

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[À propos de Universal ZTNA](#)

[Détection du réseau](#)

[Types d'application](#)

[Scénarios :](#)

[Composants architecturaux](#)

[Flux de paquets](#)

[Configurer](#)

[Diagramme du réseau](#)

[Cas de test](#)

[Cas de test 1 : Utilisateur distant - Application du cloud](#)

[Cas de test 2 - Utilisateur distant - Application locale](#)

[Cas de test 3 - Utilisateur local - Application locale](#)

[Cas de test 4 - Utilisateur local et distant - Application locale ou cloud avec TND](#)

[Dépannage](#)

[Commandes utiles :](#)

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

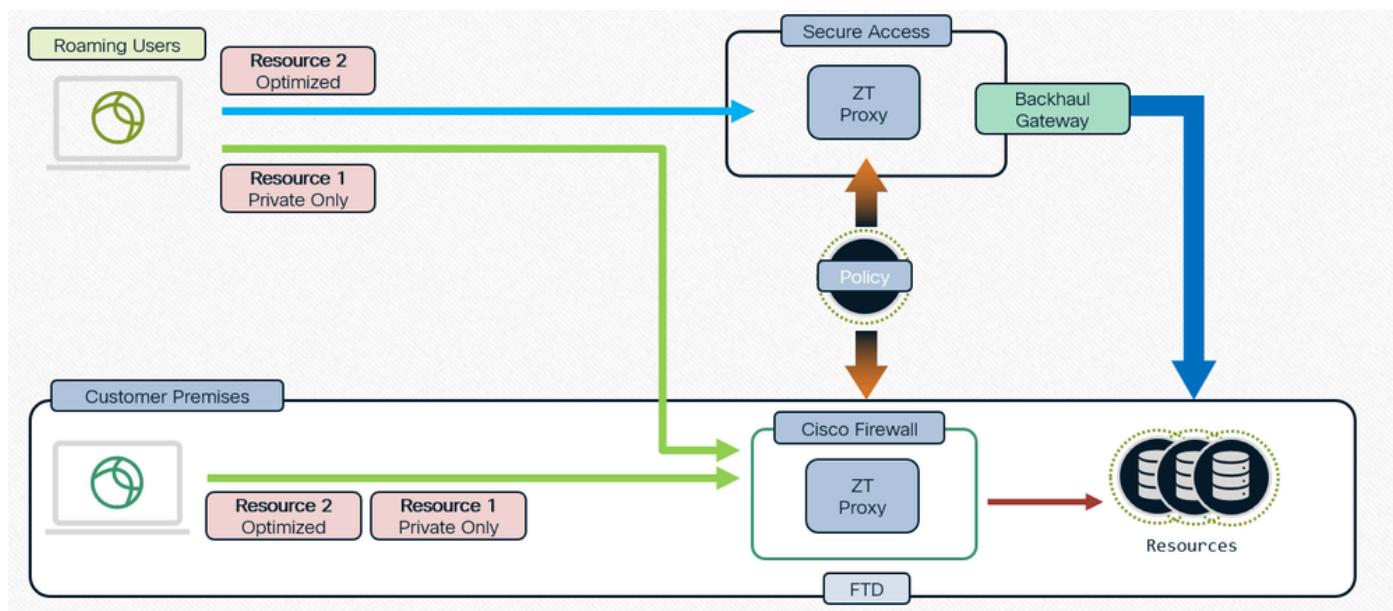
L'accès réseau sans confiance universel (uZTNA) permet aux administrateurs d'autoriser spécifiquement l'accès aux ressources réseau internes en fonction de l'identité de l'utilisateur (y

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.

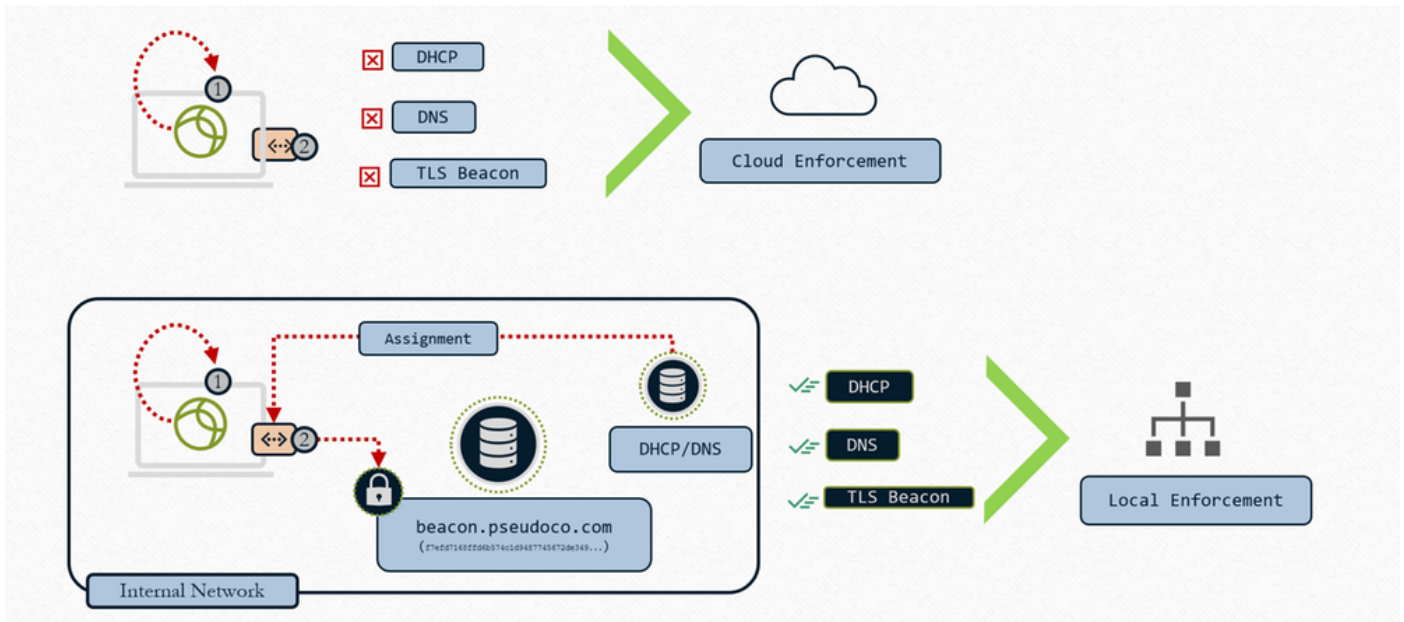
Le proxy de trafic, ainsi que l'application des politiques IPS, de fichiers et de programmes malveillants, sont effectués sur le pare-feu Firepower Threat Defense (FTD).



Politique unique, application distribuée

Détection du réseau

Détermination de l'application locale ou cloud



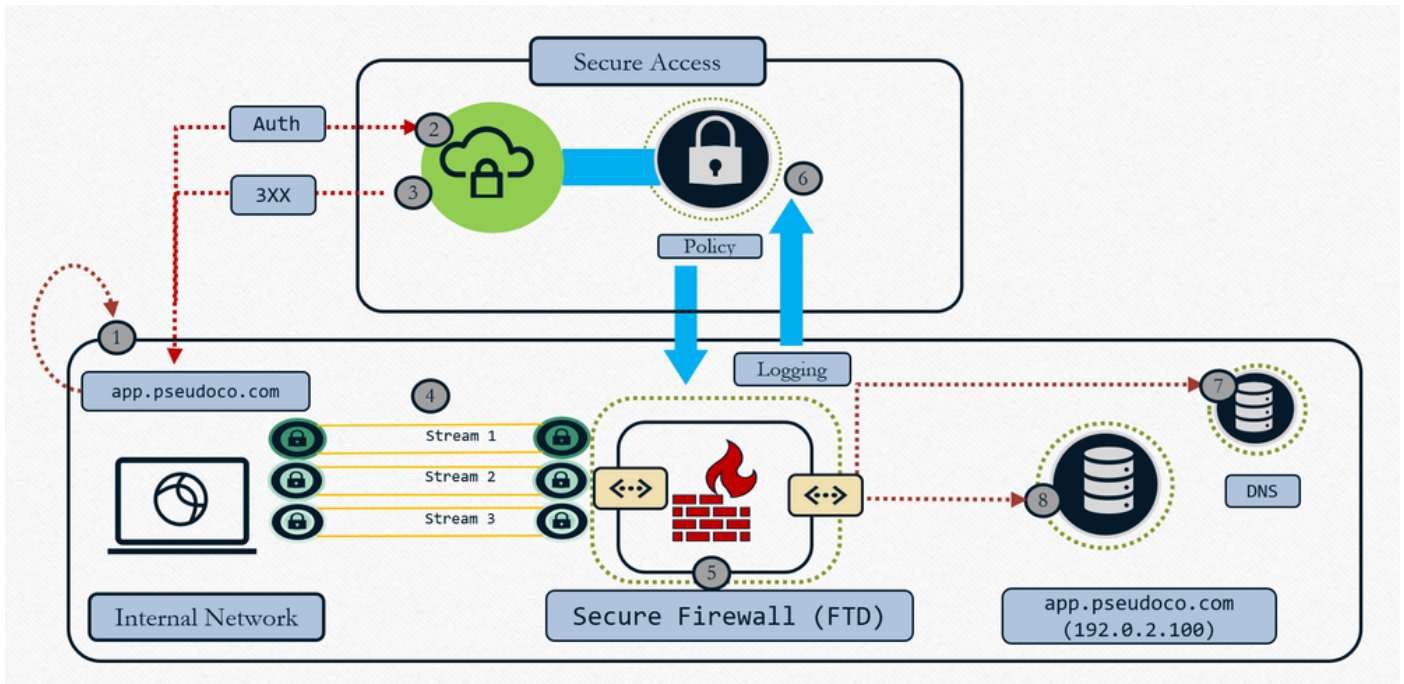
ZTNA universel : détermination de l'application cloud ou locale

- 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

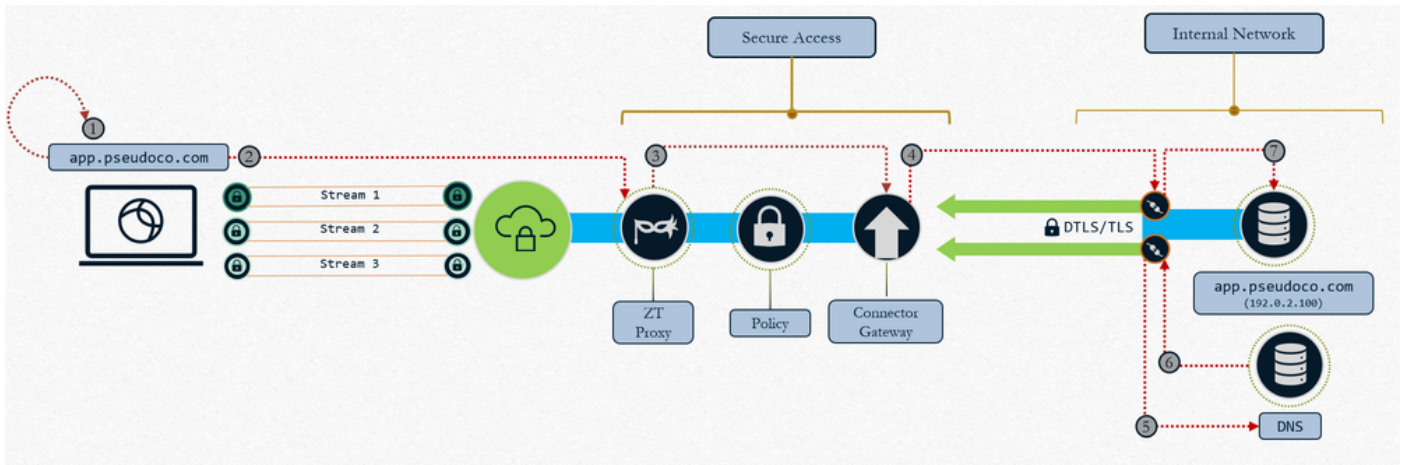
- Chemin d'application local : Application du pare-feu



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

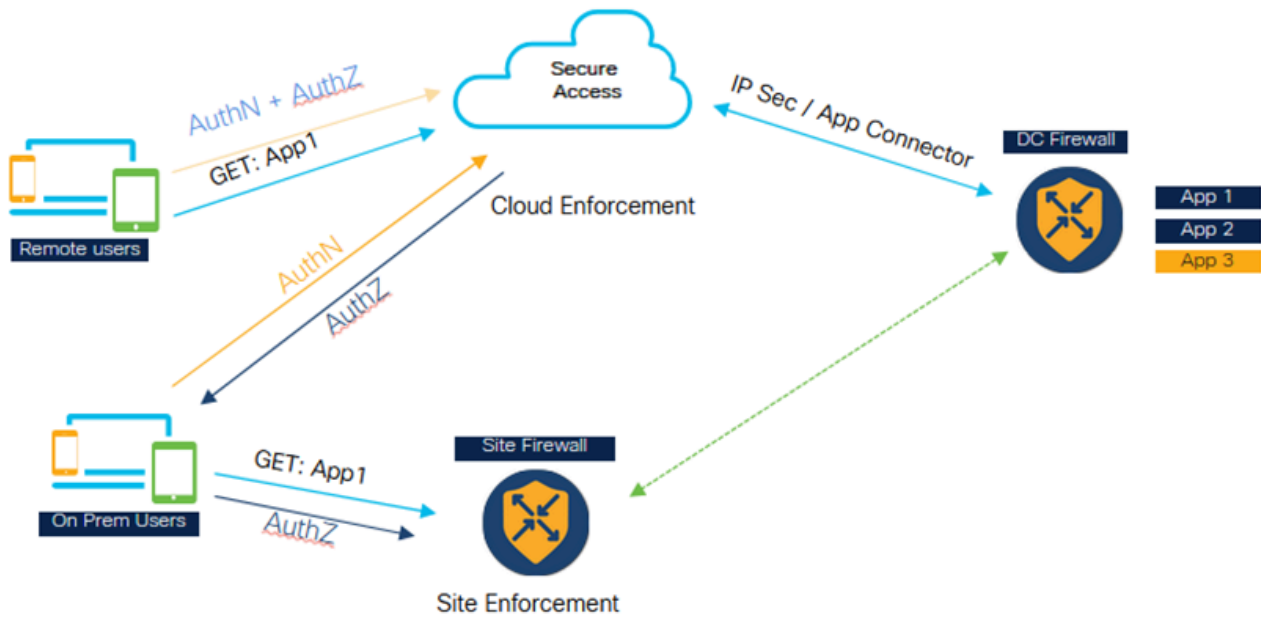


ZTNA universel : Application du cloud

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 :

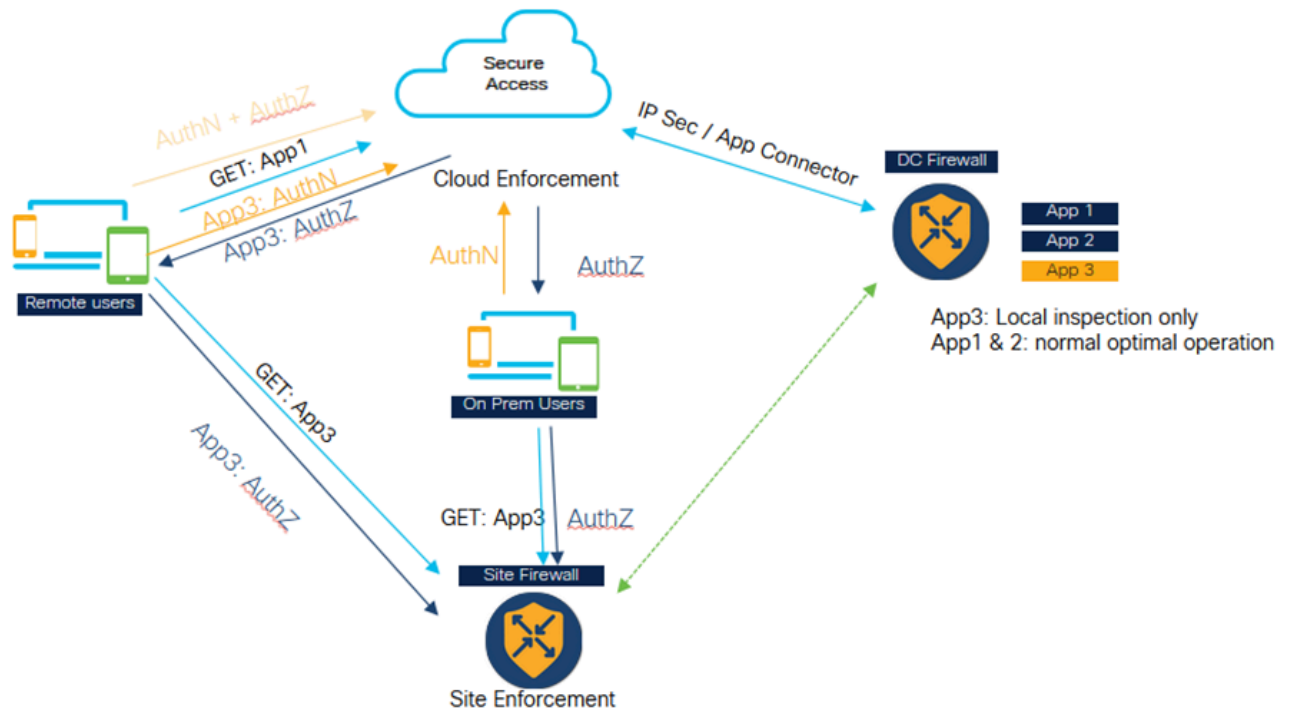
Cas 1 : ZTNA cohérent et optimisé pour les utilisateurs sur site



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

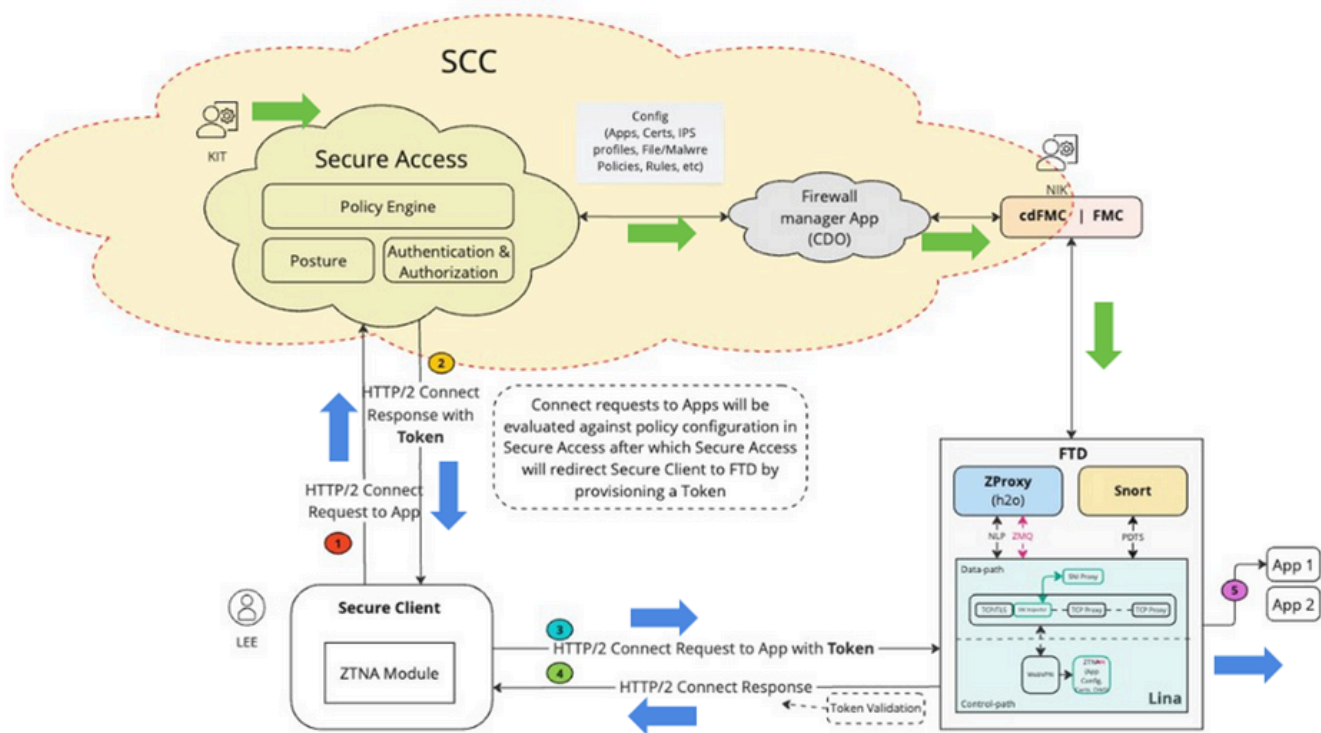
Cas 2 : Inspection privée pour les applications sensibles



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 pourrions 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

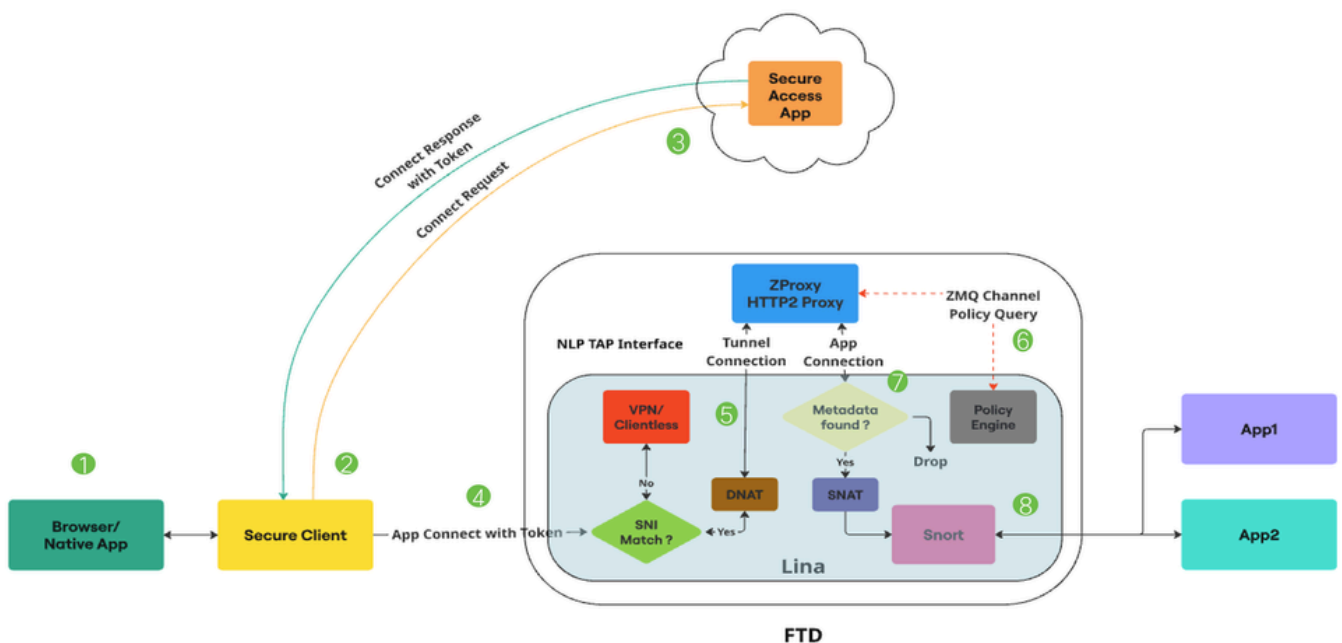
3. Secure Access redirige le client Secure vers FTD avec le jeton d'authentification.

