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

Contents

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 Diretory
- 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

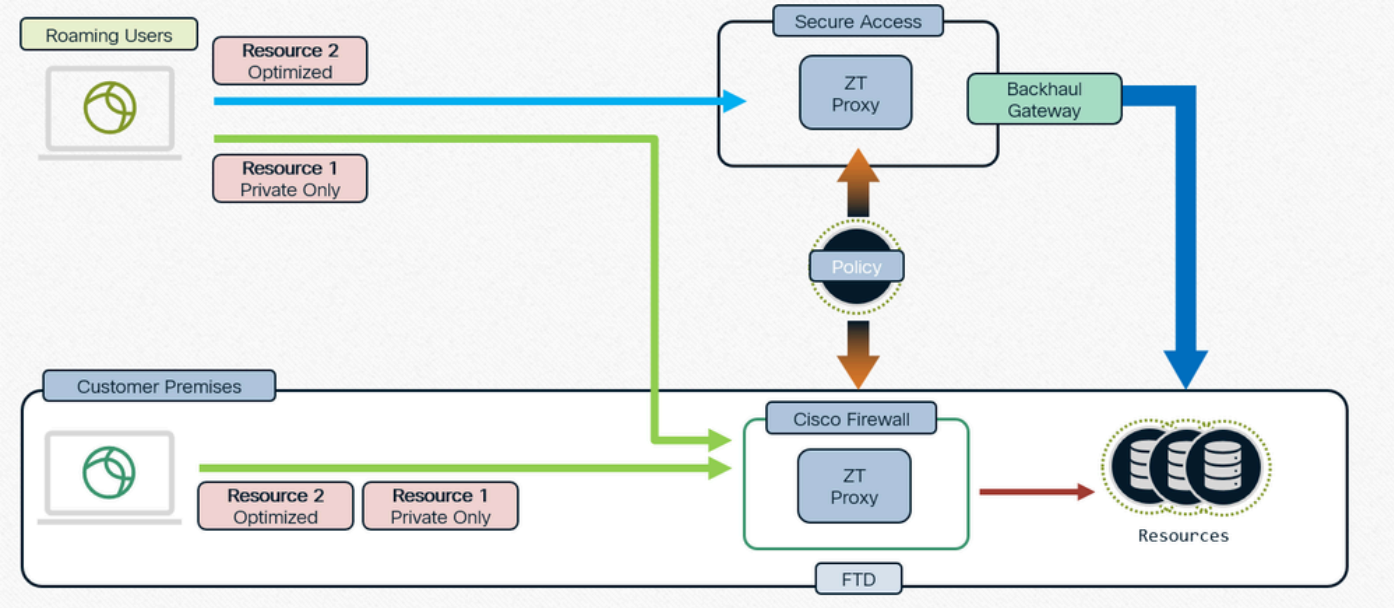
O acesso universal à rede de confiança zero (ZTNA) permite que os administradores permitam especificamente o acesso aos recursos da rede interna de acordo com a identidade do usuário

(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.

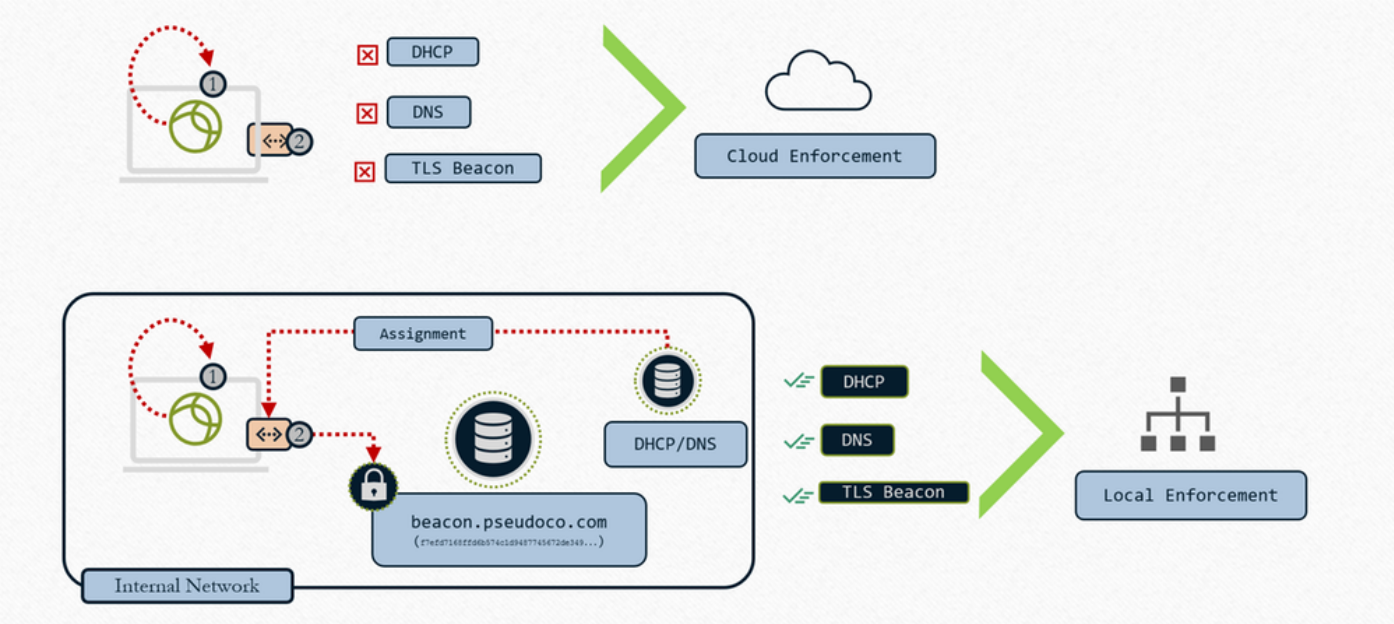
O proxy de tráfego, bem como a aplicação de políticas de IPS, arquivos e malware, é executado no Firepower Threat Defense (FTD).



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

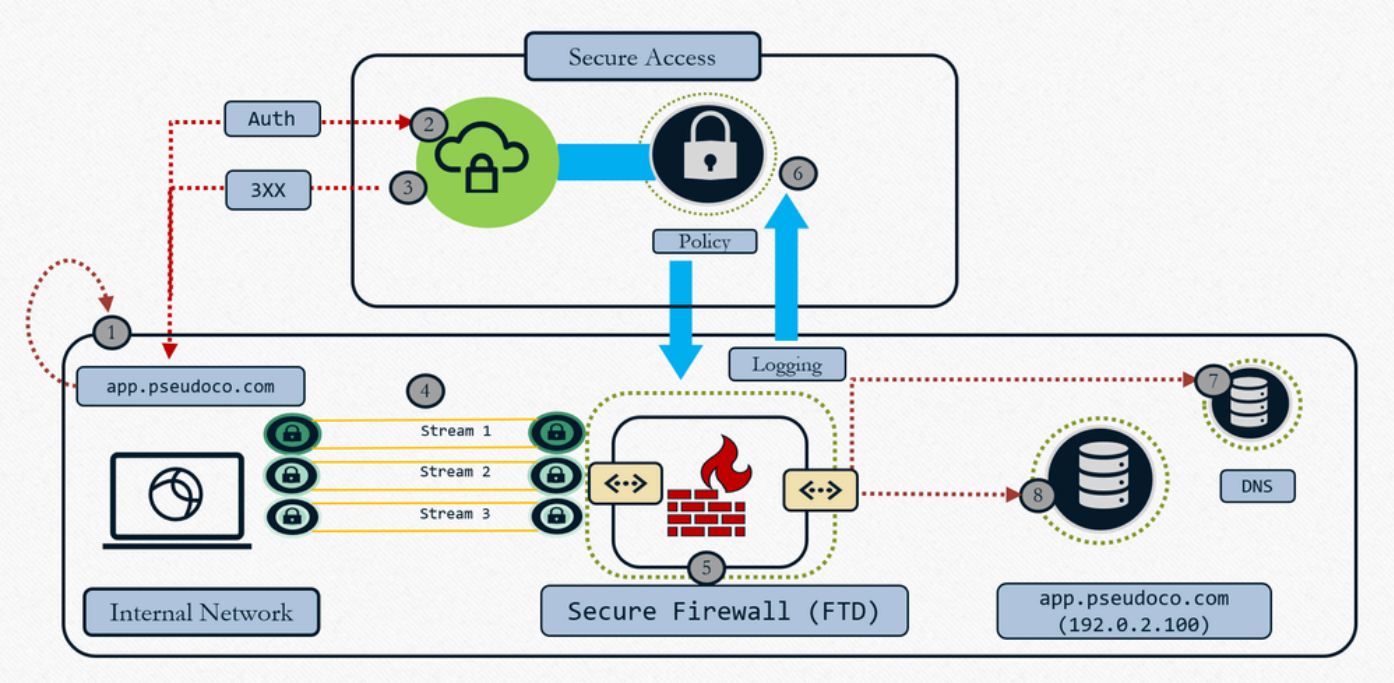
3- Se a condição corresponder - Aplicação Local

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

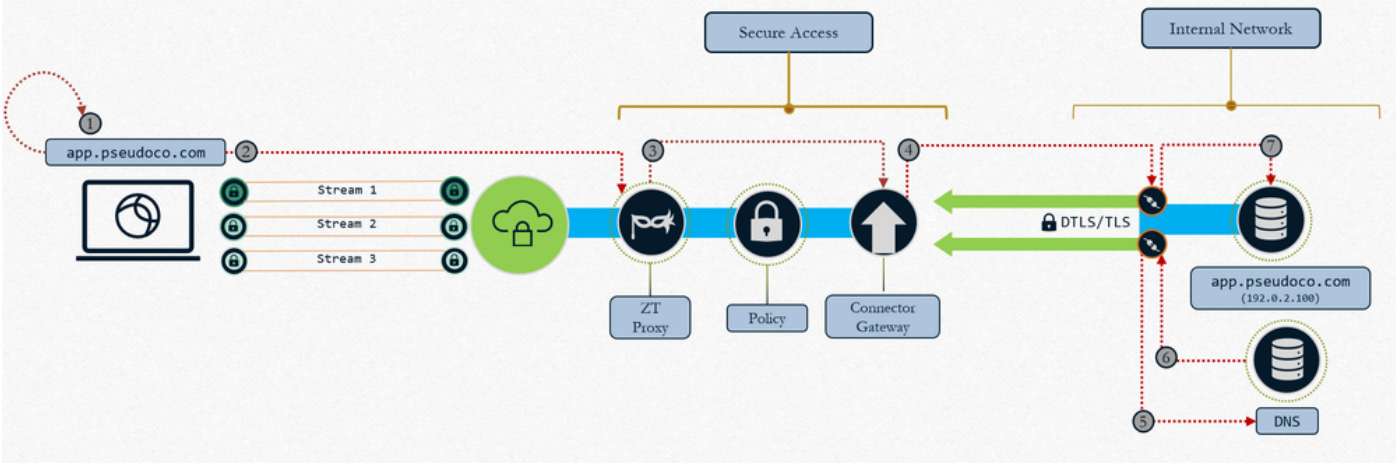
- Caminho de Imposição Local: Aplicação de firewall



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

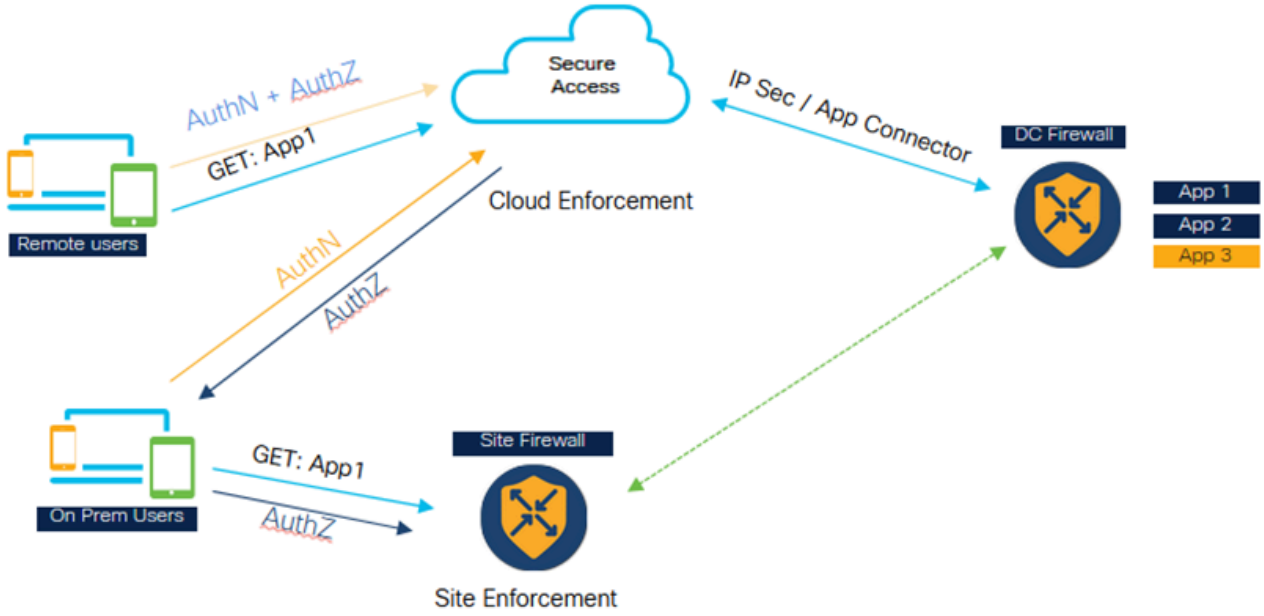


ZTNA universal: Aplicação da nuvem

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

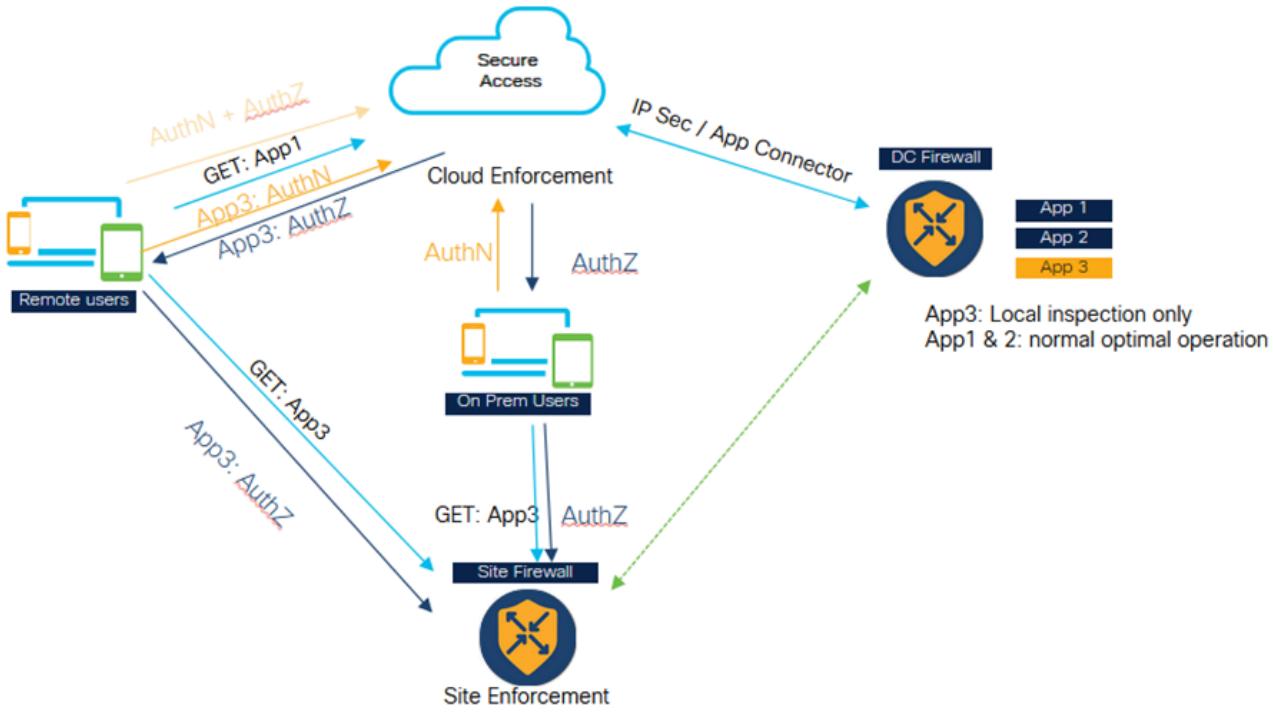
Caso 1: ZTNA consistente e otimizada para usuários no local



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

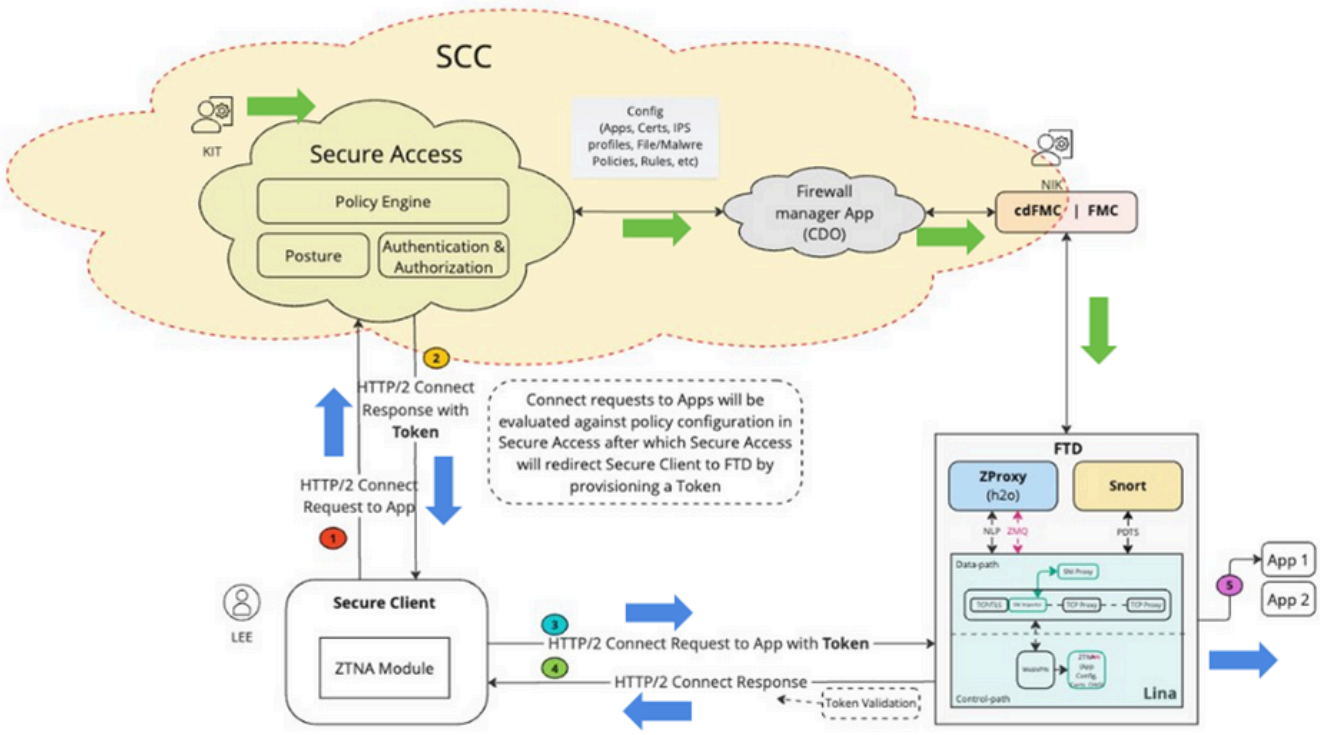
Caso 2: Inspeção Privada para Aplicações Sensíveis



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

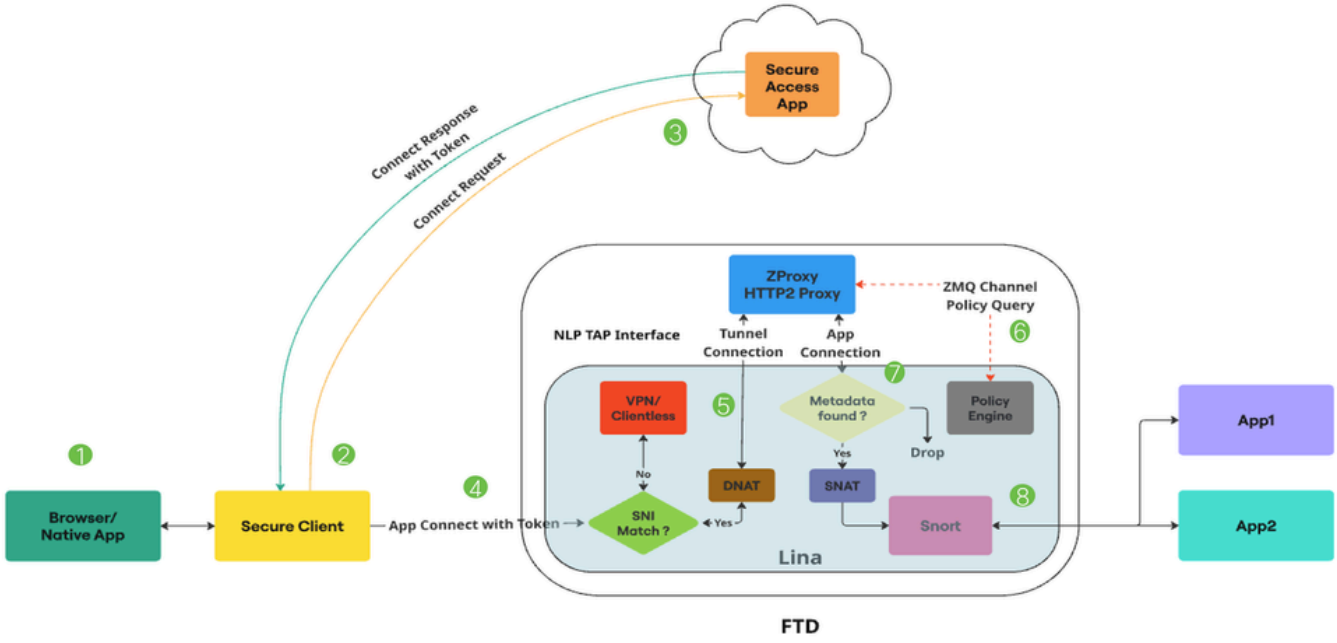
3. O Secure Access redireciona o cliente Secure para o FTD junto com o token de autenticação.

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

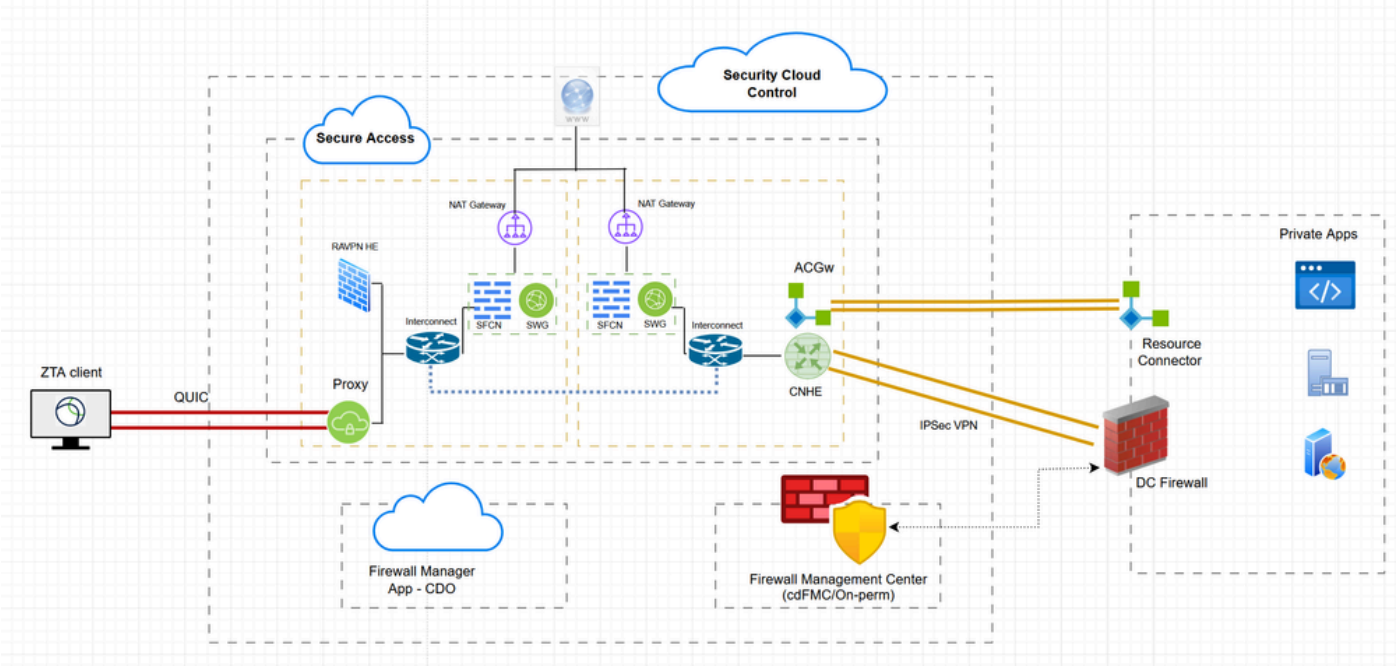
(exemplo:169.251.1.2) como IP de Origem. Isso será traduzido para o IP da interface de saída do FTD, antes de enviá-lo. Em seguida, Lina marca os fluxos de Confiança Zero Universal para inspeção do Snort somente se uma política de Arquivo ou IPS estiver presente no token de acesso.A ID da Regra obtida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

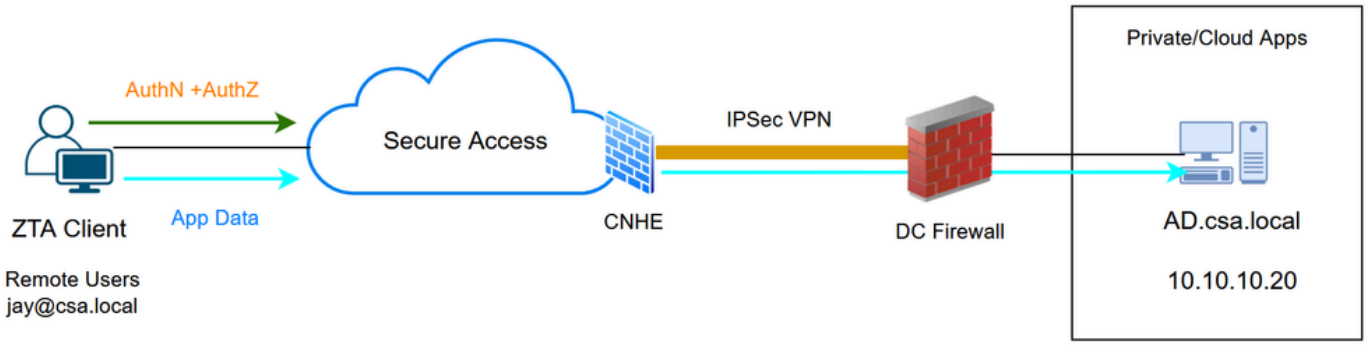


ZTNA híbrido - Diagrama de rede

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

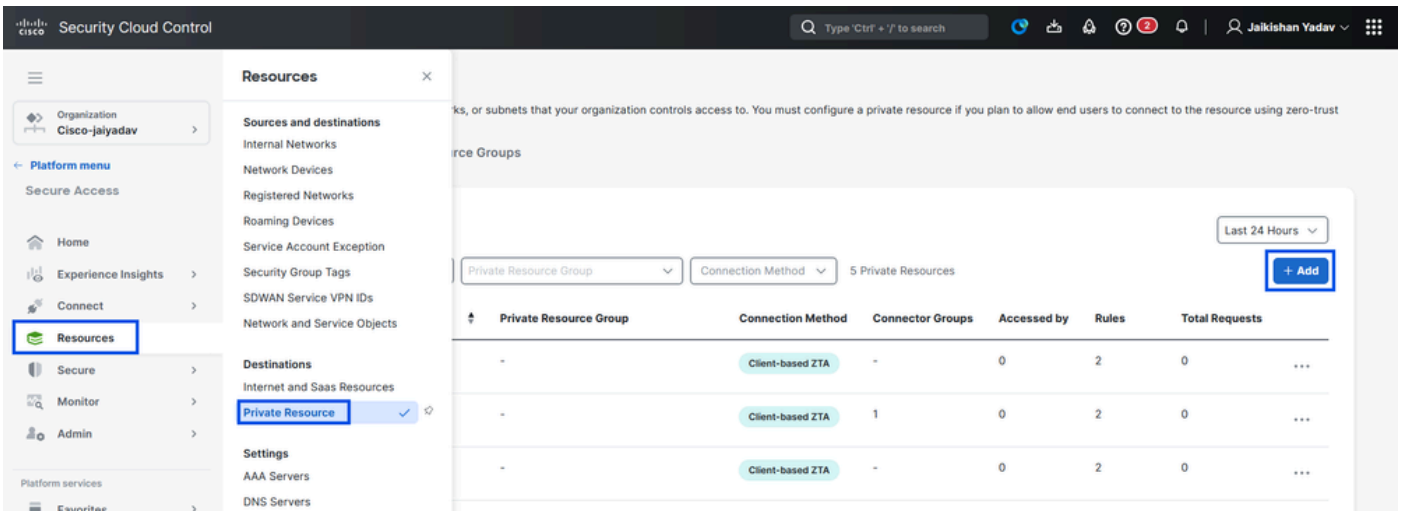


ZTA universal - Topologia de caso de teste

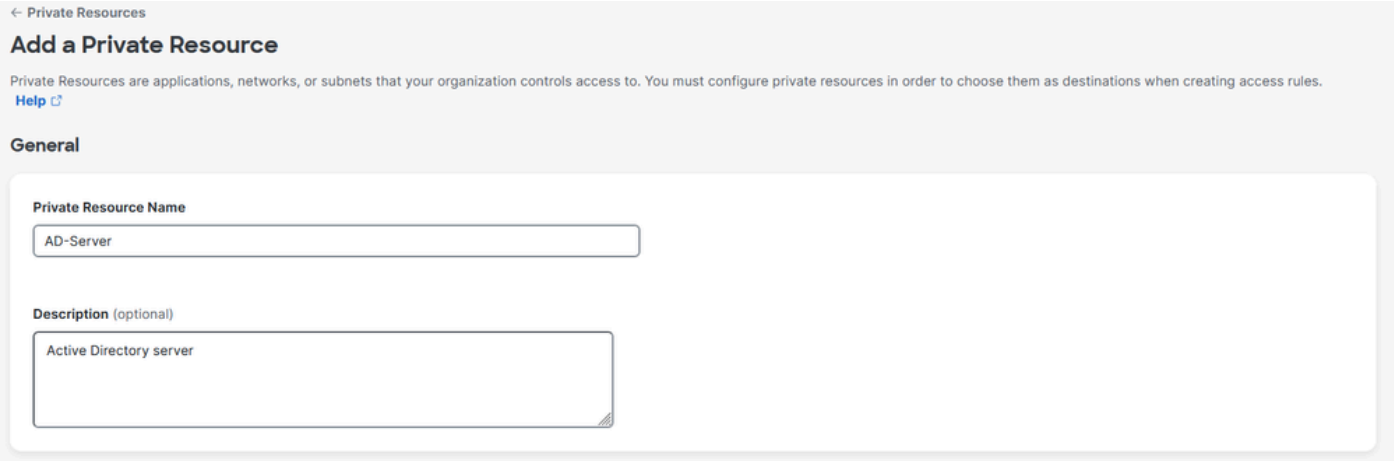
Etapa 1 - Definir um recurso privado no acesso seguro

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

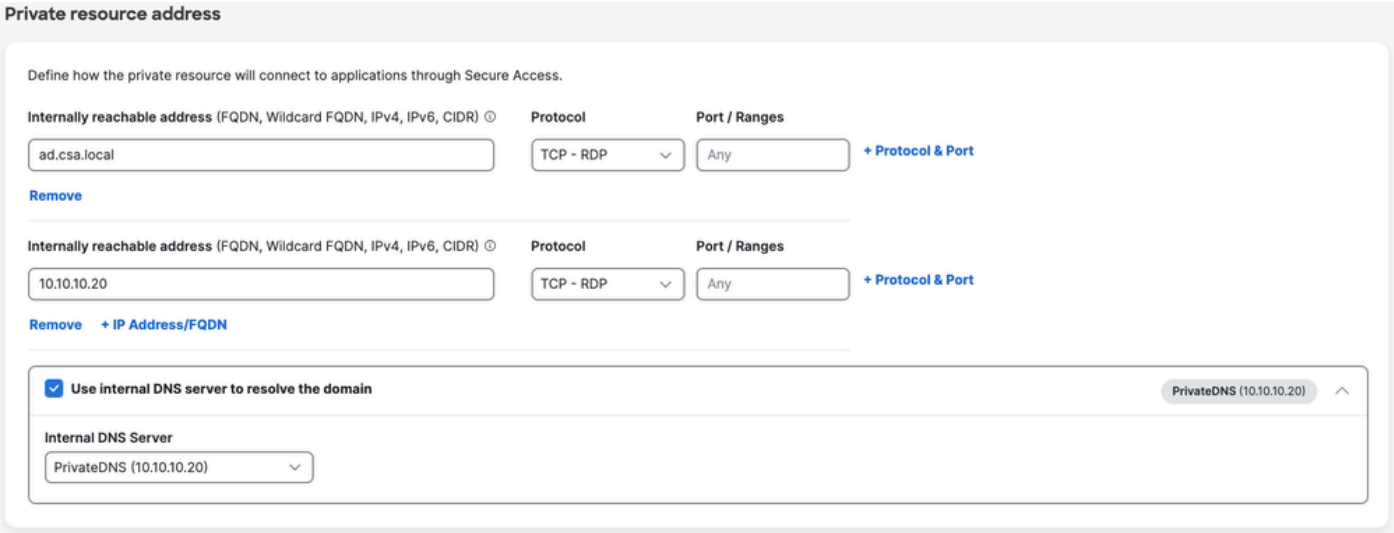


2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do recurso.

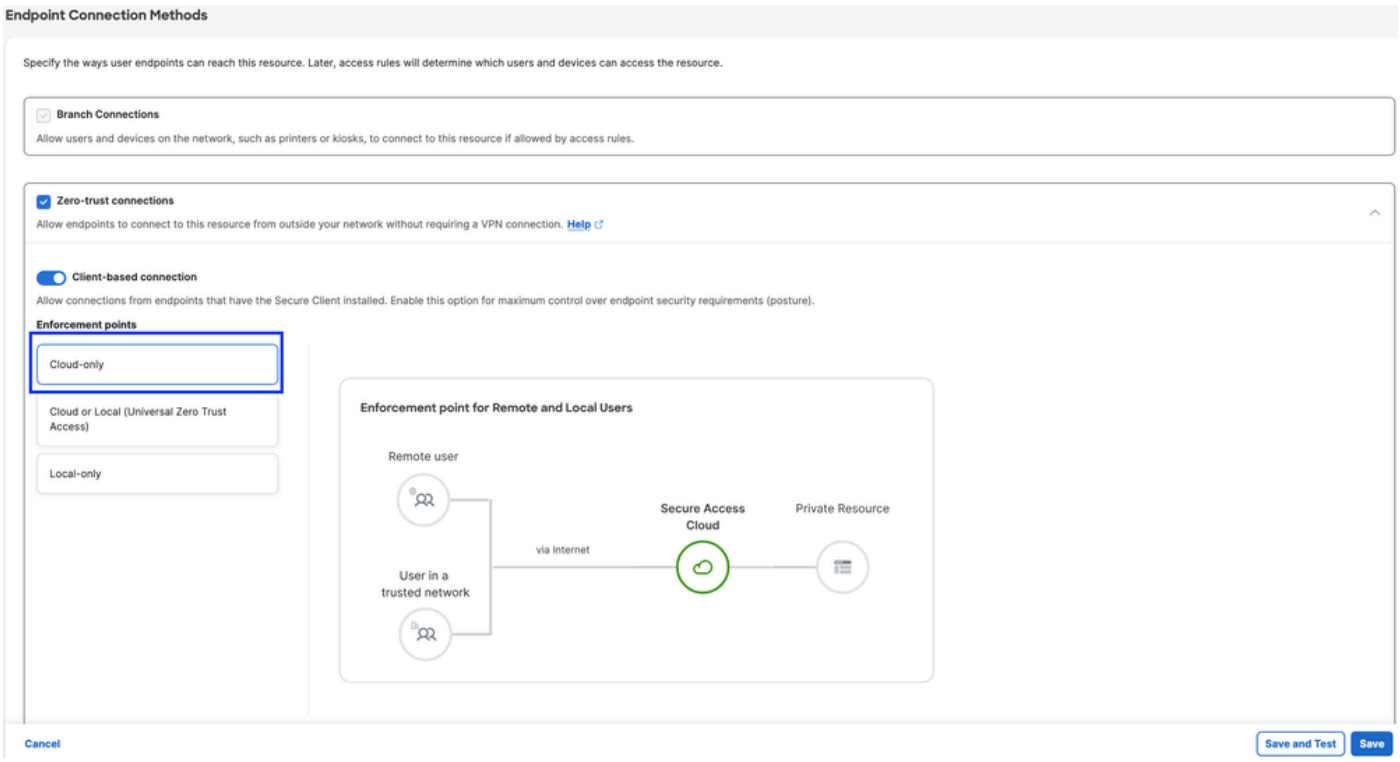


3. Informe o FQDN do recurso privado que deseja acessar. Também podemos definir o endereço IP do recurso privado . Para obter mais informações, consulte Adicionar um recurso privado

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



5. Selecionar Métodos de Conexão de Ponto de Extremidade



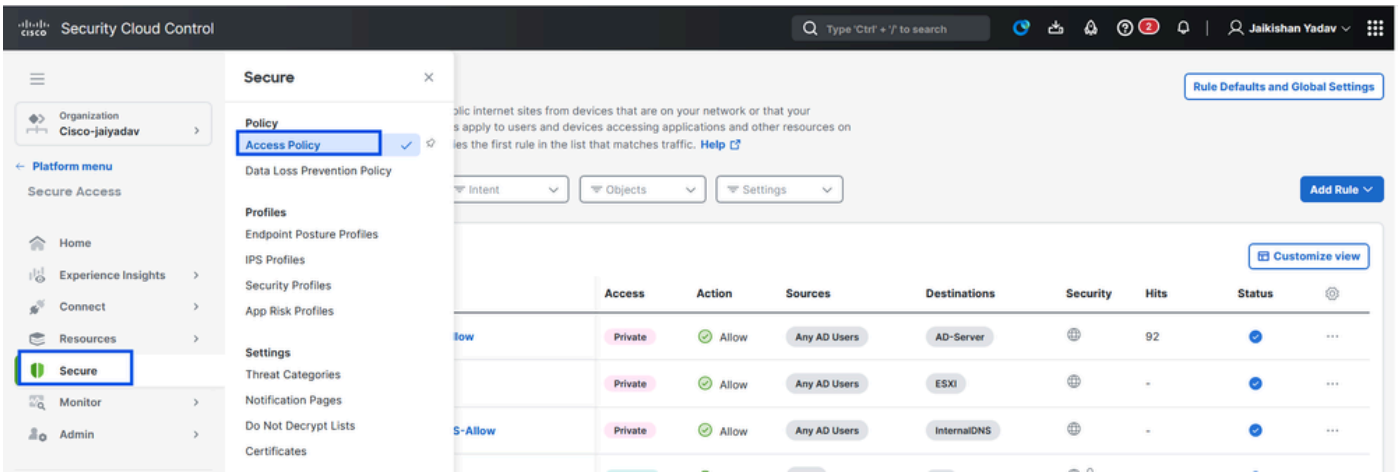
Acesso seguro - Configuração de recursos privados

6. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

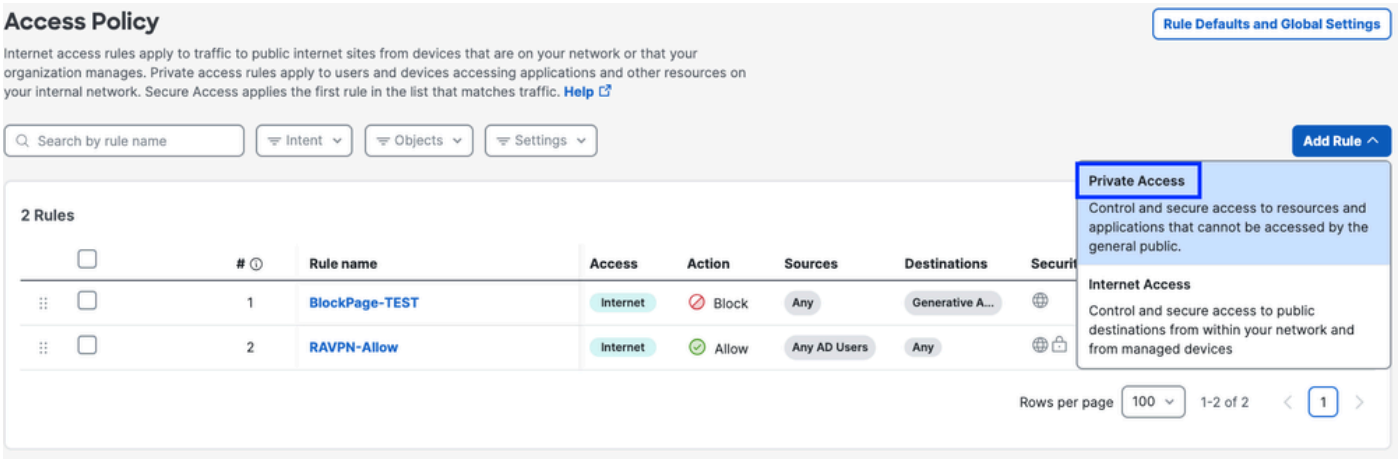
Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA . Para obter mais informações, consulte Regra de acesso privado

1. Navegue até Proteger > Política de acesso



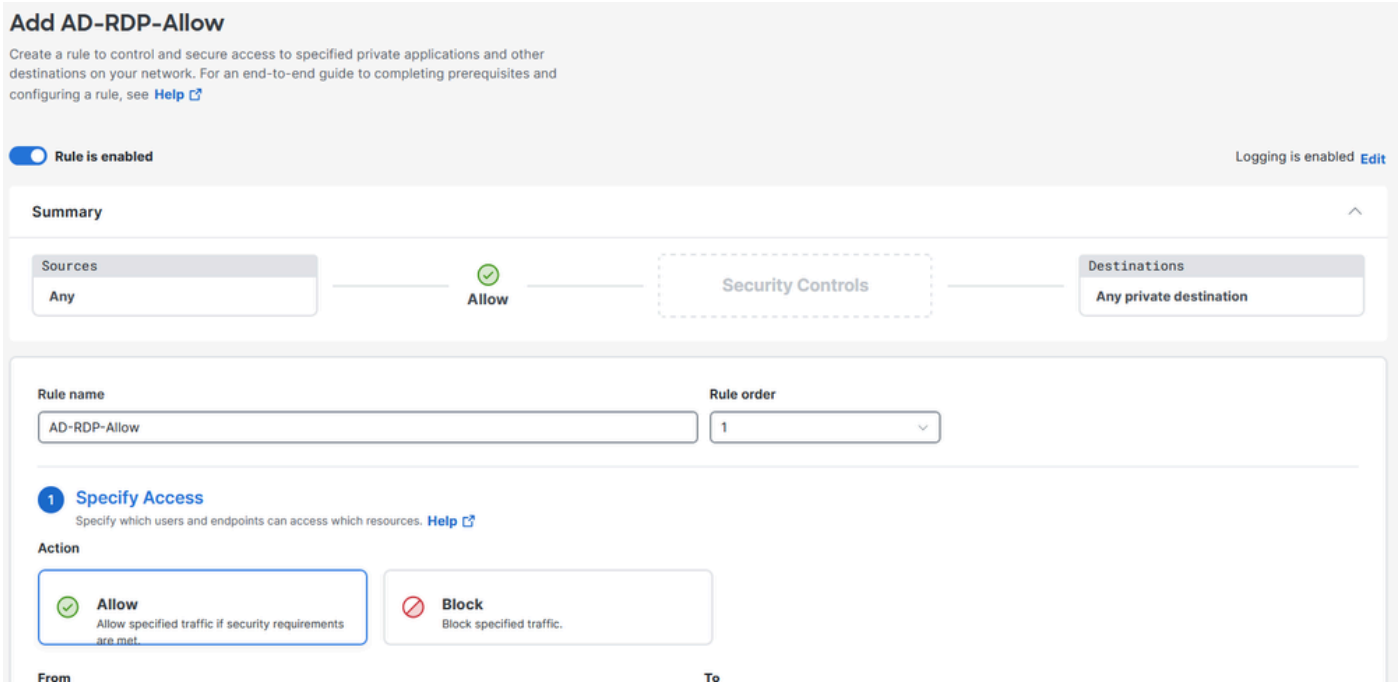
Acesso seguro - Configuração da política de acesso

2. Clique em Adicionar Regra e escolha Acesso Particular.
   Na parte superior da regra há um resumo que descreve os componentes configurados da regra.



