Cisco Secure Firewall Threat Defense SD-WAN 設計および導入ガイド

2025 年 9 月

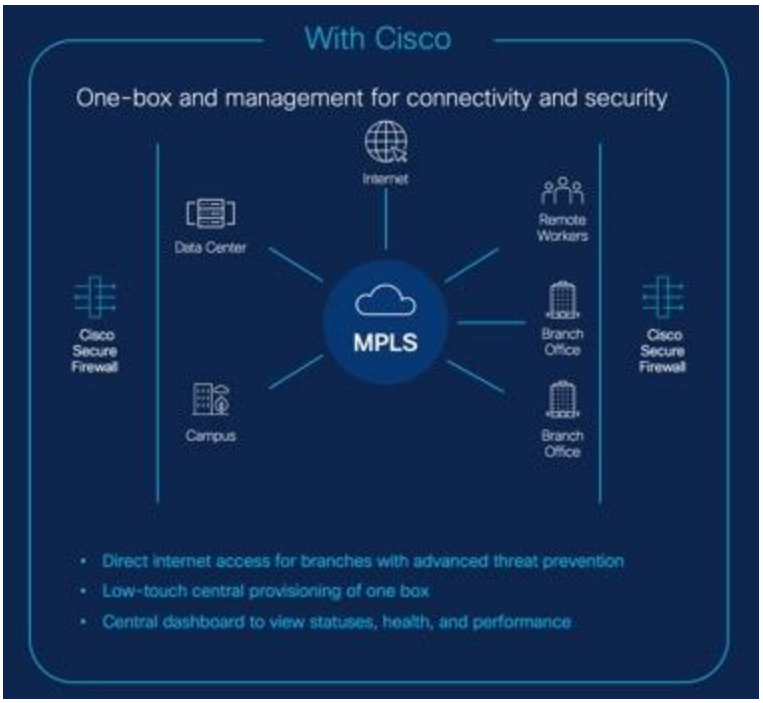
Cisco Secure Firewall SD-WAN ソリューションの概要

このドキュメントは、Cisco Secure Firewall Threat Defense および Cisco Secure Firewall Management Center を使用した Cisco SD-WAN に関する事前検証済みの設計および導入ガイドです。このガイドでは、可用性の高いフルサービスの SD-WAN ネットワークを構築するための設計ガイドライン、設定、および考慮事項について説明し、Cisco Secure Firewall を使用した Cisco SD-WAN のベストプラクティスを紹介します。

ソフトウェア定義型 WAN（SD-WAN）ソリューションは、さまざまな WAN トランスポートテクノロジー間での柔軟な接続が可能なため、広域ネットワーク（WAN）への最新のアプローチを提供します。SD-WAN（ソフトウェア定義型広域ネットワーク）によって、複数の WAN 接続で動的なポリシーベースのアプリケーションパス選択が可能になり、WAN の最適化やファイアウォールなどの追加サービスとの統合が容易になります。

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、複雑な設定が必要です。これには時間がかかり、適切に処理しないと設定エラーが発生しやすくなります。ただし、組織は Cisco Secure Firewall Management Center（Management Center）および Cisco Secure Firewall Threat Defense（Threat Defense）デバイスを活用し、簡素化された安全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

図 1.　　Cisco Secure Firewall SD-WAN ソリューション



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てセキュアなブランチ展開を簡素化する方法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 SD-WAN の機能

- 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仮想トンネルインターフェイス（VTI）VPN トンネル
  - VTI を介した IPv4 および IPv6 BGP、IPv4 および IPv6 OSPF、IPv4 EIGRP
  - スタティックまたはダイナミック IP を持つスポークをサポートするダイナミック VTI（DVTI）ハブ
- シンプルな管理：
  - SD-WAN デバイスのゼロタッチプロビジョニング
  - 簡素化されたブランチ展開のデバイステンプレート
  - 中央集中型の本社とリモートブランチ間の VPNトンネルセットアップ用 SD-WAN ウィザード
  - SD-WAN ネットワーク、アプリケーションの可視性、およびパフォーマンスモニタリングを行うための集中型 SD-WAN ダッシュボード
  - SASE 展開用の SSE 統合
- アプリケーション認識：
  - 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（DIA）
  - 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（PBR）
  - Cisco Umbrella のためのローカルトンネル ID のサポート
- 使用可能帯域幅の増加：
  - 複数の ISP と VTI にまたがるロードバランシングのための 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
- 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

Cisco Secure Firewall SD-WAN 機能

次の表に、Management Center の SD-WAN 機能を示します。

表 1. Management Center の SD-WAN 機能

機能	導入先
SD-WAN ウィザード	リリース 7.6
Cisco SD-WAN サマリーダッシュボードを使用したアプリケーションモニタリング	リリース 7.4.1

機能	導入先
Cisco SD-WAN サマリーダッシュボード	リリース 7.4
ユーザーアイデンティティと SGT を使用したポリシーベースのルーティング	リリース 7.4
HTTP パスのモニタリングを使用したポリシーベースのルーティング。	リリース 7.4
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 OSPF、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
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 および 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

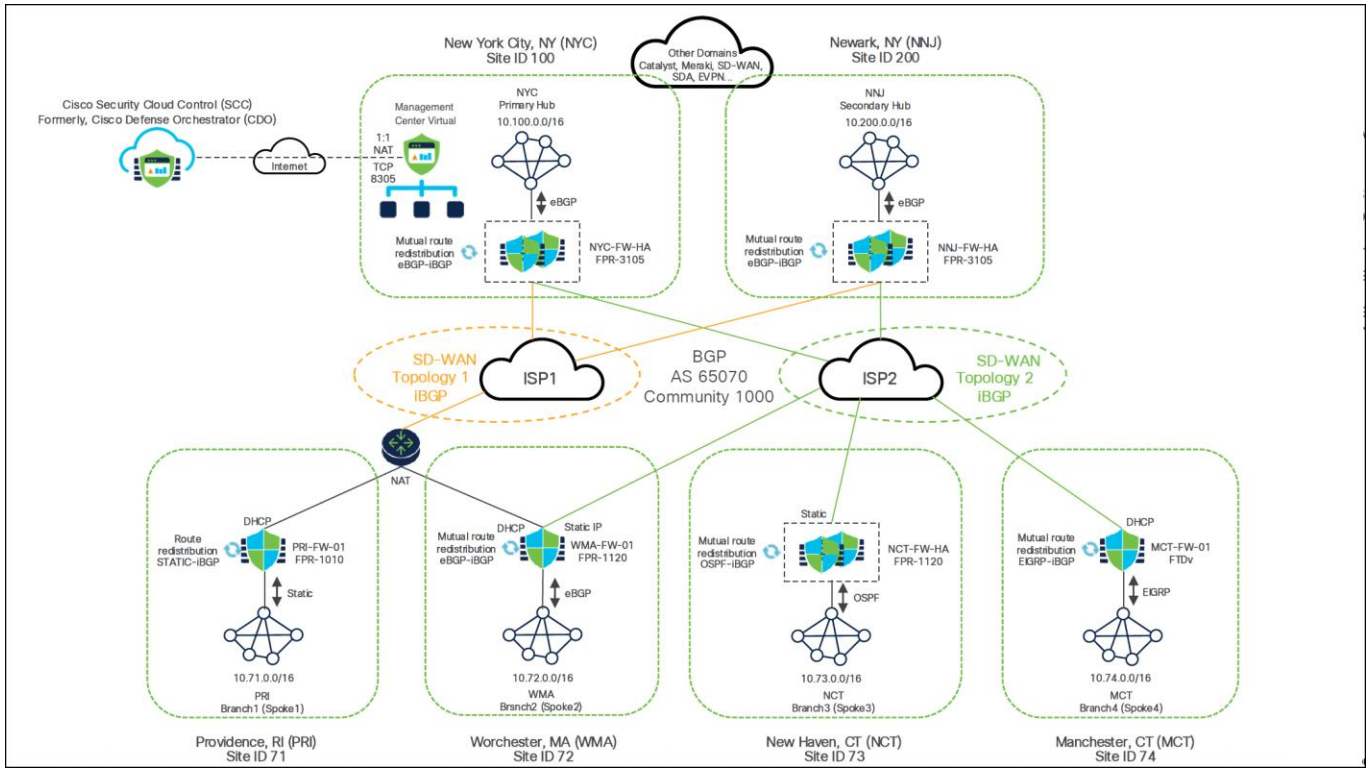
Management Center および Threat Defense デバイスを使用した SD-WAN アーキテクチャ

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Secure Firewall Management Center リリース 7.6
- Cisco Secure Firewall Threat Defense リリース 7.6

この導入ガイドの参考資料としてアーキテクチャ図を参照してください。

図 2.　　Management Center および Threat Defense デバイスを使用した SD-WAN アーキテクチャ



- **ニューヨーク市、NY（NYC）**：ファイアウォール 3105 HA ペアを備えたプライマリ SD-WAN ハブ（NYC-FW-HA）
- **ニューアーク、NY（NNJ）**：ファイアウォール 3105 HA ペアを備えたセカンダリ SD-WAN ハブ（NNJ-FW-HA）
- **ISP1 および ISP2**：すべてのハブおよびブランチデバイスがこれら 2 つのサービスプロバイダーに接続されています。
- **プロビデンス、RI（PRI）**：Firepower 1010 を備えた SD-WAN ブランチ（PRI-FW-01）
- **ウースター、MA（WMA）**：Firepower 1120 を備えた SD-WAN ブランチ（WMA-FW-01）
- **ニューヘブン、CT（NCT）**：Firepower 1120 HA ペアを備えた SD-WAN ブランチ（NCT-FW-HA）
- **マンチェスター、CT（MCT）**：Threat Defense Virtual を備えた SD-WAN ブランチ（MCT-FW-01）
- **Management Center Virtual**：すべてのハブおよびブランチデバイスを管理します。
- **Security Cloud Control（SCC）**：ゼロタッチプロビジョニング（ZTP）とその他のクラウドアシスト機能を容易にする、Cisco Security Cloud 用のシスコの統合型クラウドネイティブ セキュリティ管理インターフェイスです。**Cisco Security Cloud**

