

セキュアアクセスでのプライベートリソースアクセス用のユニバーサルZTNAの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[ユニバーサルZTNAについて](#)

[ネットワーク検出](#)

[適用のタイプ](#)

[使用例](#)

[アーキテクチャコンポーネント](#)

[パケットフロー](#)

[設定](#)

[ネットワーク図](#)

[テストケース](#)

[テストケース1: リモートユーザー-クラウドの適用](#)

[テストケース2-リモートユーザー-ローカル強制](#)

[テストケース3: ローカルユーザー: ローカル適用](#)

[テストケース4: ローカルおよびリモートユーザー: TNDによるローカルまたはクラウドの適用](#)

[トラブルシューティング](#)

[便利なコマンド:](#)

はじめに

このドキュメントでは、さまざまなトラフィックパスを使用したユニバーサルZTNA経由のプライベートリソースアクセス(PRA)の設定について説明します。

前提条件

ユニバーサルZTNAを設定する前に、次の設定を完了する必要があります

- [Cisco Secure Access上のアイデンティティプロバイダー](#)
- [証明書を使用したゼロトラストアクセスへのデバイスの登録](#)
- [Cisco Secure Firewallを使用したトンネルの設定](#)

- [リモートアクセス仮想プライベートネットワーク](#)
- [セキュアアクセス上のリソースコネクタ](#)
- [セキュリティクラウド制御のFTDオンボーディング](#)
- ハイブリッドZTNA機能フラグを各セキュアアクセステナント(SA)に対して有効にする必要があります。フラグを有効にするには、Cisco TACに連絡してください

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Accessおよびファイアウォールの脅威防御におけるIPsec VPNの設定
- Identity Provide(IdP):Active Directoryからのユーザプロビジョニング
- Cisco Secure AccessでのリモートVPNの設定
- Cisco Secure Accessでのリソースコネクタの展開
- ZTA証明書ベースの登録
- 証明書 : OpenSSL、CSR生成、証明書テンプレートなど

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Threat Defense (バージョン7.7.10)
- Cisco Secure Firepower Management Center (バージョン7.7.10)
- Cisco Secure Client (ZTAバージョン5.1.10.1720)
- Windows 11
- Windows 2019 Server – 証明機関
- ESXi上のリソースコネクタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

ユニバーサルZTNAについて

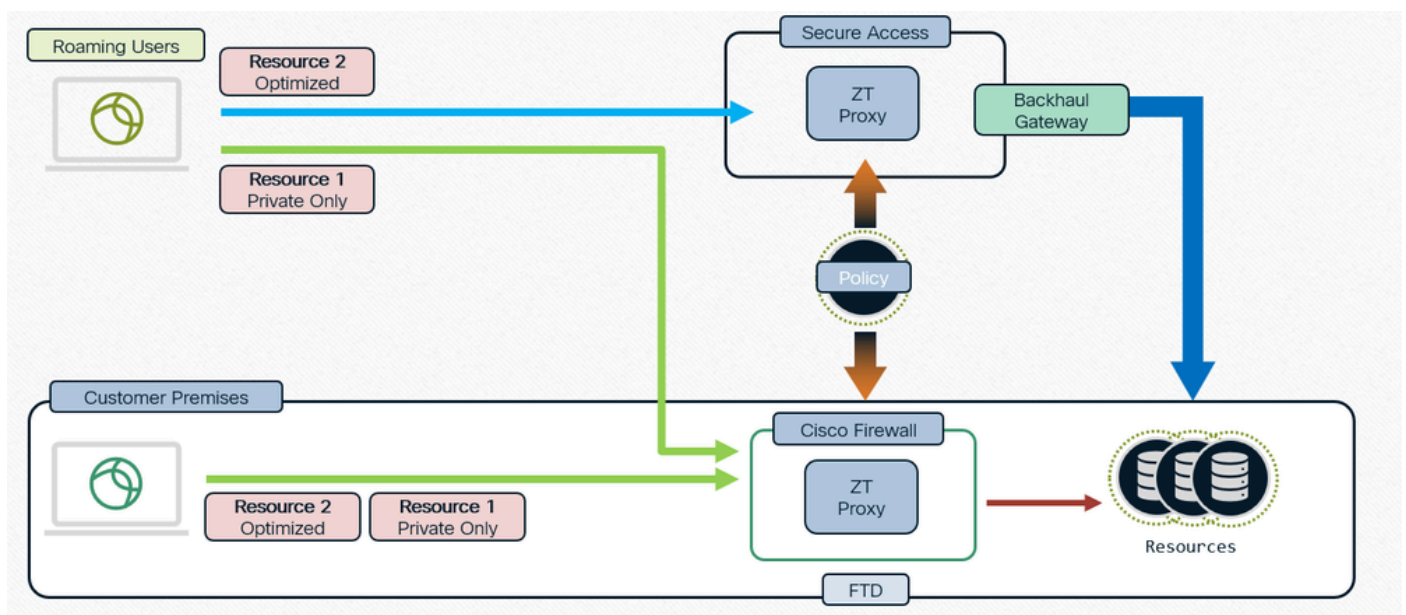
Universal zero trust network access(uZTNA)により、管理者はユーザID(ユーザの信頼とポスチャを含む)に従って、RA-VPNのようにネットワーク全体へのアクセスを許可することなく、内

部ネットワークリソースへのアクセスを特別に許可できます。uZTNAにより、管理者はリモートユーザとオンプレミスユーザの両方に対して内部リソースとアプリケーションを保護できます。

uZTNAは、あるアプリケーションに付与されたアクセスが暗黙的に他のアプリケーションへのアクセスを許可しているとは考えないため、ネットワーク攻撃を受ける可能性が低くなります。

セキュアアクセスでは、アクセスポリシーが評価されます。Secure Firewall Management Centerからデバイスに導入されたアクセスコントロールポリシーはすべて無視されます。

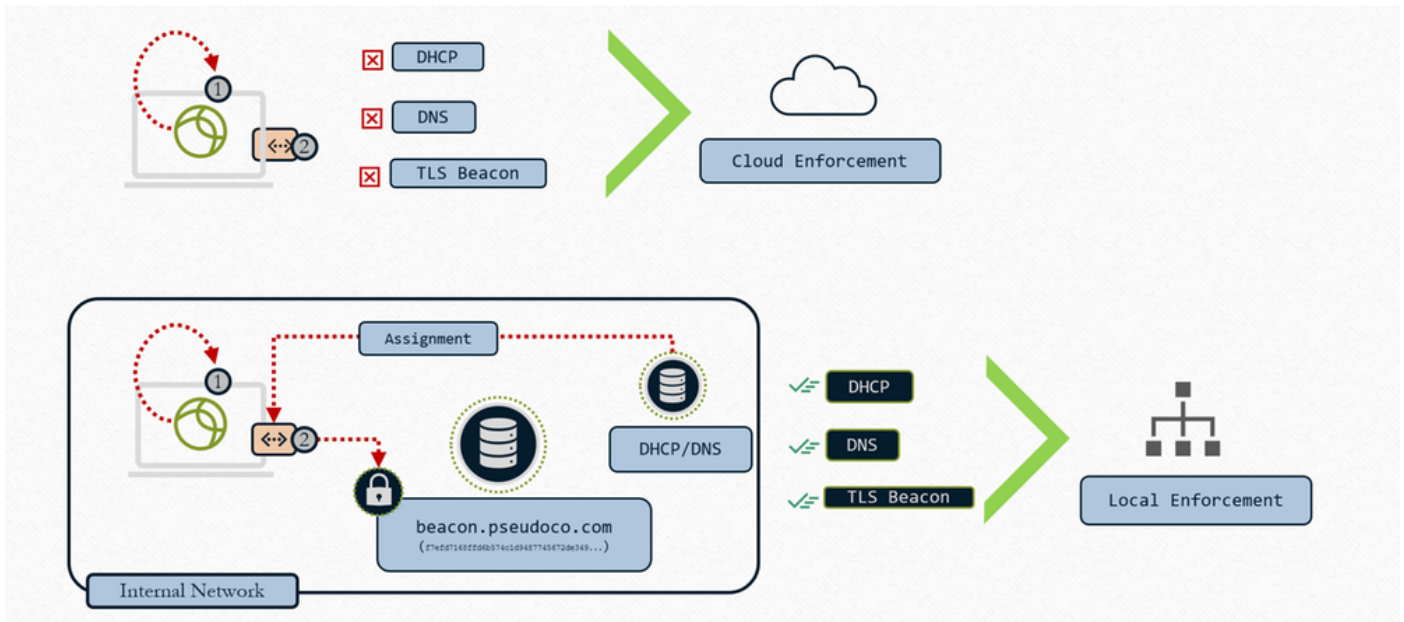
トラフィックプロキシと、IPS、ファイル、およびマルウェアのポリシー適用は、Firepower Threat Defense(FTD)で実行されます。



ポリシーの一元化、適用の分散化

ネットワーク検出

クラウドまたはローカルの適用の決定



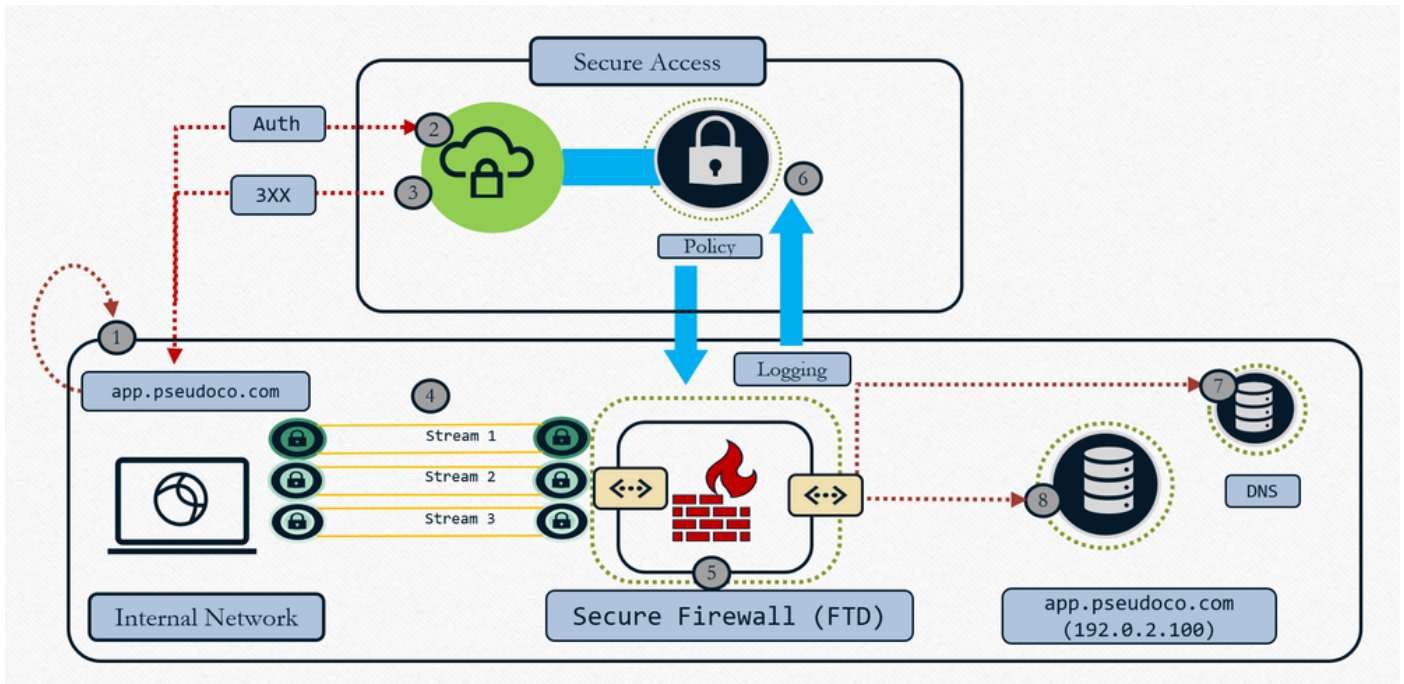
Universal ZTNA : クラウドまたはローカルの適用の決定

- 1 : クライアントがローカルインターフェイスにネットワーク設定を問い合わせる
- 2 : クライアントによるTLSビーコンの検索
- 3 - 条件が一致した場合 - ローカル強制
- 4 - 条件が一致しない場合 - クラウドの適用

リソースを「クラウドまたはローカルの適用」で設定し、TNDルールをFTDに関連付けると（デフォルト）、実際に実行されるのは、クライアントに送信されるインターセプトルールのセットにTNDルール評価が含まれることです。したがって、そのクライアントはTNDルールを評価するようにクラウドによって指示されます。接続を送信する際に、そのTND（ネットワークのフィンガープリントの評価）の結果をHTTPヘッダーに入力します。これにより、ユーザがオンプレミスなのか信頼できないネットワークなのかをプロキシに通知し、プロキシはその情報を使用して、トラフィックを適切にリダイレクトします。フィンガープリントが一致した場合（一致した場合）、ZproxyはクライアントにトラフィックをFTDにリダイレクトするよう指示し、一致しない場合はトラフィックをクラウドにリダイレクトします。『[信頼できるネットワーク検出によるゼロトラストネットワークアクセスの設定](#)』を参照してください。

適用のタイプ

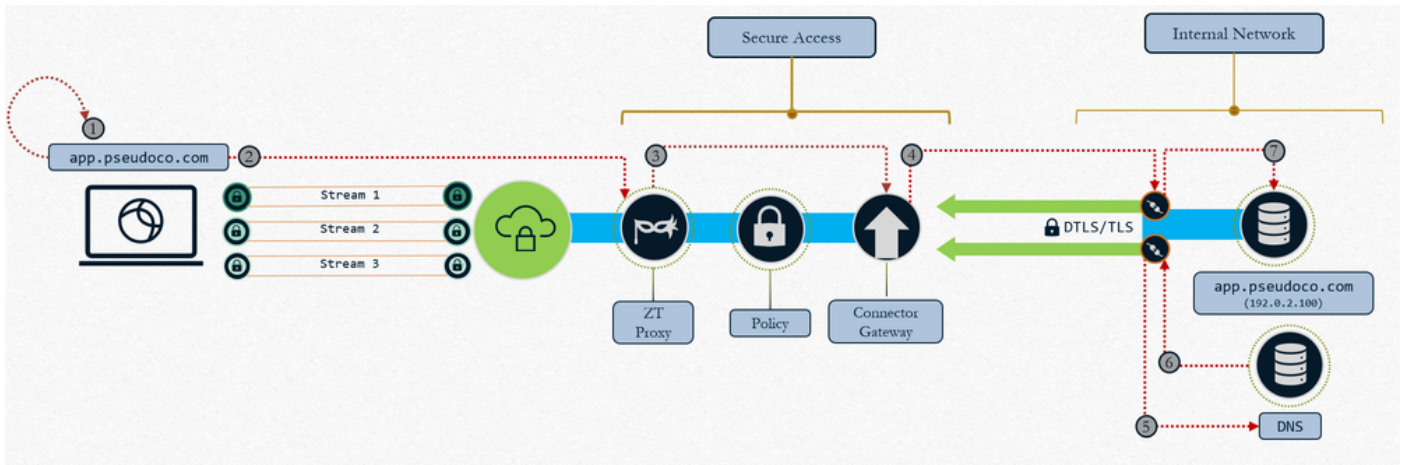
- ローカル強制パス : ファイアウォールの強制



ユニバーサルZTNA - ローカル適用

1. ユーザーがアプリケーションを要求、クライアントが要求をキャプチャし、一時的な IP (localhostの範囲) に解決
2. 認証制御トラフィックは、ポリシー評価のためにSecure Access Cloudに送信されます。
3. クラウドがFTDにリダイレクトしてデータプランを適用 (ポリシーで許可されている場合)
4. トラフィックはファイアウォールで設定されたヘッドエンド (インターフェイス) に転送される
5. クラウドで定義されたポリシーは、ローカルプロキシデータプレーンを使用して適用 (IPS、マルウェア、復号化)
6. イベントが記録され、重複データがクラウドに送信されて一貫したレポートが作成される
7. ファイアウォールは、ローカルネットワークでDNS解決を行い、リソーストラフィックをルーティングします (許可されている場合) 。
8. ファイアウォールがTCPプロキシとして動作すると、ファイアウォールはリソースへの接続 (新しいリソースへの接続) を確立します

- クラウド適用パス : オフネットワーク

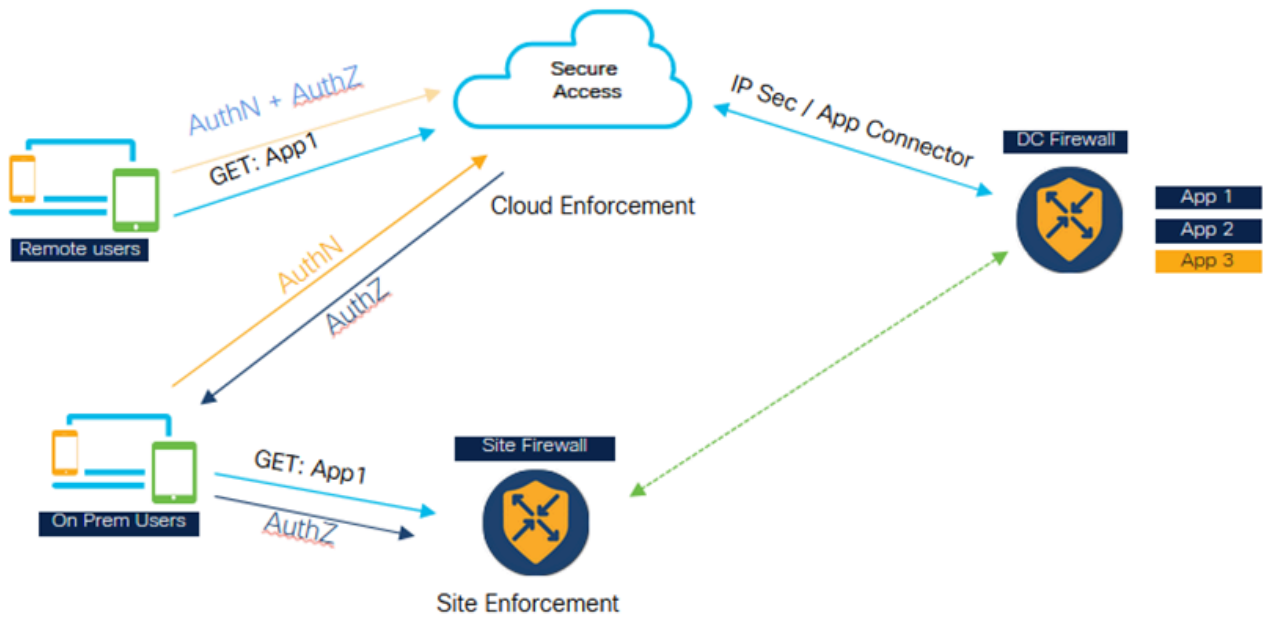


Universal ZTNA : クラウドの適用

1. ユーザがアプリケーションを要求、クライアントが要求をキャプチャし、一時的な IP (localhostの範囲) に解決
2. トラフィックは、セキュアアクセスのゼロトラストプロキシに転送される
3. TCP接続がプロキシされ、マッピングされたリソースコネクタに構築されます。ポリシーはトラフィックに適用されます。
4. ゲートウェイがリソースコネクタへの接続を確立
5. リソースコネクタはリソースIPを解決します
6. ローカルDNSがリソースIPで応答する
7. リソースコネクタがリソースへの接続を確立

使用例

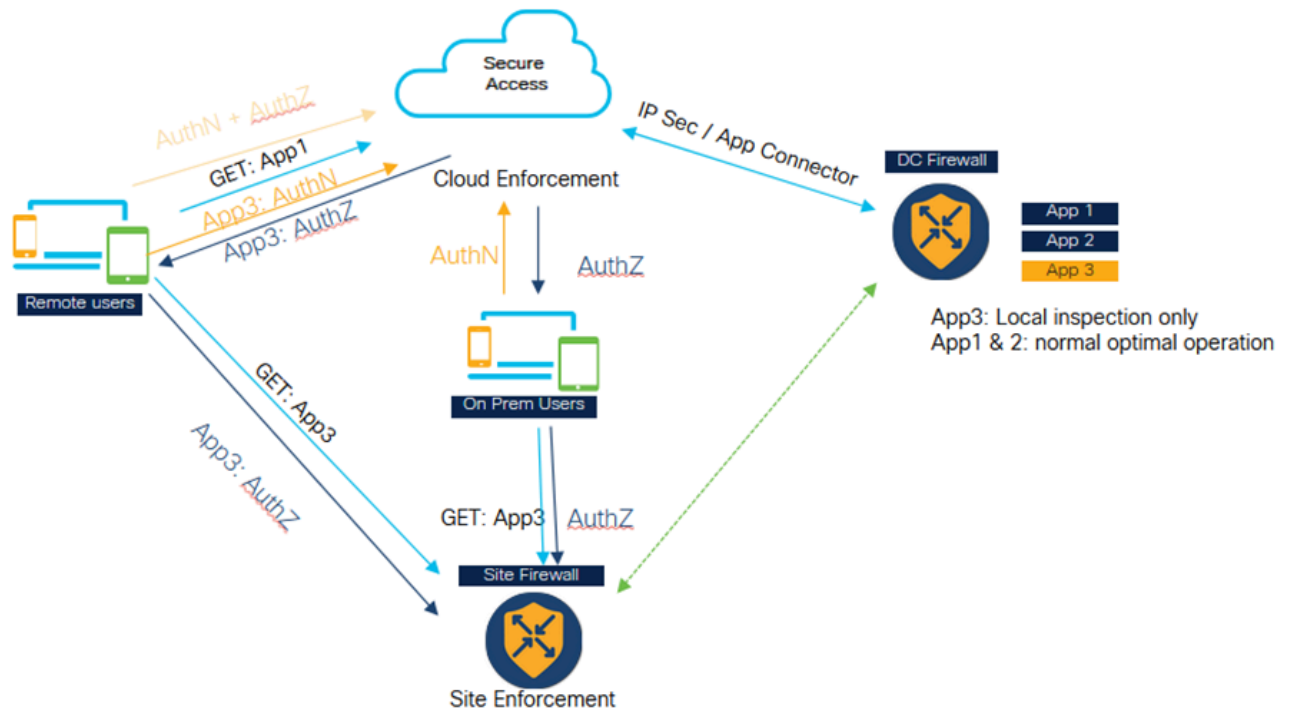
ケース1 : オンプレミス時の一貫した最適化されたユーザ向けZTNA



Universal ZTNA – 一貫性があり最適化されたZTNA (オンプレミスユーザ)

- セキュアアクセスとファイアウォールはどちらも、アプリケーションを保護するように設定されています。
- ユーザがリモートの場合、ポリシーの評価と検査のためにSecure Accessにアクセスします。
- ユーザが内部/オンプレミスの場合、ファイアウォールでプライベートトラフィックの検査を行います。
- オンプレミスのユーザは、Datapathトラフィックがファイアウォールに送信され、ポリシー設定に従って検査されるだけで、引き続きSecureにアクセスして認証と評価を行うことができます。
- ファイアウォール経由でアプリケーションにアクセスする内部ユーザは、トラフィックがクラウドに送信されてからデータセンターにバックホールされるのを回避できるため、パフォーマンス面で有利です。

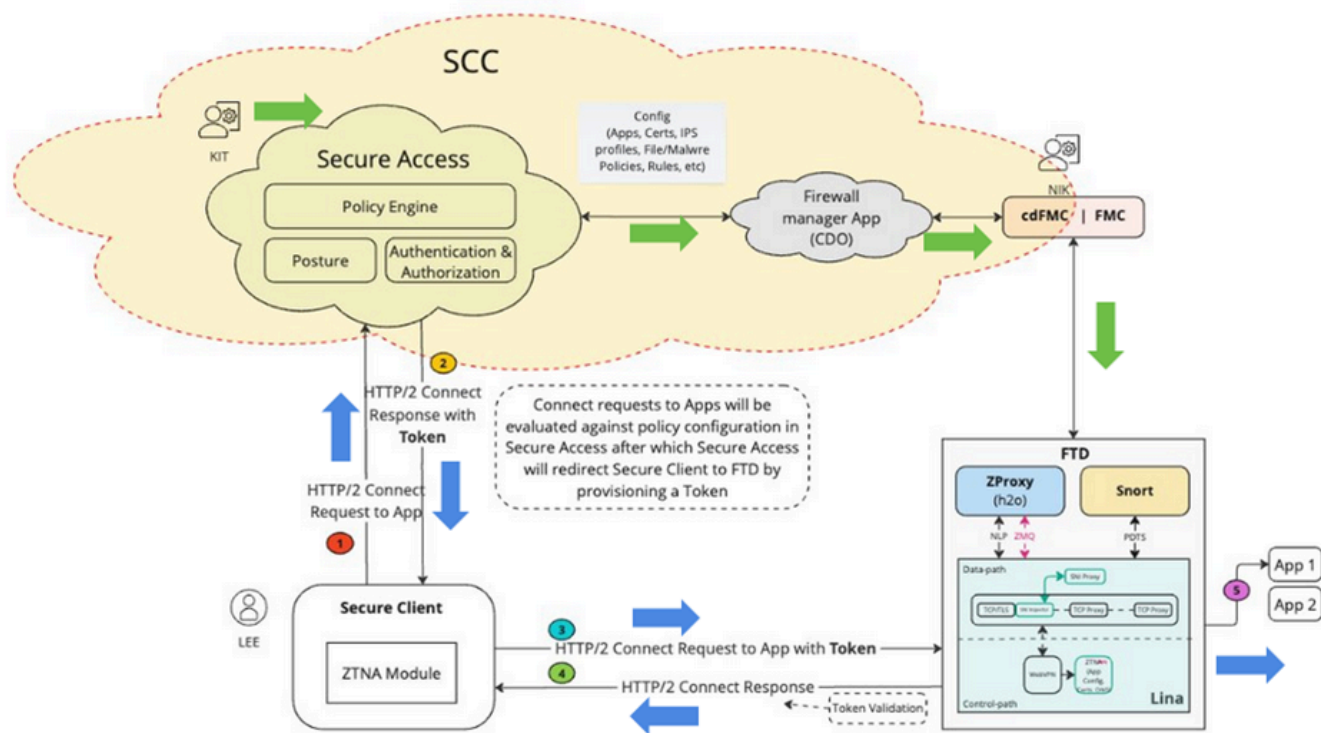
ケース2：機密アプリケーションの私的検査



Universal ZTNA : 機密アプリケーションのプライベート検査

- 特定の重要なアプリケーションは、ファイアウォールを介して常にアクセスされるように設定できます。
- アプリケーションのデータトラフィックはクラウドに送信される必要はありません。たとえば、ソースコードのような機密性の高いデータアプリケーションがあり、顧客はこれをクラウドに移行したくないと考えています。
- このようなシナリオでは、リモートとオンプレマのユーザトラフィックの両方が常にファイアウォールを通過して検査されます。ただし、このシナリオでも、認証とポリシーの評価はクラウドで常に行われ、データ部のトラフィックのみがファイアウォールを通過します。