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 cœurs 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, la connexion est abandonnée.

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. Elle sera traduite en IP de l'interface de sortie FTD, avant d'être envoyée. 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

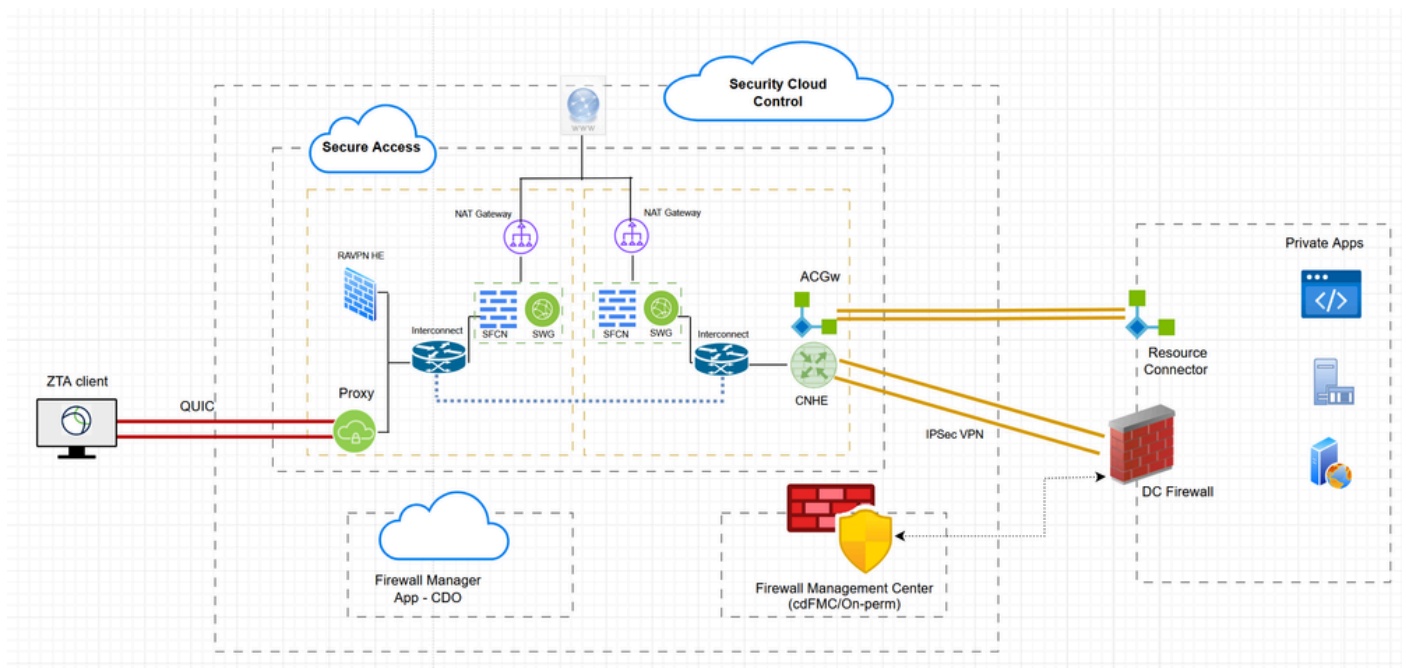
à partir du jeton d'accès est passé à Snort dans les métadonnées de connexion.

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

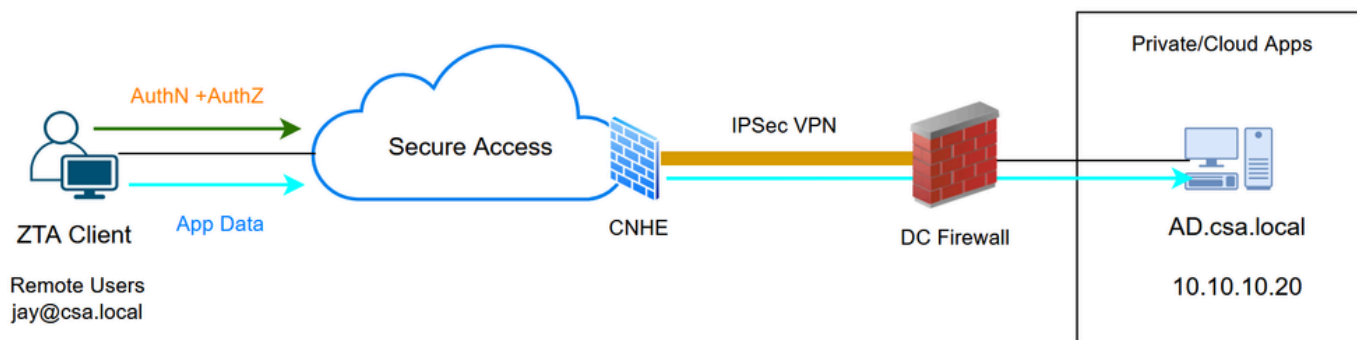


ZTNA hybride - Schéma de réseau

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

The screenshot shows the Cisco Security Cloud Control console. The left sidebar has a menu with 'Resources' highlighted. The main content area shows the 'Resources' configuration page. The 'Destinations' section is expanded to show 'Private Resource'. A table lists the configured private resources:

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

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.

← Private Resources

Add a Private Resource

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

General

Private Resource Name

Description (optional)

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

Private resource address

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

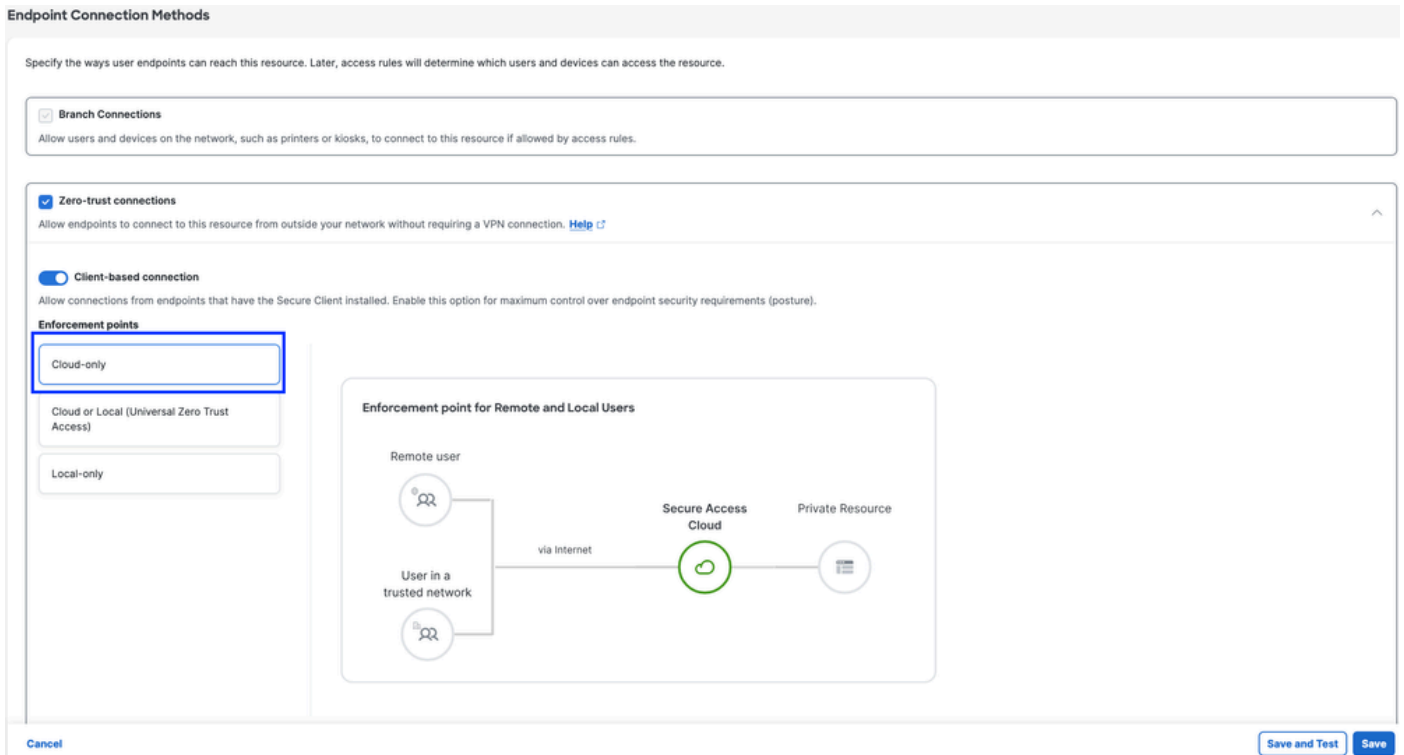
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
<input type="text" value="ad.csa.local"/>	TCP - RDP ▾	<input type="text" value="Any"/>	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.20"/>	TCP - RDP ▾	<input type="text" value="Any"/>	+ Protocol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

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

Internal DNS Server

Accès sécurisé - Configuration des ressources privées

5. Sélectionner les méthodes de connexion Endpoint



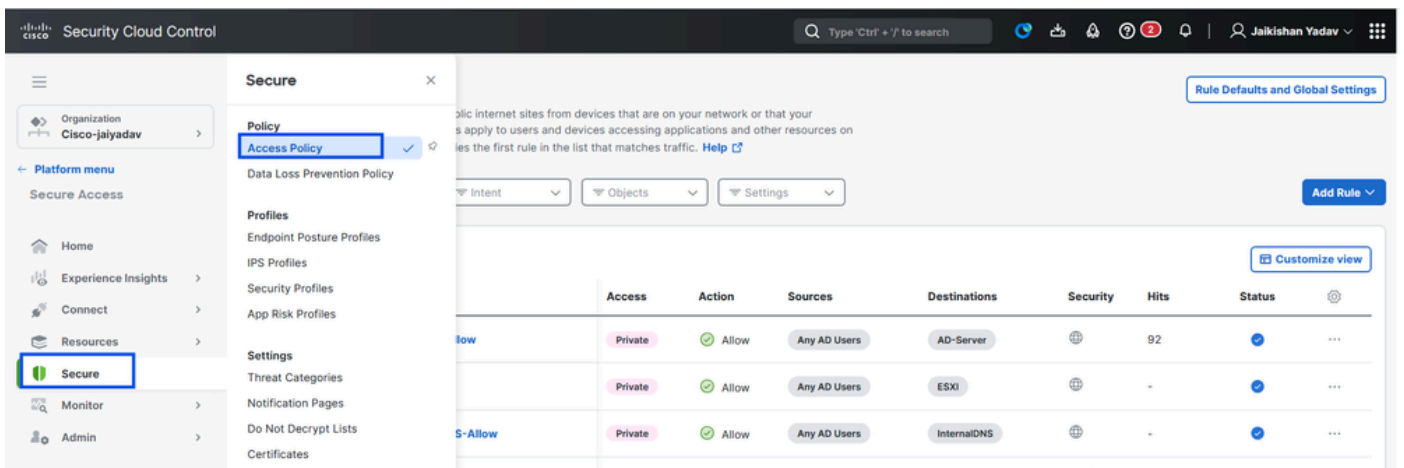
Accès sécurisé - Configuration des ressources privées

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.

Access Policy Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings Add Rule ^

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

Rows per page 1-2 of 2 < 1 >

Private Access

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

Internet Access

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

Accès sécurisé - Configuration de la stratégie d'accès

3. Ajouter un nom de règle

Add AD-RDP-Allow

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

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

Summary

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

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

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From: _____ To: _____

Accès sécurisé - Configuration de la stratégie d'accès

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

Rule name: Rule order:

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From
Specify one or more sources.

To
Specify one or more destinations.

+ AND

Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux

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

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

Private Resources: **AD-Server**

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

User Authentication Requirements

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

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

Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité

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

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

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

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

Security Profile [Rule Defaults](#)

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

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

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

Accès sécurisé - Configuration de la stratégie d'accès

7. Cliquez sur Enregistrer

Access Policy [Rule Defaults and Global Settings](#)

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

🔍 Search by rule name ▼ Intent ▼ Objects ▼ Settings [Add Rule](#)

3 Rules [Customize view](#)

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

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

Default Access Rules

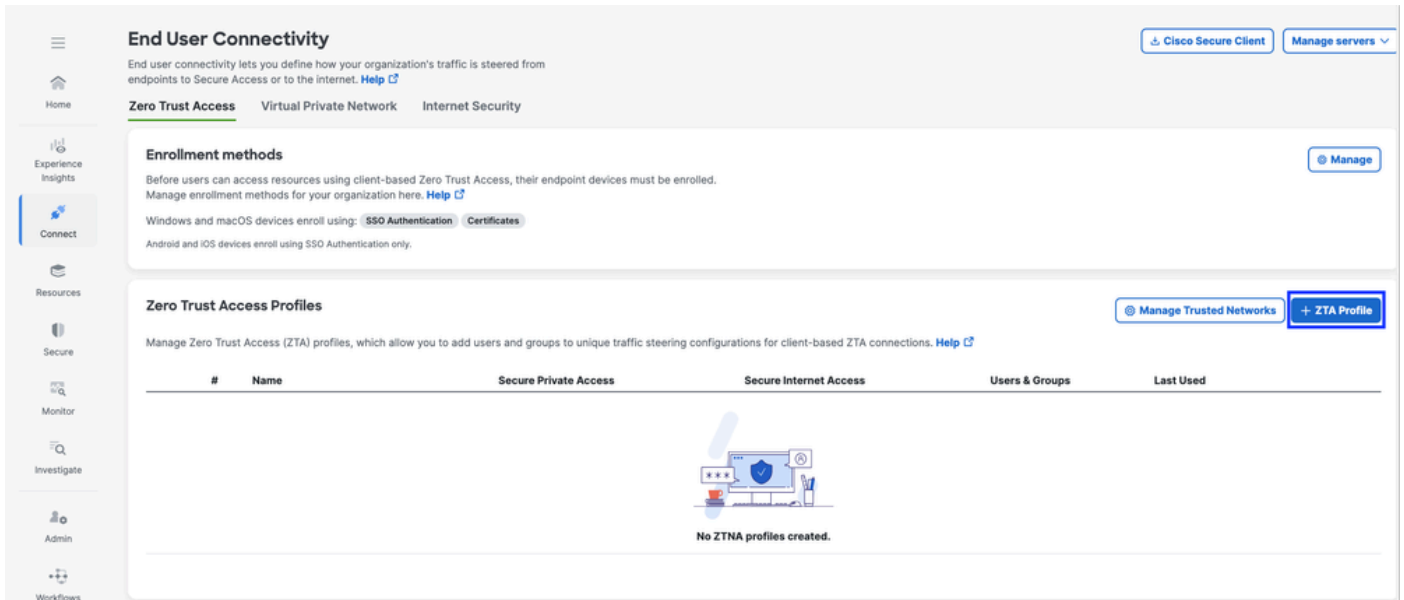
Rule name	Action	Sources	Destinations	Security	Posture	
For all private access	Block	Any	Any private destination	-	-	⋮
For all Internet access	Allow	Any	Any Internet destination	🌐🔒	-	⋮

Accès sécurisé - Configuration de la stratégie d'accès

Étape 3 - Ajoutez une ressource privée au profil ZTA

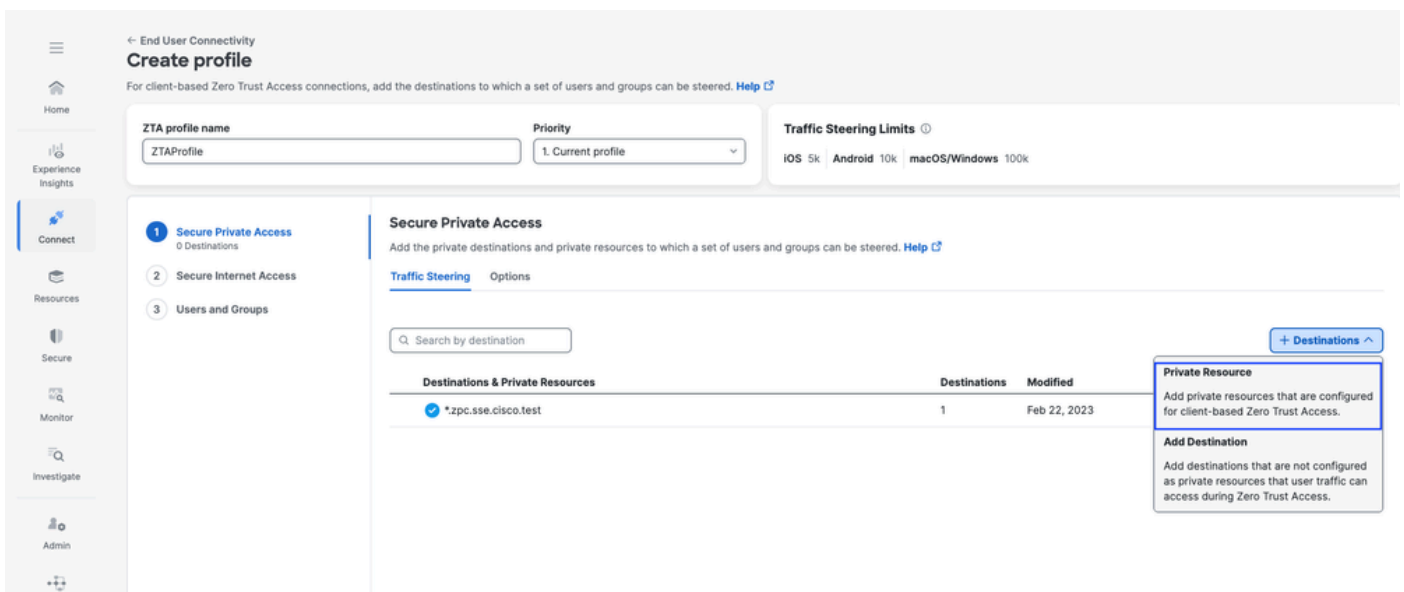
Si vous utilisez un profil ZTA personnalisé, vous devez ajouter la ressource privée correspondante au profil ZTA