ハブでは以下を使用します。

- Management Center と通信するための専用管理インターフェイス。
- ブランチの Threat Defense デバイスに接続するデータインターフェイス。

表 2. ハブおよびスポークの IP アドレス

デバイス（Device）	内部ネットワーク
ニューヨーク市、NY（NYC）	10.100.0.0/16
ニューアーク、NY（NNJ）	10.200.0.0/16
プロビデンス、RI（PRI）	10.71.0.0/16
ウースター、MA（WMA）	10.72.0.0/16
ニューヘブン、CT（NCT）	10.73.0.0/16
マンチェスター、CT（MCT）	10.74.0.0/16

Threat Defense デバイスの Management Center への導入準備

設計および設定時の注意事項

- ゼロタッチプロビジョニング（ZTP）方式：
  - Threat Defense デバイスのシリアル番号を使用
  - 次のデバイスモデルのみをサポートしています。
    - Firepower 1010
    - Firepower 1100
    - Cisco Secure Firewall 1200
    - Firepower 2100（7.4.x のみ）
    - Cisco Secure Firewall 3100
  - Management Center を Security Cloud Control と統合
- 登録キーによる方法：
  - Threat Defense デバイスの登録キーを使用
  - Threat Defense 仮想デバイスを含むすべてのデバイスタイプをサポート
  - デバイステンプレートの有無にかかわらず機能

デバイスの導入準備の方法

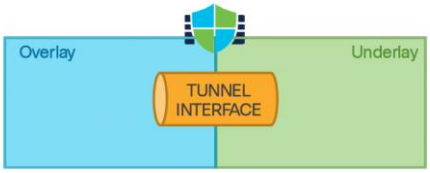
SD-WAN Threat Defense デバイスの Management Center への導入準備には複数の方法があります。

- **シリアル番号**：ZTP を使用し、そのシリアル番号を使用して 1 つ以上のデバイスの導入準備をします。「Onboard Threat Defense Device to Management Center Using ZTP」を参照してください。
- **登録キー**：登録キーを指定し、Management Center で変数を定義することで、単一のデバイスの導入準備ができます。「Onboard Threat Defense Device to Management Center Using Registration Key」を参照してください。

Threat Defense VPN トンネルインターフェイスの概要

VPN トンネルインターフェイスは、基盤となるネットワーク（アンダーレイ）と仮想オーバーレイネットワークを相互接続する論理インターフェイスです。トンネル経由でオーバーレイ通信を安全に送信します。このインターフェイスは、SD-WAN トンネル接続の基本コンポーネントであり、IPv4 と IPv6 の両方の通信をサポートします。

図 3.　　Threat Defense VPN トンネルインターフェイス



Threat Defense IPSec 仮想トンネルインターフェイス

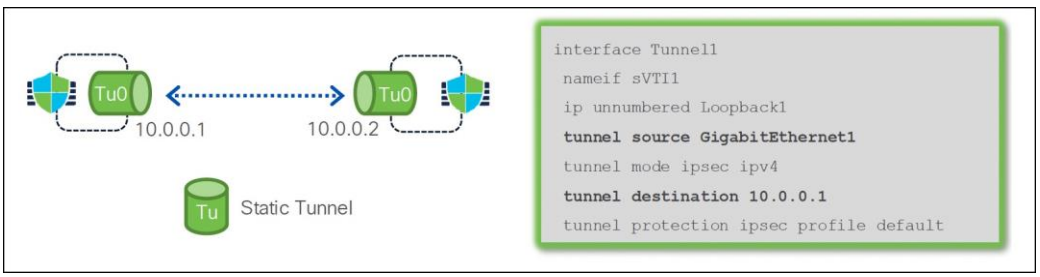
Threat Defenseは、ルーティング可能な論理インターフェイスである仮想トンネルインターフェイス（VTI）をサポートしています。このインターフェイスを使用して、スタティックおよびダイナミック ルーティング ポリシーを適用できます。VTI は、静的暗号マップのアクセスリストとリモートサブネットの追跡の必要性を削除することで VPN の設定を簡素化します。これによりルートベースの IPsec VPN が有効になり、Threat Defense デバイスはルーティング テーブル エントリに基づいて通信を暗号化または復号化します。VTI はスタティックルートとダイナミックルートをサポートしますが、マルチキャストはサポートしません。

図 4.　　Threat Defense IPSec 仮想トンネルインターフェイス

スタティック仮想トンネルインターフェイス

スタティック仮想トンネルインターフェイス（SVTI）は、バージョン 6.7 で導入されたサイト間 IPSec VPN トンネルの確立に使用されるルーティング可能な仮想インターフェイスの一種です。これらのインターフェイスは、常時接続の双方向 IPSec VPN トンネルを確立し、コネクテッドデバイスのいずれかが接続を開始できるようにします。これらのインターフェイスを使用して、2 つの Threat Defense デバイス間、または Threat Defense とその他のシスコ/サードパーティ製デバイス間にトンネルを作成できます。

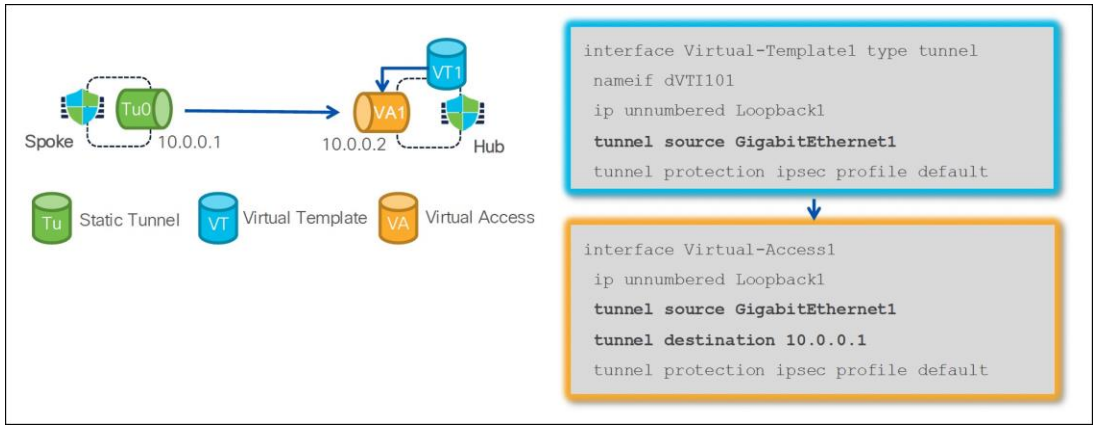
図 5.　　スタティック仮想トンネルインターフェイス



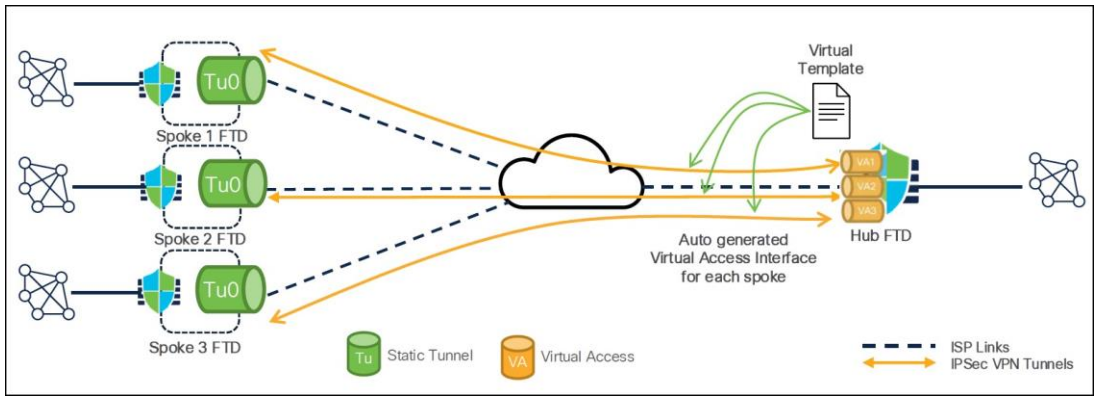
ダイナミック仮想トンネルインターフェイス

バージョン7.3で導入されたダイナミックVTIは、ポイントツーマルチポイントVPN用の仮想トンネルインターフェイスです。ダイナミック VTI では、IPsec トンネルインターフェイスの動的なインスタンス化および管理のために仮想テンプレートが使用されます。仮想テンプレートは、VPN セッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。このインターフェイスは一方向であり、スポークのみがトンネル確立接続を開始できます。

図 6.　　ダイナミック仮想トンネルインターフェイス



ハブアンドスポーク展開では、スポークデバイスがハブへの接続を開始すると、ハブは仮想テンプレートを利用して、各スポークに固有の仮想アクセスインターフェイスを作成します。



