Azure トランジット VNET DMVPN ソリューションの展開

トランジット VNet ソリューションを展開するための前提条件

- Cisco Catalyst 8000V インスタンスの Azure アカウントが必要です。
- ライセンスが登録され、有効であることを確認してください。
- スポークを設定する前に、ハブが稼働していることを確認してください。

トランジット VNet ソリューションの展開に関する制約事項

- スポーク VNet を別のクラウド サービス プロバイダーに展開することはできません。
- すべての場所にトランジット VNet ソリューションを設定することはできません。サポートされている場所のリストを表示するには、インスタンスを作成した後、[Configure Basic Settings] ページの [Location] フィールドのすべてのオプションを確認します。

Azure トランジット VNET DMVPN を展開する方法

トランジット VNet ハブの作成

この手順は、トランジット VNet ソリューションを設定する最初の手順です。これは、トランジット VNet の設定を行う必要がある展開において、非常に重要な部分です。これらの設定は、アクセスキーを使用してトランジット VNet ストレージのアカウントにメタデータとして保存される DMVPN IPsec パラメータに対応しています。スポークのテンプレートを設定するときは、TVNET ストレージのアカウントとアクセスキーのみを設定する必要があります。スポークに必要な関連する DMVPN IPsec パラメータは、デバイスから自動的に選択されます。

ステップ 1 Microsoft Azure ポータルにサインインします。

ステップ 2 [Create a Resource] をクリックし、Cisco Catalyst 8000V の展開を検索して、[Enter] を押します。システムは、DMVPN のトランジット VNET テンプレートを検索して表示します。

ステップ 3 [Transit VNET DMVPN] > [Create] を選択します。

ステップ 4 [Basics] 画面で、仮想マシンの名前、トランジット VNet ハブの名前、およびユーザー名を入力します。

Note [Transit VNet Name] には小文字のみを使用してください。

ステップ 5 [Authentication Type] ドロップダウンリストから、[SSH Public Key] を選択します。

ステップ 6 パスワードを指定し、確認用にパスワードを再入力します。

ステップ 7 [SKU] ドロップダウンリストから、適切なイメージバージョンを選択します。

ステップ 8 [Location] ドロップダウンリストから、TVNET ハブを展開できるリージョンの 1 つを選択します。

ステップ 9 Cisco C8000V の設定ページで、設定を行います。Cisco Catalyst 8000V の設定の詳細については、「*Deploying the Cisco Catalyst 8000V on Microsoft Azure*」セクションを参照してください。

ステップ 10 トランジット VNet の設定で、次の設定を行います。

a) [TVNET Storage Account] はキーワード「strg」が追加されたトランジット VNet 名に由来するストレージアカウント名です。スポークの作成時にこの値が必要です。このフィールドの値は自動入力されます。ただし、このフィールドの値は編集できます。

b) [Private TVNET Storage Account] でキーの保存に必要なストレージアカウントを選択します。このフィールドは、オートスケーラーの展開に必要です。

c) [DMVPN Tunnel ID] はすべての Cisco Catalyst 8000V デバイス（ハブとスポークの両方）でトンネルを設定するために使用されるトンネルの ID です。

d) [DMVPN Tunnel Key] は 6 ～ 8 桁の数値のトンネルキーです。

e) [IPSEC Tunnel Authentication]

f) **[IPSEC Tunnel Cipher]**

g) [IPSEC Shared Key] はトンネルを認証するためのキーワードです。

h) [DMVPN Tunnel Network] は DMVPN のオーバーレイに使用されるトンネルネットワークです。

Note デフォルトのオプションは、ハブ用に作成されたVNetとクラッシュする可能性があります。この値が既存の仮想ネットワーク（VNet）と重複しないようにしてください。

この時点では、[Configure Subnets] セクションでサブネットを設定する必要はありません。

ステップ 11 [Summary] 画面でパラメータを確認し、[OK] をクリックします。

ステップ 12 [Buy] セクションで [Create] をクリックして、トランジット VNet ハブソリューションを展開します。この手順により、次のリソースが作成されます。

