使用手动方法在安全服务边缘和SD-WAN之间配置专用应用互联

目录

简介

本文档介绍将思科安全访问与SD-WAN路由器连接起来的综合指南，侧重于安全专用应用访问。

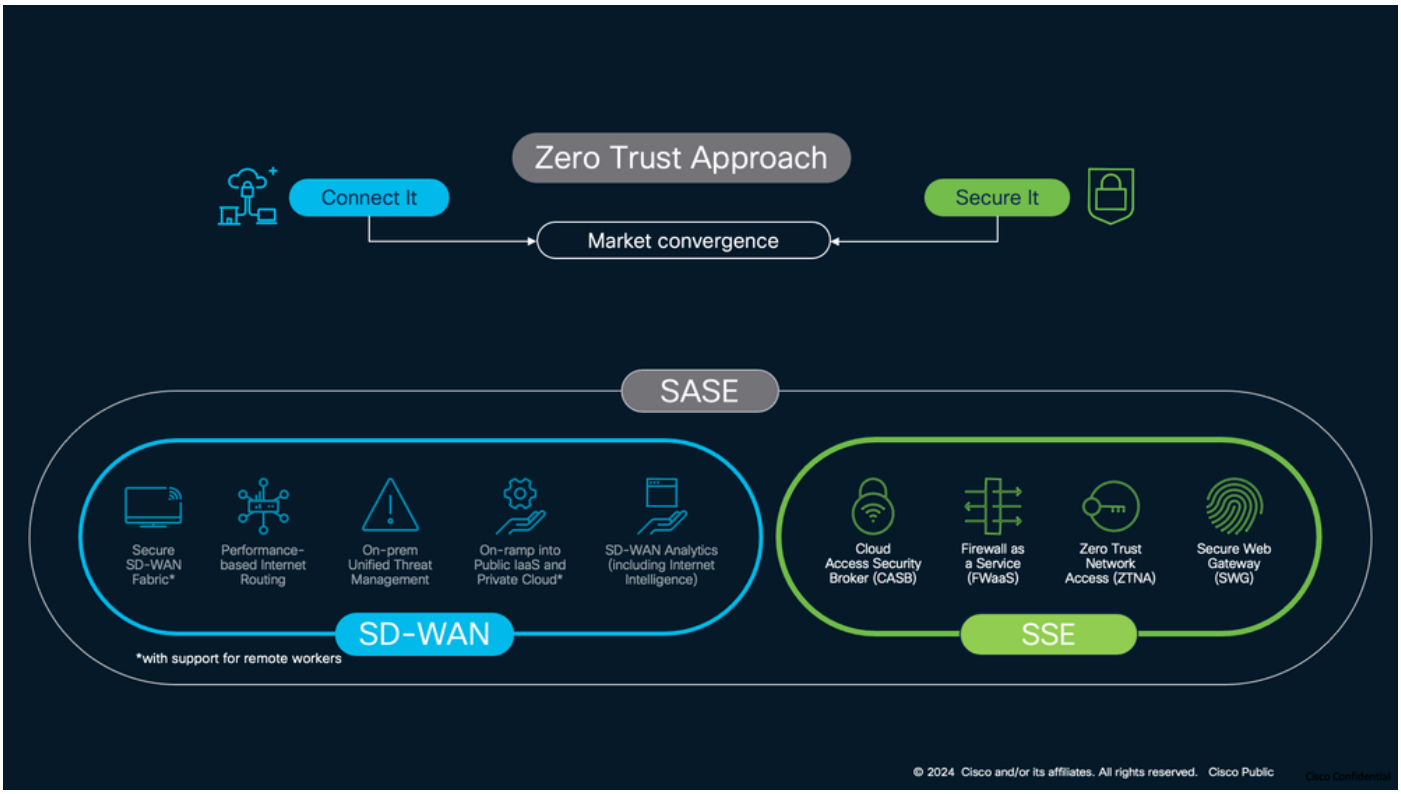
关于本指南

注：此处列出的配置是为SD-WAN的UX1.0和17.9/20.9版本开发的。

本指南对下列关键步骤进行了结构化演练：

- 定义网络隧道组(NTG)
- IPSec隧道配置：有关在Cisco SD-WAN路由器和Cisco Secure Access NTG之间设置安全IPSec隧道的详细说明。
- BGP邻居关系：分步操作通过IPSec隧道运行BGP邻居关系以确保动态路由和提高网络恢复能力。
- 专用应用访问：有关通过已建立的隧道配置和保护对专用应用的访问的指导。

图 1：思科SD-WAN和SSE零信任方法



使用SD-WAN的SSE

本指南重点介绍NTG互联的设计注意事项和部署最佳实践。在本指南中，SD-WAN控制器部署在云中，而WAN Edge路由器部署在数据中心，并连接到至少一个互联网电路。

主要假设

- 思科安全访问安全服务边缘(SSE):假设已为您的组织调配思科安全访问SSE。
- 思科SD-WAN广域网边缘路由器：假设广域网边缘路由器集成到重叠网络中，从而有效地促进用户通过SD-WAN基础设施进行通信。
- 虽然本指南主要侧重于设计和配置的SD-WAN方面，但它提供了一种将思科安全接入解决方案集成到现有网络架构中的整体方法。

关于此解决方案

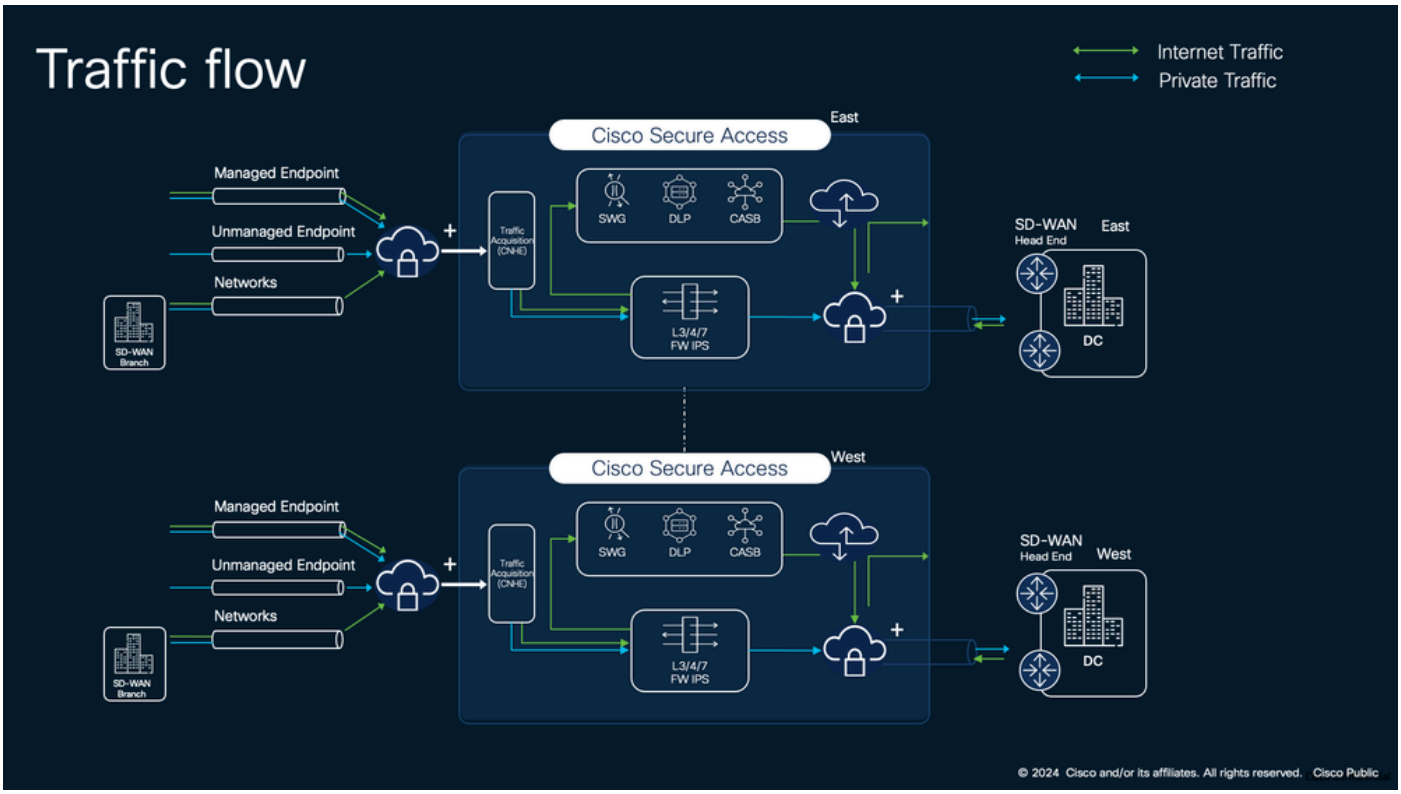
Cisco Secure Access提供的专用应用隧道为通过零信任网络访问(ZTNA)和VPN即服务(VPNaaS)连接的用户提供到专用应用的安全连接。 这些隧道使组织能够将远程用户安全地链接到托管在数据中心或私有云中的私有资源。
使用IKEv2（互联网密钥交换版本2），这些隧道组在思科安全访问和SD-WAN路由器之间建立安全的双向连接。它们通过同一组内的多个隧道支持高可用性，并通过静态和动态路由(BGP)提供灵活的流量管理。
IPsec隧道可以传输来自各种来源的流量，包括：

