تكوين ZTNA العالمية للوصول إلى الموارد الخاصة على الوصول الآمن

المحتويات

المقدمة

سنغطي في هذا المستند تكوين الوصول إلى الموارد الخاصة عبر ZTNA العالمية باستخدام مسارات حركة مرور مختلفة.

المتطلبات الأساسية

يجب إكمال التكوين التالي قبل تكوين ZTNA العام

- موفر الهوية على Cisco Secure Access
- تسجيل الأجهزة في الوصول بدون ثقة باستخدام الشهادات
- تكوين الأنفاق باستخدام جدار الحماية الآمن من Cisco

- شبكة الوصول عن بعد الخاصة الظاهرية
- موصل المواردعلى الوصول الآمن
- إدارة برنامج FTD على ميزة التحكم في سحابة الأمان
- يجب تمكين علامة ميزة ZTNA المختلطة لمستأجر الوصول الآمن الخاص، اتصل ب Cisco TAC لتمكين العلامة

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين IPsec VPN على Cisco وجدار الحماية من الآمن الوصول بالتهديد ضد الدفاع
- Identity Supply (IDp) - توفير المستخدم من Active Directory
- تكوين VPN عن بعد على Cisco Secure Access
- نشر موصل المواردعلى Cisco Secure Access
- التسجيل المستند إلى شهادة ZTA
- الشهادة - OpenSSL أو إنشاء CSR أو قوالب الشهادات وما إلى ذلك.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الدفاع الآمن ضد تهديد جدار الحماية من Cisco (الإصدار 7.7.10)
- مركز إدارة Cisco Secure Firepower (الإصدار 7.7.10)
- Cisco Secure Client (ZTA، الإصدار 5.1.10.1720)
- نظام التشغيل Windows 11
- Windows 2019 Server - المرجع المصدق
- موصل المواردعلى ESXi

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

حول ZTNA العالمية

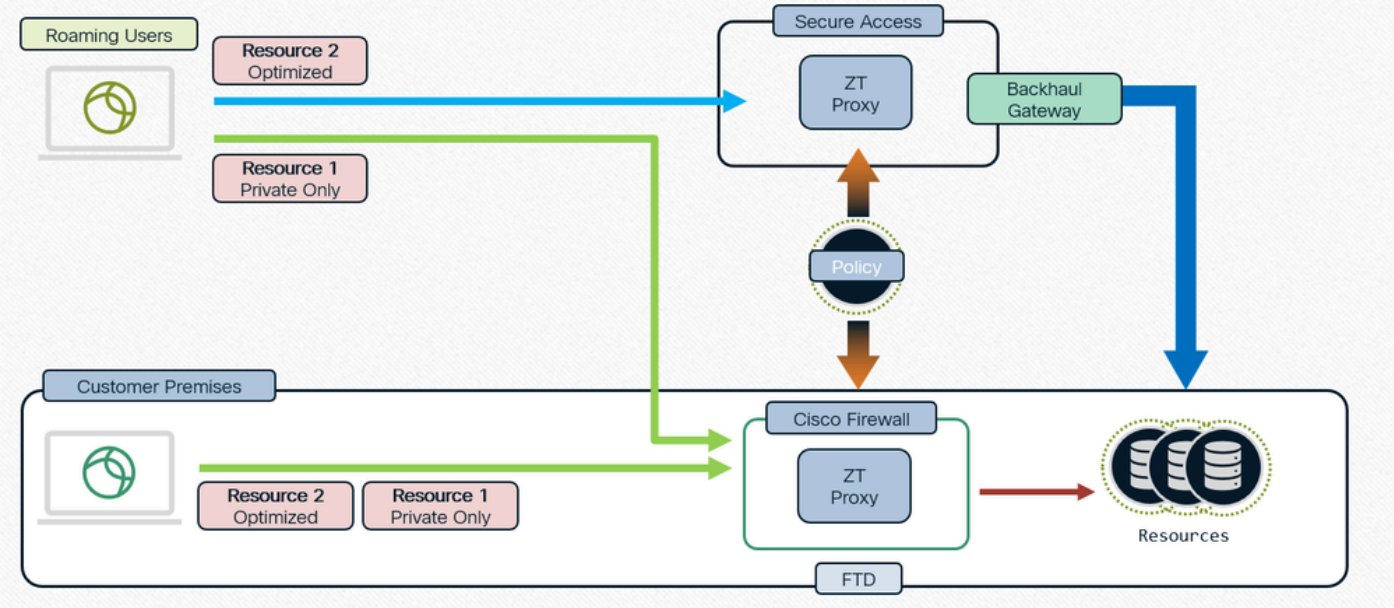
يتيح الوصول العالمي إلى الشبكة دون ثقة (uZTNA) للمستخدمين إمكانية السماح بشكل محدد بالوصول إلى موارد الشبكة الداخلية وفقا لهوية المستخدم (بما في ذلك ثقة المستخدم ووضعية المستخدم)، ودون منح حق الوصول إلى الشبكة بالكامل كما هو الحال مع

RA-VPN. كما تتيح uZTNA للمسؤولين إمكانية تأمين الموارد والتطبيقات الداخلية لكل من المستخدمين البعيدين والمقيمين.

نظرا لأن uZTNA لا يفترض أن الوصول الممنوح لأحد التطبيقات يخول ضمنيا الوصول إلى تطبيقات أخرى، يتم تقليل سطح هجوم الشبكة.

يقيم Secure Access سياسة الوصول. يتم تجاهل أي سياسات للتحكم في الوصول يتم نشرها على الأجهزة من مركز إدارة جدار الحماية الآمن.

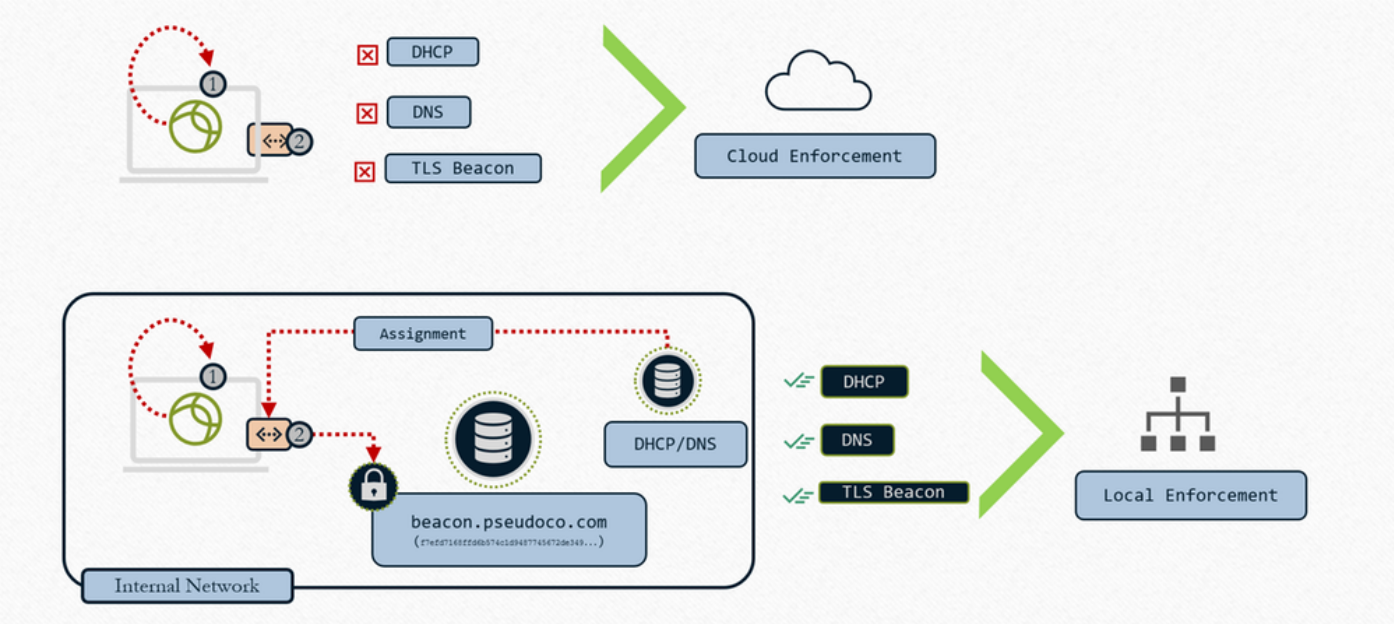
يتم إجراء وكيل حركة المرور، بالإضافة إلى فرض سياسة IPS والملفات والبرامج الضارة، على "الدفاع عن تهديد الطاقة النارية" (FTD).



سياسة واحدة، التطبيق الموزع

اكتشاف الشبكة

تحديد السحابة أو التطبيق المحلي



ZTNA العالمية - تحديد السحابة أو التنفيذ المحلي

1- يستجوب العميل الواجهة المحلية لتكوين الشبكة

2- عمليات بحث العميل عن منارة TLS

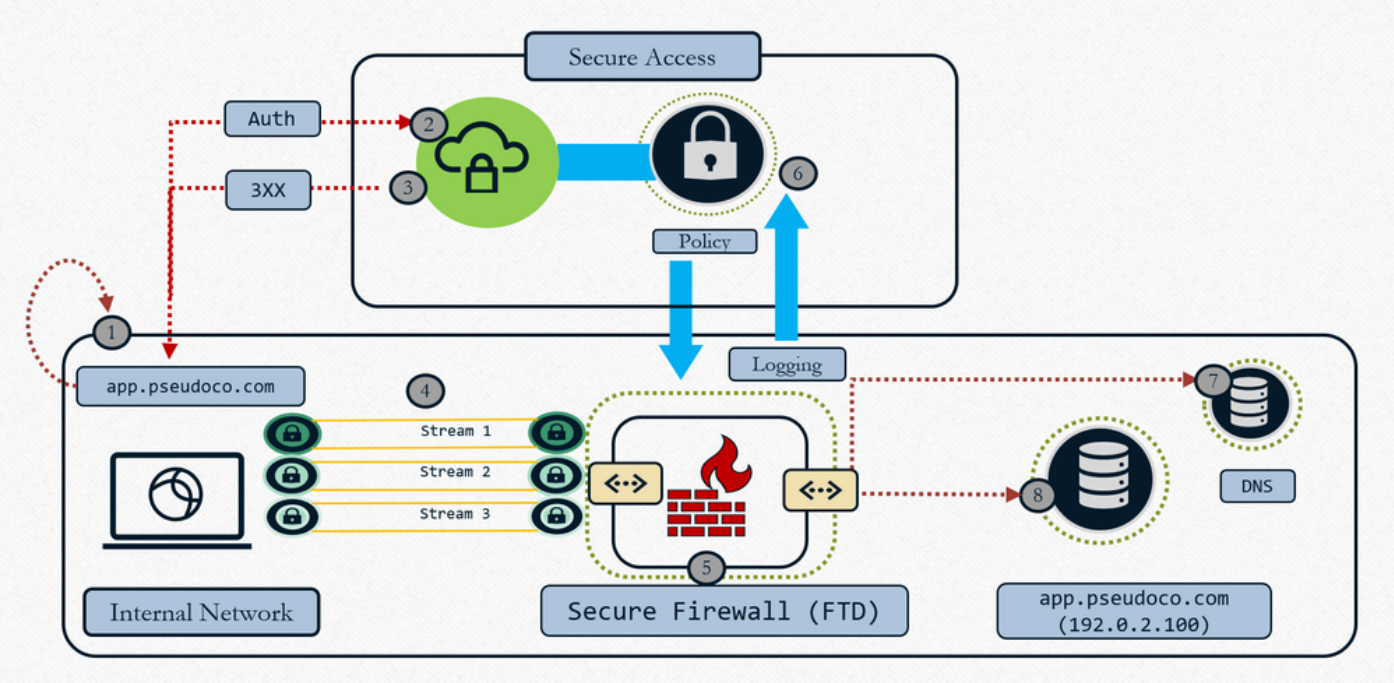
3- إذا تطابقت الظروف - الإنفاذ المحلي

4- في حالة عدم تطابق الحالة - تطبيق السحابة

عند تكوين المورد باستخدام "فرض السحابة أو المحلي" وربط قاعدة TND ب FTD، فإن ما يقوم به بالفعل هو مجموعة قواعد الاعتراض التي يتم إرسالها إلى العميل تتضمن تقييم قاعدة TND. عند قاعدة TND. لذلك، اذا العميل سوف يتم إخباره من قبل السحابة لتقييم قاعدة TND. عند إرسال الاتصال، نضع نتيجة تقييم بصمة الشبكة TND في رأس HTTP، بحيث تخبر الوكيل ما إذا كنا في حالة تشغيل أو على شبكة غير موثوق بها ثم يستخدم الوكيل تلك المعلومات ويعيد توجيه حركة مرور البيانات وفقا لذلك. في حالة تطابقات بصمات الأصابع، يطلب Zproxy من العميل إعادة توجيه حركة مرور البيانات إلى FTD وإذا لم تتطابق بصمات الأصابع فإنه يعيد توجيه حركة مرور البيانات إلى السحابة. راجع تكوين الوصول إلى الشبكة الموثوق بها دون ثقة مع اكتشاف الشبكة

أنواع التنفيذ

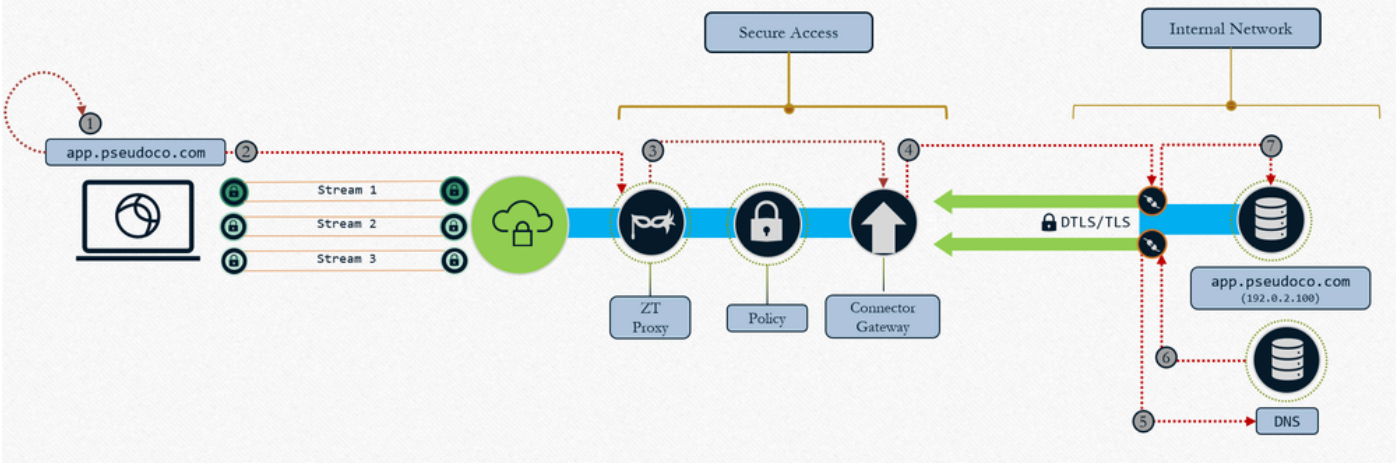
- مسار الإنفاذ المحلي: تنفيذ الجدار الناري



ZTNA العالمية - الإنفاذ المحلي

1. طلب المستخدم، يلتقط العميل ويفصل الطلب إلى IP المؤقت (نطاق المضيف المحلي)
2. يتم إرسال حركة مرور التحكم في المصادقة إلى سحابة الوصول الآمن لتقييم السياسة
3. مرتجعات السحابة يتم إعادة توجيهها إلى FTD لتطبيق خطة البيانات (إذا سمحت السياسة)
4. تم توجيه حركة المرور إلى وحدة الاستقبال والبث التي تم تكوينها لجدار الحماية (الواجهة)
5. يتم فرض النهج المعرف في السحابة (IPS، والبرامج الضارة، وفك التشفير) باستخدام مستوى بيانات الوكيل المحلي
6. تم شحن الحدث المسجل والمكرر إلى مجموعة النظراء لإعداد تقارير متسقة
7. يقوم جدار الحماية بحل DNS على الشبكة المحلية لتوجيه حركة مرور المواراد (إذا كان مسموحا)
8. يبني جدار الحماية الاتصال بالمورد (اتصال جديد تم إنشاؤه للمورد) حيث يتصرف جدار الحماية كوكيل لبروتوكول TCP

- مسار تنفيذ السحابة : الشبكة غير المتصلة

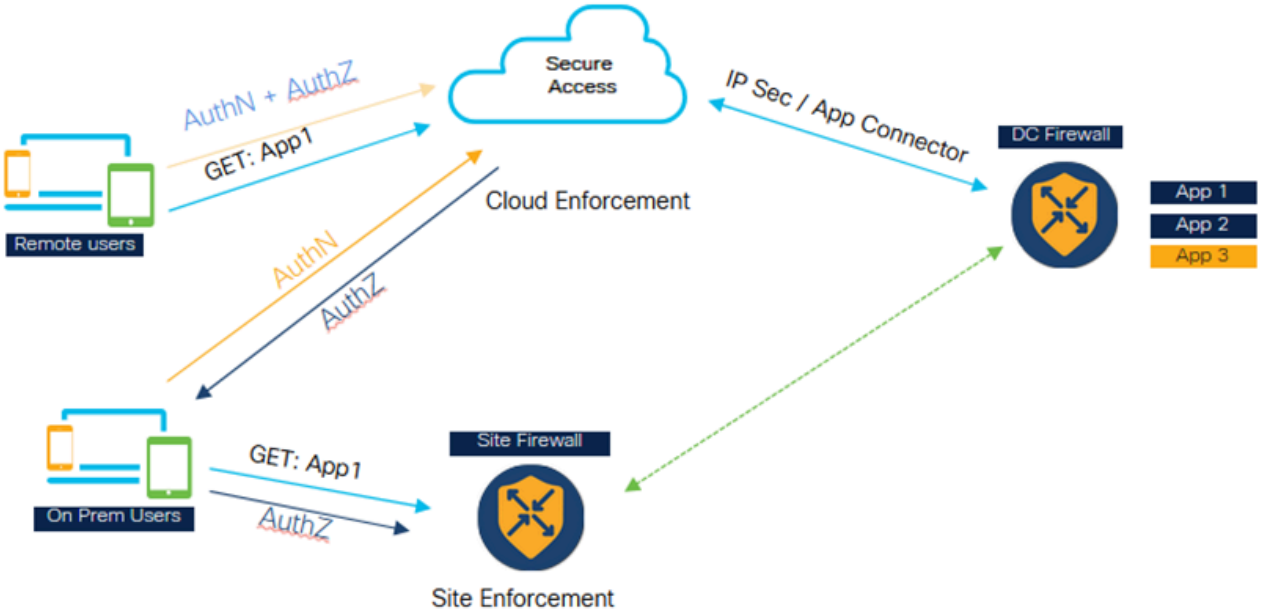


تقنية ZTNA العامة : تنفيذ السحابة

1. طلب المستخدم، يلتقط العميل ويفصل الطلب إلى IP المؤقت (نطاق المضيف المحلي)
2. يتم نقل حركة المرور إلى وكيل انعدام الثقة في الوصول الآمن
3. تم وكيل اتصال TCP وتم إنشاؤه إلى موصل المواراد الذي تم تعيينه، ويتم فرض النهج على حركة المرور
4. تحدد البوابة الاتصال بموصل المواراد
5. يقوم موصل المواراد بتحديد IP للمورد
6. تستجيب DNS المحلية باستخدام IP للمورد
7. يقوم موصل المورد بإنشاء اتصال بالمورد

حالات الاستخدام

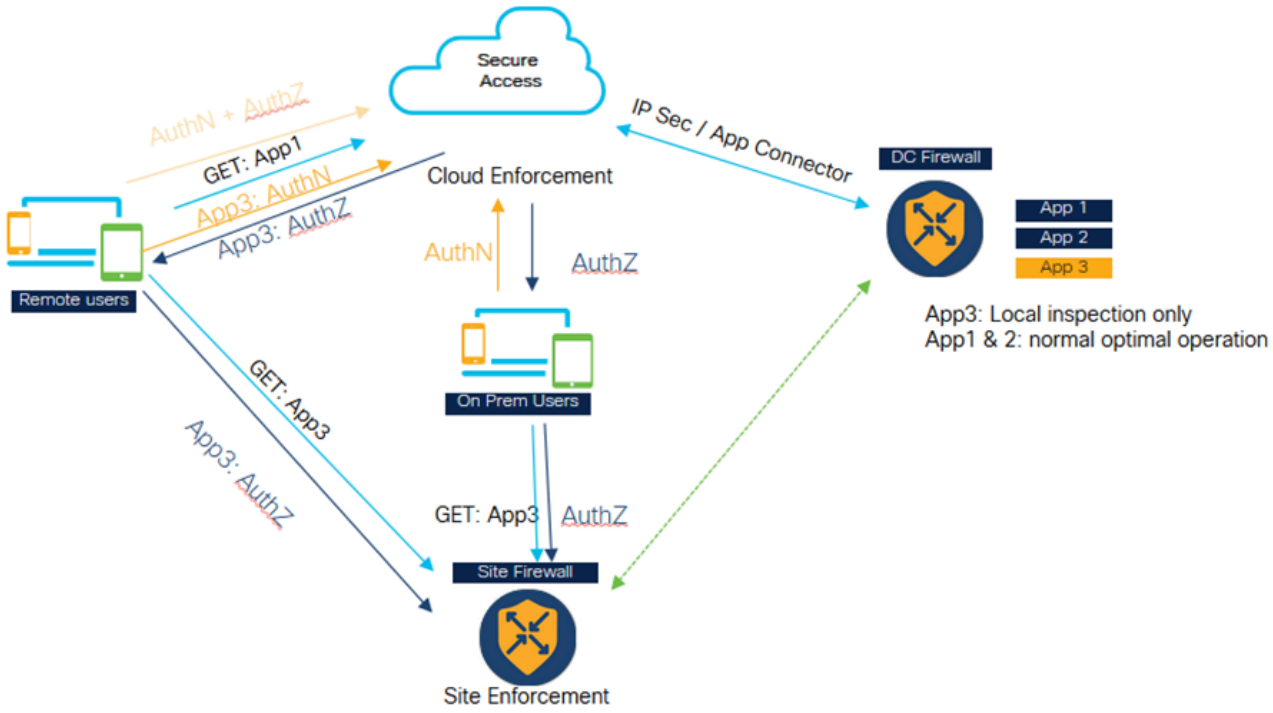
الحالة 1: ZTNA المتناسقة والمحسنة للمستخدمين عند التشغيل



ZTNA العالمية - ZTNA متناسقة ومحسنة (مستخدم محلي)

- تم تكوين كل من الوصول الآمن وجدار الحماية لحماية التطبيق.
- إذا كان المستخدم بعيد، فسيذهب إلى "الوصول الآمن" لتقييم النهج وفحصه.
- إذا كان المستخدم داخلي/داخلي، فسيتم الانتقال إلى جدار الحماية للتفتيش على حركة المرور الخاصة.
- لا يزال بإمكان المستخدم في الموقع الانتقال إلى الأمان للمصادقة والتقييم حيث تنتقل حركة مرور بيانات البيانات إلى جدار الحماية ويتم فحصها وفقا لتكوين النهج.
- يتمتع المستخدم الداخلي الذي يصل إلى التطبيق من خلال جدار الحماية بميزة الأداء حيث يعمل على تجنب حركة المرور التي تنتقل إلى السحابة ثم النقل إلى مركز البيانات من الخلف

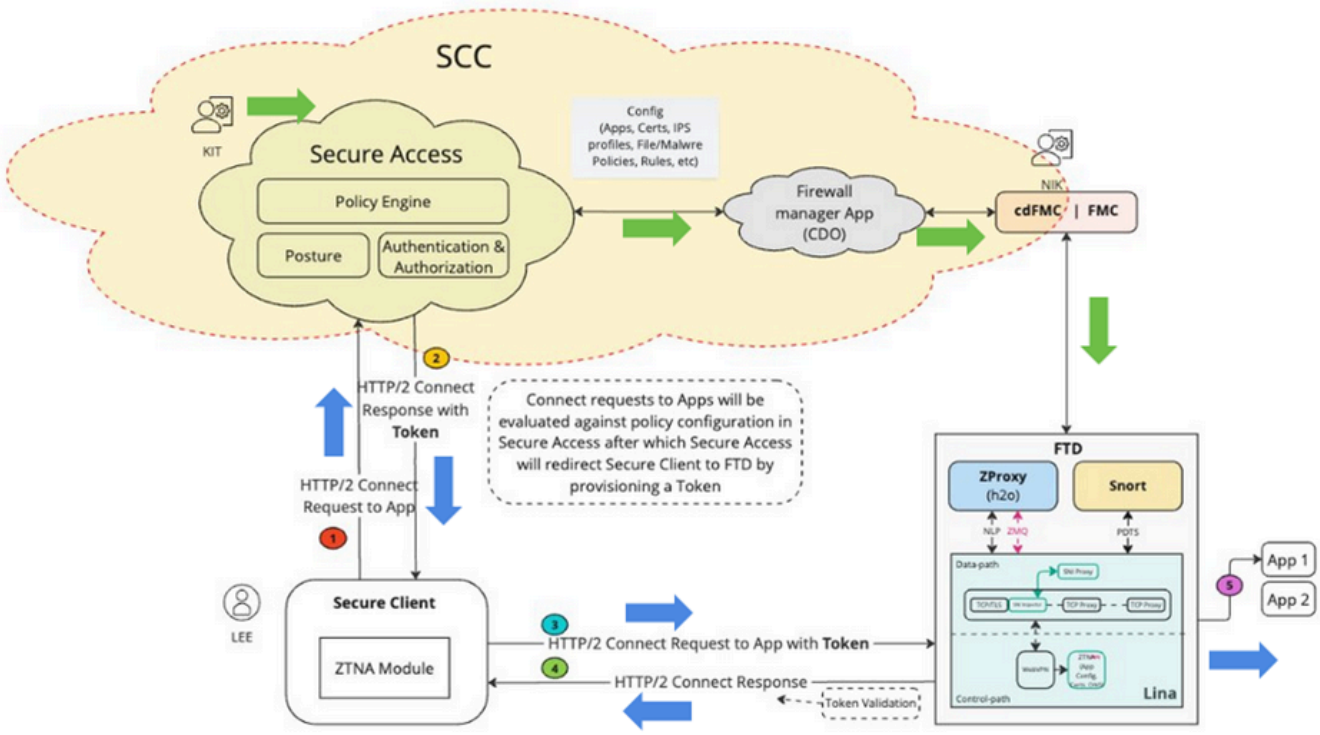
القضية 2: التفتيش الخاص على التطبيقات الحساسة



ZTNA العالمية - الفحص الخاص للتطبيقات الحساسة

- يمكن تكوين بعض التطبيقات الهامة بحيث يمكن الوصول إليها دائما من خلال جدار الحماية.
- لا تحتاج حركة مرور بيانات التطبيق إلى الانتقال إلى السحابة. على سبيل المثال، قد يكون هناك تطبيق بيانات حساس مثل التعليمات البرمجية المصدر، والذي يرغب العميل في الانتقال إلى مجموعة النظراء.
- في مثل هذه السيناريوهات، تمر حركة مرور المستخدم البعيد والمباشر دائما عبر جدار الحماية ويتم فحصها. ومع ذلك، مرة أخرى، في هذا السيناريو، تحدث المصادقة وتقييم السياسة دائما في السحابة، ويمر حركة مرور جزء البيانات فقط عبر جدار الحماية.

مكونات معمارية



ZTA العالمي - المكونات المعمارية

Security Cloud Control (SCC) وه المدير الأساسي لحل uZTNA. uZTNA هي المميزة الأولى التي يتم إنشاؤها فوق SCC.

في SCC ، لدينا إثنان من التطبيقات الدقيقة الوصول الآمن وجدار الحماية. بمجرد توفير SCC وتمكين علامات المميزة المطلوبة، سنتمكن من رؤية هذه التطبيقات الدقيقة على الجانب الأيسر من لوحة SCC.

العميل الآمن: في "العميل الآمن"، سيتعين علينا تمكين وحدة الوصول إلى Zero Trust (ZTNA) التي لا تخضع لأي ثقة (ZTNA)، حيث نحتاج إلى التسجيل في وحدة ZTNA لتكون قادرة على الوصول إلى التطبيقات.

الدفاع ضد تهديد الجدار الناري : يحمي FTD هذه التطبيقات. يقوم FTD بتشغيل وكيل ZT المعروف أيضا باسم H2O (مثل تشغيل الوكيل في Secure Access Cloud)

الآن عندما يقوم المستخدم (مثل KIT) بتكوين مورد خاص وسياسة حول تطبيق Secure Access micro، سيتم دفع هذا التكوين إلى التطبيق الصغير لجدار الحماية في SCC. يفهم تطبيق جدار الحماية العناصر الداخلية لتكوين FTD و FTD، وكيفية نشر التكوين وإدارته على FTD. لذلك، يتحقق تطبيق جدار الحماية من هذا التكوين، ويقوم باستدعاء واجهات برمجة تطبيقات FMC لدفع التكوين إلى FMC ثم نشره في نهاية المطاف على FTD. يمكن أن يحتوي FTD على خيار النشر التلقائي الذي تم تمكينه بحيث لا يضطر المسؤولون (مثل نيك) للقيام بالنشر اليدوي.

1. عندما يحاول مستخدم (مثل لي) الوصول إلى تطبيق، يتصل العميل الآمن ب Secure Access باستخدام قناة mTLS. يصادق Secure Access المستخدم باستخدام شهادة جهاز العميل. ومن ثم فإنه يقيم التخويل والوضعية والسياسات الأخرى التي تم تكوينها لذلك المستخدم ولذلك التطبيق.

2. Secure Access ، إذا تبين له أخيرا أن التطبيق محمي بواسطة جدار الحماية، فإنه يقوم بإنشاء رمز مصادقة مميز، والذي يخبر جدار الحماية بأن هذا تم مصادقته بالفعل ومرخص له. يتم تشفير رمز المصادقة المميز، وموقع بواسطة Secure Access

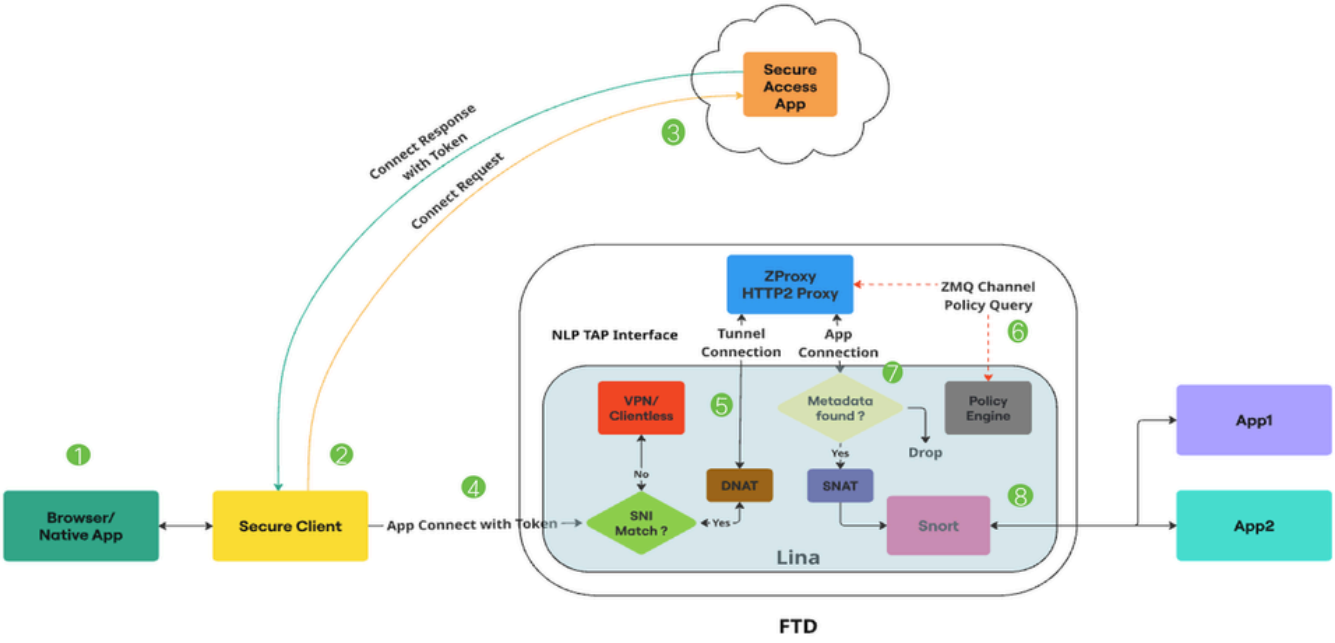
3. يعيد Secure Access توجيه العميل الآمن نحو FTD مع الرمز المميز للمصادقة.

4. يقوم Secure Client بإنشاء اتصال آخر ب FTD ، وهو اتصال HTTP2 عبر قناة mTLS. إنه يرسل طلب اتصال للتطبيق الذي يتم الوصول إليه مع الرمز المميز.

5. يقوم FTD الآن بالتحقق من صحة الرمز المميز، إذا تم التحقق من صحة الرمز المميز بنجاح، يسمح للمستخدم بالوصول إلى ذلك التطبيق. وبعد ذلك يقوم برنامج الإرساال فائق السرعة (FTD) بإرسال الإقرار مرة أخرى إلى العميل الآمن

تدفق الحزمة

تدفق حزم ZTNA التفصيلي العالمي



ZTA العالمي - تدفق الحزمة

1. يحاول المستخدم الوصول إلى تطبيق من خلال متصفح ويب أو تطبيق أصلي.

2. يعترض "العميل الآمن" الاتصال ويعرفه كمستخدم يحاول الوصول إلى مورد خاص.

3. يقوم العميل الآمن بإنشاء اتصال mTLS للوصول الآمن، وطلب الوصول إلى التطبيق.يقوم Secure Access بفحص سياسات ZTNA العالمية وتوصيفات الوضع للتوافق.إذا كان كل شيء على ما يرام، يقوم Secure Access بإنشاء رمز مميز للوصول يحتوي على معلومات أساسية مثل تفاصيل المستخدم وتفاصيل التطبيق ونهج IPS/File.

4. يتم تشفير الرمز المميز للوصول وتوقيعه بواسطة Secure Access. ثم يقوم Secure Access بإعادة توجيه العميل الآمن مع الرمز المميز إلى FTD.

5. عند وصول الحزمة إلى بيانات Lina، يعترض مقدم SNI الاتصال ويتحقق مما إذا كان اسم الخادم (امتداد SNI) في "مرحبا" العميل يطابق FQDN للوكيل الذي تم تكوينه على الجهاز.إذا تطابق SNI، يتم توجيه الاتصال إلى ZProxy. إذا لم يتطابق SNI، يتم توجيه الاتصال إلى ميزات أخرى يمكن أن تتعايش مع ZTNA العالمية.

على سبيل المثال: VPN أو Captive Portal أو ZTNA التي لا تحتاج إلى عميل. سيتم تشغيل ZProxy، الذي يدعم MASQUE عبر بروتوكول HTTP/2 على FTD كعملية غير LINA على النوى المخصصة. يستخدم الاتصال بين Lina و ZProxy واجهة NLP TAP، لمعالجة حركة مرور البيانات.تتم ترجمة IP الوجهة للاتصال إلى IP واجهة TAP بواسطة مقدم SNI.

6. عندما يستقبل ZProxy نفق اتصال mTLS من "العميل الآمن"، فإنه يتحقق من شهادة جهاز العميل المرسلة من "العميل الآمن". كما يتحقق من إرسال رمز الوصول المميز باستخدام اتصال APP. لا توجد قناة MQ بين Lina و ZProxy. يتم استخدامه بشكل أساسي لتبادل رسائل التحكم. يستخدم ZProxy هذه القناة لحل FQDN للموارد الخاصة عن طريق الاتصال ب Lina.

يتم إستخدام قناة Zero MQ أيضا لدعم المعلومات الموجودة في الرمز المميز للوصول إلى Lina.(مثال : معرف القاعدة ومعرف السياسة وما إلى ذلك) تتلقى Lina معلومات رمز الوصول المميز وتخزنها في قاعدة بيانات تعريف.

7. بمجرد تبادل رسائل التحكم، تبدأ ZProxy في إنشاء اتصال جديد للمورد الخاص. يمكن أن يكون هذا TCP أو UDP. بعد ذلك يقوم LINA بإجراء بحث بيانات تعريف db للاتصال التطبيق هذا. إذا لم يتم العثور على بيانات التعريف، يتم إسقاط الاتصال

8. بما أن اتصال التطبيق منشأ من ZProxy، فسيكون له IP داخلي (على سبيل المثال:169.251.1.2) كمصدر IP. ستتم ترجمة هذا إلى IP الخاص بواجهة الخروج الخاصة ب FTD، قبل إرسالها. ثم يقوم Lina بتعليم تدفقات Universal Zero Trust لفحص SNORT فقط في حالة وجود ملف أو نهج IPS في الرمز المميز للوصول.يتم تمرير معرف القاعدة الذي تم الحصول عليه من الرمز المميز للوصول إلى Snort في بيانات تعريف الاتصال.

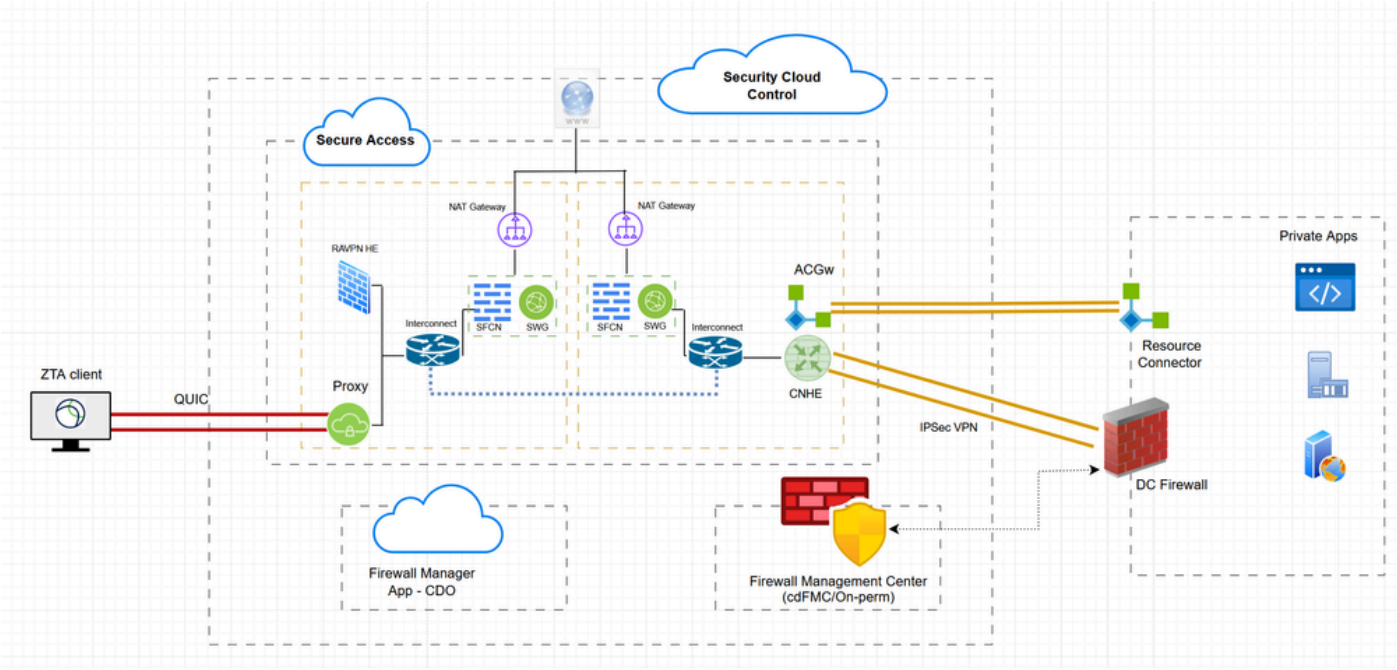
9. يتم دفع قواعد الثقة الصفرية العالمية وتعيينات سياسة الملفات و IPS المقابلة

إلى FTD عبر FMC. سيقوم المكون الإضافي "عدم الثقة" في Snort بتحميل هذه القواعد فقط SNORT Inspection ل Universal Zero Trust بتعليم تدفقات Lina سيقوم.أثناء التهيئة. في حالة ذكر نهج "ملف" أو IPS في الرمز المميز للوصول الذي تم الحصول عليه من "الوصول الآمن" للوصول إلى هذا المورد الخاص.

يتم تمرير معرف القاعدة الذي تم الحصول عليه من الرمز المميز للوصول إلى Snort عبر CONN META. بالنسبة لجميع تدفقات دفق Universal Zero Trust، سيقوم المكون الإضافي ل Zero Trust في Snort بإجراء بحث عن القاعدة لمعرف القاعدة الذي تم الحصول عليه من تعريف Conn. إذا تم العثور على تطابق القاعدة، سيتم السماح بالتدفق، وسيتم تطبيق نهج IPS و File المحددة لتلك القاعدة على التدفق. إذا لم يتم العثور على تطابق القاعدة، سيقوم المكون الإضافي Zero Trust في Snort بحظر التدفق.

التكوين

الرسم التخطيطي للشبكة



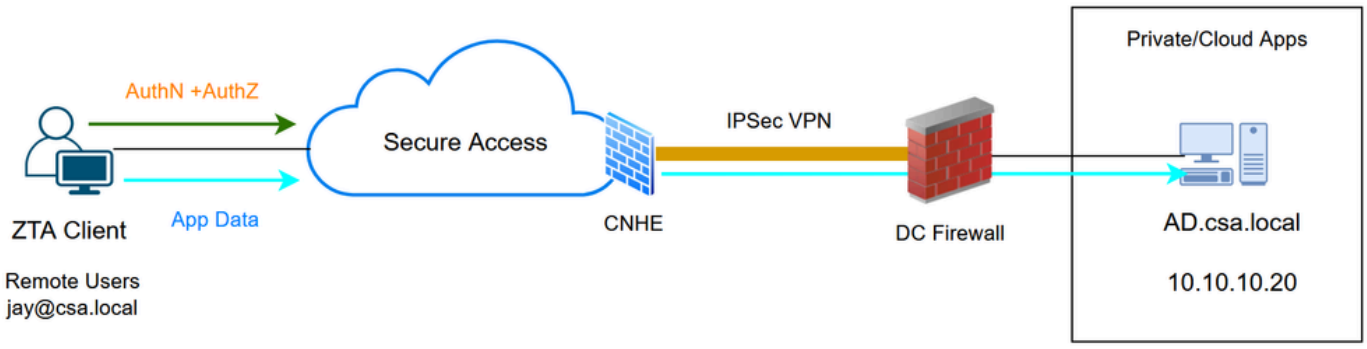
ZTNA المختلط - الرسم التخطيطي للشبكة

حالات الاختبار

حالة الاختبار 1 : المستخدم البعيد - تنفيذ السحابة

في حالة الاختبار هذه، سنقوم بالوصول إلى مورد خاص عبر مجموعة نفق الشبكة من خلال

تطبيق السحابة. في هذه الحالة، يتم اعتراض كل من تقييم السياسة وبيانات التطبيق بواسطة Secure Access عبر وحدة ZTA . هذا تدفق تقليدي حيث يمكننا الوصول إلى التطبيق الخاص من عميل ZTA المسجل عبر مجموعة نفق الشبكة أو موصل الموارد

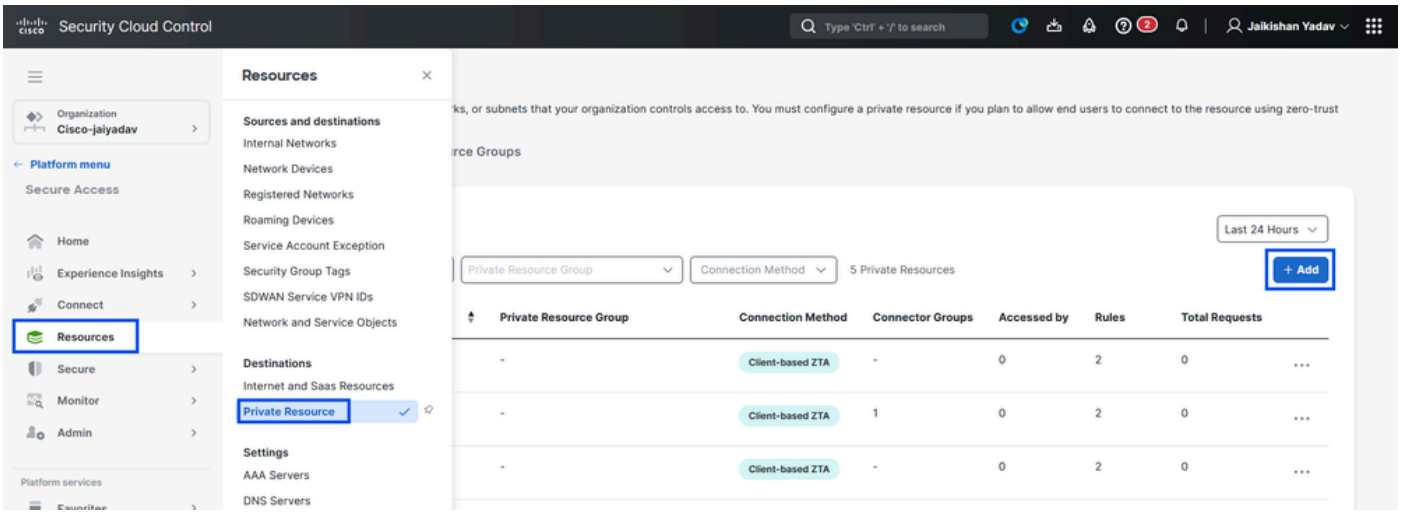


ZTA العالمي - طوبولوجيا حالة الاختبار

الخطوة 1 - تحديد مورد خاص على الوصول الآمن

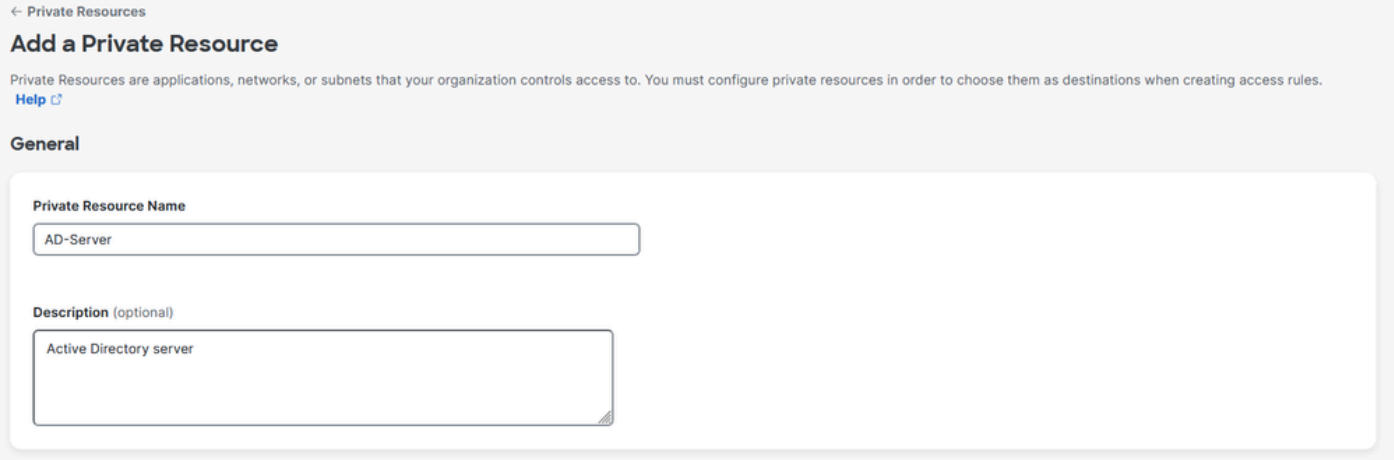
تكوين مورد خاص ليتم الوصول إليه عبر الجهاز المسجل في الوصول إلى عدم الثقة (ZTA) باستخدام فرض السحابة

1. انتقل إلى الموارد > الوجهات > الموارد الخاصة > انقر فوق +إضافة



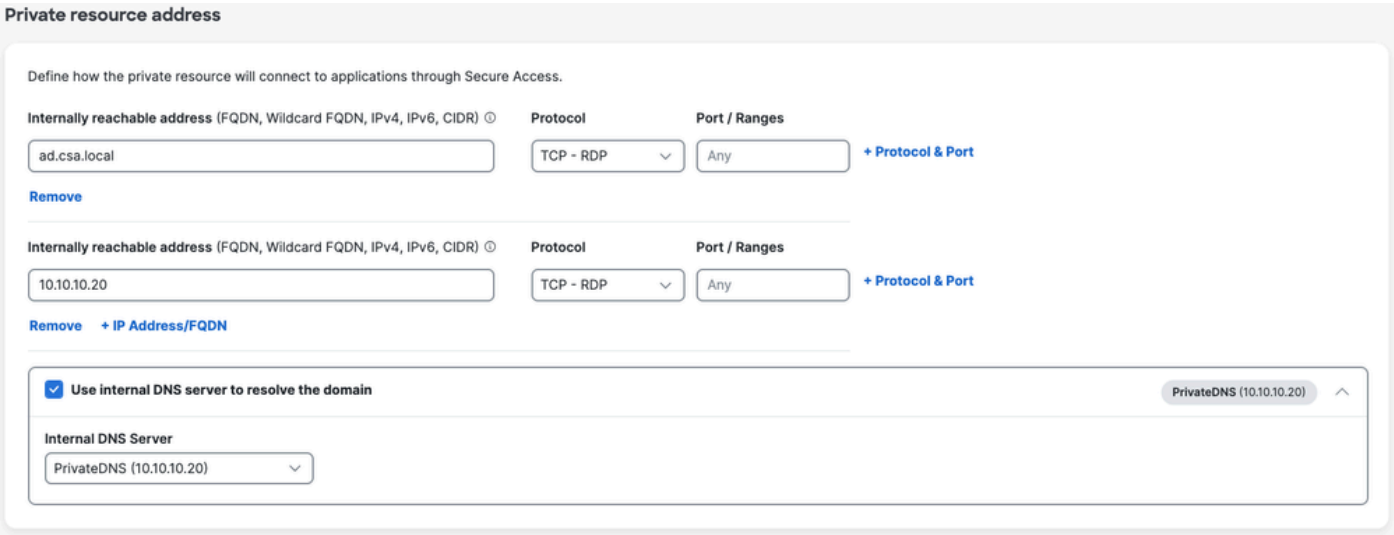
الوصول الآمن - تكوين الموارد الخاصة

2. بالنسبة إلى اسم المورد الخاص، أدخل اسما ذا معنى للمورد. للحصول على الوصف، نوصي بتوفير معلومات مثل الغرض من المورد أو اسم مالك المورد.

