検証済みプロファイル：IT 対応サービス業界（SD-Access）

2026 年 4 月 27 日

ソリューションの概要

情報技術対応サービス（ITES）組織は、カスタマーサポート、テクニカルヘルプデスク、ソフトウェア開発、データ処理など、多数の IT サービスを提供する企業です。ITES 組織はテクノロジーを活用し、多くの場合インターネットなどのデジタルネットワークを介してこれらのサービスを提供します。ITES 企業はグローバルなアウトソーシング業界に不可欠な存在であり、世界中のビジネスにコスト効率の高いソリューションを提供しています。これらの企業は高品質のサービスを提供できることで知られており、先進国では多くの場合、自社運用に比べてコストも低廉です。イノベーションを推進し、効率を向上させ、ビジネスにおいてコアコンピテンシーに注力する上で、これらの組織は重要な役割を果たします。

このシスコ検証済みプロファイルのドキュメントでは、ITES プロファイルのネットワーク展開におけるガイドラインを提供し、その課題、ソリューション、展開オプション、運用管理、および移行に焦点を当てています。検証済みのエンドツーエンドのユースケース、拡張性に関する洞察、ハードウェアとソフトウェアの推奨事項が記載されており、ネットワーク展開と組織的展開のプロセスにおいて最適な判断を下せるように支援します。さらにこのドキュメントでは、企業ネットワークに関連する設計および導入ガイドを参照することで、Cisco ソフトウェア定義型アクセス（SD-Access）の一般的な導入に関する貴重な洞察を提供します。

スコープ

このガイドは、ITES ネットワークが直面する課題、一般的なユースケース、および Cisco SD-Access によってそれらに対処する方法を理解するためのロードマップの役割を果たします。このガイドでは詳細な設定手順は説明しませんが、ITES ネットワーク戦略に関する貴重な洞察が得られます。

従来のネットワークと Cisco SD-Access の比較

このセクションでは、従来のネットワークと Cisco SD-Access の主な違いについて概説します。

従来型のネットワーク：

- 従来のネットワークでは、ネットワークデバイスを手動で設定する必要があります。
- 多くの場合、セグメンテーション用に別個のオーバーレイネットワークが必要です。
- 通常、セキュリティポリシーはネットワーク境界で適用されます。
- ネットワークの拡張は複雑で時間がかかる可能性があります。
- 多くの場合、障害対応はリアクティブであり、手動の介入が必要です。
- ネットワークトラフィックとアプリケーションのパフォーマンスに対する可視性は限られています。

Cisco SD-Access：

- SD-Access は、ポリシーベースの自動化によってネットワークのプロビジョニングと管理を自動化します。
- 接続とセグメンテーションの両方に単一のアンダーレイネットワークを使用しながら、Virtual Extensible LAN（VXLAN）オーバーレイでセキュリティグループタグ（SGT）の情報を伝送することで、ネットワーク設計をシンプル化します。
- セキュリティポリシーは、ユーザーとデバイスのアイデンティティに基づいて動的に適用されます。
- SD-Access は、自動化と一元化された制御により簡単に拡張できます。
- 障害対応は、ネットワーク全体の可視性と分析を使用してプロアクティブに行われます。
- SD-Access は、ネットワーク トラフィックとアプリケーションのパフォーマンスに関する詳細な洞察を提供します。

要約すると、Cisco SD-Access は、一元化された管理、向上した拡張性、および強化されたセキュリティ機能により、従来のネットワークに比べて合理化された柔軟なアプローチを提供します。

従来のネットワークの課題

現在では、手動での設定と統一されていない各種ツールにより、ネットワークの管理には多くの課題があります。手動操作は時間がかかり、ミスを伴うことがよくあります。環境が常に変化するため、問題の解決が追いつきません。ユーザーが増加し、さまざまなデバイスタイプが増加すると、ネットワーク全体で一貫したユーザーポリシーを設定して維持することがますます複雑になります。

- ネットワーク展開の課題：

  単一のネットワークスイッチのセットアップまたは展開には、スケジュール要件があり、さまざまなインフラストラクチャ グループを使用する必要があるため、数時間かかることがあります。場合によっては、スイッチの一括展開には数週間かかることがあります。

- ネットワークセキュリティの課題：

  セキュリティは最新ネットワークを管理するための不可欠な構成要素です。組織はリソースを保護し、リアルタイムのニーズに応じて効率的に変更を加える必要があります。従来のネットワークでは、最適なポリシーおよびセキュリティコンプライアンスを確保するために、VLAN、アクセス制御リスト（ACL）、および IP アドレスを追跡するのは困難です。

- ワイヤレスおよび有線ネットワークの課題：

  異なるシステムが組織のそれぞれの部門で管理されるため、多くの場合にまったく異なるネットワークが存在することがよくあります。通常、主要な IT ネットワークは、建物の管理システム、セキュリティシステム、およびその他の稼働システムとは別個に運用されています。これにより、調達するネットワークハードウェアが重複したり、管理プラクティスに一貫性がなくなったりします。

- ネットワーク運用における課題：

  IT チームは、旧式の変更管理ツール、生産性の維持、および問題解決の遅延にしばしば苦労します。

Cisco SD-Access の利点：

Cisco SD-Access は、急速なデジタル化の要求に対処するように設計されています。Cisco SD-Access アーキテクチャの中核の考え方は、ポリシーベースの自動化を中心にするもので、有線接続とワイヤレス接続でユーザーとデバイスのセキュアなセグメンテーションを実現します。

自動化とシンプルさにより生産性が大幅に向上します。これにより、IT 担当者が迅速にイノベーションを進め、デジタル トランスフォーメーションで業界をリードできるようになり、したがって、運用の有効性が向上します。伝送媒体（有線またはワイヤレス）に関係なく、ビジネスポリシーと連携した一貫したセグメンテーション フレームワークは、コアの有効性のために重要です。

Cisco SD-Access には、次に挙げる技術的な利点があります。

- 運用のシンプル化：

  インフラストラクチャ全体を管理するための単一の直感的なインターフェイスにより、ネットワーク運用を簡素化し、複雑さと運用のオーバーヘッドを削減します。

- 自動化：

  設定、プロビジョニング、管理などの日常的なネットワーク操作を自動化します。これにより、人的エラーのリスクが軽減され、効率が向上します。Catalyst Center は展開を合理化することで、コマンド ライン インターフェイス（CLI）でのやりとりの必要性を最小限に抑えます。

- 俊敏性：

  手動による構成手順を最小限に抑えることで、ネットワーク運用がよりアジャイルになり、ビジネス要件に沿ったものになります。

- セキュリティ

  仮想ネットワーク（VN）と SGT を通じ、強化されたセキュリティとセグメンテーションを提供します。SD-Access は、VN によるマクロセグメンテーションと SGT によるマイクロセグメンテーションによって、複雑な企業ネットワークを保護および管理するための強力なフレームワークを提供します。

- 有線/ワイヤレスネットワークに共通するポリシー：

  セグメンテーション、可視性、およびポリシーを有線ネットワークからワイヤレスネットワークに拡張します。分散型ワイヤレス終端装置は、管理と障害対応を一元化しながら、ネットワークのスループットを高めます。

- ビジネス分析のサポート:

  分析とテレメトリ情報を単一のプラットフォームに集約します。これは、ビジネス上の決定を支援し、成長や多角化の計画を容易にします。

IT 対応サービスネットワークの概要：

ITES ネットワークの課題やユースケースに合わせて、Cisco SD-Access ファブリックの新しいグリーンフィールド展開を構築するためのガイダンスと推奨事項については、SD-Access ファブリックコンポーネントの詳細を説明する今後のセクションで取り上げます。ITES セクター固有の要件と課題に対処する際に、Cisco SD-Access ソリューションが提供する利点をご確認ください。

従来のネットワークは、Cisco Prime Infrastructure または Catalyst Center を使用して管理できます。Catalyst Center は、従来のネットワークと SD-Access 環境の両方において高度な自動化、モニタリング、およびテレメトリ機能を提供します。現在 Cisco Prime Infrastructure でネットワークを管理しており、Catalyst Center への移行を計画している場合は、『Cisco Prime Infrastructure から Cisco Catalyst Center への移行ガイド』を参照してください。

既存の Cisco Catalyst レガシーネットワークを Cisco SD-Access ファブリックに移行するには、「Cisco SD-Access への移行」を参照してください。その中で、有線端末とワイヤレス端末の両方について既存のネットワークを移行するためのオプションを説明しています。

SD-Access のコンポーネント

Cisco Catalyst Center

Catalyst Center（旧 Cisco DNA Center）は、ネットワークの運用と管理を簡素化するために設計された、集中型のネットワーク管理およびオーケストレーション プラットフォームです。スイッチ、ルータ、ワイヤレスアクセスポイント（AP）などのネットワーク インフラストラクチャを管理およびモニターするための単一のダッシュボードを提供します。

Catalyst Center を使用すると、ネットワーク管理者は次のようなタスクを実行できます。

- ネットワークプロビジョニングの自動化：

  自動化されたワークフローを使用してネットワークデバイスやサービスを簡単に展開でき、設定に必要な時間と労力を削減できます。

- ネットワークの正常性のモニタリング：

  デバイスステータス、トラフィックパターン、評価指標など、ネットワーク全体を可視化し、問題を迅速に特定して解決します。

- セキュリティポリシーの導入：

  ネットワーク全体でセキュリティポリシーを定義して適用することで、コンプライアンスを維持し、脅威から保護します。

- ソフトウェア アップデートの管理：

  デバイスのソフトウェアとファームウェアを更新するプロセスを簡素化し、最新の機能とセキュリティパッチを適用してネットワークデバイスを最新の状態に必ず保ちます。

- ネットワークの問題のトラブルシュート：

  組み込みのツールと分析機能を使用して、ネットワークの問題を迅速に診断して解決し、ダウンタイムと中断を最小限に抑えます。

全体として、Catalyst Center は、組織がネットワーク業務を合理化し、効率を高め、セキュリティを強化するのに役立ち、最新のネットワーク インフラストラクチャを管理するのに不可欠なツールになっています。Catalyst Center プラットフォームは、物理アプライアンスと仮想アプライアンスの両方として、さまざまなフォームファクタで利用できます。詳細については、次のリソースを参照してください。

- 『Cisco Catalyst Center データシート』（サポートプラットフォームとスケール別）
- Cisco Catalyst Center Installation Guide [英語]

Cisco Identity Service Engine

Cisco Identity Services Engine（ISE）は、セキュリティ ポリシーの管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティ コンプライアンスを自動化し、シンプルにします。Cisco ISE は、ネットワークリソースへのセキュアなアクセスを提供し、セキュリティポリシーを適用するとともに、ネットワークアクセスを包括的に可視化します。

Cisco ISE の主要機能は、以下のとおりです。

- ポリシーベースのアクセス制御：

  ユーザーロール、デバイスタイプ、およびその他のコンテキスト情報に基づいてポリシーを定義し、適用します。

- 認証および承認：

  さまざまな認証方式（802.1X、MAB、Web 認証など）をサポートしており、状況の変化に応じてダイナミックな承認が可能になります。

- エンドポイント コンプライアンス：

  エンドポイントのセキュリティポリシーへの準拠を評価し、必要に応じて是正アクションを実行します。

- ゲストアクセス：

  カスタマイズ可能なゲストポータルとスポンサー承認ワークフローを使用して、ネットワークへのセキュアなゲストアクセスを提供します。

- 個人所有デバイスの持ち込み（BYOD）サポート：

  デバイスのオンボーディングとポリシーの適用により、セキュアな BYOD の取り組みを実現します。

- 統合とエコシステム：

  API およびパートナーエコシステムを介して、他のセキュリティおよびネットワークテクノロジーと統合します。

- 可視性とレポート：

  包括的なレポートおよび分析によって、ネットワークアクセスとセキュリティポスチャに関する洞察を得ることができます。

Cisco ISE は、シスコのセキュリティおよびネットワーク アクセス コントロール ポートフォリオの重要なコンポーネントであり、セキュリティおよびアクセス制御のニーズを満たす一元化されたスケーラブルなソリューションを組織に提供します。ISE では、スタンドアロンおよび分散型の両方の導入モデルがサポートされています。複数の分散ノードをまとめて展開して、フェールオーバーのレジリエンスと拡張性を強化できます。SD-Access の単一サイト展開については、基本的な 2 ノード ISE 展開を使用し、各 ISE ノードがすべてのサービス（または機能ないしロール）を実行することで冗長化を実現するようお勧めします。

詳細については、次のマニュアルを参照してください。

- Cisco Identity Services Engine 管理者ガイド
- Cisco Identity Services Engine パフォーマンスおよび拡張性ガイド

Cisco Catalyst 9000 シリーズ スイッチ

Cisco Catalyst 9000 シリーズ スイッチは、より柔軟で拡張性の高い設計オプションを提供します。さまざまなファブリックロールでサポートされているスイッチは、ネットワーク内のユーザーとエンドポイントに安全で高速で信頼性の高い接続を提供します。

データシートについては、Cisco Catalyst 9000 シリーズを参照してください。

Cisco Catalyst ワイヤレス LAN コントローラおよびアクセスポイント

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラおよびアクセスポイント（AP）は、オンプレミスとクラウドの両方でワイヤレスクライアントのシームレスなネットワーク管理と展開を可能にします。

Catalyst 9800 および Catalyst 9100 デバイスのデータシートについては、次を参照してください。

- Cisco Catalyst 9800 シリーズ
- Cisco Catalyst 9100 シリーズ
- シスコ アクセスポイントおよびワイヤレスコントローラ セレクタ

Cisco SD-Access ファブリック

Cisco SD-Access ファブリックは、ソフトウェア定義型ネットワーク（SDN）の概念を使用して、ネットワークのプロビジョニング、セグメンテーション、およびポリシーの適用を自動化するネットワークアーキテクチャです。最新のデジタルワークプレイスでのネットワーク運用をシンプル化し、セキュリティを強化して、ユーザー体験を向上させることを目的としています。

Cisco SD-Access ファブリックの主なコンポーネントと機能は次のとおりです。

- ネットワークのセグメント化：

  ユーザーとデバイスのアイデンティティに基づいてネットワークを仮想セグメントに分割し、アクセスポリシーとセキュリティポリシーを詳細に制御できます。

- ポリシー管理の一元化：

  ポリシーは一元的に定義され、ネットワーク全体で一貫して適用されるため、設定不良やポリシーの競合のリスクが軽減されます。

- 自動化：

  ネットワークのプロビジョニング、設定、および管理のタスクを自動化することで、手作業によるエラーを削減し、業務効率を向上させます。

- ISE：

  認証および承認サービスを提供し、承認されたユーザーとデバイスのみがネットワークにアクセスできるようにします。

- Catalyst Center：

  SD-Access の管理およびオーケストレーション プラットフォームとして機能し、ネットワーク管理と障害対応のための一括管理機能を提供します。

- 拡張性：

  大規模な展開をサポートするため、組織はニーズの拡大に応じてネットワークを簡単に拡張できます。

- 強化されたセキュリティ：

  ネットワークを動的にセグメント化し、ユーザーとデバイスのアイデンティティに基づいてセキュリティポリシーを適用することで、ネットワークセキュリティを向上させます。

全体として、Cisco SD-Access ファブリックはネットワーク管理を簡素化し、セキュリティを向上させ、拡張性を強化することを目的としており、ネットワーク インフラストラクチャの最新化を目指す組織にとって魅力的なオプションになります。

ファブリックアーキテクチャの概要

Cisco SD-Access ファブリックアーキテクチャは、ネットワーク運用を簡素化し、セキュリティを強化して、ユーザー体験を向上させるように設計されています。これは SDN の原理に基づいており、次の目標を達成するためにさまざまなコンポーネントが組み込まれています。

- アンダーレイ ネットワーク：

  デバイス間の基本的な接続を実現する物理ネットワーク インフラストラクチャ。通常、スイッチ、ルータ、ケーブルで構成されています。

- オーバーレイネットワーク：

  デバイス間の仮想的な接続を実現する、アンダーレイネットワークの上に構築された論理ネットワーク。物理的な再構成なしで、ネットワークのセグメンテーションとポリシーの適用が可能になります。

- コントロールプレーン：

  ルーティング、転送、ポリシーの適用など、ネットワークの全体的な運用を管理します。通常、Catalyst Center などの集中型コントローラを使用して実装されます。

- データプレーン：

  ネットワーク内のデータパケットの転送を実際に処理します。スイッチやルータなどのネットワークデバイスに実装され、コントロールプレーンによる指示に基づいて動作します。

- ポリシープレーン：

  アクセス制御やセグメンテーションなどのネットワークポリシーを定義して適用します。これにより、ネットワークリソースが効率的かつ安全に使用されます。

- 管理プレーン：

  ネットワークを管理およびモニタリングするためのツールとインターフェイスを提供します。設定管理、モニタリング、障害対応などの機能が含まれます。

全体として、Cisco SD-Access ファブリックアーキテクチャは、デジタルビジネスの進化するニーズに対応する拡張性、セキュリティ、および自動化機能を備えており、ネットワーク インフラストラクチャを最新化するための包括的なソリューションを提供します。

ネットワークアーキテクチャ

キャンパスにおける SD-Access アーキテクチャは、ファブリック技術によってサポートされており、物理ネットワーク（アンダーレイネットワーク）上で動作する VN（オーバーレイネットワーク）を使用して、各デバイスを接続する代替トポロジを構築できます。SD-Access では、ユーザー定義のオーバーレイネットワークは、ルーティングテーブルを分離できる仮想ルーティングおよび転送（VRF）インスタンスとしてプロビジョニングされます。

ファブリックロール

ファブリックロールは、物理ハードウェアで実行される SD-Access ソフトウェア構造です。これらのソフトウェア構造は、モジュール性と柔軟性を考慮して設計されています。たとえば、デバイスは単一のロールまたは複数のロールを実行できます。基盤となるネットワークアーキテクチャに合わせて SD-Access ファブリックロールをプロビジョニングする場合は注意が必要であり、必ず分散機能アプローチを使用します。さまざまなデバイス間でロールを分離することで、最高レベルの可用性、レジリエンス、拡張性が得られ、予測不能の事態になりません。

SD-Access ファブリックには次のロールが含まれます。

- コントロールプレーンノード
- ボーダーノード
- エッジノード
- 中間ノード
- ファブリック ワイヤレスコントローラ
- ファブリックモード AP
- ファブリックインアボックス
- 拡張ノード

コントロールプレーンノード

SD-Access ファブリックのコントロールプレーンノードは、LISP マップサーバー機能とマップリゾルバ機能を単一ノードに結合したものです。ファブリックサイト内のすべてのエンドポイントを追跡するデータベースを維持し、それらをファブリックノードにマッピングします。この設計では、エンドポイントの IP または MAC アドレスが物理的な場所（最も近いルータ）から分離されているため、効率的なネットワーク運用が保証されます。

コントロールプレーンノードの主な機能：

- ホスト トラッキング データベース（HTDB）：

  EID から RLOC へのバインディングの中央リポジトリとして機能します。このバインディングでは、RLOC はファブリックノードのループバック 0 IP アドレスです。エンドポイント登録を保存している従来の LISP サイトと同様に機能します。

- エンドポイント識別子（EID）：

  SD-Access ネットワークで MAC、IPv4、または IPv6 アドレスを使用してエンドポイントデバイスを識別します。

- マップサーバー：

  エンドポイント登録を受信し、対応する RLOC に関連付け、それに応じて HTDB を更新します。

- マップリゾルバ：

ファブリックデバイスからのクエリに応答し、EID から RLOC へのマッピングを HTDB から提供します。これにより、デバイスはトラフィックを転送するのに適切なファブリックノードを決定できます。

ボーダーノード

SD-Access ファブリック ボーダー ノードは、ファブリックサイトと外部ネットワーク間のゲートウェイとして機能し、ネットワーク仮想化のインターワーキングとファブリックを超える SGT の伝播を処理します。

ボーダーノードの主な機能：

- EID サブネットアドバタイズメント：

  ボーダー ゲートウェイ プロトコル（BGP）を使用してファブリック外に端末のプレフィックスをアドバタイズし、リターン通信が正しく転送されるようにします。

- ファブリックサイト イグジットポイント：

  LISP PxTR（プロキシトンネルルータ）を使用するエッジノードのデフォルトゲートウェイとして機能します。内部ボーダーノードは、既知のサブネットをコントロールプレーンノードに登録できます。

- ネットワーク仮想化拡張機能：

  VRF-Lite 対応および VRF 対応ルーティングプロトコルを使用して、ファブリックを超えてセグメンテーションを拡張します。

- ポリシーのマッピング：

  SGT 交換プロトコル（SXP）またはシスコメタデータのインラインタギングを通じて、ファブリック外の SGT 情報を維持します。

- VXLAN カプセル化とカプセル化解除：

  外部トラフィックをファブリックの VXLAN 向けに変換し、発信トラフィックの VXLAN 対応を削除します。このようにファブリックと非ファブリックのネットワーク間のブリッジとして機能します。

エッジノード

SD-Access ファブリックエッジノードは、従来のキャンパス LAN でアクセス層スイッチと同様に機能します。これらは、LISP において入力および出力トンネルルータ（xTR）に基づいて動作し、レイヤ 3 ルーテッドアクセス設計を使用して展開する必要があります。これらのエッジノードは、次に挙げる複数の重要な機能を実行します。

- エンドポイントの登録：

  各エッジノードは、すべてのコントロールプレーンノードとの LISP コントロールプレーンセッションを維持します。エンドポイントが検出されると、そのエンドポイントは EID テーブルと呼ばれるローカルデータベースに追加されます。エッジノードは、LISP マップ登録メッセージを送信して、コントロールプレーンの HTDB（ホストトラッキングデータベース）を更新します。

- エニーキャストレイヤ 3 ゲートウェイ：

  同じ EID サブネットを共有するすべてのエッジノードは、シームレスなモビリティと最適な転送を実現するために、共通の IP および MAC アドレスを使用します。エニーキャストゲートウェイは、ファブリック内のすべてのエッジノードで統一された、MAC アドレスを持つスイッチ仮想インターフェイス（SVI）として実装されます。

- レイヤ 2 ブリッジング：

  エッジノードは、同じ VLAN にあるエンドポイントのレイヤ 2 トラフィックを処理します。これらは、パケットをブリッジング/ルーティングするかどうかを決定し、VXLAN レイヤ 2 VNI（VLAN に相当）を使用し

てトラフィックを正しい宛先にブリッジングします。トラフィックがファブリックを出る必要がある場合は、レイヤ 2 ボーダーノードが使用されます。

- ユーザーと VN のマッピング：

  エンドポイントは、SVI および VRF にリンクされた VLAN に関連付けることで、VN に割り当てられます。このマッピングにより、コントロールプレーンレベルでも、レイヤ 2 およびレイヤ 3 LISP VNI の両方でファブリックを確実にセグメンテーションできます。

- AAA 認証：

  エッジノードは、802.1X 認証を使用してエンドポイントを VLAN に静的または動的に割り当てることができます。ネットワーク アクセス デバイス（NAD）として機能し、認証情報を収集し、認証サーバーに送信して、アクセスポリシーを適用します。

- VXLAN カプセル化とカプセル化解除：

  エッジノードがエンドポイントからのトラフィックを（直接接続、拡張ノード経由、または AP 経由で）受信すると、そのトラフィックを VXLAN でカプセル化して、ファブリック全体に転送します。宛先に応じて、トラフィックは別のエッジノードまたはボーダーノードに送信されます。カプセル化されたトラフィックがエッジノードに到達すると、カプセル化が解除されてエンドポイントに配信されます。このメカニズムにより、エンドポイントモビリティが実現し、デバイスをその IP アドレスを変更せずにエッジノード間を移動できるようになります。

中間ノード

中間ノードは、ボーダーノードとエッジノード間の接続などの、ファブリックロールで動作しているデバイス間の相互接続に使用されるレイヤ 3 ネットワークの一部です。これらの相互接続は、デバイスのグローバルルーティングテーブルに設定立され、総称して「アンダーレイネットワーク」と呼ばれます。たとえば、3 階層キャンパス展開でコアスイッチをボーダーノードとして、アクセススイッチをエッジノードとしてプロビジョニングする場合、ディストリビューションスイッチが中間ノードとして機能します。

中間ノードには、VXLAN のカプセル化、カプセル化解除、LISP コントロールプレーン メッセージング、または SGT の認識は必要ありません。これらのノードの主な機能は、IP 到達可能性と物理接続を提供しつつ、ファブリック VXLAN 情報を使用してカプセル化されたより大きなサイズの IP パケットに対応するための、拡大された MTU をサポートすることです。基本的に中間ノードは、ファブリックロールで動作しているデバイス間で IP トラフィックをルーティングおよび転送します。

ファブリック ワイヤレスコントローラ

ファブリック ワイヤレス コントローラと非ファブリック ワイヤレス コントローラは、AP イメージと設定管理、クライアントセッション管理、モビリティサービスに対応しています。ファブリック ワイヤレス コントローラは、ワイヤレスクライアントジョインイベント中にワイヤレスクライアントの MAC アドレスをファブリックコントロールプレーンの HTDB に登録したり、クライアントローミングイベント中に RLOC 関連を HTDB で更新するファブリックエッジノードを提供したりすることで、ファブリック統合のための追加サービスを提供します。ワイヤレスコントローラとのファブリックの統合は、SSID ごとに行われます。ファブリック対応 SSID 通信は、VXLAN カプセル化を使用して AP によってファブリックエッジノードにトンネリングされます。一方、中央スイッチ SSID 通信は、Control And Provisioning of Wireless Access Points（CAPWAP）プロトコルを使用して、AP によってワイヤレスコントローラにトンネリングされます。したがって、ワイヤレスコントローラは、ハイブリッドモードまたは混合モードで動作できます。ここで一部の SSID はファブリック対応ですが、他の SSID は一元的にスイッチングされます。

- 従来のデータ処理と SD-Access でのデータ処理：

  従来の Cisco Unified Wireless Network（UWN）または非ファブリック展開では、制御通信とデータ通信の両方が CAPWAP を使用してワイヤレスコントローラにトンネリングされます。CAPWAP コントロールプ

レーンの観点では、AP 管理トラフィックは一般に軽量ですが、クライアントデータトラフィックはより大きな帯域幅を消費します。ワイヤレス標準において、ワイヤレスクライアントのデータレートがますます大きくなりました。その結果、より多くのクライアントデータがワイヤレスコントローラにトンネリングされます。クライアントトラフィックの増加に対応するには、複数の広帯域幅インターフェイスを備えたより大きなワイヤレスコントローラが必要です。非ファブリックワイヤレス展開の、有線トラフィックとワイヤレストラフィックでは、ネットワーク内の適用ポイントが異なります。ワイヤレスコントローラは、ワイヤレストラフィックを有線ネットワークにブリッジングする際に、QoS とセキュリティに対処します。有線トラフィックの場合、適用はファーストホップ アクセス レイヤ スイッチで行われます。このパラダイムは、SD-Access Wireless では完全に変わります。SD-Access ワイヤレスでは、ワイヤレスコントローラと AP 間の CAPWAP トンネルは制御通信にのみ使用されます。ワイヤレス エンドポイントからのデータトラフィックはファーストホップ ファブリック エッジ ノードにトンネリングされ、有線トラフィックと同じようにセキュリティとポリシーを適用できます。

- ネットワーク接続とワイヤレスコントローラの配置：

  通常、ファブリック ワイヤレス コントローラは、ファブリック外部とファブリック境界にあるディストリビューションブロックまたはデータセンターネットワークを介して共有サービスネットワークに、グローバルルーティングテーブルに存在するワイヤレスコントローラの管理 IP アドレスで接続します。ワイヤレス AP がワイヤレスコントローラ管理用の CAPWAP トンネルを確立するには、AP が、外部デバイスにアクセスできる VN 内に存在する必要があります。つまり、AP がグローバルルーティングテーブルに展開され、ワイヤレスコントローラの管理サブネットまたは特定のプレフィックスがファブリックサイト内のグローバルルーティングテーブル （GRT）に存在する必要があるということです。SD-Access ソリューションでは、Cisco Catalyst Center は、グローバル ルーティング テーブルにマッピングされる INFRA_VN というオーバーレイ VN 内に配置するようにワイヤレス AP を設定します。このセットアップにより、ワイヤレスコントローラと AP 間の接続を確立するためのルートリークまたはフュージョンルーティング（ルーティング情報を選択的に共有するマルチ VRF デバイス）の必要がなくなります。各ファブリックサイトには、そのサイトに固有のワイヤレスコントローラが必要です。ほとんどの展開では、ローカルモード AP の遅延要件により、WAN 全体ではなく、ローカルファブリックサイト自体の内部にワイヤレスコントローラが配置されます。

- 遅延要件と展開の考慮事項：

  ファブリック AP はローカルモードで動作するため、AP とワイヤレスコントローラ間のラウンドトリップ時間（RTT）が 20 ミリ秒以下である必要があります。これは、通常、ワイヤレスコントローラが AP と同じ物理サイトに展開されることを意味します。ただし、この遅延要件が物理サイト間で専用のダーク ファイバまたは他の非常に低遅延な回線を介して満たされ、ワイヤレスコントローラが中央集中型データセンターなどの物理的に別な場所に展開される場合、ワイヤレスコントローラと AP は物理的に異なる場所に配置できます。ファブリック AP がファブリック ワイヤレス コントローラとは別に配置されるこの展開タイプは、一般的に都市エリアネットワークや SD-Access for Distributed Campus 環境で使用されます。SD-Access ネットワークのワイヤレスコントローラから WAN またはその他の高遅延回線を介して AP を展開することはできません。パフォーマンスにとって、これらのデバイス間の最大 RTT を 20 ミリ秒に維持することは重要です。

ファブリックモード AP

ファブリックモード AP は、1 つ以上のファブリック対応 SSID が設定されているファブリック ワイヤレスコントローラに関連付けられた Cisco Wi-Fi 7（802.11be）、Wi-Fi 6（802.11ax）および 802.11ac Wave 2 の AP です。これらのファブリックモード AP は、Application Visibility and Control（AVC）、Quality of Service（QoS）、およびその他のワイヤレスポリシーの適用など、従来の AP がサポートするのと同じワイヤレスメディアサービスを引き続きサポートします。ファブリック AP は、ファブリック ワイヤレス コントローラへの CAPWAP コントロール プレーン トンネルを確立し、ローカルモード AP として参加します。ファブリックサイト内のファブリック エッジ ノードまたは拡張ノードスイッチに直接接続する必要があります。データプレーンについては、ファブリック AP はファーストホップのファブリック エッジ スイッチへの VXLAN トンネルを確立し、ここでワイヤレス クライアント トラフィックが終端処理されて有線ネットワークに送られます。

ファブリック AP は特殊な有線ホストと見なされます。エッジノードは、Cisco Discovery Protocol を使用して AP を有線ホストとして認識し、特定のポート設定を適用して、AP を INFRA_VN と呼ばれる固有のオーバーレイネットワークに割り当てます。有線ホストとして、AP には専用 EID スペースがあり、コントロール プレーン ノードに登録されます。この EID スペースは、図 14 に示すように、Cisco Catalyst Center UI で事前定義された INFRA_VN オーバーレイネットワークに関連付けられています。これは、ファブリックサイト内のすべてのファブリック AP に共通の EID スペース（プレフィックススペース）および VN です。このオーバーレイ VN への割り当てにより、単一のサブネットを使用して、ファブリック サイト内で AP インフラストラクチャに対応できるため、管理がシンプルになります。

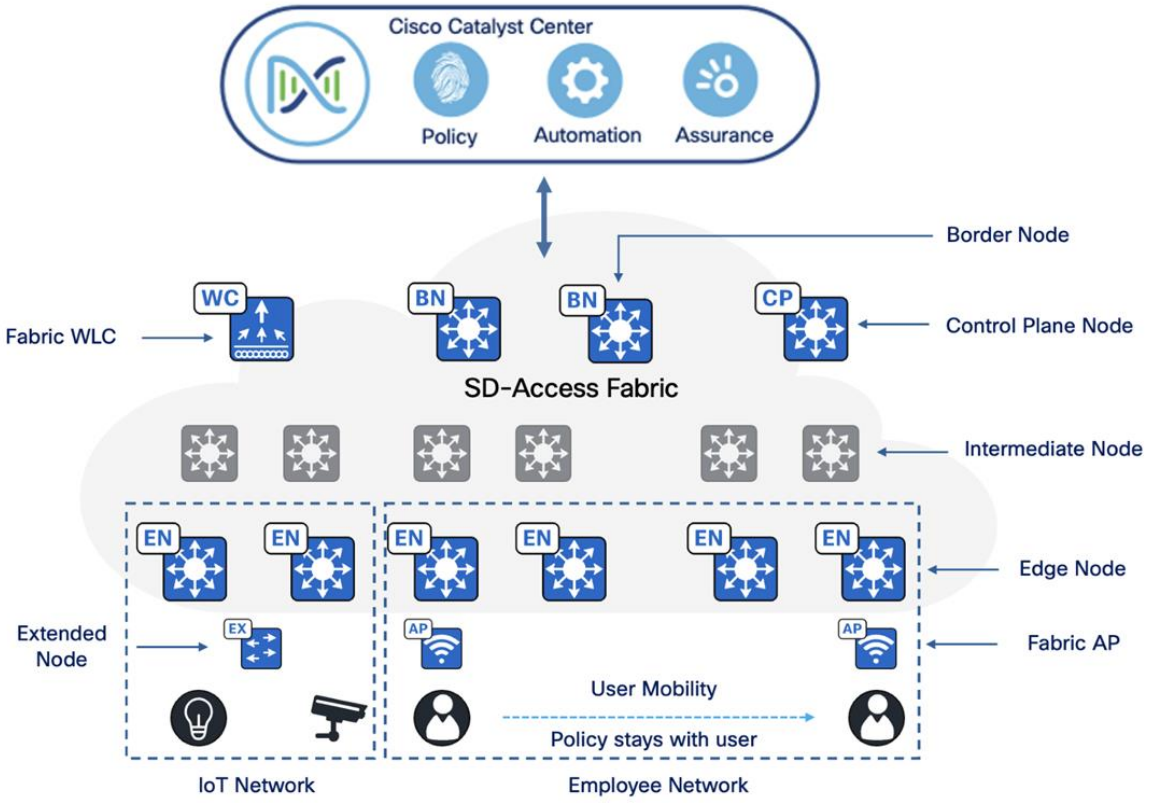
拡張ノード

SD-Access 拡張ノードを使用すると、企業ネットワークをオフィス以外のエリアに拡張できます。拡張ノードは、セグメンテーションを確保し、接続されたエンドポイントにグループベースのポリシーを適用しながら、ファブリック エッジ ノードにレイヤ 2 ポート拡張を提供します。拡張ノードを使用することで、組織は強化されたセキュリティ、シンプルな管理、一貫したポリシーの適用をはじめとする SD-Access の利点を、ネットワーク内のより広範なデバイスや端末に拡張できます。

詳細については、『Cisco Software-Defined Access Solution Design Guide』の「Extended node design」のセクションを参照してください。

図 1 では、SD-Access ファブリックの展開に関連する主要コンポーネントが強調され、SD-Access ネットワーク内におけるそれぞれの位置を示しています

図 1.　　Cisco SD-Access ファブリックのロールの例



ファブリックインアボックス

Fabric In a Box（FIAB）では、ボーダーノード、コントロールプレーンノード、エッジノードなど、従来の SD-Access ネットワークのすべての機能が単一の物理デバイスに統合されます。このデバイスは、単一のスイッチ、ハードウェアスタッキング機能を備えたスイッチ、または StackWise Virtual（SVL）展開の一部です。

