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。

Cisco Security Cloud Control の概要

Cisco Security Cloud Control は、単一の統合インターフェイスからセキュリティ製品を管理し、セキュリティの成果を達成できるようにするプラットフォームです。

プラットフォームにセキュリティ製品を統合すると、エクスペリエンスが合理化になります。Cisco セキュリティ製品のサブスクリプションを購入すると、購入したすべてのサブスクリプションに関する単一の要求コードが記載された電子メールが 1 件届きます。新しいセキュリティクラウドコントロール組織に要求コードを入力すると、すべての製品が同時に Cisco Security Cloud Control にプロビジョニングされます。

Cisco Security Cloud Control では、ユーザーとグループの管理はプラットフォームレベルで行われます。これらのユーザーとグループにロールが割り当てられ、Cisco Security Cloud Control および統合製品を管理する権限が定義されます。

製品とツール間の移動は直感に行うことができ、すべての統合製品に共通のプラットフォームメニューとツールバーが標準化されています。

Cisco Security Cloud Control は、プラットフォーム上のすべての統合製品に次のコアサービスを提供します：

- **プラットフォーム管理**：ロールベースのアクセス制御の管理、サブスクリプションの要求、製品インスタンスの標準化された地域展開などの一般的なサービスは、Security Cloud Control によって提供されます。Security Cloud Control では、これらの機能を一元化するこ

とで、プラットフォームから管理されるすべての Cisco Security 製品間でのプロビジョニングおよびアクセス管理における一貫したユーザーエクスペリエンスが保証されます。管理者は、Security Cloud Control のメインナビゲーションバーにある プラットフォーム管理メニューからこれらの共通サービスにアクセスします。

- **人工知能アシスタント**：Security Cloud Control の Cisco AI Assistant は、AI 中心のインサイト、自動化、およびコンテキストガイダンスを提供することにより、セキュリティ業務を合理化するように設計されています。管理者がセキュリティポリシーを管理し、問題をトラブルシュートし、Firewall、Duo、および Secure Access などの Cisco のセキュリティ製品全体で設定を最適化するのに役立ちます。Cisco Assistant は、自然言語処理とクロスプラットフォームインテリジェンスを活用することで、効率を向上させ、インシデント対応を迅速化し、セキュリティワークフローを簡素化します。
- **Global Search**：プラットフォーム内の製品全体の値を検索する機能です。
- **Shared Objects**：デバイスやポリシー間で共有できるオブジェクトを作成および管理します。
- **Unified documentation portal**：すべてのドキュメントにアクセスできる、ドキュメントの「ヘルプ」エクスペリエンス。

Security Cloud Control と統合される製品：

Security Cloud Control からは、次のすべてのセキュリティ製品を管理できます。

- AI Defense
- Security Cloud Control Firewall Management
- Multicloud Defense
- セキュアなアクセス
- Secure Workload

Security Cloud Control から起動できる製品

Security Cloud Control から、これらのセキュリティ製品を起動できます。起動後、これらの製品はスタンドアロン製品として動作するため、Security Cloud Control を介して管理することはできません。このような製品のライセンスは Security Cloud Control からのみ要求または非アクティブ化できます。

[Cisco Security Cloud Control] ツールバーで、9 ドットメニュー をクリックすると、次の製品が起動します：

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco Duo
- Cisco XDR

Security Cloud Control によってサポートされる製品およびソリューション

現在、Security Cloud Control と統合できる製品は次のとおりです。

AI Defense ： AI Defense はAIのユーザーとプロバイダーのリスクに対処します。Security Cloud Control のネットワーク可視性と適用ポイントを使用して、AI Defense では、分散クラウド環境全体で承認済みおよび未承認の AI ワークロード、アプリケーション、モデル、データ、およびユーザーアクセスを検出するための検出と適用の手順が追加されます。AI を搭載したサービスを開発および提供する組織の場合、AI Defense は提供前に AI モデルの脆弱性を検出します。プロンプトインジェクション、サービス妨害（DoS）、データ漏洩といった急速に進化する脅威から AI アプリケーションを保護します。 詳細については、「AI Defenseのドキュメント」を参照してください。

