Microsoft

Microsoft Azure

Microsoft Azure 自習書シリーズ No.4

企業内システムと Microsoft Azure の VPN 接続

Published: 2014 年 5 月 30 日
Updated: 2015 年 1 月 31 日
Cloudlive, Inc.

Cloudlive

Microsoft Azure 自習書 No.4

企業内システムと Microsoft Azure の VPN 接続

本ドキュメントの更新について

バージョン	更新日	内容
v1.00	2014/6/30	・初版リリース
v1.10	2014/9/30	・2014 年 9 月現在の情報に更新
v1.20	2015/1/31	・2015 年 1 月現在の情報に更新

目次

STEP 1. 仮想ネットワークの概要 と本書の目的について 5

1.1 仮想ネットワークの概要 6
1.2 シナリオ 11
1.3 ゴール 12

STEP 2. 実習の前提について 13

2.1 前提条件 14
2.2 検証済み VPN デバイス 対象機器リスト 15

STEP 3. 構築手順の概要 18

3.1 構築手順の概要 19

STEP 4. 仮想ネットワークの作成 20

4.1 作成に必要なパラメーター 21
4.2 仮想ネットワークの作成 23

STEP 5. 仮想ゲートウェイの作成 31

5.1 仮想ゲートウェイの作成 32

STEP 6. 仮想ゲートウェイの IP アドレスと 共有キーの確認 36

6.1 仮想ゲートウェイの IP アドレスの確認 37
6.2 共有キーの確認 38

STEP 7. ASA の設定 39

7.1 作成に必要なパラメーター 40
7.2 ASA に投入するコマンド 41
7.3 Config 例 45

STEP 8. 接続状態の確認 48

8.1 Azure 管理ポータル上で接続状態の確認 49
8.2 ASA の接続状態の確認 50

STEP 1. 仮想ネットワークの概要と本書の目的について

この STEP では、仮想ネットワークの概要と本書の目的について説明します。

この STEP では、次のことを学習します。

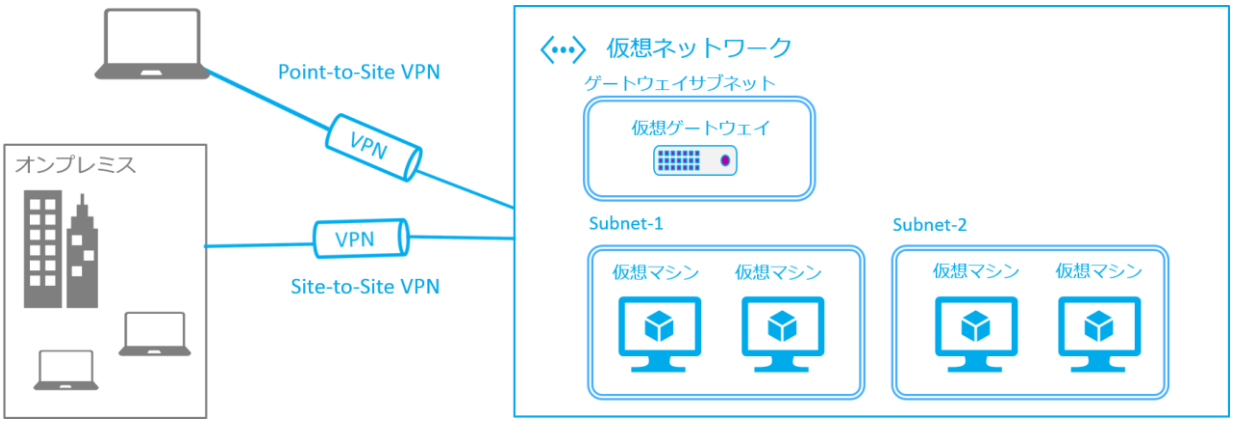
- ✓ 仮想ネットワークの概要
- ✓ シナリオ
- ✓ ゴール

1.1 仮想ネットワークの概要

仮想ネットワークについて

仮想ネットワークは、Azure 内部に仮想の L2 イーサネットを構築し、任意の IP アドレス範囲のローカル ネットワーク構成を可能にします。

また、IPsec ゲートウェイを追加し、オンプレミス ネットワークと相互接続する事で、あたかも Azure を自社のネットワークの一部として利用することができます。



Note： 仮想ネットワークのアフィニティ グループについて

以前は、各仮想ネットワークにアフィニティ グループを関連付ける必要がありました。これは要件ではなくなりました。仮想ネットワークを場所 (地域) に関連付けることができるようになりました。

リージョン仮想ネットワーク

リージョン全体をカバーする仮想ネットワークを作成することができるようになりました。 これにより、新しく仮想ネットワークを作成する際、アフィニティ グループではなく、リージョンを指定することができます。 また、このリージョン仮想ネットワークにデプロイされた新しいサービスは、そのリージョンで提供されているすべてのサービスを利用することができます。

以前は、仮想ネットワークはスケール ユニット、正確にはアフィニティ グループにバインドされていました。 アフィニティ グループとは、データセンターの 1 セクション、すなわち一定数のサーバーを指すグループ概念です。 仮想ネットワークはアフィニティ グループにバインドされていたため、間接的に一定数のサーバーにバインドされており、このスケール ユニット外のサーバーにデプロイメントを配置することができませんでした。

リージョン仮想ネットワークでは、スコープがアフィニティ グループではなくリージョン全体となるため、こうした制約から解放されます。

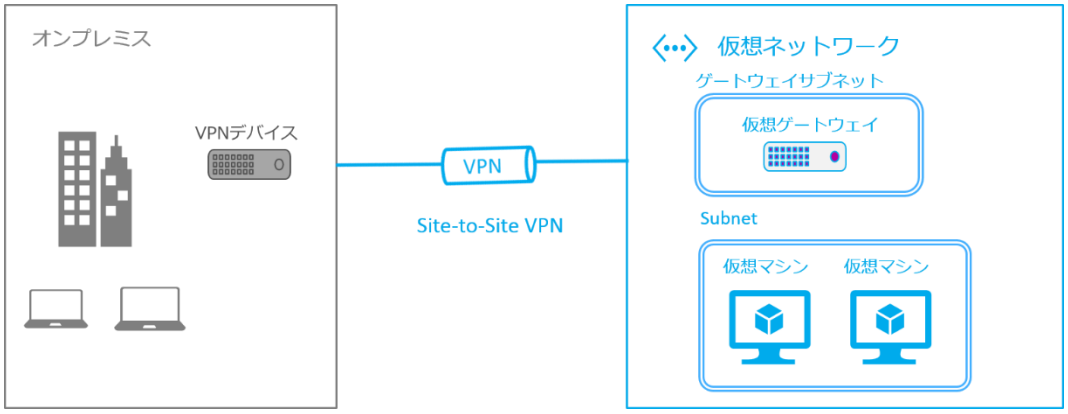
リージョン仮想ネットワークで可能になる主なシナリオを以下に示します。

- 仮想マシンの A8 や A9 サイズのインスタンスを仮想ネットワークにデプロイできます。
- 予約済み IP、内部負荷分散 (ILB)、インスタンス レベルのパブリック IP などの新機能を利用できます。
- 仮想ネットワークはシームレスにスケーリングしてリージョン全体のキャパシティを使用できますが、仮想ネットワーク内の仮想マシンの最大数は 2048 に制限されます。
- 仮想ネットワークを作成するにあたってアフィニティ グループを作成する必要はありません。
- 仮想ネットワークへのデプロイメントは、同じアフィニティ グループである必要はありません。

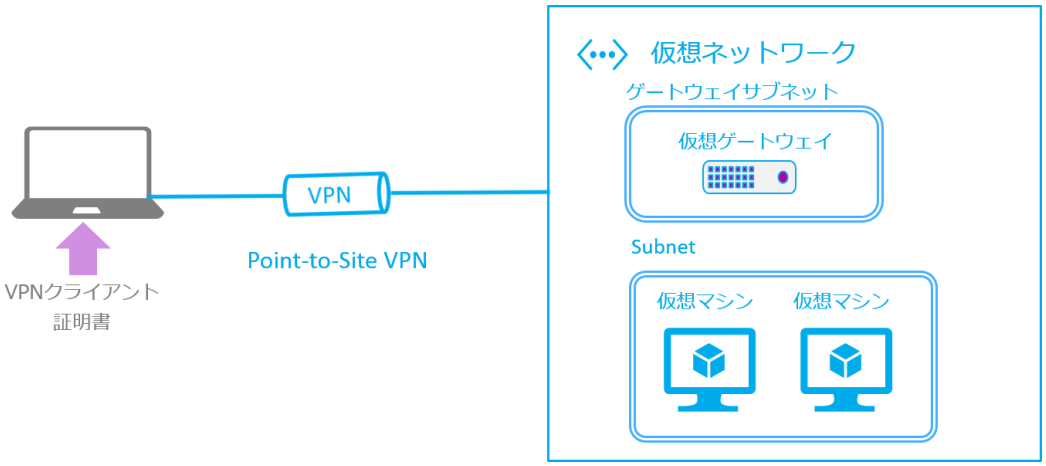
VPN について

仮想ネットワークは、VPN 接続を使用してセキュリティを確保しつつ利用することができます。

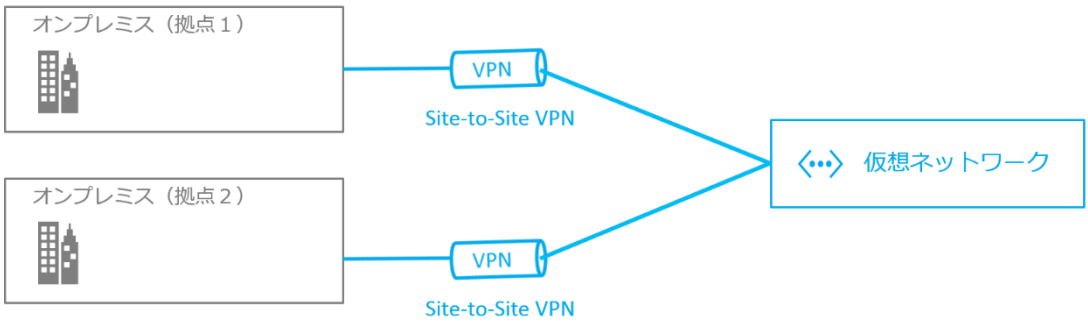
オンプレミス間との接続では、VPN デバイスによる IPsec 接続を使用して VPN 環境を実現しています。(Site to Site VPN)