- 远程访问VPN用户
- 基于浏览器或基于客户端的ZTNA连接
- 连接到思科安全访问的其他网络位置

此方法使组织能够通过统一的加密通道安全地路由所有类型的专用应用流量，从而提高安全性和运

营效率。
作为思科安全服务边缘(SSE)解决方案的一部分，思科安全接入通过单一的云托管控制台、统一客户端、集中策略创建和汇总报告简化IT运营。它在一个云交付解决方案中整合了多个安全模块，包括ZTNA、安全网络网关(SWG)、云访问安全代理(CASB)、防火墙即服务(FWaaS)、DNS安全、远程浏览器隔离(RBI)等。这一全面的方法通过应用零信任原则和实施精细的安全策略来降低安全风险

图 2：思科安全访问和专用应用之间的流量



SSE专用应用流量

本指南中介绍的解决方案解决了全面的冗余注意事项，包括数据中心中的SD-WAN路由器和安全服务边缘(SSE)端的网络隧道组(NTG)。本指南重点介绍主用/主用SD-WAN中心部署模式，这有助于保持不间断的流量流并确保高可用性。

先决条件

要求

建议您了解以下主题：

- Cisco SD-WAN配置和管理
- IKEv2和IPSec协议基础知识
- 在思科安全访问门户中配置网络隧道组
- BGP和ECMP知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 20.9.5a上的思科SD-WAN控制器
- 17.9.5a上的思科SD-WAN广域网边缘路由器
- 思科安全访问门户

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

设计

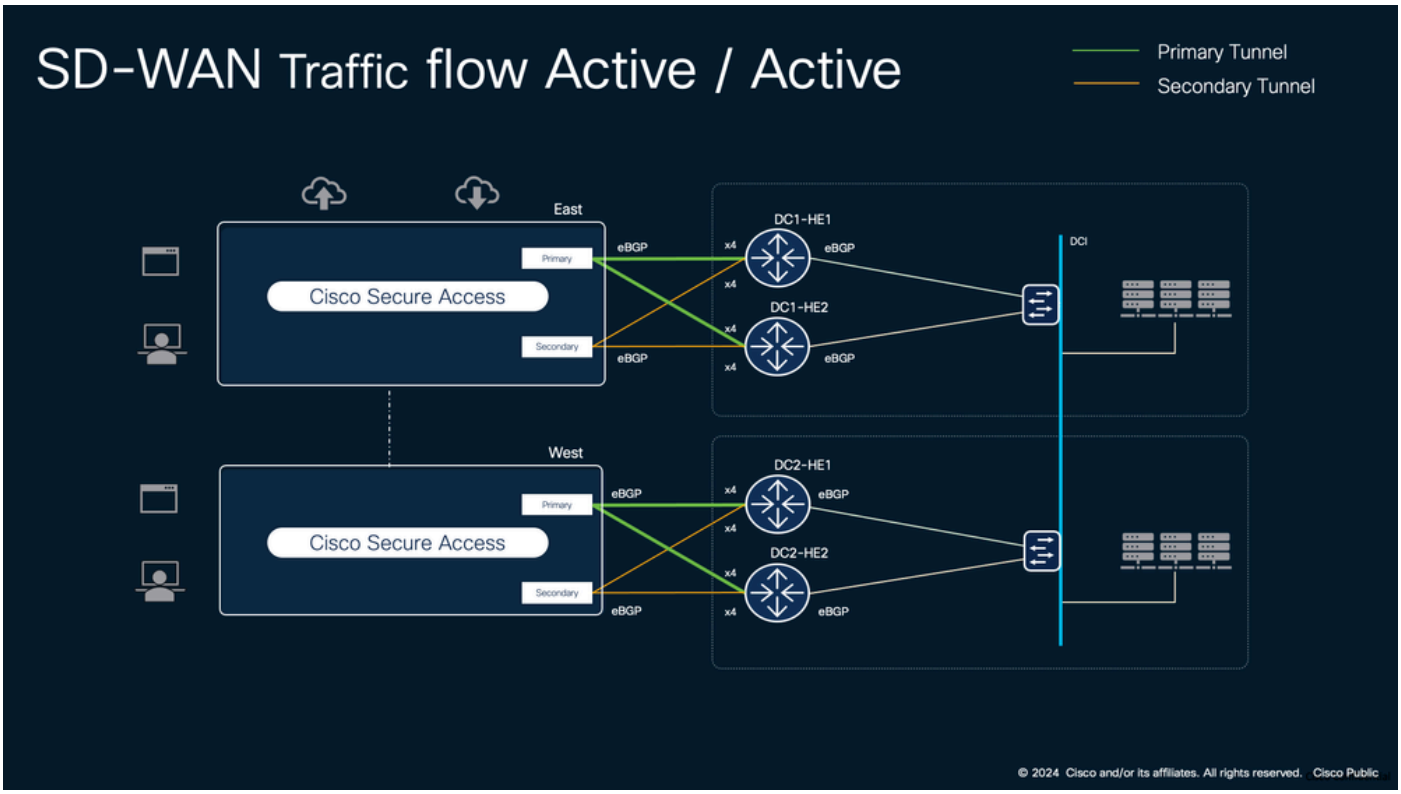
本指南介绍使用SD-WAN头端路由器主用/主用设计模型的解决方案。SD-WAN前端路由器情景中的主用/主用设计模型假设数据中心中有两台路由器，它们均连接到安全服务边缘(SSE)网络隧道组(NTG)，如图3所示。在此场景中，数据中心中的两台SD-WAN路由器（DC1-HE1和DC1-HE2）均主动处理流量。它们通过向内部DC邻居发送相同的AS路径长度(ASPL)来实现此目的。因此，来自DC内部的流量在两个头端之间实现负载均衡。

每个头端路由器可以建立多个到SSE入网点(POP)的隧道。 隧道数量取决于您的要求和SD-WAN设备型号。在此设计中：

- 每台路由器有4条隧道连接到主SSE集线器，4条隧道连接到辅助SSE集线器。
- 每个SSE中心支持的最大隧道数可能不同。有关最新信息，请参阅官方文档：https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

这些头端路由器通过通向SSE的隧道形成BGP邻居关系。通过这些邻居关系，头端向其SSE邻居通告私有应用前缀，从而支持安全且高效地将流量路由到私有资源。

图 3：SD-WAN到SSE主用/主用部署模式



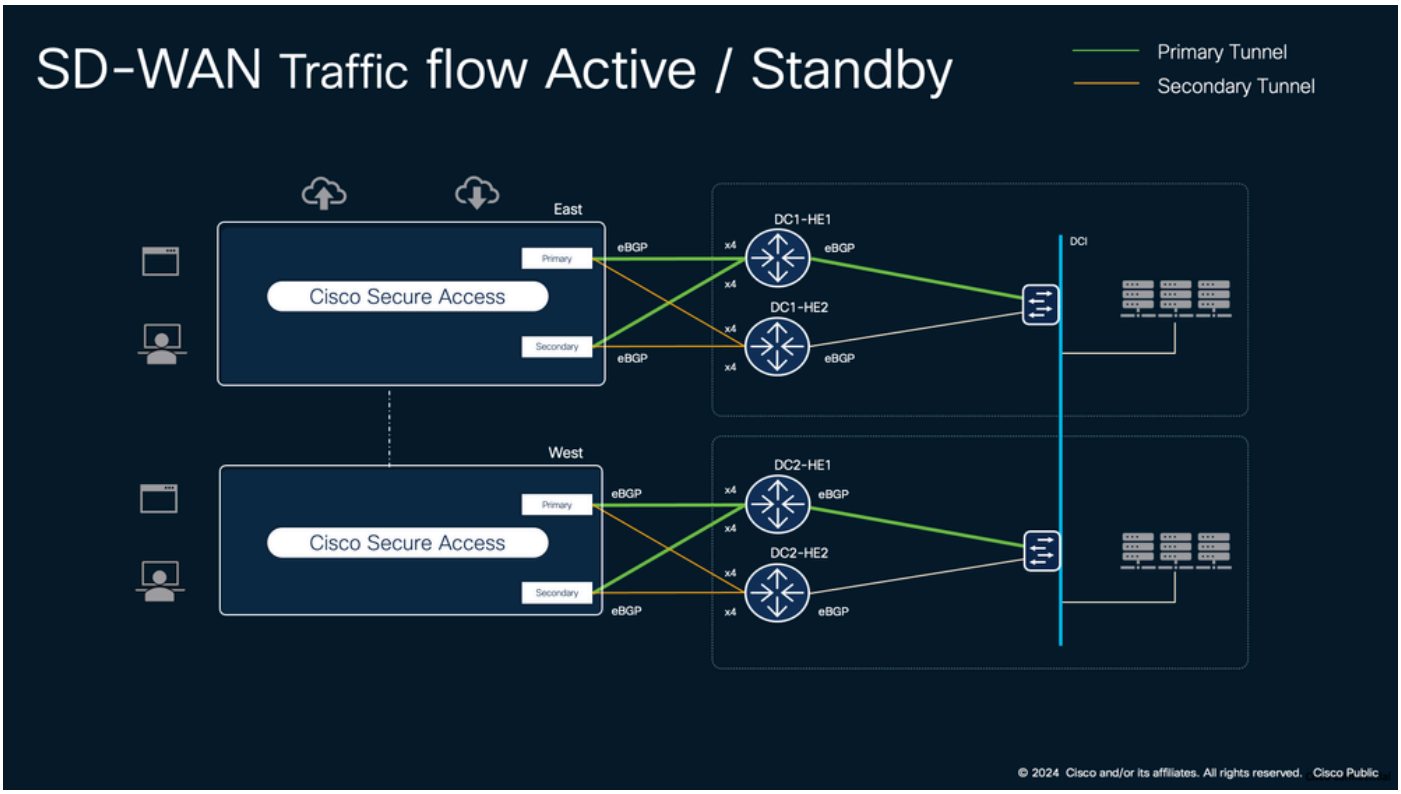
SD-WAN到SSE主用/主用部署模式

主用/备用设计将一台路由器(DC1-HE1)指定为始终主用路由器，而辅助路由器(DC1-HE2)保持备用状态。流量始终流经活动前端(DC1-HE1)，除非完全发生故障。此部署模式有一个缺点：如果通向SSE的主隧道断开，流量会切换到仅通过DC1-HE2的辅助SSE隧道，从而导致任何有状态流量重置。

