

دراوملا ىلا لوصول ةيملاعلا ZTNA نيوكت نمآلا لوصول ىلع ةصاخلا

تايوتحمل

[ةمدقملا](#)

[ةيساسال تابلطتلا](#)

[تابلطتلا](#)

[ةمدختسلا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةيملاعلا ZTNA لوح](#)

[ةكبشلا فاشكتا](#)

[ذيفنتلا عاونأ](#)

[مادختسالاتالاج](#)

[ةيرامعم تانوكم](#)

[ةمزللقفدت](#)

[نيوكتلا](#)

[ةكبشلا لىطىطختلا مسرلا](#)

[رابتخالالاتالاج](#)

[ةباحسلا ذيفنت - ديعبلا مادختسلا : 1 رابتخالالاتالاج](#)

[يلجم ذيفنت - ديعب مادختسم - 2 ةلاجلارابتخا](#)

[يلجم ذيفنت - يلجم مادختسم - 3 ةلاجلارابتخا](#)

[TND مادختساب ةباحسلا ربع ذيفنت وأ يلجم - دعب نع مادختسم ويلجم - 4 رابتخالالاتالاج](#)

[اوحالص او عا طخالالاتالاج فاشكتسا](#)

[ةديفم زماوا](#)

ةمدقملا

ةيملاعلا ZTNA ربع ةصاخلا دراوملا ىلا لوصول نيوكت دنتسملا اذه في يطغنس
ةفلتخم رورم ةكرح تاراسم مادختساب

ةيساسال تابلطتلا

ماعلا ZTNA نيوكت لبق يلاتلا نيوكتلا لامكإ بجي

- [Cisco Secure Access](#) ىلع ةيوهلا رفوم
- [تاداهشلا مادختساب ةقث نودب لوصول في ةزهجالا ليچست](#)
- [Cisco نم نمآلا ةيماحلا رادج مادختساب قافنالا نيوكت](#)

- [قبرهاظلا ةصاخلا دعب نع لوصولا ةكبش](#)
- [نمألا لوصولا ىلع دراوملا لصوم](#)
- [نامألا ةباحس يف مكحتلا ةزيم ىلع FTD جم انرب چاردا](#)
- ب لصاتا ،صاخلا نمألا لوصولا رجأت سمل ةطلتخملا ZTNA ةزيم ةمالع نيكمت بجي ةمالعل نيكمتل Cisco TAC

تاب لطلتلا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- ةيامحل رادجو Cisco نم نمألا لوصولاب ديدهتلا دض عافدلا ىلع IPsec VPN نيوكت
- Active Directory نم مدختسمل ري فوت - Identity Supply (IDp)
- Cisco Secure Access ىلع دعب نع VPN نيوكت
- Cisco Secure Access ىلع دراوملا لصوم رشن
- ZTA ةداهش ىل دن تسمل ليجستلا
- كذ ىل امو تاداهشلا بالوق وأ CSR عاشنأ وأ OpenSSL - ةداهشلا

ةمدختسمل تانوكملا

ةيلاتلا ةي داملا تانوكملا او جماربلا تارادصلا ىل دن تسمل اذ ه ي ةدراول تامولعمل دن تست

- Cisco (7.7.10 رادصإلا) نم ةيامحل رادج ديدهت دض نمألا عافدلا
- Cisco Secure Firepower (7.7.10 رادصإلا) ةرادإ زكرم
- Cisco Secure Client (ZTA، 5.1.10.1720 رادصإلا)
- Windows 11 ليغش تال ماظن
- ق دصملا عجرملا - Windows 2019 Server
- ESXi ىلع دراوملا لصوم

ةصاخ ةي لمعم ةئي ب ي ةدوجوملا ةزهجال نم دن تسمل اذ ه ي ةدراول تامولعمل عاشنأ مت تناك اذا .(يضا رتفا) حوسم نيوكتب دن تسمل اذ ه ي ةمدختسمل ةزهجال عي مج تادب رما يأل لم تحت حمل ري ثأ تلل كم ه ف نم دكأت ف ، ليغش تال دي ق ك تكبش

ةيساسأ تامولعم

ةيملعلا ZTNA لوح

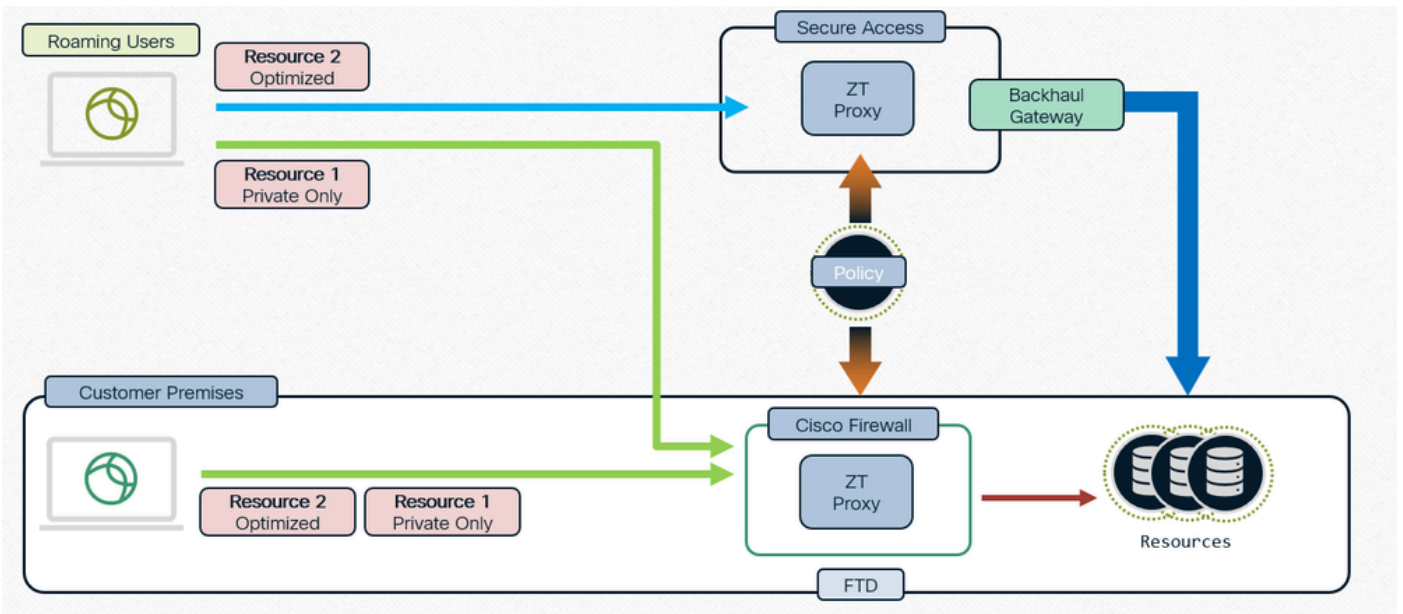
لكشب حامسلا ةينامإ ني لوؤسملل (uZTNA) ةقت نود ةكبشلا ىل يملعلا لوصولا حيتي ةقت كذ ي ف امب) مدختسمل ةيوهل اق فو ةيلخادلا ةكبشلا دراوم ىل لوصولاب ددحم عم لالحا وه امك لم الكلاب ةكبشلا ىل لوصولا قح حنم نودو ،(مدختسمل ةيعضوو مدختسمل

لكل ةيخادلا تاقىببطللاو دراوملا ني مأت ةيناكإ ني لوؤس ملل uZTNA حيتت امك RA-VPN. ني مي قمل او ني دي عبلا ني مدختس مل نم

ىلا لوصولا اي نمض لوخي تاقىببطللا دحلل حونم مل لوصولا نأ ضررت في ال uZTNA نأل ارظن ةكبشللا موجه حطس ليلقت متي، ىرخأ تاقىببطل

متي لوصولا في مكحتلل تاسايس يأ لهجت متي. لوصولا ةسايس Secure Access ميقي نمآلا ةيامللا رادج ةرادا زكرم نم ةزهجالا ىلع اهرشن

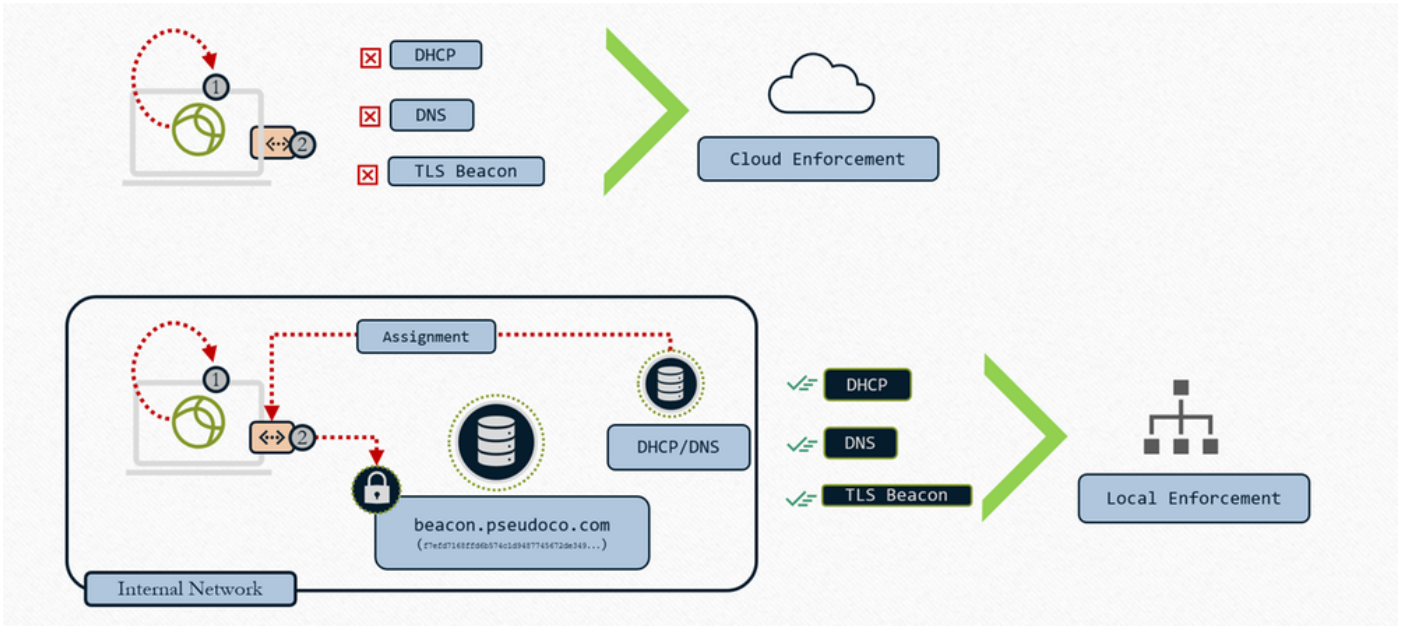
، ةراضلا جماربللاو تافل مل او IPS ةسايس ضرر في لىلا ةفاضلا اب، رورملا ةكرح ليكو ءارجإ متي (FTD) "ةيرانلا ةقائللا ديدهت نع ءافدلا" ىلع



عزوملا قي ببطللا، ةدحاو ةسايس

ةكبشللا فاشتك

يلحمللا قي ببطللا وأ ةباحسلا ديحت



يلحم ل ذيفنتل وأ ةباحسل ديحت - ةيم لال ZTNA

ةكبشل نيوكتل ةيلحم ل ةهجال ليم لال بوجتسي 1-

TLS ةرانم نع ليم لال ثحب تايلمع 2-

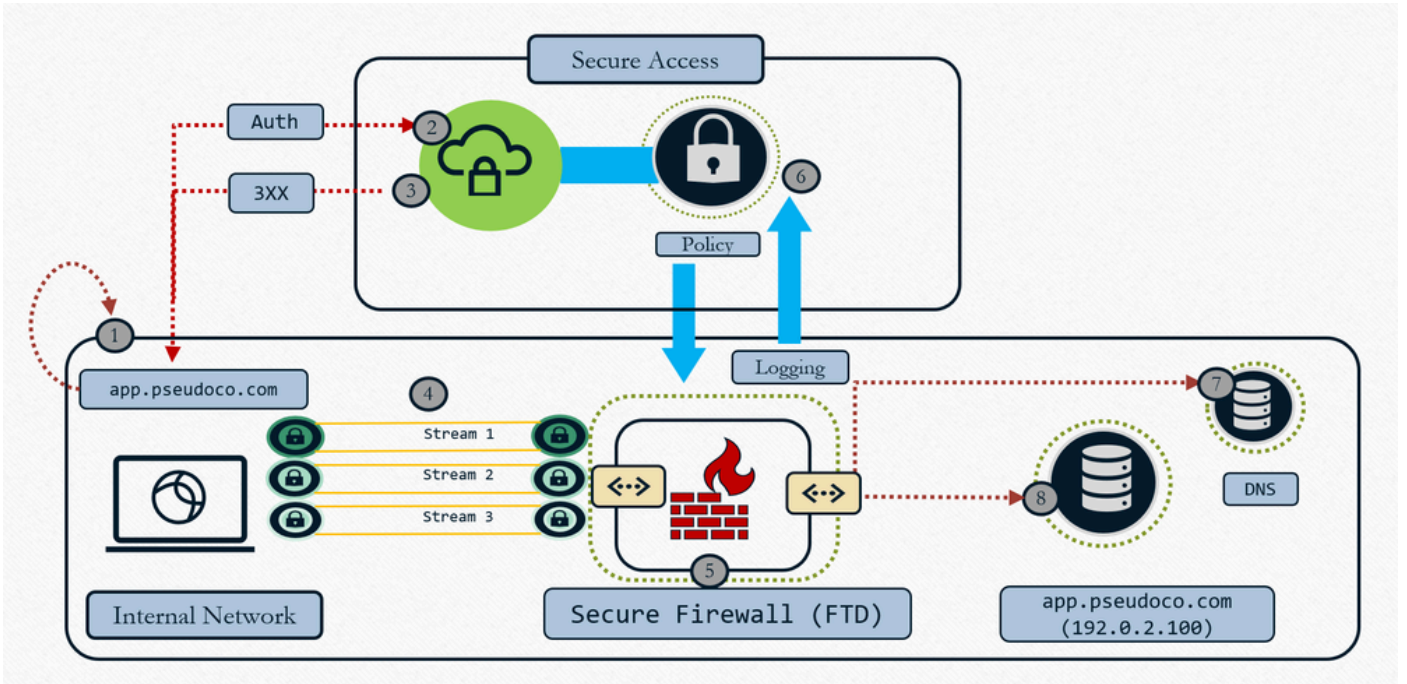
يلحم ل ذافنال - فورظال تقباطات اذا 3-

ةباحسل قيبطت - ةلجال قباطات مدع ةلاح يف 4-

ام نإف، FTD ب TND ةدعاق طبرو "يلحم ل وأ ةباحسل ضرر" مادختساب دروم ل نيوكتل دنع مبيقت نمضتت ليم لال ل اهل اسرا متي يتل ضارعالا دعاق ةعومجم وه لعفلا ب هب موقبي دنع. TND ةدعاق مبيقتل ةباحسل لبق نم هرابخ متي فوس ليم لال اذه، كذلك TND ةدعاق ربخت ثيحب، HTTP سار يف TND ةكبشلال ةمصب مبيقت ةجيتن عرضن، لاصلتال لاسرا كلت ليلكول مدختسي م ثاهب قووم ريغ ةكبش لعلع وأ ليغشت ةلاح يف انك اذا ام ليلكول تامصب تقباطات ةلاح يف. كذلك فو تانايل بال رورم ةكرح هي جوت دي عي و تامولعمل قباطات مل اذاو FTD ل انايل بال رورم ةكرح هي جوت ةداع ليم لال نم Zproxy بلطي، عبالا [لوصول نيوكتل](#) عجار. ةباحسل ل انايل بال رورم ةكرح هي جوت دي عي هناف عبالا تامصب [اهب قووم ل ةكبش لال فاشتك اعم ةقث نودب ةكبش لال ل](#)

ذيفنتل عاونأ

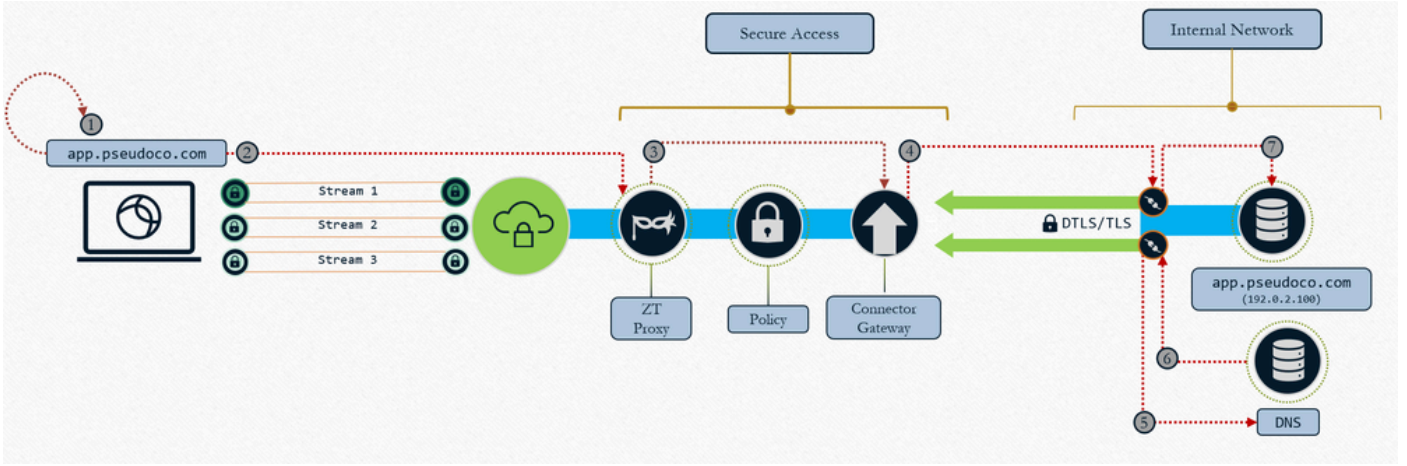
• يرانل رادل ذيفنت: يلحم ل ذافنال راسم



يحلحمل ذافنإلإ - ةيملاعأل ZTNA

1. فيضمال قاطن) تقؤمأل IP إىل بلطال لصفيو ليملعأل طقتلي، مدختسمل بلط (يحلحمل)
2. مبيقتل نمأل لوصولو ةباحس إىل ةقداصمأل يف مكحتل رورم ةكرح لاسرا متي ةسايسلا
3. تحتس اذإ) تانايبال ةطخ قيبتل FTD إىل اههيجوت ةداعإ متي ةباحسلا تاغجترم (ةسايسلا)
4. ةيامل رادجل انهنيوكت متي تال ثبلال لابقتسال ةدحو إىل رورم ةكرح هيجوت مت (ههاول)
5. (ريفتل كفو، ةراضال جاماربلالو، IPS) ةباحسلا يف فرعملال جهنللا صرف متي يحلحمل ليكولال تانايب يوتسم مادختساب
6. قستم ريراقت دادعإل ءارظنللة وومجم إىل رركملاو لجسملال شدلناحش مت
7. ناك اذإ) دراومال رورم ةكرح هيجوتل ةيحلحملال ةكبشلال إىل DNS لحب ةياملال رادج موقوي (اومسم)
8. رادج فرصتي شيح (دروملل هؤاشنإ مت ديدج لاصتال) دروملاب لاصتال ةياملال رادج ينب ي TCP لوكتوربل ليكوك ةياملال

• ةلصتمل ريغ ةكبشلال : ةباحسلا ذيفنت راسم

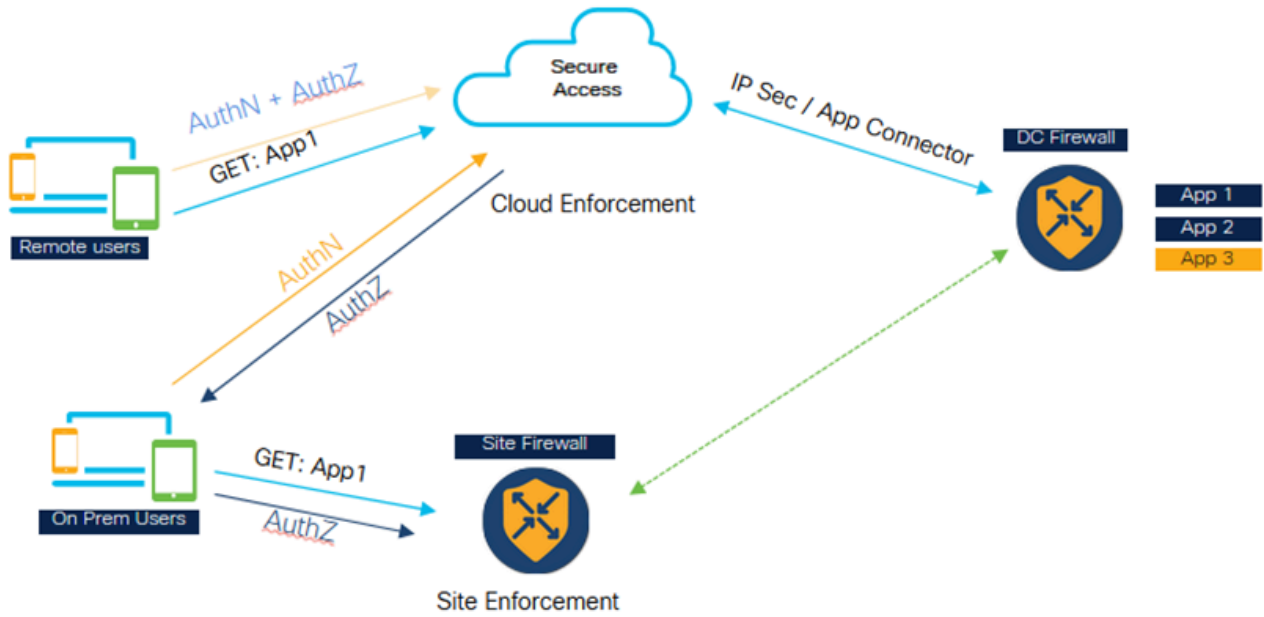


ةبأحسلا ذيفنت : ةماعلا ZTNA ةيفنقت

1. فيضم القاطن) تقؤملا IP لىإ بلطلا لصفيو ليمعلا طقتلي ،مدختسملا بلط (يلحملا
2. نمآلا لوصولا يف ةقثلا مادعنا لىكو لىإ رورملا ةكرح لقن متي
3. ضرر متيو ،هنيعت مت يذلا دراوملا لصوم لىإ هؤاشنإ متو TCP لاصتلا لىكومت رورملا ةكرح لىلع جهنلا
4. دراوملا لصوم ب لاصتالا ةباوبلا ددحت
5. دروملل IP دي دحتب دراوملا لصوم موقى
6. دروملل IP مادختساب ةيلحملا DNS بي جتست
7. دروملاب لاصتلا ءاشنإب دروملا لصوم موقى

مادختسالاتالاح

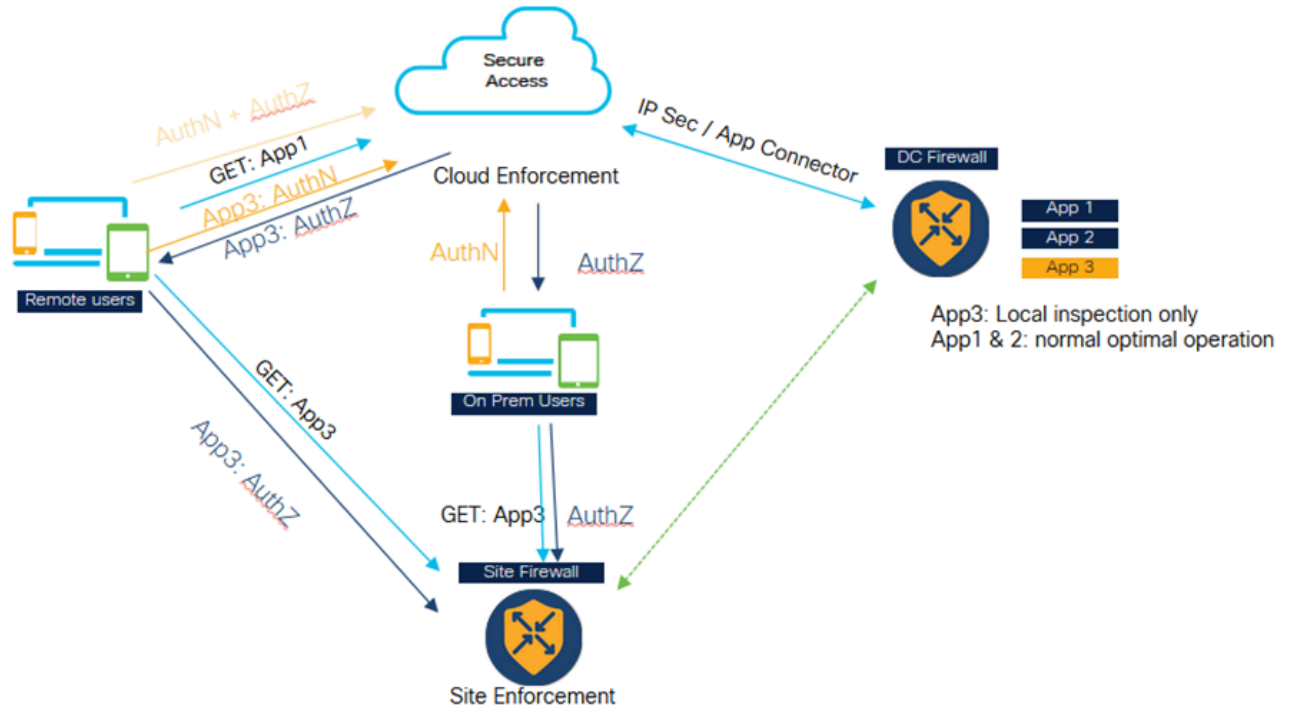
لئغشتلا دنع نيمدختسملل ةنسخملاو ةقسانتملا ZTNA: 1 ةلالا



(يحلج مدختسم) ن سحم و ق س ان تم ZTNA - ة م ل اع ل ZTNA

- ق ي ب ط ت ل ة ي ا م ح ل ر ا د ج و ن م آ ل ل و ص و ل ا ن م ل ك ن ي و ك ت م ت
- ه ص ح ف و ج ه ن ل ا م ي ي ق ت ل " ن م آ ل ل و ص و ل ا " ل ي ل ا ب ه ذ ي س ف ، د ي ع ب م د خ ت س م ل ا ن ا ك ا ذ ا
- ل ع ش ي ت ف ت ل ل ة ي ا م ح ل ر ا د ج ل ا ل ا ق ت ن ا ل ا م ت ي س ف ، ي ل خ ا د / ي ل خ ا د م د خ ت س م ل ا ن ا ك ا ذ ا ة ص ا خ ل ر و ر م ل ا ة ك ر ح
- ش ي ح م ي ي ق ت ل ا و ة ق د ا ص م ل ل ن ا م آ ل ا ل ا ل ا ق ت ن ا ل ا ع ق و م ل ا ي ف م د خ ت س م ل ا ن ا ك م ا ب ل ا ز ي ال ن ي و ك ت ل ا ق ف و ا ه ص ح ف م ت ي و ة ي ا م ح ل ر ا د ج ل ا ل ا ن ا ي ب ل ا ت ا ن ا ي ب ر و ر م ة ك ر ح ل ق ت ن ت ج ه ن ل ا
- ء ا د آ ل ا ة ز ي م ب ة ي ا م ح ل ر ا د ج ل ا ل خ ن م ق ي ب ط ت ل ا ل ا ل ص ي ي ذ ل ا ي ل خ ا د ل ا م د خ ت س م ل ا ع ت م ت ي ز ك ر م ل ا ل ا ل ق ن ل ا م ت ة ب ا ح س ل ا ل ا ل ق ت ن ت ي ت ل ر و ر م ل ا ة ك ر ح ب ن ج ت ل ع ل م ع ي ش ي ح ف ل خ ل ن م ت ا ن ا ي ب ل ا

