使用Catalyst SD-WAN自動隧道配置安全訪問，實現安全專用訪問

目錄

簡介

本文檔介紹如何使用Catalyst SD-WAN自動隧道為安全專用訪問配置安全訪問。

背景資訊

隨著組織超越傳統的基於外圍的網路，安全訪問私有資源與保護網際網路流量同等重要。應用程式不再侷限於單個資料中心，它們現在跨內部部署環境、公共雲和混合架構運行。這一轉變要求採取更加靈活和現代化的方式實現私有訪問。

這就是基於SASE的架構和思科安全訪問發揮作用的地方。思科安全接入不依賴於傳統VPN集中器和平板網路訪問，而是將私有連線作為雲交付的服務提供，將VPN即服務(VPNaaS)和零信任網路訪問(ZTNA)相結合。

對於網路級專用訪問，Cisco Secure Access使用自動化站點到站點IPsec隧道與SD-WAN整合。這些隧道允許私有流量在安全訪問和本地或雲網路之間安全流動，同時保持將安全檢查和策略實施集中到雲中。從運營的角度來看，這消除了部署和維護傳統VPN頭端的需要，並簡化了環境增長時的擴展。

在VPNaaS模型中，安全訪問充當雲中的VPN終端點。SD-WAN通過安全訪問處理智慧路由和恢復能力，並確保流量在到達私有資源之前受到一致的安全策略的保護和管理。

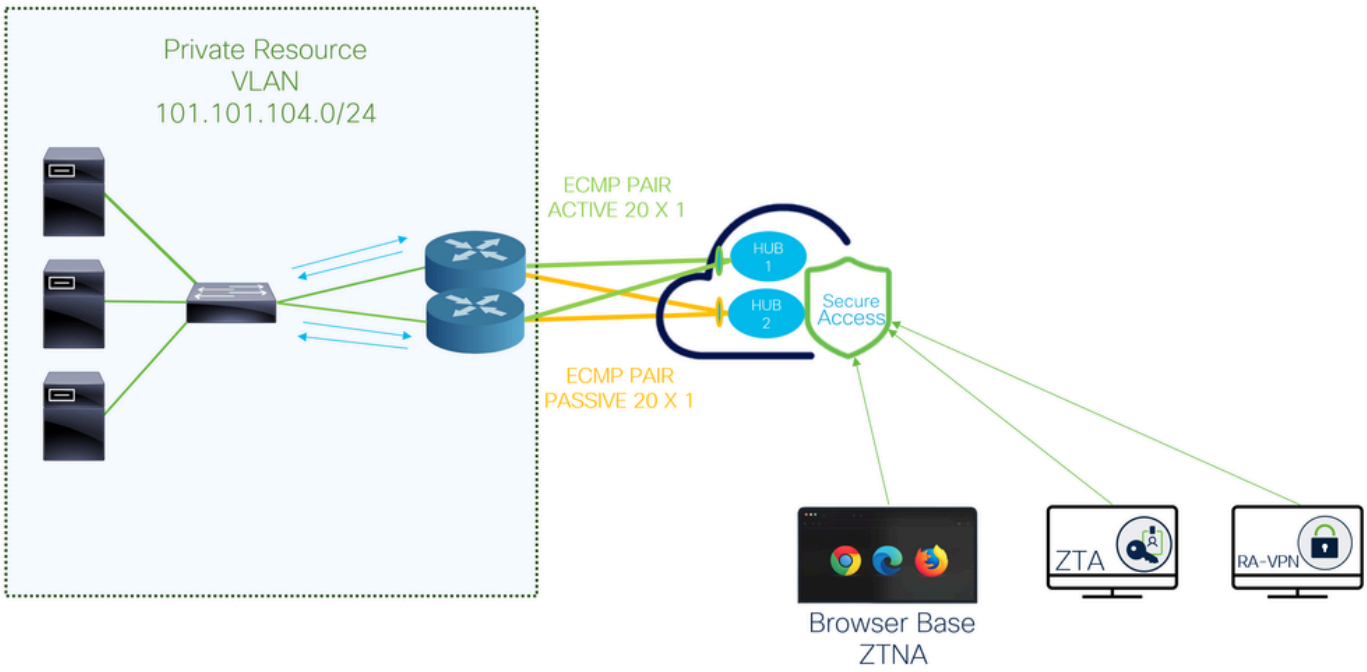
思科安全訪問還支援高級站點到站點隧道架構，包括多區域回程。此功能允許組織同時建立到多個安全訪問區域的隧道，從而提供地理冗餘和更高的可用性。通過連線到不同的區域，流量可以在發生區域故障、延遲降低或維護事件時自動進行故障切換。

例如，組織可以建立從其SD-WAN環境到倫敦和德國安全接入區域的站點到站點隧道。兩個隧道都保持活動狀態，實現了跨區域的彈性專用接入，並確保即使一個區域不可用，也能保持連續性。這種多區域設計增強了高可用性，提高了容錯能力，並符合企業級可復原性要求。

為了獲得更精細的訪問，思科安全訪問實施零信任網路訪問(ZTNA)模型。ZTNA不是授予使用者廣泛的網路連線，而是根據身份、裝置狀態和情景只允許訪問特定應用。此方法顯著減少了攻擊面，並且符合零信任原則。

ZTNA訪問通過站點到站點通道和資源聯結器的組合啟用。資源聯結器是輕量級虛擬裝置，用於建立僅出站連線到安全訪問，這意味著永遠不需要將私有資源直接暴露到網際網路上。

網路圖表



必要條件

需求

- 安全訪問知識
- Cisco Catalyst SD-WAN管理器版本20.18.2和Cisco IOS XE Catalyst SD-WAN版本17.18.2或更高版本
- 路由和交換的中級知識
- ECMP知識
- VPN知識
- 由於此整合基於受控可用性，因此需要提交TAC案例以請求在思科安全訪問中啟用該功能

採用元件

- 安全訪問租戶
- Catalyst SD-WAN管理器版本20.18.2和Cisco IOS XE Catalyst SD-WAN版本17.18.2
- Catalyst SD-WAN管理員

