AWS クラウドへの ASAv の導入

Amazon Web Services（AWS）クラウドに ASAv を展開できます。

AWS クラウドへの ASAv の導入について

Cisco 適応型セキュリティ仮想アプライアンス（ASAv）は、物理の Cisco ASA と同じソフトウェアを実行して、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。ASAv は、パブリック AWS クラウドに導入できます。その後設定を行うことで、時間の経過とともにロケーションを展開、契約、またはシフトする仮想および物理データセンターのワークロードを保護できます。

ASAv は、次の AWS インスタンスタイプをサポートしています。

表 *1 : AWS* 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	ASAv モデルのサポート	注
c3.large c4.large m4.large	• 2 vCPU • 3.75 GB • 2 つのデータ インターフェイス • 1 つの管理インターフェイス	• ASAv10 • ASAv30	リソースのアンダープロビジョニングのため、large インスタンスでの ASAv30 の使用は推奨されません。

インスタンス	属性	ASAv モデルのサポート	注
c3.xlarge c4.xlarge m4.xlarge	• 4 vCPU • 7.5 GB • 3 つのデータ インターフェイス • 1 つの管理インターフェイス	• ASAv30	xlarge インスタンスでサポートされるのは ASAv30 のみです。

AWS にアカウントを作成し、AWS ウィザードを使用して ASAv をセットアップして、Amazon Machine Image（AMI）を選択します。AMI はインスタンスを起動するために必要なソフトウェア構成を含むテンプレートです。

重要 AMI イメージは AWS 環境の外部ではダウンロードできません。

ASAv と AWS の前提条件

- aws.amazon.com でアカウントを作成します。
- 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。「ASAv のライセンス」を参照してください。
- インターフェイスの要件：
  - 管理インターフェイス
  - 内部および外部インターフェイス
  - （任意）追加のサブネット（DMZ）
- 通信パス：
  - 管理インターフェイス：ASDM に ASAv を接続するために使用され、トラフィックの通過には使用できません。
  - 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）：c3.xlarge インターフェイスを使用する場合に、DMZ ネットワークに ASAv を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 AWS のガイドラインと制限事項

サポートされる機能

AWS 上の ASAv は次の機能をサポートします。

- 次世代の Amazon EC2 Compute Optimized インスタンスファミリである Amazon EC2 C5 インスタンスのサポート
- 仮想プライベート クラウド（VPC）への導入
- 拡張ネットワーク（SR-IOV）（使用可能な場合）
- Amazon マーケットプレイスからの導入
- 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
- ルーテッド モード（デフォルト）

サポートされない機能

AWS 上の ASAv は以下をサポートしません。

- 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
- VLAN
- 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）
- マルチ コンテキスト モード
- クラスタ
- ASAv のネイティブ HA
- EtherChannel は、ダイレクト物理インターフェイスのみでサポートされる
- VM のインポート/エクスポート
- Amazon Cloudwatch
- ハイパーバイザに非依存のパッケージ
- VMware ESXi

- ブロードキャスト/マルチキャスト メッセージ

  これらのメッセージは AWS 内で伝播されないため、ブロードキャスト/マルチキャストを必要とするルーティング プロトコルは AWS で予期どおりに機能しません。VXLAN はスタティック ピアでのみ動作できます。

- Gratuitous/非要請 ARP

  これらの ARPS は AWS 内では受け入れられないため、Gratuitous ARP または非要請 ARP を必要とする NAT 設定は期待どおりに機能しません。

設定の移行と SSH 認証

SSH 公開キー認証使用時のアップグレードの影響：SSH 認証が更新されることにより、SSH 公開キー認証を有効にするための新たな設定が必要となります。そのため、アップグレード後は、公開キー認証を使用した既存の SSH 設定は機能しません。公開キー認証は、Amazon Web サービス（AWS）の ASAv のデフォルトであるため、AWS のユーザはこの問題を確認する必要があります。SSH 接続を失なう問題を避けるには、アップグレードの前に設定を更新します。または（ASDM アクセスが有効になっている場合）アップグレード後に ASDM を使用して設定を修正できます。

次は、ユーザ名「admin」の元の設定例です。

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

ssh authentication コマンドを使用するには、アップグレードの前に次のコマンドを入力します。

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

nopassword キーワードが存在している場合、これを維持するのではなく、代わりにユーザ名に対応したパスワードを設定することを推奨します。**nopassword** キーワードは、パスワードは入力不可を意味するのではなく、任意のパスワードを入力できます。9.6(2) より前のバージョンでは、**aaa** コマンドは SSH 公開キー認証に必須ではありませんでした。このため、**nopassword** キーワードはトリガーされませんでした。9.6(2) では **aaa** コマンドが必須となり、**password**（または **nopassword**）キーワードが存在する場合、自動的に **username** の通常のパスワード認証を許可するようになりました。

