使用手動方法在安全服務邊緣和SD-WAN之間配置專用應用互連

目錄

簡介

本文檔介紹將思科安全訪問與SD-WAN路由器連線起來的綜合指南，重點介紹安全專用應用訪問。

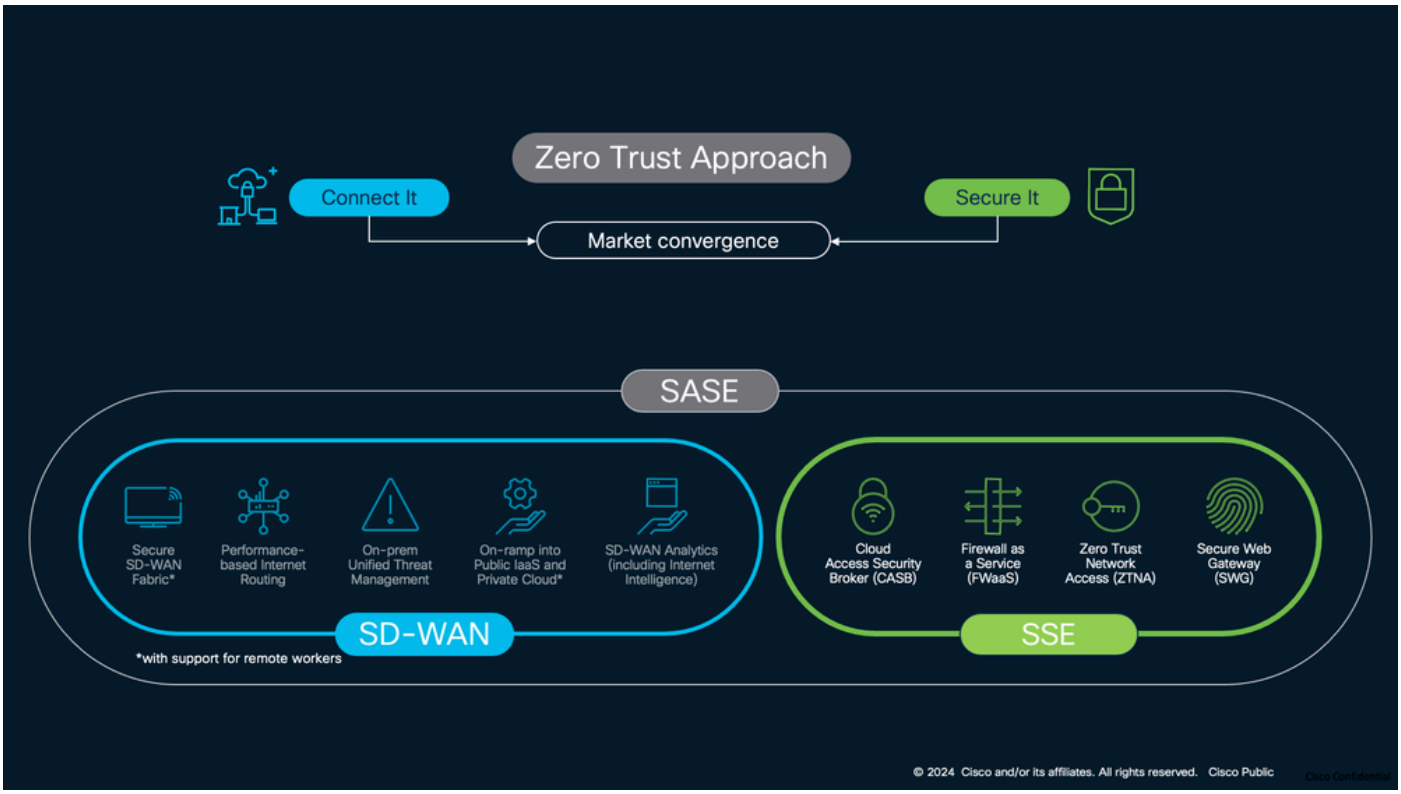
關於本指南

註：此處列出的配置是為SD-WAN的UX1.0和17.9/20.9版本開發的。

本指南提供了以下關鍵步驟的結構化演練：

- 定義網路通道組(NTG)
- IPSec通道配置：有關在Cisco SD-WAN路由器和Cisco安全訪問NTG之間設定安全IPSec隧道的詳細說明。
- BGP鄰居關係：通過IPSec隧道運行BGP鄰居的分步程式，可確保動態路由和增強的網路恢復能力。
- 專用應用程式訪問：有關配置通過已建立的隧道對專用應用的訪問並確保其安全的指導。

圖 1:Cisco SD-WAN和SSE零信任方法



採用SD-WAN的SSE

本指南重點介紹NTG互連的設計考慮事項和部署最佳實踐。在本指南中，SD-WAN控制器部署在雲中，而WAN邊緣路由器部署在資料中心並連線到至少一個網際網路電路。

主要假設

- 思科安全存取安全服務邊緣(SSE):假設已為您的組織調配了Cisco Secure Access SSE。
- Cisco SD-WAN WAN邊緣路由器：假設WAN邊緣路由器整合到重疊網路中，從而有效地幫助使用者通過SD-WAN基礎設施進行通訊。
- 雖然本指南主要側重於設計和配置中的SD-WAN方面，但它提供了一種將思科安全接入解決方案整合到現有網路架構中的整體方法。

關於此解決方案

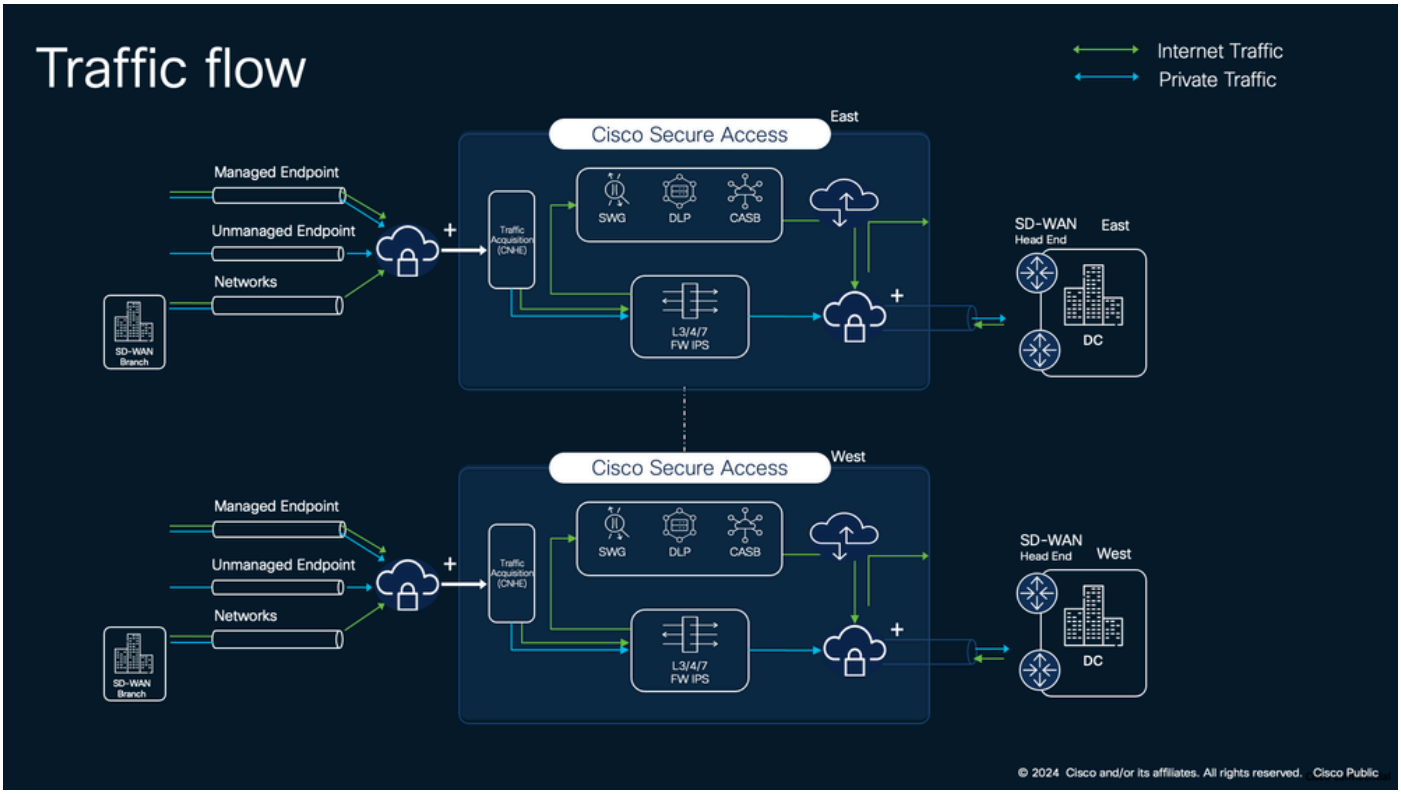
由Cisco Secure Access提供的專用應用隧道為通過零信任網路訪問(ZTNA)和VPN即服務(VPNaaS)進行連線的使用者提供到專用應用的安全連線。 通過這些隧道，組織可以將遠端使用者安全地連結至託管於資料中心或私有雲中的私有資源。
使用IKEv2（Internet金鑰交換版本2），這些隧道組在Cisco Secure Access和SD-WAN路由器之間建立安全的雙向連線。它們通過同一組內的多個隧道支援高可用性，並通過靜態和動態路由(BGP)提供靈活的流量管理。
IPsec隧道可以傳輸來自各種來源的流量，包括：

