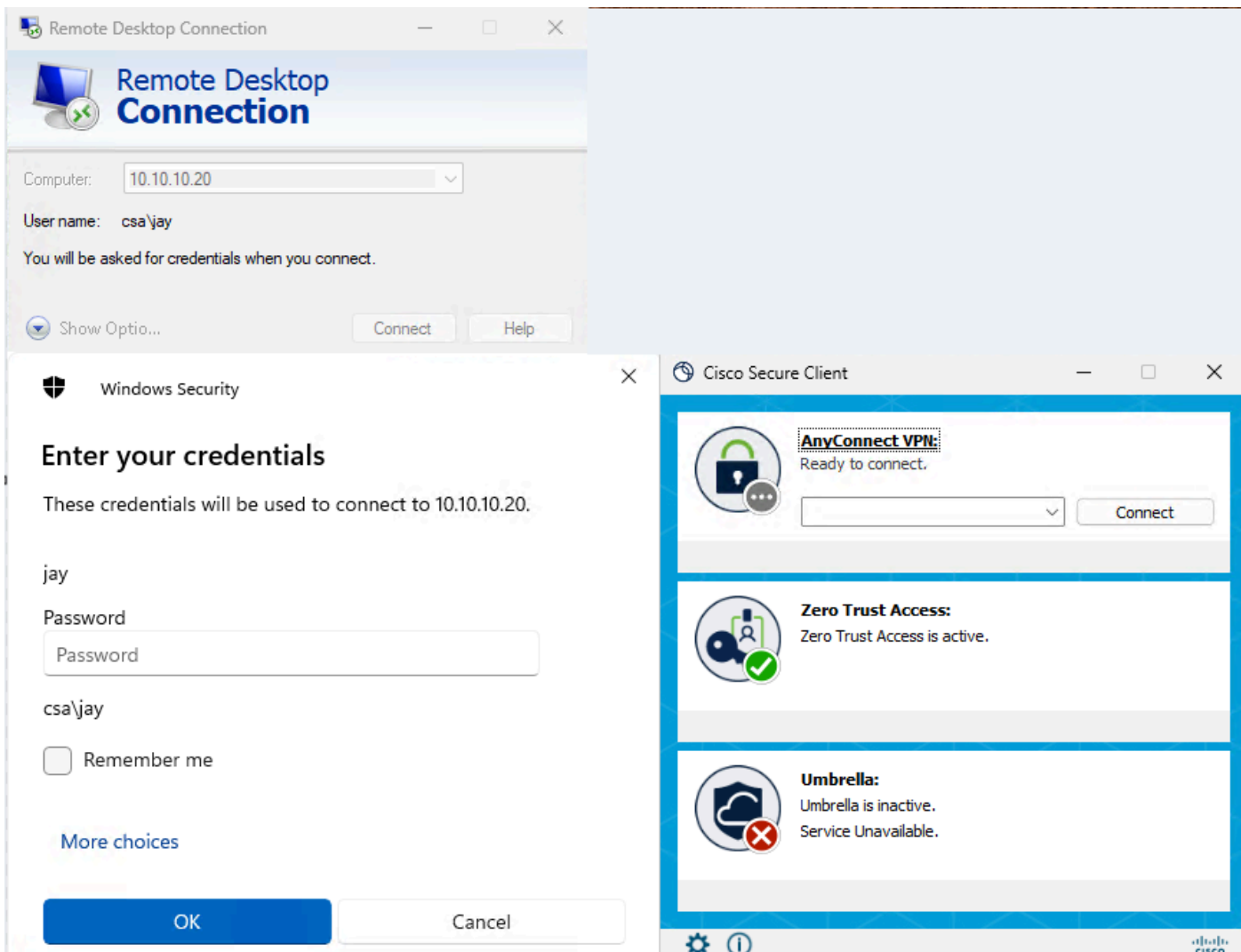
1. Acessar o Recurso Privado

Acessar a PR usando o FQDN



Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP



Acesso seguro - Teste de PR

2. Verificar com os eventos de Pesquisa de Atividade

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

Acesso seguro - Pesquisa de atividades

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

Acesso seguro - Pesquisa de atividades

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

Acesso seguro - Pesquisa de atividades

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

Acesso seguro - Pesquisa de atividades

3. Verificar os eventos de ligação do FMC

Events Troubleshooting

Destination Port / ICMP Code 3389

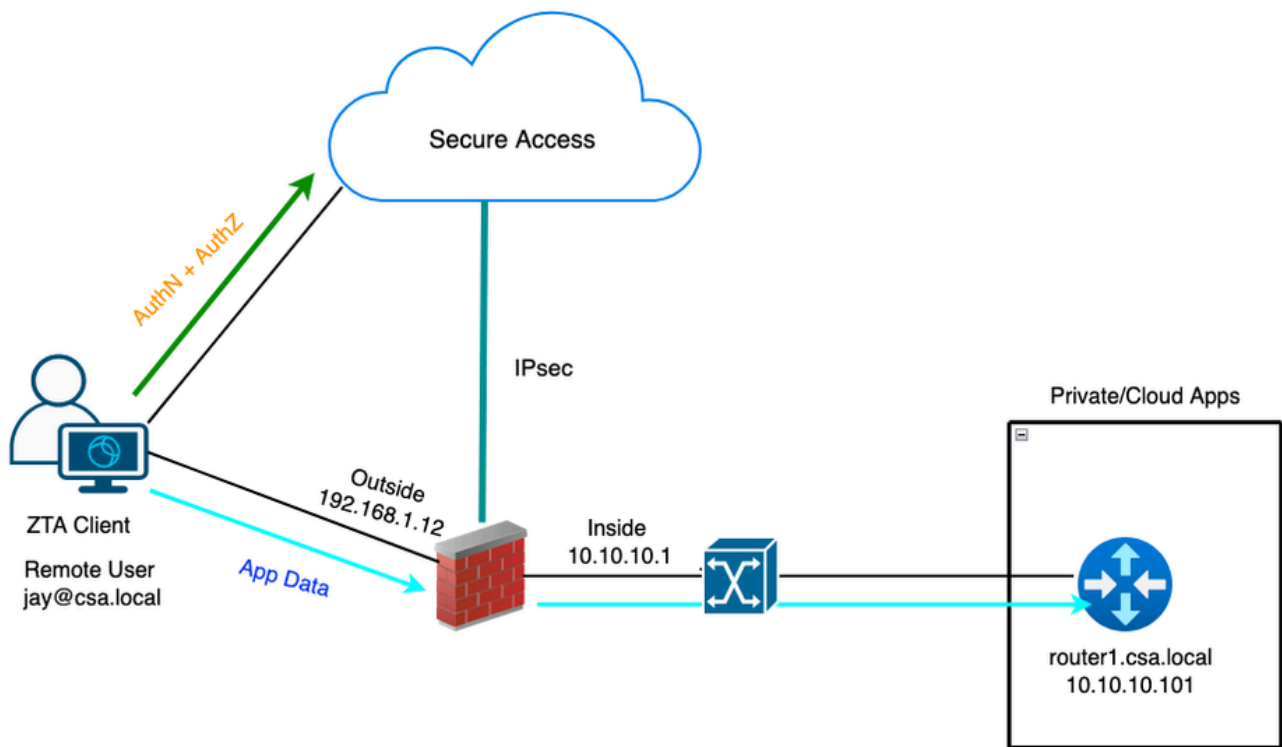
7 events Last 1 hour

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 conexão do FMC

Caso de teste 2 - Usuário remoto - Aplicação local

O acesso a um recurso privado por meio da aplicação local, nesse tipo de avaliação de política de aplicação, acontece no acesso seguro, mas os dados do aplicativo permanecem locais para o FTD. Por exemplo, um cliente ou usuário registrado ZTA conectado à rede doméstica e tentando acessar um recurso privado que está por trás da interface interna do FTD.



ZTA universal - Topologia de caso de teste

Etapa 1 - Definir um recurso privado no acesso seguro

Configurar um recurso privado para ser acessível por meio do dispositivo registrado ZTA (Zero Trust Access) com aplicação de nuvem

1. Navegue até Recursos > Destinos > Recursos particulares > Clique em +Adicionar

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

Acesso seguro - Configuração de recursos privados

2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do 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

Acesso seguro - Configuração de recursos privados

3. Informe o FQDN do recurso privado que deseja acessar. Também podemos definir o endereço IP do recurso privado. Para obter mais informações, consulte [Adicionar um recurso privado](#)

4. Selecione o servidor DNS interno para resolver o problema do domínio

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)

Acesso seguro - Configuração de recursos privados

5. Selecionar Métodos de Conexão de Ponto de Extremidade

6. Selecionar FTD como pontos de imposição locais

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



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

Acesso seguro - Configuração de recursos privados



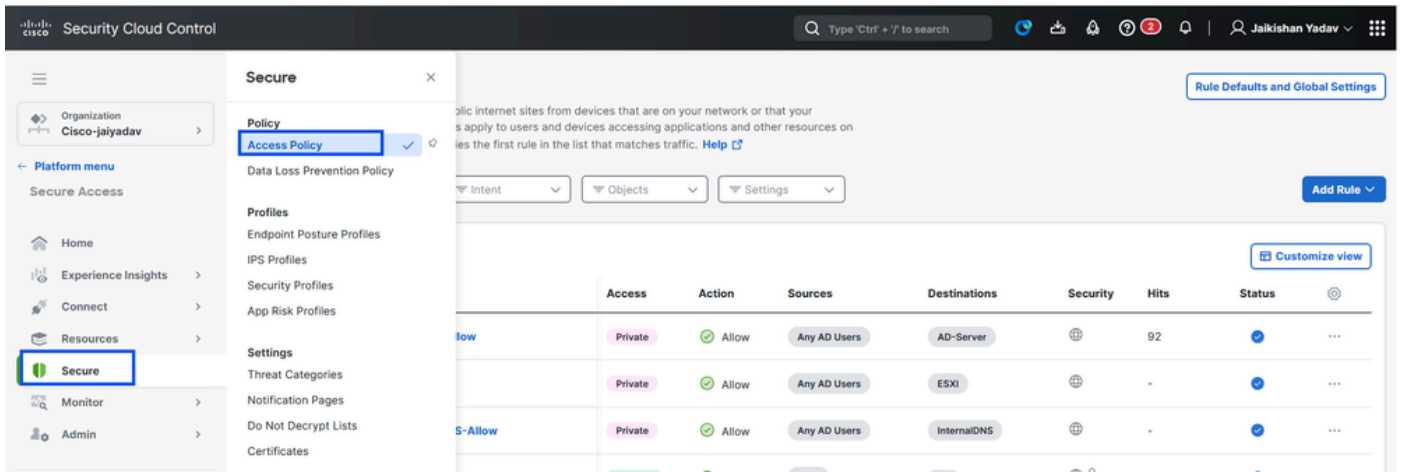
Note: Dependendo do tipo de inscrição que você selecionar, essa alteração associará automaticamente a PR ao FTD e acionará uma implantação de política

7. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA. Para obter mais informações, consulte [Regra de acesso privado](#)

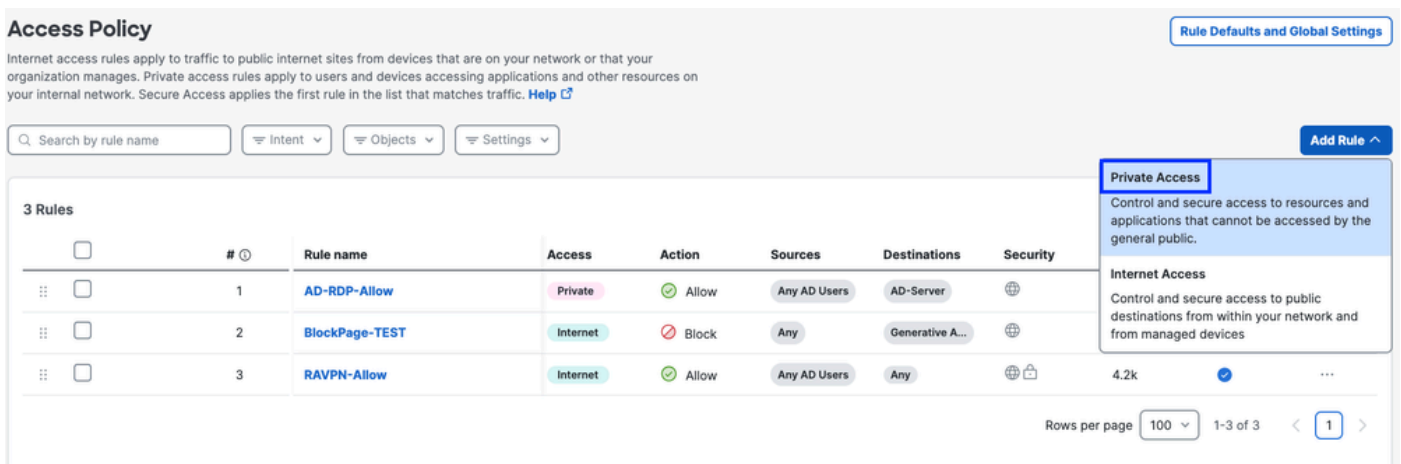
1. Navegue até Proteger > Política de acesso



Acesso seguro - Configuração de recursos privados

2. Clique em Adicionar Regra e escolha Acesso Particular.

Na parte superior da regra há um resumo que descreve os componentes configurados da regra.



Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra

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.

Acesso seguro - Configuração da política de acesso

4. Selecione a ação da regra e selecione origem e 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

Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint

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](#)

Acesso seguro - Configuração da política de acesso

6. Configurar segurança

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](#)

Acesso seguro - Configuração da política de acesso

7. Clique em Salvar

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 >

Acesso seguro - Configuração da política de acesso

Etapa 3 - Verificar a associação de PR no FTD

1. Navegue até Conectar > Conexões de Rede > FTDs

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' window with a 'Network Connections' section. Under 'Network Connections', there are two items: '0 Warning' and '1 Connected'. The '1 Connected' item is highlighted, and a 'FTDs' link is visible below it. The interface also shows a search bar at the top and a user profile 'Jaikishan Yadav'.

Acesso seguro - Verificação de PR

2. Clique em FTD > Exibir recursos associados 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	Networks
LAN (Default trusted network)	1 DNS Servers

[Edit assignment](#) [+ Trusted network](#)

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status	
Synced	1

[View resources associated to this FTD](#)

[Associate Resources](#)

Acesso seguro - Verificação de PR

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](#)

Acesso seguro - Verificação de PR

3. Clique em Close

4. Verifique se o status, o Recurso Associado e a Configuração devem estar no estado Sincronizado

The screenshot displays the 'Network Connections' section of the Palo Alto Networks management console. It shows 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. The 'FMC_FTD' entry is highlighted, showing a 'Synced' status. To the right, a detailed view for 'FMC_FTD' is shown, including 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 (LAN), and Associated Resources (1 DNS Servers).