アーキテクチャコンポーネント



ユニバーサルZTA - アーキテクチャコンポーネント

Security Cloud Control(SCC)は、uZTNAソリューションのプライマリマネージャです。uZTNAは、SCC上に構築される最初の機能です。

SCCには、2つのマイクロアプリケーションSecure AccessとFirewallがあります。SCCがプロビジョニングされ、必要な機能フラグが有効になると、SCCパネルの左側にこれらのマイクロアプリケーションが表示されるようになります。

セキュアクライアント：セキュアクライアントでは、ゼロトラストアクセスモジュール(ZTNA)を有効にする必要があります。ZTNAモジュールに登録して、アプリケーションにアクセスできるようにする必要があります。

ファイアウォール脅威対策：これらのアプリケーションを保護するFTD。FTDはH2Oとも呼ばれるZTプロキシを実行します (Secure Access Cloudで実行されるプロキシと同じ)。

ユーザ (KITなど) がSecure Accessマイクロアプリケーションでプライベートリソースとポリシーを設定すると、この設定がSCCのFirewallマイクロアプリケーションにプッシュされます。ファイアウォールアプリケーションは、FTD(FTD)の内部、FTDの設定、FTDでの設定の導入方法と管理方法を理解しています。そのため、ファイアウォールアプリケーションはこの設定を検証し、FMC APIを起動して設定をFMCにプッシュし、最終的にFTDに展開します。FTDでは自動導入オプションを有効にできるため、管理者 (Nickなど) が手動で導入を行う必要はありません。

1. ユーザー（リーなど）がアプリケーションにアクセスしようとする時、セキュアクライアントはmTLSチャンネルを使用してセキュアアクセスに接続します。セキュアアクセスでは、クライアントデバイス証明書を使用してユーザを認証します。次に、そのユーザとそのアプリケーションに設定されている許可、ポスチャ、およびその他のポリシーを評価します。

2. セキュアアクセス(SSH)：アプリケーションがファイアウォールによって保護されていることが最終的に判明した場合、認証トークン(AUTH TOKEN)が生成され、ファイアウォールにはすでに認証および認可されていることが通知されます。認証トークンは暗号化され、セキュアアクセスによって署名されます

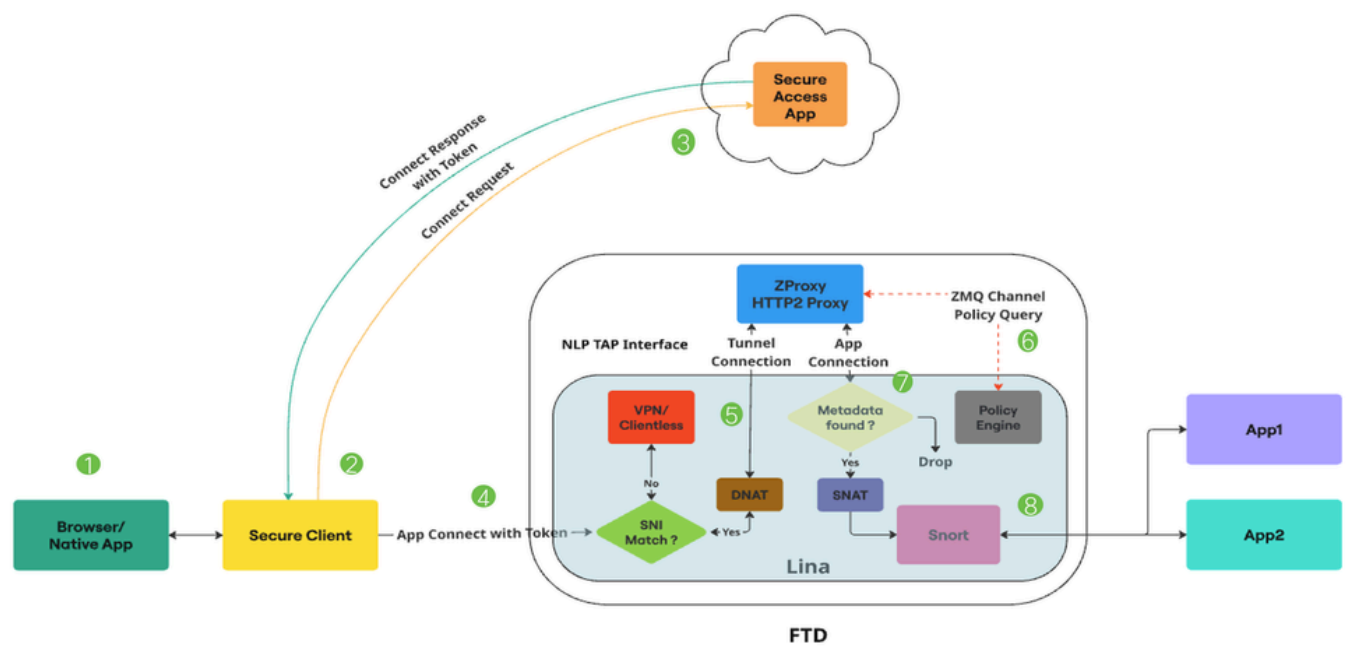
3. セキュアアクセスは、認証トークンとともにセキュアクライアントをFTDにリダイレクトします。

4. セキュアクライアントがFTDへの別の接続を確立します（これはmTLSチャンネルを介したHTTP2接続です）。アクセスされるアプリケーションのCONNECT要求をトークンとともに送信します。

5. FTDはトークンを検証します。トークンが正常に検証された場合、ユーザはそのアプリケーションにアクセスできます。次に、FTDは確認応答をセキュアクライアントに返信します

パケット フロー

ユニバーサルZTNA詳細パケットフロー



ユニバーサルZTA - パケットフロー

1. ユーザーがWebブラウザまたはネイティブ・アプリケーションを介してアプリケーションにアクセスしようとする。
2. セキュアクライアントは接続を代行受信し、プライベートリソースにアクセスしようとしているユーザとして識別します。
3. セキュアクライアントは、アプリケーションへのアクセスを要求して、セキュアアクセスへのmTLS接続を確立します。セキュアアクセスは、ユニバーサルZTNAポリシーとポストチャプロファイルのコンプライアンスを確認します。すべてが正しい場合、Secure Accessは、ユーザの詳細、アプリケーションの詳細、IPS/ファイルポリシーなどの重要な情報を含むアクセストークンを生成します。
4. アクセストークンは、セキュアアクセスによって暗号化され、署名されます。その後、セキュアアクセスはセキュアクライアントをトークンとともにFTDにリダイレクトします。
5. パケットがLina Datapathに到達すると、SNIチェッカーは接続を代行受信し、Client Helloのサーバ名 (SNI拡張子) がデバイスで設定されているプロキシFQDNに一致するかどうかを確認します。SNIが一致する場合、接続はZProxyに誘導されます。SNIが一致しない場合は、Universal ZTNAと共存できる他の機能に接続されます。

例：VPN、キャプティブポータル、クライアントレスZTNA HTTP/2プロトコルを介したMASQUEをサポートするZProxyは、専用コア上の非LinaプロセスとしてFTD上で実行されます。LinaとZProxy間の通信では、データトラフィックの処理にNLP Tap Interfaceを使用します。接続の宛先IPは、SNIチェッカーによってTAP interface IPに変換されます。

6. ZProxyがセキュアクライアントからmTLSトンネル接続を受信すると、セキュアクライアントから送信されたクライアントデバイス証明書を検証します。また、APP Connectで送信されたアクセストークンの検証も行います。LinaとZProxyの間にはゼロMQチャンネルがあります。主に制御メッセージの交換に使用されるZProxyはこのチャンネルを使用して、Linaと通信し、プライベートリソースのFQDN解決を行います。

ゼロMQチャンネルは、アクセストークン内に存在する情報をLinaに伝播するためにも使用されます。(例：ルールID、ポリシーIDなど) Linaは、アクセストークン情報を受け取り、それをメタデータデータベースに格納します。

7. 制御メッセージが交換されると、ZProxyはプライベートリソースへの新しい接続を開始します。これはTCPまたはUDPです。次に、Linaはこのアプリケーション接続に対してメタデータデータベースの検索を実行します。メタデータが見つからない場合、Connectionはドロップされます。
8. アプリケーション接続はZProxyから発信されるため、内部IP (例：169.251.1.2) が送信元IPになります。これは、FTD出カインターフェイスのIPに変換されてから送信されます。次に、Linaは、FileポリシーまたはIPSポリシーがアクセストークンに存在する場合にのみ、Snortインス

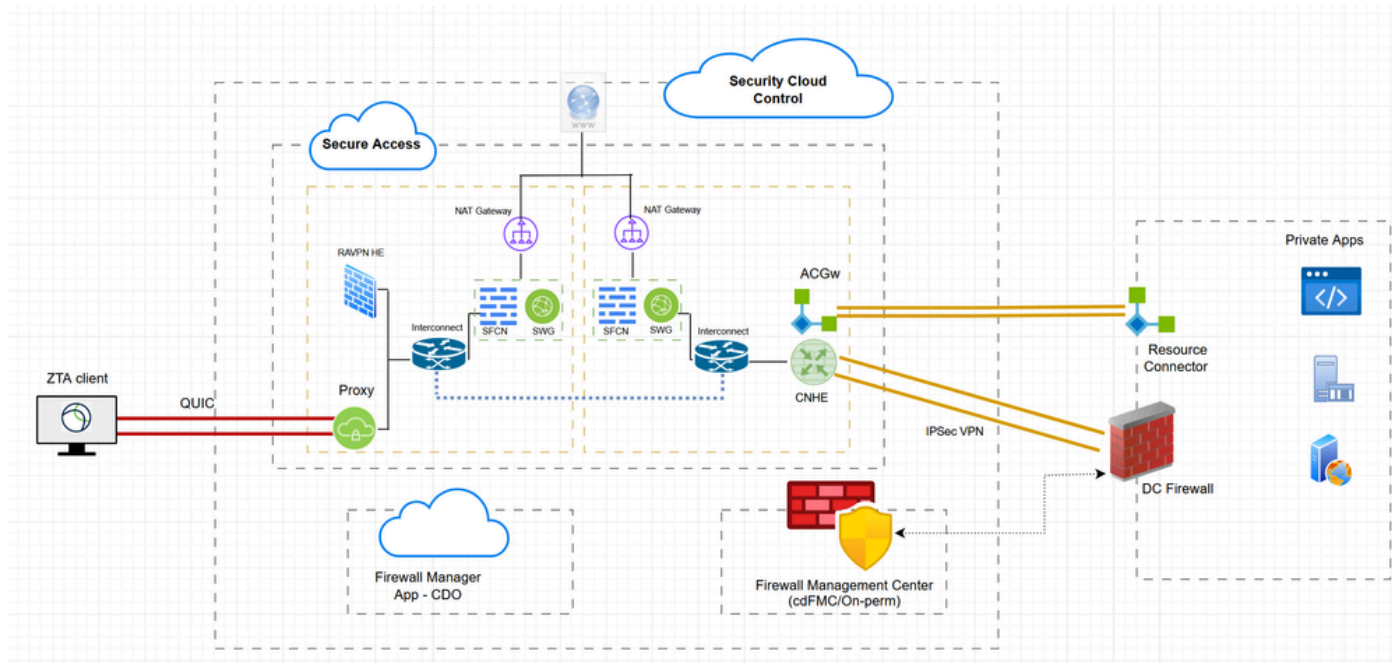
ペクシオン用にUniversal Zero Trust(UZT)フローをマークします。アクセストークンから取得したルールIDは、接続メタデータでSnortに渡されます。

9. ユニバーサルゼロ信頼(UZT)ルールと対応するファイルおよびIPSポリシーマッピングは、FMCを介してFTDにプッシュされます。Snortのゼロトラストプラグインは、初期化時にこれらのルールをロードします。Linaは、Secure Accessから取得したアクセストークンに、そのプライベートリソースへのアクセス用にファイルまたはIPSポリシーが指定されている場合にのみ、Snortインスペクション用にユニバーサルゼロトラストストリームフローをマークします。

アクセストークンから取得したルールIDは、Conn Meta経由でSnortに渡されます。すべてのユニバーサルゼロトラストストリームフローについて、Snortのゼロトラストプラグインは、Conn Metaから取得したルールIDのルールルックアップを実行します。ルール的一致が見つかった場合、フローが許可され、そのルールに固有のIPSポリシーとファイルポリシーがフローに適用されます。一致するルールが見つからない場合、Snortのゼロトラストプラグインによってフローがブロックされます。

設定

ネットワーク図

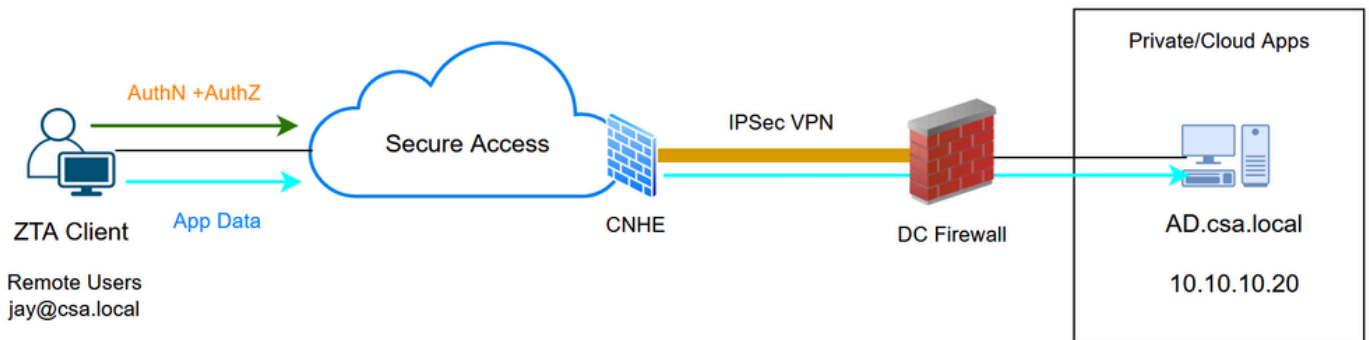


ハイブリッドZTNA : ネットワーク図

テストケース

テストケース1：リモートユーザ – クラウドの適用

このテストケースでは、Cloud Enforcement経由でNetwork Tunnel Groupを介してプライベートリソースにアクセスします。この場合、ポリシー評価とアプリケーションデータの両方が、ZTAモジュール(SGT)を介したセキュアアクセスによって代行受信されます。これは、ZTAに登録されたクライアントからネットワークトンネルグループまたはリソースコネクタを介してプライベートアプリケーションにアクセスできる従来のフローです



ユニバーサルZTA – テストケースのトポロジ

手順1：セキュアアクセスでのプライベートリソースの定義

クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

1. Resources > Destinations > Private Resourcesの順に移動し、+Addをクリックします。

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

セキュアアクセス：プライベートリソースの設定

2. 「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。

← 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)

セキュアアクセス：プライベートリソースの設定

3. アクセスするプライベートリソースのFQDNを入力します。また、プライベートリソースのIPアドレスを定義することもできます。詳細については、「[プライベートリソースの追加](#)」を参照してください。

4. ドメインを解決する内部DNSサーバーを選択します

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			
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
<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

セキュアアクセス：プライベートリソースの設定

5. エンドポイント接続方法の選択

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

Enforcement point for Remote and Local Users



Cancel

Save and Test Save

セキュアアクセス：プライベートリソースの設定

6. 「保存」をクリックします。

手順2：プライベートアクセスルールの作成

Secure Access上のプライベートアクセスを、ユニバーサルZTA登録済みユーザによるアクセスとなるように設定します（デフォルト）。詳細については、「[プライベートアクセスルール](#)」を参照してください

1. Secure > Access Policyの順に移動します。

Access	Action	Sources	Destinations	Security	Hits	Status
Low	Private	Allow	Any AD Users	AD-Server	92	On
	Private	Allow	Any AD Users	ESXI	-	On
S-Allow	Private	Allow	Any AD Users	InternalDNS	-	On

セキュアアクセス：アクセスポリシーの設定

2. Add Ruleをクリックし、Private Accessを選択します。

ルールの上には、ルールの設定済みコンポーネントを説明する要約が表示されます。

The screenshot shows the 'Access Policy' management page. At the top right, there is a link for 'Rule Defaults and Global Settings'. Below the header, there is a search bar and filter options for 'Intent', 'Objects', and 'Settings'. A table lists 2 rules:

	#	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	🌐🔒

A tooltip for 'Private Access' is shown, describing it as 'Control and secure access to resources and applications that cannot be accessed by the general public.' Another tooltip for 'Internet Access' describes it as 'Control and secure access to public destinations from within your network and from managed devices.' At the bottom right, there are pagination controls: 'Rows per page 100', '1-2 of 2', and a page indicator '1'.

セキュアアクセス：アクセスポリシーの設定

3. ルール名の追加

The screenshot shows the 'Add AD-RDP-Allow' rule configuration page. It includes a toggle for 'Rule is enabled' and a link for 'Logging is enabled Edit'. A 'Summary' section shows a flow diagram: 'Sources: Any' leads to 'Action: Allow', which leads to 'Security Controls' (dashed box), which leads to 'Destinations: Any private destination'. Below this, there are fields for 'Rule name' (AD-RDP-Allow) and 'Rule order' (1). A 'Specify Access' section is active, showing two action options: 'Allow' (selected) and 'Block'. The 'From' and 'To' fields are visible at the bottom.

セキュアアクセス：アクセスポリシーの設定

4. ルール処理を選択し、ソースと宛先を選択します

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
Specify one or more sources.
AD Users • Any AD Users

To
Specify one or more destinations.
Private Resources • AD-Server

+ AND

セキュアアクセス : アクセスポリシーの設定

5. エンドポイント要件の設定

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

Zero-Trust Client-based Posture Profile **Rule Defaults**
Requirements for end-user devices on which the Cisco Secure Client is installed.
Profile: **None** | Requirements: **None**
Private Resources: **AD-Server**

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

User Authentication Requirements

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

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

Cancel Back Next

セキュアアクセス : アクセスポリシーの設定

6. セキュリティの設定

✓ **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](#)

セキュアアクセス：アクセスポリシーの設定

7. Saveをクリックします。

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="text"/>
<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

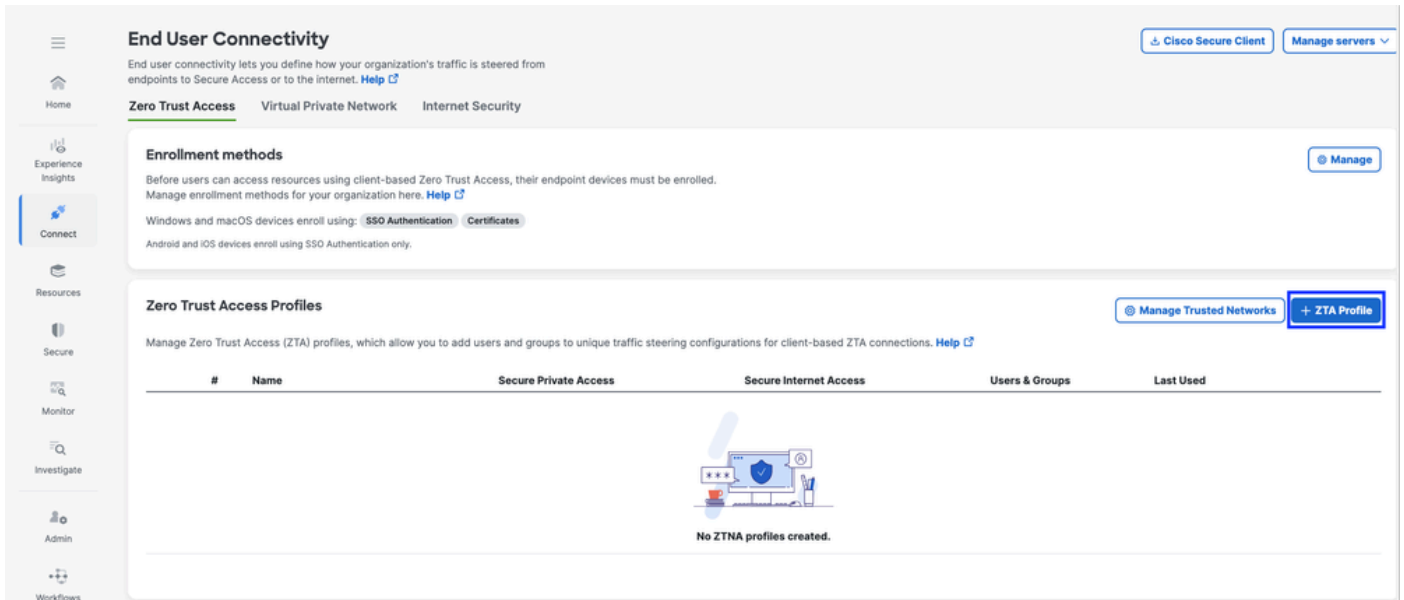
Rule name	Action	Sources	Destinations	Security	Posture	<input type="text"/>
For all private access	Block	Any	Any private destination	-	-	...
For all Internet access	Allow	Any	Any Internet destination	🌐🔒	-	...