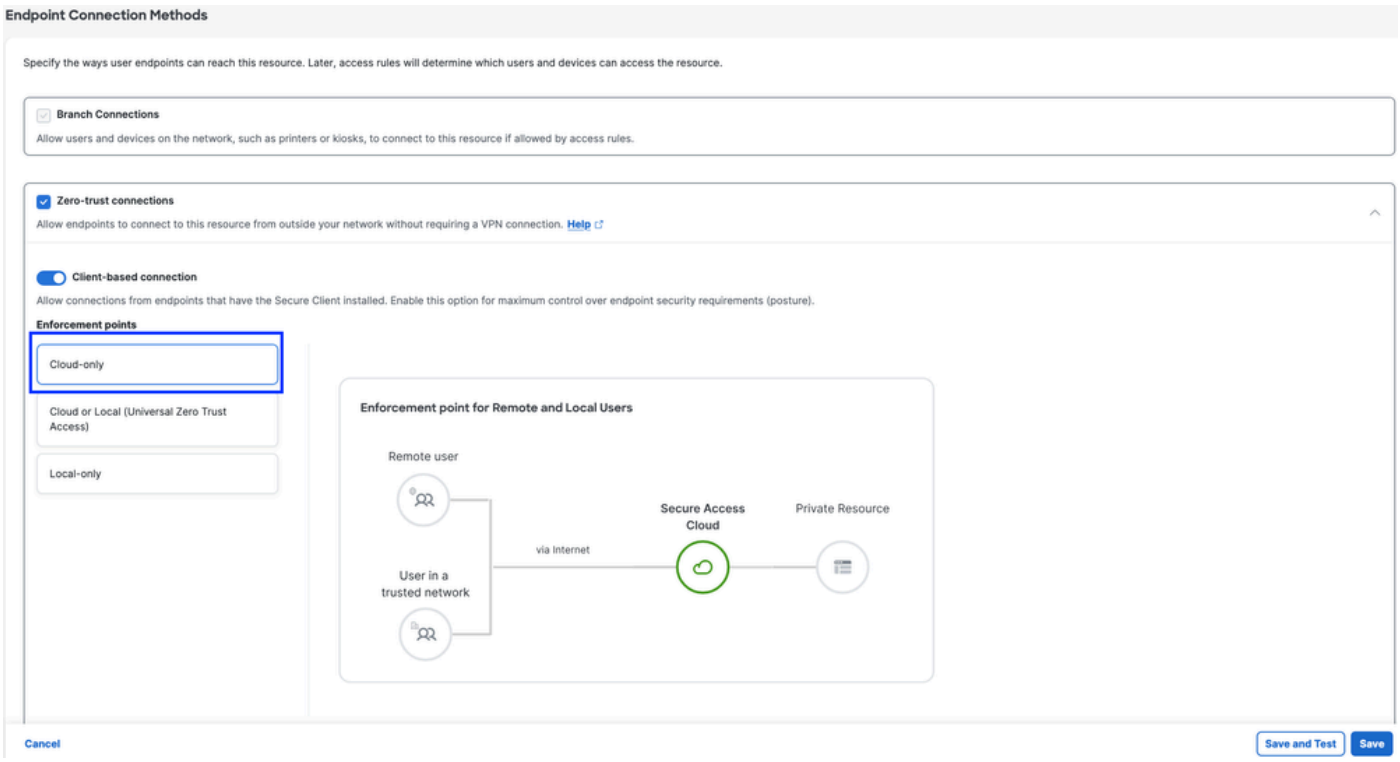


3. أدخل FQDN للمورد الخاص الذي تريد الوصول إليه . كما يمكنك تحديد عنوان IP الخاص باﻟﻤﻮرد الخاص . لمزيد من المعلومات، راجع [إضافة مورد خاص]

4. حدد خادم DNS الداخلي لحل المجال



5. تحديد أسلوب اتصال نقطة النهاية



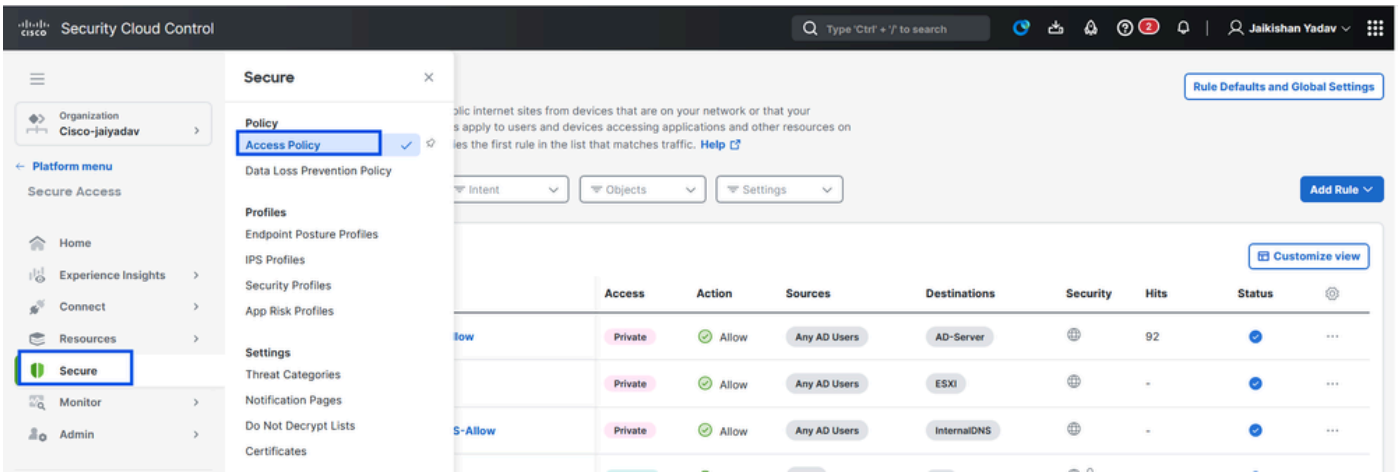
الوصول الآمن - تكوين الموارد الخاصة

6. انقر فوق حفظ

الخطوة 2 - إنشاء قاعدة وصول خاصة

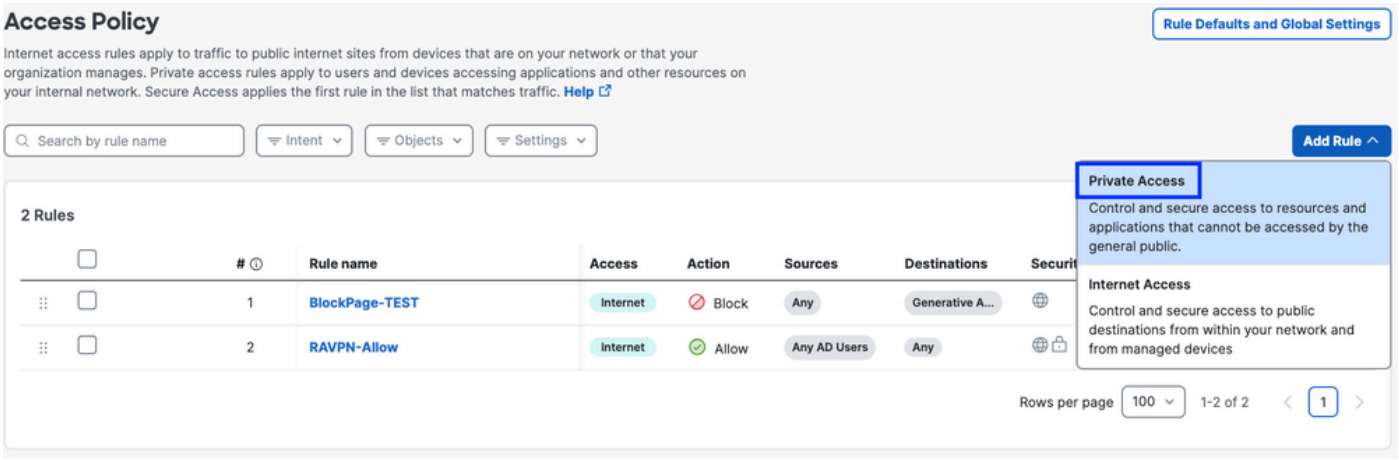
يتمكن المستخدمون المسجلون في ZTA العالمية من Secure Access من تكوين وصول خاص على Secure Access. لمزيد من المعلومات، راجع قاعدة الوصول الخاص. من الوصول إليه .

1. انتقل إلى آمن > نهج الوصول



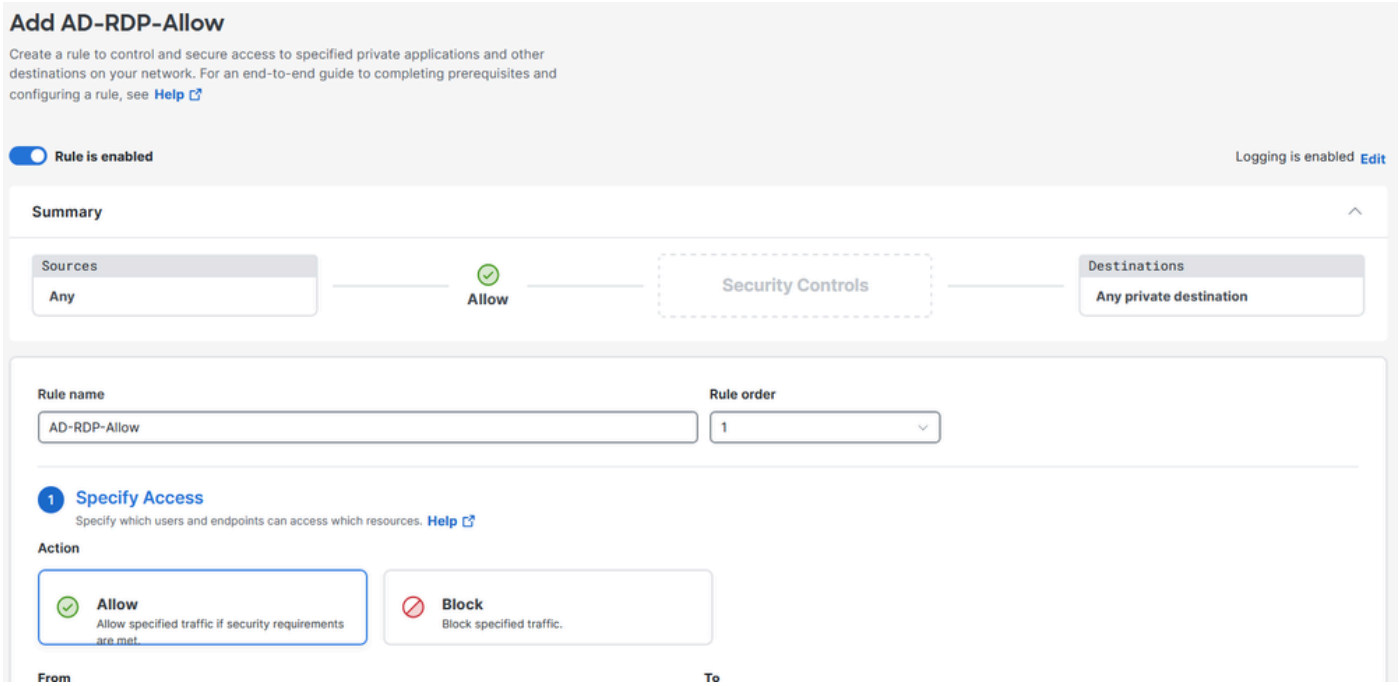
الوصول الآمن - تكوين سياسة الوصول

2. انقر فوق إضافة قاعدة، ثم أختر Private Access.
في أعلى القاعدة يوجد ملخص يصف المكونات المكونة للقاعدة الخاصة بك.



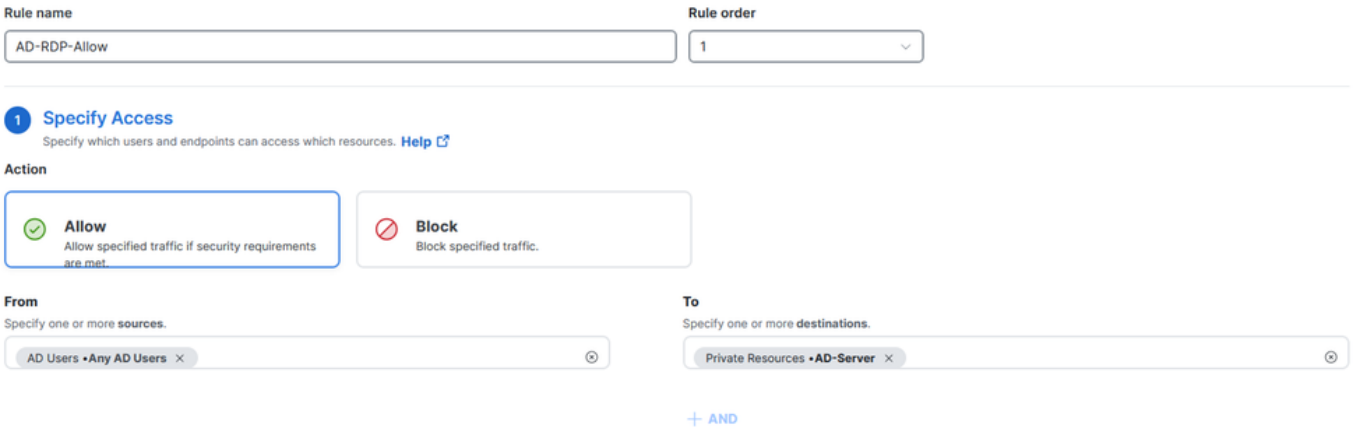
الوصول الآمن - تكوين سياسة الوصول

3. إضافة اسم قاعدة



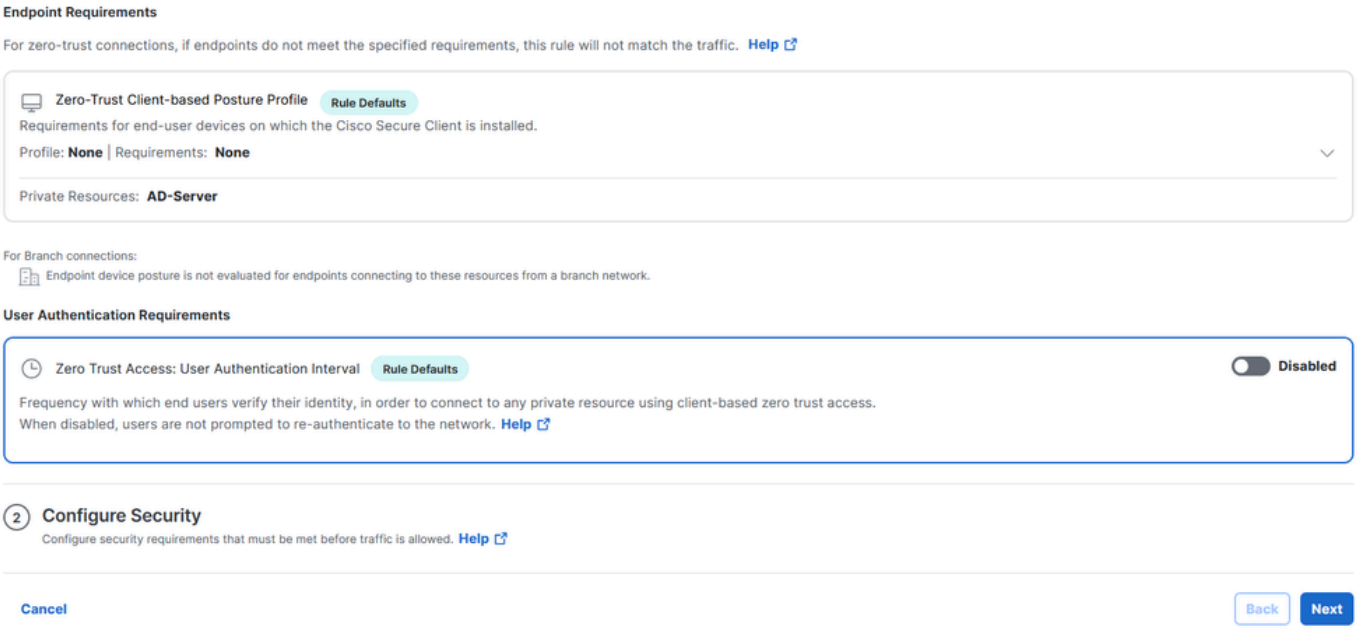
الوصول الآمن - تكوين سياسة الوصول

4. حدد إجراء القاعدة وحدد المصدر والوجهة



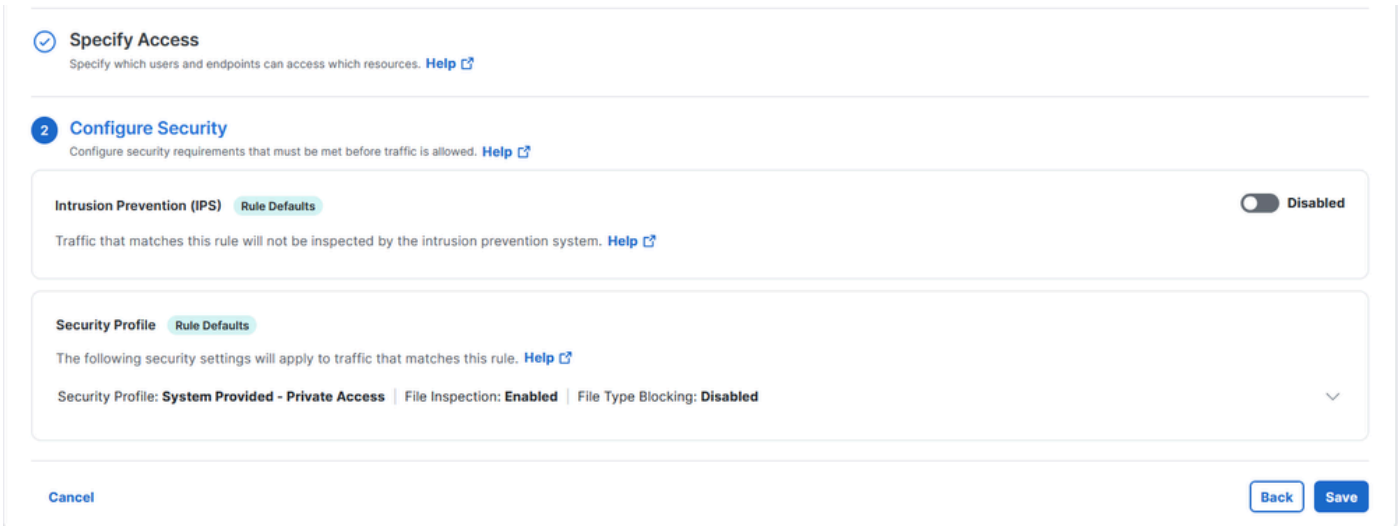
الوصول الآمن - تكوين سياسة الوصول

5. تكوين متطلبات نقطة النهاية



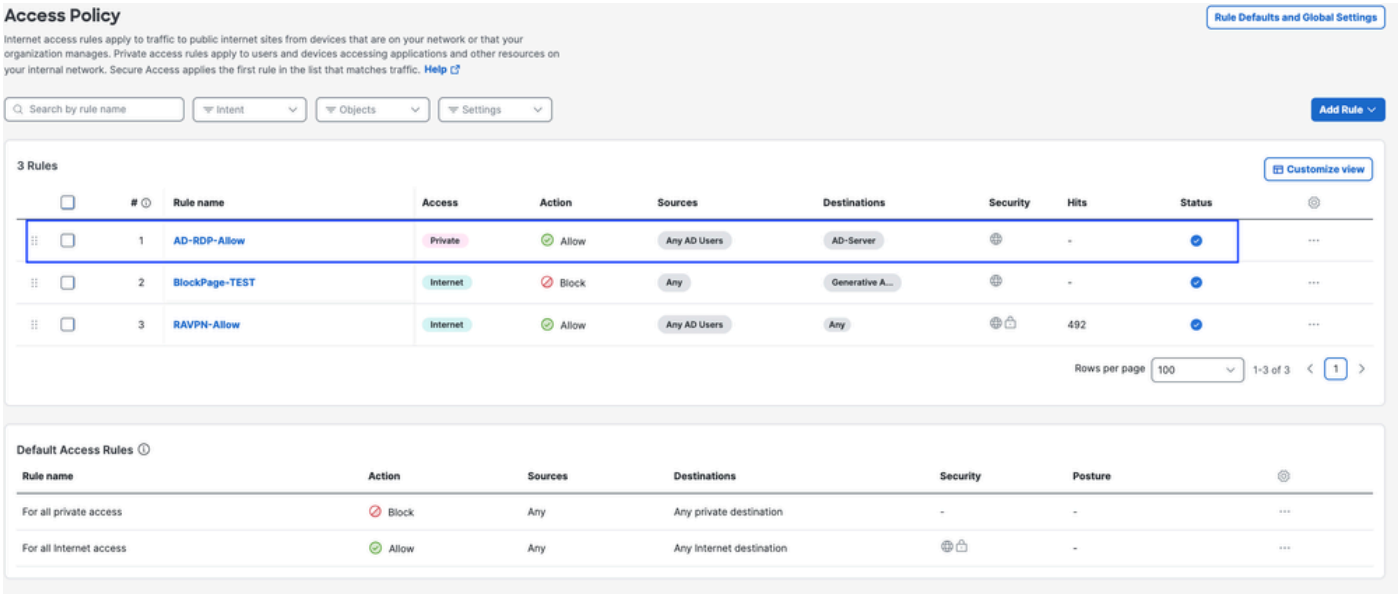
الوصول الآمن - تكوين سياسة الوصول

6. تكوين الأمان



الوصول الآمن - تكوين سياسة الوصول

7. انقر فوق حفظ

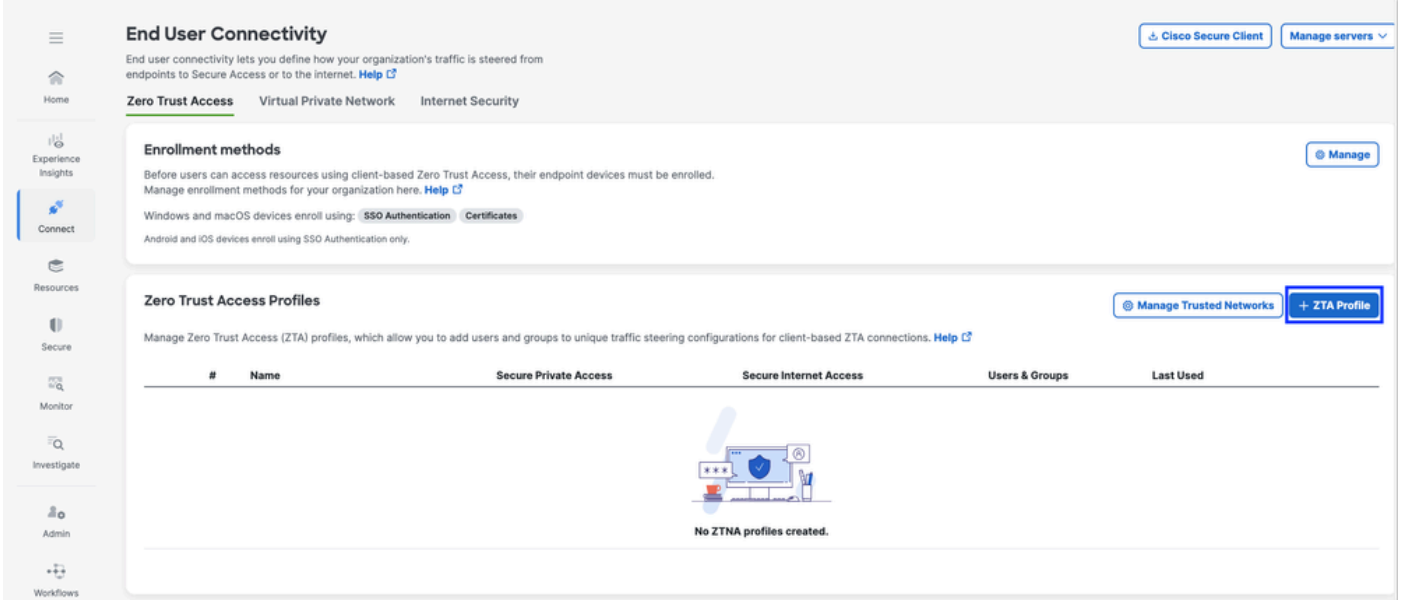


الوصول الآمن - تكوين سياسة الوصول

الخطوة - 3 إضافة مورد خاص إلى ملف تعريف ZTA

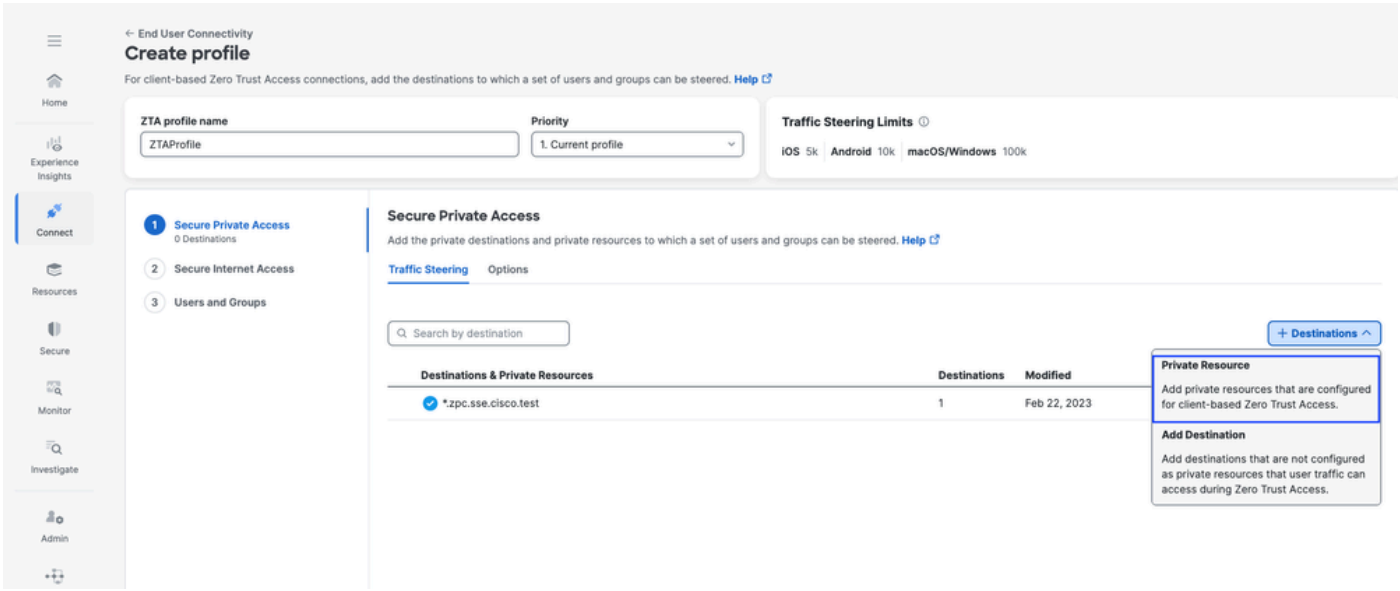
إذا كنت تستخدم ملف تعريف ZTA مخصص، فإنك تحتاج لإضافة المورد الخاص المعني إلى ملف تعريف ZTA

1. انتقل إلى الاتصال > اتصال المستخدم النهائي > الوصول إلى انعدام الثقة وانقر فوق +ملف تعريف ZTA

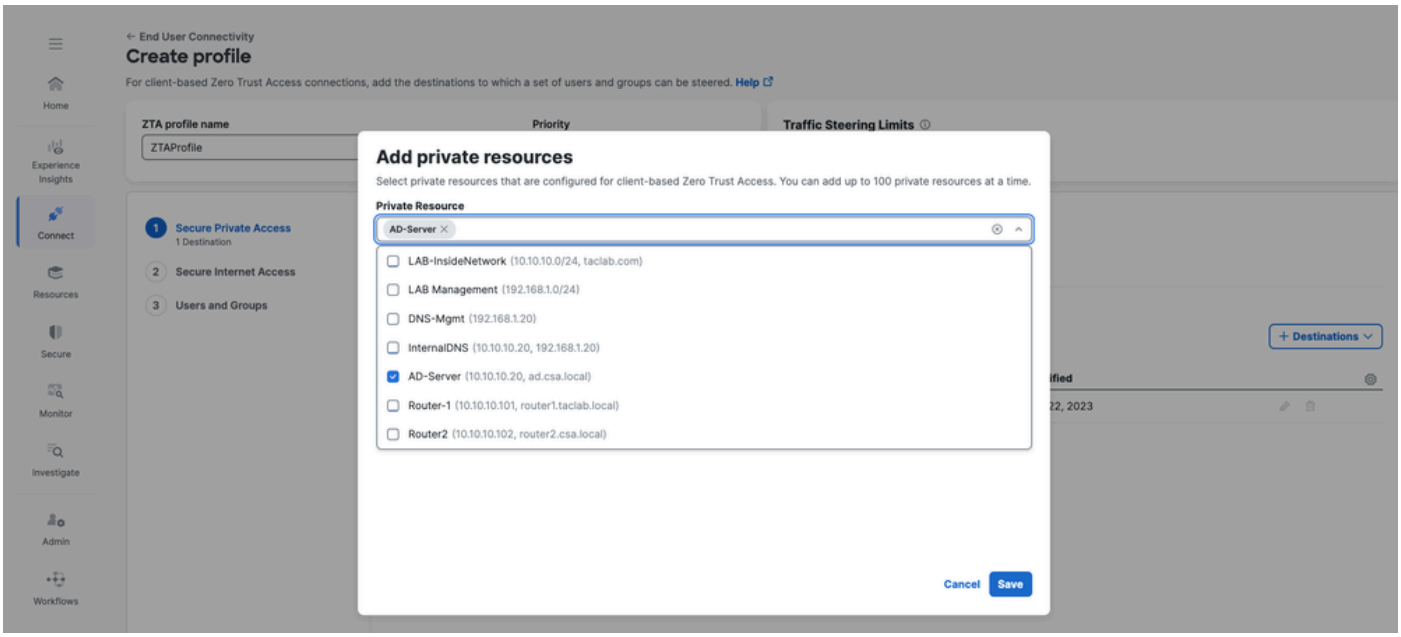


الوصول الآمن - ملف تعريف ZTA

2. إضافة المورد الخاص

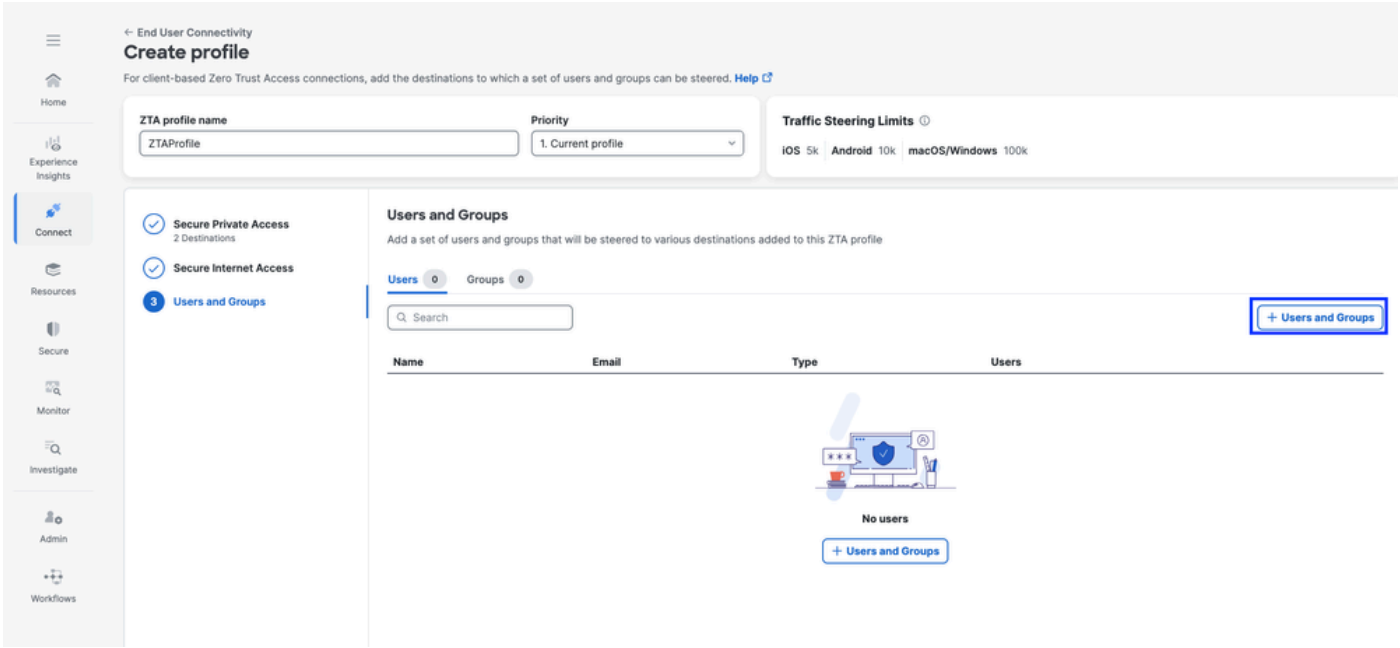


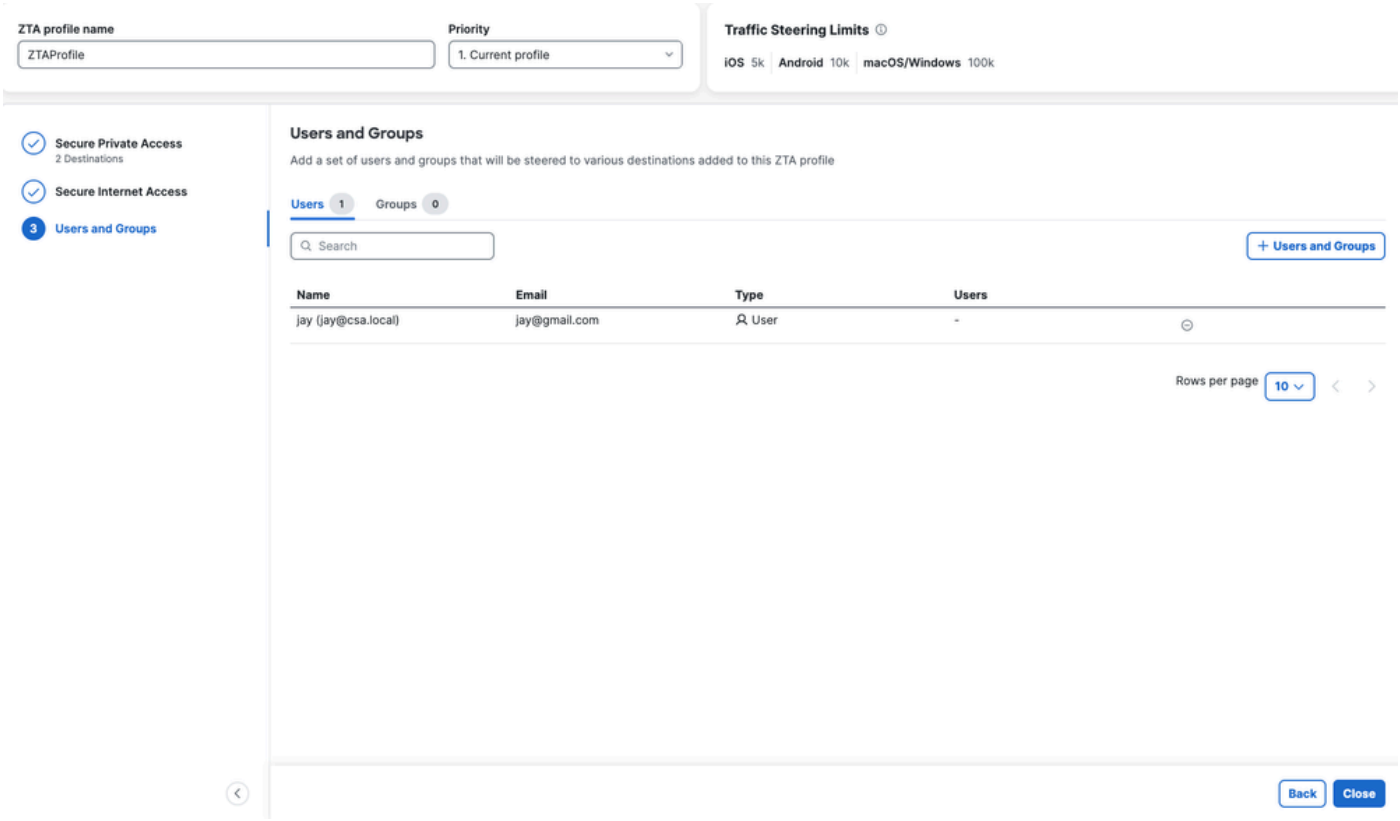
الوصول الآمن - ملف تعريف ZTA



الوصول الآمن - ملف تعريف ZTA

3. إضافة مستخدمين ومجموعات





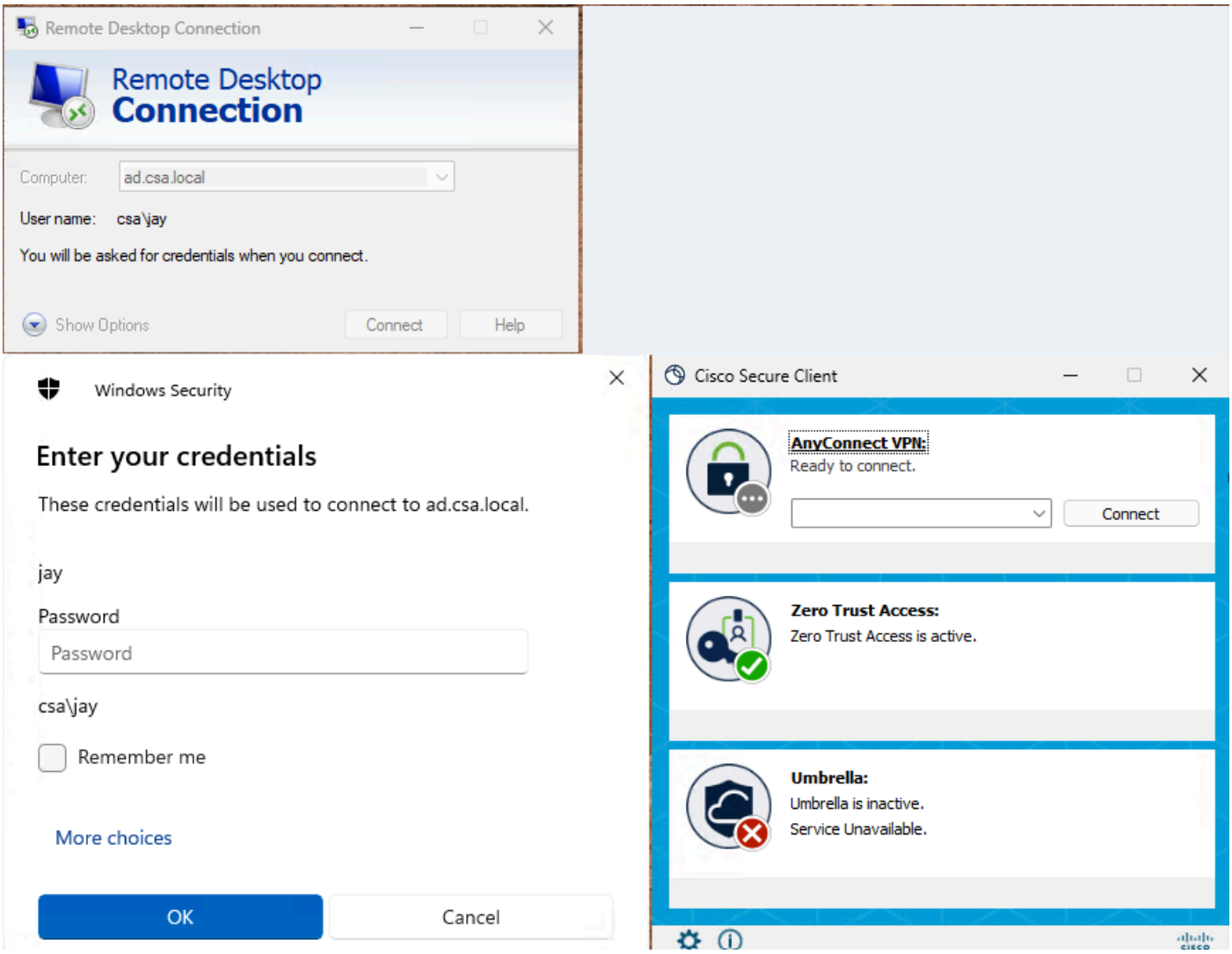
الوصول الآمن - ملف تعريف ZTA

ملاحظة: قد يستغرق الأمر من 15 إلى 20 دقيقة دفع التكوين ومزامنته مع العميل للمورد الخاص المعين

