Cisco Defense Orchestrator による ASA の管理

Cisco Defense Orchestrator による ASA の管理

Cisco Defense Orchestrator（CDO）はクラウドベースのマルチデバイスマネージャであり、すべての ASA デバイスのセキュリティポリシーを、シンプルで一貫性のあるセキュアな方法で管理できます。

このドキュメントの目的は、Cisco Defense Orchestrator（CDO）を初めて使用するお客様に、オブジェクトとポリシーの標準化、管理対象デバイスのアップグレード、VPN ポリシーの管理、リモートワーカーの監視に使用できる機能の概要を提供することです。このマニュアルでは、次のことを前提としています。

- 30 日間のトライアル用アカウントを作成している。または CDO を購入しており、シスコが CDO テナントを作成している。
- ネットワーク管理者新規 CDO テナントへの初回ログインユーザーを設定している。
- すでに ASA が構成されており、企業で使用している。
- CDO で管理する ASA にインターネットから直接アクセスできない場合は、ネットワークに Secure Device Connector（SDC）を展開する必要があります。SDC は、CDO と ASA 間の通信を管理します。詳細については、CDO の VM イメージを使用した Secure Device Connector の展開 または 自身の VM 上での Secure Device Connector の展開 を参照してください。

このドキュメントでは、デバイスオーケストレーションアクティビティの概要に続いて、CDO の CLI インターフェイス、変更ログ、パブリック REST API を紹介し、CDO がデバイスに実行できるその他の管理機能の一部を紹介します。

Cisco Defense Orchestrator による ASA の管理

はじめに

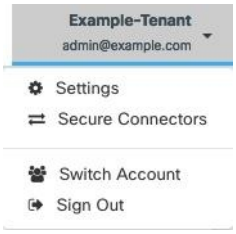
Secure Device Connector

デバイスのログイン情報を使用して CDO を ASA に接続する場合、CDO と ASA 間の通信を管理するために、ネットワークに Secure Device Connector（SDC）をダウンロードして展開することがベストプラクティスです。デバイスのログイン情報を使用して、すべての ASA の CDO への導入準備を行うことができます。ASA と CDO 間の通信を SDC で管理しない場合で、デバイスにインターネットから直接アクセスできる場合は、ネットワークに SDC をインストールする必要はありません。Cloud Connector を使用して ASA の CDO への導入準備を行うことができます。

テナントに複数の SDC を展開すると、パフォーマンスを低下させることなく、CDO テナントでより多くのデバイスを管理できます。1 つの SDC が管理できるデバイスの数は、それらのデバイスに導入されている機能と、構成ファイルのサイズによって異なります。ただし、展開計画の目安として、1 つの SDC で約 500 台のデバイスをサポートできることを想定しています。

SDC を表示するには：

1. CDO にログインします。
2. ユーザーメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。



デバイスの導入準備

ASA の CDO への導入準備は、まとめて、または一度に 1 つずつ実行できます。CDO でサポートされる ASA ソフトウェアおよびハードウェアの説明については、ASA サポート詳細 を参照してください。

テナントに追加する CDO ユーザーを作成する

Cisco Defense Orchestrator（CDO）には、読み取り専用、編集専用、展開専用、管理者、およびネットワーク管理者など、さまざまなユーザーロールがあります。ユーザーロールは、各テナントのユーザーごとに設定されます。1 人の CDO ユーザーが複数のテナントにアクセスできる場合、ユーザー ID は同じでも、テナントごとにロールが異なる場合があります。インターフェイスまたはドキュメントが読み取り専用ユーザー、管理者ユーザー、ネットワーク管理者ユーザーに言及している場合、特定のテナントにおけるそのユーザーの権限レベルを説明しています。異なるタイプのユーザーに付与される権限については、ユーザの役割 を参照してください。

テナントが作成された際、ネットワーク管理者ユーザーが自動的に割り当てられています。ネットワーク管理者は、テナントに他のユーザーを作成する権限を持ちます。これらの新しい

Cisco Defense Orchestrator による ASA の管理

ユーザーがテナントに接続するには、CDO のユーザーレコードと同じ E メールアドレスで Cisco Secure Sign-On アカウントを持っているか、それを作成する必要があります。CDO でユーザーレコードを作成するには、ユーザーロールのユーザーレコードの作成 を参照してください。