セキュアアクセス：アクセスポリシーの設定

手順 – 3 ZTAプロファイルへのプライベートリソースの追加

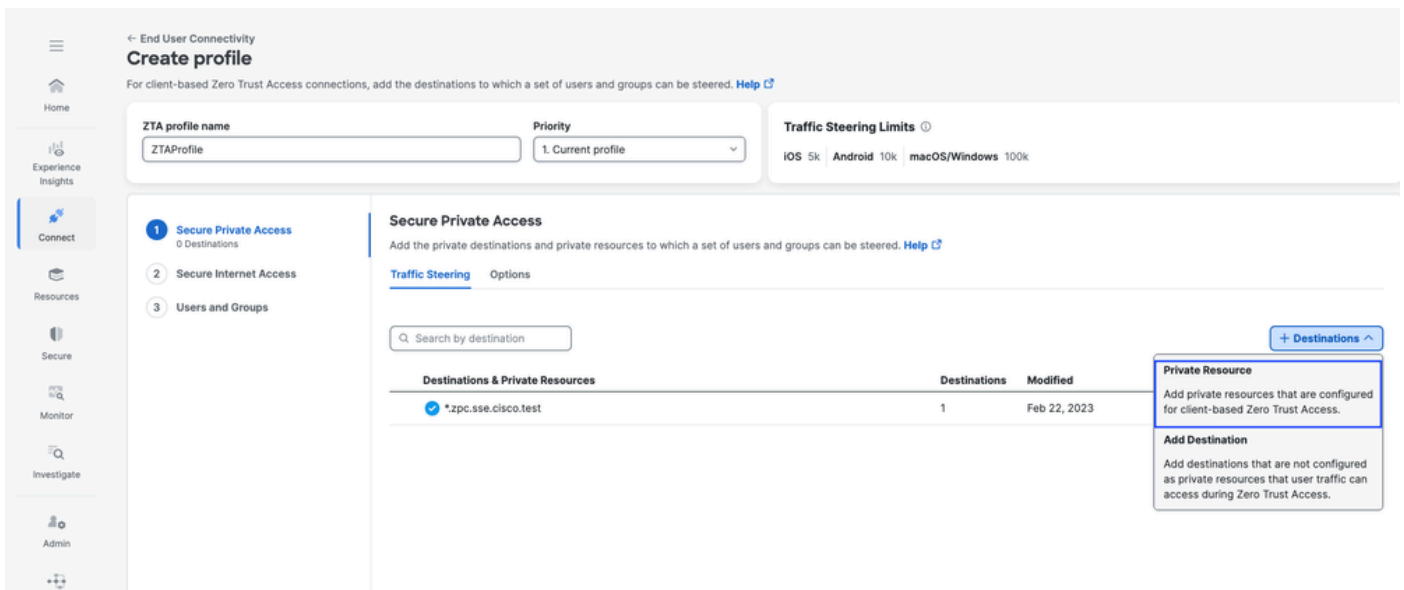
カスタムZTAプロファイルを使用している場合は、それぞれのプライベートリソースをZTAプロファイルに追加する必要があります

1. Connect > End User Connectivity > Zero Trust Accessの順に移動し、+ZTA Profileをクリックします。

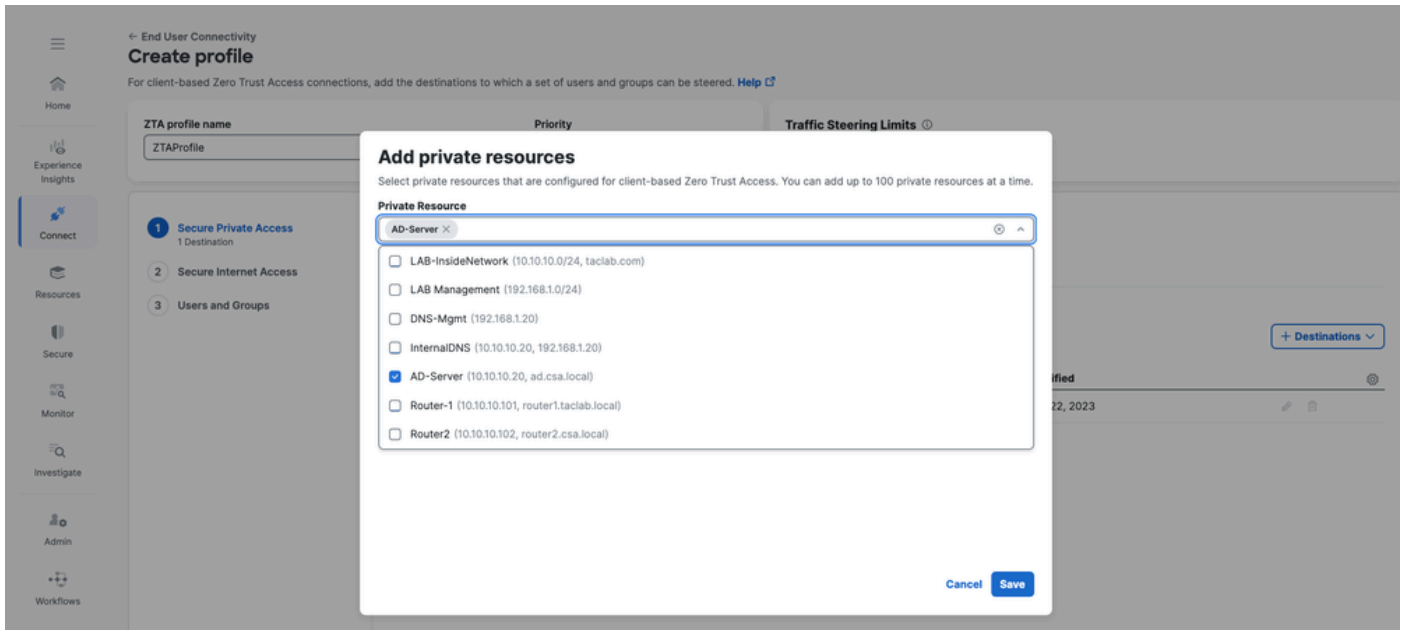


セキュアアクセス – ZTAプロフィール

2. プライベートリソースの追加

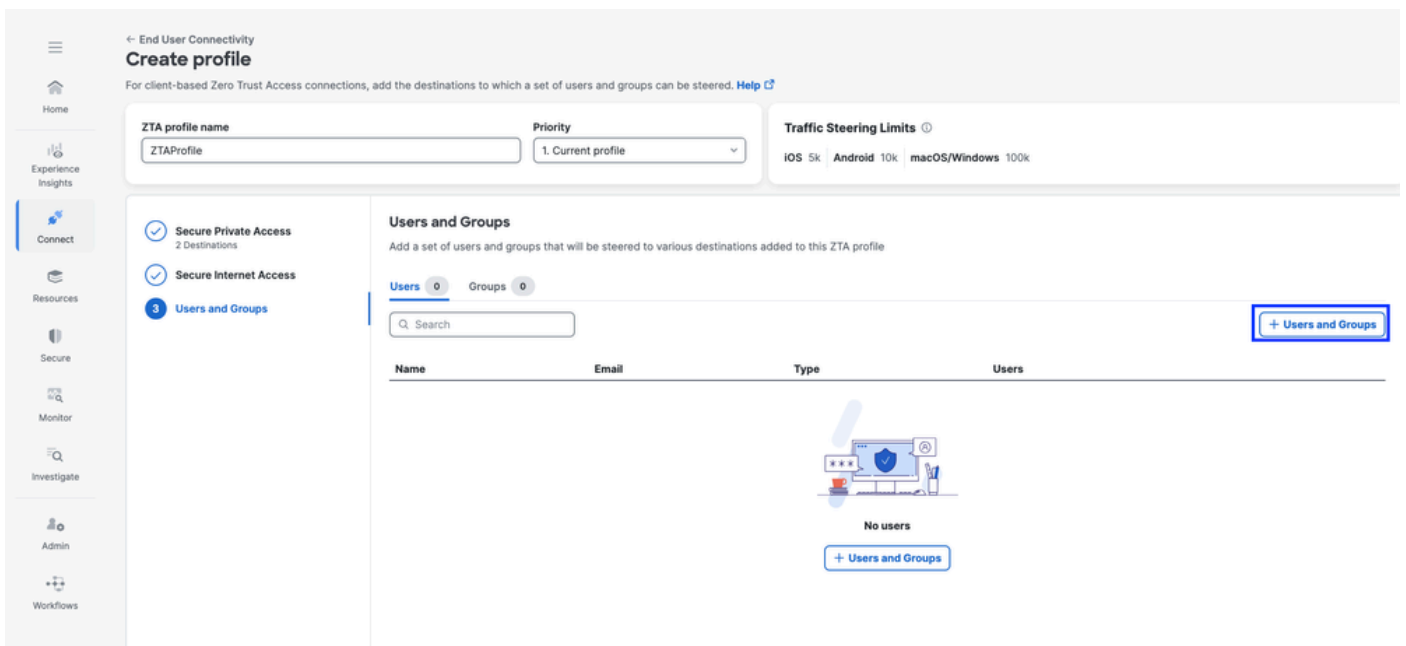


セキュアアクセス – ZTAプロフィール



セキュアアクセス - ZTAプロフィール

3. ユーザーとグループの追加



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

セキュアアクセス - ZTAプロフィール

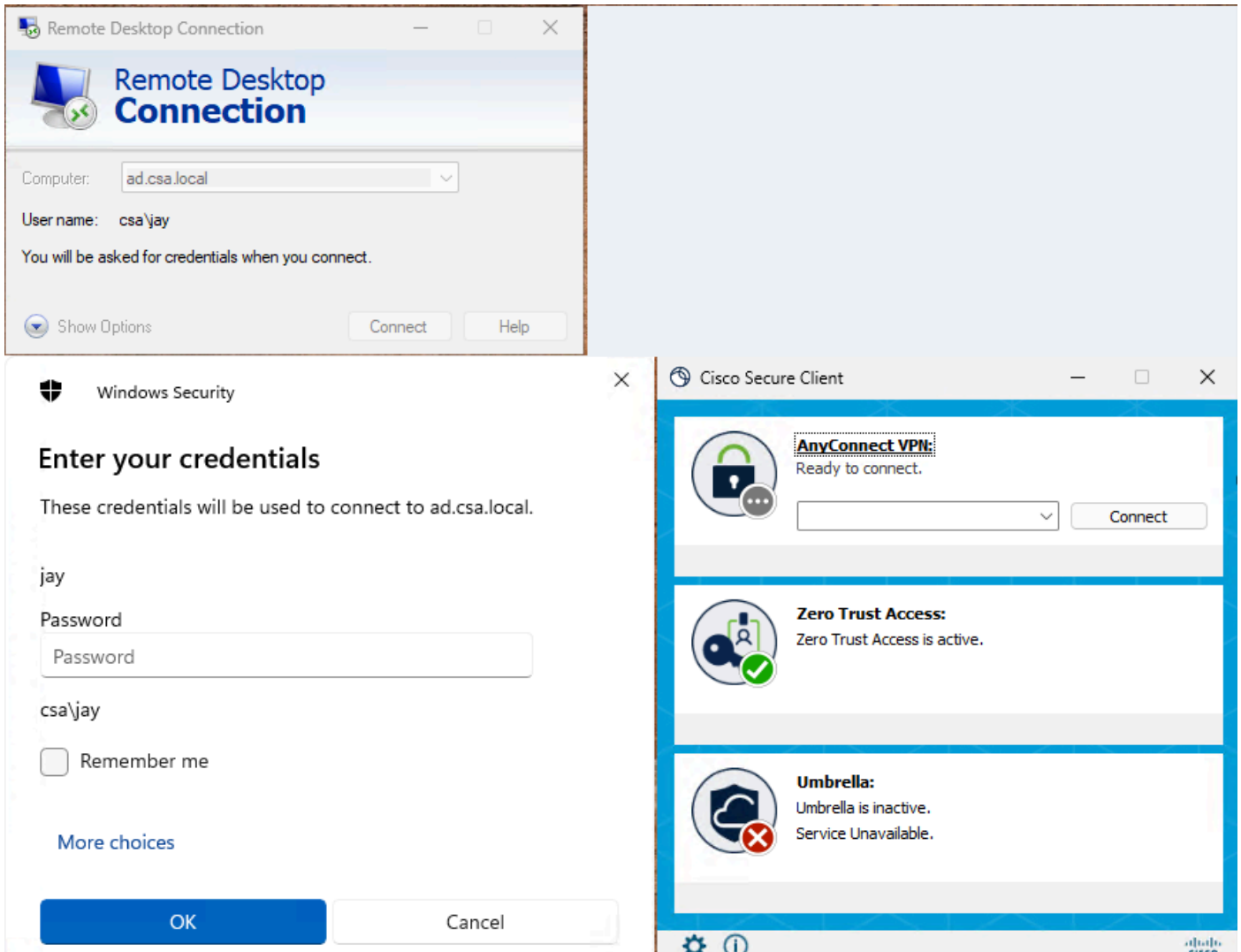


注：割り当てられたプライベートリソースの設定をプッシュしてクライアントに同期するには、最大で15 ~ 20分かかる場合があります

ステップ4：プライベートリソースへのアクセスを確認する

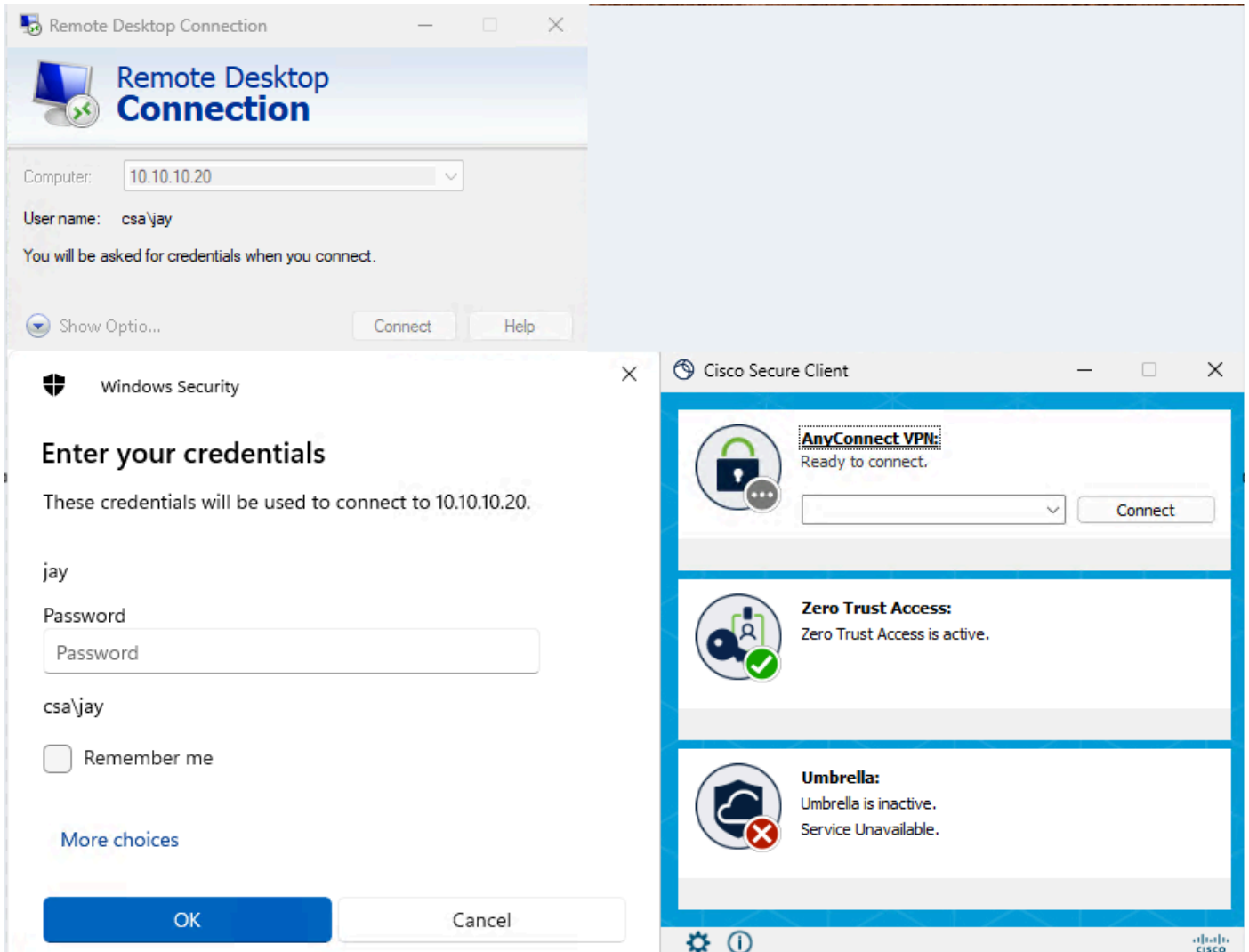
1. プライベートリソースへのアクセス

FQDNを使用してPRにアクセスします



セキュアなアクセス - PRテスト

IPアドレスを使用してPRにアクセスします



セキュアなアクセス – PRテスト

2. アクティビティ検索イベントで確認する

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

セキュアアクセス – アクティビティ検索

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 PORT 3389 Restore to previous state Save Search

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

Response Select All
 Allowed Advanced
 Blocked

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

Enforced By Select All
 Secure Access Cloud
 FTD
 Umbrella Cloud

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

Event Details

Identity
jay (jay@csa.local)
Win1

Rule Name
AD-RDP-Allow

Resource/Application
AD-Server

Zero Trust Access Profile
Default ZTA Profile

Trusted Network
No Match

Enforcement Point
Secure Access Cloud

Destination
ad.csa.local

Destination IP
10.10.10.20

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

セキュアアクセス - アクティビティ検索

Activity Search Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 Restore to default layout Save Search

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

Response Select All
 Allowed Advanced
 Blocked

Identity Type Select All
 AD Users
 AD Groups

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

セキュアアクセス - アクティビティ検索

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
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

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

セキュアアクセス - アクティビティ検索

3. FMC接続イベントの確認

Events Troubleshooting

Destination Port / ICMP Code 3389

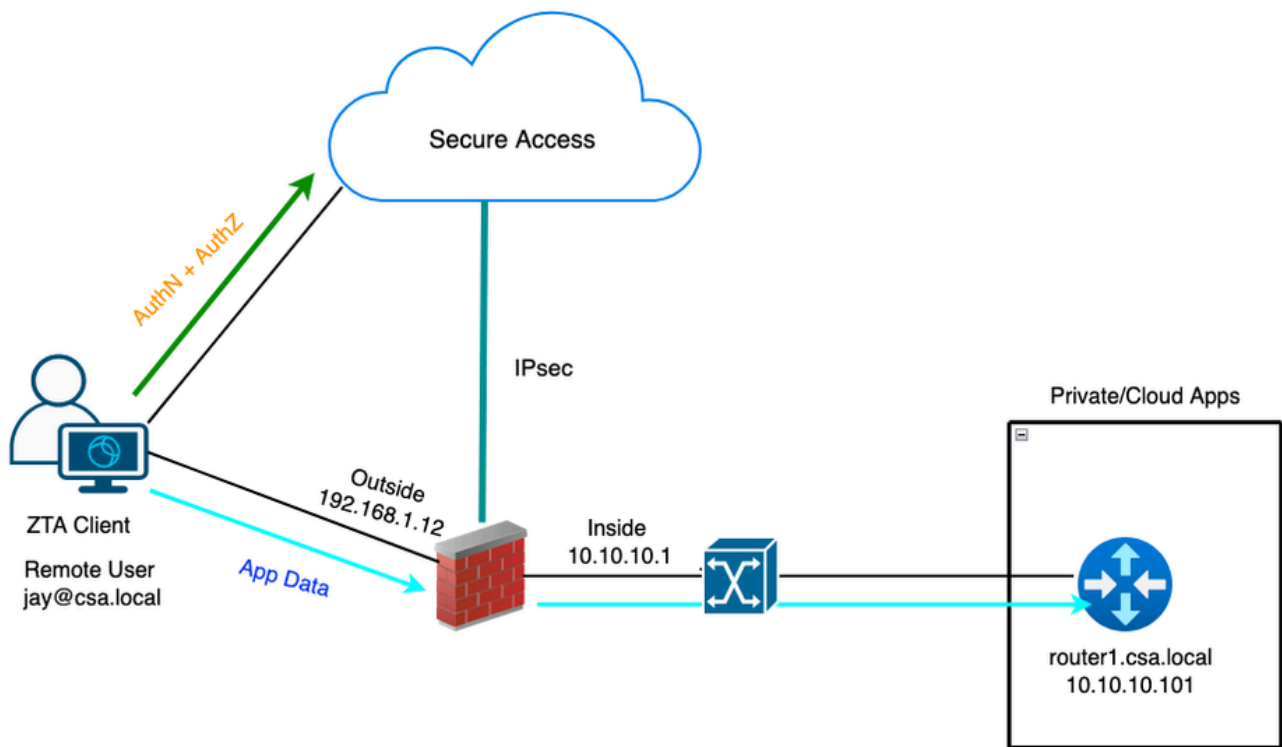
7 events Last 1 hour

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		

FMC接続イベント

テストケース2 - リモートユーザー - ローカル強制

このタイプの強制ポリシー評価では、ローカルの強制を介したプライベートリソースへのアクセスはセキュアアクセスで行われますが、アプリケーションデータはFTDのローカルに残ります。たとえば、ZTAに登録済みのクライアントまたはユーザがホームネットワークに接続し、FTD内部インターフェイス(SVI)の背後にあるプライベートリソースにアクセスしようとした場合です。



ユニバーサルZTA – テストケースのトポロジ

手順1：セキュアアクセスでのプライベートリソースの定義

クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

1. Resources > Destinations > Private Resourcesの順に移動し、+Addをクリックします。

The screenshot shows the Cisco Security Cloud Control interface. The 'Resources' page is open, and the 'Private Resource' tab is selected. The table below shows the configuration for 5 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

セキュアアクセス：プライベートリソースの設定

2. 「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。

← 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)

セキュアアクセス：プライベートリソースの設定

3. アクセスするプライベートリソースのFQDNを入力します。また、プライベートリソースのIPアドレスを定義することもできます。詳細については、「[プライベートリソースの追加](#)」を参照してください。

4. ドメインを解決する内部DNSサーバーを選択します

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="router1.csa.local"/>	<input type="text" value="Any TCP"/>	<input type="text" value="22"/>	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.101"/>	<input type="text" value="Any TCP"/>	<input type="text" value="22"/>	+ Protocol & Port
Remove	+ IP Address/FQDN		

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

Internal DNS Server

セキュアアクセス：プライベートリソースの設定

5. エンドポイント接続方法の選択

6. ローカル強制ポイントとしてFTDを選択します。

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... X Search by FTD na... v

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

セキュアアクセス：プライベートリソースの設定



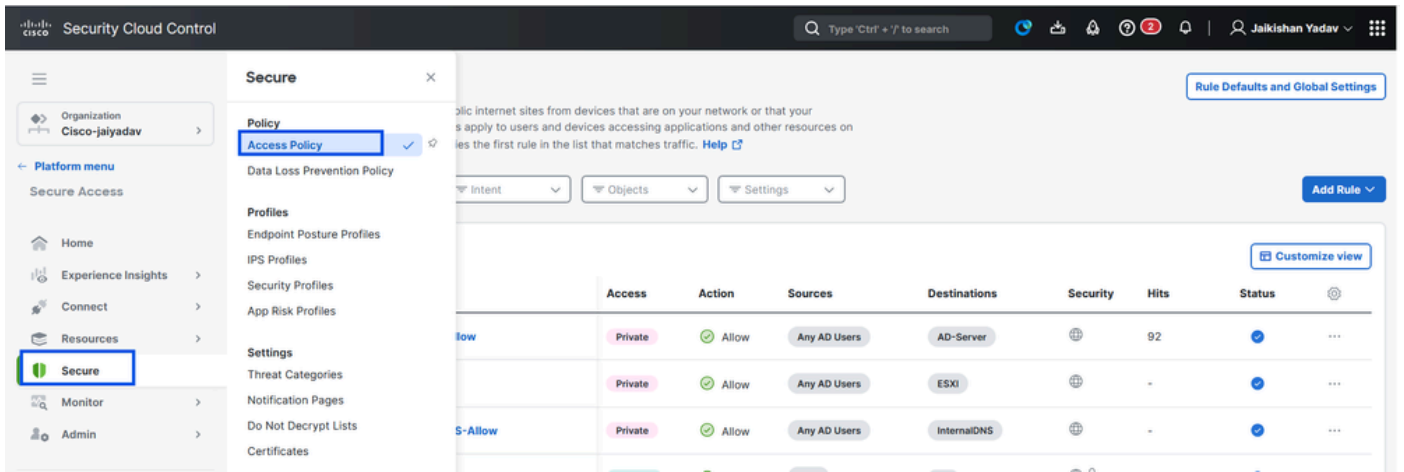
注：選択する登録のタイプ（IPアドレスまたは非IPアドレス）に応じて、この変更によりPRがFTDに自動的に関連付けられ、ポリシーの導入がトリガーされます。

7. 「保存」をクリックします。

手順2：プライベートアクセスルールの作成

Secure Access上のプライベートアクセスを、ユニバーサルZTA登録済みユーザによるアクセスとなるように設定します（デフォルト）。詳細については、「[プライベートアクセスルール](#)」を参照してください

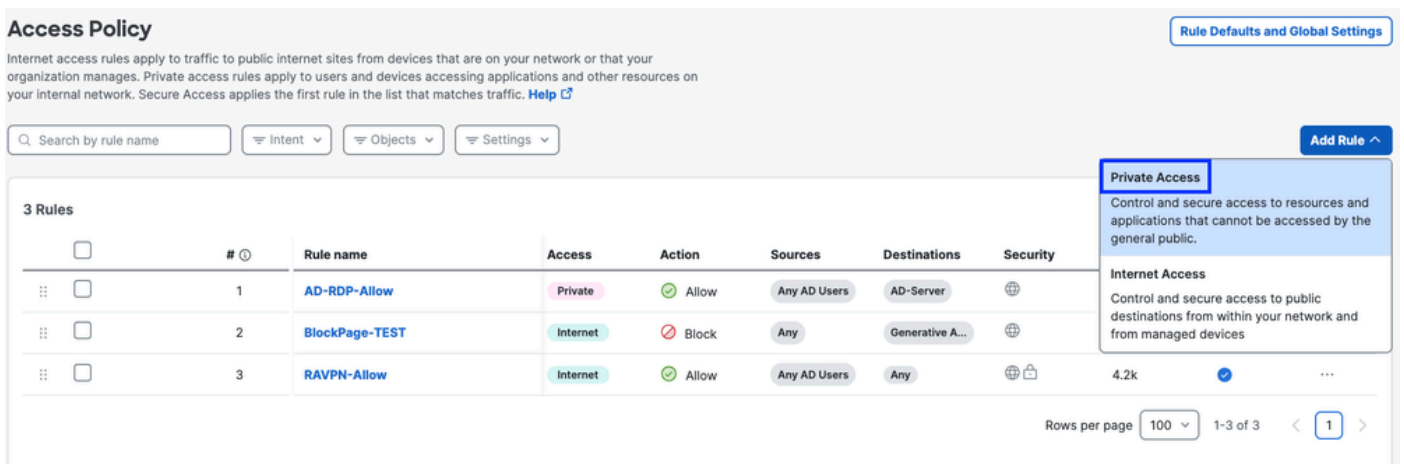
1. Secure > Access Policyの順に移動します。



セキュアアクセス：プライベートリソースの設定

2. Add Ruleをクリックし、Private Accessを選択します。

ルールの上には、ルールの設定済みコンポーネントを説明する要約が表示されます。



セキュアアクセス：アクセスポリシーの設定

3. ルール名の追加

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.

