Mejore el rendimiento de Catalyst 8000V en Azure

Contenido

Introducción

Este documento explica cómo mejorar el rendimiento de Cisco Catalyst 8000V implementado en Azure.

Mejora del rendimiento de Catalyst 8000V en Azure

Con Cisco Cloud OnRamp para varias nubes, los usuarios pueden implementar routers virtuales Cisco Catalyst 8000V en NVA en Azure directamente con SD-WAN Manager (UI o API).

La automatización de Cloud OnRamp permite a los usuarios crear y descubrir sin problemas WAN virtuales, hubs virtuales y crear conexiones a redes virtuales en Azure.

Una vez que Cisco Catalyst 8000V se implementa en Azure, los appliances virtuales se pueden supervisar y administrar desde el Administrador de SD-WAN.

Este documento explica cómo mejorar el rendimiento en Azure desde tres perspectivas:

- instalación de la licencia HSEC;
- limitaciones de rendimiento en el puerto TCP 12346 en Azure;
- velocidad negociada automáticamente en la interfaz de transporte.

Instalación de la licencia HSEC

Los dispositivos que utilizan licencias inteligentes mediante políticas y que deben admitir un rendimiento de tráfico cifrado de 250 Mbps o superior requieren una licencia HSEC.

Este es un requisito de la regulación de control de exportaciones de Estados Unidos. Puede utilizar Cisco SD-WAN Manager para instalar licencias HSEC.

Cisco SD-WAN Manager se pone en contacto con Cisco Smart Software Manager (SSM), que proporciona un código de autorización de licencia inteligente (SLAC) para cargar en un

dispositivo.

La carga del SLAC en un dispositivo habilita una licencia HSEC.

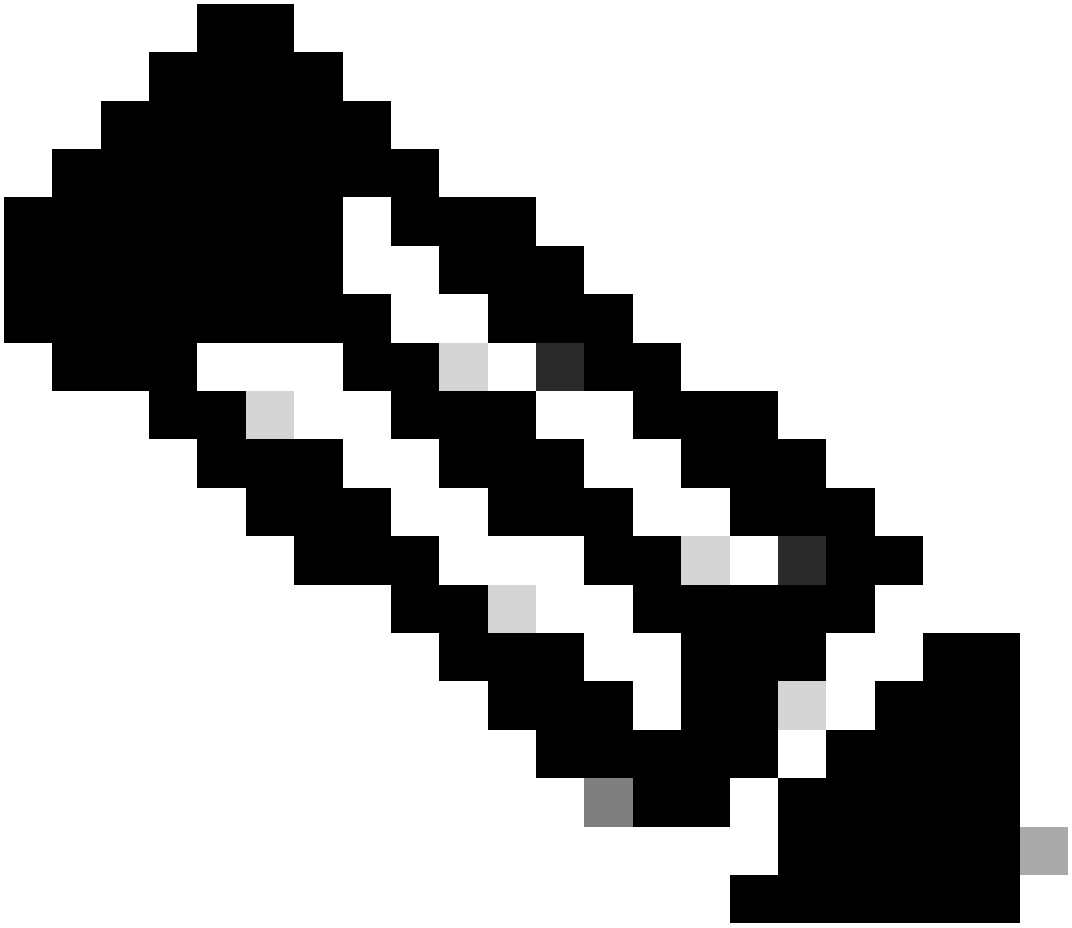
Refiérase a Administración de Licencias HSEC en Cisco Catalyst SD-WAN para obtener detalles sobre la instalación y administración de las licencias.

