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

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

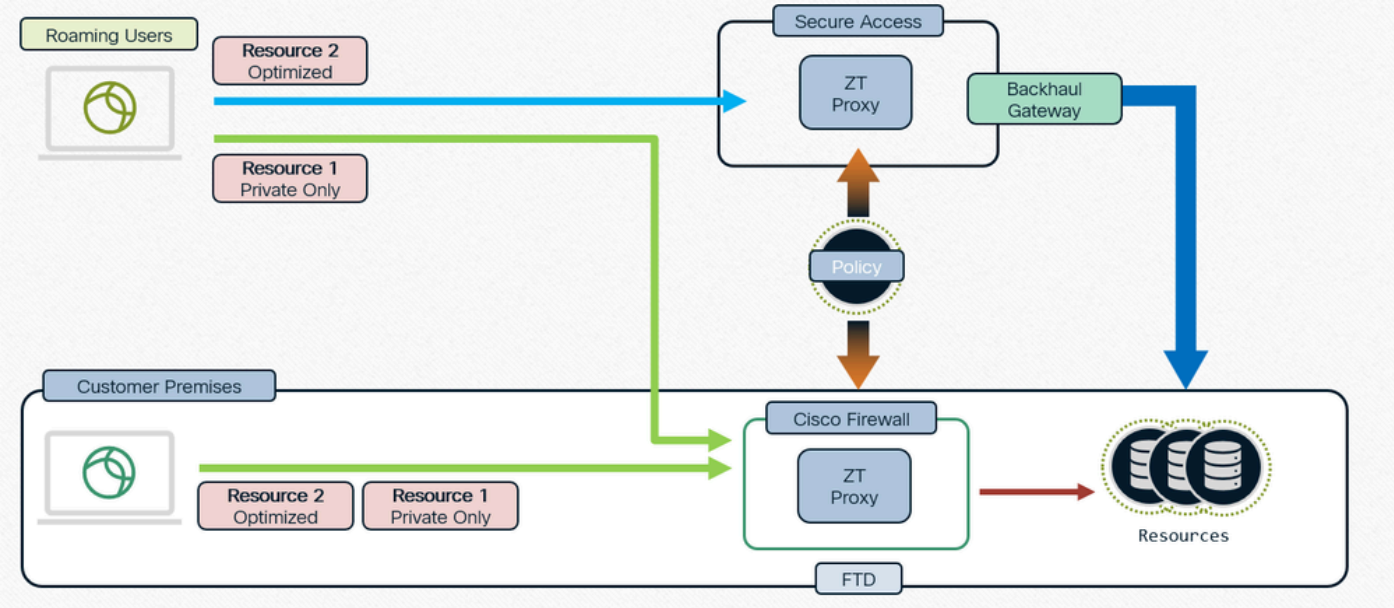
Universal zero trust network access(uZTNA)により、管理者はユーザID（ユーザの信頼とポスチャを含む）に従って、RA-VPNのようにネットワーク全体へのアクセスを許可することなく、内

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。

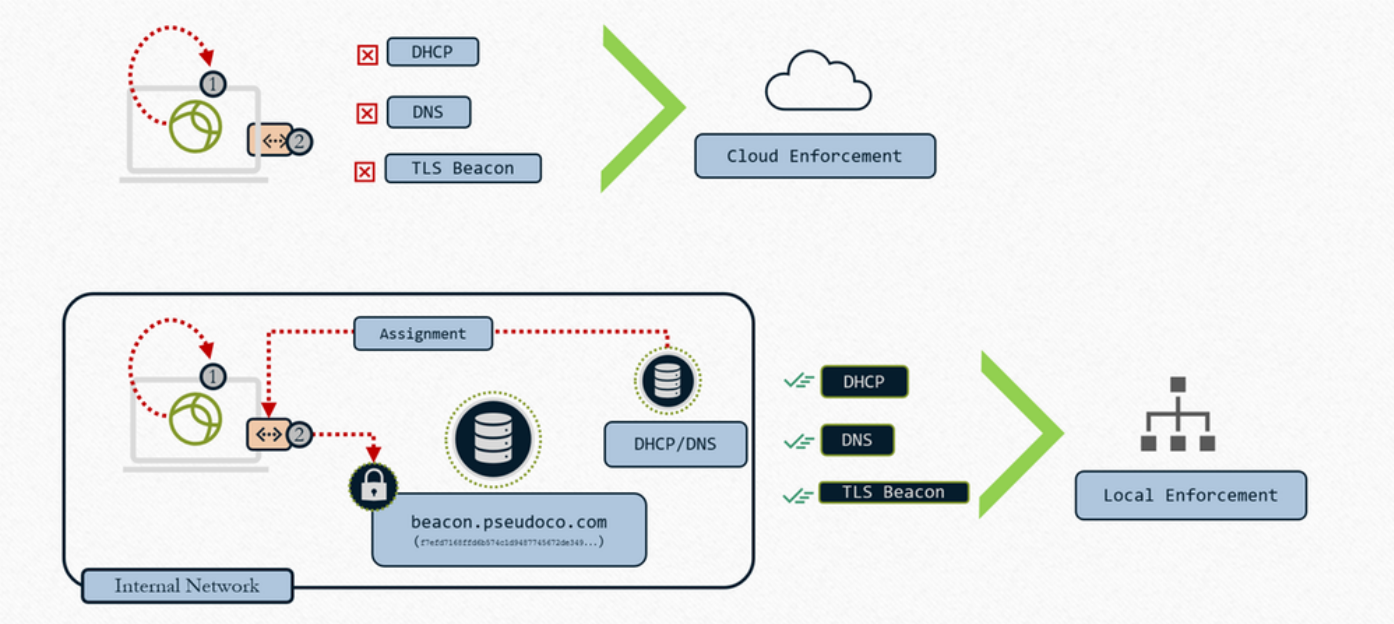
トラフィックプロキシと、IPS、ファイル、およびマルウェアのポリシー適用は、Firepower Threat Defense(FTD)で実行されます。



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

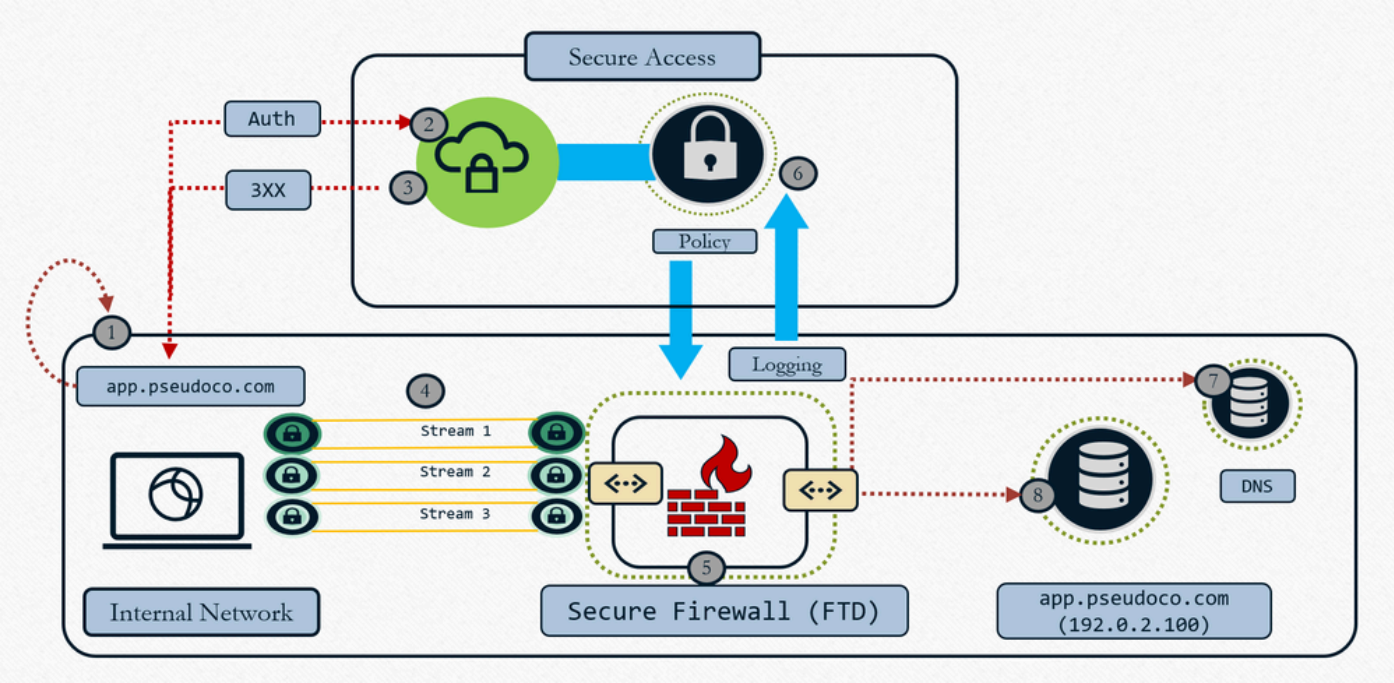
3 – 条件が一致した場合 – ローカル強制

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

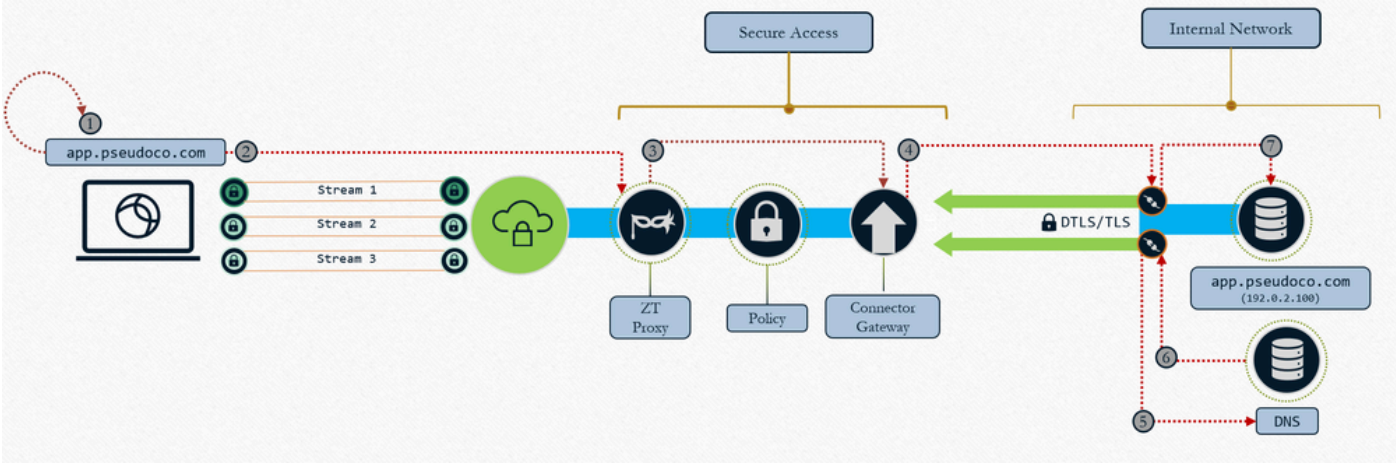
- ローカル強制パス：ファイアウォールの強制



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

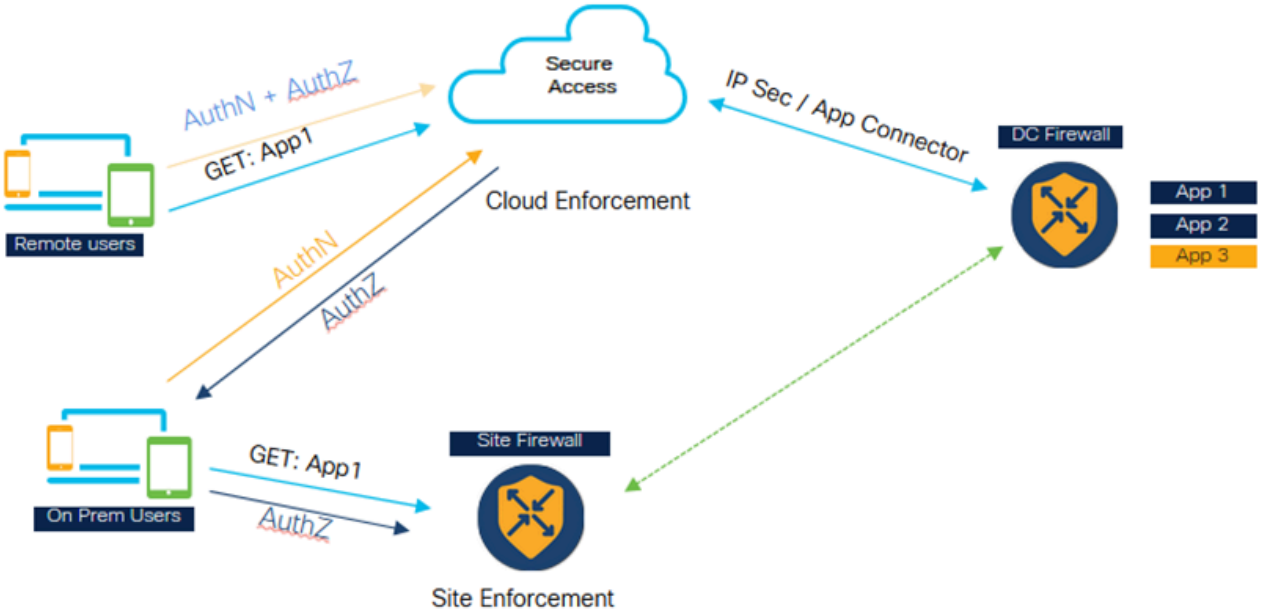


Universal ZTNA：クラウドの適用

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

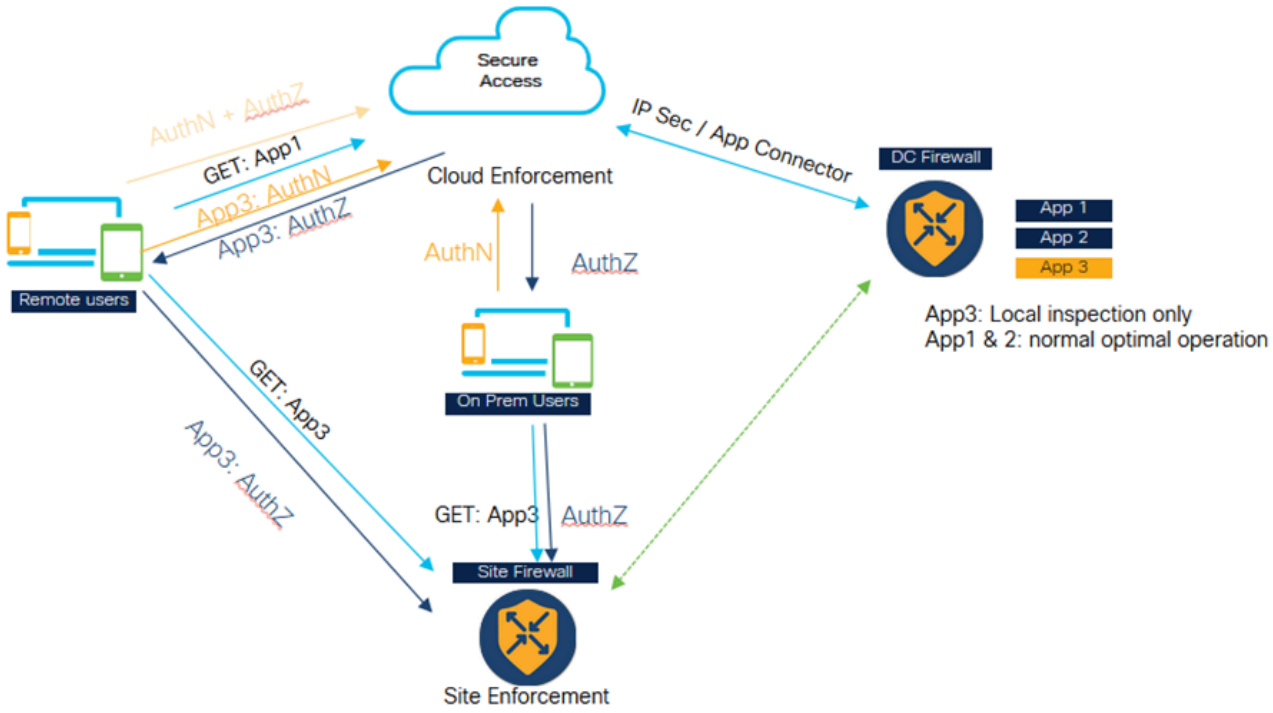
ケース1：オンプレミス時の一貫した最適化されたユーザ向けZTNA



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

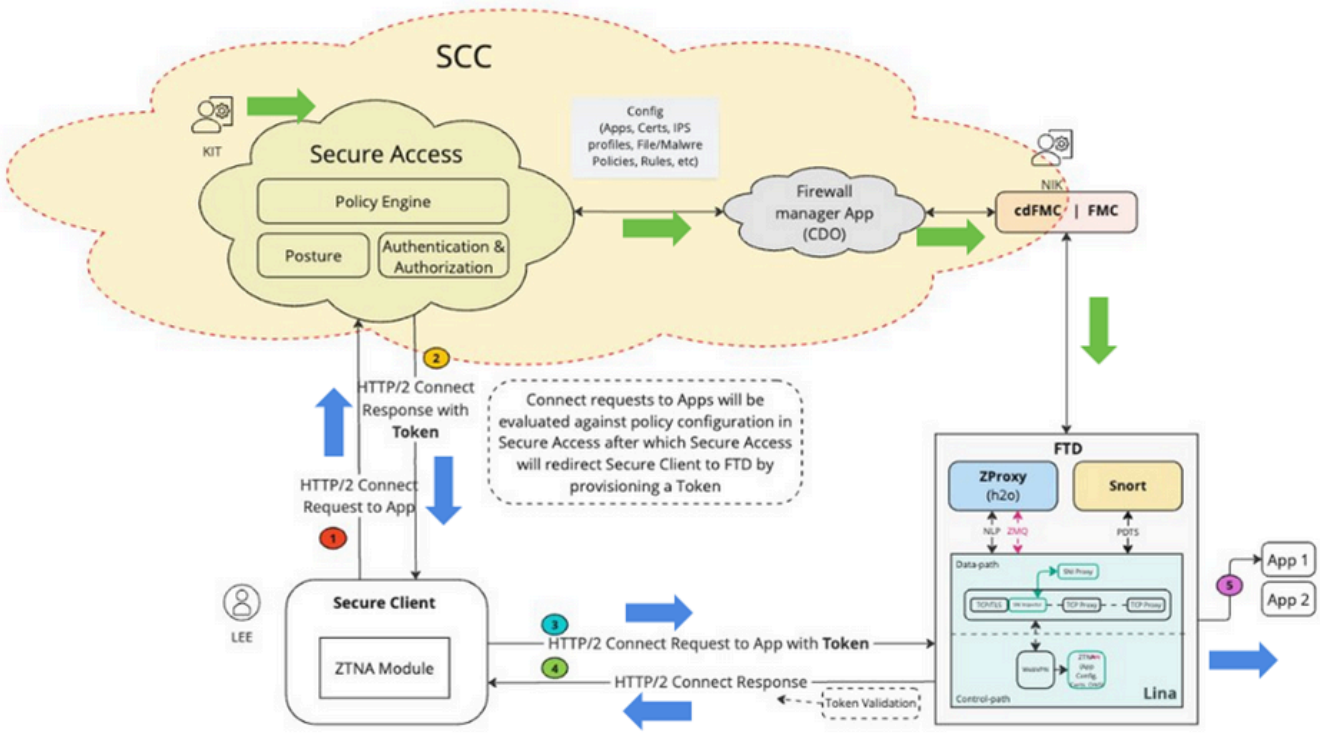
ケース2：機密アプリケーションの私的検査



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、リモートとオンパー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と、セキュアクライアントはmTLSチャ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

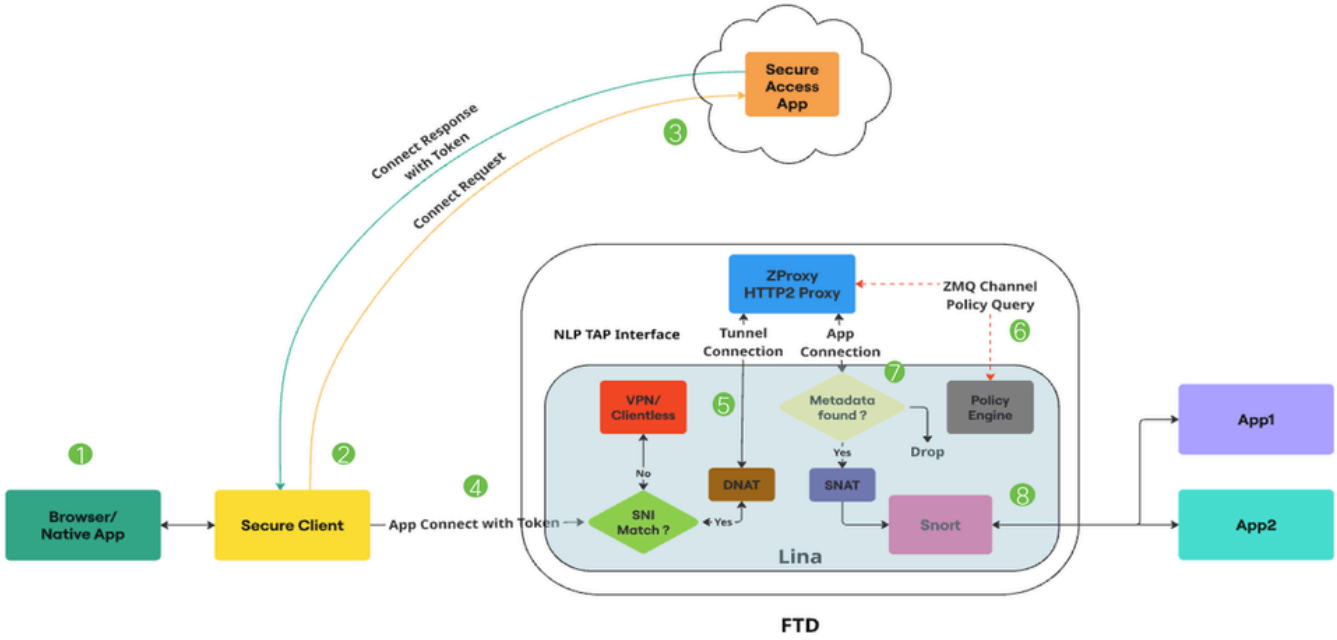
3. セキュアアクセスは、認証トークンとともにセキュアクライアントをFTDにリダイレクトします。

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出力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

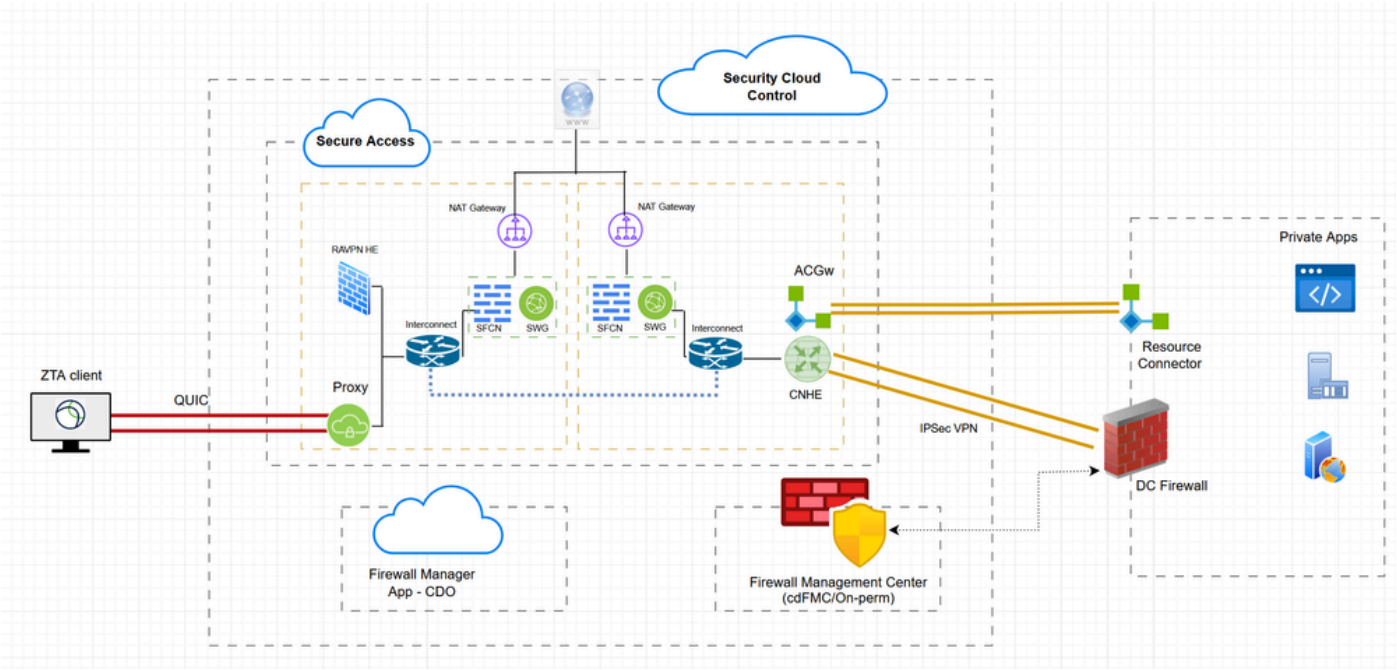
ペクション用にUniversal Zero Trust(UZT)フローをマークします。アクセストークンから取得したルールIDは、接続メタデータでSnortに渡されます。

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。 ルールの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

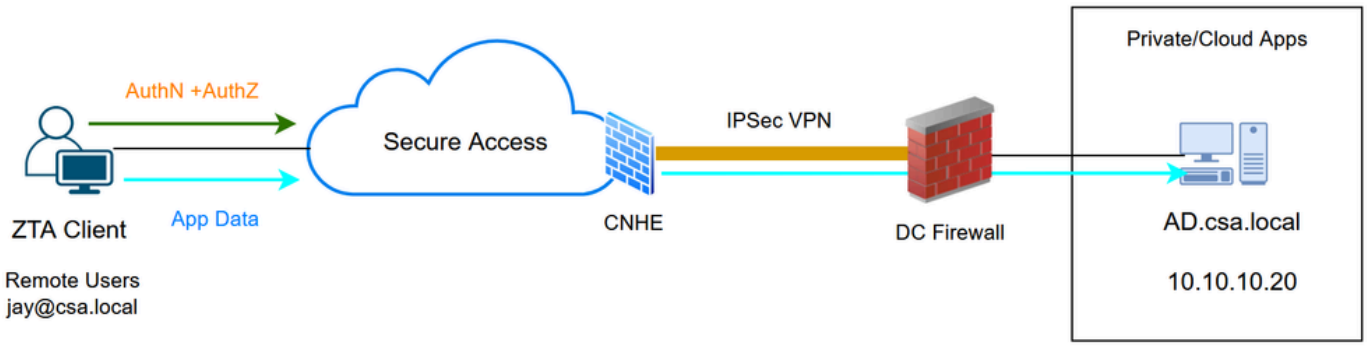


ハイブリッドZTNA：ネットワーク図

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

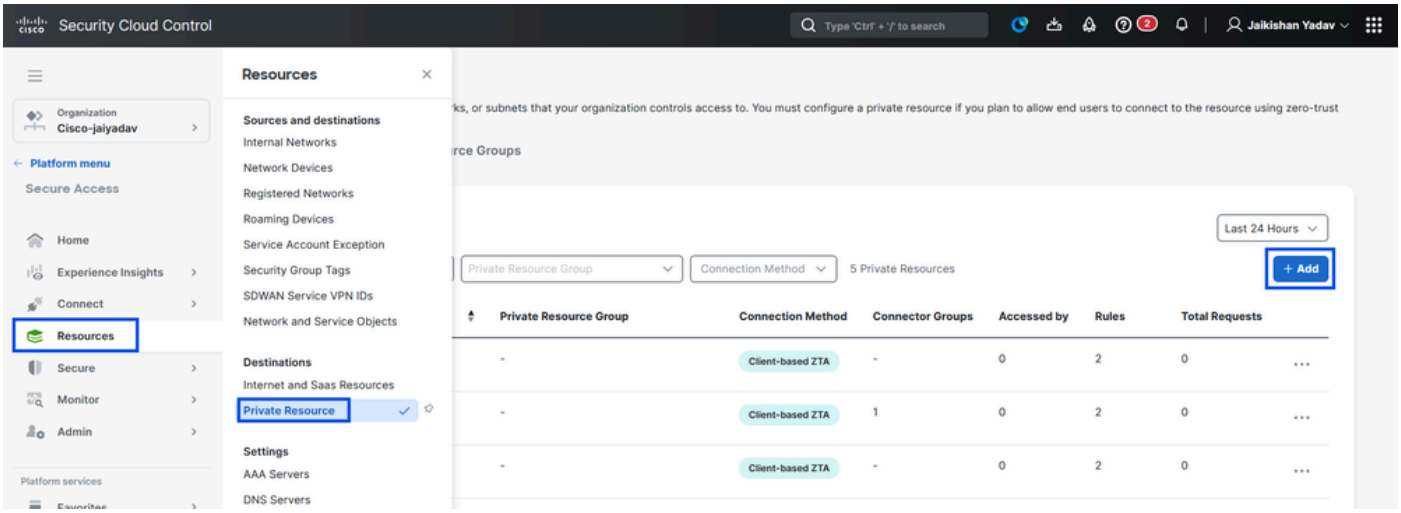


ユニバーサルZTA – テストケースのトポロジ

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

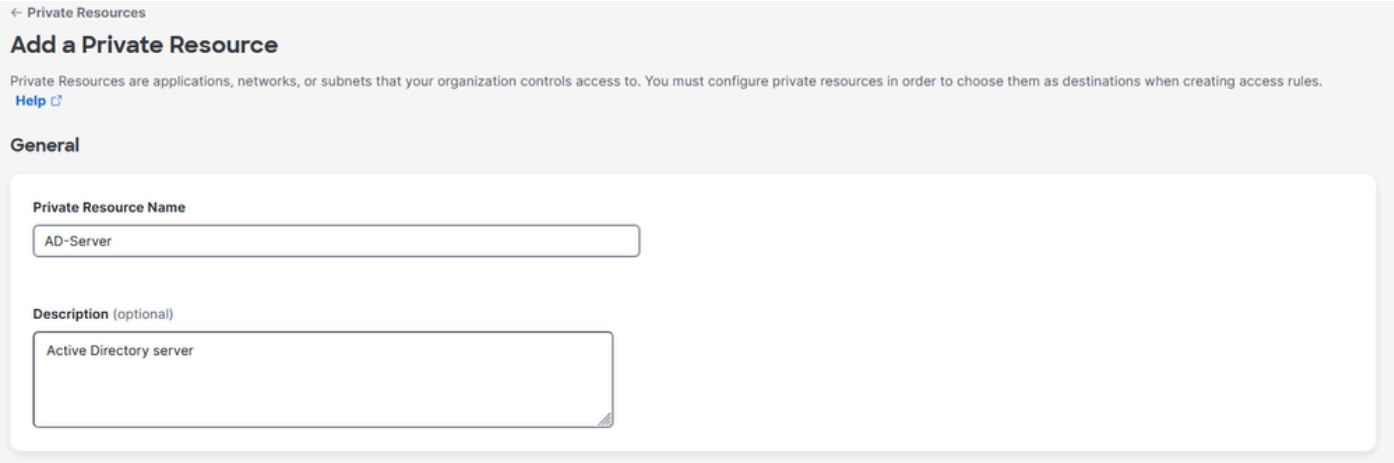
クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

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



セキュアアクセス：プライベートリソースの設定

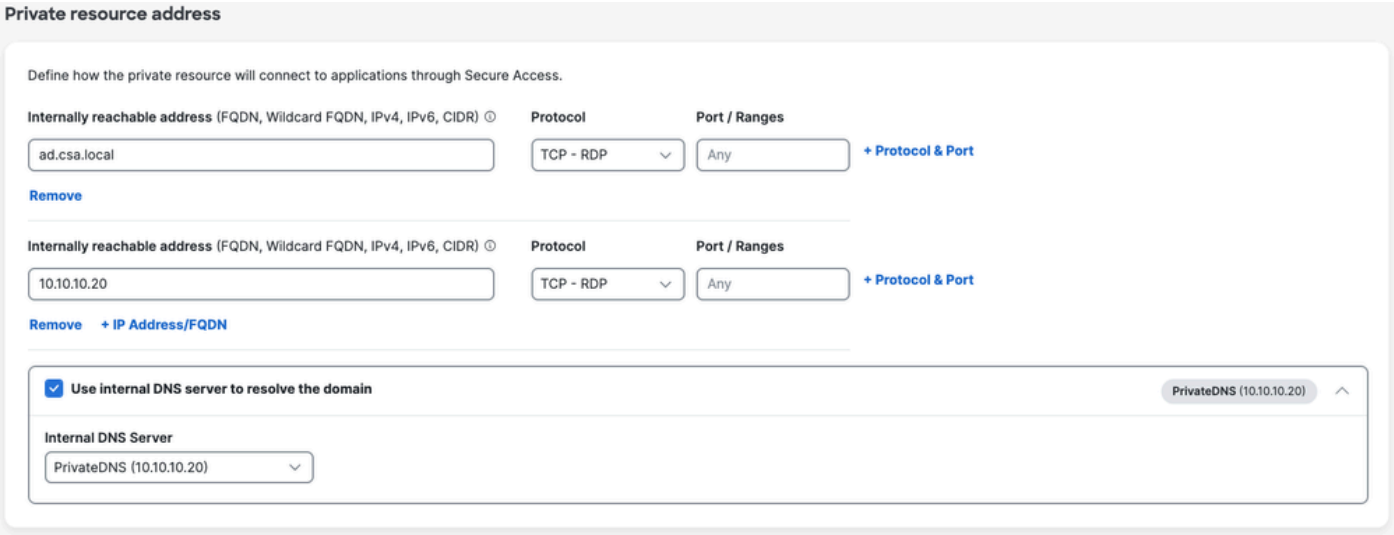
2.「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。



セキュアアクセス：プライベートリソースの設定

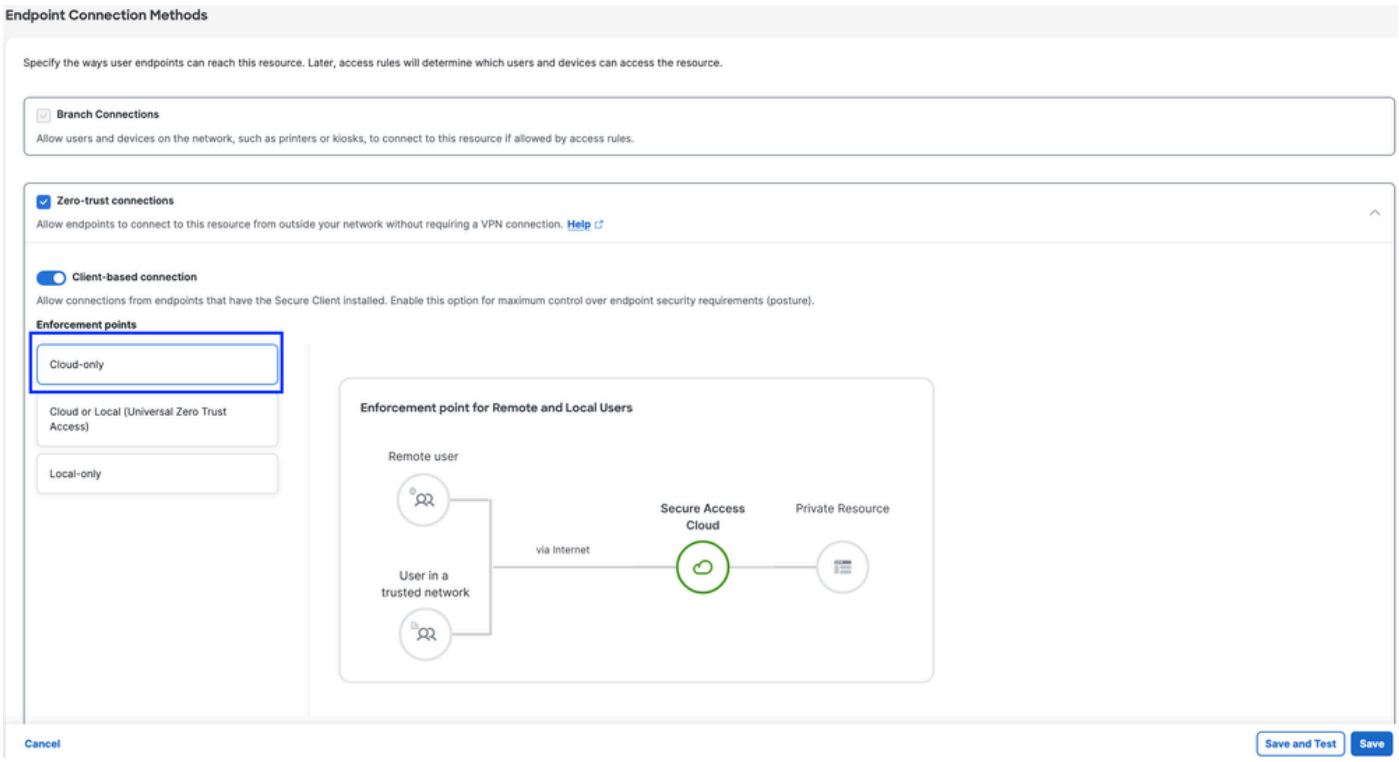
3. アクセスするプライベートリソースのFQDNを入力します。また、プライベートリソースのIPアドレスを定義することもできます。詳細については、「プライベートリソースの追加」を参照してください。

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



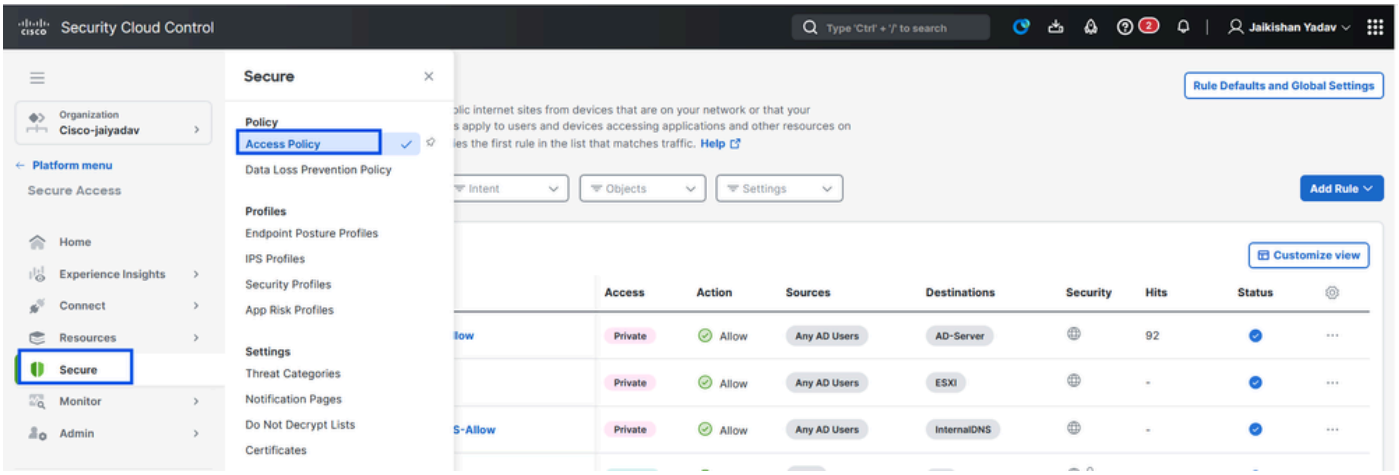
セキュアアクセス：プライベートリソースの設定

6. 「保存」をクリックします。

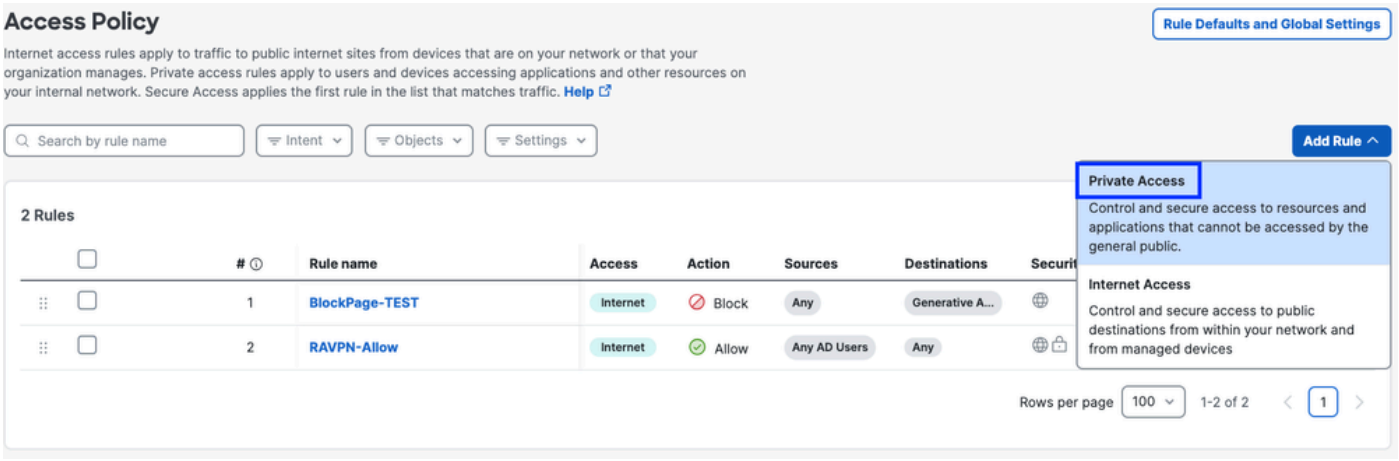
手順2：プライベートアクセスルールの作成

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

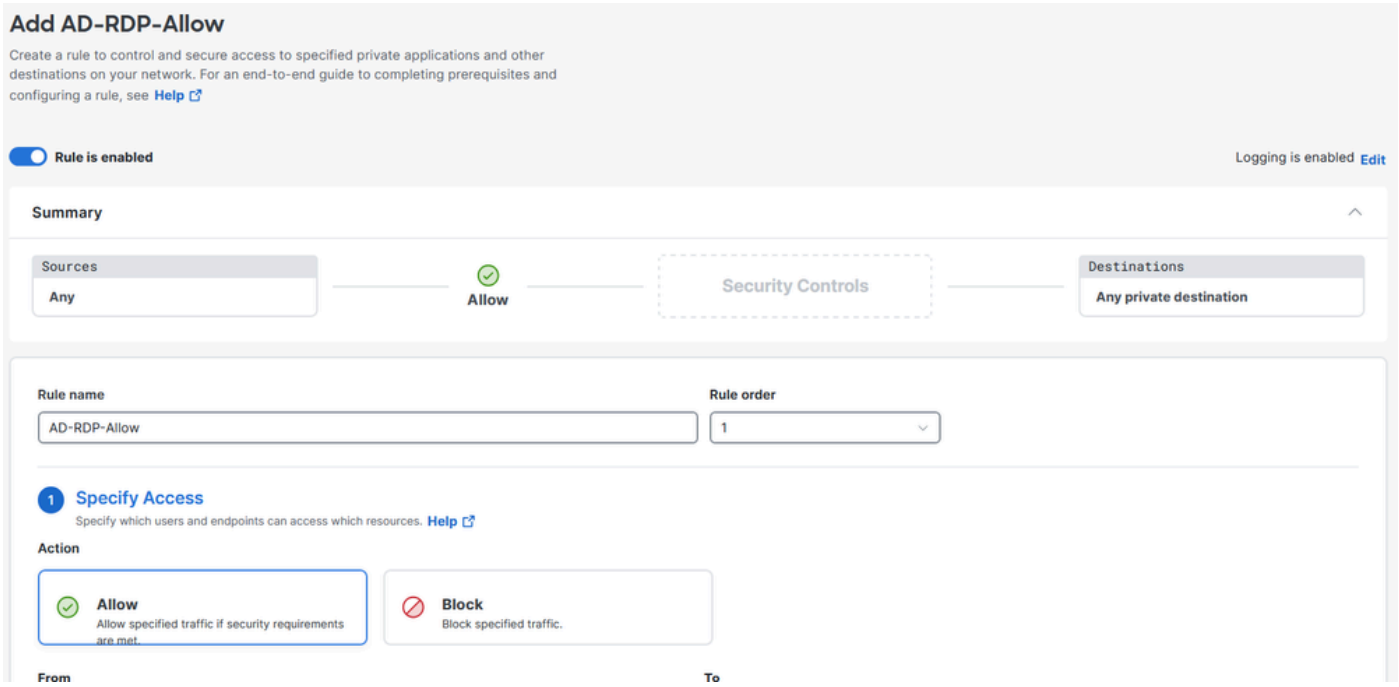
1. Secure > Access Policyの順に移動します。



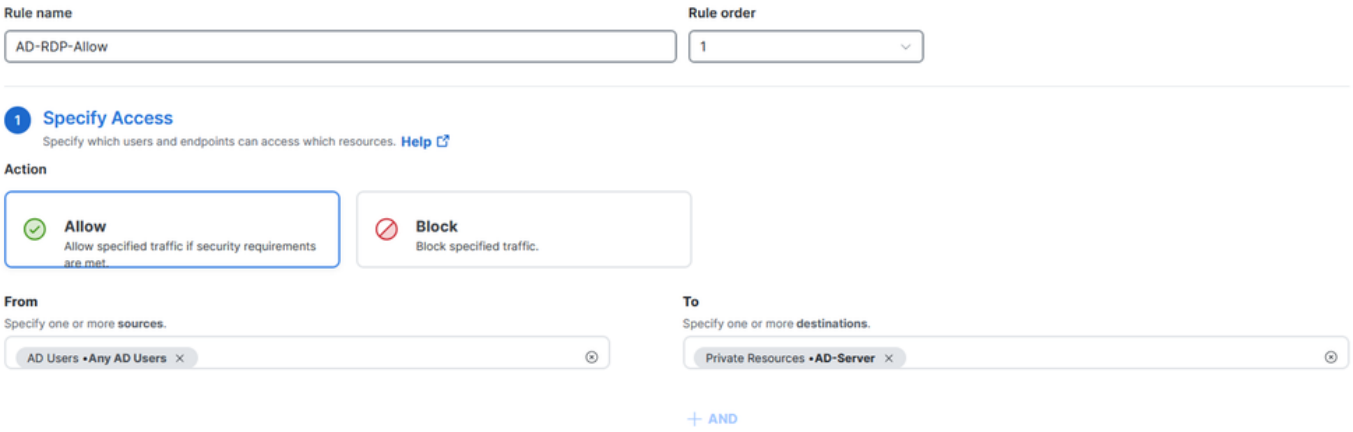
2. Add Ruleをクリックし、Private Accessを選択します。
ルールの上部には、ルールの設定済みコンポーネントを説明する要約が表示されます。