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

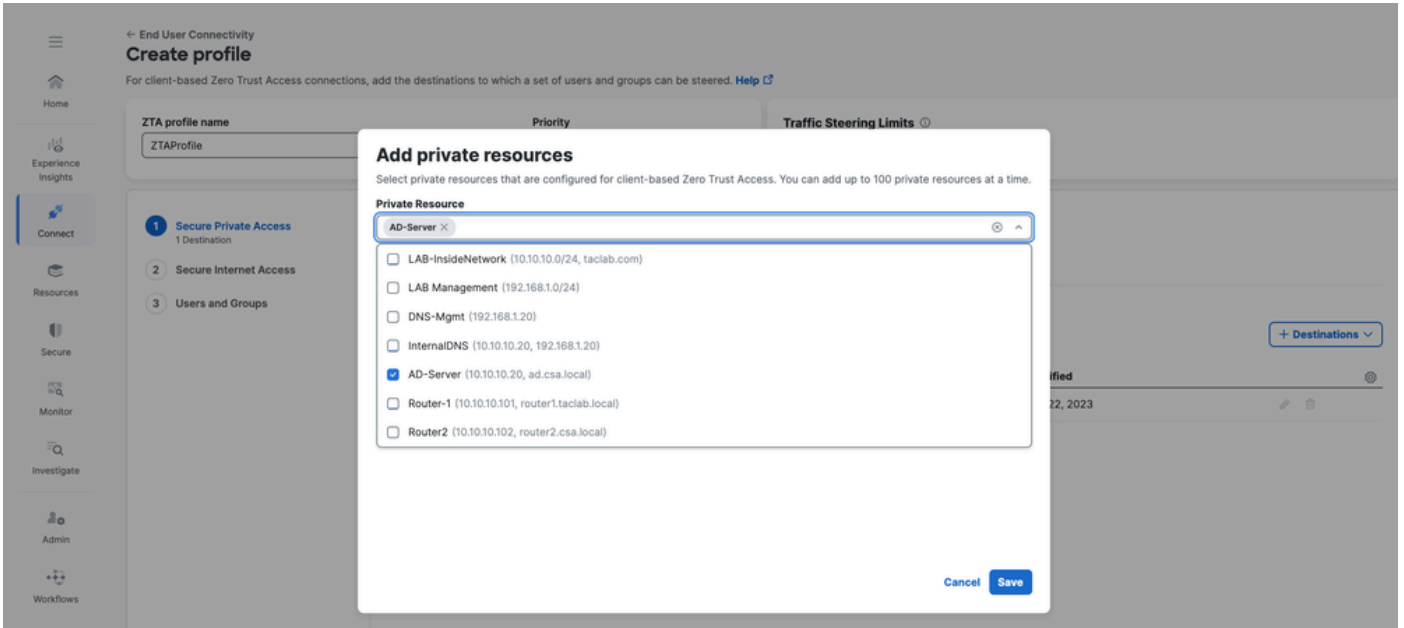


Accès sécurisé - Profil ZTA

2. Ajouter la ressource privée

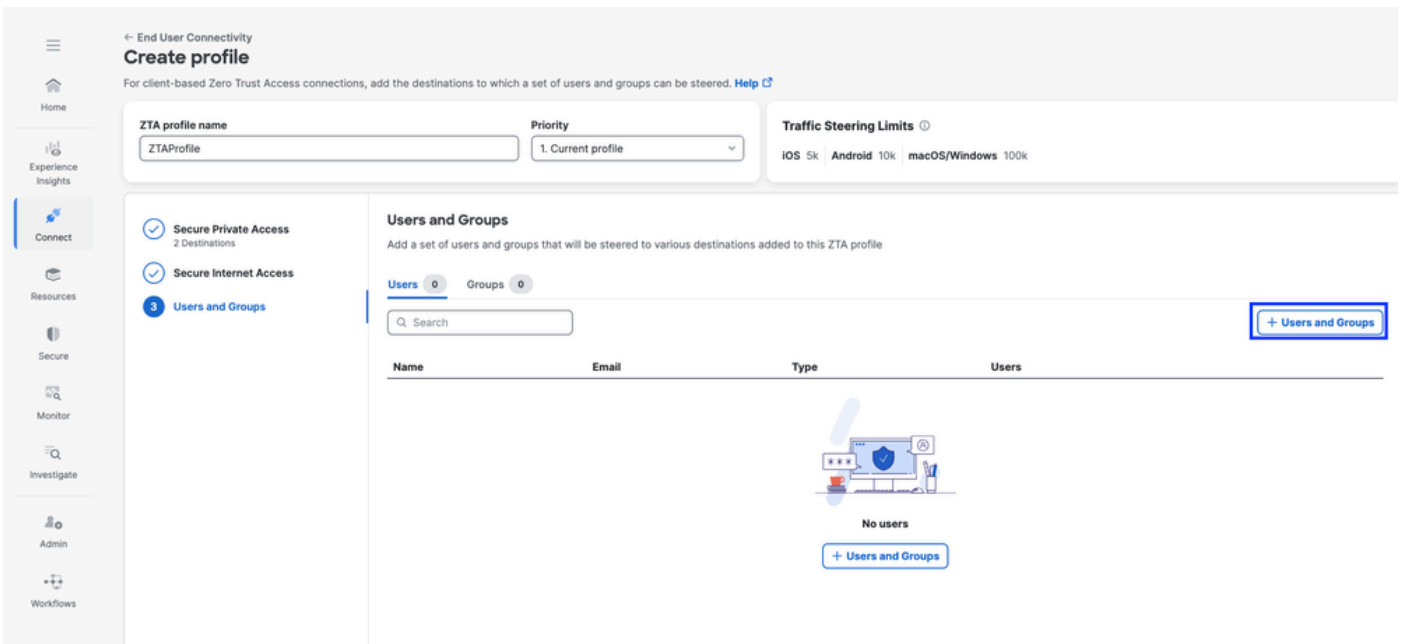


Accès sécurisé - Profil ZTA



Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes



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

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

Users and Groups

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

Users 1 | Groups 0

Q Search + Users and Groups

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

Rows per page: 10

Back Close

Accès sécurisé - Profil ZTA

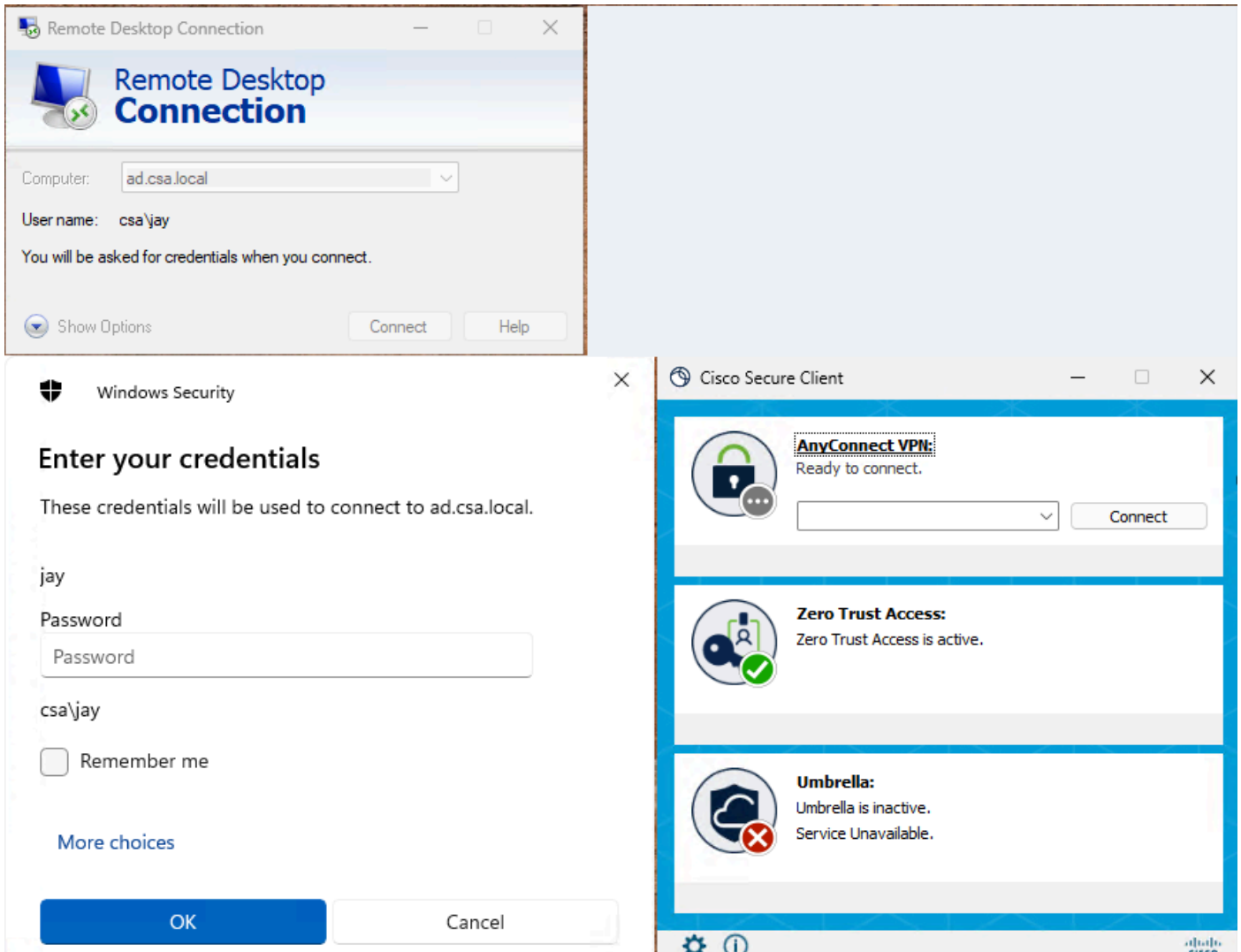


Remarque : La transmission et la synchronisation de la configuration au client pour la ressource privée attribuée peut prendre de 15 à 20 minutes

Étape 4 - Vérifiez l'accès à la ressource privée

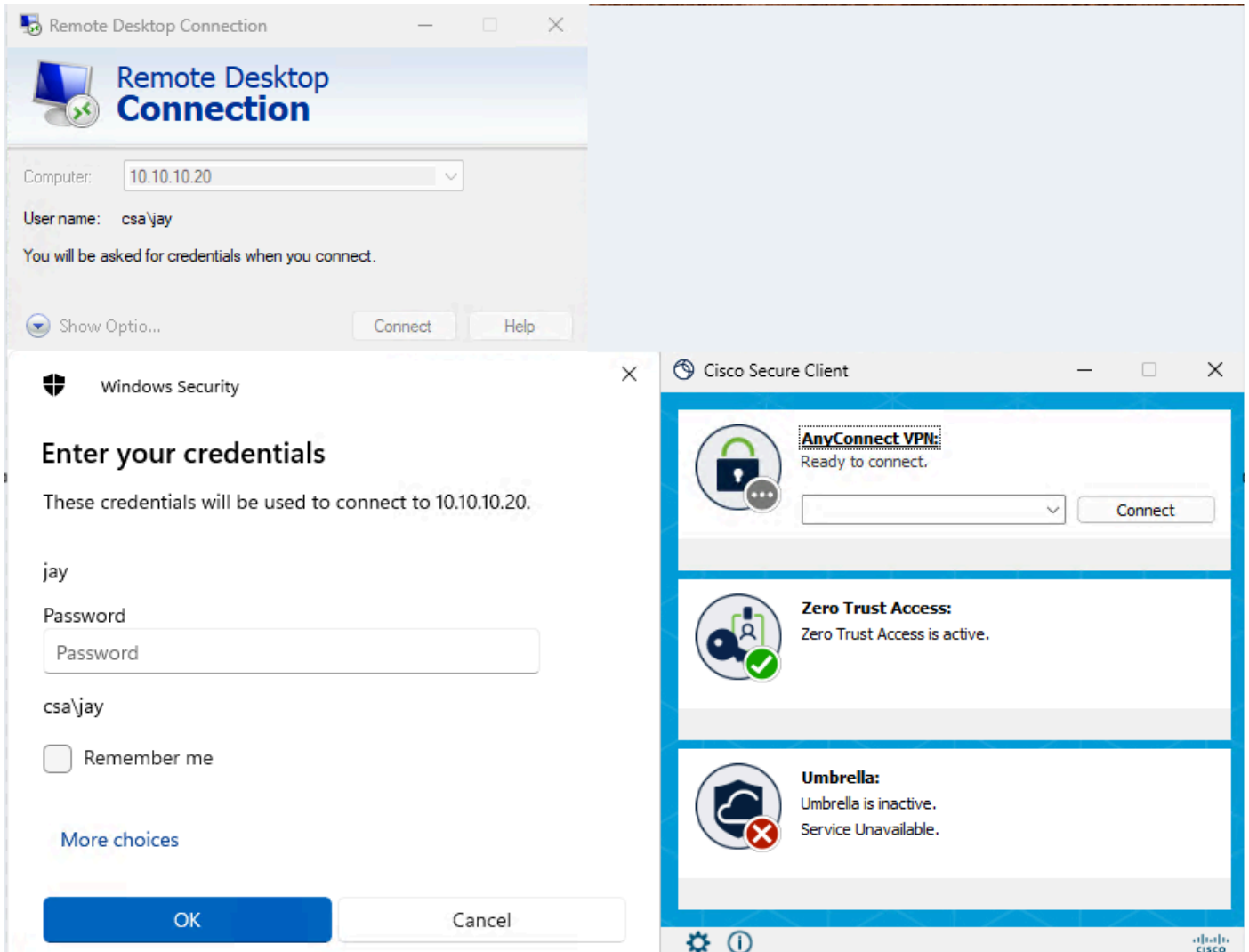
1. Accéder à la ressource privée

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

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 RESPONSE Allowed Restore to default layout Save Search

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

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

Accès sécurisé - Recherche d'activité

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 PORT 3389 Restore to previous state Save Search

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

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

Event Details

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

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

Accès sécurisé - Recherche d'activité

Activity Search Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 Restore to default layout Save Search

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

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

Accès sécurisé - Recherche d'activité

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 Restore to default layout Save Search

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

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 12, 2026 5:51 AM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: AD-RDP-Allow

Resource/Application: AD-Server

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: 10.10.10.20

Destination IP

Accès sécurisé - Recherche d'activité

3. Vérifiez les événements de connexion FMC

Events Troubleshooting

Destination Port / ICMP Code 3389

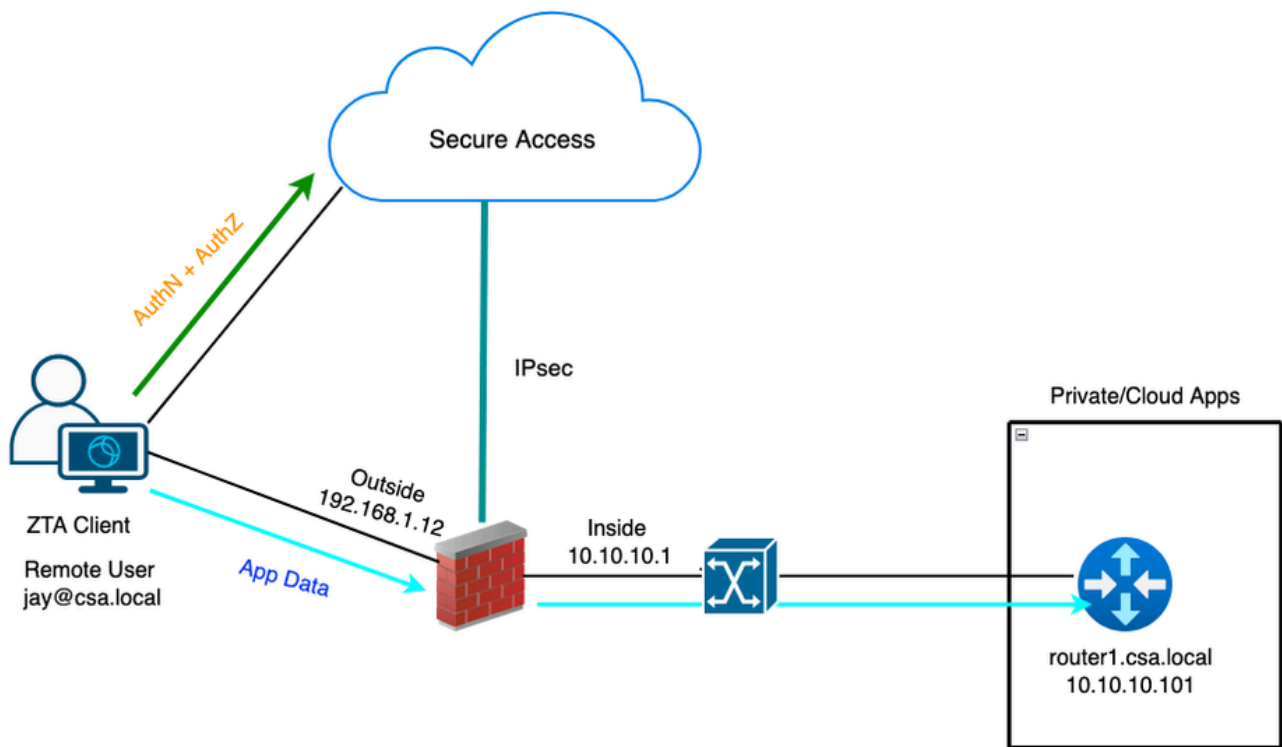
7 events Last 1 hour

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

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

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

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.

← Private Resources

Add a Private Resource

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

General

Private Resource Name

Router1

Description (optional)

Router1 PR for UZTNA testing

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

Private resource address

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

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

Use internal DNS server to resolve the domain

Internal DNS Server: PrivateDNS (10.10.10.20)

Accès sécurisé - Configuration des ressources privées

5. Sélectionner les méthodes de connexion Endpoint

6. Sélectionnez FTD comme points d'application locaux

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

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

Enforcement point for Remote User



Enforcement point for Local user



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

Change the remotely reachable addresses

Cancel

Save and Test

Save

Accès sécurisé - Configuration des ressources privées



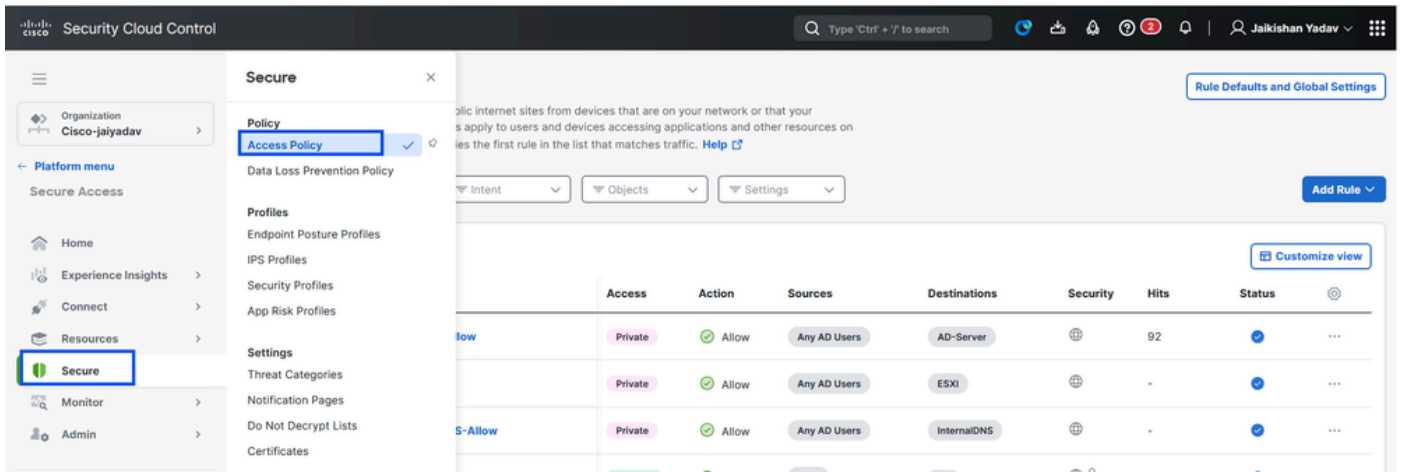
Remarque : Selon le type d'inscription sélectionné, cette modification associera automatiquement le PR au FTD et déclenchera un déploiement de stratégie

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](#)

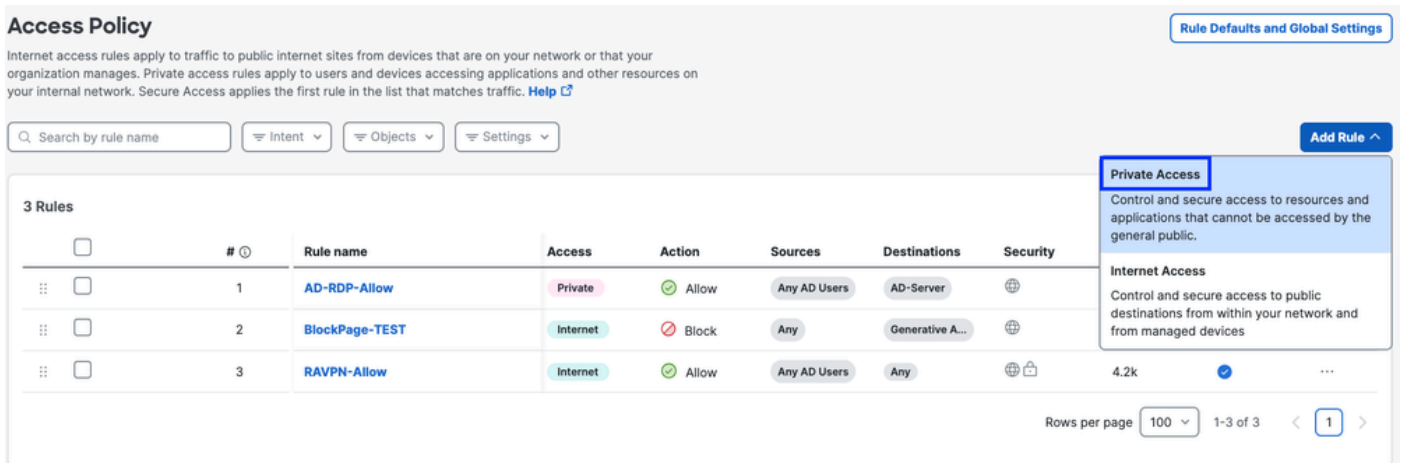
1. Accédez à Secure > Access Policy



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

Add Router1-SSH

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

Accès sécurisé - Configuration de la stratégie d'accès

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

Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

From

Specify one or more sources.

AD Users - Any AD Users

To

Specify one or more destinations.

Private Resources - Router1

+ AND

Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux

Endpoint Requirements

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

Zero-Trust Client-based Posture Profile [Rule Defaults](#)
Requirements for end-user devices on which the Cisco Secure Client is installed.
Profile: **None** | Requirements: **None**
Private Resources: **Router-1**

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

User Authentication Requirements

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

2 Configure Security

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

[Cancel](#)

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

Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité

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

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

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

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

[Cancel](#)

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

Accès sécurisé - Configuration de la stratégie d'accès

7. Cliquez sur Enregistrer

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

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

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

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

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows the 'Connect' section with 'Network Connections' selected. Below this, there are two tabs: 'Network Groups' and 'FTDs', with 'FTDs' being the active tab. The 'FTDs' tab displays a summary of connections: 0 Warning and 1 Connected. Below this, there is a section for '2 Tunnel Groups' with an '+ Add' button.

Accès sécurisé - Vérification PR

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

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

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

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status	
Synced	1

[View resources associated to this FTD](#)

[Associate Resources](#)

Accès sécurisé - Vérification PR

Resources associated with FMC_FTD

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

Q Search by resource name

Configuration status

1 Resources

[Associate Resources](#)

Resource name

Status

Router1

Synced

[Close](#)

Accès sécurisé - Vérification PR

3. Cliquez sur Fermer

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

The screenshot displays the Palo Alto Networks management console. On the left, the 'Network Connections' page shows a table of FTDs configured for Universal Zero Trust Access. The table has columns for FTD Name, Version, FMC, UZTA Configuration status, and Associated Resources. One FTD, 'FMC_FTD', is listed with version v10.0.0, FMC, and a 'Synced' status. On the right, a detailed view for 'FMC_FTD' is shown, including Firewall Details (Device FQDN: ftd.csa.local, Auto deployment: Yes), UZTA Configuration status (Synced, Last synced at 31 Dec 2025, at 2:51 AM UTC), Assigned Trusted Network (LAN, 1 DNS Servers), and Associated Resources (1 resource associated by status).