セキュアアクセス：アクセスポリシーの設定

4. ルール処理を選択し、ソースと宛先を選択します

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

セキュアアクセス：アクセスポリシーの設定

5. エンドポイント要件の設定

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](#)

セキュアアクセス：アクセスポリシーの設定

6. セキュリティの設定

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](#)

セキュアアクセス：アクセスポリシーの設定

7. Saveをクリックします。

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 >

セキュアアクセス：アクセスポリシーの設定

手順3:FTDでのPRの関連付けを確認します

1. 「接続」>「ネットワーク接続」>「FTDs」に移動します。

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' window with a 'Network Connections' tab selected. Below the tab, there are two status indicators: '0 Warning' and '1 Connected'. The 'FTDs' tab is also visible and highlighted.

セキュアアクセス – PR検証

2. 「FTD」>「このFTDに関連付けられたリソースの表示」の順にクリックします。

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 [Close]

Firewall Details [Expand]

Device FQDN: ftd.csa.local [Edit]
 Auto deployment: Yes

UZTA Configuration status [Expand]

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

Assigned Trusted Network [Expand]

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

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

Associated Resources [Expand] 1

RESOURCES ASSOCIATED BY STATUS

Status: Synced 1

[View resources associated to this FTD](#)

[Associate Resources](#)

セキュアアクセス – PR検証

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](#)

セキュアアクセス – PR検証

3. 「閉じる」をクリックします。

4. ステータスを確認します (図1の矢印Aを参照)。関連するリソースと設定は同期済み状態である必要があります

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

セキュアアクセス – PR検証

5. 設定がFTDにプッシュされたことを確認します。

FTD cliにログインし、LINAモードに移動します。

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:PRの確認

手順4:ZTAプロファイルへのプライベートリソースの追加

1. Connect > End User Connectivity > Zero Trust Accessの順に移動し、3つのドットをクリックしてZTAプロファイルを編集します

The screenshot shows the 'End User Connectivity' dashboard. Under 'Zero Trust Access Profiles', there is a table with the following data:

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

The 'Edit' button for the 'ZTAProfile' row is circled in red.

セキュアアクセス – ZTAプロファイル

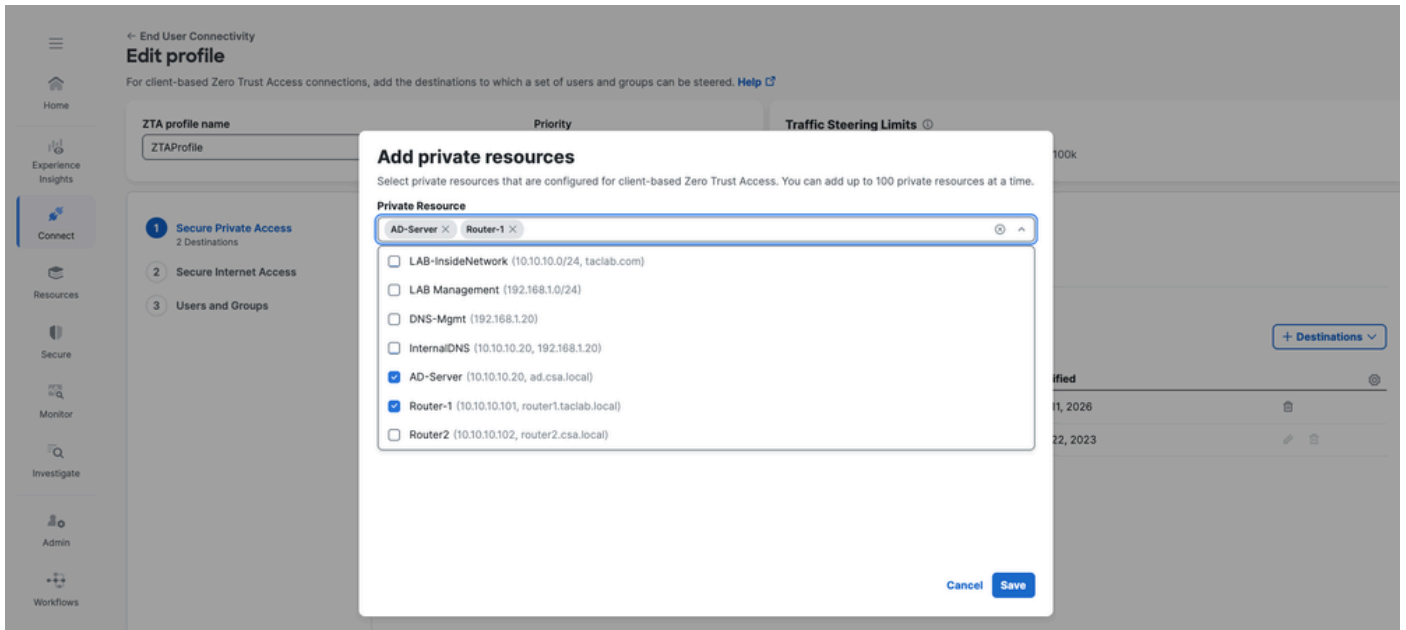
2. プライベートリソースの追加

The screenshot shows the 'Create profile' page for ZTA. The 'Secure Private Access' section is active, and a 'Private Resource' is being added. The table below shows the 'Destinations & Private Resources' section:

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

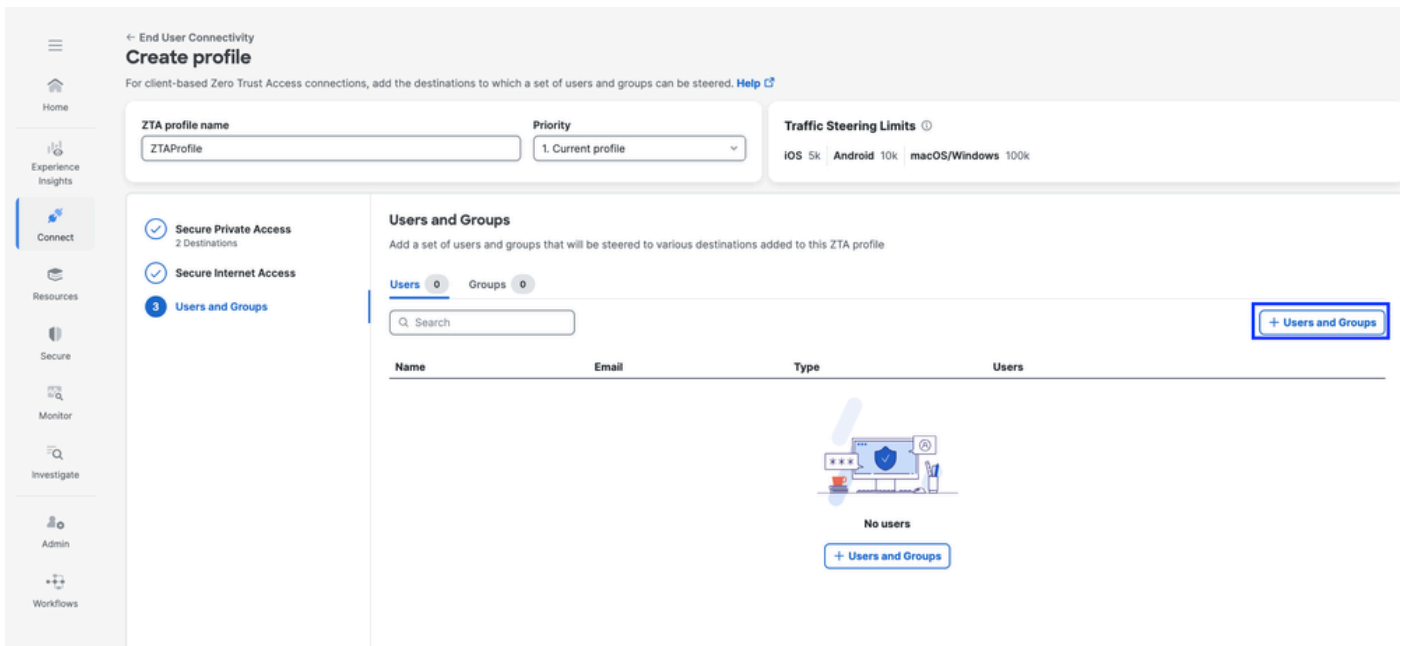
The 'Private Resource' section is highlighted with a red box, showing the text: 'Add private resources that are configured for client-based Zero Trust Access.' and 'Add Destination: Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.'

セキュアアクセス – ZTAプロファイル



セキュアアクセス - ZTAプロフィール

3. ユーザーとグループの追加



セキュアアクセス - ZTAプロフィール

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

セキュアアクセス - ZTAプロファイル

ステップ5: プライベートリソースへのアクセスを確認する

1. リモートユーザがFTD FQDNを解決できることを確認します

```
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
```

セキュアなアクセス – PRテスト

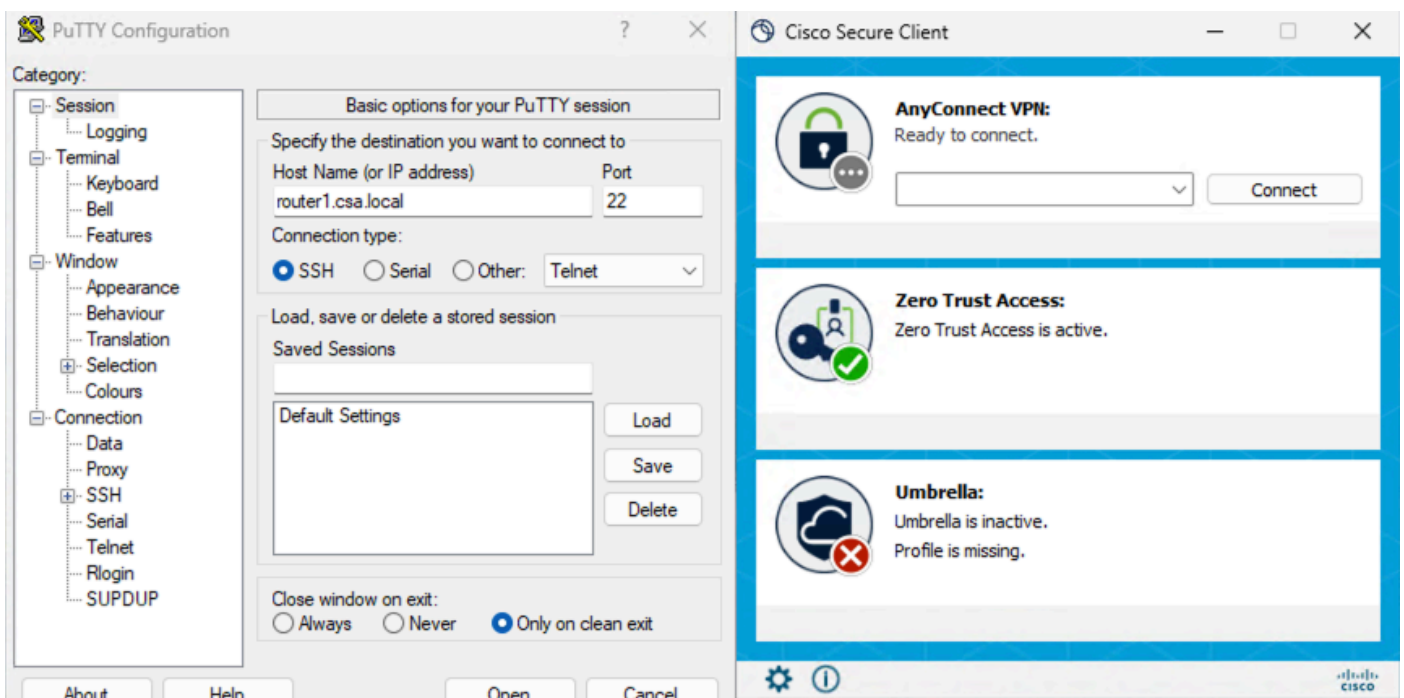
2. FTDがFQDNを使用してプライベートリソースに到達できることを確認します。

```
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# █
```

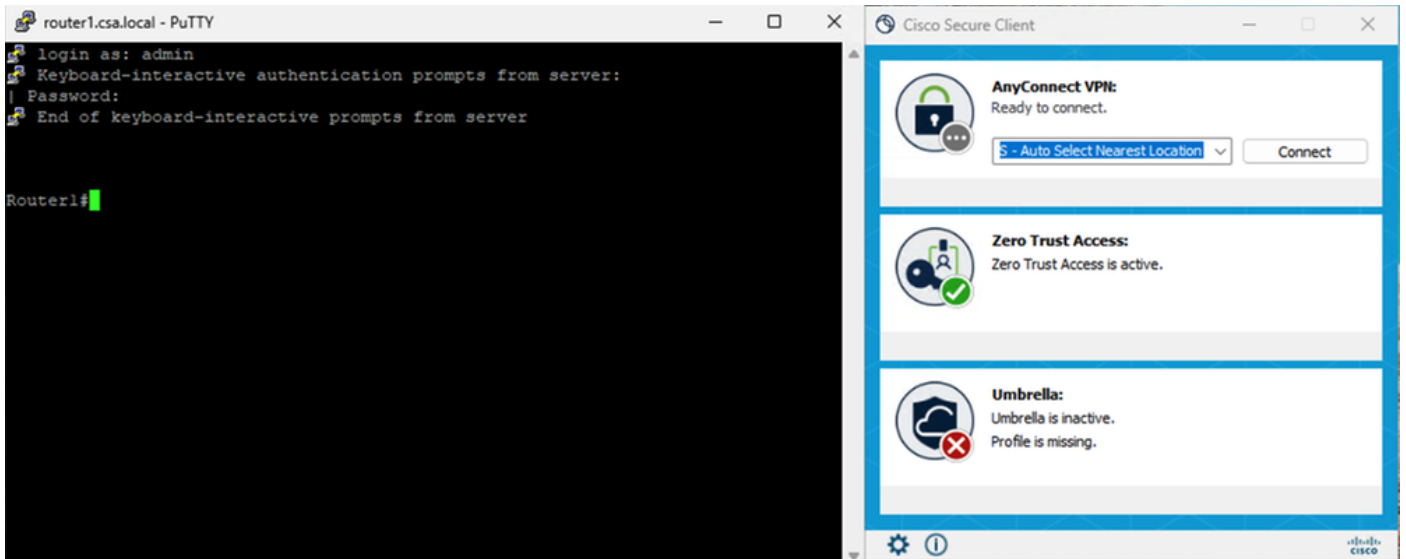
セキュアなアクセス – PRテスト

3. プライベートリソースへのSSH接続をテストする

FQDNを使用してPRにアクセスします

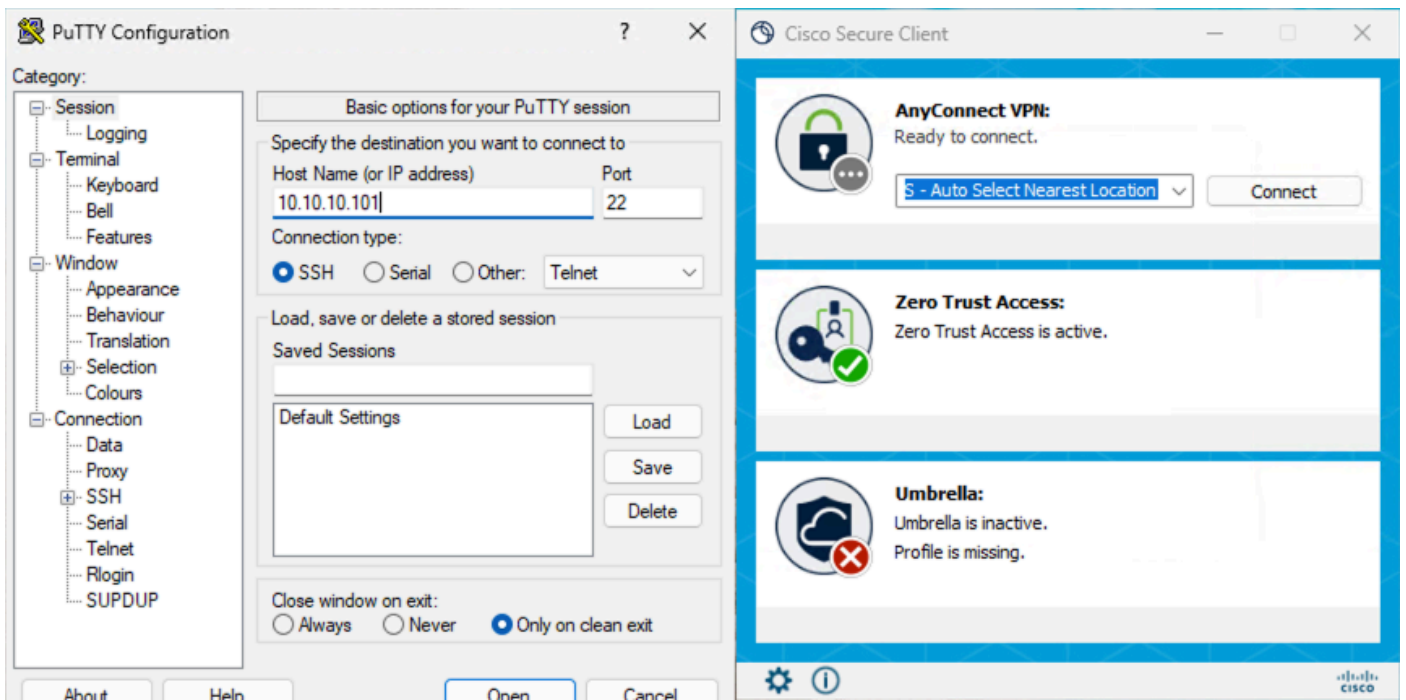


セキュアなアクセス – PRテスト

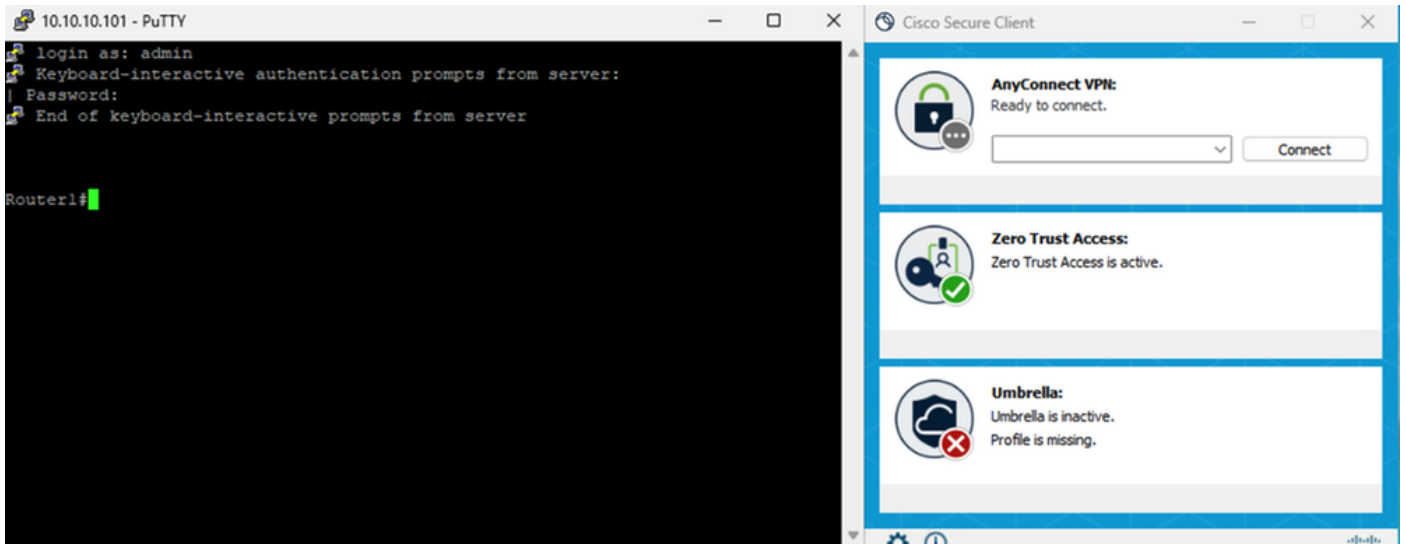


セキュアなアクセス – PRテスト

IPアドレスを使用してPRにアクセスします



セキュアなアクセス – PRテスト



セキュアなアクセス – PRテスト

4. セキュアアクセスアクティビティ検索ログの確認

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
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
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
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

セキュアアクセス – アクティビティ検索

Event Details

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

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: -

セキュアアクセス – アクティビティ検索

Activity Search

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

IP ADDRESS: 10.10.10.101 X RESPONSE: Allowed X

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

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location	Location IP
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.39.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.39.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.39.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.39.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.39.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.39.159.129
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462		US	76.39.159.129

セキュアアクセス – アクティビティ検索

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

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:56 PM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD > FMC_FTD

Destination: 10.10.10.101

Destination IP: 10.10.10.101

セキュアアクセス – アクティビティ検索

5. FMC接続イベントの確認

Firewall Management Center

Events & Logs / Analysis / Unified Events

Search: [] Deploy [] [] [] [] admin

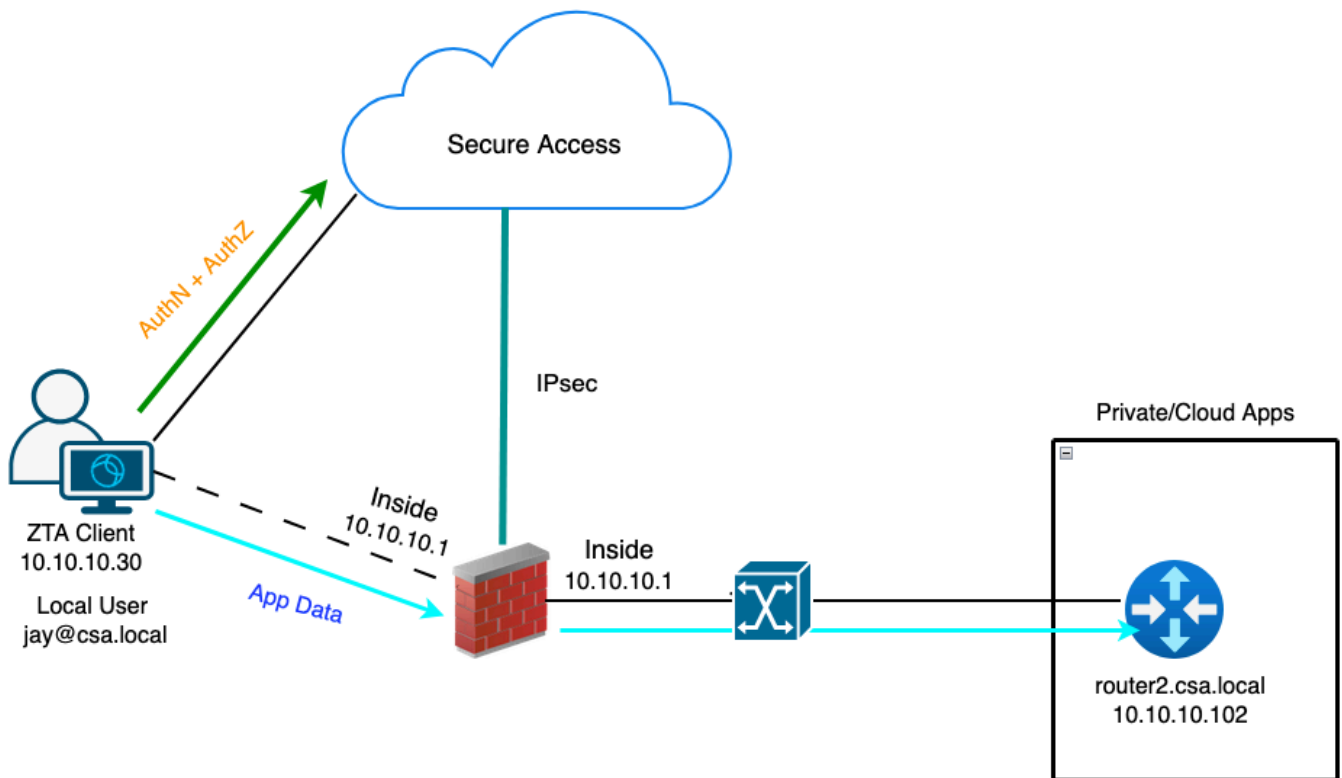
Monitor: Destination IP: 10.10.10.101

6 events

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

テストケース3：ローカルユーザ：ローカル適用

ローカルユーザーとしてローカルエンフォースメントを介してプライベートリソースにアクセスする場合、このタイプのエンフォースメントポリシーの評価はセキュアアクセスで行われますが、アプリケーションデータはFTDのローカルに留まります。たとえば、ZTAに登録済みのクライアントまたはユーザがホームネットワークに接続し、FTD内部インターフェイス(SVI)の背後にあるプライベートリソースにアクセスしようとした場合です。プライベートリソースがDMZまたはFTDの他のインターフェイスの背後にある場合、クライアントIPまたはネットワークとプライベートリソース間のトラフィックを許可するために、FTD上にアクセスルールを作成する必要があります。