3. ルール名の追加

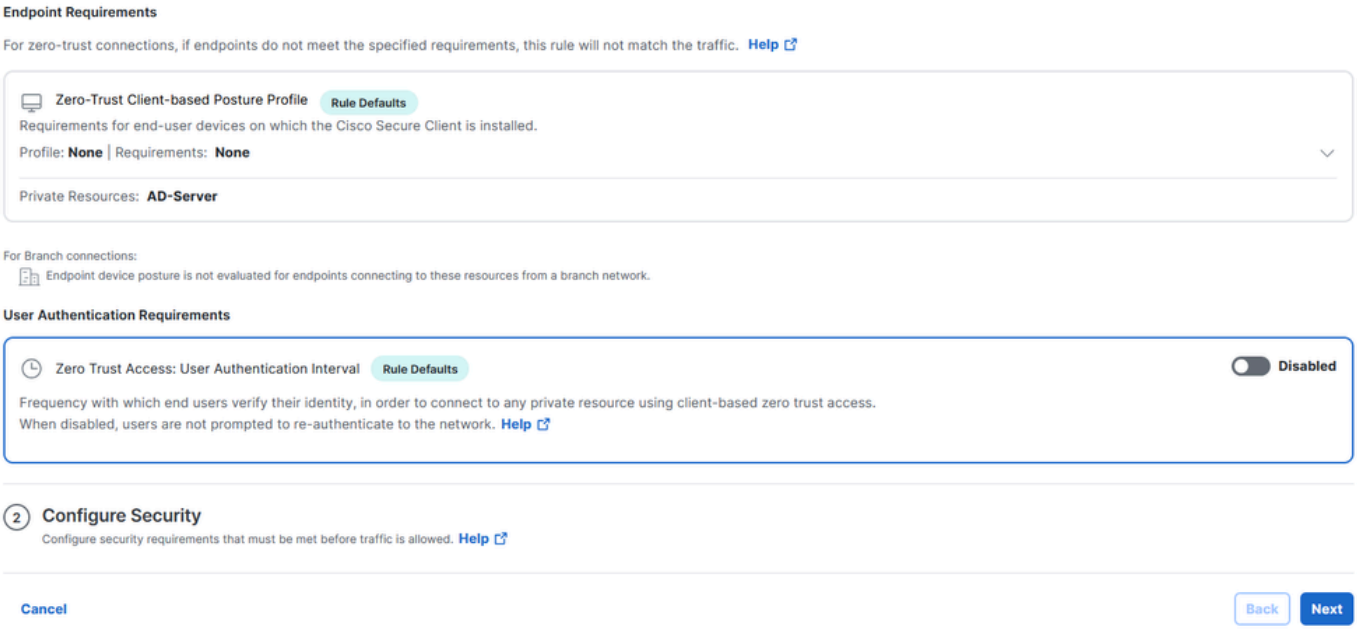


4. ルール処理を選択し、ソースと宛先を選択します



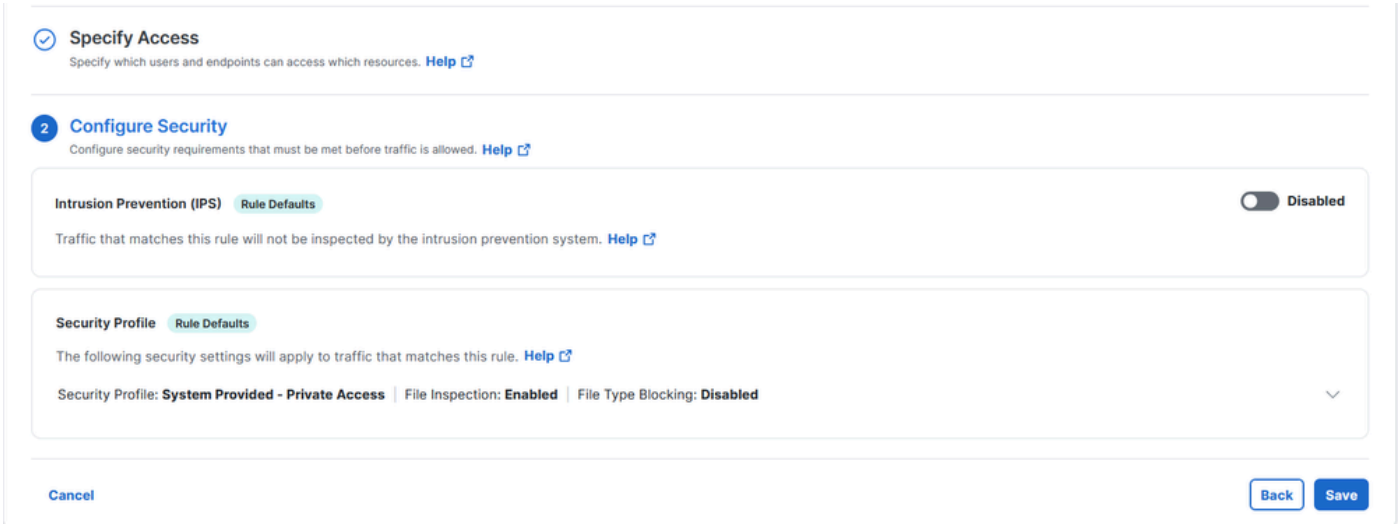
セキュアアクセス：アクセスポリシーの設定

5. エンドポイント要件の設定

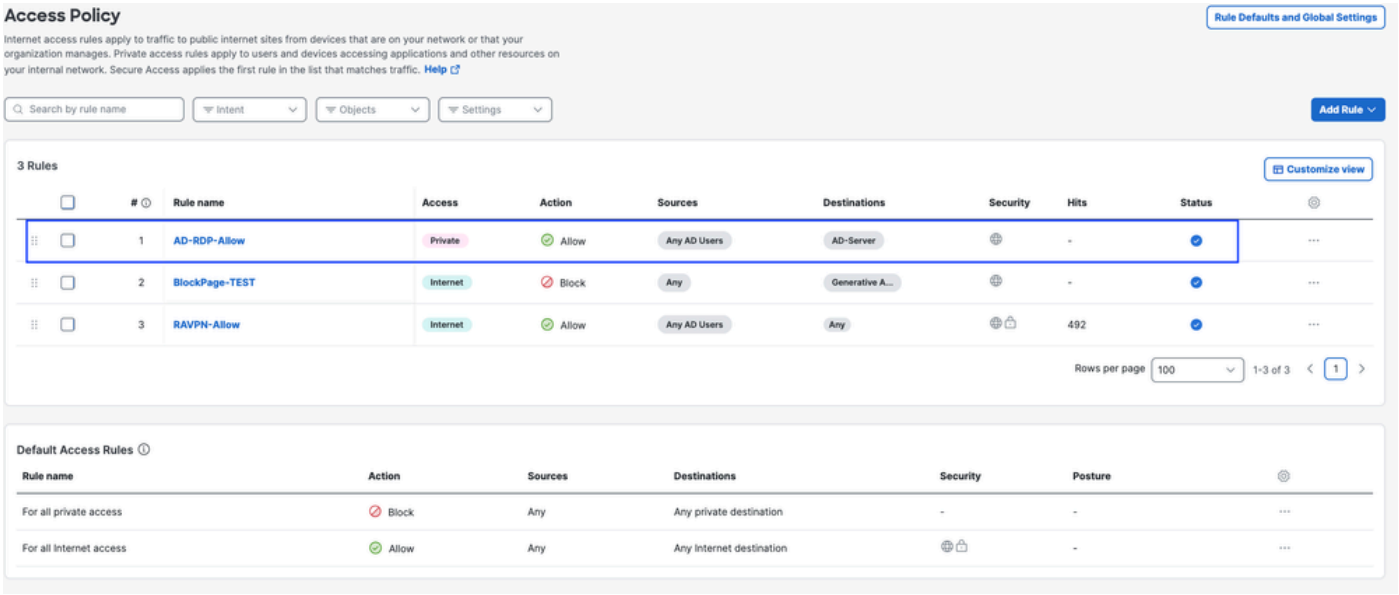


セキュアアクセス：アクセスポリシーの設定

6. セキュリティの設定



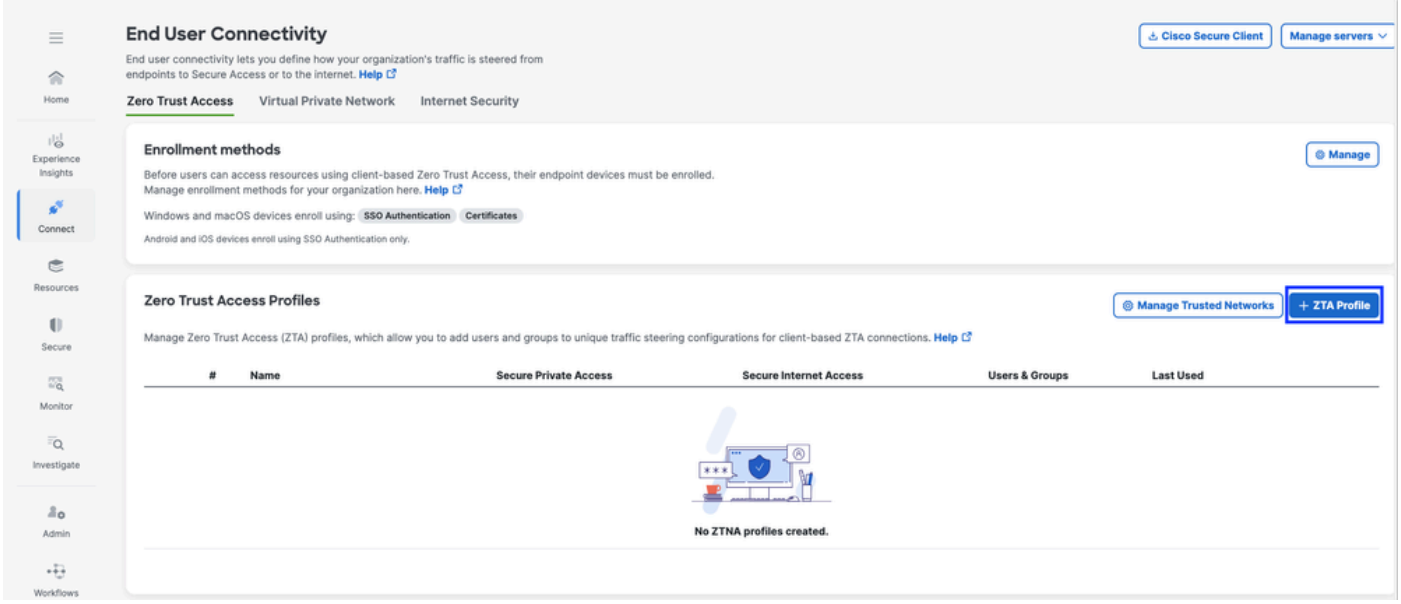
7. Saveをクリックします。



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

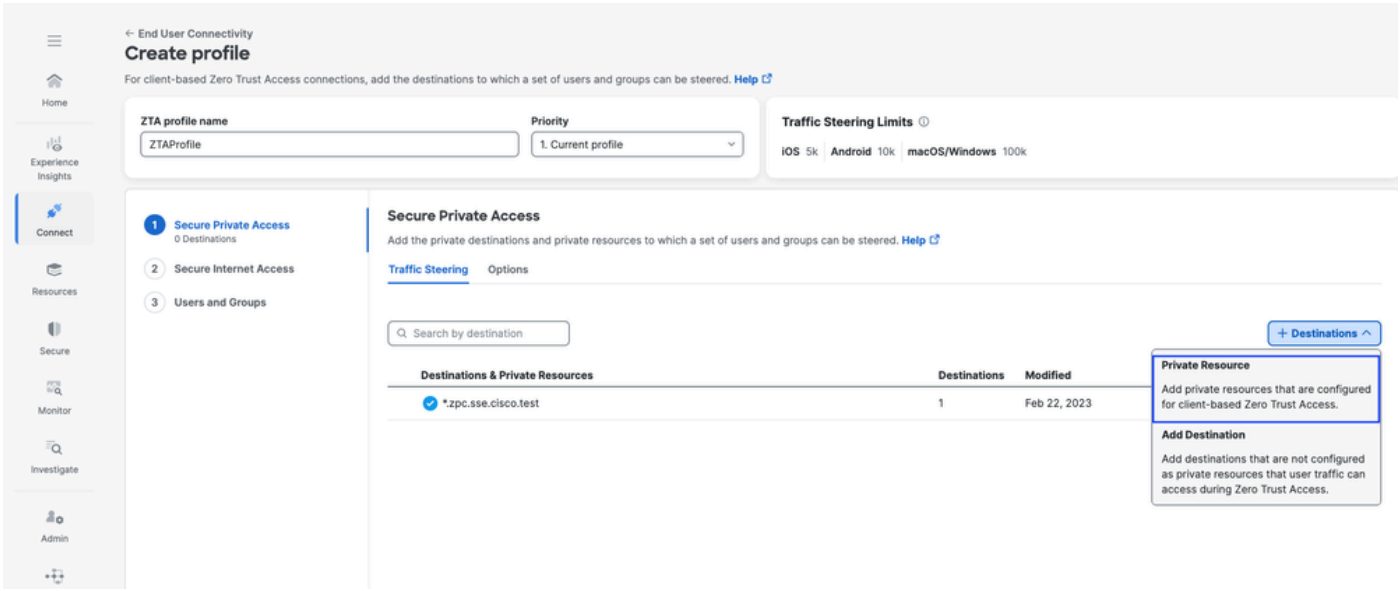
カスタムZTAプロファイルを使用している場合は、それぞれのプライベートリソースをZTAプロファイルに追加する必要があります