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

End User Connectivity

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

Zero Trust Access | Virtual Private Network | Internet Security

Enrollment methods Manage

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

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

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

Context menu options: Edit, Delete

Accès sécurisé - Profil ZTA

2. Ajouter la ressource privée

Create profile

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

ZTA profile name: ZTAProfile | Priority: 1. Current profile

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

1 Secure Private Access (0 Destinations)

2 Secure Internet Access

3 Users and Groups

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

Traffic Steering | Options

Search by destination

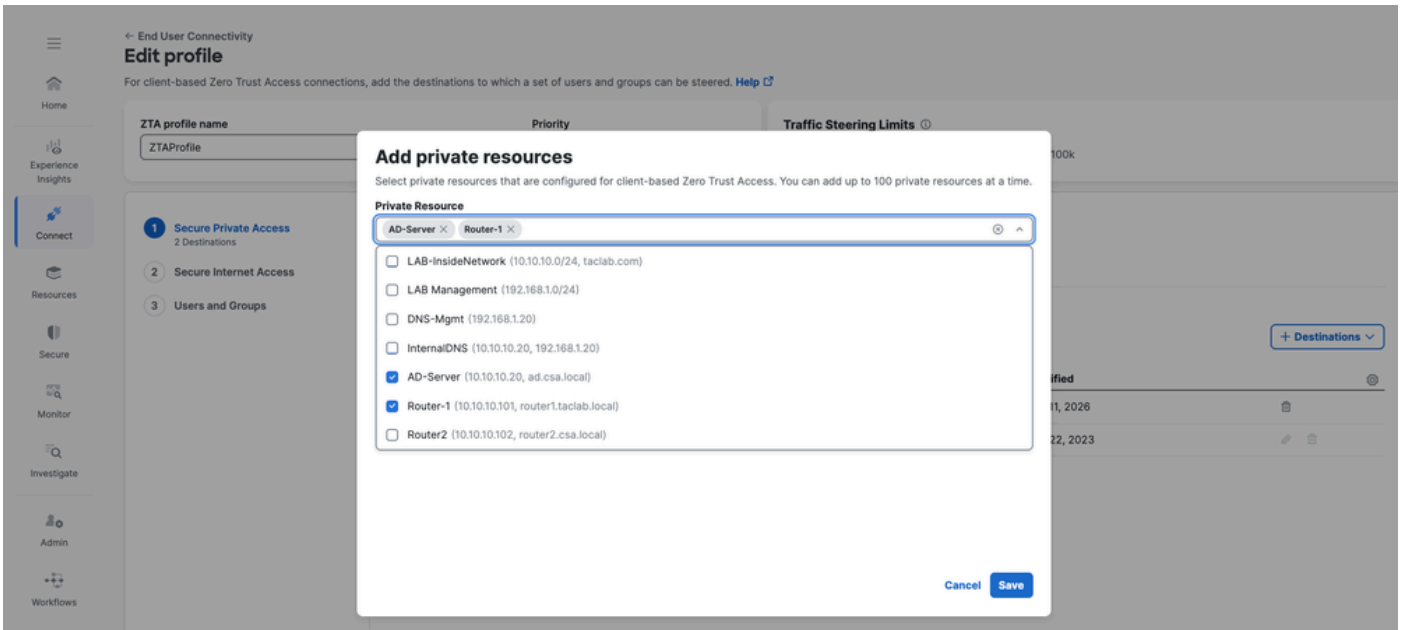
Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

+ Destinations

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

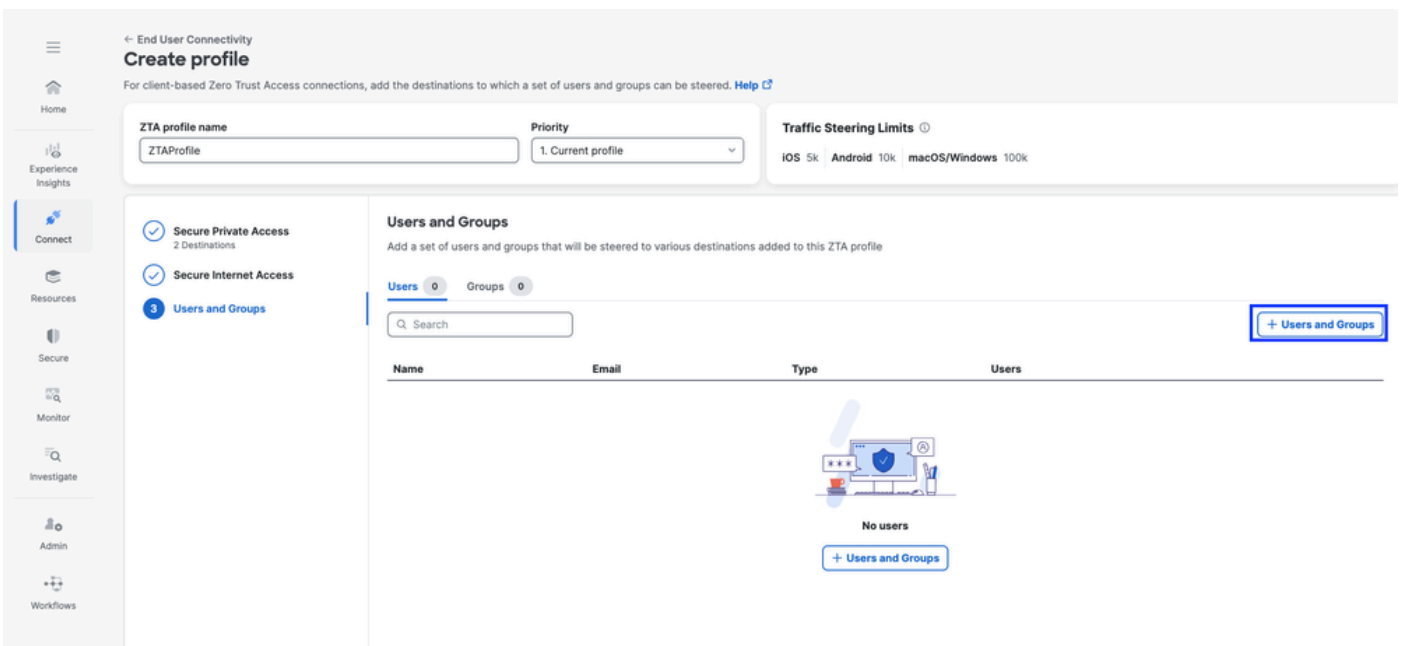
Add Destination
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Accès sécurisé - Profil ZTA



Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes



Accès sécurisé - Profil ZTA

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

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

Users and Groups

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

Users: 1 | Groups: 0

 + Users and Groups| Name | Email | Type | Users |
| --- | --- | --- | --- |
| jay (jay@csa.local) | jay@gmail.com | User | - |

Rows per page: 10

Back Close

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
```

Accès sécurisé - Test PR

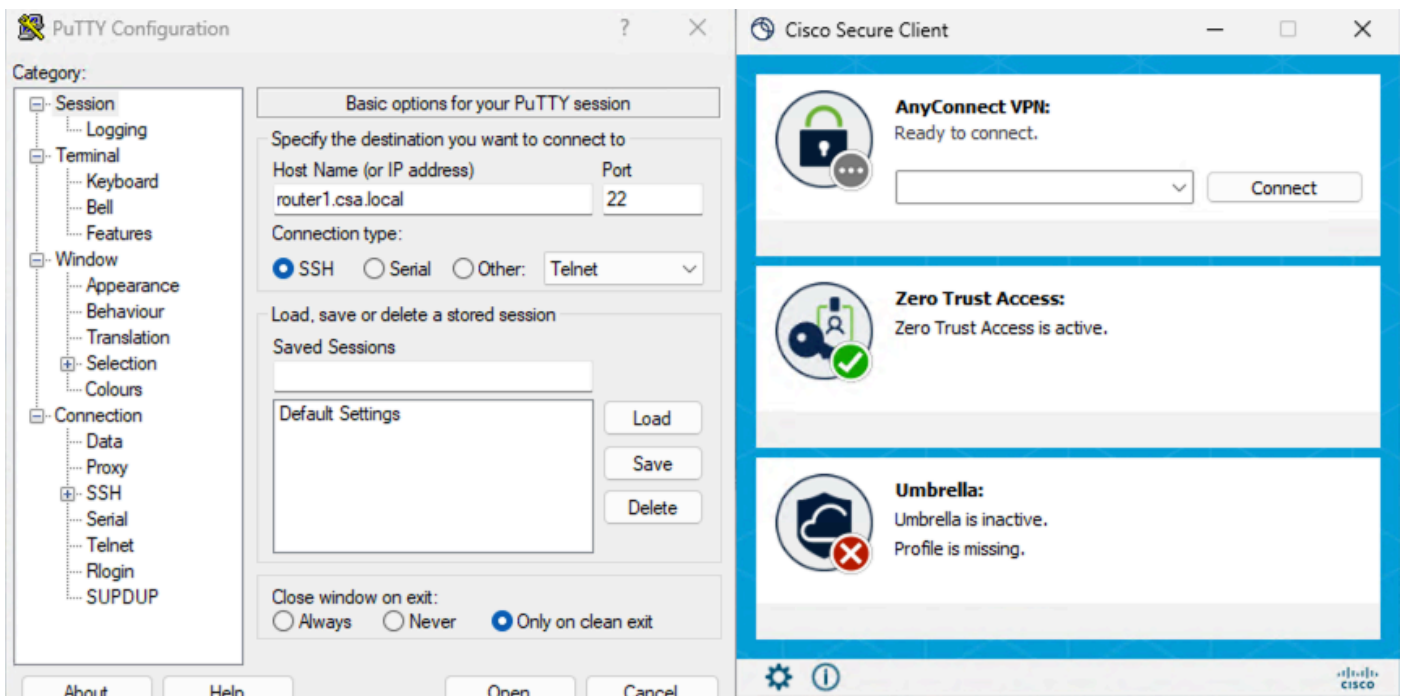
2. Vérifiez que FTD peut accéder à une ressource privée à l'aide du nom de domaine complet

```
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# █
```

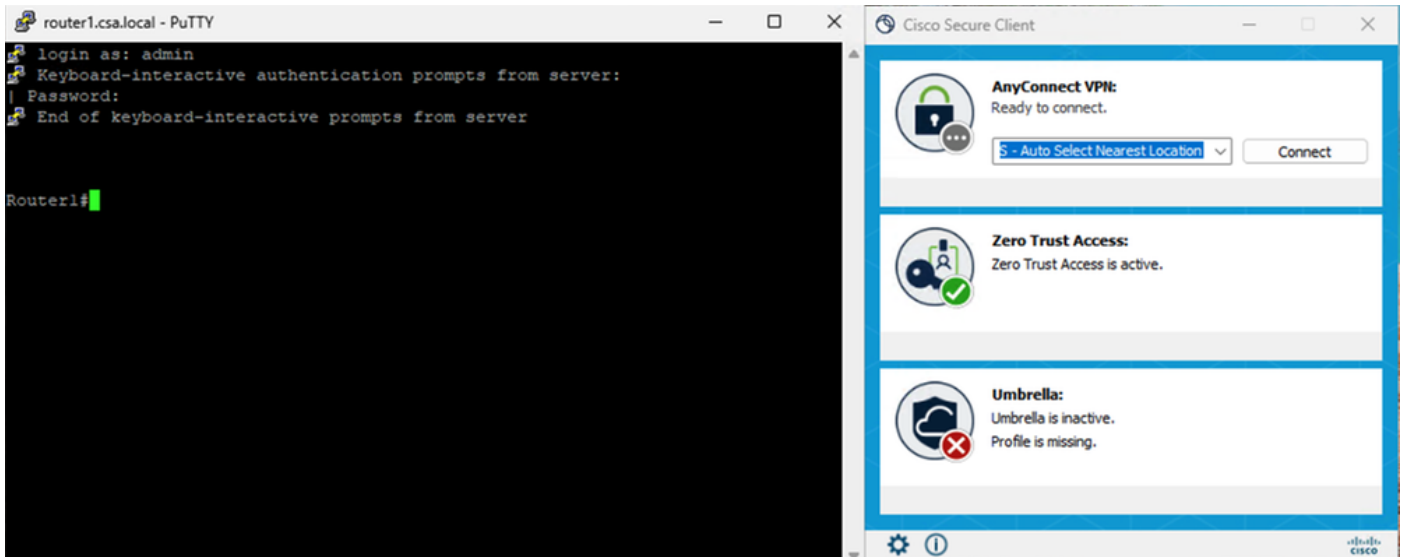
Accès sécurisé - Test PR

3. Tester la connexion SSH à la ressource privée

Accéder au RP à l'aide du FQDN

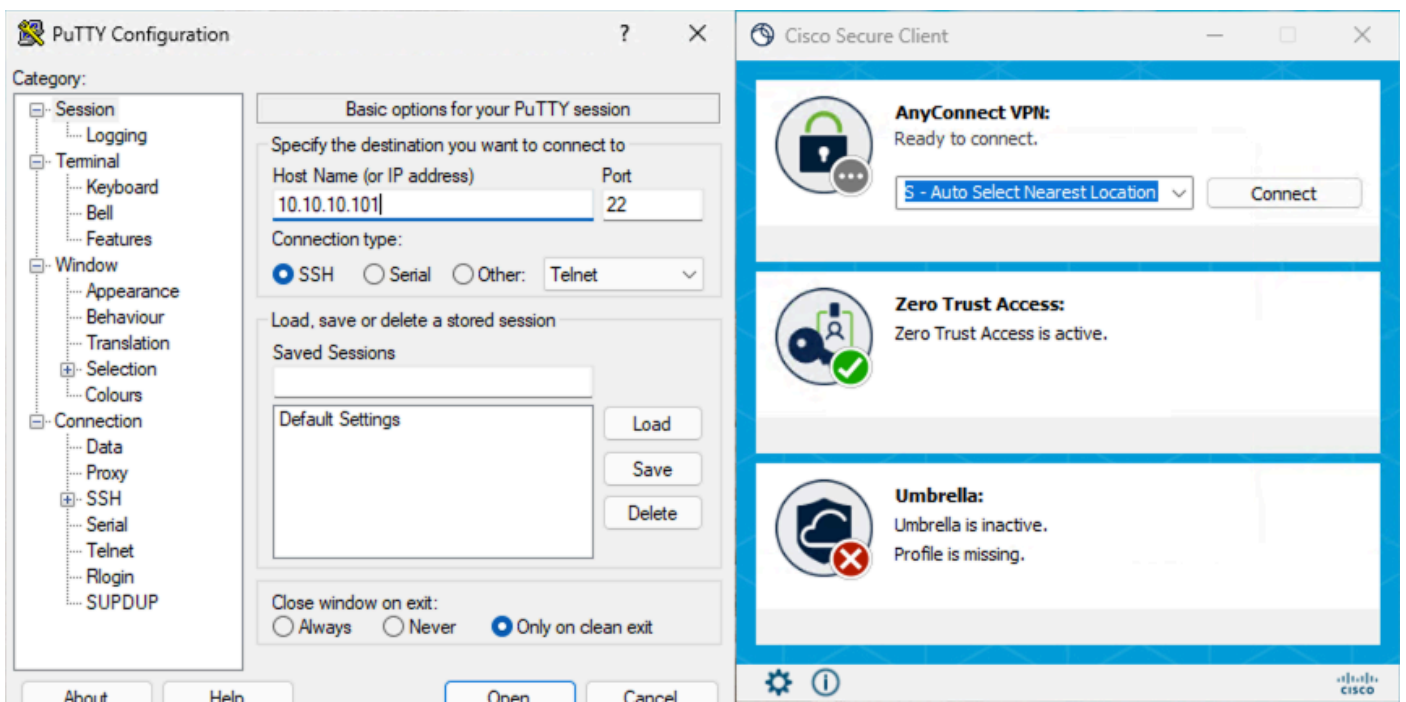


Accès sécurisé - Test PR

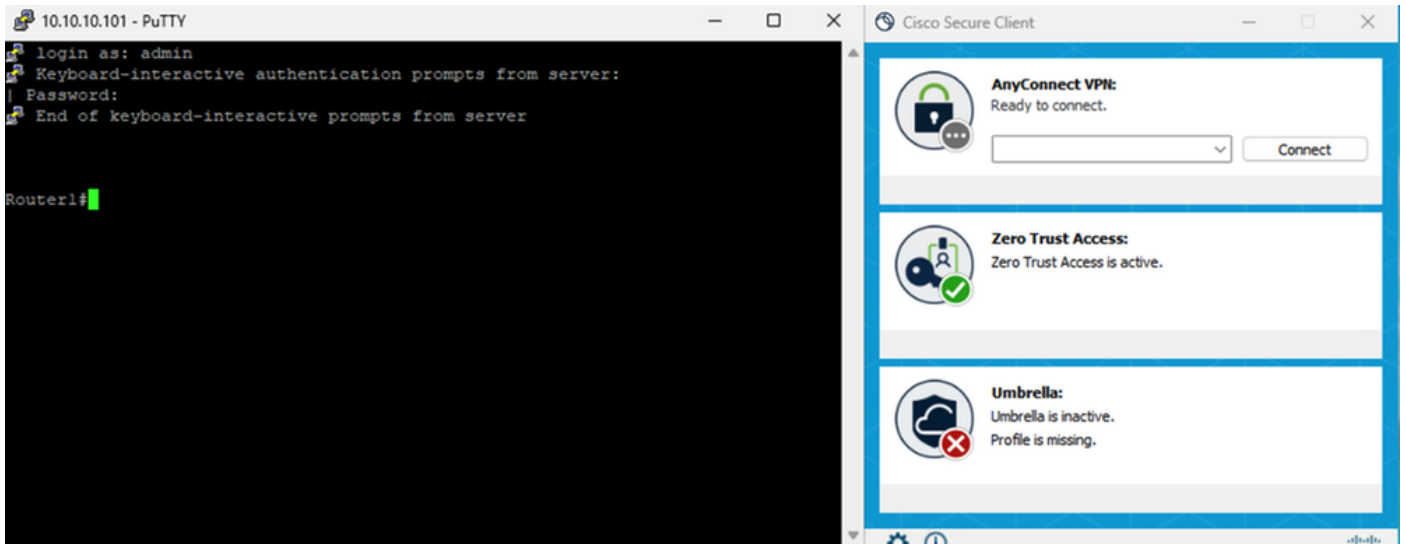


Accès sécurisé - Test PR

Accéder au RP en utilisant l'adresse IP



Accès sécurisé - Test PR



Accès sécurisé - Test PR

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

Activity Search

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

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

Accès sécurisé - Recherche d'activité

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

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:55 PM

Access details

Identity: jay (jay@csa.local)

Win: Win10

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD> FMC_FTD

Destination: router1.csa.local

Destination IP: -

Accès sécurisé - Recherche d'activité

Activity Search

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

IP ADDRESS: 10.10.10.101 X RESPONSE: Allowed X

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

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

Accès sécurisé - Recherche d'activité

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

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:56 PM

Access details

Identity: jay (jay@casa.local)

Win1

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD> FMC_FTD

Destination: 10.10.10.101

Destination IP: 10.10.10.101

Accès sécurisé - Recherche d'activité

5. Vérifier les événements de connexion FMC

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

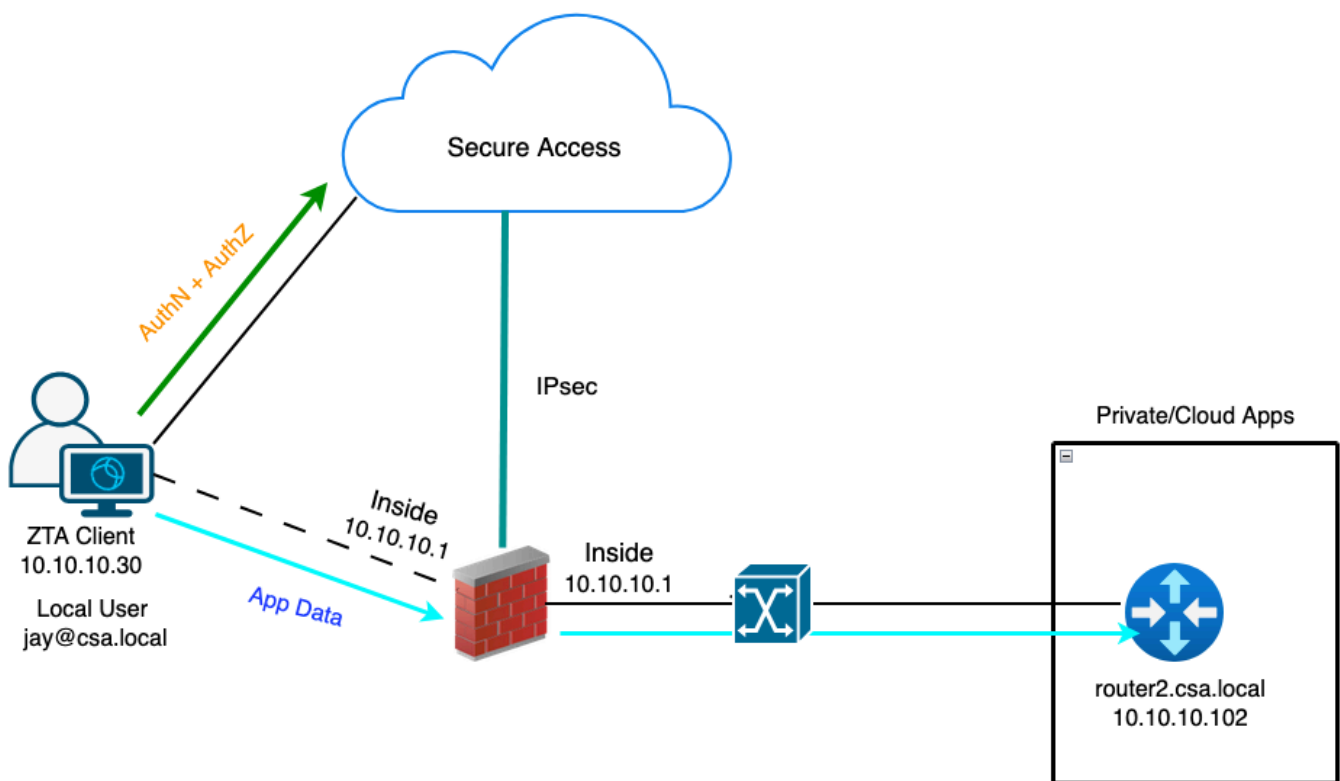
Search: [Destination IP: 10.10.10.101] Refresh

6 events

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

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.

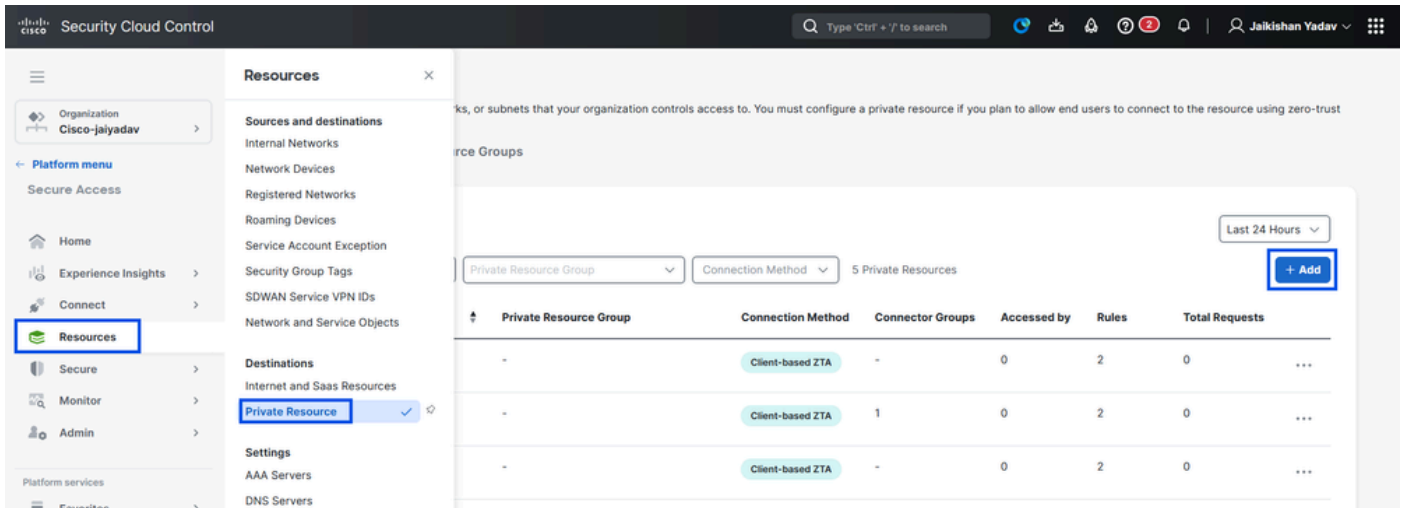


ZTA universel - Topologie de cas de test

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

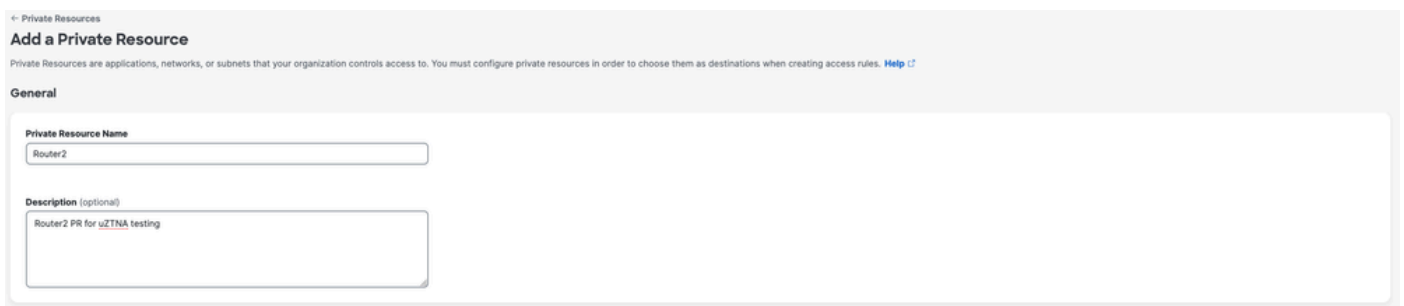
Configurer une ressource privée pour qu'elle soit accessible via un périphérique inscrit ZTA (Zero Trust Access) avec application cloud

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

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) Protocol Port / Ranges + Protocol & Port

[Remove](#)

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) Protocol Port / Ranges + Protocol & Port

[Remove](#) + IP Address/FQDN

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

Internal DNS Server

Accès sécurisé - Configuration des ressources privées

5. Sélectionner les méthodes de connexion Endpoint

6. Sélectionnez FTD comme points d'application locaux

Endpoint Connection Methods

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

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

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

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

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

Enforcement point for Remote User

Remote user Local Firewall

Enforcement point for Local user

User in a trusted network Local Firewall

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

Change the remotely reachable addresses

[Cancel](#) [Save and Test](#) [Save](#)

Accès sécurisé - Configuration des ressources privées



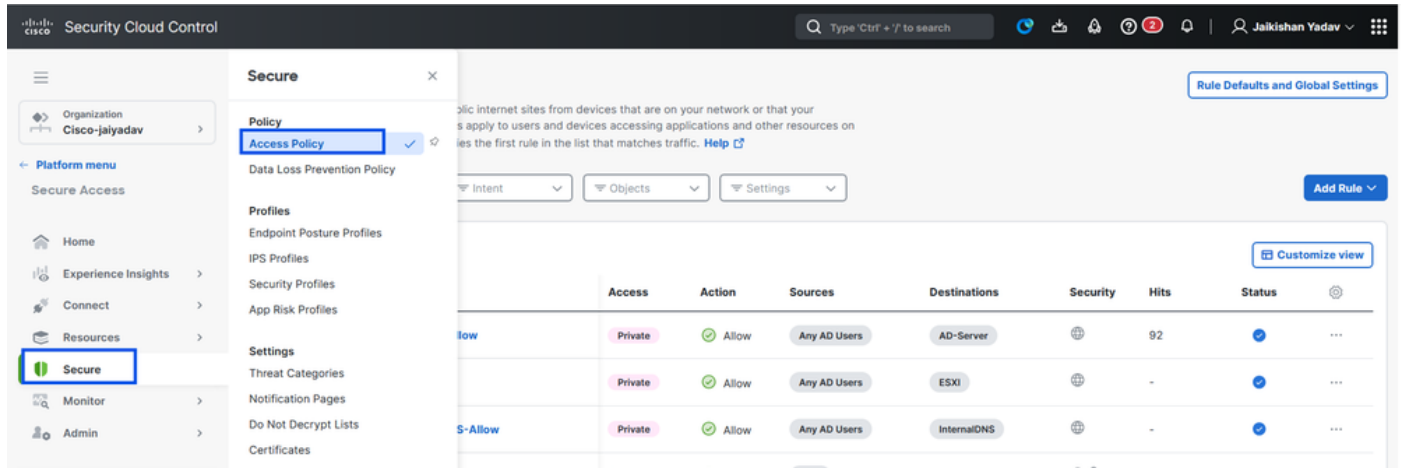
Remarque : Selon le type d'inscription sélectionné, cette modification associera automatiquement le PR au FTD et déclenchera un déploiement de stratégie

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](#)

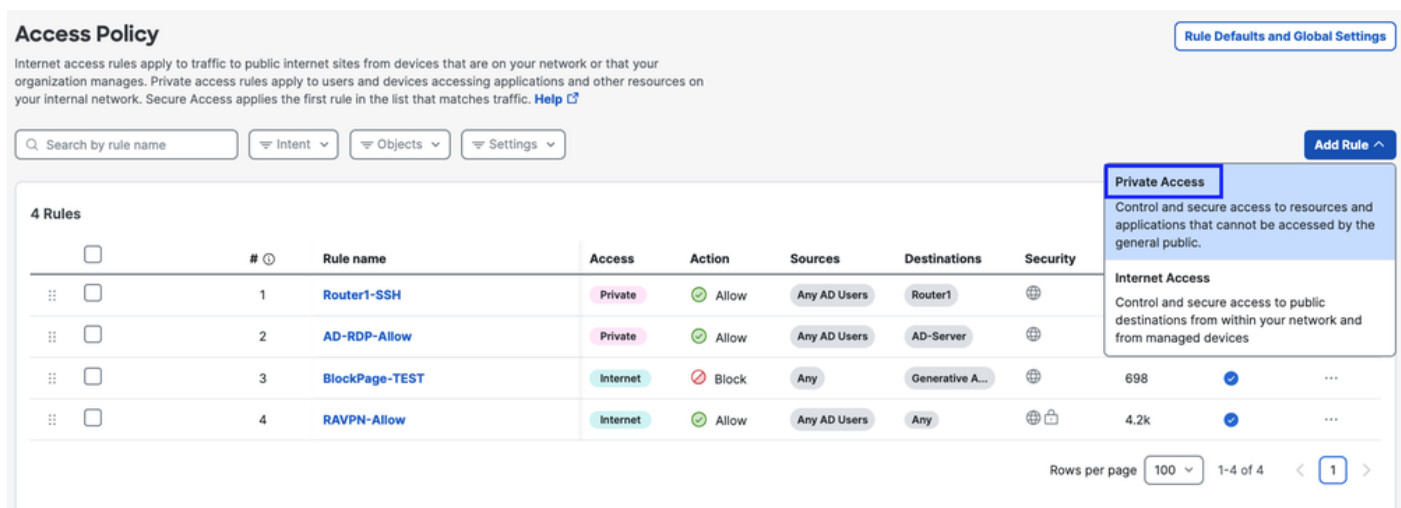
1. Accédez à Secure > Access Policy



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

Add Router2-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Accès sécurisé - Configuration de la stratégie d'accès

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

Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources

AD Users - Any AD Users

To

Specify one or more destinations

Private Resources - Router2

+ AND

Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux

Endpoint Requirements

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

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

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

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

Private Resources: **Router2**

For Branch connections:

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

User Authentication Requirements

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

Disabled

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

2 Configure Security

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

[Cancel](#)

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

Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité

Specify Access

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

2 Configure Security

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

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

Disabled

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

Security Profile [Rule Defaults](#)

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

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

[Cancel](#)

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

Accès sécurisé - Configuration de la stratégie d'accès

7. Cliquez sur Enregistrer

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

5 Rules

Customize view

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

Rows per page 100 1-5 of 5 1

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

The screenshot shows the Cisco Security Cloud Control interface. The 'Connect' menu is open, highlighting 'Network Connections'. The main content area shows 'FTDs' with a status of '1 Connected' and '0 Warning'. There are filters for 'Region' and 'Status' and an '+ Add' button.

Accès sécurisé - Vérification PR

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

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

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

Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

Device FQDN ftd.csa.local
Auto deployment Yes

UZTA Configuration status

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

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status
Synced 2

View resources associated to this FTD

Associate Resources

Accès sécurisé - Vérification PR

Resources associated with FMC_FTD

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

Search by resource name

Configuration status

2 Resources

Associate Resources

Resource name	Status
Router1	Synced
Router2	Synced

Close

3. Cliquez sur Fermer

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

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

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

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