Security Cloud Control Firewall Management ： Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのセキュリティポリシーマネージャで、シスコのファイアウォールやその他のデバイス全体でポリシーを簡素化および統合します。 詳細については、『Cisco Security Cloud Control ドキュメント』の「ファイアウォール」を参照してください。

Multicloud Defense ： Multicloud Defense は、マルチクラウドセキュリティに対する簡素化および高度に自動化されたアプローチを提供します。このソリューションにより、組織は単一の SaaS 提供コントロールプレーンと、一元化または分散された PaaS 提供データプレーンアーキテクチャを使用して、マルチクラウド環境を管理および保護できます。 Multicloud Defense では、すべての主要なクラウドプロバイダーで継続的な可視性、統合された保護、およびダイナミックなポリシー更新が提供されるため、各クラウドプロバイダーごとにソリューションごとに個別のポイントソリューションを用意する必要がなくなります。詳細については、「Multicloud Defenseのドキュメント」を参照してください。

セキュアなアクセス ：Cisco セキュアなアクセス は、インターネットベースの脅威に対して複数のレベルの防御を提供するクラウドベースのプラットフォームです。組織のネットワークから接続する場合でも、ネットワークからローミングする場合でも、インターネット、SaaS アプリケーション、およびプライベートデジタルリソースに安全に接続できます。ポリシールールを使用して、リソース、ユーザー、デバイスのコレクションにセキュリティ管理を構成および適用します。 詳細については、「Secure Access Documentation」を参照してください。 セキュアなアクセス サブスクリプションには、追加料金なしで Security Cloud Control を介した Identity Intelligence 統合も含まれます。これには、スタンドアロン Identity Intelligence ダッシュボードへのアクセスは含まれません。詳細については、「Cisco Identity Intelligence と Cisco Secure Access の統合」を参照してください。

Secure Workload ：Cisco Secure Workload（旧称 Tetration）は、単一のコンソールからあらゆるワークロード、環境、または場所にゼロトラストのマイクロセグメンテーションをシームレスに提供します。包括的な可視性と強力な AI/ML 主導の自動化により、Secure Workload はラテラルムーブメントを防止し、攻撃対象領域を縮小し、ワークロードの動作の異常を特定し、

脅威を迅速に修復し、コンプライアンスを継続的に監視します。 詳細については、「Secure Workload Documentation」を参照してください。

Security Cloud Control Firewall Management の概要

Security Cloud Control Firewall Management （旧 Cisco Defense Orchestrator）は、分散環境でのセキュリティポリシーの管理を簡素化し、すべての管理対象ファイアウォールで一貫したポリシーを提供します。ファイアウォールとデバイスは、Security Cloud Control の **[Products]** の下にリストされている **[Firewall]** で管理されます。

不整合を特定し、解決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します。このプラットフォームでは、オブジェクトとポリシーの共有だけでなく、設定テンプレートの作成も可能になり、デバイス間でのポリシーの一貫性が保証されます。

Adaptive Security Device Manager（ASDM）などのローカルデバイスマネージャと共存すると、Security Cloud Control はそれ自体と他のマネージャの両方によって行われた設定の変更を追跡し、不一致を調整します。

直感的なユーザーインターフェイスを備えており、単一のプラットフォームからさまざまなデバイスを管理できます。高度なユーザーは、より効率的な管理のために拡張CLIインターフェイスを使用することもできます。

このプラットフォームは、ガイド付きの「Day 0」エクスペリエンスを提供し、オンプレミスまたは Cloud-Delivered Firewall Management Centerへの Threat Defense デバイスの迅速なオンボーディングを容易にします。潜在的な利点があり、それらのアクティブ化と設定を支援する主な機能に焦点を当てています。

Onboard Devices

デバイスをオンボードする前に、ウィザードのインストールとデバイスを完了し、デバイスにライセンスが付与されていることを確認します。次に、Security Cloud Control Firewall Management のオンボーディングウィザードを使用してデバイスをオンボーディングします。Security Cloud Control では、大規模な展開を簡単に管理できます。

「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。

（注） デバイスを Security Cloud Control Firewall Management テナントに導入準備すると、そのデバイスは、別の Security Cloud Control Firewall Management テナントに移行できません。デバイスを新しいテナントに移動させる場合は、古いテナントからデバイスを削除して、新しいテナントにオンボーディングし直す必要があります。