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

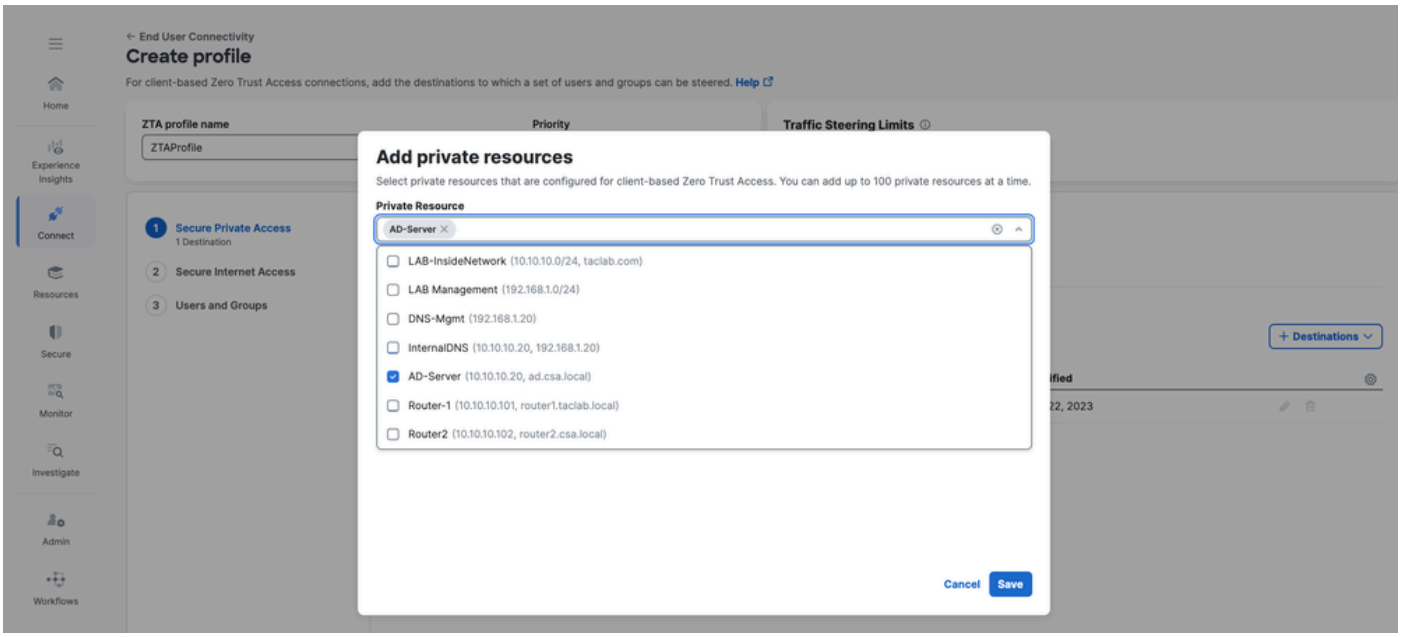


セキュアアクセス – ZTAプロファイル

2. プライベートリソースの追加

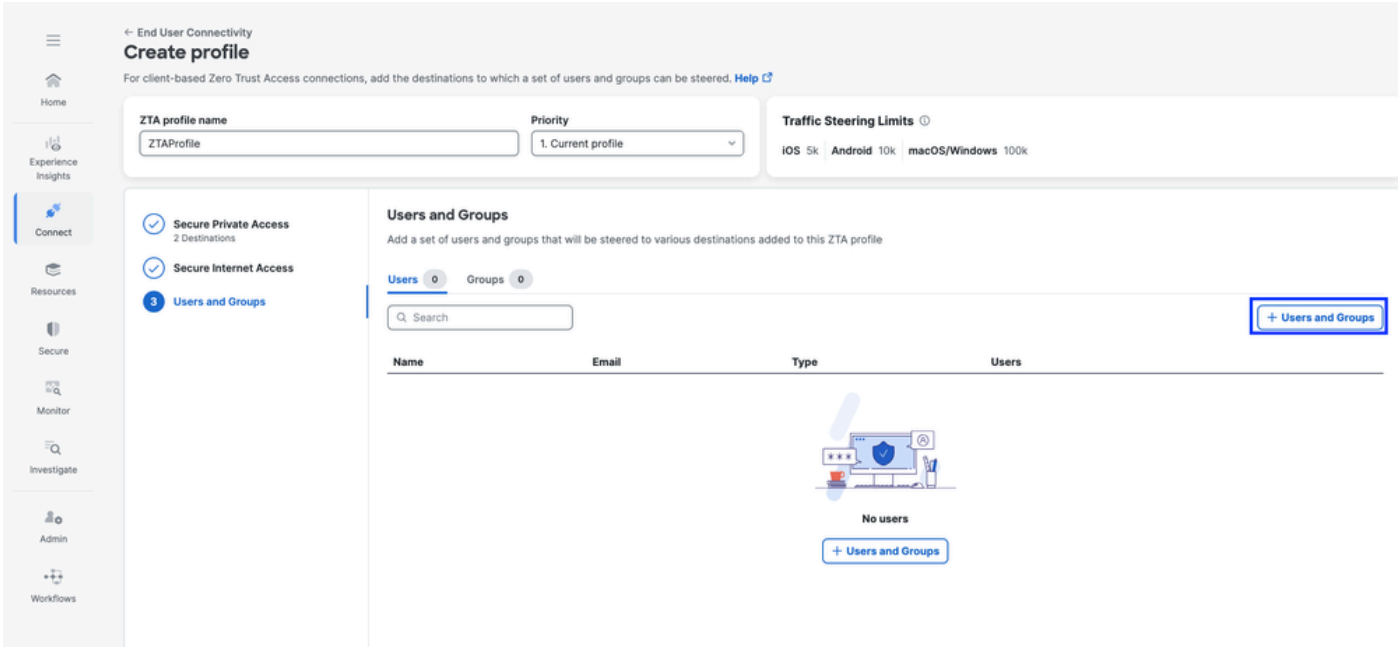


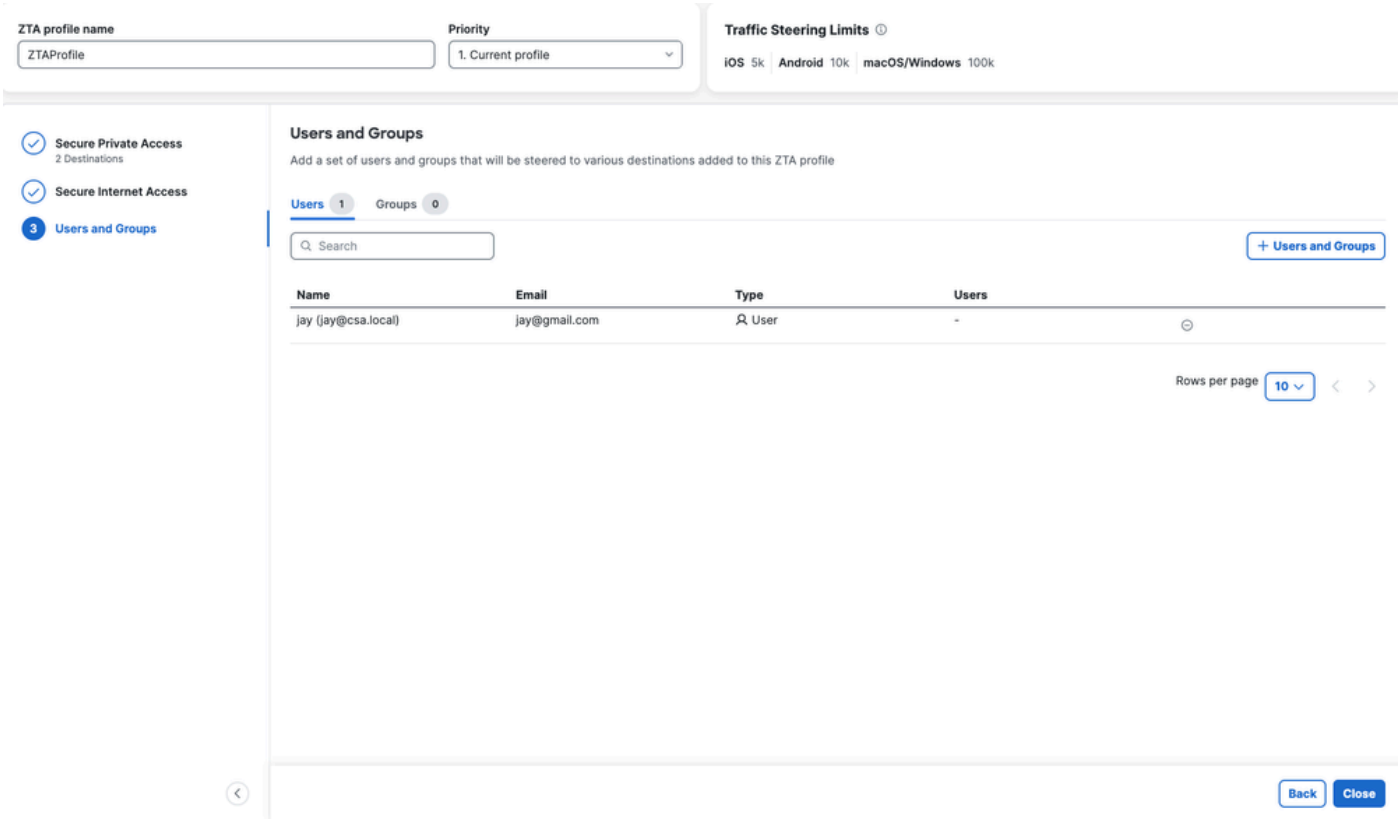
セキュアアクセス – ZTAプロファイル



セキュアアクセス – ZTAプロファイル

3. ユーザーとグループの追加





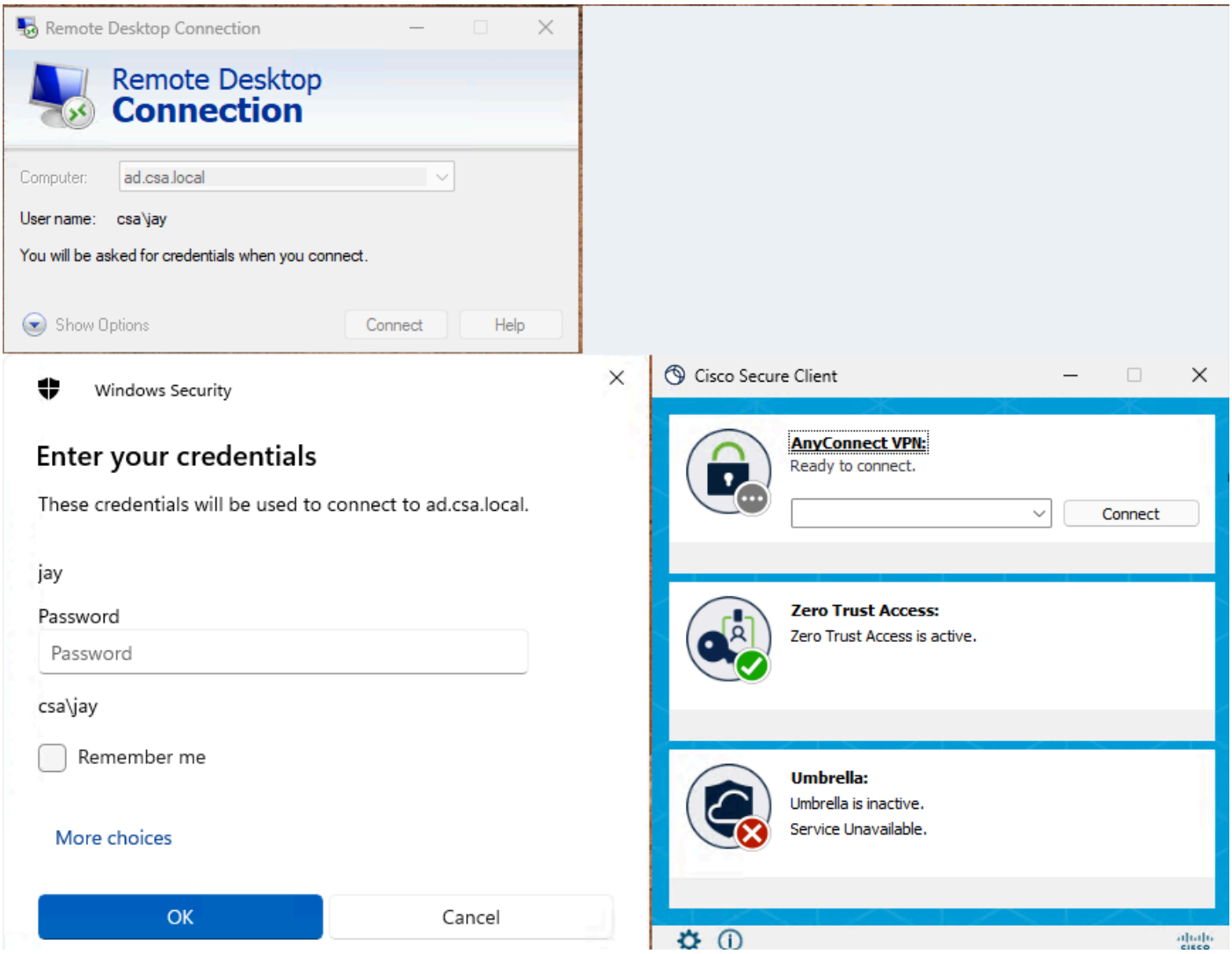
セキュアアクセス – ZTAプロファイル

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

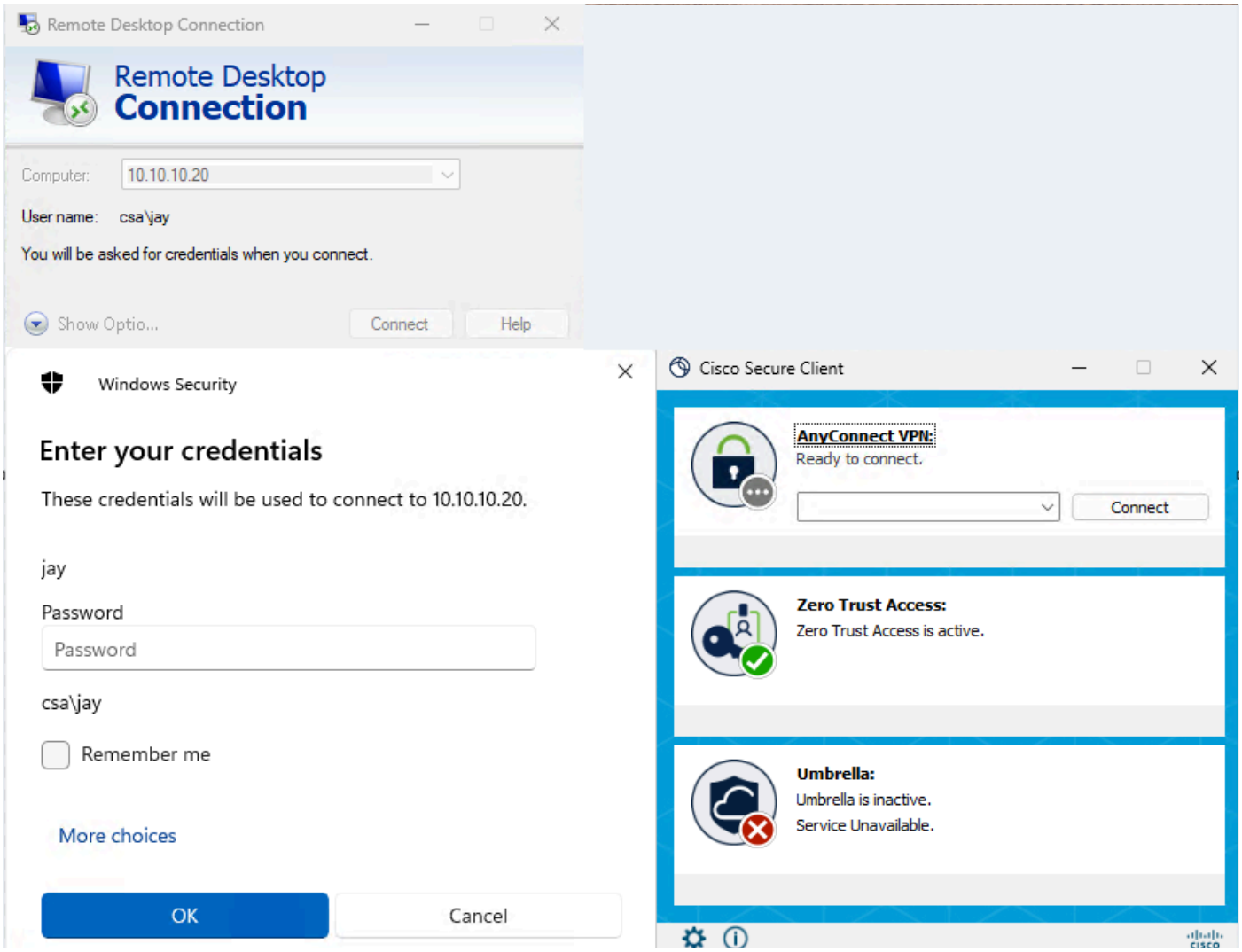
1. プライベートリソースへのアクセス

FQDNを使用してPRにアクセスします



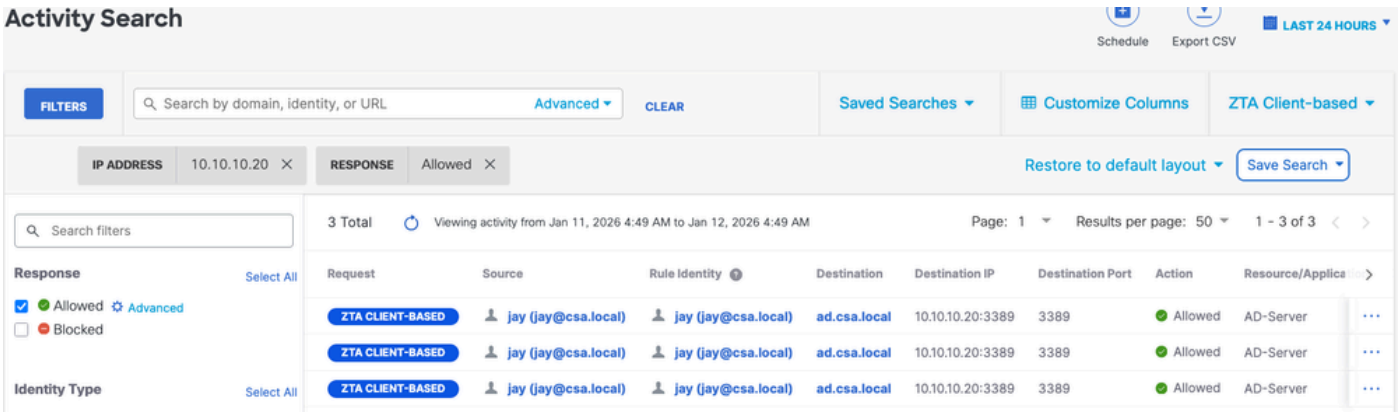
セキュアなアクセス – PRテスト

IPアドレスを使用してPRにアクセスします

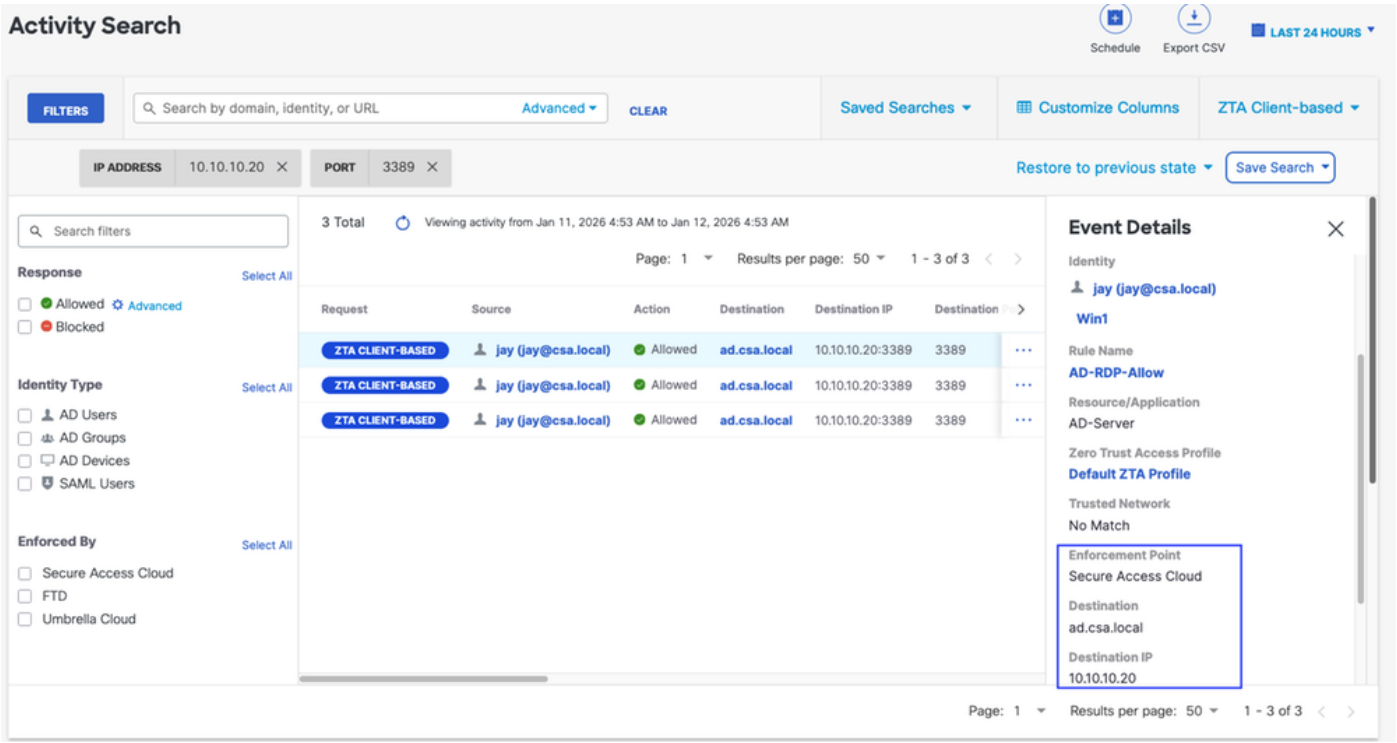


セキュアなアクセス – PRテスト

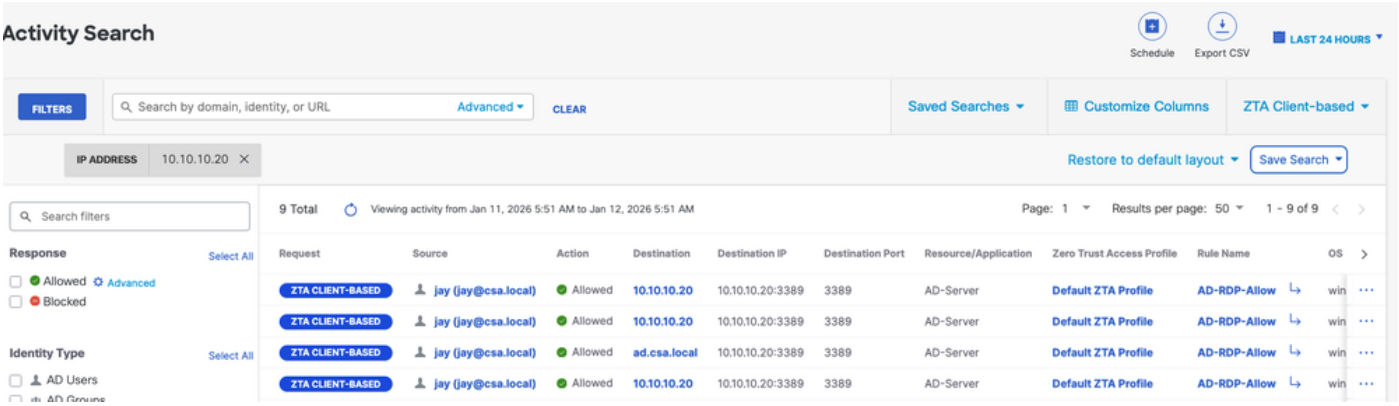
2. アクティビティ検索イベントで確認する



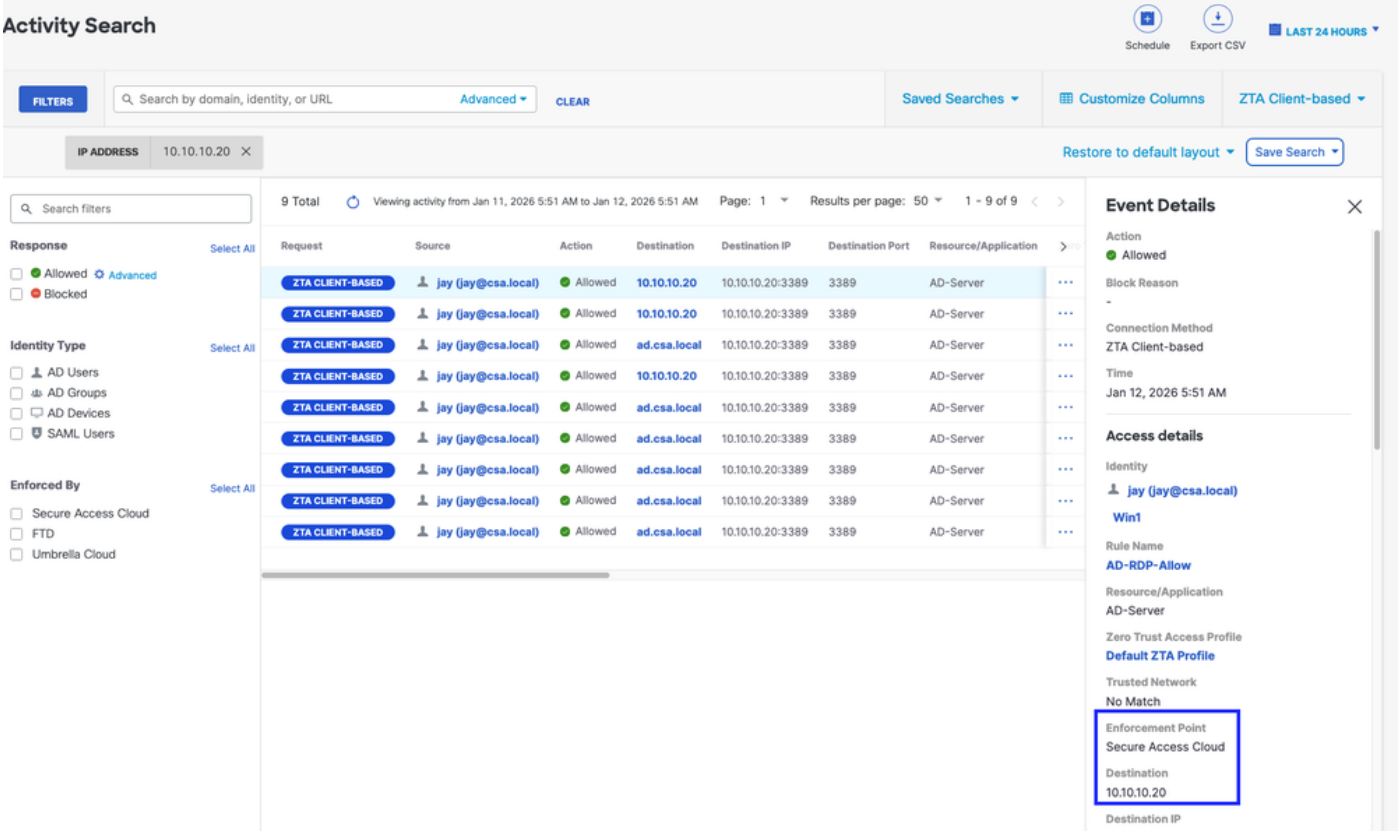
セキュアアクセス – アクティビティ検索



セキュアアクセス – アクティビティ検索

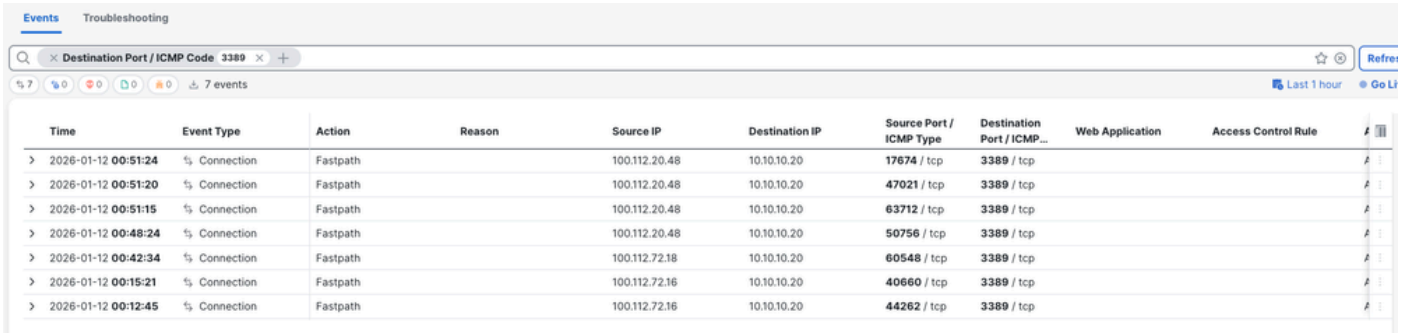


セキュアアクセス – アクティビティ検索



セキュアアクセス – アクティビティ検索

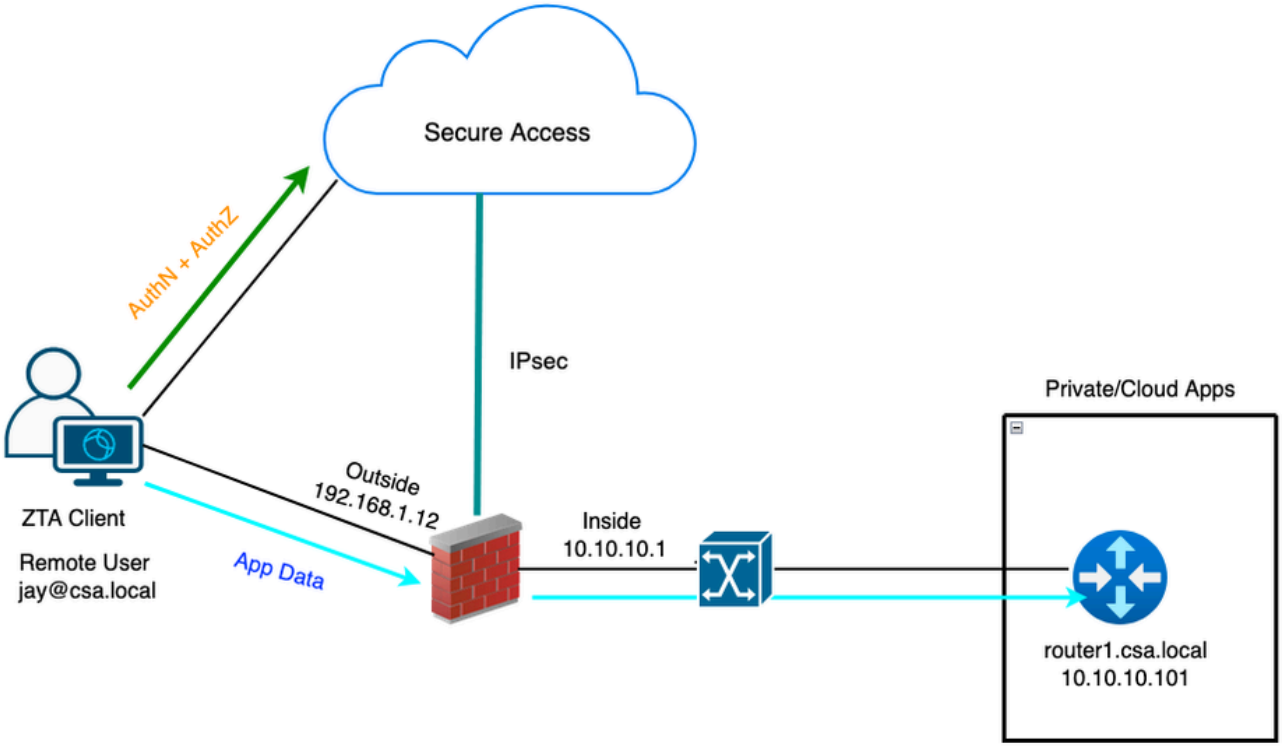
3. FMC接続イベントの確認



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。

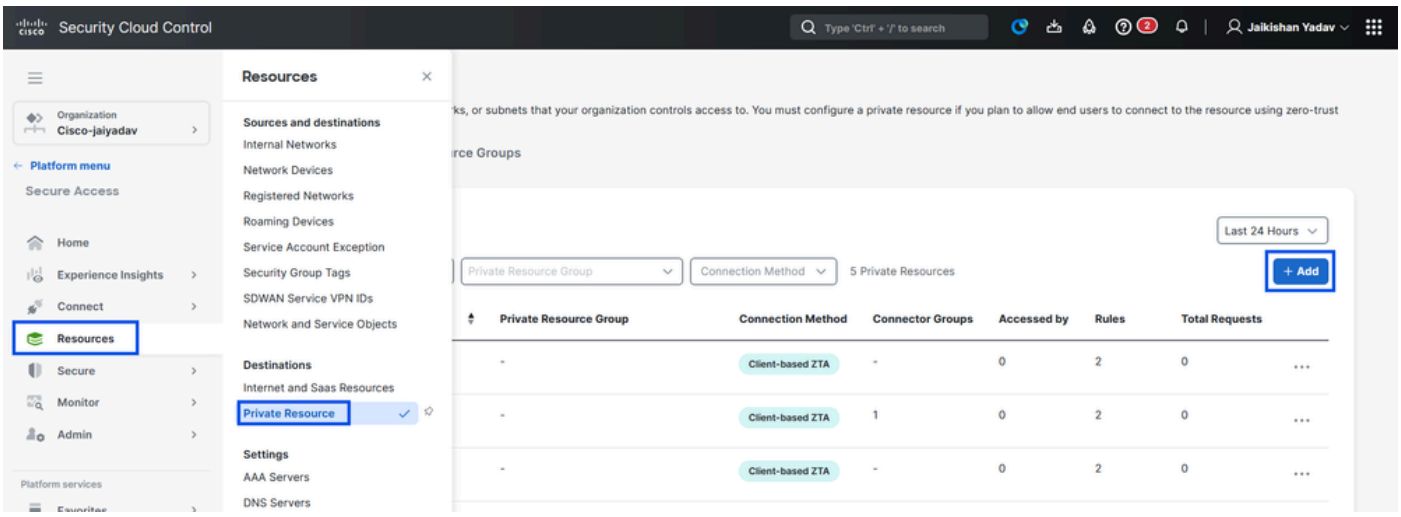


ユニバーサルZTA – テストケースのトポロジ

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

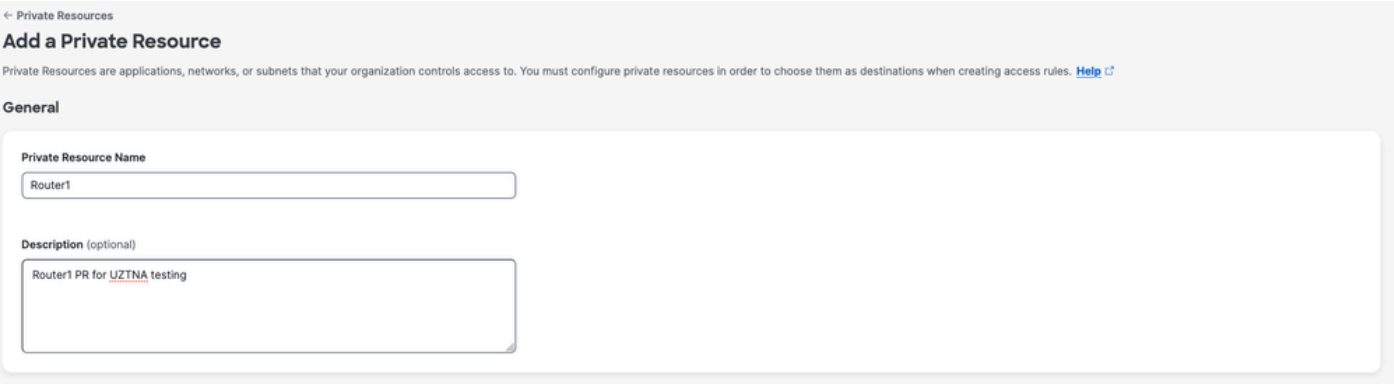
クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

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



セキュアアクセス：プライベートリソースの設定

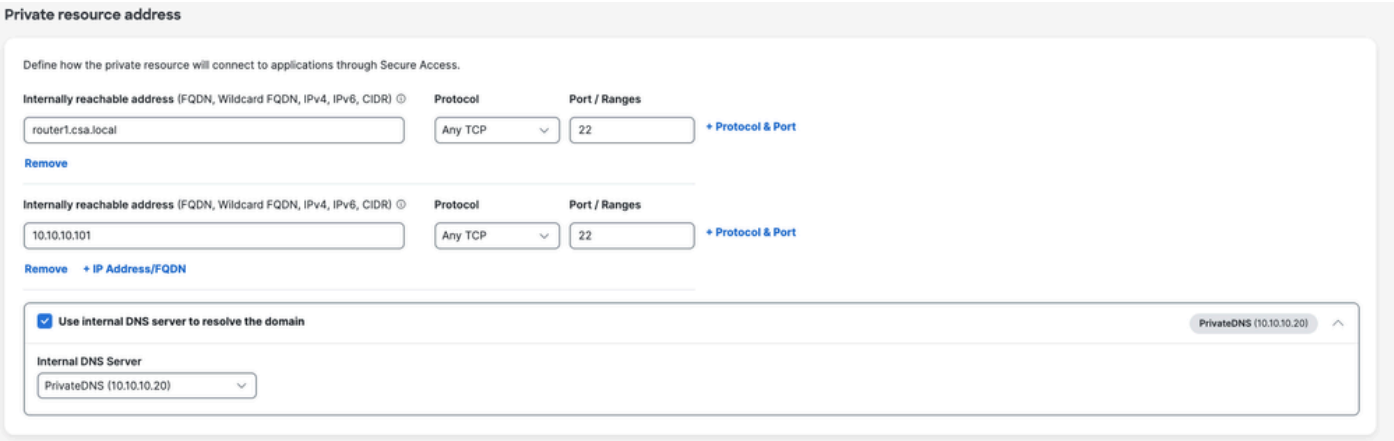
2.「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。



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。

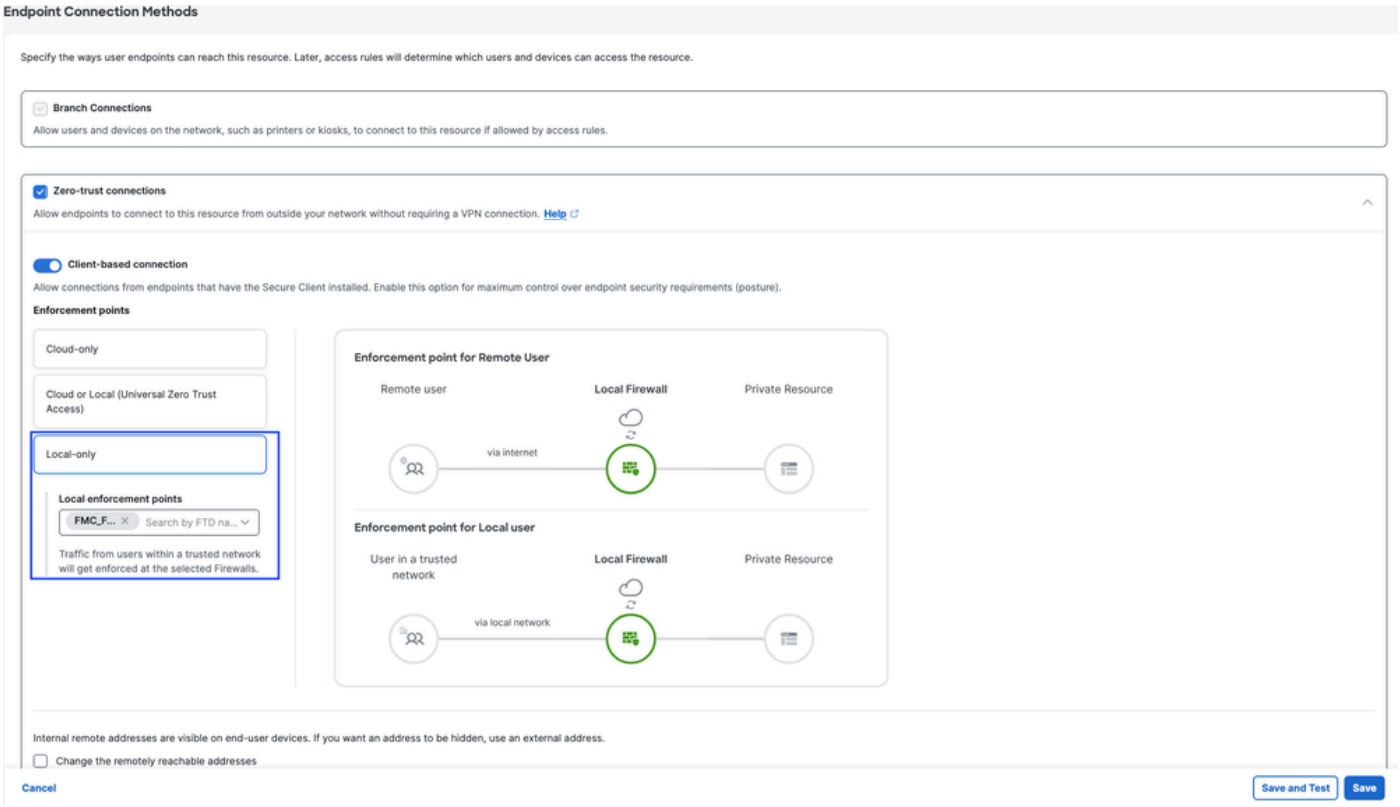
4. ドメインを解決する内部DNSサーバーを選択します



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。



セキュアアクセス：プライベートリソースの設定

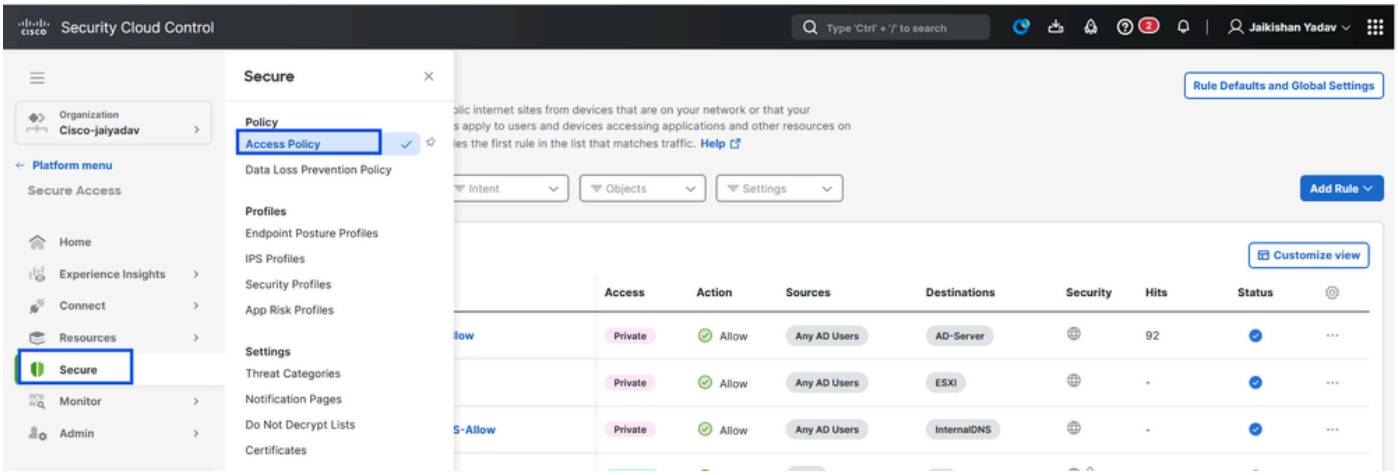
注：選択する登録のタイプ（IPアドレスまたは非IPアドレス）に応じて、この変更によりPRがFTDに自動的に関連付けられ、ポリシーの導入がトリガーされます。

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

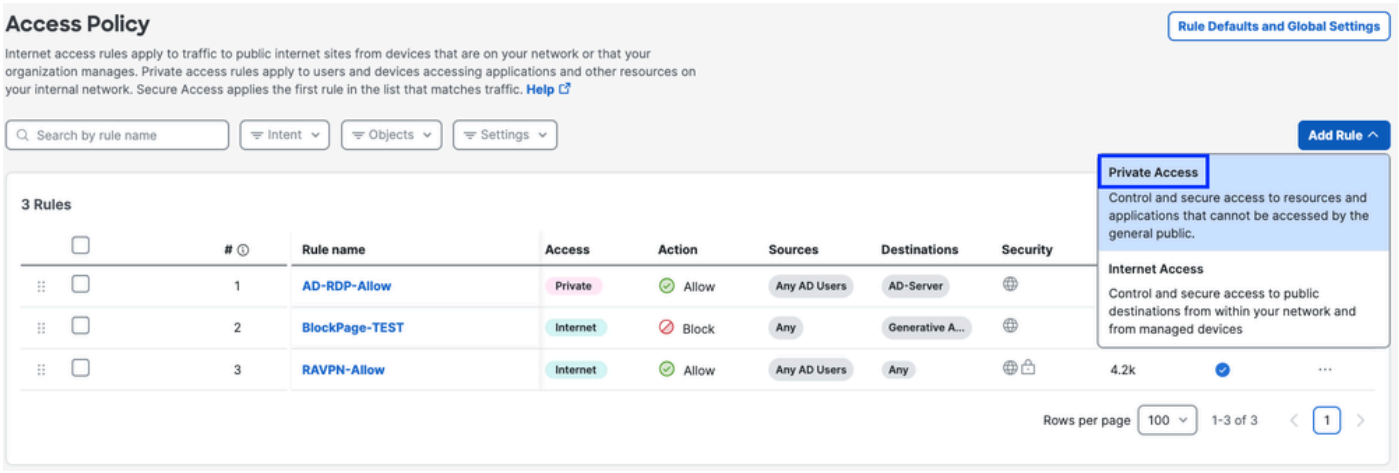
Secure Access上のプライベートアクセスを、ユニバーサルZTA登録済みユーザによるアクセスとなるように設定します（デフォルト）。詳細については、「プライベートアクセスルール」を参照してください