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

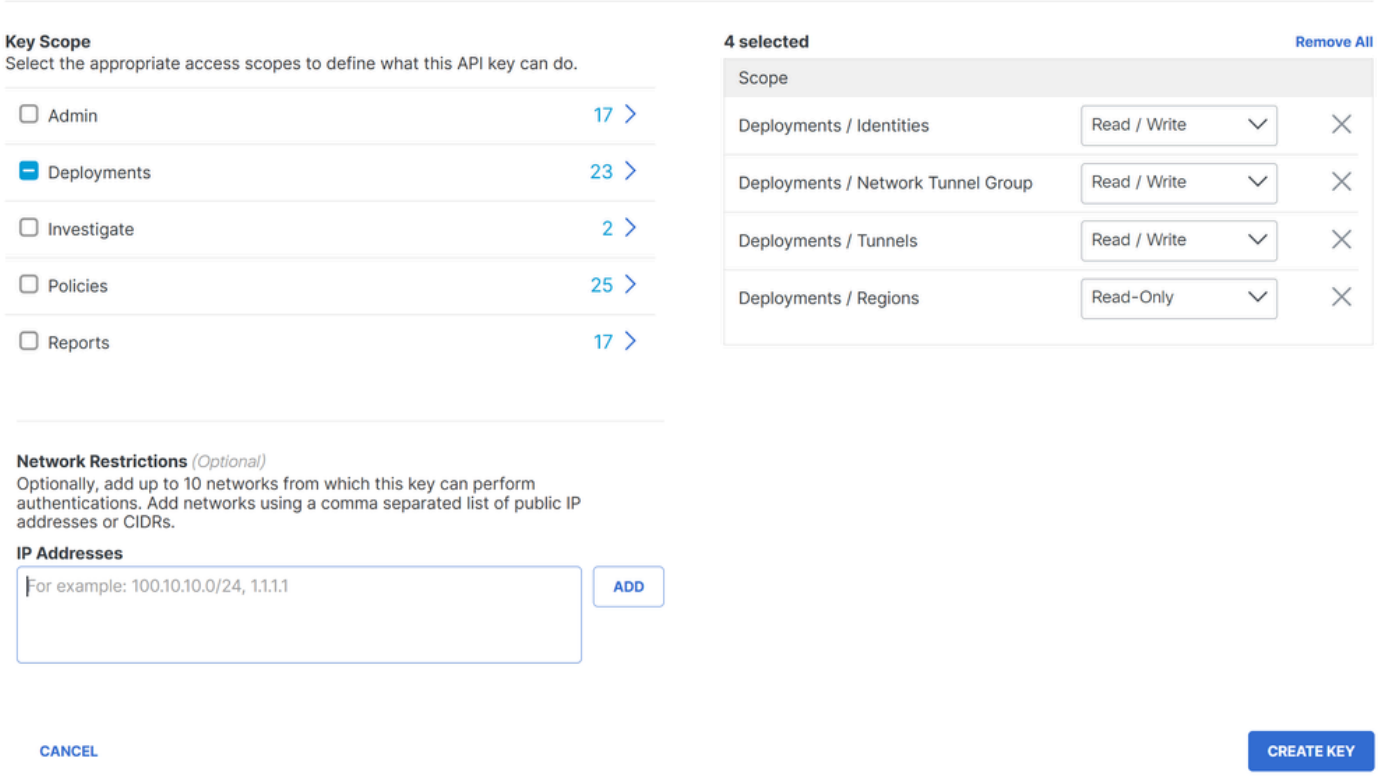
安全訪問配置

API建立

若要使用安全存取建立自動通道，請檢查以下步驟：

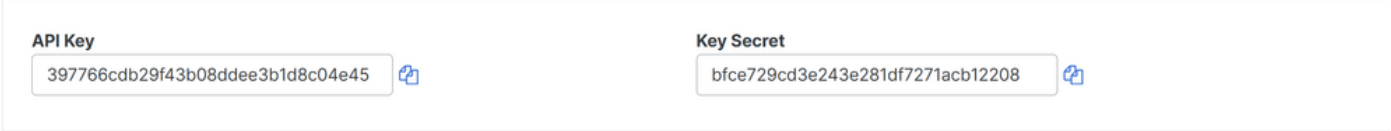
導航到Secure Access Dashboard。

- 按一下 Admin > API Keys
- 按一下 Add
- 選擇下一個選項：
  - Deployments / Network Tunnel Group:讀取/寫入
  - Deployments / Tunnels:讀取/寫入
  - Deployments / Regions:唯讀
  - Deployments / Identities:讀取/寫入
  - Expiry Date:永不過期



附註：或者，新增最多10個網路，這些網路可使用此金鑰執行身份驗證。使用逗號分隔的公共IP地址或CIDR清單新增網路。

- 單擊CREATE KEY，完成和的API Key創Key Secret。



注意：在按一下ACCEPT AND CLOSE之前先複製這些內容;否則，您需要再次建立這些檔案，並刪除未複製的檔案。

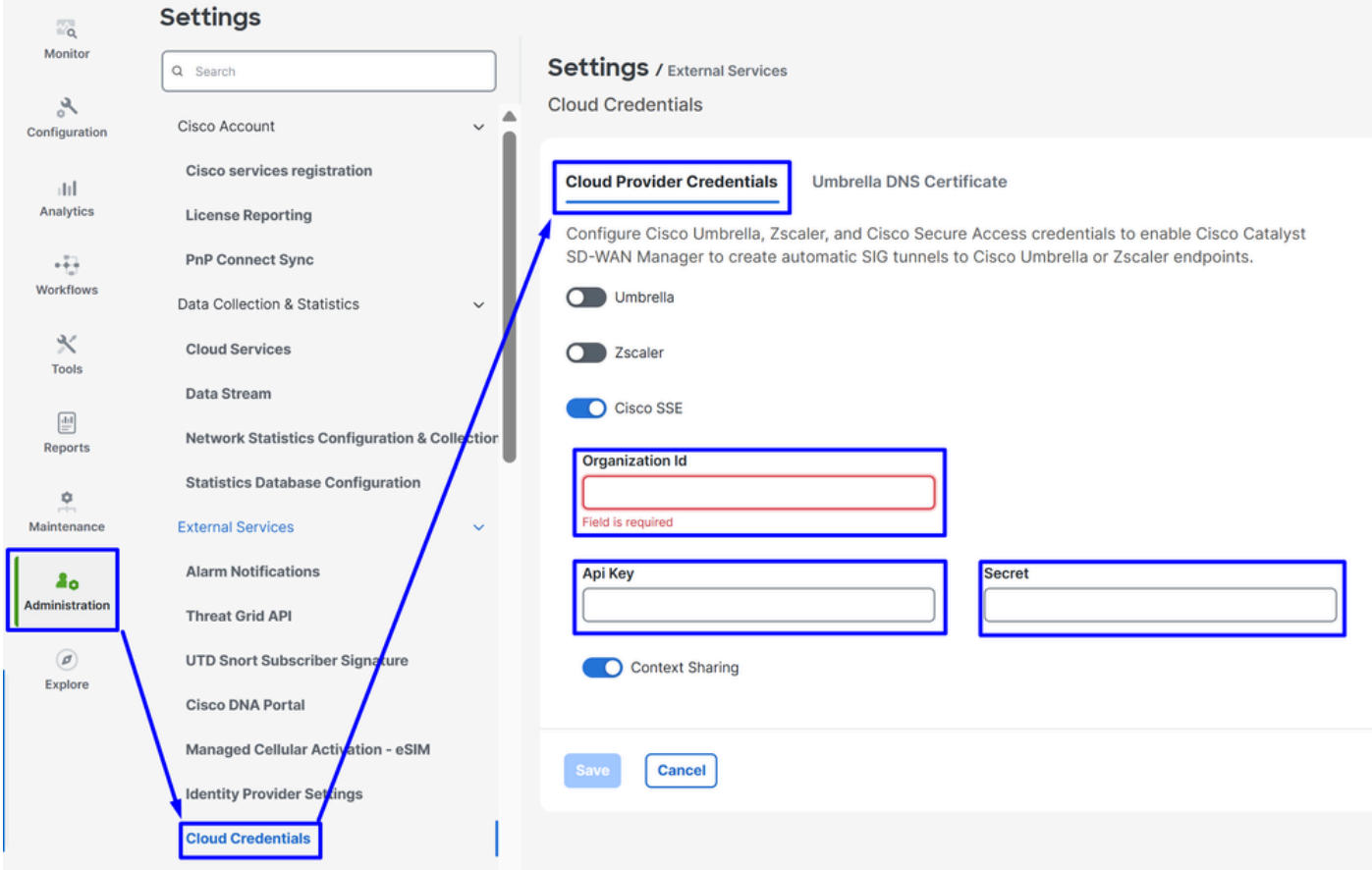
然後按一下ACCEPT AND CLOSE完成定稿。

SD-WAN配置

API整合

導航到Catalyst SD-WAN Manager:

- 按一下**Administration**>Settings > Cloud Credentials
- 然後點選Cloud Provider Credentials，啟用Cisco SSE並填充API和組織設定



