

Miglioramento del throughput di Catalyst 8000V in Azure

Sommario

[Introduzione](#)

[Miglioramento del throughput di Catalyst 8000V in Azure](#)

[Installazione della licenza HSEC](#)

[Limitazioni del throughput sulla porta TCP 12346 in Azure](#)

[Velocità negoziata automaticamente sull'interfaccia di trasporto](#)

Introduzione

Questo documento spiega come migliorare le prestazioni di Cisco Catalyst 8000Vs distribuito in Azure.

Miglioramento del throughput di Catalyst 8000V in Azure

Con Cisco Cloud onRamp per Multicast, gli utenti possono distribuire router virtuali Cisco Catalyst 8000V in NVA in Azure direttamente con SD-WAN Manager (UI o API).

L'automazione Cloud onRamp consente agli utenti di creare e individuare in modo semplice la WAN virtuale, gli hub virtuali e di creare connessioni alle reti virtuali in Azure.

Dopo aver distribuito Cisco Catalyst 8000Vs in Azure, le appliance virtuali possono essere monitorate e gestite da SD-WAN Manager.

Questo documento spiega come migliorare le prestazioni in Azure da tre prospettive:

- installazione della licenza HSEC;
- limitazioni di velocità effettiva sulla porta TCP 12346 in Azure;
- velocità con negoziazione automatica sull'interfaccia di trasporto.

Installazione della licenza HSEC

Per i dispositivi che utilizzano criteri di gestione licenze Smart e che devono supportare un throughput del traffico crittografato pari a 250 Mbps o superiore, è necessaria una licenza HSEC.

Questo è un requisito della normativa statunitense sul controllo delle esportazioni. È possibile utilizzare Cisco SD-WAN Manager per installare le licenze HSEC.

Cisco SD-WAN Manager contatta Cisco Smart Software Manager (SSM), che fornisce un codice di autorizzazione della licenza intelligente (SLAC) da caricare su un dispositivo.

Il caricamento dello SLAC su un dispositivo attiva una licenza HSEC.

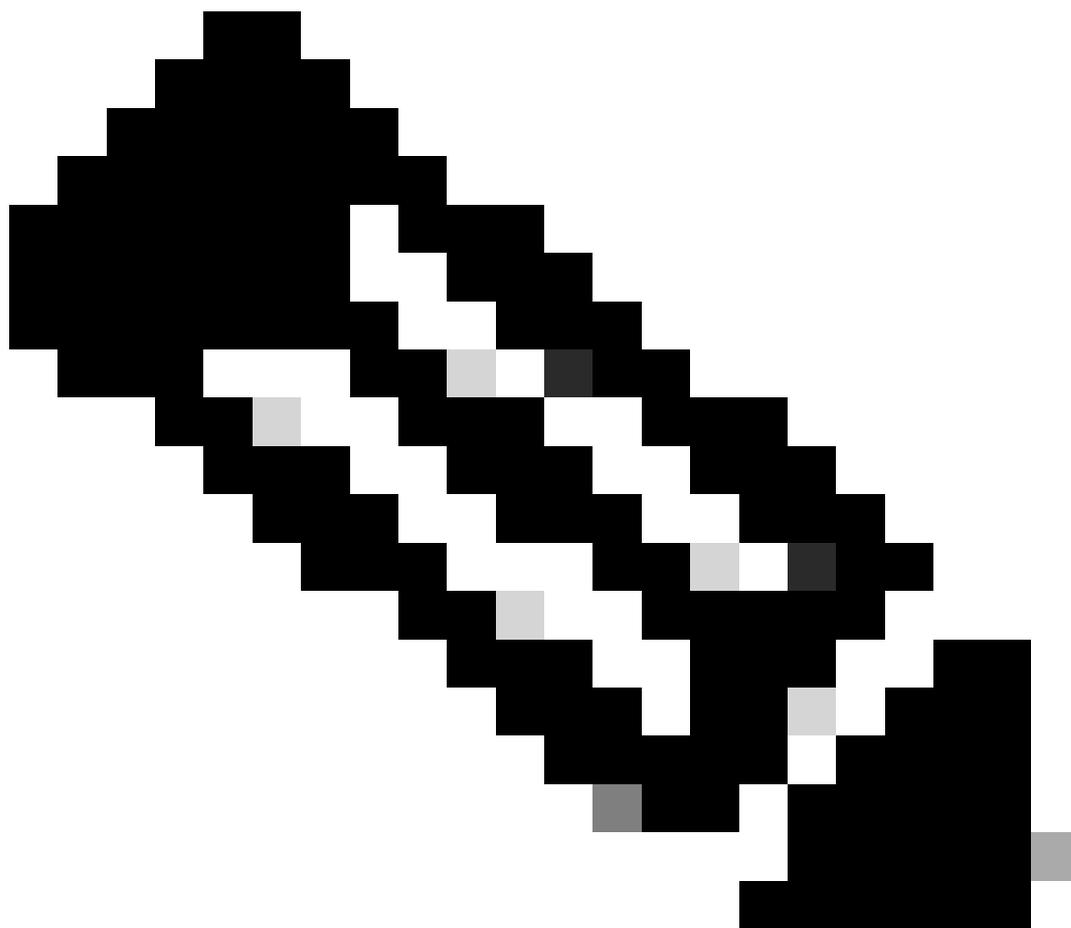
Per i dettagli sull'installazione e la gestione delle licenze, consultare il documento sulla [gestione delle licenze HSEC in Cisco Catalyst SD-WAN](#).

