AWS での Threat Defense Virtual の展開

この章では、AWS ポータルから Threat Defense Virtual を展開する方法について説明します。

概要

AWS はパブリッククラウド環境です。Threat Defense Virtual は、次のインスタンスタイプの AWS 環境でゲストとして実行されます。

表 *1:* システム要件

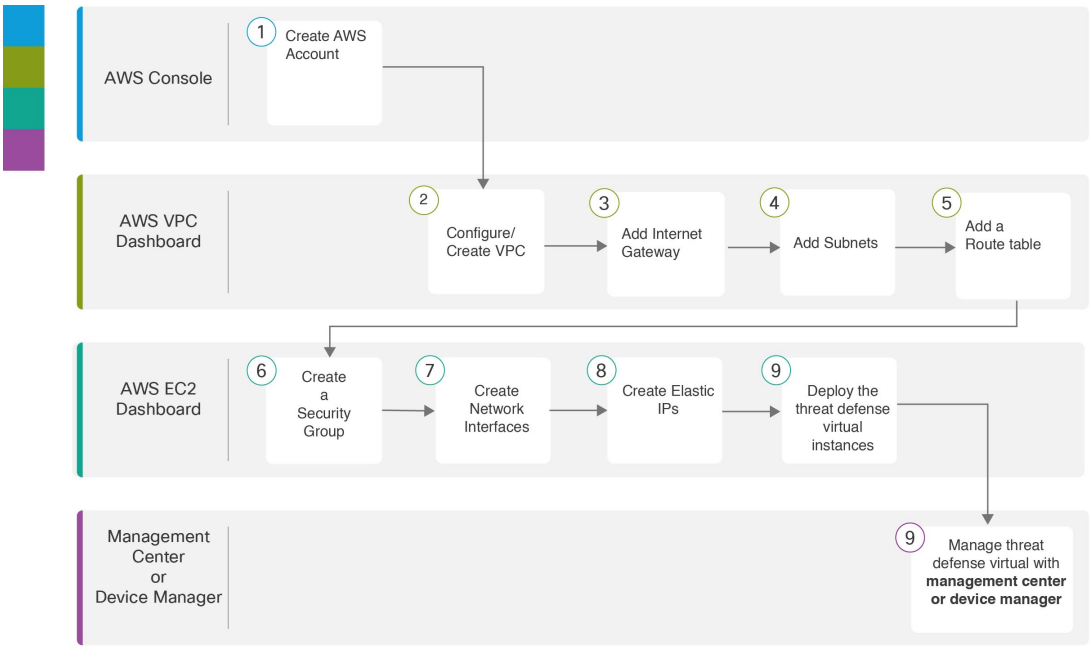
インスタンス タイプ	Threat Defense Virtual	vCPU	メモリ（GB）	インターフェイスの最大数
c5a.xlarge	7.1.0 以上	4	8	4
c5a.2xlarge		8	16	4
c5a.4xlarge		16	32	8
c5ad.xlarge		4	8	4
c5ad.2xlarge		8	16	4
c5ad.4xlarge		16	32	8
c5d.xlarge		4	8	4
c5d.2xlarge		8	16	4
c5d.4xlarge		16	32	8
c5n.xlarge		4	10.5	4
c5n.2xlarge		8	21	4
c5n.4xlarge		16	54	8
m5n.xlarge		4	16	4
m5n.2xlarge		8	32	4
m5n.4xlarge		16	64	8
m5zn.xlarge		4	16	4
m5zn.2xlarge		8	32	4
c5.xlarge	6.6.0 以上	4	8	4
c5.2xlarge		8	16	4
c5.4xlarge		16	32	8
c4.xlarge	6.4.0 以降	4	7.5	4
c3.xlarge		4	7.5	4

（注） Threat Defense Virtual では、インスタンスサイズのサイズ変更によるインスタンスタイプの変更はサポートされていません。新規展開でのみ、異なるインスタンスサイズで Threat Defense Virtual を展開できます。

AWS マーケットプレイスにリストされている NGFWv でサポートされている EC2 インスタンスタイプについては、https://aws.amazon.com/marketplace/pp/prodview-p2336sqyya34e#pdp-overview を参照してください。

エンドツーエンドの手順

次のフローチャートは、Amazon Web Services（AWS）に Threat Defense Virtual を展開する際のワークフローを示しています。



	ワークスペース	手順
1	AWS コンソール	www.amazon.com：AWS コンソールでユーザーアカウントを作成します。
2	AWS VPC ダッシュボード	VPC の作成：AWS アカウント専用の VPC を作成および設定します。
3	AWS VPC ダッシュボード	インターネット ゲートウェイの追加：VPC をインターネットに接続するために、インターネットゲートウェイを追加します。
4	AWS VPC ダッシュボード	サブネットの追加：VPC にサブネットを追加します。

	ワークスペース	手順
5	AWS VPC ダッシュボード	ルートテーブルの追加：VPC 用に設定したゲートウェイにルートテーブルを接続します。
6	AWS EC2 ダッシュボード	セキュリティ グループの作成：許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティグループを作成します。
7	AWS EC2 ダッシュボード	ネットワーク インターフェイスの作成：静的 IP アドレスを使用して、Threat Defense Virtual のネットワーク インターフェイスを作成します。
8	AWS EC2 ダッシュボード	Elastic IP の作成：Elastic IP は、Threat Defense Virtual および他のインスタンスへのリモートアクセスに使用されるパブリック IP 用に予約されます。
9	AWS EC2 ダッシュボード	Threat Defense Virtual の導入：AWS ポータルから Threat Defense Virtual を展開します。
10	Management Centerまたは Device Manager	Threat Defense Virtual を次のように管理します。 • Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 • Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理

Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual デバイスの管理には次の 2 つのオプションを選択できます。

Secure Firewall Management Center

多数のデバイスを管理している場合、または Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの Device Manager の代わりに Management Center を使用してデバイスを設定します。

重要 Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager のオンボード管理サービスは無効になります。

注意 現在、シスコには Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

（注） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

AWS ソリューションの概要

AWS は、Amazon.com によって提供されるリモート コンピューティング サービスの集合で、Web サービスとも呼ばれており、クラウド コンピューティング プラットフォームを構成します。これらのサービスは、世界の 11 の地理的地域で運用されます。通常、Secure Firewall Management Center Virtual（旧称 Firepower Management Center Virtual）および Threat Defense Virtual を展開する際には、以下の AWS サービスに精通している必要があります。

- Amazon Elastic Compute Cloud（EC2）：仮想コンピュータをレンタルして、お客様独自のアプリケーションおよびサービス（ファイアウォールなど）を Amazon のデータセンターで起動および管理できるようにする Web サービス。
- Amazon Virtual Private Cloud（VPC）：Amazon パブリック クラウド内の隔離されたプライベート ネットワークを設定できるようにする Web サービス。EC2 インスタンスは VPC 内で実行されます。

- Amazon Simple Storage Service（S3）：データ ストレージ インフラストラクチャを提供する Web サービス。

AWS でアカウントを作成し、VPC および EC2 コンポーネントを（AWS ウィザードまたは手動設定のいずれかを使用して）設定し、Amazon Machine Image（AMI）インスタンスを選択します。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。

Note 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。

前提条件

- AWS アカウントhttp://aws.amazon.com/ で 1 つ作成できます。
- Threat Defense Virtual コンソールにアクセスするには、SSH クライアント（例：Windows の場合は PuTTY、MacOS の場合はターミナル）が必要です。
- Cisco スマートアカウント。Cisco Software Central で 1 つ作成できます。https://software.cisco.com/
- Threat Defense Virtual へのライセンス付与。

  Cisco Secure Firewall Management Center

  - Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「Licensing the System」を参照してください。

  Secure Firewall デバイスマネージャ

  - Secure Firewall デバイスマネージャ からセキュリティサービスのすべてのパフォーマンス階層型ライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、「Threat Defense Virtual のライセンス」を参照してください。

- Threat Defense Virtual インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Threat Defense Virtual を Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。

    、管理インターフェイスの代わりに、必要に応じて、データインターフェイスを Management Center の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。

データインターフェイスから Management Center へのアクセスは、高可用性の展開ではサポートされません。Management Center へのアクセスに関するデータインターフェイス設定の詳細については、『FTD command reference』の **configure network management-data-interface** コマンドを参照してください。

- トラフィック インターフェイス（2）：Threat Defense Virtual を内部のホストおよびパブリック ネットワークに接続するために使用されます。

- 通信パス：
  - Threat Defense Virtual にアクセスするためのパブリック IP/Elastic IP。

サポートされるソフトウェア プラットフォーム

Threat Defense Virtual Auto Scale ソリューションは、Management Center によって管理される Threat Defense Virtual に適用可能です。ソフトウェアバージョンには依存しません。『Cisco Firepower Compatibility Guide』には、オペレーティングシステムとホスティング環境の要件を含む、シスコのソフトウェアとハードウェアの互換性が記載されています。

- Firepower Management Centers: Virtual の表には、AWS 上の Management Center Virtual における互換性および仮想ホスティング環境の要件が一覧表示されています。
- Firepower Threat Defense Virtual Compatibility の表には、AWS 上の Threat Defense Virtual における互換性および仮想ホスティング環境の要件が一覧表示されています。

Note AWS Auto Scale ソリューションを導入するためには、AWS 上で Threat Defense Virtual バージョン 6.4 以上を使用する必要があります。メモリベースのスケーリングを使用するには、Management Center バージョン 6.6 以降を実行している必要があります。

注意事項と制約事項

サポートされる機能

- 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）。
- Amazon マーケットプレイスからの導入
- L3 ネットワークの導入
- ルーテッドモード（デフォルト）
- ERSPAN を使用するパッシブモード

- クラスタリング (バージョン 7.2 以降) 詳細については、『パブリッククラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。
- Amazon CloudWatch によって記録されたヘルスモニタリングのメトリクス
- ジャンボ フレーム
- スナップショット (バージョン 7.2 以降)
- IPv6

サポートされない機能

- 複製
- トランスペアレントモード、インラインモード、パッシブモード
- Transport Layer Security（TLS）サーバーアイデンティティ検出は、AWS での Geneve シングルアームセットアップではサポートされていません。

ライセンシング

- シスコ スマート ライセンス アカウントを使用する BYOL（Bring Your Own License）がサポートされています。
- PAYG（Pay As You Go）ライセンス。顧客がシスコ スマート ライセンシングを購入せずに Threat Defense Virtual を実行できる従量制課金モデル。登録された PAYG Threat Defense Virtual デバイスでは、ライセンス供与されたすべての機能（マルウェア、脅威、URL フィルタリング、VPN など）が有効になっています。これらのライセンス機能には、登録済みの Management Center でアクティブとして自動的にフラグが付けられます。ライセンス供与された機能は、Management Center から編集または変更することはできません（バージョン 6.5 以上）。