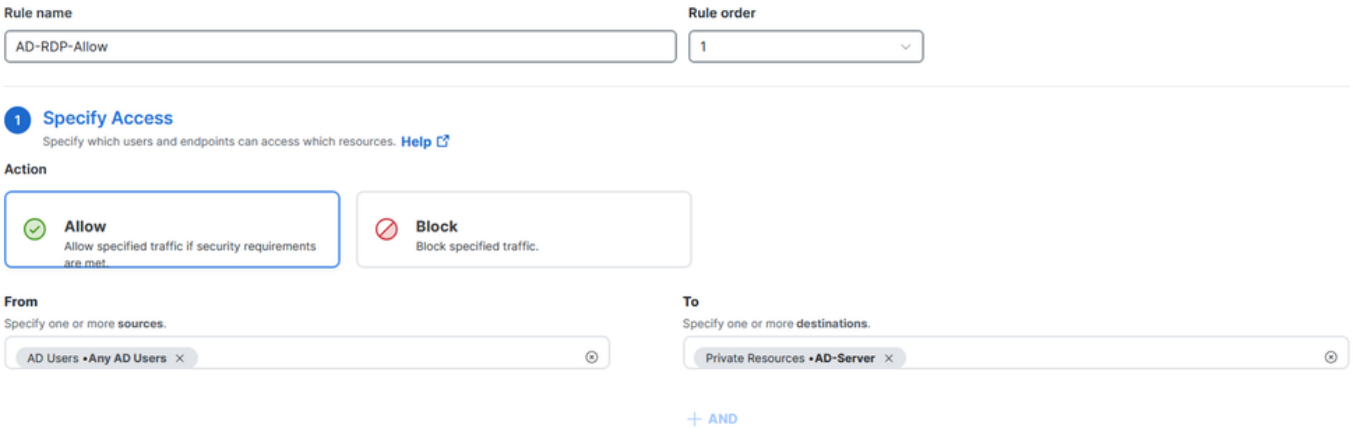
Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra



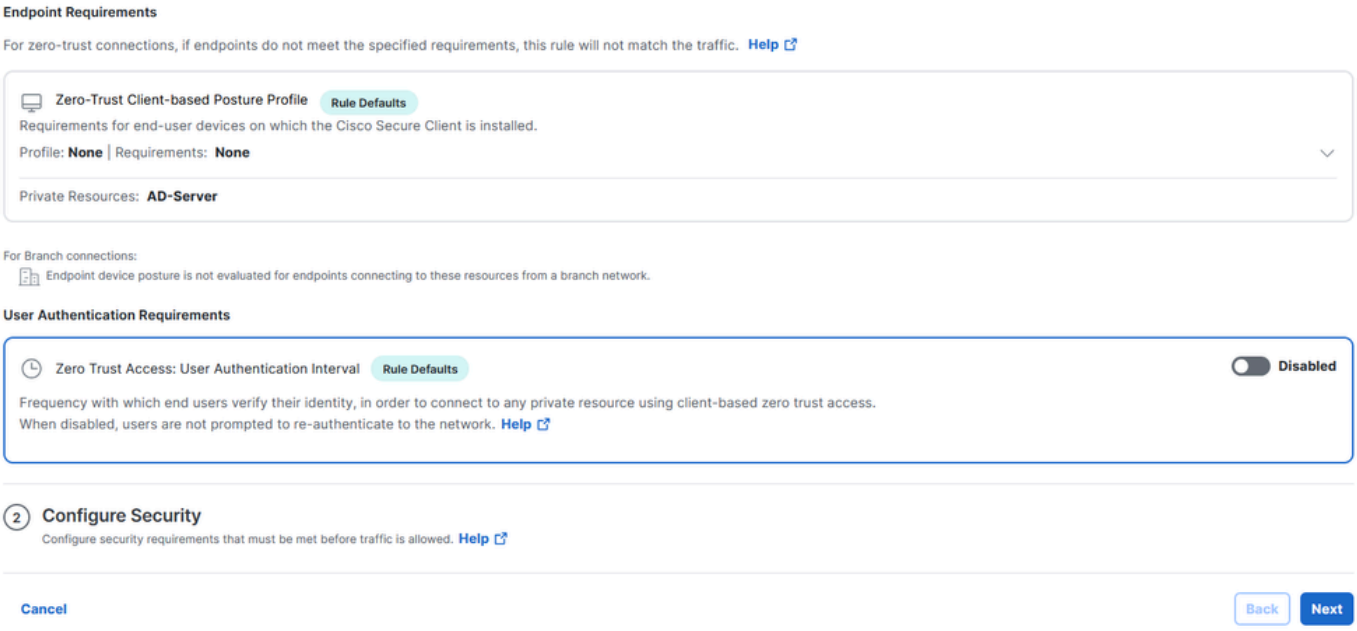
Acesso seguro - Configuração da política de acesso

4. Selecione a ação da regra e selecione origem e destino



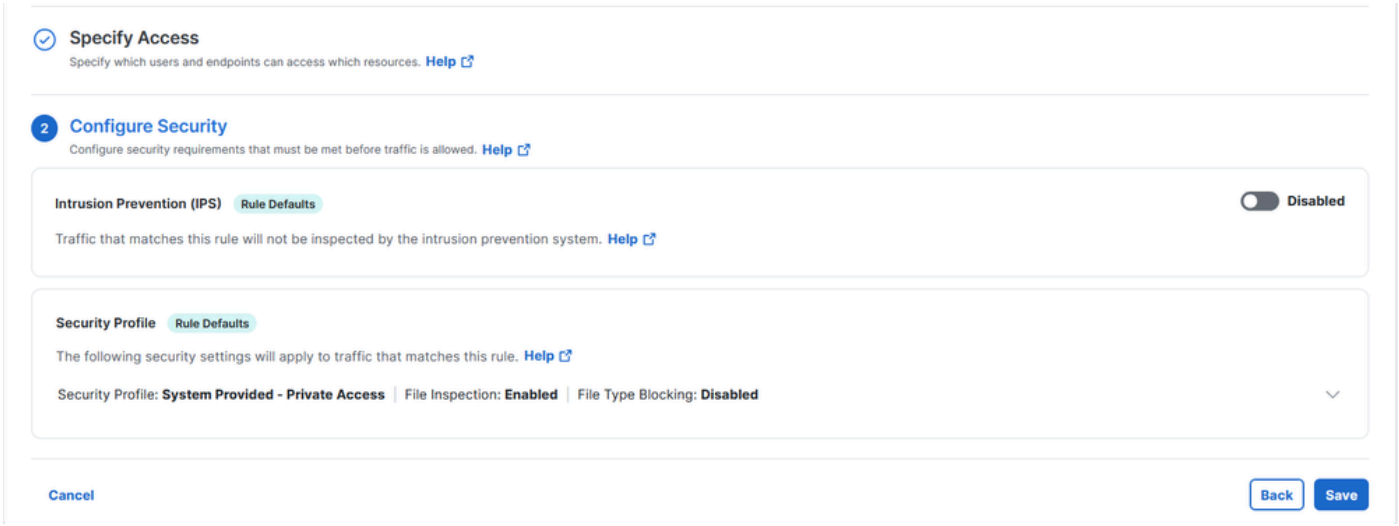
Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint



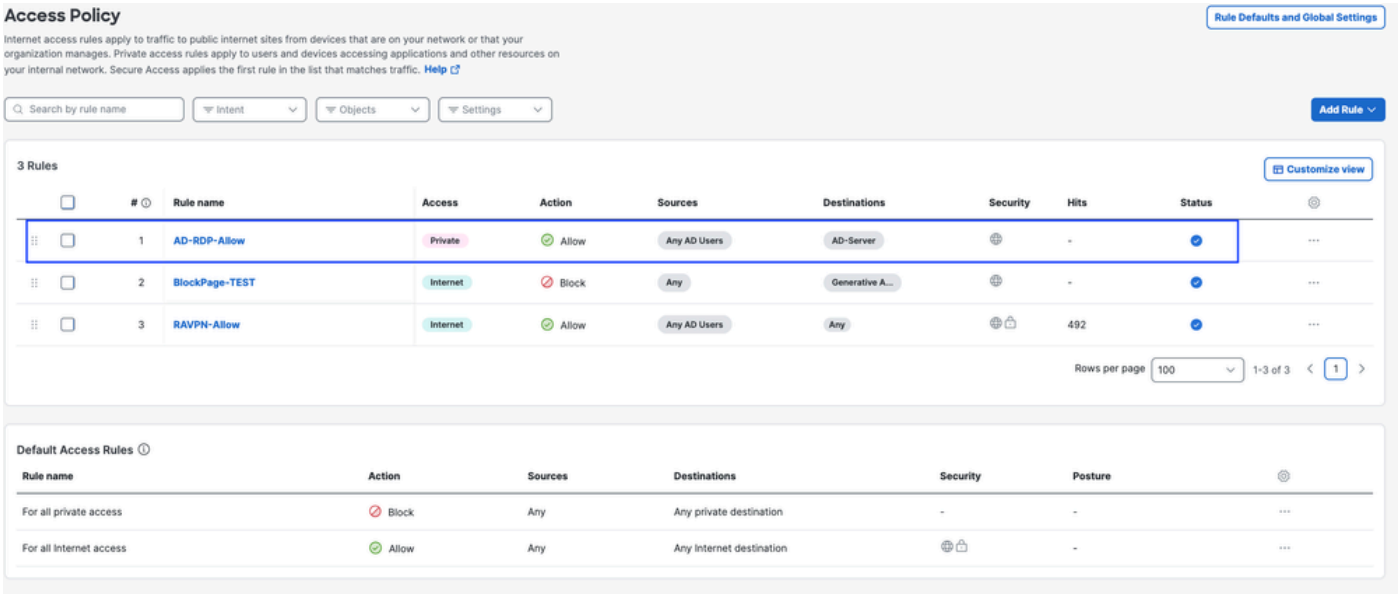
Acesso seguro - Configuração da política de acesso

6. Configurar segurança



Acesso seguro - Configuração da política de acesso

7. Clique em Salvar

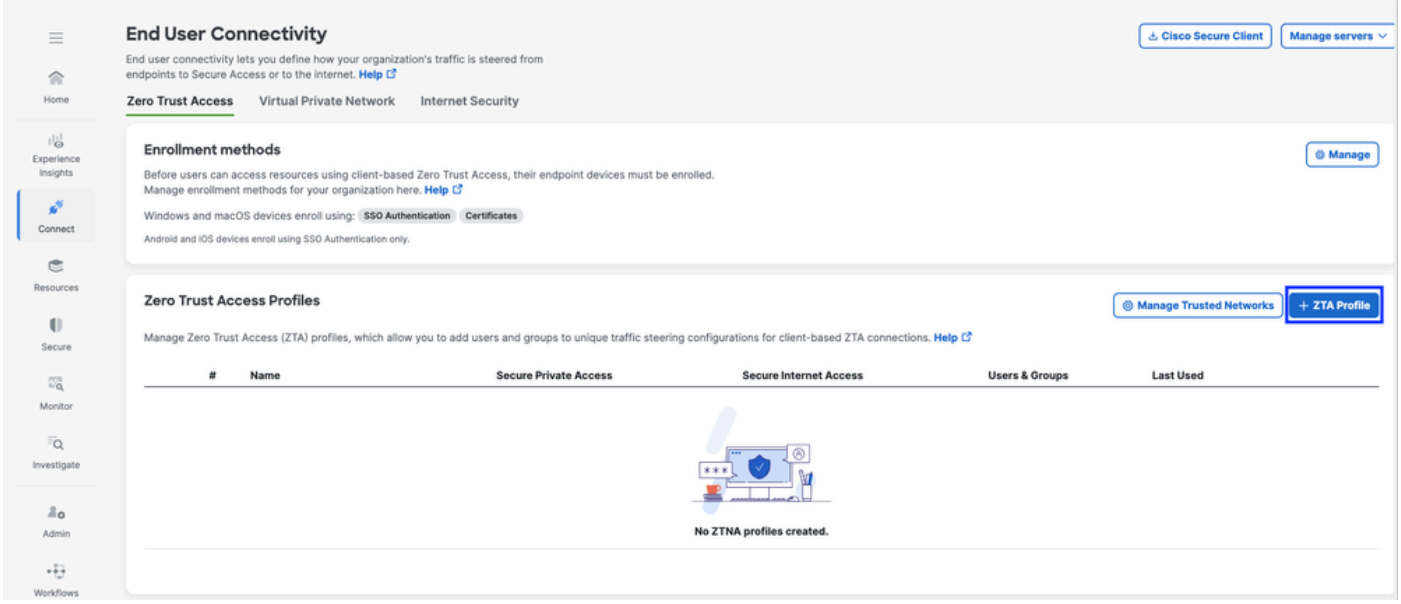


Acesso seguro - Configuração da política de acesso

Etapa - 3 Adicionar recurso privado ao perfil ZTA

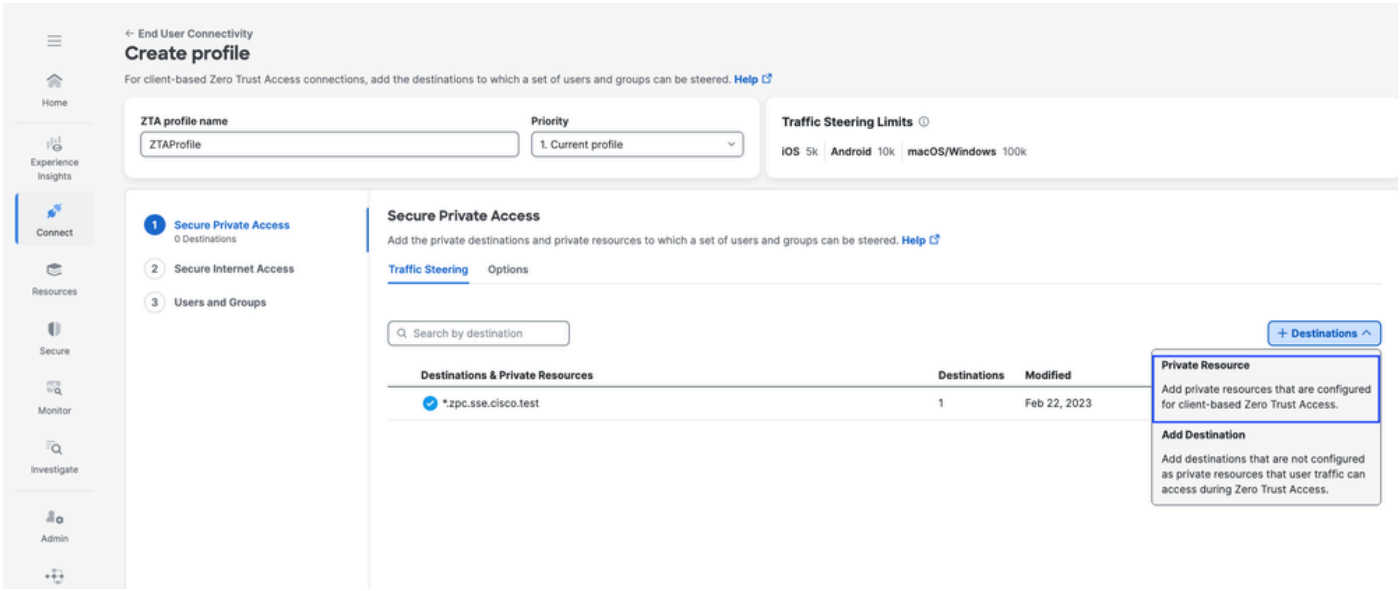
Se estiver usando um perfil ZTA personalizado, você precisará adicionar o respectivo recurso privado ao perfil ZTA

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

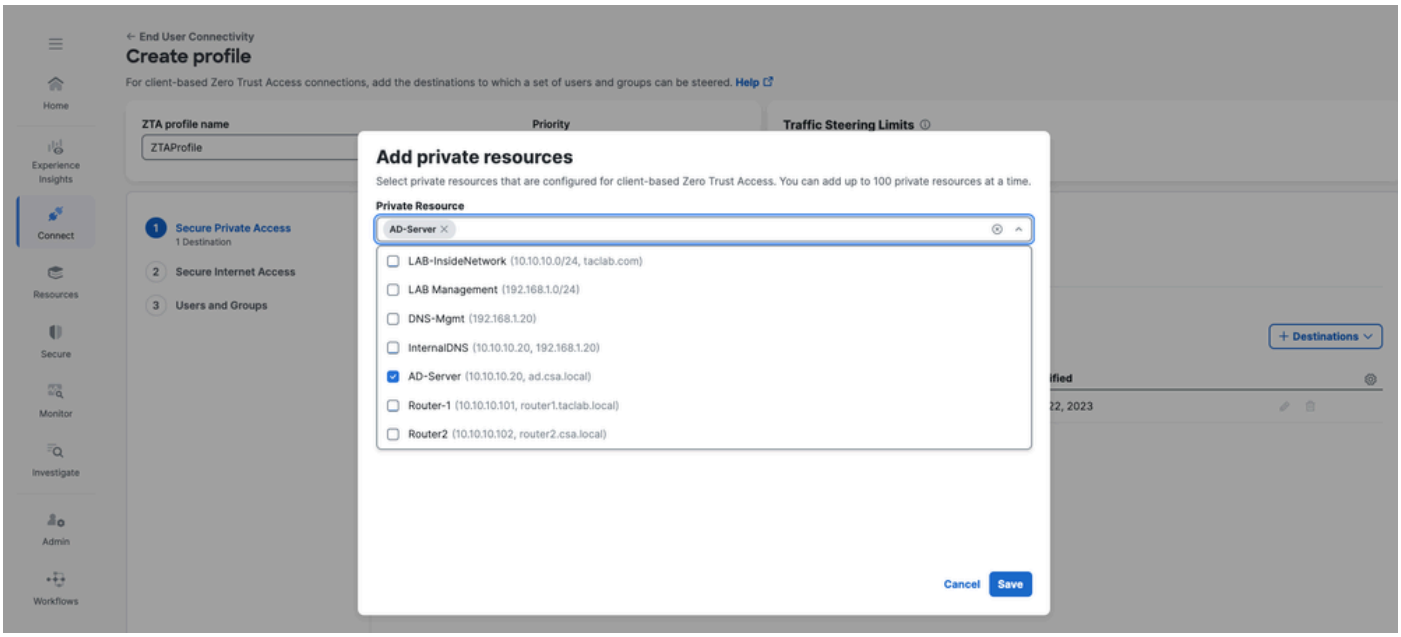


Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

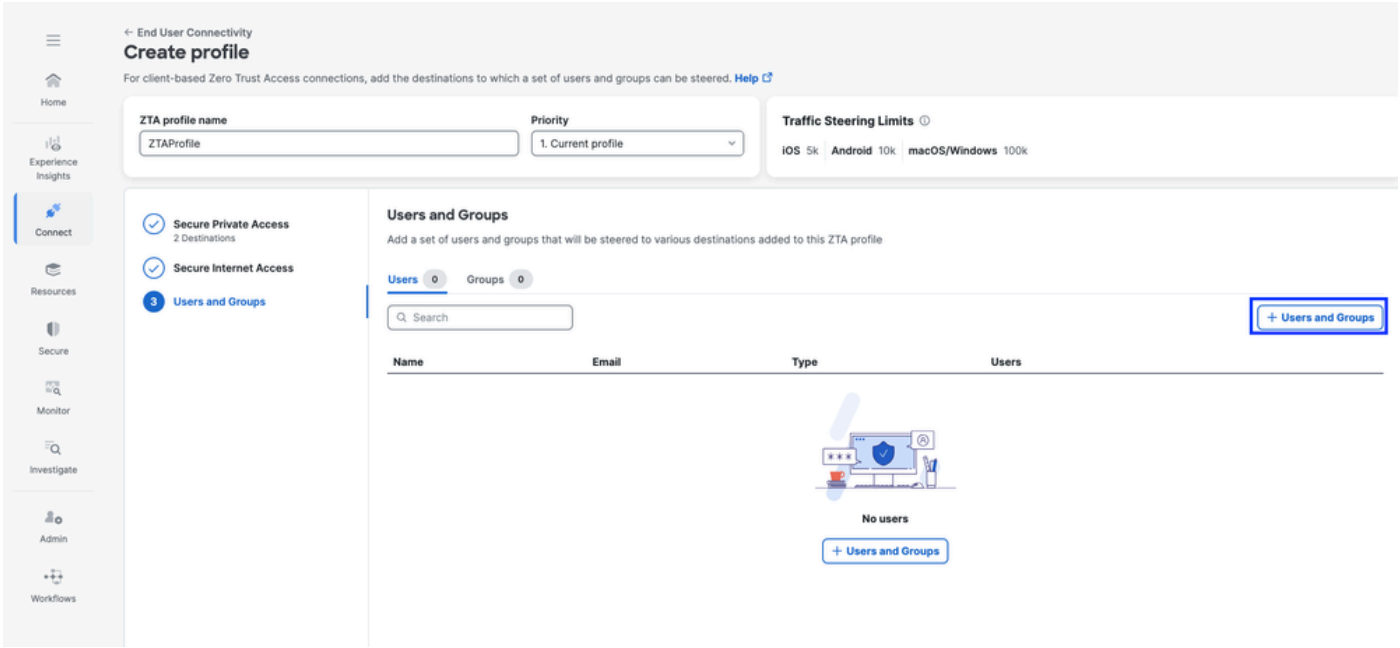


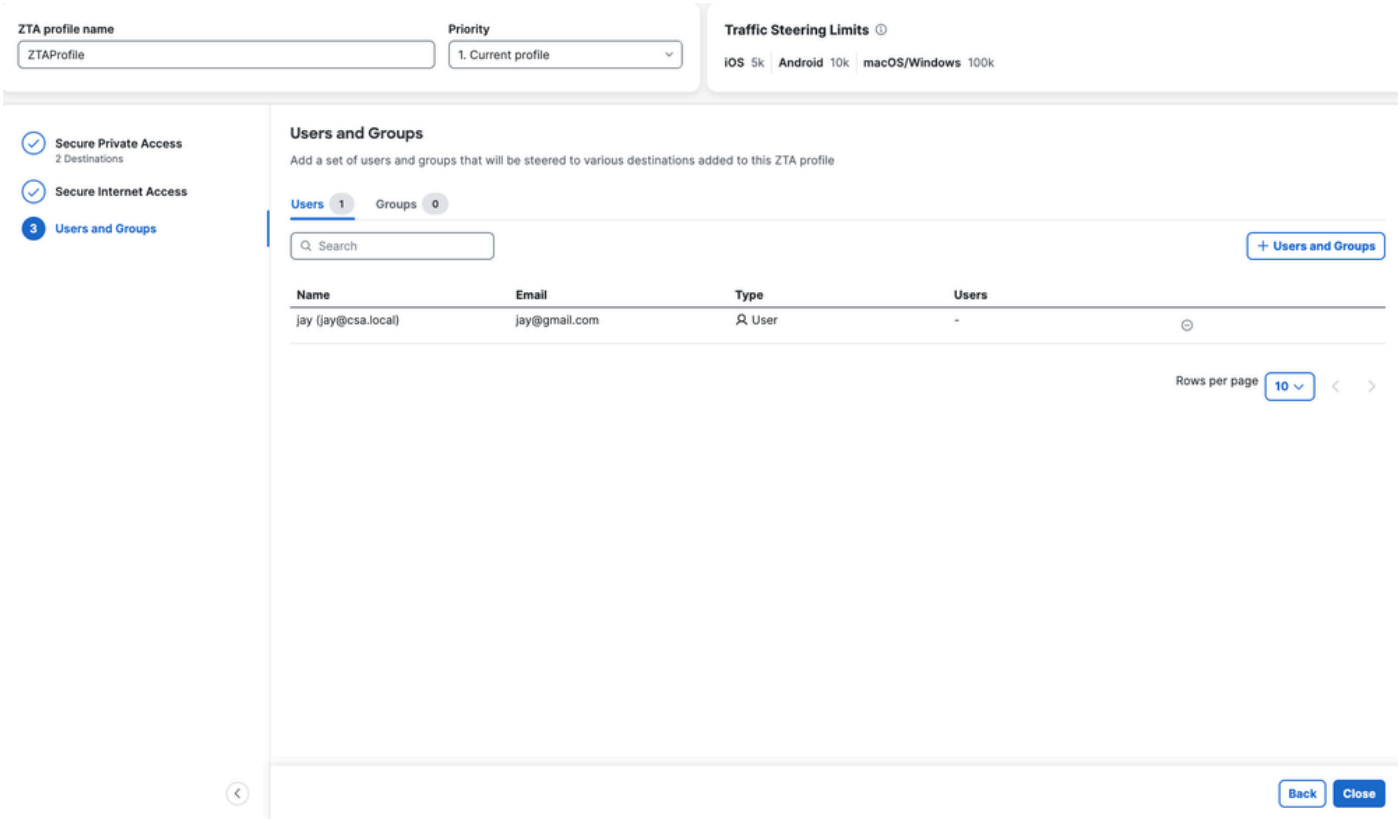
Acesso seguro - perfil ZTA



Acesso seguro - perfil ZTA

3. Adicionar usuários e grupos





Acesso seguro - perfil ZTA

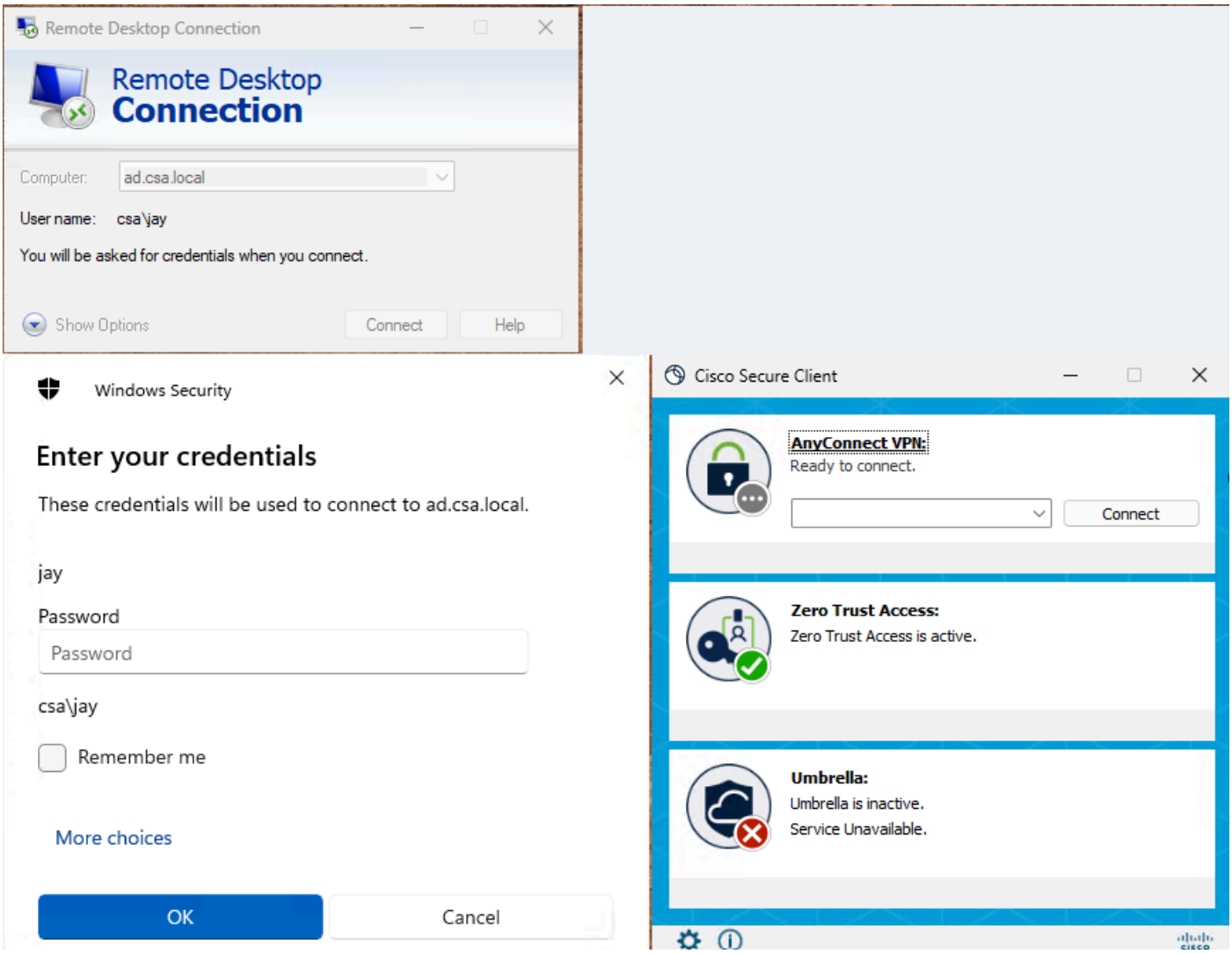
Note: Pode levar de 15 a 20 minutos para enviar e sincronizar a configuração para o cliente para o recurso privado atribuído

---

Etapa - 4 Verificar o acesso ao recurso privado

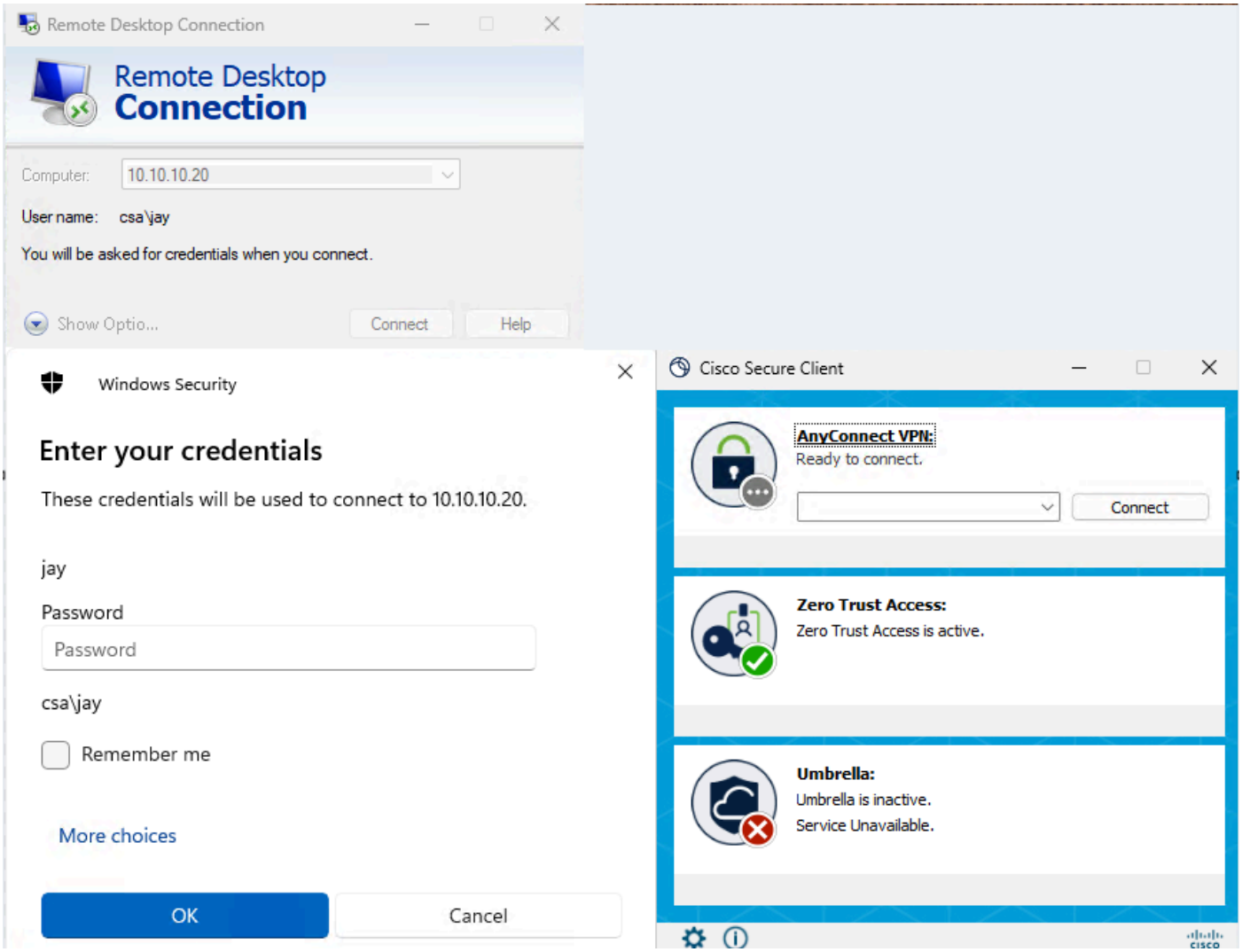
1. Acessar o Recurso Privado

Acessar a PR usando o FQDN



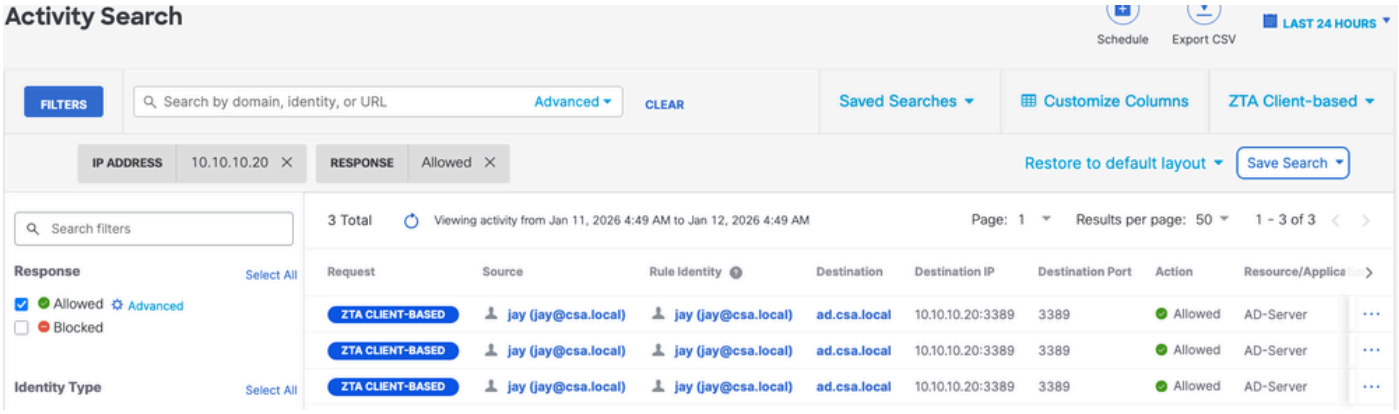
Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP

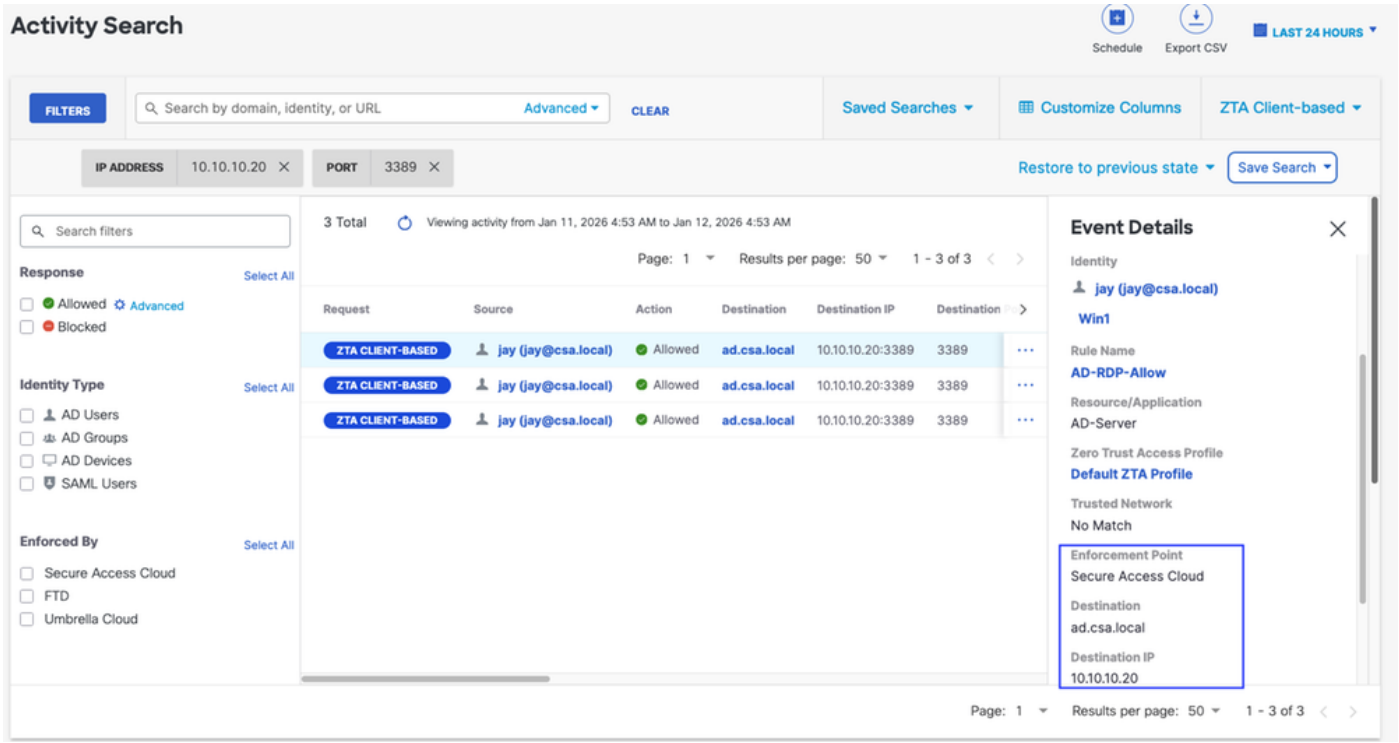


Acesso seguro - Teste de PR

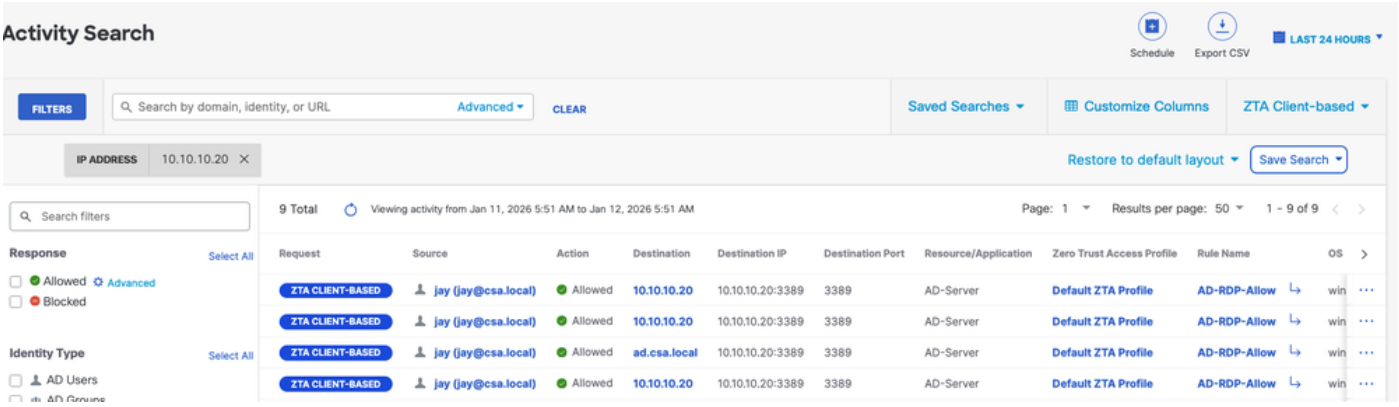
2. Verificar com os eventos de Pesquisa de Atividade



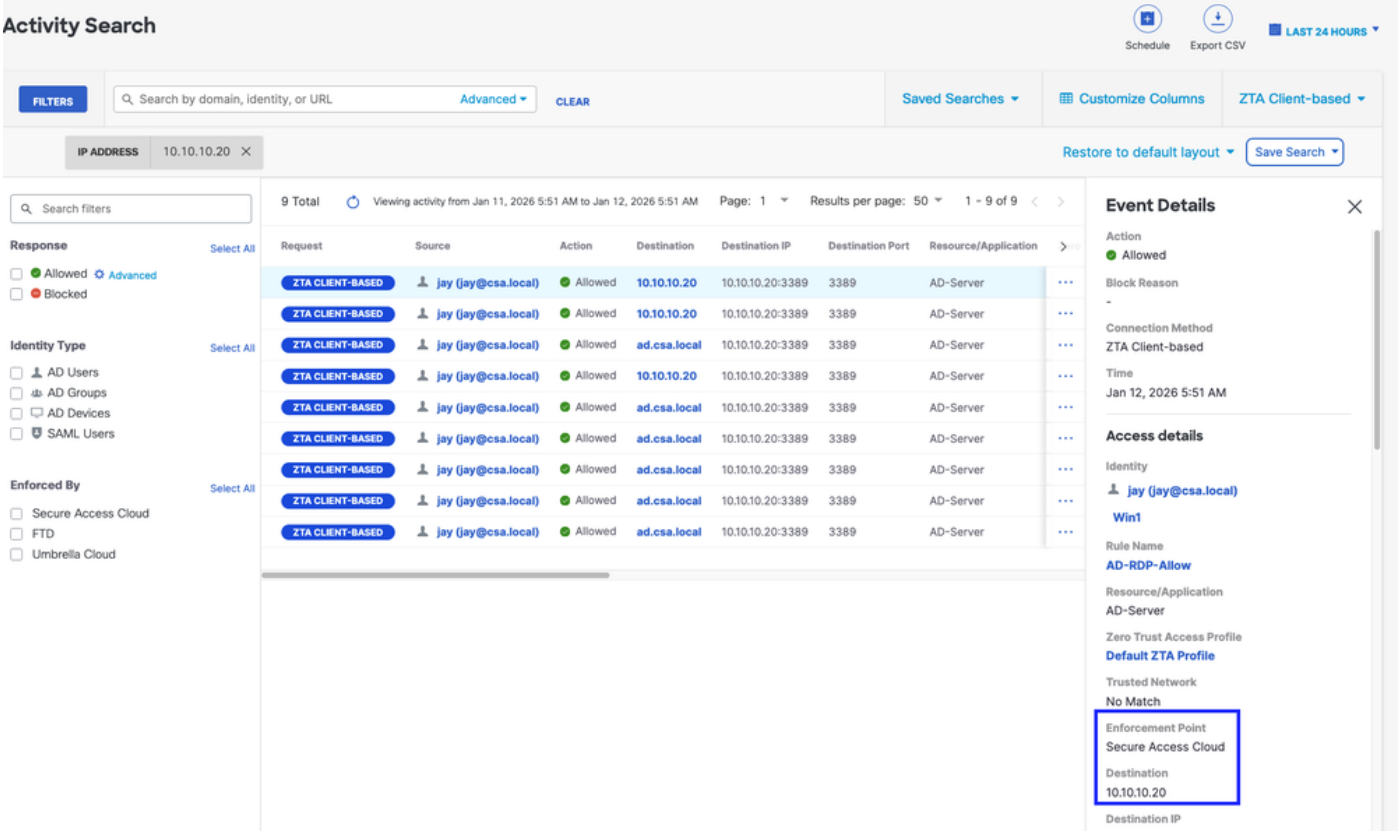
Acesso seguro - Pesquisa de atividades



Acesso seguro - Pesquisa de atividades

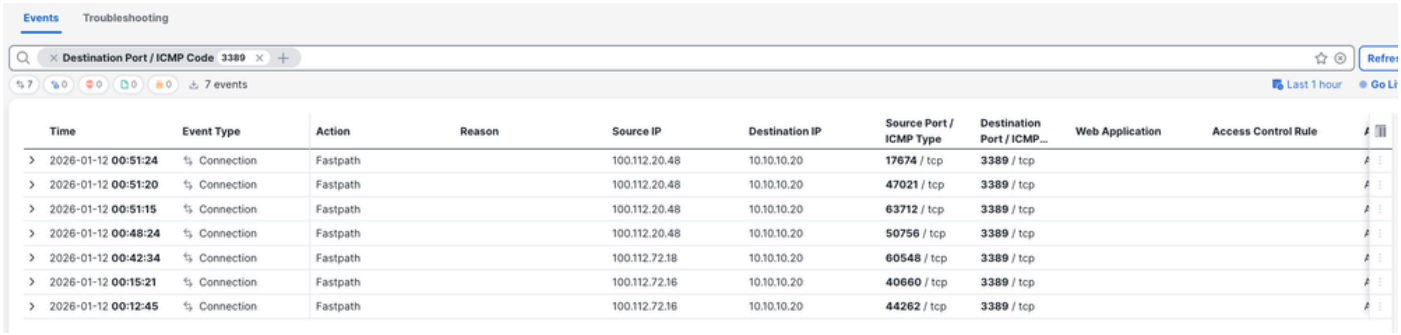


Acesso seguro - Pesquisa de atividades



Acesso seguro - Pesquisa de atividades

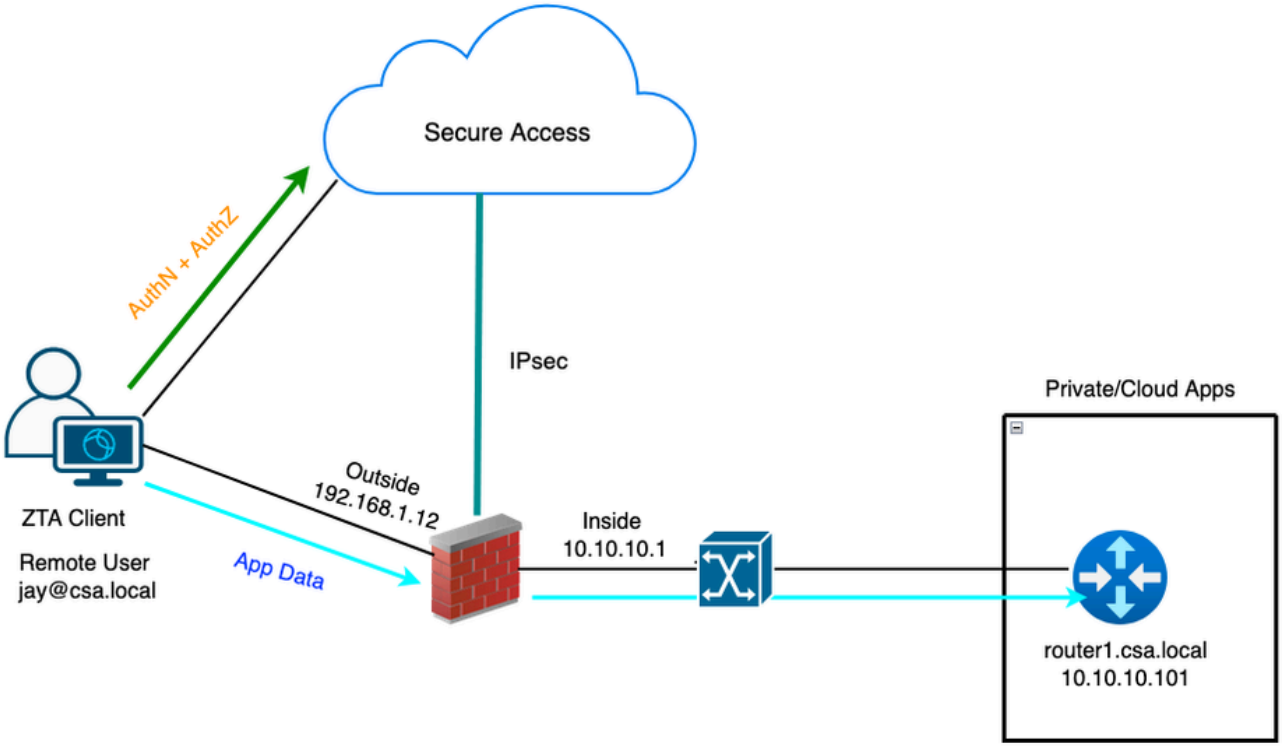
3. Verificar os eventos de ligação do FMC



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 .