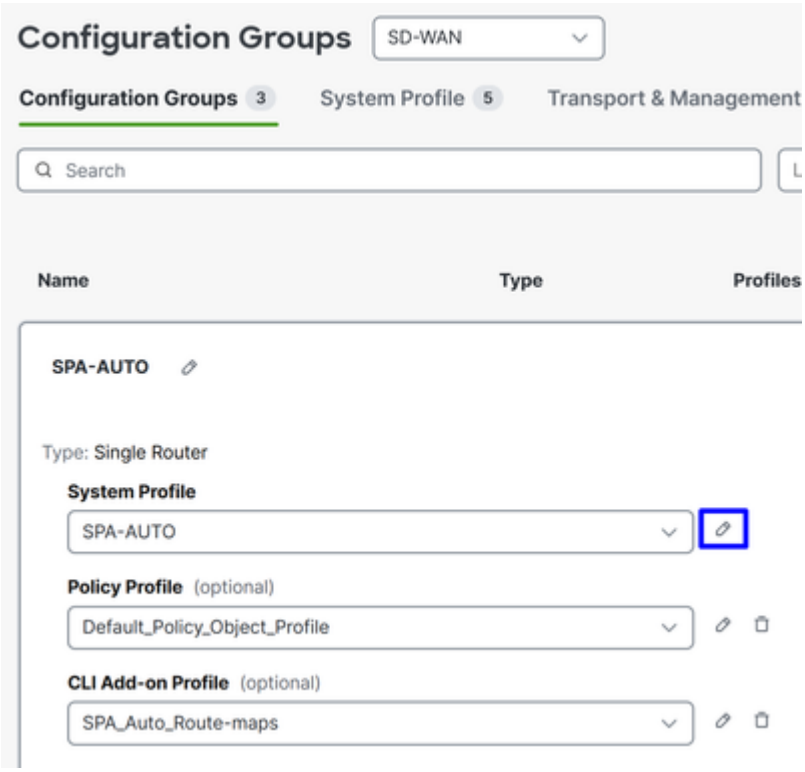
- Organization ID:您可以從SSE控制面板的URL獲取該資訊 https://dashboard.sse.cisco.com/org/xxxxx
- Api Key:從安全存取組態步驟中複製它
- Secret：從安全訪問配置步驟複製它

然後，按一下該Save按鈕。

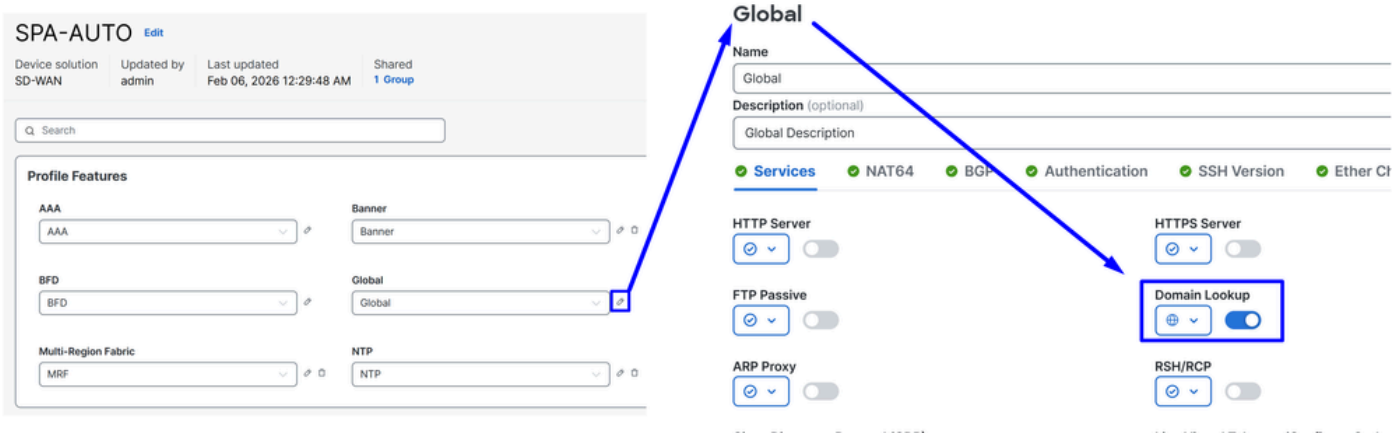
附註：繼續下一步之前，您需要確保SD-WAN管理器和Catalyst SD-WAN邊緣具有DNS解析和網際網路訪問。

要檢查DNS-Lookup是否已啟用，請導航至：

- 按一下Configuration > Configuration Groups
- 按一下邊緣裝置的配置檔案並編輯系統配置檔案



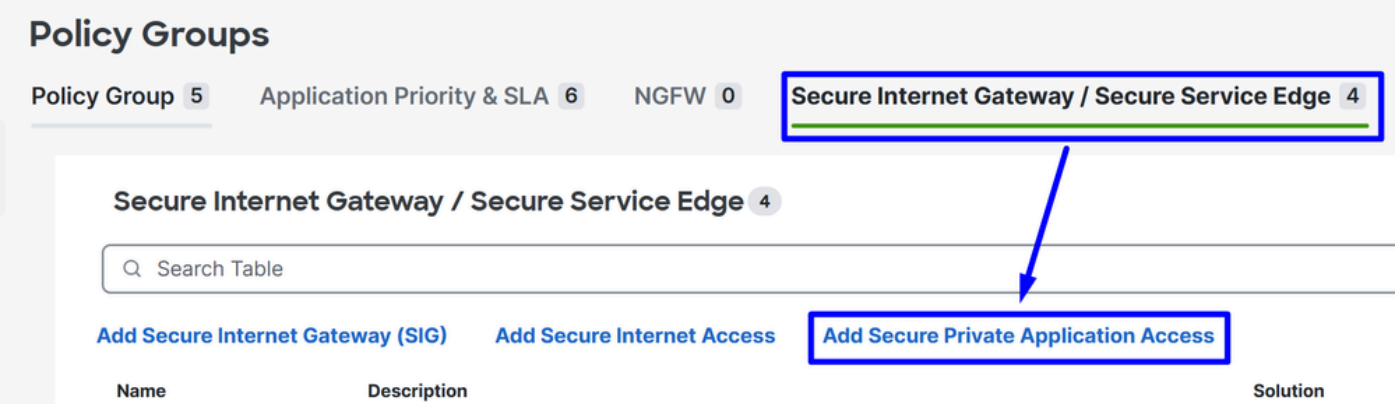
- 然後編輯Global選項，並確保啟用選項Domain Resolution



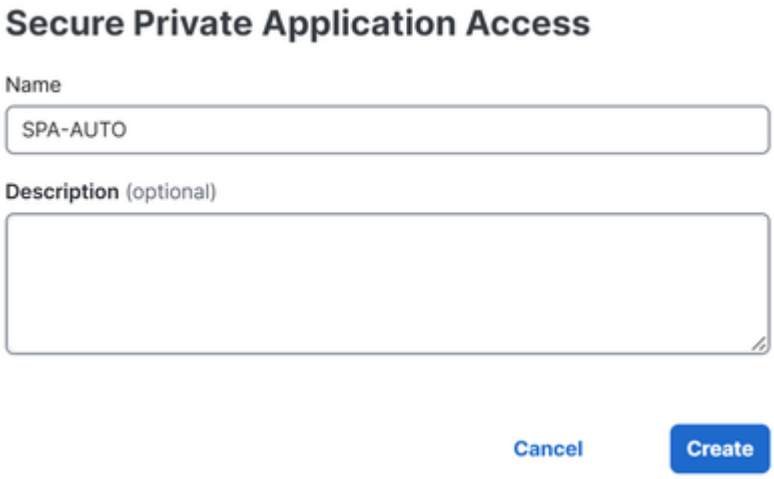
配置策略組

導覽至Configuration > Policy Groups:

- 按一下Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



- 配置名稱並點選 Create

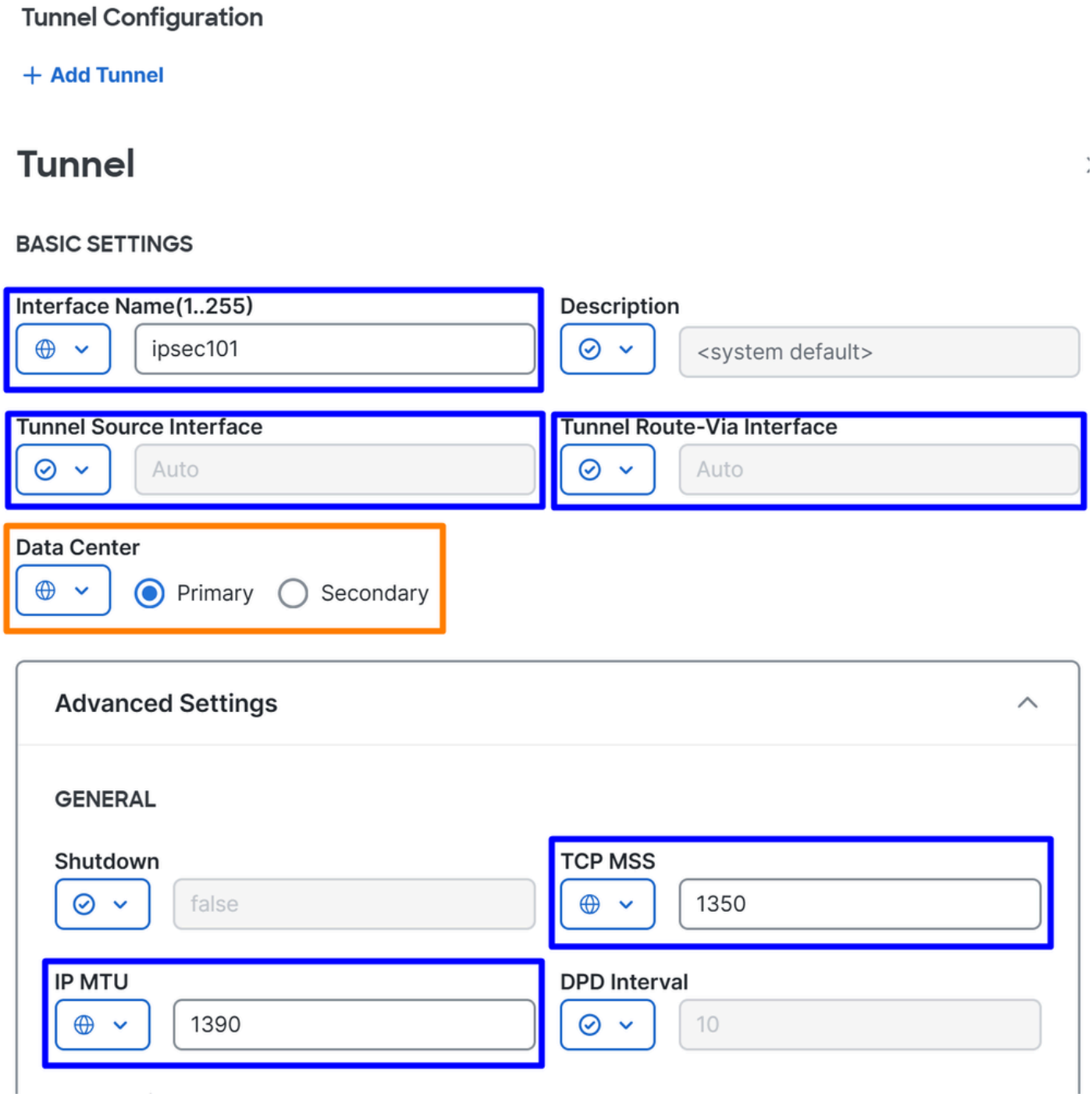


接下來的配置允許您在Catalyst SD-WAN邊緣中部署配置後建立隧道：

- Configuration
  - Segment (VPN):選擇要通過安全訪問承載應用程式的VRF
  - Cisco Secure Access Region:選擇距離應用程式託管的SD-WAN中心或分支機構最近的區域

接下來，定義通道配置。建立到主安全訪問資料中心的隧道處於活動狀態，而建立到輔助安全訪問資料中心的隧道則作為備份運行。

在Tunnel Configuration下，按一下+ Add Tunnel:



- Tunnel
  - Interface Name:指定隧道名稱，每次新增新隧道時，都會自動更新該名稱
  - Tunnel Source Interface:不需要更改此設定。如果保留為Auto，系統會自動建立帶有/31掩碼的環回介面。
  - Tunnel Route-Via Interface:無需更改此設定。預設情況下，它使用邊緣路由器上的第一個NATed物理WAN介面，但是如果需要特定的WAN介面，則可以更改該介面
  - Data Center:相應地選擇「主要」或「輔助」。如果已經配置了主隧道，則選擇Secondary。在正常情況下，可以將一個隧道配置為主隧道，將另一個隧道配置為輔助隧道
  - Advanced Settings
    - IP MTU:使用1390
    - TCP MSS:使用1350

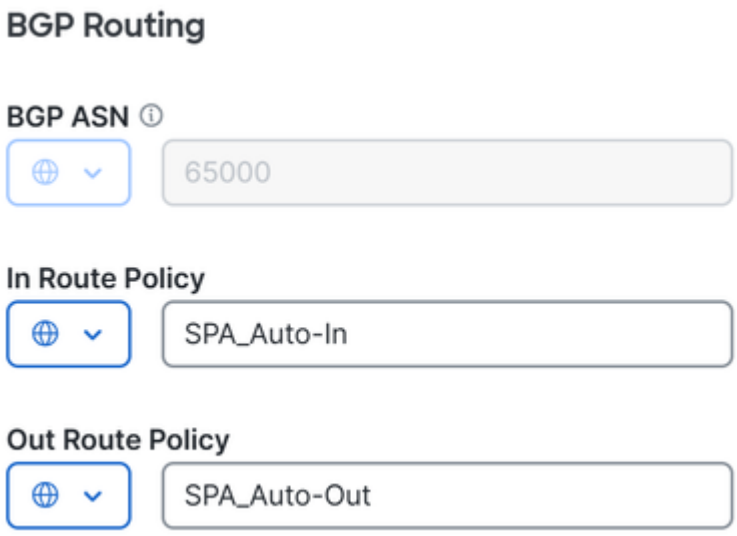
附註：如果要建立多個隧道以啟用ECMP並增加隧道容量，則可以為每台路由器配置最多10個活動/10個備份隧道。每個NTG提供最×10 Gbps和4 Gbps。

