提高Azure中Catalyst 8000V的吞吐量

目录

简介

本文档说明如何改进在Azure中部署的Cisco Catalyst 8000的性能。

Azure中的Catalyst 8000V吞吐量改进

借助适用于多云的Cisco Cloud OnRamp，用户可直接使用SD-WAN Manager（UI或API）在Azure中的NVA中部署Cisco Catalyst 8000V虚拟路由器。

通过Cloud OnRamp自动化，用户可以无缝创建和发现虚拟WAN、虚拟集线器并建立到Azure中虚拟网络的连接。

在Azure中部署Cisco Catalyst 8000Vs后，即可通过SD-WAN Manager监控和管理虚拟设备。

本文档从三个角度说明如何提高Azure性能：

- 安装HSEC许可证；
- Azure中TCP端口的12346量限制；
- 传输接口上的自动协商速度。

安装HSEC许可证

使用使用策略的智能许可且必须支持250 Mbps或更高的加密流量吞吐量的设备需要HSEC许可证。

这是美国出口管制法规的一项要求。您可以使用Cisco SD-WAN Manager安装HSEC许可证。

思科SD-WAN管理器与思科智能软件管理器(SSM)联系，后者提供智能许可证授权码(SLAC)以加载到设备。

在设备上加载SLAC将启用HSEC许可证。

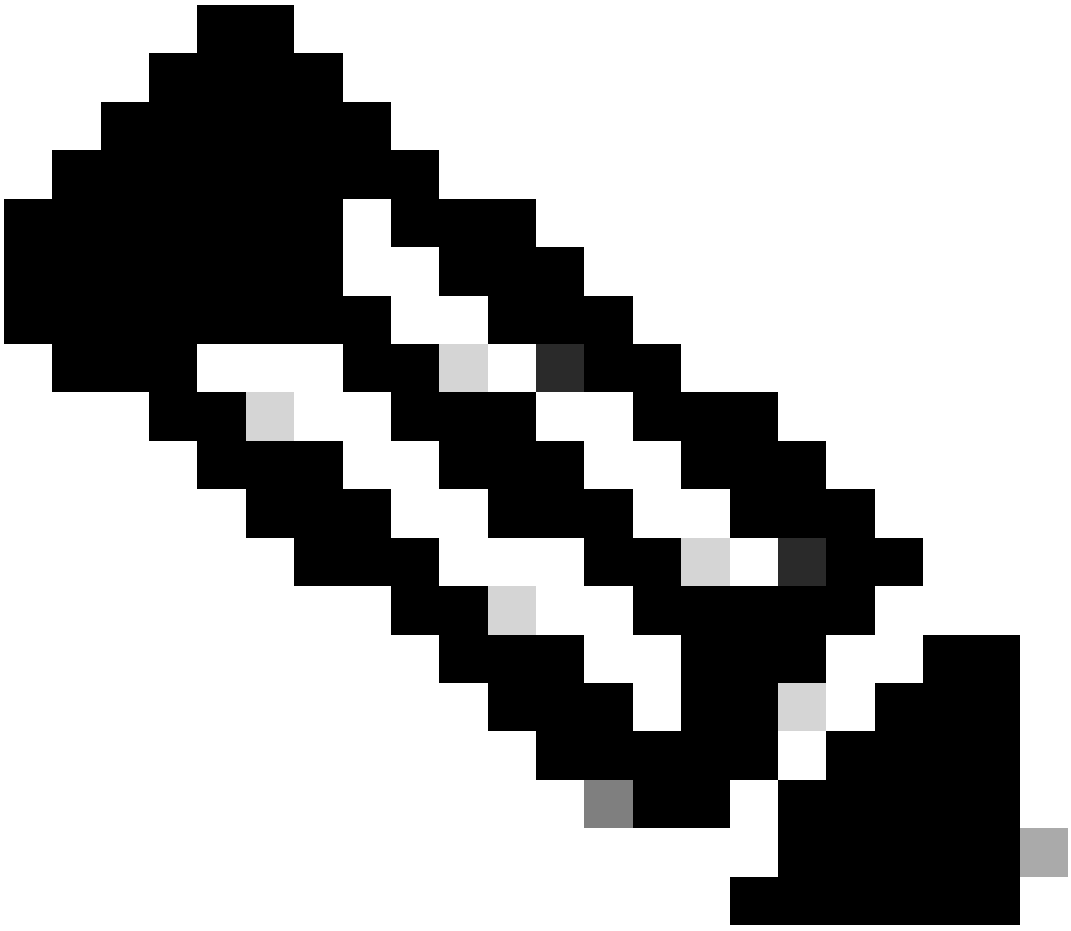
有关安装和管理许可证的详细信息，请参阅在Cisco Catalyst SD-WAN中管理HSEC许可证。