VPN クライアントソフトウェアを使ったリモートアクセス接続で VPN 環境を実現することもできます。(Point to Site VPN)



Site-to-Site VPN を複数のネットワーク（拠点）に同時接続することもできます。(マルチサイト VPN 構成)

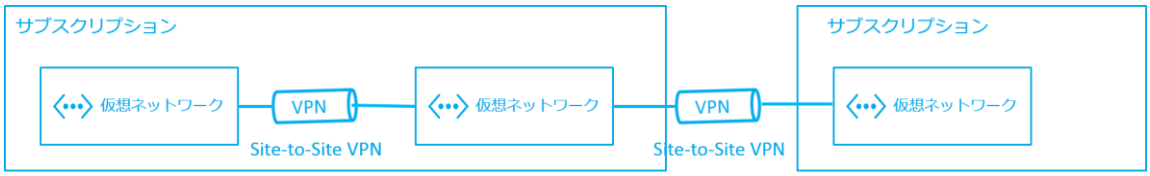


Note： マルチサイト VPN 接続の注意点

- 1 つの仮想ネットワークから同時に接続可能なネットワークの数は標準のゲートウェイで最大 10 拠点、ハイパフォーマンスゲートウェイの場合は最大 30 拠点。
- 各ネットワークの IP アドレスが重複することがないこと
- 設定は PowerShell を利用する必要がある

詳しくは、「マルチサイト VPN の構成 (http://msdn.microsoft.com/ja-jp/library/azure/dn690124.aspx)」をご参照ください。

仮想ネットワーク間を接続する構成を実現することもできます。



- Site-to-Site VPN を利用して仮想ネットワーク同士を接続可能
- マルチサイト VPN で複数の仮想ネットワークでも接続可能
- 異なる地域、異なるサブスクリプション間でも接続可能

Note：仮想ネットワーク間の接続の構成の注意点
• マルチサイト VPN の注意点と同じ点に注意 • 仮想ネットワークは動的ルーティングであること • すべての仮想ネットワークに同じ共有キーを PowerShell を利用して設定する

詳しくは、「VNet 間の接続の構成 (http://msdn.microsoft.com/ja-jp/library/azure/dn690122.aspx)」をご参照ください。

本自習書では、Site to Site VPN 環境の構築手順をご紹介しています。

1.2 シナリオ

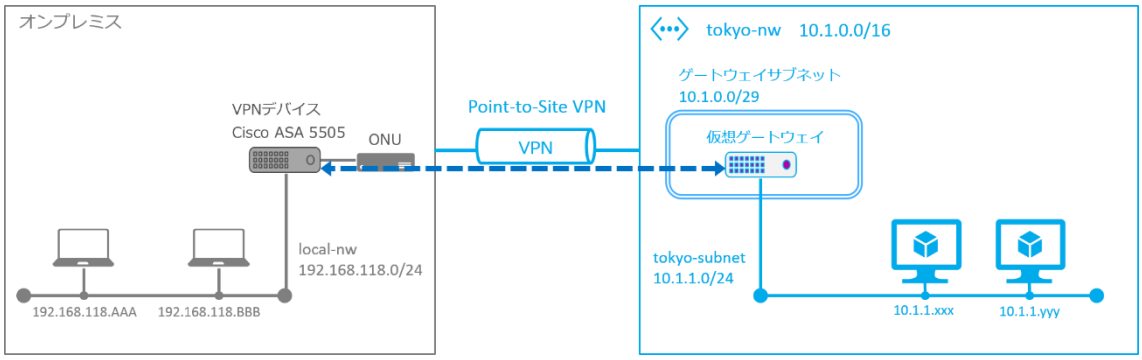
本書では以下のような構成で、仮想ネットワークとオンプレミス間を VPN 接続する環境を構築します。

仮想ネットワーク

- サブネットを 1 つ作成
- Site to Site VPN を構成

オンプレミス

- ISP から払い出された固定グローバル IP アドレスを使用して接続
- ISP の ONU と VPN デバイスを直接繋ぐ(FW などを間に挟まない)
- VPN デバイスは Cisco ASA5505(以降「ASA」と記載)を 1 台使用
- オンプレミス内の既存セグメント 1 つを仮想ネットワークと VPN で接続



1.3 ゴール

上記のシナリオで環境を構築し、以下が確認できたことをもってゴールとします。

- Azure 管理ポータルで、VPN 接続が確認できること
- ASA のステータスで、VPN 接続が確認できること

※ 実際に VPN 経由で通信できているかを確認するには、仮想ネットワーク上に仮想マシンを作成し、オンプレミス側のマシンとの間で疎通確認を行う必要があります。

STEP 2. 実習の前提について

この STEP では、この自習書で実習を行うために必要な前提について説明します。

この STEP では、次のことを学習します。

- ✓ 前提条件
- ✓ 検証済み VPN デバイス 対象機器

2.1 前提条件

- Azure 管理ポータルへサインインできるアカウントを持っていることを前提としています。
- VPN 接続用のインターネット回線があることを前提としています。 加えて、固定グローバル IP アドレスが必要となります。
- 仮想ネットワークとオンプレミスを VPN 接続するには、オンプレミス側に VPN デバイスを設置する必要があります。

  今回は Cisco 社の ASA 5505 を使用し、シングル構成での構築を行います。
  ASA の操作方法については Cisco 社の情報をご確認ください。
  また、次項目の検証済み VPN デバイスの対象機器リストを参考に、導入機器を検討してください。
- Azure 管理ポータルへのサインインの手順は省略しています。

2.2 検証済み VPN デバイス 対象機器リスト

メーカー（ 五十音順）	製品名	備考
アライドテレシス	AR415S	動的ルーティング互換性なし
	AR550S	動的ルーティング互換性なし
	AR560S	動的ルーティング互換性なし
	AR570S	動的ルーティング互換性なし
インターネットイニシアティブ	SEIL/X1	
	SEIL/X2	
	SEIL/B1	
	SEIL/x86	
F5 ネットワークス	BIG-IP シリーズ	動的ルーティング互換性なし
Cisco	ASA	動的ルーティング互換性なし
	ASR	
	ISR	
Citrix	CloudBridge MPX アプライアンスまたは VPX 仮想アプライアンス	動的ルーティング互換性なし
ジュニパーネットワークス	SRX シリーズ	
	SSG シリーズ	
	ISG シリーズ	
	J シリーズ	
パロアルトネットワークス	PA-200	
	PA-500	
	PA-2020,PA-2050	
	PA-3020,PA-3050	
	PA-4020,PA-4050,PA-4060	
	PA-5020,PA-5050,PA-5060	

メーカー (五十音順)	製品名	備考
富士通	Si-R G100	
	Si-R G200	
	IPCOM EX 1100 SC	
	IPCOM EX 1300 SC	
	IPCOM EX 2300 SC	
	IPCOM EX 2500 SC	
	IPCOM EX 1100 NW	
	IPCOM EX 1300 NW	
	IPCOM EX 2300 NW	
	IPCOM EX 2500 NW	
	IPCOM EX 2300 IN	
	IPCOM EX 2500 IN	
ヤマハ	RTX810	
	RTX1200	
	RTX3500	
	RTX5000	
	FWX120	
日本電気株式会社	UNIVERGE IX2105	
	UNIVERGE IX2207	
	UNIVERGE IX2025	
	UNIVERGE IX2215	
	UNIVERGE IX3010	
	UNIVERGE IX3110	
Microsoft	ルーティングとリモート アクセス サービス(Windows2012)	静的ルーティング互換性なし

※2015 年 1 月時点

参考 URL
http://msdn.microsoft.com/ja-jp/windowsazure/dn132612.aspx
http://msdn.microsoft.com/library/azure/jj156075.aspx

記載のない製品については、メーカーにお問い合わせ願います。

STEP 3. 構築手順の概要

この STEP では、構築手順の概要について説明します。

この STEP では、次のことを学習します。

✓ 構築手順の概要

3.1 構築手順の概要

以下のような順序で構築を進めます。

- 仮想ネットワークの作成（STEP 4）
- 仮想ゲートウェイの作成（STEP 5）
- Azure 側グローバル IP アドレスと共有キーの確認（STEP 6）
- Cisco ASA の設定（STEP 7）
- 接続状態の確認（STEP 8）

STEP 4. 仮想ネットワークの作成

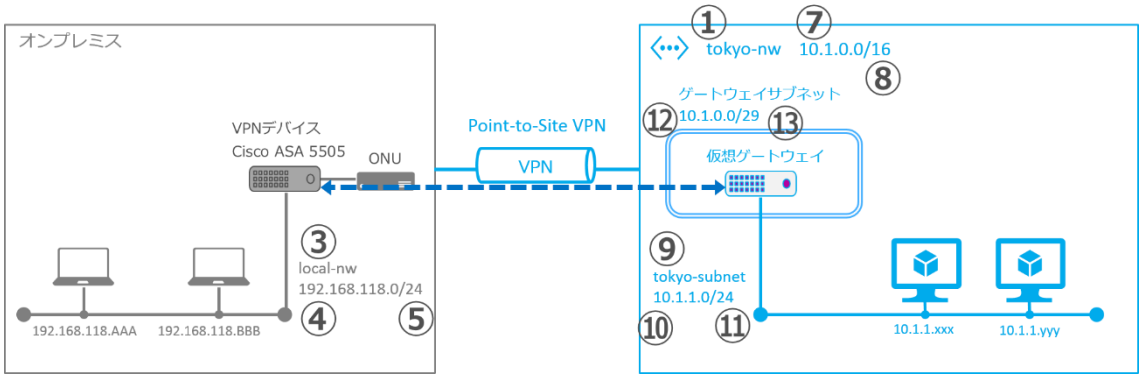
この STEP では、仮想ネットワークの作成手順について説明します。

この STEP では、次のことを学習します。

- ✓ 作成に必要なパラメーター
- ✓ 仮想ネットワークの作成

4.1 作成に必要なパラメーター

仮想ネットワークの作成に必要なパラメーターは以下の通りです。(②、⑥は図には表されていません)