Note PAYG ライセンスは、Device Manager モードで展開されている Threat Defense Virtual デバイスではサポートされていません。

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Firepower Management Center Administration Guide』の「Licenses」の章を参照してください。

Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual のバージョン 7.0.0 リリース以降では、Threat Defense Virtual は導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。

Table 2: Threat Defense Virtual 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	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5	4 コア/8 GB	100 Mbps	50
FTDv10	4 コア/8 GB	1 Gbps	250
FTDv20	4 コア/8 GB	3Gbps	250
FTDv30	8 コア/16 GB	5 Gbps	250
FTDv50	12 コア/24 GB	10 Gbps	750
FTDv100	16 コア/34 GB	16 Gbps	10,000

パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「AWS での仮想化の調整と最適化」を参照してください。

Receive Side Scaling：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

Threat Defense Virtual の制限事項

- 推奨されるインスタンスは c5.xlarge です。c3.xlarge インスタンスでは AWS リージョンでの可用性が制限されます。
- 起動時には、2 つの管理インターフェイスが構成されている必要があります。
- 起動するには、2 つのトラフィック インターフェイスと 2 つの管理インターフェイス（合計 4 つのインターフェイス）が必要です。

Note Threat Defense Virtual はこの 4 つのインターフェイスがなければ起動しません。

- AWS でトラフィック インターフェイスを設定する場合、[送信元/宛先の変更の確認（Change Source/Dest. Check）] オプションを無効にする必要があります。
- IP アドレス（IPv4 および IPv6）設定は（CLI から設定したものでも Management Center から設定したものでも）AWS コンソールで作成されたものと一致する必要があります。展開時に設定を書き留めてください。

- Threat Defense Virtual を登録した後、インターフェイスを編集し、Management Center で有効にする必要があります。IP アドレスは、AWS で設定されたインターフェイスと一致している必要があることに注意してください。
- トランスペアレント モード、インライン モード、パッシブ モードは現時点でサポートされていません。
- インターフェイスを変更するには、AWS コンソールから変更を行う必要があります。AWS コンソールで、Management Center からインターフェイスの登録を解除し、AWS AMI ユーザーインターフェイスを使用しているインスタンスを停止します。次に、変更するインターフェイスを切り離し、新しいインターフェイスを接続します（起動するには、2 つのトラフィック インターフェイスと 2 つの管理インターフェイスが必要であることに注意してください）。ここで、インスタンスを起動し、Management Center に再登録します。

  Management Center から、デバイスインターフェイスを編集し、AWS コンソールから行った変更と一致するように、IP アドレス（IPv4 および IPv6）と他のパラメータを変更します。

Note IPv6 は、デュアルスタック（IPv4 + IPv6）モードでのみ使用できます。

- ブート後にインターフェイスを追加することはできません。
- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

AWS 環境の設定

Threat Defense Virtual を AWS に展開するには、展開に固有の要件および設定を使用して Amazon VPC を設定する必要があります。ほとんどの環境では、セットアップ ウィザードに従ってセットアップを実行できます。AWS では、概要から詳細機能に至るまで、サービスに関する有用な情報を扱ったオンライン ドキュメントを提供しています。詳細については、https://aws.amazon.com/documentation/gettingstarted/ を参照してください。

AWS のセットアップを適切に制御するために、続くセクションでは、Threat Defense Virtual インスタンスの起動前の VPC および EC2 構成について説明します。

- VPC の作成, on page 11

はじめる前に

- AWS アカウントを作成します。
- AMI を Threat Defense Virtual インスタンスに使用できることを確認します。

VPC の作成

仮想プライベート クラウド（VPC）は、AWS アカウント専用の仮想ネットワークです。これは、AWS クラウド内の他の仮想ネットワークから論理的に分離されています。Management Center Virtual や Threat Defense Virtual インスタンスなどの AWS リソースを VPC に起動できます。VPC を設定できます。さらに、その IP アドレス範囲を選択し、サブネットを作成し、ルート テーブル、ネットワーク ゲートウェイ、およびセキュリティ設定を作成できます。

VPC とサブネットで IPv6 CIDR ブロックを有効にする方法については、AWS のドキュメント『Enable IPv6 in a VPC with a public and private subnet』を参照してください。

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

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 [サービス（Services）] > [VPC] の順にクリックします。

ステップ 3 [VPCダッシュボード（VPC Dashboard）] > [使用するVPC（Your VPCs）] の順にクリックします。

ステップ 4 [VPCの作成（Create VPC）] をクリックします。

ステップ 5 [VPCの作成（Create VPC）] ダイアログボックスで、次のものを入力します。

a) VPC を識別するユーザー定義の [名前タグ（Name tag）]。

b) IP アドレスの **IPv4 CIDR ブロック**。CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。たとえば、「10.0.0.0/24」と入力します。

c) IP アドレスの **IPv6 CIDR ブロック**。CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。[::/0] が例として挙げられます。

d) 仮想プライベートクラウドで IPv6 を有効にするには、**Amazon 提供の IPv6 CIDR ブロック**として **IPv6 CIDR ブロック**を選択します。
e) [デフォルト（Default）] の [テナント（Tenancy）] 設定。この VPC で起動されたインスタンスが、起動時に指定されたテナント属性を使用するようにします。

ステップ 6 [はい、作成します（Yes, Create）] をクリックして、VPC を作成します。

What to do next

Note 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。

次のセクションで説明されているように、VPC にインターネット ゲートウェイを追加します。

インターネット ゲートウェイの追加

VPC をインターネットに接続するために、インターネット ゲートウェイを追加できます。VPC の外部の IP アドレスのトラフィックをインターネット ゲートウェイにルーティングできます。

はじめる前に

- Threat Defense Virtual のインスタンスの VPC を作成します。

ステップ 1 [サービス（Services）] > [VPC] の順にクリックします。
ステップ 2 [VPC ダッシュボード（VPC Dashboard）] > [インターネットゲートウェイ（Internet Gateway）] の順にクリックしてから、[インターネットゲートウェイの作成（Create Internet Gateway）] をクリックします。
ステップ 3 ユーザー定義の [名前タグ（Name tag）] を入力してゲートウェイを特定し、[はい、作成します（Yes, Create）] をクリックしてゲートウェイを作成します。
ステップ 4 前のステップで作成したゲートウェイを選択します。
ステップ 5 [VPCに接続（Attach to VPC）] をクリックして、以前に作成した VPC を選択します。
ステップ 6 [はい、接続します（Yes, Attach）] をクリックして、ゲートウェイを VPC に追加します。

デフォルトでは、ゲートウェイが作成されて VPC に接続されるまで、VPC で起動されたインスタンスはインターネットと通信できません。

What to do next

次のセクションで説明されているように、VPC にサブネットを追加します。

サブネットの追加

Threat Defense Virtual のインスタンスが接続できる VPC の IP アドレス範囲をセグメント化することができます。セキュリティおよび運用のニーズに応じて、インスタンスをグループ化するためのサブネットを作成できます。Threat Defense Virtual では、管理用のサブネットとトラフィック用のサブネットを作成する必要があります。

はじめる前に

- Threat Defense Virtual のインスタンスの VPC を作成します。

ステップ 1 [サービス（Services）] > [VPC] の順にクリックします。

ステップ 2 [VPCダッシュボード（VPC Dashboard）]>[サブネット（Subnets）] の順にクリックして、[サブネットの作成（Create Subnet）] をクリックします。

ステップ 3 [サブネットの作成（Create Subnet）] ダイアログボックスで、次のものを入力します。

a) サブネットを識別するユーザー定義の [名前タグ（Name tag）]。

b) このサブネットに使用する [VPC]。

c) このサブネットが存在する [可用性ゾーン（Availability Zone）]。 [設定なし（No Preference）] を選択して、Amazon が選択するゾーンを選びます。

d) IP アドレスの [CIDRブロック（CIDR block）]（IPv4 および IPv6）。サブネットの IP アドレスの範囲は、VPC の IP アドレス範囲のサブセットである必要があります。ブロック サイズは、/16 ネットワーク マスクから /28 ネットワーク マスクの範囲で指定する必要があります。サブネットのサイズは VPC のサイズと同じにすることができます。

ステップ 4 [はい、作成します（Yes, Create）] をクリックして、サブネットを作成します。

ステップ 5 必要な数のサブネットについて、手順を繰り返します。管理トラフィックには別のサブネットを作成し、データ トラフィックに必要な数のサブネットを作成します。

What to do next

次のセクションで説明されているように、VPC にルート テーブルを追加します。

ルート テーブルの追加

VPC 用に設定したゲートウェイにルート テーブルを接続できます。また、複数のサブネットを 1 つのルート テーブルに関連付けることができます。しかし、1 つのサブネットは一度に 1 つのルート テーブルにしか関連付けることができません。

ステップ 1 [サービス（Services）] > [VPC] の順にクリックします。

ステップ 2 [VPCダッシュボード（VPC Dashboard）] > [ルートテーブル（Route Tables）] の順にクリックしてから、[ルートテーブルの作成（Create Route Table）] をクリックします。

ステップ 3 ルート テーブルを識別するユーザー定義の [名前タグ（Name tag）] を入力します。

ステップ 4 このルート テーブルを使用する [VPC] をドロップダウン リストから選択します。

ステップ 5 [はい、作成します（Yes, Create）] をクリックして、ルート テーブルを作成します。

ステップ 6 作成したルート テーブルを選択します。

ステップ 7 [ルート（Routes）] タブをクリックして、詳細ペインにルート情報を表示します。

ステップ 8 [編集（Edit）] をクリックして、[別のルートを追加（Add another route）] をクリックします。

a) [宛先（Destination）] 列に、「0.0.0.0/0」、または、IPv6 トラフィックについてはすべて [::/0] を入力します。

b) [ターゲット（Target）] 列で、ゲートウェイを選択します。

ステップ 9 [保存（Save）] をクリックします。

What to do next

次のセクションで説明するように、セキュリティ グループを作成します。

セキュリティ グループの作成

許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティ グループを作成できます。各インスタンスに割り当てることができる、さまざまな異なるルールを使用して、複数のセキュリティ グループを作成できます。