- 1 つの可用性セットに展開された 2 つの Cisco Catalyst 8000V インスタンス（C8000V1 および C8000V2）仮想マシン
- 2 つのストレージディスク（Cisco Catalyst 8000V ごとに 1 つ）
- 4 つの NIC（Cisco Catalyst 8000V インスタンスごとに 2 つの NIC）
- トランジット VNET 全体に 1 つのセキュリティグループ（インバウンド用に SSH のみを開きます）
- 2 つのパブリック IP（インスタンスごとに 1 つの PIP）
- 2 つのルートテーブル（インスタンスのサブネットごとに 1 つの RT）
- 2 つのストレージアカウント（Cisco Catalyst 8000V 診断用の 1 つのストレージとトランジット VNET メタデータ用の 1 つのストレージ）
- 1 つの VNET /16 CIDR
- 1 つの Resource-Manager グループを使用して展開された上記すべて（この RG を削除すると、上記のすべてのコンポーネントが削除されます）

展開が完了し、リソースが作成されるまでに数分かかります。[All Resources] をクリックし、[Group By Type] オプションを選択することで、展開をモニタリングできます。展開が完了すると、[notification] パネルに「Deployment Succeeded」というメッセージが表示されます。

Azure DMVPN スポーク VNET の作成

Before you begin

トランジット VNet ソリューションのスポークを作成する前に、ハブが正常に作成されていることを確認してください。

ステップ 1 Microsoft Azure Marketplace から、[Cisco CSR 1000V DMVPN Transit VNet] テンプレートを検索して選択します。

ステップ 2 テンプレートをクリックし、ドロップダウンリストから必要となる適切なスポークオプションを選択します。

ステップ 3 [Create] をクリックします。

ステップ 4 [Basics settings] 画面で、次の設定の詳細を指定していることを確認します。

a) [Filename] でこのフィールドにトランジット VNet の名前を指定します。
b) [Transit VNet Storage Name] は、ハブ構成の TVNET ストレージアカウントの値と同じです。この名前は、キーワード「strg」が追加されたトランジット VNet 名に由来します。
c) [Storage Key] にアクセスするには、[public Hub] を検索してクリックし、[Access Key] オプションをクリックします。

ステップ 5 [Basics Settings] 画面で他の値を設定し、[OK] をクリックします。

ステップ 6 Cisco Catalyst 8000V の設定画面で、フィールドを設定するか、そのままにするか（デフォルト値）を選択できます。

パラメータの詳細については、「*How to Deploy a Cisco Catalyst 8000V on Microsoft Azure*」を参照してください。

Note 可用性ゾーンは、Microsoft Azure のすべてのリージョンでまだ完全にはサポートされていません。したがって、ソリューションテンプレートには可用性ゾーンのオプションはありませんが、「Availability-Sets」を使用して復元力が考慮されています。詳細については、Microsoft Azure のドキュメント（https://docs.microsoft.com/en-us/azure/availability-zones/az-overview）を参照してください。

ステップ 7 [Virtual Network] の横にある矢印をクリックして仮想ネットワークの値を指定し、[OK] をクリックします。

ステップ 8 [Address Space] フィールドに、Classless Inter-Domain Routing（CIDR）表記を使用して、仮想ネットワークのアドレスを入力します。

Note VNET CIDR は、TVNET-HUB の Cisco Catalyst 8000V デバイスに使用される物理 IP アドレスのサブネットを示します。CIDR ブロックは通常、2 つの /24 サブネットにさらにサブネット化される /16 サブネットです。各サブネットの最初の 3 つの IP アドレスは、Azure ルートテーブルおよびその他のサービス用に予約されます。IP 割り当てはサブネットの 4 番目の IP から始まり、動的に割り当てられるパブリック IP に自動的にマッピングされます。パブリック IP はインターネットへのアクセスを可能にするため、DMVPN シナリオの NBMA アドレスになります。