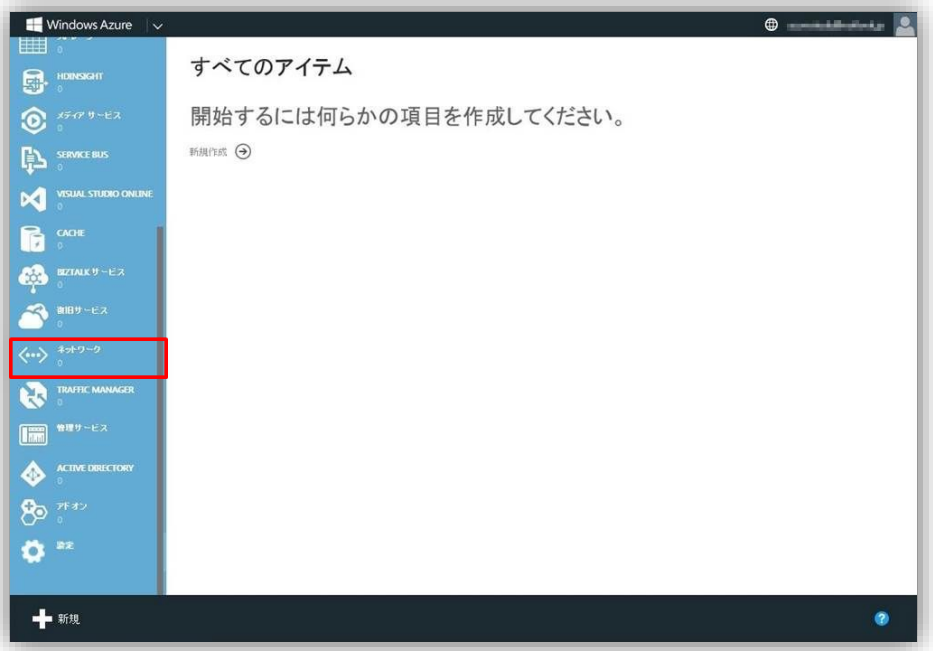
番号	名前	詳細	今回設定する値
①	仮想ネットワークの名前	仮想ネットワーク全体の名前	tokyo-nw
②	仮想ネットワークを配置する場所	仮想ネットワークを配置するリージョン	日本 (東)
③	オンプレミス側セグメントの名前	オンプレミス側の既存セグメントの Azure 上の名前	local-nw
④	オンプレミス側セグメントの開始 IP	オンプレミス側の既存セグメントのネットワークアドレス	192.168.118.0
⑤	オンプレミス側セグメントの CIDR(アドレス数)	オンプレミス側の既存セグメントのサブネットマスク	/24
⑥	VPN デバイスの IP アドレス	VPN デバイスの WAN 側（Azure 向け）のアドレス	ISP から払い出された固定 IP アドレス
⑦	仮想ネットワークのアドレス空間の開始 IP	仮想ネットワーク全体のネットワークアドレス	10.1.0.0
⑧	仮想ネットワークのアドレス空間の CIDR(アドレス数)	仮想ネットワーク全体のサブネットマスク	/16

番号	名前	詳細	今回設定する値
⑨	仮想ネットワークのサブネットの名前	仮想ネットワーク内に作成するセグメントの名前	tokyo-Subnet1
⑩	仮想ネットワークのサブネットの開始 IP	仮想ネットワーク内に作成するセグメントのネットワークアドレス	10.1.1.0
⑪	仮想ネットワークのサブネットの CIDR(アドレス数)	仮想ネットワーク内に作成するセグメントのサブネットマスク	/24
⑫	仮想ゲートウェイの開始 IP	仮想ネットワーク側の VPN ゲートウェイ装置が配置されるセグメントのネットワークアドレス	デフォルト値（10.1.0.0）
⑬	仮想ゲートウェイの CIDR(アドレス数)	仮想ネットワーク側の VPN ゲートウェイ装置が配置されるセグメントのサブネットマスク	デフォルト値（/29）