FIAB には次の利点があります。

- 簡易性
- 高いコスト効果
- 展開の高速化
- ブランチおよび小規模な展開に最適

詳細については、『Cisco Catalyst 9000 Platform StackWise Virtual White Paper』を参照してください。

SD-Access 組み込み型ワイヤレス

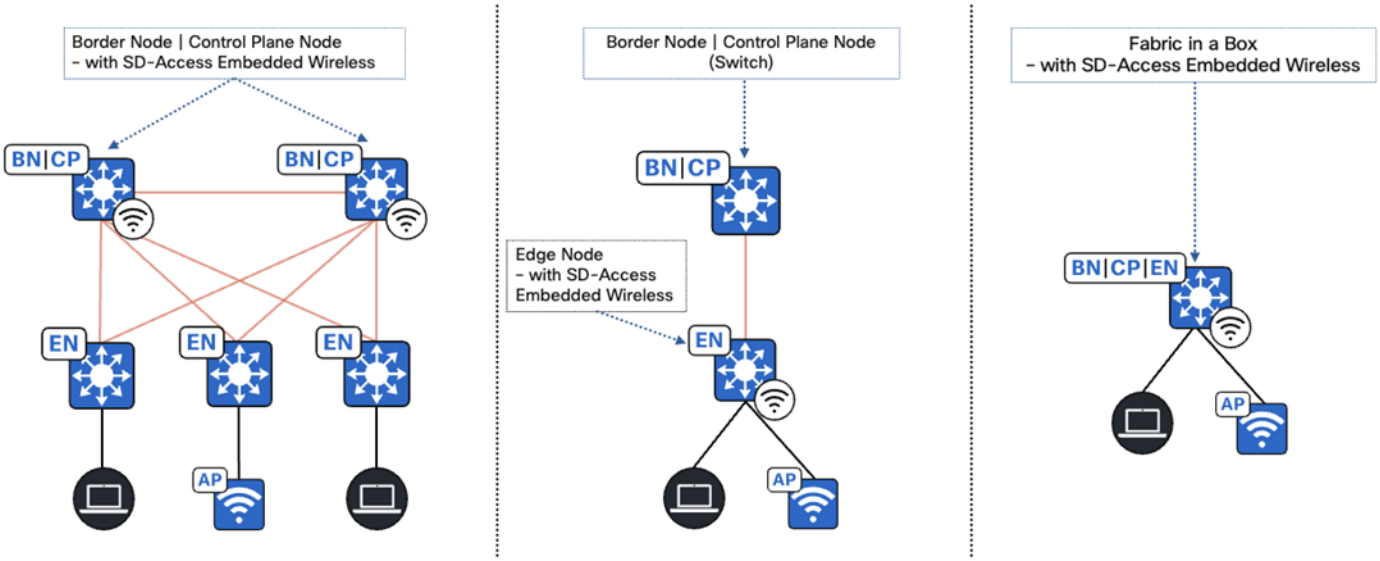
分散型のブランチや小規模キャンパスの場合、Catalyst 9000 シリーズ スイッチ用のソフトウェアパッケージとして入手可能な Cisco Catalyst 9800 組み込み型ワイヤレスコントローラを使用することで、ハードウェアワイヤレスコントローラなしでワイヤレスコントローラ機能を実現できます。

Catalyst 9800 組み込み型ワイヤレスコントローラは、次の 3 つのトポロジでの SD-Access 展開に対応しています。

- Cisco Catalyst 9000 シリーズ スイッチが、同じ場所に配置されたボーダーおよびコントロールプレーンとして機能する。
- ボーダーおよびコントロールプレーンノードがルーティング プラットフォーム上にある場合に、Cisco Catalyst 9000 シリーズ スイッチがエッジノードとして機能する。
- Cisco Catalyst 9000 シリーズ スイッチがファブリック統合として機能する。

技術的なヒント： Catalyst 9200、9200L、9500X、および 9600 シリーズ スイッチを除くすべての Catalyst 9000 スイッチは、SD-Access 組み込み型ワイヤレス機能をサポートしています。組み込み型コントローラは、SD-Access 展開で使用されるファブリックモード AP のみをサポートしています。

図 2.　　SD-Access 組み込み型ワイヤレス対応トポロジ



トランジット

トランジットにより、複数のファブリックサイトを接続したり、ファブリックサイトをデータセンターやインターネットなどの非ファブリックドメインにリンクしたりできます。トランジットは、ファブリックサイト間またはファブリックサイトと外部ドメイン間の接続のボーダーノード設定を、Catalyst Center がどのように自動化するかを定義する Cisco SD-Access コンストラクトです。

トランジットには次の 2 つのタイプがあります。

- IP ベースのトランジット：

  IP ベースのトランジットでは、ファブリック VXLAN ヘッダーが削除され、元のネイティブ IP パケットが送られます。ネイティブ IP 形式の場合は、ファブリックサイト間の従来のルーティングおよびスイッチングプロトコルを使用してパケットが転送されます。SD-Access トランジットとは異なり、IP ベースのトランジットでは、VRF-Lite 接続を使用してアップストリーム ピアデバイスへのプロビジョニングが行われます。通常、IP ベースのトランジットはデータセンター、WAN、またはインターネットに接続します。VRF 認識ピアを使用した共有サービスに接続するには、IP ベースのトランジットを使用します。

- SD-Access トランジット：

  SD-Access トランジットでは、VXLAN カプセル化が使用され、アップストリーム ピアへの VRF-Lite 接続に依存しません。IP ベースのトランジットと同様に、パケットはファブリックサイト間で従来のルーティングおよびスイッチングプロトコルを使用して転送されます。ただし、IP ベースのトランジットとは異なり、SD-Access トランジットは SD-WAN や Dynamic Multipoint VPN（DMVPN）と同様に、WAN/MAN ネットワーク上で動作するオーバーレイです。

IP ベースのトランジットと SD-Access トランジットの比較を次に示します。

IP ベースのトランジット：

- 既存の IP インフラストラクチャを活用：

  従来の IP ベースのルーティングプロトコルを使用して、ファブリックサイトに接続します。

- VRF の再マッピングが必要：

  VRF と SGT をサイト間で再マッピングする必要があり、複雑さが増します。

- 既存の IP ネットワークに適している：

このアプローチは、IP ベースの WAN インフラストラクチャがすでに確立されている場合に最適です。

- 柔軟性を提供：

  ルーティングプロトコルとトラフィック エンジニアリング オプションの点でより柔軟性があります。

SD-Access トランジット：

- ネイティブ SD-Access ファブリック：

  サイト間の通信に LISP、VXLAN、および CTS を使用します。

- SGT の保持：

  ファブリックサイト全体で SGT を維持することで、セキュリティとポリシーの適用を強化します。

- 集中管理：

  ドメイン全体のコントロールプレーンノードを使用して、シンプルな管理を実現します。

- 専用インフラストラクチャが必要：

  SD-Access トランジット コントロールプレーン用に追加のインフラストラクチャが必要です。

SD-Access トランジットを使用する場合は、次の主な考慮事項を確認してください。

- 接続は、キャンパスネットワークの Cisco SD-Access に使用される MTU の推奨設定に対応している必要があります。
- IP 到達可能性は、ファブリックサイト間に存在する必要があります。具体的には、すべてのファブリックノード間に既知のアンダーレイルートが存在している必要があります。デフォルトルートは、この目的には使用できません。
- マルチキャスト通信が SD-Access トランジットを通過する場合、アンダーレイ SSM に対応している必要があります。

詳細については、Cisco SD-Access を参照してください。

互換性マトリックス

Catalyst Center は、シスコのエンタープライズ スイッチング、ルーティング、およびモビリティ製品を対象としています。サポートされているシスコ製品の完全なリストについては、互換性マトリックスを参照してください。

- Cisco Catalyst Center 互換性マトリックス
- Cisco SD-Access 互換性マトリックス

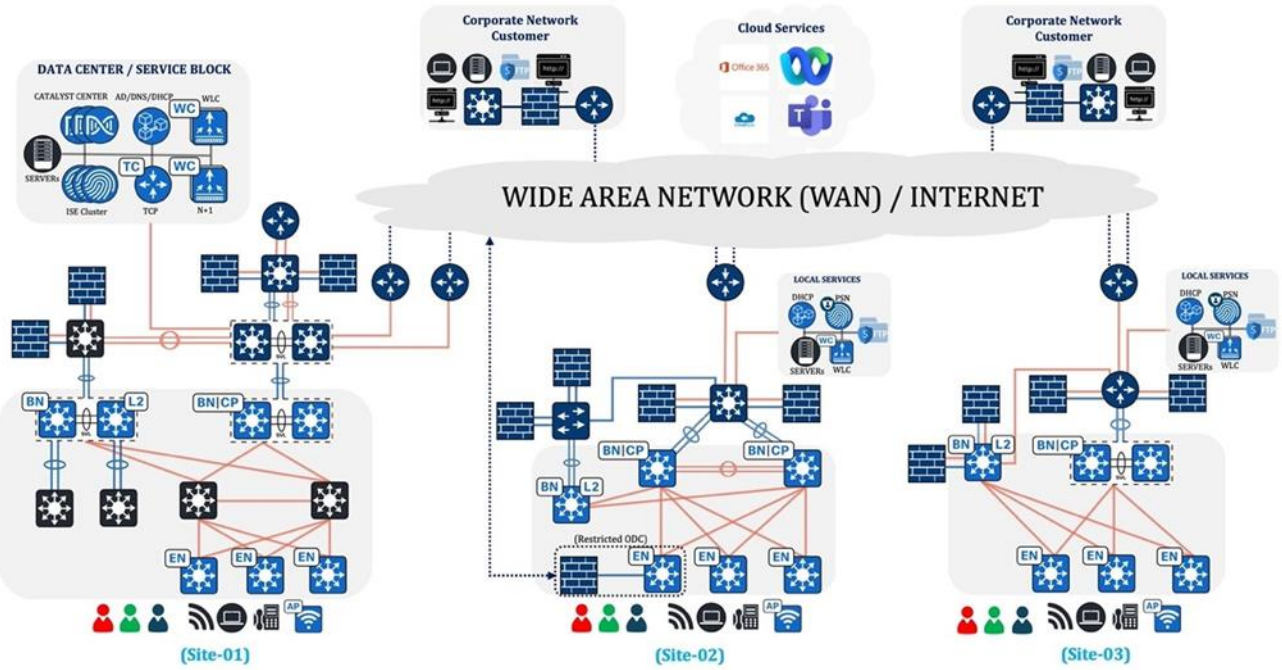
ITES プロファイルの展開

このセクションでは ITES セクター向けの設計ガイダンスを提供し、その要件と、安全性と柔軟性を備えたシンプルなネットワークを構築するための Cisco SD-Access の使用方法に焦点を当てます。

ここで説明するトポロジ、ユースケース、およびソリューションは、ITES の標準的な展開オプションを満たしつつ、そのテーマと要件に対処することを目的としています。

ITES ソリューショントポロジ

図 3.　　SD-Access を使用した ITES 向けのネットワーク設計



トポロジ内のデバイスとファイアウォールの配置の概要を以下に示します。

Site-01：大規模拠点

- Cat9600 SVL スイッチは、ボーダーノードとコントロールプレーンノードの両方として機能します。
- Cat9500 SVL スイッチは、専用のレイヤ 2 ボーダーノードとして機能します。
- Cat9300 および 9400 スイッチはエッジノードとして機能します。
- ゲートウェイとして機能する C2S/S2S ファイアウォールは、レイヤ 2 ボーダー外に配置された集約スイッチに接続されます。
- ゲートウェイとして機能しない C2S/S2S ファイアウォールは、フュージョンノード外に位置している集約スイッチに接続されます。

Site-02：中規模拠点

- Cat9500 スイッチは、ボーダーノードとコントロールプレーンノードの両方として機能します。
- Cat9500 スイッチは、専用のレイヤ 2 ボーダーノードとして機能します。

- Cat9200 および 9400 スイッチはエッジノードとして機能します。
- ゲートウェイとして機能する C2S/S2S ファイアウォールは、レイヤ 2 ボーダー外に配置された集約スイッチに接続されます。
- ゲートウェイとして機能しない C2S/S2S ファイアウォールは、フュージョンノードに直接接続されます。

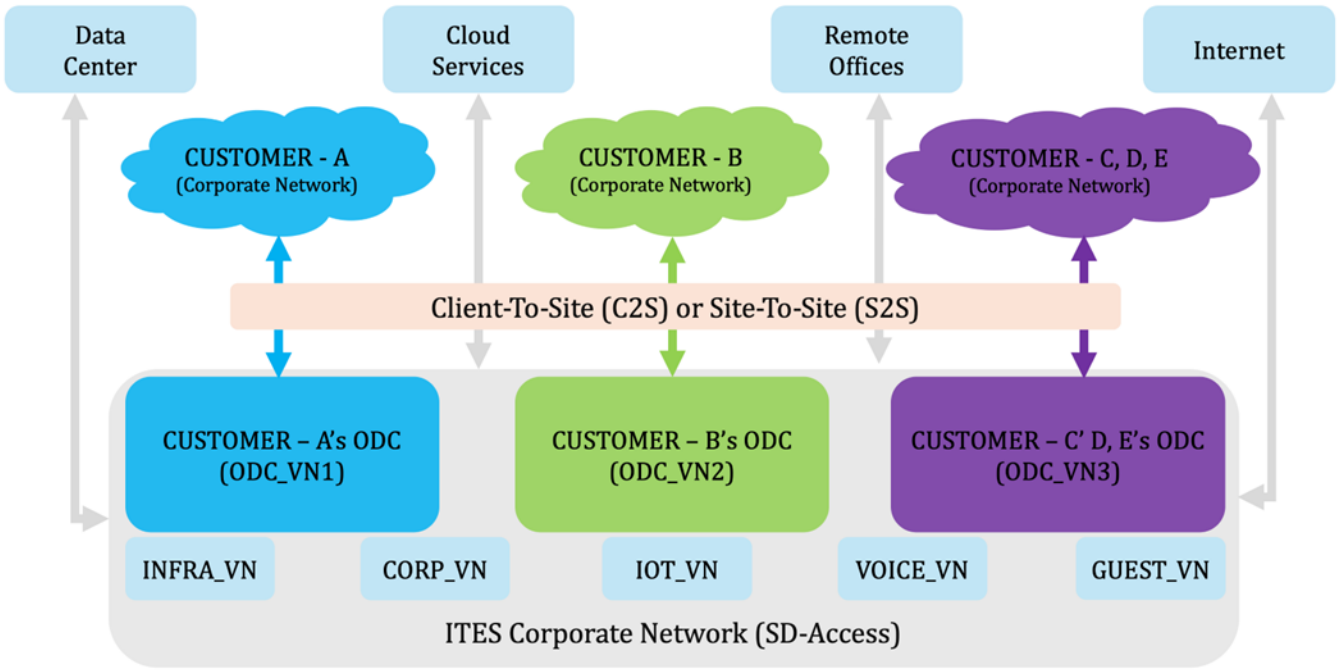
Site-03：小規模拠点

- Cat9500 SVL スイッチは、ボーダーノードとコントロールプレーンノードの両方として機能します。
- Cat9500 スイッチは、専用のレイヤ 2 ボーダーノードとして機能します。
- Cat9300 スイッチはエッジノードとして機能します。
- ゲートウェイとして機能する C2S/S2S ファイアウォールは、レイヤ 2 ボーダーに直接接続されます。
- ゲートウェイとして機能しない C2S/S2S ファイアウォールは、フュージョンノードに直接接続されます。

ITES 論理図

図 4 は ITES 環境のネットワークアーキテクチャの概要で、顧客ネットワークと ITES 企業ネットワーク間の接続を示しています。SD-Access インフラストラクチャ内のさまざまなセグメントにまたがる、セキュアで効率的なデータフローが強調されています。

図 4.　　ITES 環境の論理図



ビジネスの成果と課題

ITES（情報技術対応サービス）は、テクノロジーによって可能になる、さまざまなプロセスとサービスのアウトソーシングを指します。あらゆる業界のビジネスで ITES の活用が進んでおり、効率の向上、コストの削減、カスタマー エクスペリエンスの強化を実現しています。ただし、他のビジネスと同様、ITES には次のような独自の課題と潜在的成果があります。

- セキュリティ
- コンプライアンス
- 使用可能
- 財務
- エクスペリエンス

セキュリティ

ITES 企業において、セキュリティ対策の強化、リスクの軽減、そしてコンプライアンスの確実な遵守は、堅牢なセキュリティプロトコルを導入し、定期的なリスク評価を実施して、業界固有の規制や基準に従うことで実現できます。サイバーセキュリティの脅威は、ITES 企業の最高情報セキュリティ責任者（CISO）にとって最大の懸念事項となっています。ハイブリッドワークへの迅速な移行と顧客に対するデジタルビジネスサービスの進化により、サイバー犯罪者が利用できる攻撃対象領域ベクトルは大幅に増加しています。これらの脅威が放置されると、悪意のある攻撃者が脆弱性をエクスプロイトし、財務面でも評判に関しても重大な損害をもたらす可能性があります。CISO グループは、基本的なセキュリティプラクティスとプロセスを定期的に確認します。

コンプライアンス

ITES 企業にとって規制基準を遵守することは、業務における信頼、セキュリティ、および合法性を維持する上で不可欠です。多くの場合、これらの企業は機密データの処理や、さまざまな業界のクライアントに対する重要サービスの提供を委任されています。したがって、コンプライアンス規制を遵守し、データの機密性、完全性、可用性を確保することが重要です。規則遵守がなされないと、ITES 企業に法的影響が及ぶだけでなく、自社の評判が低下し、貴重なクライアントの信頼を失うリスクがあります。したがって、コンプライアンスへの能動的なアプローチこそが、今日の規制環境における ITES 企業の成功と持続可能性にとって重要です。

運用

ITES 企業にとってネットワークの稼働時間は、業務を円滑に進めてビジネス目標を達成する上で不可欠です。ITES ネットワークはミッションクリティカルなので、可用性を可能な限り 100% に近づけることが最終的な目標になります。ファイブナインの可用性（99.999% の稼働時間）は、この目標の達成に向けた大きな一歩です。これは、年間のダウンタイムがわずか 5 分 16 秒しか許されないことを意味します。シームレスで中断のないサービスは、ITES 顧客の生産性とビジネスの成功に不可欠です。ITES 企業は、自動化、モニタリング、ロードバランシング、およびフェールオーバーのメカニズムを導入することで、99.999% の可用性というベンチマークを達成するだけでなく、それを超えることすら可能になります。

財務

運用コストは、ITES ビジネスの大きな焦点です。数千もの拠点への展開を自動化しつつ、オンサイトのネットワーク運用の必要性を可能な限り最小限に抑えることで、コストを合理化し、収益を向上させます。ITES セクターでは大規模なマルチサイト展開が一般的であり、多くの場合、広範な地理的エリアに分散している数百のオフショア開発センター（ODC）が含まれます。このようなネットワークをボックスごとに、またはサイトごとにオンサイトチームで管理することは、大きな課題となります。

ITES の複雑な要件に対処するには、任意のサイトや ODC をあらゆる場所で迅速にセットアップし、リモートで管理するためのソリューションが必要です。これにより、ITES 組織は効率性の高い IT スタッフを維持できます。これを実現するには、ネットワークの自動化とモニタリングを導入して、展開と障害対応の手順を合理化する必要があります。

エクスペリエンス

重要なビジネス機能をサポートする最新のテクノロジーを戦略的に活用して、ユーザー体験とアプリケーション体験を強化します。セキュリティ、コンプライアンス、および可用性に関する懸念以外にも、QoS が一貫していないか低速であるネットワークは、顧客の満足度を低下させ、財務的な損失につながる可能性があります。時間的制約のある業務などの環境では、遅延は重大な問題であり、低遅延と一貫した QoS が組織の要件を満たす上で重要です。

ITES ビジネスの成果に対するソリューション

このセクションでは、ITES ネットワーク展開について定義されたビジネス成果を達成するためのソリューションを概説します。

セキュリティ上の課題

情報技術対応サービス（ITES）セクターは、攻撃対象領域の増加、データ侵害、組織内に潜む脅威、規制のコンプライアンス要件、洗練されたサイバー攻撃、テレワークのセキュリティなど、複雑かつダイナミックな環境に起因するセキュリティ上の重大な課題に直面しています。シスコの SD-Access フレームワークは、次に挙げる包括的なツールと機能のセットを通じて、これらの課題に対処します。

- マクロセグメンテーション
- マイクロセグメンテーション
- ポリシー実施モデル
- グループベースのポリシー分析
- セグメントの最適化と管理
- AI エンドポイント分析
- ゼロトラストソリューションによるエンドポイントセキュリティ
- ゲストユーザーの分離
- 外部ゲートウェイによるセキュリティの強化

マクロセグメンテーション

ITES ネットワークの場合、推奨されるセグメンテーション戦略を導入するために、従業員、モニタリングデバイス、ゲストなどのネットワーク端末に異なる仮想化ルーティングと VRF を割り当てます。SD-Access では、端末を異なる VRF にマクロセグメント化する機能が提供されます。これは、Catalyst Center を使用してネットワーク内で設定できます。

VN の導入に関する例を次に示します。

- INFRA VN：

  この VN は、AP、および接続用のクラシックノードとポリシー拡張ノード専用であり、グローバル ルーティング テーブルにマッピングされます。

- Employee VN：

  この VN は通常の従業員アクセスに使用し、すべての内部ユーザーに安全で分離された接続を提供します。

- Guest VN：

  この VN は、訪問者やゲストにインターネットアクセスを提供しますが、訪問者やゲストが内部ネットワークにアクセスできないようにします。

- Monitoring VN：

  この VN はネットワークのモニタリングおよび管理デバイス専用です。通常のユーザートラフィックから隔離します。

- ODC VN：

  クライアントのプロジェクトに取り組む従業員についてはこの VN を使用し、クライアントの企業ネットワークへの安全かつ分離された接続を実現します。

SD-Access ネットワークに VN を導入することで、ITES 企業はさまざまなタイプの通信を効果的にセグメント化して保護し、ネットワーク全体のパフォーマンスとセキュリティを向上させることができます。

マイクロセグメンテーション

マイクロセグメンテーションは、SD-Access VN 内でセキュリティを詳細に設定できるように、セキュリティグループを使用してトラフィックを分類し、ポリシーを適用することで、ネットワークアクセス制御のプロビジョニングと管理を簡素化します。

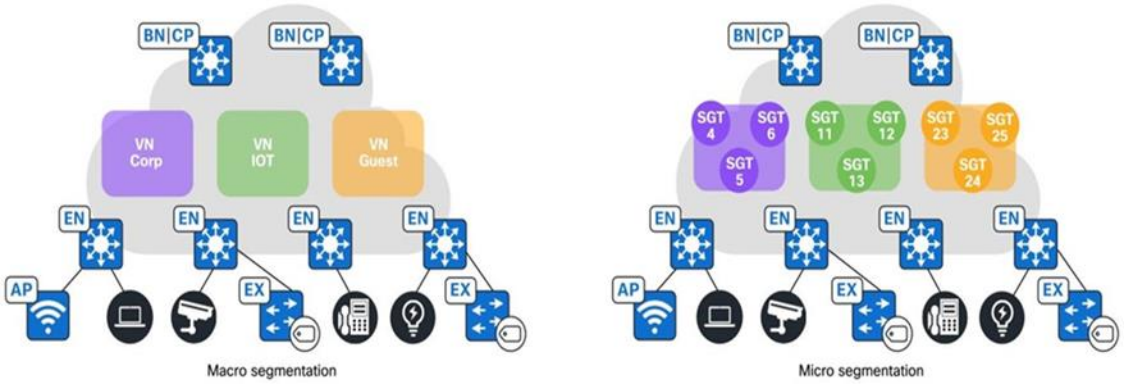
通常、単一の VN 内では、所属部門で従業員をグループ化するか、プリンタなどのデバイスを異なるセキュリティグループに配置することによって、さらにセグメント化する必要があります。従来、これは、IP ACL によって適用される異なるサブネットにグループを配置することによって行われていました。一方、Cisco SD-Access ではマイクロセグメンテーションの柔軟性があり、ユーザーおよびエンドポイント中心のアプローチで同じサブネットを使用することができます。ダイナミック認証では、認証情報に基づいてさまざまな SGT が割り当てられ、セキュリティ グループ アクセス制御リスト（SGACL）によってこれらの SGT ベースのルールが適用されます。

ユーザーがネットワークに接続すると、802.1X や MAC 認証バイパス（MAB）などの方法で認証されます。次に、ネットワーク承認によって、アイデンティティ、LDAP グループのメンバーシップ、場所、アクセスタイプなどの情報を使用してユーザートラフィックが分類されます。この分類情報は、トラフィックを許可するか拒否するかを決定するために、動的にダウンロードされたポリシーを適用するネットワークデバイスに伝播されます。

詳細については、『Software-Defined Access Macrosegmentation Deployment Guide』を参照してください。

図 5 に、マクロセグメンテーションとマイクロセグメンテーションの例を示します。

図 5.　　マクロセグメンテーションとマイクロセグメンテーションの例



ポリシー実施モデル

Cisco TrustSec は、ネットワークアクセスのプロビジョニングと管理を簡素化し、組織全体にセキュリティポリシーを適用するように設計されたセキュリティソリューションです。従来の IP ベースの方法ではなく、ロールとポリシーに基づいた包括的なセグメンテーションとアクセス制御が可能になり、有線およびワイヤレス環境全体でセキュリティと運用の効率が向上します。

コンピューティングおよびネットワークセキュリティの適用では、ポリシー適用モデルは一般に次の 2 つのカテゴリに分類されます。

- 拒否リストモデル（デフォルトで IP を許可）：

  デフォルトアクションでは IP 通信が許可されており、制限はセキュリティ グループ アクセス コントロール リスト（SGACL）を使用して明示的に設定する必要があります。ネットワーク内のトラフィックフローの把握が不完全な場合に、このモデルを使用します。導入は比較的簡単です。

- 許可リストモデル（デフォルトで IP を拒否）：

  デフォルトアクションでは IP トラフィックが拒否されるため、必要なトラフィックは SGACL を使用して明示的に許可する必要があります。お客様がネットワーク内のトラフィック フローについて十分に理解している場合は、このモデルを使用します。コントロールプレーントラフィックはアクティブ化時にすべてのトラフィックをブロックする可能性があるため、詳細な調査が必要です。

ポリシー適用モデルの詳細については、『SDA を使用した ISE TrustSec Allow-List モデル（デフォルトの IP 拒否）の有効化』を参照してください。

グループベースのポリシー分析

注目度の高いサイバー攻撃のニュースにより、ITES 組織は境界でのセキュリティを超えて内部ネットワークのセグメンテーションを導入するようになりました。ただし、ネットワーク内のユーザーとデバイスの動作が十分可視化できないと、効果的なセグメンテーションポリシーを作成することが困難になります。ビジネスでは、この複雑な状況に対処するためのソリューションが求められています。

シスコは、Catalyst Center で、グループベースポリシー分析（GBPA）を実現することにより、これらの課題に対処するソリューションを提供します。GBPA により、ネットワーク管理者は次のことが可能になります。

- グループの相互関係を検出して可視化：

  GBPA はネットワーク通信フローを分析して、部門や機能などのさまざまなネットワークグループがどのように通信しているかを特定します。

- 通信パターンの特定：

  GBPA は、さまざまなグループで使用される個別のポートとプロトコルを特定し、ネットワークの動作に関する詳細な洞察を提供します。

- ポリシー作成を簡素化：

  GBPA は、検出された情報に基づいてグループ間の通信を制御するための効果的なセキュリティポリシーを構築するプロセスを合理化します。

図 6.　　セキュリティ グループポリシー分析の論理図

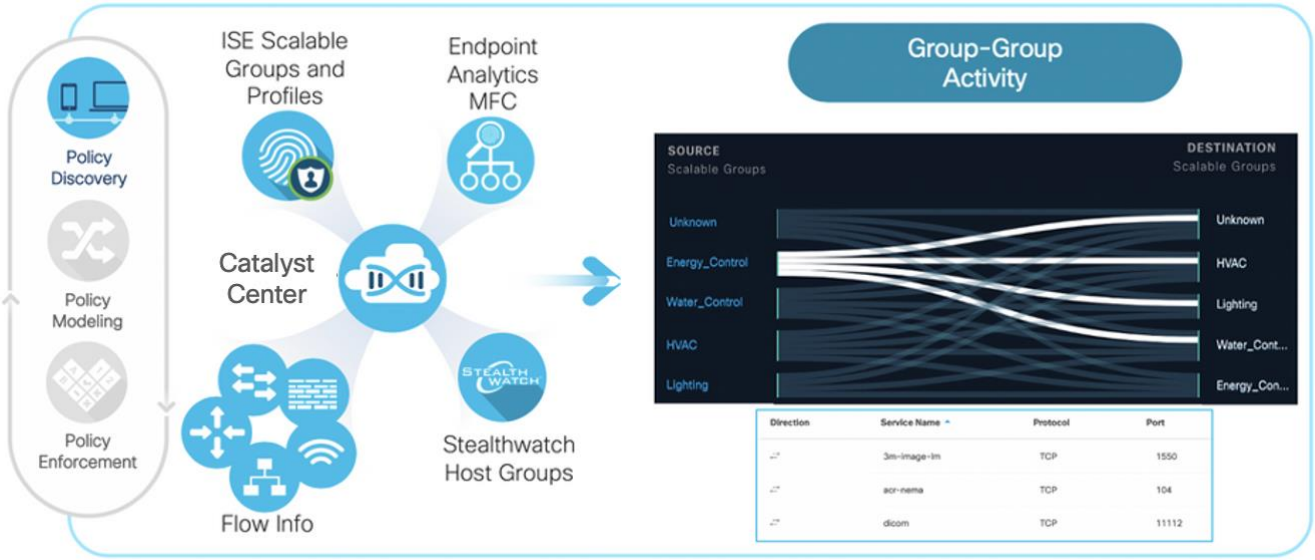


図 6 に示すように、GBPA は次のソースからの情報を利用して、ネットワークの全体的なビューを作成します。

- Cisco Identity Services Engine（ISE）：
  ISE と統合すると、GBPA は、接続されたデバイスのさまざまなタイプを分類する、スケーラブルグループおよびプロファイルグループとして定義されたネットワークグループについて学習します。
- エンドポイント分析：

  エンドポイント分析では、機械学習と多要素分類を利用してネットワーク上の未識別デバイスを減らし、セグメンテーション用のより正確なプロファイルグループを提供します。
- Cisco Secure Network Analytics（オプション）：

  Cisco Secure Network Analytics（SNA）と統合すると、GBPA は SNA によって特定されたホストグループについて学習でき、ネットワークの可視性がさらに強化されます。
- NetFlow データの統合：

  GBPA は、ネットワークデバイスからの NetFlow データを組み込み、グループ情報のコンテキストを提供します。この結合データは、グラフや表によって可視化されるため、管理者はグループの連携動作に基づいてネットワークの動作を明確に把握できます。

GBPA は、ネットワーク検出、可視化、およびセキュリティポリシー要件を分析するためのツールによって、ネットワーク管理者を支援します。この包括的なアプローチにより、今日のダイナミックな脅威状況においてより効果的でターゲットを絞ったセキュリティポリシーを作成できます。

セグメントの最適化と管理

ファブリックゾーンは SD-Access アーキテクチャの基本的なコンポーネントで、大規模な展開を管理、保護、および最適化するための構造化されたアプローチを提供します。

- 管理性：

  ファブリックゾーンは、物理的または論理的な境界（建物、フロア、部門など）に基づくデバイスの論理的なグループ化を可能にします。
- セキュリティ

  ファブリックゾーンにより、サイト内の VN と IP プールのプロビジョニングをきめ細かく制御できます。
- 拡張性とパフォーマンス：

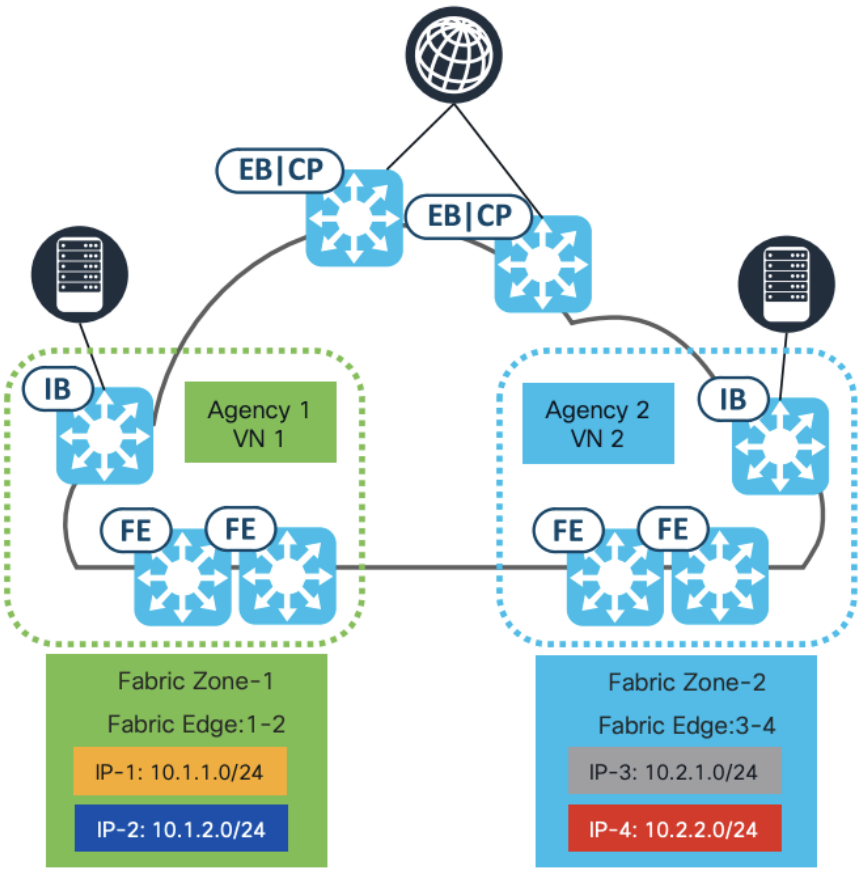
  ファブリックゾーンでは、デバイスをゾーンにグループ化することで、ファブリックエッジノード全体のプロビジョニング時間を短縮します。

ファブリックゾーンは、レイヤ 2 VN とエニーキャストゲートウェイをファブリックサイトの特定のセクション（個々の建物など）内に限定する手段を提供します。これらは必須ではなく、ファブリックサイト内に限定され、エッジノードと拡張ノードのみを含みます。ファブリックゾーンを使用する場合、指定された VN とエニーキャストゲートウェイ（IP アドレスプール）のみが各ファブリックゾーン内のエッジノードに割り当てられます。

ファブリックゾーンが存在しない場合、すべての VN とエニーキャストゲートウェイはファブリックサイト内のすべてのエッジノードに割り当てられます。設計階層要素がファブリックゾーンに再配置されると、この要素と同じレベルかそれより下でプロビジョニングされたすべての既存のエッジノードが、自動的にファブリックゾーンに転送されます。この移行によってユーザー通信が中断されることはありません。

図 7 にファブリックゾーン設定の例を示します。

図 7.　　SD-Access ファブリックゾーンの例



AI エンドポイント分析

シスコの次世代エンドポイント可視性ソリューションである Cisco AI（人工知能）エンドポイント分析は、ネットワークと IT エコシステムの詳細な洞察を提供し、すべての端末を可視化して検索可能にします。次の技術を使用して、企業内の不明な端末の数を検出および削減します。

- ディープ パケット インスペクション（DPI）：

  IT、ビルディングオートメーション、および医療機関のエンドポイントのアプリケーションと通信プロトコルをスキャンおよび把握することで、詳細なエンドポイントコンテキストを収集します。

- 機械学習（ML）：

  共通の属性を持つエンドポイントを直感的にわかるようにグループ化し、IT 管理者によるラベル付けを支援します。これらの一意のラベルは、提案として他の組織と匿名で共有されます。これにより、不明なエンドポイントの数を減らし、新しいラベルに基づいてグループ化できます。

- サードパーティ製品およびシスコ製品との統合：

  プロファイル端末に対して使用する追加のネットワークおよび非ネットワークコンテキストを提供します。

つまり、Cisco AI エンドポイント分析は、エンドポイントの可視性の欠落を、高い忠実度で解消するという、セキュリティポリシーを導入する際に多くのお客様が直面する重要な課題に対処します。これは、新しいアプリケーションとして Cisco Catalyst Center リリース 2.1.2.x 以上で使用できます。Cisco Catalyst Advantage 以上のサブスクリプションレベルをお持ちのお客様が、Cisco AI エンドポイント分析にアクセスできます。このテクノロジー入門では、Cisco AI エンドポイント分析と、シスコのお客様に提供される利点について説明します。

詳細については、次のマニュアルを参照してください。

- Cisco SD-Access AI エンドポイント分析
- Cisco Catalyst Center ユーザーガイド - AI エンドポイント分析

ゼロトラストソリューションによるエンドポイントセキュリティ

SD-Access のゼロトラストソリューションを使用した端末セキュリティは、ノート PC、スマートフォン、IoT デバイスなど、SD-Access 環境内の端末を保護することを目的としたネットワークセキュリティへの包括的なアプローチです。ゼロトラストの原則を適用することは、ネットワーク境界内にあるデバイスやユーザーであっても、自動的に信頼されないことを意味します。ネットワークリソースへのアクセスを許可する前に、各デバイスが検証および認証されます。

Cisco SD-Access ゼロトラスト セキュリティソリューションは、次の機能を使用してネットワーク アクセス ポリシーを自動化します。

- エンドポイントの可視性：

  エンドポイントを識別してグループ化します。トラフィックフロー分析を通じて相互作用をマッピングし、アクセスポリシーを定義します。

- 信頼のモニタリング：

  エンドポイントの動作を継続的に監視し、脆弱性をスキャンして、持続的なアクセスの信頼性を検証し、不正なエンドポイントや侵害されたエンドポイントを隔離します。

- ネットワークのセグメント化：

  マルチレベル セグメンテーションにより、グループベースのアクセスポリシーを実施し、ネットワークの保護を強化できます。

Cisco SD-Access では、IEEE 802.1x メカニズムを使用して、AP やスイッチなどのネットワークデバイスに対してセキュアなオンボードを実行できます。これにより、すべてのエッジノードのアクセスポートでのクローズド認証を維持することで、未承認デバイスの接続からネットワークが保護されます。クローズド認証を使用してセキュアにオンボードされたスイッチは、サプリカントベースの拡張ノード（SBEN）と呼ばれます。