Cisco Secure Firewall Management Center を使用した SD-WAN オーバーレイの展開

リモートブランチを中央本社に接続するセキュアなネットワークインフラストラクチャを確立するのは困難です。SD-WAN トポロジ内でこれらのデバイスを手動で設定して展開するのは、時間がかかるうえエラーが発生しやすいため、さまざまな場所でネットワーク設定の不整合が発生したり、セキュリティの脆弱性が発生したりする可能性があります。

Management Center では、新しい SD-WAN ウィザードを使用して、中央の本社（ハブ）とリモートのブランチサイト（スポーク）間の VPN トンネルおよびルーティング設定を簡単に設定できます。このウィザードでは、ハブにダイナミック仮想トンネルインターフェイス（DVTI）を、スポークに SVTI（スタティック仮想トンネルインターフェイス）を使用して、ルートベースの VPN トンネルを、オーバーレイネットワークの BGP 設定とともに自動的に設定します。

ワークフローおよび Management Center の SD-WAN ウィザードを使用した SD-WAN オーバーレイの設定の詳細については、「Deploy an SD-WAN Overlay Using Cisco Secure Firewall Management Center」を参照してください。

ダイレクト インターネット アクセスを使用したアプリケーション通信のルーティング

このセクションでは、ダイレクト インターネット アクセス（DIA）を使用したアプリケーション通信のルーティングに関する情報を提供します。

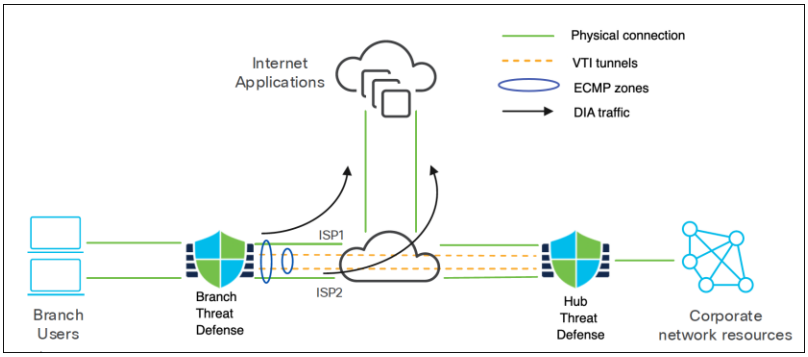
従来のネットワークの課題

従来のネットワーク展開では、セントラルサイトの境界ファイアウォールを使用して、ローカルユーザーとブランチユーザーの両方にセキュアなアクセスを提供しています。このアーキテクチャでは必要な接続が可能になりますが、暗号化された VPN トンネルを介してセントラルサイトを通過するすべてのインターネット通信をルーティングします。この方法では、パケットの遅延、ドロップ、およびジッターが増加する可能性があります。さらに多くの場合、コストが高くなり、帯域幅の消費が増え、ネットワーク管理がより複雑になります。

ダイレクト インターネット アクセスの概要

従来のネットワークの問題に対処する方法の 1 つが、ダイレクト インターネット アクセス（DIA）の導入です。DIA は、Cisco Secure Firewall で使用できる主要な SD-WAN 機能です。これはポリシーベースのルーティング（PBR）を利用しており、アプリケーション認識型ルーティングとも呼ばれます。

DIAでは、分散拠点からのアプリケーション通信がインターネットに直接ルーティングされるため、本社のインターネット宛通信のトンネリングを回避できます。この機能により遅延が短縮され、ユーザー体験が向上します。ブランチの Firewall Threat Defense デバイスは、インターネット イグジット ポイントを使用して設定されます。PBR ポリシーは入力インターフェイスに適用され、拡張アクセス制御リストで定義されたネットワーク、ポート、ユーザー名、ユーザーグループ、アプリケーション、セキュリティグループタグ（SGT）などの属性に基づいて通信を識別します。識別された通信は、出力インターフェイスを介してインターネットに直接転送されます。



PBR を使用してトラフィックを誘導する方法には以下があります。

- 送信元 IP アドレスベースのルーティング（バージョン 7.1 以降）
- アプリケーション認識型ルーティング（バージョン 7.1 以降）
- パスモニタリングを使用したアプリケーション認識型ルーティング
  - IP ベース（バージョン 7.2 以降）

- HTTP ベース（バージョン 7.4 以降）
- アイデンティティベースのルーティング（AD ユーザー、ユーザーグループ、および SGT）（バージョン 7.4 以降）

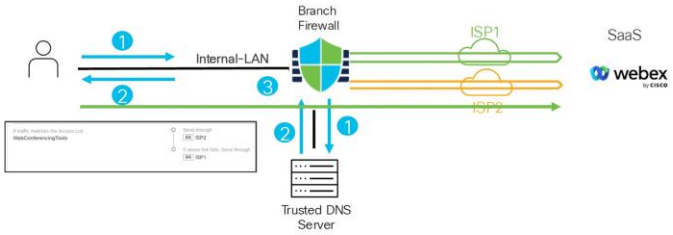
ポリシーベースルーティングのタイプ

アプリケーション認識型ルーティング

Threat Defense デバイスは、アプリケーションに基づいて通信をインターネットに直接送信します。

Management Center を使用したアプリケーション認識型ルーティングのユーザーワークフローは次のとおりです。

1. ユーザーが、いずれかの信頼できる DNS サーバーに対して 1 つまたは複数のアプリケーションの DNS 要求を開始します。
2. Threat Defense デバイスは、DNS 応答をスヌーピングし、ドメイン情報とそれに対応する IP アドレスを保存します。
3. アプリケーション通信は、PBR ポリシーのインターフェイス順序に基づいて出力インターフェイスに転送されます。



この例では、PBR ポリシーは、ISP2 インターフェイスを介して Webex などの Web 会議アプリケーション通信を送信し、ISP2 が失敗した場合は ISP1 に自動フォールバックします。

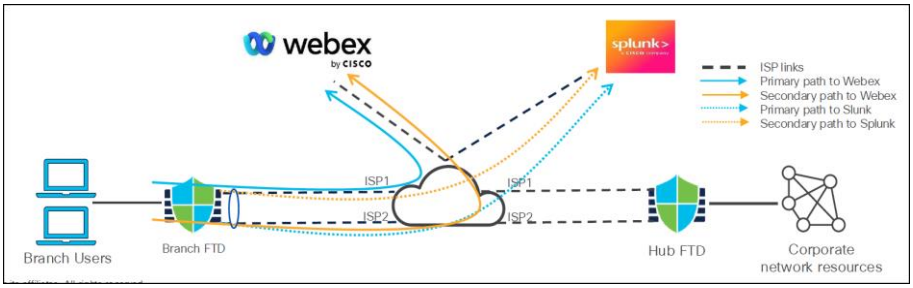
パスモニタリングを使用したアプリケーション認識型ルーティング

Threat Defense デバイスは、リアルタイムメトリックを評価し、最適に計算されたパスを使用して、アプリケーション認識型通信をインターネットに送信します。パスモニタリングで設定されたインターフェイスの場合、Threat Defense デバイスは ICMP または HTTP プローブを使用してこれらのメトリックを算出し、通信をルーティングするためのベストパスを決定します。

パスのモニタリングに使用されるダイナミックメトリックは次のとおりです。

- ラウンドトリップ時間（RTT）
- ジッタ
- 平均オピニオン評点（MOS）
- パケット損失

この例では、Webex および Splunk アプリケーションのベストパスが、パスモニタリングメトリックに基づいて動的に選択されます。



IP ベースのパスモニタリングのコンポーネント

- パスモニタリングモジュール（PMM）：ICMP プローブを使用してメトリックを収集します。
- ポリシーベースルーティング（PBR）エンジン：PMM からの最適なメトリックに従って、出力インターフェイスを介して通信をルーティングします。

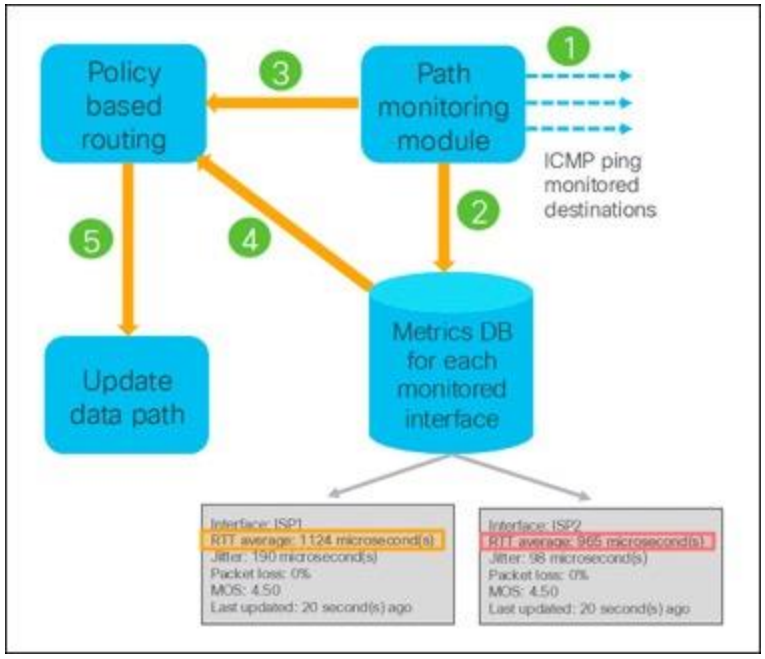
ICMP を使用したインターフェイスモニタリングのプローブ間隔は 1 秒です。

IP ベースのパスモニタリングのアーキテクチャ

Management Center での IP ベースのパスモニタリングを使用したアプリケーション認識型ルーティングのワークフローは次のとおりです。

1. PMM は、モニタリング対象の接続先に ICMP プローブを送信します。
2. PMM は、インターフェイスメトリックを計算してデータベースに保存します。
3. PMMは、PBR エンジンの更新に関するインターフェイスのリストを提供します。
4. PBR エンジンは、PMM データベースから最新のメトリックを取得します。
5. PBR エンジンは、インターフェイスとメトリックに基づいて、ルーティングの更新をデータパスにプッシュします。