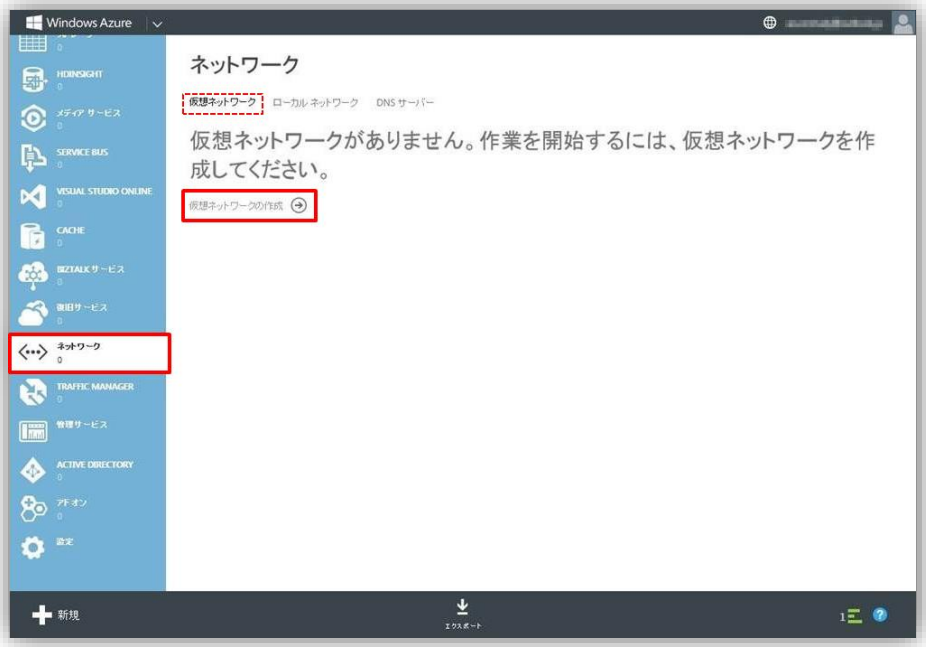
4.2 仮想ネットワークの作成

1. Azure 管理ポータルにサインインします。

2. 画面左側のメニューから「ネットワーク」をクリックします。



3. 「ネットワーク – 仮想ネットワーク」が表示されます。次に、「仮想ネットワークの作成」をクリックします。

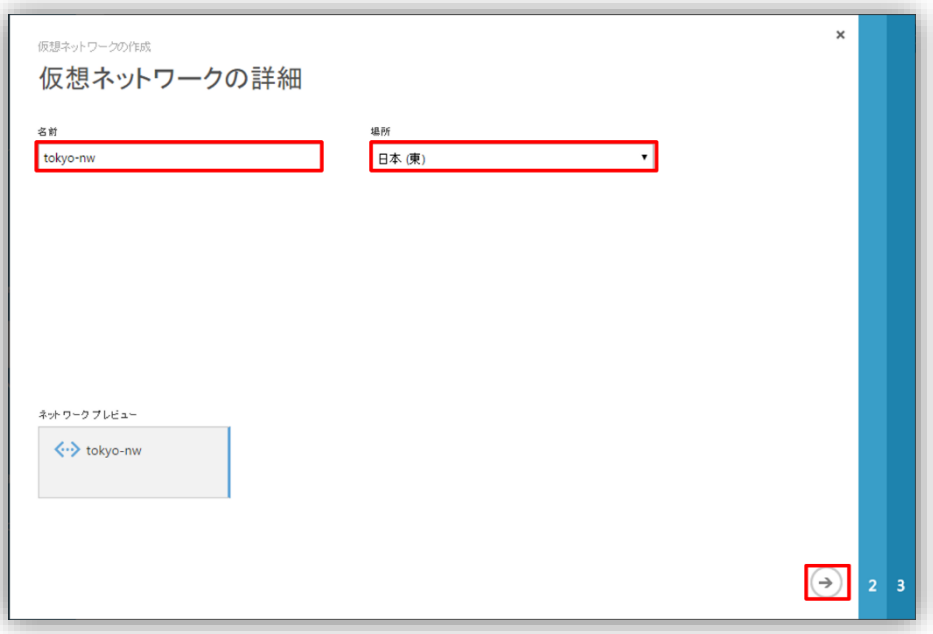


4. 「仮想ネットワークの作成 – 新規」が表示されます。次に、「ネットワークサービス – 仮想ネットワーク – カスタム作成」を選択します。

5. 「仮想ネットワークの作成 – 仮想ネットワークの詳細」が表示されます。

次に「名前」を入力し、「場所」を選択します。今回は「名前」「tokyo-nw」と入力し、「場所」は「日本（東）」を選択します。

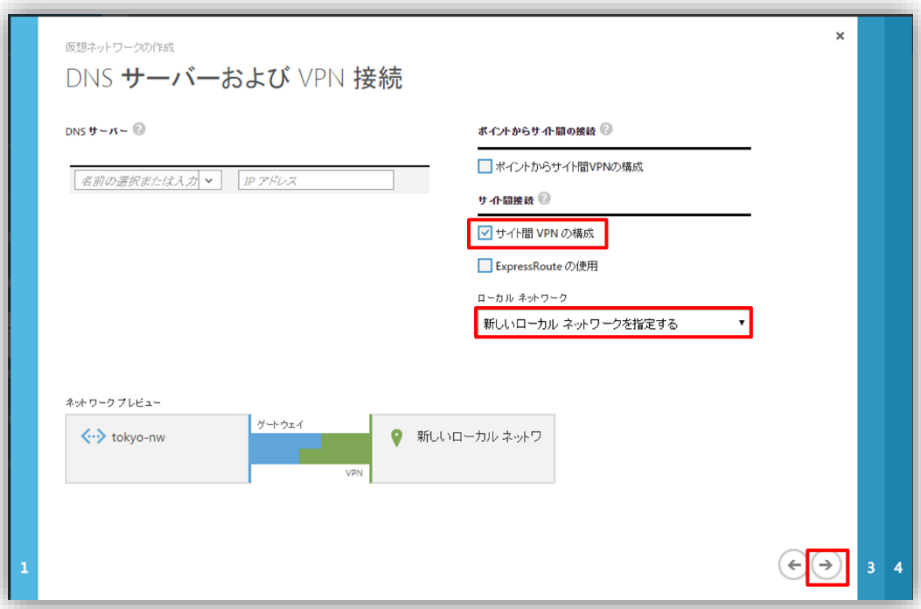
入力および選択が終わったら、右下の「→」をクリックします。



6. 「仮想ネットワークの作成 – DNS サーバーおよび VPN 接続」が表示されます。

「サイト間 VPN の構成」にチェックを入れ、今回は「ローカルネットワーク」に「新しいローカル ネットワークを指定する」を選択します。

選択が終わったら、右下の「→」をクリックします。



Note： DNS サーバーについて

DNS サーバーを設定することによって、Azure 上に構築した仮想マシンに DNS サーバーの設定が DHCP で払い出しされます。DNS サーバーの IP アドレスが決まっていない場合は、後から設定することも可能です。

7. 「仮想ネットワークの作成 – サイト間接続」が表示されます。

次に「名前」「VPN デバイスの IP アドレス」「開始 IP」を入力し、「CIDR(アドレス数)」を選択します。

今回は「名前」に「local-nw」、「アドレス空間」に「192.168.118.0」を入力し、「CIDR(アドレス数)」は「/24(256)」を選択します。

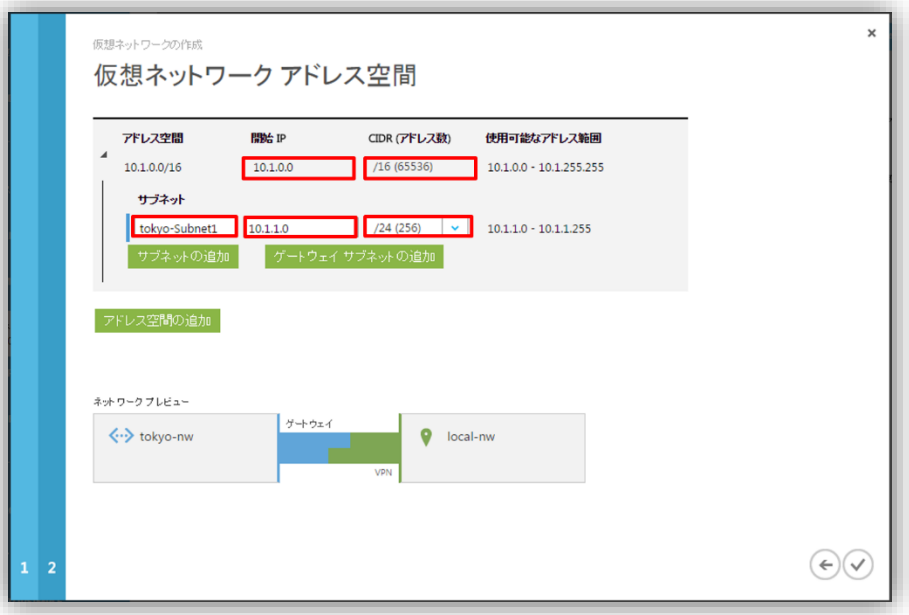
※「VPN デバイスの IP アドレス」については、ISP より払い出されたグローバル固定 IP アドレスを入力してください。入力および選択が終わったら、右下の「→」をクリックします。

8. 「仮想ネットワークの作成 – 仮想ネットワーク アドレス空間」が表示されます。

次に「アドレス空間の開始 IP」「サブネットの名前」「サブネットの開始 IP」を入力し、「アドレス空間の CIDR(アドレス数)」「サブネットの CIDR(アドレス数)」を選択します。

今回は「アドレス空間の開始 IP」に「10.1.0.0」と入力し、「アドレス空間の CIDR(アドレス数)」に「/16(65531)」を選択します。

続けて、「サブネットの名前」に「tokyo-Subnet1」、「サブネットの開始 IP」に「10.1.1.0」と入力し、「サブネットの CIDR(アドレス数)」に「/24(256)」を選択します。

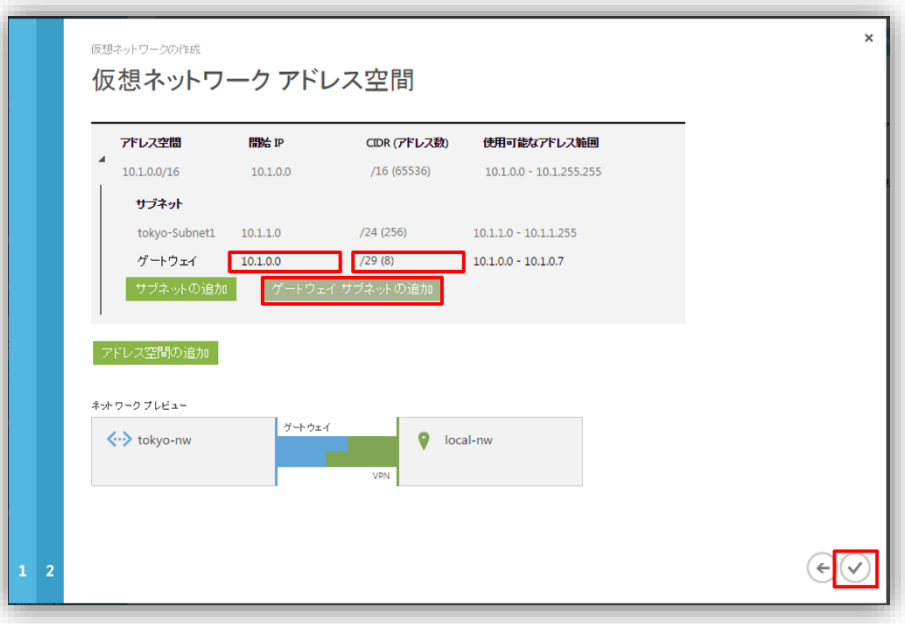


9. 続けて「ゲートウェイサブネットの追加」をクリックします。

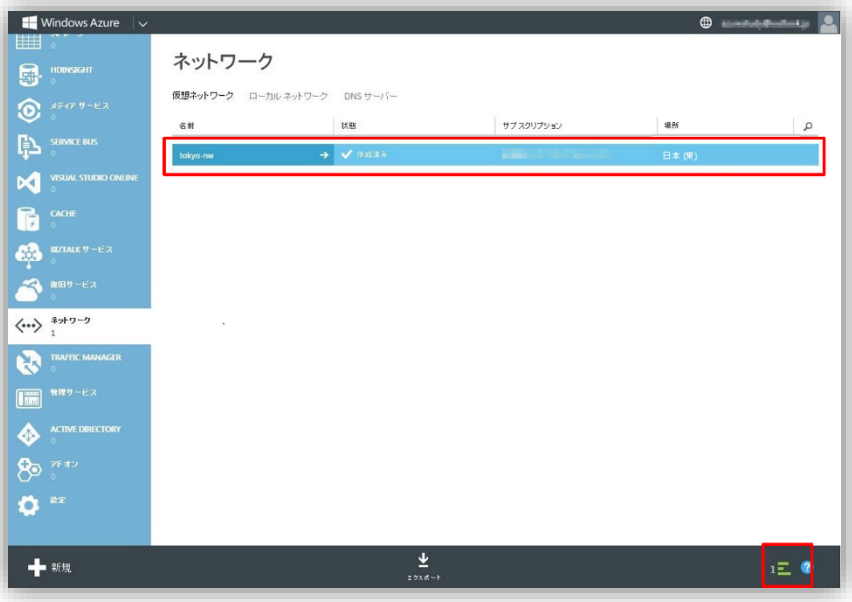
サブネットの行に「ゲートウェイ」が追加されますので、「ゲートウェイの開始 IP」を入力し、「ゲートウェイの CIDR(アドレス数)」を選択します。

