Configurer le ZTNA universel pour l'accès aux ressources privées sur l'accès sécurisé

Table des matières

Introduction

Dans ce document, nous allons couvrir la configuration pour l'accès aux ressources privées via Universal ZTNA avec différents chemins de trafic.

Conditions préalables

La configuration suivante doit être effectuée avant la configuration Universal ZTNA

- Fournisseur d'identité sur Cisco Secure Access
- Inscrire des périphériques sans accès sécurisé à l'aide de certificats
- Configuration des tunnels avec Cisco Secure Firewall

- Réseau privé virtuel à accès distant
- Connecteur de ressources sur accès sécurisé
- Intégration FTD sur le contrôle cloud de la sécurité
- L'indicateur de fonctionnalité ZTNA hybride doit être activé pour le locataire d'accès sécurisé respectif. Contactez le TAC Cisco pour activer l'indicateur

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN IPsec sur Cisco Secure Access et Firewall Threat Defense
- Fournisseur d'identités (IdP) - Approvisionnement utilisateur à partir d'Active Directory
- Configuration VPN à distance sur Cisco Secure Access
- Déploiement de Resource Connector sur Cisco Secure Access
- Inscription basée sur les certificats ZTA
- Certificat - OpenSSL, génération CSR, modèles de certificats, etc.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Threat Defense (Version 7.7.10)
- Cisco Secure Firepower Management Center (Version 7.7.10)
- Client sécurisé Cisco (ZTA version 5.1.10.1720)
- Windows 11
- Windows 2019 Server - Autorité de certification
- Connecteur de ressources sur ESXi

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

À propos de Universal ZTNA

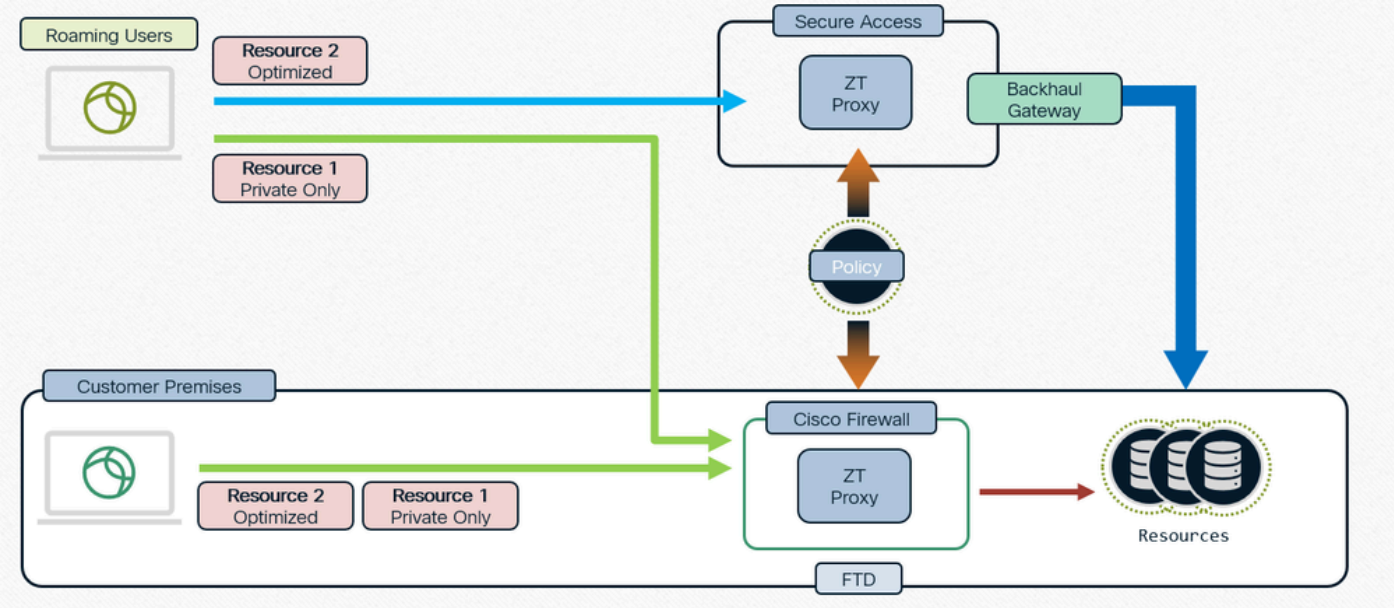
L'accès réseau sans confiance universel (uZTNA) permet aux administrateurs d'autoriser spécifiquement l'accès aux ressources réseau internes en fonction de l'identité de l'utilisateur (y

compris la confiance et la position de l'utilisateur), et sans accorder l'accès à l'ensemble du réseau comme avec RA-VPN. uZTNA permet aux administrateurs de sécuriser les ressources et les applications internes pour les utilisateurs distants et sur site.

Comme Zuta ne suppose pas que l'accès accordé à une application autorise implicitement l'accès à d'autres applications, la surface d'attaque du réseau est réduite.

Secure Access évalue la stratégie d'accès. Toutes les stratégies de contrôle d'accès déployées sur les périphériques à partir du Centre de gestion du pare-feu sécurisé sont ignorées.

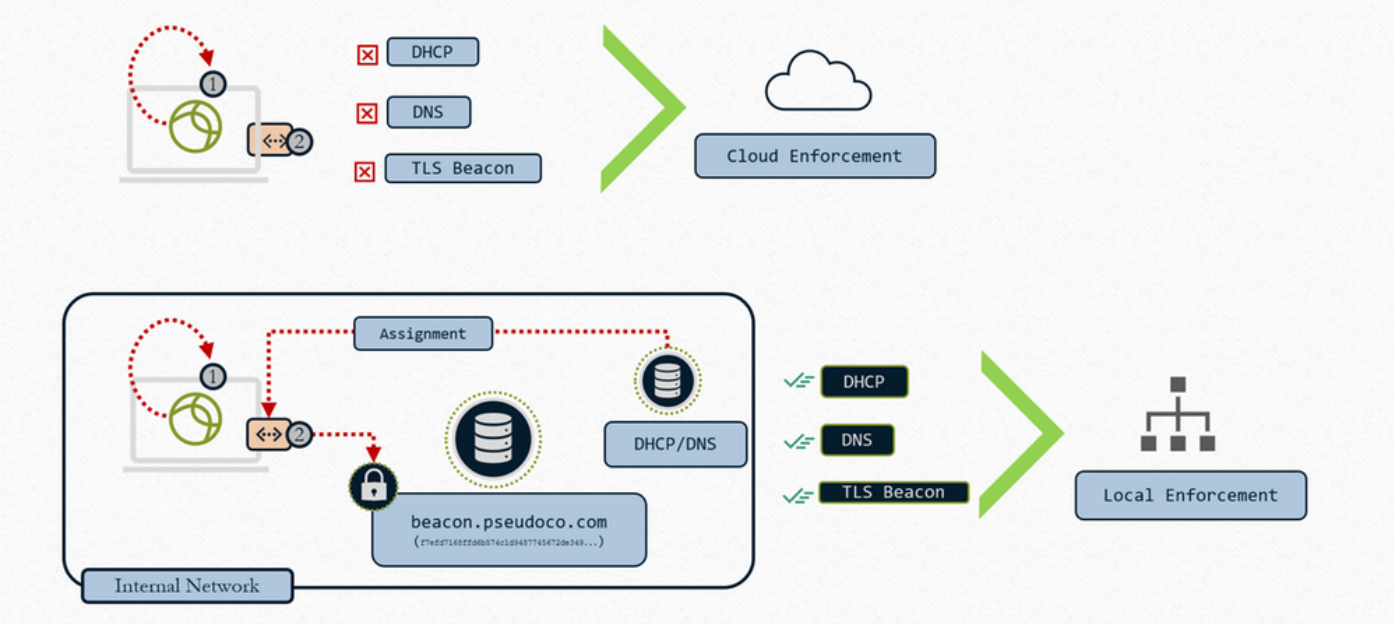
Le proxy de trafic, ainsi que l'application des politiques IPS, de fichiers et de programmes malveillants, sont effectués sur le pare-feu Firepower Threat Defense (FTD).



Politique unique, application distribuée

Détection du réseau

Détermination de l'application locale ou cloud



ZTNA universel : détermination de l'application cloud ou locale

1- Le client interroge l'interface locale pour la configuration du réseau

2- Le client recherche la balise TLS

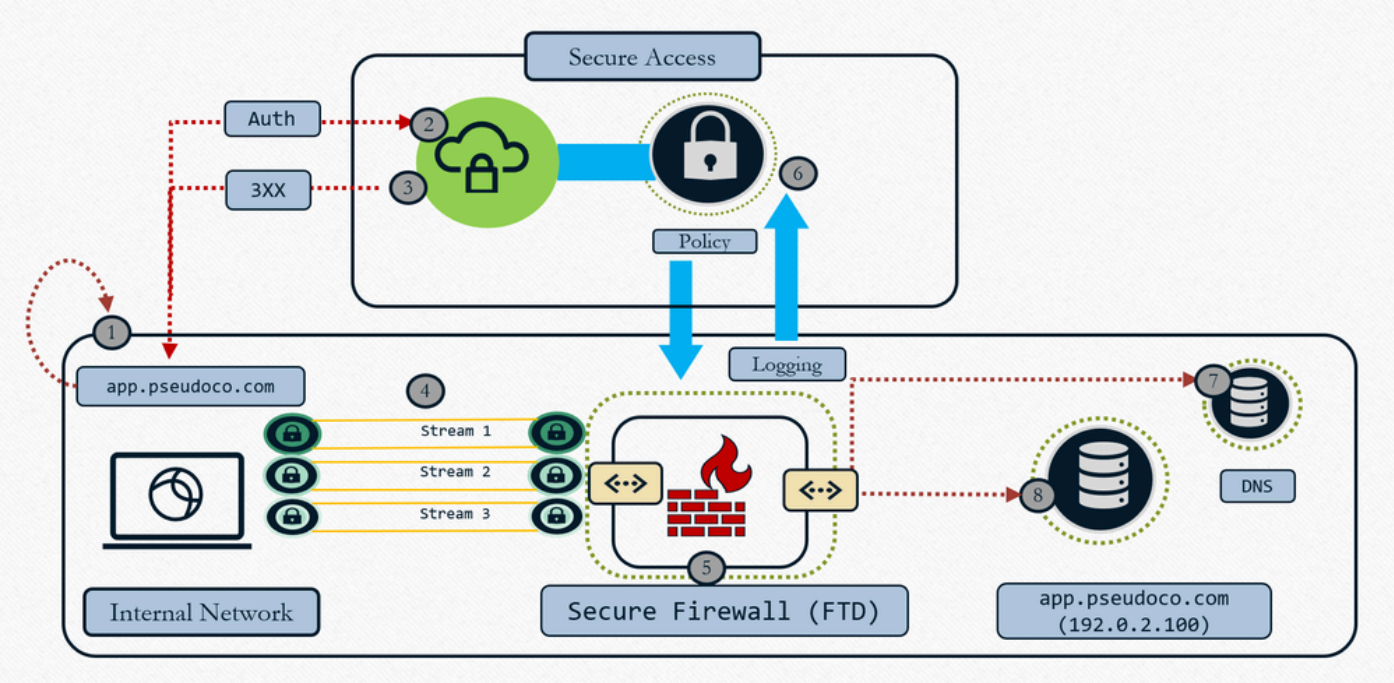
3- Si la condition correspond - Application locale

4- Si la condition ne correspond pas - Application du cloud

Lorsque nous configurons la ressource avec « Cloud ou application locale » et associons la règle TND à FTD , ce qu'elle fait réellement est que l'ensemble des règles d'interception qui est envoyé au client inclura l'évaluation de la règle TND. Ainsi, le cloud demandera à ce client d'évaluer la règle TND. Lorsque nous envoyons la connexion, nous plaçons le résultat de cette évaluation TND - empreinte réseau dans l'en-tête HTTP de sorte que indique au proxy si nous sommes sur un réseau permanent ou non fiable, puis le proxy utilise ces informations et redirige le trafic en conséquence. Si l'empreinte correspond, Zproxy indique au client de rediriger le trafic vers FTD et si l'empreinte ne correspond pas, il redirige le trafic vers le cloud. Référez-vous Configurer un accès réseau sans confiance avec la détection de réseau sécurisé

Types d'application

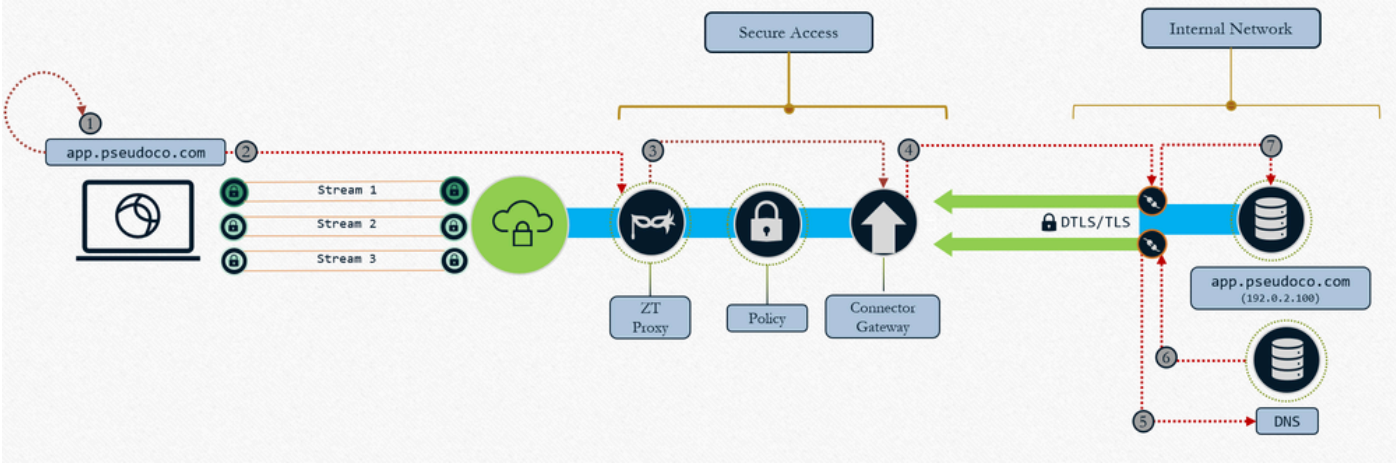
- Chemin d'application local : Application du pare-feu



ZTNA universel - Application locale

1. Demande utilisateur App, le client capture et résout la demande en IP éphémère (plage d'hôtes locaux)
2. Le trafic de contrôle d'authentification est envoyé au cloud d'accès sécurisé pour évaluation des politiques
3. Le cloud renvoie la redirection vers FTD pour l'application du plan de données (si la politique le permet)
4. Trafic dirigé vers la tête de réseau configurée par le pare-feu (interface)
5. La politique définie dans le cloud est appliquée (IPS, programmes malveillants, décryptage) à l'aide du plan de données proxy local
6. Événements consignés et doublons envoyés au cloud pour un reporting cohérent
7. Le pare-feu effectue une résolution DNS sur le réseau local pour acheminer le trafic de ressources (si autorisé)
8. Le pare-feu établit une connexion à une ressource (nouvelle connexion établie à une ressource) lorsque le pare-feu se comporte comme un proxy TCP

- Chemin d'application cloud : Réseau OFF

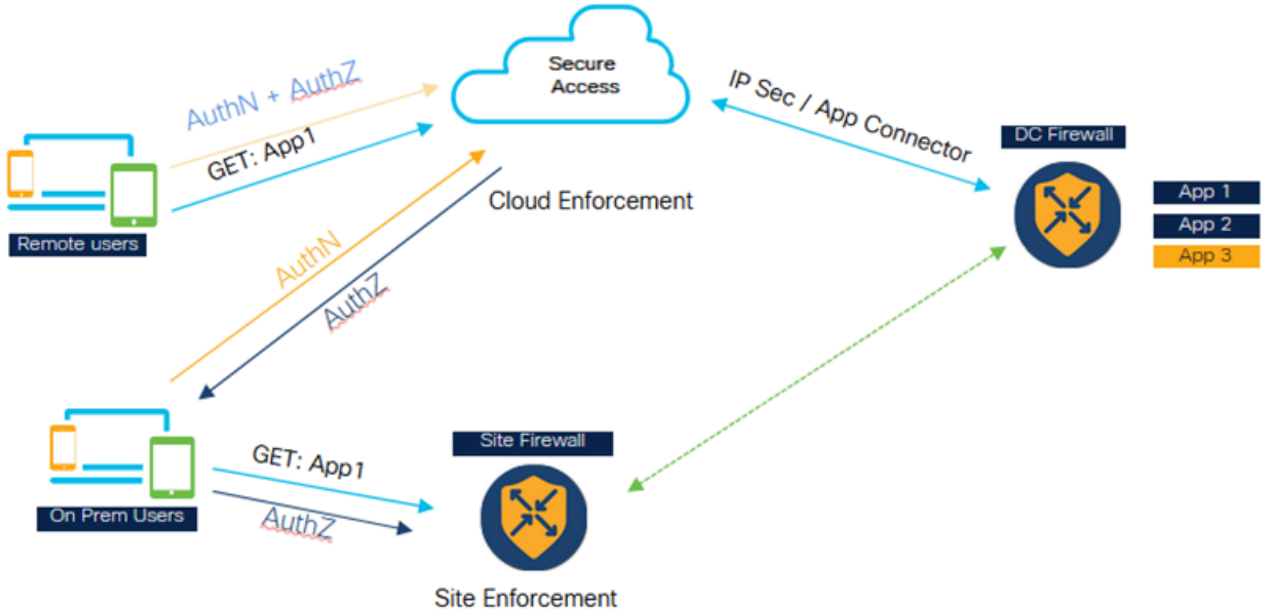


ZTNA universel : Application du cloud

1. Demande utilisateur App, le client capture et résout la demande en IP éphémère (plage d'hôtes locaux)
2. Le trafic est acheminé vers le proxy Zero Trust dans Secure Access
3. La connexion TCP est mise en proxy et créée sur le connecteur de ressources mappé. La stratégie est appliquée au trafic
4. La passerelle établit la connexion au connecteur de ressources
5. Le connecteur de ressource résout l'IP de ressource
6. Le DNS local répond avec l'adresse IP de la ressource
7. Le connecteur de ressource établit la connexion à la ressource

Scénarios :

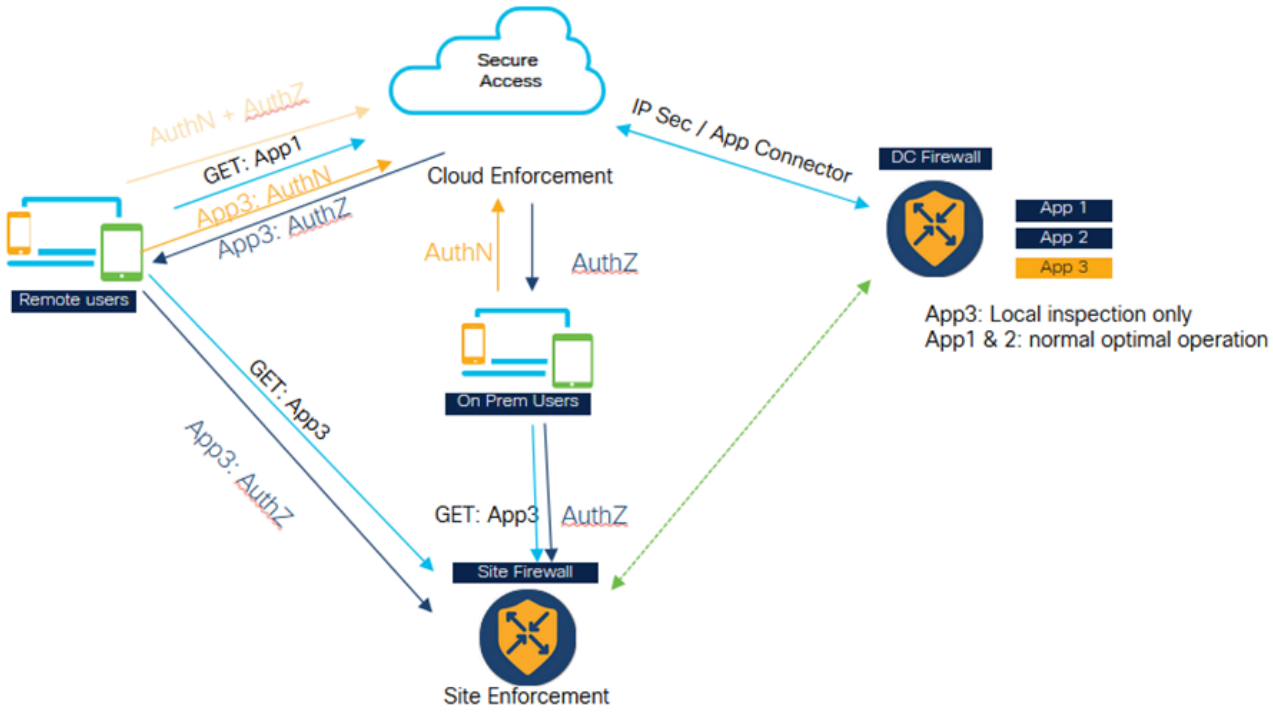
Cas 1 : ZTNA cohérent et optimisé pour les utilisateurs sur site



ZTNA universel : ZTNA cohérent et optimisé (utilisateur sur site)

- L'accès sécurisé et le pare-feu sont configurés pour protéger l'application.
- Si l'utilisateur est distant, il accède à Secure Access pour l'évaluation et l'inspection des politiques.
- Si l'utilisateur est interne/sur site, il accède au pare-feu pour l'inspection du trafic privé.
- Sur site, l'utilisateur peut toujours accéder à Secure pour l'authentification et l'évaluation, juste le trafic Datapath est acheminé vers le pare-feu et inspecté selon la configuration de la stratégie.
- L'utilisateur interne qui accède à l'application via le pare-feu bénéficie d'un avantage en termes de performances, car il évite le trafic vers le cloud, puis le réacheminement vers le data center

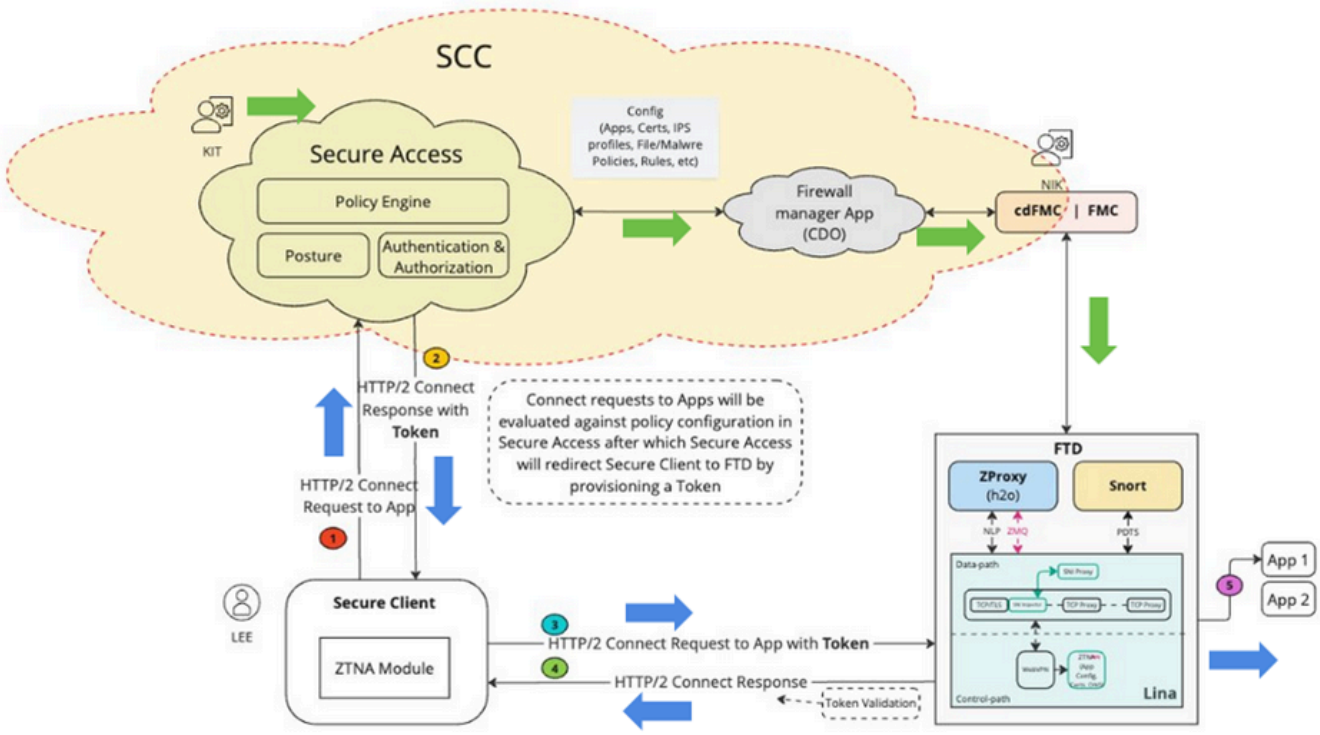
Cas 2 : Inspection privée pour les applications sensibles



Universal ZTNA - Inspection privée pour applications sensibles

- Certaines applications critiques peuvent être configurées pour être toujours accessibles via le pare-feu.
- Le trafic de données d'application n'a pas besoin d'aller dans le cloud. Par exemple, il peut y avoir une application de données sensibles comme le code source, que le client ne veut pas aller dans le cloud.
- Dans de tels scénarios, le trafic des utilisateurs distants et permanents passe toujours par le pare-feu et est inspecté. Cependant, dans ce scénario, l'authentification et l'évaluation des politiques sont toujours en cours dans le cloud, seul le trafic de la partie données passe par le pare-feu.

Composants architecturaux



Universal ZTA - Composants architecturaux

Security Cloud Control (SCC) est le gestionnaire principal de la solution ZuTNA. Zuta est la première fonctionnalité à être construite sur SCC.

Dans SCC , nous avons deux micro-applications Secure Access et Firewall. Une fois que , SCC est configuré et que les indicateurs de fonctionnalité requis sont activés, nous pourrons voir ces micro-applications sur le côté gauche du panneau SCC.

Client sécurisé : Dans le client sécurisé, nous devons activer le module ZTNA (Zero Trust Access Module), nous devons nous inscrire dans le module ZTNA pour pouvoir accéder aux applications.

Protection pare-feu : FTD protégeant ces applications. FTD exécute un proxy ZT également appelé H2O (comme le proxy s'exécute dans le cloud d'accès sécurisé)

Désormais, lorsqu'un utilisateur (par exemple, un KIT) configure une ressource privée et une stratégie sur la micro-application Secure Access, cette configuration est envoyée à la micro-application Firewall dans SCC. L'application de pare-feu comprend les éléments internes du FTD, la configuration du FTD, comment déployer et gérer la configuration sur le FTD. Ainsi, l'application Firewall valide cette configuration et appelle les API FMC pour transmettre la configuration à FMC, puis la déployer sur FTD. L'option de déploiement automatique du FTD peut être activée afin que les administrateurs (par exemple Nick) n'aient pas à effectuer de déploiement manuel.

1. Lorsqu’un utilisateur (par exemple Lee) tente d’accéder à une application, le client sécurisé se connecte à Secure Access via le canal mTLS. Secure Access authentifie l'utilisateur à l'aide du certificat du périphérique client. Il évalue ensuite les autorisations, la position et les autres stratégies configurées pour cet utilisateur et pour cette application.

2. Secure Access, s'il découvre finalement que l'application est protégée par le pare-feu, génère un jeton d'authentification , qui indique au pare-feu qu'il est déjà authentifié et autorisé. Le jeton d'authentification est chiffré et signé par Secure Access

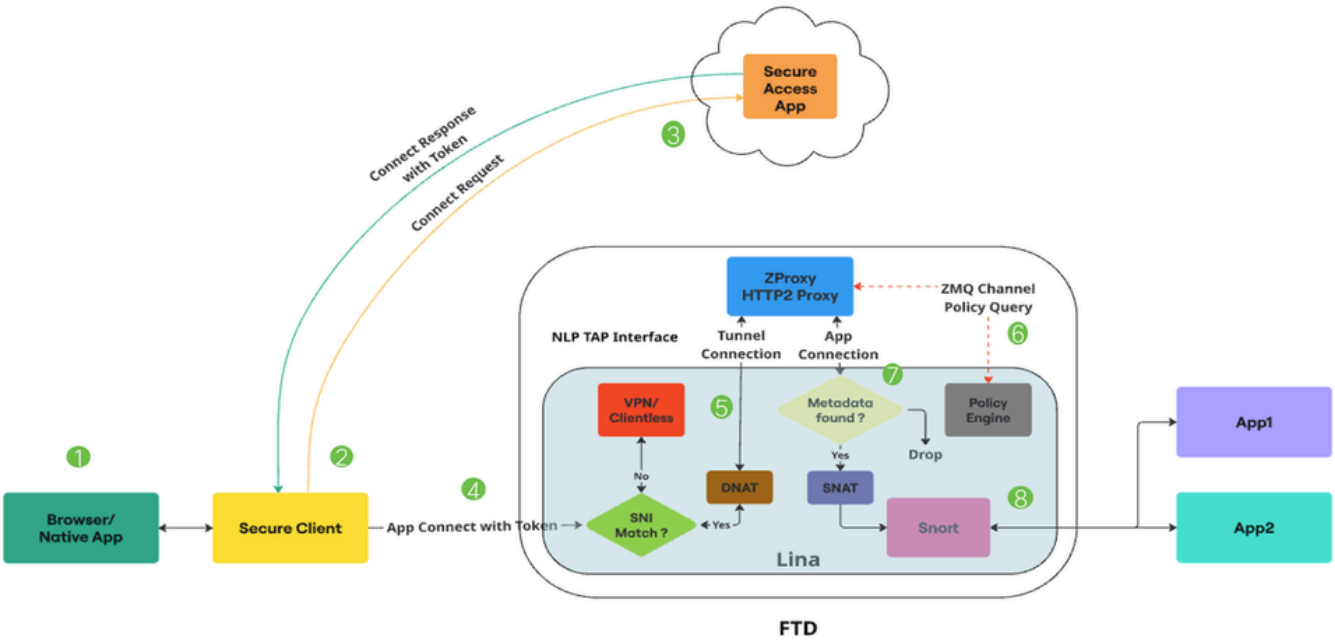
3. Secure Access redirige le client Secure vers FTD avec le jeton d'authentification.

4. Secure Client établit une autre connexion à FTD , il s’agit d’une connexion HTTP2 sur le canal mTLS. Il envoie une requête CONNECT pour l'application en cours d'accès avec le jeton.

5. FTD valide maintenant le jeton, si le jeton est validé avec succès, l'utilisateur est autorisé à accéder à cette application. FTD renvoie ensuite l’accusé de réception au client sécurisé

Flux de paquets

Flux de paquets ZTNA détaillé universel



Universal ZTA - Flux de paquets

1. L'utilisateur tente d'accéder à une application via un navigateur Web ou une application native.

2. Le client sécurisé intercepte la connexion et l'identifie comme un utilisateur essayant d'accéder à une ressource privée.

3. Le client sécurisé établit une connexion mTLS à l'accès sécurisé, demandant l'accès à l'application.L'accès sécurisé vérifie la conformité aux stratégies ZTNA universelles et aux profils de posture.Si tout va bien, l'accès sécurisé génère un jeton d'accès contenant des informations essentielles telles que les détails utilisateur, les détails de l'application et la stratégie IPS/File.

4. Le jeton d'accès est chiffré et signé par Secure Access. Secure Access redirige ensuite le client sécurisé avec le jeton vers le FTD.

5. Lorsque le paquet atteint le chemin de données Lina, le contrôleur SNI intercepte la connexion et vérifie si le nom du serveur (extension SNI) dans le paquet Hello du client correspond au nom de domaine complet du proxy configuré sur le périphérique.Si SNI correspond, la connexion est dirigée vers ZProxy. Si SNI ne correspond pas, la connexion est dirigée vers d'autres fonctionnalités qui peuvent coexister avec Universal ZTNA.

Exemple : VPN, Captive Portal ou ZTNA sans client. ZProxy, qui prend en charge le protocole MASQUE sur HTTP/2, s'exécutera sur le FTD en tant que processus non-Lina sur des coeurs dédiés. La communication entre Lina et ZProxy utilise l'interface NLP Tap pour gérer le trafic de données.L'adresse IP de destination de la connexion est traduite en adresse IP d'interface TAP par le contrôleur SNI.

6. Lorsque le ZProxy reçoit la connexion de tunnel mTLS du client sécurisé, il vérifie le certificat de périphérique client envoyé par le client sécurisé. Il vérifie également le jeton d'accès envoyé avec APP Connect. Il y a un canal Zero MQ entre Lina et ZProxy. Il est principalement utilisé pour échanger des messages de contrôle. ZProxy utilise ce canal pour la résolution FQDN des ressources privées en communiquant avec Lina.

Zero MQ Channel est également utilisé pour propager les informations présentes dans le jeton d’accès vers Lina.(Exemple : ID de règle, ID de stratégie, etc.) Lina reçoit les informations de jeton d'accès et les stocke dans une base de données de métadonnées.

7. Une fois les messages de contrôle échangés, ZProxy lance une nouvelle connexion vers la ressource privée. Il peut s'agir de TCP ou UDP. Lina effectue ensuite une recherche de base de données de métadonnées pour cette connexion d'application. Si les métadonnées sont introuvables, Connection est abandonné

8. Puisque la connexion de l'application provient de ZProxy, elle aura une adresse IP interne (exemple : 169.251.1.2) comme adresse IP source. Il sera traduit en IP de l'interface de sortie FTD, avant de l'envoyer. Lina marque ensuite les flux Universal Zero Trust pour l'inspection Snort uniquement si une stratégie Fichier ou IPS est présente dans le jeton d'accès.L'ID de règle obtenu

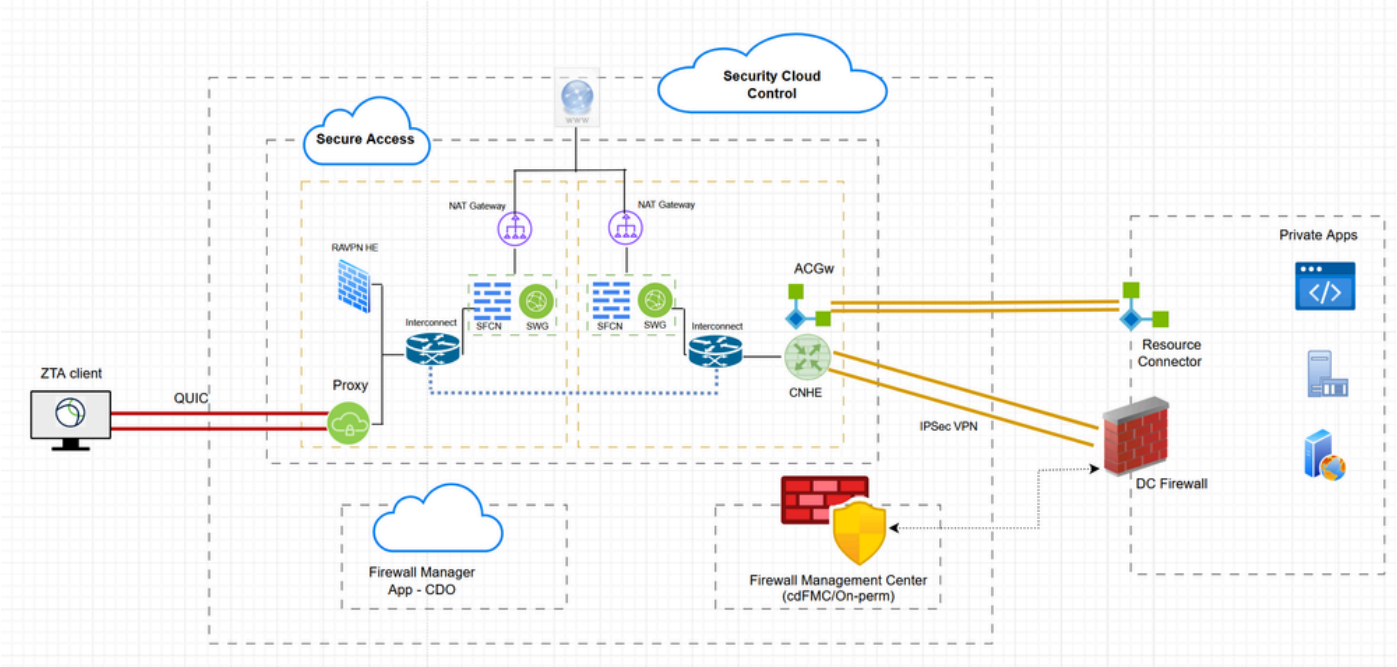
à partir du jeton d'accès est passé à Snort dans les métadonnées de connexion.

9. Les règles d'approbation automatique universelle et les mappages de stratégie de fichier et IPS correspondants sont envoyés au FTD via le FMC. Le plug-in Zero Trust dans Snort chargera ces règles pendant l'initialisation.Lina marquera les flux de flux Universal Zero Trust pour l'inspection Snort uniquement si une stratégie de fichier ou IPS est mentionnée dans le jeton d'accès obtenu à partir de Secure Access pour accéder à cette ressource privée.

L'ID de règle obtenu à partir du jeton d'accès est transmis à Snort via Conn Meta. Pour tous les flux de flux Universal Zero Trust, le plug-in Zero Trust de Snort effectue une recherche de règle pour l'ID de règle obtenu à partir de Conn Meta. Si une correspondance de règle est trouvée, le flux est autorisé et les stratégies IPS et de fichier spécifiques à cette règle sont appliquées au flux. Si aucune correspondance de règle n'est trouvée, le plug-in Zero Trust de Snort bloque le flux.

Configurer

Diagramme du réseau

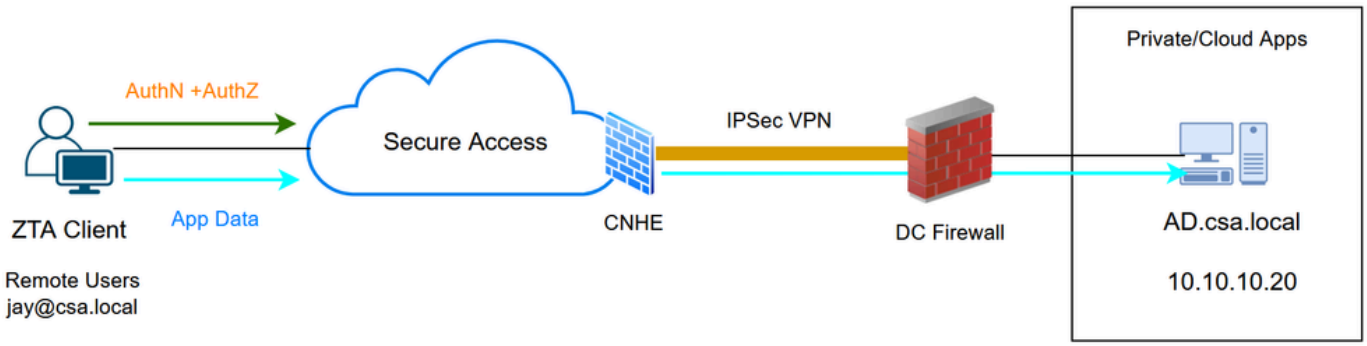


ZTNA hybride - Schéma de réseau

Cas de test

Cas de test 1 : Utilisateur distant - Application du cloud

Dans ce cas de test, nous allons accéder à une ressource privée sur le groupe de tunnels réseau via l'application cloud. Dans ce cas, les données d'évaluation de stratégie et d'application seront interceptées par Secure Access via le module ZTA . Il s'agit d'un flux traditionnel dans lequel une application privée est accessible à partir d'un client inscrit ZTA via un groupe de tunnels réseau ou un connecteur de ressources

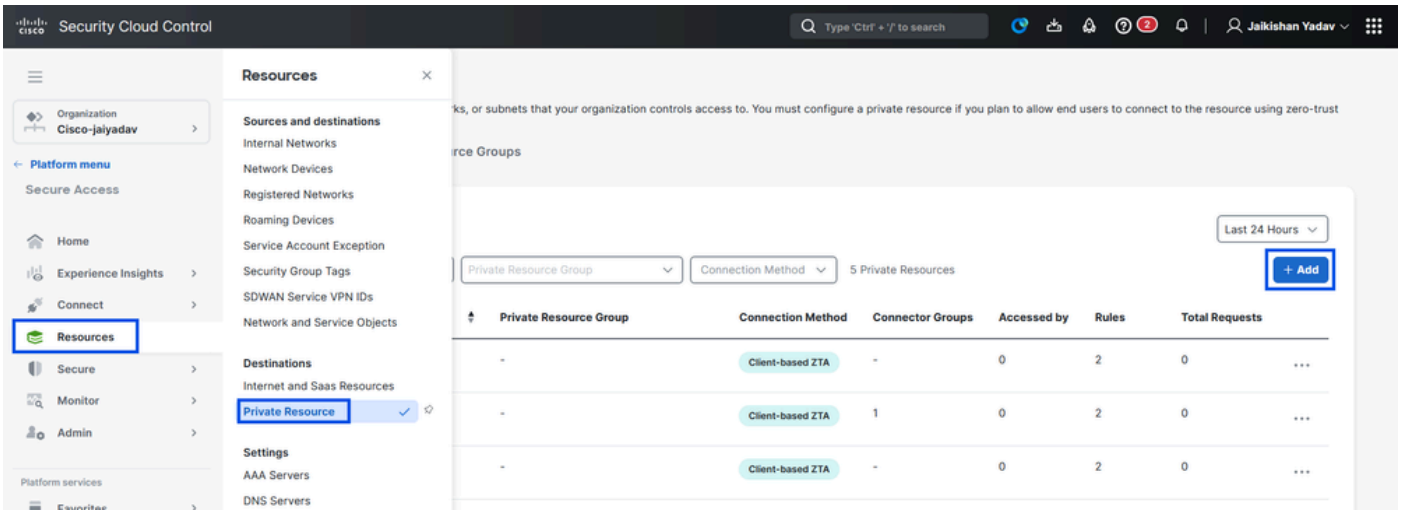


ZTA universel - Topologie du cas de test

Étape 1 : définition d'une ressource privée sur un accès sécurisé

Configurer une ressource privée pour qu'elle soit accessible via un périphérique inscrit ZTA (Zero Trust Access) avec application cloud

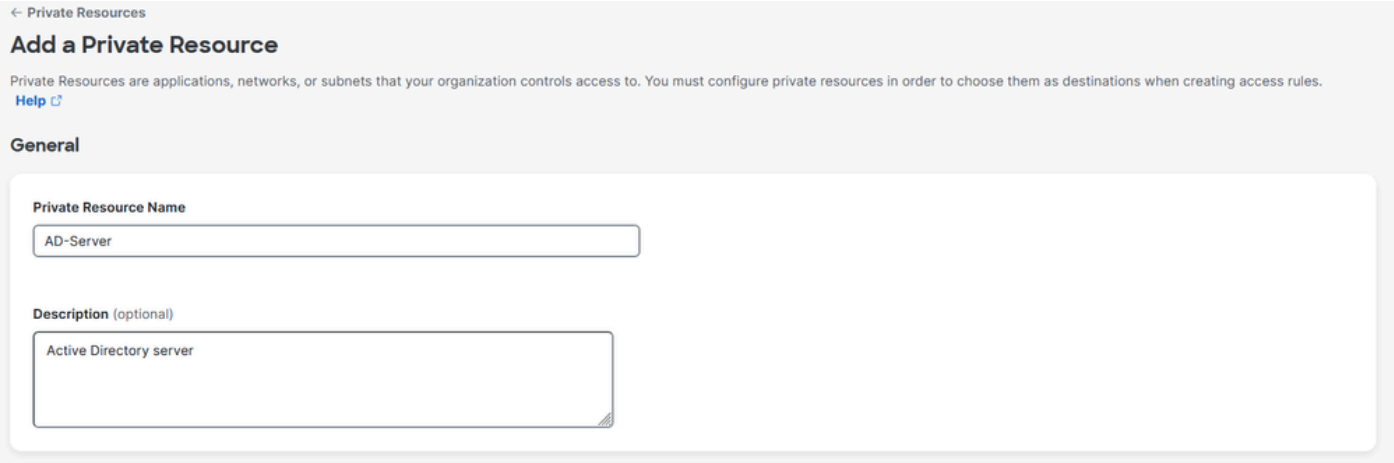
1. Accédez à Ressources > Destinations > Ressources privées > Cliquez sur +Ajouter



Accès sécurisé - Configuration des ressources privées

2. Dans le champ Nom de la ressource privée, entrez un nom significatif pour la ressource. Pour

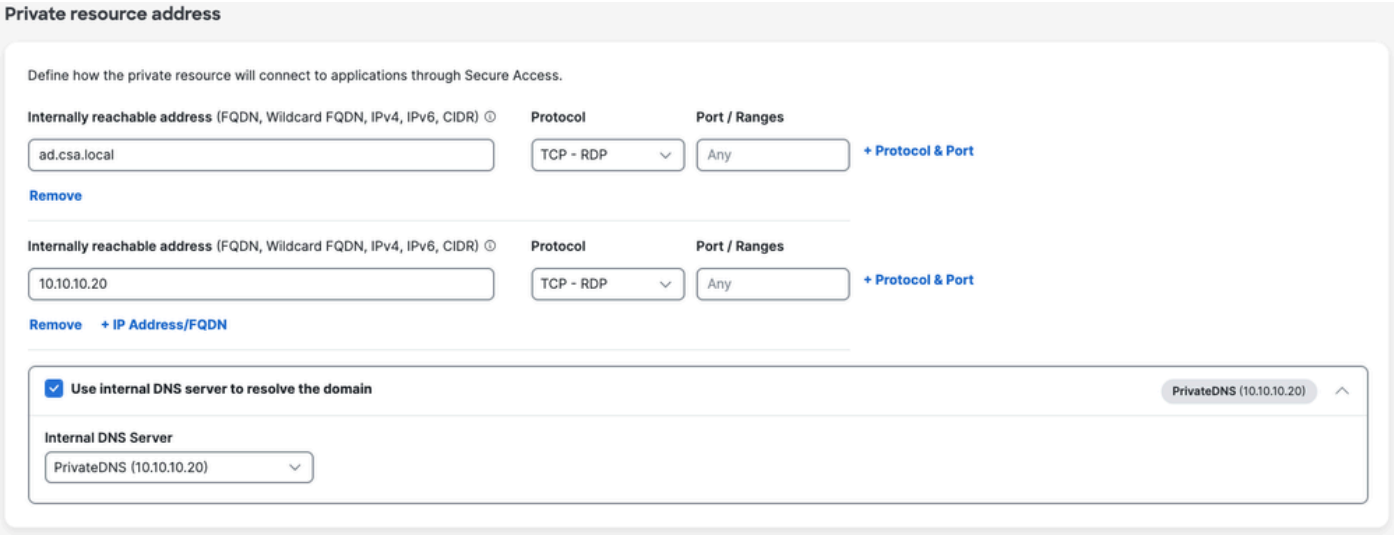
Description, nous vous recommandons de fournir des informations telles que l'objectif de la ressource ou le nom du propriétaire de la ressource.



