CISCO VALIDATED DESIGN

SD-Access セグメンテーション設計ガイド

2018 年 5 月

目次

はじめに 1

インテント（目的）ベースのネットワーキングとセグメンテーション 2

SD-Access での仮想ネットワークと SGT について理解する 4

ファブリック外部に送信されるトラフィックへのポリシー適用 9

ネットワーク セグメントの定義 16

仮想ネットワークまたは拡張可能グループ タグ 17

使用例 21

大学 21

製造業 22

医療 24

PCI および小売 26

電力 26

付録 A：ネットワーク セグメンテーションの概要：簡単な経緯 28

VLAN およびプライベート VLAN 28

仮想ルーティング/フォワーディング インスタンス 29

Cisco TrustSec：ソフトウェアデファインド セグメンテーション 31

付録 B：リファレンス 34

はじめに

サイバー攻撃の数は日々増え続けており、あらゆるタイプの組織が攻撃対象になっています。攻撃側も、個人から、犯罪組織、国家の支援を受けたハッカーまでさまざまです。クレジット カード データの取得による金銭的利益、ランサムウェアによる恐喝、個人データへのアクセスによる ID 窃盗、サービスの中断など、その目的を問わず、攻撃の頻度は増え続け、高度化しています。さらに、利用できるオープンソースのコードベースやツールが増え、攻撃に高度なスキルが求められなくなったことで、比較的技術の低い攻撃者でも攻撃しやすくなっています。

そのため組織は、組織を守るテクノロジーや製品の特定に苦慮し、それらを取得して導入/運用するために必要な予算の確保も困難になっています。Cisco Firepower® 次世代ファイアウォールおよび侵入防御システム、Cisco® Web セキュリティ アプライアンス（WSA）、Cisco Advanced Malware Protection や、ネットワークの可視性を高める Cisco Stealthwatch®、認可されたユーザ、ゲスト、IoT デバイスに対するポリシー適用とセキュアなネットワーク アクセスを実現する Cisco Identity Services Engine などの製品はすべて、組織を保護する多層防御戦略にとって効果的です。採用を決めると、重点は導入戦略の定義に移ります。導入戦略とは、認可されたユーザだけがネットワークにアクセスできるようにし、エンドポイントからデータセンターにわたって通信をモニタして異常な動作を検知することで、組織の重要な資産やデータを保護するためのものです。

他のすべてのセキュリティ製品の基盤として考慮すべき、もう 1 つ非常に効果的な戦略は、ネットワーク セグメンテーションによって攻撃の範囲を限定することです。ネットワーク セグメンテーションとは、1 つのルーティング テーブルを使用する 1 つの大規模なネットワークを、任意の数の小規模な仮想/論理ネットワークまたはゾーンに分解もしくは分割するプロセスです。セグメント化されたネットワークと、セグメント内外にポリシーを適用するセキュリティ制御によって、次のことが可能になります。

- セグメント間を分離することで、法規制に準拠する
- 攻撃対象領域を最小限に抑え、1 つのセグメントに限定することで、水平方向のマルウェア伝播を制限する
- セグメント間に適用ポイントを導入し、ステートフル パケット インスペクションを実装する
- さらに細かいマイクロセグメンテーションが可能な環境を構築する

このドキュメントでは、ネットワークをセグメント化する、Cisco SD-Access の優れた機能について詳細に説明します。アーキテクチャに関する理解を深め、さらに戦略的なアプローチを進めるために役立ちます。

ネットワーク セグメンテーションについてなじみがない場合は、先に進む前に付録 A を参照してください。ネットワーク セグメンテーションの経緯について簡単に説明しています。また、Cisco TrustSec® ソフトウェア デファインド セグメンテーション アーキテクチャについて理解するために、『TrustSec User-to-Data-Center Access Control Using TrustSec Design Guide（TrustSec を利用したユーザからデータセンターへのアクセス制御設計ガイド）』[英語] を読むことをお勧めします。Cisco TrustSec ソリューションについて理解していることは非常に重要です。Scalable Group Tag（SGT; 拡張可能グループ タグ）と、SD-Access 内のグループベースのアクセス制御ポリシーで SGT を使用する基本になるためです。TrustSec の概要も、付録 A に記載されています。

インテント（目的）ベースのネットワーキングとセグメンテーション

元々ネットワーク セグメンテーションは、ネットワークの安定性とパフォーマンスを向上させる戦略に関係するものでした。その後、ネットワークをセグメント化またはコンパートメント化し、セグメント内およびセグメント間での制御を可能にしてポリシーを適用するという、セキュリティ戦略を反映するものに進展してきました。

現在、VLAN とプライベート VLAN で、レイヤ 3 IP サブネットに対して基本的なレイヤ 2 セグメンテーションを行っている組織もまだありますが、多くの組織では、ネットワーク セグメンテーションの主要な手段として、VRF または Cisco TrustSec を利用したソフトウェアデファインド セグメンテーションを使用するようになっています。VRF ではルーティング環境とスイッチング環境が完全に分離されるため、802.1Q トランクまたは GRE で VRF-Lite を使用する多くの組織や、基盤となるトランスポートとして MPLS を使用する組織で、VRF が一般的なネットワーク セグメンテーション テクノロジーになっています。VRF が使用される一方で、データ プレーンの分離や、ルーティング/コントロール プレーンに関する VRF 固有の考慮事項に対応する必要のない、Cisco TrustSec を使用した論理的なグループベースのセグメンテーションを行うお客様も増えています。このドキュメントの「ネットワーク セグメントの定義」セクションで説明するように、どちらのアプローチにもそれぞれの利点があり、両方のテクノロジーを導入しているお客様もいます。VRF と Cisco TrustSec ソフトウェアデファインド セグメンテーションは、ネットワークをセグメント化する非常に効果的な方法として、当面利用され続けるでしょう。この仮想/論理セグメンテーションを通じて、セキュリティ ポリシーが展開されます。

