Verbeterde doorvoer op Catalyst 8000V in Azure

Inhoud

Inleiding

In dit document wordt uitgelegd hoe u de prestaties kunt verbeteren van Cisco Catalyst 8000Vs die in Azure is geïmplementeerd.

Catalyst 8000V doorvoerverbetering in Azure

Met Cisco Cloud OnRamp voor Multicloud kunnen gebruikers Cisco Catalyst 8000V virtuele routers direct in NVA in Azure implementeren met SD-WAN Manager (UI of API).

Cloud OnRamp-automatisering stelt gebruikers in staat om naadloos virtueel WAN, virtuele hubs en verbindingen met virtuele netwerken in Azure te maken en te ontdekken.

Zodra Cisco Catalyst 8000V's in Azure zijn geïmplementeerd, kunnen de virtuele apparaten worden bewaakt en beheerd vanuit SD-WAN Manager.

In dit document wordt uitgelegd hoe u de prestaties in Azure kunt verbeteren vanuit drie invalshoeken:

- installatie van een HSEC-licentie;
- doorvoerbeperkingen op de TCP 12346-poort in Azure;
- automatisch overeengekomen snelheid op de transportinterface.

Installatie van HSEC-licentie

Voor apparaten die gebruikmaken van Smart Licensing Using Policy en die een gecodeerde doorvoer van 250 Mbps of meer moeten ondersteunen, is een HSEC-licentie vereist.

Dit is een vereiste van de Amerikaanse exportcontroleregeling. U kunt Cisco SD-WAN Manager gebruiken om HSEC-licenties te installeren.

Cisco SD-WAN Manager neemt contact op met Cisco Smart Software Manager (SSM), die een Smart License Authorization Code (SLAC) biedt om op een apparaat te laden.

Als u de SLAC op een apparaat laadt, wordt een HSEC-licentie ingeschakeld.

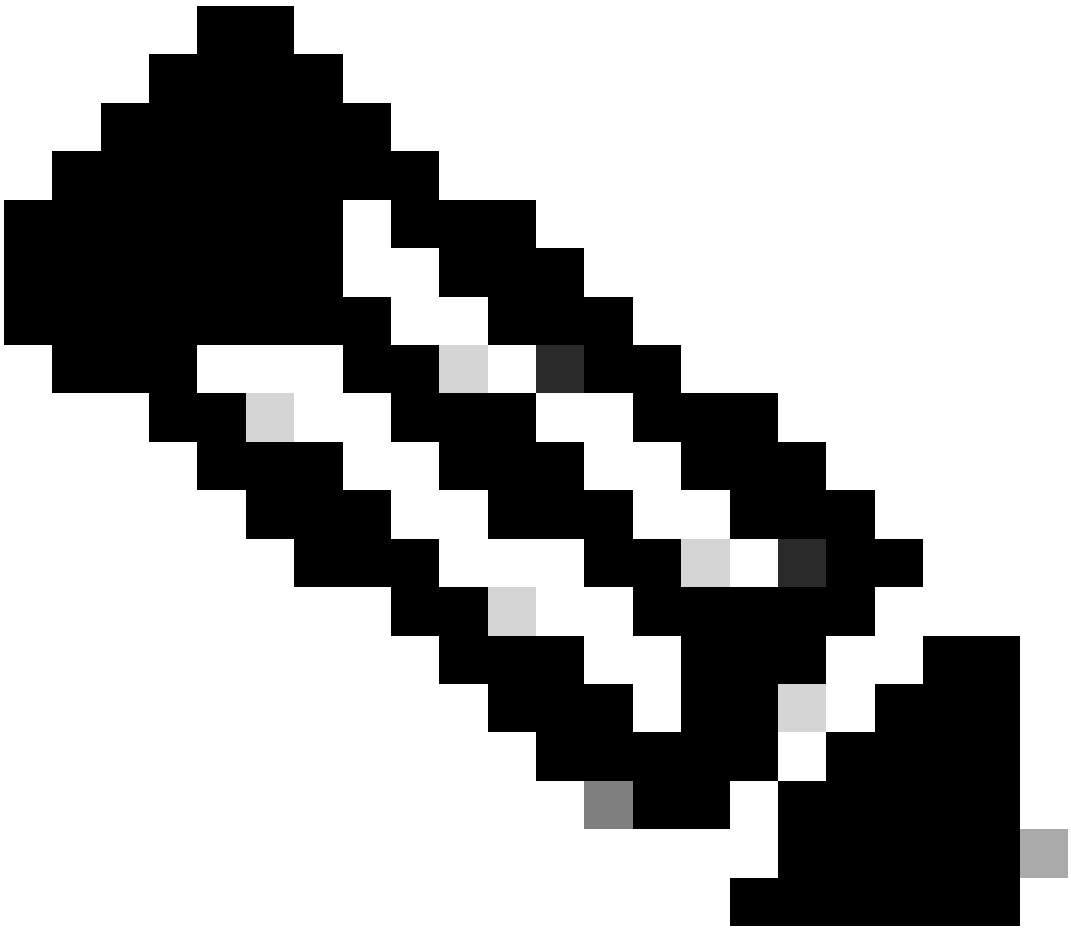
Raadpleeg HSEC-licenties beheren in Cisco Catalyst SD-WAN voor meer informatie over het installeren en beheren van de licenties.