الخطوة 4 - التحقق من الوصول إلى المورد الخاص

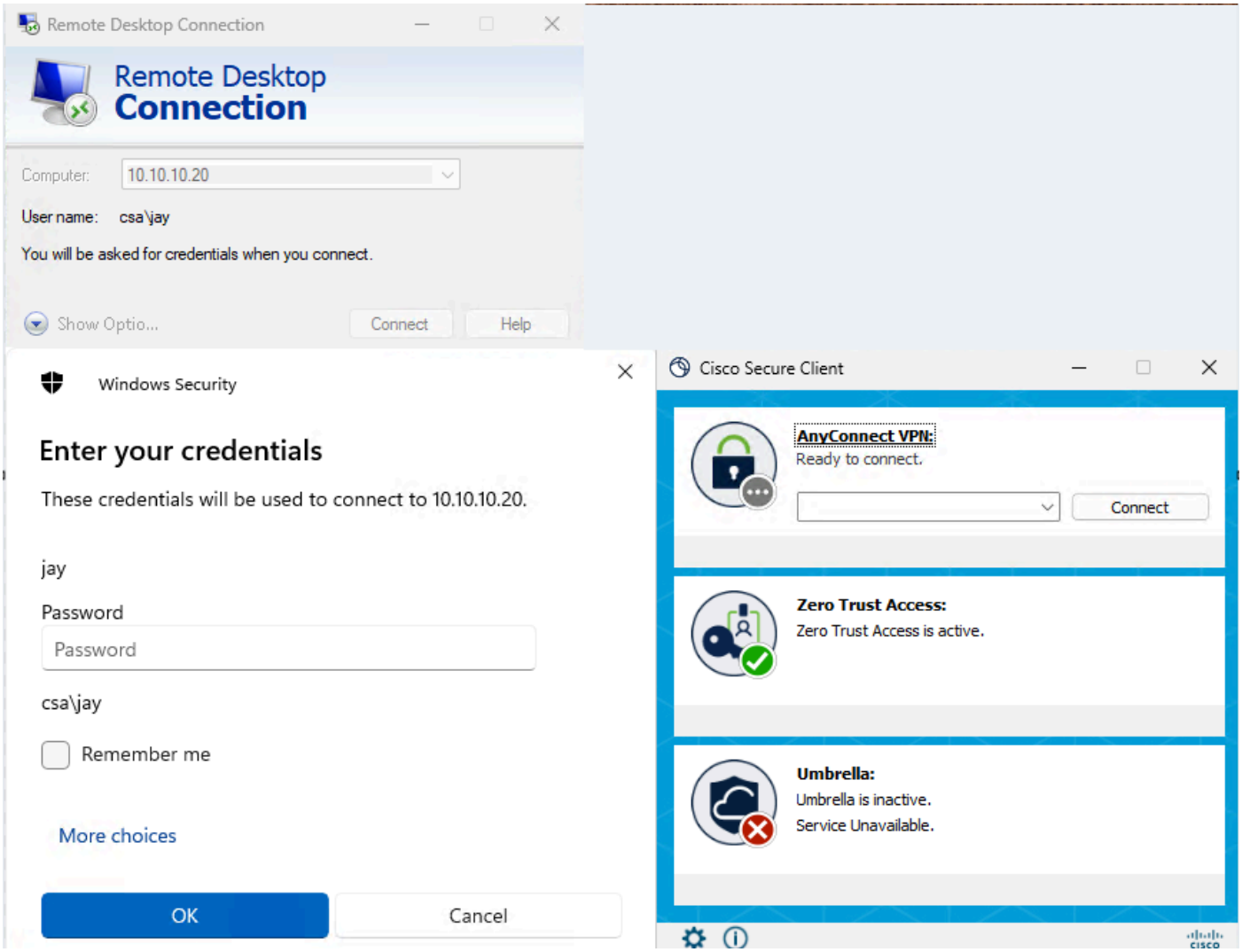
1. الوصول إلى المورد الخاص

الوصول إلى PR باستخدام FQDN



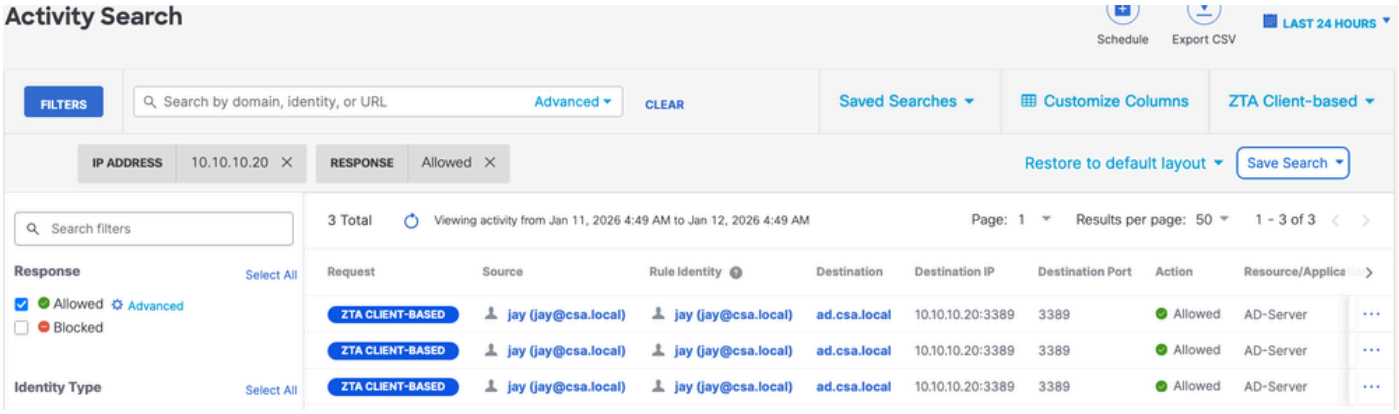
الوصول الآمن - إختبار العلاقات العامة

الوصول إلى PR باستخدام عنوان IP

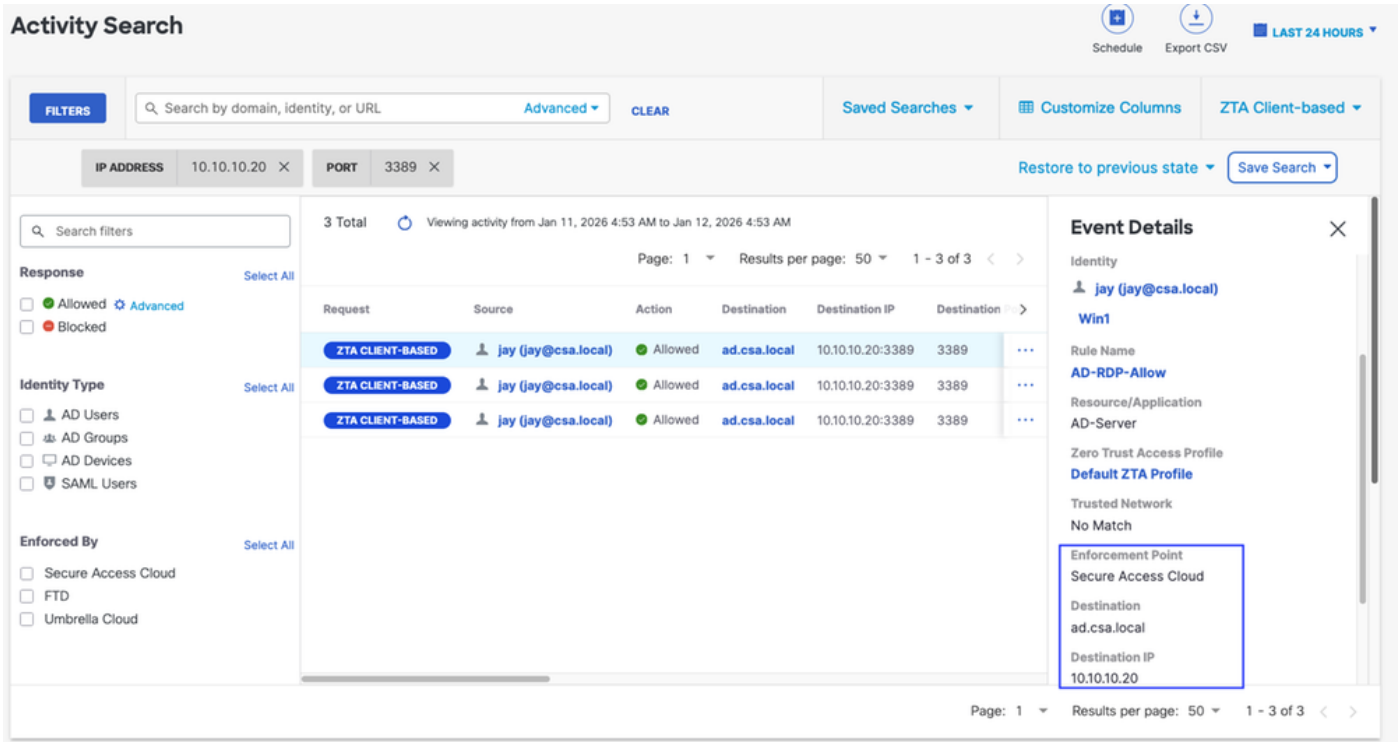


الوصول الآمن - إختبار العلاقات العامة

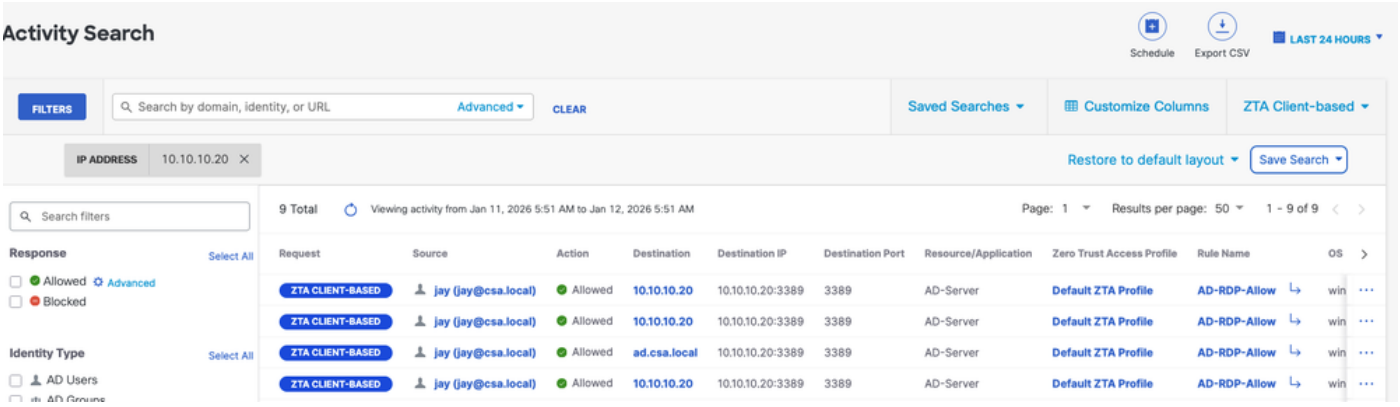
2. التحقق باستخدام أحداث البحث عن النشاط



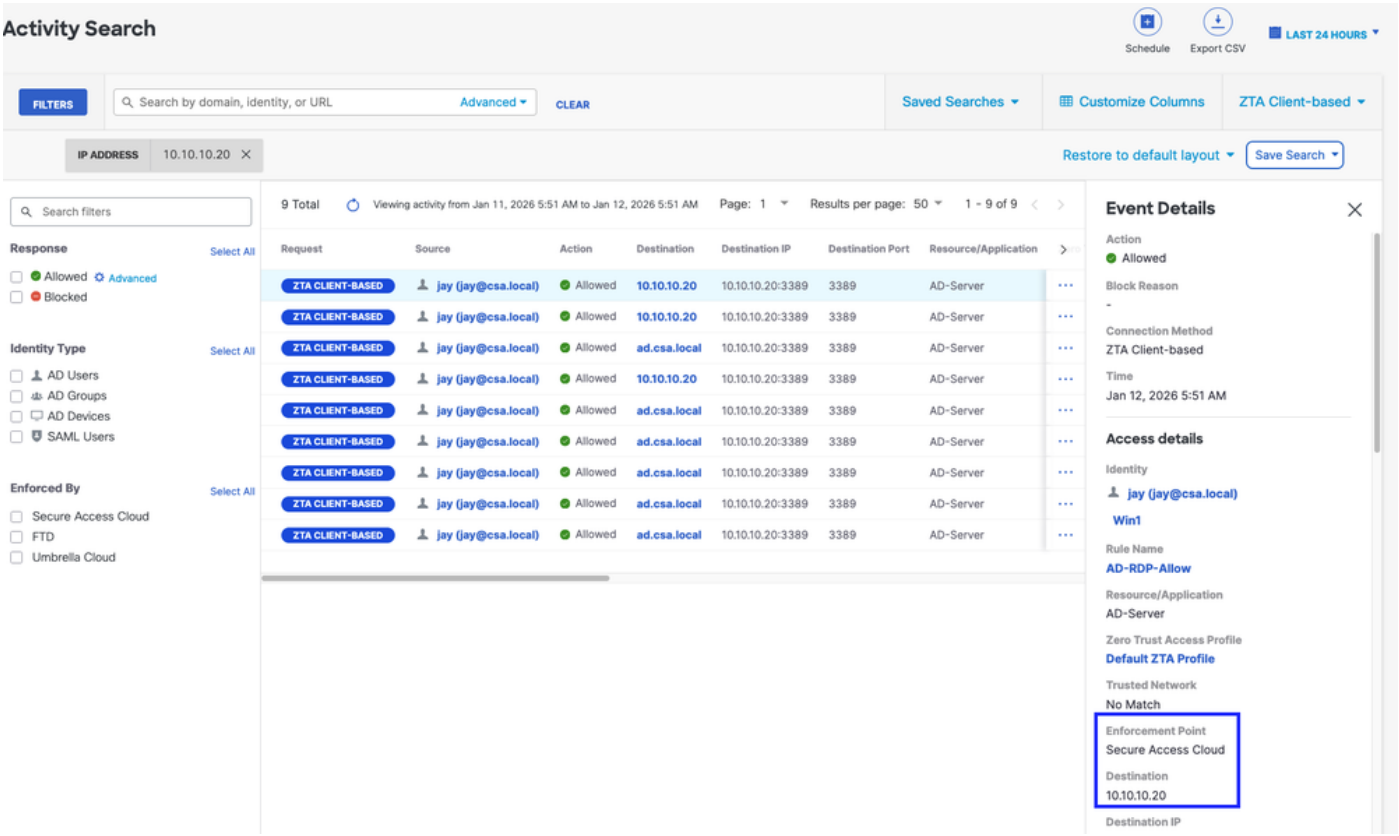
الوصول الآمن - البحث عن الأنشطة



الوصول الآمن - البحث عن الأنشطة

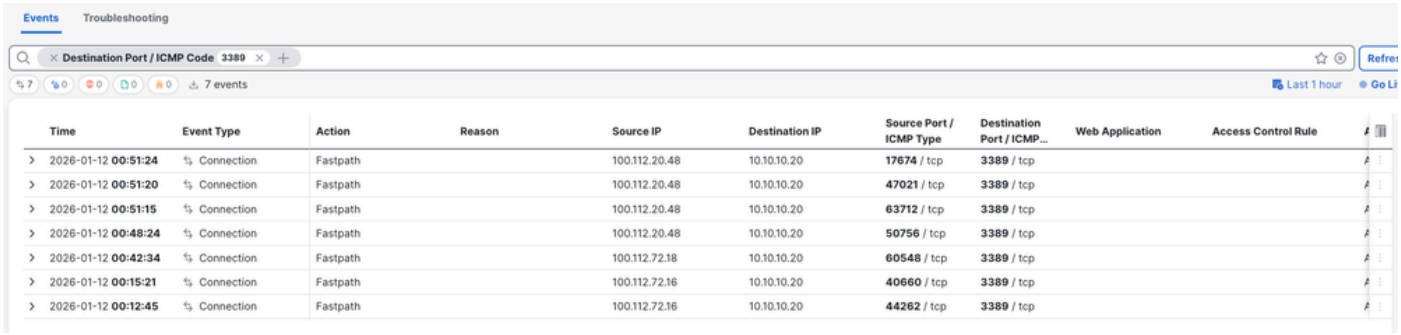


الوصول الآمن - البحث عن الأنشطة



الوصول الآمن - البحث عن الأنشطة

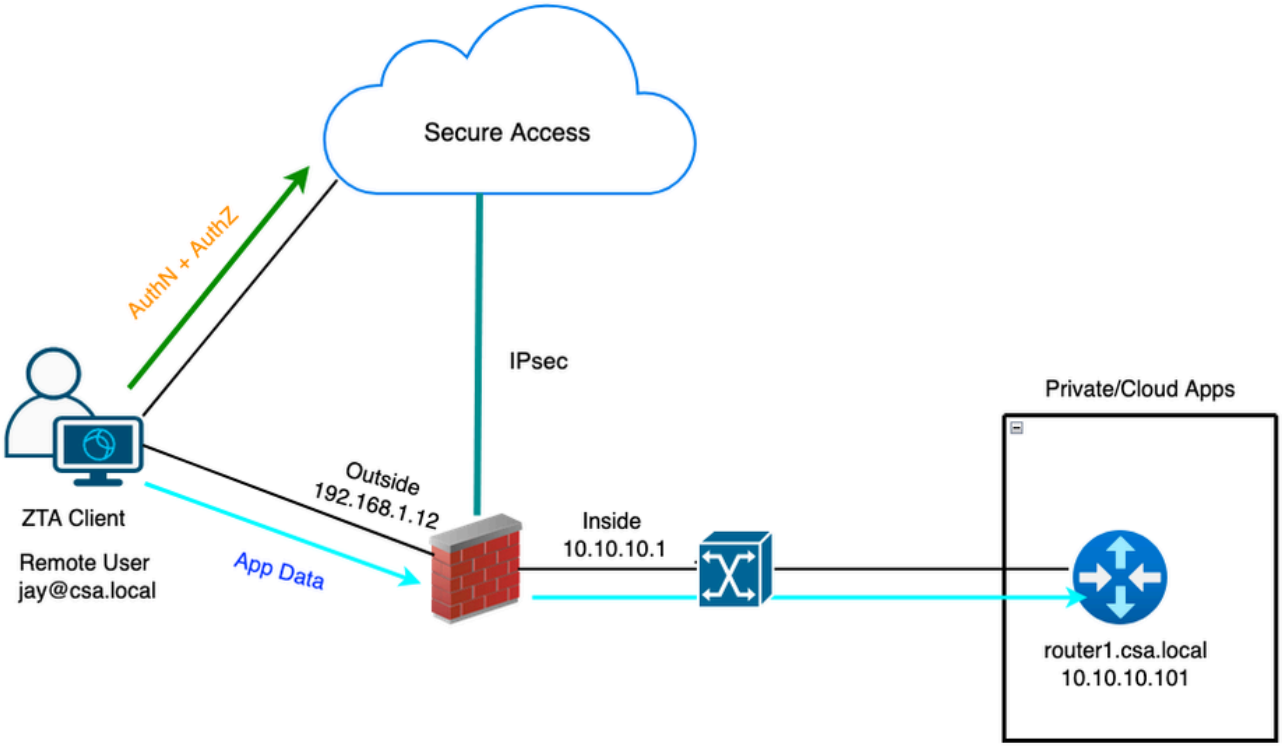
3. التحقق من أحداث اتصال FMC



أحداث اتصال FMC

إختبار الحالة 2 - مستخدم بعيد - تنفيذ محلي

الوصول إلى مورد خاص عبر التطبيق المحلي ، في هذا النوع من تقييم سياسة الإنفاذ يتم على Secure Access ولكن تبقى بيانات التطبيق محلية على FTD. على سبيل المثال، عميل أو مستخدم مسجل في ZTA متصل بشبكة منزلية ويحاول الوصول إلى مورد خاص موجود خلف FTD داخل الواجهة .

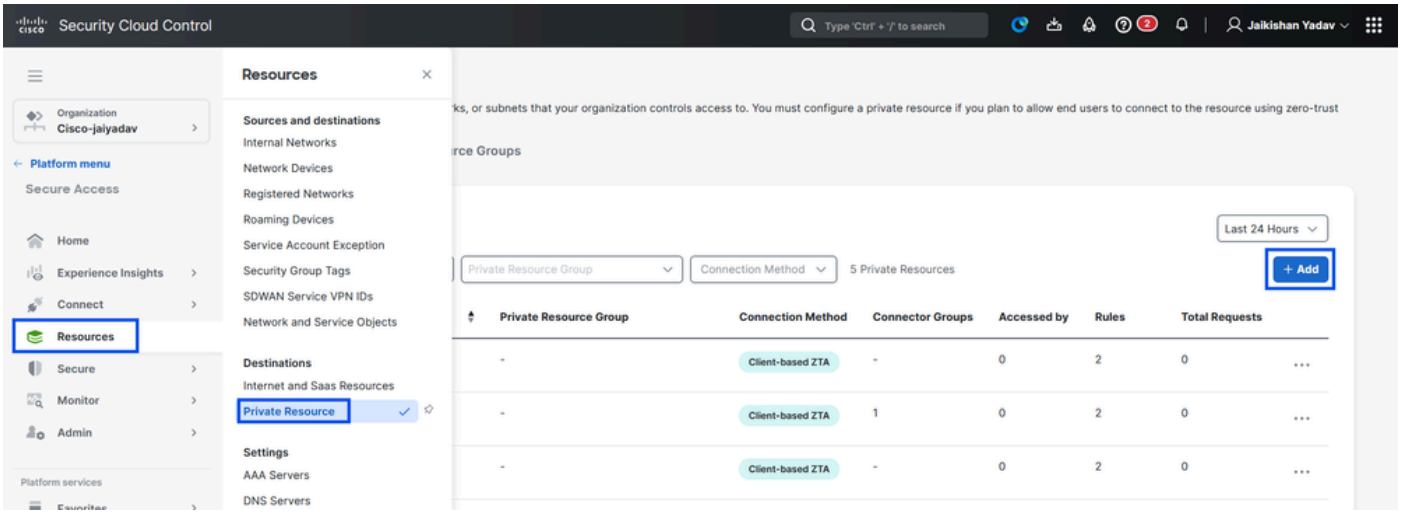


ZTA العالمي - طوبولوجيا حالة الاختبار

الخطوة 1 - تحديد مورد خاص على الوصول الآمن

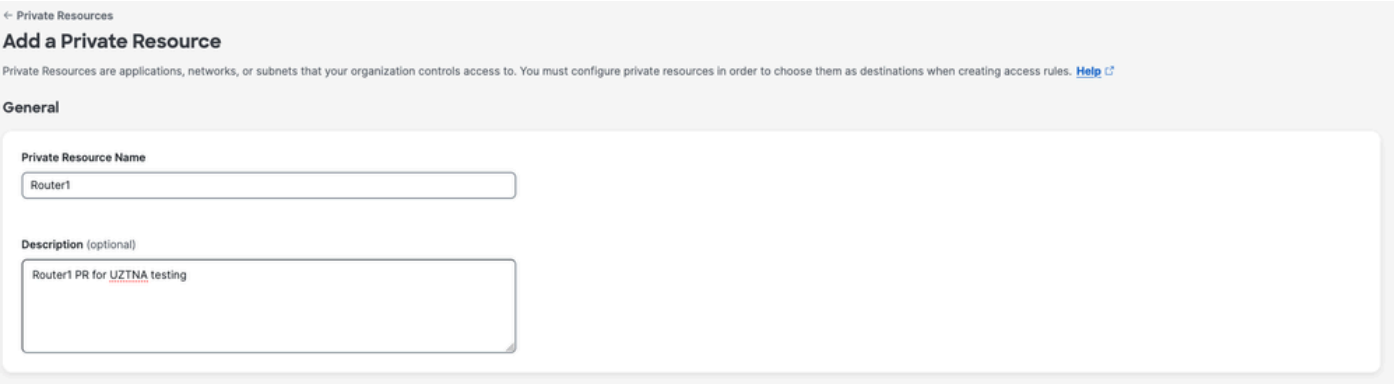
تكوين مورد خاص ليتم الوصول إليه عبر الجهاز المسجل في الوصول إلى عدم الثقة (ZTA) باستخدام فرض السحابة

1. انتقل إلى الموارد > الوجهات > الموارد الخاصة > انقر فوق +إضافة.



الوصول الآمن - تكوين الموارد الخاصة

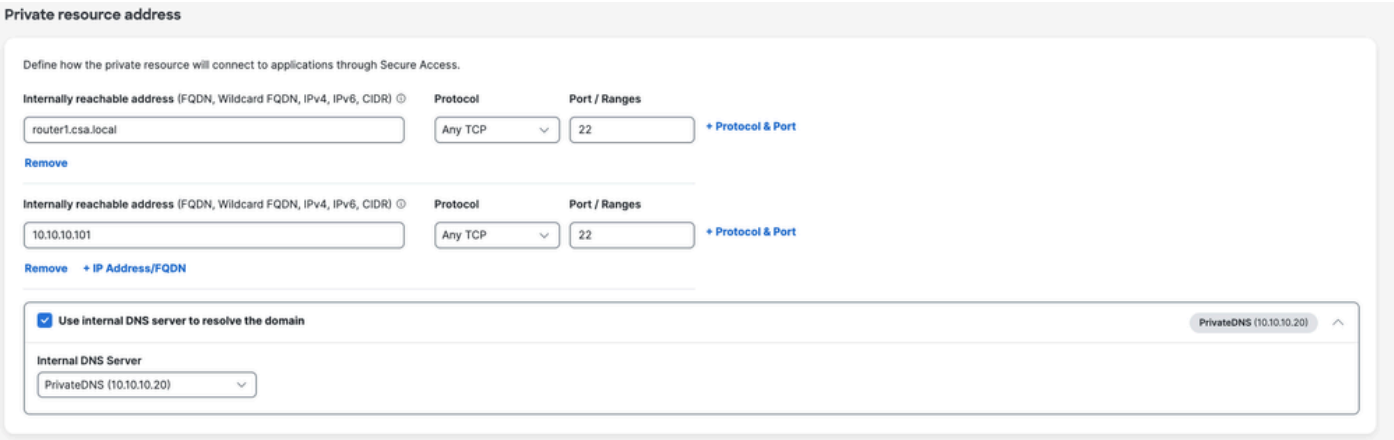
2. بالنسبة إلى اسم المورد الخاص، أدخل اسما ذا معنى للمورد. للحصول على الوصف، ونصي بتوفير معلومات مثل الغرض من المورد أو اسم مالك المورد.



الوصول الآمن - تكوين الموارد الخاصة

3. أدخل FQDN للمورد الخاص الذي تريد الوصول إليه . كما يمكنك تحديد عنوان IP الخاص بالمورد الخاص . لمزيد من المعلومات، راجع [إضافة مورد خاص]

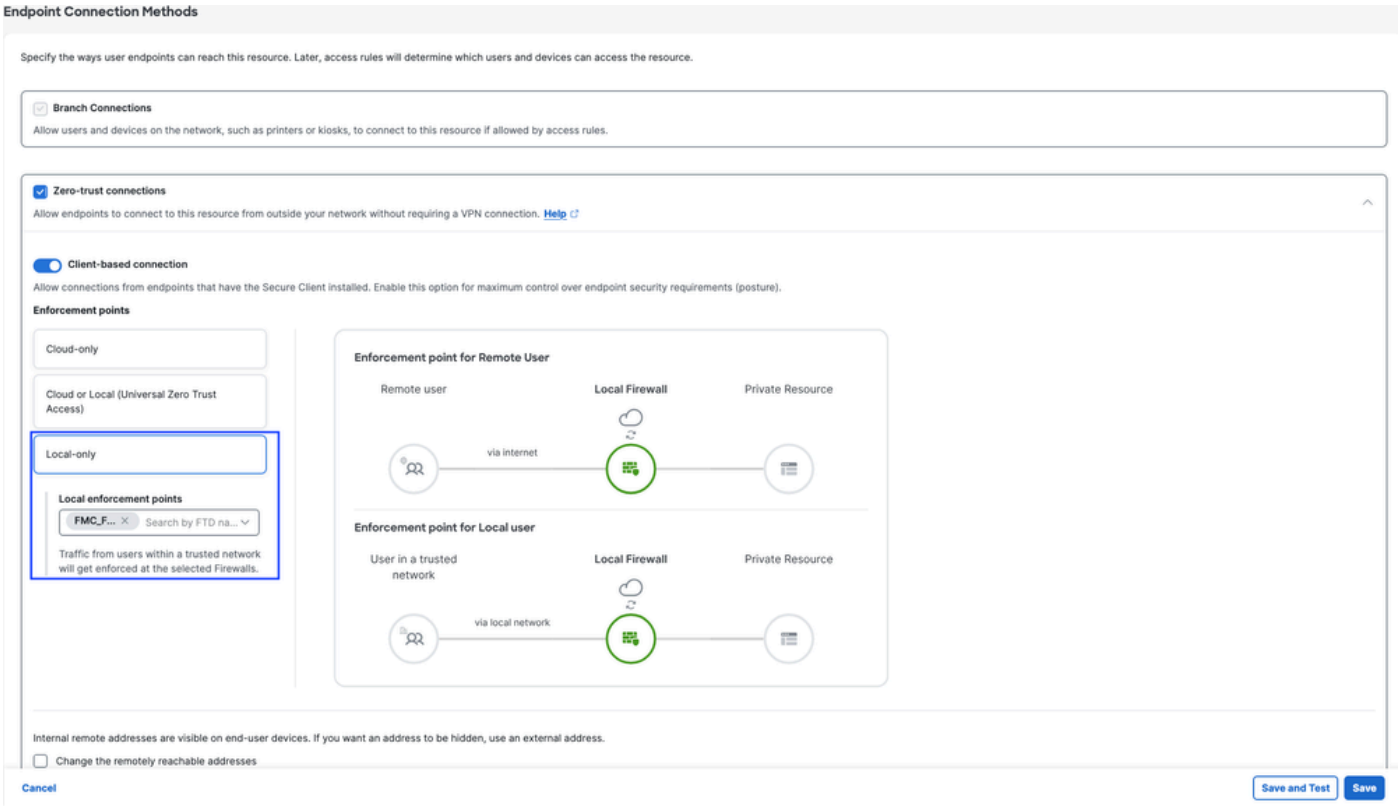
4. حدد خادم DNS الداخلي لحل المجال



الوصول الآمن - تكوين الموارد الخاصة

5. تحديد أسلوب اتصال نقطة النهاية

6. حدد FTD كنقاط تنفيذ محلية



الوصول الآمن - تكوين الموارد الخاصة

ملاحظة: اعتمادا على نوع التسجيل الذي تحدده ، سيقوم هذا التغيير بإقران PR وسيؤدي إلى تشغيل نشر النهج تلقائيا ب FTD

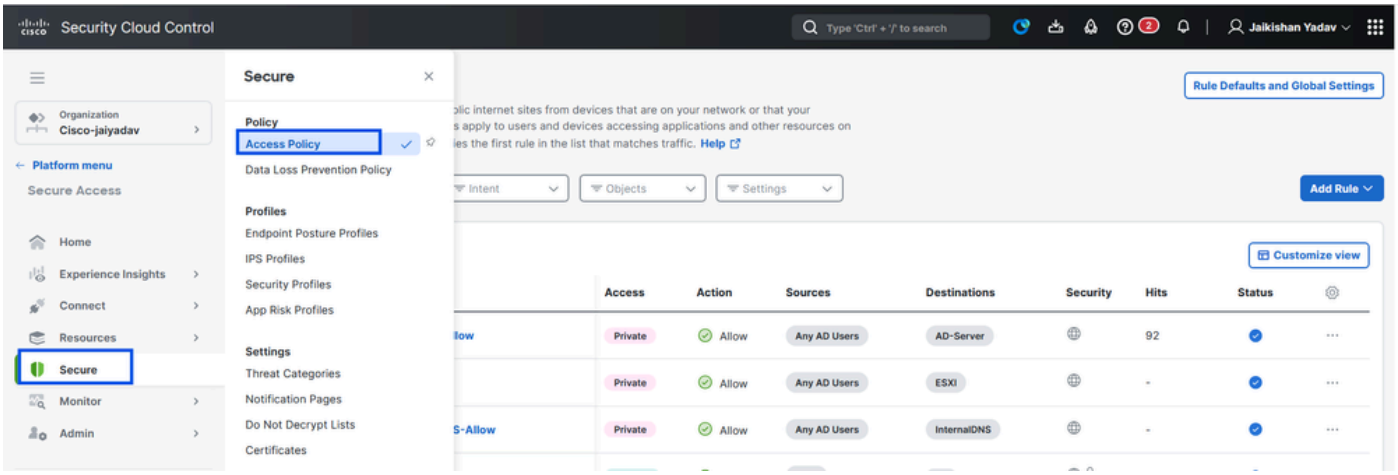
---

7. انقر فوق حفظ

الخطوة 2 - إنشاء قاعدة وصول خاصة

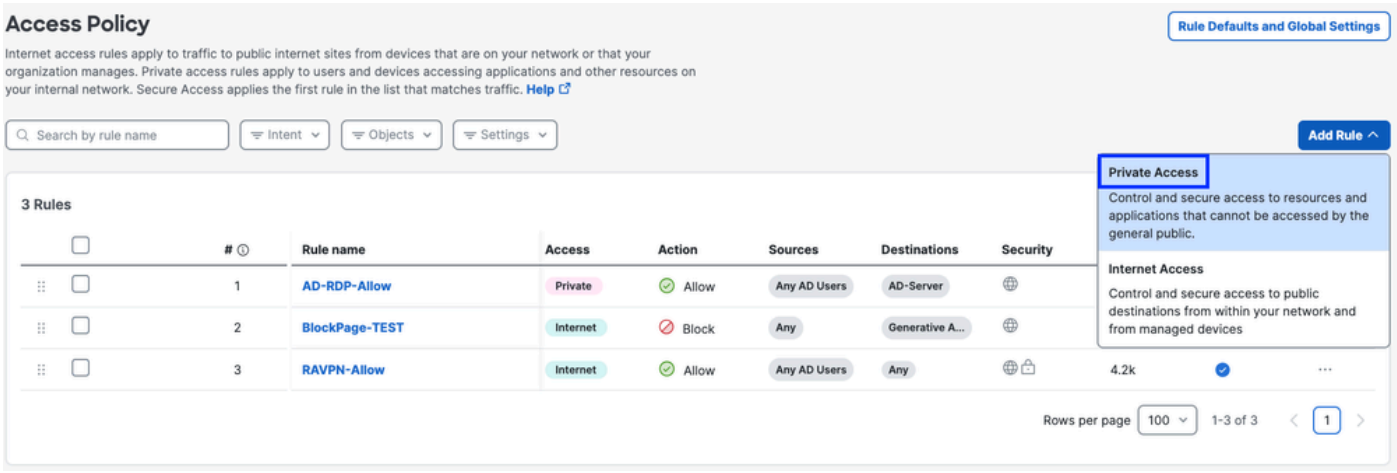
تكوين وصول خاص على Secure Access ليتمكن المستخدمون المسجلون في ZTA العالمية من الوصول إليه . لمزيد من المعلومات، راجع قاعدة الوصول الخاص

1. انتقل إلى آمن > نهج الوصول



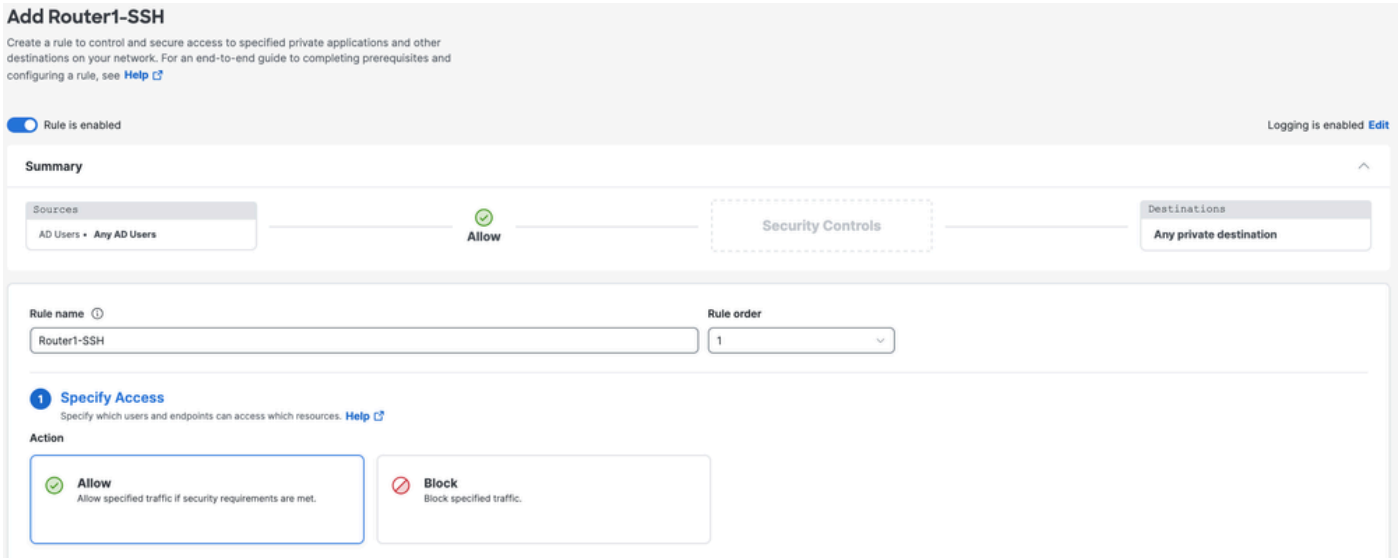
الوصول الآمن - تكوين المواردالخاصة

2. انقر فوق إضافة قاعدة، ثم أختر Private Access.
في أعلى القاعدة يوجد ملخص يصف المكونات المكونة للقاعدة الخاصة بك.



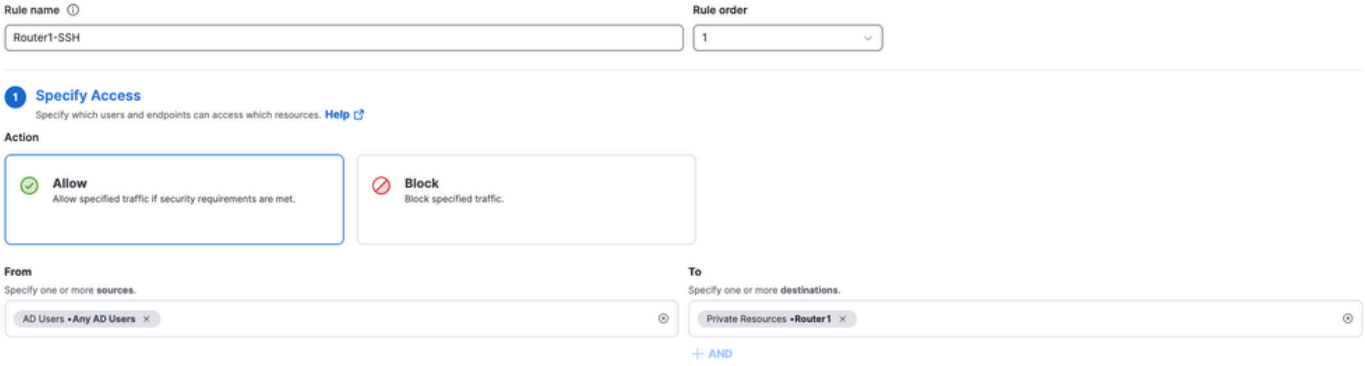
الوصول الآمن - تكوين سياسة الوصول

3. إضافة اسم قاعدة



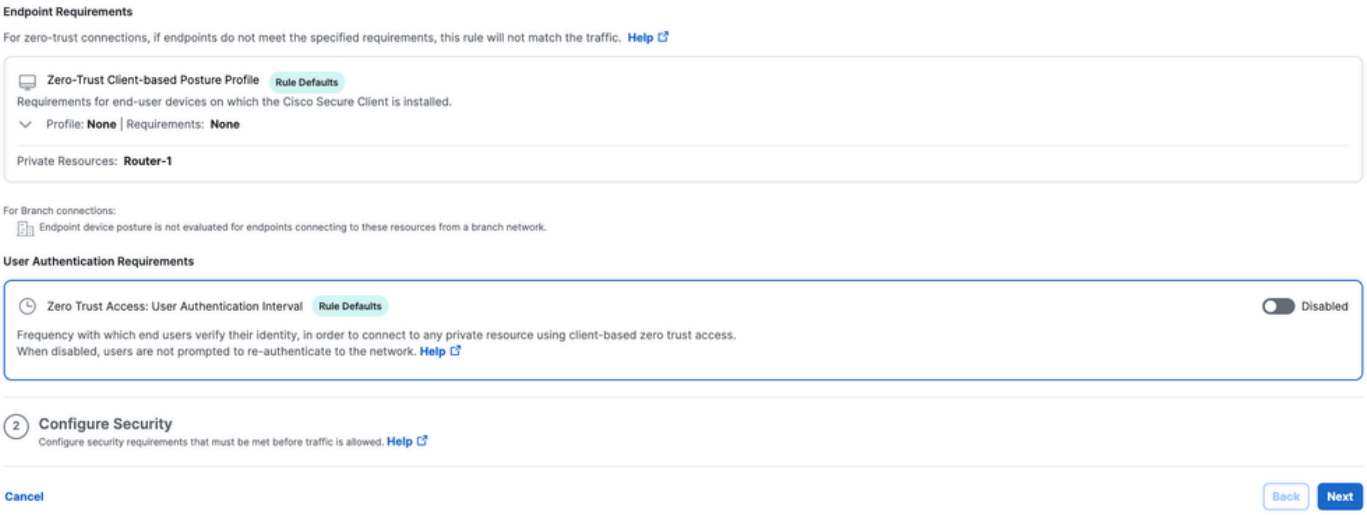
الوصول الآمن - تكوين سياسة الوصول

4. حدد إجراء القاعدة وحدد المصدر والوجهة



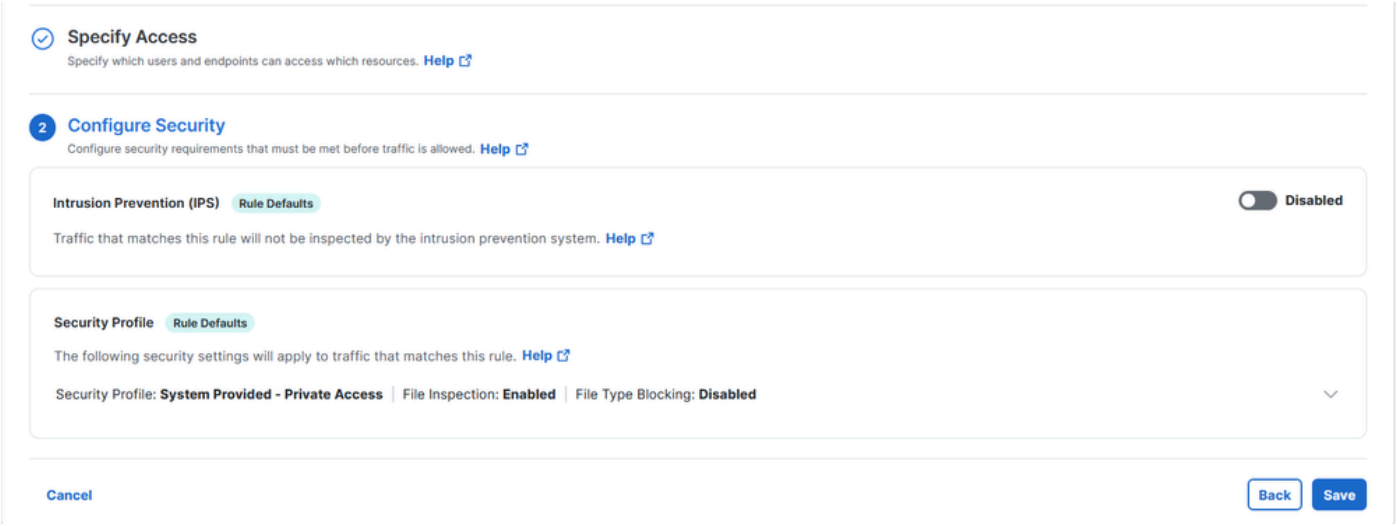
الوصول الآمن - تكوين سياسة الوصول

5. تكوين متطلبات نقطة النهاية



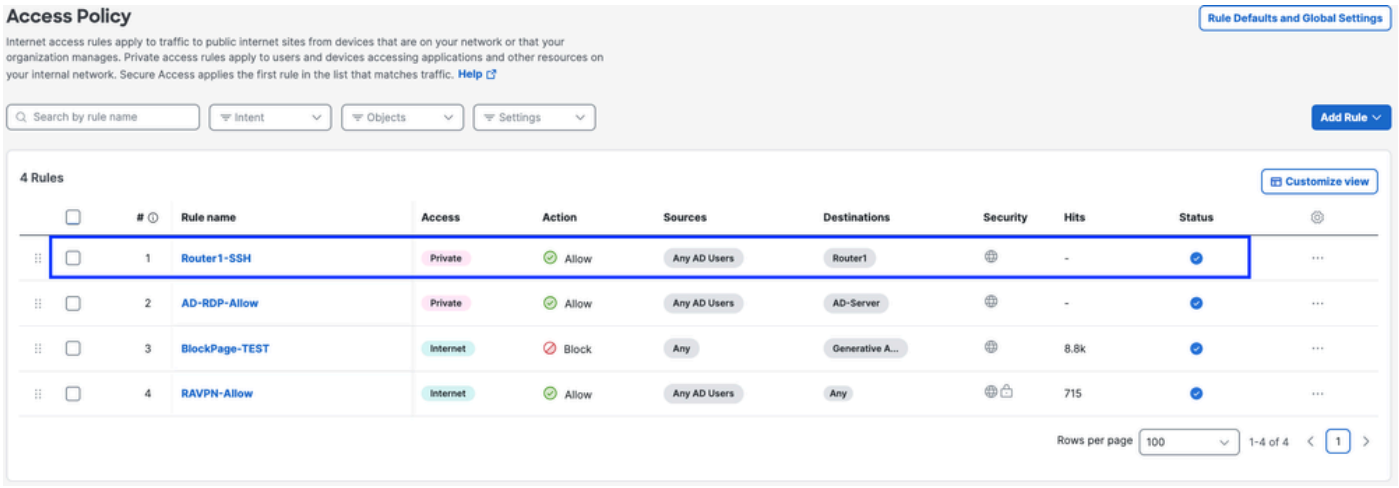
الوصول الآمن - تكوين سياسة الوصول

6. تكوين الأمان



الوصول الآمن - تكوين سياسة الوصول

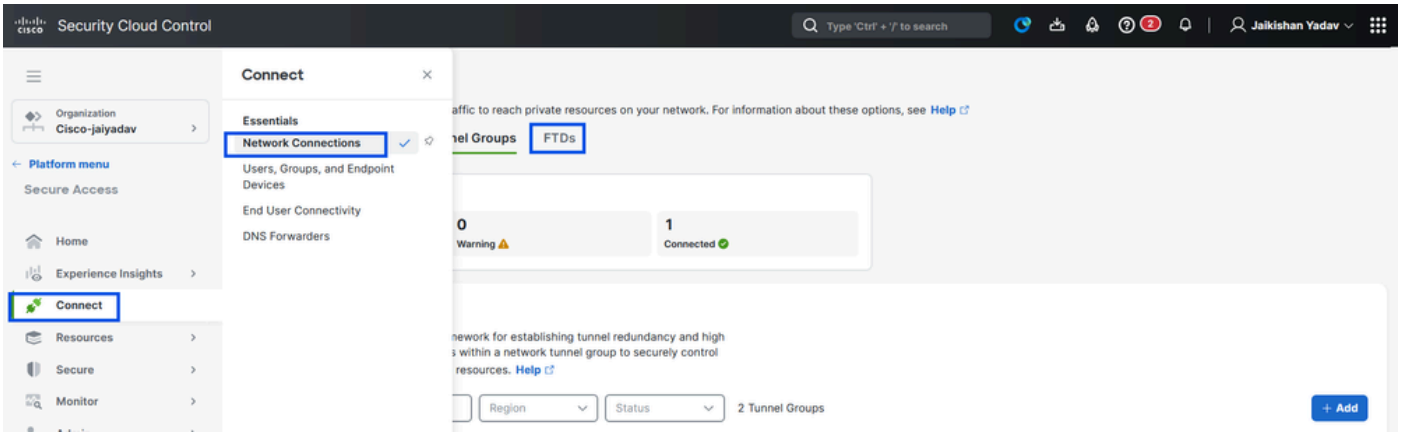
7. انقر فوق حفظ



الوصول الآمن - تكوين سياسة الوصول

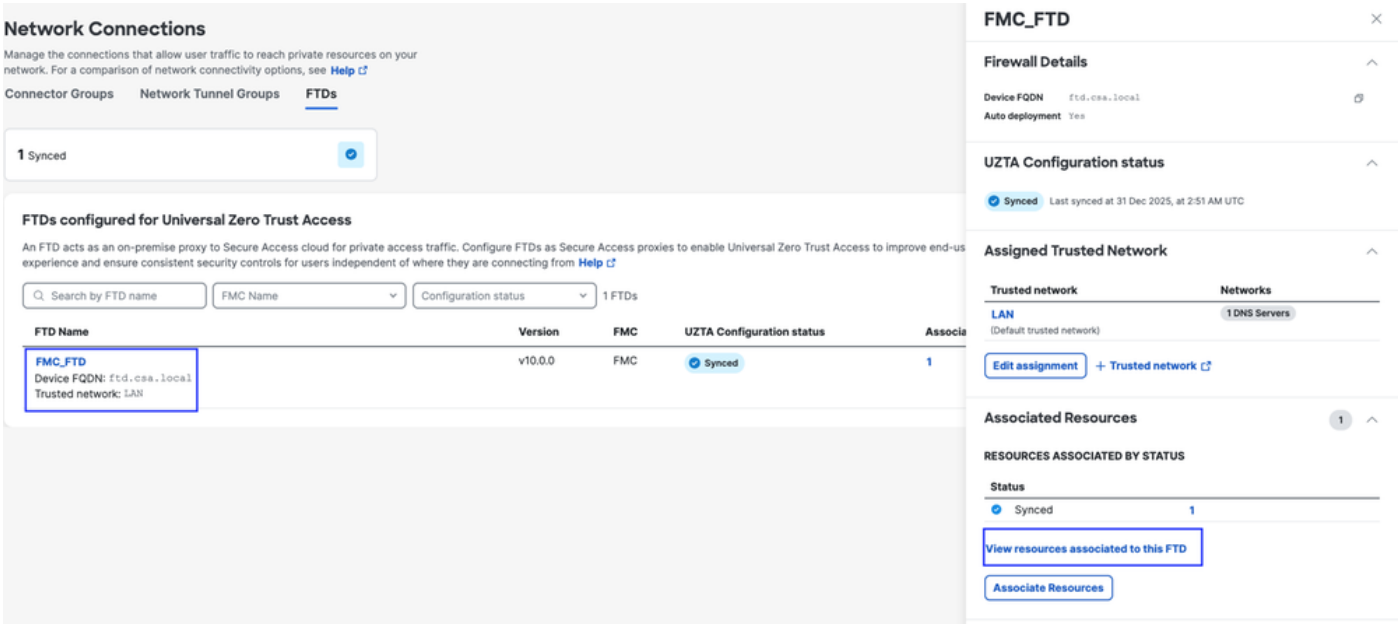
الخطوة 3 - التحقق من اقتران العلاقات العامة على FTD