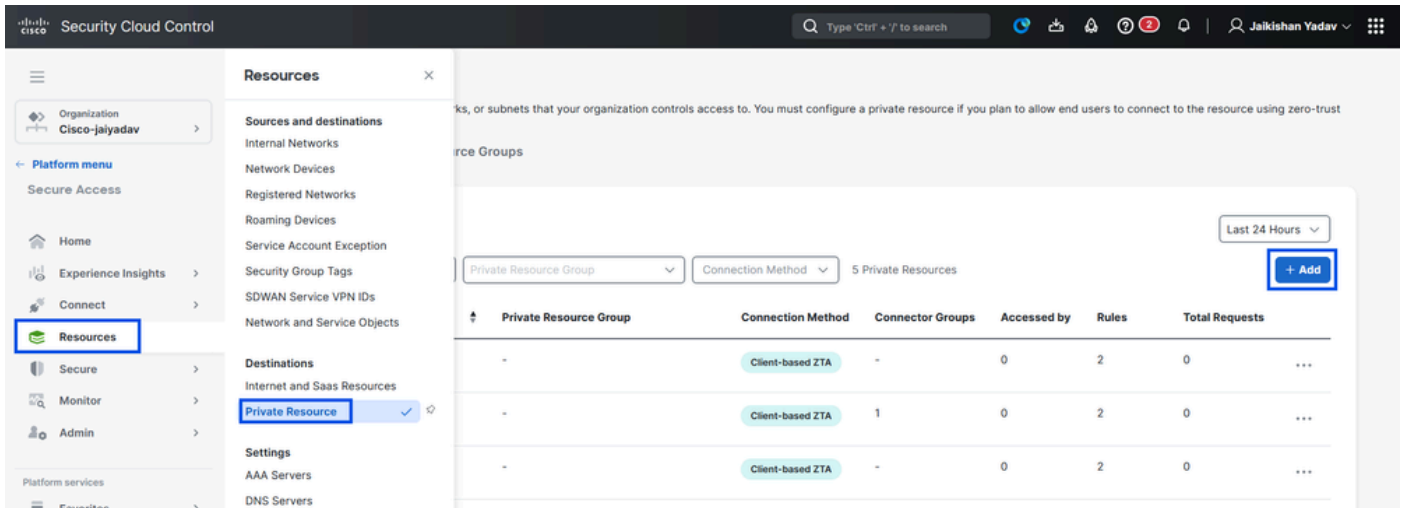


ユニバーサルZTA – テストケースのトポロジ

手順1：セキュアアクセスでのプライベートリソースの定義

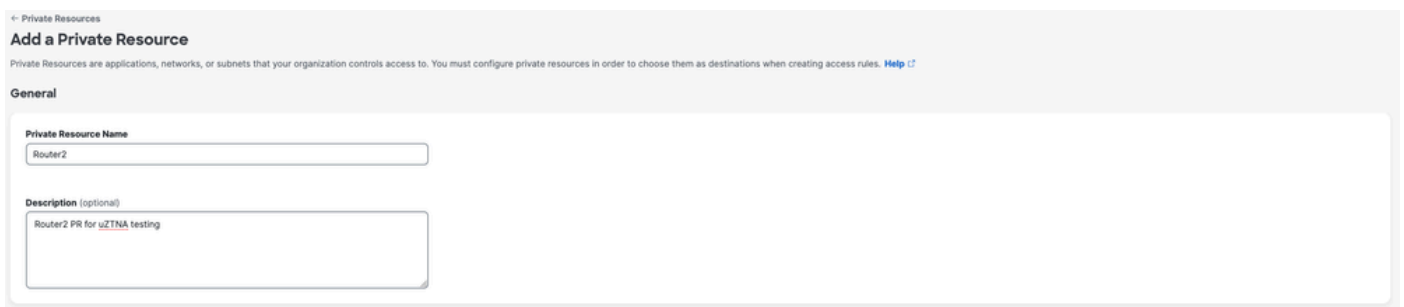
クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

1. Resources > Destinations > Private Resourcesの順に移動し、+Addをクリックします。



セキュアアクセス：プライベートリソースの設定

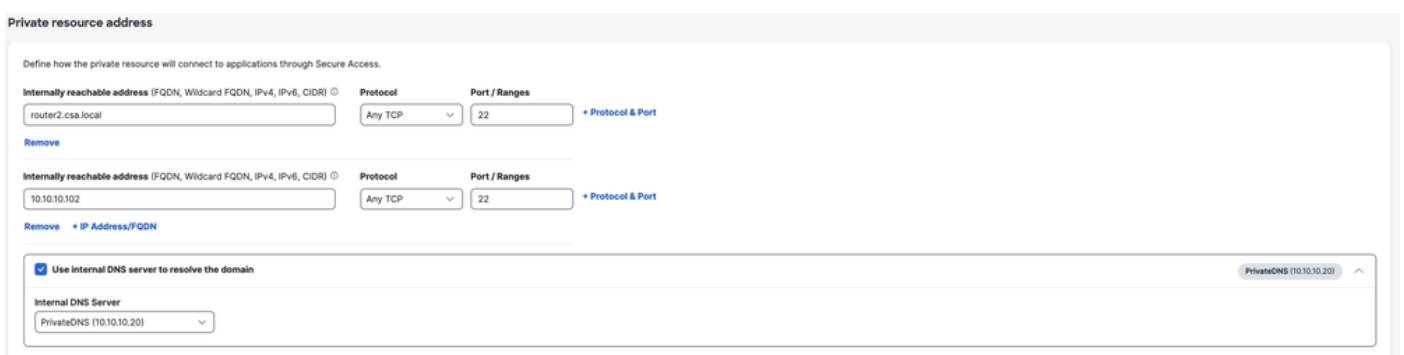
2. 「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。



セキュアアクセス：プライベートリソースの設定

3. アクセスするプライベートリソースのFQDNを入力します。また、プライベートリソースのIPアドレスを定義することもできます。詳細については、「[プライベートリソースの追加](#)」を参照してください。

4. ドメインを解決する内部DNSサーバーを選択します



セキュアアクセス：プライベートリソースの設定

5. エンドポイント接続方法の選択

6. ローカル強制ポイントとしてFTDを選択します。

Endpoint Connection Methods

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

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

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

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

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

Enforcement point for Remote User

Remote user Local Firewall Private Resource

via internet

Enforcement point for Local user

User in a trusted network Local Firewall Private Resource

via local network

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

セキュアアクセス：プライベートリソースの設定



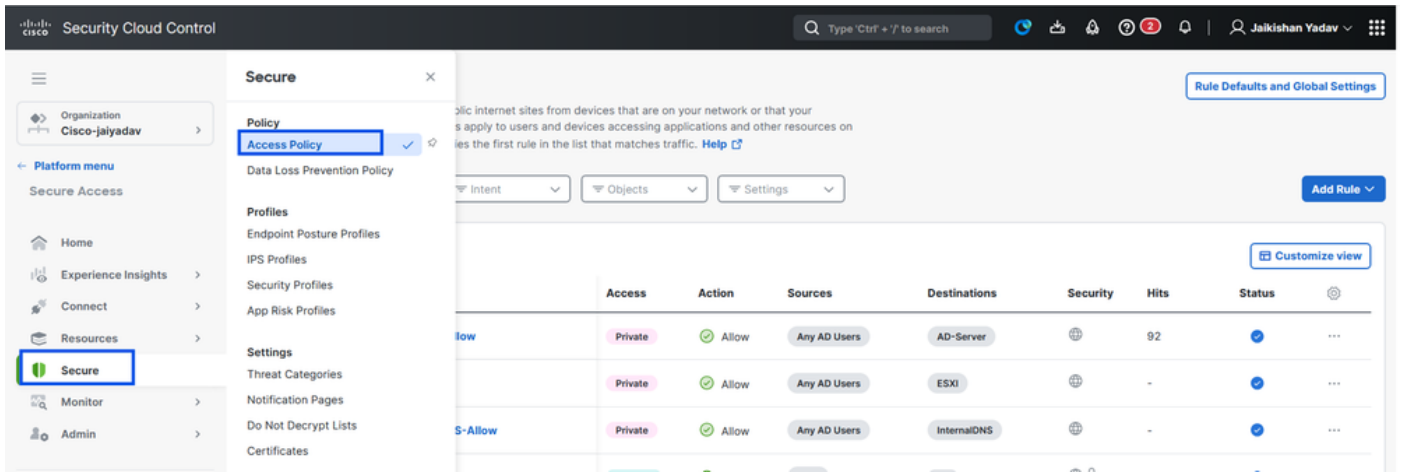
注：選択する登録のタイプ（IPアドレスまたは非IPアドレス）に応じて、この変更によりPRがFTDに自動的に関連付けられ、ポリシーの導入がトリガーされます。

7. 「保存」をクリックします。

手順2：プライベートアクセスルールの作成

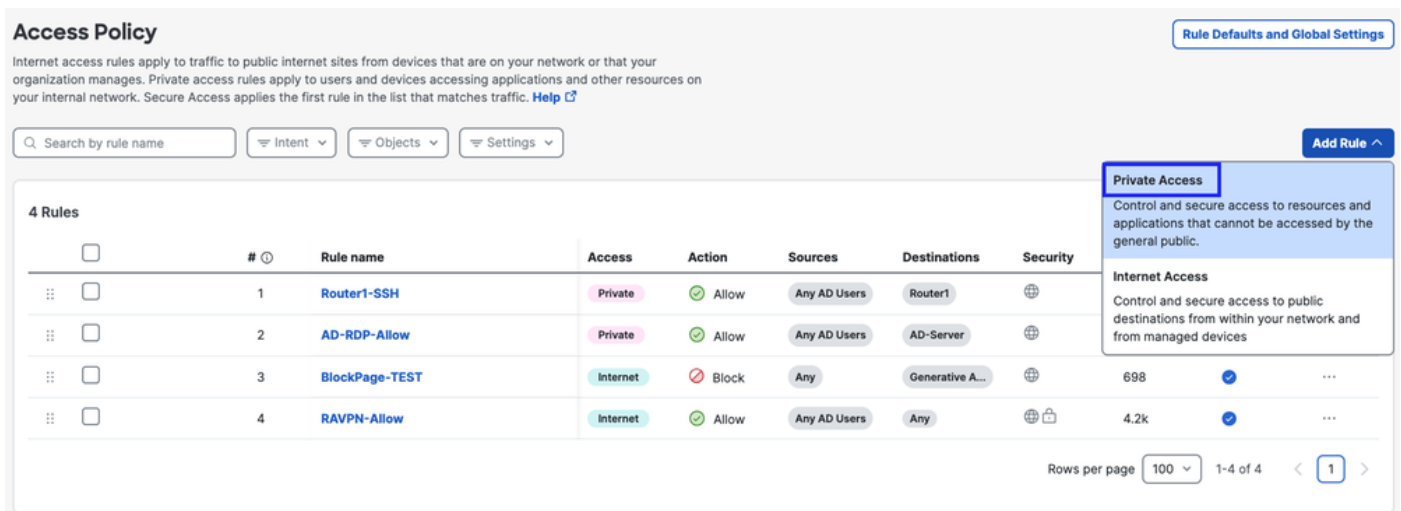
Secure Access上のプライベートアクセスを、ユニバーサルZTA登録済みユーザによるアクセスとなるように設定します（デフォルト）。詳細については、「[プライベートアクセスルール](#)」を参照してください

1. Secure > Access Policyの順に移動します。



セキュアアクセス：アクセスポリシーの設定

2. Add Ruleをクリックし、Private Accessを選択します。
 ルールの上には、ルールの設定済みコンポーネントを説明する要約が表示されます。



セキュアアクセス：アクセスポリシーの設定

3. ルール名の追加

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.

セキュアアクセス：アクセスポリシーの設定

4. ルール処理を選択し、ソースと宛先を選択します

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

セキュアアクセス：アクセスポリシーの設定

5. エンドポイント要件の設定

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](#)

セキュアアクセス：アクセスポリシーの設定

6. セキュリティの設定

1 Specify Access

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

2 Configure Security

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

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

Disabled

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

Security Profile [Rule Defaults](#)

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

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



[Cancel](#)

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

セキュアアクセス：アクセスポリシーの設定

7. Saveをクリックします。

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

セキュアアクセス：アクセスポリシーの設定

手順3:FTDでのPRの関連付けを確認します

1. 「接続」>「ネットワーク接続」>「FTDs」に移動します。

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

セキュアアクセス – PR検証

2. 「FTD」をクリック>「このFTDに関連付けられたリソースの表示」をクリックします。

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](#)

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local

Auto deployment: Yes

UZTA Configuration status

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

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources 2

RESOURCES ASSOCIATED BY STATUS

Status: Synced 2

View resources associated to this FTD

Associate Resources

セキュアアクセス – PR検証

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 2 Resources [Associate Resources](#)

Resource name	Status
Router1	Synced
Router2	Synced

Close

セキュアアクセス – PR検証

3. 「閉じる」をクリックします。

4. ステータスを確認します (図1の矢印Aを参照)。関連するリソースと設定は同期済み状態である必要があります

The screenshot displays the 'Network Connections' page in the Palo Alto Networks management console. The 'FTDs' tab is selected, showing a table of configured FTDs. The table has columns for 'FTD Name', 'Version', 'FMC', and 'UZTA Configuration status'. One FTD, 'FMC_FTD', is listed with version 'v10.0.0' and FMC 'FMC'. Its 'UZTA Configuration status' is 'Synced', which is highlighted with a blue box. To the right, a detailed view for 'FMC_FTD' is shown, including 'Firewall Details' (Device FQDN: ftd.csa.local, Auto deployment: Yes), 'UZTA Configuration status' (Synced, last synced at 12 Jan 2026, 6:29 AM UTC), 'Assigned Trusted Network' (LAN, 1 DNS Servers), and 'Associated Resources' (2 resources associated by status: Synced).

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

セキュアアクセス – PR検証

5. 設定がFTDにプッシュされたことを確認します。

FTD cliにログインし、LINAモードに移動します。

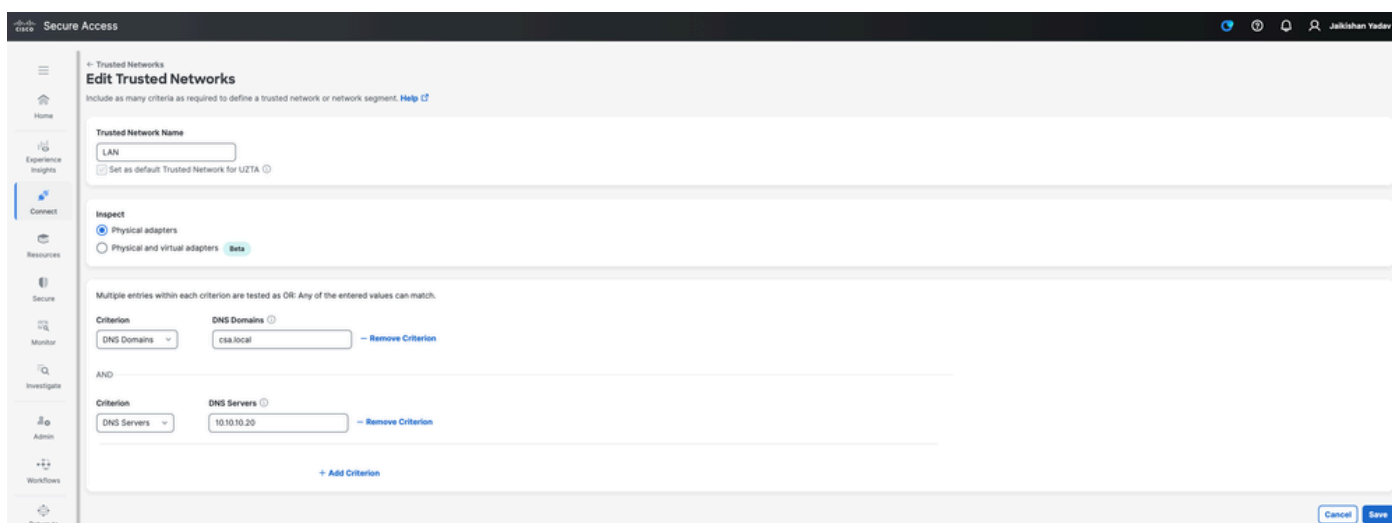
```
# show running-config object application
```

```
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
```

セキュアアクセス – PR検証

ステップ – 4 設定「信頼できるネットワークまたはZTA設定の管理」

Connect > End User Connectivity > Zero Trust Access > ZTA Settingsの順に移動し、Trusted Networksを設定します。



セキュアアクセス : TNDの設定

ステップ5 ZTAプロファイルへのプライベートリソースの追加

1. Connect > End User Connectivity > Zero Trust Accessの順に移動し、3つのドットをクリックしてZTAプロファイルを編集します

End User Connectivity

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

Enrollment methods

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 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

Callout box: Edit, Delete

セキュアアクセス – ZTAプロフィール

2. プライベートリソースの追加

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](#)

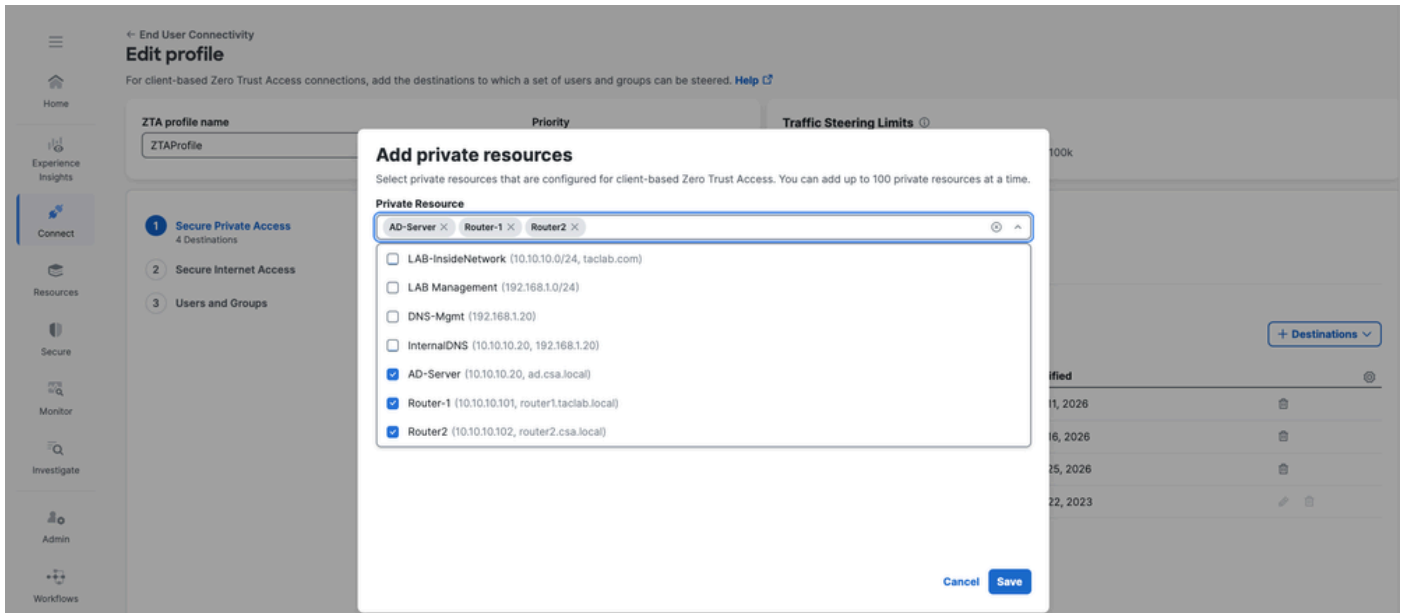
Traffic Steering Options

Search by destination

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

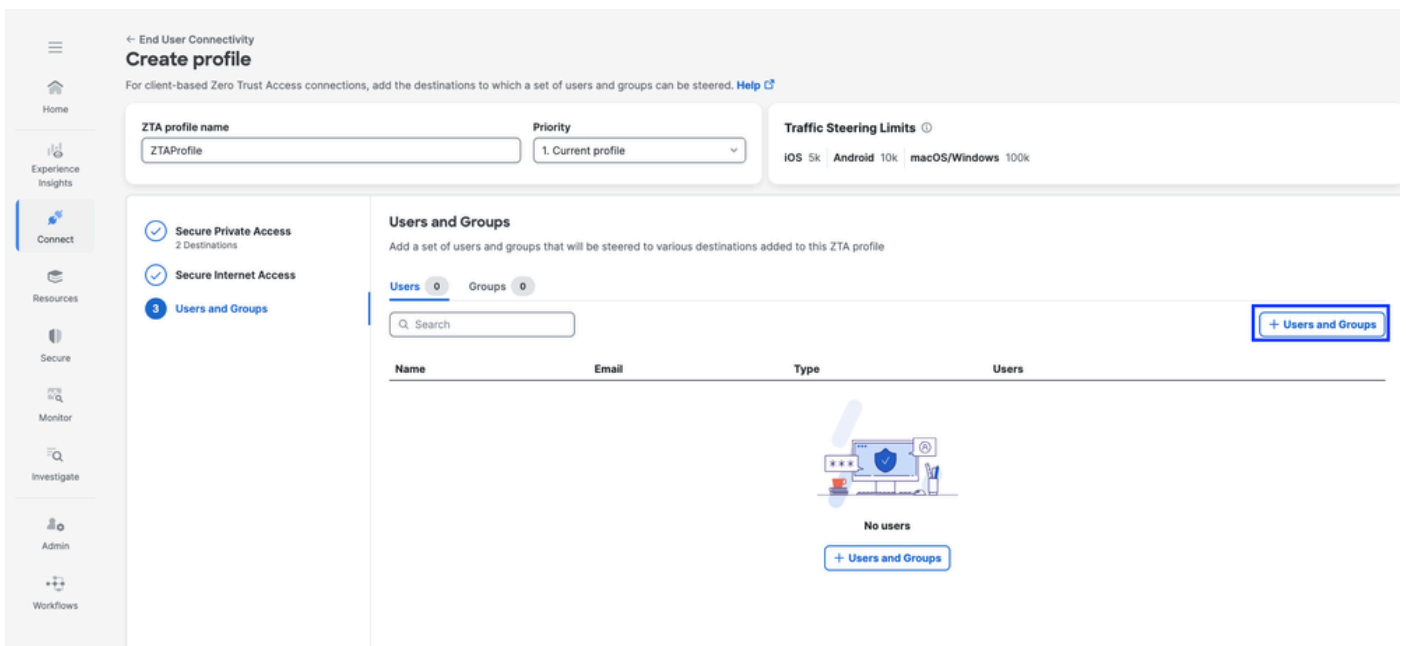
Callout box: Private Resource (Add private resources that are configured for client-based Zero Trust Access), Add Destination (Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.)