図 7.　　IP ベースのパスモニタリングを使用したアプリケーション認識型ルーティングのワークフロー



この例では、ISP2 インターフェイスの RTT が ISP1 の RTT より低いため、PBR エンジンはこのメトリックを受信し、ISP2 インターフェイスを介して通信を誘導します。

HTTP ベースのパスモニタリングのコンポーネント

- HTTP クライアント：モニタリング対象のドメインまたはアプリケーションに HTTP プローブを送信し、応答を PMM に転送します。
- パスモニタリングモジュール：ICMP または HTTP プローブを介してメトリックを計算し、保存します。
- ポリシーベース ルーティング エンジン：PMM からの最適なメトリックに従って、出力インターフェイスを介して通信をルーティングします。

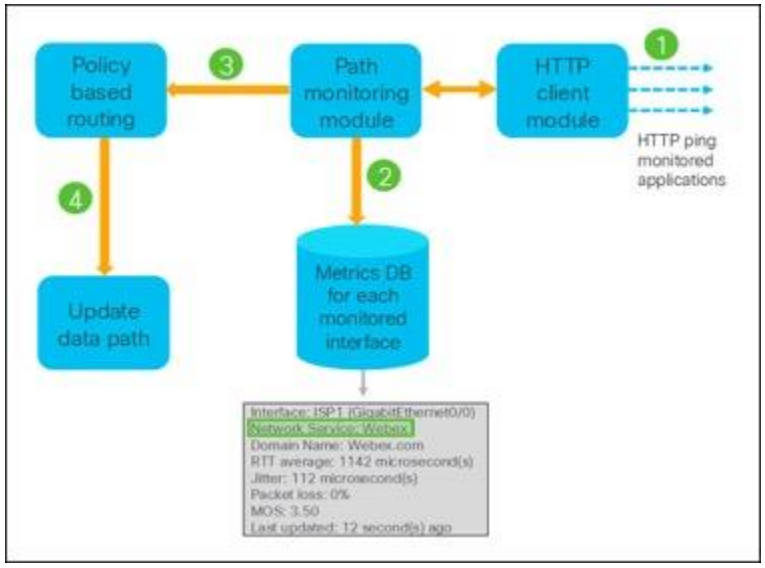
アプリケーションモニタリングのプローブ間隔は 10 秒です。

HTTP ベースのパスモニタリングのアーキテクチャ

Management Center での HTTP ベースのパスモニタリングを使用したアプリケーション認識型ルーティングのワークフローは次のとおりです。

1. HTTP クライアントモジュールは、DNS エントリが指定されたドメインに関してスヌーピングされると、アプリケーション モニタリングを開始します。
2. PMM は、インターフェイスメトリックを計算してデータベースに保存します。
3. PMM は、ドメインごとのメトリック値と出力インターフェイスを PBR エンジンに 30 秒ごとに提供します。
4. PBR エンジンは、インターフェイスとメトリックに基づいて、ルーティングの更新をデータパスにプッシュします。

図 8.　　HTTP ベースのパスモニタリングを使用したアプリケーション認識型ルーティングのワークフロー



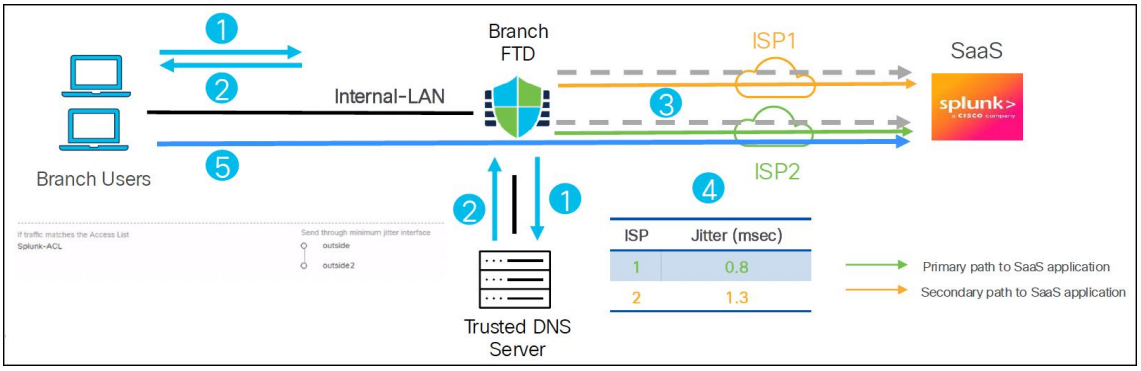
注：　緑色で強調表示されたセクションは、HTTP クライアントモジュールが ISP1 インターフェイスを介して Webex アプリケーション通信のパスメトリックを収集する方法を示します。

HTTPベースのパスモニタリングを使用したアプリケーション認識型ルーティングのユーザーワークフローは次のとおりです。

1. ユーザーが 1 つまたは複数のアプリケーションの DNS 要求を開始します。
2. Threat Defense デバイスは、DNS 応答をスヌーピングし、ドメイン情報とそれに対応する IP アドレスを保存します。
3. HTTP クライアントモジュールは、パスモニタリングが有効になっている出力インターフェイスで設定されたアプリケーションに HTTP プローブを送信します。

   注：　デフォルトでは、インターフェイスの HTTP ベースのアプリケーション モニタリングは有効になっています。

4. PMM は、各インターフェイスのメトリックを計算して保存し、PBR エンジンと共有します。
5. アプリケーション 通信は、最適なメトリックに基づいて出力インターフェイスに転送されます。



この例では、PBRポリシーは、最小のジッターでインターフェイス（outsideまたはoutside2）を介してSplunkアプリケーション通信をルーティングします。

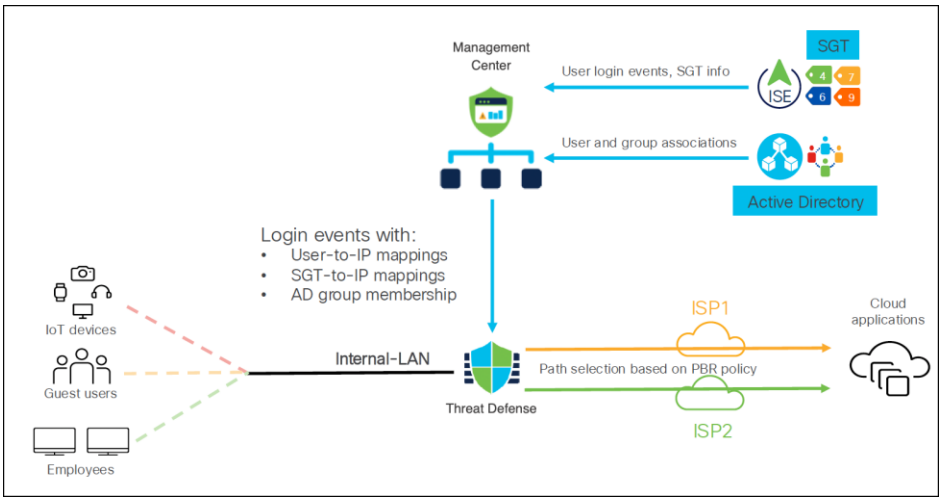
アイデンティティ認識型ルーティング

ThreatDefenseデバイスでのアイデンティティ認識型ルーティングは、次のような属性に基づいてネットワーク通信をルーティングすることにより、アプリケーション認識型ルーティングを拡張します。

- ユーザーアイデンティティ
- Microsoft Active Directory（AD）グループ
- セキュリティグループタグ（SGT）

この機能により、ユーザーアイデンティティまたはSGTに基づいて通信のセグメンテーションが可能になり、従業員、請負業者、ゲスト、およびIoTデバイスごとに異なるアクセスが可能になります。Microsoft AD との統合は必須であり、Cisco Identity Services Engine（ISE）は任意です。ISE が統合されていない場合は、Management Center でローカルに SGT を設定できます。

注： Cisco ISE とローカル SGT を同時に使用することはできません。



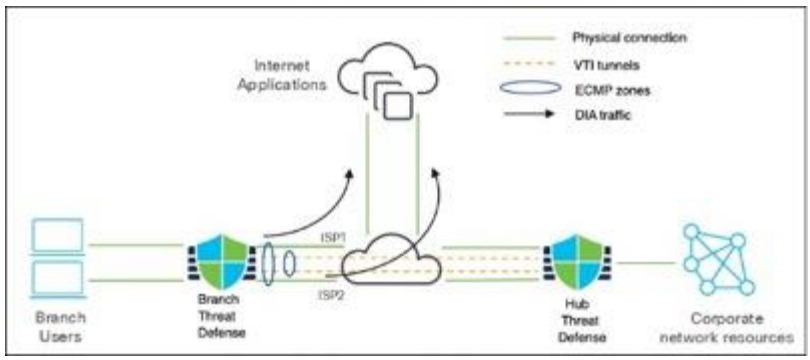
Management Center は次のような情報を受信します。

- ユーザーログインイベントと SGT（アイデンティティおよびアクセスサーバーである ISE から）
- ユーザーとグループの関連付け（AD サーバーから）

この情報は、ユーザーアイデンティティ、ユーザーグループ、または SGT に基づいて出力インターフェイスを通信に許可する PBR ルールを作成するために使用されます。