ステップ 1 [サービス（Services）] > [EC2] の順にクリックします。

ステップ 2 [EC2ダッシュボード（EC2 Dashboard）] > [セキュリティグループ（Security Groups）] の順にクリックします。

ステップ 3 [セキュリティグループの作成（Create Security Group）] をクリックします。

ステップ 4 [セキュリティグループの作成（Create Security Group）] ダイアログボックスで、次の内容を入力します。

a) セキュリティ グループを識別するユーザー定義の [セキュリティグループ名（Security group name）]。

b) このセキュリティ グループの [説明（Description）]。

c) このセキュリティ グループに関連付けられた VPC。

ステップ 5 [セキュリティグループルール（Security group rules）] を設定します。

a) [インバウンド（Inbound）] タブをクリックして、[ルールの追加（Add Rule）] をクリックします。

Note Management Center Virtual を AWS の外部から管理するには、HTTPS および SSH アクセスが必要です。それに基づいて、送信元 IP アドレスを指定する必要があります。また、Management Center Virtual と Threat Defense Virtual の両方を AWS VPC 内で設定している場合、プライベート IP 管理サブネットアクセスを許可する必要があります。

b) [アウトバウンド（Outbound）] タブをクリックしてから、[ルールの追加（Add Rule）] をクリックして、アウトバウンドトラフィックのルールを追加するか、デフォルトの [すべてのトラフィック（All traffic）]（[タイプ（Type）] の場合）および [任意の宛先（Anywhere）]（[宛先（Destination）] の場合）のままにします。

ステップ 6 セキュリティ グループを作成するには、[作成（Create）] をクリックします。

What to do next

次のセクションで説明されているように、ネットワーク インターフェイスを作成します。

ネットワーク インターフェイスの作成

Threat Defense Virtual のネットワーク インターフェイスは、静的 IP アドレス（IPv4 および IPv6）または DHCP を使用して作成できます。具体的な展開の必要に応じてネットワーク インターフェイス（内部および外部）を作成します。

ステップ 1 [サービス（Services）] > [EC2] の順にクリックします。

ステップ 2 [EC2ダッシュボード（EC2 Dashboard）] > [ネットワークインターフェイス（Network Interfaces）] の順にクリックします。

ステップ 3 [ネットワークインターフェイスの作成（Create Network Interface）] をクリックします。

ステップ 4 [ネットワークインターフェイスの作成（Create Network Interface）] ダイアログボックスで、次のものを入力します。

a) ネットワーク インターフェイスに関するオプションのユーザー定義の [説明（Description）]。

b) ドロップダウン リストから [サブネット（Subnet）] を選択します。Threat Defense Virtual インスタンスを作成する VPC のサブネットが選択されていることを確認します。

c) [プライベートIP（Private IP）] アドレスを入力します。静的 IP アドレス（IPv4 および IPv6）または自動生成（DHCP）を使用できます。

d) [セキュリティグループ（Security groups）] を 1 つ以上選択します。セキュリティ グループの必要なポートがすべて開いていることを確認します。

ステップ 5 [ネットワーク インターフェイスの作成（Create network interface）] をクリックして、ネットワーク インターフェイスを作成します。

ステップ 6 作成したネットワーク インターフェイスを選択します。

ステップ 7 右クリックして、[送信元/宛先の変更の確認（Change Source/Dest. Check）]を選択します。

ステップ 8 [送信元または送信先の確認（Source/destination check）] の下にある [有効化（Enable）] チェックボックスをオフにして、[保存（Save）] をクリックします。

What to do next

次のセクションで説明するように、Elastic IP アドレスを作成します。

Elastic IP の作成

インスタンスが作成されると、パブリック IP アドレスはそのインスタンスに関連付けられます。インスタンスを停止してから開始すると、そのパブリック IP アドレス（IPv4 および IPv6）

は自動的に変更されます。この問題を解決するには、Elastic IP アドレッシングを使用して、永続的なパブリック IP アドレスをそのインスタンスに割り当てます。Elastic IP は、Threat Defense Virtual および他のインスタンスへのリモート アクセスに使用されるパブリック IP 用に予約されます。

Note 少なくとも、Threat Defense Virtual 管理インターフェイス用と診断インターフェイス用の Elastic IP アドレスを作成してください。

ステップ 1 [サービス（Services）] > [EC2] の順にクリックします。
ステップ 2 [EC2ダッシュボード（EC2 Dashboard）] > [Elastic IP（Elastic IPs）] の順にクリックします。
ステップ 3 [新規アドレスの割り当て（Allocate New Address）] をクリックします。
ステップ 4 必要な数の Elastic IP およびパブリック IP について、この手順を繰り返します。
ステップ 5 [はい、割り当てます（Yes, Allocate）] をクリックして、Elastic IP を作成します。
ステップ 6 展開に必要な数の Elastic IP について、この手順を繰り返します。

What to do next

次のセクションで説明されているように、Threat Defense Virtual を展開します。

Threat Defense Virtual の導入

Before you begin

次のことを推奨します。

- AWS 環境の設定, on page 10の説明に従って、AWS VPC および EC2 のエレメントを設定します。
- AMI が Threat Defense Virtual インスタンスで使用できることを確認します。

ステップ 1 https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。
ステップ 2 Amazon マーケットプレイスにログイン後、Threat Defense Virtual（Cisco Firepower NGFW Virtual（NGFWv）：BYOL）用に提供されているリンクをクリックします。

Note すでに AWS を使用していた場合、リンクを有効にするには、いったんサインアウトしてから、サインインし直す必要があります。

ステップ 3 [続行（Continue）] をクリックしてから、[手動起動（Manual Launch）] タブをクリックします。
ステップ 4 [条件に同意する（Accept Terms）] をクリックします。

ステップ 5 [EC2コンソールを使用して起動する（Launch with EC2 Console）] をクリックします。

ステップ 6 Threat Defense Virtual でサポートされる [インスタンスタイプ（Instance Type）] を選択します。推奨タイプは c4.xlarge です。

ステップ 7 画面下部にある [次：インスタンスの詳細の設定（Next: Configure Instance Details）] ボタンをクリックします。

- 前に作成した VPC に一致するように [ネットワーク（Network）] を変更します。
- 前に作成した管理サブネットに一致するように [サブネット（Subnet）] を変更します。IP アドレスを指定するか、または自動生成を使用できます。
- [パブリック IP（Public IP）]（IPv4 および IPv6）の [自動生成（Auto-generate）] を有効にすることができます。
- 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。IPv6 移行の詳細については、「AWS IPv6 の概要」と「AWS VPC」を参照してください。
- [ネットワーク インターフェイス（Network Interfaces）] の下にある [デバイスの追加（Add Device）] ボタンをクリックして、eth1 ネットワーク インターフェイスを追加します。
- eth0 に使用される、事前に作成した管理サブネットに一致するように、[サブネット（Subnet）] を変更します。

Note Threat Defense Virtual には 2 つの管理インターフェイスが必要です。

- [高度な詳細（Advanced Details）] の下で、デフォルトのログイン情報を追加します。デバイス名とパスワードの要件に合わせて、以下の例を変更してください。

注意：[高度な詳細（Advanced Details）] フィールドにデータを入力する際には、プレーンテキストのみを使用してください。テキストエディタからこの情報をコピーする場合、プレーンテキストとしてのみコピーしてください。[高度な詳細（Advanced Details）] フィールドに Unicode データ（空白を含む）をコピーする場合、インスタンスが破損する可能性があります。破損した場合は、インスタンスを終了して、作成し直す必要があります。

Management Center を使用して Threat Defense Virtual を管理するためのサンプルログイン設定：

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<your_hostname>",
            "IPv6Mode": "dhcp",
            "ManageLocally": "No",
            "FmcIp":  "<IP address of FMC>",
            "FmcRegKey":"<registration_passkey>",
            "FmcNatId":"<NAT_ID_if_required>"
}
```

Device Manager を使用して Threat Defense Virtual を管理するためのサンプルログイン設定：

