Cisco Defense Orchestrator での FTD の管理

Cisco Defense Orchestrator での FTD の管理

CDO は、FTD デバイスへの簡素化された管理インターフェイスとクラウドアクセスを提供します。Firepower Device Manager（FDM）管理者は、FDM インターフェイスと CDO インターフェイスの間に多くの類似点があることに気付くでしょう。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 CDO を構築しました。

CDO を使用して、物理または仮想 FTD デバイスの次の側面を管理します。

- FTD のオンボーディング
- Device Management
- デバイスのアップグレード
- インターフェイス管理
- ルーティング
- 高可用性
- 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
- リモート アクセス VPN
- ネットワークのモニタリング
- Cisco Security Analytics and Logging

Cisco Defense Orchestrator での FTD の管理

FTD ソフトウェアと Firepower ハードウェアのサポート

CDO は Firepower バージョン 6.4 以降のバージョンをサポートしており、さまざまな Firepower ハードウェア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、「Firepower Threat Defense のサポートの詳細」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 CDO 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 FTD 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、CDO 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 FTD 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 CDO にオンボードする前に、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基本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 FTD 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 CDO 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。**

CDO ユーザーインターフェイス

CDO GUI および CLI インターフェイス

CDO 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、CDO から直接 FTD 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、「FTD コマンド ライン インターフェイスのドキュメント」および CDO コマンドライン インターフェイスの使用 を参照してください。

FTD API のサポート

CDO は、デバイスの REST API を使用して FTD 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。

Cisco Defense Orchestrator での FTD の管理

- 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。

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

FTD デバイスのオンボーディング

FTD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 FTD 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+ を実行する FTD のオンボード」を参照してください。

次の追加の方法を使用して、FTD を CDO 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 FTD のオンボーディング
- デバイスのシリアル番号を使用した設定済み FTD のオンボード
- 新しい FTD デバイスのロータッチプロビジョニング

Device Management

CDO 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、FTD 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**：FTD のライセンスを取得してオンボーディングすると、FTD システム設定を CDO 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**：FTD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、FTD 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 FTD デバイスのアップグレード。
- 複数の FTD デバイスのアップグレード。
- FTD HA ペアのアップグレード。

Cisco Defense Orchestrator での FTD の管理

インターフェイス管理

CDO を使用して、FTD 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。CDO 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**。CDO を使用すると、FTD 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。CDO を使用すると、Firepower Threat Defense 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。CDO 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。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。CDO を使用して、Firepower Threat Defense 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、「FTD 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、「Firepower Threat Defense 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。

Cisco Defense Orchestrator での FTD の管理

- **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 ポリシーは、アクセスコントロールルールに照らして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。FTD は、アクセスコントロールルールの条件を、アクセス コントロール ポリシーに表示される順序で、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、FTD はルールで定義されたアクションを実行します。CDO 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。6.7 以降でサポート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。詳細はについては、「FTD 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 FTD 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。必要に応じて、CDO の一致ルールアクションを変更して、イベントの処理方法をオーバーライドするオプションが用意されています。CDO は、FTD 6.4 および FTD 6.6.1 のすべてのバージョンで IPS ルールの調整をサポートします。CDO は、FTD 6.5 の任意のバージョン、6.6.1 以外の FTD 6.6 の任意のバージョン、または FTD 6.7 の任意のバージョンでの IPS ルールの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。CDO 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。

Cisco Defense Orchestrator での FTD の管理

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。

CDO 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

CDO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。共有オブジェクトが何らかの「問題」を引き起こし、複数のポリシーまたはデバイス間で完全に共有されなくなる場合があります。CDO 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

Cisco Defense Orchestrator での FTD の管理

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

Firepower Threat Defense（FTD）テンプレートは、オンボードされた FTD 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する他の FTD デバイスを設定できます。FTDテンプレートは、デバイス間のポリシーの一貫性を促進します。詳細については、「FTD テンプレート」を参照してください。

高可用性

CDO を使用すると、FTD 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、CDO 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。

CDO で HA FTD ペアをアップグレードできます。詳細については、「FTD 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

バーチャル プライベート ネットワーク（VPN）は、セキュアでないネットワーク経由で相互にプライベートデータを安全に送信し、それによりネットワーク同士を接続する複数のリモートピアで構成されています。CDO は、トンネルを使用してデータパケットを通常の IP パケット内でカプセル化し、IP ベースのネットワーク経由で転送しま。その際、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。CDO は、FTD デバイスで RA VPN をセットアップするための直感的な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、FTD への RA VPN 接続が可能です。

Cisco Defense Orchestrator（CDO）は、FTD デバイスでの RA VPN 機能の次の側面をサポートしています。

- 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）

Cisco Defense Orchestrator での FTD の管理

- 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 FTD 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

CDO は、セキュリティポリシーの影響を要約したレポートを発行し、セキュリティポリシーによってトリガーされた重要なイベントの表示方法を提供します。また CDO は、デバイスに加えた変更をログに記録し、それらの変更にラベルを付ける方法を提供します。これにより、CDO で行った操作をヘルプチケットやその他の操作要求に関連付けることができます。

[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 FTD 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、脅威、IPS 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、「FTD 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 Firepower Threat Defense（FTD）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、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、CDO 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。

Firewall Analytics and Monitoring パッケージを使用すると、システムは Secure Cloud Analytics 動的エンティティモデリングを FTD イベントに適用し、動作モデリング分析を使用して Secure Cloud Analytics の観測値とアラートを生成できます。**Total Network Analytics and Monitoring** パッケージを使用すると、システムは FTD イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、プロビジョニングされた Cisco Secure Cloud Analytics ポータルを CDO からクロス起動できます。詳細については、「Cisco Security Analytics and Logging」を参照してください。

ログの変更

変更ログは、CDO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。
- CDO 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、CDO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。

Cisco Defense Orchestrator での FTD の管理