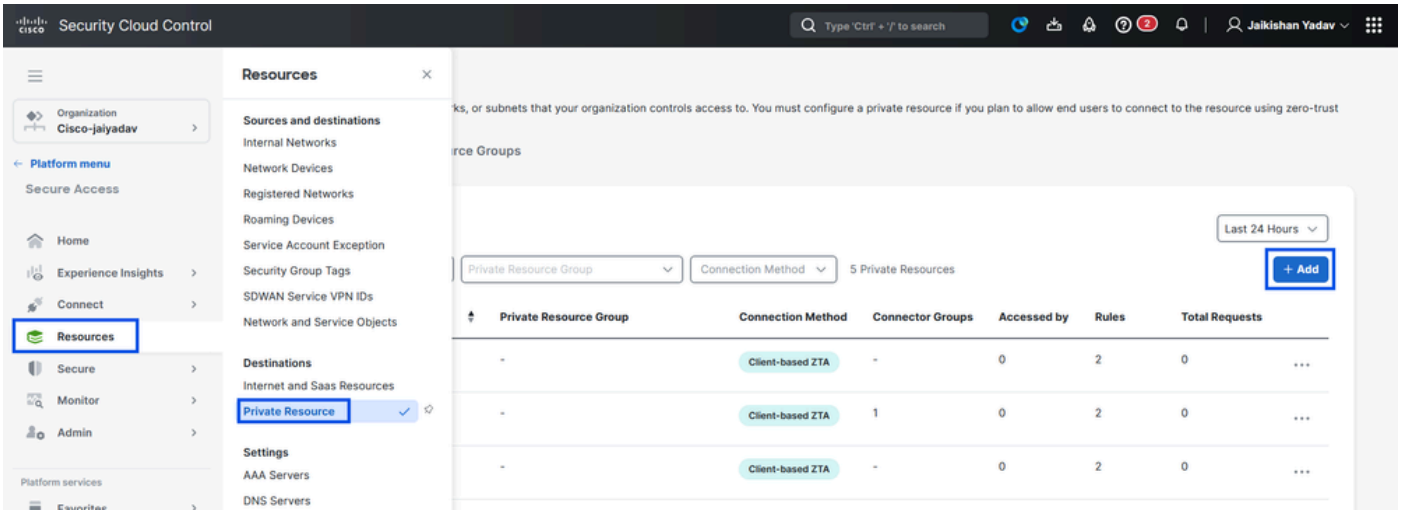


ZTA universal - Topologia de caso de teste

Etapa 1 - Definir um recurso privado no acesso seguro

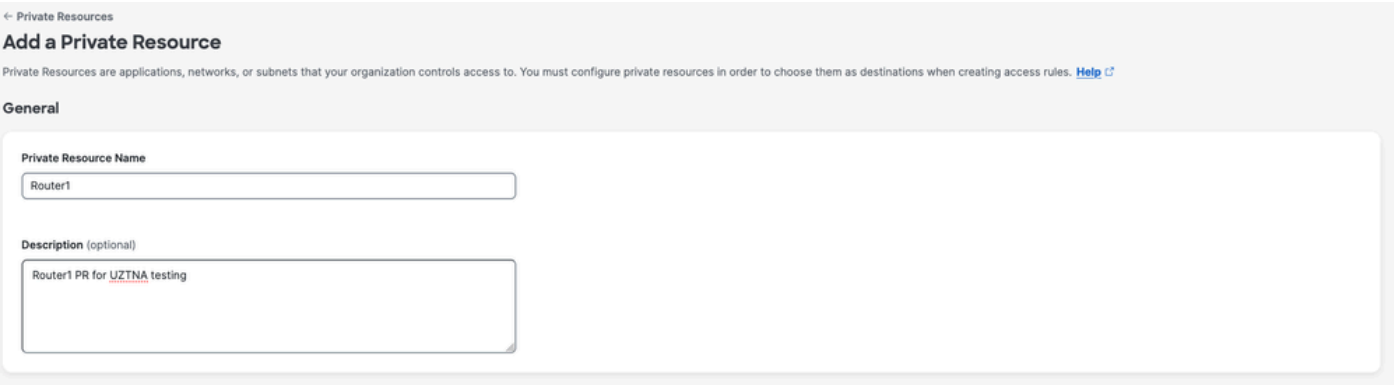
Configurar um recurso privado para ser acessível por meio do dispositivo registrado ZTA (Zero Trust Access) com aplicação de nuvem

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



Acesso seguro - Configuração de recursos privados

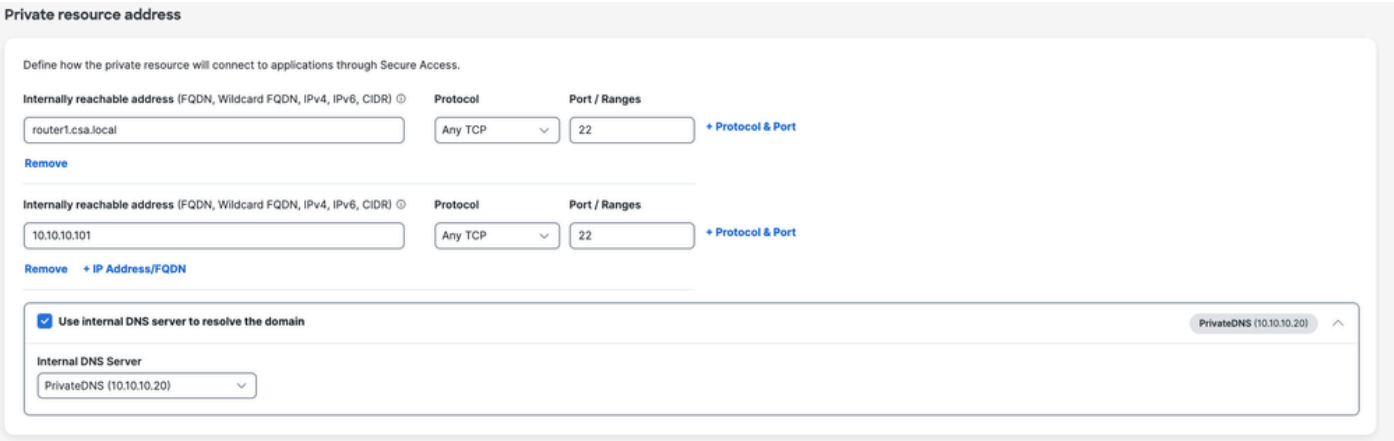
2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do recurso.



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

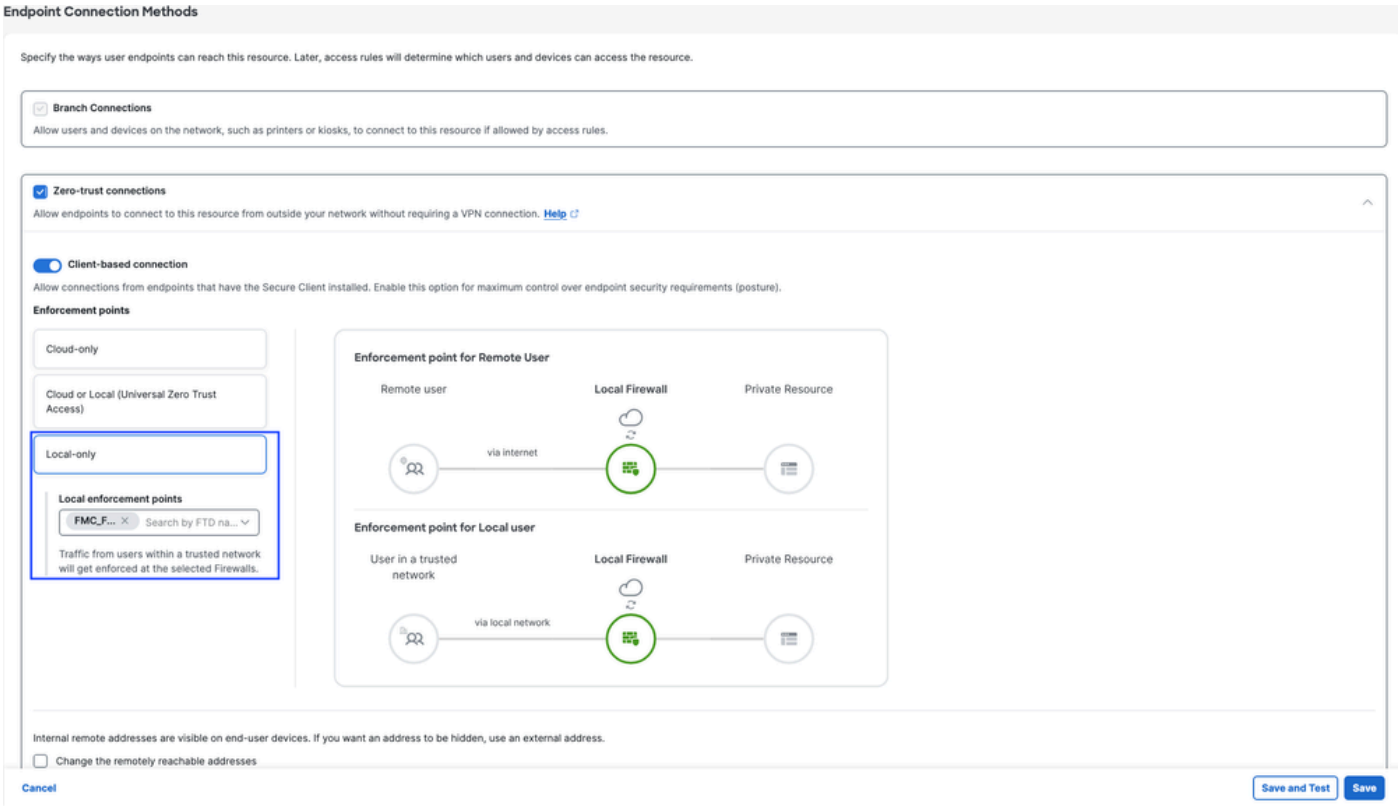
4. Selecione o servidor DNS interno para resolver o problema do domínio



Acesso seguro - Configuração de recursos privados

5. Selecionar Métodos de Conexão de Ponto de Extremidade

6. Selecionar FTD como pontos de imposição locais



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

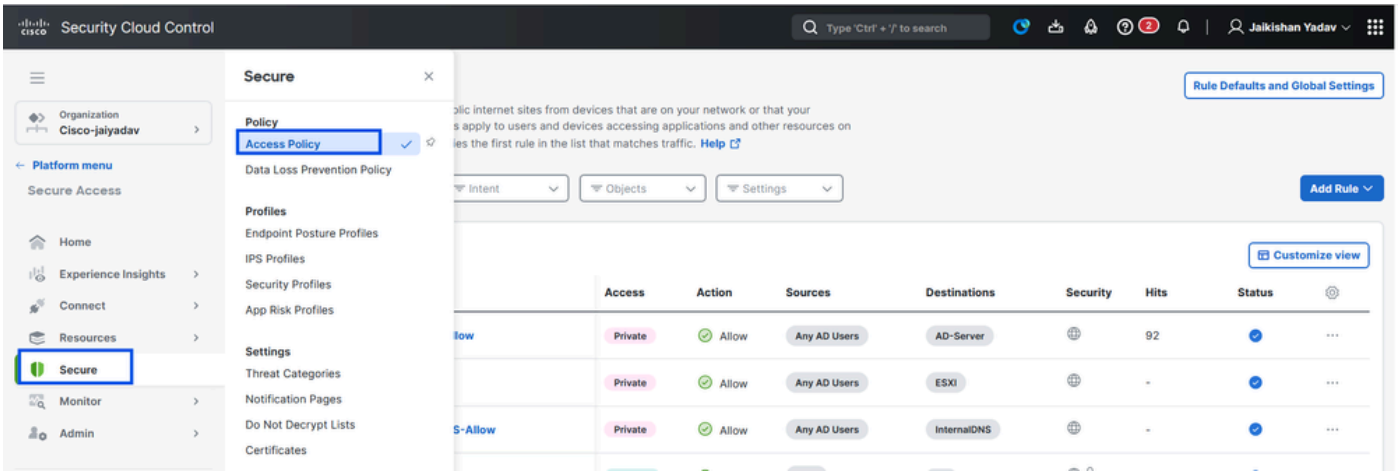
---

7. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

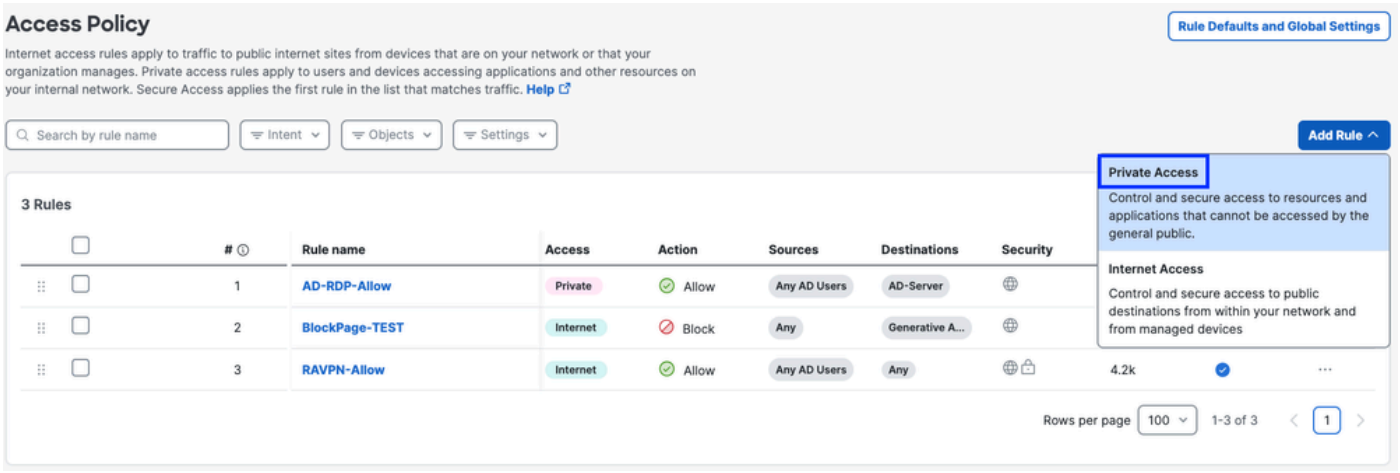
Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA . Para obter mais informações, consulte Regra de acesso privado

1. Navegue até Proteger > Política de acesso



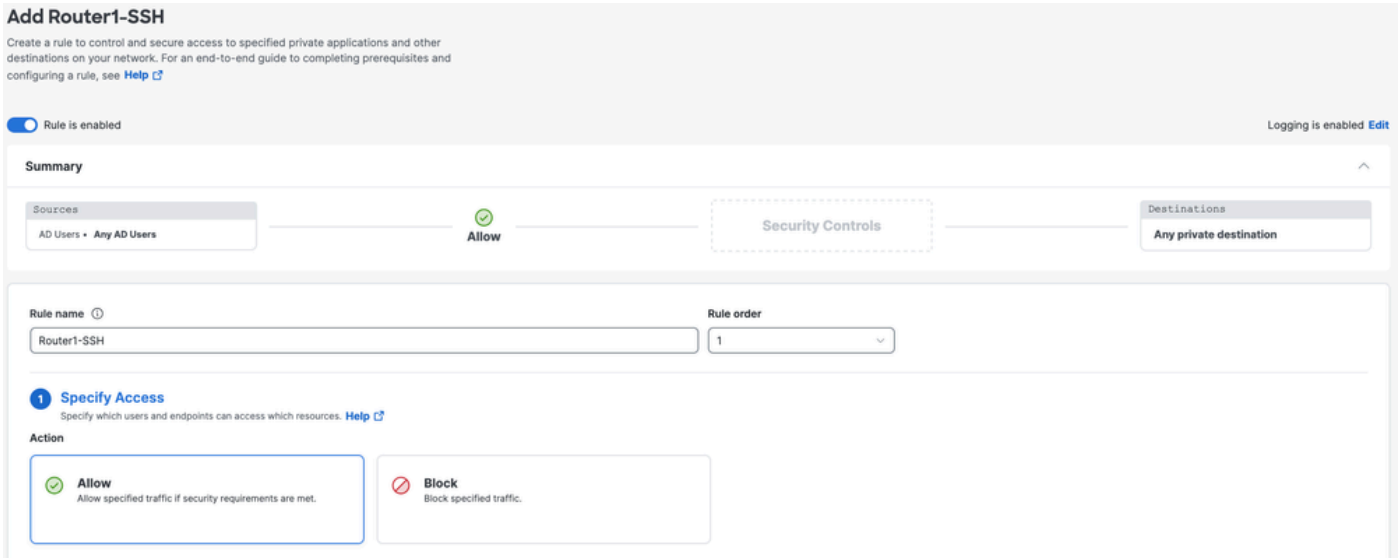
Acesso seguro - Configuração de recursos privados

2. Clique em Adicionar Regra e escolha Acesso Particular.
   Na parte superior da regra há um resumo que descreve os componentes configurados da regra.



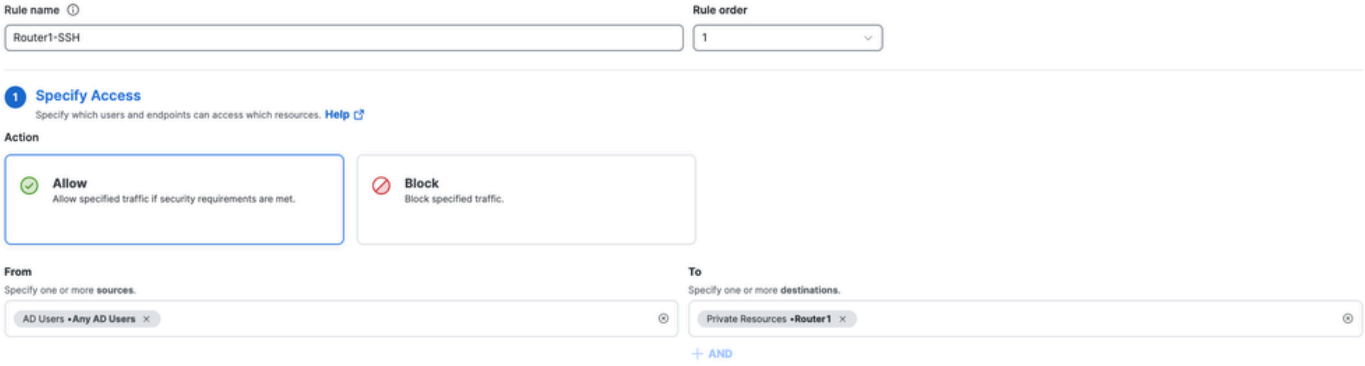
Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra



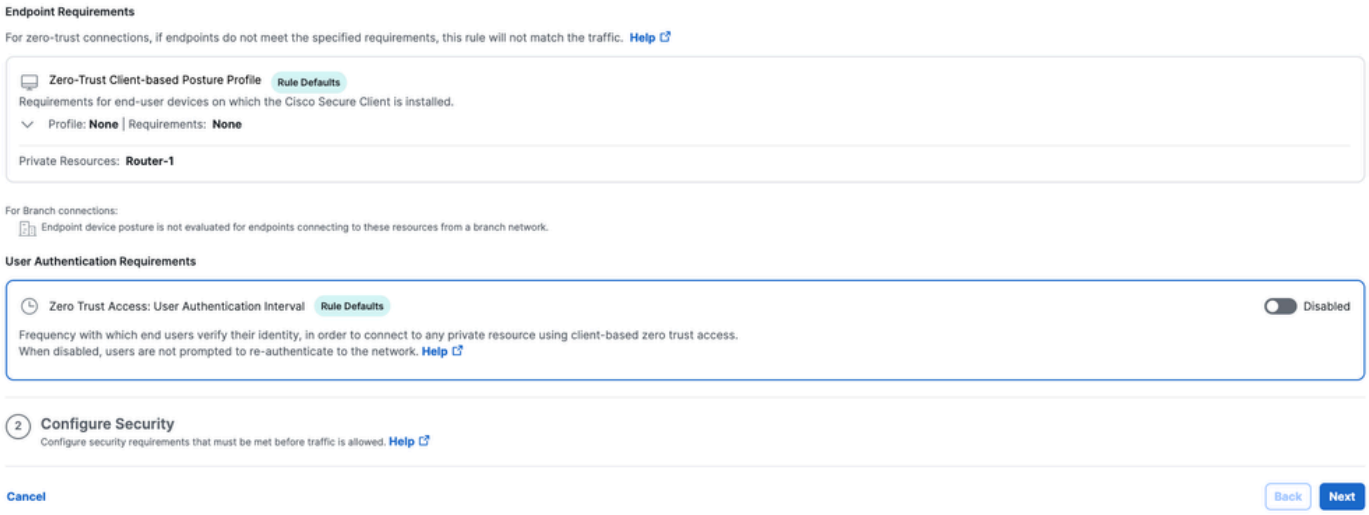
Acesso seguro - Configuração da política de acesso

4. Selecione a ação da regra e selecione origem e destino



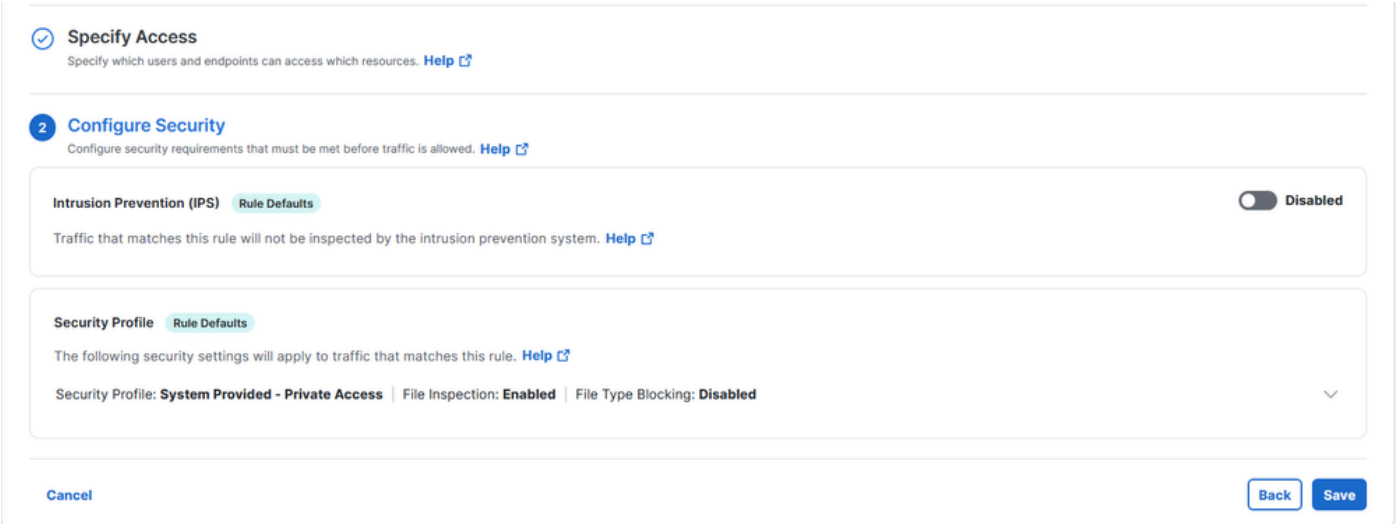
Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint



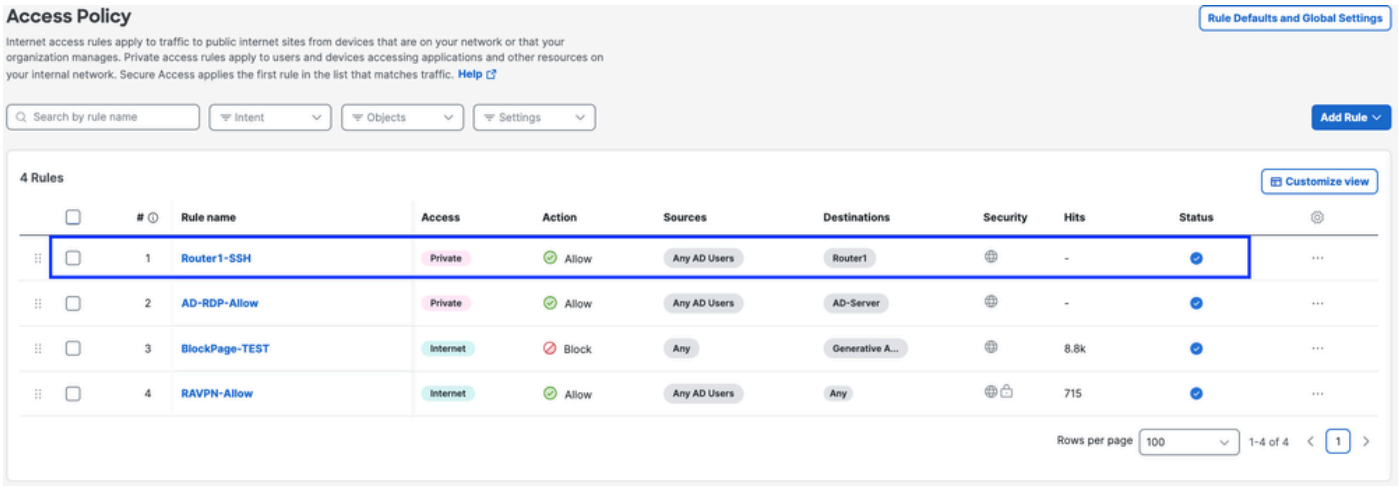
Acesso seguro - Configuração da política de acesso

6. Configurar segurança



Acesso seguro - Configuração da política de acesso

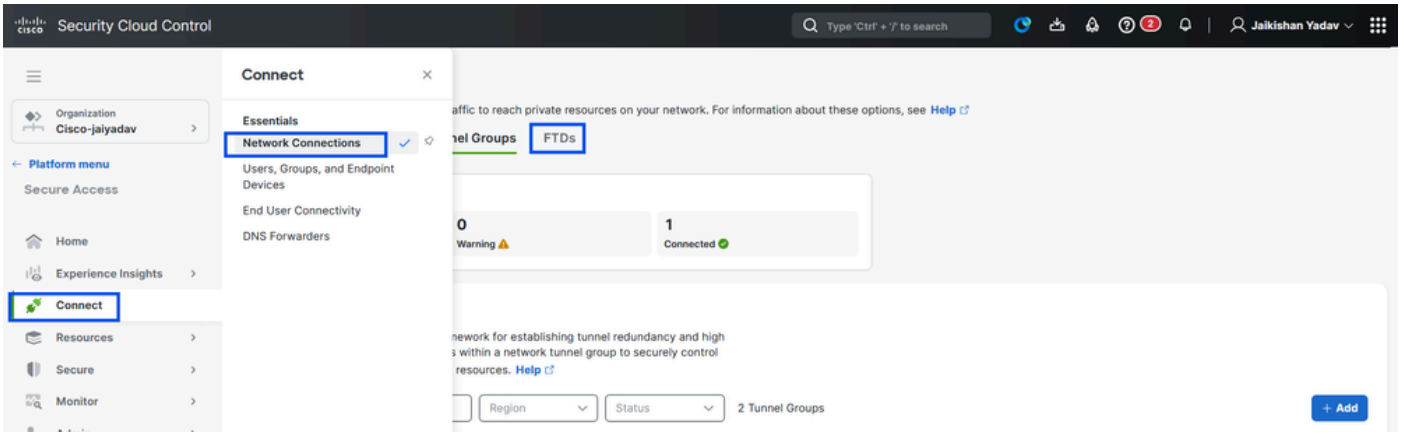
7. Clique em Salvar



Acesso seguro - Configuração da política de acesso

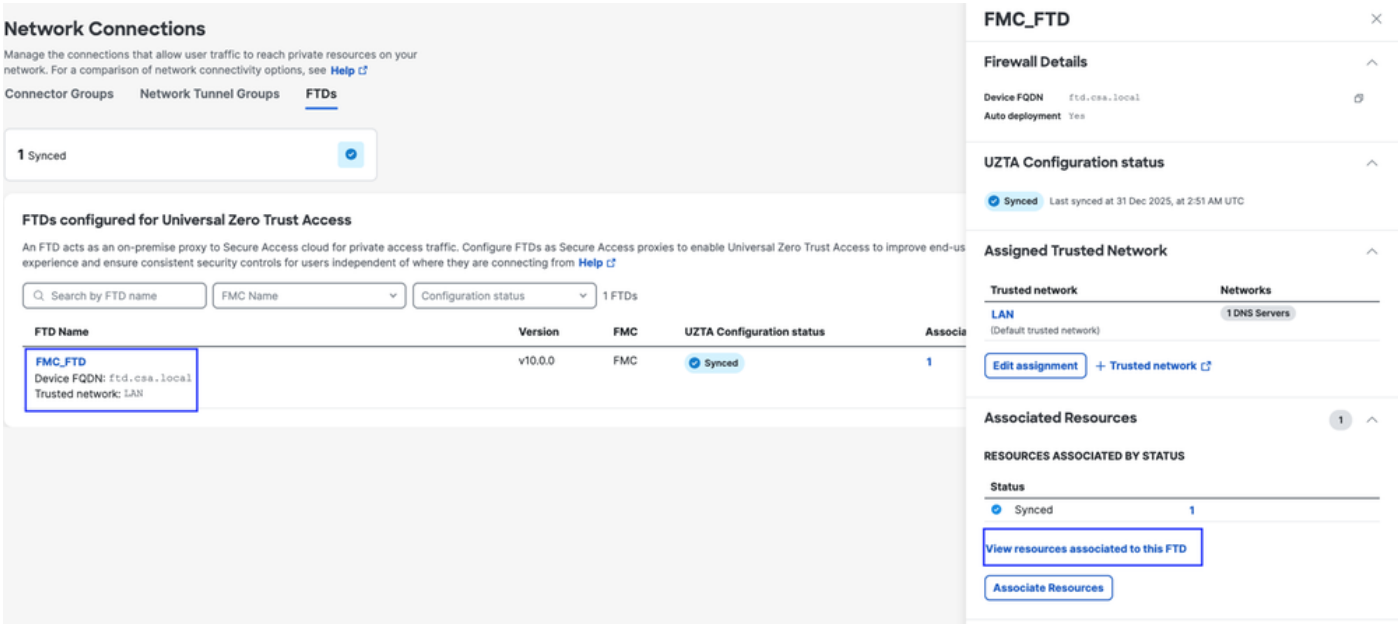
Etapa 3 - Verificar a associação de PR no FTD