SBEN は、エッジノードへのアップリンクで EAP-TLS 認証を使用するサプリカントを持つように、Cisco Catalyst Center によってポリシー拡張ノードとしてプロビジョニングされます。EAP-TLS 証明書は、Cisco Catalyst Center 認証局（CA）を使用して Cisco Catalyst Center によってプロビジョニングされます。オンボーディングが成功した後は、ポートへのアクセスは認証ステータスのみに基づいて行われます。デバイスまたはポートがダウンすると、認証セッションがクリアされ、ポートでトラフィックが許可されなくなります。ポートが復旧すると、dot1x 認証を経て、Cisco SD-Access ネットワークへのアクセスが回復します。

AP のセキュアなオンボーディングは、クローズド認証ポートで AP を承認し、PnP ワークフローのために DHCP/DNS および Cisco Catalyst Center への制限付きアクセスを許可することで実現します。Cisco Catalyst Center の PnP ワークフローは、AP で dot1x サプリカントを有効にするように強化され、AP はこのサプリカントを使用して Cisco ISE で認証されます。

詳細については、『Cisco Catalyst Center ユーザーガイド』の「サプリカントベースの拡張ノードの設定」セクションを参照してください。

ゲストユーザーの分離

SD-Access のゲストワイヤレス展開では、VN と SGT の導入を通じて企業のネットワークからの堅牢な分離を実現します。ゲストアクセス専用の VN を作成し、SGT を使用してゲスト通信にタグを付け、きめ細かなアクセスポリシーを適用します。これらのポリシーにより、ゲストユーザーは企業のリソースにアクセスできず、許可された特定のサービスにインターネットアクセスが制限されます。この分離は、定義済みのポリシーに従って通信の

フィルタ処理と転送を行うファブリックエッジノードとボーダーノードによって適用されます。これにより、ゲストユーザーは企業のネットワークの完全性を侵害することなく、分離されたセキュアな接続を利用できます。

マルチサイト展開の場合、SD-Access はマルチサイト リモート ボーダー（MSRB）を活用して、地理的に分散した場所でもセキュアなゲストワイヤレス体験を利用できるようにします。MSRB 機能を使用すると、リモートサイトからホームサイトを経由してゲスト通信をインターネットに直接ルーティングできるため、遅延が最小限に抑えられ、帯域幅の使用量が最適化されます。すべてのサイトで同じ VN および SGT ポリシーを維持することで、ユーザーの場所に関係なく、一貫性のあるセキュアなゲスト体験を実現します。このアプローチにより、ゲスト通信が複数のサイトを通過する場合でも、企業のネットワークから分離された状態が保たれます。また、SD-Access ファブリック内でのポリシー制御を一元化することで管理がシンプル化されます。

Cisco Catalyst Center により、Cisco AireOS および Polaris ベースのワイヤレス LAN コントローラ（Cisco Catalyst 9800 および Cisco Catalyst 9000 プラットフォームの組み込み型ワイヤレス）上で中央 Web 認証（CWA）、外部 Web 認証（EWA）、およびホットスポット SSID が設定され、SD-Access ネットワークでのゲストアクセスフローが有効になります。

詳細については、こちらの設定ガイドを参照してください。

- Cisco Catalyst Center SD-Access Guest Automation

外部ゲートウェイによるセキュリティの強化

SD-Access では、デフォルトゲートウェイが、特定のファブリックサイト内の VN にある各サブネットの全エッジノードに存在します。リモートサブネット宛てのトラフィックは、エッジノードのデフォルトゲートウェイによって処理された後、適切な宛先にルーティングされます。

多くのネットワークでは、デフォルトゲートウェイをローカルエッジノードではなく外部ファイアウォール上に設置する必要があります。ファイアウォール トラフィック検査は、このようなネットワークにおける一般的なセキュリティおよびコンプライアンスの要件です。ファブリック機能の外部でゲートウェイを有効にすることにより、デフォルトゲートウェイがエッジノードでプロビジョニングされません。その代わりに、ファイアウォールなどの外部デバイス上でプロビジョニングすることができ、接続先に到達する前にトラフィックを検査できます。

コンプライアンス規制

コンプライアンス規制とは、組織が特定の業界や管轄権内で合法的に業務を行うにあたって従う必要がある、一連のルールと基準を指します。これらのテクノロジーは、規制対応プロセスを自動化し、データセキュリティを向上させ、規制要件を効果的に満たすリアルタイムのモニタリングおよびレポート機能を有効にすることで、規則遵守を保証します。業界規制に準拠し続けることは必ずしも簡単ではありません。Cisco SD-Access には、このプロセスを簡素化できる複数の機能が用意されています。

- ロールベース アクセス コントロール
- 監査ログ
- 設定コンプライアンス
- 設定のばらつき

ロールベース アクセス コントロール

Catalyst Center のロールベースアクセスコントロール（RBAC）は、組織内の個別ユーザーのロールに基づいて、各機能と操作へのアクセスを制御する方法を提供します。RBAC は、最小権限の原則を適用するのに役立ち、ユーザーが自分のロールに必要なリソースにのみアクセスできるようにします。Catalyst Center は、ローカルまたは外部の RADIUS/TACACS データベースのいずれかに基づいてユーザーに権限を割り当てることがで

きる柔軟性をサポートしています。ユーザーにロールを割り当てたり、Catalyst Center 内の特定のアプリケーションへのアクセスを許可したりできます。

詳細については、『Cisco Catalyst Center 管理者ガイド』の「ユーザーの管理」セクションを参照してください。

監査ログ

監査ログは、Catalyst Center アプリケーション内で発生したイベントまたはアクションのレコードを指します。これらのログには通常、アクションを行ったユーザー、実行されたアクション、およびアクションが発生した時刻などの詳細が含まれます。監査ログは、管理者がネットワーク インフラストラクチャに加えられた変更を追跡し、セキュリティ侵害の可能性を特定して、ユーザーが適切な手順に従っていることを確認するのに役立つため、セキュリティおよびコンプライアンスの目的で重要です。管理者は、監査ログを確認することにより、Catalyst Center アプリケーション内のアクティビティを把握し、必要に応じて適切なアクションを実行できます。

詳細については、『Cisco Catalyst Center 管理者ガイド』の「監査ログの表示」セクションを参照してください。

設定コンプライアンス

コンプライアンスは、元のコンテンツに影響を与えることなく注入または再設定される可能性がある、ネットワークのインテント逸脱やアウトオブバンドの変更を特定するのに役立ちます。ネットワーク管理者は Catalyst Center で、ソフトウェアイメージ、PSIRT、およびネットワークプロファイルなど、コンプライアンスのさまざまな側面の規則遵守要件を満たさないデバイスを簡単に特定できます。

次のスケジュールオプションを使用して、コンプライアンスチェックを自動化したり、オンデマンドで実行したりできます。

- コンプライアンスチェックの自動化：

  Catalyst Center でデバイスから収集された最新のデータを使用します。このコンプライアンスチェックは、インベントリや SWIM などさまざまなサービスからのトラップと通知をリッスンして、データを評価します。

- 手動コンプライアンスチェック：

  Catalyst Center でコンプライアンスを手動でトリガーできるようにします。

- スケジュールされたコンプライアンスチェック：

  スケジュールされたコンプライアンスジョブは毎日午後 11:00 に実行され、過去 7 日間コンプライアンスチェックを受けていないデバイスのコンプライアンスチェックをトリガーします。

Catalyst Center は現在、以下のタイプのコンプライアンスチェックをサポートしています。

- ネットワークデバイスで設定を実行するときに、そのデバイスに対して Catalyst Center が保持するスタートアップ設定ビューと異なる場合のコンプライアンスエラーのフラグを設定します。
- ゴールデンイメージがネットワークデバイスで実行されていないことを示すソフトウェアイメージコンプライアンスのフラグを設定します。
- SD-Access ファブリックワークフローによって展開された設定が改ざんされていて、アウトオブバンド PSIRT コンプライアンスに違反している場合、ファブリック コンプライアンス エラーとしてフラグを設定し、ネットワークに脆弱性が存在することをネットワーク管理者に警告します。
- Catalyst Center で特定のサイトに対して呼び出されたインテントに従ってデバイスが設定を実行していない場合、ネットワーク コンプライアンス アラートが表示されます。

詳細については、『Cisco Catalyst Center ユーザーガイド』の「ネットワークデバイスのコンプライアンス監査」を参照してください。

設定のばらつき

設定のばらつきは、ネットワークデバイスの実際の構成設定が、時間の経過とともに意図した状態や事前定義された状態から逸脱する場合に発生します。多くの場合、ITES 組織ではコンプライアンス要件により、すべてのネットワークデバイスについて設定のアーカイブを維持する必要があります。Catalyst Center は設定のばらつきに対するサポートを提供し、ユーザーがデバイス設定の変更を追跡およびモニターできるようにします。この機能を使用すると、ユーザーは各デバイスの現在の設定を確認し、前月からの変更履歴を分析して、時間の経過とともに特定のデバイスの設定がどのように変化したかを把握できます。

詳細については、『Cisco Catalyst Center ユーザーガイド』の「デバイスの構成ドリフト」を参照してください。

業務効率

業務効率は ITES ビジネスにとって極めて重要であり、生産性、コスト効率、およびサービスの品質を直接向上させます。この効率性により、従業員の成果の最大化、デジタル トランスフォーメーションの取り組みの合理化、および評判とブランド価値の向上が可能になります。SD-Access は、業務効率に関する以下の重要な側面に対処します。

- 高可用性（HA）
- システムのレジリエンス
- レポート
- 効率的な障害対応

高可用性（HA）

高可用性（HA）は、ハードウェア障害やソフトウェアのバグなどの技術的な問題が発生している場合でも、システムとアプリケーションが最小限の中断でユーザーがアクセスできるようにする重要な要素です。次に、以下のコンポーネントで HA を実現するための概要を示します。

- ディザスタ リカバリ
- レジリエンスのあるネットワークアーキテクチャ
- フォールバックセグメント

ディザスタ リカバリ

ITES 組織では、管理、制御、またはデータプレーンの障害に対する許容度が低くなります。Catalyst Center は、クラスタ内とクラスタ間の両方のレジリエンスをサポートしています。Catalyst Center におけるディザスタリカバリの導入は、メインサイト、リカバリサイト、および監視サイトの 3 つのコンポーネントで構成されます。メインサイトとリカバリサイトは、常にアクティブまたはスタンバイのいずれかのロールで運用されます。アクティブサイトでネットワークを管理する一方、スタンバイサイトでは、アクティブサイトで継続的に更新されるデータとマネージドサービスの最新のコピーが維持されます。アクティブサイトがダウンすると、Catalyst Center で自動的にフェールオーバーが開始され、スタンバイサイトを新しいアクティブサイトにするために必要なタスクが実行されます。

詳細については、『Cisco Catalyst Center 管理者ガイド』の「ディザスタリカバリの実装」セクションを参照してください。

レジリエンスのあるネットワークアーキテクチャ

SD-Access のレジリエンス ネットワーク アーキテクチャは、可用性と信頼性の高いインフラストラクチャを提供するように設計されています。これにより、中断期間中も重要なサービスの運用を維持できます。

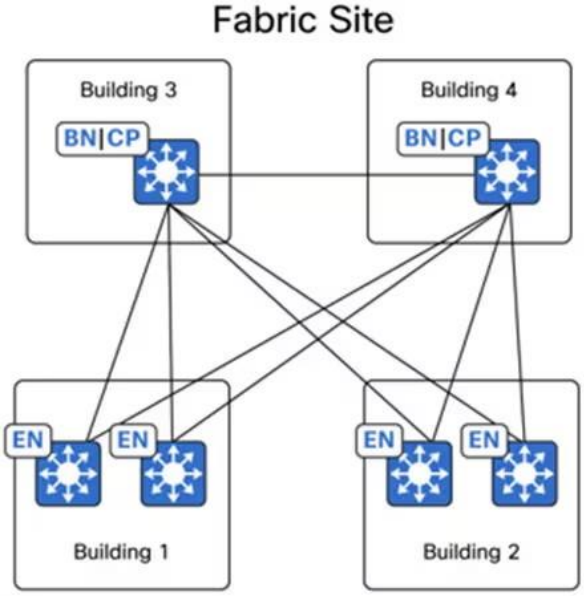
- SVL では仮想スイッチングシステム（VSS）と同様に、コントロールおよび管理プレーンレベルで 2 台の物理スイッチを単一の論理スイッチに統合することで、レイヤ 2 の運用がシンプル化されます。これにより、

スパニングツリープロトコルと First Hop Redundancy Protocol（FHRP）の要件、およびそれらの関連設定を削除できます。

- レイヤ 3 のルーテッドアクセスでは、レイヤ 2 とレイヤ 3 の境界がディストリビューション層からアクセス層に移行します。これにより、レイヤ 2 の隣接関係（アジャセンシー）と冗長化を管理するための、ディストリビューションおよびコラスプトコアレイヤへの依存度が軽減されます。

ITES ネットワークでは、スタッキングや SVL などの従来のレジリエンス方式に加えて、重要なアプリケーションがデータセンターへ継続的に接続できるよう、地域ハブやキャンパス本部で建物関連の障害からの保護が必要となります。

図 8.　　レジリエンスネットワーク設計の例



Cisco SD-Access は、ファブリックボーダーを単一のファブリックサイトの下に統合しつつ、異なる物理サイトに配置することを可能にする、柔軟な展開アーキテクチャを提供します。図に示すように、建物 1 ～ 4 は同じファブリックサイトに属しており、コロケートされたボーダーノードとコントロールプレーンノードが異なる建物に配置されています。Cisco SD-Access では、これらのボーダーノード展開で柔軟に優先順位を指定できます。これにより、ボーダーノードに優先順位を設定でき、つまりトラフィックのアクティブボーダーとして専用で使用できます。建物で障害が発生した場合、代替の建物にあるボーダーノードは、エッジノードからのすべてのトラフィックをシームレスに引き継ぐことができます。

フォールバックセグメント

Cisco SD-Access では、WAN の障害などによって ISE サーバーへの接続が失われた場合でも、端末が最小限のネットワーク接続レベルを維持できるようにする、クリティカル VLAN 機能をサポートしています。すでにオンボーディングされている有線クライアントにおいて、ISE ポリシーサービスノードへの接続が失われた場合、システムは定期的な再承認を一時停止して、認証パスの中断がデータプレーンに影響を与えないようにします。オンボーディングされていないクライアントでは、ISE への接続が失われた場合、クリティカル VLAN 機能によって特定の VLAN に割り当てられ、ネットワークに制限付きでアクセスできます。

これらのクリティカル VLAN では、ISE が存在しない場合にマイクロセグメンテーションを使用してポリシーを適用できますが、これを実現するには、VLAN-SGT マッピングをはじめとするクリティカル VLAN のエニーキャストゲートウェイのプロビジョニング時にセキュリティグループを割り当て、ダウンロードされる適切なポリシーマトリックスをスイッチに設定します。要約すると、SD-Access のクリティカル VLAN では、デバイスが正しく認証できない場合でも、ネットワークから完全に切断されることはありませんが、修復および障害対応のためにアクセスが制限されています。

システムのレジリエンス

システムのレジリエンスを確保するには、ネットワーク インフラストラクチャの重要なコンポーネントに高可用性（HA）および冗長化のソリューションを導入することが重要です。次に、以下のコンポーネントでこれを実現する方法の概要を示します。

- Catalyst Center HA
- ISE HA
- シスコ ワイヤレス LAN コントローラの冗長化

Catalyst Center HA

Catalyst Center の HA は、ダウンタイムを最小限に抑え、ネットワークのレジリエンスを向上させるように設計された機能です。これにより、ハードウェアまたはソフトウェアの障害時に重要なサービスが利用可能であり続けます。Catalyst Center の HA では通常、ハードウェアおよびソフトウェアの冗長構成を展開して、フェールオーバーがシームレスに進み、運用を継続できます。これにより、組織は予期せぬイベントが発生した場合でも、ネットワークの安定性と信頼性を維持できます。

詳細については、『Cisco Catalyst Center ハイアベイラビリティガイド』を参照してください。

ISE HA

Cisco ISE は、次の 2 つの主な設定で展開できます。

- スタンドアロン展開：

  スタンドアロン展開では、単一の ISE ノードが、管理、ポリシーサービス、モニタリングなど必要なすべての機能を提供します。この設定は、単一のノードでワークロードを処理でき、冗長化が重要な要件ではない小規模ネットワークに適しています。

- 分散型の展開：

  分散型の展開では、ISE ノードは複数の物理マシンまたは仮想マシンに分散され、拡張性、冗長性、および高可用性（HA）を実現します。この設定は、拡張性と冗長性が重要な大規模ネットワークに適しています。

各展開オプションには独自の利点があり、拡張性、冗長性、およびパフォーマンスに関するネットワークの特定の要件に基づいて選択されています。フェールオーバーをサポートし、パフォーマンスを改善するために、複数の Cisco ISE ノードを分散方式でセットアップできます。

詳細については、『Cisco Identity Services Engine インストールガイド』の「分散デプロイメント環境のシナリオ」を参照してください。

シスコ ワイヤレス LAN コントローラの冗長化

シスコ ワイヤレス LAN コントローラの冗長化は、ワイヤレスネットワーク サービスを継続的に維持する上で重要です。HA ペアセットアップでは、2 台のワイヤレスコントローラがペアとして設定されます。一方のワイヤレスコントローラはプライマリ（アクティブ）コントローラとして機能し、すべてのワイヤレス クライアントとトラフィックを管理します。もう一方のワイヤレス コントローラはセカンダリ（スタンバイ）コントローラとして機能します。セカンダリコントローラは、プライマリコントローラの設定および状態と同期し続けています。

プライマリコントローラで問題が発生した場合、セカンダリコントローラがシームレスに引き継ぎ、中断のないワイヤレスサービスが保証されます。この冗長性機能では、ワイヤレスコントローラのハードウェアまたはソフトウェアの障害時にフェールオーバー機能が提供され、ワイヤレスネットワークの信頼性が大幅に向上しています。その結果、ユーザー体験で中断が最小限に抑えられ、ワイヤレスネットワークへの接続が維持されます。

詳細については、『Cisco Catalyst 9800 Series Wireless Controllers High Availability SSO Deployment Guide』を参照してください。

レポート

Catalyst Center レポート機能には、ネットワークの運用効率に関する実用的な洞察を得るための包括的なツールスイートが用意されています。この機能により、柔軟なスケジュール設定と構成オプションを使用して、複数形式でデータを生成できるため、特定の運用ニーズに合わせてカスタマイズできます。

レポート機能は、次のようなさまざまなユースケースをサポートしています。

- キャパシティ プランニング：

  ネットワーク内のデバイスの使用率を把握します。

- パターン変更分析：

  クライアント、デバイス、バンド、アプリケーションなどの使用パターンの変更を追跡します。

- 運用レポート：

  アップグレードの完了やプロビジョニングの失敗などのネットワーク運用に関するレポートを確認できます。

- ネットワークの正常性評価：

  詳細なレポートを通じてネットワークの全体的な正常性状態を評価します。

Catalyst Center のレポート機能を活用することで、ネットワークの運用効率が大幅に向上し、スムーズな稼働でパフォーマンスの高いネットワーク環境が保証されます。

詳細については、『Cisco Catalyst Center プラットフォーム ユーザーガイド』の「レポート」セクションを参照してください。

効率的な障害対応

効率的な障害対応は、ITES 顧客の事業運営をサポートする上で不可欠なコンポーネントです。Catalyst Center は、これらのニーズを効果的に満たすよう設計された包括的なデバッグ機能を提供します。これらの機能により、IT 管理者は Catalyst Center の問題を迅速に特定、診断、および解決することができ、ネットワーク インフラストラクチャの継続的かつ最適なパフォーマンスが保証されます。障害対応には次のツールが役立ちます。

- 検証ツール：

  Catalyst Center 2.3.5.x より前は、監査およびアップグレード準備状況分析ツール（AURA）によってクラスターのアップグレードの準備状況を評価していました。2.3.5.x で完全に導入された制限付きシェルにより、ほとんどの AURA アップグレードチェックが Catalyst Center で実行されるようになりました。検証ツールは、Catalyst Center アプライアンスハードウェアと接続された外部システムの両方をテストし、ネットワークに重大な影響を与える前に対処する必要がある問題を特定します。

  詳細については、次のマニュアルを参照してください。

  - Cisco DNA Center のアップグレード準備の検証
  - 検証ツールの使用
  - System Analyzer ツールの使用

- System Analyzer：

  障害対応のニーズに対処するために、System Analyzer ツールによってログファイルを効率的に取得できます。Catalyst Center と接続されたネットワークコンポーネントの最適な機能と信頼性を確実に維持できるよう、System Analyzer は包括的な評価と診断を行います。System Analyzer の機能をモニタリング、診断、パフォーマンスの最適化に活用することで、組織は業務効率を向上させ、セキュリティ基準のコンプライアンスを維持し、信頼性の高い ITES サービスを提供することができます。

全体として、Catalyst Center の検証ツールと System Analyzer は、ITES ネットワーク管理者にとって非常に重要な資産です。これらのツールにより、能動的なメンテナンス、効率的な障害対応、およびネットワークの安定性の向上が可能になり、ITES の業務効率が大幅に向上します。

財務効率

運用コストを削減して収益を増加させることは、ITES ビジネスにとって重要な優先事項です。大規模なマルチサイトネットワークの展開とモニタリングを自動化することで、ITES 組織は運用コストを大幅に削減し、管理プロセスを合理化して、効率的な IT 運用を維持することができます。このアプローチにより、複雑なネットワークであっても手動の介入を最小限に抑えて管理できるようになり、全体的な生産性と収益性が向上します。

次に、ITES 組織で財務効率を達成するために活用されるアプローチの一部を示します。

- 自動化およびモニタリング
- IP アドレス管理の統合
- IT サービス管理の統合
- SD-Access 拡張

自動化およびモニタリング

自動化とモニタリングは、現代の IT インフラストラクチャ管理に不可欠な要素です。自動化には、ソフトウェアの展開、設定の管理、システムのプロビジョニング、ワークフローのオーケストレーションなどのタスクを含めることができます。反復的な時間のかかるタスクを自動化することで、組織は効率を向上させ、エラーを削減し、人的リソースを解放して、より戦略的な活動に集中できます。一方で、モニタリングでは、IT システム、ネットワーク、アプリケーション、およびサービスのパフォーマンスと正常性を継続的に観察および分析します。

次に、以下のコンポーネントに対してこれらの戦略を導入する方法の概要を示します。

- LAN の自動化
- プラグアンドプレイ（PnP）および返品許可（RMA）
- ソフトウェアイメージの管理
- インテリジェントキャプチャ
- アシュアランスと可視性

LAN の自動化

Catalyst Center の LAN 自動化は、ネットワークデバイスの設定とプロビジョニングを自動化することにより、ネットワーク インフラストラクチャの展開と管理を簡素化するように設計された機能です。この自動化により、複雑な手動設定によるエラーの可能性が軽減され、より効率的で信頼性の高いネットワーク運用が実現します。

シスコの LAN 自動化には、主に以下のような利点があります。

- ゼロタッチプロビジョニング：

  ネットワークデバイスが動的に検出およびオンボーディングされ、工場出荷時の状態からネットワークに完全に統合されるまでが自動化されます。

- エンドツーエンドのトポロジ：

  新しいネットワークシステムとその物理的接続を検出するように、ダイナミック検出をモデル化してプログラミングすることができます。それらの新しいシステムをレイヤ 3 IP アドレッシングおよびルーティングプロトコルを使用して自動化し、エンドツーエンドのルーティングトポロジを動的に構築できます。

- レジリエンス：

LAN 自動化には、転送トポロジと冗長性を最適化するシステムとネットワークの設定パラメータが統合されています。LAN 自動化でシステムレベルの冗長性を確保し、ベストプラクティスを自動的に適用することで、計画的または計画外のネットワーク停止時もクラス最高水準のレジリエンスが提供されます。

- セキュリティ

  シスコ推奨のネットワークアクセスおよびインフラストラクチャの保護パラメータが自動的に適用され、最初の導入時点からセキュリティが提供されます。

- コンプライアンス：

  LAN 自動化によって人的ミスや設定の誤りが排除され、IT リソースの浪費につながるルールや設定の不整合を減らすことができます。新しいシステムのオンボーディング時、LAN 自動化で Catalyst Center のグローバルに管理されるパラメータを自動化することにより、ネットワーク インフラストラクチャ全体でコンプライアンスが確保されます。

詳細については、『Cisco Catalyst Center SD-Access LAN 自動化導入ガイド』を参照してください。

プラグアンドプレイ（PnP）および返品許可（RMA）

Catalyst Center は、Cisco Catalyst スイッチ、ルータ、およびワイヤレス AP の展開を簡素化するプラグアンドプレイ（PnP）機能を備えています。PnP を使用すると、ネットワーク管理者は、手動設定なしで新しいデバイスをネットワークに簡単にオンボーディングできます。PnP 機能を備えたデバイスは、Catalyst Center などの PnP サーバーから必要なソフトウェアイメージと設定を自動的にダウンロードできるため、展開プロセスが迅速かつ効率的になります。

Catalyst Center は、返品許可（RMA）プロセスをサポートします。ハードウェア障害または交換の場合、管理者は RMA 機能を使用して障害のあるデバイスの返品と交換を簡単に管理できます。これには、RMA リクエストの生成、RMA のステータスの追跡、および一元化されたインターフェイスを介した交換プロセスの管理が含まれます。全体として、Catalyst Center の PnP および RMA 機能により、デバイスの展開と交換のプロセスが合理化され、複雑さが軽減されて、ネットワーク管理効率が向上します。

詳細については、『Network Device Onboarding for Cisco Catalyst Center Deployment Guide』を参照してください。

ソフトウェアイメージの管理

Catalyst Center のソフトウェアイメージ管理（SWIM）機能は、ネットワーク内の Catalyst スイッチ、ルータ、およびワイヤレスデバイス全体におけるソフトウェアイメージの管理プロセスをシンプル化および自動化します。ブランチやキャンパスで Catalyst 9000 シリーズ スイッチのアップグレードを自動化するネットワーク管理者は、Catalyst Center SWIM ソリューションを使用できます。

Catalyst Center はネットワーク内のデバイスのイメージタイプとバージョンに従い、固有のソフトウェアイメージをすべて保存します。SWIM を使用すると、ソフトウェアイメージを表示、インポート、および削除したり、ネットワークのデバイスにプッシュしたりできます。ソフトウェアアップグレードは、ソフトウェアの配布とアクティブ化を切り離して、メンテナンスウィンドウ内のダウンタイムを最小限に抑えることで最適化できます。全体として、SWIM は、Catalyst デバイス全体のソフトウェアイメージの管理を簡素化および自動化することで、運用効率を向上させ、ダウンタイムを短縮し、ネットワークのセキュリティとコンプライアンスを維持できます。

詳細については、『SWIM Deployment Guide』を参照してください。

インテリジェントキャプチャ

Catalyst Center インテリジェントキャプチャ（iCap）は、ネットワークの障害対応とパフォーマンスのモニタリングを強化するために設計された強力な機能です。高度な分析と機械学習を活用して、ネットワークトラフィックとクライアントの動作に関する詳細な洞察が提供されます。iCap は、Catalyst Center と AP 間の直接

通信リンクをサポートしているため、各 AP は Catalyst Center と直接通信できます。Catalyst Center はこのチャンネルを使用して、パケットキャプチャ（PCAP）データ、AP とクライアントの統計情報、およびスペクトルデータを受信できます。gRPC を介した AP から Catalyst Center への直接リンクにより、iCap では、ワイヤレスコントローラからは入手できない AP のデータにアクセスできます。

詳細については、『Cisco Intelligent Capture Deployment Guide』を参照してください。

アシュアランスと可視性

Catalyst Center は、ネットワークのデバイスとサービスを自動化することでネットワークを管理し、ネットワークのアシュアランスと分析の機能を提供します。Catalyst Center は、ネットワークデバイス、Cisco ISE、ユーザー、端末、アプリケーション、およびネットワーク全体のその他の統合からテレメトリを収集します。Catalyst Center のネットワーク分析は、さまざまなソースからのデータを関連付けて、管理者やオペレータが次の包括的なネットワークインサイトを提供できるようにします。

- デバイス 360 およびクライアント 360：

  さまざまな時間や各種のアプリケーションからの、デバイスまたはクライアントの接続（トポロジ、スループット、および遅延に関する情報を含む）を表示します。

- ネットワークタイムトラベル：

  過去にさかのぼって、ネットワークの問題の原因を確認する機能です。

- アプリケーション体験：

  コアビジネスにとって重要なアプリケーションを、ユーザー単位でこれまでにないレベルにまで可視化し、それらのパフォーマンスを制御します。

- ネットワーク分析：

  ネットワークで見つかった問題に対する修正処置についての推奨事項を提供します。これらのアクションには、ネットワーク管理者が実行する手順をエンジンにより指定するガイド付き修復が含まれる場合があります。

詳細については、『Cisco Catalyst Assurance User Guide』を参照してください。

IP アドレス管理の統合

Catalyst Center における IP アドレス管理（IPAM）の統合により、ネットワーク内の IP アドレスを管理するプロセスが合理化されます。この統合により、IP アドレスの割り当て、追跡、および管理を自動化および簡素化するための中央集中型プラットフォームが提供されます。SD-Access 展開では、IPAM の統合により、既存の IP アドレス範囲への Catalyst Center のアクセスが提供されます。Catalyst Center で新しい IP アドレスプールを設定すると、IPAM サーバーが自動的に更新されるため、IP アドレスの管理タスクが軽減されます。

Catalyst Center には、IPAM プロバイダー Infoblox 用と Bluecat 用の 2 つのサードパーティ統合モジュールが含まれています。他の IPAM プロバイダーは、Catalyst Center IPAM プロバイダーの仕様を満たす IPAM プロバイダー REST API サービスを提供することで、Catalyst Center で使用するように設定できます。

詳細については、「IP アドレスマネージャの設定」を参照してください。

IT サービス管理（ITSM）の統合

IT サービス管理（ITSM）とは、ビジネスのニーズを満たす高品質の IT サービスの導入と管理を指します。ServiceNow は、組織が IT サービスを自動化および合理化できるようにする一連のアプリケーションを提供する人気のある ITSM プラットフォームです。

Catalyst Center と ServiceNow の統合により、次の機能がサポートされます。

- Catalyst Center を ITSM のインシデント、イベント、変更、および問題管理プロセスに統合します。

- Catalyst Center を ITSM の承認および事前承認チェーンに統合します。
- Catalyst Center を正式な変更およびメンテナンス ウィンドウ スケジュールに統合します。

統合の範囲は、主に、アシュアランスとメンテナンスの問題がないか、およびコンプライアンス、セキュリティ、その他の運用でのトリガーのためにソフトウェアイメージを更新する必要があるイベントがないか、ネットワークをチェックするためのものです。これらの問題に関する詳細は、ITSM（ServiceNow）システムまたは REST エンドポイントに公開されます。

詳細については、『Cisco Catalyst Center ITSM 統合ガイド』を参照してください。

SD-Access 拡張

SD-Access 拡張機能は、組織が SD-Access ファブリックの範囲を拡張できるようにする重要な機能です。これにより、より広範な環境とデバイスで一貫したポリシーの適用、セキュリティの強化、管理の簡素化、およびネットワークパフォーマンスの向上が実現します。

拡張ノードはレイヤ 2 モードで SD-Access に接続するため、IoT エンドポイントの接続が容易になりますが、ファブリックテクノロジーはサポートされていません。Catalyst Center を使用すると、拡張ノードを PnP で接続して工場出荷時のリセット状態からオンボーディングすることができます。これにより、拡張ネットワークでのセキュリティ制御が有効になり、拡張ノードに接続されているエンドポイントにファブリックポリシーが適用されます。

SD-Access 拡張機能を導入するにあたり、企業の管理者は次の 3 つの異なるタイプで使用可能な拡張ノードを展開できます。

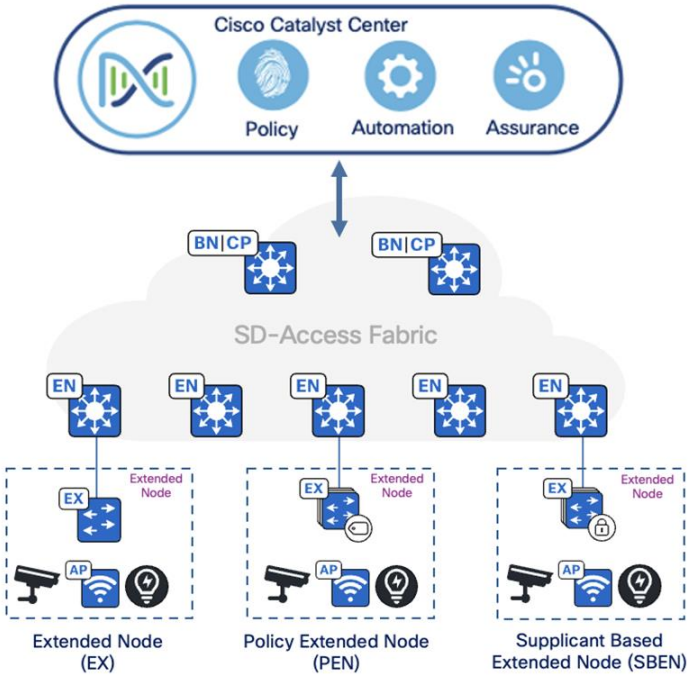
- 拡張ノード（EX）：
  拡張ノードは、Cisco SD-Access ネットワークのファブリックエッジノードに接続するレイヤ 2 スイッチです。SD-Access 機能をすべてサポートしているわけではない IoT エンドポイントおよびその他のデバイスの接続を提供します。拡張ノードは通常、Catalyst Center のような集中型コントローラを使用して管理および設定されます。LISP、VXLAN、SGACL の適用などの高度なネットワーク機能について、ファブリックエッジに依存しています。
- ポリシー拡張ノード（PEN）：
  ポリシー拡張ノードは、追加の機能を提供する特定のタイプの拡張ノードです。802.1X/MAB 認証を実行し、VLAN と SGT を端末に動的に割り当て、SGACL を適用することができます。このタイプのノードでは、標準の拡張ノードに比べて詳細なレベルのポリシー制御が提供されるため、より柔軟なネットワークのセグメンテーションとセキュリティ設定が可能になります。
- SBEN：
  SBEN は、より厳格なオンボーディングプロセスを実行する拡張ノードです。これには、IEEE 802.1X サプリカントの設定が必要であり、完全な認証と承認のプロセスが完了してから、SD-Access ネットワークへの導入が許可されます。この方法では、承認されたデバイスのみがネットワークにアクセスできるようにすることで、セキュリティを強化できます。SBEN は、多くの場合、セキュリティ要件が強化された環境で使用されます。

重要なポイント：

- 拡張ノードは、SD-Access に直接参加できない端末に対して接続を提供します。
- PEN はポリシー適用機能を強化します。
- SBEN によって、802.1X 認証を介したより厳格なセキュリティ対策を導入できます。

図 9 は、拡張ノード（EX）、ポリシー拡張ノード（PEN）、および SBEN を使用した企業ネットワークを示しています。

図 9.　　SD-Access ネットワーク内のさまざまなタイプの拡張ノード



- 詳細については、『Cisco Software-Defined Access Solution Design Guide』の「Extended node design」セクションを参照してください。
- 拡張ノードと PEN の詳細については、『Connected Communities Infrastructure - General Solution Design Guide』を参照してください。

エクスペリエンスの向上

最新のテクノロジーを戦略的に使用してユーザーエクスペリエンスとカスタマーエクスペリエンスを向上させるには、QoS を優先し、アプリケーションの可視性を活用するとともに、ビデオストリーミングを導入する必要があります。これは特に、パフォーマンスが事業運営や顧客満足度に直接影響を与える環境に当てはまります。今日の競争環境において、QoS を優先することは単なる選択肢ではなく、優れたユーザー体験および顧客体験を提供するために必要です。

次に、これらの領域を強化するための戦略を概説します。

- QoS
- アプリケーションの可視性
- サイトをまたがるビデオ ストリーミング

QoS

QoS は、選択したタイプのネットワーク通信に対してサービスの優先順位付けや差別化を行うネットワーク機能を指します。QoS を設定することで、ネットワークリソースが効率的に利用されると同時に、企業レベルの音声品質の確保や、ビデオの高い Quality of Experience（QoE）の提供などのビジネス目標を達成できます。Catalyst Center は、アプリケーションポリシーを介したネットワークでの QoS の設定を容易にします。

これらのポリシーには、次のコアパラメータが含まれています。

- アプリケーション セット：

  類似のネットワークトラフィック要件を持つアプリケーションのグループ。各アプリケーション セットには、トラフィックの優先順位を決定するビジネスとの関連性グループ（ビジネス関連、デフォルト、またはビジネ