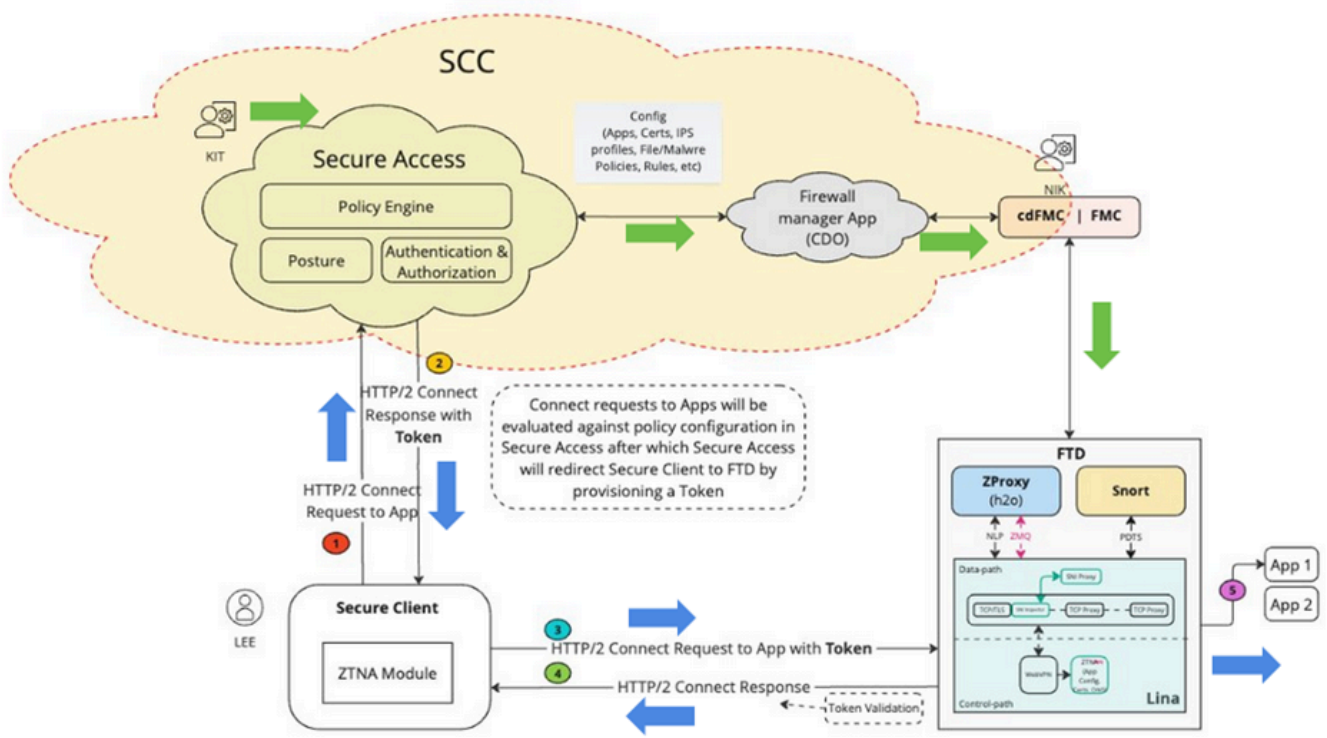
ة س ا س ح ل ا ت ا ق ي ب ط ت ل ا ل ع ص ا خ ل ا ش ي ت ف ت ل ا : 2 ة ي ض ق ل ا



أساسيات تقييد الوصول - سياسة الوصول ZTNA

- راجع لال دخول نم امئاد اهيلي لوصول نكمي شيحب ةماهال تاقيدببطلالضعب نيوكت نكمي ةياملال.
- لالاملاليلبسيلع . ةباحسلاليلالاقتنالاليلالقيببطلالانايبرورم ةكرجاتالال ال يذالو ، ردمالال ةيجمربال تاميلعلالال لثم ساسح تانايب قيببطلالكانه نوكي دق ءارظنالال ةومجميلالاقتنالاليلاليمعلالباغري.
- راجع ربع امئاد رشابلالو ديعلالمدختسملال رورم ةكر رمت ، تاهويرانيسلالهذه لثميل ميبقتو ةقداصلالشدحت ، ويرانيسلالاذهيل ، يرخأ ةرم ، كلذعمو . اهلصف متيو ةياملال ةياملال راجع ربع طقف تانايبالعز رورم ةكر رميو ، ةباحسلاليلالامئاد ةسايسلال

ةيرامعم تانوكم



ةيرام عمل تانوك مل - يملع ال ZTA

يتل ال لولوال ةزيم ال يه uZTNA. ل حل يساس ال ريدمل الوه Security Cloud Control (SCC) قوف اهؤاشنإ م تي

ري فوت درجم ب. ةيامل رادج و نم ال لوصول ةقيقدل ةاقيبطتل نم نانثا انيدل ، SCC ي لعل ةقيقدل ةاقيبطتل هذه ةيؤر نم نكمت نس ، ةبولطم ال ةزيم ال تامال ع نيكمت و SCC ةحول نم رسي ال بانجال

Zero Trust ال لوصول ةدحو ني نكمت انيل ع ني عتيس ، "نم ال لي عمل" ي : نم ال لي عمل ال نوكتل ZTNA ةدحو ي ف لي ج ستل ال ال ج اتحن شج ، (ZTNA) ةقت ال ع ض خ ال ال ي ت ال (ZTNA) ةاقيبطتل ال لوصول ال ع ةرداق

ZT ليلي و لي غ شت ب FTD موق ي . ةاقيبطتل هذه FTD ي محي : يران ال رادج ال ديدهت دض ع ا ف دل ال Secure Access Cloud ي ف ليلي و ال لي غ شت لثم) H2O م ساب اضي ا فورعمل ال

Secure Access micro ةي ب ط ل و ح ة سايس و صا خ دروم ني و ك ت ب (KIT لثم) م د خ ت س م ال موق ي ا م د ن ع ن ال م ه ف ي SCC. ةي ا م ح ال رادج ر ي غ ص ال ال ني و ك ت ال ا ذ ه ع ف د م ت ي س ، Secure Access micro ه ت ر ا د ا و ني و ك ت ال ر ش ن ة ي ف ي و ، FTD و FTD ني و ك ت ال ةي ل خ ا د ال ر ص ا ن ع ال ةي ا م ح ال رادج ةي ب ط ت ا ه ا و ا ع ا د ت س ا ب موق ي و ، ني و ك ت ال ا ذ ه نم ةي ا م ح ال رادج ةي ب ط ت ق ق ح ت ي ، ك ل ذ ل FTD. لعل ف ا ط م ال ةي ا ه ن ي ف ه ر ش ن م ث FMC ال ني و ك ت ال ع ف د ل FMC ةاقيبطتل ةج م ر ب ر ط ض ي ال ش ج ب ه ن ي ك م ت م ي ذ ل ا ي ئ ا ق ل ت ال ر ش ن ال ر ا ي خ ال ع ف T D ي و ت ح ي ن ا ن ك م ي . ي و د ي ال ر ش ن ل ا ب م ا ي ق ل ل (ك ي ن لثم) ن و ل و و س م ال

Secure ب نم آلا ليمعلا لصتي ، قيبطت لى لوصول (يل لثم) مدختسم لواحي ام دنع . 1. زاهج ةداهش مادختساب مدختسم ل Secure Access قداصي . mTLS ةانق مادختساب Access كذل اهنوكت مت يتل اىر آلا تاسايس لاولا ةيعضولاولا ليوختلا ميقى هناف مئ نم و . ليمعلا قيبطتلا كذلوم مدختسم ل

موقى هناف ، ةيماحل رادج ةطساوب يمحم قيبطتلا نأ اريخأ هل نيبت اذا ، Secure Access . 2. هل صخرمو لعف لاب هتقداصم مت اذه نأب ةيماحل رادج ربخي يذلاو ، زيمم ةقداصم زمر عاشناب Secure Access ةطساوب عقومو ، زيمم ل ةقداصم ل زمر ريفشت متي

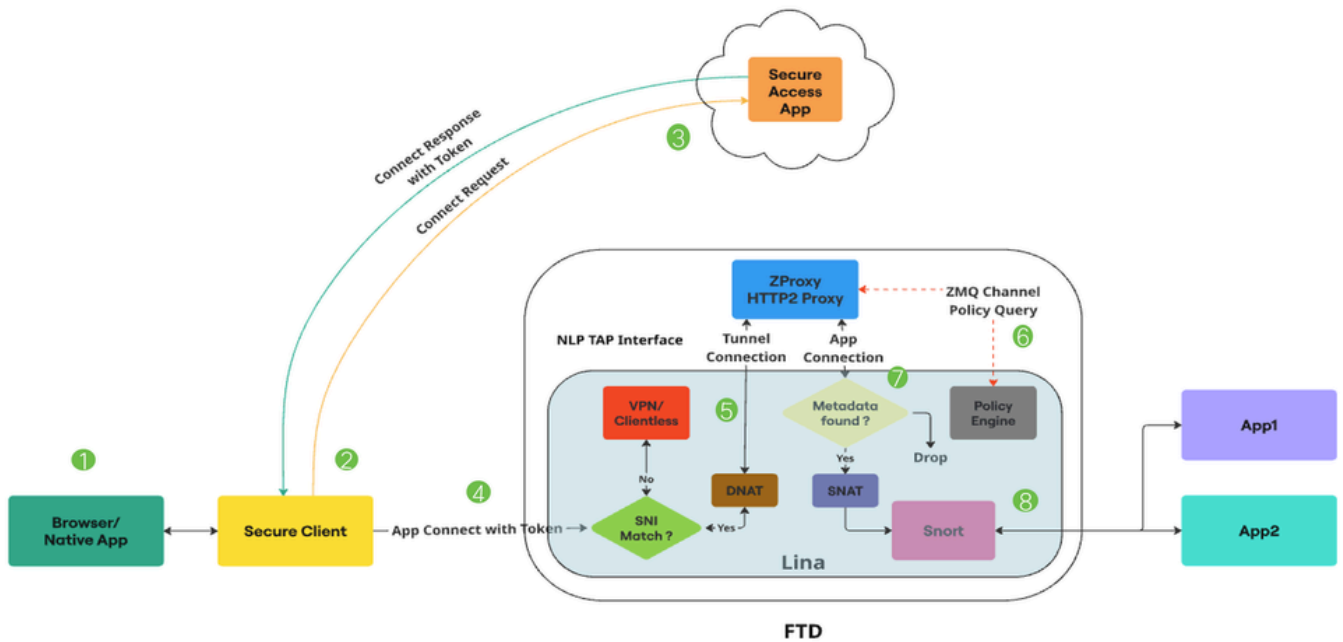
3. ةقداصم ل زيمم ل زمر ل عم FTD وحن نم آلا ليمعلا هيحوت Secure Access دي عي .

4. هنا . mTLS ةانق ربع HTTP2 لاصتا وهو ، FTD ب رخأ لاصتا عاشناب Secure Client موقى . زيمم ل زمر ل عم هي لوصول متي يذلا قيبطتلا ل لاصتا بلط لسري

5. زيمم ل زمر ل ةحص نم ققحتلا مت اذا ، زيمم ل زمر ل ةحص نم ققحتلا نألا FTD موقى . لاسر ل اجم انرب موقى كذل دعبو . قيبطتلا كذل لوصولاب مدختسم ل حمسي ، حاجنب نم آلا ليمعلا لى لى رخأ ةرم رارق ل لاسراب (FTD) ةعرسلا قئاف

ةمزحلا قفدت

يمعلا لى لى صفتلا ZTNA مزح قفدت



ةمزحلا قفدت - يمعلا ل ZTA

1. يلى صأ قيبطت وأ بيوح فصتم لالخنم قيبطت لى لوصولا مدختسم ل لواحي .

2. صاخ دروم ىلإ لوصولو لواحې مدختسمك هفرعيو لاصلتالا "نمآلا ليمعلا" ضررتعي .

3. ىلإ لوصولو بلطو ،نمآلا لوصولو mTLS لاصلتا عاشناب نمآلا ليمعلا موقوي .
عضولا تافيصوتو ةيملاعلا ZTNA تاسايس صحفب Secure Access موقوي .قيبطتلا
لوصولو زيمم زمر عاشناب Secure Access موقوي ،ماري ام ىلع عيش لك ناك اذا .قفاوتلل
جهنو قيبطتلا لىصافتو مدختسملا لىصافت لثم ةيساسا تامولعم ىلع يوتحي
IPS/File.

4. Secure موقوي مث . Secure Access ةطساوب هعيقوتو لوصولو زيمملا زمرلا ريفشت متي .
FTD ىلإ زيمملا زمرلا عم نمآلا ليمعلا هيجوت ةداعاب Access

5. مسا ناك اذا ام ققحتي و لاصلتالا SNI ققدم ضررتعي ، Lina تانايب ىلإ ةمزحلا لوصولو دنع .
اذا .زاهجلا ىلع هنويكت مت يذلا ليكولل FQDN قباطي ليمعلا "ابحرم" يف (SNI دادتما) مدخال
ىلإ لاصلتالا هيجوت متي ، SNI قباطي مل اذا . ZProxy ىلإ لاصلتالا هيجوت متي ، SNI قباطت
ةيملاعلا ZTNA عم شيعتت نأ نكمي رخأ تازيم .

متيس . ليمع ىلإ جاتحت ال يتللا ZTNA وأ Captive Portal و VPN :لاثملا لىبس ىلع
ىلإ LINA ريغ ةيملاعك FTD ىلع HTTP/2 لوكتورب ربع MASQUE معدي يذلا ، ZProxy لىغشت
رورم ةكرح ةجلاعمل ، NLP TAP ةهجاو ZProxy و Lina نياب لاصلتالا مدختسي . ةصصخملال يونلا
SNI ققدم ةطساوب TAP ةهجاول IP ىلإ لاصلتالا ةهجاول IP ةمجرت متت . تانايبلا

6. ةداهش نم ققحتي هناف ، "نمآلا ليمعلا" نم mTLS قفن لاصلتا ZProxy لىبقتسي ام دنع .
زيمملا لوصولو زمر لاسرا نم ققحتي امك . "نمآلا ليمعلا" نم ةلسرملال ليمعلا زاهج
يساسا لكشب همادختسا متي . ZProxy و Lina نياب MQ ةانق دجوت ال . APP لاصلتا مادختساب
قيرط نع ةصاخلا دراوملل FQDN لجل ةانقلا هذه ZProxy مدختسي . مكحتلا لئاسر لدابتل
Lina ب لاصلتالا

ىلإ لوصولو زيمملا زمرلا يف ةدوجوملا تامولعملال معدل اضيأ Zero MQ ةانق مادختسا متي
لوصولو زمر تامولعملال Lina ىقلتت (كلذ ىلإ امو ةيساسالال فرعمو ةدعاقلا فرعم : لاثم) . Lina
فيعرت تانايب ةدعاق يف اهنزختو زيمملا

7. نأ نكمي . صاخلا دروملل ديج لاصلتا عاشناب يف ZProxy أدبت ، مكحتلا لئاسر لدابت درجمب .
قيبطتلا لاصلتالا db فيرعت تانايب شحب ءارجاب LINA موقوي كلذ دعب . UDP و TCP اذه نوكتي
لاصلتالا طاقسا متي ، فيرعتلا تانايب ىلع روثعلا متي مل اذا . اذه

8. لىبس ىلع) يلىخاد IP هل نوكتيسف ، ZProxy نم أشنم قيبطتلا لاصلتا نأ امب .
FTD ، ب ةصاخلا جورخلا ةهجاوب صاخلا IP ىلإ اذه ةمجرت متتس . IP رصمك (169.251.1.2 :لاثملا
يف طقف SNORT صحفل Universal Zero Trust تاقفدت ميلعتب Lina موقوي مث . اهالاسرا لىبق
مت يذلا ةدعاقلا فرعم ريرمت متي . لوصولو زيمملا زمرلا يف IPS جهن وأ فلم دوجو ةلاح
لاصلتالا فيرعت تانايب يف Snort ىلإ لوصولو زيمملا زمرلا نم هيلع لوصوللا

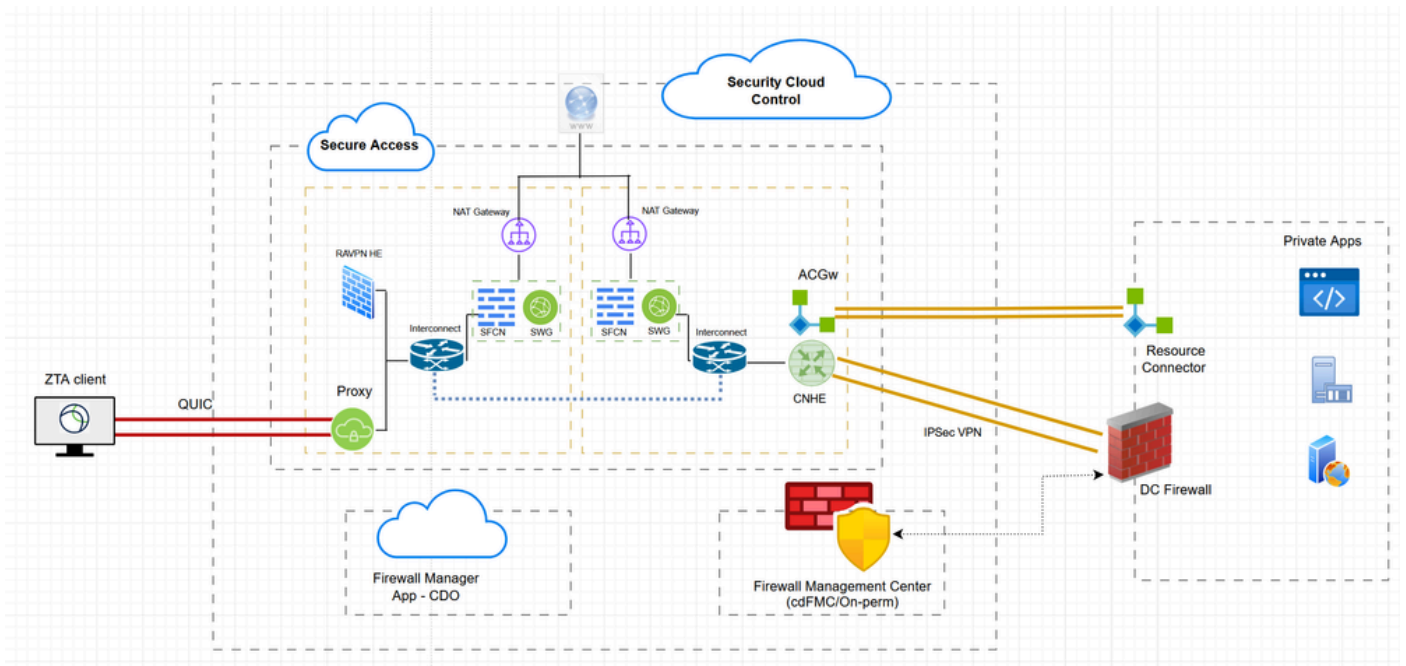
9. ةلباقملا IPS و تافللملا ةيساسا تانييغتو ةيملاعلا ةيفرصلال ةقثلا دعاقو عفد متي .

دعاوقلا هذه لي محتب Snort في "ةقثلا مدع" يفاضلا نوكملا موقيس. FMC ربع FTD لى لى
 طبق SNORT Inspection ل Universal Zero Trust تاقفدت مي لعتب Lina موقيس. ةئيهتلا ءانثأ
 لوصولاً" نم هيلع لوصول مت يذلا لوصولل زيمملا زمرلا في IPS وأ "فلم" جهن ركذ ةلاح في
 صاخلا دروملا اذ لى لوصول "نمألا

ربع Snort لى لوصولل زيمملا زمرلا نم هيلع لوصول مت يذلا ةدعاقلا فرعم ريرمت متي
 يفاضلا نوكملا موقيس، Universal Zero Trust قفدت تاقفدت عيمجل ةبسنلاب. CONN META.
 نم هيلع لوصول مت يذلا ةدعاقلا فرعمل ةدعاقلا نع شحب ءارجاب Snort في Zero Trust ل
 قيبطت متيسو، قفدتلاب حامسلا متيس، ةدعاقلا قباطت لىل روثعلا مت اذ Conn. فيرعت
 ةدعاقلا قباطت لىل روثعلا متي مل اذ. قفدتلا لىل ةدعاقلا كليل ةدحمل File و IPS جهن
 قفدتلا رطحب Snort في Zero Trust يفاضلا نوكملا موقيس

نوكتلا

ةكبشلل يطيختلا مسرلا



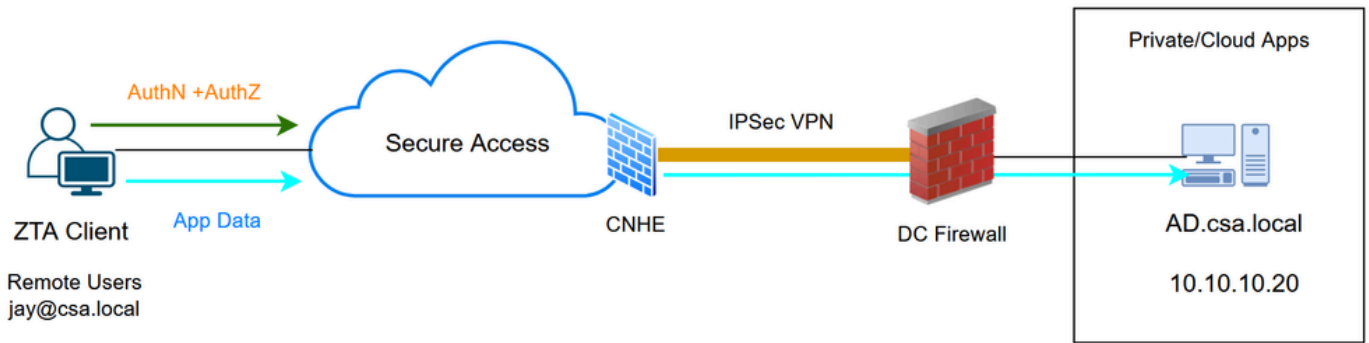
ةكبشلل يطيختلا مسرلا - طلتخملا ZTNA

رابتخالا تالاح

ةباحسلا ذيفنت - دي عبال مدختسمل : 1 رابتخالا ةلاح

لالخ نم ةكبشلا قفن ةومجم ربع صاخ دروم لى لوصولاب موقنس، هذه رابتخالا ةلاح في

قېبطلاتانايبو ةسايسال مېيقت نم لك ضارعا متي ، ةلالا هذه في . ةباحسالا قېبطلات
 لىل لوصولا اننكمي شيح يديلقت قفدت اذه . ZTA ةدحو ربع Secure Access ةطساوب
 دراومال لصوم و ءكبشالا قفنة ومجم ربع لجسمال ZTA ليمع نم صاخالا قېبطلالا

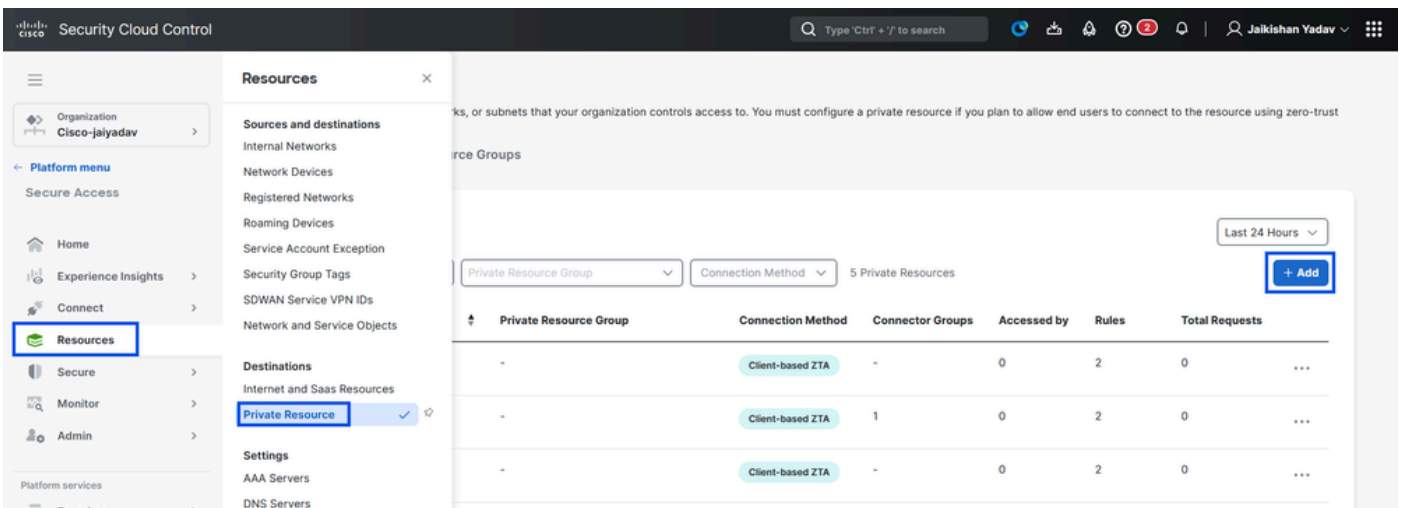


رابتلالا ةلالا ايحولوبط - يم لال ZTA

نم آل لوصولا لىل صاخ دروم ديدحت - 1 ةوطخلالا

(ZTA) ةقثالا مدع لىل لوصولا في لجسمال زاھجال ربع هيل لوصولا متيل صاخ دروم نيوكت
 ةباحسالا صرف مادختساب

1. ءفاضا + قوف رقنا > ةصاخالا دراومال > تاهجولا > دراومال لىل لقتنا



ةصاخالا دراومال نيوكت - نم آل لوصولا

يصوصون ، فصولا لىل لوصولال . درومال لىل نم اذا ماسا لخدأ ، صاخالا درومال ماسا لىل ةبسنلاب .
 درومال كلام ماسا و درومال نم ضرغالا لثم تامولعم ريفوتب

Add a Private Resource

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

General

Private Resource Name

AD-Server

Description (optional)

Active Directory server

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

3. صاخلا IP ناووع دي دحت اننك مي امك . هيلإ لوصولا ديرت يذلا صاخلا دروملل FQDN لخدأ .
[صاخ دروم ةفاضلا](#) عجار ، تامولعمل نم ديزمل . صاخلا دروملاب

4. لاجملا لحل ي لخدلا DNS مداخ ددح .