セキュアアクセス – ZTAプロフィール



セキュアアクセス - ZTAプロフィール

3. ユーザーとグループの追加



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	-

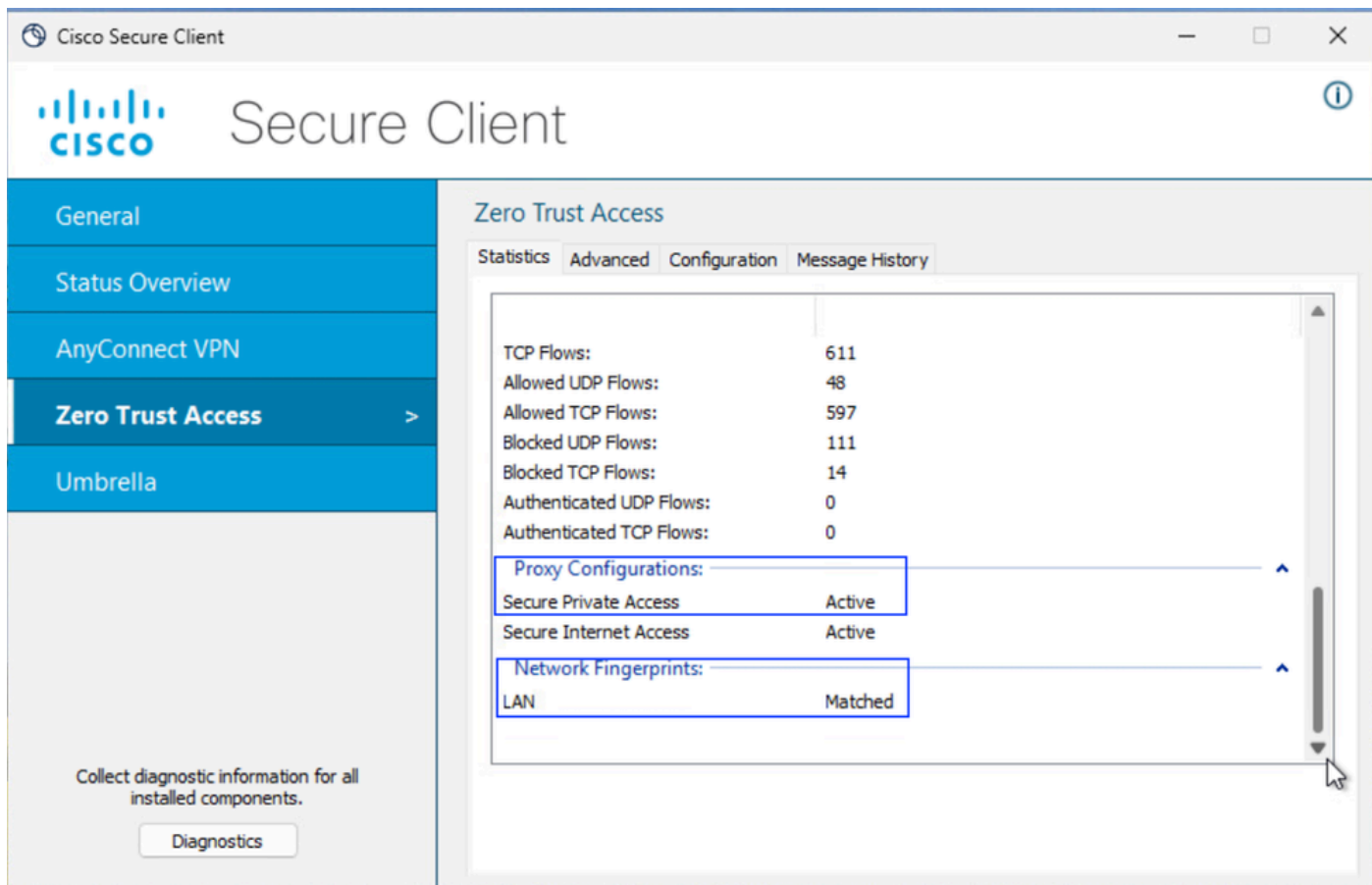
Rows per page: 10 < >

Back Close

セキュアアクセス - ZTAプロファイル

手順6 : プライベートリソースへのアクセスを確認する

1. ZTA TNDのネットワークフィンガープリントを確認する



セキュアなアクセス – PRテスト

2. リモートユーザがFTD FQDNを解決できることを確認します

```
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
```

セキュアなアクセス – PRテスト

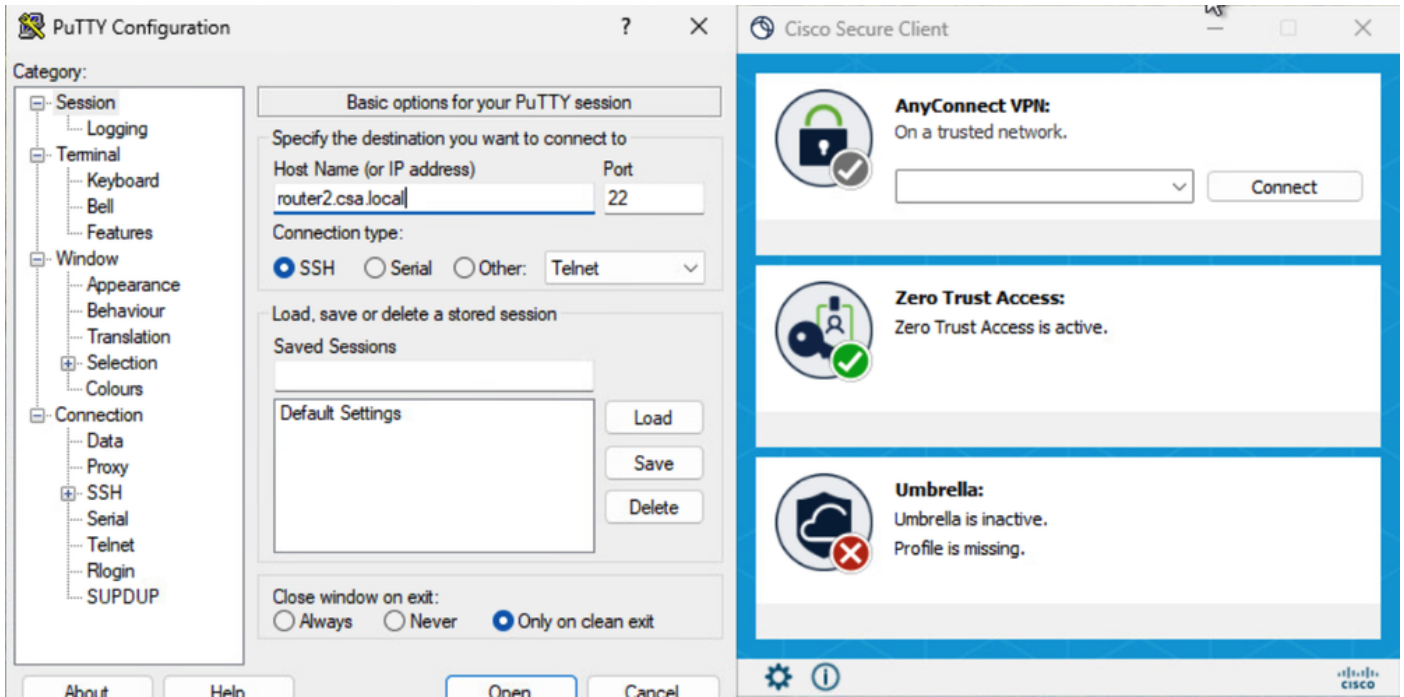
3. FTDがFQDNを使用してプライベートリソースに到達できることを確認します。

```
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# █
```

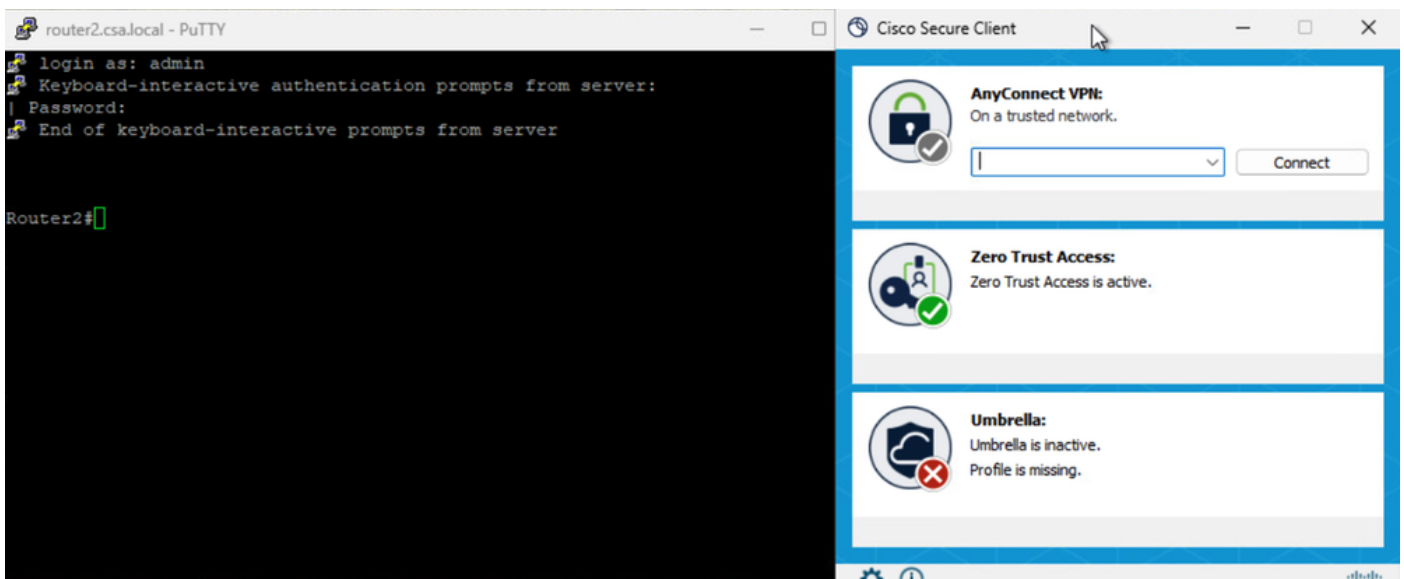
セキュアなアクセス – PRテスト

4. プライベートリソースへのSSH接続をテストする

FQDNを使用してPRにアクセスします

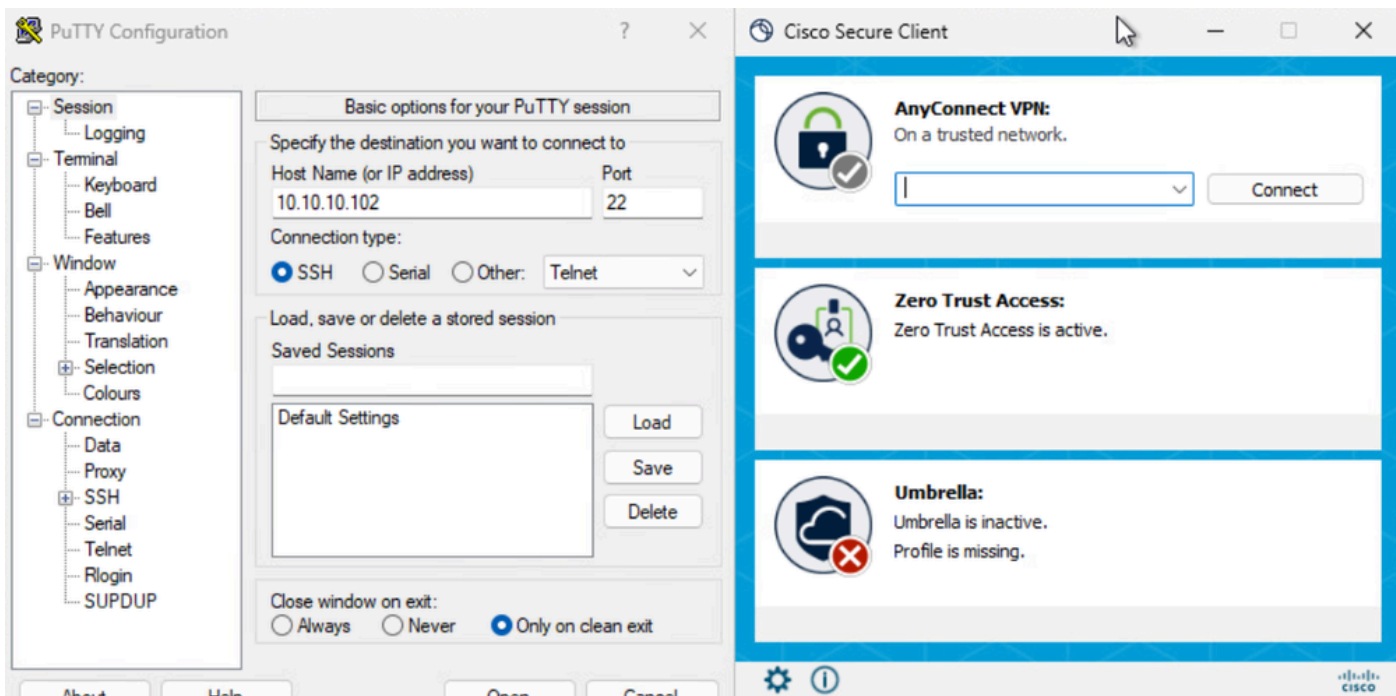


セキュアなアクセス - PRテスト

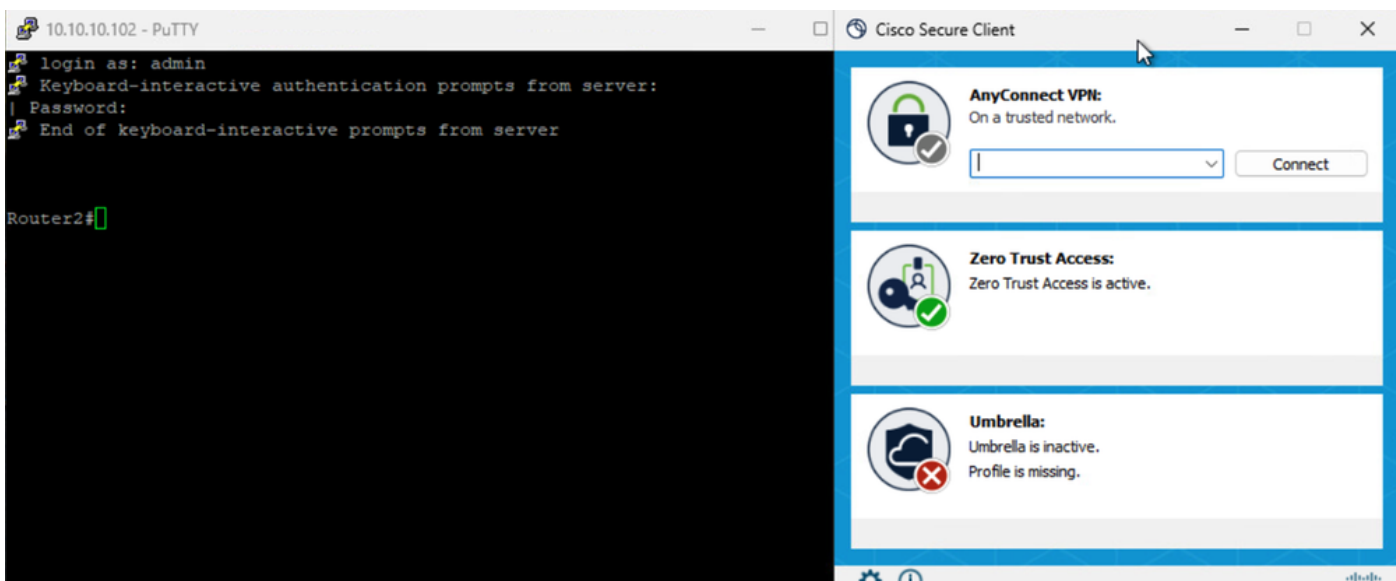


セキュアなアクセス - PRテスト

IPアドレスを使用してPRにアクセスします



セキュアなアクセス - PRテスト



セキュアなアクセス - PRテスト

5. セキュアアクセスアクティビティの検索ログの確認

Activity Search

Activity Search interface showing search filters and results. The search criteria is set to "DOMAIN" with the value "router2.csa.local". The results table shows 8 total entries, all with a response of "Allowed".

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

セキュアアクセス - アクティビティ検索

Activity Search

Activity Search interface showing search filters and results. The search criteria is set to "RESPONSE" with the value "Allowed". The results table shows 17 total entries, all with a response of "Allowed". An "Event Details" sidebar is open on the right, showing details for a specific event.

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)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.64	192.168.1.64	7680	Allowed	LAB Manager
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.23	192.168.1.23	7680	Allowed	LAB Manager

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 3:33 AM

Access details

Identity: jay (jay@csa.local)

ZTNA Client

Rule Name: Router2-SSH-Allow

Resource/Application: Router2

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: FTD > FMC_FTD

Destination: router2.csa.local

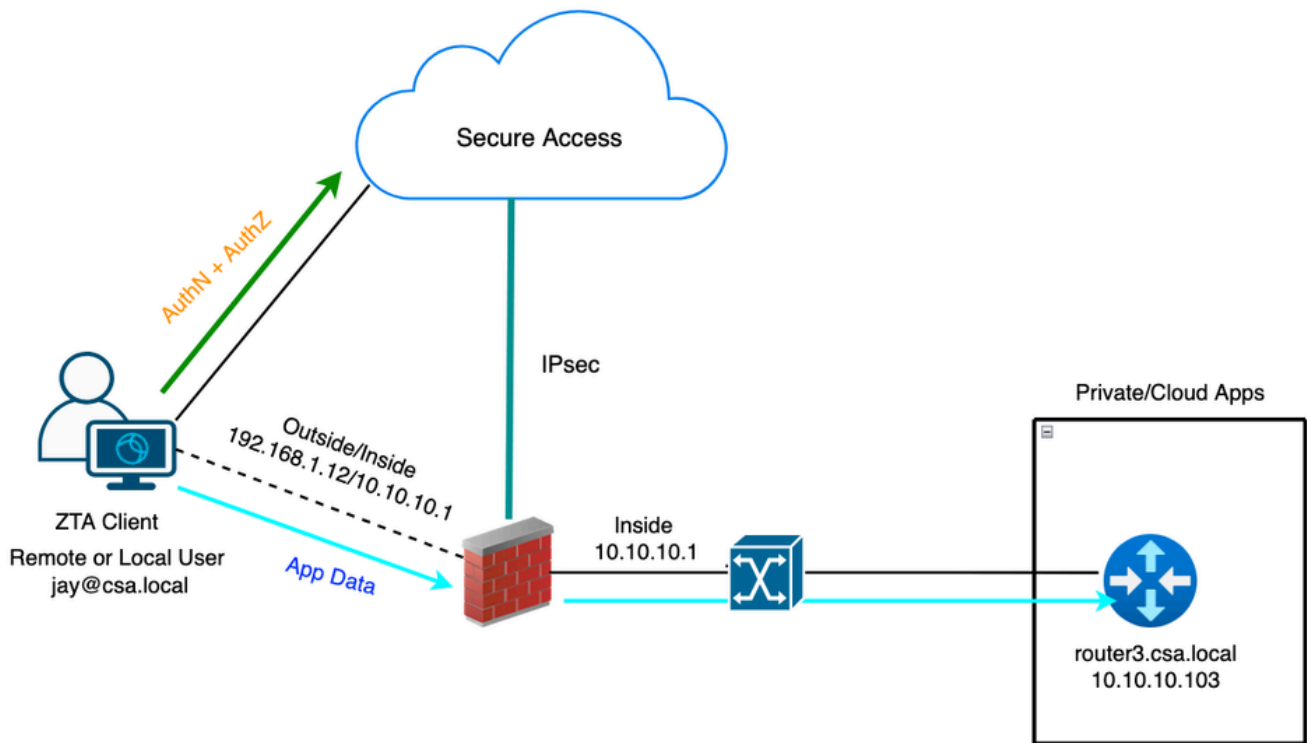
セキュアアクセス - アクティビティ検索

Activity Search

Activity Search interface showing search filters and results. The search criteria is set to "IP ADDRESS" with the value "10.10.10.102" and "RESPONSE" with the value "Allowed". The results table shows 19 total entries, all with a response of "Allowed".

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)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow
Allowed	ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow

セキュアアクセス - アクティビティ検索



ユニバーサルZTA – テストケースのトポロジ

手順1：セキュアアクセスでのプライベートリソースの定義

クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

1. Resources > Destinations > Private Resourcesの順に移動し、+Addをクリックします。

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

セキュアアクセス：プライベートリソースの設定

2. 「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。

← 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)

セキュアアクセス：プライベートリソースの設定

3. アクセスするプライベートリソースのFQDNを入力します。また、プライベートリソースのIPアドレスを定義することもできます。詳細については、「[プライベートリソースの追加](#)」を参照してください。

4. ドメインを解決するDNSサーバーを選択します

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="router3.csa.local"/>	Any TCP	22	+ Protocol & Port
Remove			
<input type="text" value="192.168.1.103"/>	Any TCP	22	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.103"/>	Any TCP	22	+ Protocol & Port
Remove + IP Address/FQDN			

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

セキュアアクセス：プライベートリソースの設定

5. エンドポイント接続方法の選択

6. ローカル強制ポイントとしてFTDを選択します。

Endpoint Connection Methods

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

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

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

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

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

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

Local-only

Enforcement point for Remote User

Remote user Secure Access Cloud Private Resource

via Internet

Enforcement point for Local user

User in a trusted network Local Firewall Private Resource

via local network

Cancel Save and Test Save

セキュアアクセス：プライベートリソースの設定

プライベートリソースがRC経由でアクセス可能な場合はRCを選択し、プライベートリソースがNetwork Tunnel Group(IPsec Tunnel)経由でアクセス可能な場合は空白のままにします。

Resource Connector Groups

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

セキュアアクセス：プライベートリソースの設定



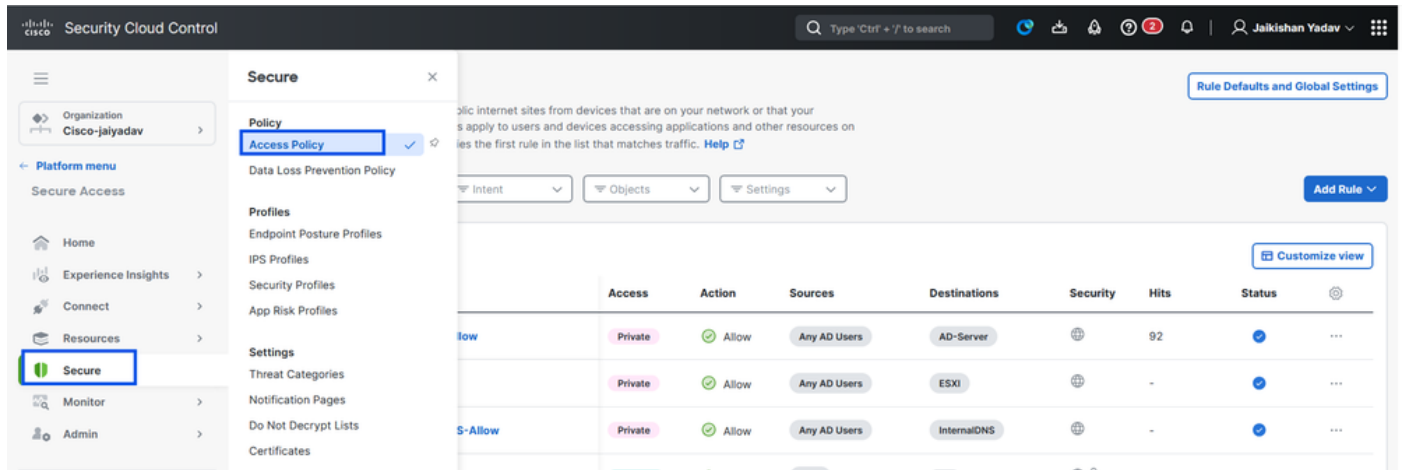
注：選択する登録のタイプ（IPアドレスまたは非IPアドレス）に応じて、この変更によりPRがFTDに自動的に関連付けられ、ポリシーの導入がトリガーされます。

7. 「保存」をクリックします。

手順2：プライベートアクセスルールの作成

Secure Access上のプライベートアクセスを、ユニバーサルZTA登録済みユーザによるアクセスとなるように設定します (デフォルト)。詳細については、「[プライベートアクセスルール](#)」を参照してください

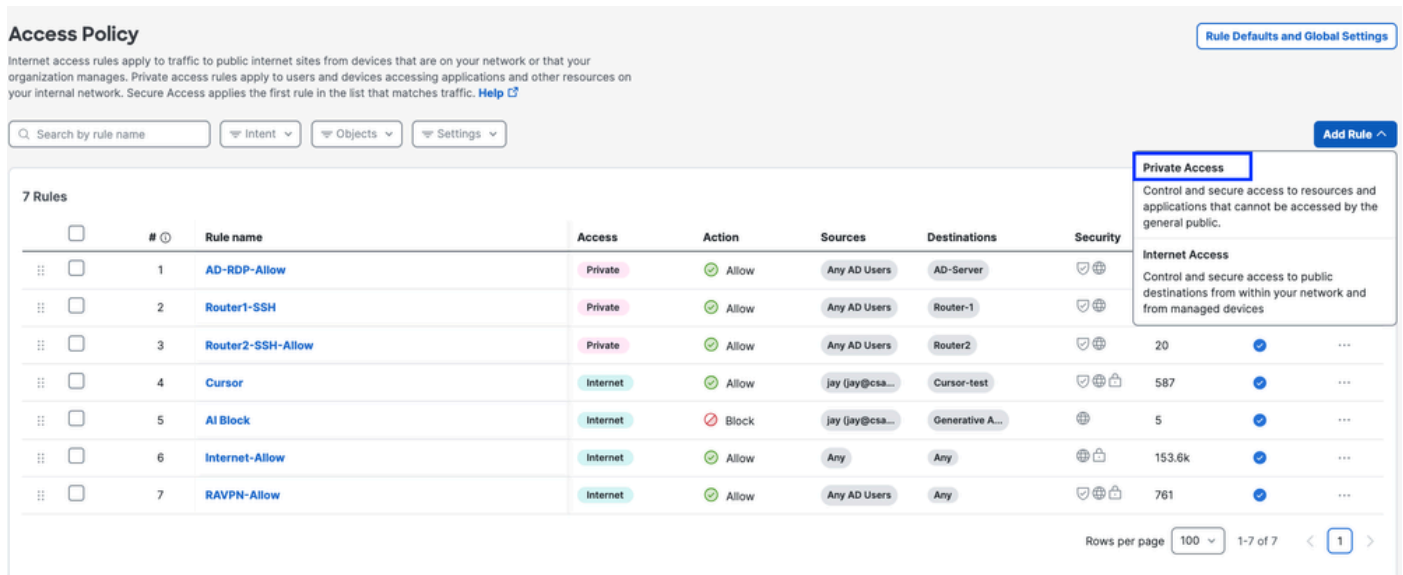
1. Secure > Access Policyの順に移動します。



セキュアアクセス：アクセスポリシーの設定

2. Add Ruleをクリックし、Private Accessを選択します。

ルールの上には、ルールの設定済みコンポーネントを説明する要約が表示されます。



セキュアアクセス：アクセスポリシーの設定

3. ルール名の追加

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.

