Microsoft Azure クラウドへの ASA 仮想 の導入

Microsoft Azure クラウドに ASA 仮想 を導入できます。

重要 9.13(1) 以降では、サポートされているすべての ASA 仮想 vCPU/メモリ構成ですべての ASA 仮想 ライセンスを使用できるようになりました。これにより、ASA 仮想 を使用しているお客様は、さまざまな VM リソースフットプリントで実行できるようになります。また、サポート対象の Azure インスタンスタイプの数も増えます。

概要

ASA 仮想 のニーズに合わせて Azure 仮想マシンの階層とサイズを選択します。すべての ASA 仮想 ライセンスを、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できます。そのため、さまざまな Azure インスタンスタイプで ASA 仮想 を実行できます。

表 *1: Azure* でサポートされているインスタンス タイプ

インスタンス	属性		インターフェイス
	vCPU	メモリ（**GB**）	
D3、D3_v2、DS3、DS3_v2	4	14	4
D4、D4_v2、DS4、DS4_v2	8	28	8
D5、D5_v2、DS5、DS5_v2	16	72	8
D8_v3	8	32	4
D16_v3	16	64	4
D8s_v3	8	32	4
D16s_v3	16	64	8
F4、F4s	4	8	4
F8、F8s	8	16	8
F16、F16s	16	32	8
F8s_v2	8	16	4
F16s_v2	16	32	8
Standard_D8_v4	8	32	4
Standard_D16_v4	16	64	8
Standard_D8s_v4	8	32	4
Standard_D16s_v4	16	64	8
Standard_D8_v5	8	32	4
Standard_D16_v5	16	64	8
Standard_D8s_v5	8	32	4
Standard_D16s_v5	16	64	8

表 *2 : ASA* 仮想 権限付与に基づくライセンス機能の制限

パフォーマンス階層	インスタンスタイプ（コア/RAM）	レート制限（Rate Limit）	RA VPN セッション制限
ASAv5	D3_v2 4 コア/14 GB	100 Mbps	50
ASAv10	D3_v2 4 コア/14 GB	1 Gbps	250
ASAv30	D3_v2 4 コア/14 GB	[2 Gbps]	750
ASAv50	D4_v2 8 コア/28 GB	5.5 Gbps	10,000
ASAv100	D5_v2 16 コア/56 GB	11 Gbps	20,000

次の方法で Microsoft Azure に ASA 仮想 を導入できます。

- 標準的な Azure パブリック クラウドおよび Azure Government 環境で、Azure Resource Manager を使用してスタンドアロン ファイアウォールとして導入
- Azure Security Center を使用して統合パートナー ソリューションとして導入
- 標準的な Azure パブリック クラウドおよび Azure Government 環境で、Azure Resource Manager を使用してハイ アベイラビリティ（HA）ペアとして導入

（注） ASA 仮想の HA セットアップで予期しないフェールオーバーが発生した場合は、ASA 仮想 ピアインスタンスまたは Azure サービスとの通信で短時間の中断が発生していないか、 ログを確認します。このようなフェールオーバーが発生した場合は、DHCP を介して IP アドレスを割り当てるのではなく、管理インターフェイスに静的 IP アドレスを設定することを推奨します。

「Azure Resource Manager からの ASA 仮想 の導入 （14 ページ）」を参照してください。標準的な Azure パブリッククラウドおよび Azure Government 環境で ASA 仮想 HA 構成を導入できます。

前提条件

- Azure.com でアカウントを作成します。

Microsoft Azure でアカウントを作成したら、ログインして、Microsoft Azure Marketplace 内で ASA 仮想 を選択し、ASA 仮想 を導入できます。

- ASA 仮想 へのライセンス付与。

  ASA 仮想 にライセンスを付与するまでは、100 回の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。「Smart Software Licensing for the ASA 仮想」を参照してください。

（注） Azure に導入する場合、ASA 仮想 にはデフォルトで 2Gbps の権限が付与されています。100Mbps および 1Gbps の権限付与を使用できます。ただし、100Mbps または 1Gbps の権限付与を使用できるように、スループットレベルを明示的に設定する必要があります。

- インターフェイスの要件：

  4 つのネットワーク上の 4 つのインターフェイスとともに ASA 仮想 を導入する必要があります。任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、パブリック IP アドレス [英語] を参照してください。

- 管理インターフェイス：

  Azure では、最初に定義されたインターフェイスが常に管理インターフェイスです。

（注） IPv6 導入の場合、VNet およびサブネットの作成時に IPv6 を設定します。

- 通信パス：
  - 管理インターフェイス：SSH アクセス、および ASA 仮想 を ASDM に接続するために使用されます。

（注） Azure Accelerated Networking は、管理インターフェイスではサポートされていません。

  - 内部インターフェイス（必須）：内部ホストに ASA 仮想 を接続するために使用されます。
  - 外部インターフェイス（必須）：ASA 仮想 をパブリック ネットワークに接続するために使用されます。
  - DMZ インターフェイス（任意）：Standard_D3 インターフェイスを使用する場合に、ASA 仮想 を DMZ ネットワークに接続するために使用されます。

- ASA 仮想 ハイパーバイザおよび仮想プラットフォームのサポート情報については、Cisco Secure Firewall ASA の互換性 [英語] を参照してください。

注意事項と制約事項

サポートされる機能

- Microsoft Azure クラウドからの導入
- Azure Accelerated Networking（AN）
- 選択したインスタンスタイプに基づく最大 16 個の vCPU

（注） Azure では L2 vSwitch 機能は設定できません。

- インターフェイスのパブリック IP アドレス

  任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、パブリック IP アドレス [英語] を参照してください。

- ルーテッド ファイアウォール モード（デフォルト）

（注） ルーテッド ファイアウォール モードでは、ASA 仮想 はネットワーク内の従来のレイヤ 3 境界となります。このモードには、各インターフェイスの IP アドレスが必要です。Azure は VLAN タグ付きインターフェイスをサポートしていないため、IP アドレスはタグなしのトランク以外のインターフェイスで設定する必要があります。

- IPv6

Azure DDoS Protection 機能

Microsoft Azure の Azure DDoS Protection は、ASA 仮想 の最前線に実装された追加機能です。仮想ネットワークでこの機能を有効にすると、ネットワークで予想されるトラフィックの 1 秒あたりのパケット数に応じて、一般的なネットワーク層攻撃からアプリケーションを保護するのに役立ちます。この機能は、ネットワーク トラフィック パターンに基づいてカスタマイズできます。

Azure DDoS Protection 機能の詳細については、『Azure DDoS Protection Standard overview』[英語] を参照してください。

パスワードの設定

設定したパスワードが次のガイドラインに準拠していることを確認します。パスワードは、以下のルールに従う必要があります。

- 12 文字以上 72 文字以下の英数字文字列である必要があります。
- 小文字と大文字、数字、および「\」、「-」以外の特殊文字で構成されます。
- ASCII 文字を 3 文字以上繰り返す、または連続して使用することはできません。
- ディクショナリで使用されている単語は使用しないでください。

次に示すような展開の問題が発生した場合や、起動ログにその他のパスワード関連のエラーが見つかった場合は、設定したパスワードがパスワードの複雑さに関するガイドラインに準拠しているかどうかを確認する必要があります。

展開エラー

- `OS Provisioning failed for VM 'TEST-CISCO-TDV-QC' due to an internal error. (Code: OSProvisioningInternal Error)`
- `OS Provisioning failed for VM 'TEST-CISCO-ASAVM' due to an internal error. InternalDetail: RoleInstanceContainerProvisioningDetails: MediaStorageAccountName:ProvisionVmWithUpdate; MediaStorageHostName:ProvisionVmWithUpdate; MediaRelativeUrl:ProvisionVmWithUpdate; MediaTenantSecretId:00000000-0000-0000-0000-000000000000; ProvisioningResult:Failure; ProvisioningResultMessage:[ProtocolError] [CopyOvfEnv] Error mounting dvd: [OSUtilError] Failed to mount dvd device Inner error: [mount -o ro -t udf,iso9660 /dev/hdc /mnt/cdrom/secure] returned 32: mount: /mnt/cdrom/secure: no medium found on /dev/hdc`

シリアルコンソールログを参照することで、これらのパスワード関連のエラーを確認および再確認できます。次に、シリアルコンソールログからのエラーの詳細の例を示します。

```
10150 bytes copied in 0.80 secs
Waagent - 2024-08-02T00:46:55.889400Z INFO Daemon Create user account if not exists
Waagent - 2024-08-02100:46:55.890685Z INFO Daemon Set user password.
ERROR: Password must contain:
ERROR: a value that has less than 3 repetitive or sequential ASCII characters.
Invalid Eg:aaaauser, user4321, aaabc789
Failed to add username "cisco"
ADD_USER reply indicates failure
```

既知の問題

アイドル タイムアウト

Azure 上の ASA 仮想 には、VM で設定可能なアイドルタイムアウトがあります。最小設定値は 4 分、最大設定値は 30 分です。ただし、SSH セッションでは最小設定値は 5 分、最大設定値は 60 分です。

（注） ASA 仮想 のアイドルタイムアウトにより、SSH タイムアウトは常に上書きされ、セッションが切断されることに注意してください。セッションがどちらの側からもタイムアウトしないように、VM のアイドルタイムアウトを SSH タイムアウトに合わせることができます。

プライマリ ASA 仮想 からスタンバイ ASA 仮想 へのフェールオーバー

Azure での ASA 仮想 HA 導入で Azure のアップグレードが発生すると、プライマリ ASA 仮想 からスタンバイ ASA 仮想 へのフェールオーバーが発生する場合があります。Azure のアップグレードにより、プライマリ ASA 仮想 が一時停止状態になります。プライマリ ASA 仮想 が一時停止している場合、スタンバイ ASA 仮想 は hello パケットを受信しません。スタンバイ ASA 仮想 がフェールオーバーホールド時間を経過しても hello パケットを受信しない場合、スタンバイ ASA 仮想 へのフェールオーバーが発生します。