Limitazioni del throughput sulla porta TCP 12346 in Azure

Attualmente, l'automazione implementa C8000V con un'interfaccia di trasporto (Gigabit Ethernet1) e un'interfaccia di servizio (Gigabit Ethernet2).

A causa dei limiti di Azure in entrata sulla porta SD-WAN TCP 12346, il throughput può essere limitato per ogni interfaccia di trasporto quando il traffico entra nell'infrastruttura di Azure.

Il limite in entrata di 200.000 PPS è imposto dall'infrastruttura di Azure e pertanto gli utenti non possono raggiungere più di ~1 Gbps per ogni istanza NVA C8000V (un esempio di presupposto: dimensioni del pacchetto pari a 600 MB, calcolo: $600B * 8 = 4800 \text{ bit}$; $4800b * 200 \text{ Kpps} = 960 \text{ Mbps}$).

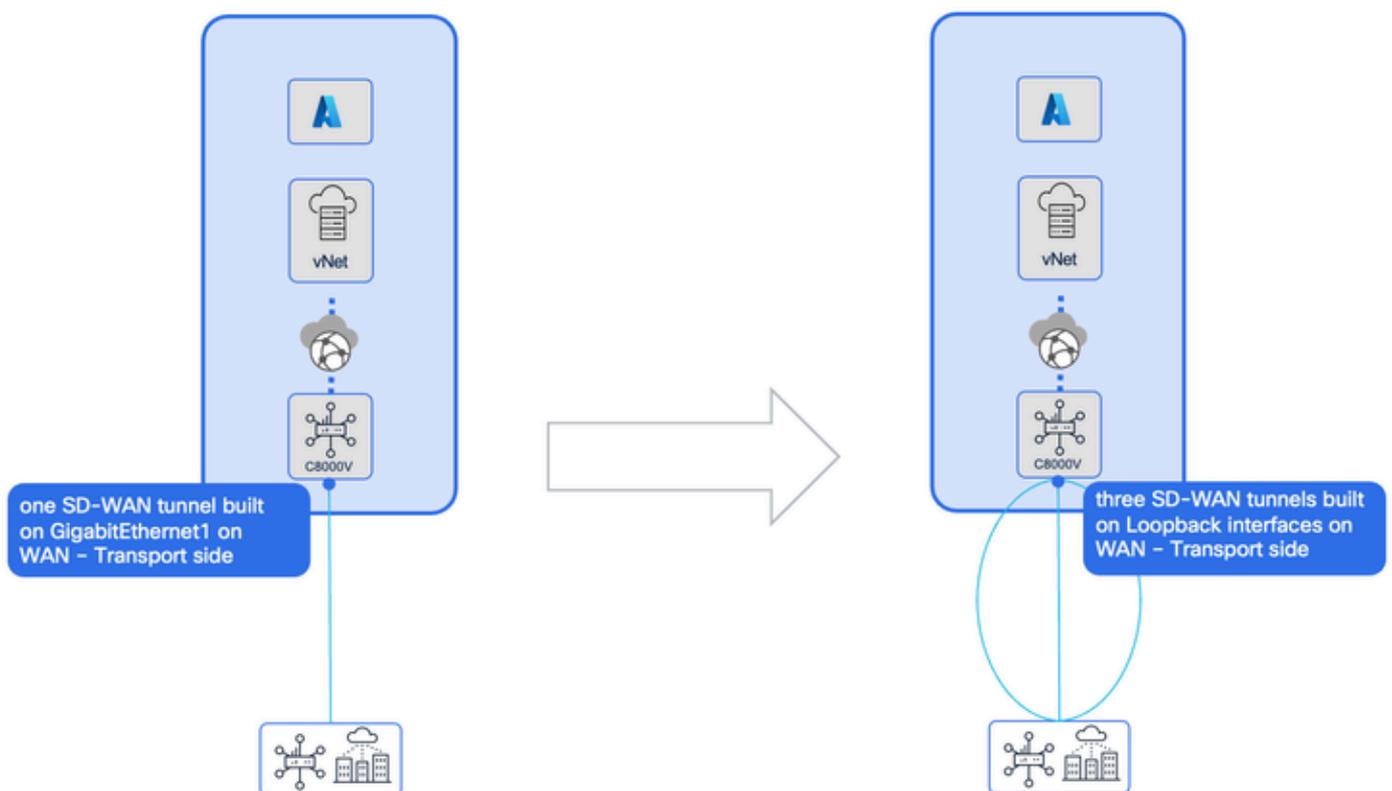


Nota: Azure può aumentare il limite in ingresso a 400.000 PPS per richiesta (ticket). I clienti devono contattare direttamente Azure e richiedere l'aumento.

Per superare questo limite, Cisco ha collaborato con Azure per consentire ai rami SD-WAN di compilare più tunnel SD-WAN per ogni istanza NVA.

Per apportare questa modifica alla configurazione, l'amministratore deve effettuare le seguenti operazioni:

1. In SD-WAN Manager, distribuire il gateway cloud con C8000V in Azure utilizzando l'automazione Cloud OnRamp.
2. Nel portale di Azure, modificare le impostazioni IP per NVA nell'hub virtuale.
3. In SD-WAN Manager, creare ed eseguire il push di un nuovo gruppo di configurazione utilizzando le impostazioni dal portale del cloud.