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

Acesso seguro - Verificação de PR

5. Verifique se a configuração foi enviada por push para o FTD

Faça login no FTD cli e navegue até o 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 - Verificação de PR

Etapa - 4 Adicionar recurso privado ao perfil ZTA

1. Navegue até Connect > End User Connectivity > Zero Trust Access e clique em 3 pontos para editar o 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](#)

Zero Trust Access | Virtual Private Network | Internet Security

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

Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

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: ZTAProfile | Priority: 1. Current profile

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

Search by destination

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

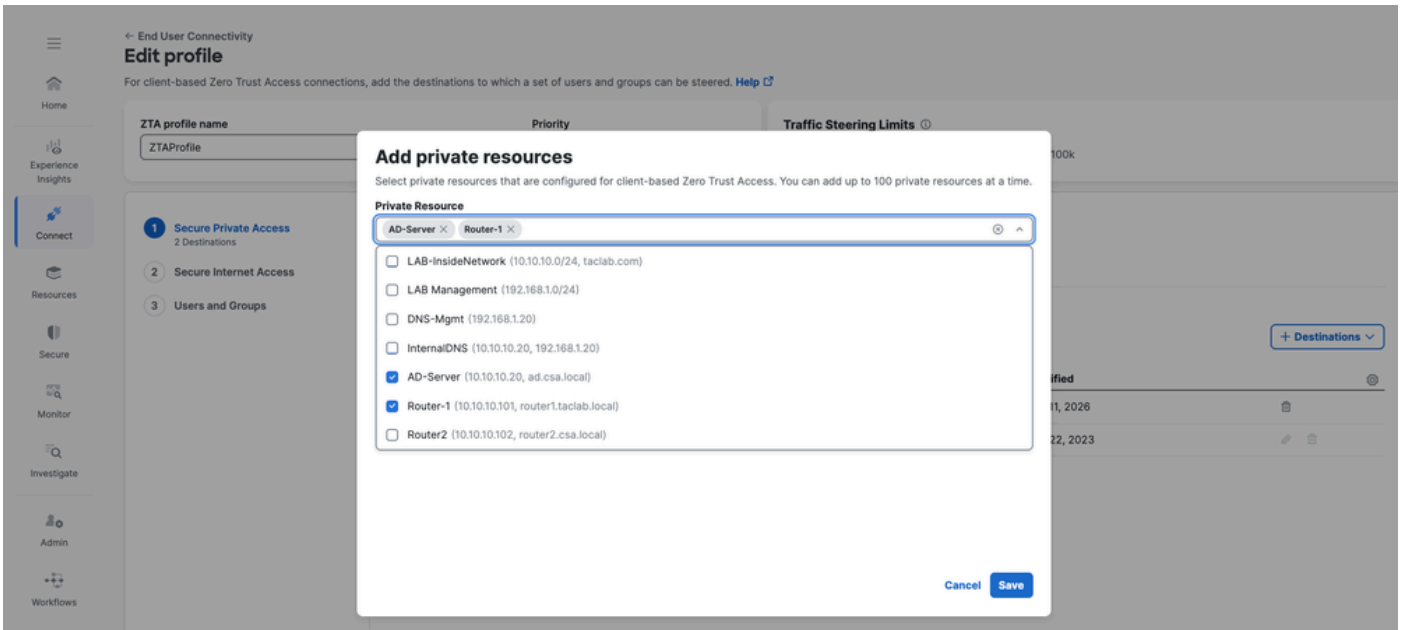
Private Resource

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

Add Destination

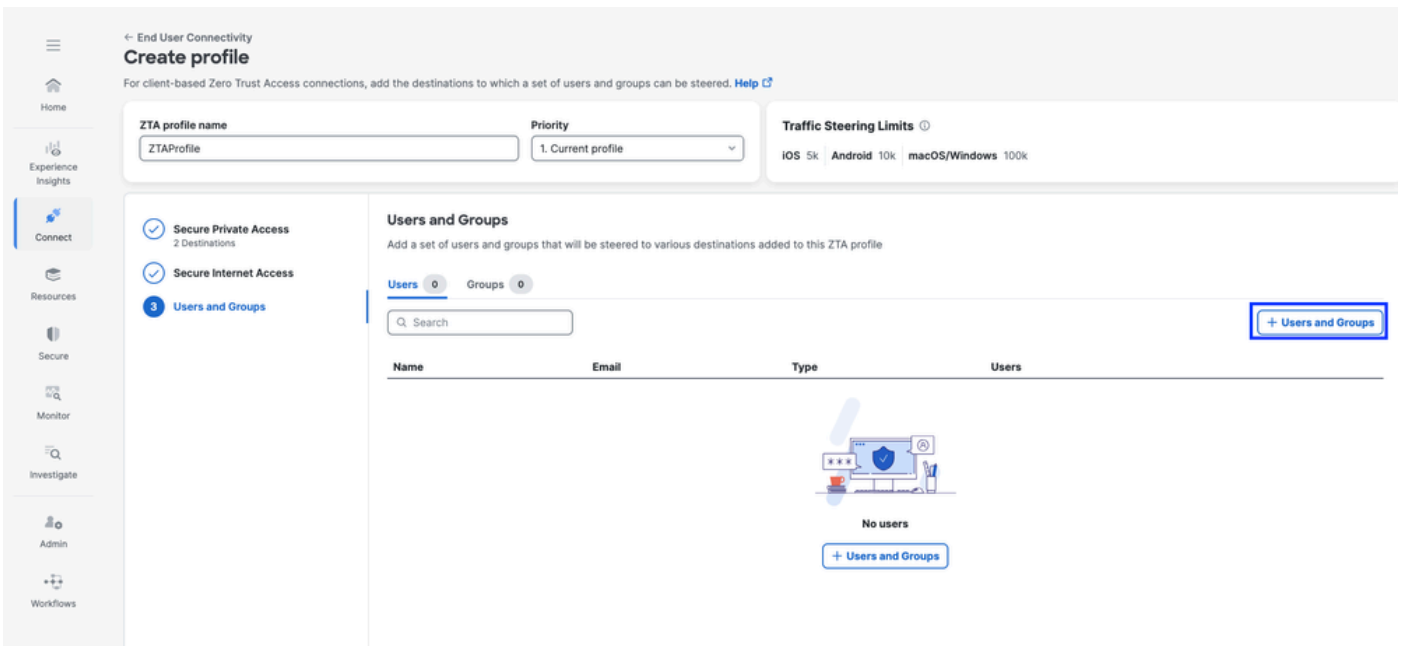
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Acesso seguro - perfil ZTA



Acesso seguro - perfil ZTA

3. Adicionar usuários e grupos



Acesso 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

Search:

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

Rows per page: 10

Back Close

Acesso seguro - perfil ZTA

Etapa 5 - Verificar o acesso ao recurso privado

1. Verifique se o usuário remoto pode resolver o FQDN do 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
```

Acesso seguro - Teste de PR

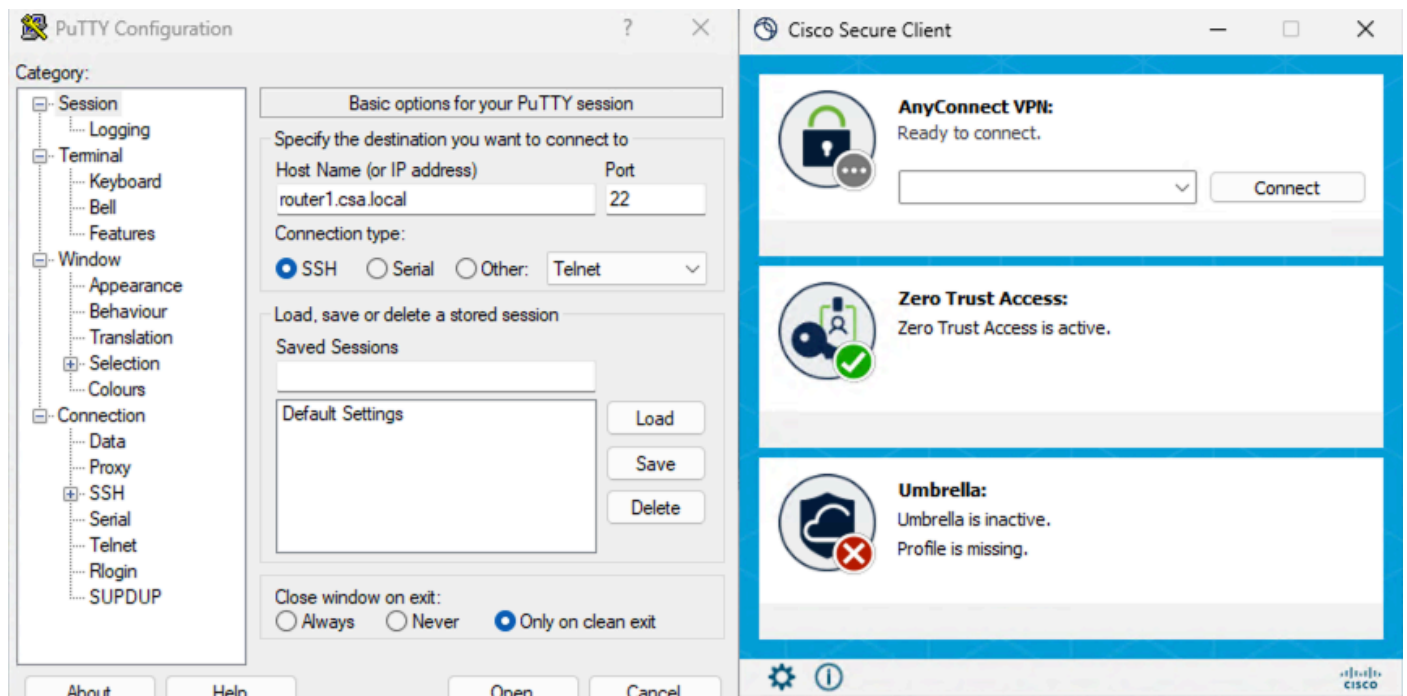
2. Verificar se o FTD pode acessar o recurso privado usando o FQDN