1. Navegue até Conectar > Conexões de Rede > FTDs

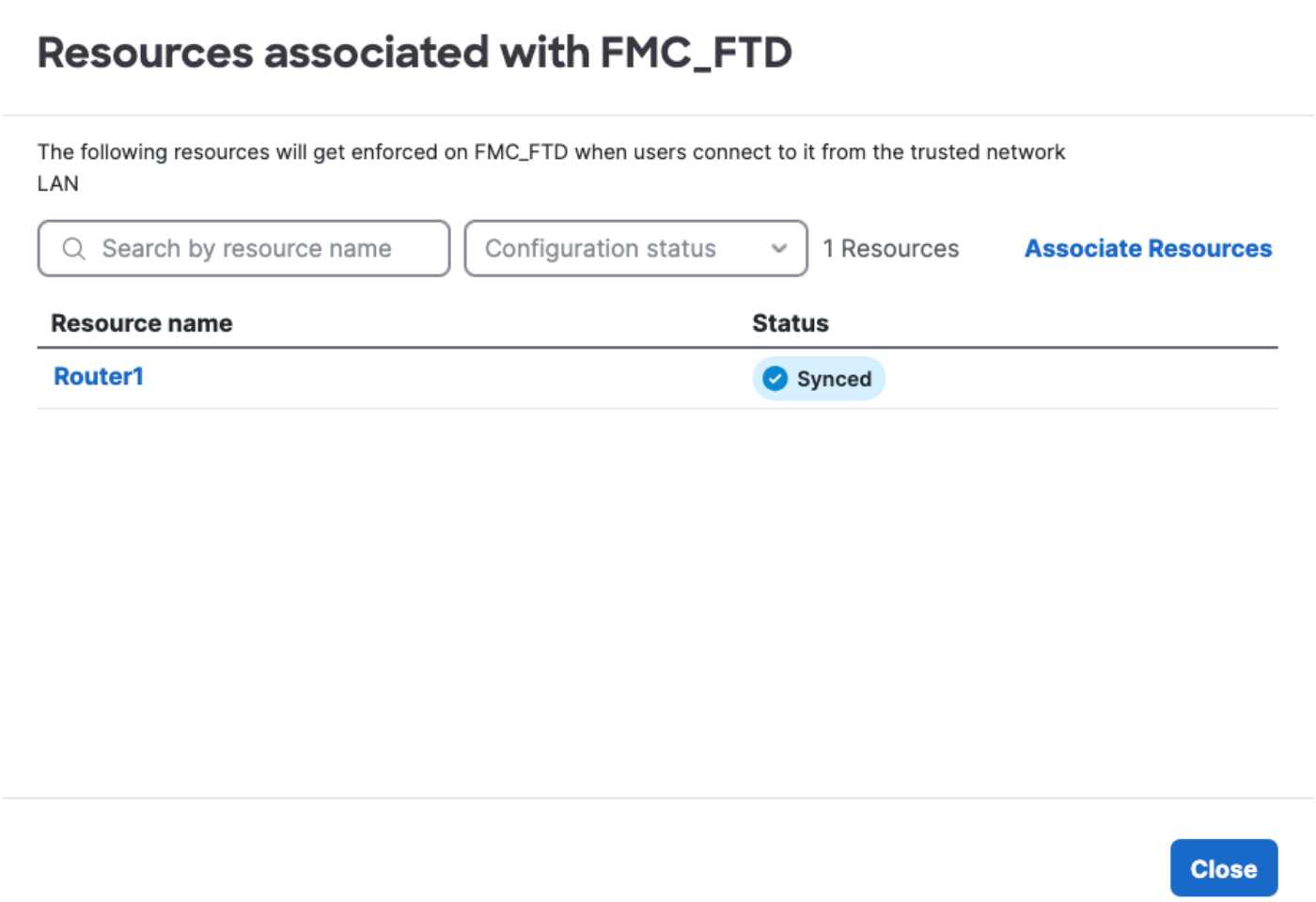


Acesso seguro - Verificação de PR

2. Clique em FTD > Exibir recursos associados a este FTD



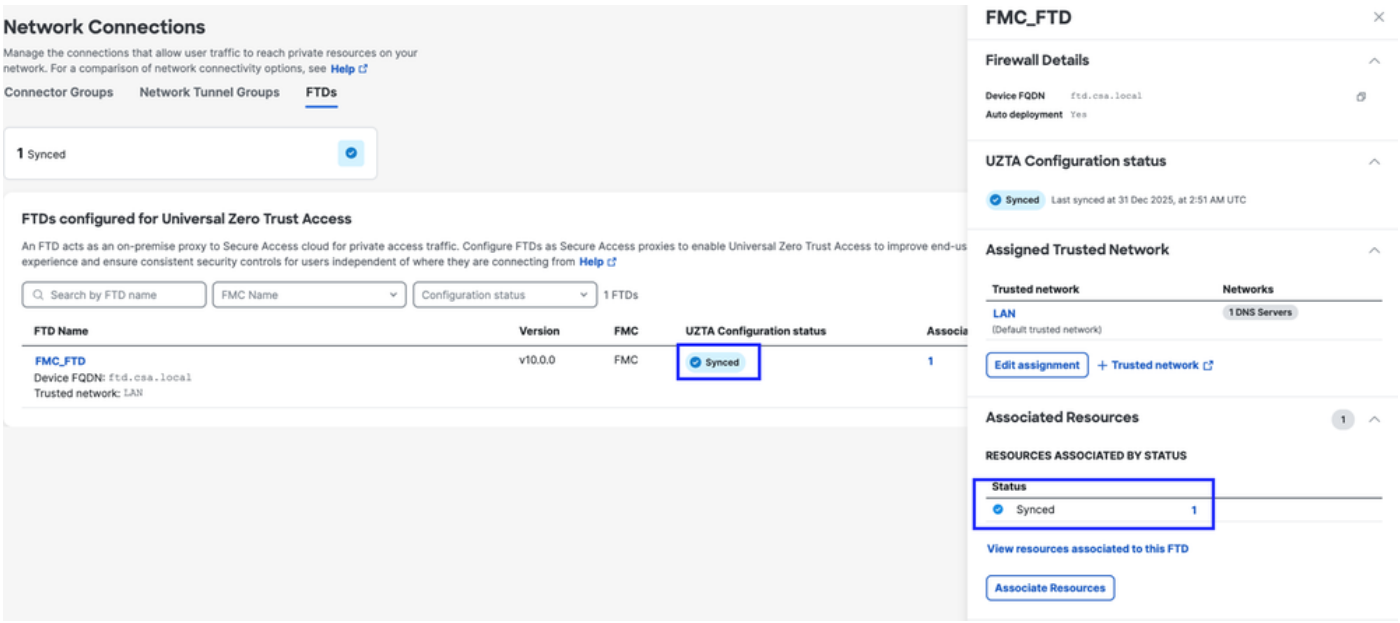
Acesso seguro - Verificação de PR



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



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

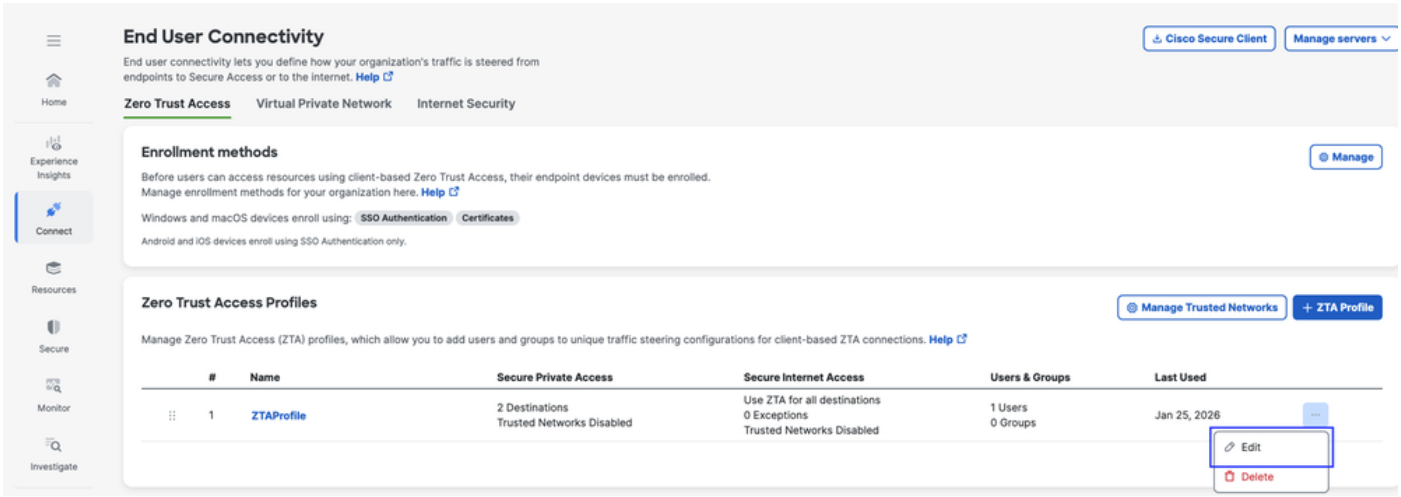
show running-config object application

```
> 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

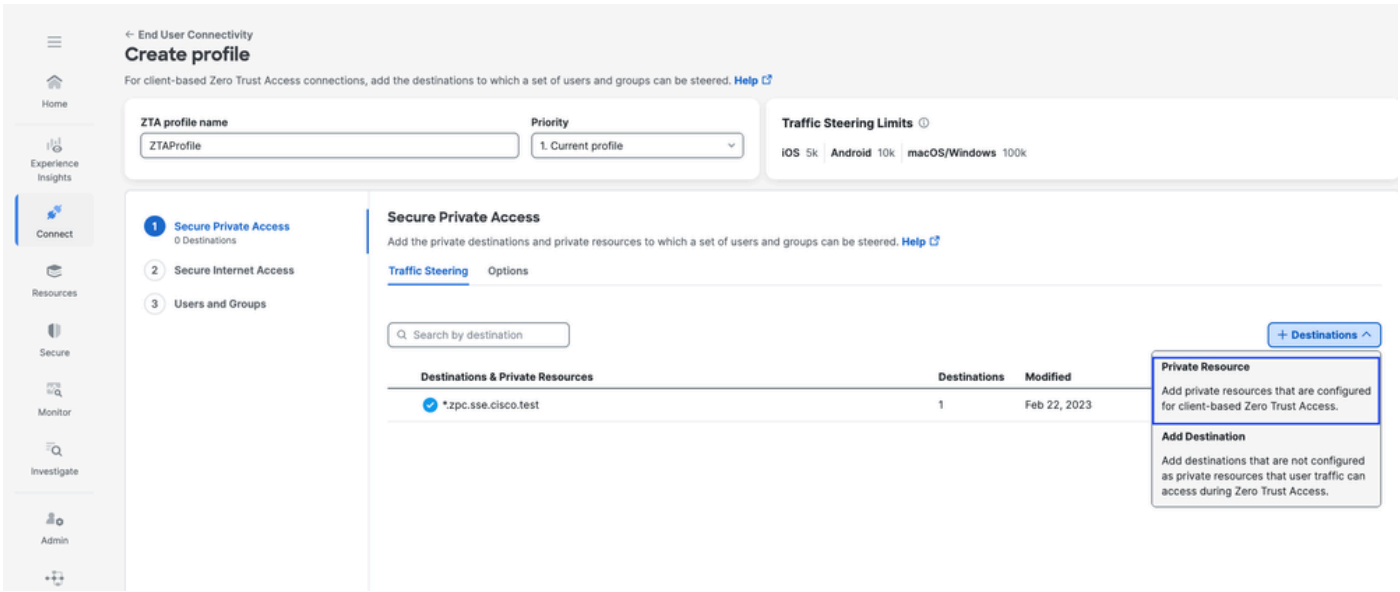
Etapa - 4 Adicionar recurso privado ao perfil ZTA

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

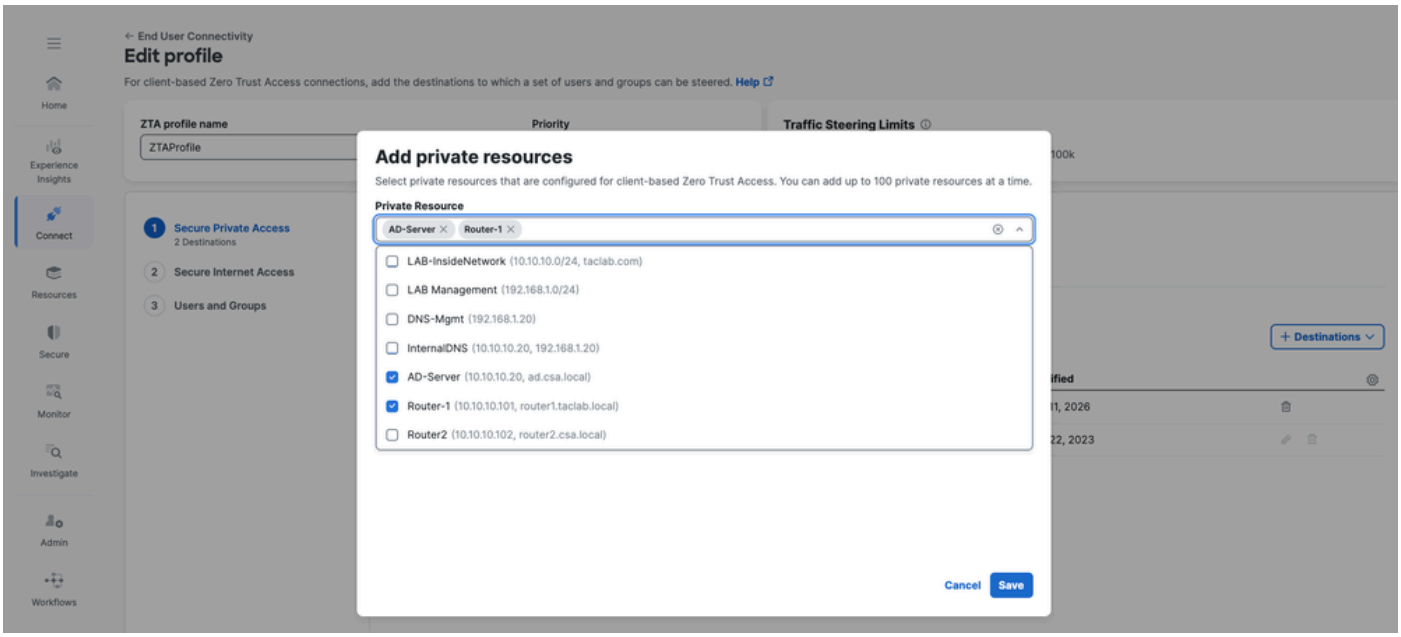


Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

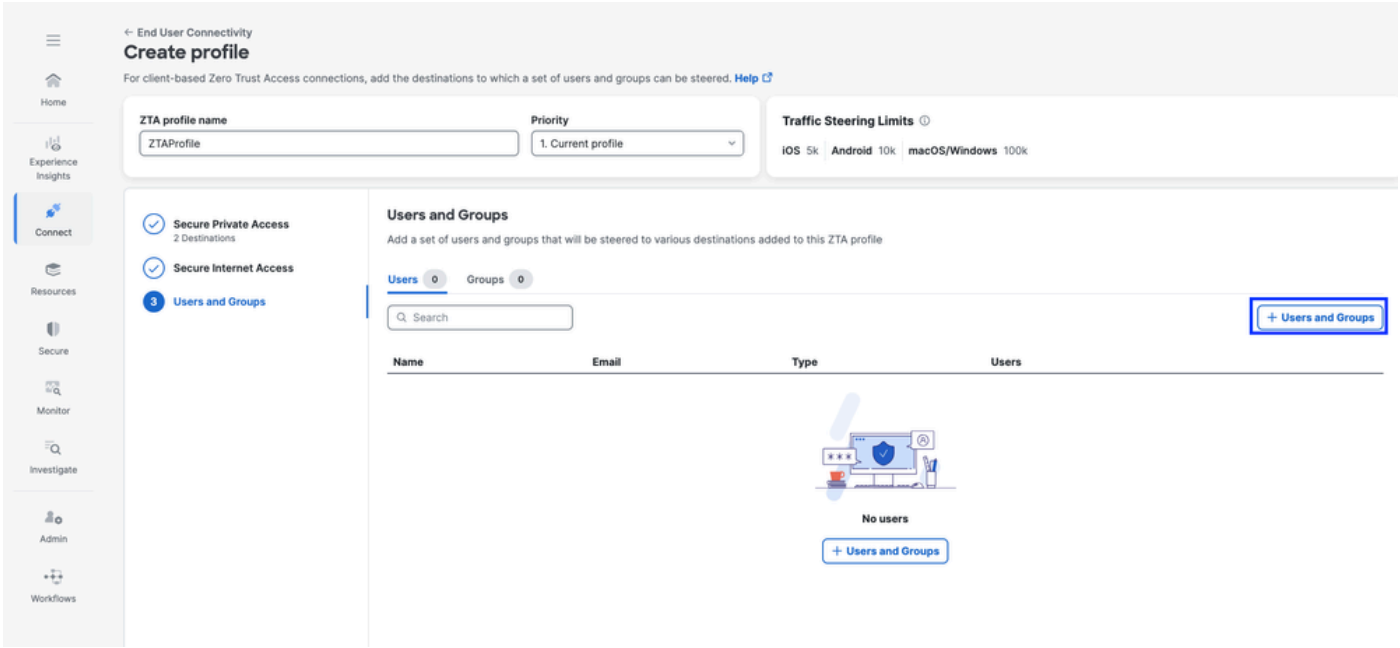


Acesso seguro - perfil ZTA

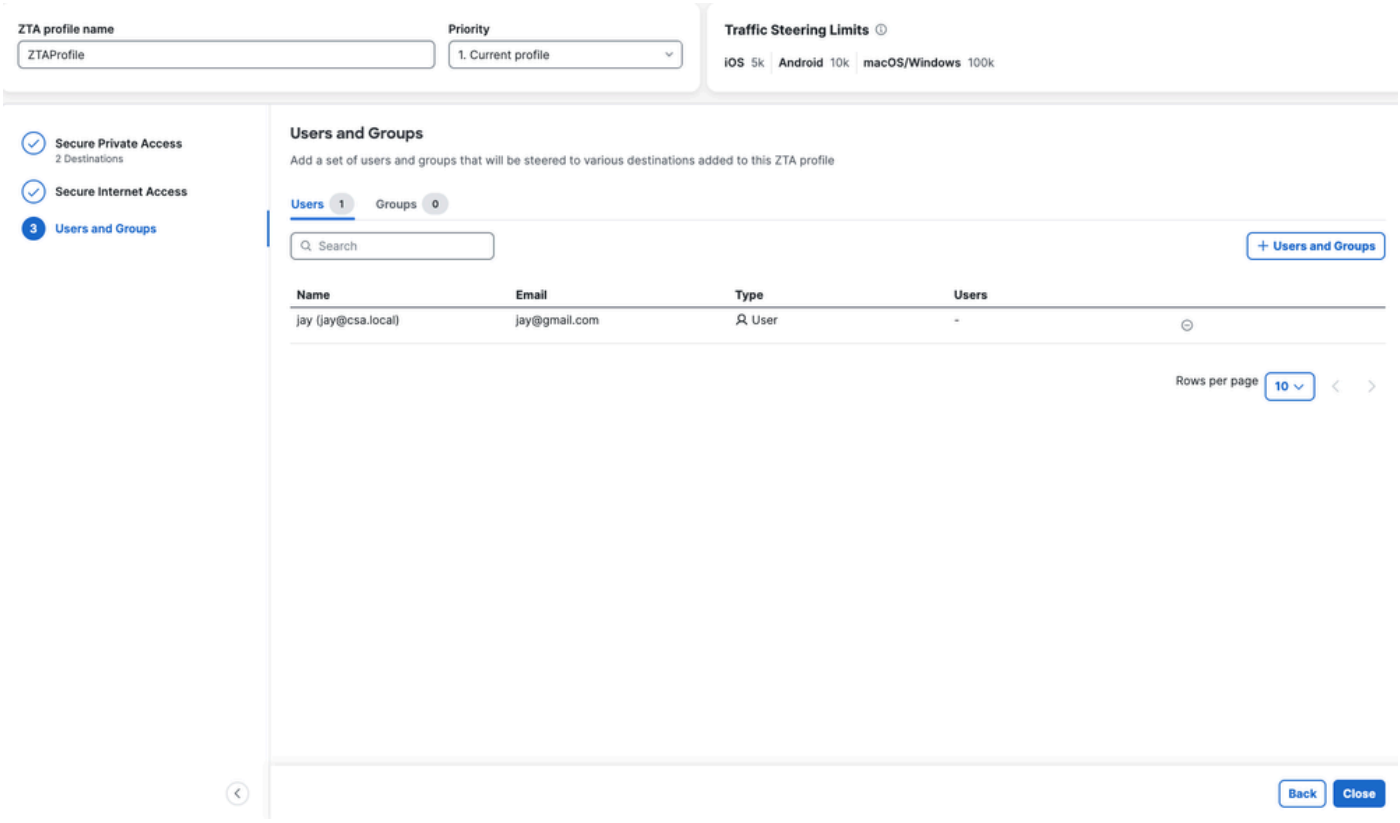


Acesso seguro - perfil ZTA

3. Adicionar usuários e grupos



Acesso seguro - perfil ZTA



Acesso seguro - perfil ZTA

Etapa 5 - Verificar o acesso ao recurso privado

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

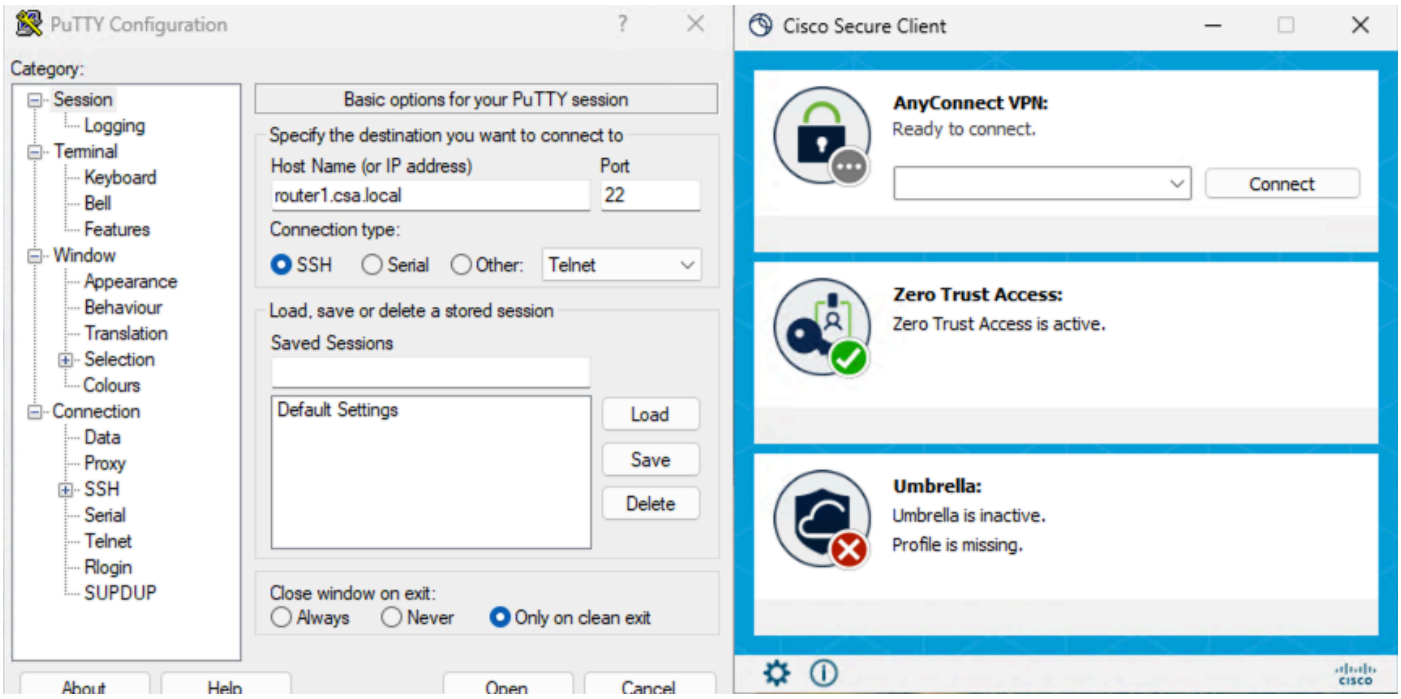
```
PS C:\Users\jay> ping ftd.csa.local

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
```

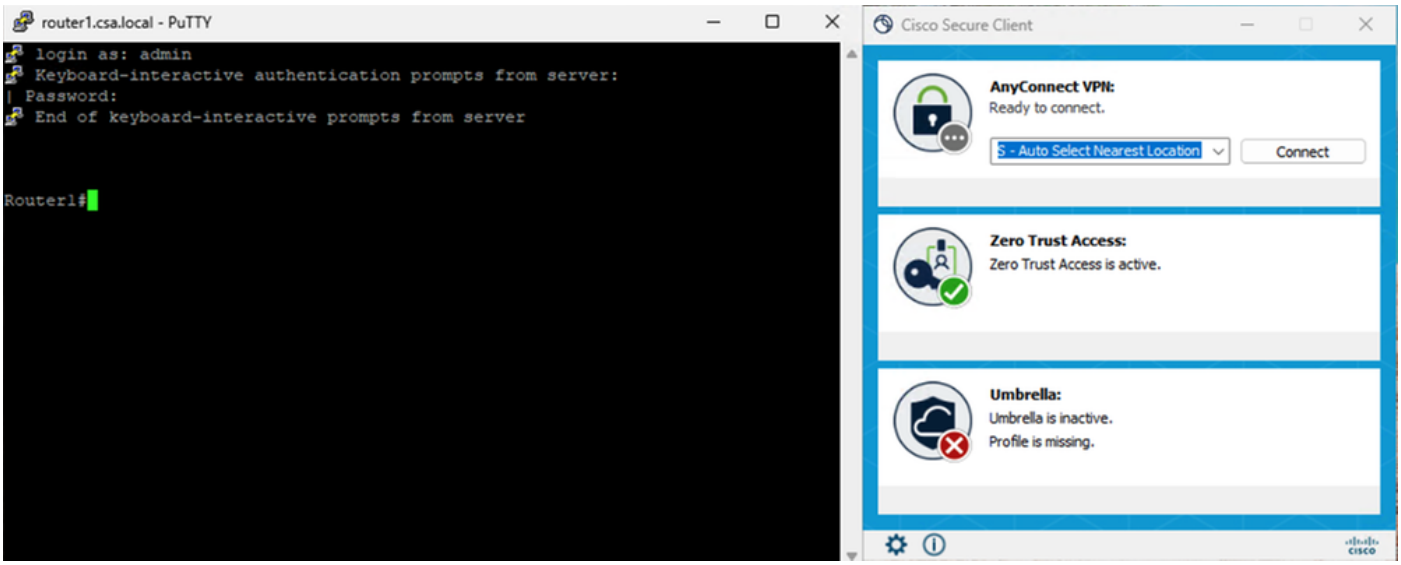
2. Verificar se o FTD pode acessar o recurso privado usando o FQDN