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ

ad.csa.local

Protocol

TCP - RDP

Port / Ranges

Any

+ Protocol & Port

Remove

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ

10.10.10.20

Protocol

TCP - RDP

Port / Ranges

Any

+ Protocol & Port

Remove + IP Address/FQDN

Use internal DNS server to resolve the domain

PrivateDNS (10.10.10.20) ^

Internal DNS Server

PrivateDNS (10.10.10.20)

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

5. ةياهنلا ةطقن لاصتا بيلاسأ دي دحت .

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Enforcement point for Remote and Local Users



Cancel

Save and Test Save

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

6. طافح قوف رقنا

ةصاخ لوصولو ةدعاق ءاشنإ - 2 ةوطخل

ةيملاعال ZTA يف نولجسمل نومدختسمل انكمتيل Secure Access لىل صاخ لوصولو نيوكت
[صاخلا لوصولو ةدعاق](#) عجار ، تامولعمل نم ديزمل . هيل لوصولو نم

لوصولو جهن > نمآلا لىل لقتنا 1.

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

لوصولو ةسايس نيوكت - نمآلا لوصولو

2. Private Access رتخأ مٲ ، ءءءاق ءفاضا قوف رقنا . كٲ ءصاخال ءءءاق لل ءنوكملا ءانوكملا فصى صءلم ءءوي ءءءاقلا ىلعأ ىف

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

2 Rules

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

Rows per page 100 1-2 of 2 < 1 >

Private Access

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

Internet Access

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

لوصول ءسايس نيوكٲ - نمآلا لوصول

3. ءءءاق مسا ءفاضا .

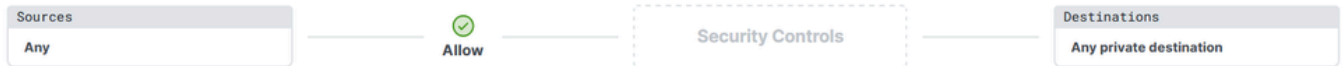
Add AD-RDP-Allow

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

Rule is enabled

Logging is enabled Edit

Summary



Rule name

AD-RDP-Allow

Rule order

1

1 Specify Access

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

Action

Allow

Allow specified traffic if security requirements are met.

Block

Block specified traffic.

From

To

لوصول ءسايس نيوكٲ - نمآلا لوصول

4. ءءءاق ءءءاقلا ءءءاقلا ءءءاقلا

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

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources.

AD Users • Any AD Users

To

Specify one or more destinations.

Private Resources • AD-Server

+ AND

لوصول ة سايس نيوكت - نم آلا لوصول

ةياهنلا ةطقن تابلطتم نيوكت 5.

Endpoint Requirements

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

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

For Branch connections:

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

User Authentication Requirements

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

2 Configure Security

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

Cancel

Back

Next

لوصول ة سايس نيوكت - نم آلا لوصول

نام آلا نيوكت 6.

Specify Access

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

2 Configure Security

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

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

Disabled

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

Security Profile [Rule Defaults](#)

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

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

Cancel

Back

Save

لوصول ة سايس نيوكت - نم آلا لوصول

7. ظفح قوف رقنا

Access Policy

[Rule Defaults and Global Settings](#)

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

Search by rule name Intent Objects Settings

Add Rule

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	🌐	-	🟢
2	BlockPage-TEST	Internet	Block	Any	Generative A...	🌐	-	🟢
3	RAVPN-Allow	Internet	Allow	Any AD Users	Any	🌐🔒	492	🟢

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

Default Access Rules

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

لوصول ة سايس نيوكت - نم آلا لوصول

ZTA فيرعت فلم إلى صاخ دروم ة فاضا 3 - ة و ط خ ل

إلى ينعمل صاخ ل دروم ل ة فاضا ل جاتحت كن إف ، ص ص خ م ZTA فيرعت فلم مدختست تنك إذا ZTA فيرعت فلم

قوف رقنا و ة قث ل م ادعنا إلى لوصول > يئاهن ل مدختست م ل لاصتا > ل لاصتا إلى لقتنا 1. ZTA فيرعت فلم +

End User Connectivity

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

Zero Trust Access | Virtual Private Network | Internet Security

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

Enrollment methods [Manage](#)

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

Windows and macOS devices enroll using: [SSO Authentication](#) | [Certificates](#)

Android and iOS devices enroll using SSO Authentication only.

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

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

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
<p>No ZTNA profiles created.</p>					

ZTA فيرعت فلم - نمآل لوصول

صاخال دروملا ةفاضلا 2.

Create profile

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

ZTA profile name: Priority:

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

1 Secure Private Access (0 Destinations)

2 Secure Internet Access

3 Users and Groups

Secure Private Access

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

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

Search by destination:

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

[+ Destinations](#)

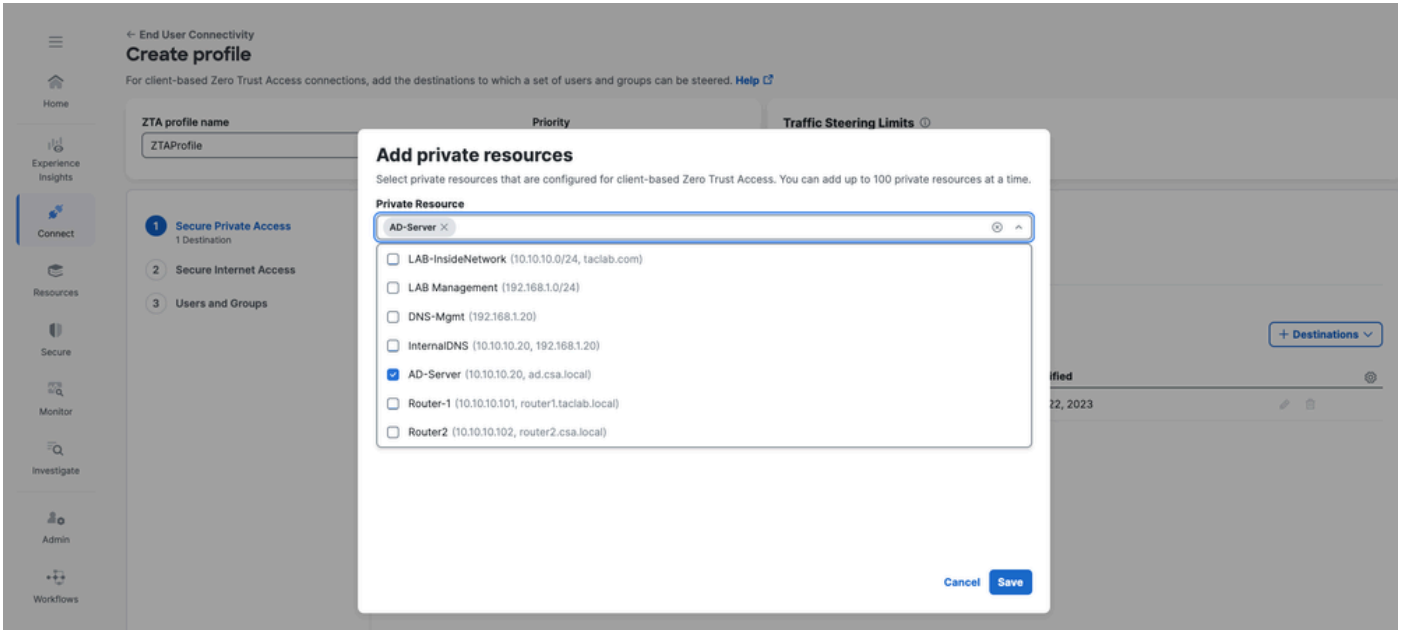
Private Resource

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

Add Destination

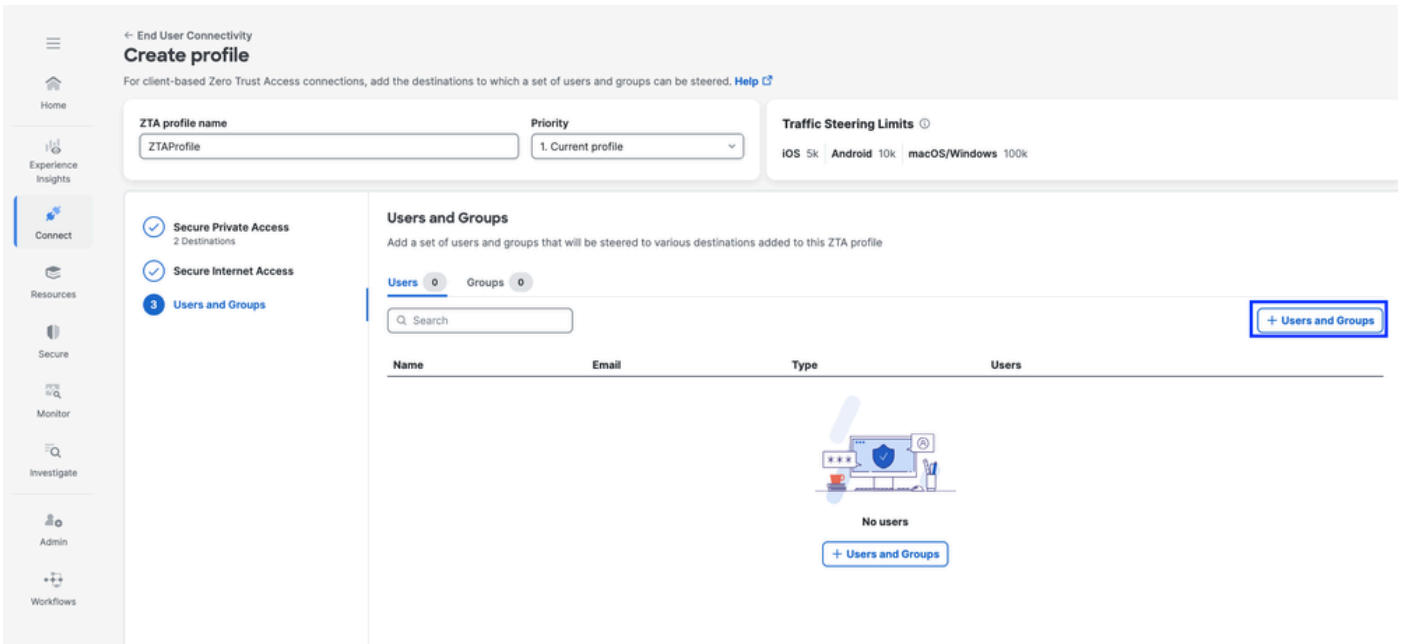
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

ZTA فيرعت فلم - نمآل لوصول



ZTA فيرعت فلم - نم آلا لوصول

تاعومجم وني مدختسم ةفاضل 3.



ZTA profile name: ZTAProfile

Priority: 1. Current profile

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

Secure Private Access: 2 Destinations

Secure Internet Access

Users and Groups: 3

Users and Groups

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

Users: 1 | Groups: 0

Search:

+ Users and Groups

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

Rows per page: 10

Back Close

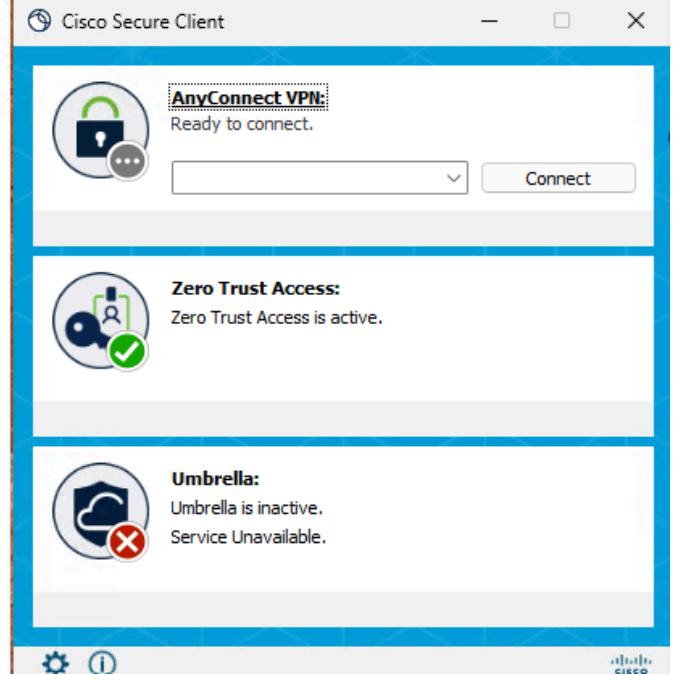
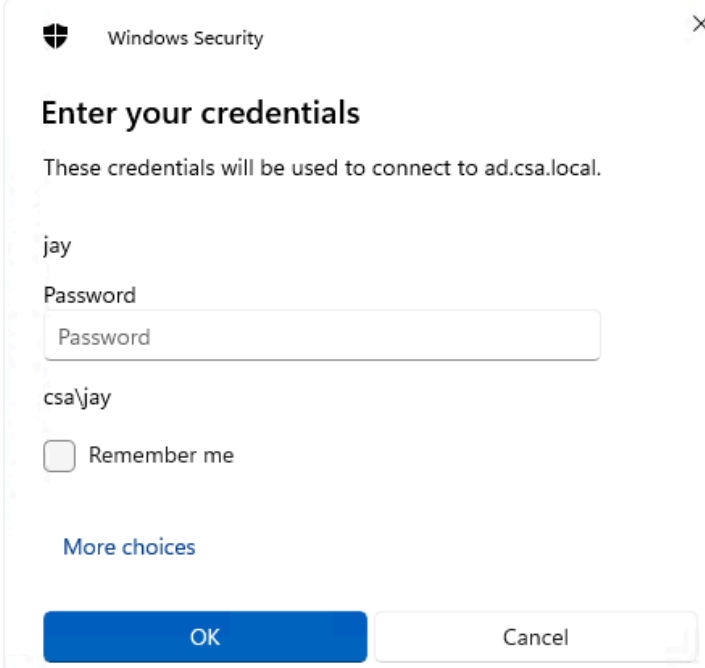
ZTA فيرعت فلم - نمآلا لوصولا

لېمعال عم هت نمامزم ونيوكتال عفدة قيقد 20 ىل 15 نم رمالا قرغتسي دق: ةظالم
نيعمال صاخلا دروملل

صاخلا دروملا ىل لوصولا نم ققحتال 4 - ةوطخال

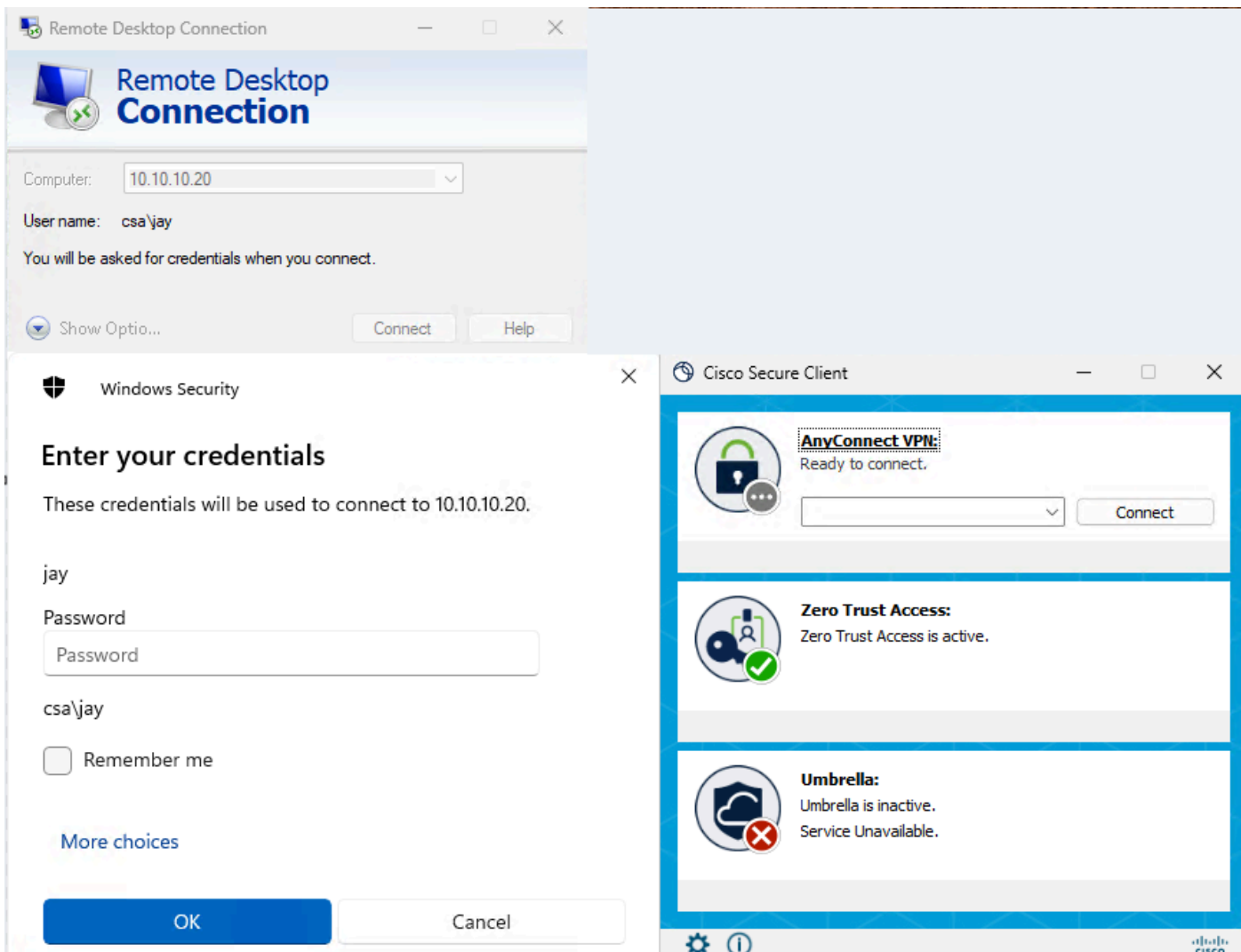
صاخلا دروملا ىل لوصولا 1.

FQDN مادختساب PR ىل لوصولا



ةم اءال اءاقالءال رابءءء - نم آالا لوصولا

IP ناوع ماءءءسااب PR لى لوصولا



عمارة اتصالات العمل رابته - نم آلا لوصول

طاشنل نع شحبل اذح امدخت ساب ققحت ال 2.

Activity Search

Filters: IP ADDRESS 10.10.10.20, RESPONSE Allowed

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

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

ةطشنال نع شحبل ال - نم آلا لوصول

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 PORT 3389 Restore to previous state Save Search

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

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

Event Details

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

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

ةطش نأل نع شحبلا - نم آلا لوصولا

Activity Search

Schedule Export CSV LAST 24 HOURS

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

IP ADDRESS 10.10.10.20 Restore to default layout Save Search

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

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

ةطش نأل نع شحبلا - نم آلا لوصولا

Activity Search Schedule Export CSV LAST 24 HOURS

FILTERS Advanced CLEAR Saved Searches Customize Columns ZTA Client-based

IP ADDRESS 10.10.10.20 Restore to default layout Save Search

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

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 12, 2026 5:51 AM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: AD-RDP-Allow

Resource/Application: AD-Server

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: 10.10.10.20

Destination IP

ةطشنأل نع ثحبلا - نمأل لوصول

FMC لاصتا اءاأ نم ققحتلا 3.

Events Troubleshooting

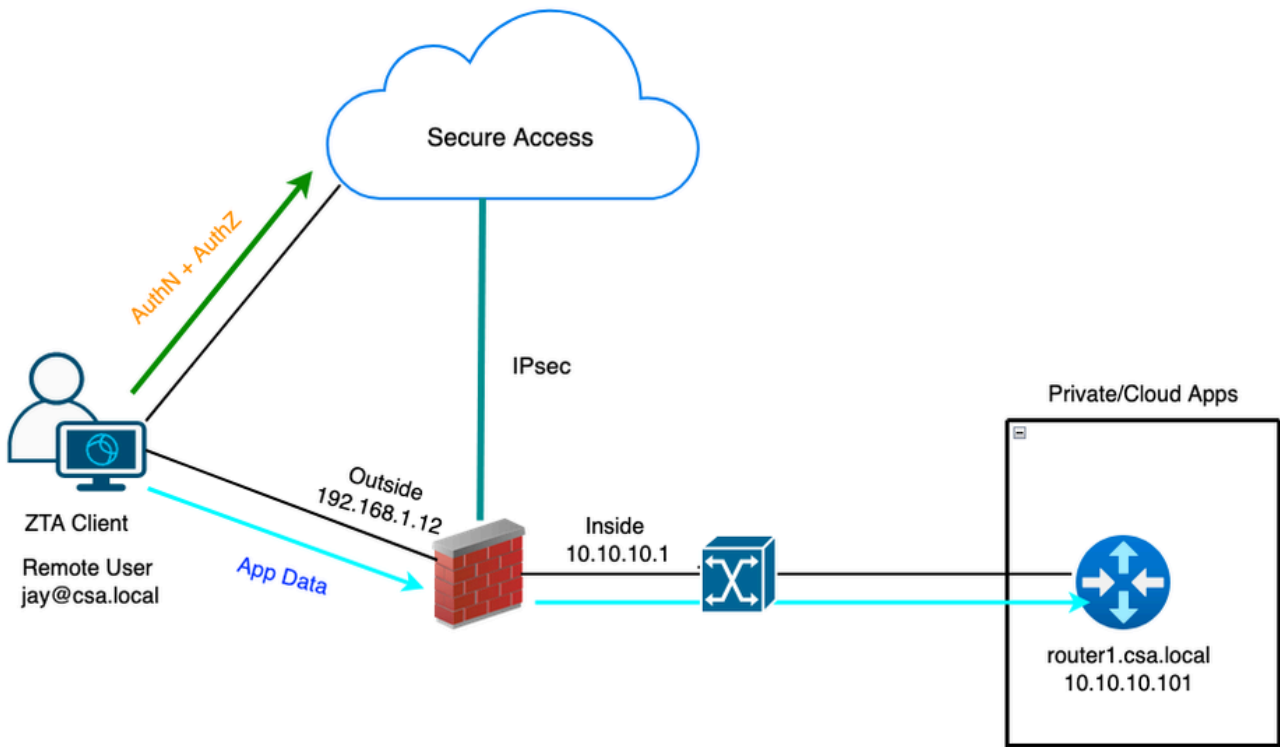
7 events Last 1 hour Go Li

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

FMC لاصتا اءاأ

يلحم ذيفنت - ديعب مدختسم - 2 ةلجال رابءا

ذافنإل ةسايس مءيقن نم عونلا اءه يف ، يلحملل قيبطتلا ربع صاخ دروم يل لوصولل ليلبس لعل. FTD لعل ةيلحملل قيبطتلا اءاأ بيقب نكلل Secure Access لعل مءي دروم يل لوصولل لولول ةيلزنم ءكبشب لصتم ZTA يف لءسم مدختسم وأ ليعم ، لاءملا . ةءاولل لءاد FTD فلء ءووم صاخ



رابط خال الة ايجولوبط - یم الة ال ZTA

نم الة لوصول الة صاخ دروم ديدحت - 1 ة وطلخ ال

(ZTA) ة قث الة مدع الة لوصول الة ف لچسمل زاهال ربع الة لوصول الة متيل صاخ دروم نيوكت ة باحس الة صرف مادختساب

1. ة اضا + قوف رقنا > ة صاخ الة دراوم الة > تاهجول > دراوم الة الة لقتنا

The screenshot shows the Cisco Security Cloud Control interface. The Resources section is active, displaying a table of Private Resources. The table has the following columns: Private Resource Group, Connection Method, Connector Groups, Accessed by, Rules, and Total Requests. There are three entries in the table, all for Client-based ZTA.

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

ة صاخ الة دراوم الة نيوكت - نم الة لوصول الة

2. يصبون، فصولا يلعل لوصحلل. دروملل ينعم اذ امسا لخدأ، صاخلل دروملا مسا يلإ ةبسنلاب. دروملا كلام مسا وأ دروملا نم ضرغللا لثم تامولعم ريفوتب

← Private Resources

Add a Private Resource

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

General

Private Resource Name

Description (optional)

ةصاخلل دراوملا نيوكت - نمآلا لوصولا

3. صاخلل IP ناوئع ديدحت اننكمي امك . هيلإ لوصولا ديرت يذلا صاخلل دروملل FQDN لخدأ. [صاخ دروم ةفاضلا](#) عجار، تامولعملل نم ديزمل . صاخلل دروملاب

4. لاجملل لجل يلخادلل DNS مداخ ددح

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR)	Protocol	Port / Ranges	
<input type="text" value="router1.csa.local"/>	Any TCP	22	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.101"/>	Any TCP	22	+ Protocol & Port
Remove			+ IP Address/FQDN

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

Internal DNS Server

ةصاخلل دراوملا نيوكت - نمآلا لوصولا

5. ةياهنلا ةطقن لاصتا بيلاسأ ديدحت

6. ةيلحم ذيفنت طاقنك FTD ددح

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

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

Enforcement point for Remote User



Enforcement point for Local user



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

Change the remotely reachable addresses

Cancel

Save and Test Save

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

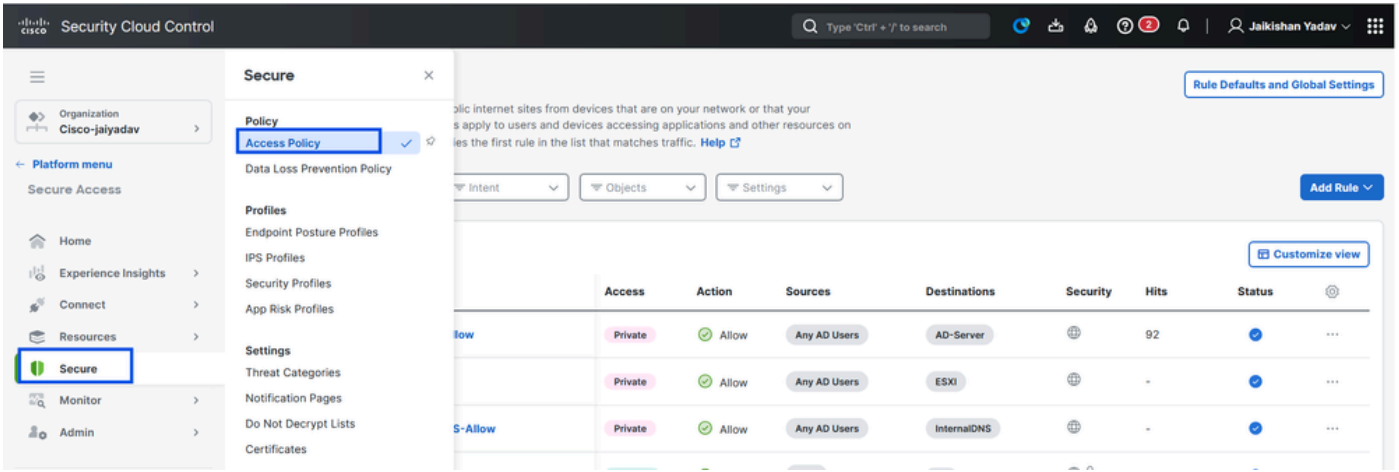
PR نارقاب ريغيغتللا اذه موقيس ، هددحت يذلا ليچستلا عون ىلع ادامتعا :ةظحالم
جهنلا رشن ليغشت ىلا يدؤيسو FTD ب ايئاقلت

7. ظفح قوف رقنا

ةصاخ لوصولو ةدعاق عاشنإ - 2 ةوطخلا

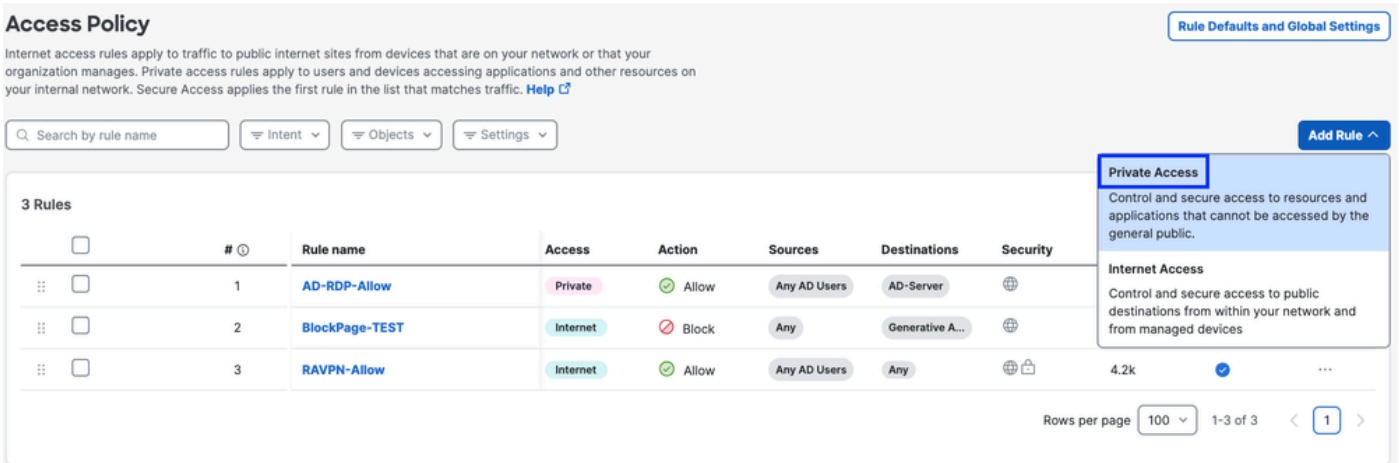
ةيملاعال ZTA يف نولجسملل نومدختسملل نكمتيل Secure Access ىلع صاخ لوصولو نيوكت
[صاخلا لوصولو ةدعاق](#) عجار ، تامولعملل نم ديزمل . هيلا لوصولو نم

لوصولو جهن > نمآلا لقتنا 1.