ポリシー オーケストレーション

ポリシーオーケストレーションには、オブジェクトとポリシーのレビューが含まれます。ASA のポリシーを処理する際は、CDO では「アクセスグループ」が「アクセスポリシー」と呼ばれることに注意してください。ASA のアクセスポリシーを探すには、CDO メニューバーの [ポリシー] > [ASA アクセスポリシー] の順に移動します。

ネットワークオブジェクトの問題を解決する

年月が経つにつれて、使用されなくなったオブジェクト、他のオブジェクトと重複したオブジェクト、デバイス間で値が一致しないオブジェクトがセキュリティデバイスに存在している場合があります。オーケストレーションタスクの第一歩としてこれらのオブジェクトの問題を修正します。

以下の順序でオブジェクトの問題に対処します。初期の手順で行う作業により、後の手順で対処する必要がある問題の多くが解決される場合があります。

1. 未使用のオブジェクトを解決する。未使用オブジェクト とは、デバイスに存在するが、別のオブジェクト、アクセスリスト、または NAT ルールによって参照されていないオブジェクトです。

2. 重複オブジェクトを解決する。重複オブジェクト とは、同じデバイス上にある、名前は異なるが値は同じである 2 つ以上のオブジェクトです。通常、重複したオブジェクトは誤って作成され、同じ目的を果たし、さまざまなポリシーによって使用されます。重複オブジェクトの問題を解決した後、CDO は、影響を受けるすべてのオブジェクト参照を残されたオブジェクト名で更新します。

3. 不整合オブジェクトを解決する。不整合オブジェクト とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーが異なる構成の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。これはセキュリティ上の問題となる場合があります。古いリソースを保護するルールが設定されている可能性があります。

シャドウルールの修正

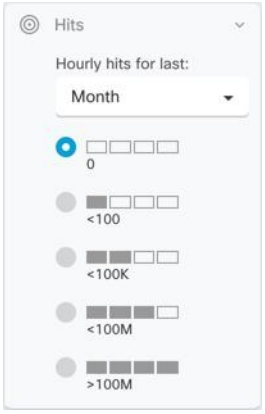
ネットワークオブジェクトの問題を解決したら、次にシャドウルールのネットワークポリシーを確認して修正します。**シャドウルール**は、ASA のアクセスポリシーページで半月のバッジ

Cisco Defense Orchestrator による ASA の管理

◑ で示されます。アクセスポリシーのルールはリストで構成され、上から下に 1 つずつ評価されます。ネットワークトラフィックはポリシー内のシャドウルールより上位のルールと一致するため、ポリシー内のシャドウルールが一致することはありません。ヒットすることのないシャドウルールがある場合は、それを削除するか、ポリシーを編集してルールを有効にします。

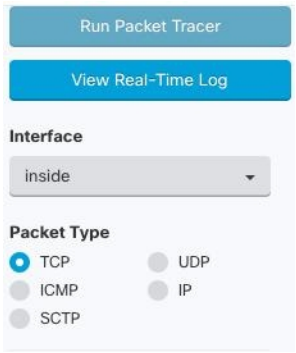
ポリシーのヒット率の評価

ポリシーのルールが実際にネットワークトラフィックを評価しているかどうかを判断します。CDO は、ポリシーのルールのヒット率データを毎時間収集します。デバイスが CDO によって管理されている時間が長いほど、特定のルールのヒット率データが持つ意味は大きくなります。特定の期間のヒット数で ASA アクセスポリシーをフィルタ処理して、ヒットしているかどうかを確認します。ヒットしていない場合は、ポリシーを作成し直すか削除することを検討してください。



ポリシーのトラブルシュート

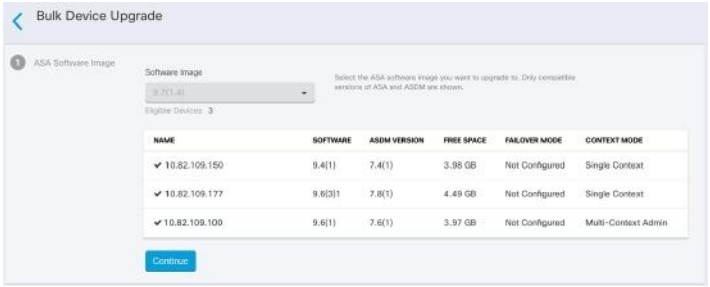
ASA パケットトレーサーを使用して、模擬パケットに対するポリシーの適用をテストして、ルールによってアクセスが誤ってブロックまたは許可されていないかを判断できます。