Accès sécurisé - Configuration des ressources privées

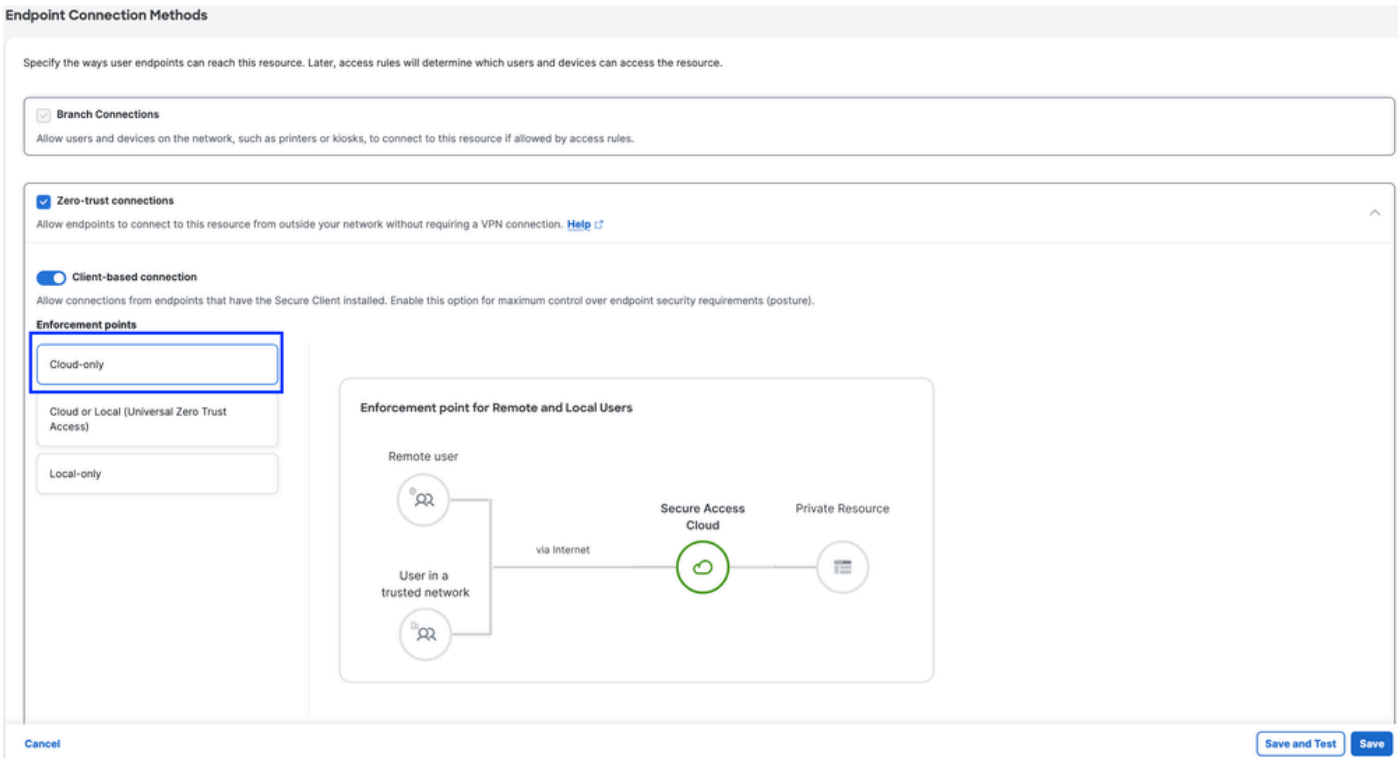
3. Entrez le nom de domaine complet de la ressource privée à laquelle vous souhaitez accéder. Nous pouvons également définir l'adresse IP de la ressource privée . Pour plus d'informations, voir Ajouter une ressource privée

4. Sélectionnez le serveur DNS interne pour résoudre le domaine



Accès sécurisé - Configuration des ressources privées

5. Sélectionner les méthodes de connexion Endpoint



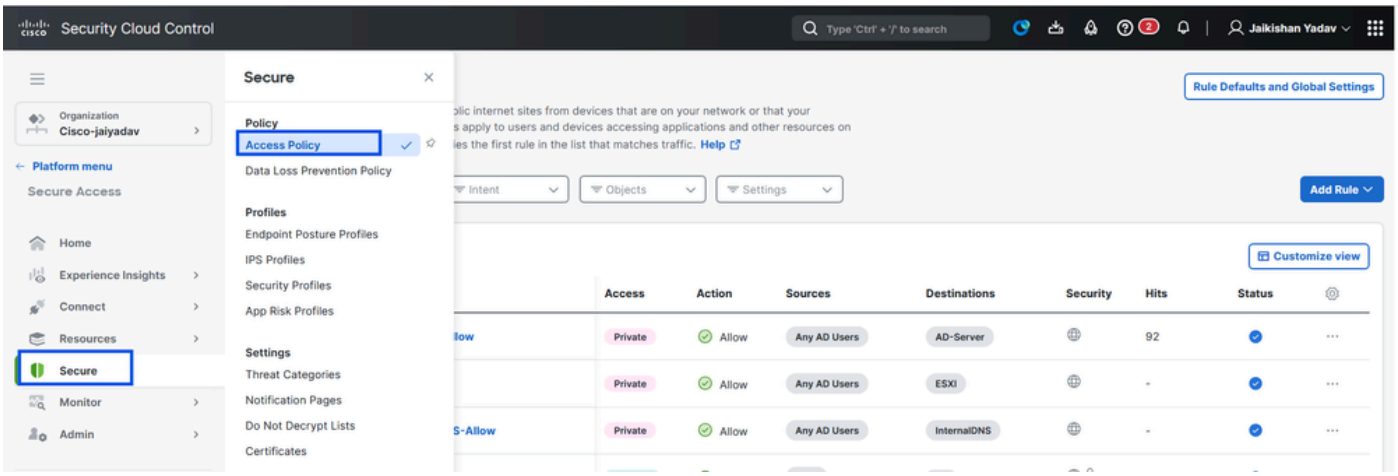
Accès sécurisé - Configuration des ressources privées

6. Cliquez sur Save (enregistrer)

Étape 2 : création d'une règle d'accès privé

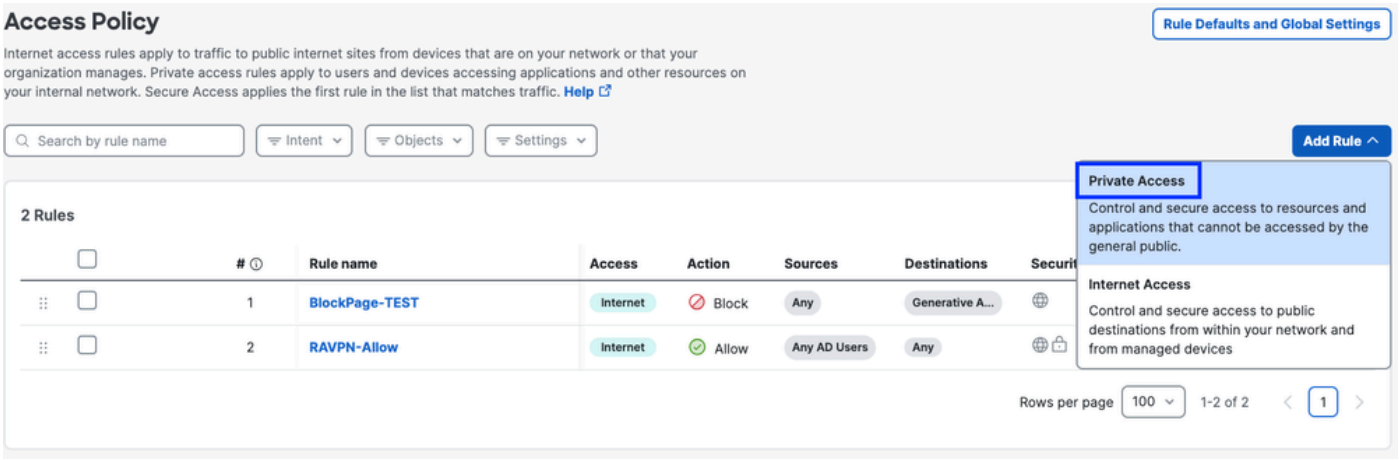
Configurez un accès privé sur Secure Access pour que les utilisateurs inscrits à Universal ZTA puissent y accéder. Pour plus d'informations, consultez Règle d'accès privé

1. Accédez à Secure > Access Policy



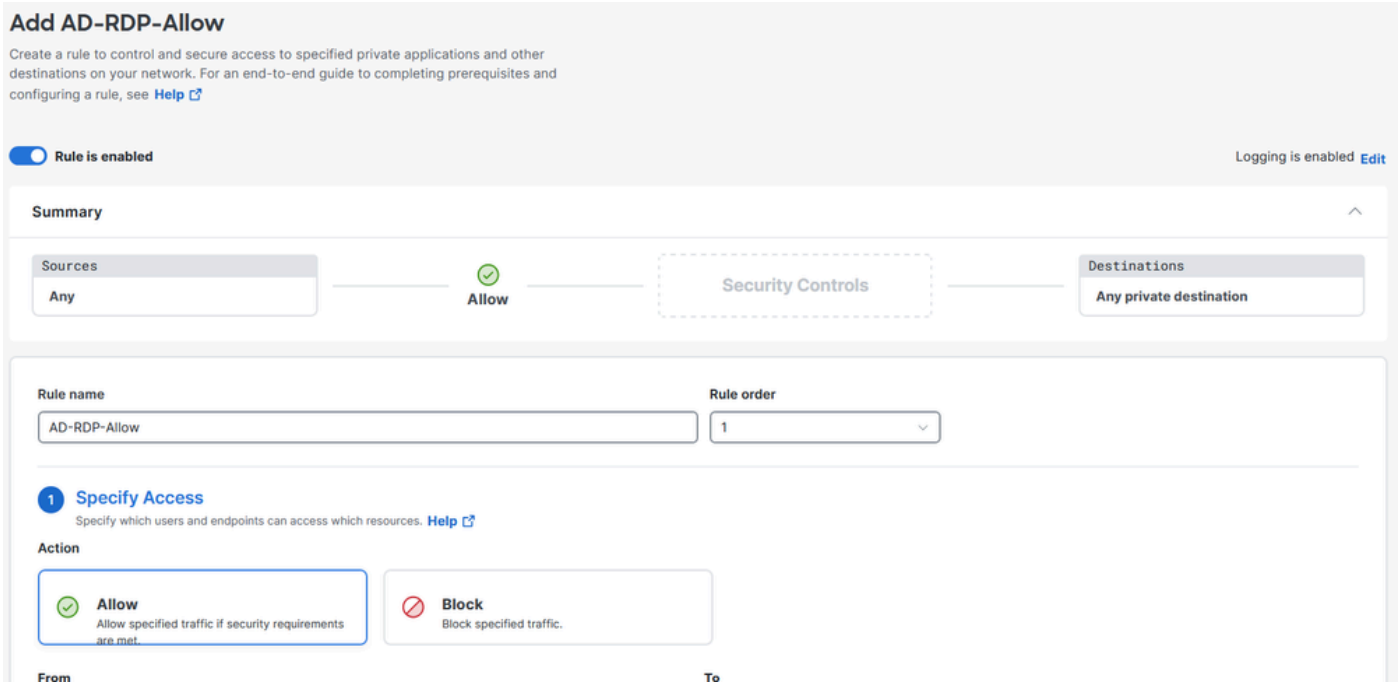
Accès sécurisé - Configuration de la stratégie d'accès

2. Cliquez sur Ajouter une règle, puis choisissez Accès privé.
   En haut de la règle se trouve un résumé qui décrit les composants configurés de votre règle.



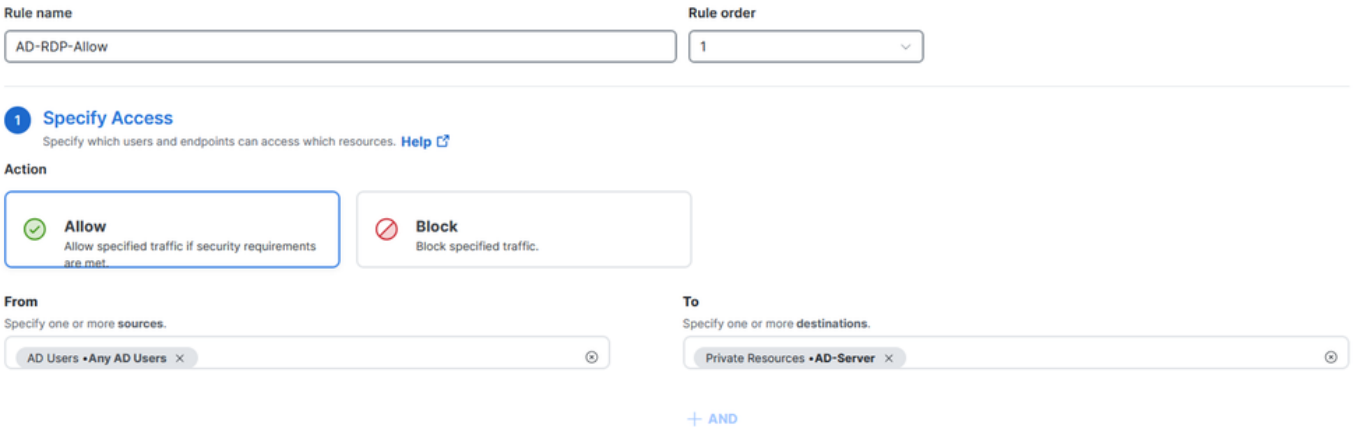
Accès sécurisé - Configuration de la stratégie d'accès

3. Ajouter un nom de règle



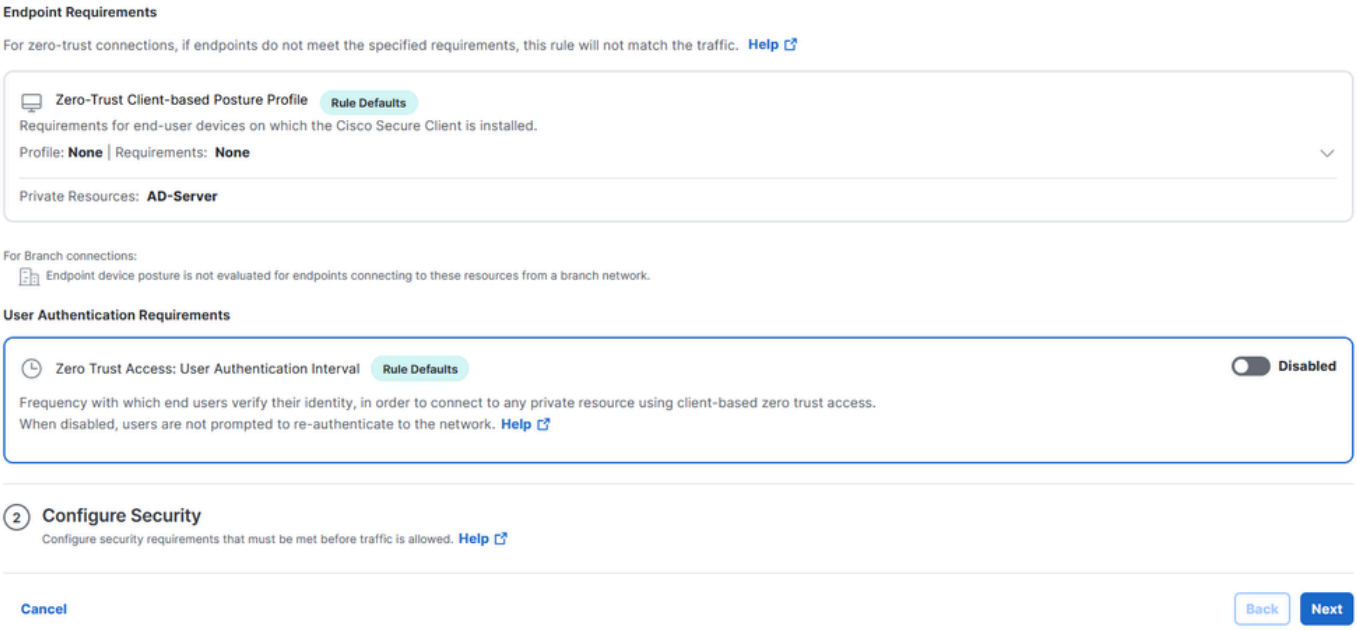
Accès sécurisé - Configuration de la stratégie d'accès

4. Sélectionnez l'action de règle et sélectionnez l'origine et la destination



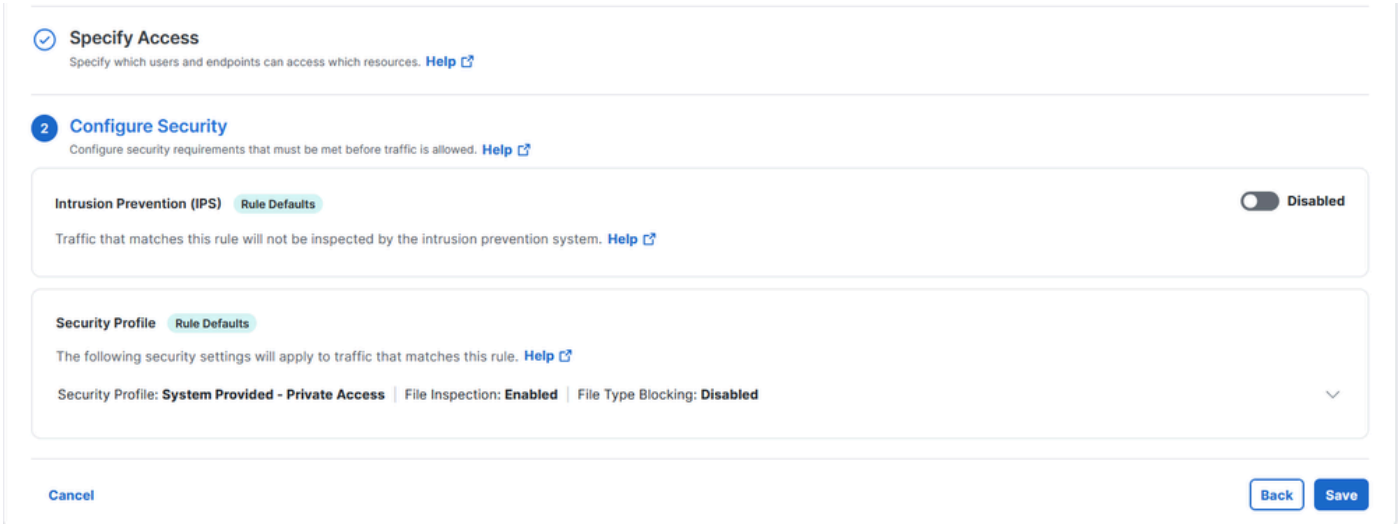
Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux



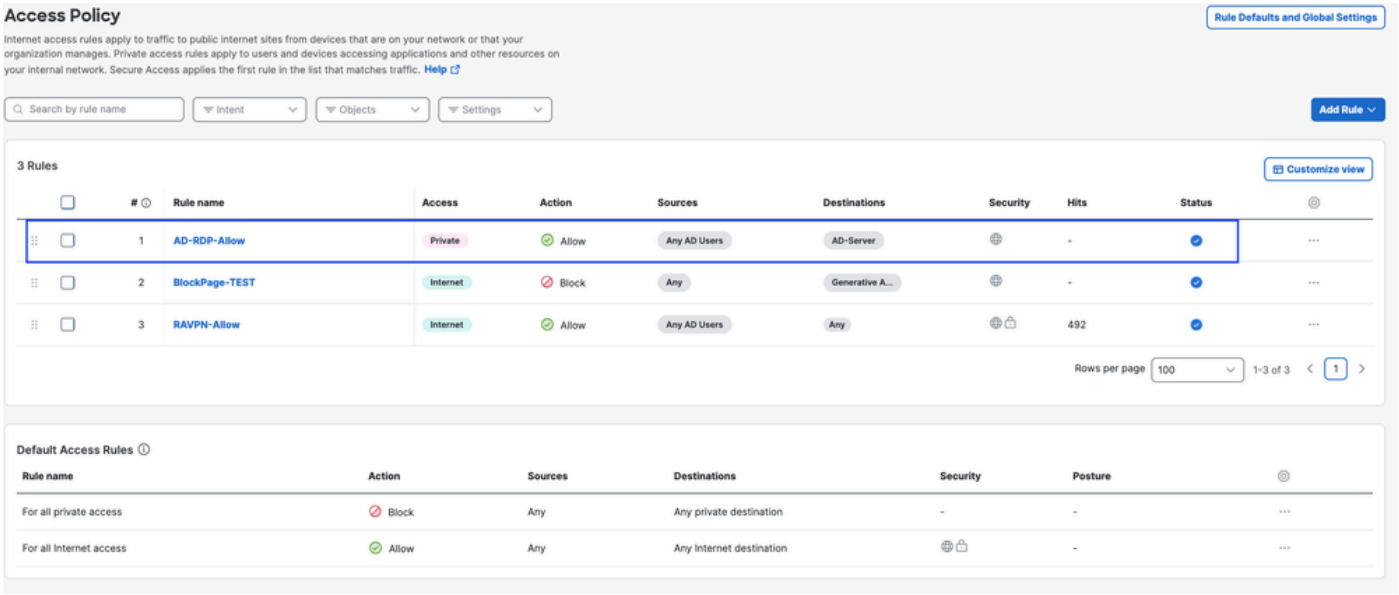
Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité



Accès sécurisé - Configuration de la stratégie d'accès

7. Cliquez sur Enregistrer

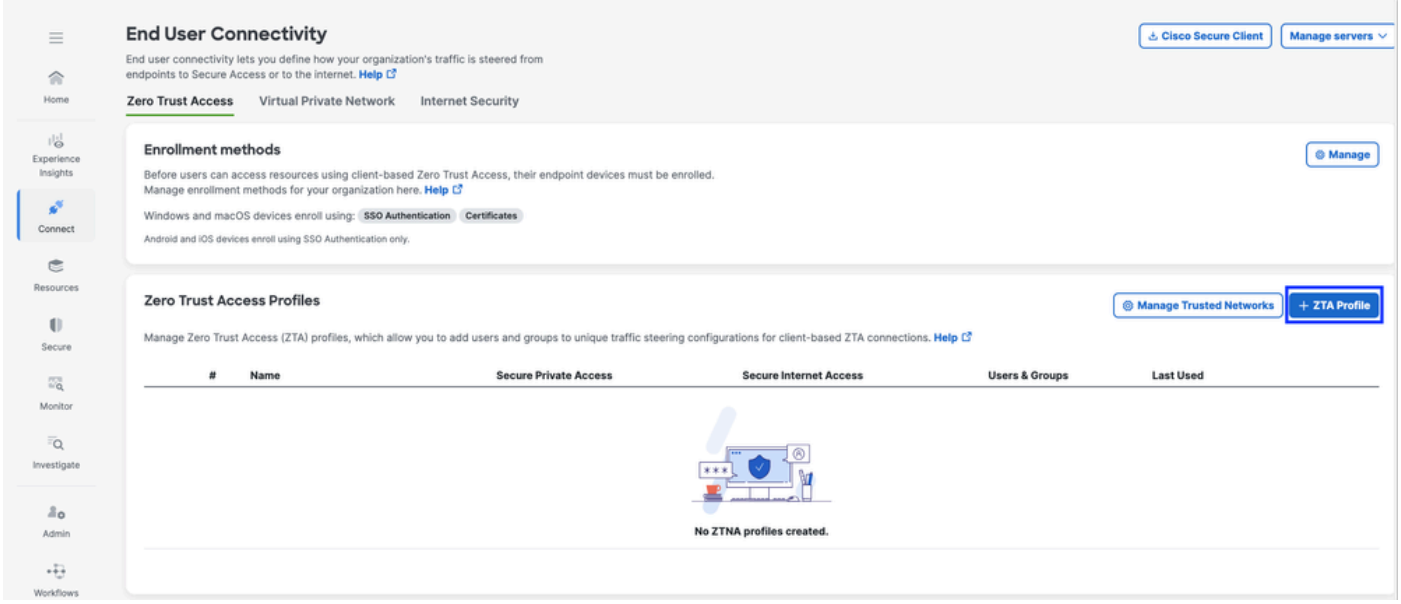


Accès sécurisé - Configuration de la stratégie d'accès

Étape 3 - Ajoutez une ressource privée au profil ZTA

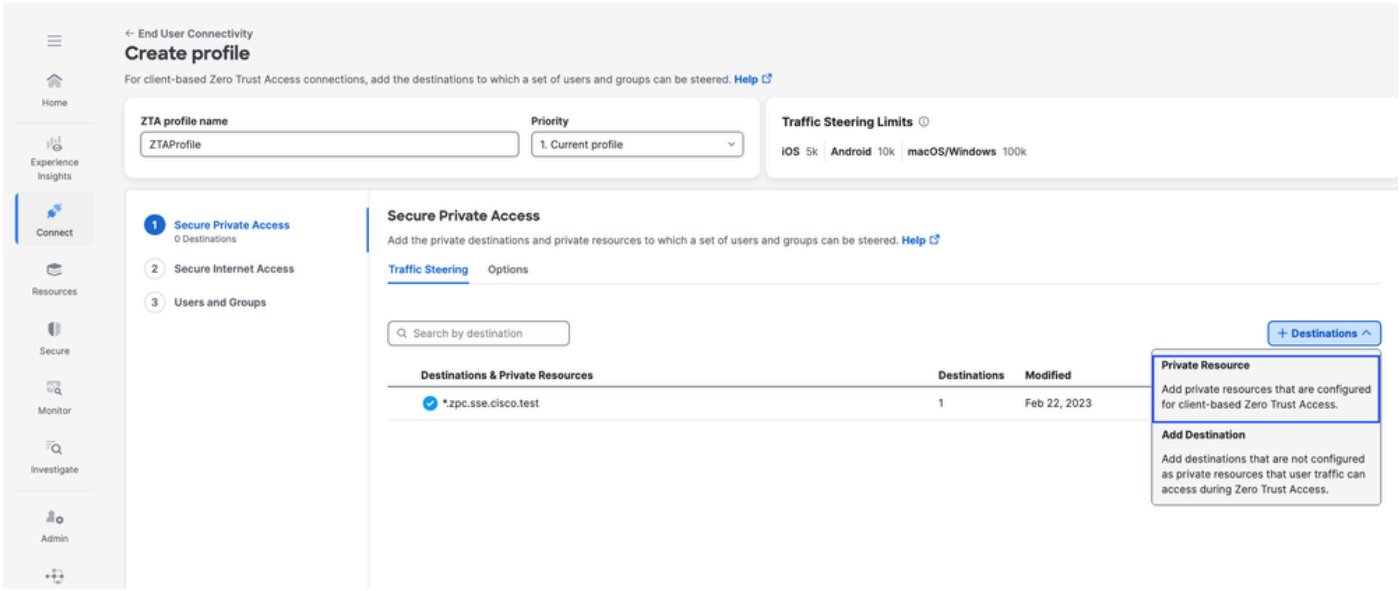
Si vous utilisez un profil ZTA personnalisé, vous devez ajouter la ressource privée correspondante au profil ZTA

1. Accédez à Connect > End User Connectivity > Zero Trust Access et cliquez sur +ZTA Profile

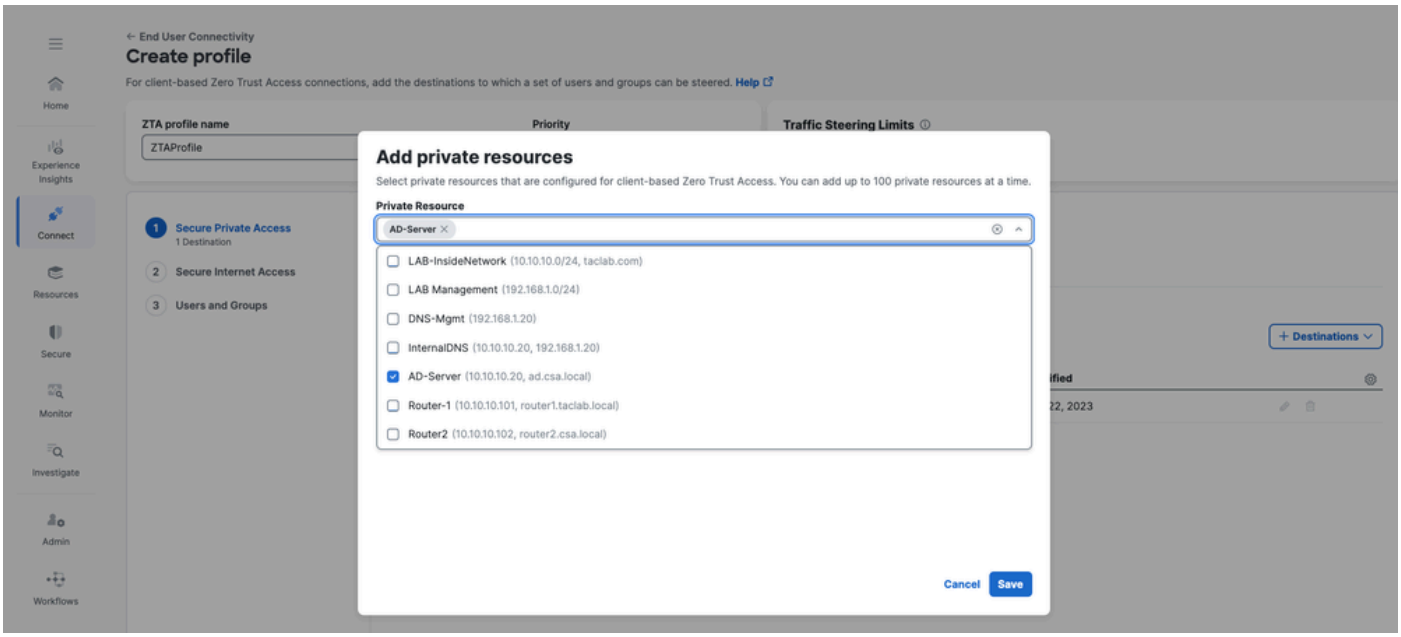


Accès sécurisé - Profil ZTA

2. Ajouter la ressource privée

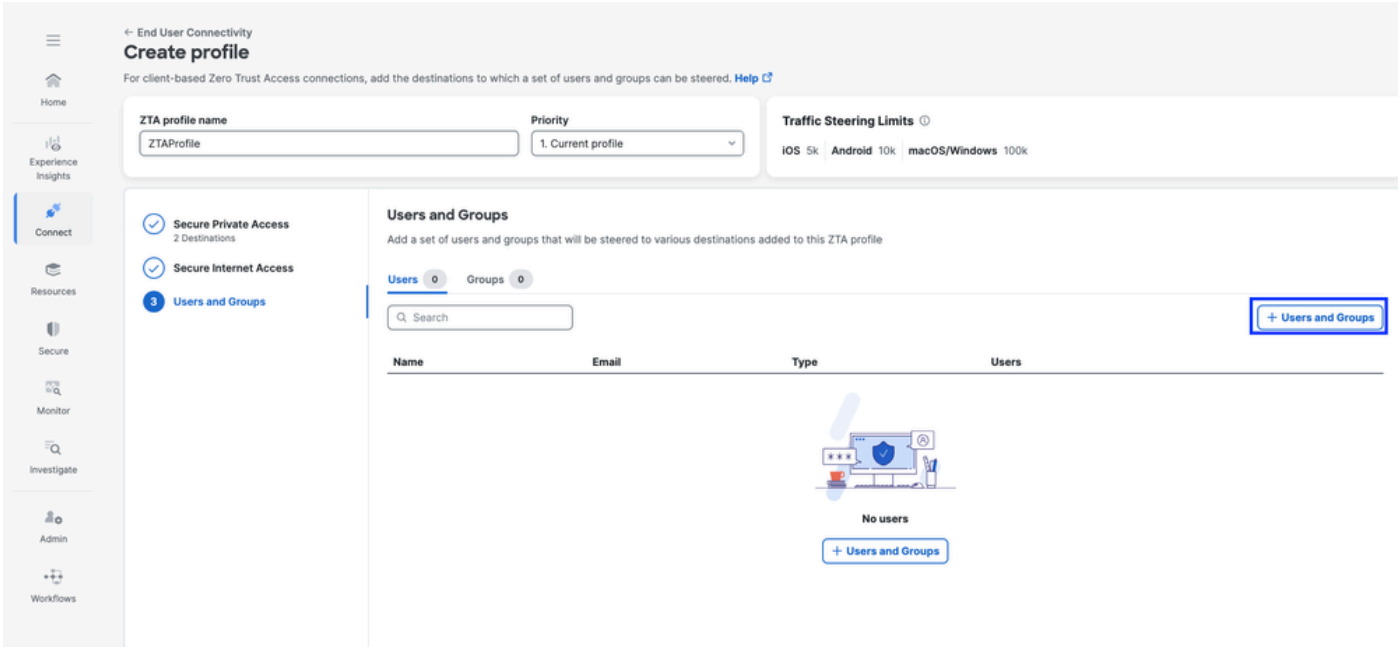


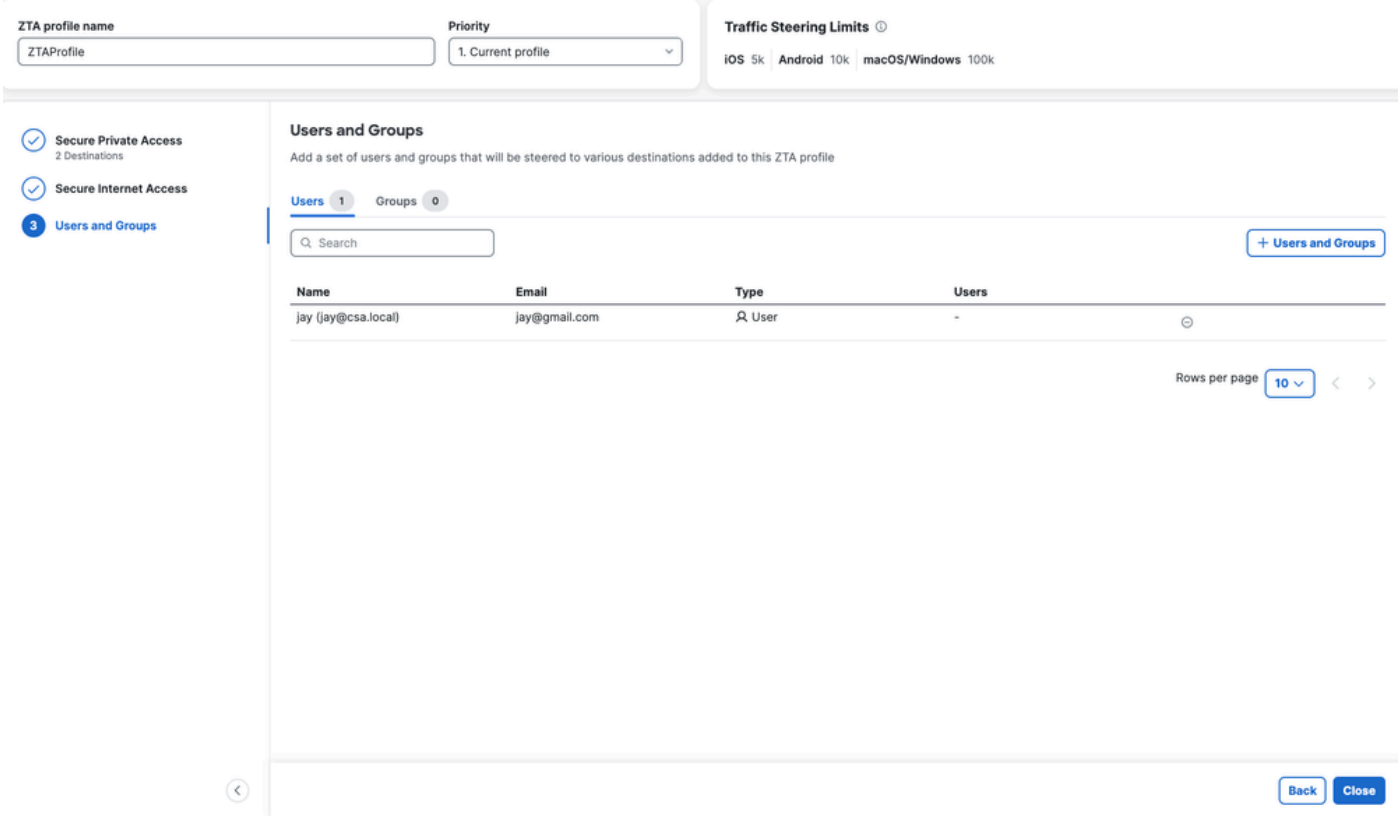
Accès sécurisé - Profil ZTA



Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes





Accès sécurisé - Profil ZTA

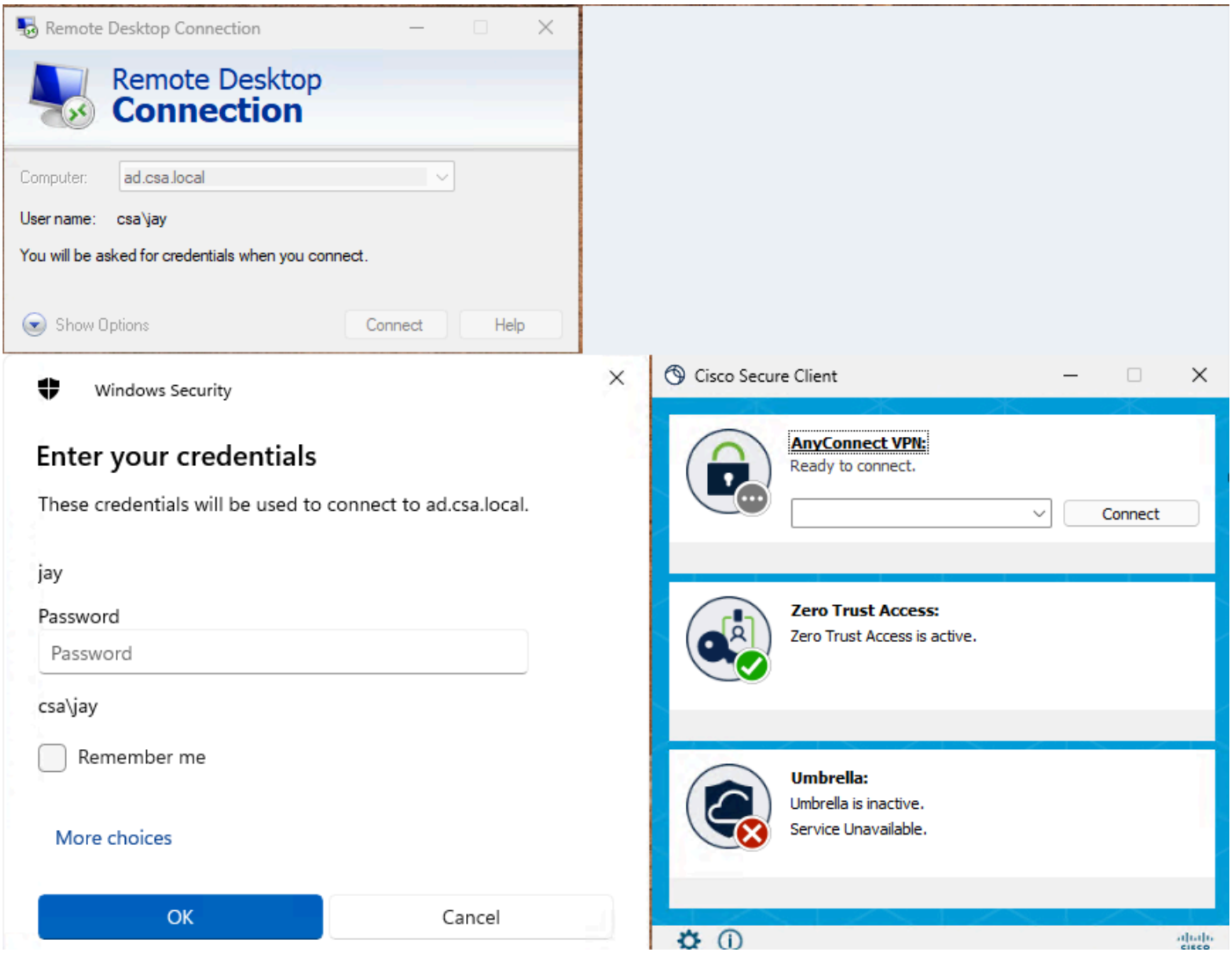
Remarque : La transmission et la synchronisation de la configuration au client pour la ressource privée attribuée peut prendre de 15 à 20 minutes

---

Étape 4 - Vérifiez l’accès à la ressource privée

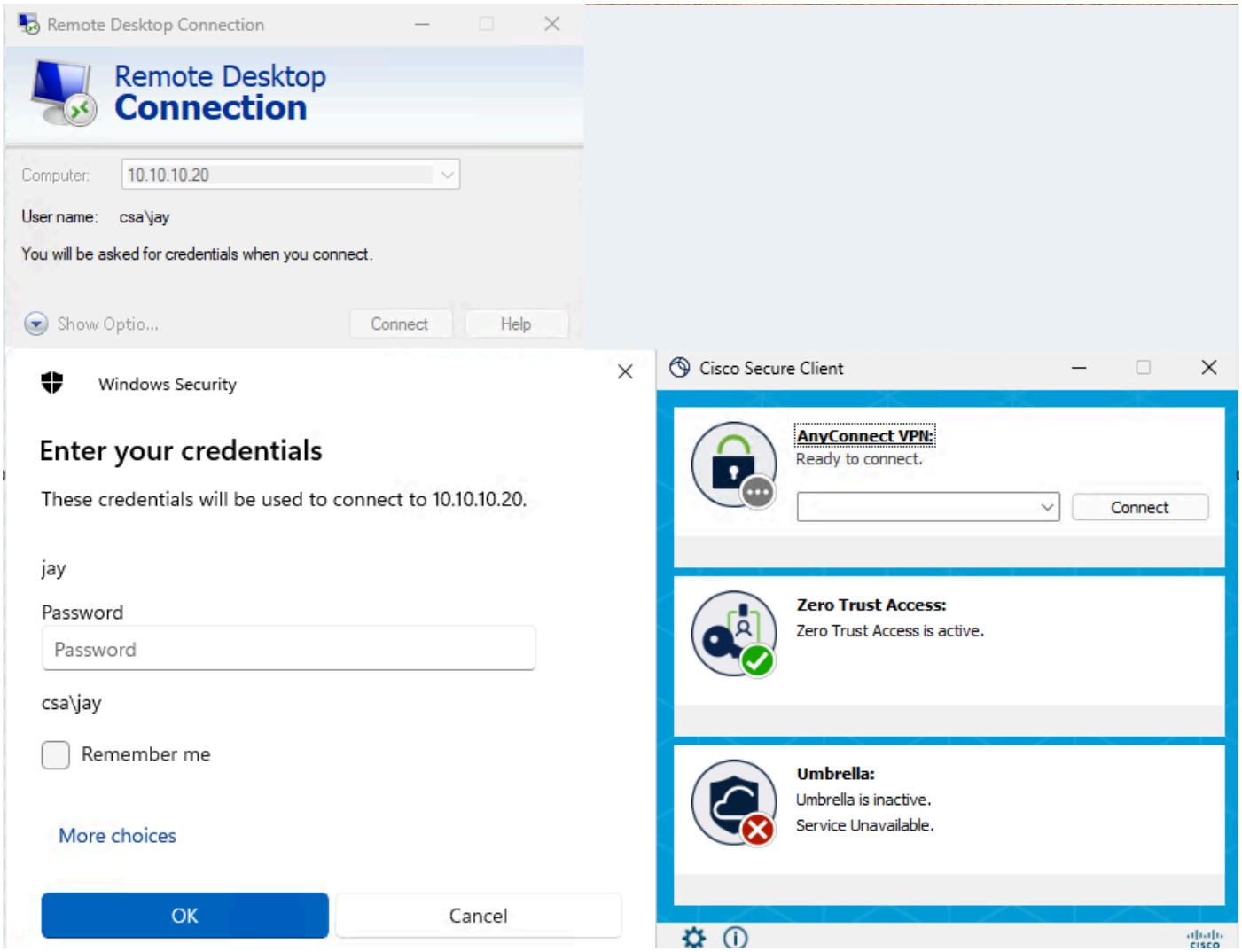
1. Accéder à la ressource privée

Accéder au RP à l'aide du FQDN



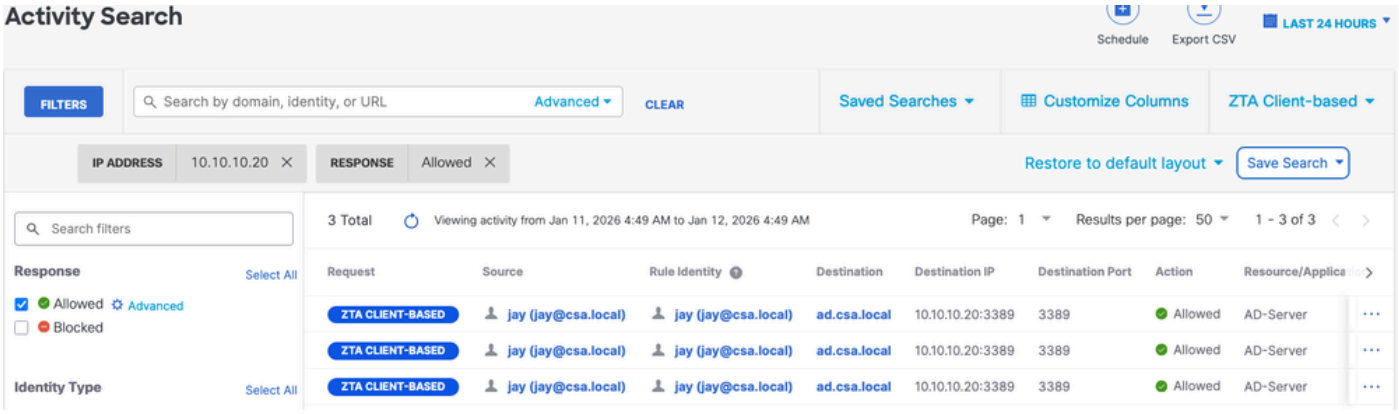
Accès sécurisé - Test PR

Accéder au RP en utilisant l'adresse IP

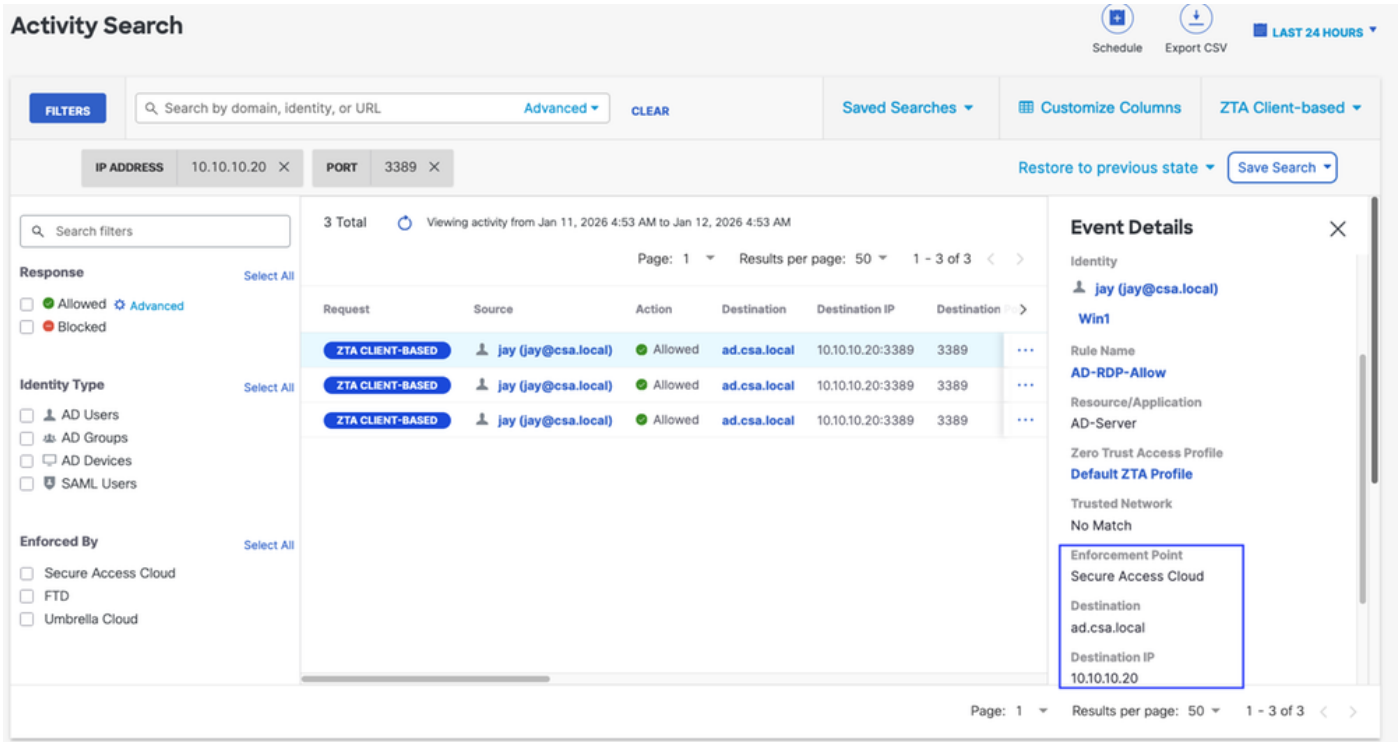


Accès sécurisé - Test PR

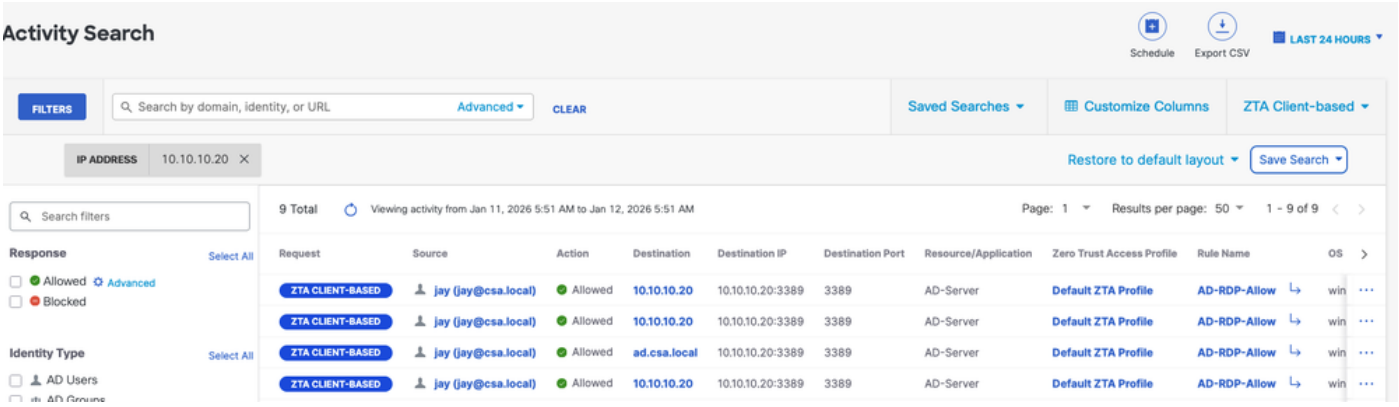
2. Vérifiez avec les événements de recherche d'activité