在主用/备用模式中，BGP AS路径长度用于在数据中心内和向SSE引导流量。DC1-HE1向ASPL为2的SSE BGP邻居发送前缀更新，而DC1-HE2向ASPL为3的邻居发送更新。DC1-HE1的内部DC邻居通告的AS路径长度比DC1-HE2短，从而确保DC1-HE1的流量优先级。（客户可以选择其他属性或协议来影响流量优先级。）

客户可以根据自己的特定需求选择主用/主用或主用/备用部署模式。

图 4：SD-WAN到SSE主用/备用部署模式



SD-WAN到SSE主用/备用部署模式

配置

本节介绍以下过程：

1. 验证在思科安全访问门户中调配网络隧道组的必备条件。
2. 使用IPsec手动方法配置思科安全访问网络隧道组(NTG)的SD-WAN互联。
3. 配置BGP邻居关系

注意：此配置基于主用/主用部署模式

程序1.验证思科安全访问门户上的网络隧道组配置

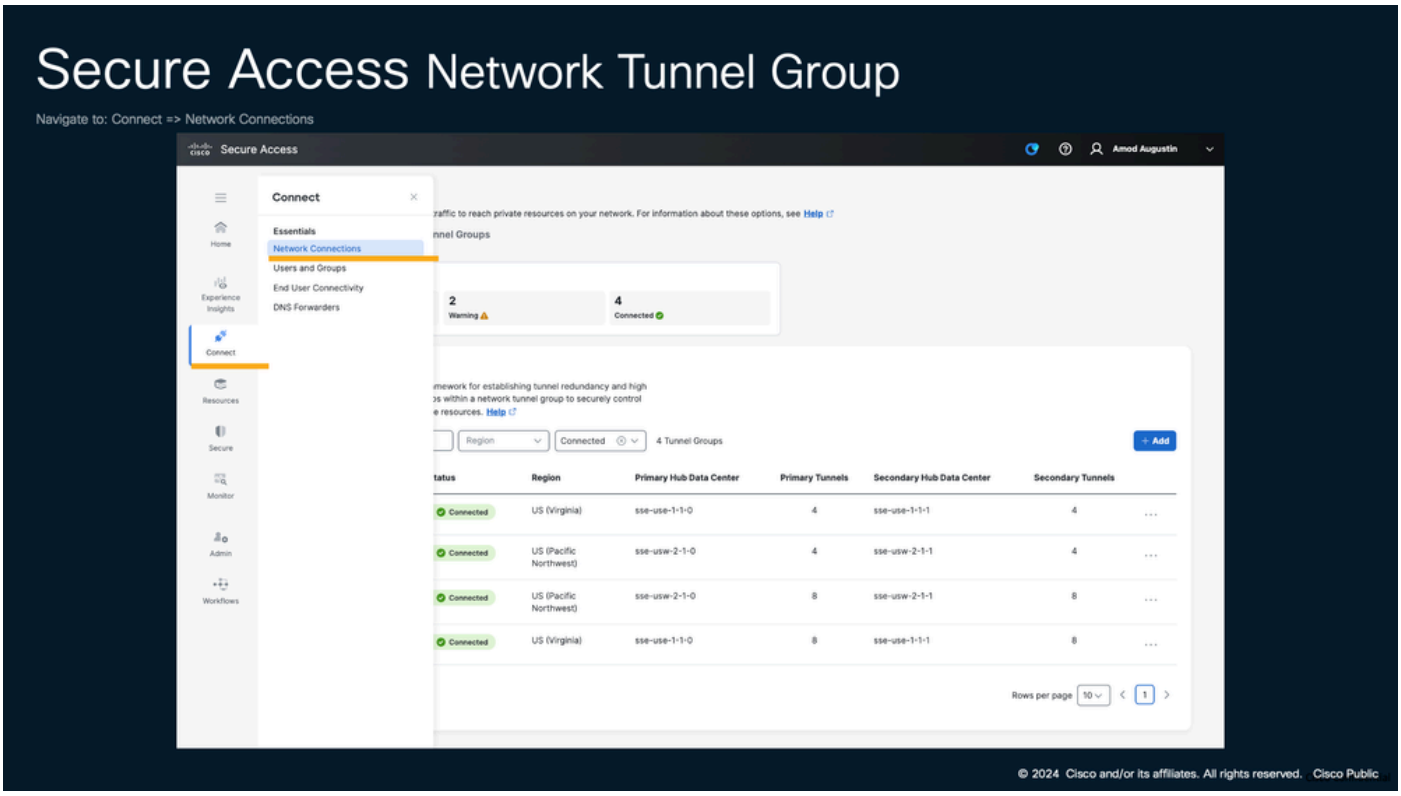
本指南未介绍如何配置网络隧道组。请查看此参考。

- 添加网络隧道组：SSE文档
- 使用带BGP的ECMP在Cisco安全访问和Cisco IOS XE路由器之间配置网络隧道

导航到Cisco Secure Access并确保已调配网络隧道组(NTG)。对于当前设计，我们需要在两个不同的入网点(POP)中调配NTG。 在本指南中，我们在美国（弗吉尼亚）POP和美国（太平洋西北）POP中使用NTG。

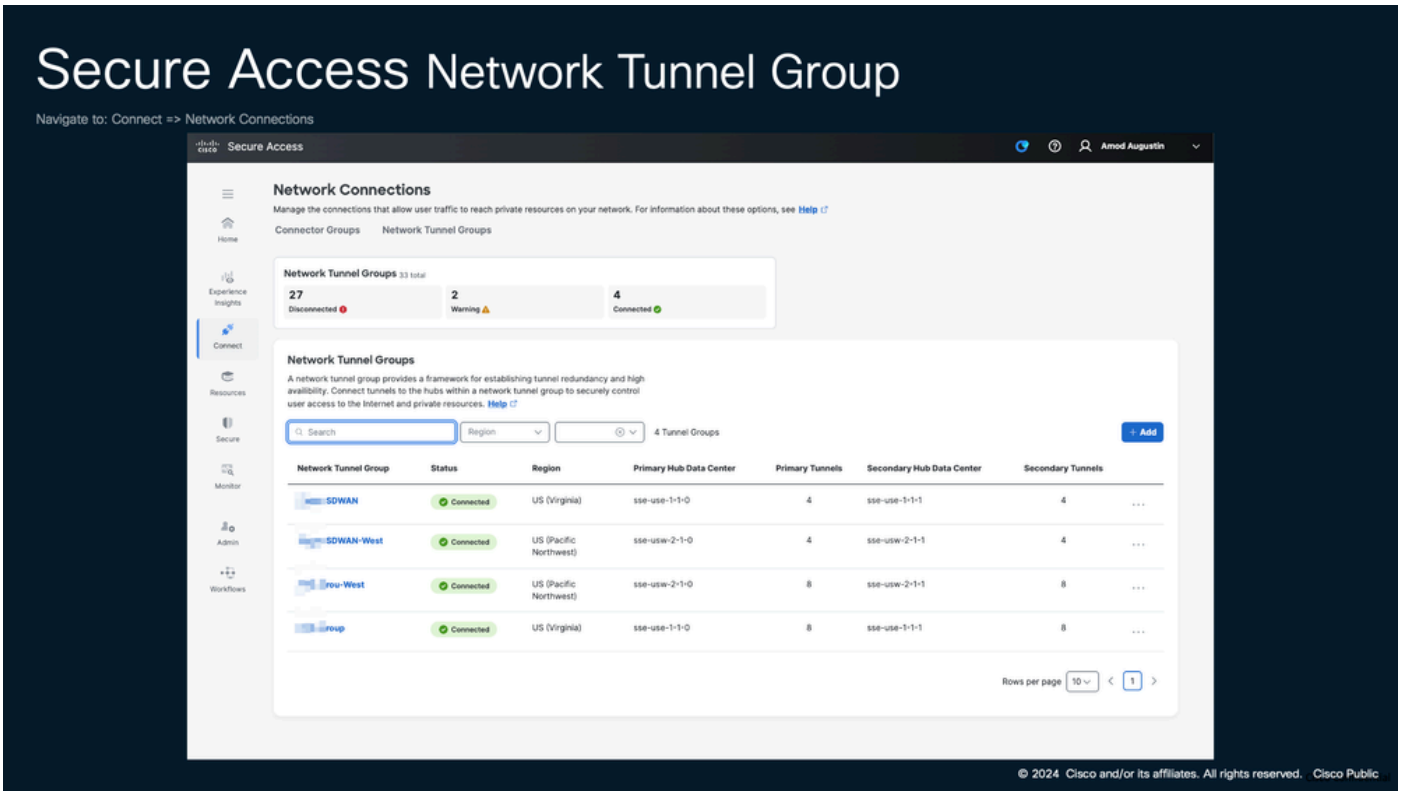
注意:POP的名称和位置可能有所不同，但关键概念是在地理位置接近您的数据中心的位置调配多个NTG。此方法有助于优化网络性能并提供冗余。