Limitaciones de rendimiento en el puerto TCP 12346 en Azure

Actualmente, la automatización implementa C8000V con una interfaz de transporte (GigabitEthernet1) y una interfaz de servicio (GigabitEthernet2).

Debido a las limitaciones de entrada de Azure en el puerto SD-WAN TCP 12346, el rendimiento se puede limitar por interfaz de transporte a medida que el tráfico entra en la infraestructura de Azure.

La infraestructura de Azure impone el límite de 200 000 PPS entrantes, por lo que los usuarios no pueden alcanzar más de ~1 Gbps por instancia de NVA de C8000V (una suposición de ejemplo: un tamaño de paquete de 600B, cálculo: 600 B * 8 = 4800 bits; 4800b * 200 Kpps = 960 Mbps).

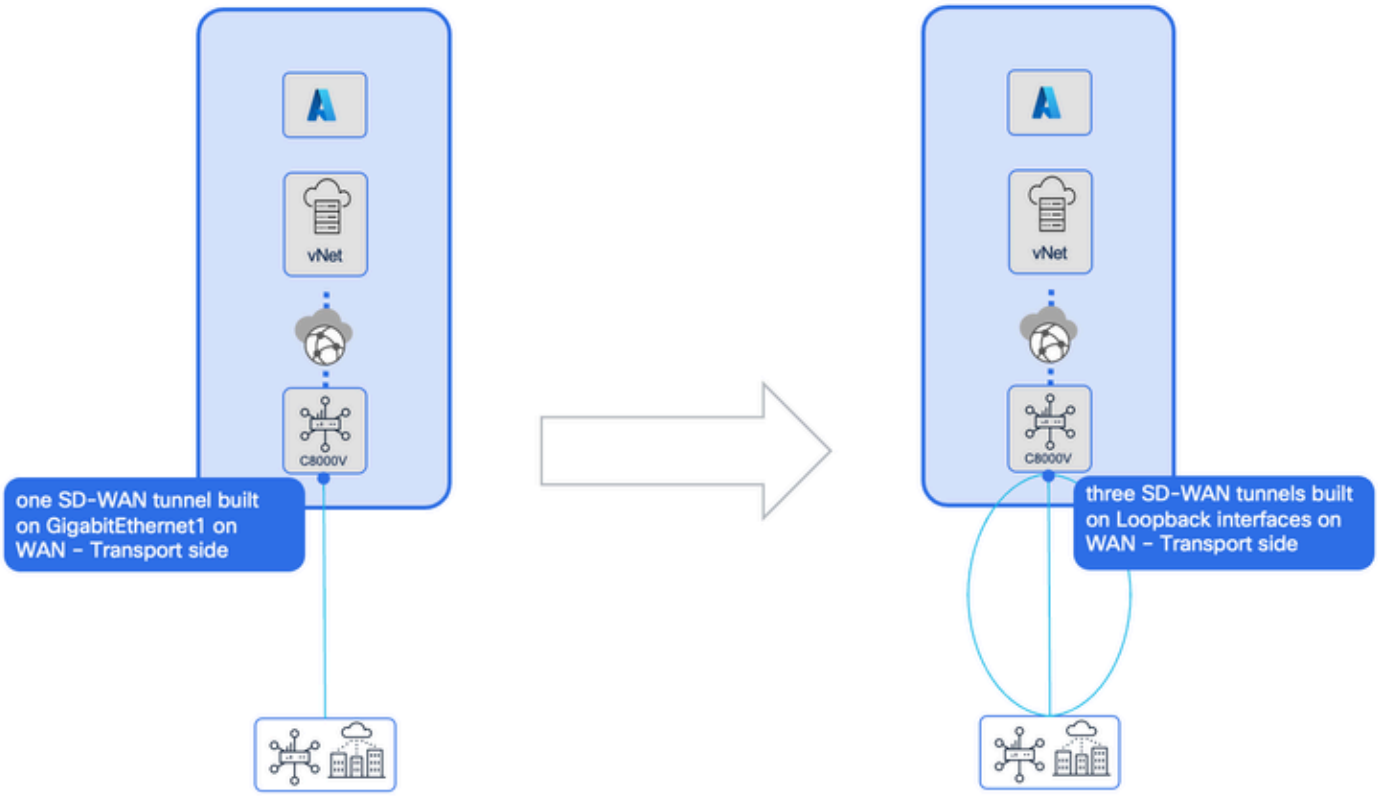