等コストマルチパス（ECMP）

バージョン 7.0 以降は、Management Center UI から ECMP を設定できます。ネットワーク通信を複数の等コストパスで送信できます。ECMP は、物理インターフェイスと VTI インターフェイスの両方をサポートし、ゾーン内に最大 8 つのインターフェイスを設定できます。



ダイレクト インターネット アクセスのコンポーネント

- 信頼できる DNS サーバー：**DIA のアプリケーション検出では、信頼できる DNS サーバーを介した DNS スヌーピングを使用して、アプリケーションまたはアプリケーションのグループを解決します。**
- **脆弱性データベース（VDB）**：Threat Defense デバイスは、アプリケーション検出のために、アプリケーションに関連付けられているドメインのリストを VDB から取得します。
- **ネットワークサービスオブジェクト（NSO）**：PBR 内で使用される、特定のアプリケーションに関連付けられたオブジェクト。NSO は事前に定義されており、Management Center によって Threat Defenseデバイスに展開されます。
- **ネットワーク サービス グループ（NSG）**：Threat Defense デバイスが PBR 設定に基づいてパスを決定するために使用するアプリケーションのグループ。複数の NSO を単一の NSG に含めることができます。Management Center は、PBR 拡張アクセスリストに基づいて NSG を自動的に生成します。

ポリシーベースルーティングの操作順序

1. Threat Defense デバイスは、トップダウン順で PBR ポリシーに対してパケットを評価します。
2. PBR エンジンは、最初の一致に基づいて出力インターフェイスを使用します。
3. 新しいエントリが PBR ポリシーの末尾に追加されます。

技術的なヒント： 複雑な PBR ポリシーがある場合は、必ず最も具体的なルールを最上位に設定してください。

4. エントリの順序を変更するには、目的のシーケンスにドラッグアンドドロップします。
5. 一致が見つからない場合、PBR エンジンは通常のルーティングにフォールバックします。

注： PBR は通常のルーティング上で機能するため、アクティブなルーティングテーブルの一部でなくても、異な

るインターフェイスを経由するルートをデバイス上で使用できるようにしてください。

ダイレクト インターネット アクセスの設定

Management Center での DIA のワークフロー、設定、および検証の詳細については、「Route Application Traffic to the Internet Using DIA in Cisco Secure Firewall Management Center」を参照してください。

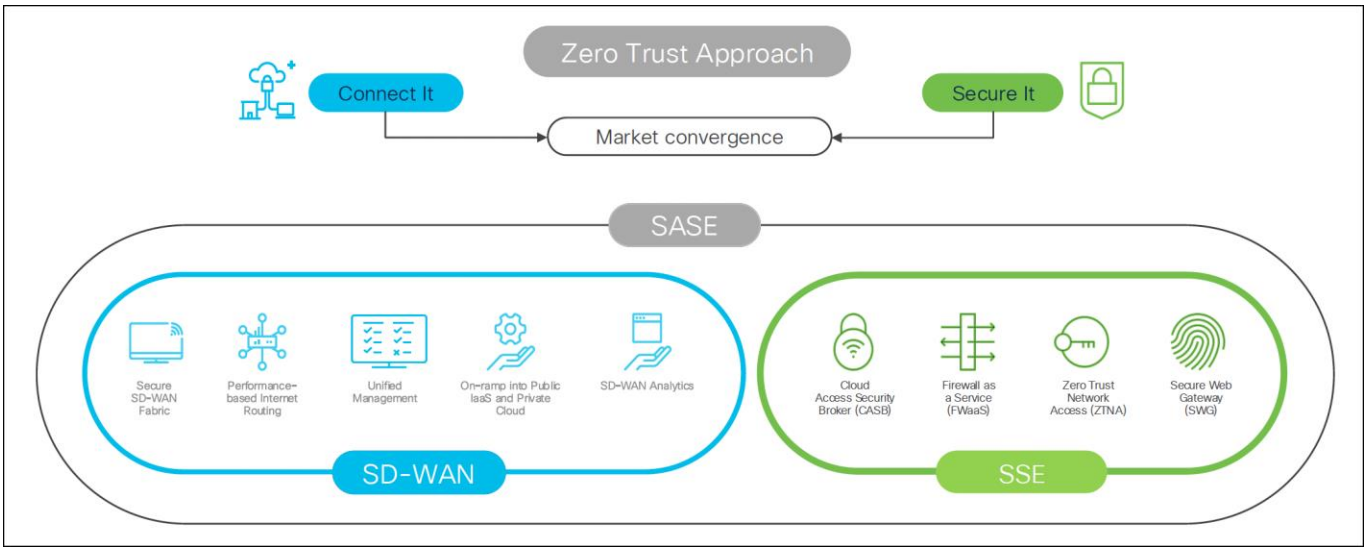
SASE および SSE ソリューションと Threat Defense の統合

リモートで作業し、クラウドアプリケーションを使用する人が増えると、データセンターに焦点を当てた従来のセキュリティモデルの効果が低下し、ユーザーのパフォーマンスが低下する可能性があります。Secure Access Service Edge（SASE）は、クラウドを使用して、ネットワークおよびセキュリティサービスとユーザーおよびデバイスの距離を近付ける新しい方法です。SASE は、どこからでもユーザーがアプリケーションやデータに安全にアクセスできるようにします。SASE は、すべてクラウドから提供されるソフトウェア定義型広域ネットワーク（SD-WAN）とさまざまなセキュリティサービスを統合します。これにより、組織は複雑なインフラストラクチャを管理することなく、任意のユーザーまたはデバイスを任意のアプリケーションに安全に接続できます。

ネットワーク全体を変更せずにセキュリティを向上させたい企業にとっては、セキュリティサービスエッジ（SSE）が適切なオプションです。重要なセキュリティ機能が SSE から提供され、セキュリティがシンプルになり、ユーザー体験が向上します。SSE の主な機能には、DNS レイヤセキュリティ、セキュア Web ゲートウェイ（SWG）、サービスとしてのファイアウォール（FWaaS）、クラウド アクセス セキュリティ ブローカ（CASB）、ゼロトラスト ネットワーク アクセス（ZTNA）などがあります。SSE は SASE フレームワークのセキュリティ部分であり、単独で、またはネットワーク機能も含まれる完全な SASE セットアップへの最初のステップとして使用できます。

SASE および SSE とは

図 9.　　SASE および SSE ソリューション



- セキュア アクセス サービスエッジ（SASE）：
  - ネットワーキング（SD-WAN）機能とセキュリティ（SSE）機能を統合します。
  - セキュア Web ゲートウェイ（SWG）、クラウド アクセス セキュリティ ブローカ（CASB）、データ損失防止（DLP）、次世代ファイアウォール（NGFW）、ゼロトラスト ネットワーク アクセス（ZTNA）などのセキュリティ機能を、SD-WAN（ソフトウェア定義型広域ネットワーク）などのネットワーク機能と組み合わせて提供します。

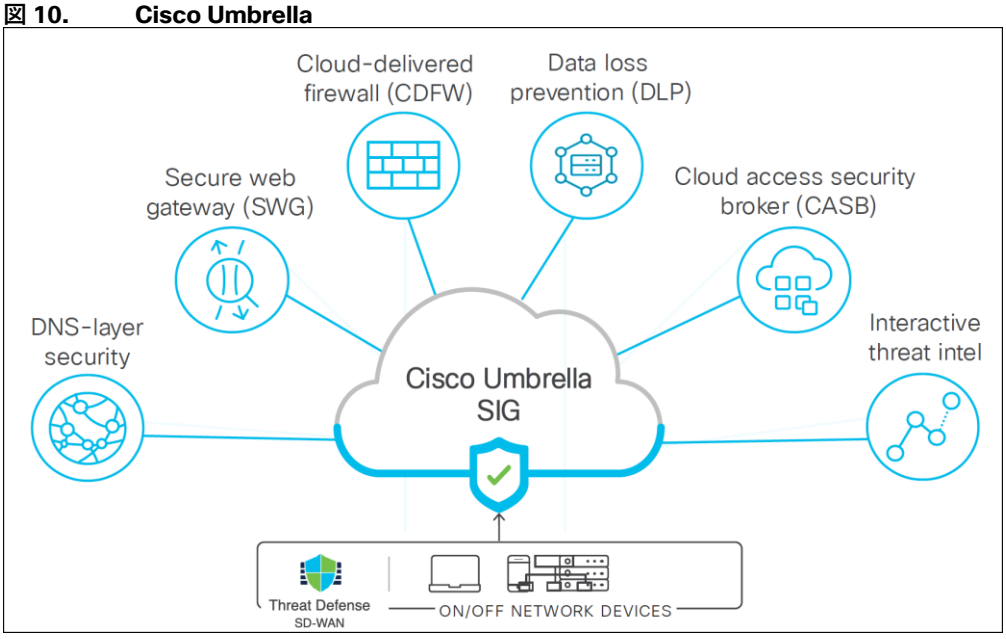
- デバイスまたはエンティティのアイデンティティ、リアルタイムコンテキスト、セキュリティおよびコンプライアンスポリシーに基づいて、ゼロトラストアクセスを有効にします。
- シスコのソリューションは、Cisco SD-WAN（Catalyst、Meraki、Threat Defense）と Cisco Umbrella および Cisco Secure Access です。