今回はデフォルト値を使用します。

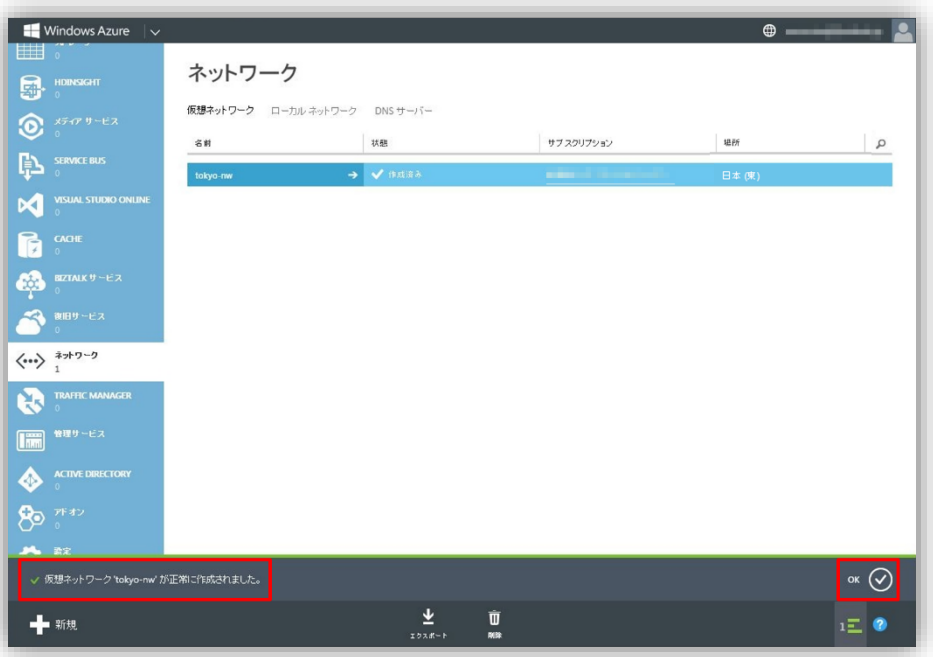
入力および選択が終わったら、右下のチェックをクリックします。



10. 「ネットワーク – 仮想ネットワーク」に戻ります。作成中の仮想ネットワークがリストに表示されます。この段階ではまだ作成は完了していません。右下に作成中であることを示すアイコンが表示されます。