Azure中TCP端口的12346量限制

目前，该自动化可将C8000V部署为一个传输接口(GigabitEtherent1)和一个服务接口(GigabitEtherent2)。

由于Azure对SD-WAN端口TCP 12346的入站限制，当流量进入Azure基础设施时，吞吐量可以基于每个传输接口进行限制。

200K PPS的入站限制由Azure基础设施强制实施，因此用户每个C8000V NVA实例不能超过~1Gbps(示例假设：数据包大小为600B，计算：600B * 8 = 4800位；4800b * 200Kpps = 960 Mbps)。

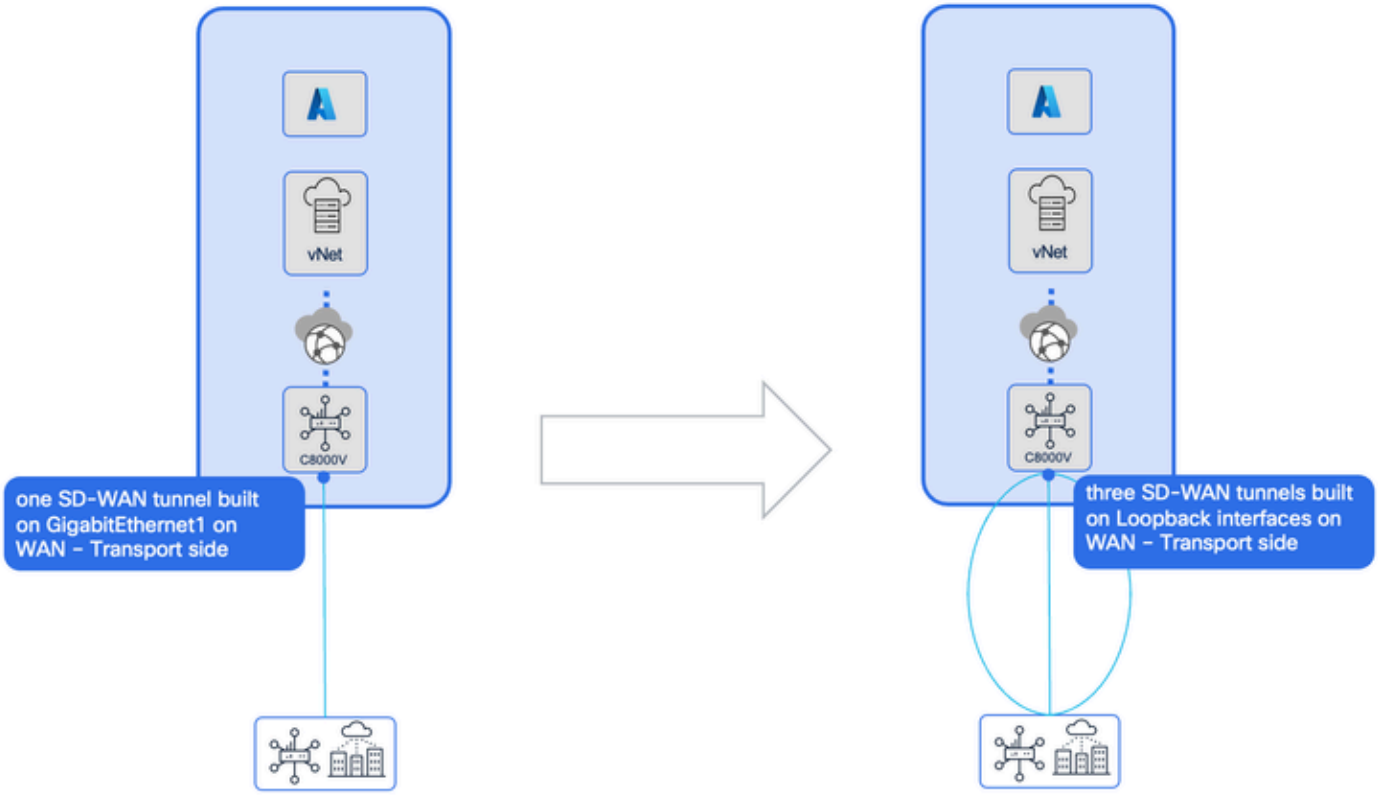


> 注意：Azure可以将入站限制增加到每个案例（票证）的400K PPS。客户需要直接联系Azure并请求增加。

为了克服这一限制，思科与Azure合作，允许SD-WAN分支机构为每个NVA实例构建多个SD-WAN隧道。

要进行此配置更改，管理员必须执行以下步骤:

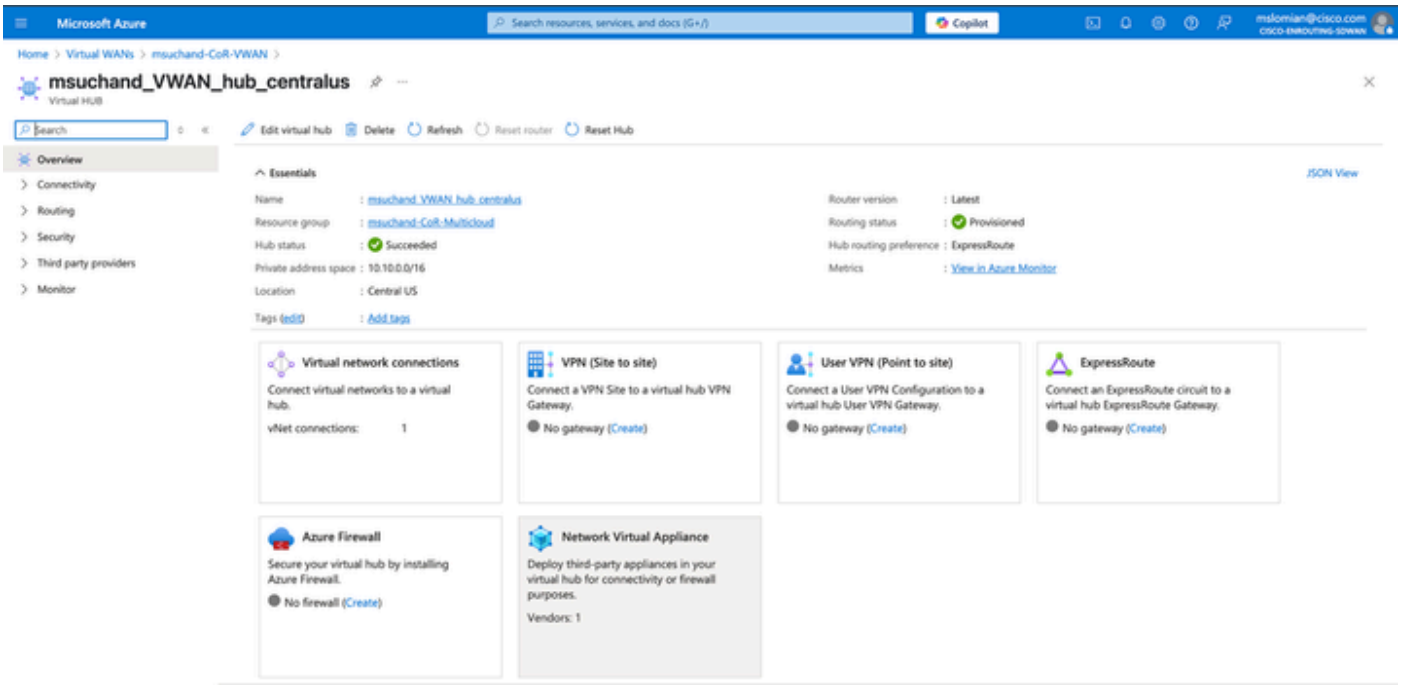
1. 在SD-WAN Manager中，使用Cloud OnRamp自动化在Azure中部署带C8000V的云网关。
2. 在Azure门户中，更改虚拟中心中NVA的IP设置。
3. 在SD-WAN Manager中，使用云门户中的设置创建和推送新的配置组。



