Microsoft Azure クラウドへの ASAv の導入

Microsoft Azure クラウドに ASAv を導入できます。

Microsoft Azure クラウドへの ASAv の導入について

Microsoft Azure は、プライベート Microsoft Hyper V ハイパーバイザを使用するパブリック クラウド環境です。ASAv は、Hyper V ハイパーバイザの Microsoft Azure 環境でゲストとして実行されます。Microsoft Azure 上の ASAv は、4 つの vCPU、14 GB、4 つのインターフェイスをサポートする Standard D3 の 1 つのインスタンス タイプをサポートします。

Microsoft Azure に ASAv を導入するには、2 つの方法（Azure Resource Manager を使用したスタンドアロン ファイア ウォールとして、または、Azure Security Center を使用した統合パートナー ソリューションとして）があります。Microsoft Azure への ASAv の導入、58 ページを参照してください。

ASAv および Azure の前提条件およびシステム要件

- 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 ASAv を選択し、ASAv を導入できます。

- ASAv にライセンスを付与します。

  ASAv にライセンスを付与するまでは、100 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 ASAv（ASAv の Smart Software Licensing）」を参照してください。

- 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 ASAv を導入する必要があります。

  - 管理インターフェイス

    注：エッジ ファイアウォール構成の場合、管理インターフェイスは、「外部」インターフェイスとしても使用されます。

    注：Azure では、最初に定義されたインターフェイス（常に、管理インターフェイス）が、それに Azure パブリック IP アドレスを関連付けることができる唯一のインターフェイスです。このため、Azure 内の ASAv は管理インターフェイス上でのデータ トラフィックの通過を許可します。そのため、管理インターフェイスの初期設定には、**管理専用**の設定は含まれていません。

  - 内部および外部インターフェイス
  - 追加のサブネット（DMZ または選択したネットワーク）
- 通信パス：
  - 管理インターフェイス：SSH アクセスと、ASAv を ASDM に接続するために使用されます。
  - 内部インターフェイス（必須）：内部ホストに ASAv 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）：ASAv 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、ASAv を DMZ ネットワークに接続するために使用されます。
- ASAv のシステム要件については、「Cisco ASA Compatibility」を参照してください。

ASAv および Azure のガイドラインと制限事項

サポートされる機能

- Microsoft Azure クラウドからの導入
- インスタンスあたり最大 4 つの vCPU
- L3 ネットワークのユーザ導入

  注：Azure は設定可能な L2 vSwitch 機能は提供していません。
- 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、ASAv 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。

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）
- IPv6
- ユーザ 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
- インターフェイスのパブリック IP アドレス

  Management 0/0 インターフェイスのみが、それに関連付けられたパブリック IP アドレスを保持できます。
- 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 ポリシーによって、インターフェイスの無差別モードでの動作は許可されていないため、ASAv のトランスペアレント ファイアウォール モードでの動作は阻止されます。