- セキュリティサービスエッジ（SSE）
  - SASE のセキュリティの側面を特に重視しています。
  - Web、クラウドサービス、およびプライベートアプリケーションへのアクセスを保護します。
  - ネットワークベースおよび API ベースの統合によって適用される、アクセス制御、脅威保護、データセキュリティ、セキュリティモニタリング、および許容可能な使用制御などの機能が含まれます。
  - クラウドベースのサービスを提供します。これにはオンプレミスまたはエージェントベースのコンポーネントを含めることができます。
  - シスコのソリューションは Cisco Secure Access です。

Cisco SASE ソリューション：Cisco Umbrella および Threat Defense を使用したセキュアなインターネットトラフィック

Cisco Umbrella は、クラウドベースのセキュア インターネット ゲートウェイ プラットフォームです。インターネットの脅威に対する防御を複数のレベルで提供します。DNS レイヤセキュリティ、SWG、クラウド提供型ファイアウォール、DLP、CASB、および脅威インテリジェンスを統合して、すべてのブランチに拡張性の高いセキュリティを提供します。リモートまたはオンプレミスユーザーからインターネットに向かうトラフィックは、ブランチから最も近い Cisco Umbrella ポイントに自動的にルーティングされ、検査を受けた後、アクセスが許可または拒否されます。

図 10.　　Cisco Umbrella

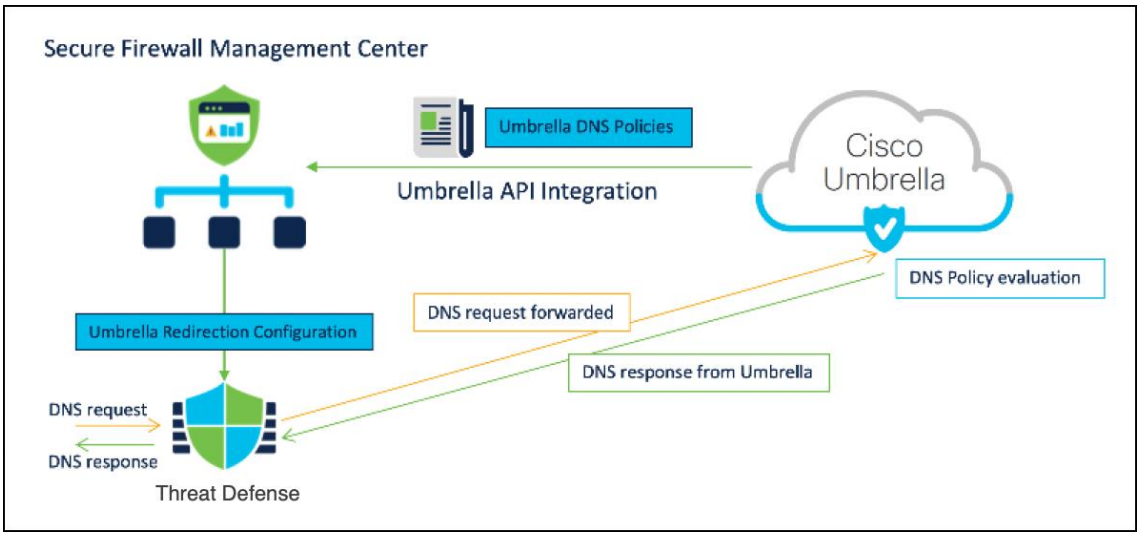


Cisco Umbrella の統合のユースケース

シスコ ファイアウォールは、次の 2 つの方法で Cisco Umbrella と統合できます。

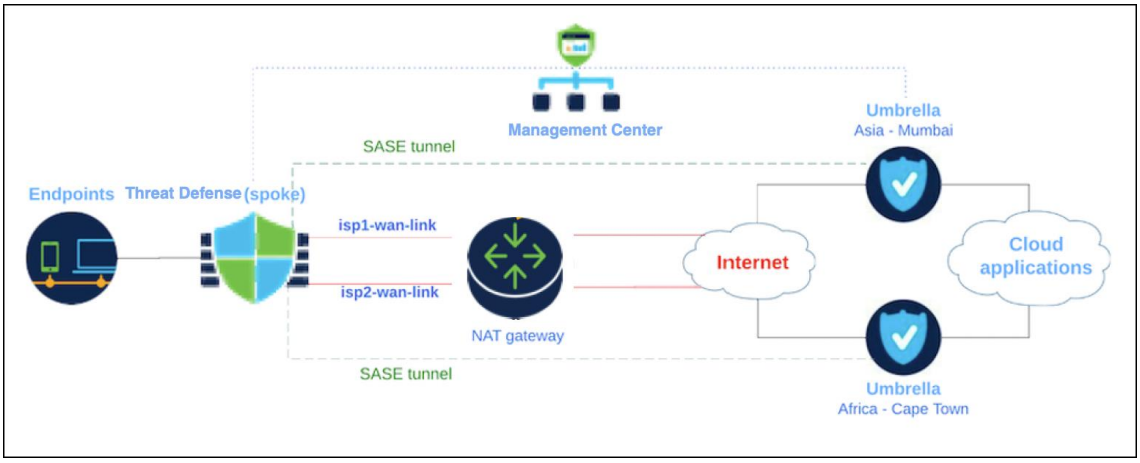
- 一貫した DNS ポリシーにより、すべてのブランチのインターネットトラフィックを保護。
  - すべてのブランチに共通の DNS ポリシー
  - マルチレイヤ DNS セキュリティ（Management Center および Cisco Umbrella DNS ポリシー）
  - 接続が確立される前に DNS 層でユーザーとアプリケーションを保護することで、結果として生じるパケット処理を減らし、より迅速な保護を実現します。
  - ハイブリッドワーカーに統一されたドメインネームシステム（DNS）ポリシーを提供します。

図 11.　　Cisco Umbrella を使用した一貫した DNS ポリシーによりすべてのブランチのインターネット通信を保護します。



- Cisco Umbrella 自動トンネルを使用してすべてのブランチのインターネットトラフィックを保護。
  - SASE ソリューションの導入
  - Threat Defense および Cisco Umbrella でトンネルを自動的に設定します。
  - ハイブリッドワーカーに統一された DNS 制御ポリシーと Web ポリシー検査を提供します。
  - インターネットパフォーマンスの向上（インターネット通信は Cisco Umbrella にルーティング）

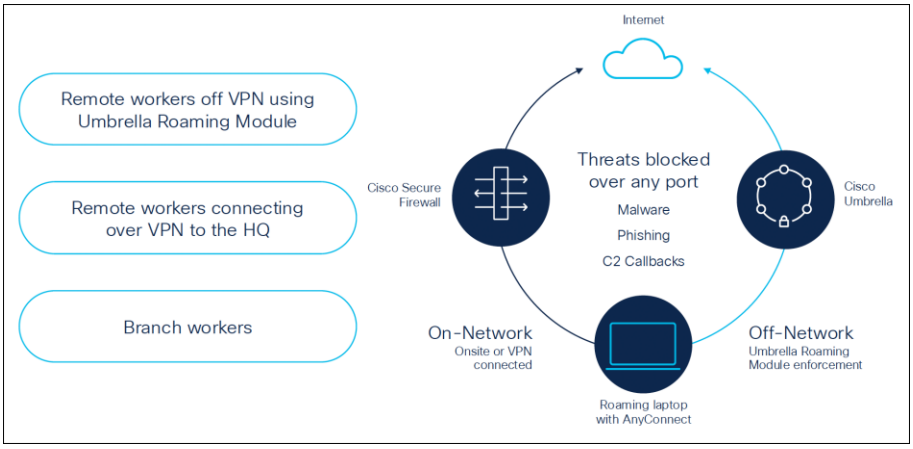
図 12.　Cisco Umbrella 自動トンネルを使用したすべてのブランチのインターネット通信の保護



共通のセキュリティポリシースタック

共通のセキュリティ ポリシー スタックは、オンプレミス、または VPN 経由で Threat Defense デバイスに接続されているなどの場所を問わず、ユーザーが一貫したセキュリティ保護を受けるように設計されています。ユーザーがリモートの場合、Cisco Umbrella はローミングモジュールを介してリモートのユーザーに DNS および Web ポリシーの検査を提供します。ブランチファイアウォールの内側にいるか、VPN 経由で接続しているユーザーには、一貫したセキュリティのために同じポリシーを適用できます。

図 13.　Cisco Umbrella を使用した共通のセキュリティ ポリシー スタック



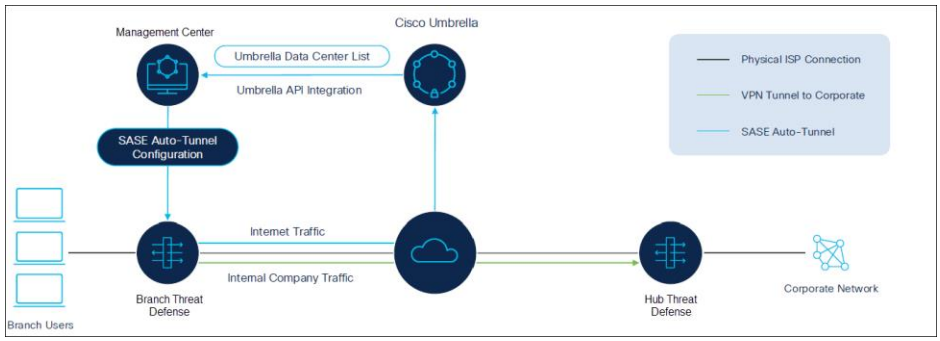
Cisco Umbrella 自動トンネルと Threat Defense を使用したセキュアなインターネット通信

