Microsoft Azure の Cisco Catalyst 8000V の設定

次の章では、Microsoft Azure 用に Cisco Catalyst 8000V インスタンスを設定する方法について説明します。

ルートテーブルの更新

Microsoft Azure では、すべての VM がハイパーバイザのルータにパケットを送信し、ハイパーバイザはそのサブネットに関連付けられたルーティングテーブルに基づいてパケットを転送します。

Cisco Catalyst 8000V VM が作成されると、サブネットごとにルートテーブルが作成されます。2 つの vNIC を持つ Cisco Catalyst 8000V VM の場合、Cisco Catalyst 8000V を指す 2 番目の（内部に面した）サブネットに対してデフォルトルートが作成されます。このサブネット上に作成されたすべての VM は、デフォルトゲートウェイとして Cisco Catalyst 8000V を使用します。3 つ以上の vNIC を持つ Cisco Catalyst 8000V VM の場合、デフォルトルートを定義してサブネットに適用する必要があります。

ステップ 1 [Route Tables] をクリックします。
[Settings] ペインを展開します。

ステップ 2 [Route Tables] ペインに移動し、ターゲットのルートテーブルを選択します。

ステップ 3 [All Settings] をクリックします。

ステップ 4 [Settings] ペインで [Routes] をクリックします。

ルートを追加または変更します。

セキュリティグループの更新

セキュリティグループは、特定のインターフェイスに対してどのポート/宛先をハイパーバイザが許可または拒否するかを制御するものです。Cisco Catalyst 8000V を作成すると、デフォルトで最初のサブネットのインバウンドインターフェイスに新しいセキュリティグループが作成されます。この展開を通じてデプロイされた Cisco Catalyst 8000V 仮想マシンの場合、インバウンド インターネット トラフィック用に次のポートが追加されます。TCP 22、UDP 500、および UDP 4500。他のポートの使用は拒否されます。

ステップ 1 左側のパネルで [Network security groups] をクリックします。

[Network security groups] ペインが表示され、セキュリティグループのリストが表示されます。

ステップ 2 ターゲットのネットワーク セキュリティ グループをクリックします。

セキュリティグループの詳細を示すペインが表示されます。

ステップ 3 [All Settings] をクリックします。

ステップ 4 [Settings] ペインで、[Inbound Security Rules] をクリックします。

ステップ 5 [Network Security Rules] で、[Add] をクリックしてルールを追加します。

IPsec VPN の設定

次の例は、Microsoft Azure で実行されている Cisco Catalyst 8000V インスタンス用に設定された IPsec VPN を示しています。

```
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-md5-hmac
 mode transport
crypto ipsec profile P1
 set transform-set T1
interface Tunnel0
 ip address 3.3.3.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 104.45.154.184
 tunnel protection ipsec profile P1
end
```

```
!!!! To test, create loop back interface and static route!!!!!
interface Loopback1
 ip address 5.5.5.5 255.255.255.255
end
ip route 6.6.6.6 255.255.255.255 Tunnel0
```

ベストプラクティスと注意事項

1. リソースはリソースグループに保持することを推奨します。グループ内のすべてのリソースをクリーンアップするには、関連するリソースグループを削除します。
2. Cisco Catalyst 8000V VM が削除されても、VM のすべてのリソース（ルートテーブル、セキュリティグループ、パブリック IP、ネットワーク インターフェイス）が削除されるわけではありません。その後、以前と同じ名前で新たに Cisco Catalyst 8000V を作成すると、以前のリソースが再利用される可能性があります。これらのリソースを再利用したくない場合は、次のいずれかのアクションを選択します。
   - 各リソースを手動で削除します。
   - 個々のリソースを含むリソースグループを削除します。
   - 別の名前で新しいCisco Catalyst 8000V VM を作成します。
3. 展開テンプレートを使用して Cisco Catalyst 8000V インスタンスを作成する場合は、パブリック IP アドレスが Microsoft Azure で静的として設定されていることを確認してください。これを行うには、Microsoft Azure でパブリック IP アドレスに移動します。設定で、アドレスが動的または静的として表示されているかどうかを確認します。[Static] オプションを選択します。デフォルトのオプションは動的であることに注意してください。