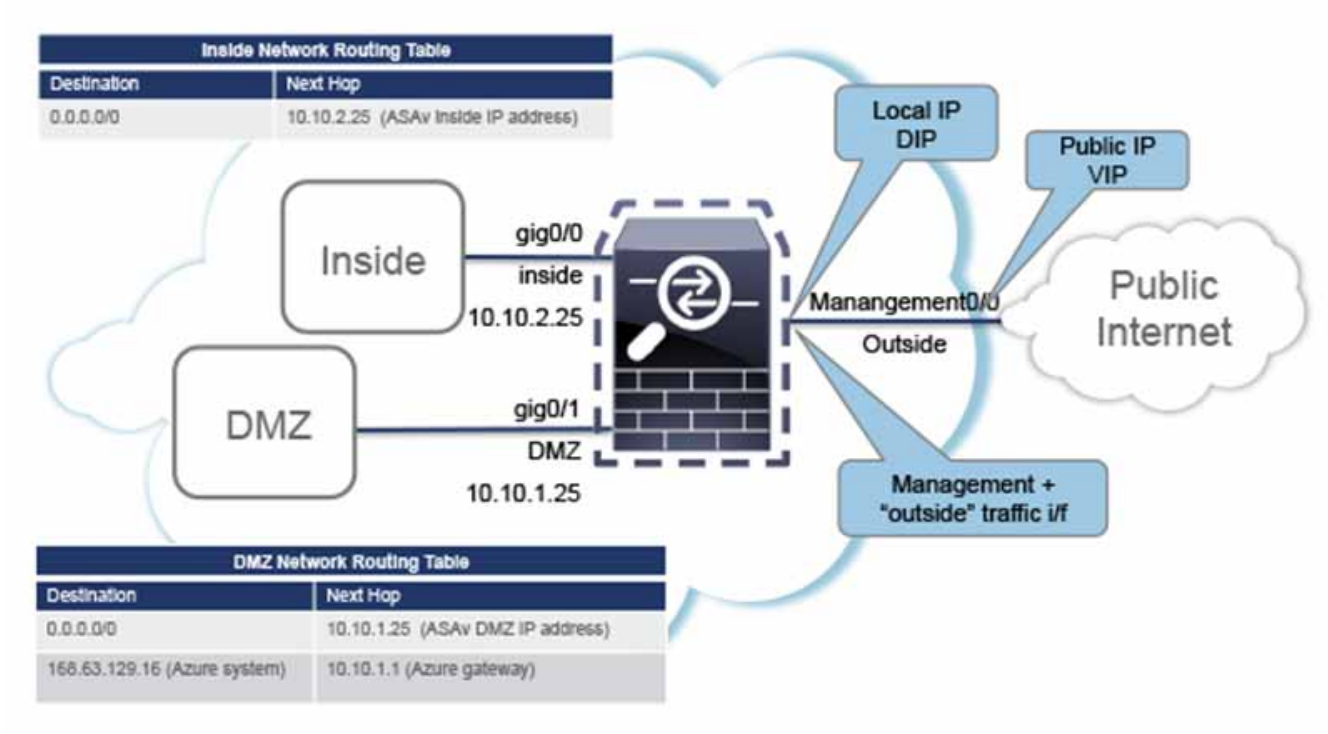
- マルチ コンテキスト モード
- クラスタ
- ASAv のネイティブ HA
- VM のインポート/エクスポート
- デフォルトでは、Azure クラウド内で稼働する ASAv の FIPS モードは無効になっています。

  注意: 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、それ以降 ASAv に SSH 接続できなくなります。そのため、グループの変更が、最初に ASAv を管理する唯一の方法となります。

Azure 上の ASAv のネットワーク トポロジの例

図 1（55 ページ）は、Azure 内に設定された 3 つのサブネット（管理、内部、DMZ）を備えた、ルーテッド ファイアウォール モードの ASAv の推奨トポロジを示しています。4 番目の必須インターフェイス（外部）は示されていません。

図 1　Azure への ASAv の導入の例



導入時に作成されるリソース

Azure に ASAv を導入すると、次のリソースが作成されます。

- ASAv 仮想マシン（VM）
- 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）

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

- 4 枚の NIC（名前は、*vm name*-Nic0、*vm name*-Nic1、*vm name*-Nic2、*vm name*-Nic3）

  これらの NIC は、それぞれ ASAv 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。

- セキュリティ グループ（名前は、*vm name*-SSH-SecurityGroup）

  セキュリティ グループは、ASAv 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（導入時に選択した値に従って命名）

  パブリック IP アドレスは、Management 0/0 にマッピングされる VM の Nic0 に関連付けられます。Azure では、パブリック IP アドレスを最初の NIC のみに関連付けることができます。

  注: パブリック IP アドレスを選択する必要があります（新規または既存）。[None] オプションはサポートされていません。

- 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）

  テーブル（名前は、*subnet name*-ASAv-RouteTable）

  各ルーティング テーブルには、ASAv 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 テーブルとユーザ定義のルーティング テーブルの組み合わせです。