```
#Sensor
```

```
{
            "AdminPassword": "<your_password>",
            "Hostname": "<your_hostname>",
            "ManageLocally": "Yes"
}
```

ステップ 8 [次：ストレージの追加（Next: Add Storage）] をクリックします。

デフォルト値で続行できます。

ステップ 9 [次：タグ インスタンス（Next: Tag Instance）] をクリックします。

タグは大文字と小文字を区別するキーと値のペアで構成されます。たとえば、[キー（Key）]=名前、[値（Value）] = ファイアウォールでタグを定義できます。

ステップ 10 [次：セキュリティ グループの設定（Next: Configure Security Group）] を選択します。

ステップ 11 [既存のセキュリティグループを選択する（Select an existing Security Group）] をクリックして、以前に設定されたセキュリティ グループを選択するか、または新しいセキュリティ グループを作成できます。セキュリティ グループの作成の詳細については、AWS の資料を参照してください。

ステップ 12 [確認して起動する（Review and Launch）] をクリックします。

ステップ 13 [起動（Launch）] をクリックします。

ステップ 14 既存のキー ペアを選択するか、新しいキー ペアを作成します。

Note 既存のキー ペアを選択することも、新しいキー ペアを作成することもできます。キー ペアは、AWS が保存する公開キーと、ユーザーが保存する秘密キー ファイルで構成されます。これらを一緒に使用すると、インスタンスに安全に接続できます。キー ペアはインスタンスへの接続に必要となる場合があるため、必ず既知の場所に保存してください。

ステップ 15 [インスタンスの起動（Launch Instances）] をクリックします。

ステップ 16 [起動の表示（View Launch）] をクリックし、プロンプトに従います。

ステップ 17 [EC2ダッシュボード（EC2 Dashboard）] > [ネットワーク インターフェイス（Network Interfaces）] の順にクリックします。

ステップ 18 AWS 環境の設定, on page 10で以前に作成したインターフェイス トラフィックを特定し、[接続（Attach）] をクリックします。これは、Threat Defense Virtual インスタンス上の **eth2** インターフェイスになります。

ステップ 19 AWS 環境の設定, on page 10で以前に作成したインターフェイス トラフィックを特定し、[接続（Attach）] をクリックします。これは、Threat Defense Virtual インスタンス上の **eth3** インターフェイスになります。

Note 4 つのインターフェイスを設定する必要があります。設定しないと、Threat Defense Virtual の起動プロセスが完了しません。

ステップ 20 [EC2ダッシュボード（EC2 Dashboard）] > [インスタンス（Instances）] の順にクリックします。

ステップ 21 インスタンスを右クリックし、[インスタンスの設定（Instance Settings）] > [システムログの取得（Get System Log）] の順に選択して、ステータスを表示します。

Note 接続の問題に関する警告が表示される可能性があります。これが予想されるのは、EULA が完了するまで eth0 インターフェイスがアクティブにならないためです。

ステップ 22 20 分後、Threat Defense Virtual を Management Center に登録します。

What to do next

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。
- [ローカルマネージャを有効にする（Enable Local Manager）] で [はい（Yes）] を選択した場合は、統合されている Device Manager を使用して Threat Defense Virtual を管理します。「Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。

管理オプションの選択方法の概要については、「Secure Firewall Threat Defense Virtual デバイスの管理方法」を参照してください。

イメージスナップショットを使用した Threat Defense Virtual

AWS ポータルで Amazon Machine Image（AMI）スナップショットを使用して Threat Defense Virtual を作成および展開できます。イメージスナップショットは、状態データのない、複製された Threat Defense Virtual イメージインスタンスです。

Threat Defense Virtualスナップショットの概要

Threat Defense Virtual インスタンスのスナップショットイメージを作成するプロセスは、Threat Defense Virtual および FSIC に対して実行される最初のブート手順をスキップすることにより、初期システムの初期化時間を最小限に抑えるのに役立ちます。スナップショットイメージは、事前に入力されたデータベースと Threat Defense Virtual 初期ブートプロセスで構成されます。これにより、イメージは Management Center またはその他の管理センターのシステム ID に関連する一意の ID（UUID、シリアル番号）を再生成できます。このプロセスは、自動スケール展開に不可欠な Threat Defense Virtual の起動時間を短縮するのに役立ちます。

Threat Defense Virtual スナップショット AMI の作成

Threat Defense Virtual のイメージスナップショットの作成は、既存の Threat Defense Virtual イメージを複製して、Azure ポータルで Threat Defense Virtual のプレーンインスタンスを作成するプロセスです。

Before you begin

- Threat Defense Virtual バージョン 7.2 以降を展開している必要があります。Threat Defense Virtual の展開については、「AWS での Threat Defense Virtual の展開, on page 1」を参照してください。
- イメージスナップショットの準備をしている Threat Defense Virtual インスタンスを Management Center Virtual や Device Manager などのマネージャに登録しないでください。

ステップ 1 Threat Defense Virtual インスタンスを展開した AWS コンソールに移動します。

Note イメージスナップショットとして複製する予定の Threat Defense Virtual インスタンスが Management Center に登録されていないこと、または他のローカルマネージャに設定されたり設定が適用されたりしていないことを確認します。

ステップ 2 次のスクリプトを使用して、エキスパートシェルからプレスナップショット プロセスを実行します。

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

スクリプトで `prepare_snapshot` コマンドを使用すると、スクリプトの実行の確認を求める中間メッセージが表示されます。スクリプトを実行するには、[Y] を押します。

または、`root@firepower:/ngfw/var/common# prepare_snapshot -f` のように、このコマンドに `-f` を追加して、ユーザーの確認メッセージをスキップしてスクリプトを直接実行することもできます。

このスクリプトは、Threat Defense Virtual インスタンスに関連付けられたすべての回線設定、展開されたポリシー、設定されたマネージャ、UUID を削除します。処理が完了すると、Threat Defense Virtual インスタンスはシャットダウンされます。Threat Defense Virtual インスタンスは、AWS ポータルの [インスタンス（Instances）] ページに一覧表示されます。

ステップ 3 http://aws.amazon.com/ にログインし、地域を選択します。

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、ウィンドウ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。目的の地域に属していることを定期的に確認してください。

What to do next

スナップショット AMI を使用して Threat Defense Virtual インスタンスを展開します。参照 スナップショット AMI を使用した Threat Defense Virtual インスタンスの展開, on page 21

Note Threat Defense Virtual コンソールから CLI コマンド **show version** および **show snapshot detail** を実行すると、作成した Threat Defense Virtual のイメージスナップショットのバージョンと詳細を確認できます。

スナップショット AMI を使用した Threat Defense Virtual インスタンスの展開

Before you begin

次のことを推奨します。

- AWS 環境の設定, on page 10の説明に従って、AWS VPC および EC2 のエレメントを設定します。
- AMI が Threat Defense Virtual インスタンスで使用できることを確認します。

ステップ 1 https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。

ステップ 2 **[EC2ダッシュボード（EC2 Dashboard）] > [インスタンス（Instances）]**の順にクリックします。イメージのスナップショットを作成するために展開した Threat Defense Virtual インスタンスが [インスタンス（Instances）] ページに表示されます。

Note イメージのスナップショットを作成するには、操作ステータス（[インスタンス状態（Instance Status）]）が [停止（Stopped）] の Threat Defense Virtual インスタンスを常に選択する必要があります。