1. Secure > Access Policyの順に移動します。



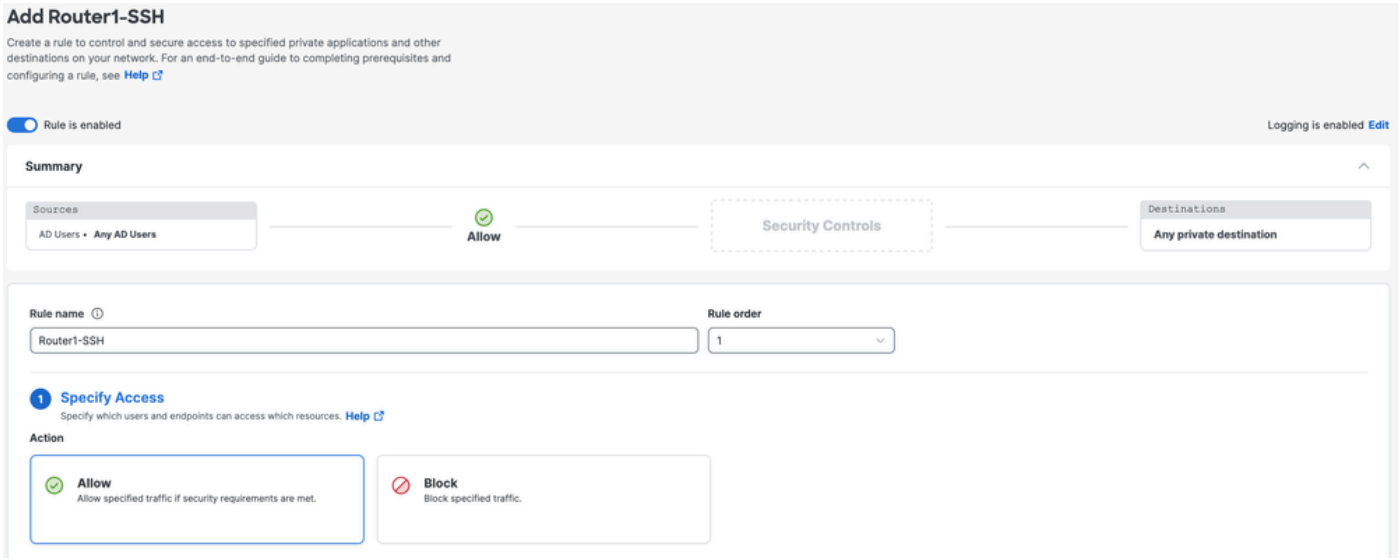
セキュアアクセス：プライベートリソースの設定

2. Add Ruleをクリックし、Private Accessを選択します。
ルールの上部には、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。



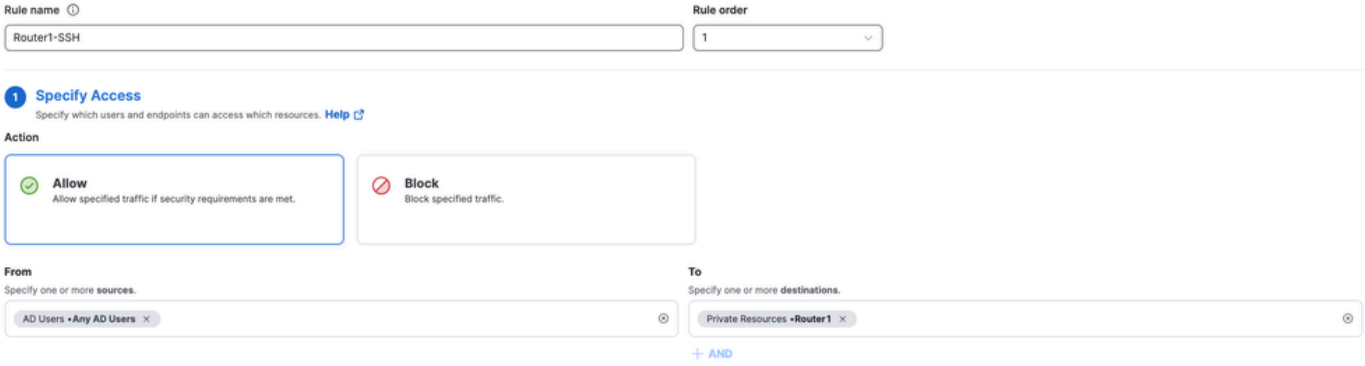
セキュアアクセス：アクセスポリシーの設定

3. ルール名の追加



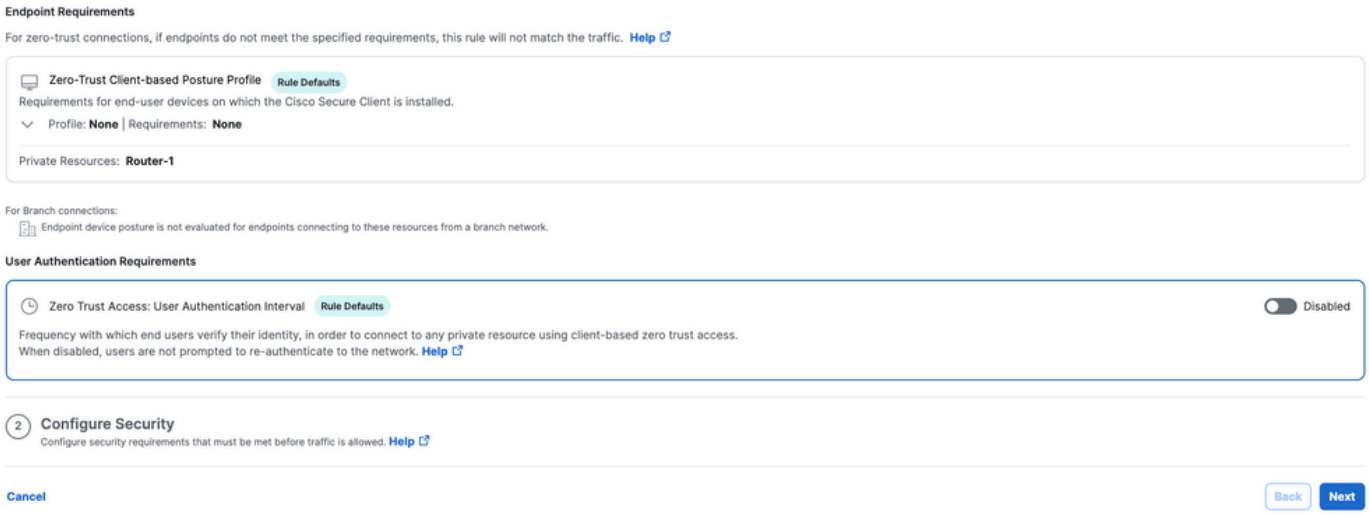
セキュアアクセス：アクセスポリシーの設定

4. ルール処理を選択し、ソースと宛先を選択します



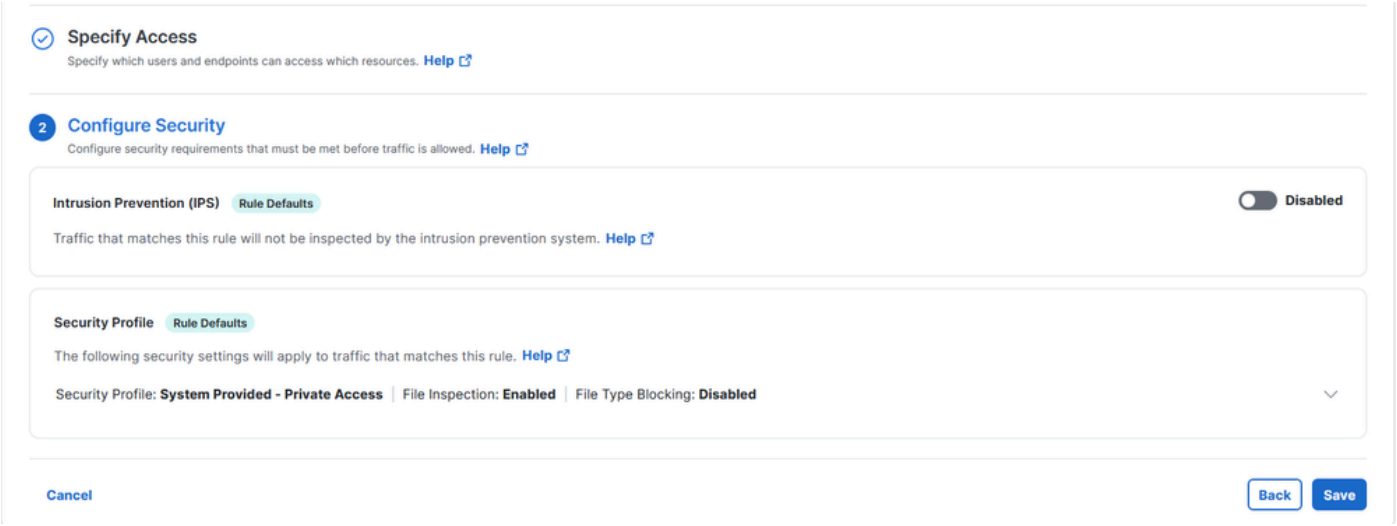
セキュアアクセス：アクセスポリシーの設定

5. エンドポイント要件の設定



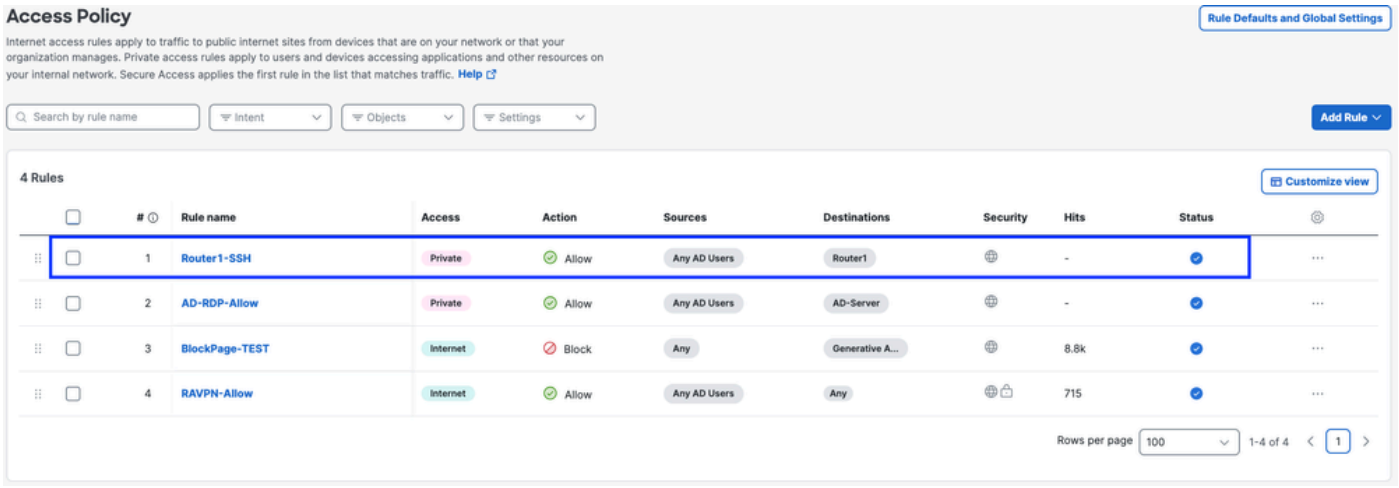
セキュアアクセス：アクセスポリシーの設定

6. セキュリティの設定



セキュアアクセス：アクセスポリシーの設定

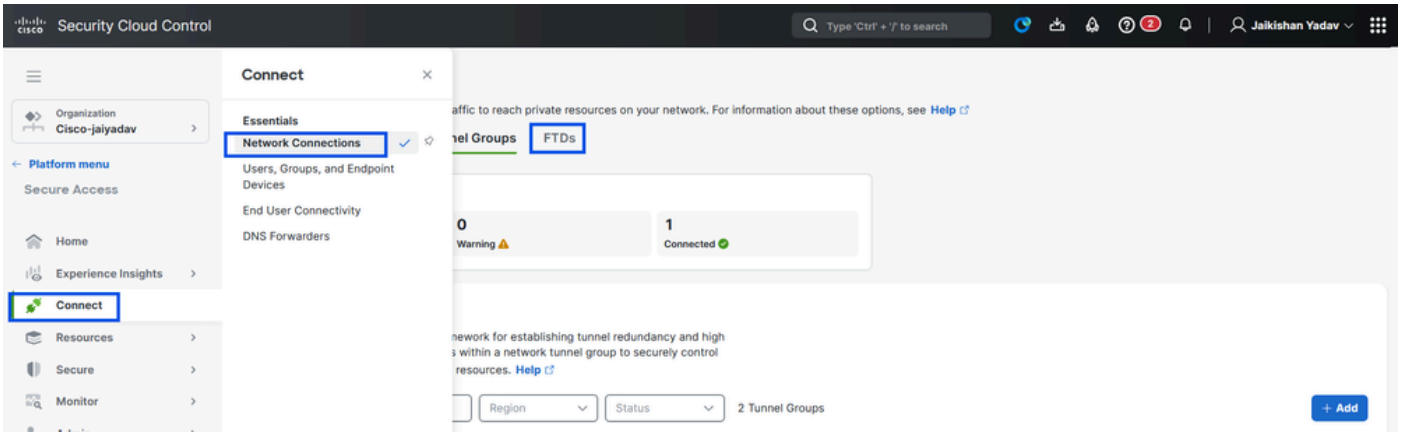
7. Saveをクリックします。



セキュアアクセス：アクセスポリシーの設定

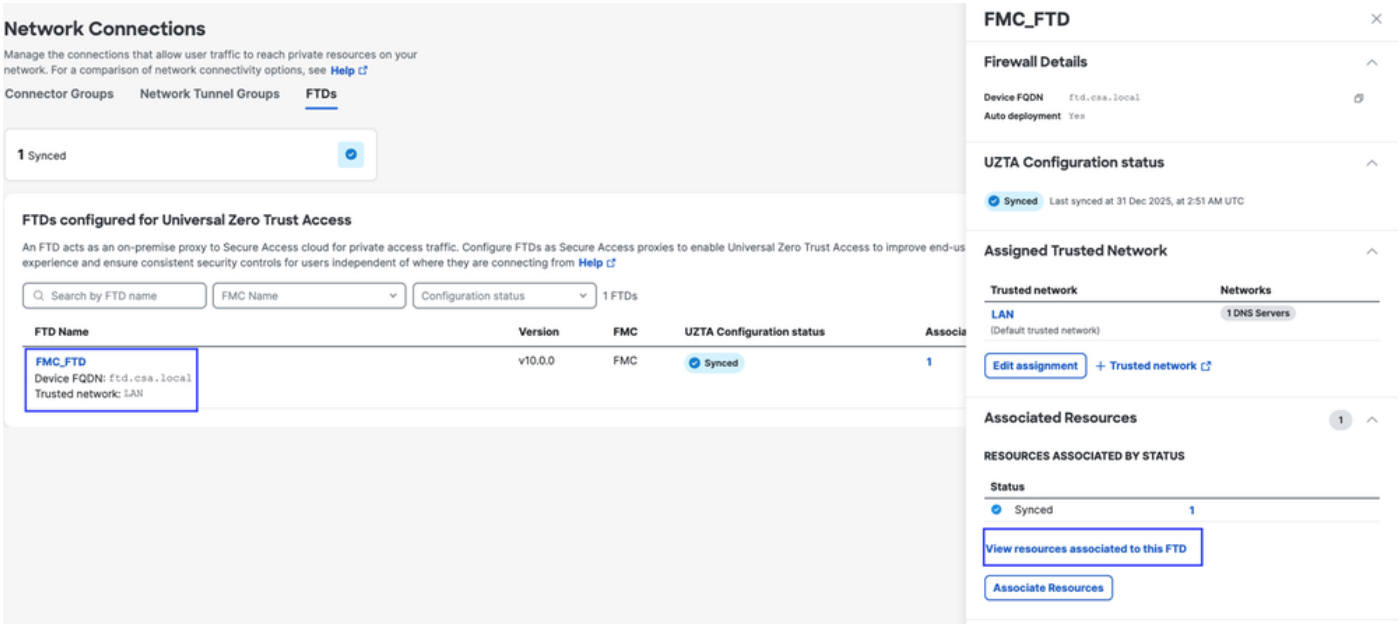
手順3:FTDでのPRの関連付けを確認します

1. 「接続」>「ネットワーク接続」>「FTDs」に移動します。

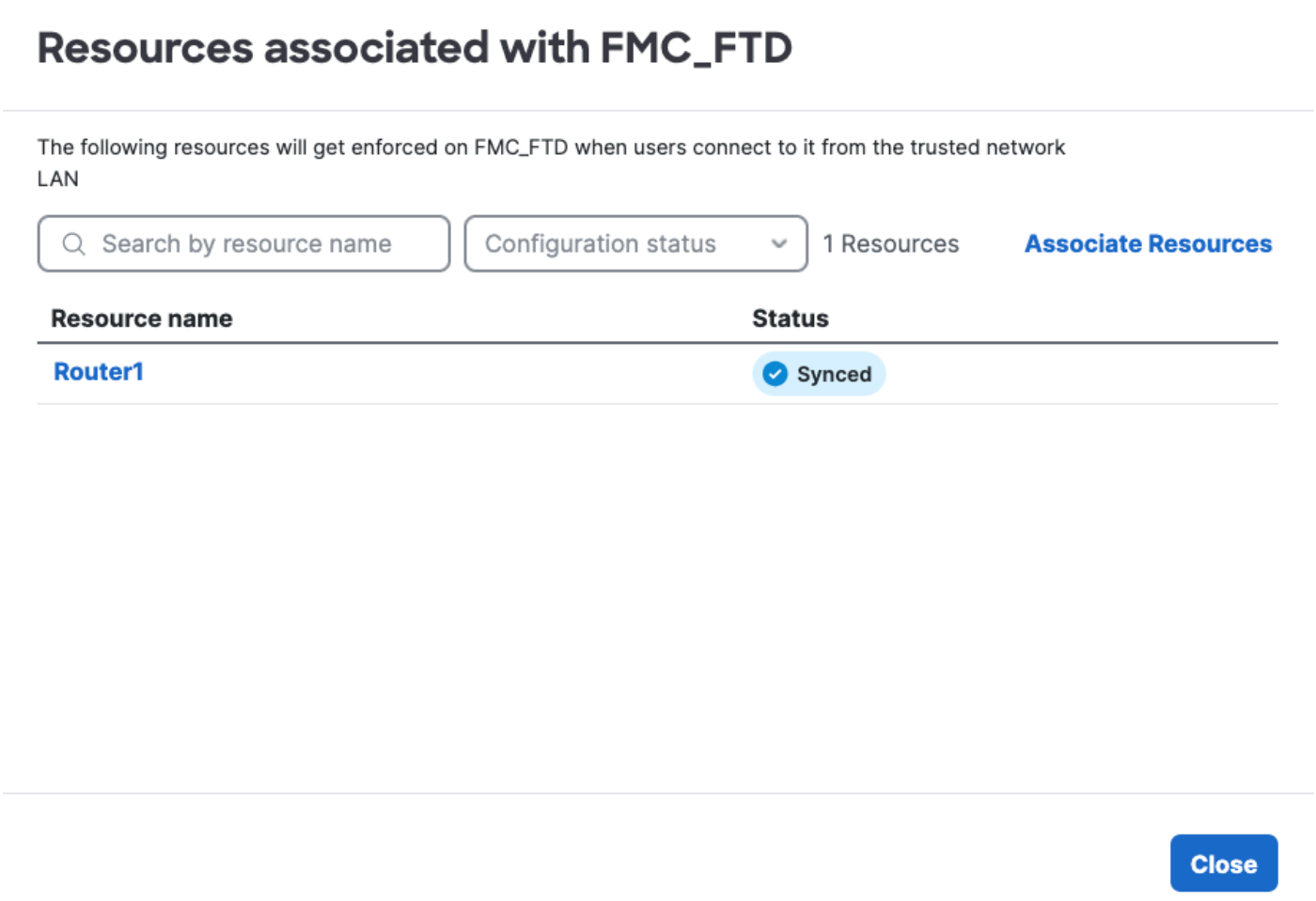


セキュアアクセス – PR検証

2. 「FTD」 >「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。



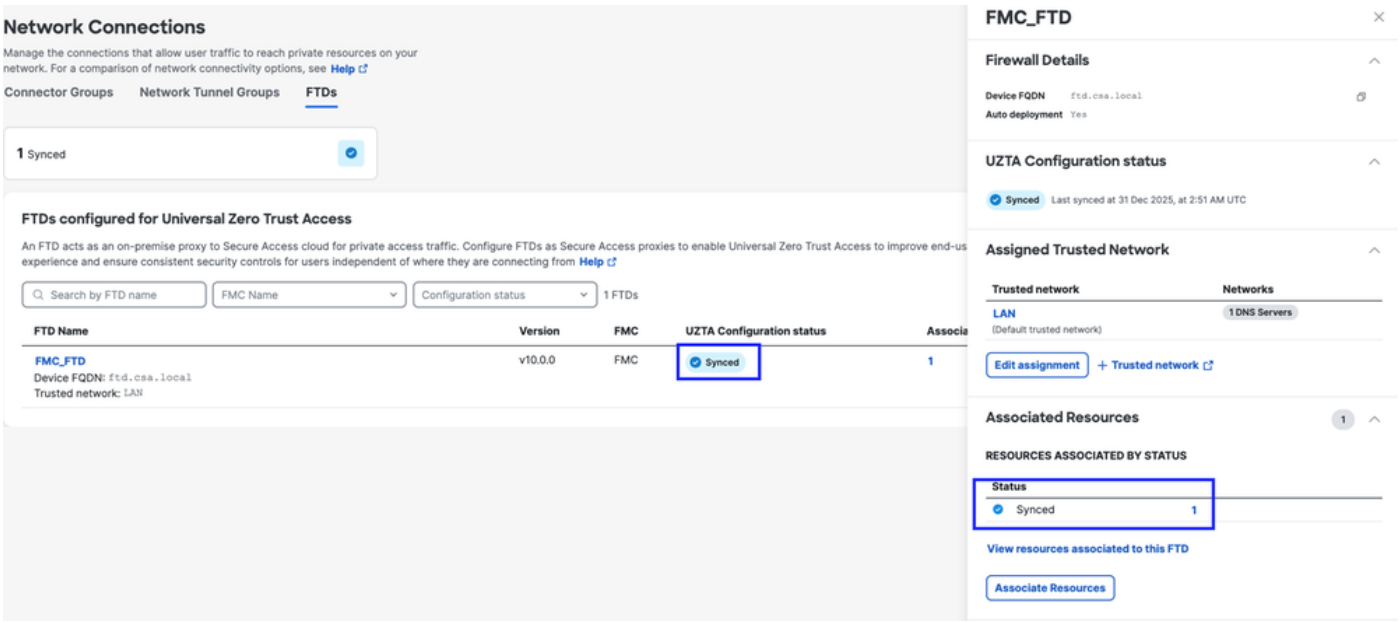
セキュアアクセス – PR検証



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



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。

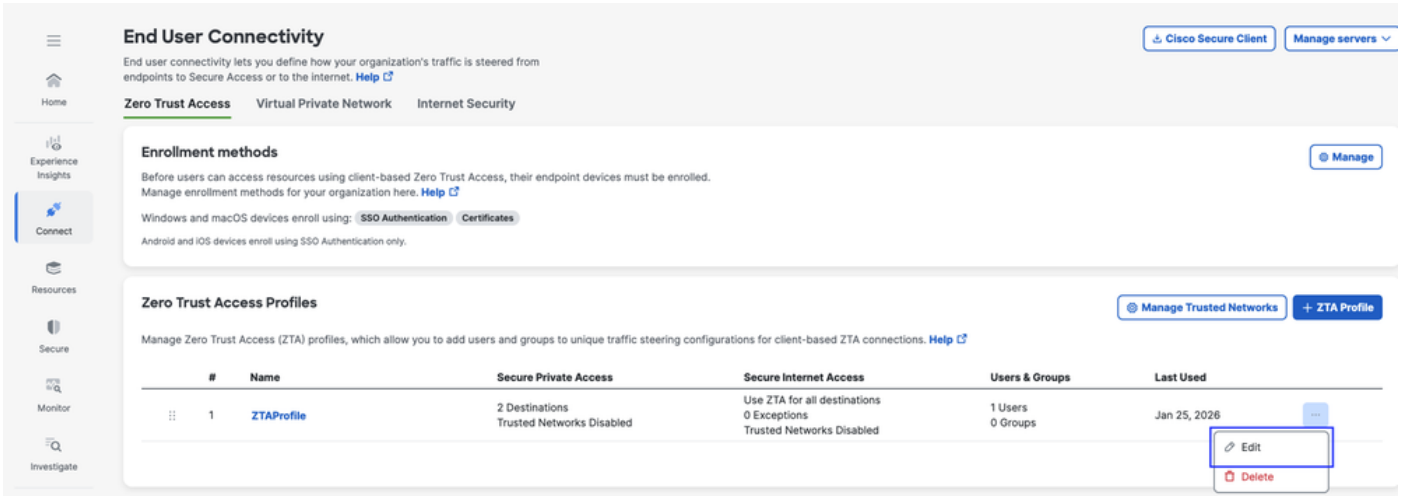
show running-config object application

```
> 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

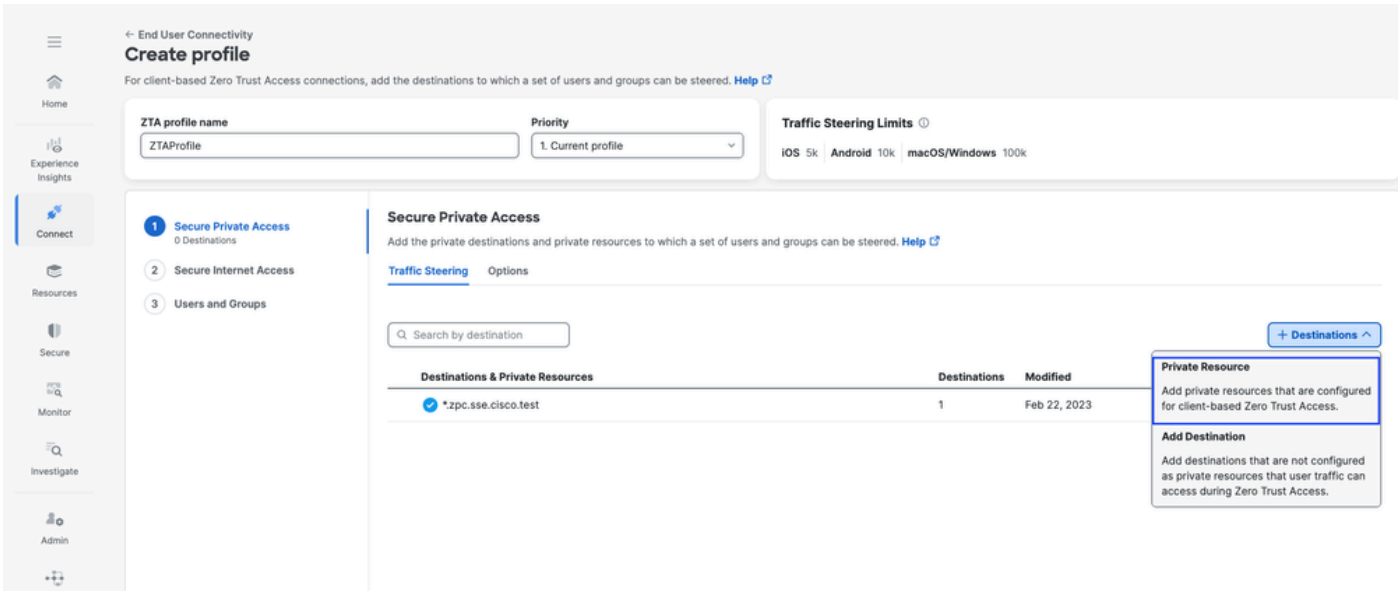
手順4:ZTAプロファイルへのプライベートリソースの追加

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

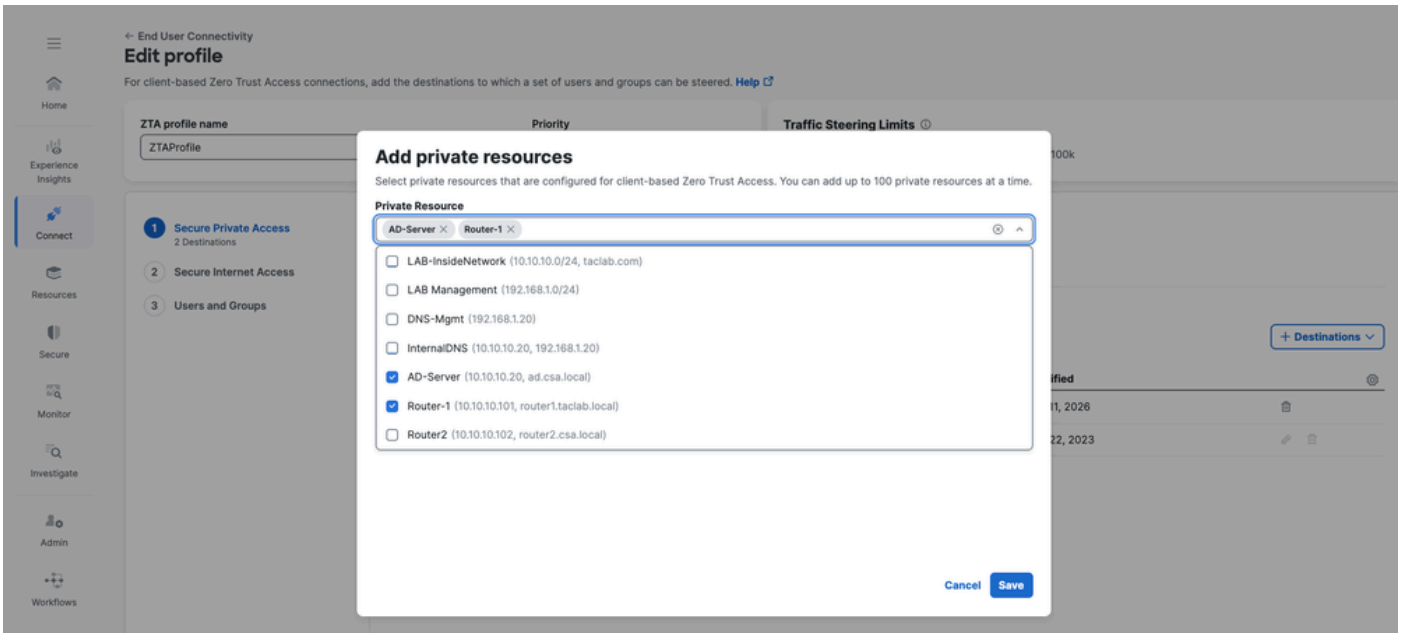


セキュアアクセス – ZTAプロファイル

2. プライベートリソースの追加

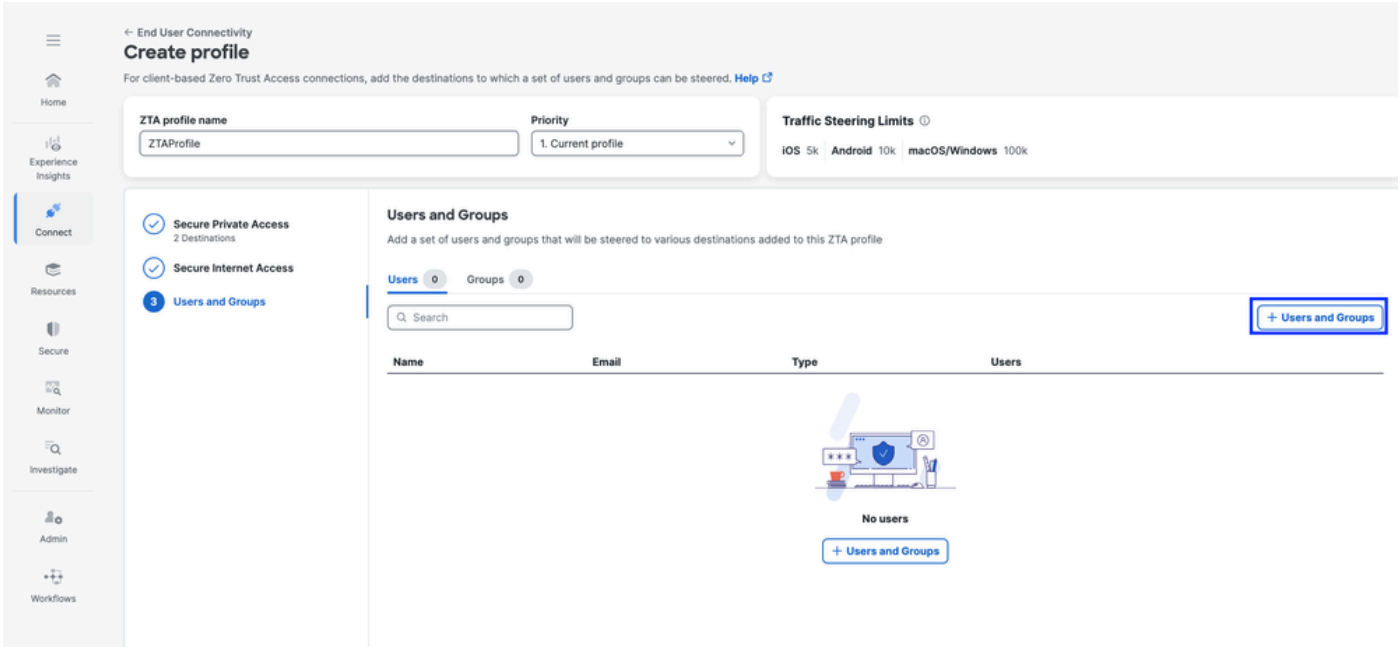


セキュアアクセス – ZTAプロファイル

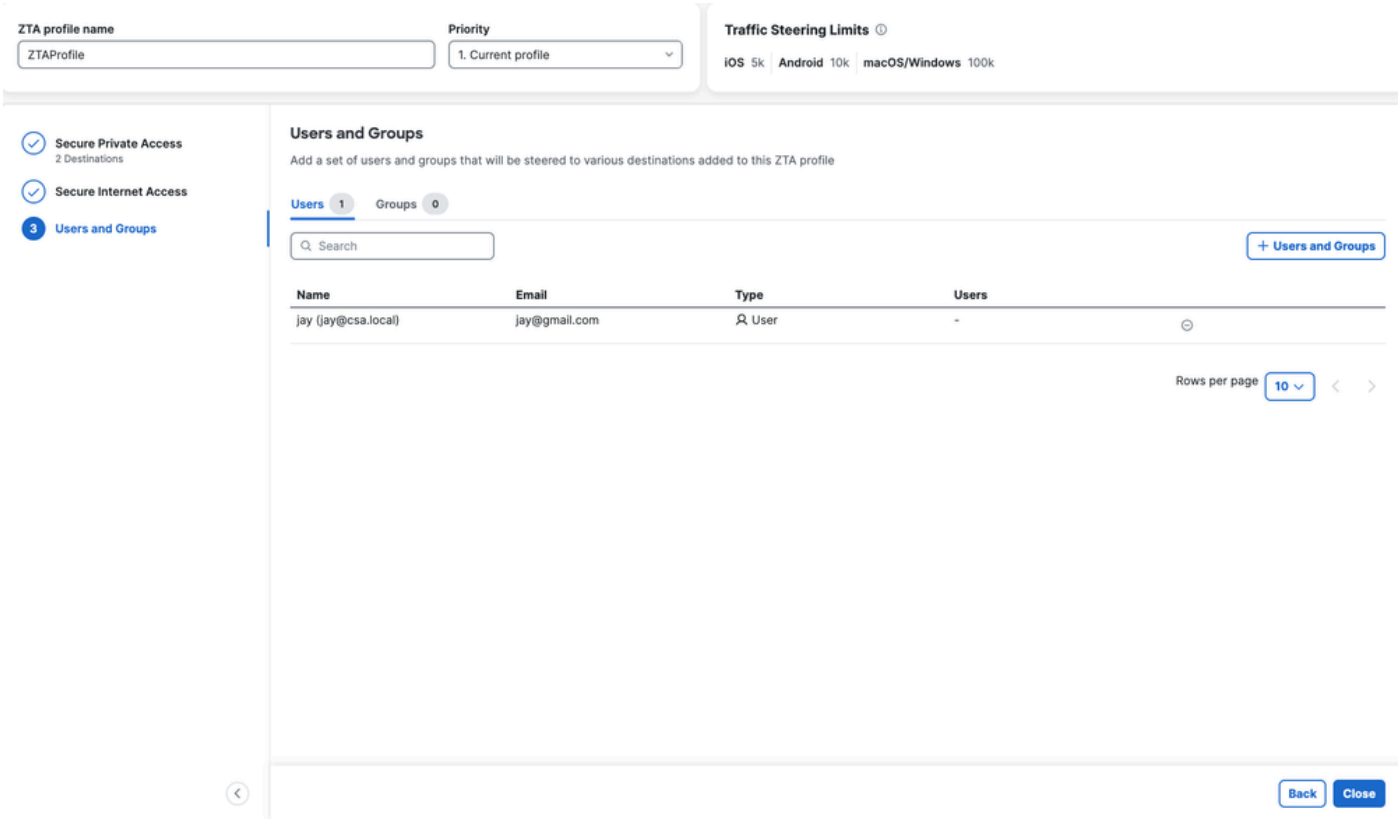


セキュアアクセス – ZTAプロファイル

3. ユーザーとグループの追加



セキュアアクセス – ZTAプロファイル



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

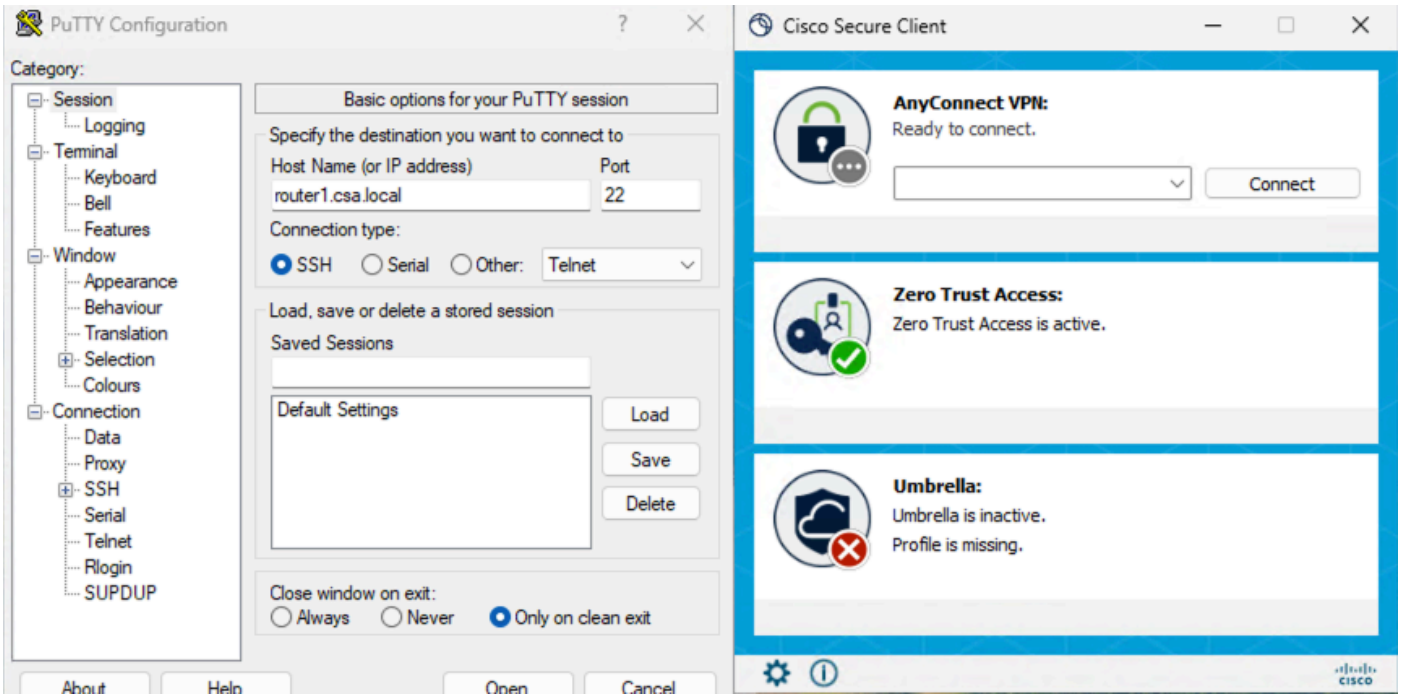
```
PS C:\Users\jay> ping ftd.csa.local

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
```

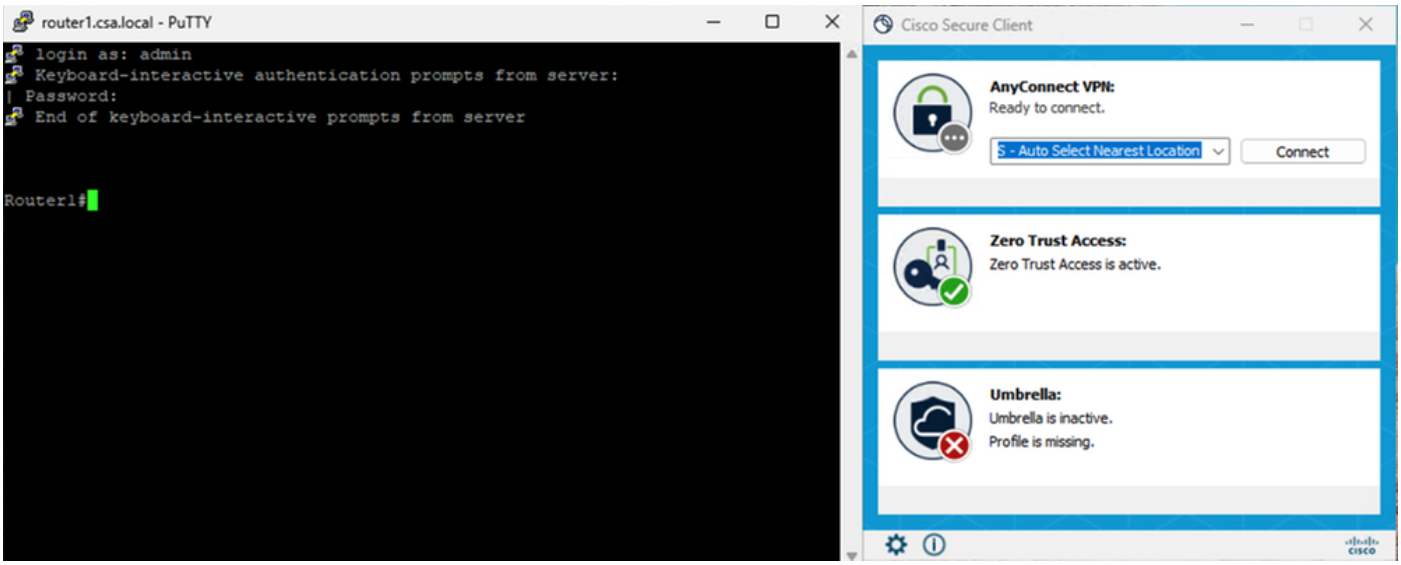
2. FTDがFQDNを使用してプライベートリソースに到達できることを確認します。