組織のビジネス要件に従ってセキュリティ ポリシーを適用するためのネットワーク セグメンテーション戦略は、通常は 1 つの場所に限定されるものではありません。たとえば、複数の建物と何千台ものデバイスで構成されたキャンパス全体に導入されたり、それぞれには少数のデバイスしかない店舗や支店などのリモート サイトに適用されたりします。ネットワーク セグメントとそのポリシーは、ビジネス関連のアプリケーションや機能が存在する場所であれば、組織内のどこにでも展開できます。これまで VRF または Cisco TrustSec を導入する場合には、ネットワーク インフラストラクチャを手動で設定することが不可欠でした。VRF を VRF-Lite または MPLS を通じて拡張するにも、Cisco TrustSec SGT を伝播するにも、多くの場合ホップバイホップで、設定を手動で完了させる必要がありました。

Cisco Software-Defined Access（SD-Access）の導入と、さらに広範な Cisco Digital Network Architecture（DNA）によって、ネットワーク セグメンテーションを導入する方法が再び進化しつつあります。『Cisco Intent-Based Networking（シスコ インテントベース ネットワーキング）』ホワイト ペーパーには次のように記載されています。

インテントベース ネットワーキング ソリューションを導入すれば、個々のネットワーク要素を手動で抽出して設定を調整しなければならなかったのが、コントローラによってポリシーベースで抽象化することができるようになります。そのため、オペレータは容易にインテント（目的とする結果）を表現し、その後、意図したとおりにネットワークが動作していることを検証できます。

読者へのヒント

シスコのインテントベース ネットワーキング アーキテクチャの詳細については、https://www.cisco.com/c/ja_jp/solutions/intent-based-networking.html を参照してください。

Cisco IBN のホワイト ペーパーについては、https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-09-intent-networking-wp-cte-en.pdf?oid=wpren006178 [英語] を参照してください。

シスコ インテントベース ネットワーキング（IBN）と SD-Access などのイネーブリング テクノロジーの主な利点の 1 つは、コンプライアンスのためのセキュリティ ポリシーを組織全体に適用できることです。したがって IBN の範囲は、データセンターやクラウド環境からキャンパスやリモート ロケーションにまで拡張され、従業員、請負業者、ベンダーを問わず、ネットワークへのリモート アクセスにも適用されます。IBN を構成する自動化と制御を実現するコントローラによって、セキュリティ ポリシーがネットワーク全体に確実に適用されてリスクが低減し、ポリシーもビジネス要件に準拠したものになります。ビジネス インテントがキャプチャされてネットワーク ポリシーに変換され、インフラストラクチャ全体に適用されます。

データセンターにおける同様の例としては、Cisco Application Policy Infrastructure Controller（APIC）を搭載した、シスコ アプリケーション セントリック インフラストラクチャ（Cisco ACI™）が、ビジネス要件をセキュア ゾーンやエンクレーブに変換できるアーキテクチャを実現しています。Cisco ACI を導入することで、階層化されたアプリケーション間の特定の通信だけを許可したり、アプリケーションやユーザなどの外部リソースへのアクセスを許可したりする一方で、その他すべての不正アクセスをブロックするコントラクトまたはポリシーを作成できます。Cisco ACI ポリシー モデルでは、VRF とグループベースのエンドポイント グループ（EPG）の両方によってセグメント化されます。EPG は、変換可能であることを含め、多くの点で SGT に似ています。コントラクトは、EPG セキュリティ ポリシーとアプリケーション ネットワーク プロファイルを使用して定義され、データセンター内外と、アプリケーション-データ リポジトリ間の通信の制御に適用されます。

読者へのヒント

APIC ポリシー モデルの詳細については、ホワイト ペーパー（https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731310.html [英語]）を参照してください。

Cisco DNA Center™ と Cisco ISE は、SD-Access アーキテクチャ内で連動し、計画、設定、セグメンテーション、アイデンティティ サービス、ポリシー サービスの自動化を実現します。Cisco ISE は DNA Center と動的に情報を交換しながら、デバイス プロファイリング、アイデンティティ サービス、ポリシー サービスを提供します。DNA Center は、自動化コンポーネントとアシュアランス コンポーネントで構成され、それらが連動してクローズドループの自動化システムを形成し、キャンパス環境で Cisco IBN のフル機能を実現するために必要な、設定、モニタリング、およびレポーティング機能を提供します。

DNA Center を導入しても、ISE はそのまま別のアプライアンスとして展開され、SD-Access キャンパス ファブリックにアイデンティティ サービスとポリシー サービスを提供します。DNA-C ユーザ インターフェイスを利用して SGT を作成する場合は、ISE ユーザ インターフェイスも起動され、そこでタスクが完了します。ISE にはすべての拡張可能グループ情報が保持され、後で DNA-C でポリシー作成に使用されます。ポリシーとそれに対応するコントラクトは DNA-C で作成されますが、どちらも Representational State Transfer アプリケーション プログラミング インターフェイス（REST API）コールを通じて ISE に戻されます。ISE は、SGT、ポリシー、コントラクト（SGACL）の単一の参照点として、それらをネットワーク インフラストラクチャに動的に配布します。

SD-Access 内のセグメンテーションは、VRF と同様の仮想ネットワーク（VN）と、Cisco TrustSec Scalable Group Tag（SGT）を組み合わせて使用することで可能になります。セグメンテーションはインテント主導型または専用の仮想ネットワークだけでも構成できますが、Cisco TrustSec SGT は、グループ メンバーシップに基づいて論理的にセグメント化します。Cisco TrustSec によって細かい粒度のレイヤが追加され、単一の VN 内で複数の SGT を使用して、マイクロセグメンテーションを実現できます。

読者へのヒント

SD-Access の詳細については、https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/software-defined-access/index.html と、https://www.cisco.com/c/ja_jp/solutions/design-zone/uc.html の『Cisco Validated Design SD-Access Design Guide（SD-Access シスコ検証済みデザイン ガイド）』を参照してください。