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、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 FDM-Managed デバイスの管理

重要 Secure Firewall Device Manager （FDM）のサポートと機能は、要求があった場合にのみ利用できます。テナントで Firewall Device Manager サポートがまだ有効になっていない場合は、FDM-managed デバイスを管理したり、デバイスに展開したりすることはできません。サポートチームにリクエストを送信して、このプラットフォームを有効にします。

Security Cloud Control（旧称 Cisco Defense Orchestrator）では、シンプルな管理インターフェイスと Secure Firewall Device Manager デバイスへのクラウドアクセスが提供されます。FDM-managed の管理者にとって、デバイスインターフェイスと Security Cloud Control インターフェイスの間には多くの類似点があります。私たちは、マネージャ間で可能な限り一貫性を保つという考えで Security Cloud Control を構築しました。

Security Cloud Control を使用して、物理または仮想 FDM-managed デバイスの次の側面を管理します。

- FDM 管理対象デバイスの導入準備
- デバイス管理
- デバイスのアップグレード
- ASA から FTD への移行
- インターフェイス管理
- ルーティング
- ハイ アベイラビリティ
- セキュリティ ポリシー
- ポリシーと構成の一貫性を促進する
- サイト間 VPN
- Remote Access VPN
- ネットワークのモニタリング

- シスコのセキュリティ分析とロギング

ソフトウェアおよびハードウェアのサポート

Security Cloud Control はバージョン 6.4 以降をサポートしており、さまざまなデバイスまたは仮想マシンにインストールできます。詳細については、「FDM-Managed サポートの詳細」を参照してください。

スマート ライセンスの管理

Cisco スマートライセンスを使用して、デバイスを Security Cloud Control にオンボーディング中、またはオンボーディングした後に FDM-managed デバイスにライセンスを付与できます。スマートライセンスはワークフローに組み込まれており、Security Cloud Control インターフェイスから簡単にアクセスできます。詳細については、「スマートライセンスの適用または更新」を参照してください。

（注） オンボードするデバイスがソフトウェアバージョン 6.4 または 6.5 を実行しており、すでにスマートライセンスが付与されている場合、デバイスは Cisco Smart Software Manager に登録されている可能性があります。**登録キーを使用してデバイスを Security Cloud Control にオンボードする前に、Cisco Smart Software Manager からデバイスの登録を解除する必要があります。**登録を解除すると、仮想アカウントでデバイスに関連付けられているライセンスとすべてのオプションライセンスが解放されます。

オンボードするデバイスがソフトウェアバージョン 6.6 以降を実行しており、すでに Cisco Cloud に登録されている場合は、**登録キーを使用してデバイスを Security Cloud Control にオンボードする前に、Cisco Cloud サービスからデバイスを登録解除する必要があります。**

Security Cloud Control ユーザーインターフェイス

Security Cloud Control GUI および CLI インターフェイス

Security Cloud Control は、グラフィック ユーザー インターフェイス（GUI）とコマンド ライン インターフェイス（CLI）の両方を提供する Web ベースの管理製品で、デバイスを 1 つずつまたは一括で管理できます。

CLI インターフェイスを使用すると、Security Cloud Control から直接 FDM-managed デバイスにコマンドを送信できます。CLI マクロを使用して、よく使用されるコマンドを保存して実行します。詳細については、Security Cloud Control コマンドライン インターフェイス ツールの使用を参照してください。

API サポート

Security Cloud Control は、デバイスの REST API を使用して FDM-managed デバイスで高度なアクションを実行できる API ツールのインターフェイスを提供します。さらに、このインターフェイスは次の機能を提供します。

- 実行済みの API コマンドの履歴を記録します。
- 再利用できるシステム定義の API マクロを提供します。
- 標準 API マクロを使用して、すでに実行したコマンドから、または別のユーザー定義マクロからユーザー定義 API マクロを作成できます。