图 5：思科安全访问网络隧道组



思科安全访问网络隧道组

图 6：思科安全访问网络隧道组列表



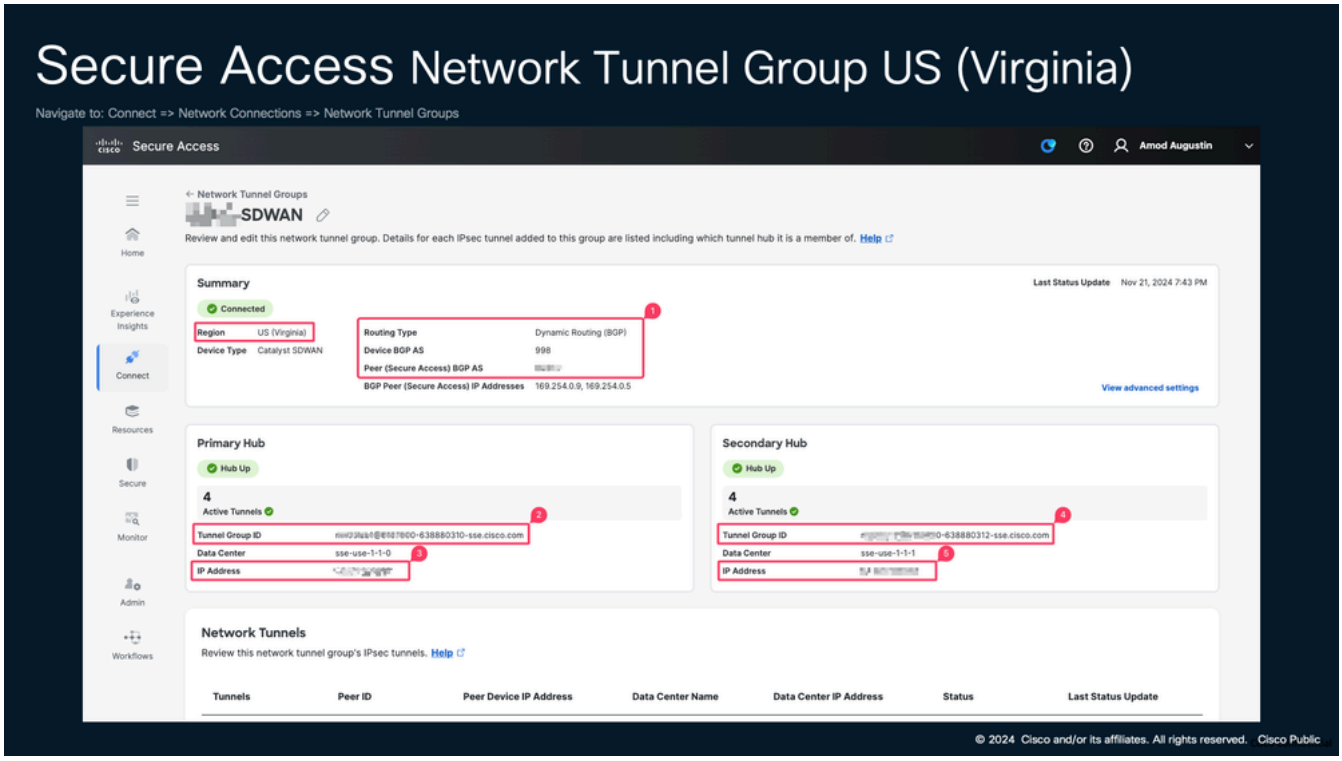
安全访问网络隧道组列表

确保您注意到了隧道口令（在创建隧道期间只显示一次）。

注意：Add a Network Tunnel Group中的步骤6

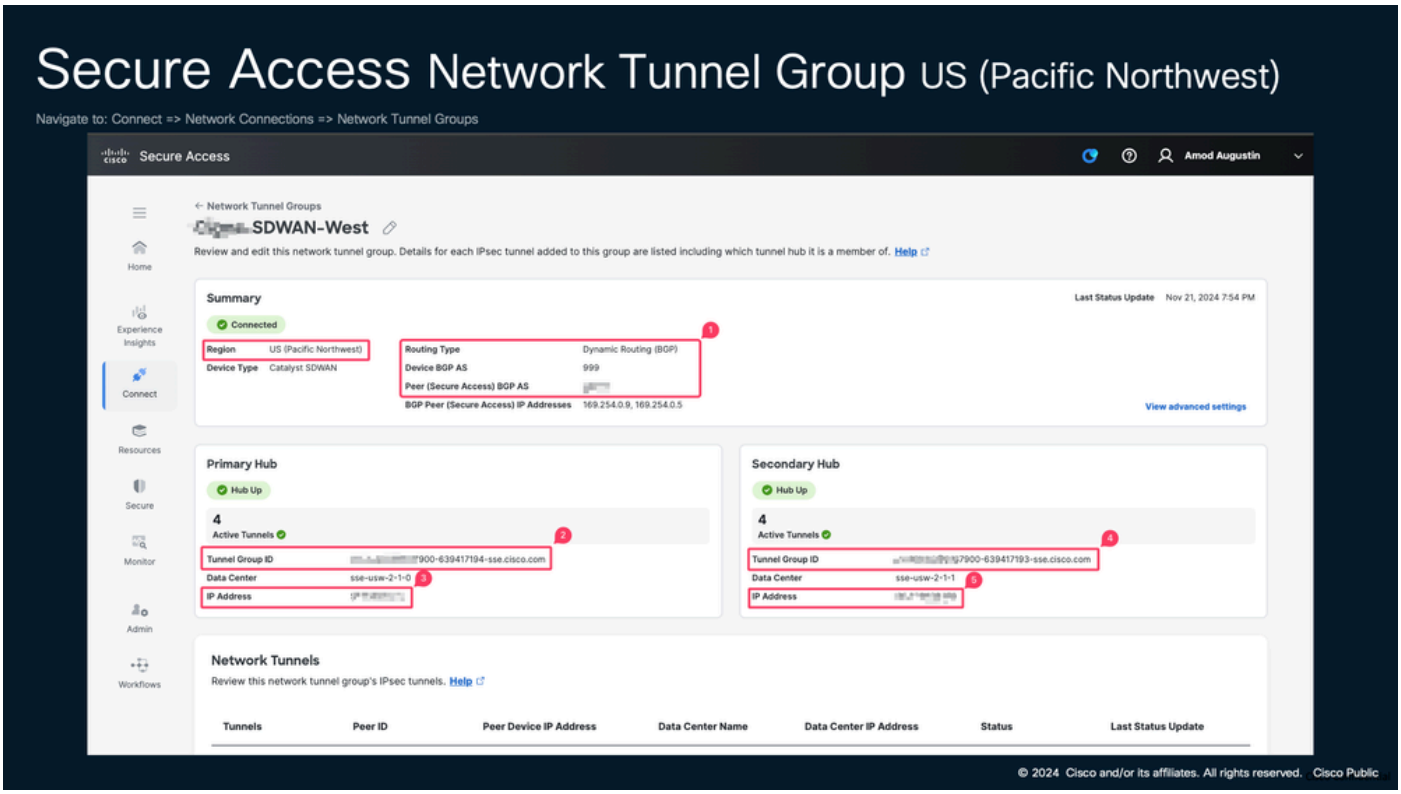
另请记下我们在IPSec配置期间使用的隧道组属性。屏幕快照（图6）取自实验室环境，用于根据设计或使用建议创建NTG组的生产场景。