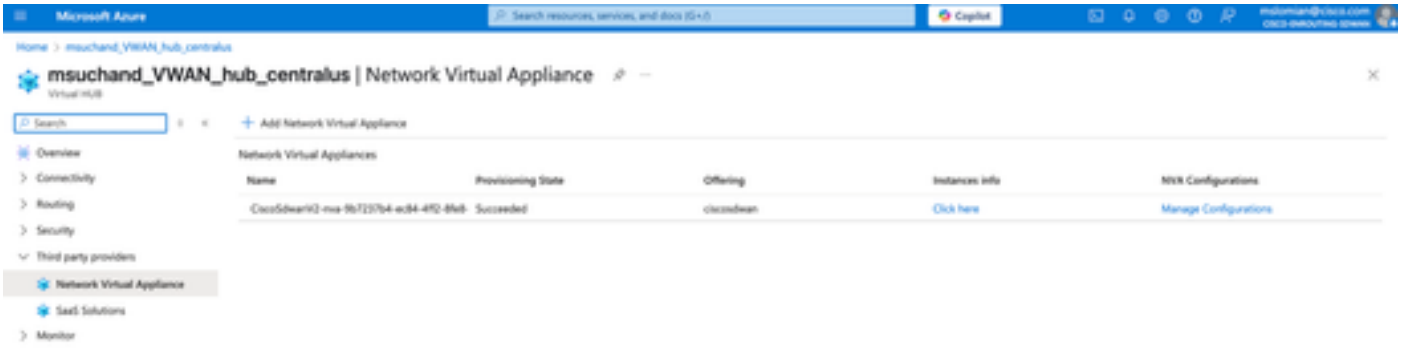
步骤 1：

使用此Youtube频道或发行说明中提供的操作步骤，在Azure中部署Cisco Catalyst 8000V。

步骤 2：
要更改IP设置，请在虚拟中心导航到Azure porta > Virtual WANs > selected virtual WAN > virtual hub > NVA。



在NVA的虚拟中心视图中，导航到第三方提供商>管理配置。



在NVA配置中，导航到接口IP配置和添加配置。分配IP地址最多可能需要30分钟，

步骤 3：

分配地址后，记下这些地址并转至SD-WAN Manager。所有C8000V都需要此配置更新。

它可以通过CLI插件完成（它会附加模板/配置文件中的任何内容）。 请参阅以下示例配置：

```
interface Loopback 1000
```

```
    ip address 10.0.0.244 255.255.255.255
    no shut
exit
interface Loopback 2000
    ip address 10.0.0.246 255.255.255.255
    no shut
exit
interface Loopback 3000
    ip address 10.0.0.247 255.255.255.255
    no shut
exit
interface GigabitEthernet1
    speed 10000
    no ip dhcp client default-router distance 1
    no ip address dhcp client-id GigabitEthernet1
    ip unnumbered Loopback1000
exit
interface GigabitEthernet2
    speed 10000
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.241 → 10.0.0.241 IP is Loopback 1000 IP -3
ip route 10.0.0.241 255.255.255.255 GigabitEthernet1 → 10.0.0.241 IP is Loopback 1000 IP -3
interface Tunnel1
    no shutdown
    ip unnumbered Loopback1000
    ipv6 unnumbered Loopback1000
    tunnel source Loopback1000
    tunnel mode sdwan
interface Tunnel2
    no shutdown
    ip unnumbered Loopback2000
    ipv6 unnumbered Loopback2000
    tunnel source Loopback2000
    tunnel mode sdwan
interface Tunnel3
    no shutdown
    ip unnumbered Loopback3000
    ipv6 unnumbered Loopback3000
    tunnel source Loopback3000
    tunnel mode sdwan
sdwan
 interface Loopback1000
   tunnel-interface
    encapsulation ipsec weight 1
    no border
    color biz-internet
    no last-resort-circuit
    no low-bandwidth-link
    no vbond-as-stun-server
    vmanage-connection-preference 5
    port-hop
    carrier                       default
    nat-refresh-interval          5
    hello-interval                1000
    hello-tolerance               12
    no allow-service all
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    allow-service sshd
    no allow-service netconf
```

```
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
 exit
exit
interface Loopback2000
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 4
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
 exit
exit
interface Loopback3000
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color custom1
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 3
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
```

```
    no allow-service snmp
    no allow-service bfd
  exit
 exit
 interface GigabitEthernet1
  no tunnel-interface
  exit
 exit
```