11. 「仮想ネットワーク “tokyo-nw“ が正常に作成されました」のメッセージが表示されたら、チェックをクリックしてメッセージをクリアします。



STEP 5. 仮想ゲートウェイの作成

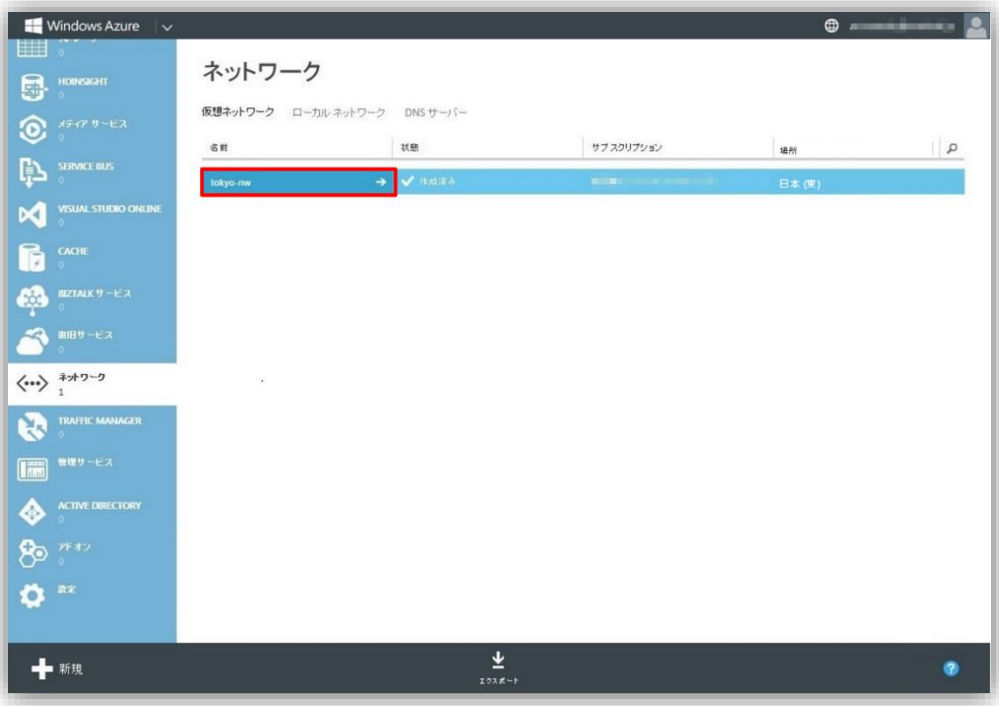
この STEP では、仮想ネットワークの作成手順について説明します。

この STEP では、次のことを学習します。

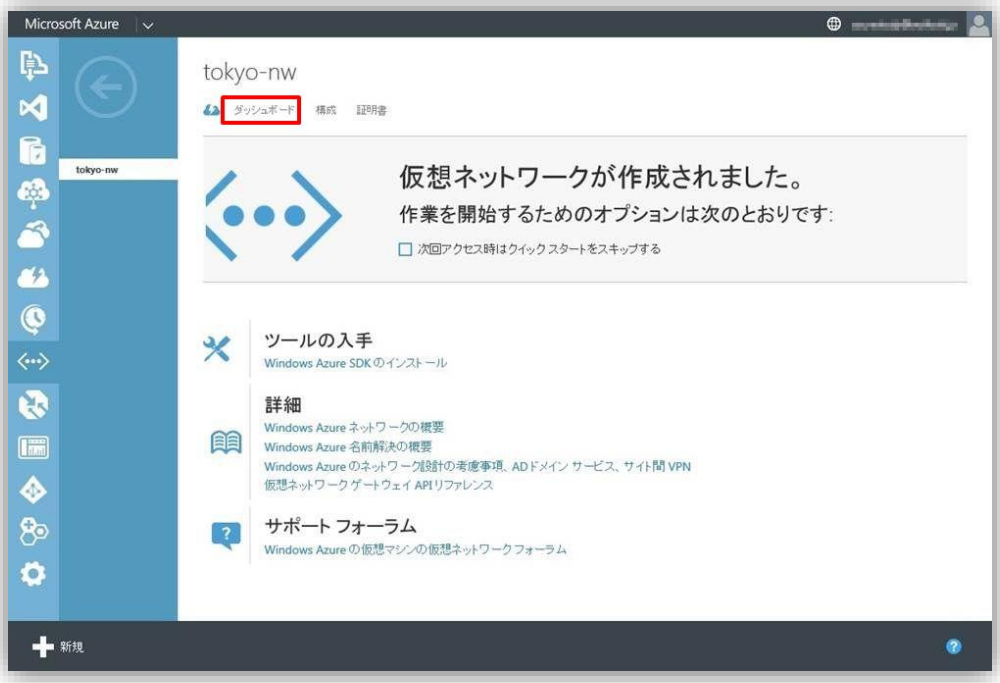
✓ 仮想ゲートウェイの作成

5.1 仮想ゲートウェイの作成

1. 作成した「tokyo-nw」をクリックします。

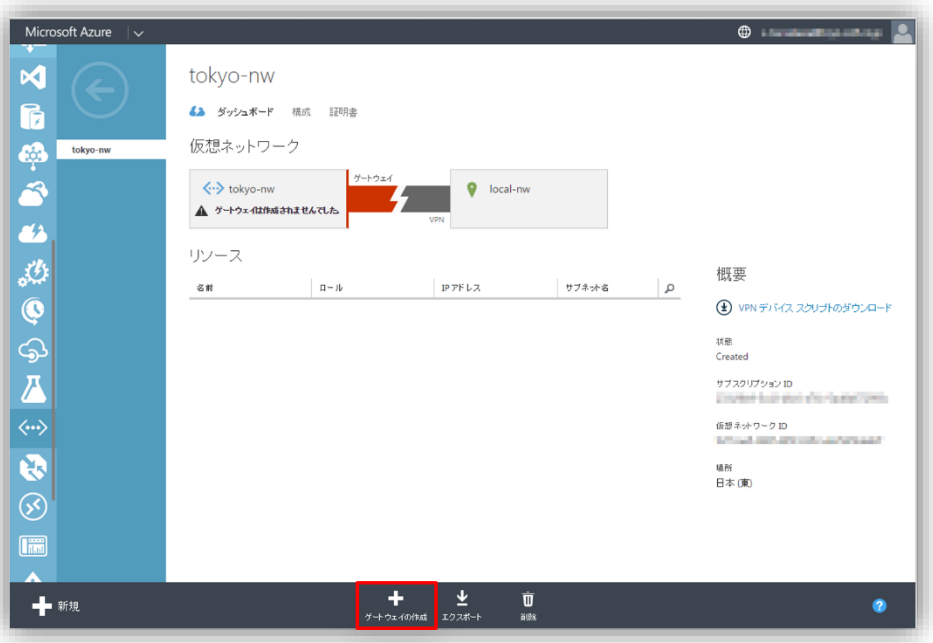


2. 「クイックスタート」が表示されます。次に「ダッシュボード」をクリックします。



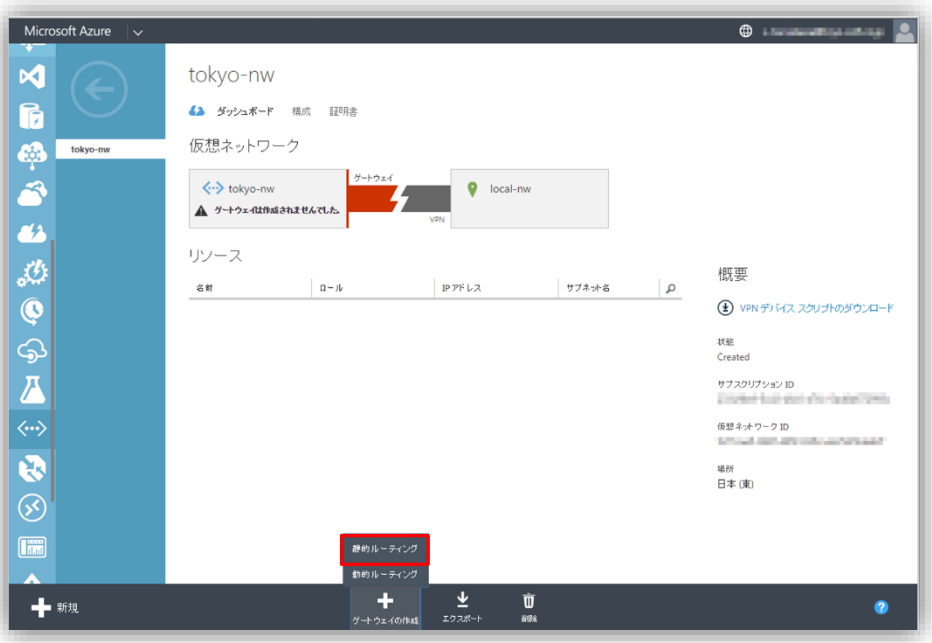
3. 「ダッシュボード」が表示されます。

次に画面下部の「ゲートウェイの作成」をクリックします。

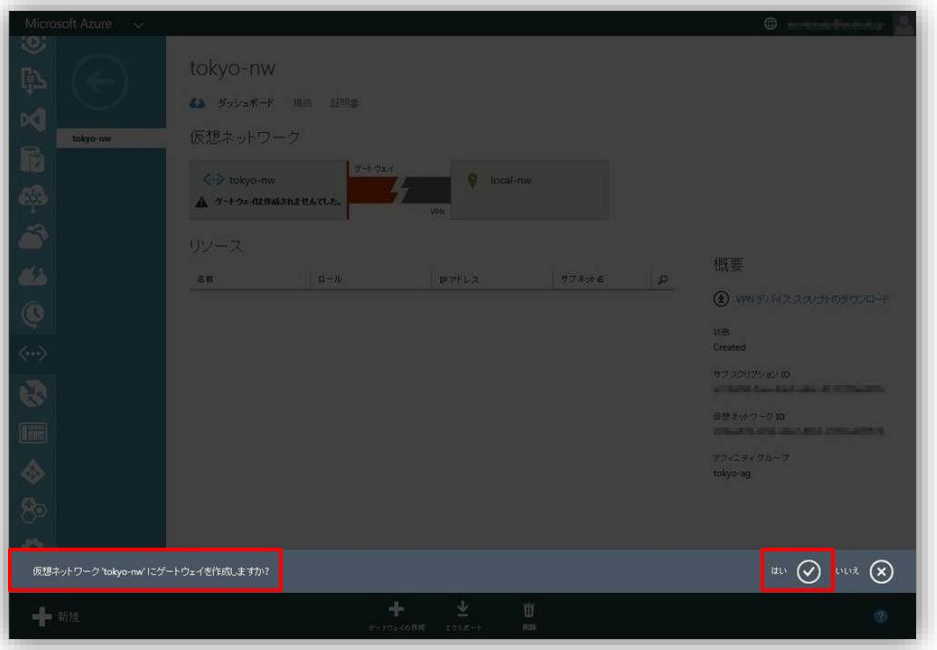


4. 「静的ルーティング/動的ルーティング」のリストが表示されます。

今回は「静的ルーティング」をクリックします。



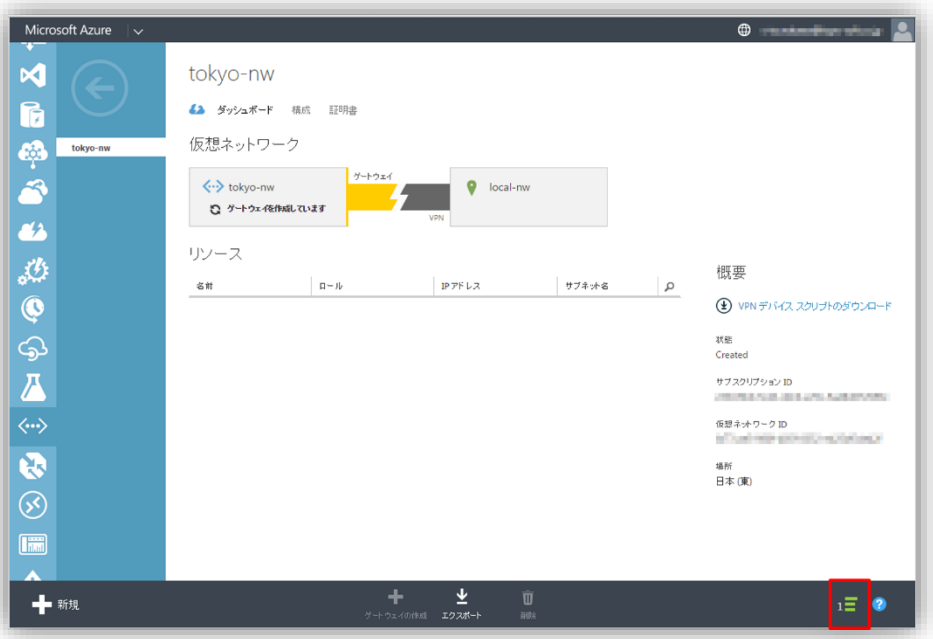
5. 「仮想ネットワーク ”tokyo-nw” にゲートウェイを作成しますか？」のメッセージが表示されます。 「はい」をクリックします。



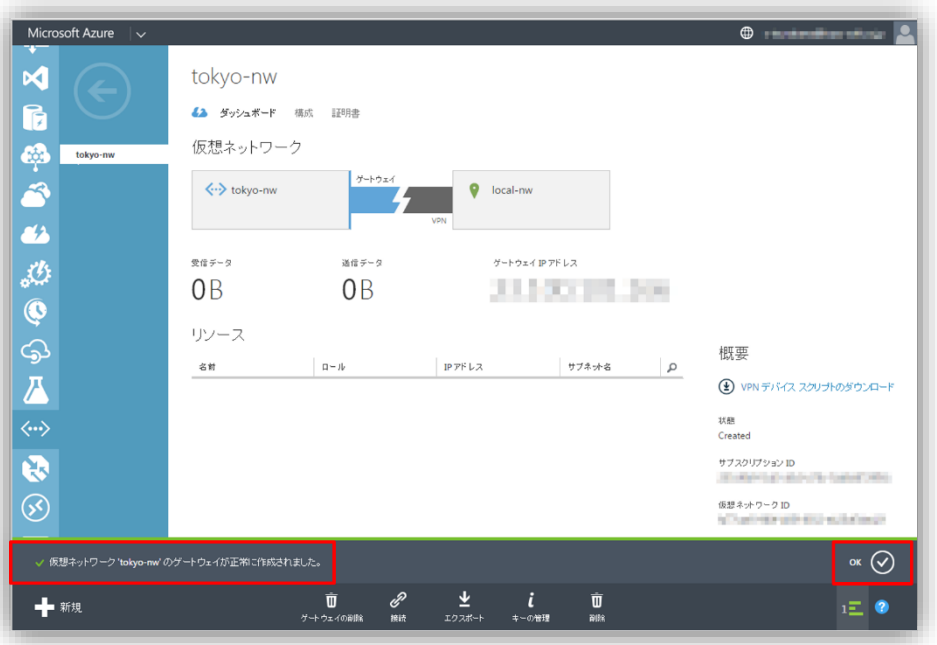
6. 「ダッシュボード」に戻ります。

この段階ではまだ作成は完了していません。右下に作成中であることを示すアイコンが表示されます。

※ 仮想ゲートウェイの作成完了には約 10 分かかります。



7. 「仮想ネットワーク “tokyo-nw“ のゲートウェイが正常に作成されました」のメッセージが表示されたら、チェックをクリックしてメッセージをクリアします。