```
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#
```


3. プライベートリソースへのSSH接続をテストする

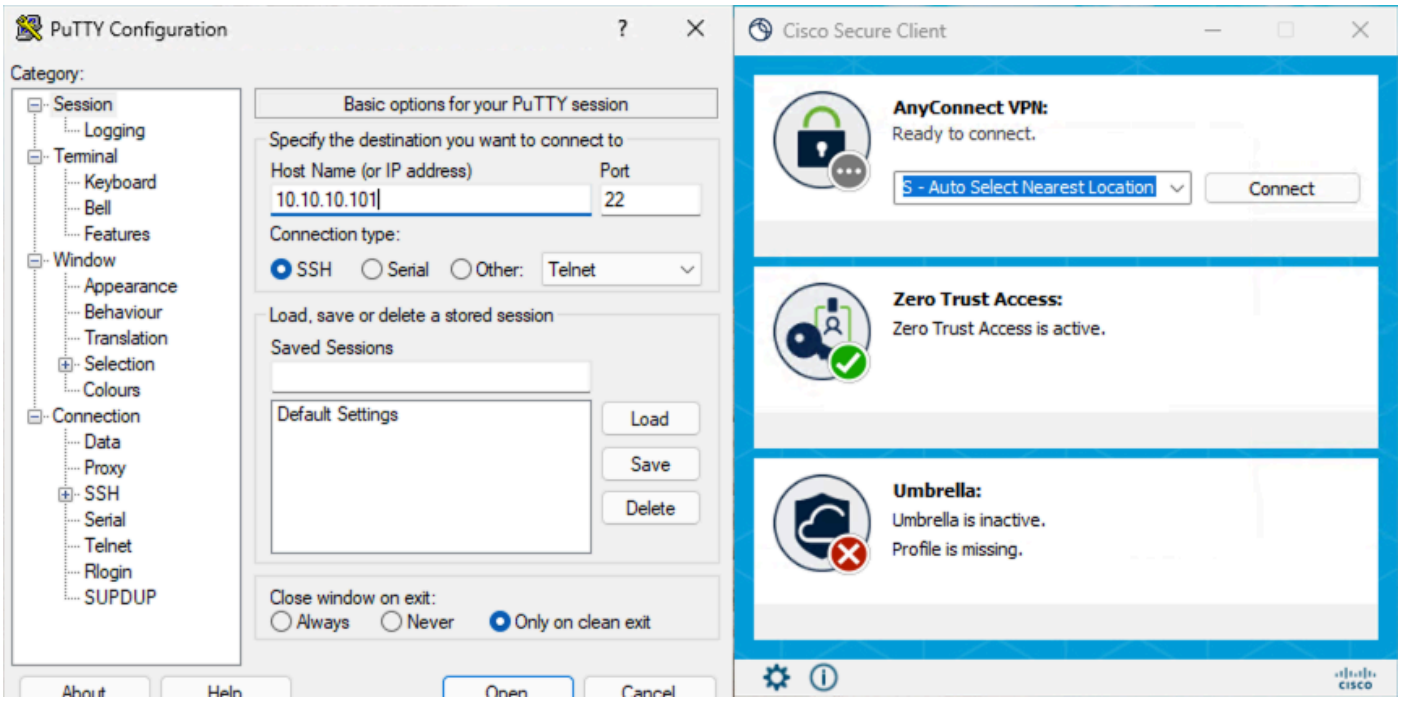
FQDNを使用してPRにアクセスします



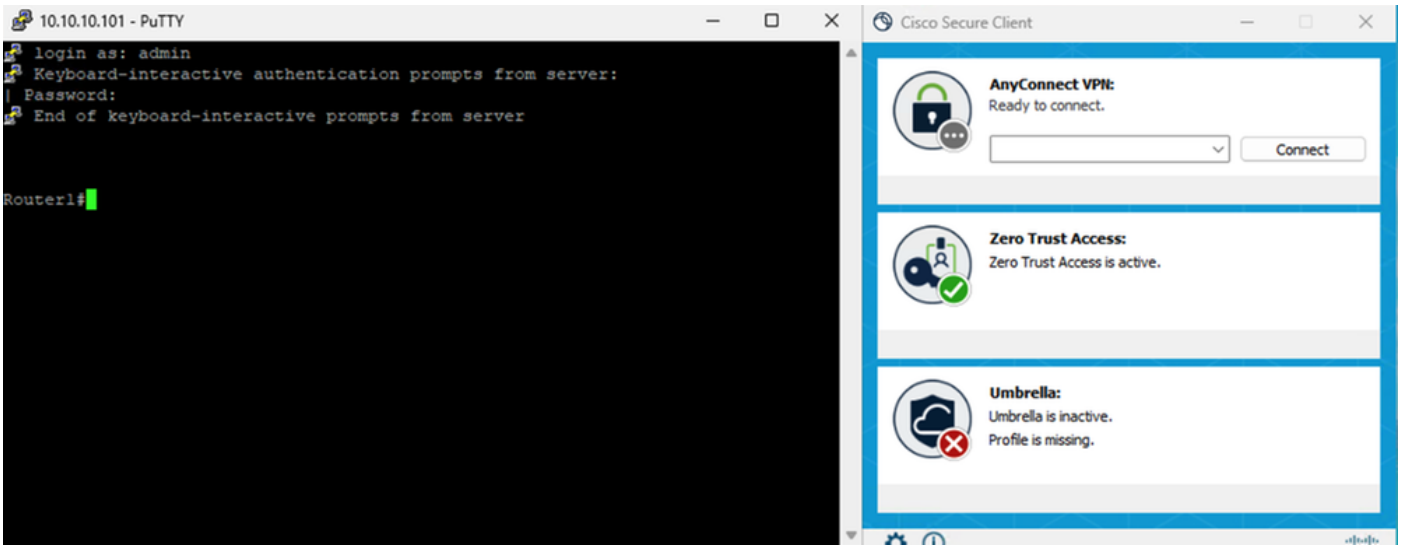


セキュアなアクセス – PRテスト

IPアドレスを使用してPRにアクセスします

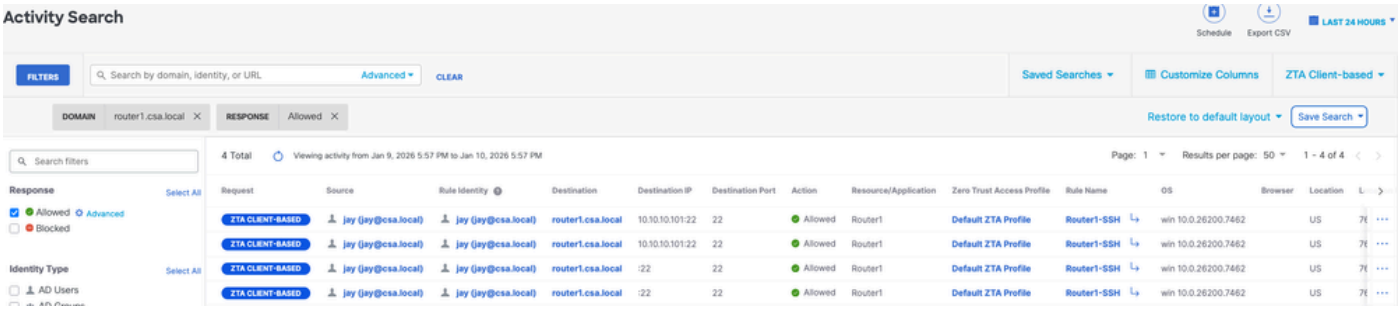


セキュアなアクセス – PRテスト

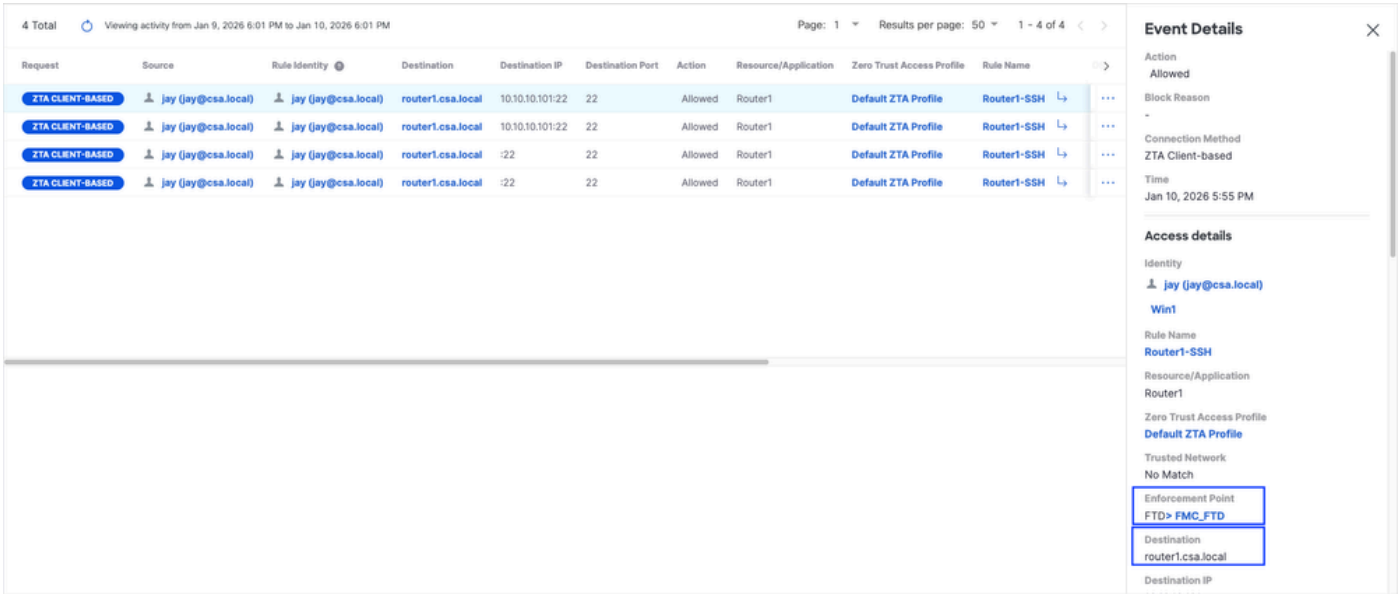


セキュアなアクセス – PRテスト

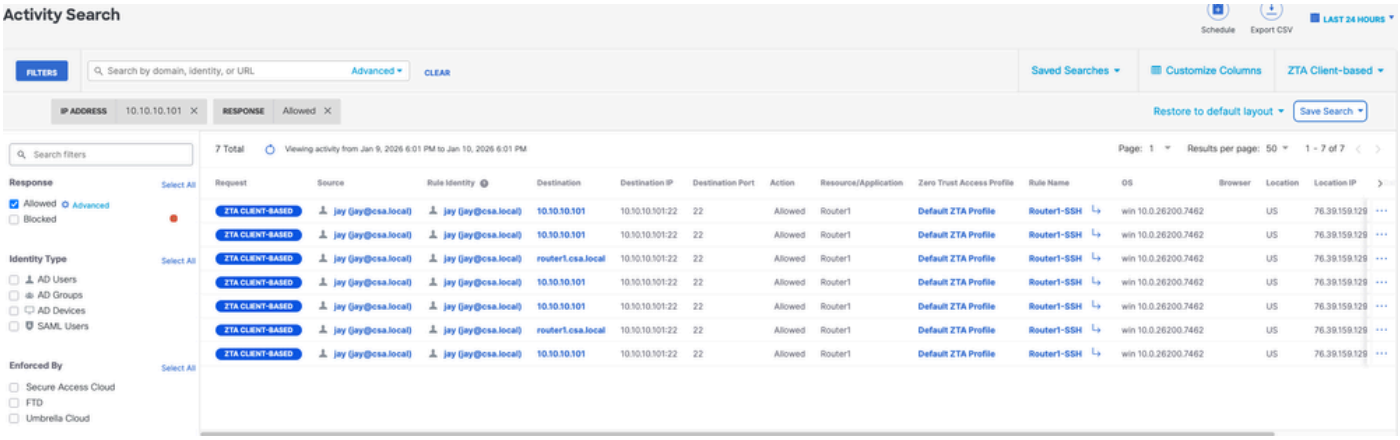
4. セキュアアクセスアクティビティ検索ログの確認



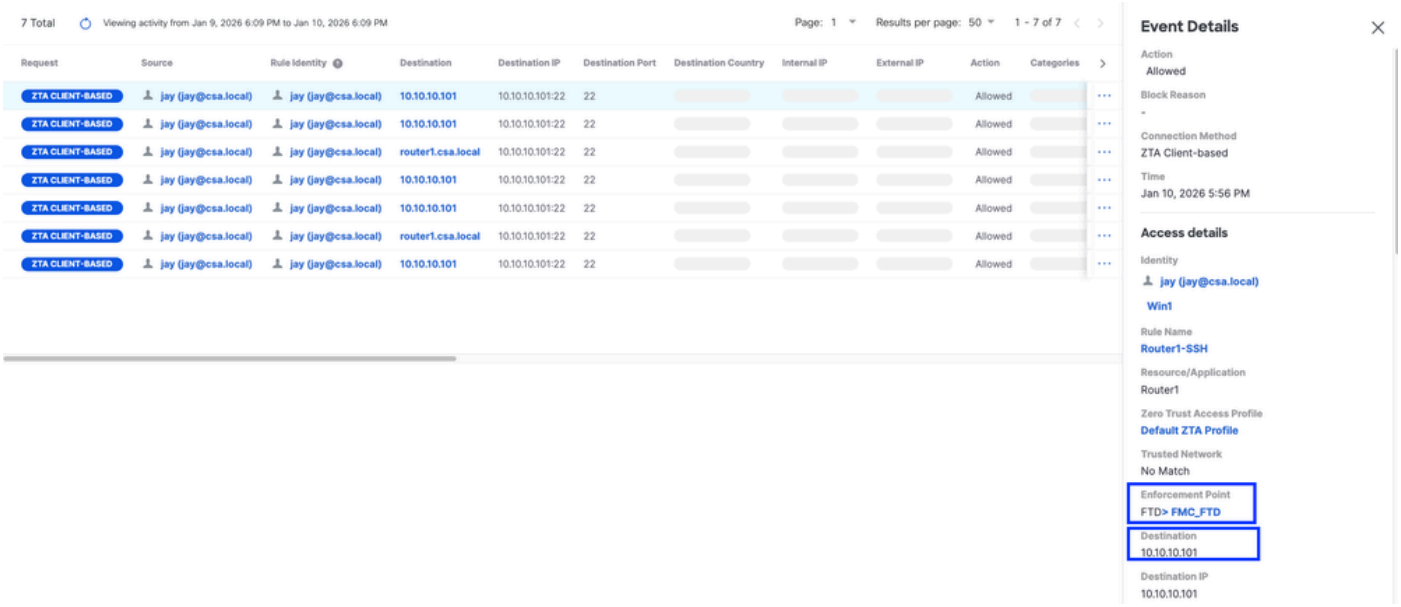
セキュアアクセス – アクティビティ検索



セキュアアクセス – アクティビティ検索

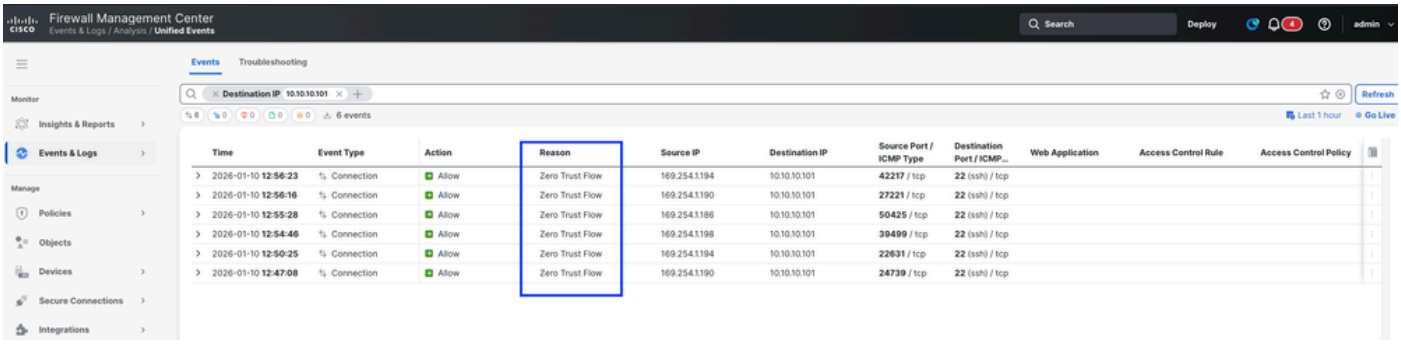


セキュアアクセス – アクティビティ検索



セキュアアクセス – アクティビティ検索

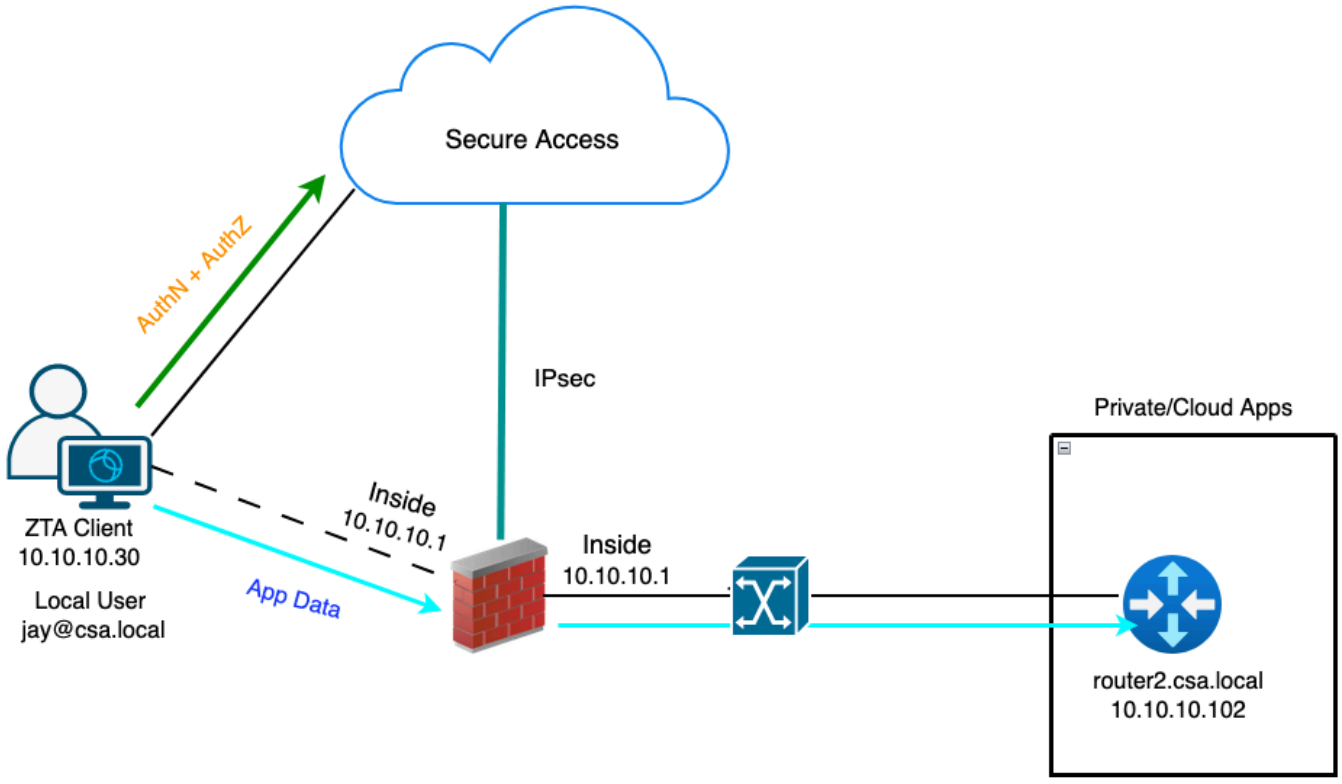
5. FMC接続イベントの確認



FMC接続イベント

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。

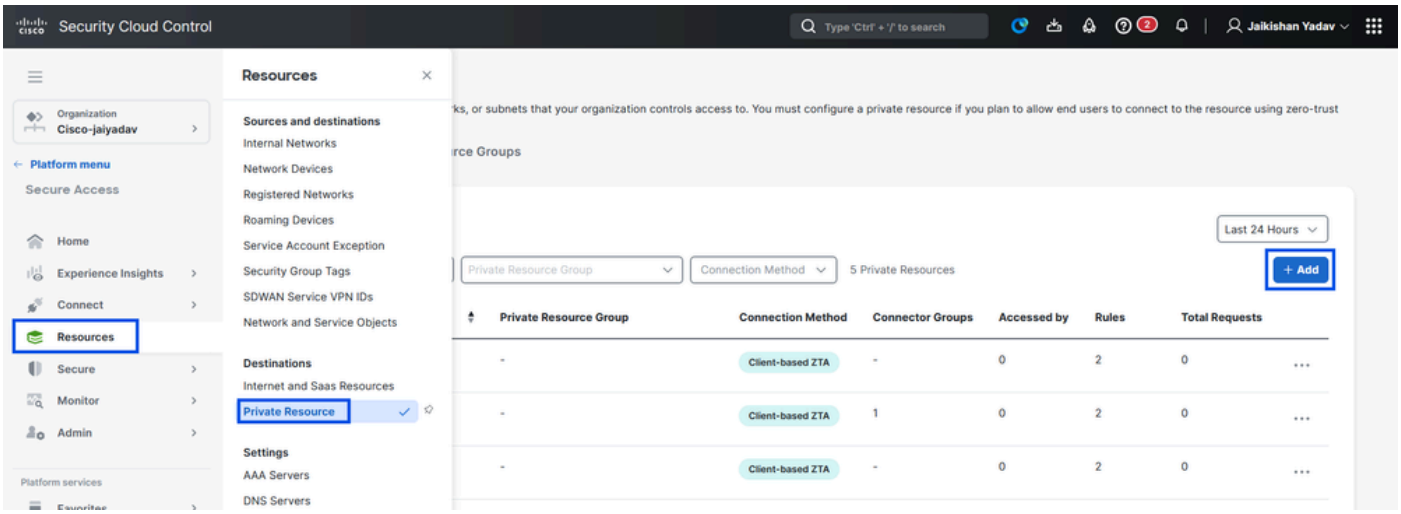


ユニバーサルZTA – テストケースのトポロジ

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

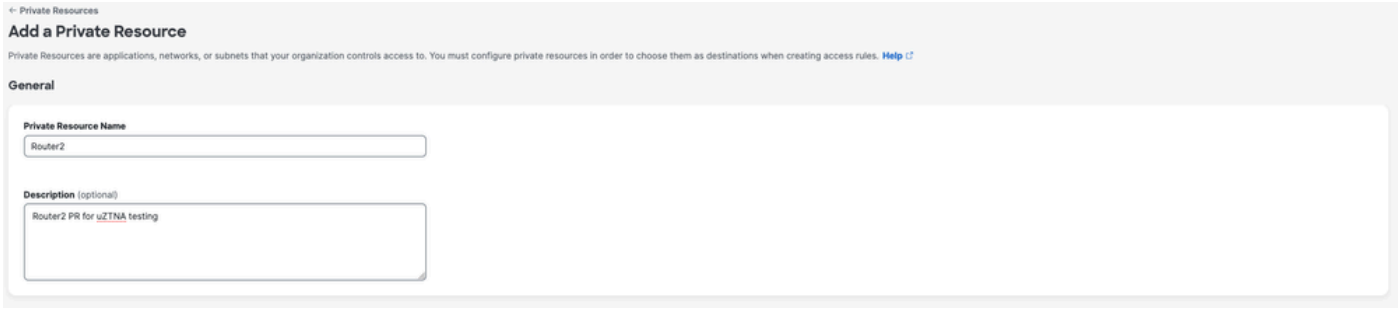
クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

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

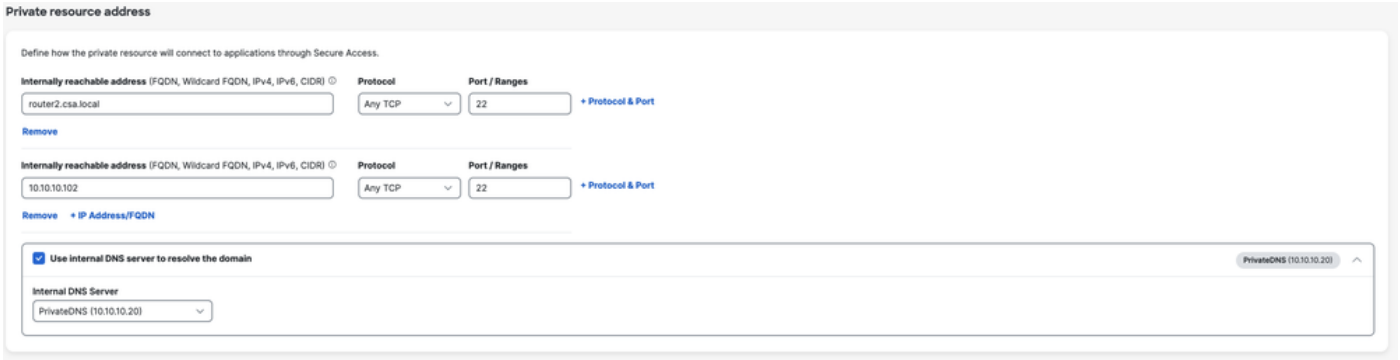
2.「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。



セキュアアクセス：プライベートリソースの設定

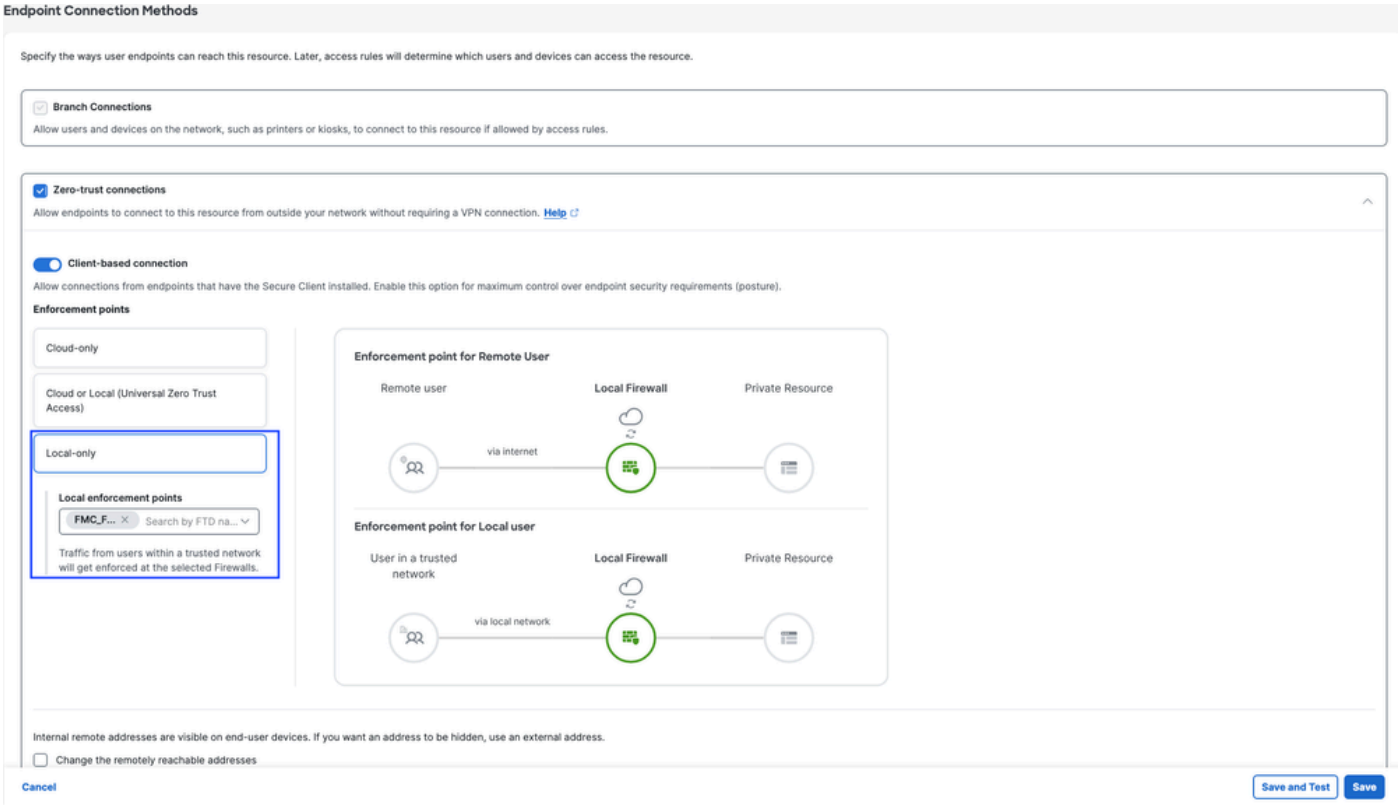
3. アクセスするプライベートリソースのFQDNを入力します。また、プライベートリソースのIPアドレスを定義することもできます。詳細については、「プライベートリソースの追加」を参照してください。

4. ドメインを解決する内部DNSサーバーを選択します



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。



セキュアアクセス：プライベートリソースの設定

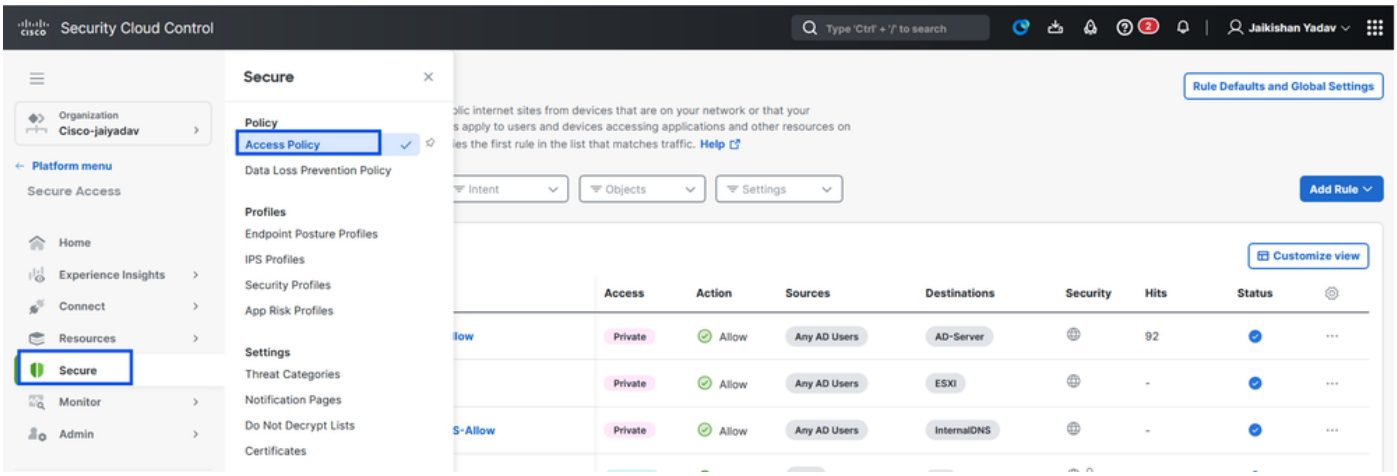
注：選択する登録のタイプ（IPアドレスまたは非IPアドレス）に応じて、この変更によりPRがFTDに自動的に関連付けられ、ポリシーの導入がトリガーされます。

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

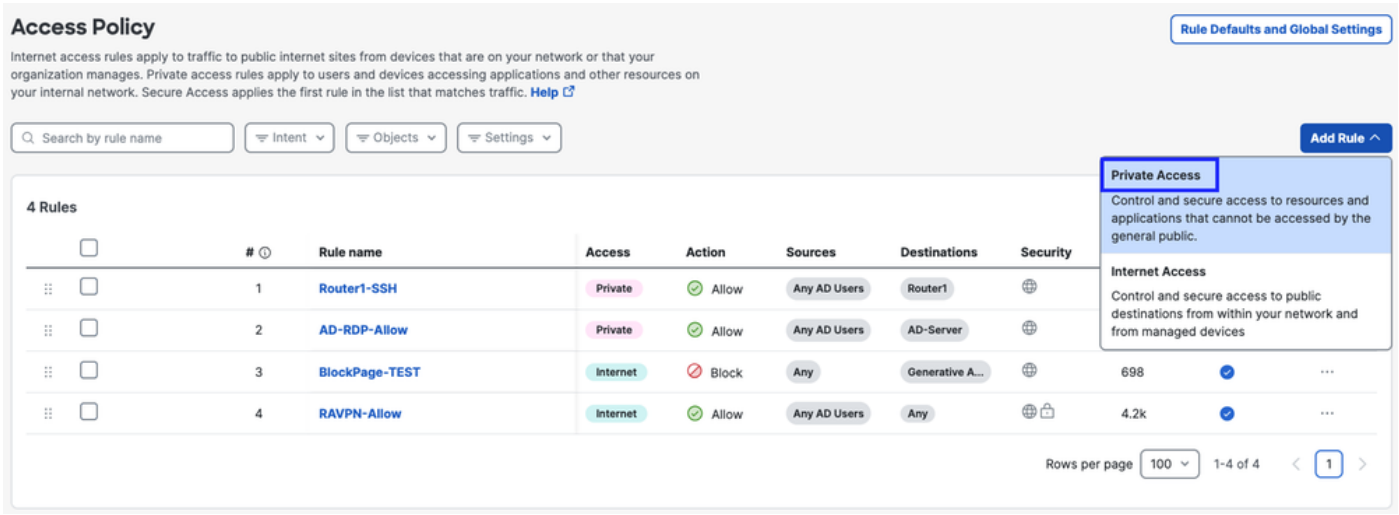
Secure Access上のプライベートアクセスを、ユニバーサルZTA登録済みユーザによるアクセスとなるように設定します（デフォルト）。詳細については、「プライベートアクセスルール」を参照してください

1. Secure > Access Policyの順に移動します。



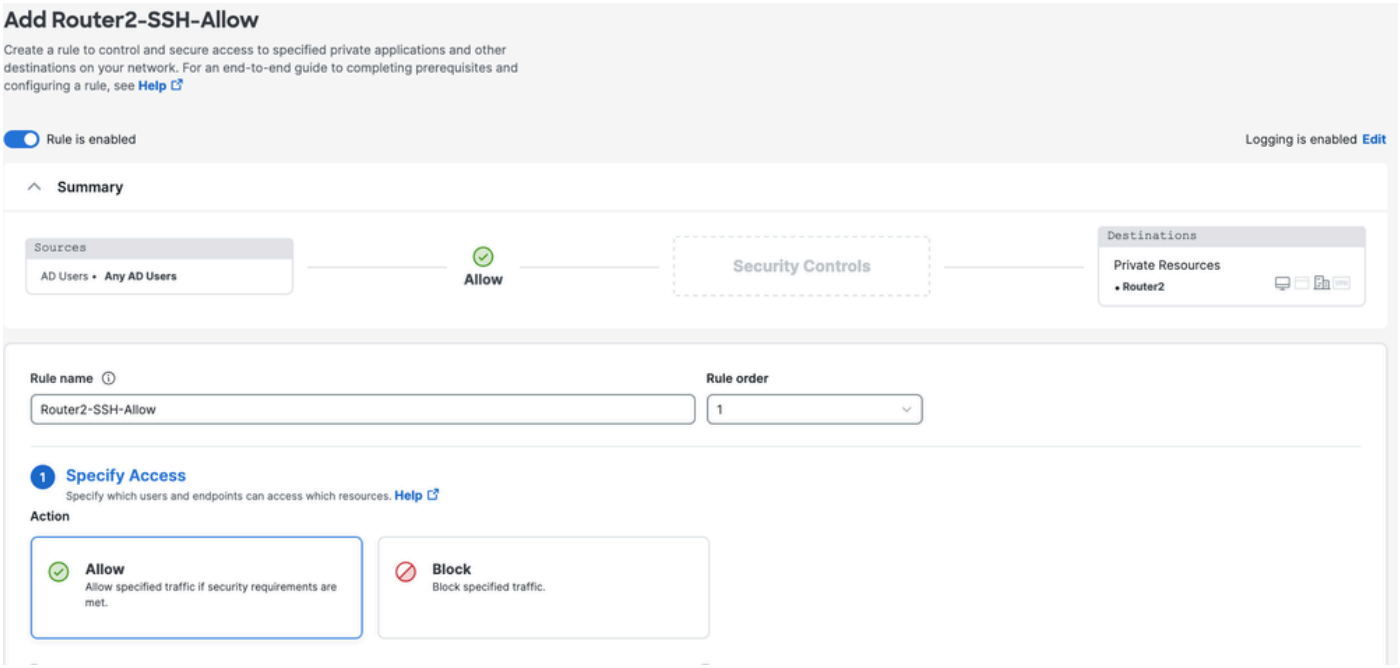
セキュアアクセス：アクセスポリシーの設定

2. Add Ruleをクリックし、Private Accessを選択します。
ルールの上部には、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。



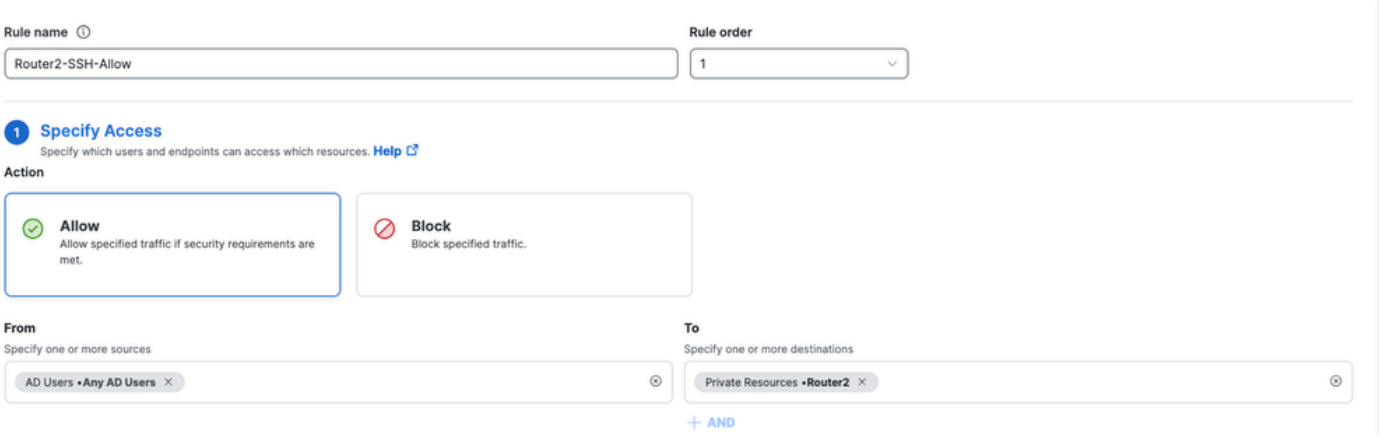
セキュアアクセス：アクセスポリシーの設定

3. ルール名の追加



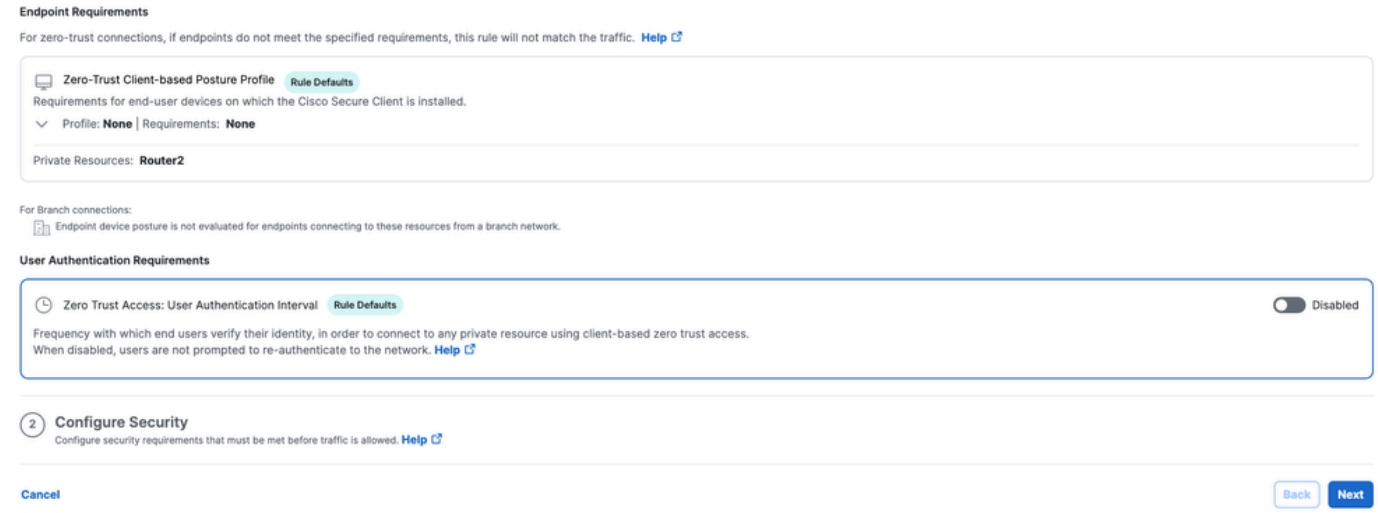
セキュアアクセス：アクセスポリシーの設定

4. ルール処理を選択し、ソースと宛先を選択します



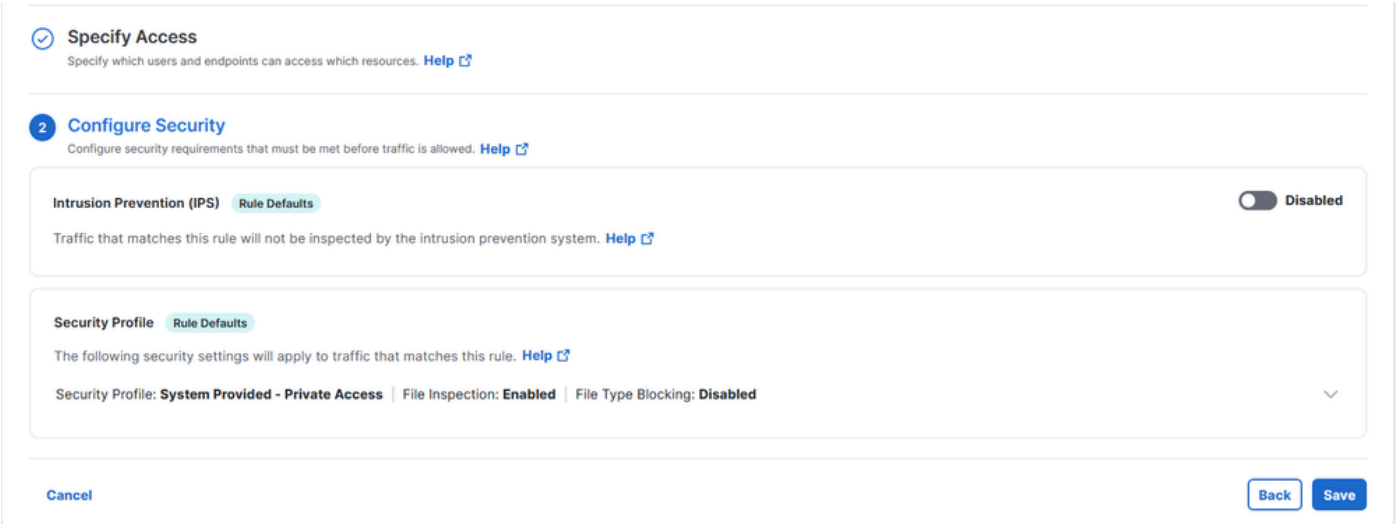
セキュアアクセス：アクセスポリシーの設定

5. エンドポイント要件の設定



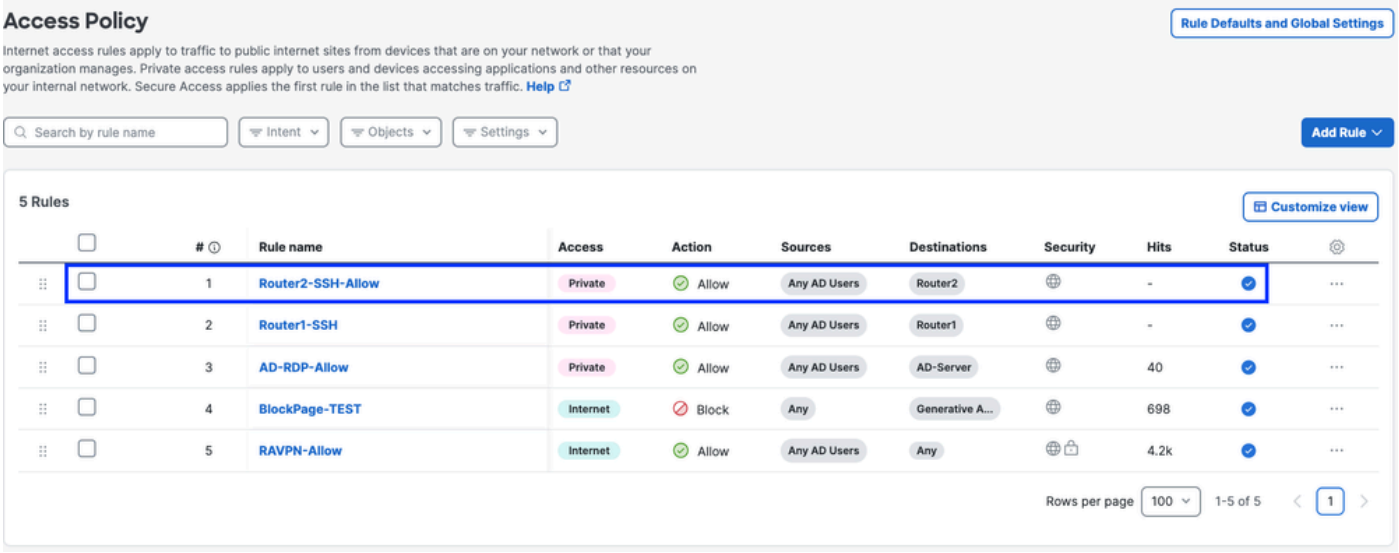
セキュアアクセス：アクセスポリシーの設定

6. セキュリティの設定



セキュアアクセス：アクセスポリシーの設定

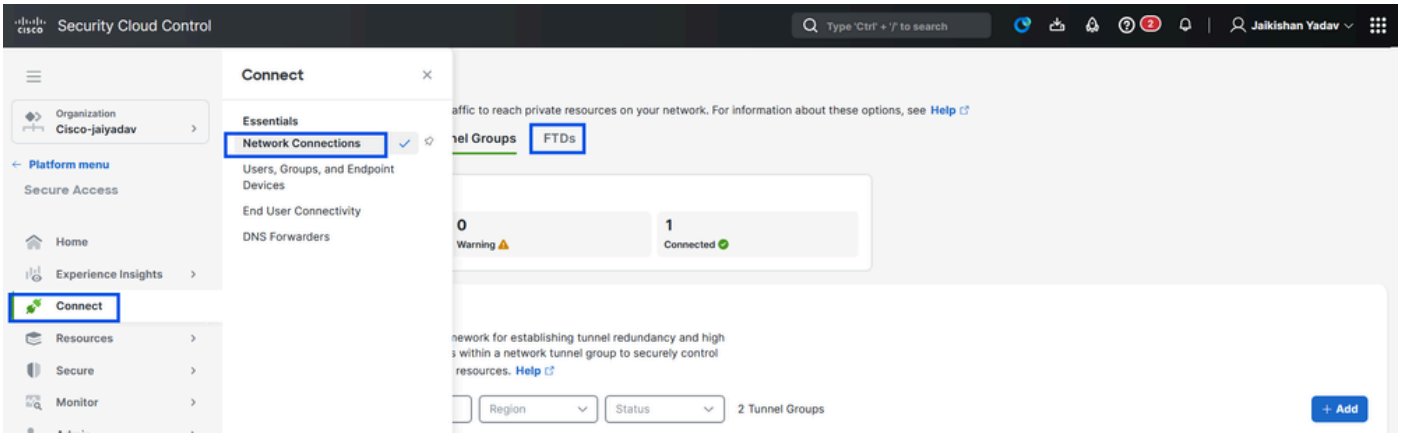
7. Saveをクリックします。



セキュアアクセス：アクセスポリシーの設定

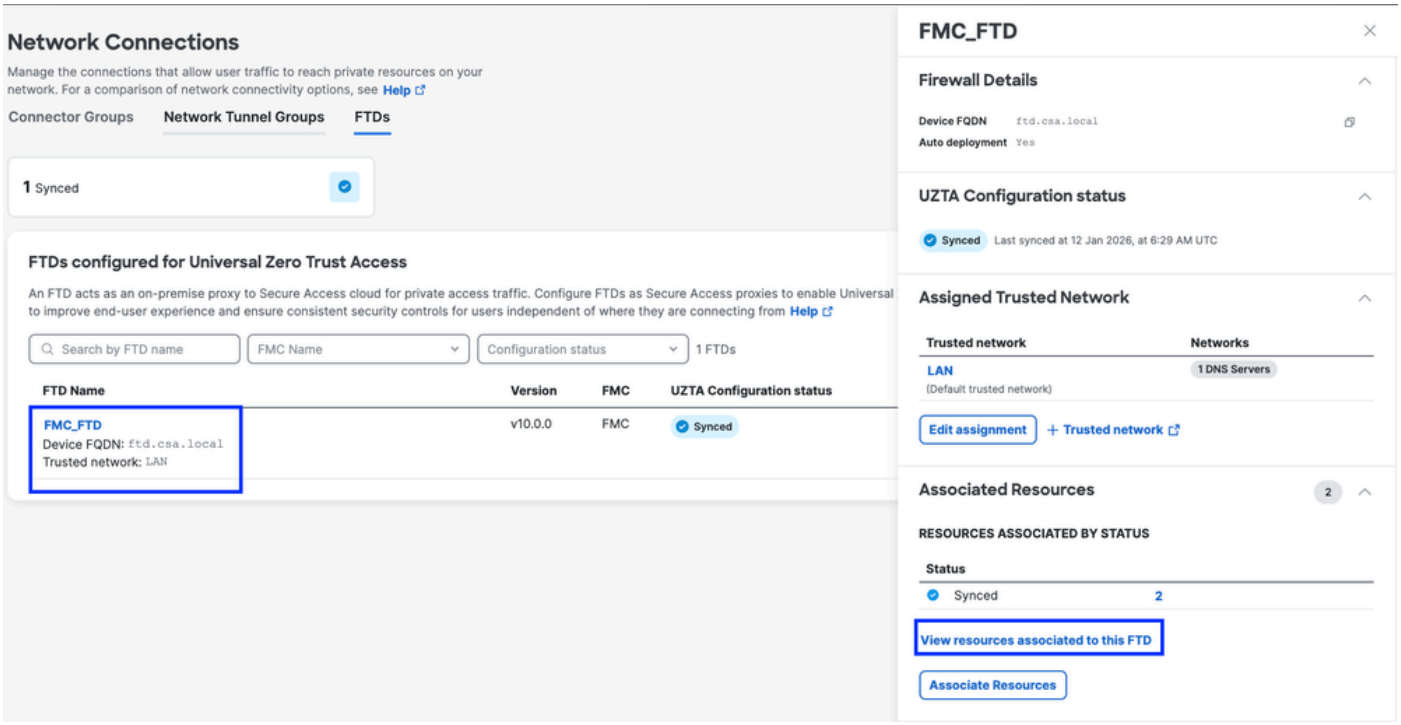
手順3:FTDでのPRの関連付けを確認します

1. 「接続」>「ネットワーク接続」>「FTDs」に移動します。

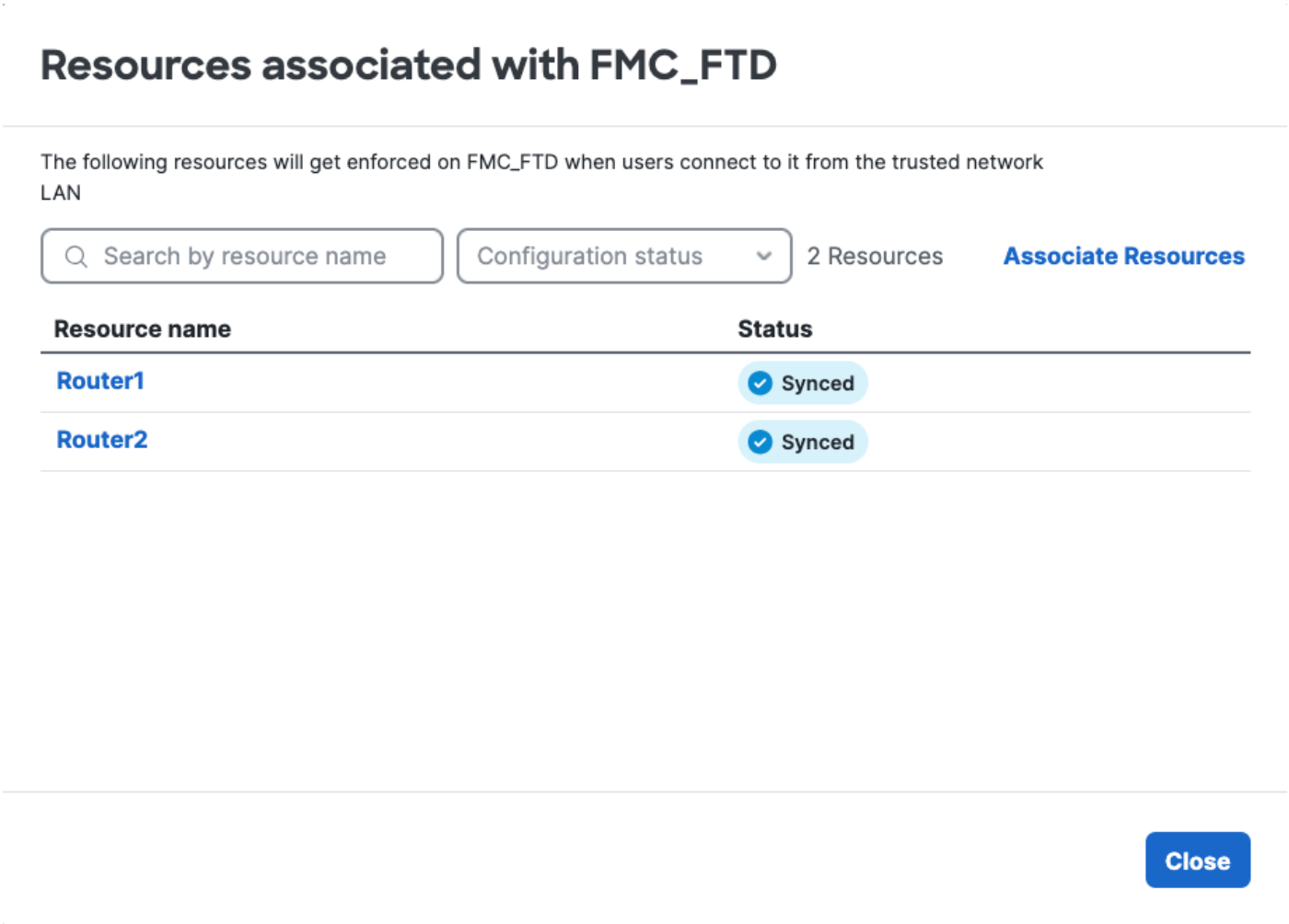


セキュアアクセス – PR検証

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。

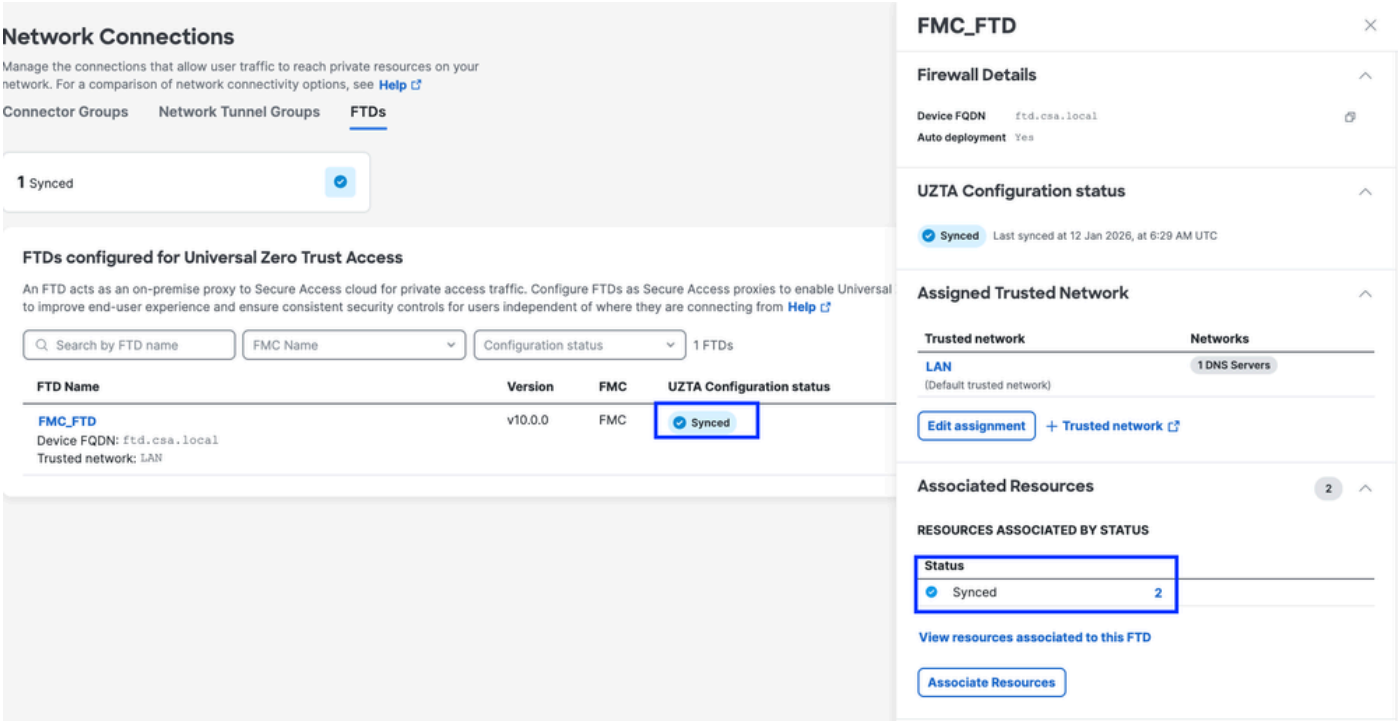


セキュアアクセス – PR検証



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



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。

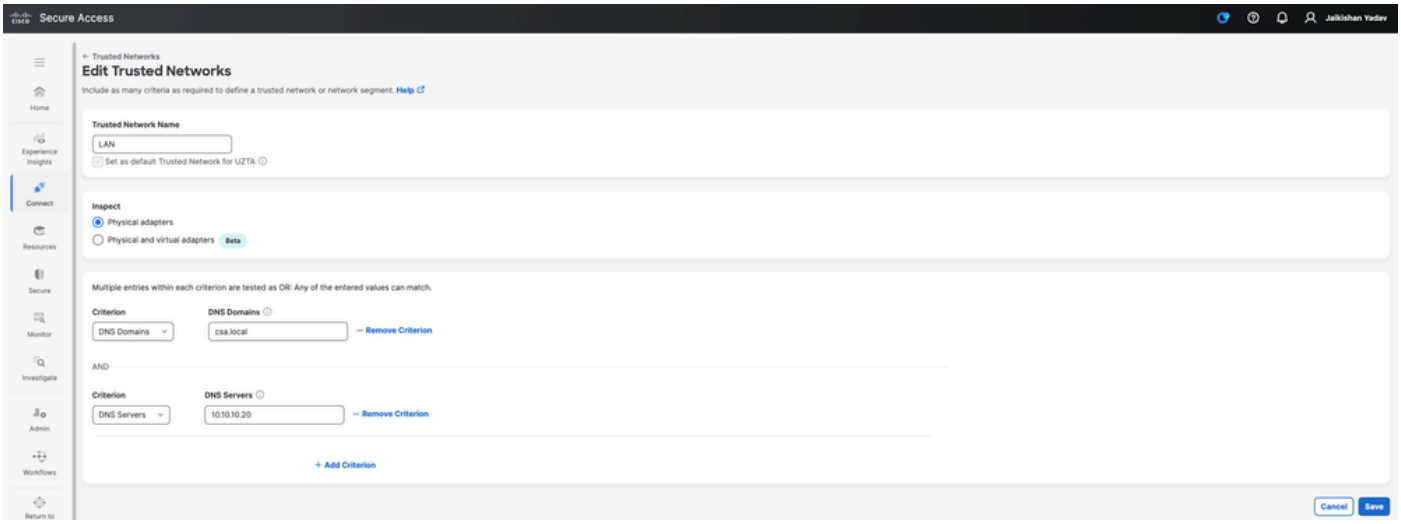
show running-config object application

```
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」

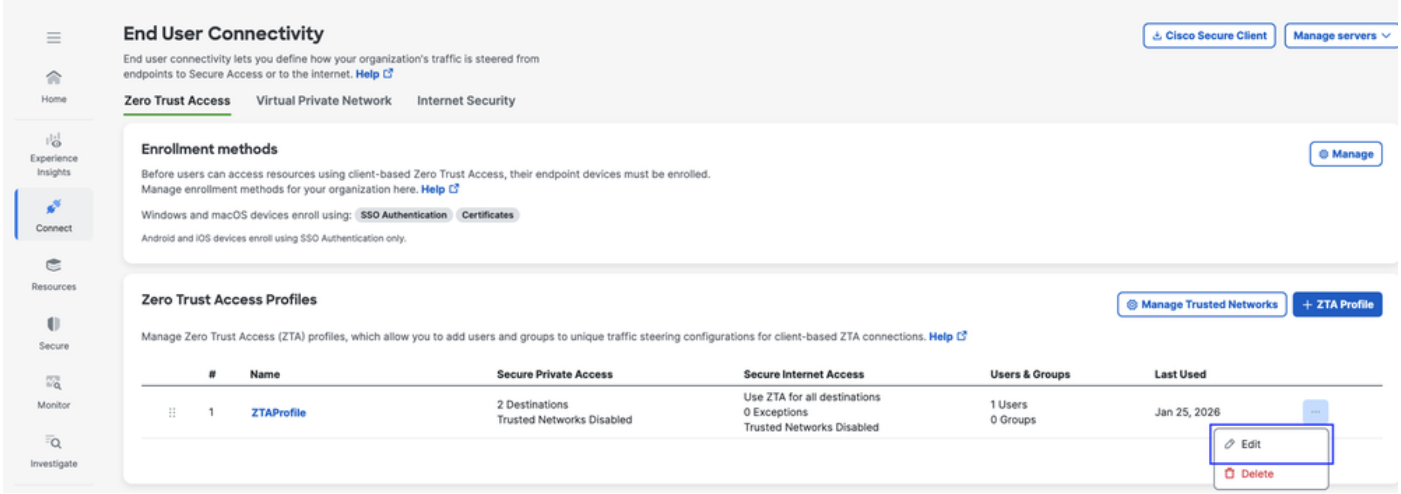
Connect > End User Connectivity > Zero Trust Access > ZTA Settingsの順に移動し、Trusted Networksを設定します。