- 遠端訪問VPN使用者
- 基於瀏覽器或基於客戶端的ZTNA連線
- 連線到思科安全訪問的其他網路位置

此方法允許組織通過統一加密的管道安全路由所有型別的專用應用流量，從而增強安全性和運營效

率。
作為思科安全服務邊緣(SSE)解決方案的一部分，思科安全訪問通過單個雲託管控制檯、統一客戶端、集中策略建立和彙總報告簡化IT運營。它在一個雲交付的解決方案中整合了多個安全模組，包括ZTNA、安全Web網關(SWG)、雲訪問安全代理(CASB)、防火牆即服務(FWaaS)、DNS安全、遠端瀏覽器隔離(RBI)等等。這一全面的方法通過應用零信任原則和實施精細的安全策略來降低安全風險

圖 2:思科安全訪問和專用應用之間的流量



SSE專用應用流量

本指南中介紹的解決方案解決了全面的冗餘注意事項，包括資料中心中的SD-WAN路由器以及安全服務邊緣(SSE)端的網路隧道組(NTG)。本指南重點介紹主動/主動SD-WAN中心部署模式，這有助於保持不間斷的流量流並確保高可用性。

必要條件

需求

建議您瞭解以下主題：

- Cisco SD-WAN配置和管理
- IKEv2和IPSec協定基礎知識
- 在思科安全存取入口中設定網路通道群組
- BGP和ECMP知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 20.9.5a上的Cisco SD-WAN控制器
- 17.9.5a上的Cisco SD-WAN廣域網邊緣路由器
- 思科安全存取入口網站

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。

設計

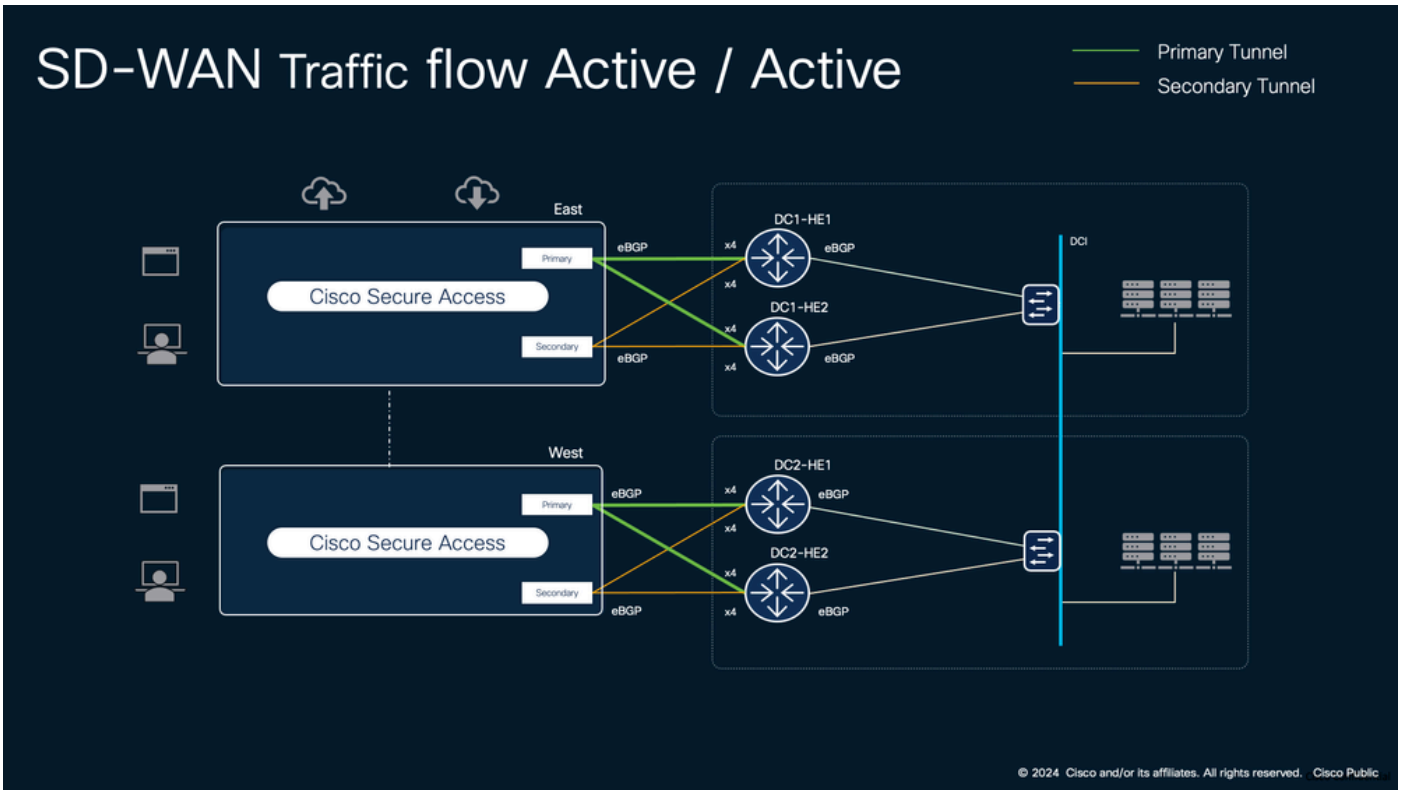
本指南介紹使用SD-WAN頭端路由器的主動/主動設計模型的解決方案。SD-WAN頭端路由器情景中的主用/主用設計模型假設資料中心中有兩台路由器，它們都連線到安全服務邊緣(SSE)網路隧道組(NTG)，如圖3所示。在此場景中，資料中心中的兩台SD-WAN路由器（DC1-HE1和DC1-HE2）都主動處理流量流。它們通過向內部DC鄰居傳送相同的AS路徑長度(ASPL)來實現這一點。因此，來自DC內部的流量在兩個頭端之間均衡。

每個頭端路由器都可以建立多個到SSE存在點(POP)的隧道。 通道數量根據您的要求和SD-WAN裝置型號而有所不同。在此設計中：

- 每台路由器有4個通往主要SSE集線器的通道和4個通往輔助SSE集線器的通道。
- 每個SSE中心支援的最大隧道數可能不同。有關最新資訊，請參閱官方文檔：https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

這些頭端路由器在通往SSE的通道上形成BGP鄰居。通過這些鄰居關係，頭端向其SSE鄰居通告私有應用程式字首，從而支援安全且有效的流量到私有資源的路由。

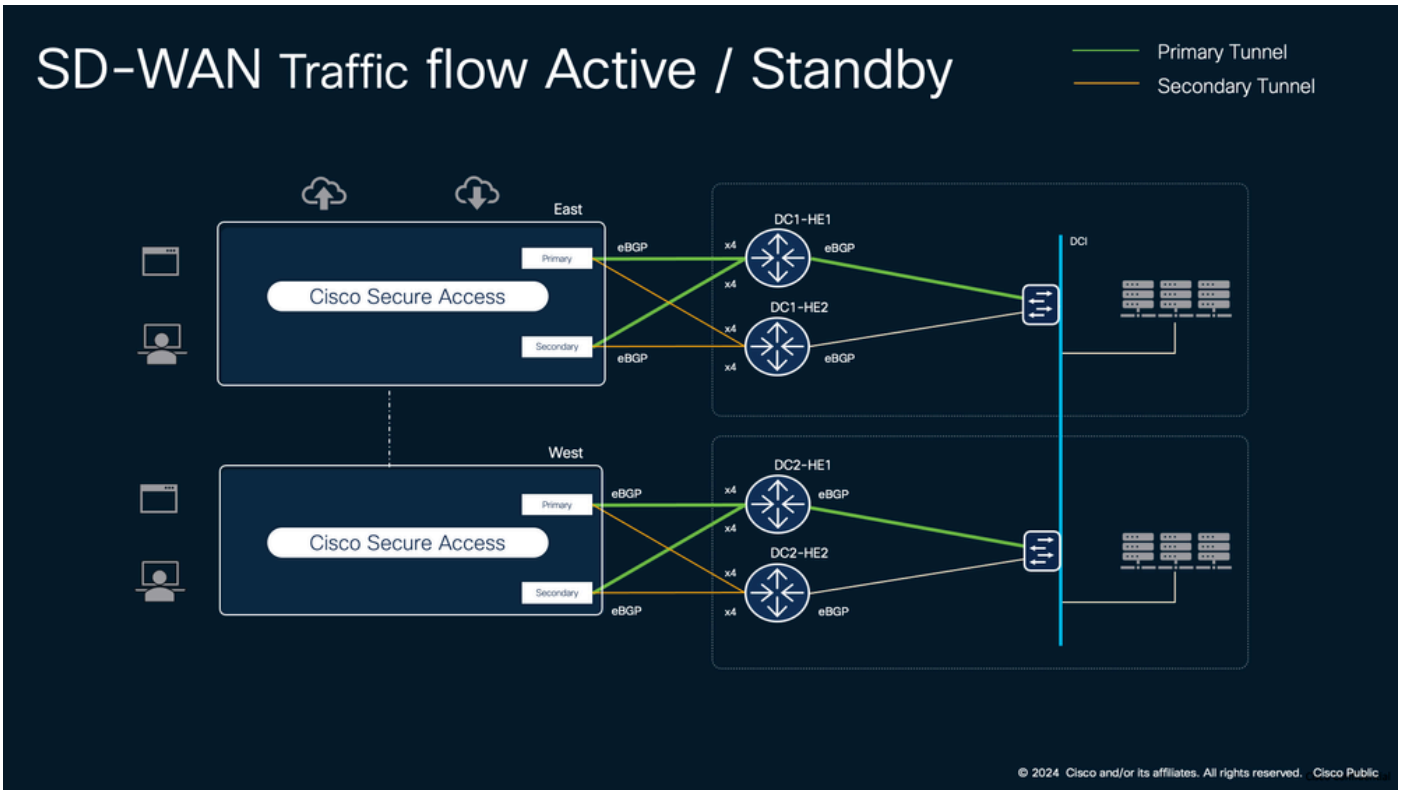
圖 3:SD-WAN到SSE主動/主動部署模式



SD-WAN到SSE主動/主動部署模式

主用/備用設計將一台路由器(DC1-HE1)指定為始終主用，而輔助路由器(DC1-HE2)保持備用狀態。流量始終流經活動前端(DC1-HE1)，除非完全失敗。此部署模式有一個缺點：如果通向SSE的主隧道關閉，流量將切換到僅通過DC1-HE2的輔助SSE隧道，從而導致任何有狀態流量重置。
在主用/備用模式中，BGP AS-Path Length用於引導資料流內和指向SSE的流量。DC1-HE1向ASPL為2的SSE BGP鄰居傳送字首更新，而DC1-HE2向ASPL為3的鄰居傳送更新。DC1-HE1的內部DC鄰居通告AS路徑長度短於DC1-HE2的字首，從而確保DC1-HE1的流量偏好。（客戶可以選擇其他屬性或協定來影響流量偏好。）
客戶可以根據其特定需求選擇主用/主用或主用/備用部署模式。