ステップ 3 [インスタンス（Instances）]ページで、対応する[インスタンス状態（Instance Status）]が[停止（Stopped）]と示されている Threat Defense Virtual インスタンスを特定して選択します。

ステップ 4 [アクション（Actions）] ドロップダウンメニューから、[イメージとテンプレート（Image and templates）]をポイントし、[イメージの作成（Create Image）] をクリックします。

ステップ 5 [イメージの作成（Create Image）] ページで、イメージのスナップショットの名前と説明を入力します。

ステップ 6 [再起動なし（No reboot）]セクションの下にある[有効化（Enable）]チェックボックスをオンにします。

ステップ 7 [Create Image] をクリックします。Threat Defense Virtual のイメージスナップショット AMI が作成されます。

ステップ 8 **[イメージ（Images）] > [AMI（AMIs）]**の順にクリックします。このページでは、新しく作成したイメージのスナップショット AMI を表示できます。

ステップ 9 イメージスナップショット AMI を選択します。

ステップ 10 [起動（Launch）] をクリックして、イメージスナップショット AMI を使用して新しい Threat Defense Virtual インスタンスを展開します。

ステップ 11 Threat Defense Virtual インスタンスの展開を続行します。Threat Defense Virtual の導入, on page 16または AWS での Threat Defense Virtual Auto Scale ソリューションについてを参照してください。

Amazon GuardDuty サービスと Threat Defense Virtual の統合

Amazon GuardDuty は AWS 環境において、VPC ログ、CloudTrail 管理イベントログ、CloudTrail S3 データイベントログ、DNS ログといったさまざまなソースからのデータを処理して、不正の可能性がある悪意のあるアクティビティを特定する監視サービスです。

概要

シスコでは、管理センターとデバイスマネージャを介して Amazon GuardDuty サービスと Secure Firewall Threat Defense Virtual を統合するソリューションを提供しています。

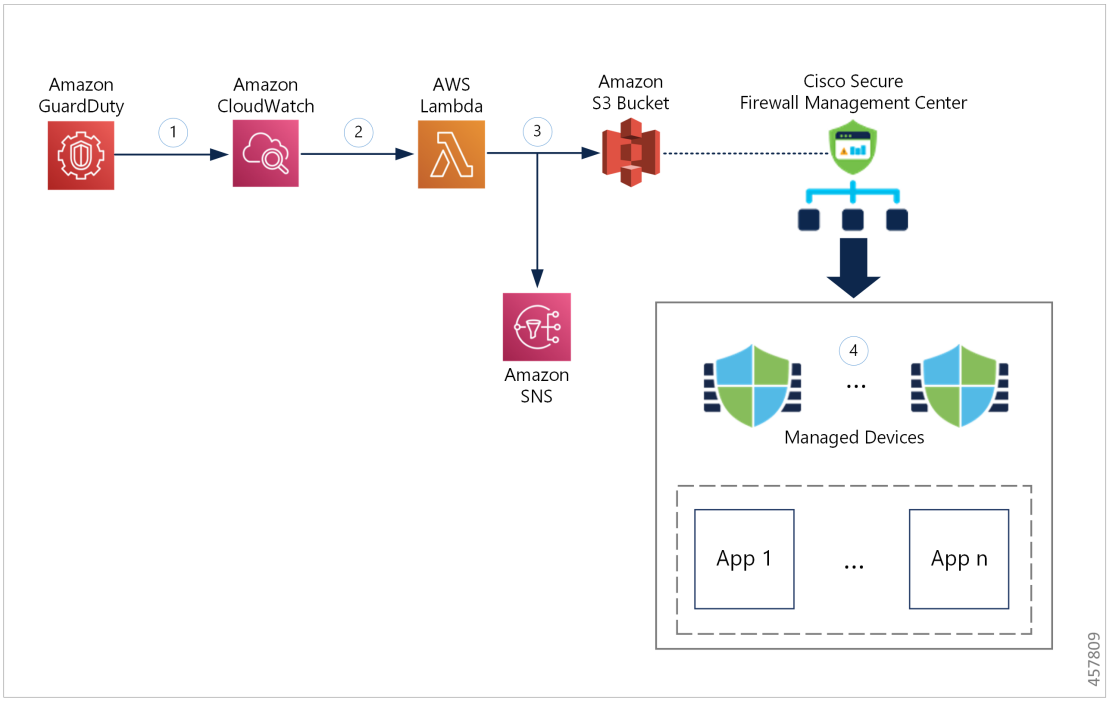
このソリューションでは、Amazon GuardDuty から受け取った脅威分析データや検出結果（脅威、攻撃などを生成する悪意のある IP）を使用して、その情報（悪意のある IP）をマネージャ（Secure Firewall Management Center Virtual および Secure Firewall デバイスマネージャ）経由で Secure Firewall Threat Defense Virtual にフィードし、これらのソース（悪意のある IP）が発生源となる将来の脅威から基盤となるネットワークやアプリケーションを保護します。

エンドツーエンドの手順

次の統合ソリューションとワークフローの図は、Amazon GuardDuty の Secure Firewall Threat Defense Virtual との統合を理解するのに役立ちます。

セキュリティ インテリジェンス ネットワーク フィードを使用した Secure Firewall Management Center Virtual との統合

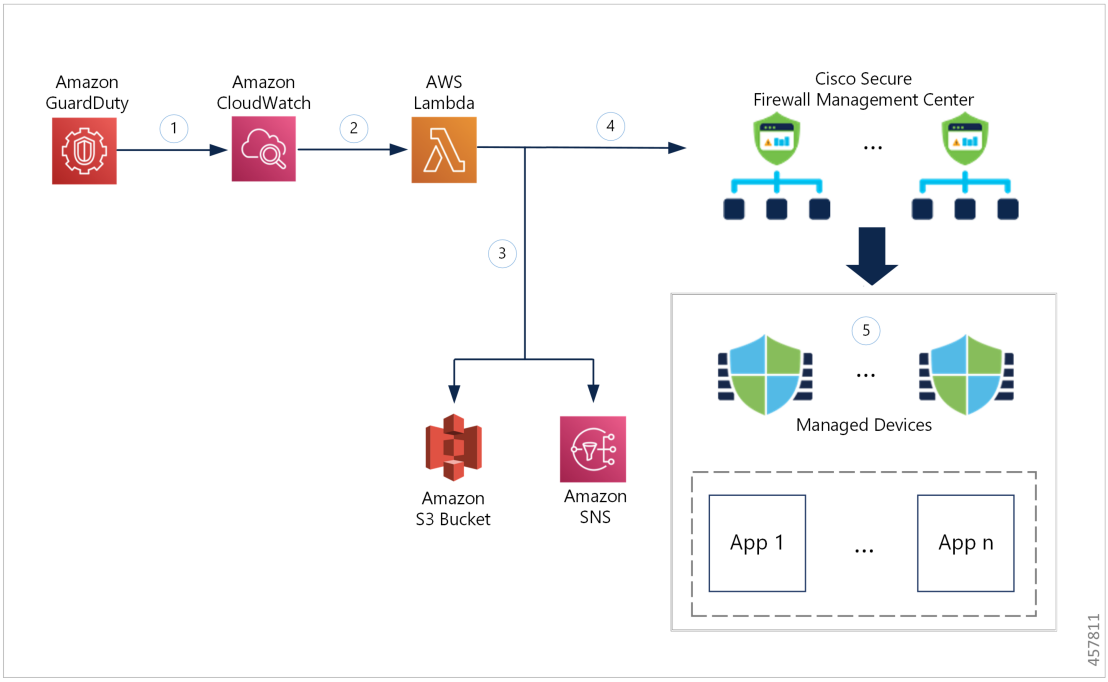
次のワークフロー図は、セキュリティ インテリジェンス ネットワーク フィード URL を使用した Secure Firewall Management Center Virtual と Amazon GuardDuty の統合ソリューションを示しています。



1	GuardDuty サービスは、悪意のあるアクティビティを検出すると、脅威の検出結果を CloudWatch に送信します。
2	CloudWatch イベントにより、AWS Lambda 関数がアクティブ化されます。
3	Lambda 関数は、S3 バケットのレポートファイル内に記載された悪意のあるホストを更新し、SNS 経由で通知を送信します。
4	Secure Firewall Management Center のアクセス コントロール ポリシーは、設定されたアクションに基づいてトラフィックを処理するように対象デバイスに指示します。たとえば、GuardDuty によって報告された悪意のあるホストからのトラフィックをブロックします。 このアクセスポリシーでは、セキュリティインテリジェンス ネットワーク フィードが、Lambda 関数によって提供された悪意のある IP アドレスレポートファイルの S3 オブジェクト URL と共に使用されます。

ネットワーク オブジェクト グループを使用した Secure Firewall Management Center Virtual との統合

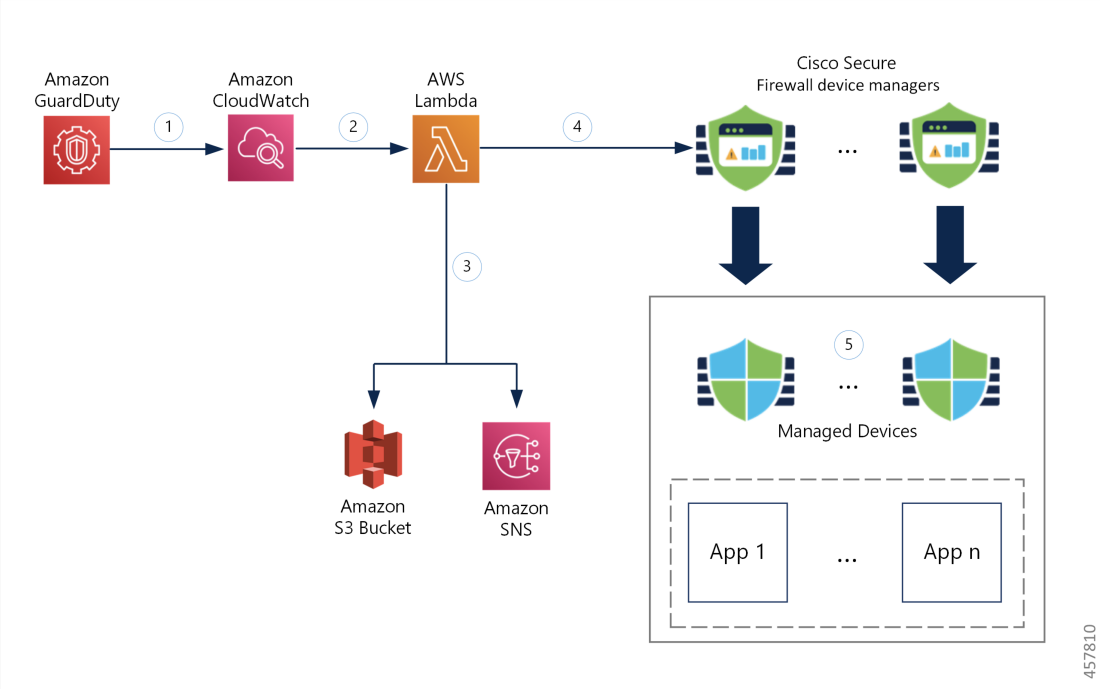
次のワークフロー図は、ネットワーク オブジェクト グループを使用した Secure Firewall Management Center Virtual と Amazon GuardDuty の統合ソリューションを示しています。



1	GuardDuty サービスは、悪意のあるアクティビティを検出すると、脅威の検出結果を CloudWatch に送信します。
2	CloudWatch イベントにより、AWS Lambda 関数がアクティブ化されます。
3	Lambda 関数は、S3 バケットのレポートファイル内に記載された悪意のあるホストを更新し、SNS 経由で通知を送信します。
4	Lambda 関数は、悪意のあるホスト IP アドレスを追加して Secure Firewall Management Center Virtual のネットワーク オブジェクト グループを設定または更新します。
5	Secure Firewall Management Center のアクセス コントロール ポリシーは、設定されたアクションに基づいてトラフィックを処理するように対象デバイスに指示します。たとえば、GuardDuty によって報告された悪意のあるホストからのトラフィックをブロックします。 このアクセス コントロール ポリシーは、Lambda 関数によって検出された悪意のある IP アドレスが追加されたネットワーク オブジェクト グループを使用します。

ネットワーク オブジェクト グループを使用した Secure Firewall Device Manager との統合

次のワークフロー図は、ネットワーク オブジェクト グループを使用した Secure Firewall Device Manager と Amazon GuardDuty の統合ソリューションを示しています。



1	GuardDuty サービスは、悪意のあるアクティビティを検出すると、脅威の検出結果を CloudWatch に送信します。
2	CloudWatch イベントにより、AWS Lambda 関数がアクティブ化されます。
3	Lambda 関数は、S3 バケットのレポートファイル内に記載された悪意のあるホストを更新し、SNS 経由で通知を送信します。
4	Lambda 関数は、悪意のあるホスト IP アドレスを追加して Secure Firewall Device Manager のネットワーク オブジェクト グループを設定または更新します。
5	Secure Firewall Device Manager のアクセス コントロール ポリシーは、設定されたアクションに基づいてトラフィックを処理するように管理対象デバイスに指示します。たとえば、GuardDuty によって報告された悪意のあるホストからのトラフィックをブロックします。 このアクセス コントロール ポリシーは、Lambda 関数によって検出された悪意のある IP アドレスが追加されたネットワーク オブジェクト グループを使用します。

この統合の主要コンポーネント

コンポーネント	説明
Amazon GuardDuty	特定のリージョン（EC2、S3、IAM など）のさまざまな AWS リソースについて、脅威検出結果の生成を行う Amazon サービス。

Amazon Simple Storage Service（S3）	ソリューションに関連するさまざまなアーティファクトを保存するために使用される Amazon サービスは以下のとおりです。 • Lambda 関数の zip ファイル • Lambda レイヤの zip ファイル • Cisco Secure Firewall Management Center Secure Firewall と Device Manager 構成の入力ファイル（.ini） • Lambda 関数によって報告された悪意のある IP アドレスのリストが保存された出力レポートファイル（.txt）
Amazon CloudWatch	Amazon サービスは次の目的で使用されます。 • GuardDuty サービスで報告された検出結果についてモニタリングし、Lambda 関数をトリガーして検出結果を処理します。 • CloudWatch ロググループで Lambda 関数に関連するアクティビティをロギングします。
Amazon Simple Notification Service（SNS）	電子メール通知をプッシュするために使用される Amazon サービスです。この電子メール通知には、次の内容が含まれます。 • Lambda 関数によって正常に処理された GuardDuty 検出結果の詳細。 • Lambda 関数によって Cisco Secure Firewall Manager で実行された更新の詳細。 • Lambda 関数によって発生した重大なエラー。
AWS Lambda 関数	AWS サーバーレス コンピューティング サービスはイベントに応じてコードを実行し、基盤となるコンピューティングリソースを自動的に管理します。CloudWatch イベントルールが GuardDuty の検出結果に基づいて Lambda 関数をトリガーします。Lambda 関数はこの連携で以下を実行します。 • GuardDuty の検出結果を処理して、重大度、接続方向、悪意のある IP アドレスの存在など、必要なすべての基準が満たされていることを確認します。 •（設定に応じて）悪意のある IP アドレスを追加して、Cisco Secure Firewall Manager のネットワーク オブジェクト グループを更新します。 • S3 バケットのレポートファイルで悪意のある IP アドレスを更新します。 • Cisco Secure Firewall の管理者に対して、さまざまなマネージャの更新やエラーについて通知します。