ステップ 9 [Configure the Subnets] の横にある矢印をクリックし、[OK] をクリックします。

ステップ 10 [Summary] 画面で、設定されたパラメータを確認します。テンプレートを検証したら、[OK] をクリックします。

ステップ 11 [Create] をクリックして、TVNet スポークソリューションを展開します。

Note 作成する追加のスポークごとに、手順 1 ～ 10 に従います。

設定の確認

トランジット VNET ハブでの確認

次のコマンドは、スポークがトランジット VNet Hub1 への DMVPN トンネルを正常に確立し、EIGRP ルートを Transit VNet Hub1 と交換できることを示しています。このソリューションにより、DMVPN フェーズ 3 の機能である NHRP ショートカットスイッチングが有効になります。これらのコマンドを Transit VNet Hub2 で実行すると、コマンド出力は Transit VNet Hub1 と同様になります。これは、スポークが両方のトランジット VNet ハブの Cisco Catalyst 8000V への DMVPN トンネルを正常に確立し、EIGRP ルートを両方のハブと正常に交換したことを示しています。ハブは、復元力を高めるためにアクティブ-アクティブモードで展開されます。

ステップ 1 `show ip interface brief` コマンドを実行します。

Example:

```
Transit-Hub# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.1.0.4        YES DHCP   up                    up
GigabitEthernet2       10.1.1.5        YES DHCP   up                    up
Tunnel11               172.16.1.1      YES TFTP   up                    up
VirtualPortGroup0      192.168.35.1    YES TFTP   up                    up
p1-tvnet-csr-1#
```

設定出力の強調表示されている部分に注目してください。これは、トンネルが稼働していることを示しています。システムがこの設定出力にトンネルを表示しない場合は、ゲストシェルに移動して TVNet のログを確認する必要があります。`show log` コマンドを実行して、TVNet のログにアクセスします。

ステップ 2 スポークからの 2 つの DMVPN 接続の IKE セッションを表示するには、`show crypto isakmp sa` コマンドを実行します。

Example:

```
Transit-Hub# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.0.4        168.62.164.228  QM_IDLE           1042 ACTIVE
10.1.0.4        40.114.69.24    QM_IDLE           1043 ACTIVE
IPv6 Crypto ISAKMP SA
```

ステップ 3 スポークからの 2 つの DMVPN 接続の IPsec セッションを表示するには、`show crypto session` コマンドを実行します。

Example:

```
Transit-Hub# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
```

```
Peer: 40.114.69.24 port 4500 fvrf: (none) ivrf: tvnet-Tun-11
      Phase1_id: 12.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 10.1.0.4/4500 remote 40.114.69.24/4500 Active
          Capabilities:DN connid:1043 lifetime:18:32:04
  IPSEC FLOW: permit 47 host 10.1.0.4 host 40.114.69.24
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 32 drop 0 life (KB/Sec) 4607996/3474
        Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4607998/3474
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 168.62.164.228 port 4500 fvrf: (none) ivrf: tvnet-Tun-11
      Phase1_id: 11.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 10.1.0.4/4500 remote 168.62.164.228/4500 Active
          Capabilities:DN connid:1042 lifetime:18:02:01
  IPSEC FLOW: permit 47 host 10.1.0.4 host 168.62.164.228
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 32 drop 0 life (KB/Sec) 4607970/2427
        Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4607982/2427
```

ステップ 4 `show dmvpn` コマンドを実行して、デバイスの DMVPN のステータスを表示します。

Example:

```
Transit-Hub# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.114.69.24       172.16.1.137    UP     1w3d    DN
     1 168.62.164.228     172.16.1.147    UP     1w3d    DN
```

ステップ 5 `show vrf` コマンドを実行して、トランジット VNet 上の各スポークからの表示ルートを表示します。

Example:

```
Transit-Hub# show vrf
  Name                             Default RD            Protocols   Interfaces
  tvnet-Tun-11                     64512:11              ipv4        Tu11
```

ステップ 6 `show ip eigrp vrf <vrf-name> neighbors` コマンドを実行して、EIGRP ネイバーのステータスを表示します。

Example:

```
Transit-Hub# show ip eigrp vrf tvnet-Tun-11 neighbors
EIGRP-IPv4 Neighbors for AS(64512) VRF(tvnet-Tun-11)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
```

```
1   172.16.1.137            Tu11                     14 1w3d       13  1398  0  12
0   172.16.1.147            Tu11                     10 1w3d       12  1398  0  12
```