```
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#
```


3. Testar a conexão SSH com o recurso privado

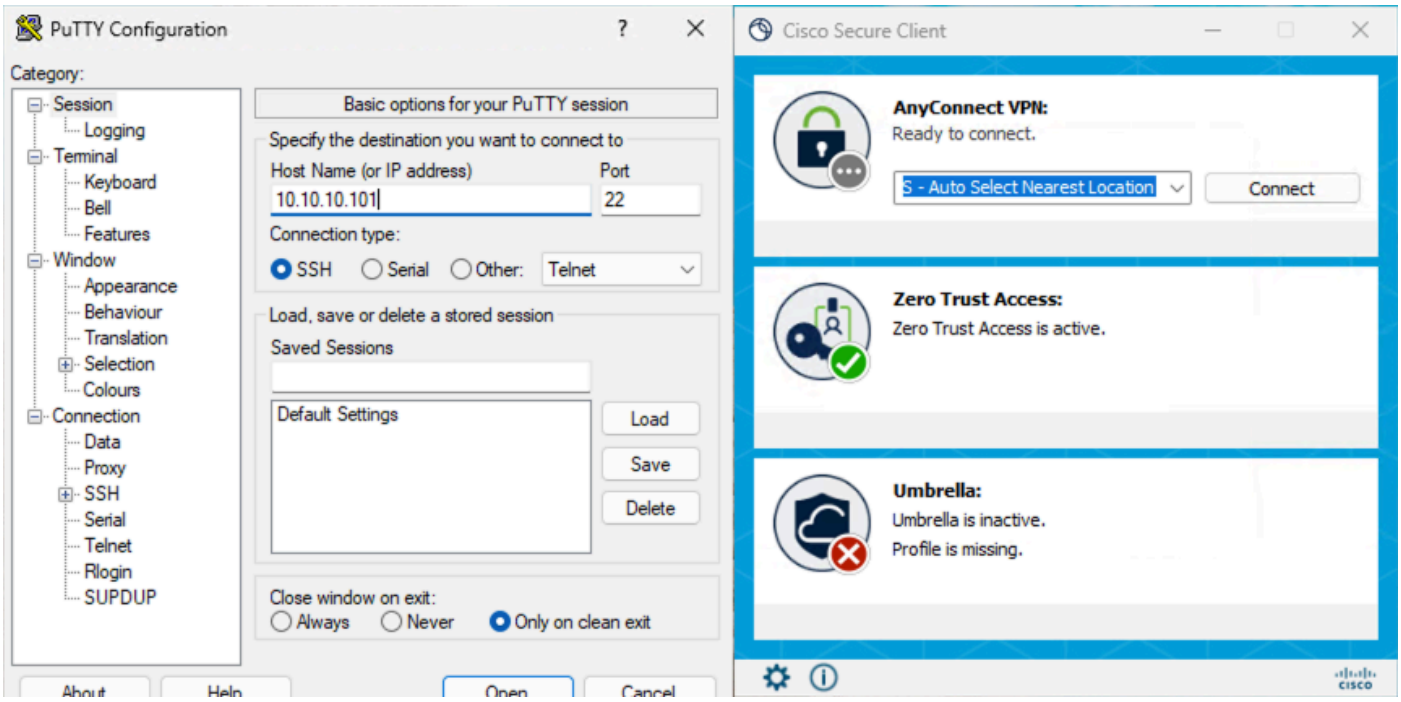
Acessar a PR usando o FQDN



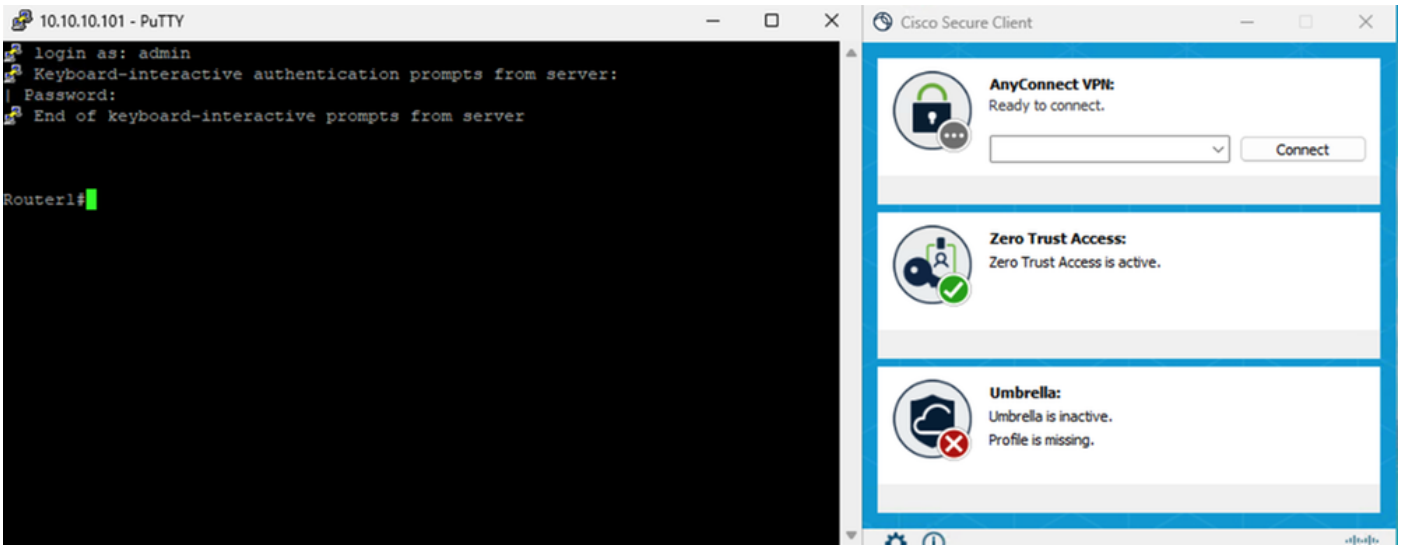


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP

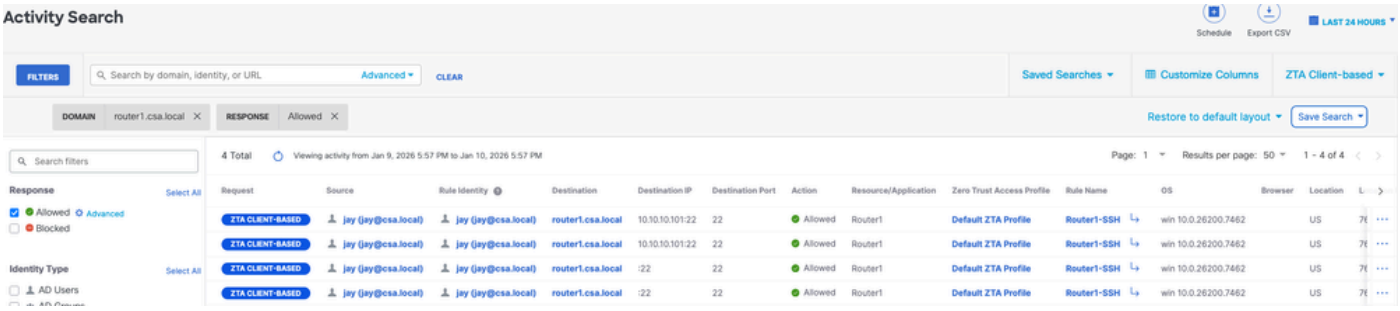


Acesso seguro - Teste de PR

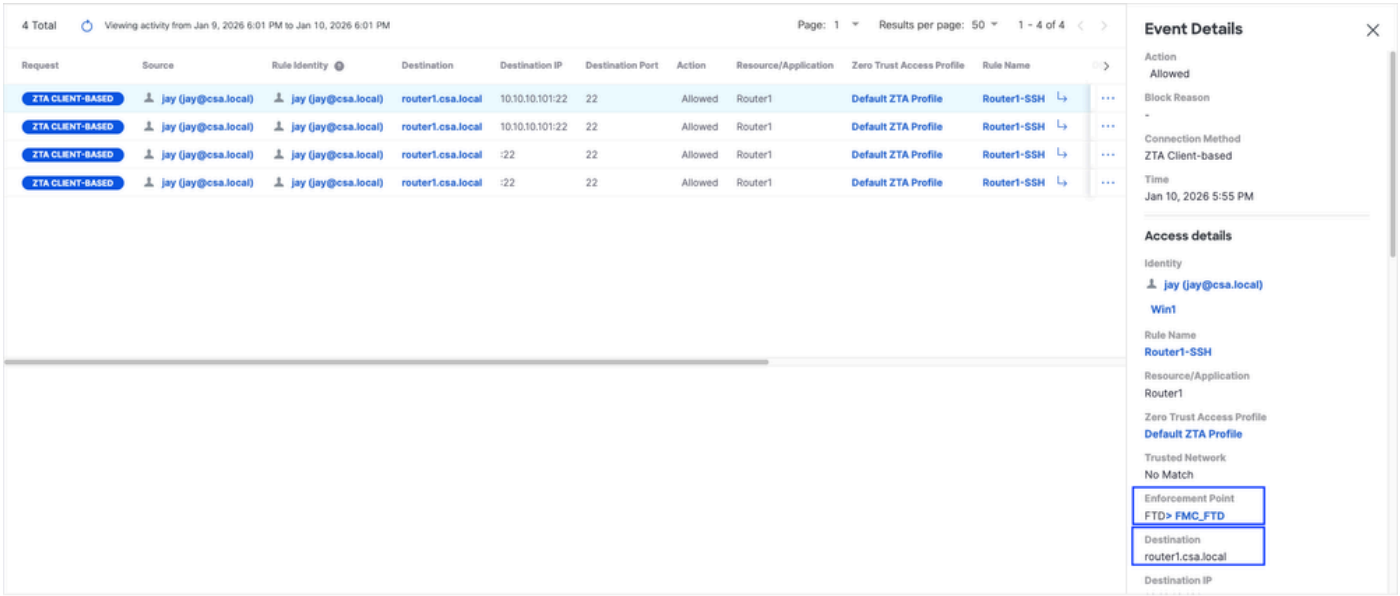


Acesso seguro - Teste de PR

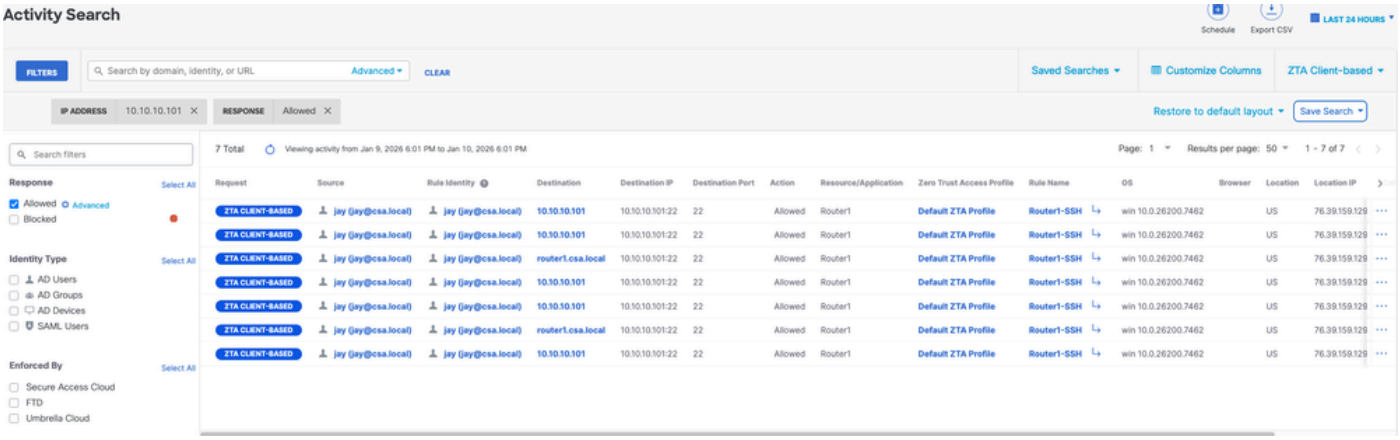
4. Verificar logs de Pesquisa de Atividade de Acesso Seguro



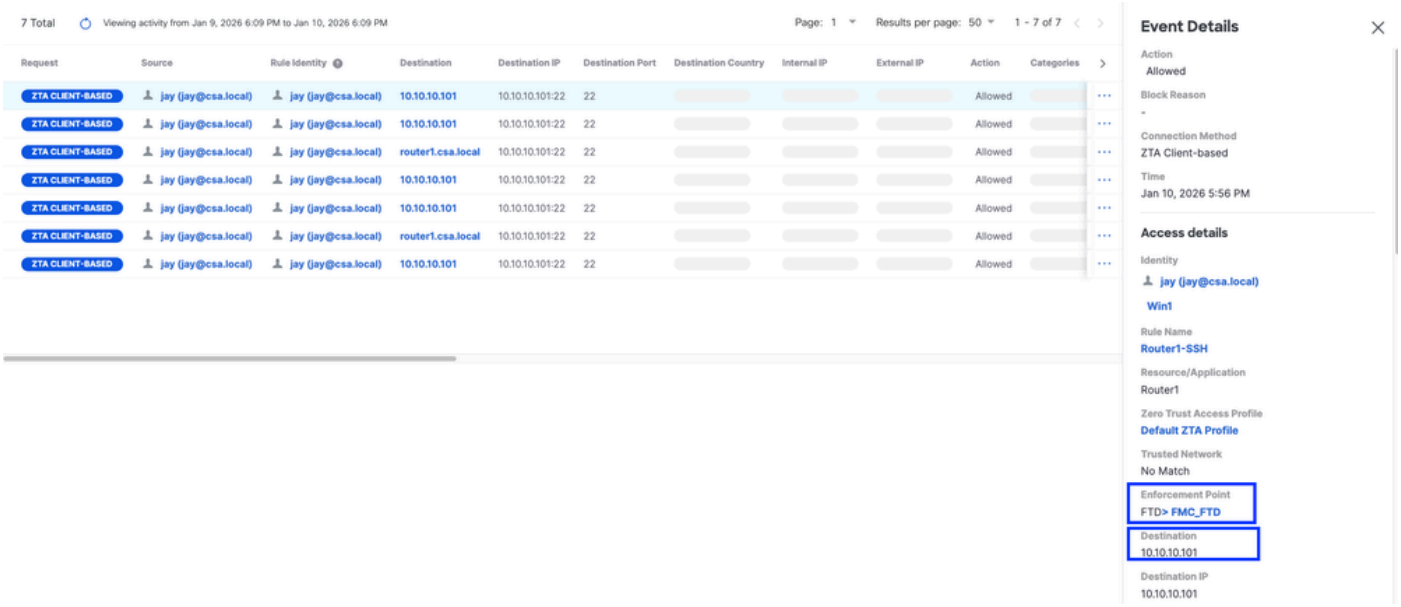
Acesso seguro - Pesquisa de atividades



Acesso seguro - Pesquisa de atividades

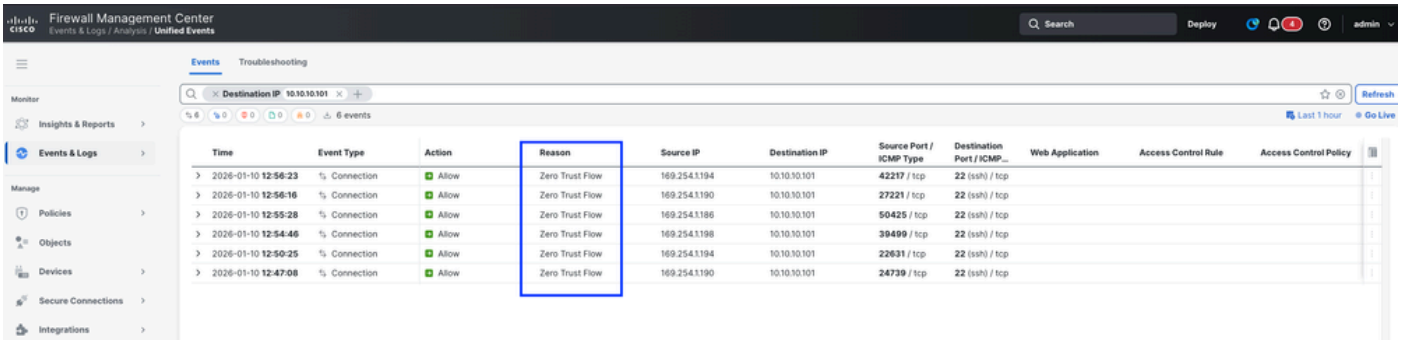


Acesso seguro - Pesquisa de atividades



Acesso seguro - Pesquisa de atividades

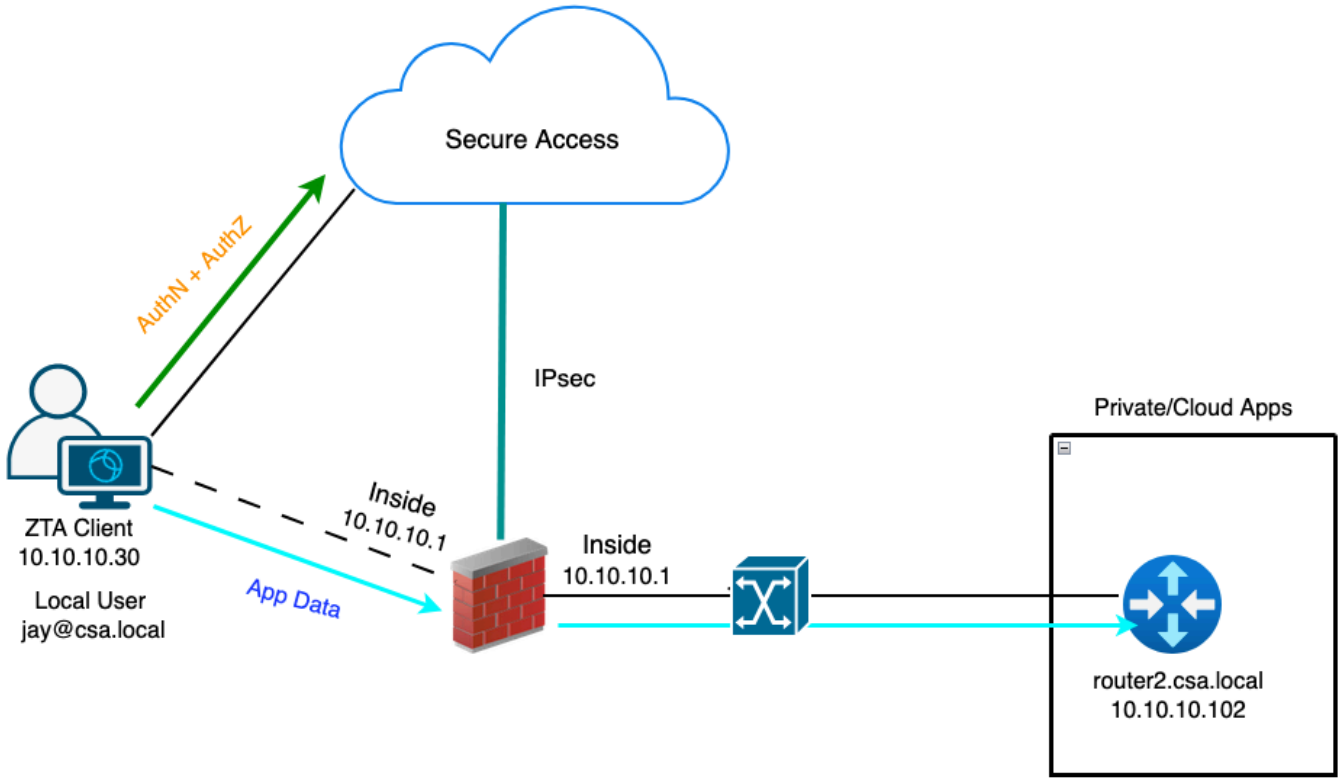
5. Verificar os eventos de conexão do FMC



Eventos de conexão do FMC

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.

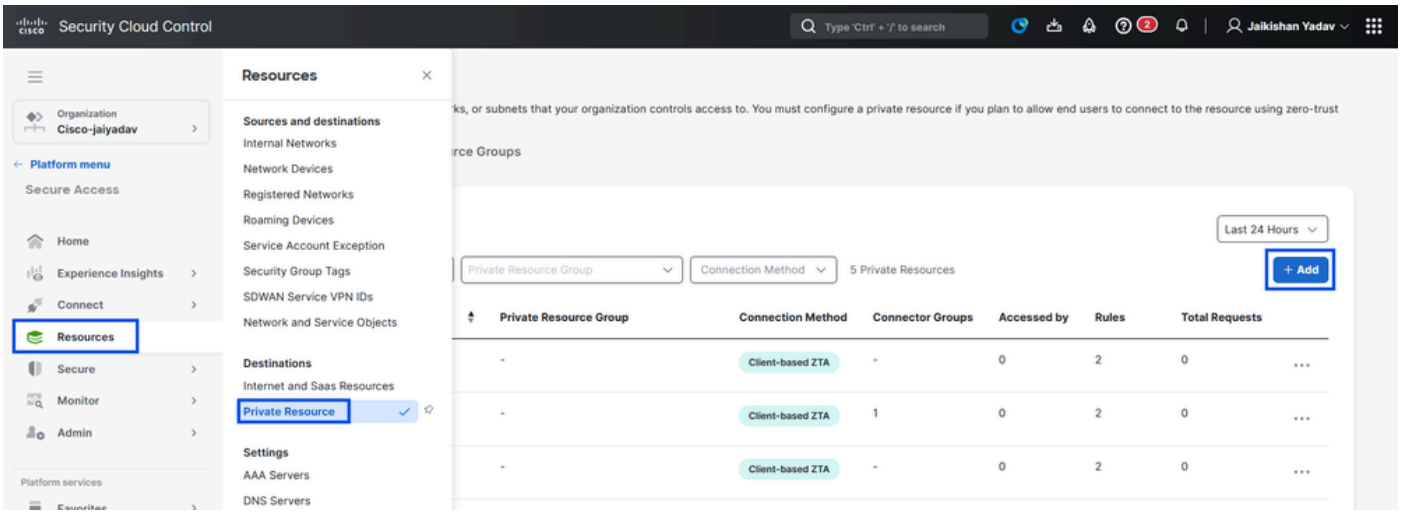


ZTA universal - Topologia de caso de teste

Etapa 1 - Definir um recurso privado no acesso seguro

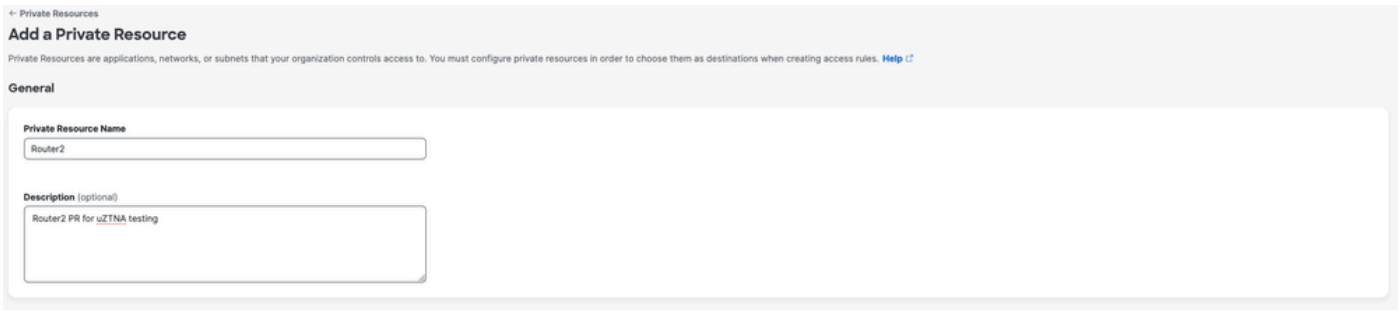
Configurar um recurso privado para ser acessível por meio do dispositivo registrado ZTA (Zero Trust Access) com aplicação de nuvem

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



Acesso seguro - Configuração de recursos privados

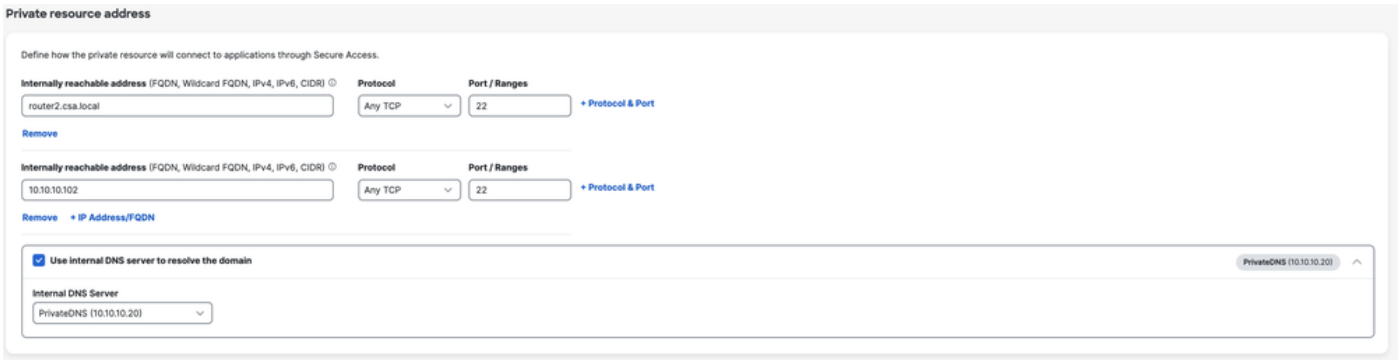
2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do recurso.



Acesso seguro - Configuração de recursos privados

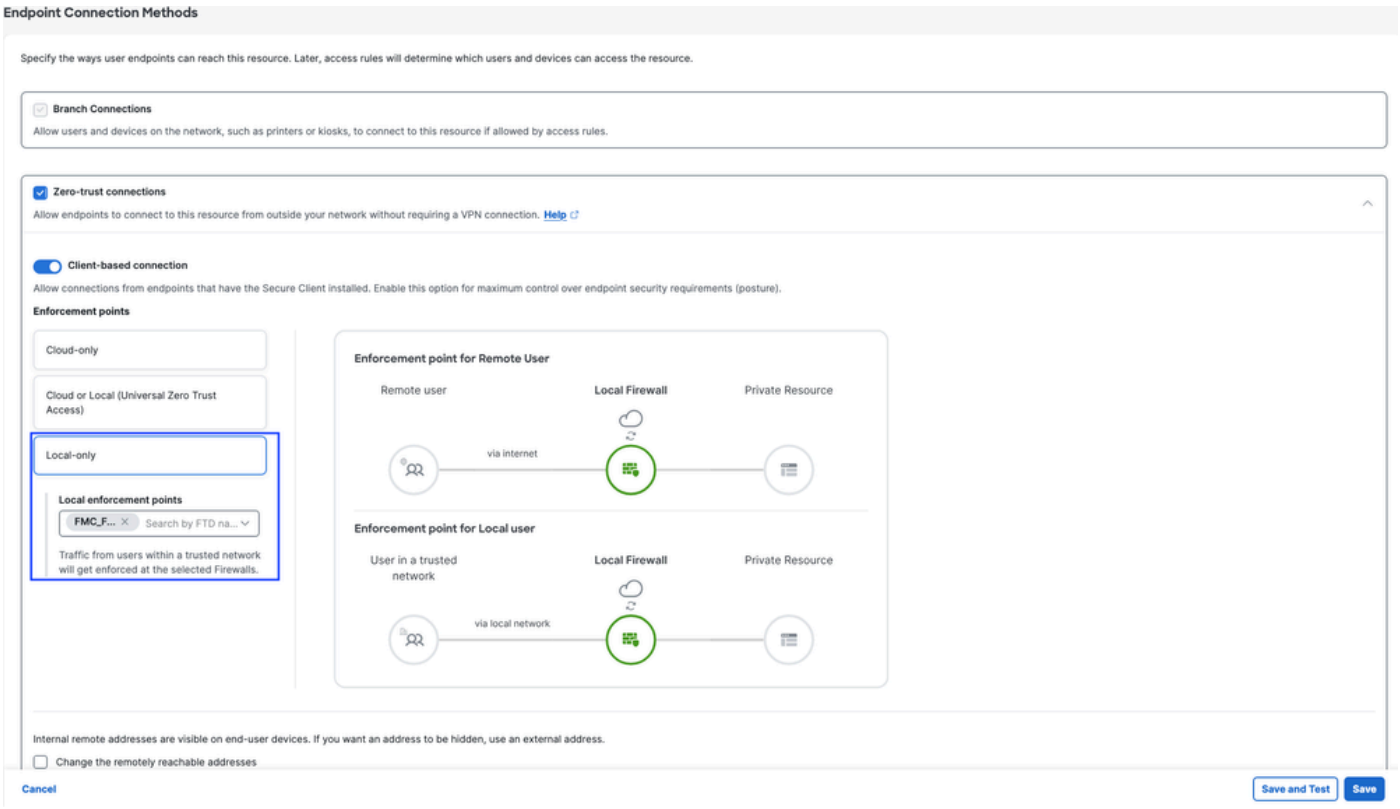
3. Informe o FQDN do recurso privado que deseja acessar. Também podemos definir o endereço IP do recurso privado . Para obter mais informações, consulte Adicionar um recurso privado

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



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

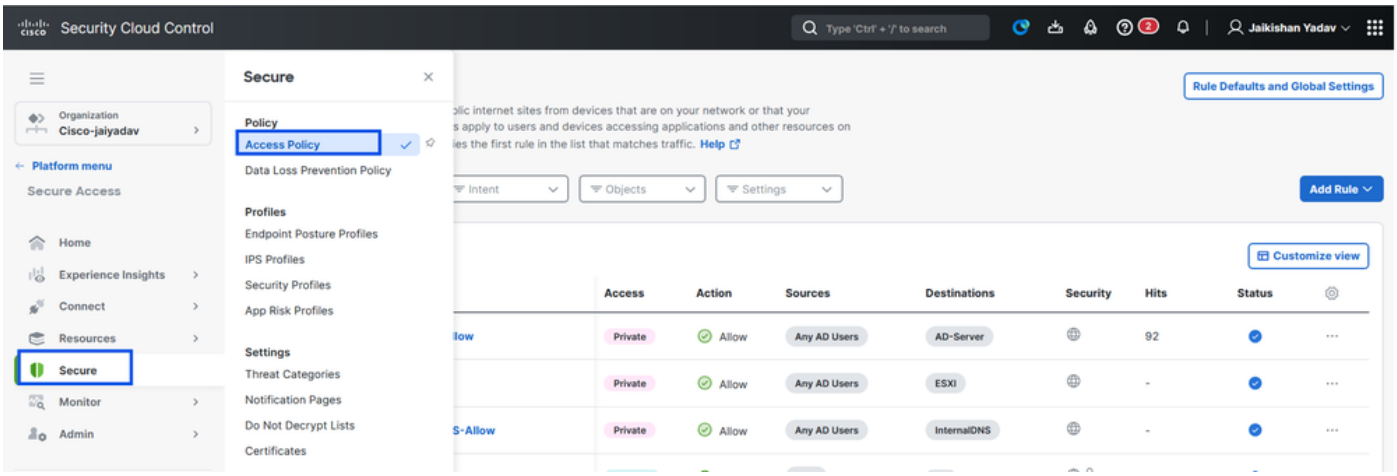
---

7. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

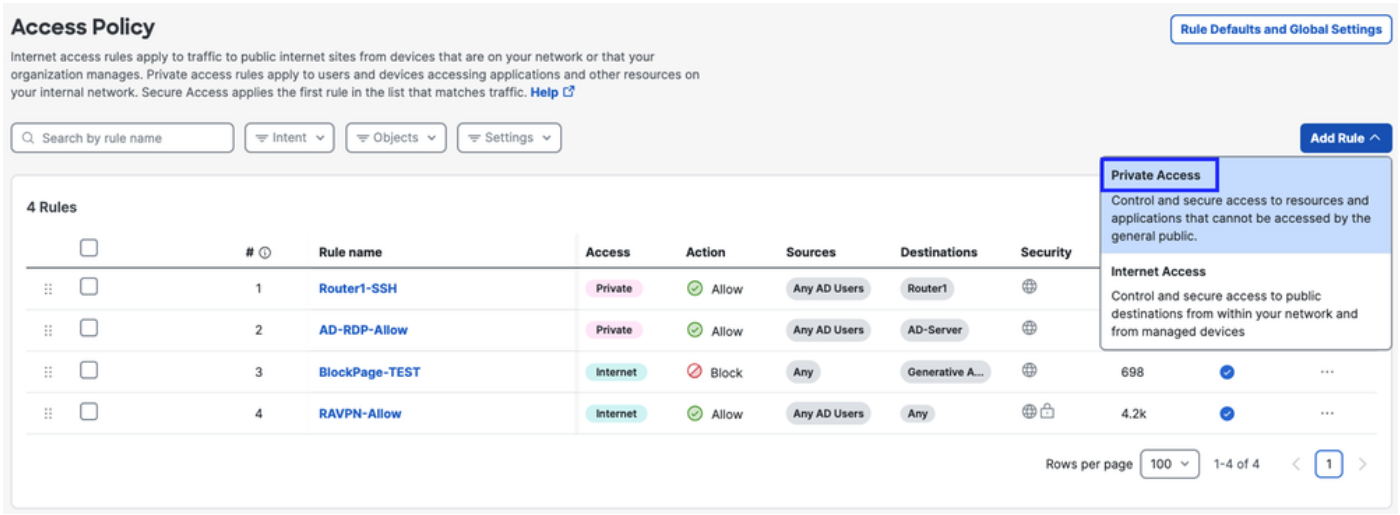
Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA . Para obter mais informações, consulte Regra de acesso privado

1. Navegue até Proteger > Política de acesso



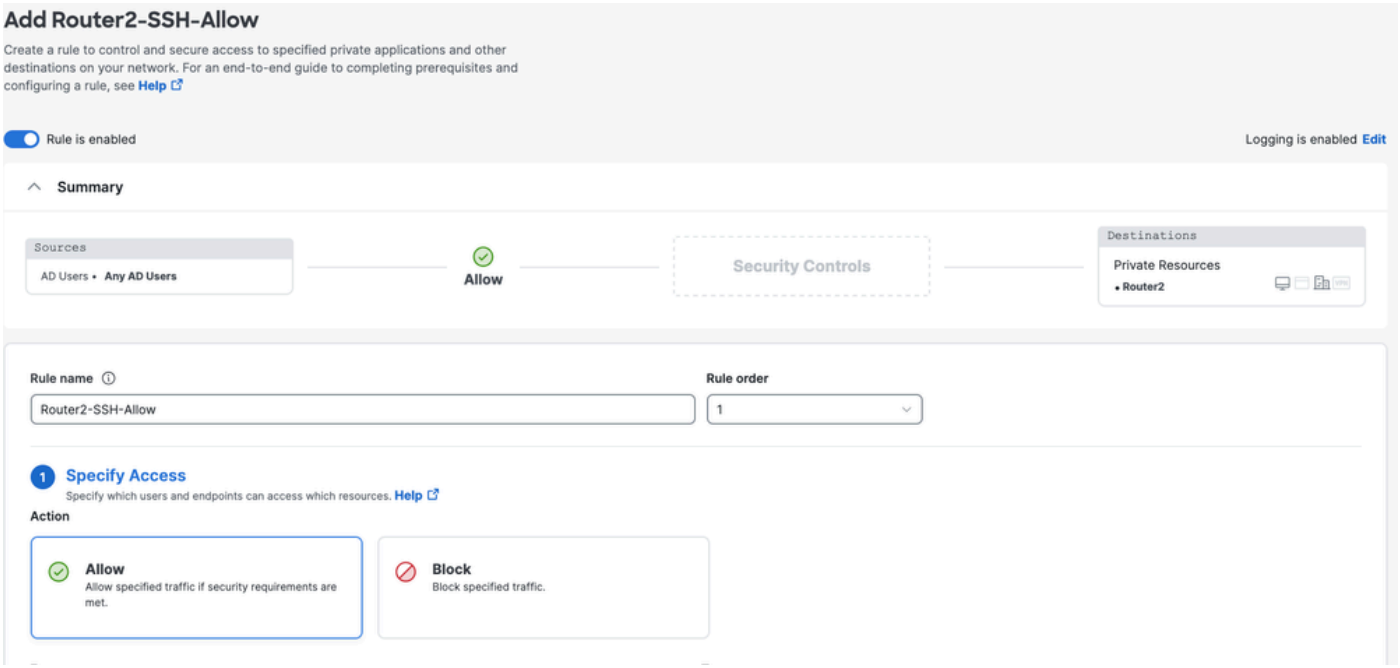
Acesso seguro - Configuração da política de acesso

2. Clique em Adicionar Regra e escolha Acesso Particular.
   Na parte superior da regra há um resumo que descreve os componentes configurados da regra.



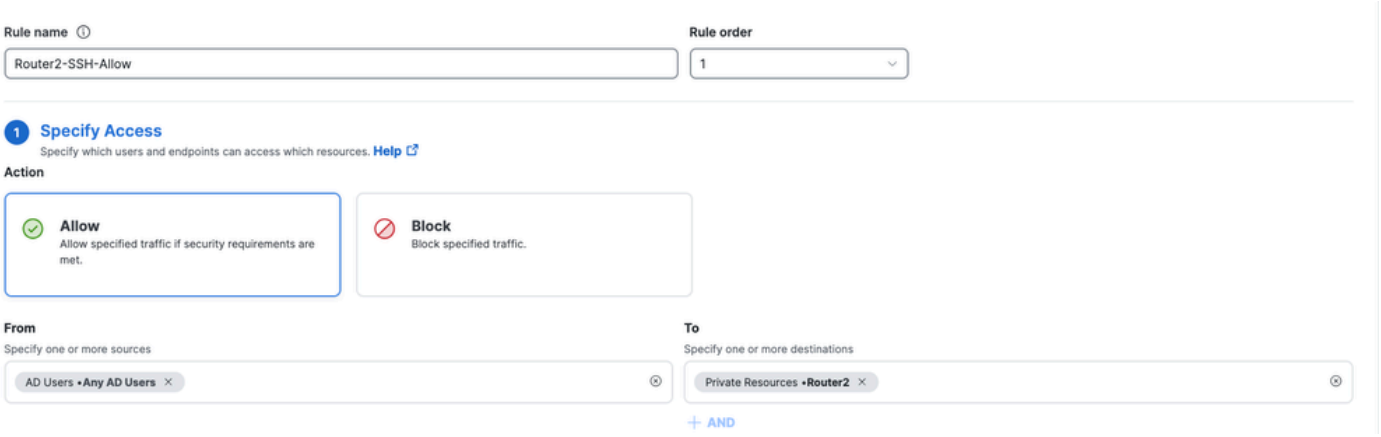
Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra



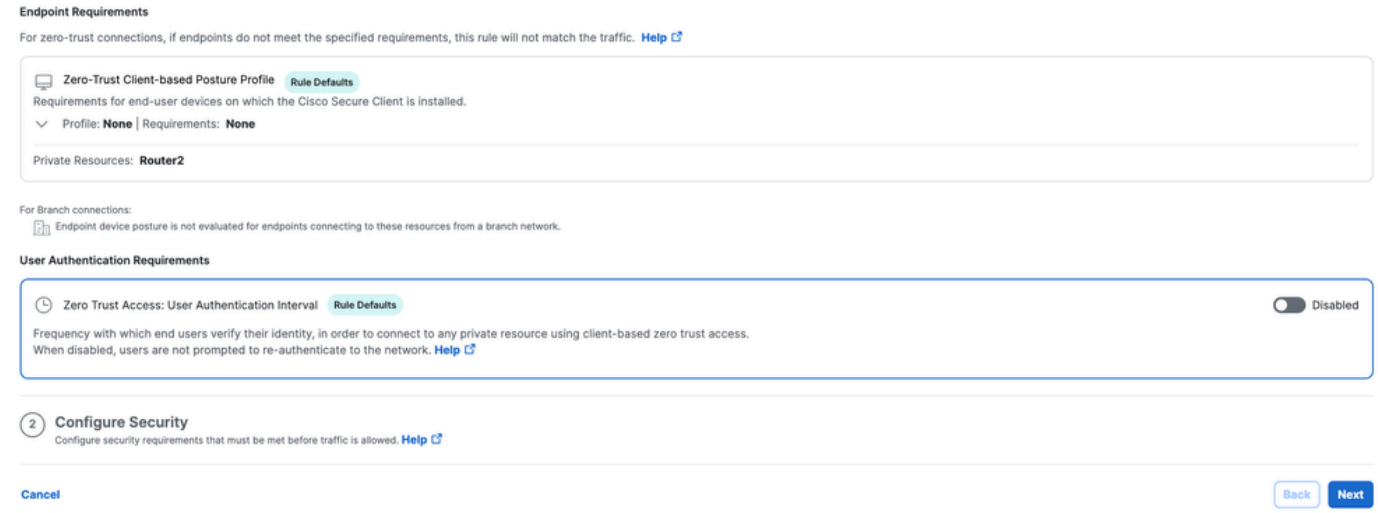
Acesso seguro - Configuração da política de acesso

4. Selecione a ação da regra e selecione origem e destino



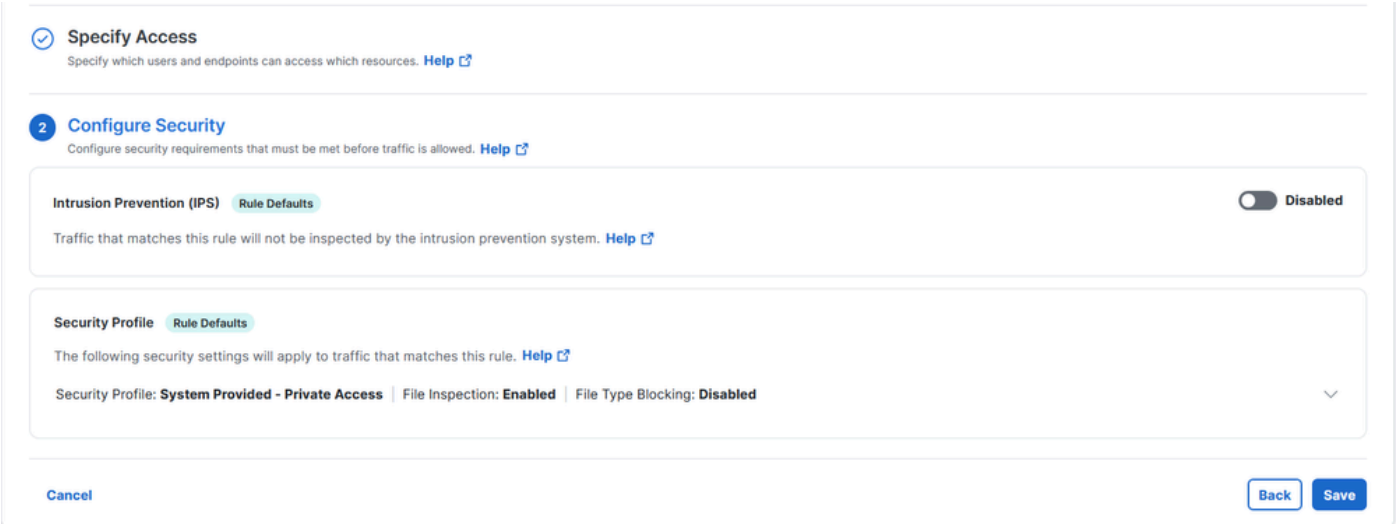
Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint



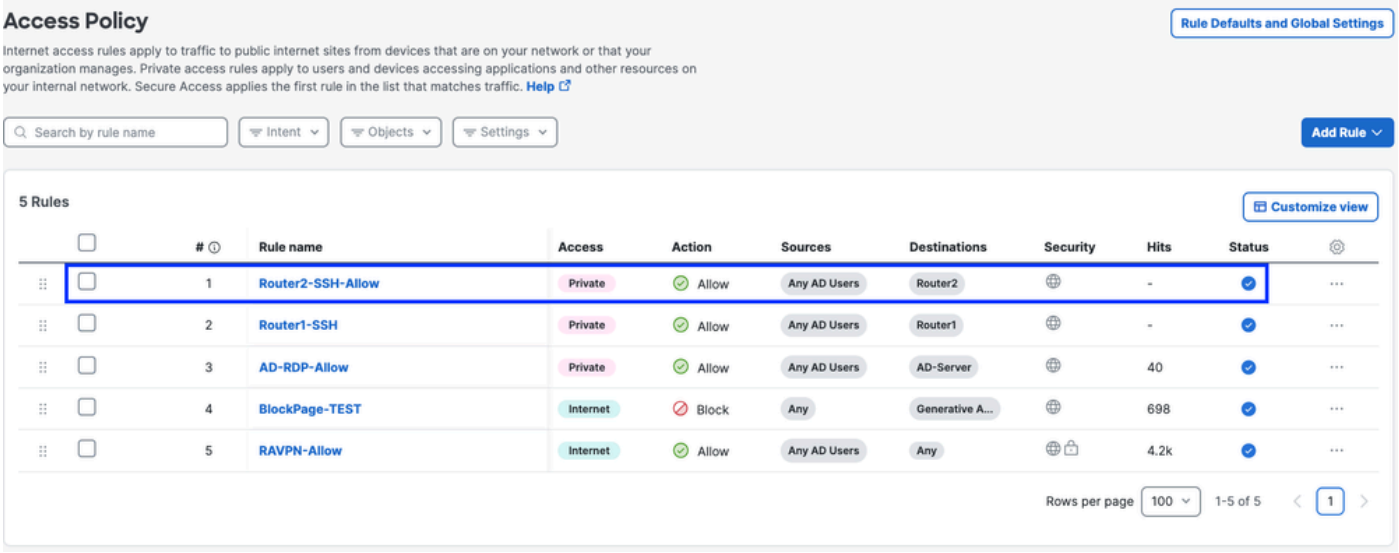
Acesso seguro - Configuração da política de acesso

6. Configurar segurança



Acesso seguro - Configuração da política de acesso

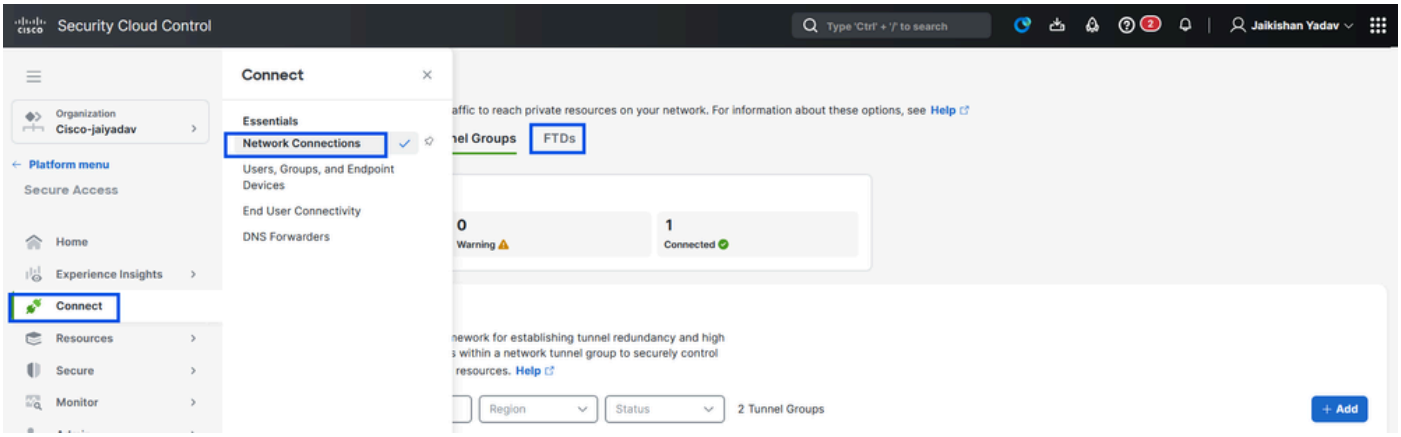
7. Clique em Salvar



Acesso seguro - Configuração da política de acesso

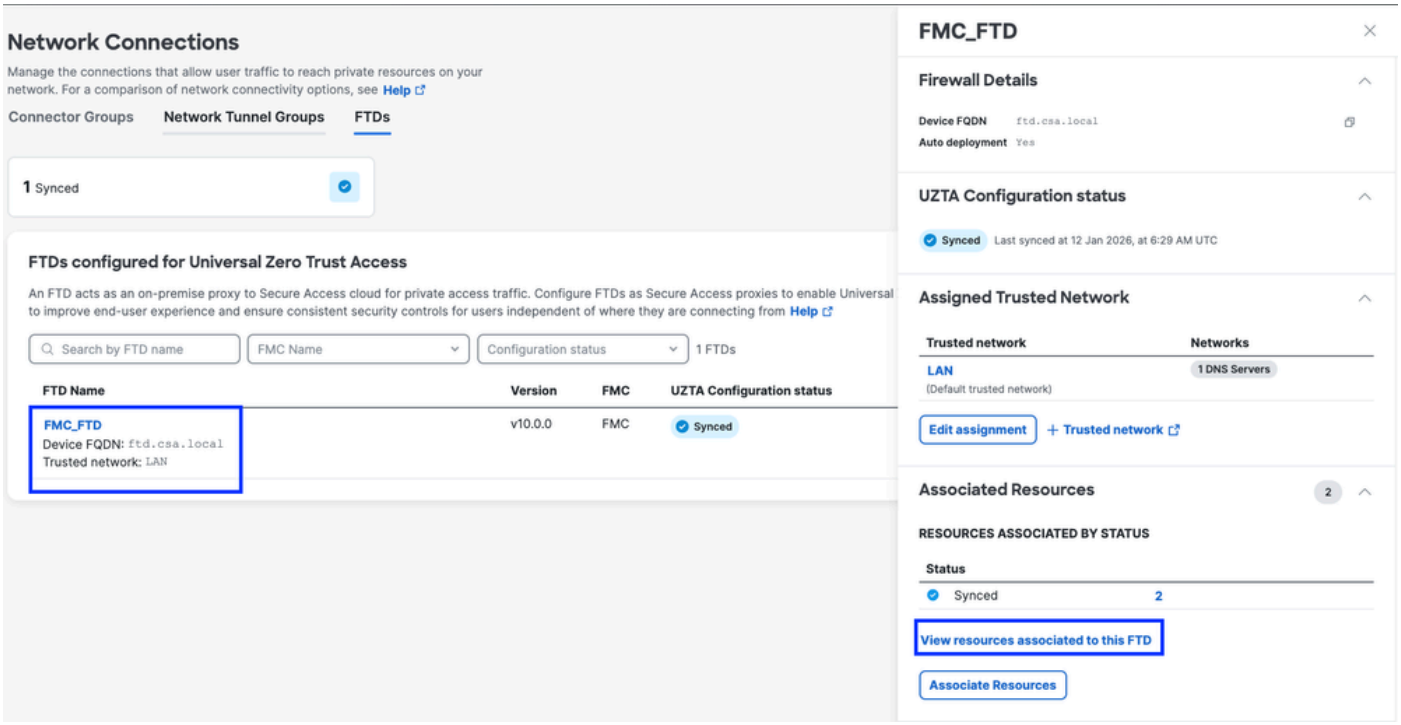
Etapa 3 - Verificar a associação de PR no FTD

1. Navegue para conectar > Conexões de Rede > FTDs

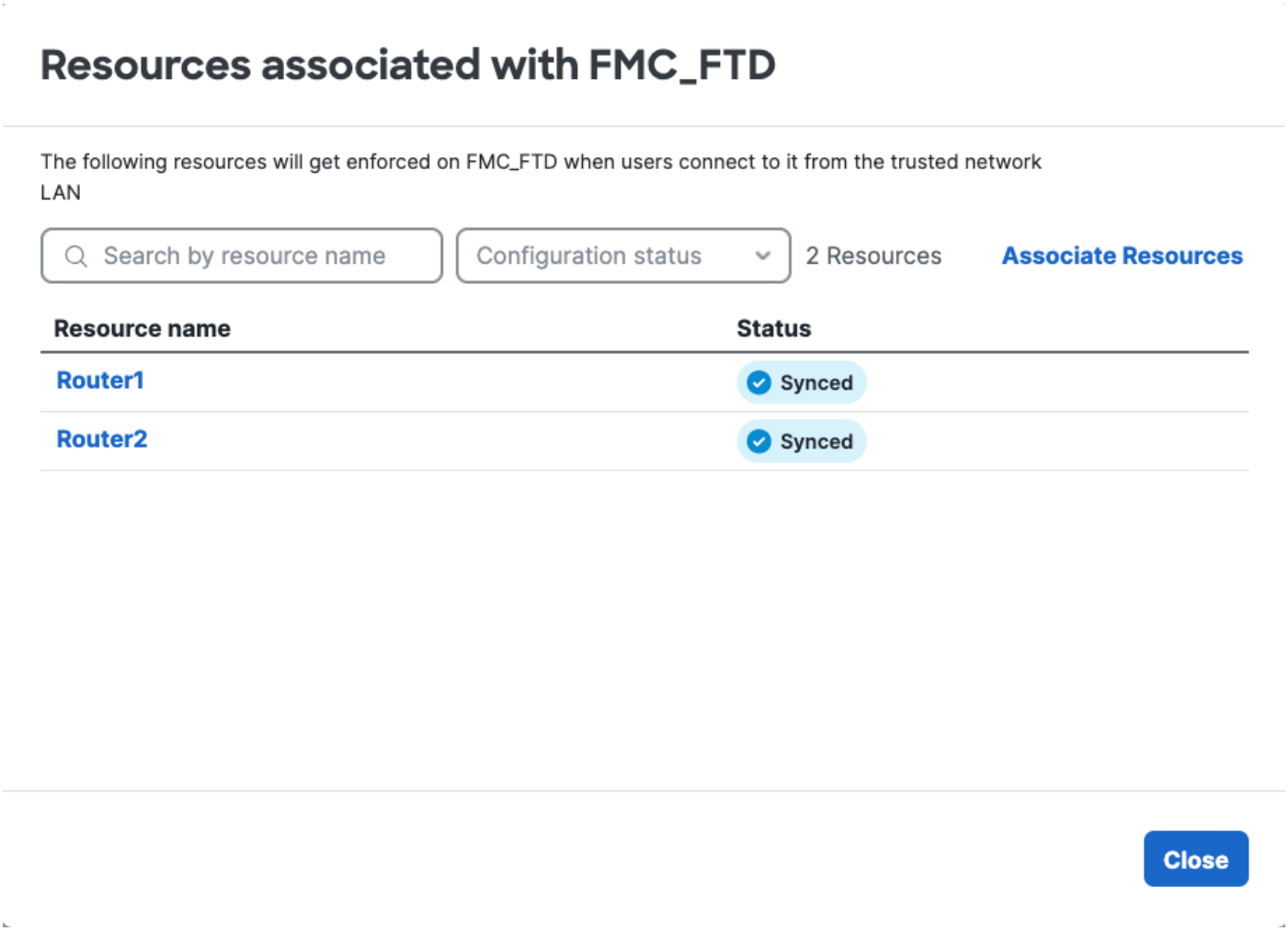


Acesso seguro - Verificação de PR

2. Clique no FTD > Exibir recursos associados a este FTD

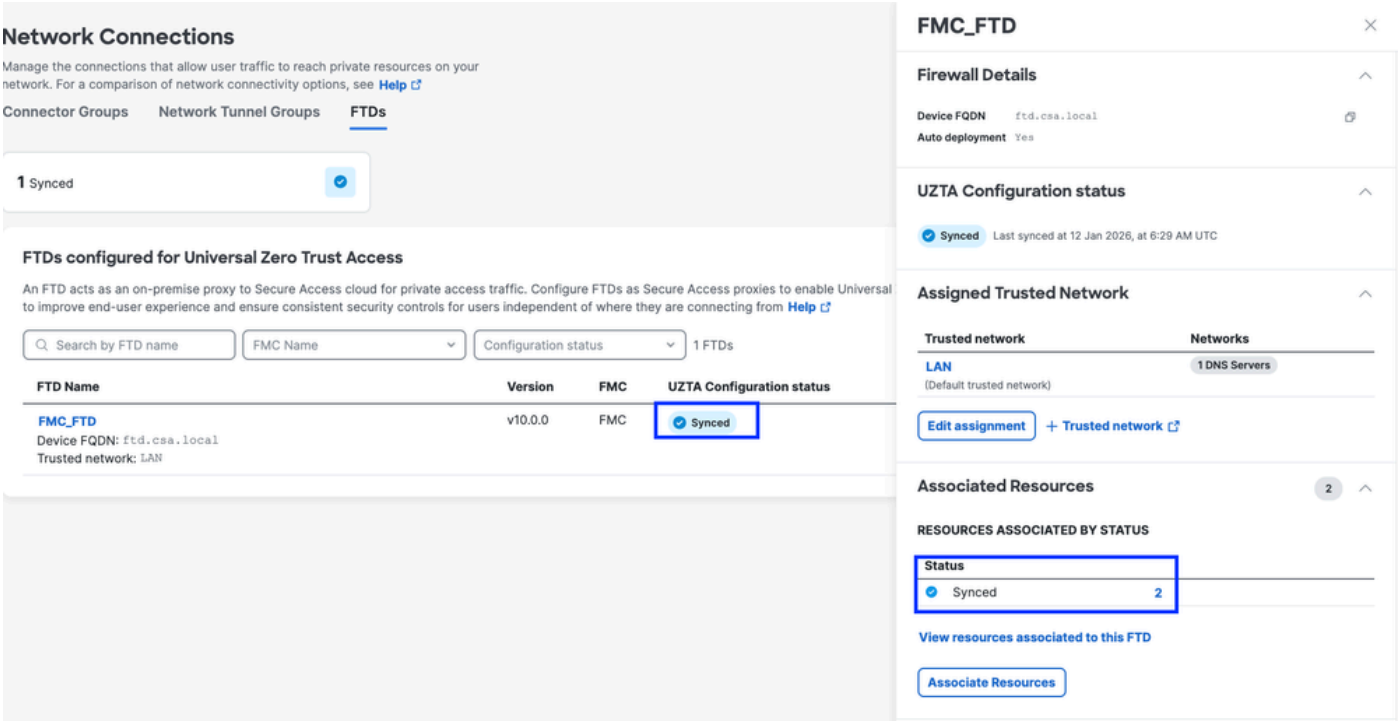


Acesso seguro - Verificação de PR



3. Clique em Close

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



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

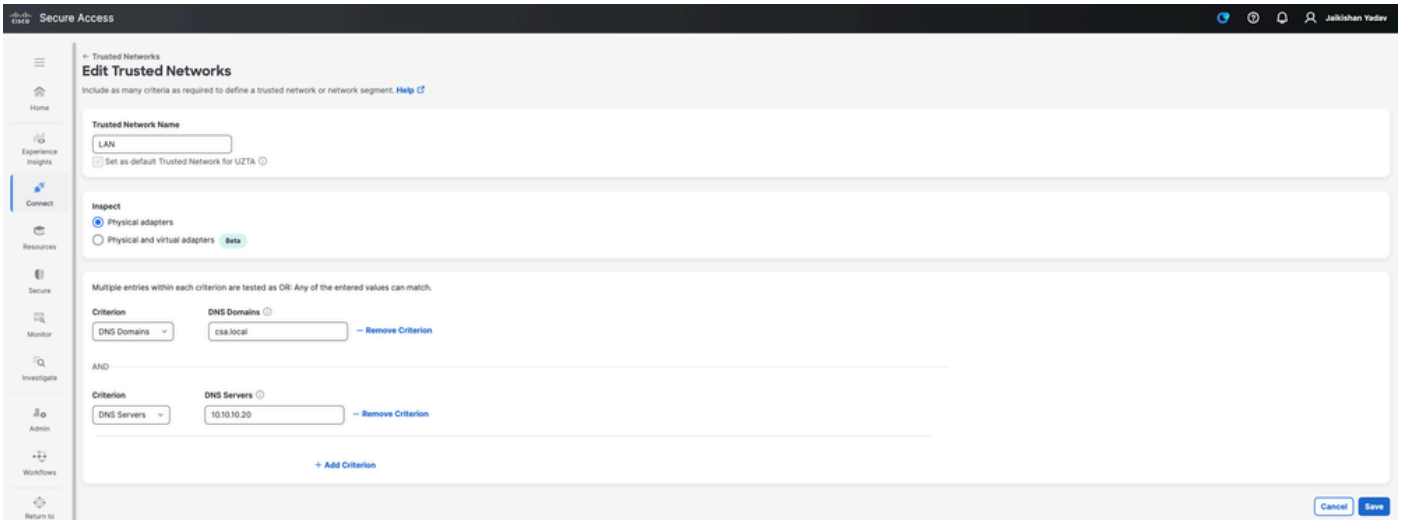
show running-config object application

```
ftd# sh run 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"

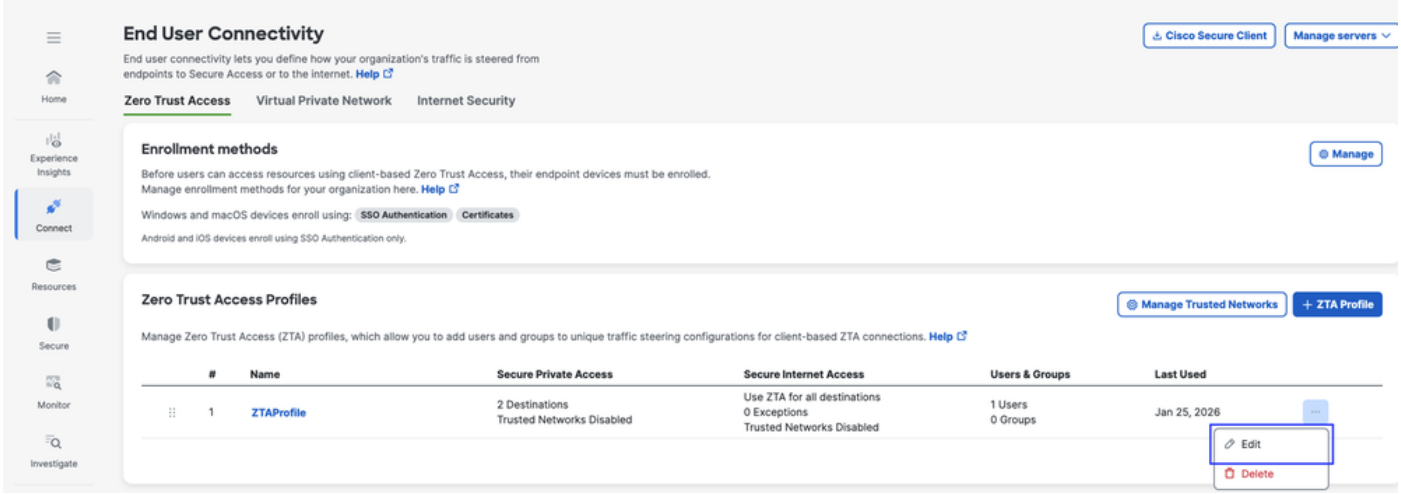
Navegue para Connect > End User Connectivity > Zero Trust Access > ZTA Settings e configure Trusted Networks



Acesso seguro - Configuração TND

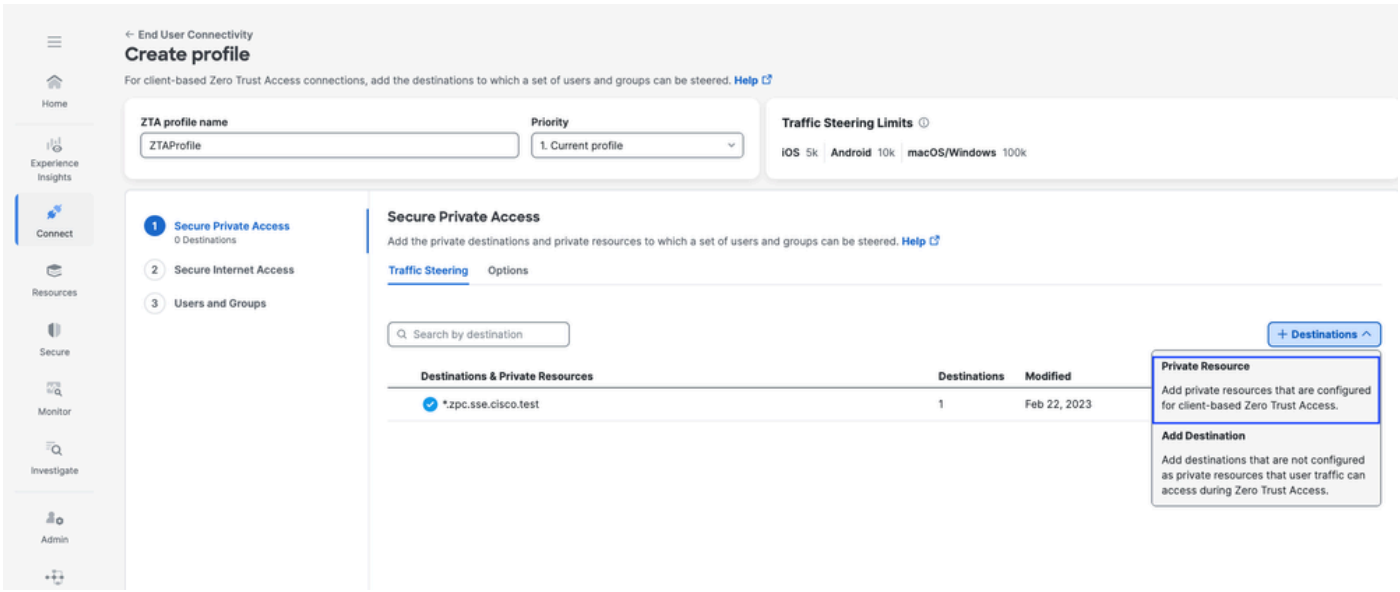
Etapa -5 Adicionar recurso privado ao perfil ZTA