セキュアアクセス：TNDの設定

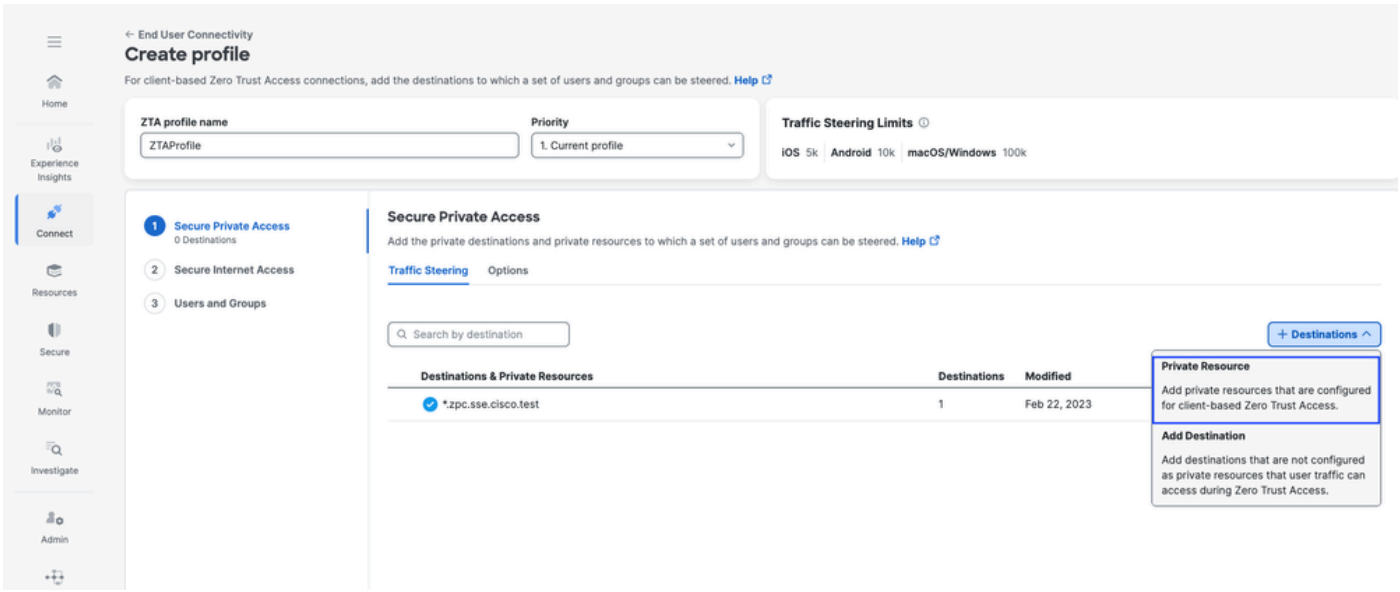
ステップ5 ZTAプロファイルへのプライベートリソースの追加

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

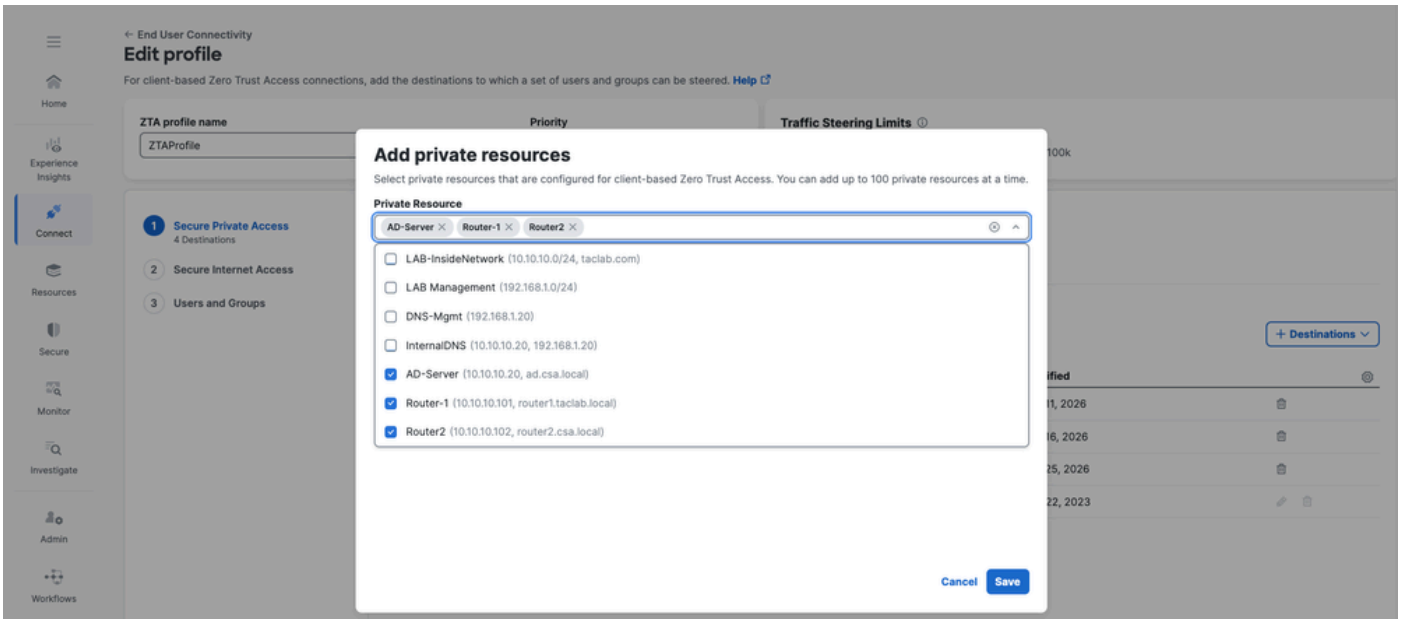


セキュアアクセス – ZTAプロファイル

2. プライベートリソースの追加

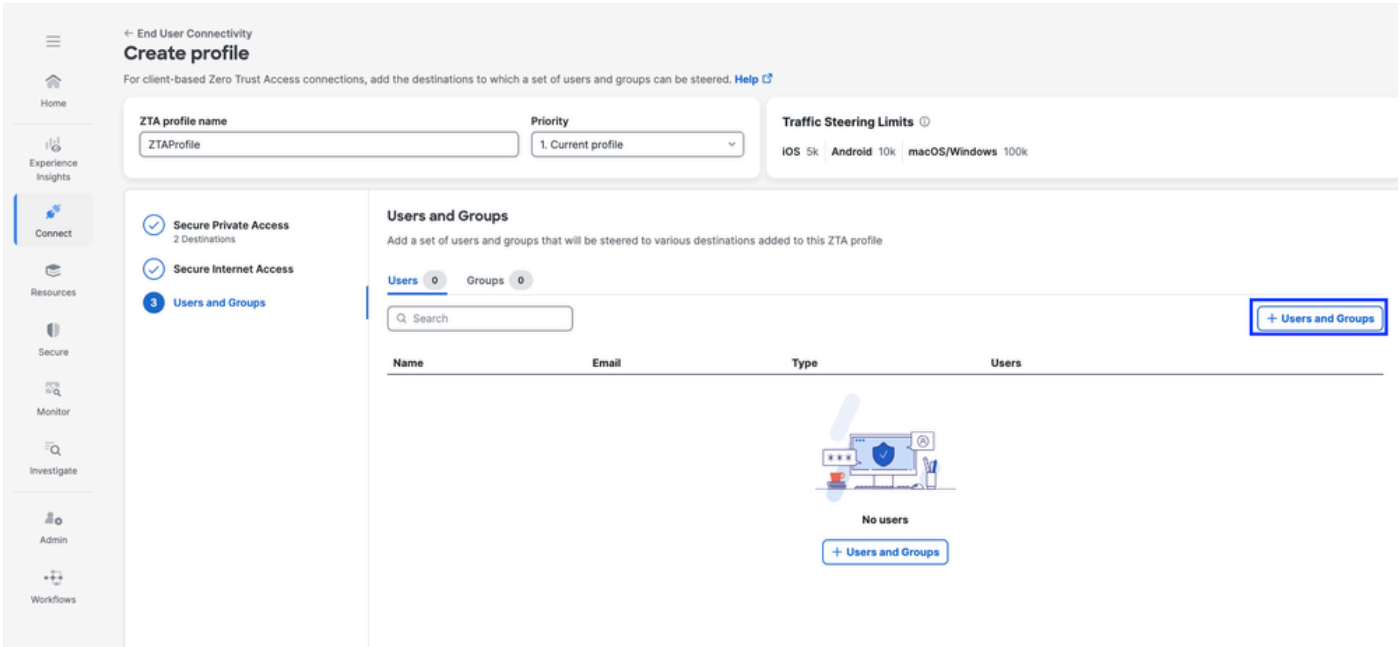


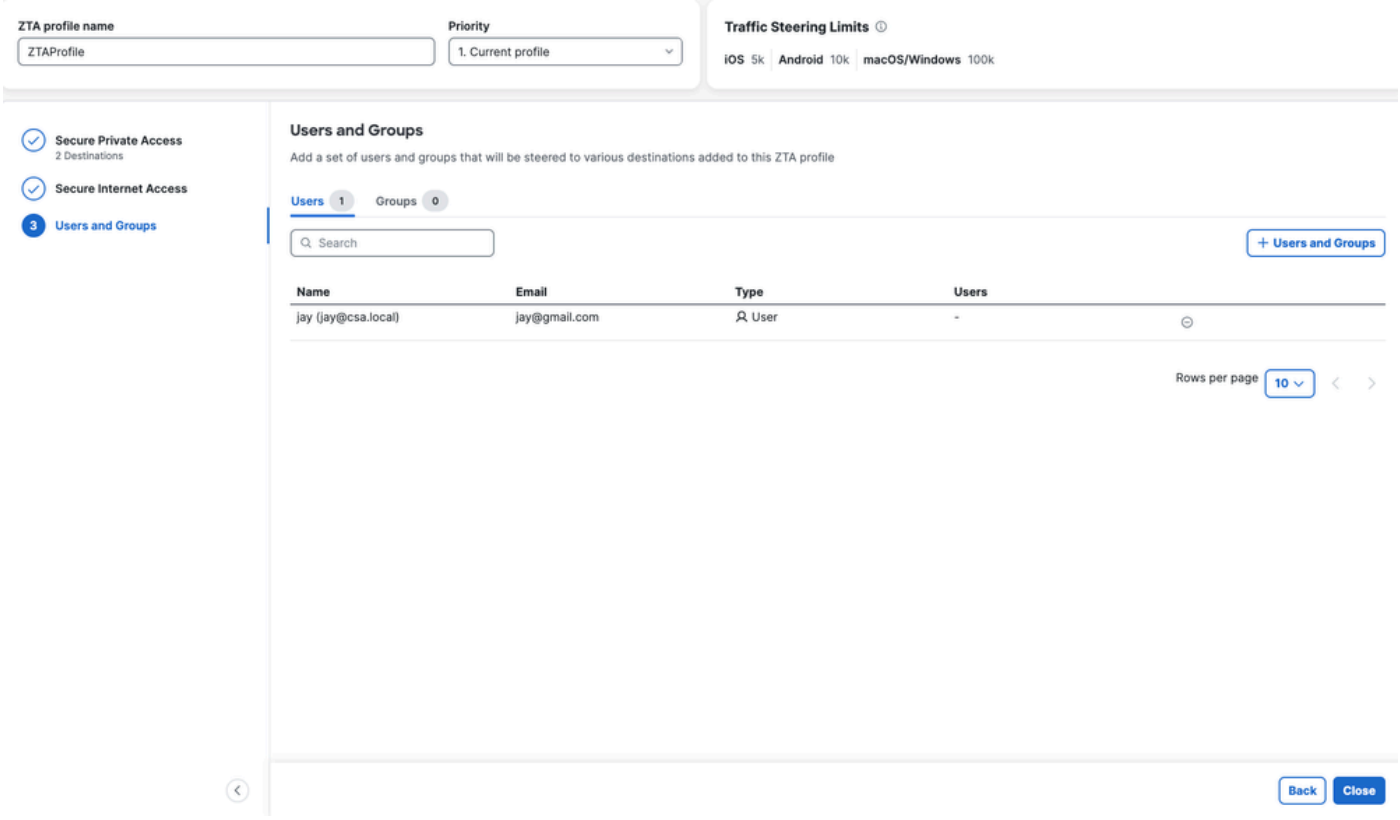
セキュアアクセス – ZTAプロファイル



セキュアアクセス – ZTAプロファイル

3. ユーザーとグループの追加

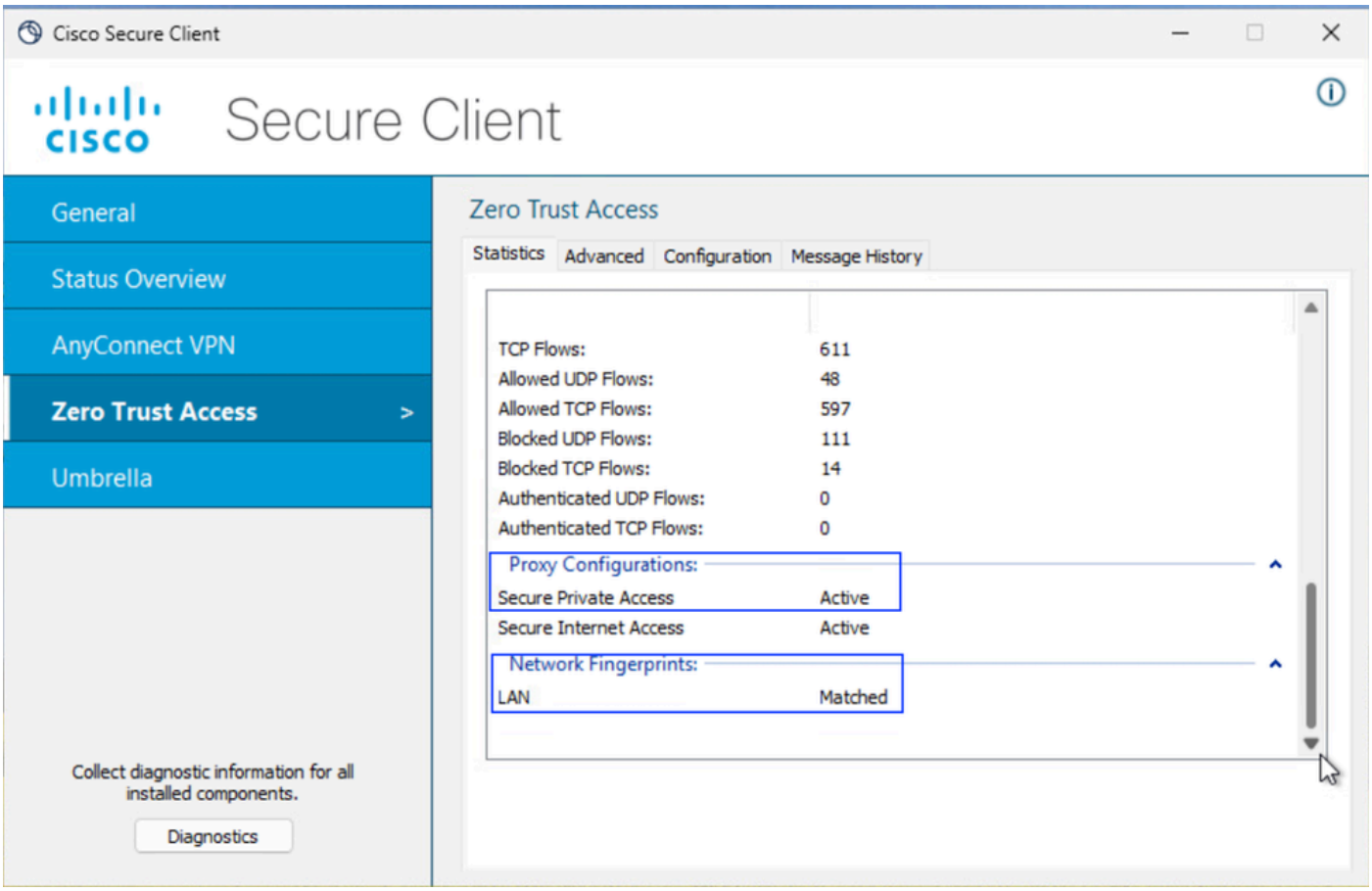




セキュアアクセス – ZTAプロファイル

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

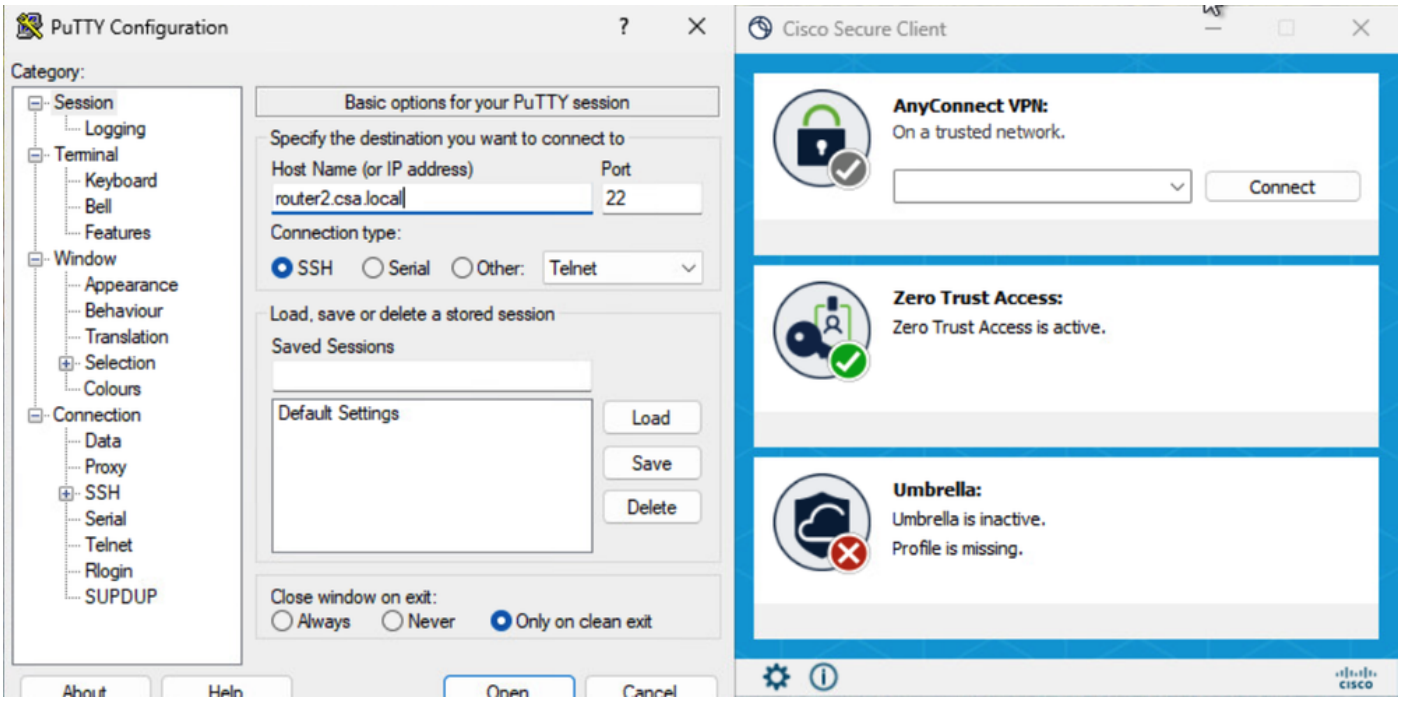
```
C:\Users\jay>ping ftd.csa.local

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
```


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。

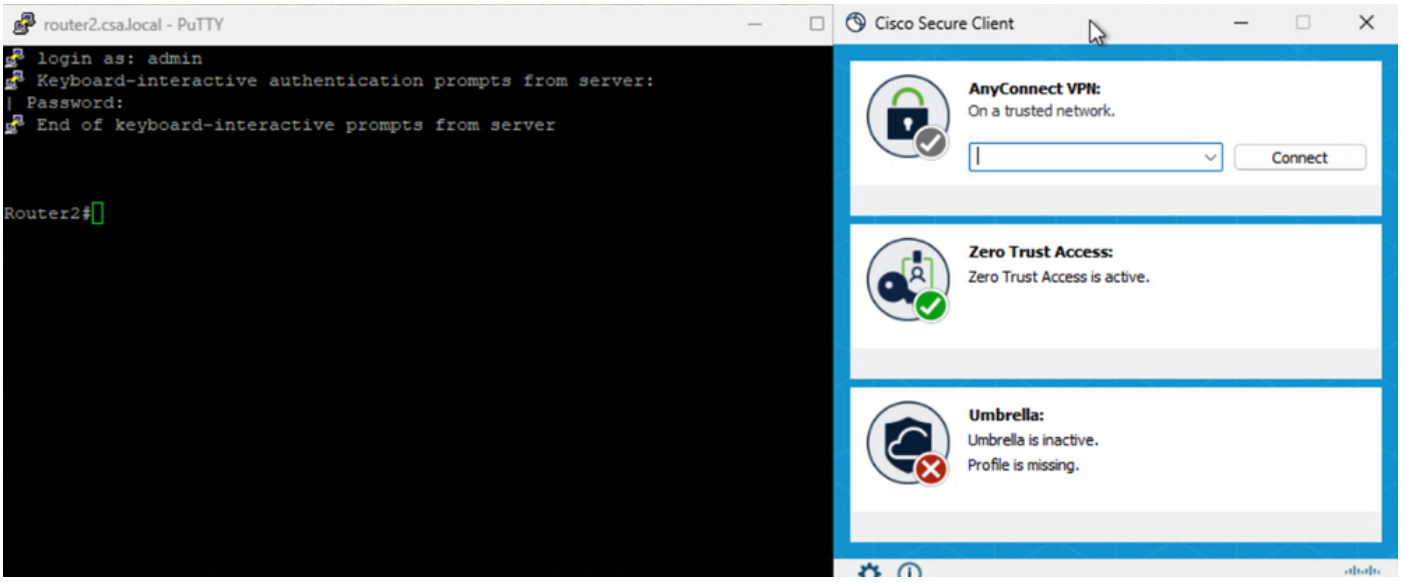
```
ftd# ping router2.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/60 ms
ftd#
```


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

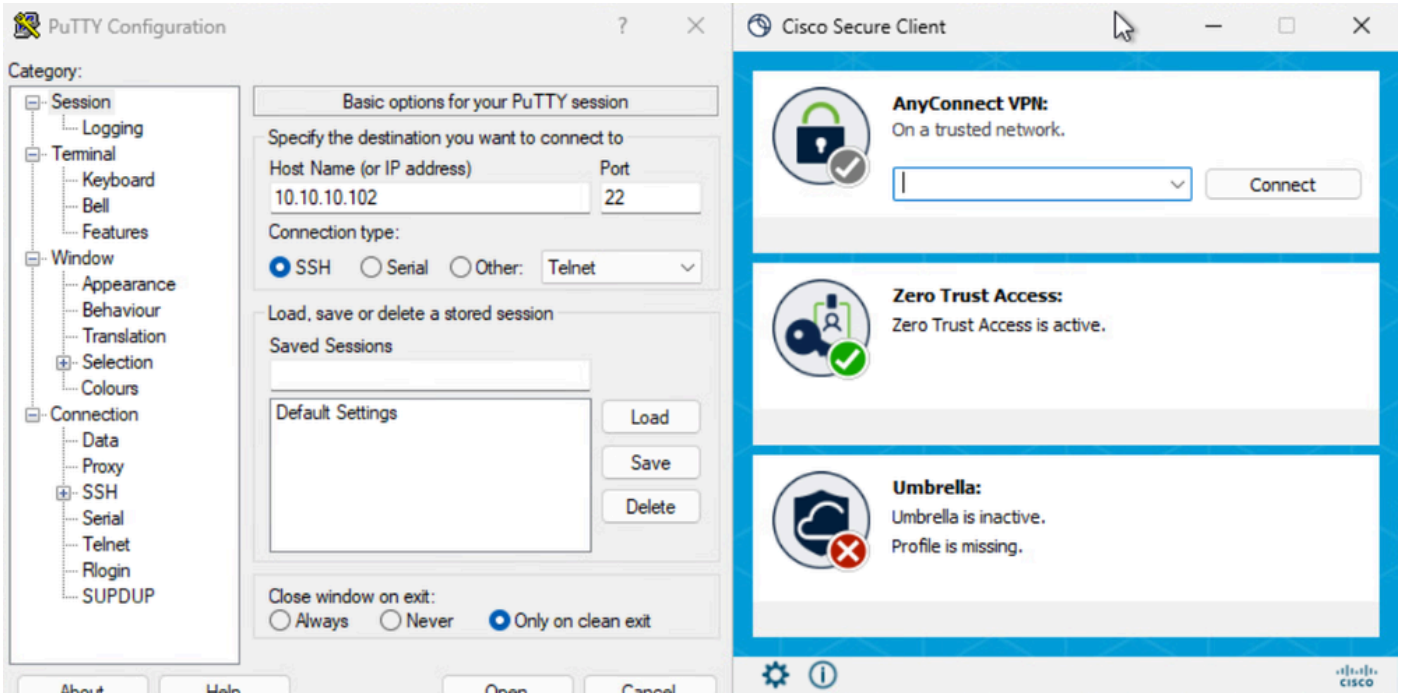


セキュアなアクセス – PRテスト

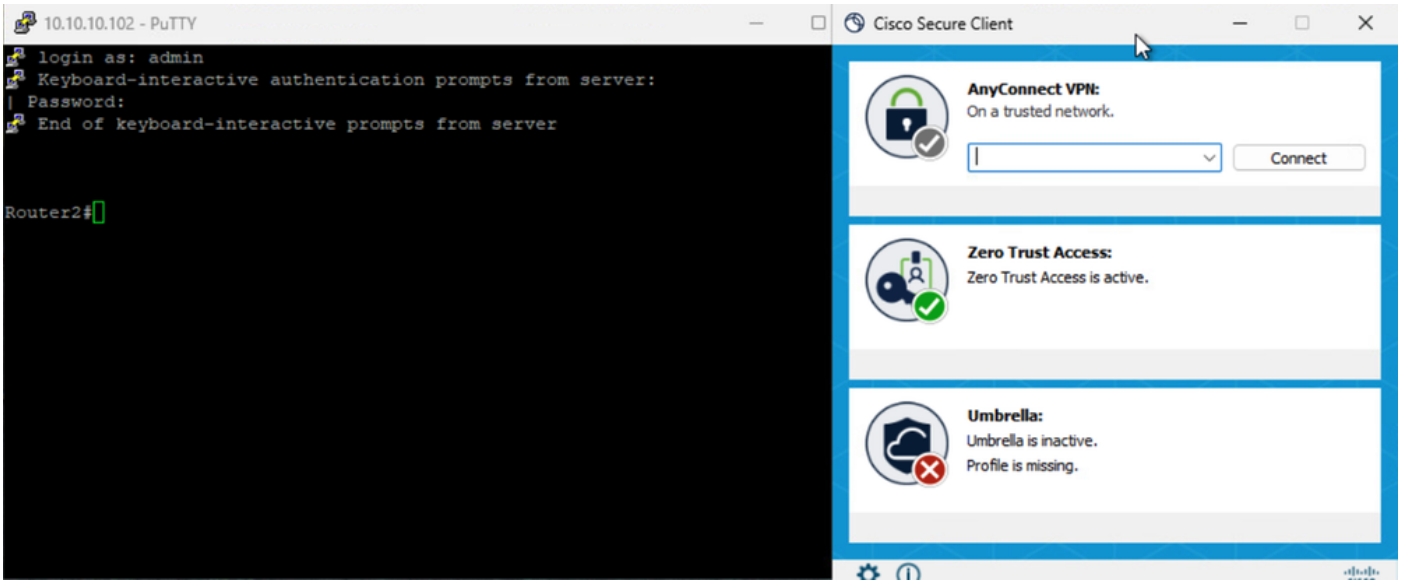


セキュアなアクセス – PRテスト

IPアドレスを使用してPRにアクセスします

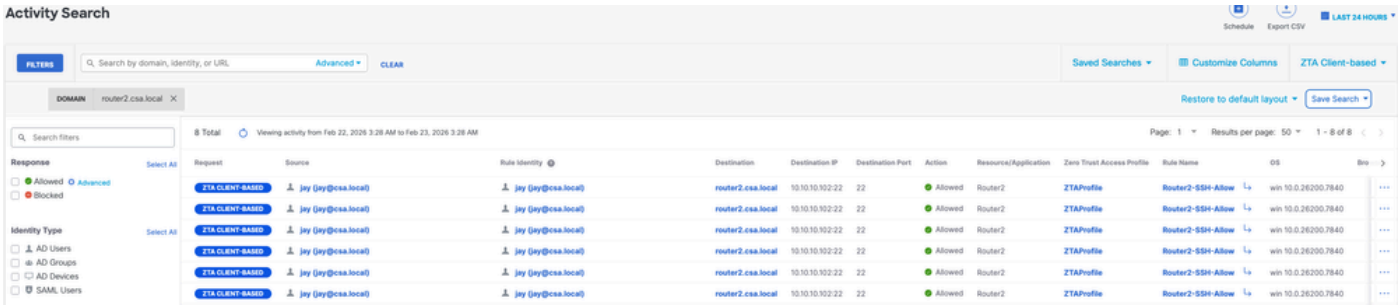


セキュアなアクセス – PRテスト

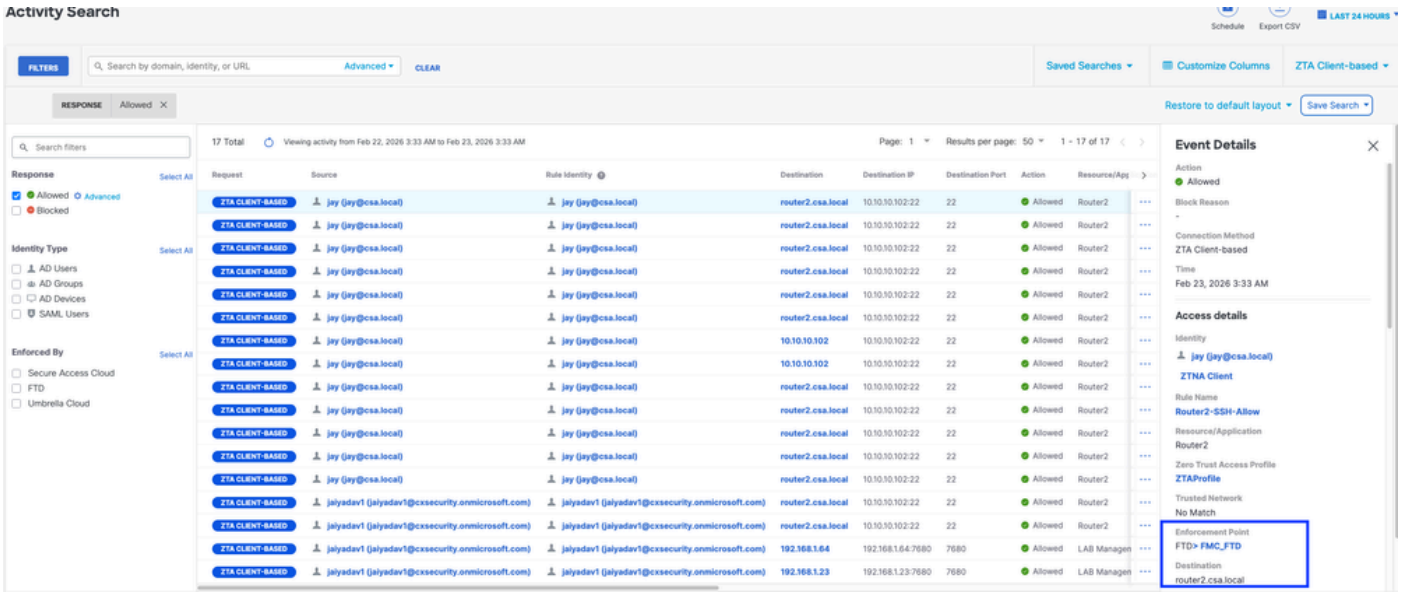


セキュアなアクセス – PRテスト

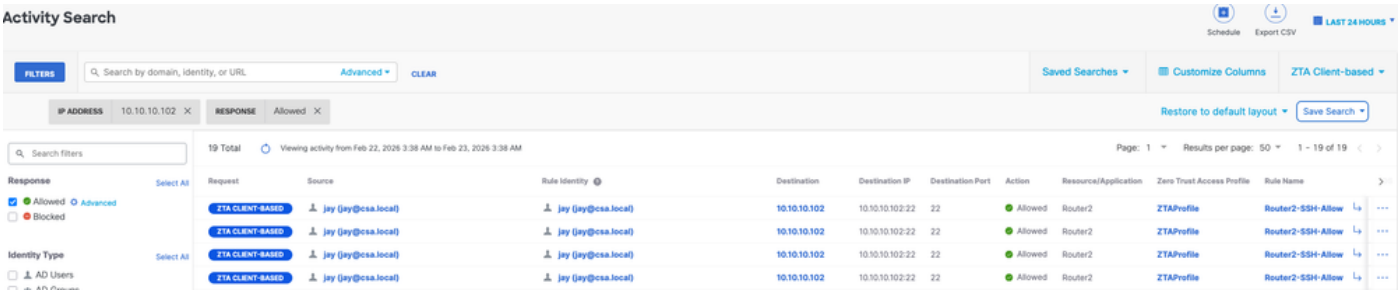
5. セキュアアクセスアクティビティの検索ログの確認



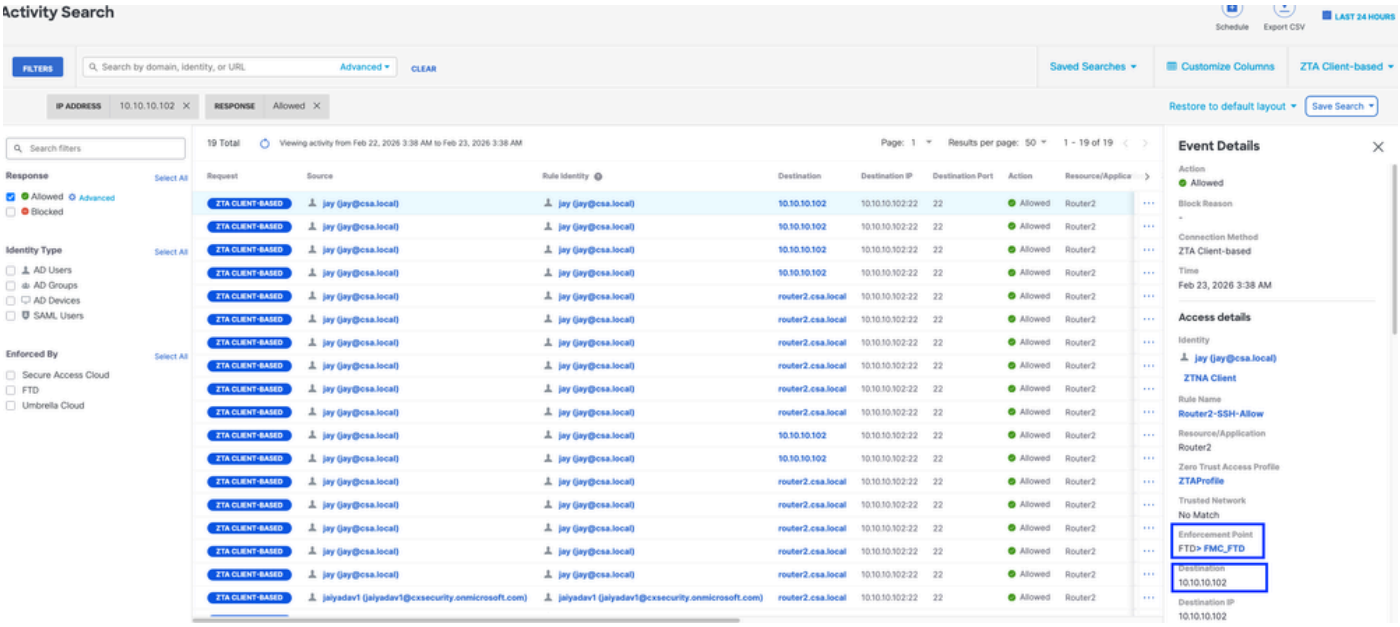
セキュアアクセス – アクティビティ検索



セキュアアクセス – アクティビティ検索

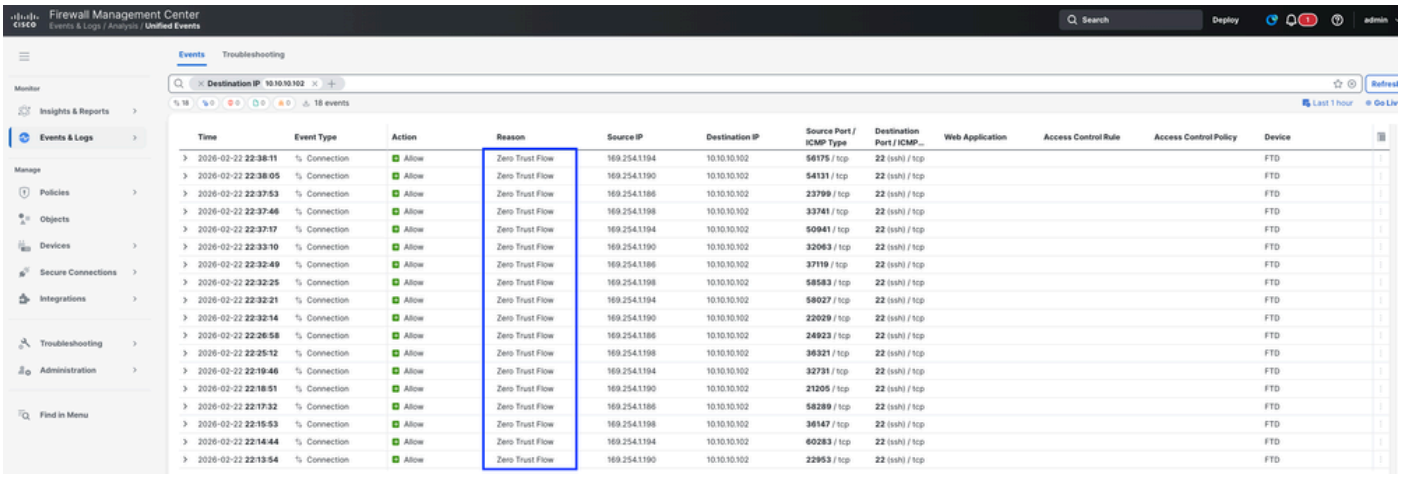


セキュアアクセス – アクティビティ検索



セキュアアクセス – アクティビティ検索

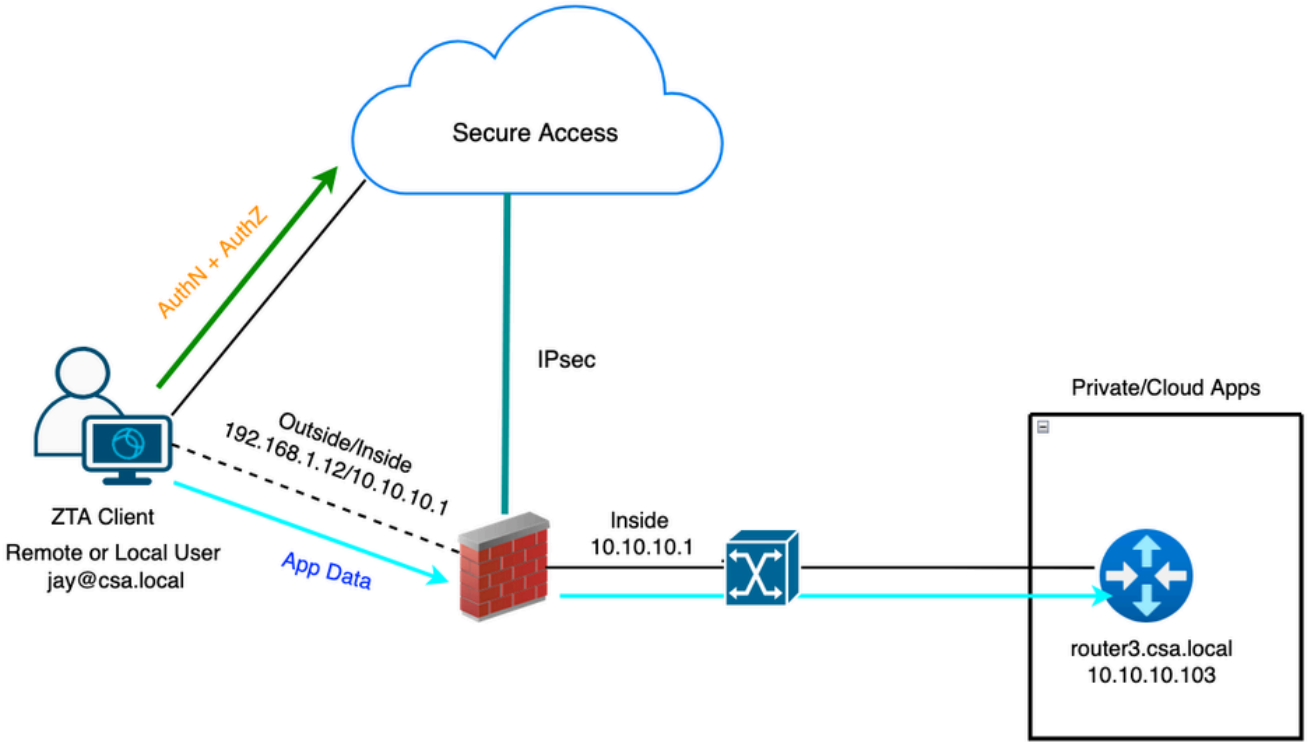
6. FMC接続イベントの確認



FMC接続イベント

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

この場合、適用のタイプはユーザの場所によって異なります。ユーザがローカルまたは信頼されたFTDゾーン（内部、DMZなど）の背後にある場合、適用はローカルになります（テストケース3）。 一般的に、ユーザがリモートの場合、エンフォースメントはクラウドになります（テストケース1）。 ユーザの場所は、ネットワークのフィンガープリントまたはTNDの設定に基づいて決定されます。ネットワークのフィンガープリントが一致する場合は、ユーザのローカルが「ローカル」になり、一致しない場合は、ユーザのローカルが「リモート」と見なされます。

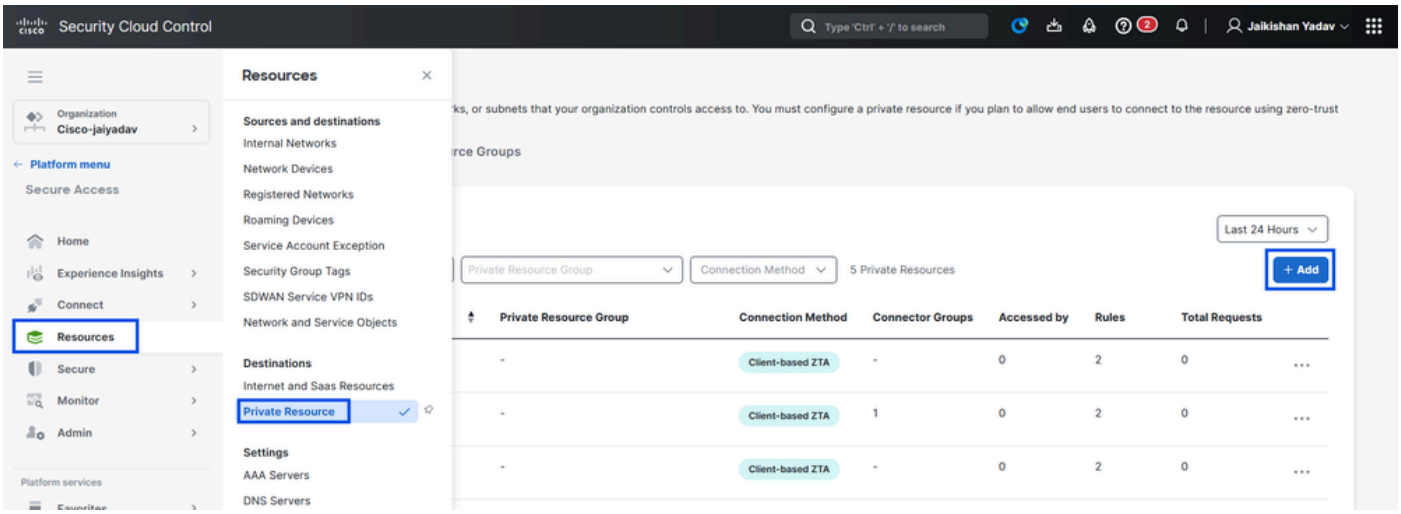


ユニバーサルZTA – テストケースのトポロジ

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

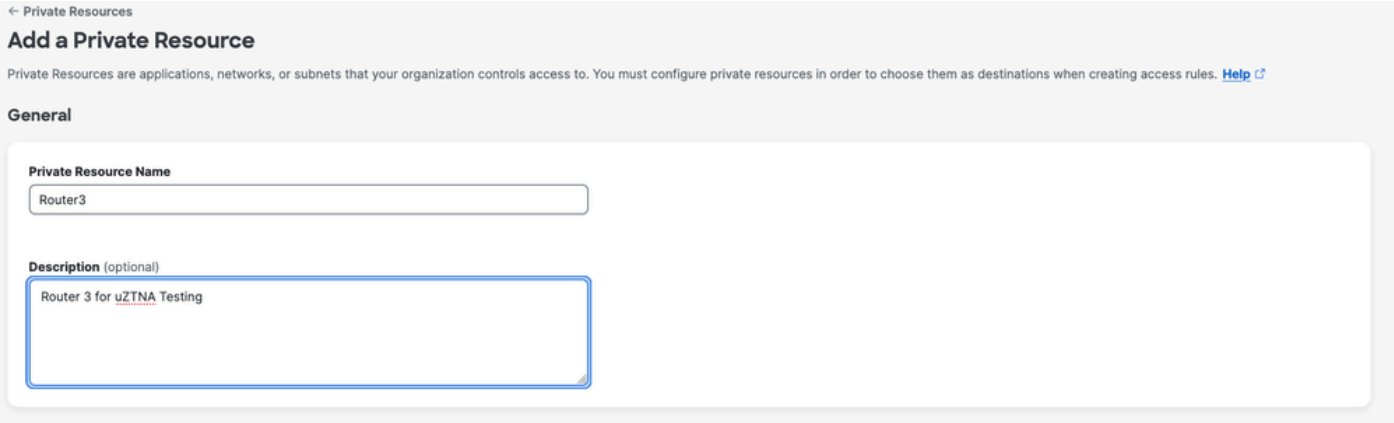
クラウドを適用したゼロトラストアクセス(ZTA)登録済みデバイス経由でアクセスできるように、プライベートリソースを設定します。

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

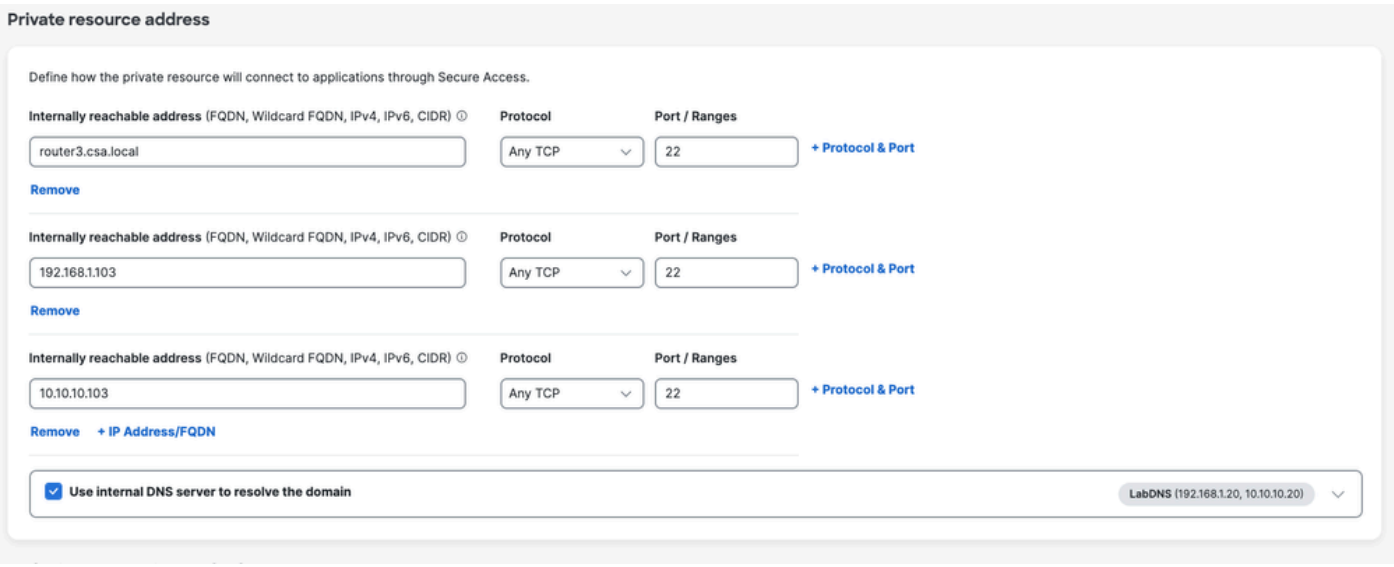
2.「プライベート・リソース名」に、リソースのわかりやすい名前を入力します。説明については、リソースの目的やリソース所有者の名前などの情報を提供することをお勧めします。



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。

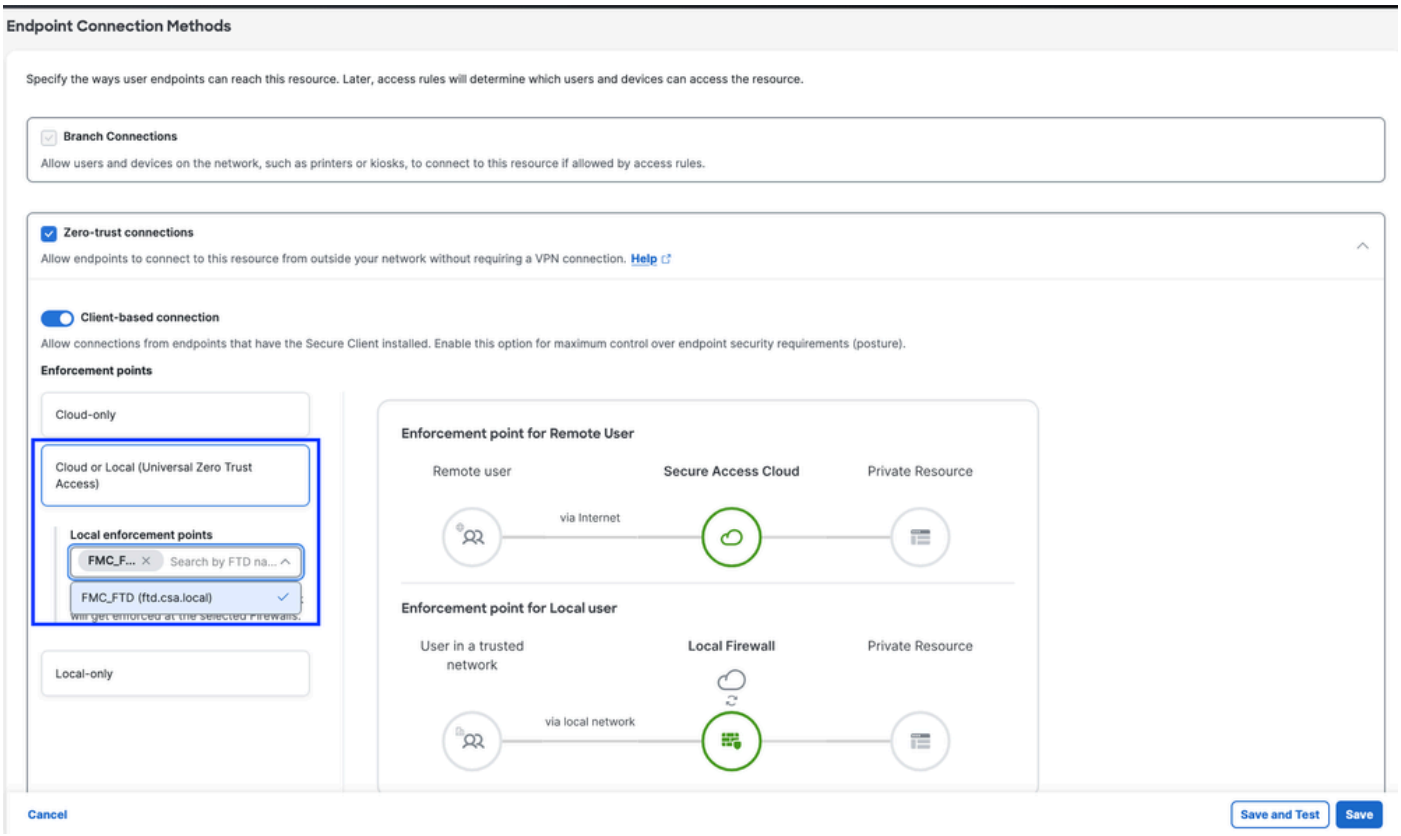
4. ドメインを解決するDNSサーバーを選択します



セキュアアクセス：プライベートリソースの設定

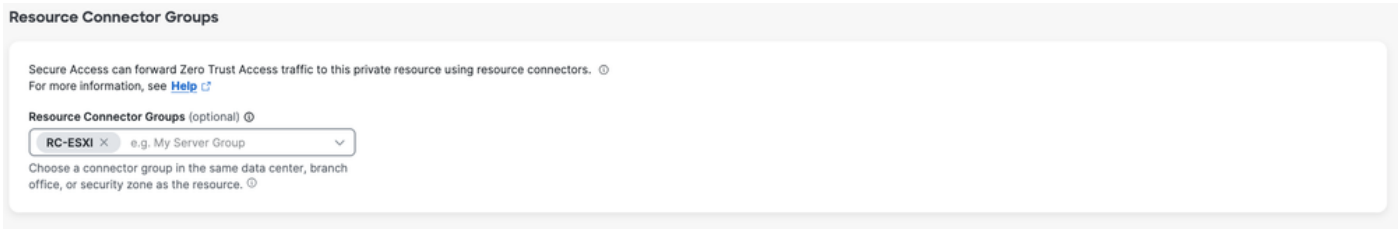
5. エンドポイント接続方法の選択

6. ローカル強制ポイントとしてFTDを選択します。



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。



セキュアアクセス：プライベートリソースの設定

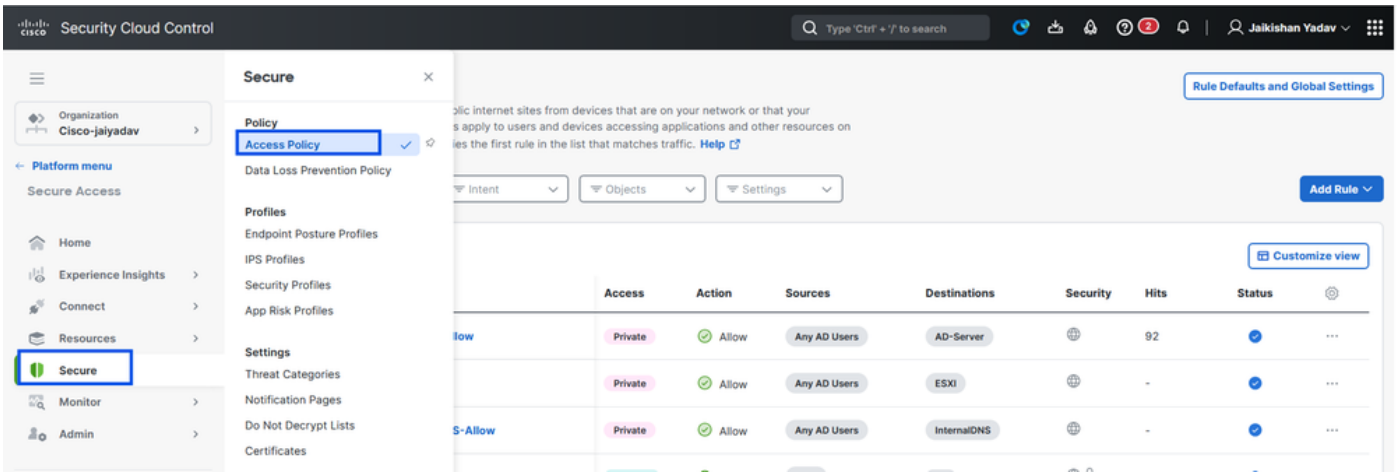
注：選択する登録のタイプ（IPアドレスまたは非IPアドレス）に応じて、この変更によりPRがFTDに自動的に関連付けられ、ポリシーの導入がトリガーされます。

