Branch Threat Defense の設定

Cisco Branch Threat Defense の概要

Cisco Branch Threat Defense は、保護を強化し、セキュリティ製品を重複して導入する必要がないことで時間と資金を節約するルータ セキュリティ テクノロジーです。このテクノロジーは、直接インターネット接続を使用してデータ センターをバイパスするブランチ オフィスにおけるセキュリティの脆弱性を軽減し、企業の支社、本社、およびデータ センターの間の通信を暗号化します。『Cisco Branch Threat Defense Guide』を参照してください。

Cisco Prime Infrastructure を使用して、規制コンプライアンスの使用例から開始して、Branch Threat Defense を設定し、ゾーンベースのファイアウォール（ZBFW）、Snort 侵入防御システム（IPS）、クラウド Web セキュリティ（CWS）、OpenDNS などのテクノロジーを設定できます。

関連トピック

サポート対象の IOS-XE プラットフォーム （1 ページ）
サポート対象の IOS-XE バージョン （2 ページ）
Branch Threat Defense を有効にするための前提条件 （2 ページ）
Branch Threat Defense ウィザードの使用 （2 ページ）

サポート対象の IOS-XE プラットフォーム

Branch Threat Defense 機能は、Cisco 4000 シリーズ サービス統合型ルータ（ISR）でサポートされます。

サポート対象の IOS-XE バージョン

Branch Threat Defense 機能は、Cisco IOS-XE リリース 15.5(3)S1（OpenDNS が設定されている場合は 16.3.1）および以降のリリースでサポートされます。

Branch Threat Defense を有効にするための前提条件

- この機能は、セキュリティ ライセンスを必要とするセキュリティ パッケージでのみ使用できます。ライセンスの取得については、シスコ サポートにお問い合わせください。
- Cisco 4000 シリーズ ISR に少なくとも 8 GB の RAM があることを確認してください。詳細については、『Security Configuration Guide for Branch Threat Defense』の「Virtual Service Resource Profile」の項を参照してください。
- プロビジョニング対象の各ルータには、ファイル システム上の同じ場所に Snort IPS OVA がすでに存在している必要があります。先に進む前に、「Copy OVA to Device」CLI テンプレートを使用して Snort IPS OVA をプロビジョニング対象の各デバイスに配布します。

関連トピック

サポート対象の IOS-XE プラットフォーム （1 ページ）
サポート対象の IOS-XE バージョン （2 ページ）
Branch Threat Defense ウィザードの使用 （2 ページ）

Branch Threat Defense ウィザードの使用

ステップ 1 **[サービス（Services）] > [ネットワーク サービス（Network Services）] > [Branch Threat Defense]** を選択します。

ステップ 2 [次へ（Next）] をクリックして設定を選択します。

ステップ 3 [設定の選択（Choose Configuration）] ページの説明を読み、[使用例の選択（Select a Use Case）] ドロップダウン リストから必要な使用例を選択します。

設定オプションは、選択した使用例によって異なります。

ステップ 4 必要な設定オプションを選択し、[次へ（Next）] をクリックします。

ステップ 5 設定するデバイスを選択し、[次へ（Next）] をクリックします。

ステップ 6 設定値を入力するか、または選択した使用例に応じて、インポート/エクスポートアイコンを使用して、**ZBFW**、**Snort IPS CLI**、**CWS**、および **OpenDNS** を設定します。

ステップ 7 [適用（Apply）] をクリックし、[次へ（Next）] をクリックして [CLI サマリー（CLI Summary）] タブに移動すると、デバイスおよびテンプレートの設定値を確認できます。

ステップ 8 [準備およびスケジュール（Prepare and Schedule）] タブを使用して導入ジョブのスケジュールを設定します。

ステップ 9 [次へ（Next）] をクリックし、[確認（Confirmation）] タブで [展開（Deploy）] をクリックして、Branch Threat Defense を導入します。

ステップ 10 [ジョブ ステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] にジョブの詳細を表示します。

関連トピック

Cisco Branch Threat Defense の概要 （1 ページ）
サポート対象の IOS-XE プラットフォーム （1 ページ）
サポート対象の IOS-XE バージョン （2 ページ）
Branch Threat Defense を有効にするための前提条件 （2 ページ）