スと無関係）に分類されます。各グループの QoS パラメータは、Cisco Validated Design（CVD）に従って定義され、特定のビジネス目標に合わせて調整を行えます。

- サイトの範囲：

  アプリケーション ポリシーが適用される範囲を定義します。たとえば、有線ポリシーは指定されたサイト範囲内のすべての有線デバイスに適用され、ワイヤレスポリシーは定義された範囲内の特定のサービスセット識別子（SSID）を使用するデバイスに適用されます。

アプリケーションの可視性

アプリケーションの可視性は、ネットワーク管理者が対象ネットワーク上で実行されているアプリケーションを確認し、そのパフォーマンスをモニターして、ネットワークリソースがどのように使用されているかを把握できる機能です。これは、最適なネットワークパフォーマンスを維持し、セキュリティを確保し、ユーザー体験を向上させるために重要です。

Catalyst Center を使用すると、ネットワークを通過するアプリケーションデータを管理し、洞察を得ることができます。これには、組み込みアプリケーション、カスタムアプリケーションの特定、およびネットワークトラフィックの分類が含まれます。アプリケーション可視性サービスは、Catalyst Center 内でアプリケーションスタックとしてホストされているため、特定のデバイスでコントローラベースのアプリケーション認識（CBAR）機能を有効にして、数千のネットワークと自社製のアプリケーションおよびネットワークトラフィックを分類することができます。

アプリケーションの可視性は、詳細なパケット検査、フロー分析、およびアプリケーション認識テクノロジーを組み合わせにより実現し、ネットワーク アクティビティとアプリケーション パフォーマンスの包括的なビューを提供します。CBAR を導入することで、組織は重要なアプリケーションを最適に動作させることができるため、全体的な生産性とユーザーの満足度が向上します。

次のパッケージをインストールできます。

- Application policy：

  キャンパスやブランチ内の LAN、WAN、およびワイヤレスで QoS ポリシーを自動化できます。

- Application registry：

  アプリケーションとアプリケーションセットを表示、管理、および作成できます。

- Application visibility service：

  Network-Based Application Recognition（NBAR）および CBAR の技術を使用してアプリケーションを分類できます。

サイトをまたがるビデオ ストリーミング

ITES 組織は、さまざまな地域に所在する複数の分散拠点全体で定期的な従業員トレーニングセッションを実施する必要があります。これらのトレーニングセッションには、プレゼンテーション、デモンストレーション、およびインタラクティブな Q&A セッションのライブ動画配信が含まれます。ネットワークに大きな負荷をかけることなく、すべてのブランチに動画コンテンツを効率的に同時配信するために、組織はマルチキャストテクノロジーを利用します。

そうしたマルチキャストデータは、地域のデータセンターや企業のデータセンターなどのさまざまな送信元からストリーミングされます。Cisco SD-Access アーキテクチャは、エンドツーエンドのシームレスなマルチキャストデータ通信に必要な柔軟性を提供します。それにより、大規模な企業ネットワーク内のどこからでも、世界中の至るところにそれらの通信を流すことができます。Cisco SD-Access は、ヘッドエンド レプリケーション モードとネイティブ マルチキャスト モードの両方をサポートしており、SD-Access ファブリック内でも、またはその外部でも、マルチキャスト RP（ランデブーポイント）を柔軟に割り当てることができます。

SD-Access は、マルチキャスト通信を転送するための 2 つのトランスポート方法をサポートしています。一方はオーバーレイを使用する方法（ヘッドエンド レプリケーション）で、もう一方はアンダーレイを使用する方法（ネイティブマルチキャスト）です。

- ヘッドエンド レプリケーション

  ヘッドエンド レプリケーション（または入力レプリケーション）は、マルチキャスト送信元がファブリック オーバーレイ内にある場合はマルチキャスト ファーストホップ ルータ（FHR）によって、送信元がファブリックサイト外にある場合はボーダーノードによって行われます。

- ネイティブマルチキャスト：

  ネイティブマルチキャストでは、入力ファブリックノードでユニキャスト レプリケーションを行う必要はありません。代わりに、中間ノードを含むアンダーレイ全体が、レプリケーションを処理するために使用されます。ネイティブマルチキャストをサポートするには、ファーストホップルータ（FHR）、ラストホップルータ（LHR）、およびそれらの間にあるすべてのネットワーク インフラストラクチャ コンポーネントを有効にする必要があります。

SD-Access フレームワーク内でマルチキャストテクノロジーを活用することで、ITES 組織は大規模な従業員トレーニングセッションを効果的に実施でき、分散拠点全体でより良いコミュニケーションと学習を促進できます。

ネットワーク展開のオプション

次のセクションでは、ITES ネットワークの展開オプションについて説明します。

ファブリック サイト リファレンス モデル

物理的拠点への展開では、大規模なブランチ、地域ハブ、本社、小規模なリモートオフィスなど、さまざまなタイプのサイトごとに異なるテンプレートを使用できます。その根底にある設計上の課題は、既存のネットワーク展開と配線を調べ、これらのエリアで SD-Access ファブリックサイトを階層化する方法を提案することです。参照モデルのテンプレートを作成することで、このプロセスをシンプル化および合理化できます。テンプレートを使用すると、端末数と多次元の設計要素に基づくリファレンスカテゴリが得られるので、一般的なサイト設計を理解するのに役立つとともに、類似のサイズのサイトを設計するためのガイドラインが得られます。

各ファブリックサイトには、リストされているカテゴリから適切にサイズ設定された、コントロールプレーンノード、エッジノード、ボーダーノード、およびワイヤレスコントローラのサポートセットが含まれます。また、存続可能性の要件を満たすために、ISE PSN はサイト全体に分散されます。

ファブリックサイト参照モデルの一般的なタイプは次のとおりです。

- FIAB サイト
- 小規模サイト
- 中規模サイト
- 大規模サイト

技術的なヒント： これらの参照モデルは、価値のあるガイダンスを提供します。特定のネットワークの要件および制約事項に基づいて、調整が必要になる場合があります。SD-Access ファブリックの最適な展開を実現するために、ネットワーク設計の専門家に相談してください。

詳細については、『 Cisco SD-Access Solution Design Guide』を参照してください。

FIAB サイト参照モデル

FIAB サイト参照モデルは、通常 1000 個未満のエンドポイントをサポートする小規模な大学キャンパスまたはリモートサイト向けに設計されています。この設計の中心となるコンポーネントは、コントロールプレーンノード、ボーダーノード、およびエッジノードの 3 つのファブリックロールをすべて担うスイッチスタックまたは SVL です。スイッチスタック FIAB 展開では、一般に SD-Access 組み込み型ワイヤレスを使用してサイトローカル ワイヤレスコントローラ機能を提供します。サイトには、WAN またはインターネットの回線と遅延に応じて、ISE PSN も含まれる場合があります。

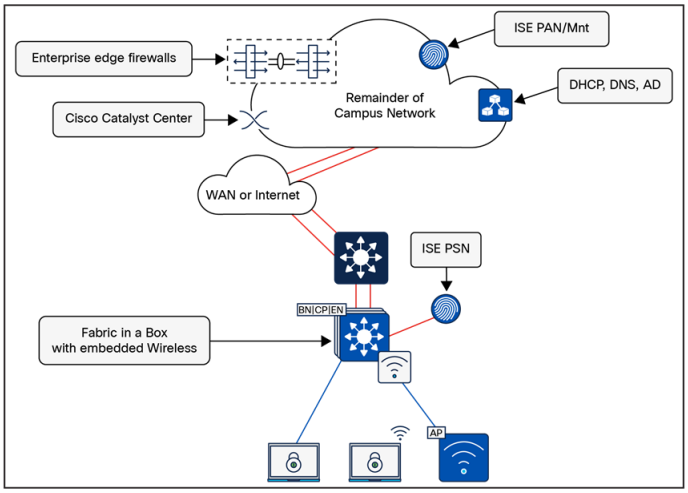
同様のサイト設計サイズに関するガイドラインについては、表 1 を参照してください。これらの数値は一般的な推奨値であり、このサイズのサイトで使用される特定のネットワークデバイスの制限を正確に表しているわけではありません。

表 1. FIAB サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	1000
コントロール プレーン ノード数	1
外部ボーダーノード数	1

ネットワーク要素	スケール
AP、ターゲットの上限	50

図 10.　　FIAB サイト設計の物理トポロジ



FIAB サイトに関する考慮事項：

- 端末数が少なく、結果として影響が大きくないため、高可用性（HA）とサイトの存続可能性は、ボックス設計のファブリックの一般的な要件ではありません。すべての参照設計では、DHCP、DNS、ワイヤレスコントローラ、および ISE などのサイトローカルサービスによってレジリエンスと存続可能性が向上しますが、複雑さが増し、サービスブロックなどの追加の機器が必要になります。
- この設計の HA は StackWise-480 または SVL を通じて提供され、いずれも複数の物理スイッチを 1 つの論理スイッチに結合します。シャーシベースのスイッチを使用する場合、デュアルスーパーバイザと電源によって冗長性が確保されます。
- ワイヤレスコントローラは、FIAB に直接接続された物理ユニットとして展開することも、組み込み Catalyst 9800 コントローラとして展開することもできます。スイッチスタックまたは冗長スーパーバイザを備えた組み込み Catalyst 9800 を使用すると、AP とクライアントのステートフル スイッチオーバー（SSO）が自動的に提供されます。

小規模サイト参照モデル

中規模サイト参照モデルは、複数の建物、または複数の配線用ボックスがある単一の建物向けに設計されており、通常は 10,000 未満の端末をサポートします。物理ネットワークは通常、コラプストコア/ディストリビューションレイヤとアクセスレイヤの 2 層設計です。

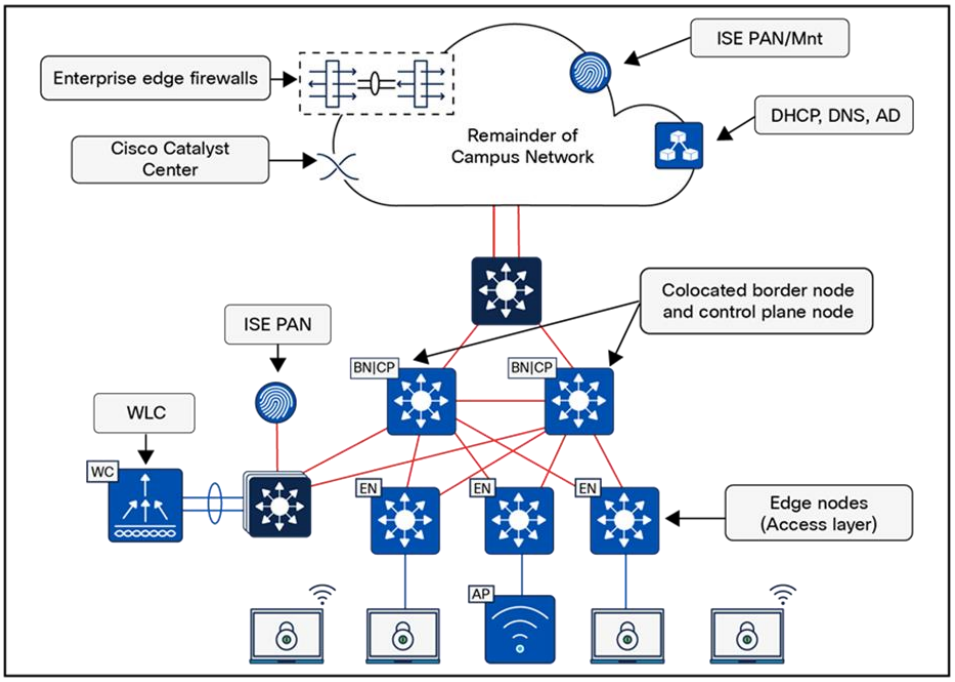
同様のサイトサイズの一般的な設計ガイドラインについては、表 2 を参照してください。これらの数値は基準点であり、このような設計で使用される特定のデバイスの制限を正確に表しているわけではありません。

表 2.　　小規模サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	10,000
ファブリックノード、ターゲットの上限	100

ネットワーク要素	スケール
コントロール プレーン ノード数	2
外部ボーダーノード数	2
AP、ターゲットの上限	500

図 11.　　小規模サイト参照設計の物理トポロジ



小規模サイトの考慮事項：

- 小規模な展開では、SD-Access ファブリックサイトは通常 2 階層設計を使用して実装されます。小規模なサイトでは、コラプストコアスイッチでボーダーおよびコントロールプレーンノードの機能を同じ場所に配置し、それらをペアとして展開することで高可用性が実現します。レジリエンスを確保し、オーバーレイとアンダーレイの両方に代替転送パスを提供するには、コラプストコアスイッチをクロスリンクで直接接続する必要があります。
- クライアントと AP の数のために、専用のワイヤレスコントローラを使用する必要があります。物理接続を介してワイヤレスコントローラの高可用性リンクを確立するために、サービスブロックが展開されます。ワイヤレスコントローラはレイヤ 2 ポートチャネルを介してサービス ブロック スイッチに接続し、冗長インターフェイスを確保します。サービスブロックは、スイッチスタックか SVL のいずれかで構成され、レイヤ 3 ルーテッドリンクを介して両方のコラスプトコアスイッチに接続します。DHCP、DNS、およびその他の共有サービスがサイトローカルである場合、サービスブロックは VRF 対応ピアとして展開される可能性があります。

中規模サイト参照モデル

中規模サイト参照モデルは、複数の建物、または複数の配線用ボックスがある単一の建物に適用され、通常は 50,000 未満の端末をサポートするように設計されています。物理ネットワークは、通常、コア レイヤ、ディストリビューション レイヤ、およびアクセス レイヤで構成される 3 階層アーキテクチャに従います。ボーダーおよびコントロールプレーンノードの機能は、同じ場所に配置したり、別々のデバイスに展開したりできます。

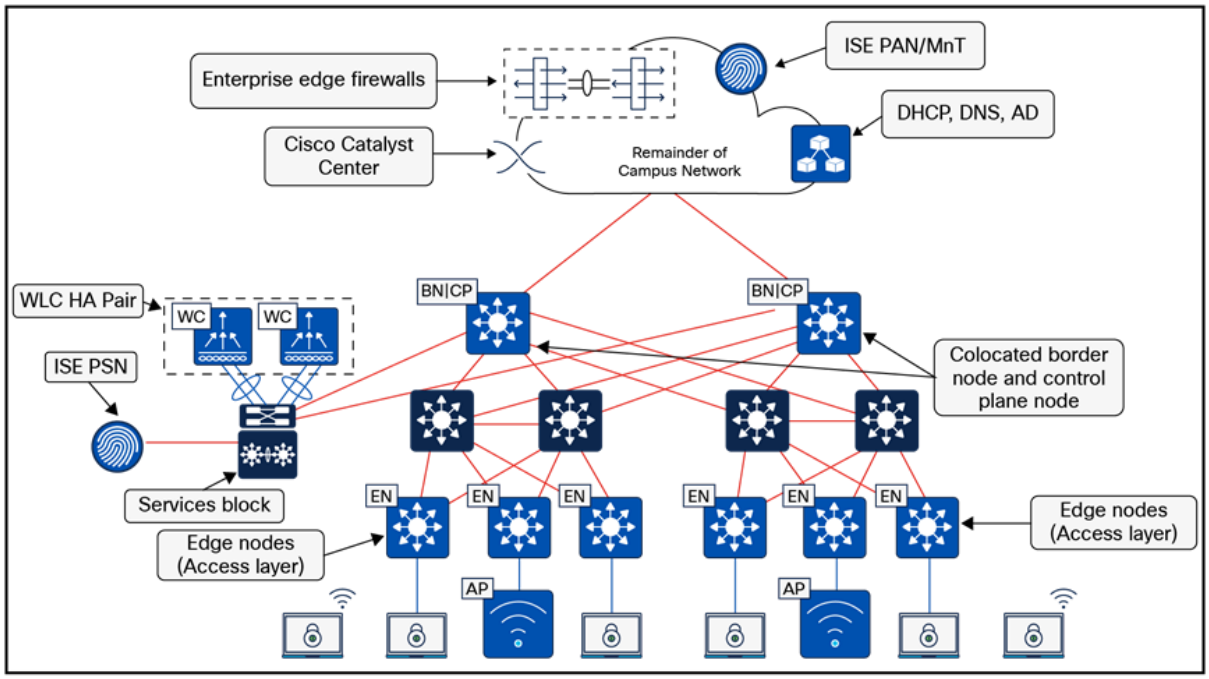
この規模のサイトの一般的な設計ガイドラインについては、表 3 を参照してください。これらの数値は推奨事項であり、特定のネットワークデバイスの制限を正確に表しているわけではありません。最大のエンドポイント

キャパシティをサポートするには、Cisco Catalyst Center の大規模アプライアンスが必要であり、場合によっては特大サイズのアプライアンスが必要になることもあります。

表 3. 中規模サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	50,000
ファブリックノード、ターゲットの上限	500
コントロールプレーンノード（FEW/SD-Access ワイヤレスの場合は最大 2 つ）	2 ～ 6
外部ボーダーノード数	2
AP、ターゲットの上限	2500

図 12. 中規模サイト参照設計の物理トポロジ



中規模サイトの考慮事項：

- 中規模サイトでは、オーバーレイとアンダーレイのレジリエンシと代替転送パスの両方について、アクセス層を除く所定のレイヤですべてのデバイスが相互にクロスリンクされている必要があります。複数のディストリビューション ブロックを相互に接続する必要はありませんが、ブロック内のすべてのディストリビューション スイッチに相互接続する必要があります。専用コントロールプレーンノードが使用される場合、通常はコアスイッチに接続され、さまざまなディストリビューション ブロック間でエッジノードの高い可用性が確保されます。最適な転送と冗長性を得るには、両方のコアスイッチに接続する必要があります。インターフェイスと光ファイバが使用可能な場合は、相互にクロスリンクすることもできますが、これは厳密な要件ではありません。
- 物理ワイヤレスコントローラは、ワイヤレスユーザースケールに対応できるように展開する必要があります。高可用性（HA）を有効にするには、ワイヤレスコントローラの HA-SSO ペアを、レイヤ 2 ポートチャネルを使用したサービスブロックへの冗長物理接続によって展開します。通常、サービスブロックは SVL として

動作する固定設定スイッチを用いて実装され、レイヤ 3 ルーテッドリンクを介してコアに接続されます。DHCP、DNS、およびその他の共有サービスがサイトローカルである場合、このサービスブロックは VRF 対応ピアとして機能する可能性があります。

大規模サイト参照モデル：

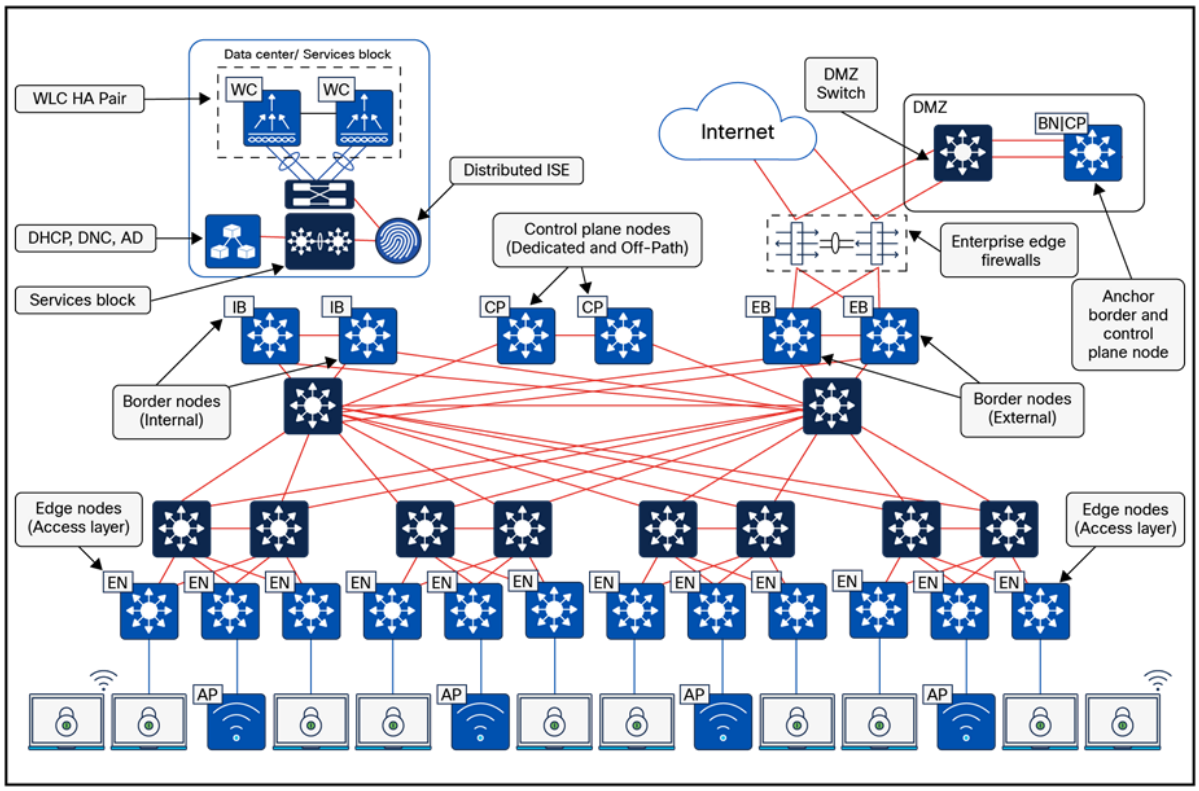
大規模サイト参照モデルは、複数の建物、または複数の配線用ボックスがある単一の建物に適用されます。通常、物理ネットワークは 3 階層アーキテクチャ（コア、ディストリビューション、およびアクセス）に従い、最大 100,000 の端末をサポートするように設計されています。

この規模のサイトの一般的な設計ガイドラインについては、表 4 を参照してください。これらの数値は基準点であり、特定の設計内の特定のデバイスの制限事項に対応していない場合があります。最大エンドポイントキャパシティをサポートするには、少なくとも特大規模の Cisco Catalyst Center アプライアンスが必要であり、特大規模の Catalyst Center アプライアンスの 3 ノードクラスタが必要になる場合があります。Cisco Catalyst Center データシートには、SD-Access ファブリックサイトの実装に使用されるさまざまなネットワーク インフラストラクチャ デバイスの拡張性に関する詳細が示されています。

表 4. 大規模サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	50,000
ファブリックノード、ターゲットの上限	500
コントロールプレーンノード（FEW/SD-Access ワイヤレスの場合は最大 2 つ）	2 ～ 6
ボーダーノード数（内部として 2 つ、外部として 2 つ） * 非常に例外的な設計シナリオでは、内部ボーダーノードの複数のペアが存在する可能性があります。	2 ～ 4*
外部ボーダーノード数	2
AP、ターゲットの上限	2500

図 13.　　大規模サイト参照設計の物理トポロジ



大規模サイトの考慮事項：

- 通常、Cisco Catalyst Center およびプライマリ ISE PSN は大規模サイトに展開されます。
- コントロールプレーンノードとボーダーノードは専用デバイスにする必要があり、通常は冗長ペアとして展開されます。専用コントロールプレーンノードを各コアスイッチに接続して、レジリエンスを確保し、冗長転送パスを提供する必要があります。インターフェイスと光ファイバが使用可能な場合は、コントロールプレーンノードを相互リンクすることを推奨します（必須ではありませんが、追加のアンダーレイ転送パスが提供されるため）。
- 1 つ以上のワイヤレスコントローラ HA-SSO ペアが、レイヤ 2 ポート チャネルを使用してサービスブロックへの冗長な物理接続で展開されます。サービスブロックは通常オンプレミス データセンター ネットワークの一部です。
- 内部専用ボーダーノードは、ファブリックサイトをデータセンターコアに接続するときによく使用されます。一方、外部専用ボーダーノードは、サイトを MAN、WAN、インターネットに接続するときに使用されます。ボーダーノードの数が増えると、SD-Access の管理負荷とルーティングの複雑さが増大するため、ネットワーク設計要件を満たす最小数のボーダーノードを展開することを推奨します。このサイトを外部リソースに接続するときには、冗長化された専用ルーティング インフラストラクチャとファイアウォールが使用されますが、ボーダーノードは、このインフラストラクチャとフルメッシュで相互接続される必要があります。
- 大規模なサイトには、ゲストワイヤレス用のアンカー付きファブリック ボーダーおよびコントロールプレーンノードが展開される緩衝地帯（DMZ）が含まれている場合があります。

分散キャンパス参照モデル向けの SD-Access

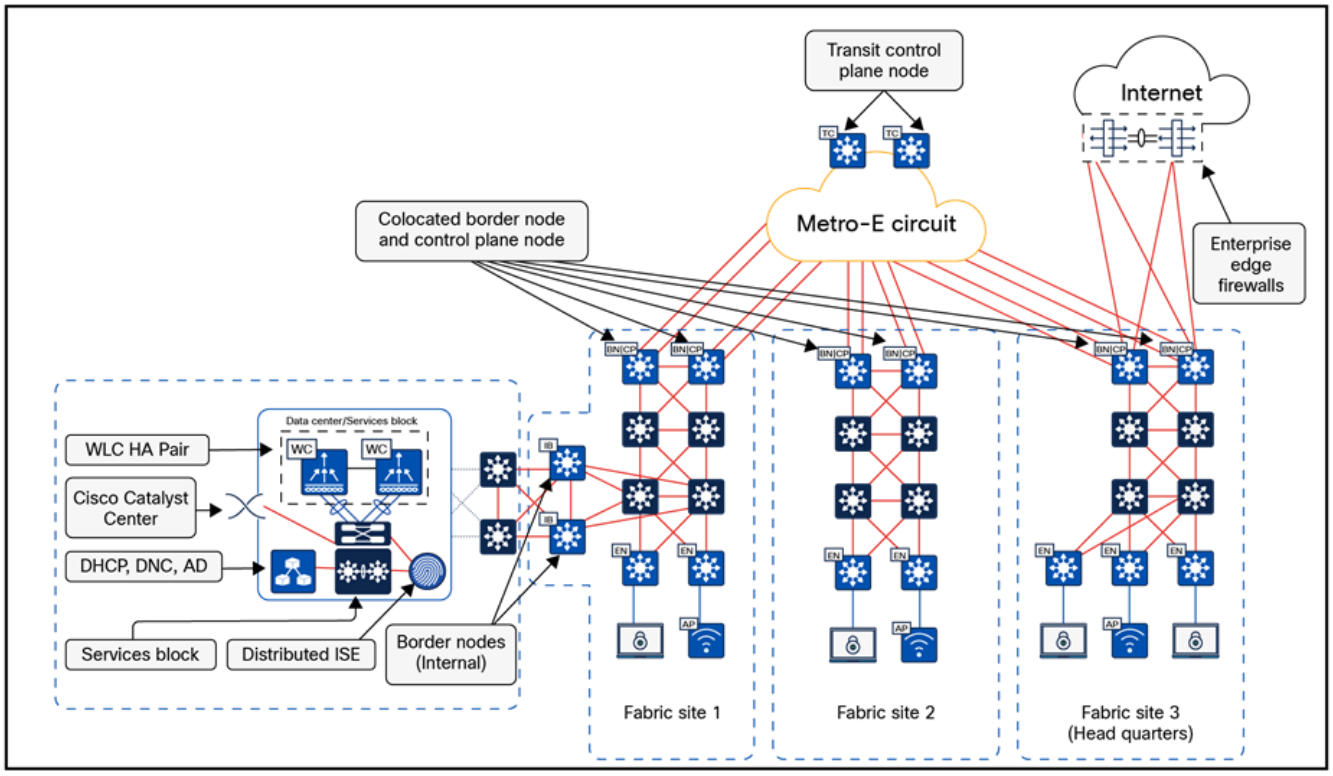
分散キャンパス向けの SD-Access は、サイト全体でセキュリティポリシー構造（VRF と SGT）を維持しながら、独立した複数のファブリックサイトを接続するソリューションです。LISP プロトコルを介したコントロールプレーンシグナリングは、ファブリック VXLAN カプセル化とともに、ファブリックサイト間で使用されます。これにより、マクロセグメンテーションとマイクロセグメンテーションのポリシー構成（それぞれ VRF および

SGT）が確実に保持されます。その結果、ネットワークはアドレス非依存状態のままであり、グループメンバーシップに基づいてエンドツーエンドポリシーが適用されます。

図 14 では、各ファブリックサイトは、メトロイーサネット（Metro-E）専用回線を介して接続されています。この展開は、同じ地理的エリア内に分散した複数の建物が存在する大規模な企業キャンパスを表しており、各建物は独立したファブリックサイトとして動作します。この回線に接続されているボーダーノードは、コントロールプレーンノードと同じ場所に配置された、外部ボーダーとして設定されます。IGP ピアリングが回線全体で行われ、デバイスのループバック インターフェイス（RLOC）間の IP 到達可能性が確立されます。Metro-E 回線は、ファブリックサイト間での SD-Access トランジットとして機能します。

本社ではインターネットに直接アクセスできますが、ファブリックサイト 1 では共有サービスがホストされているデータセンターに接続します。ファブリックサイト 1 の内部ボーダーノードがデータセンター プレフィックスをオーバーレイスペースにインポート（登録）すると、各ファブリックサイトの VN がこれらのサービスにアクセスできるようになります。インターネット向けトラフィックの場合、パケットは本部に戻ると、インターネットに出力する前に共通のセキュリティスタックを通過します。トランジット コントロールプレーン ノードは別のエリアに展開され、SD-Access トランジット Metro-E ネットワークを介してアクセスできますが、ファブリックサイト間のダイレクト転送パス上にはありません。

図 14.　　分散キャンパス参照設計向けの SD-Access の物理トポロジ



分散キャンパスに関する考慮事項：

- 分散キャンパスソリューションを構成するコアコンポーネントは、SD-Access トランジットノードとトランジット コントロール プレーン ノードです。これらのアーキテクチャ構造は、分散型キャンパス展開でのみ使用されます。SD-Access トランジットは、同じ都市、同じ WAN 上、または大規模企業キャンパス内の建物間にあるファブリックサイト間の物理ネットワーク接続として機能します。

技術的なヒント：　標準の 1,500 バイト MTU を使用した広範囲の展開では、クライアントや AP に接続された SVI で 1,250 などの小さな tcp adjust-mss 値を設定できます。UDP アプリケーションで tcp adjust-mss 値よりも大きい MTU 値が使用されている場合は、UDP アプリケーションサーバーで MTU 値を調整しま

す。また、TCP 以外の MTU を減らすために必要なアプリケーション制御通信が行われるように、ネットワーク全体で ICMP タイプ 3、コード 4 をエンドツーエンドで許可することを推奨します。

ワイヤレス設計

大学の設定においてシスコの SD-Access フレームワーク内でワイヤレスソリューションを設計する場合、シームレスな運用と管理を実現するために、複数のコンポーネントを設定して統合する必要があります。有線ネットワークに SD-Access ファブリックを導入している大学には、ワイヤレスアクセスを導入する際に 2 つのオプションがあります。

- SD-Access ワイヤレスアーキテクチャ
- Cisco Unified Wireless Network ワイヤレスオーバーザトップ

SD-Access ワイヤレスアーキテクチャ

ワイヤレス コントロールプレーンを有線のオーバーレイ コントロールプレーンと統合することで、Cisco SD-Access は独自の差別化要因を実現しています。Cisco SD-Access ワイヤレスは、分散データプレーンを備えたワイヤレスコントローラを介して集中型のコントロールおよび管理プレーンを提供し、優れた集中型ワイヤレス設計と分散型ワイヤレス設計の両方を実現できるようになっています。

ワイヤレスコントローラはコントロールプレーンノードと統合し、オンボーディング時にエンドポイントを登録し、ローミング時に位置を更新します。これは、ワイヤレス コントロール プレーンと有線コントロールプレーンの間に相乗作用が発生する最初のインスタンスです。有線とワイヤレスのこの独自の統合は、ネットワークユーザーと、それらをサポートする運用チームに、いくつかの利点をもたらします。

- 簡素化：

  ネットワークは、有線クライアントとワイヤレスクライアントの両方に対して単一のサブネットを持つことができます。

- ポリシーの一貫性：

  有線ポリシーをワイヤレス通信に拡張し、両方をエッジノードで適用します。

- パフォーマンスの向上：

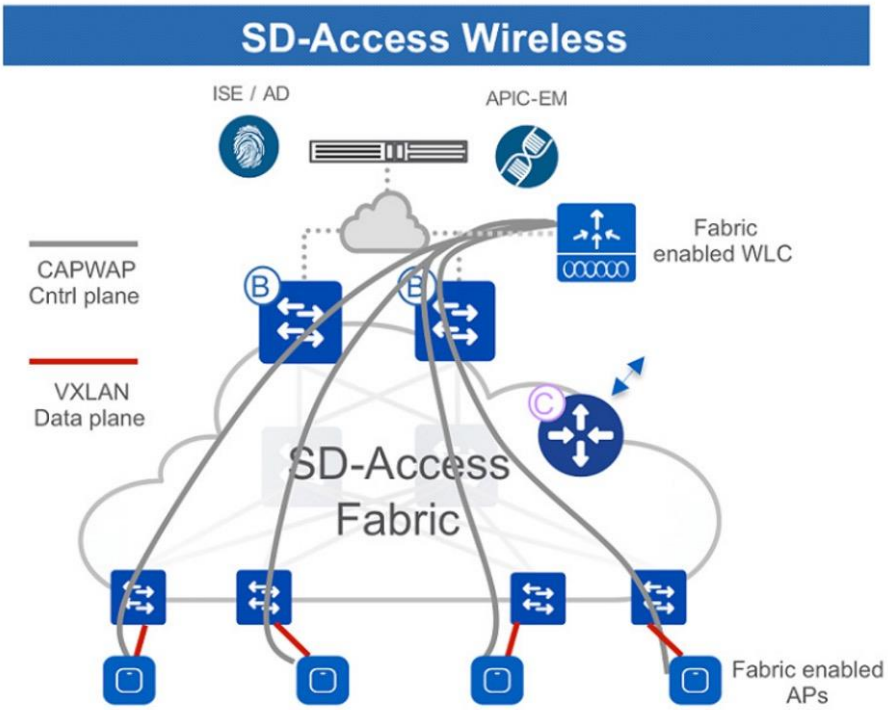
  ワイヤレスローミングはレイヤ 2 であり、いかなる形態のアンカーリングも必要ありません。

- 分散データプレーン：

  集中スイッチド ワイヤレス アーキテクチャに比べて、より高い全体的なワイヤレススループットを実現します。

図 15 は、Cisco SD-Access ワイヤレス内のコントロールプレーンとデータプレーンの通信フローを示しています。

図 15.　SD-Access ワイヤレスのコントロールプレーンとデータプレーンの通信フロー



Cisco Unified Wireless Network（UWN）ワイヤレスオーバーザトップ（OTT）

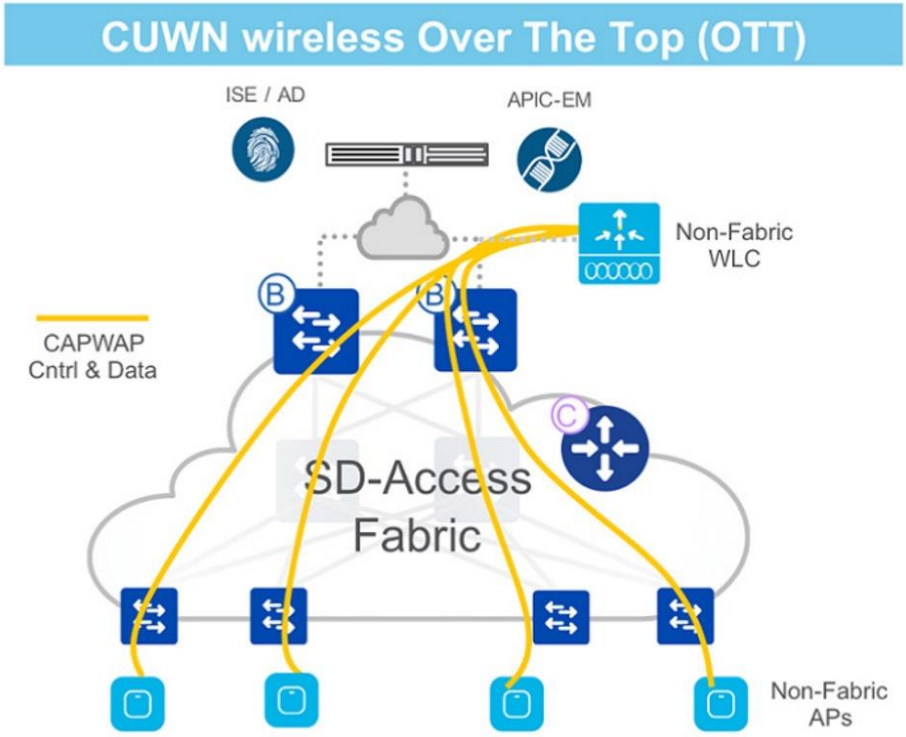
Cisco SD-Access　は、ワイヤレスオーバーザトップ（OTT）と呼ばれる集中型のワイヤレス展開を柔軟にサポートします。このサポートは、次のような複数のシナリオで重要です。