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

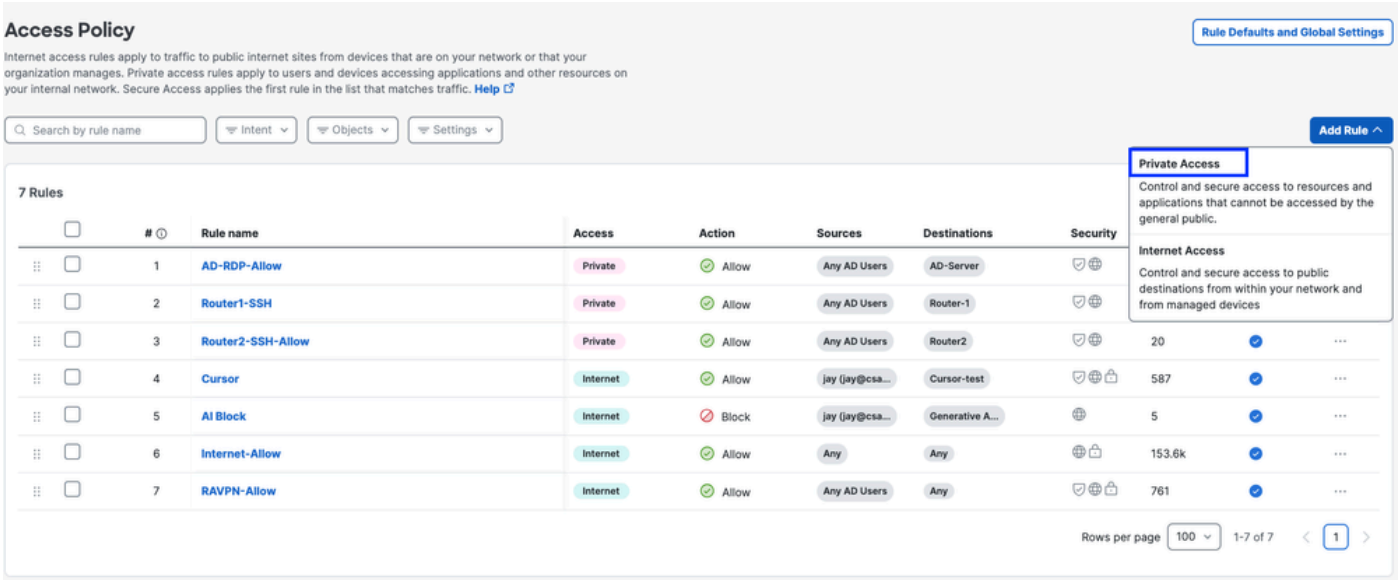
Secure Access上のプライベートアクセスを、ユニバーサルZTA登録済みユーザによるアクセスとなるように設定します（デフォルト）。詳細については、「プライベートアクセスルール」を参照してください

1. Secure > Access Policyの順に移動します。



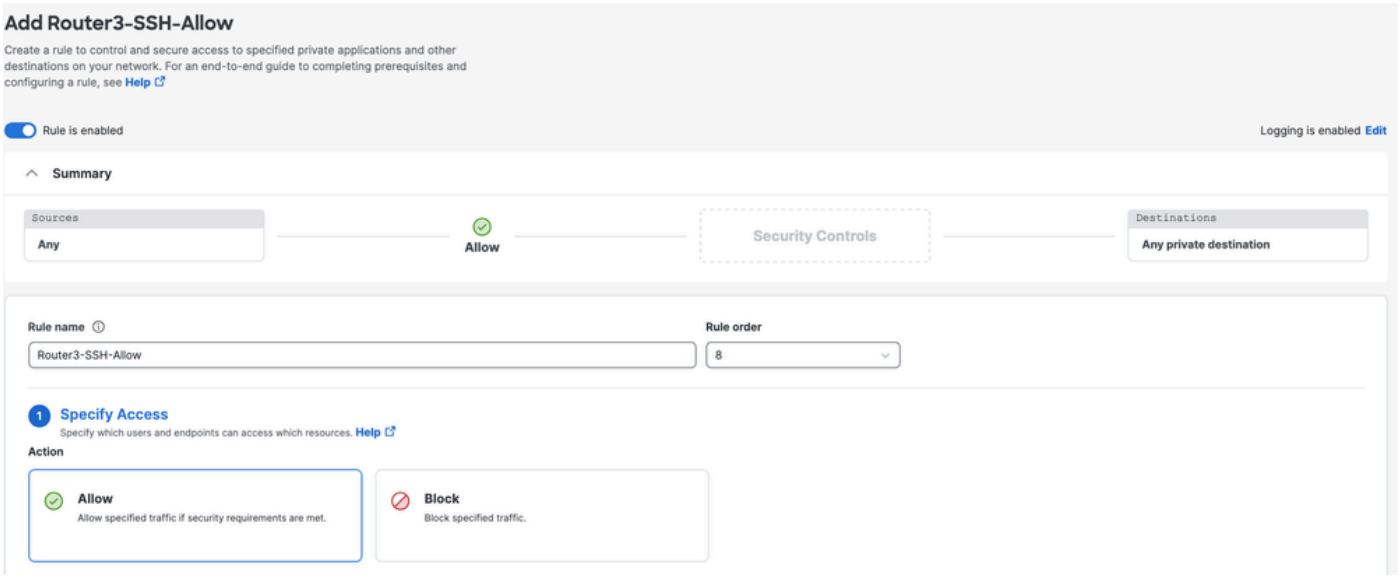
セキュアアクセス：アクセスポリシーの設定

2. Add Ruleをクリックし、Private Accessを選択します。
ルールの上部には、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。



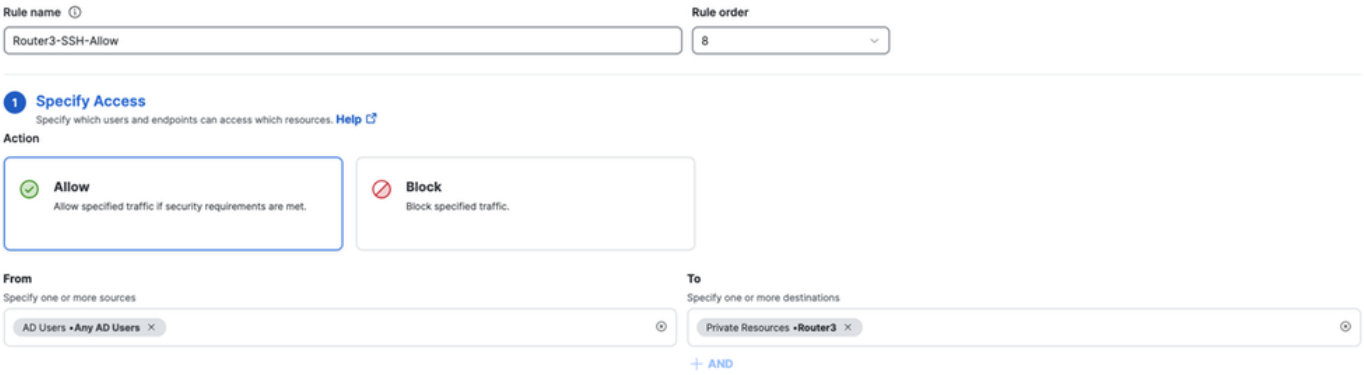
セキュアアクセス：アクセスポリシーの設定

3. ルール名の追加



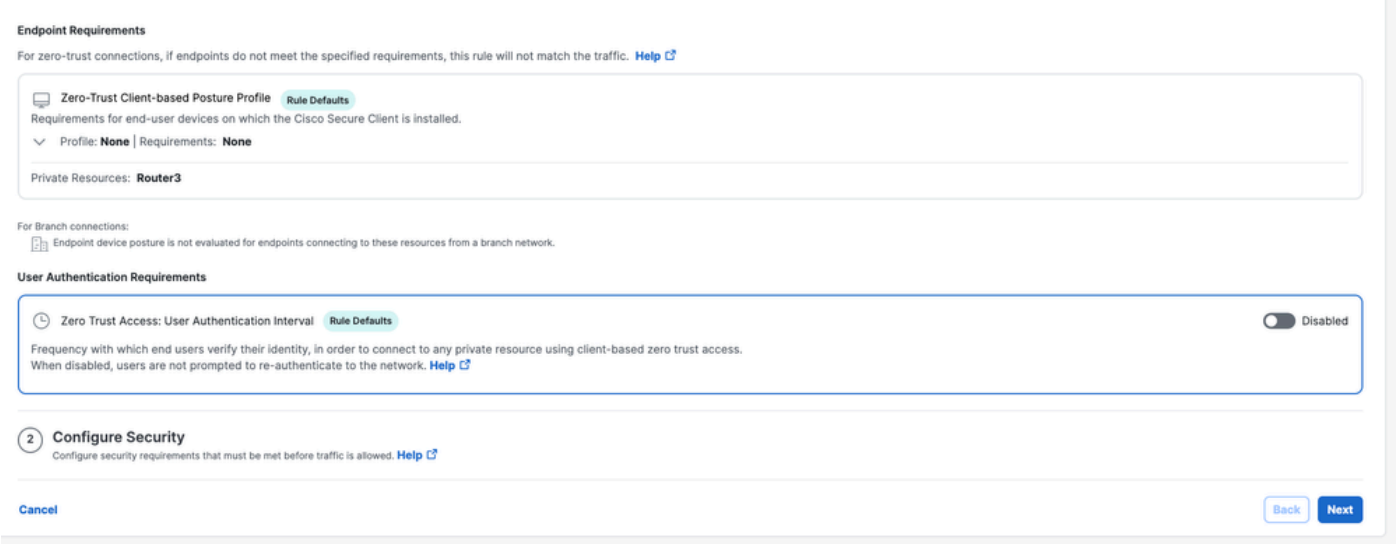
セキュアアクセス：アクセスポリシーの設定

4. ルール処理を選択し、ソースと宛先を選択します

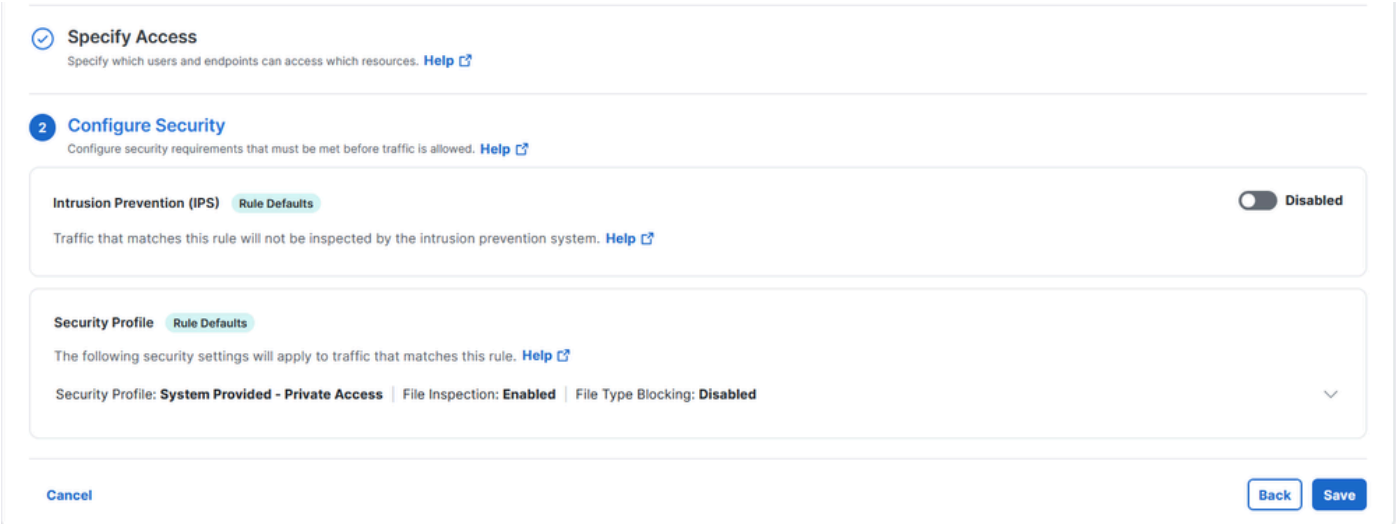


セキュアアクセス：アクセスポリシーの設定

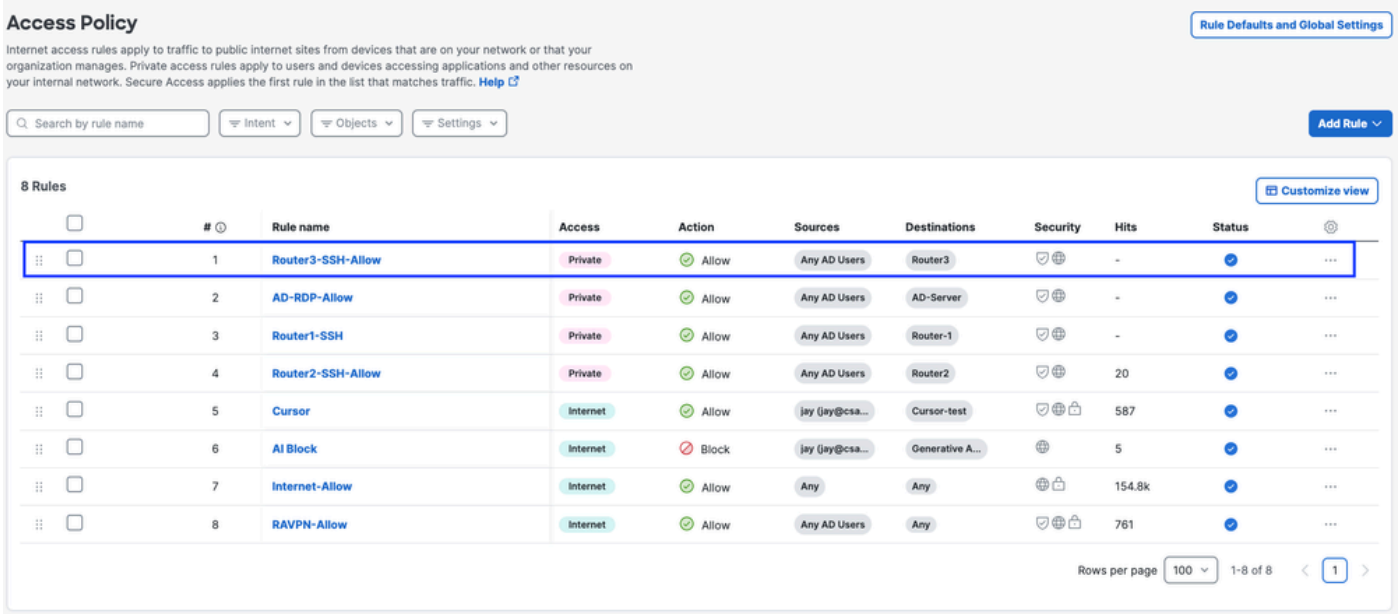
5. エンドポイント要件の設定



6. セキュリティの設定



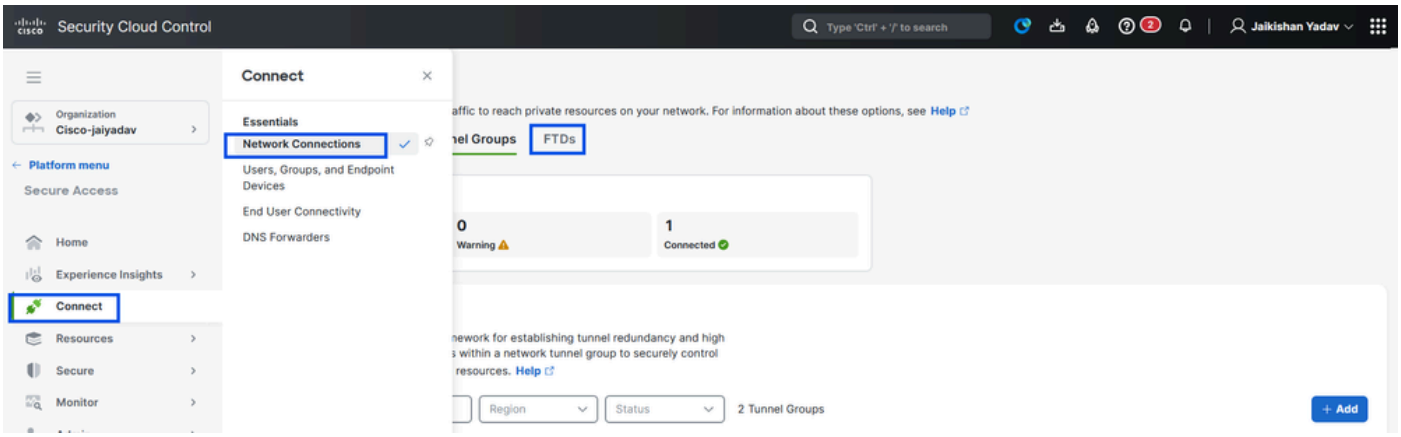
7. Saveをクリックします。



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。

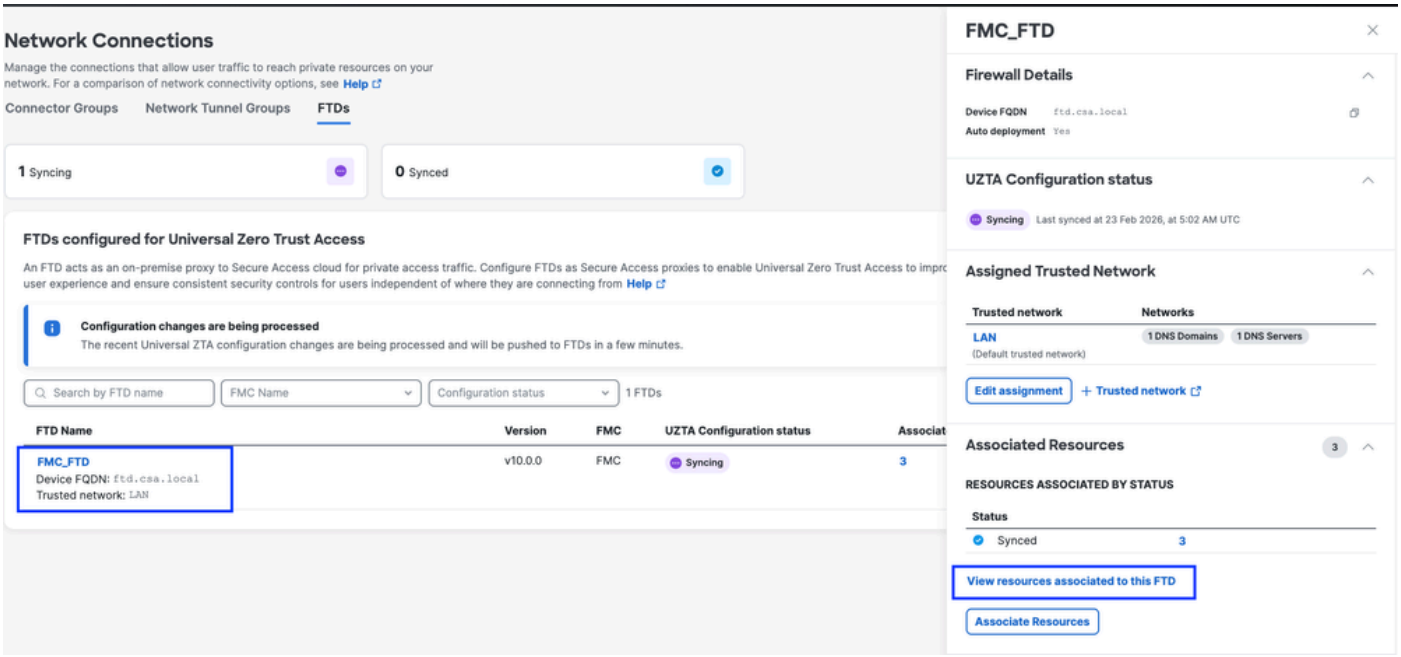


セキュアアクセス – PR検証

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
```

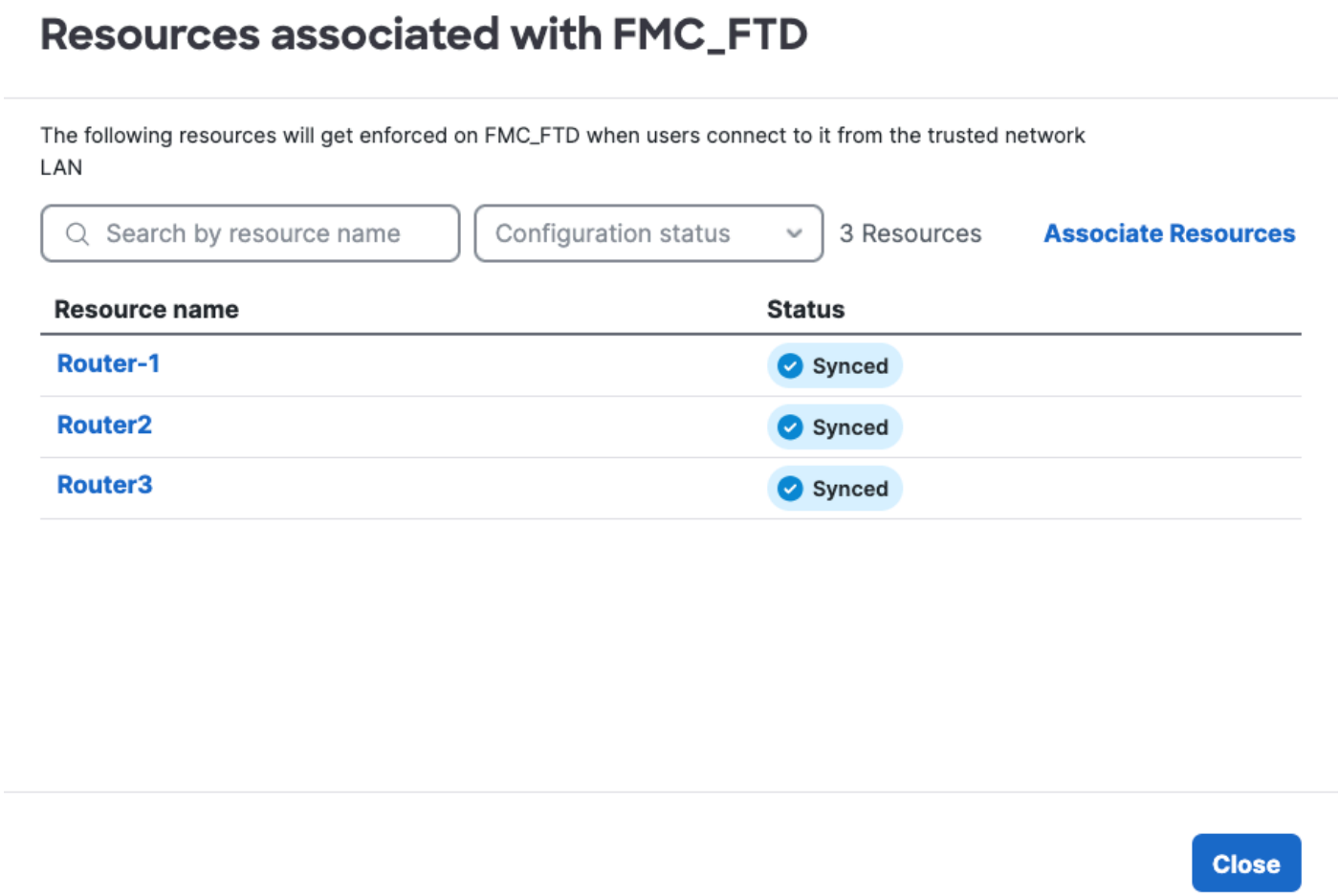
セキュアアクセス – PR検証



セキュアアクセス – PR検証

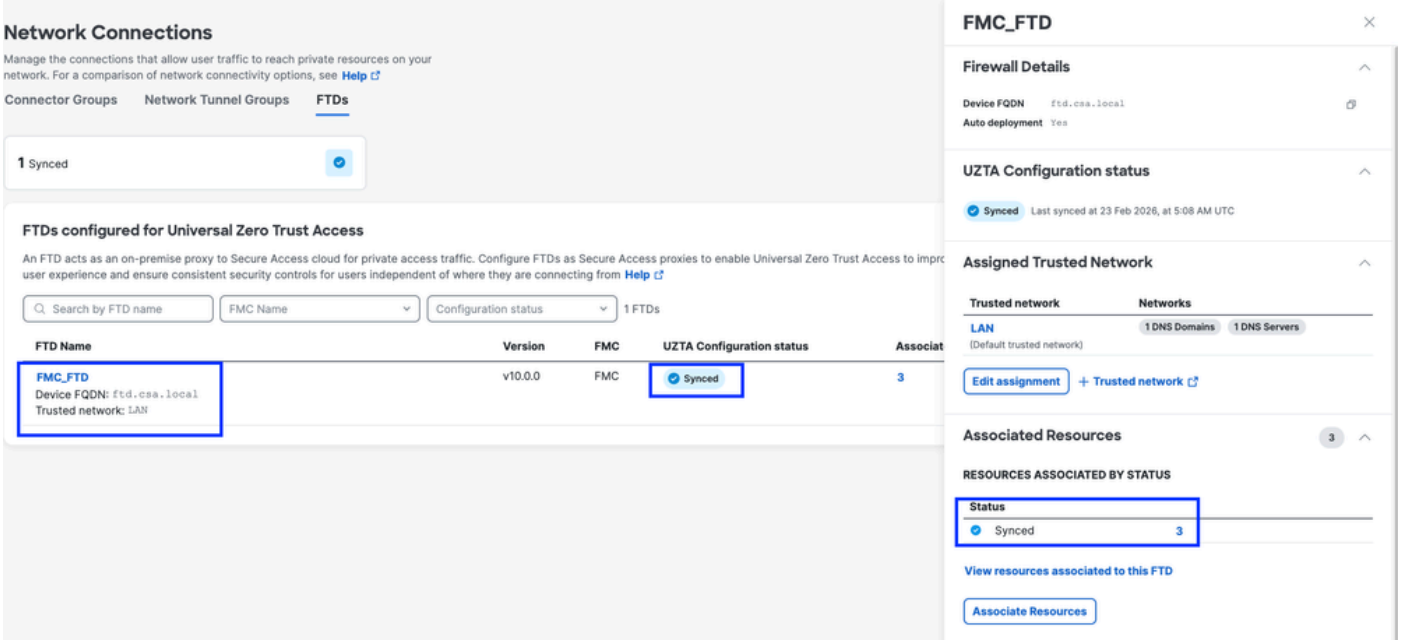
```
C:\Users\jay>ping ftd.csa.local

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



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



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。

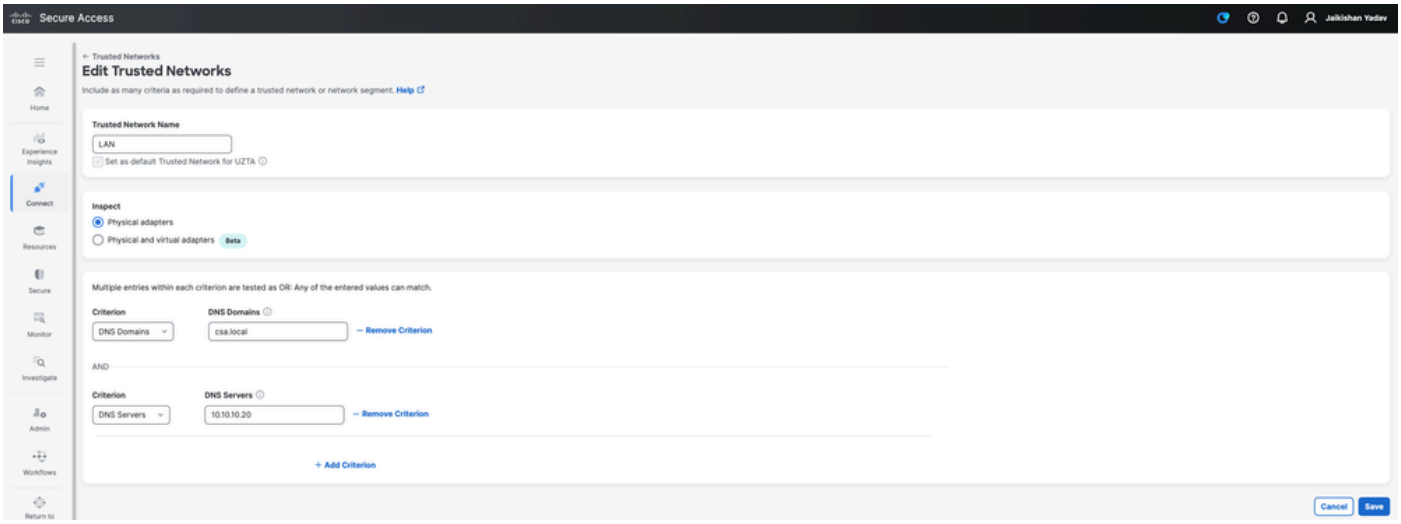
show running-config object application

```
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

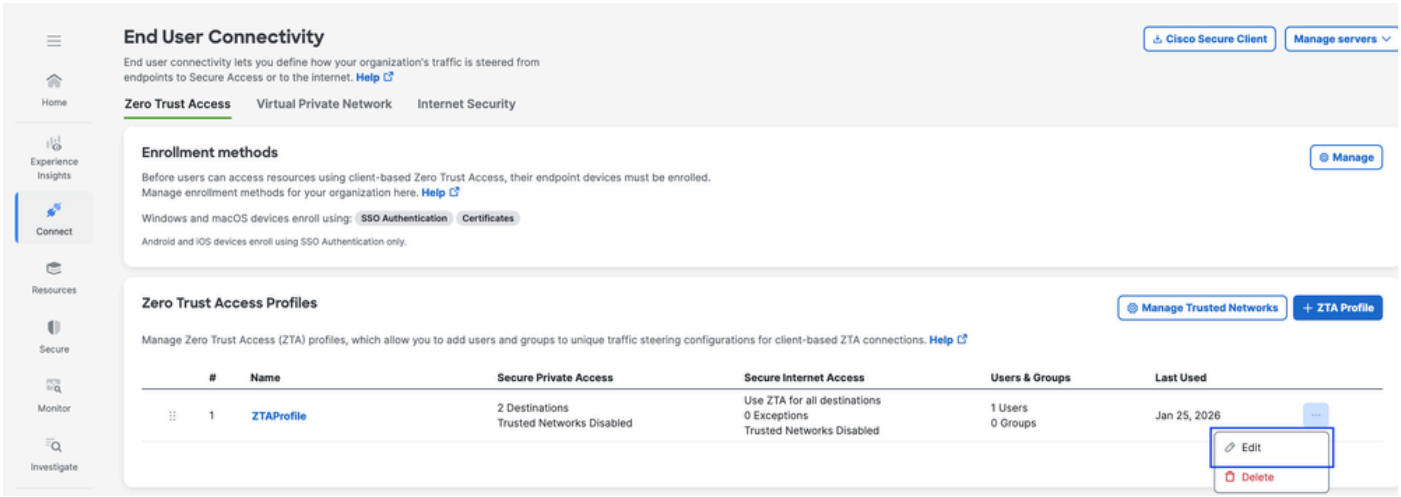
Connect > End User Connectivity > Zero Trust Access > ZTA Settingsの順に移動し、Trusted Networksを設定します。



セキュアアクセス：ZTA TNDの設定

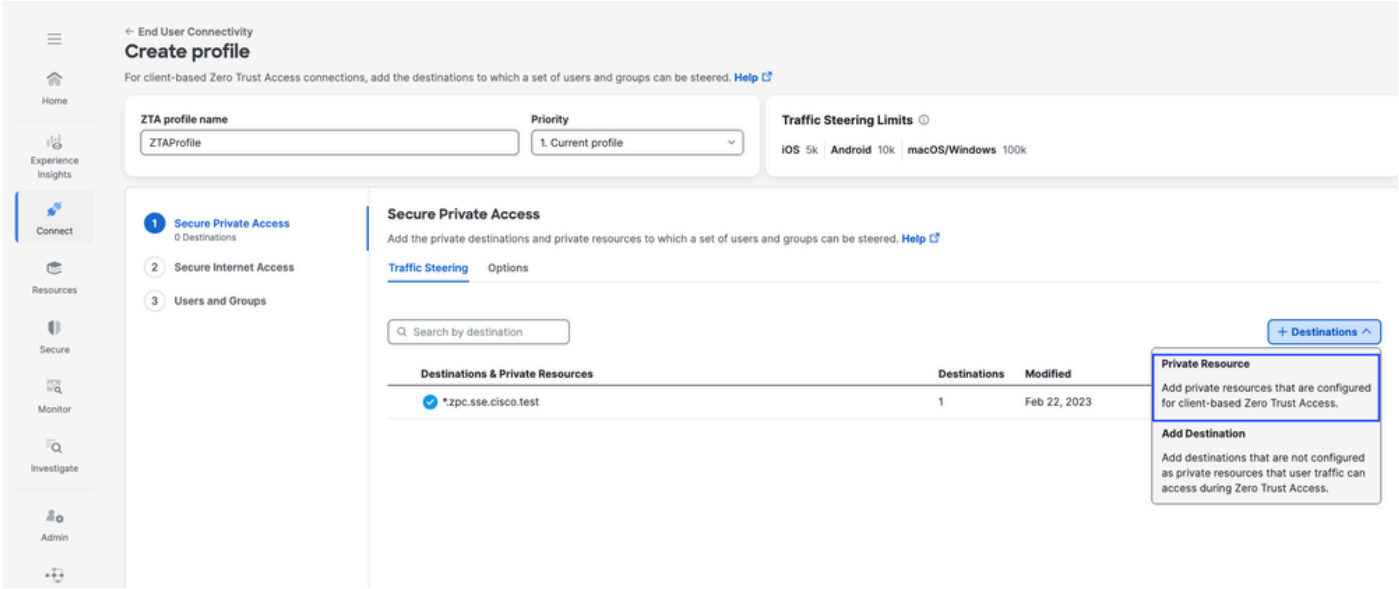
ステップ5 ZTAプロファイルへのプライベートリソースの追加

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

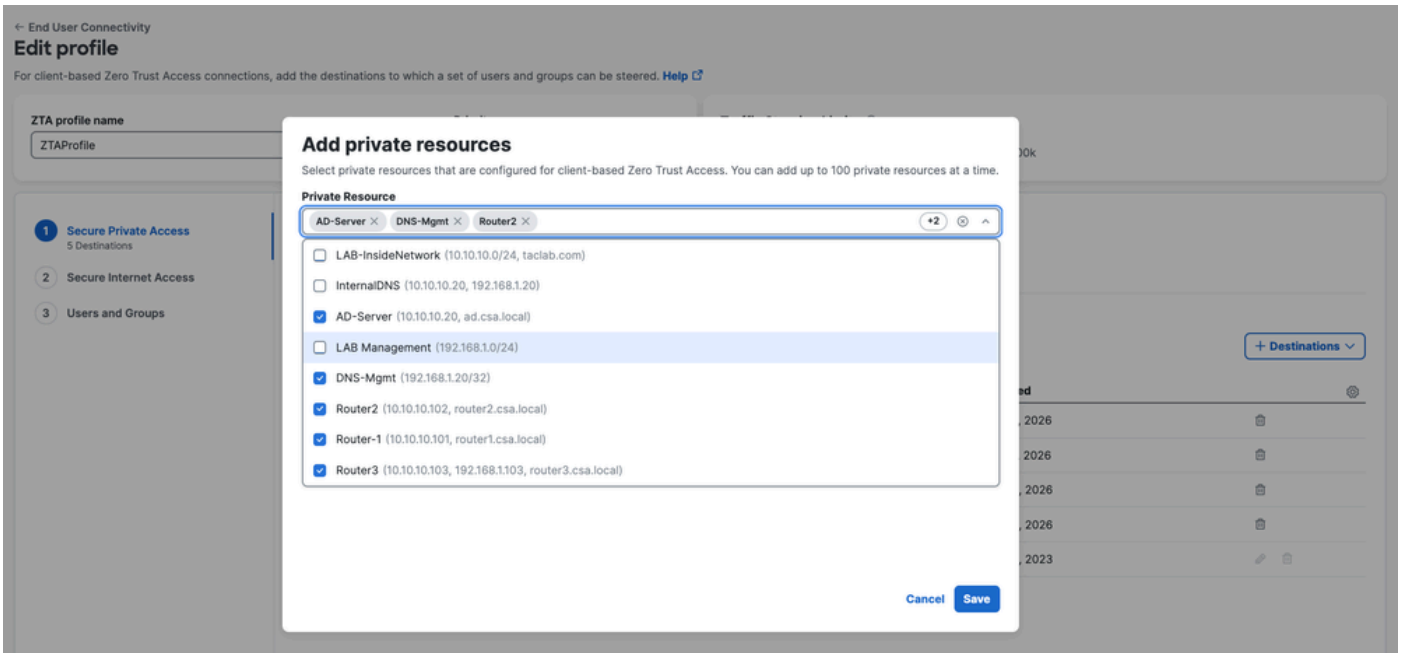


セキュアアクセス – ZTAプロファイル

2. プライベートリソースの追加

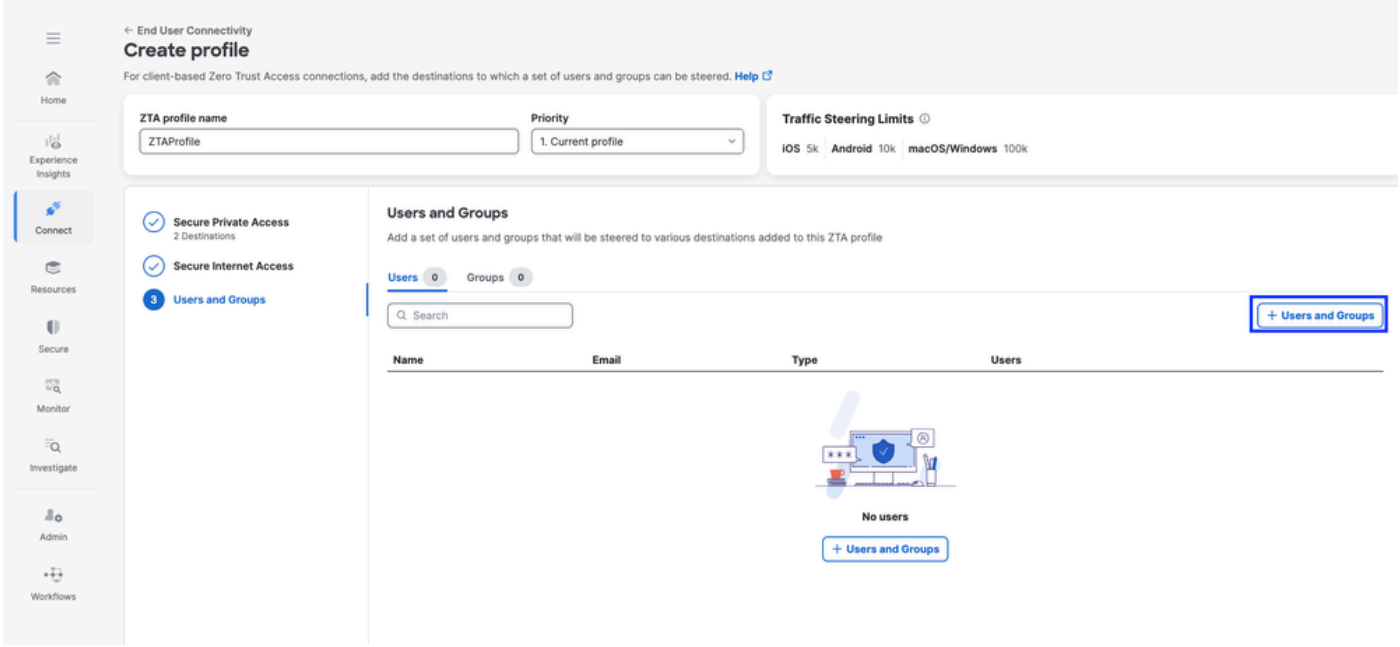


セキュアアクセス – ZTAプロファイル

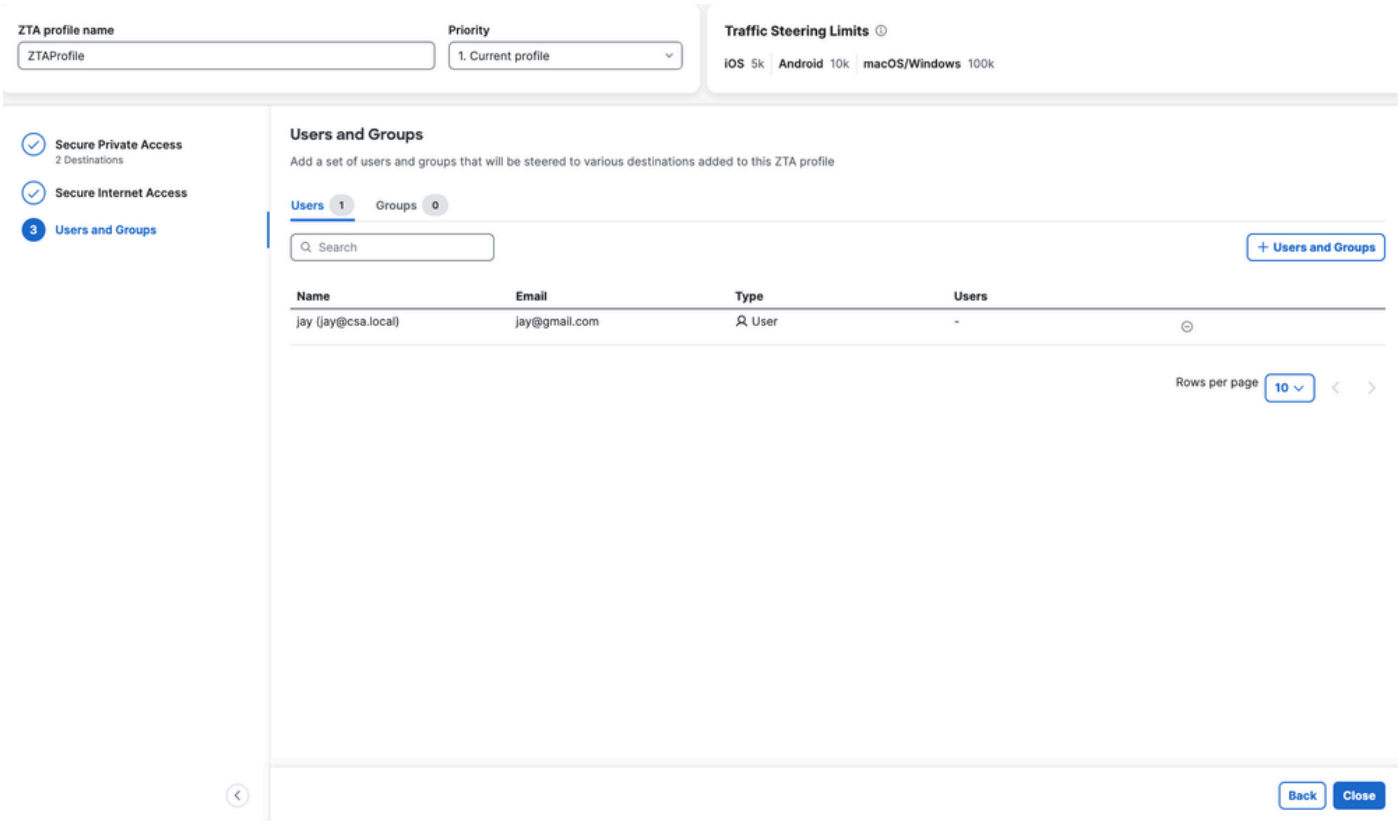


セキュアアクセス – ZTAプロファイル

3. ユーザーとグループの追加



セキュアアクセス – ZTAプロファイル

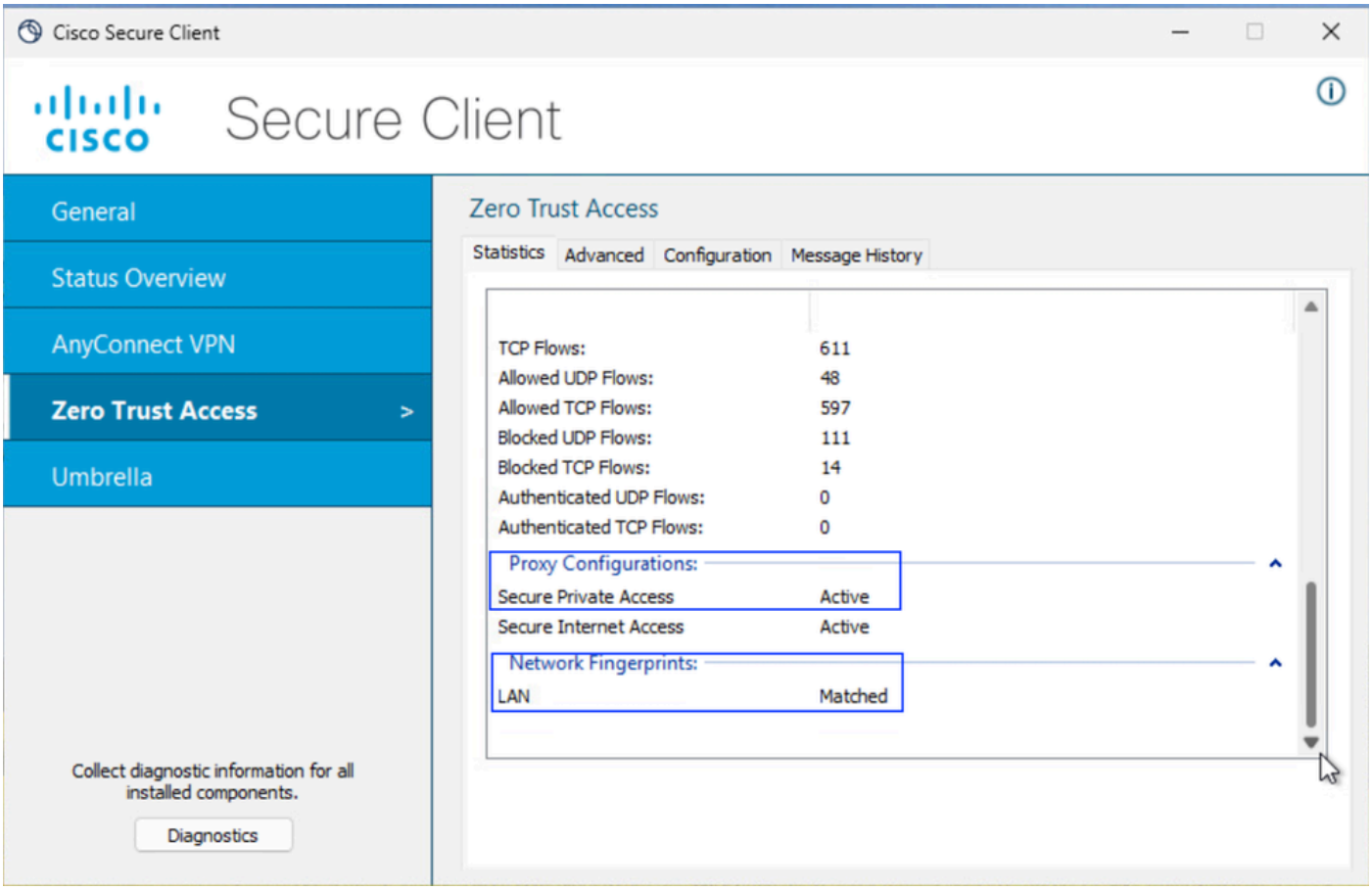


セキュアアクセス – ZTAプロファイル

手順6：プライベートリソースへのアクセスを確認する

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

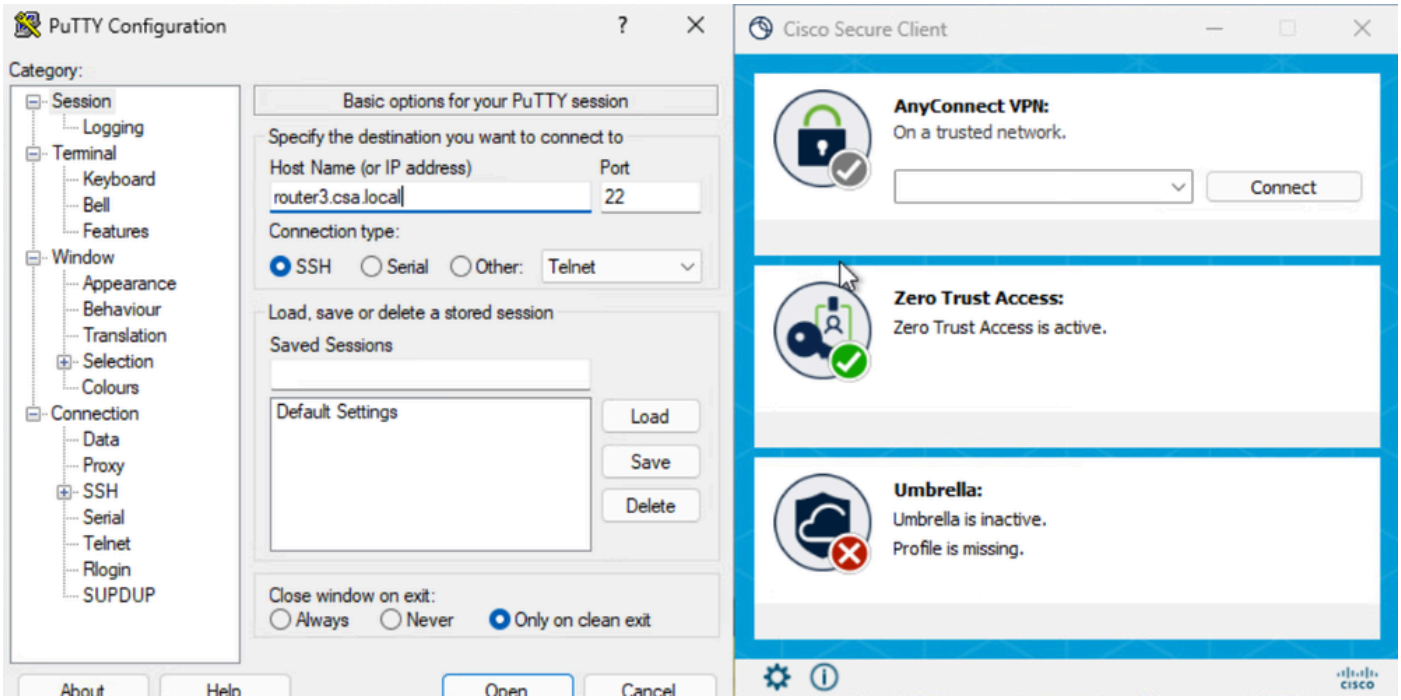
3. FTDがFQDNを使用してプライベートリソースに到達できることを確認します。