ةصاخلا دراوملا نيوكت - نمآلا لوصولا

2. Private Access رتخأ مث ،ةدعاق ةفاضإ قوف رقنا .
 لكب ةصاخلا ةدعاقلا ةنوكملا تانوكملا فصي صخلم دجوي ةدعاقلا ىلعأ يف



لوصولا ةسايس نيوكت - نمآلا لوصولا

ةدعاق مساة فاضإ 3.

Add Router1-SSH

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

لوصول ةسايس نيوكت - نمآلا لوصول

ةهول او ردصم لادحو ةدعاق ل اءارج اددح .4

Rule name ⓘ

Router1-SSH

Rule order

1

1 Specify Access

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

Action



Allow

Allow specified traffic if security requirements are met.



Block

Block specified traffic.

From

Specify one or more sources.

AD Users - Any AD Users

To

Specify one or more destinations.

Private Resources - Router1

+ AND

لوصول ةسايس نيوكت - نمآلا لوصول

ةياهن للة طقن تابلطتم نيوكت .5

Endpoint Requirements

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

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

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

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

Private Resources: **Router-1**

For Branch connections:

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

User Authentication Requirements

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

Disabled

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

2 Configure Security

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

Cancel

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

لوصول ةسايس نيوكت - نمآلا لوصول

6. نامآلا نيوكت

Specify Access

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

2 Configure Security

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

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

Disabled

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

Security Profile [Rule Defaults](#)

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

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

Cancel

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

لوصول ةسايس نيوكت - نمآلا لوصول

7. ظفح قوف رقنا

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

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

لوصول ةسايس نيوكت - نمآلا لوصول

FTD لىلع ةماعلا تاقالعل نارتقا نم ققحتلا - 3 ةوطخلا

FTDs > ةكبشلا تالاصتإ > لاصتا لىل لقتنا 1.

Security Cloud Control

Organization: Cisco-jaiyadav

Platform menu: Secure Access, Home, Experience Insights, **Connect**, Resources, Secure, Monitor

Connect

Essentials: Network Connections (selected), Users, Groups, and Endpoint Devices, End User Connectivity, DNS Forwarders

Tunnel Groups: FTDs

0 Warning, 1 Connected

Region: [Dropdown], Status: [Dropdown], 2 Tunnel Groups

+ Add

ةماعلا تاقالعل نم ققحتلا - نمآلا لوصول

اذه FTD ب ةنرتقملا دراوملا ضرع > FTD قوف رقنا 2.

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

Device FQDN ftd.csa.local
Auto deployment Yes

UZTA Configuration status

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

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status	
Synced	1

View resources associated to this FTD

Associate Resources

ةم اءال اءالءال نم ققءءال - نم آال لوصولا

Resources associated with FMC_FTD

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

Q Search by resource name

Configuration status

1 Resources

Associate Resources

Resource name

Status

Router1

Synced

Close

ةم اءال اءالءال نم ققءءال - نم آال لوصولا

3. قالغإ قوف رقنا

4. نم ازملا ةلاح يف نيوكتلاو نرتقملا دروملا نوكي نأ بجي هنا نم وةلاحلل نم ققحت

The screenshot displays the 'Network Connections' page in the Palo Alto Networks management console. The main area shows a table of FTDs configured for Universal Zero Trust Access. A single FTD, 'FMC_FTD', is listed with a 'Synced' status. The right-hand pane provides detailed information for 'FMC_FTD', including Firewall Details (Device FQDN: ftd.csa.local, Auto deployment: Yes), UZTA Configuration status (Synced, Last synced at 31 Dec 2025, at 2:51 AM UTC), Assigned Trusted Network (LAN), and Associated Resources (1 Synced).

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

ةم اءلا اءالءلا نم ققحتلا - نم آلا لوصولا

5. فTD لىل نيوكتلا عفء نم ققحت

LINA عضو لىل لقتناو فTD ب ةصاخلا (CLI) رماوالا رطس ةهءاوى لىل لوءءلا لىءس تب مق

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# █
```

ةم اءلا اءالءلا نم ققحتلا - فTD

ZTA فيرعت فلم لإصاخ دروم ة فاضا 4 - ة و طخل

قوف رقناو ة قثلا مادعنا لإوصولا > يئاهنلا مدختس مللا لصتا > لاصتالا لإلقتنا 1.
ZTA فيرعت فلم ريرحتل طاقن 3

End User Connectivity

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

Enrollment methods

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles

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

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

ZTA فيرعت فلم - نمآلا لوصولا

صاخلا دروملا ة فاضا 2.

Create profile

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

ZTA profile name: ZTAProfile

Priority: 1. Current profile

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

1 Secure Private Access
0 Destinations

2 Secure Internet Access

3 Users and Groups

Secure Private Access

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

Traffic Steering Options

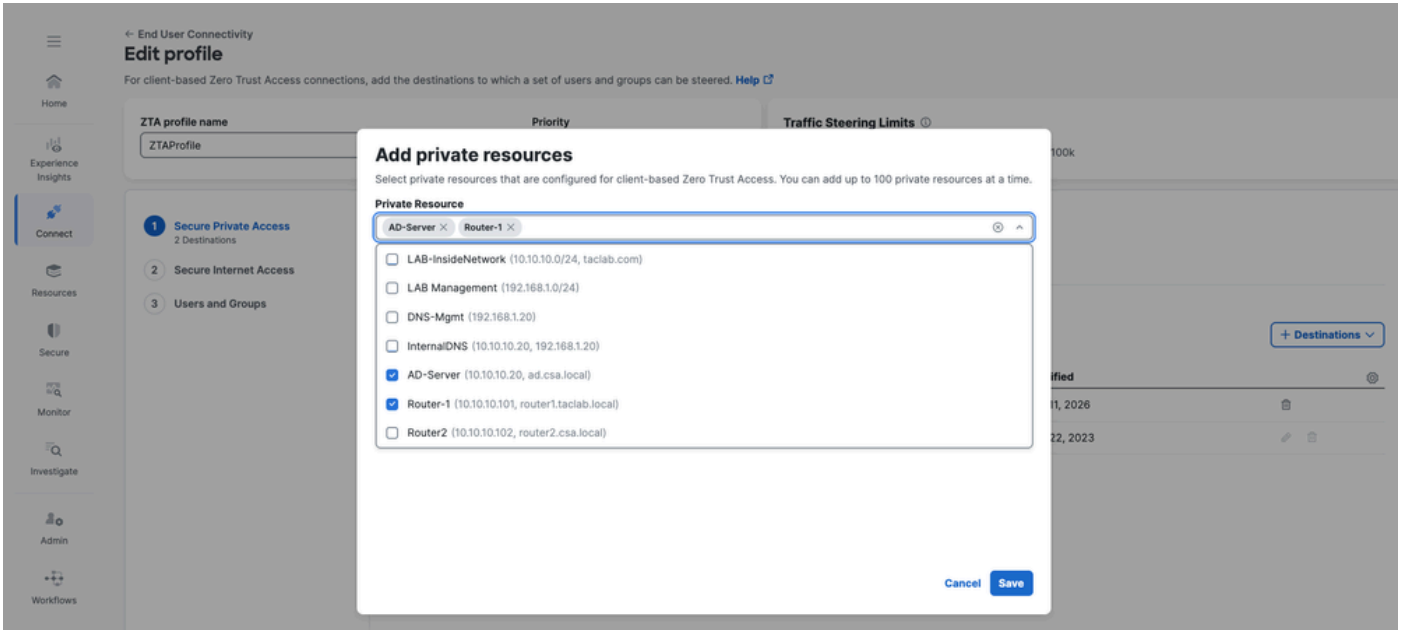
Search by destination

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

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

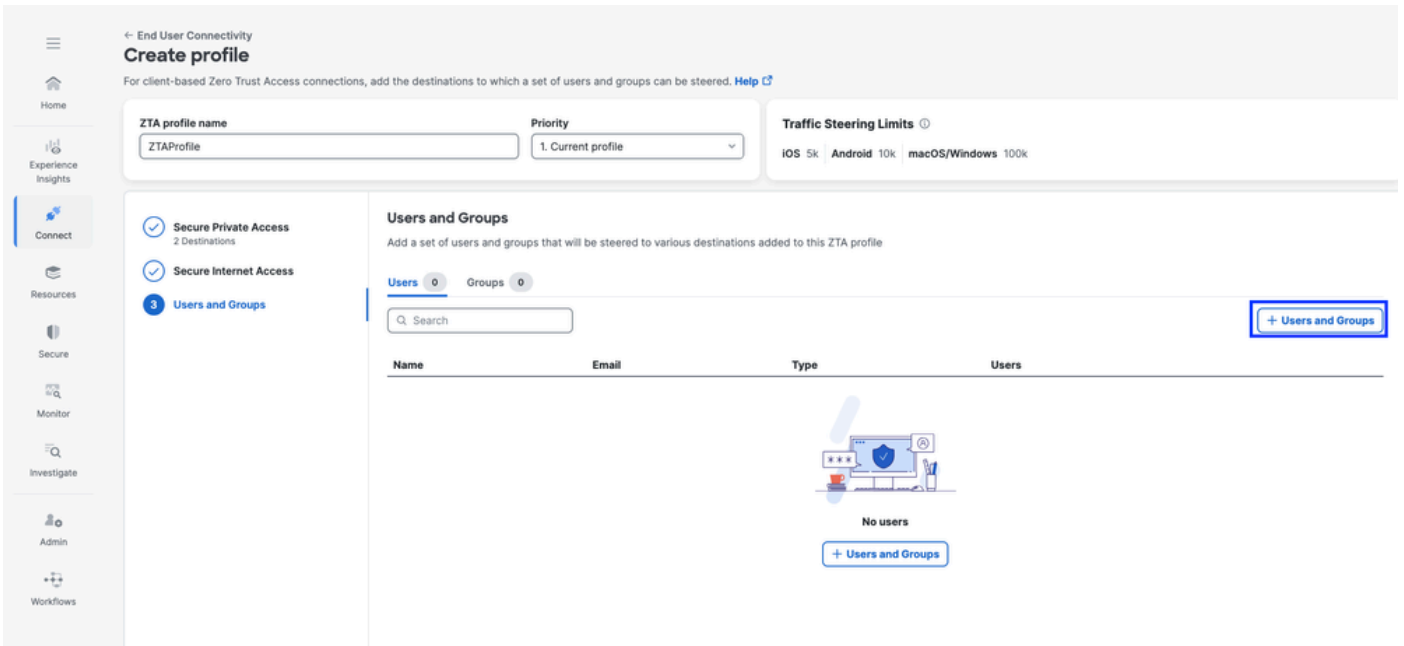
Add Destination
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

ZTA فيرعت فلم - نمآلا لوصولا



ZTA فيرعت فلم - نمآلا لوصولا

تاعومجم وني مدختسم ةفاضلا 3.



ZTA فيرعت فلم - نمآلا لوصولا

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

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

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

Users: 1 | Groups: 0

Search:

[+ Users and Groups](#)

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

Rows per page: 10

[Back](#) [Close](#)

ZTA فيرعت فلم - نم آلا لوصولا

صاخال دروملا إلى لوصولا نم ققحتال 5 - ةوطخال

1. FTD FQDN لىل عديع بل مدختسملا ةردق نم ققحتال

```
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
```

ةماعةال تاقالعال رابتهإ - نمآلا لوصولا

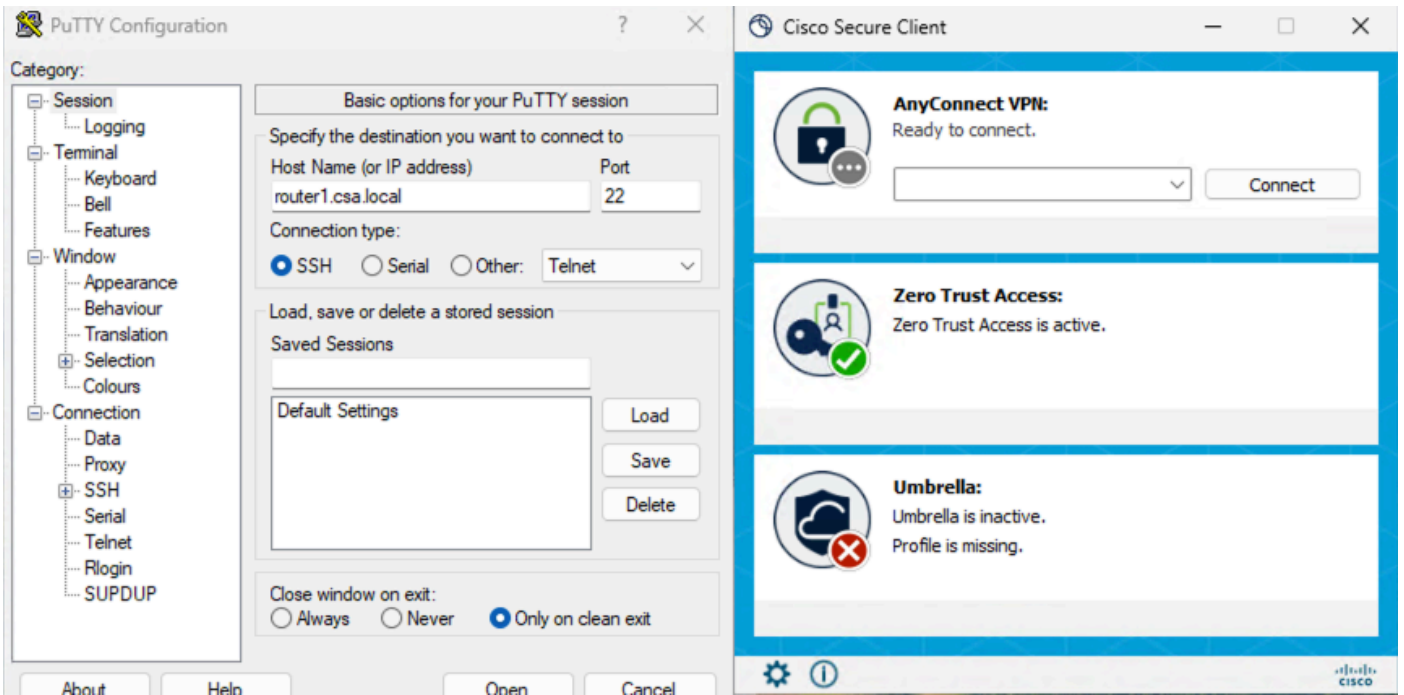
2. FQDN ماذختهساب ةصاخال دراومال ال فTD لوصولا نم ققحتال .