圖 4:SD-WAN到SSE主用/備用部署模式



SD-WAN到SSE主用/備用部署模式

設定

本節介紹以下過程：

1. 驗證在Cisco Secure Access門戶中調配網路隧道組的先決條件。
2. 使用IPsec手動方法配置思科安全訪問網路隧道組(NTG)的SD-WAN互連。
3. 配置BGP鄰居關係

附註：此配置基於主用/主用部署模式

程式1.驗證思科安全訪問門戶上的網路隧道組配置

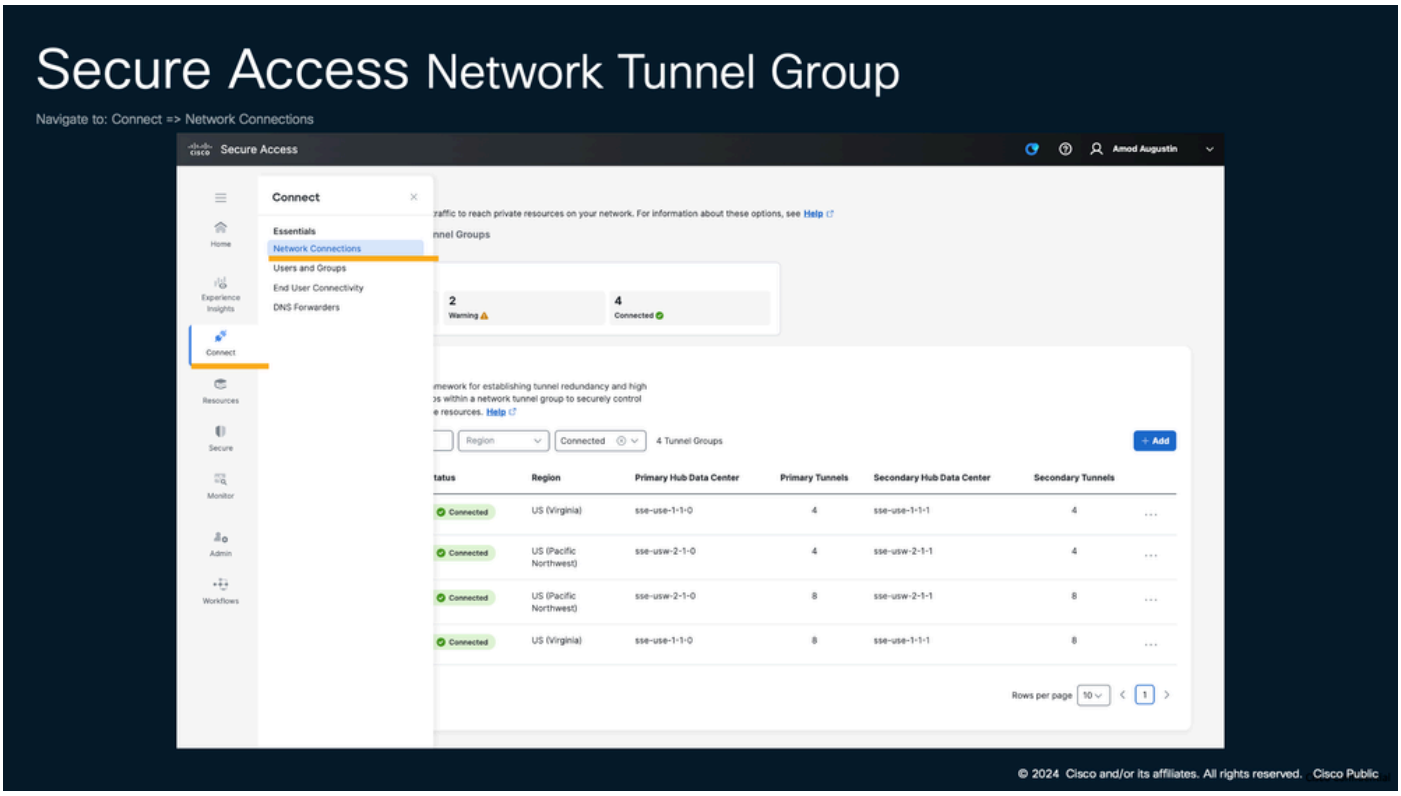
本指南未介紹如何配置網路隧道組。請檢視此參考資料。

- 新增網路隧道組：SSE文檔
- 使用帶BGP的ECMP配置Cisco安全訪問和Cisco IOS XE路由器之間的網路隧道

導覽至Cisco Secure Access，並確保已布建網路通道組(NTG)。對於當前設計，我們需要在兩個不同的入網點(POP)中設定NTG。 在本指南中，我們在美國（維吉尼亞）POP和美國（太平洋西北）POP中使用NTG。

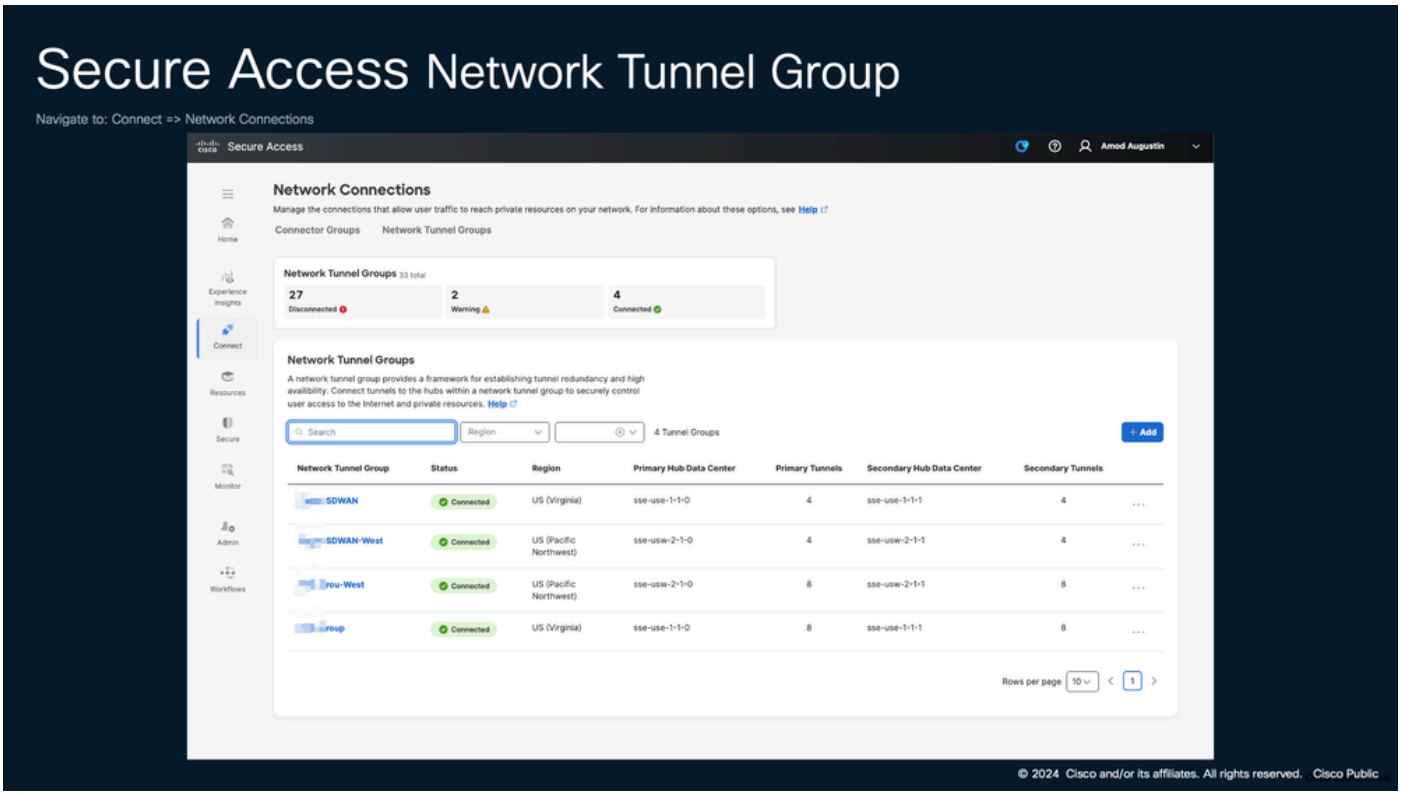
注意:POP的名稱和位置可能有所不同，但關鍵概念是在地理位置接近您資料中心的位置調配多個NTG。此方法有助於最佳化網路效能並提供冗餘。