```
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# █
```

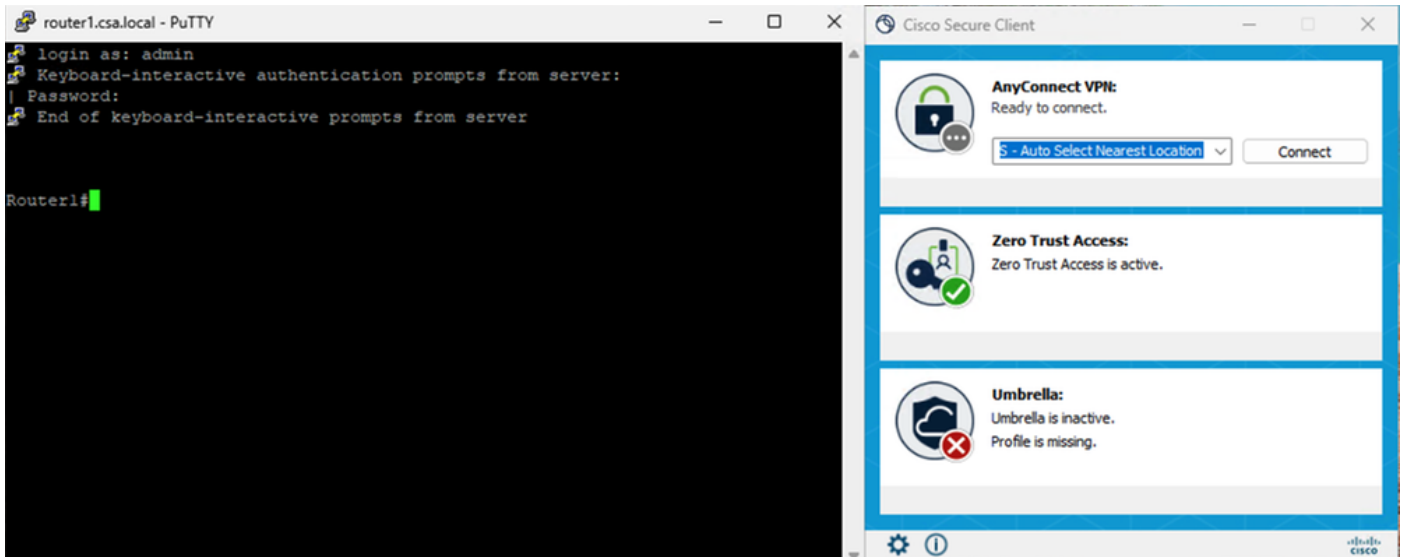
Acesso seguro - Teste de PR

3. Testar a conexão SSH com o recurso privado

Acessar a PR usando o FQDN

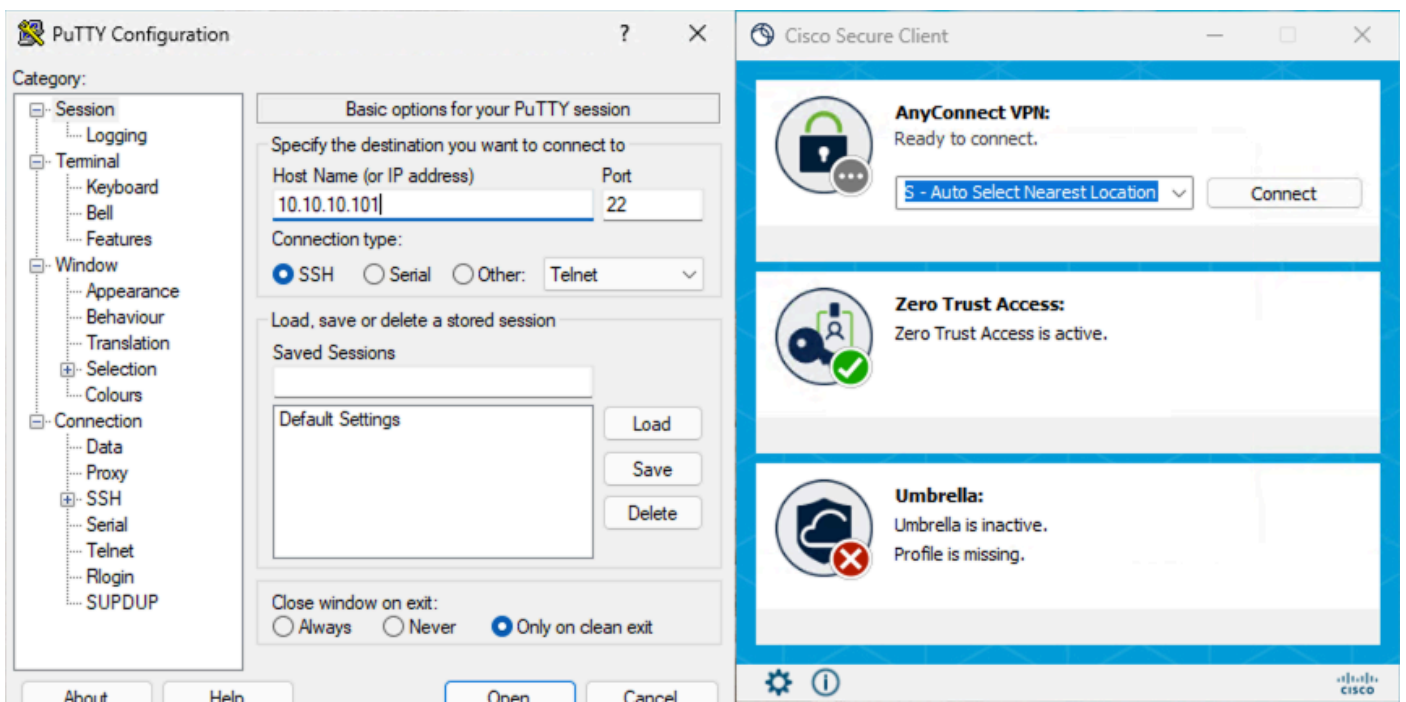


Acesso seguro - Teste de PR

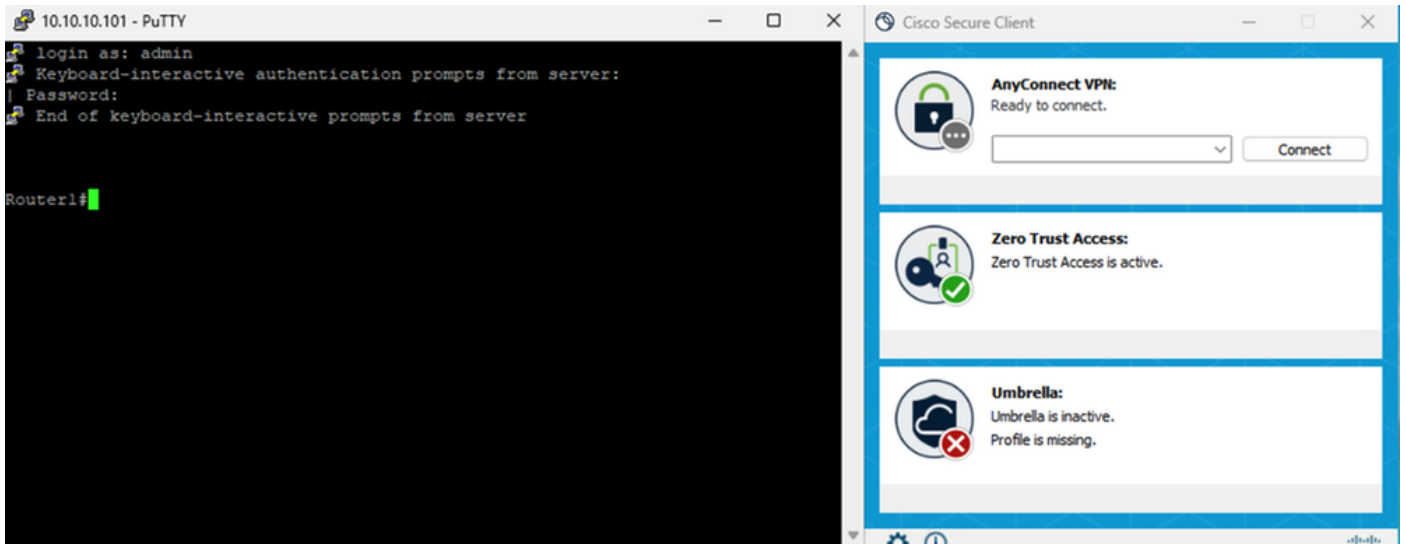


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP



Acesso seguro - Teste de PR



Acesso seguro - Teste de PR

4. Verificar logs de Pesquisa de Atividade de Acesso Seguro

Activity Search

Filters: Search by domain, identity, or URL. Domain: router1.csa.local, Response: Allowed. 4 Total results.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location
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
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
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
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

Acesso seguro - Pesquisa de atividades

4 Total results. Viewing activity from Jan 9, 2026 6:01 PM to Jan 10, 2026 6:01 PM.

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: -

Acesso seguro - Pesquisa de atividades

Activity Search

Search by domain, identity, or URL **Advanced** CLEAR

Filters: 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

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	76.39.159.129
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	76.39.159.129
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	76.39.159.129
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	76.39.159.129
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	76.39.159.129
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	76.39.159.129
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	76.39.159.129

Acesso seguro - Pesquisa de atividades

7 Total Viewing activity from Jan 9, 2026 6:09 PM to Jan 10, 2026 6:09 PM

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

Acesso seguro - Pesquisa de atividades

5. Verificar os eventos de conexão do FMC

Firewall Management Center Events & Logs / Analysis / Unified Events

Search Deploy admin

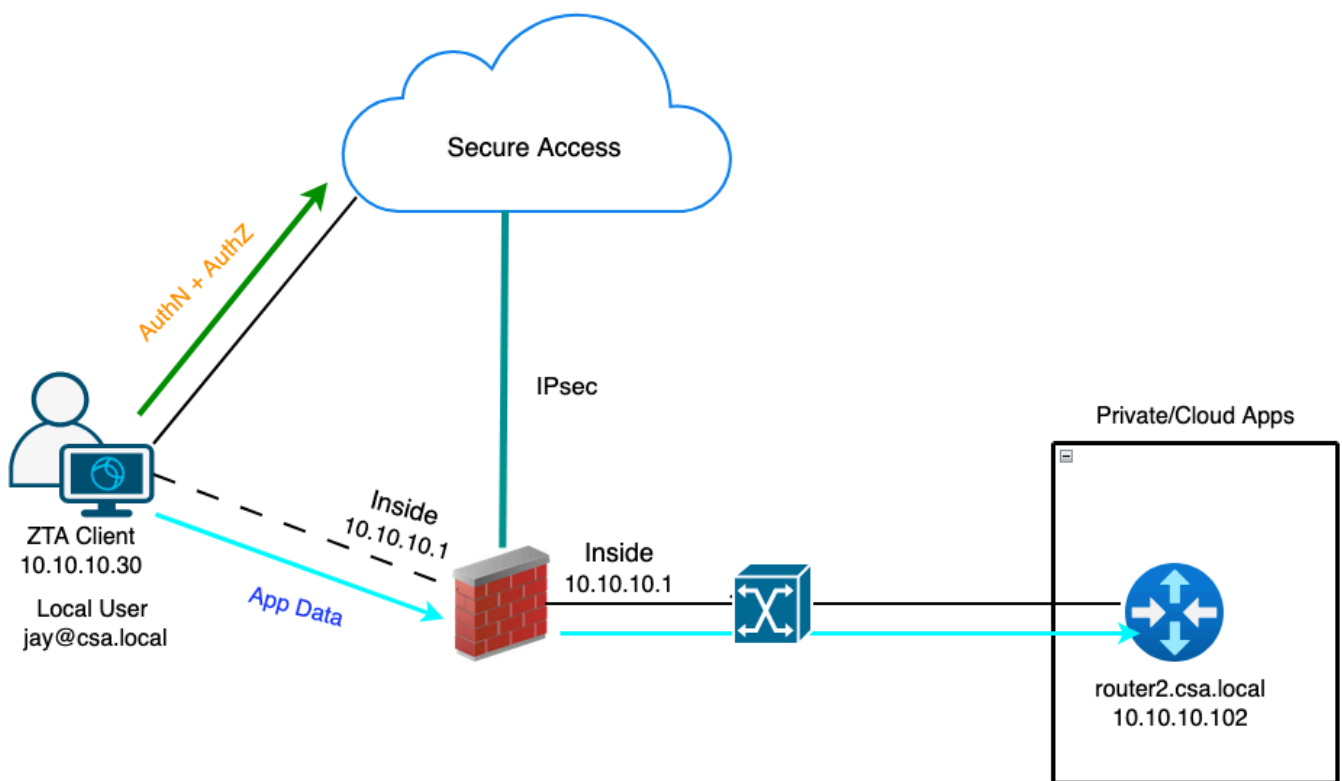
Monitor Destination IP: 10.10.10.101

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 teste 3 - Usuário local - Aplicação local

Acessar um recurso privado por meio da aplicação local como um usuário local, nesse tipo de avaliação de política de aplicação acontece no acesso seguro, mas os dados do aplicativo permanecem locais para o FTD. Por exemplo , um cliente ou usuário registrado ZTA conectado à rede doméstica e tentando acessar um recurso privado que está por trás da interface interna do FTD . Se o recurso privado estiver por trás do DMZ ou de qualquer outra interface do FTD, teríamos que criar uma regra de acesso no FTD para permitir o tráfego entre o IP do cliente ou a rede e o recurso privado.

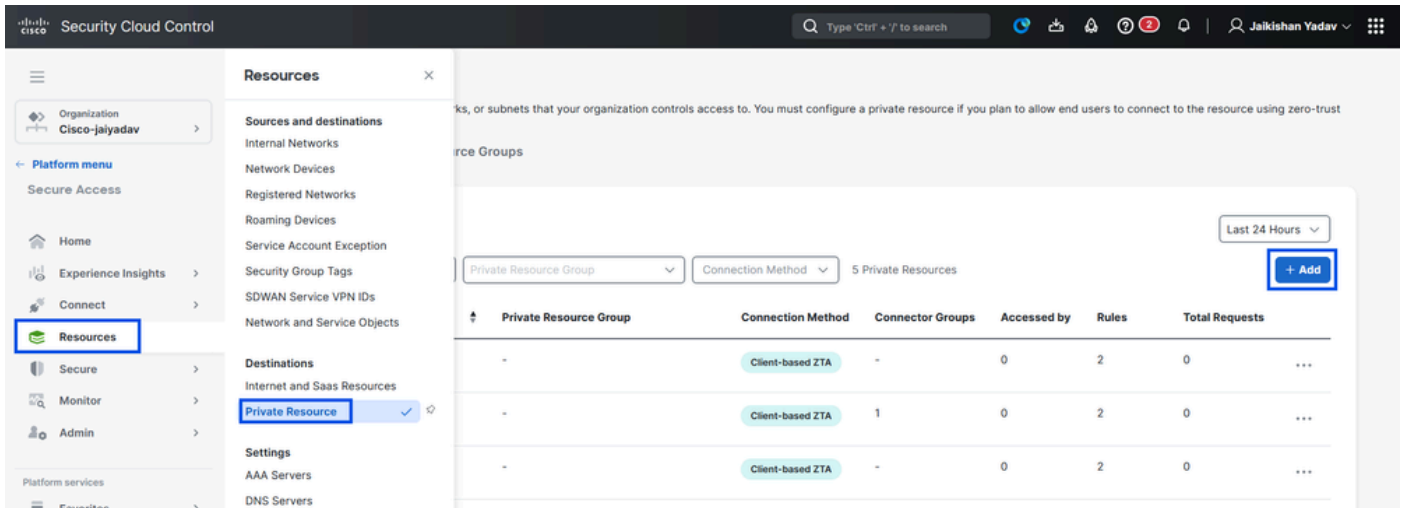


ZTA universal - Topologia de caso de teste

Etapa 1 - Definir um recurso privado no acesso seguro

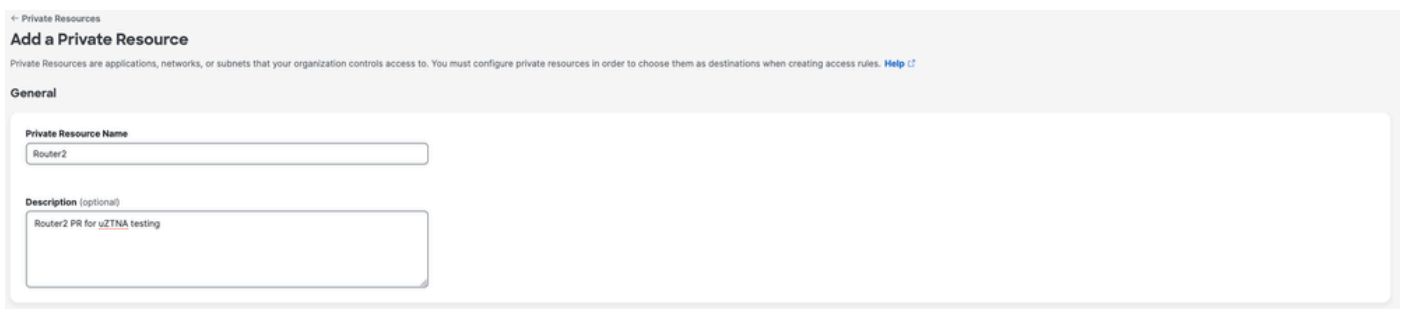
Configurar um recurso privado para ser acessível por meio do dispositivo registrado ZTA (Zero Trust Access) com aplicação de nuvem

1. Navegue até Recursos > Destinos > Recursos particulares > Clique em +Adicionar



Acesso seguro - Configuração de recursos privados

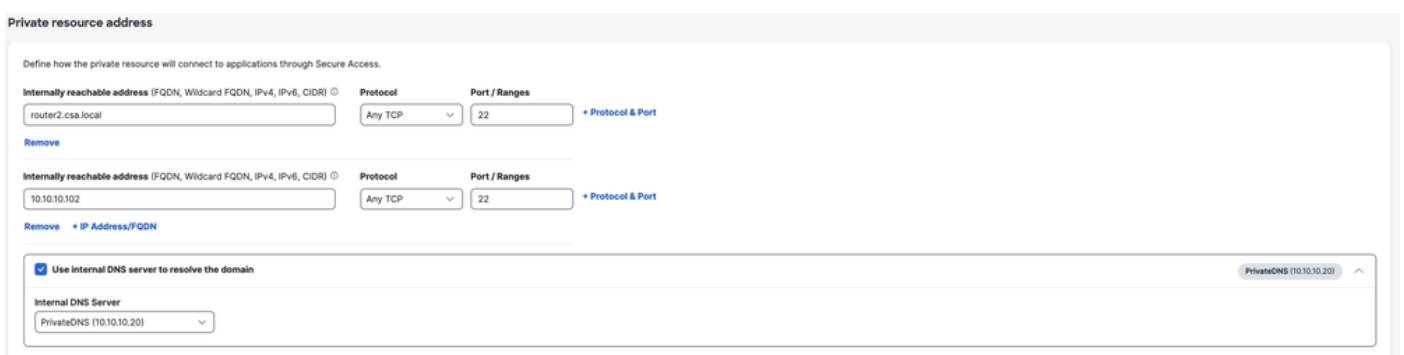
2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do recurso.



Acesso seguro - Configuração de recursos privados

3. Informe o FQDN do recurso privado que deseja acessar. Também podemos definir o endereço IP do recurso privado. Para obter mais informações, consulte [Adicionar um recurso privado](#)

4. Selecione o servidor DNS interno para resolver o problema do domínio



5. Selecionar Métodos de Conexão de Ponto de Extremidade

6. Selecionar FTD como pontos de imposição locais

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



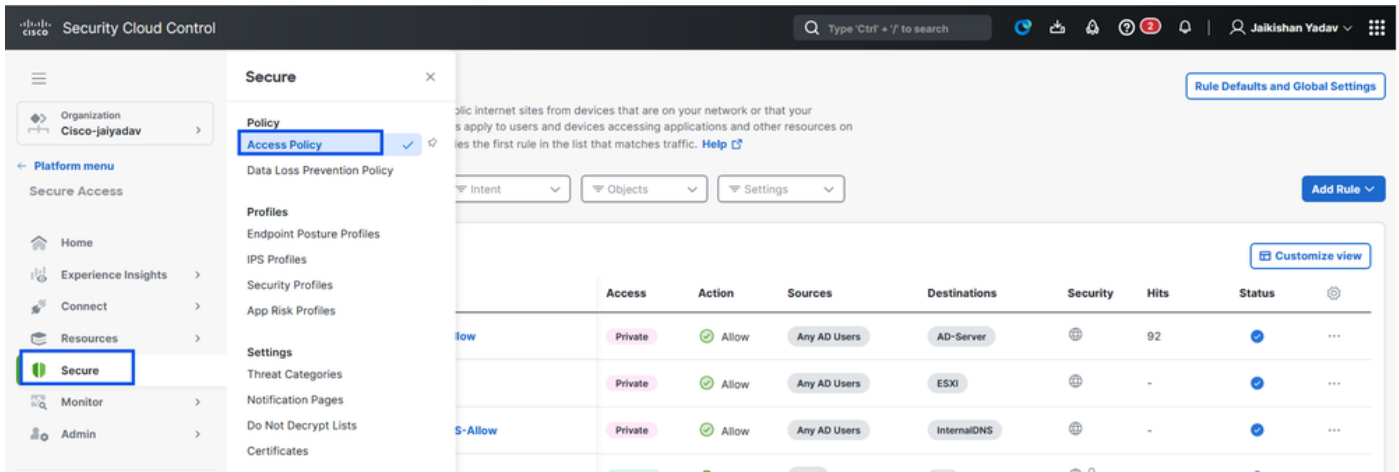
Note: Dependendo do tipo de inscrição que você selecionar , essa alteração associará automaticamente a PR ao FTD e acionará uma implantação de política

7. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA . Para obter mais informações, consulte [Regra de acesso privado](#)

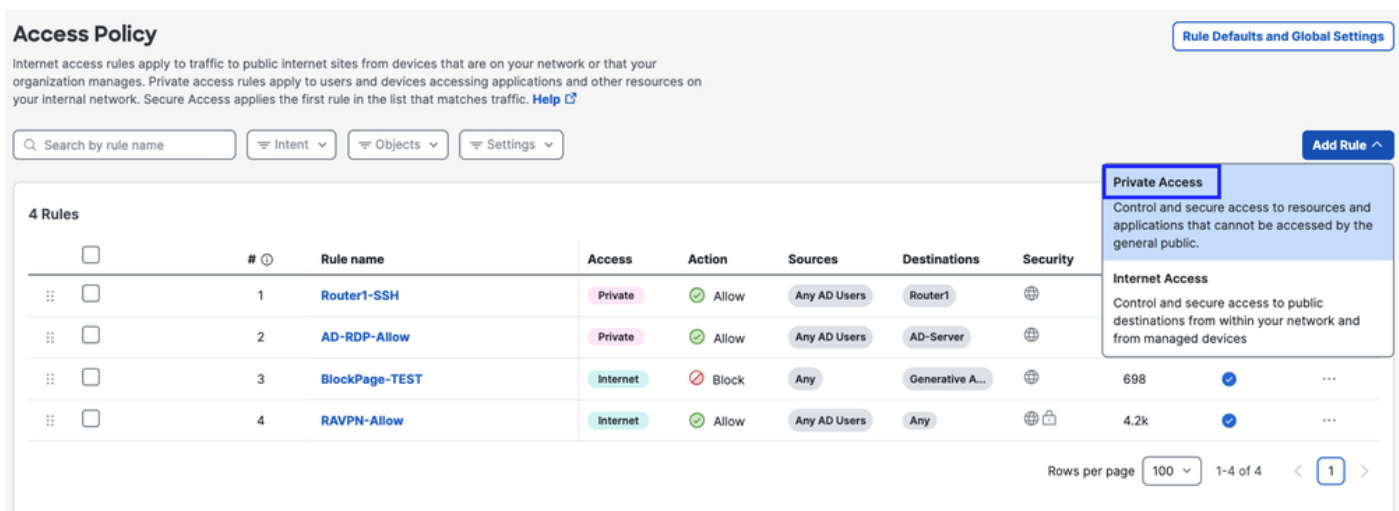
1. Navegue até Proteger > Política de acesso



Acesso seguro - Configuração da política de acesso

2. Clique em Adicionar Regra e escolha Acesso Particular.

Na parte superior da regra há um resumo que descreve os componentes configurados da regra.



Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra

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.

Acesso seguro - Configuração da política de acesso

4. Selecione a ação da regra e selecione origem e 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

Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint

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](#)

Acesso seguro - Configuração da política de acesso

6. Configurar segurança

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](#)

Acesso seguro - Configuração da política de acesso

7. Clique em Salvar

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

Acesso seguro - Configuração da política de acesso

Etapa 3 - Verificar a associação de PR no FTD

1. Navegue para conectar > Conexões de Rede > FTDs

The screenshot shows the Cisco Security Cloud Control interface. The 'Connect' section is active, with 'Network Connections' selected under 'Essentials'. The 'FTDs' tab is highlighted, showing a summary of 0 Warning and 1 Connected. The interface includes a search bar, navigation menu, and a table for Tunnel Groups.

Acesso seguro - Verificação de PR

2. Clique no FTD > Exibir recursos associados 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	Networks
LAN (Default trusted network)	1 DNS Servers

Edit assignment + Trusted network

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status
Synced 2

View resources associated to this FTD

Associate Resources

Acesso seguro - Verificação de PR

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. Clique em Close

4. Verifique se o status, o Recurso Associado e a Configuração devem estar no estado Sincronizado

The screenshot displays the 'Network Connections' page in the Palo Alto Networks management console. The 'FTDs' tab is active, showing a summary of '1 Synced' FTDs. Below this, a table lists the configured FTDs 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 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 12 Jan 2026, 6:29 AM UTC), 'Assigned Trusted Network' (LAN, 1 DNS Servers), and 'Associated Resources' (2 resources associated).

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

5. Verifique se a configuração foi enviada por push para o FTD

Faça login no FTD cli e navegue até o modo LINA

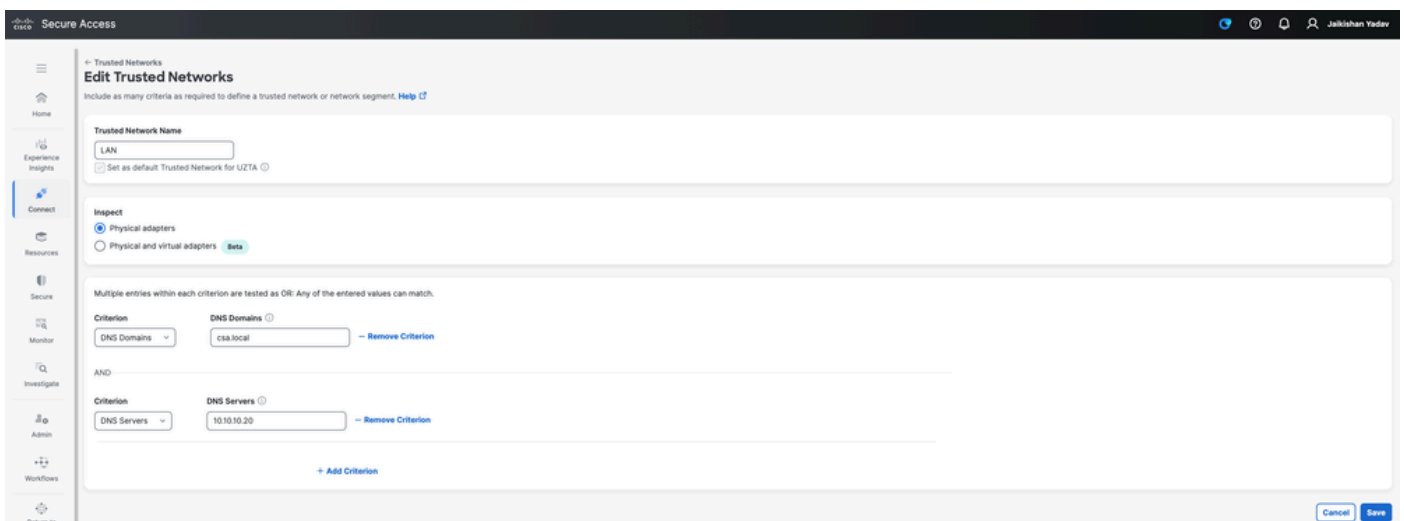
show running-config object application

