はじめに

Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのプラットフォームで、Cisco のファイアウォールおよびデバイス全体でセキュリティポリシー管理を統合し、簡素化します。ポリシーの一貫性が合理化され、直感的で高度なインターフェイスが提供され、複数のデバイスマネージャ間での設定の変更が調整されます。

Security Cloud Control Firewall Management の概要

Security Cloud Control Firewall Management （旧Cisco Defense OrchestratorまたはCDO）は、Cisco IOS や SSH などの Cisco ファイアウォールやその他のデバイス間でセキュリティポリシーを簡素化し、統合するのに役立つクラウドベースのセキュリティポリシーマネージャです。ファイアウォールとデバイスは、Security Cloud Control ダッシュボードの**[Products]** の下にリストされている **[Firewall]** から管理できます。

Security Cloud Control Firewall Management は、セキュリティポリシー内の不整合を特定し、修正するためのツールを提供することにより、セキュリティポリシーを最適化するのに役立ちます。オブジェクトとポリシーを共有できるだけでなく、設定テンプレートを作成することで、デバイス間でのポリシーの一貫性を維持できます。

Security Cloud Control Firewall Management は Cisco Adaptive Security Device Manager（ASDM）と共存するため、ASDM によって行われた設定の変更が追跡され、違いが調整されます。

さまざまなデバイスを一元的に管理できます。上級ユーザーは、従来の CLI インターフェイスに新しい機能拡張を追加して、管理の効率をさらに向上させます。

Security Cloud Control Firewall Management では、ガイド付きの「Day 0」エクスペリエンスも提供され、Threat Defense デバイスをオンプレミスまたは Cloud-Delivered Firewall Management Center にすばやくオンボーディングできます。また、有効化および設定するのに役立つその他の主要な機能も紹介されています。

デバイスのオンボーディング要件

デバイスを導入準備する前に、次の前提条件を満たしてください。

- インストールウィザードを完了します。
- デバイスのライセンスを取得します。

これらの前提条件を満たした後、Security Cloud Control Firewall Management オンボーディングウィザードを使用してデバイスを導入準備します。

「デバイスとサービスのオンボーディング」を参照してください。

次の制約事項に注意してください。

- 組織に関連付けられている Security Cloud Control Firewall Management にデバイスを導入準備した後は、それらのデバイスを別の組織に移行できません。
- デバイスを新しい組織に移動するには、新しい組織にデバイスを再度オンボーディングする必要があります。

Security Cloud Control のサポート対象デバイスの完全なリストについては、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 を参照してください。

シスコ オンライン プライバシー ポリシー

Cisco Systems, Inc. およびその子会社（以下総称して「シスコ」といいます）は、皆様のプライバシーを保護し、シスコの Web サイト、ならびに製品およびサービス（以下「ソリューション」）を快適にお使いいただけるよう全力を尽くします。『シスコ オンライン プライバシー ポリシー』をよく読み、シスコがユーザーの個人情報を収集、使用、共有、保護する方法を明確に理解してください。

Security Cloud Control による SSH デバイスの管理

汎用 SSH デバイスには、汎用 SSH インターフェイスを使用して管理される、Cisco IOS を実行していないその他の SSH 対応デバイスが含まれます。SSH を使用してアクセス可能な Linux サーバー、Unix ベースのシステム、またはサードパーティのネットワークアプライアンスなどのデバイス。汎用 SSH とは、リモートでネットワークデバイスに安全にアクセスして管理するための標準的な方法としてセキュアシェル（SSH）プロトコルを使用することを指します。これらのデバイスには、デバイスの IP または FQDN、SSH ポート、およびログイン情報を指定することで、Security Cloud Control を介してオンボーディングおよび管理できる SSH を使用してアクセスできます。

これらのデバイスでサポートされている機能は次のとおりです。

- SSH デバイスのオンボーディング。SSH デバイスに保存されている、高レベルの権限を持つユーザーのユーザー名とパスワードを使用して、デバイスをオンボーディングできます。

- デバイスの構成ファイルを表示する。デバイス構成ファイルを表示できます。
- デバイスからのポリシーと設定の変更を確認します。ファイアウォールからの変更の読み取りSSHデバイスからコンフィギュレーション ファイルが読み取られると、Security Cloud Control のデータベースに保存されます。
- アウトオブバンド変更検出。デバイスで[競合検出（Conflict Detection）]を有効にすると、Security Cloud Control は 10 分ごとにデバイスの設定の変更をチェックします。変更がある場合、デバイスのステータスは[競合検出（Conflict Detected）]に変わり、競合を解決可能になります。
- Security Cloud Control コマンドライン インターフェイス ツールの使用。Security Cloud Control のコマンドライン インターフェイスを介して、すべての SSH デバイスコマンドをデバイスに発行できます。
- 個々の CLI コマンドおよびコマンドのグループを、編集および再利用可能な「マクロ」に変換できます。Security Cloud Control が提供するシステム定義マクロを使用して、頻繁に実行するタスク用に独自のマクロを作成できます。
- SSH フィンガープリントの変更の検出と管理。デバイスのログイン情報またはプロパティが変更され、それによって SSH フィンガープリントが変更された場合、Security Cloud Control はその変更を検出し、新しいフィンガープリントを確認して許可する機会を提供します。
- 変更ログ。変更ログには、SSHデバイスに発行するすべてのコマンドがキャプチャされます。

Security Cloud Control Firewall Management ダッシュボード

Security Cloud Control Firewall Management ダッシュボードは、さまざまなカテゴリにわたって組織レベルの詳細をモニタリングおよび管理するための中央ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

ダッシュボードをカスタマイズする

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードウィジェットを選択または選択解除し、ドラッグアンドドロップして希望の順序に配置します。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。有効にすると、次のウィジェットが表示できます。

- **設定状態**：デバイス上の設定と、Security Cloud Control によって維持されているデバイス上の設定との不一致を示します。この比較は、存在する可能性のある不整合や競合を特定するのに役立ちます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理**： 変更ログを管理して、正確な運用管理を実現できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「ログの変更」を参照してください。

- **RA VPN セッション**：リモートアクセス VPN セッションをモニターするのに役立ちます。

  詳細については、「RA VPN セッション」を参照してください。

- **全体のインベントリ**：すべてのデバイスの正常性とステータスをモニターするのに役立ちます。ウィジェットには、**[Issues]**、**[Pending Actions]**、**[Other]**、**[Online]** に分類されたデバイス、およびハードウェアサポートの最終日に近づいているデバイス、またはすでにハードウェアサポートの最終日に達しているデバイスが表示されます。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN**： サイト間 VPN 接続を管理および評価するのに役立ちます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

  詳細については、「サイト間 VPN」を参照してください。

- **アカウントとアセット**：

  - マルチクラウドアカウントとリソースを効果的に追跡および管理できます。ここから Multicloud Defense Controller を起動できます。
  - **[+Add Account]** をクリックして、新しいアカウントを追加します。

  詳細については、「Multicloud Defense コントローラ」を参照してください。

- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。**許可されたトラフィック**（デフォルト）と**ブロックされた**トラフィックの間でフィルタ処理できます。

- **上位の侵入およびマルウェアイベント**： 上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。**許可されたイベント**（デフォルト）と**ブロックされた**イベントの間でフィルタ処理できます。

アナウンスメント

[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目のいずれかについて詳細が必要な場合は、関連ドキュメントへのリンクが提供されます。

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。