API ツールの詳細については、API ツールを使用するを参照してください。

FDM-Managed デバイスの導入準備

FDM-managed デバイスをオンボードする前に、一般的なデバイス要件とオンボーディングの前提条件を確認してください。

登録トークンを使用して FDM-managed デバイスをオンボードするのがベストプラクティスです。詳細については、「登録キーを使用したソフトウェアバージョン 6.6 以降を実行する FDM 管理対象デバイスの導入準備」を参照してください。

次の追加の方法を使用して、FDM-managed デバイスを Security Cloud Control にオンボードすることもできます。

- ユーザー名、パスワード、IP アドレスを使用した FDM-Managed デバイスの導入準備
- デバイスのシリアル番号を使用した構成済み FDM 管理対象デバイスの導入準備
- FDM-Managedを使用した Zero-Touch Provisioning デバイスの導入準備ワークフローと前提条件

デバイス管理

Security Cloud Control を使用してソフトウェアをアップグレードし、ハイアベイラビリティを設定し、FDM-managed デバイスのデバイス設定とネットワークリソースの設定を行います。

- **システム設定**：FDM-managed デバイスのライセンスを取得してオンボーディングすると、FDM-managed デバイス設定を Security Cloud Control から完全に管理できるようになります。管理アクセスプロトコル、ログ設定、DHCP および DNS サーバーの相互作用、デバイスのホスト名、使用するタイムサーバー、および URL フィルタリング設定を構成できます。
- **FTD セキュリティデータベースの更新**：必要に応じてデバイスをチェックして更新する定期的なタスクを実行して、デバイスを最新の状態に保ち、最新のセキュリティデータベースの更新に対応します。
- **ハイアベイラビリティ**：FDM-Managed ハイアベイラビリティページで HA の設定と操作を管理します。

デバイスのアップグレード

次のいずれかの方法を使用して、FDM-managed デバイスへの即時アップグレードを実行するか、スケジュールを設定します。

- 単一 FDM-managed デバイスのアップグレード。
- 複数の FDM-managed デバイスのアップグレード。
- FDM-managed HA ペアのアップグレード。

インターフェイス管理

Security Cloud Control を使用して、FDM-managed デバイスのデータインターフェイスまたは管理/診断インターフェイスを設定および編集できます。

ルーティング

ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。ルーティングには、最適なルーティングパスの決定と、ネットワーク経由のパケットの転送という 2 つの基本的なアクティビティが含まれます。Security Cloud Control を使用して、ルーティングの次の側面を構成します。

- **スタティックルートおよびデフォルトルートの設定**。Security Cloud Control を使用すると、FDM-managed デバイスのデフォルトルートおよびその他のスタティックルートを定義できます。
- **ブリッジグループのサポート**。ブリッジグループは 1 つ以上のインターフェイスをグループ化する仮想インターフェイスです。インターフェイスをグループ化する主な理由は、スイッチド インターフェイスのグループを作成することにあります。Security Cloud Control を使用すると、デバイスのブリッジグループを設定および編集できます。
- **NAT（ネットワーク アドレス変換）**。NAT ルールは、内部（プライベート）ネットワークからインターネットへのトラフィックのルーティングに役立ちます。NAT ルールは、内部 IP アドレスをネットワークの外部から隠蔽することにより、セキュリティの役割も果たします。Security Cloud Control を使用して、デバイスの NAT ルールを作成および編集できます。詳細については、ネットワーク アドレス変換を参照してください。

セキュリティ ポリシー

セキュリティポリシーは、ネットワークトラフィックが目的の宛先に到達できるようにする、または到達できないようにすることを最終的な目標として、ネットワークトラフィックを検査します。Security Cloud Control を使用して、デバイスのセキュリティポリシーのすべてのコンポーネントを管理します。

- **ルールをコピーして貼り付けます**。ポリシー間でルールをコピーして貼り付けることで、ポリシー同士でルールを簡単に共有できます。詳細については、「FDM アクセスコントロールルールのコピー」を参照してください。
- **SSL 復号ポリシー**。HTTPS など一部のプロトコルは、セキュア ソケット レイヤ（SSL）またはその後継バージョンである Transport Layer Security（TLS）を使用して、セキュアな転送のためにトラフィックを暗号化します。システムでは暗号化された接続を検査できないため、アクセス判断のために上位層のトラフィック特性を考慮したアクセスルールを適用する場合は、SSL 復号ポリシーを適用して暗号化された接続を復号する必要がありま