```

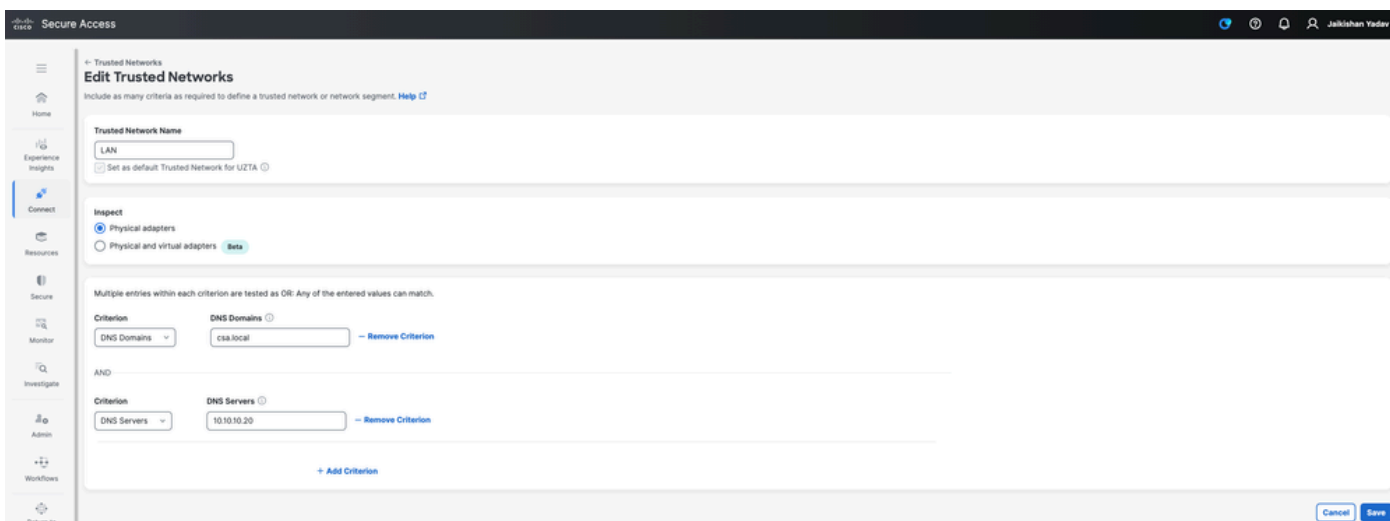
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal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

End User Connectivity

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

Zero Trust Access | Virtual Private Network | Internet Security

[Cisco Secure Client](#) | [Manage servers](#)

Enrollment methods [Manage](#)

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles [Manage Trusted Networks](#) | [+ ZTA Profile](#)

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

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

[Edit](#) | [Delete](#)

Accès sécurisé - Profil ZTA

2. Ajouter la ressource privée

Create profile

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

ZTA profile name: Priority:

Traffic Steering Limits

IOS 5k | Android 10k | macOS/Windows 100k

1 Secure Private Access (0 Destinations)

2 Secure Internet Access

3 Users and Groups

Secure Private Access

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

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

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

[+ Destinations](#)

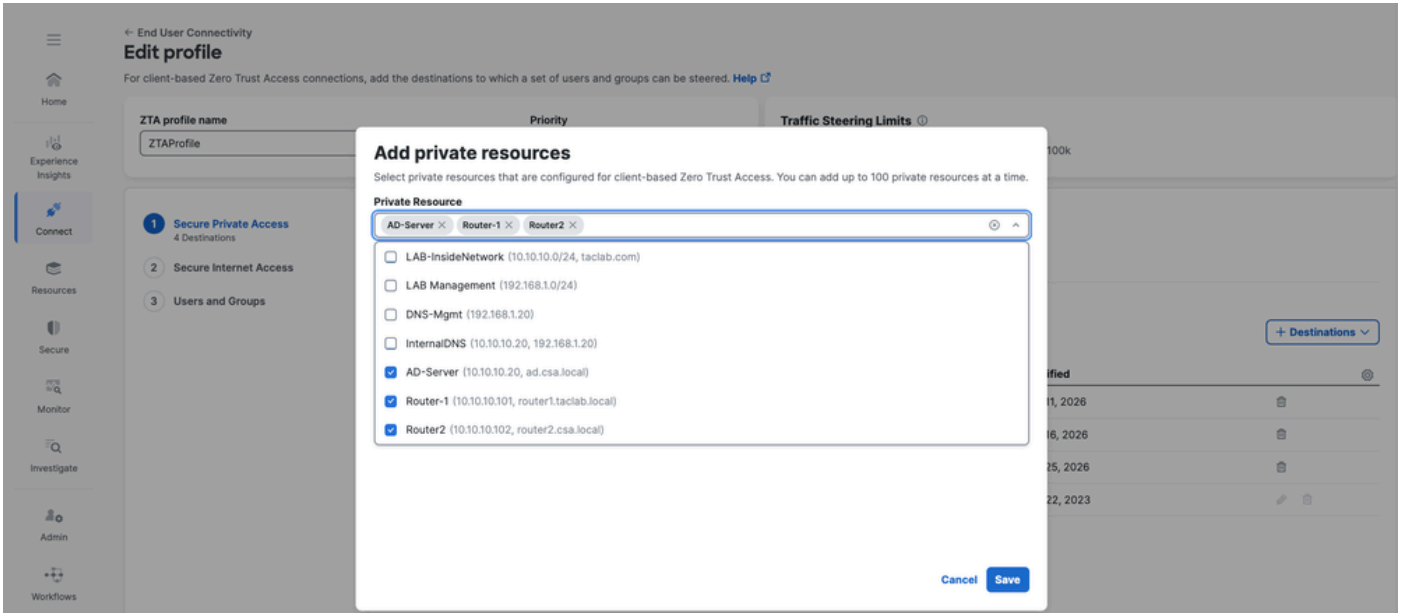
Private Resource

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

Add Destination

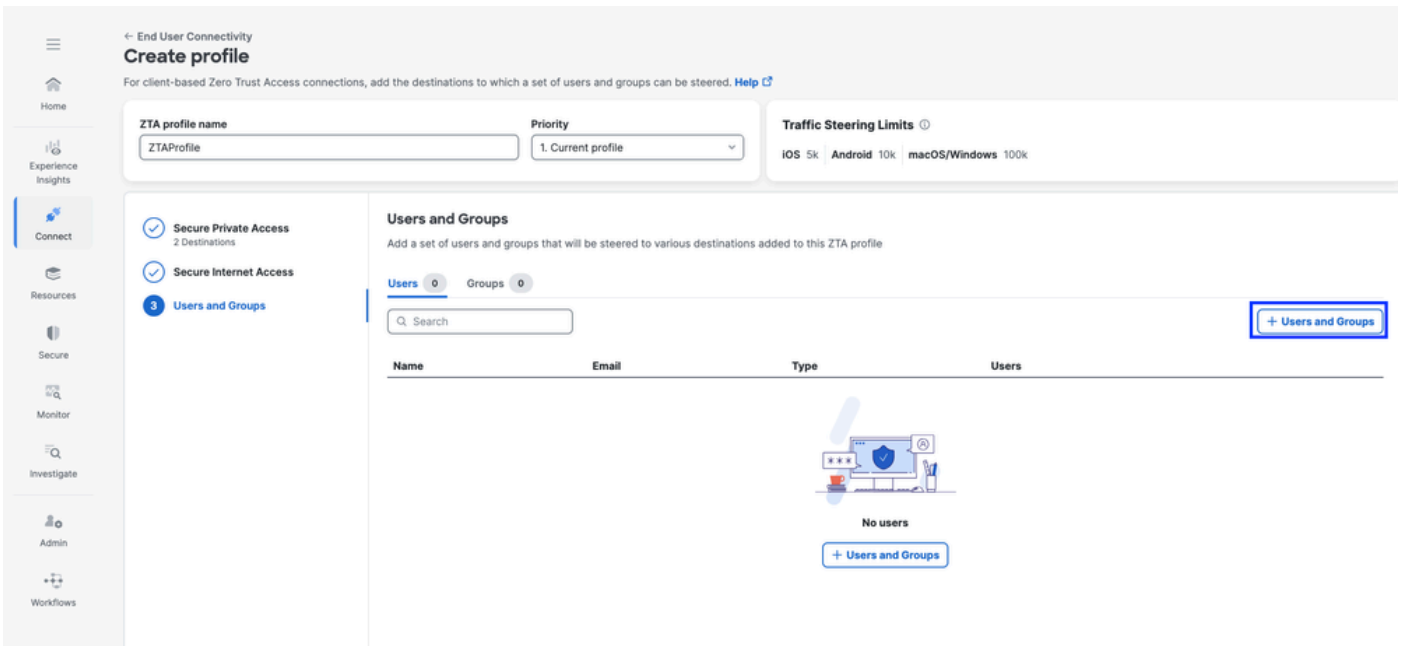
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Accès sécurisé - Profil ZTA



Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes



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

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

Users and Groups

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

Users 1 | Groups 0

Q Search + Users and Groups

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

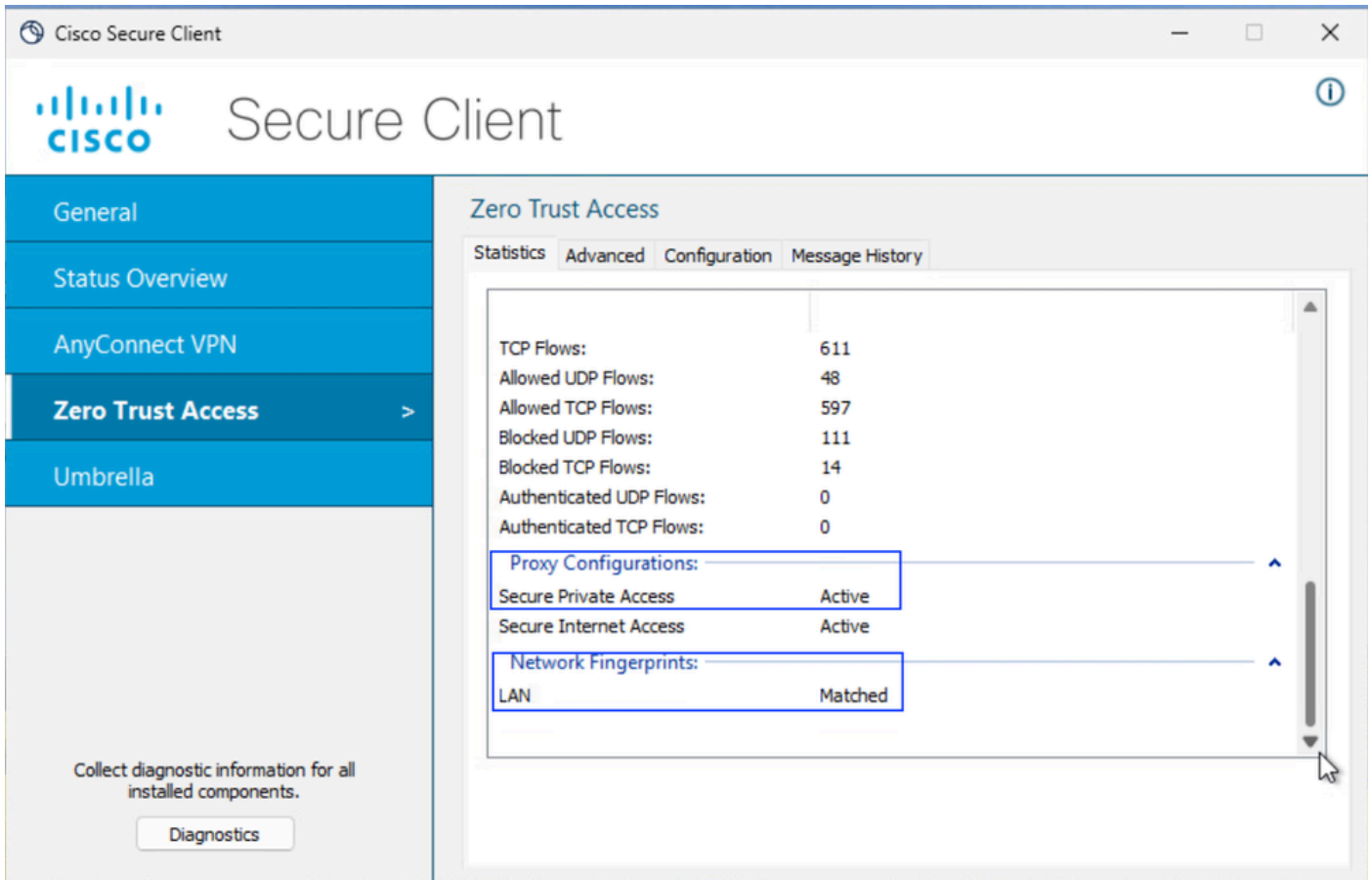
Rows per page: 10

Back Close

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

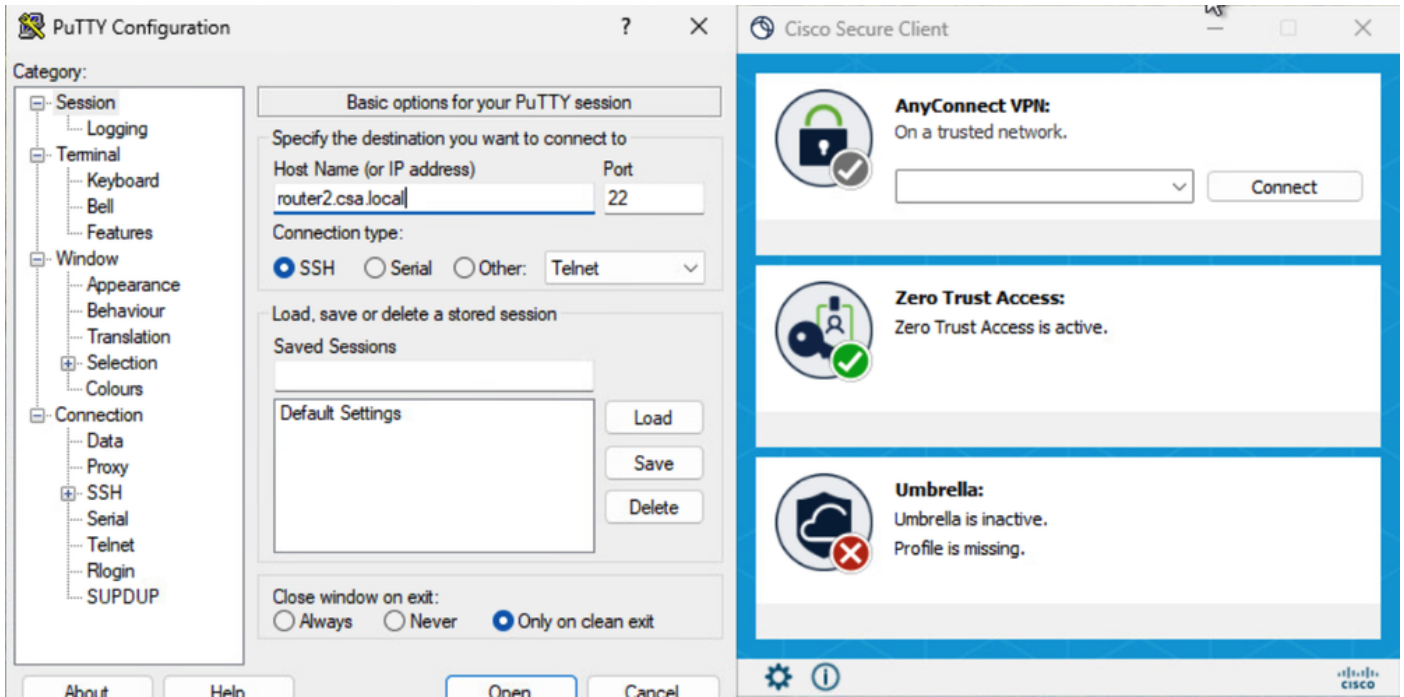
3. Vérifiez que FTD peut atteindre une ressource privée à l'aide du nom de domaine complet

```
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# █
```

