AzureでCatalyst 8000Vのスループットを向上

内容

はじめに

このドキュメントでは、Azureに導入されたCisco Catalyst 8000Vsのパフォーマンスを向上させる方法について説明します。

AzureでのCatalyst 8000Vスループットの向上

マルチクラウド向けCisco Cloud OnRampを使用すると、Cisco Catalyst 8000V仮想ルータをSD-WAN Manager（UIまたはAPI）を使用してAzureのNVAに直接導入できます。

Cloud OnRampの自動化により、ユーザーは仮想WAN、仮想ハブをシームレスに作成および検出し、Azureの仮想ネットワークへの接続を構築できます。

AzureにCisco Catalyst 8000Vsを導入すると、SD-WAN Managerから仮想アプライアンスを監視および管理できるようになります。

このドキュメントでは、次の3つの観点からAzureのパフォーマンスを向上させる方法について説明します。

- hsecライセンスのインストール
- azureのTCP 12346ポートのスループット制限
- トランスポートインターフェイスの自動ネゴシエート速度。

HSECライセンスのインストール

Smart Licensing Using Policyを使用するデバイスで、250 Mbps以上の暗号化トラフィックスループットをサポートする必要がある場合は、HSECライセンスが必要です。

これは、米国の輸出管理規制の要件です。Cisco SD-WAN Managerを使用してHSECライセンスをインストールできます。

Cisco SD-WAN ManagerはCisco Smart Software Manager(SSM)と通信します。SSMは、デバイスにロードするためのスマートライセンス認証コード(SLAC)を提供します。

デバイスにSLACをロードすると、HSECライセンスが有効になります。

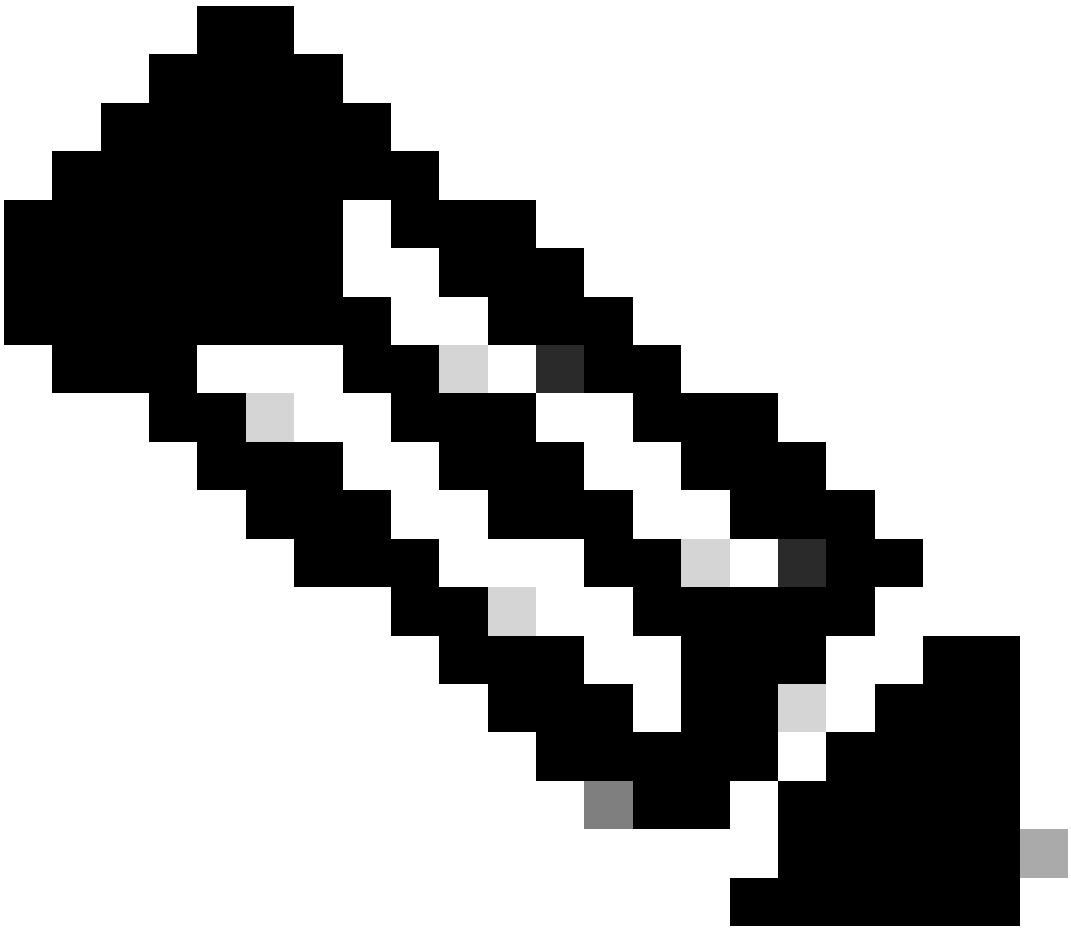
ライセンスのインストールと管理の詳細は、『Cisco Catalyst SD-WANでのHSECライセンスの管理』を参照してください。