圖 5:思科安全存取網路通道群組



思科安全存取網路通道群組

圖 6:思科安全存取網路通道群組清單



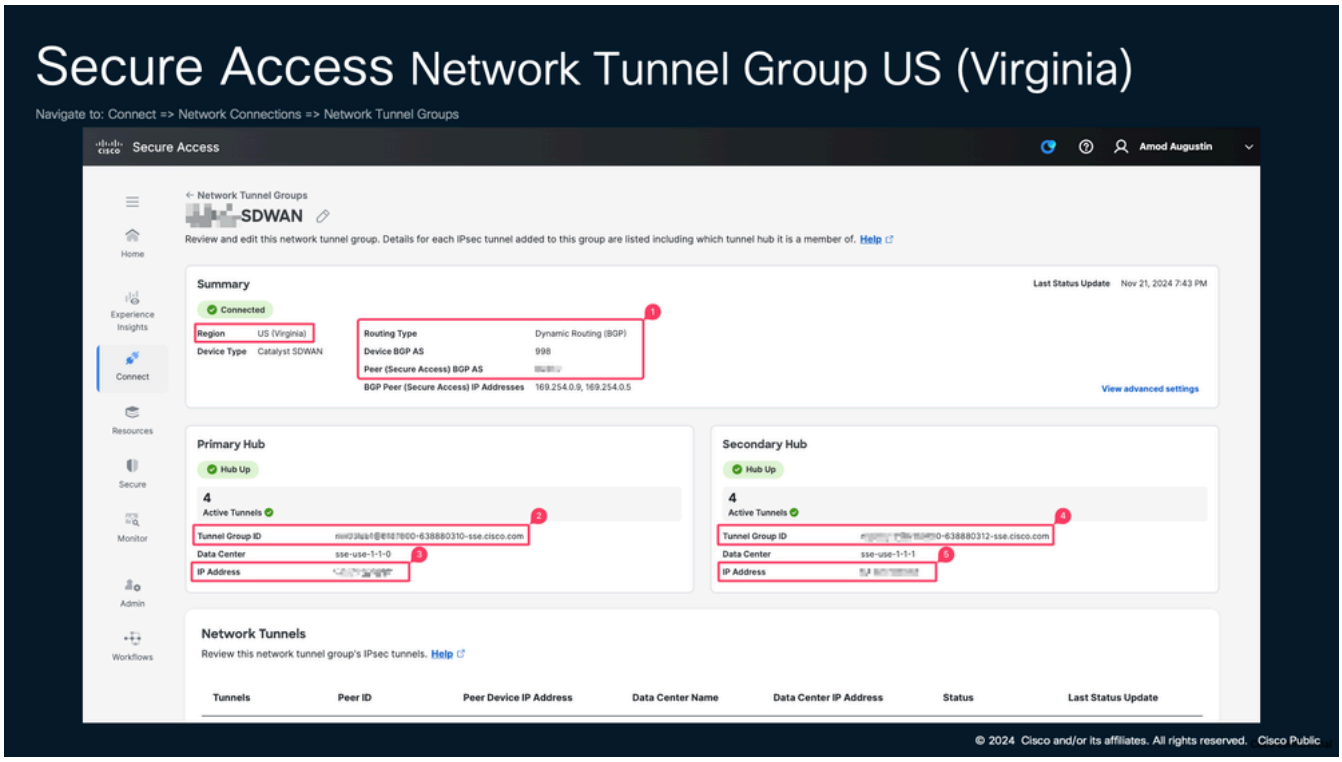
安全訪問網路隧道組清單

請確定您已注意到通道密碼短語（在通道建立期間只顯示一次）。

附註：新增網路隧道組中的步驟6

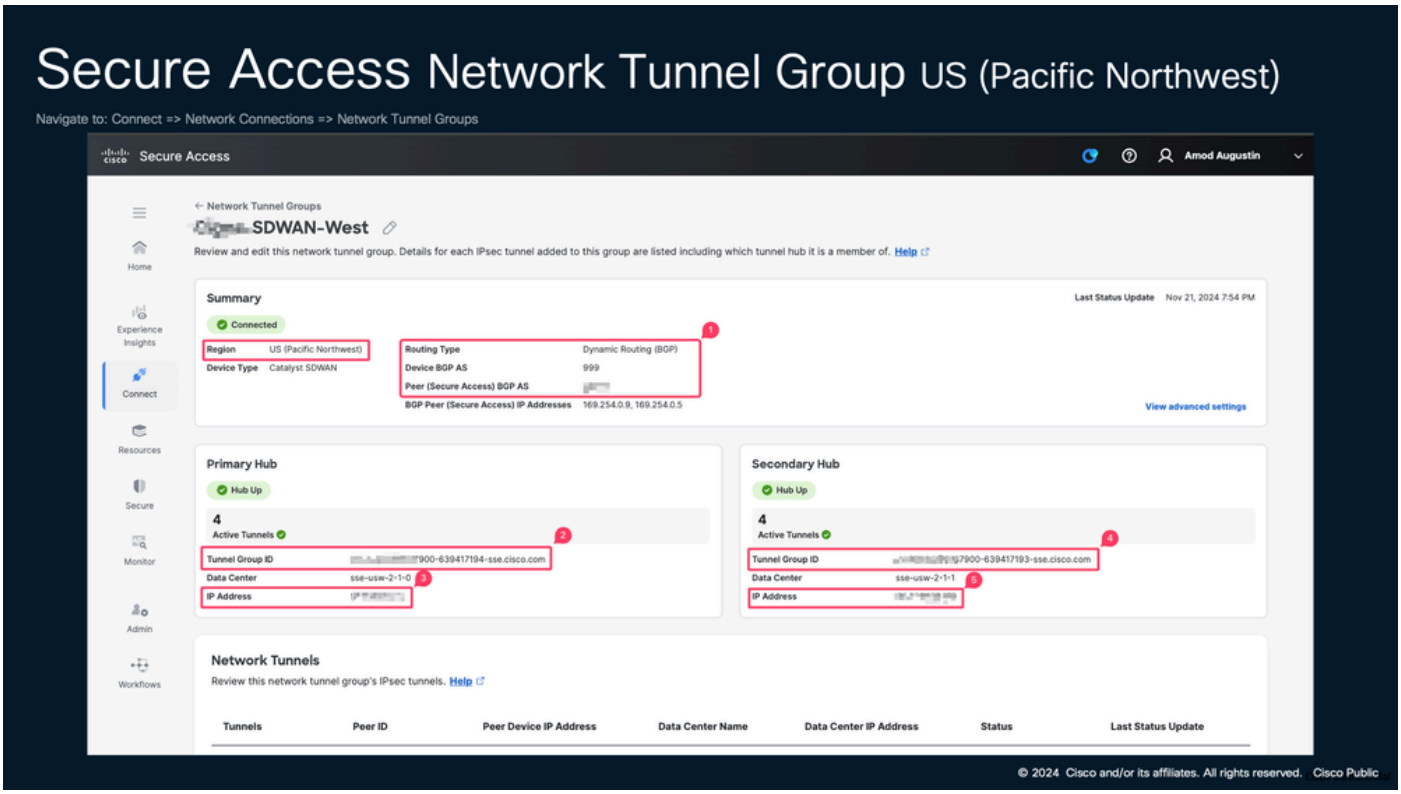
另外請記下我們在IPSec配置期間使用的隧道組屬性。螢幕快照（圖6）取自實驗室環境，用於根據設計或使用建議建立NTG組的生產場景。

圖7：安全訪問網路隧道組（美國，維吉尼亞）



安全存取網路通道組US（維吉尼亞）

圖8：安全接入網路隧道組US（太平洋西北部）

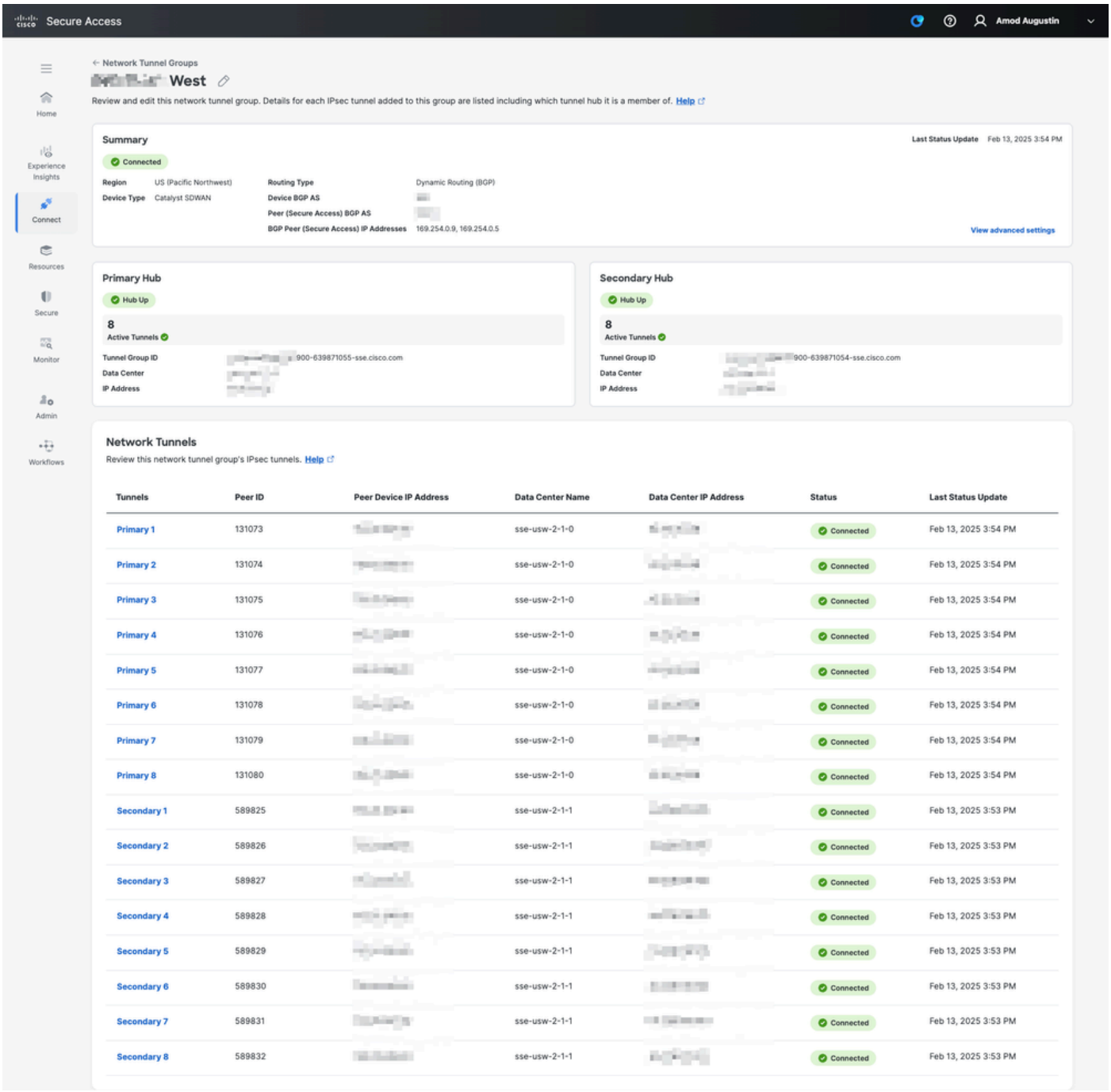


安全存取網路通道組US（太平洋西北）

圖8顯示主要和輔助集線器上只有4個隧道。但是，在控制器環境中成功測試了最多8個通道。最大隧道支援可能因所使用的硬體裝置和當前的SSE隧道支援而異。有關最新資訊，請參閱官方文檔：https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels和相應硬體裝置的發行說明。