Management Center によって自動トンネル設定が有効になり、Cisco Umbrella Secure Internet Gateway（SIG）とシームレスに統合できます。この統合により、ネットワークデバイスは DNS および Web 通信を Cisco Umbrella SIG に転送し、SIG トンネルを使用して検査およびフィルタリングができるようになります。

Management Center は、直感的なステップバイステップ ウィザードを使用してトンネルのセットアッププロセスを合理化し、Threat Defense デバイスと Cisco Umbrella の両方で必要な設定を削減します。Management Center は Cisco Umbrella API を使用することで Cisco Umbrella データセンターのリストを取得し、Management Center 内の Cisco Umbrella 接続設定で指定されたパラメータを使用してネットワークトンネルを設定します。

Threat Defense デバイスと Cisco Umbrella の間にネットワークトンネルを確立すると、オンプレミスユーザーとローミングユーザーの両方に DNS ポリシーと Web ポリシーが一貫して適用されます。

図 14.　Threat Defense を使用した Cisco Umbrella 自動トンネル



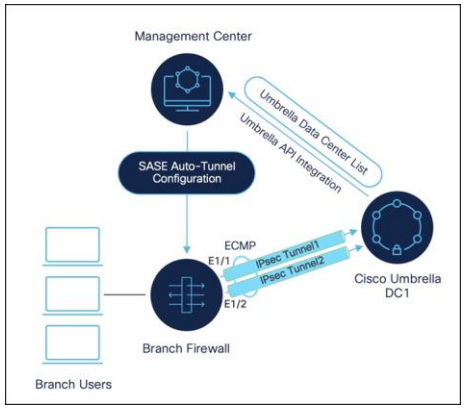
Threat Defense デバイスを使用した Cisco Umbrella 自動トンネルの高可用性

Threat Defense デバイスを使用した Cisco Umbrella 自動トンネルの高可用性を次の 2 つの方法で実現できます。

1. 高可用性はファイアウォールで実現されます。

   アクティブ/アクティブな高可用性のために、単一の Cisco Umbrella データセンターに対して最大で 8 つのアクティブトンネルを設定できます。この ECMP ベースのセットアップにより冗長性が実現され、帯域幅が増加します。

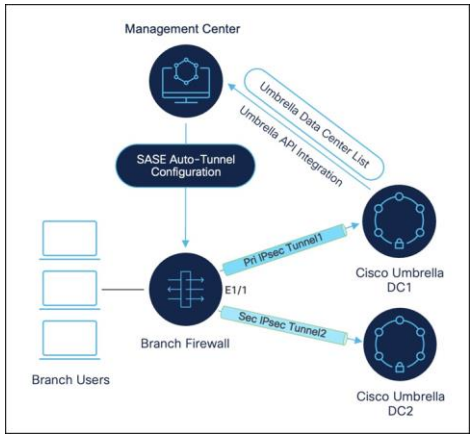
図 15.　Threat Defense デバイスを使用した高可用性



2. 異なる Cisco Umbrella データセンターを使用して高可用性を実現できます。

   アクティブ/バックアップの高可用性のために、各 Cisco Umbrella データセンターに対して最大で 8 つのアクティブトンネルと 8 つのバックアップトンネルを設定できます。このセットアップにより、Cisco Umbrella ヘッドエンド障害に対する保護が確保されます。

図 16.　　さまざまな Cisco Umbrella データセンターを使用した高可用性



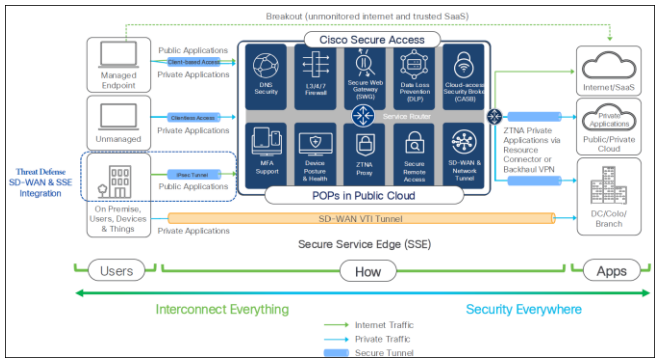
Cisco Umbrella SASE 自動トンネルの設定

Management Center での Cisco Umbrella SASE 自動トンネルのワークフロー、前提条件、設定、および検証の詳細については、「Secure Internet Traffic Using Cisco Umbrella and Threat Defense」を参照してください。

Cisco SSE ソリューション：Cisco Secure Access および Threat Defense を使用したセキュアなインターネット通信

Cisco Secure Access 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シスコの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。

図 17.　　Cisco Secure Access のアーキテクチャ



管理対象か非管理対象かにかかわらず、Cisco Secure Access は、リソースやアプリケーションへのセキュアなアクセスをユーザーと端末に提供するように設計されています。ホスティングの場所（オンプレミス、データセンター、またはプライベートクラウド）は問いません。Cisco Secure Access は、接続とセキュリティの両方を実現するインフラストラクチャとして機能します。次のような、最新のネットワークに不可欠なさまざまなセキュリティ機能が組み込まれています。

- **クライアントベースアクセス（管理対象端末）**：組織によって管理されるデバイス向けに設計されています。クライアントは端末にインストールされ、Cisco Secure Access へのセキュアで永続的な接続が確立されます。
- **クライアントレスアクセス**：クライアントのインストールを必要とせず、管理対象外デバイス（個人デバイス、パートナーアクセスなど）のセキュアなアクセスを提供します。
- **パブリックアプリケーション**：これには、一般的なインターネットアクセスや信頼できる Software-as-a-Service（SaaS）アプリケーションが含まれます。
- **プライベートアプリケーション**：オンプレミスのデータセンター、パブリックまたはプライベートクラウド、分散拠点など、さまざまな場所に存在する可能性があります。

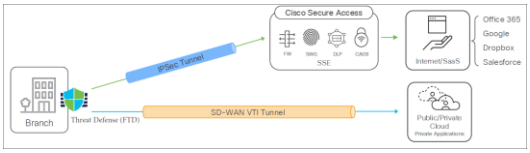
統合セキュリティサービス

- **DNS Security**：悪意のあるドメインやコマンドアンドコントロール コールバックから保護します。
- **L3/4/7 ファイアウォール**：精度の高いネットワークおよびアプリケーション層通信フィルタリングを提供し、ポリシーを適用します。
- **セキュア Web ゲートウェイ（SWG）**：Web コンテンツをフィルタ処理し、アクセプタブル ユース ポリシーを適用して、Web ベースの脅威から保護します。
- **データ損失防止（DLP）**：Web、クラウド、または端末のいずれのチャネルを経由しても、機密データが組織の管理対象から外れることを防ぎます。
- **クラウド アクセス セキュリティ ブローカ（CASB）**：セキュリティポリシーをクラウドアプリケーションに拡張し、SaaS および IaaS 環境のコンプライアンスとデータ保護を保証します。
- **デバイスポスチャと正常性**：アクセスを許可する前に、接続中のデバイスのセキュリティコンプライアンスと正常性を評価し、信頼できるデバイスのみが接続できるようにします。
- **ZTNA プロキシ**：プライベート アプリケーションをネットワークに直接公開することなく、セキュアで最も権限のないアクセスを可能にします。
- **セキュアなリモートアクセス**：リモートユーザーが企業の技術情報を使用するためのセキュアな接続を提供します。
- **パブリッククラウドでの POP**：Cisco Secure Access は、パブリッククラウド環境内に戦略的に配置されたアクセスポイント（POP）から機能し、世界中の低遅延アクセスを保証します。
- **Microsoft および Google サービスのテナント制御**：ユーザーがアクセスできる Microsoft および Google テナントを指定および管理する機能を提供し、セキュリティとコンプライアンスを強化します。

Threat Defense SD-WA ブランチのセキュア インターネット アクセス（SIA）アーキテクチャ

この例のトポロジは、Cisco Secure Access と統合された Threat Defense および SD-WAN（ソフトウェア定義型広域ネットワーク）を使用して分散拠点でのインターネットアクセスを保護するための基本的なアーキテクチャを示しています。

図 18.　　セキュアインターネットアクセスアーキテクチャ



「Threat Defense SD-WAN ブランチのセキュア インターネット アクセス（SIA）アーキテクチャ」では次の詳細を考慮してください。

- **分散拠点**：Threat Defense デバイスが展開されているユーザーのローカルネットワークを表します。
- **Threat Defense**: ブランチでセキュリティゲートウェイとして機能します。セキュア インターネットアクセス（SIA）ユースケース用の Cisco Secure Access への手動 IPSec トンネルを確立します。
- **SD-WAN VTI トンネル**：SIA 通信は、特に Threat Defense デバイスから Cisco Secure Access への手動 IPSec トンネルを使用します。
- **Cisco Secure Access**：これはシスコの Security Service Edge プラットフォームであり、クラウドにさまざまなセキュリティ機能を提供します。このアーキテクチャには以下が含まれます。
  - **FW**（ファイアウォール）：基本的なネットワークのフィルタリング
  - **SWG**（セキュア Web ゲートウェイ）：Web ベースの脅威から保護し、Web ポリシーを適用します。
  - **DLP**（データ損失防止）：機密データが組織の管理対象から外れることを防ぎます。
  - **CASB**（クラウド アクセス セキュリティ ブローカ）：セキュリティポリシーをクラウドアプリケーションに拡張します。
  - **SSE**（セキュリティサービスエッジ）：包括的なクラウド提供型セキュリティフレームワーク。
- **インターネット/SaaS リソース**：Cisco Secure Access を介して安全にアクセスされる、パブリック インターネット リソースや Office 365、Google、Dropbox、Salesforce などの Software-as-a-Service アプリケーションを表します。
- **パブリック/プライベートクラウドアプリケーション**：パブリックまたはプライベートクラウドでホストされているプライベートアプリケーションにもアクセスできることを示します。