ASA と ASDM のアップグレード

次に、ASA と ASDM を最新バージョンにアップグレードします。お客様は、CDO を使用して ASA をアップグレードすると、75% ～ 90% の時間を節約できると報告しています。

Cisco Defense Orchestrator による ASA の管理



CDO は、シングルコンテキストまたはマルチコンテキストモードで、個々の ASA または複数の ASA にインストールされている ASA および ASDM イメージをアップグレードできるウィザードを提供しています。CDO は、ASA および ASDM イメージのデータベースを維持します。

CDO は、必要なアップグレード互換性チェックをバックグラウンドで実行します。ウィザードは、互換性のある ASA および ASDM イメージを選択し、それらをインストールし、デバイスをリブートしてアップグレードを完了するプロセスを導きます。CDO で選択したイメージが ASA にコピーおよびインストールされているものであることを検証することにより、CDO はアップグレードプロセスを保護します。

CDO は定期的にデータベースを確認し、最新の ASA および ASDM イメージをデータベースに追加します。CDO は、一般に利用可能な（GA）イメージのみをサポートし、データベースにカスタムイメージを追加しません。リストに特定の GA イメージがない場合は、[サポートに連絡] ページから Cisco TAC にお問い合わせください。確立されたサポートチケット SLA によってリクエストを処理し、リストにない GA イメージをアップロードします。

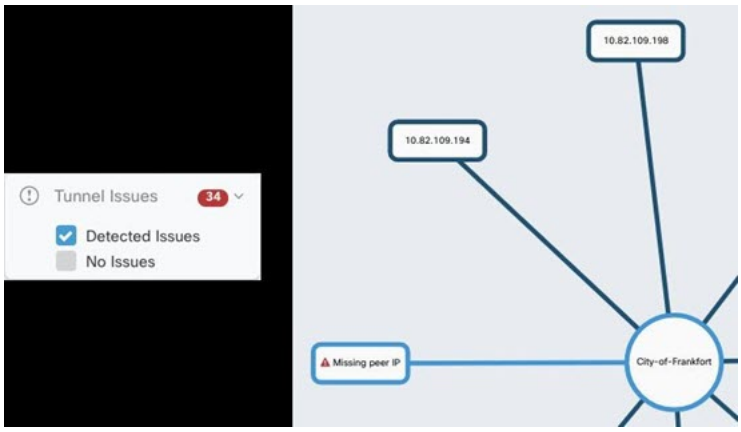
単一 ASA 上の ASA と ASDM イメージのアップグレード を確認してから、独自のリポジトリからのイメージを含む複数の ASA のアップグレード で ASA のアップグレードについてさらに学習してください。

VPN 接続の監視と管理

サイト間 VPN の問題を確認する

CDO は、ネットワーク内の ASA デバイスに存在する VPN の問題を報告します。環境の表示方法は 2 つあります。VPN ピアのリストを示す表と、ハブ アンド スポーク トポロジで VPN 接続を示すマップです。サイドバーのフィルタを使用して、注意が必要な VPN トンネルを検索します。

Cisco Defense Orchestrator による ASA の管理



以下の方法で、CDO を使用して VPN トンネルを評価します。

- サイト間 VPN トンネルの接続の確認
- ピアが欠落している VPN トンネルを見つける
- 暗号化キーの問題がある VPN ピアを見つける
- トンネルに対して定義された不完全な、または誤った構成のアクセスリストを見つける
- トンネル構成の問題を見つける

管理されていないサイト間 VPN ピアの導入準備を行う

CDO は、管理されていない VPN ピアも識別します。このようなデバイスを見つけたら、管理対象外 VPN ピアの導入準備 を使用してデバイスの導入準備を行い、CDO で同様に管理します。