1. انتقل إلى اتصال > إتصالات الشبكة > FTDs



الوصول الآمن - التحقق من العلاقات العامة

2. انقر فوق FTD > عرض الموارد المقترنة ب FTD هذا



الوصول الآمن - التحقق من العلاقات العامة

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 | 1 Resources | Associate Resources

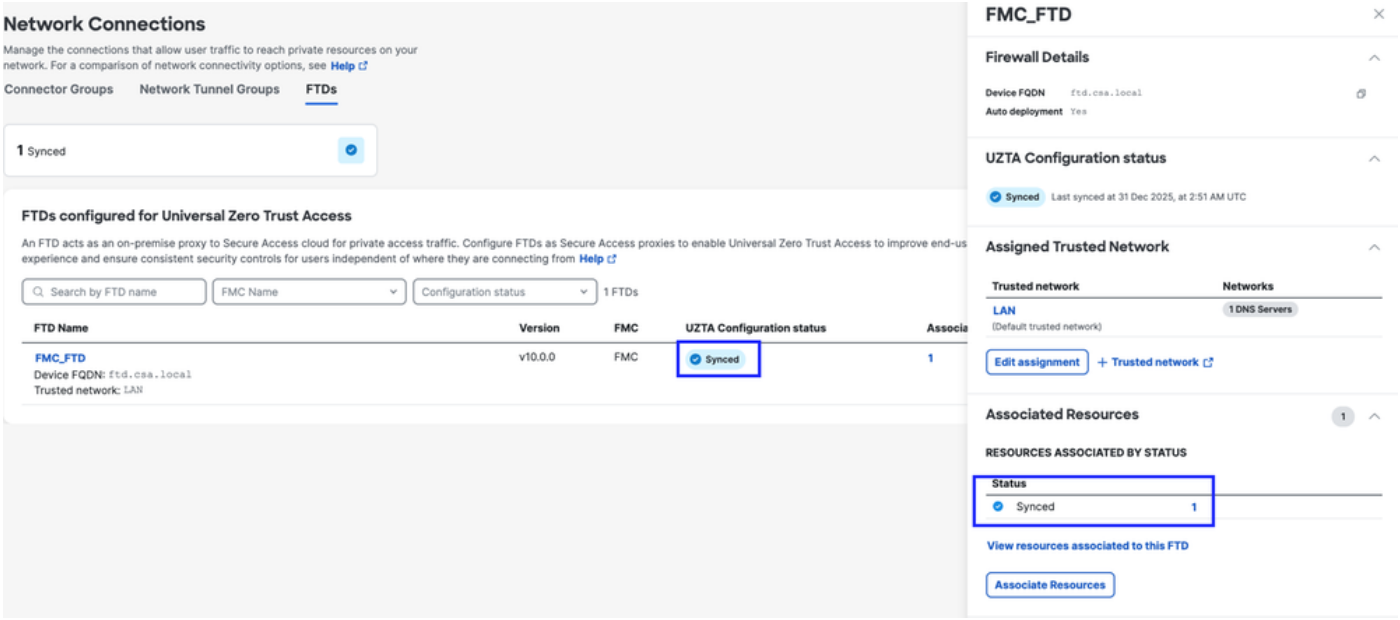
Resource name	Status
Router1	Synced

Close

الوصول الآمن - التحقق من العلاقات العامة

3. انقر فوق إغلاق

4. تحقق من الحالة ومن أنه يجب أن يكون المورد المقترن والتكوين في حالة المزامنة



الوصول الآمن - التحقق من العلاقات العامة

5. تحقق من دفع التكوين إلى FTD

قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة ب FTD وانتقل إلى وضع LINA

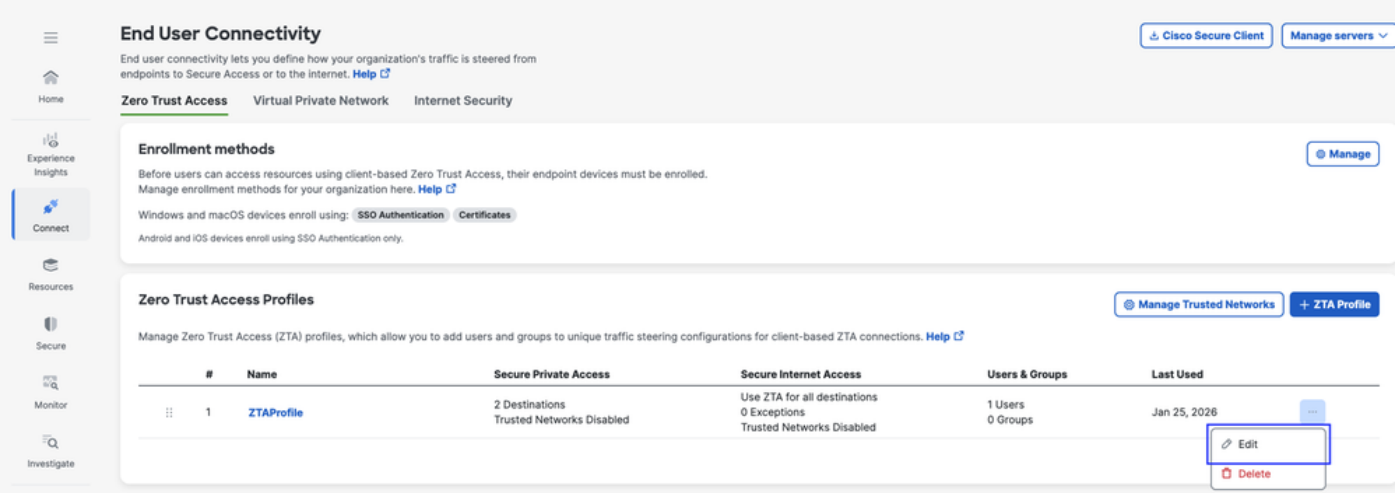
show running-config object application

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

FTD - التحقق من العلاقات العامة

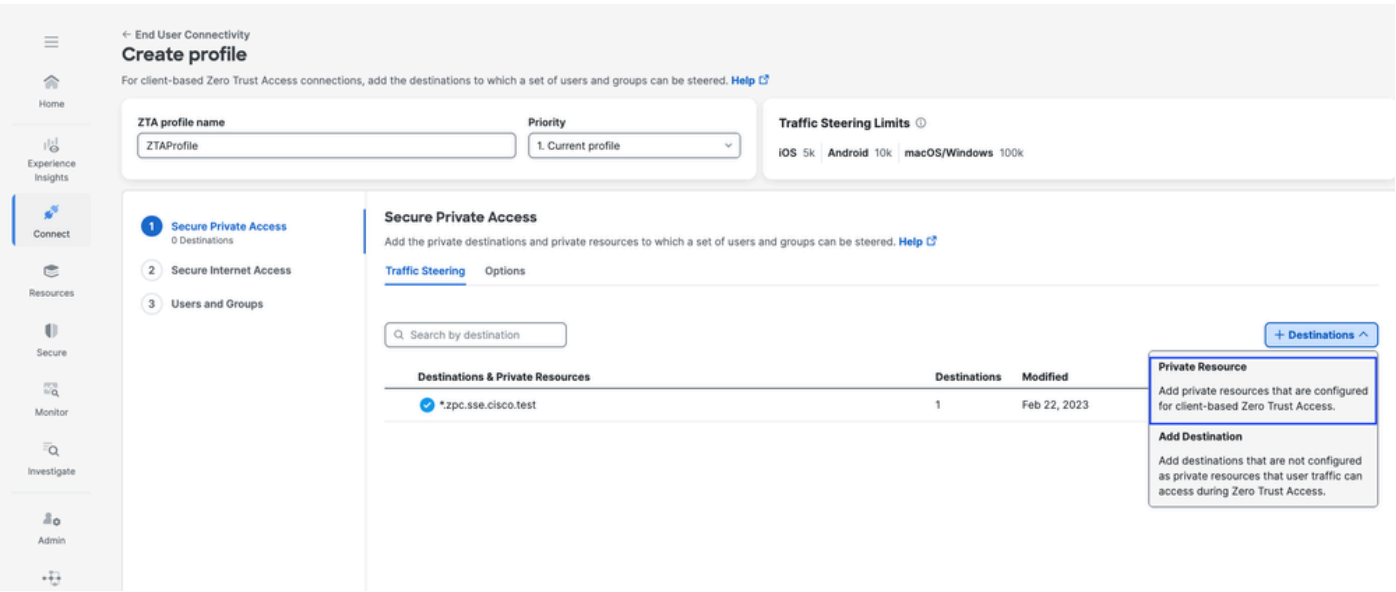
الخطوة - 4 إضافة مورد خاص إلى ملف تعريف ZTA

1. انتقل إلى الاتصال > اتصال المستخدم النهائي > الوصول إلى انعدام الثقة وانقر فوق 3 نقاط لتحرير ملف تعريف ZTA

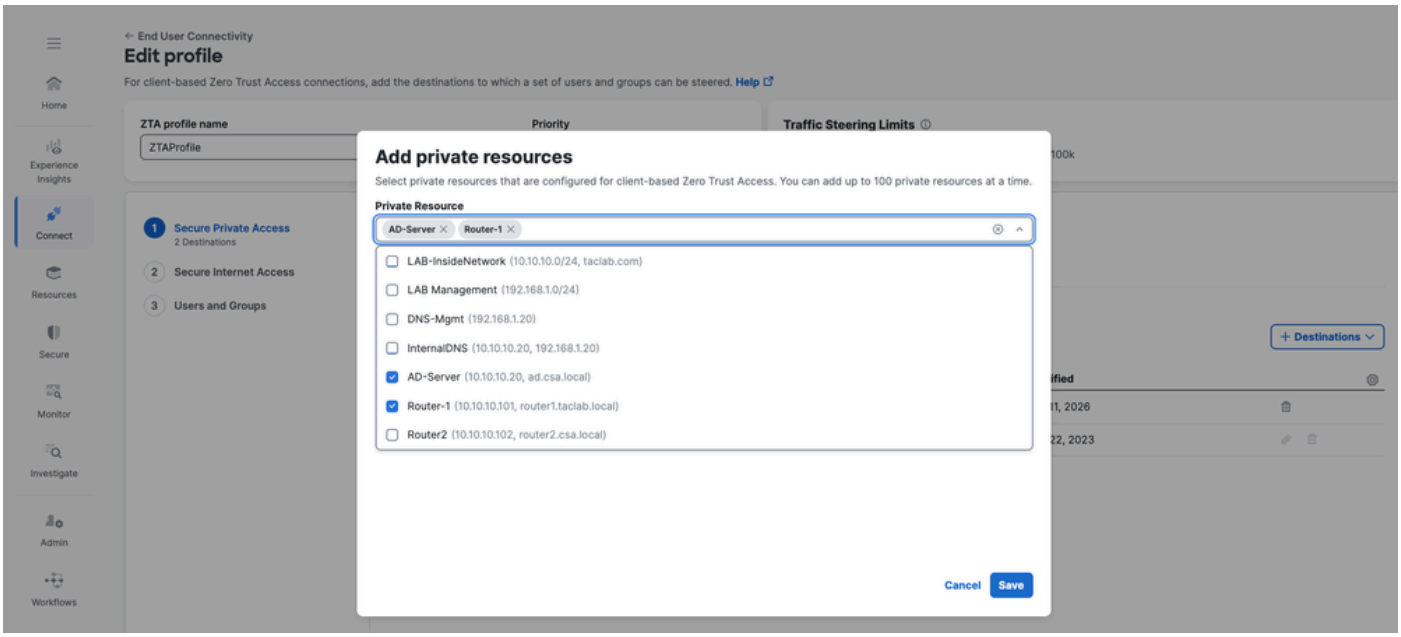


الوصول الآمن - ملف تعريف ZTA

2. إضافة المورد الخاص

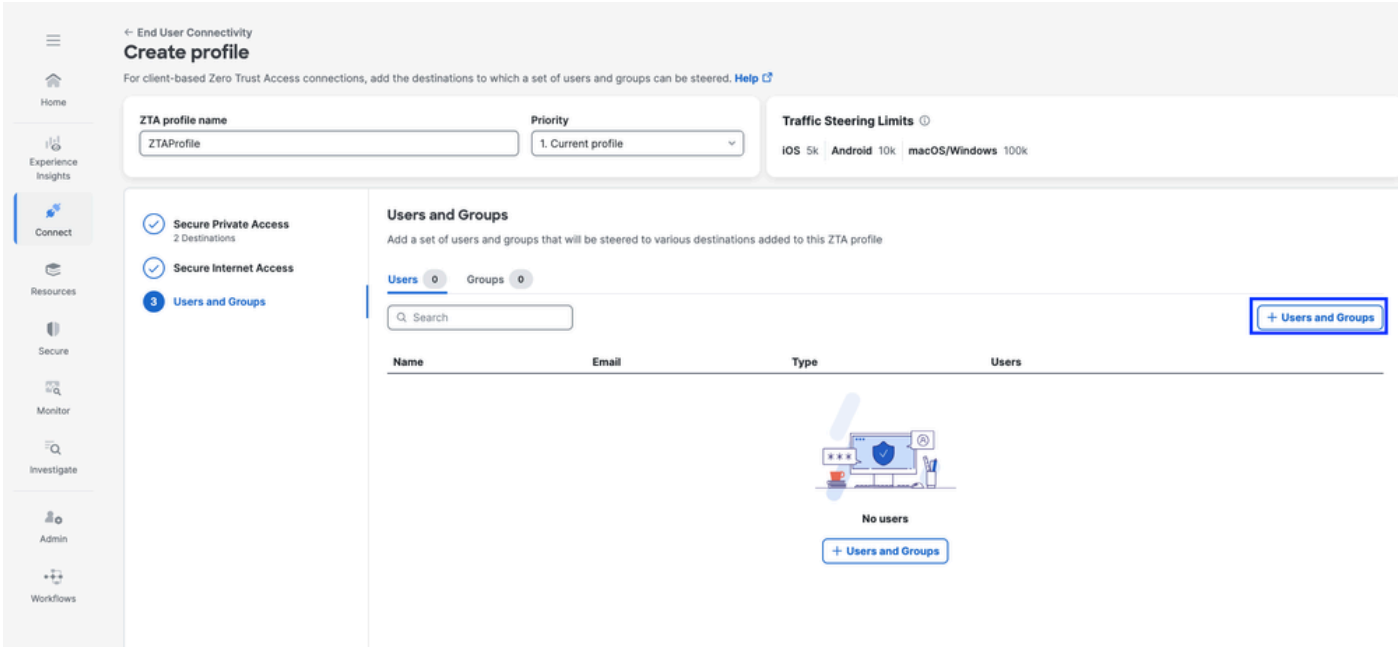


الوصول الآمن - ملف تعريف ZTA

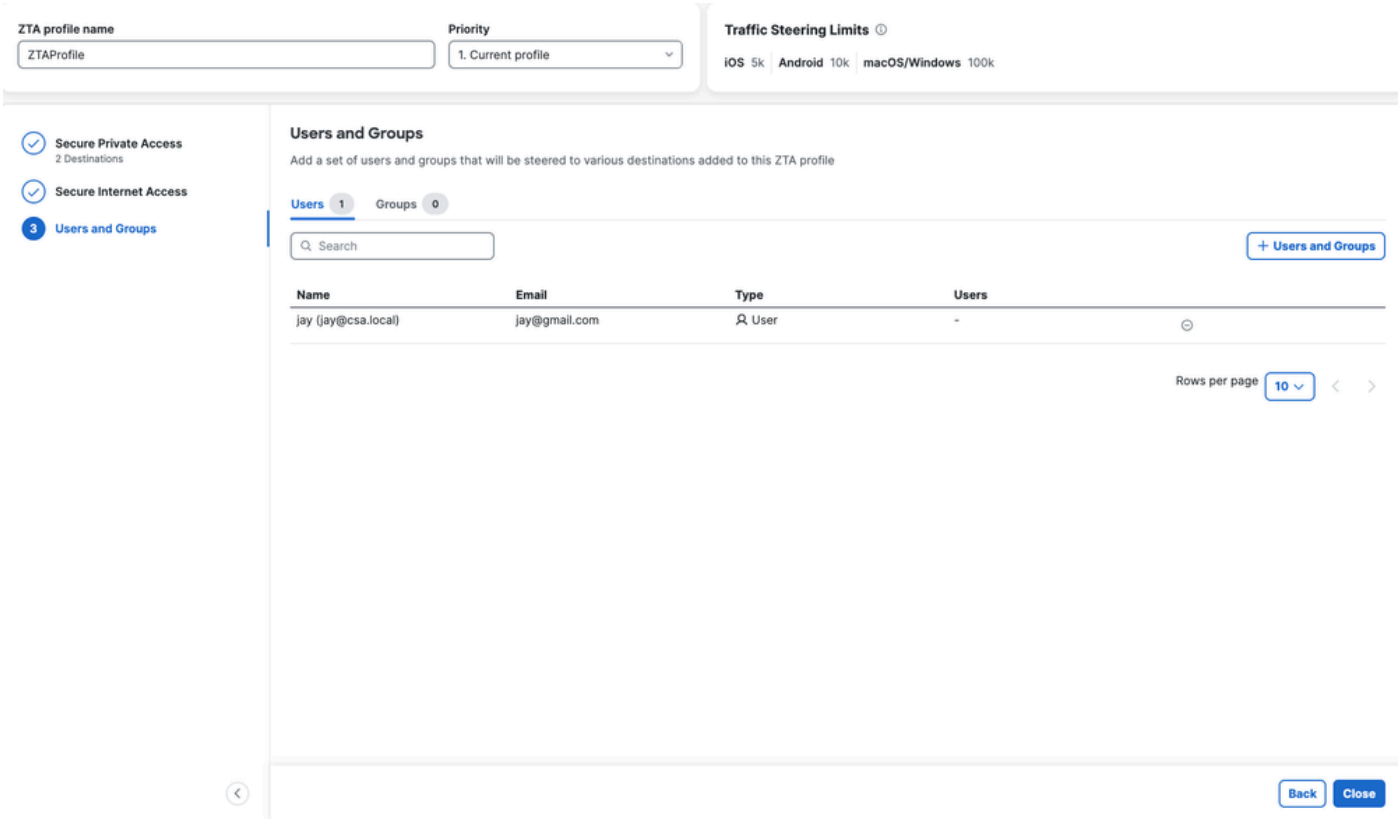


الوصول الآمن - ملف تعريف ZTA

3. إضافة مستخدمين ومجموعات



الوصول الآمن - ملف تعريف ZTA



ZTA ملف تعريف - الوصول الآمن

الخطوة 5 - التحقق من الوصول إلى المورد الخاص

1. التحقق من قدرة المستخدم البعيد على حل FTD FQDN

```
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
```

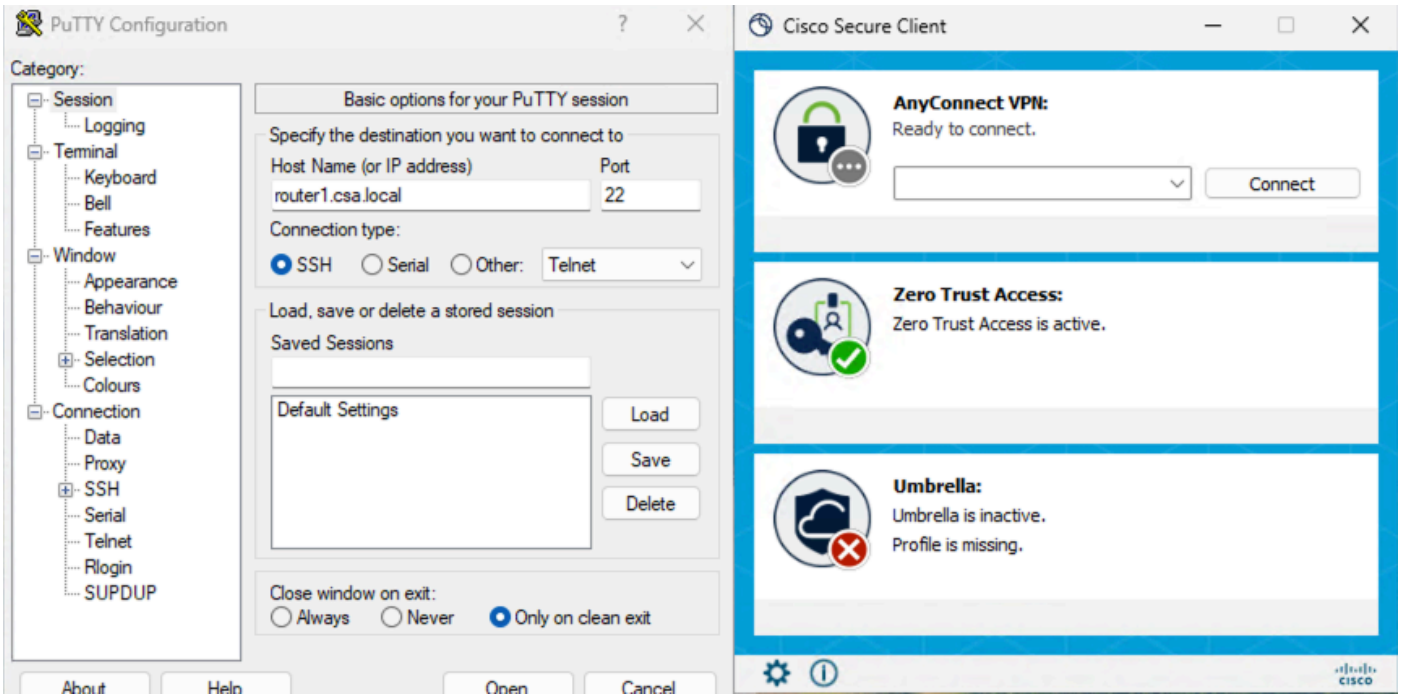
2. التحقق من إمكانية وصول FTD إلى الموارد الخاصة باستخدام FQDN

```
ftd> en
Password:
ftd# ping router1.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ftd#
```

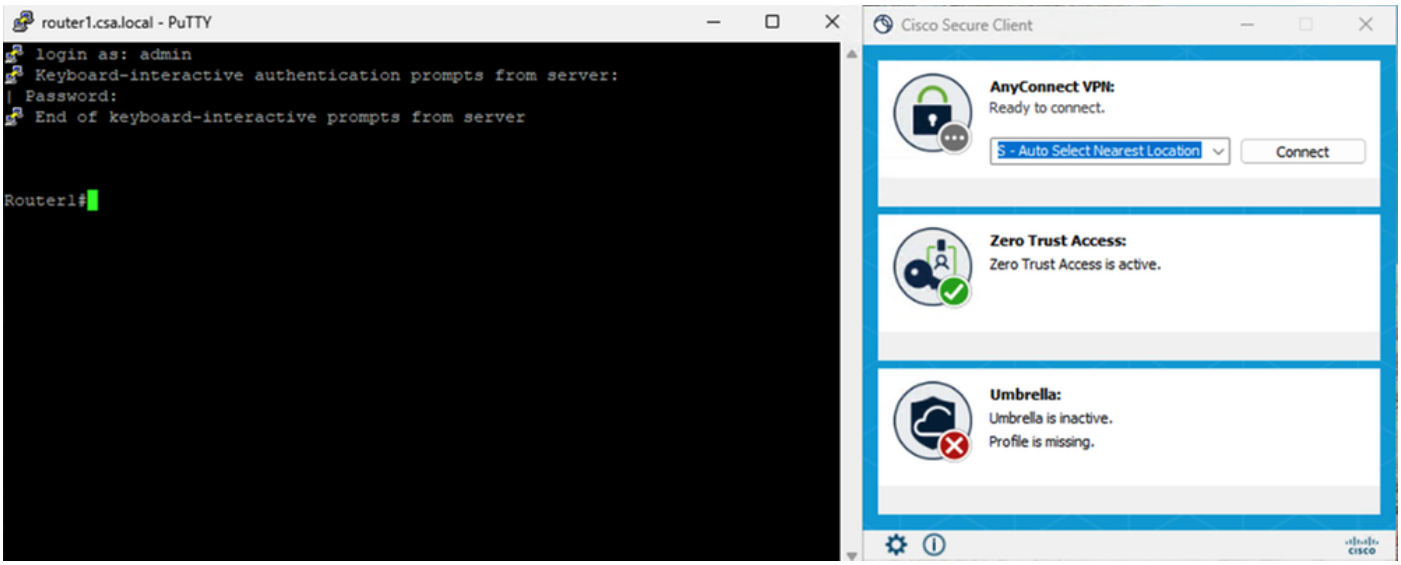
الوصول الآمن - إختبار العلاقات العامة

3. إختبار اتصال SSH بالمورد الخاص

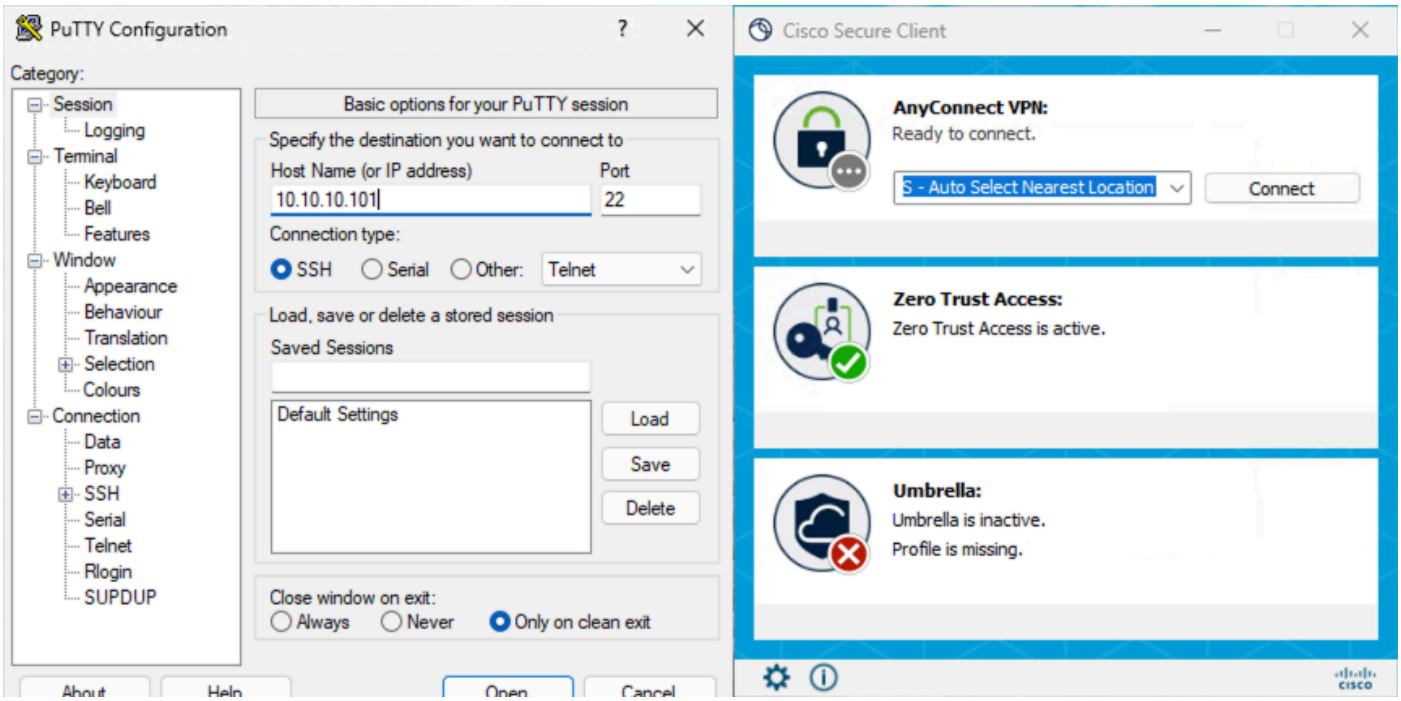
الوصول إلى PR باستخدام FQDN

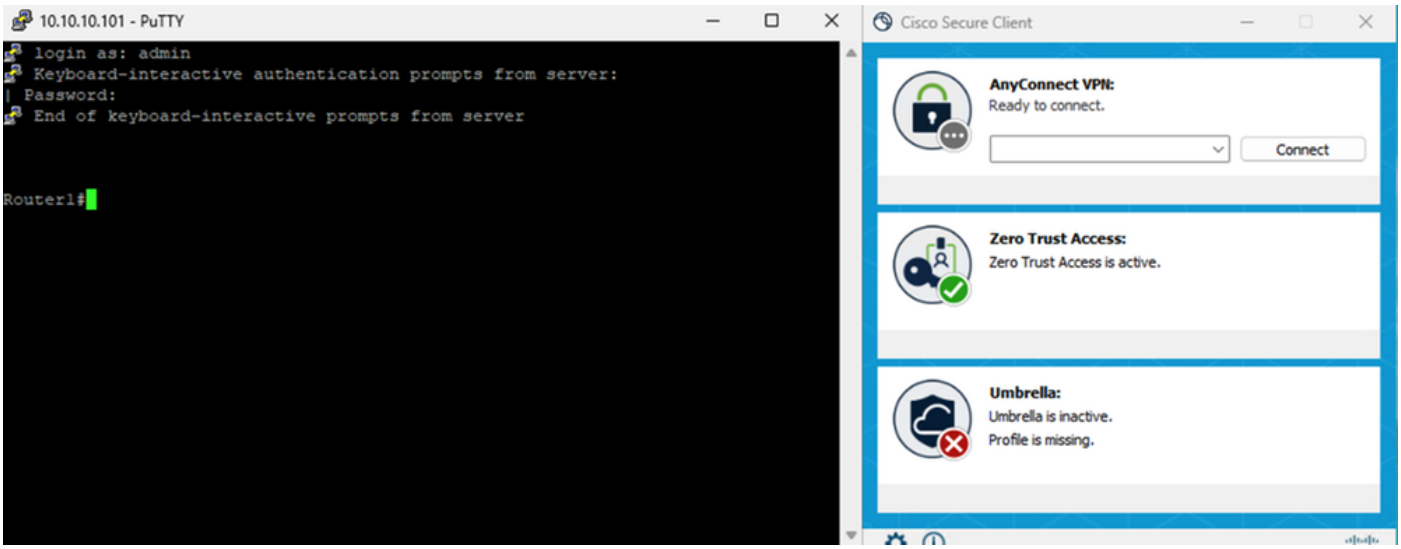


الوصول الآمن - إختبار العلاقات العامة



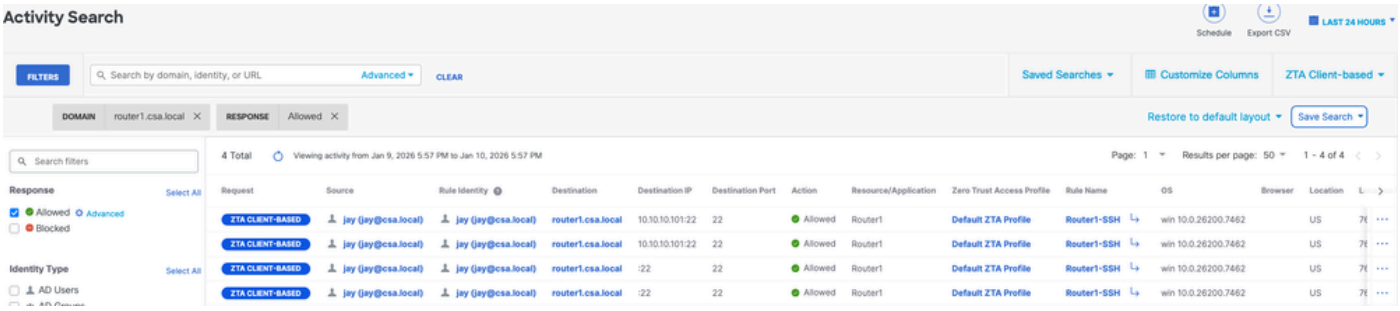
الوصول إلى PR باستخدام عنوان IP



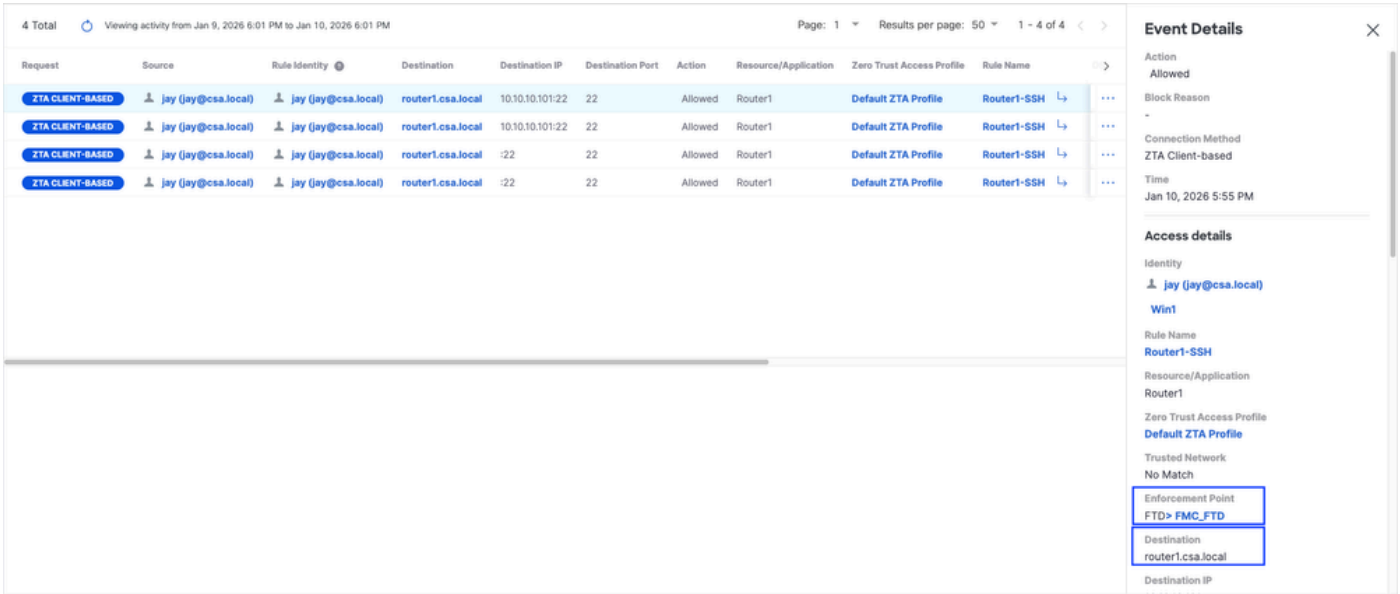


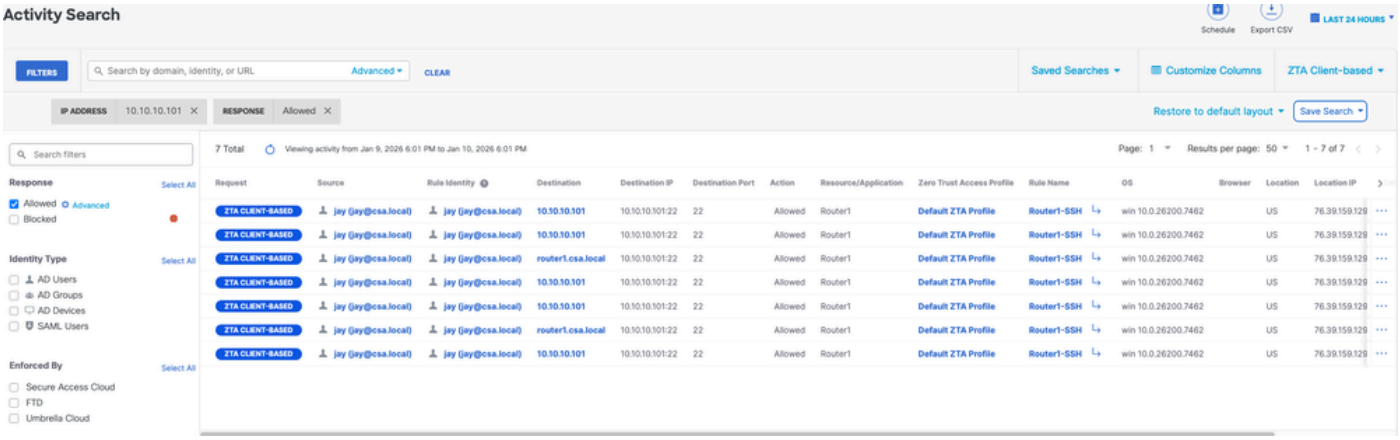
الوصول الآمن - إختبار العلاقات العامة

4. التحقق من سجلات البحث عن نشاط الوصول الآمن

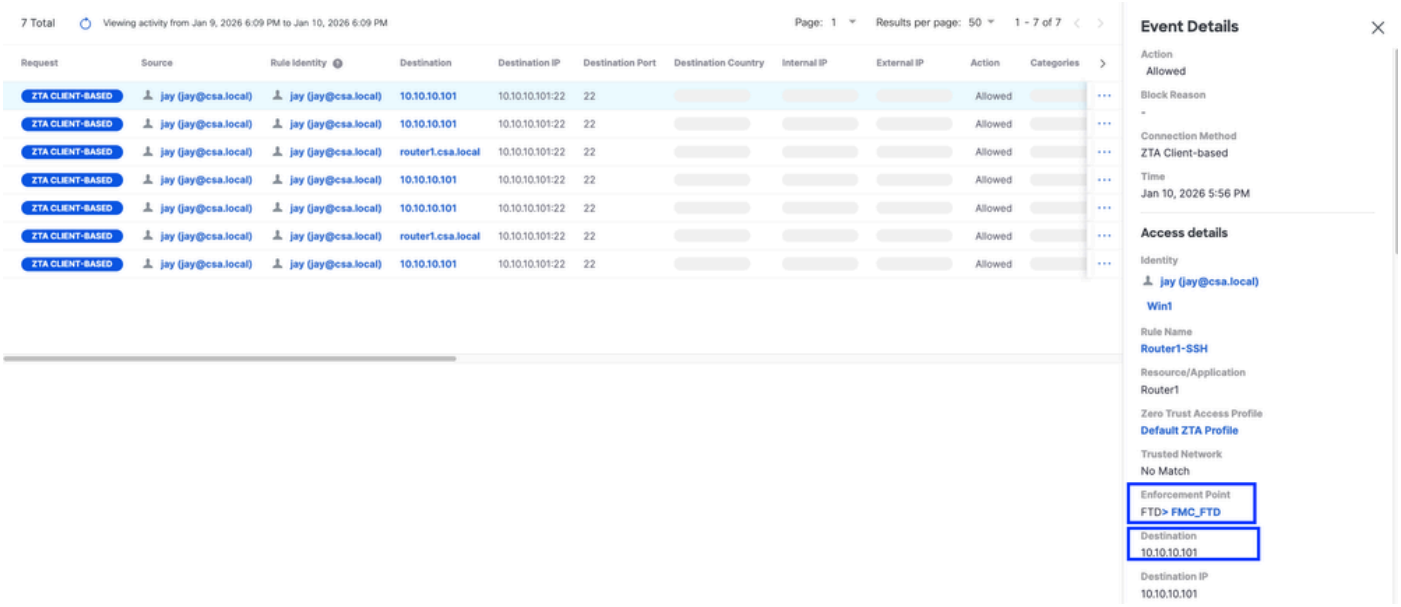


الوصول الآمن - البحث عن الأنشطة



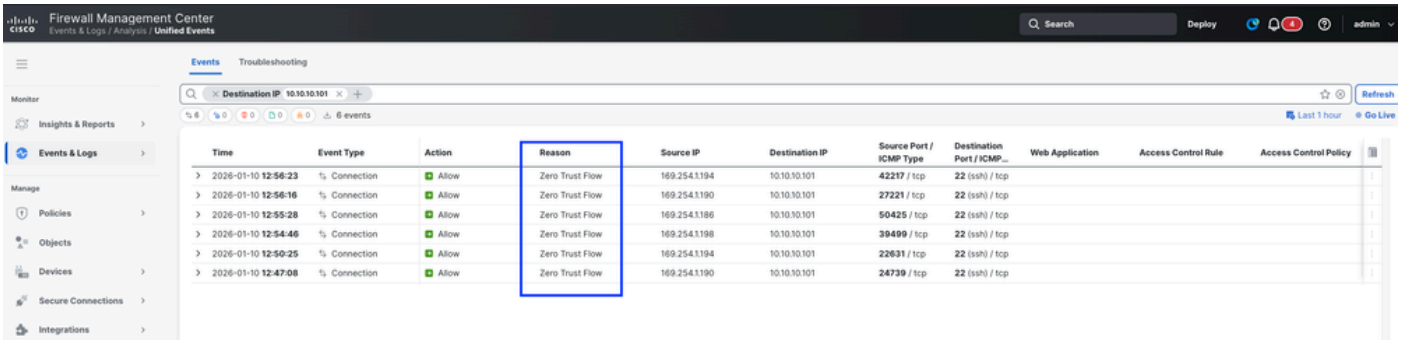


الوصول الآمن - البحث عن الأنشطة



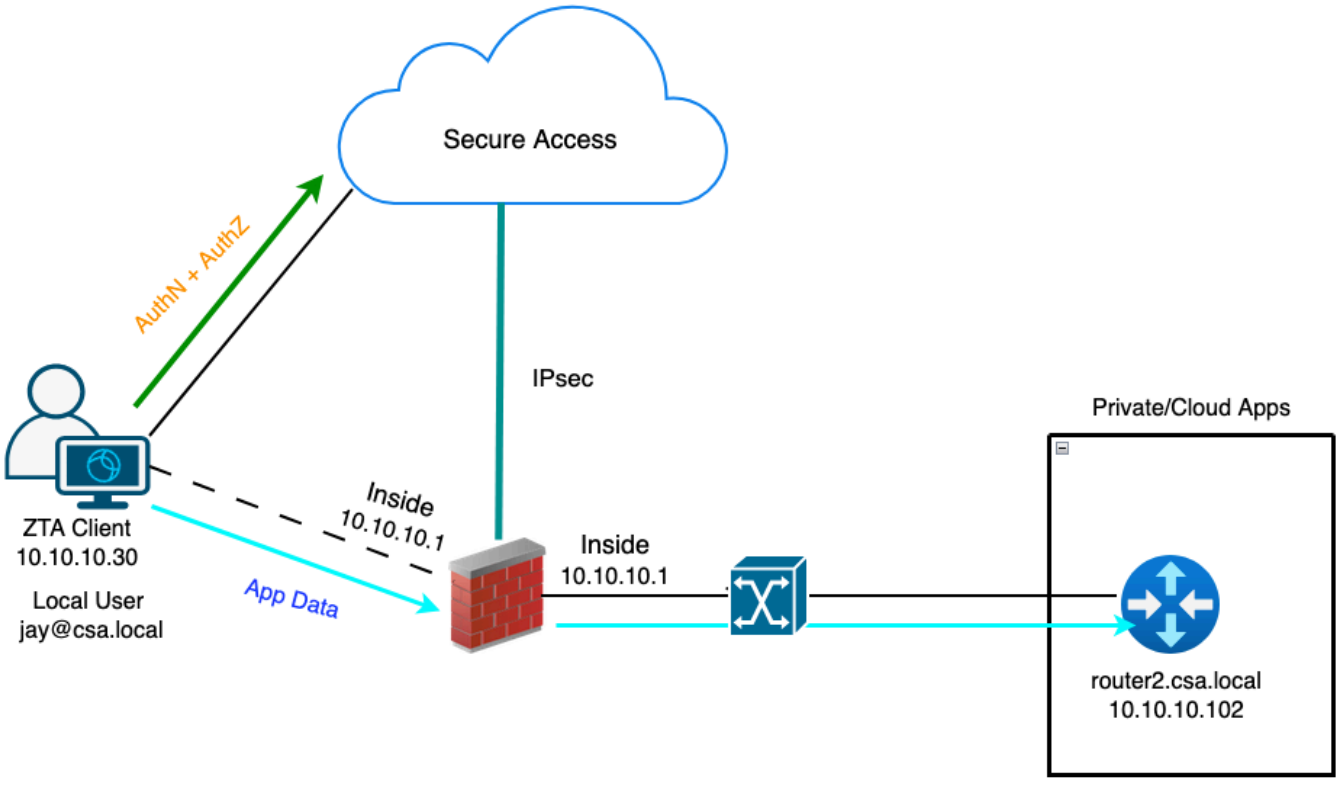
الوصول الآمن - البحث عن الأنشطة

5. التحقق من أحداث اتصال FMC



إختبار الحالة 3 - مستخدم محلي - تنفيذ محلي

الوصول إلى مورد خاص من خلال التطبيق المحلي كمستخدم محلي، في هذا النوع من تقييم سياسة الإنفاذ يتم على Secure Access ولكن تبقى بيانات التطبيق محلية على FTD. على سبيل المثال، عميل أو مستخدم مسجل في ZTA متصل بشبكة منزلية ويحاول الوصول إلى مورد خاص موجود خلف FTD داخل الواجهة . إذا كان المورد الخاص خلف DMZ أو أي واجهة أخرى ل FTD، فسيتعين علينا إنشاء قاعدة وصول على FTD للسماح بحركة المرور بين Private Resource و الشبكة أو Client IP.