Doorvoerbeperkingen op TCP 12346-poort in Azure

Momenteel implementeert de automatisering C8000V met één transportinterface (GigabitEthernet1) en één serviceinterface (GigabitEthernet2).

Als gevolg van Azure inbound beperkingen op SD-WAN poort TCP 12346, kan de doorvoer worden beperkt op per-transport interface basis als het verkeer komt Azure infrastructuur.

De inkomende limiet van 200K PPS wordt afgedwongen door Azure-infrastructuur en gebruikers kunnen dus niet meer dan ~1Gbps per C8000V NVA-instantie bereiken (een voorbeeld: een pakketgrootte van 600B, berekening: 600B * 8 = 4800bits; 4800b * 200Kpps = 960 Mbps).



Opmerking: Azure kan de inkomende limiet verhogen tot 400K PPS per geval (ticket) basis. Klanten moeten rechtstreeks contact opnemen met Azure en de verhoging

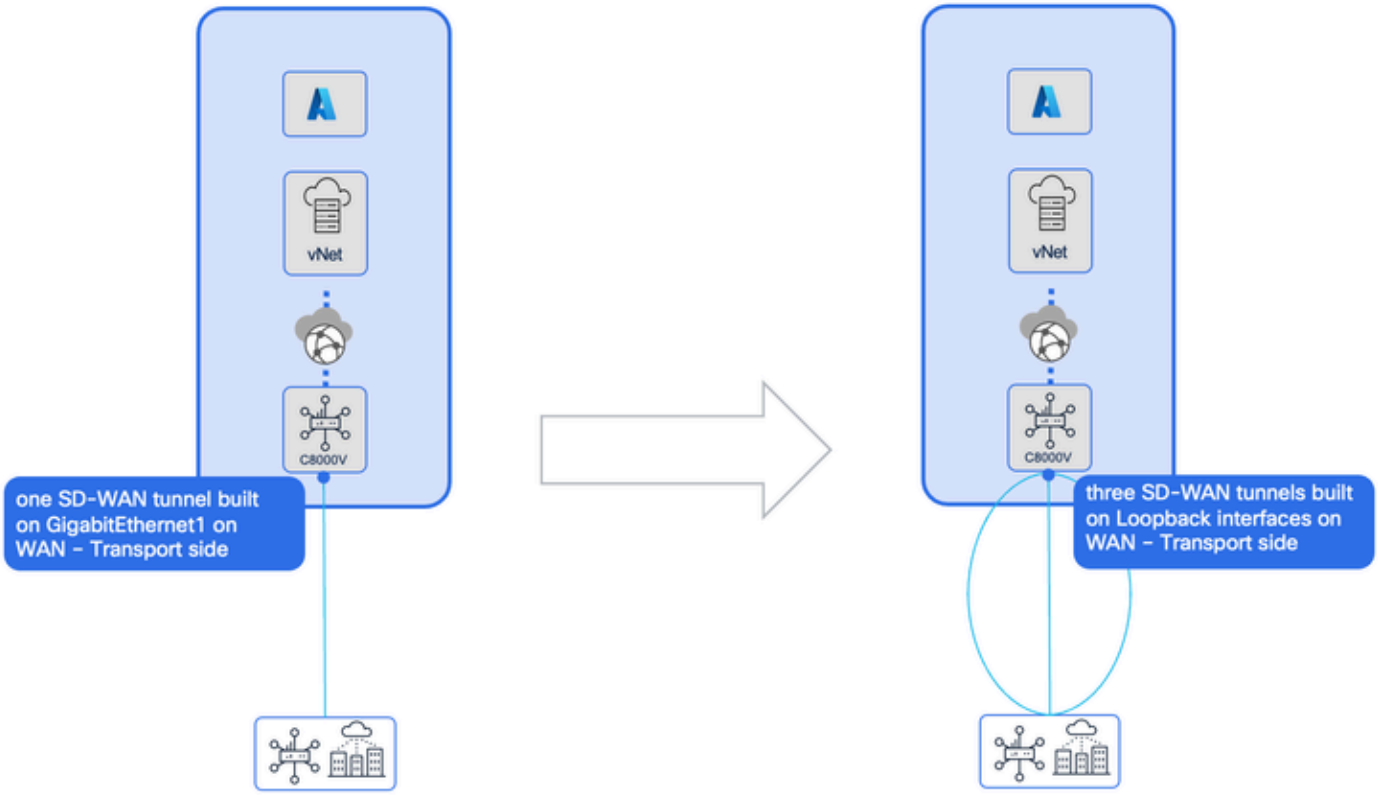
---

aanvragen.

Om deze beperking te overwinnen, werkte Cisco samen met Azure om SD-WAN-takken in staat te stellen meerdere SD-WAN-tunnels voor elke NVA-instantie te bouwen.

Als u deze configuratie wilt wijzigen, moet de beheerder deze stappen volgen:

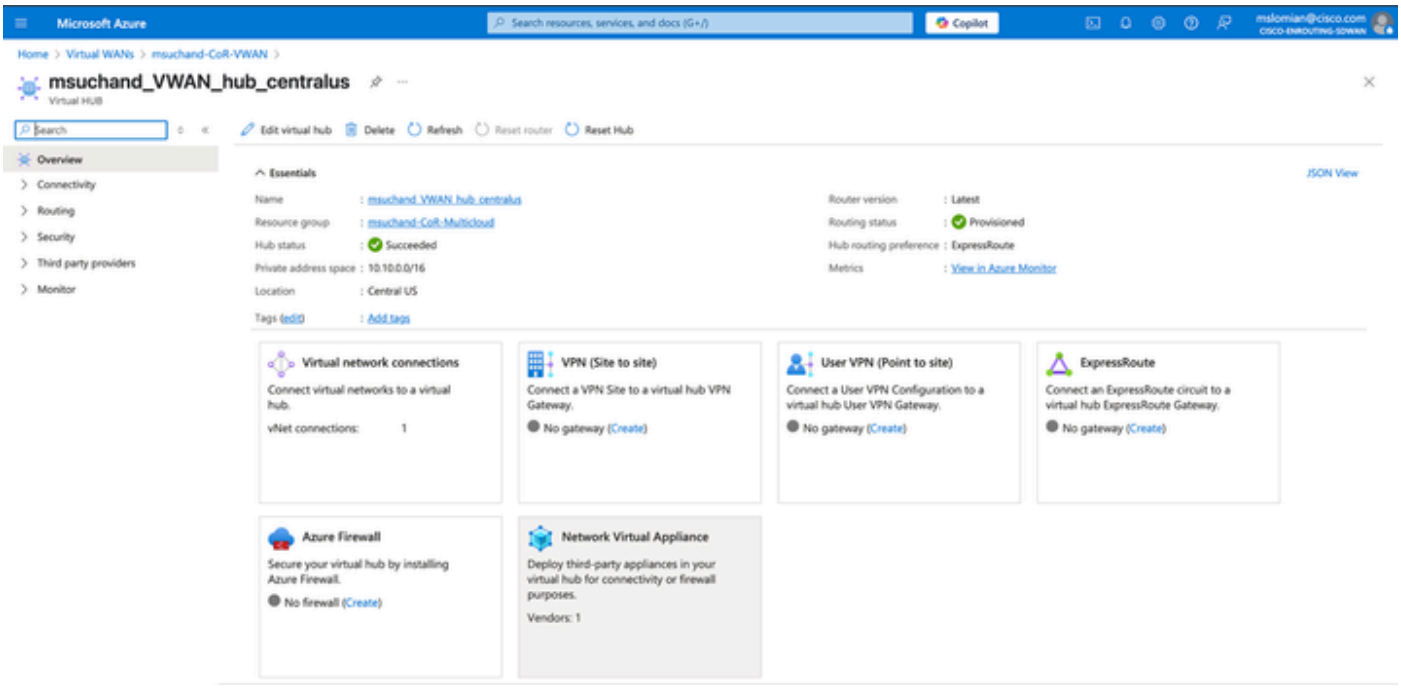
1. Implementeer in SD-WAN Manager de cloudgateway met C8000V in Azure met behulp van Cloud OnRamp-automatisering.
2. Wijzig in Azure-portal de IP-instellingen voor NVA in de virtuele hub.
3. In SD-WAN Manager kunt u een nieuwe configuratiegroep maken en pushen met behulp van de instellingen van het cloudportaal.