AzureのTCP 12346ポートのスループット制限

現在、この自動化では、トランスポートインターフェイス(GigabitEtherent1)とサービスインターフェイス(GigabitEtherent2)を1つずつ備えたC8000Vを導入しています。

SD-WANポートのTCP 12346でのAzureの受信制限により、トラフィックがAzureインフラストラクチャに入ると、トランスポートインターフェイスごとにスループットが制限される場合があります。

200K PPSの受信制限はAzureインフラストラクチャによって適用されるため、ユーザーはC8000V NVAインスタンスごとに1Gbpsを超える速度を達成できません（例：600Bのパケットサイズ、計算：600B * 8 = 4800ビット、4800b * 200Kpps = 960 Mbps）。



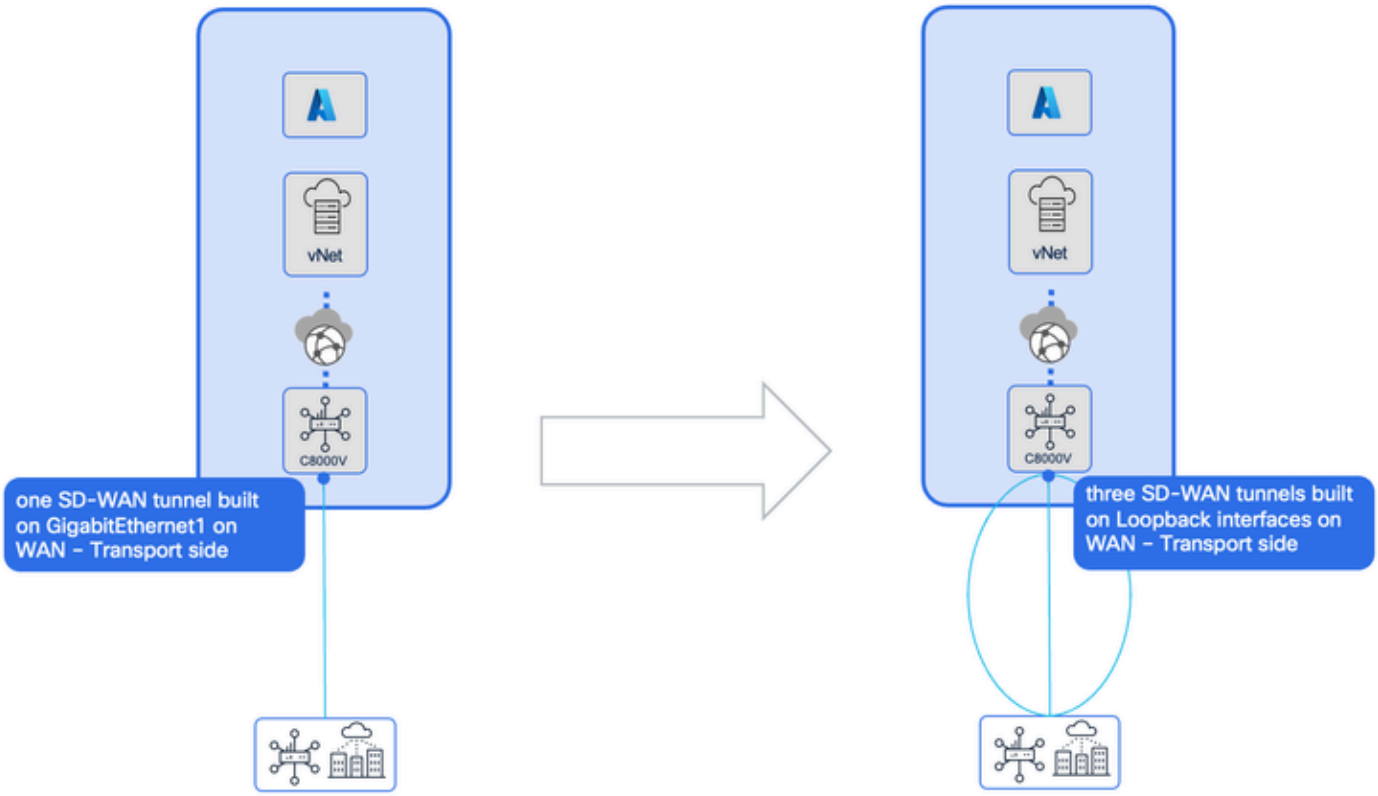
注: Azureでは、サポート案件（チケット）ごとに受信制限を400,000 PPSまで増やすこ