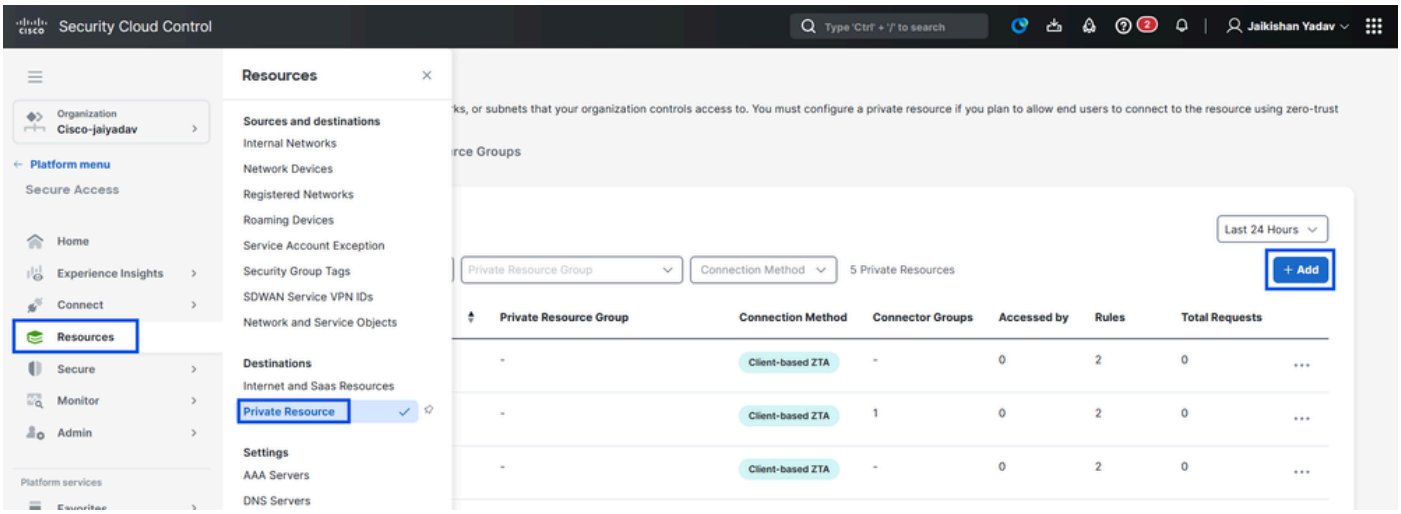


ZTA العالمي - طوبولوجيا حالة الاختبار

الخطوة 1 - تحديد مورد خاص على الوصول الآمن

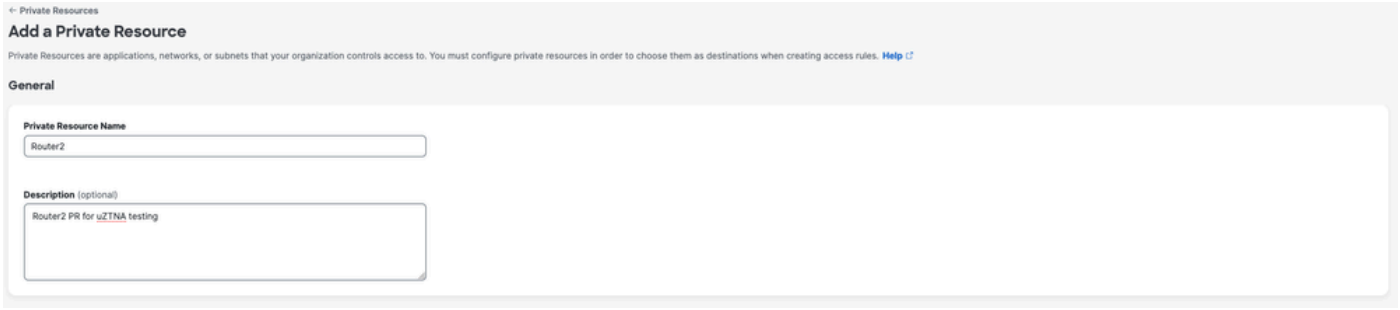
تكوين مورد خاص ليتم الوصول إليه عبر الجهاز المسجل في الوصول إلى عدم الثقة (ZTA) باستخدام فرض السحابة

1. انتقل إلى الموارد > الوجهات > الموارد الخاصة > انقر فوق +إضافة



الوصول الآمن - تكوين الموارد الخاصة

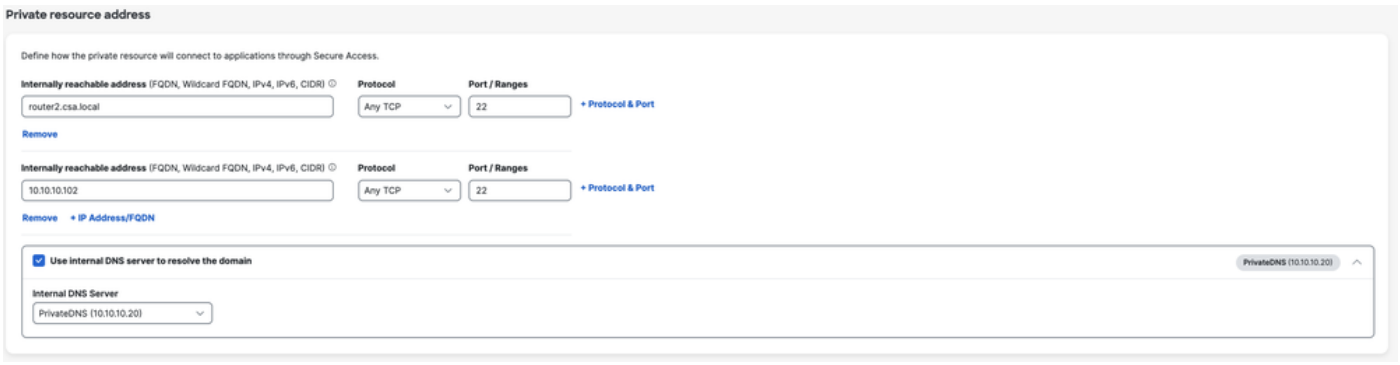
2. بالنسبة إلى اسم المورد الخاص، أدخل اسما ذا معنى للمورد. للحصول على الوصف، ونصي بتوفير معلومات مثل الغرض من المورد أو اسم مالك المورد.



الوصول الآمن - تكوين الموارد الخاصة

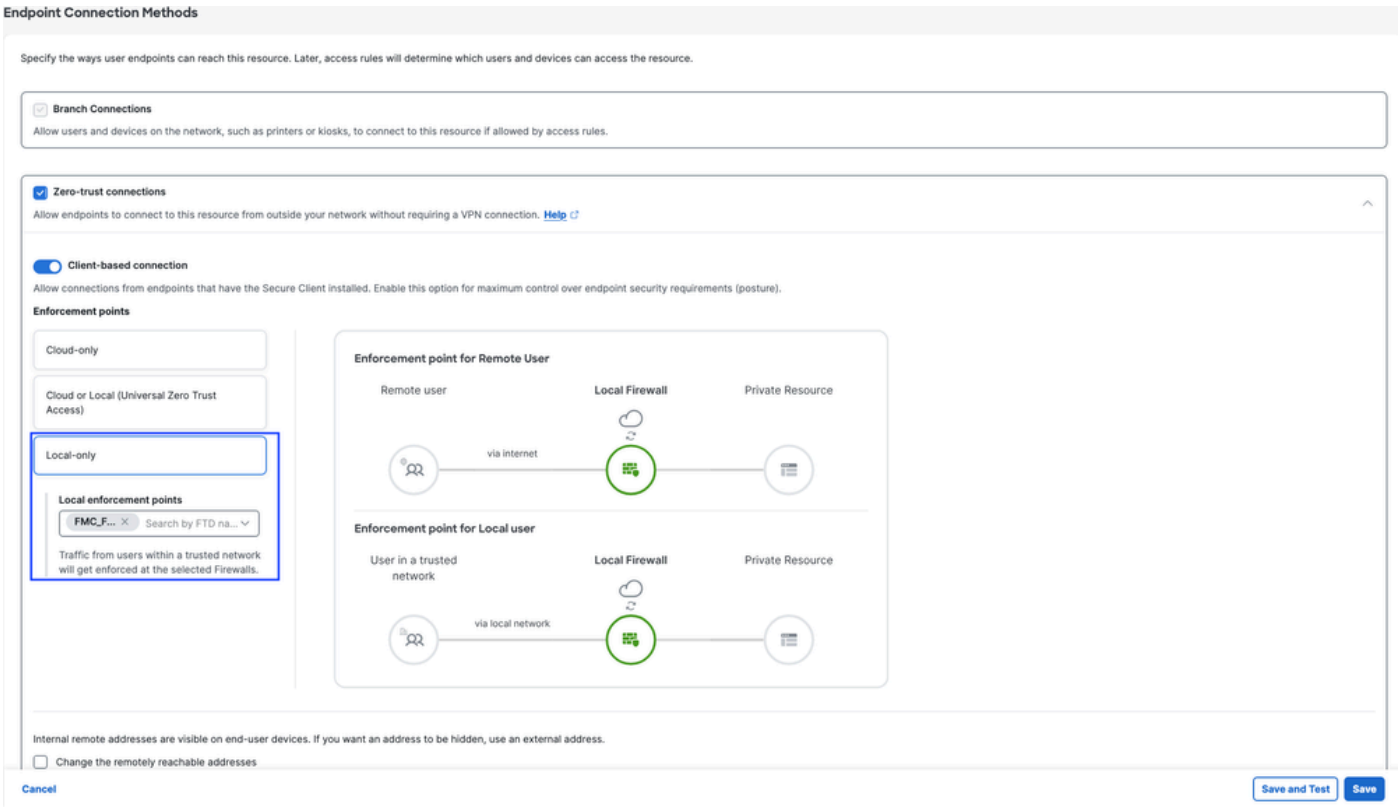
3. أدخل FQDN للمورد الخاص الذي تريد الوصول إليه . كما يمكنك تحديد عنوان IP الخاص بالمورد الخاص . لمزيد من المعلومات، راجع إضافة مورد خاص

4. حدد خادم DNS الداخلي لحل المجال



5. تحديد أسلوب اتصال نقطة النهاية

6. حدد FTD كنقاط تنفيذ محلية



الوصول الآمن - تكوين المواقع الخاصة

ملاحظة: اعتمادا على نوع التسجيل الذي تحدده ، سيقوم هذا التغيير بإقران PR وسيؤدي إلى تشغيل نشر النهج تلقائيا ب FTD

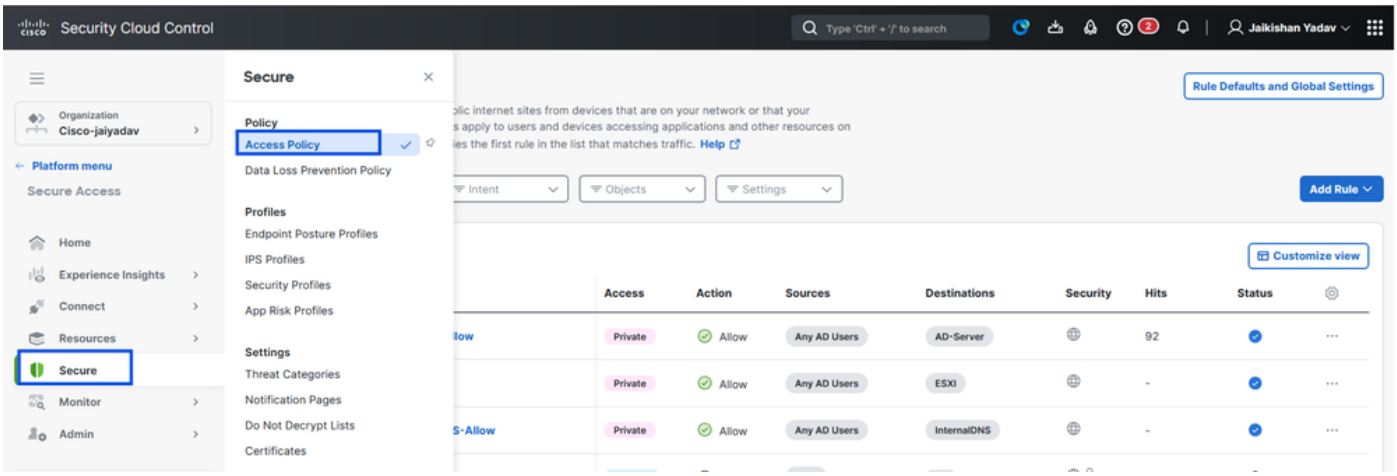
---

7. انقر فوق حفظ

الخطوة 2 - إنشاء قاعدة وصول خاصة

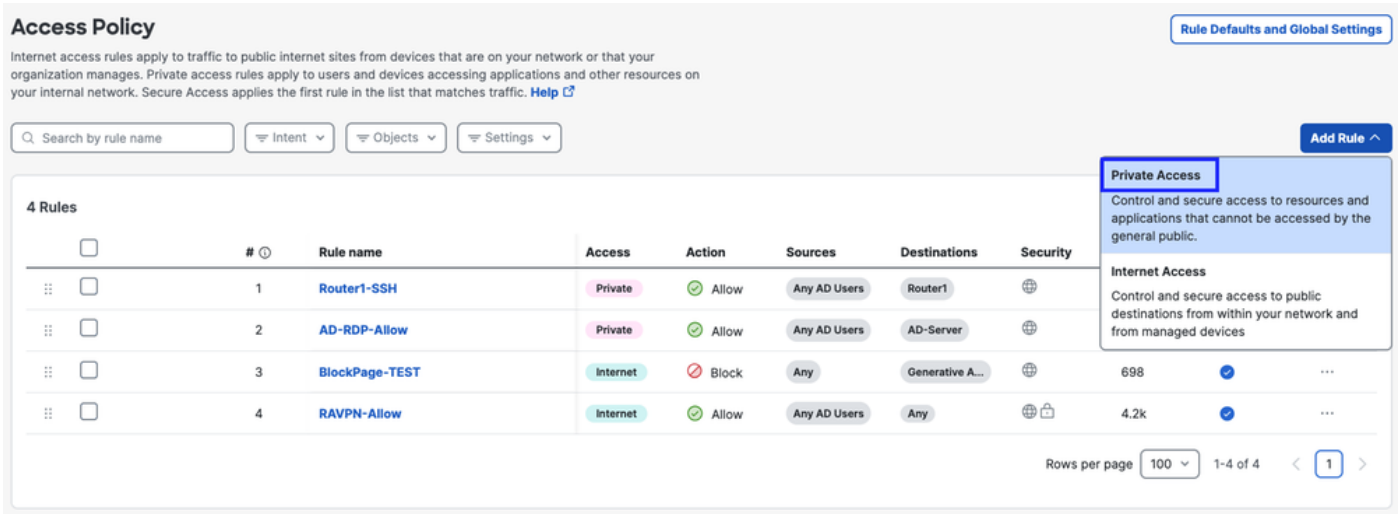
يتمكن المستخدمون المسجلون في ZTA العالمية من Secure Access تكوين وصول خاص على قاعدة الوصول الخاص. لمزيد من المعلومات، راجع قاعدة الوصول الخاص . من الوصول إليه

1. انتقل إلى آمن > نهج الوصول



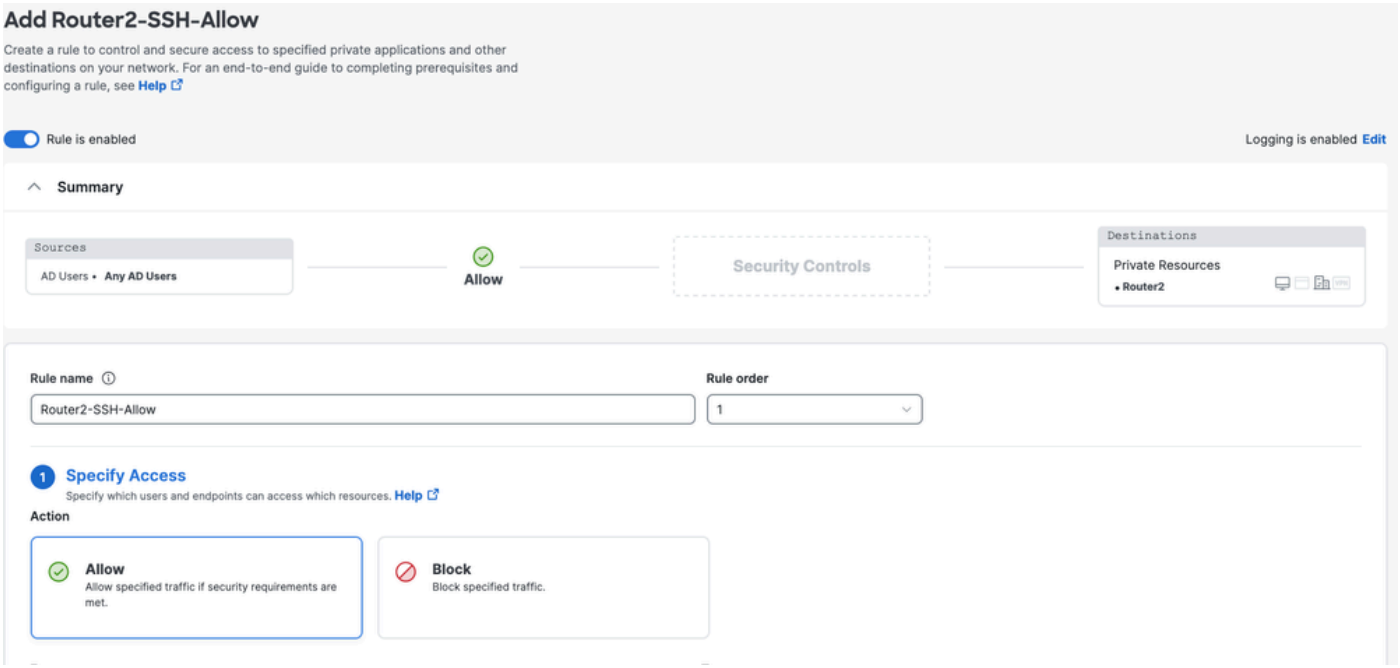
الوصول الآمن - تكوين سياسة الوصول

2. انقر فوق إضافة قاعدة، ثم أختر Private Access.
في أعلى القاعدة يوجد ملخص يصف المكونات المكونة للقاعدة الخاصة بك.



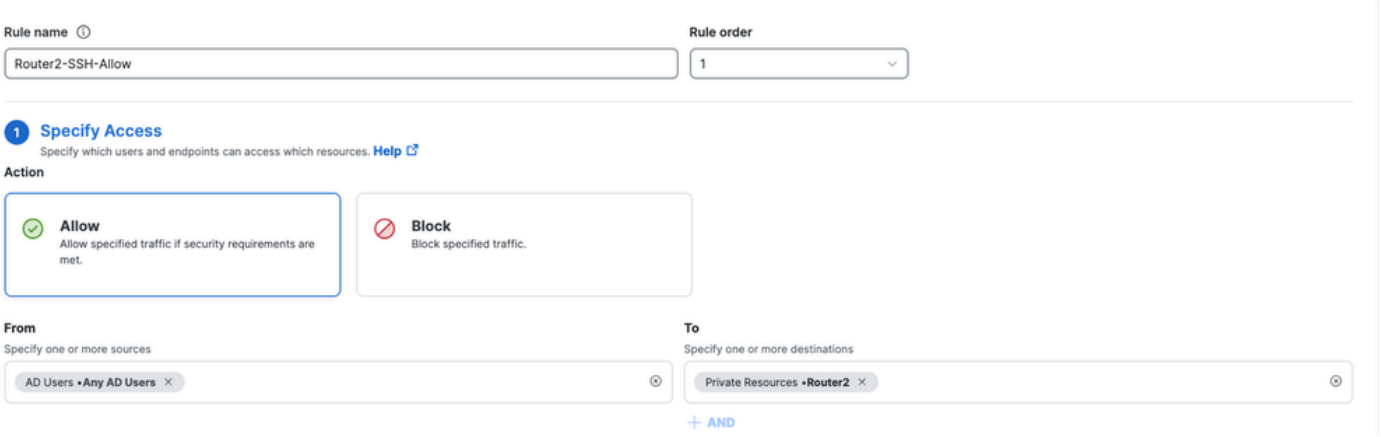
الوصول الآمن - تكوين سياسة الوصول

3. إضافة اسم قاعدة



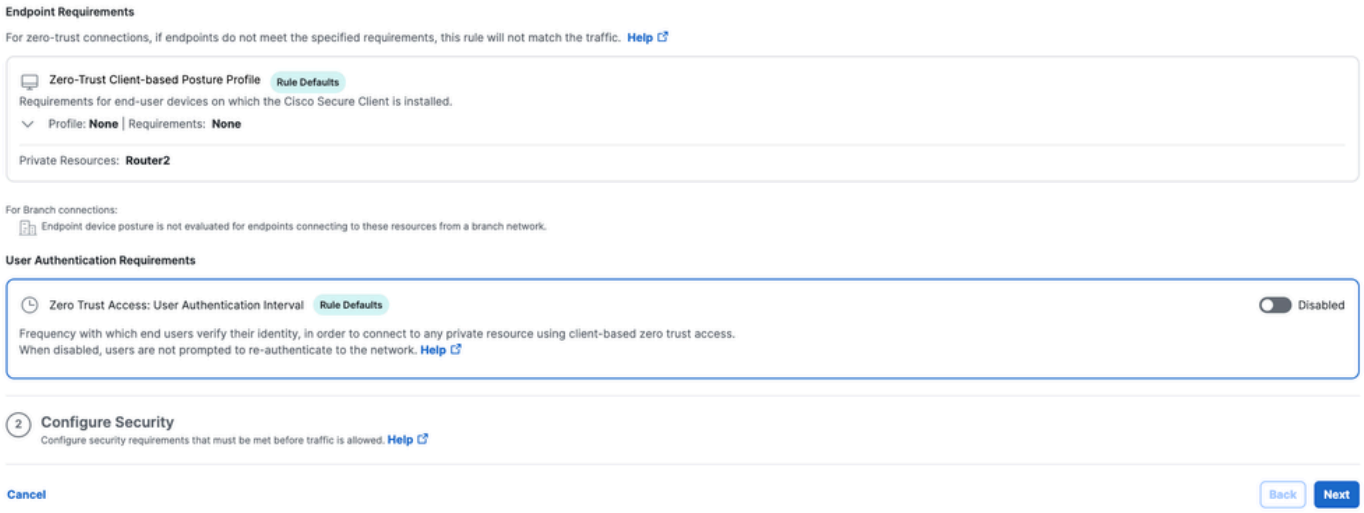
الوصول الآمن - تكوين سياسة الوصول

4. حدد إجراء القاعدة وحدد المصدر والوجهة



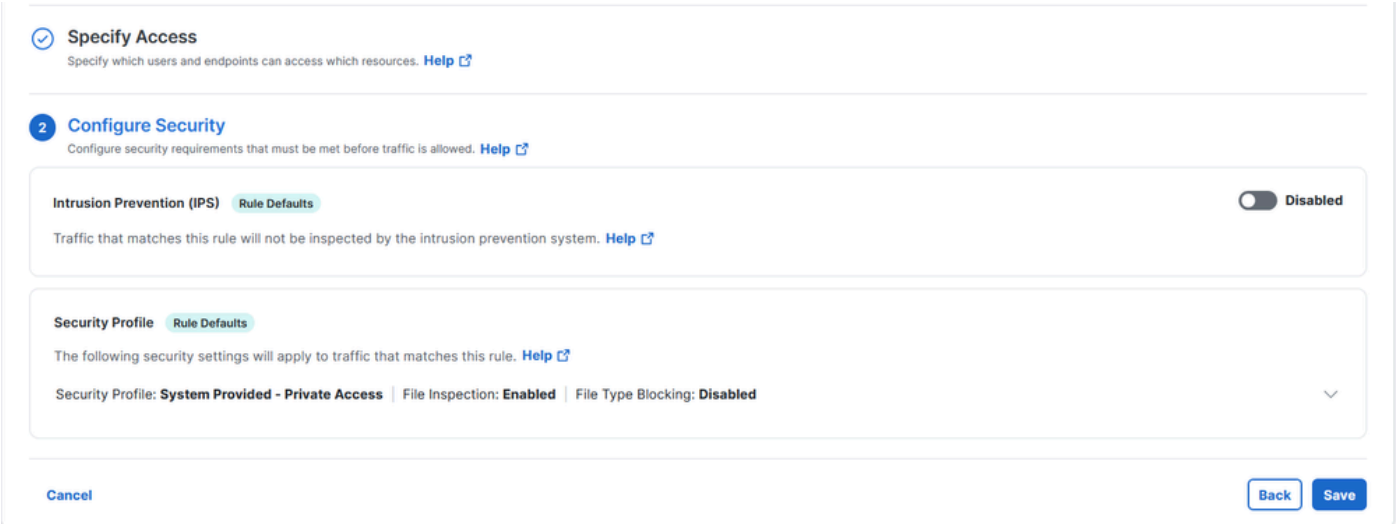
الوصول الآمن - تكوين سياسة الوصول

5. تكوين متطلبات نقطة النهاية



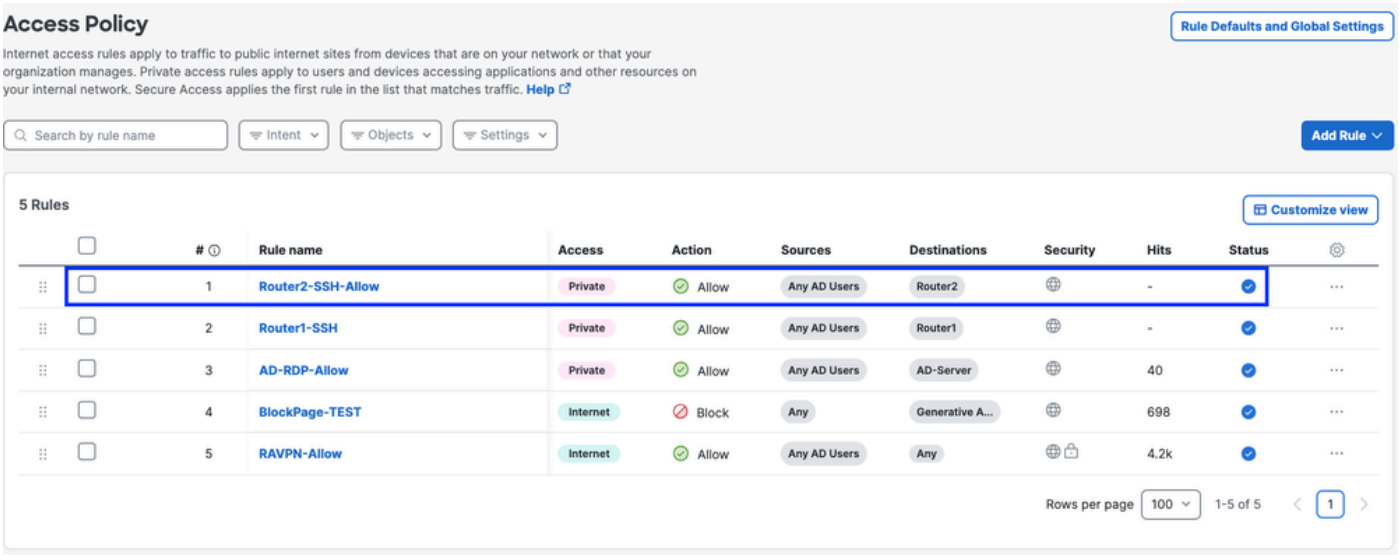
الوصول الآمن - تكوين سياسة الوصول

6. تكوين الأمان



الوصول الآمن - تكوين سياسة الوصول

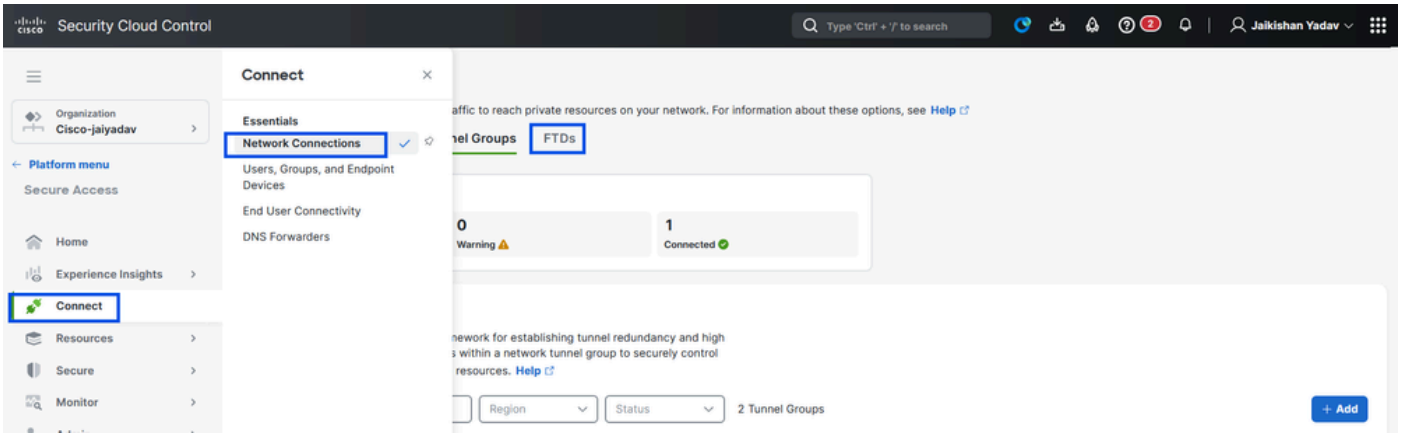
7. انقر فوق حفظ



الوصول الآمن - تكوين سياسة الوصول

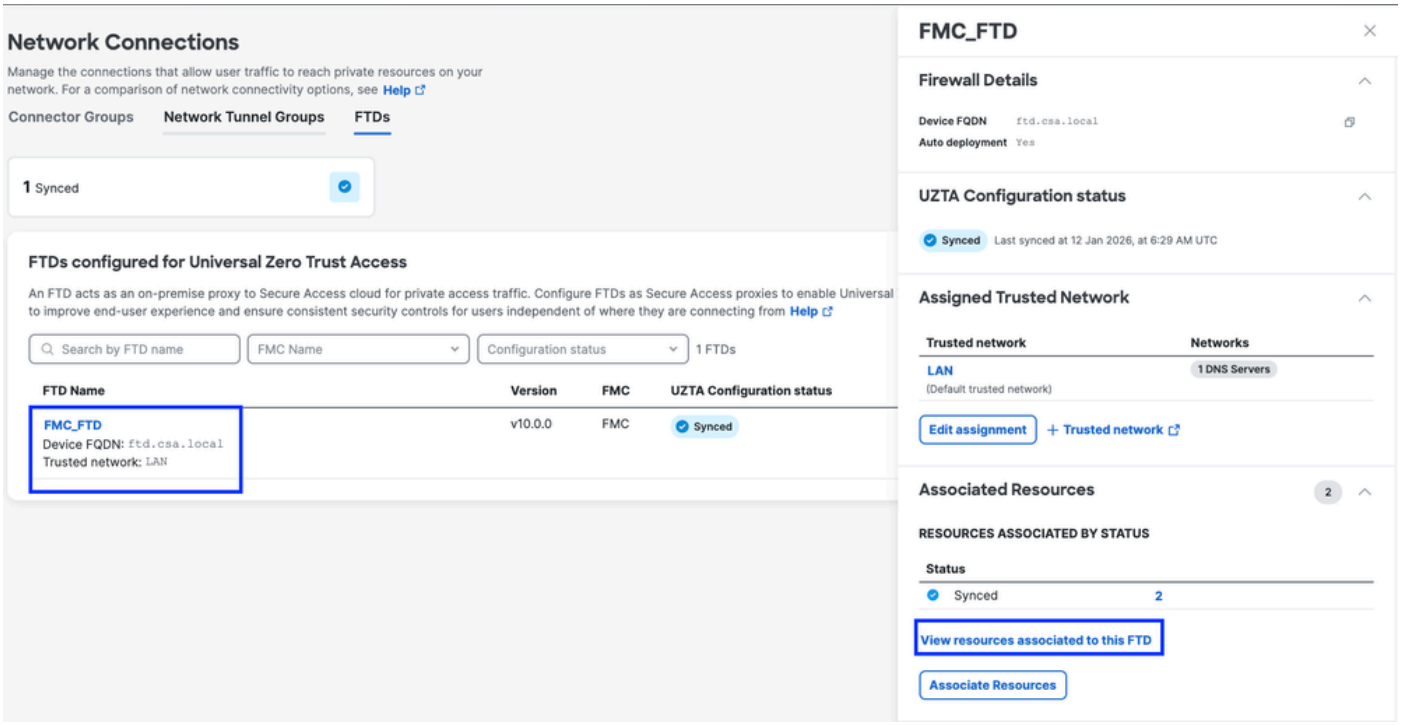
الخطوة 3 - التحقق من اقتران العلاقات العامة على FTD

1. انتقل للاتصال > إتصالات الشبكة > FTDs

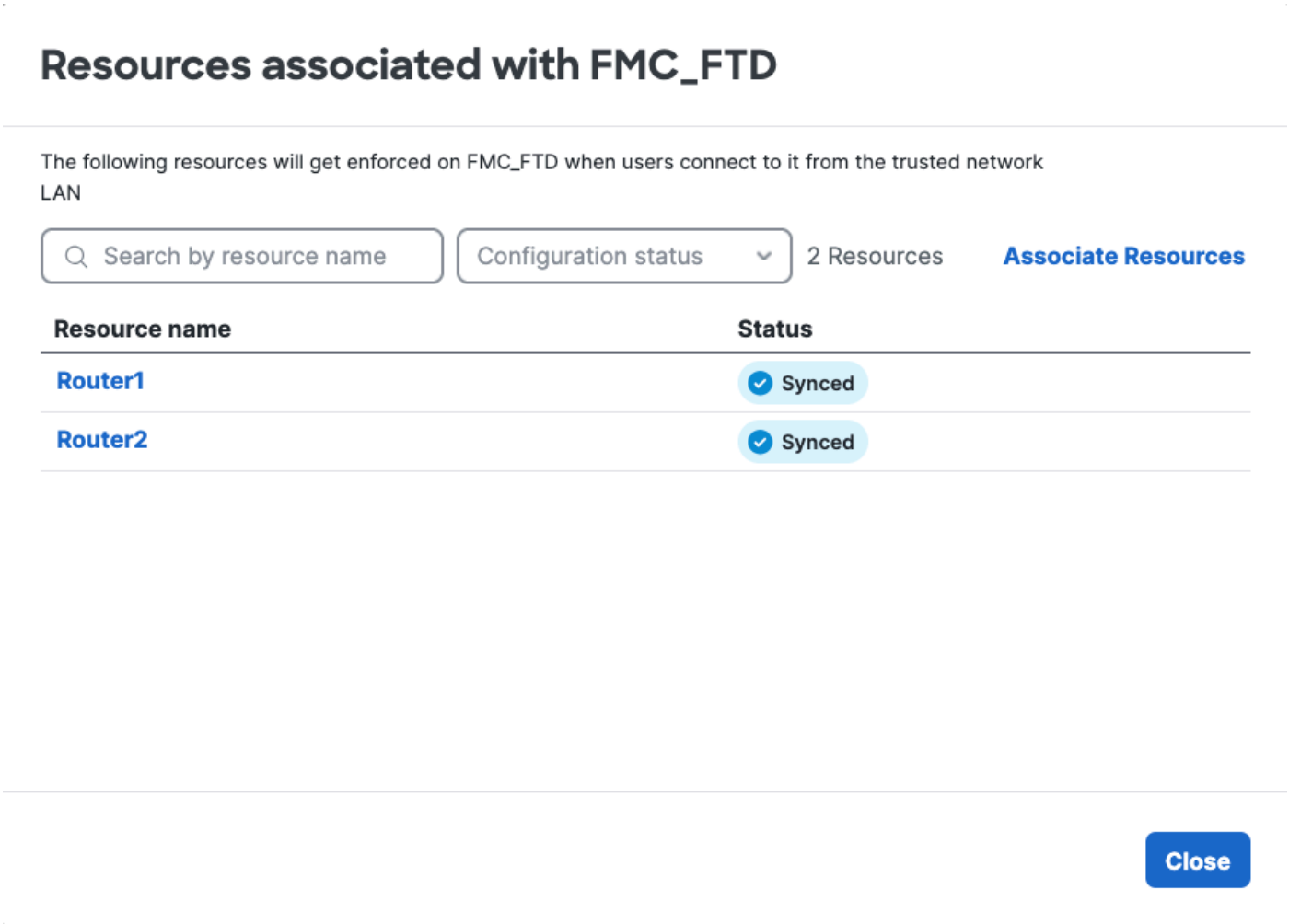


الوصول الآمن - التحقق من العلاقات العامة

2. انقر فوق FTD > عرض الموارد المقترنة ب FTD هذا

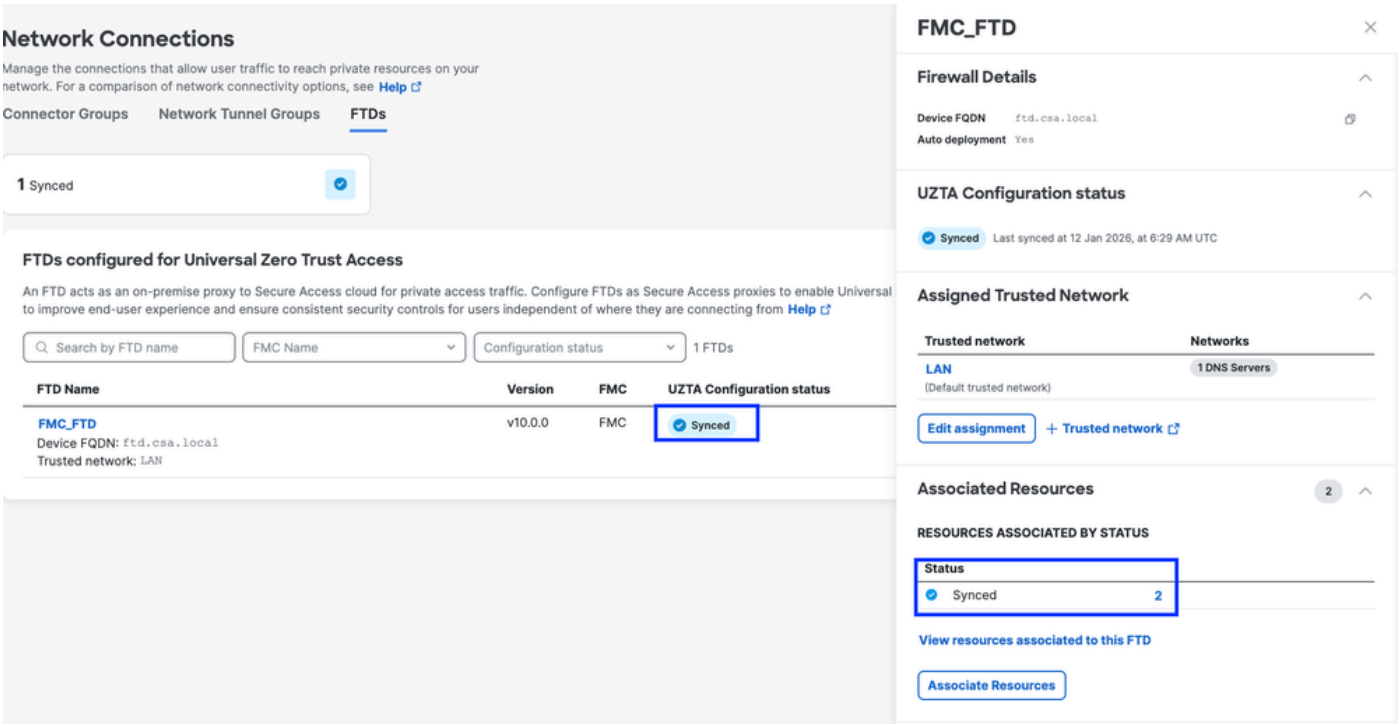


الوصول الآمن - التحقق من العلاقات العامة



3. انقر فوق إغلاق

4. تحقق من الحالة ومن أنه يجب أن يكون المورد المقترن والتكوين في حالة المزامنة



الوصول الآمن - التحقق من العلاقات العامة

5. تحقق من دفع التكوين إلى FTD

قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة ب FTD وانتقل إلى وضع LINA

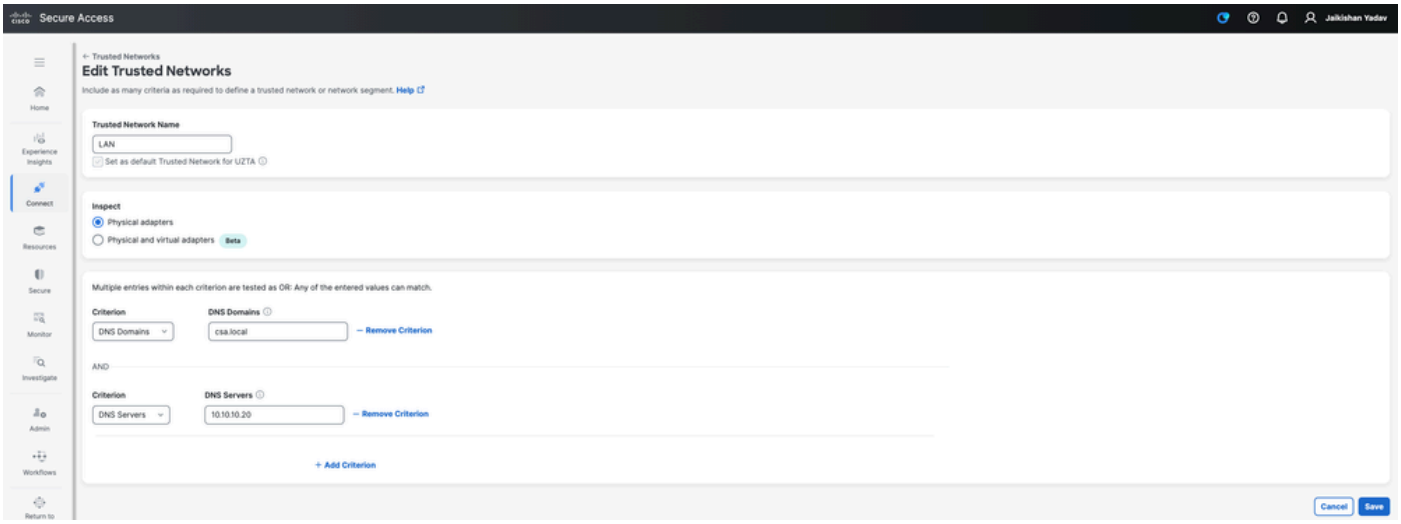
show running-config object application

```
ftd# sh run ob application
object application PR_Router1
 id 427221
 internal domain router1.csa.local tcp eq 22
 internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
 external domain router1.csa.local
 external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
 id 434482
 internal domain router2.csa.local tcp eq 22
 internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
 external domain router2.csa.local
 external subnet 10.10.10.102 255.255.255.255
```

الوصول الآمن - التحقق من العلاقات العامة

الخطوة 4 - configure "إدارة الشبكات الموثوق بها أو إعدادات ZTA"

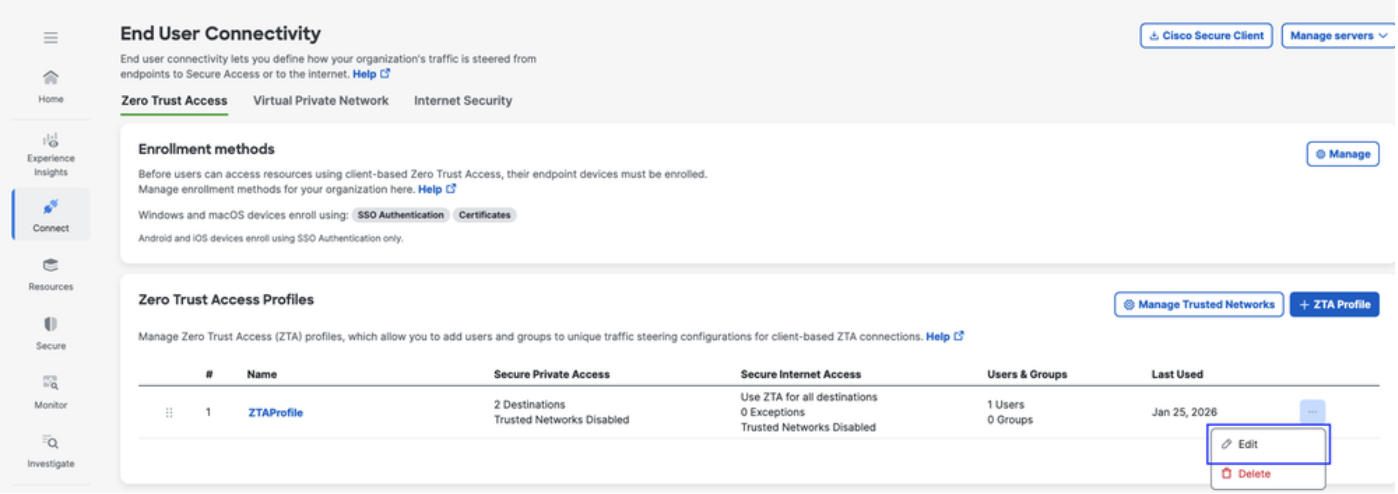
انتقل إلى الاتصال > اتصال المستخدم النهائي > الوصول إلى انعدام الثقة > إعدادات ZTA وتكوين الشبكات الموثوق بها



الوصول الآمن - تكوين TND

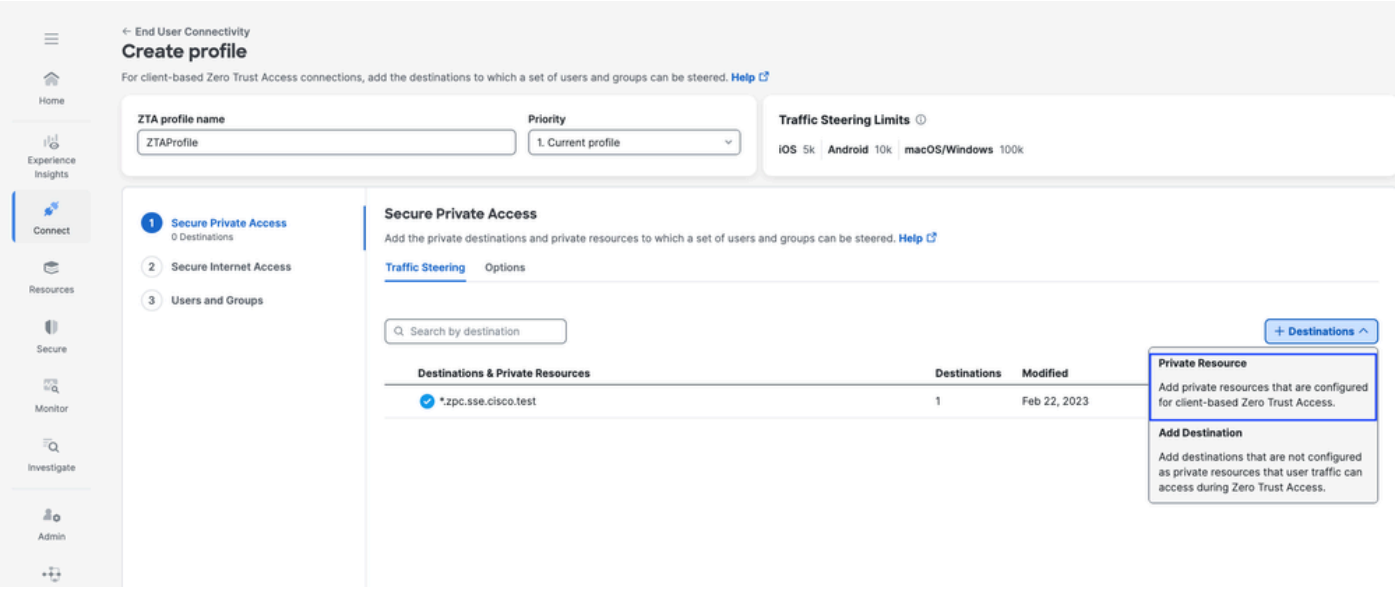
الخطوة 5- إضافة مورد خاص إلى ملف تعريف ZTA

1. انتقل إلى الاتصال > اتصال المستخدم النهائي > الوصول إلى انعدام الثقة وانقر فوق 3 نقاط لتحرير ملف تعريف ZTA