```
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
```

Acesso seguro - Verificação de PR

Etapa - 4 Configurar " Gerenciar redes confiáveis ou configurações ZTA"

Navegue para Connect > End User Connectivity > Zero Trust Access > ZTA Settings e configure Trusted Networks



Acesso seguro - Configuração TND

Etapa -5 Adicionar recurso privado ao perfil ZTA

1. Navegue até Connect > End User Connectivity > Zero Trust Access e clique em 3 pontos para editar o 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	ZTAPProfile	2 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	1 Users 0 Groups	Jan 25, 2026

Edit Delete

Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

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](#)

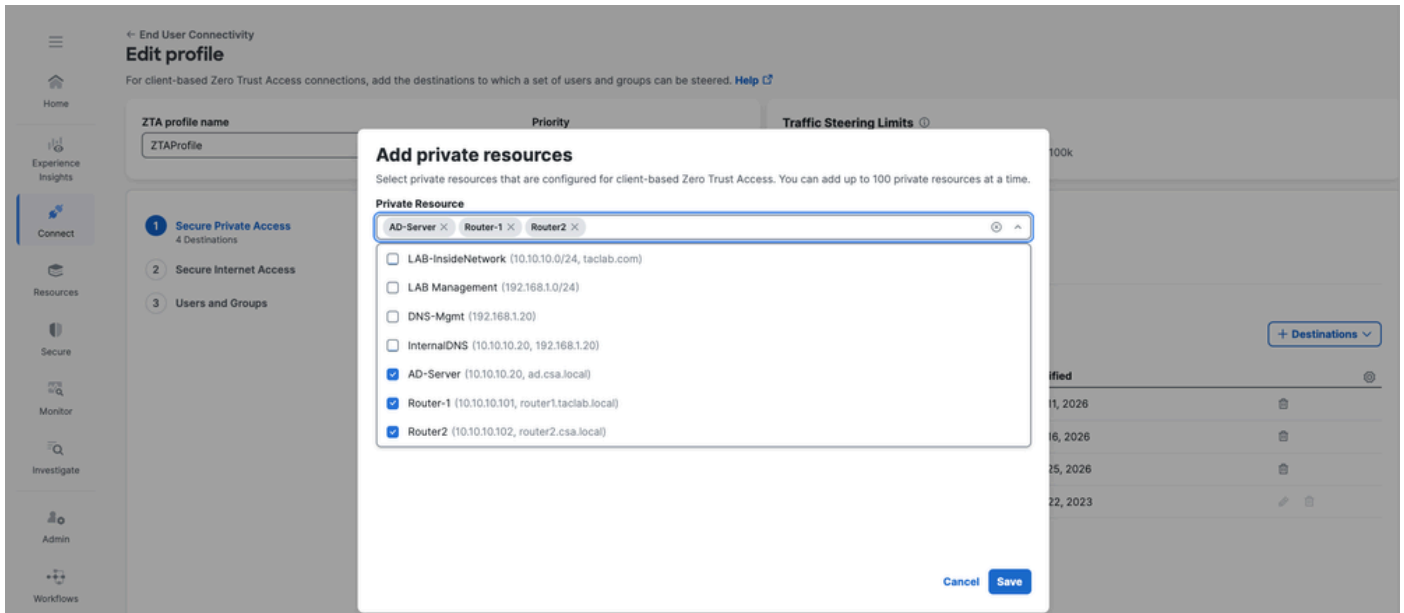
Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

+ Destinations

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

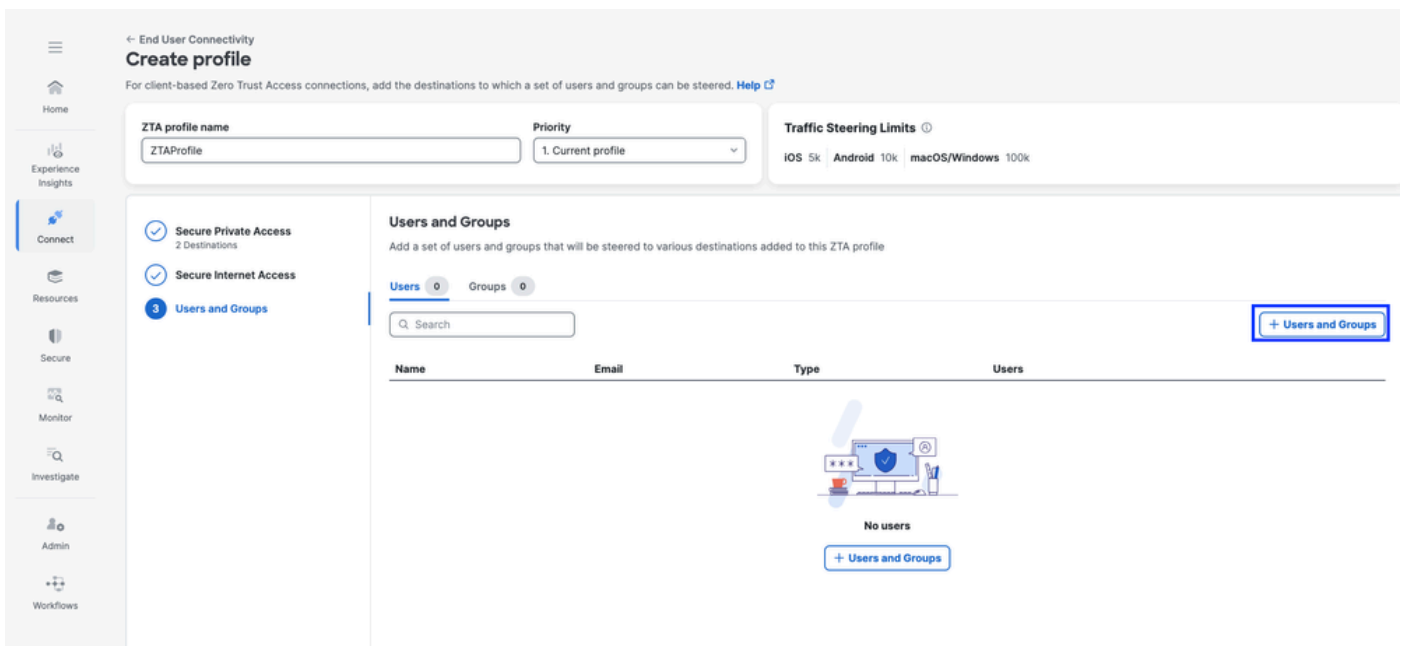
Add Destination
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Acesso seguro - perfil ZTA



Acesso seguro - perfil ZTA

3. Adicionar usuários e 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	-

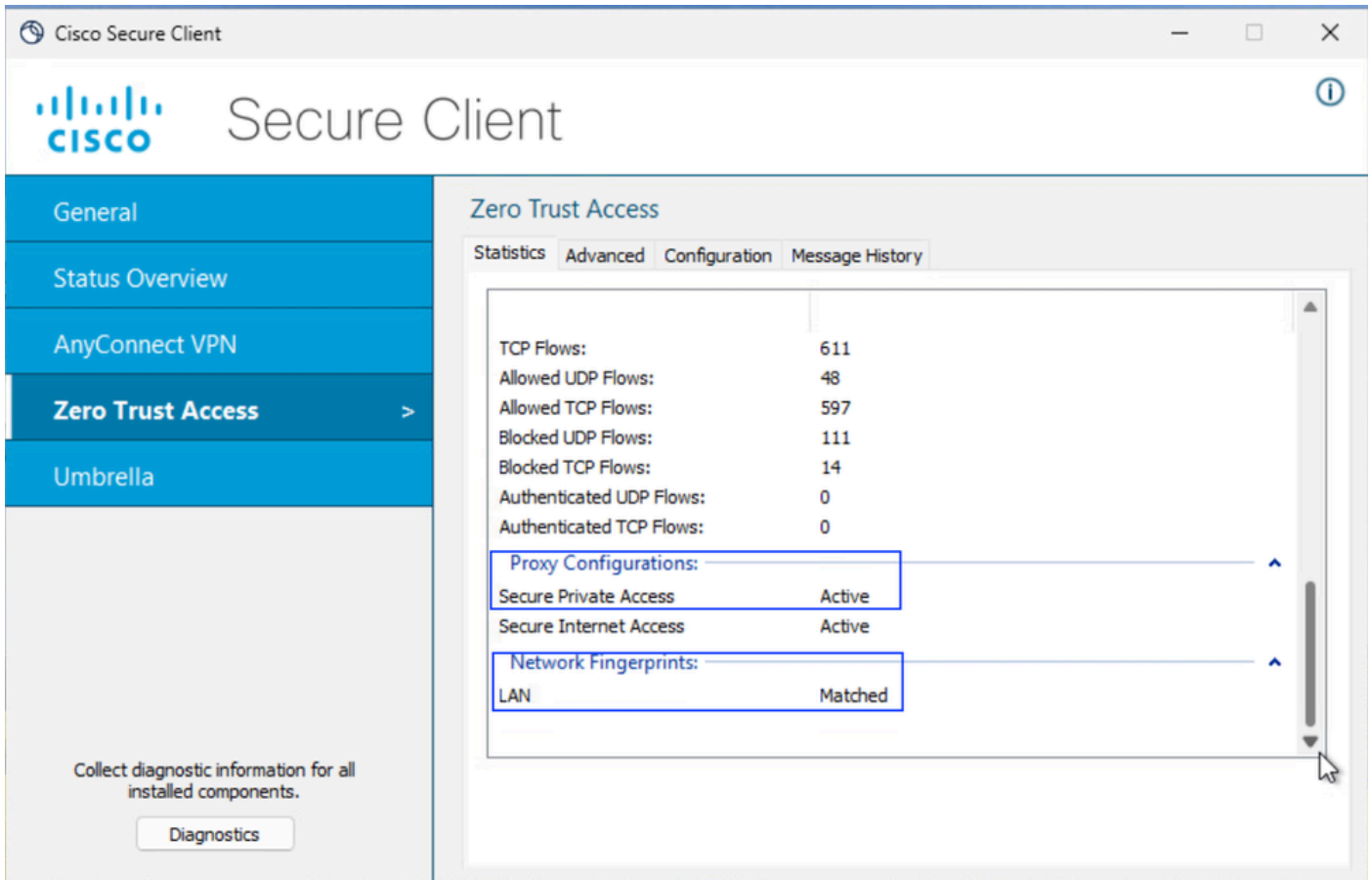
Rows per page: 10 < >

Back Close

Acesso seguro - perfil ZTA

Etapa - 6 Verificar o acesso ao recurso privado

1. Verifique a impressão digital de rede para ZTA TND



Acesso seguro - Teste de PR

2. Verifique se o usuário remoto pode resolver o FQDN do 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
```

Acesso seguro - Teste de PR

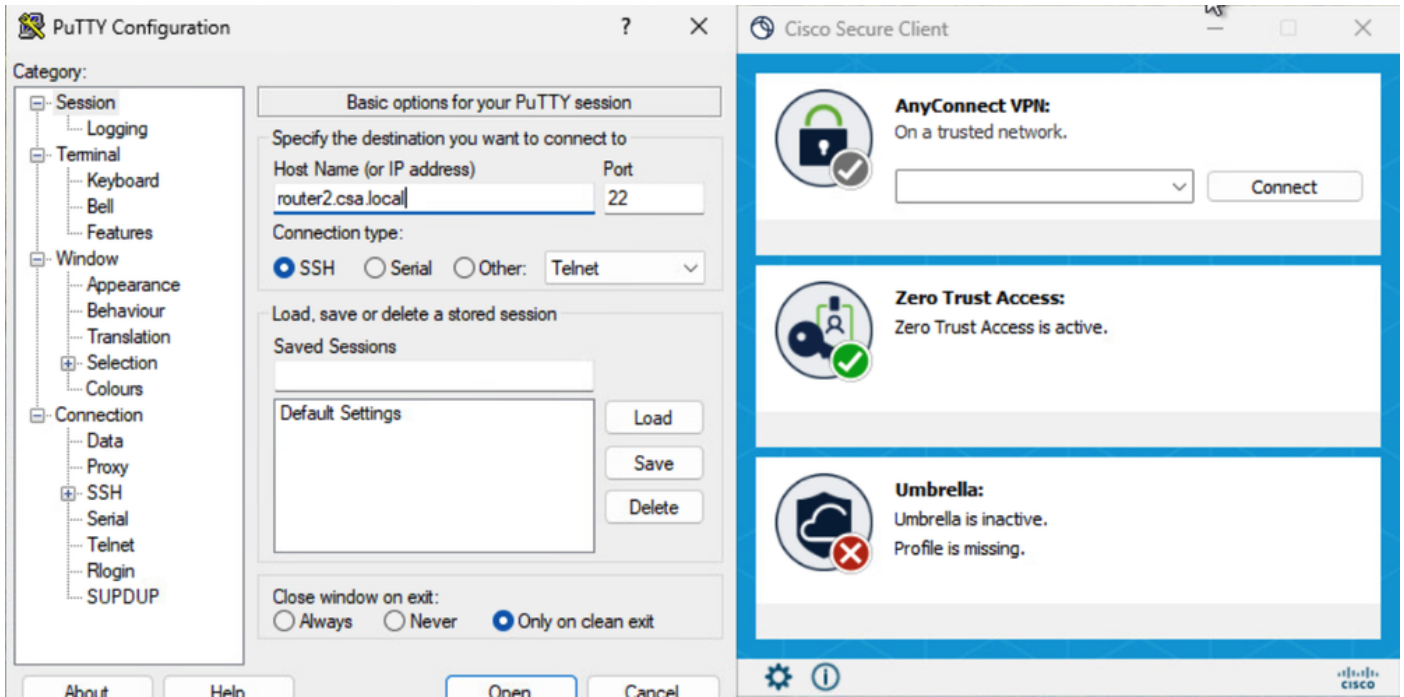
3. Verificar se o FTD pode acessar o recurso privado usando o FQDN

```
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# █
```