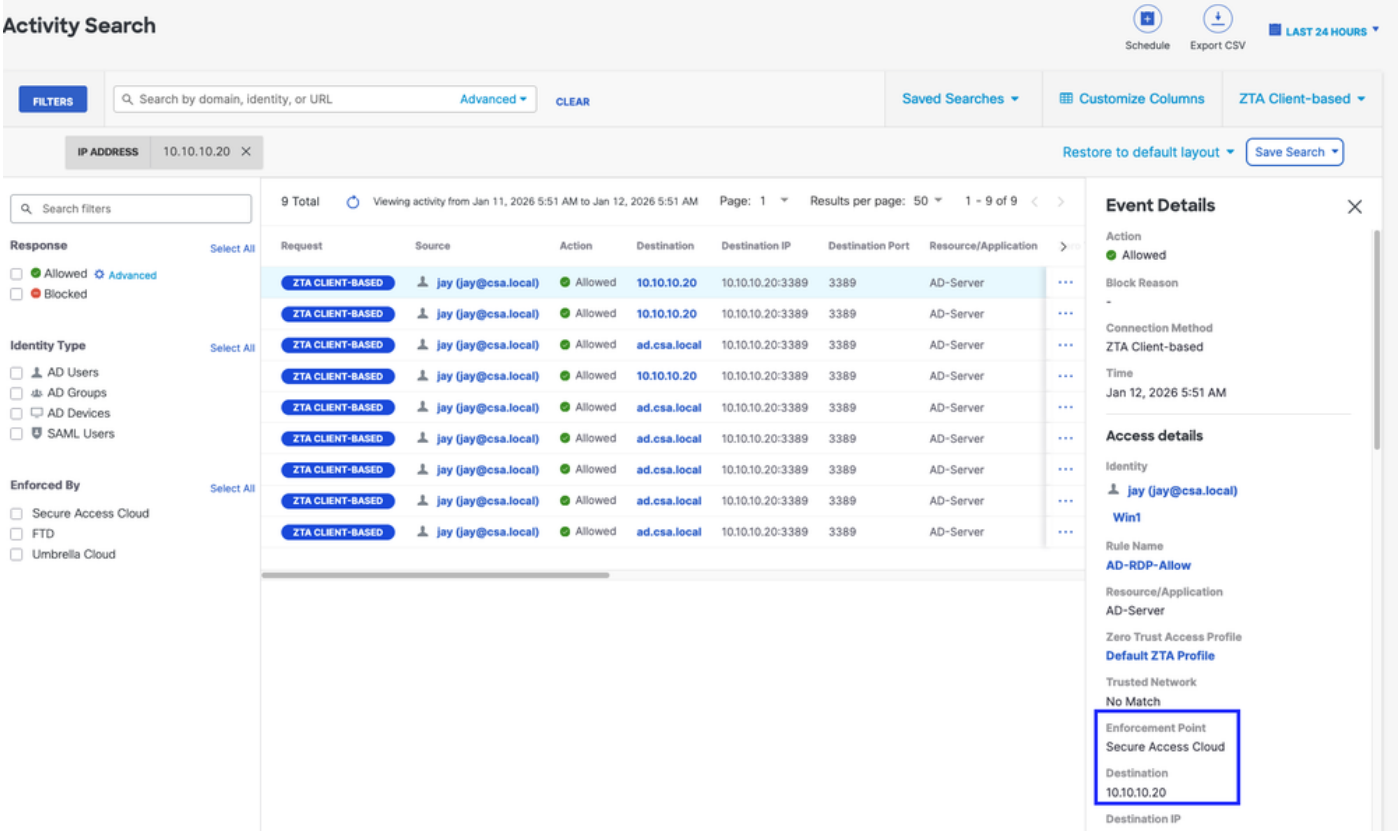
Accès sécurisé - Recherche d'activité



Accès sécurisé - Recherche d'activité

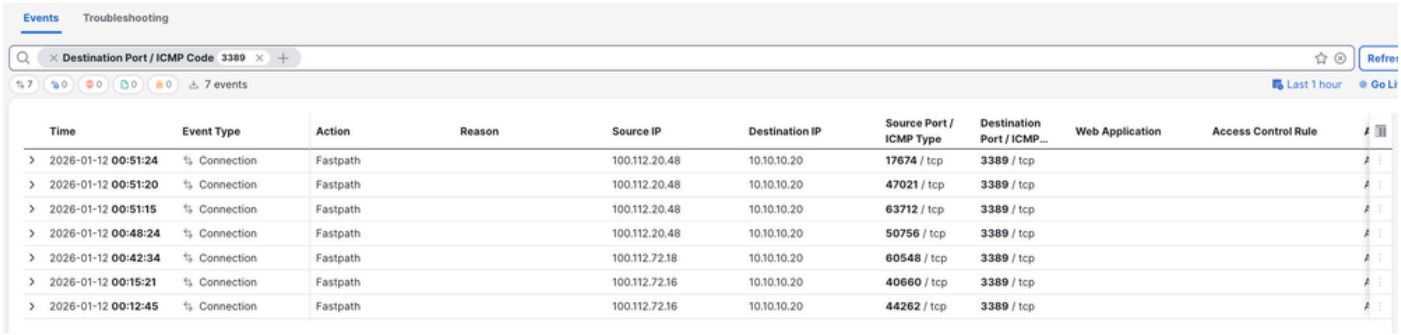


Accès sécurisé - Recherche d'activité



Accès sécurisé - Recherche d'activité

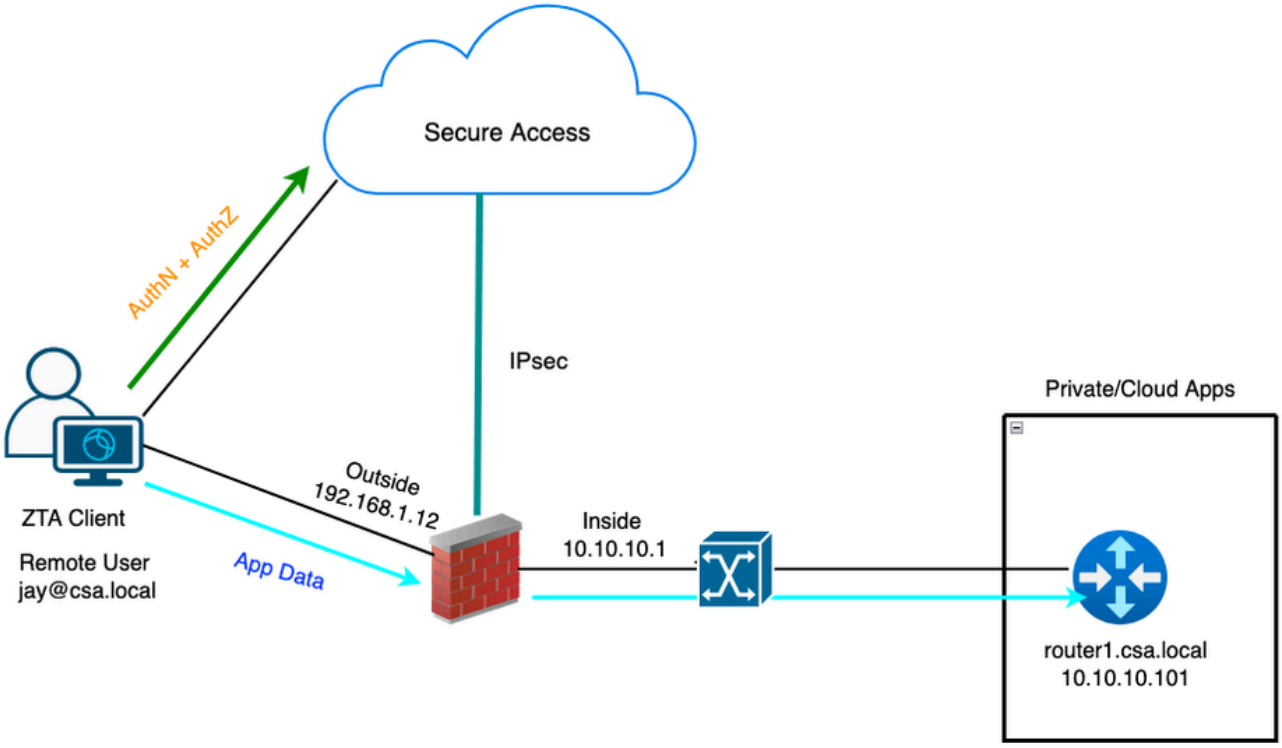
3. Vérifiez les événements de connexion FMC



Événements de connexion FMC

Cas de test 2 - Utilisateur distant - Application locale

Accès à une ressource privée via l'application locale , dans ce type d'évaluation de stratégie d'application se produit sur l'accès sécurisé mais les données d'application restent locales à FTD. Par exemple , un client ou un utilisateur inscrit ZTA connecté au réseau domestique et essayant d' accéder à une ressource privée qui se trouve derrière l' interface interne FTD .

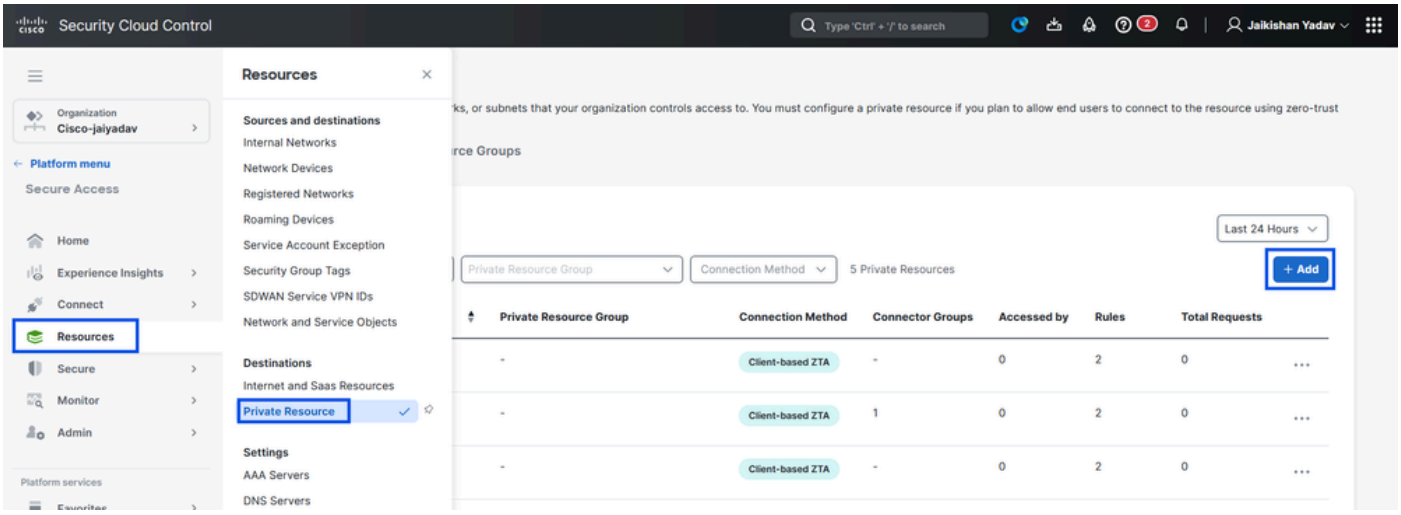


ZTA universel - Topologie du cas de test

Étape 1 : définition d'une ressource privée sur un accès sécurisé

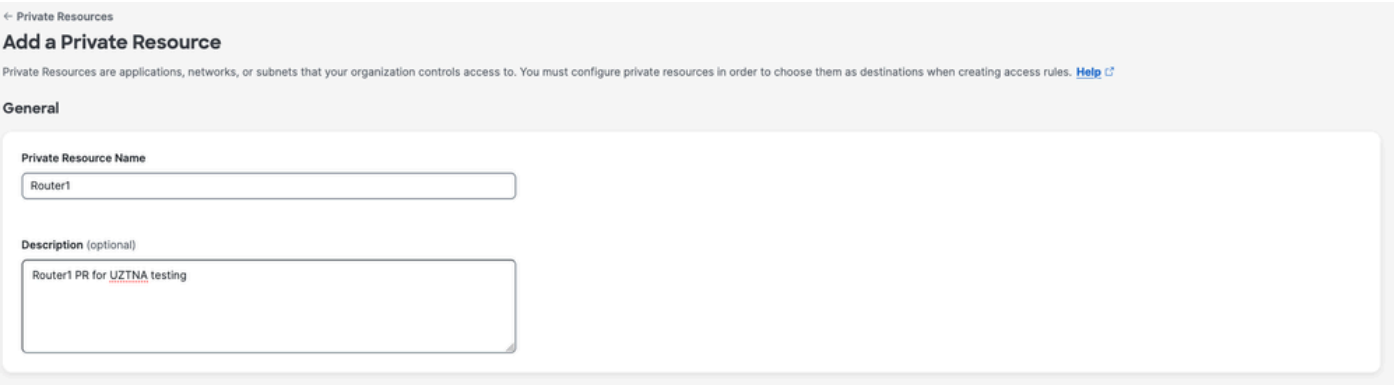
Configurer une ressource privée pour qu'elle soit accessible via un périphérique inscrit ZTA (Zero Trust Access) avec application cloud

1. Accédez à Ressources > Destinations > Ressources privées > Cliquez sur +Ajouter



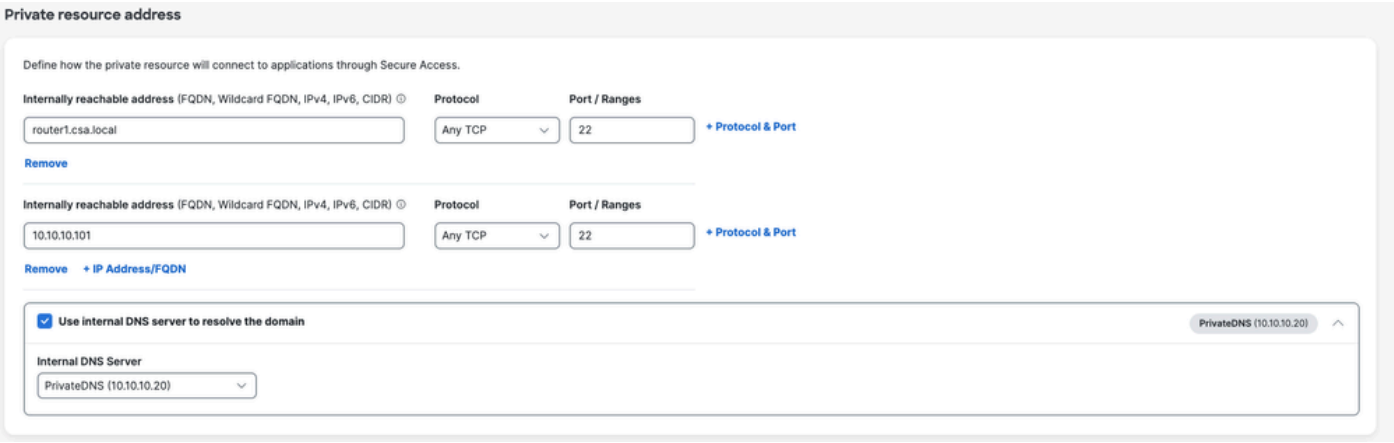
Accès sécurisé - Configuration des ressources privées

2. Dans le champ Nom de la ressource privée, entrez un nom significatif pour la ressource. Pour Description, nous vous recommandons de fournir des informations telles que l'objectif de la ressource ou le nom du propriétaire de la ressource.



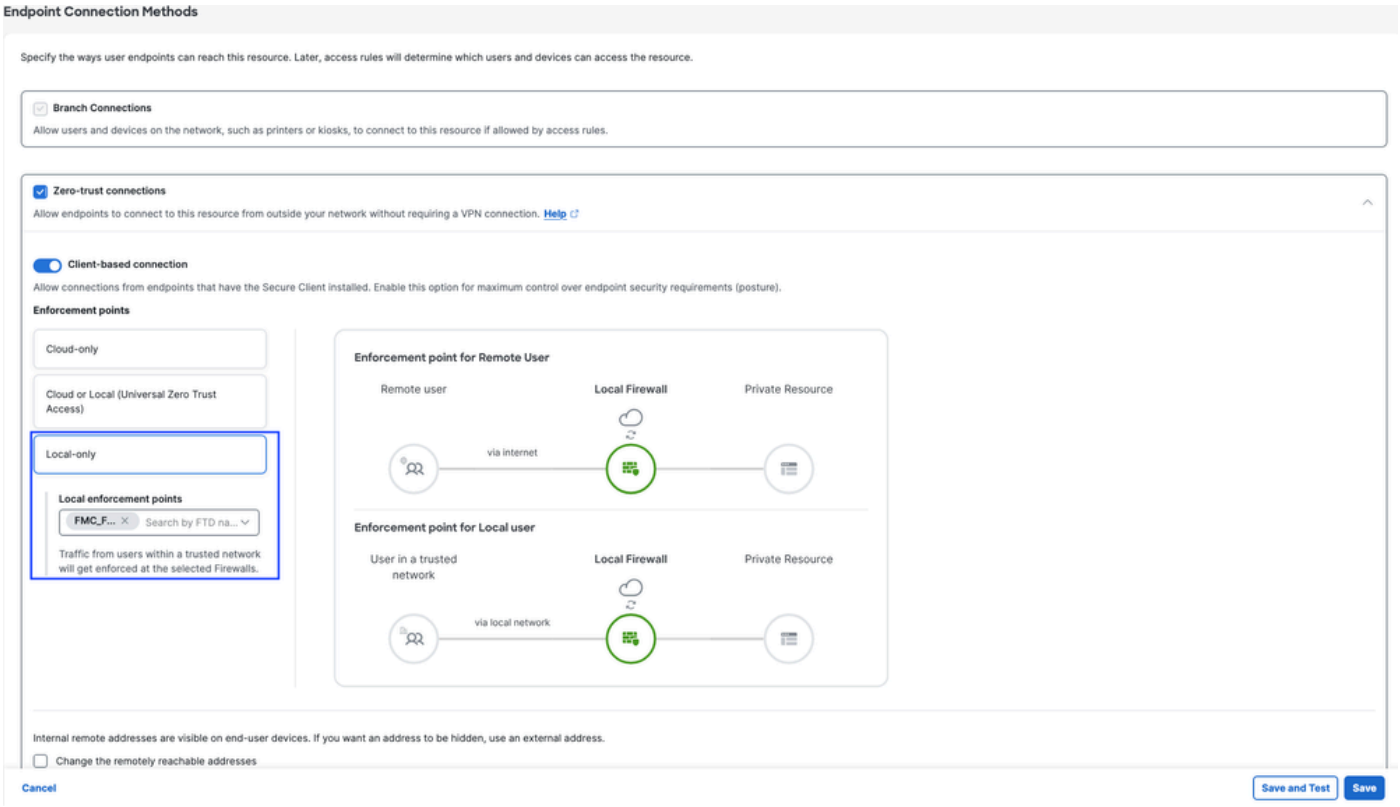
3. Entrez le nom de domaine complet de la ressource privée à laquelle vous souhaitez accéder. Nous pouvons également définir l'adresse IP de la ressource privée . Pour plus d'informations, voir Ajouter une ressource privée

4. Sélectionnez le serveur DNS interne pour résoudre le domaine



5. Sélectionner les méthodes de connexion Endpoint

6. Sélectionnez FTD comme points d'application locaux



Accès sécurisé - Configuration des ressources privées

Remarque : Selon le type d'inscription sélectionné, cette modification associera automatiquement le PR au FTD et déclenchera un déploiement de stratégie

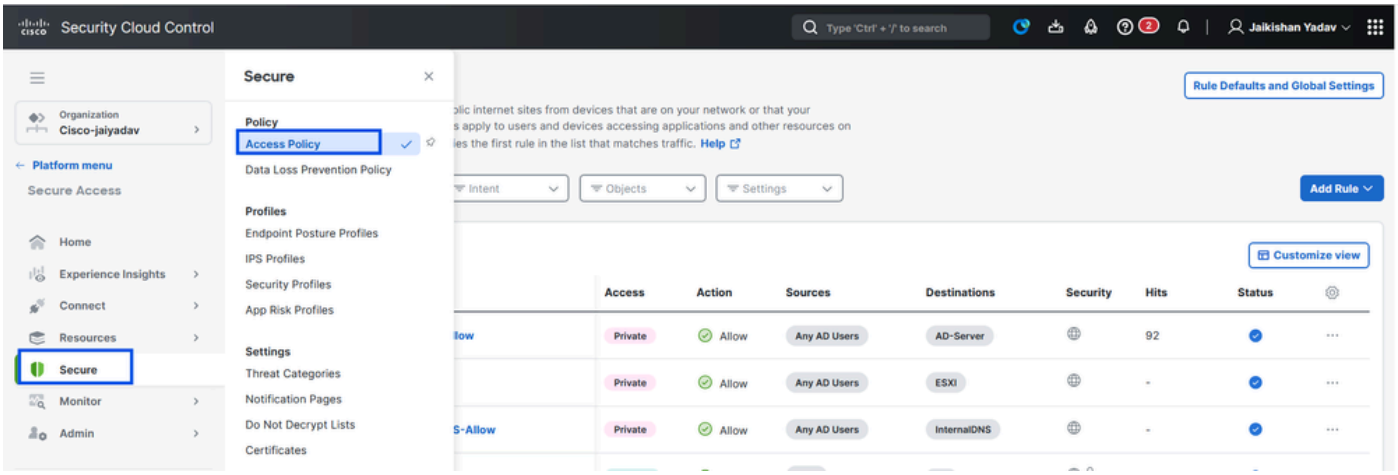
---

7. Cliquez sur Save (enregistrer)

Étape 2 : création d'une règle d'accès privé

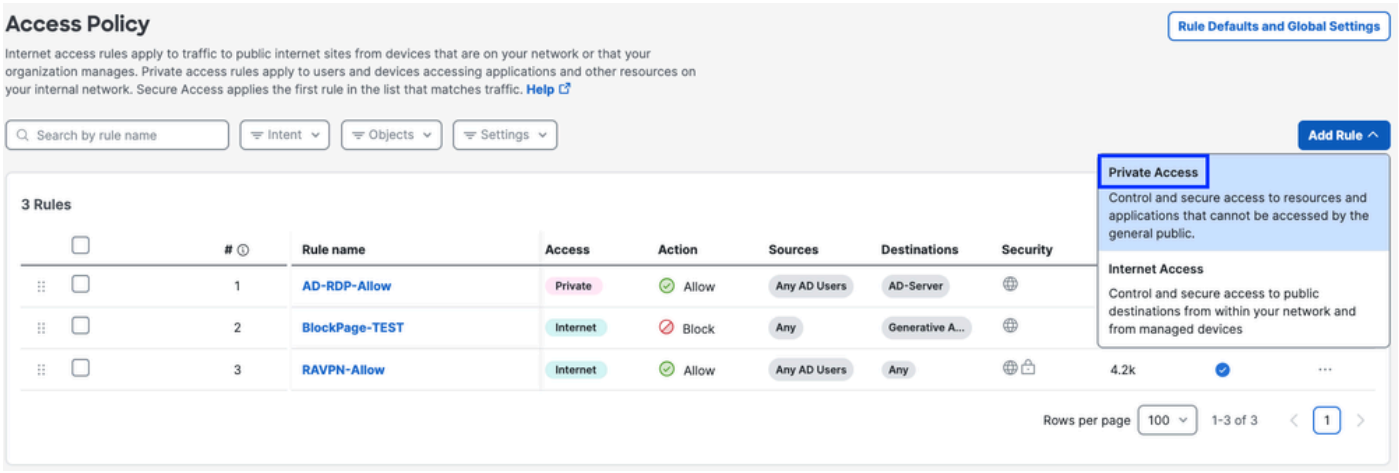
Configurez un accès privé sur Secure Access pour que les utilisateurs inscrits à Universal ZTA puissent y accéder. Pour plus d'informations, consultez Règle d'accès privé

1. Accédez à Secure > Access Policy



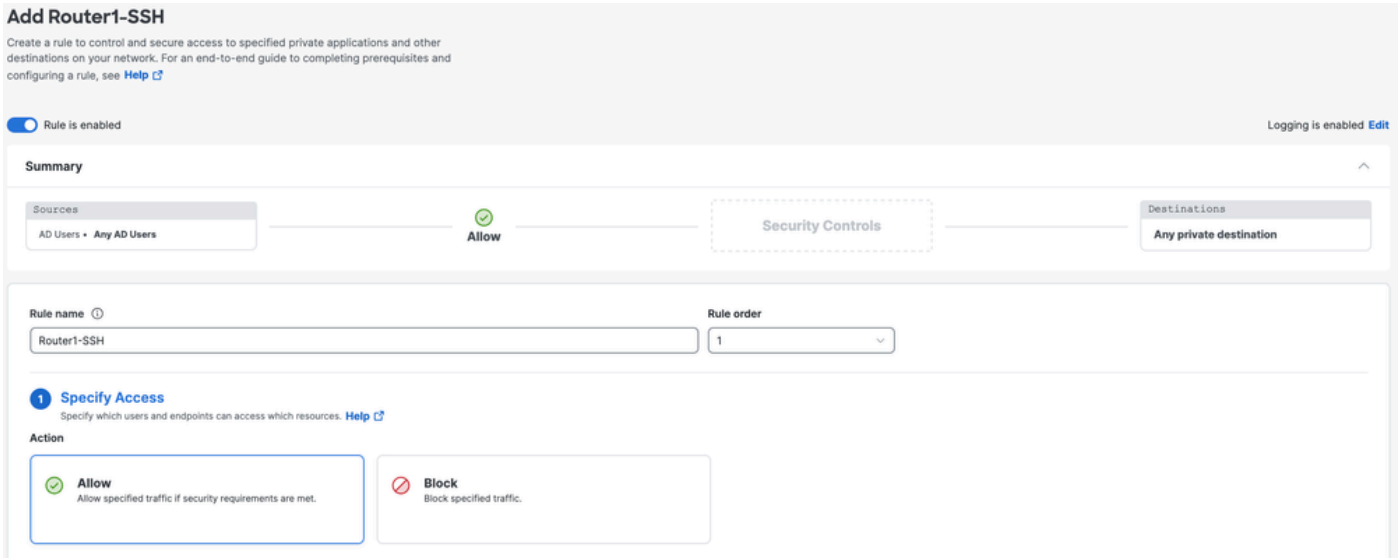
Accès sécurisé - Configuration des ressources privées

2. Cliquez sur Ajouter une règle, puis choisissez Accès privé.
   En haut de la règle se trouve un résumé qui décrit les composants configurés de votre règle.



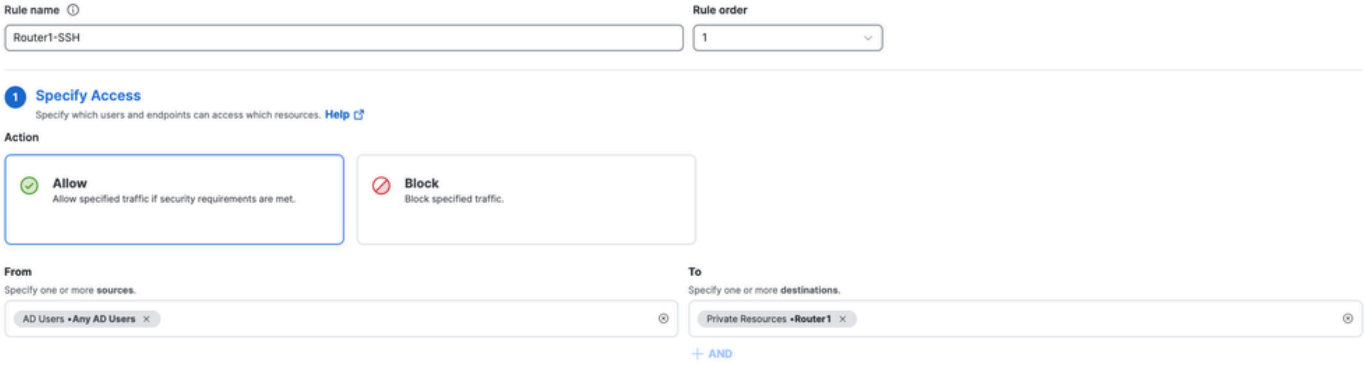
Accès sécurisé - Configuration de la stratégie d'accès

3. Ajouter un nom de règle



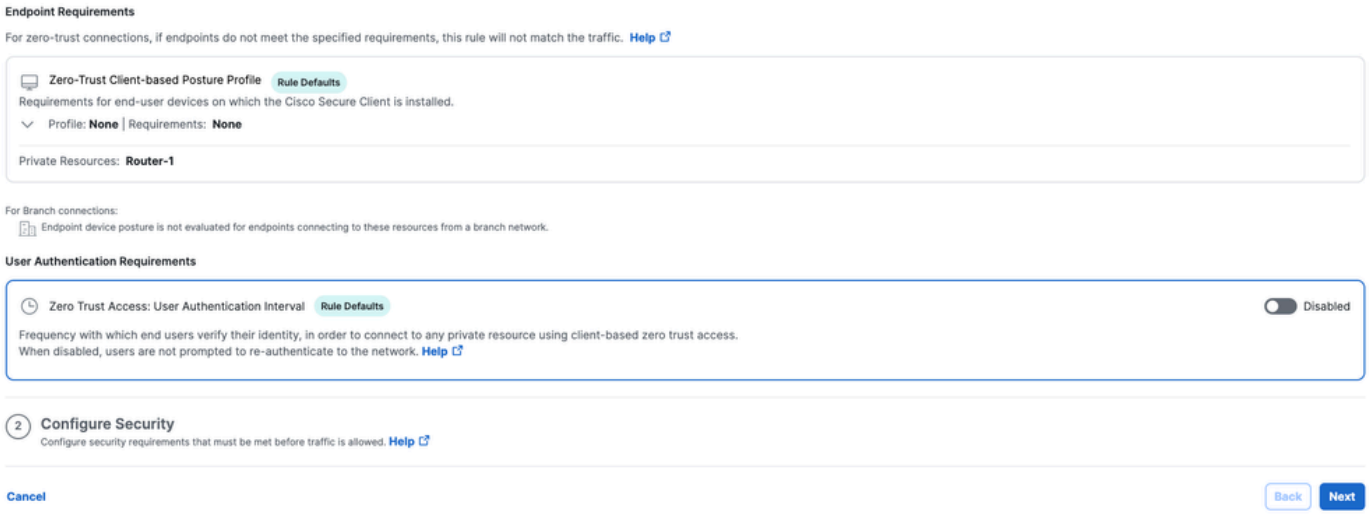
Accès sécurisé - Configuration de la stratégie d'accès

4. Sélectionnez l'action de règle et sélectionnez l'origine et la destination



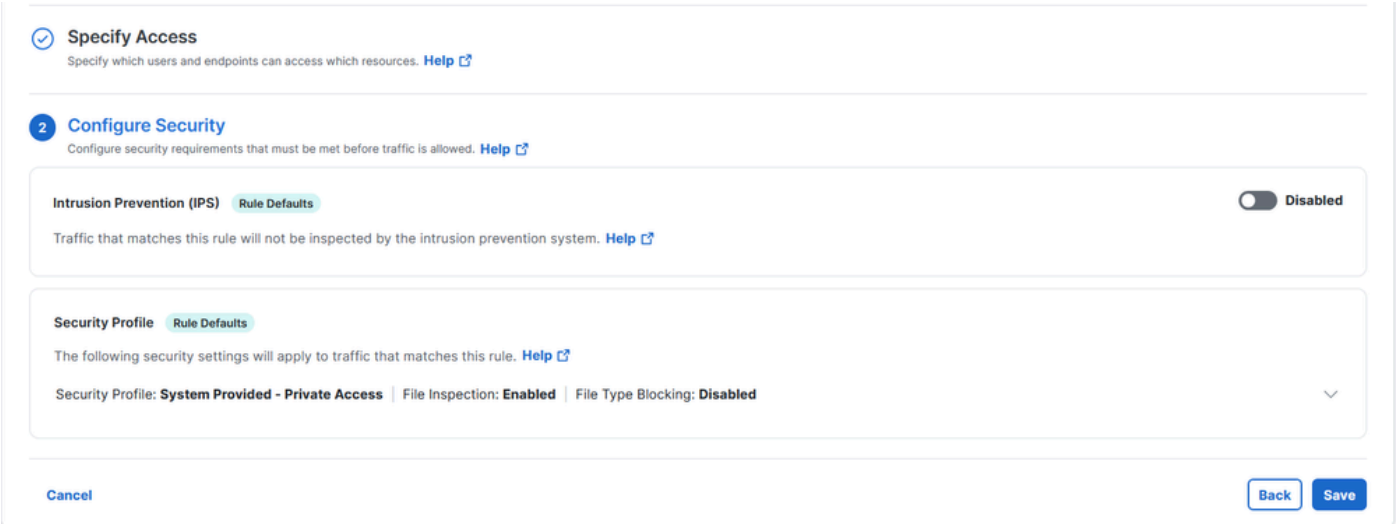
Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux



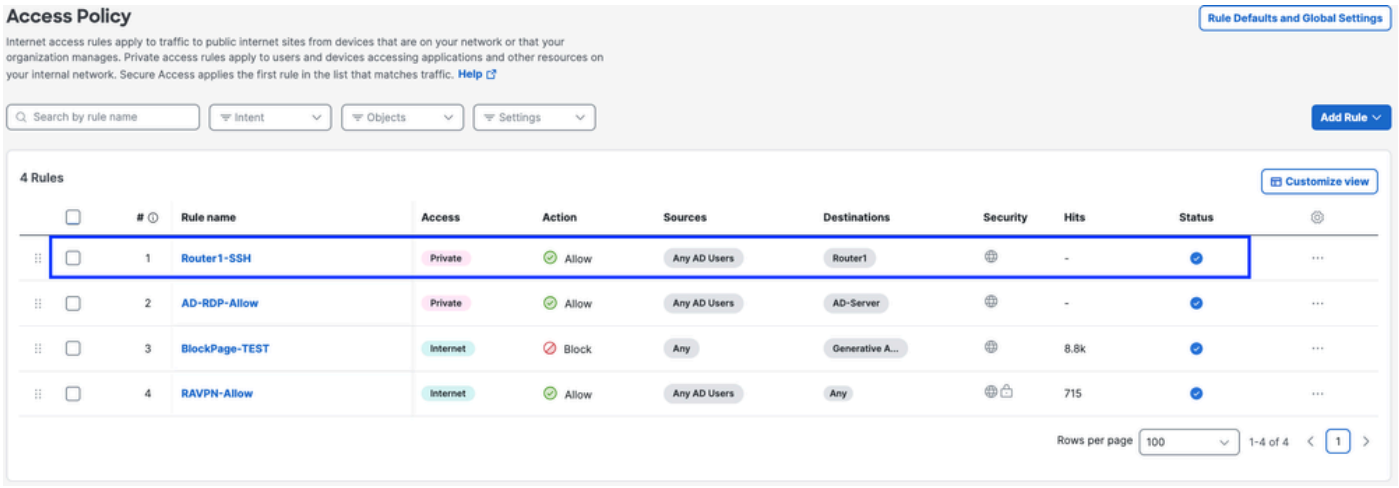
Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité



Accès sécurisé - Configuration de la stratégie d'accès

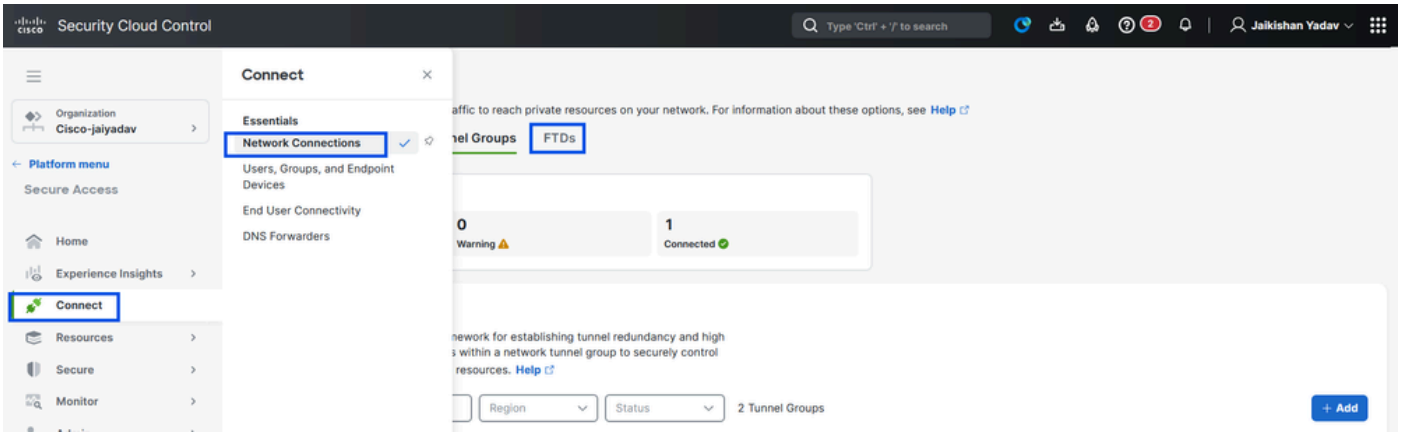
7. Cliquez sur Enregistrer



Accès sécurisé - Configuration de la stratégie d'accès

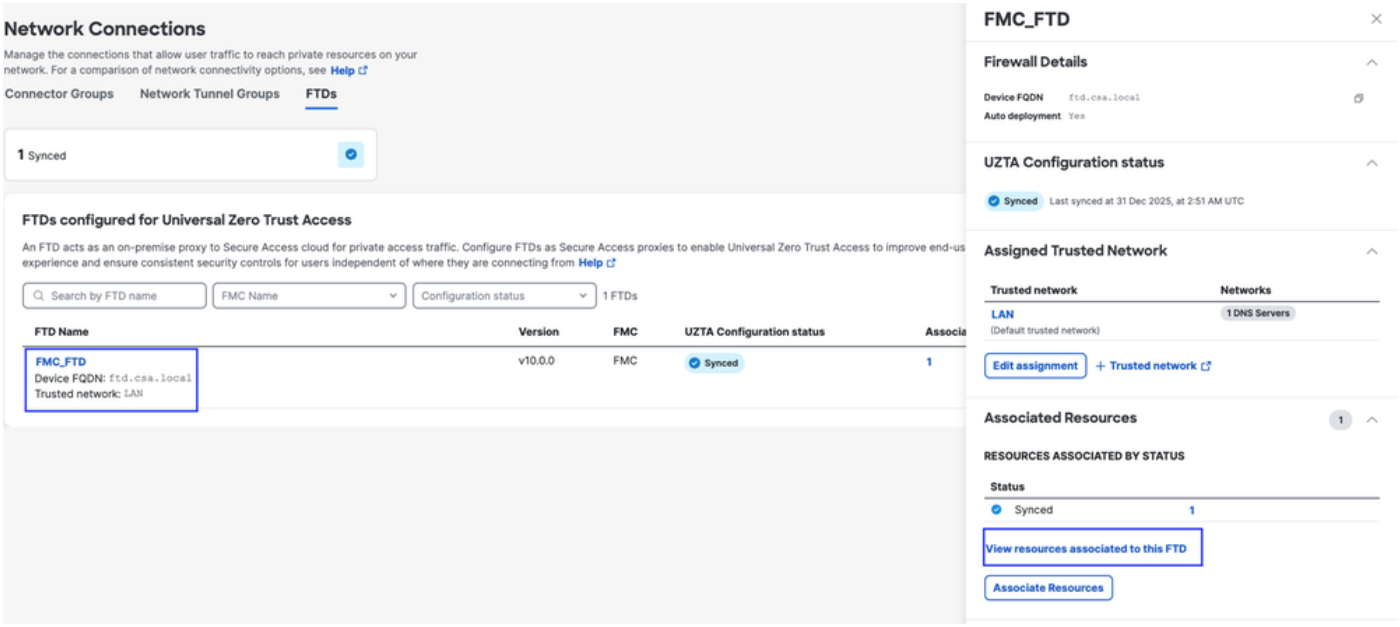
Étape 3 - Vérifiez l'association de PR sur le FTD