Nota: Azure puede aumentar el límite de entrada a 400 000 PPS por caso (ticket). Los clientes deben ponerse en contacto con Azure directamente y solicitar el aumento.

Para superar esta limitación, Cisco colaboró con Azure para permitir que las sucursales de SD-WAN construyeran varios túneles de SD-WAN para cada instancia de NVA.

Para realizar este cambio de configuración, el administrador debe seguir estos pasos:

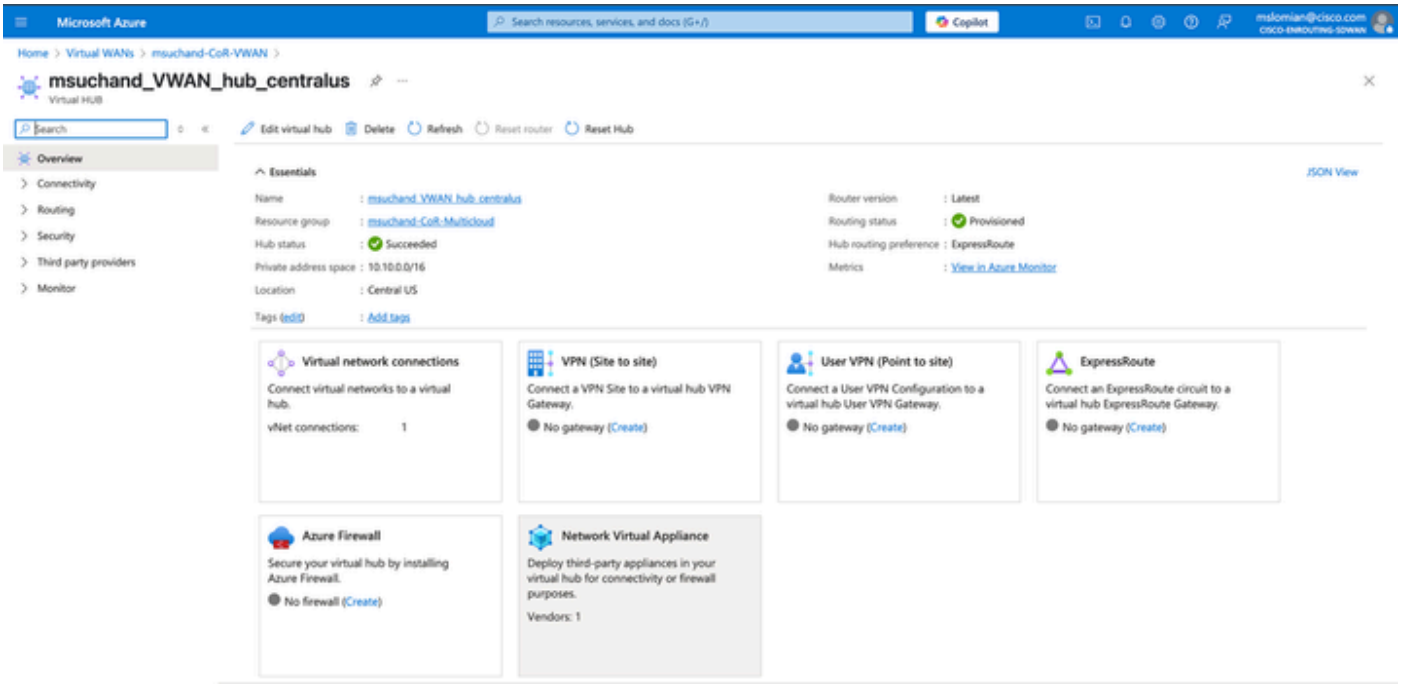
1. En SD-WAN Manager, implemente el gateway de la nube con C8000V en Azure mediante la automatización de Cloud OnRamp.
2. En el portal de Azure, cambie la configuración de IP para NVA en el hub virtual.
3. En el Administrador de SD-WAN, cree e inserte un nuevo grupo de configuración utilizando la configuración del portal de la nube.