また、フェールオーバーホールド時間を経過していなくてもフェールオーバーが発生する可能性があります。プライマリ ASA 仮想 が一時停止状態に入ってから 19 秒後に再開するシナリオを考えてみましょう。フェールオーバーホールド時間は 30 秒ですが、クロックは約 2 分ごとに同期されるため、スタンバイ ASA 仮想 は正しいタイムスタンプの hello パケットを受信しません。その結果、プライマリ ASA 仮想 からスタンバイ ASA 仮想 へのフェールオーバーが発生します。

（注） この機能は IPv4 のみをサポートし、ASA Virtual HA は IPv6 設定ではサポートされません。

サポートされない機能

- コンソールアクセス（管理は、ネットワーク インターフェイスを介して SSH または ASDM を使用して実行される）
- ユーザー インスタンス インターフェイスの VLAN タギング
- ジャンボ フレーム
- Azure の観点からの、デバイスが所有していない IP アドレスのプロキシ ARP
- 無差別モード（スニファなし、またはトランスペアレント モードのファイアウォールのサポート）

（注） Azure ポリシーでは、インターフェイスは無差別モードでは動作できないため、ASA 仮想 はトランスペアレント ファイアウォール モードでは動作しません。

- マルチ コンテキスト モード
- クラスタ
- ASA 仮想 ネイティブ HA。

（注） ステートレスのアクティブ/バックアップ高可用性（HA）設定で ASA 仮想 を Azure に展開できます。

- VM のインポート/エクスポート
- デフォルトでは、Azureクラウド内で稼働する ASA 仮想 の FIPS モードは無効になっています。

（注） FIPS モードを有効にする場合は、**ssh key-exchange group dh-group14-sha1** コマンドを使用して、Diffie-Helman キー交換グループをより強力なキーに変更する必要があります。Diffie-Helman グループを変更しないと、ASA 仮想 に SSH 接続できなくなるため、グループの変更が、最初に ASA 仮想 を管理する唯一の方法です。

- Azure での Gen 2 VM の生成
- 展開後の VM のサイズ変更
- VM の OS ディスクの Azure ストレージ SKU を Premium から Standard SKU に移行または更新、およびその逆

導入時に作成されるリソース

Azure に ASA 仮想 を展開すると、次のリソースが作成されます。

- ASA 仮想 マシン
- リソース グループ（既存のリソース グループを選択していない場合）

  ASA 仮想 リソースグループは、仮想ネットワークとストレージアカウントで使用するリソースグループと同じである必要があります。

- vm name-Nic0、vm name-Nic1、vm name-Nic2、vm name-Nic3 という名前の 4 つの NIC

  これらの NIC は、それぞれ ASA 仮想 インターフェイスの Management 0/0、GigabitEthernet 0/0、GigabitEthernet 0/1、および GigabitEthernet 0/2 にマッピングされます。

（注） 要件に基づいて、IPv4 のみまたはデュアルスタック（IPv4 および IPv6 が有効）で VNet を作成できます。

- VM 名-SSH-SecurityGroup という名前のセキュリティ グループ

  セキュリティグループは、ASA 仮想 Management 0/0 にマッピングされる VM の Nic0 にアタッチされます。

  セキュリティ グループには、VPN 目的で SSH、UDP ポート 500、および UDP 4500 を許可するルールが含まれます。導入後に、これらの値を変更できます。

- パブリック IP アドレス（展開時に選択した値に従って命名）。

  パブリック IP アドレス（IPv4 のみまたはデュアルスタック（IPv4 および IPv6））。

  任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、「パブリック IP アドレス」を参照してください。

- 4 つのサブネットを備えた仮想ネットワーク（既存のネットワークを選択していない場合）
- サブネットごとのルーティング テーブル（既存の場合は最新のもの）

  このテーブルの名前は、サブネット名-ASAv-RouteTable です。

  各ルーティングテーブルには、ASA 仮想 IP アドレスを持つ他の 3 つのサブネットへのルートがネクストホップとして含まれています。トラフィックを他のサブネットまたはインターネットに到達させる必要がある場合は、デフォルト ルートを追加することもできます。

- 選択したストレージ アカウントの起動時診断ファイル

  起動時診断ファイルは、ブロブ（サイズの大きいバイナリ オブジェクト）内に配置されます。

- 選択したストレージ アカウントのブロブおよびコンテナ VHD にある 2 つのファイル（名前は、*vm name*-disk.vhd および *vm name*-<uuid>.status）
- ストレージ アカウント（既存のストレージ アカウントが選択されていない場合）

（注） VM を削除すると、保持を希望する任意のリソースを除き、これらの各リソースを個別に削除する必要があります。

Azure ルーティング

Azure 仮想ネットワークでのルーティングは、仮想ネットワークの有効なルーティング テーブルによって決まります。有効なルーティング テーブルは、既存のシステム ルーティング テーブルとユーザー定義のルーティング テーブルの組み合わせです。

（注） ASA 仮想 では、Azure クラウドルーティングの特性により、EIGRP や OSPF などのダイナミックな内部ルーティングプロトコルを使用できません。有効なルーティングテーブルは、仮想クライアントにスタティック/ダイナミック ルートが設定されているかどうかに関係なく、ネクスト ホップを決定します。

現在、有効なルーティング テーブルまたはシステム ルーティング テーブルはどちらも表示できません。

ユーザー定義のルーティング テーブルは表示および編集できます。システム テーブルとユーザー定義のテーブルを組み合わせて有効なルーティング テーブルを形成した場合、最も限定的なルート（同位のものを含め）がユーザー定義のルーティング テーブルに含められます。システム ルーティング テーブルには、Azure の仮想ネットワーク インターネット ゲートウェイを指すデフォルト ルート（0.0.0.0/0）が含まれます。また、システム ルーティング テーブルには、Azure の仮想ネットワーク インフラストラクチャ ゲートウェイを指すネクスト ホップとともに、他の定義済みのサブネットへの限定的なルートが含まれます。

ASA 仮想 を介してトラフィックをルーティングするために、ASA 仮想 導入プロセスで、ASA 仮想 をネクストホップとして使用する他の 3 つのサブネットへのルートが各サブネットに追加されます。サブネット上の ASA 仮想 インターフェイスを指すデフォルトルート（0.0.0.0/0）を追加することもできます。これで、サブネットからのトラフィックはすべて ASA 仮想 を介して送信されますが、場合によっては、トラフィックを処理する前に、ASA 仮想 ポリシーを設定する必要があります（通常は NAT/PAT を使用）。

システムルーティングテーブル内の既存の限定的なルートのために、ユーザー定義のルーティングテーブルに、ネクストホップとして ASA 仮想 を指す限定的なルートを追加する必要があります。追加しないと、ユーザー定義のテーブル内のデフォルトルートではなく、システム ルーティング テーブル内のより限定的なルートが選択され、トラフィックは ASA 仮想 をバイパスします。

仮想ネットワーク内の VM のルーティング設定

Azure 仮想ネットワーク内のルーティングは、クライアントの特定なゲートウェイ設定ではなく、有効なルーティングテーブルに依存します。仮想ネットワーク内で稼働するクライアントは、DHCPによって、それぞれのサブネット上の 1 アドレスとなるルートを指定されることがあります。これはプレースホルダで、仮想ネットワークのインフラストラクチャ仮想ゲートウェイにパケットを送信するためにだけ使用されます。パケットは、VM から送信されると、有効なルーティング テーブル（ユーザー定義のテーブルによって変更された）に従ってルーティングされます。有効なルーティング テーブルは、クライアントでゲートウェイが 1 として、または ASA 仮想 アドレスとして設定されているかどうかに関係なく、ネクストホップを決定します。

Azure VM ARP テーブルには、すべての既知のホストに対して同じ MAC アドレス（1234.5678.9abc）が表示されます。これによって、Azure VM からのすべてのパケットが、有効なルーティングテーブルを使用してパケットのパスを決定する Azure ゲートウェイに到達するように保証されます。

（注） ASA 仮想 では、Azure クラウドルーティングの特性により、EIGRP や OSPF などのダイナミックな内部ルーティングプロトコルを使用できません。有効なルーティングテーブルは、仮想クライアントにスタティック/ダイナミック ルートが設定されているかどうかに関係なく、ネクスト ホップを決定します。

（注） IPv6だけを使用して、仮想ネットワーク、サブネット、インターフェースなどを構築することはできません。デフォルトではIPv4が使用され、IPv6も一緒に有効にできます。

IP Addresses

次の情報はAzureのIPアドレスに適用されます。

- ASA仮想インターフェイスのIPアドレスを設定するには、DHCPを使用する必要があります。さらに、DHCPを使用してIPv6アドレスを取得するためには、ASA仮想の最初のNICにマッピングされるManagement 0/0が**必要です**。

  Azureインフラストラクチャは、Azureに設定されたIPアドレスが確実にASA仮想インターフェイスに割り当てられるように動作します。

- Management 0/0には、それが接続されているサブネット内のプライベートIPアドレスが割り当てられます。

  パブリックIPアドレスは、プライベートIPアドレスに関連付けられる場合があり、Azureインターネット ゲートウェイはNAT変換を処理します。

- 任意のインターフェイスにパブリックIPアドレスを割り当てることができます。

- 仮想マシンスケールセット（VMSS）のASA仮想アプライアンスに接続されているネットワーク インターフェイスで**IP転送**を有効にすることができます。ネットワークトラフィックの宛先がネットワーク インターフェイスで設定されているIPアドレスのいずれでもない場合、このオプションを有効にすると、そのようなネットワークトラフィックが仮想マシンで設定されているIPアドレス以外の他のIPアドレスに転送されます。ネットワーク インターフェイスでIP転送を有効にする方法については、Azureのドキュメント「Enable or disable IP forwarding」を参照してください。

- ダイナミック パブリックIPアドレスはAzureの停止/開始サイクル中に変更される場合があります。ただし、Azureの再起動時およびASA仮想のリロード時には、パブリックIPアドレスは保持されます。