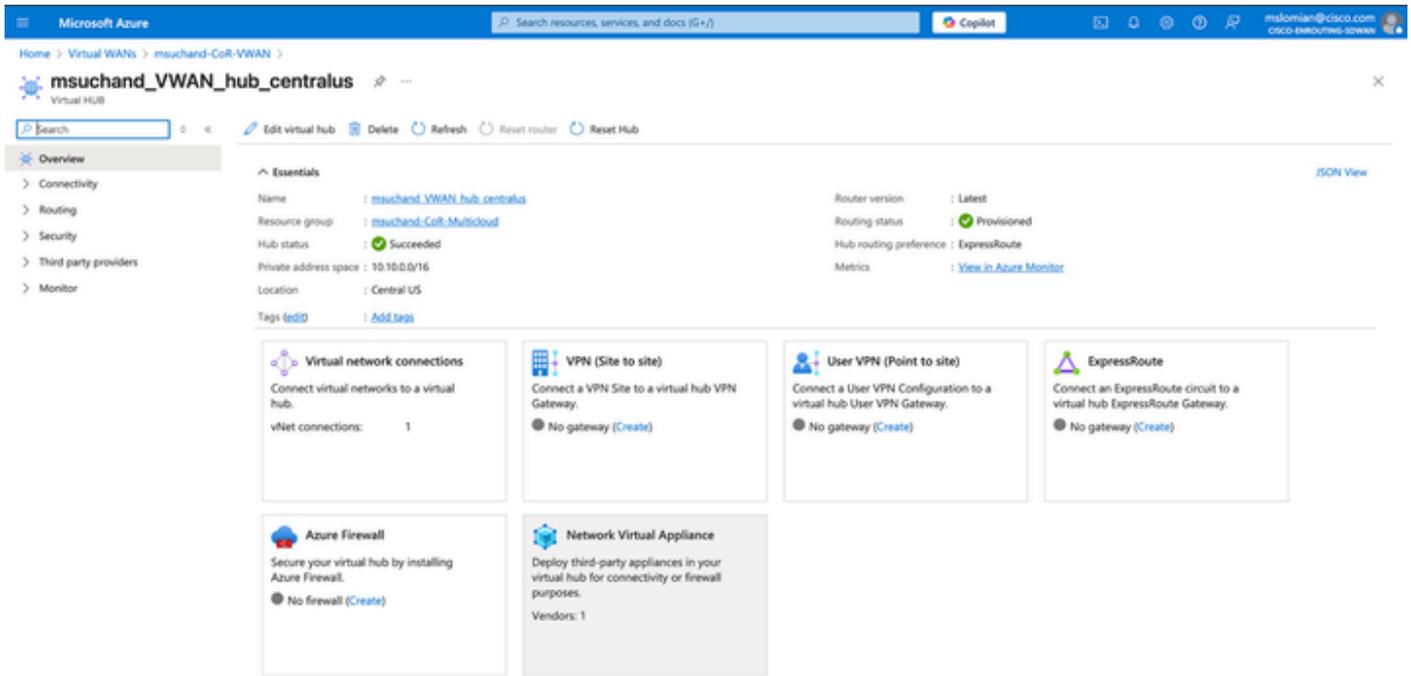


Passaggio 1:

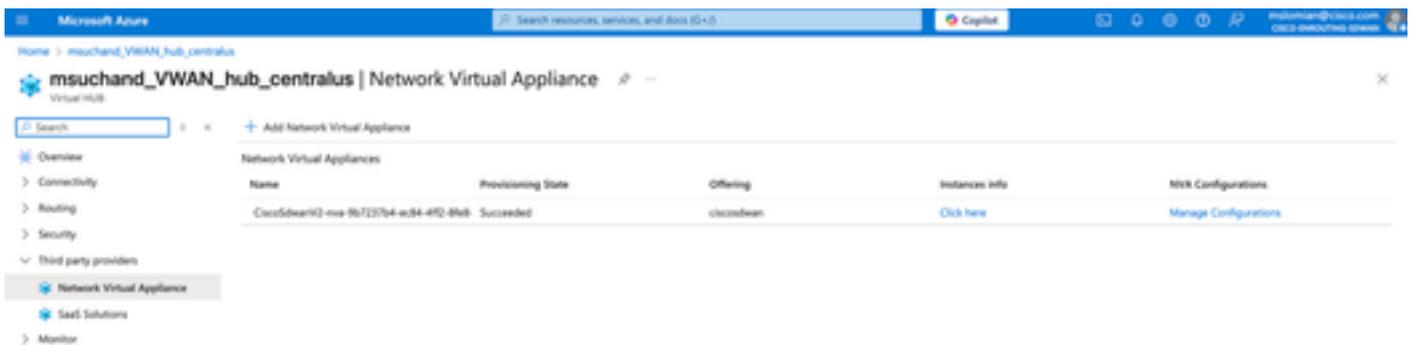
Distribuire Cisco Catalyst 8000V in Azure usando la procedura indicata qui in questo [canale di YouTube](#) o nelle [note sulla versione](#).