セキュアアクセス：アクセスポリシーの設定

4. ルール処理を選択し、ソースと宛先を選択します

Rule name Rule order

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

To

+ AND

セキュアアクセス：アクセスポリシーの設定

5. エンドポイント要件の設定

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

セキュアアクセス：アクセスポリシーの設定

6. セキュリティの設定

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

セキュアアクセス：アクセスポリシーの設定

7. Saveをクリックします。

Access Policy Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings Add Rule

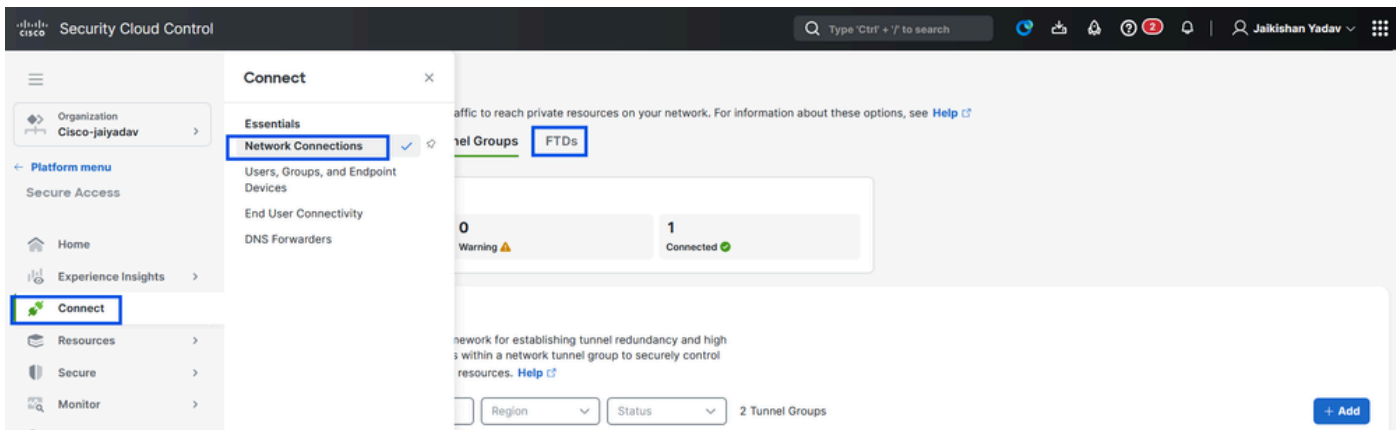
#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	Router3-SSH-Allow	Private	Allow	Any AD Users	Router3	Shield	-	On
2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	Shield	-	On
3	Router1-SSH	Private	Allow	Any AD Users	Router-1	Shield	-	On
4	Router2-SSH-Allow	Private	Allow	Any AD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

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

セキュアアクセス：アクセスポリシーの設定

手順3:FTDでのPRの関連付けを確認します

1. 「接続」>「ネットワーク接続」>「FTDs」に移動します。



セキュアアクセス – PR検証

2. 「FTD」をクリック>「このFTDに関連付けられたリソースの表示」をクリックします。

```
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
```

セキュアアクセス – PR検証

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Syncing ● 0 Synced ●

FTDs configured for Universal Zero Trust Access

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

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

Trusted network: LAN (Default trusted network) Networks: 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](#)

セキュアアクセス – PR検証

```
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

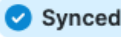
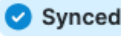
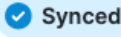
Name: ftd.csa.local
Addresses: 192.168.1.12
```

セキュアアクセス - PR検証

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

セキュアアクセス – PR検証

3. 「閉じる」をクリックします。

4. ステータスを確認します (図1の矢印Aを参照)。関連するリソースと設定は同期済み状態である必要があります

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)
 Networks: 1 DNS Domains, 1 DNS Servers
 Edit assignment + Trusted network

Associated Resources
 RESOURCES ASSOCIATED BY STATUS
 Status: Synced (3)
 View resources associated to this FTD
 Associate Resources

セキュアアクセス – PR検証

5. 設定がFTDにプッシュされたことを確認します。

FTD cliにログインし、LINAモードに移動します。

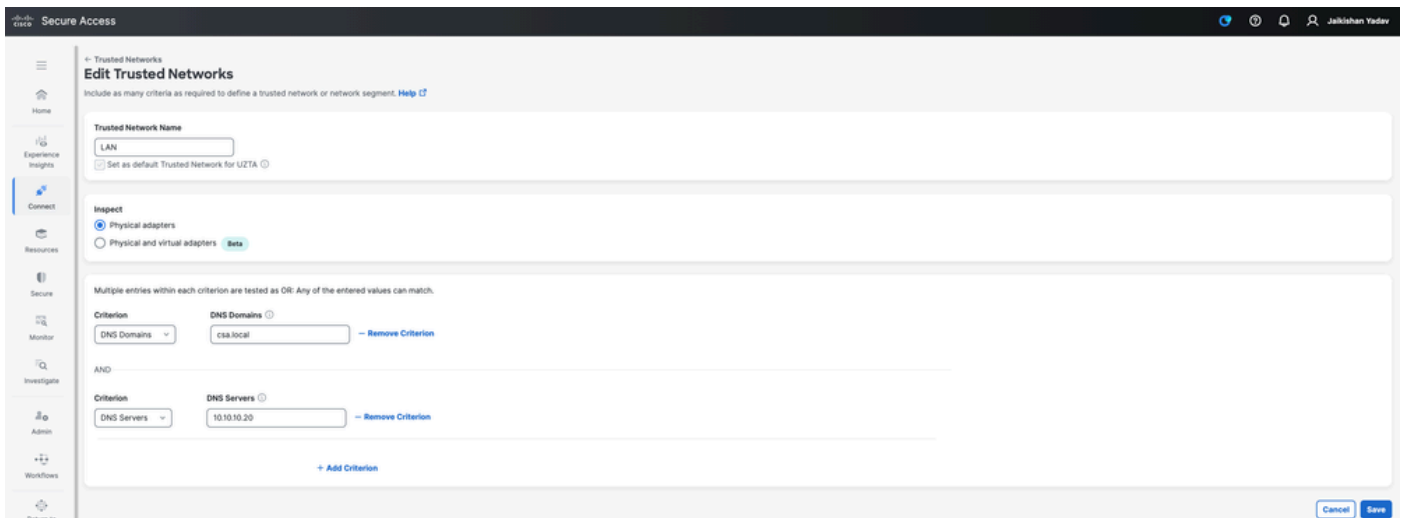
show running-config object application

```
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
```

セキュアアクセス – PR検証

ステップ4: 「信頼できるネットワークまたはZTA設定の管理」の設定または確認

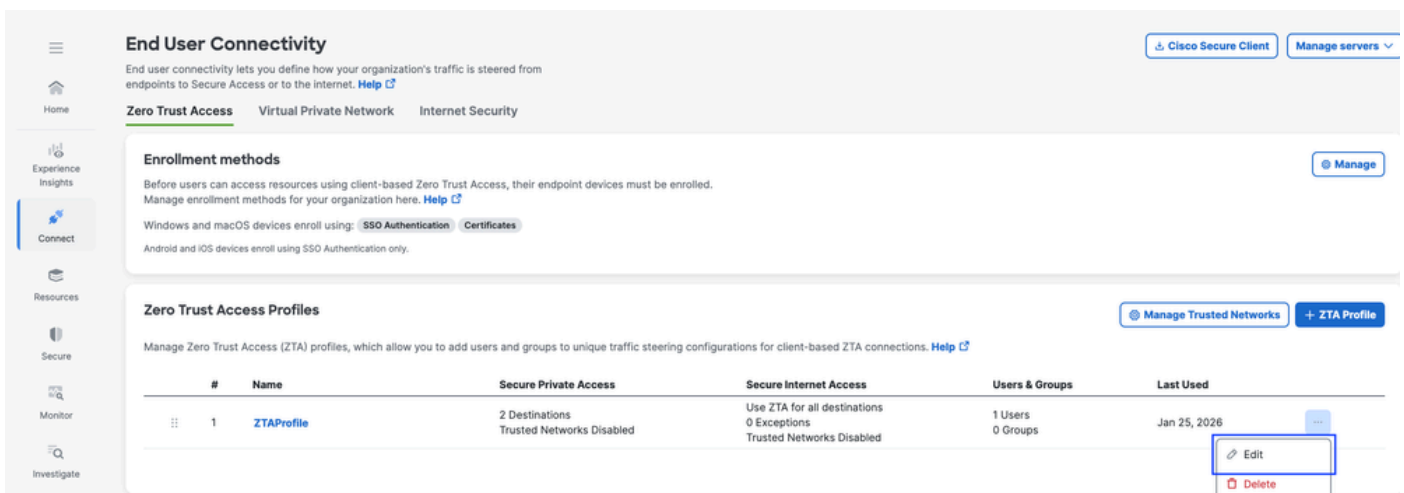
Connect > End User Connectivity > Zero Trust Access > ZTA Settingsの順に移動し、Trusted Networksを設定します。



セキュアアクセス : ZTA TNDの設定

ステップ5 ZTAプロファイルへのプライベートリソースの追加

1. Connect > End User Connectivity > Zero Trust Accessの順に移動し、3つのドットをクリックしてZTAプロファイルを編集します



セキュアアクセス – ZTAプロファイル

2. プライベートリソースの追加

The screenshot shows the 'Create profile' page for 'ZTAProfile'. The 'Secure Private Access' step is active, showing a table of destinations and private resources. A tooltip is visible on the right side of the table.

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.

セキュアアクセス - ZTAプロフィール

The screenshot shows the 'Edit profile' page for 'ZTAProfile'. A modal window titled 'Add private resources' is open, showing a list of private resources to be added to the profile.

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.

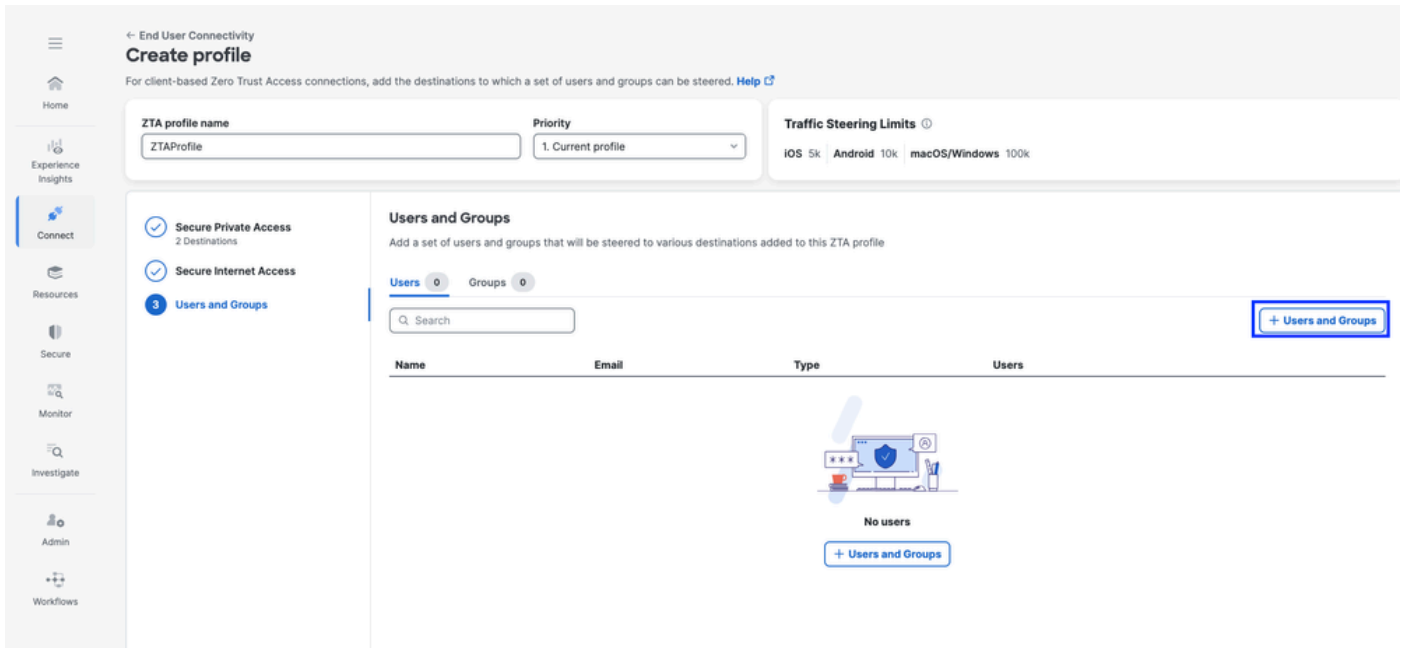
Private Resource

- 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)

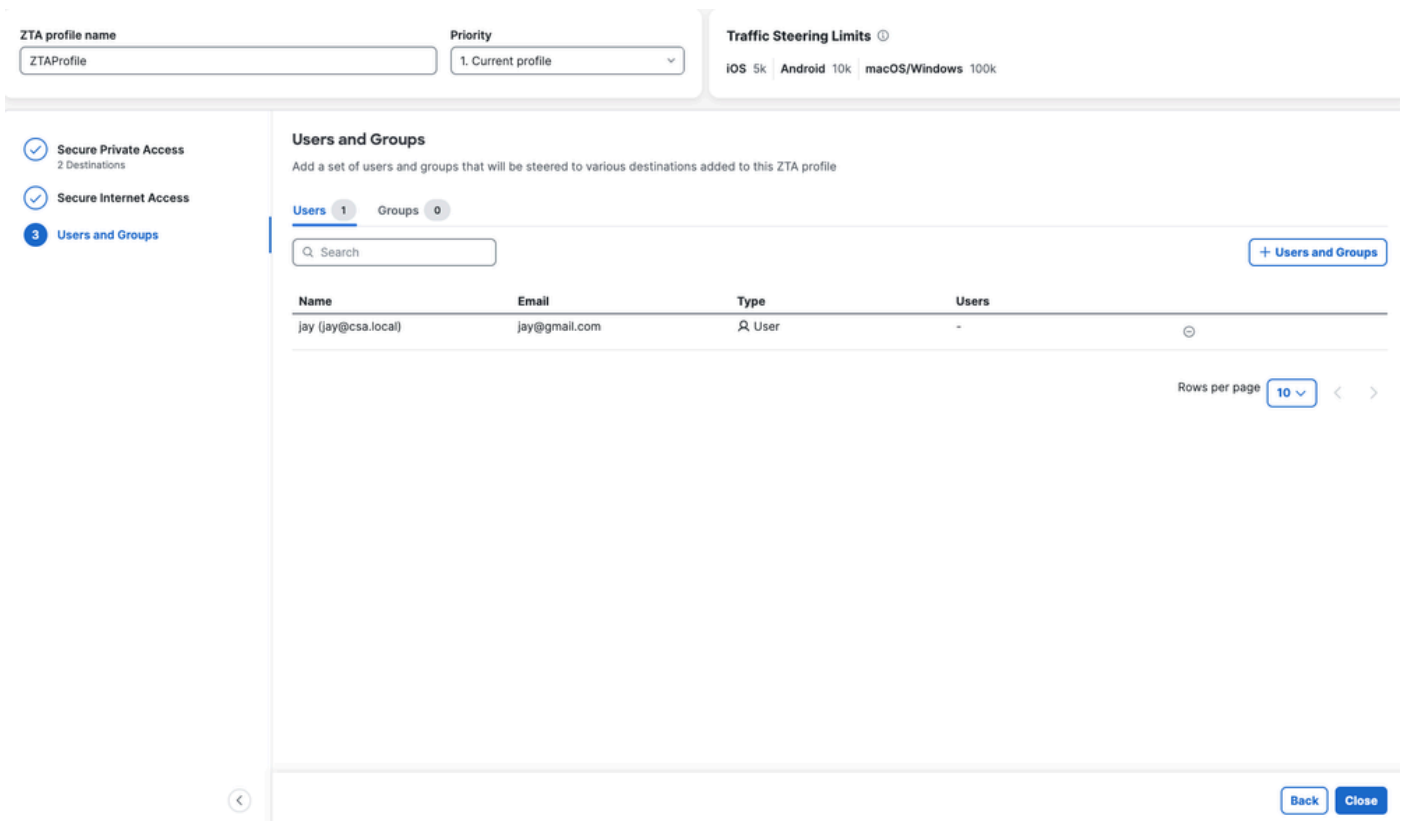
Cancel Save

セキュアアクセス - ZTAプロフィール

3. ユーザーとグループの追加



セキュアアクセス - ZTAプロフィール

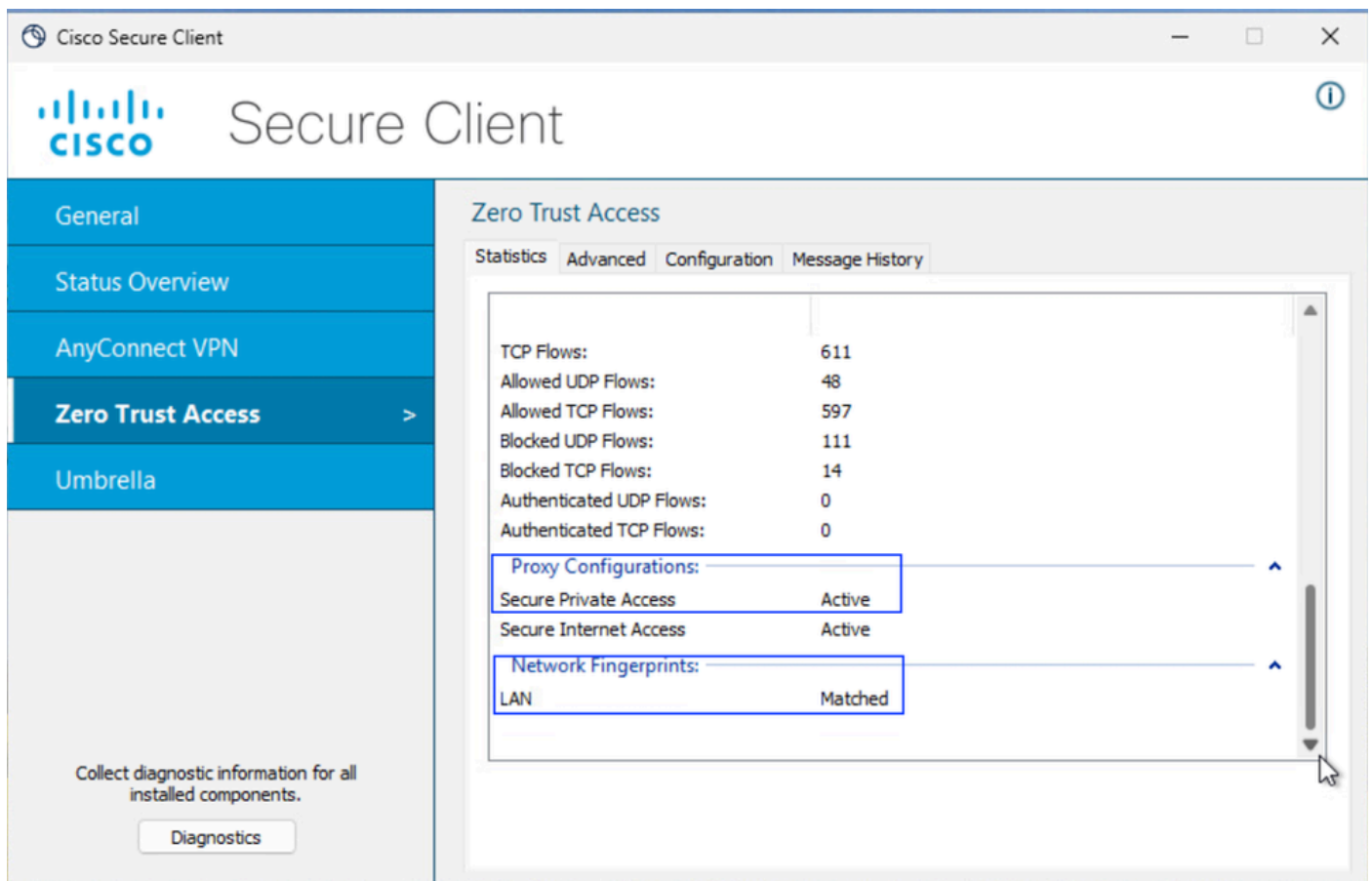


セキュアアクセス - ZTAプロフィール

手順6 : プライベートリソースへのアクセスを確認する

ユーザがローカルの場合

1. ZTA TNDのネットワークフィンガープリントを確認します。ユーザがローカルで、セキュアプライベートアクセスがアクティブであるかどうかで一致する必要があります。



セキュアなアクセス – PRテスト

2. リモートユーザがFTD FQDNを解決できることを確認します

```
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
```

セキュアなアクセス - PRテスト

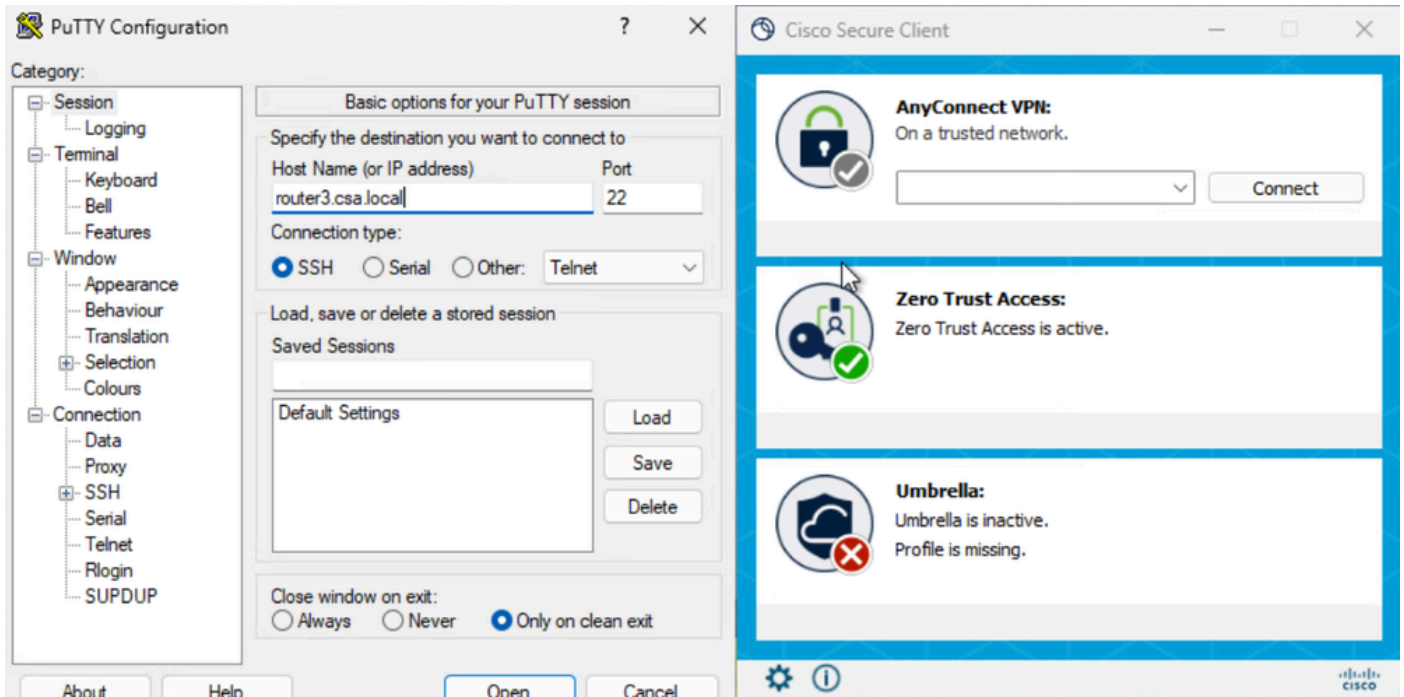
3. FTDがFQDNを使用してプライベートリソースに到達できることを確認します。

```
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# █
```