- スタティック パブリックIPアドレスはAzure内でそれらを変更するまで変わりません。

DNS

すべてのAzure仮想ネットワークが、次のように使用できる168.63.129.16で、組み込みのDNSサーバーにアクセスできます。

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

この構成は、Smart Licensing を設定し、専用の DNS サーバーをセットアップしていない場合に使用できます。

Accelerated Networking（AN）

Azure の Accelerated Networking（AN）機能により、VM に対するシングルルート I/O 仮想化（SR-IOV）が可能になります。これにより、VM NIC がハイパーバイザをバイパスしてその下の PCIe カードに直接アクセスできるようになり、ネットワークが高速化します。AN は VM のスループットパフォーマンスを大幅に向上させ、コアの追加（つまり VM の拡大）にも対応します。

AN はデフォルトではディセーブルになっています。Azure は、事前プロビジョニングされた仮想マシンでの AN の有効化をサポートしています。Azure で VM を停止し、ネットワークカードのプロパティを更新して *enableAcceleratedNetworking* パラメータを true に設定するだけです。Microsoft のドキュメント『Enable accelerated networking on existing VMs』を参照してください。その後、VM を再起動します。

Mellanox ハードウェアのサポート

Microsoft Azure クラウドには、AN 機能をサポートする Mellanox 4（MLX4）と Mellanox 5（MLX5）の 2 種類のハードウェアがあります。ASA 仮想 は、リリース 9.15 以降の次のインスタンスに対する Mellanox ハードウェアの AN をサポートしています。

- D3、D3_v2、DS3、DS3_v2
- D4、D4_v2、DS4、DS4_v2
- D5、D5_v2、DS5、DS5_v2
- D8_v3、D8s_v3
- D16_v3、D16s_v3
- F4、F4s
- F8、F8s、F8s_v2
- F16、F16s、F16s_v2

（注） MLX4（Mellanox 4）は connectx3 = cx3 とも呼ばれ、MLX5（Mellanox 5）は connectx4 = cx4 とも呼ばれます。

VM の導入に Azure が使用する NIC（MLX4 または MLX5）は指定できません。シスコでは、高速ネットワーキング機能を使用するために、ASA 仮想 9.15 バージョン以降にアップグレードすることを推奨しています。

ASA 仮想 の導入

Microsoft Azure に ASA 仮想 を導入できます。

- 標準的な Azure パブリッククラウドおよび Azure Government 環境で、Azure Resource Manager を使用してスタンドアロン ファイアウォールとして ASA 仮想 を導入します。「Azure Resource Manager からの ASAv の導入」を参照してください。
- Azure Security Center を使用して、Azure 内の統合パートナーソリューションとして ASA 仮想 を導入します。セキュリティを重視するお客様には、Azure ワークロードを保護するためのファイアウォールオプションとして ASA 仮想 が提供されます。セキュリティ イベントとヘルスイベントが単一の統合ダッシュボードからモニターされます。「Azure Security Center からの ASAv の導入」を参照してください。
- Azure Resource Manager を使用して ASA 仮想 高可用性ペアを導入します。冗長性を確保するために、ASA 仮想 をアクティブ/バックアップ高可用性（HA）設定で導入できます。パブリッククラウドでの HA では、アクティブな ASA 仮想 の障害時に、バックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーできるステートレスなアクティブ/バックアップソリューションが実装されます。「Azure Resource Manager からの ASA 仮想 for High Availability の導入 （18 ページ）」を参照してください。
- VHD（cisco.com から入手可能）から管理対象イメージを使用し、カスタムテンプレートで ASA 仮想 または ASA 仮想 高可用性ペアを導入します。シスコでは、圧縮仮想ハードディスク（VHD）を提供しています。この VHD を Azure にアップロードすることで、ASA 仮想 の導入プロセスを簡素化できます。管理対象イメージと 2 つの JSON ファイル（テンプレートファイルおよびパラメータファイル）を使用して、単一の協調操作で ASA 仮想 のすべてのリソースを導入およびプロビジョニングできます。カスタムテンプレートを使用するには、VHD およびリソーステンプレートを使用した Azure からの ASA 仮想 の導入（20 ページ）を参照してください。

（注） マーケットプレイスでシスコのオファーを検索すると、アプリケーションオファーと仮想マシンオファーという、名前は似ているものの、オファーのタイプが異なる 2 つの異なるオファーが見つかる場合があります。

マーケットプレイス展開の場合は、アプリケーションオファーのみを使用します。

マーケットプレイスでは、VMSR（仮想マシンソフトウェア予約）プランを持つ仮想マシンオファーが表示される場合があります。これらは、特にチャネル/リセールのための特定のマルチパーティ プライベート オファー プランであり、通常の展開では無視するべきものです。

アプリケーション マーケットプレイスで利用可能なアプリケーションオファー

- Cisco Secure Firewall ASA Virtual：BYOL と PAYG
- Cisco Secure Firewall ASA Virtual：高可用性ペア：BYOL

Azure Resource Manager からの ASA 仮想 の導入

次の手順は、ASA 仮想 で Microsoft Azure をセットアップする手順の概略を示しています。Azure の設定の詳細な手順については、『Azure を使ってみる』を参照してください。

Azure に ASA 仮想 を導入すると、リソース、パブリック IP アドレス、ルートテーブルなどのさまざまな設定が自動的に生成されます。導入後に、これらの設定をさらに管理できます。たとえば、アイドルタイムアウト値を、デフォルトの短いタイムアウトから変更することができます。

手順

ステップ 1 Azure Resource Manager（ARM）ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 Cisco ASAv のマーケットプレイスを検索し、導入する ASA 仮想 をクリックします。

ステップ 3 基本的な設定を行います。

a) 仮想マシンの名前を入力します。この名前は Azure サブスクリプション内で一意である必要があります。

重要
名前が一意でなく、既存の名前を再使用すると、導入に失敗します。

b) ユーザー名を入力します。

c) 認証タイプとして、[Password] または [SSH public key] を選択します。

[Password] を選択した場合は、パスワードを入力して確定します。パスワードの複雑さに関するガイドラインについては、「パスワードの設定」を参照してください。

d) クラスタとして展開する ASAv を使用している場合は、[ASAv Day 0構成（user-data）（ASAv Day0 configuration (user-data)）] フィールドで基本的な Day 0 構成を作成して詳細を入力します。

Azure で ASAv の day0 構成を作成する方法については、『Deploy a Cluster for the ASA Virtual for the Private Cloud』ガイドの「Configure the ASA Virtual Clustering Using a Day0 Configuration」を参照してください。

e) サブスクリプション タイプを選択します。

f) [Resource group] を選択します。

リソース グループは、仮想ネットワークのリソース グループと同じである必要があります。

g) 場所を選択します。

場所は、ネットワークおよびリソース グループと同じである必要があります。

h) [OK] をクリックします。

ステップ 4 ASA 仮想 の設定項目を設定します。

a) 仮想マシンのサイズを選択します。
b) ストレージ アカウントを選択します。

既存のストレージアカウントを使用するか、新しいストレージアカウントを作成できます。ストレージ アカウントの場所はネットワークおよび仮想マシンと同じである必要があります。

c) [Name] フィールドに IP アドレスのラベルを入力し、[OK] をクリックして、パブリック IP アドレスを要求します。

Azure は、VM を停止して再起動すると変更される可能性のある、ダイナミック パブリック IP をデフォルトでは作成します。固定 IP アドレスを優先する場合は、ポータルのパブリック IP を開き、ダイナミック アドレスからスタティック アドレスに変更します。

d) 必要に応じて、DNS のラベルを追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、*<dnslabel>.<location>.cloupapp.azure.com* の形式になります。

e) 既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。
f) ASA 仮想 を導入する 4 つのサブネットを設定し、[OK] をクリックします。

重要
各インターフェイスを一意のサブネットにアタッチする必要があります。

g) [OK] をクリックします。

ステップ 5 構成サマリを確認し、[OK] をクリックします。

ステップ 6 利用条件を確認し、[Create] をクリックします。

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の開始」を参照してください。

Azure Security Center からの ASA 仮想 の導入

Microsoft Azure Security Center は、お客様がクラウド導入に対するセキュリティ リスクを防御、検出、および軽減できるようにする Azure 向けのセキュリティ ソリューションです。Security Center のダッシュボードから、セキュリティ ポリシーを設定したり、セキュリティ設定をモニターしたり、セキュリティ アラートを表示したりできます。

Security Center は、Azure リソースのセキュリティ状態を分析して、潜在的なセキュリティの脆弱性を特定します。推奨事項のリストに従い、必要なコントロールを設定するプロセスを実行します。対象には、Azure のお客様に対するファイアウォール ソリューションとしての ASA 仮想 の導入を含めることができます。

Security Center の統合ソリューションのように、数クリックで ASA 仮想 をすばやく導入し、単一のダッシュボードからセキュリティイベントと正常性イベントをモニターできます。次の手

順は、Security Center から ASA 仮想 を導入する手順の概要です。詳細については、『Azure Security Center』を参照してください。

手順

ステップ 1 Azure ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 Microsoft Azure メニューから、[Security Center] を選択します。

初めて Security Center にアクセスする場合は、[Welcome] ブレードが開きます。**[Yes! I want to Launch Azure Security Center]** を選択して、[Security Center] ブレードを開き、データ収集を有効にします。

ステップ 3 [Security Center] ブレードで、[Policy] タイルを選択します。

ステップ 4 [Security policy] ブレードで、[Prevention policy] を選択します。

ステップ 5 [Prevention policy] ブレードで、セキュリティ ポリシーの一部として表示する推奨事項をオンにします。

a) [Next generation firewall] を [On] に設定します。これで、ASA 仮想 が Security Center 内の推奨ソリューションとなります。

b) 必要に応じて、他の推奨事項を設定します。

ステップ 6 [Security Center] ブレードに戻って、[Recommendations] タイルを選択します。

Security Center は、Azure リソースのセキュリティ状態を定期的に分析します。Security Center が潜在的なセキュリティの脆弱性を特定すると、[Recommendations] ブレードに推奨事項が表示されます。

