AWS クラウドへの ASA 仮想 の導入

Amazon Web Services（AWS）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 AWS インスタンスタイプの数も増えます。

AWS クラウドへの ASA 仮想 の導入について

ASA 仮想 は、物理 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。ASA 仮想 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。

ASA 仮想 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		インターフェイス
	vCPU	メモリ（GB）	
c5.xlarge	4	8	4

インスタンス	属性		インターフェイス
	vCPU	メモリ（GB）	
c5.2xlarge	8	16	4
c4.large	2	3.75	3
c4.xlarge	4	7.5	4
c4.2xlarge	8	15	4
c3.large	2	3.75	3
c3.xlarge	4	7.5	4
c3.2xlarge	8	15	4
m4.large	2	4	3
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
c5a.large	2	4	3
c5a.xlarge	4	8	4
c5a.2xlarge	8	16	4
c5a.4xlarge	16	32	8
c5ad.large	2	4	3
c5ad.xlarge	4	8	4
c5ad.2xlarge	8	16	4
c5ad.4xlarge	16	32	8
c5d.large	2	4	3
c5d.xlarge	4	8	4
c5d.2xlarge	8	16	4
c5d.4xlarge	16	32	8
g4ad.4xlarge	16	64	3
g4dn.xlarge	4	16	3
g4dn.2xlarge	8	32	3
g4dn.4xlarge	16	64	3
i3en.large	2	16	3
i3en.xlarge	4	32	4
i3en.2xlarge	8	64	4

インスタンス	属性		インターフェイス
	vCPU	メモリ（GB）	
i3en.3xlarge	12	96	4
inf1.xlarge	4	8	4
inf1.2xlarge	8	16	4
m5.large	2	8	3
m5.xlarge	4	16	4
m5.2xlarge	8	32	4
m5.4xlarge	16	64	8
m5a.large	2	8	3
m5a.xlarge	4	16	4
m5a.2xlarge	8	32	4
m5a.4xlarge	16	64	8
m5ad.large	2	8	3
m5ad.xlarge	4	16	4
m5ad.2xlarge	8	32	4
m5ad.4xlarge	16	64	8
m5d.large	2	8	3
m5d.xlarge	4	16	4
m5d.2xlarge	8	32	4
m5d.4xlarge	16	64	8
m5dn.large	2	8	3
m5dn.xlarge	4	16	4
m5dn.2xlarge	8	32	4
m5dn.4xlarge	16	64	8
m5n.large	2	8	3
m5n.xlarge	4	16	4
m5n.2xlarge	8	32	4
m5n.4xlarge	16	64	8
m5zn.large	2	8	3
m5zn.xlarge	4	16	4
m5zn.2xlarge	8	32	4
m5zn.3xlarge	12	48	8

インスタンス	属性		インターフェイス
	vCPU	メモリ（GB）	
r5.large	2	16	3
r5.xlarge	4	32	4
r5.2xlarge	8	64	4
r5.4xlarge	16	128	8
r5a.large	2	16	3
r5a.xlarge	4	32	4
r5a.2xlarge	8	64	4
r5a.4xlarge	16	128	8
r5ad.large	2	16	3
r5ad.xlarge	4	32	4
r5ad.2xlarge	8	64	4
r5ad.4xlarge	16	128	8
r5b.large	2	16	3
r5b.xlarge	4	32	4
r5b.2xlarge	8	64	4
r5b.4xlarge	16	128	8
r5d.large	2	16	3
r5d.xlarge	4	32	4
r5d.2xlarge	8	64	4
r5d.4xlarge	16	128	8
r5dn.large	2	16	3
r5dn.xlarge	4	32	4
r5dn.2xlarge	8	64	4
r5dn.4xlarge	16	128	8
r5n.large	2	16	3
r5n.xlarge	4	32	4
r5n.2xlarge	8	64	4
r5n.4xlarge	16	128	8
z1d.large	2	16	3
z1d.xlarge	4	32	4
z1d.2xlarge	8	64	4

インスタンス	属性		インターフェイス
	vCPU	メモリ（GB）	
z1d.3xlarge	12	96	8

ヒント　M4 または C4 インスタンスタイプを使用している場合は、パフォーマンスを向上させるために、Nitro ハイパーバイザと Elastic Network Adapter（ENA）インターフェイスドライバを使用する C5 または M5 インスタンスタイプに移行することを推奨します。

AWS にアカウントを作成し、AWS ウィザードを使用して ASA 仮想 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。

ASA 仮想 と AWS の前提条件

- aws.amazon.com でアカウントを作成します。
- 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。「ASA 仮想 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 ASA 仮想 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 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）：c3.xlarge インターフェイスを使用する場合、DMZ ネットワークに ASA 仮想 を接続するために使用されます。

- ASA 仮想 システム要件については、Cisco Secure Firewall ASA の互換性 [英語] を参照してください。

ASA 仮想 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 ASA 仮想 は、次の機能をサポートしています。

- 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）への展開
- 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展開
- L3 ネットワークのユーザー展開
- ルーテッド モード（デフォルト）
- Amazon CloudWatch

サポートされない機能

AWS 上の ASA 仮想 は、以下の機能をサポートしていません。

- 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）
- 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
- ASA 仮想 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
- 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。

- IPv6

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 Services（AWS）の ASA 仮想 のデフォルトであるため、AWS ユーザーにはこの問題が表示されます。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、ユーザー名「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、代わりにユーザー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。