此處提供了8通道設定的示例。

圖8a:最多8個通道的NTG通道



SSE NTG最多8個通道

程式2.使用IPsec手動方法配置思科安全訪問網路隧道組(NTG)的SD-WAN互連。

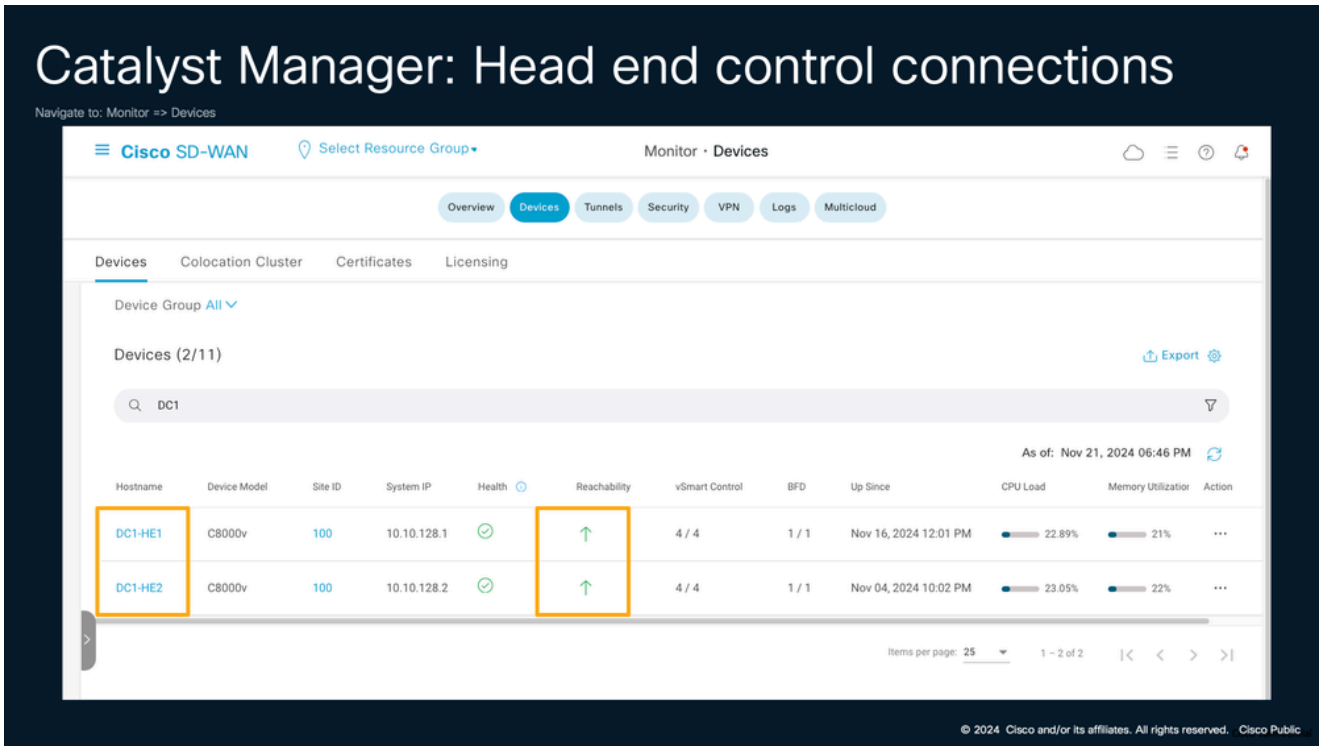
此程式示範如何在執行17.9版的Cisco Catalyst SD-WAN管理器20.9和Cisco Catalyst邊緣路由器上使用功能模板連線網路隧道組(NTG)。