読者へのヒント

SD-Access が登場する以前は、SGT という略語は「セキュリティ グループ タグ」を意味していました。SD-Access が登場してからは、将来的に SGT が他の目的に使用される可能性があることから、「拡張可能グループ タグ」を表すようになっています。例としては、Software-Defined Access（SD-Access）に先立って TrustSec に導入された、Quality of Service（QoS）やポリシーベース ルーティングが挙げられます。

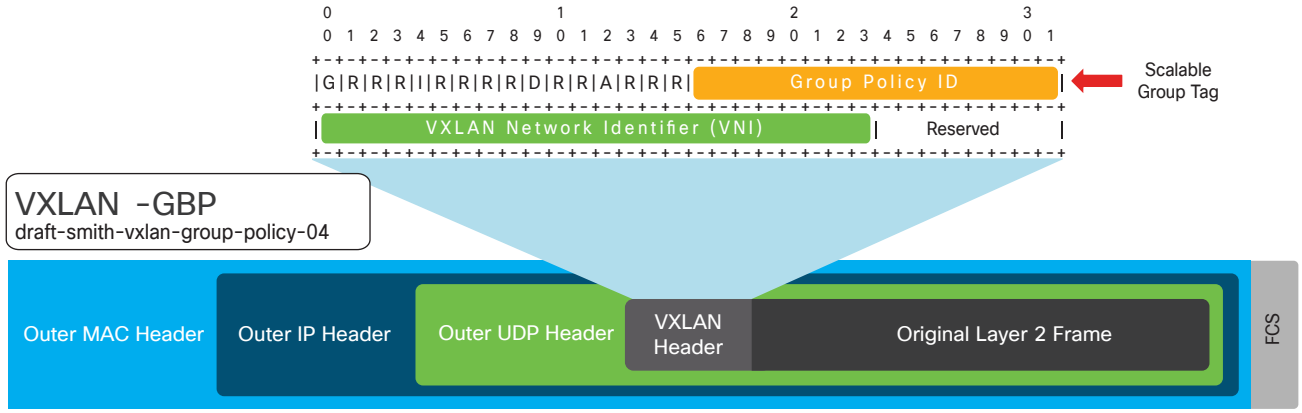
この設計ガイドでは、特に SD-Access におけるセグメンテーションとポリシー構造を取り上げています。一方で、SD-Access や SD-WAN などのその他のテクノロジーが、Cisco ACI をベースに、どのようにデータセンターや、Cisco TrustSec/VRF を導入したインフラストラクチャと連携するかを理解することが重要です。組織が完全な IBN モデルへの移行プロセスを開始する中で、これらのテクノロジーがどのように連携し、環境間でどのようにポリシーが変換されるかを理解することは重要です。Cisco ACI、VRF、Cisco TrustSec など、既存のセグメンテーション戦略は、マクロセグメンテーション レベルの仮想ネットワークと、マイクロセグメンテーション レベルの拡張可能グループを構造化し、SD-Access ファブリックに投入する方法を決定する際に影響します。

SD-Access での仮想ネットワークと SGT について理解する

仮想ネットワーク

仮想ネットワークは、先に説明した VRF と同様に、1 つの VN 内のトラフィックとデバイスを、他の VN のトラフィックとデバイスから完全に分離します。SD-Access ファブリック内では、仮想ネットワークを識別する情報は、図 1 に示すように、VXLAN ヘッダー内の VXLAN Network Identifier（VNI）フィールドで伝送されます。

図 1. VXLAN-GBP ヘッダー



VRF の従来の機能とは異なり、SD-Access ファブリック**内部**で LISP によってコントロール プレーンの転送情報が提供されるため、SD-Access ファブリックでは仮想ネットワークごとに個別のルーティング テーブルを必要としません。SD-Access ファブリック外部との境界である SD-Access ボーダーで、仮想ネットワークは VRF インスタンスに直接マッピングされ、場合によってはファブリックを超えて拡張されます。VRF 間の分離を維持するには、VRF-Lite や MPLS などのパス分離技術が使用されます。さらに、ファブリックのエンドポイント ID（EID）によって表される SD-Access IP アドレッシング情報は、BGP、EIGRP、OSPF などのルーティング プロトコルに再配布され、仮想ネットワークの拡張に使用されます。

DNA Center には、デフォルトですべてのユーザとエンドポイントが属する単一の仮想ネットワーク、DEFAULT_VN があります。DNA Center と ISE が統合されると、デフォルトの仮想ネットワークに ISE から拡張可能グループが追加されます。これらの拡張可能グループは、DEFAULT_VN で使用することも、新しい仮想ネットワークを定義して使用することもできます。

ファブリック外部の VRF は、VRF ごとに個別のルーティング テーブルを使用して相互の通信を分離するため、VRF 間の通信を実現するには、外部のネットワーク デバイスにトラフィックを転送する必要があります。また、ファイアウォール、レイヤ 3 スイッチ、またはルータを使用し、各 VRF に保持されているルーティング情報をリークすることで、仮想ネットワーク間の通信を実現するとともに、コントロール ポイントを設定して確立されたセキュリティ ポリシーを適用します。以前説明したように、これらのネットワーク デバイスは一般に「フュージョン」ファイアウォールまたはルータと呼ばれます。現在これらのフュージョン ルータまたはファイアウォールは、ファブリックの外部に配置する必要があります。

拡張可能グループ タグ

前述のように SGT は、拡張可能グループに関連付けられる 16 ビットのグループ ID で表され、グループのメンバーはビジネス ロールまたはビジネス機能に基づいて設定されます。デフォルトで、16 進数のタグ ID が 1 つ関連付けられた拡張可能グループが事前に複数定義されています。また、自分でタグ ID を選択して新しい拡張可能グループを定義することもできます。医療機関でのユーザ ロールを例にすると、ユーザを、医師、看護師、画像処理技術者、薬剤師、患者、ゲストに分類できます。同様に、IP カメラ、HVAC コントロール、キーパッド/スワイプ、デジタル サイネージなどの各種デバイスに、一意の SGT を割り当てることができます。SD-Access 内で SGT を使用する方法については、現在の非ファブリック ネットワークの Cisco TrustSec とほとんど変わっていません。SGT はそのまま、デバイスまたはユーザを論理的にセグメント化する方法として使用できます。将来的に、SGT から抽出される情報またはインテントは変わる可能性があります。