ステップ 7 [Recommendations] ブレードで [Add a Next Generation Firewall] 推奨事項を選択して、詳細を表示したり、問題を解決するためのアクションを実行したりします。

ステップ 8 [新規作成（Create New）] または [既存のソリューションを使用（Use existing solution）] を選択してから、導入する ASA 仮想 をクリックします。

ステップ 9 基本的な設定を行います。

a) 仮想マシンの名前を入力します。この名前は Azure サブスクリプション内で一意である必要があります。

重要
名前が一意でなく、既存の名前を再使用すると、導入に失敗します。

b) ユーザー名を入力します。

c) 認証のタイプとして、パスワードまたは SSH キーのいずれかを選択します。

パスワードを選択した場合は、パスワードを入力して確定します。パスワードの複雑さに関するガイドラインについては、「パスワードの設定」を参照してください。

d) サブスクリプション タイプを選択します。

e) リソース グループを選択します。

リソース グループは、仮想ネットワークのリソース グループと同じである必要があります。

f) 場所を選択します。

場所は、ネットワークおよびリソース グループと同じである必要があります。

g) [OK] をクリックします。

ステップ 10 ASA 仮想 の設定項目を設定します。

a) 仮想マシンのサイズを選択します。

ASA 仮想 では、Standard D3 および Standard D3_v2 がサポートされます。

b) ストレージ アカウントを選択します。

既存のストレージ アカウントを使用するか、新しいストレージ アカウントを作成できます。ストレージ アカウントの場所はネットワークおよび仮想マシンと同じである必要があります。

c) [Name] フィールドに IP アドレスのラベルを入力し、[OK] をクリックして、パブリック IP アドレスを要求します。

Azure は、VM を停止して再起動すると変更される可能性のある、ダイナミック パブリック IP をデフォルトでは作成します。固定 IP アドレスを優先する場合は、ポータルのパブリック IP を開き、ダイナミック アドレスからスタティック アドレスに変更します。

d) 必要に応じて、DNS のラベルを追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、*<dnslabel>.<location>.cloupapp.azure.com* の形式になります。

e) 既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。

f) ASA 仮想 を導入する 4 つのサブネットを設定し、[OK] をクリックします。

重要
各インターフェイスを一意のサブネットにアタッチする必要があります。

g) [OK] をクリックします。

ステップ 11 構成サマリを確認し、[OK] をクリックします。

ステップ 12 利用条件を確認し、[Create] をクリックします。

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の開始」を参照してください。
- Security Center 内の推奨事項がどのように Azure リソースの保護に役立つかの詳細については、Security Center から入手可能なマニュアルを参照してください。

Azure Resource Manager からの ASA 仮想 for High Availability の導入

次の手順は、Microsoft Azure で高可用性（HA）ASA 仮想 ペアを設定する手順の概略を示しています。Azure の設定の詳細な手順については、『Azure を使ってみる』を参照してください。

Azure の ASA 仮想 HA では、2 つの ASA 仮想 を可用性セットに導入し、リソース、パブリック IP アドレス、ルートテーブルなどの各種設定を自動的に生成します。導入後に、これらの設定をさらに管理できます。

手順

ステップ 1 Azure ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 マーケットプレイスで [Cisco ASAv] を検索し、[ASAv 4 NIC HA] をクリックして、フェールオーバー ASA 仮想 構成を導入します。

ステップ 3 [Basics] 設定を構成します。

a) ASA 仮想 マシン名のプレフィックスを入力します。ASA 仮想 の名前は「プレフィックス」-A と「プレフィックス」-B になります。

重要
既存のプレフィックスを使用していないことを確認します。使用すると、導入は失敗します。

b) ユーザー名を入力します。

これは両方の仮想マシンの管理ユーザー名です。

重要
Azure では、admin というユーザー名は使用できません。

c) 両方の仮想マシンに認証タイプとして、[Password] または [SSH public key] のいずれかを選択します。

[Password] を選択した場合は、パスワードを入力して確定します。パスワードの複雑さに関するガイドラインについては、「パスワードの設定」を参照してください。

d) サブスクリプション タイプを選択します。

e) [Resource group] を選択します。

[Create new] を選択して新しいリソース グループを作成するか、[Use existing] で既存のリソース グループを選択します。既存のリソース グループを使用する場合は、空である必要があります。そうでない場合は、新しいリソース グループを作成する必要があります。

f) [Location] を選択します。

場所は、ネットワークおよびリソース グループと同じである必要があります。

g) [OK] をクリックします。

ステップ 4 [Cisco ASAv settings] を設定します。

a) 仮想マシンのサイズを選択します。
b) [Managed] または [Unmanaged OS disk] ストレージを選択します。

重要
ASA HA モードでは常に [Managed] を使用します。

ステップ 5 [ASAv-A] 設定を構成します。

a) （オプション）[Create new] を選択して、[Name] フィールドに IP アドレスのラベルを入力し、[OK] をクリックしてパブリック IP アドレスを要求します。パブリック IP アドレスが必要ない場合は、[None] を選択します。

（注）
Azure は、VM を停止して再起動すると変更される可能性のある、ダイナミック パブリック IP をデフォルトでは作成します。固定 IP アドレスを優先する場合は、ポータルのパブリック IP を開き、ダイナミック アドレスからスタティック アドレスに変更します。

b) 必要に応じて、DNS のラベルを追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、*<dnslabel>.<location>.cloupapp.azure.com* の形式になります。

c) ASAv-A 起動時診断のストレージ アカウントに必要な設定を構成します。

ステップ 6 [ASAv-B] 設定についても、この手順を繰り返します。

ステップ 7 既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。

a) ASA 仮想 を導入する 4 つのサブネットを設定し、[OK] をクリックします。

重要
各インターフェイスを一意のサブネットにアタッチする必要があります。

b) [OK] をクリックします。

ステップ 8 構成の [Summary] を確認し、[OK] をクリックします。

ステップ 9 利用条件を確認し、[Create] をクリックします。

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の開始」を参照してください。
- Azure の ASA 仮想 HA 構成の詳細については、『ASA Series General Operations Configuration Guide』の「Failover for High Availability in the Public Cloud」の章を参照してください。

VHD およびリソーステンプレートを使用した Azure からの ASA 仮想 の導入

シスコが提供する圧縮 VHD イメージを使用して、独自のカスタム ASA 仮想 イメージを作成できます。VHD イメージを使用して展開するには、Azure ストレージ アカウントに VHD イメージをアップロードする必要があります。次に、アップロードしたディスク イメージおよび Azure Resource Manager テンプレートを使用して、管理対象イメージを作成できます。Azure テンプレートは、リソースの説明とパラメータの定義が含まれている JSON ファイルです。

始める前に

- ASA 仮想 テンプレートの展開には、JSON テンプレートおよび対応する JSON パラメータ ファイルが必要です。テンプレートファイルは、次の GitHub リポジトリからダウンロードできます。

  https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure

- テンプレートとパラメータファイルを構築する手順については、付録：Azure リソース テンプレートの例 （41 ページ）を参照してください。

- この手順では、Azure に Linux VM が存在している必要があります。一時的な Linux VM（Ubuntu 16.04 など）を使用して、Azure に圧縮 VHD イメージをアップロードすることをお勧めします。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短くなります。

  VM を作成する必要がある場合は、次のいずれかの方法を使用します。

  - Azure CLI による Linux 仮想マシンの作成
  - Azure ポータルでの Linux 仮想マシンの作成

- Azure サブスクリプションには、ASA 仮想 を展開する場所で使用可能なストレージアカウントが必要です。

手順

ステップ 1 https://software.cisco.com/download/home ページから、ASA 仮想 圧縮 VHD イメージをダウンロードします。

a) [Products] > [Security] > [Firewalls] > [Adaptive Security Appliances (ASA)] > [Adaptive Security Appliance (ASA) Software] に移動します。

b) [Adaptive Security Virtual Appliance (ASAv)] をクリックします。

手順に従ってイメージをダウンロードしてください。

たとえば、asav9-14-1.vhd.bz2

ステップ 2 Azure の Linux VM に圧縮 VHD イメージをコピーします。

Azure との間でファイルをやり取りするために使用できるオプションが数多くあります。この例では、SCP（セキュア コピー）を示します。

```
# scp /username@remotehost.com/dir/asav9-14-1.vhd.bz2 <linux-ip>
```

ステップ 3 Azure の Linux VM にログインし、圧縮 VHD イメージをコピーしたディレクトリに移動します。

ステップ 4 ASA 仮想 VHD イメージを解凍します。

ファイルを解凍または圧縮解除するために使用できるオプションが数多くあります。この例では Bzip2 ユーティリティを示しますが、Windows ベースのユーティリティも正常に機能します。

```
# bunzip2 asav9-14-1.vhd.bz2
```

ステップ 5 Azure ストレージ アカウントのコンテナに VHD をアップロードします。既存のストレージ アカウントを使用するほか、新規に作成することもできます。ストレージ アカウント名には、小文字と数字のみを使用できます。

ストレージ アカウントに VHD をアップロードするために使用できるオプションが数多くあります。AzCopy、Azure Storage Copy Blob API、Azure Storage Explorer、Azure CLI、Azure ポータルなどです。ASA 仮想 と同等の大きさのファイルには、Azure ポータルを使用しないことを推奨します。

次の例は、Azure CLI を使用した構文を示しています。

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

ステップ 6 VHD から管理対象イメージを作成します。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) [追加（Add）] をクリックして、新しいイメージを作成します。
c) 次の情報を入力します。

- [サブスクリプション（Subscription）]：ドロップダウンリストからサブスクリプションを選択します。
- [リソースグループ（Resource group）]：既存のリソースグループを選択するか、新しいリソースグループを作成します。
- [名前（Name）]：管理対象イメージのユーザー定義の名前を入力します。
- [リージョン（Region）]：VM が展開されるリージョンを選択します。
- [OSタイプ（OS type）]：OS タイプとして [Linux] を選択します。
- [VMの世代（VM generation）]：[世代1（Gen 1）] を選択します。