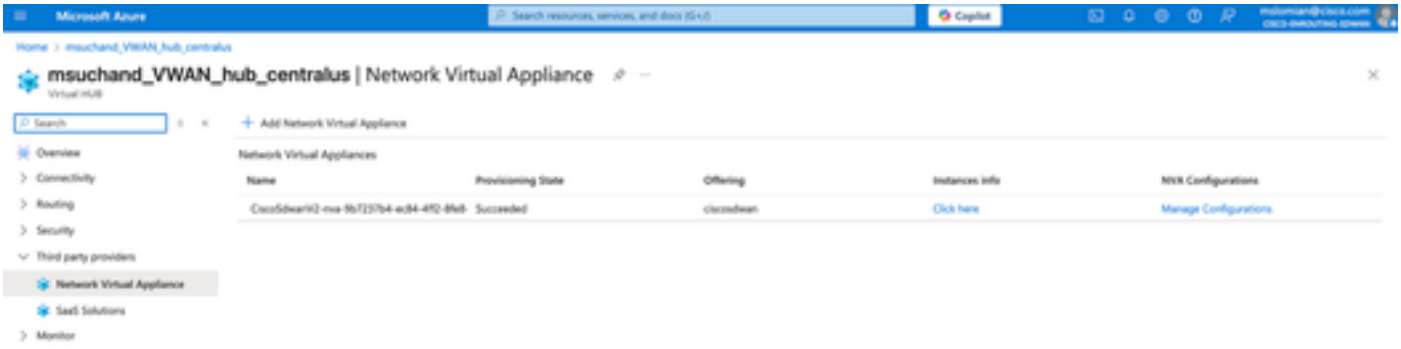
Stap 1:

Implementeer Cisco Catalyst 8000V in Azure met behulp van de procedure die hier te vinden is op dit YouTube-kanaal of Release Notes.

Stap 2:
Voor het wijzigen van de IP-instellingen gaat u naar Azure porta > Virtual WAN's > Selected Virtual WAN > Virtual Hub > NVA in Virtual Hub.



Navigeer in de virtuele hubweergave op NVA naar Externe providers > Configuraties beheren.



Navigeer in de NVA-configuratie naar Interface IP Configurations en voeg configuraties toe. Het kan tot 30 minuten duren om IP-adressen toe te wijzen,

Stap 3:

Zodra adressen zijn toegewezen, noteer ze en ga naar SD-WAN Manager. Alle C8000V's hebben deze configuratie-update nodig.