- SD-Access ワイヤレス対応ではない既存のシスコ ワイヤレス コントローラおよび AP。
- ネットワーク内にサードパーティ製ワイヤレス デバイスが存在する。
- 有線ネットワークとワイヤレスネットワークで移行ペースが対称ではない。

ワイヤレス OTT 展開では、ワイヤレスの制御、管理、およびデータプレーンのトラフィックは、AP とワイヤレスコントローラ間の CAPWAP トンネル内のファブリックを通過します。この CAPWAP トンネルは、Cisco SD-Access　ファブリックをトランスポートメディアとして利用します。他のベンダーのワイヤレス機器は異なるトンネリングプロトコルを使用する場合がありますが、SD-Access ファブリックをトランスポートとして使用するという概念は同じです。

図 16 は、ワイヤレス OTT におけるコントロールプレーンおよびデータプレーン通信のフローを示しています。

図 16. ワイヤレス **OTT** におけるコントロールプレーンおよびデータプレーン通信のフロー



詳細については、『Cisco SD-Access Wireless Design 』および『Cisco Wireless Design and Deployment Guide』を参照してください。

マルチサイト リモート ボーダー

マルチサイト リモート ボーダー（MSRB）は、ファブリックネットワーク内の信頼できない通信のルーティングを、ファイアウォールや DMZ などの指定された場所に一元化します。たとえば、ゲスト VN が複数のサイトにまたがるシナリオでは、DMZ にあるリモート境界をすべてのゲストトラフィックが通過するようにすることで、企業トラフィックから効果的に隔離できます。

マルチサイトネットワーク展開では、指定された MSRB が、複数のサイトにまたがる特定の VN に対するトラフィックを管理します。この設定により、複数のファブリックサイトにまたがる統合サブネットを維持しながら、複数のファブリックサイトに VN を展開できます。複数のファブリックサイト間でサブネットを一貫して維持することで、IP アドレスの使用を最適化できます。これにより、その VN の一元化されたエントリポイントとイグジットポイントが確立され、次の複数の利点があります。

- 集中管理：

  アンカーボーダーと呼ばれる、共通のボーダースイッチを指定して、さまざまなサイトにまたがる特定の VN の全トラフィックを処理できます。これにより、管理とポリシー適用が簡素化されます。

- サブネットの一貫性：

  マルチサイト リモート ボーダーを使用すると、すべてのサイトで VN に同じサブネットを使用できます。これにより、ロケーションごとに異なるサブネットを管理する必要がなくなり、IP アドレス空間を節約し、設定が簡素化されます。

- トラフィックの分離：

  MSRB は、ゲスト Wi-Fi などからの信頼できないトラフィックを隔離するのに特に役立ちます。さまざまなサイトにまたがるすべてのゲストトラフィックは、セキュリティ上の理由で DMZ などの中央の場所にトンネリングできます。

MSRB のコンテキストで使用される一般的な用語を次に示します。

- アンカー VN：

  ネットワーク内の複数のファブリックサイトにまたがって存在する VN です。関連付けられた IP サブネットとセグメントは、これらの複数のサイトで共通です。

- アンカーサイト：

  アンカー VN の共通のボーダーとコントロールプレーンをホストするファブリックサイトです。アンカーサイトは、アンカー VN の入力および出力通信を処理します。

- アンカーリングサイト：

  アンカー VN が展開されているアンカーサイト以外のファブリックサイトです。

- アンカー ボーダー ノード/MSRB：

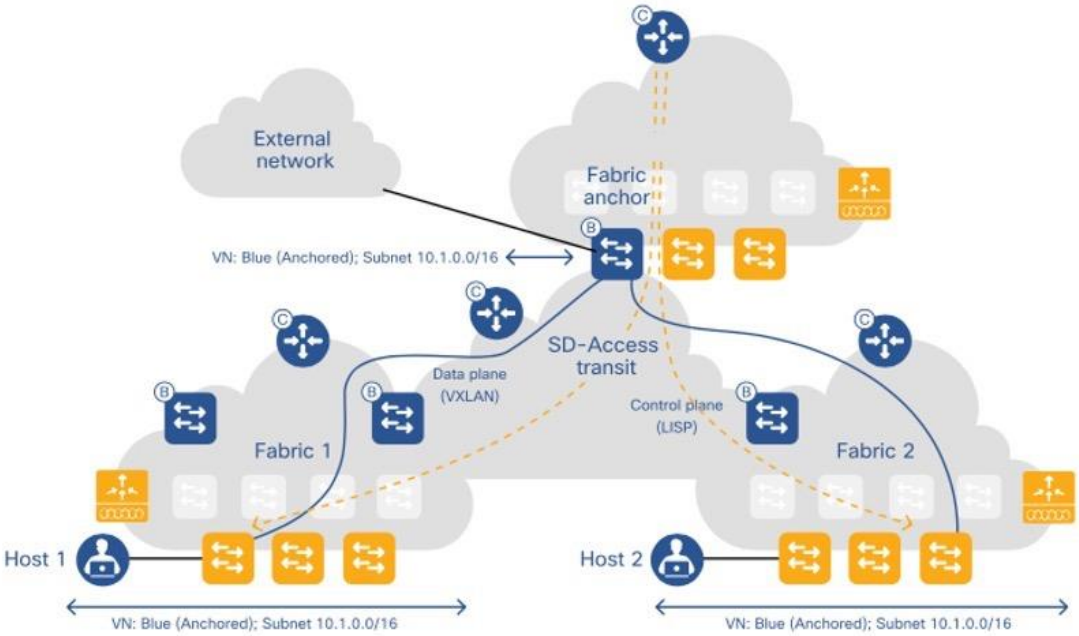
  アンカー VN との間のトラフィックの入出力場所を提供する、アンカーサイトのファブリックボーダーノードです。

- アンカー コントロール プレーン ノード：

  アンカー VN のエンドポイントの登録を受け入れ、要求に応答する、アンカーサイトのファブリック コントロール プレーン ノードです。

基本的に、MSRB は、ネットワーク管理を簡素化し、隔離されたトラフィックのセキュリティを強化して、複数のサイトがある Cisco SD-Access 展開における IP アドレスの使用を最適化します。

図 17.　　MSRB 展開の例



詳細については、『LISP VXLAN Fabric Configuration Guide』を参照してください。

技術的なヒント：	追加の 50 バイトの VXLAN ヘッダーオーバーヘッドに対応するために、パス全体の最大伝送ユニット（MTU）を考慮することが重要です。アンカーサイト ボーダー ノードの到達可能性のために複数の IP ネットワークを横断する可能性があるため、このことは特に重要です。

LISP のパブリッシュとサブスクライブの設計

LISP パブリッシュとサブスクライブ（Pub/Sub）モデルは、従来の LISP アーキテクチャを大幅に拡張したものです。ネットワークにあるエンドポイントの位置情報の配信が合理化され、すべてのノードがタイムリーで正確なデータを受信するようになります。LISP Pub/Sub モデルは、効率的で拡張性があり、ダイナミック環境を管理する機能を備えているため、最新の大規模なネットワーク設計において重要な要素です。

LISP Pub/Sub の設計では、LISP サイト登録テーブルをファブリック内のコントロールプレーンノードに登録するための追加のプロトコルは必要ありません。LISP Pub/Sub 機能は、Catalyst Center によって完全に自動化されます。これにより、SD-Access ファブリックの展開がシンプル化され、手動によるルーティング設定の必要がなくなります。

LISP Pub/Sub アーキテクチャは、次のような他の機能を構成するために採用されています。

- LISP ダイナミック デフォルト ボーダー ノード
- LISP バックアップインターネット
- LISP アフィニティ ID
- LISP エクストラネット

LISP Pub/Sub は、情報のルーティングにパブリッシュおよびサブスクライブモデルを使用します。エッジノードは、両方のボーダーノードのネクストホップ IP を持つデフォルトルートにサブスクライブします。ボーダーノードがアップストリーム接続（および BGP ピアリング）を失うと、影響を受ける VN のルーティングテーブルからデフォルトルートも削除されます。その後、ボーダーノードがコントロールプレーンを更新して、デフォルトルートに使用されないようにします。その結果、コントロールプレーンは、デフォルトルートに登録しているすべてのエッジノードに通知し、機能不全ルートの使用を停止し、残りのアクティブなボーダーノードへのデフォルトルートに依存するようにします。このアプローチにより、ルーティングの冗長性を維持するためのボーダーノード間での VRF/VN ごとの BGP ピアリングの必要がなくなり、手動の設定が削減されます。

展開の考慮事項：

- LISP/BGP ファブリックサイトと LISP Pub/Sub ファブリックサイトは、同じ SD-Access トランジット コントロール プレーン ノードで共存できません。
- 一方からもう一方への移行はまだサポートされていません。
- LISP Pub/Sub は、新しいネットワークの導入でのみ推奨されます。

Cisco SD-Access への移行

以降のセクションでは、SD-Access ファブリックのコンポーネントと、ITES の要件と課題に対応するにあたって SD-Access ソリューションが提供する利点について説明します。それを通じ、金融ネットワークの課題とユースケースに対応する SD-Access ファブリックの新規グリーンフィールド展開を構築するためのガイドラインと推奨事項を提供します。

グリーンフィールド SD-Access ネットワークは、インフラストラクチャ コンポーネントを組み込み、それらを相互接続し、Cisco Catalyst Center を Cisco PnP および LAN 自動化とともに使用して、ネットワークアーキテクチャのプロビジョニングをゼロから自動化することで確立できます。ただし、既存のネットワークに移行するには別の計画が必要になります。

考慮すべき事項には、次のものがあります。

- ネットワークをレイヤ 3 ルーテッドアクセスモデルに設定し直す必要がありますか。
- ネットワーク内のコンポーネントは、ターゲットの SD-Access トポロジで必要な規模をサポートしていますか。または、ハードウェアおよびソフトウェア プラットフォームを強化する必要がありますか。
- 組織では、IP アドレッシングと DHCP スコープ管理の変更に対応できますか。
- 新しいオーバーレイと共通サービス（インターネット、DNS/DHCP、データセンター アプリケーションなど）を統合する戦略はどのようなものですか。
- SGT かダイナミック ACL がすでに導入されていますか。またポリシー適用ポイントはどこですか。SGT と複数のオーバーレイを使用してファブリック内でセグメント化と仮想化を行う場合、ファブリックを超えて拡張するにはどのような要件がありますか。セグメンテーションと仮想化を拡張してサポートするために必要な、Cisco TrustSec、VRF-Lite、MPLS、またはその他のテクノロジーをサポートするインフラストラクチャは確立されていますか。
- ローミング ドメイン内のワイヤレスカバレッジは、ある時点でアップグレードできますか。あるいはネットワークでオーバーザトップ（OTT）戦略を採用する必要がありますか。

移行戦略

既存のネットワークを SD-Access に移行するには、次の 3 つの主な方法があります。

- 並列：

  この方法では、SD-Access ネットワークが既存のブラウンフィールド ネットワークと並行して確立されます。各スイッチは、ケーブルを物理的に接続することで、ブラウンフィールド ネットワークから SD-Access ネットワークに移行されます。この方法では、変更管理とロールバックの手順がシンプルになります。ただし、ブラウンフィールド ネットワークで現在セットアップされている以外のラックスペース、電源、およびケーブル配線インフラストラクチャが追加で必要です。

- 増分：

  この戦略では、従来のスイッチをブラウンフィールド ネットワークから移行し、SD-Access ファブリック エッジノードに変換します。後で説明するレイヤ 2 ボーダーハンドオフによって、この段階的な移行が容易になります。この方法は、SD-Access をサポートできる機器がすでに存在しているネットワークや、スペースや電源が限られているなどの制約がある環境に適しています。

- ハイブリッド：

  ハイブリッドアプローチでは、並列戦略と増分戦略の両方の要素を組み合わせます。たとえば、コアスイッチの新しいペアがボーダーノードとして設定され、コントロールプレーンノードが追加および設定されるとともに、ブラウンフィールド アクセス スイッチが SD-Access ファブリックエッジノードに段階的に変換されます。

既存の従来のネットワークを Cisco SD-Access に移行するための完全なガイダンスとさまざまなオプションについては、『Cisco Software-Defined Access for Industry Verticals』の「Migration to Cisco SD-Access」の章を参照してください。

ファブリックワイヤレスの移行

SSID がキャンパスのワイヤレスコントローラによって管理されている、2 つのフロアで構成される建物内のサンプルネットワークを考えてください。ファブリックワイヤレスに移行する場合は、既存の SSID と、ユーザーの移行先となるファブリック SSID との間では、シームレスなローミングが使用できないことを理解する必要があります。AP はアクセススイッチに接続し、集中型ワイヤレスコントローラへの CAPWAP トンネルを確立して、すべてのワイヤレス管理、制御、およびデータ通信を処理します。

ワイヤレスを Cisco SD-Access ファブリックに統合するには、まず既存の建物のネットワーク内に有線ファブリックを作成します。有線ファブリックは、前述の標準モデル（並列、増分、またはハイブリッド）のいずれかを使用して展開できます。AP が接続されているアクセススイッチがファブリックエッジになっても、ユーザーは引き続き既存の SSID に接続し、一元的なスイッチングを行えます。これにより、有線ネットワークの移行中に既存のワイヤレスサービスに大きな影響を与えることなく、ワイヤレスネットワークをファブリック全体で機能させることができます。

ブラウンフィールド ワイヤレスコントローラは、ファブリックへの移行中もサポートされますが、Cisco IOS XE イメージおよびプラットフォームに関する SD-Access 互換性マトリックスに準拠している必要があります。Cisco Catalyst Center を介して検出された場合、システムはワイヤレスコントローラの既存の設定を変更せずに認識します。

ファブリックワイヤレスへの移行は段階的に実行でき、最小の移行単位はサイト階層内のフロアになります。環境によっては、管理者は建物またはエリア全体を移行することもできます。ワイヤレスネットワーク プロファイルを作成し、SSID をファブリック対応として設定して、特定のフロアに割り当てることで、既存の SSID を OTT からファブリック対応に段階的に移行できます。この段階的なアプローチにより、スムーズかつ制御された移行を実現できます。すべてのフロア、建物、またはエリアがファブリックベースの SSID にマッピングされると、ファブリック対応ワイヤレスへの移行は完了であり、その時点でセグメンテーションポリシーを定義できます。

移行時の主な考慮事項として、OTT モードで動作している SSID とファブリックモードで動作している SSID との間では、シームレスなローミングが行われないことが挙げられます。移行中に、OTT SSID と重複しない IP プールを定義することが重要です。既存のワイヤレスコントローラがある場合は、それを再利用して、ファブリックサイトと従来のワイヤレスネットワークの両方を管理できます。ただし、ワイヤレスコントローラがファブリックサイトを管理するように変換された後は、複数の従来のワイヤレスサイトと並行して単一のファブリックサイトのみを監視できます。

レイヤ 2 ボーダーハンドオフ

レイヤ 2 ボーダーハンドオフによって、SD-Access ネットワークと従来のネットワーク間のシームレス コミュニケーションが容易になります。これは、両方の環境のホストが同じレイヤ 2 ドメイン上にある場合と同様に通信できるようにする、オーバーレイサービスを提供することで実現します。この機能は、従来のネットワークから SD-Access ネットワークに移行する際に不可欠です。IP の再アドレッシングを必要とせずに、従来のネットワーク内の端末を引き続き配置しつつ、SD-Access 端末との接続をテストできます。その後、ケーブルの物理的な再配置を伴う並行アプローチか、従来のアクセススイッチを SD-Access ファブリックエッジ ノードに変換する増分アプローチのいずれかで、移行を進めることができます。

レイヤ 2 ボーダーハンドオフでは、ファブリックサイトと従来のネットワークの VLAN セグメントで同じサブネットを共有できます。ファブリック環境と非ファブリック環境の間で VLAN 変換または VLAN 拡張を実行するボーダーノードを介して、通信が容易になります。Cisco Catalyst Center は、LISP コントロールプレーン設定、VLAN 変換、SVI セットアップ、およびボーダーノード上の従来のネットワークへのトランクポート接続を自動化します。

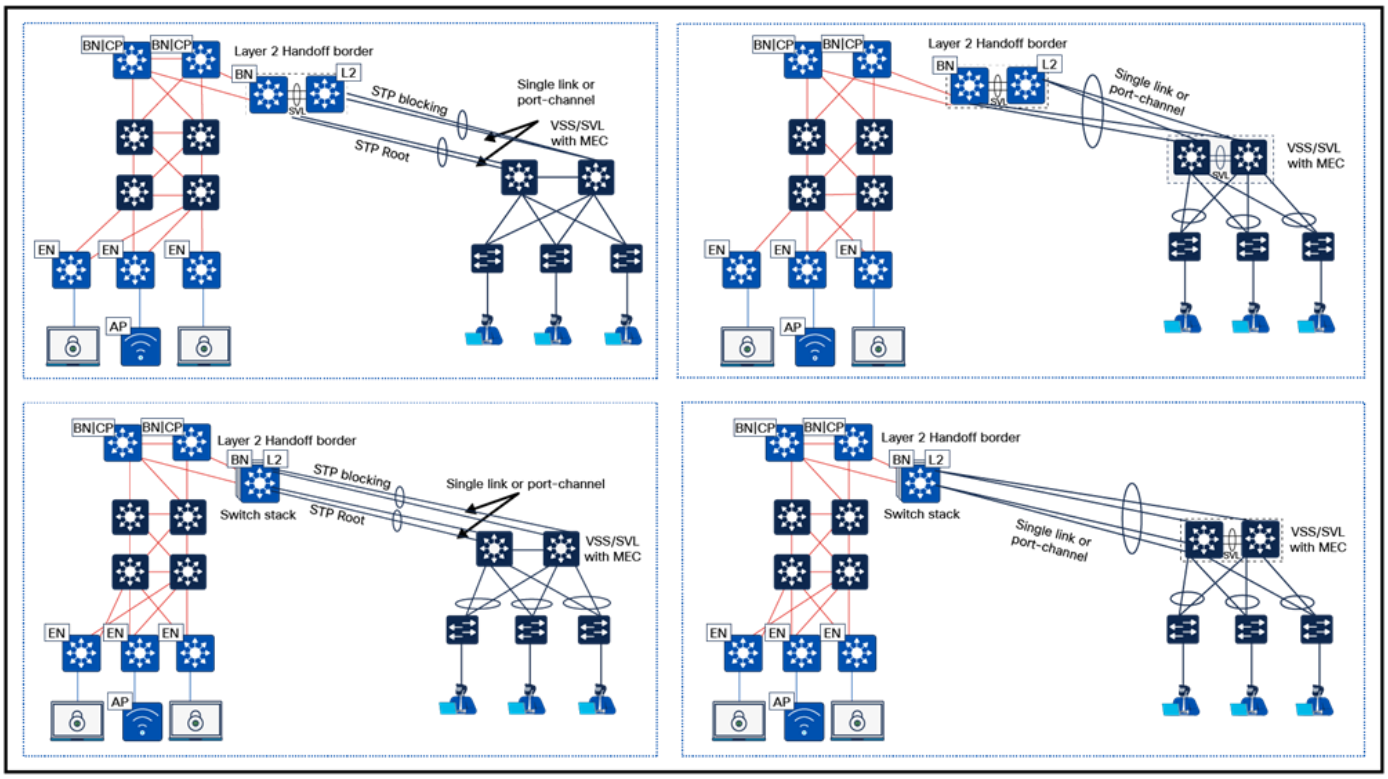
レイヤ 2 ハンドオフ全体でマルチキャスト通信がサポートされ、従来のネットワークと SD-Access ネットワーク間のマルチキャスト通信を実現します。マルチキャスト転送メカニズムは、ファブリック内と同様に、レイヤ 2 ボーダーノード全体で一貫して機能します。一方、従来のネットワークは標準のレイヤ 2 フラッディング手法を使用して、マルチキャストパケットを引き続き処理します。

オペレーショナル テクノロジー（OT）、モノのインターネット（IoT）、および建物管理システム（BMS）を SD-Access に移行する場合は、レイヤ 2 ボーダーハンドオフをレイヤ 2 フラッディングと組み合わせて使用できます。これは、ファブリックサイトと従来のネットワーク間におけるイーサネットのブロードキャストベース Wake-on-LAN 機能をサポートしており、OT および BMS システム（通常はブロードキャスト通信を使用）をファブリックに段階的に移行させることができます。

展開モデルとトポロジ

従来のネットワークスイッチは、レイヤ 2 ハンドオフを使用して単一のボーダーノードに接続することができます。従来のネットワークスイッチを複数のボーダーノードにマルチホームすることはできません。ただし、デュアルホーミングはリンク集約を使用することでサポートされます。従来のネットワークスイッチが、ハードウェア スイッチスタックや SVL などの、マルチボックスの単一論理ボックス構造で動作する場合、マルチシャーシ EtherChannel（MEC）はシングルボーダーでサポートされます。ボーダーノード自体の冗長化は、ハードウェアスタッキングや SVL によって実現できます。

図 18.　　レイヤ 2 ボーダーハンドオフのトポロジ



オフショア開発センターの展開向けのバーチャル プライベート ネットワーク（VPN）

ITES 組織のセキュアなオフショア開発センターでは、リモートチーム、データセンター、およびクライアントネットワーク間の安全な接続のために、信頼性の高いバーチャル プライベート ネットワーク（VPN）が重要です。これによってデータを暗号化してサイバー脅威から保護するとともに、セキュリティ規制のコンプライアンスを保証します。要件に応じて、ITES 組織は次の VPN タイプから選択します。

- サイト間 VPN
- クライアント - サイト間 VPN

サイト間 VPN

サイト間 VPN は、同じ組織に所属する、地理的に離れた複数のオフィスや物理的場所の間でセキュアな接続を実現する VPN セットアップのタイプです。この接続は多くの場合 VPN トンネルと呼ばれ、各サイトがプライベートネットワークで接続されているかのように、インターネットなどのパブリックネットワークを介してデータやリソースをセキュアに送信できます。

通常、サイト間 VPN はルータやファイアウォールなどのネットワークゲートウェイ間で確立され、それらのネットワークゲートウェイはサイトに出入りする通信の暗号化と復号を行うように設定されます。このセットアップはビジネスで一般的に使用され、オフィス間の通信を安全に保ち、不正な第三者によって傍受されないようにします。

クライアント - サイト間 VPN

クライアント - サイト間 VPN はリモートアクセス VPN とも呼ばれ、個々のユーザーが職場のネットワークなどのリモートネットワークに任意の場所から接続できるようにする VPN のタイプです。これは、ユーザーのデバイスにインストールされた VPN クライアントソフトウェアによって実現され、リモートサイトに配置された VPN サーバーへのセキュアな接続を確立します。

接続すると、ユーザーのデバイスはリモートネットワークの一員になり、ユーザーがネットワークのローカル環境内に物理的に存在する場合と同様に、ネットワークリソースにアクセスできます。一般的に、このタイプの VPN はリモートワーカー、移動中の人、または外部の場所から組織のネットワークへのセキュアなアクセスを必要とするユーザーによって使用されます。

要約すると、サイト間 VPN とクライアント - サイト間 VPN の両方で、暗号化やその他のセキュリティメカニズムが用いられ、パブリックインターネットを介して送信されるデータの機密性を維持し、不正アクセスから確実に保護します。

検証済みのソリューションのユースケース

このセクションでは、信頼できるテンプレートとして機能する、ITES 向けに検証された重要なユースケースの一部について説明します。これにより、組織は IT インフラストラクチャを構築することができ、それらの設計が綿密なテストを受け、特定のビジネスニーズに合わせてカスタマイズされていることが保証されます。

Day 0 および Day 1 ネットワーク立ち上げのユースケース

- ネットワーク インフラストラクチャを立ち上げ、グリーンフィールド キャンパスのすべての機能を統合する。
- ネットワークデバイスとファブリックのプロビジョニングを自動化および簡素化する。
- Catalyst Center を使用してインベントリをモニターし、ネットワークデバイスを管理する。
- デバイスとクライアントの認証および承認のために Cisco ISE と統合する。
- Catalyst Center を使用してワイヤレスコントローラと AP を管理および展開する。
- ネットワークデバイスおよび AP 用のプラグアンドプレイを介してデバイスの導入準備を行う。
- 共有サービスに Cisco Catalyst を使用して、複数のサイトのネットワーク設定を管理する。
- SD-Access マルチサイト キャンパスを展開し、キャンパス全体のトラフィックを管理する。

Day n ネットワーク運用ユースケース

- Catalyst Center を使用して、スイッチ、ルータ、ワイヤレスコントローラなどの複数のデバイスをアップグレードする。
- 新しいフロアを既存のファブリックサイトにオンボードする。
- 有線およびワイヤレスクライアントを含む新しいファブリックノードをオンボードする。
- ブラウンフィールド AP を Wave2 から 11 Ax に置き換える。
- 組み込み型ワイヤレスコントローラと共に FIAB を使用して、新しい小規模サイトを追加する。
- 別の Flex OTT 展開を使用して、新しい小規模ファブリックサイトを追加する。
- Day-*n* ログイン情報の変更（デバイスパスワードの変更やネットワークデバイスの更新など）を行う。
- テンプレートを使用して、レイヤ 2 およびレイヤ 3 ハンドオフリンクで VLAN を許可する。

技術的なヒント： アップリンクポートの「switchport mode trunk」および「switchport trunk allowed vlan all」をトリガーする操作を行った後は、必ずテンプレートを再プロビジョニングする必要があります。

セグメンテーションとポリシーのユースケース

- 組織全体に仮想ネットワークを導入して、一貫したマクロセグメンテーションを実現する。
- SGT を使用した仮想ネットワーク内のマイクロセグメンテーションで、グループベースのアクセスポリシーを使用する。
- 認証を使用して、有線およびワイヤレスクライアントのセキュアな導入準備を実現する。
- ファブリック内のさまざまな入出力通信ポイントでポリシーを適用する。
- 新しいセグメントの追加と、デバイスおよびユーザー向けのグループベースのアクセスポリシーを含む運用シナリオ。

セキュリティユースケース

- Catalyst Center で、信頼できる CA FQDN ベースの証明書を適用および使用する。

- 外部 AAA 認証を使用して、きめ細かい役割別のユーザーを作成し、監査ログを使用して Catalyst Center のアクティビティをチェックする。
- 監査ポリシーの変更、ポリシー変更の展開、およびこれらの展開のステータスをモニターする。

SD-Access ワイヤレスのユースケース

- ブランチの従業員とユーザー向けに、企業 SSID を使用したワイヤレスクライアントの導入準備を行う。
- CWA ポータルを使用して、ブランチのユーザーにゲストワイヤレスアクセスを提供する。
- Catalyst 9800 シリーズ ワイヤレスコントローラを使用して、HA モードでワイヤレス インフラストラクチャを展開する。
- マルチサイト リモート ボーダーを使用して、ファイアウォール上でゲスト SSID 通信ポリシーを適用する。

堅牢性のユースケース

- 既存のアプリケーション、通信、およびユーザーへの影響を最小限に抑えながら、デバイスまたはリンクの障害から自動的に回復する。
- Catalyst Center を 3 ノード HA モードにする。Catalyst Center でサービスやノードの障害が発生した場合、システムはユーザーの介入なしで回復する必要があります。
- PSN および pxGrid ノードのフェールオーバーによる、Cisco ISE 分散ノードのフェールオーバー。
- Cisco Catalyst ワイヤレス LAN コントローラおよび AP のフェールオーバー。
- ファブリック内のリンクおよびネットワークデバイスの障害を含むフェールオーバーシナリオ。
- Catalyst Center コントローラの設定とデータを、一度だけ、またはスケジュールに従ってバックアップする。
- 新しい Cisco Catalyst クラスターでバックアップを復元し、デバイスを管理できることを確認する。
- ネットワーク、ポリシー、およびデバイス接続の変化を伴う長期的な安定性。

アシュアランスと分析を用いたモニタリングと障害対応のユースケース

- ネットワーク、有線ユーザー、およびワイヤレスユーザーの状態を、統合インターフェイスからモニターする。
- ネットワークとデバイスに関する深刻かつ重大な問題や、その他の進行中の問題をモニターし、アシュアランスの推奨措置に従って問題を解決する。
- 個々のデバイス、有線ユーザー、またはワイヤレスユーザーの包括的なビューを取得し、詳細情報を取得する。
- アプリケーションの可視性を使用して、ユーザーによるアプリケーションデータの使用状況を詳細に追跡する。

パフォーマンスとスケールのユースケース

- すべてのソリューションを統合したマルチディメンションのスケール設定と、ネットワークの安定性の確認。

ITES ODC 展開モデル

ファブリック外部の専用ファイアウォールとゲートウェイを使用したサイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- すべての通信がファイアウォールを通過し、監査とコンプライアンスのためにログ記録されていることを確認します。
- ネットワーク間のセキュアなデータ転送を確保します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- ODC 専用ファイアウォールを導入します。

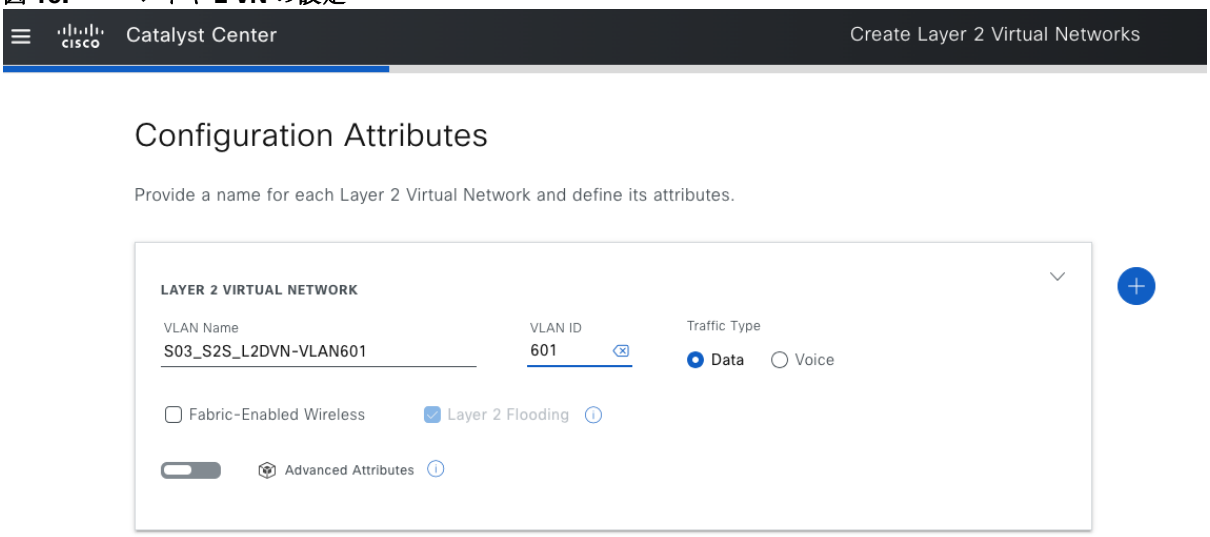
技術要件：

- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- ファブリック外部のゲートウェイを含むレイヤ 2 VN を導入します。
- セキュアなデータ転送のためにサイト間 VPN を設定します。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- ファイアウォール インターフェイスを設定して、専用 ODC からの通信を管理します。

手順 1。

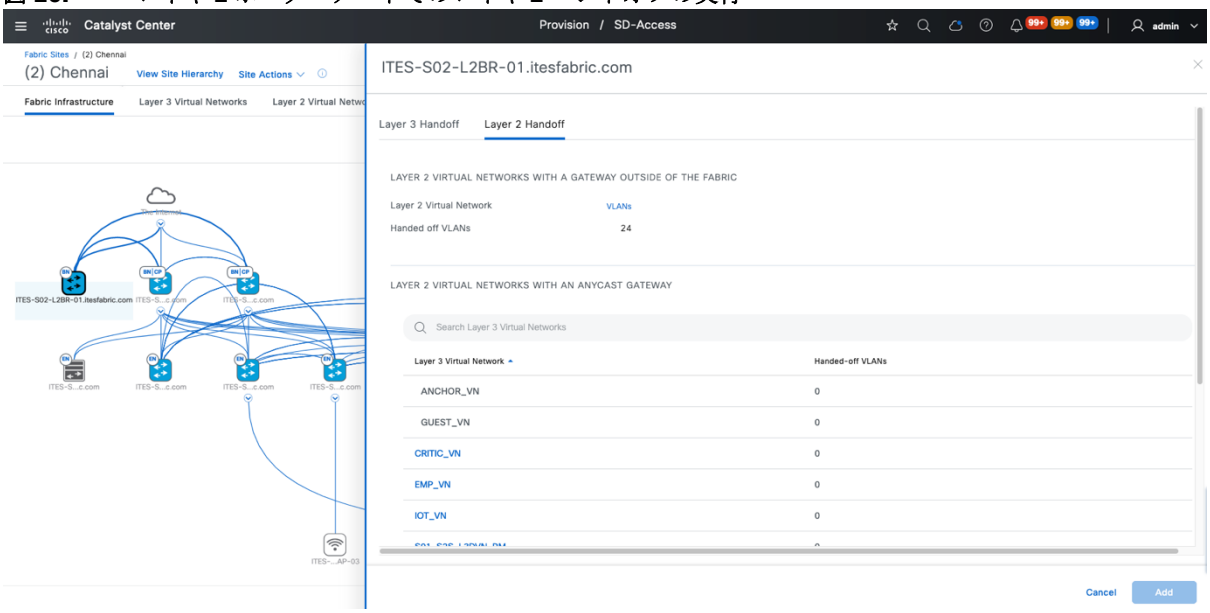
ステップ 1. 適切な VLAN ID を使用してレイヤ 2 VN を設定し、サイトに割り当てます。

図 19.　　レイヤ 2 VN の設定



ステップ 2. 専用ボーダーノードでレイヤ 2 ハンドオフを設定します。ファブリック外のゲートウェイを使用してレイヤ 2 VN からアクセスできる VLAN を有効にします。

図 20.　　レイヤ 2 ボーダーノードでのレイヤ 2 ハンドオフの実行



技術的なヒント：　ファイアウォールに面するレイヤ 2 ボーダーノードのアップリンクポートは、スタンドアロンインターフェイスまたはポートチャネルの一部として、トランクとして設定されます。

ステップ 3. ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング
- サイト間 VPN

ステップ 4. ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

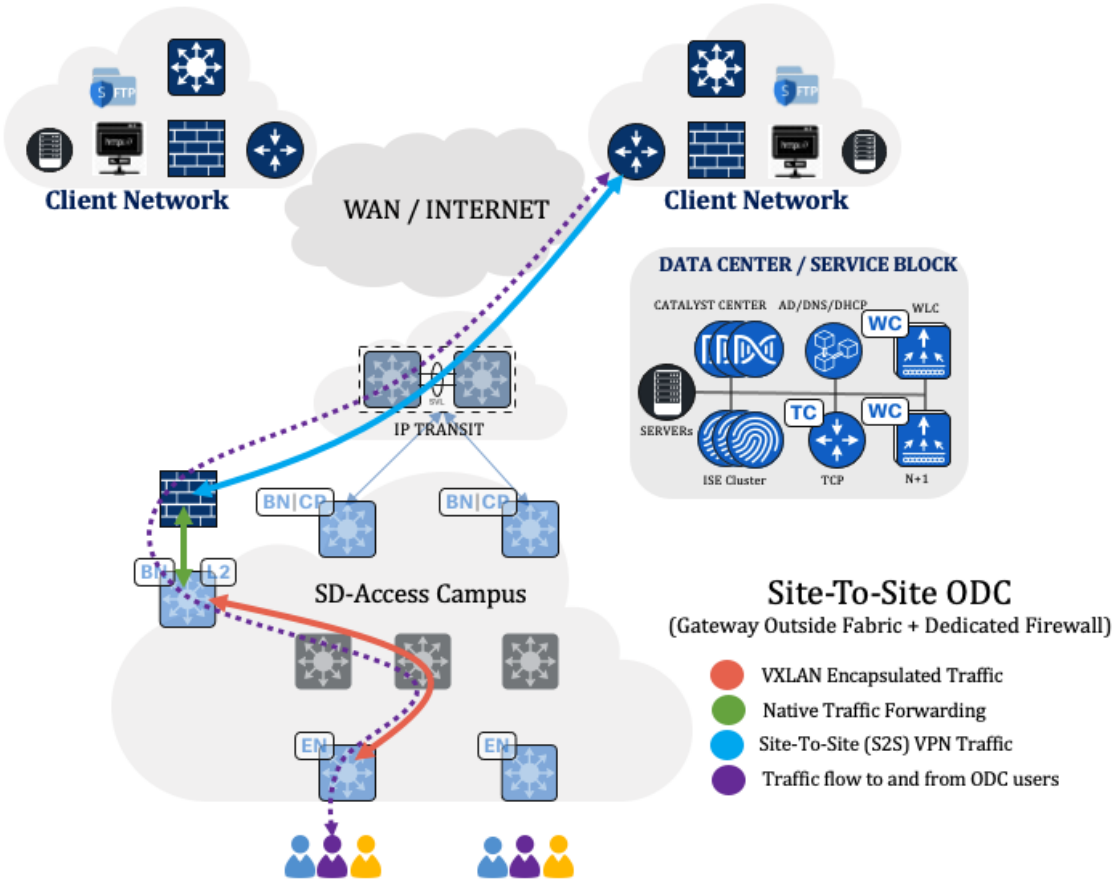
ステップ 5. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