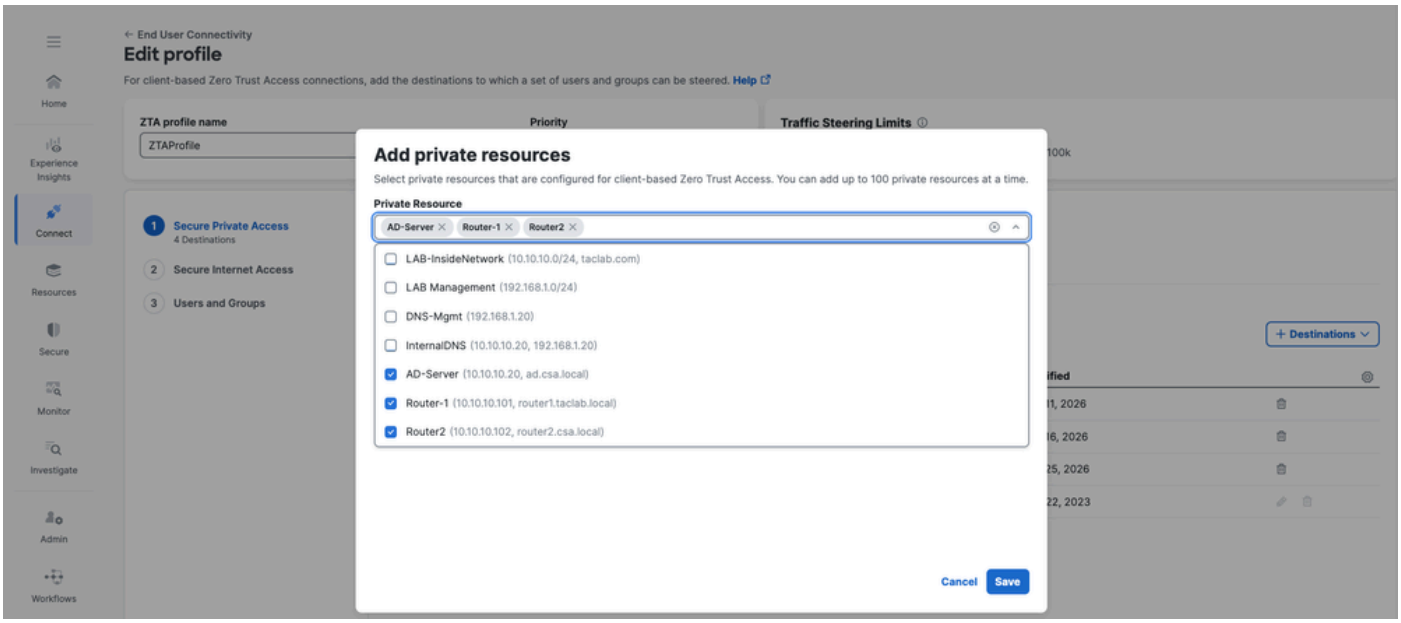


الوصول الآمن - ملف تعريف ZTA

2. إضافة المورد الخاص

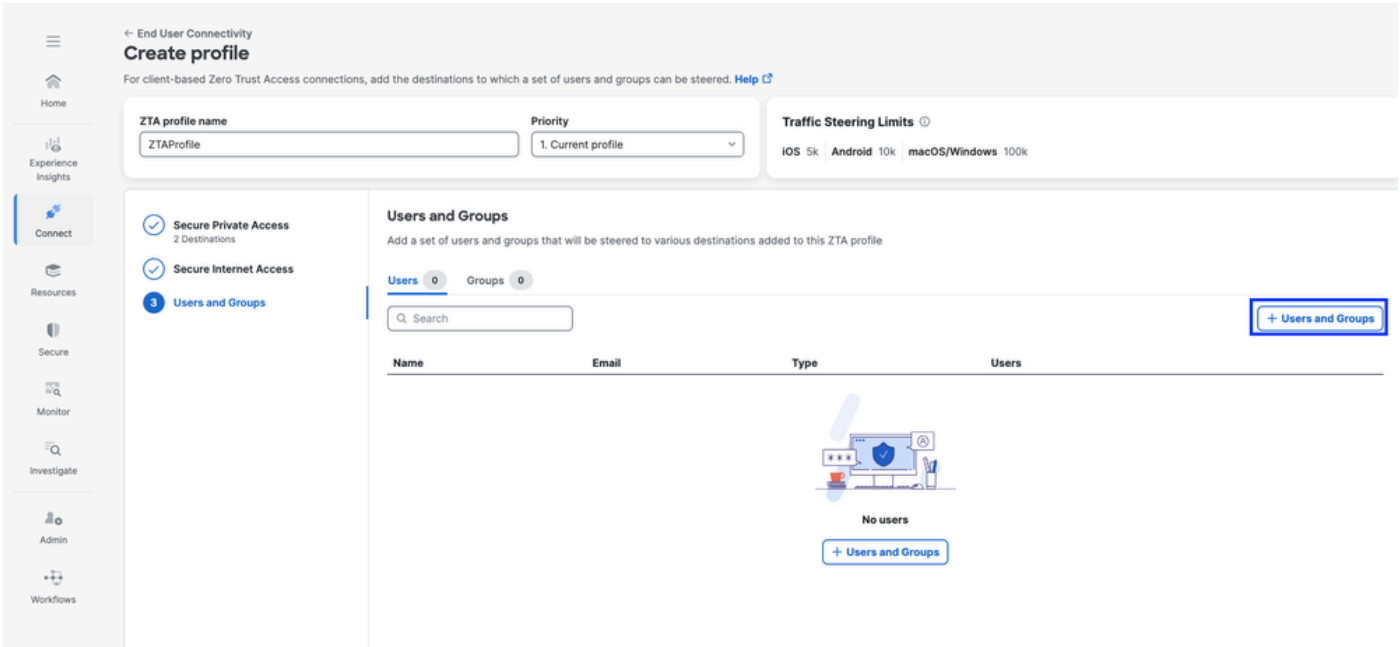


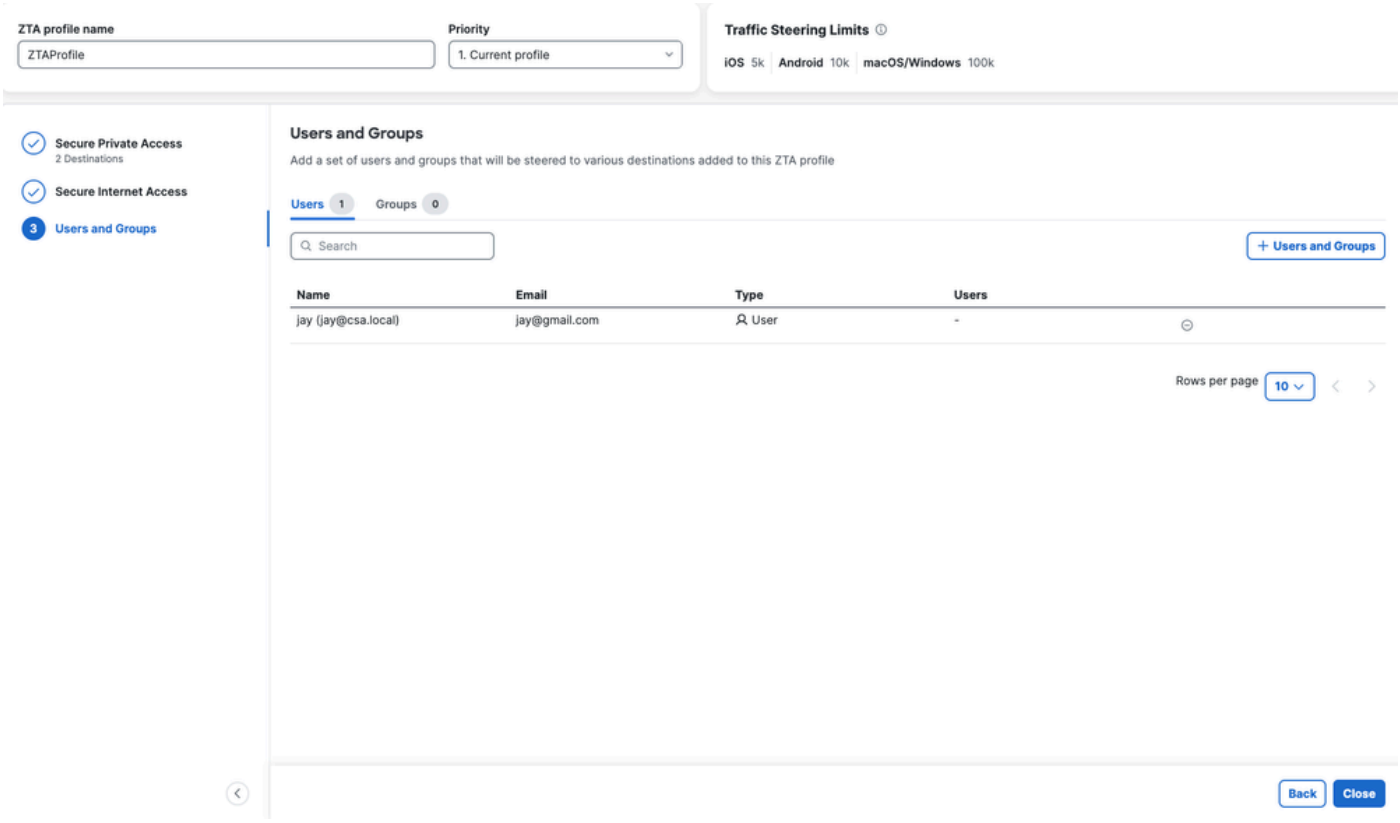
الوصول الآمن - ملف تعريف ZTA



الوصول الآمن - ملف تعريف ZTA

3. إضافة مستخدمين ومجموعات

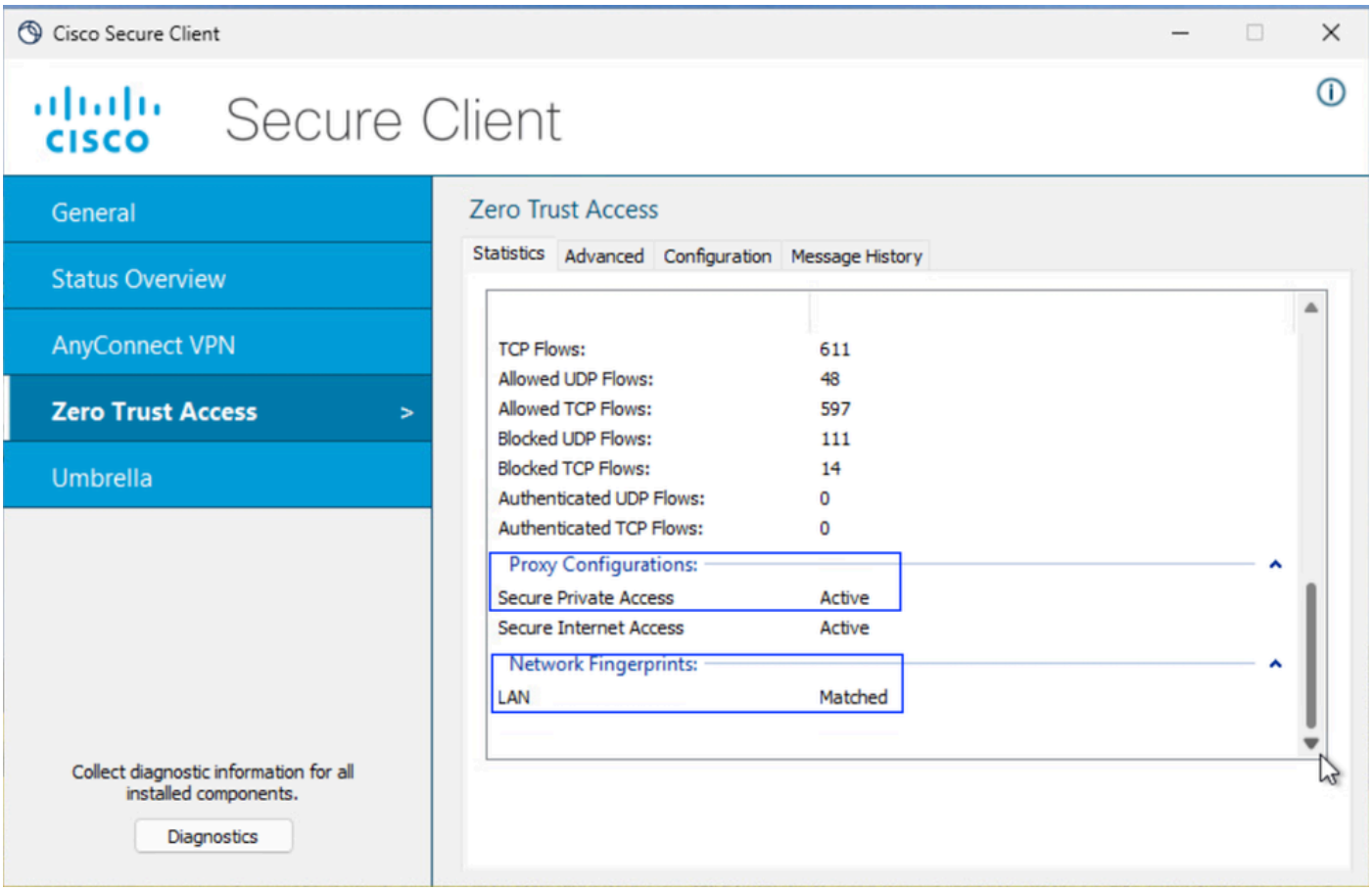




الوصول الآمن - ملف تعريف ZTA

الخطوة 6 - التحقق من الوصول إلى المورد الخاص

1. التحقق من بصمة إصبع الشبكة ل ZTA TND



الوصول الآمن - إختبار العلاقات العامة

2. التحقق من قدرة المستخدم البعيد على حل FTD FQDN

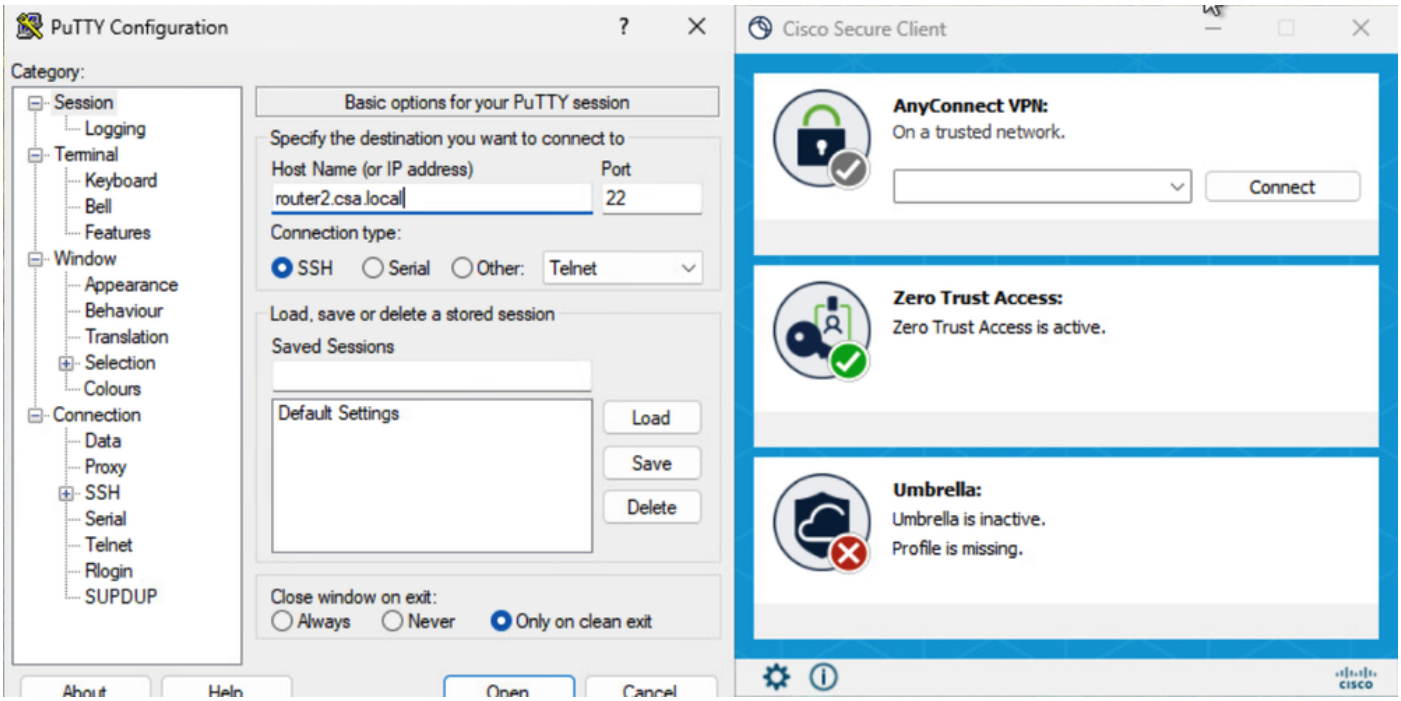
```
C:\Users\jay>ping ftd.csa.local

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. التحقق من إمكانية وصول FTD إلى الموارد الخاصة باستخدام FQDN

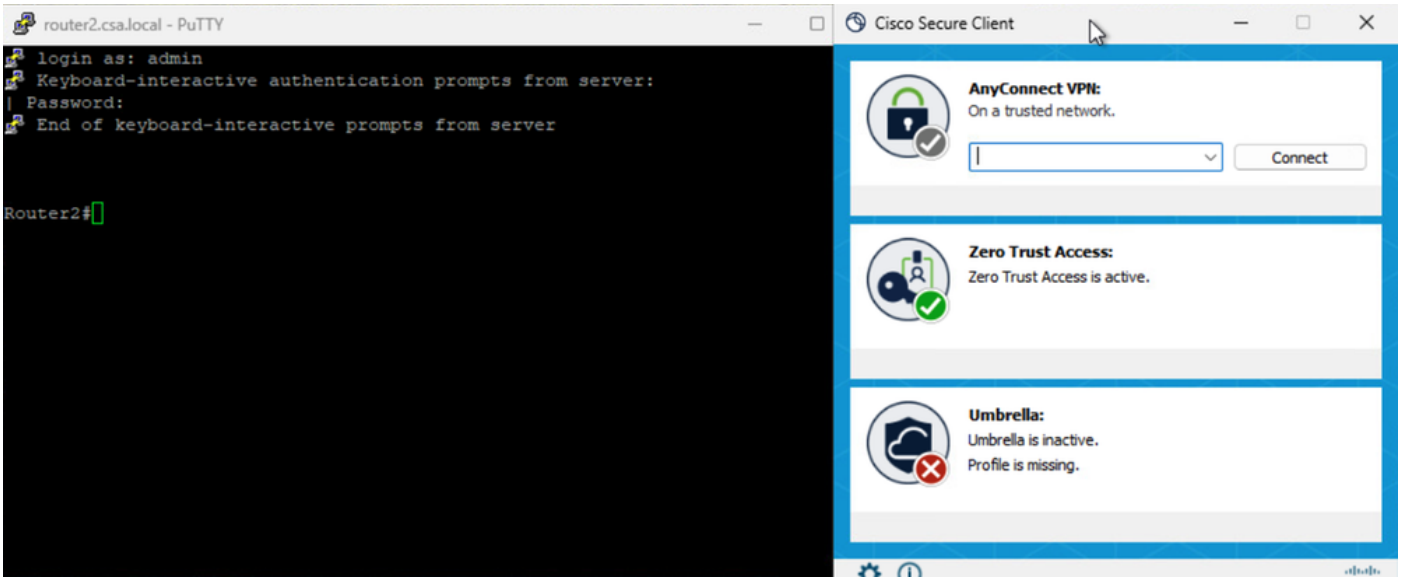
```
ftd# ping router2.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/60 ms
ftd#
```


4. إختبار اتصال SSH بالمورد الخاص

الوصول إلى PR باستخدام FQDN

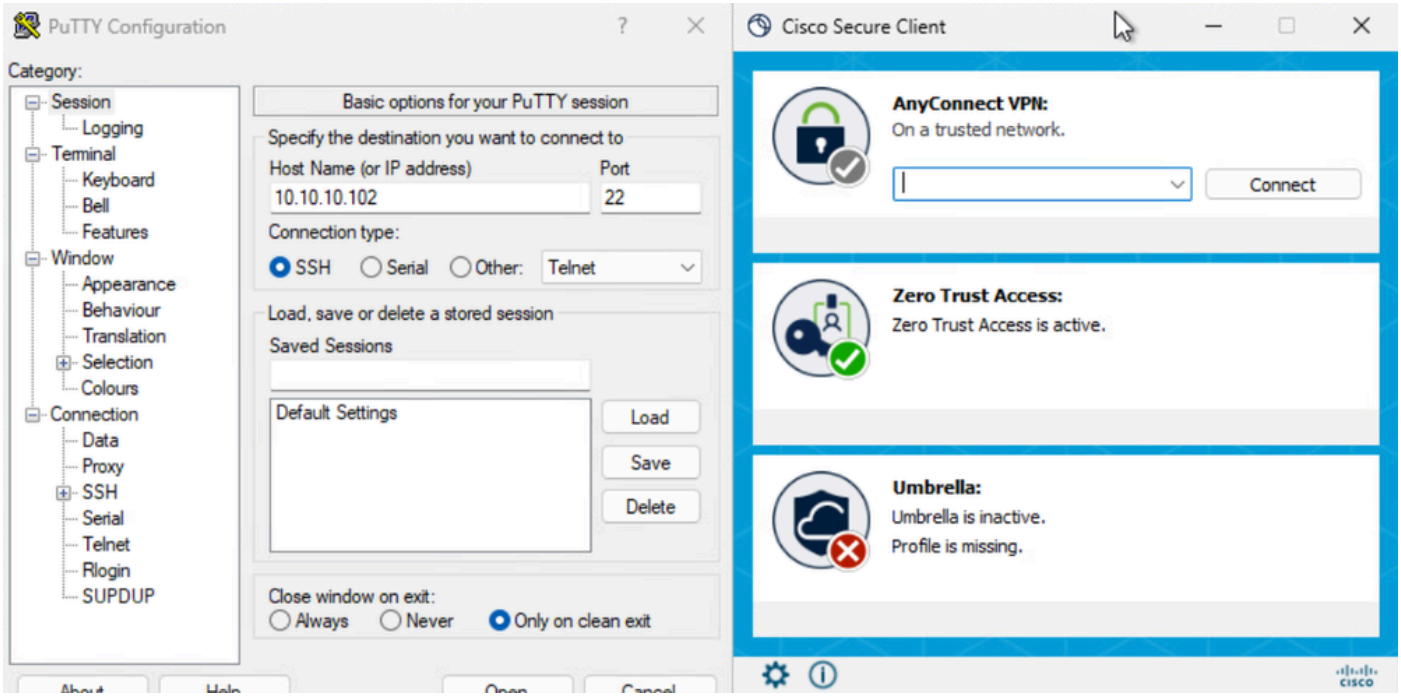


الوصول الآمن - إختبار العلاقات العامة

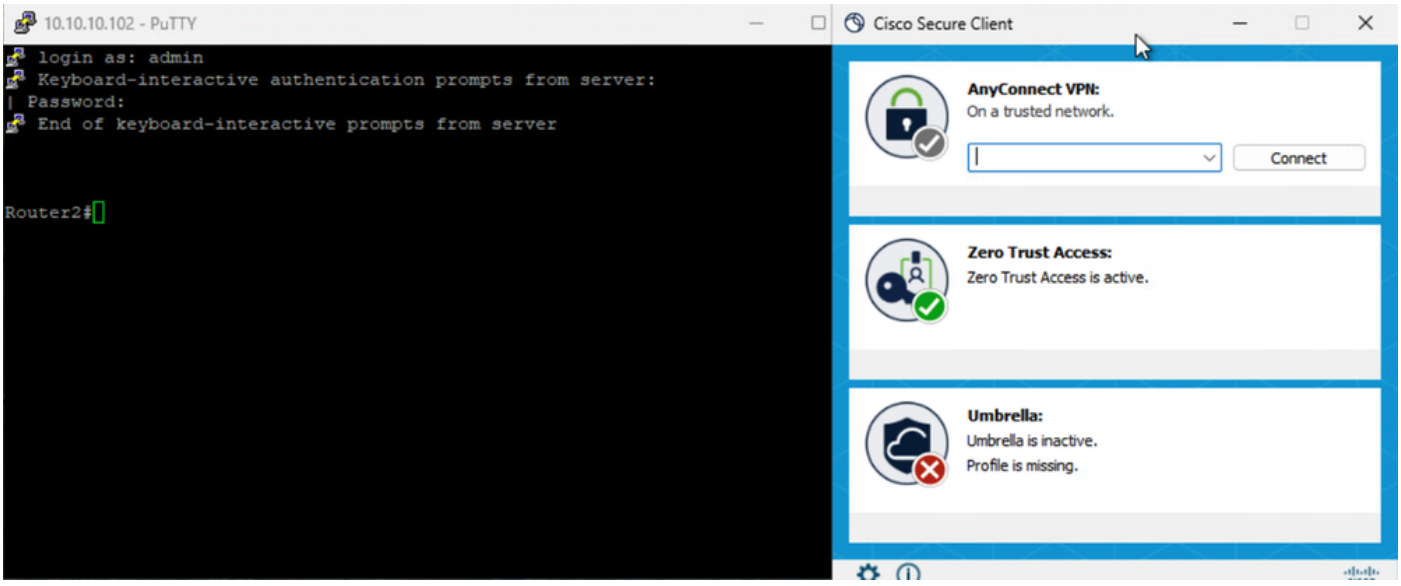


الوصول الآمن - إختبار العلاقات العامة

الوصول إلى PR باستخدام عنوان IP

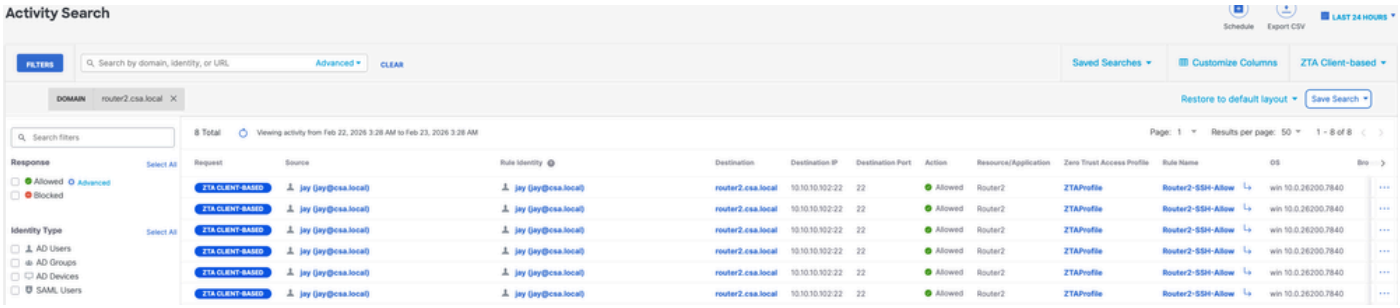


الوصول الآمن - إختبار العلاقات العامة

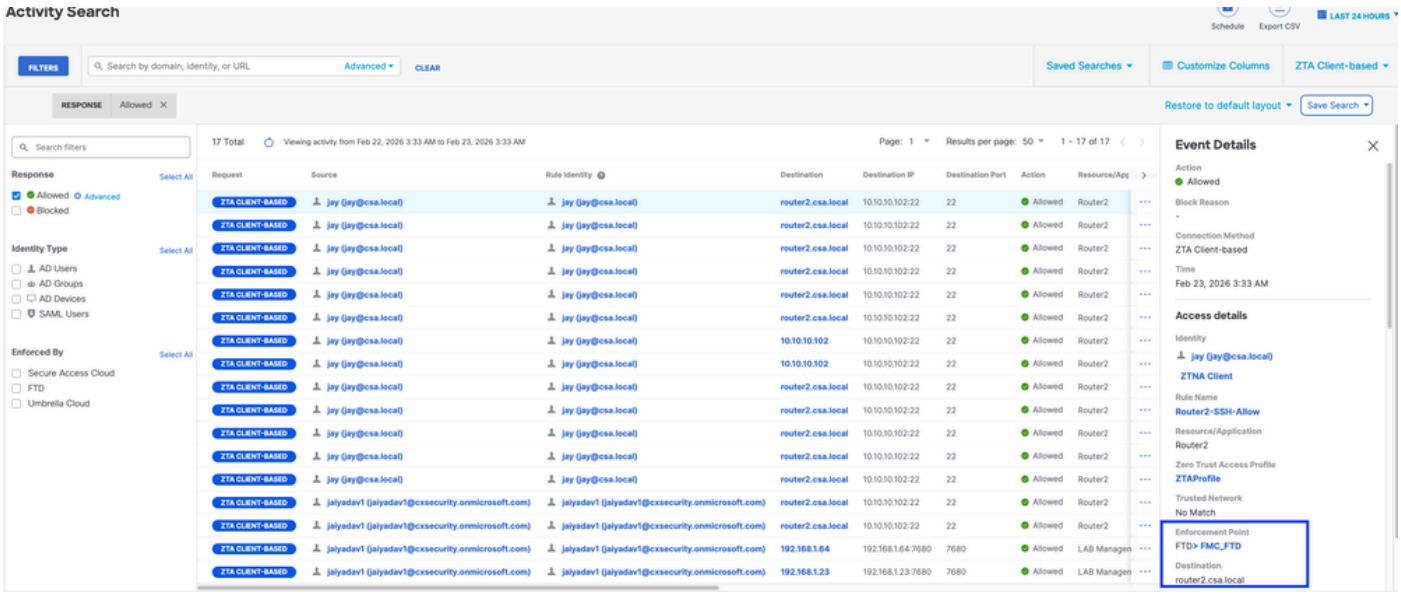


الوصول الآمن - إختبار العلاقات العامة

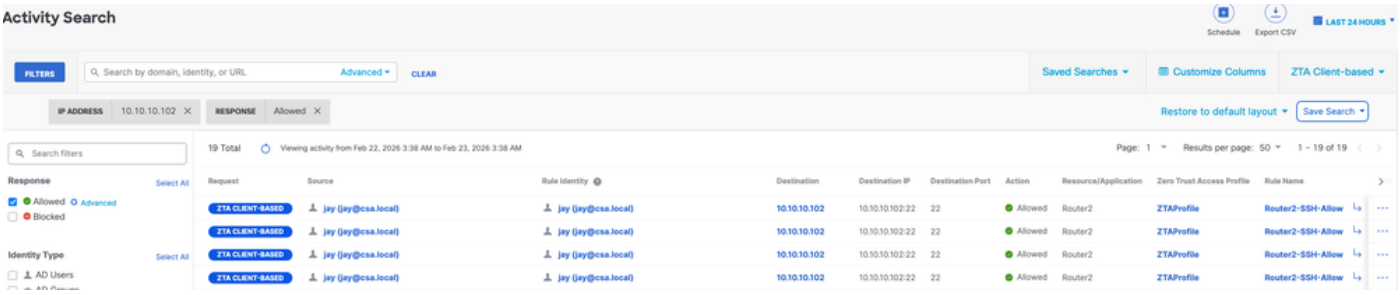
5. التحقق من سجلات خادم نشاط الوصول الآمن



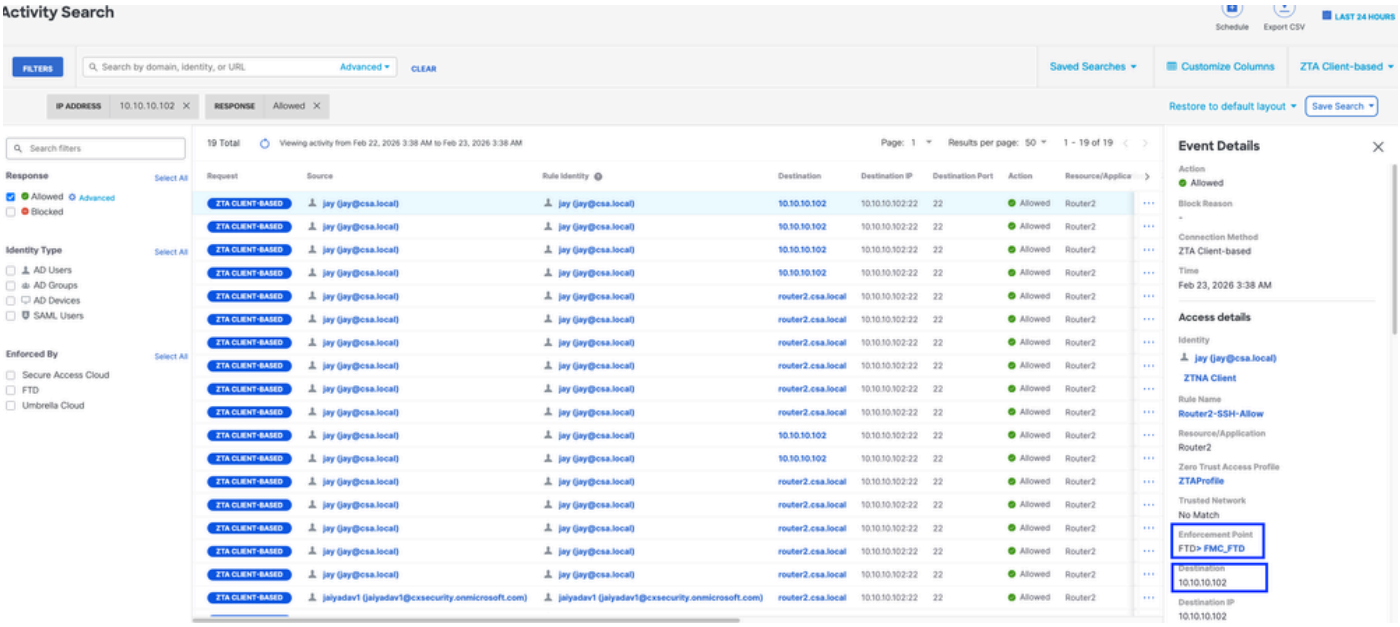
الوصول الآمن - البحث عن الأنشطة



الوصول الآمن - البحث عن الأنشطة

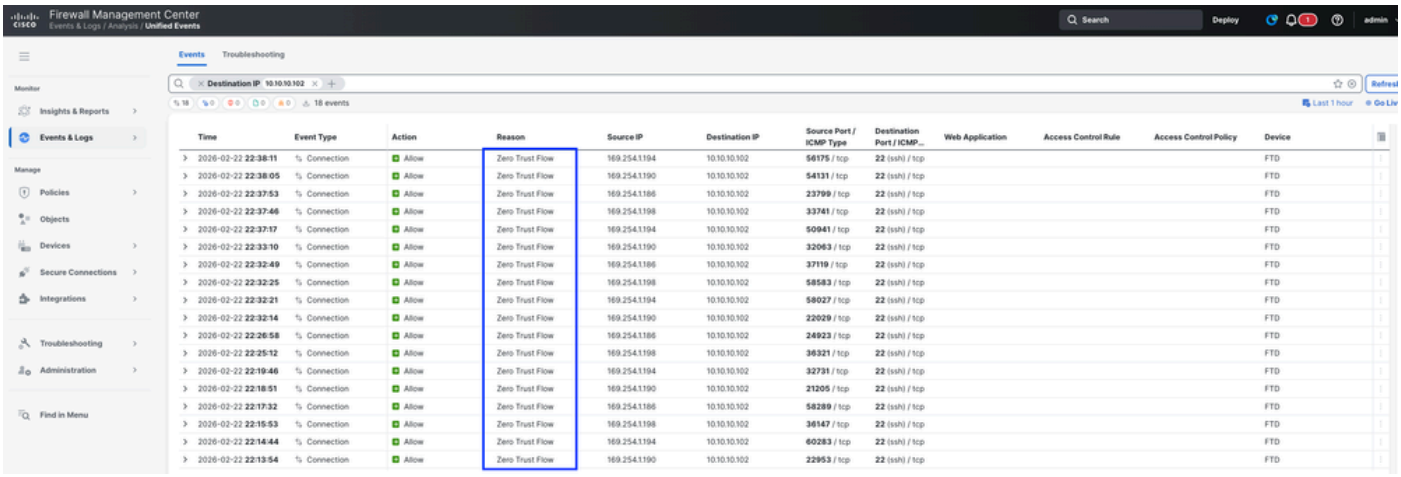


الوصول الآمن - البحث عن الأنشطة



الوصول الآمن - البحث عن الأنشطة

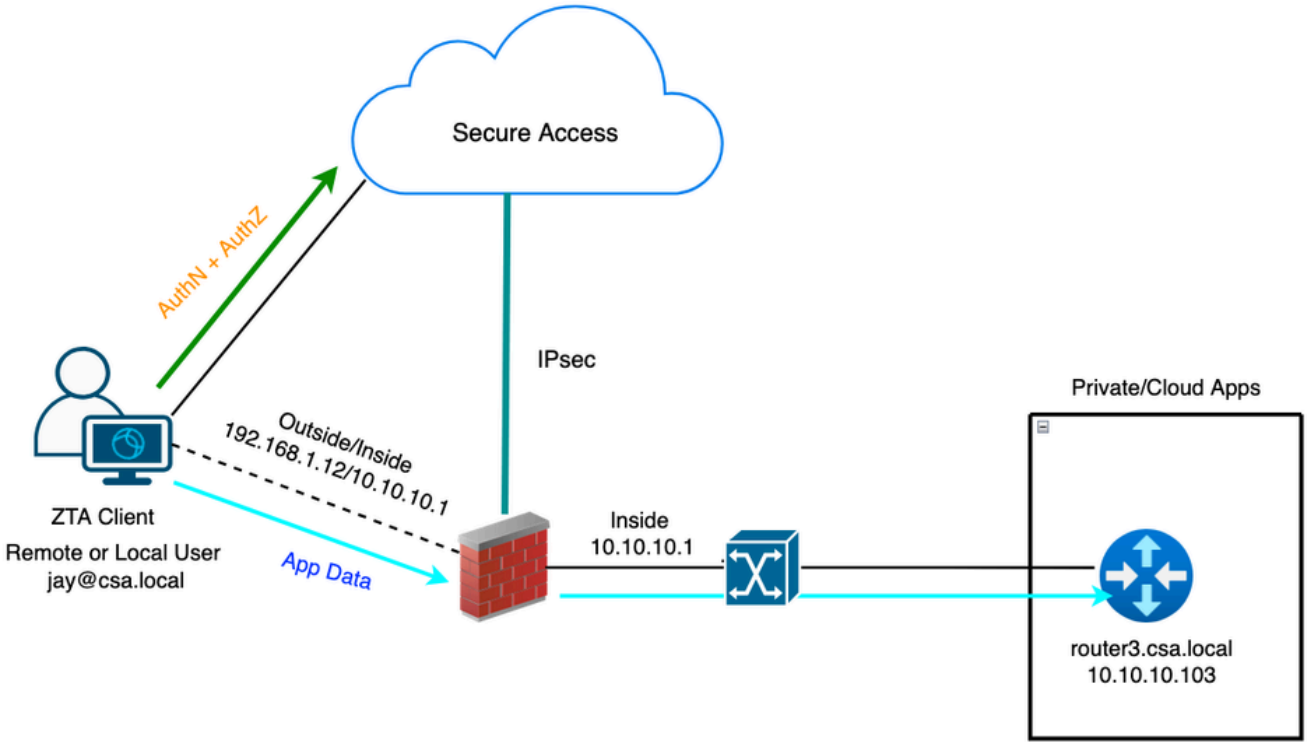
6. التحقق من أحداث اتصال FMC



أحداث اتصال FMC

حالة الاختبار 4 - مستخدم محلي ومستخدم عن بعد - محلي أو تنفيذ عبر السحابة باستخدام TND

في هذه الحالة، يعتمد نوع الإنفاذ على موقع المستخدم، وإذا كان المستخدم محليا أو خلف منطقة FTD موثوق بها (في الداخل، DMZ وما إلى ذلك)، يكون الإنفاذ محليا (حالة الاختبار 3). وعلى وجه الخصوص، إذا كان المستخدم بعيدا، فسيكون الإنفاذ عبارة عن Cloud (حالة الاختبار 1). سيتم تحديد موقع المستخدم استنادا إلى بصمة الإصبع في الشبكة أو إعداد TND، وإذا تطابقت بصمة الإصبع في الشبكة فسيكون المستخدم المحلي محليا وإذا لم يكن متطابقا فسيتم إعتبار المستخدم المحلي هو البعيد .

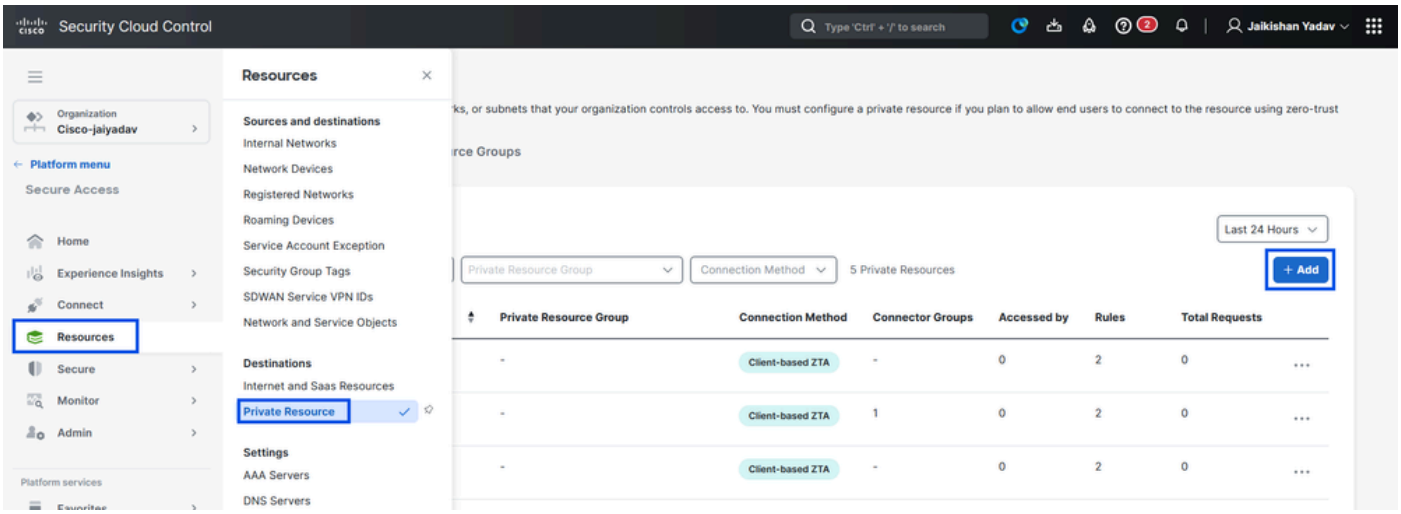


مخطط توضيحي لحالة الاختبار - طبوغرافيا ZTA

الخطوة 1 - تحديد مورد خاص على الوصول الآمن

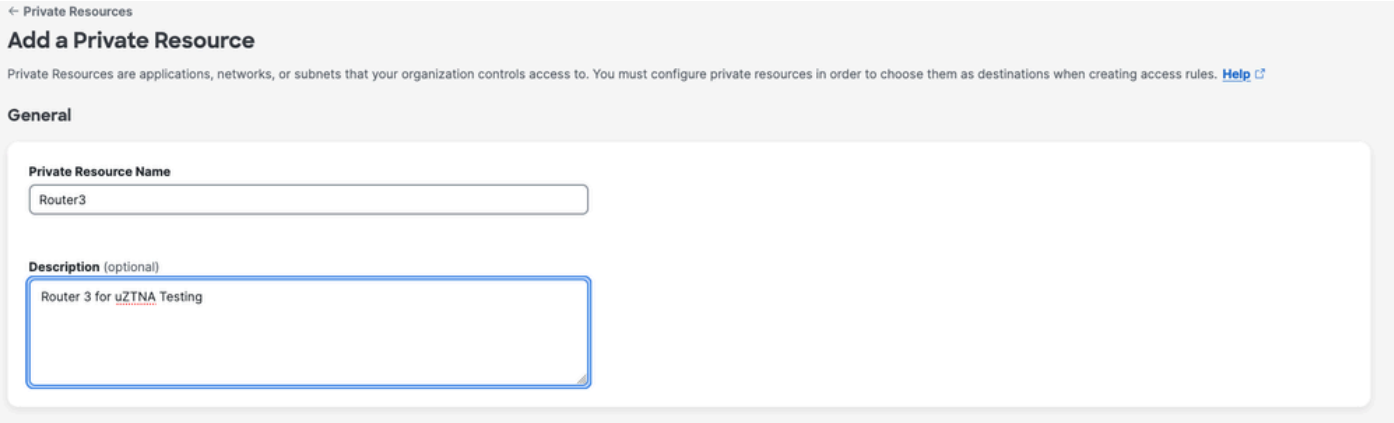
تكوين مورد خاص ليتم الوصول إليه عبر الجهاز المسجل في الوصول إلى عدم الثقة (ZTA) باستخدام فرض السحابة

1. انتقل إلى الموارد > الوجهات > الموارد الخاصة > انقر فوق +إضافة



الوصول الآمن - تكوين الموارد الخاصة

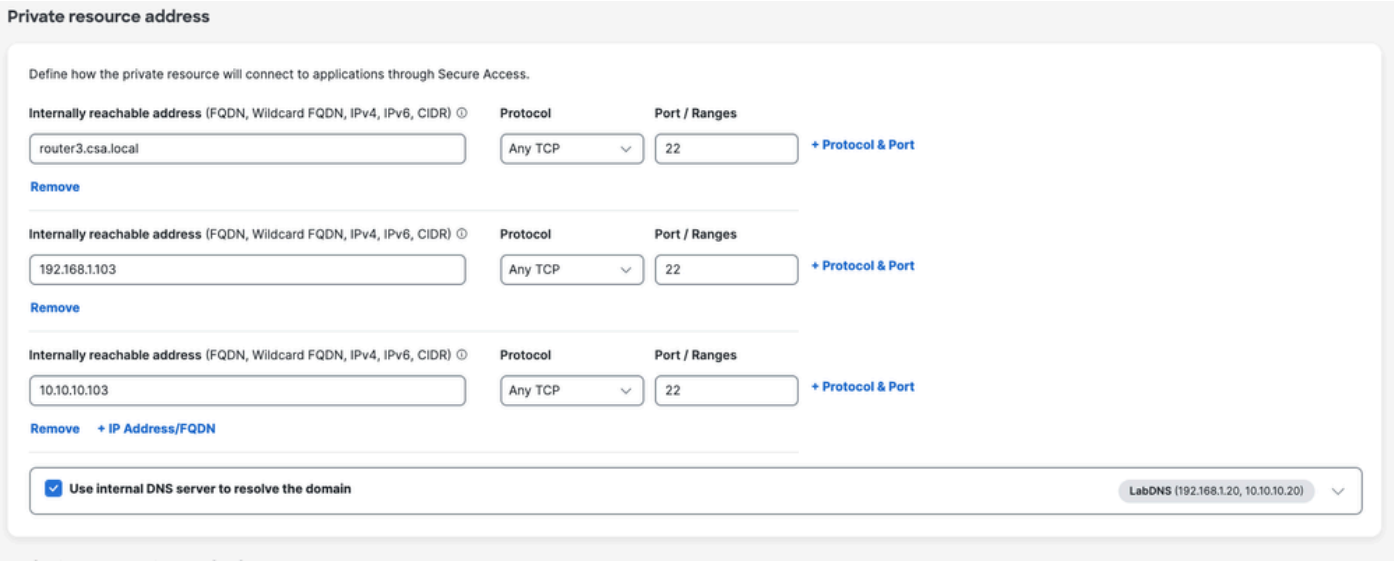
2. بالنسبة إلى اسم المورد الخاص، أدخل اسما ذا معنى للمورد. للحصول على الوصف، ونصي بتوفير معلومات مثل الغرض من المورد أو اسم مالك المورد.



الوصول الآمن - تكوين الموارد الخاصة

3. أدخل FQDN للمورد الخاص الذي تريد الوصول إليه . كما يمكنك تحديد عنوان IP الخاص بالمورد الخاص . لمزيد من المعلومات، راجع [إضافة مورد خاص]

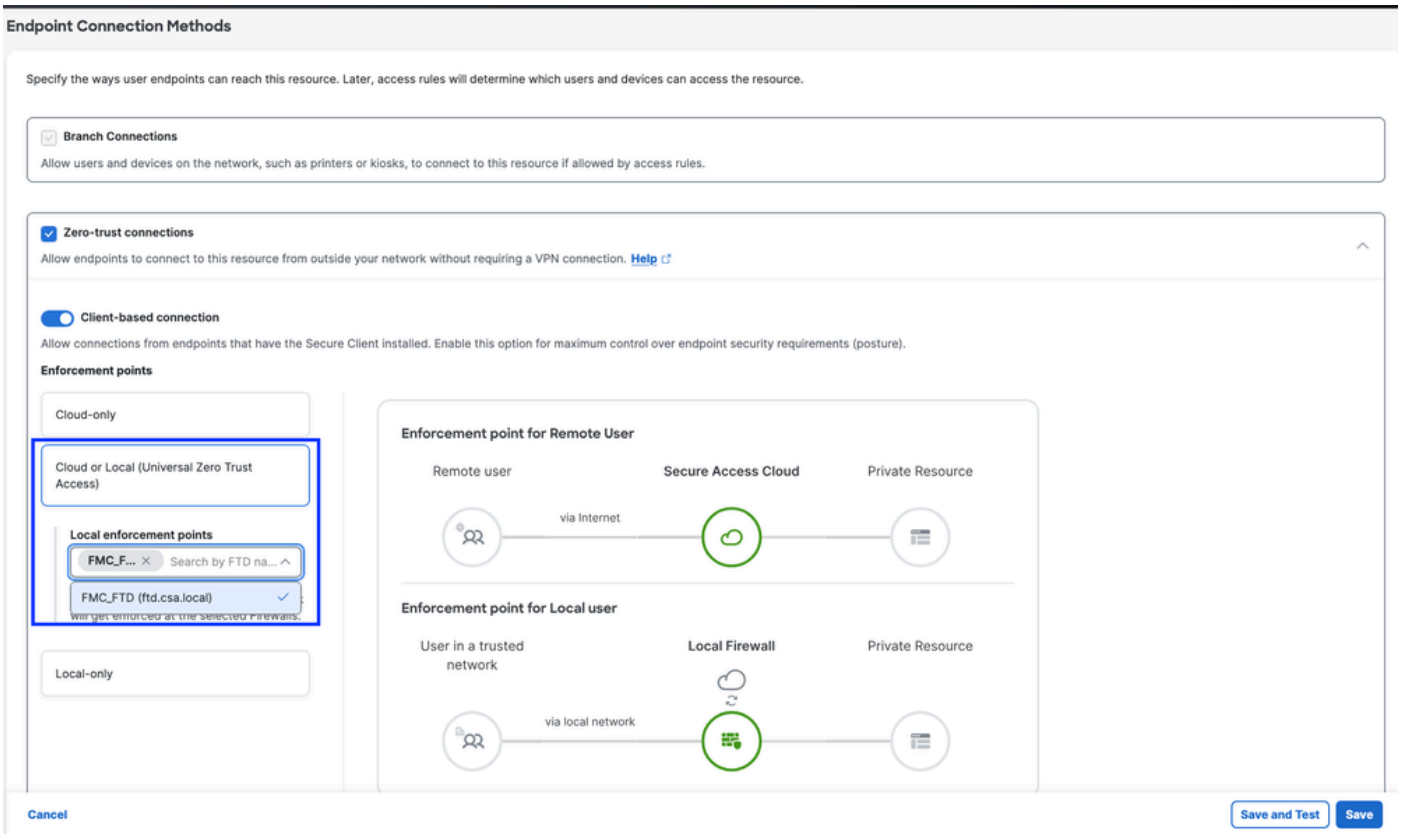
4. حدد خادم DNS لحل المجال



الوصول الآمن - تكوين الموارد الخاصة

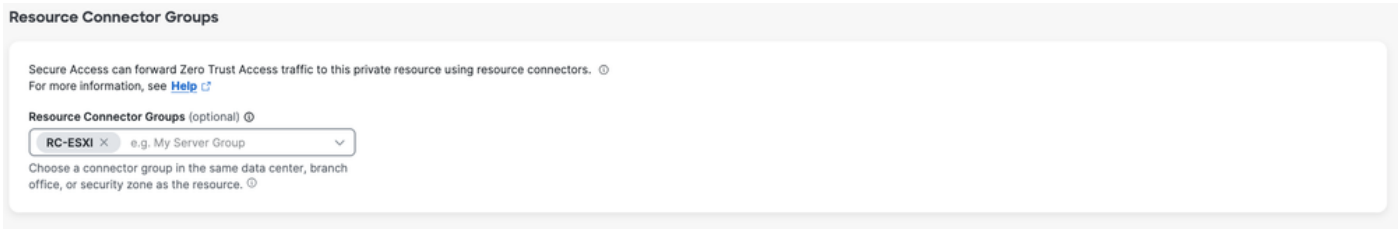
5. تحديد أسلوب اتصال نقطة النهاية

6. حدد FTD كنقاط تنفيذ محلية



الوصول الآمن - تكوين الموارد الخاصة

حدد RC إذا كان يمكن الوصول إلى المورد الخاص عبر RC، وإلا فاتركه فارغا إذا كان يمكن الوصول إلى المورد الخاص عبر مجموعة نفق الشبكة (نفق IPsec).



الوصول الآمن - تكوين الموارد الخاصة

ملاحظة: اعتمادا على نوع التسجيل الذي تحدده ، سيقوم هذا التغيير بإقران PR تلقائيا ب FTD وسيؤدي إلى تشغيل نشر النهج

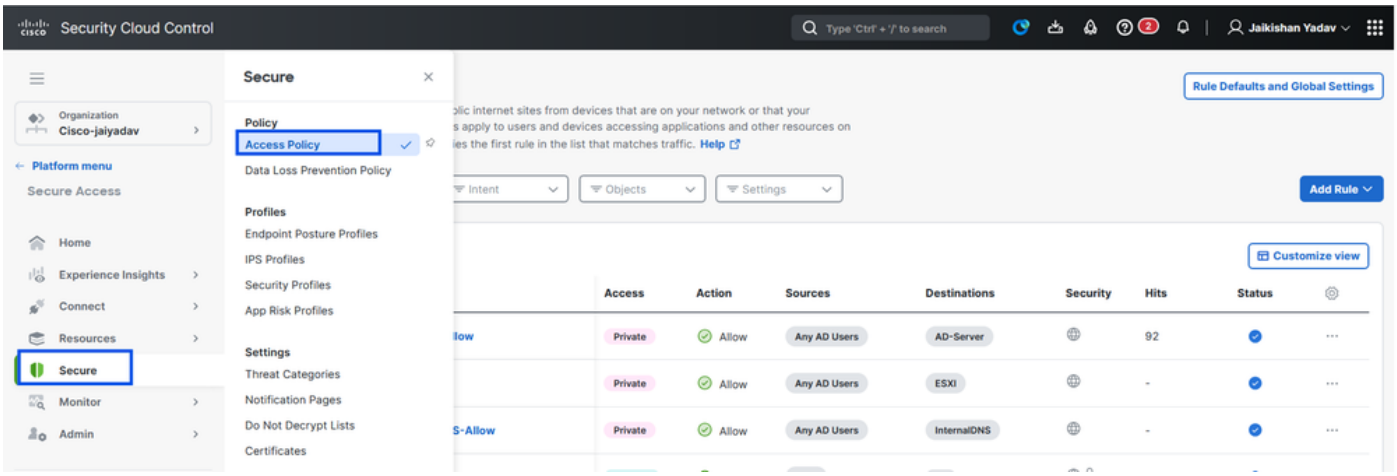
---

7. انقر فوق حفظ

الخطوة 2 - إنشاء قاعدة وصول خاصة

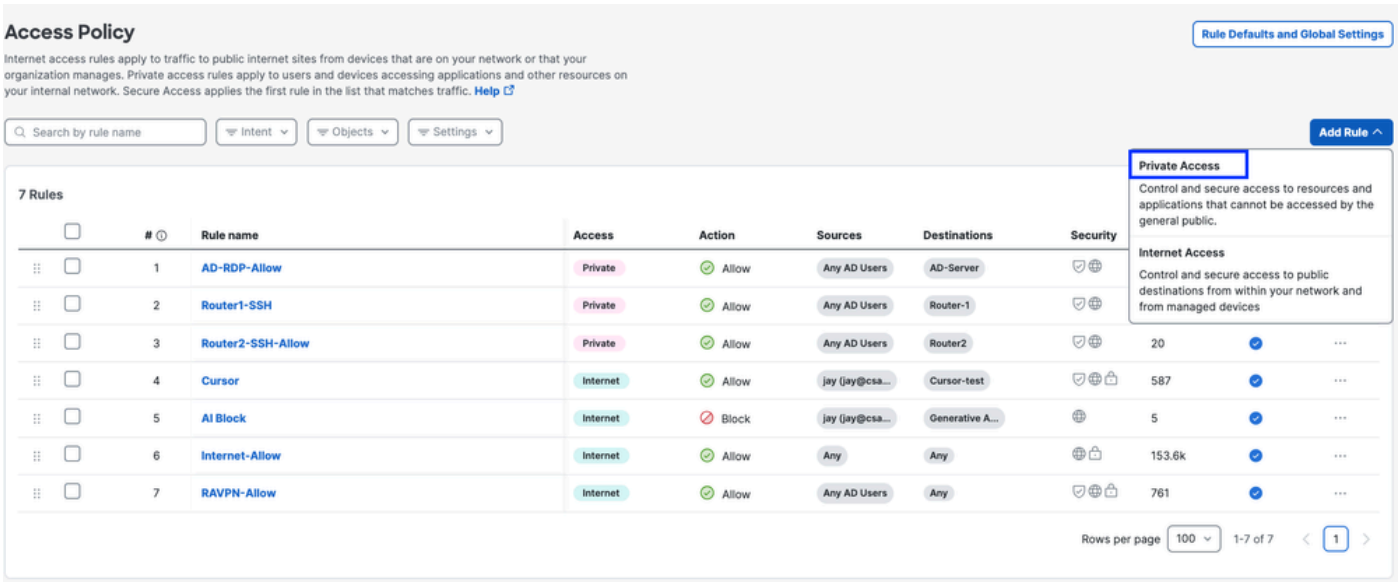
تكوين وصول خاص على Secure Access ليتمكن المستخدمون المسجلون في ZTA العالمية من الوصول إليه . لمزيد من المعلومات، راجع [قاعدة الوصول الخاص]

1. انتقل إلى آمن > نهج الوصول



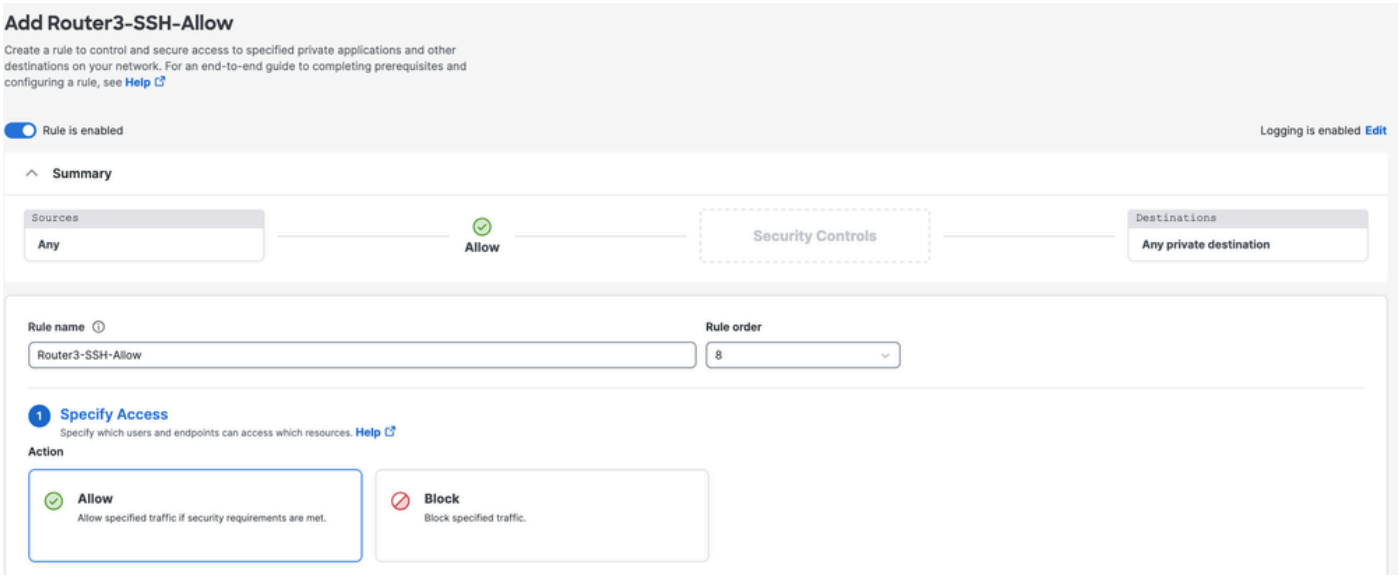
الوصول الآمن - تكوين سياسة الوصول

2. انقر فوق إضافة قاعدة، ثم أختر Private Access.
في أعلى القاعدة يوجد ملخص يصف المكونات المكونة للقاعدة الخاصة بك.



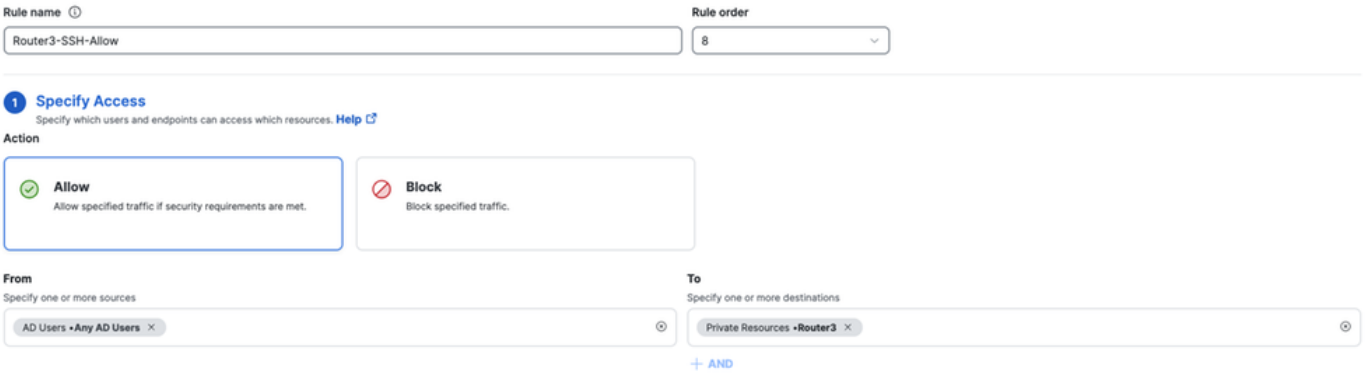
الوصول الآمن - تكوين سياسة الوصول

3. إضافة اسم قاعدة



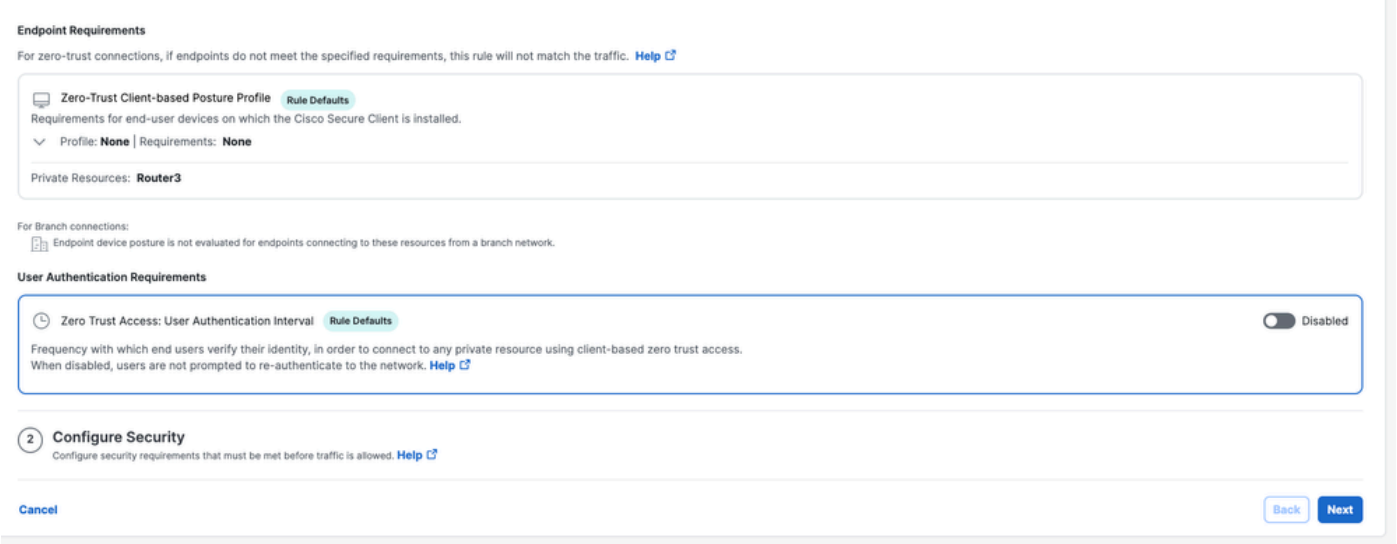
الوصول الآمن - تكوين سياسة الوصول

4. حدد إجراء القاعدة وحدد المصدر والوجهة



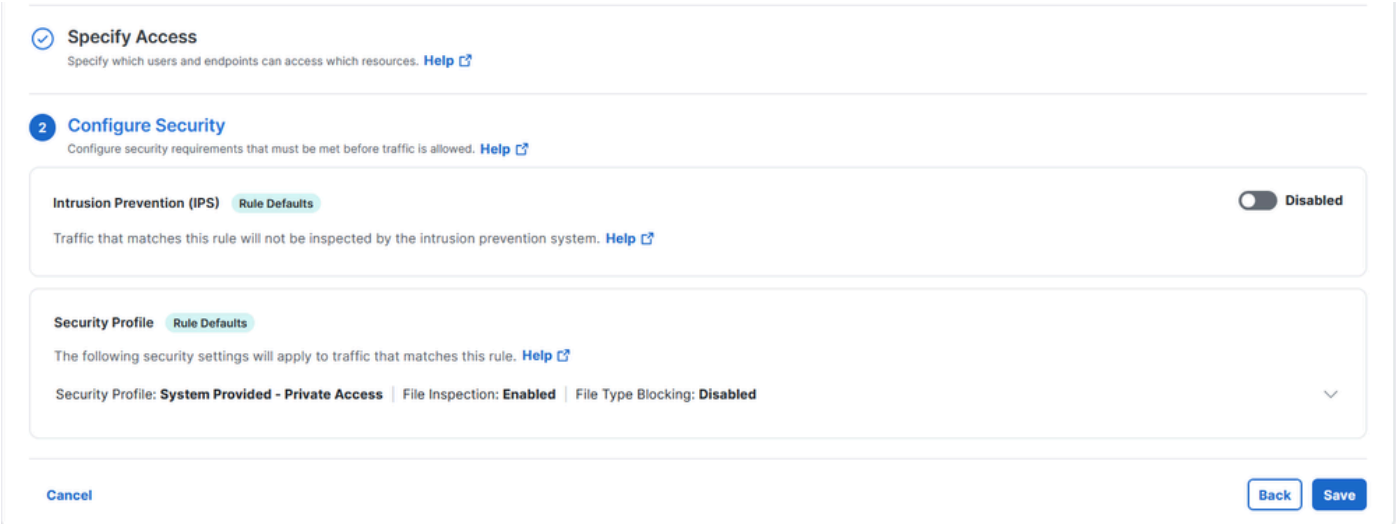
الوصول الآمن - تكوين سياسة الوصول

5. تكوين متطلبات نقطة النهاية



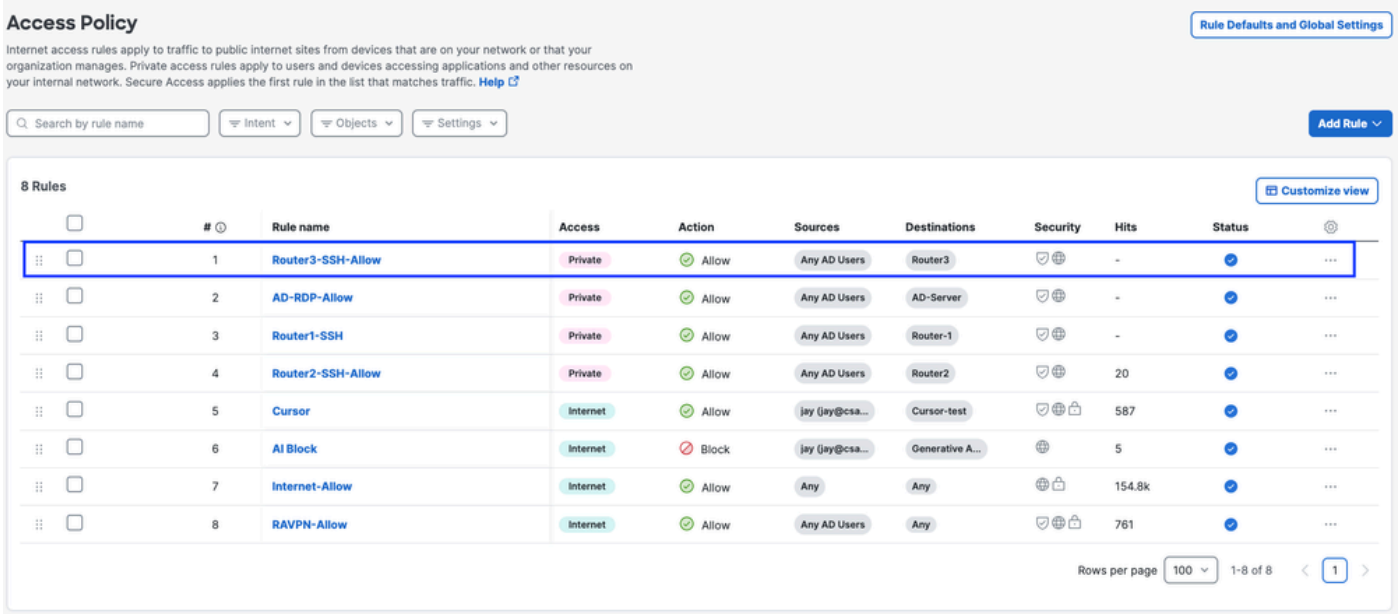
الوصول الآمن - تكوين سياسة الوصول

6. تكوين الأمان



الوصول الآمن - تكوين سياسة الوصول

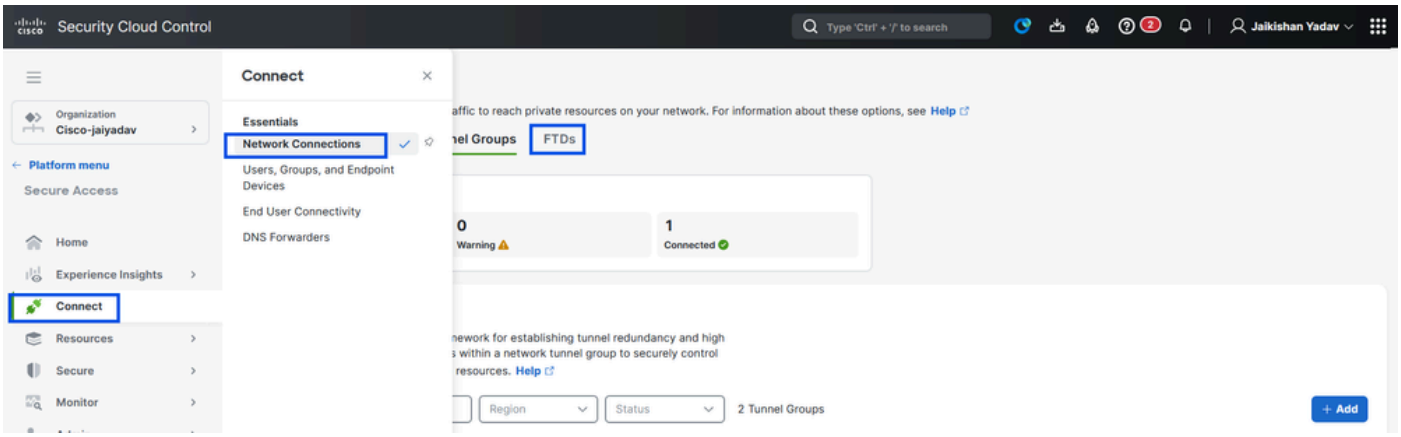
7. انقر فوق حفظ



الوصول الآمن - تكوين سياسة الوصول

الخطوة 3 - التحقق من اقتران العلاقات العامة على FTD

1. انتقل للاتصال > إتصالات الشبكة > FTDs

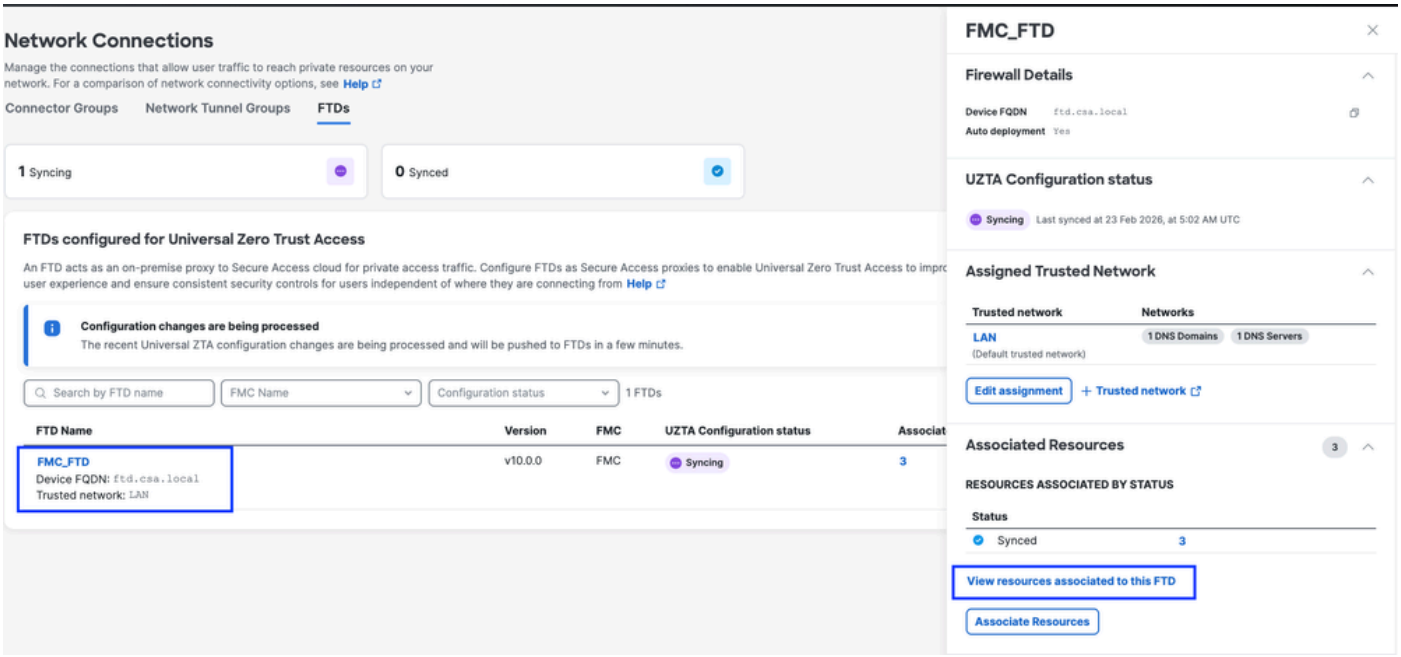


الوصول الآمن - التحقق من العلاقات العامة

2. انقر فوق FTD > عرض الموارد المقترنة ب FTD هذا

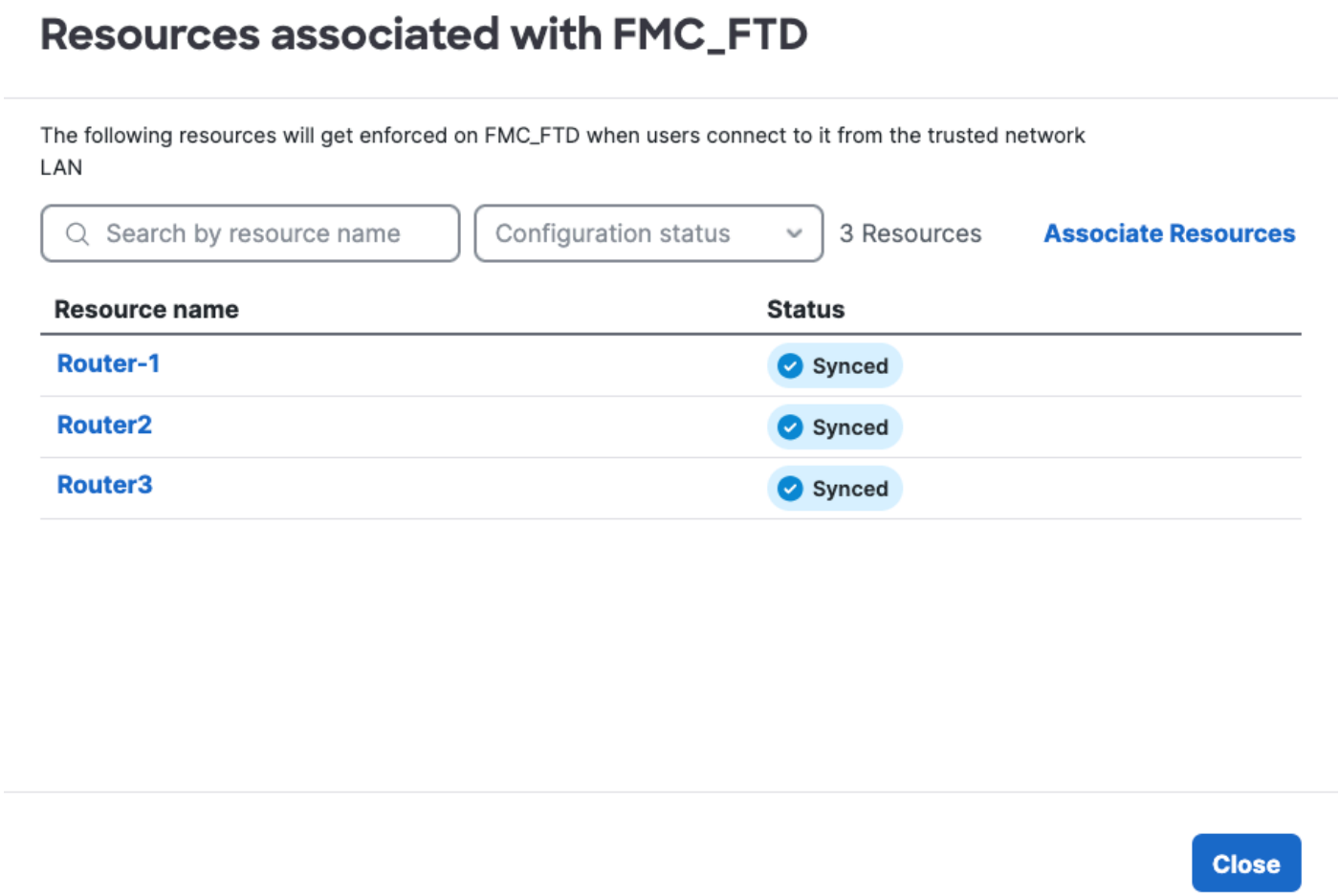
```
C:\Users\jay>ping ftd.csa.local