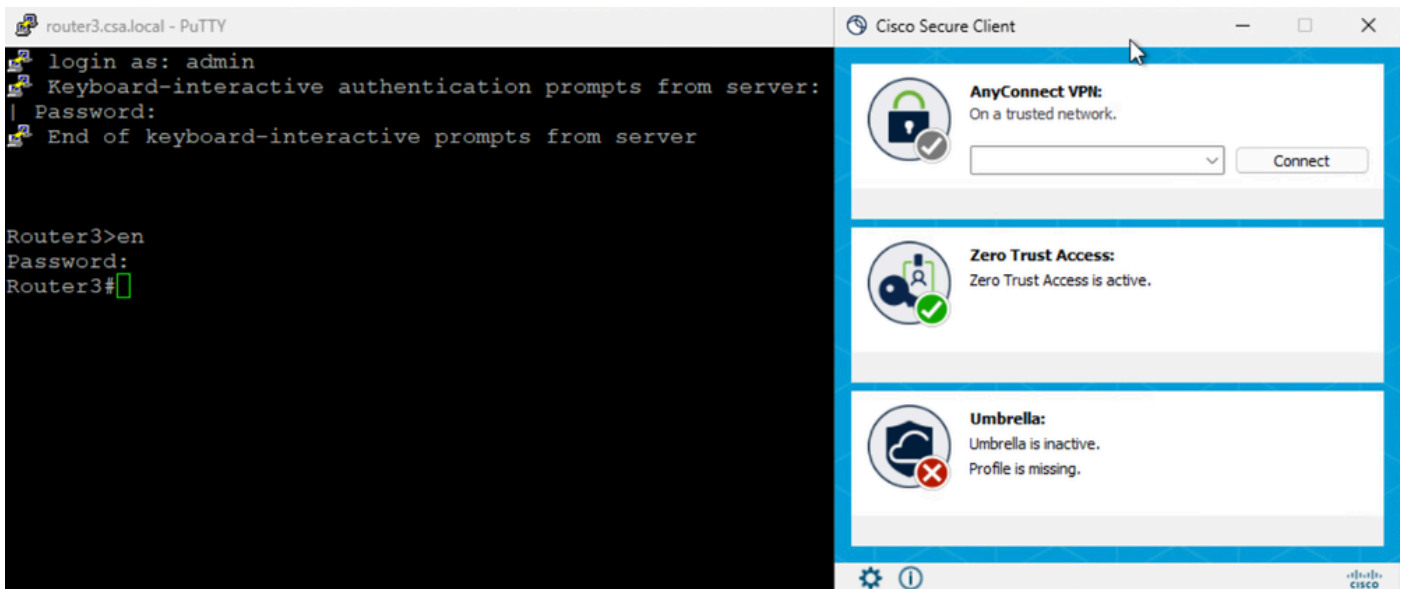
セキュアなアクセス - PRテスト

4. プライベートリソースへのSSH接続をテストする

FQDNを使用してPRにアクセスします

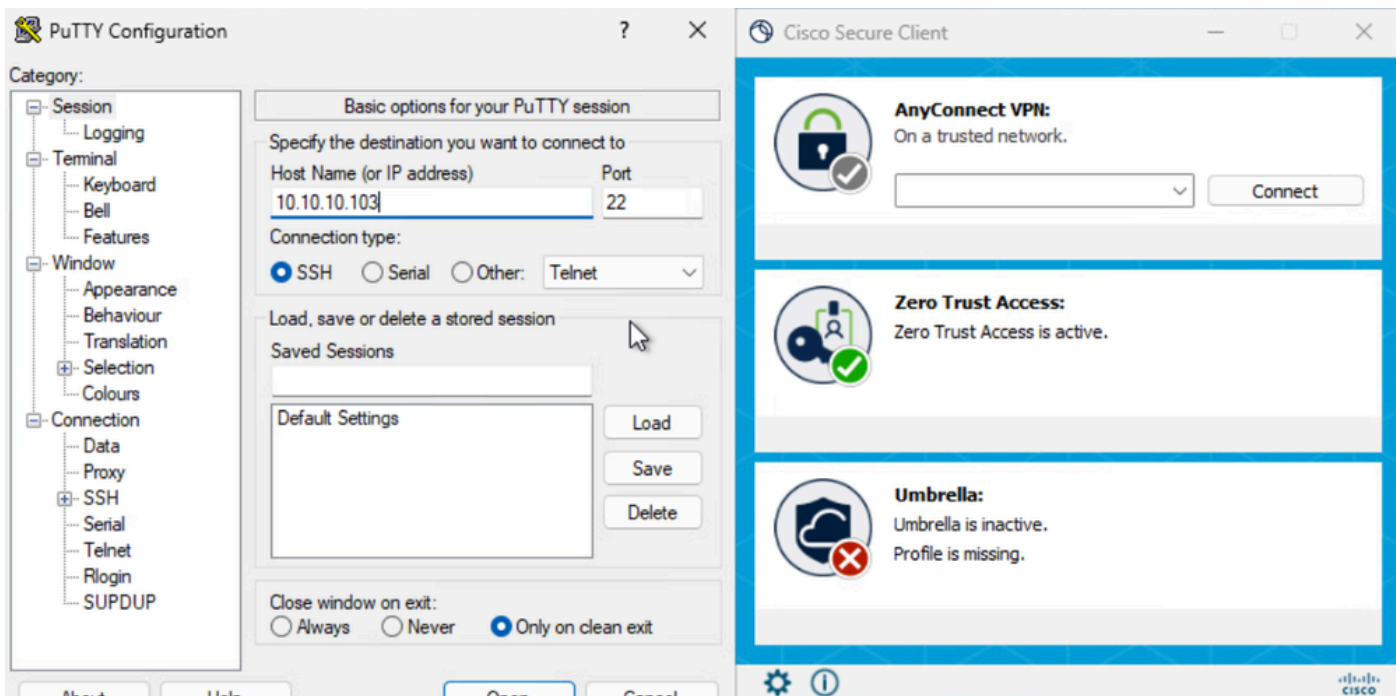


セキュアなアクセス - PRテスト

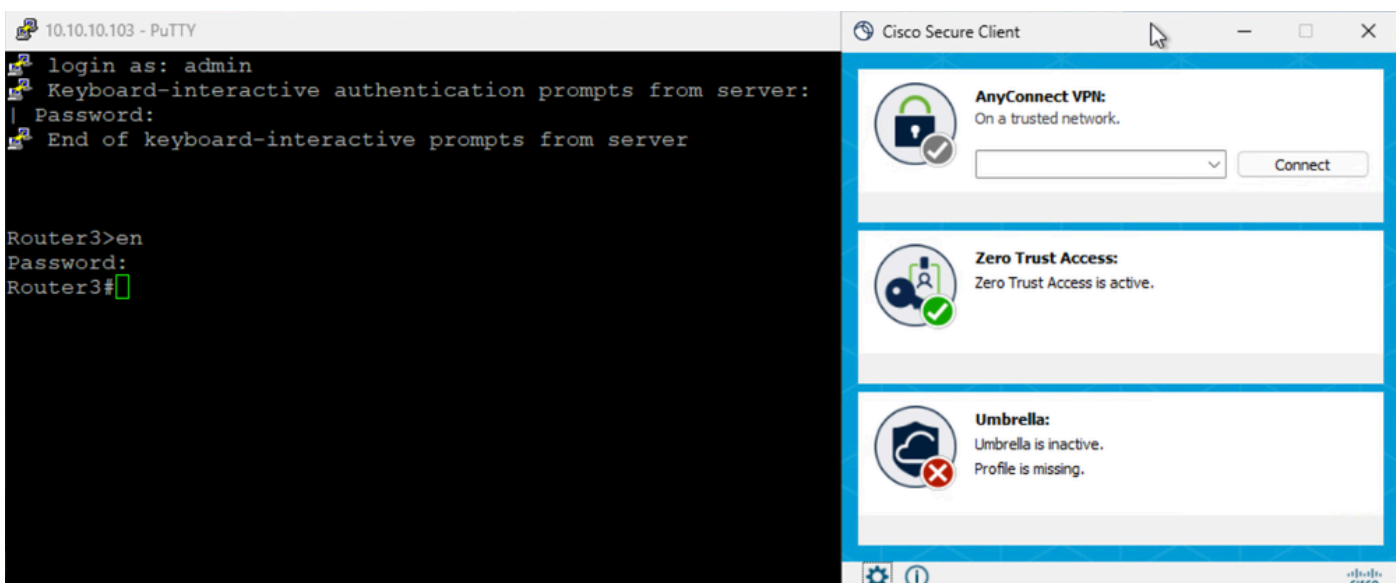


セキュアなアクセス - PRテスト

IPアドレスを使用してPRにアクセスします



セキュアなアクセス – PRテスト



セキュアなアクセス – PRテスト

5. セキュアアクセスアクティビティの検索ログの確認

Activity Search

Search by domain, identity, or URL

Filters: DOMAIN router3.csa.local

4 Total Viewing activity from Feb 22, 2026 6:41 AM to Feb 23, 2026 6:41 AM

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840

セキュアアクセス – アクティビティ検索

Activity Search

Search by domain, identity, or URL

Filters: RESPONSE Allowed

26 Total Viewing activity from Feb 22, 2026 6:41 AM to Feb 23, 2026 6:41 AM

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router3.csa.local		22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed				
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed				
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed				
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed				
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed				
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed				
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102:22	22	Allowed				
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102:22	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow	win 10.0.26200.7840

Event Details

Allowed

Block Reason

Connection Method
ZTA Client-based

Time
Feb 23, 2026 6:40 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
LAN

Enforcement Point
FTD> FMC_FTD

Destination
router3.csa.local

Destination IP

セキュアアクセス – アクティビティ検索

6. FMC接続イベントの確認

Firewall Management Center

Events & Logs / Analysis / Unified Events

Search

Destination IP: 10.10.10.103

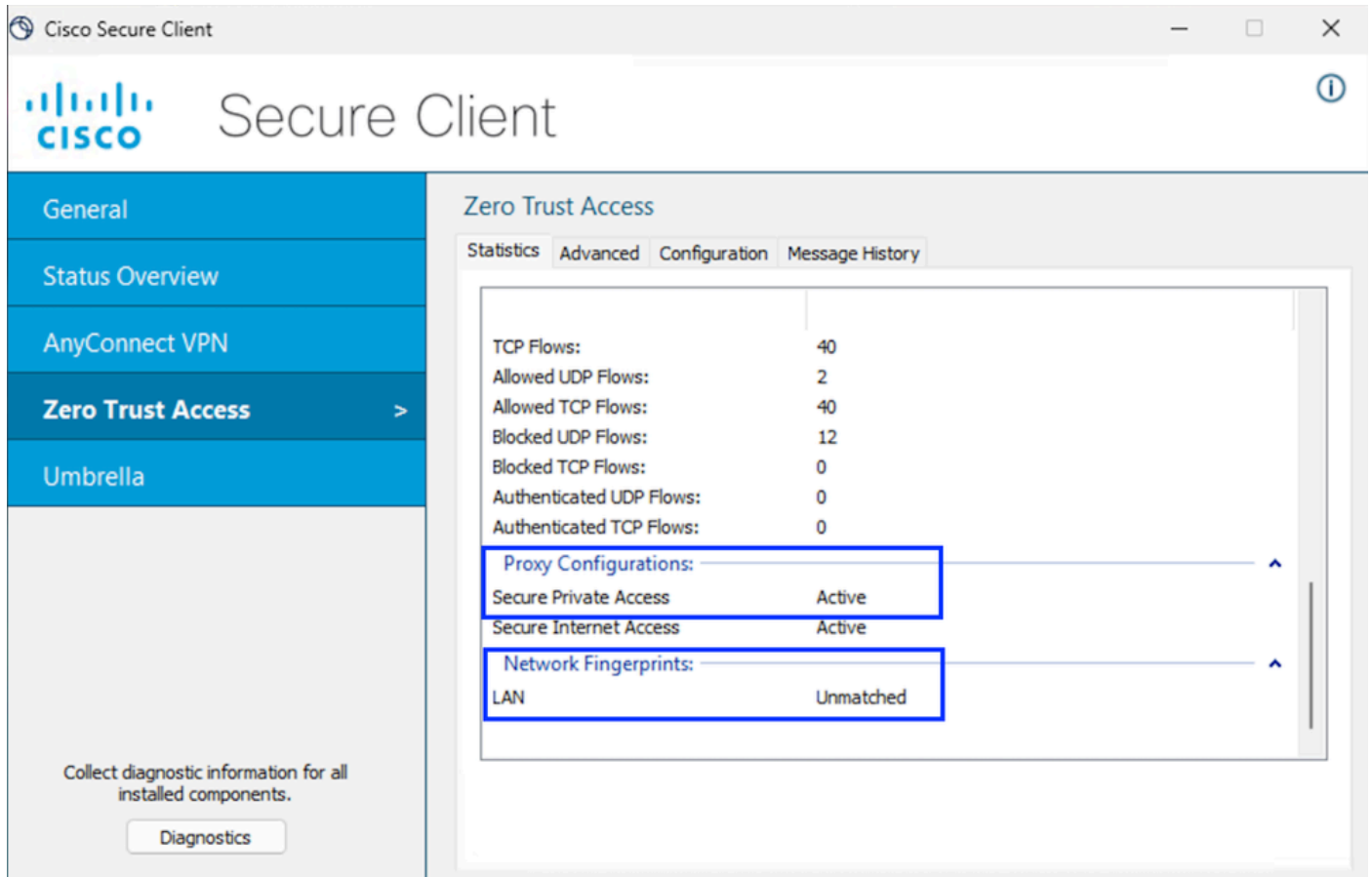
4 events

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Type	Web Application	Access Control Rule
2026-02-23 01:40:54	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.103	37877 / tcp	22 (ssh) / tcp		
2026-02-23 01:40:47	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.103	22981 / tcp	22 (ssh) / tcp		
2026-02-23 01:40:41	Connection	Allow	Zero Trust Flow	169.254.1186	10.10.10.103	57951 / tcp	22 (ssh) / tcp		
2026-02-23 01:40:33	Connection	Allow	Zero Trust Flow	169.254.1198	10.10.10.103	51673 / tcp	22 (ssh) / tcp		

FMC接続イベント

ユーザがリモートの場合

1. ZTA TNDのネットワークフィンガープリントを確認します。ユーザがリモートの場合には一致しません



The screenshot shows the Cisco Secure Client interface. The left sidebar contains navigation options: General, Status Overview, AnyConnect VPN, Zero Trust Access (selected), and Umbrella. The main content area is titled 'Zero Trust Access' and has tabs for Statistics, Advanced, Configuration, and Message History. The 'Statistics' tab is active, displaying a table of network flow statistics. Below the statistics, there are expandable sections for 'Proxy Configurations' and 'Network Fingerprints'. The 'Network Fingerprints' section is expanded, showing 'LAN' with a status of 'Unmatched'.

Category	Value
TCP Flows:	40
Allowed UDP Flows:	2
Allowed TCP Flows:	40
Blocked UDP Flows:	12
Blocked TCP Flows:	0
Authenticated UDP Flows:	0
Authenticated TCP Flows:	0

Category	Status
Secure Private Access	Active
Secure Internet Access	Active

Category	Status
LAN	Unmatched

セキュアなアクセス – PRテスト

2. リモートユーザがFTD FQDNを解決できることを確認します

```

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

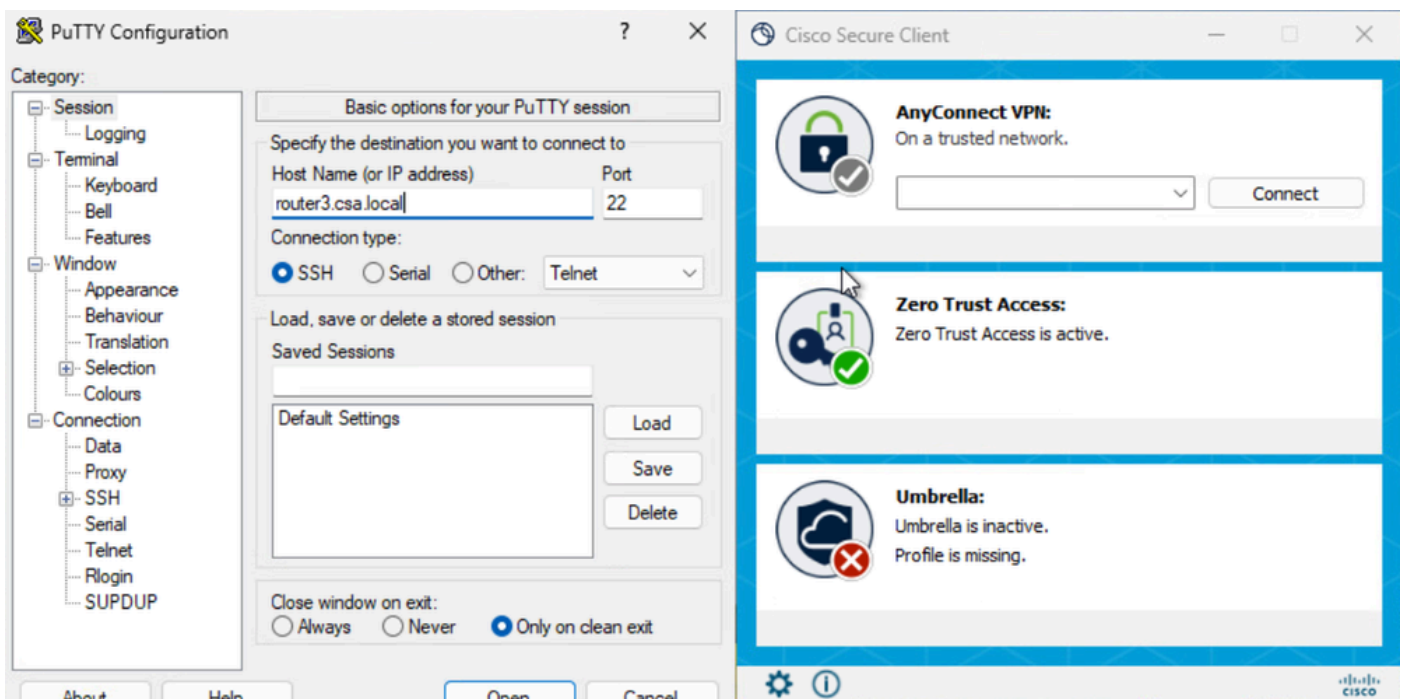
Name: ftd.csa.local
Addresses: 192.168.1.12

```

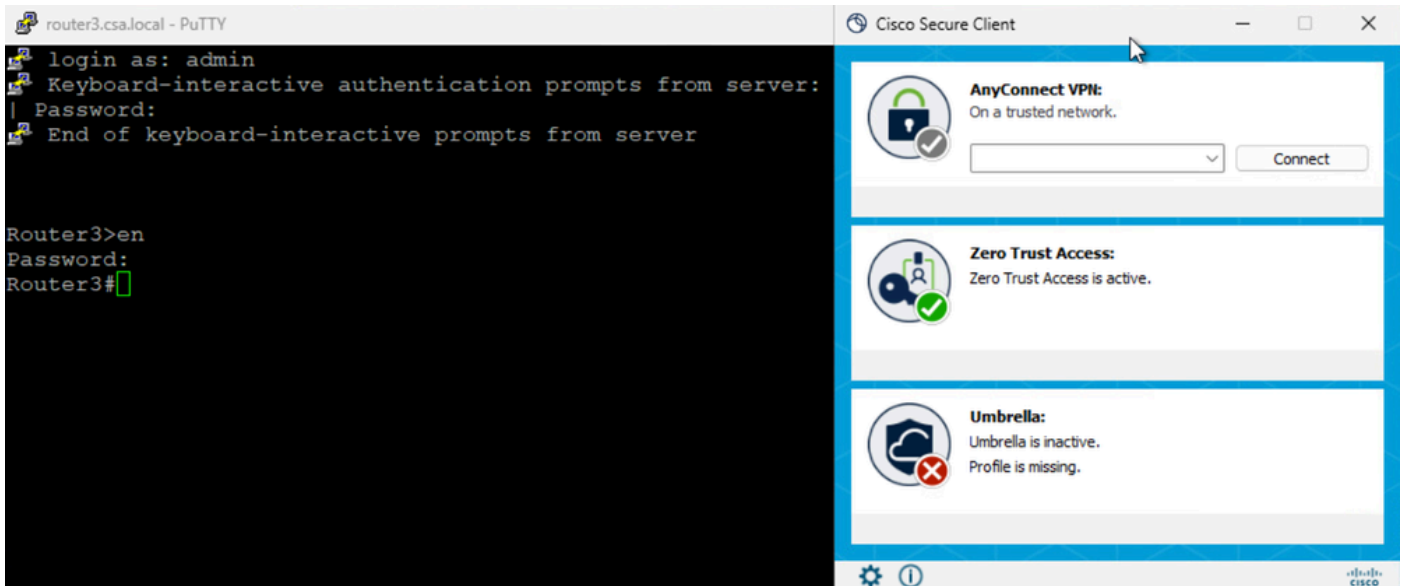
セキュアなアクセス – PRテスト

3. プライベートリソースへのSSH接続をテストする

FQDNを使用してPRにアクセスします

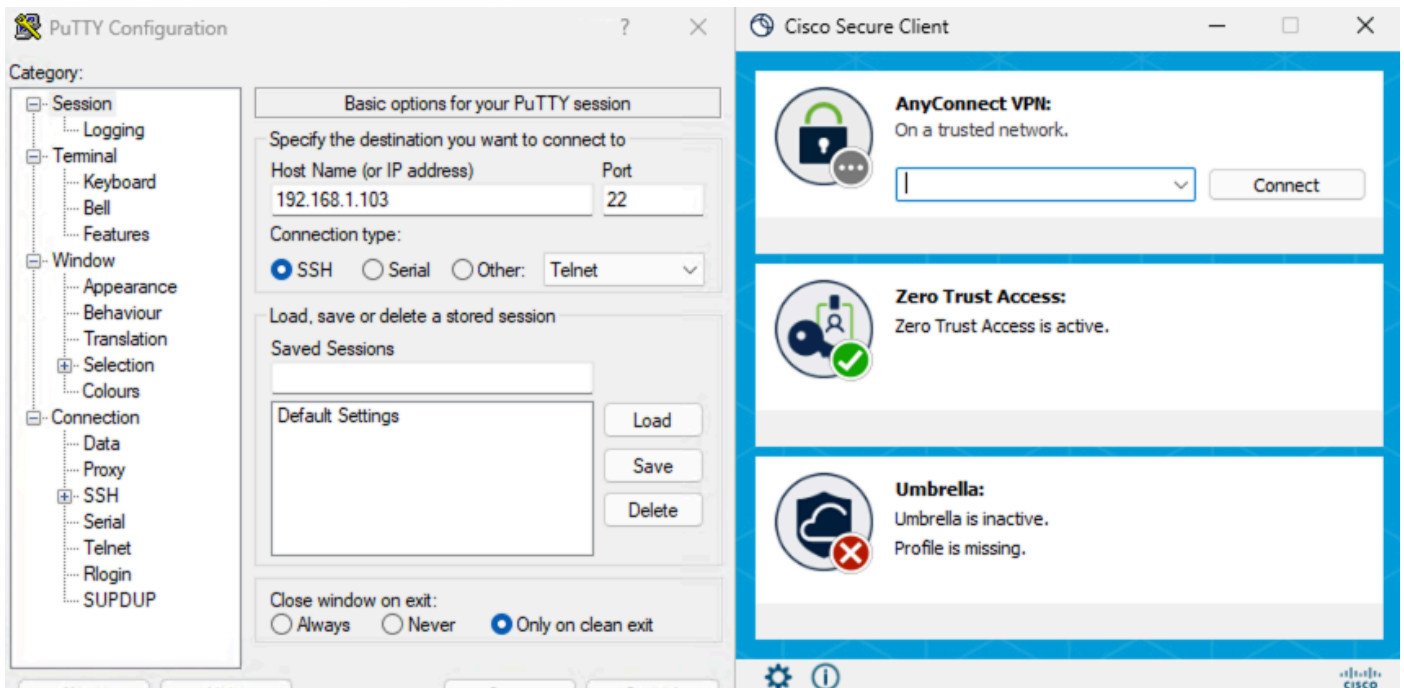


セキュアなアクセス – PRテスト

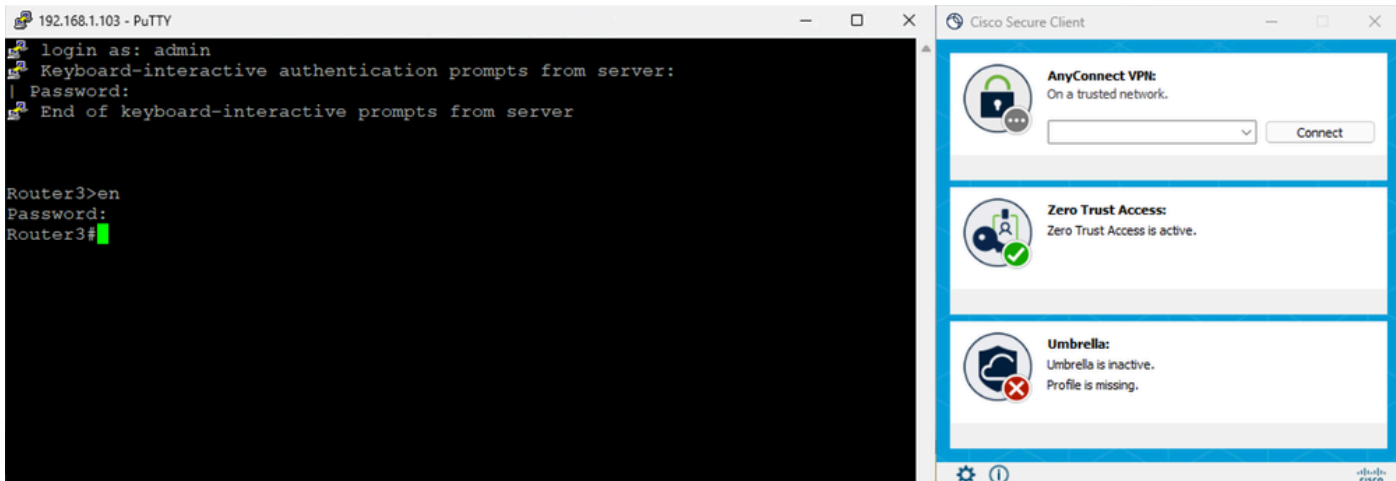


セキュアなアクセス - PRテスト

IPアドレスを使用してPRにアクセスします



セキュアなアクセス - PRテスト



セキュアなアクセス – PRテスト

5. セキュアアクセスアクティビティの検索ログの確認

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

セキュアアクセス – アクティビティ検索

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	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	10.10.10.103-22	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

トラブルシューティング

便利なコマンド:

- > show allocate-core profileの順に選択します。
- > show asp inspect-dp snort (隠しコマンド)
- > sh running-config universal-zero-trust (信頼できない場合)
- > show interface ip briefコマンド

> debug universal-zero-trust zproxy 7

! エキスパートモードに移行します

tail -f /ngfw/var/log/messages

show conn all

show nat detail

show asp table socket

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。