STEP 6. 仮想ゲートウェイの IP アドレスと共有キーの確認

この STEP では、仮想ゲートウェイの IP アドレスと共有キーの確認について説明します。

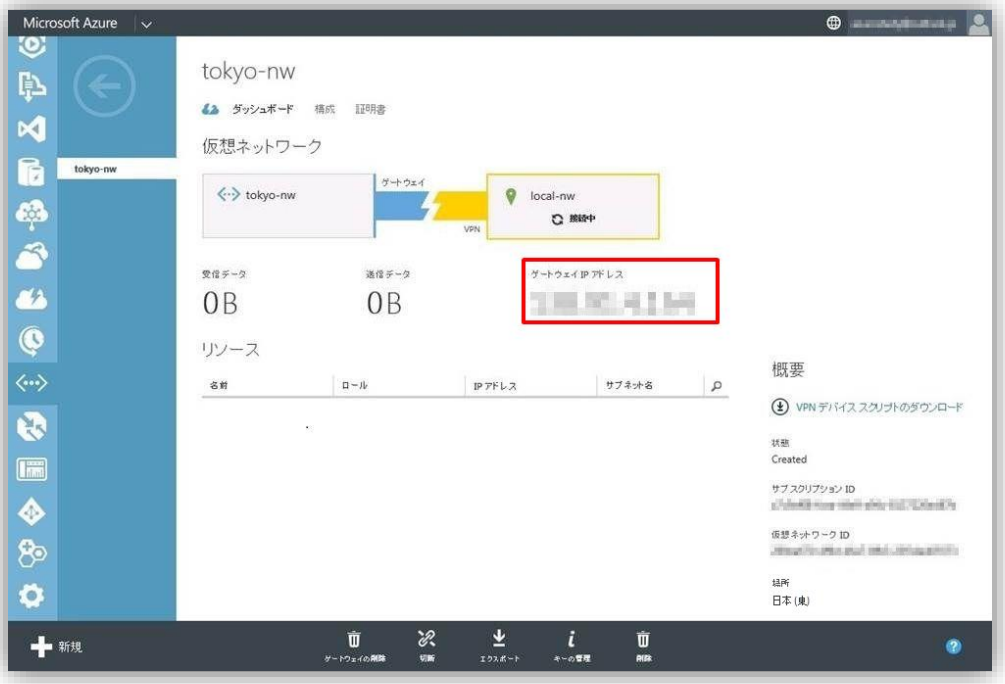
この STEP では、次のことを学習します。

- ✓ 仮想ゲートウェイの IP アドレスの確認
- ✓ 共有キーの確認

6.1 仮想ゲートウェイの IP アドレスの確認

ASA に設定する、仮想ゲートウェイの IP アドレスを確認します。

1. 「仮想ネットワーク > tokyo-nw > ダッシュボード」から確認できます。

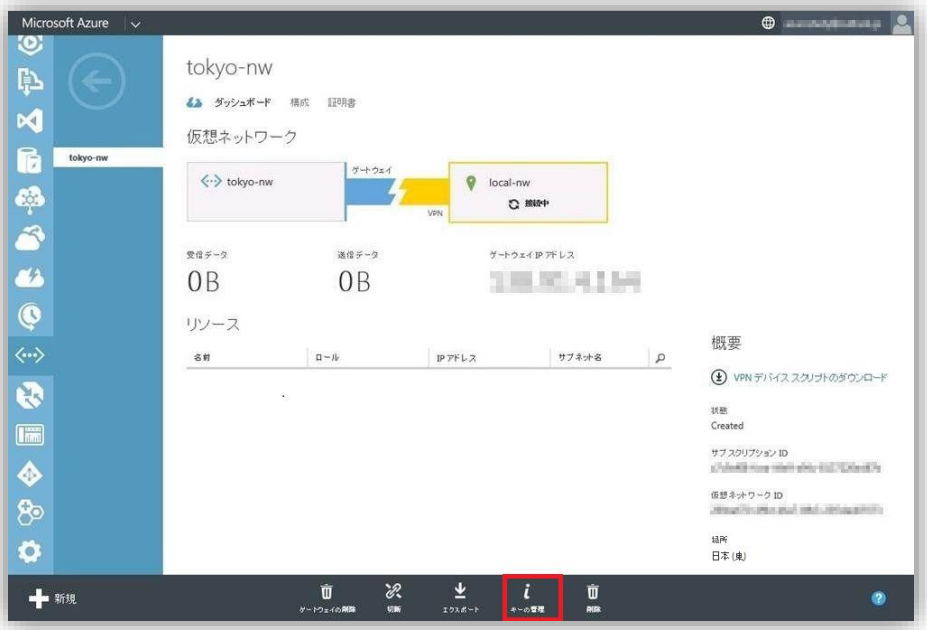


6.2 共有キーの確認

VPN 通信に必要となる共有キーを取得します。

1. 「仮想ネットワーク > tokyo-nw > ダッシュボード」を開きます。

次に画面下部の「キーの管理」をクリックします。



2. 「共有キーの管理」が表示されます。

表示された共有キーをコピーし、右下のチェックをクリックして閉じます。

STEP 7. ASA の設定

この STEP では、ASA の設定手順について説明します。

この STEP では、次のことを学習します。

- ✓ 作成に必要なパラメーター
- ✓ ASA に投入するコマンド
- ✓ Config 例

7.1 作成に必要なパラメーター

ASA の設定に必要なパラメーターは以下の通りです。

※今回のシナリオに基づく一例であり、構築する環境によって異なりますのでご注意ください。

※ASA の操作方法については Cisco 社の情報をご確認願います。

名前	詳細	今回設定する値
WAN 側 I/F の vlanID	任意の ID 番号	10
WAN 側 I/F の IP アドレス	ISP から払い出された固定グローバル IP アドレス	xxx.xxx.xxx.xxx
ISP への接続情報	ユーザー名、パスワード	ユーザー名 xxxxxx@xxx.xxx.jp パスワード xxxxxxxxxx
LAN 側 I/F の IP アドレス	該当のセグメント上の IP アドレス	192.168.118.200 255.255.255.0
LAN 側の VPN 接続セグメント	該当のセグメント	192.168.118.0 255.255.255.0
Azure 側の VPN 接続サブネット	該当のサブネット	10.1.0.0 255.255.0.0
仮想ゲートウェイの IP アドレス	STEP 7 で確認したアドレス	yyy.yyy.yyy.yyy
共有キー	STEP 7 で確認した共有キー	zzzzzzzzzz

7.2 ASA に投入するコマンド

I/F 設定

今回は Ethernet0/0 を WAN 側として vlan10 を設定し、それ以外を LAN 側として使用します。

(物理 I/F はデフォルトで vlan1 が割り当てられているため、LAN 側物理 I/F の設定は不要です)

※ 使用する物理 I/F が shutdown されている場合は、適宜 no shutdown コマンドを実施してください。

vlan1 には LAN 側の IP アドレス「192.168.118.200/-255.255.255.0」を設定し、vlan10 には WAN 側(ISP)の固定グローバル IP アドレスを設定します。

※ WAN 側の設定は ISP の契約内容や NW 構成などにより異なります。

1. まず WAN 側物理 I/F に割り当てる vlan10 を設定します。

```
Ciscoasa(config)# interface vlan 10
Ciscoasa(config-if)# nameif outside
Ciscoasa(config-if)# security-level 0
Ciscoasa(config-if)#ip address xxx.xxx.xxx.xxx 255.255.255.255 pppoe setroute
Ciscoasa(config-if)#no shutdown
Ciscoasa(config-if)#exit
Ciscoasa(config)#
```

ISP から払い出された固定グローバル IP アドレス

2. 次に vlan10 を WAN 側物理 I/F に割り当てます。

```
Ciscoasa(config)# interface Ethernet0/0
Ciscoasa(config-if)# switchport access vlan 10
Ciscoasa(config-if)#exit
Ciscoasa(config)#
```

3. ISP に接続するための設定をします。

```
Ciscoasa(config)#vpdn group pppoe request dialout pppoe
Ciscoasa(config)#vpdn group pppoe localname xxxxxx@xxx.xxx.jp
Ciscoasa(config)#vpdn group pppoe ppp authentication pap
Ciscoasa(config)#vpdn username xxxxxx@xxx.xxx.jp password xxxxxxxxxx
```

ISP の接続情報(ユーザー名、パスワード)
ユーザー名は 2 行目と 4 行目に同じものを使います

4. LAN 側 I/F(vlan1)の設定をします。

```
Ciscoasa(config)# interface vlan 1
Ciscoasa(config-if)#nameif inside
Ciscoasa(config-if)#security-level 100
Ciscoasa(config-if)#ip address 192.168.118.200 255.255.255.0
Ciscoasa(config-if)#no shutdown
Ciscoasa(config-if)#exit
Ciscoasa(config)#
```

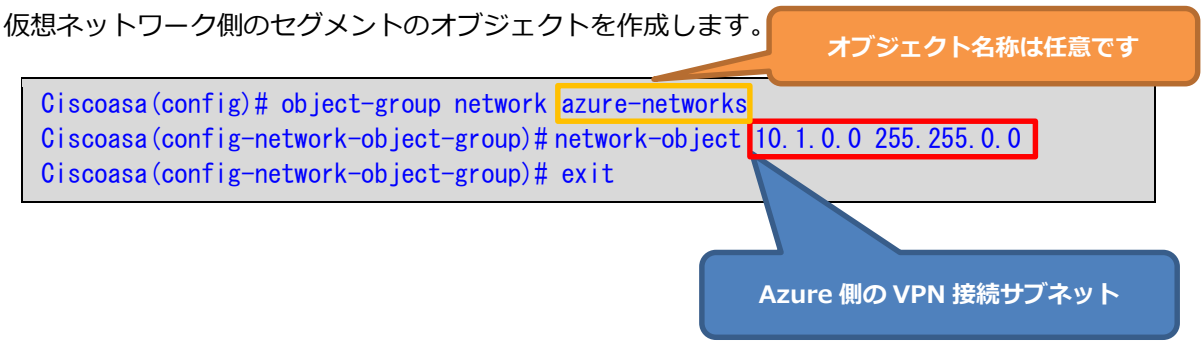
LAN 側 I/F の IP アドレス

VPN 設定

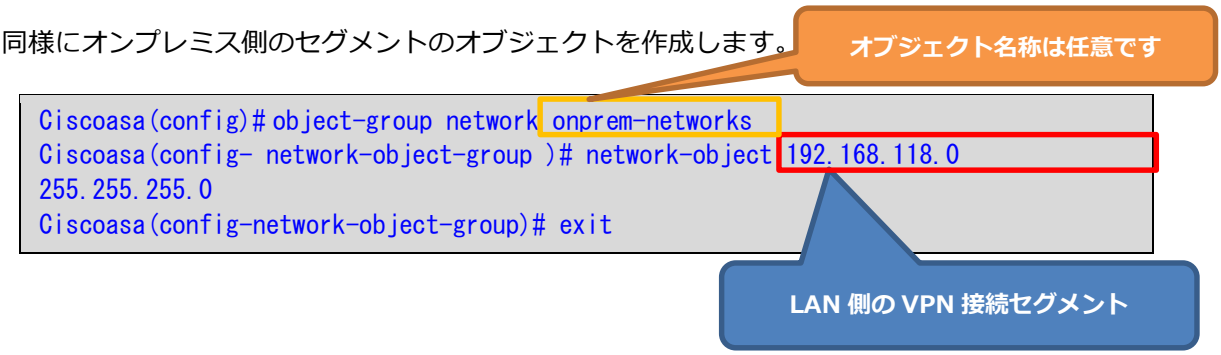
以下の設定を追加します。

1. VPN 間通信のための ACL と NAT の設定

   仮想ネットワーク側のセグメントのオブジェクトを作成します。



2. 同様にオンプレミス側のセグメントのオブジェクトを作成します。



3. 作成したオブジェクトをパラメーターにして、VPN 通信の許可設定をします。

```
Ciscoasa(config)# access-list azure-vpn-acl extended permit ip object-group
onprem-networks object-group azure-networks
```

4. 同様に NAT の設定をします。

```
Ciscoasa(config)# nat (inside,outside) source static onprem-networks onprem-
networks destination static azure-networks azure-networks
```