す。詳細については、「FDM-Managedデバイスの SSL 復号ポリシー」を参照してください。

- **ID ポリシー**。ID ポリシーを使用して、接続からユーザーアイデンティティ情報を収集できます。その後で、ダッシュボードにユーザーアイデンティティに基づく使用状況を表示し、ユーザーまたはユーザー グループに基づくアクセス コントロールを設定できます。
- **セキュリティ インテリジェンス ポリシー**。セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。システムは、トラフィックをアクセス コントロール ポリシーで評価する前にドロップすることにより、使用されるシステムリソースの量を減らします。
- **アクセス コントロール ポリシー**。アクセス コントロール ポリシーでは、アクセスコントロールルールを基準にネットワークトラフィックを評価することで、ネットワークリソースへのアクセスを制御します。Secure Firewall Device Manager は、アクセスコントロールルールの基準を、アクセス コントロール ポリシーに表示される順番でネットワークトラフィックと比較します。アクセスコントロールルールのすべてのトラフィック条件が一致すると、Secure Firewall Device Manager はルールで定義されたアクションを実行します。Security Cloud Control を使用して、アクセス コントロール ポリシーのすべての側面を設定できます。
- TLS 1.3 セキュリティアイデンティティ検出。バージョン 6.7 以降に導入されているこの機能を使用すると、TLS 1.3 で暗号化されたトラフィックで URL フィルタリングとアプリケーション制御を実行できます。詳細については、「TLS Server Identity Discovery in Firepower Threat Defense」を参照してください。
- **侵入ポリシー**。Firepower システムには複数の侵入ポリシーが付属しています。これらのポリシーは、侵入ルールとプリプロセッサ ルールの状態を設定し、詳細設定を構成する Cisco Talos Security Intelligence and Research Group によって設計されています。侵入ポリシーはアクセスコントロールルールの一部の要素です。詳細については、「FDM アクセスコントロールルールの侵入ポリシーの設定」を参照してください。

（注） Snort 3 は、バージョン 6.7 以降を実行している FDM-managed デバイスで使用できます。Snort 2 と Snort 3 は自由に切り替えることができますが、互換性がない設定のリスクがあることに注意してください。Snort 3、サポートされているデバイスとソフトウェア、および制限の詳細については、「Snort 3.0 へのアップグレード」を参照してください。

- **脅威イベント**。脅威イベントは、Cisco Talos の侵入ポリシーの 1 つに一致した後にドロップされた、またはアラートを生成したトラフィックのレポートです。ほとんどの場合、IPS ルールを調整する必要はありません。必要な場合、一致するルールのアクションを Security Cloud Control で変更することで、イベントの処理方法を上書きするオプションがあります。Security Cloud Control は、バージョン 6.4 および 6.6.1 のすべてのバージョンで IPS ルー

ル調整をサポートしています。Security Cloud Control は、バージョン 6.5、6.6.1 以外の 6.6 バージョン、または 6.7 バージョンでの IPS ルール調整をサポートしていません。

- **NAT（ネットワーク アドレス変換）**。NAT ルールは、内部（プライベート）ネットワークからインターネットへのトラフィックのルーティングに役立ちます。NAT ルールは、内部 IP アドレスをネットワークの外部から隠蔽することにより、セキュリティの役割も果たします。Security Cloud Control を使用して、Firepower Threat Defense 用の NAT ルールを作成および編集できます。

ポリシーと構成の一貫性を促進する

オブジェクト管理（Object Management）

オブジェクトは、1つ以上のセキュリティポリシーで使用できる情報のコンテナです。オブジェクトを使用するとポリシーの一貫性を簡単に維持できます。これは、オブジェクトを変更すると、そのオブジェクトを使用する他のすべてのポリシーに影響を与えるためです。オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

Security Cloud Control を使用して、次のオブジェクトタイプを作成および管理します。

- Active Directory レルム
- AnyConnect クライアント プロファイル
- アプリケーション フィルタ
- 証明書
- DNS Group
- 位置情報（GeoLocation）
- ID ソース
- IKEv1 ポリシー
- IKEv1 IPSec プロポーザル
- IKEv2 ポリシー
- IKEv2 IPSec プロポーザル
- ネットワーク（Network）
- RA VPN グループポリシー
- セキュリティゾーン
- サービス
- セキュリティグループタグ
- Syslog サーバー