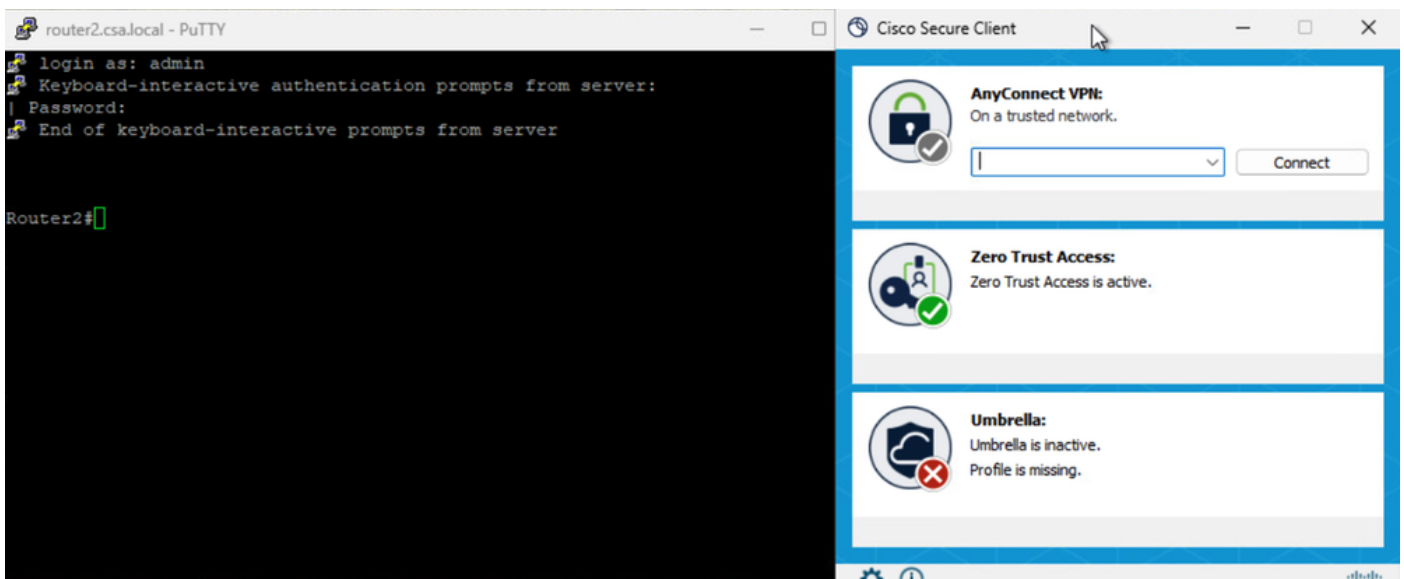
Acesso seguro - Teste de PR

4. Testar a conexão SSH com o recurso privado

Acessar a PR usando o FQDN

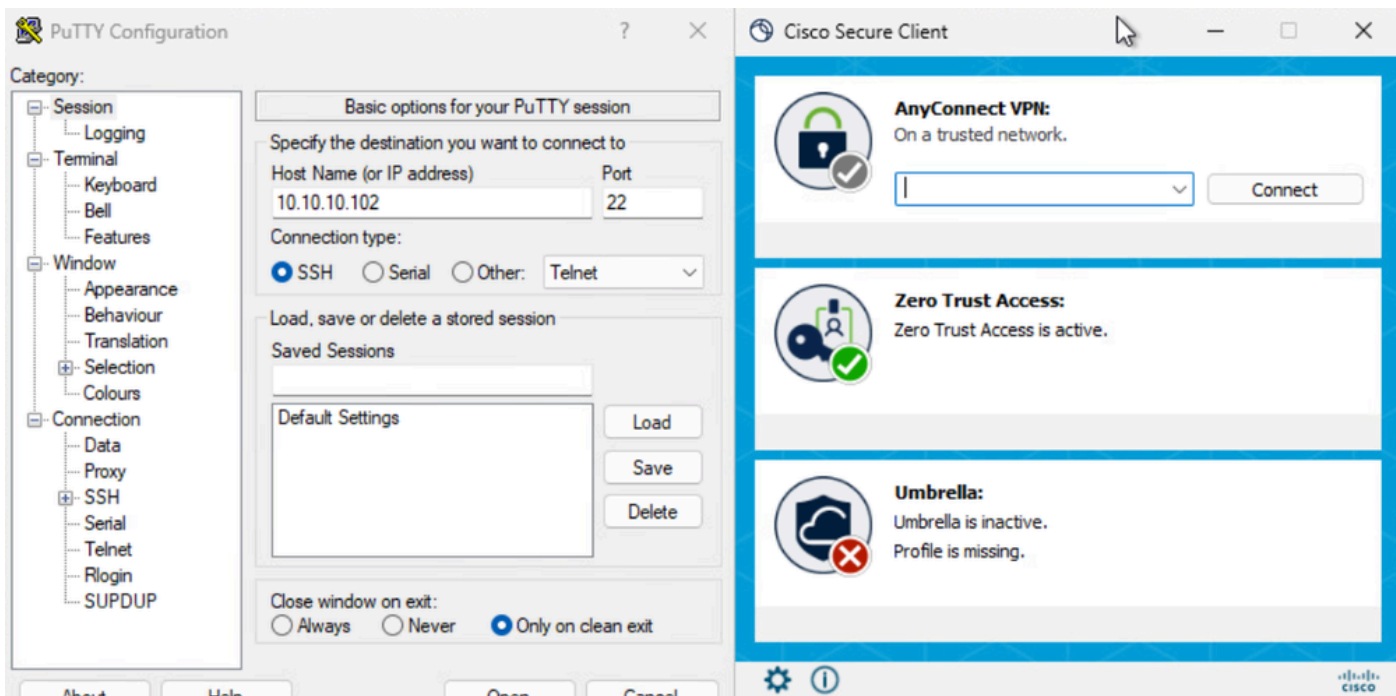


Acesso seguro - Teste de PR

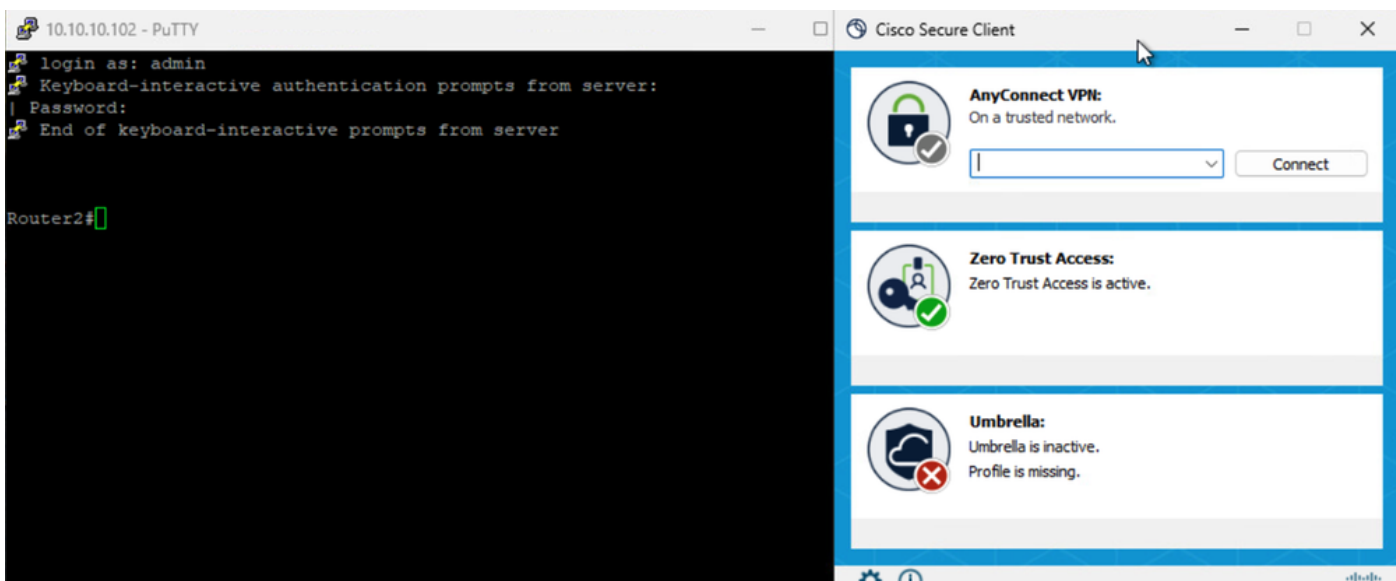


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP



Acesso seguro - Teste de PR



Acesso seguro - Teste de PR

5. Verificar logs de Pesquisa de Atividade de Acesso Seguro

Activity Search

Activity Search interface showing search filters and results for domain router2.csa.local.

Filters: DOMAIN: router2.csa.local

Search filters: Search by domain, identity, or URL

Response: Allowed, Advanced, Blocked

Identity Type: AD Users, AD Groups, AD Devices, SAML Users

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS
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

Acesso seguro - Pesquisa de atividades

Activity Search

Activity Search interface showing search filters and results for response Allowed.

Filters: RESPONSE: Allowed

Search filters: Search by domain, identity, or URL

Response: Allowed, Advanced, Blocked

Identity Type: AD Users, AD Groups, AD Devices, SAML Users

Enforced By: Secure Access Cloud, FTD, Umbrella Cloud

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/App
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

Event Details:

- Action: Allowed
- Block Reason: -
- Connection Method: ZTA Client-based
- Time: Feb 23, 2026 3:33 AM
- Access details:
 - Identity: jay (jay@csa.local)
 - ZTNA Client
 - Rule Name: Router2-SSH-Allow
 - Resource/Application: Router2
 - Zero Trust Access Profile: ZTAProfile
 - Trusted Network: No Match
 - Enforcement Point: FTD > FMC_FTD
 - Destination: router2.csa.local

Acesso seguro - Pesquisa de atividades

Activity Search

Activity Search interface showing search filters and results for IP address 10.10.10.102.

Filters: IP ADDRESS: 10.10.10.102, RESPONSE: Allowed

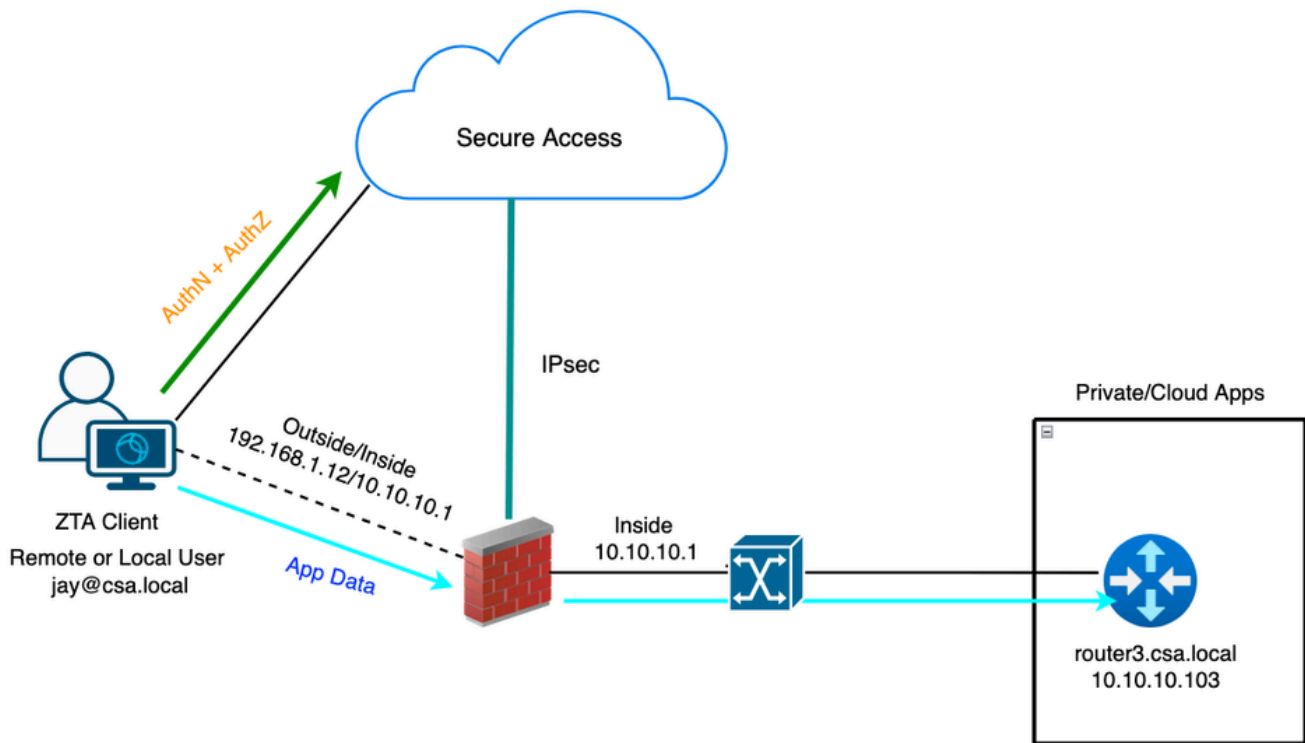
Search filters: Search by domain, identity, or URL

Response: Allowed, Advanced, Blocked

Identity Type: AD Users, AD Groups, AD Devices, SAML Users

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)	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

Acesso seguro - Pesquisa de atividades



ZTA universal - Topologia de caso de teste

Etapa 1 - Definir um recurso privado no acesso seguro

Configurar um recurso privado para ser acessível por meio do dispositivo registrado ZTA (Zero Trust Access) com aplicação de nuvem

1. Navegue até Recursos > Destinos > Recursos particulares > Clique em +Adicionar

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar shows the navigation menu with 'Resources' selected. The main content area displays the 'Resources' configuration page. The page title is 'Resources' and it includes a search bar and a user profile. The main content area shows a table of private resources with columns for 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. A '+ Add' button is visible in the top right corner of the table area.

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

Acesso seguro - Configuração de recursos privados

2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do 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

Acesso seguro - Configuração de recursos privados

3. Informe o FQDN do recurso privado que deseja acessar. Também podemos definir o endereço IP do recurso privado. Para obter mais informações, consulte [Adicionar um recurso privado](#)

4. Selecione o servidor DNS para resolver o domínio

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)

Acesso seguro - Configuração de recursos privados

5. Selecionar Métodos de Conexão de Ponto de Extremidade

6. Selecionar FTD como pontos de imposição locais

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... 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

Acesso seguro - Configuração de recursos privados

Selecione RC se o recurso privado estiver acessível por RC, caso contrário, deixe-o em branco se o recurso privado estiver acessível por meio do grupo de túnel de rede (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. ⓘ

Acesso seguro - Configuração de recursos privados



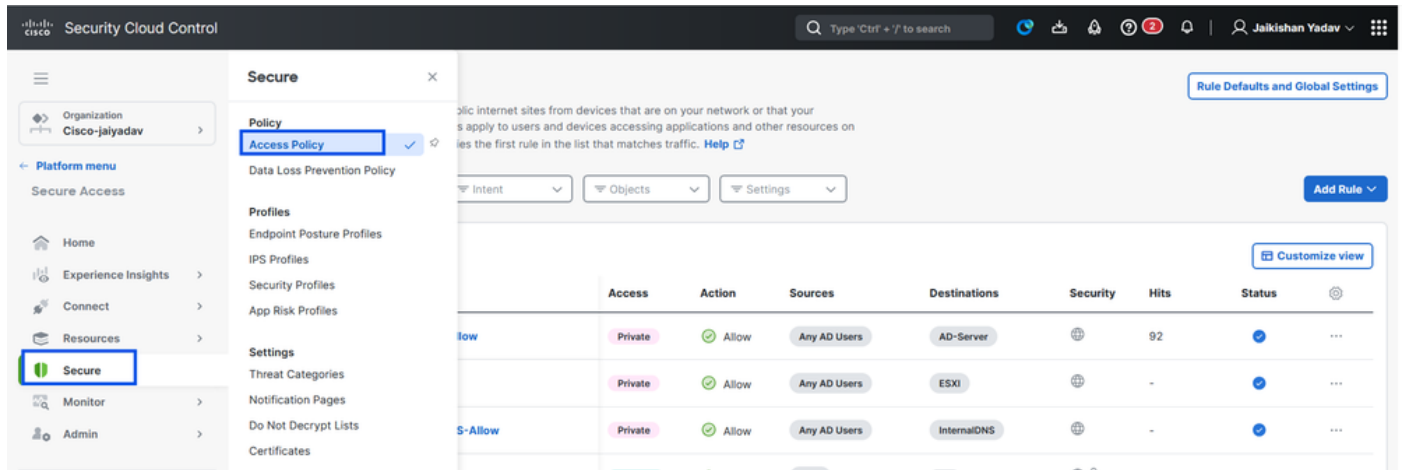
Note: Dependendo do tipo de inscrição que você selecionar, essa alteração associará automaticamente a PR ao FTD e acionará uma implantação de política

7. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA . Para obter mais informações, consulte [Regra de acesso privado](#)

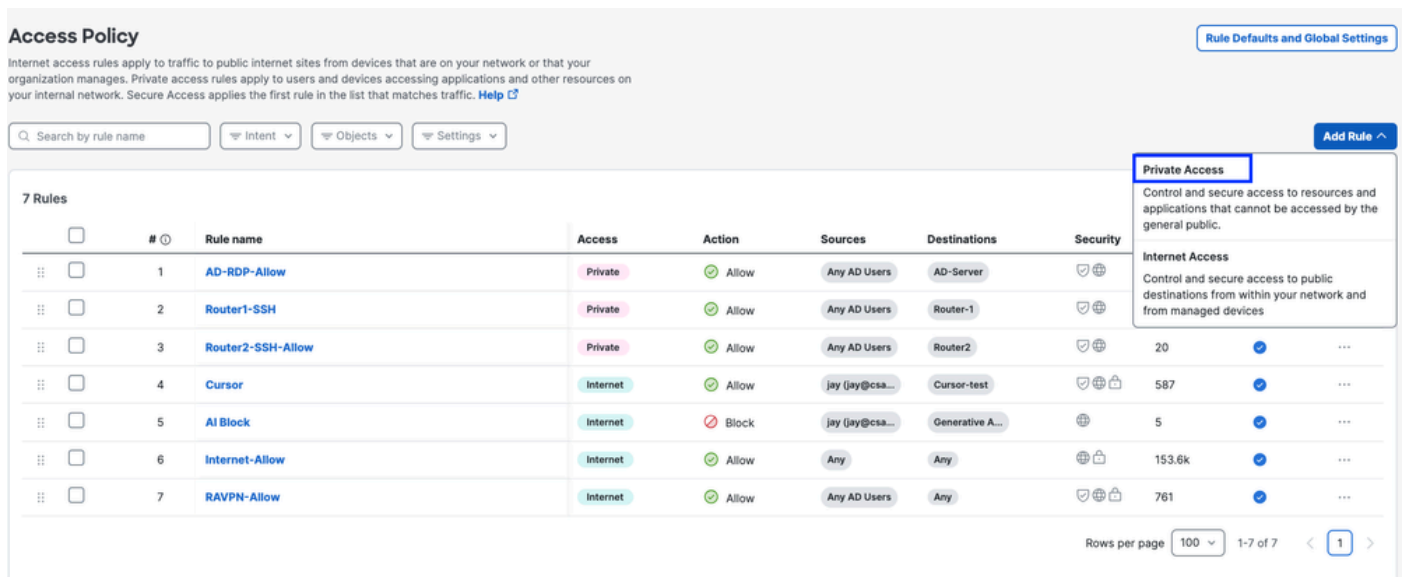
1. Navegue até Proteger > Política de acesso



Acesso seguro - Configuração da política de acesso

2. Clique em Adicionar Regra e escolha Acesso Particular.

Na parte superior da regra há um resumo que descreve os componentes configurados da regra.



Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra

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

Two action options are shown:

- Allow** (selected, indicated by a green checkmark): Allow specified traffic if security requirements are met.
- Block** (indicated by a red X): Block specified traffic.

Acesso seguro - Configuração da política de acesso

4. Seleccione a ação da regra e seleccione origem e destino

Rule name: Router3-SSH-Allow | Rule order: 8

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

Action

Allow (selected): 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 • Router3

+ AND

Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint

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](#)

Acesso seguro - Configuração da política de acesso

6. Configurar segurança

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](#)

Acesso seguro - Configuração da política de acesso

7. Clique em Salvar

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

Acesso seguro - Configuração da política de acesso

Etapa 3 - Verificar a associação de PR no FTD

1. Navegue para conectar > Conexões de Rede > 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 'Connect' dialog box with 'Essentials' selected. Under 'Essentials', 'Network Connections' is checked. Below this, there are two status indicators: '0 Warning' and '1 Connected'. The 'FTDs' section is also visible, showing a list of tunnel groups with filters for 'Region' and 'Status'.

Acesso seguro - Verificação de PR

2. Clique no FTD > Exibir recursos associados 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

```

Acesso seguro - Verificação de PR

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 <small>(Default trusted network)</small>	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](#)

Acesso seguro - Verificação de PR

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

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

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

C:\Users\jay>

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

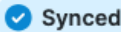
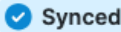
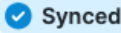
Name: ftd.csa.local
Addresses: 192.168.1.12
```

Acesso seguro - Verificação de PR

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

Acesso seguro - Verificação de PR

3. Clique em Close

4. Verifique se o status, o Recurso Associado e a Configuração devem estar no 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

Acesso seguro - Verificação de PR

5. Verifique se a configuração foi enviada por push para o FTD

Faça login no FTD cli e navegue até o modo LINA

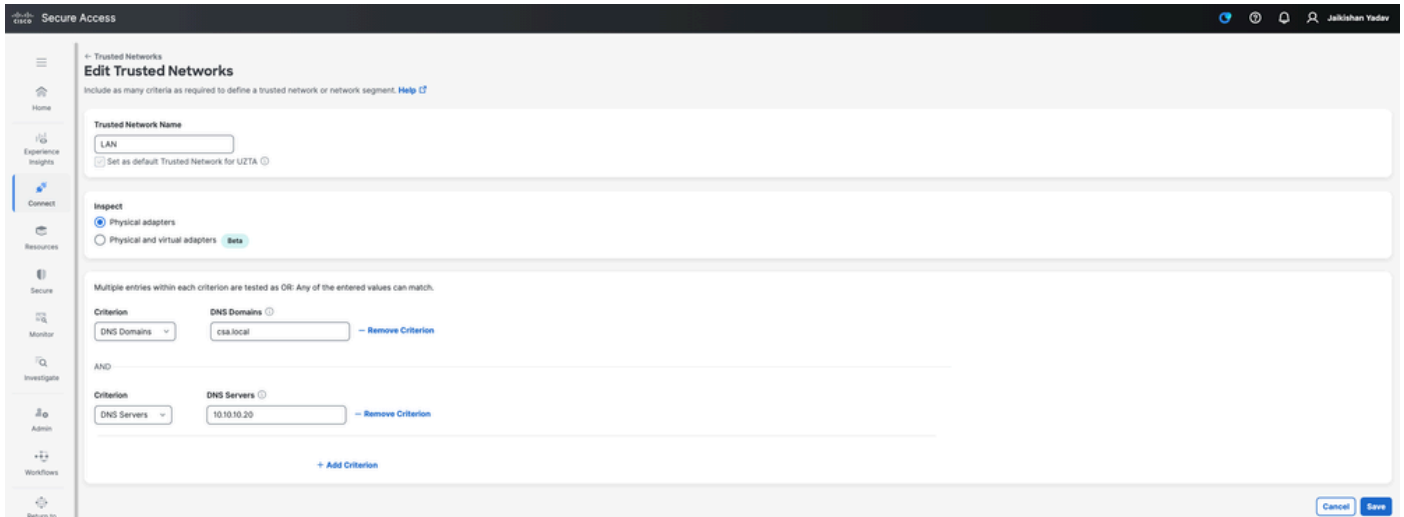
show running-config object application

```
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
```

Acesso seguro - Verificação de PR

Etapa - 4 Configurar ou verificar " Gerenciar redes confiáveis ou configurações ZTA"

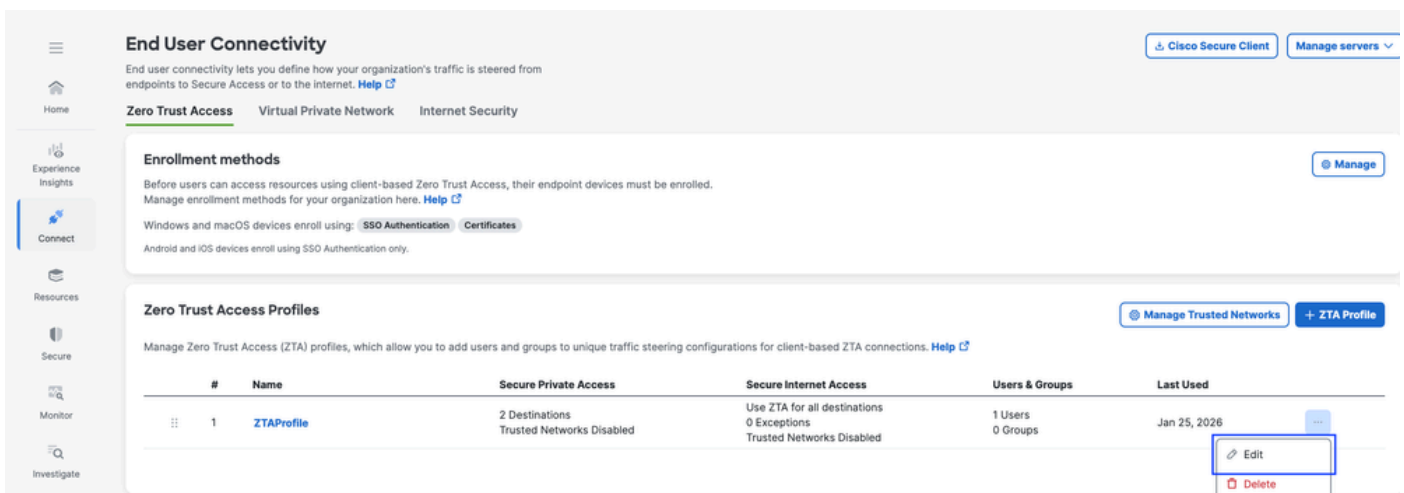
Navegue para Connect > End User Connectivity > Zero Trust Access > ZTA Settings e configure Trusted Networks



Acesso seguro - Configuração ZTA TND

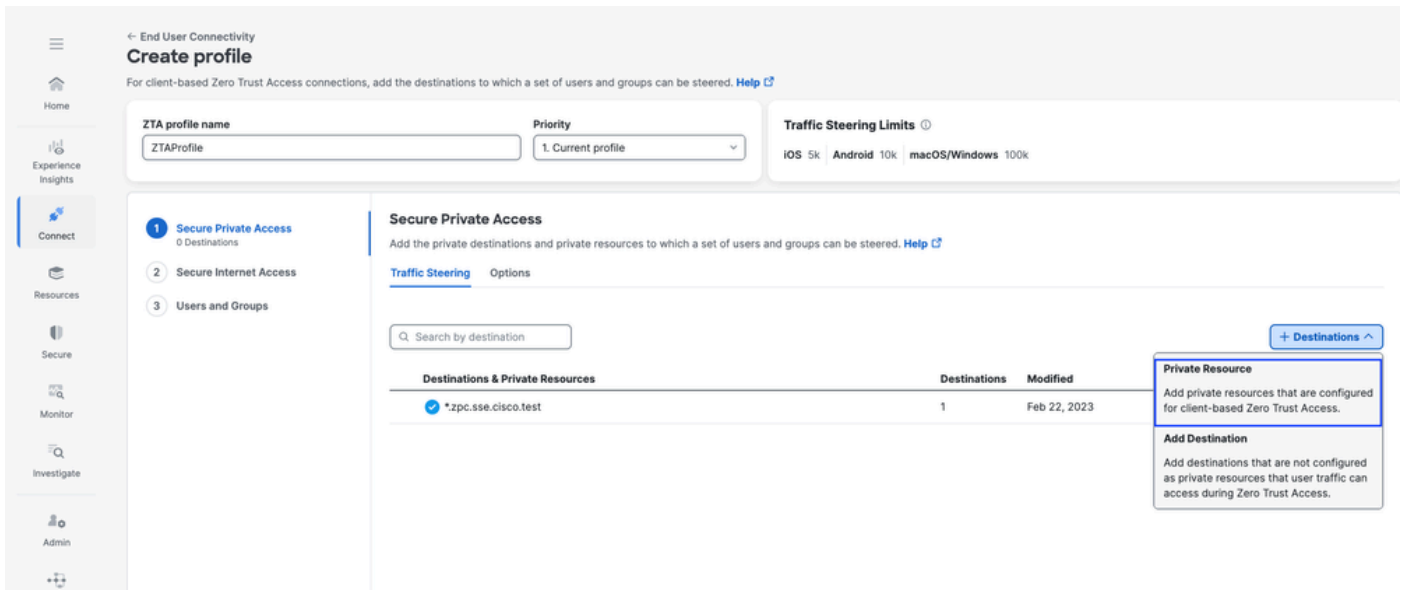
Etapa 5 - Adicionar recurso privado ao perfil ZTA