CloudFormation テンプレート	AWS での連携に必要なさまざまなリソースを展開するために使用されます。 CloudFormation テンプレートには、次のリソースが含まれています。 • **AWS::SNS::Topic**：電子メール通知をプッシュするための SNS トピック。 • **AWS::Lambda::Function, AWS::Lambda::LayerVersion**：Lambda 関数とレイヤファイル。 • **AWS::Events::Rule**：GuardDuty の検出結果イベントに基づいて Lambda 関数をトリガーする CloudWatch イベントルール。 • **AWS::Lambda::Permission**：Lambda 関数をトリガーする CloudWatch イベントルールのアクセス許可。 • **AWS::IAM::Role、AWS::IAM::Policy**：各種 AWS リソースの Lambda 関数へのさまざまなアクセス許可を付与する IAM ロールとポリシーリソース。 このテンプレートは、展開をカスタマイズするためのユーザー入力を取り込みます。

サポートされるソフトウェア プラットフォーム

- GuardDuty 統合ソリューションは、Secure Firewall Management Center Virtual または Secure Firewall Device Manager によって管理される Secure Firewall Threat Defense Virtual に適用できます。
- Lambda 関数は、管理センターのネットワーク オブジェクト グループと、任意の仮想プラットフォームに展開されたデバイスマネージャを更新できます。Lambda 関数がパブリック IP アドレスを介してこれらのマネージャに接続できることを確認してください。

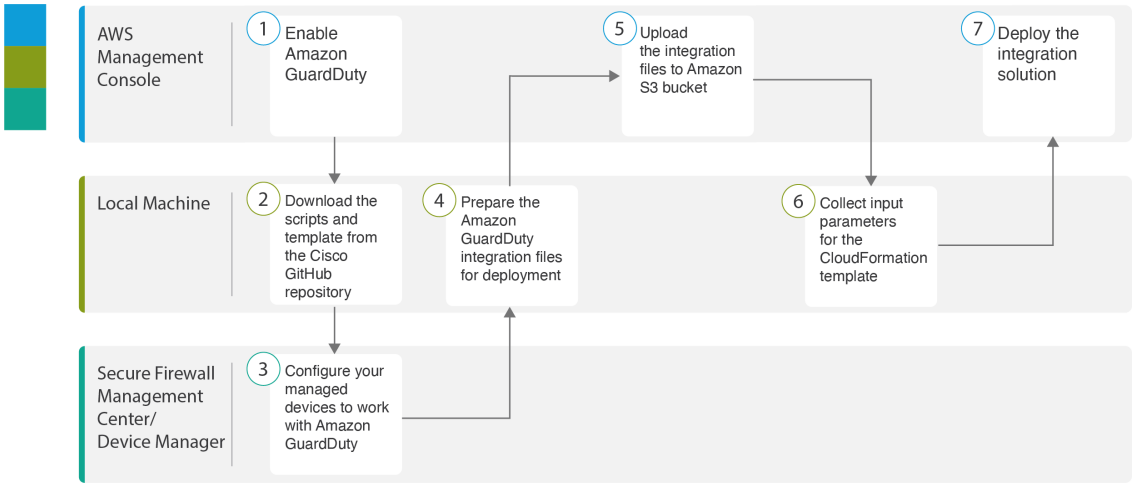
注意事項と制約事項

- Lambda 関数は、悪意のある IP アドレスを追加した Cisco Secure Firewall マネージャのネットワーク オブジェクト グループの更新のみを実行します。したがって、これらの更新または変更を管理対象デバイスに展開する必要があります。
- この統合で使用される AWS のサービスはリージョン固有です。したがって、異なるリージョンの GuardDuty 検出結果を使用する場合は、リージョン固有のインスタンスを展開する必要があります。
- Lambda 関数は、REST API を介して Cisco Secure Firewall マネージャを更新します。したがって、他の方法やマネージャ（Cisco Defense Orchestrator など）を使用することはできません。

- パスワードベースのログインのみを使用できます。他の認証方式はサポートされていません。
- 入力ファイルで暗号化されたパスワードを使用している場合は、次の点に注意してください。
  - 対称 KMS キーを使用した暗号化のみがサポートされます。
  - すべてのパスワードは、Lambda 関数にアクセス可能な単一の KMS キーを使用して暗号化する必要があります。

Amazon GuardDuty と Secure Firewall Threat Defense の統合

次のタスクを実行して、Amazon GuardDuty と Secure Firewall Threat Defense を統合します。



	ワークスペース	手順
1	AWS 管理コンソール	AWS での Amazon GuardDuty サービスの有効化 （29 ページ）
2	Local Machine	Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションリポジトリのダウンロード （29 ページ）
3	Secure Firewall Management CenterまたはSecure Firewall Device Manager	Amazon GuardDuty と連携するための管理対象デバイスの設定 （30 ページ）
4	Local Machine	展開に向けた Amazon GuardDuty リソースファイルの準備 （33 ページ）
5	AWS 管理コンソール	Amazon Simple Storage Service へのファイルのアップロード （37 ページ）

	ワークスペース	手順
6	Local Machine	CloudFormation テンプレートの入力パラメータの収集 （37 ページ）
7	AWS 管理コンソール	スタックの展開 （40 ページ）

AWS での Amazon GuardDuty サービスの有効化

ここでは、AWS で Amazon GuardDuty サービスを有効にする方法について説明します。

始める前に

すべての AWS リソースが同じリージョンにあることを確認します。

ステップ 1 https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。

ステップ 2 [サービス（Services）] > [GuardDuty] を選択します。

ステップ 3 [GuardDuty] ページで [利用を開始する（Get Started）] をクリックします。

ステップ 4 [GuardDutyの有効化（Enable GuardDuty）] をクリックして、Amazon GuardDuty サービスを有効にします。

GuardDuty の有効化の詳細については、AWS ドキュメントの『Getting started with GuardDuty』[英語] を参照してください。

次のタスク

Cisco GitHub リポジトリから Amazon GuardDuty ソリューションファイル（テンプレートとスクリプト）をダウンロードします。Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションリポジトリのダウンロード （29 ページ） を参照してください。

Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションリポジトリのダウンロード

Amazon GuardDuty ソリューションに必要なファイルをダウンロードします。Secure Firewall Threat Defense Virtual の該当するバージョン用の導入スクリプトとテンプレートは、次の Cisco GitHub リポジトリから入手できます。

https://github.com/CiscoDevNet/cisco-ftdv

以下は、Cisco GitHub リポジトリリソースのリストです。

ファイル	説明
READ.MD	ReadMe ファイル

ファイル	説明
configuration/	Secure Firewall Threat Defense Virtual マネージャの構成ファイルテンプレート。
images/	Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションの図が格納されています。
lambda/	Lambda 関数の Python ファイル。
templates/	導入用の CloudFormation テンプレート

Amazon GuardDuty と連携するための管理対象デバイスの設定

Lambda 関数は Amazon GuardDuty の検出結果を処理し、CloudWatch イベントをトリガーした悪意のある IP アドレスを特定します。Secure Firewall Threat Defense Virtual は 次のいずれかの方法で Secure Firewall Management Center Virtual および Secure Firewall Device Manager を介してこの脅威データを受信します。

- **ネットワーク オブジェクト グループの更新**：Lambda 関数は、悪意のある IP アドレスを追加してマネージャのネットワーク オブジェクト グループを更新します。次に、このネットワーク オブジェクト グループを使用してトラフィックを処理するアクセス コントロール ポリシーを設定できます。この方法は Secure Firewall Management Center Virtual と Secure Firewall Device Manager が対象です。
- **セキュリティ インテリジェンス ネットワーク フィード**：Lambda 関数は、悪意のある IP アドレスを追加して Amazon S3 バケット内のレポートファイルを作成または更新します。レポートファイルの URL を使用してセキュリティ インテリジェンス フィードを設定し、このフィードを使用してトラフィックを処理するアクセス コントロール ポリシーを設定できます。この方法は Secure Firewall Management Center Virtual のみが対象です。

レポートファイルの URL を使用したセキュリティ インテリジェンス ネットワーク フィードの設定

ここでは、Secure Firewall Management Center Virtual でセキュリティ インテリジェンス ネットワーク フィードを設定する方法について説明します。

始める前に

- Secure Firewall Management Center Virtual で脅威ライセンスが有効になっていることを確認します。「脅威ライセンス」を参照してください。
- Amazon S3 バケットで使用可能なレポートファイルの URL を作成して書き留めておきます。
- Secure Firewall Management Center Virtual から Amazon S3 バケット内のレポートファイルにアクセスできることを確認します。

ステップ 1 Secure Firewall Management Center Virtual にログインします。

ステップ 2 Amazon S3 バケットのレポートファイル URL を使用して、セキュリティ インテリジェンス ネットワーク フィードを作成します。セキュリティ インテリジェンス ネットワーク フィードを手動で作成する方法については、「カスタム セキュリティ インテリジェンス フィード」を参照してください。

ステップ 3 トラフィックを処理するセキュリティ インテリジェンス ネットワーク フィード URL を使用して、アクセス コントロール ポリシーやアクセス制御ルールを作成または更新します。「手動 URL フィルタリング オプション」および「アクセス コントロール ルールの作成と編集」を参照してください。

（注） 展開の前または後に、セキュリティ インテリジェンス ネットワーク フィードを作成し、アクセス コントロール ポリシーの URL を更新できます。Amazon S3 バケットに出力レポートファイルを作成している場合は、展開前にセキュリティ インテリジェンス ネットワーク フィードを作成できます。展開後にセキュリティ インテリジェンス ネットワーク フィードを作成している場合は、Amazon GuardDuty から最初の検出結果の電子メール通知を受信するまで待ち、その電子メール通知で指定された URL を使用してセキュリティ インテリジェンス ネットワーク フィードを設定します。