- URL

オブジェクトの問題を解決する

Security Cloud Control は、複数のデバイスで使用されるオブジェクトを「共有オブジェクト」と呼び、オブジェクトページでこのバッジ でそれらを識別します。共有オブジェクトは、ある「問題」を発生させて、複数のポリシーやデバイス間で完全には共有できなくなる場合があります。Security Cloud Control を使用すると、重複オブジェクトの問題の解決、未使用オブジェクトの問題の解決、および不整合オブジェクトの問題の解決が容易になり、デバイスとオブジェクトのリポジトリを管理できます。

テンプレート

Secure Firewall Device Manager テンプレートは、オンボードされた FDM-managed デバイスの設定の完全なコピーです。その後、そのテンプレートを変更し、それを使用して管理対象の他の FDM-managed デバイスを設定できます。Secure Firewall Device Manager テンプレートを使用すると、デバイス間でポリシーの一貫性が高まります。詳細については、「FDM テンプレート」を参照してください。

高可用性

Security Cloud Control を使用すると、FDM 管理対象デバイスの高可用性ペアを簡単に設定および管理できます。既存の HA ペアをオンボードするか、Security Cloud Control で HA ペアを作成できます。HA 構成により、アップグレード期間中や予期しないデバイス障害など、デバイスが使用できないシナリオでも安全なネットワークを維持することができます。フェールオーバーモードでは、スタンバイデバイスはすでにアクティブになるように構成されています。つまり、HA デバイスの 1 つが使用できなくなっても、もう一方のデバイスはトラフィックの処理を続行します。

Security Cloud Control で FDM-managed HA ペアをアップグレードできます。詳細については、「FDM-Managed ハイアベイラビリティペアのアップグレード」を参照してください。

バーチャル プライベート ネットワークの設定

サイト間 VPN

仮想プライベートネットワーク（VPN）は、非セキュアなネットワークでプライベートデータを相互に安全に送信する複数のリモートピアで構成され、ネットワーク間を接続するものです。Security Cloud Control は、トンネルを使用してデータパケットを通常の IP パケット内にカプセル化し、IP ベースのネットワークを経由して転送します。暗号化を使用してプライバシーを確保し、認証を使用してデータの整合性を確保します。詳細については、「サイト間 VPN」を参照してください。

仮想プライベートネットワークの詳細は、『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』を参照してください。

リモート アクセス VPN

リモートアクセス（RA）VPN を使用すると、サポートされているラップトップ、デスクトップ、およびモバイルデバイスを使用して、個人がネットワークへの安全な接続を確立できます。Security Cloud Control は FDM-managed デバイスで RA VPN を直感的に設定できるユーザーインターフェイスを提供します。AnyConnect はエンドポイントデバイスでサポートされている唯一のクライアントで、FDM-managed デバイスへの RA VPN 接続が可能です。

Security Cloud Control は、FDM-managed デバイスでの RA VPN 機能の次の側面をサポートします。

- プライバシー、認証、およびデータ整合性のための Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）
- SSL クライアントベースのリモートアクセス
- IPv4 および IPv6 のアドレッシング
- 複数の FDM-managed デバイス間での共有 RA VPN 設定

詳細については、「RA VPN」を参照してください。仮想プライベートネットワークの詳細は、『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』を参照してください。

ネットワークのモニタリング

Security Cloud Control は、セキュリティポリシーの影響をまとめたレポートと、そのセキュリティポリシーによってトリガーされる重要なイベントを表示する方法を提供します。Security Cloud Control は、デバイスへの変更をログに記録し、その変更にラベルを付ける方法も提供します。これにより、Security Cloud Control での作業をヘルプチケットなどの操作要求に関連付けできます。

[エグゼクティブサマリー（Executive Summary）] レポート

エグゼクティブ サマリー レポートには、暗号化されたトラフィック、傍受された脅威、検出された Web カテゴリなどの運用統計のコレクションが表示されます。レポートのデータは、ネットワークトラフィックが FDM-managed デバイスでアクセスルールまたはポリシーをトリガーしたときに生成されます。デバイスがレポートに反映されるイベントを生成できるように、マルウェア、ライセンスと、アクセスルールのファイルロギングを有効にすることをお勧めします。