```
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#
```

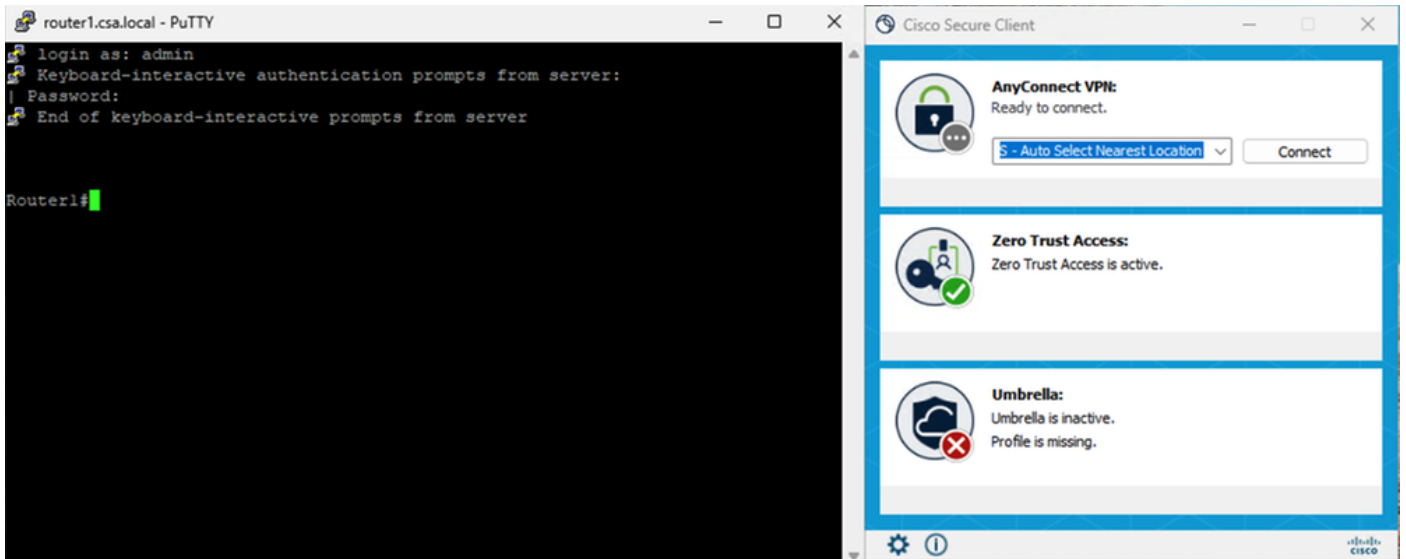
ةماعةال تاقالعال رابتهإ - نمآلا لوصولا

3. صاخال دروملاب SSH لاصتا رابتهإ .

FQDN ماذختهساب PR ال لوصولا

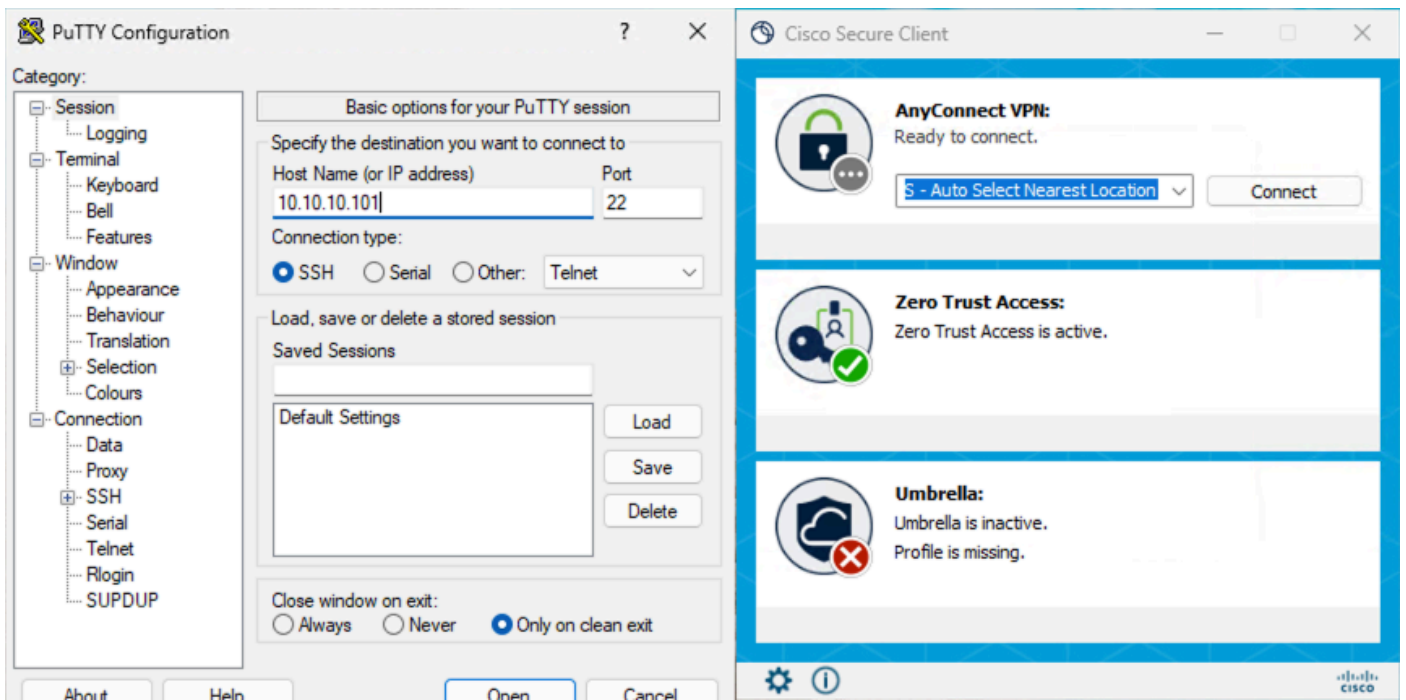


ةماعةال تاقالعال رابتهإ - نمآلا لوصولا

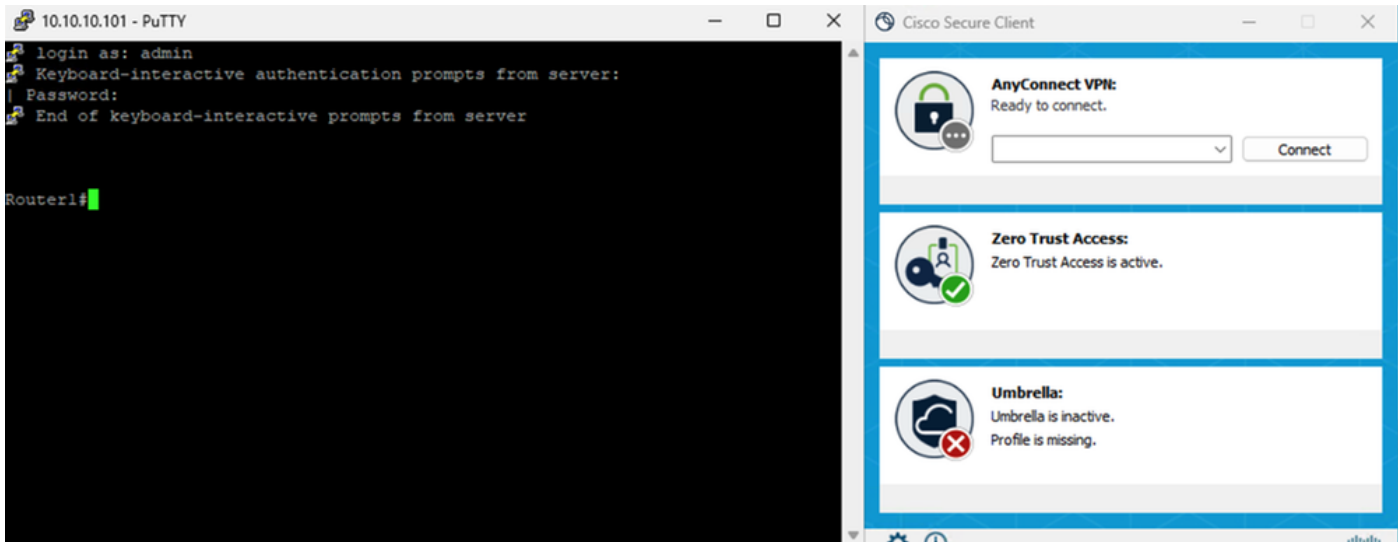


عمال تاقال عمل رابتخ | - نم آلا لوصول

IP ناوع مادختساب PR يلى لوصول



عمال تاقال عمل رابتخ | - نم آلا لوصول



عمال اتقال عل رابتخ | - نم آلا لوصول

4. نم آلا لوصول طاشن نع شحبلا تالجس نم ققحتلا

Activity Search

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

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

ةطشنأل نع شحبلا - نم آلا لوصول

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:55 PM

Access details

Identity: jay (jay@csa.local)

Win: Win10

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD > FMC_FTD

Destination: router1.csa.local

Destination IP: 10.10.10.101

ةطشنألانع شحبلا - نمآلا لوصول

Activity Search

Search filters: 7 Total | Viewing activity from Jan 9, 2026 6:01 PM to Jan 10, 2026 6:01 PM

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

ةطشنألانع شحبلا - نمآلا لوصول

7 Total | Viewing activity from Jan 9, 2026 6:09 PM to Jan 10, 2026 6:09 PM

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

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:56 PM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD> FMC_FTD

Destination: 10.10.10.101

Destination IP: 10.10.10.101

ةطشنألانع شحبلا - نمآلا لوصول

FMC لاصتا اءاء نم ققءءلا 5.

Firewall Management Center

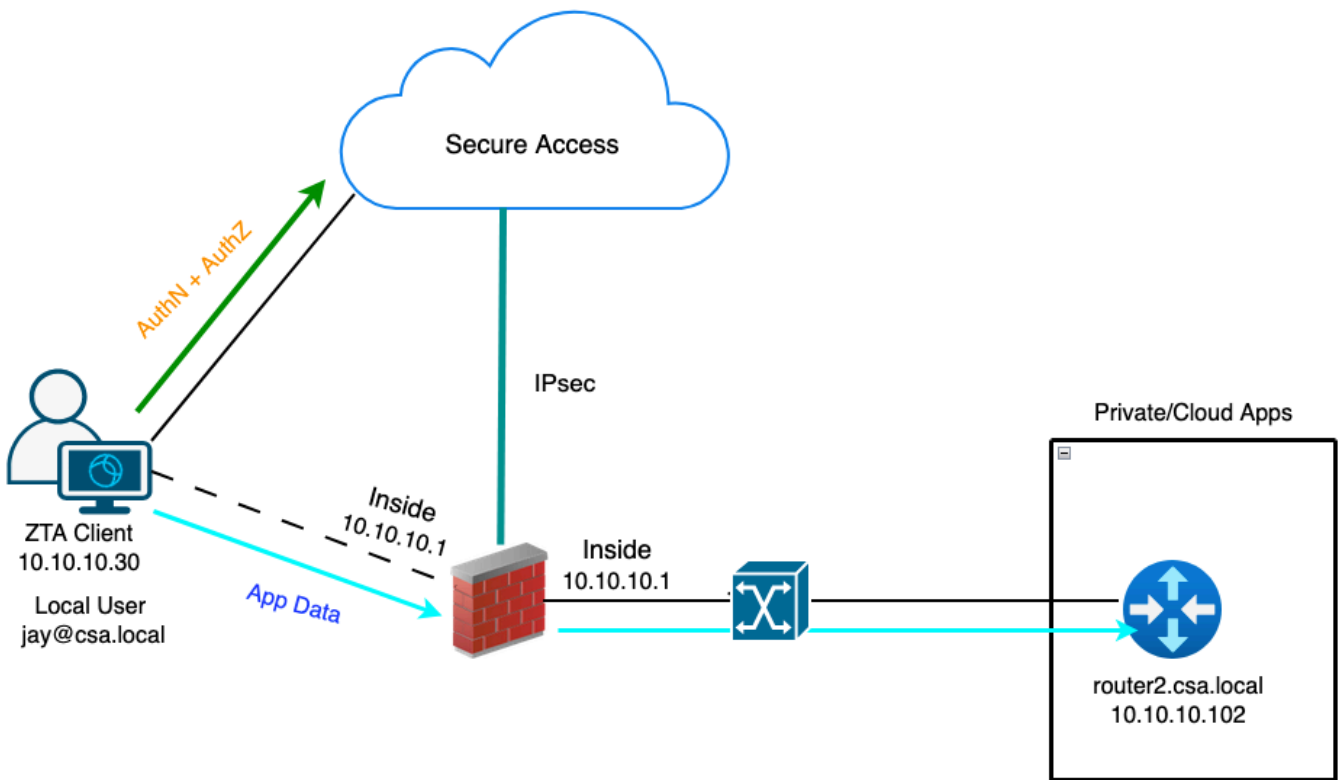
Events & Logs / Analysis / Unified Events

Search: Destination IP: 10.10.10.101

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

يلحم ذيفنت - يلحم مدختسم - 3 ةلاحال رابتحا

ميفيقت نم عونلا اذه يف ، يلحم مدختسمك يلحملا قيبطتلا لالخال نم صاخ دروم ىلا لوصولا FTD. ىلع ةيلحم قيبطتلا تانايب يقبت نكلو Secure Access ىلع متي ذافنإلا ةسايس لواحيو ةيلزمنة ةكبش ب لصتم ZTA يف لجسم مدختسم وأ ليمع ، لاثملا ليبس ىلع ةهجاو ي أو DMZ فلخال صاخلا دروملا ناك اذا . ةهجاو لا لخال FTD فلخال دوجوم صاخ دروم ىلا لوصولا نيب رورملا ةكرب حامسلل FTD ىلع لوصولو ةدعاق عاشنإ انيلع نياعتيسف ، FTD ل ىرخأ Private Resource و ةكبشلا وأ Client IP

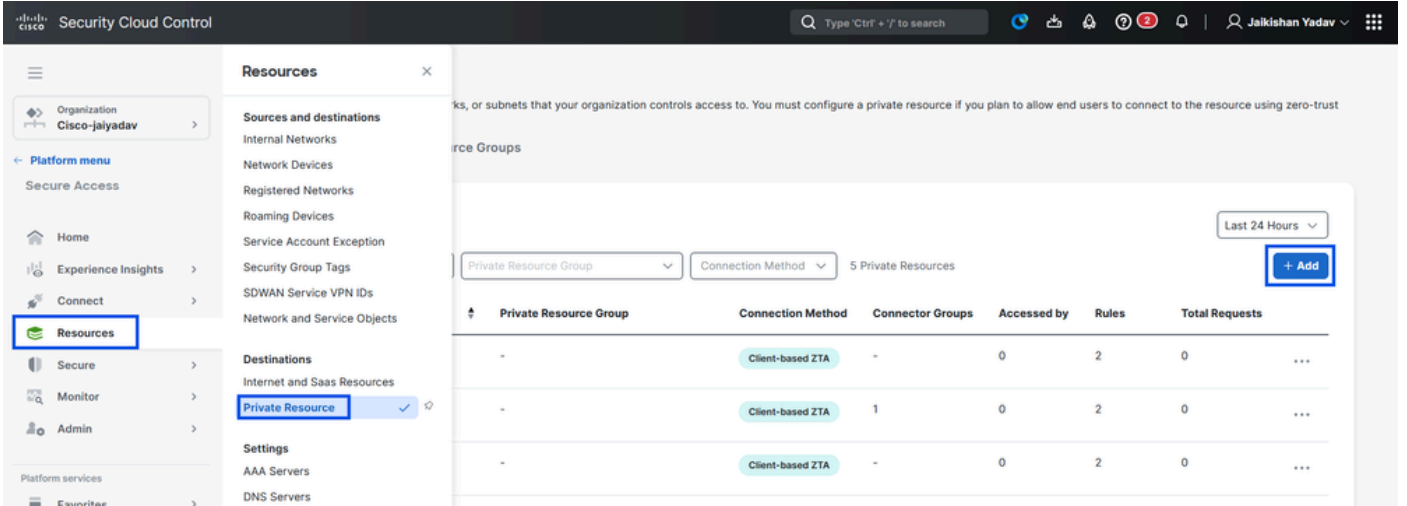


رابتحالا ةلاح ايجولوبط - يملاعلا ZTA

نمآلا لوصولا ىلع صاخ دروم ديدحت - 1 ةوطخال

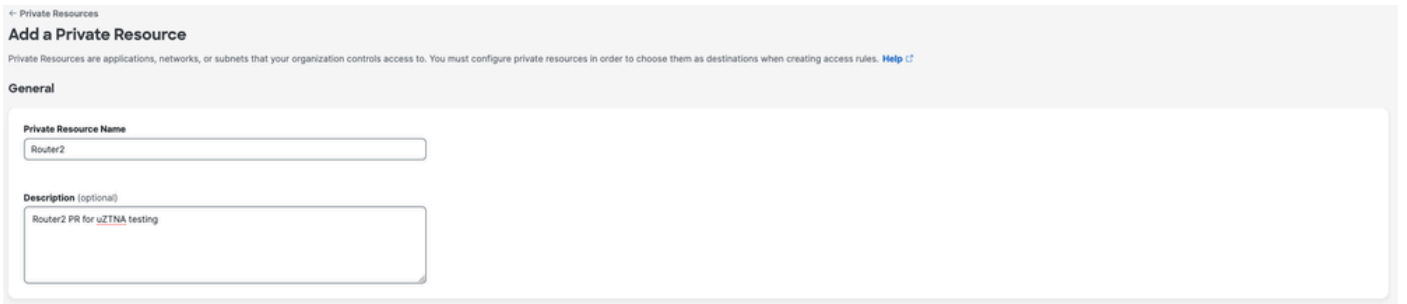
(ZTA) ةقثلا مدع ىلا لوصولا يف لجسملا زاهجال ربع هيللا لوصولا متيل صاخ دروم نيوكت ةباحسلا صرف مادختساب

1. ةفاضل + قوف رقنا > ةصاخلا دراوملا > تاهجولا > دراوملا ىلا لقتنا



صخال دراومل نيوكت - نمآال لوصول

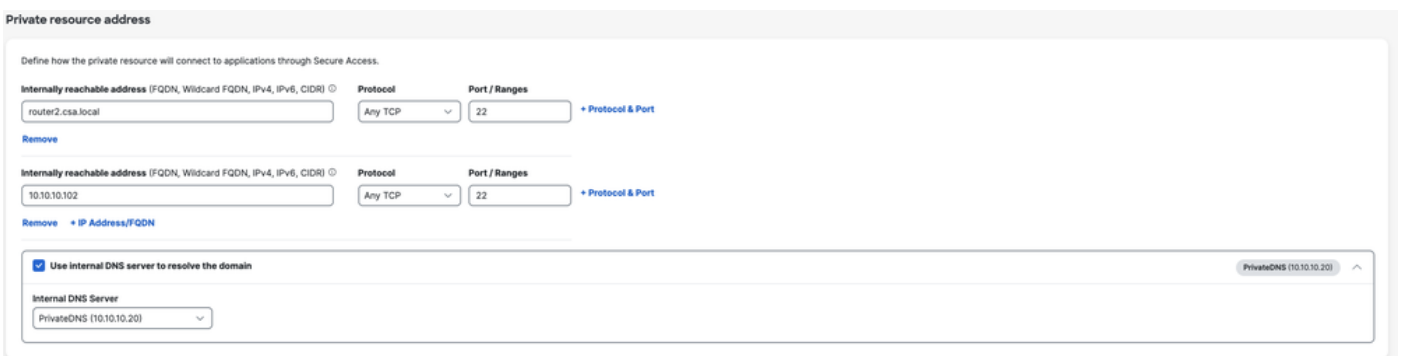
2. ي صون ، فصولا يلعل لوصولل . دروملل ينعم اذا م سالا لخدأ ، صخال دراومل م سالا لة بسنلاب . درومل كلام م سالا دراومل نم ضرغلالم لثم تامولعم ريفوتب .



صخال دراومل نيوكت - نمآال لوصول

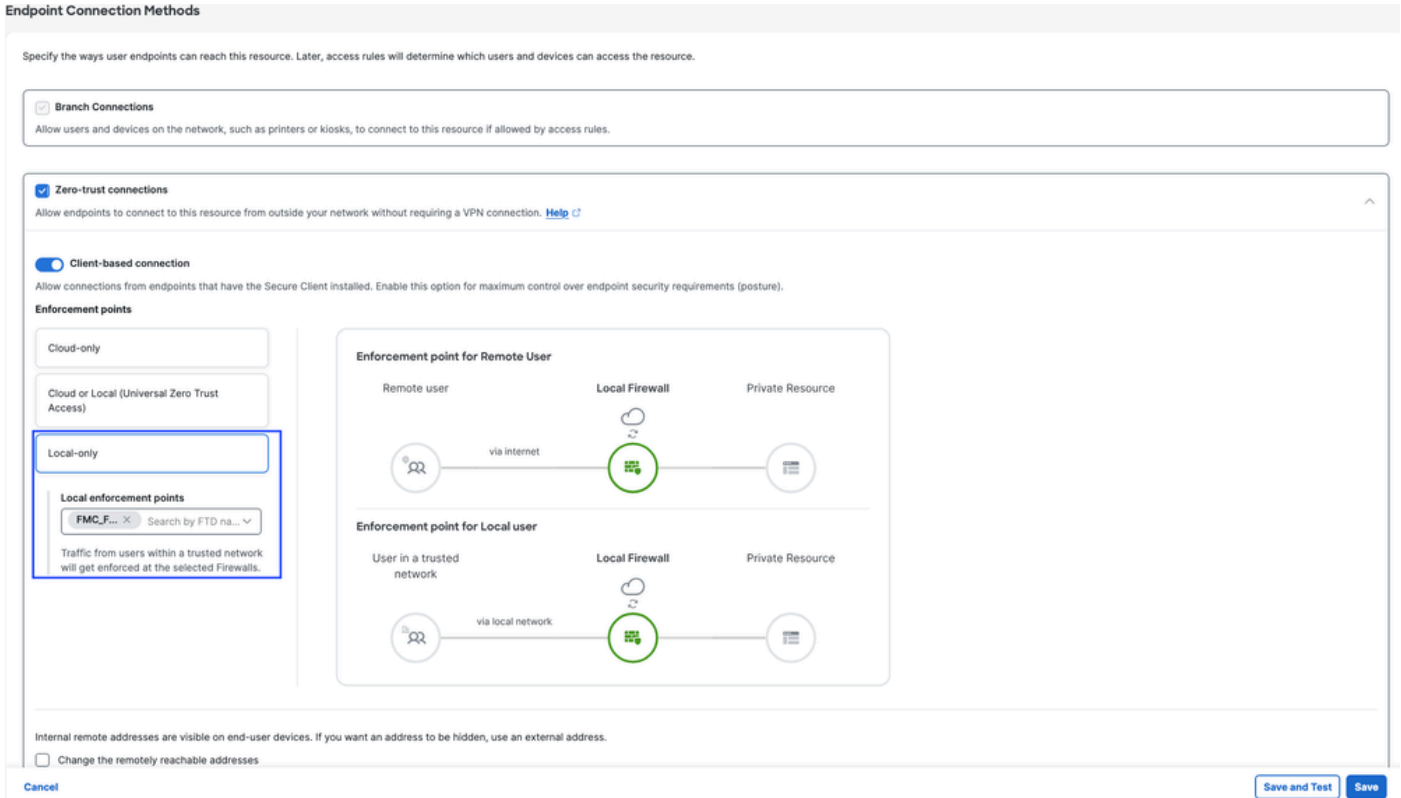
3. صخال IP ناووع ديدحت اننكمي امك . هيل لوصولا ديرت يذلا صخال دراومل ل FQDN لخدأ . [صخال دروم ةفاضلا](#) عجار ، تامولعمل نم ديزمل . صخال دراومللاب

لاجملا لجل يلخادلا DNS م داخ دح .



5. ةياهنلا ةطقن لاصتا بيلاسأ ديدحت

6. ةيلحم ذيفنت طاقنك FTD ددح



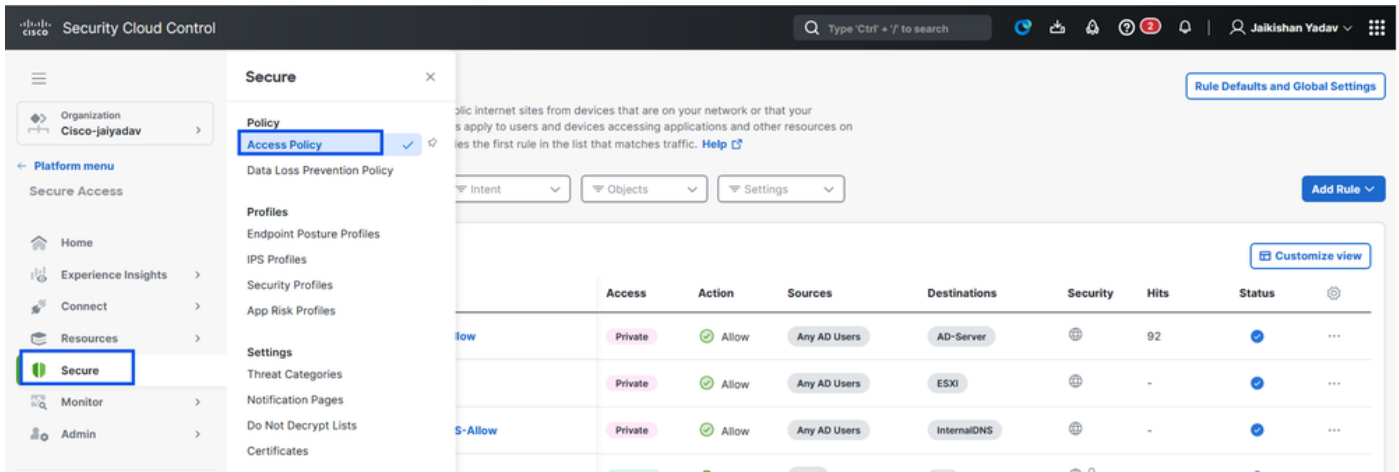
PR نارقاب ريغيغتللا اذه موقيس ، هددحت يذلا ليچستلا عون ىلع ادامتعا :ةطحالم
جهنلا رشن ليغشت ىلا يدؤيسو FTD ب ايئاقلت

7. ظفح قوف رقنا

ةصاخ لوصولو ةدعاق عاشنإ - 2 ةوطخلا

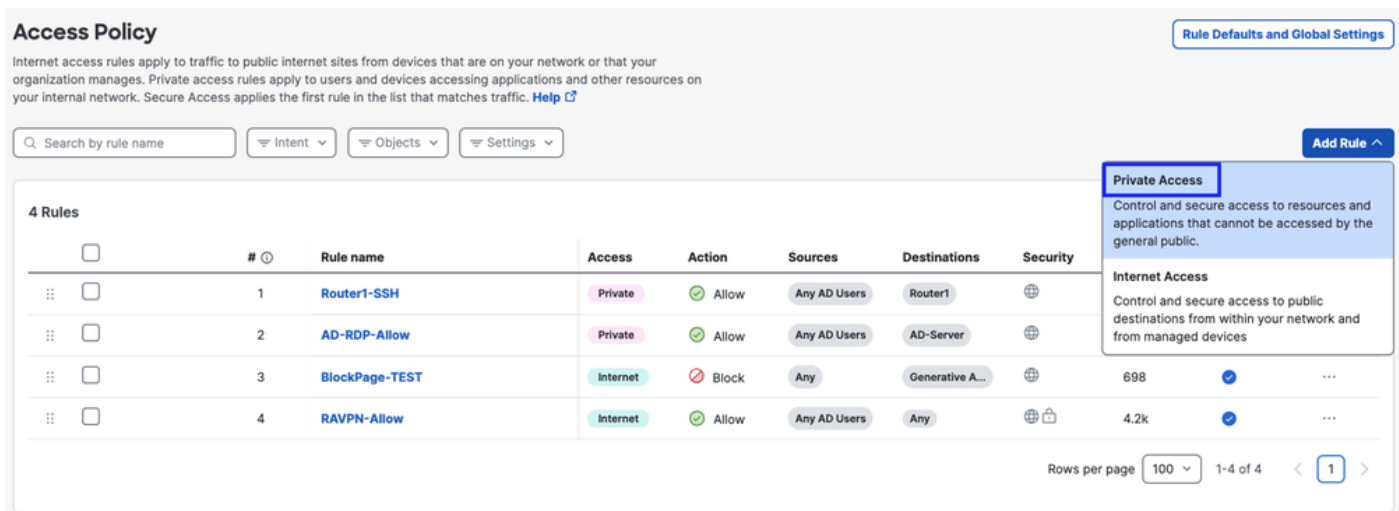
ةيملاعال ZTA يف نولجسمل نومدختسمل انكمتيل Secure Access ىلع صاخ لوصولو نيوكت
[صاخلا لوصولو ةدعاق](#) عجار ، تامولعمل نم ديزمل . هيل لوصولو نم

1. لوصولو جهن > نمآلا لىلا لقتنا



لوصول ةسايس نيوكت - نمآلا لوصول

2. Private Access رتخأ مٲ، ةءءاق ةفاضا قوف رقنا .
 كٲ ةصاآلا ةءءاقلا ءنوكملا ءانوكملا فصي صآلم ءءوي ةءءاقلا لعلأ يف .



لوصول ةسايس نيوكت - نمآلا لوصول

3. ةءءاق مسا ةفاضا .

Add Router2-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

لوصول ةسايس نيوكت - نمآل لوصول

ةهول و ردصم ل دحو ةدعاق ل ارج دح .4

Rule name

Router2-SSH-Allow

Rule order

1

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources

AD Users - Any AD Users

To

Specify one or more destinations

Private Resources - Router2

+ AND

لوصول ةسايس نيوكت - نمآل لوصول

ةياهن ل ةطقن تابلطتم نيوكت .5

Endpoint Requirements

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

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

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

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

Private Resources: **Router2**

For Branch connections:

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

User Authentication Requirements

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

Disabled

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

2 Configure Security

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

Cancel

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

لوصول ةسايس نيوكت - نمآلا لوصول

6. نامآلا نيوكت

Specify Access

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

2 Configure Security

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

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

Disabled

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

Security Profile [Rule Defaults](#)

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

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

Cancel

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

لوصول ةسايس نيوكت - نمآلا لوصول

7. ظفح قوف رقنا

Access Policy

Rule Defaults and Global Settings

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

Search by rule name Intent Objects Settings

Add Rule

5 Rules

Customize view

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

Rows per page 100 1-5 of 5 1

لوصول ةسايس نيوكت - نم آلا لوصول

FTD ىلع ةماعلا تاقالعل نارتقا نم ققحتلا - 3 ةوطخلا

FTDs > ةكبشلا تالاصتإ > لاصتالل لقتنا 1.

Security Cloud Control

Organization: Cisco-jalyadav

Platform menu: Secure Access, Home, Experience Insights, **Connect**, Resources, Secure, Monitor

Connect

Essentials: **Network Connections**, Users, Groups, and Endpoint Devices, End User Connectivity, DNS Forwarders

Tunnel Groups: FTDs

0 Warning, 1 Connected

Region, Status, 2 Tunnel Groups, + Add

ةماعلا تاقالعل نم ققحتلا - نم آلا لوصول

اذه FTD ب ةنرتقملا دراوملا ضرع > FTD قوف رقنا 2.

Network Connections

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

Connector Groups **Network Tunnel Groups** FTDs

1 Synced

FTDs configured for Universal Zero Trust Access

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

Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

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

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status: Synced (2)

[View resources associated to this FTD](#)

[Associate Resources](#)

معاملة اتصالات العمل - تم قححت ال - ن مآل لوصول

Resources associated with FMC_FTD

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

Search by resource name Configuration status 2 Resources [Associate Resources](#)

Resource name	Status
Router1	Synced
Router2	Synced

[Close](#)

3. قالغا قوف رقنا

4. نمازملا ةلاح يف نيوكتلا و نرتقملا دروملا نوكي نأ بجي هنا نمو ةلاحلا نم ققحت.

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

5. فTD لىل نيوكتلا عفد نم ققحت

LINA عضو لىل لقتناو فTD ب ةصاخلا (CLI) رماوالا رطس ةهجاو لىل لوخدلا ليچستب مق

show running-config object application

```

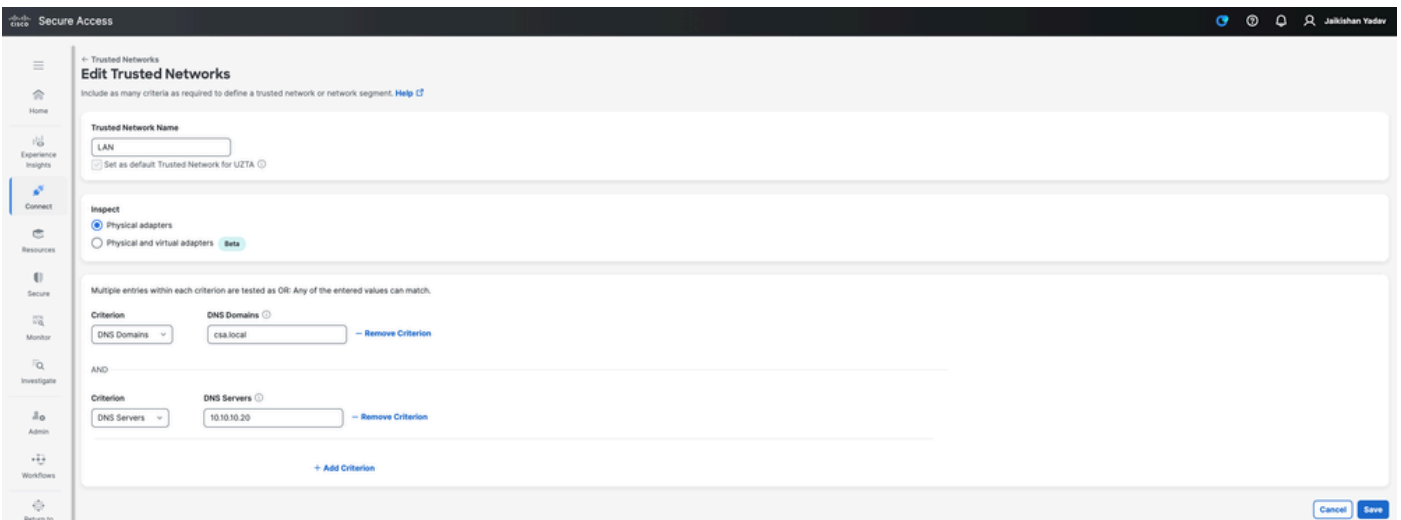
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal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

```

ةماعة لاقالعة نم ققحتللا - نمآلا لوصولا

"ZTA تاداعا وا هب قووملا تاكبشلا ةرادا " 4 configure - ةوطخلا

ZTA تاداعا > ةقثلا مادعنا لوصولا > ةئاهنلا مدختسملا لاصتا > لاصتالا للاقنا
 هب قووملا تاكبشلا نيوكتو



TND نيوكت - نمآلا لوصولا

ZTA فيرعت فلم لاصتا دروم ةفاضلا 5- ةوطخلا

قوف رقناو ةقثلا مادعنا لوصولا > ةئاهنلا مدختسملا لاصتا > لاصتالا للاقنا 1.
 ZTA فيرعت فلم ريرحتل طاقن 3

End User Connectivity Cisco Secure Client Manage servers

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

Zero Trust Access Virtual Private Network Internet Security

Enrollment methods Manage

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

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

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles Manage Trusted Networks + ZTA Profile

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

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

Edit Delete

ZTA فيرعت فلم - نمآلا لوصولا

صاخلا دروملا ةفاضإ 2.

← End User Connectivity

Create profile

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

ZTA profile name: ZTAProfile Priority: 1. Current profile

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

1 Secure Private Access 0 Destinations

2 Secure Internet Access

3 Users and Groups

Secure Private Access

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

Traffic Steering Options

Search by destination

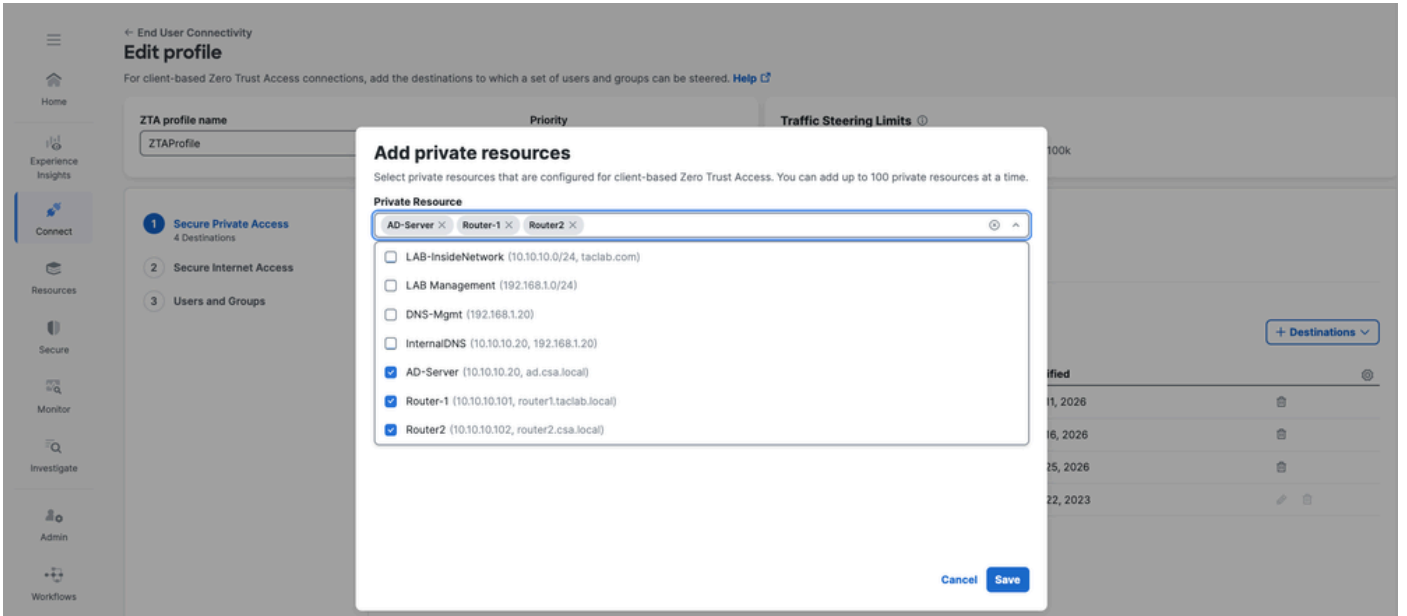
Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

+ Destinations ^

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

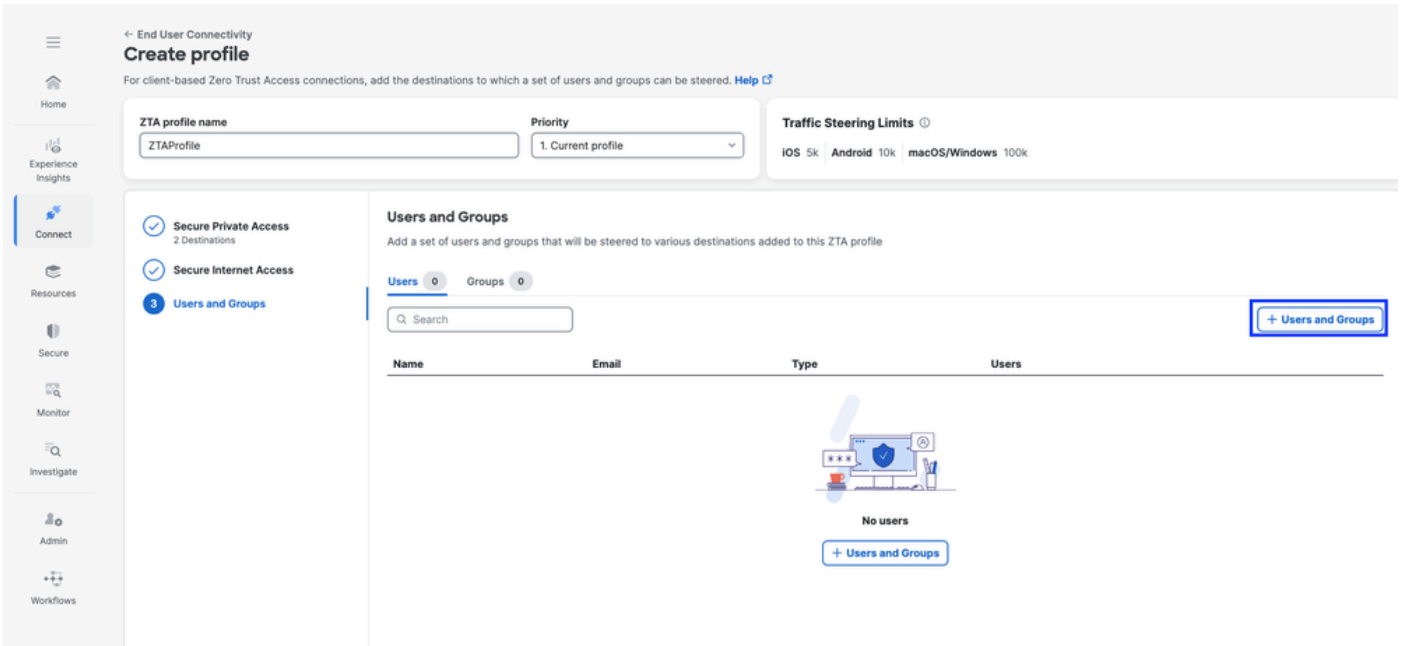
Add Destination
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

ZTA فيرعت فلم - نمآلا لوصولا



ZTA فيرعت فلم - نمآلا لوصولا

تاعومجم وني مدختسم ةفاضلا 3.



ZTA profile name: ZTAProfile

Priority: 1. Current profile

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

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

Users and Groups

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

Users 1 | Groups 0

Q Search + Users and Groups

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

Rows per page: 10

Back Close

ZTA فيرعت فلم - نمآلا لوصولا

صاخلا دروملا ىلا لوصولا نم ققحتلا 6 - ةوطخلا

1. ZTA TND ل ةكبشلا عبصا ةمصب نم ققحتلا

The screenshot displays the Cisco Secure Client interface. On the left is a navigation menu with options: General, Status Overview, AnyConnect VPN, Zero Trust Access (highlighted with a right arrow), and Umbrella. Below the menu is a 'Diagnostics' button with the text 'Collect diagnostic information for all installed components.' The main content area is titled 'Zero Trust Access' and contains four tabs: Statistics, Advanced, Configuration, and Message History. The 'Statistics' tab is active, showing a list of flow statistics:

TCP Flows:	611
Allowed UDP Flows:	48
Allowed TCP Flows:	597
Blocked UDP Flows:	111
Blocked TCP Flows:	14
Authenticated UDP Flows:	0
Authenticated TCP Flows:	0

Below the statistics are two expandable sections:

- Proxy Configurations:**
 - Secure Private Access: Active
 - Secure Internet Access: Active
- Network Fingerprints:**
 - LAN: Matched

ةم اءال ءاقالءال رابءءءا - نم آال لوصولا

2. FTD FQDN ءء ءءءبءال مءءءءءال ءرءء نم قءءءال