- Cisco ISE とレイヤ 2 ボーダーノードの間で SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

ステップ 6. 認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 21 のようになります。

図 21.　　外部ゲートウェイと専用ファイアウォールを使用したサイト間 ODC での通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

ファブリック外部の共有ファイアウォールとゲートウェイを使用したサイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- すべての通信がファイアウォールを通過し、監査とコンプライアンスのためにログ記録されていることを確認します。
- ネットワーク間のセキュアなデータ転送を確保します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- 複数の ODC に同じファイアウォールを使用します。

技術要件：

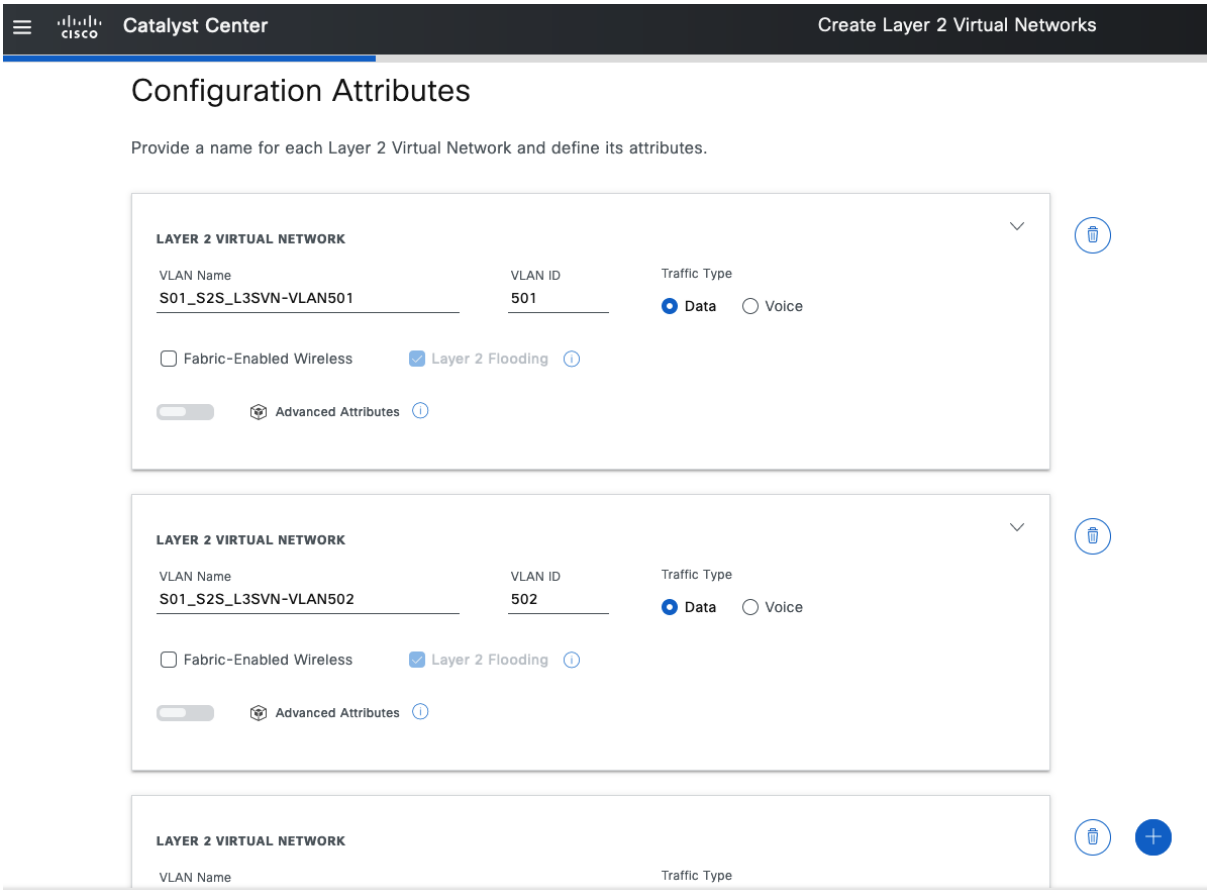
- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- ファブリック外部のゲートウェイを含むレイヤ 2 VN を導入します。
- セキュアなデータ転送のためにサイト間 VPN を設定します。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。

- 各 ODC からの通信を個別に処理するようにファイアウォール インターフェイスを設定します。

手順 2。

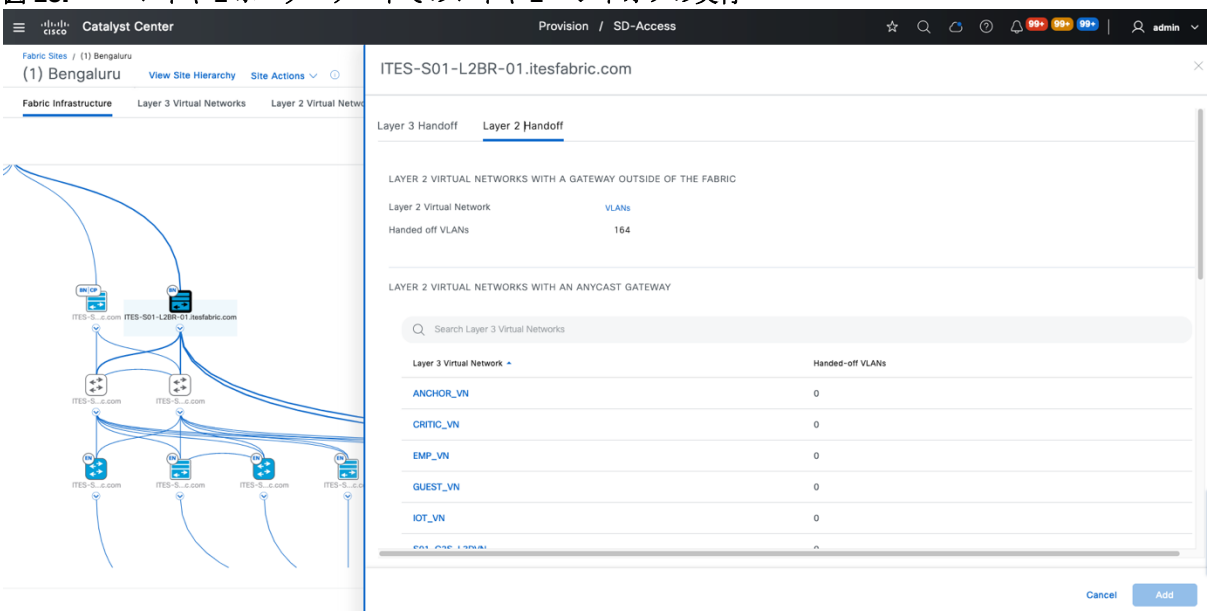
ステップ **1.** 適切な VLAN ID を使用してレイヤ 2 VN を設定し、サイトに割り当てます。

図 22.　　レイヤ 2 VN の設定



ステップ **2.** 専用ボーダーノードでレイヤ 2 ハンドオフを設定します。ファブリックエリア外のゲートウェイを使用してレイヤ 2 VN からアクセスできる VLAN を有効にします。

図 23.　　レイヤ 2 ボーダーノードでのレイヤ 2 ハンドオフの実行



ステップ 3.　ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）。
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング
- サイト間 VPN

ステップ 4.　ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

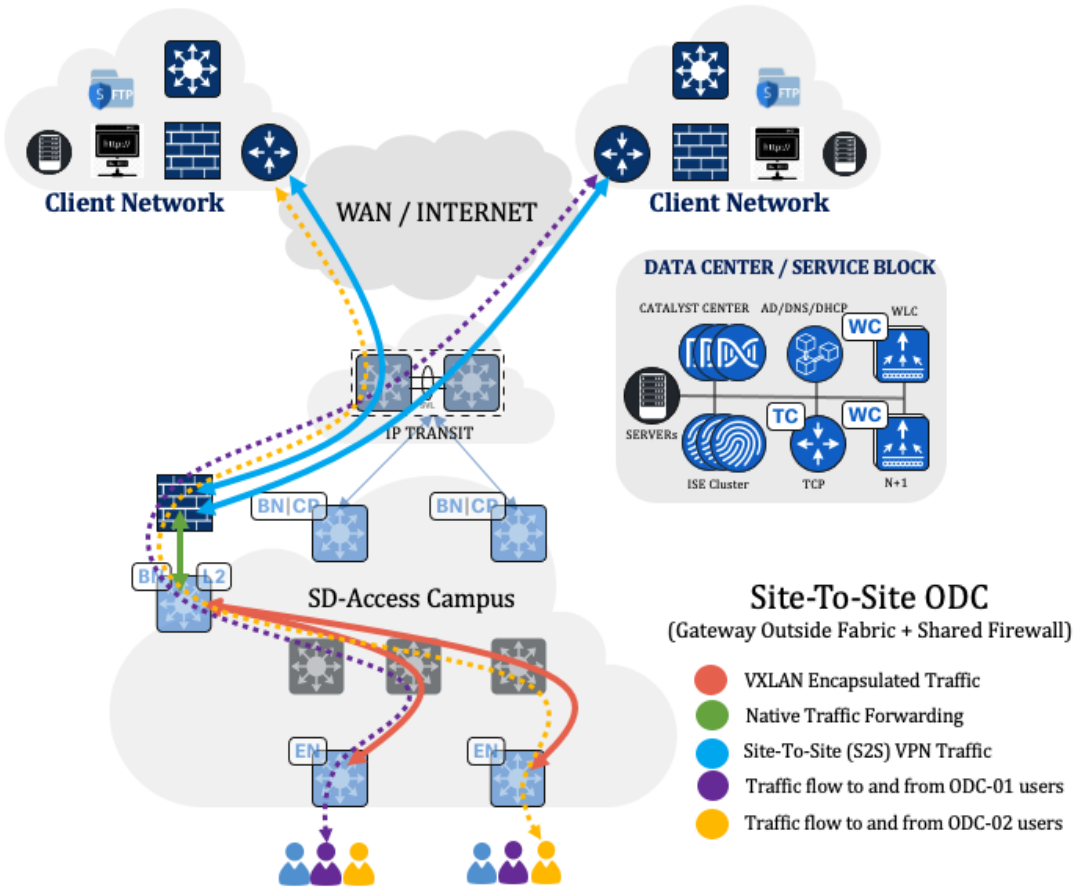
ステップ 5.　許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

- Cisco ISE とレイヤ 2 ボーダーノードの間で SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

ステップ 6.　認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 24 のようになります。

図 24.　　外部ゲートウェイと共有ファイアウォールを使用したサイト間 ODC での通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

ファブリック外部の専用ファイアウォールとゲートウェイを使用したクライアント - サイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- クライアントのゲートウェイとして機能するようにファイアウォールを設定し、監査およびコンプライアンス用にすべての通信をログ記録します。
- VPN クライアントを使用して、クライアントネットワークに安全に接続します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- ODC 専用ファイアウォールを導入します。

技術要件：

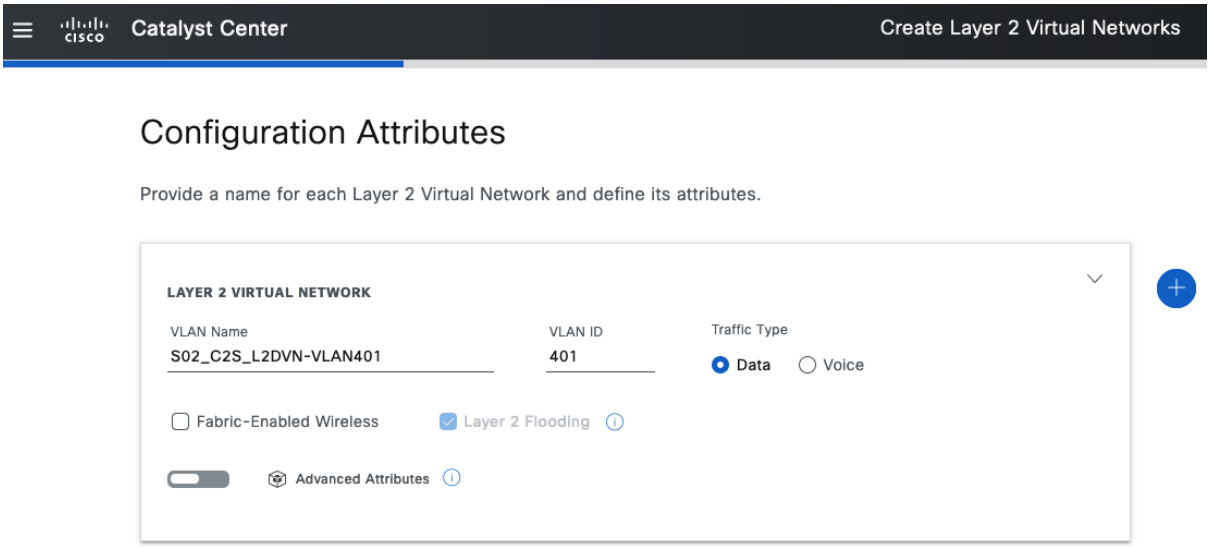
- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- ファブリック外部のゲートウェイを含むレイヤ 2 VN を導入します。
- ODC ユーザーのラップトップおよびデスクトップに VPN クライアントをインストールして、設定を行います。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。

- ファイアウォールを設定して、専用 ODC からの通信を管理します。

手順 3。

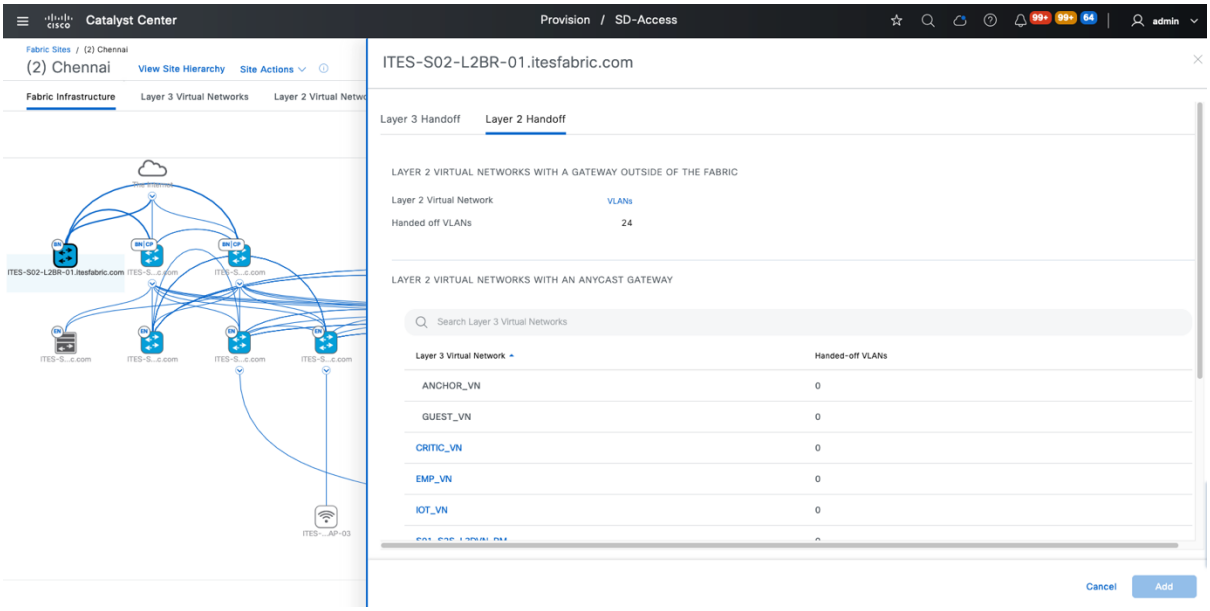
ステップ 1. 適切な VLAN ID を使用してレイヤ 2 VN を設定し、サイトに割り当てます。

図 25.　　レイヤ 2 VN の設定



ステップ 2. 専用ボーダーノードでレイヤ 2 ハンドオフを設定します。ファブリックエリア外のゲートウェイを使用してレイヤ 2 VN からアクセスできる VLAN を有効にします。

図 26.　　レイヤ 2 ボーダーノードでのレイヤ 2 ハンドオフの実行



技術的なヒント： ファイアウォールに面するレイヤ 2 ボーダーノードのアップリンクポートは、スタンドアロンインターフェイスまたはポートチャネルの一部として、トランクとして設定されます。

ステップ 3. ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング

ステップ 4. ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

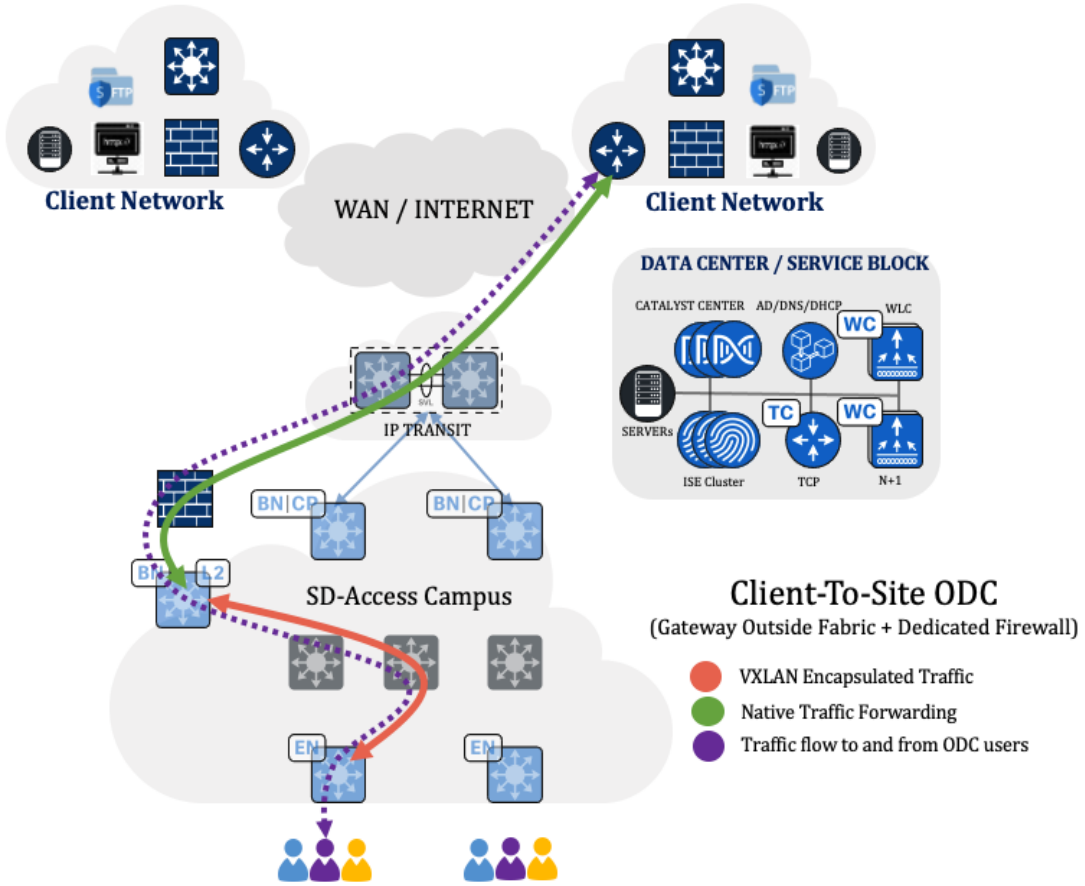
ステップ 5. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

- Cisco ISE とレイヤ 2 ボーダーノードの間で SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

ステップ 6. 認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 27 のようになります。

図 27.　外部ゲートウェイと専用ファイアウォールを使用したクライアント - サイト間 ODC における通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

ファブリック外部の共有ファイアウォールとゲートウェイを使用したクライアント - サイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- クライアントのゲートウェイとして機能するようにファイアウォールを設定し、監査およびコンプライアンス用にすべての通信をログ記録します。
- VPN クライアントを使用して、クライアントネットワークに安全に接続します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- 複数の ODC に同じファイアウォールを使用します。

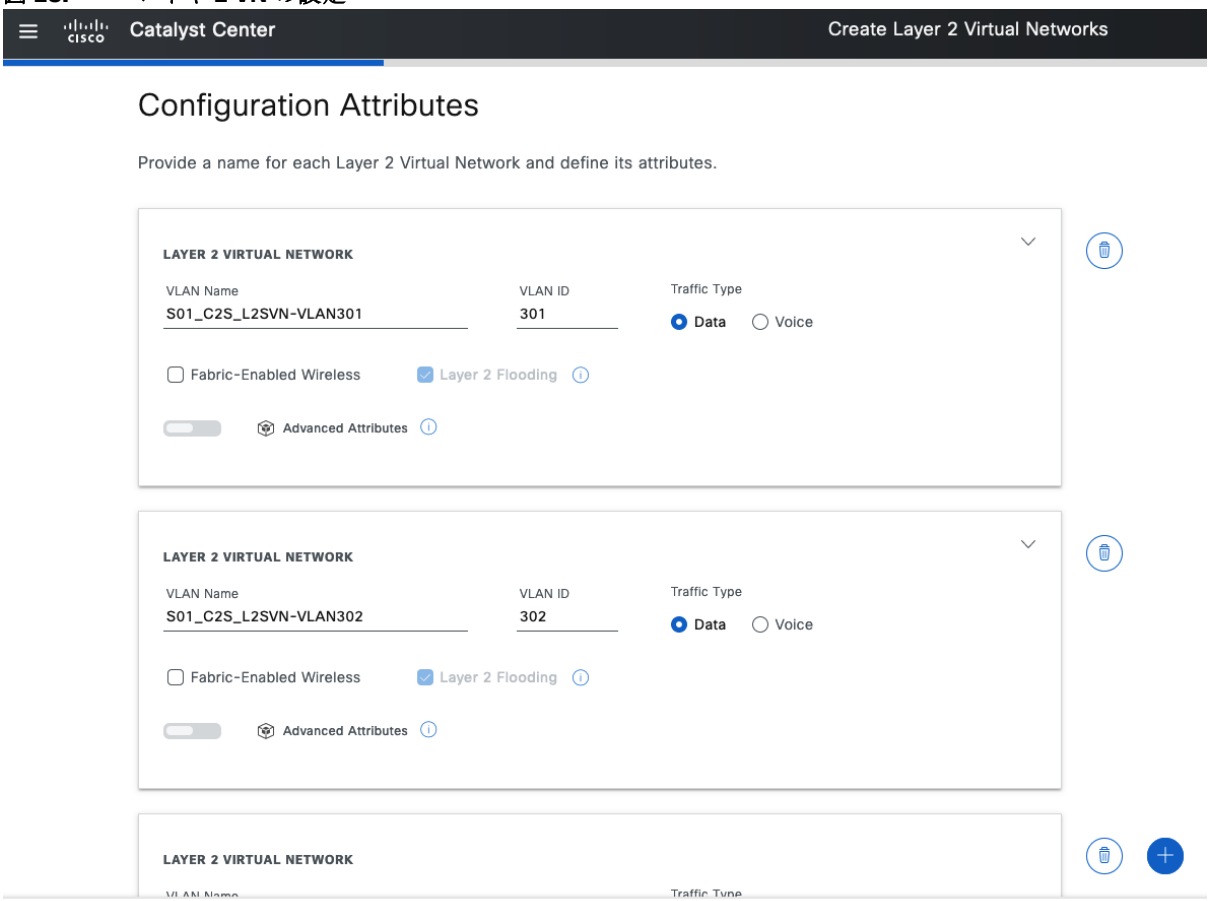
技術要件：

- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- ファブリック外部のゲートウェイを含むレイヤ 2 VN を導入します。
- ODC ユーザーのラップトップおよびデスクトップに VPN クライアントをインストールして、設定を行います。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- 各 ODC からの通信を個別に処理するようにファイアウォール インターフェイスを設定します。

手順 4。

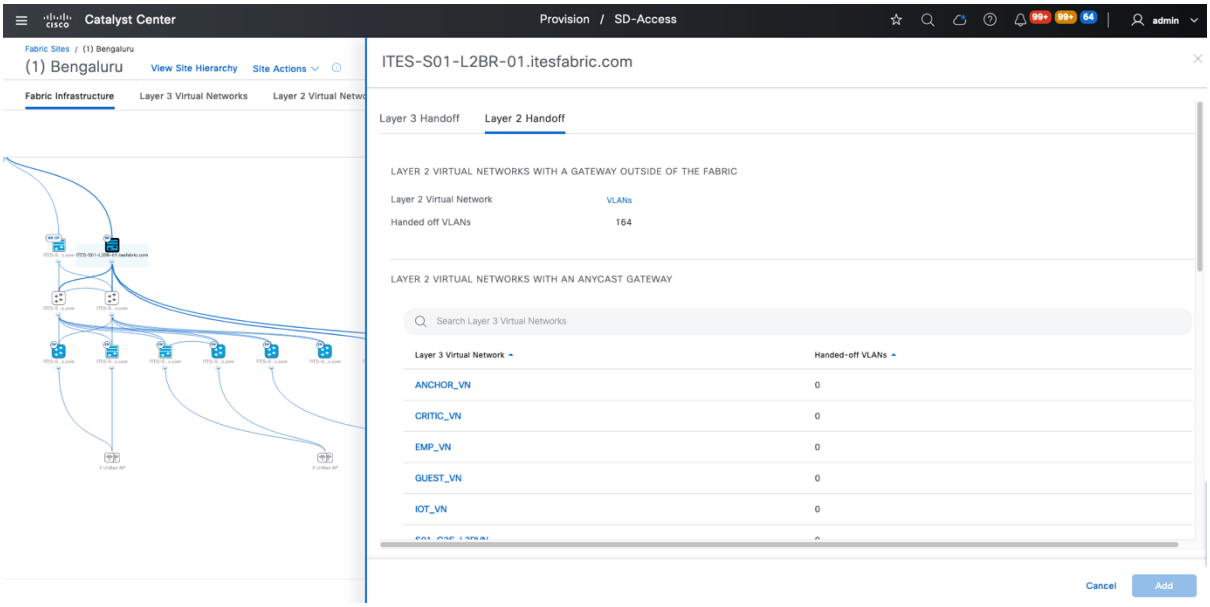
ステップ 1. 適切な VLAN ID を使用してレイヤ 2 VN を設定し、サイトに割り当てます。

図 28.　　レイヤ 2 VN の設定



ステップ 2. 専用ボーダーノードでレイヤ 2 ハンドオフを設定します。ファブリックエリア外のゲートウェイを使用してレイヤ 2 VN からアクセスできる VLAN を有効にします。

図 29.　　レイヤ 2 ボーダーノードでのレイヤ 2 ハンドオフの実行



技術的なヒント：　ファイアウォールに面するレイヤ 2 ボーダーノードのアップリンクポートは、スタンドアロンインターフェイスまたはポートチャネルの一部として、トランクとして設定されます。

ステップ 3. ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング

ステップ 4. ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

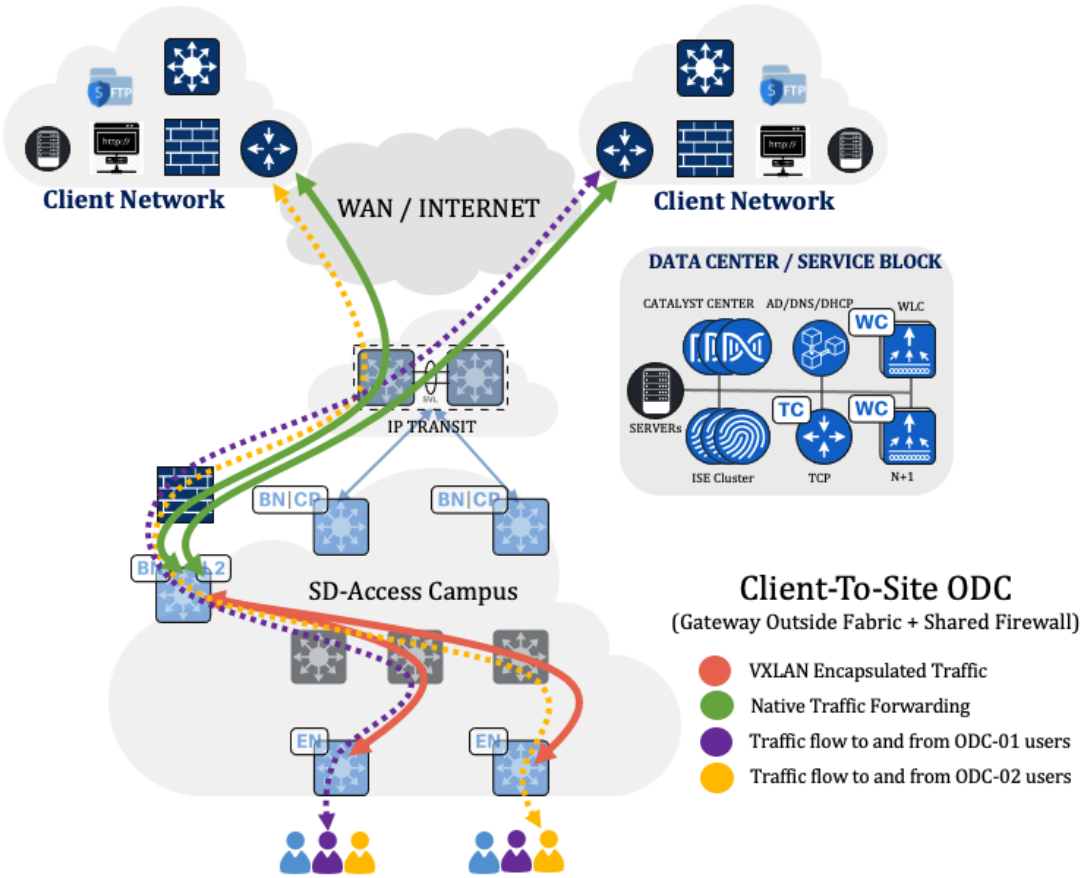
ステップ 5. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

- Cisco ISE とレイヤ 2 ボーダーノードの間で SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

ステップ 6. 認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 30 のようになります。

図 30.　外部ゲートウェイと共有ファイアウォールを使用したクライアント - サイト間 ODC の通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

専用ファイアウォールとエニーキャストゲートウェイを使用したサイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- すべての通信がファイアウォールを通過し、監査とコンプライアンスのためにログ記録されていることを確認します。
- ネットワーク間におけるデータのセキュアな転送を確保します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- ODC 専用ファイアウォールを導入します。

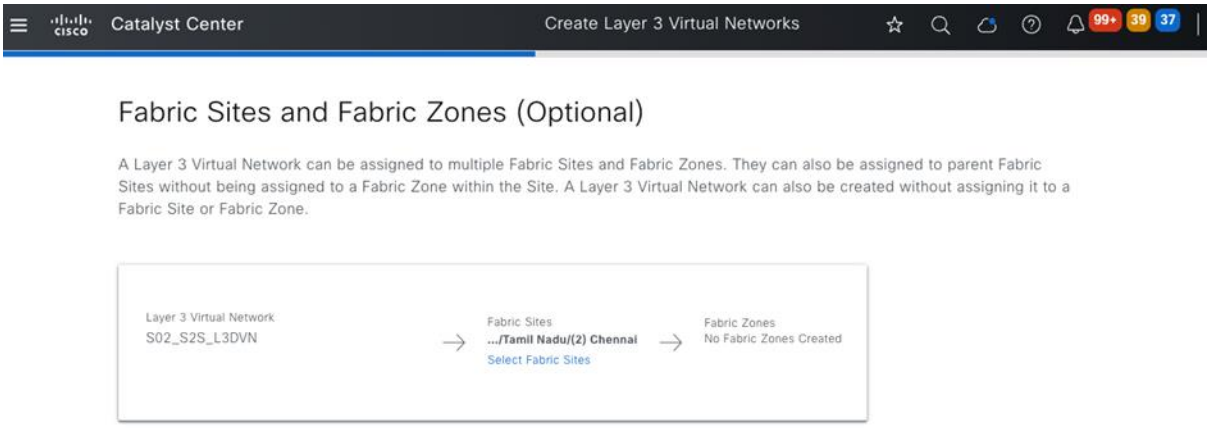
技術要件：

- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- フュージョンデバイスからファイアウォールにすべての通信をリダイレクトしてから、接続先に転送します。
- セキュアなデータ転送のためにサイト間 VPN を設定します。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- ファイアウォール インターフェイスを設定して、専用 ODC からの通信を管理します。

手順 5。

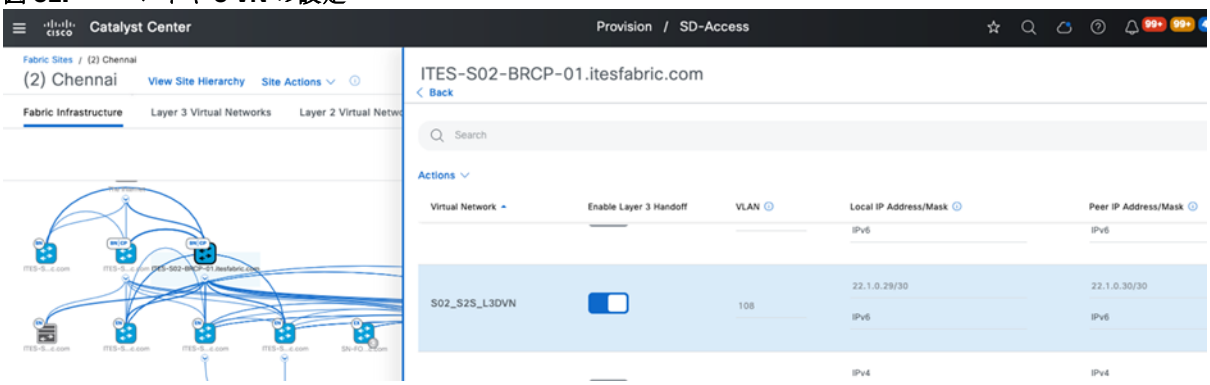
ステップ 1. サイトでレイヤ 3 VN を設定してから、必要なエニーキャストゲートウェイをプロビジョニングします。

図 31.　　レイヤ 3 仮想ネットワークの設定



ステップ 2. 新しく追加した VN のボーダーノードでレイヤ 3 ハンドオフを設定してから、eBGP セッションが稼働していることを確認します。

図 32.　　レイヤ 3 VN の設定



ステップ 3. ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング
- サイト間 VPN

ステップ 4. ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

ステップ 5. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

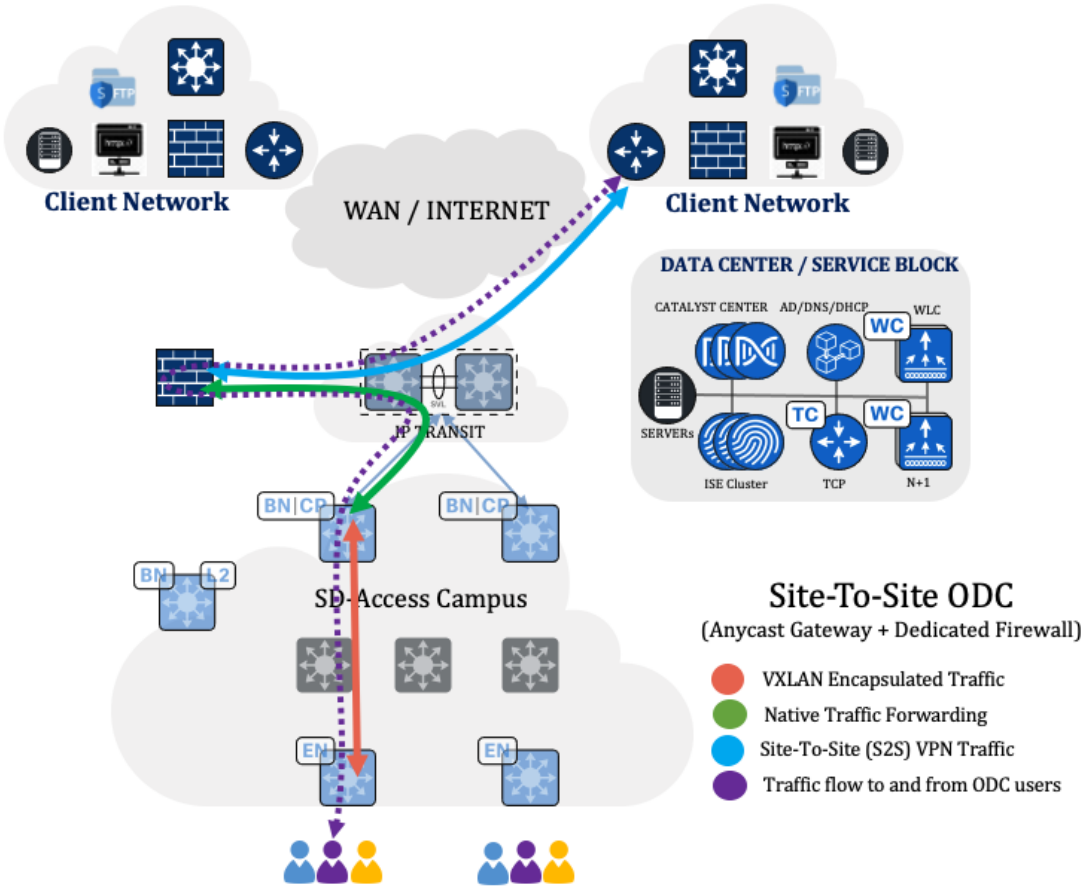
- Cisco ISE と VN のレイヤ 3 ボーダーノードの間で VRF 対応 SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