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

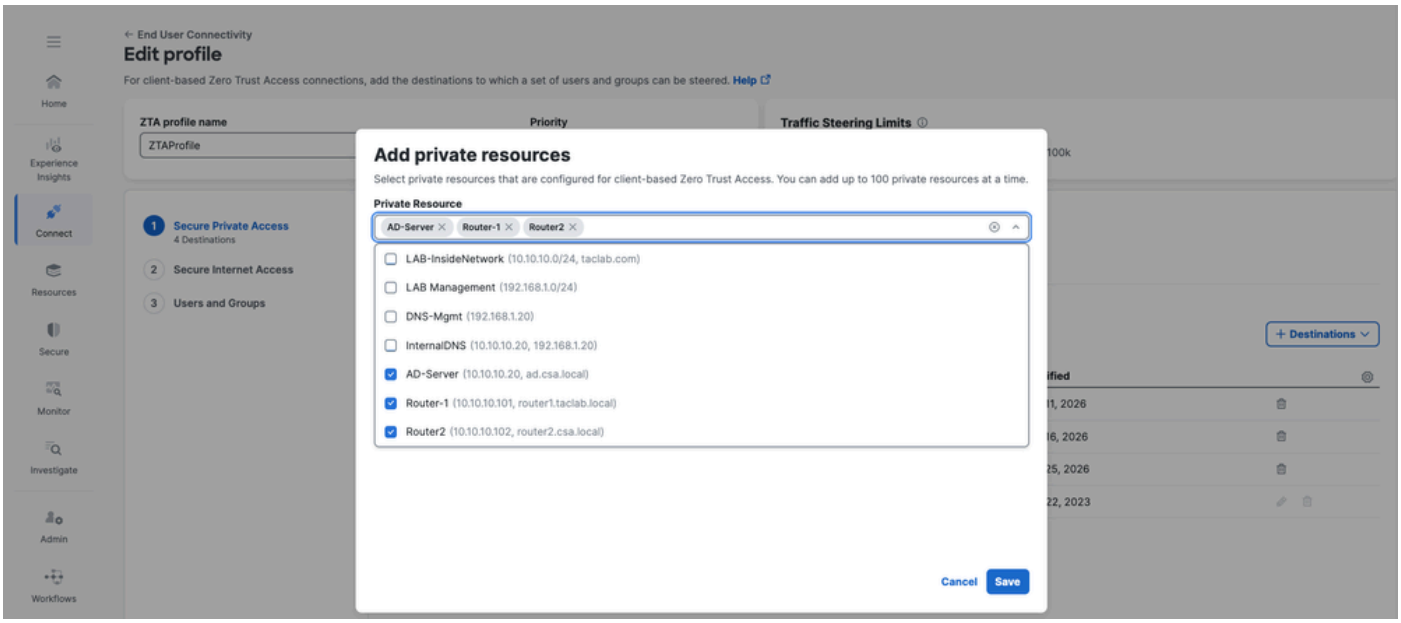


Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

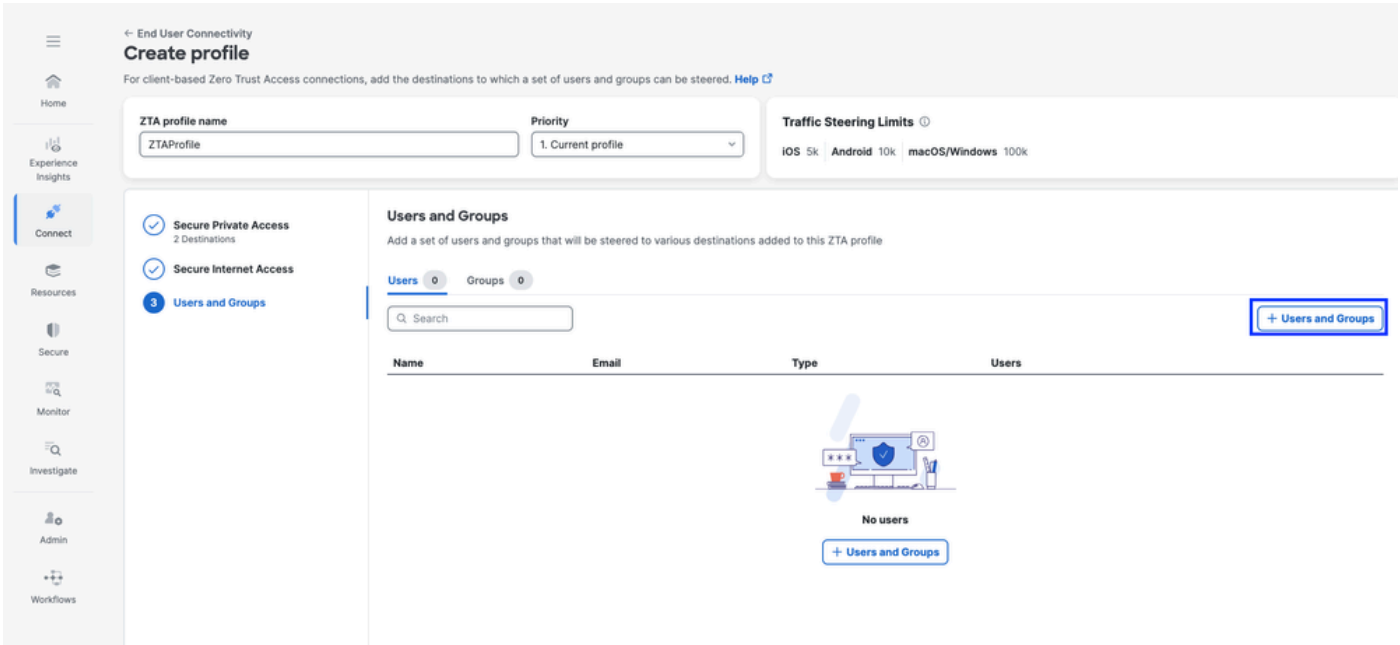


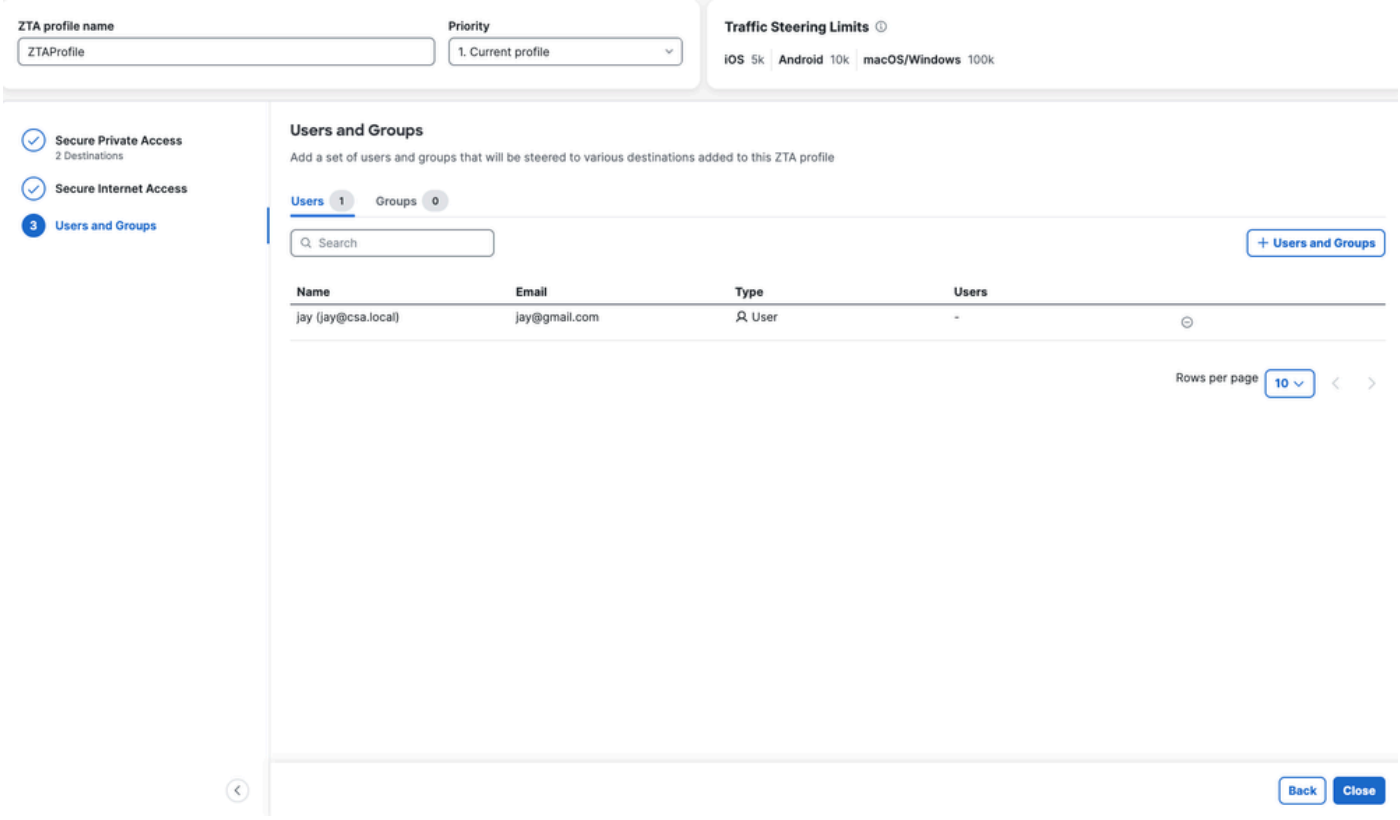
Acesso seguro - perfil ZTA



Acesso seguro - perfil ZTA

3. Adicionar usuários e grupos

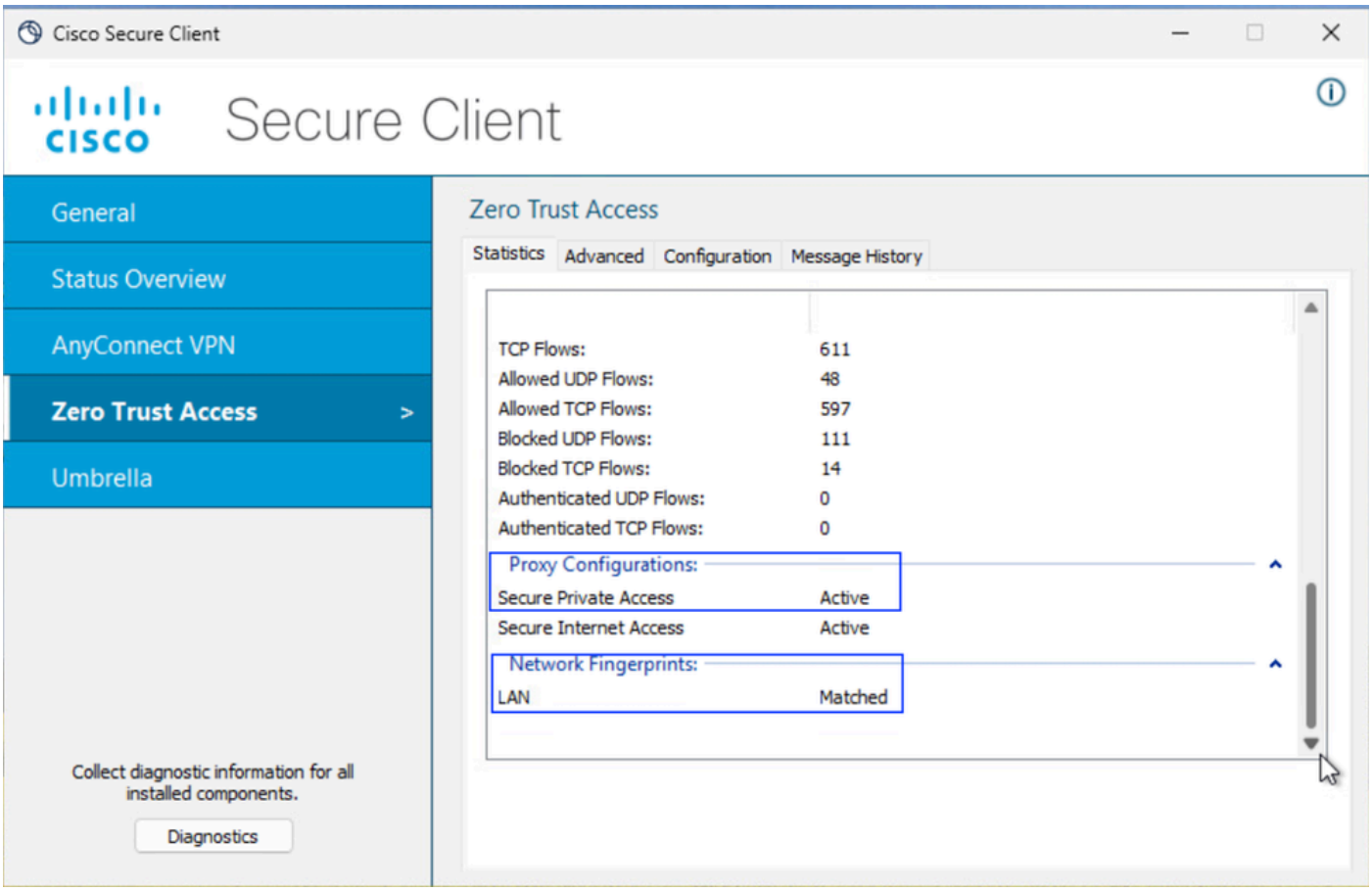




Acesso seguro - perfil ZTA

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

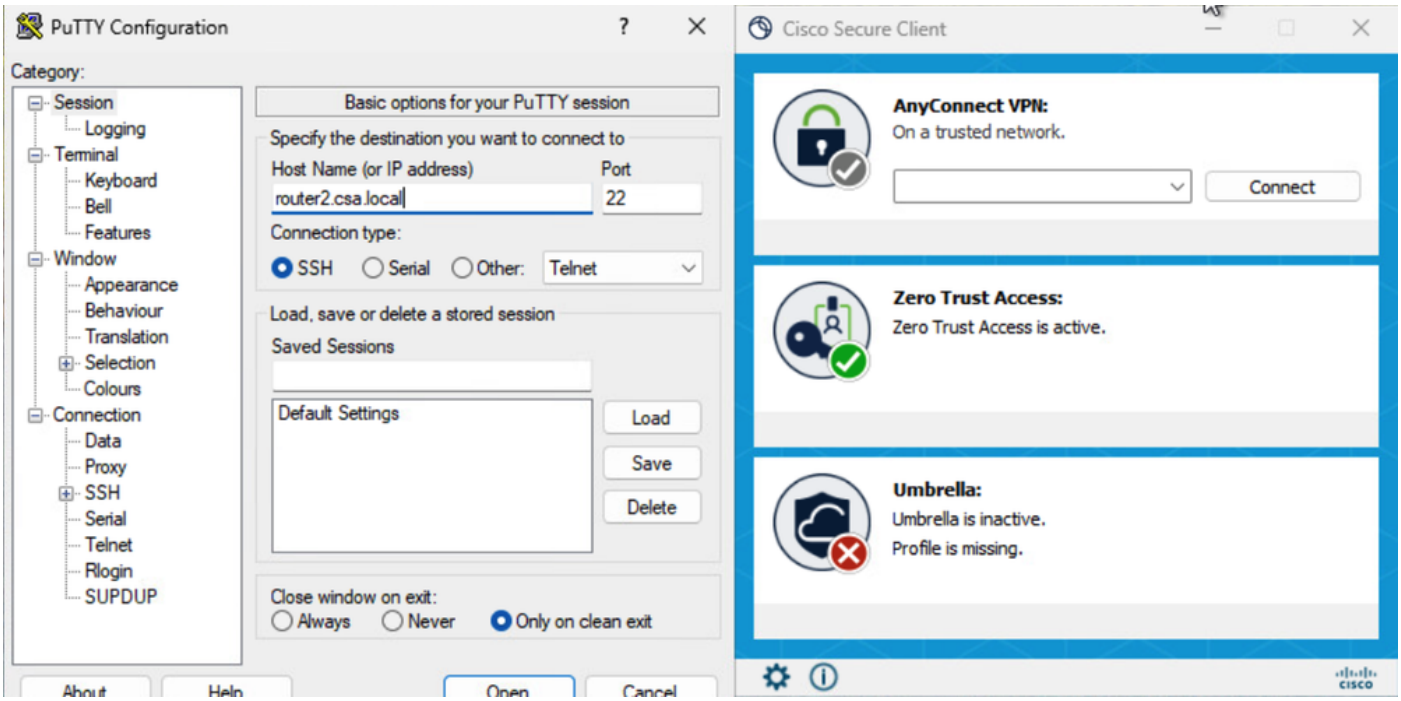
3. Verificar se o FTD pode acessar o recurso privado usando o FQDN

```
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#
```

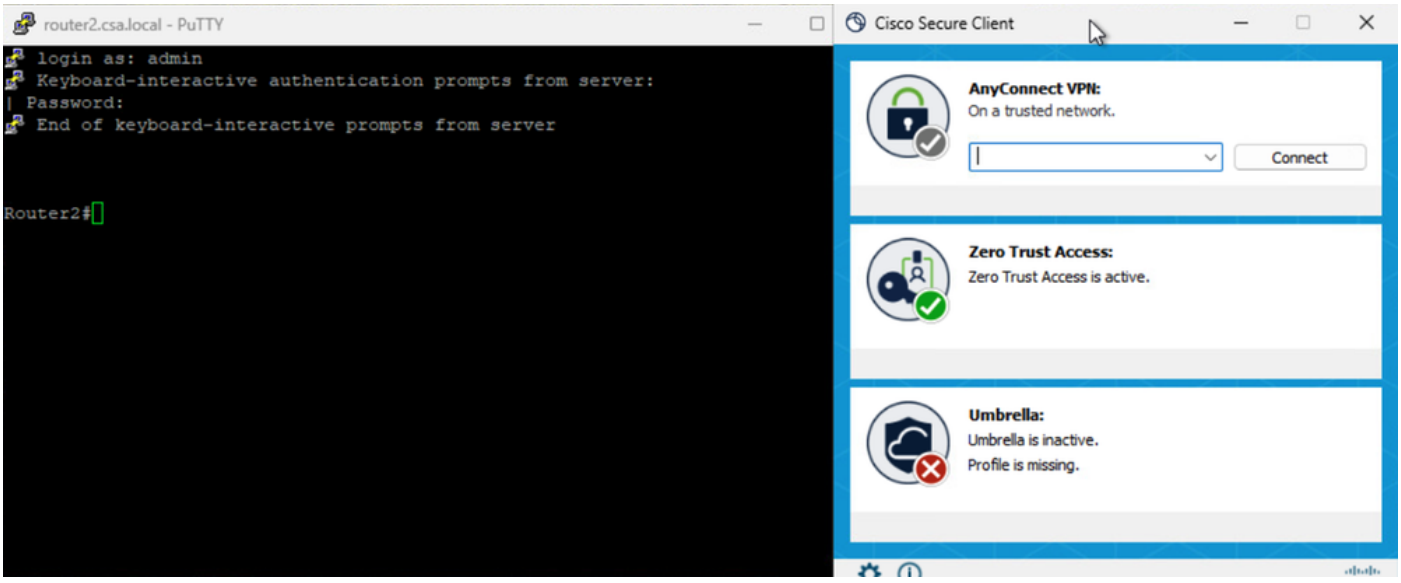
Acesso seguro - Teste de PR

4. Testar a conexão SSH com o recurso privado

Acessar a PR usando o FQDN

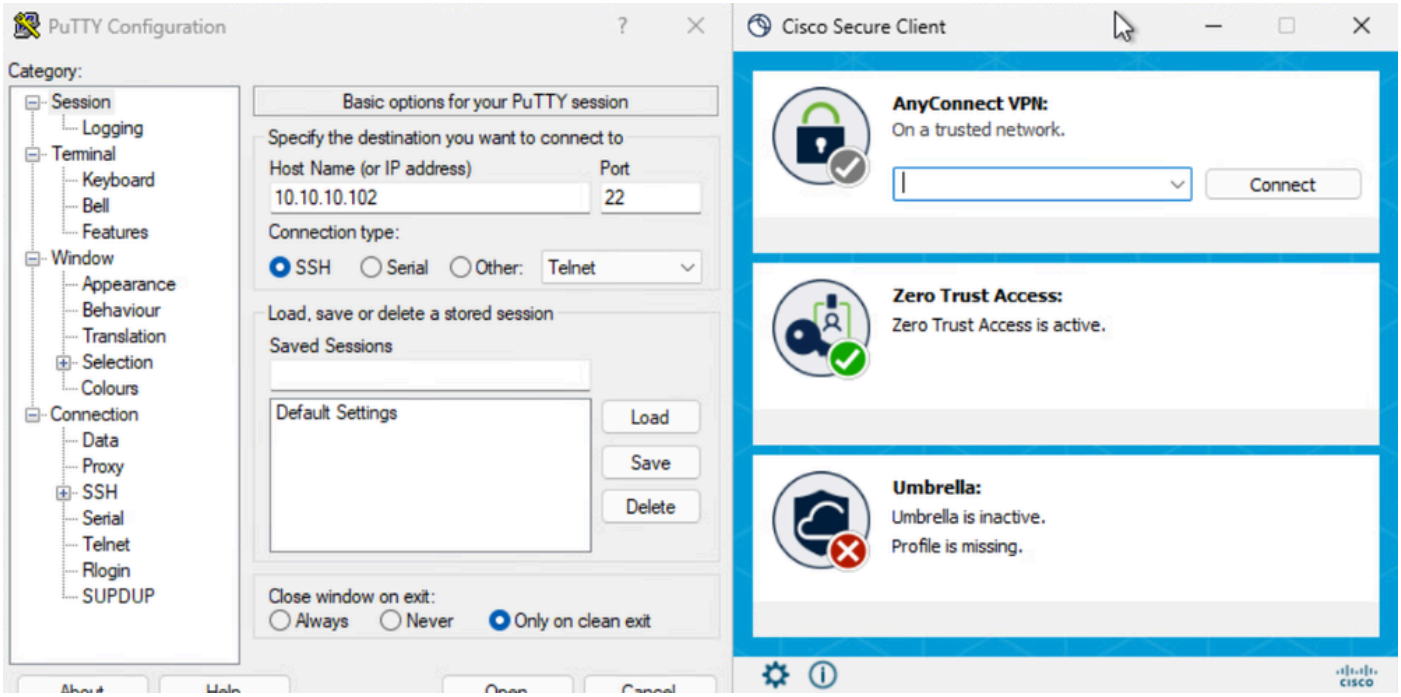


Acesso seguro - Teste de PR

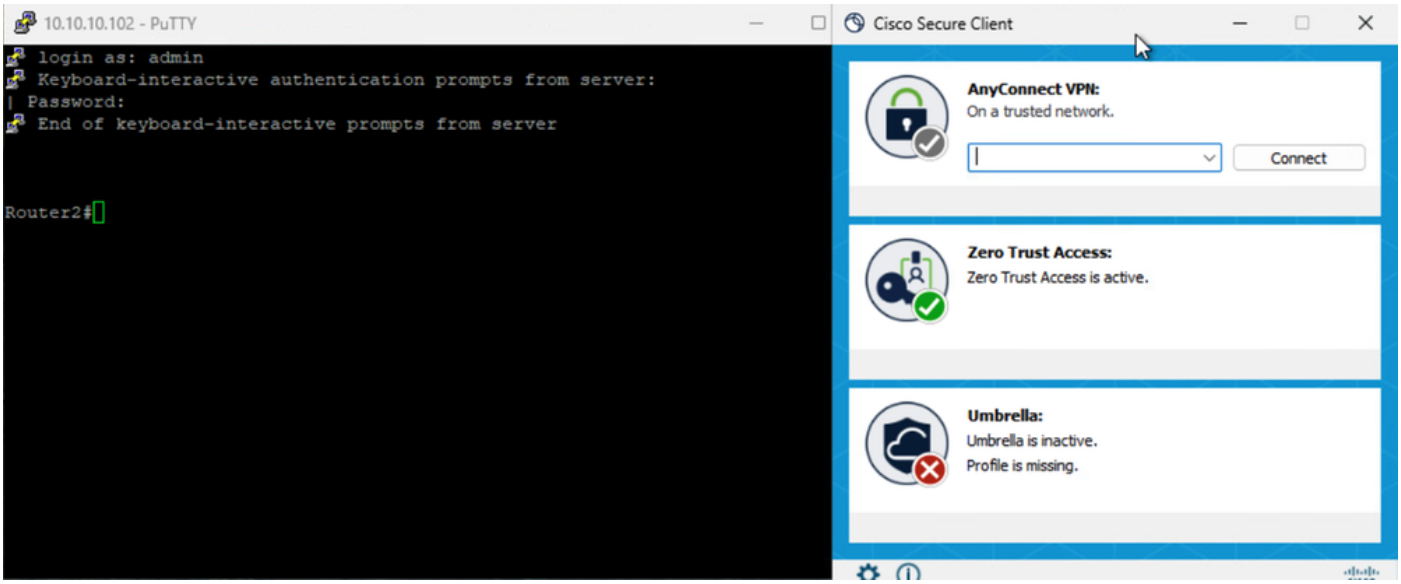


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP

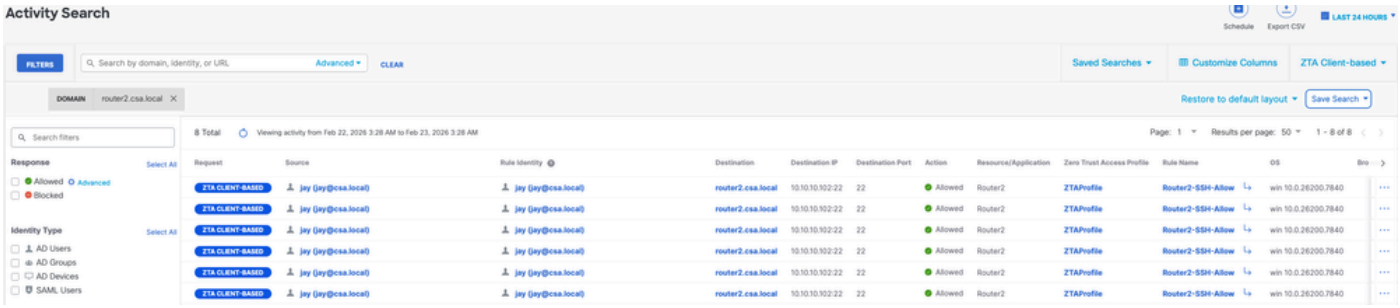


Acesso seguro - Teste de PR

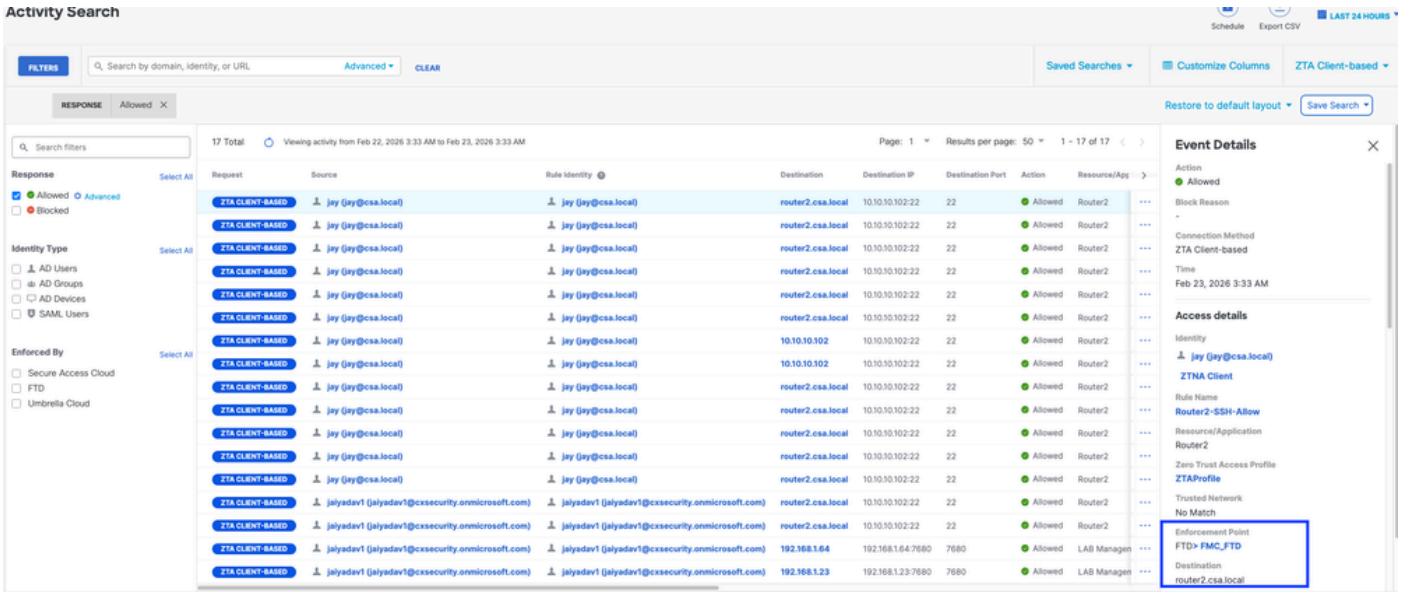


Acesso seguro - Teste de PR

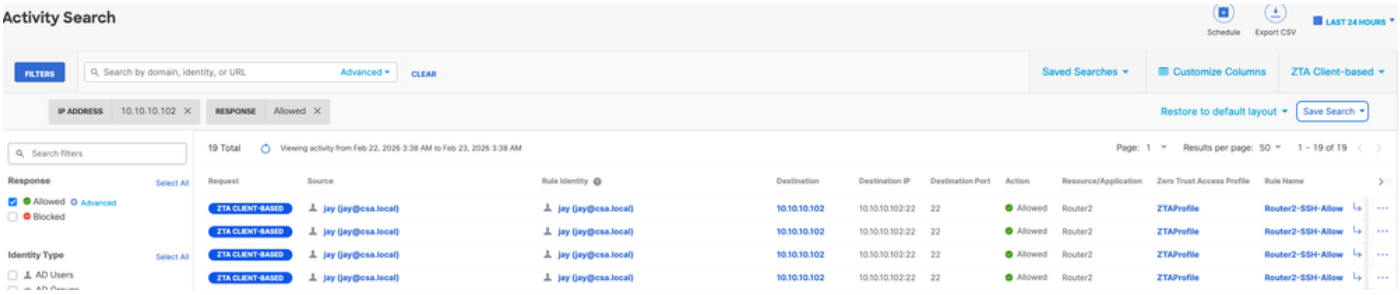
5. Verificar logs de Pesquisa de Atividade de Acesso Seguro



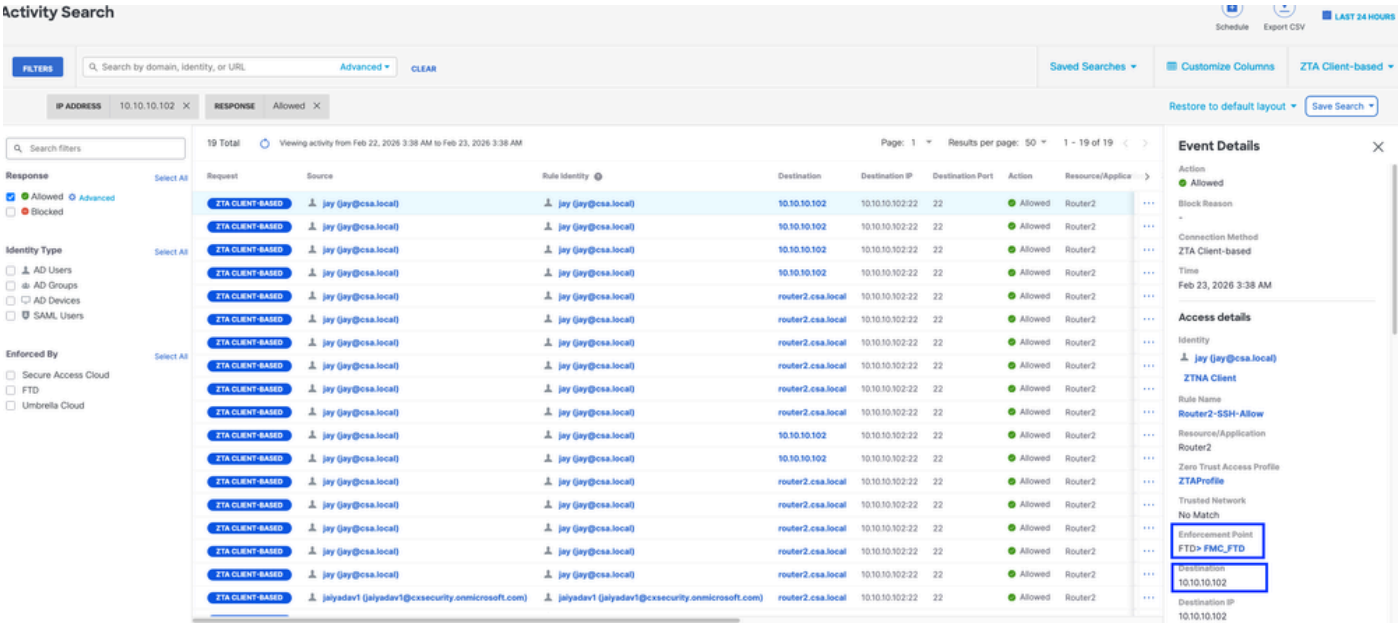
Acesso seguro - Pesquisa de atividades



Acesso seguro - Pesquisa de atividades

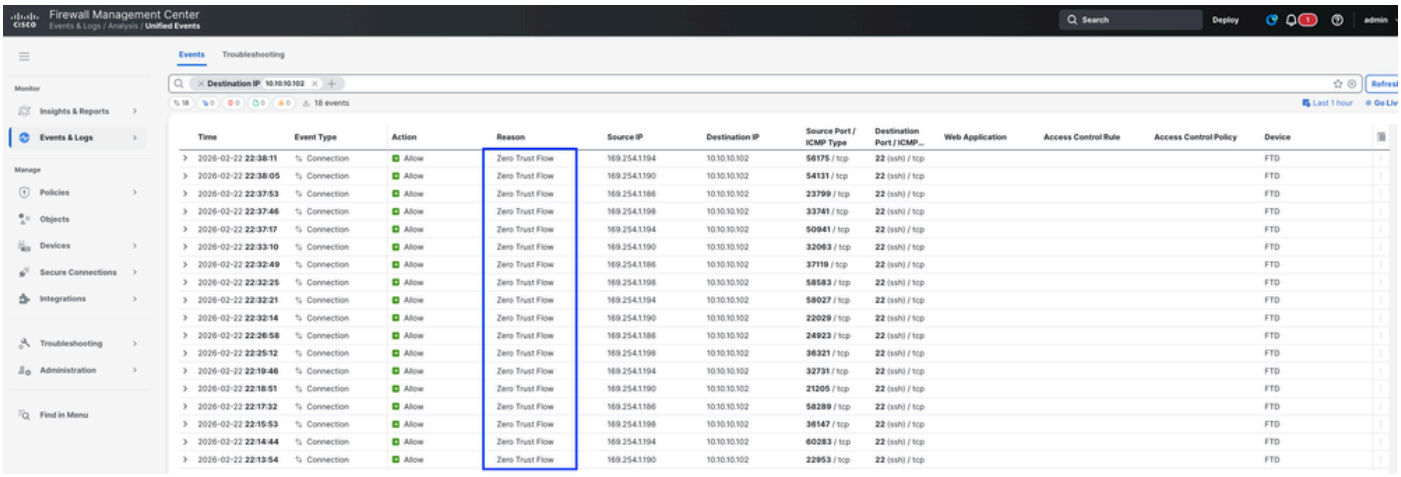


Acesso seguro - Pesquisa de atividades



Acesso seguro - Pesquisa de atividades

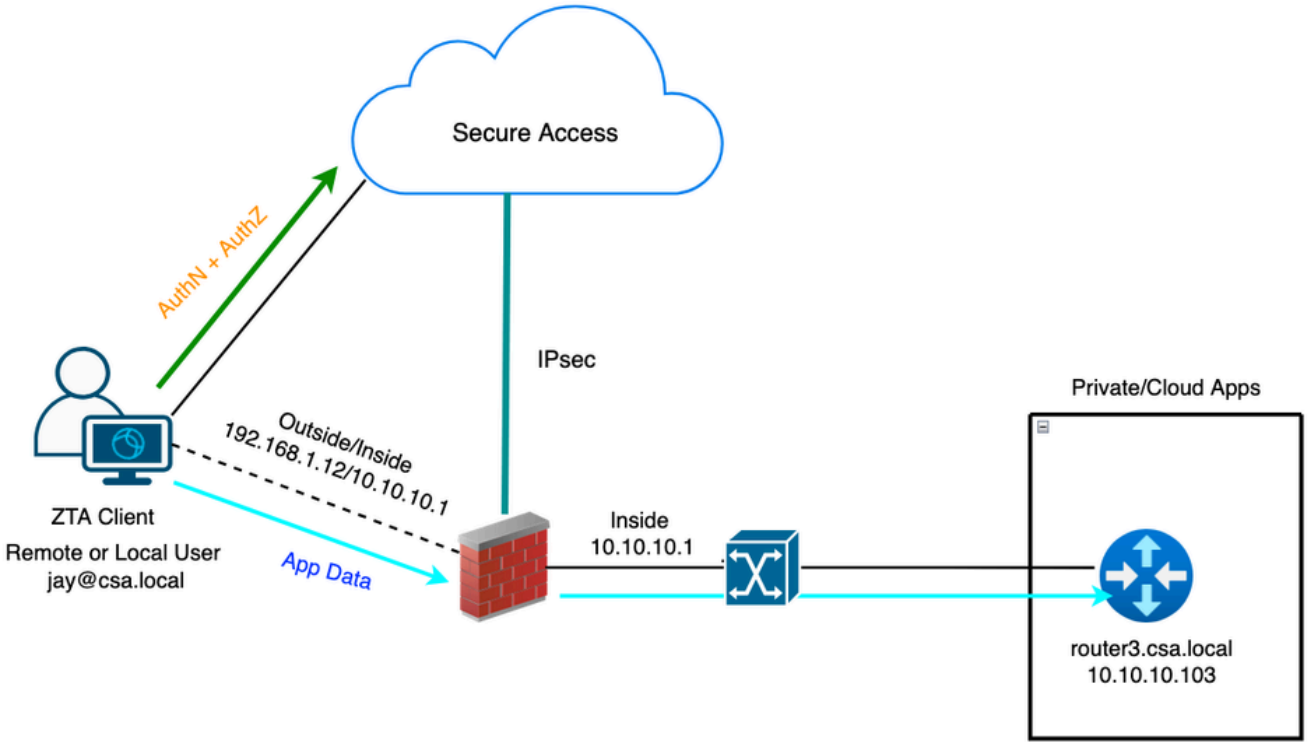
6. Verificar os eventos de conexão do FMC



Eventos de conexão do FMC

Caso de teste 4 - Usuário local e remoto - Aplicação local ou em nuvem com TND

Nesse caso, o tipo de imposição depende do local do usuário. Se o usuário for Local ou estiver atrás de uma zona FTD confiável (interna, DMZ, etc.), a imposição será Local (Caso de teste 3). Da mesma forma, se o usuário for remoto, a aplicação será na nuvem (Teste de Caso 1). A localização do usuário será decidida com base na impressão digital de rede ou na configuração TND, se a impressão digital de rede corresponder, o local do usuário será Local e, se não for uma correspondência, o local do usuário será considerado Remoto .

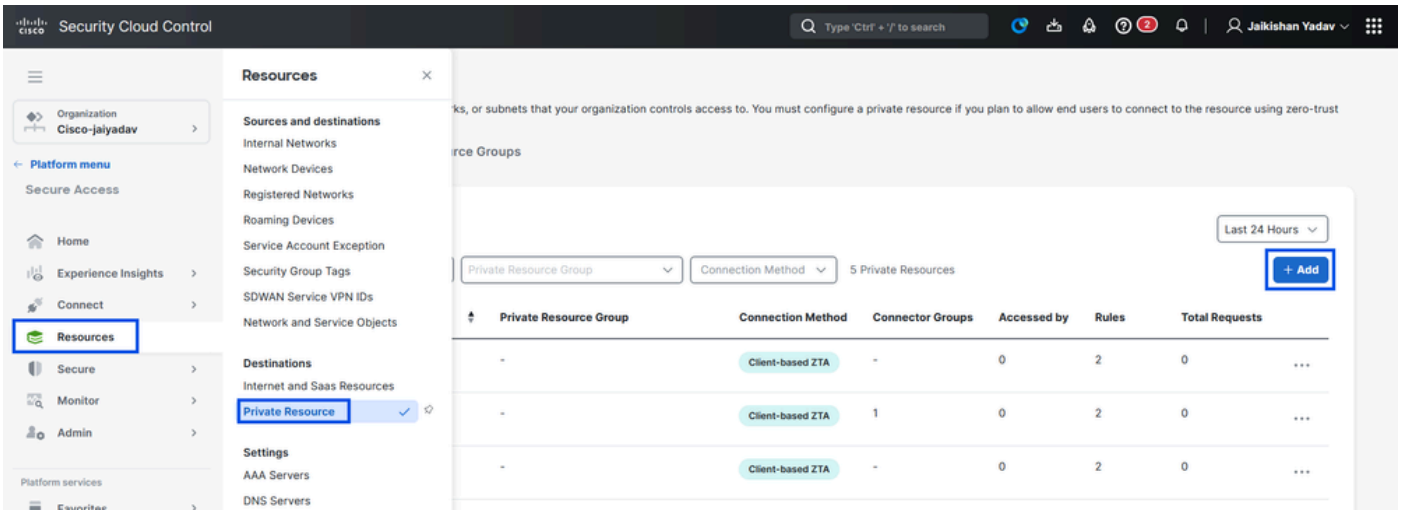


ZTA universal - Topologia de caso de teste

Etapa 1 - Definir um recurso privado no acesso seguro

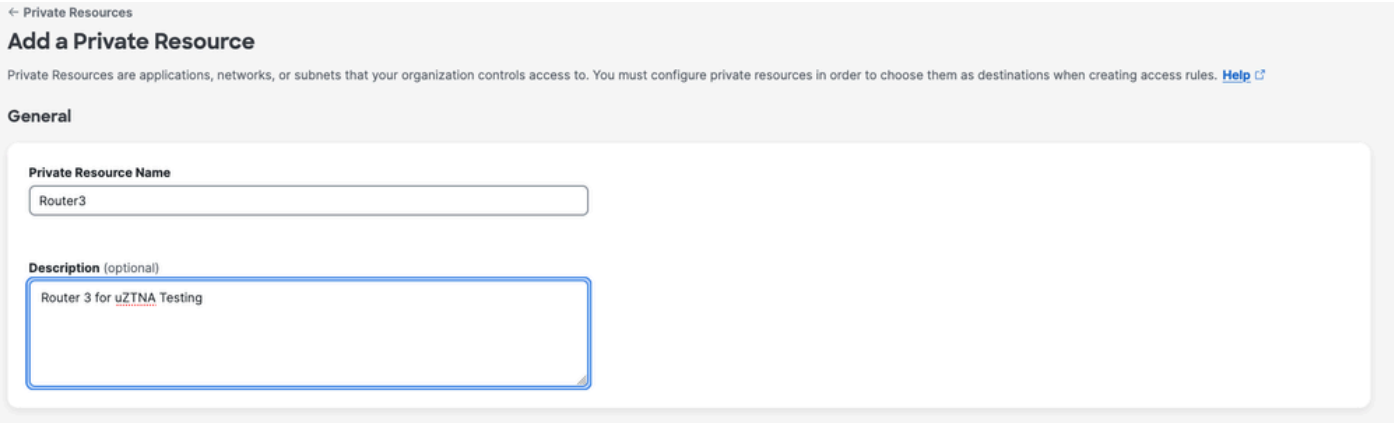
Configurar um recurso privado para ser acessível por meio do dispositivo registrado ZTA (Zero Trust Access) com aplicação de nuvem

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



Acesso seguro - Configuração de recursos privados

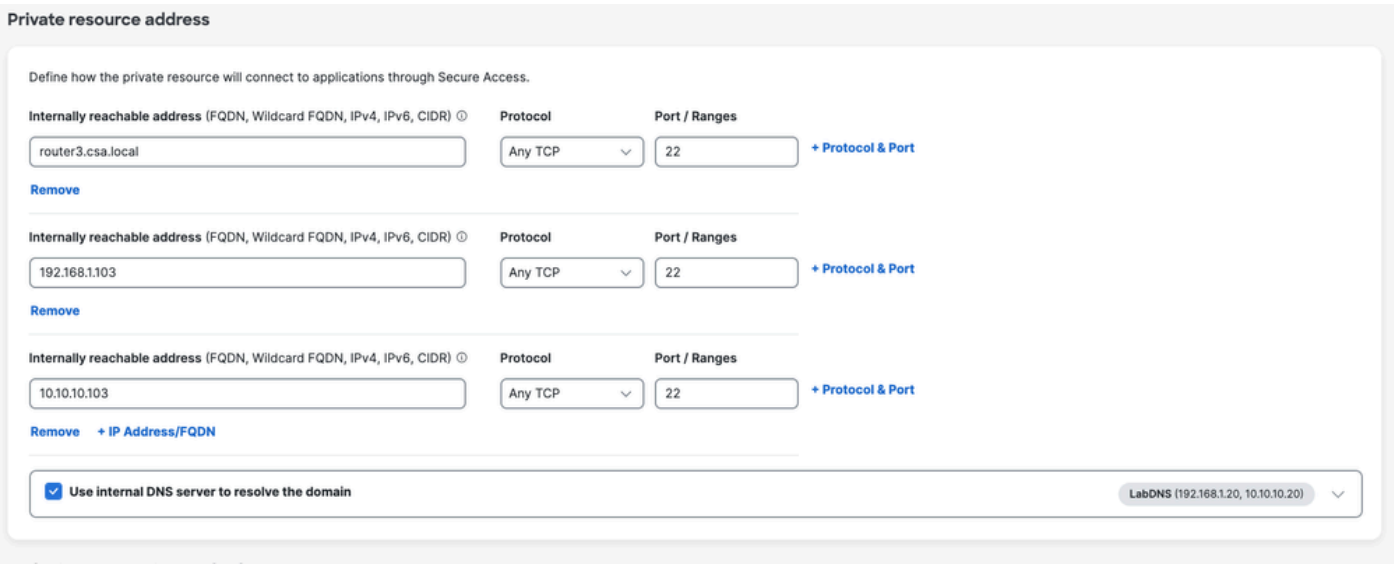
2. Para Nome do Recurso Particular, informe um nome significativo para o recurso. Para Descrição, recomendamos que você forneça informações como a finalidade do recurso ou o nome do proprietário do recurso.



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

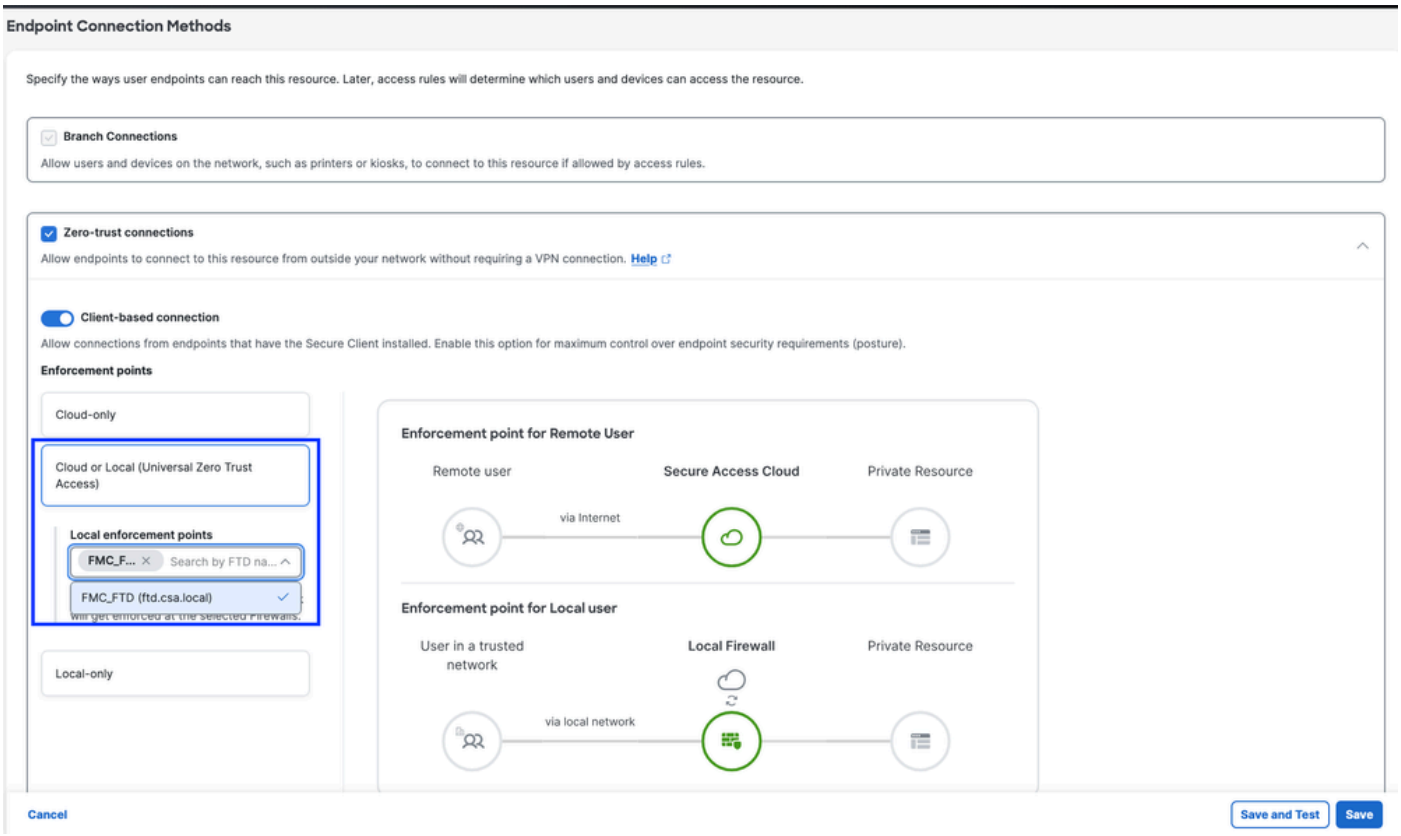
4. Selecione o servidor DNS para resolver o domínio



Acesso seguro - Configuração de recursos privados

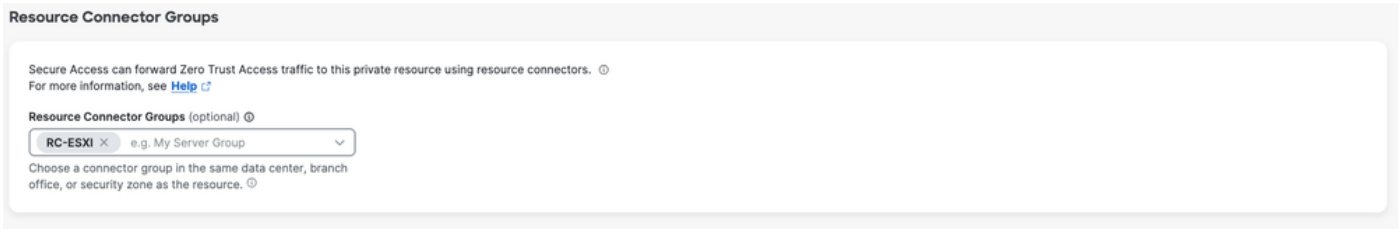
5. Selecionar Métodos de Conexão de Ponto de Extremidade

6. Selecionar FTD como pontos de imposição locais



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).