注: 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。

ASAv を介してトラフィックをルーティングするために、ASAv 導入プロセスで、ASAv 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 ASAv 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。これは、サブネットからのすべてのトラフィックを ASAv を介して送信します。そのトラフィックを処理する前に、ASAv ポリシーを設定する必要が生じる場合があります（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、ユーザ定義のルーティング テーブルに、ネクストホップとして ASAv 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、トラフィックが ASAv をバイパスしてしまいます。

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 ASAv 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。

IP アドレス

次の情報は Azure の IP アドレスに適用されます。

- ASAv 上の最初の NIC（Management 0/0 にマッピングされる）には、アタッチ先のサブネット内のプライベート IP アドレスが付与されます。

  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。

- VM の最初の NIC のみにパブリック IP アドレスをアタッチできます。
- 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 ASAv のリロード時には、それらは保持されます。
- 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。
- ASAv インターフェイスは、DHCP を使用して、自身の IP アドレスを設定します。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 ASAv インターフェイスに割り当てられるように確保します。

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 サーバをセットアップしていない場合に使用できます。

Microsoft Azure への ASAv の導入

次の 2 つの方法のどちらかで ASAv を Microsoft Azure に導入できます。

- ASAv を Azure Resource Manager を使用したスタンドアロン ファイアウォールとして導入します。Azure Resource Manager からの ASAv の導入、58 ページを参照してください。
- ASAv を Azure Security Center を使用した Azure 内の統合パートナー ソリューションとして導入します。セキュリティを重視するお客様には、ASAv を Azure ワークロードを保護するためのファイアウォール オプションとして提案します。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されます。Azure Security Center からの ASAv の導入、59 ページを参照してください。

Azure Resource Manager からの ASAv の導入

次の手順は、ASAv 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 のセットアップ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 ASAv 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

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。

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

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。

      注: 既存の名前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。

   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。

4. ASAv 設定を構成します。

   a. 仮想マシンのサイズを選択します。

      注: ASAv で使用できる唯一のサイズが Standard D3 です。

   b. ストレージ アカウントを選択します。

注: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 アカウントを作成することができます。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。

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。

注: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. ASAv 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。

注: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。

5. 構成サマリを確認し、[OK] をクリックします。

6. 利用条件を確認し、[Create] をクリックします。

次の作業

- 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、79 ページを参照してください。

Azure Security Center からの ASAv 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。推奨事項のリストが、必要なコントロールを設定するためのプロセスを誘導します。これには、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 ASAv 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として、数クリックで ASAv 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 イベントとヘルス イベントをモニタできます。次のリストは、Security Center から ASAv を導入するための手順概要です。詳細については、『Azure Security Center』を参照してください。

手順

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。

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。

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

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

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。これにより、ASAv が Security Center 内の推奨ソリューションであることが確認されます。
   b. 必要に応じて、他の推奨事項を設定します。
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。
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。
8. [Create New] または [Use existing solution] を選択してから、導入する ASAv をクリックします。
9. 基本的な設定を行います。
   c. 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。

      注:既存の名前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。
   d. ユーザ名を入力します。
   e. 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。
   f. サブスクリプション タイプを選択します。
   g. 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。
   h. 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。
   i. [OK] をクリックします。
10. ASAv 設定を構成します。
   a. 仮想マシンのサイズを選択します。

      注:ASAv で使用できる唯一のサイズが Standard D3 です。
   b. ストレージ アカウントを選択します。

      注: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 アカウントを作成することができます。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。

      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。

      注: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. ASAv 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。

   注: 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。

11. 構成サマリを確認し、[OK] をクリックします。
12. 利用条件を確認し、[Create] をクリックします。

次の作業

- 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、79 ページ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。

Microsoft Azure への ASAv の導入