1. Navegue até Connect > End User Connectivity > Zero Trust Access e clique em 3 pontos para editar o perfil ZTA

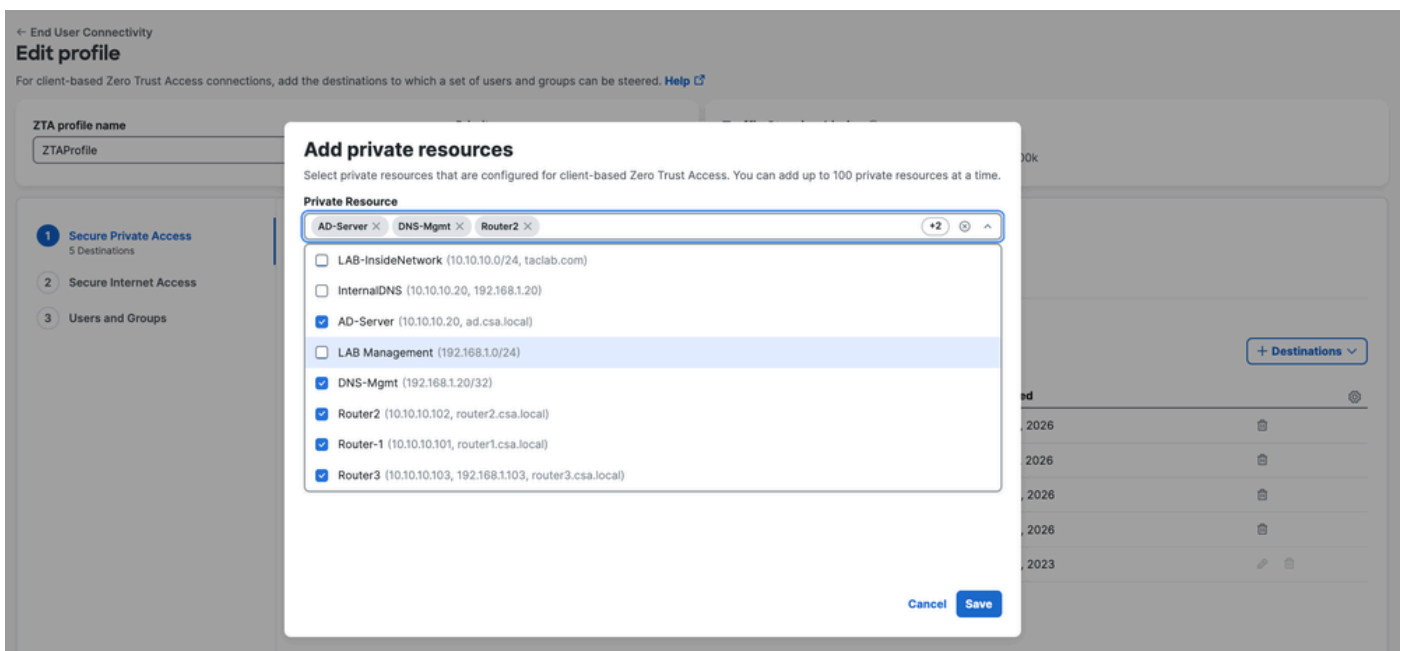


Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

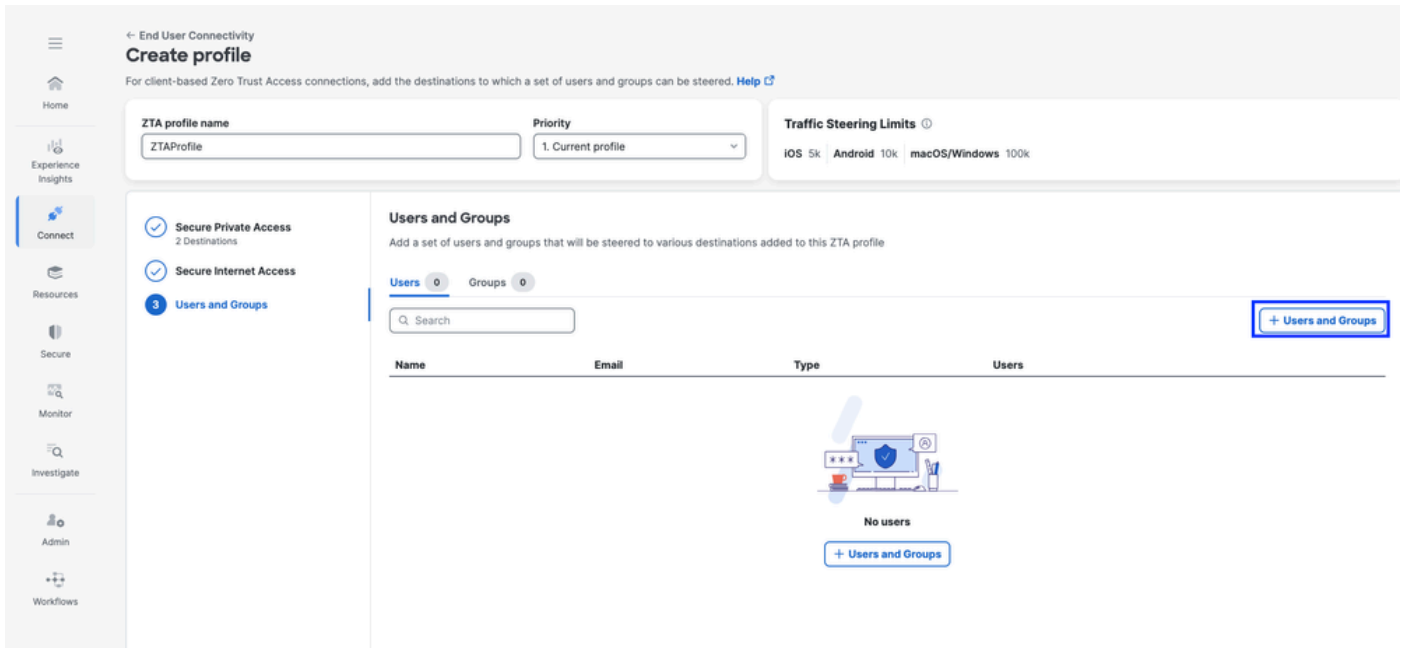


Acesso seguro - perfil ZTA

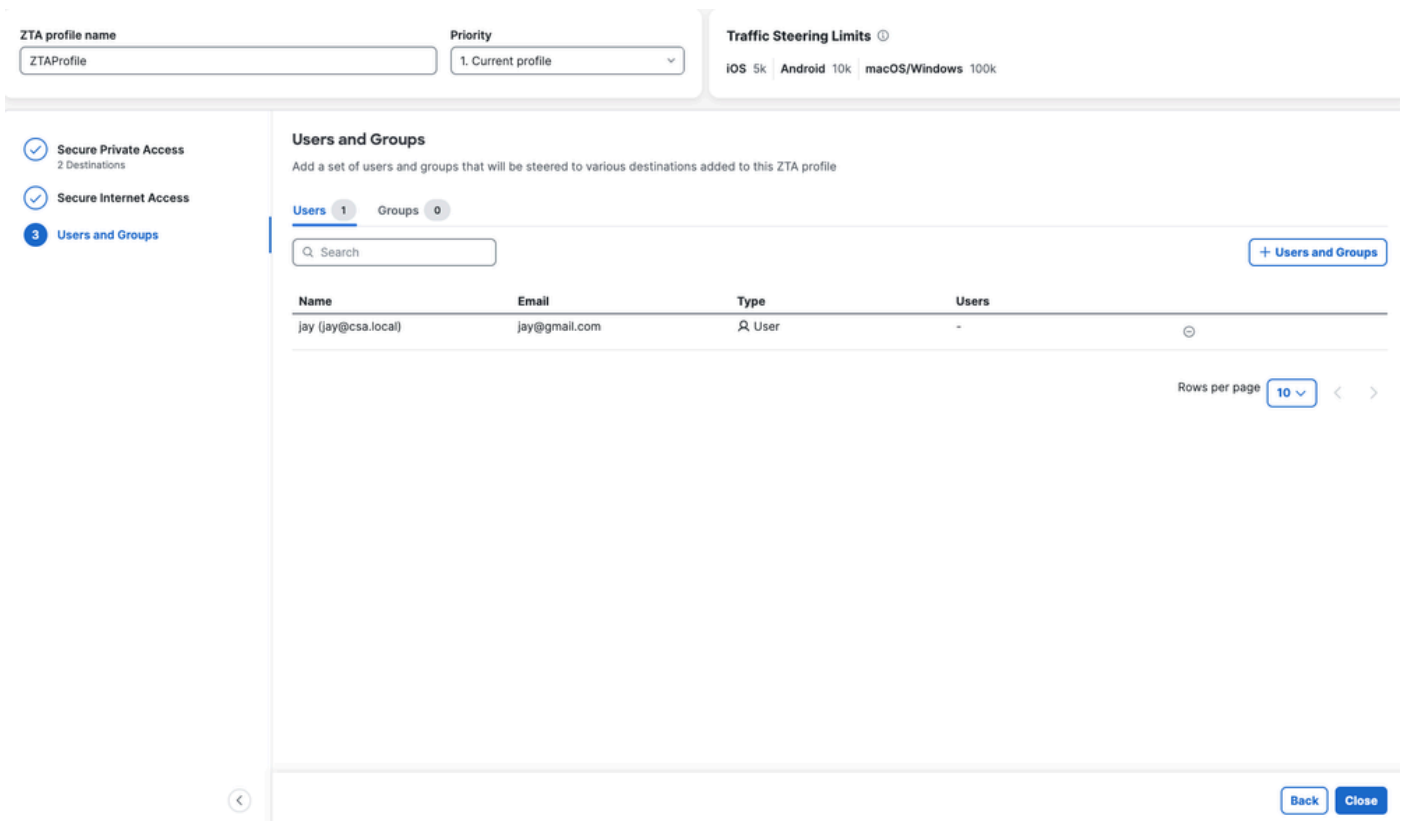


Acesso seguro - perfil ZTA

3. Adicionar usuários e grupos



Acesso seguro - perfil ZTA

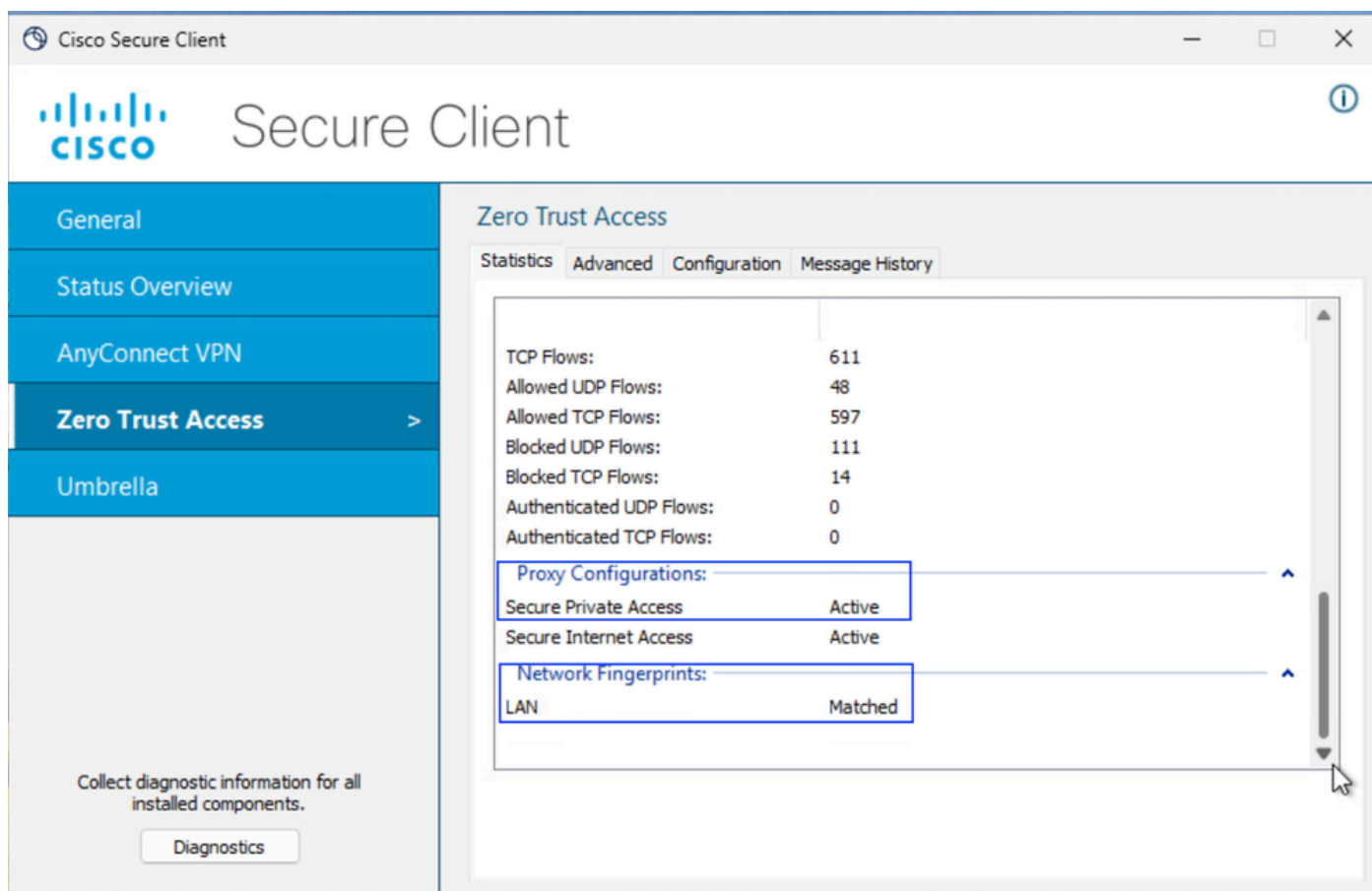


Acesso seguro - perfil ZTA

Etapa - 6 Verificar o acesso ao recurso privado

Quando o usuário for Local

1. Verifique a impressão digital de rede para ZTA TND; ela deve corresponder se o usuário é Local e o Acesso privado seguro deve estar Ativo



Acesso seguro - Teste de PR

2. Verifique se o usuário remoto pode resolver o FQDN do 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
```

Acesso seguro - Teste de PR

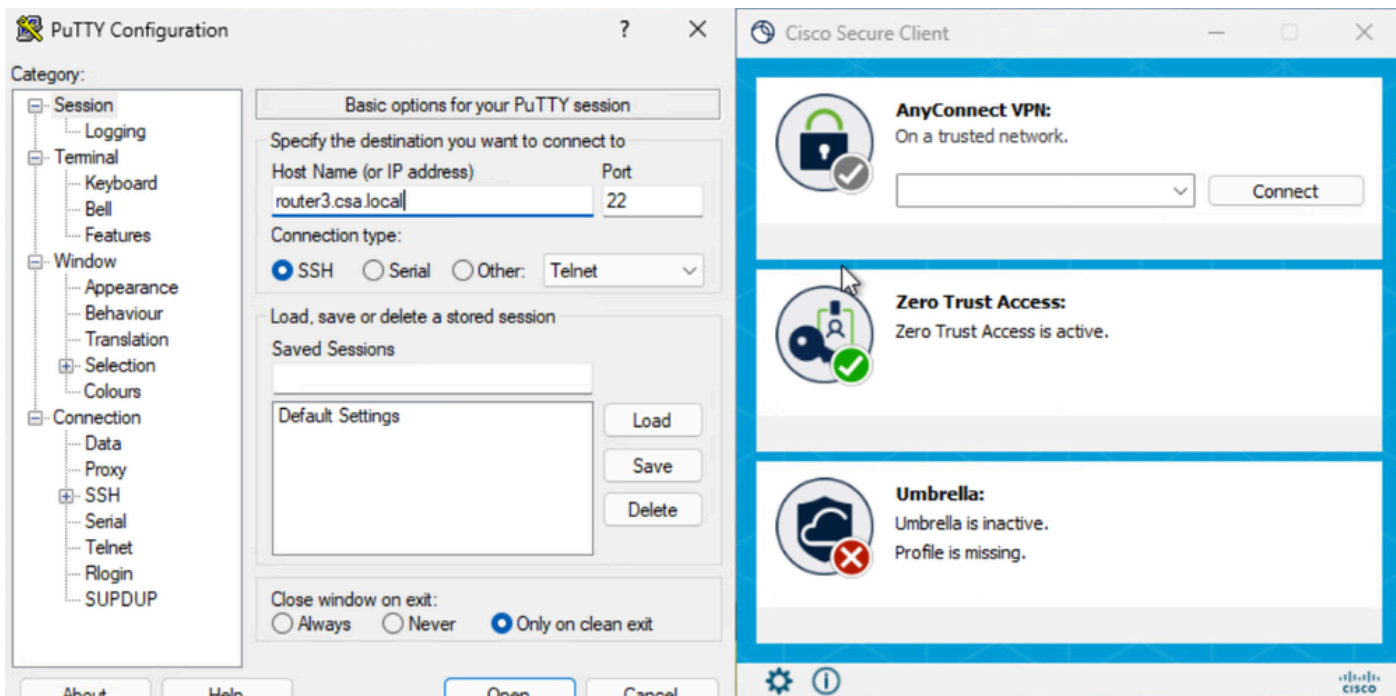
3. Verificar se o FTD pode acessar o recurso privado usando o FQDN