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
```

الوصول الآمن - التحقق من العلاقات العامة



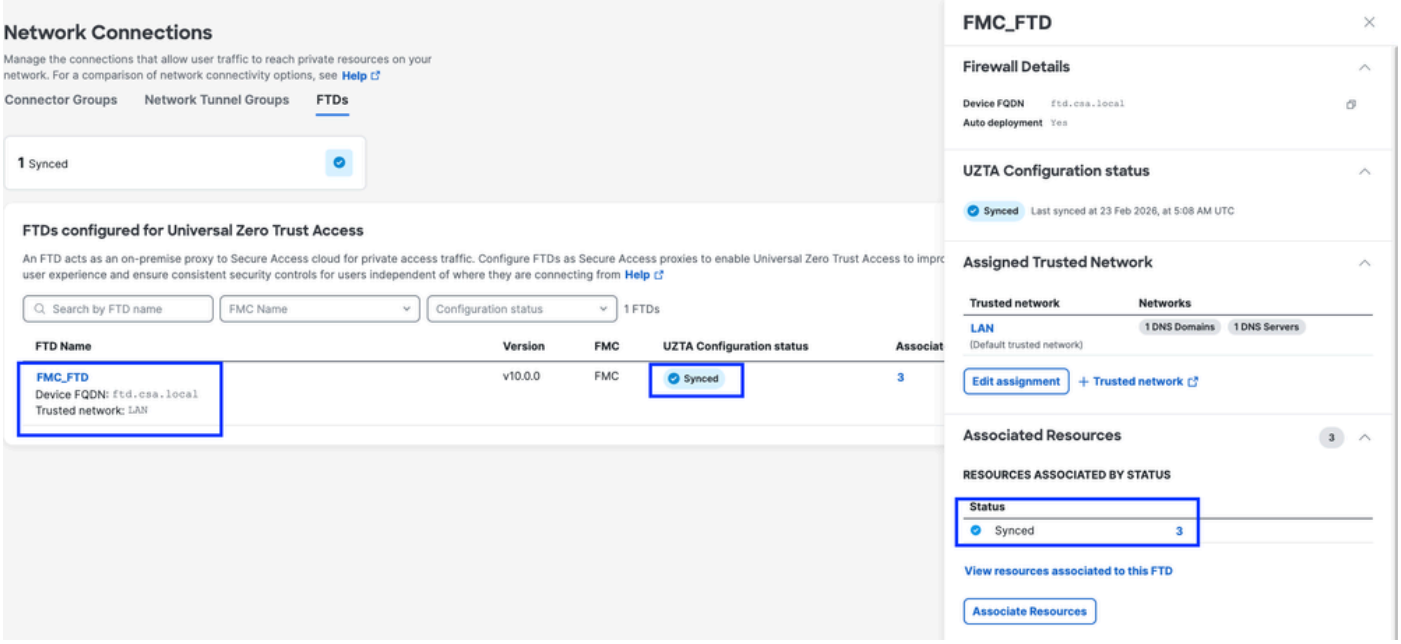
الوصول الآمن - التحقق من العلاقات العامة

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

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server:  AD.csa.local
Address:  192.168.1.20

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



3. انقر فوق إغلاق

4. تحقق من الحالة ومن أنه يجب أن يكون المورد المقترن والتكوين في حالة المزامنة



الوصول الآمن - التحقق من العلاقات العامة

5. تحقق من دفع التكوين إلى FTD

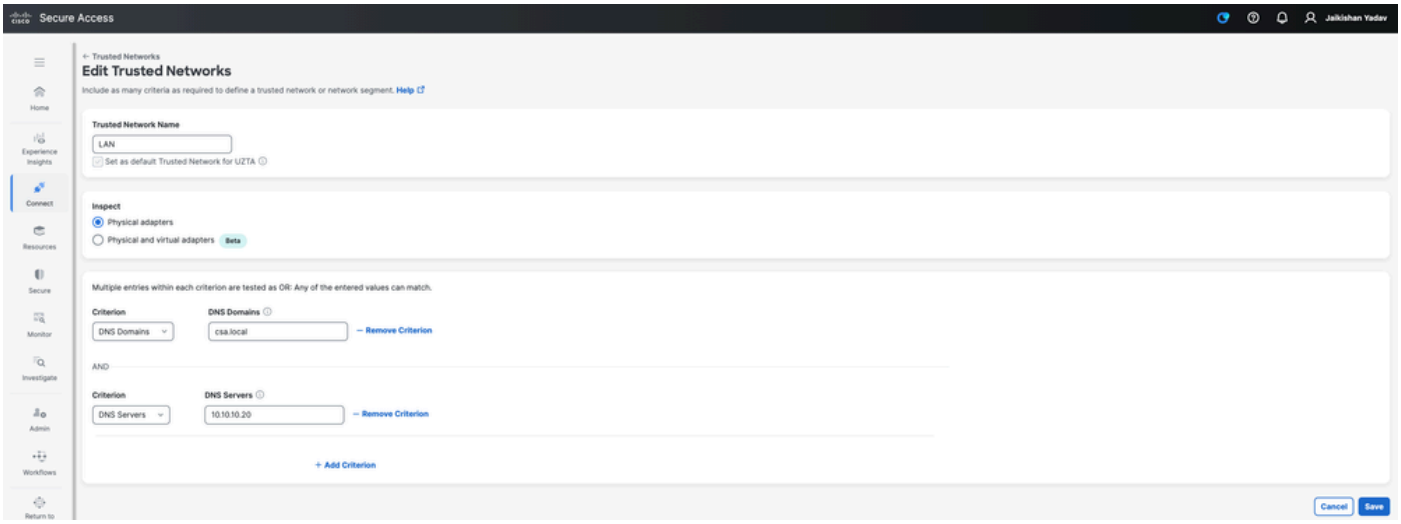
قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة ب FTD وانتقل إلى وضع LINA

show running-config object application

```
ftd# sh run object application
object application PR_Router2
 id 443200
 internal domain router2.csa.local tcp eq 22
 internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
 external domain router2.csa.local
 external subnet 10.10.10.102 255.255.255.255
object application PR_Router-1
 id 438025
 internal domain router1.csa.local tcp range 1 65535
 internal subnet 10.10.10.101 255.255.255.255 tcp range 1 65535
 external domain router1.csa.local
 external subnet 10.10.10.101 255.255.255.255
object application PR_Router3
 id 468677
 internal domain router3.csa.local tcp eq 22
 internal subnet 192.168.1.103 255.255.255.255 tcp eq 22
 internal subnet 10.10.10.103 255.255.255.255 tcp eq 22
 external domain router3.csa.local
 external subnet 10.10.10.103 255.255.255.255
 external subnet 192.168.1.103 255.255.255.255
```

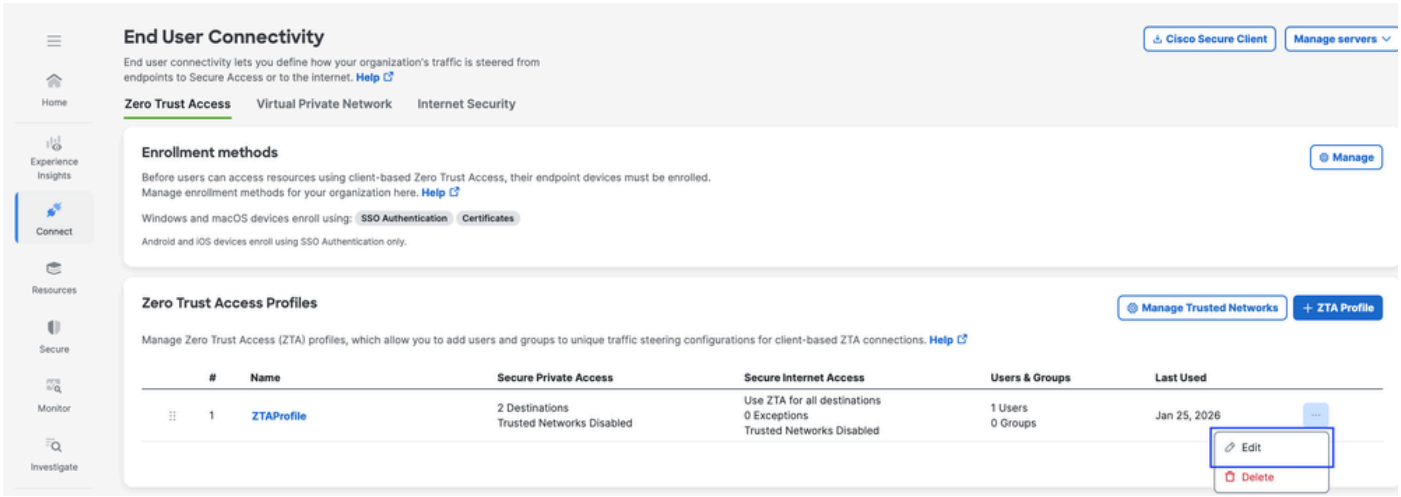
" الخطوة - 4 تكوين الشبكات الموثوق بها أو إعدادات ZTA أو التحقق منها

انتقل إلى الاتصال > اتصال المستخدم النهائي > الوصول إلى انعدام الثقة > إعدادات ZTA وتكوين الشبكات الموثوق بها

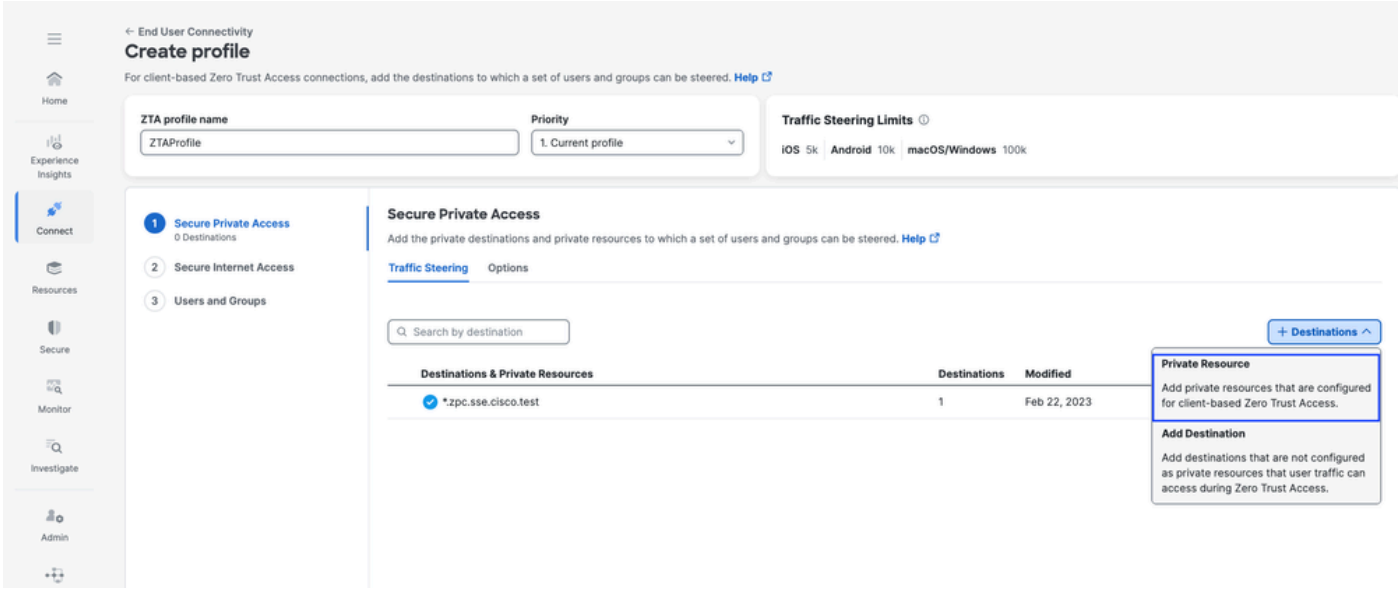


الخطوة - 5 إضافة مورد خاص إلى ملف تعريف ZTA

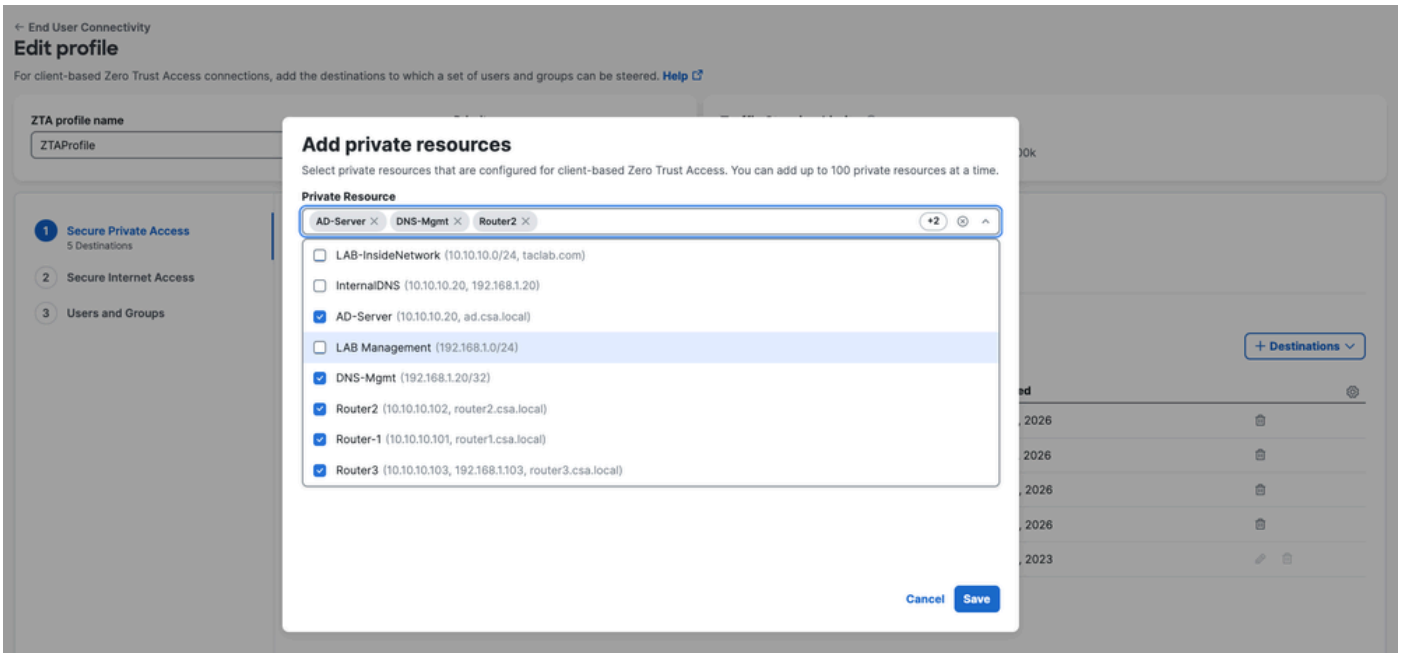
1. انتقل إلى الاتصال > اتصال المستخدم النهائي > الوصول إلى انعدام الثقة وانقر فوق 3 نقاط لتحرير ملف تعريف ZTA



2. إضافة المورد الخاص

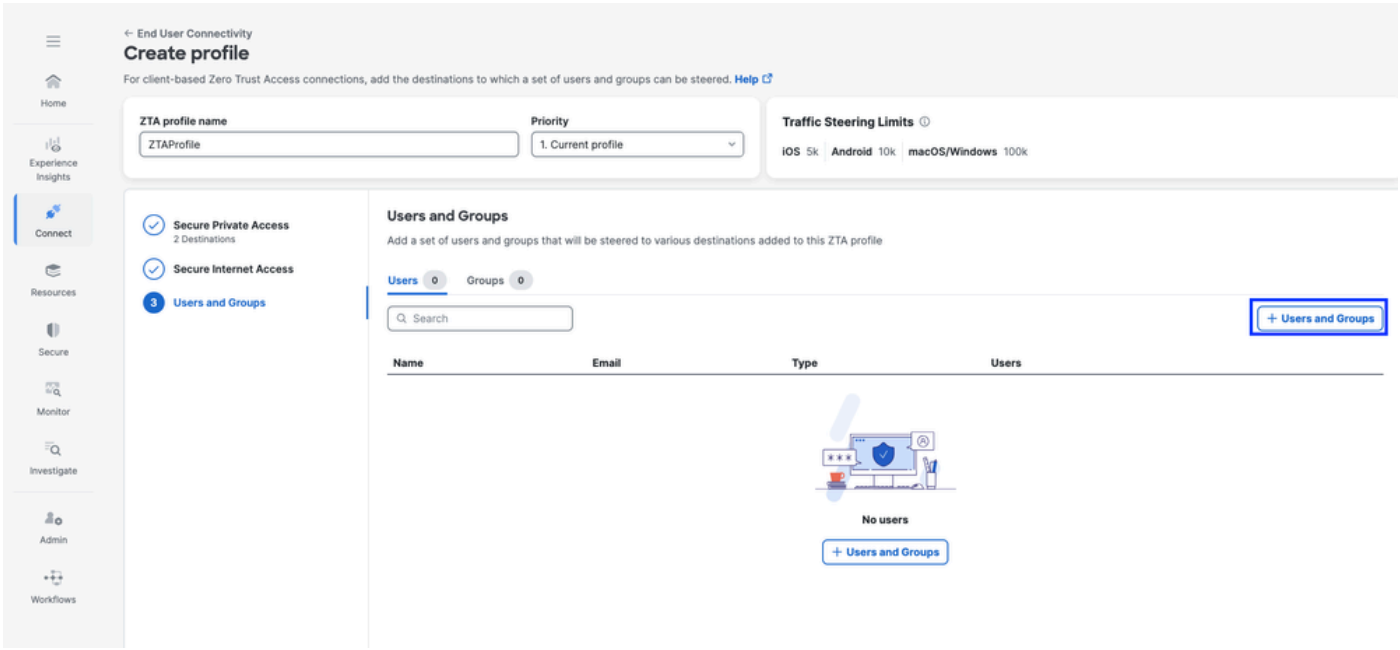


الوصول الآمن - ملف تعريف ZTA

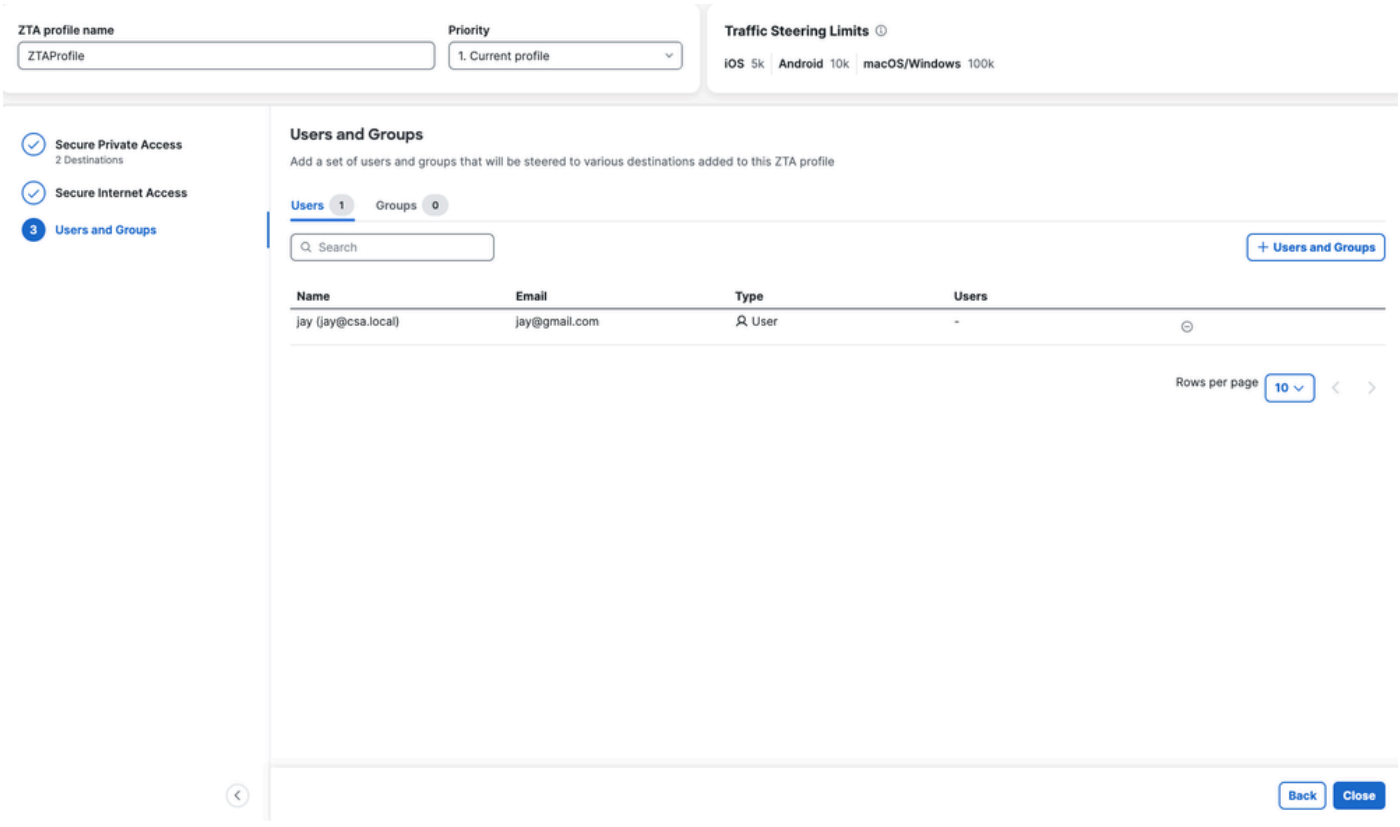


الوصول الآمن - ملف تعريف ZTA

3. إضافة مستخدمين ومجموعات



الوصول الآمن - ملف تعريف ZTA

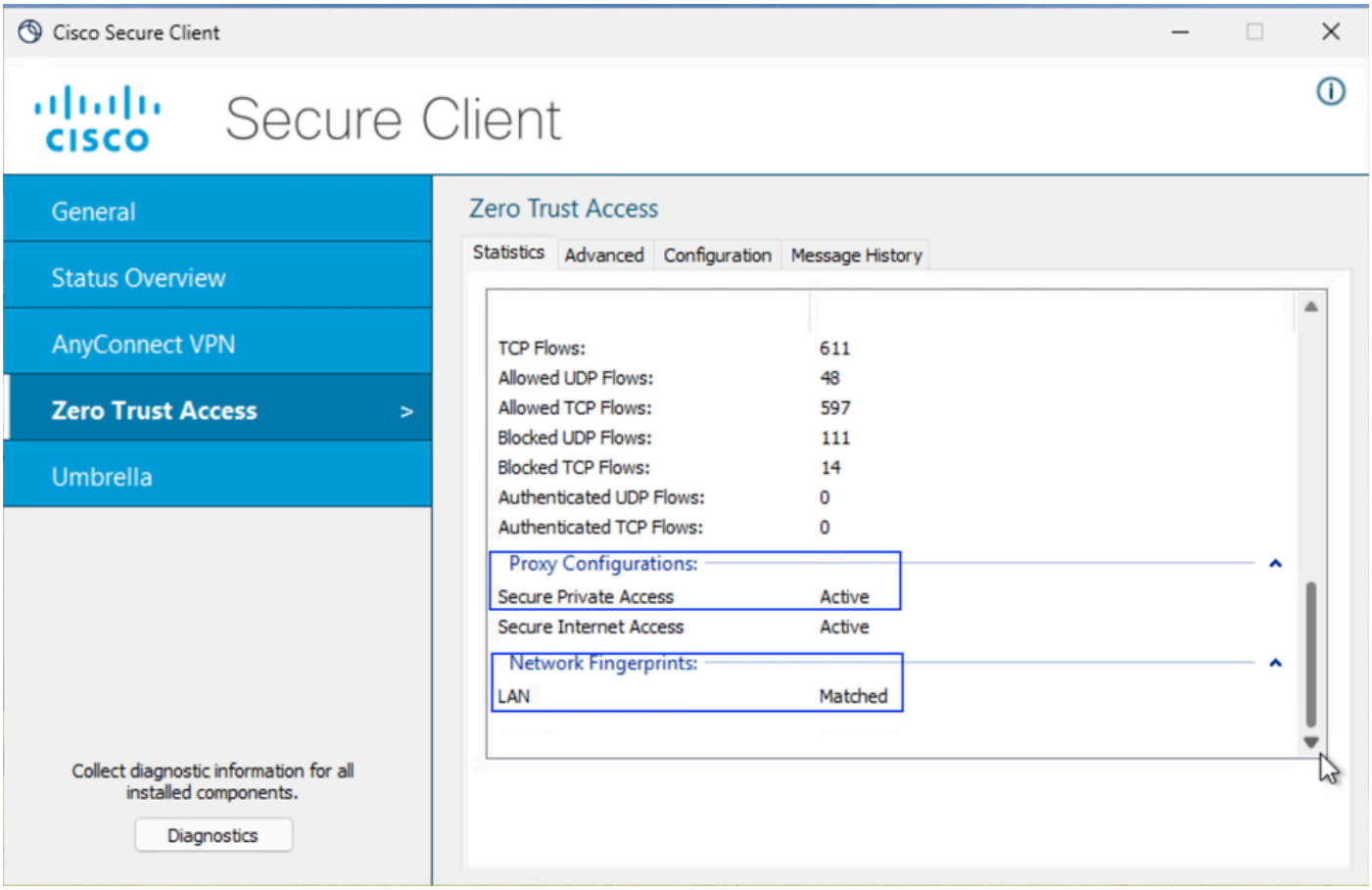


الوصول الآمن - ملف تعريف ZTA

الخطوة 6 - التحقق من الوصول إلى المورد الخاص

عندما يكون المستخدم محلي

1. تحقق من بصمة الشبكة ل ZTA TND، ويجب أن تتطابق إذا كان المستخدم محلي وآمن
وصول خاص يجب أن يكون نشطا



الوصول الآمن - إختبار العلاقات العامة

2. التحقق من قدرة المستخدم البعيد على حل FTD FQDN

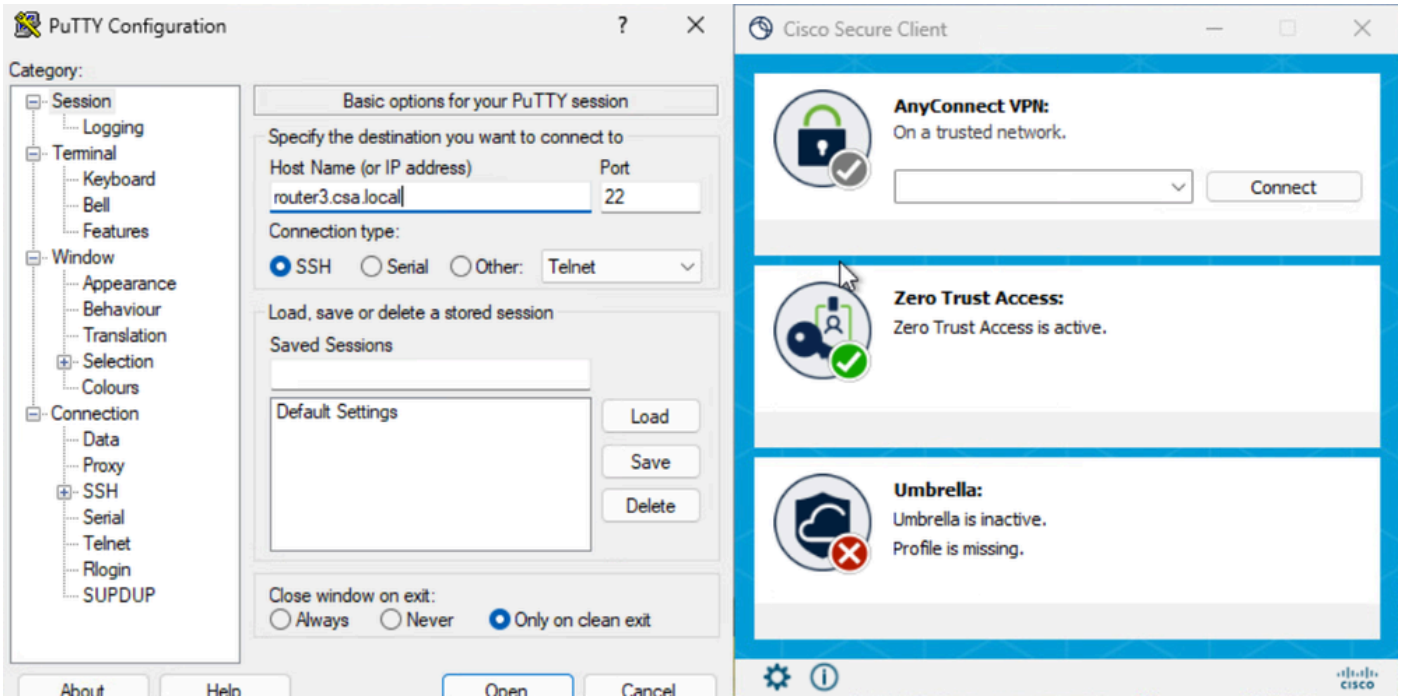
```
C:\Users\jay>ping ftd.csa.local