Acesso seguro - Configuração de recursos privados

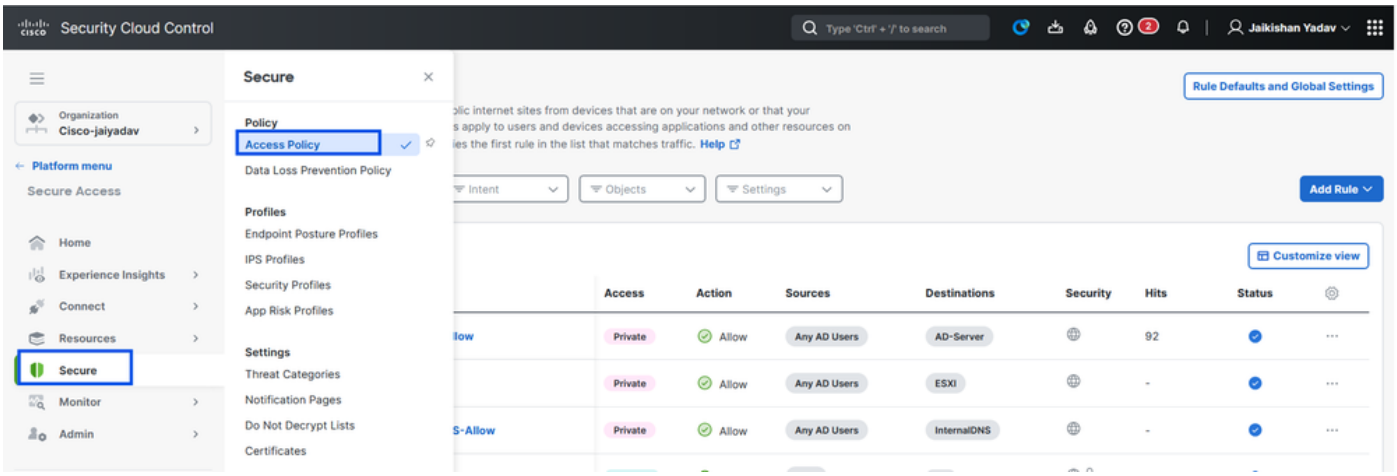
Note: Dependendo do tipo de inscrição que você selecionar , essa alteração associará automaticamente a PR ao FTD e acionará uma implantação de política

7. Clique em Salvar

Etapa 2 - Criar uma regra de acesso privado

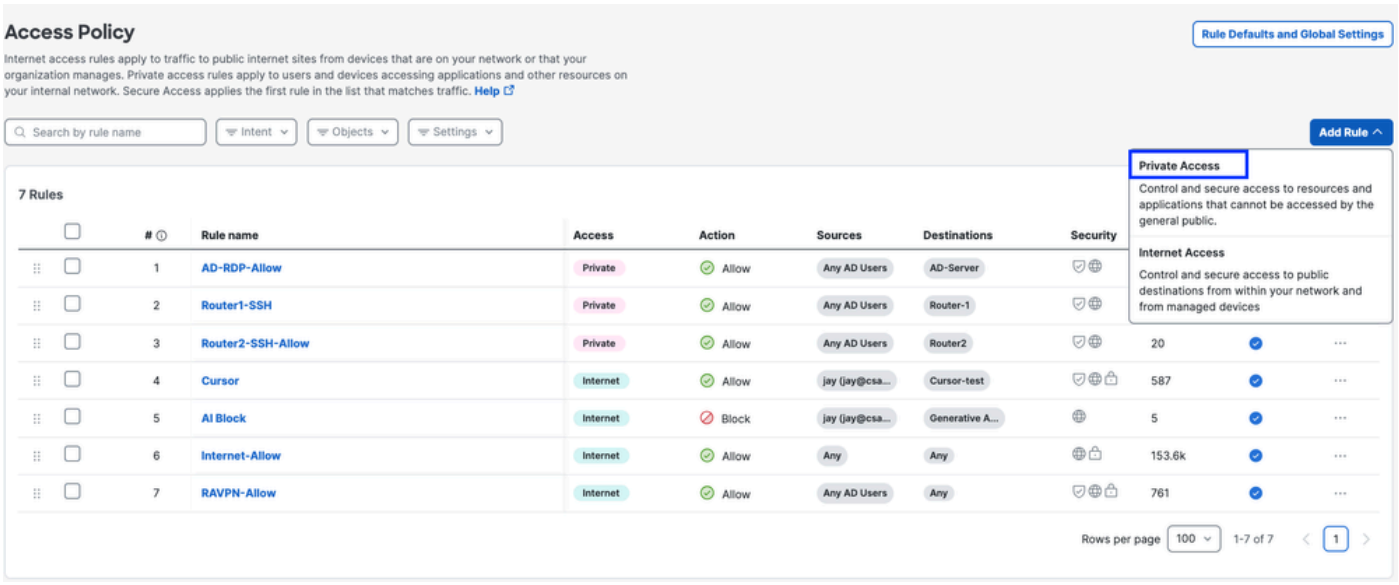
Configure um acesso privado no Secure Access para ser acessado por usuários registrados no Universal ZTA . Para obter mais informações, consulte Regra de acesso privado

1. Navegue até Proteger > Política de acesso



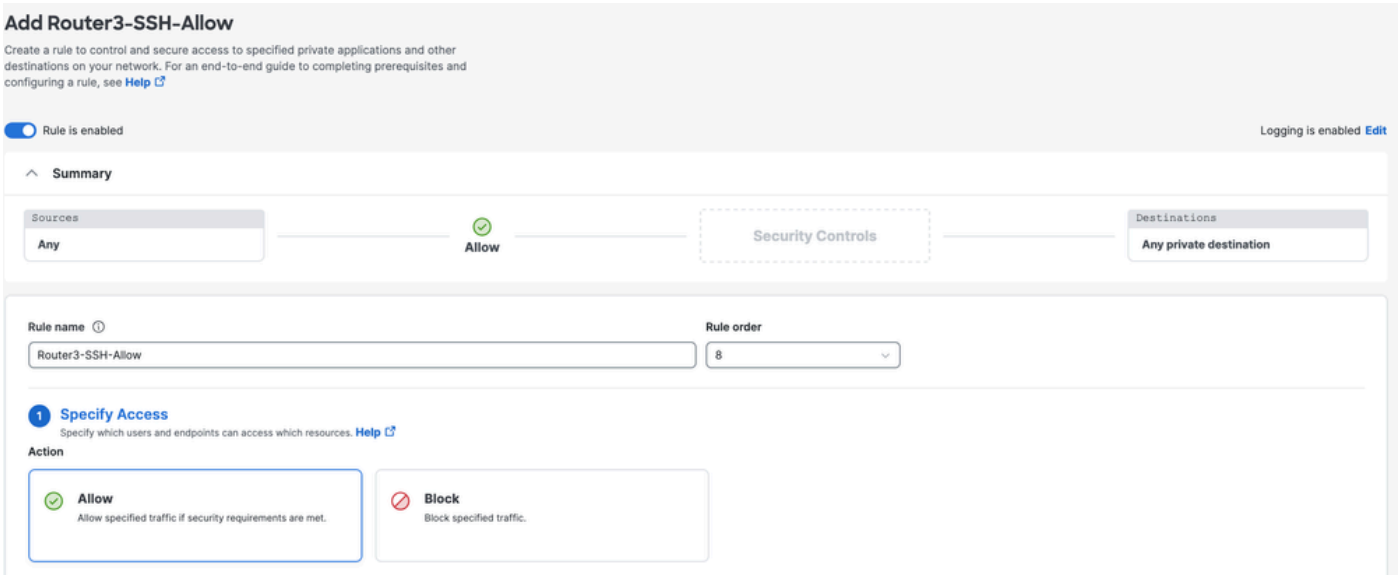
Acesso seguro - Configuração da política de acesso

2. Clique em Adicionar Regra e escolha Acesso Particular.
   Na parte superior da regra há um resumo que descreve os componentes configurados da regra.



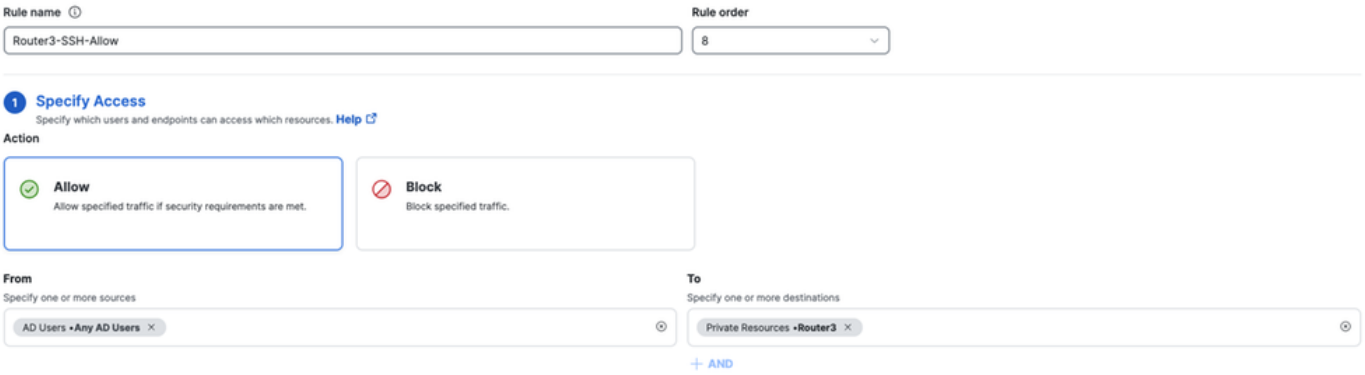
Acesso seguro - Configuração da política de acesso

3. Adicionar um Nome de Regra



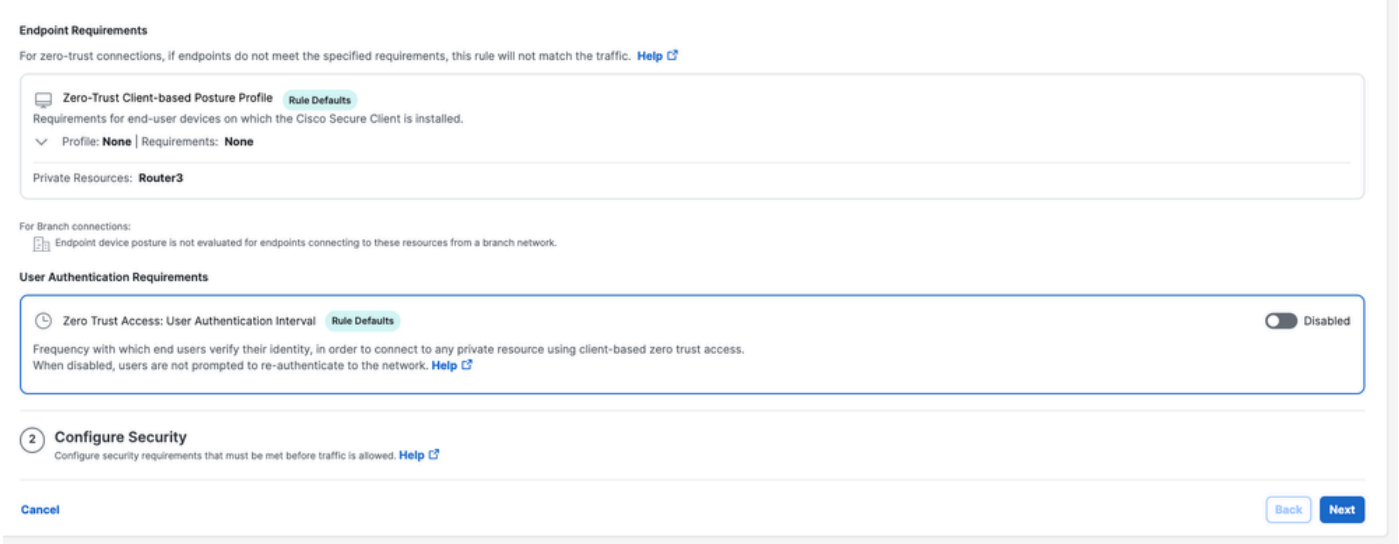
Acesso seguro - Configuração da política de acesso

4. Selecione a ação da regra e selecione origem e destino



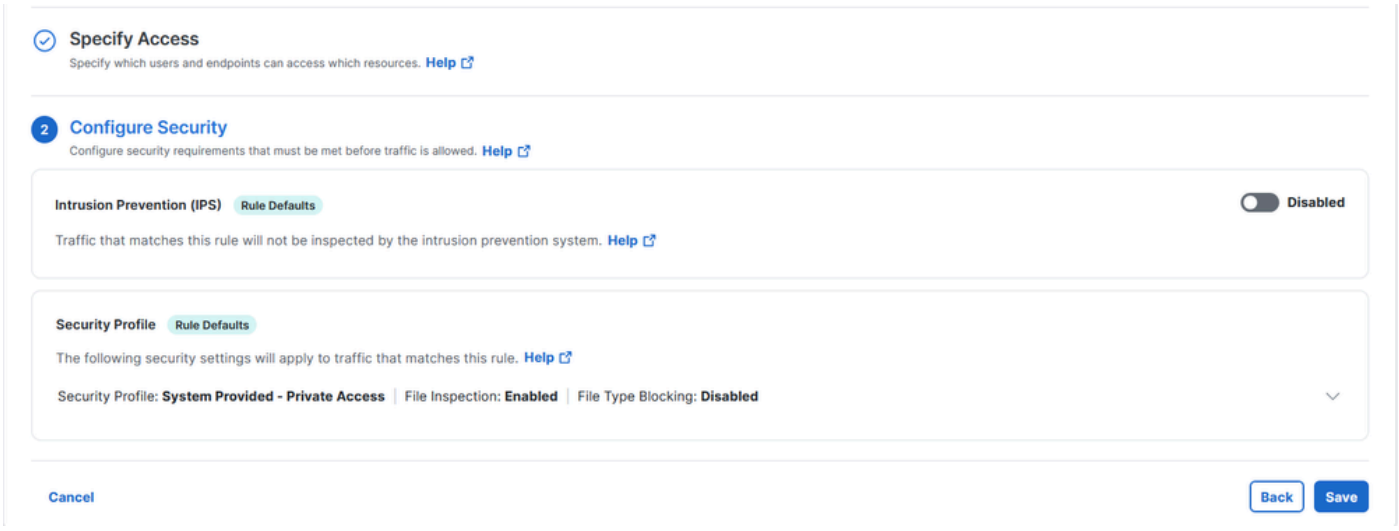
Acesso seguro - Configuração da política de acesso

5. Configurar Requisitos de Endpoint



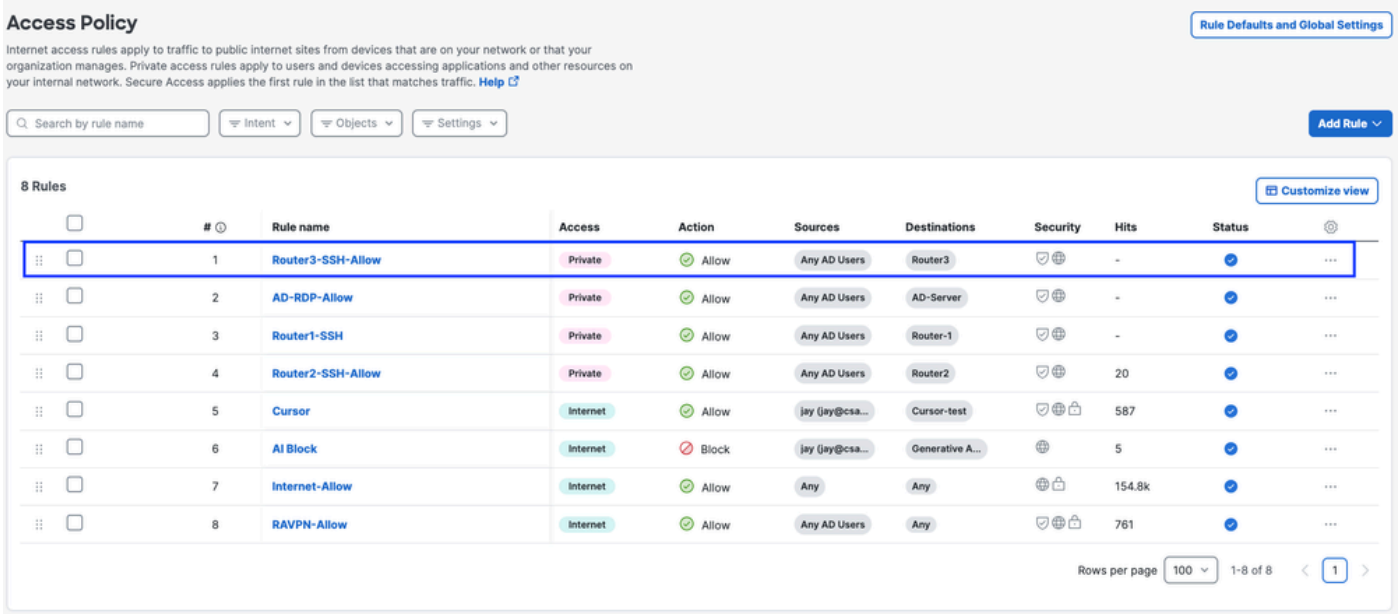
Acesso seguro - Configuração da política de acesso

6. Configurar segurança



Acesso seguro - Configuração da política de acesso

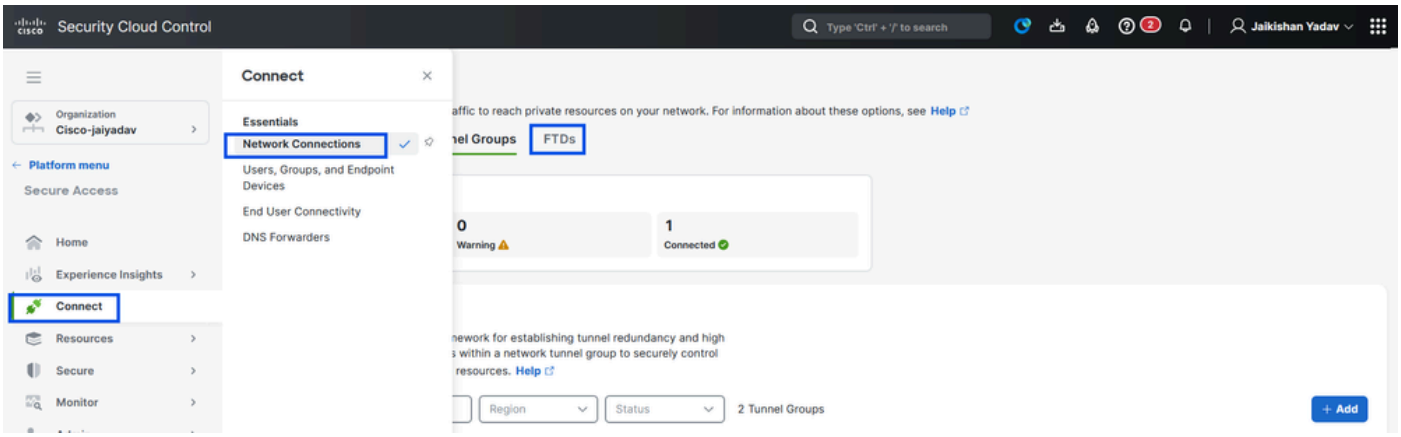
7. Clique em Salvar



Acesso seguro - Configuração da política de acesso

Etapa 3 - Verificar a associação de PR no FTD

1. Navegue para conectar > Conexões de Rede > FTDs

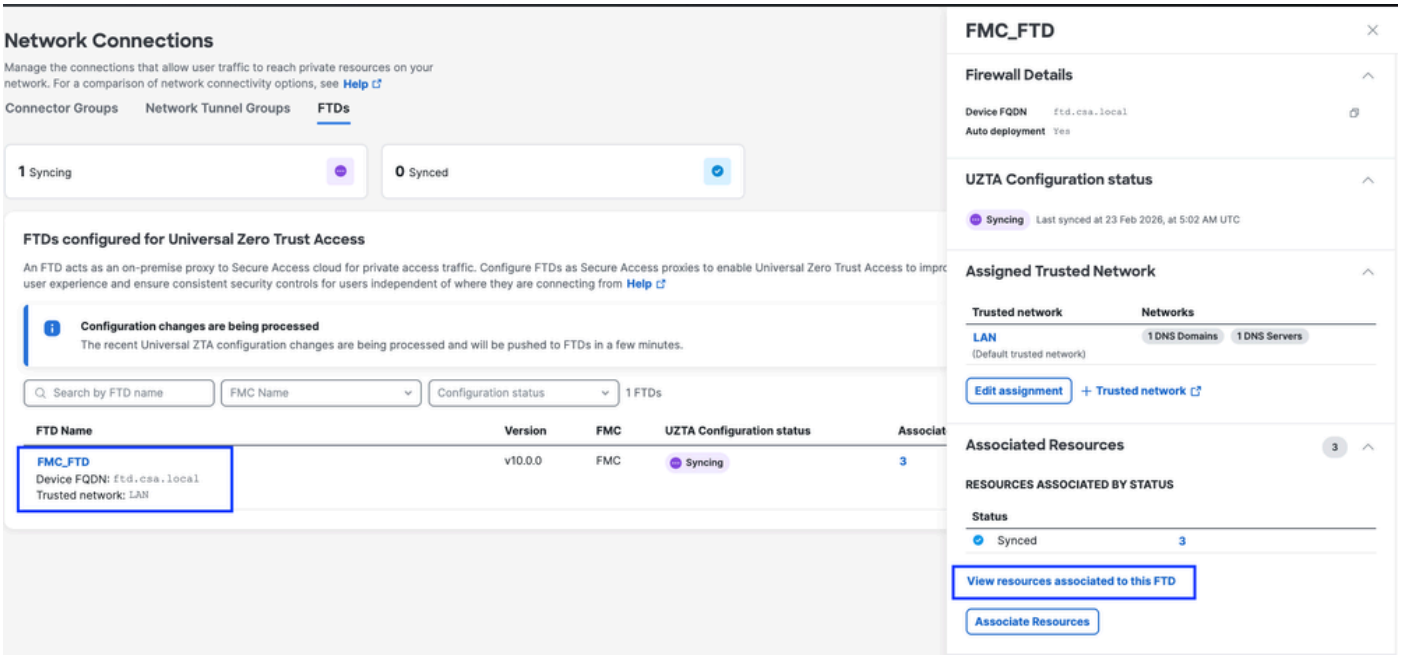


Acesso seguro - Verificação de PR

2. Clique no FTD > Exibir recursos associados a este FTD

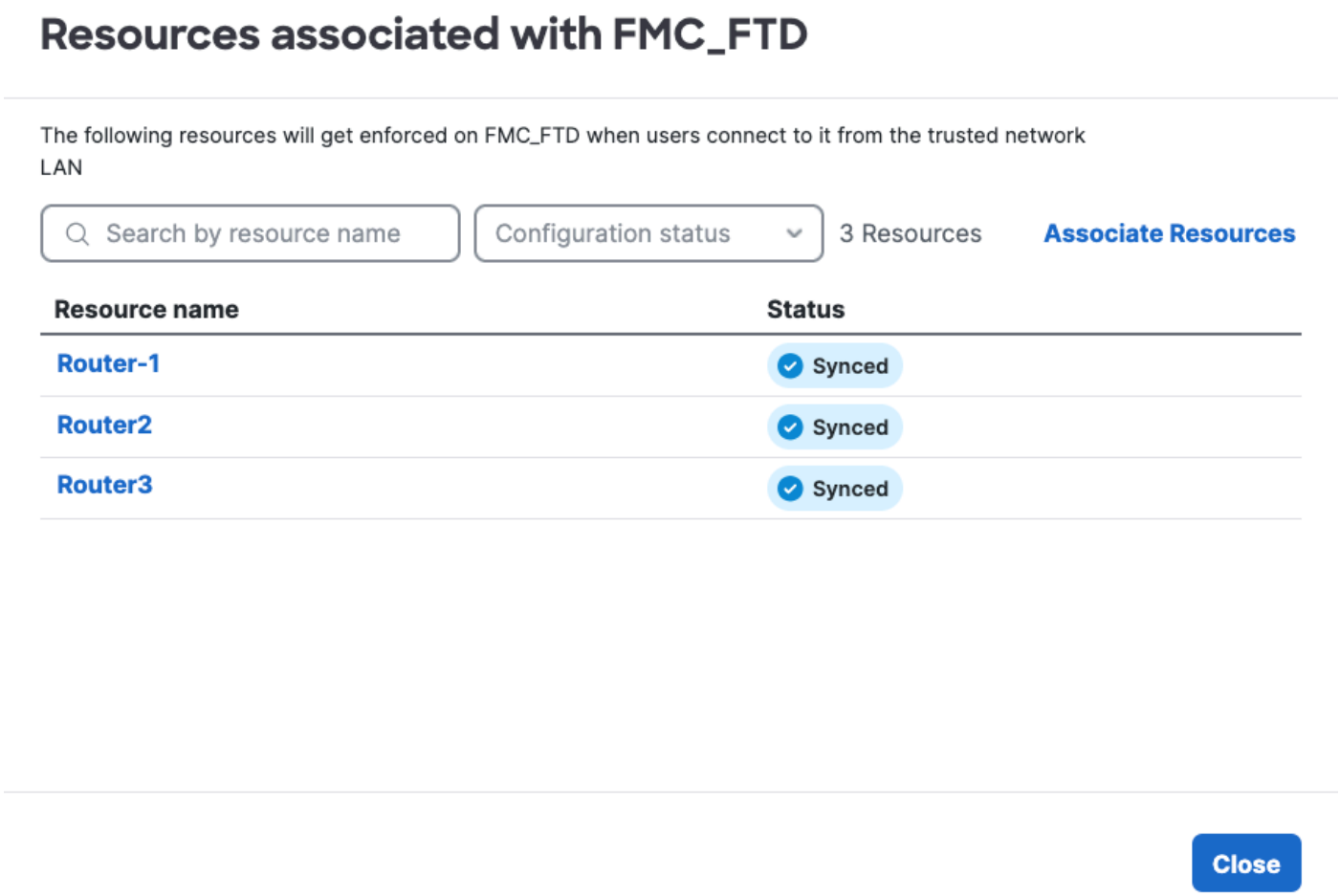
```
C:\Users\jay>ping ftd.csa.local

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



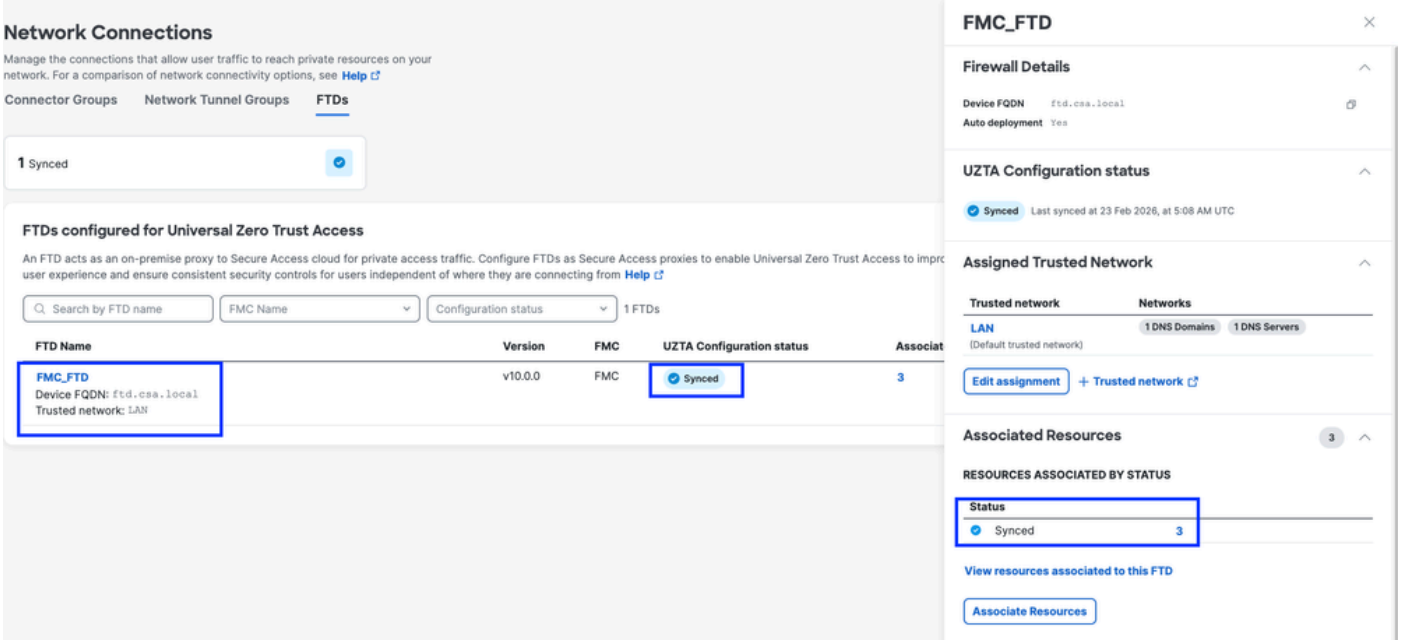
Acesso seguro - Verificação de PR

```
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
```



3. Clique em Close

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



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

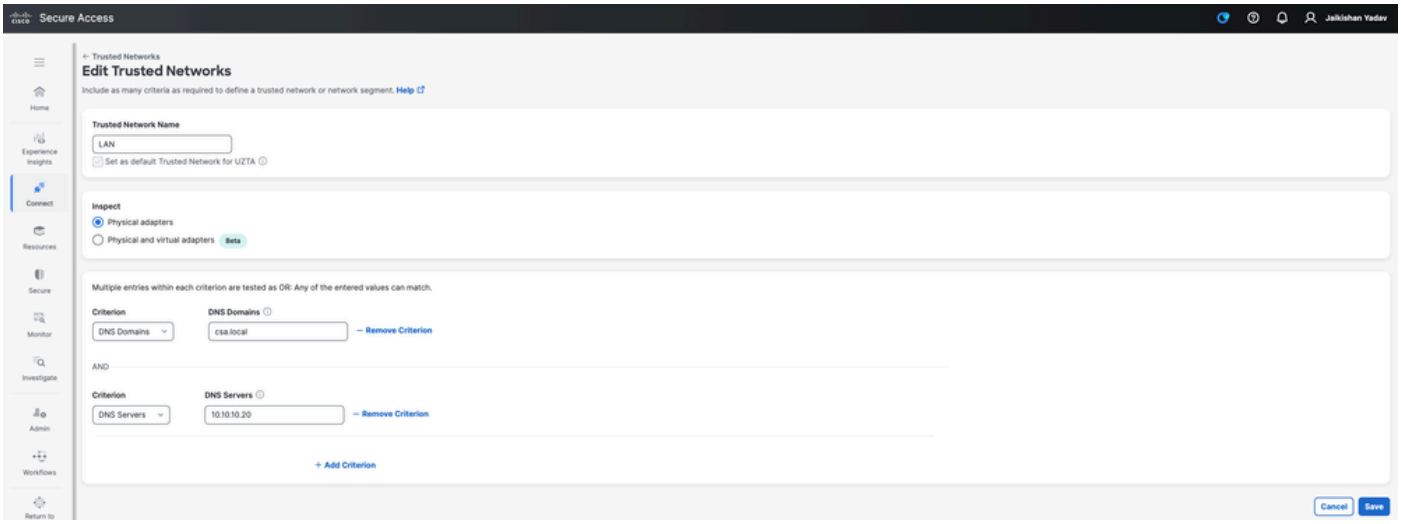
show running-config object application

```
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"

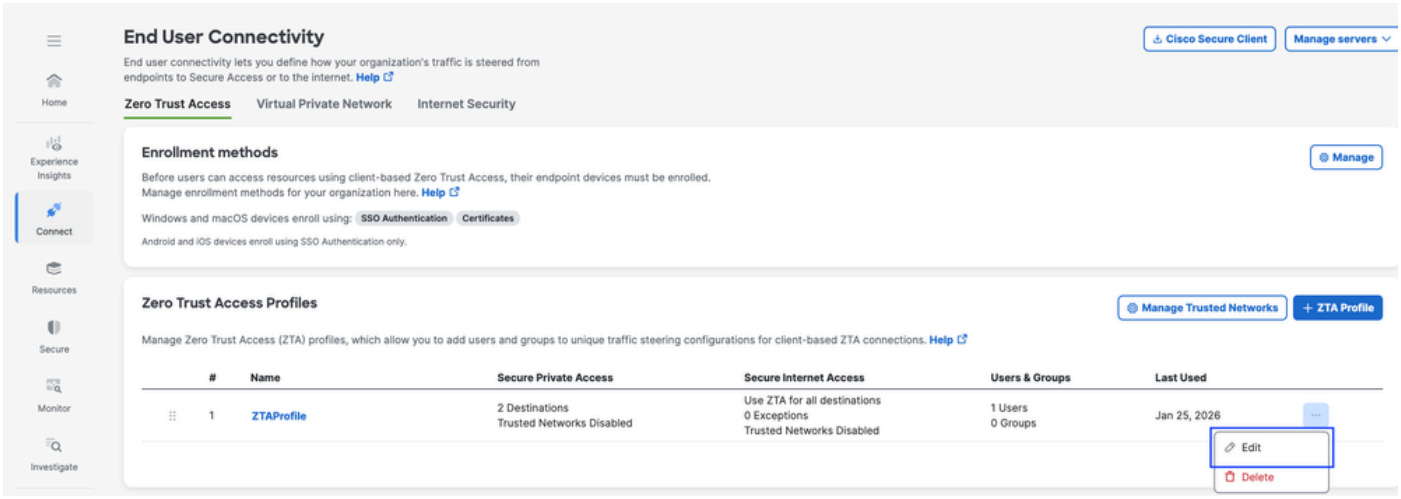
Navegue para Connect > End User Connectivity > Zero Trust Access > ZTA Settings e configure Trusted Networks



Acesso seguro - Configuração ZTA TND

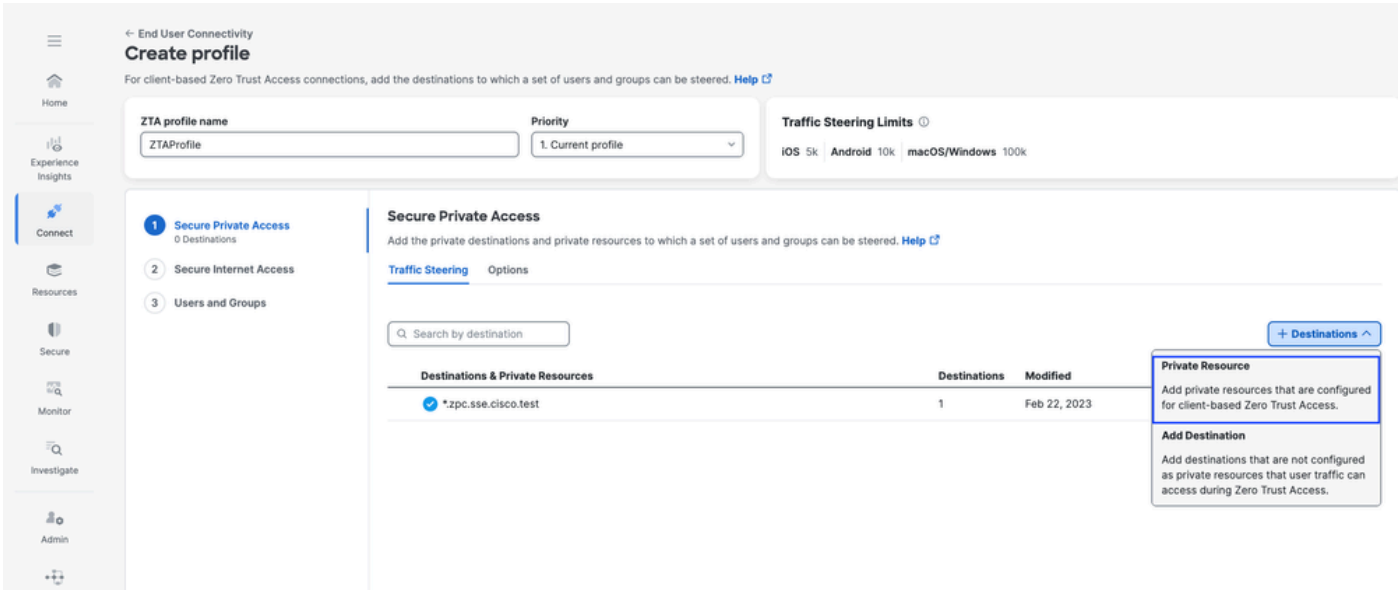
Etapa 5 - Adicionar recurso privado ao perfil ZTA