```

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

```

ةم اءال ءاقالءال رابءءء - نم آال لوصولا

3. فءء فءء ساء ءصاءال ءراومال ال فءء لوصول ءي ناءم نم ققءءال.

```

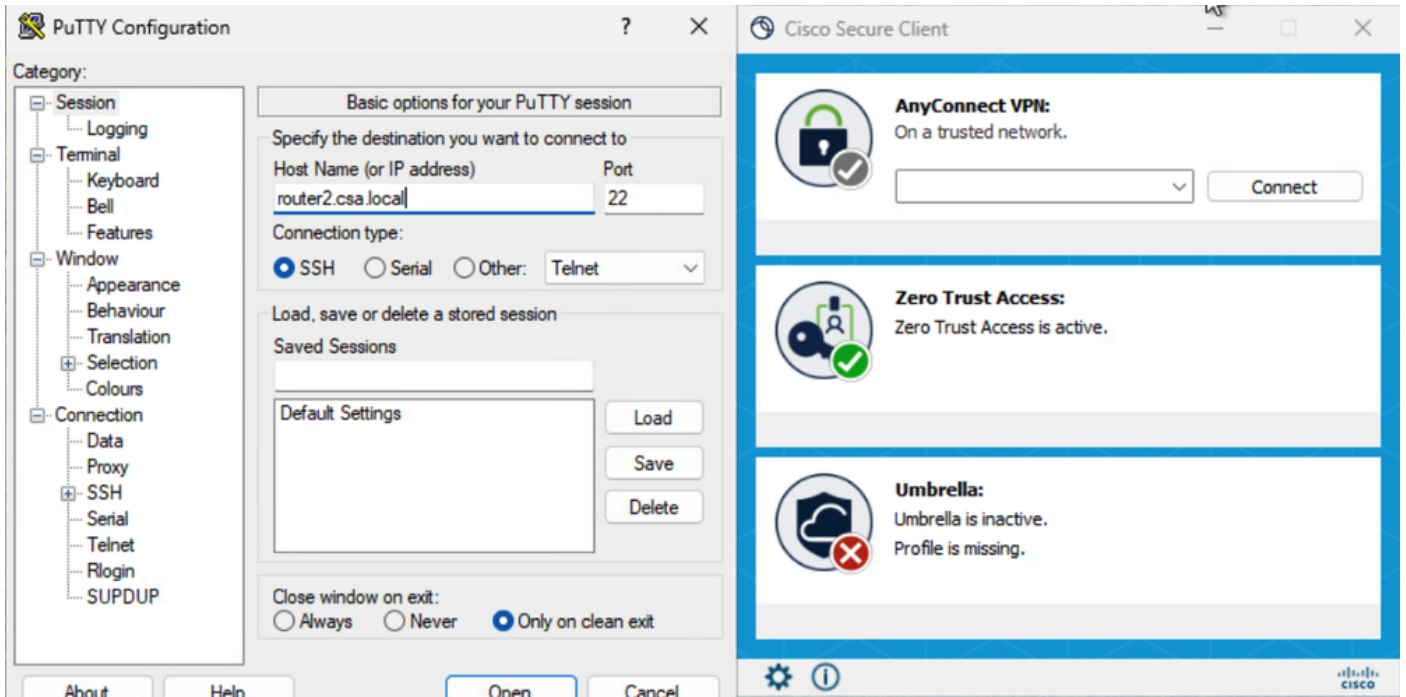
ftd# ping router2.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/60 ms
ftd# █

```

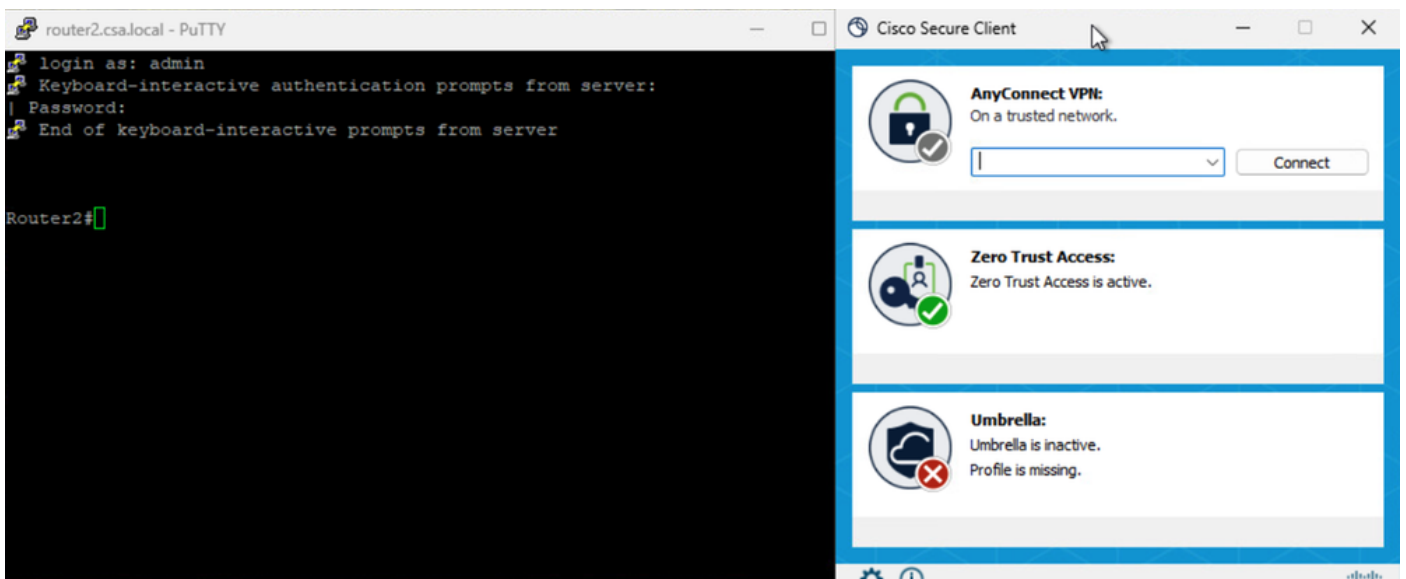
ةم اءال ءاقالءال رابءءء - نم آال لوصولا

4. صاءال ءروملاب SSH لاصءا رابءءء.

فءء فءء ساء فءء لوصولا

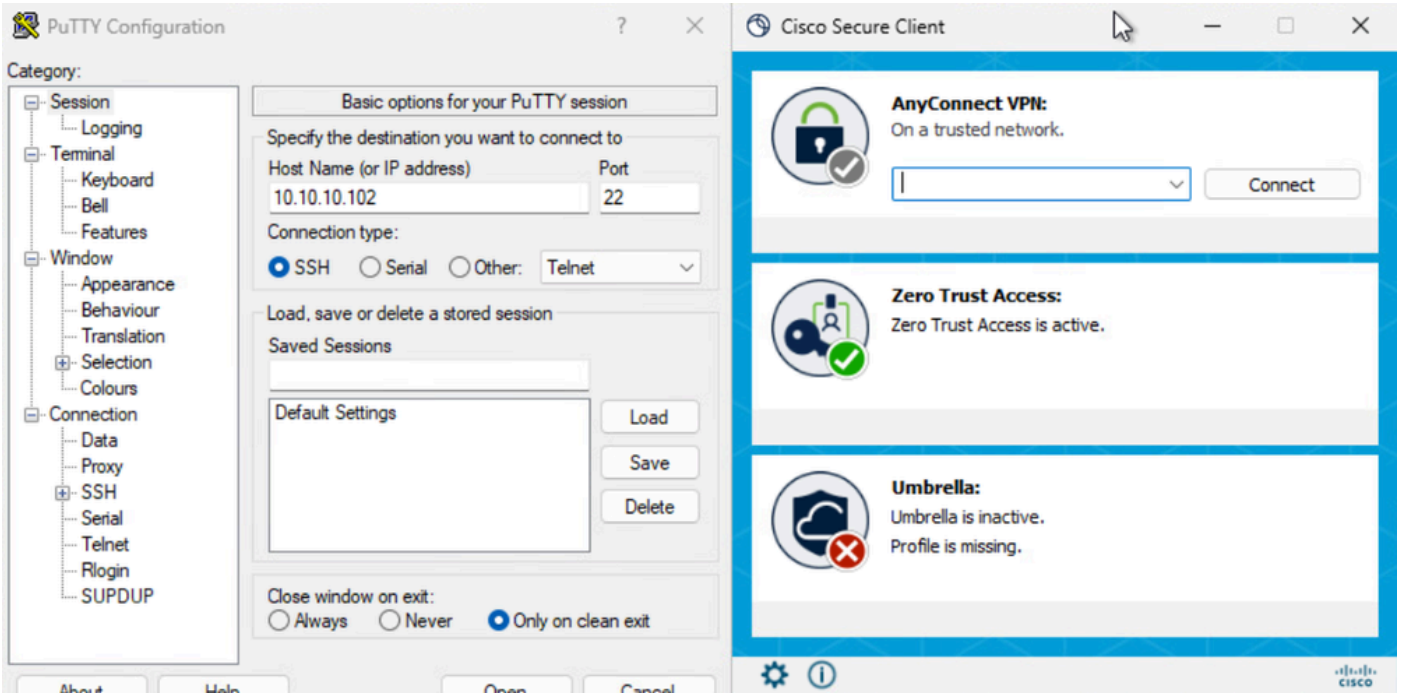


ةم اءال اءالء راءءء - نم آال لوصول

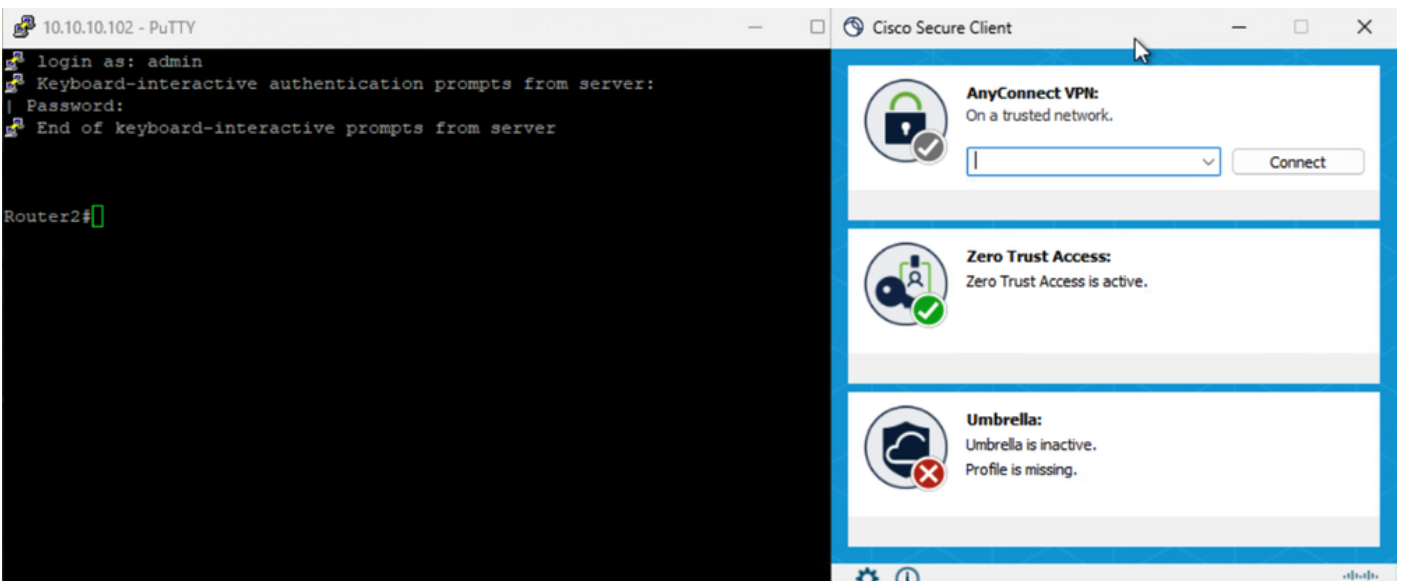


ةم اءال اءالء راءءء - نم آال لوصول

IP ناوع مءءءءءاب PR لى لوصول

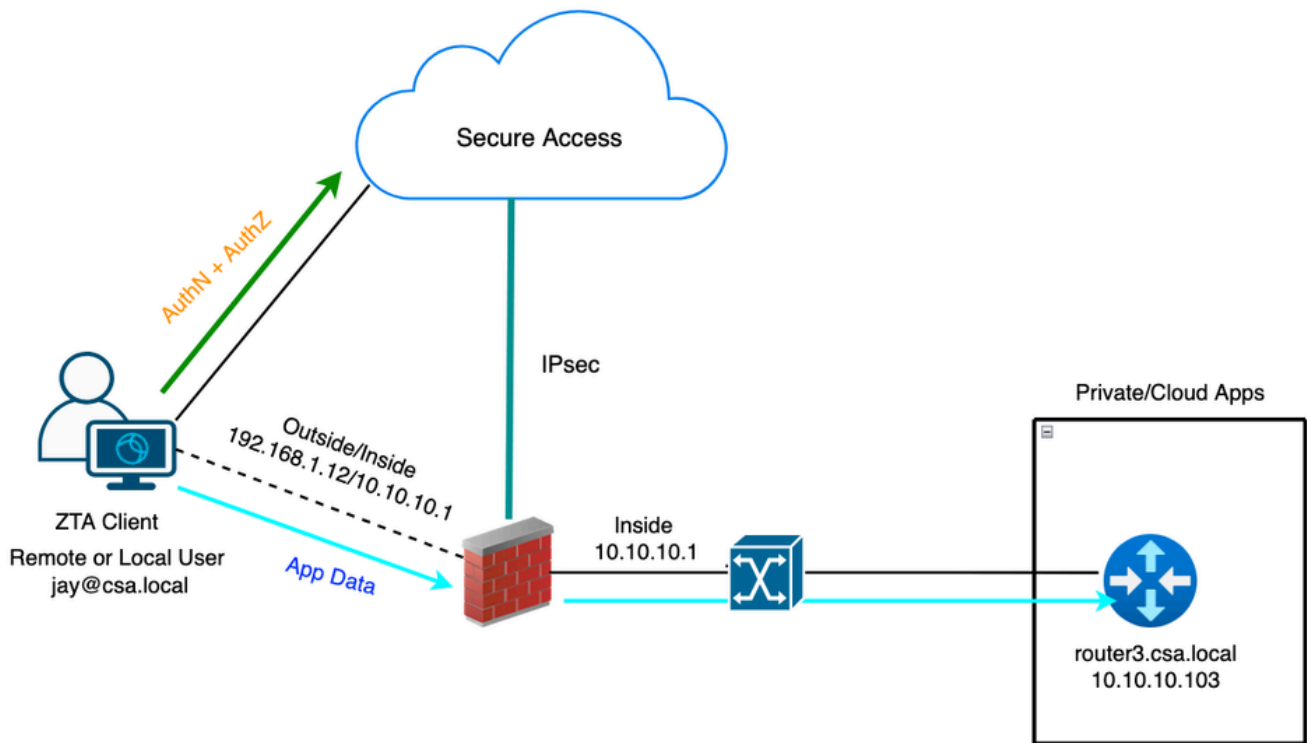


ةم اءال اءالء راءءء - نم آال لوصول



ةم اءال اءالء راءءء - نم آال لوصول

5. نم آال لوصول طاشن مءاءء الءءس نم ققءءال

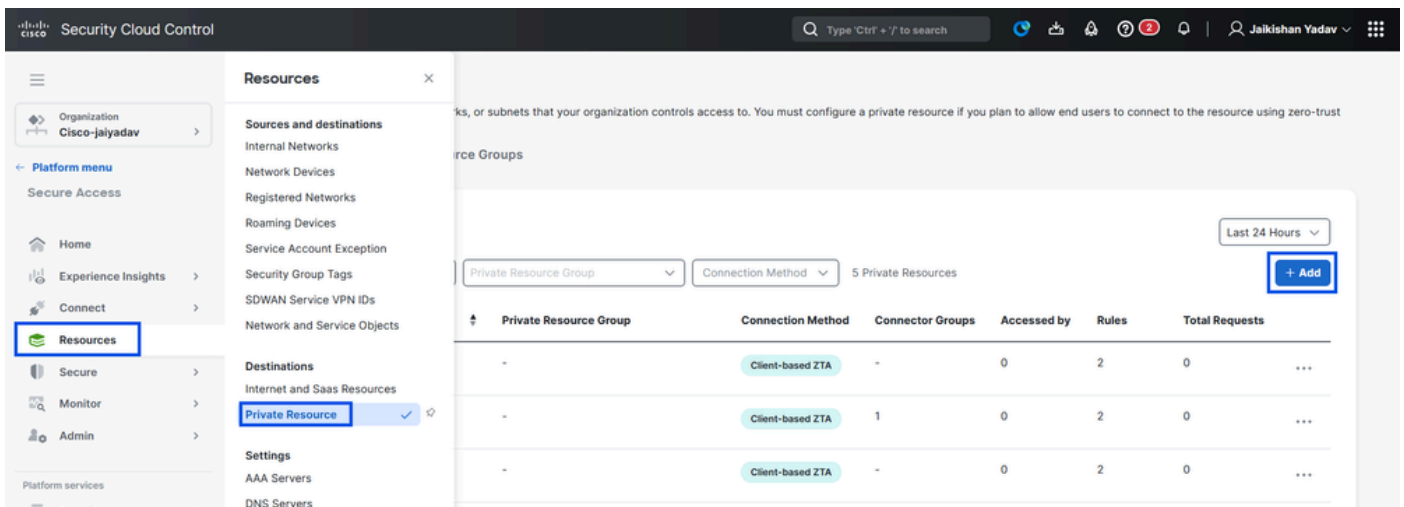


رابطخالال ةلأح ايجولوبط - يملاعلا ZTA

نمآلا لوصولال ةلأح صأخ دروم ديدحت - 1 ةوطخال

(ZTA) ةقثلال مدع ةلأح لوصولال يف لجسمل زاهجال ربع هيلال لوصولال متيل صأخ دروم نيوكت ةبأحسال صرف مادختساب

1. ةفاضلأ قوف رقنا > ةصأخالل دراومال > تاهجول > دراومال ةلأح لوصولال



ةصأخالل دراومال نيوكت - نمآلا لوصولال

يصوصون، فصولا يلع لوصول. دروملل ينعم اذا ماسا لخدأ، صاخلا دروملا ماسا يلى ةبسنلاب 2. دروملا كلام ماسا وأ دروملا نم ضرغلا لثم تامولعم ريفوتب

← Private Resources

Add a Private Resource

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

General

Private Resource Name

Description (optional)

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

صاخلا IP ناوع ديدحت اننكمي امك . هيلى لوصولا ديرت يذلا صاخلا دروملل FQDN لخدأ 3. [صاخ دروم ةفاضلا](#) عجار، تامولعمل نم ديزمل . صاخلا دروملاب

لاجملا لحل DNS مداخل ددح 4.

Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
<input type="text" value="router3.csa.local"/>	Any TCP	22	+ Protocol & Port
Remove			
<input type="text" value="192.168.1.103"/>	Any TCP	22	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.103"/>	Any TCP	22	+ Protocol & Port
Remove + IP Address/FQDN			

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

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

ةياهنلا ةطقن لاصتا بيلاسأ ديدحت 5.

ةيلحم ذيفنت طاقنك FTD ددح 6.

Endpoint Connection Methods

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

Branch Connections

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

Zero-trust connections

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

Client-based connection

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

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

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

FMC_FTD (ftd.csa.local) ✓

Will get enforced at the selected firewalls.

Local-only

Enforcement point for Remote User



Enforcement point for Local user



Cancel

Save and Test Save

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

نكمي ناك اذا اغراف هكرتاف الؤ، RC ربع صاخلا دروملا ىلا لوصولا نكمي ناك اذا RC ددح (IPsec قفن) ةكبشلا قفن ةعومجم ربع صاخلا دروملا ىلا لوصولا

Resource Connector Groups

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

Resource Connector Groups (optional)

RC-ESXI e.g. My Server Group

Choose a connector group in the same data center, branch office, or security zone as the resource.

ةصاخلا دراوملا نيوكت - نمآلا لوصولا

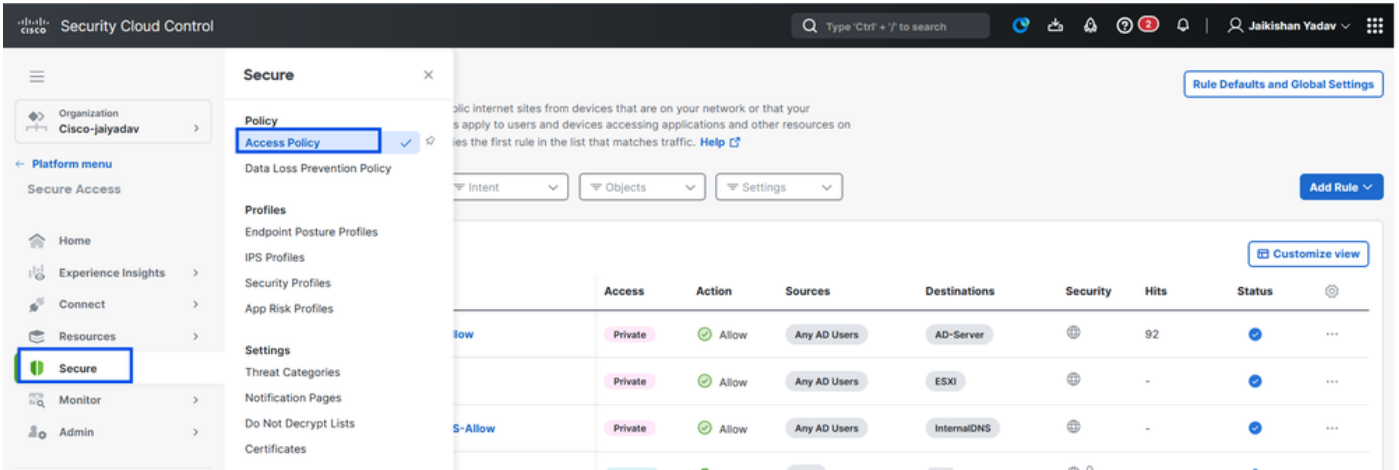
PR نارقاب ريغيغتلا اذه موقيس ، هددحت يذلا ليچستلا عون ىلع ادامتعا :ةظحالم جهنلا رشن ليغشت ىلا يدؤيسو FTD ب ايئاقلت

ظفح قوف رقنا 7.

ةصاخ لوصولو ةدعاق عاشنإ - 2 ةوطخلا

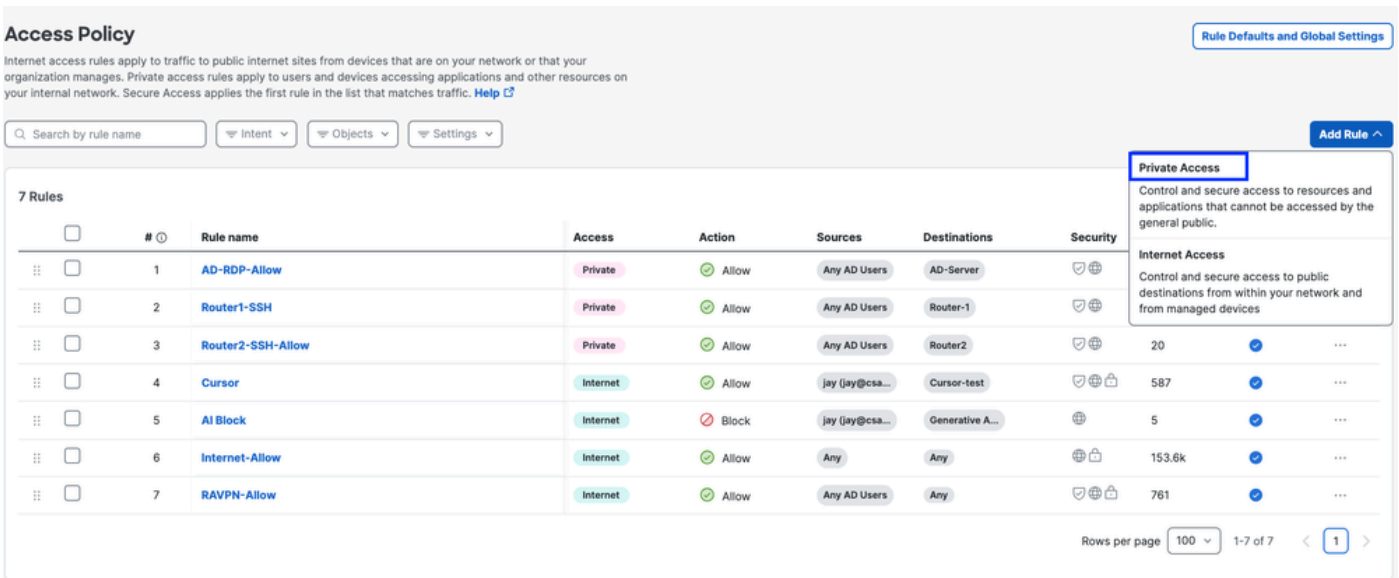
في عمل ال ZTA في نولجسمل نوم دختسمل انكمتيل Secure Access لى صاخ لوصو نيوكت
صاخلا لوصولا دعاق عجار، تامولعمل نم ديزمل . هيل لوصولا نم

1. لوصولا جهن > نم آلى لقتنا



لوصولا ةسايس نيوكت - نم آلا لوصولا

2. Private Access رتخأ مث ، دعاق ةفاضل قوف رقتنا .
 لكب ةصاخلا دعاقلا ل نوكملا تانوكملا فصلي صخلم دجوي دعاقلا لىل عأ في



لوصولا ةسايس نيوكت - نم آلا لوصولا

3. دعاق مسافاضا

Add Router3-SSH-Allow

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

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

لوصول ةسايس نيوكت - نمآلا لوصول

ةهجولاو ردصملا دحو ةدعاقلا ءارجا دح. 4.

Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

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

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From

Specify one or more sources

AD Users • Any AD Users

To

Specify one or more destinations

Private Resources • Router3

+ AND

لوصول ةسايس نيوكت - نمآلا لوصول

ةياهنلا ةطقن تابلطتم نيوكت. 5.

Endpoint Requirements

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

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

For Branch connections:

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

User Authentication Requirements

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

2 Configure Security

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

Cancel

Back Next

لوصول ةسايس نيوكت - نمآلا لوصول

6. نامآلا نيوكت

Specify Access

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

2 Configure Security

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

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

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

Cancel

Back Save

لوصول ةسايس نيوكت - نمآلا لوصول

7. ظفح قوف رقنا

Access Policy

[Rule Defaults and Global Settings](#)

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

Search by rule name Intent Objects Settings

[Add Rule](#)

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

Rows per page 100 1-8 of 8

لوصول ةسايس نيوكت - نم آل لوصول

FTD ىلع ةماعلا تاقالعل نارثقا نم ققحتلا - 3 ةوطخلا

FTDs > ةكبشلا تالاصتلا > لاصتال لقتنا 1.

The screenshot shows the Cisco Security Cloud Control interface. The 'Connect' section is active, displaying 'Network Connections' under 'Essentials'. A 'Warning' icon is visible next to the '0' count, and a 'Connected' icon is next to the '1' count. The 'FTDs' tab is selected, showing a '2 Tunnel Groups' summary. The interface includes a search bar, navigation menu, and various status indicators.

ةماعلا تاقالعل نم ققحتلا - نم آل لوصول

اذه FTD ب ةنرتقملا دراوملا ضرع > FTD قوف رقنا 2.