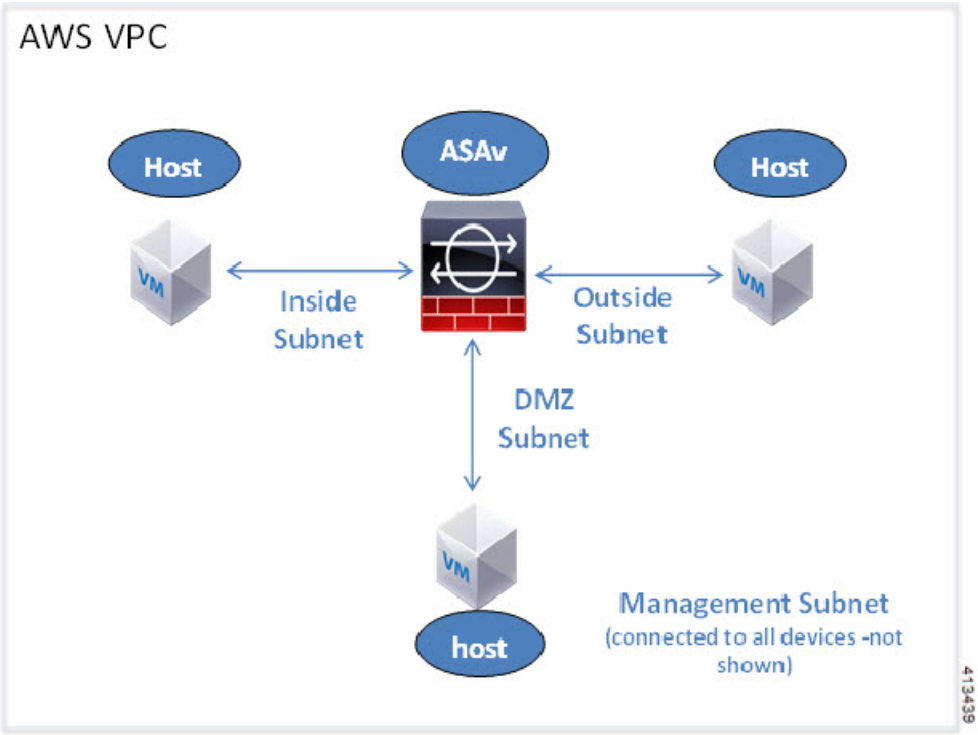
アップグレード後は、 **username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザがパスワードを入力できなくするよう指定できるようになります。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

AWS 上の ASAv のネットワーク トポロジの例

次の図は、ASAv 用に AWS 内で設定された 4 つのサブネット（管理、内部、外部、および DMZ）を備える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。

図 *1 : AWS* への *ASAv* の導入の例



AWS への ASAv の導入

次の手順は、ASAv で AWS をセットアップする手順の概略を示しています。設定の詳細な手順については、『Getting Started with AWS』を参照してください。

ステップ 1 aws.amazon.com にログインし、地域を選択します。

（注） AWS は互いに分離された複数の地域に分割されます。地域は、画面の右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。定期的に、目的の地域内に存在していることを確認してください。

ステップ 2 **[My Account]** > **[AWS Management Console]** をクリックし、[Networking] で **[VPC]** > **[Start VPC Wizard]** をクリックして、単一のパブリック サブネットを選択して VPC を作成し、次を設定します（特記のないかぎり、デフォルト設定を使用できます）。

- 内部および外部のサブネット：VPC およびサブネットの名前を入力します。
- インターネット ゲートウェイ：インターネット経由の直接接続を有効にします（インターネット ゲートウェイの名前を入力します）。
- 外部テーブル：インターネットへの発信トラフィックを有効にするためのエントリを追加します（インターネット ゲートウェイに 0.0.0.0/0 を追加します）。

ステップ 3 **[My Account]** > **[AWS Management Console]** > **[EC2]** をクリックし、さらに、[Create an Instance] をクリックします。

- AMI（たとえば、Ubuntu Server 14.04 LTS）を選択します。

  イメージ配信通知で識別された AMI を使用します。
- ASAv（たとえば、c3.large）によってサポートされるインスタンス タイプを選択します。
- インスタンスを設定します（CPU とメモリは固定です）。
- [Advanced Details] で、必要に応じて第 0 日用構成を追加します。第 0 日用構成にスマート ライセンスなどの詳細情報を設定する方法の詳細については、「第 0 日のコンフィギュレーション ファイルの準備」を参照してください。

  第 0 日用構成の例

```
! ASA Version 9.4.1.200
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 30
username admin nopassword privilege 15
username admin attributes
service-type admin
! required config end
! example dns configuration
dns domain-lookup management
DNS server-group DefaultDNS
! where this address is the .2 on your public subnet
name-server 172.19.0.2
! example ntp configuration
name 129.6.15.28 time-a.nist.gov
name 129.6.15.29 time-b.nist.gov
name 129.6.15.30 time-c.nist.gov
ntp server time-c.nist.gov
ntp server time-b.nist.gov
ntp server time-a.nist.gov
```

- ストレージ（デフォルトを受け入れます）。

- タグ インスタンス：デバイスを分類するため、多数のタグを作成できます。タグを容易に見つけるために使用できる名前を付けます。
- セキュリティ グループ：セキュリティ グループを作成して名前を付けます。セキュリティ グループは、着信および発信トラフィックを制御するためのインスタンスの仮想ファイアウォールです。

  デフォルトでは、セキュリティ グループはすべてのアドレスに対して開かれています。ASAv のアクセスに使用するアドレスからの SSH 接続だけを許可するように、ルールを変更します。
- 設定を確認し、[Launch] をクリックします。

ステップ 4 キー ペアを作成します。

注意 キー ペアにわかりやすい名前を付け、キーを安全な場所にダウンロードします。再度、ダウンロードすることはできません。キー ペアを失った場合は、インスタンスを破棄し、それらを再度導入する必要があります。

ステップ 5 [Launch Instance] をクリックして、ASAv を導入します。

ステップ 6 **[My Account]** > **[AWS Management Console]** > **[EC2]** > **[Launch an Instance]** > **[My AMIs]** をクリックします。

ステップ 7 ASAv のインターフェイスごとに [Source/Destination Check] が無効になっていることを確認します。

AWS のデフォルト設定では、インスタンスは、その IP アドレス宛てのトラフィックの受信のみが許可され、さらに、自身の IP アドレスからのトラフィックの送信のみが許可されます。ASAv のルーテッド ホップとしての動作を有効にするには、ASAvの各トラフィック インターフェイス（内部、外部、およびDMZ）の [Source/Destination Check] を無効にする必要があります。