Passaggio 2:

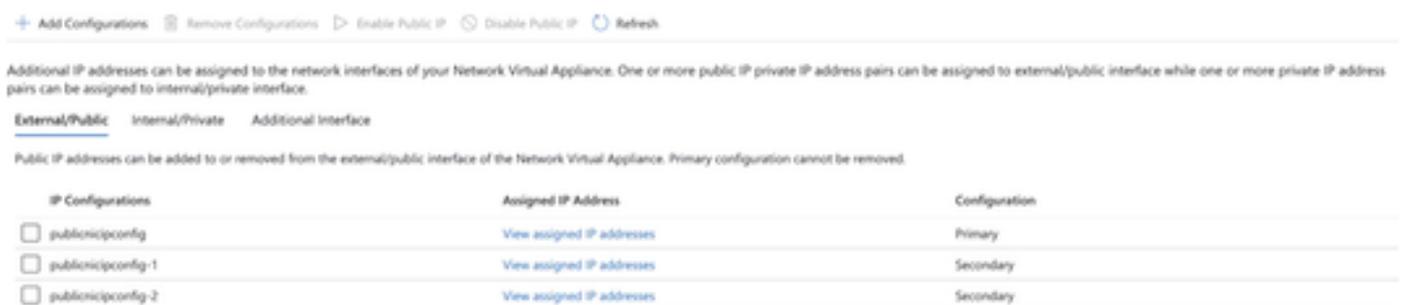
Per modificare le impostazioni IP, passare a Portale di Azure > WAN virtuali > WAN virtuale scelta > Hub virtuale > NVA nell'hub virtuale.



Nella visualizzazione dell'hub virtuale su NVA, passare a Provider di terze parti > Gestisci configurazioni.



Nella configurazione NVA, passare a Configurazioni IP interfaccia e Aggiungi configurazioni. L'assegnazione degli indirizzi IP può impiegare fino a 30 minuti,



Passaggio 3:

Una volta assegnati gli indirizzi, prenderne nota e andare a SD-WAN Manager. Tutti i C8000V necessitano di questo aggiornamento della configurazione.

Può essere eseguito da CLI Addon (aggiunge qualsiasi cosa sia presente in modelli / profili di

configurazione). Per ulteriori informazioni, fare riferimento al seguente esempio di configurazione:

```
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
```

Velocità negoziata automaticamente sull'interfaccia di trasporto

L'interfaccia di trasporto Cisco su Cisco Catalyst 8000V, che viene utilizzata nei modelli predefiniti o nei gruppi di configurazione generati automaticamente (Gigabit Ethernet1), è configurata con la funzione di negoziazione automatica per garantire che la connessione sia stabilita.

Per ottenere prestazioni migliori (superiori a 1 Gb), si consiglia di impostare la velocità sulle interfacce su 10 Gb. Ciò è applicabile anche all'interfaccia di servizio (Gigabit Ethernet2). Per verificare la velocità negoziata, eseguire i comandi seguenti:

```
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: Sebbene questo articolo sia incentrato sulla distribuzione C8000V in Azure con l'automazione Cloud OnRamp (NVA), la velocità negoziata automaticamente è applicabile anche alle distribuzioni Azure in VPNet, AWS e Google.

Per modificare questa impostazione, apportare le modifiche desiderate nel modello (Configurazione > Modelli > Modello funzionalità > Interfaccia VPN Cisco Ethernet) / gruppo di configurazione ([vedere la guida](#)). In alternativa, gli amministratori possono modificare questa impostazione nella CLI, se il dispositivo è gestito dalla CLI.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).