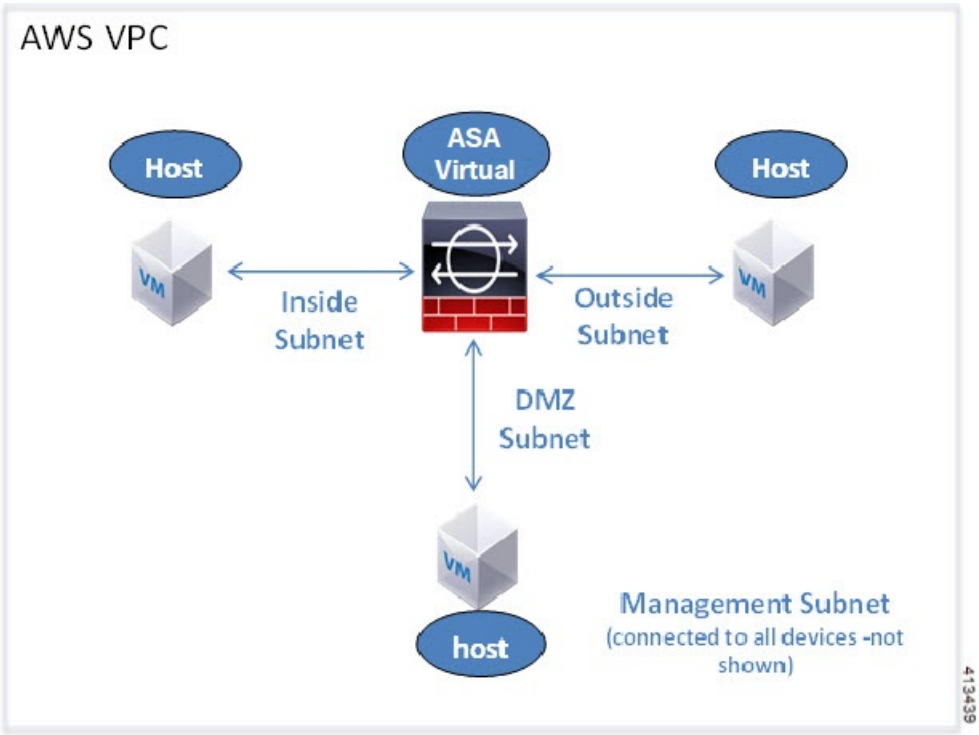
アップグレード後は、 **username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザーがパスワードを入力できなくするよう指定できるようになります。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

AWS 上の ASA 仮想 のネットワークトポロジの例

次の図は、ASA 仮想 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）を備えたルーテッド ファイアウォール モードの ASA 仮想 の推奨トポロジを示しています。

図 *1: AWS* への *ASA* 仮想 の導入例



AWS での ASA 仮想 の展開

次の手順は、ASA 仮想 で AWS をセットアップする手順の概略です。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 は互いに分かれた複数の地域に分割されています。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。目的の地域内に存在していることを定期的に確認してください。

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。
- ASA 仮想 でサポートされるインスタンスタイプ（c3.large など）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）。
- [高度な詳細（Advanced Details）] セクションを導入し、[ユーザーデータ（User data）] フィールドに、オプションで第 0 日用構成を入力できます。これは、ASA 仮想 の起動時に適用される ASA 仮想 構成を含むテキスト入力です。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。
  - **管理インターフェイス**：第 0 日用構成を選択する場合は、管理インターフェイスの詳細を指定する**必要**があります。これは DHCP を使用するように設定する必要があります。
  - **データインターフェイス**：データインターフェイスの IP アドレスは、その情報を第 0 日用構成の一部として指定した場合にのみ割り当てられ、設定されます。データインターフェイスは、DHCP を使用するように設定できます。または、接続するネットワーク インターフェイスがすでに作成されていて、IP アドレスがわかっている場合は、第 0 日用構成で IP の詳細を指定できます。
  - **第 0 日用構成なし**：第 0 日用構成を指定**せず**に ASA 仮想 を導入すると、ASA 仮想 はデフォルトの ASA 仮想 構成を適用し、AWS メタデータサーバーから接続されたインターフェイスの IP を取得し、IP アドレスを割り当てます（データインターフェイスに IP は割り当てられますが、ENI はダウンします）。Management0/0 インターフェイスが起動し、DHCP アドレスで設定された IP を取得します。Amazon EC2 および Amazon VPC の IP アドレッシングについては、「VPC での IP アドレッシング」を参照してください。
- **第 0 日用構成の例**：

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!
crypto key generate rsa modulus 2048
ssh 0 0 management
```

```
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

no shutdown
!
interface G0/1
nameif inside
ip address dhcp

no shutdown
!
```

- 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。ASA 仮想 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 [インスタンスの起動（Launch Instance）] をクリックして、ASA 仮想 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 ASA 仮想 のインターフェイスごとに [送信元または宛先の確認（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（IPv4）のトラフィックのみを受信でき、インスタンスは独自の IP アドレス（IPv4）からのみトラフィックを送信できます。ASA 仮想 のルーテッ

ドホップとしての動作を有効にするには、ASA 仮想 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 [送信元または宛先の確認（Source/Destination Check）] を無効にする必要があります。

AWS での ASA 仮想 のパフォーマンス調整

VPN の最適化

AWS c5 インスタンスは、以前の c3、c4、および m4 インスタンスよりもはるかに高いパフォーマンスを提供します。c5 インスタンスファミリでのおおよその RA VPN スループット（AES-CBC 暗号化による 450B TCP トラフィックを使用する DTLS）は、以下のようである必要があります。

- 0.5 Gbps（c5.large）
- 1 Gbps（c5.xlarge）
- 2 Gbps（c5.2xlarge）

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。