Paso 1:

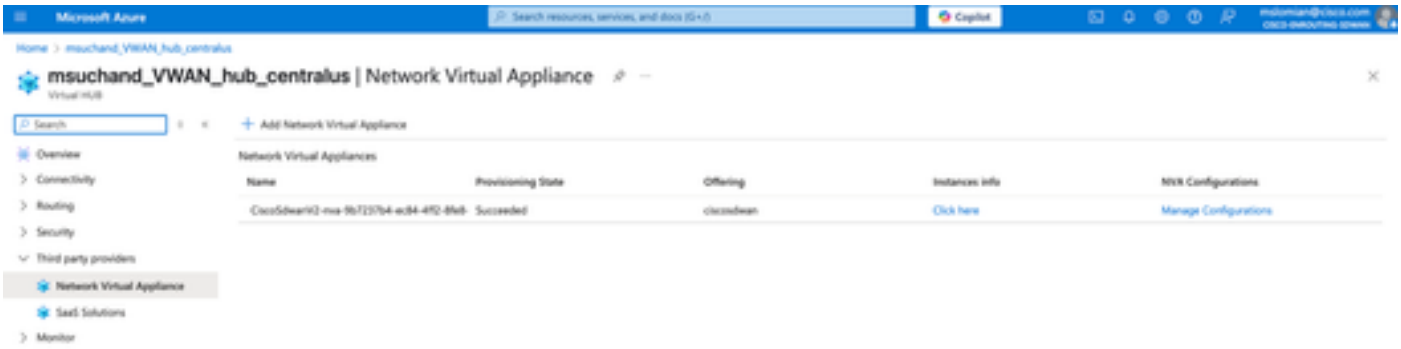
Implemente Cisco Catalyst 8000V en Azure con el procedimiento que se encuentra aquí en este canal de Youtube o en las Notas de la versión.

Paso 2:
Para cambiar la configuración de IP, navegue hasta Azure Portal > Virtual WAN > WAN virtual seleccionada > Virtual Hub > NVA en Virtual Hub.



En la vista del hub virtual en NVA, navegue hasta Proveedores externos > Administrar

configuraciones.



En la configuración de NVA, navegue hasta Interface IP Configurations y Add Configurations. La asignación de direcciones IP puede tardar hasta 30 minutos.

Paso 3:

Una vez que se asignan las direcciones, tome nota de ellas y vaya al Administrador de SD-WAN. Todos los C8000V necesitan esta actualización de configuración.