图7：安全访问网络隧道组US（弗吉尼亚）



安全访问网络隧道组US（弗吉尼亚）

图8：安全接入网络隧道组US（太平洋西北部）

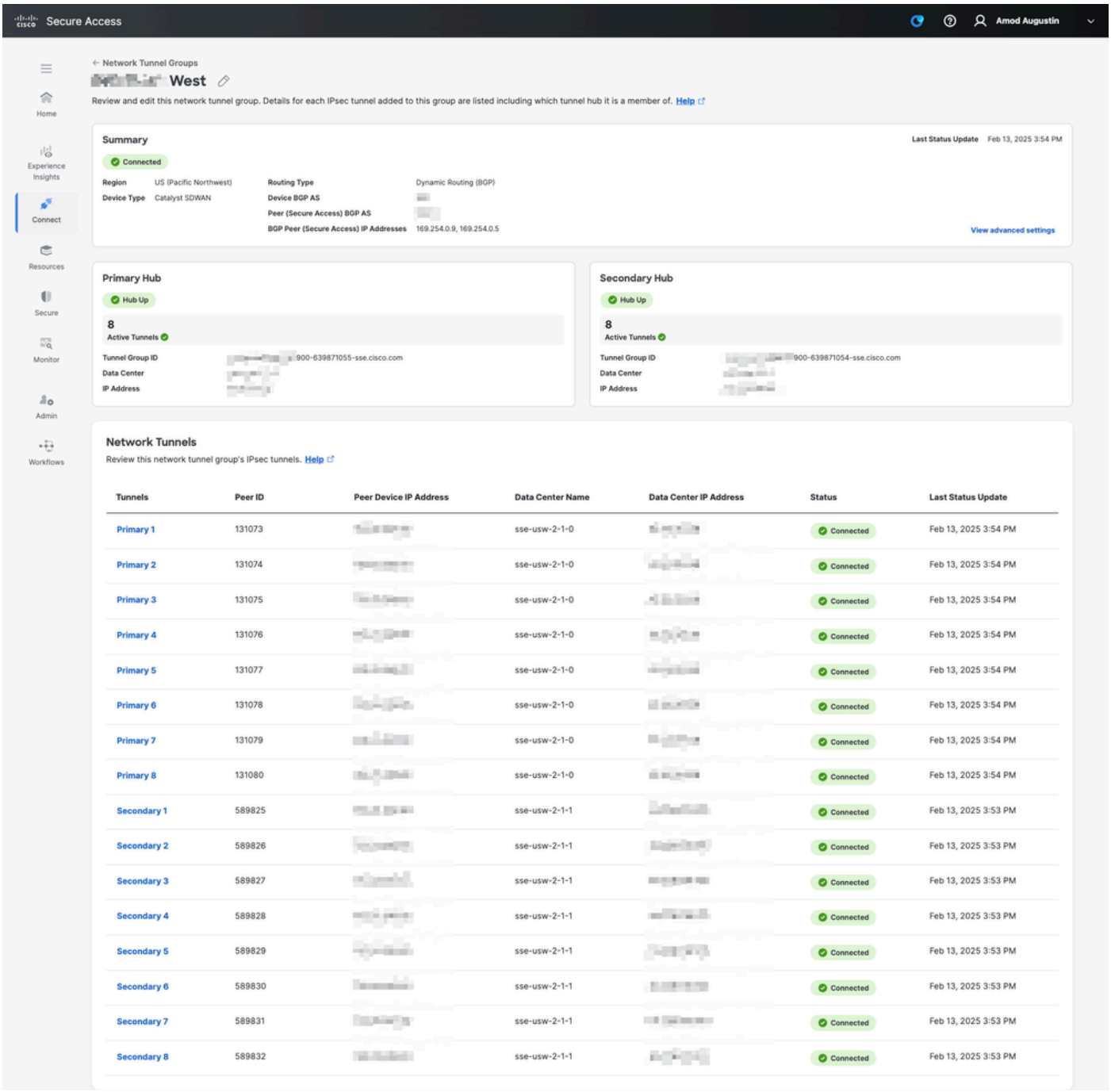


安全访问网络隧道组US（太平洋西北部）

图8显示主要和辅助集线器上只有4个隧道。但是，已在控制器环境中成功测试了最多8个隧道。最大隧道支持可能因所使用的硬件设备和当前的SSE隧道支持而异。有关最新信息，请参阅官方文档：https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels和相应硬件设备的发行说明。

此处提供了8通道设置的示例。

图8a:最多8个隧道的NTG隧道



SSE NTG最多支持8个隧道

程序2.使用IPsec手动方法配置思科安全访问网络隧道组(NTG)的SD-WAN互联。

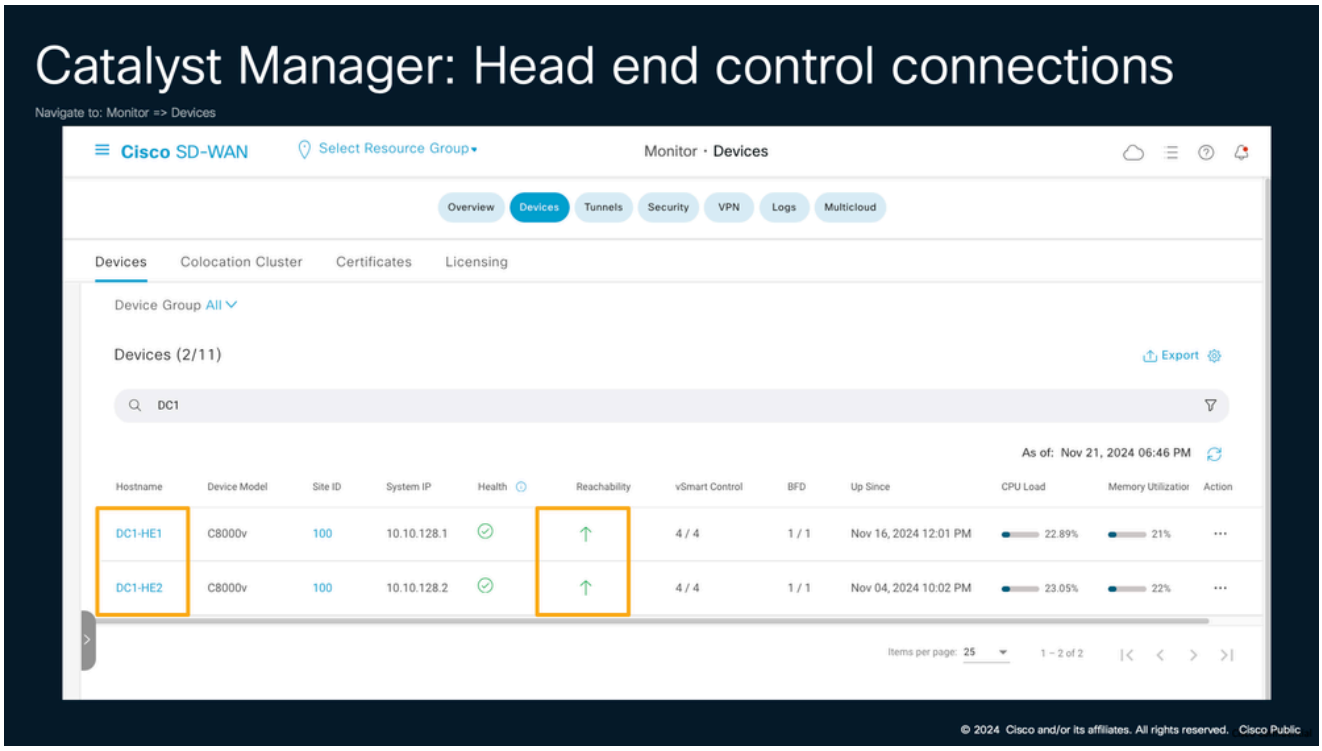
此过程演示如何使用运行17.9版本的Cisco Catalyst SD-WAN Manager 20.9和Cisco Catalyst Edge路由器上的功能模板连接网络隧道组(NTG)。