```

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
Address:  192.168.1.12

```

ةم اءال اءالء الء نم قءءء الء - نم آال لوءولء

Network Connections

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

Connector Groups Network Tunnel Groups **FTDs**

1 Syncing 0 Synced

FTDs configured for Universal Zero Trust Access

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

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

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

Associated Resources 3

RESOURCES ASSOCIATED BY STATUS

Status: Synced 3

[View resources associated to this FTD](#)

[Associate Resources](#)

ةم اءال اءالء الء نم قءءء الء - نم آال لوءولء

```
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
```

ةمإعلا تاقالعلال نم ققحتلا - نمآلا لوصولا

Resources associated with FMC_FTD

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

<input type="text" value="Search by resource name"/>	<input type="text" value="Configuration status"/>	3 Resources	Associate Resources
Resource name	Status		
Router-1	<input checked="" type="checkbox"/> Synced		
Router2	<input checked="" type="checkbox"/> Synced		
Router3	<input checked="" type="checkbox"/> Synced		

Close

ةم اءال اءاقال اءال نم ققءءال - نم آال لوصول

قءلءا قوف رقنا 3.

ةنم اءمال ءلءل ف نل وءءل او نرءق مءل ءروم ل نوكل نأ بءل هنأ نم وءلءل نم ققءء 4.

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

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

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

Q Search by FTD name FMC Name Configuration status 1 FTDs

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

FMC_FTD

Firewall Details

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

UZTA Configuration status

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

Assigned Trusted Network

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

Edit assignment + Trusted network

Associated Resources 3

RESOURCES ASSOCIATED BY STATUS

Status: Synced 3

View resources associated to this FTD

Associate Resources

ةمإعلا تاقالعلل نم ققحتلا - نمآلا لوصولا

5. فTD لىل نىوكتلا عفد نم ققحت

LINA عضو لىل لقتناو FTD ب ةصاخلا (CLI) رماوالا رطس ةهجاو لىل لوخدلا لىجستب مق

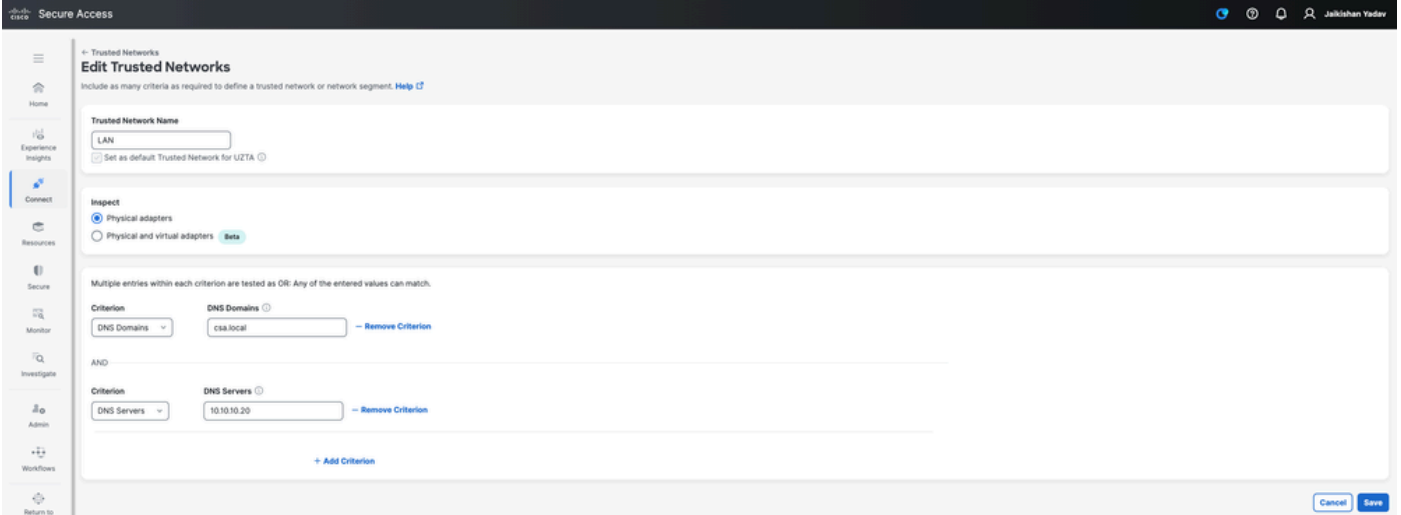
show running-config object application

```
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
```

ةم اءل اءالءل نم قءءءل - نم آل لوءول

" اءنم قءءءل و آ ZTA اءاءءل و آه ب قوءومل اءكبلل نل ءوء 4 - ءوءل

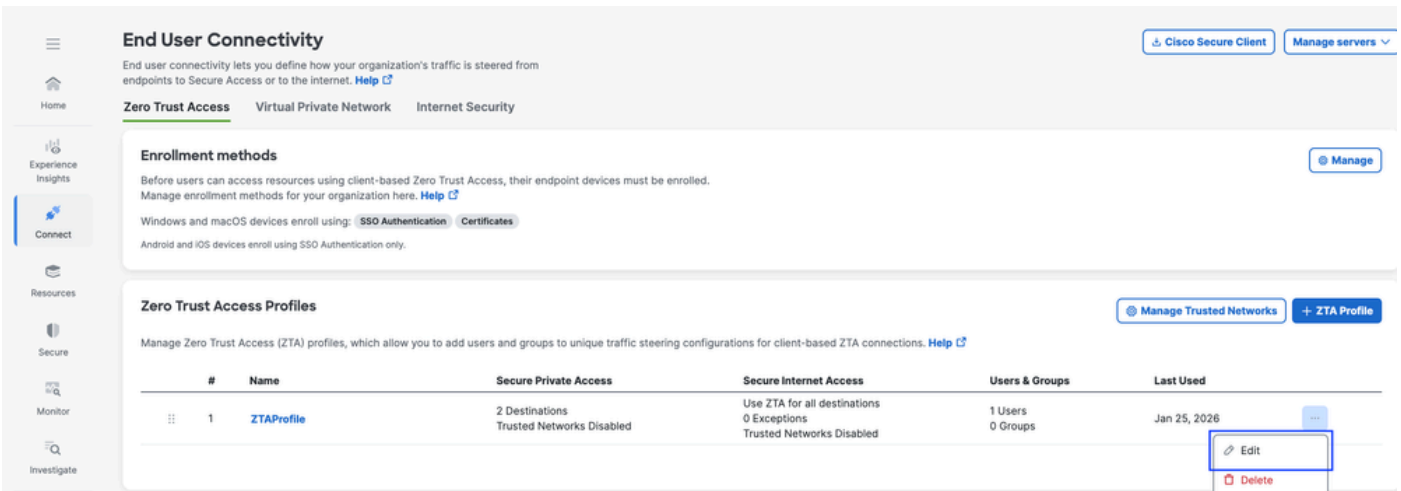
ZTA اءاءءل > ءقءل اءءءنل ل لوءول > ءئاهنل اءءءسمل لاءءل > لاءءال ل لءءنل
ه ب قوءومل اءكبلل نل ءوءل



ZTA TND نل ءوء - نم آل لوءول

ZTA ءلءء ءلم ل لءل صاء ءروم ءءاضل 5 - ءوءل

قوء رءنل ءقءل اءءءنل ل لوءول > ءئاهنل اءءءسمل لاءءل > لاءءال ل لءءنل 1.
ZTA ءلءء ءلم رلءءل ءاقن 3



ZTA ءلءء ءلم - نم آل لوءول

صاخال درومال ةفاضل 2.

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

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

1 Secure Private Access
0 Destinations

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

Traffic Steering | Options

Search by destination

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

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

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

ZTA فيرعت فلم - نمآلا لوصولا

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

ZTA profile name: ZTAProfile

1 Secure Private Access
5 Destinations

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

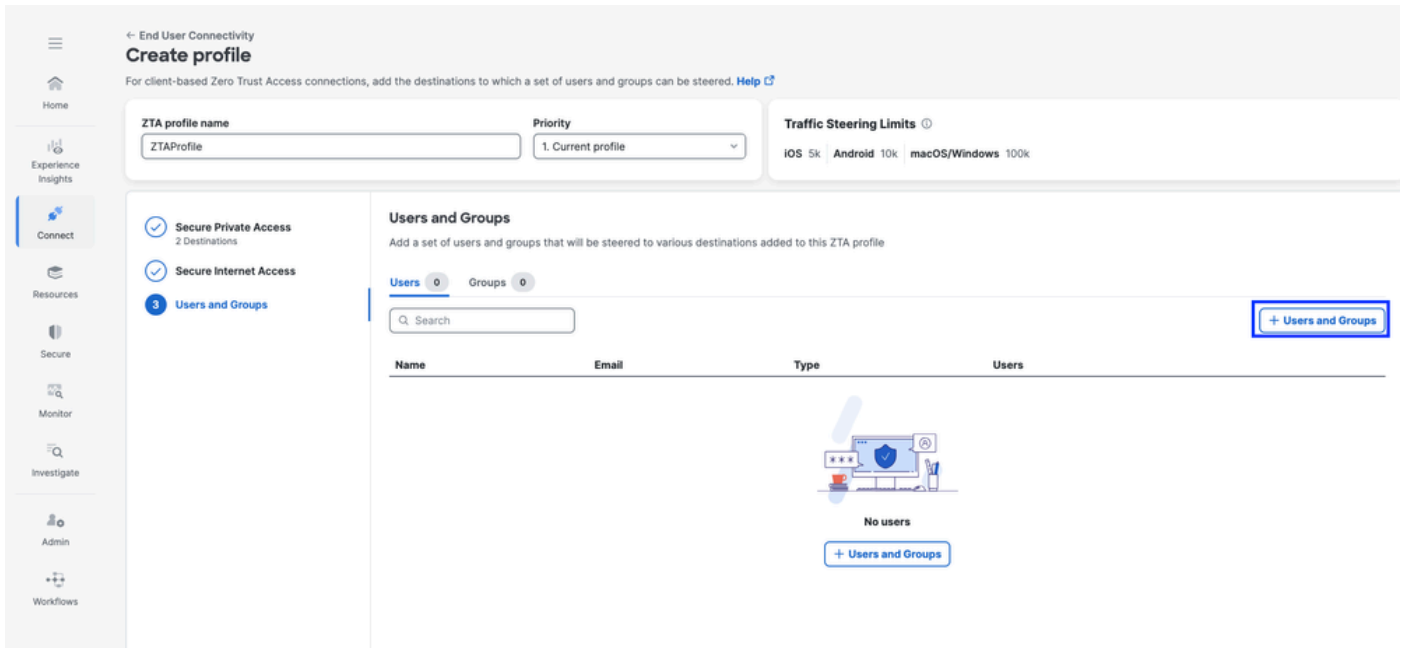
Private Resource

- AD-Server (10.10.10.20, ad.csa.local)
- DNS-Mgmt (192.168.1.20/32)
- Router2 (10.10.10.102, router2.csa.local)
- Router-1 (10.10.10.101, router1.csa.local)
- Router3 (10.10.10.103, 192.168.1.103, router3.csa.local)

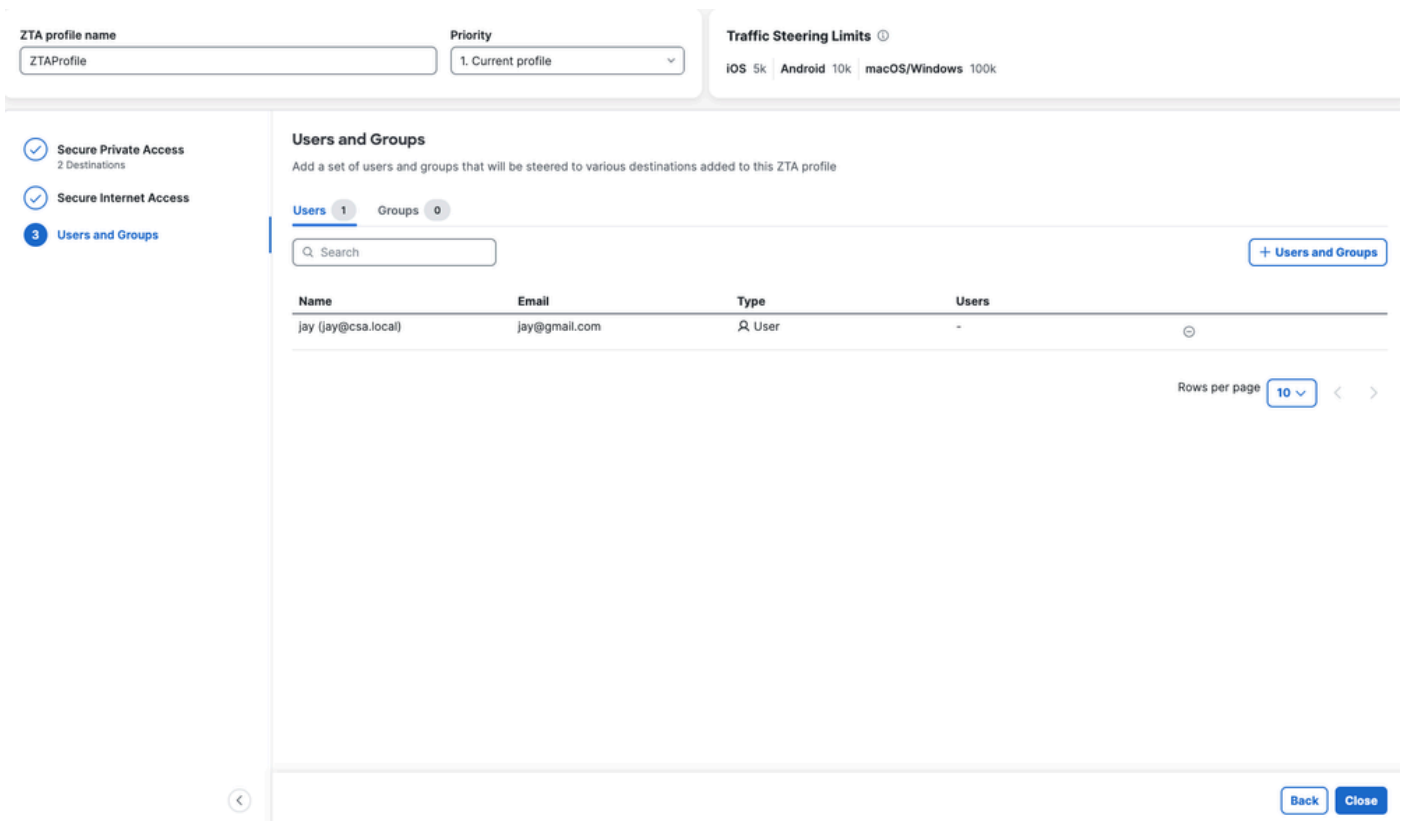
Cancel Save

ZTA فيرعت فلم - نمآلا لوصولا

تاعومومو ني مدختسم ةفاضل 3.



ZTA فيرعت فلم - نمآلا لوصولا

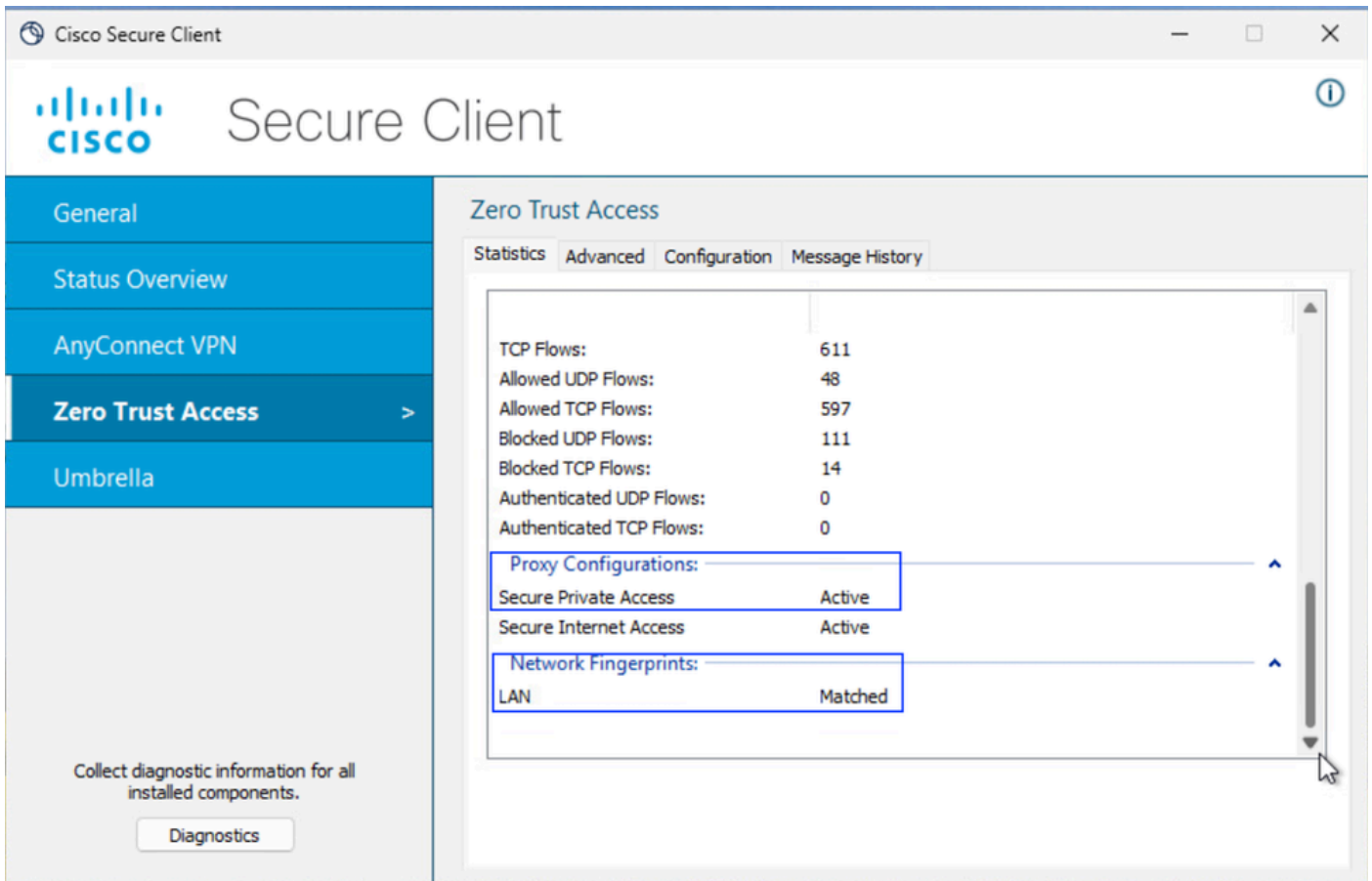


ZTA فيرعت فلم - نمآلا لوصولا

صاخال دروملا إلى لوصولا نم ققحتال 6 - ةوطخال

يلحم مدختسملا نوكي ام دنع

1. نم آوي لح م مدختس م ل انا اذ ا ق باطت ن ا ب جي و ، ZTA TND ل ا ك ب ش ل ا م ص ب ن م ق ق ح ت .
اطش ن نو ك ي ن ا ب ج ي ص ا خ ل و ص و



ة م ا ل ا ت ا ق ا ل ع ل ا ر ا ب ت خ ا - ن م ا ل ا ل و ص و ل ا

2. ل ح ي ل ع د ي ع ب ل ا م د خ ت س م ل ا ة ر د ق ن م ق ق ح ت ل ا . 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

```

ةم اءل اءاقل اءل راءءءء - نء آلا لوصولا

3. FQDN مءءءءءءء صاءءل ءراومل ال ال فءء لوصول ءل نء ققءءل ال

```

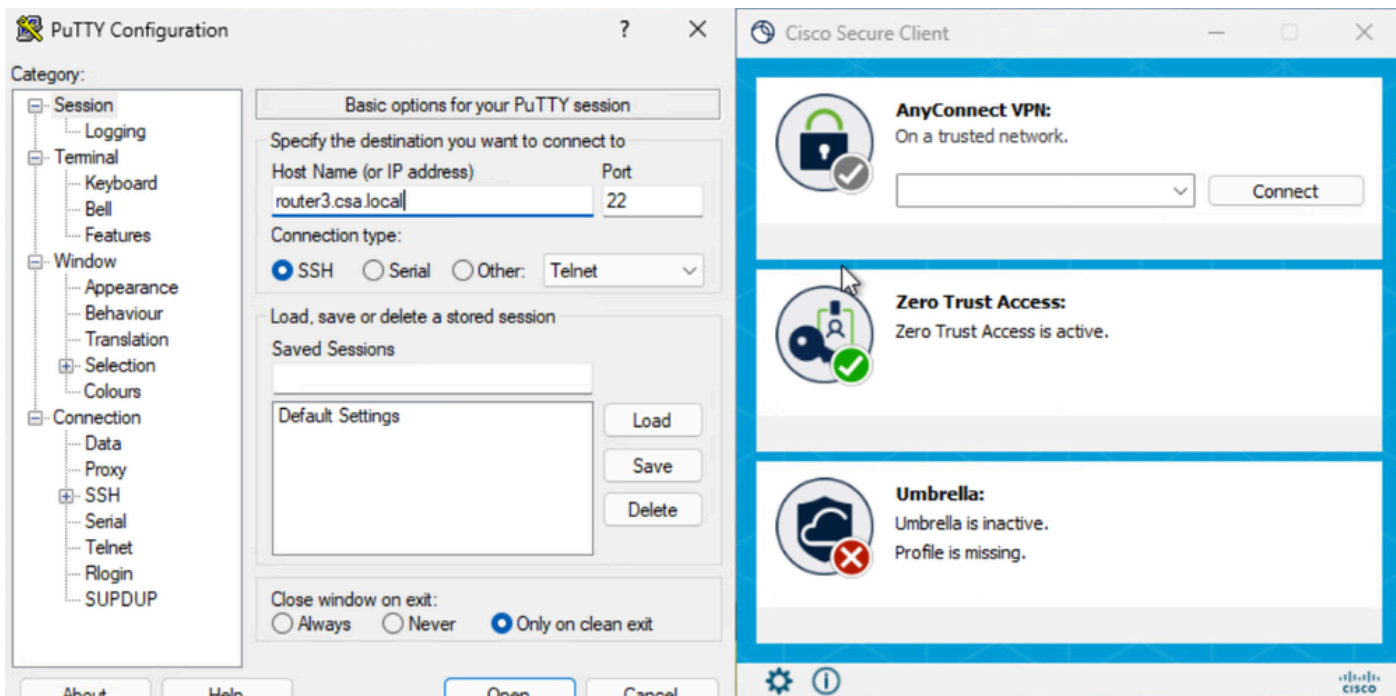
ftd# ping router3.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.103, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd# █

