Security Cloud Control でのデバイスのオンボーディング

ライブデバイスとモデルデバイスの両方を Security Cloud Control に導入準備できます。モデルデバイスはアップロードされた構成ファイルであり、Security Cloud Control を使用して表示および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が Security Cloud Control をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

この章は、次のセクションで構成されています。

AWS VPC のオンボーディング

AWS VPC を Security Cloud Control にオンボーディングするには、以下の手順に従います。

始める前に

（注） Security Cloud Control は、ピアリングされた AWS VPC をサポートしていません。ピア VPC で定義されたセキュリティグループを参照する、ピアリングされた VPC をオンボーディングしようとすると、オンボーディングプロセスは失敗します。

Amazon Web Service（AWS）仮想プライベートクラウド（VPC）を Security Cloud Control にオンボーディングする前に、以下の前提条件を確認してください。

- AWS VPC をオンボーディングするには、VPC のアクセスキーとシークレットアクセスキーが必要です。両方のログイン情報は、[アイデンティティ管理とアクセス管理（IAM）（Identity and Access Management (IAM)）] コンソールを使用して生成されます。セキュリ

ティログイン情報の詳細については、セキュリティログイン情報の理解と取得に関する資料を参照してください。

- Security Cloud Control が AWS VPC と通信できるように IAM 権限を設定します。IAM ユーザーの権限の変更の詳細については、『Changing Permissions for an IAM User』を参照してください。必要な権限については、以下の例を参照してください。

```
"cloudformation:CreateStack",
"cloudformation:CreateStackInstances",
"cloudformation:DescribeStackInstance",
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
"cloudformation:DescribeStacks",
"ec2:AllocateAddress",
"ec2:AllocateHosts",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateInternetGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:DescribeAddresses",
"ec2:DescribeAddressesAttribute",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeInstanceStatus",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcs",
"ec2:DescribeVpnGateways",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySecurityGroupRules",
"ec2:ModifySubnetAttribute",
```

```
"ec2:RunInstances",
"sts:GetCallerIdentity"
```

手順

ステップ 1 **セキュリティデバイス**を選択します。

ステップ 2  をクリックして、デバイスの導入準備を開始します。

ステップ 3 [AWS VPC] タイルをクリックします。

ステップ 4 [アカウント（Account）] ページで、次の詳細を入力します。

a) AWS アカウントに接続するためのアクセスキー ID とシークレットアクセスキーを入力します。生成された名前のリストは、ログイン情報を提供した AWS VPC から取得されます。

b) [接続（Connect）] をクリックします。

ステップ 5 [VPC] ページで、次の詳細を入力します。

a) ドロップダウンメニューからリージョンを選択します。VPC が配置されているリージョンを選択します。

b) [選択（Select）] をクリックします。

c) ドロップダウンメニューを使用して、正しい AWS VPC を選択します。生成された名前のリストは、ログイン情報を提供した AWS VPC から取得されます。

（注）
AWS VPC ID の名前は一意であり、2 つ以上のインスタンスが同じ ID を持つことはできません。

d) [選択（Select）] をクリックします。

ステップ 6 [名前（Name）] ページで、次の詳細を入力します。

a) Security Cloud Control UI で表示する名前を入力します。

b) [続行（Continue）] をクリックします。

ステップ 7 （オプション）[ラベル（Labels）] ページでデバイスのラベルを入力して、[続行（Continue）] をクリックします。

（注）
AWS VPC のラベルを作成する場合、ラベルはデバイスに自動的に同期されません。AWS コンソールで、ラベルをタグとして手動で再作成する必要があります。AWS VPC でのラベルとタグの詳細については、AWS VPC のラベルとタグ を参照してください。

オンボーディングが成功すると、[セキュリティデバイス（Security Devices）] ページで、[設定ステータス（Configuration Status）] が [同期済み（Synced）] に変わり、[接続（Connectivity）] が [オンライン（Online）] に変わります。

関連情報：

- AWS VPC 接続ログイン情報の更新

- AWS VPC ポリシー
- AWS とその他の管理対象デバイス間でオブジェクトを共有する

Security Cloud Control Firewall Management でサポートされるデバイス、ソフトウェア、ハードウェア

Security Cloud Control Firewall Management は、複数のセキュリティ プラットフォームにわたってセキュリティポリシーとデバイス設定を管理できるクラウドベースの管理ソリューションです。

このセクションでは、Security Cloud Control Firewall Management でファイアウォール、クラウド、SD-WAN、Cisco IOS、Cisco Umbrella、および管理センターの統合を管理するためにサポートされているデバイスタイプ、ソフトウェア、ハードウェア、および制約事項について説明します。

サポートの範囲

Security Cloud Control Firewall Management は、複数のセキュリティ プラットフォームにわたってセキュリティポリシーとデバイス設定を管理するためのクラウドベースソリューションです。資料によると、次の管理エリアのサポートが特定されています。

- Cisco Secure Firewall ASA（オンプレミスと仮想）
- Cisco Secure Firewall Threat Defense（FTD）（オンプレミスと仮想）
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center（オンプレミス）
- Cisco Meraki MX
- Cisco IOS デバイス
- Cisco Umbrella
- AWS セキュリティグループ

Security Cloud Control Firewall Management ドキュメントでは、Security Cloud Control Firewall Managementがサポートするデバイス、ソフトウェア、およびハードウェアが示されています。ドキュメントにソフトウェアのバージョンまたはデバイスタイプのサポートが明示的に記載されていない場合、Security Cloud Control Firewall Management はそれをサポートしません。