1. Accédez à Connect > Network Connections > FTDs

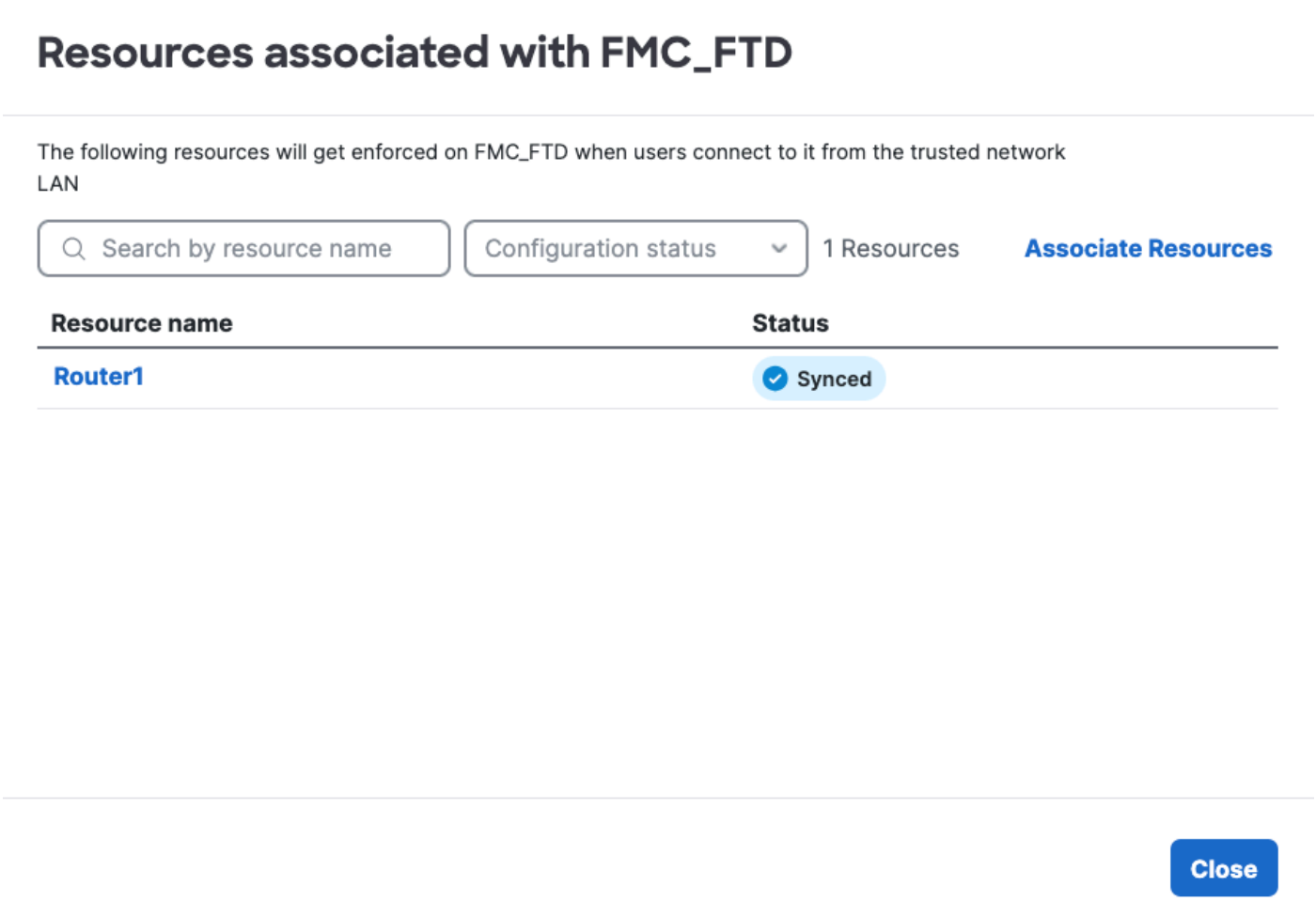


Accès sécurisé - Vérification PR

2. Cliquez sur le FTD > Afficher les ressources associées à ce FTD



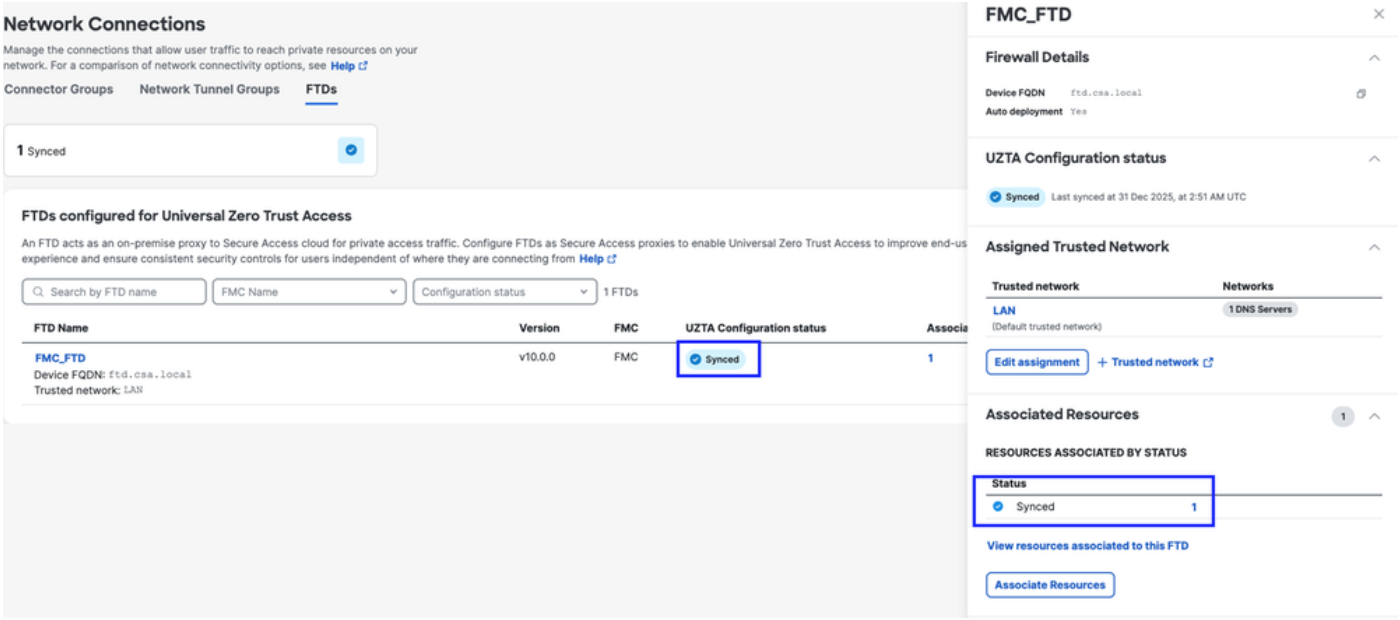
Accès sécurisé - Vérification PR



Accès sécurisé - Vérification PR

3. Cliquez sur Fermer

4. Vérifiez l'état , la ressource associée et la configuration doivent être à l'état Synchronisé



Accès sécurisé - Vérification PR

5. Vérifiez que la configuration a été poussée vers FTD

Connectez-vous à l'interface de ligne de commande FTD et passez en mode LINA

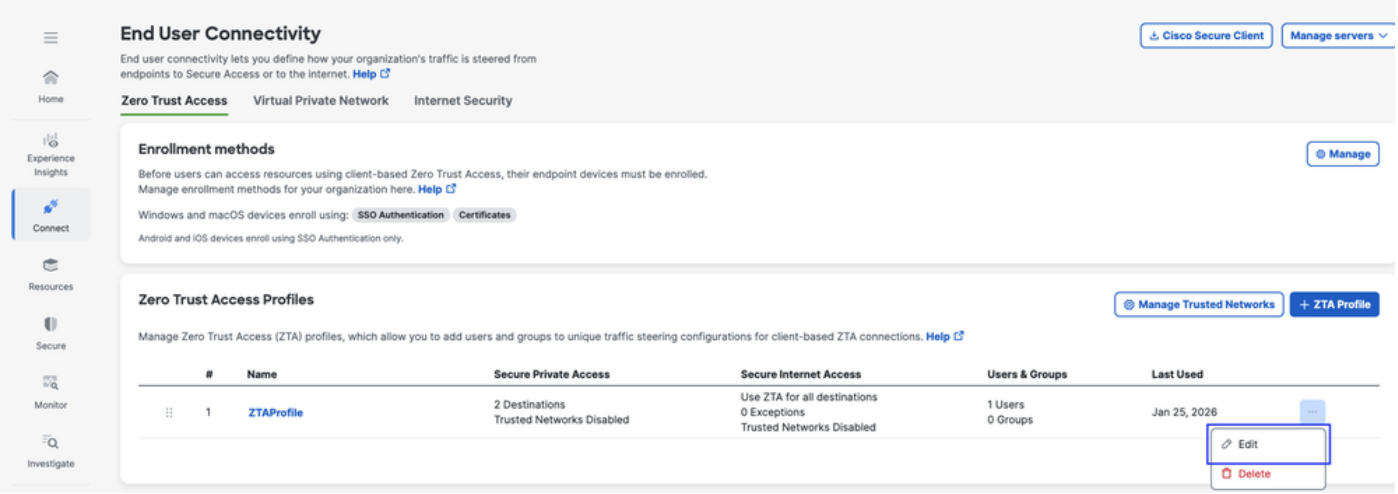
show running-config object application

```
> 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 - Vérification PR

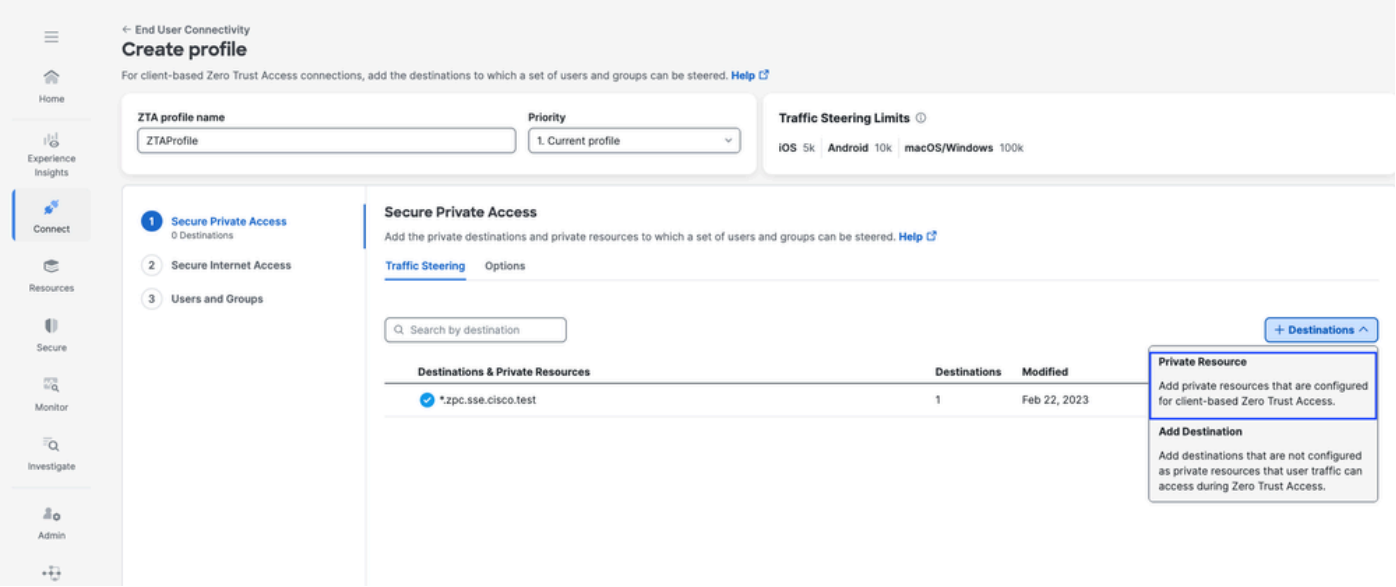
Étape 4 - Ajoutez une ressource privée au profil ZTA

1. Accédez à Connect > End User Connectivity > Zero Trust Access et cliquez sur 3 points pour modifier le profil ZTA

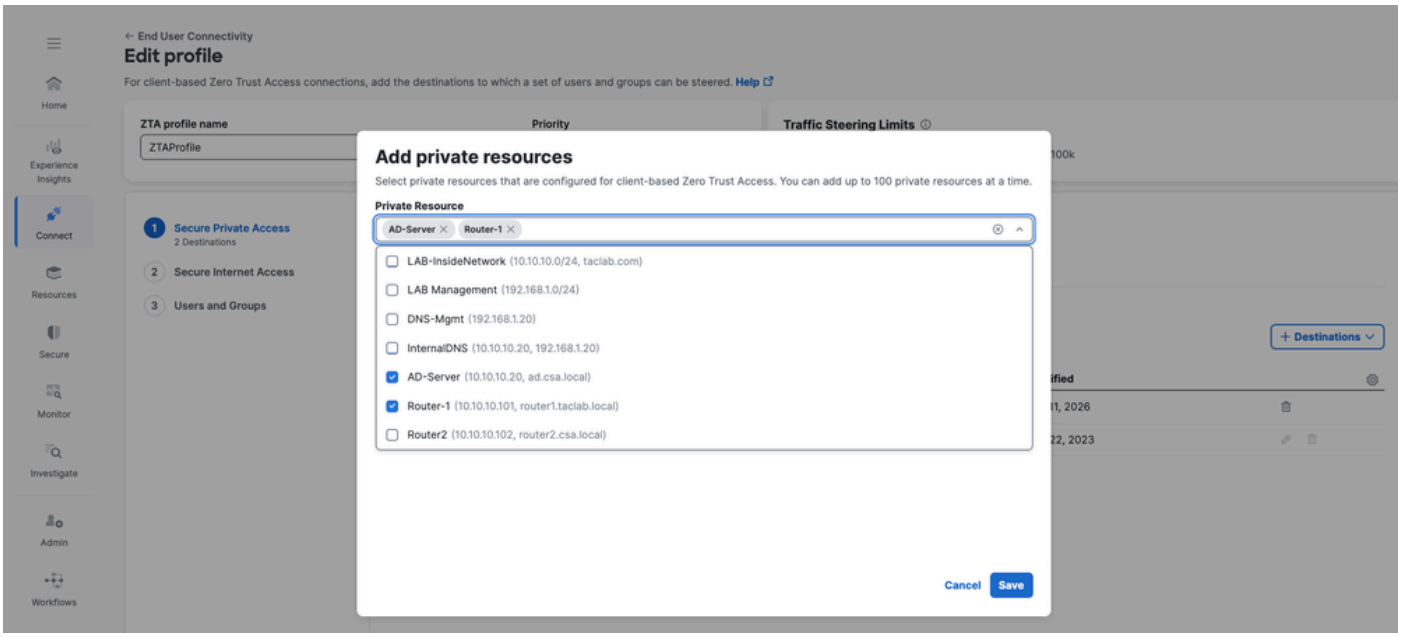


Accès sécurisé - Profil ZTA

2. Ajouter la ressource privée

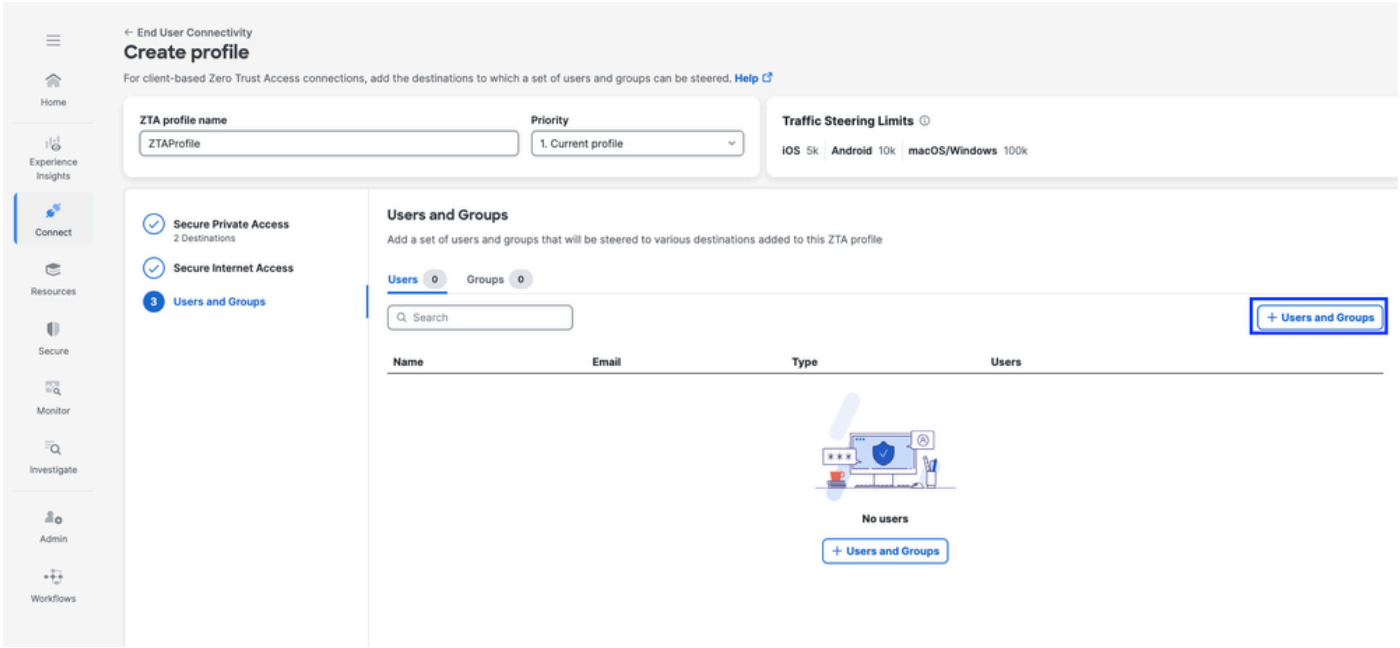


Accès sécurisé - Profil ZTA

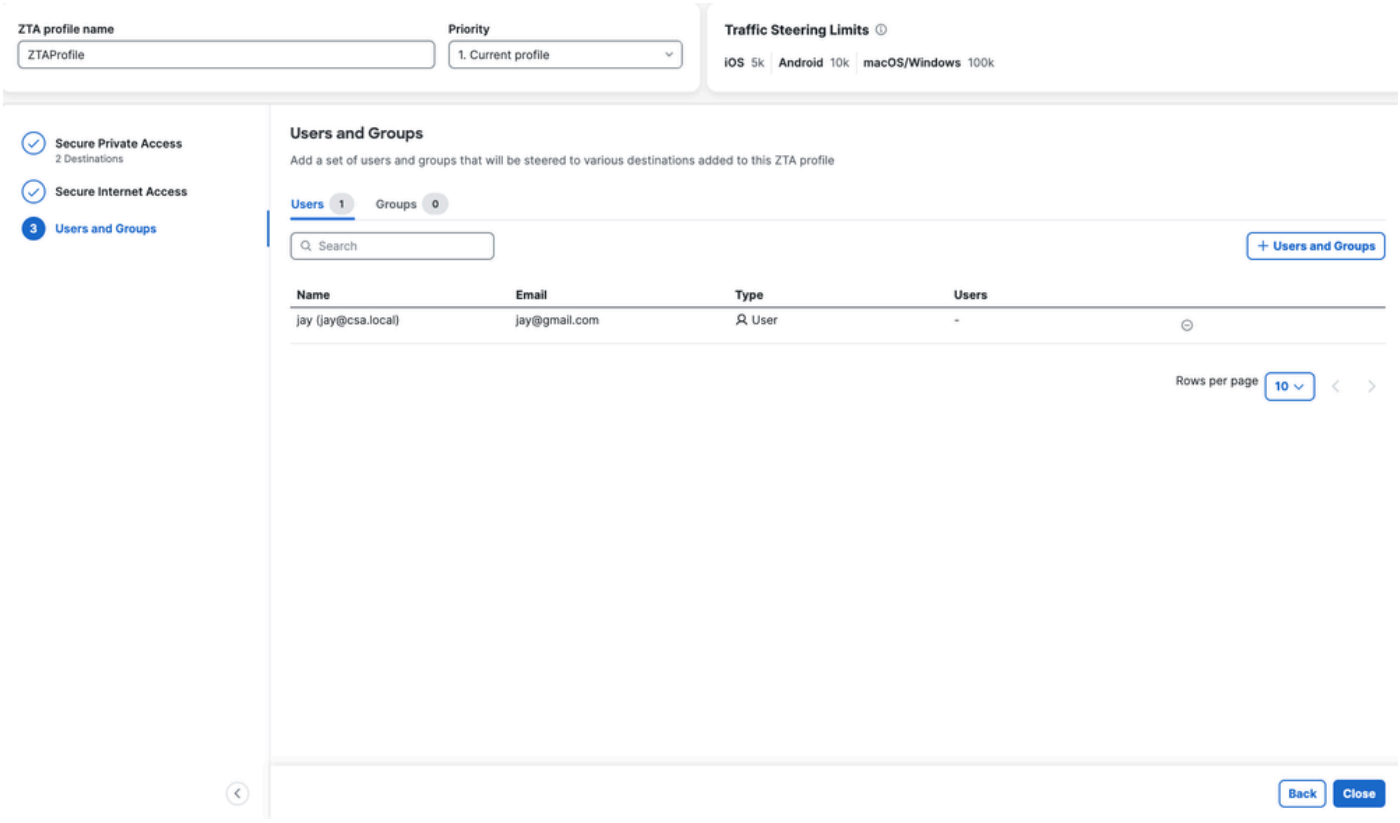


Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes



Accès sécurisé - Profil ZTA



Accès sécurisé - Profil ZTA

Étape 5 - Vérifiez l'accès à la ressource privée

1. Vérifier que l'utilisateur distant peut résoudre le FQDN FTD

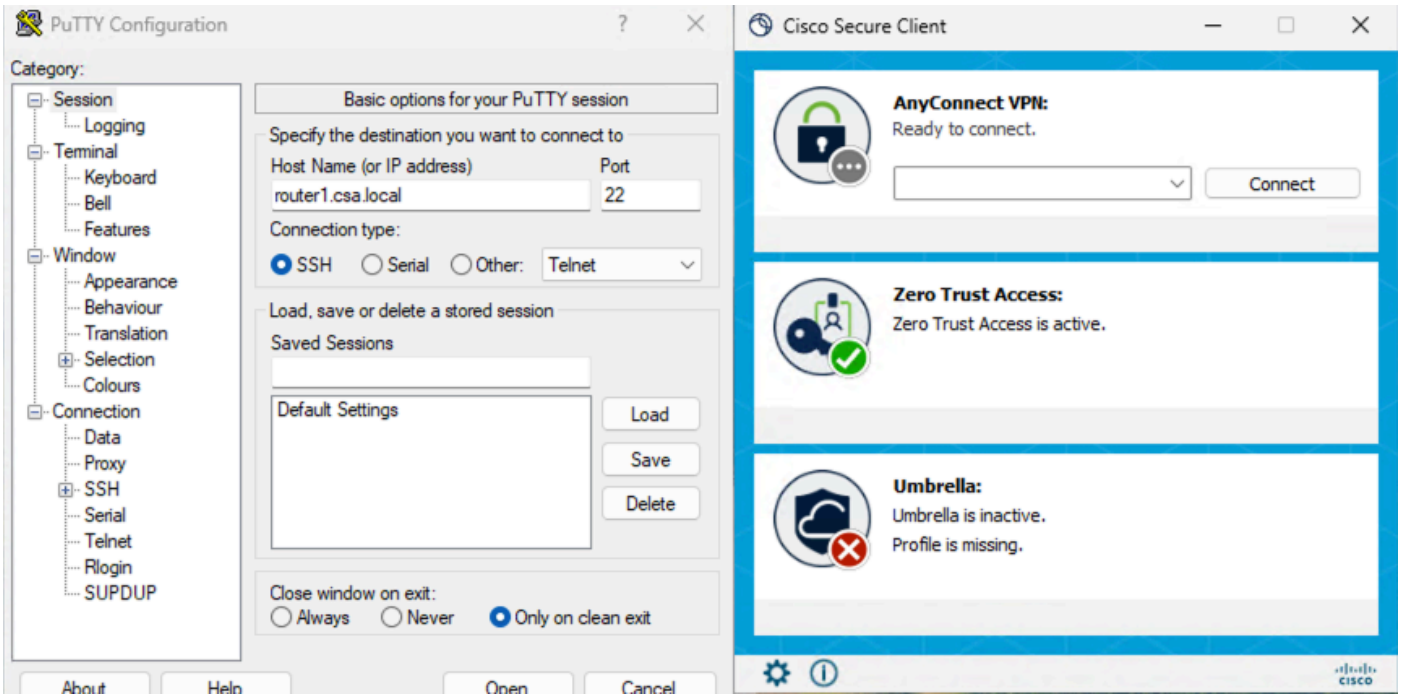
```
PS C:\Users\jay> ping ftd.csa.local

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
```

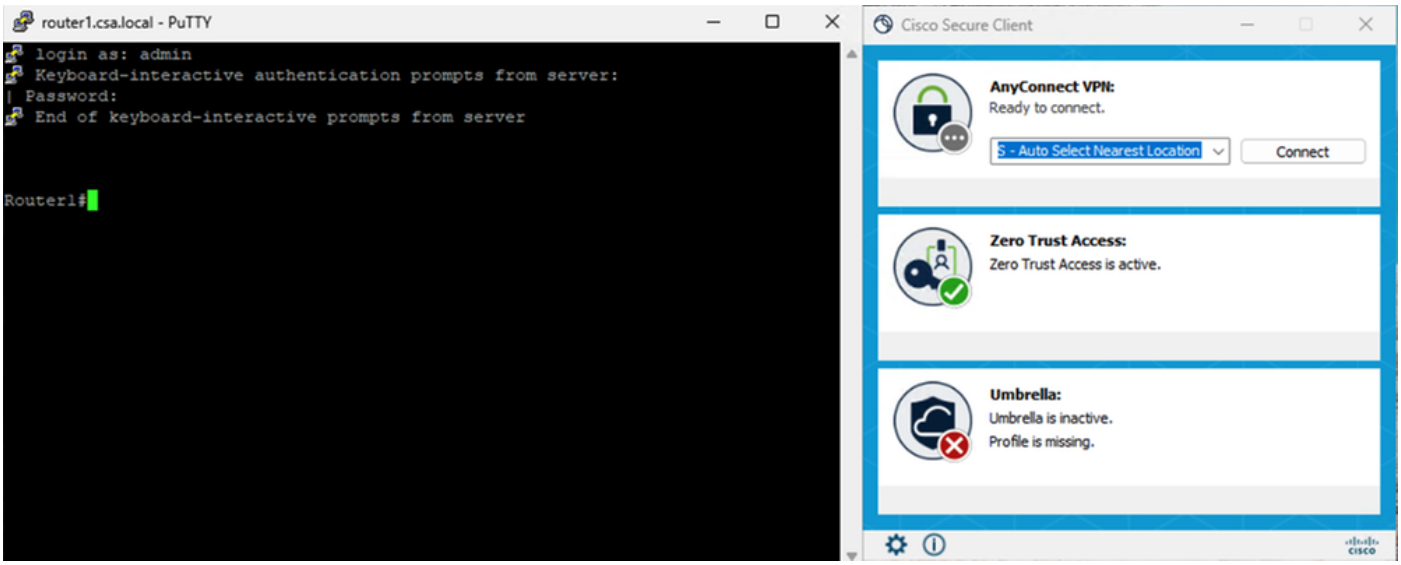
2. Vérifiez que FTD peut accéder à une ressource privée à l'aide du nom de domaine complet

```
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. Tester la connexion SSH à la ressource privée

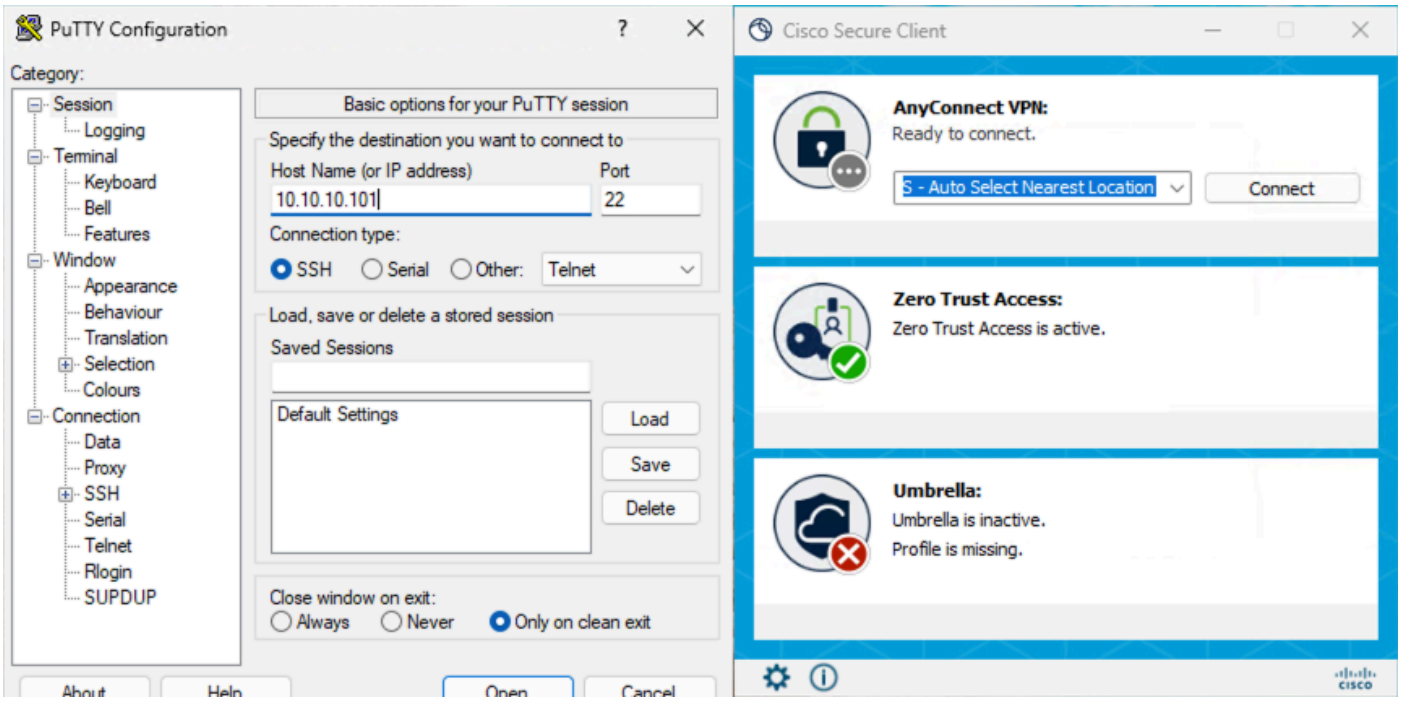
Accéder au RP à l'aide du FQDN



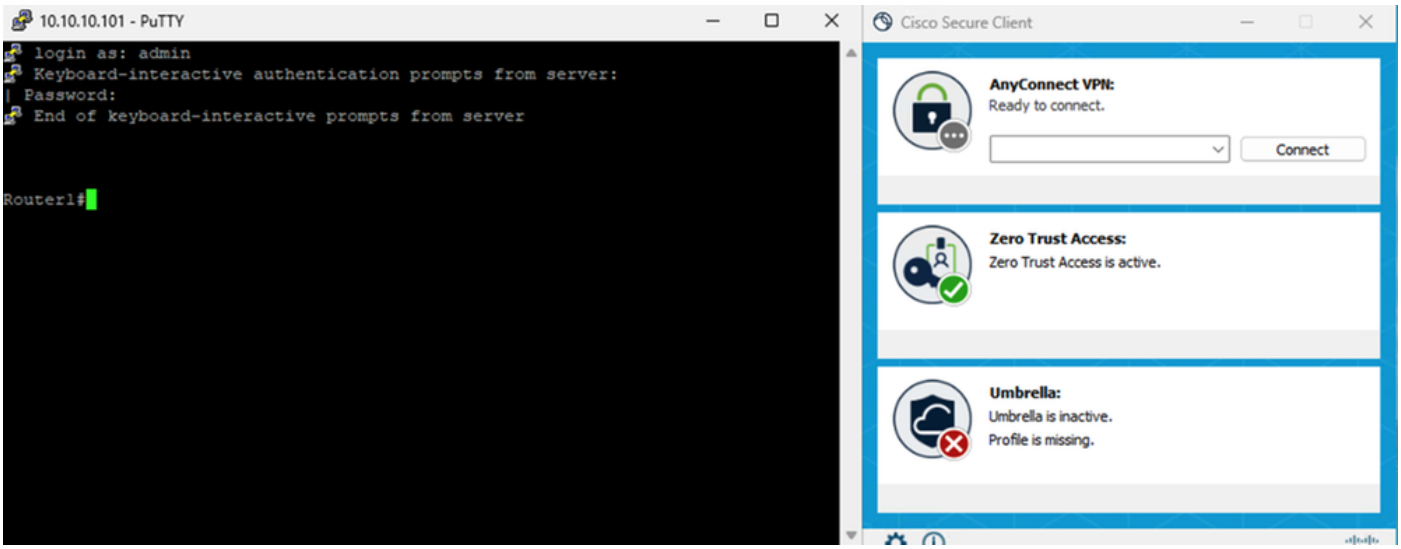


Accès sécurisé - Test PR

Accéder au RP en utilisant l'adresse IP

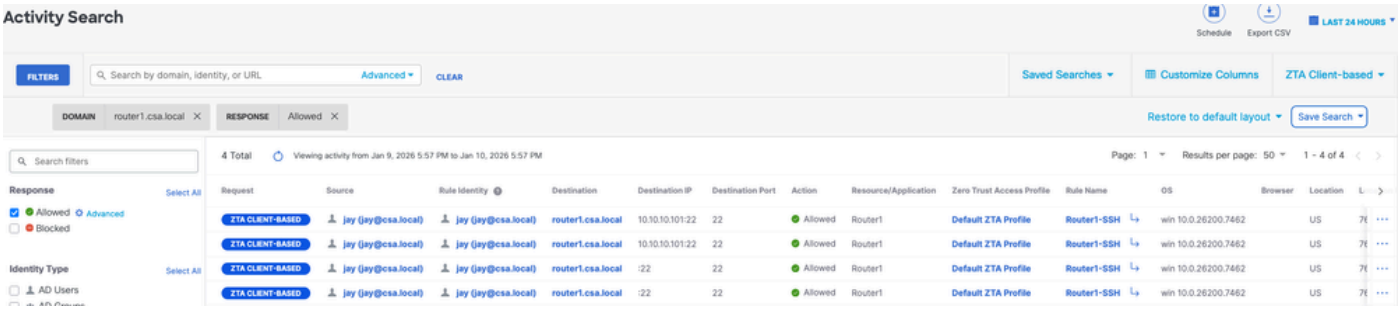


Accès sécurisé - Test PR

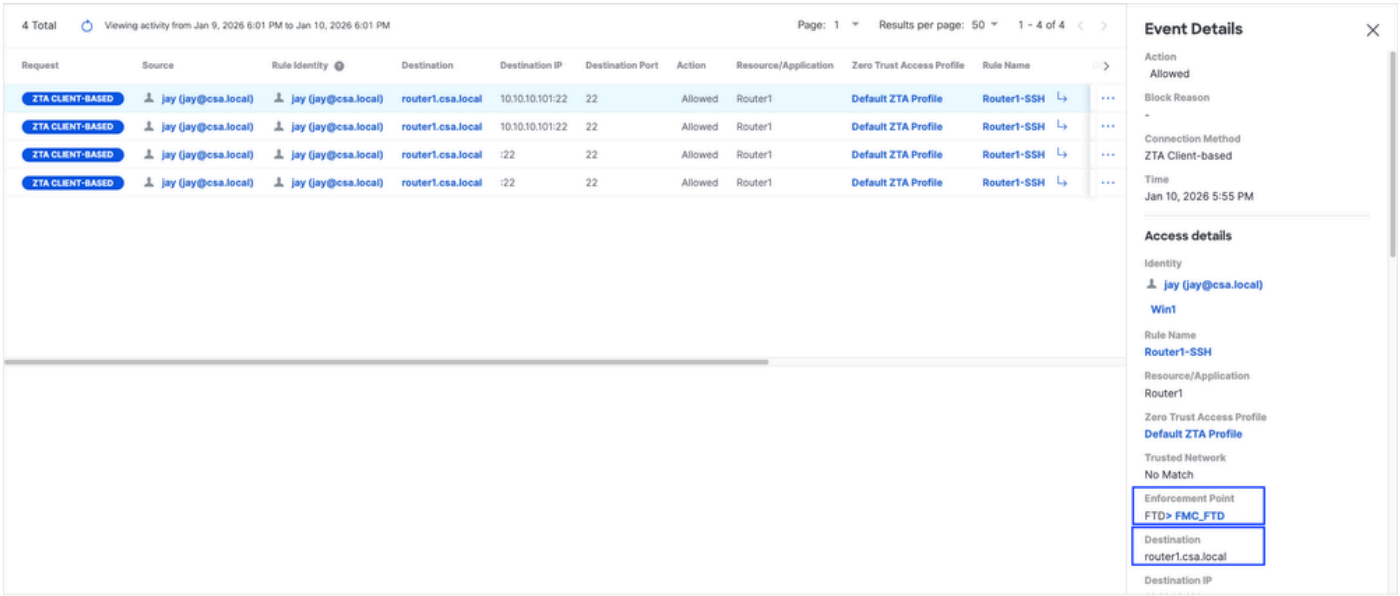


Accès sécurisé - Test PR

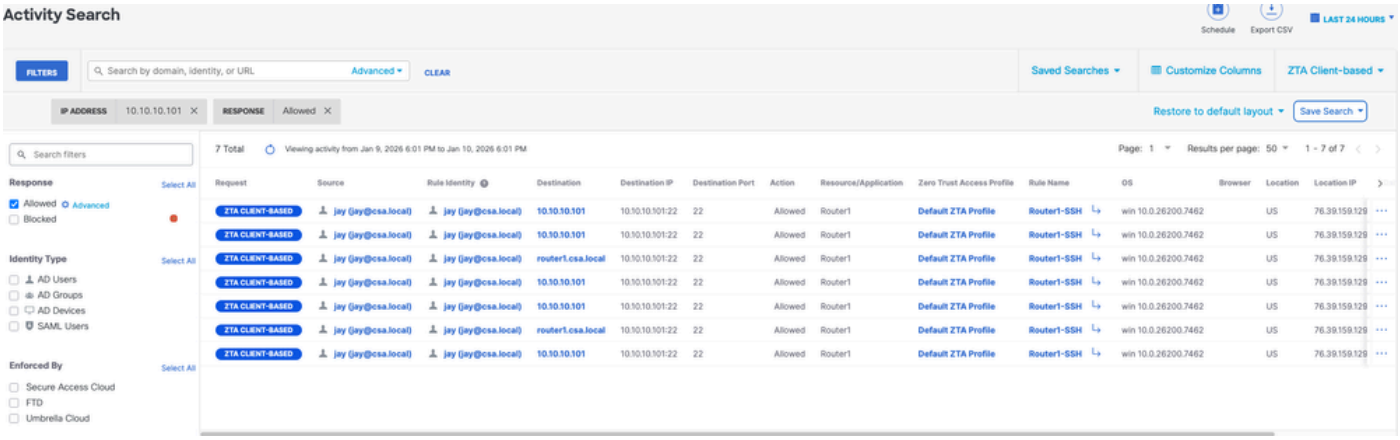
4. Vérifier les journaux de recherche d'activité Secure Access



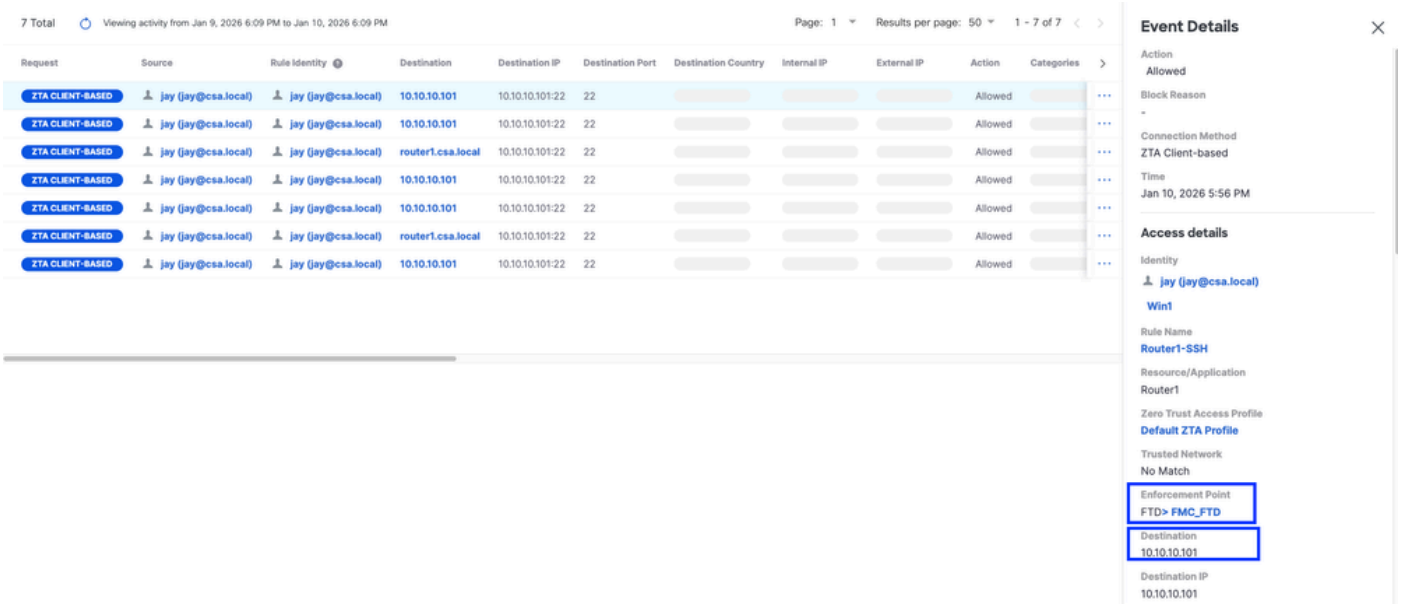
Accès sécurisé - Recherche d'activité



Accès sécurisé - Recherche d'activité

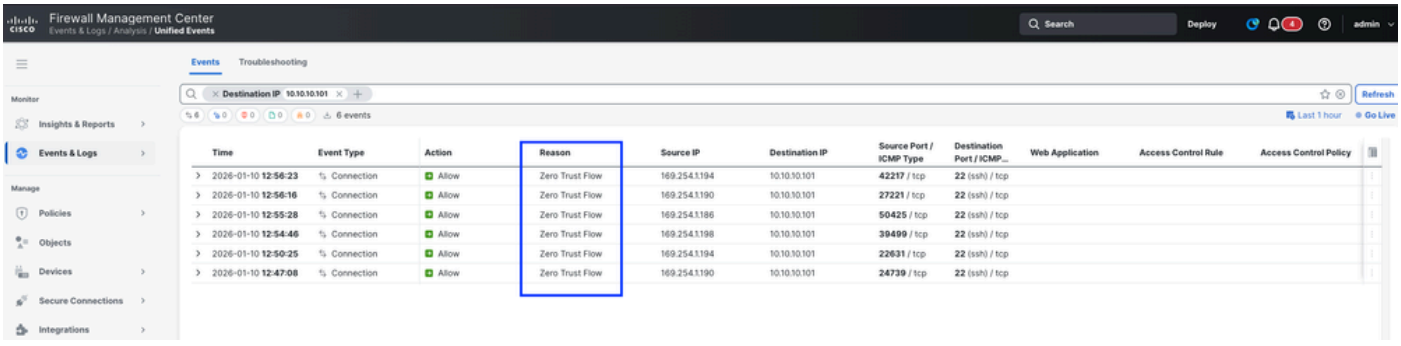


Accès sécurisé - Recherche d'activité



Accès sécurisé - Recherche d'activité

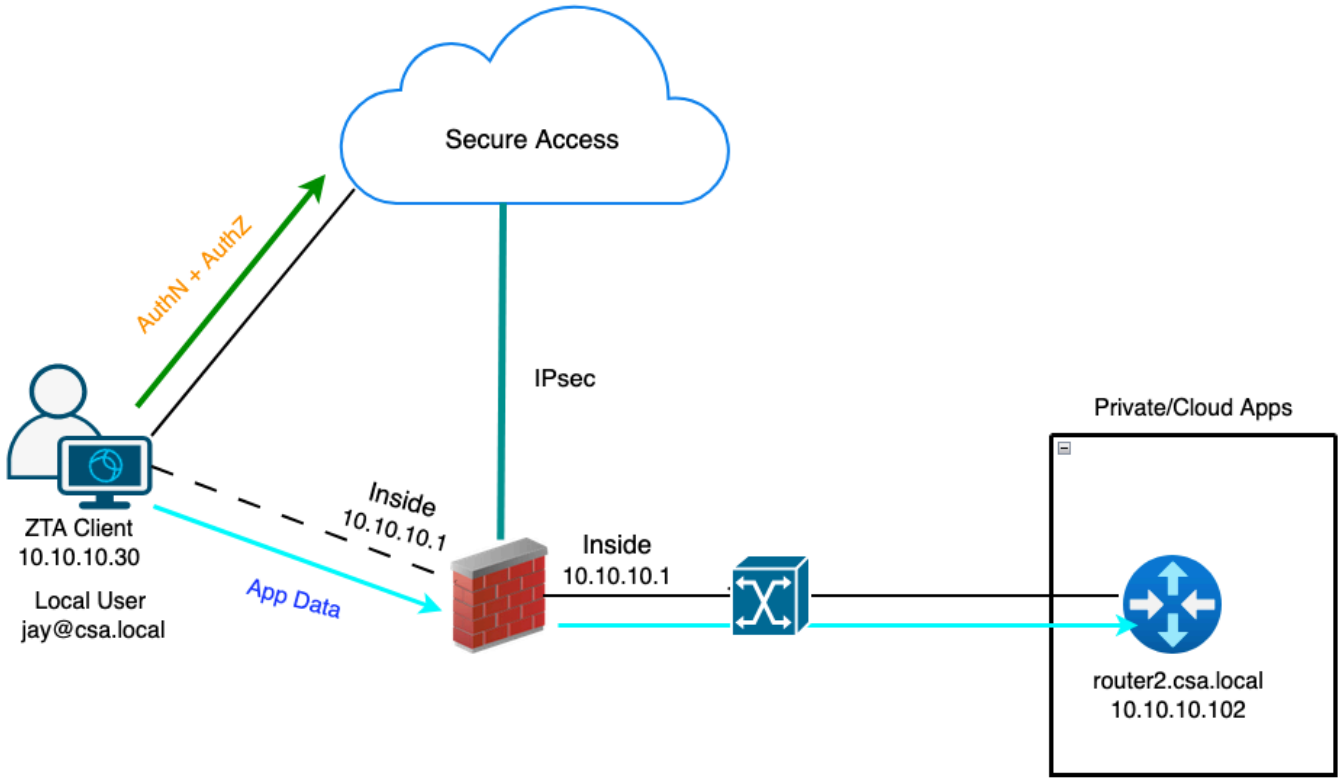
5. Vérifier les événements de connexion FMC



Événements de connexion FMC

Cas de test 3 - Utilisateur local - Application locale

L'accès à une ressource privée via l'application locale en tant qu'utilisateur local, dans ce type d'évaluation de stratégie d'application se produit sur l'accès sécurisé, mais les données d'application restent locales à FTD. Par exemple , un client ou un utilisateur inscrit ZTA connecté au réseau domestique et essayant d' accéder à une ressource privée qui se trouve derrière l' interface interne FTD . Si la ressource privée se trouve derrière DMZ ou toute autre interface du FTD, alors nous devrions créer une règle d'accès sur le FTD pour permettre le trafic entre l'IP client ou le réseau et la ressource privée.