SSH 接続の問題

Cisco Catalyst 8000V を最初にデプロイした後、または Cisco Catalyst 8000V をリロードまたは再起動した後に、Microsoft Azure での Cisco Catalyst 8000V への SSH 接続を確立できない場合があります。Azure ポータルでは、Cisco Catalyst 8000V インスタンスは実行状態です。次の 3 つのシナリオでは、SSH を使用した接続に失敗した場合の回避策を提案します。

シナリオ 1Cisco Catalyst 8000V の起動直後に SSH アクセスを試みた

起動直後に Cisco Catalyst 8000V にアクセスしようとすると、SSH 接続の確立に失敗する場合があります。インスタンスの展開を開始してから、SSH 接続が利用可能になるまで約 5 分かかります。

シナリオ 2 Microsoft Azure インフラストラクチャのバインドの問題

Microsoft Azure サポートでは、次の手順を実行することを推奨します。

1. パブリック IP アドレスを持つ Cisco Catalyst 8000V インターフェイスで、プライベート IP アドレスをサブネット内の新しい静的 IP アドレスに再割り当てします。

2. Azure ポータルで PowerShell を開きます。
3. ARM VM を更新します。

   次の Azure のドキュメントを参照してください。https://docs.microsoft.com/en-us/powershell/module/azurerm.compute/update-azurermvm?view=azurermps-5.6.0
4. PowerShell で次のコマンドを実行してください。

   $vm = Get-AzureRmVM -Name "reload-lnx" **-ResourceGroupName** "reload-rg"

   Update-AzureRmVM -VM $vm -ResourceGroupName "reload-rg"
5. パブリック IP アドレスがアタッチされているネットワーク インターフェイスをリセットします。

   ネットワーク インターフェイスのリセットの詳細については、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/reset-network-interface を参照してください。
6. [VM] > [Networking] を選択し、ネットワーク インターフェイスを選択します。
7. [IP configurations] に移動し、IP 名を選択します。
8. インターフェイスに割り当てられているプライベート IP アドレスが静的に設定されている場合は、手順 **13** で使用するためにアドレスを書き留めます。
9. [Assignment] で、[Static] をクリックします。
10. [IP Address] フィールドで、使用可能な IP アドレスを使用します。ネットワーク インターフェイスが接続されているサブネット内で使用可能な IP アドレスを選択します。
11. [Save] をクリックして、保存が完了するまで待ちます。
12. SSH を使用してルータへの接続を再試行します。
13. 静的 IP アドレスを追加（または変更）して VM にアクセスした後、このインターフェイスに最初に割り当てた IP アドレス（手順 **8** を参照）が静的に設定されている場合は、IP アドレスを静的から動的に変更できます。または、IP アドレスを元のアドレス（手順 **8** で書き留めたアドレス）に再設定できます。

シナリオ 3 アイドル端末のタイムアウトの設定不備

Cisco Catalyst 8000V への SSH セッションを開始するときは、次のように端末の VTY タイムアウトを無限に設定しないでください。`exec-timeout 0 0` タイムアウトにはゼロ以外の値を使用します。たとえば、`exec-timeout 4 0` などです。このコマンドは、4 分 0 秒のタイムアウトを指定します。

`exec-timeout 0 0` コマンドが問題を引き起こす理由は次のとおりです。

Azure では、コンソールのアイドル期間に 4 分から 30 分のタイムアウトが適用されます。アイドルタイマーが期限切れになると、Azure は SSH セッションを切断します。しかし、`exec-timeout 0 0` コンフィギュレーション コマンドによってタイムアウトが無限に設定されていると、セッションは Cisco Catalyst 8000V からはクリアされません。切断により、端末セッションが孤立します。Cisco Catalyst 8000V のセッションは無期限に開いたままになります。新しい SSH セッ

ションを確立しようとすると、新しい仮想端末セッションが使用されます。このパターンが引き続き発生すると、許可されている同時端末セッションの数に達し、新しいセッションを確立できなくなります。

`exec-timeout` コマンドを正しく設定することに加えて、次の例に示すコマンドを使用して、アイドル状態の仮想端末セッションを削除することもお勧めします。

```
Router# show users
Line User Host(s) Idle Location
2 vty 0 cisco idle 00:07:40 128.107.241.177
* 3 vty 1 cisco idle 00:00:00 128.107.241.177

Router# clear line 2
```

上記のシナリオの回避策が効果がない場合は、最後の手段として、Azure ポータルから Cisco Catalyst 8000V インスタンスを再起動できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。