```
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# █
```

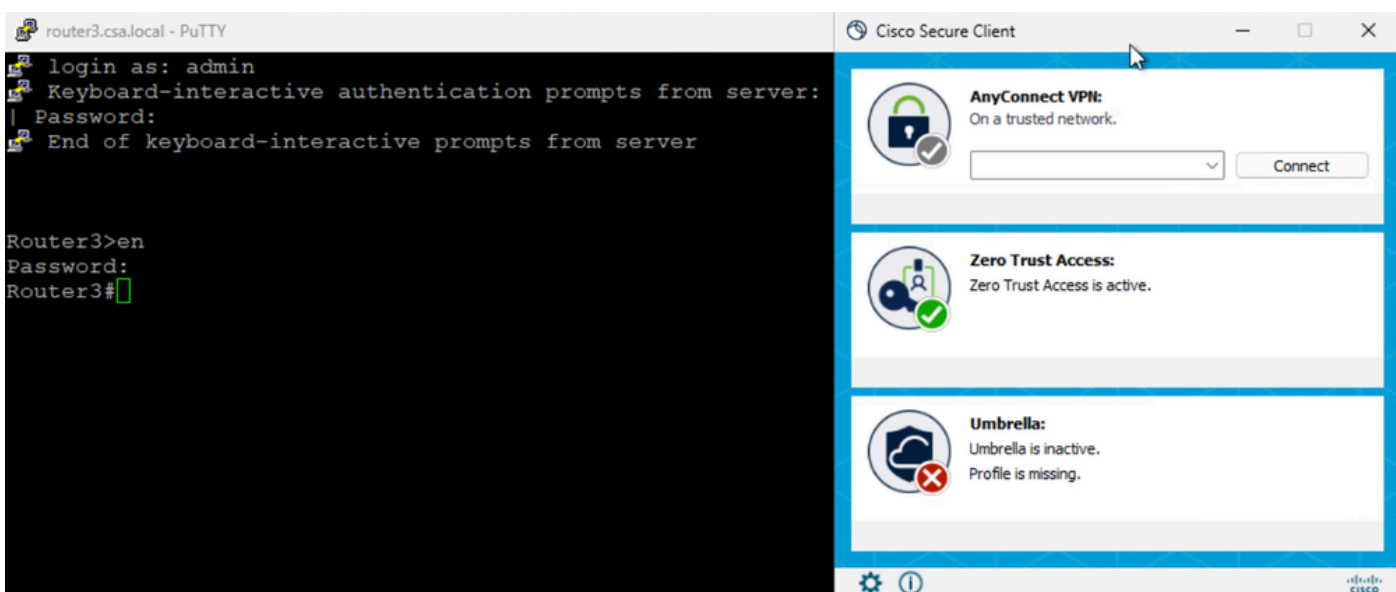
Acesso seguro - Teste de PR

4. Testar a conexão SSH com o recurso privado

Acessar a PR usando o FQDN

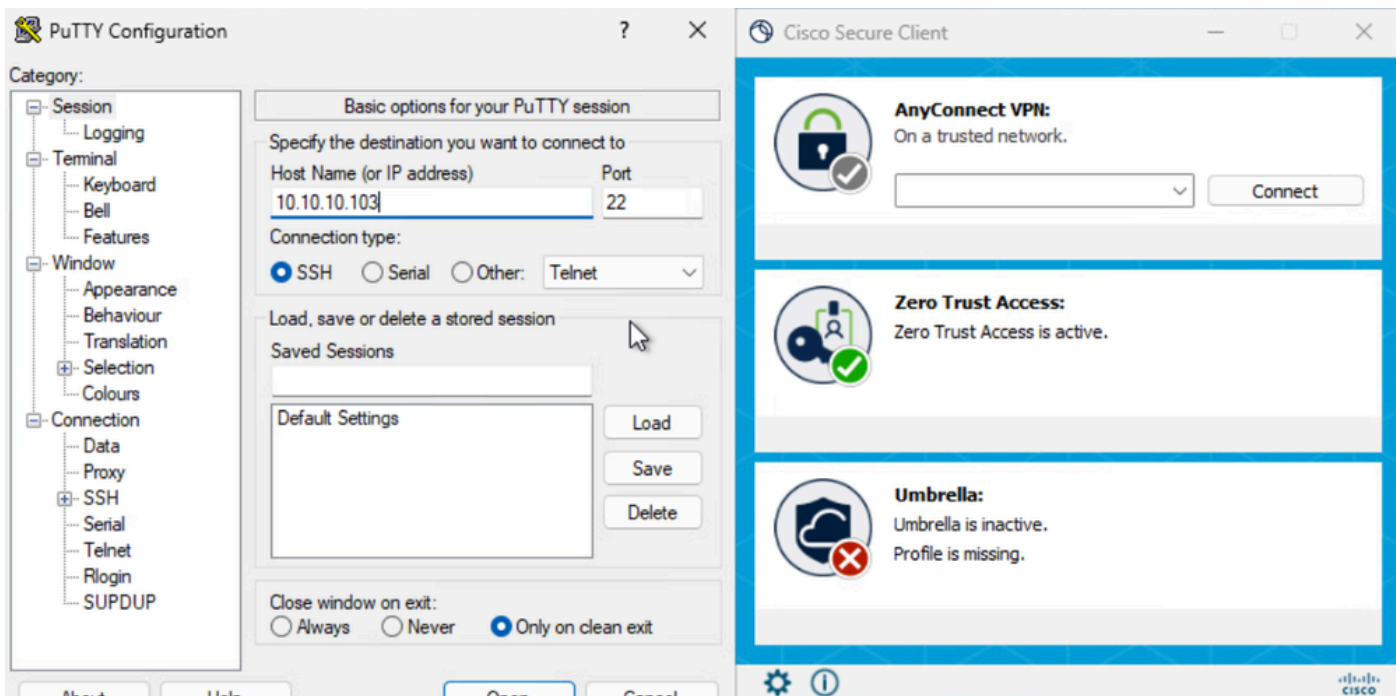


Acesso seguro - Teste de PR

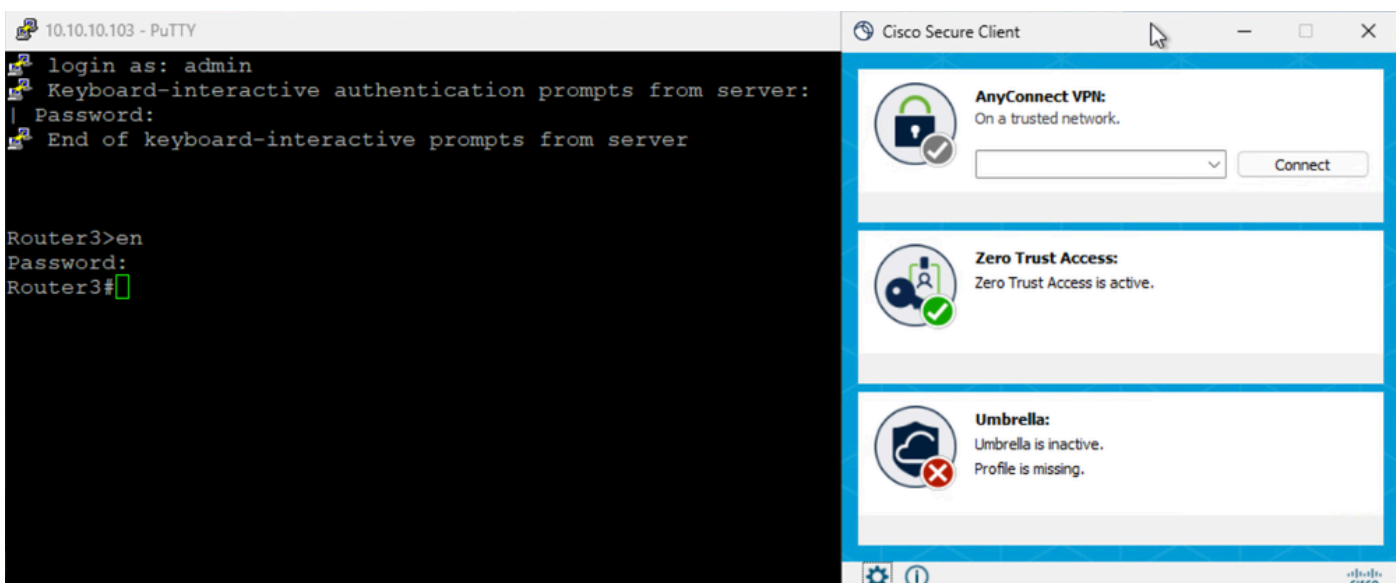


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP



Acesso seguro - Teste de PR

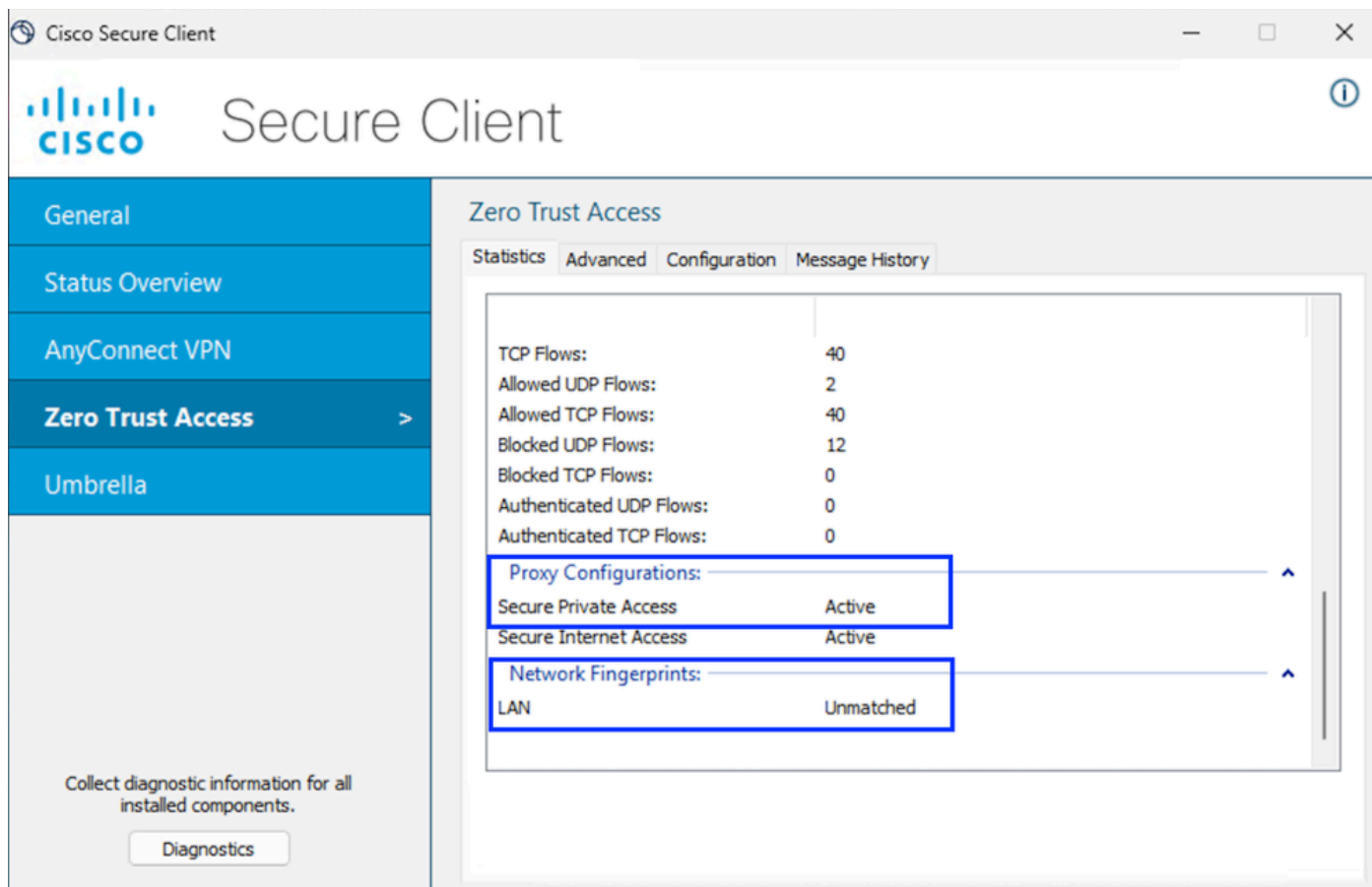


Acesso seguro - Teste de PR

5. Verificar logs de Pesquisa de Atividade de Acesso Seguro

Quando o usuário for Remoto

1. Verifique a impressão digital de rede para ZTA TND; ela não deve coincidir se o usuário for remoto



Acesso seguro - Teste de PR

2. Verifique se o usuário remoto pode resolver o FQDN do 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>

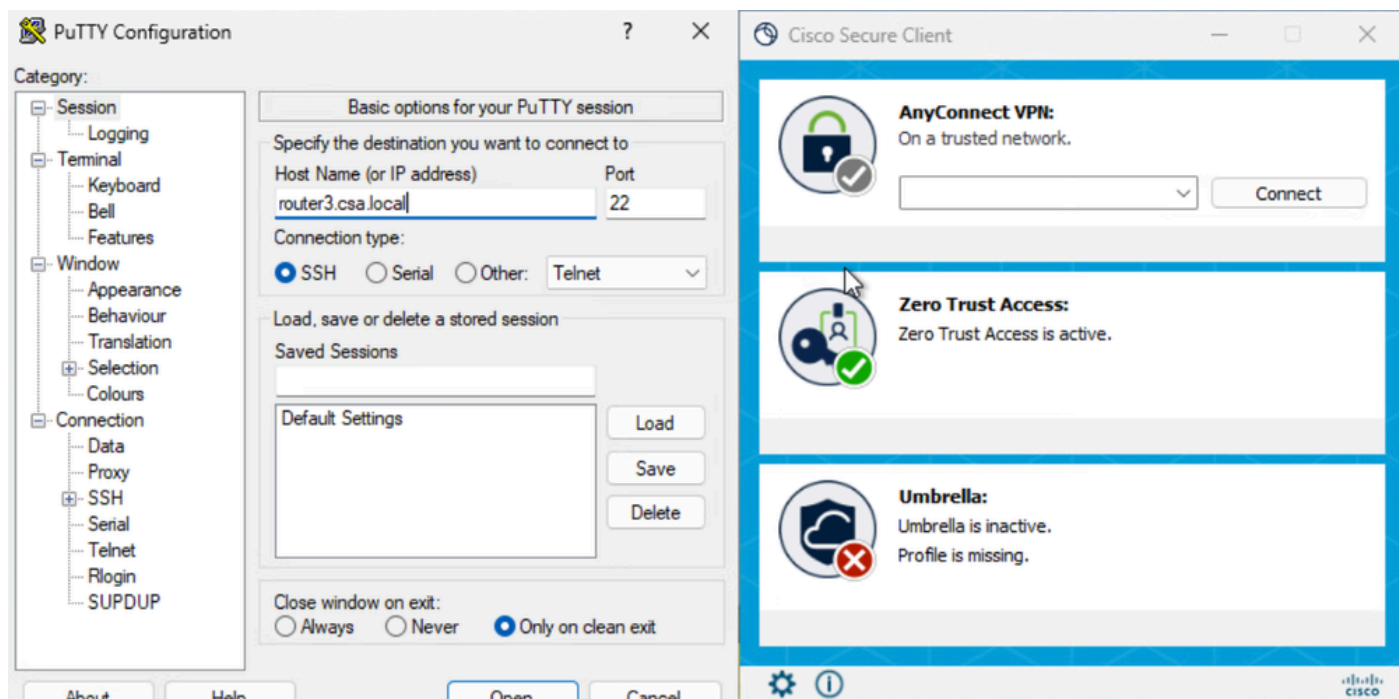
C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

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

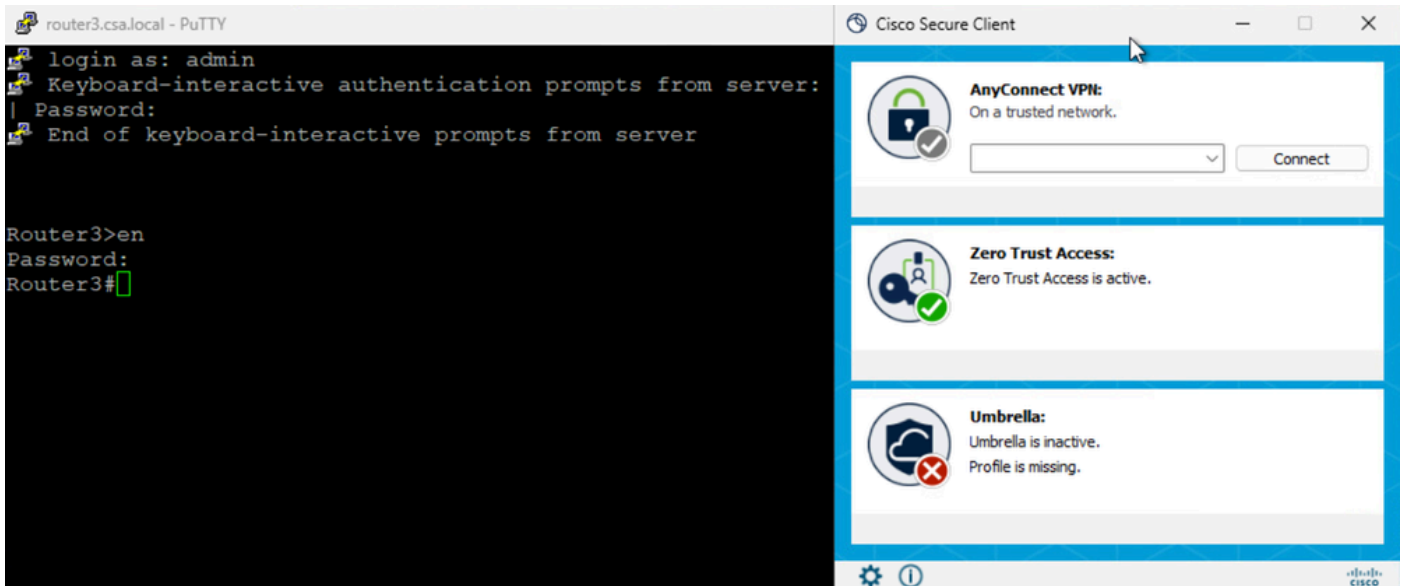
Acesso seguro - Teste de PR

3. Testar a conexão SSH com o recurso privado

Acessar a PR usando o FQDN

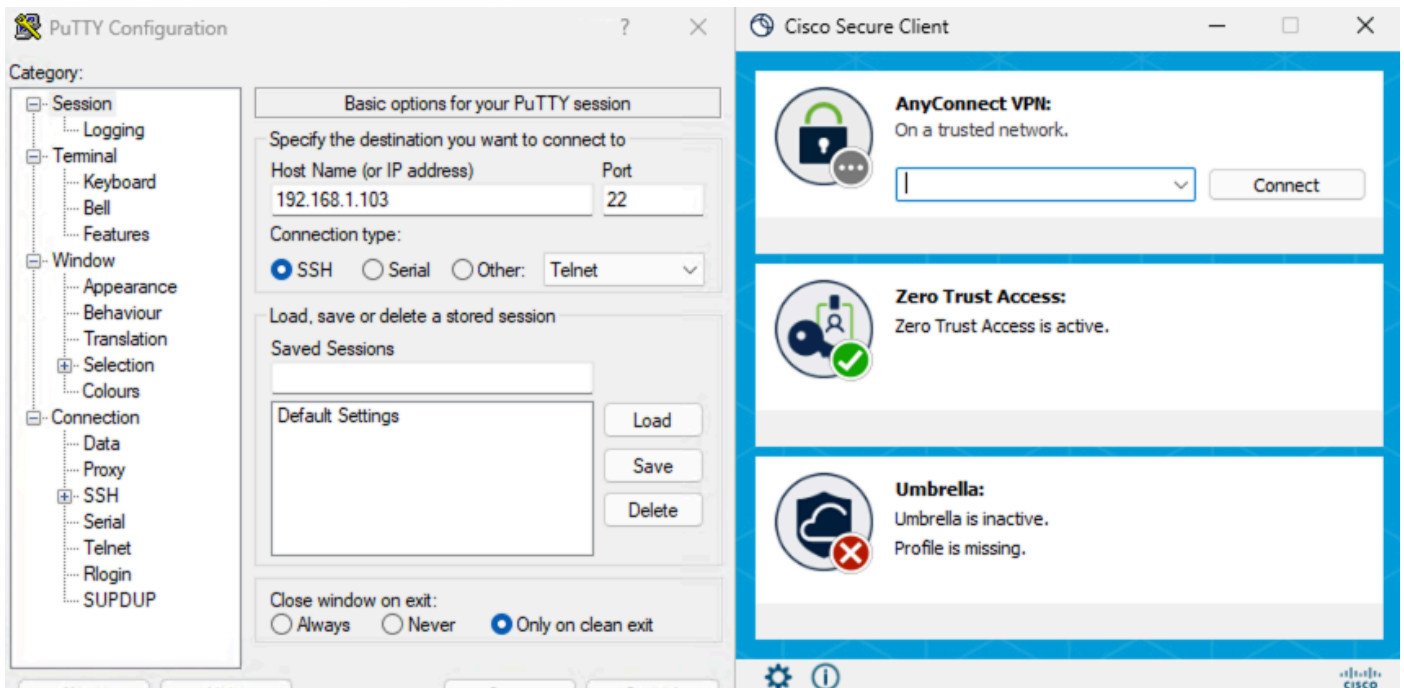


Acesso seguro - Teste de PR

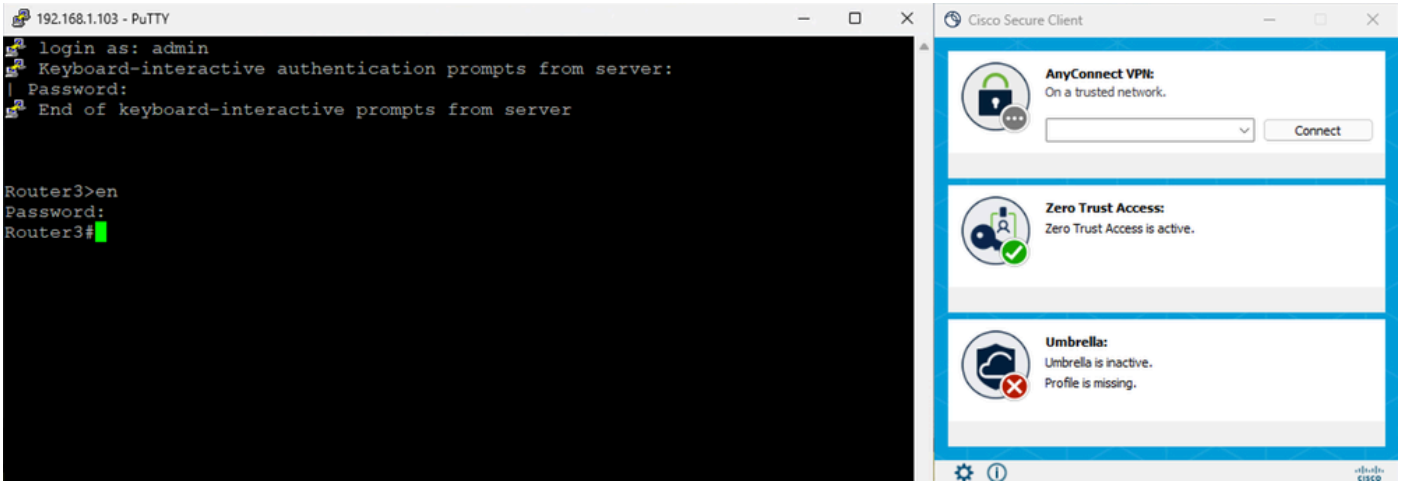


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP



Acesso seguro - Teste de PR



Acesso seguro - Teste de PR

5. Verificar logs de Pesquisa de Atividade de Acesso 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	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow

Acesso seguro - Pesquisa de atividades

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

Troubleshooting

Comandos úteis:

```
> 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
```

! e, em seguida, vá para o modo de especialista

```
# tail -f /ngfw/var/log/messages
```

```
# show conn all
```

```
# show nat detail
```

```
# show asp table socket
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.