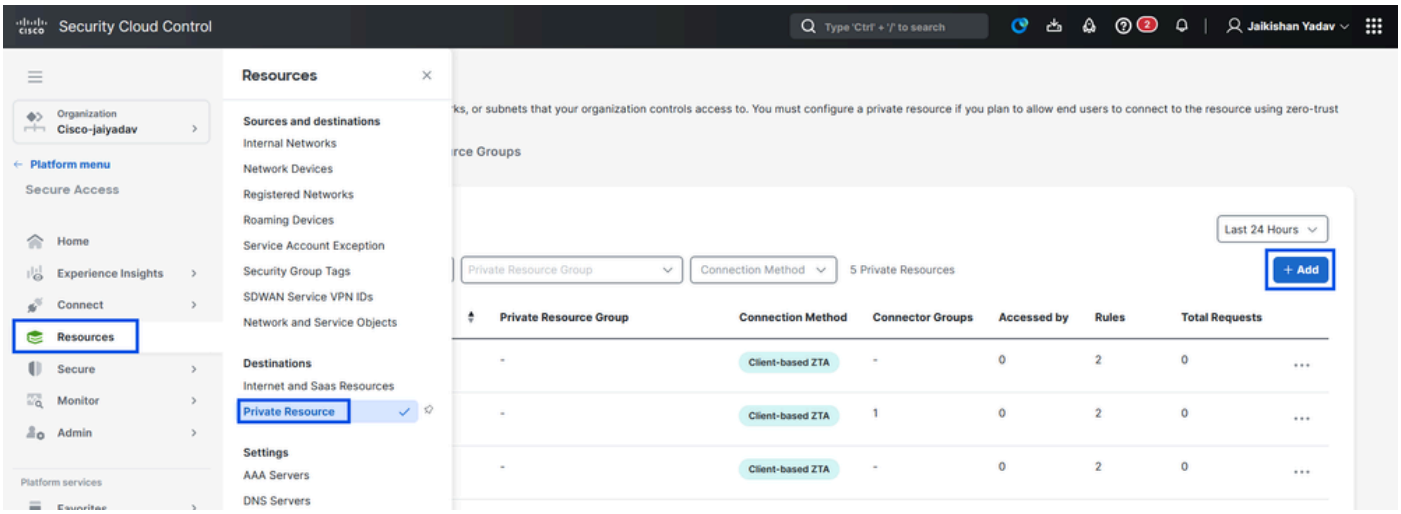


ZTA universel - Topologie de cas de test

Étape 1 : définition d'une ressource privée sur un accès sécurisé

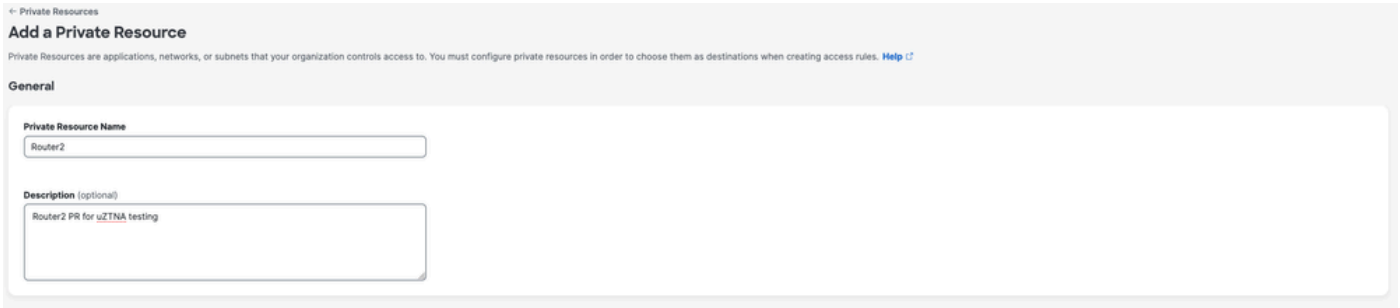
Configurer une ressource privée pour qu'elle soit accessible via un périphérique inscrit ZTA (Zero Trust Access) avec application cloud

1. Accédez à Ressources > Destinations > Ressources privées > Cliquez sur +Ajouter



Accès sécurisé - Configuration des ressources privées

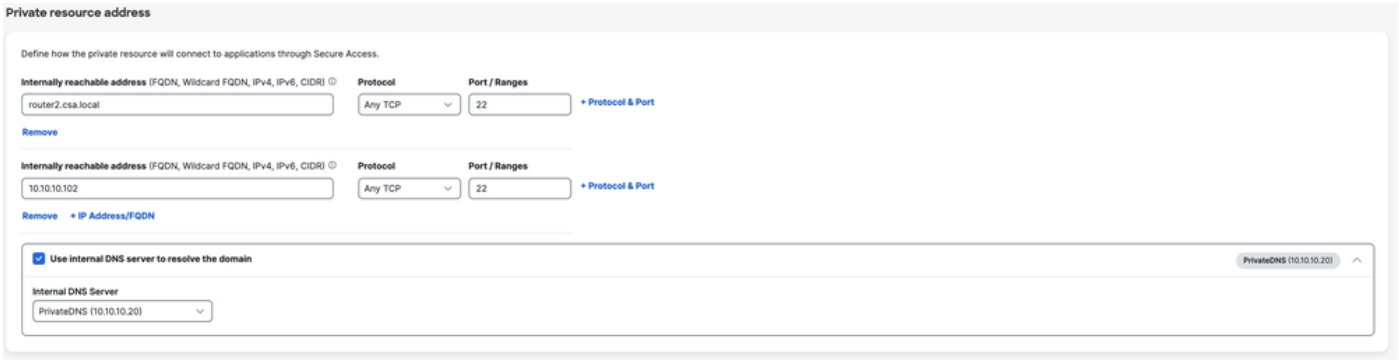
2. Dans le champ Nom de la ressource privée, entrez un nom significatif pour la ressource. Pour Description, nous vous recommandons de fournir des informations telles que l'objectif de la ressource ou le nom du propriétaire de la ressource.



Accès sécurisé - Configuration des ressources privées

3. Entrez le nom de domaine complet de la ressource privée à laquelle vous souhaitez accéder. Nous pouvons également définir l'adresse IP de la ressource privée . Pour plus d'informations, voir Ajouter une ressource privée

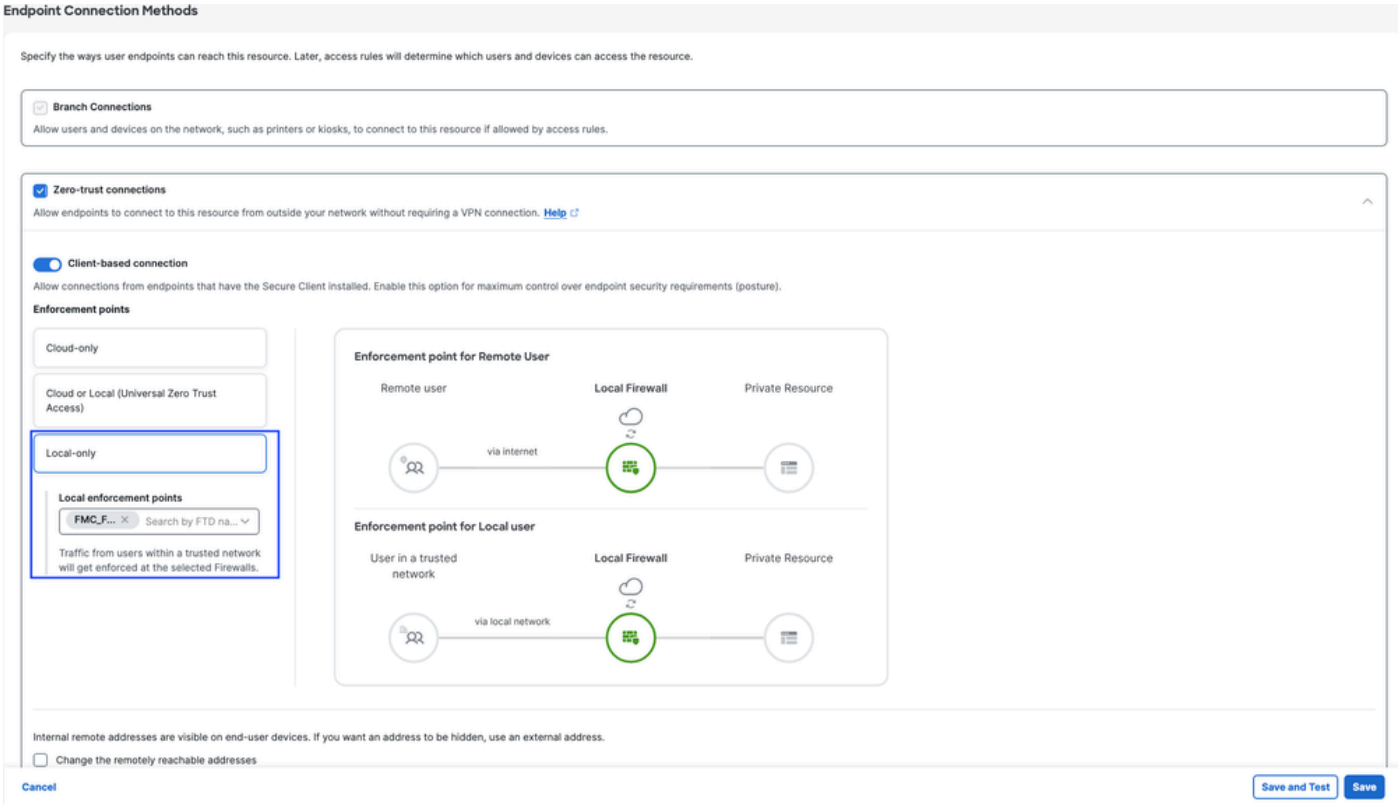
4. Sélectionnez le serveur DNS interne pour résoudre le domaine



Accès sécurisé - Configuration des ressources privées

5. Sélectionner les méthodes de connexion Endpoint

6. Sélectionnez FTD comme points d'application locaux



Accès sécurisé - Configuration des ressources privées

Remarque : Selon le type d'inscription sélectionné, cette modification associera automatiquement le PR au FTD et déclenchera un déploiement de stratégie

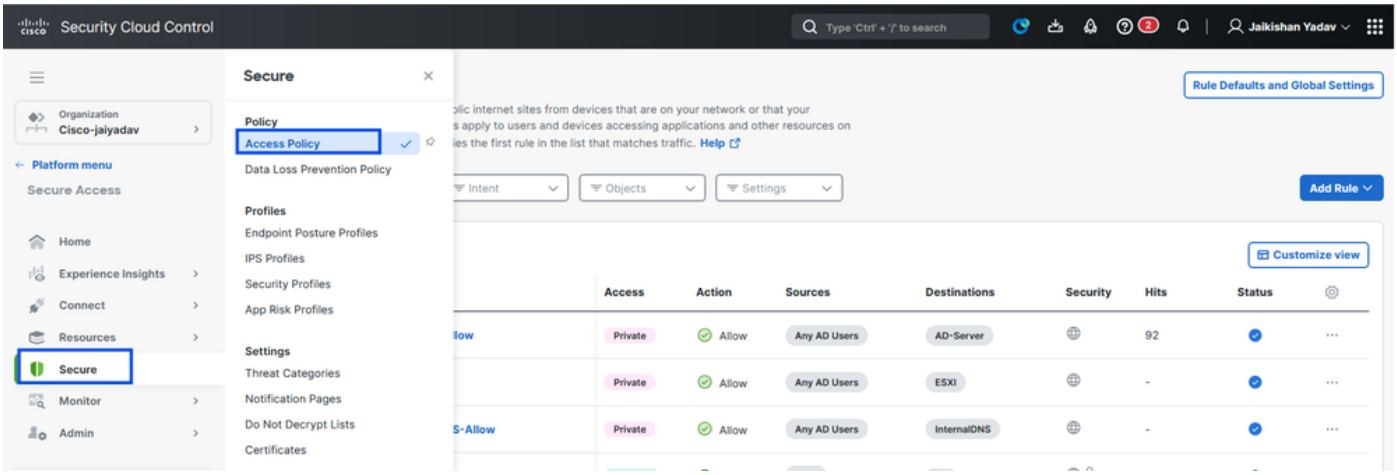
---

7. Cliquez sur Save (enregistrer)

Étape 2 : création d'une règle d'accès privé

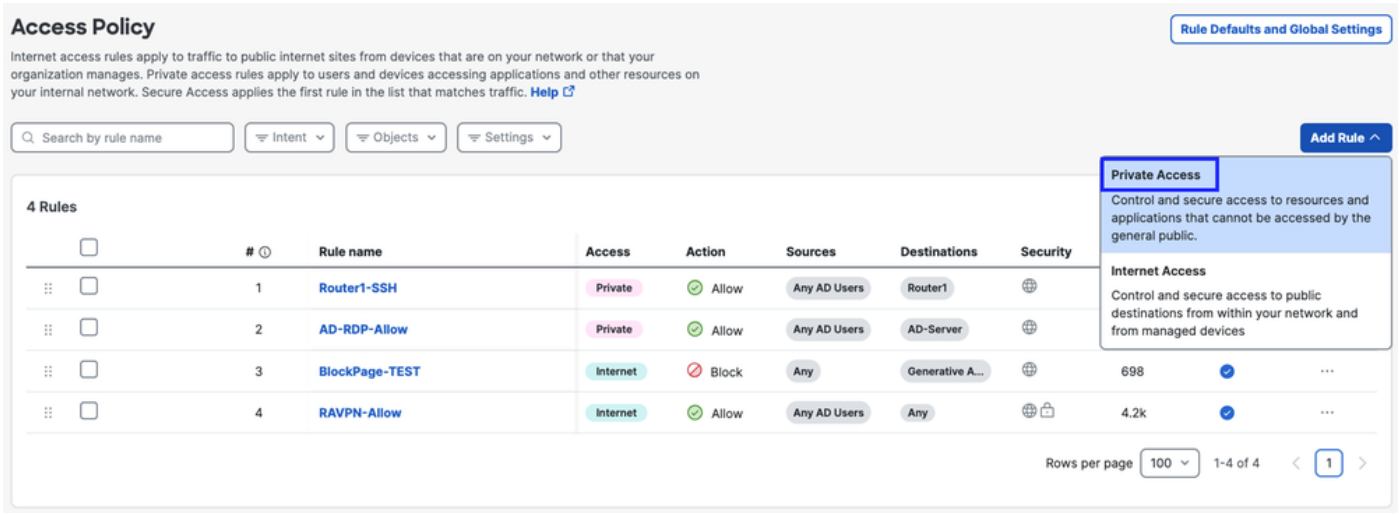
Configurez un accès privé sur Secure Access pour que les utilisateurs inscrits à Universal ZTA puissent y accéder. Pour plus d'informations, consultez [Règle d'accès privé]

1. Accédez à Secure > Access Policy



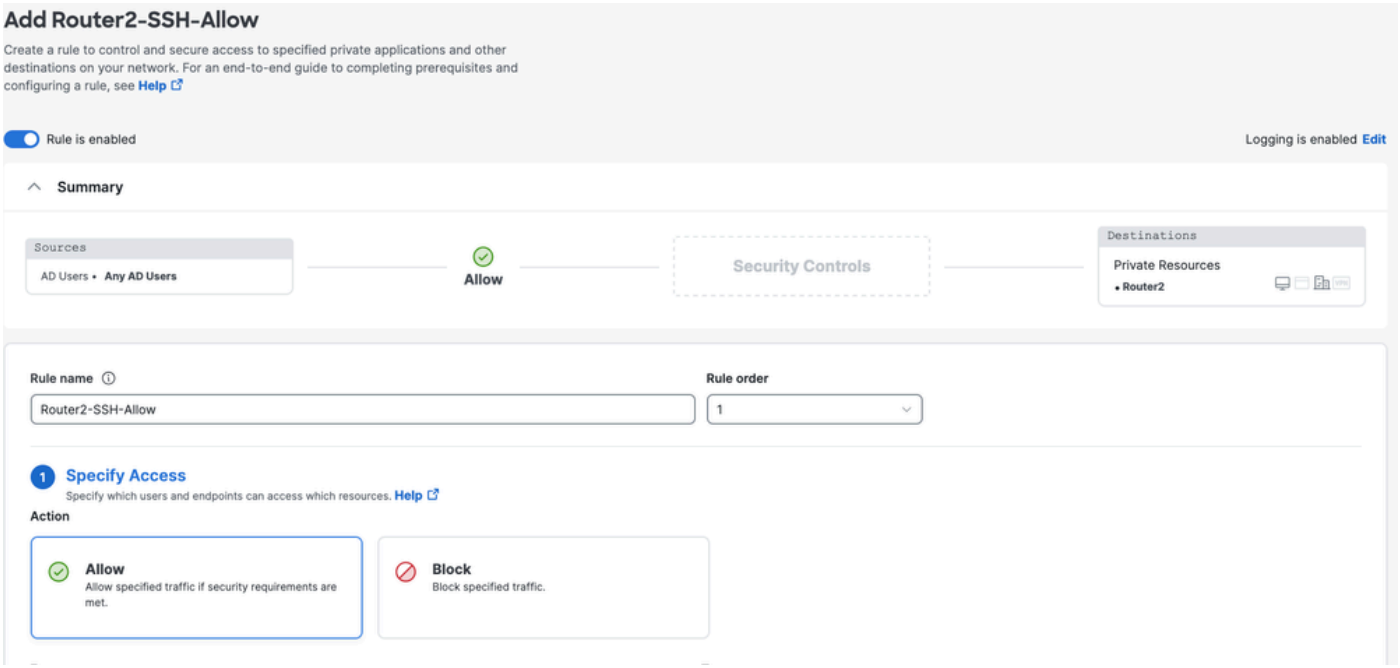
Accès sécurisé - Configuration de la stratégie d'accès

2. Cliquez sur Ajouter une règle, puis choisissez Accès privé.
   En haut de la règle se trouve un résumé qui décrit les composants configurés de votre règle.



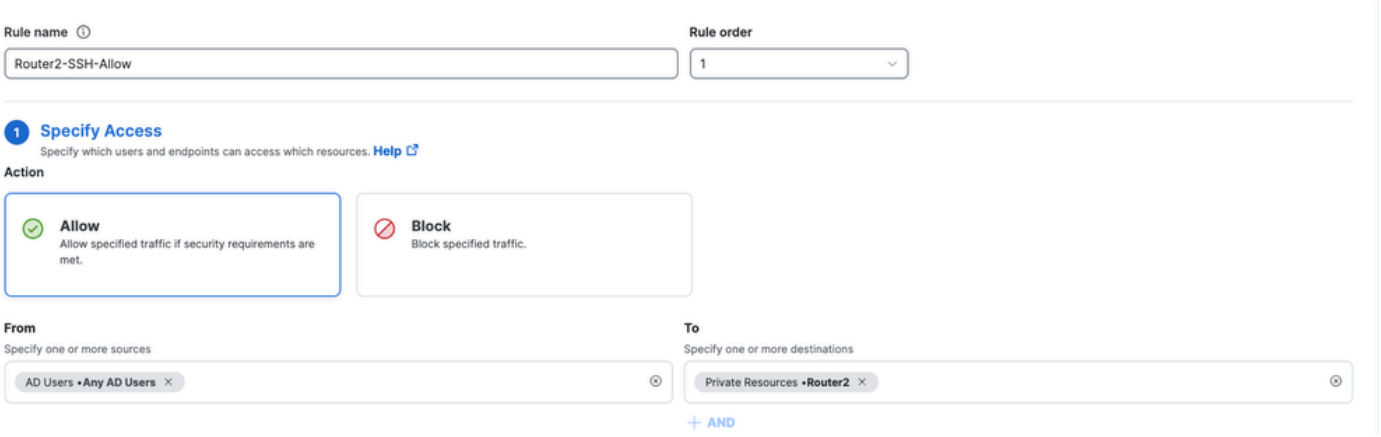
Accès sécurisé - Configuration de la stratégie d'accès

3. Ajouter un nom de règle



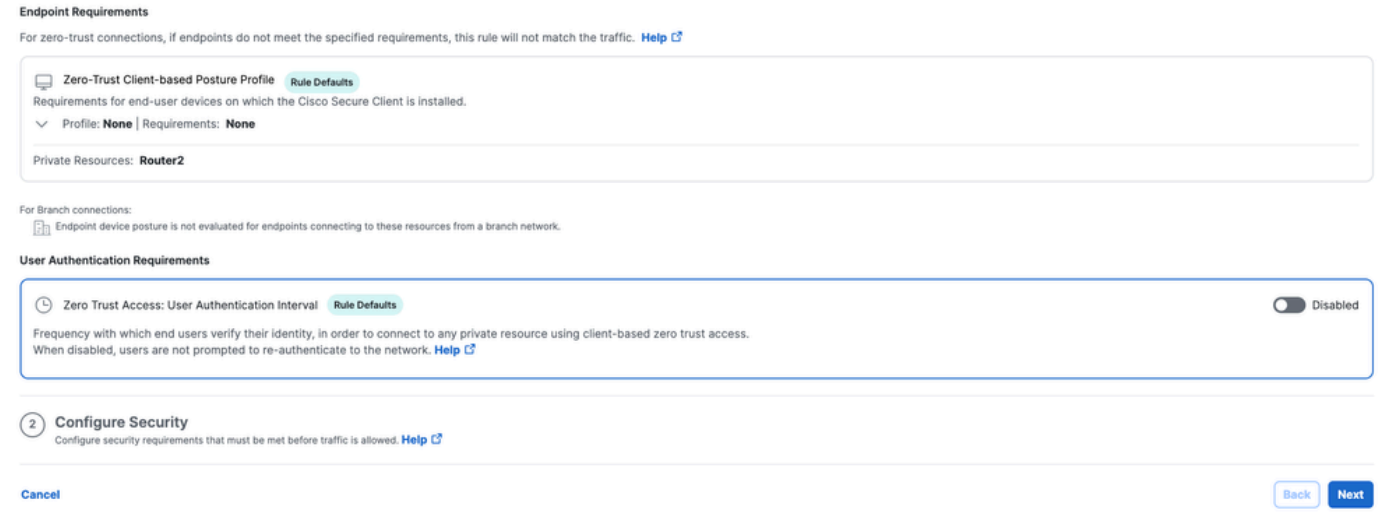
Accès sécurisé - Configuration de la stratégie d'accès

4. Sélectionnez l'action de règle et sélectionnez l'origine et la destination



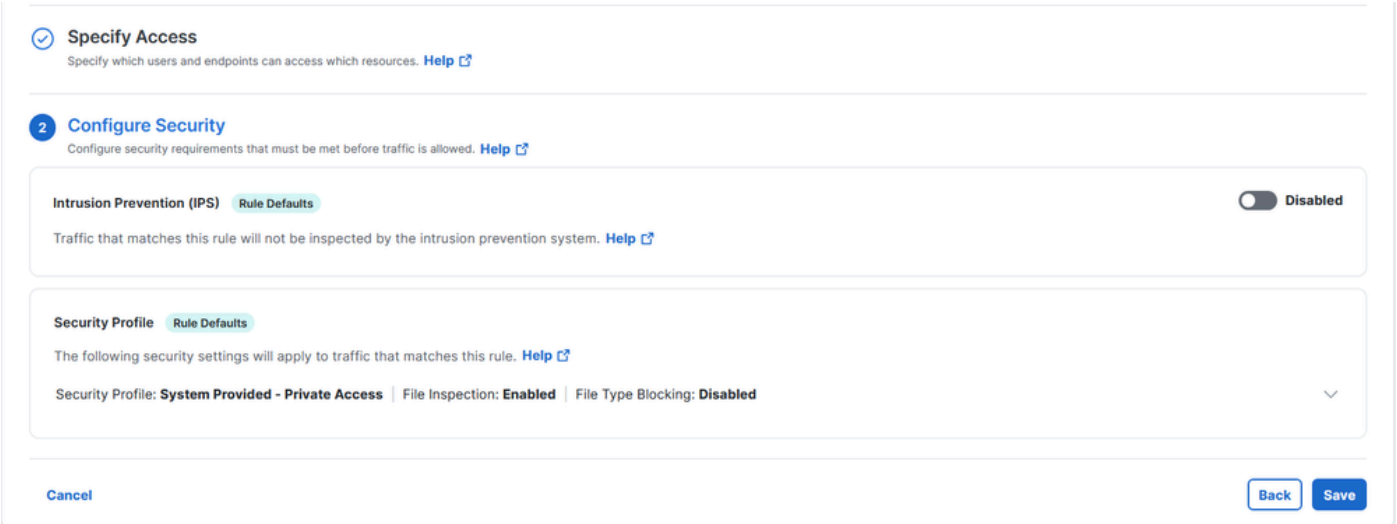
Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux



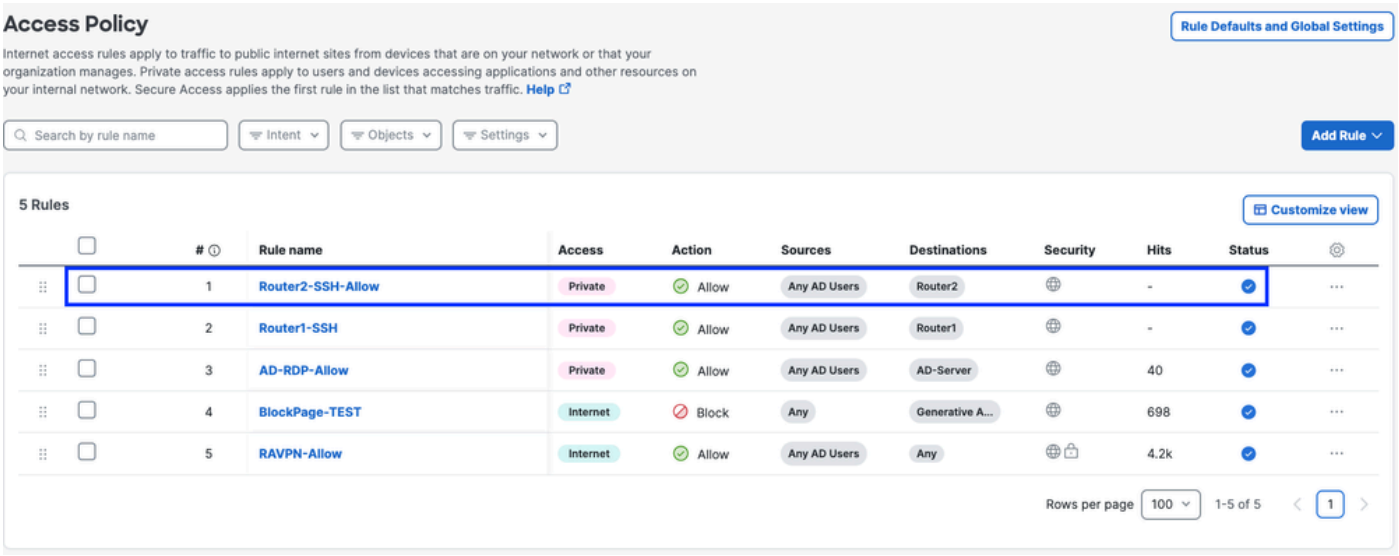
Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité



Accès sécurisé - Configuration de la stratégie d'accès

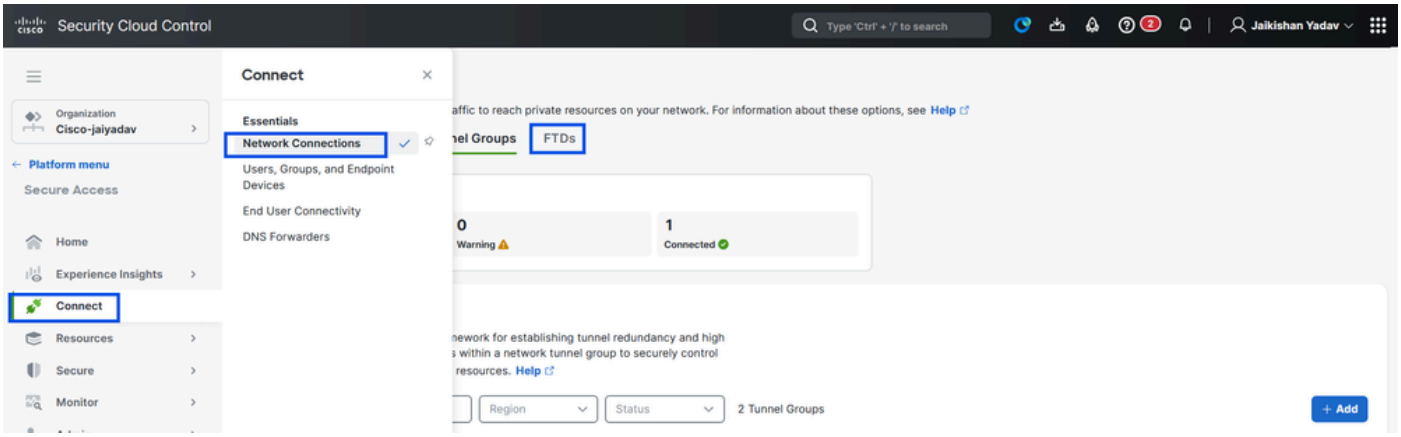
7. Cliquez sur Enregistrer



Accès sécurisé - Configuration de la stratégie d'accès

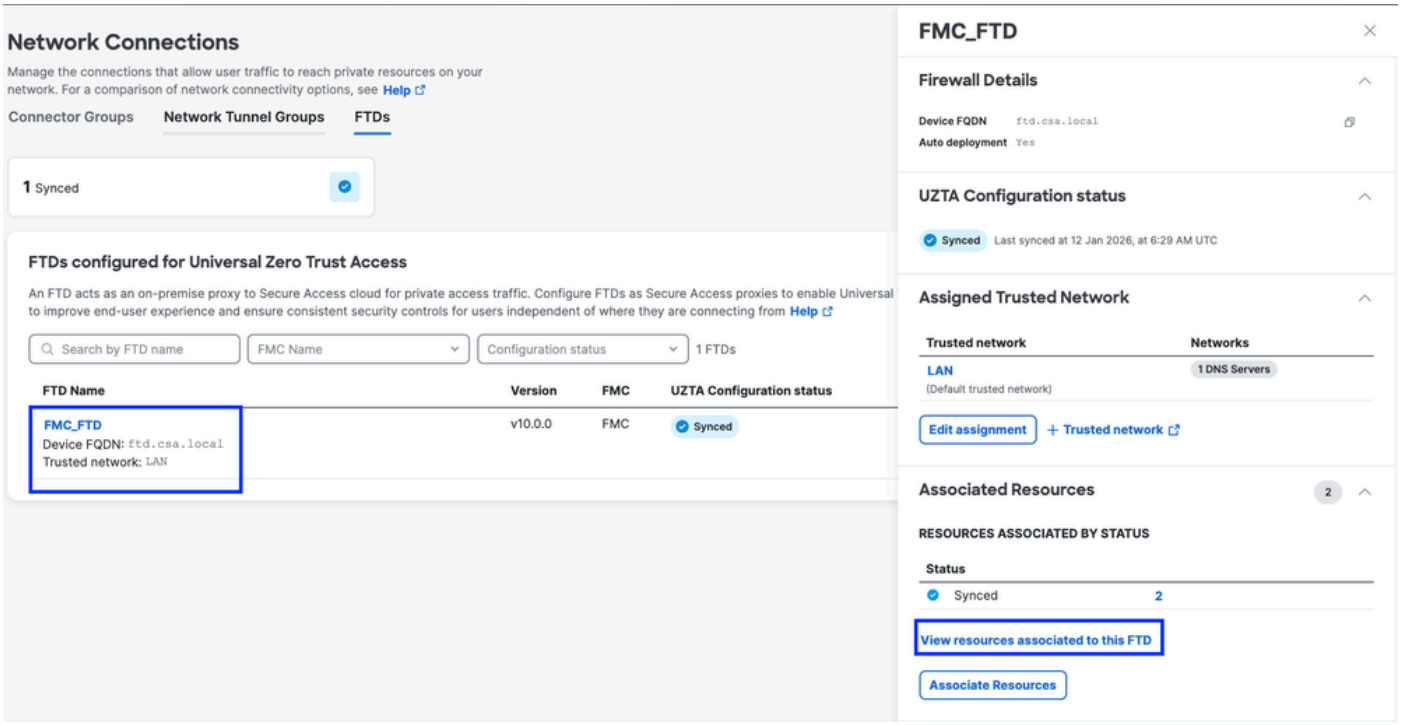
Étape 3 - Vérifiez l'association de PR sur le FTD

1. Accédez à connect > Network Connections > FTDs

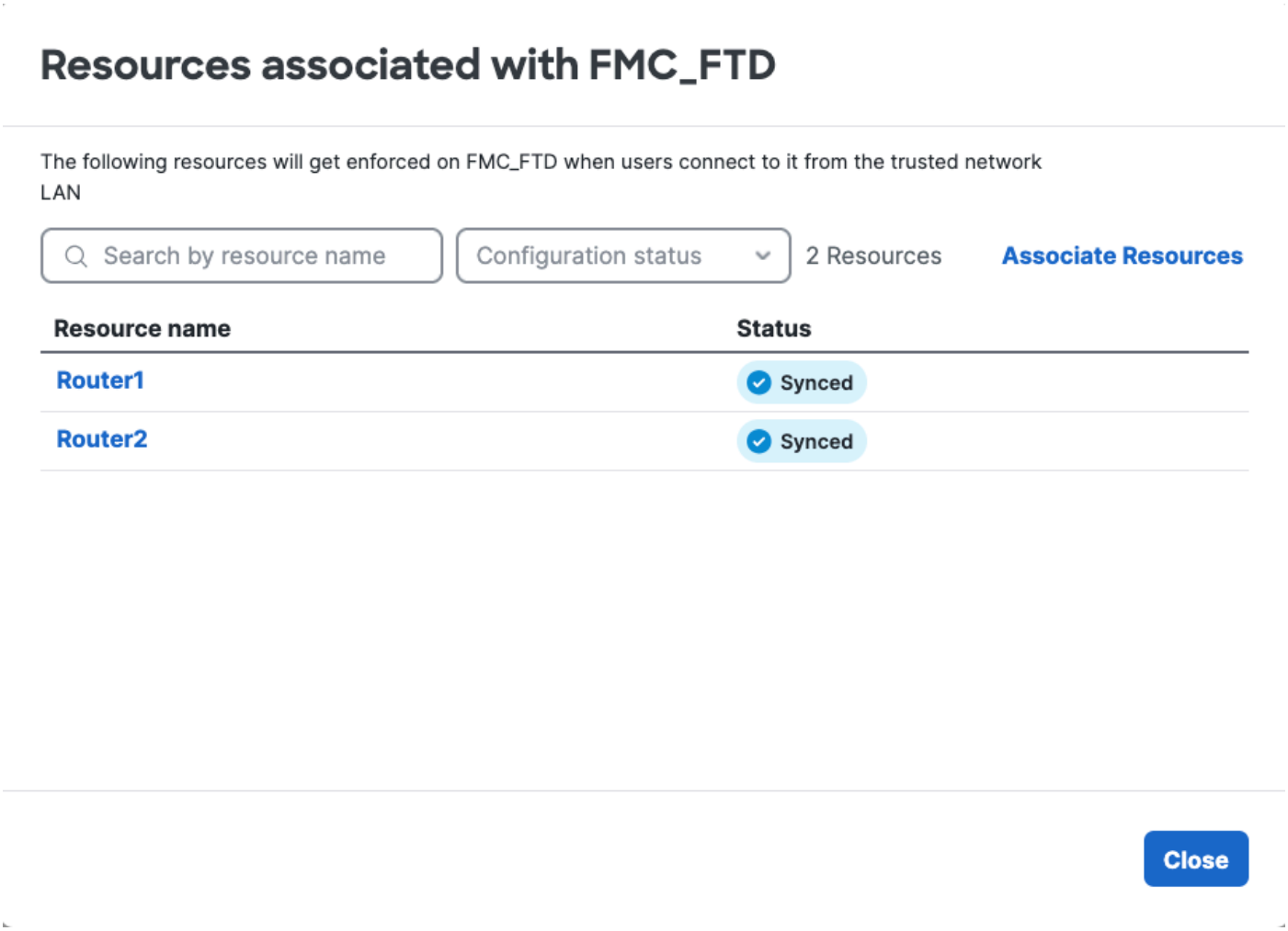


Accès sécurisé - Vérification PR

2. Cliquez sur le FTD > Afficher les ressources associées à ce FTD

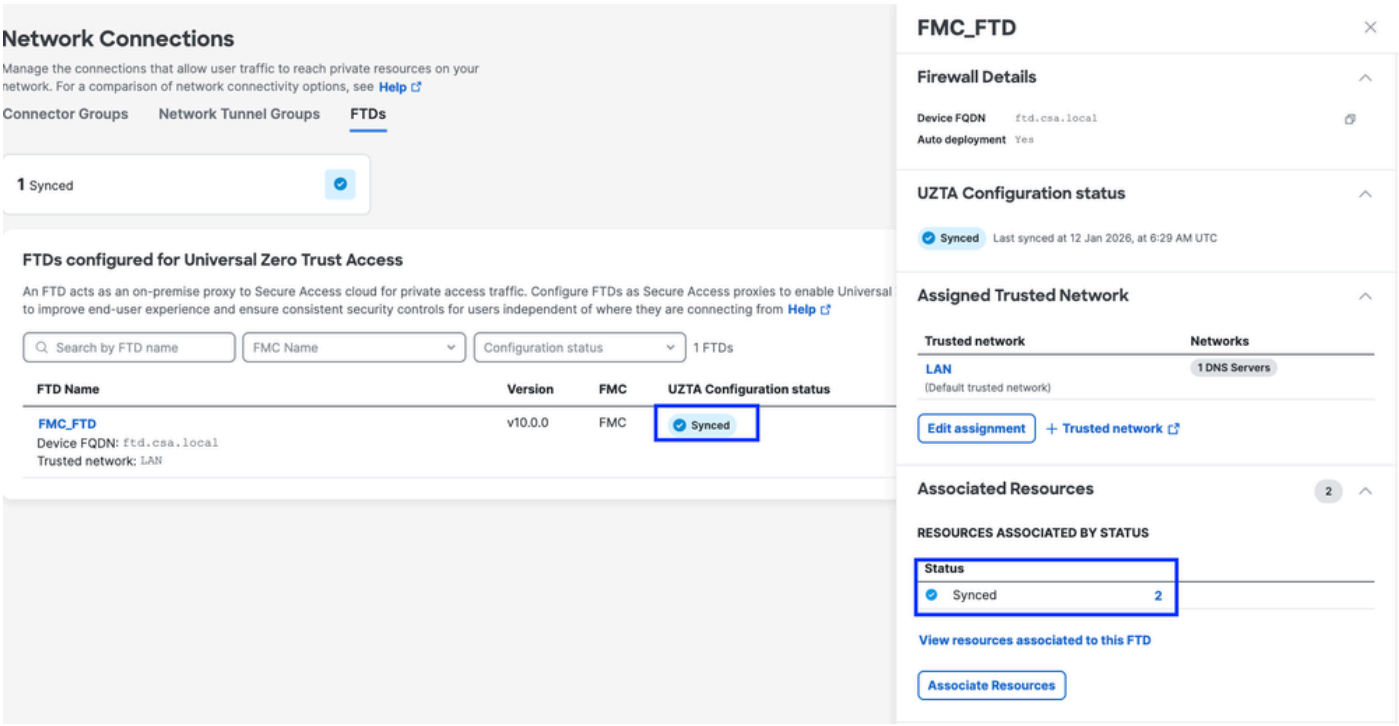


Accès sécurisé - Vérification PR



3. Cliquez sur Fermer

4. Vérifiez l'état , la ressource associée et la configuration doivent être à l'état Synchronisé



Accès sécurisé - Vérification PR

5. Vérifiez que la configuration a été poussée vers FTD

Connectez-vous à l'interface de ligne de commande FTD et passez en mode LINA

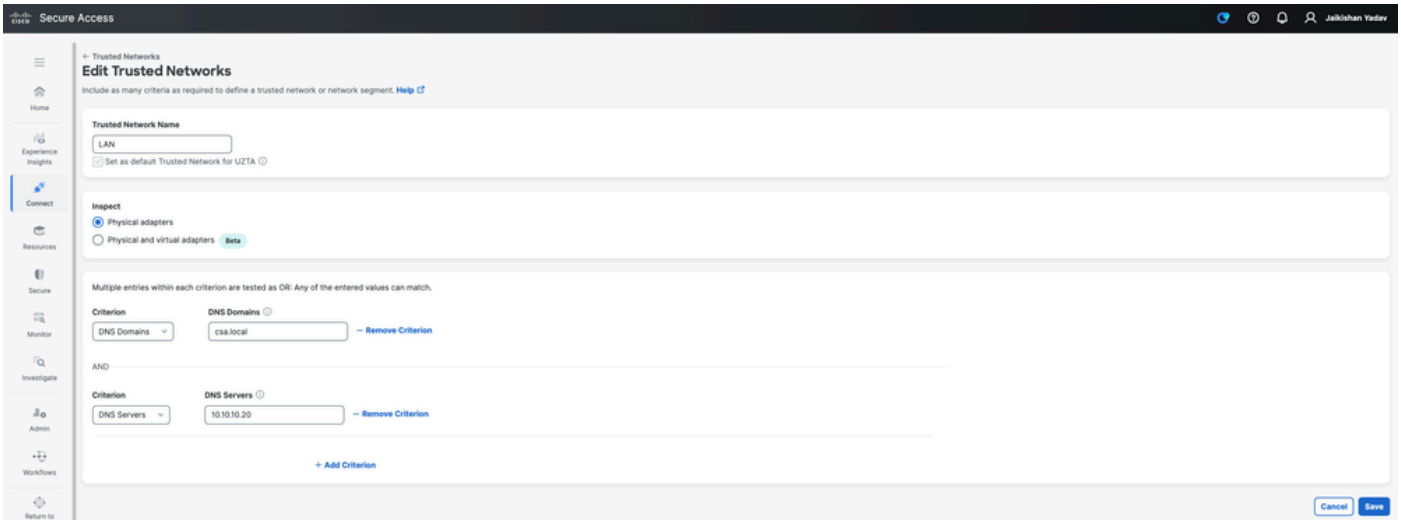
show running-config object application

```
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
```

Accès sécurisé - Vérification PR

Étape 4 - Configurez « Gérer les réseaux approuvés ou les paramètres ZTA »

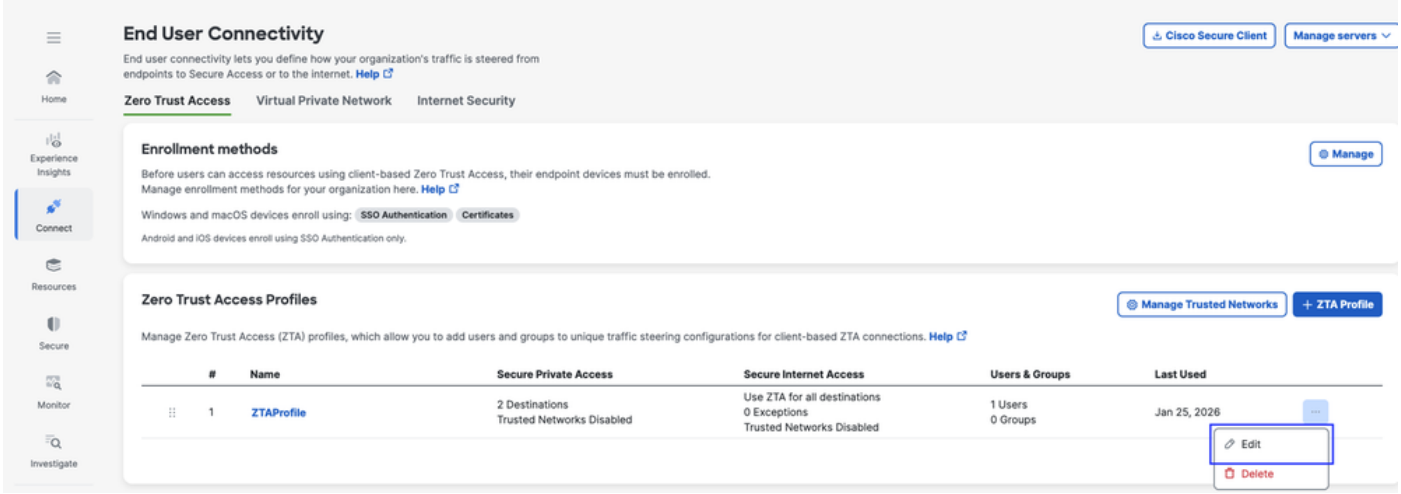
Naviguez jusqu'à Connect > End User Connectivity > Zero Trust Access > ZTA Settings et configurez Trusted Networks



Accès sécurisé - Configuration TND

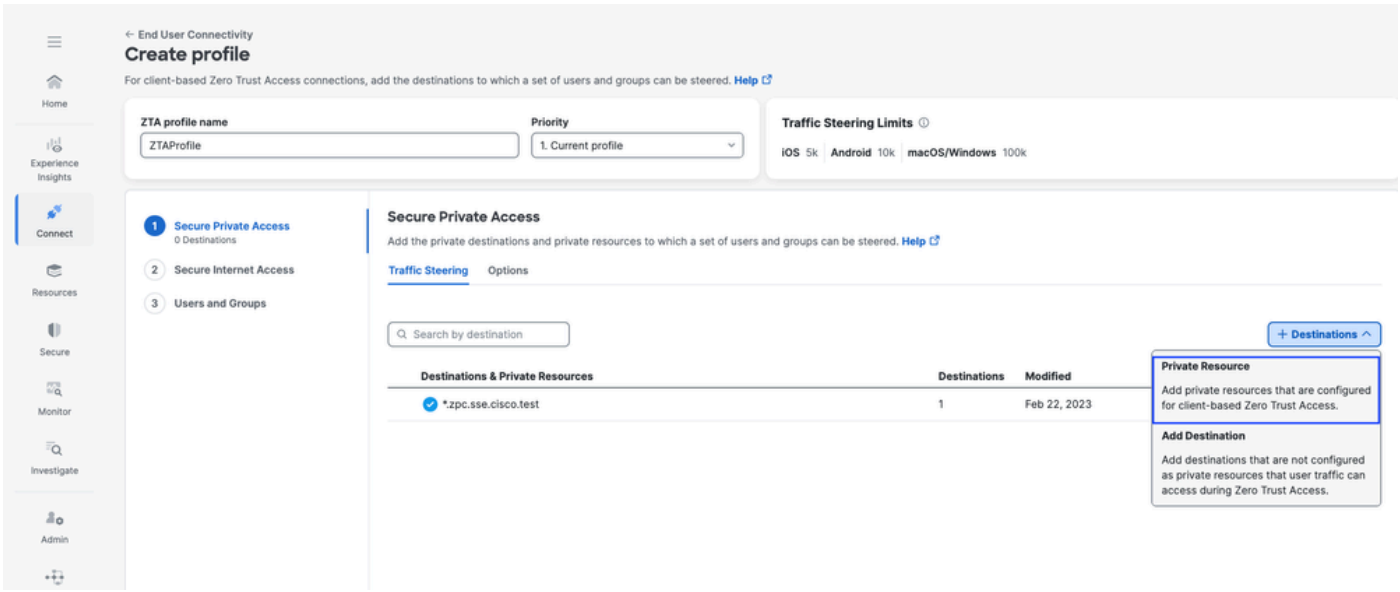
Étape -5 - Ajoutez une ressource privée au profil ZTA