注意：本指南假设现有的SD-WAN重叠部署采用中心辐射型或全网状拓扑，其中集线器充当数据中心中托管专用应用的接入点。此程序也可用于分支机构或云部署。

在继续操作之前，请确保满足以下前提条件：

1. 设备上已启用控制连接，以允许从Cisco Catalyst SD-WAN Manager进行必要的更新。

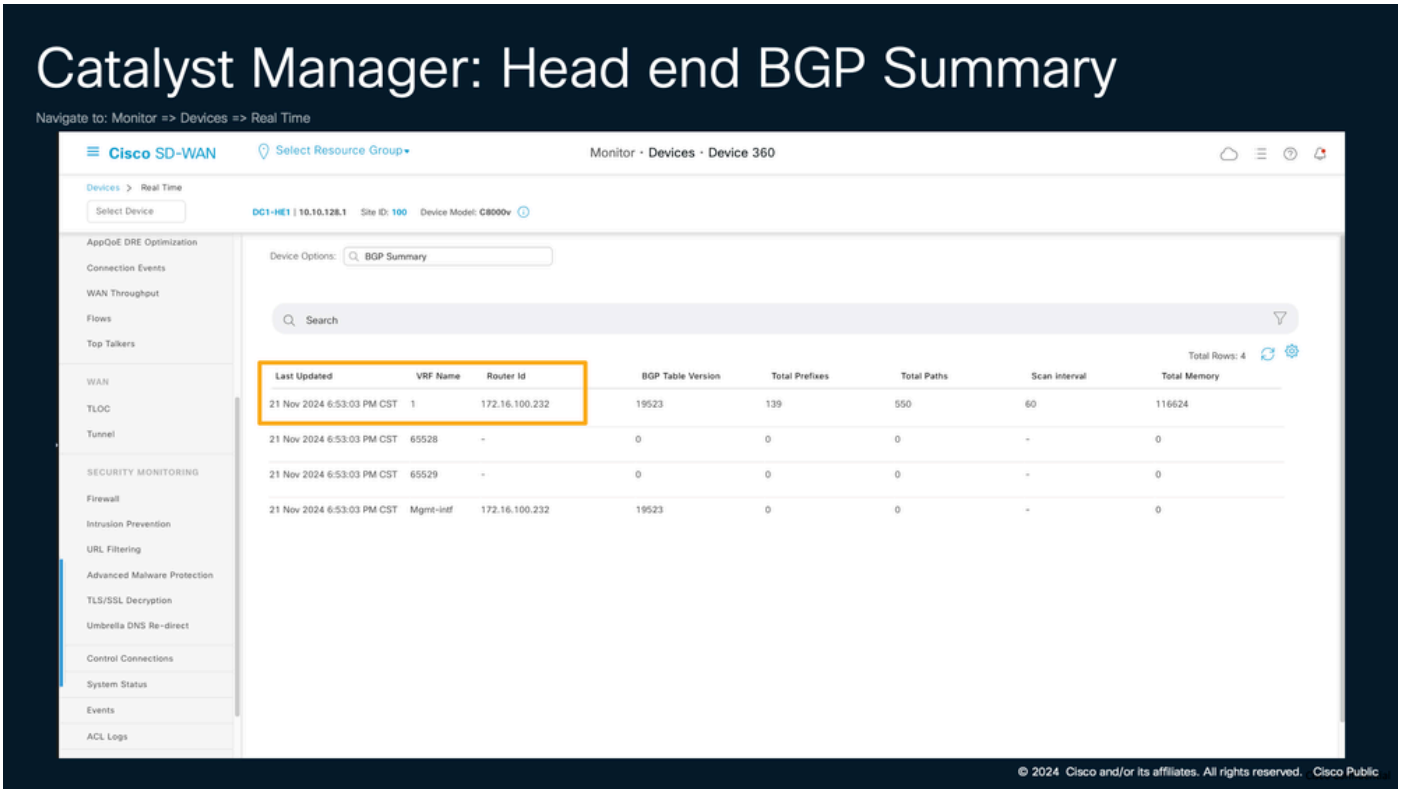
图 9：Cisco Catalyst SD-WAN管理器：头端控制连接



Catalyst管理器：头端控制连接

2. 配置服务端VPN并使用路由协议通告前缀。本指南使用BGP作为服务端的路由协议。

图 10：Cisco Catalyst SD-WAN管理器：头端BGP摘要



要使用手动IPSec方法配置带有网络隧道组(NTG)的SD-WAN互联，请完成以下步骤：

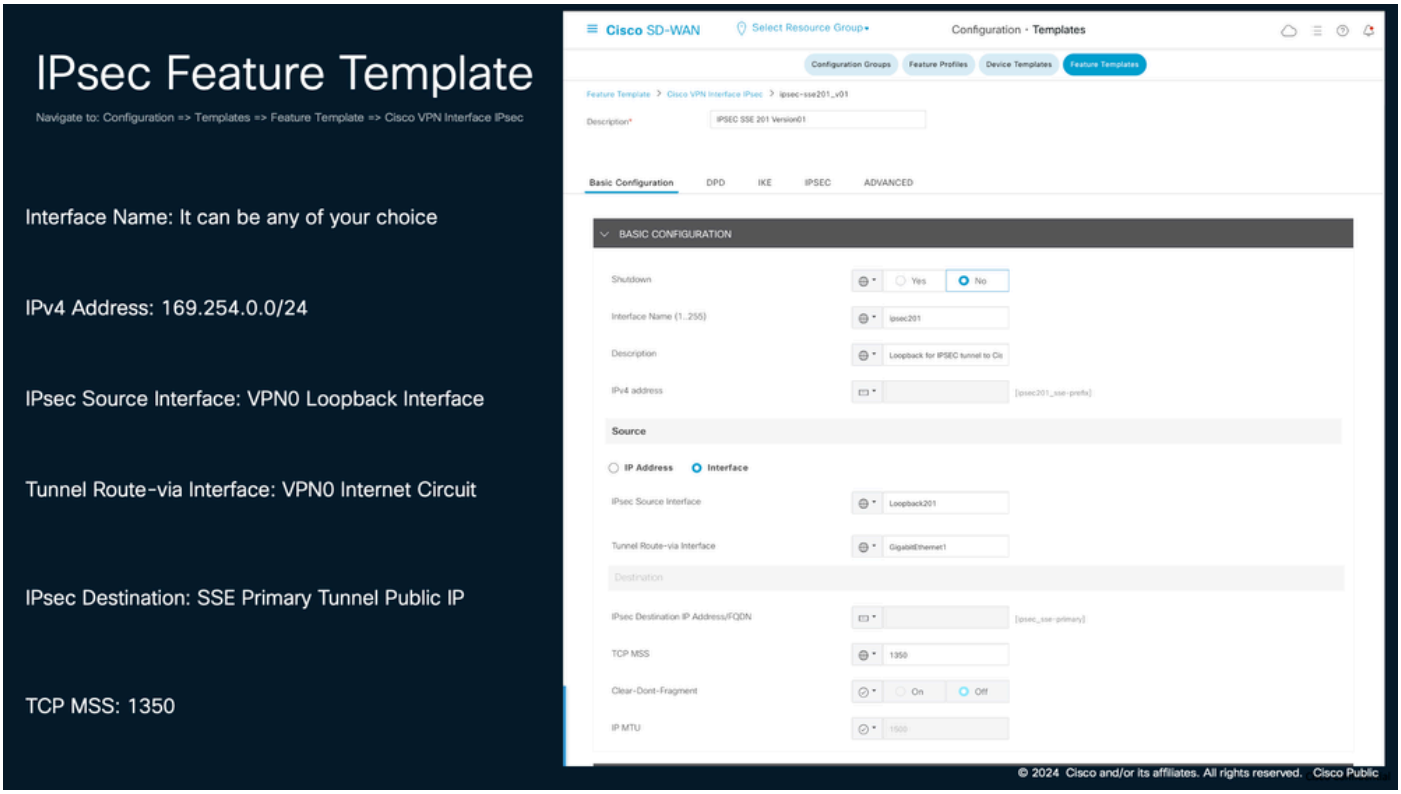
注意：对于部署所需的隧道数，重复此步骤。

有关隧道限制，请参阅官方文档：https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

这些步骤详细说明了将DC1-HE1（数据中心1前端1）连接到SSE弗吉尼亚主集线器的过程。此配置在数据中心中的SD-WAN路由器与位于弗吉尼亚入网点(POP)的思科安全接入网络隧道组(NTG)之间建立安全隧道

步骤 1：创建IPSec功能模板
创建IPSec功能模板以定义用于将SD-WAN头端路由器连接到NTG的IPSec隧道的参数。

图11:IPsec功能模板：基本配置



IPsec功能模板：基本配置

接口名称:它可以由您选择
IPv4地址：SSE根据您选择的子网划分要求监听169.254.0.0/24，最佳做法是使用/30。在本指南中，我们省略了第一个地址块供将来使用。

IPsec源接口：定义对于当前IPsec接口唯一的VPN0环回接口。为了保持一致性和进行故障排除，建议使用相同的编号。
通过接口的隧道路由：指向可用作连接到SSE的底层接口（必须能够访问Internet）