Cisco Secure Firewall ASA

Cisco 適応型セキュリティアプライアンス（ASA）は、ファイアウォール、VPN、および侵入防御機能を統合したセキュリティデバイスです。Security Cloud Control は、Cisco ASA デバイスの管理をサポートすることで、設定管理を合理化し、ネットワークインフラストラクチャ全体での適合規格の遵守をサポートします。

Cisco Secure Firewall Threat Defense

Cisco Cisco Secure Firewall Threat Defense は、従来のファイアウォール機能と高度な脅威防御機能を統合します。その機能には、侵入防御、アプリケーション制御、URL フィルタリング、高度なマルウェア防御などのセキュリティ機能が含まれます。

Cisco Secure Firewall Threat Defense デバイスは、Cisco ASA ハードウェアアプライアンス、シスコのファイアウォール ハードウェア アプライアンス、および仮想環境にデプロイできます。Cisco Firewall Management Center、Firewall Device Manager などの管理インターフェイスを使用して、脅威防御デバイスを管理できます。

Firewall Threat Defense は、従来のファイアウォール機能と高度な脅威防御機能を統合します。侵入防御、アプリケーション制御、URL フィルタリング、高度なマルウェア防御などを含む包括的なセキュリティ機能を提供します。FTD は、ASA ハードウェアアプライアンス、Cisco ファイアウォール ハードウェア アプライアンス、および仮想環境に展開できます。Threat Defense デバイスの管理は、Cisco Firewall Management Center、Security Cloud Control Firewall Management、Firewall Device Manager などのさまざまな管理インターフェイスを介して実行できます。

ソフトウェアおよびハードウェア互換性の詳細については、Cisco Secure Firewall Threat Defense 互換性ガイドを参照してください。

Firewall Device Manager は、Threat Defense デバイス管理用に明示的に設計された Web ベースの管理インターフェイスです。Threat Defense デバイスを設定およびモニターするためのシンプルなアプローチを提供するため、小規模な展開や、直感的なインターフェイスを求める組織に最適です。

FDM は、ネットワーク設定、アクセス コントロール ポリシー、NAT ルール、VPN 設定、モニタリング、および基本的なトラブルシューティングに関する基本的な設定機能を提供します。通常、Web ブラウザを介してアクセスする FDM は、FTD デバイスで直接使用できるため、追加の管理サーバーやアプライアンスは必要ありません。

Cisco Catalyst SD-WAN Manager

Security Cloud Control によって、Catalyst SD-WAN およびブランチ WAN の環境を中央管理できるようになり、組織がネットワーク全体でセキュリティポリシーを効率的に設定、監視、および適用できるようになります。この統合により、Catalyst SD-WAN Manager での高度なトラブルシューティング、ルールの最適化、および変更管理も容易になります。

ソフトウェアとハードウェアの互換性の詳細については、「Cisco Catalyst SD-WAN Device Compatibility」を参照してください。

Cisco Secure Firewall Management Center

Security Cloud Control Firewall Management は、セキュアな統合を確立し、セキュリティデバイスを検出し、一元化されたポリシー管理を有効にすることで、オンプレミスの Firewall Management Center の管理を簡素化します。ファイアウォールルール、VPN 設定、侵入防御ポリシーなどのセキュリティポリシーを、FMC 下にあるすべてのデバイスにわたって効率的に管理および展開できます。

Cisco Meraki MX

Cisco Meraki MX アプライアンスは、分散型デプロイメント用のエンタープライズグレードセキュリティおよびSD-WAN次世代ファイアウォールアプライアンスです。Security Cloud Control Firewall Management は、Cisco Meraki MX デバイス上のレイヤ 3 ネットワークルールの管理をサポートします。

Cisco Meraki デバイスを Security Cloud Control Firewall Management にオンボーディングすると、Security Cloud Control Firewall Management は Cisco Meraki ダッシュボードと通信してそのデバイスを管理します。Security Cloud Control Firewall Management は設定要求を Cisco Meraki ダッシュボードに転送し、Cisco Meraki ダッシュボードは新しい設定をデバイスに適用します。

Cisco Meraki MX に関する Security Cloud Control Firewall Management のサポートには、ポリシーの一元管理、バックアップと復元、モニタリングとレポート、コンプライアンスチェック、自動化機能などがあります。

Cisco IOS デバイス

Cisco IOS ソフトウェアは、ルーティング、スイッチング、その他のネットワーキングプロトコルなどのネットワーク機能を管理します。Cisco IOS には、シスコのネットワークデバイスを設定および維持するための機能とコマンドが含まれています。

Cisco Umbrella

Security Cloud Control Firewall Management は、Cisco Umbrella と Cisco ASA の統合などの統合を介して Cisco Umbrella を管理します。この統合により、管理者はインターフェイスごとのポリシーを使用して、Cisco適応型セキュリティアプライアンス（ASA）デバイスを Cisco Umbrella 設定に含めることができます。

この統合により、Cisco ASA デバイスが DNS クエリを Cisco Umbrella にリダイレクトすることが可能になり、Cisco Umbrella の DNS セキュリティ、Web フィルタリング、および脅威インテリジェンス機能を活用することも可能になります。

AWS セキュリティグループ

Security Cloud Control Firewall Management は、Amazon Web Services（AWS）仮想プライベートクラウド（VPC）向けのシンプル化された管理インターフェイスを提供します。ソースを基盤とする機能には、AWS サイト間 VPN 接続のモニタリング、AWS デバイスへの変更の追跡、AWS サイト間 VPN トンネルの表示が含まれます。

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。

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。

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。