注意：本指南假設現有SD-WAN重疊部署採用中心輻射型或全網狀拓撲，其中集線器作為託管於資料中心的專用應用的接入入口點。此過程還可以應用於分支或雲部署。

繼續之前，請確保滿足以下前提條件：

1. 裝置上已啟用控制連線，以允許從Cisco Catalyst SD-WAN Manager進行必要的更新。

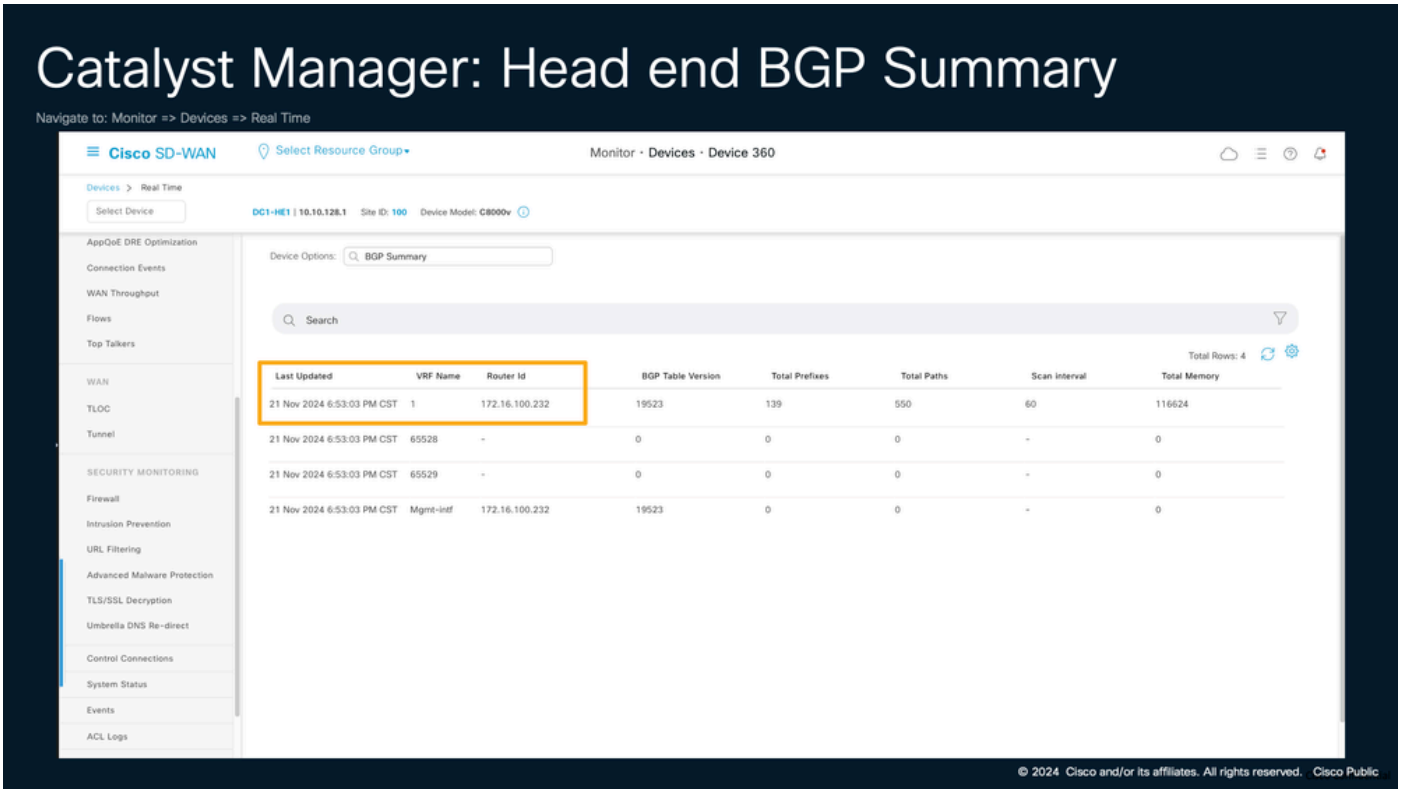
圖 9:Cisco Catalyst SD-WAN管理器：頭端控制連線



Catalyst管理器：頭端控制連線

2. 服務端VPN已配置並使用路由協定通告字首。本指南使用BGP作為服務端的路由協定。

圖 10:Cisco Catalyst SD-WAN管理器：頭端BGP摘要



要使用手動IPSec方法配置帶有網路隧道組(NTG)的SD-WAN互聯，請完成以下步驟：

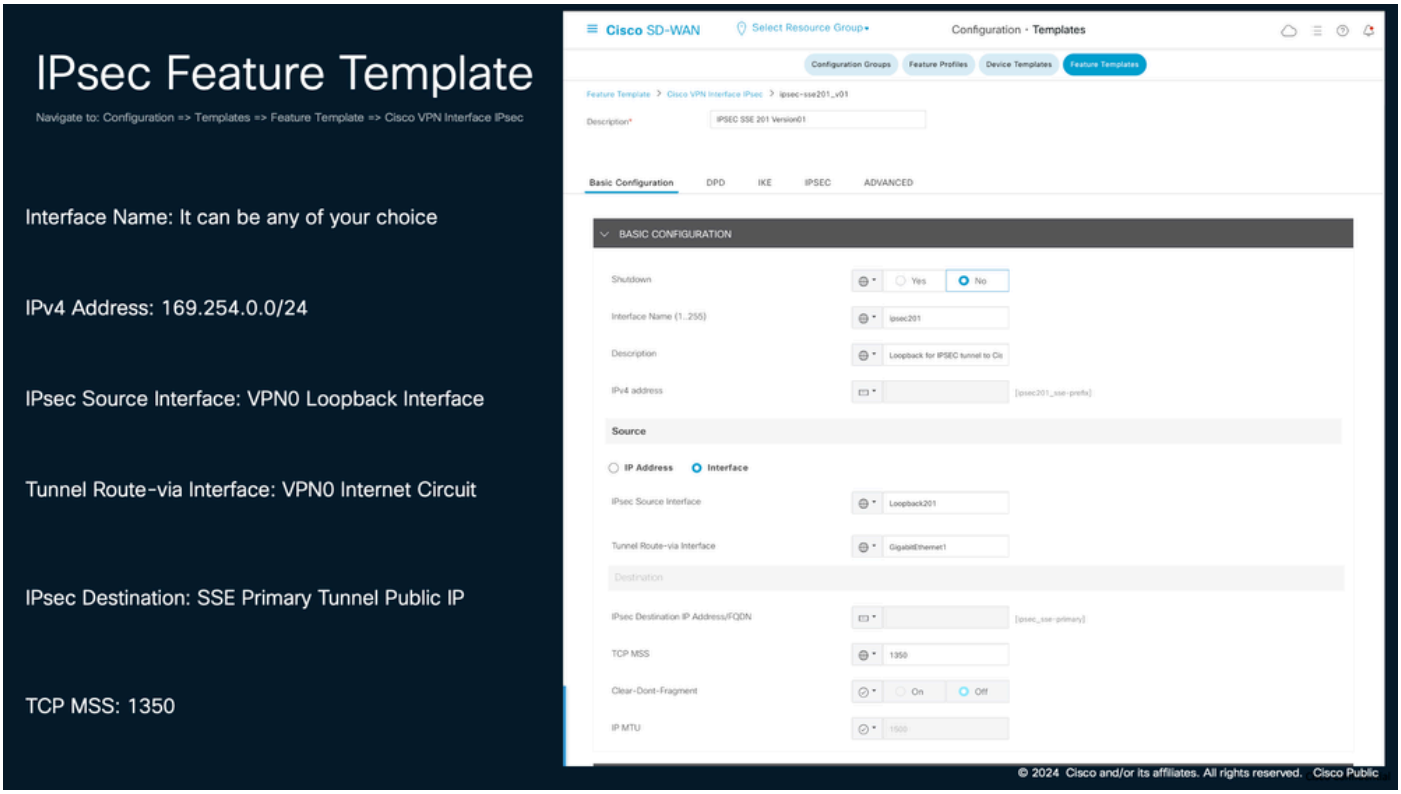
附註：對部署所需的隧道數重複此步驟。

請參閱有關通道限制的正式文檔：https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

這些步驟詳細說明了將DC1-HE1（資料中心1頭端1）連線到SSE Virginia Primary Hub的過程。此組態會在資料中心的SD-WAN路由器與位於維吉尼亞網真點(POP)的思科安全存取網路通道組(NTG)之間建立安全通道

步驟 1:建立IPSec功能模板
建立IPSec功能模板，以定義連線SD-WAN頭端路由器和NTG的IPSec隧道的引數。

圖11: IPsec功能模板：基本配置



IPsec功能模板：基本配置

介面名稱：你可以隨便選
IPv4地址：SSE根據您選擇的子網劃分要求監聽169.254.0.0/24，最佳做法請與/30一起使用。在本指南中，我們遺漏了第一個地址塊以供將來使用。

IPsec來源介面：定義當前IPsec介面唯一的VPN0環回介面。為了保持一致性和進行故障排除，建議使用相同的編號。
Tunnel Route-via Interface:指向可以用作底層到達SSE的介面（必須能夠訪問網際網路）

IPsec目標： 主集線器IP地址

請參閱圖7：安全訪問網路隧道組US(Virginia)這是35.171.214.188

TCP MSS:此值應為1350(參考:https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

範例：DC1-HE1向SSE Virginia Primary Hub遷移

介面名稱：ipsec201

描述：到Cisco的IPSEC隧道的環回

IPv4地址：169.254.0.x/30

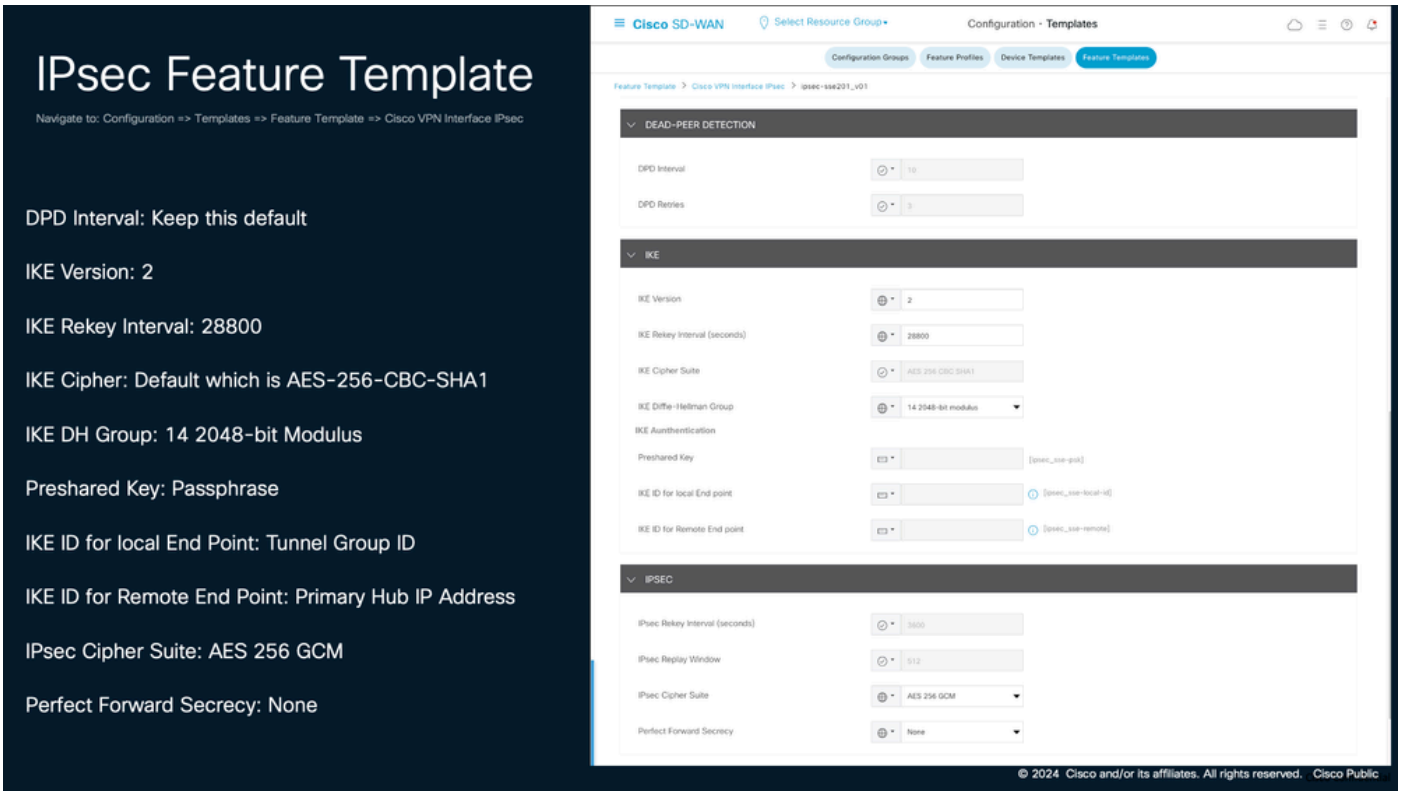
IPsec源介面：環回201

Tunnel Route-via Interface:GigabitEthernet1

IPsec目標IP地址/FQDN:35.xxx.xxx.xxx

TCP MSS:1350

圖12: IPsec功能模板：IKE IPSEC



IPsec功能模板：IKE IPSEC

DPD間隔：保留此預設值
IKE版本：2
IKE重新生成金鑰間隔：28800
IKE密碼：預設值為AES-256-CBC-SHA1
IKE DH組：14 2048位模數
預共用金鑰：密碼
本地終端的IKE ID:隧道組ID

請參閱圖7: Secure Access Network Tunnel Group US(Virginia)這是mn03lab1+201@8167900-638880310-sse.cisco.com

---

附註：每個隧道必須具有唯一的終結點才能執行此操作；使用"+loopbackID"示例：mn03lab1+202@8167900-638880310-sse.cisco.com、mn03lab1+203@8167900-638880310-sse.cisco.com等。

遠端終端的IKE ID:主集線器IP地址
IPsec密碼套件：AES 256 GCM
完全向前保密：無

參考：https://docs.sse.cisco.com/sse-user-guide/docs/configure-tunnels-with-catalyst-sdwan#define-the-feature-template