注：　ファイアウォールを通過する VN 通信を設定して、Cisco ISE サーバーとレイヤ 3 ボーダーノードとの間の SXP 通信に特化した TCP バイパスを許可します。

ステップ 6. 認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 33 のようになります。

図 33.　　エニーキャストゲートウェイと専用ファイアウォールを使用したサイト間 ODC の通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

共有ファイアウォールとエニーキャストゲートウェイを使用したサイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- すべての通信がファイアウォールを通過し、監査とコンプライアンスのためにログ記録されていることを確認します。
- ネットワーク間におけるデータのセキュアな転送を確保します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- 複数の ODC に同じファイアウォールを使用します。

技術要件：

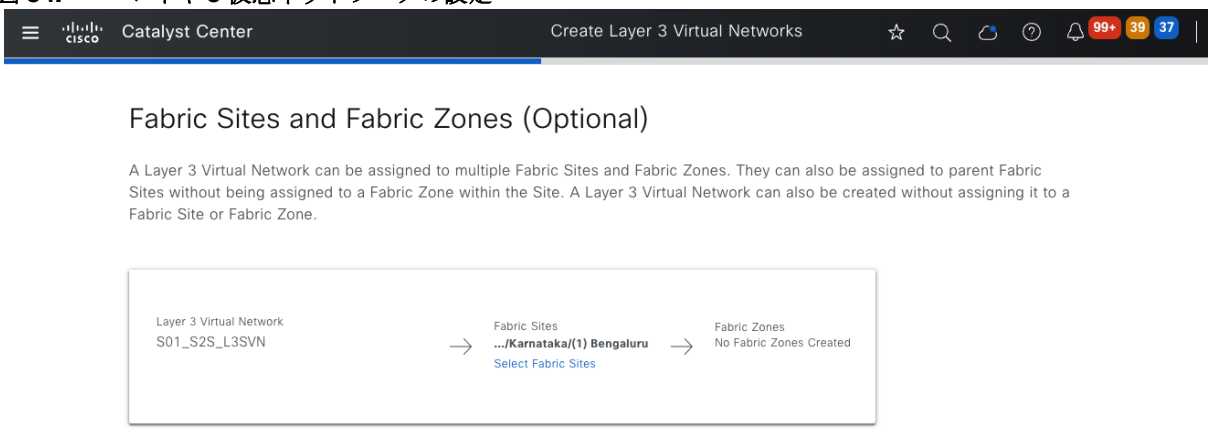
- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- フュージョンデバイスからファイアウォールにすべての通信をリダイレクトしてから、接続先に転送します。
- セキュアなデータ転送のためにサイト間 VPN を設定します。

- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- 各 ODC からの通信を個別に処理するようにファイアウォール インターフェイスを設定します。

手順 6。

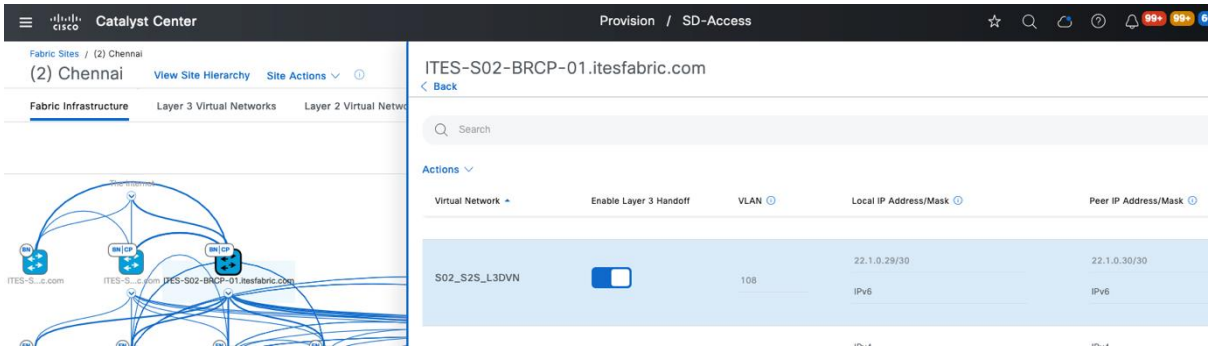
ステップ 1. サイトでレイヤ 3 VN を設定してから、必要なエニーキャストゲートウェイをプロビジョニングします。

図 34.　　レイヤ 3 仮想ネットワークの設定



ステップ 2. 新しく追加した VN のボーダーノードでレイヤ 3 ハンドオフを設定してから、eBGP セッションが稼働していることを確認します。

図 35.　　ボーダーノードでのレイヤ 3 ハンドオフの実行



ステップ 3. ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング
- サイト間 VPN

ステップ 4. ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

ステップ 5. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

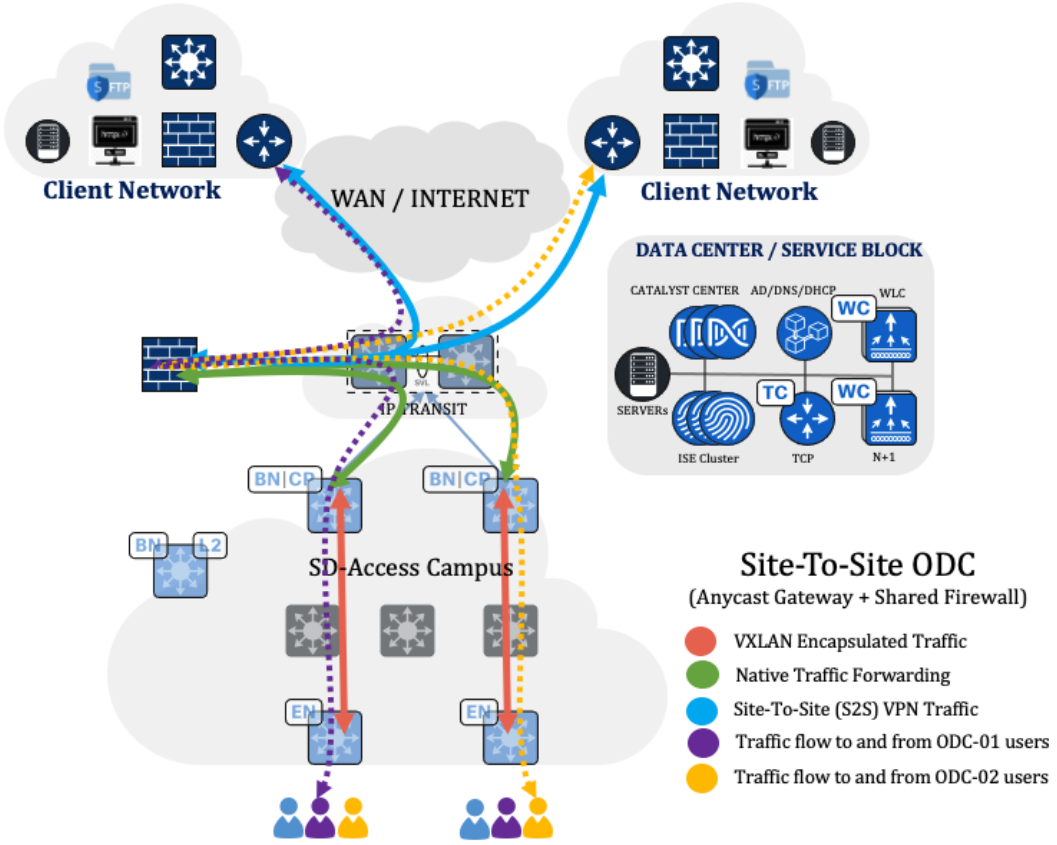
- Cisco ISE と VN のレイヤ 3 ボーダーノードの間で VRF 対応 SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

注： ファイアウォールを通過する VN 通信を設定して、Cisco ISE サーバーとレイヤ 3 ボーダーノードとの間の SXP 通信に特化した TCP バイパスを許可します。

ステップ 6. 認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 36 のようになります。

図 36.　エニーキャストゲートウェイと共有ファイアウォールを使用したサイト間 ODC の通信フロー



注： 通信のフローを示す凡例と矢印を参照してください。

専用ファイアウォールとエニーキャストゲートウェイを使用したクライアント - サイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。

- すべての通信がファイアウォールを通過し、監査とコンプライアンスのためにログ記録されていることを確認します。
- VPN クライアントを使用して、クライアントネットワークに安全に接続します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- ODC 専用ファイアウォールを導入します。

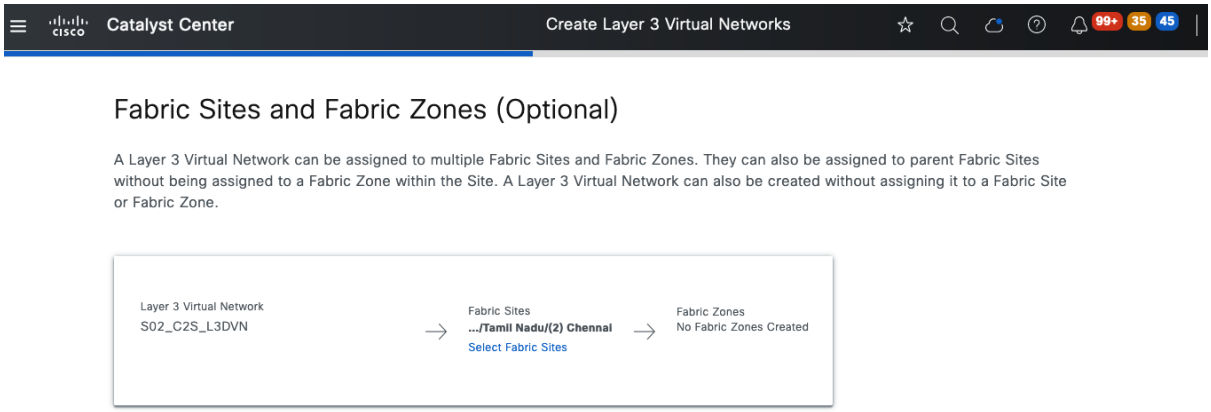
技術要件：

- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- フュージョンデバイスからファイアウォールにすべての通信をリダイレクトしてから、接続先に転送します。
- ODC ユーザーのラップトップおよびデスクトップに VPN クライアントをインストールして、設定を行います。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- ファイアウォール インターフェイスを設定して、専用 ODC からの通信を管理します。

手順 7。

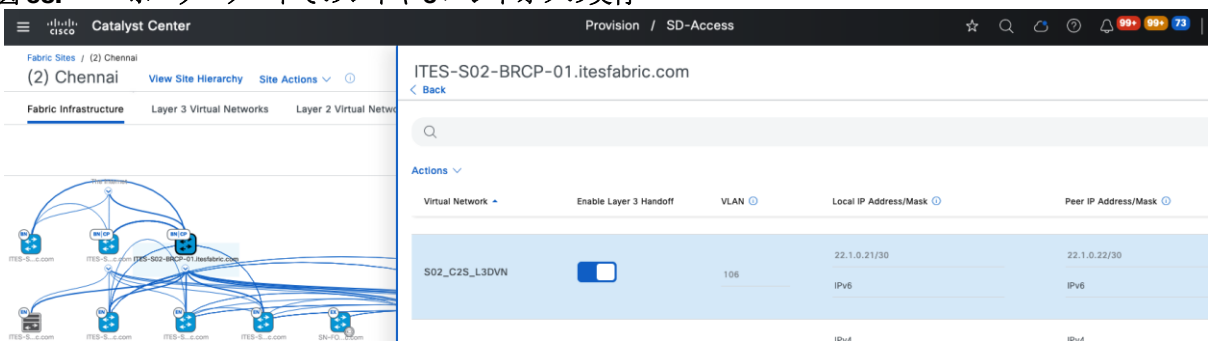
ステップ 1. サイトでレイヤ 3 VN を設定してから、必要なエニーキャストゲートウェイをプロビジョニングします。

図 37.　　レイヤ 3 VN の設定



ステップ 2. 新しく追加した VN のボーダーノードでレイヤ 3 ハンドオフを設定してから、eBGP セッションが稼働していることを確認します。

図 38.　　ボーダーノードでのレイヤ 3 ハンドオフの実行



ステップ 3. ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング

ステップ 4. ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

ステップ 5. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

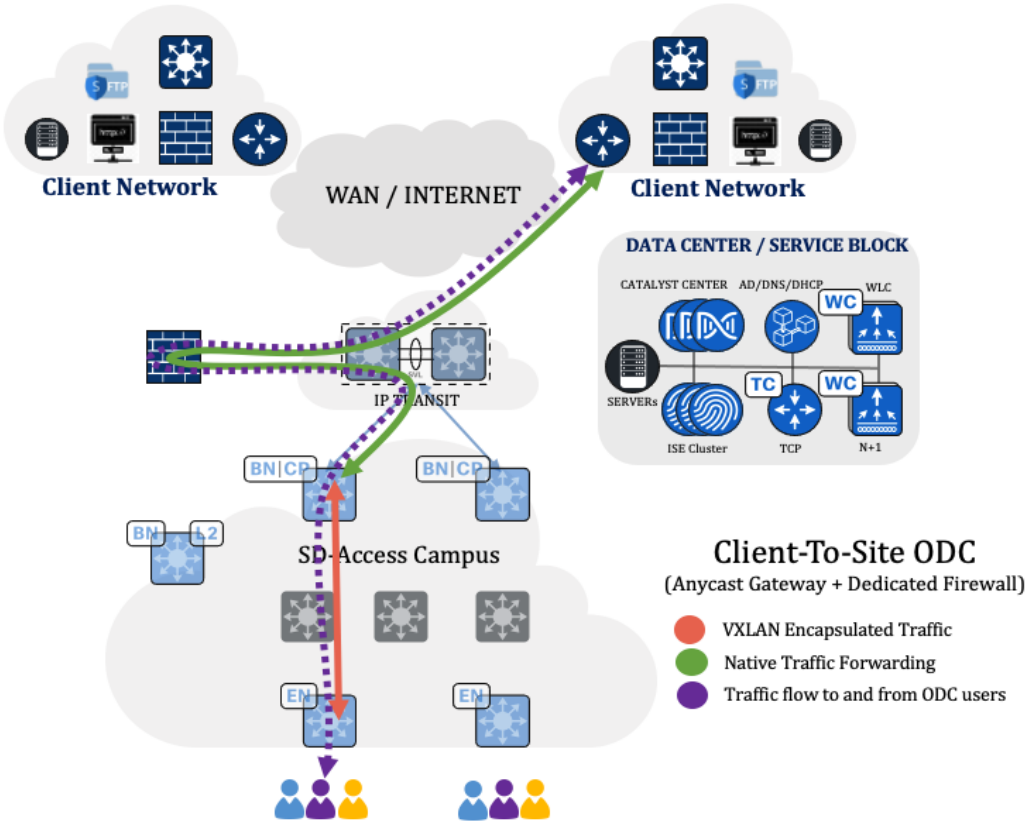
- Cisco ISE と VN のレイヤ 3 ボーダーノードの間で VRF 対応 SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

注： ファイアウォールを通過する VN 通信を設定して、Cisco ISE サーバーとレイヤ 3 ボーダーノードとの間の SXP 通信に特化した TCP バイパスを許可します。

ステップ 6. 認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 39 のようになります。

図 39.　エニーキャストゲートウェイと専用ファイアウォールを使用したクライアント - サイト間 ODC の通信フロー



注： 通信のフローを示す凡例と矢印を参照してください。

共有ファイアウォールとエニーキャストゲートウェイを使用したクライアント - サイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- すべての通信がファイアウォールを通過し、監査とコンプライアンスのためにログ記録されていることを確認します。
- VPN クライアントを使用して、クライアントネットワークに安全に接続します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- 複数の ODC に同じファイアウォールを使用します。

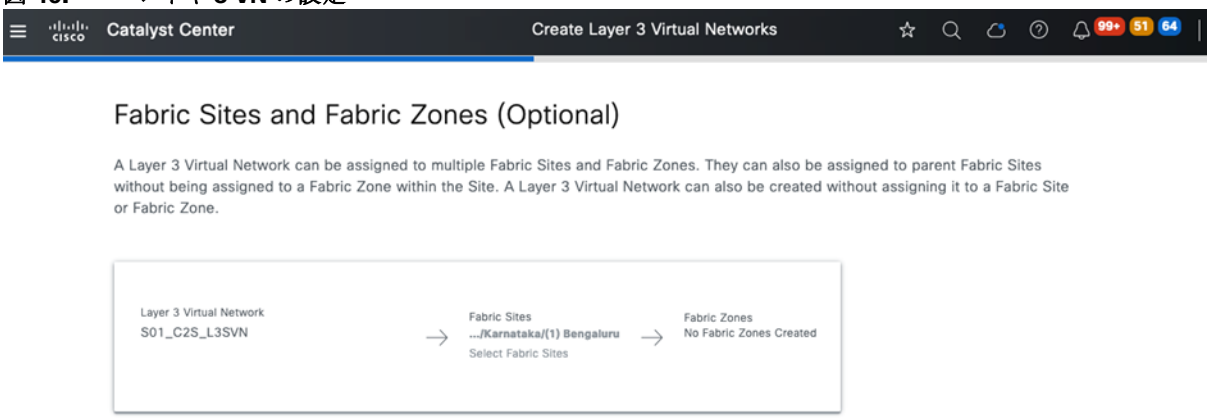
技術要件：

- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- フュージョンデバイスからファイアウォールにすべての通信をリダイレクトしてから、接続先に転送します。
- ODC ユーザーのラップトップおよびデスクトップに VPN クライアントをインストールして、設定を行います。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- 各 ODC からの通信を個別に処理するようにファイアウォール インターフェイスを設定します。

手順 8。

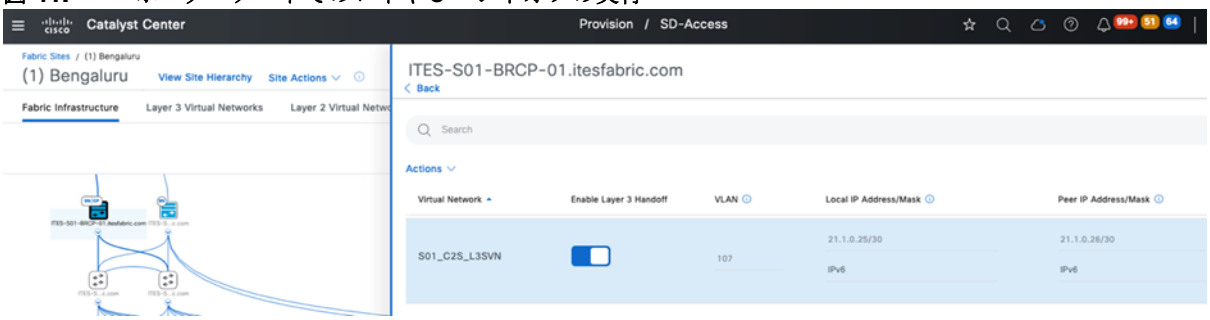
ステップ 1. サイトでレイヤ 3 VN を設定してから、必要なエニーキャストゲートウェイをプロビジョニングします。

図 40. レイヤ 3 VN の設定



ステップ 2. 新しく追加した VN のボーダーノードでレイヤ 3 ハンドオフを設定してから、eBGP セッションが稼働していることを確認します。

図 41.　　ボーダーノードでのレイヤ 3 ハンドオフの実行



ステップ 3.　ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング
- サイト間 VPN

ステップ 4.　ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

ステップ 5.　許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

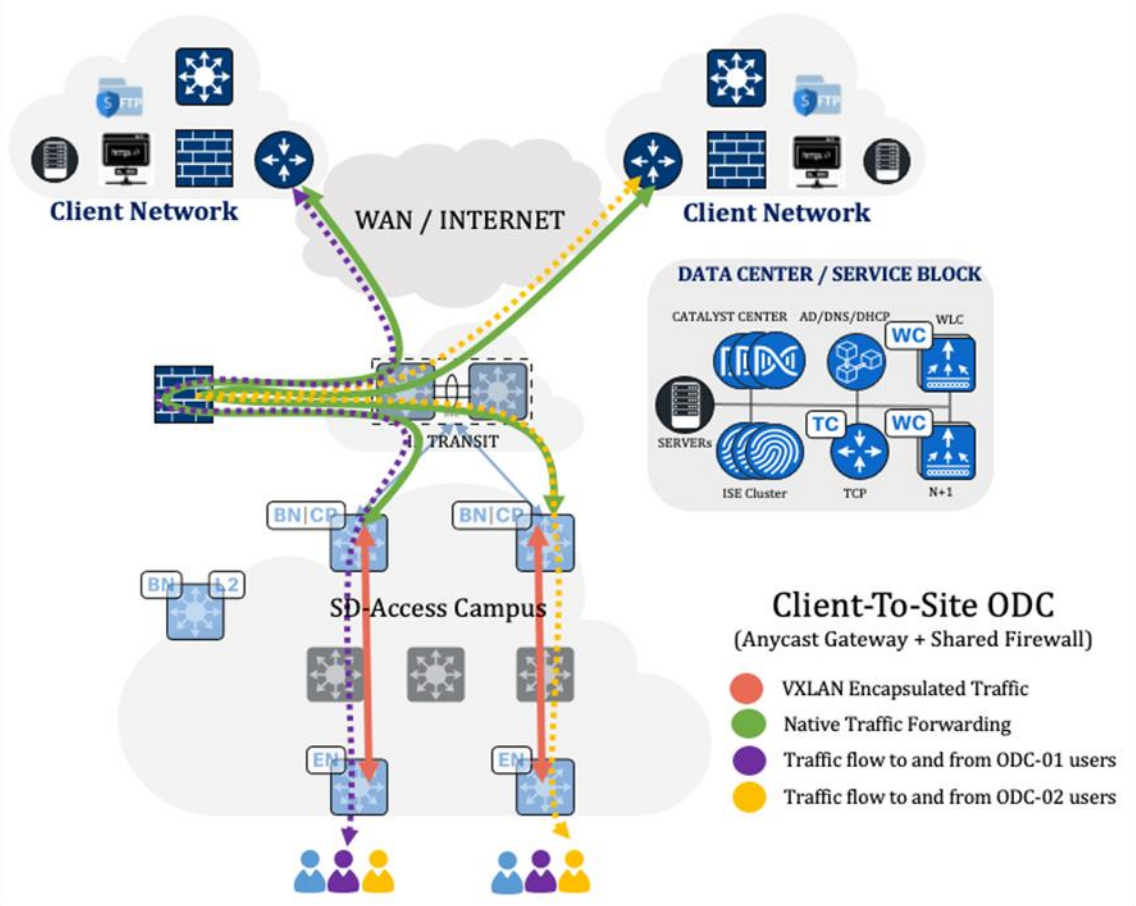
- Cisco ISE と VN のレイヤ 3 ボーダーノードの間で VRF 対応 SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

注：　ファイアウォールを通過する VN 通信を設定して、Cisco ISE サーバーとレイヤ 3 ボーダーノードとの間の SXP 通信に特化した TCP バイパスを許可します。

ステップ 6.　認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 42 のようになります。

図 42.　　エニーキャストゲートウェイと専用ファイアウォールを使用したサイト間 ODC の通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

エッジに接続され、ゲートウェイとして機能している専用ファイアウォールを使用したサイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- クライアントのゲートウェイとして機能するようにファイアウォールを設定し、監査およびコンプライアンス用にすべての通信をログ記録します。
- 専用ファイアウォールがファブリックエッジノードに直接接続されていることを確認します。
- ネットワーク間におけるデータのセキュアな転送を確保します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- ODC 専用ファイアウォールを導入します。

技術要件：

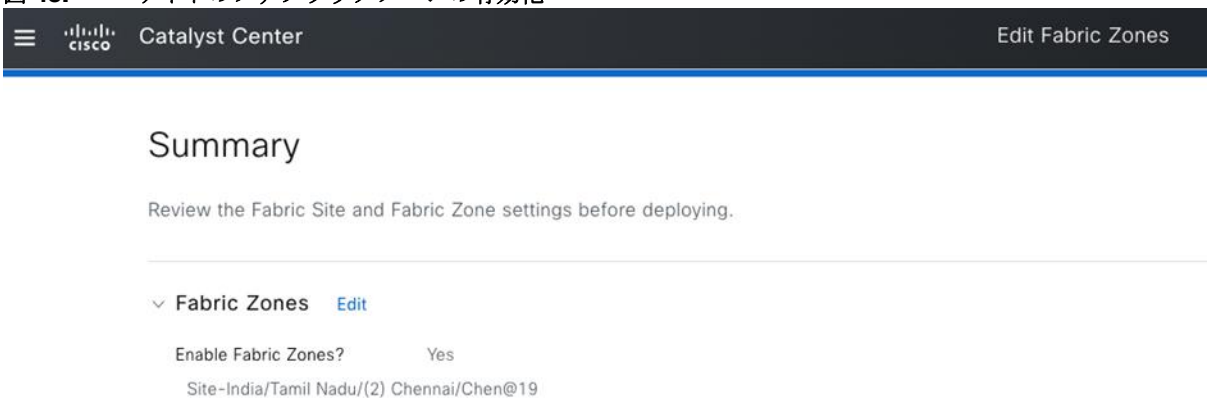
- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- レイヤ 2 VN をプロビジョニングし、ファブリックゾーンに追加します。

- すべての ODC ユーザーおよびシステム、ならびにファイアウォールが、ファブリックゾーン内のエッジノード上で接続されていることを確認します。ファイアウォールに接続するポートは、トランクポートとして設定する必要があります。
- セキュアなデータ転送のためにサイト間 VPN を設定します。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- ファイアウォール インターフェイスを設定して、専用 ODC からの通信を管理します。

手順 9。

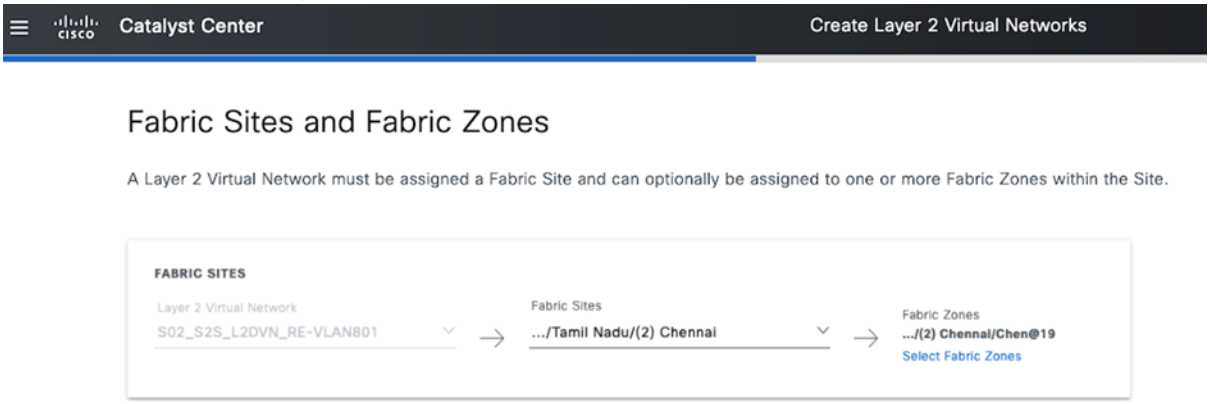
ステップ 1. ODC ユーザー、システム、およびファイアウォールがエッジノードに接続されているサイトのファブリックゾーンを有効にします。

図 43.　サイトのファブリックゾーンの有効化



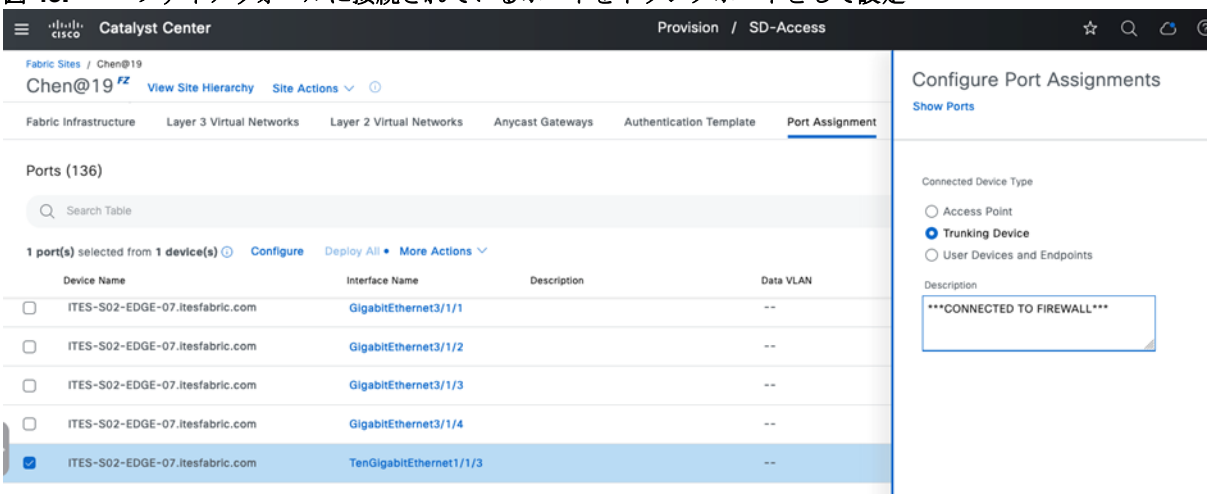
ステップ 2. 適切な VLAN 識別子を使用してレイヤ 2 VN を作成します。次に、ファブリックサイトとファブリックゾーンの両方にその VN を割り当てます。

図 44.　レイヤ 2 VN の設定



ステップ 3. エッジノードのファイアウォールに接続されているポートを、トランクポートとして設定します。

図 45.　　ファイアウォールに接続されているポートをトランクポートとして設定



ステップ 4. ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング
- サイト間 VPN

ステップ 5. ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

ステップ 6. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

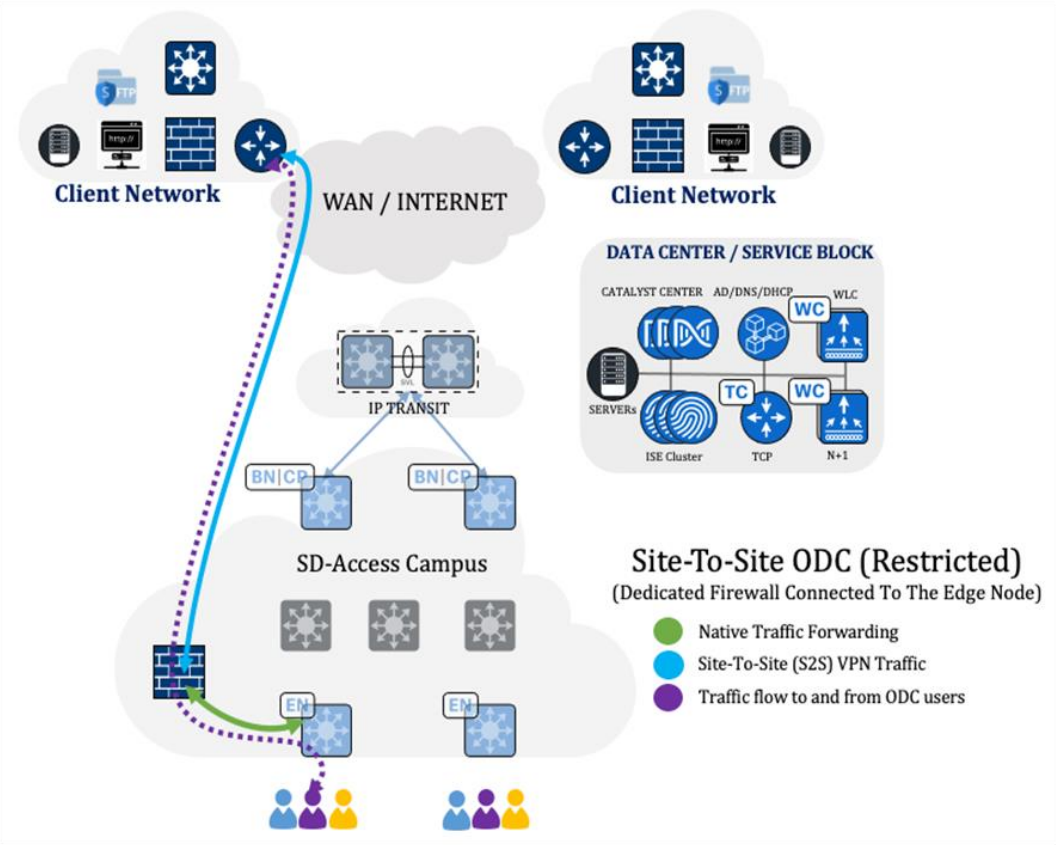
- Cisco ISE と VN のレイヤ 3 ボーダーノードの間で VRF 対応 SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

注：　ファイアウォールを通過する VN 通信を設定して、Cisco ISE サーバーとレイヤ 3 ボーダーノードとの間の SXP 通信に特化した TCP バイパスを許可します。

ステップ 7. 認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 46 のようになります。

図 46.　　エッジノードに接続されている専用ファイアウォールを使用したサイト間 ODC の通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

エッジに接続され、ゲートウェイとして機能している専用ファイアウォールを使用したクライアント - サイト間 ODC

ビジネス要件：

- Cisco SD-Access を使用して ODC を確立します。
- 専用ファイアウォールがファブリックエッジノードに直接接続されていることを確認します。
- クライアントのゲートウェイとして機能するようにファイアウォールを設定し、監査およびコンプライアンス用にすべての通信をログ記録します。
- VPN クライアントを使用して、クライアントネットワークに安全に接続します。
- 該当する ODC 内のシステムに対する ODC ユーザーのアクセスを制限します。
- ODC 専用ファイアウォールを導入します。

技術要件：

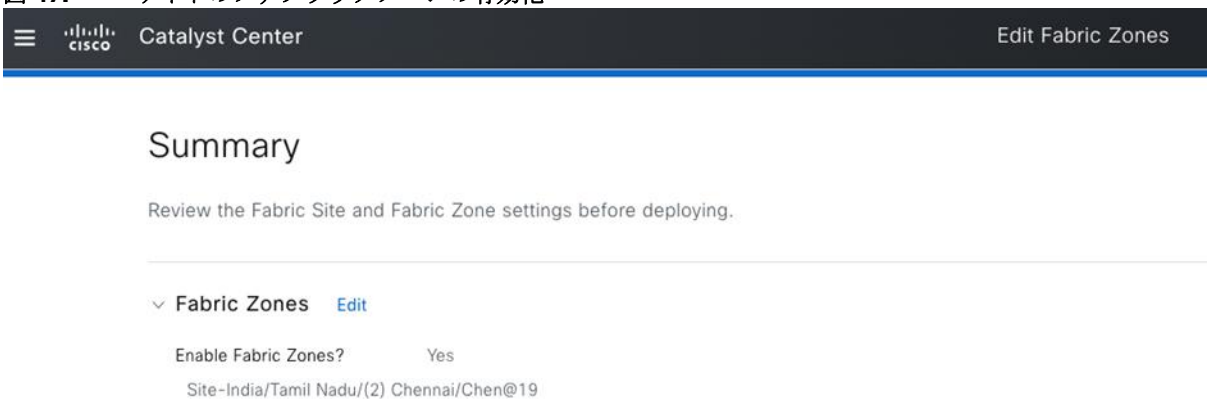
- Catalyst Center を使用して Cisco SD-Access ネットワークをプロビジョニングします。
- レイヤ 2 VN をプロビジョニングし、ファブリックゾーンに追加します。
- すべての ODC ユーザー、システム、およびファイアウォールが、ファブリックゾーン内のエッジノードに接続されていることを確認します。ファイアウォールに接続するポートは、トランクポートとして設定する必要があります。

- ODC ユーザーのラップトップおよびデスクトップに VPN クライアントをインストールして、設定を行います。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- ファイアウォールを設定して、専用 ODC からの通信を管理します。