SD-Access 内での SGT の作成および使用方法の主な違いは、SGT を定義するプロセスが DNA Center で開始し、組織によって確立された仮想ネットワーク内で使用されることです。グローバル ルーティング テーブルが SD-Access ファブリックのアンダーレイ用に予約されるため、SGT と SGT による論理セグメンテーションは DEFAULT_VN で作成されて使用されるか、ユーザが作成したその他の仮想ネットワークに割り当てられます。現在、拡張可能グループは単一の仮想ネットワークでのみ使用できます。

SD-Access ネットワーク内での SGT の伝播は、TrustSec インライン タギングとは異なり、ホップバイホップ方式では実行されず、図 1 に示したように、VXLAN ヘッダーで送信されます。図に示すように、SGT と VNI はどちらも、SD-Access ファブリック内の VXLAN トンネル エンドポイント間の通信用に、VXLAN ヘッダー内に保持されます。

前述のように、SD-Access 内のセグメンテーションは、仮想ネットワークと SGT によって、それぞれマクロ レベルとマイクロレベルで実行されます。仮想ネットワークは SD-Access ファブリック内で相互に完全に分離され、1 つの VN 内のエンドポイントと他の VN 内のエンドポイント間でマクロセグメンテーションが行われます。デフォルトでは、仮想ネットワーク内のすべてのエンドポイントは相互に通信できます。各仮想ネットワークには固有のルーティング インスタンスがあるため、VN 間の通信に必要な VRF 間の転送を行うためには、外部の非ファブリック デバイスとしてフュージョン ルータまたはファイアウォールが必要になります。このフュージョン デバイスに、標準の IP ベースの ACL、拡張可能グループ タグ、または両方の組み合わせに基づいて、ポリシーを導入できます。エンドポイントが割り当てられた SGT に基づいて、仮想ネットワーク内のトラフィックに、DNA Center で定義されたポリシーを適用することもできます。これらのポリシーまたは SGACL は、許可/拒否というシンプルな形式にすることも、レイヤ 4 アクセス制御エントリに基づいて、特定の TCP/UDP ポートを明示的に許可/拒否することも可能です。このエントリは、DNA Center のコントラクトと呼ばれます。DNA Center では、ポリシー、および関連するコントラクトが設定され、REST API を通じて ISE に送信されます。ISE では、接続されているデバイスに関連付けられた SGT 用のポリシーのみに従って、エッジ ノードを更新します。ポリシーは、宛先を指定した出力時に適用されます。

図 2 に、仮想ネットワーク間の通信に使用するフュージョン ファイアウォールと、ネットワーク内の他の場所に送信されるトラフィックを示します。標準の ACL、または SGT によるグループベースのポリシーを使用して、エンドポイント間のトラフィックを制御するフュージョン ファイアウォールでファイアウォール ルールが定義されます。ファイアウォールで TrustSec を有効にする利点は 2 つあります。1 つは、外部に送信するトラフィックまたは VN 間トラフィックに対して、IP アドレスではなく SGT に基づいて、ポリシーを適用できることです。もう 1 つは、ネットワーク内でインライン タギングが有効である場合に、LAN または WAN 内の他の非ファブリック領域に対して、SD-Access ファブリックを超えてタグ付きトラフィックを伝播できることです。それによってグループベースのポリシーをネットワーク全体に拡張できます。図 2 に示すファイアウォールでは、SGT 情報を必要とせず、標準の IP ベースのアクセス リストを使用できます。

読者へのヒント

このドキュメントで説明したフュージョン ファイアウォールは、SD-Access ボーダー ノードや外部のインフラストラクチャに隣接するレイヤ 3 であると見なされます。

ルール内で SGT を使用するファイアウォールは、Scalable Group Firewall（SGFW）と呼ばれます。SGFW は、ISE から名前と拡張可能グループ タグの値だけを受け取ります。実際のポリシー/ルールを受け取ることはありません。スイッチでは SGACL が DNA Center で設定され、ISE によって導入されますが、SGT ベースのルール定義は、CLI またはその他の管理ツールを使用して、ローカルの SGFW で実行できます。

読者へのヒント

SGFW の設定の詳細については、『Access Control Using Security Group Firewall（セキュリティ グループ ファイアウォールを使用したアクセス制御）』[英語] を参照してください。