範例：

IKE版本：2
IKE重新生成金鑰間隔：28800
IKE密碼：AES-256-CBC-SHA1
IKE DH組：14 2048位模數
預共用金鑰：*****

附註：新增網路隧道組中的步驟6

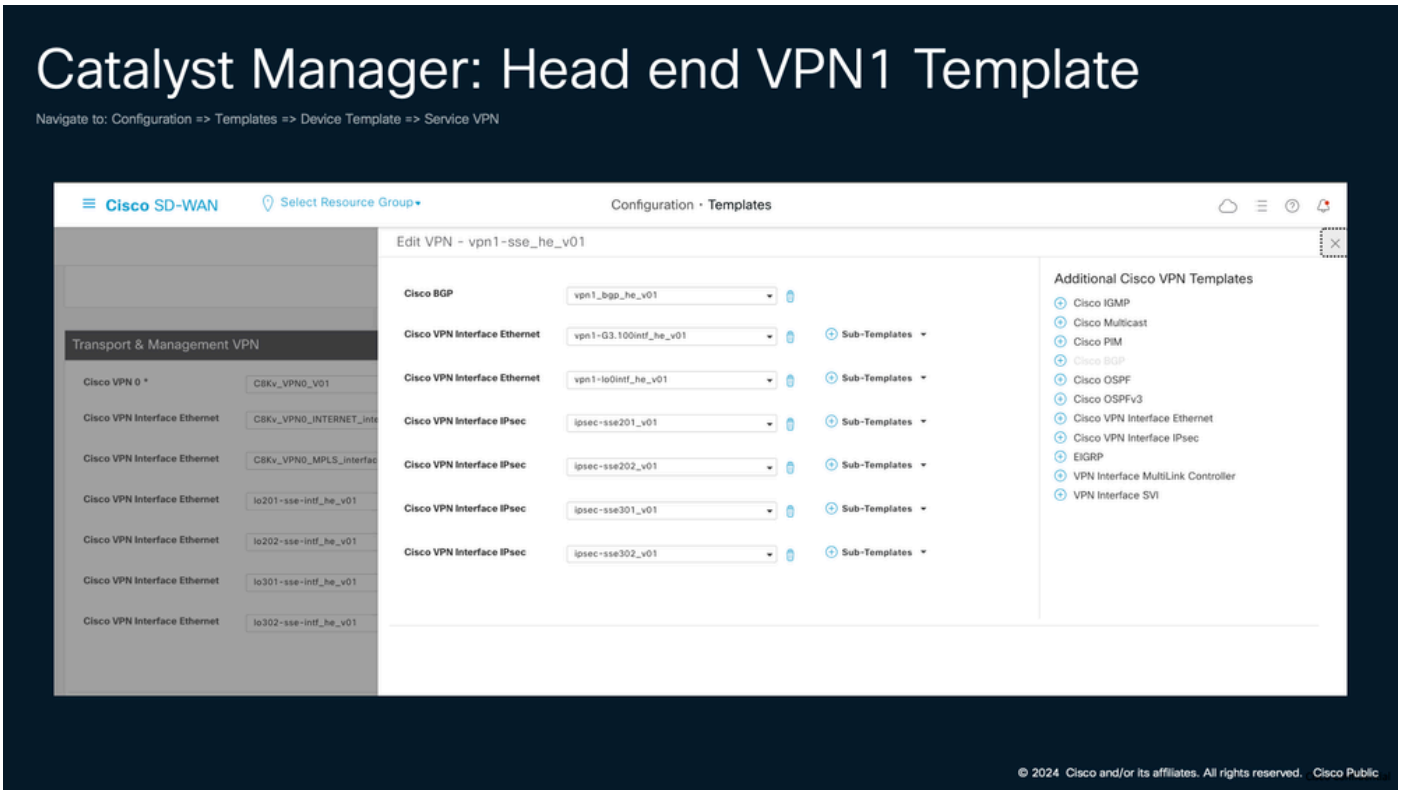
本地終端的IKE ID:mn03lab1@8167900-638880310-sse.cisco.com
遠端終端的IKE ID:35.171.xxx.xxx
IPsec密碼套件：AES 256 GCM
完全向前保密：無