とができます。お客様はAzureに直接お問い合わせいただき、引き上げをリクエストする必要があります。

この制限を克服するために、シスコはAzureと協力して、SD-WANブランチが各NVAインスタンスに対する複数のSD-WANトンネルを構築できるようにしました。

この設定変更を行うには、管理者が次の手順に従う必要があります。

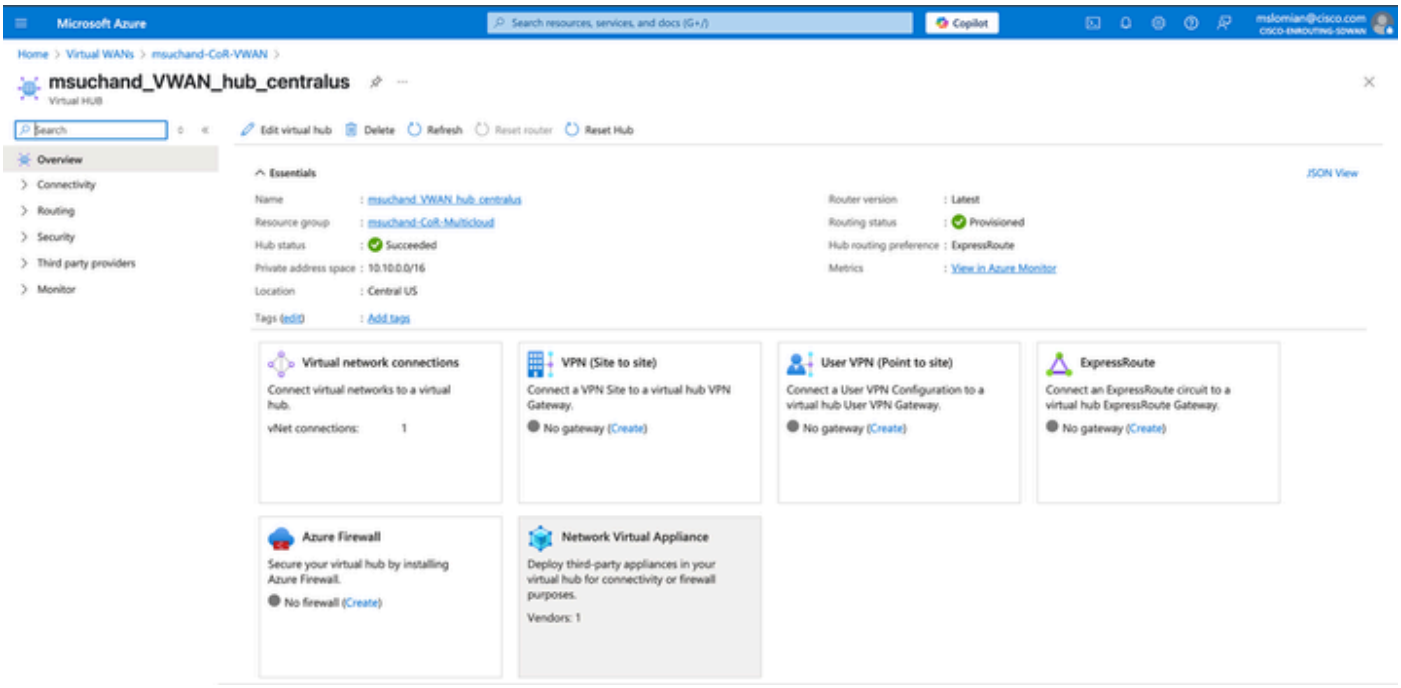
1. SD-WAN Managerで、Cloud OnRampオートメーションを使用してAzureにC8000Vを備えたクラウドゲートウェイを導入します。
2. Azureポータルで、仮想ハブのNVAのIP設定を変更します。
3. SD-WAN Managerで、クラウドポータルの設定を利用して新しい構成グループを作成し、プッシュします。