図 2. フュージョン ファイアウォールによるポリシー適用

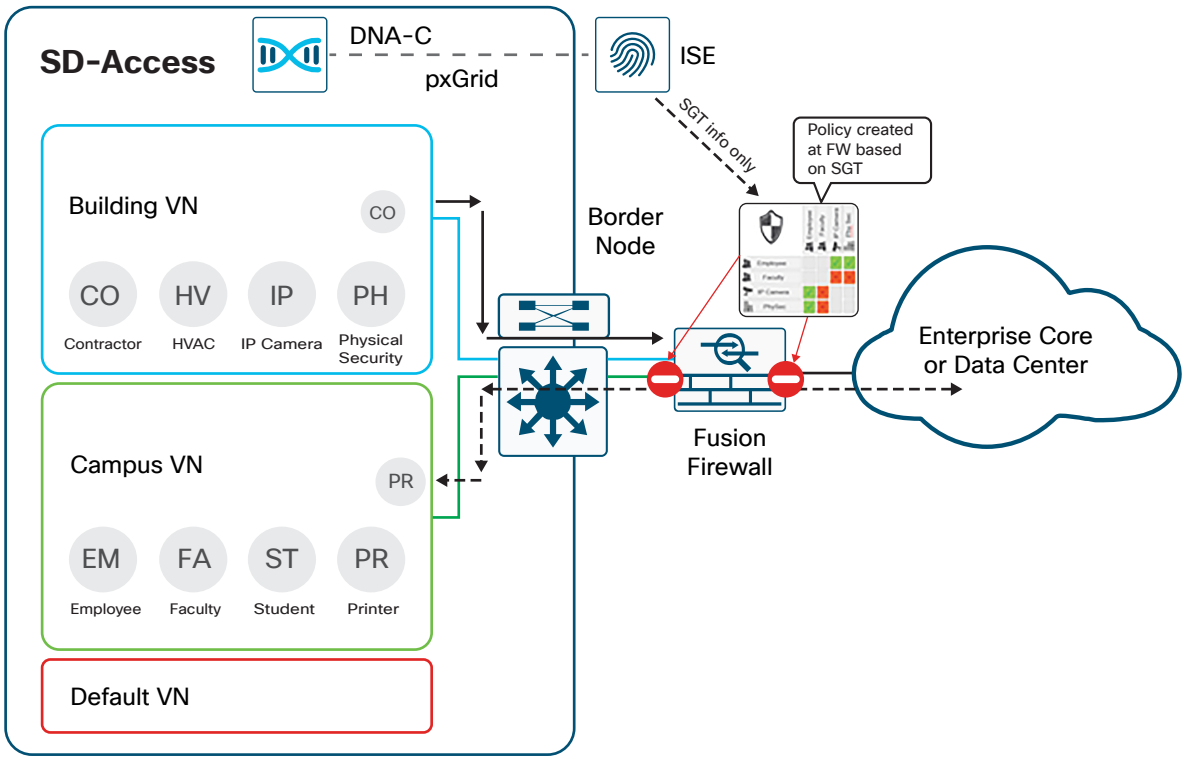


図 2 では、Building VN から送信されたトラフィックが Campus VN またはファブリック外部に送信され、拡張可能グループに基づいてファイアウォールで適用されたポリシーに従って、転送またはドロップされます。

拡張可能グループと IP アドレスまたはネットワーク オブジェクトに基づいてファイアウォールを使用する場合は、各 VN について専用のインターフェイスまたはサブインターフェイスを確保する以外に、特に考慮事項はありません。ただし、ファイアウォール ルール内で IP アドレスを使用する場合には、エンドポイントのアドレッシングが変更された場合に、新しいアドレスが反映されるようにファイアウォール ルールを更新する必要があります。

各 VN 専用のインターフェイスに加えて、SGFW を導入して、SGT に基づいてポリシーを適用する場合には、トラフィックの送信元である各エンドポイントに関連する拡張可能グループ情報が SGFW に伝播され、ルールの作成に使用できるようにする必要があります。さらに、次のセクションで説明するように、SGT だけを使用して SGFW でポリシーを適用する場合には、宛先 IP-SGT のマッピングも必要になります。

技術的なヒント

SGFW は、ASA OS を実行する ASA、もしくは、ASA OS または Firepower Threat Defense（FTD）ソフトウェアを実行する Cisco Firepower™ 次世代ファイアウォール（NGFW）アプライアンスを使用します。ASA OS の場合は、ファイアウォール ルールで送信元/宛先の SGT または IP アドレスを任意に組み合わせて使用できます。NGFW FTD ソフトウェアを使用している場合は、送信元の SGT だけが指定され、宛先は IP アドレスに基づくオブジェクトになります。もう 1 つの違いは、ファイアウォールで ASA OS が実行中の場合に、SGT Exchange Protocol over TCP（SXP）が使用されることです。

ポリシー適用のための拡張可能グループ タグの伝播

SGFW をフュージョン ファイアウォールに導入するには、すべてのポリシー適用が SGFW で行われる場合、ファイアウォールに入るトラフィックに関する拡張可能グループ情報が必須となり、オプションで宛先が必要になります。SD-Access 以外で Cisco TrustSec を導入する場合には、送信元 SGT を取得し、さらに宛先の IP-SGT マッピング情報を得ることができる最初のネットワーク デバイスで、適用されます。SGFW の適用に関する検討事項の前に、SGT の伝播について説明します。

SGT 情報を伝播するには、Cisco ISE を使用して、SXP または pxGrid を通じて IP-SGT マッピング情報を SGFW にアドバタイズします。その場合は、拡張可能グループ名に加えて、関連付けられた 16 ビット SGT ID をファイアウォールと交換するように、Cisco ISE を設定する必要があります。SXP または pxGrid を使用する場合、タグなしトラフィックが SGFW に到着すると、拡張可能グループ マッピング データベースがチェックされ、ISE から取得された SGT ID にソース トラフィックが関連付けられます。

注意

SD-Access では、ISE とフュージョン ファイアウォール間で SXP または pxGrid を使用した場合のみ、ファブリック エンドポイントの拡張可能グループ タグ情報をフュージョン ファイアウォールに伝播できます。インライン タギングは、SD-Access ボーダー ノードと、この時点でボーダー ノードに隣接するレイヤ 3 であるフュージョン ファイアウォールまたはその他のデバイス間ではサポートされません。

読者へのヒント

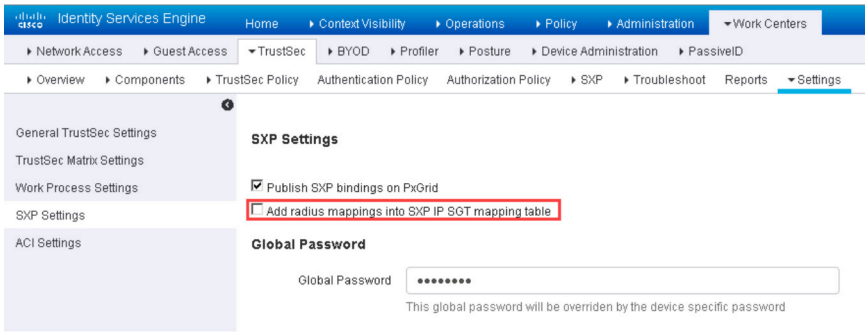
SGFW の設定の詳細については、『Access Control Using Security Group Firewall（セキュリティ グループ ファイアウォールを使用したアクセス制御）』[英語] を参照してください。