Interface Name	Description	Tunnel Source Interface	Tunnel Route-Via Interface	Data Center	Action
ipsec101		Auto	Auto	Primary	
ipsec102		Auto	Auto	Secondary	
ipsec103		Auto	Auto	Primary	
ipsec104		Auto	Auto	Secondary	
ipsec105		Auto	Auto	Primary	
ipsec106		Auto	Auto	Secondary	
ipsec107		Auto	Auto	Primary	
ipsec108		Auto	Auto	Secondary	
ipsec109		Auto	Auto	Primary	
ipsec110		Auto	Auto	Secondary	
ipsec111		Auto	Auto	Primary	
ipsec112		Auto	Auto	Secondary	
ipsec113		Auto	Auto	Primary	
ipsec114		Auto	Auto	Secondary	
ipsec115		Auto	Auto	Primary	
ipsec116		Auto	Auto	Secondary	
ipsec117		Auto	Auto	Primary	
ipsec118		Auto	Auto	Secondary	
ipsec119		Auto	Auto	Primary	
ipsec120		Auto	Auto	Secondary	

MAXIMUM OF 10 TUNNELS PER HUB
10 x 1 Primary
10 x 1 Secondary

注意：如果為每台路由器部署多個隧道，請確保傳輸介面能夠保持合併的所有活動隧道的聚合頻寬。例如，如果兩條隧道每條最高可傳輸1 Gbps，則傳輸鏈路必須支援至少2 Gbps的吞吐量。

配置隧道後，請繼續執行BGP配置。



- **BGP Routing**
  - BGP ASN:指定SD-WAN集線器的AS編號。AS服務64512保留用於安全訪問，不能使用。有關BGP的詳細資訊，請參見
  - In Route Policy:系統使用語句自動建立此入站路由策略deny all，以防止路由問題。必須通過CLI Add-On Template手動修改它，才能允許/拒絕合適的路由。
  - Out Route Policy:deny all 系統使用語句建立此出站路由策略以避免路由問題。必須通過手動編輯該策略才能允許CLI Add-On Template/拒絕相應的路由。

警告：從2025年11月開始，所有新建立的安全訪問組織預設使32644公共ASN組來在網路隧道組中的BGP對等。在2025年11月之前建立的現有組織繼續使用之前為64512全接入BGP對等體保留的私有ASN路由。如果將專用AS編號64512分配給網路上的裝置，則它無法與為對等（安全訪問）BGP AS 64512配置的網路隧道組對等。

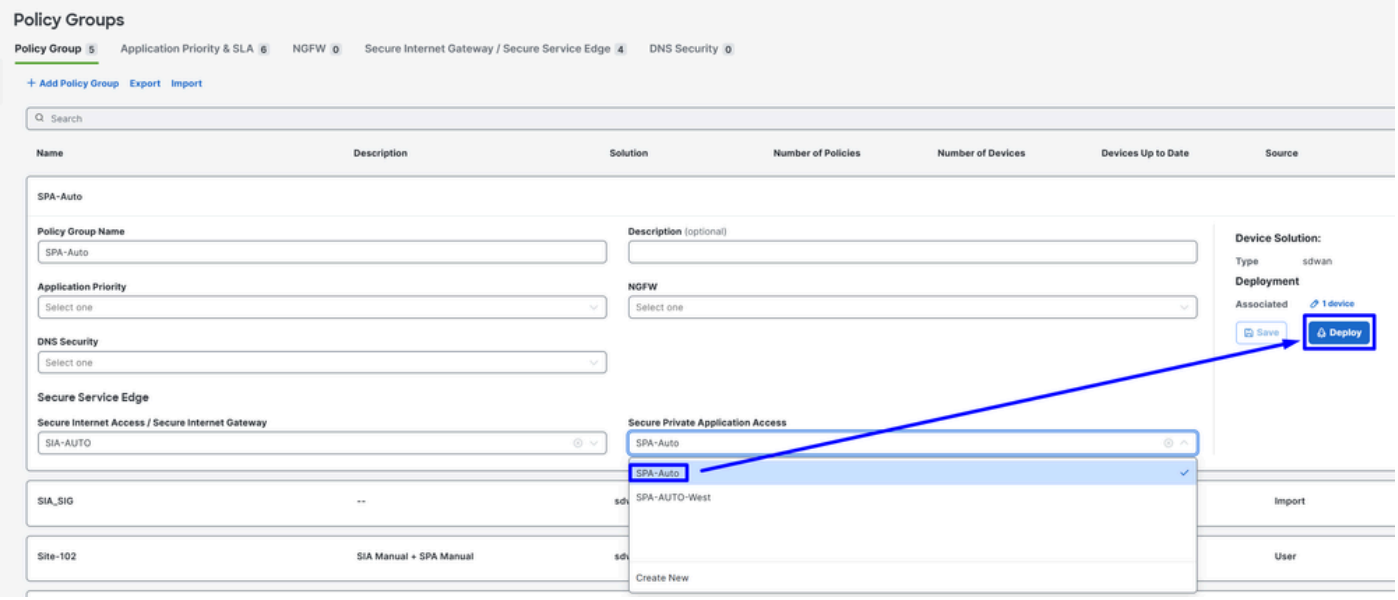
在中BGProute-map新策略後，系統會自動為每個BGP鄰居建立下一Deploy個and配置Policy Group。

```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

R104#sh run | s r b
router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 activate
 neighbor 169.254.0.3 send-community both
 neighbor 169.254.0.3 route-map SPA_Auto-In in
 neighbor 169.254.0.3 route-map SPA_Auto-Out out
 ...
 maximum-paths 32
exit-address-family
```

完成後，按一下Save，繼續執行策略部署以啟動隧道。

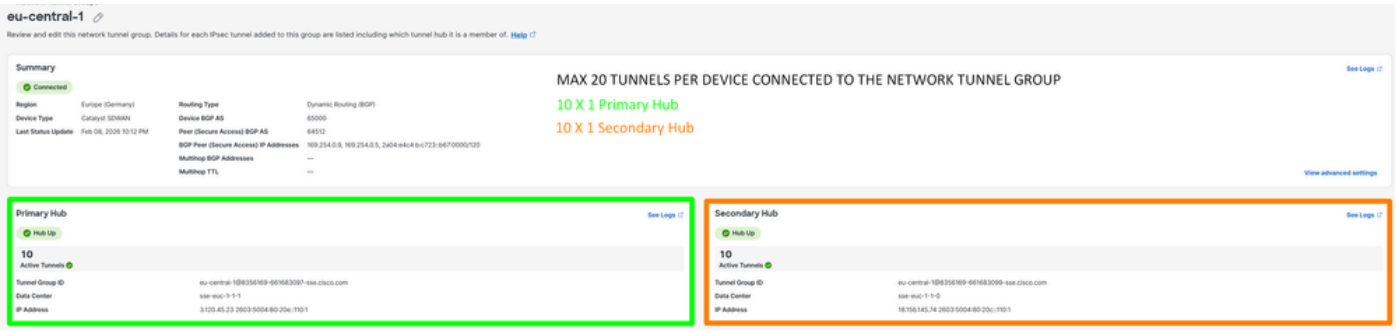
- 按一下Configuration> Policy Groups
- 在Policy > Secure Service EdgeSecure Private Application Access > 下選擇，然後點選最近為SPA建立的配置檔案。
- 按一下Deploy以完成