  （注）
  [世代2（Gen 2）] はサポートされていません。

- [ストレージブロブ（Storage blob）]：ストレージアカウントを参照して、アップロードした VHD を選択します。

- [アカウントタイプ（Account type）]：要件に応じて、ドロップダウンリストから [Standard HDD]、[Standard SSD]、または [Premium SSD] を選択します。

  このイメージの展開用に計画している VM サイズを選択する場合は、選択したアカウントタイプがその VM サイズでサポートされていることを確認します。

- [ホストキャッシング（Host caching）]：ドロップダウンリストから [読み取り/書き込み（Read/write）] を選択します。

- [データディスク（Data disks）]：デフォルトのままにして、データディスクを追加しないでください。

d) [作成（Create）] をクリックします。

「イメージが正常に作成されました（Successfully created image）」というメッセージが [通知（Notifications）] タブの下に表示されるまで待ちます。

（注）
管理対象イメージが作成されたら、アップロードした VHD とアップロード ストレージ アカウントを削除できます。

ステップ 7 新規に作成した管理対象イメージのリソース ID を取得します。

Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。リソース ID は、この管理対象イメージから新しい ASA 仮想 ファイアウォールを展開するときに必要になります。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) 前のステップで作成した管理対象イメージを選択します。
c) [概要（Overview）] をクリックして、イメージのプロパティを表示します。
d) クリップボードに**リソース ID** をコピーします。

リソース ID は、次の形式を取ります。

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>
/providers/Microsoft.Compute/<container>/ <vhdname>

ステップ 8 管理対象イメージおよびリソーステンプレートを使用して、ASA 仮想 ファイアウォールを構築します。

a) [新規（New）] を選択し、オプションから選択できるようになるまで [テンプレート展開（Template Deployment）] を検索します。
b) [作成（Create）] を選択します。
c) [エディタで独自のテンプレートを構築する（Build your own template in the editor）] を選択します。

カスタマイズできる空白のテンプレートが作成されます。テンプレートを作成する方法の例については、リソース テンプレートの作成 （42 ページ）を参照してください。

d) カスタマイズした JSON テンプレート コードをウィンドウに貼り付け、[保存（Save）] をクリックします。
e) ドロップダウン リストから [サブスクリプション（Subscription）] を選択します。
f) 既存の**リソース グループ**を選択するか、新しいリソース グループを作成します。
g) ドロップダウン リストから [ロケーション（Location）] を選択します。

h) 前ステップからの管理対象イメージの[リソースID（Resource ID）]を[VM管理対象イメージID（Vm Managed Image Id）]フィールドに貼り付けます。

ステップ 9 [カスタム展開（Custom deployment）]ページの最上部にある[パラメータの編集（Edit parameters）]をクリックします。カスタマイズできるパラメータ テンプレートが作成されます。

a) [ファイルのロード（Load file）]をクリックし、カスタマイズした ASA 仮想 パラメータファイルを参照します。パラメータ テンプレートを作成する例については、パラメータ ファイルの作成 （51 ページ）を参照してください。

b) カスタマイズした JSON パラメータ コードをウィンドウに貼り付け、[保存（Save）]をクリックします。

ステップ 10 カスタム展開の詳細を確認します。[基本（Basics）]と[設定（Settings）]の情報（[リソースID（Resource ID）]など）が、想定した展開設定に一致することを確認します。

ステップ 11 利用規約を確認し、[I agree to the terms and conditions stated above] チェックボックスをオンにします。

ステップ 12 [購入（Purchase）]をクリックし、管理対象イメージおよびカスタムテンプレートを使用して ASA 仮想 ファイアウォールを導入します。

テンプレート ファイルとパラメータ ファイルに競合がなければ、展開が正常に完了しているはずです。

管理対象イメージは、同じサブスクリプションおよび地域内の複数の展開に使用できます。

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の開始」を参照してください。

制限付きのAzureプライベートマーケットプレイス環境でのAzureマーケットプレイスオファーの展開

これは、Azure プライベート マーケットプレイスのユーザーにのみ適用されます。Azure プライベート マーケットプレイスを使用している場合は、それぞれのプライベート マーケットプレイスで、ユーザーに対してアプリケーション オファーおよび必要な仮想マシンオファー（非表示）の両方が有効になっていることを確認します。

仮想マシンのオファーとプラン（非表示）：

- パブリッシャー ID：**cisco**
- Cisco Secure Firewall ASA Virtual VM オファー（両方の Cisco Secure Firewall ASA Virtual アプリケーションオファーに使用）
  - オファー ID：**cisco-asav**
  - BYOL プラン ID：**asav-azure-byol**
  - PAYG プラン ID：**asav-azure-payg**

ユーザーがマーケットプレイスから表示されているアプリケーションオファーを展開すると、PAYG または BYOL ライセンスのユーザー選択に基づいて、VM オファープランから対応するイメージが参照され、展開されます。

したがって、展開を機能させるには、アプリケーションと VM の両方のオファーが Azure テナント/サブスクリプションのプライベート マーケットプレイスで有効になっていて、利用できる必要があります。

プライベート マーケットプレイスでこれらのアプリケーションオファーと VM オファーを有効にする方法については、Azure のドキュメントを参照してください。

- プライベート Azure マーケットプレイスを使用してガバメントとコントロールを実施する [英語]
- プライベート マーケットプレイスにオファーを追加する [英語]
- Set-AzMarketplacePrivateStoreOffer [英語]

アプリケーションオファーはマーケットプレイスに表示されるため、Azure UI を介して簡単に有効にできます。

プライベート マーケットプレイスで非表示の仮想マシンオファーを有効にするには、CLI コマンドの使用が必要となる場合があります（このドキュメントの作成時点では、CLI の方法のみが可能です）。

サンプルコマンド

Cisco Secure Firewall ASA Virtual BYOL プランは、次に示すようなサンプルコマンドを使用して有効にできます：

```
$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = '<publisher-id>.<vm-offer-id>'
  SpecificPlanIdsLimitation =@('<plan-id-under-vm-offer>')
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = 'cisco.cisco-asav'
  SpecificPlanIdsLimitation =@('asav-azure-byol')
}
Set-AzMarketplacePrivateStoreOffer @Params
```

（注） サンプルコマンドは参考用です。詳細については、Azure のドキュメントを確認してください。

参照エラーメッセージ

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
      "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be
purchased due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
```