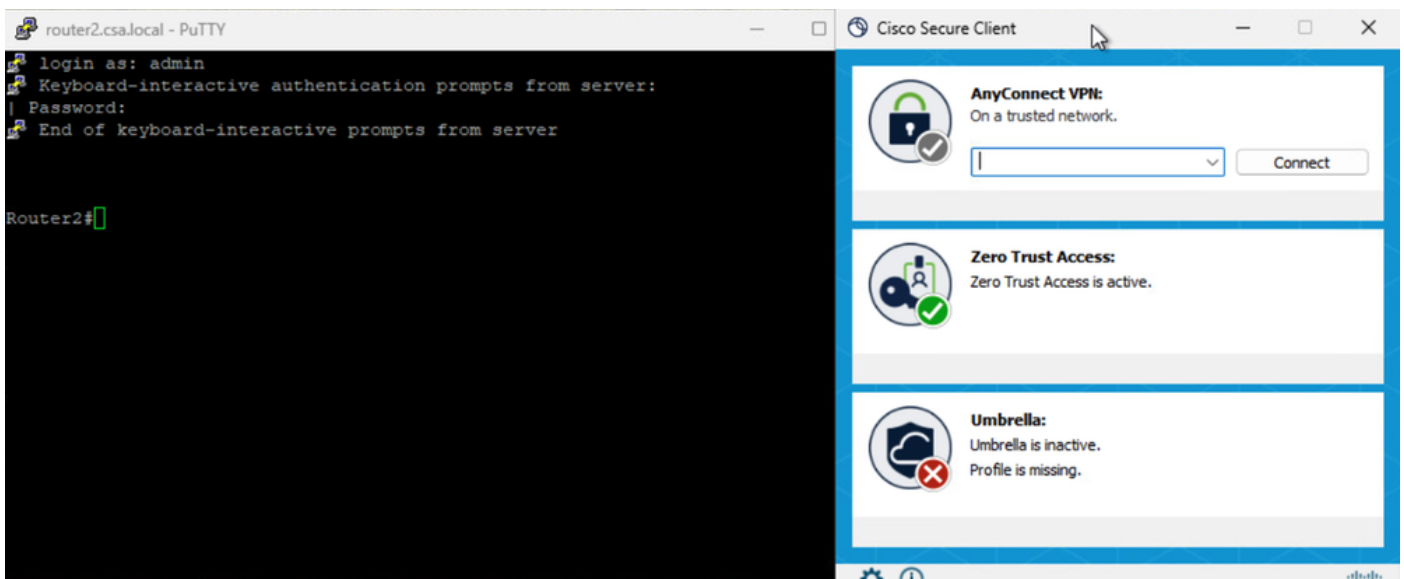
Accès sécurisé - Test PR

4. Tester la connexion SSH à la ressource privée

Accéder au RP à l'aide du FQDN

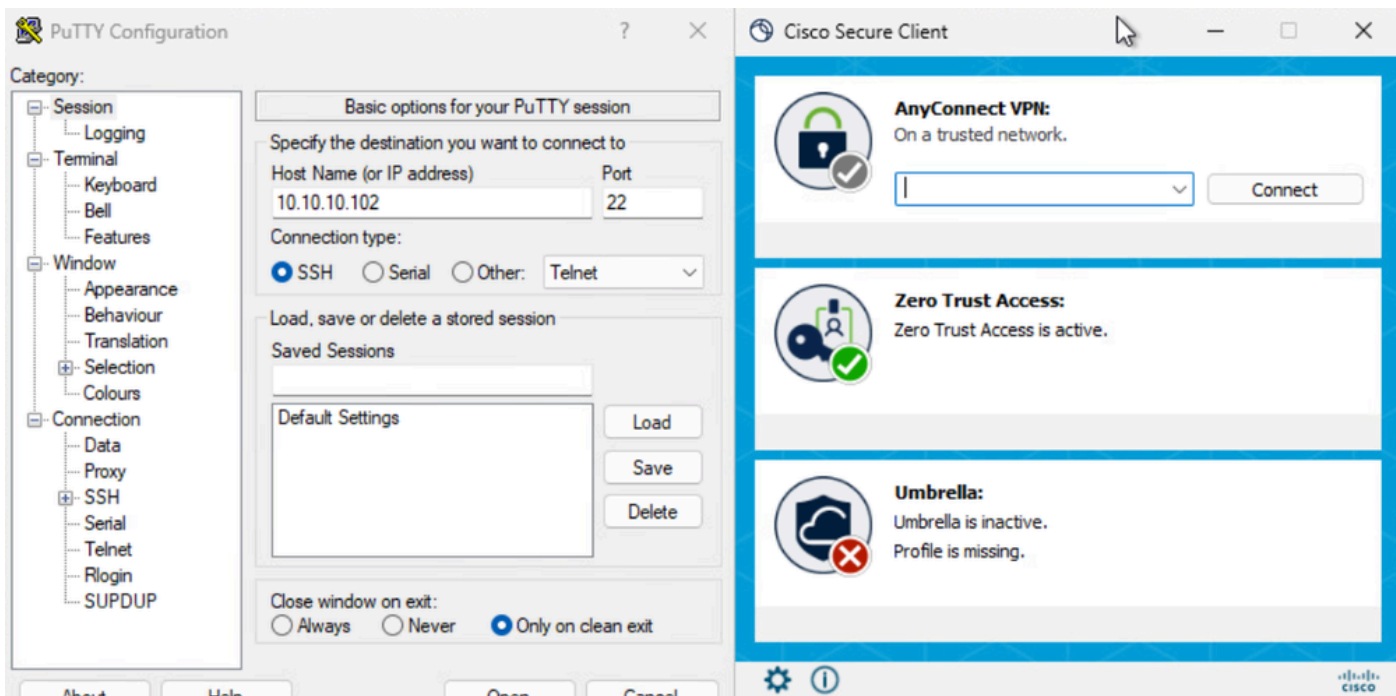


Accès sécurisé - Test PR

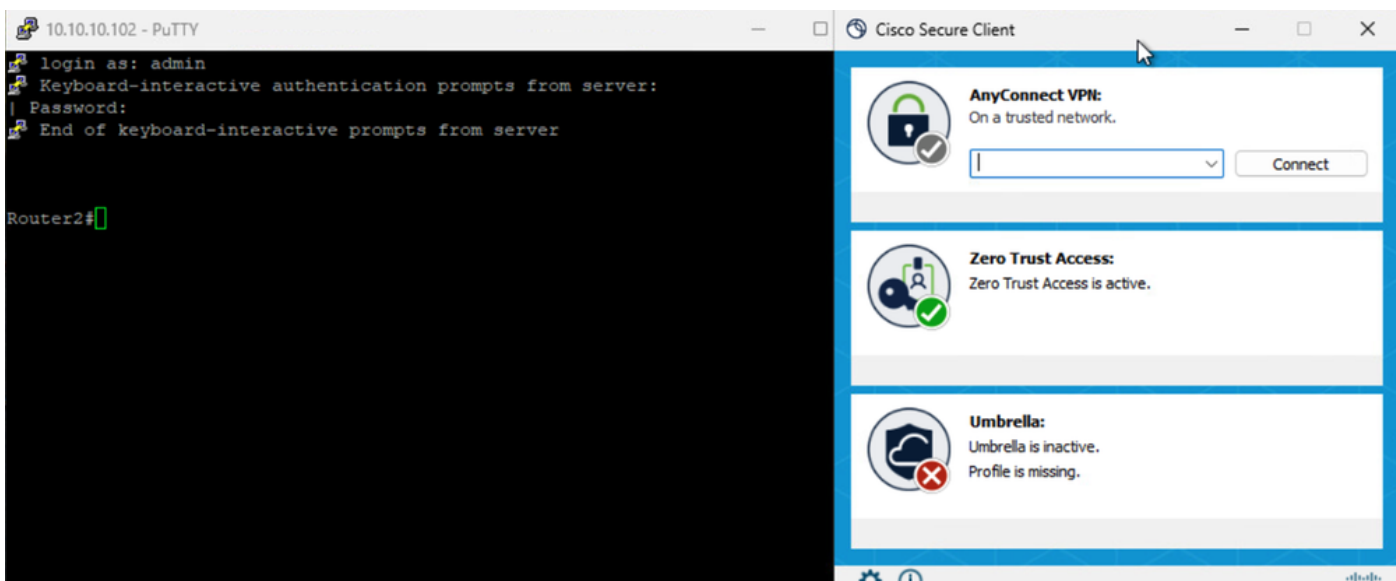


Accès sécurisé - Test PR

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

Activity Search

Activity Search interface showing a search for domain 'router2.csa.local'. The interface includes filters for Response (Allowed, Advanced, Blocked) and Identity Type (AD Users, AD Groups, AD Devices, SAML Users). The search results table shows 8 total results, all with a response of 'Allowed' and identity 'jey (jey@csa.local)'. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, OS, and Bro.

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

Accès sécurisé - Recherche d'activité

Activity Search

Activity Search interface showing a search for response 'Allowed'. The interface includes filters for Response (Allowed, Advanced, Blocked) and Identity Type (AD Users, AD Groups, AD Devices, SAML Users). The search results table shows 17 total results. An 'Event Details' sidebar is open for the selected row, showing details for the 'Allowed' action, including the connection method 'ZTA Client-based', time 'Feb 23, 2026 3:33 AM', and access details for user 'jey (jey@csa.local)' using rule 'Router2-SSH-Allow' and resource 'Router2'. The destination IP '192.168.1.23' is highlighted in a blue box.

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

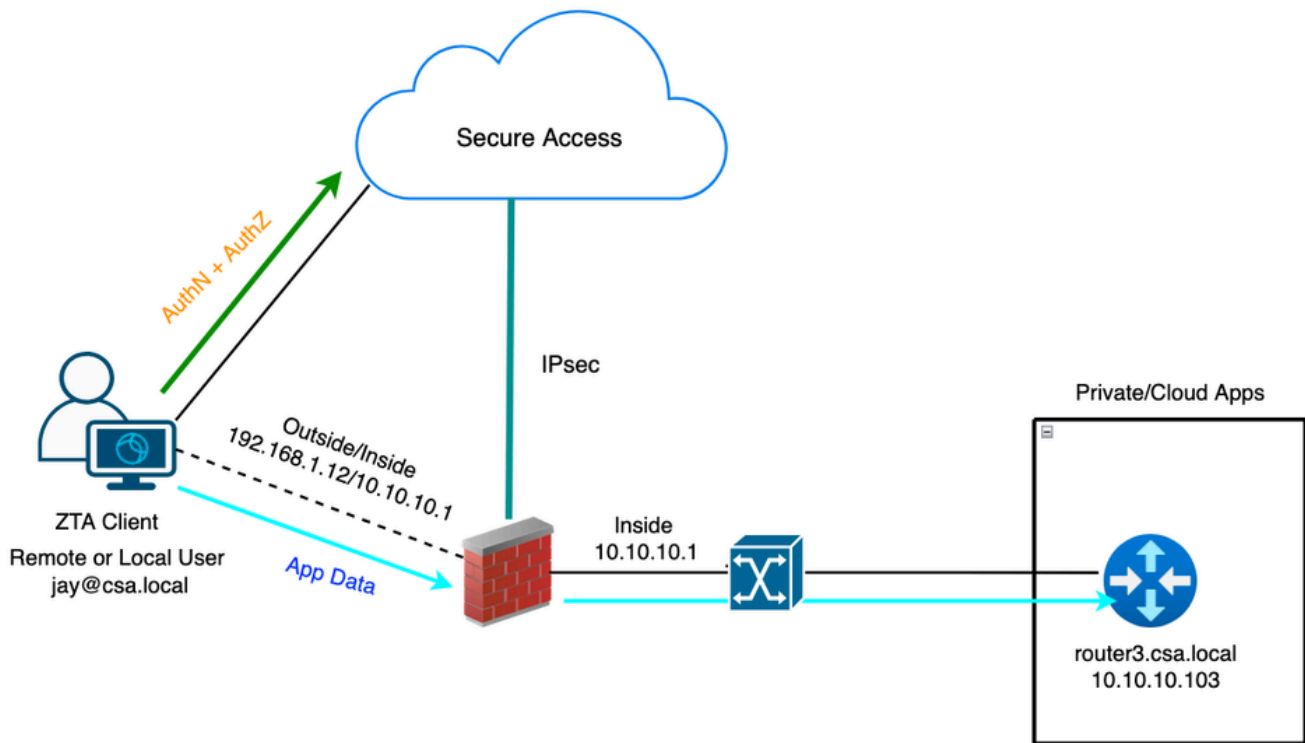
Accès sécurisé - Recherche d'activité

Activity Search

Activity Search interface showing a search for IP address '10.10.10.102' and response 'Allowed'. The interface includes filters for Response (Allowed, Advanced, Blocked) and Identity Type (AD Users, AD Groups, AD Devices, SAML Users). The search results table shows 19 total results, all with a response of 'Allowed' and identity 'jey (jey@csa.local)'. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, and Bro.

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

Accès sécurisé - Recherche d'activité



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

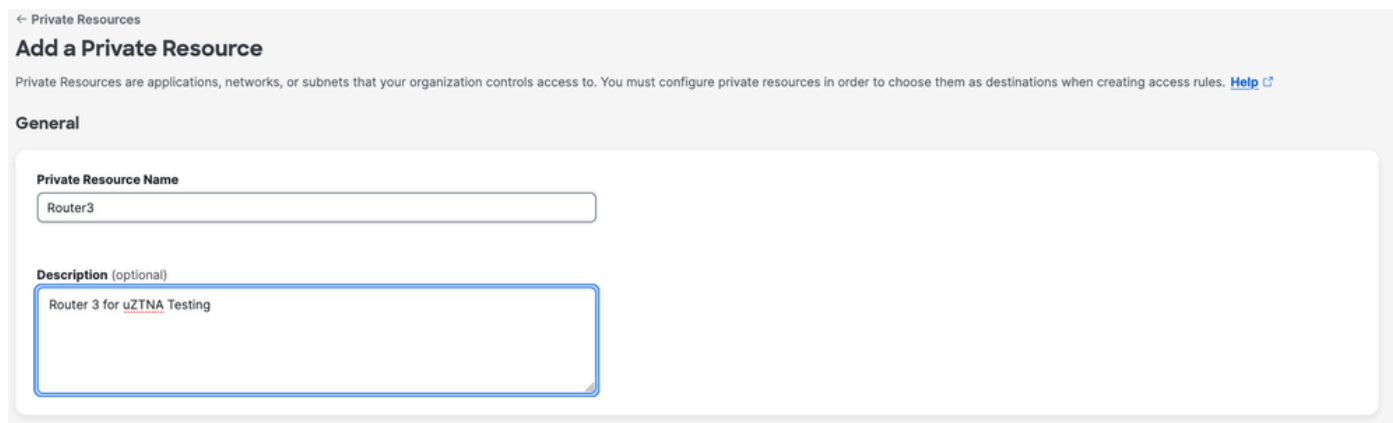
1. Accédez à Ressources > Destinations > Ressources privées > Cliquez sur +Ajouter

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a menu with 'Resources' highlighted. The main content area shows the 'Resources' configuration page. The page title is 'Resources' and it includes a search bar and a user profile 'Jaikishan Yadav'. The page content is divided into 'Sources and destinations' and 'Destinations'. Under 'Destinations', 'Private Resource' is selected. The 'Private Resource' section shows a table with 5 Private Resources. The table has columns for Private Resource Group, Connection Method, Connector Groups, Accessed by, Rules, and Total Requests. The table shows three rows of data:

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

Accès sécurisé - Configuration des ressources privées

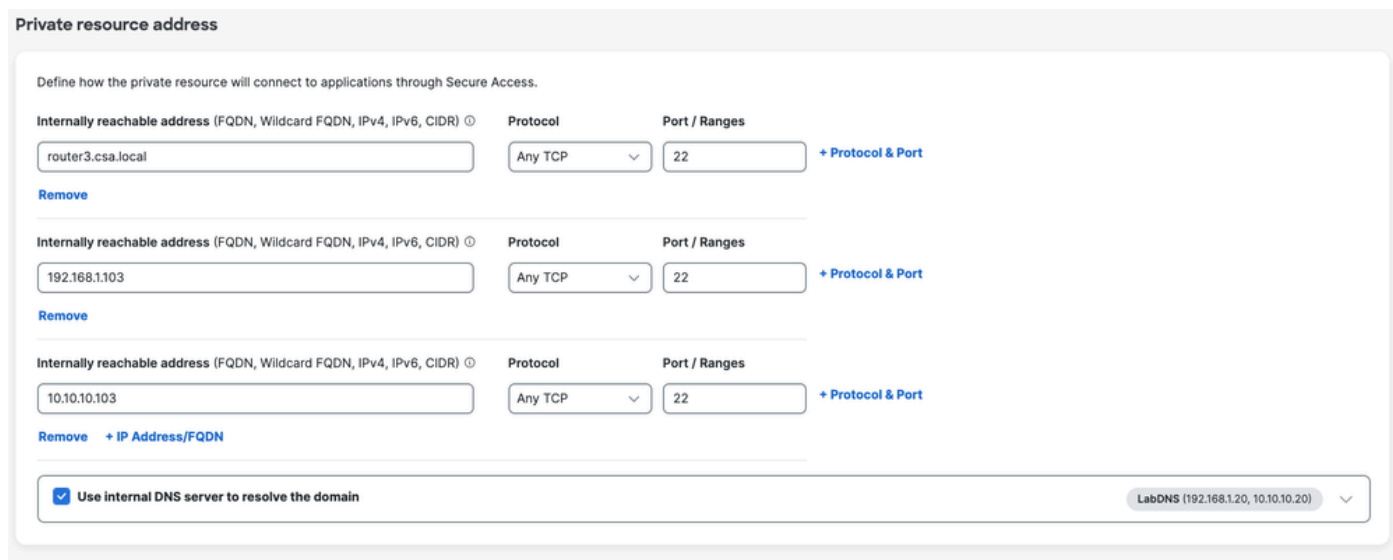
2. Dans le champ Nom de la ressource privée, entrez un nom significatif pour la ressource. Pour Description, nous vous recommandons de fournir des informations telles que l'objectif de la ressource ou le nom du propriétaire de la ressource.



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

Endpoint Connection Methods

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

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

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

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

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

FMC_FTD (ftd.csa.local) ✓
Will get enforced at the selected firewalls.

Local-only

Enforcement point for Remote User

Remote user — via Internet — Secure Access Cloud — Private Resource

Enforcement point for Local user

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

Cancel Save and Test Save

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).

Resource Connector Groups

Secure Access can forward Zero Trust Access traffic to this private resource using resource connectors. [Help](#)

For more information, see [Help](#)

Resource Connector Groups (optional) [?](#)

RC-ESXI x e.g. My Server Group

Choose a connector group in the same data center, branch office, or security zone as the resource. [?](#)

Accès sécurisé - Configuration des ressources privées



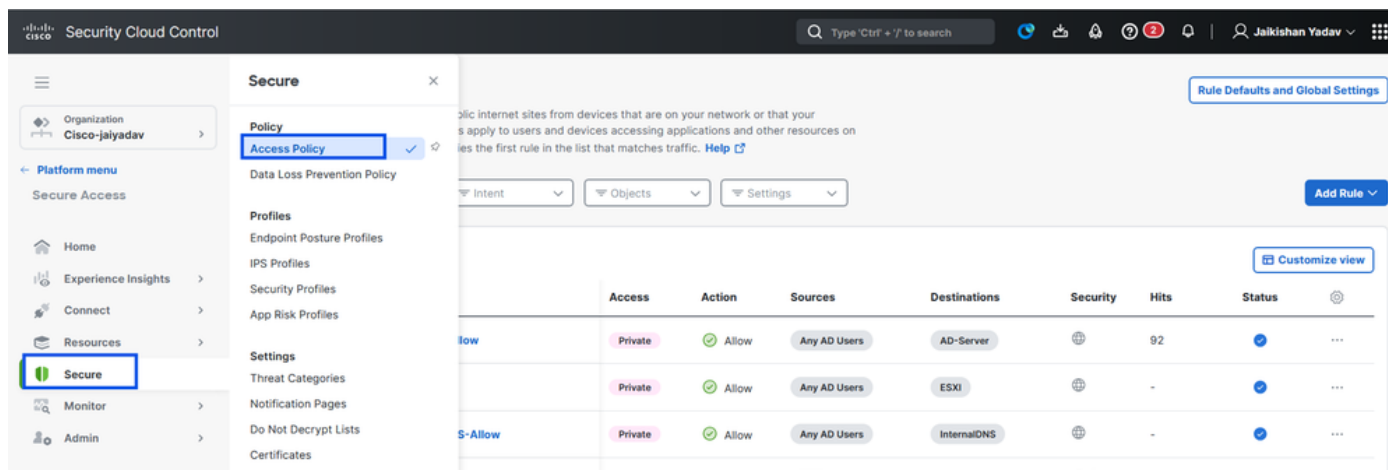
Remarque : Selon le type d'inscription sélectionné, cette modification associera automatiquement le PR au FTD et déclenchera un déploiement de stratégie

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](#)

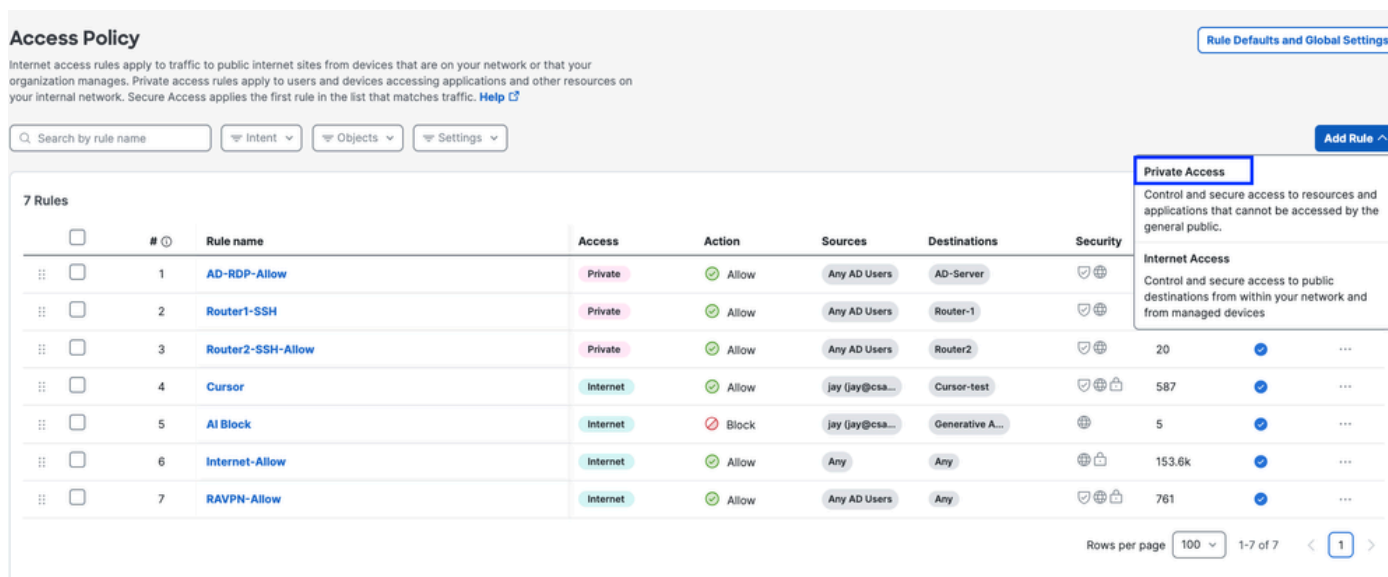
1. Accédez à Secure > Access Policy



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

Add Router3-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

Accès sécurisé - Configuration de la stratégie d'accès

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

Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources

AD Users • Any AD Users

To

Specify one or more destinations

Private Resources • Router3

+ AND

Accès sécurisé - Configuration de la stratégie d'accès

5. Configuration requise des terminaux

Endpoint Requirements

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

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

For Branch connections:

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

User Authentication Requirements

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

2 Configure Security

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

Cancel

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

Accès sécurisé - Configuration de la stratégie d'accès

6. Configurer la sécurité

Specify Access

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

2 Configure Security

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

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

Security Profile

[Rule Defaults](#)

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

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

Cancel

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

Accès sécurisé - Configuration de la stratégie d'accès

7. Cliquez sur Enregistrer

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

8 Rules Customize view

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

Rows per page 100 1-8 of 8 1

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

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

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

The screenshot displays the Palo Alto Networks management console. On the left, the 'Network Connections' section shows '1 Syncing' and '0 Synced' FTDs. A notification states 'Configuration changes are being processed'. Below is a table of FTDs:

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

On the right, the 'FMC_FTD' details panel shows 'Firewall Details' (Device FQDN: ftd.csa.local), 'UZTA Configuration status' (Syncing, last synced at 23 Feb 2026), and 'Assigned Trusted Network' (LAN). The 'Associated Resources' section shows 3 resources associated by status (Synced).