さらに、ファイアウォールで ASA OS オペレーティング システムが実行されている場合、ISE では SXP を使用して IP-SGT マッピング情報をアドバタイズします。また、Cisco Firepower NGF で FTD OS が実行されている場合、Cisco ISE は pxGrid を使用して IP-SGT マッピング情報をアドバタイズします。

SXP と pxGrid のどちらを使用して IP-SGT マッピング情報をアドバタイズするかは、SGFW のオペレーティング システムによって決まります。ASA または Cisco Firepower アプライアンスのいずれかで ASA OS が実行されている場合は、ファブリックに接続されているエンドポイントの IP-SGT マッピング情報のアドバタイズに SXP が使用されます。Firepower NGFW で FTD ソフトウェアが使用されている場合は、Firepower NGFW へのマッピング情報のパブリッシュに pxGrid が使用されます。それにより、RADIUS 認可中に学習された、ファブリック エッジ ノードに接続されたデバイスのマッピング情報をアドバタイズするように、ISE を設定できます（次のヒントを参照）。図 3 に示すように、この設定により、ファブリックに接続されているデバイスについて、IP アドレスおよび関連付けられた SGT が SGFW に登録されます。

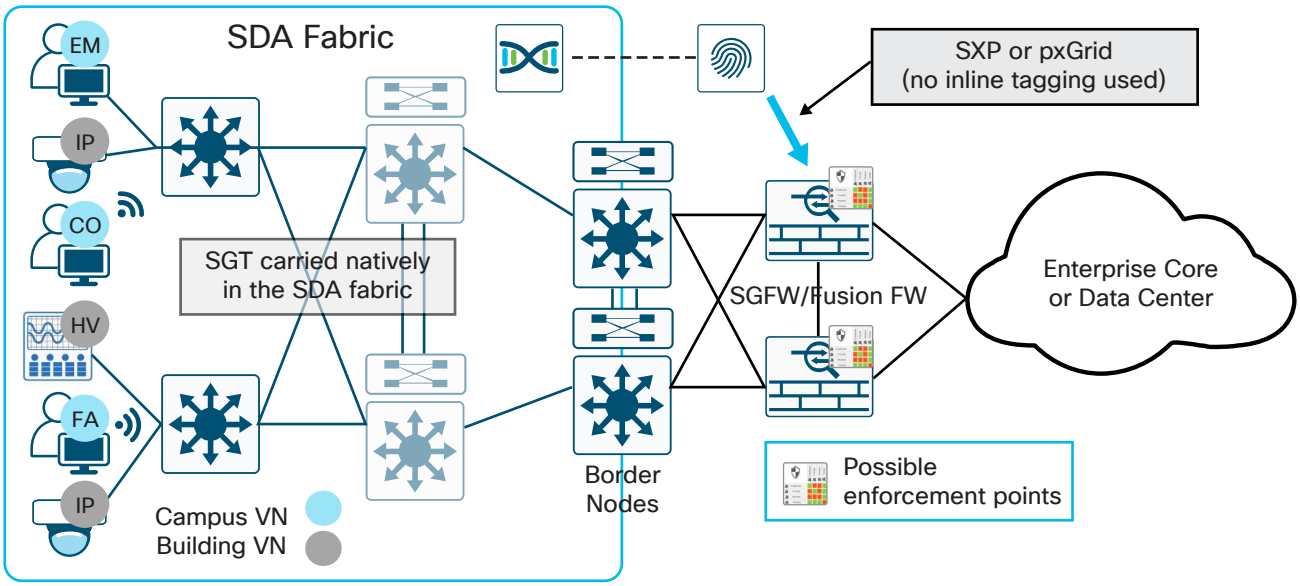
読者へのヒント

ISE の [TrustSec] > [設定（Settings）] ページでは、SXP でアドバタイズ、または pxGrid でパブリッシュする IP-SGT マッピング情報に RADIUS セッション マッピング情報を追加できます。次のスクリーンショットを参照してください。



このマッピングは、dot1x/MAB 認証対応のすべてのシスコ スイッチと、ISE を RADIUS サーバとして使用するサードパーティ製スイッチで実行できます。シスコ スイッチの場合、このマッピング情報は、ファブリック エッジ ノードに導入されても、ネットワークのファブリック外の部分に導入されても利用可能です。

図 3. フュージョン ファイアウォール対応の SXP



さらに、ISE で手動で作成されたか、または Application Policy Infrastructure Controller（APIC）が制御する ACI ファブリックが存在する場合に ACI 統合を通じて動的に学習された IP-SGT マッピング情報を、サーバまたは他の非ファブリック エンドポイントに対してアドバタイズできます。それによって、ファブリック外部を宛先とする通信にポリシーが適用されます。ISE で IP-SGT マッピング情報を手動で作成することは、もちろん SD-Access ファブリック外部のエンドポイントに限定されるものではなく、ファブリック内で dot1x または MAB 認証を使用せず、手動でマッピングを作成する必要があるエンドポイントにも該当します。