ASA リモートアクセス VPN のサポート

CDO を使用することで、リモートアクセス仮想プライベートネットワーク（RA VPN）構成を作成して、ユーザーが ASA 経由で接続中にエンタープライズリソースにセキュアにアクセスできるようになります。ASA の CDO への導入準備が行われると、ASDM または Cisco Security Manager（CSM）を使用して設定済みのすべての RA VPN 設定が CDO によって認識されるため、CDO で管理できるようになります。

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、RA VPN 接続が可能です。

CDO は、ASA デバイスでの RA VPN 機能の次の側面をサポートします。

- 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 ASA デバイス間での共有 RA VPN 構成

詳細については、ASA のリモートアクセス VPN を設定するを参照してください。

Cisco Defense Orchestrator による ASA の管理

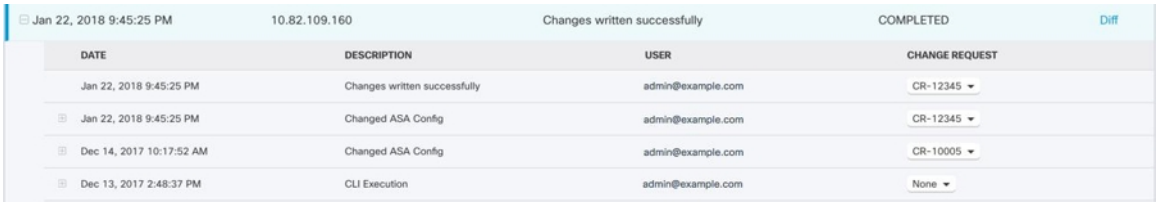
デバイス構成同期を監視する

CDO は、データベースに保存したデバイス構成と、ASA にインストールされている構成を定期的に比較します。CDO への導入準備がされた ASA は、引き続きデバイスの Adaptive Security Device Manager（ASDM）によって管理できます。そのため CDO はその構成がデバイスの構成と同じであることを確認し、相違点があれば警告します。[同期済み]、[非同期]、[競合検出] のデバイスの状態の詳細は、競合検出 を参照してください。

変更ログで変更を追跡する

デバイスの構成に加えた変更は、変更ログ に記録されます。変更ログには、CDO からデバイスに展開された変更、デバイスから CDO にインポートされた変更などの情報が表示されます。ここでは変更の「差分」、変更の時期、変更者といった変更内容も表示できます。

企業の追跡番号を使用するカスタムラベルを作成して、加えた変更に適用することもできます。変更ログでは、そのカスタムラベル、日付範囲、特定のユーザー、変更タイプで変更のリストをフィルタ処理して、目的の変更を見つけることができます。



以前の構成を復元する

ASA に加えた変更を「元に戻す」必要がある場合、CDO を使用してデバイスを以前の構成に復元できます。詳細については、ASA 設定の復元を参照してください。

コマンド ライン インターフェイスとコマンドマクロを使用してデバイスを管理する

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。

ASA CLI のユーザーは、シスコの CLI ツールの追加機能を活用できます。SSH セッションでデバイスに接続するのではなく、CDO の CLI ツールを使用するべき理由は以下のとおりです。

- CDO は、コマンドに必要なユーザーモードを認識します。コマンドを実行するために権限レベルを上げたり下げたりする必要はありません。また、コマンドを実行するために特定のコマンドコンテキストを入力する必要もありません。
- CDO はコマンド履歴を保持しているため（）、リストから選択するだけで簡単にコマンドを再実行できます。
- CLI アクションは変更ログに記録されるため、送信されたコマンドと実行されたアクションを確認できます。
- コマンドは一括モードで実行できるため、オブジェクトまたはポリシーを複数のデバイスに同時に展開できます。

Cisco Defense Orchestrator による ASA の管理

- CDO は CLI マクロを提供します（）。. CLI マクロはすぐに実行可能なコマンドで、格納された状態からそのまま使用できます。または、CLI コマンドの「空白を埋めて」から実行することもできます。これらのコマンドを 1 つのデバイスで実行することも、コマンドを複数の ASA に同時に送信することもできます。
- CLI は、完全な ASA 構成ファイルを提供します。これを表示することも、上級ユーザーの場合は直接編集して変更を保存することもできます。CLI コマンドを実行して変更する必要はありません。