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

Resources associated with FMC_FTD

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

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

Resource name	Status
Router-1	✓ Synced
Router2	✓ Synced
Router3	✓ Synced

Close

Accès sécurisé - Vérification PR

- 3. Cliquez sur Fermer
- 4. Vérifiez l'état , la ressource associée et la configuration doivent être à l'état Synchronisé

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources (3)

RESOURCES ASSOCIATED BY STATUS

Status: **Synced** (3)

View resources associated to this FTD

Associate Resources

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

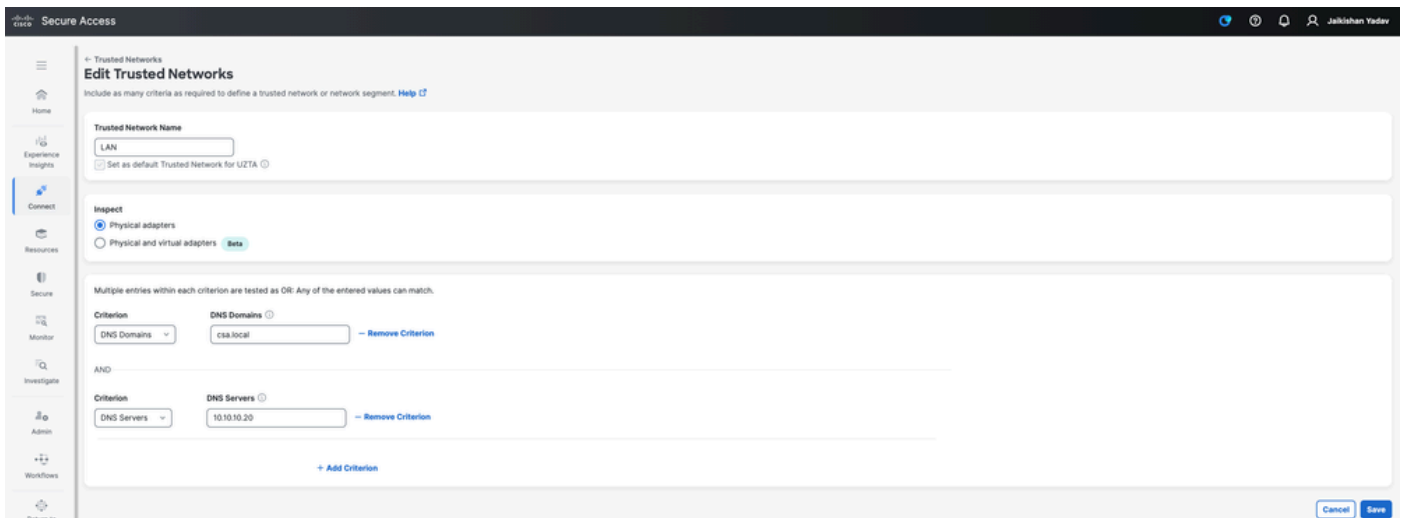
show running-config object application

```
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 »

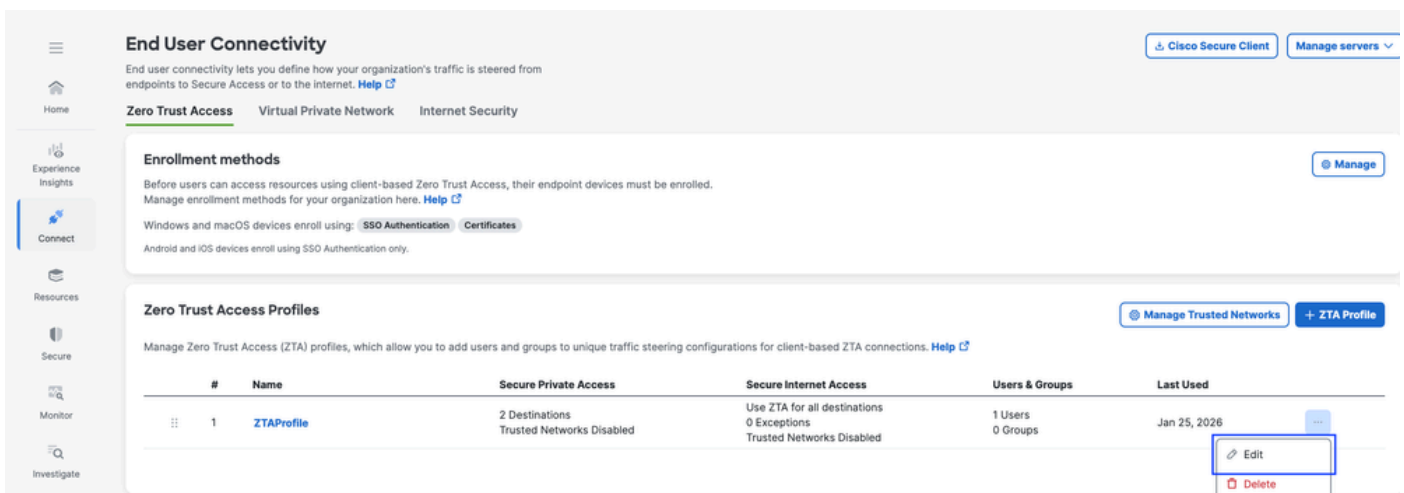
Naviguez jusqu'à Connect > End User Connectivity > Zero Trust Access > ZTA Settings et configurez Trusted Networks



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

The screenshot shows the 'Create profile' page for a Zero Trust Access (ZTA) profile. The profile name is 'ZTAProfile' and the priority is '1. Current profile'. The traffic steering limits are set to 5k for iOS, 10k for Android, and 100k for macOS/Windows. The 'Secure Private Access' section is active, showing a table of destinations and private resources. A tooltip is visible over the table, explaining the difference between 'Private Resource' and 'Add Destination'.

Destinations & Private Resources	Destinations	Modified
<input checked="" type="checkbox"/> *.zpc.sse.cisco.test	1	Feb 22, 2023

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

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

Accès sécurisé - Profil ZTA

The screenshot shows the 'Edit profile' page for a Zero Trust Access (ZTA) profile. A modal window titled 'Add private resources' is open, allowing the user to select private resources for the profile. The modal lists several resources, including 'AD-Server', 'DNS-Mgmt', and 'Router2', which are currently selected.

Add private resources
Select private resources that are configured for client-based Zero Trust Access. You can add up to 100 private resources at a time.

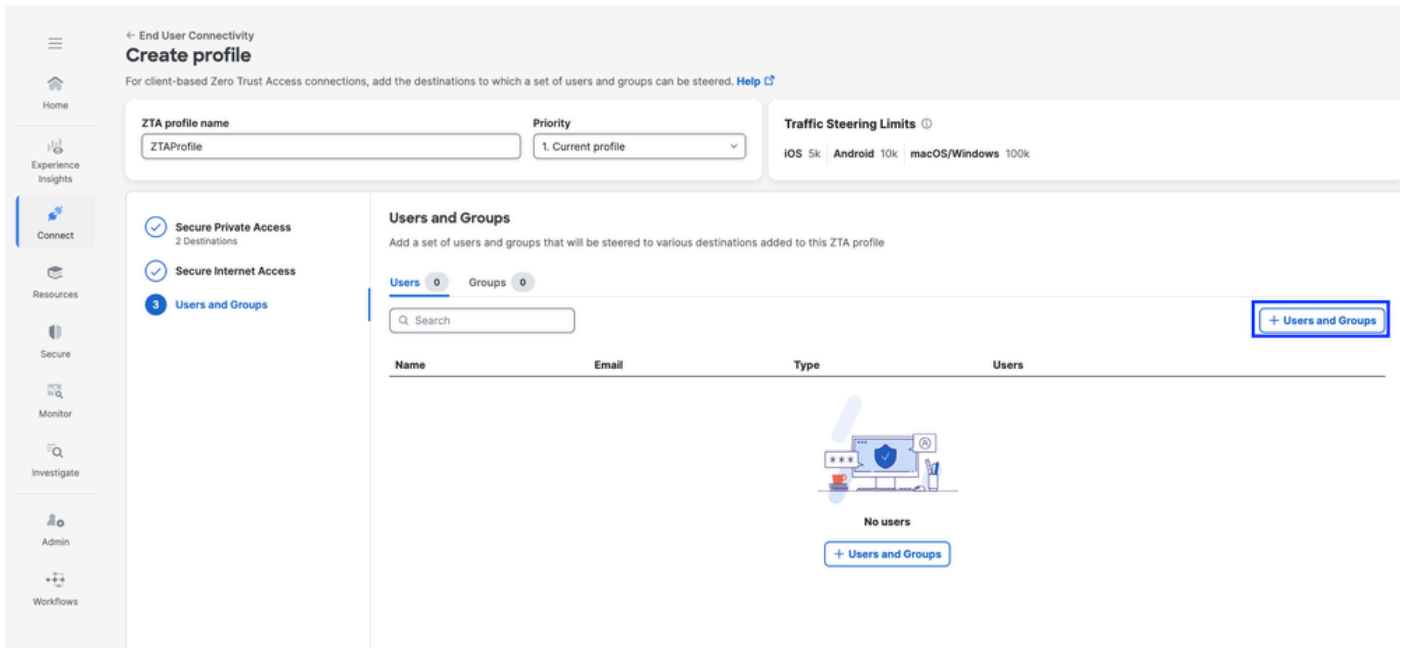
Private Resource

- LAB-InsideNetwork (10.10.10.0/24, taclab.com)
- InternalDNS (10.10.10.20, 192.168.1.20)
- AD-Server (10.10.10.20, ad.csa.local)
- LAB Management (192.168.1.0/24)
- DNS-Mgmt (192.168.1.20/32)
- Router2 (10.10.10.102, router2.csa.local)
- Router-1 (10.10.10.101, router1.csa.local)
- Router3 (10.10.10.103, 192.168.1.103, router3.csa.local)

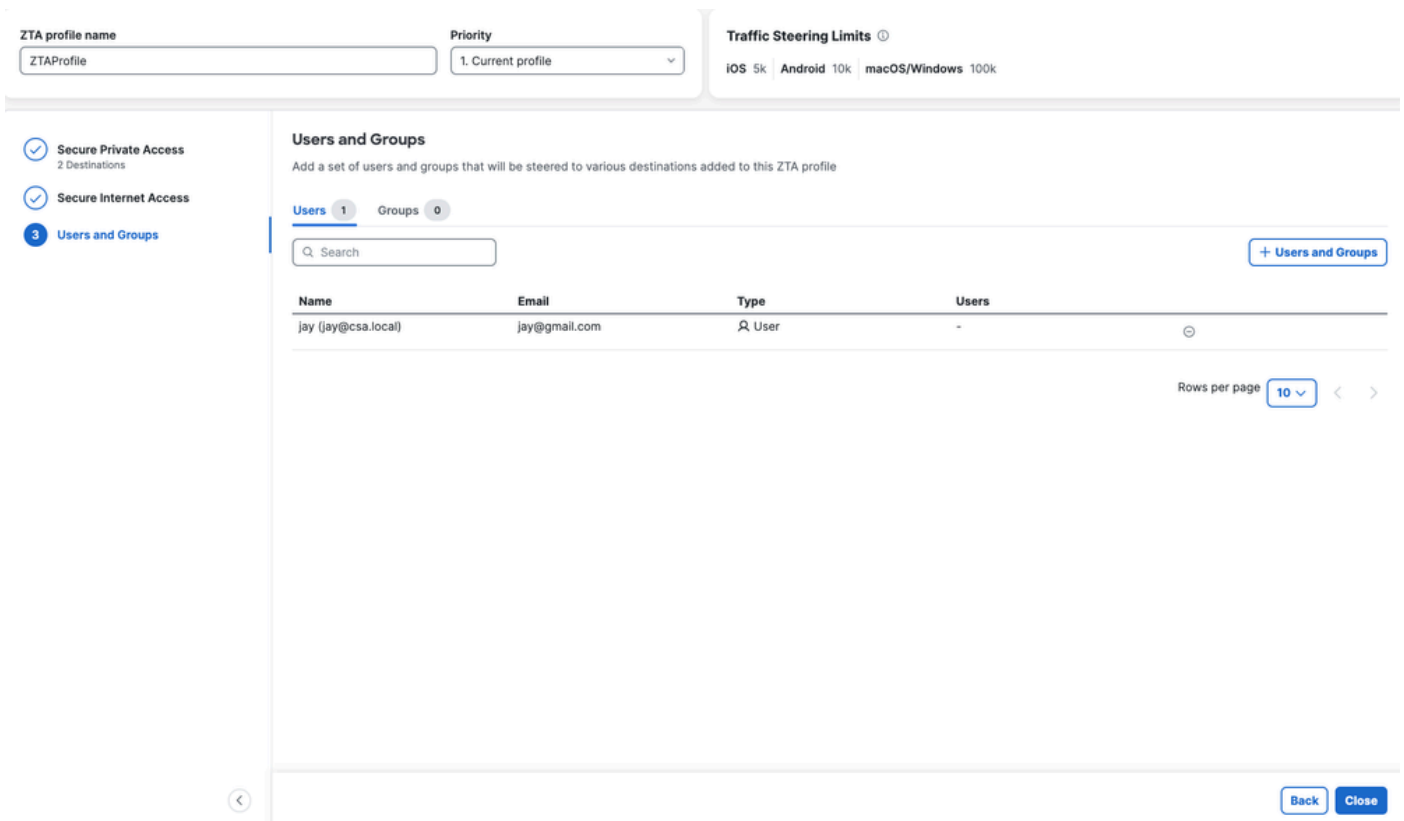
Cancel Save

Accès sécurisé - Profil ZTA

3. Ajouter des utilisateurs et des groupes



Accès sécurisé - Profil ZTA

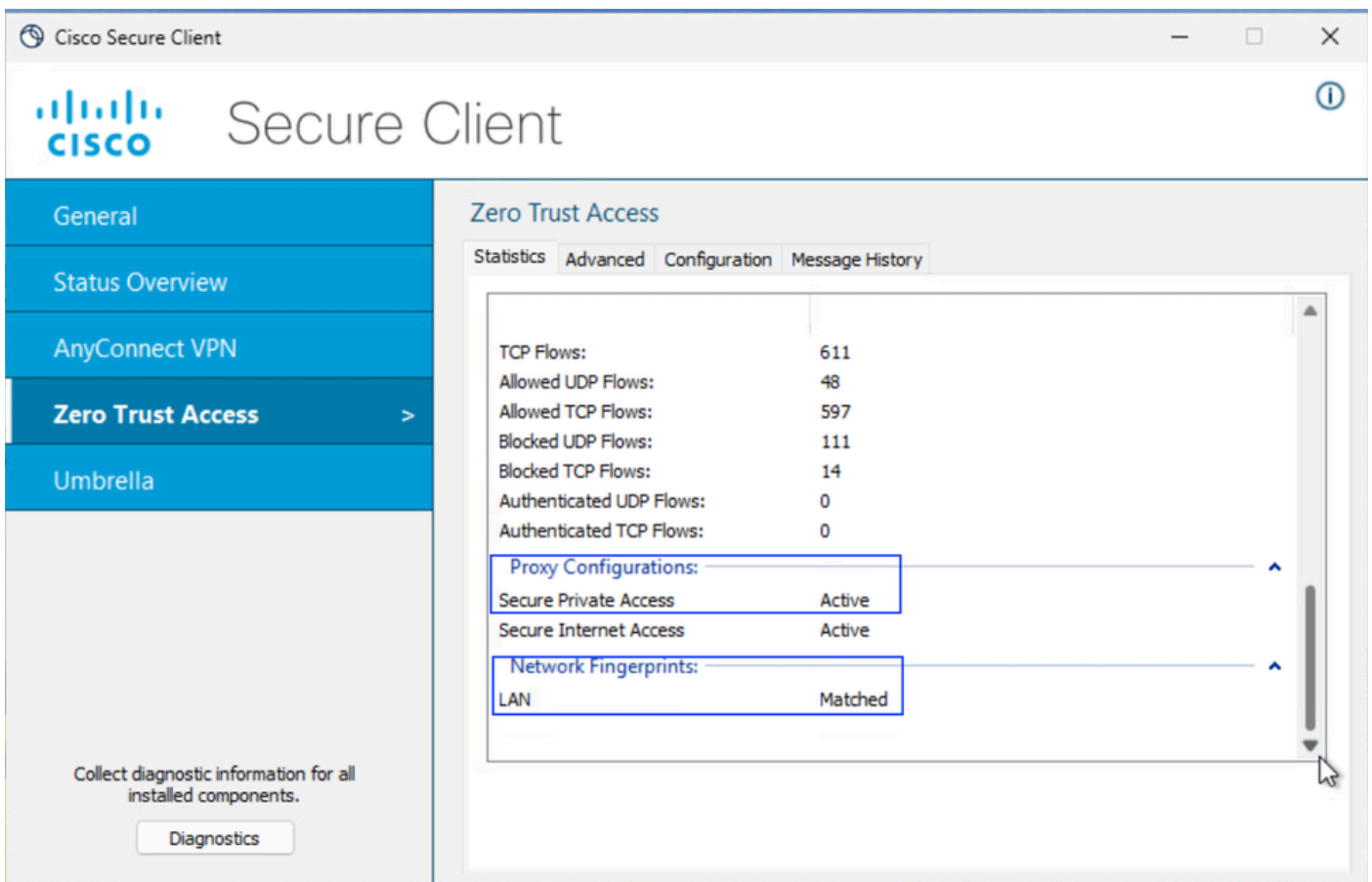


Accès sécurisé - Profil ZTA

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

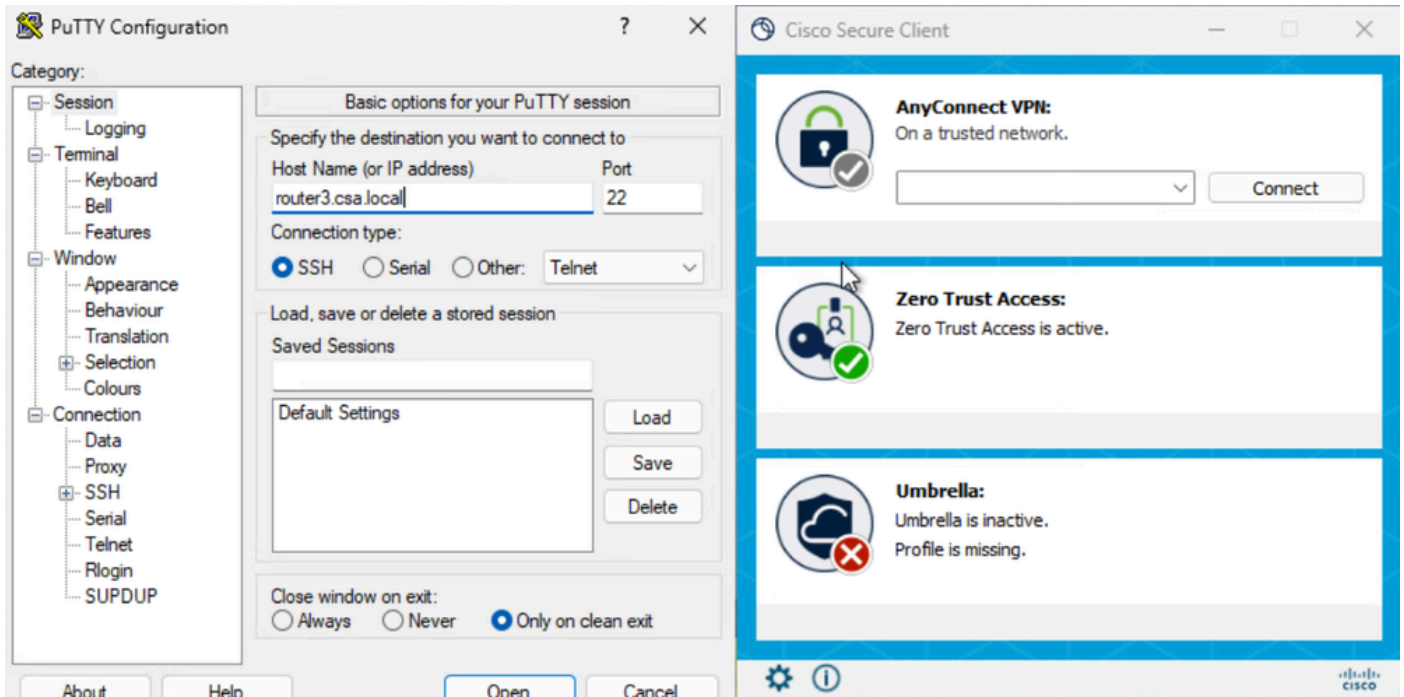
3. Vérifiez que FTD peut atteindre une ressource privée à l'aide du nom de domaine complet