ステップ 7 `show ip route vrf <vrf-name>VRF` コマンドを実行して VRF に固有のルートを表示します。

Example:

```
Transit-Hub# show ip route vrf tvnet-Tun-11
Routing Table: tvnet-Tun-11
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      11.0.0.0/24 is subnetted, 2 subnets
D EX     11.1.0.0 [170/26880256] via 172.16.1.147, 1w1d, Tunnel11
D EX     11.1.1.0 [170/26880256] via 172.16.1.147, 1w1d, Tunnel11
      12.0.0.0/24 is subnetted, 2 subnets
D EX     12.1.0.0 [170/26880256] via 172.16.1.137, 1w1d, Tunnel11
D EX     12.1.1.0 [170/26880256] via 172.16.1.137, 1w1d, Tunnel11
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Tunnel11
L        172.16.1.1/32 is directly connected, Tunnel11
D EX  192.168.35.0/24 [170/26905600] via 172.16.1.147, 1w1d, Tunnel11
                      [170/26905600] via 172.16.1.137, 1w1d, Tunnel11
```

スポークとハブ間の接続の確認

次のコマンドは、スポークが両方の Cisco Catalyst 8000V TVNET ハブに接続されていて、両方のハブからの EIGRP ルートを交換できることを示しています。DMVPN ソリューションは DMVPN-Phase3（NHRP ショートカットスイッチング）として展開され、ハブはアクティブ-アクティブモードで展開されるため、スポーク 2 への EIGRP ルートはスポーク 2 のトンネルオーバーレイ IP アドレスを指します。

ステップ 1 `show ip interface brief` コマンドを実行して、デバイスのインターフェイスの IP アドレスを表示します。

Example:

```
Spoke# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       11.1.0.4        YES DHCP   up                    up
GigabitEthernet2       11.1.1.4        YES DHCP   up                    up
Tunnel11               172.16.1.147    YES TFTP   up                    up
VirtualPortGroup0      192.168.35.1    YES TFTP   up                    up
```

ステップ 2 `show dmvpn` コマンドを実行して、デバイスの DMVPN のステータスを確認します。

Example:

```
Spoke# show dmvpn
```

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
============================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.117.131.133       172.16.1.1    UP     1w3d     S
     1 40.117.128.85        172.16.1.2    UP     1w3d     S
```

強調表示されている設定出力に注目してください。これは、スポークが作動していて、ハブとの接続が確立されていることを示しています。

ステップ 3 スポークからの 2 つの DMVPN 接続の IKE セッションを表示するには、`show crypto isakmp sa` コマンドを実行します。

Example:

```
Spoke# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
40.117.131.133  11.1.0.4        QM_IDLE           1025 ACTIVE
40.117.128.85   11.1.0.4        QM_IDLE           1026 ACTIVE
IPv6 Crypto ISAKMP SA
```

ステップ 4 スポークからの 2 つの DMVPN 接続の IPsec セッションを表示するには、`show crypto session` コマンドを実行します。

Example:

```
Spoke# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.131.133 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.131.133/4500 Active
          Capabilities:DN connid:1025 lifetime:17:33:41
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.131.133
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 2250 drop 0 life (KB/Sec) 4607927/726
        Outbound: #pkts enc'ed 2251 drop 0 life (KB/Sec) 4607957/726
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.128.85 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.5
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.128.85/4500 Active
```

```
        Capabilities:DN connid:1026 lifetime:17:33:44
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.128.85
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 2252 drop 0 life (KB/Sec) 4607960/2046
        Outbound: #pkts enc'ed 2253 drop 0 life (KB/Sec) 4607976/2046
```

ステップ 5 EIGRP ネイバーのステータスを表示するには、`show up eigrp neighbor` コマンドを実行します。

Example:

```
Spoke# show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(64512)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.16.1.2              Tu11                     13 1w3d       24  1362  0  23
0   172.16.1.1              Tu11                     12 1w3d        8  1362  0  23
```

ステップ 6 EIGRP ルート情報を表示するには、show ip route eigrp コマンドを実行します。

Example:

```
Spoke# show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 11.1.0.1 to network 0.0.0.0
      12.0.0.0/24 is subnetted, 2 subnets
D EX     12.1.0.0 [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
                  [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
D EX     12.1.1.0 [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
                  [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
```

スポーク間の接続の確認

次のコマンドは、2 つのスポーク間の接続をテストするのに役立ちます。サポートされる機能は DMVPN フェーズ 3 であるため、**traceroute** コマンドはスポーク 1 からスポーク 2 に送信されたパケットを表示します。ただし、スポーク 1 がパケットをハブに送信してスポーク 2 のアドレスを取得するため、NHRP 解決のために最初のパケットが失われます。スポーク 1 がアドレスを受信すると、スポーク 1 とスポーク 2 の間に動的 IPsec トンネルが確立されます。

```
Spoke1# clear crypto sa counters
Spoke1# ping 12.1.1.4 source gigabitEthernet 2 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 12.1.1.4, timeout is 2 seconds:
Packet sent with a source address of 11.1.1.4
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 1/1/6 ms
Spoke# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
```

```
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.117.131.133       172.16.1.1    UP     1w3d     S
     1 40.117.128.85        172.16.1.2    UP     1w3d     S
     1 40.114.69.24       172.16.1.137    UP 00:00:07    DN
Spoke# traceroute 12.1.1.4 source gigabitEthernet 2
Type escape sequence to abort.
Tracing the route to 12.1.1.4
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.137 2 msec *  3 msec
p1spoke1#
p1spoke1#
p1spoke1#sh crypto sess detail | i pkts
        Inbound:  #pkts dec'ed 101 drop 0 life (KB/Sec) 4607985/3581
        Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4607989/3581
        Inbound:  #pkts dec'ed 12 drop 0 life (KB/Sec) 4607924/621
        Outbound: #pkts enc'ed 14 drop 0 life (KB/Sec) 4607955/621
        Inbound:  #pkts dec'ed 13 drop 0 life (KB/Sec) 4607957/1941
        Outbound: #pkts enc'ed 13 drop 0 life (KB/Sec) 4607975/1941
Spoke# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 00:00:36
Session status: UP-ACTIVE
Peer: 40.114.69.24 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 12.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.114.69.24/4500 Active
          Capabilities:DN connid:1027 lifetime:23:59:23
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.114.69.24
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 101 drop 0 life (KB/Sec) 4607985/3563
        Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4607989/3563
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.131.133 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.131.133/4500 Active
          Capabilities:DN connid:1025 lifetime:17:31:38
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.131.133
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 16 drop 0 life (KB/Sec) 4607923/603
        Outbound: #pkts enc'ed 18 drop 0 life (KB/Sec) 4607955/603
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.128.85 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.5
      Desc: (none)
  Session ID: 0
```

```
IKEv1 SA: local 11.1.0.4/4500 remote 40.117.128.85/4500 Active
        Capabilities:DN connid:1026 lifetime:17:31:41
IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.128.85
      Active SAs: 2, origin: crypto map
      Inbound:  #pkts dec'ed 17 drop 0 life (KB/Sec) 4607957/1923
      Outbound: #pkts enc'ed 17 drop 0 life (KB/Sec) 4607975/1923
```

トラブルシューティング

展開のステータスを表示するには、Cisco Catalyst 8000V インスタンスにログインして `show log` コマンドを実行します。展開が成功すると、「[AzureTransitVNET] Success.Configured all the required IOS configs」というメッセージが表示されます。

トランジット VNet ソリューションの設定中にこのメッセージが表示されず、エラーが発生した場合は、次のことを確認してください。

- DMVPN トンネルがハブとスポークの間に確立されているか確認します。ほとんどの場合、次の値に問題がある可能性があります。TransitVNETname、TransitVNETStoragename、または TransitVNETStoragekey。
- Guestshell が、インストールされる TVNet パッケージ用に立ち上がり、稼働しているか確認します。

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。