CDO パブリック API

CDO はパブリック API を公開しており、ドキュメント、例、実験用のプレイグラウンドを提供しています。パブリック API の目標は、通常は CDO UI で実行できる多くのことをコードで実行するためのシンプルで効果的な方法を提供することです。

この API を使用するには、GraphQL の知識が必要です。学ぶのは非常に簡単で、詳細で読みやすい公式ガイド（https://graphql.org/learn/）が提供されています。GraphQL を選択した理由は、柔軟で、厳密に型指定され、自動文書化されるためです。

完全なスキーマドキュメントを見つけるには、GraphQL Playground に移動し、ページの右側にある [ドキュメント] タブをクリックするだけです。

このリンクから、またはユーザーメニューから [</>CDO API] を選択して、CDO パブリック API を起動できます。

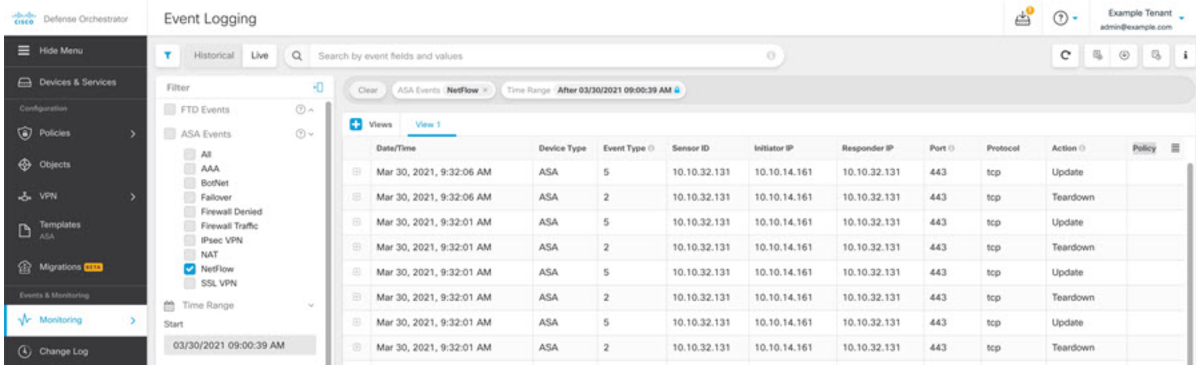
CDO と SecureX の統合

Cisco SecureX プラットフォームは、広範なシスコの統合セキュリティポートフォリオとお客様のインフラストラクチャを接続することで、一貫した操作性を提供します。これにより可視性が統一され、自動化が実現し、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティが強化されます。統合プラットフォームで技術を連携することで、SecureX は測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。詳細（SecureX と CDO）とハウツー（CDO の SecureX への追加）もご覧ください。

Cisco Security Analytics and Logging

追加のライセンスを使用すると、Cisco Security Analytics and Logging で Syslog イベントと Netflow Secure Event Logging（NSEL）イベントを ASA から Secure Event Connector（SEC）に直接送信し、それから Cisco Cloud に転送できます。クラウドに転送されると、CDO の [イベントロギング] ページでこれらのイベントを表示できます。そこでイベントをフィルタ処理して確認することで、ネットワークでどのセキュリティルールがトリガーされているかを明確に把握できます。

Cisco Defense Orchestrator による ASA の管理



イベントのモニタリングに加えて、CDO から Secure Cloud Analytics ポータルを起動して、ログに記録されたイベントの動作分析を実行できます。

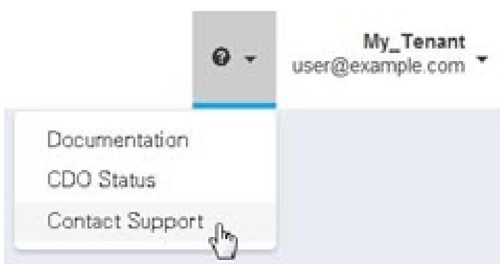
Cisco Security Analytics and Logging の導入方法の詳細は、ASA デバイスに安全なロギング分析（SaaS）を導入する を参照してください。

次の作業

これで、ASA の導入準備とポリシーのオーケストレーションを開始できます。

サポートが必要な場合

CDO GUI のサポートメニューをクリックして、サポートに連絡して質問したり、製品ドキュメントを読んだりできます。



Cisco Defense Orchestrator による ASA の管理