1. Accédez à Connect > End User Connectivity > Zero Trust Access et cliquez sur 3 points pour modifier le profil ZTA

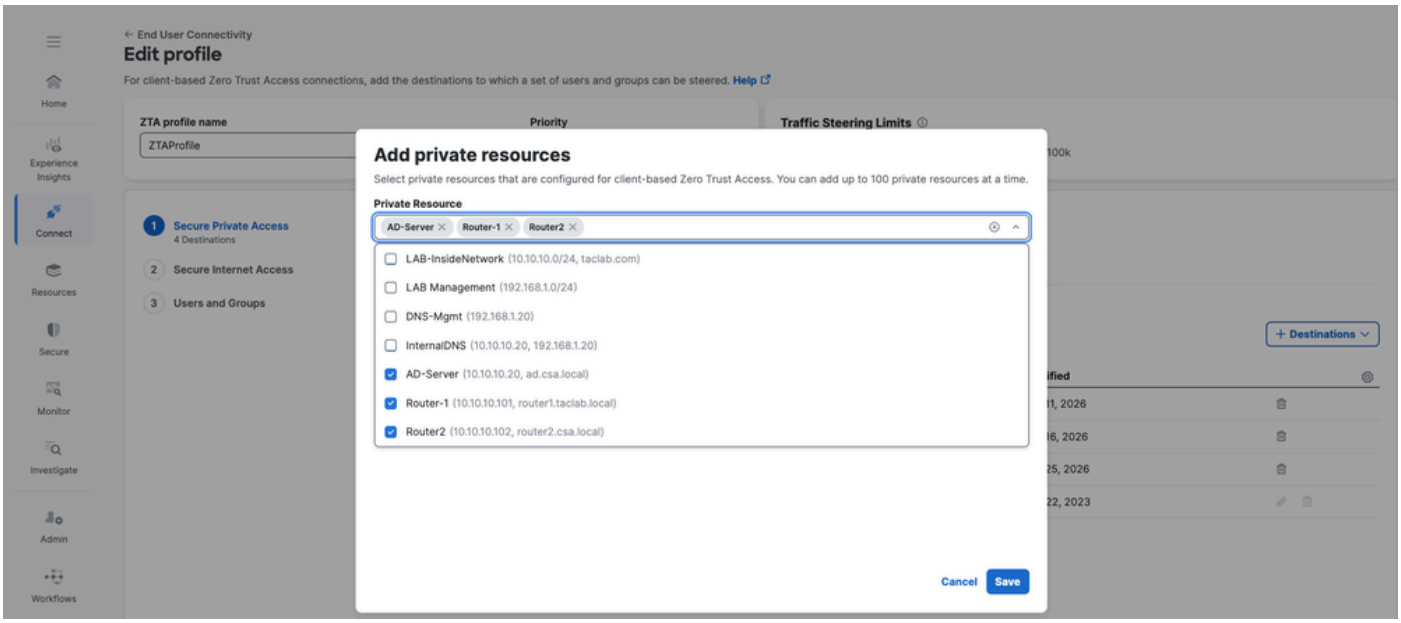


Accès sécurisé - Profil ZTA

2. Ajouter la ressource privée

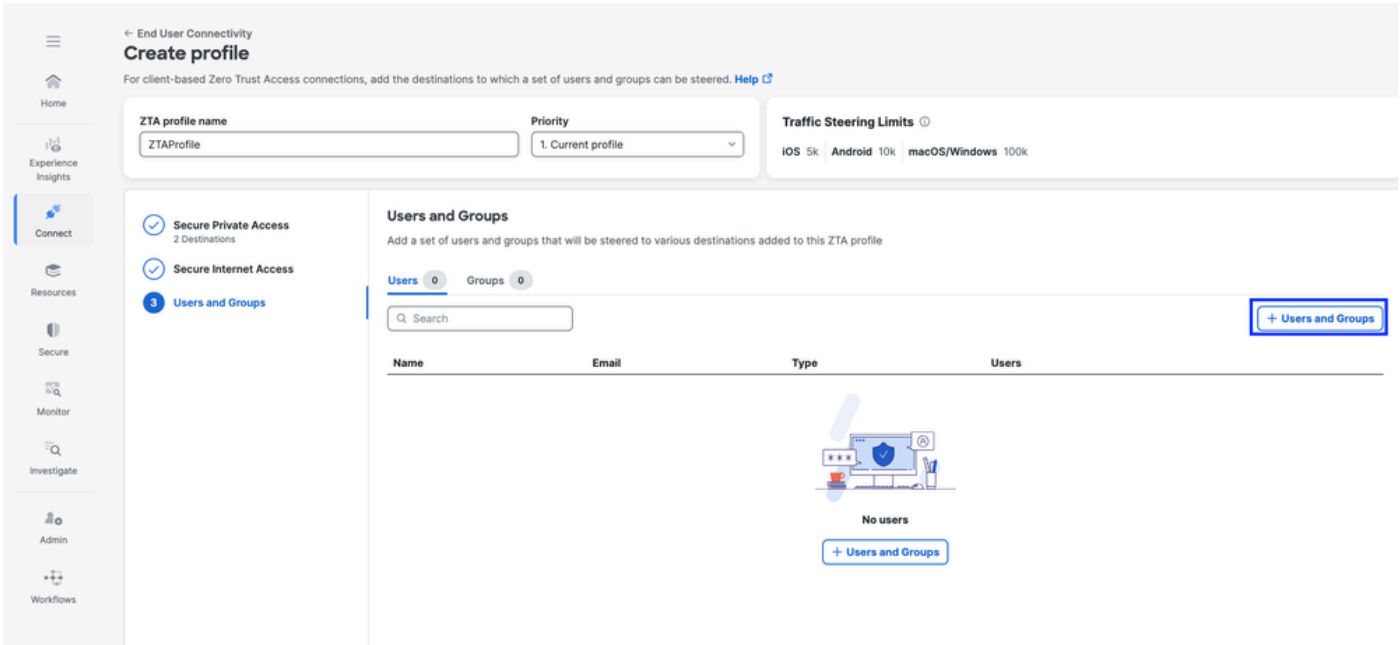


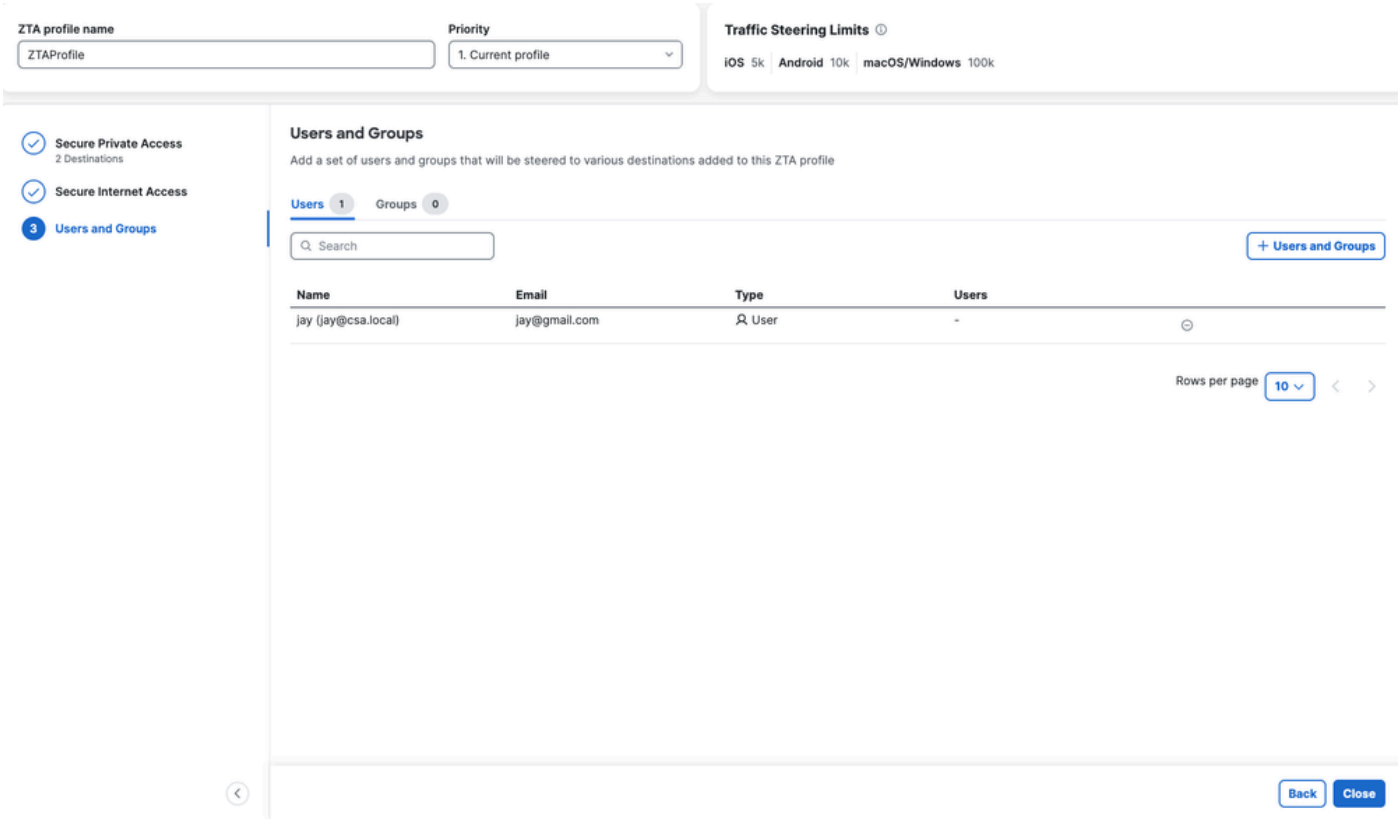
Accès sécurisé - Profil ZTA



Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes

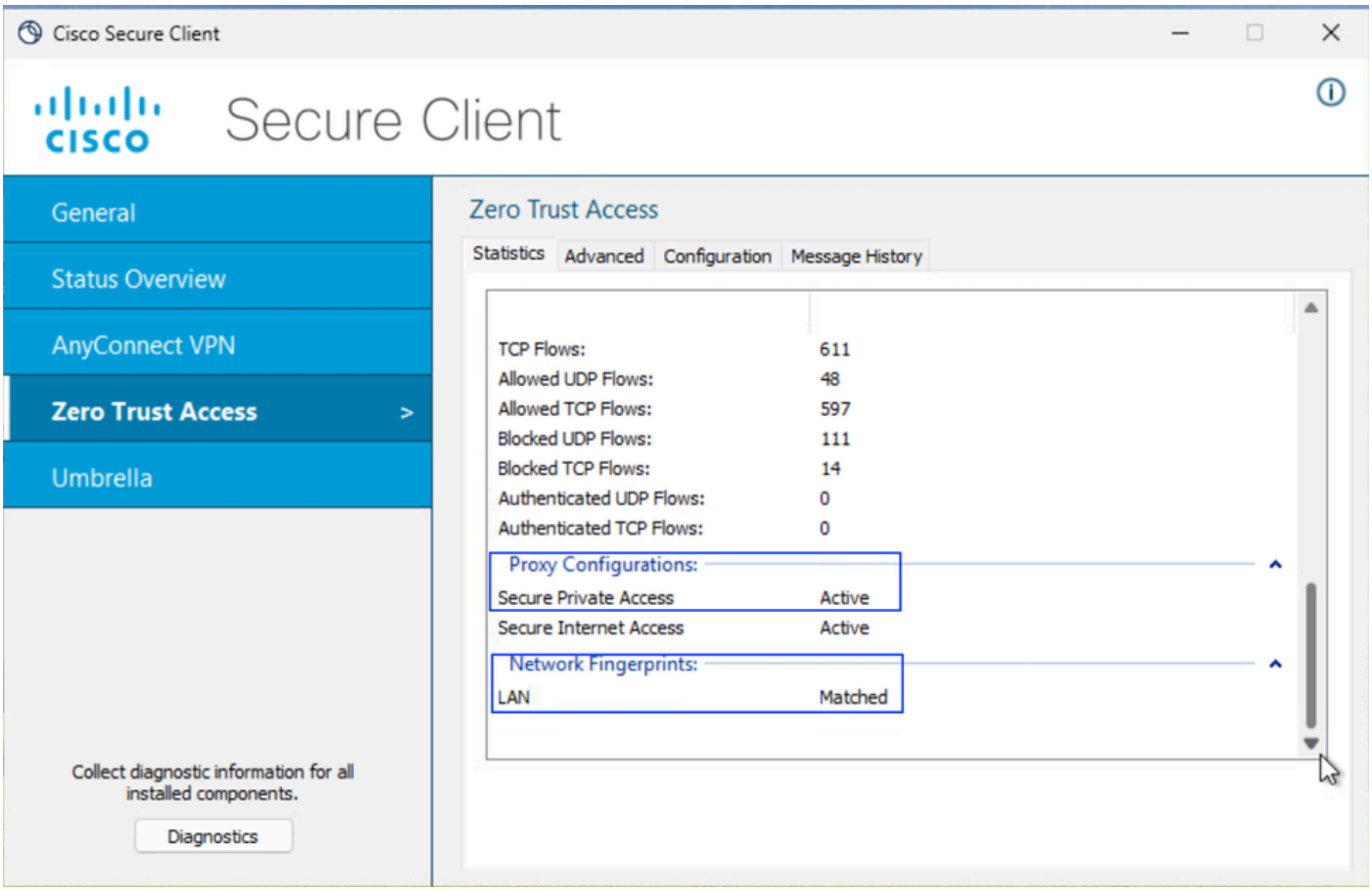




Accès sécurisé - Profil ZTA

Étape 6 - Vérifiez l’accès à la ressource privée

1. Vérification de l'empreinte numérique du réseau pour ZTA TND



Accès sécurisé - Test PR

2. Vérifier que l'utilisateur distant peut résoudre le FQDN 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
```

Accès sécurisé - Test PR

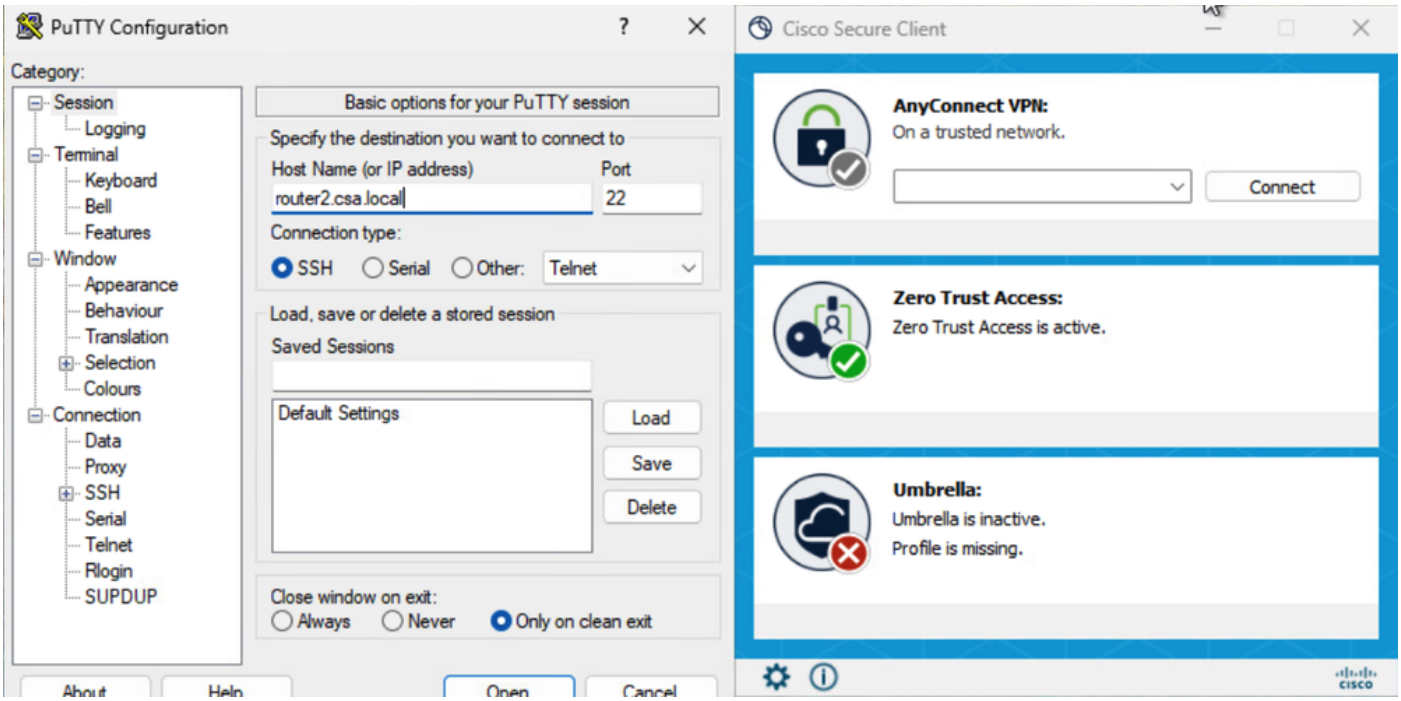
3. Vérifiez que FTD peut atteindre une ressource privée à l'aide du nom de domaine complet

```
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#
```

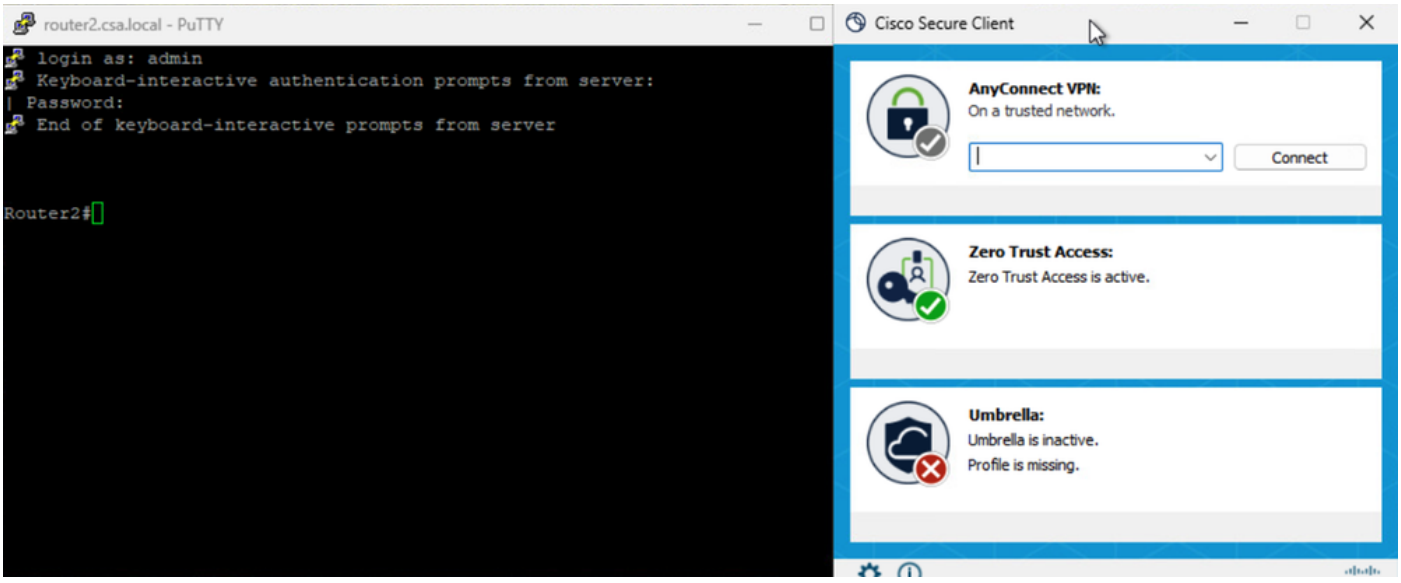
Accès sécurisé - Test PR

4. Tester la connexion SSH à la ressource privée

Accéder au RP à l'aide du FQDN

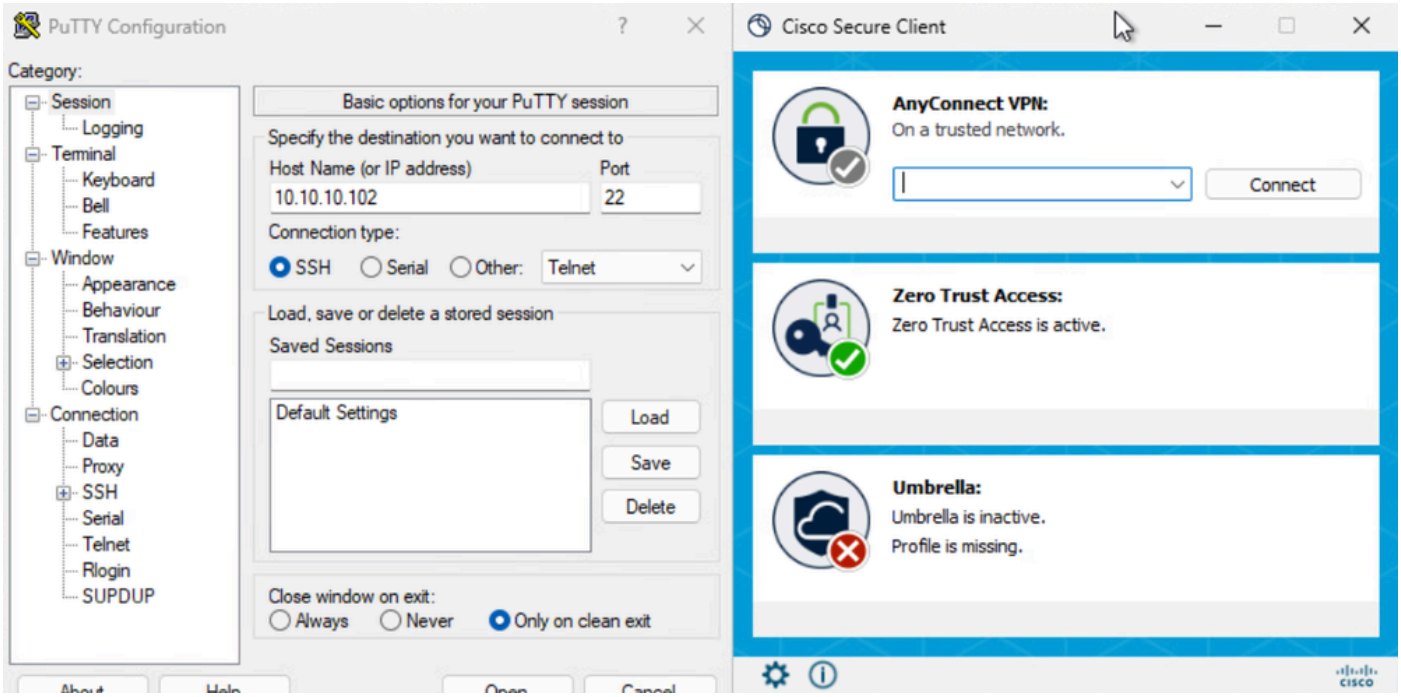


Accès sécurisé - Test PR

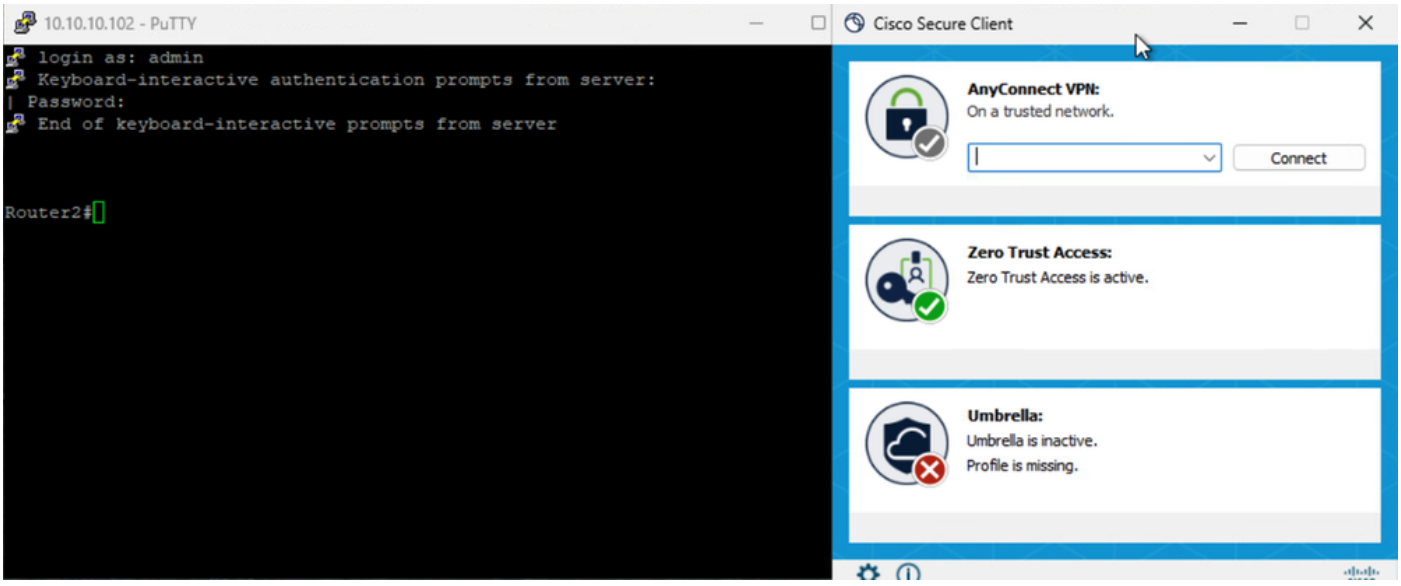


Accès sécurisé - Test PR

Accéder au RP en utilisant l'adresse IP

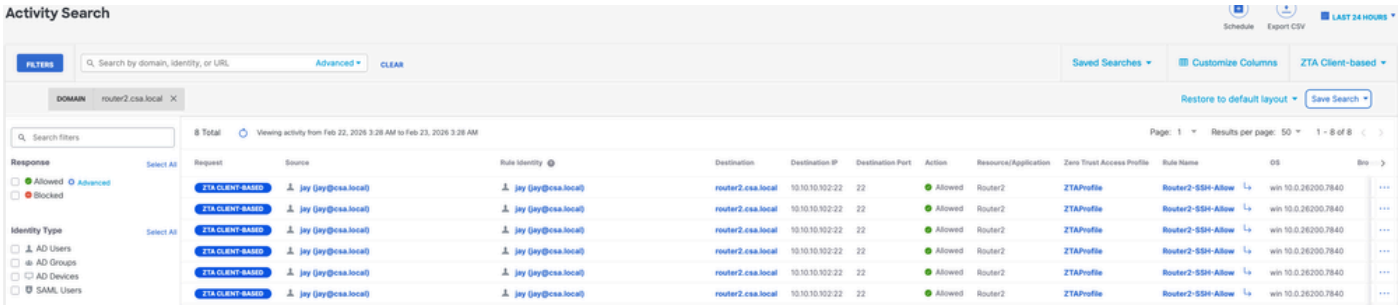


Accès sécurisé - Test PR

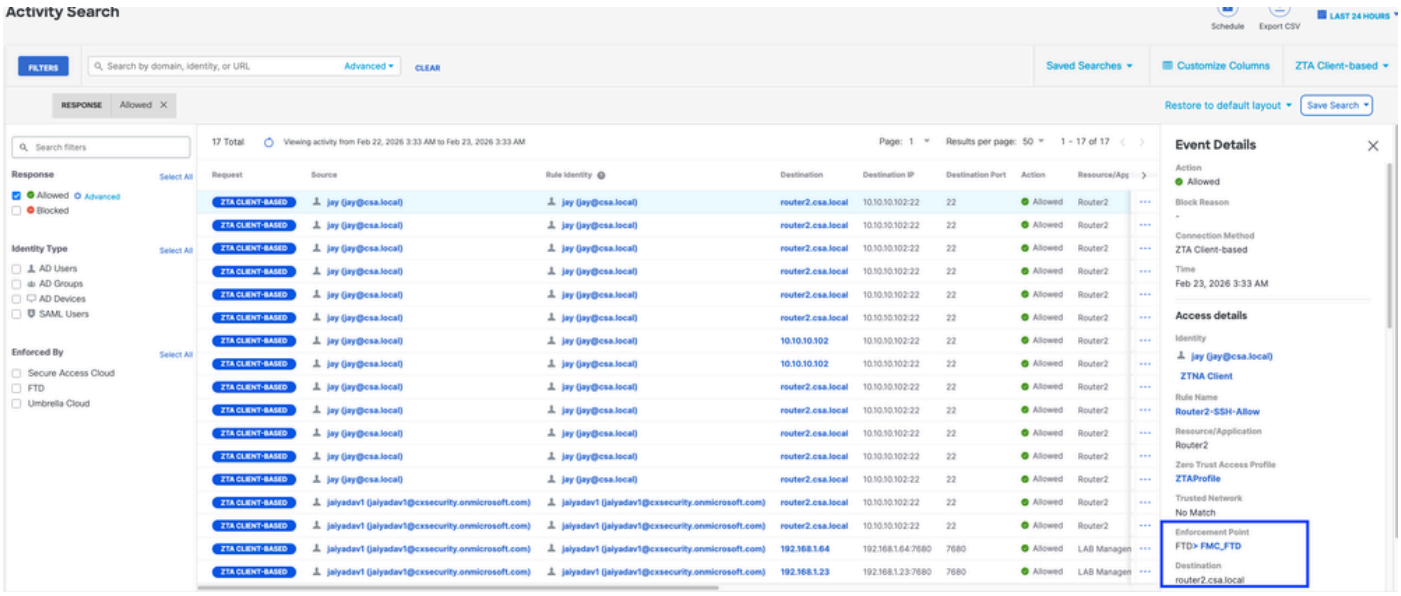


Accès sécurisé - Test PR

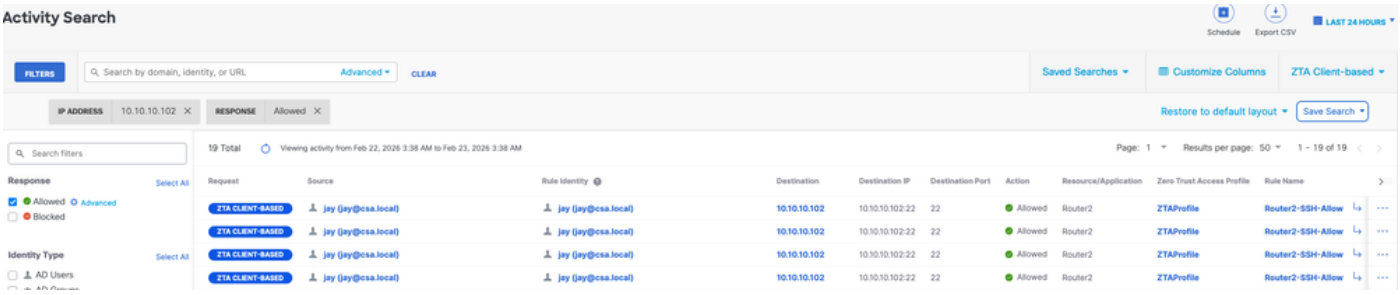
5. Vérification des journaux de recherche d'activité Secure Access



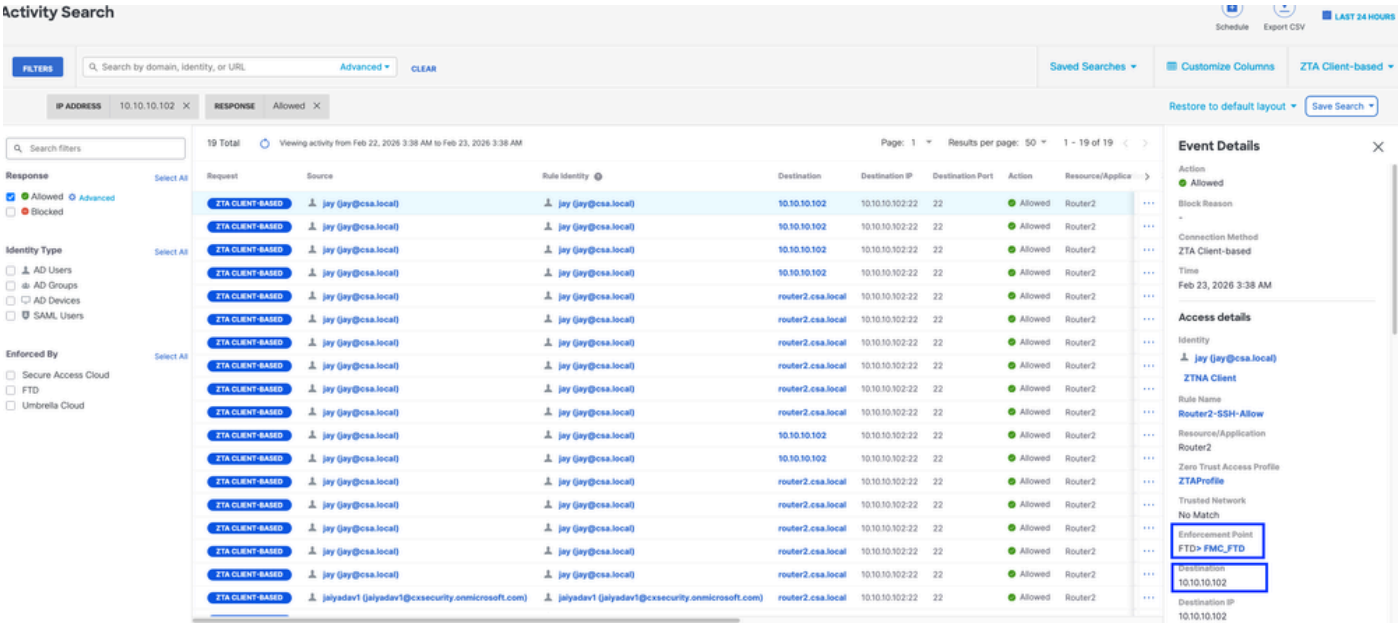
Accès sécurisé - Recherche d'activité



Accès sécurisé - Recherche d'activité

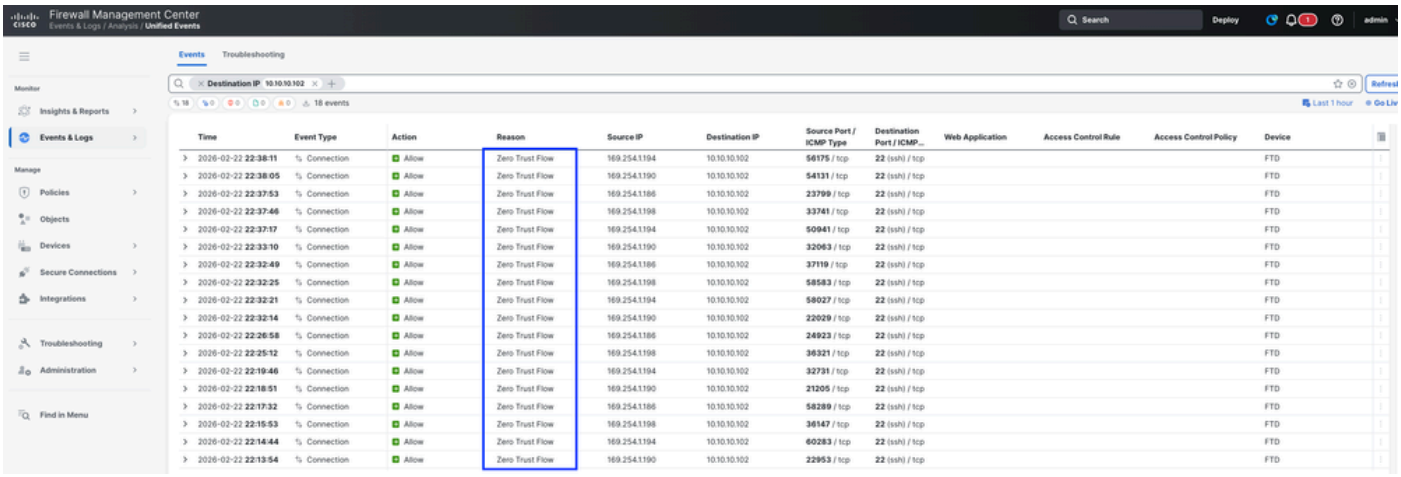


Accès sécurisé - Recherche d'activité



Accès sécurisé - Recherche d'activité

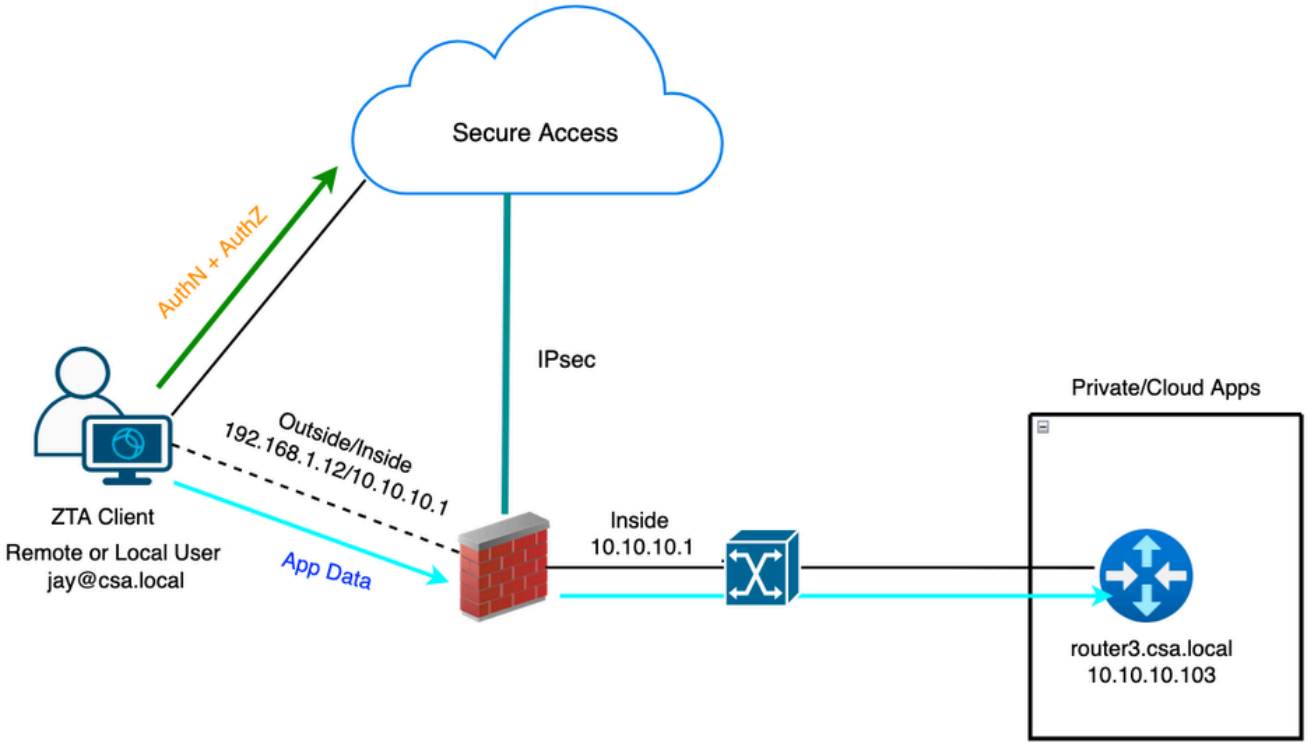
6. Vérifier les événements de connexion FMC



Événements de connexion FMC

Cas de test 4 - Utilisateur local et distant - Application locale ou cloud avec TND

Dans ce cas, le type d'application dépend de l'emplacement de l'utilisateur. Si l'utilisateur est Local ou se trouve derrière une zone FTD approuvée (interne, DMZ, etc.), l'application sera Local (cas de test 3). De même, si l'utilisateur est distant, l'application sera dans le cloud (cas de test 1). L'emplacement de l'utilisateur sera déterminé en fonction du paramètre Network Fingerprint (Empreinte réseau) ou TND. Si l'empreinte réseau correspond, l'emplacement local de l'utilisateur sera Local et s'il ne correspond pas, l'emplacement local de l'utilisateur sera considéré comme Remote .

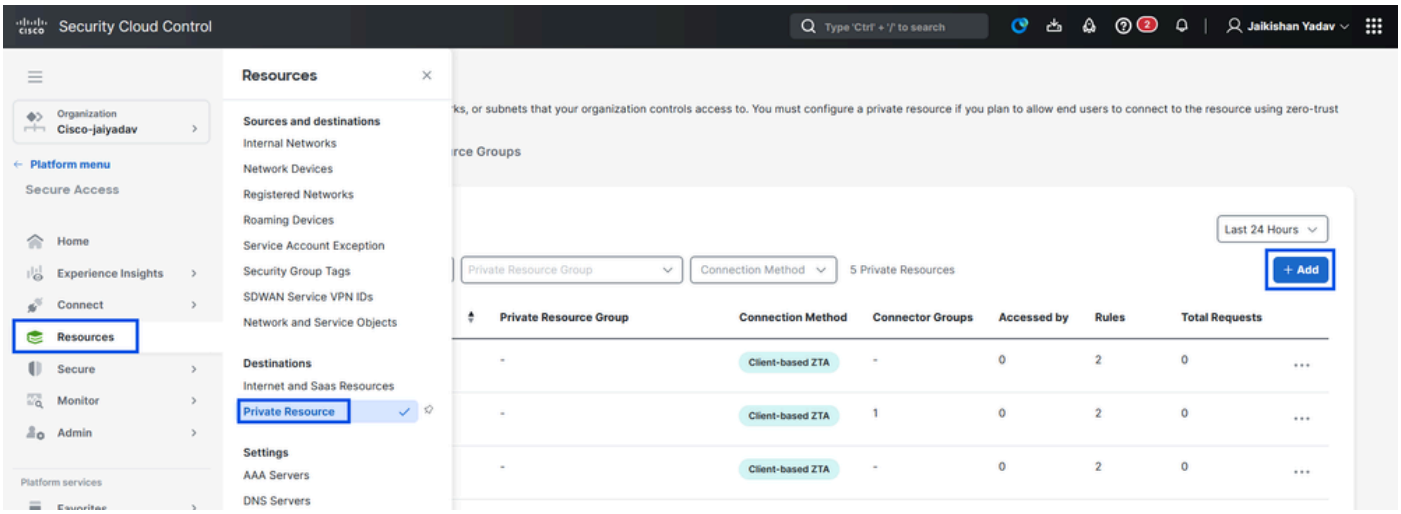


ZTA universel - Topologie de cas de test

Étape 1 : définition d'une ressource privée sur un accès sécurisé

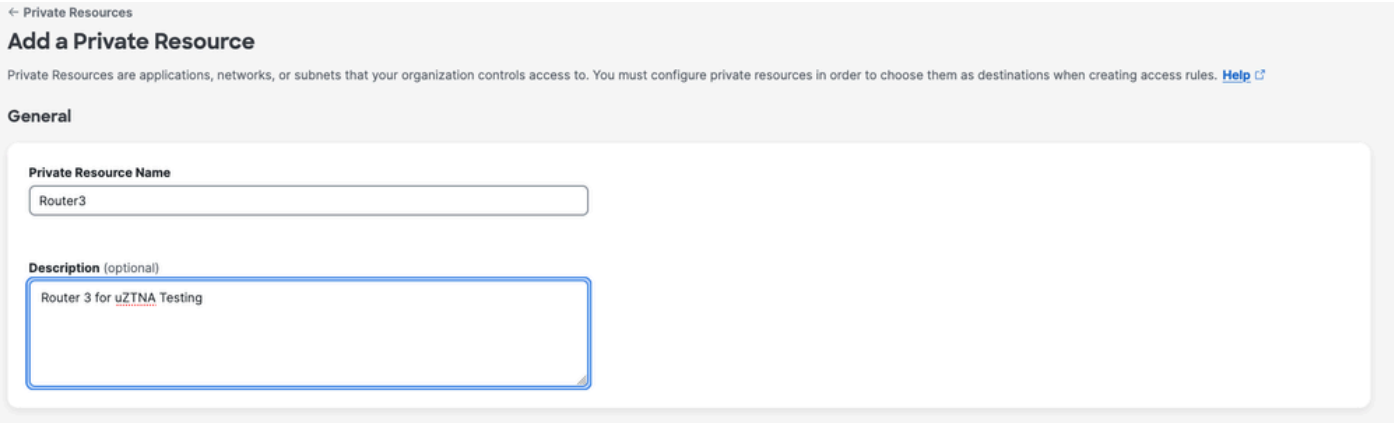
Configurer une ressource privée pour qu'elle soit accessible via un périphérique inscrit ZTA (Zero Trust Access) avec application cloud

1. Accédez à Ressources > Destinations > Ressources privées > Cliquez sur +Ajouter



Accès sécurisé - Configuration des ressources privées

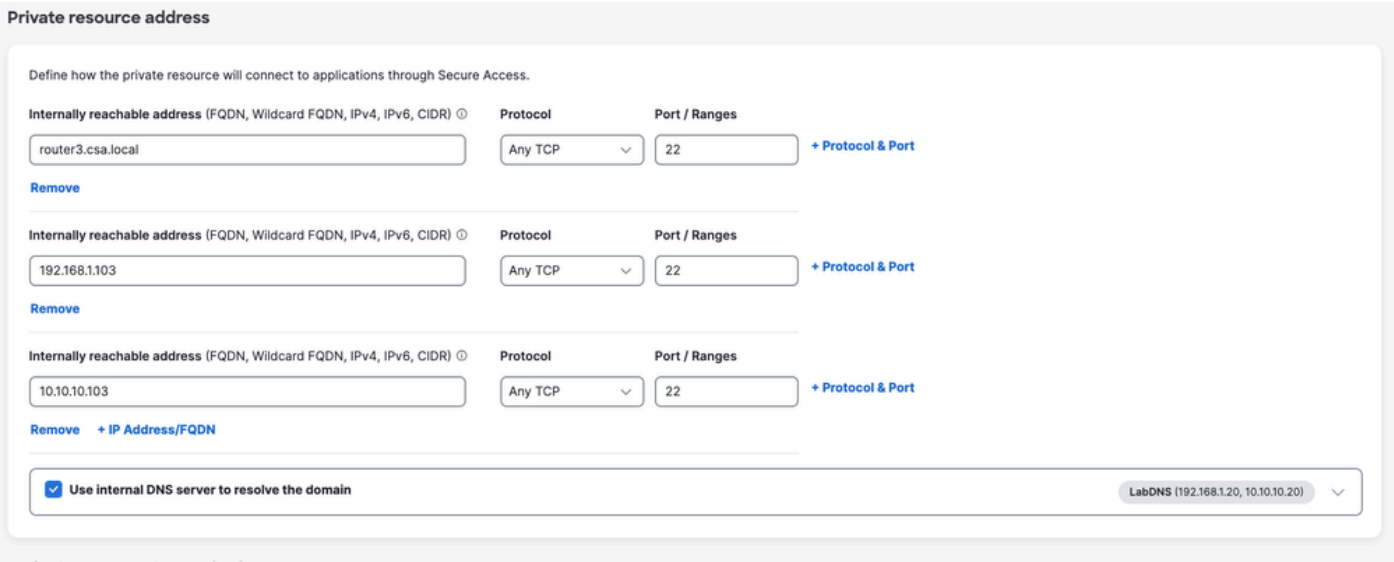
2. Dans le champ Nom de la ressource privée, entrez un nom significatif pour la ressource. Pour Description, nous vous recommandons de fournir des informations telles que l'objectif de la ressource ou le nom du propriétaire de la ressource.



Accès sécurisé - Configuration des ressources privées

3. Entrez le nom de domaine complet de la ressource privée à laquelle vous souhaitez accéder. Nous pouvons également définir l'adresse IP de la ressource privée . Pour plus d'informations, voir Ajouter une ressource privée

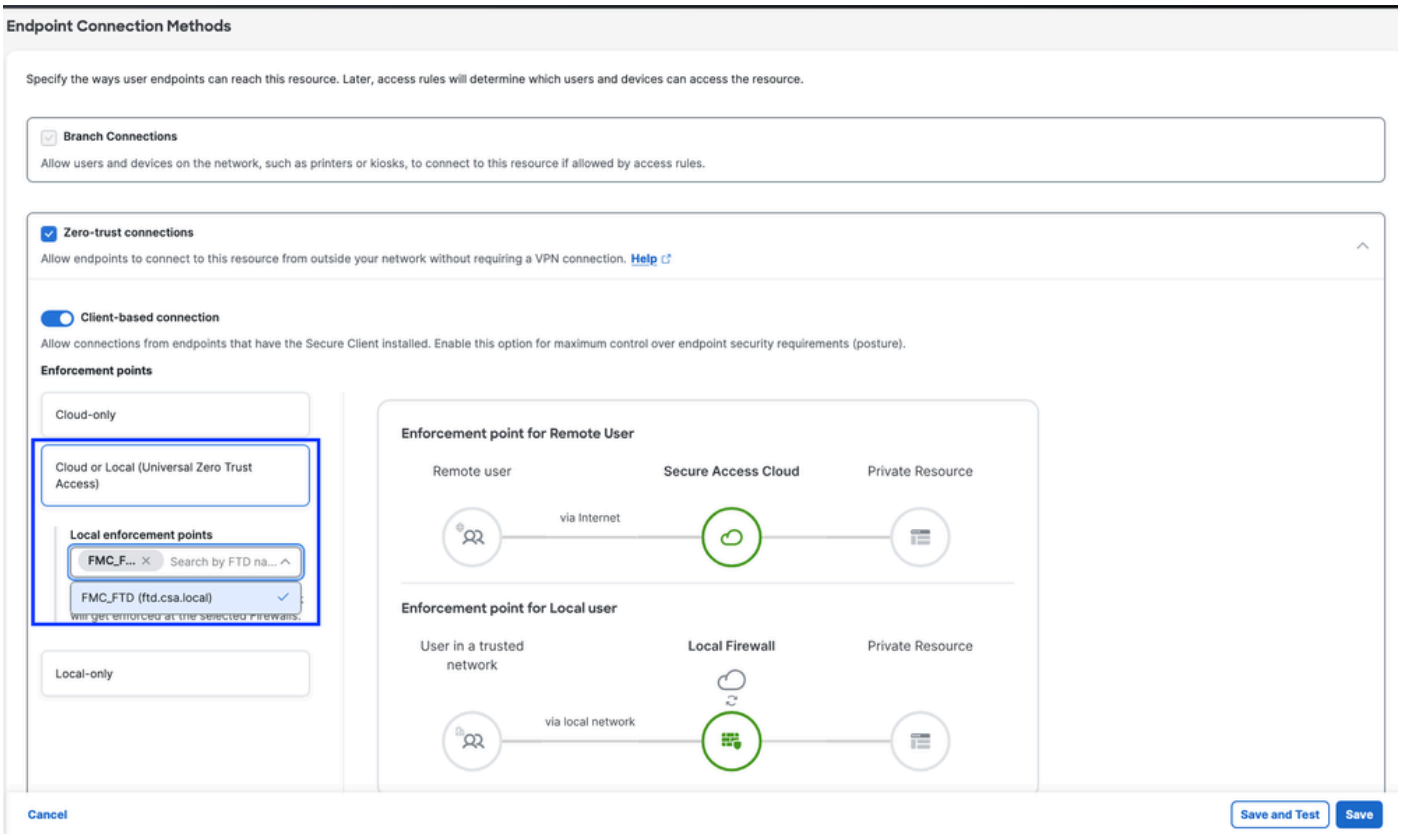
4. Sélectionnez le serveur DNS pour résoudre le domaine



Accès sécurisé - Configuration des ressources privées

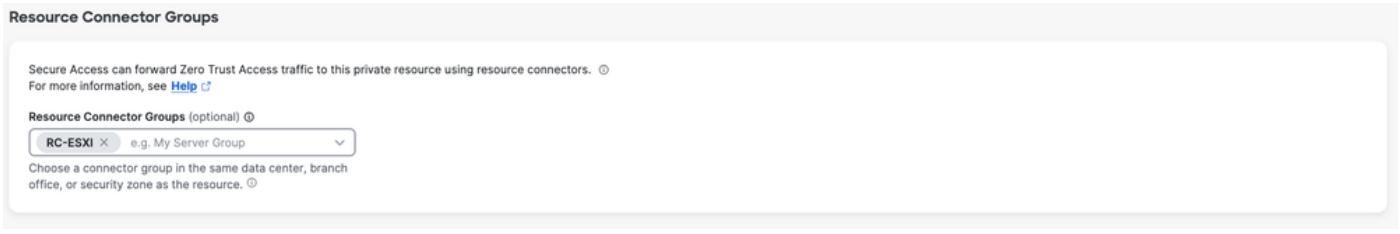
5. Sélectionner les méthodes de connexion Endpoint

6. Sélectionnez FTD comme points d'application locaux



Accès sécurisé - Configuration des ressources privées

Sélectionnez RC si la ressource privée est accessible sur RC , sinon laissez vide si la ressource privée est accessible sur le groupe de tunnels réseau (tunnel IPsec).



Accès sécurisé - Configuration des ressources privées

Remarque : Selon le type d'inscription sélectionné, cette modification associera automatiquement le PR au FTD et déclenchera un déploiement de stratégie

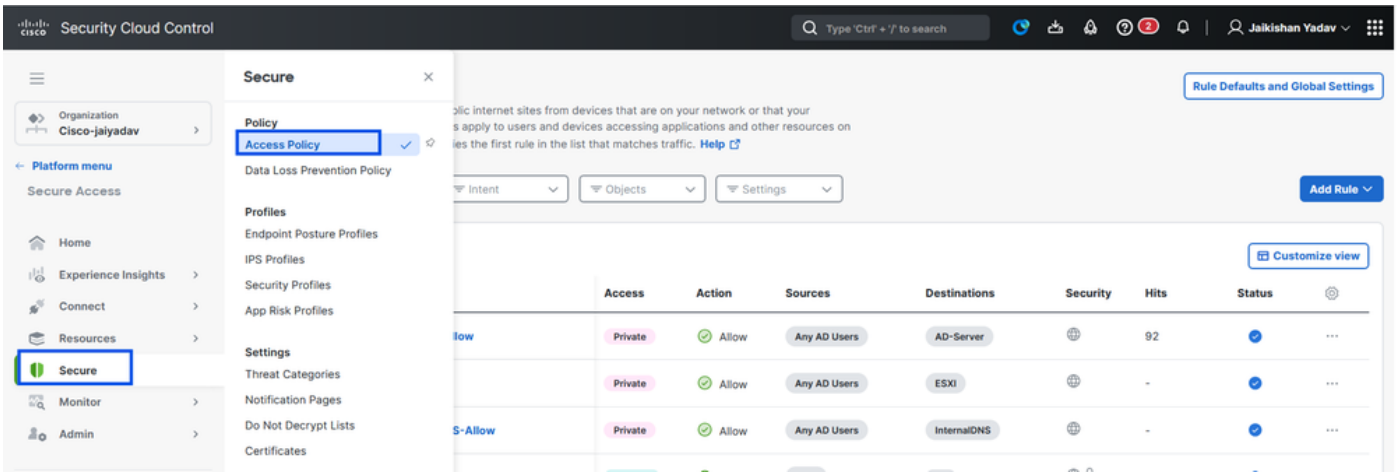
---

7. Cliquez sur Save (enregistrer)

Étape 2 : création d'une règle d'accès privé

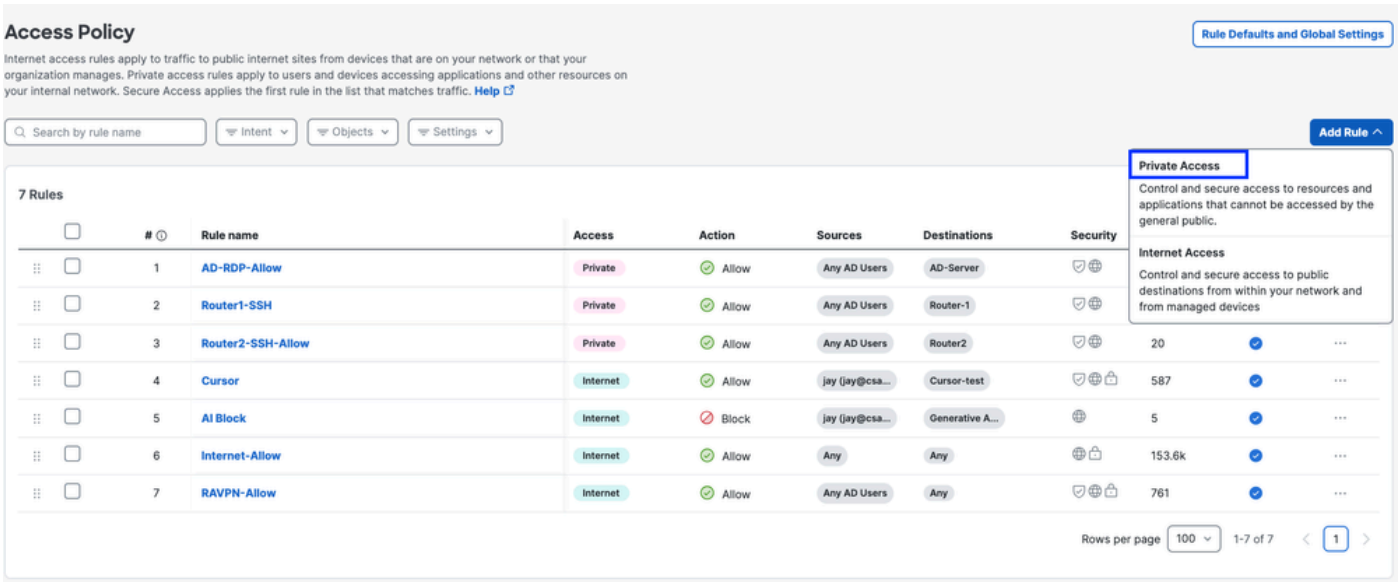
Configurez un accès privé sur Secure Access pour que les utilisateurs inscrits à Universal ZTA puissent y accéder. Pour plus d'informations, consultez [Règle d'accès privé]

1. Accédez à Secure > Access Policy



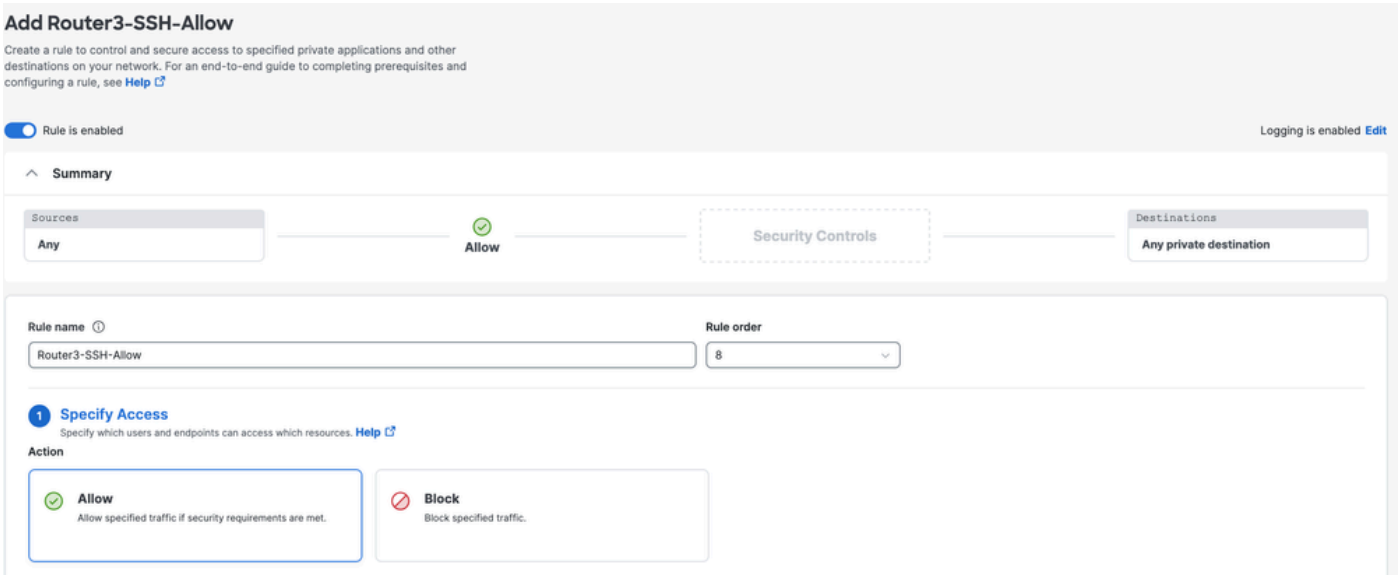
Accès sécurisé - Configuration de la stratégie d'accès

2. Cliquez sur Ajouter une règle, puis choisissez Accès privé.
   En haut de la règle se trouve un résumé qui décrit les composants configurés de votre règle.



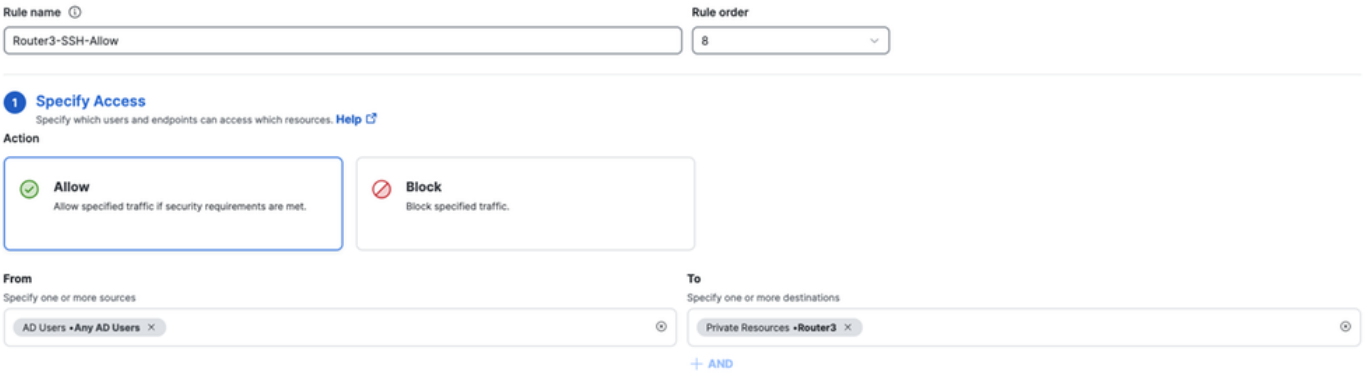
Accès sécurisé - Configuration de la stratégie d'accès

3. Ajouter un nom de règle



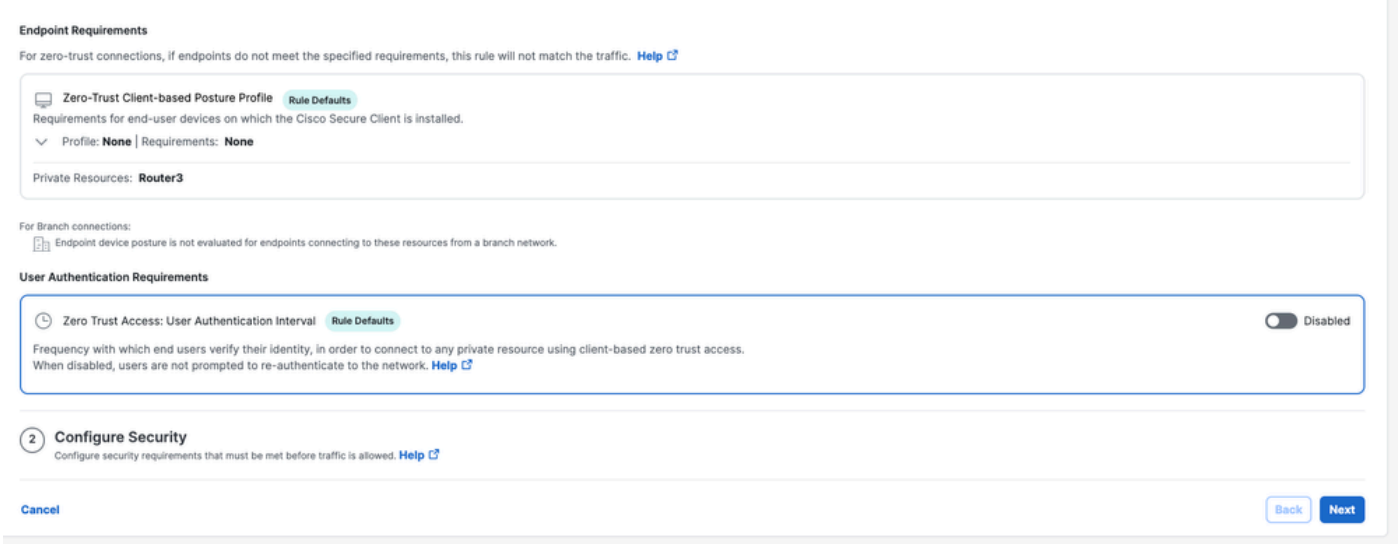
Accès sécurisé - Configuration de la stratégie d'accès

4. Sélectionnez l'action de règle et sélectionnez l'origine et la destination



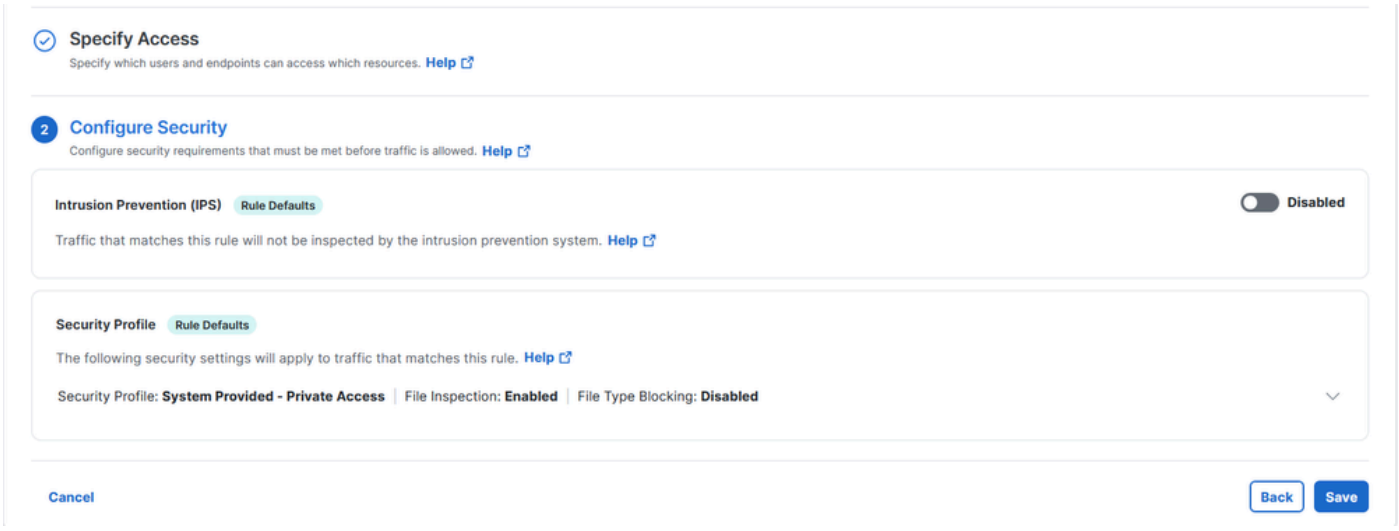
Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux



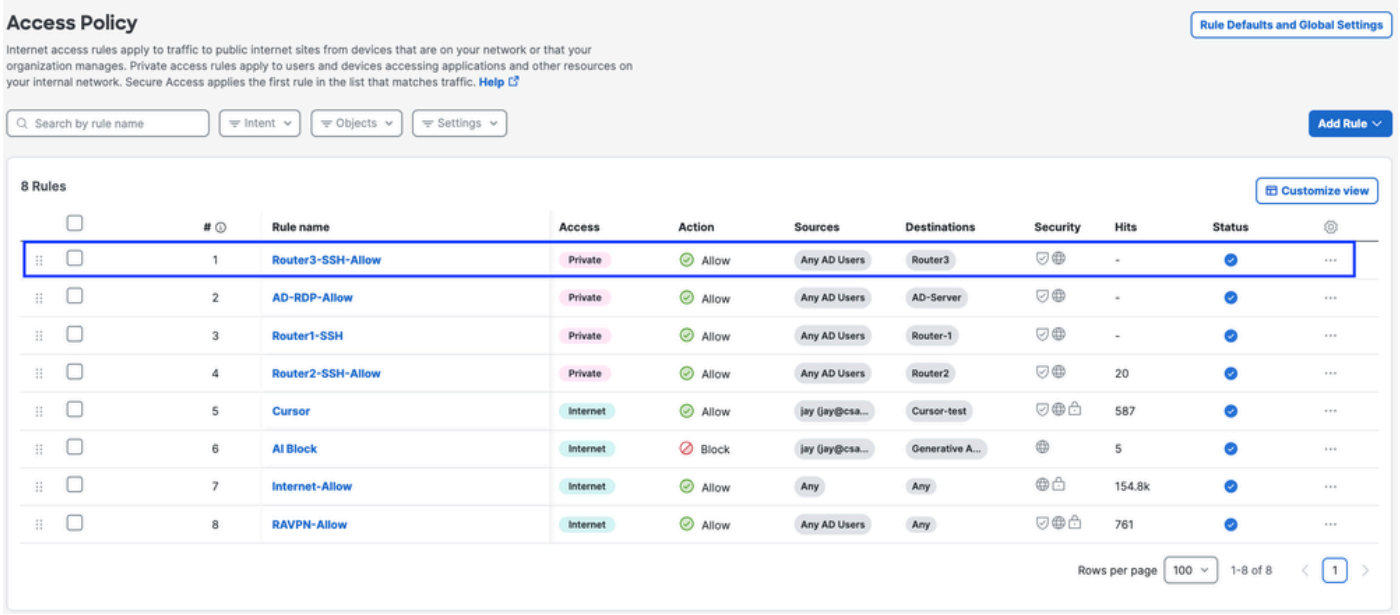
Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité



Accès sécurisé - Configuration de la stratégie d'accès

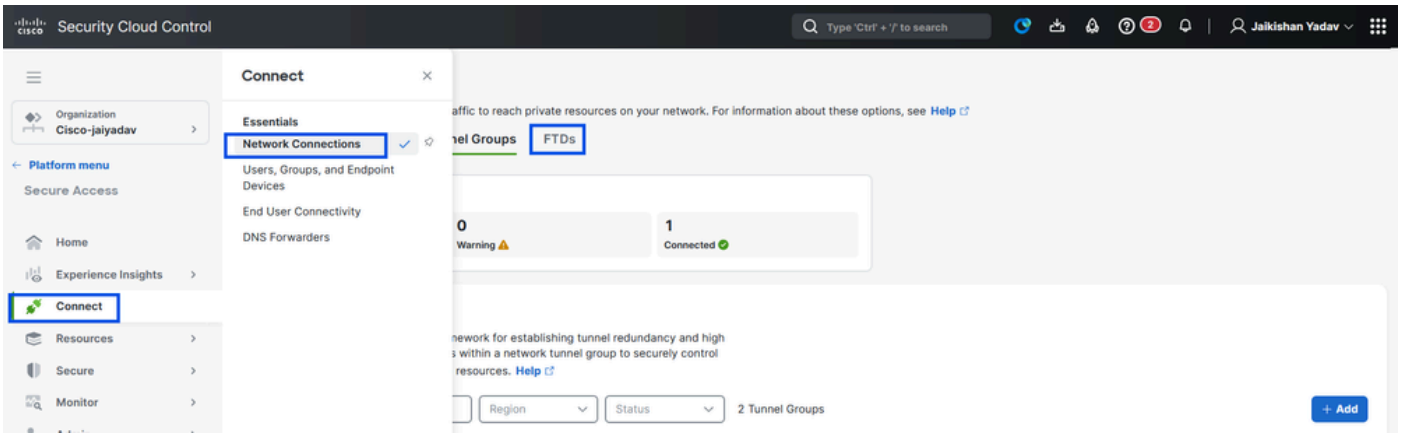
7. Cliquez sur Enregistrer



Accès sécurisé - Configuration de la stratégie d'accès

Étape 3 - Vérifiez l'association de PR sur le FTD

1. Accédez à connect > Network Connections > FTDs

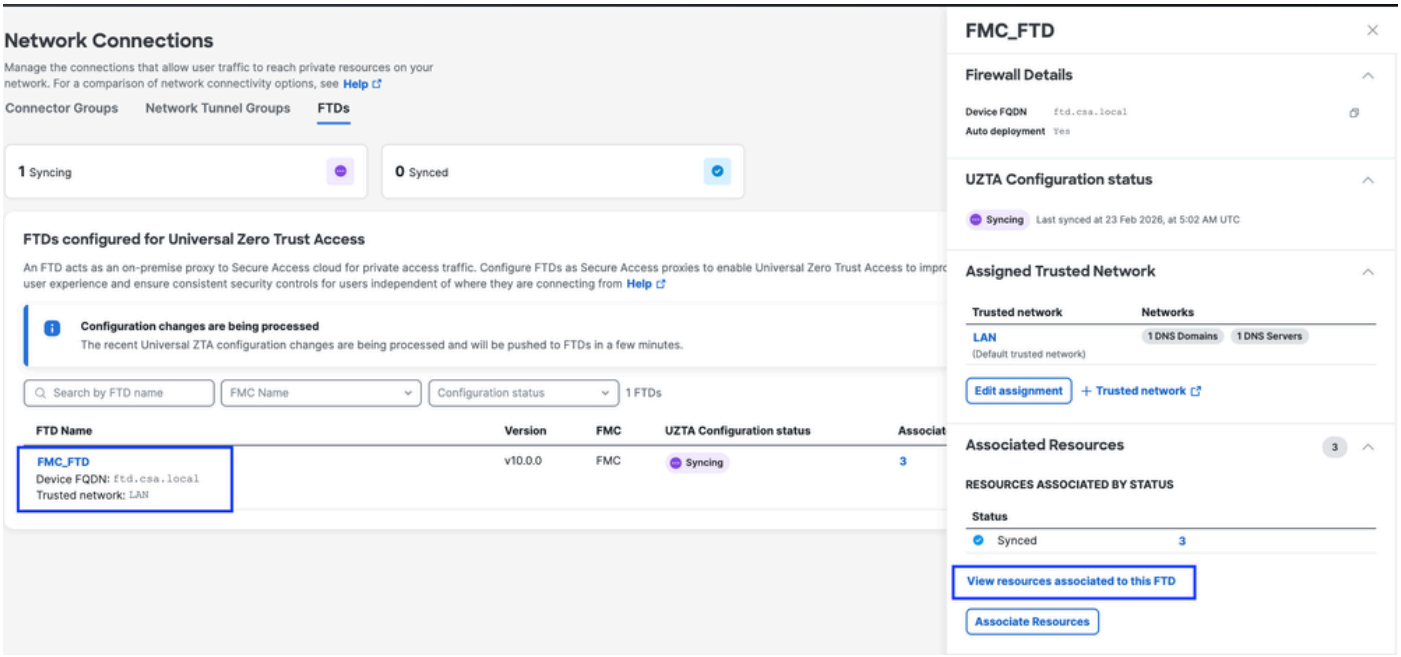


Accès sécurisé - Vérification PR

2. Cliquez sur le FTD > Afficher les ressources associées à ce 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
```