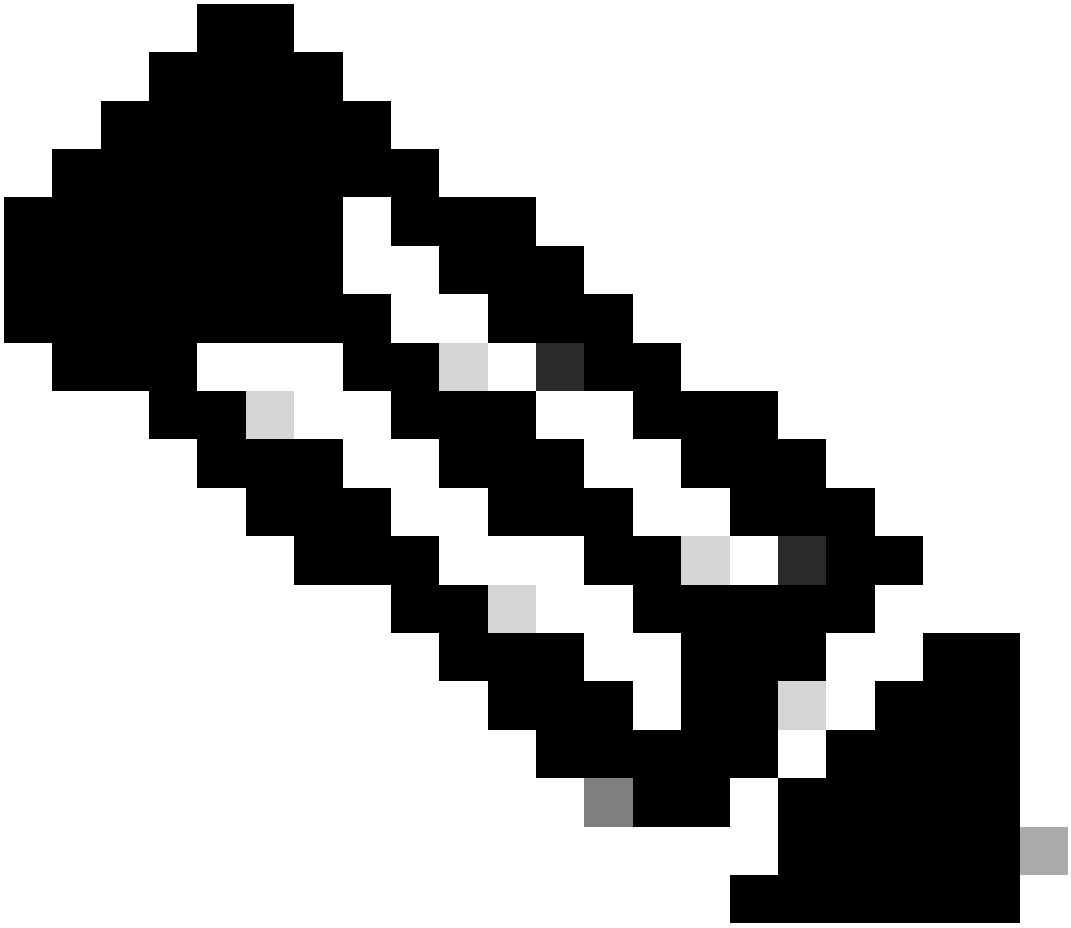
传输接口上的自动协商速度

在默认模板或自动生成的配置组(GigabitEthernet1)中使用的Cisco Catalyst 8000V上的Cisco传输接口配置为negotiate auto以确保已建立连接。

为了获得更好的性能（高于1Gb），建议将接口速度设置为10Gb。这也适用于服务接口(GigabitEthernet2)。 要验证协商的速度，请运行以下命令：

```
azure-central-us-1#sh int gi1
GigabitEthernet1 is up, line protocol is up
  Hardware is vNIC, address is 000d.3a92.e2ff (bia 000d.3a92.e2ff)
  Internet address is 10.48.0.244/28
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,

…
azure-central-us-1#sh int gi2
GigabitEthernet2 is up, line protocol is up
  Hardware is vNIC, address is 000d.3a92.ea8a (bia 000d.3a92.ea8a)
  Internet address is 10.48.0.229/28
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
```



注意：虽然本文重点介绍在Azure中通过Cloud OnRamp自动化(NVA)部署C8000V，但自动协商速度也适用于VNet、AWS和Google部署中的Azure部署。

要更改此设置，请在模板(Confusation > Templates > Feature Template > Cisco VPN Interface Ethernet)/配置组中进行更改(请参阅指南)。 或者，如果设备由CLI管理，管理员可以在CLI中编辑此项。

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）。