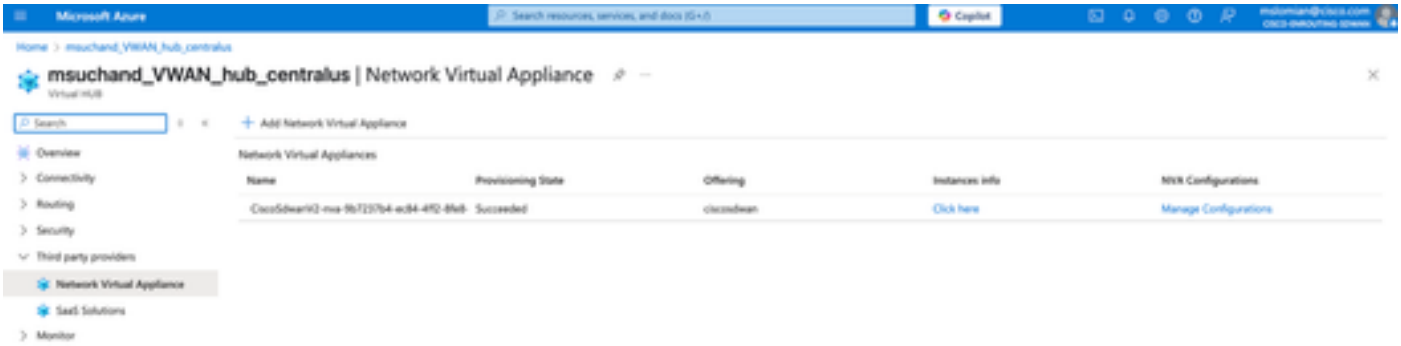
ステップ 1：

このYoutubeチャネルまたはリリースノートにある手順を使用して、AzureでCisco Catalyst 8000Vを導入します。

ステップ 2：
IP設定を変更するには、仮想ハブでAzure porta > Virtual WANs > chosen virtual WAN > virtual hub > NVAの順に選択します。



NVAの仮想ハブビューで、サードパーティプロバイダー>設定の管理に移動します。



NVA設定で、Interface IP Configurationsに移動し、Add Configurationsを選択します。IPアドレスの割り当てに最大30分かかる場合があります。

ステップ 3：

アドレスを割り当てたら、アドレスをメモし、SD-WAN Managerに移動します。すべてのC8000Vで、この構成の更新が必要です。

これはCLIアドオンで実行できます（テンプレート/設定プロファイルに含まれる内容が追加されます）。 次の設定例を参照してください。

```
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
```