```
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#
```

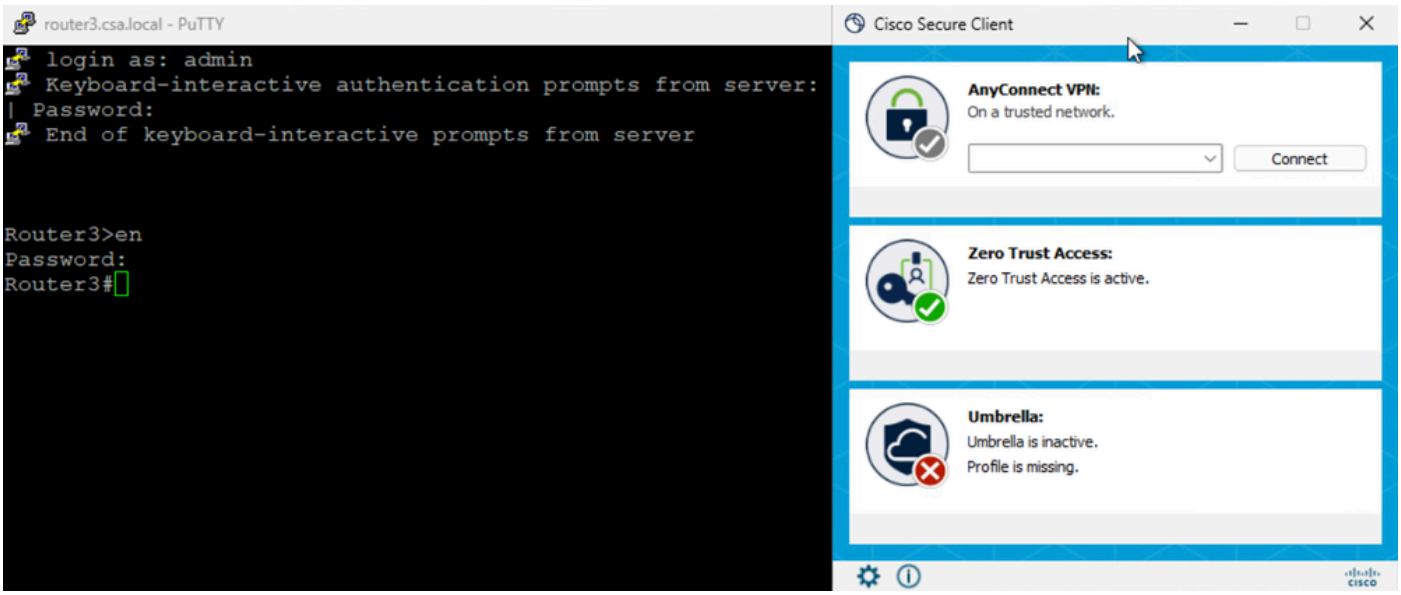
セキュアなアクセス – PRテスト

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

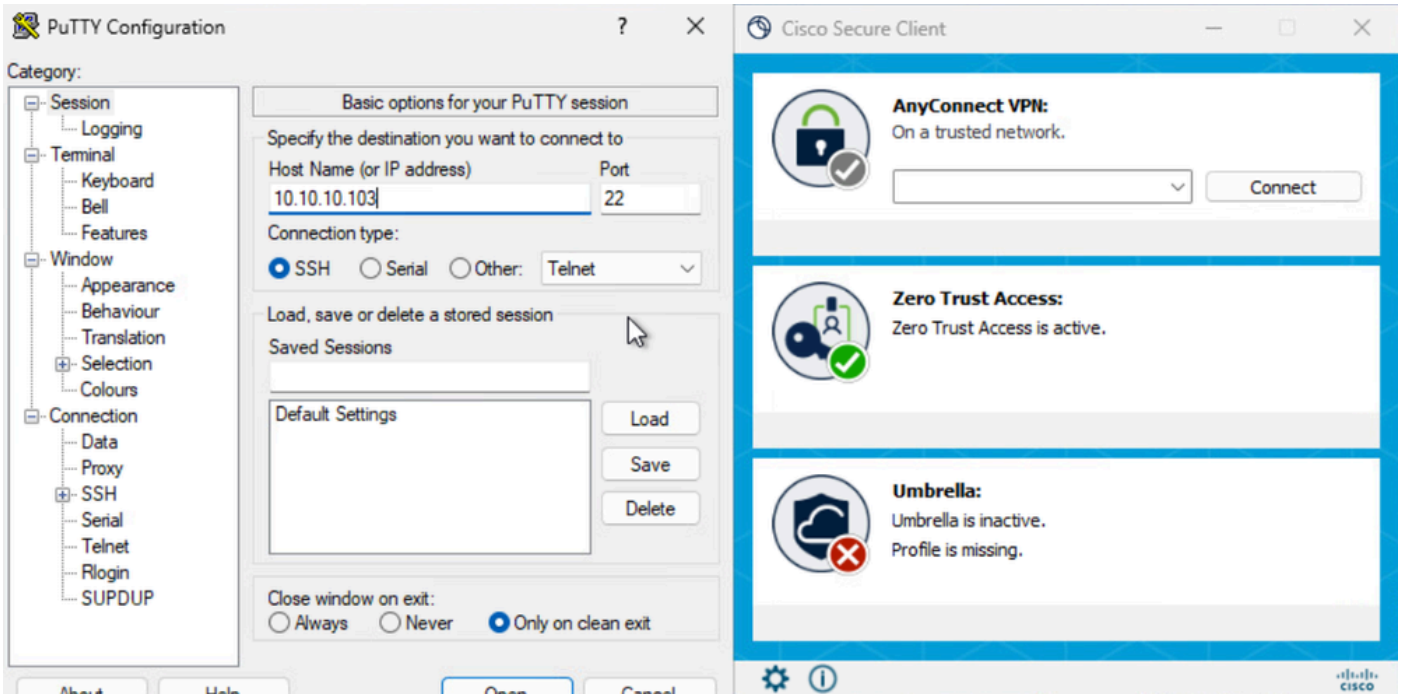


セキュアなアクセス – PRテスト

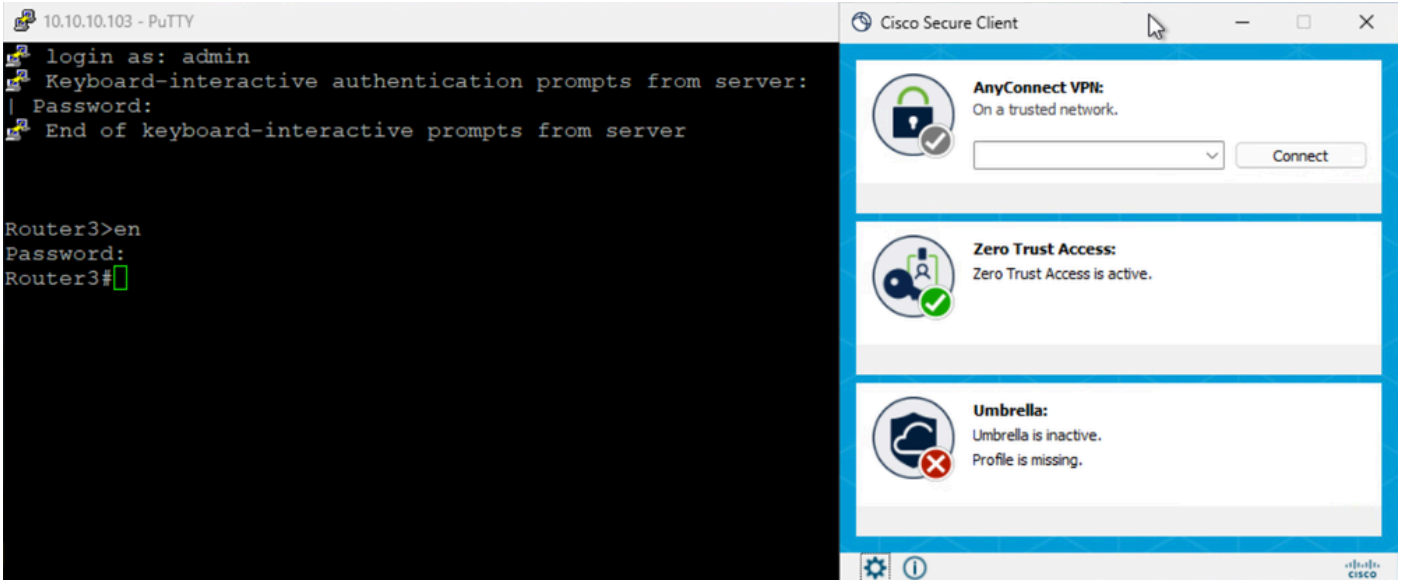


セキュアなアクセス – PRテスト

IPアドレスを使用してPRにアクセスします

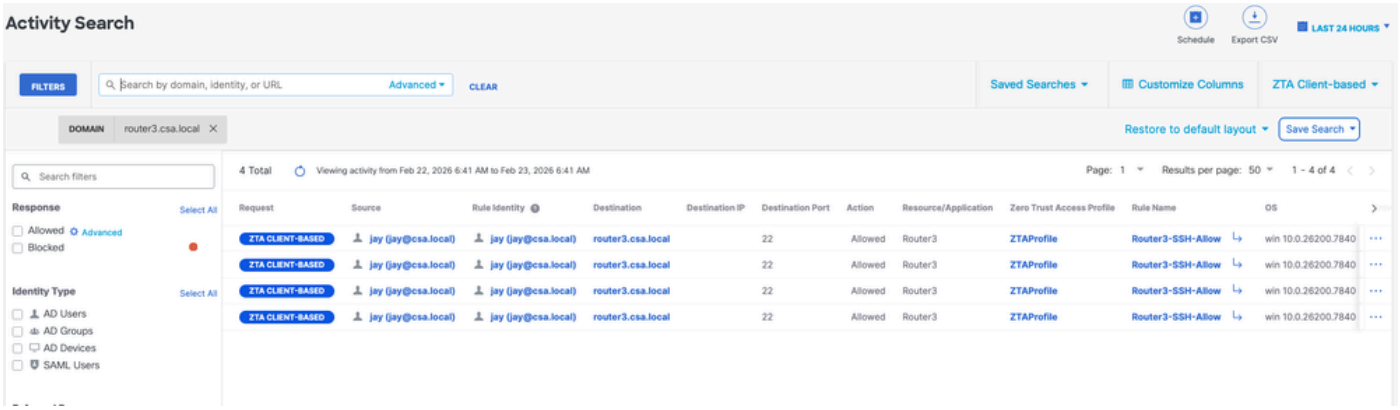


セキュアなアクセス – PRテスト

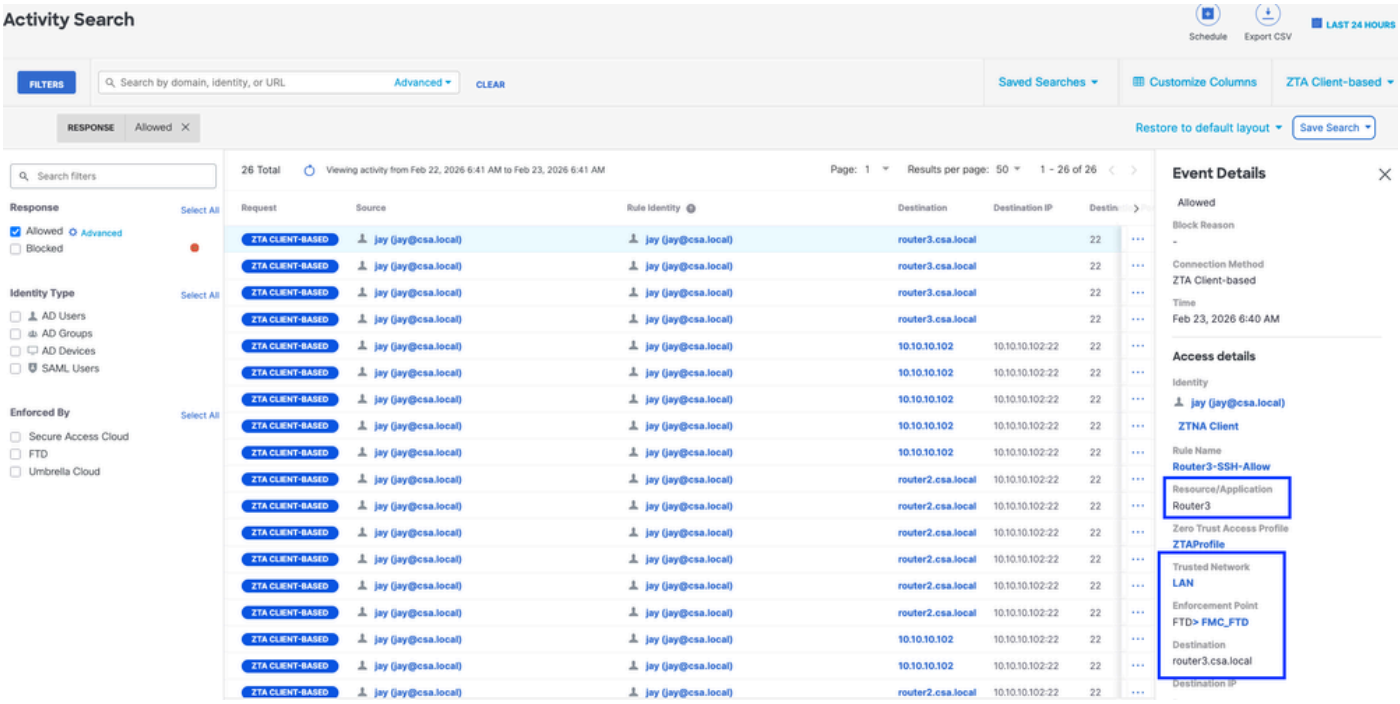


セキュアなアクセス – PRテスト

5. セキュアアクセスアクティビティの検索ログの確認

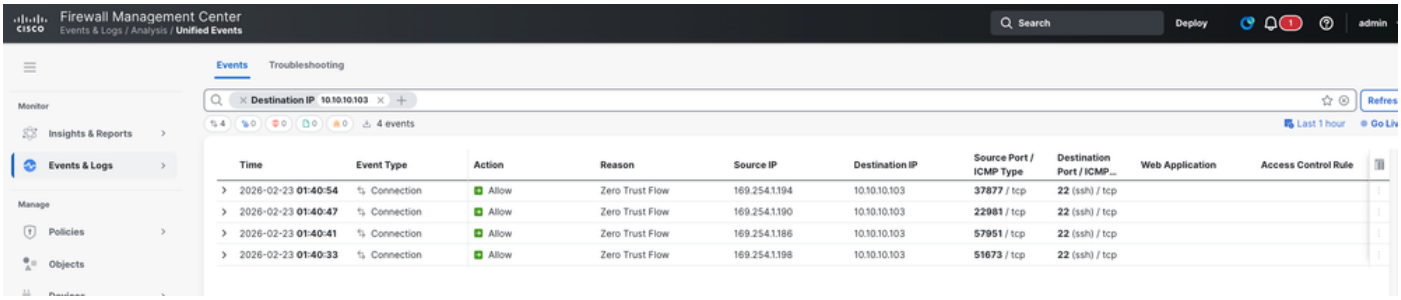


セキュアアクセス – アクティビティ検索



セキュアアクセス – アクティビティ検索

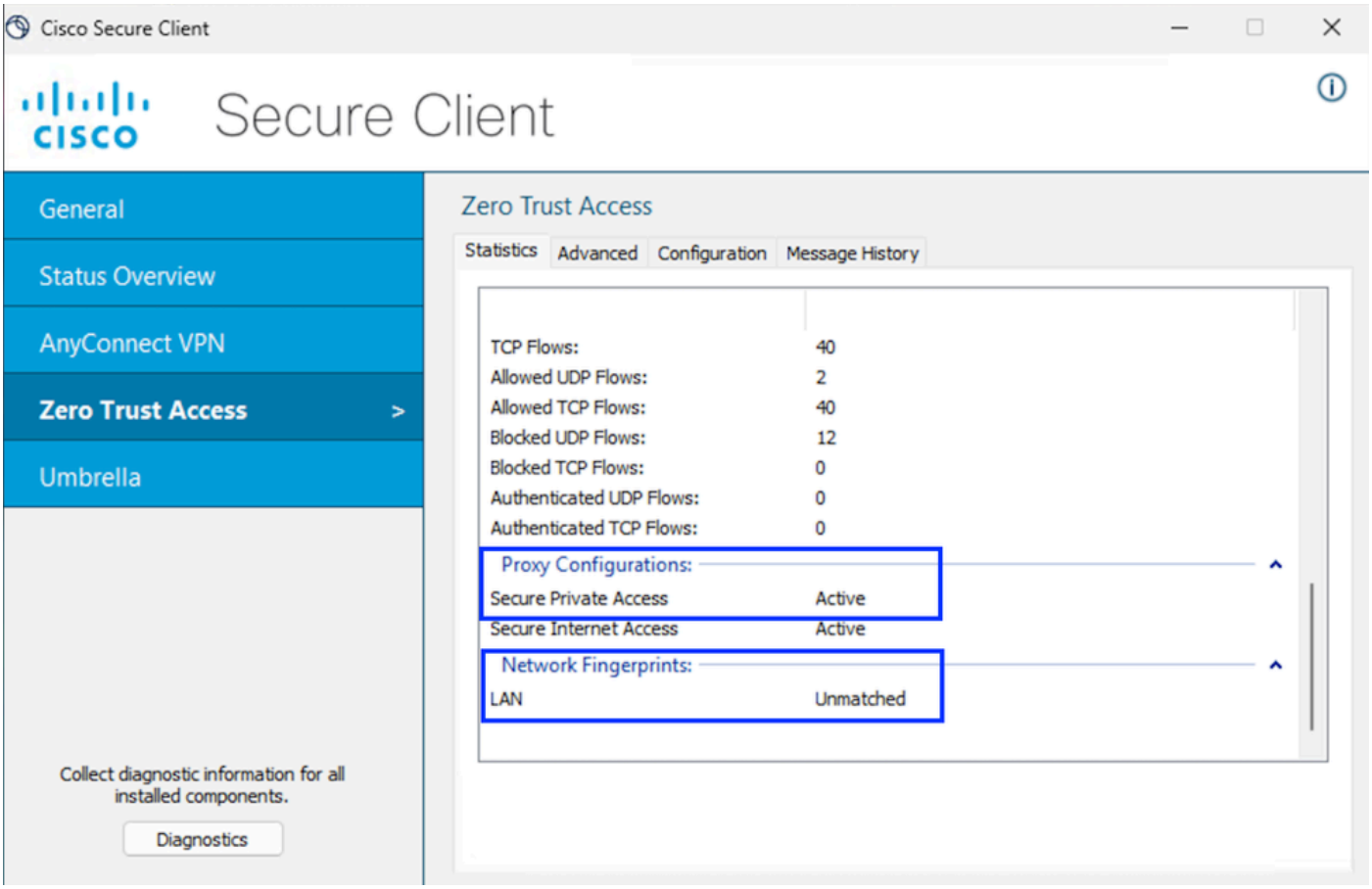
6. FMC接続イベントの確認



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は一致しません



セキュアなアクセス – PRテスト

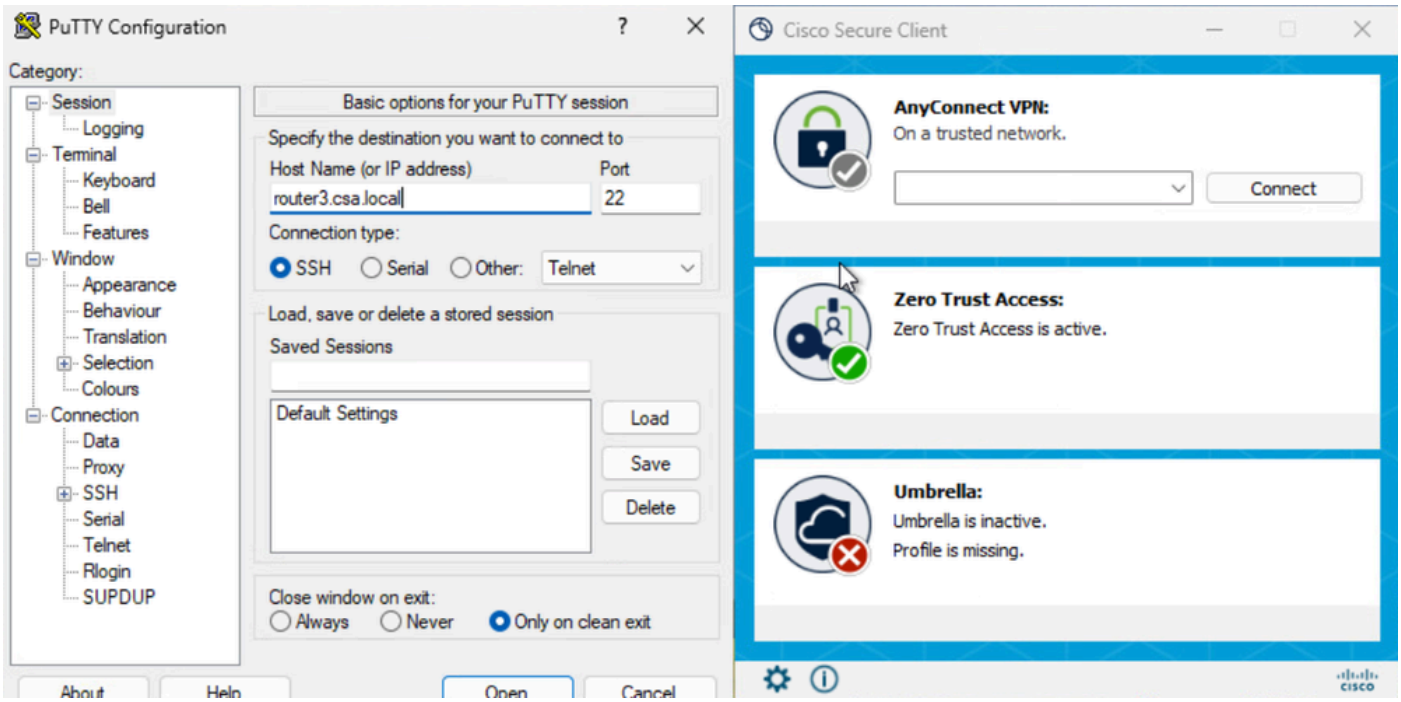
2. リモートユーザがFTD FQDNを解決できることを確認します

```
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
```

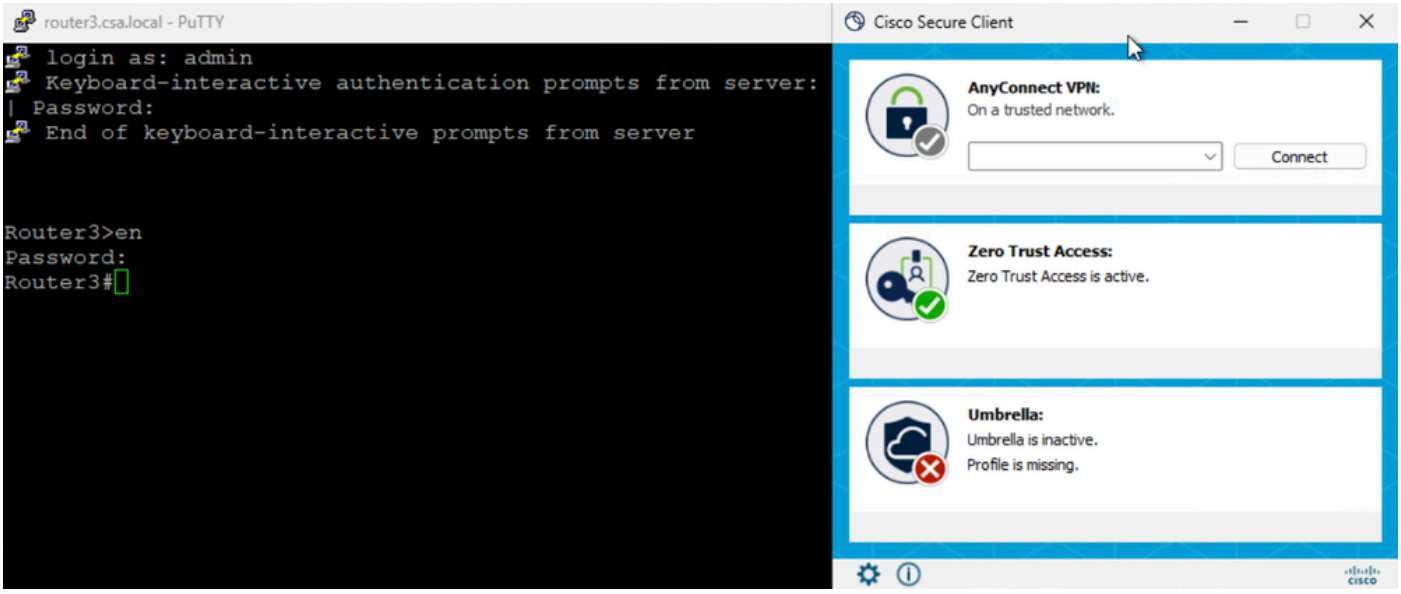
セキュアなアクセス – PRテスト

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

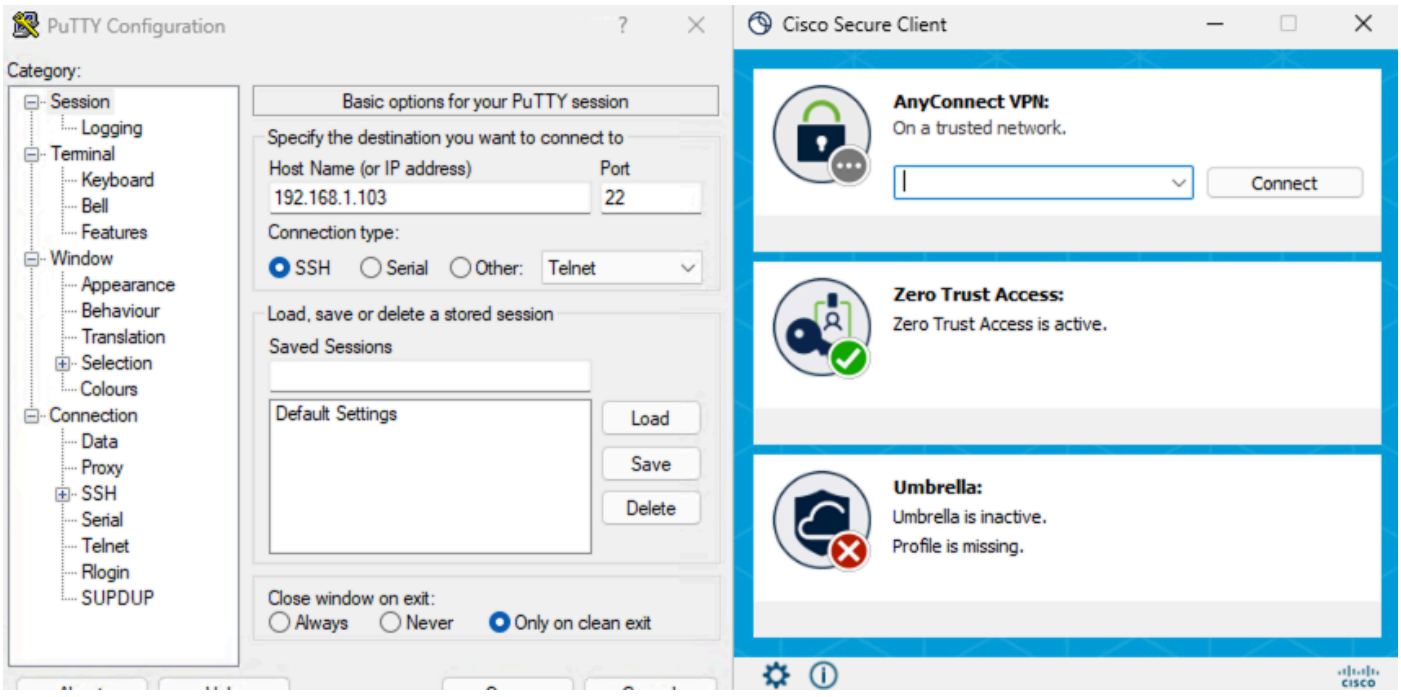


セキュアなアクセス – PRテスト

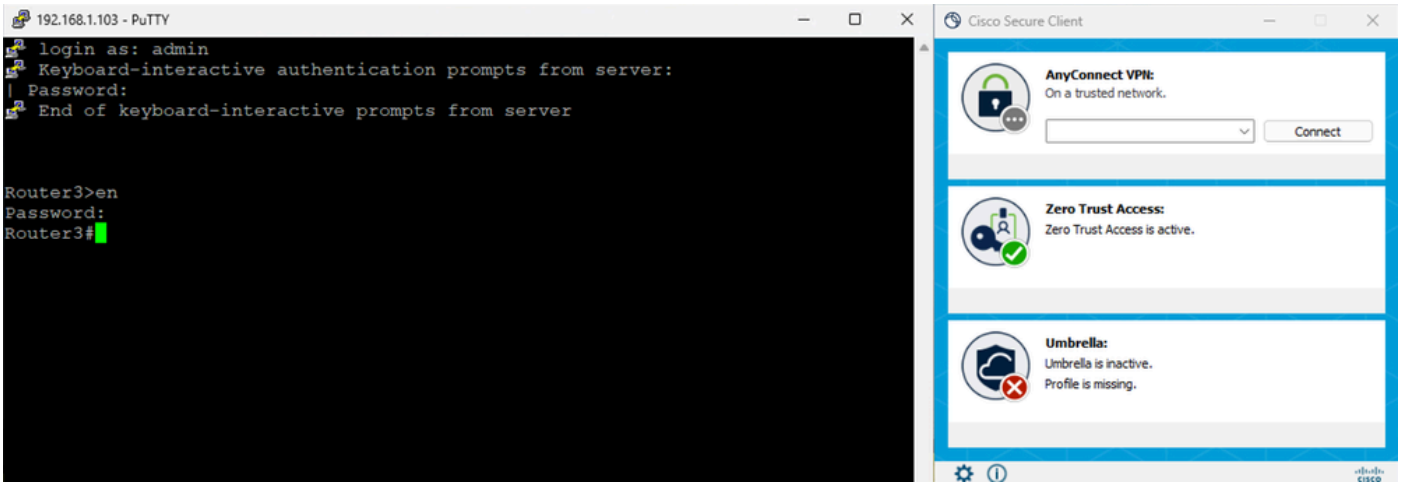


セキュアなアクセス – PRテスト

IPアドレスを使用してPRにアクセスします

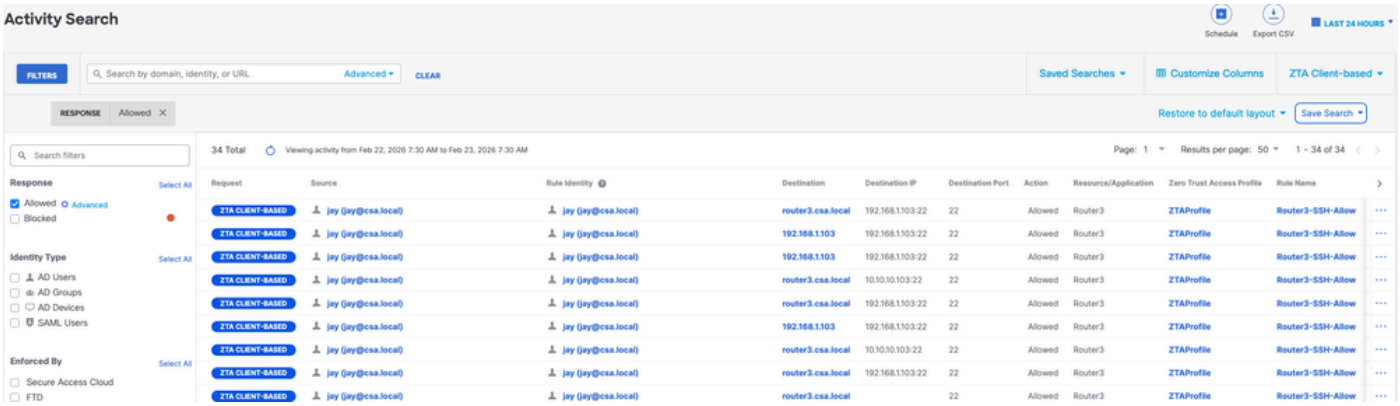


セキュアなアクセス – PRテスト

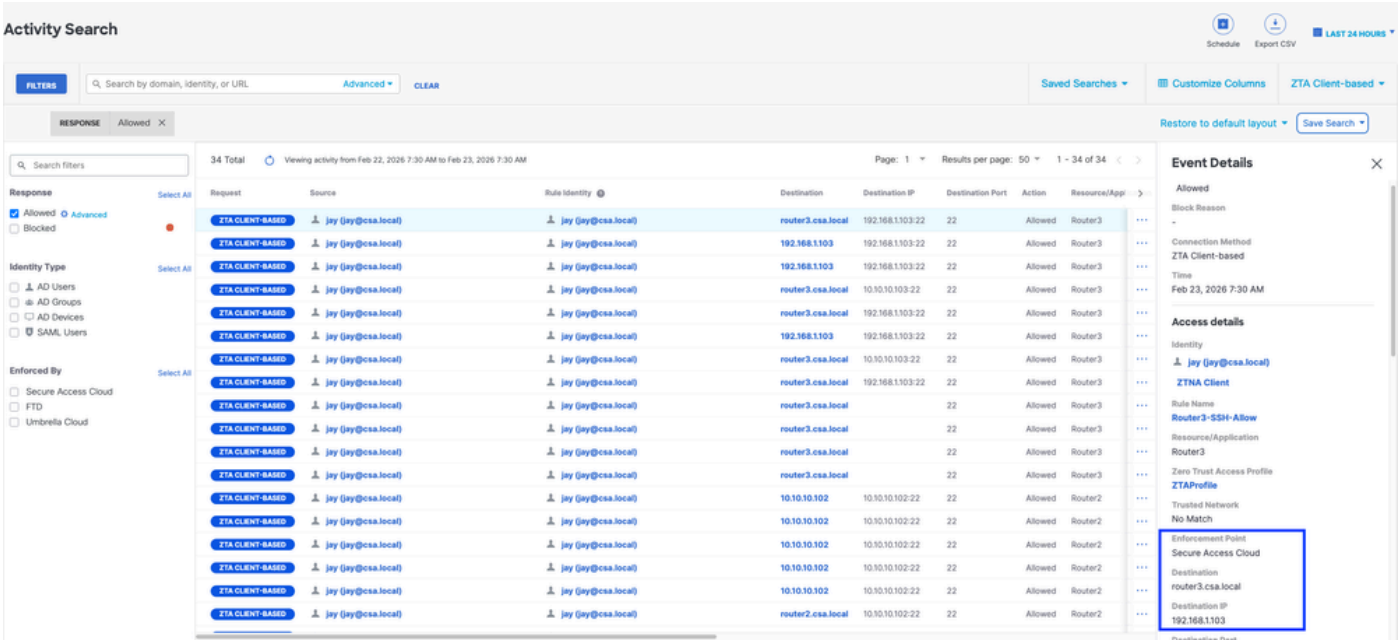


セキュアなアクセス – PRテスト

5. セキュアアクセスアクティビティの検索ログの確認



セキュアアクセス – アクティビティ検索



トラブルシュート

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。