```
This plan is not available for purchase because it needs to be added to your tenant's
Private Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors
for details. "
}
```

マーケットプレイスオファーの展開中には、上記のエラーが発生することがあります。これを解決するには、アプリケーションと VM の両方のオファーを Azure テナント/サブスクリプションで有効にし、利用可能にする必要があります。

Azure での IPv6 サポート対象 ASA 仮想 の展開

この章では、Azure ポータルから IPv6 サポート対象の ASA 仮想 を展開する方法について説明します。

Azure での IPv6 をサポートする展開について

ASA 仮想 製品は、 9.19 以降、IPv4 と IPv6 の両方をサポートします。Azure では、仮想ネットワークを作成または使用する Marketplace サービスから ASA 仮想 を直接展開できますが、現在、Azure の制限により、Marketplace アプリケーション製品は、IPv4 ベースの VNet/サブネットのみを使用または作成するように制限されています。IPv6 アドレスを既存の VNet に手動で設定することはできますが、IPv6 サブネットで設定された VNet に新しい ASA 仮想 インスタンスを追加することはできません。Azure では、Marketplace を介してリソースを展開する方法以外の代替アプローチを使用してサードパーティのリソースを展開するように、一定の制限を課しています。

シスコは現在、IPv6 アドレッシングをサポートするために ASA 仮想 を展開する 2 つの方法を提供しています。

次の 2 つの異なるカスタム IPv6 テンプレートが提供されます。

- [カスタムIPv6テンプレート（ARMテンプレート）（Custom IPv6 template (ARM template)）]：Azure 上の Marketplace イメージを内部的に参照する Azure Resource Manager（ARM）テンプレートを使用して、IPv6 設定の ASA 仮想 を展開するために提供されます。このテンプレートには、IPv6 サポート対象の ASA 仮想 を展開するように設定可能なリソースとパラメータ定義を含む JSON ファイルが含まれています。このテンプレートを使用するには、「Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開 （27 ページ）」を参照してください。

  プログラムによる展開は、PowerShell、Azure CLI、ARM テンプレート、または API を介してカスタムテンプレートを展開するために、Azure Marketplace 上の VM イメージへのアクセスを許可するプロセスです。VM へのアクセスを許可せずに、これらのカスタムテンプレートを VM に展開することは制限されています。このようなカスタムテンプレートを VM に展開しようとすると、次のエラーメッセージが表示されます。

Legal terms have not been accepted for this item on this subscription. To accept legal terms ….and configure programmatic deployment for the Marketplace item …..

次のいずれかの方法を使用して、Azureでのプログラムによる展開を有効にして、Marketplaceイメージを参照するカスタム IPv6（ARM）テンプレートを展開できます。

- **Azure ポータル**：カスタム IPv6 テンプレート（ARM テンプレート）を展開するために、Azure Marketplace で利用可能な ASA 仮想 の提供に対応するプログラムによる展開オプションを有効にします。
- **Azure CLI**：CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

- **カスタム VHD イメージと IPv6 テンプレート（ARM テンプレート）**：Azure で VHD イメージと ARM テンプレートを使用して管理対象イメージを作成します。このプロセスは、VHD とリソーステンプレートを使用した ASA 仮想 の展開に似ています。このテンプレートは、展開中に管理対象イメージを参照し、IPv6 サポート対象の ASA 仮想 を展開するために Azure にアップロードして設定できる ARM テンプレートを使用します。VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開 （33 ページ）を参照してください。

カスタム IPv6 テンプレートを使用した Marketplace イメージまたは VHD イメージを参照して、カスタム IPv6 テンプレート（ARM テンプレート）を使用して ASA 仮想 を展開するプロセス。

ASA 仮想 の展開に含まれる手順は次のとおりです。

表 *3:*

手順	**Process**
1	IPv6 サポート対象の ASA 仮想 の展開を計画している Azure で、Linux VM を作成します。
2	Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して ASA 仮想 を展開する場合に**のみ**、Azure ポータルまたは Azure CLI でプログラムによる展開オプションを有効にします。
3	展開のタイプに応じて、次のカスタムテンプレートをダウンロードします。 • Azure Marketplace 参照イメージを使用したカスタム IPv6 テンプレート。 カスタム IPv6（ARM）テンプレートを使用した VHD イメージ。

4	カスタム IPv6（ARM）テンプレートの IPv6 パラメータを更新します。 （注） Marketplaceイメージバージョンに相当するソフトウェアイメージバージョンのパラメータ値は、Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して ASA 仮想を展開する場合にのみ必要です。ソフトウェアバージョンの詳細を取得するには、コマンドを実行する必要があります。
5	Azure ポータルまたは Azure CLI を使用して ARM テンプレートを展開します。

Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開

Marketplaceイメージを参照し、カスタムIPv6テンプレート（ARMテンプレート）を使用してASA 仮想 を展開するプロセス。

手順

ステップ 1 Azure ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 次の方法で、Azure ポータルまたは Azure CLI を使用してプログラムによる展開を有効にします。

Azure ポータルでこのオプションを有効にするには、次の手順を実行します。

a) [Azure（サービス）（Azure Services）] で [サブスクリプション（Subscriptions）] をクリックして、サブスクリプション ブレード ページを表示します。
b) 左側のペインで、[設定（Settings）] オプションの [プラグラムによる展開（Programmatic Deployment）] をクリックします。

VM に展開されたすべてのタイプのリソースが、関連するサブスクリプション製品とともに表示されます。

c) [ステータス（Status）] 列で、カスタム IPv6 テンプレートのプログラムによる展開のために取得する ASA 仮想 製品に対応する [有効化（Enable）] ボタンをクリックします。

または

Azure CLI を使用してこのオプションを有効にするには、次の手順を実行します。

a) Linux VM に移動します。
b) 次の CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

コマンドの実行時に、イメージのサブスクリプションごとに 1 回だけ規約に同意する必要があります。

 # Accept terms

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # Review that terms were accepted (i.e., accepted=true)

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-asav'
- **<sku/plan>**：'asav-azure-byol'

以下は、BYOL サブスクリプションプランで展開するためのプログラムによる ASA 仮想 の展開を有効にするコマンドスクリプトの例です。

- **az vm image terms show -p cisco -f cisco-ftdv --plan asav-azure-byol**

ステップ 3 次のコマンドを実行して、Marketplace イメージバージョンに相当するソフトウェアバージョンの詳細を取得します。

az vm image list --all -p <publisher> -f <offer> -s <sku>

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-asav'
- **<sku>**：'asav-azure-byol'

以下は、 ASA 仮想 用の Marketplace イメージバージョンに相当するソフトウェアバージョンの詳細を取得するコマンドスクリプトの例です。

az vm image list --all -p cisco -f cisco-ftdv -s asav-azure-byol

ステップ 4 表示される使用可能な Marketplace イメージバージョンのリストから、いずれかの ASA 仮想 バージョンを選択します。

ASA 仮想 の IPv6 サポート展開の場合は、 ASA 仮想 バージョンを 919* 以上として選択する必要があります。

ステップ 5 Cisco GitHub リポジトリから Marketplace カスタム IPv6 テンプレート（ARM テンプレート）をダウンロードします。

ステップ 6 パラメータ テンプレート ファイル（JSON）で展開値を指定して、パラメータファイルを準備します。

次の表で、 ASA 仮想 カスタム展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

パラメータ名	許可される値/タイプの例	説明
vmName	cisco-asav	Azure で ASA 仮想 VM に名前を付けます。

パラメータ名	許可される値/タイプの例	説明
softwareVersion	919.0.24	Marketplace イメージバージョンのソフトウェアバージョン。
adminUsername	hjohn	ASA 仮想 にログインするユーザー名。 管理者に割り当てられる予約名「admin」は使用できません。
adminPassword	E28@4OiUrhx!	管理者アカウントのパスワード。 パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。パスワードの複雑さに関するガイドラインについては、「パスワードの設定」を参照してください。
vmStorageAccount	hjohnvmsa	Azure ストレージ アカウント。既存のストレージアカウントを使用するほか、新規に作成することもできます。ストレージアカウント名は、3 ～ 24 文字の長さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。
availabilityZone	0	展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。 可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。

パラメータ名	許可される値/タイプの例	説明
userData	`!\ninterface management0\/0\nmanagement-only\nnameif management\nsecurity-level 100\nip address dhcp setroute\nipv6 enable\nipv6 address dhcp\nno shutdown\n!\ncrypto key generate rsa modulus 2048\nssh 0 0 management\nssh timeout 60\nssh version 2\nusername admin password E28@4OiUrhx! privilege 15\nenable password E28@4OiUrhx!\nusername admin attributes\nservice-type admin\naaa authentication ssh console LOCAL\n!\naccess-list allow-all extended permit ip any any\naccess-group allow-all global\n!\ndns domain-lookup management\ndns server-group DefaultDNS\nname-server 8.8.8.8\n!`	仮想マシンに渡されるユーザーデータ。
virtualNetworkResourceGroup	cisco-asav-rg	仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	cisco-asav-vnet	仮想ネットワークの名前。
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。
virtualNetworkAddressPrefixes	10.151.0.0/16	これは仮想ネットワークの IPv4 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	これは仮想ネットワークの IPv6 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1Name	mgmt	管理サブネット名。

パラメータ名	許可される値/タイプの例	説明
Subnet1Prefix	10.151.1.0/24	これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet1StartAddress	10.151.1.4	管理インターフェイスの IPv4 アドレス。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理インターフェイスの IPv6 アドレス。
Subnet2Name	diag	データインターフェイス 1 のサブネット名。
Subnet2Prefix	10.151.2.0/24	これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet2StartAddress	10.151.2.4	データインターフェイス 1 の IPv4 アドレス。
subnet2v6StartAddress	ace:cab:deca:2222::6	データインターフェイス 1 の IPv6 アドレス。
Subnet3Name	inside	データインターフェイス 2 のサブネット名。
Subnet3Prefix	10.151.3.0/24	これはデータインターフェイス 2 サブネット IPv4 プレフィック

パラメータ名	許可される値/タイプの例	説明
		スで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	これはデータインターフェイス 2 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet3StartAddress	10.151.3.4	データインターフェイス 2 の IPv4 アドレス。
subnet3v6StartAddress	ace:cab:deca:3333::6	データインターフェイス 2 の IPv6 アドレス。
Subnet4Name	outside	データインターフェイス 3 のサブネット名。
Subnet4Prefix	10.151.4.0/24	これはデータインターフェイス 3 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	これはデータインターフェイス 3 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet4StartAddress	10.151.4.4	データインターフェイス 3 の IPv4 アドレス。
subnet4v6StartAddress	ace:cab:deca:4444::6	データインターフェイス 3 の IPv6 アドレス。
vmSize	Standard_D4_v2	ASA 仮想 VM のサイズ。Standard_D3_v2 がデフォルトです。。

ステップ 7 ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で ASA 仮想 ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』
- 『Deploy a local ARM template through CLI』

次のタスク

SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の開始」を参照してください。Security Center 内の推奨事項がどのように Azure リソースの保護に役立つかの詳細については、Security Center から入手可能なマニュアルを参照してください。

VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開

シスコが提供する圧縮 VHD イメージを使用して、独自のカスタム ASA 仮想 イメージを作成できます。このプロセスは、VHD とリソーステンプレートを使用した ASA 仮想 の展開に似ています。

始める前に

- Github の VHD および ARM の最新テンプレートを使用した ASA 仮想 の展開には、JSON テンプレートおよび対応する JSON パラメータファイルが必要です。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。
- この手順では、Azure に Linux VM が存在している必要があります。一時的な Linux VM（Ubuntu 16.04 など）を使用して、Azure に圧縮 VHD イメージをアップロードすることをお勧めします。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短くなります。

  VM を作成する必要がある場合は、次のいずれかの方法を使用します。

  - Azure CLI による Linux 仮想マシンの作成
  - Azure ポータルによる Linux 仮想マシンの作成

- Azure サブスクリプションには、 ASA 仮想 を展開する場所で使用可能なストレージアカウントが必要です。

手順

ステップ 1 シスコ ダウンロード ソフトウェア ページから ASA 仮想 圧縮 VHD イメージ（*.bz2）をダウンロードします。

a) [Products] > [Security] > [Firewalls] > [Adaptive Security Appliances (ASA)] > [Adaptive Security Appliance (ASA) Software] に移動します。
b) [Adaptive Security Virtual Appliance (ASAv)] をクリックします。

手順に従ってイメージをダウンロードしてください。

たとえば、asav9-14-1.vhd.bz2

ステップ 2 「VHD およびリソーステンプレートを使用した Azure からの ASA Virtual の展開」の**ステップ 2** から**ステップ 8** の手順を実行します。。

ステップ 3 [カスタム展開（Custom deployment）] ページの最上部にある [パラメータの編集（Edit parameters）] をクリックします。カスタマイズできるパラメータ テンプレートが作成されます。

a) [ファイルのロード（Load file）] をクリックし、カスタマイズした ASA 仮想 パラメータファイルを参照します。VHD およびカスタム IPv6（ARM）テンプレートを使用した Azure への ASA 仮想 の展開例は、Github を参照してください。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。
b) カスタマイズした JSON パラメータコードをウィンドウに貼り付け、[保存（Save）] をクリックします。

次の表で、 ASA 仮想 展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

パラメータ名	許可される値/タイプの例	説明
vmName	cisco-asav	Azure で ASA 仮想 VM に名前を付けます。
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/images/{image-name}	展開に使用されるイメージの ID。Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。
adminUsername	hjohn	ASA 仮想にログインするユーザー名。 管理者に割り当てられる予約名「admin」は使用できません。
adminPassword	E28@4OiUrhx!	管理者アカウントのパスワード。 パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。
vmStorageAccount	hjohnvmsa	Azure ストレージ アカウント。既存のストレージ アカウントを使用するほか、新規に作成することも

パラメータ名	許可される値/タイプの例	説明
		できます。ストレージアカウント名は、3 ～ 24 文字の長さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。
availabilityZone	0	展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。 可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。
userData	`!\ninterface management0\/0\nmanagement-only\nnameif management\nsecurity-level 100\nip address dhcp setroute\nipv6 enable\nipv6 address dhcp\nno shutdown\n!\ncrypto key generate rsa modulus 2048\nssh 0 0 management\nssh timeout 60\nssh version 2\nusername admin password E28@4OiUrhx! privilege 15\nenable password E28@4OiUrhx!\nusername admin attributes\nservice-type admin\naaa authentication ssh console LOCAL\n!\naccess-list allow-all extended permit ip any any\naccess-group allow-all global\n!\ndns domain -lookup management\ndns server-group DefaultDNS\nname-server 8.8.8.8\n!`	仮想マシンに渡されるユーザーデータ。
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}`	第 0 日構成で ASA 仮想 に表示されるフィールド。デフォルトでは、設定対象となる次の 3 つのキーと値のペアがあります。 • 「admin」ユーザーパスワード • CSF-MCv ホスト名

パラメータ名	許可される値/タイプの例	説明
		• 管理用の CSF-MCv ホスト名または CSF-DM。 「ManageLocally : yes」：これにより、CSF-DM が Threat Defense Virtual マネージャとして使用されるように設定されます。 CSF-MCv を Threat Defense Virtual マネージャとして設定し、CSF-MCv で同じ設定をするのに必要なフィールドに入力することもできます。
virtualNetworkResourceGroup	cisco-asav	仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	cisco-asav-vnet	仮想ネットワークの名前。
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。
virtualNetworkAddressPrefixes	10.151.0.0/16	これは仮想ネットワークの IPv4 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	これは仮想ネットワークの IPv6 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1Name	mgmt-ipv6	管理サブネット名。
Subnet1Prefix	10.151.1.0/24	これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が

パラメータ名	許可される値/タイプの例	説明
		「new」に設定されている場合にのみ必要です。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet1StartAddress	10.151.1.4	管理インターフェイスの IPv4 アドレス。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理インターフェイスの IPv6 アドレス。
Subnet2Name	diag	データインターフェイス 1 のサブネット名。
Subnet2Prefix	10.151.2.0/24	これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet2StartAddress	10.151.2.4	データインターフェイス 1 の IPv4 アドレス。
subnet2v6StartAddress	ace:cab:deca:2222::6	データインターフェイス 1 の IPv6 アドレス。
Subnet3Name	inside	データインターフェイス 2 のサブネット名。
Subnet3Prefix	10.151.3.0/24	これはデータインターフェイス 2 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。

パラメータ名	許可される値/タイプの例	説明
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	これはデータインターフェイス 2 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet3StartAddress	10.151.3.4	データインターフェイス 2 の IPv4 アドレス。
subnet3v6StartAddress	ace:cab:deca:3333::6	データインターフェイス 2 の IPv6 アドレス。
Subnet4Name	outside	データインターフェイス 3 のサブネット名。
Subnet4Prefix	10.151.4.0/24	これはデータインターフェイス 3 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	これはデータインターフェイス 3 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet4StartAddress	10.151.4.4	データインターフェイス 3 の IPv4 アドレス。
subnet4v6StartAddress	ace:cab:deca:4444::6	データインターフェイス 3 の IPv6 アドレス。
vmSize	Standard_D4_v2	ASA 仮想 VM のサイズ。Standard_D3_v2 がデフォルトです。。

ステップ 4 ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で ASA 仮想 ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』

- 『Deploy a local ARM template through CLI』

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の開始」を参照してください。

制限付きのAzureプライベートマーケットプレイス環境でのAzureマーケットプレイスオファーの展開

これは、Azure プライベート マーケットプレイスのユーザーにのみ適用されます。Azure プライベート マーケットプレイスを使用している場合は、それぞれのプライベート マーケットプレイスで、ユーザーに対してアプリケーション オファーおよび必要な仮想マシンオファー（非表示）の両方が有効になっていることを確認します。

仮想マシンのオファーとプラン（非表示）：

- パブリッシャー ID：**cisco**
- Cisco Secure Firewall ASA Virtual VM オファー（両方の Cisco Secure Firewall ASA Virtual アプリケーションオファーに使用）
  - オファー ID：**cisco-asav**
  - BYOL プラン ID：**asav-azure-byol**
  - PAYG プラン ID：**asav-azure-payg**

ユーザーがマーケットプレイスから表示されているアプリケーションオファーを展開すると、PAYG または BYOL ライセンスのユーザー選択に基づいて、VM オファープランから対応するイメージが参照され、展開されます。

したがって、展開を機能させるには、アプリケーションと VM の両方のオファーが Azure テナント/サブスクリプションのプライベート マーケットプレイスで有効になっていて、利用できる必要があります。

プライベート マーケットプレイスでこれらのアプリケーションオファーと VM オファーを有効にする方法については、Azure のドキュメントを参照してください。

- プライベート Azure マーケットプレイスを使用してガバメントとコントロールを実施する [英語]
- プライベート マーケットプレイスにオファーを追加する [英語]
- Set-AzMarketplacePrivateStoreOffer [英語]

アプリケーションオファーはマーケットプレイスに表示されるため、Azure UI を介して簡単に有効にできます。

プライベート マーケットプレイスで非表示の仮想マシンオファーを有効にするには、CLI コマンドの使用が必要となる場合があります（このドキュメントの作成時点では、CLI の方法のみが可能です）。

サンプルコマンド

Cisco Secure Firewall ASA Virtual BYOL プランは、次に示すようなサンプルコマンドを使用して有効にできます：