重複這些步驟，為主要和輔助安全接入集線器配置所需的隧道。對於2x2設定，您將總共建立四個隧道：

- 從DC1-HE1到主要安全接入集線器的兩個隧道
- 從DC1-HE1到輔助安全接入集線器的兩個隧道

建立模板後，我們將在圖13所示的服務端vrf上使用模板，並在圖14所示的全域性vrf上使用定義的環回。

圖13: Catalyst SD-WAN管理器：頭端VPN1模板2x2



Catalyst管理器：頭端VPN1模板

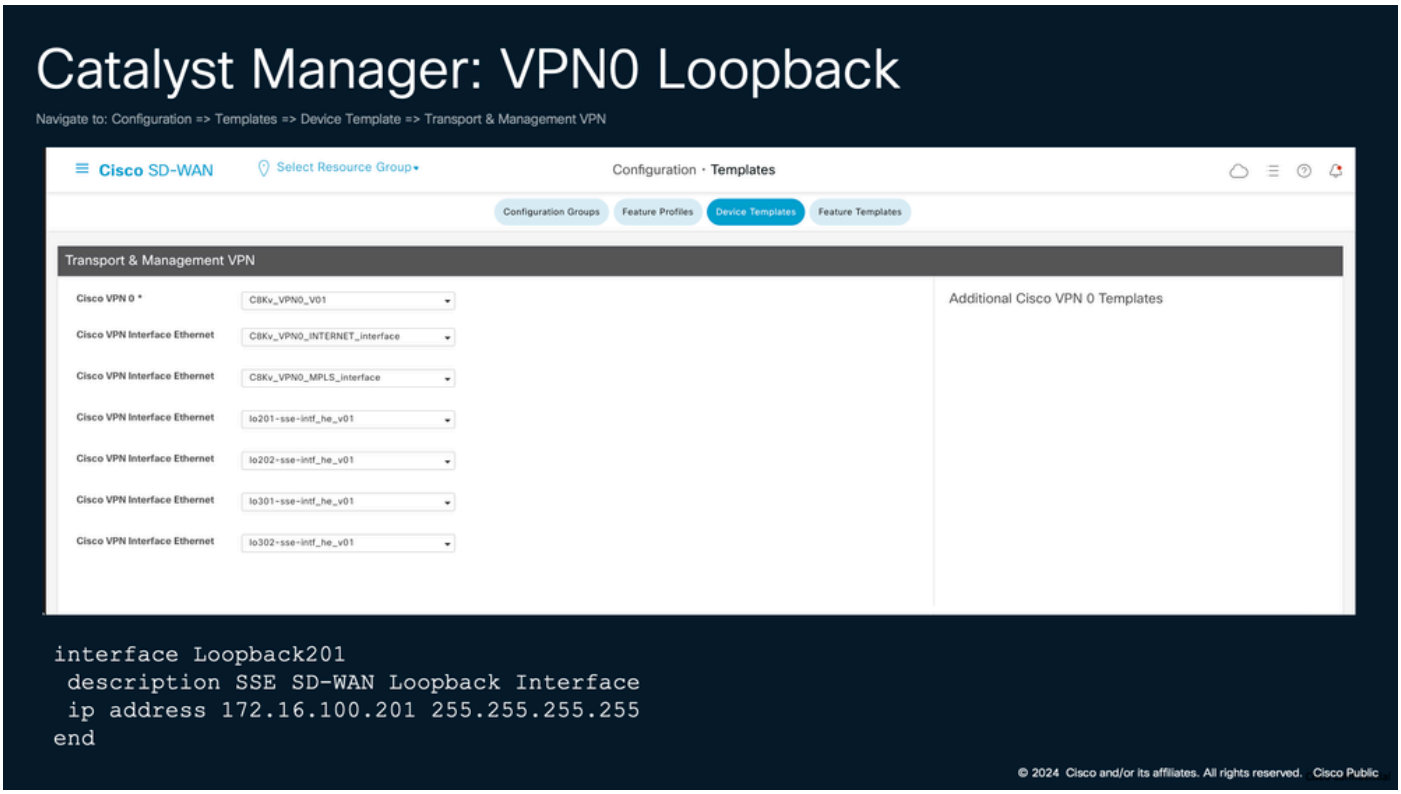
步驟 2:定義全域性VRF中的環回

在全域性VRF（虛擬路由和轉發）表中配置環回介面。此環回用作步驟1中建立的IPSec隧道的源介面。

步驟1中引用的所有環回必須在全域性VRF中定義。

IP地址可以在任何RFC1918範圍內定義。

圖14: Catalyst SD-WAN管理器：VPN0環回

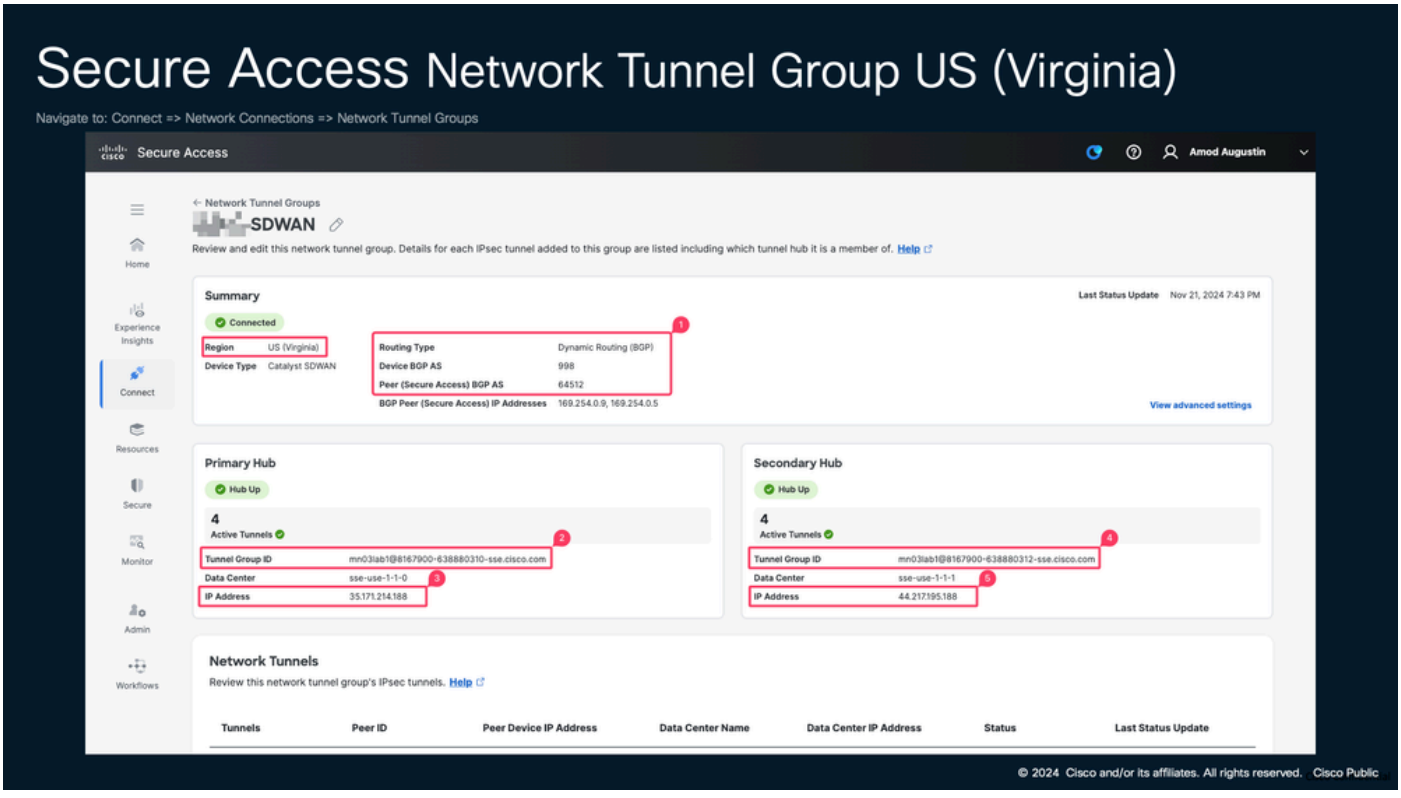


Catalyst管理器：VPN0環回

程式3.配置BGP鄰居關係

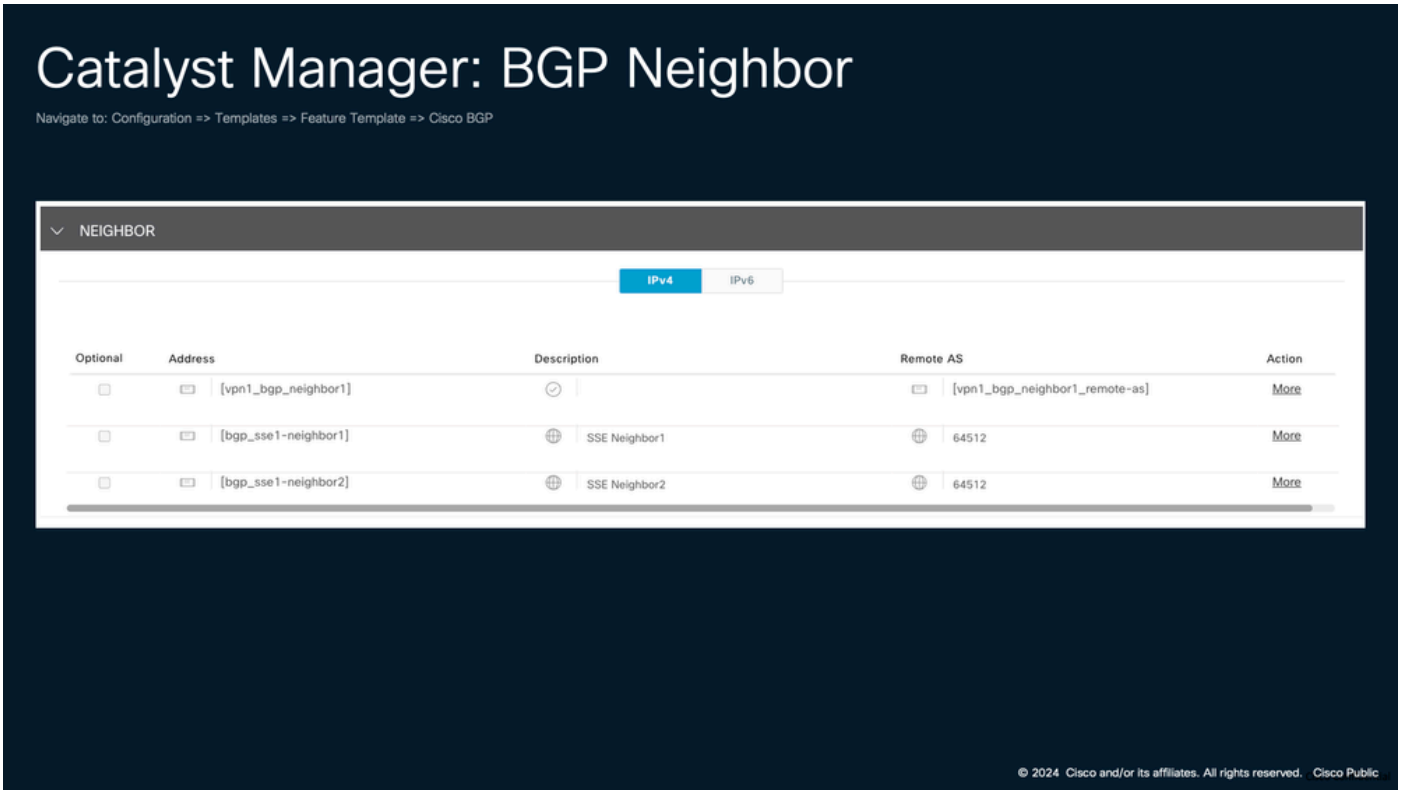
使用BGP功能模板為所有隧道介面定義BGP鄰居關係。請參閱思科安全存取入口中各自的網路通道組BGP設定以設定BGP值。

圖 15:安全存取網路通道組US（維吉尼亞）



在本示例中，我們使用圖15（框1）中的資訊來使用功能模板定義BGP。

圖 16:Catalyst SD-WAN管理員BGP鄰居



Catalyst SD-WAN管理員BGP鄰居

使用功能模板生成的配置：

```
router bgp 998
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf 1
  network 10.10.128.1 mask 255.255.255.255
  neighbor 169.254.0.5 remote-as 64512
  neighbor 169.254.0.5 description SSE Neighbor1
  neighbor 169.254.0.5 ebgp-multihop 5
  neighbor 169.254.0.5 activate
  neighbor 169.254.0.5 send-community both
  neighbor 169.254.0.5 next-hop-self
  neighbor 169.254.0.9 remote-as 64512
  neighbor 169.254.0.9 description SSE Neighbor2
  neighbor 169.254.0.9 ebgp-multihop 5
  neighbor 169.254.0.9 activate
  neighbor 169.254.0.9 send-community both
  neighbor 169.254.0.9 next-hop-self
  neighbor 169.254.0.105 remote-as 64512
  neighbor 169.254.0.105 description SSE Neighbor3
  neighbor 169.254.0.105 ebgp-multihop 5
  neighbor 169.254.0.105 activate
  neighbor 169.254.0.105 send-community both
  neighbor 169.254.0.105 next-hop-self
```

```
  neighbor 169.254.0.109 remote-as 64512
  neighbor 169.254.0.109 description SSE Neighbor4
  neighbor 169.254.0.109 ebgp-multihop 5
  neighbor 169.254.0.109 activate
  neighbor 169.254.0.109 send-community both
  neighbor 169.254.0.109 next-hop-self
  neighbor 172.16.128.2 remote-as 65510
  neighbor 172.16.128.2 activate
  neighbor 172.16.128.2 send-community both
  neighbor 172.16.128.2 route-map sse-routes-in in
  neighbor 172.16.128.2 route-map sse-routes-out out
  maximum-paths eibgp 4
  distance bgp 20 200 20
 exit-address-family
DC1-HE1#
```

驗證

```
DC1-HE1#show ip route vrf 1 bgp | begin Gateway
Gateway of last resort is not set

35.0.0.0/32 is subnetted, 1 subnets
B 35.95.175.78 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
44.0.0.0/32 is subnetted, 1 subnets
B 44.240.251.165 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
100.0.0.0/8 is variably subnetted, 17 subnets, 2 masks
B 100.81.0.58/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.59/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.60/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.61/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.62/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.63/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.64/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.65/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h

DC1-HE1#show ip bgp vpnv4 all summary
BGP router identifier 172.16.100.232, local AS number 998

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.0.5 4 64512 12787 13939 3891 0 0 4d10h 18
169.254.0.9 4 64512 66124 64564 3891 0 0 3d01h 18
169.254.0.13 4 64512 12786 13933 3891 0 0 4d10h 18
169.254.0.17 4 64512 12786 13927 3891 0 0 4d10h 18
172.16.128.2 4 65510 83956 84247 3891 0 0 7w3d 1

DC1-HE1#show ip interface brief | include Tunnnel
Tunnel1 192.168.128.202 YES TFTP up up
```

```
Tunnel4 198.18.128.11 YES TFTP up up
Tunnel100022 172.16.100.22 YES TFTP up up
Tunnel100023 172.16.100.23 YES TFTP up up
Tunnel100201 169.254.0.6 YES other up up
Tunnel100202 169.254.0.10 YES other up up
Tunnel100301 169.254.0.14 YES other up up
Tunnel100302 169.254.0.18 YES other up up
```

參考

主用/主用實施具有來自與SD-WAN頭端連線的核心交換機的多路徑。

圖 17:BGP鄰居的主用/主用方案

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *m   1.1.1.1/32       172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
<snip>
```

主用/主用BGP鄰居

由於ASPL預置（使用到鄰居的路由對映完成），主用/備用實施將具有一個從核心交換機到SD-WAN頭端的有效路徑。

圖 18:BGP鄰居的主用/備用方案

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *    1.1.1.1/32       172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 *    [redacted]32     172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 *    [redacted]/32    172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 <snip>
```

主用/備用BGP鄰居

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）。