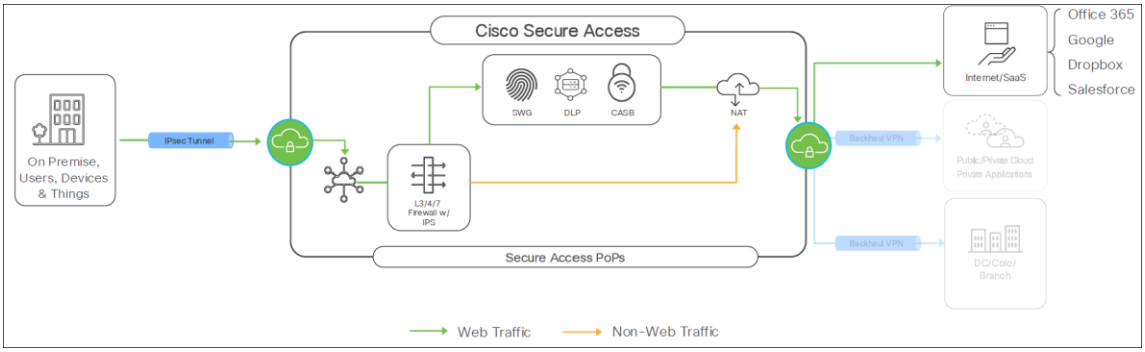
「**ブランチのセキュアなインターネットアクセスのユースケース**」では、ブランチからパブリッククラウドまたはヘッドエンドの場所に拡張される SD-WAN 仮想トンネルインターフェイス（VTI）VPN トンネルを利用します。これらの SD-WAN VTI トンネルは、他のネットワーク設定と共存するように設計されています。この IPsec トンネルの主な目的は、クラウドでホストされているかオンプレミスでホストされているかにかかわらず、ブランチから Web アプリケーションやその他のリソースへのセキュアなアクセスを提供することです。

現在、これらの IPsec トンネルは手動で設定されています。これらのトンネルの通信リダイレクトは、Cisco Umbrella で観察されるものと同様の方法、ポリシーベースルーティング（PBR）を使用して管理されます。

Threat Defense SD-WAN ブランチのセキュア インターネット アクセスの通信フロー

このトポロジは、分散拠点から Cisco Secure Access を介してインターネットまたは SaaS アプリケーションへ送信される通信に対し適用される正確なパスとセキュリティ機能の詳細を示しています。

図 19.　　SD-WAN（ソフトウェア定義型広域ネットワーク）の通信フロー



トンネルのセットアップ：

- **トンネルの設定**：これらのトンネルは、アクティブ-アクティブまたはアクティブ-バックアップのいずれかの設計で設定できます。
- **帯域幅**：ファイアウォールから Secure Access への各トンネルは最大 1Gbpsをサポートします。
- **拡張性**：1 Gbps を超える帯域幅を実現するには、ECMP（Equal-Cost Multi-Path）を使用できます。
- **サポートされるシナリオ**：このセットアップでは、重複およびアウトバウンド NAT シナリオもサポートされます。

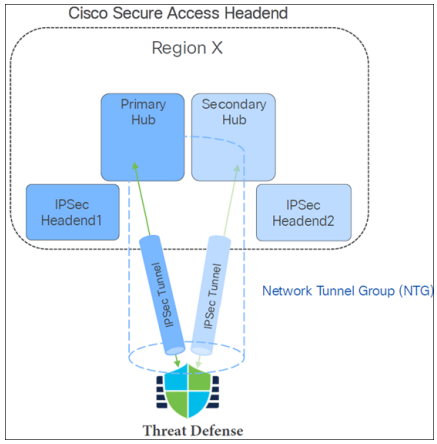
Threat Defense SD-WAN ブランチからセキュア インターネット アクセス（SIA）への通信フローの主要コンポーネントを次に示します。これには Web 通信と非 Web 通信の両方が含まれます。

- **オンプレミスのセットアップ**：オンプレミスの Cisco Secure Firewall は、Cisco Secure Access Intra への IPSec トンネルを確立します。
- **接続先**：このトンネルは、通信をインターネットまたは SaaS アプリケーションに誘導します。

Threat Defense SD-WAN ブランチのセキュア インターネット アクセスの高可用性（HA）

このセクションでは、Threat Defense SD-WAN ブランチのセキュア インターネット アクセス（SIA）展開で高可用性（HA）を実現し、コンポーネントの障害やデータセンターの障害の発生時にも継続的にセキュアなインターネットアクセスを提供する方法について説明します。

図 20.　　SD-WAN ブランチのセキュア インターネット アクセス HA



この統合における高可用性は、主に次の 2 つの冗長性によって実現されます。

1. Cisco Secure Access ヘッドエンドの冗長性

   Cisco Secure Access ヘッドエンドは、継続的なサービスを提供するために冗長性を持たせて設計されています。

   - メカニズム：ブランチの Threat Defense デバイスは、Cisco Secure Access リージョン内のプライマリハブとセカンダリハブの両方に接続するように設定されています。これは、リモートサイトが Cisco Secure Access への 2 つのトンネルを確立できるネットワーク トンネル グループ（NTG）の概念によって容易になります。プライマリハブで障害が発生した場合、セカンダリハブを介して接続が維持されます。
   - コンポーネント：
     - Cisco Secure Access Headend（リージョン X）：さまざまなリージョンに展開される Cisco Secure Access のクラウドベースのインフラストラクチャ。
     - ネットワーク トンネル グループ（NTG）：冗長性を提供する IPSec ヘッドエンドの論理グループ。
     - IPSec Headend1（プライマリハブ）：Threat Defense デバイスが IPsec トンネル用にアクティブに使用するプライマリデータセンターまたはアクセスポイント（PoP）。
     - IPSec Headend2（セカンダリハブ）：プライマリハブが使用できなくなった場合に引き継ぎ準備ができているセカンダリまたはバックアップデータセンター/PoP。
   - スイッチオーバー条件：システムは、次のシナリオでプライマリハブからセカンダリハブに自動的に切り替わります。
     - データセンター（DC）オフライン：メンテナンスまたはその他の計画された理由によりプライマリデータセンターがオフラインになっている場合。
     - データセンター（DC）障害：プライマリデータセンターの計画外の中断または障害が発生した場合。
   - 利点：この冗長性により、プライマリデータセンターの稼働状況にかかわらず、ブランチユーザーはインターネットおよびプライベートリソースへの接続を維持できます。

2. Threat Defense（ファイアウォール）側の冗長性

Threat Defense（ファイアウォール）側にも冗長性が導入されているため、レジリエンスの高いトンネル接続が実現されます。

- トンネル設定：Threat Defense では、次の 2 タイプのトンネル冗長性を設定できます。
  - アクティブ/バックアップトンネル：一方のトンネルはアクティブで、すべてのアウトバウンドおよびインバウンド通信に使用され、もう一方のトンネルはスタンバイとして機能します。
  - アクティブ/アクティブトンネル：複数のトンネルが同時にアクティブになり、アウトバウンド通信とインバウンド通信の両方に等コストマルチパス（ECMP）を利用します。この設定では、最大 16 個のトンネル（ECMP ゾーンでは最大で 8 個のインターフェイスがサポートされるため、アクティブ × 8 + バックアップ × 8）がサポートされます。
- スイッチオーバーメカニズム：FTD は、次の方法を使用してトンネル間の通信を切り替えます。
- スタティックルーティングの IKE デッドピア検出（DPD）：スタティックルーティングが使用されている場合、IKE DPD は IPsec トンネルピアの稼働状況をモニターします。プライマリピアが応答しなくなると（デッドピア）と、FTD はトンネルを自動的にセカンダリハブに切り替えます。
- BGP（ボーダー ゲートウェイ プロトコル）タイマー：ダイナミックルーティングの場合、BGP は到達可能性情報のアドバタイズに使用されます。プライマリパス上の BGP ピアリングが停止すると、Threat Defense は次の BGP ペアにピボットし、セカンダリトンネルを介して Cisco Secure Access に接続するために通信をルーティングします。

ブランチ ネットワーク セキュリティのための Cisco Secure Access と Threat Defense デバイスの統合

Secure Access と Threat Defense デバイスのワークフロー、前提条件、設定、および検証の詳細については、「Secure Branch Using Cisco Secure Access and Threat Defense」を参照してください。

まとめ

この包括的なガイドでは、Cisco Secure Firewall Threat Defense および Management Center を利用して、可用性が高くセキュアな SD-WAN ネットワークを構築する方法を説明します。合理化されたデバイスの導入準備およびウィザード駆動の SD-WAN トポロジの作成から、高度なルーティング機能の再配布およびポリシーベースルーティング（PBR）を使用したインテリジェントなダイレクト インターネット アクセス（DIA）まで、このドキュメントにはエンドツーエンドの展開に関する情報が含まれます。Cisco Umbrella と Cisco Secure Access for SASE/SSE の戦略的統合に重点を置き、堅牢なクラウドネイティブのセキュリティ、アプリケーションとアイデンティティに基づく通信ステアリング、および最新の保護されたブランチ環境のための高可用性について説明しています。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。