ステップ 4 Secure Firewall Management Center Virtual に設定の変更を展開します。「設定変更の展開」を参照してください。

次のタスク

展開に向けて Amazon GuardDuty ソースファイルを準備します。展開に向けた Amazon GuardDuty リソースファイルの準備 （33 ページ） を参照してください。

ネットワーク オブジェクト グループの作成

Secure Firewall Management Center Virtual および Secure Firewall デバイスマネージャ で Lambda 関数のネットワーク オブジェクト グループを設定または作成して、Amazon GuardDuty によって検出された悪意のある IP アドレスを更新する必要があります。

Lambda 関数でネットワーク オブジェクト グループを設定しない場合、デフォルト名 **aws-gd-suspicious-hosts** のネットワーク オブジェクト グループが Lambda 関数によって作成され、悪意のある IP アドレスが更新されます。

Secure Firewall Management Center Virtual でのネットワーク オブジェクト グループの作成

ここでは、Secure Firewall Management Center Virtual でネットワーク オブジェクト グループを作成する方法について説明します。

ステップ 1 Secure Firewall Management Center Virtual にログインします。

ステップ 2 ダミーの IP アドレスを使用してネットワーク オブジェクト グループを作成します。「ネットワークオブジェクト」を参照してください。

ステップ 3 ネットワーク オブジェクト グループを使用してトラフィックを処理するためのアクセス コントロール ポリシーやアクセス制御ルールを作成または更新します。「アクセス コントロール ポリシーの管理」および「アクセス コントロール ルールの作成および編集」を参照してください。

ヒント　Lambda 関数が悪意のある IP アドレスを追加してネットワーク オブジェクト グループを更新していることを確認した後に、アクセス コントロール ポリシーやアクセス制御ルールを作成または更新することもできます。

ステップ 4 設定変更を管理対象デバイスに展開します。「設定変更の展開」を参照してください。

次のタスク

展開に向けて Amazon GuardDuty ソースファイルを準備します。展開に向けた Amazon GuardDuty リソースファイルの準備 （33 ページ） を参照してください。

Secure Firewall Device Manager のネットワーク オブジェクト グループの作成

ここでは、Secure Firewall デバイスマネージャ でネットワーク オブジェクト グループを作成する方法について説明します。

ステップ 1 Secure Firewall Device Manager にログインします。

ステップ 2 ダミーの IP アドレスを使用してネットワーク オブジェクト グループを作成します。「ネットワークオブジェクトとグループの設定」を参照してください。

ステップ 3 ネットワーク オブジェクト グループを使用してトラフィックを処理するためのアクセス コントロール ポリシーやアクセス制御ルールを作成または更新します。「アクセス コントロール ポリシーの設定」および「アクセス制御ルールの設定」を参照してください。

ヒント　Lambda 関数が悪意のある IP アドレスを追加してネットワーク オブジェクト グループを更新していることを確認した後に、アクセス コントロール ポリシーやアクセス制御ルールを作成または更新することもできます。

ステップ 4 設定変更を管理対象デバイスに展開します。「変更の展開」を参照してください。

次のタスク

展開に向けて Amazon GuardDuty ソースファイルを準備します。展開に向けた Amazon GuardDuty リソースファイルの準備 （33 ページ） を参照してください。

Secure Firewall Management Center Virtual で Lambda 関数を利用するためのユーザーアカウントの作成

Lambda 関数には、管理センターとデバイスマネージャでネットワーク オブジェクト グループを更新するための管理者権限を持つユーザーアカウントが必要です。したがって、管理センターとデバイスマネージャで管理者権限を持つ排他的なユーザーアカウントを作成する必要が

あります。ユーザーアカウントの作成は、ネットワーク オブジェクト グループの更新メソッドを使用する場合にのみ必要です。

ユーザーアカウントの作成の詳細については、以下を参照してください。

- FDM および FTD ユーザ アクセスの管理
- FMC のユーザーアカウント

（任意）パスワードの暗号化

必要に応じて、入力構成ファイルに暗号化されたパスワードを指定できます。プレーンテキスト形式でパスワードを指定することもできます。

Lambda関数にアクセスできる単一のKMSキーを使用して、すべてのパスワードを暗号化します。**aws kms encrypt --key-id** <*KMS-ARN*> **--plaintext** <*password*> コマンドを使用して暗号化されたパスワードを生成します。このコマンドを実行するには、AWS CLI をインストールして設定する必要があります。

（注） パスワードが対称 KMS キーを使用して暗号化されていることを確認します。

AWS CLI については、AWS のコマンド ライン インタフェース [英語] を参照してください。マスターキーと暗号化の詳細については、パスワードの暗号化と KMS に関する AWS ドキュメントのキーの作成 [英語] と AWS CLI コマンドリファレンス [英語] を参照してください。

例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext <password>
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

CiphertextBlob キーの値をパスワードとして使用する必要があります。

展開に向けた Amazon GuardDuty リソースファイルの準備

Amazon GuardDuty ソリューションの展開リソースファイルは、Cisco GitHub リポジトリで入手できます。

AWS に Amazon GuardDuty ソリューションを展開する前に、次のファイルを準備する必要があります。

- Secure Firewall Threat Defense Virtual マネージャの構成入力ファイル
- Lambda 関数の zip ファイル

- Lambda レイヤの zip ファイル

構成入力ファイルの準備

構成テンプレートでは、Amazon GuardDuty ソリューションと連携する管理センターまたはデバイスマネージャの詳細を定義する必要があります。ネットワーク オブジェクト グループの更新メソッドで管理センターやデバイスマネージャと Amazon GuardDuty の統合を計画している場合にのみ、構成ファイルを更新することを推奨します。

始める前に

- 構成ファイルにユーザーアカウントの詳細を指定する前に、デバイスマネージャのユーザーアカウントを認証および検証します。
- 構成ファイルで複数の管理センターやデバイスマネージャを設定している場合は、各管理センターやデバイスマネージャのパラメータが構成ファイルに1つだけ入力され、重複するエントリがないことを確認します。
- 管理センターとデバイスマネージャの IP アドレスと名前を書き留めておく必要があります。
- 管理センターとデバイスマネージャでこれらのネットワーク オブジェクト グループにアクセスして更新するには、Lambda 関数の管理者権限を持つユーザーアカウントを作成しておく必要があります。

ステップ 1 Amazon GuardDuty リソースファイルをダウンロードしたローカルマシンにログインします。

ステップ 2 **ngfwv-template > configuration** フォルダを参照します。

ステップ 3 テキストエディタツールで `ngfwv-manager-config-input.ini` ファイルを開きます。

このファイルには、Amazon GuardDuty ソリューションの統合と展開を計画している管理センターまたはデバイスマネージャの詳細を入力する必要があります。

ステップ 4 各パラメータに対応する管理センターまたはデバイスマネージャに関する以下の詳細を入力します。

パラメータ	説明
[ngfwv-1]	セクション名：管理センターまたはデバイスマネージャの一意の識別子。
public-ip	管理センターまたはデバイスマネージャの IP アドレス。
device-type	管理センターまたはデバイスマネージャを介して Amazon GuardDuty ソリューションを展開する管理対象デバイスのタイプ。使用できる値は FMC または FDM です。

パラメータ	説明
ユーザー名	管理センターまたはデバイスマネージャにログインするためのユーザー名。
パスワード	管理センターまたはデバイスマネージャにログインするためのパスワード。パスワードには、プレーンテキスト形式または KMS を使用して暗号化された文字列を使用できます。
object-group-name	Lambda 関数が悪意のあるホスト IP を追加して更新するネットワーク オブジェクト グループの名前。複数のネットワーク オブジェクト グループ名を入力する場合は、カンマ区切り値になっていることを確認してください。

ステップ 5 `ngfwv-manager-config-input.ini` ファイルを保存して閉じます。

次のタスク

Lambda 関数のアーカイブファイルを作成します。Lambda 関数のアーカイブファイルの準備（35 ページ） を参照してください。

Lambda 関数のアーカイブファイルの準備

ここでは、Linux 環境で Lambda 関数ファイルをアーカイブする方法について説明します。

（注） アーカイブプロセスは、ファイルのアーカイブを実行するローカルマシンのオペレーティングシステムによって異なる場合があります。

ステップ 1 Amazon GuardDuty リソースをダウンロードしたローカルマシンで CLI コンソールを開きます。

ステップ 2 `/lambda` フォルダに移動し、ファイルをアーカイブします。

以下は、Linux ホストからのサンプルトランスクリプトです。