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

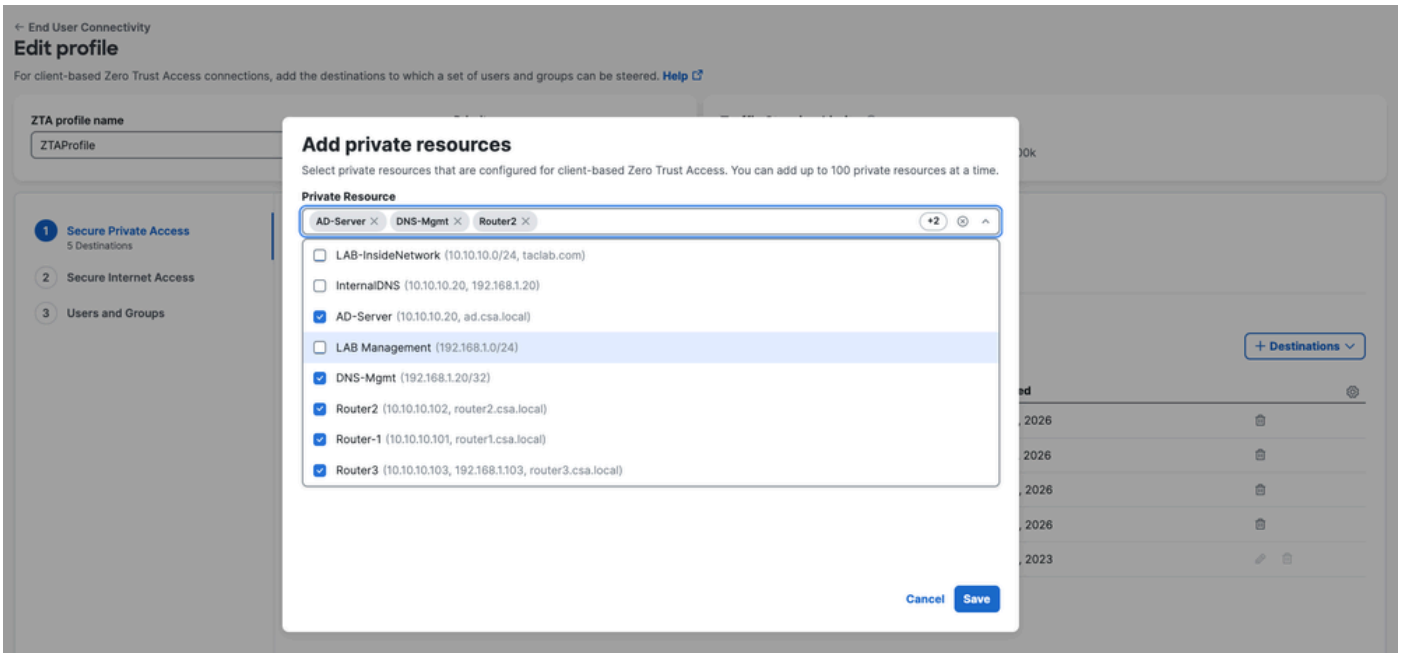


Acesso seguro - perfil ZTA

2. Adicionar o Recurso Particular

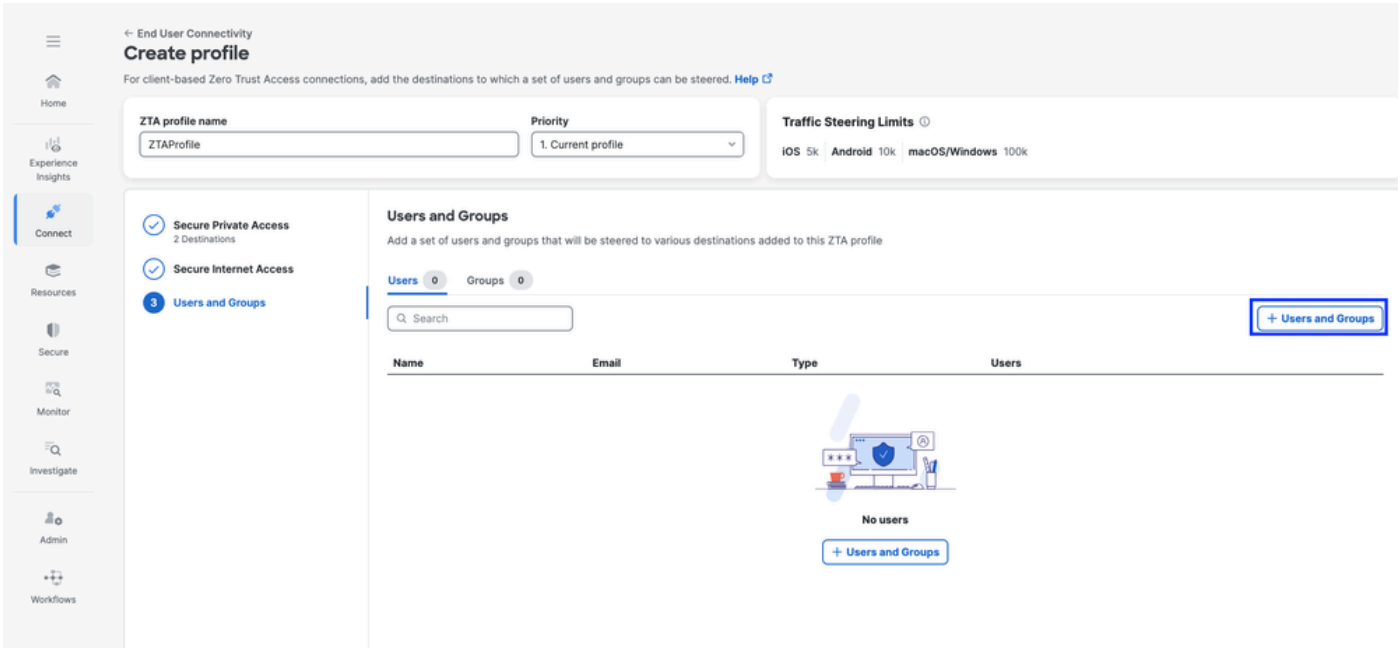


Acesso seguro - perfil ZTA

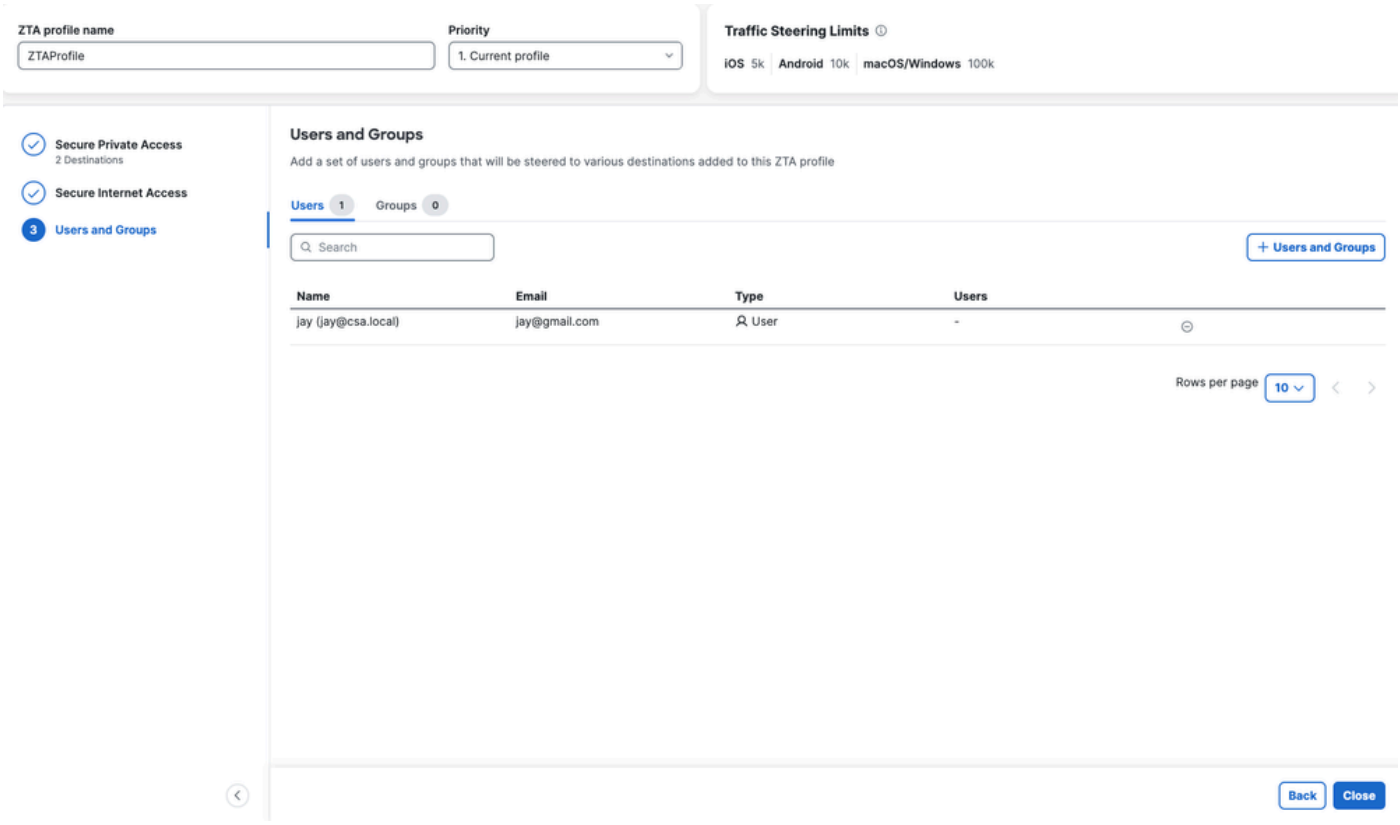


Acesso seguro - perfil ZTA

3. Adicionar usuários e grupos



Acesso seguro - perfil ZTA

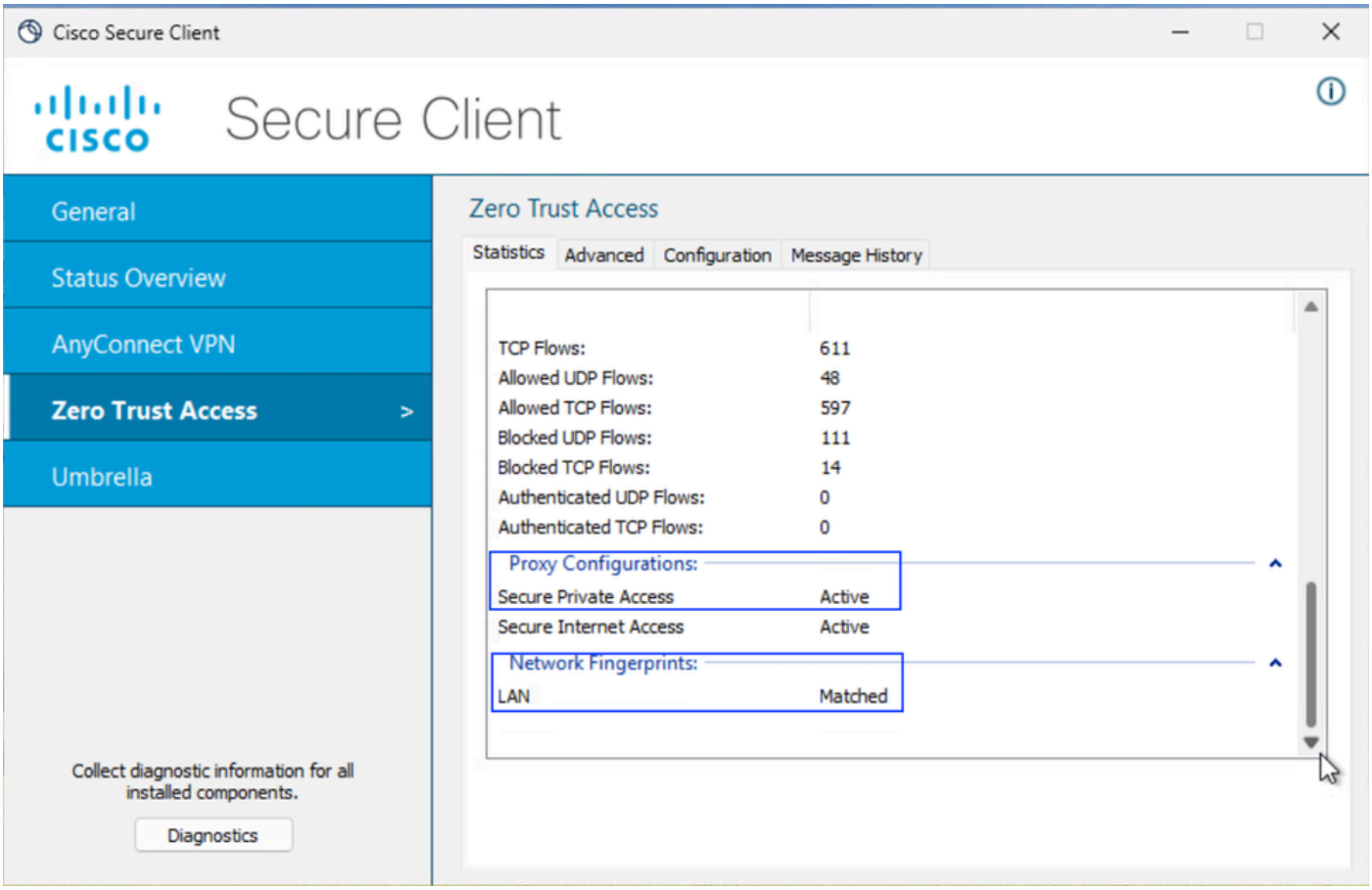


Acesso seguro - perfil ZTA

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

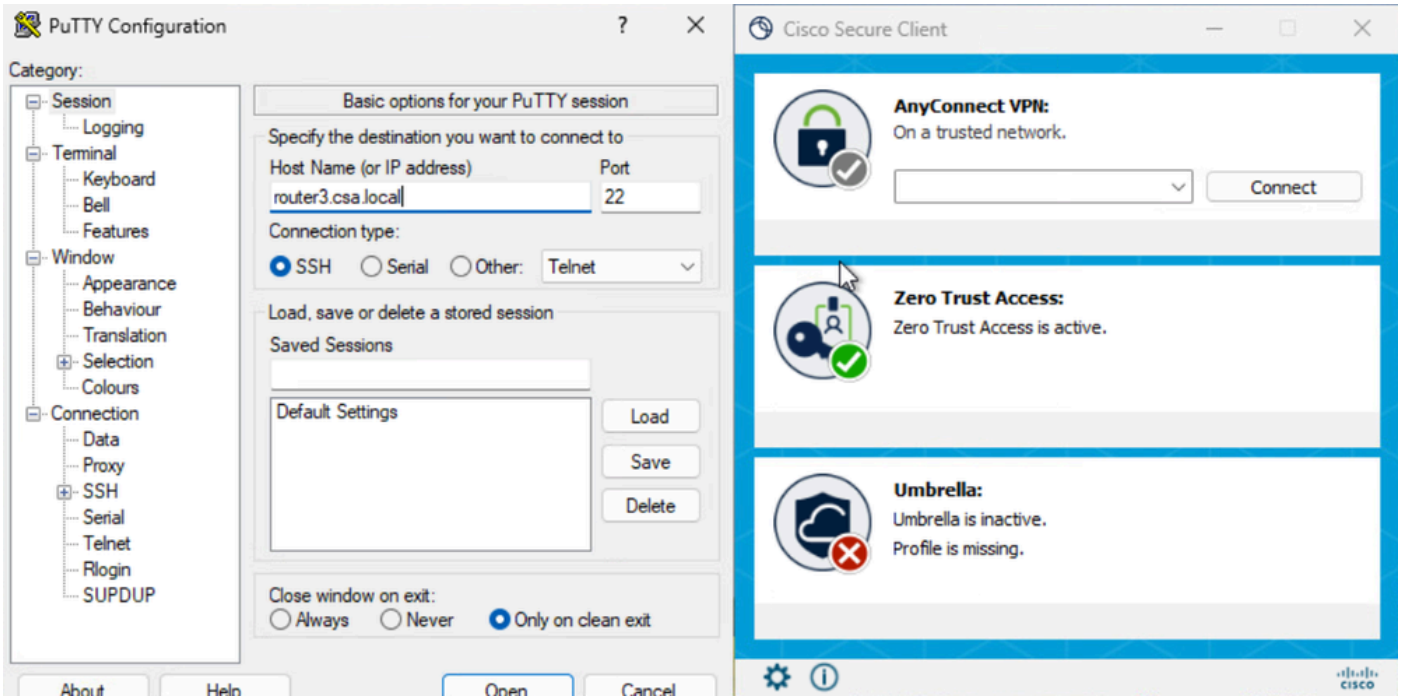
3. Verificar se o FTD pode acessar o recurso privado usando o FQDN

```
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#
```

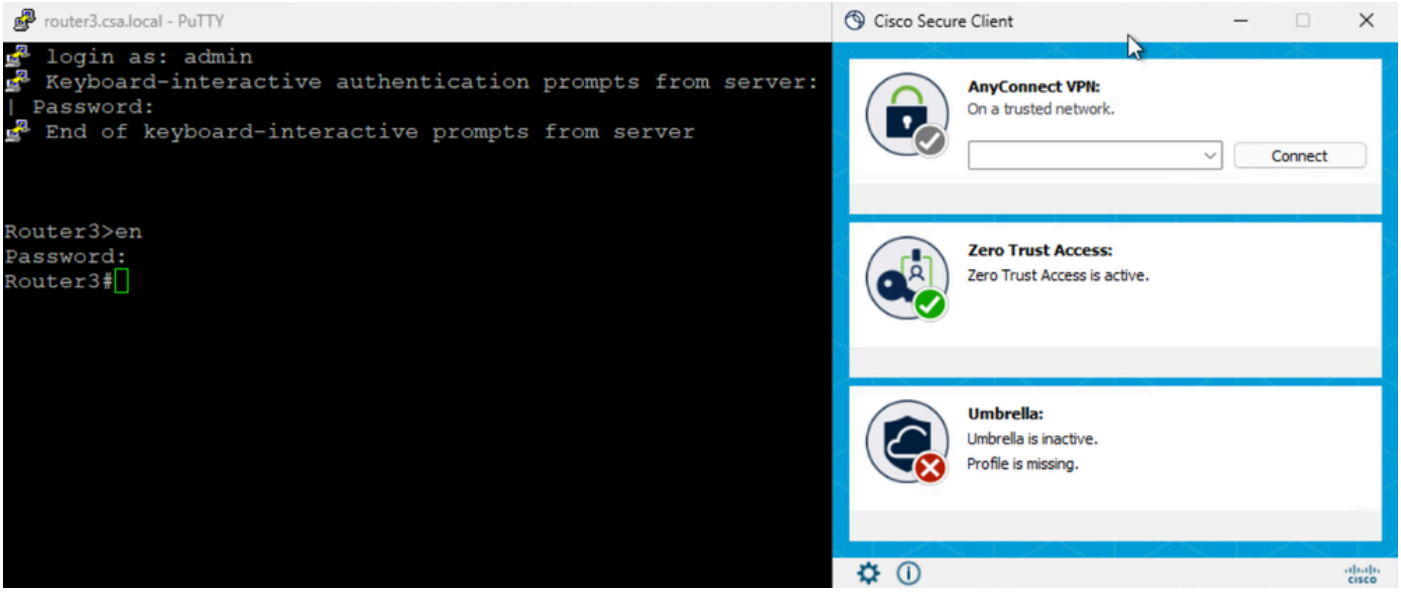
Acesso seguro - Teste de PR

4. Testar a conexão SSH com o recurso privado

Acessar a PR usando o FQDN

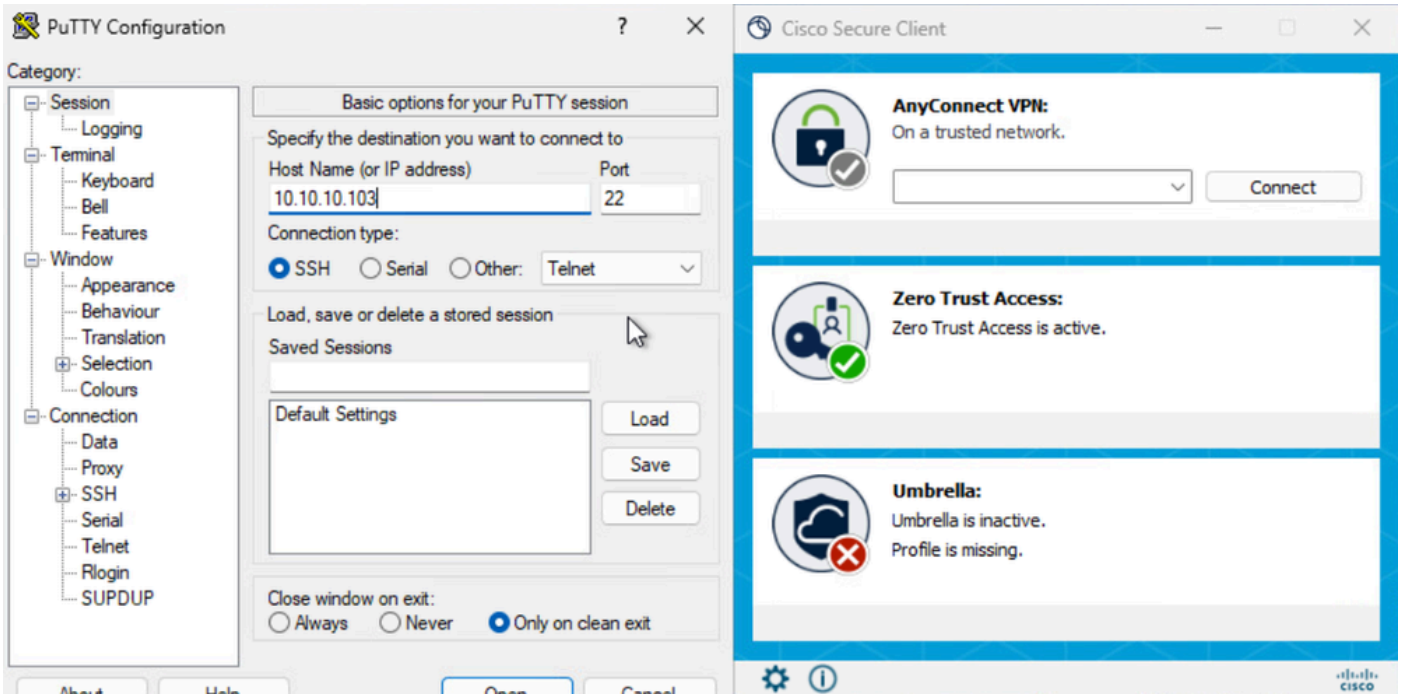


Acesso seguro - Teste de PR

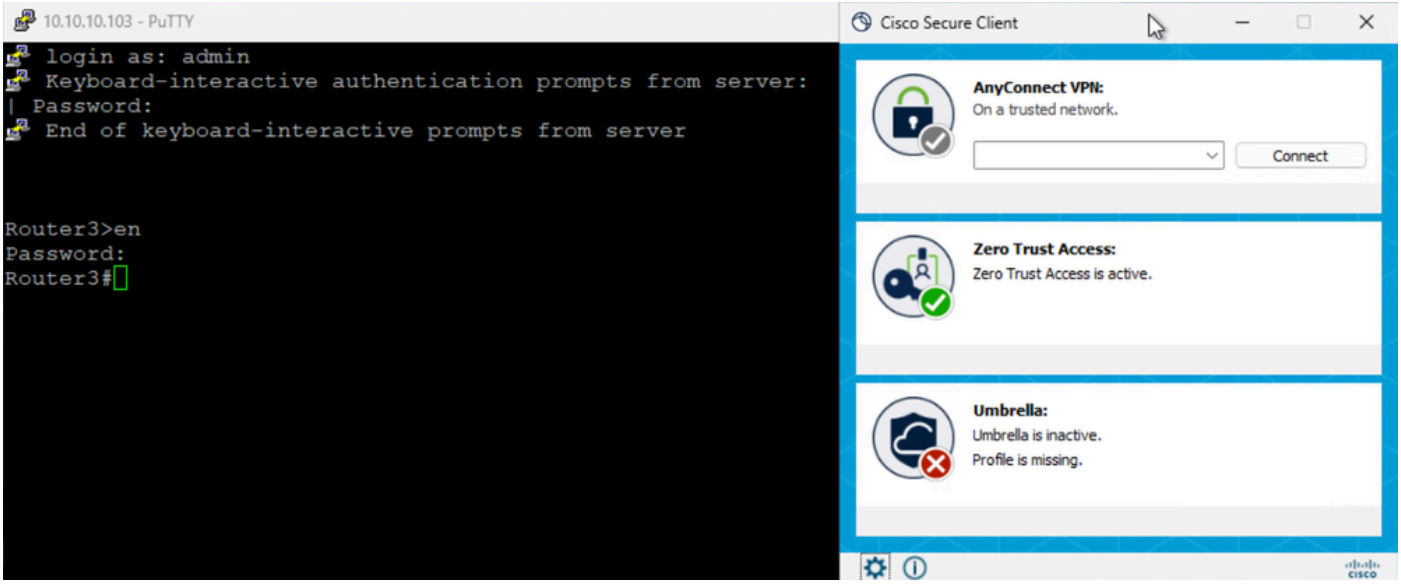


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP

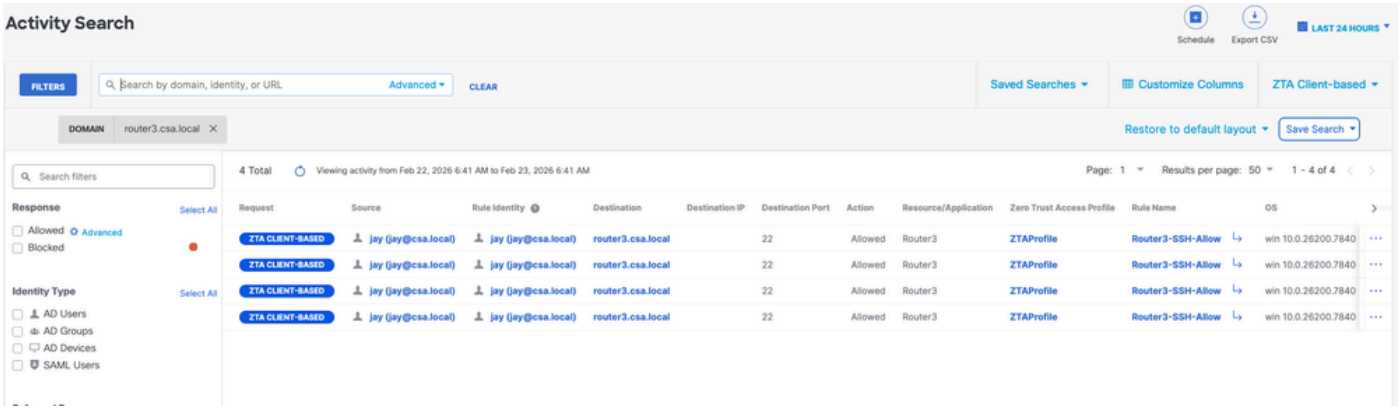


Acesso seguro - Teste de PR

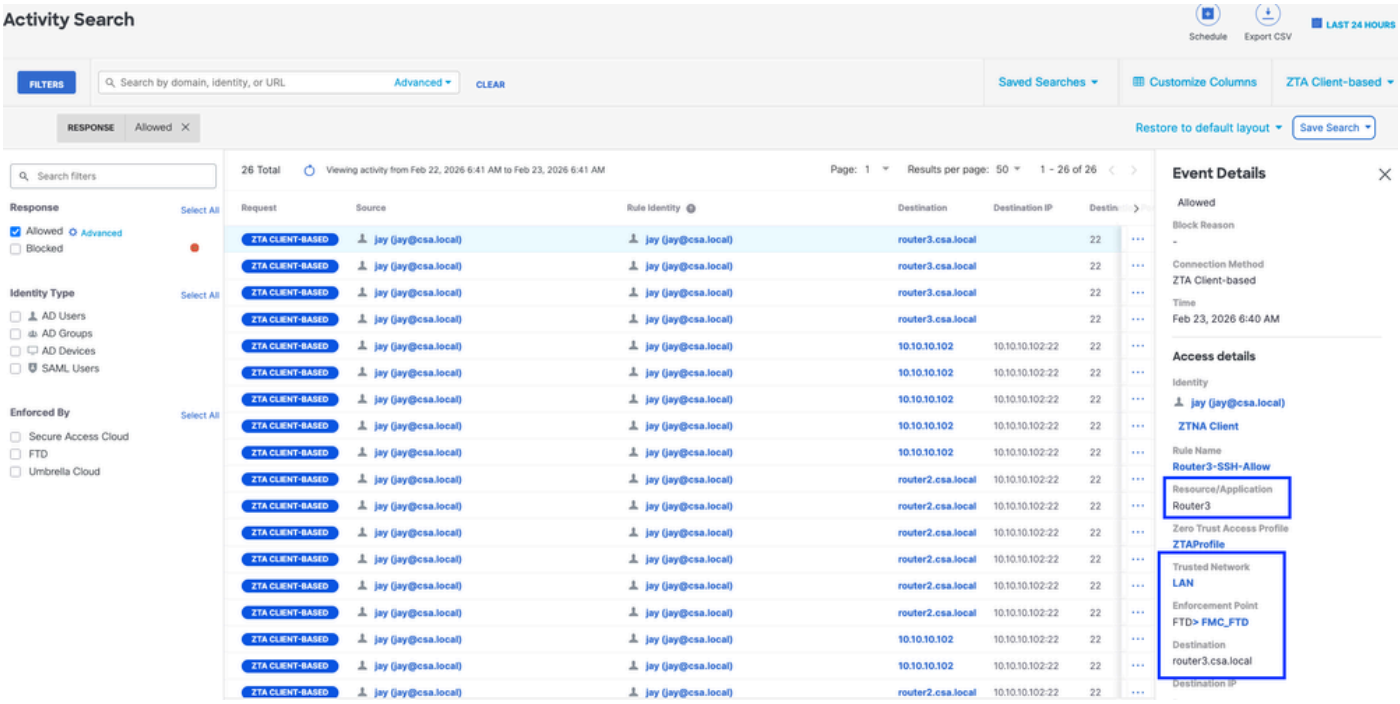


Acesso seguro - Teste de PR

5. Verificar logs de Pesquisa de Atividade de Acesso Seguro

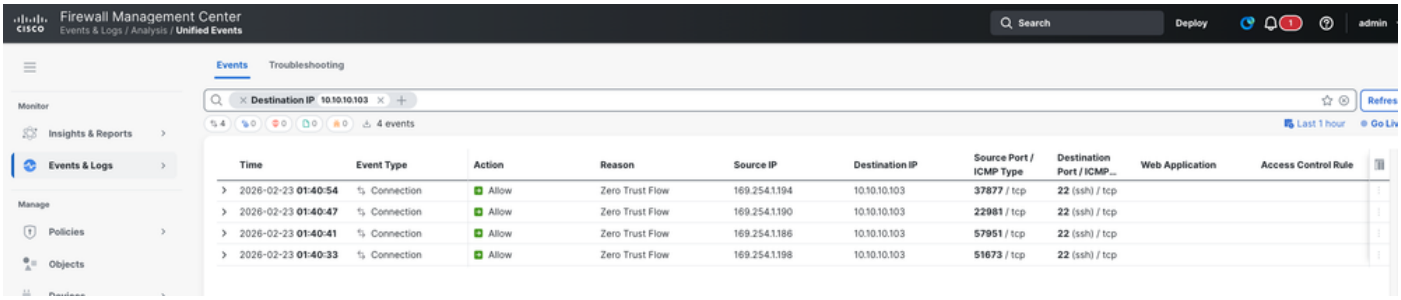


Acesso seguro - Pesquisa de atividades



Acesso seguro - Pesquisa de atividades

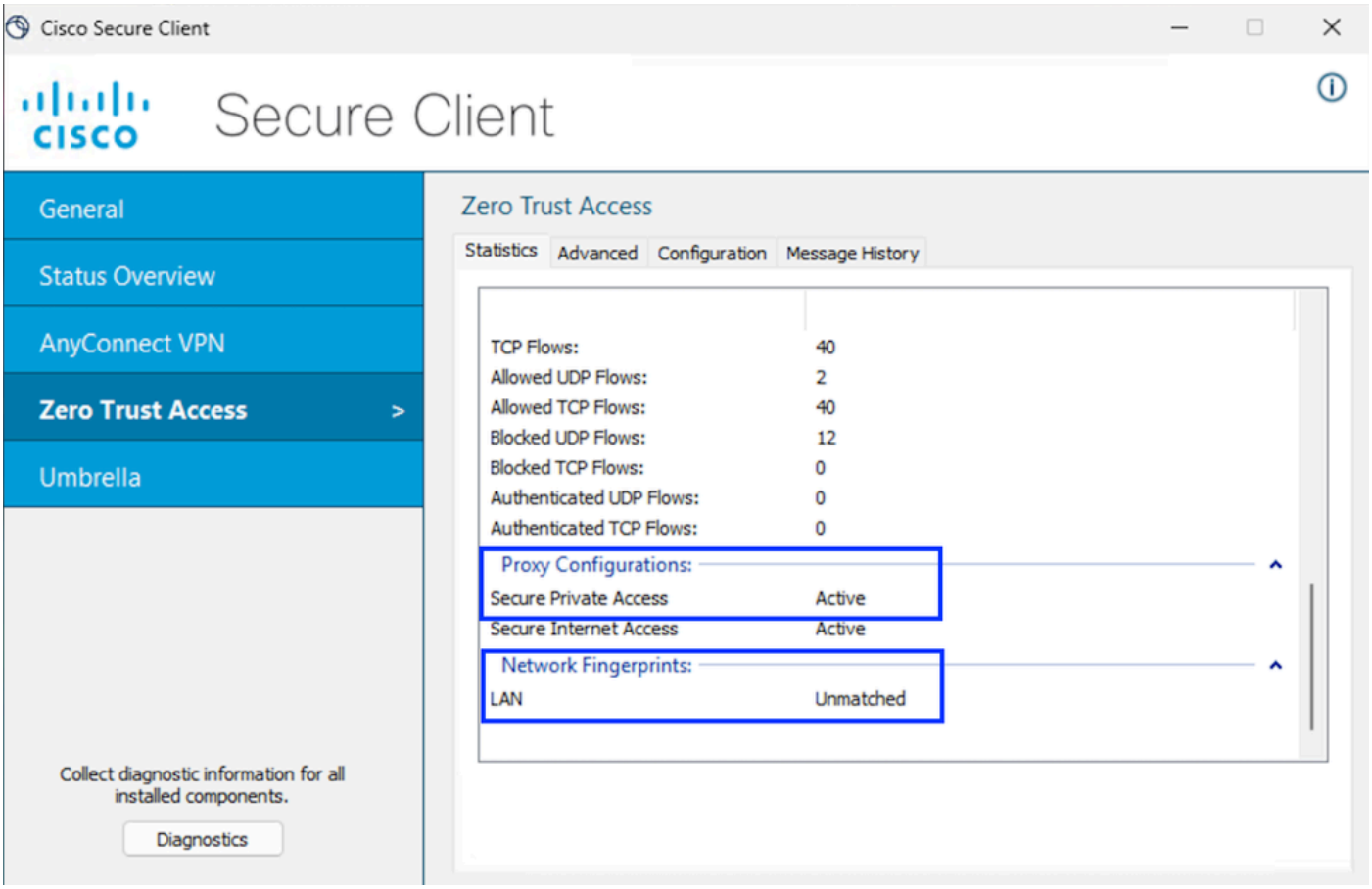
6. Verificar os eventos de conexão do FMC



Eventos de conexão do FMC

Quando o usuário for Remoto

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



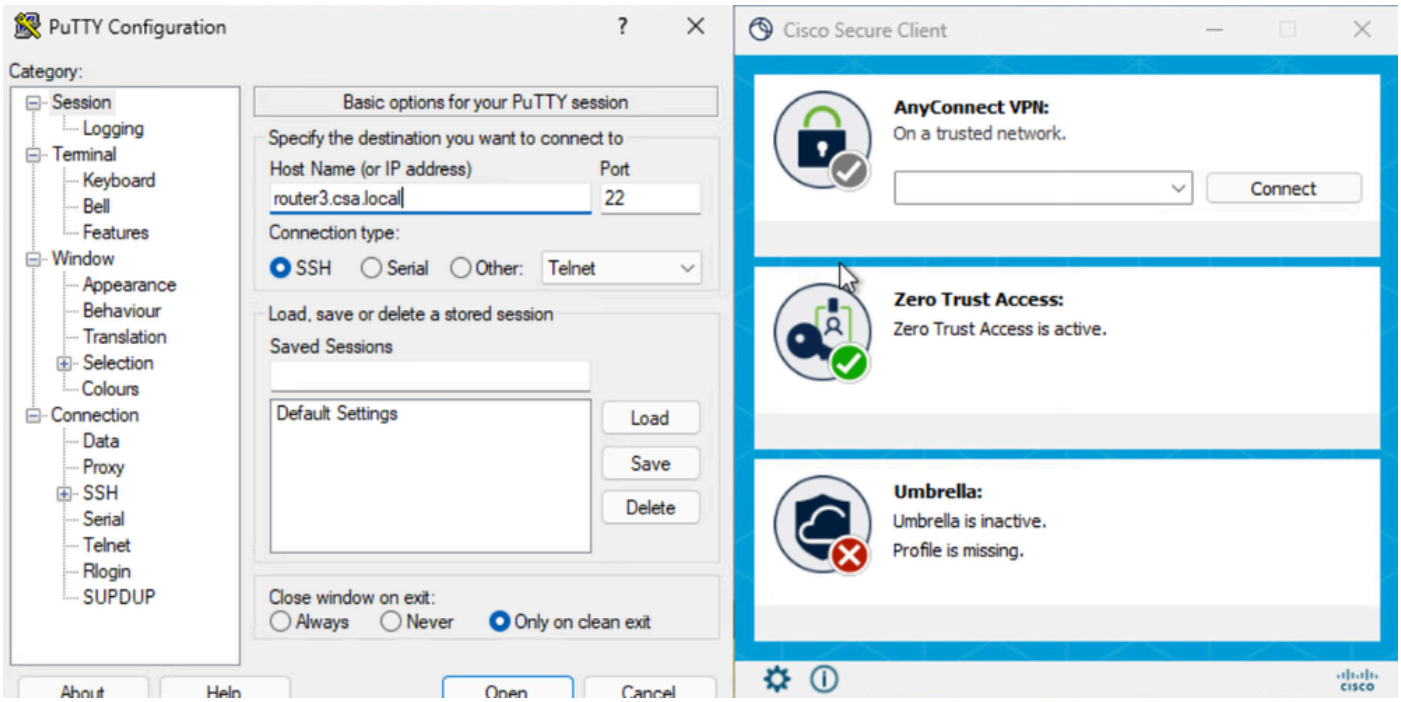
Acesso seguro - Teste de PR

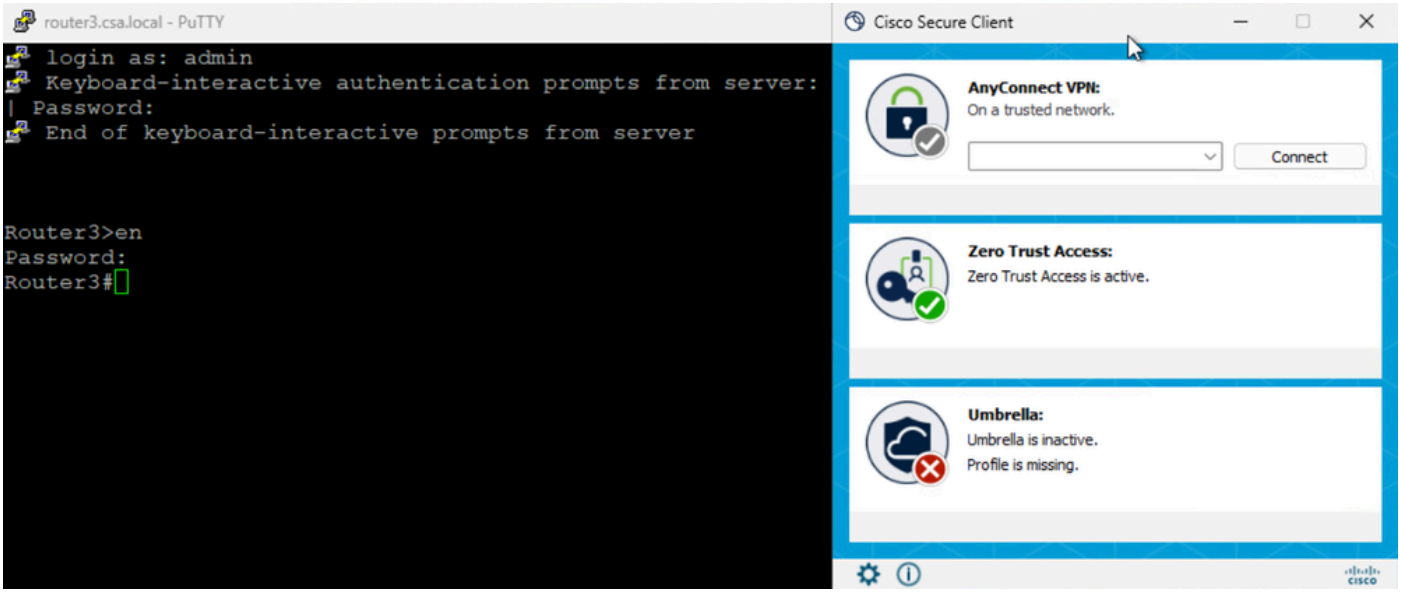
2. Verifique se o usuário remoto pode resolver o FQDN do FTD

```
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
```


3. Testar a conexão SSH com o recurso privado

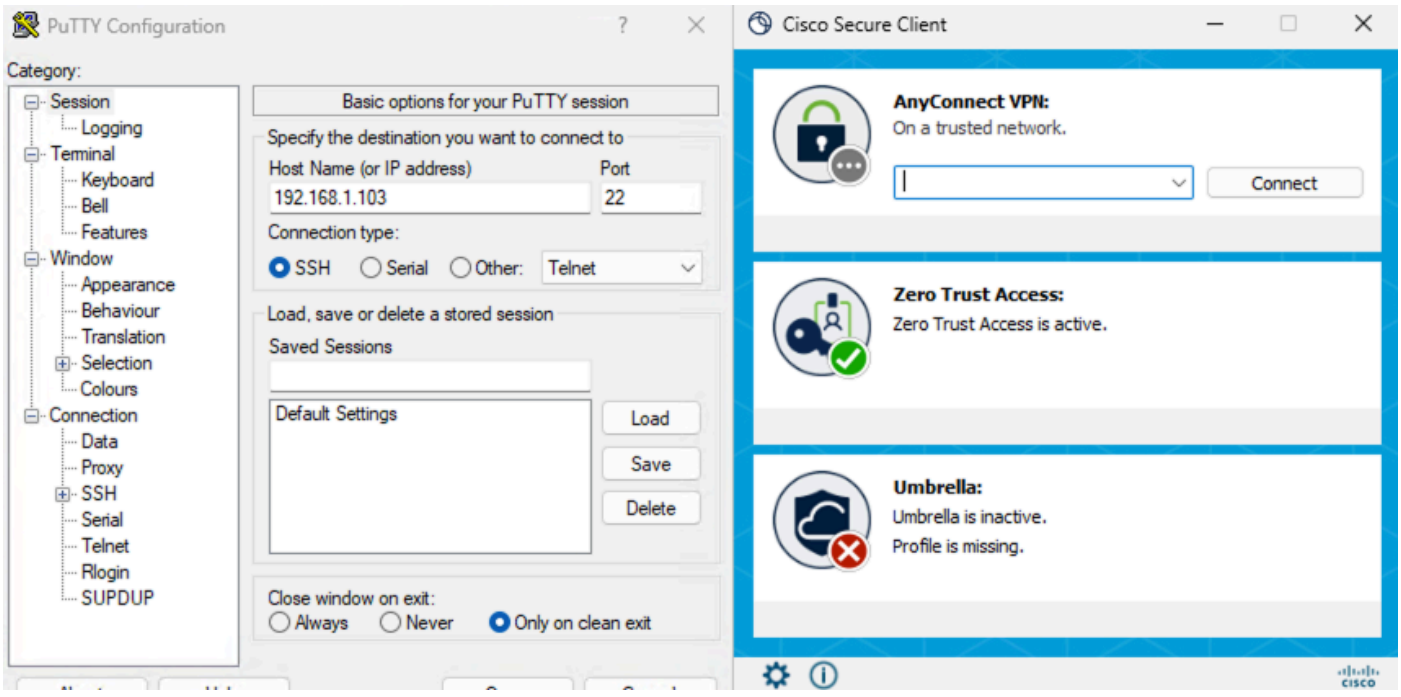
Acessar a PR usando o FQDN



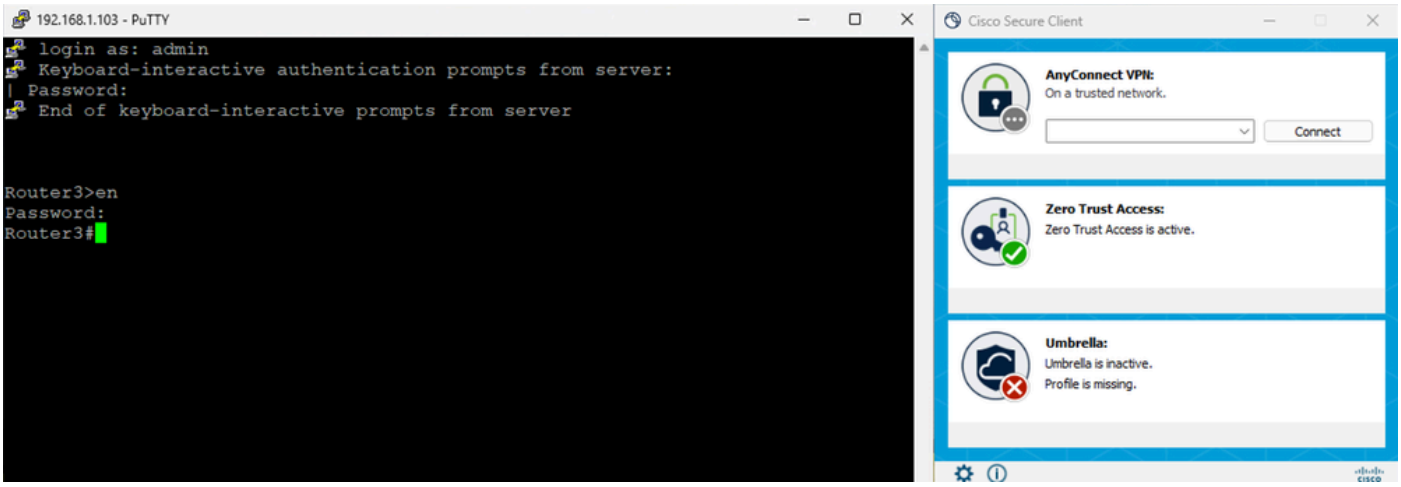


Acesso seguro - Teste de PR

Acessar o PR usando o endereço IP

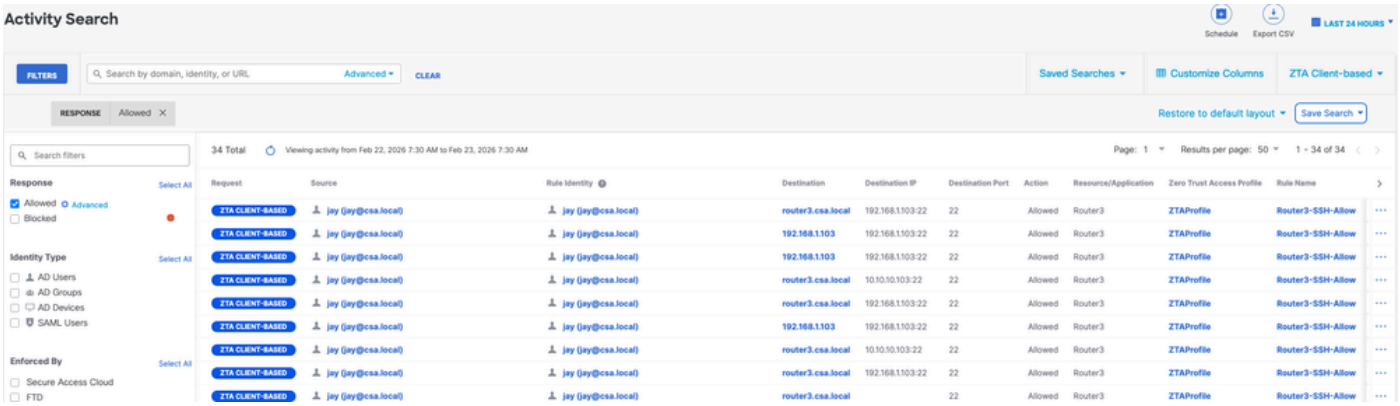


Acesso seguro - Teste de PR

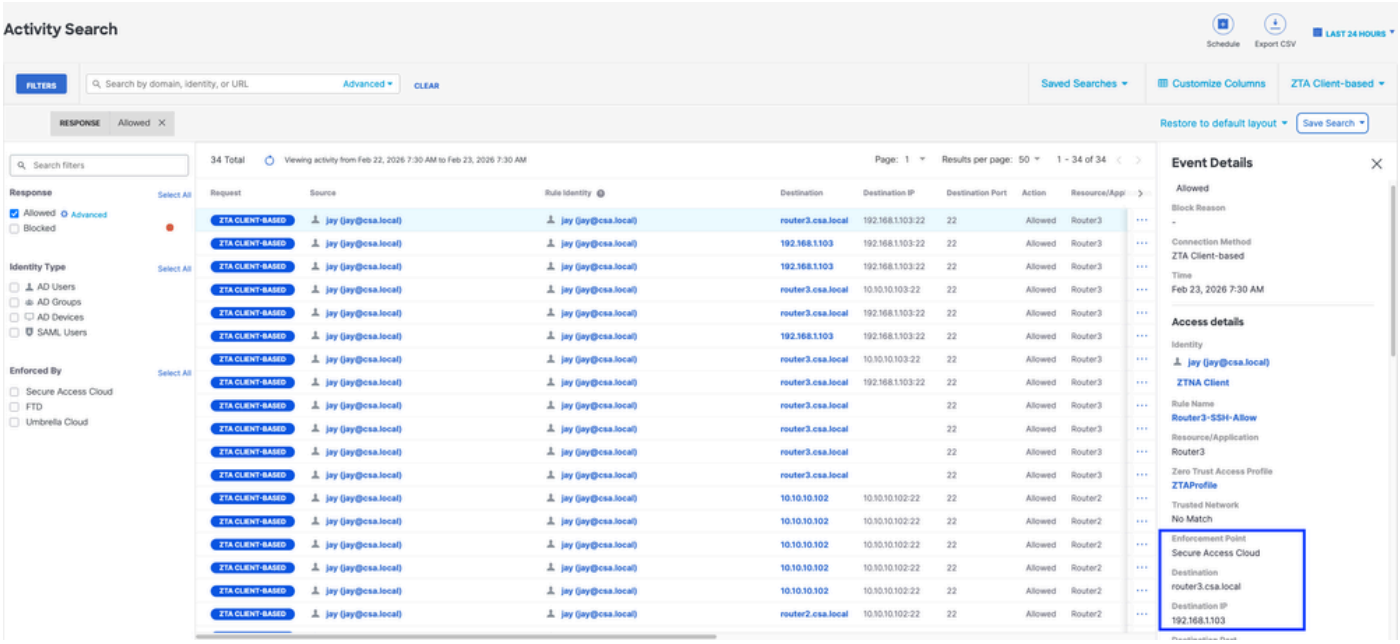


Acesso seguro - Teste de PR

5. Verificar logs de Pesquisa de Atividade de Acesso Seguro



Acesso seguro - Pesquisa de atividades



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.