```
$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = '<publisher-id>.<vm-offer-id>'
  SpecificPlanIdsLimitation =@('<plan-id-under-vm-offer>')
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = 'cisco.cisco-asav'
  SpecificPlanIdsLimitation =@('asav-azure-byol')
}
Set-AzMarketplacePrivateStoreOffer @Params
```

（注） サンプルコマンドは参考用です。詳細については、Azure のドキュメントを確認してください。

参照エラーメッセージ

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
      "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be
purchased due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
This plan is not available for purchase because it needs to be added to your tenant's
Private Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors
for details. "
}
```

マーケットプレイスオファーの展開中には、上記のエラーが発生することがあります。これを解決するには、アプリケーションと VM の両方のオファーを Azure テナント/サブスクリプションで有効にし、利用可能にする必要があります。

付録：Azure リソース テンプレートの例

この項では、ASA 仮想 を展開するために使用できる Azure Resource Manager テンプレートの構造について説明します。Azure リソース テンプレートは JSON ファイルです。必須の全リソースの展開を簡素化するため、この例には 2 つの JSON ファイルが含まれています。

- **テンプレート ファイル**：これは、リソース グループ内のすべてのコンポーネントを展開するメイン リソース ファイルです。
- **パラメータ ファイル**：このファイルには、ASA 仮想 を正常に展開するために必要なパラメータが含まれています。このファイルには、サブネット情報、仮想マシンの階層とサイズ、ASA 仮想 のユーザー名とパスワード、ストレージコンテナの名前など、詳細な情報が含まれています。このファイルは Azure Stack Hub 展開環境用にカスタマイズできます。

テンプレート ファイルの形式

この項では、Azure Resource Manager テンプレートの構造について説明します。次の例は、テンプレート ファイルを縮小表示したもので、テンプレートのさまざまな部分を示しています。

Azure Resource Manager JSON テンプレート ファイル

```
{
    "$schema":
"http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "",
    "parameters": { },
    "variables": { },
    "resources": [ ],
    "outputs": { }
}
```

テンプレートは、ASA 仮想 展開の値を作成するために使用できる JSON および式で構成されています。その最も単純な構造では、テンプレートに次の要素が含まれています。

表 *4 :* 定義済みの *Azure Resource Manager JSON* テンプレート ファイル要素

要素	必須	説明
$schema	あり	テンプレート言語のバージョンを説明する JSON スキーマ ファイルの場所。前の図に示した URL を使用します。
contentVersion	あり	テンプレートのバージョン（1.0.0.0 など）。この要素には任意の値を指定できます。テンプレートを使用してリソースを展開するときは、この値を使用して、適切なテンプレートが使用されていることを確認できます。

要素	必須	説明
パラメータ	なし	展開を実行してリソース展開をカスタマイズするときに指定する値。パラメータにより、展開時に値を入力できます。絶対に必要というわけではありませんが、指定しないと、JSONテンプレートは毎回同じパラメータでリソースを展開します。
変数	なし	テンプレート言語式を簡素化するためにテンプレートで JSON フラグメントとして使用される値。
リソース	あり	リソース グループで展開または更新されるリソース タイプ。
outputs	なし	展開後に返される値。

JSONテンプレートは、展開するリソース タイプを宣言するためだけでなく、その関連する設定パラメータを宣言するためにも利用できます。次の例は、新しい ASA 仮想 を展開するテンプレートを示しています。

リソース テンプレートの作成

以下の例を使用して、テキストエディタを使用した独自の導入テンプレートを作成できます。

手順

ステップ 1 次の例に示したテキストをコピーします。

例：

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string",
            "defaultValue": "ngfw",
            "metadata": {
                "description": "Name of the NGFW VM"
            }
        },
        "vmManagedImageId": {
            "type": "string",
            "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",

            "metadata": {
                "description": "The ID of the managed image used for deployment.
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"