レポートに記載される内容と、それを使用してネットワーク インフラストラクチャを改善する方法の詳細については、「FDM-Managedデバイスのエグゼクティブ サマリー レポート」を参照してください。レポートを作成および管理するには、「レポートの管理」を参照してください。

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging を使用すると、すべての FDM-managed デバイスからの接続、侵入、ファイル、マルウェア、セキュリティ インテリジェンスのイベントをキャプチャし、Security Cloud Control の 1 ヵ所で表示できます。

イベントは Cisco Cloud に保存され、Security Cloud Control の [イベントロギング（Event Logging）]ページから表示できます。イベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。それらの機能は、**Logging and Troubleshooting** パッケージで提供されます。

ログの変更

Security Cloud Control での変更ログの管理 は、Security Cloud Control で行われた設定変更を継続的にキャプチャします。

この単一のビューには、サポートされているすべてのデバイスとサービスにわたる変更が含まれます。変更ログの機能の一部を次に示します。

- デバイス構成に加えられた変更の対照比較
- すべての変更ログエントリの平易な英語のラベル。
- デバイスのオンボーディングと削除を記録します。
- Security Cloud Control の外部で発生するポリシー変更の競合の検出。
- インシデントの調査またはトラブルシューティング中に、誰が、何を、いつを回答。
- 完全な変更ログまたは一部のみを CSV ファイルとしてダウンロード可能。

変更要求管理

変更要求管理により、サードパーティのチケットシステムで開かれた変更要求とそのビジネス上の正当性を、変更ログのイベントに関連付けることができます。変更要求管理を使用して、Security Cloud Control で変更要求を作成し、作成した変更要求を一意の名前で識別し、変更の説明を入力して、変更要求を変更ログイベントに関連付けます。後で変更要求名を変更ログで検索できます。

ファイアウォール ダッシュボード

ファイアウォールダッシュボードは、さまざまなカテゴリ全体でテナントレベルの詳細をモニタリングおよび管理するための中心ハブです。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. ダッシュボードに表示するウィジェットを選択または選択解除します。
3. ウィジェットをドラッグアンドドロップして、希望に応じて配置できます。

ダッシュボードは、**[Top Insights & Alerts]**、**[Top Actions]**、および **[Top Information]** の 3 つの主要なセクションに分割されています。各セクションでは、最適なセキュリティおよび運用管理を維持するために役立つさまざまなカテゴリのインサイトが提供されます。

上位のインサイトとアラート

このセクションは、テナントに対して **AIOps インサイト**が有効になっている場合にのみ表示されます。エレメントフロー、RA VPN 予測、アクセス制御ポリシーの異常、CPU およびメモリの使用率が高い、Snort CPU およびメモリの使用率が原因で発生する高トラフィックに関連するインサイトを表示できます。

上位アクション

このセクションは、テナントに対して **AIOps インサイト**が有効になっている場合にのみ表示されます。有効にすると、次のウィジェットが表示できます。

- **ポリシーアナライザおよびオプティマイザ**：セキュリティポリシーを分析し、異常を検出し、ファイアウォールのパフォーマンスを向上させるための最適化推奨事項を提供します。

  詳細については、「ポリシーアナライザおよびオプティマイザ」を参照してください。

- **AIOps インサイト**：設定、正常性と操作、またはトラフィックとキャパシティごとに異常を分類する、すべてのアクティブなインサイトと傾向に関する詳細情報を提供します。

  詳細については、「AIOps インサイト」を参照してください。

- **機能導入**：使用パターンを最適化し、セキュリティ対策を強化するための機能導入率に関するインサイトを提供します。

  詳細については、「機能の導入状況の評価と改善」を参照してください。

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、「変更ログ」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、**問題**、**保留中のアクション**、**その他**、および**オンライン**に分類されたデバイスの総数が表示されます。