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. التحقق من إمكانية وصول FTD إلى الموارد الخاصة باستخدام FQDN

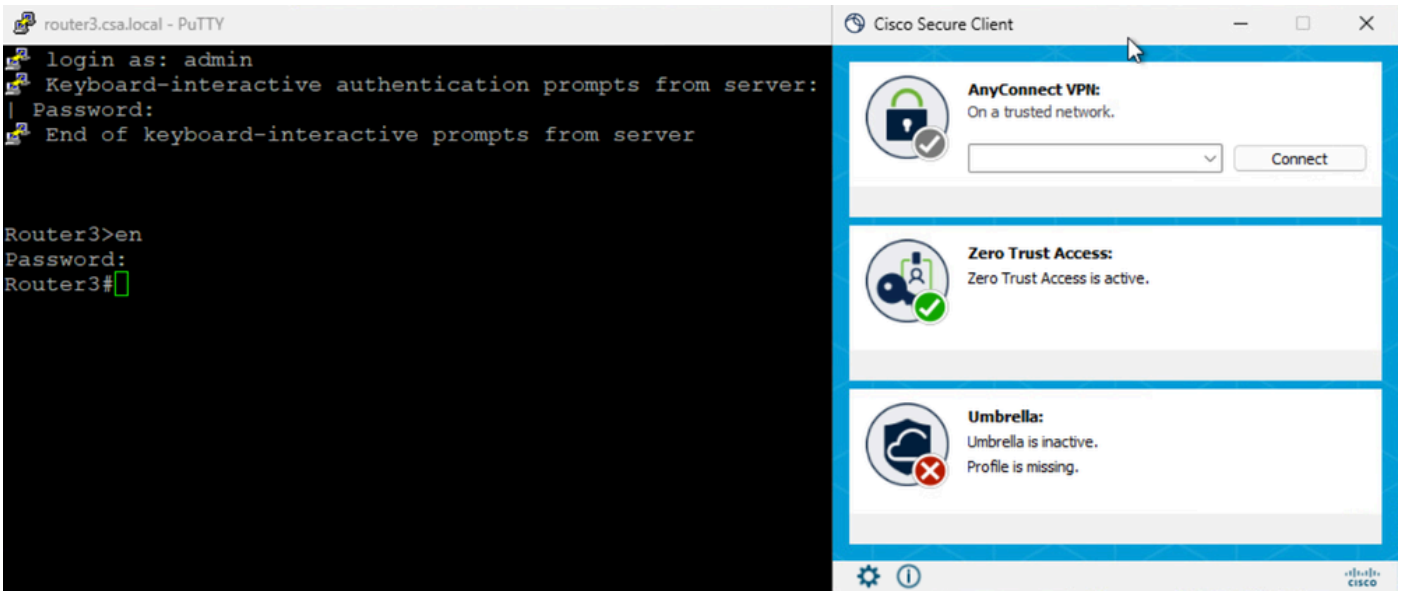
```
ftd# ping router3.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.103, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd#
```


4. إختبار اتصال SSH بالمورد الخاص

الوصول إلى PR باستخدام FQDN

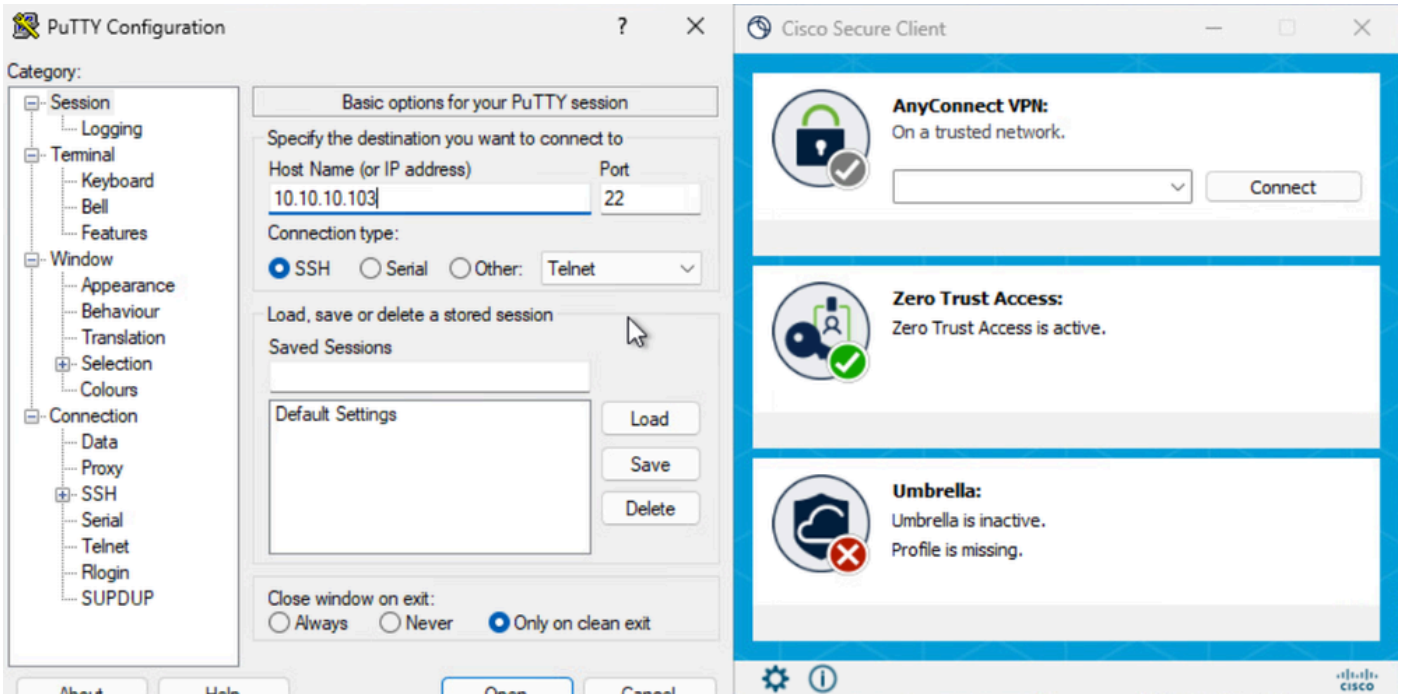


الوصول الآمن - إختبار العلاقات العامة

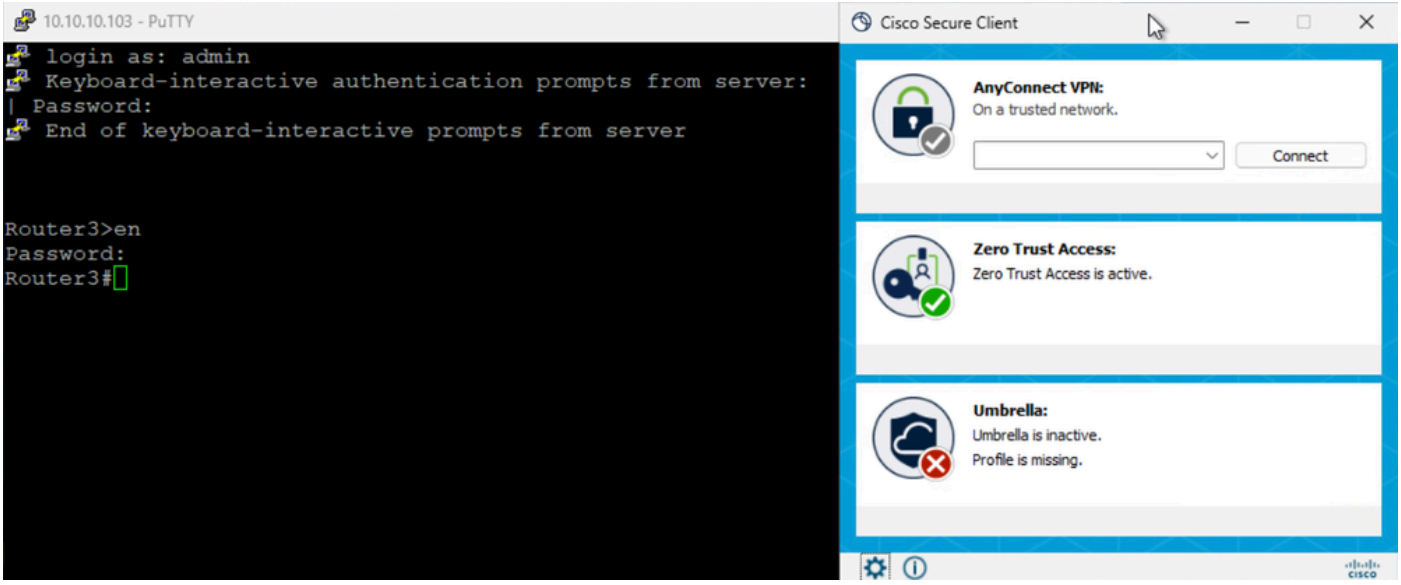


الوصول الآمن - إختبار العلاقات العامة

الوصول إلى PR باستخدام عنوان IP

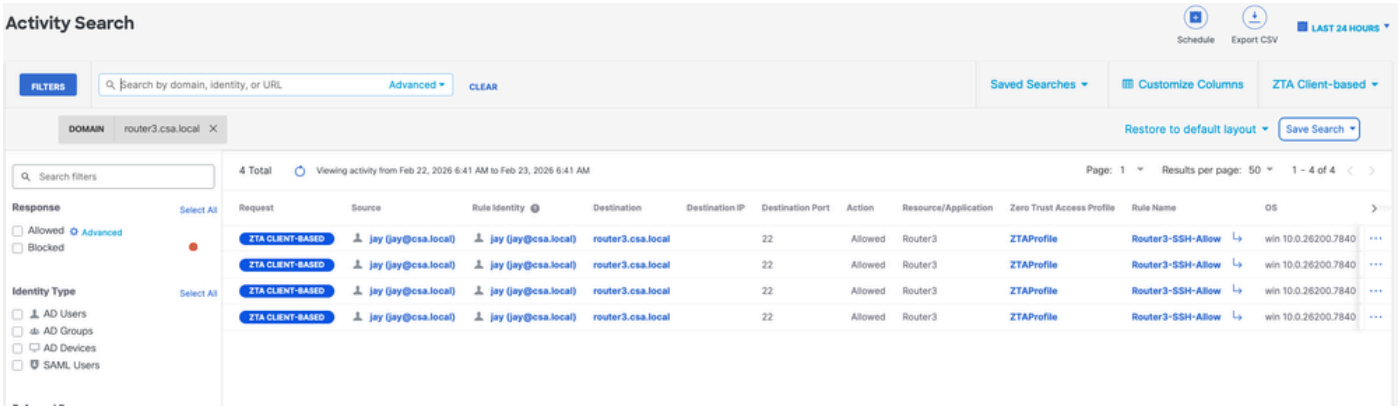


الوصول الآمن - إختبار العلاقات العامة

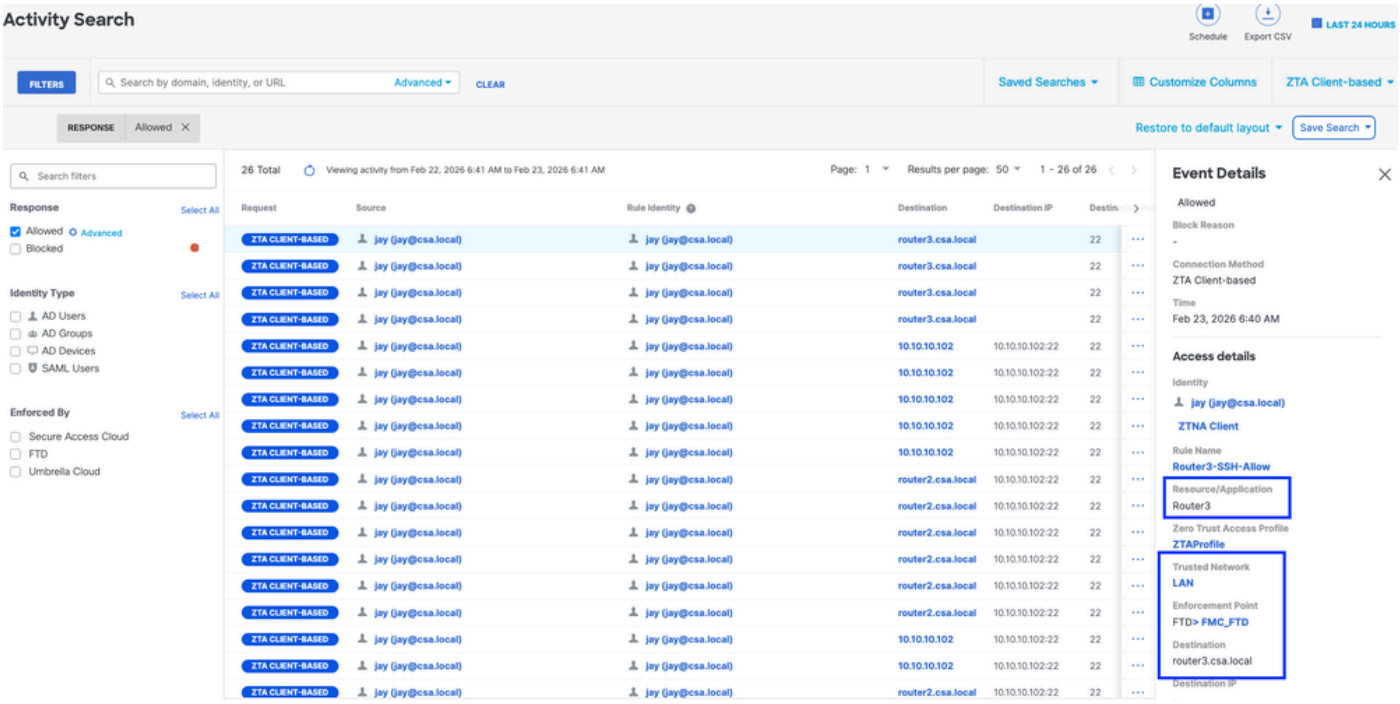


الوصول الآمن - إختبار العلاقات العامة

5. التحقق من سجلات خادم نشاط الوصول الآمن

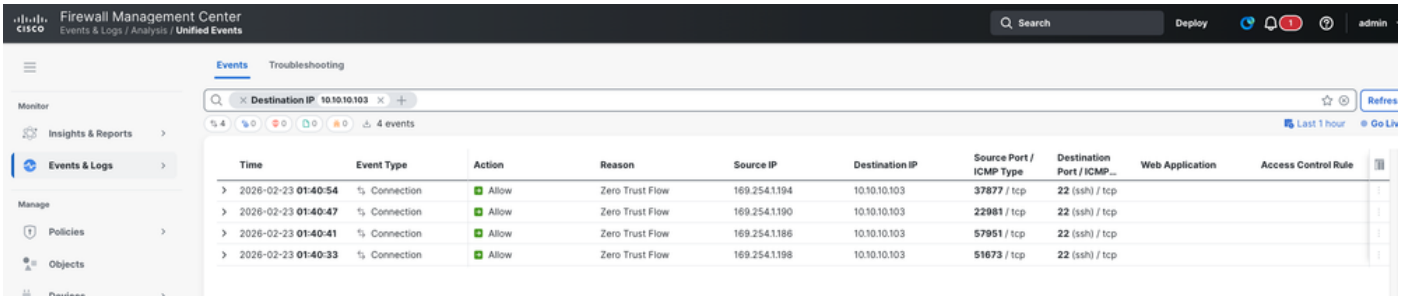


الوصول الآمن - البحث عن الأنشطة



الوصول الآمن - البحث عن الأنشطة

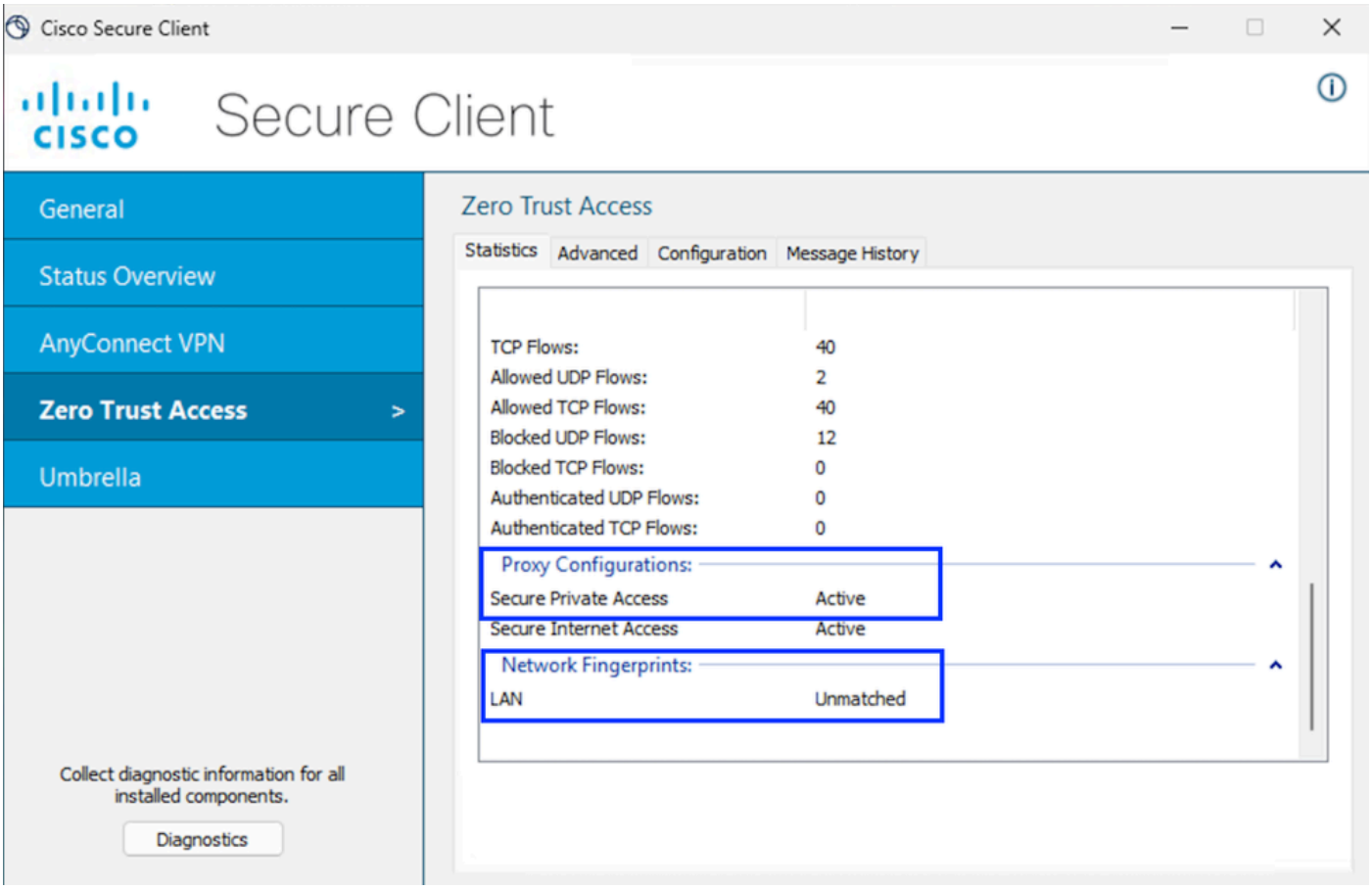
6. التحقق من أحداث اتصال FMC



أحداث اتصال FMC

عندما يكون المستخدم بعيد

1. على سبيل المثال، بصمة الشبكة ل ZTA TND، يجب عدم مطابقتها إذا كان المستخدم بعيد



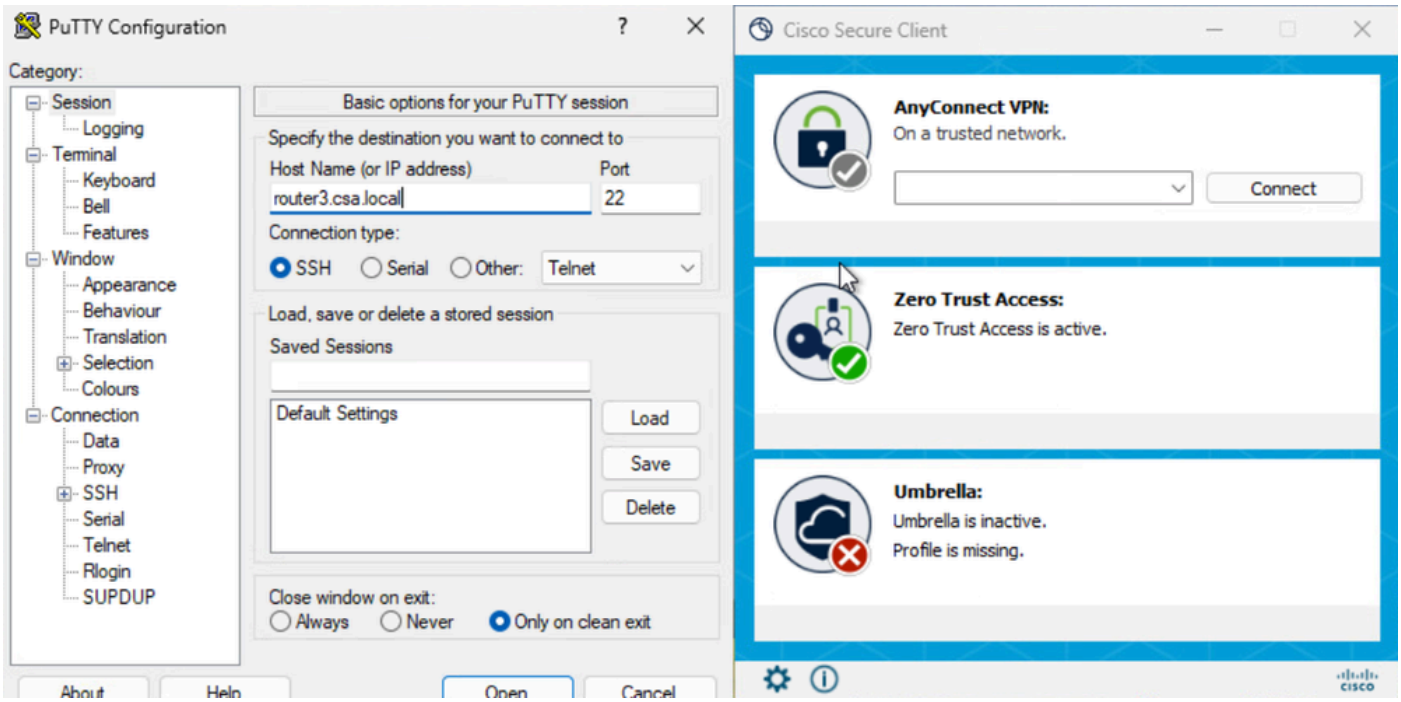
الوصول الآمن - إختبار العلاقات العامة

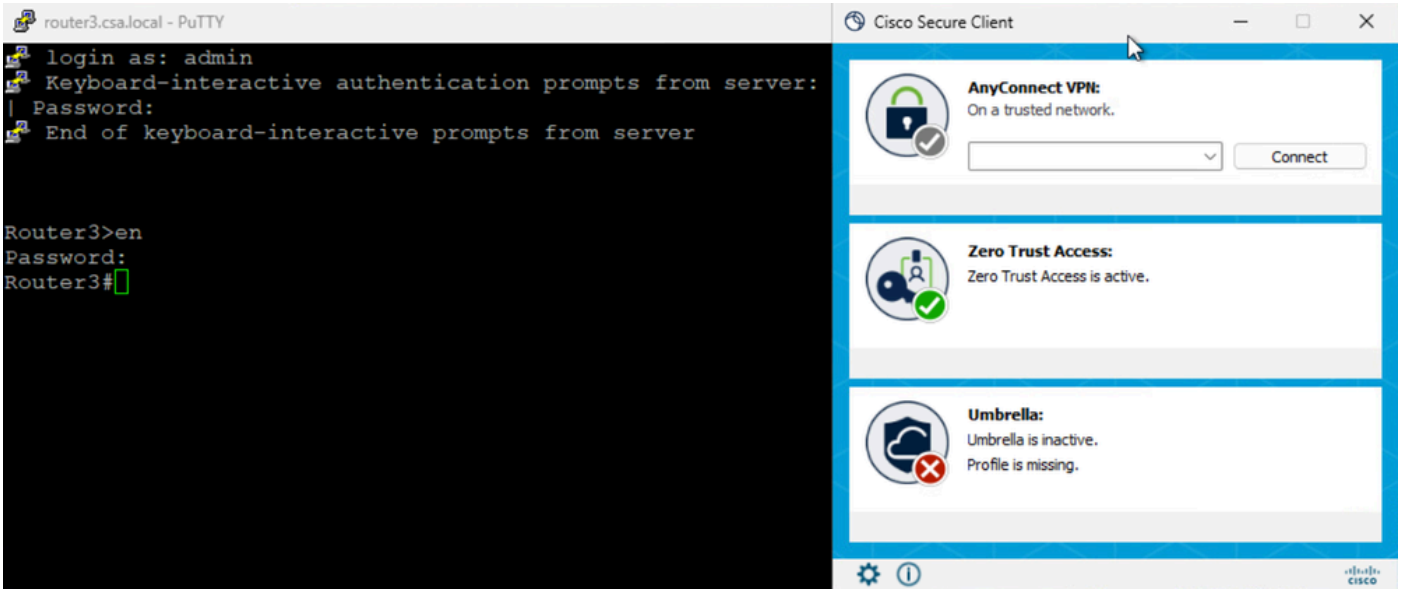
2. التحقق من قدرة المستخدم البعيد على حل FTD FQDN

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

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server:  AD.csa.local
Address:  192.168.1.20

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

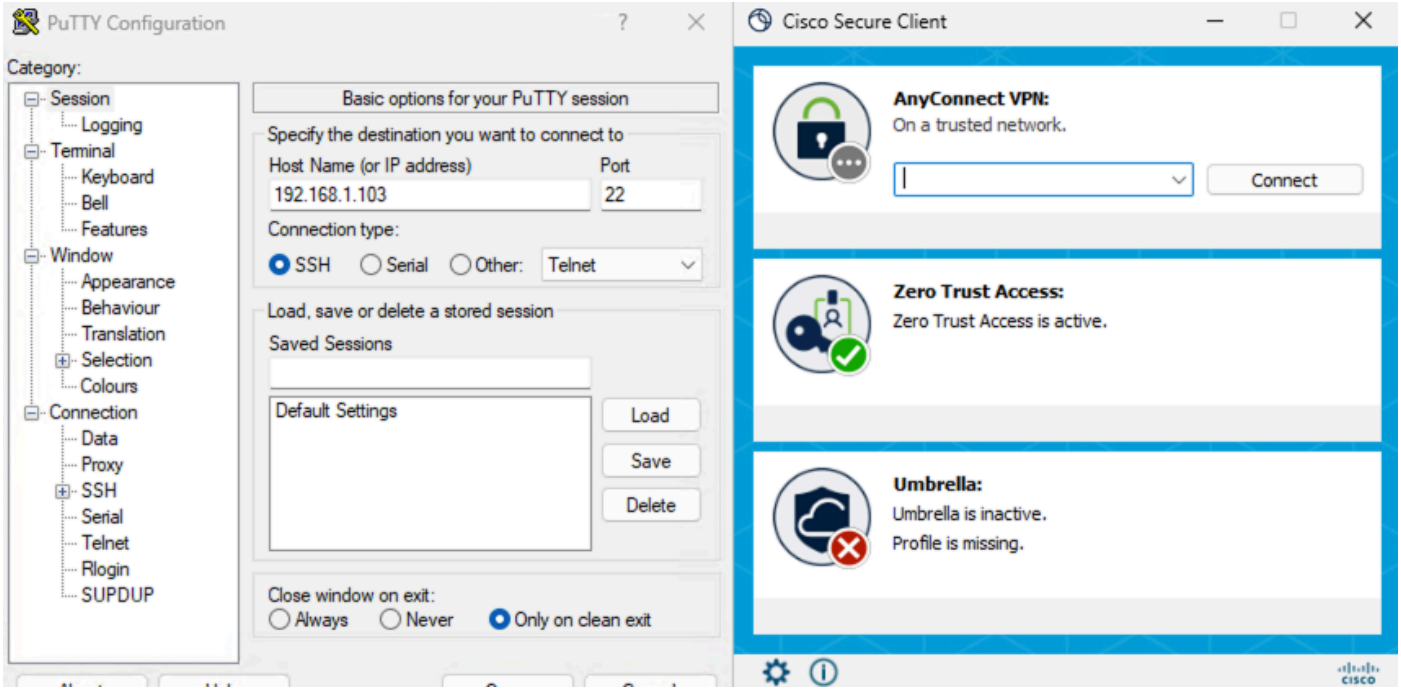

3. إختبار اتصال SSH بالمورد الخاص

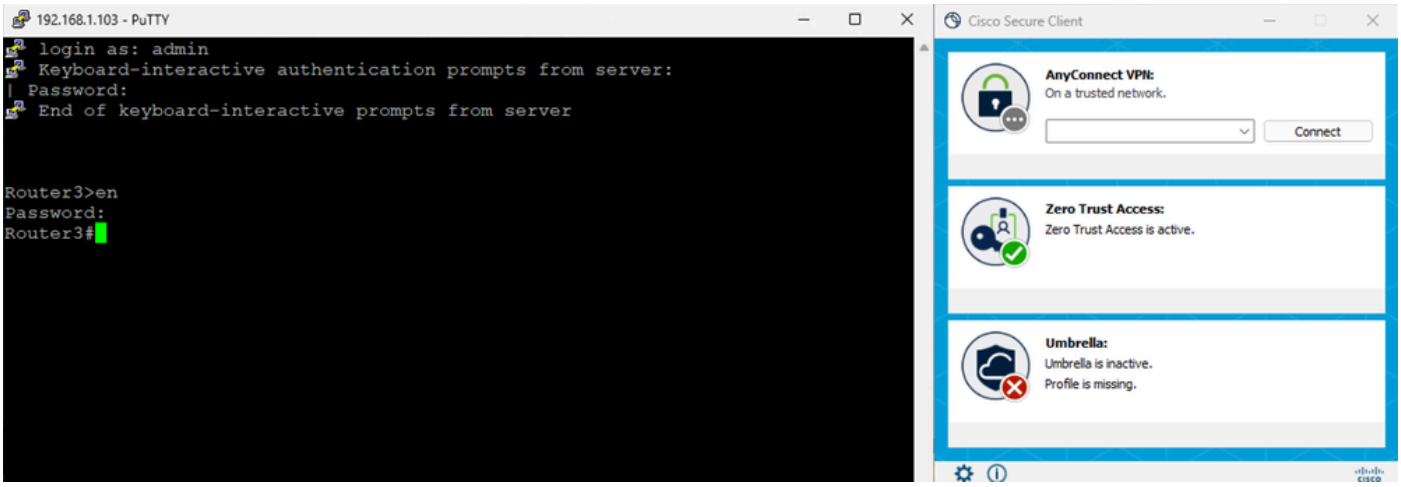
الوصول إلى PR باستخدام FQDN





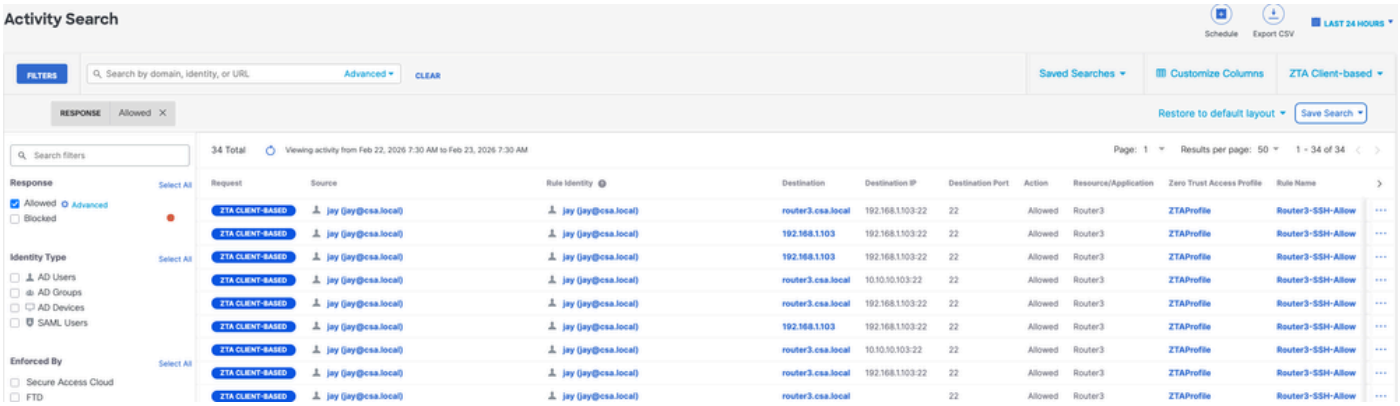
الوصول إلى PR باستخدام عنوان IP



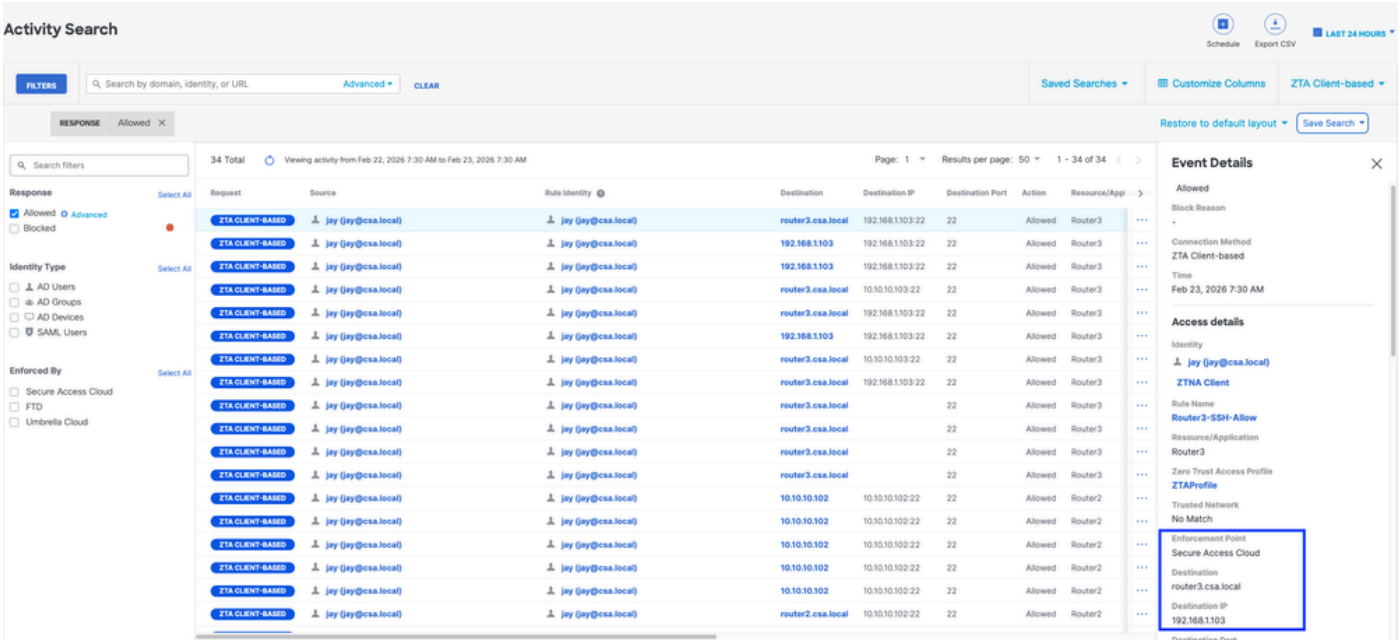


الوصول الآمن - إختبار العلاقات العامة

5. التحقق من سجلات خادم نشاط الوصول الآمن



الوصول الآمن - البحث عن الأنشطة



استكشاف الأخطاء وإصلاحها

أوامر مفيدة:

> إظهار ملف تخصيص المركز
> إظهار فحص برنامج ASP-DP
> sh running-config universal-zero-trust
> إظهار موجز IP للواجهة

> debug universal-zero-trust zproxy 7

وبعدين برنامج على وضع الخبير!

tail -f /ngfw/var/log/messages

إظهار الكل

عرض تفاصيل nat

إظهار أم ذخ جدول ASP

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).