要在中驗證Secure Access，請執行以下步驟：

- 按一下Connect> Network Connections

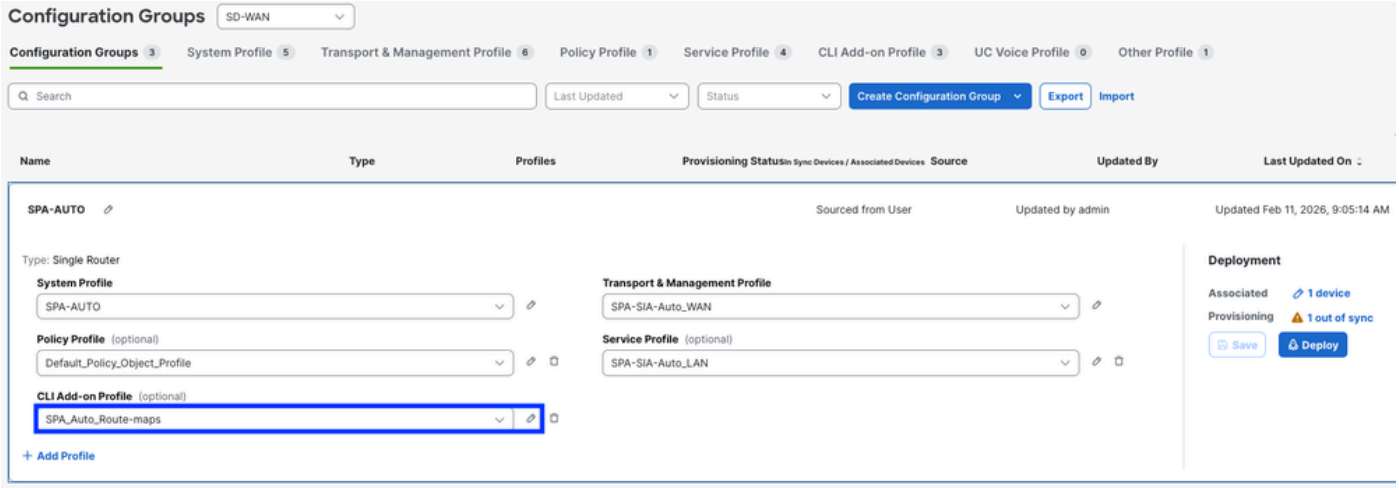
隧道建立



配置路由

導航至Configure> Configuration Groups

- 按一下您的Configuration Group，然後建立/編輯 CLI Add-on Profile



要允許BGP路由交換，請使用之前配置的In Route Policy**Out Route Policy**和。 您可以找到路由配置的一個基本CLI Add-On示例。此模板提供了一個起點，必須根據需要進行自定義：

```
ip bgp-community new-format
ip prefix-list default-route seq 5 permit 0.0.0.0/0 le 32

route-map SPA_Auto-In permit 10
match ip address prefix-list default-route
route-map SPA_Auto-In deny 65534
description Default Deny Configured from Secure Private Application Access feature

route-map SPA_Auto-Out permit 10
match ip address prefix-list default-route
description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
description Default Deny Configured from Secure Private Application Access feature

router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
network 172.16.104.0 mask 255.255.255.0
```

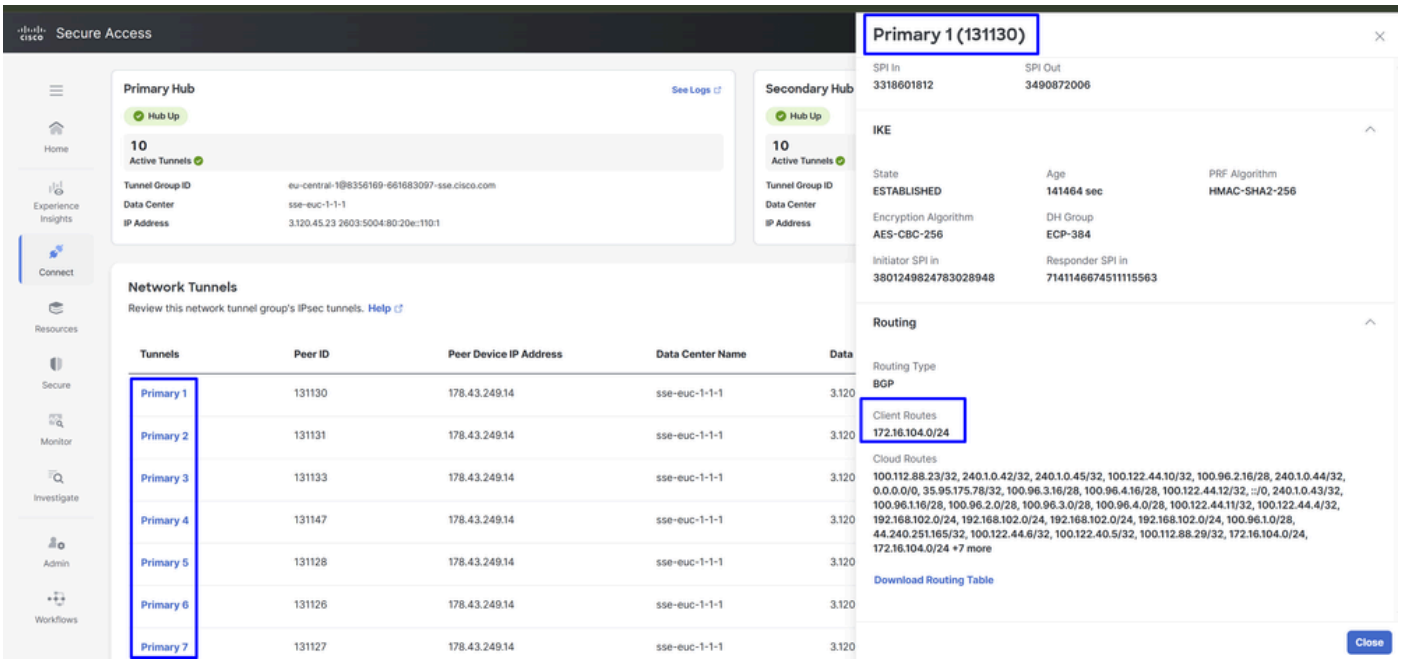
警告：在定義通過BGP路由對映允許傳入和傳出的網路時，需要仔細規劃。如以上示例所示，允許所有路由可能會引入意外的路由行為。為實現最佳部署，請在路由對映中僅明確指定必要的網路，以確保路由結果可控制且可預測

現在您可以繼續 Deploy the changes

要驗證是否在中收到了BGP路由Secure Access,請檢查後續步驟：

- 按一下Connect> Network Connections > Network Tunnel Groups並select輸入NTG名稱

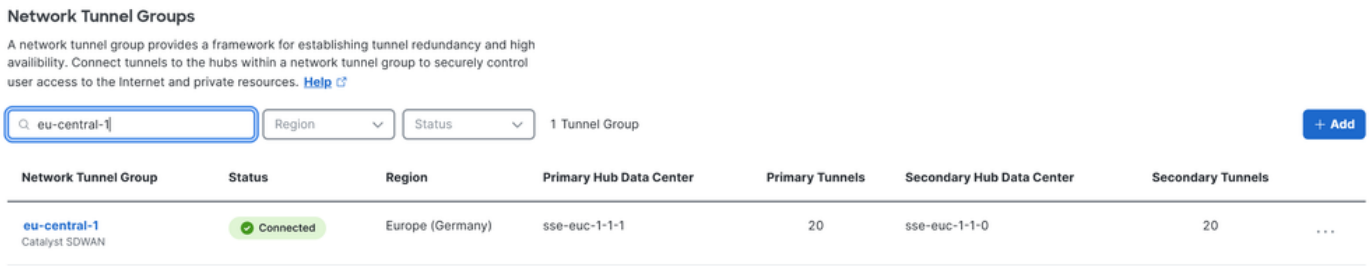
路由建立



附註：在本示例中，企業使用者子網172.16.104.0/24通過BGP通告到安全訪問。這樣可以在Catalyst SD-WAN和SSE環境之間正確路由。

同一策略可以應用於Catalyst SD-WAN集線器中的兩個WAN邊緣，從而產生20個活動隧道和20個備用隧道。通道的總數取決於每個邊緣上配置的通道數。連線到兩個安全接入集線器（集線器1和集線器2）的任何路由器都會在所有已建立的隧道中形成ECMP對。