IPsec目标： 主集线器IP地址

请参阅图7：安全访问网络隧道组US(Virginia)这是35.171.214.188

TCP MSS:应设置为1350(参考：https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

示例：DC1-HE1指向SSE Virginia Primary Hub

接口名称:ipsec201

说明：通向思科的IPSEC隧道的环回

IPv4地址：169.254.0.x/30

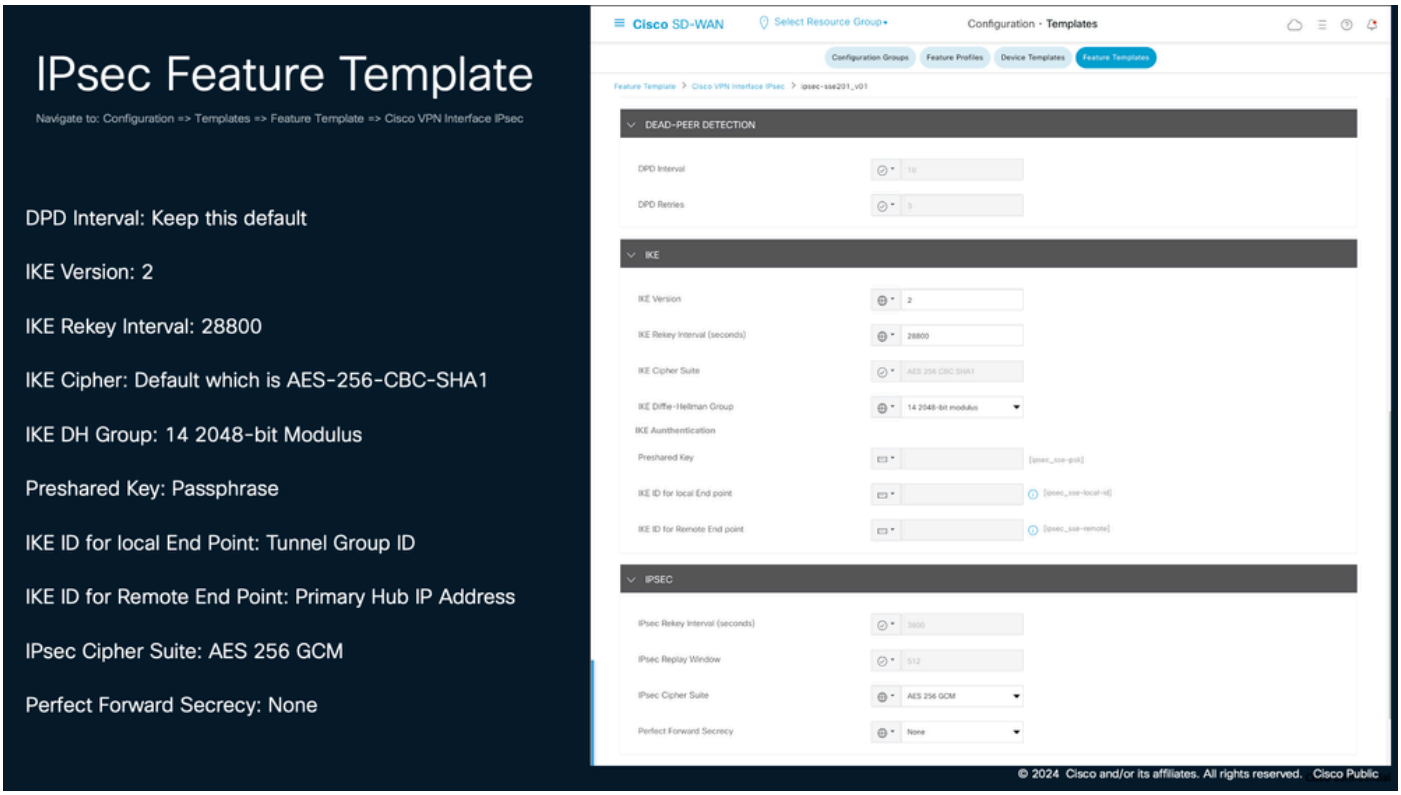
IPsec源接口：Loopback201

隧道路由通过接口：GigabitEthernet1

IPsec目标IP地址/FQDN:35.xxx.xxx.xxx

TCP MSS:1350

图12:IPsec功能模板：IKE IPSEC



IPsec功能模板：IKE IPSEC

DPD间隔：保留此默认值
IKE版本：2
IKE密钥更新间隔：28800
IKE密码：默认值为AES-256-CBC-SHA1
IKE DH组：14 2048位模数
Preshared Key：口令
本地终端的IKE ID:隧道组ID

请参阅图7：安全访问网络隧道组US(Virginia)此为mn03lab1+201@8167900-638880310-sse.cisco.com

注意：每个隧道必须具有唯一的终端；使用“+loopbackID”示例：mn03lab1+202@8167900-638880310-sse.cisco.com、mn03lab1+203@8167900-638880310-sse.cisco.com等。

远程终端的IKE ID:主集线器IP地址
IPsec密码套件：AES 256 GCM
Perfect Forward Secrecy：无

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

示例：

IKE版本：2
IKE密钥更新间隔：28800
IKE密码：AES-256-CBC-SHA1
IKE DH组：14 2048位模数
Preshared Key：*****

注意：Add a Network Tunnel Group中的步骤6

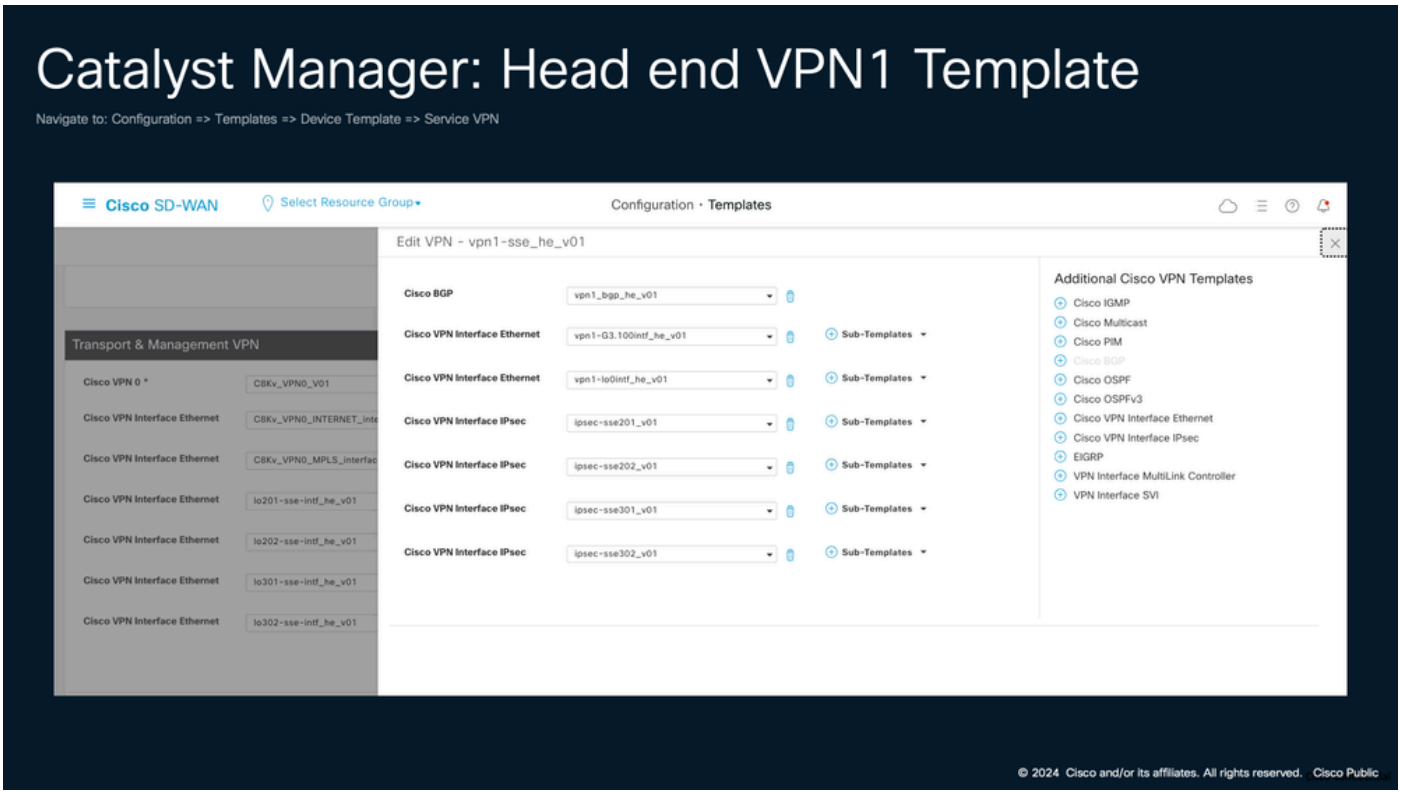
本地终端的IKE ID:mn03lab1@8167900-638880310-sse.cisco.com
远程终端的IKE ID:35.171.xxx.xxx
IPsec密码套件：AES 256 GCM
Perfect Forward Secrecy：无