            }
        },
```

```
        "adminUsername": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Username for the Virtual Machine. admin, Administrator among other
 values are disallowed - see Azure docs"
            }
        },
        "adminPassword": {
            "type": "securestring",
            "defaultValue" : "",
            "metadata": {
                "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars
 and have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
            }
        },
        "vmStorageAccount": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "A storage account name (boot diags require a storage account).
Between 3 and 24 characters. Lowercase letters and numbers only"
            }
        },
        "virtualNetworkResourceGroup": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network's Resource Group"
            }
        },
        "virtualNetworkName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network"
            }
        },
        "mgmtSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv management interface will attach to this subnet"
            }
        },
        "mgmtSubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
            }
        },
        "diagSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
            }
        },
        "diagSubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
```

```
            }
        },
        "gig00SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
            }
        },
        "gig00SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
            }
        },
        "gig01SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
            }
        },
        "gig01SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
            }
        },
        "VmSize": {
            "type": "string",
            "defaultValue": "Standard_D3_v2",
            "allowedValues": [ "Standard_D3_v2" , "Standard_D3" ],
            "metadata": {
                "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
            }
        }
    },
    "variables": {

        "virtualNetworkID":
"[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
parameters('virtualNetworkName'))]",

        "vmNic0Name":"[concat(parameters('vmName'),'-nic0')]",
        "vmNic1Name":"[concat(parameters('vmName'),'-nic1')]",
        "vmNic2Name":"[concat(parameters('vmName'),'-nic2')]",
        "vmNic3Name":"[concat(parameters('vmName'),'-nic3')]",

        "vmNic0NsgName":"[concat(variables('vmNic0Name'),'-NSG')]",

        "vmMgmtPublicIPAddressName": "[concat(parameters('vmName'),'nic0-ip')]",
        "vmMgmtPublicIPAddressType": "Static",
        "vmMgmtPublicIPAddressDnsName": "[variables('vmMgmtPublicIPAddressName')]"
    },
    "resources": [
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/publicIPAddresses",
            "name": "[variables('vmMgmtPublicIPAddressName')]",
            "location": "[resourceGroup().location]",
            "properties": {
              "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
```

```
              "dnsSettings": {
                "domainNameLabel": "[variables('vmMgmtPublicIPAddressDnsName')]"
              }
            }
        },
        {
            "apiVersion": "2015-06-15",
            "type": "Microsoft.Network/networkSecurityGroups",
            "name": "[variables('vmNic0NsgName')]",
            "location": "[resourceGroup().location]",
            "properties": {
                "securityRules": [
                    {
                        "name": "SSH-Rule",
                        "properties": {
                            "description": "Allow SSH",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "22",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 100,
                            "direction": "Inbound"
                        }
                    },
                    {
                        "name": "SFtunnel-Rule",
                        "properties": {
                            "description": "Allow tcp 8305",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "8305",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 101,
                            "direction": "Inbound"
                        }
                    }
                ]
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic0Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Network/networkSecurityGroups/',variables('vmNic0NsgName'))]",
                "[concat('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('mgmtSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('mgmtSubnetName'))]"
                            },
```

```
                            "publicIPAddress":{
                                "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
                            }
                        }
                    }
                ],
                "networkSecurityGroup": {
                    "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
                },
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic1Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('diagSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('diagSubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic2Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig00SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig00SubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic3Name')]",
```

```
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig01SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig01SubnetName'))]"

                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[concat(parameters('vmStorageAccount'))]",
            "apiVersion": "2015-06-15",
            "location": "[resourceGroup().location]",
            "properties": {
              "accountType": "Standard_LRS"
            }
        },
        {
            "apiVersion": "2017-12-01",
            "type": "Microsoft.Compute/virtualMachines",
            "name": "[parameters('vmName')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic0Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic1Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic2Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic3Name'))]"
            ],
            "properties": {
                "hardwareProfile": {
                    "vmSize": "[parameters('vmSize')]"
                },
                "osProfile": {
                    "computername": "[parameters('vmName')]",
                    "adminUsername": "[parameters('AdminUsername')]",
                    "adminPassword": "[parameters('AdminPassword')]"
                },
                "storageProfile": {
                    "imageReference": {
                        "id": "[parameters('vmManagedImageId')]"
                    },
                    "osDisk": {
                        "osType": "Linux",
                        "caching": "ReadWrite",
                        "createOption": "FromImage"
                    }
                },
                "networkProfile": {
                    "networkInterfaces": [
                        {
                            "properties": {
```

```
                                "primary": true
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
                        }
                    ]
                },
                "diagnosticsProfile": {
                    "bootDiagnostics": {
                        "enabled": true,
                        "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
                    }
                }
            }
        }
    ],
    "outputs": {  }
}
```

ステップ 2 このファイルを、たとえば **azureDeploy.json** というように、JSON ファイルとしてローカルに保存します。

ステップ 3 ファイルを編集し、導入パラメータに合うテンプレートを作成します。

ステップ 4 VHD およびリソーステンプレートを使用した Azure からの ASA 仮想 の導入 （20 ページ）で説明しているように、このテンプレートを使用して ASA 仮想 を展開します。

パラメータ ファイルの形式

新しい展開を開始するときには、リソーステンプレートにパラメータが定義されています。展開を開始するには、これらを入力しておく必要があります。リソーステンプレートに定義したパラメータを手動で入力することも、パラメータをテンプレートパラメータ JSON ファイルに配置しておくこともできます。

パラメータ ファイルには、パラメータ ファイルの作成 （51 ページ）のパラメータの例に表示される各パラメータの値が含まれています。これらの値は、展開時にテンプレートに自動的に渡されます。さまざまな展開シナリオに合わせて複数のパラメータ ファイルを作成できます。

この例の ASA 仮想 テンプレートの場合、パラメータ ファイルに次のパラメータを定義する必要があります。

表 *5 : ASA* 仮想 パラメータの定義

フィールド	説明	例
vmName	Azure における ASA 仮想 マシンの名前。	cisco-asav
vmManagedImageId	展開に使用される管理対象イメージの ID。Azure の内部では、あらゆるリソースがリソース IDに関連付けられています。	/subscriptions/73d2537e-ca44-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv910-Managed-Image
adminUsername	ASA 仮想 にログインするためのユーザー名。予約名の「admin」にすることはできません。	jdoe
adminPassword	管理者アカウントのパスワード。これは、12 ～ 72 文字の長さで、1 つの小文字、1 つの大文字、1 つの数字、1 つの特殊文字のうち 3 つを含める必要があります。	Pw0987654321
vmStorageAccount	Azure ストレージアカウント。既存のストレージ アカウントを使用するほか、新規に作成することもできます。ストレージ アカウント名は、3 ～ 24 文字で、小文字と数字のみ含めることができます。	ciscoasavstorage
virtualNetworkResourceGroup	仮想ネットワークのリソースグループの名前。ASA 仮想 は常に新しいリソースグループに配置されます。	ew-west8-rg
virtualNetworkName	仮想ネットワークの名前。	ew-west8-vnet

フィールド	説明	例
mgmtSubnetName	管理インターフェイスは、このサブネットに接続されます。これは、Nic0（最初のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	mgmt
mgmtSubnetIP	管理インターフェイス IP アドレス。	10.8.0.55
gig00SubnetName	GigabitEthernet 0/0 インターフェイスは、このサブネットに接続されます。これは、Nic1（2番目のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	inside
gig00SubnetIP	GigabitEthernet 0/0 インターフェイス IP アドレス。これは、ASA 仮想 の最初のデータインターフェイス用です。	10.8.2.55
gig01SubnetName	GigabitEthernet 0/1 インターフェイスは、このサブネットに接続されます。これは、Nic2（3番目のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	outside
gig01SubnetIP	GigabitEthernet 0/1 インターフェイス IP アドレス。これは、ASA 仮想 の 2 番目のデータインターフェイス用です。	10.8.3.55

フィールド	説明	例
gig02SubnetName	GigabitEthernet 0/2 インターフェイスは、このサブネットに接続されます。これは、Nic3（4番目のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	dmz
gig02SubnetIP	GigabitEthernet 0/2 インターフェイスの IP アドレス。これは、ASA 仮想 の 3 番目のデータインターフェイス用です。	10.8.4.55
vmSize	ASA 仮想 VM に使用する VM のサイズ。Standard_D3_V2 と Standard_D3 がサポートされています。Standard_D3_V2 がデフォルトです。	Standard_D3_V2 または Standard_D3

パラメータ ファイルの作成

以下の例を使用して、テキスト エディタを使用した独自のパラメータ ファイルを作成できます。

（注） 次の例は、IPV4 専用です。

手順

ステップ 1 次の例に示したテキストをコピーします。

例：

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ffldb61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"
```

```
    },
    "adminUsername": {
      "value": "jdoe"
    },
    "adminPassword": {
      "value": "Pw0987654321"
    },
    "vmStorageAccount": {
      "value": "ciscoasavstorage"
    },
    "virtualNetworkResourceGroup": {
      "value": "ew-west8-rg"
    },
    "virtualNetworkName": {
      "value": "ew-west8-vn"
    },
    "mgmtSubnetName": {
      "value": "mgmt"
    },
    "mgmtSubnetIP": {
      "value": "10.8.3.77"
    },
    "gig00SubnetName": {
      "value": "inside"
    },
    "gig00SubnetIP": {
      "value": "10.8.2.77"
    },
    "gig01SubnetName": {
      "value": "outside"
    },
    "gig01SubnetIP": {
      "value": "10.8.1.77"
    },
    "gig02SubnetName": {
      "value": "dmz"
    },
    "gig02SubnetIP": {
      "value": "10.8.0.77"
    },
    "VmSize": {
      "value": "Standard_D3_v2"
    }
  }
}
```

ステップ 2 このファイルを、たとえば**azureParameters.json** というように、JSON ファイルとしてローカルに保存します。

ステップ 3 ファイルを編集し、導入パラメータに合うテンプレートを作成します。

ステップ 4 VHD およびリソーステンプレートを使用した Azure からの ASA 仮想 の導入 （20 ページ） で説明しているように、このパラメータ テンプレートを使用して ASA 仮想 を展開します。

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。