例如，如果Catalyst SD-WAN邊緣1有10個隧道，而Catalyst SD-WAN邊緣2有10個隧道，則安全訪問將在20個活動隧道中形成ECMP。相同行為適用於輔助SSE中心。

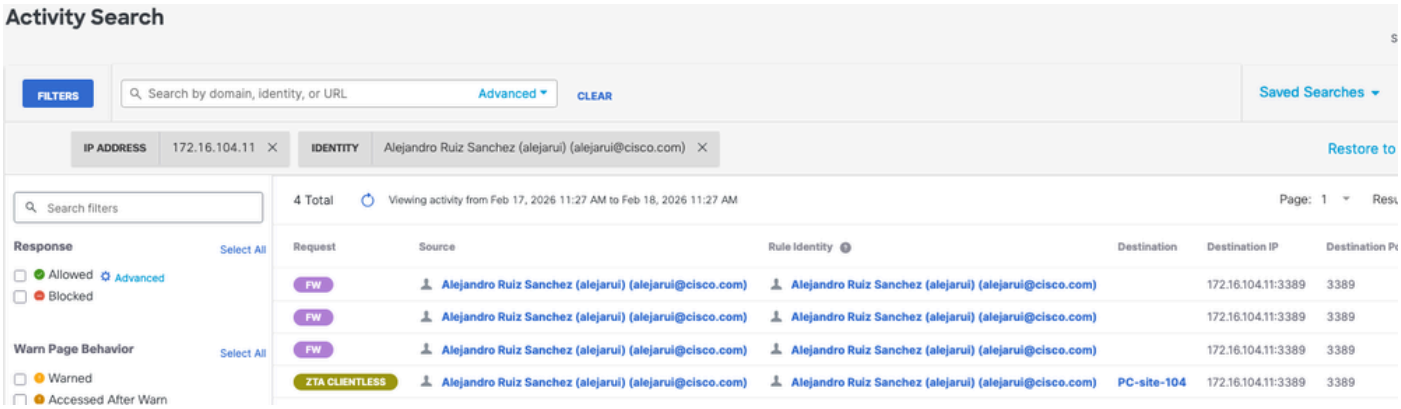


驗證

若要驗證流量是否正在通過Cisco Secure Access，請導覽至Events或Activity Search，然後Network-Wide Path Insights按通道身分進行過濾：

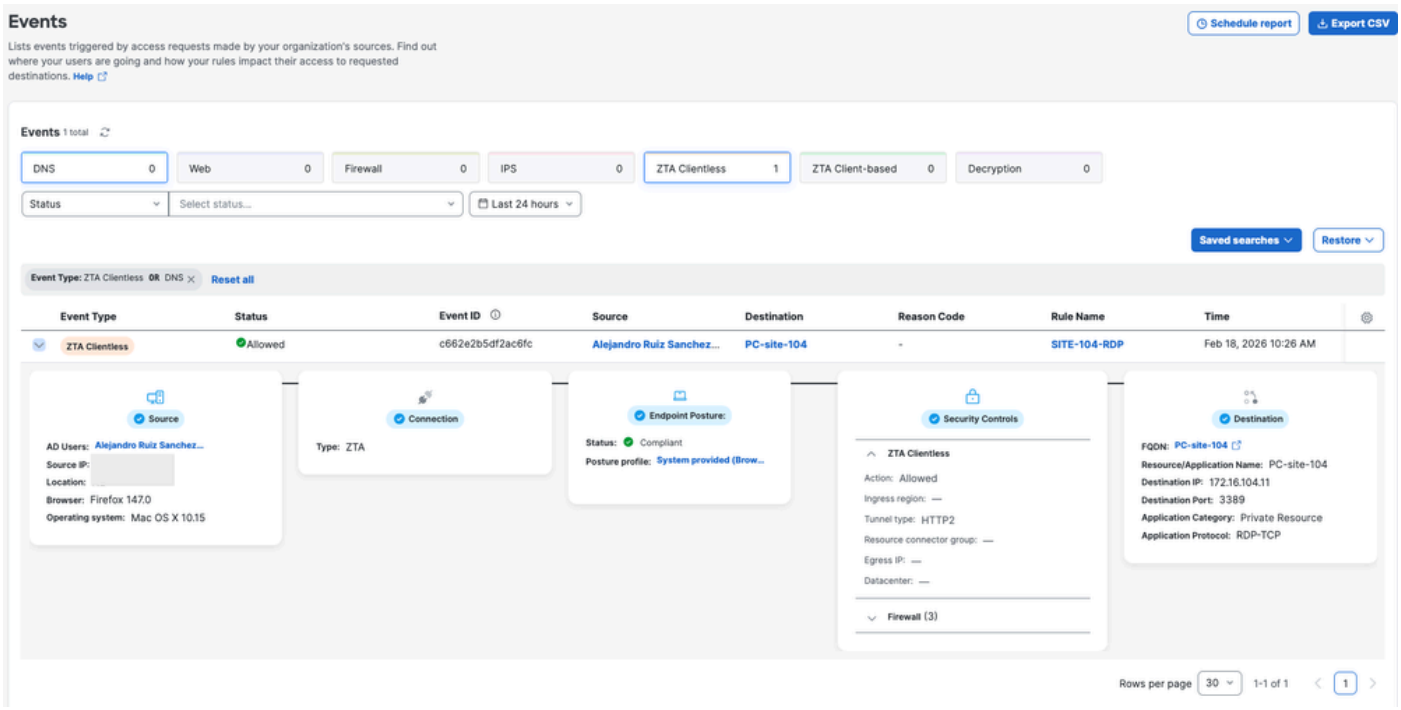
安全訪問 — 活動搜尋

導覽至Monitor>Activity Search:



安全訪問 — 事件

導覽至Monitor>Events:

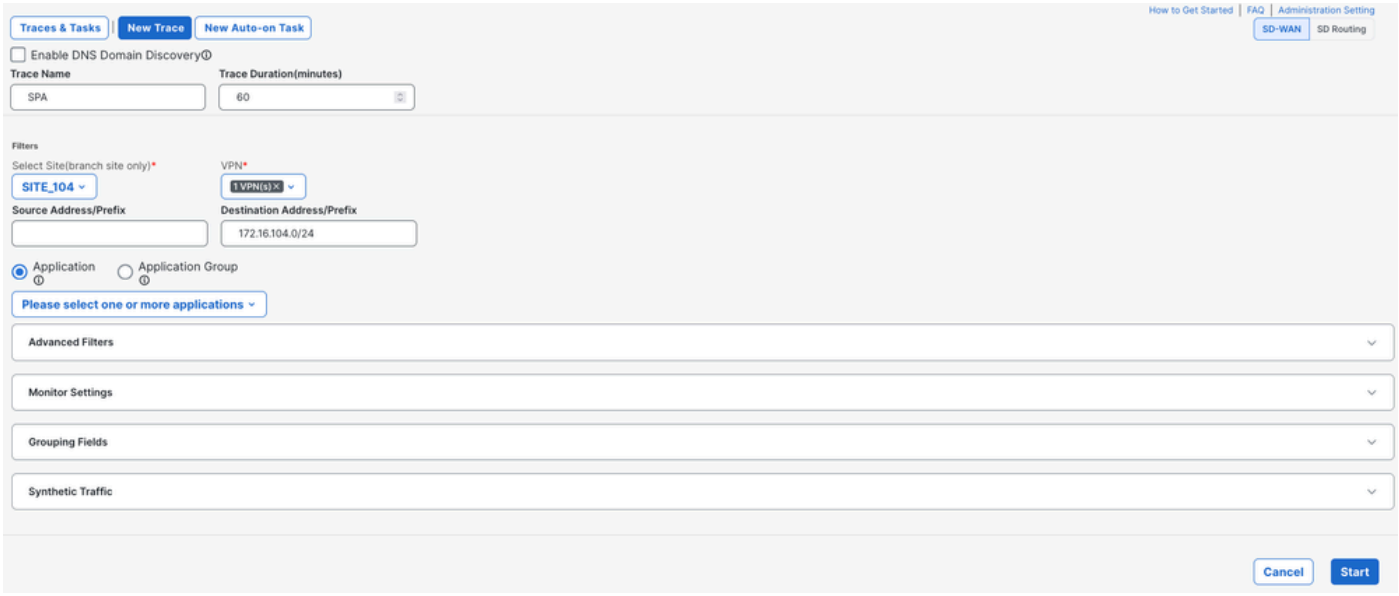


附註：請確保您的預設策略已啟用日誌記錄，預設情況下已禁用。

Catalyst SD-WAN管理員 — 網路範圍路徑洞察

導航到Catalyst SD-WAN Manager:

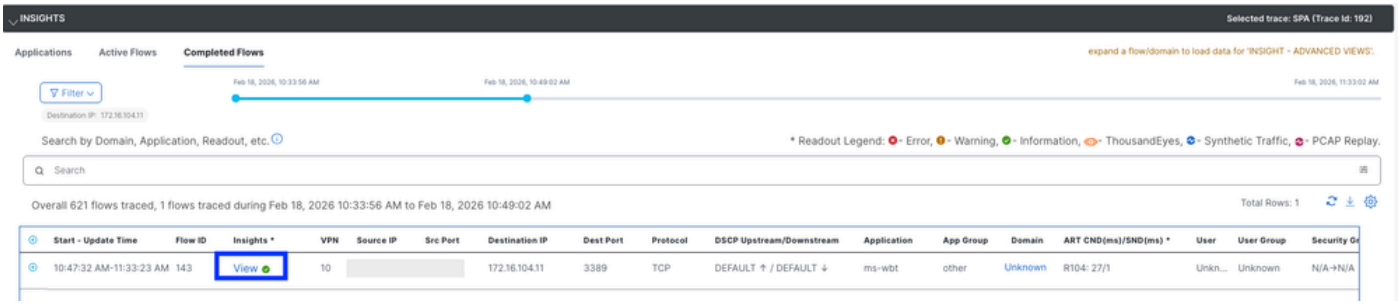
- 按一下Tools> Network-Wide Path Insights
- 按一下 New Trace



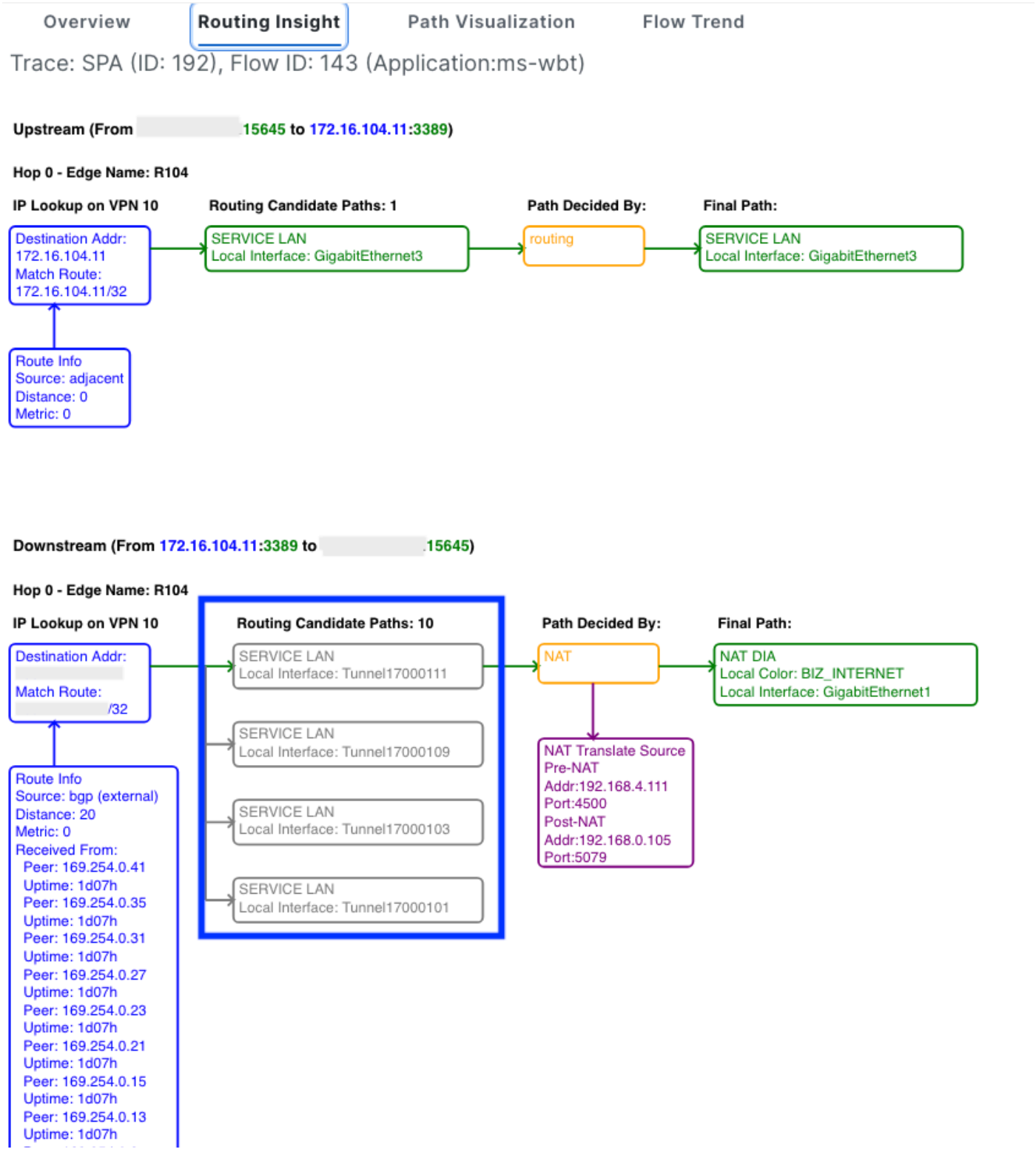
- Trace Name:（可選）指定跟蹤名稱
- Site:選擇專用資源所在的站點
- VPN:選擇專用資源所在的VPN ID
- Source/Destination Address:（可選）輸入IP或將其保留為空白，以捕獲根據和選擇過濾的所有Site流VPN量

啟動跟蹤

找到流量並按一下Insights列上的View



routing Insights列顯示候選路徑並顯示用於安全訪問的IPSec隧道



相關資訊

- 思科技術支援與下載
- Cisco Secure Access幫助中心
- Cisco SASE設計手冊
- 使用SD-WAN自動隧道配置安全訪問，以實現安全的網際網路訪問
- Cisco Catalyst SD-WAN安全配置指南，Cisco IOS XE Catalyst SD-WAN版本17.x

- Cisco SASE解決方案：Cisco Catalyst SD-WAN與思科安全訪問整合概覽

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。