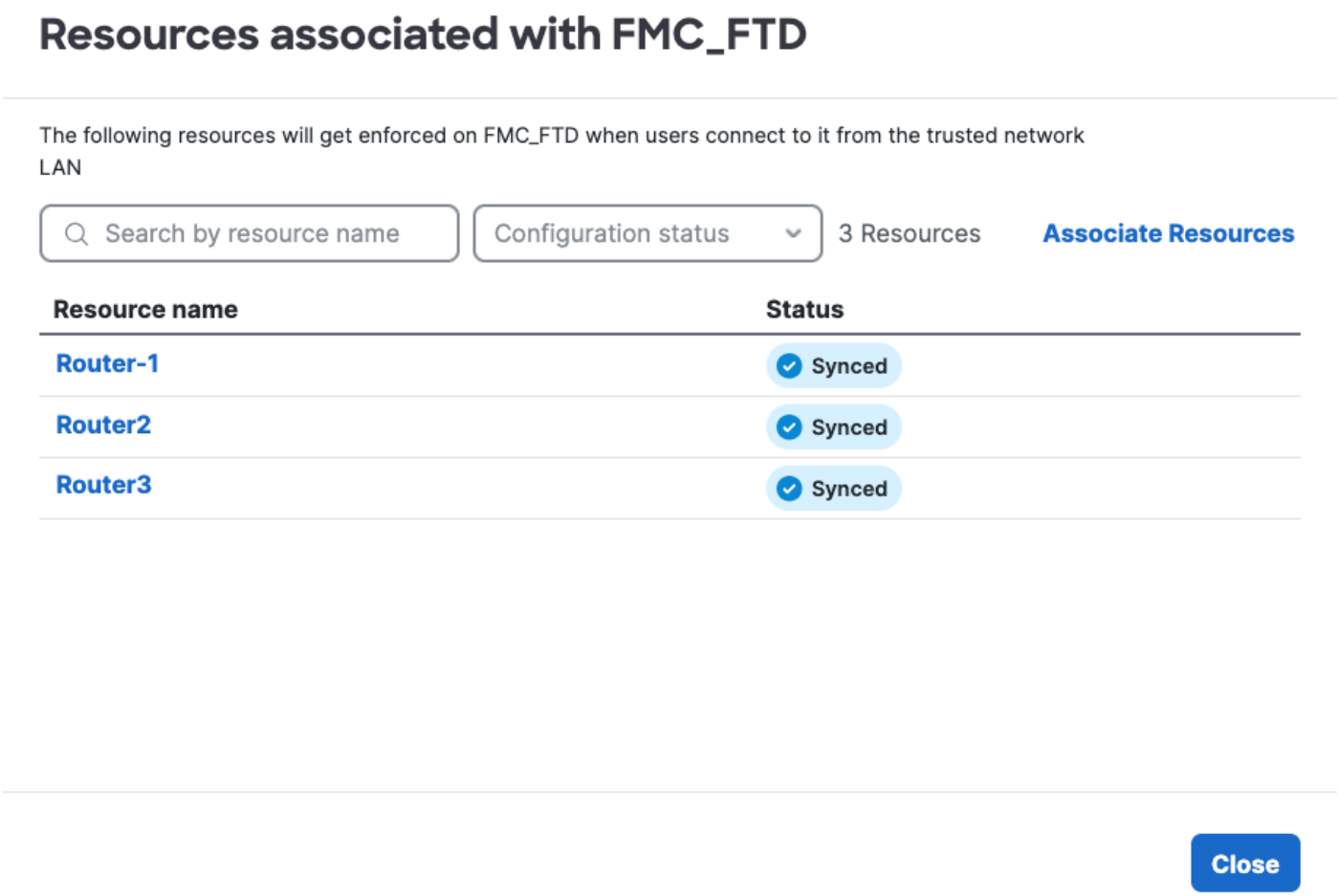
Accès sécurisé - Vérification PR



Accès sécurisé - Vérification PR

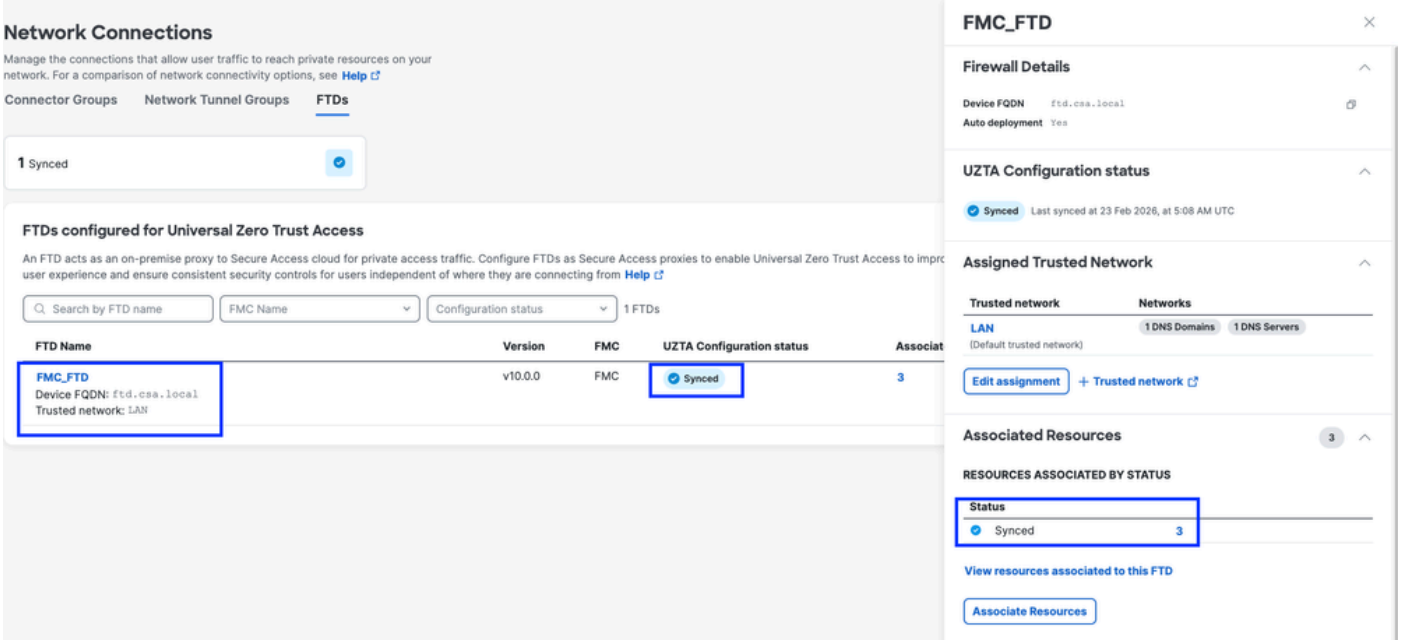
```
C:\Users\jay>ping ftd.csa.local

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
```

Accès sécurisé - Vérification PR



3. Cliquez sur Fermer

4. Vérifiez l'état , la ressource associée et la configuration doivent être à l'état Synchronisé



Accès sécurisé - Vérification PR

5. Vérifiez que la configuration a été poussée vers FTD

Connectez-vous à l'interface de ligne de commande FTD et passez en mode LINA

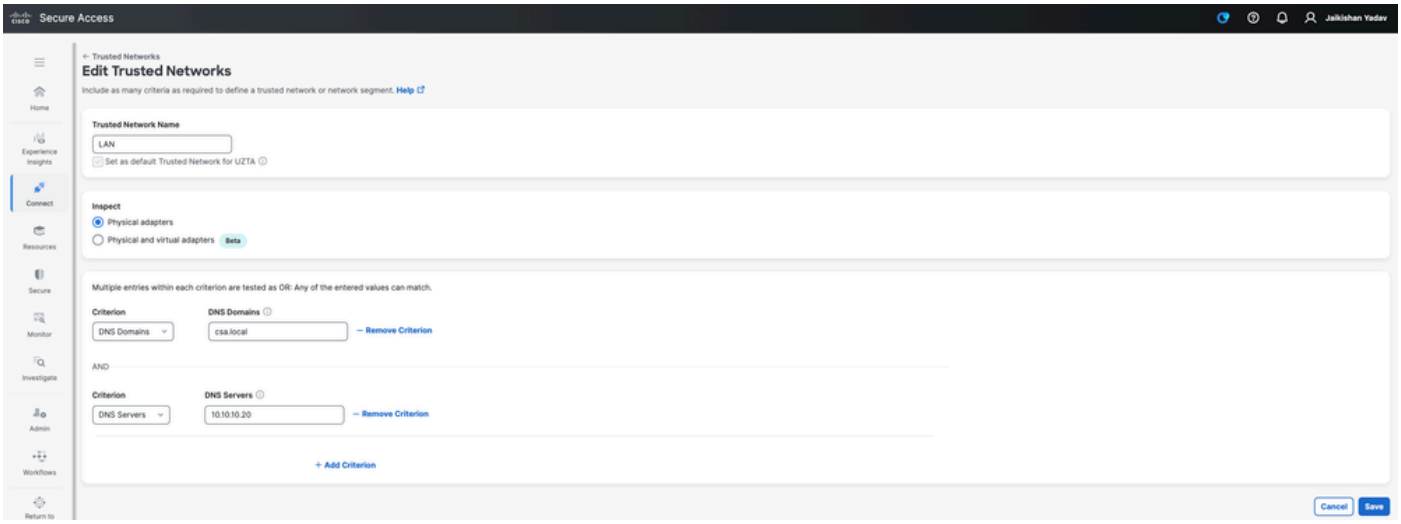
show running-config object application

```
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
```

Accès sécurisé - Vérification PR

Étape 4 - Configurez ou vérifiez « Gérer les réseaux de confiance ou les paramètres ZTA »

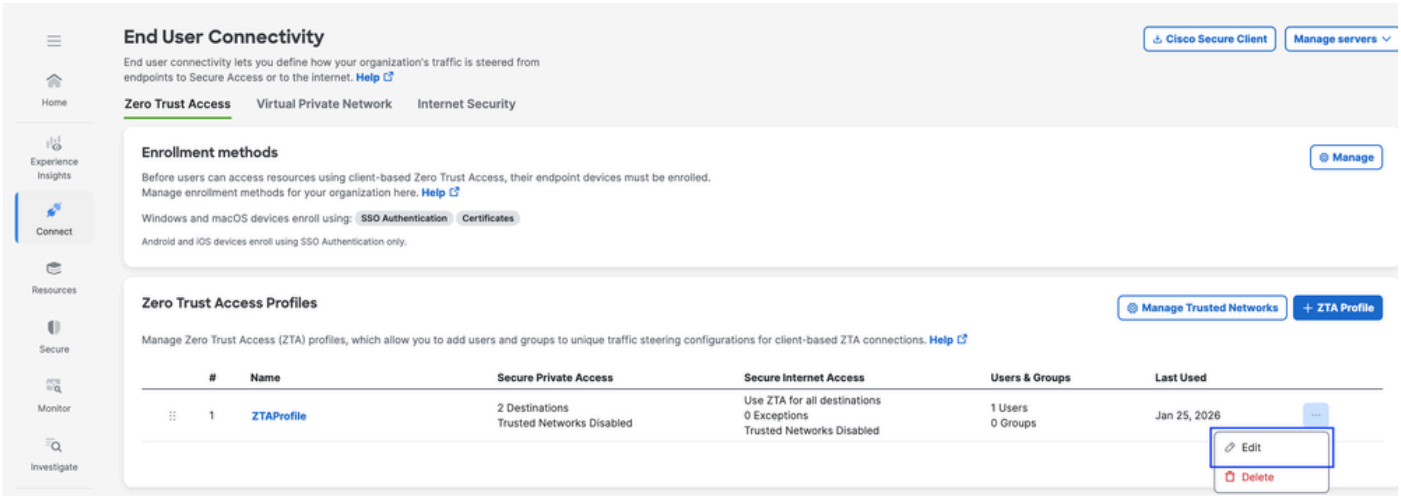
Naviguez jusqu'à Connect > End User Connectivity > Zero Trust Access > ZTA Settings et configurez Trusted Networks



Accès sécurisé - Configuration ZTA TND

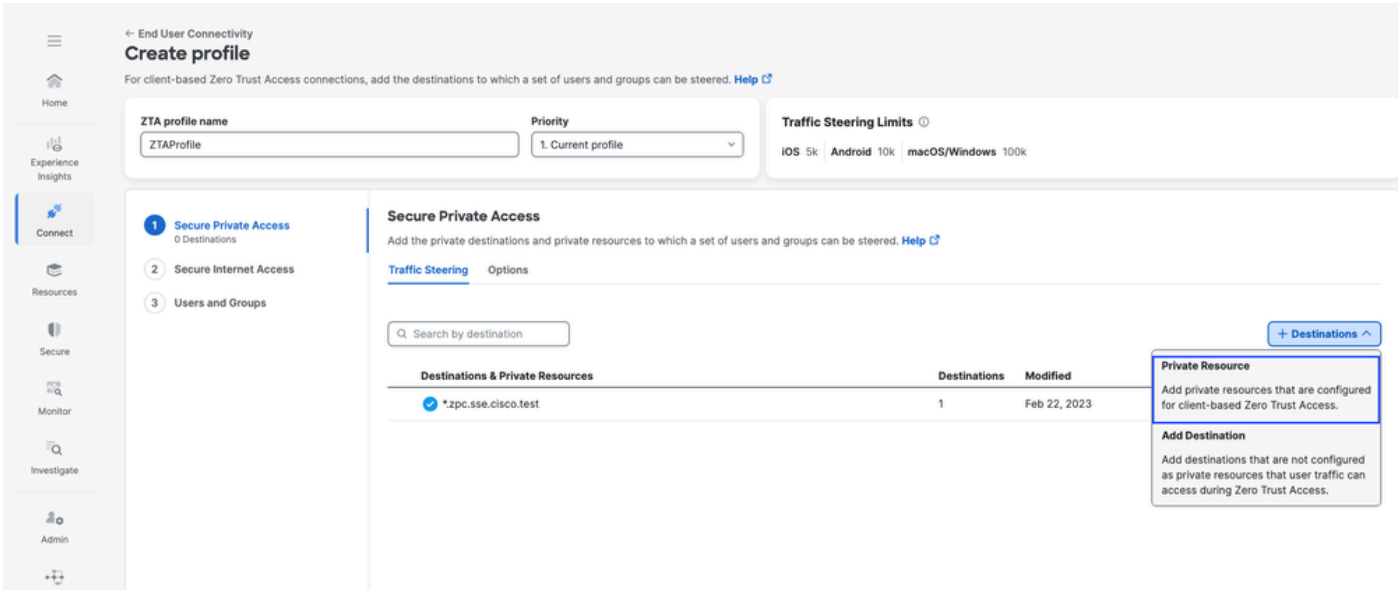
Étape 5 - Ajoutez une ressource privée au profil ZTA