```

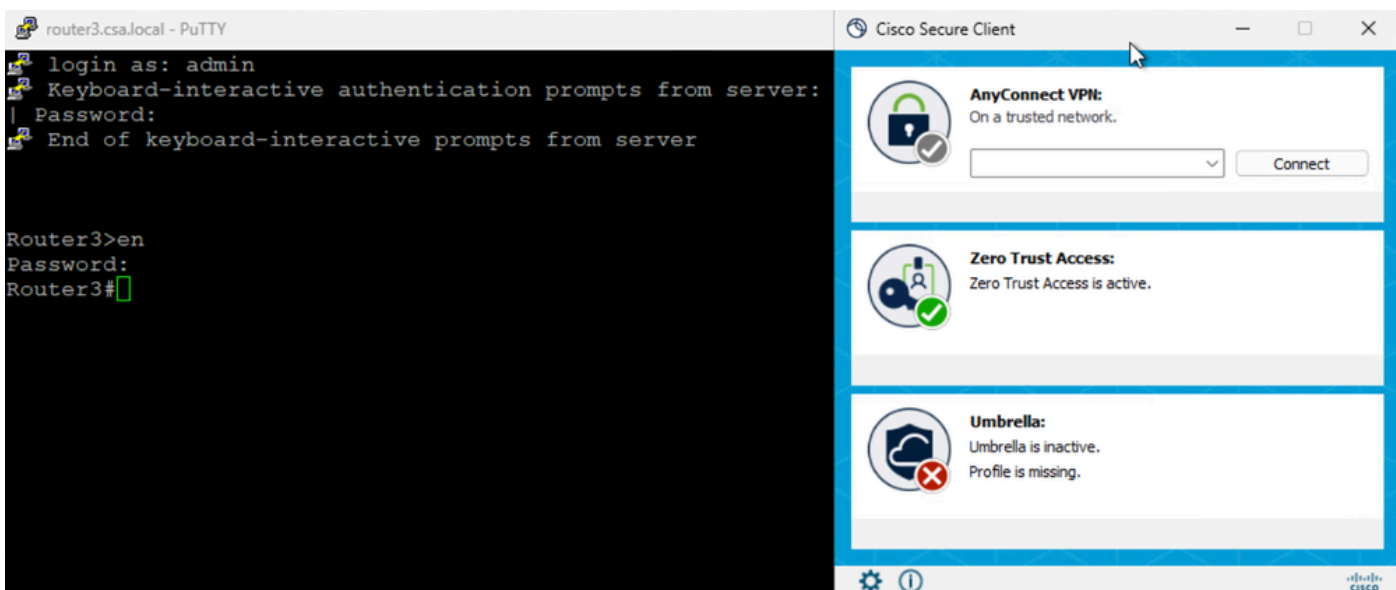
ةم اءل اءاقل اءل راءءءء - نء آلا لوصولا

4. صاءءل ءرومل اء SSH لاصءا راءءءء

FQDN مءءءءءءء PR ال لوصولا

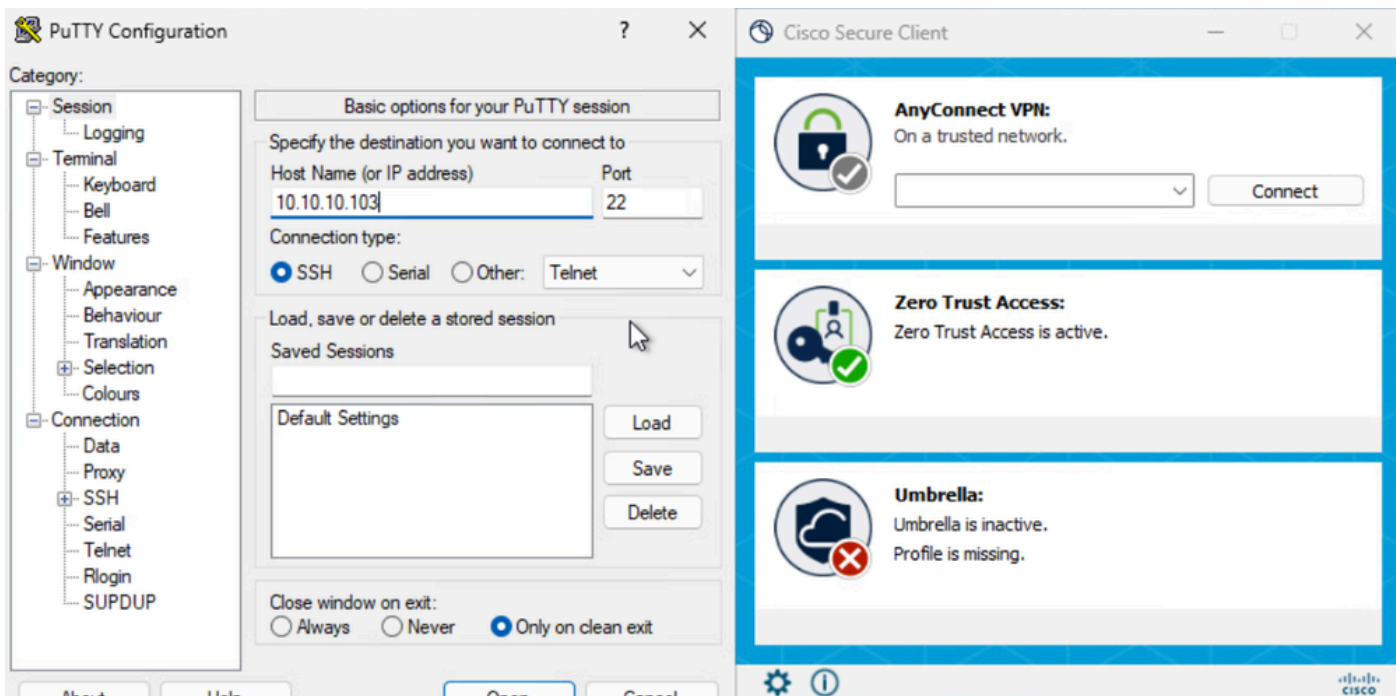


ةم اءال اءالء راءءء - نم آلا لوصول

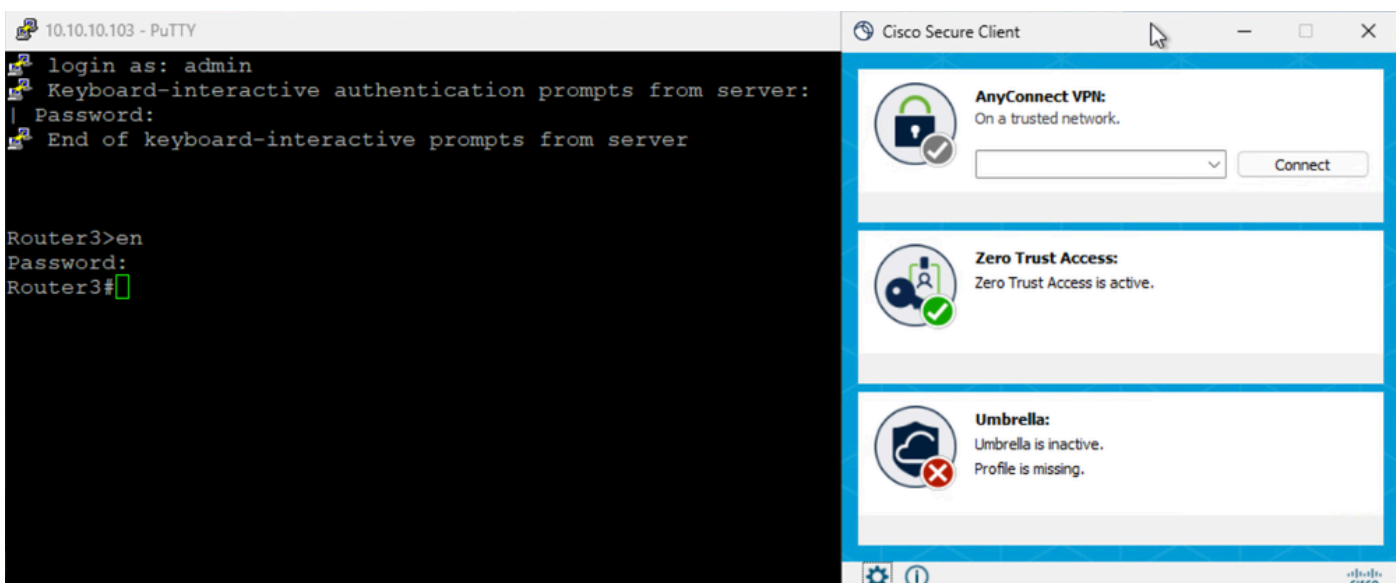


ةم اءال اءالء راءءء - نم آلا لوصول

IP ناوع مءءءءاب PR ءل لوصول



ةم اءالء اءالء راءءءء - نم آالء لوصولء



ةم اءالء اءالء راءءءء - نم آالء لوصولء

5. نم آالء لوصولء طاشن مءاءء الءءء نم ققءءءالء

Activity Search

Search by domain, identity, or URL Advanced CLEAR

Filters: **DOMAIN** router3.csa.local

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

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

ةطشنأل نع شحبلا - نمآلا لوصولا

Activity Search

Search by domain, identity, or URL Advanced CLEAR

Filters: **RESPONSE** Allowed

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

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

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 6:40 AM

Access details

Identity: jay (jay@csa.local)

ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: LAN

Enforcement Point: FTD> FMC_FTD

Destination: router3.csa.local

Destination IP: 10.10.10.102

ةطشنأل نع شحبلا - نمآلا لوصولا

FMC لاصتا اءءء نم ققءءلا 6.

Firewall Management Center

Events & Logs / Analysis / Unified Events

Search: Deploy admin

Events Troubleshooting

Destination IP: 10.10.10.103

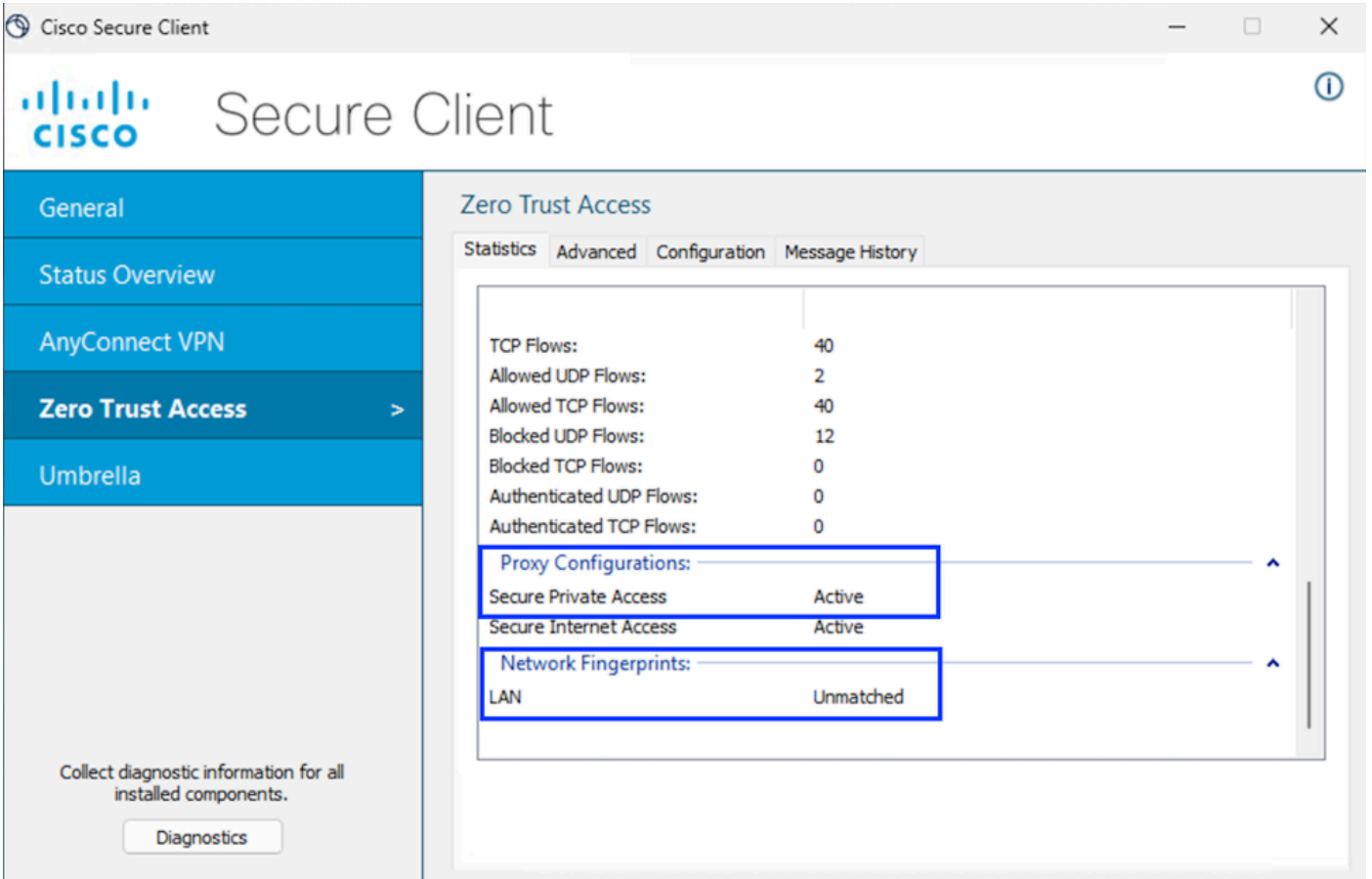
4 events

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

FMC لاصتا اءءء

ديعب مدختسمل نوکي آمدنع

1. مدختسمل ناک اذا اهتقباطم مدع بجي، ZTA TND ل ةكبشلا ةمصب، لاثملا لپس یلع ديعب



ةماعلا تاقالعل رابتخا - نمآلا لوصولا

2. ل یلع ديعبلا مدختسمل ةردق نم ققحتلا

```
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>

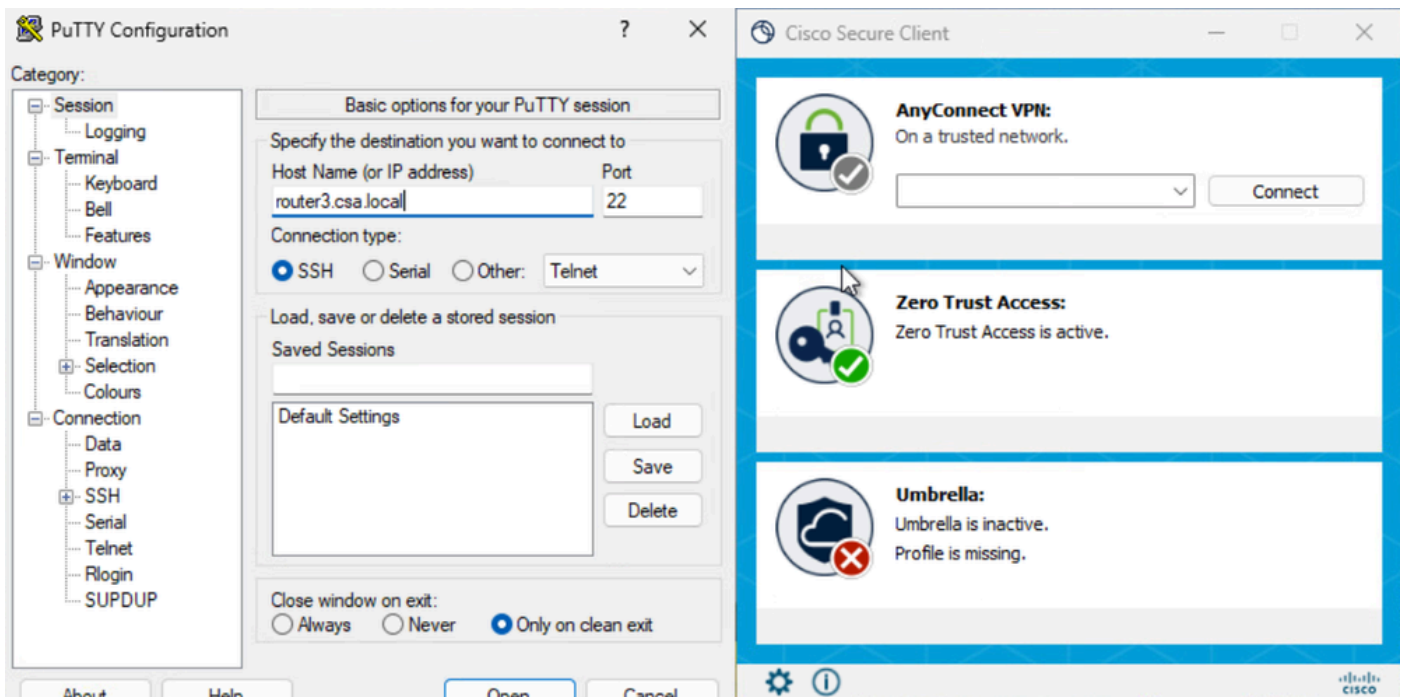
C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

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

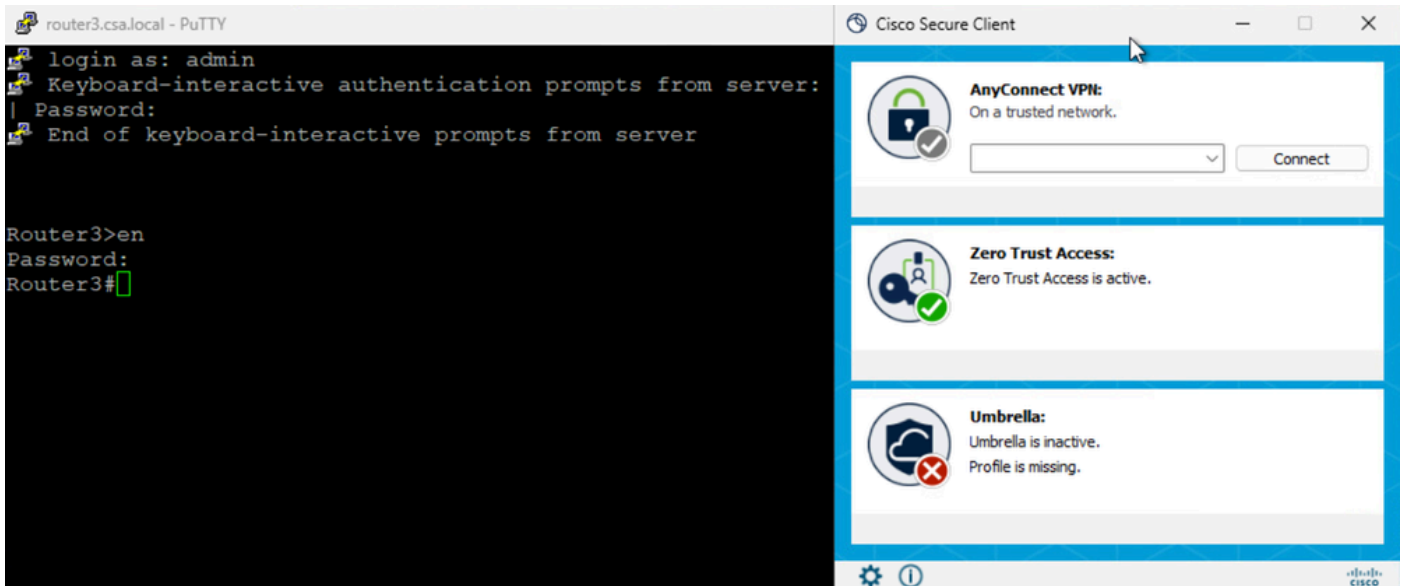
تم اعادة اتصالات الـ رابته | - نم آلا لوصول

3. صاخال دروملاب SSH لاصتا رابته |

FQDN م ادختساب PR لى لوصول

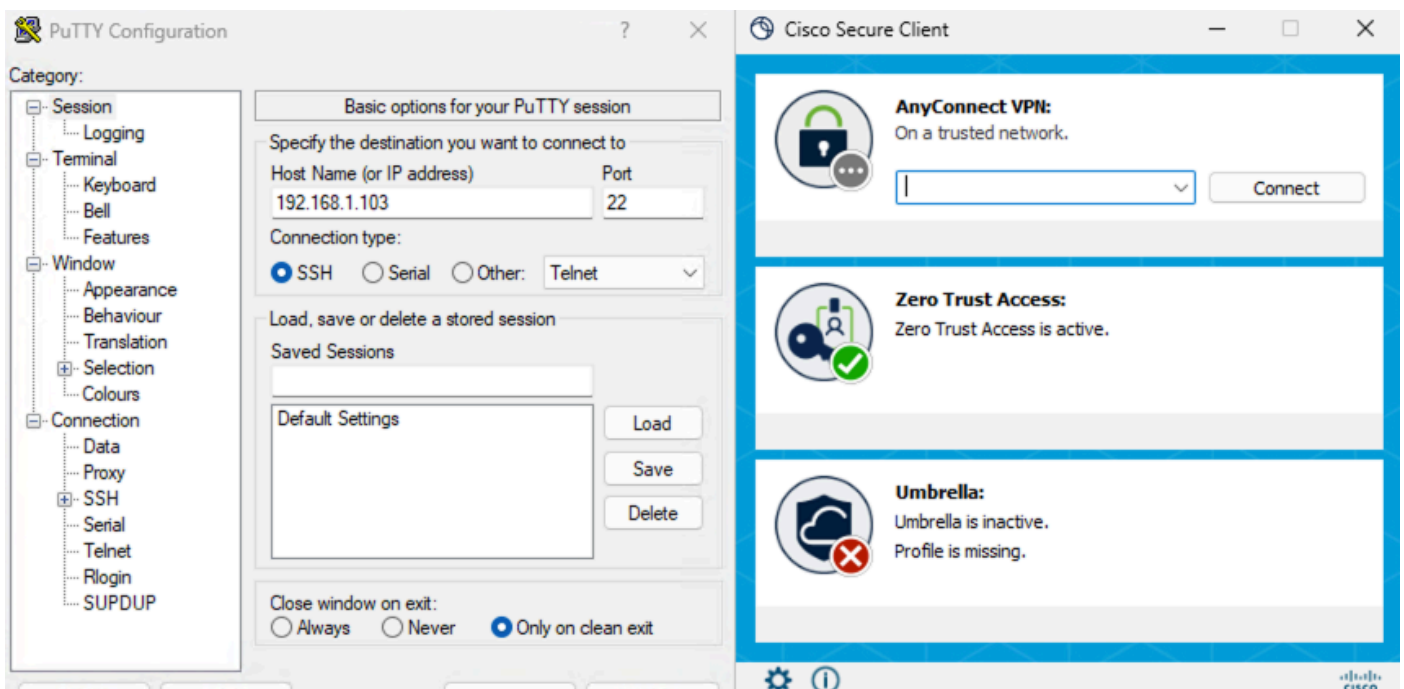


تم اعادة اتصالات الـ رابته | - نم آلا لوصول

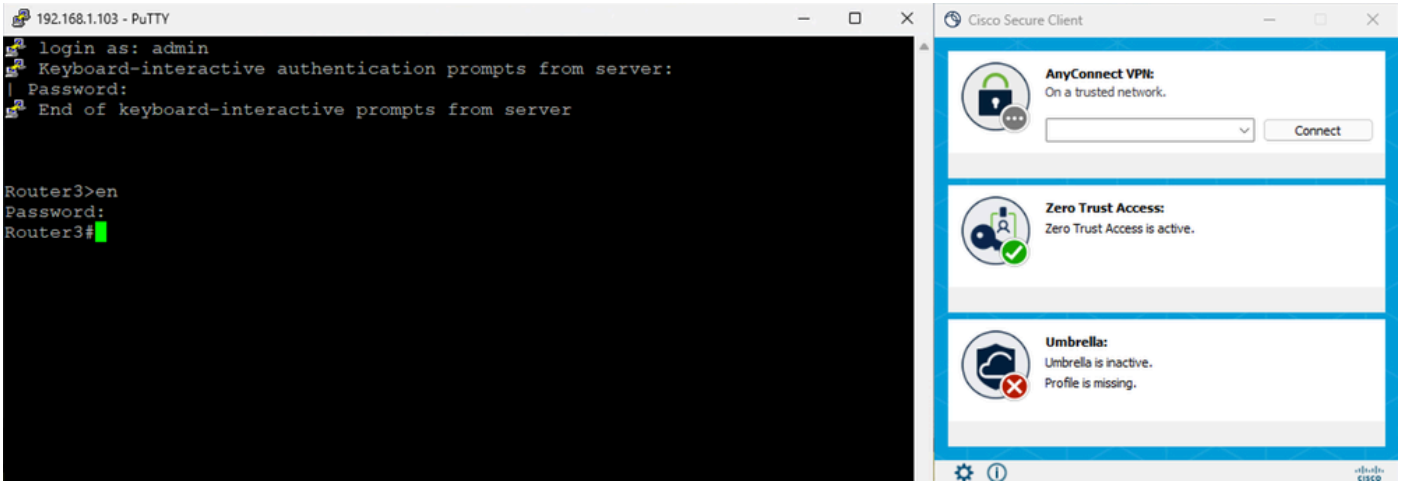


ةماعلا تاقالعل رابتخا - نمآلا لوصول

IP ناوئع مادختساب PR ىلا لوصول



ةماعلا تاقالعل رابتخا - نمآلا لوصول



عمال تاقال عمل راب تخ | - نم آلا لوصول

5. نم آلا لوصول طاشن مداخل تالجس نم ققحت ال

Activity Search

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

Response: Allowed

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM

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

طاشن آلا نع شح بل - نم آلا لوصول

Activity Search

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

Response: Allowed

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM

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

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 7:30 AM

Access details

Identity: Jay (Jay@csa.local)

ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: router3.csa.local

Destination IP: 192.168.1.103

اهحالصإو ءاطخال فاشكتسا

ةديفم رماوأ

```
> زكرملا صيصخت فلم راهظإ  
> ASP-DP لوكوتورب صحف راهظإ  
> sh running-config universal-zero-trust  
> ةهجالل IP زجوم راهظإ
```

```
> debug universal-zero-trust zproxy 7
```

ررربخال عضو لىع وهورب نيديعبو!

```
# tail -f /ngfw/var/log/messages
```

```
# لكلا راهظإ
```

```
# لىصافت ضرع nat
```

```
# ASP لودج ذخأم راهظإ
```