5. IKE フェーズ 1 の設定をします。

```
Ciscoasa(config)#crypto ikev1 enable outside
Ciscoasa(config)#crypto ikev1 policy 10
Ciscoasa(config-ikev1-policy)# authentication pre-share
Ciscoasa(config-ikev1-policy)# encryption aes-256
Ciscoasa(config-ikev1-policy)# hash sha
Ciscoasa(config-ikev1-policy)# group 2
Ciscoasa(config-ikev1-policy)# lifetime 28800
Ciscoasa(config-ikev1-policy)# exit
```

6. IKE フェーズ 2 の設定をします。

```
Ciscoasa(config)#crypto ipsec ikev1 transform-set azure-ipsec-proposal-set esp-
aes-256 esp-sha-hmac
Ciscoasa(config)#crypto ipsec security-association lifetime seconds 3600
Ciscoasa(config)#crypto ipsec security-association lifetime kilobytes 102400000
```

7. 暗号マップの設定をします。

```
Ciscoasa(config)#crypto map azure-crypto-map 10 match address azure-vpn-acl
Ciscoasa(config)#crypto map azure-crypto-map 10 set peer yyy.yyy.yyy.yyy
Ciscoasa(config)#crypto map azure-crypto-map 10 set ikev1 transform-set azure-
ipsec-proposal-set
Ciscoasa(config)#crypto map azure-crypto-map interface outside
```

8. トンネル設定をします。

```
Ciscoasa(config)# tunnel-group yyy.yyy.yyy.yyy type ipsec-l2l
Ciscoasa(config)# tunnel-group yyy.yyy.yyy.yyy ipsec-attributes
Ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key zzzzzzzzzz
```

9. TCP MMS(最大セグメントサイズ)の設定をします。

```
Ciscoasa(config)#sysopt connection tcpmss 1350
```

※ その他の設定については、環境により異なりますので、Cisco 社の情報をご確認ください。

7.3 Config 例

ASA の Config 例を以下に示します。
※VPN 接続に関する設定以外の部分については、Cisco 社の情報を確認してください。

```
sh conf
: Saved
: Written by enable_15 at 00:00:00.000 JST Sun Jun 1 20xx
!
ASA Version 8.4(4)1
!
hostname ciscoasa
enable password abcdefghijklmn encrypted
passwd abcdefghijklmn encrypted
names
!
interface Ethernet0/0
 switchport access vlan 10
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.118.200 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 pppoe client vpdn group pppoe
 ip address xxx.xxx.xxx.xxx 255.255.255.255 pppoe setroute
!
ftp mode passive
clock timezone JST 9
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object-group network azure-networks
 network-object 10.1.0.0 255.255.0.0
object-group network onprem-networks
```

```
 network-object 192.168.118.0 255.255.255.0
access-list azure-vpn-acl extended permit ip object-group onprem-networks object-group
azure-networks
no pager
logging asdm informational
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (inside,outside) source static onprem-networks onprem-networks destination static
azure-networks azure-networks
!
object network obj_any
 nat (inside,outside) dynamic interface
!
nat (inside,outside) after-auto source dynamic any interface
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 192.168.118.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
sysopt connection tcpmss 1350
crypto ipsec ikev1 transform-set azure-ipsec-proposal-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec security-association lifetime kilobytes 102400000
crypto map azure-crypto-map 10 match address azure-vpn-acl
crypto map azure-crypto-map 10 set peer yyy.yyy.yyy.yyy
crypto map azure-crypto-map 10 set ikev1 transform-set azure-ipsec-proposal-set
crypto map azure-crypto-map interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 28800
telnet 192.168.118.0 255.255.255.0 inside
telnet timeout 5
ssh 192.168.118.0 255.255.255.0 inside
ssh timeout 60
ssh key-exchange group dh-group1-sha1
console timeout 0
```

```
vpdn group pppoe request dialout pppoe
vpdn group pppoe localname xxxxxx@xxx.xxx.jp
vpdn group pppoe ppp authentication pap
vpdn username  xxxxxx@xxx.xxx.jp  password xxxxxxxxxx

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
tunnel-group yyy.yyy.yyy.yyy type ipsec-l2l
tunnel-group yyy.yyy.yyy.yyy ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:1dd952a70e1d7fbe14f3459242907575
ciscoasa#
```

設定した共有キーは非表示化され「*****」となります

STEP 8. 接続状態の確認

この STEP では、VPN 接続状態の確認手順について説明します。

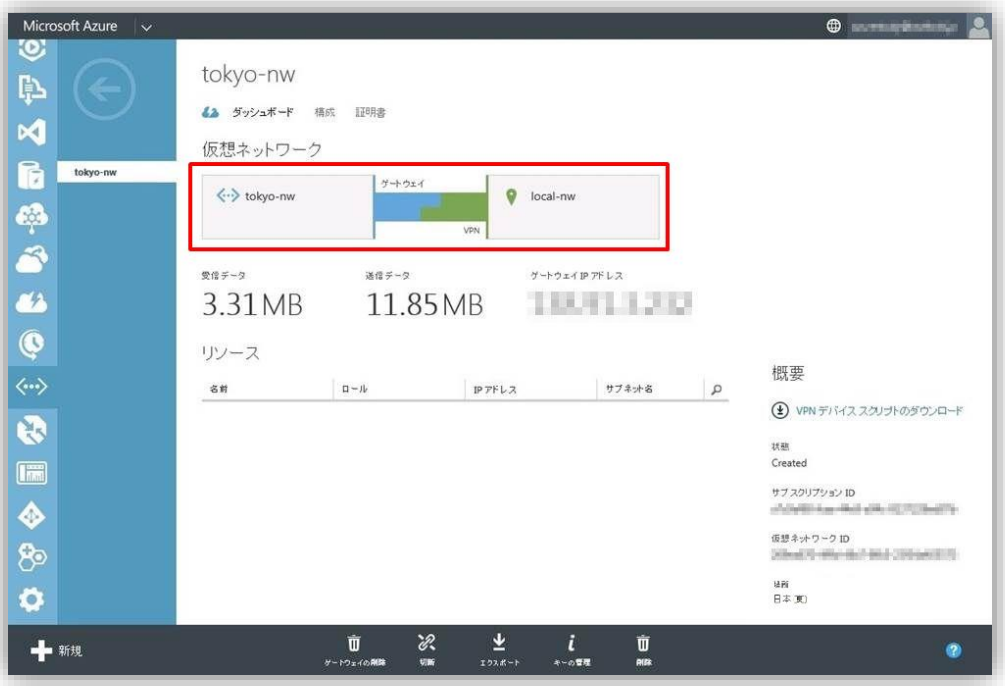
この STEP では、次のことを学習します。

- ✓ Azure 管理ポータル上で接続状態の確認
- ✓ ASA の接続状態の確認

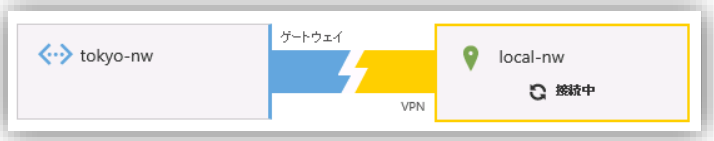
8.1 Azure 管理ポータル上で接続状態の確認

「仮想ネットワーク > tokyo-nw > ダッシュボード」を開き、仮想ネットワークの状態を確認します。

以下のように、仮想ネットワークとローカルネットワークが繋がっていれば、VPN 接続されている状態です。



VPN 接続されていない場合は、以下のようになります。



※ VPN デバイスを接続した直後は状態が更新されないことがありますので、少し時間をおいてから再度確認してください。また、状態が更新されない場合はブラウザの再読み込み(Ctrl＋F5)を試してください。

8.2 ASA の接続状態の確認

ASA から接続状態の確認を行うには、特権モードで「sh isakmp sa」コマンドを実行します。

実行結果の「State」の部分が「MM_ACTIVE」となっていれば、VPN 接続されている状態です。

```
ciscoasa# sh isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: yyy.yyy.yyy.yyy
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

(コマンド実行例)

※State が MM_ACTIVE でない場合は、以下を確認してください。

- 設定が正しいか…Config の再確認
- I/F の状態…物理 I/F・論理 I/F ともに up になっているか、I/F でエラーが発生していないか
- インターネット接続の状態…プロバイダ情報の確認、インターネット向けに ping が通るか

  ※ 仮想ゲートウェイの IP アドレスは ping 応答しません
- ログの確認…IPSEC 関連のログに異常がないか

  ※ 接続に成功した場合、「PHASE 1 COMPLETED」「PHASE 2 COMPLETED」といったログが出力されます

おわりに

この自習書では、仮想ネットワークとオンプレミス間を VPN 接続する環境の構築について学習しました。

仮想ネットワーク上のサーバーに VPN 経由で接続することで、セキュリティを確保しつつクラウドのメリットを得ることができます。

なお、Azure にサーバーを構築するために、以下の自習書についてもご参考ください。

- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、Active Directory、ファイルサーバー連携」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携」

この自習書が仮想ネットワークを利用する手助けになれば幸いです。

執筆者プロフィール

Cloudlive 株式会社（http://www.cloudlive.jp/）

Cloudlive

皆様が Microsoft Azure の恩恵を受け、最大限に活用できるよう、支援することをミッションとした企業です。24/365 の運用監視や、各種コンサルティング、開発支援を行っています。
Azure の 2008 年プレビュー時から、Azure 事業に取り組んでおり、Windows, Linux ともに日本 TOP のノウハウと実績を持ちます。Microsoft Azure MVP 経験者が 4 名在籍しており、Microsoft 本社へフィードバックや情報交換も頻繁に行うとともに、変化の速いクラウド業界において最新のノウハウを提供します。お困りの点がありましたら、ぜひご相談ください。本書に対する感想や、ご意見もお待ちしています。