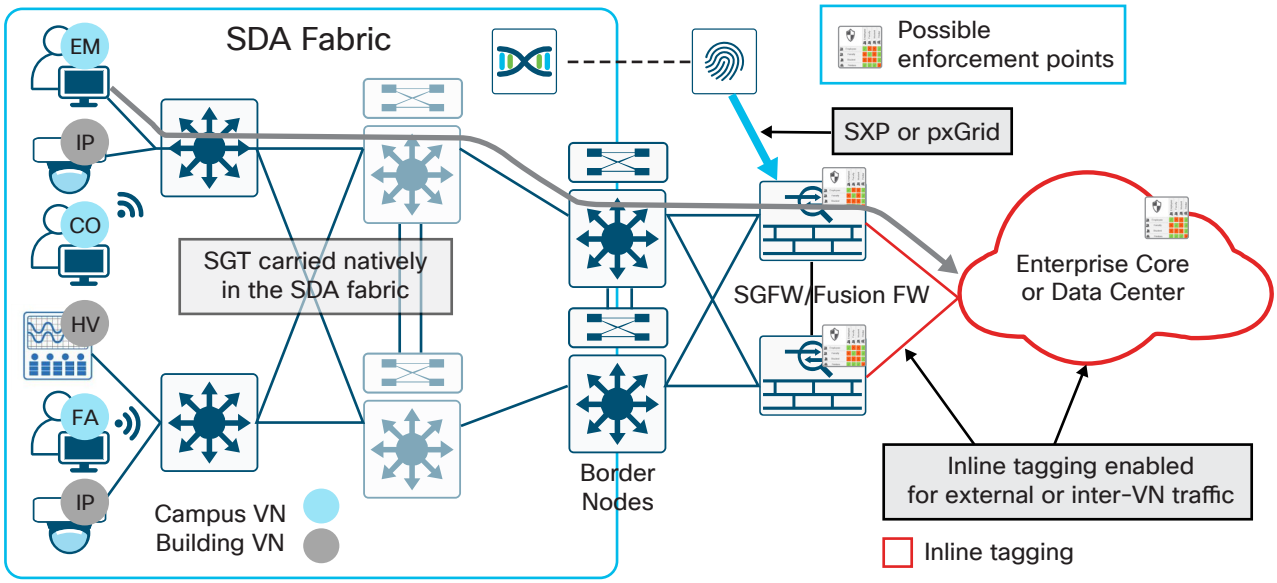
SGFW でポリシーを適用さず、SGFW を超えてネットワークの他の領域に SGT を伝播できるようにするには、ファイアウォールの出力インターフェイスでインライン タギングを有効にする方法が最も効率的です。SGFW が、SGT を組み込んだフレームを単純に転送するためです。この転送は、実行中のファイアウォール OS で行われます。トラフィックが SGFW に到達する

と、IP-SGT ルックアップとポリシーのチェックが行われます。トラフィックが許可され、SGFW の出力インターフェイスでインライン タギングが有効になっていると、関連付けられた SGT がイーサネット ヘッダーの CMD フィールドに付与されてトラフィックが転送されます。図 4 に示すように、このシナリオは、Cisco TrustSec® インライン タギングが、SGFW/フュージョン ファイアウォールを超えたインフラストラクチャで有効になっていることを前提としています。

読者へのヒント

Cisco TrustSec インライン タギングの詳細については、『User-to-Data-Center Access Control Using TrustSec Deployment Guide（TrustSec を利用したユーザからデータセンターへのアクセス制御導入ガイド）』[英語] と『User-to-Data-Center Control Using TrustSec Design Guide（TrustSec を利用したユーザからデータセンターへのアクセス制御設計ガイド）』[英語] を参照してください。

図 4. フュージョン ファイアウォールからの出力に対するインライン タギング



ネットワークの他の領域に SXP でアドバタイズすることも可能です。詳細については、この後の適用に関するセクションで説明されています。

ファブリック外部に送信されるトラフィックへのポリシー適用

SD-Access ファブリックの外部に送信されるトラフィックに対して、SGT に基づいてポリシーを適用する方法には、次の 3 つのオプションがあります。

1. SGFW として機能しているフュージョン ファイアウォールで適用する。
2. 宛先、またはパス内の別の場所で適用する。
3. ボーダー ノードで適用する。

SGT ベースの適用に SD-Access ボーダー ノードを使用する方法は、ファブリックの外部に送信するファブリック トラフィックについてのみ有効です。アウトバウンド トラフィックのタイプと規模に応じて、SD-Access ボーダー ノードで多数のソフトウェアおよびハードウェア リソースが必要になる場合があります。これらの理由から、各種のプラットフォームと、サポートされる IP-SGT マッピング数と SGACL 数に関するスケーラビリティの違いについては、このドキュメントの対象外です。

前述のように、SGT に基づくポリシー適用は、送信元と宛先両方の SGT を取得する、適用デバイスの機能に応じて異なります。ファブリック エンドポイントの SGT 情報は、ボーダー ノードに到達するトラフィックの VXLAN ヘッダーで伝播されます。ただし、宛先 SGT はボーダー ノードでは認識されないため、Cisco ISE が SXP でアドバタイズする必要があります。シスコ ファイ

アウォールはボーダー ノードとしてはサポートされていないため、この説明は、サポートされているシスコ ルータおよびスイッチについてのみ該当します。ルータやスイッチなどのネットワーク デバイスで SXP による IP-SGT マッピング情報の取得を有効にする場合は、考慮すべき点がいくつかあります。

- TrustSec ポリシー適用のために ISE でネットワーク デバイスを定義すると、ネットワーク デバイスは SGT のマッピング情報を学習した時点で ISE と通信し、宛先 SGT に関連付けられたポリシーを取得します。ルータまたはスイッチの場合、ダウンロードされた SGACL は、それぞれメモリまたは TCAM を消費します。SGT とそれに関連付けられたポリシーが多いと、ルータではメモリの使用量が過大になり、スイッチでは TCAM が枯渇する場合があります。その結果、一部の SGACL がインストールされない可能性があります。
- ネットワーク デバイスでは、保存できる IP-SGT マッピングの数が明確に制限されています。マッピング数が増加すれば、消費されるメモリも増大します。サポートされている数を超えると、マッピング情報がメモリにインストールされず、それらのマッピングに固有のポリシーが適用されなくなります。

これらの理由から、ボーダー ノードとしてサポートされる各種のプラットフォームと、サポートされる IP-SGT マッピング数と SGACL 数に関するスケーラビリティの違いについては、このドキュメントの対象外です。

読者へのヒント

SD-Access ボーダー ノードでのポリシー適用の詳細については、「Enforcing Policy on an SD-Access Border Node（SD-Access ボーダー ノードでのポリシー適用）」[英語] を参照してください。

IP-SGT マッピング数と SGACL 数に関する、プラットフォームのスケーラビリティの詳細については、TrustSec システム速報 [英語] を参照してください。