```
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# █
```

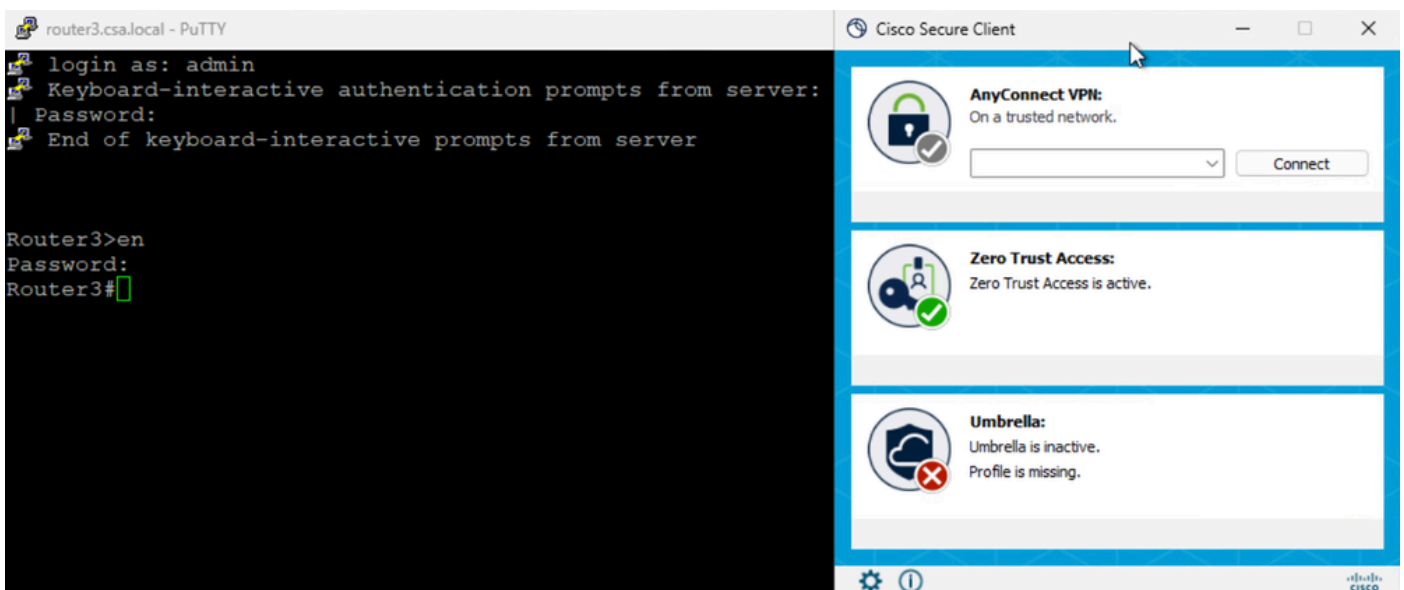
Accès sécurisé - Test PR

4. Tester la connexion SSH à la ressource privée

Accéder au RP à l'aide du FQDN

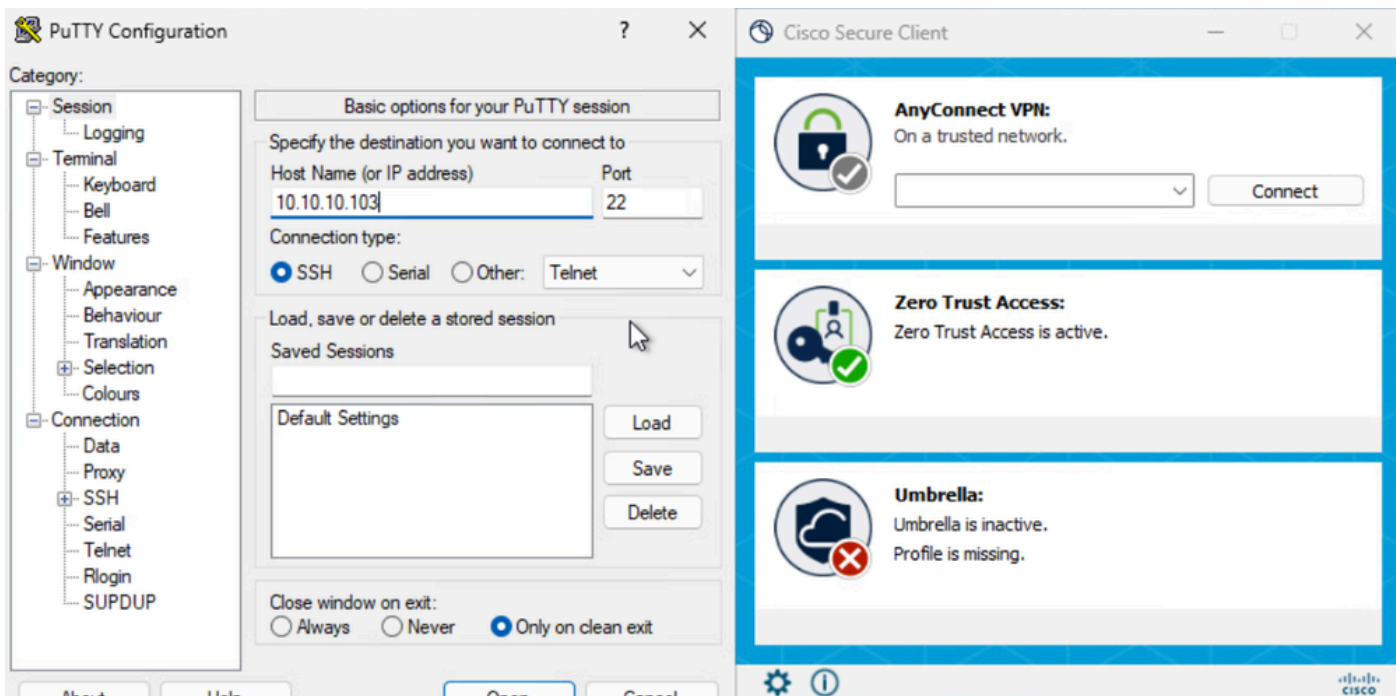


Accès sécurisé - Test PR

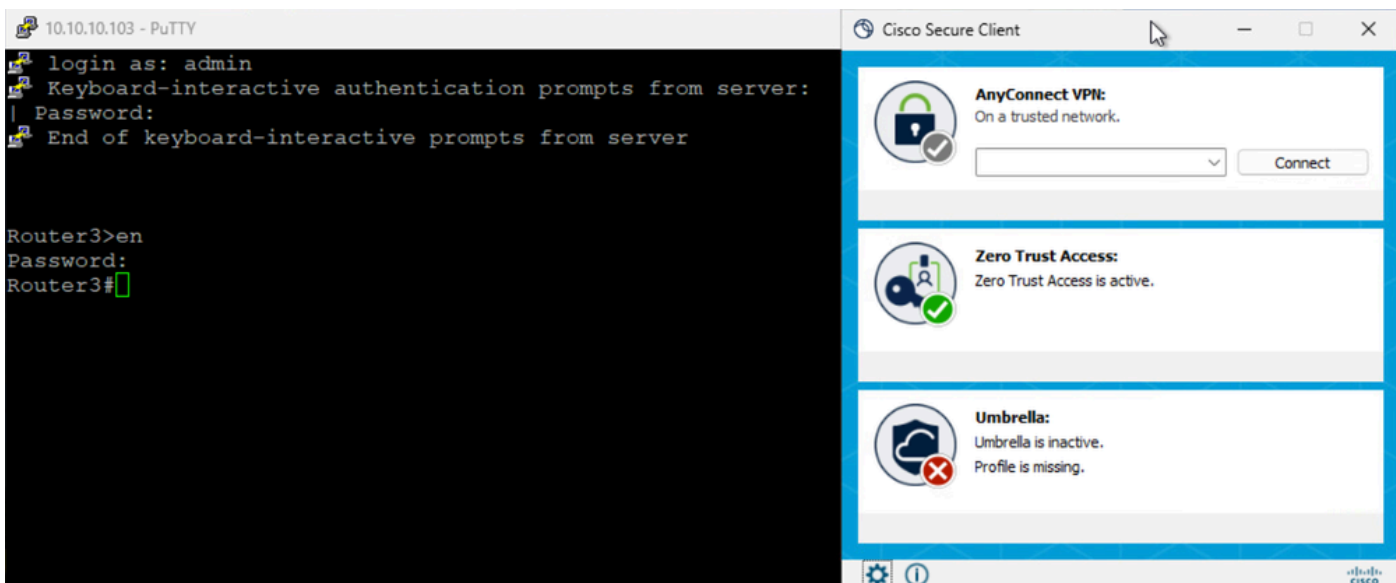


Accès sécurisé - Test PR

Accéder au RP en utilisant l'adresse IP



Accès sécurisé - Test PR

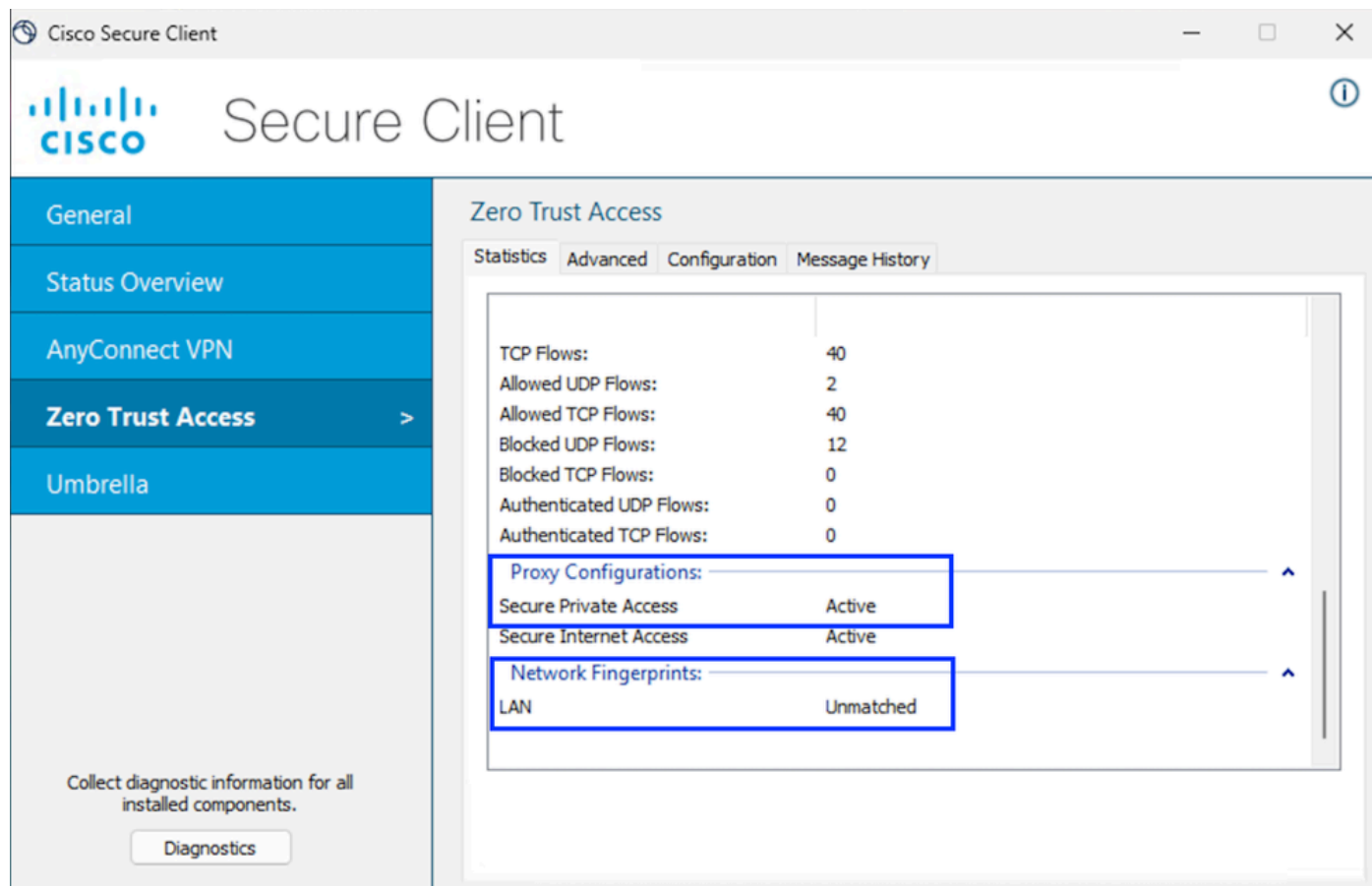


Accès sécurisé - Test PR

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

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

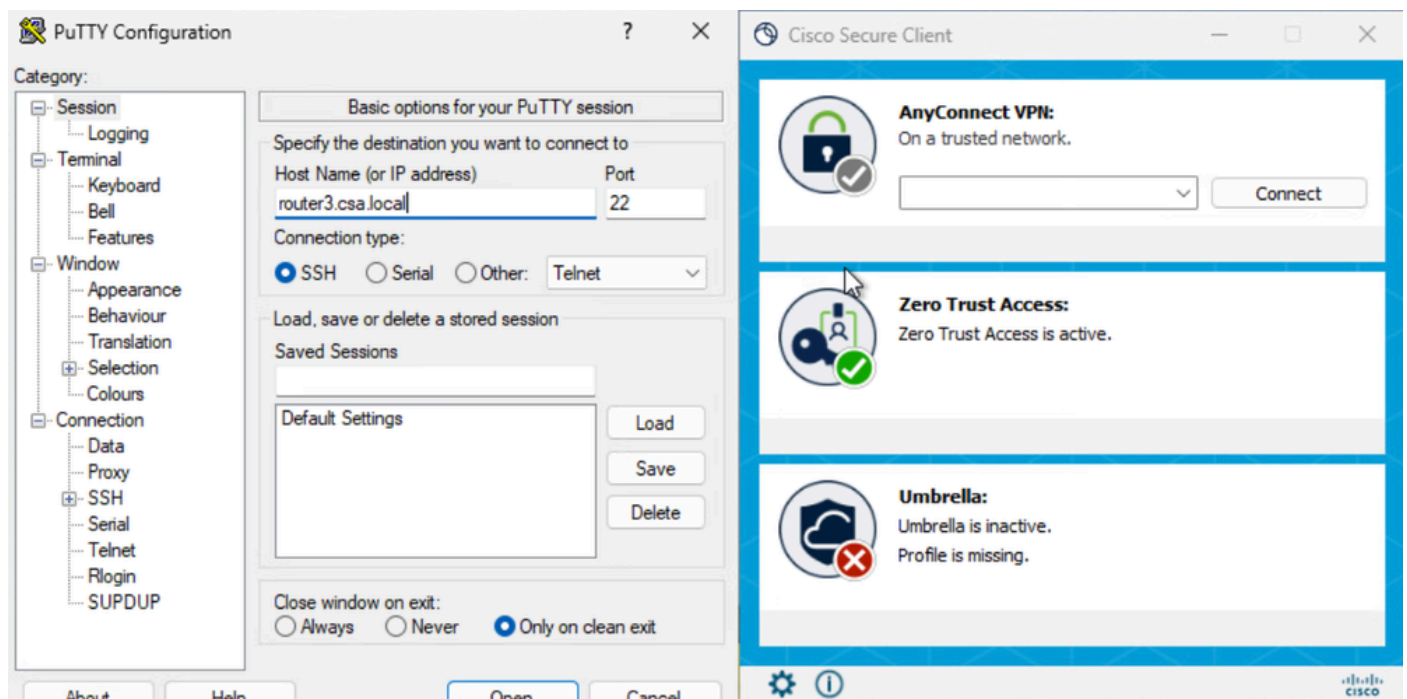
Name: ftd.csa.local
Addresses: 192.168.1.12

```

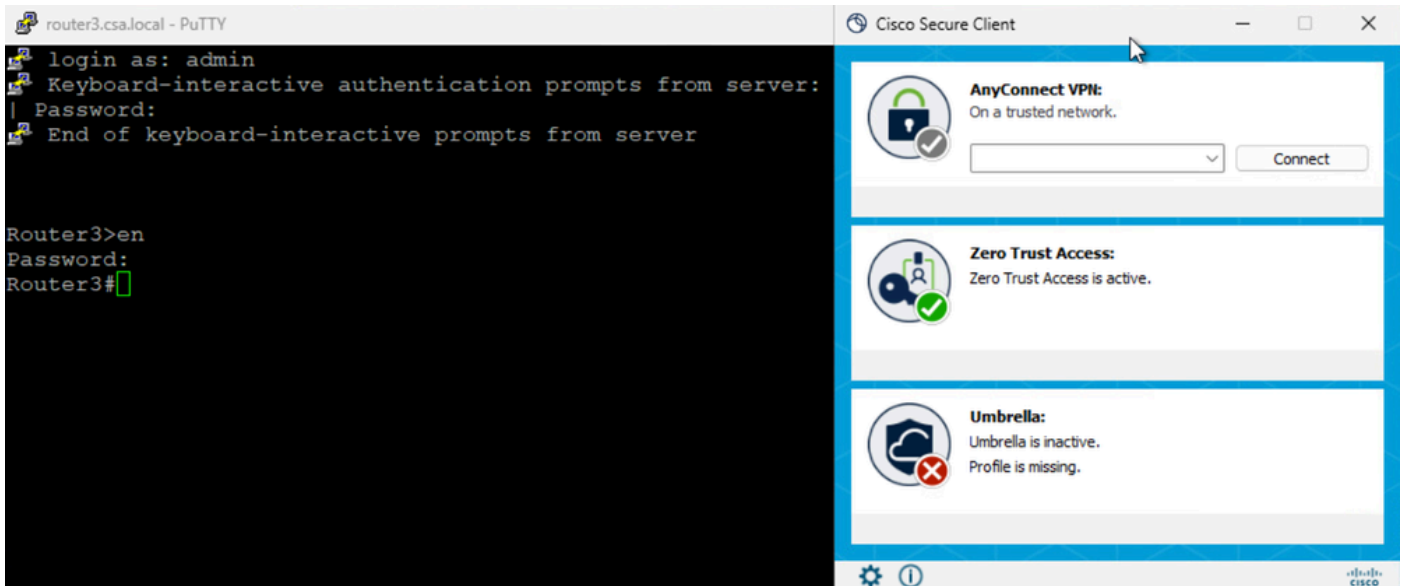
Accès sécurisé - Test PR

3. Tester la connexion SSH à la ressource privée

Accéder au RP à l'aide du FQDN

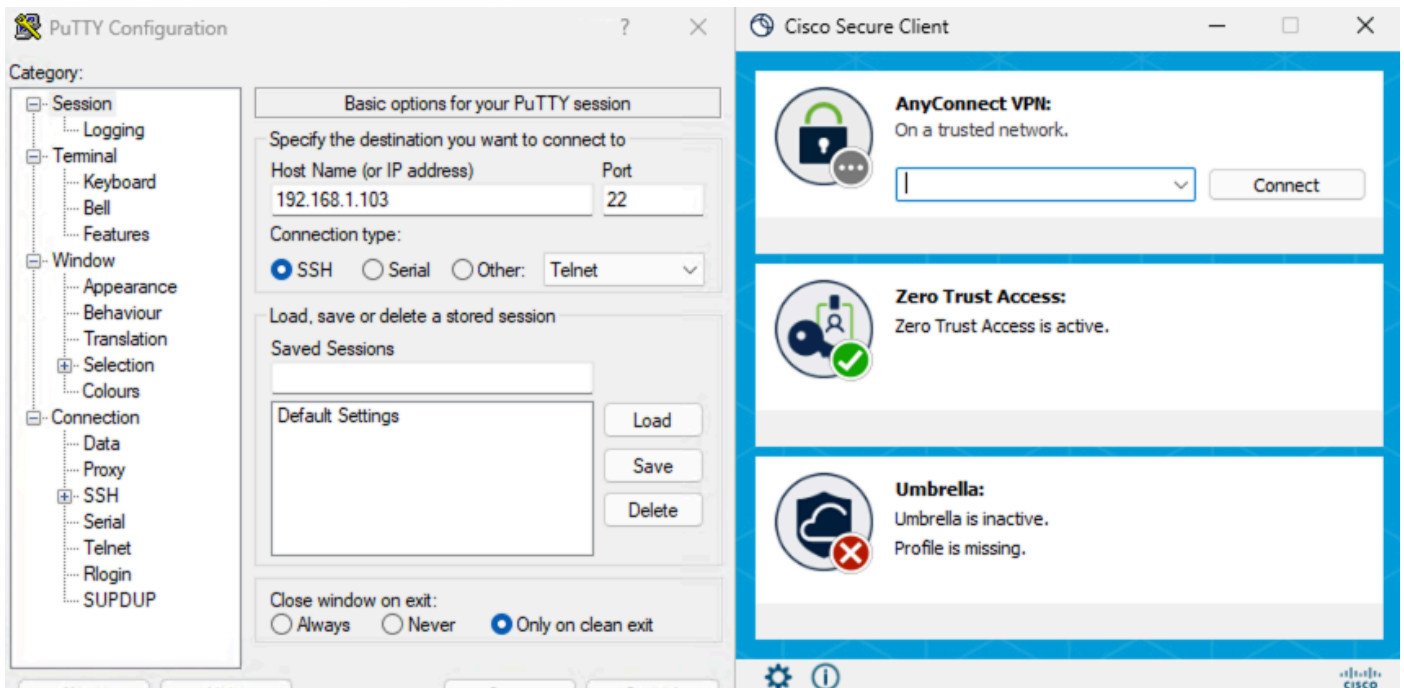


Accès sécurisé - Test PR

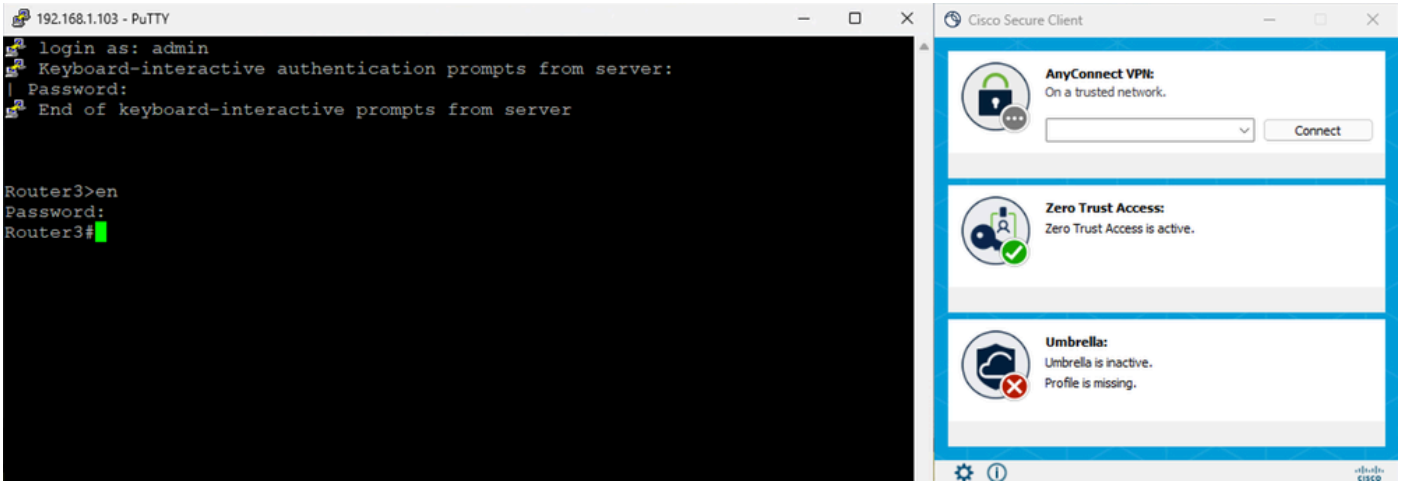


Accès sécurisé - Test PR

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

Activity Search

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

RESPONSE: Allowed

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

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

Accès sécurisé - Recherche d'activité

Activity Search

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

RESPONSE: Allowed

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

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

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 7:30 AM

Access details

Identity: Jay (jay@csa.local)

ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: router3.csa.local

Destination IP: 192.168.1.103

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.