手順 10。

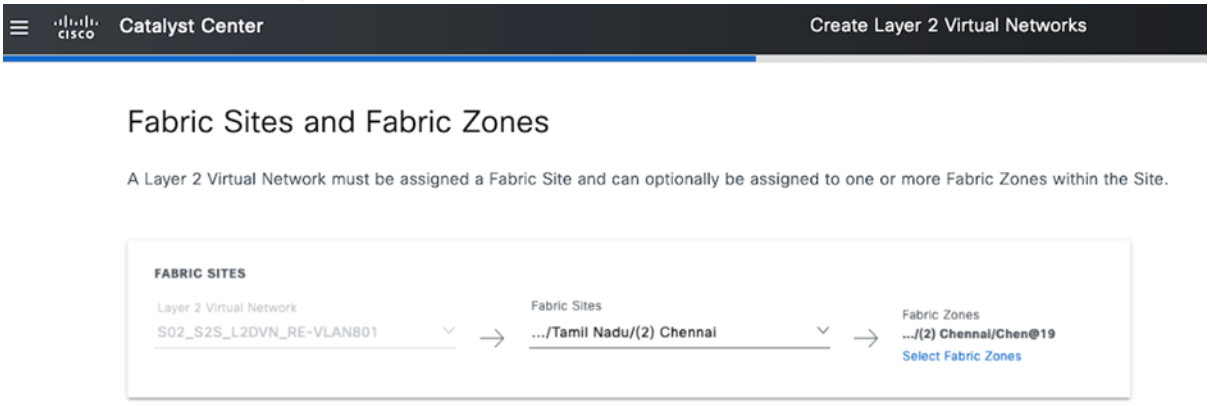
ステップ 1. ODC ユーザー、システム、およびファイアウォールがエッジノードに接続されているサイトのファブリックゾーンを有効にします。

図 47.　サイトのファブリックゾーンの有効化



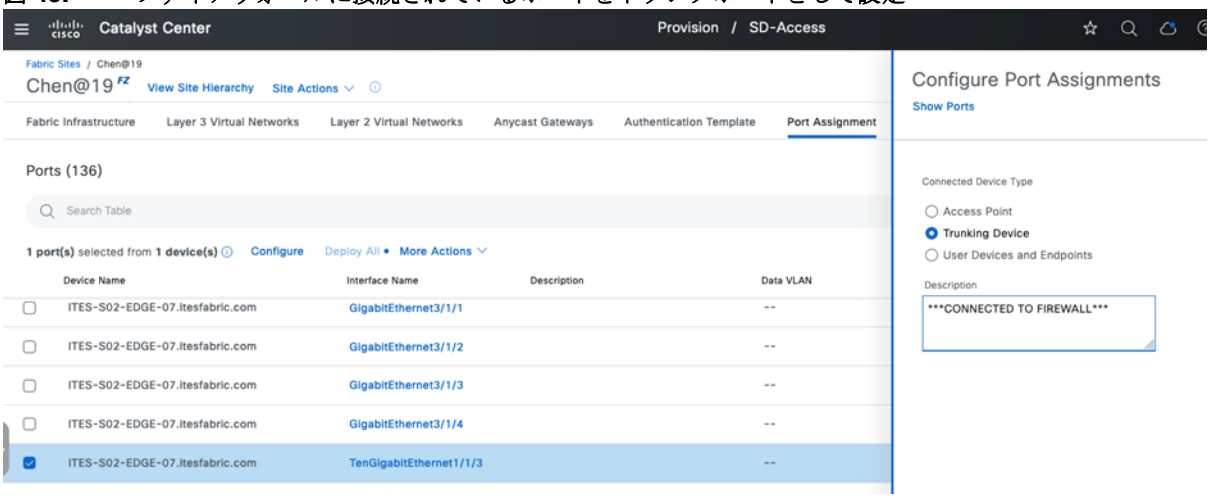
ステップ 2. 適切な VLAN 識別子を使用してレイヤ 2 VN を作成します。次に、ファブリックサイトとファブリックゾーンの両方にその VN を割り当てます。

図 48.　レイヤ 2 VN の設定



ステップ 3. エッジノードのファイアウォールに接続されているポートを、トランクポートとして設定します。

図 49.　　ファイアウォールに接続されているポートをトランクポートとして設定



ステップ 4.　ファイアウォールでエンドツーエンド通信を有効にします。少なくとも次の項目を設定する必要があります。

- 内部インターフェイス（ODC のクライアントゲートウェイとして、物理インターフェイスかサブインターフェイスを指定）
- 外部インターフェイス
- ファイアウォールポリシー
- 到達可能性を実現するためのルーティング

ステップ 5.　ODC ユーザーと企業ユーザーの両方に対して適切な認証と承認が行われるように Cisco ISE を設定します。

ステップ 6.　許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

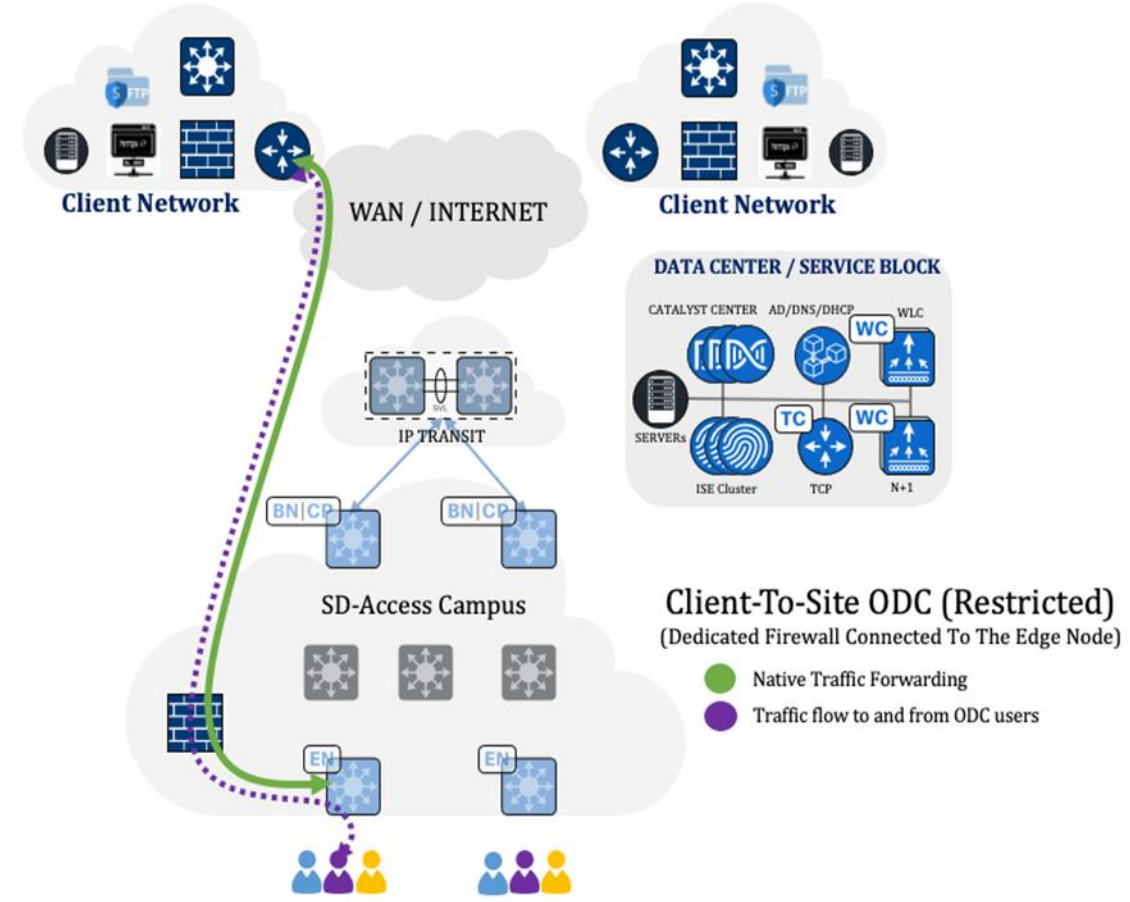
- Cisco ISE と VN のレイヤ 3 ボーダーノードの間で VRF 対応 SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

注：　ファイアウォールを通過する VN 通信を設定して、Cisco ISE サーバーとレイヤ 3 ボーダーノードとの間の SXP 通信に特化した TCP バイパスを許可します。

ステップ 7.　認証が正常に完了すると、エンドユーザーは承認されたすべてのリソースにアクセスできるようになります。

展開が成功すると、ODC とクライアントのネットワーク間の通信フローは図 50 のようになります。

図 50.　　エッジノードに接続されている専用ファイアウォールを使用したクライアント - サイト間 ODC の通信フロー



注：　通信のフローを示す凡例と矢印を参照してください。

専用ファイアウォールとエニーキャストゲートウェイを使用したサイト間 ODC のロケーション非依存アクセス

ビジネス要件：

- ITES 顧客のオフィス再開（RTO）要件は次のとおりです。
  - ODC クライアントの場所を抽象化し、任意の ITES サイトから作業できるようにします。
  - クライアント通信は分類され、外部への送信のためにホームロケーションにトンネリングされる必要があります。
- 既存のサイト間 ODC ユーザーは、任意の ITES サイトから作業できる必要があります。
- ODC ユーザーは、場所に関係なく、それぞれの ODC 内のシステムにのみアクセスできる必要があります。
- ホームロケーションのサイト間 ODC に既存の専用ファイアウォールを利用します。

技術要件：

- サイト非依存クライアント用のレイヤ 3 VN をプロビジョニングします。これはドキュメント全体で「ローミング VN」と呼ばれます。
- ホームサイトを除くすべての必要なリモートサイトで、ローミング VN の下にエニーキャストゲートウェイを展開します。

- ルータをインストールして、ローミング VN 通信用の SGT ベースのポリシーベースルーティング（PBR）を導入します。
- ローミングユーザーに対して適切な認証と承認が行われるように Cisco ISE を設定します。
- マクロ（VN）またはマイクロ（SGT）セグメンテーションを使用して、ODC ユーザーとシステムを分離します。
- ローミングユーザー用に新しく追加されたサブネットに対応するように、既存のファイアウォールポリシーとサイト間 VPN 設定を更新します。

技術的なヒント： 通常、ローミング VN は、さまざまな地理的場所でのシームレスな接続性とモビリティを容易にする仮想ネットワークです。これにより、ユーザーはサイト間を移動した場合でも、一貫したネットワークアクセスとサービスを引き続き利用できます。ローミング VN は、ITES インフラストラクチャ内の物理的な場所に関係なく、ユーザーエクスペリエンスの継続性と安全性を維持する上で不可欠です。

前提条件：

- LISP Pub/Sub トランジットを使用したマルチサイト SD-Access。
- SGT ベースの PBR を実行するルータ。
- ホームサイトで専用ファイアウォールを使用したサイト間 ODC。

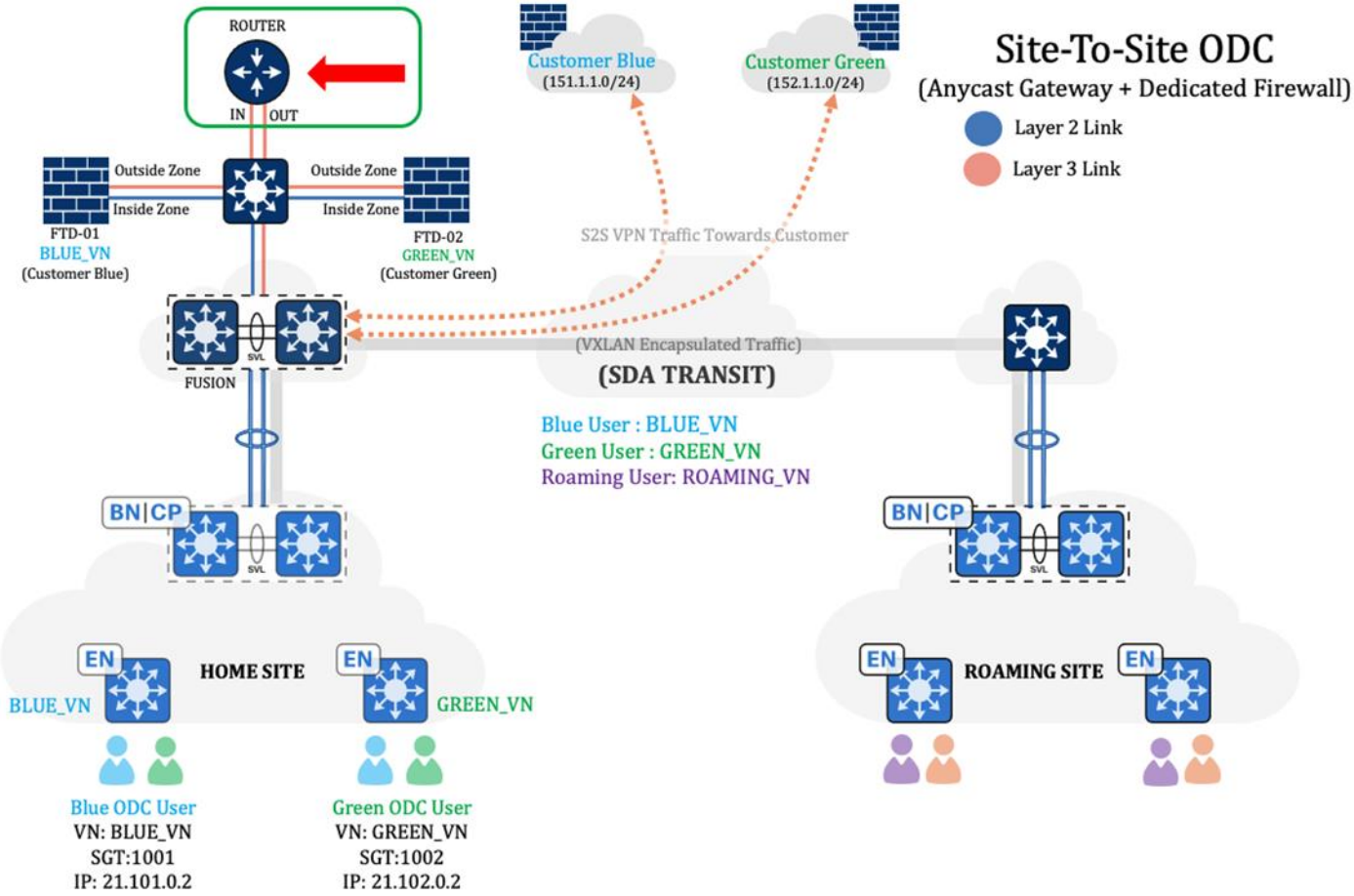
手順 11。

ステップ 1. ローミング VN と呼ばれる、ロケーション非依存クライアント用のレイヤ 3 VN をプロビジョニングし、SD-Access トランジット（つまり LISP Pub/Sub）を介して接続された、ホームサイトを含むすべての必要なリモートサイトに展開します。

ステップ 2. ホームサイトを除くすべての必要なリモートサイトで、ローミング VN の下にエニーキャストゲートウェイを展開します。次に、通信の外部送信のために、ホームサイトでレイヤ 3 ハンドオフを実行します。

ステップ 3. ホームロケーションにルータをインストールして、SGT ベースの PBR を導入します。ルータの配置については、図 51 のトポロジを参照してください。

図 51.　　ホームサイトに展開されたルータ



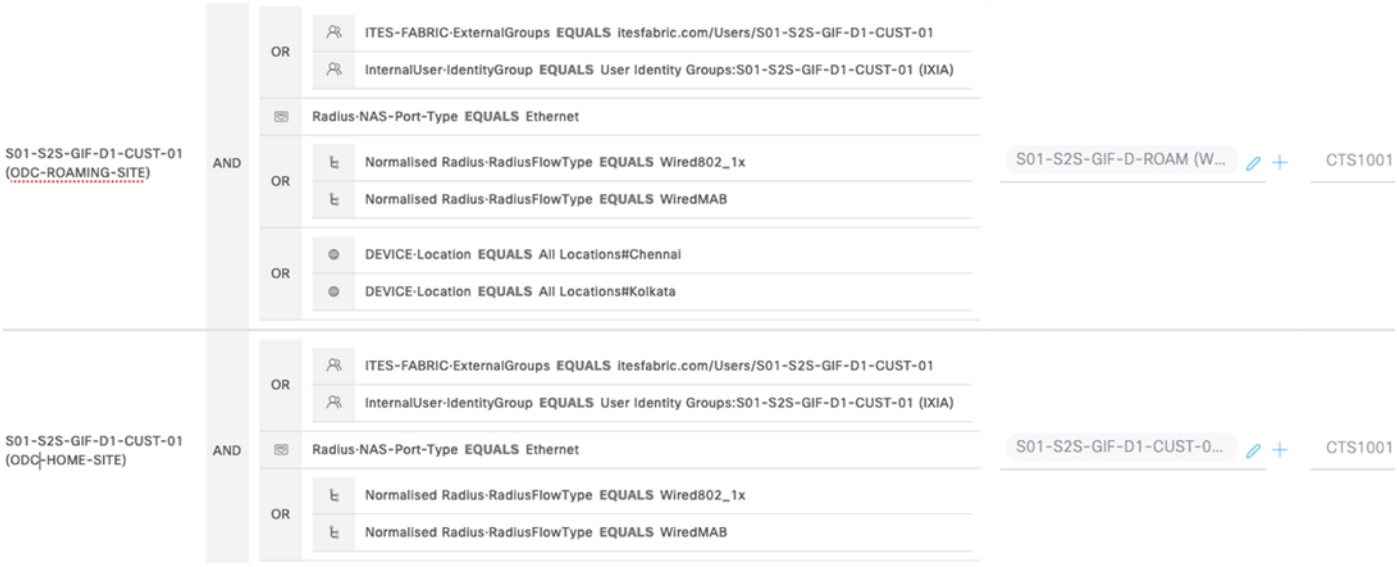
ステップ 4.　ローミングサイトからオンボーディングする際に、ローミングユーザーに対して適切な認証と承認が行われるようにするには、次の手順に従って ISE を設定します。

i. 各ローミングサイトの ISE で、ネットワークデバイス グループの下にロケーションを作成します。

ii. 既存のネットワーク アクセス デバイス（NAD）のロケーションを更新し、それぞれのロケーションに割り当てます。

iii. ローミングユーザーのオンボーディング用に、認証プロファイルと認証ポリシーを設定します。

図 52.　　ホームユーザーおよびローミングユーザー用に作成されたサンプル認証ポリシー



技術的なヒント：　エンドユーザーの認証前に適切な属性が確実に照合されるよう、ローミングユーザーのポリシーはホームユーザーのポリシーの上に配置します。

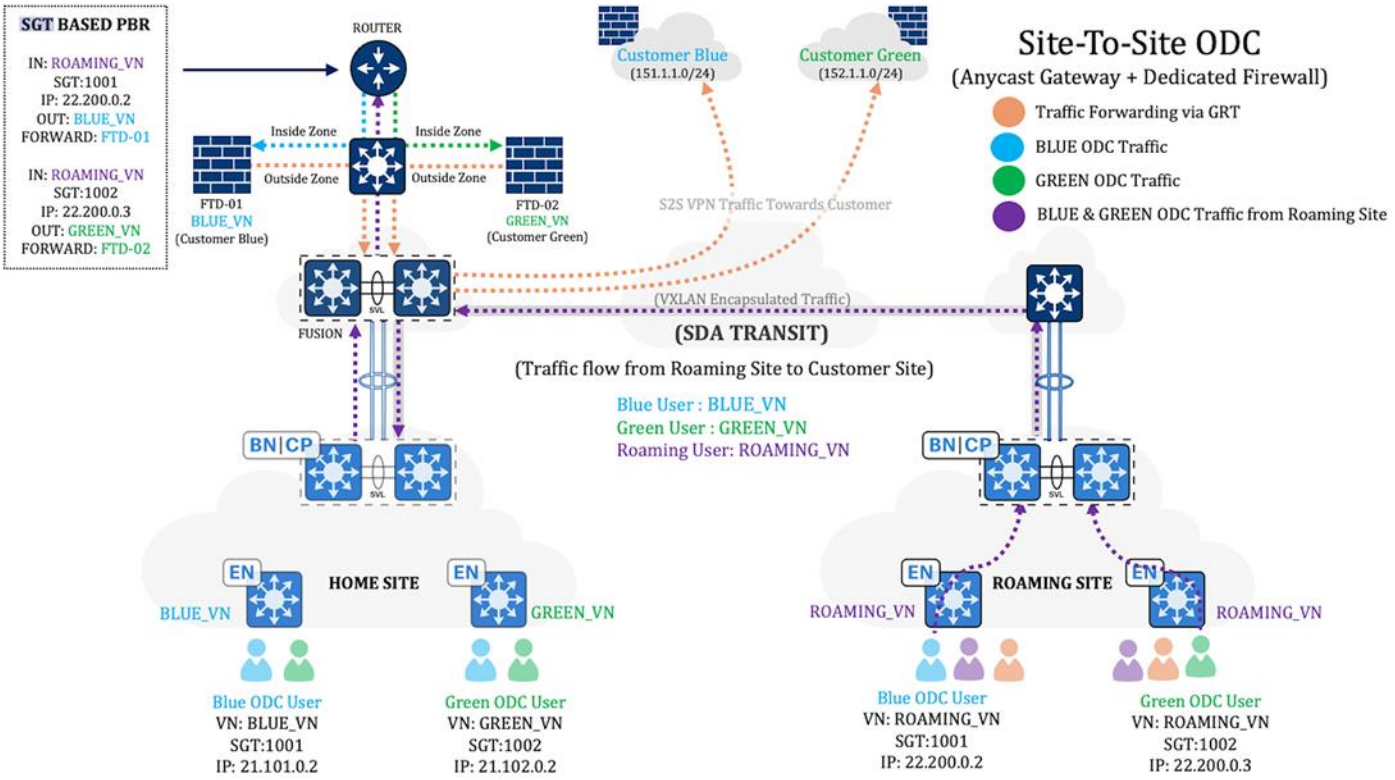
ステップ 5.　既存のサイト間ファイアウォールポリシーを更新して、ローミング VN サブネットからの通信を許可します。さらに、サイト間 VPN 用の保護されたネットワークとしてローミング VN サブネットを含め、それに応じて NAT ポリシーを更新します。

ステップ 6.　顧客サイトを宛先とする通信のルーティングを設定します。

- 顧客サイトを宛先とする、ホームサイトのサイト間 ODC ユーザーからの通信は、その ODC の専用ファイアウォールに転送する必要があります。
- 顧客ネットワークを宛先とする、ローミングサイトのサイト間 ODC ユーザーからの通信（つまり、ローミング VN 通信）は、ルータを接続先にする必要があり、そこで SGT ベースの PBR によって適切なファイアウォールにルーティングされます。

注：　ローミングクライアントのタグがステアリングルータまで保持されていることを確認してください。

図 53.　　顧客ネットワークを宛先とする通信



注：　通信のフローを示す凡例と矢印を参照してください。

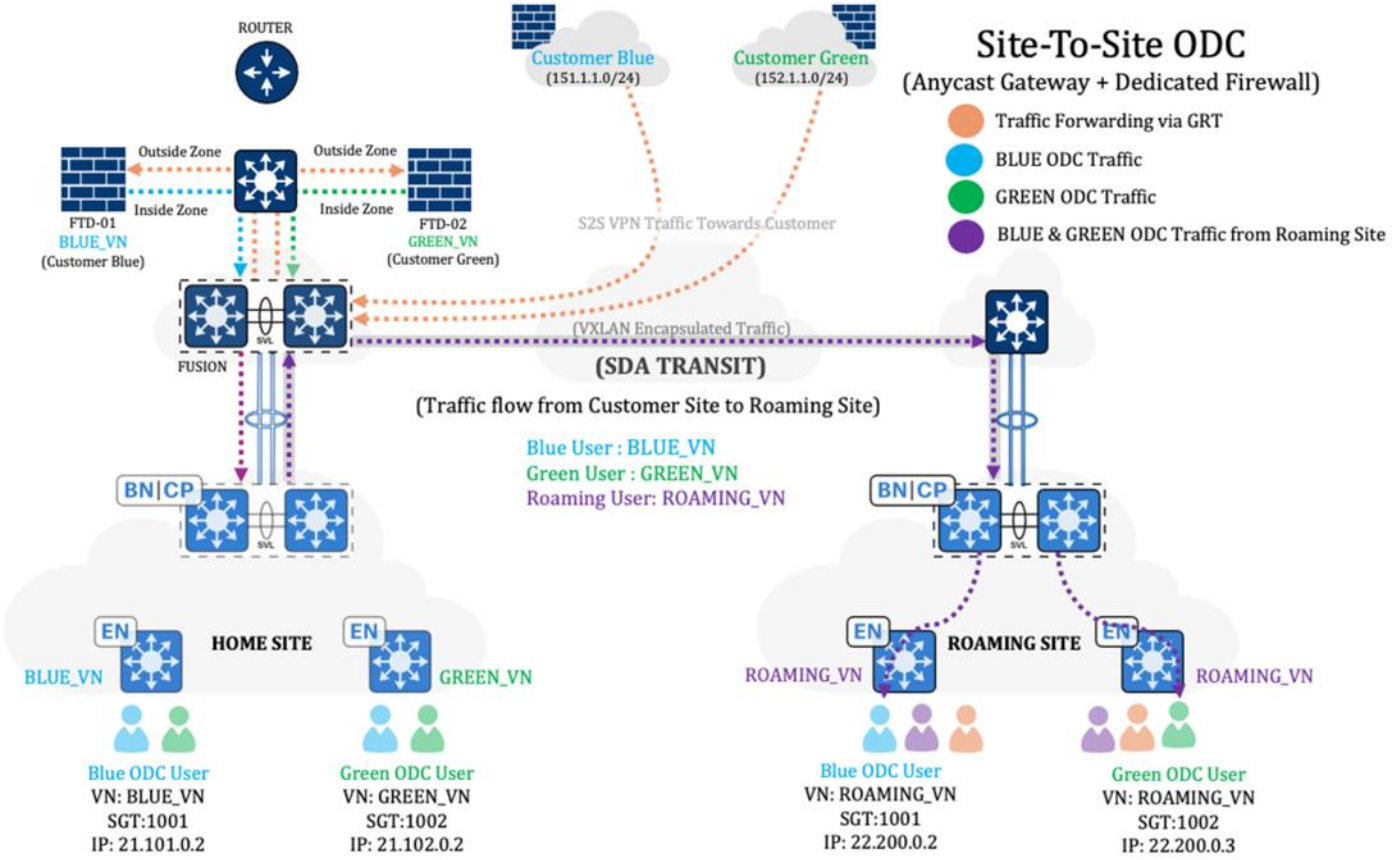
次に、図 53 に示すトポロジでの、ローミングサイトから顧客サイトへの通信フローの概要を示します。

- ローミングサイトからのローミングクライアント通信（紫色のフロー）は、ホームサイトのボーダーノードとフュージョンを介してルータに転送されます。
- 次に、ルータが SGT ベースの PBR を実行し、SGT 1001 の入力通信を Customer Blue のファイアウォール（FTD-01）の内部ゾーンに、SGT 1002 の通信を Customer Green のファイアウォール（FTD-02）の内部ゾーンに転送します。

ステップ 7. ローミングサイトを宛先とする通信のルーティングを、以下のように設定します。

- リターン通信、つまり顧客サイトを起点とする、ローミングサイト宛ての通信をフュージョンノードに転送するように、サイト間 ODC ファイアウォールを設定します。
- サイト間 ODC VN がローミングサブネットについての情報を、またはローミングサブネットがサイト間 ODC VN についての情報を収集できるように、フュージョンノードで VRF ルートリークを設定します。

図 54.　　ローミングサイトを宛先とする通信



注：　通信のフローを示す凡例と矢印を参照してください。

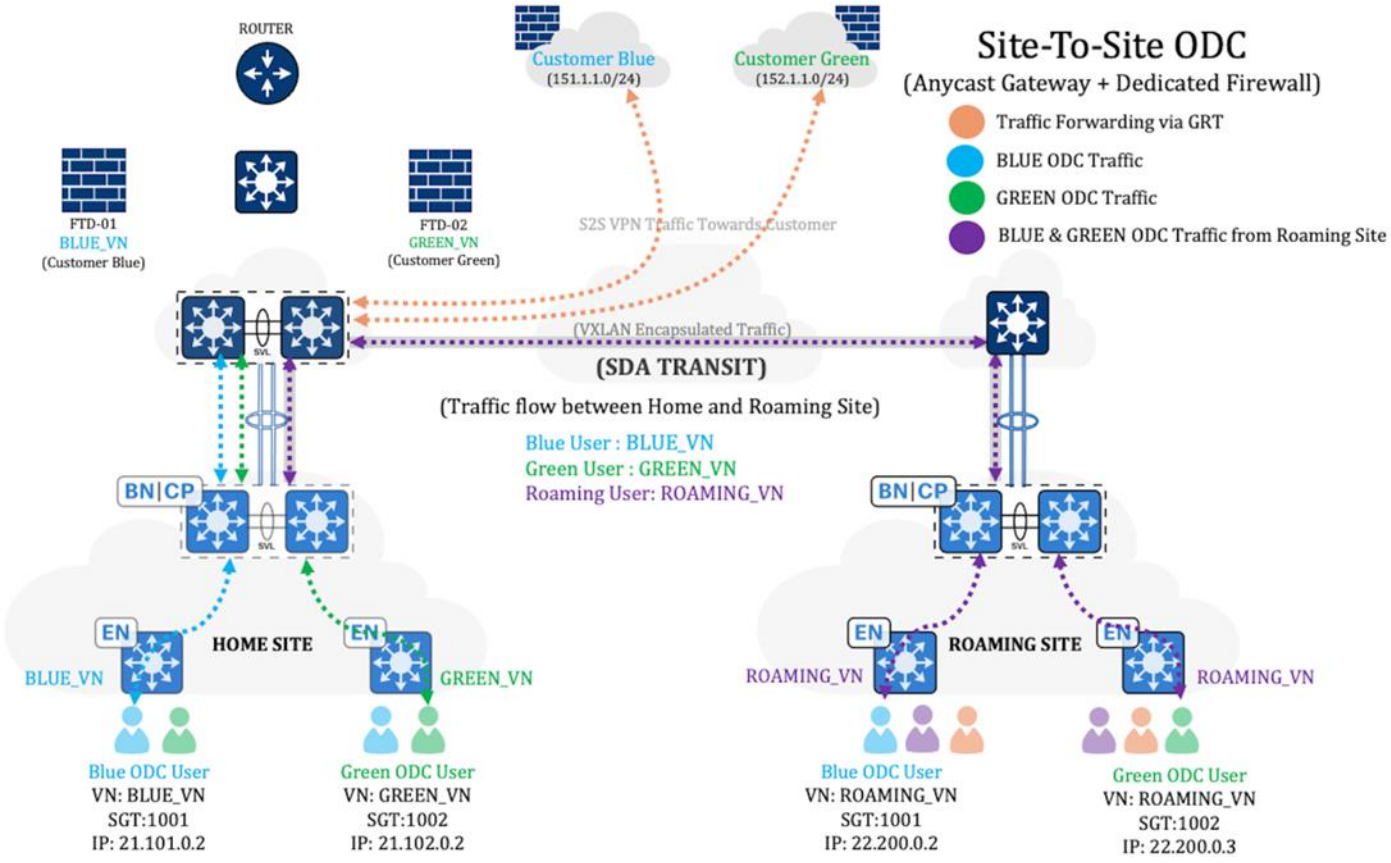
次に、図 54 に示すトポロジでの、顧客サイトからローミングサイトへの通信フローの概要を示します。

- 顧客サイトから発信され、ローミングサイトの Blue ODC および Green ODC クライアントを宛先とする通信は、まず顧客の専用ファイアウォールで受信されてから、そのファイアウォールによってフュージョンノードに転送されます。
- フュージョンノードは、この通信をホームサイトのボーダーノードでローミング VN に渡し、その後ローミング VN がローミングサイトに送信します。

ステップ 8. ホームサイトとローミングサイトからオンボーディングされたサイト間 ODC ユーザー同士の通信は、ホームサイトで Cisco SD-Access を介して他のサイトにインターネット経由でアクセスできる場合に限り、ルート交換の一部として適切に機能します。そうでない場合は、次のタスクを実行する必要があります。

- ホームサイトのボーダーノード上のローミング VN が、サイト間 ODC サブネットを認識するようにします。
- ルートを LISP インスタンスにインポートします。

図 55.　　ホームサイトとローミングサイト間の通信



注：　通信のフローを示す凡例と矢印を参照してください。

ステップ 9. 許可リスト（デフォルトの拒否 IP）が有効になっている場合は、次のオプションのいずれかを選択します。また、送信元および接続先のセキュリティタグに正しいポリシーマトリックスが設定されていることを確認します。

- Cisco ISE と VN のレイヤ 3 ボーダーノードの間で VRF 対応 SXP セッションを確立し、接続先アドレスのセキュリティタグを取得します。
- サブネットから SGT へのマッピングを手動で設定します。

ハードウェアとソフトウェアの仕様

この ITES 分野は、表に記載されているハードウェアおよびソフトウェアでテストされています。Cisco SD-Access ソリューションでサポートされているハードウェアの完全なリストについては、「Cisco Software Defined Access Compatibility Matrix」を参照してください。

ハードウェアまたはソフトウェア コンポーネント	サポートされるソフトウェア バージョン	
Catalyst Center アプライアンス （*部品番号：DN3-HW-APL-XL*）	2.3.7.9	2.3.7.10
Identity Services Engine（ISE）	3.3 パッチ 4	3.4 パッチ 3
コントロールプレーンノード *Cisco Catalyst 8000V Edge ソフトウェア*	17.12.4b、17.15.2a	17.12.4b、17.15.2a
ファブリックボーダーノード *Cisco Catalyst 9500 および 9600 シリーズ スイッチ*	17.9.6a、17.12.5、17.15.3	17.12.6、17.15.4d、17.18.3
ファブリック エッジ ノード *Cisco Catalyst 9200、9300 および 9400 シリーズ スイッチ*	17.9.6a、17.12.5、17.15.3	17.12.6、17.15.4d、17.18.3
ワイヤレスコントローラ *Cisco Catalyst 9800-40 および 9800-CL*	17.12.5、17.9.6	17.12.6、17.15.4d、17.18.3
Cisco Secure Firewall Management Center（FMC）： *Management Center Virtual*	7.4.2	7.4.2
Cisco Secure Firewall Threat Defense（FTD） *Firewall Threat Defense Virtual および Cisco Firepower 1150*	7.4.2	7.4.2

多次元尺度値

カテゴリ	値
インベントリ内のデバイス（ルータ、スイッチ、ワイヤレスコントローラ）	5000
ファブリックサイトの数	100
建物とフロアの数	4000
サイトあたりの IP プールの数	1000
サイトあたりの VN の数	128
サイトあたりのワイヤレスコントローラの数	HA で 2
AP の数（ファブリックおよび非ファブリック）	8000
SGT の数	4000
グループベースのポリシーの数	12,000
エンドポイントの数	100,000（30% 有線、70% ワイヤレス）
ルートマップエントリ（一致および設定）：SGT ベースのポリシーベースルーティング（PBR）用	125

注： 公式にサポートされているスケールの概要はこの データシートにあります。ここに示すデータはラボで検証済みです。

効率的な展開を実現できる Network as Code（NaC）

ITES ネットワークの展開では、Network as Code（NaC）アプローチが採用されています。これにより、ITES インフラストラクチャにおける一貫性、拡張性、および再現性のある設定を実現できます。Cisco Catalyst Center ベースの展開用に開発された Ansible Playbook を利用することで、展開ライフサイクル全体を完全に自動化します。これには、プロビジョニングと初期設定から最終的な検証までの、すべての内容が含まれます。これにより、手動の労力と人的エラーの可能性が大幅に削減されます。これによって業務効率が向上し、変更の実装が迅速化されるとともに、アジャイルなネットワーク管理に関する最新の DevOps 原則と一致します。

ネットワーク自動化のプラクティスの詳細については、自動化リポジトリを確認することをお勧めします。このリポジトリでは、実用的な例、ITES ネットワークの展開に合わせて調整された再利用可能な Ansible Playbook、および拡張性と効率性に優れたネットワーク運用をサポートするように設計された実証済みのベストプラクティスを紹介しています。リポジトリにアクセスしてより深いインサイトを取得し、自動化プロセスを開始してください。

詳細については、次のリポジトリを参照してください。

https://github.com/DNACENSolutions/NetworkasCode_CVPs

https://github.com/DNACENSolutions/NetworkasCode_CVPs/tree/main/nac_ites_sda

シスコの関連ドキュメントへのリンク

- Cisco SD-Access Solution Design Guide（CVD）
- Catalyst Center のユーザーロール権限
- ディザスタリカバリの実装
- Cisco Catalyst Center リリースノート
- Cisco Catalyst Center Security Best Practices Guide
- ソフトウェア定義アクセス（SD-Access）プロビジョニングのベストプラクティスガイド

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。

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。

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。