Se puede hacer mediante el complemento de CLI (se añade lo que haya en las plantillas / perfiles de configuración). Consulte este ejemplo de configuración:

```
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
```

Velocidad negociada automáticamente en la interfaz de transporte

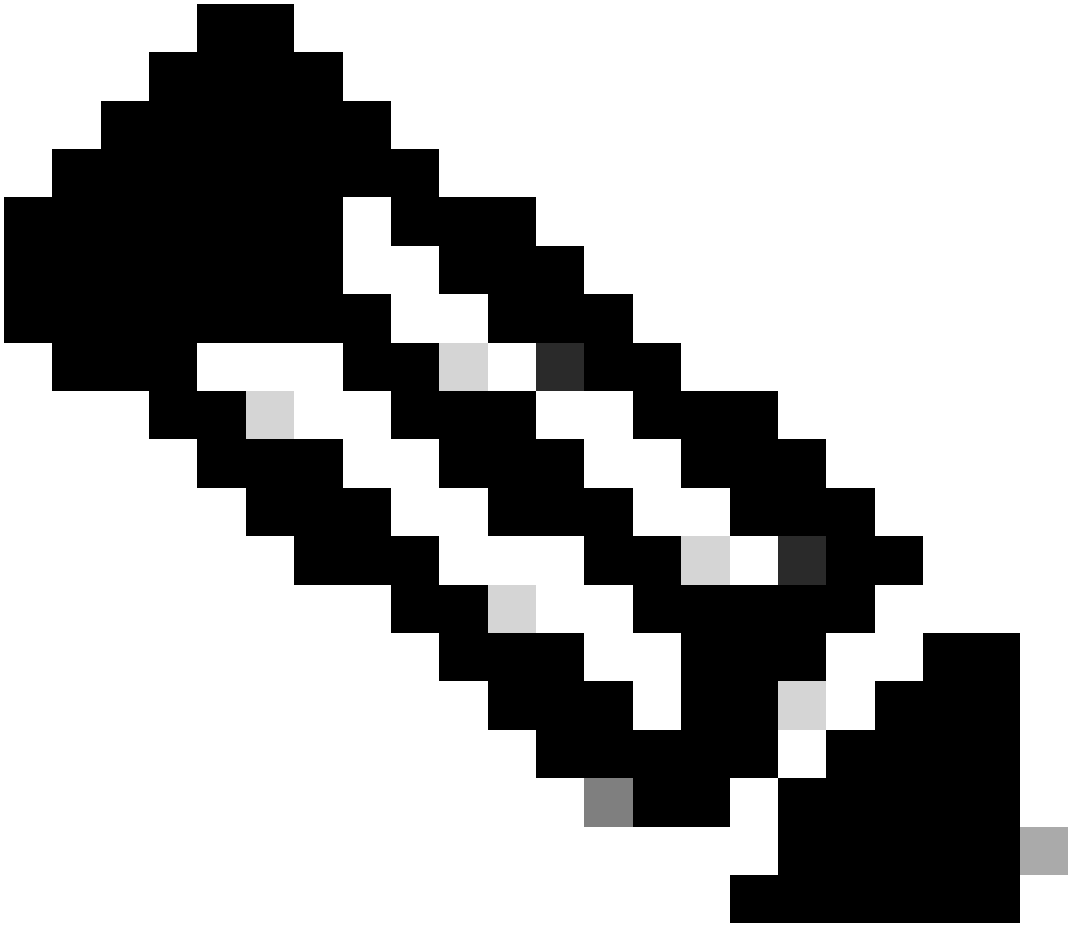
La interfaz de transporte de Cisco en Cisco Catalyst 8000V, que se utiliza en plantillas predeterminadas o grupos de configuración generados automáticamente (GigabitEthernet1), se

configura con negotiate auto para garantizar que se establece la conexión.

Para obtener un mejor rendimiento (por encima de 1 Gb), se recomienda establecer la velocidad en las interfaces en 10 Gb. Esto también se aplica a la interfaz de servicio (GigabitEthernet2). Para verificar la velocidad negociada, ejecute estos comandos:

```
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,
```



Nota: Aunque este artículo se centra en la implementación de C8000V en Azure con la automatización de Cloud OnRamp (NVA), la velocidad negociada automáticamente también se aplica a las implementaciones de Azure en VNets, AWS y Google.

Para cambiar esto, realice cambios en la plantilla (Configuration > Templates > Feature Template > Cisco VPN Interface Ethernet) / grupo de configuración (vea la guía). De forma alternativa, los administradores pueden editar esta información en CLI, si el dispositivo está administrado por CLI.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).