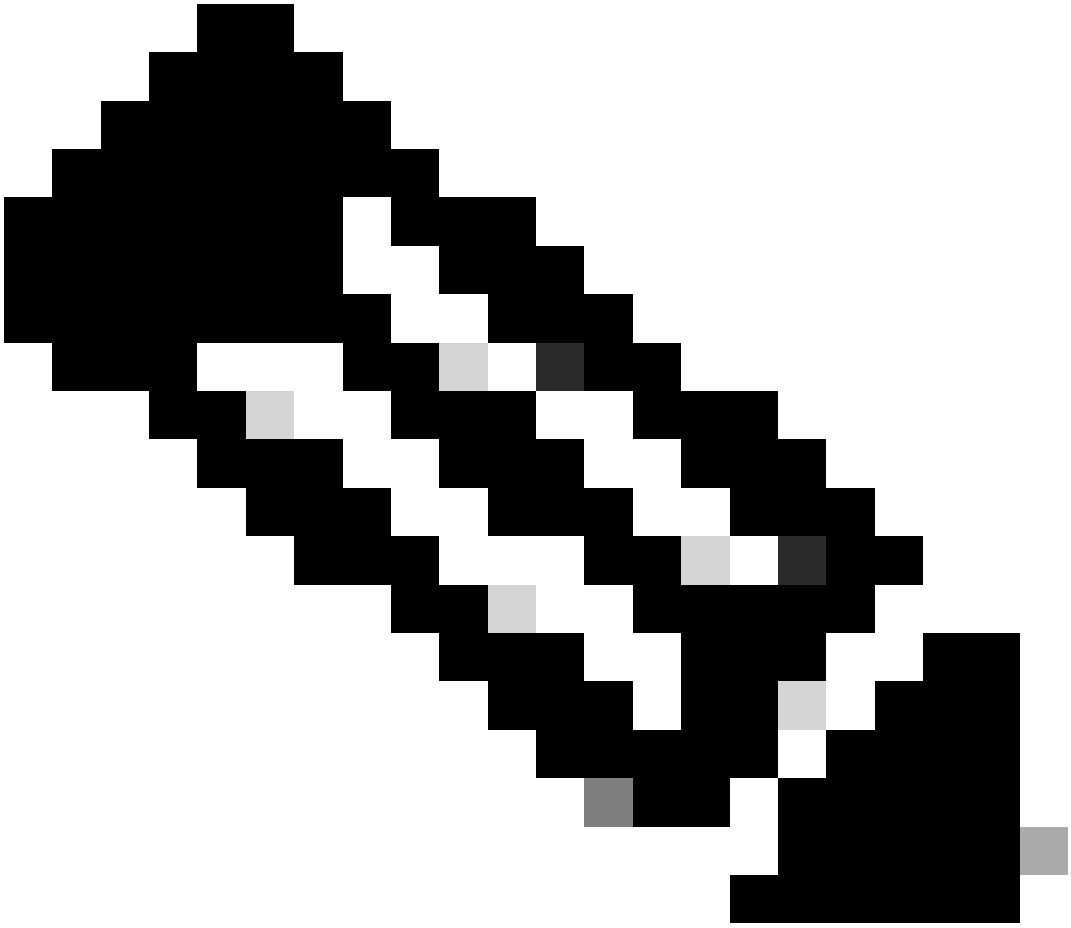
トランスポートインターフェイスの自動ネゴシエート速度

デフォルトテンプレートまたは自動生成された設定グループ(GigabitEthernet1)で使用されるCisco Catalyst 8000V上のCiscoトランスポートインターフェイスは、接続が確立されていることを確認するために、negotiate autoで設定されます。

より優れたパフォーマンス（1 Gb以上）を得るには、インターフェイスの速度を10 Gbに設定することをお勧めします。これは、サービスインターフェイス(GigabitEthernet2)にも適用されます。 ネゴシエートされた速度を確認するには、次のコマンドを実行します。

```
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：この記事では、Cloud OnRamp Automation(NVA)を使用したAzureでのC8000Vのデプロイに焦点を当てていますが、自動ネゴシエートされた速度は、VNets、AWS、およびGoogleのデプロイのAzureデプロイにも適用されます。

これを変更するには、テンプレート(設定>テンプレート>機能テンプレート> Cisco VPNインターフェイスイーサネット)/設定グループを変更します(ガイドを参照)。 または、デバイスがCLIで管理されている場合、管理者はこれをCLIで編集できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。