重复上述步骤，为主要和辅助安全接入集线器配置所需的隧道。对于2x2设置，您将总共创建四个隧道：

- 从DC1-HE1到主要安全接入集线器的两个隧道
- 从DC1-HE1到辅助安全访问集线器的两个隧道

创建模板后，我们将在图13所示的服务端vrf上使用模板，并在图14所示的全局vrf上使用所定义的环回。

图13: Catalyst SD-WAN Manager:头端VPN1模板2x2



Catalyst管理器：头端VPN1模板

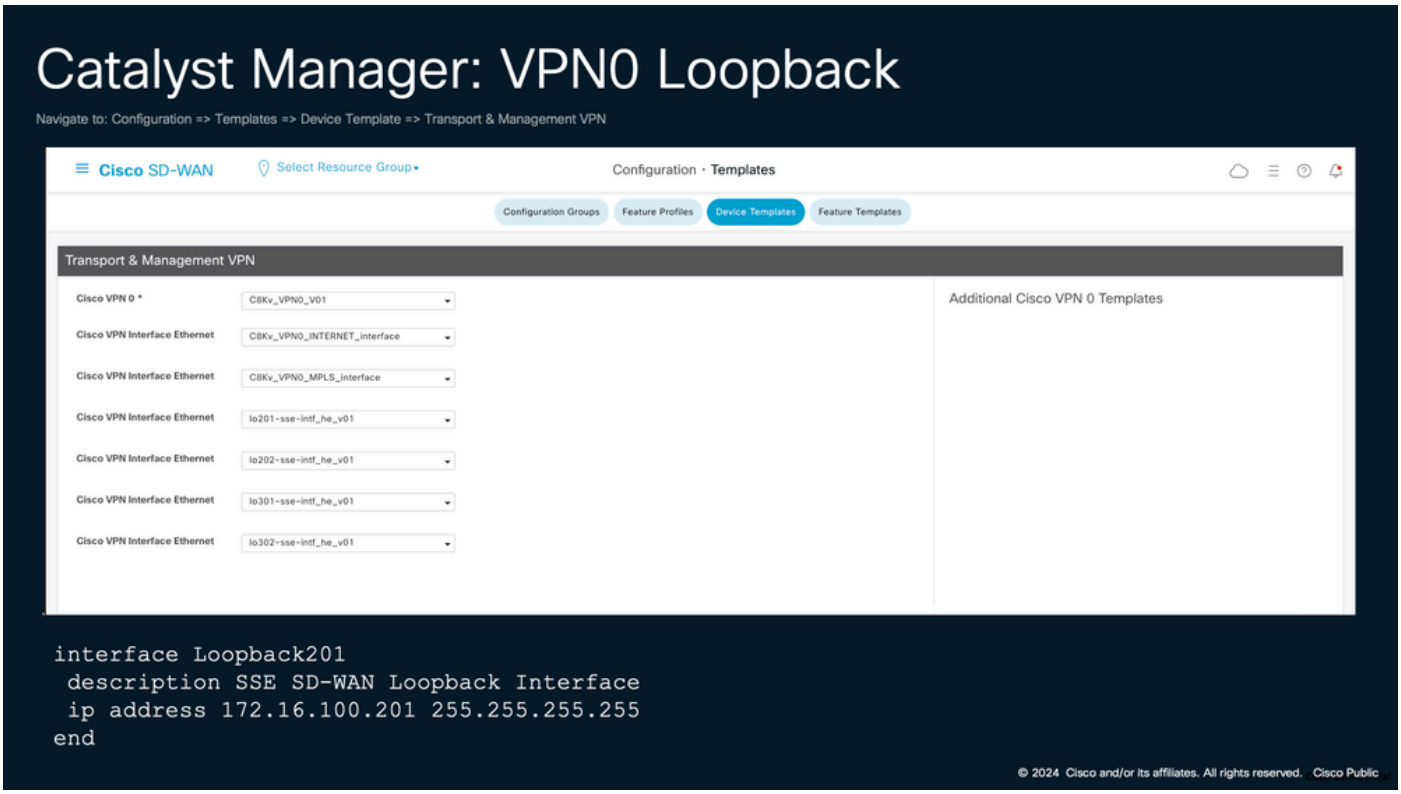
步骤 2：定义全局VRF中的环回

在全局VRF（虚拟路由和转发）表中配置环回接口。此环回用作第1步中创建的IPSec隧道的源接口。

步骤1中引用的所有环回必须在全局VRF中定义。

IP地址可在任何RFC1918范围内定义。

图14: Catalyst SD-WAN Manager:VPN0环回

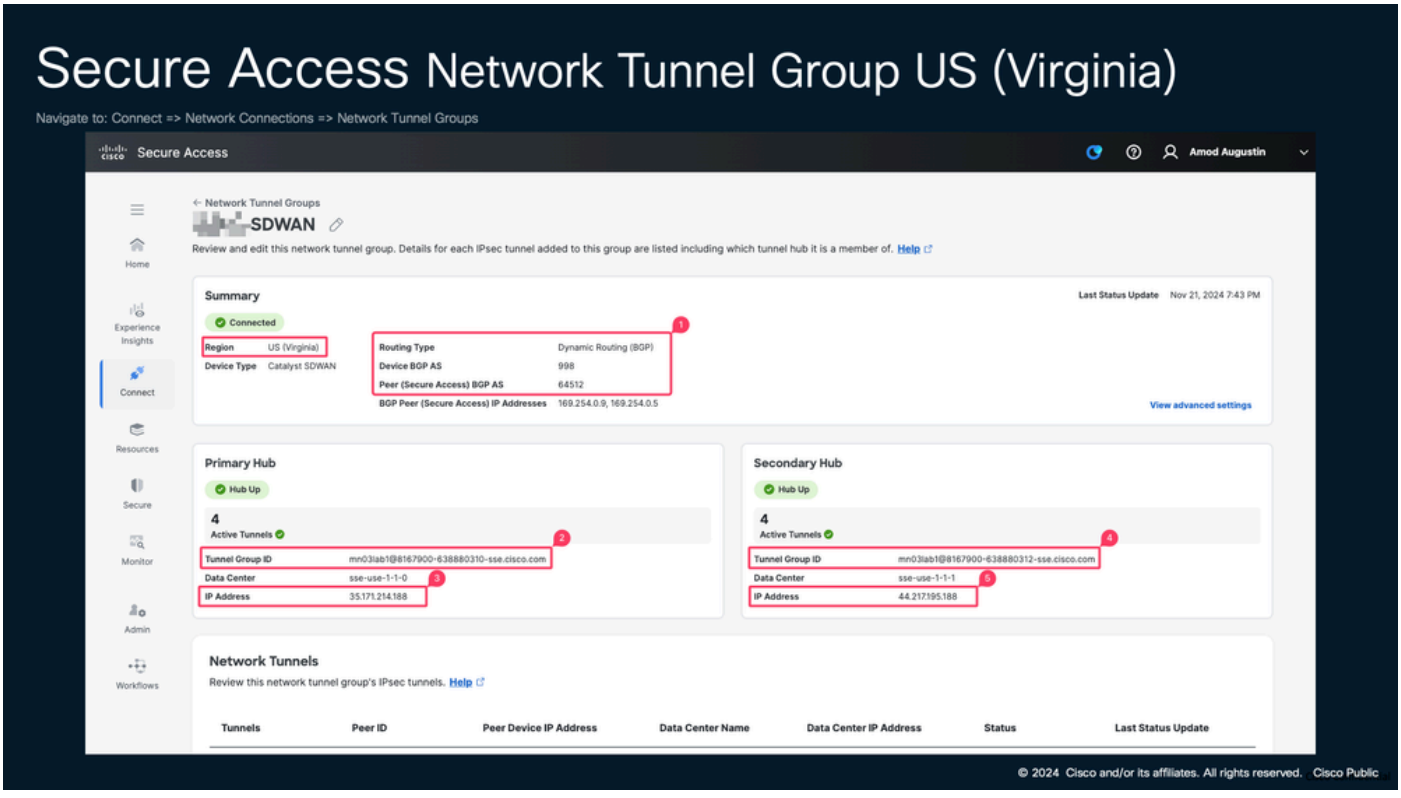


Catalyst管理器：VPN0环回

程序3.配置BGP邻居关系

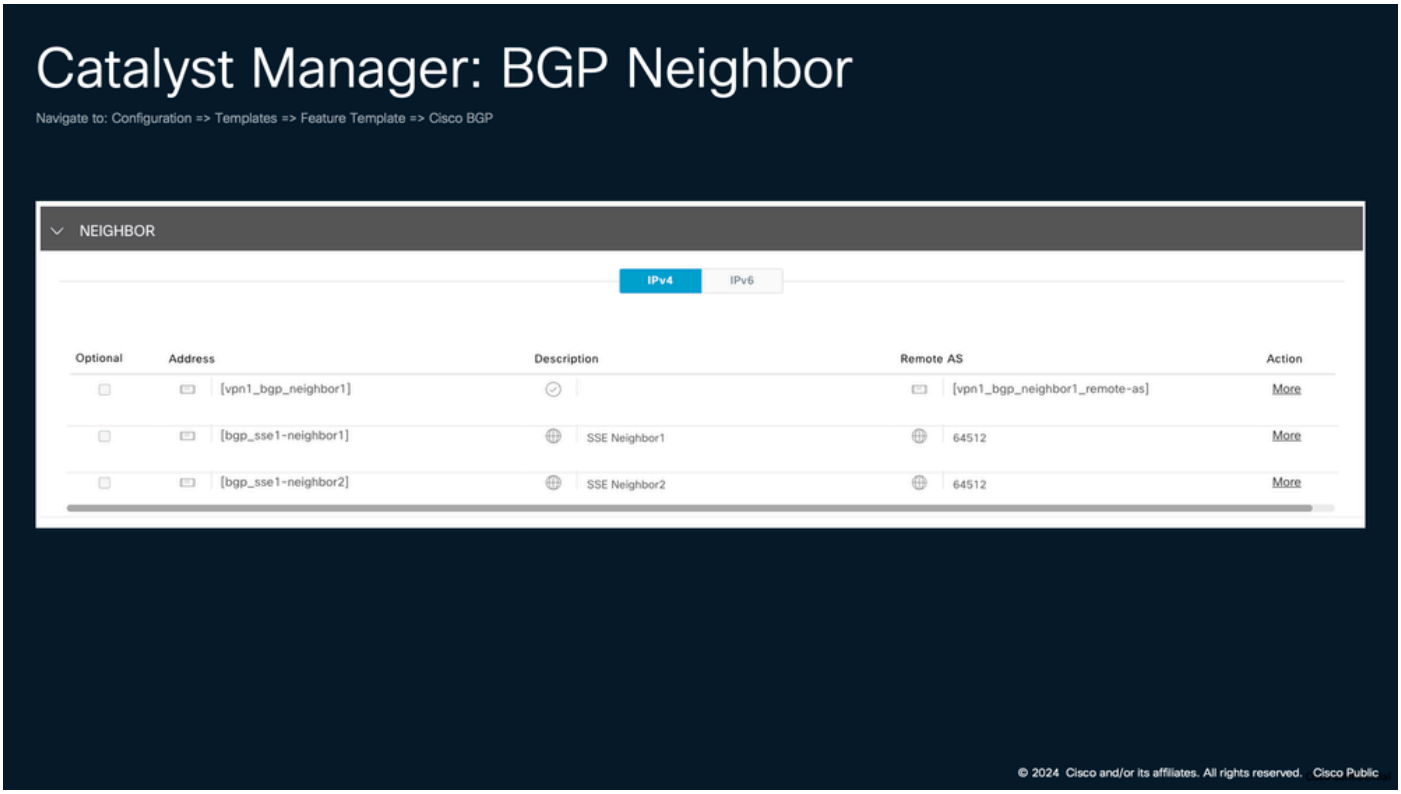
使用BGP功能模板为所有隧道接口定义BGP邻居关系。请参阅Cisco安全访问门户中相应的网络隧道组BGP配置以配置BGP值。

图 15：安全访问网络隧道组US（弗吉尼亚）



在本例中，我们使用图15中的信息（框1）定义使用功能模板的BGP。

图 16：Catalyst SD-WAN Manager BGP邻居



Catalyst SD-WAN Manager BGP邻居

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#
```

确认

```
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
```

参考

主用/主用实施具有来自与SD-WAN头端连接的核心交换机的多路径。

图 17：BGP邻居的主用/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邻居

由于ASPL预置（使用到邻居的路由映射完成），主用/备用实施将具有从核心交换机到SD-WAN头端的一条主用路径。

图 18：BGP邻居的主用/备用方案

```
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/备用BGP邻居

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。