使用する前に

この章では、Cisco Secure Firewall の機能と、サポートされているブランチおよび WAN の機能の概要について説明します。

- この資料について （1 ページ）
- Cisco Secure Firewall （1 ページ）
- ブランチの簡素化の概要 （2 ページ）
- 機能 （3 ページ）

この資料について

このガイドでは、Cisco Secure Firewall でサポートされているブランチおよび WAN の機能を使用する主な使用例について詳しく説明します。

各アプローチは、ネットワークで考えられるすべてのニーズに対応するものではありません。ネットワークを構築するときのモデルとして使用してください。例で示されている機能を使用せずに、実際のニーズに合うように機能を追加したり置き換えたりすることもできます。

このガイドは、Cisco Secure Firewall に精通していることを前提としています。設定の詳細については、『Cisco Secure Firewall Management Center Administration Guide, 7.3』および『Cisco Secure Firewall Management Center Device Configuration Guide, 7.3』を参照してください。

Cisco Secure Firewall

Cisco Secure Firewall は、Snort IPS、URL フィルタリング、マルウェア防御などの最先端機能を備えた、非常に堅牢なファイアウォール ソリューションです。

この包括的な製品により、物理、プライベート、およびパブリッククラウド環境で一貫したセキュリティポリシーを適用することで、脅威からの保護が大幅に簡素化されます。

さらに、ネットワークインフラストラクチャを広範囲に可視化し、潜在的な脅威の発生源とアクティビティを迅速に特定します。この情報を活用することで、攻撃によって運用が中断される前に、攻撃を阻止するための措置を迅速に講じることができます。

従来のファイアウォール機能に加えて、次の機能が提供されます。

1. アプリケーションの可視化と制御
2. ユーザーアイデンティティの認識と制御
3. 侵入防止と侵入検知
4. SSL/TLS の復号
5. レピュテーションベースのブロッキング
6. ファイルとマルウェアの防御
7. バーチャル プライベート ネットワーク（VPN）

ネットワーク展開のセキュリティを向上させるために、Cisco Secure Firewall は、以降のリリースで次のような追加のセキュリティ機能を提供します。

- 暗号化された可視性エンジン（EVE）。完全な中央のメインシステム（MITM）の復号を導入することなく、暗号化されたトラフィックの検査を強化します。
- エレファントフローの検出。エレファントフロー（通常は 1 GB/10 秒を超えるフロー）を検出して修復し、高い CPU 使用率とパケットドロップを回避します。
- Cisco Secure Dynamic Attribute Connector（CSDAC）。従来の IP/ネットワークベースのポリシー設定ではなく、ポリシー設定用のタグとラベルを活用することで、セキュリティポリシー管理に俊敏性とインテリジェンスをもたらします。

ブランチの簡素化の概要

組織が複数のブランチロケーションに業務を拡大するにつれて、セキュアで合理化された接続を確保することが最優先されるようになります。セキュアなブランチ ネットワーク インフラストラクチャを展開するには、複雑な設定と管理のプロセスが必要です。これには時間がかかり、適切に処理しないとセキュリティの脆弱性が発生しやすくなります。ただし、組織はセキュアなファイアウォール ソリューションを活用して、簡素化されたセキュアなブランチ展開を実現することで、これらの課題を克服できます。

このガイドでは、堅牢なファイアウォール ソリューションを使用した、セキュアなブランチ展開の簡素化の概念について説明します。セキュアなファイアウォールをブランチ ネットワーク アーキテクチャの基本コンポーネントとして統合することで、組織は展開プロセスを簡素化しながら、強力なセキュリティベースラインを確立することができます。このアプローチにより、組織は統合されたセキュリティポリシーを適用し、トラフィックルーティングを最適化し、復元力のある接続を確保することができます。

Cisco Secure Firewall でサポートされているブランチおよび WAN の簡素化機能の一部を次に示します。

- **セキュアで柔軟な接続**：
  - 本社（ハブ）とブランチ（スポーク）の間のルートベース（VTI）VPN トンネル
  - VTI を介した IPv4 および IPv6 BGP、IPv4 および IPv6 OSPFv2/v3、IPv4 EIGRP

- スタティックまたはダイナミック IP を持つスポークのための DVTI のサポート

- **ネットワークのダウンタイムがほぼゼロの高可用性**：
  - デュアル ISP 設定
  - アプリケーションベースのインターフェイス モニタリングに基づく最適なパス選択
- **使用可能帯域幅の増加**：
  - 複数の ISP にまたがるロードバランシングのための ECMP のサポート
  - SVTI のための ECMP のサポート
  - PBR を使用したアプリケーションベースのロードバランシング
- **パブリッククラウドおよびゲストユーザーのダイレクト インターネット アクセス**：
  - 一致基準としてアプリケーションを使用したポリシーベースルーティング
  - Cisco Umbrella のためのローカルトンネル ID のサポート
- **シンプルな管理**：
  - SASE：Cisco Umbrella 自動トンネルの展開
  - DVTI ハブスポークトポロジの簡素化

機能

次の表に、一般的に使用される WAN 機能の一部を示します

機能	導入されたリリース
VTI のループバック インターフェイス サポート	リリース 7.3
サイト間 VPN を使用したダイナミック VTI（DVTI）のサポート	リリース 7.3
Cisco Umbrella 自動トンネル	リリース 7.3
VTI の IPv4 および IPv6 BGP、IPv4 および IPv6 OSPFv2/v3、IPv4 EIGRP のサポート	リリース 7.3
ハブアンドスポークトポロジを使用したルートベースのサイト間 VPN	リリース 7.2
パスのモニタリングによるポリシーベースのルーティング	リリース 7.2
サイト間 VPN 監視ダッシュボード	リリース 7.1

機能	導入されたリリース
ダイレクト インターネット アクセス/ポリシーベースルーティング	リリース 7.1
WAN インターフェイスを使用した Equal-Cost-Multi-Path（ECMP）ゾーン	リリース 7.1
VTI インターフェイスを使用した Equal-Cost-Multi-Path（ECMP）ゾーン	リリース 7.1
ルートベースのサイト間 VPN 向けバックアップ用 VTI	リリース 7.0
サイト間 VPN を使用したスタティック VTI（SVTI）のサポート	リリース 6.7

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。