```
$ cd lambda
$ zip ngfwv-gd-lambda.zip *.py
adding: aws.py (deflated 71%) adding: fdm.py (deflated 79%)
adding: fmcv.py (deflated 79%)
adding: main.py (deflated 73%)
adding: utils.py (deflated 65%)
$
```

zip ファイル `ngfwv-gd-lambda.zip` が作成されます。

ステップ 3 終了して CLI コンソールを閉じます。

次のタスク

zip ファイル `ngfwv-gd-lambda.zip` を使用して、Lambda レイヤの zip ファイルを作成します。Lambda レイヤファイルの準備 （36 ページ）を参照してください

Lambda レイヤファイルの準備

ここでは、Linux 環境で Lambda レイヤファイルをアーカイブする方法について説明します。

（注） アーカイブプロセスは、ファイルのアーカイブを実行するローカルマシンのオペレーティングシステムによって異なる場合があります。

ステップ 1 Amazon GuardDuty リソースをダウンロードしたローカルマシンで CLI コンソールを開きます。

ステップ 2 CLI コンソールで次のアクションを実行します。

以下は、Python 3.9 がインストールされている Ubuntu 22.04 などの Linux ホストでのサンプルトランスクリプトです。

```
$ mkdir -p layer
$ virtualenv -p /usr/bin/python3.9 ./layer/
$ source ./layer/bin/activate
$ pip3.9 install cffi==1.15.0
$ pip3.9 install cryptography==37.0.2
$ pip3.9 install paramiko==2.7.1
$ pip3.9 install requests==2.23.0
$ mkdir -p ./python/.libs_cffi_backend/
$ cp -r ./layer/lib/python3.9/site-packages/* ./python/
$ zip -r ngfwv-gd-lambda-layer.zip ./python
```

zip ファイル `ngfwv-gd-lambda-layer.zip` が作成されます。

Lambda レイヤを作成するには、Python 3.9 とその依存関係をインストールする必要があることに注意してください。

以下は、Ubuntu 22.04 などの Linux ホストに Python 3.9 をインストールするためのサンプルトランスクリプトです。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

ステップ 3 終了して CLI コンソールを閉じます。

次のタスク

Amazon S3 バケットでは、Secure Firewall Threat Defense Virtual の構成ファイル、Lambda 関数の zip ファイル、および Lambda レイヤの zip ファイルをアップロードする必要があります。Amazon Simple Storage Service へのファイルのアップロード （37 ページ）を参照してください

Amazon Simple Storage Service へのファイルのアップロード

すべての Amazon GuardDuty ソリューション アーティファクトを準備したら、AWS ポータルの Amazon Simple Storage Service（S3）バケットフォルダにファイルをアップロードする必要があります。

ステップ 1 https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。

ステップ 2 Amazon S3 コンソールを開きます。

ステップ 3 Amazon GuardDuty アーティファクトをアップロードするための Amazon S3 バケットを作成します。Amazon S3 の作成 [英語] を参照してください。

ステップ 4 次の Amazon GuardDuty アーティファクトを Amazon S3 バケットにアップロードします。

- Secure Firewall Threat Defense Virtual構成ファイル：`ngfwv-config-input.ini`

  （注） 管理センターでセキュリティ インテリジェンスのネットワーク フィード メソッドを使用して Amazon GuardDuty ソリューションを展開する場合、このファイルをアップロードする必要はありません。

- Lambda レイヤ zip ファイル：`ngfwv-gd-lambda-layer.zip`
- Lambda 関数 zip ファイル：`ngfwv-gd-lambda.zip`

次のタスク

Amazon GuardDuty リソースの展開に使用する CloudFormation テンプレートを準備します。CloudFormation テンプレートの入力パラメータの収集 （37 ページ） を参照してください。

CloudFormation テンプレートの入力パラメータの収集

シスコでは、AWS の Amazon GuardDuty ソリューションに必要なリソースを展開する際に使用する CloudFormation テンプレートを提供しています。展開する前に、次のテンプレートパラメータの値を収集します。

Template Parameters

パラメータ	説明	例
展開名*	このパラメータに入力する名前は、Cloud Formation テンプレートによって作成されるすべてのリソースのプレフィックスとして使用されます。	**cisco-ngfwv-gd**
GD 検出結果の最小の重大度レベル*	Amazon GuardDuty の検出結果で処理の対象となる最小重大度レベルは、**1.0** から **8.9** の範囲にする必要があります。報告された検出結果の重大度が最小範囲よりも低い場合は無視されます。 重大度の分類は次のとおりです。 • 低：1.0 ～ 3.9 中：4.0 ～ 6.9 高：7.0 ～ 8.9	**4.0%**
管理者の電子メール ID*	管理センターまたはデバイスマネージャ の Lambda 関数によって実行された更新に関する通知を受信する Secure Firewall Threat Defense Virtual マネージャ の管理者の電子メールアドレス。	**abc@xyz.com**
S3 バケット名*	Amazon GuardDuty アーティファクトファイル （Lambda 関数の zip ファイル、Lambda レイヤの zip ファイル、および Secure Firewall Threat Defense Virtual 設定マネージャファイル）が格納された Amazon S3 バケットの名前。	例：**ngfwv-gd-bucket**
S3 バケットフォルダ/パスプレフィックス	構成ファイルが保存されている Amazon S3 バケットのパスまたはフォルダ名。フォルダがない場合は、このフィールドを空白のままにします。	例：「」または「**cisco/ngfwv-gd/**」
Lambda レイヤの zip ファイル名*	Lambda レイヤの zip ファイル名。	例：`ngfwv-gd-lambda-layer.zip`

パラメータ	説明	例
Lambda 関数の zip ファイル名*	Lambda 関数の zip ファイル名。	例：`ngfwv-gd-lambda.zip`
Cisco Secure Firewall Management Center Secure Firewall と Device Manager マネージャの構成ファイル名	Cisco Firewall Threat Defense Virtual のマネージャ設定の詳細が保存された ***.ini** ファイル（パブリック IP、ユーザー名、パスワード、デバイスタイプ、ネットワーク オブジェクト グループ名など）。 （注） このファイルは、Amazon GuardDuty との統合でネットワーク オブジェクト グループの更新メソッドを使用している場合にのみ必要です。 セキュリティ インテリジェンス フィード メソッドを使用している場合は、この入力をスキップできます。	例：`ngfwv-config-input.ini`
パスワードの暗号化に使用される KMS キーの ARN	既存の KMS（パスワードの暗号化に使用される AWS KMS キー）の ARN。Secure Firewall Threat Defense Virtual の構成入力ファイルでプレーンテキスト パスワードが指定されている場合は、このパラメータを空のままにしておくことができます。指定する場合、Secure Firewall Threat Defense Virtual の構成入力ファイルに記載されているすべてのパスワードを暗号化する必要があります。パスワードの暗号化には、指定された ARN のみを使用する必要があります。暗号化パスワードの生成：aws kms encrypt --key-id <KMS ARN> --plaintext <password>	例：**arn:aws:kms:<region>:<awsaccountid>:key/<keyid>**
デバッグログの有効化/無効化*	CloudWatch で Lambda 関数のデバッグログを有効または無効にします。	例：**enable** または **disable**

*：必須フィールド

次のタスク

CloudFormationテンプレートを使用してスタックを展開します。スタックの展開 （40ページ）を参照してください

スタックの展開

Amazon GuardDuty ソリューションを導入するためのすべての前提条件プロセスを完了した後に、AWS CloudFormation スタックを作成します。対象ディレクトリのテンプレートファイル（`templates/cisco-ngfwv-gd-integration.yaml`）を使用し、「CloudFormation テンプレートの入力パラメータの収集」で収集したパラメータを指定します。

ステップ 1 AWS コンソールにログインします。

ステップ 2 [サービス（Services）] > [CloudFormation] > [スタック（Stacks）] > [スタックの作成（Create stack）]（新しいリソースを使用）> [テンプレートの準備（Prepare template）]（テンプレートはフォルダ内にあります）> [テンプレートの指定（Specify template）] > [テンプレートソース（Template source）]（ターゲットディレクトリ `templates/cisco-ngfwv-gd-integration.yaml` からテンプレートファイルをアップロード）> [スタックの作成（Create Stack）] の順に操作を行います。

AWS でスタックを展開する方法の詳細については、AWS ドキュメント [英語] を参照してください。

次のタスク

展開を検証します。展開の検証 （41 ページ） を参照してください。

また、Amazon GuardDuty によって報告された脅威検出の更新に関する電子メール通知を受信するように登録します。電子メール通知の登録 （40 ページ） を参照してください。

電子メール通知の登録

CloudFormation テンプレートでは、GuardDutyの検出結果の更新に関する通知を受信するように、電子メール ID が設定されています。これは Lambda 関数によって実行されます。AWS に CloudFormation テンプレートを展開すると、Amazon Simple Notification Service（SNS）サービスを介してこの電子メール ID に電子メール通知が送信され、通知の更新を登録するように要求されます。

ステップ 1 電子メール通知を開きます。

ステップ 2 電子メール通知で利用可能な**サブスクリプション**リンクをクリックします。

次のタスク

展開を検証します。展開の検証 （41 ページ） を参照してください。

展開の検証

この項で説明されているように、AWS には Amazon GuardDuty ソリューションを検証するオプションがあります。CloudFormation の展開が完了したら、以下に示す展開の検証手順を実行できます。

始める前に

展開を検証するためのコマンドを実行するには、AWS コマンド ライン インターフェイス（CLI）がインストールおよび設定されていることを確認します。AWS CLI のドキュメントについては、AWS のコマンド ライン インターフェイス [英語] を参照してください。

ステップ 1 AWS 管理コンソールにログインします。

ステップ 2 [サービス（Services）] > [GuardDuty] > [設定（Settings）] > [GuardDutyのが概要（About GuardDuty）] > [ディテクタID（Detector ID）] に移動して、ディテクタ ID を書き留めます。

このディテクタ ID は、Amazon GuardDuty のサンプル検出結果を生成するために必要です。

ステップ 3 AWS CLI コンソールを開き、次のコマンドを実行して Amazon GuardDuty のサンプル検出結果を生成します。

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

ステップ 4 Amazon GuardDuty コンソールの結果リストでサンプルの検出結果を確認します。

サンプル検出結果には、プレフィックス **[sample]** が含まれています。接続方向、リモート IP アドレスなどの属性を参照して、サンプル検出結果の詳細を確認できます。

ステップ 5 Lambda 関数が実行されるのを待ちます。

Lambda 関数がトリガーされたら、以下を確認します。

- 受信した Amazon GuardDuty の検出結果と、Lambda 関数によって実行された Secure Firewall Threat Defense Virtual マネージャ の更新に関する詳細が記載された電子メール通知。
- レポートファイルが Amazon S3 バケットに生成されているかどうかを確認します。レポートファイルには、サンプルの Amazon GuardDuty の検出結果によって報告された悪意のある IP アドレスが含まれています。レポートファイル名は、`<deployment-name>-report.txt` の形式になっています。
- ネットワーク オブジェクト グループの更新メソッドの場合：設定されたマネージャ（Secure Firewall Management Center Virtual または Secure Firewall デバイスマネージャ）で、サンプルの検出結果から更新された悪意のある IP アドレスを追加してネットワーク オブジェクト グループが更新されていることを確認します。

- セキュリティ インテリジェンス フィード メソッドの場合：レポートファイルの URL が管理センターの設定で既に更新されているかどうかを確認します。レポートファイル URL の最終更新タイムスタンプは、管理センターの次のパスで表示できます。
  - [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence ）] > [ネットワークリストとフィード（Network Lists and Feeds）] > 設定したフィードを選択
  - または、フィードを手動で更新してから、[最終更新（Last Updated）] のタイムスタンプを確認することもできます。次のパスでフィードを選択して更新できます。

    [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence ）] > [ネットワークリストとフィード（Network Lists and Feeds）] > [フィードの更新（Update Feeds）]

ステップ 6 [AWSコンソール（AWS Console）] > [サービス（Services）] > [CloudWatch] > [ログ（Logs）] > [ロググループ（Log groups）] に移動し、ロググループを選択して、CloudWatch コンソールで Lambda ログを確認します。CloudWatch のロググループ名は、 `<deployment-name>-lambda` の形式になっています。

ステップ 7 展開を検証した後、次のようにサンプル検出結果によって生成されたデータをクリーンアップすることを推奨します。

a) AWS コンソールから [サービス（Services）] > [GuardDuty] > [結果（Findings）] > [結果を選択（Select the finding）] > [アクション（Actions）] > [アーカイブ（Archive）] に移動して、サンプルの検出結果データを表示します。

b) ネットワーク オブジェクト グループに追加された悪意のある IP アドレスを削除して、キャッシュされたデータを Secure Firewall Management Center Virtual から消去します。

c) Amazon S3 バケットのレポートファイルをクリーンアップします。サンプルの検出結果で報告された悪意のある IP アドレスを削除することで、ファイルを更新できます。

既存のソリューション展開構成の更新

展開後に S3 バケットや S3 バケットフォルダとパスプレフィックス値を更新しないことを推奨します。ただし、展開したソリューションの構成を更新する必要がある場合は、AWS コンソールの [CloudFormation] ページで [スタックの更新（Update Stack）] オプションを使用します。

以下のパラメータを更新できます。

パラメータ	説明
Secure Firewall Threat Defense Virtual マネージャの構成ファイル名	Amazon S3 バケットの構成ファイルを追加または更新します。以前のファイルと同じ名前でファイルを更新できます。構成ファイル名が変更された場合は、AWS コンソールの [ス

パラメータ	説明
	タックの更新（Update stack）]オプションを使用して、このパラメータを更新できます。
GD 検出結果の最小の重大度レベル*	AWS コンソールの [スタックの更新（Update stack）]オプションを使用して、パラメータ値を更新します。
管理者の電子メール ID*	AWS コンソールの [スタックの更新（Update stack）] オプションを使用して、電子メール ID のパラメータ値を更新します。SNS サービスコンソールを介して電子メールのサブスクリプションを追加または更新することもできます。
S3 バケット名*	Amazon S3 バケット内の zip ファイルを新しい名前で更新してから、AWS コンソールの [スタックの更新（Update Stack）] オプションを使用してパラメータを更新します。
Lambda レイヤの zip ファイル名*	Amazon S3 バケット内の Lambda レイヤ zip ファイル名を新しい名前で更新してから、AWS コンソールの [スタックの更新（Update stack）] オプションを使用して、このパラメータ値を更新します。
Lambda 関数の zip ファイル名*	Amazon S3 バケット内の Lambda 関数 zip ファイルを新しい名前で更新してから、AWS コンソールの [スタックの更新（Update stack）] オプションを使用して、このパラメータ値を更新します。
パスワードの暗号化に使用される KMS キーの ARN	AWS コンソールの [スタックの更新（Update stack）]オプションを使用して、パラメータ値を更新します。
デバッグログの有効化/無効化*	AWS コンソールの [スタックの更新（Update stack）]オプションを使用して、パラメータ値を更新します。

ステップ 1 AWS 管理コンソールに進みます。

ステップ 2 必要に応じて、新しいバケットとフォルダを作成します。

ステップ 3 以下に示すアーティファクトが古いバケットから新しいバケットにコピーされていることを確認します。

- Secure Firewall Threat Defense Virtual構成ファイル：`ngfwv-config-input.ini`

- Lambda レイヤ zip ファイル：`ngfwv-gd-lambda-layer.zip`
- Lambda 関数 zip ファイル：`ngfwv-gd-lambda.zip`
- Output レポートファイル：`<deployment-name>-report.txt`

ステップ 4 パラメータ値を更新するには、**Services > CloudFormation > Stacks > > Update (Update Stack) > Prepare template > Use current template > Next >** <*update parameters*>**> Update Stack** に移動します。

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。