Het kan worden gedaan door CLI Addon (het voegt wat is in sjablonen / configuratieprofielen). Zie dit voorbeeld van configuratie:

```
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
```

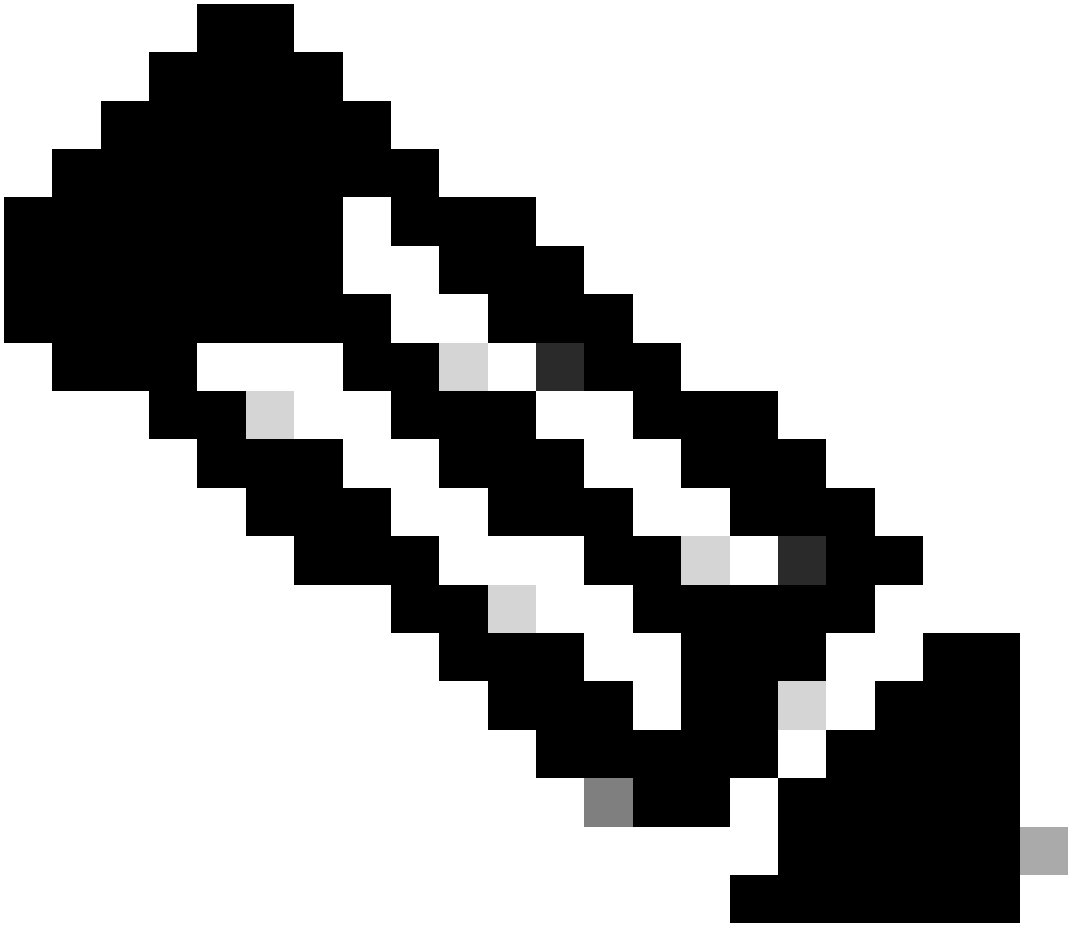
Auto-onderhandelde snelheid op transportinterface

Cisco-transportinterface op Cisco Catalyst 8000V, die wordt gebruikt in standaardsjablonen of automatisch gegenereerde configuratiegroepen (GigabitEthernet1), is geconfigureerd met automatisch onderhandelen om ervoor te zorgen dat de verbinding tot stand is gebracht.

Om betere prestaties te krijgen (meer dan 1 Gb), wordt aanbevolen om de snelheid op interfaces in te stellen op 10 Gb. Dit geldt ook voor de service-interface (Gigabit Ethernet2). Voer de volgende opdrachten uit om de overeengekomen snelheid te controleren:

```
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,
```



Opmerking: Hoewel dit artikel is gericht op C8000V-implementatie in Azure met Cloud OnRamp-automatisering (NVA), is de snelheid waarmee automatisch wordt onderhandeld ook van toepassing op Azure-implementaties in VNets-, AWS- en Google-implementaties.

Wijzig dit in sjabloon (Configuratie > Sjablonen > Functiesjabloon > Cisco VPN Interface Ethernet) / configuratiegroep (zie de handleiding). Als alternatief kunnen beheerders dit bewerken in CLI, als het apparaat CLI-beheerd is.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.