1. Accédez à Connect > End User Connectivity > Zero Trust Access et cliquez sur 3 points pour modifier le profil ZTA

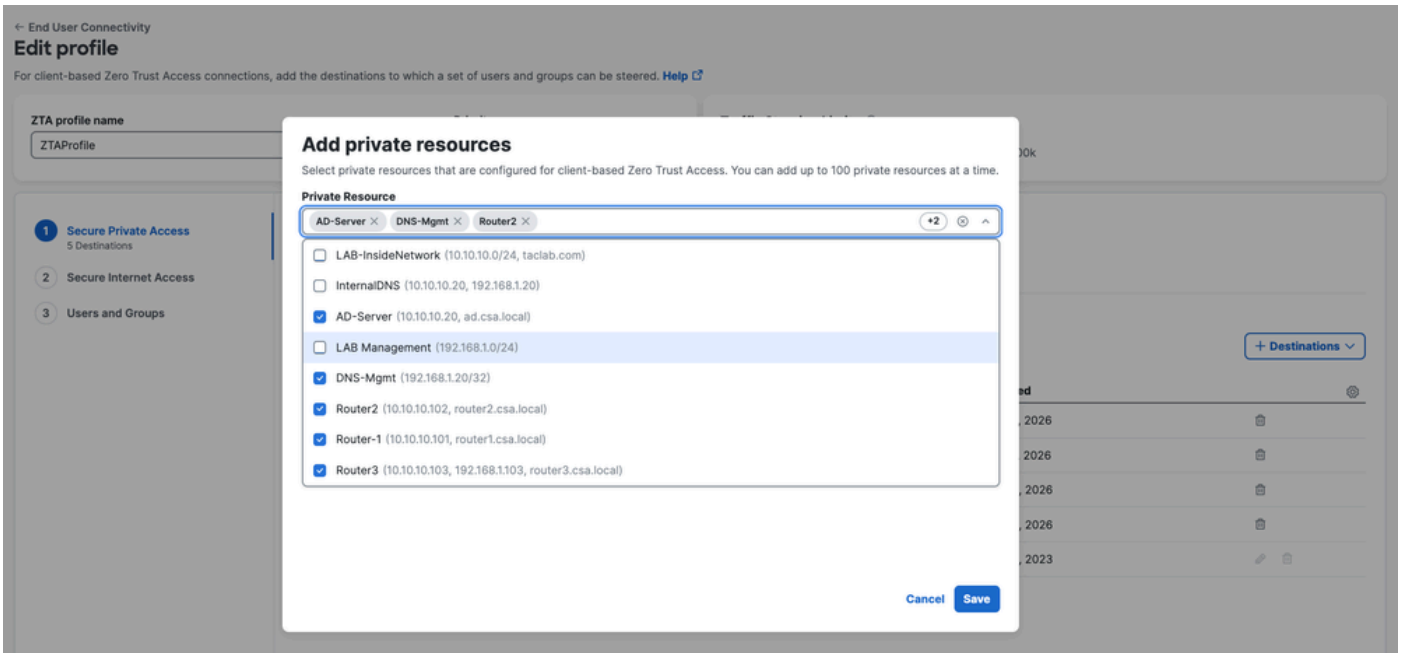


Accès sécurisé - Profil ZTA

2. Ajouter la ressource privée

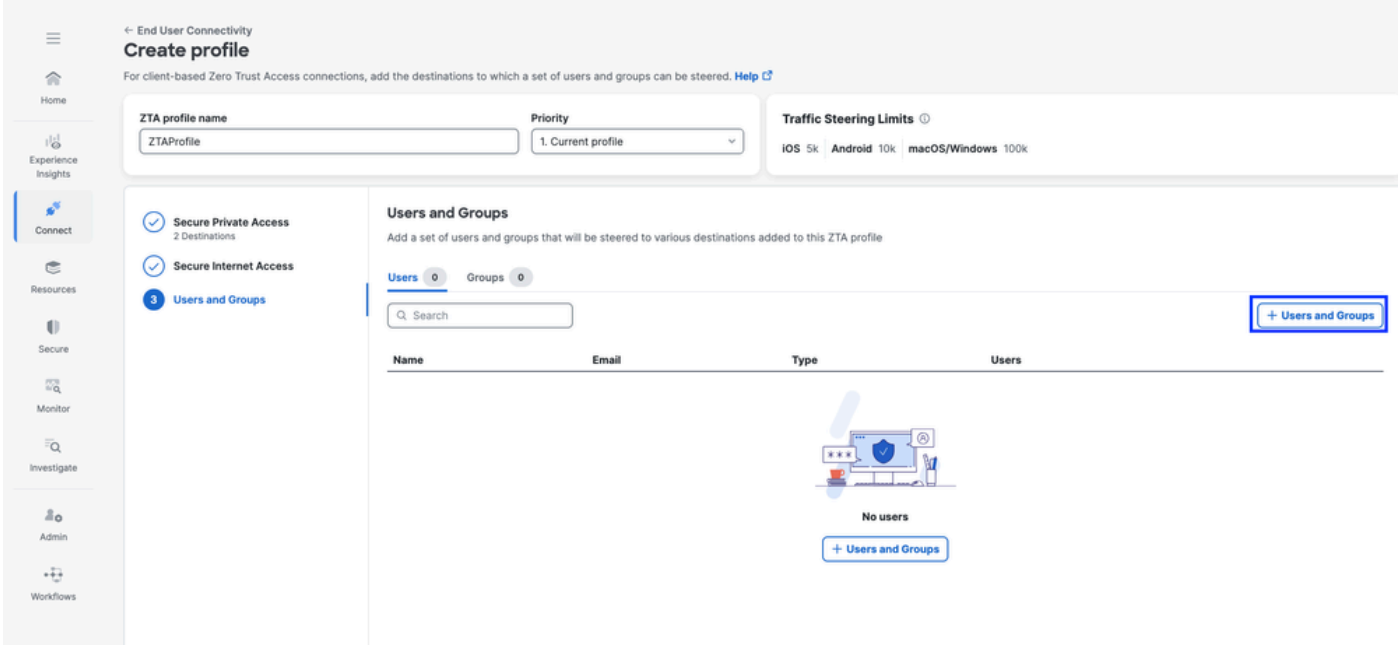


Accès sécurisé - Profil ZTA

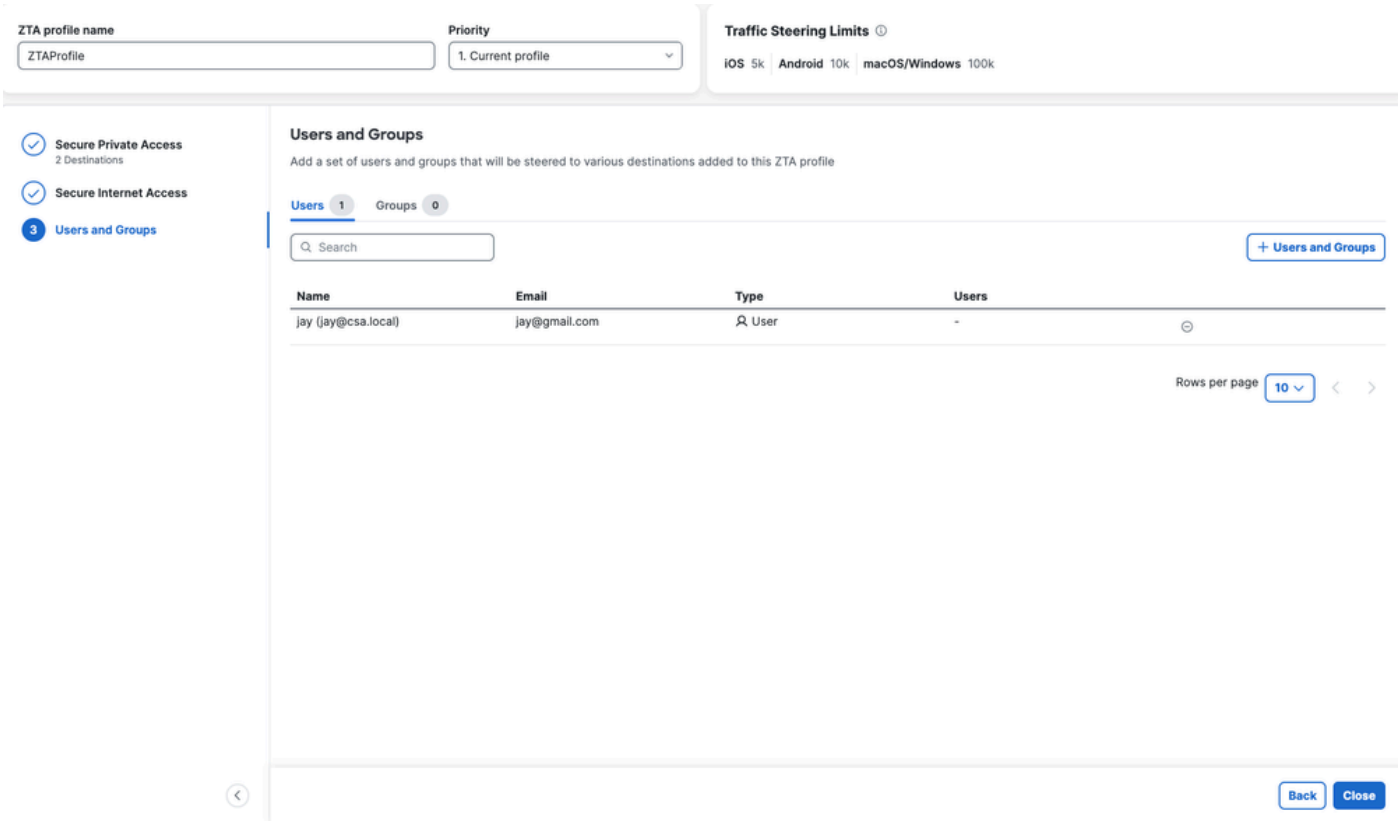


Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes



Accès sécurisé - Profil ZTA

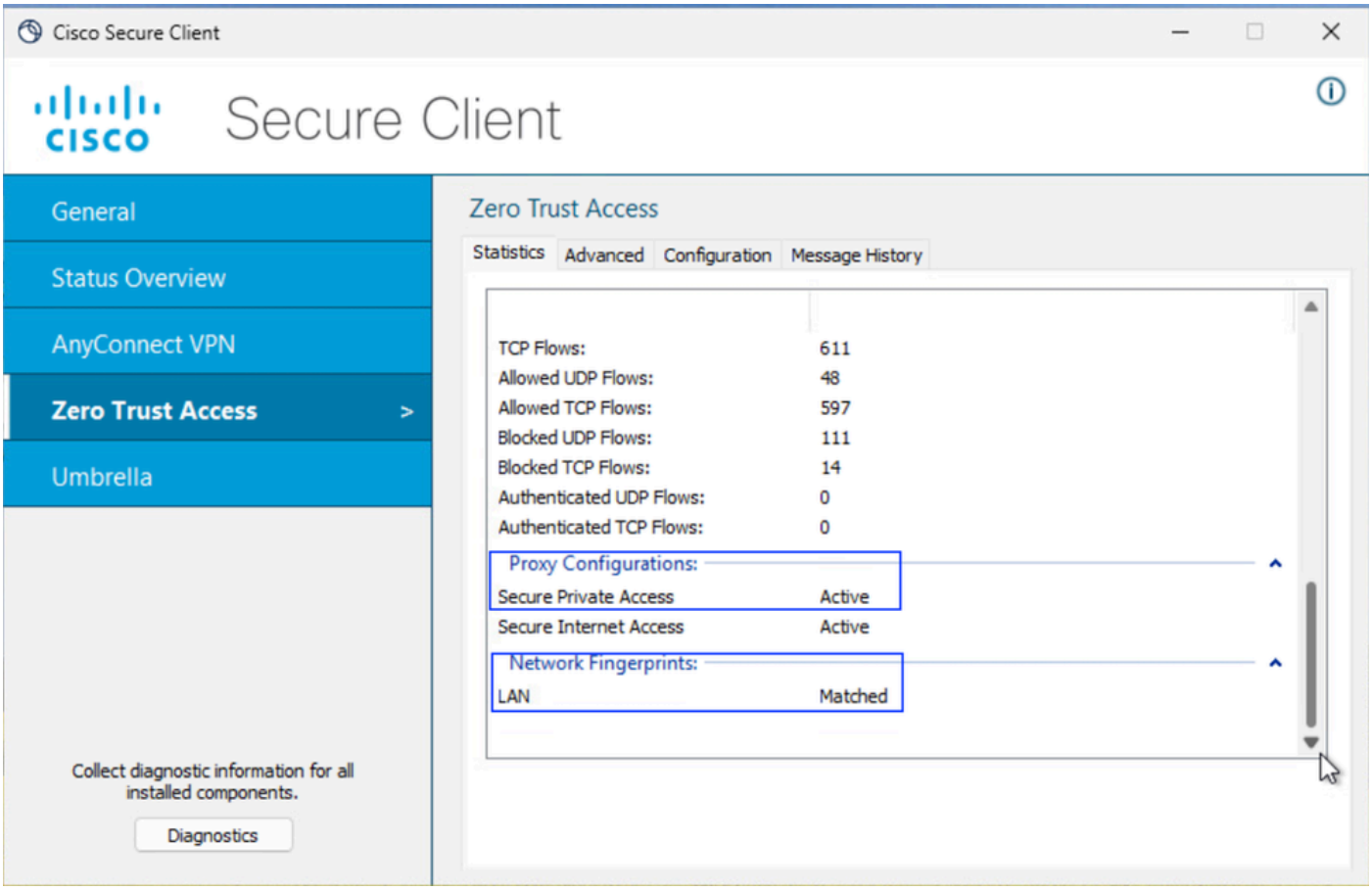


Accès sécurisé - Profil ZTA

Étape 6 - Vérifiez l’accès à la ressource privée

Lorsque l'utilisateur est Local

1. Vérifiez l'empreinte numérique du réseau pour ZTA TND, elle doit correspondre si l'utilisateur est local et si l'accès privé sécurisé doit être actif



Accès sécurisé - Test PR

2. Vérifier que l'utilisateur distant peut résoudre le FQDN 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
```

Accès sécurisé - Test PR

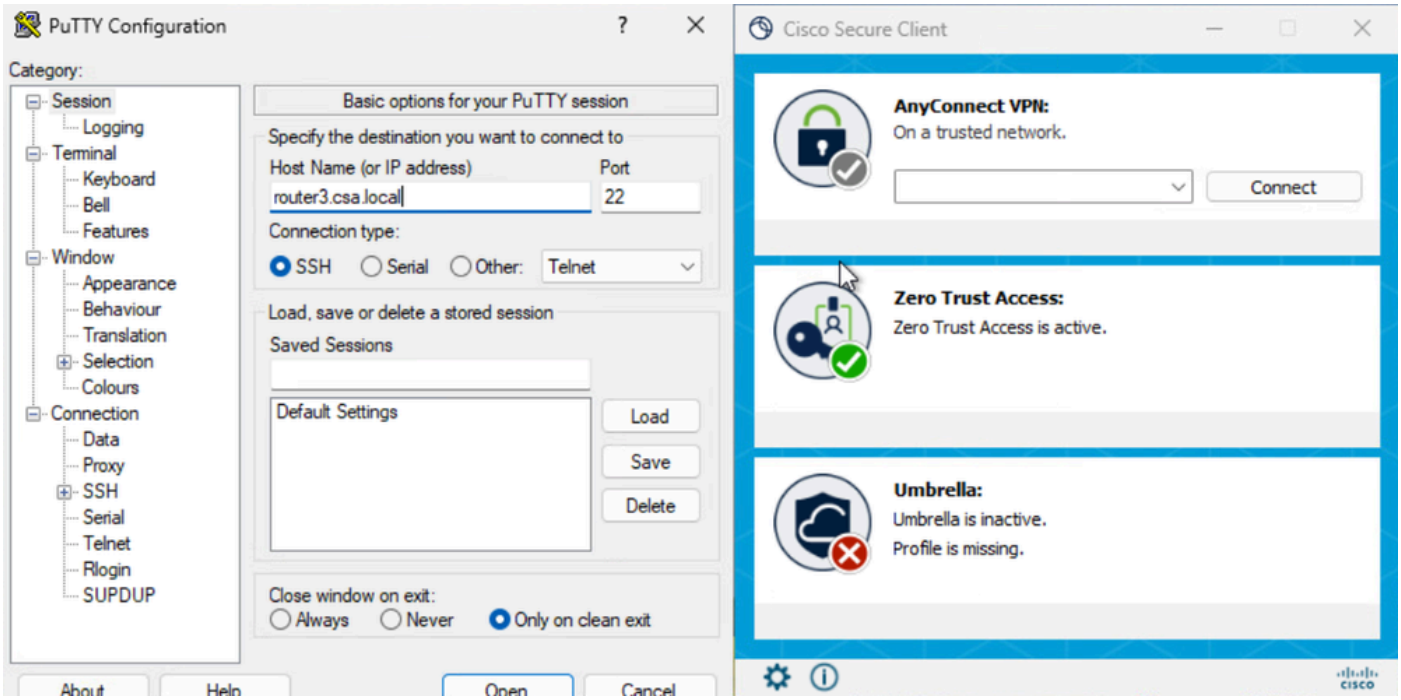
3. Vérifiez que FTD peut atteindre une ressource privée à l'aide du nom de domaine complet

```
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#
```

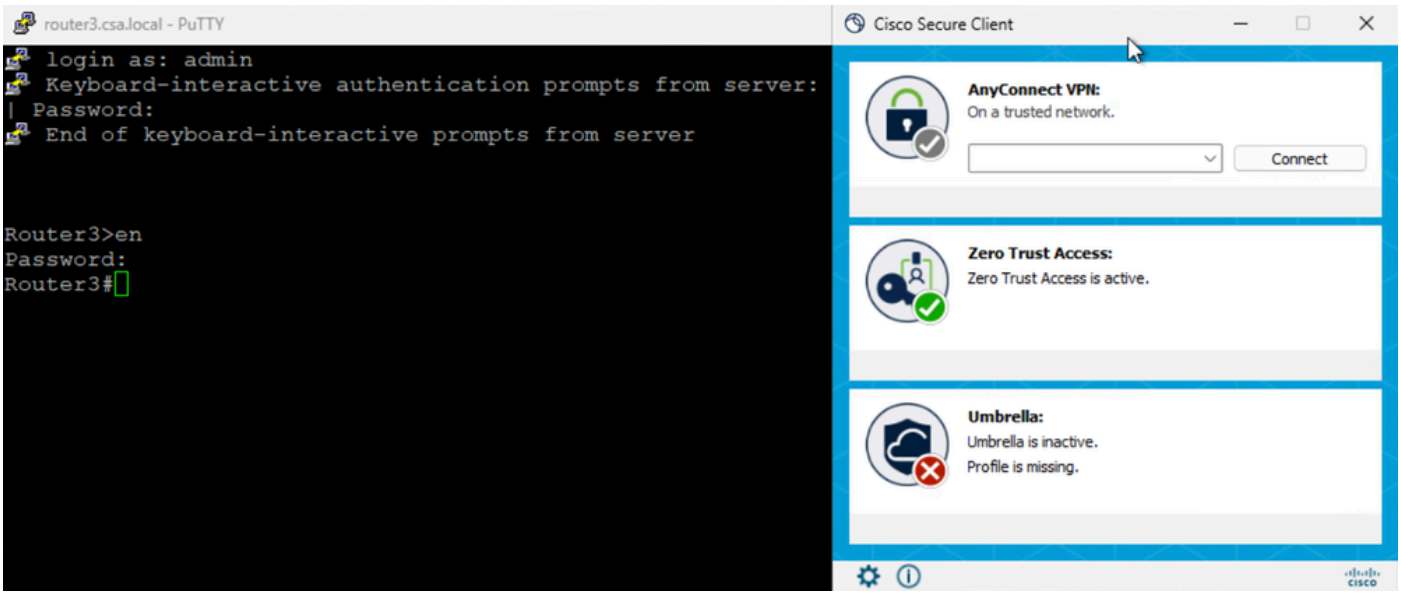
Accès sécurisé - Test PR

4. Tester la connexion SSH à la ressource privée

Accéder au RP à l'aide du FQDN

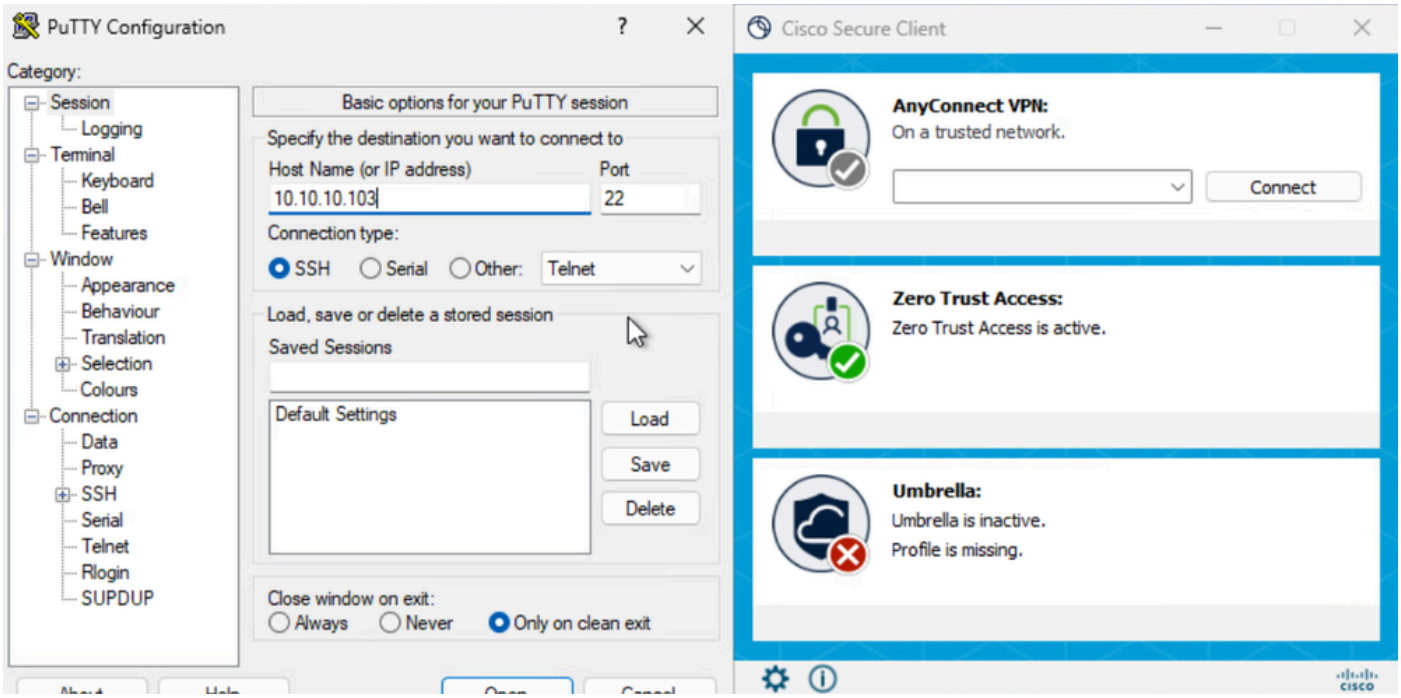


Accès sécurisé - Test PR

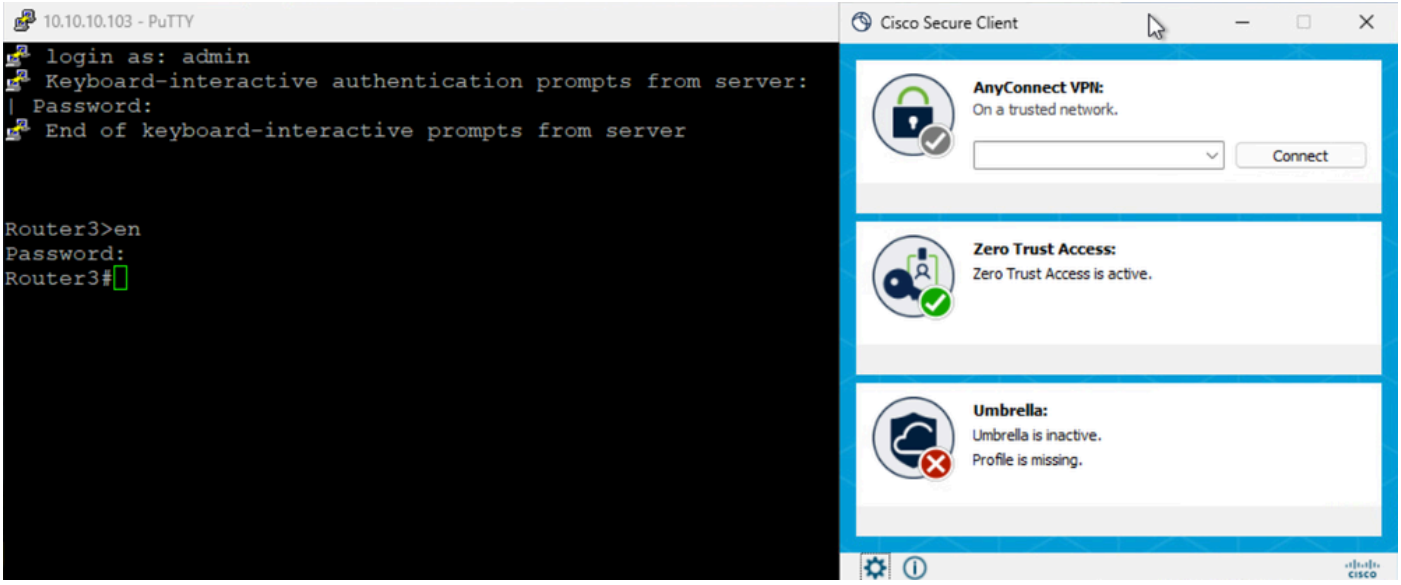


Accès sécurisé - Test PR

Accéder au RP en utilisant l'adresse IP

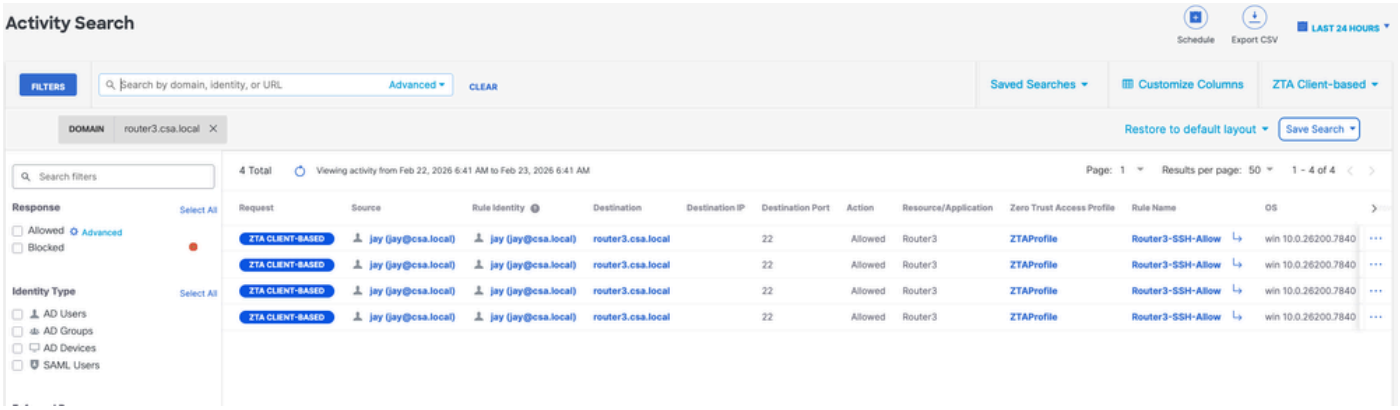


Accès sécurisé - Test PR

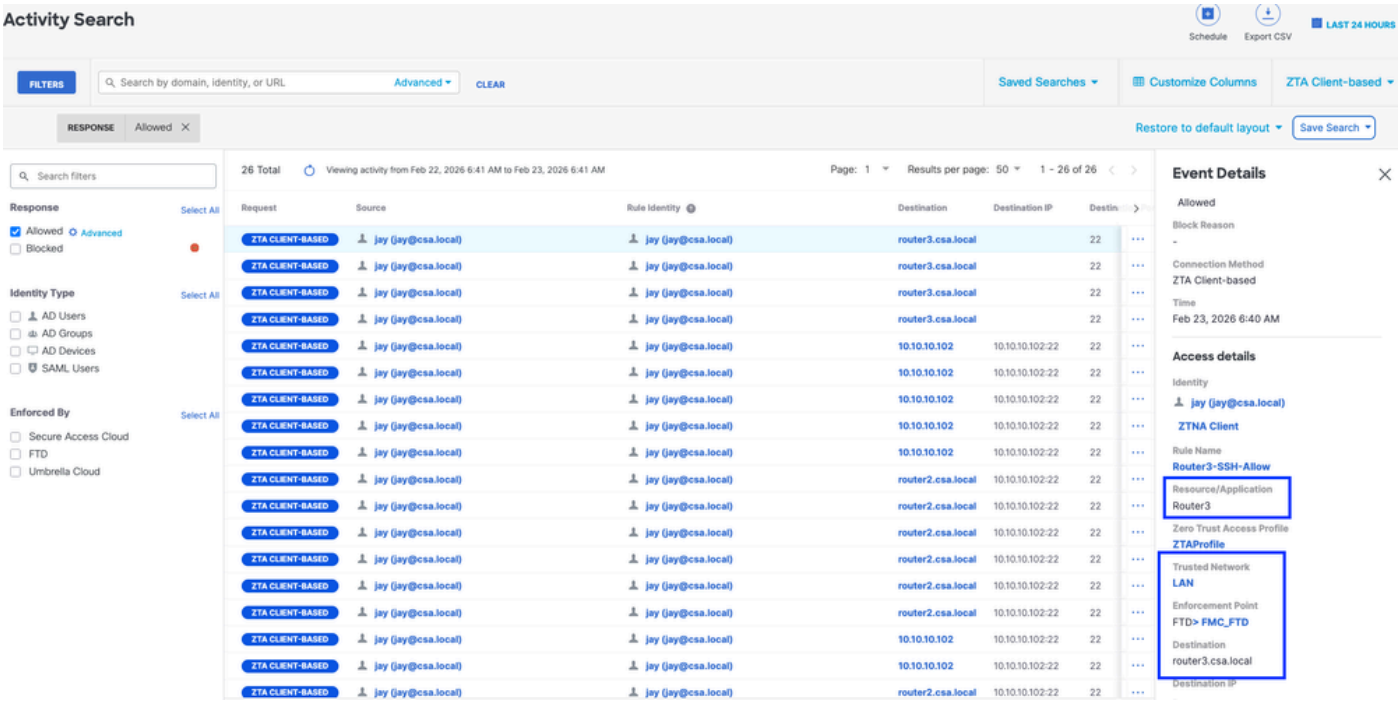


Accès sécurisé - Test PR

5. Vérification des journaux de recherche d'activité Secure Access

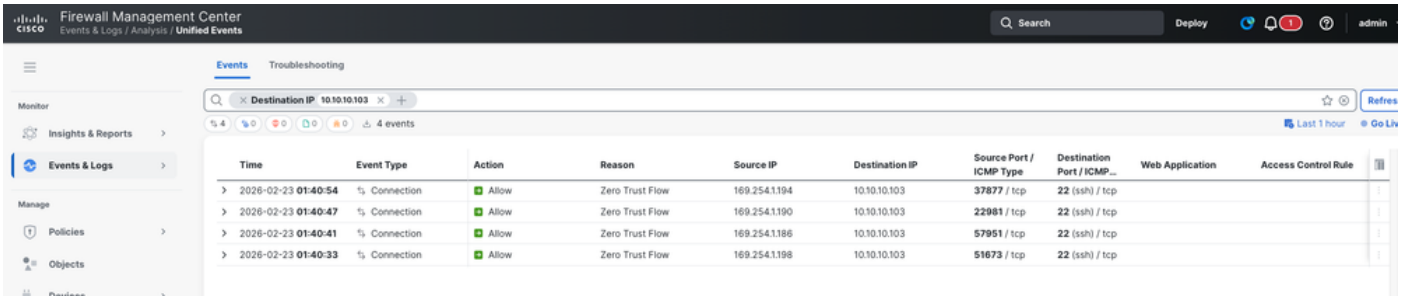


Accès sécurisé - Recherche d'activité



Accès sécurisé - Recherche d'activité

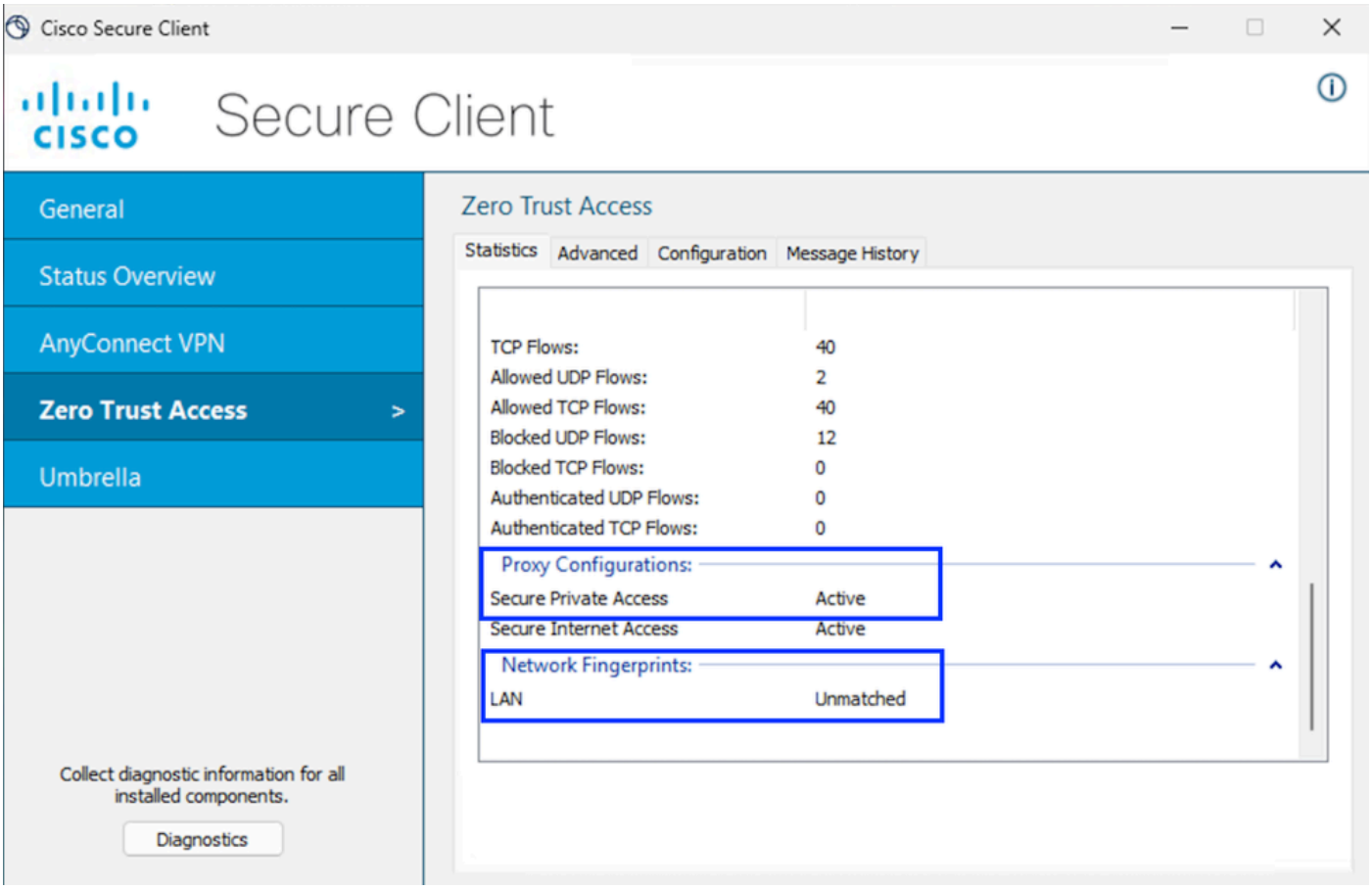
6. Vérifier les événements de connexion FMC



Événements de connexion FMC

Lorsque l'utilisateur est distant

1. Vérifiez l'empreinte digitale du réseau pour ZTA TND, elle ne doit pas correspondre si l'utilisateur est distant



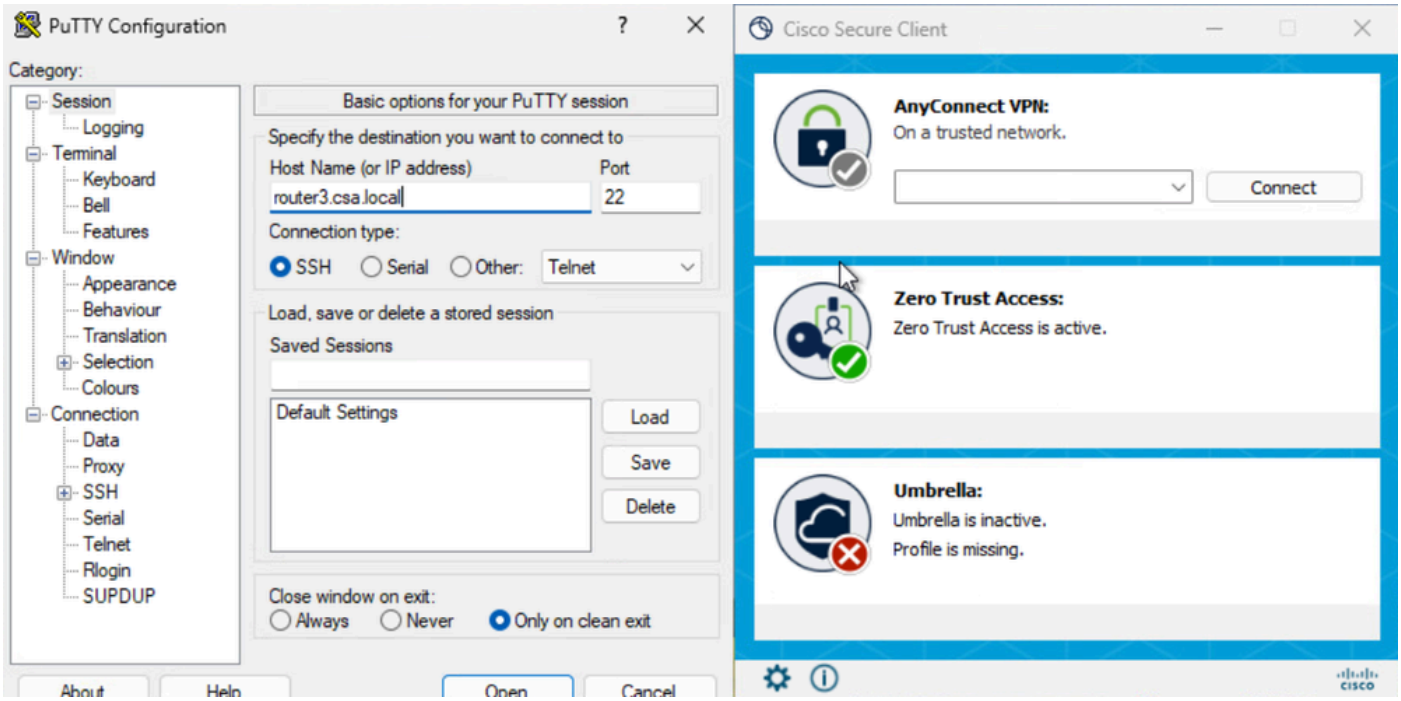
Accès sécurisé - Test PR

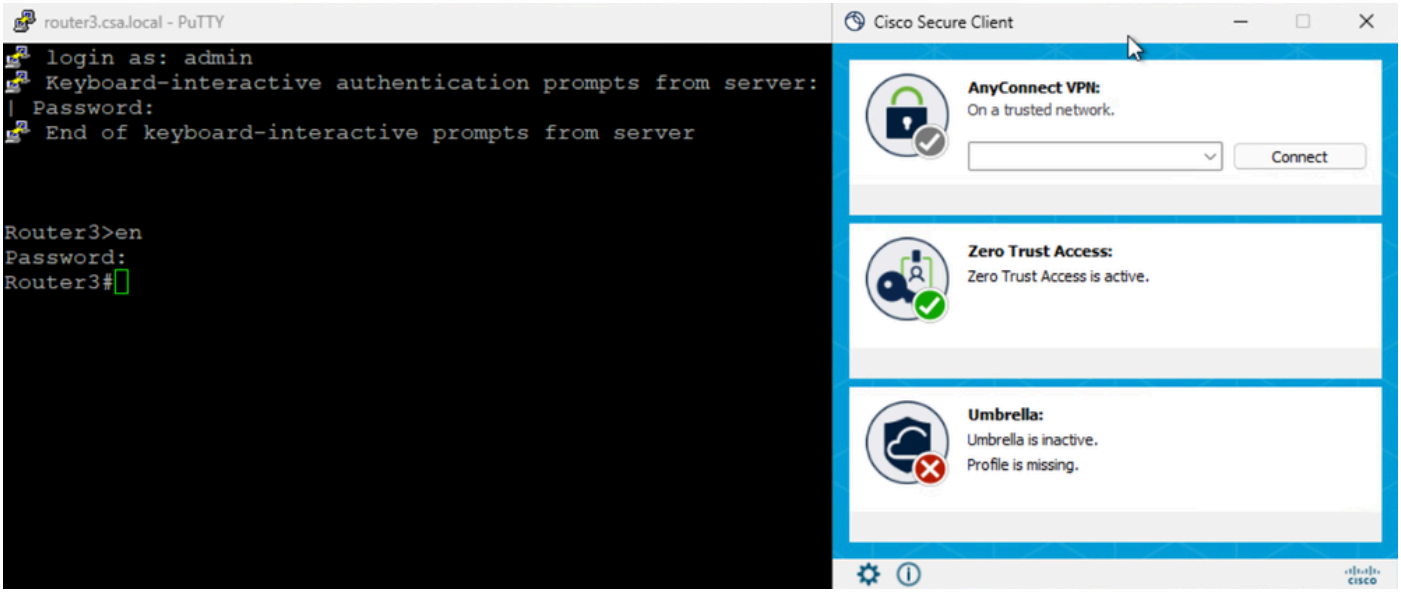
2. Vérifier que l'utilisateur distant peut résoudre le FQDN FTD

```
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. Tester la connexion SSH à la ressource privée

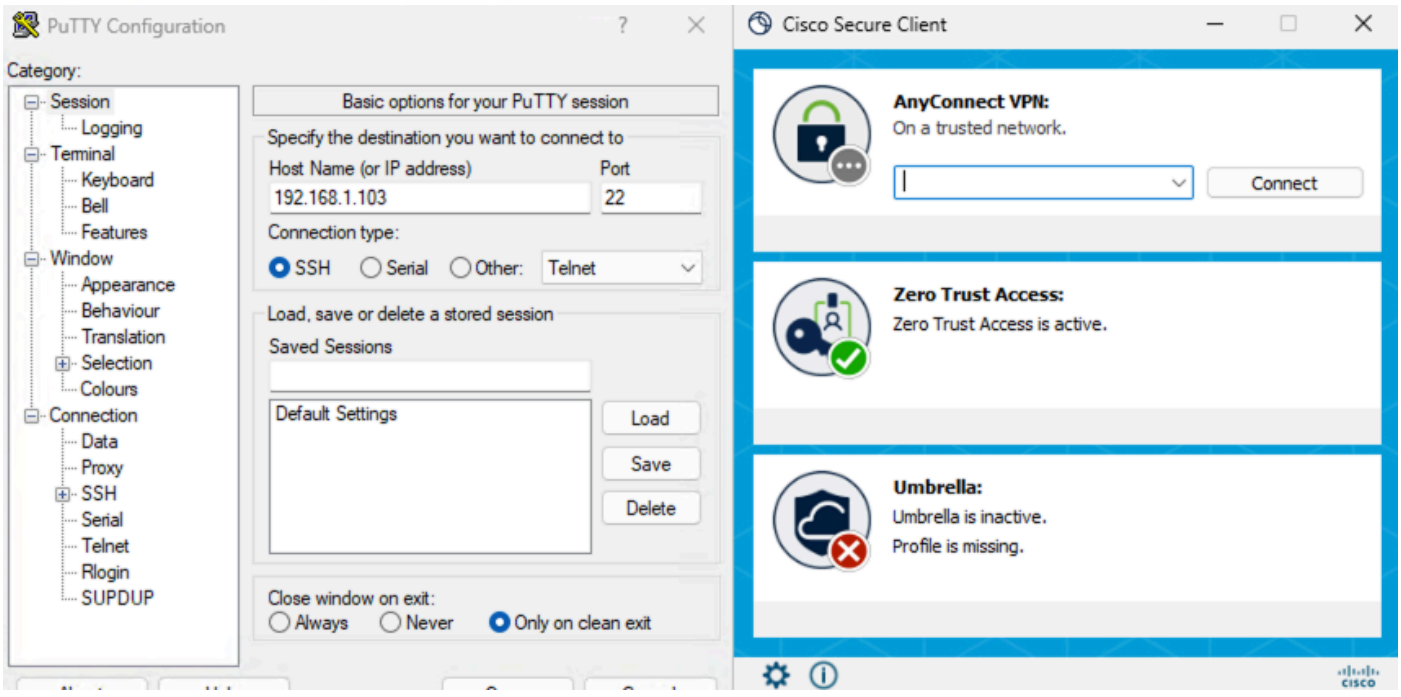
Accéder au RP à l'aide du FQDN



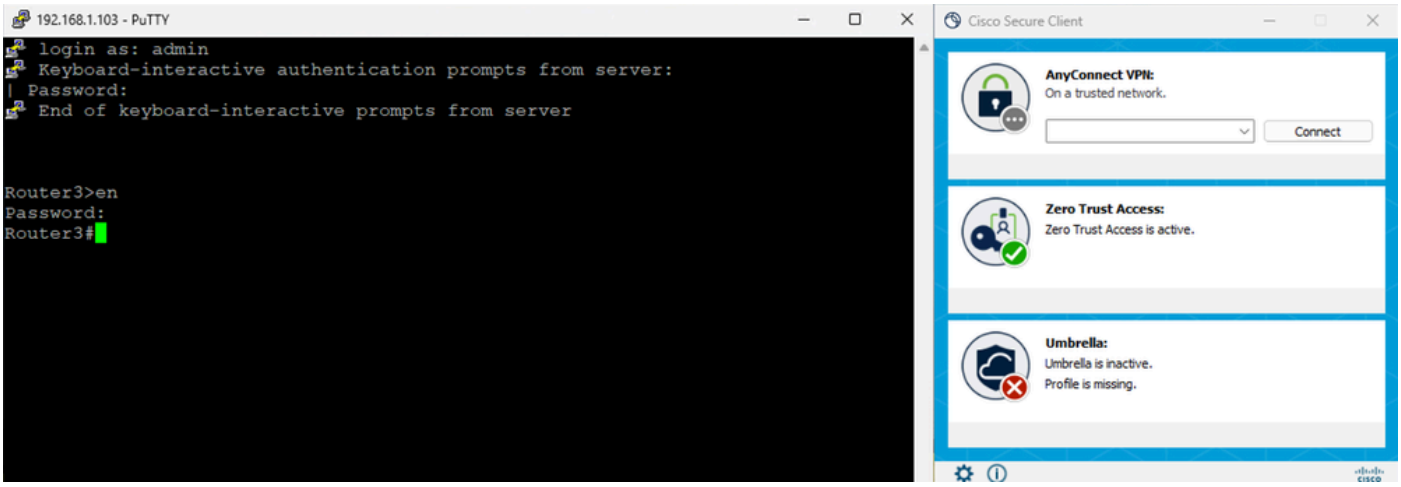


Accès sécurisé - Test PR

Accéder au RP en utilisant l'adresse IP

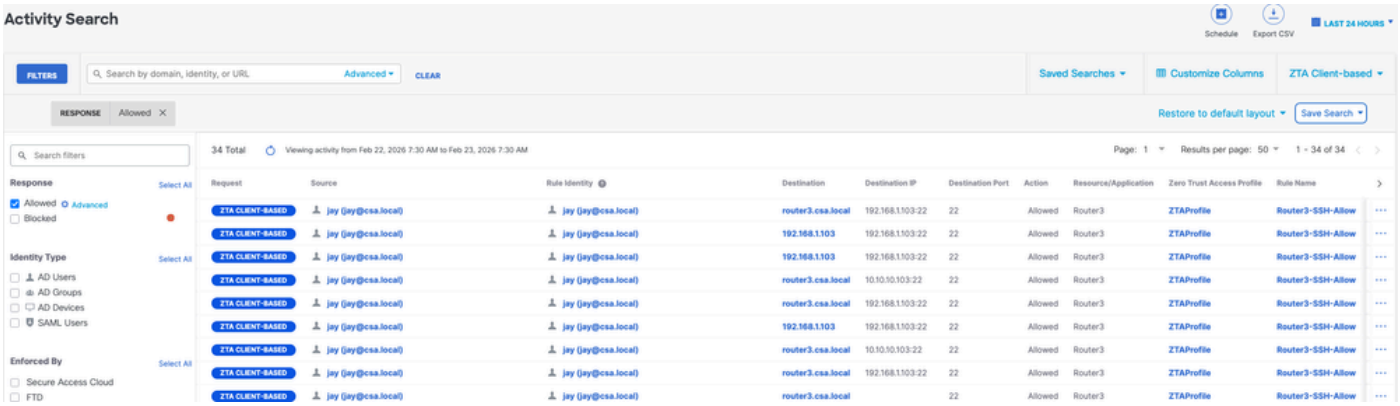


Accès sécurisé - Test PR

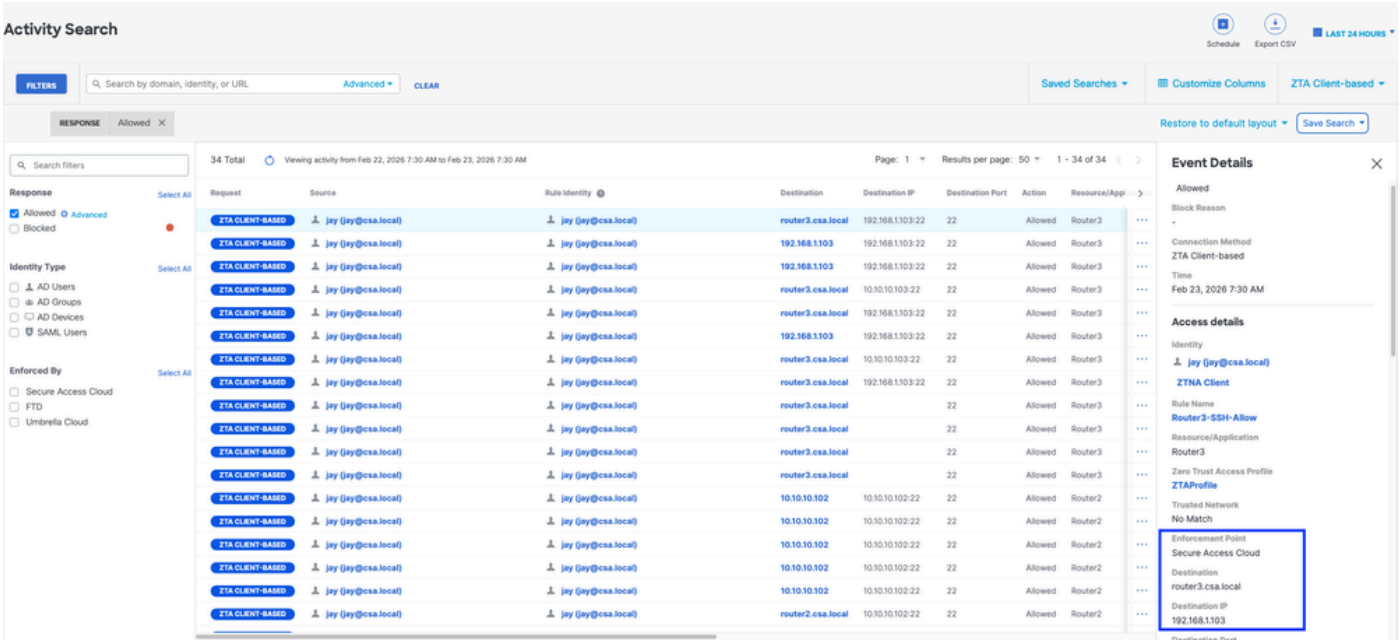


Accès sécurisé - Test PR

5. Vérification des journaux de recherche d'activité Secure Access



Accès sécurisé - Recherche d'activité



Dépannage

Commandes utiles :

> 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

! puis passez en mode expert

tail -f /ngfw/var/log/messages

show conn all

show nat detail

show asp table socket

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.