  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**：

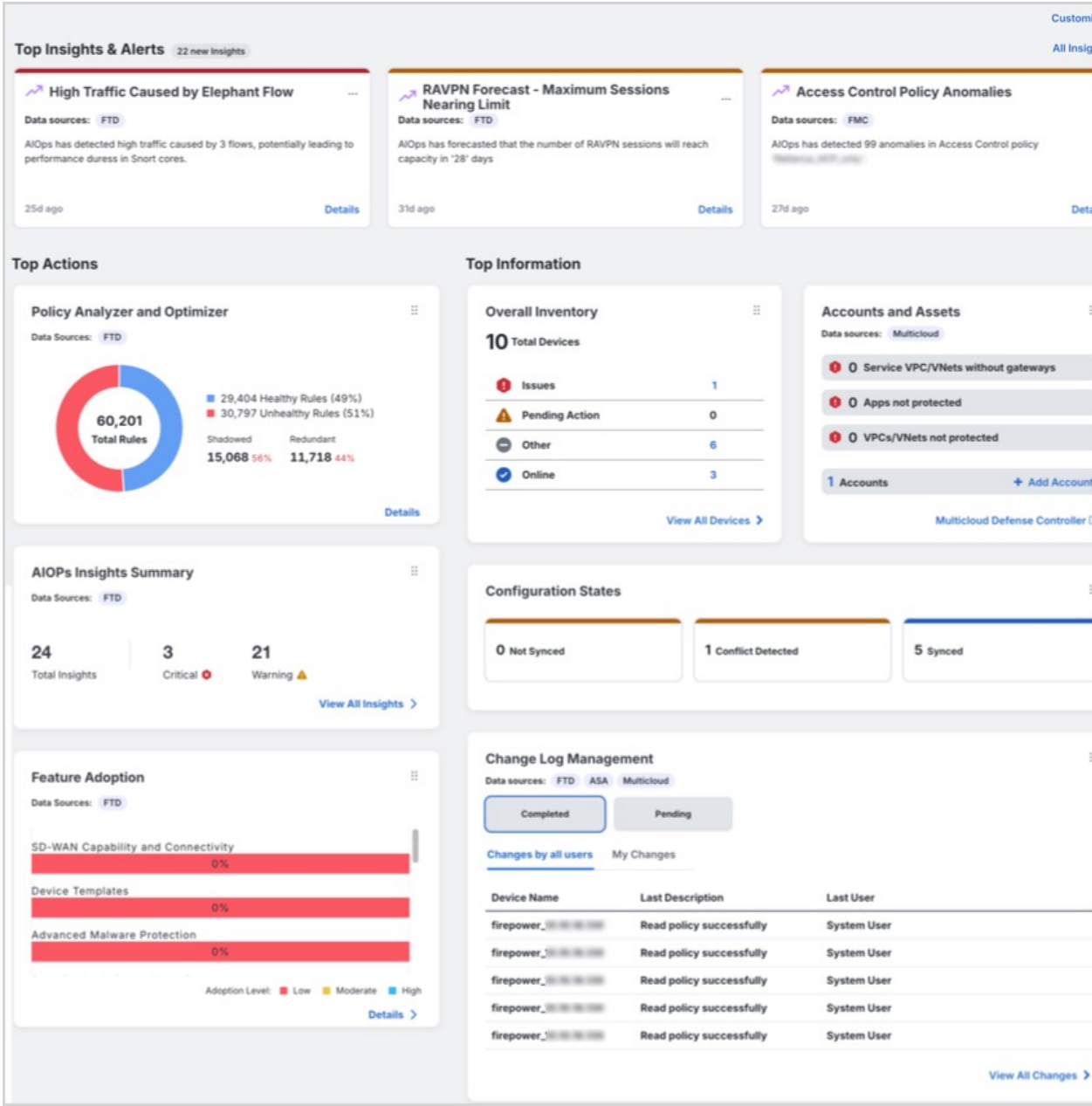
  - マルチクラウドのアカウントとリソースを効果的に追跡して管理するのに役立ちます。ここから Multicloud Defense Controller を起動できます。
  - **[+Add Account]** をクリックして、新しいアカウントを追加します。

  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。

- **トップ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。

図 *1 : AIOps* インサイトが有効になっているダッシュボード



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に関する詳細を知りたい場合は、関連する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。