オプション 1：SGFW として機能しているフュージョン ファイアウォールで適用する

最初のオプションでは、フュージョン SGFW の SD-Access ファブリックから送信されるすべてのトラフィックに、グループベースのポリシーを適用できます。SGFW を超えるファブリック エンドポイントの SGT を伝播する必要はありません。先に説明したように、最初のオプションでは、認証されたファブリック エンドポイントの IP-SGT マッピング情報を、ISE が SGFW にアドバタイズします。次に、SGFW でポリシーが、宛先 SGT か IP アドレスのどちらを使用するかを決定する必要があります。

フュージョン ファイアウォールと FTD のどちらで ASA OS を使用するかに応じて、ルール内で宛先を特定する方法が異なります。ASA OS では、送信元か宛先にかかわらず、SGT または IP アドレスをどのような組み合わせでも使用できます。FTD が宛先 SGT をサポートする場合には、更新する必要があります。

作成するポリシーが、SGFW で送信元 SGT と宛先 IP アドレスによって構成されている場合には、ルールの作成と適用を進めることができます。その場合、オペレーティング システムがなんであるかは関係なく、また、送信元 SGT 情報が ISE と SGFW との間で、SXP によって伝播されるか、pxGrid によって伝播されるかも問いません。

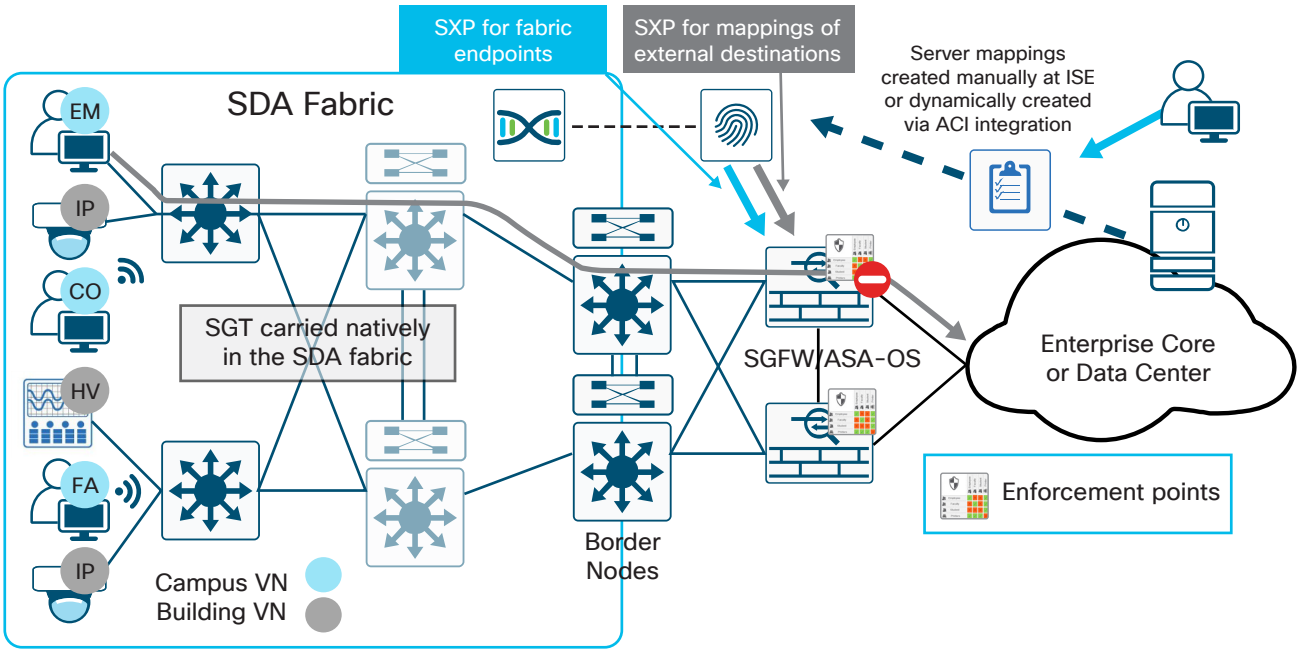
SGFW で ASA OS を実行していて、ルールにおいて送信元と宛先の両方で SGT 情報を使用することを決めた場合は、外部であっても別の仮想ネットワーク内であっても、これらの宛先に関する IP-SGT マッピング情報を、SXP で SGFW にアドバタイズする必要があります。SGT に基づくポリシー適用は、宛先に関する IP-SGT マッピング情報が設定された最初のネットワーク デバイスで行われるという、基本的なルールを覚えておいてください。

読者へのヒント

シスコ ファイアウォールでの IP-SGT マッピング数に関する問題と、SGT ベースのポリシー適用に関する問題は、実行されているオペレーティング システムに関係なく、事実上心配する必要はありません。最新モデルの Cisco ASA ファイアウォールと FTD ベースのすべての Firepower アプライアンスは、通常 75 ～ 200 万件の IP-SGT マッピングに対応できます。SGT に基づくルールでは、IP アドレスやネットワーク オブジェクトに基づく同等のルールに比べて、実際にメモリの消費量が大幅に少なくなります。IP-SGT マッピング数に関する、プラットフォームのスケーラビリティの詳細については、TrustSec システム速報 [英語] を参照してください。

ASA OS を実行する SGFW に宛先 IP-SGT マッピング情報を設定するには、SGFW でスタティック マッピングを作成する方法と、SXP を使用する方法の 2 つがあります。推奨されるアプローチは、ISE での集中管理型設定です。ISE でマッピングを手動で作成し、SGFW にアドバタイズできます。SGFW にアドバタイズするマッピング情報を ISE で作成する場合、ホスト アドレスまたはサブネットにすることが可能です。さらに、先に述べたように、ACI データセンターがある場合には、ISE と APIC を統合して、ACI ファブリック内のサーバに対して IP-SGT マッピングを動的に作成できます。これらのマッピング情報は、SGFW にも自動的にアドバタイズできます。この導入を図 5 に示します。

図 5. 外部トラフィックに対する SGFW での適用



オプション 2：宛先または宛先までのパスでの適用

宛先、または宛先までのパス上のデバイスで適用する場合は、適用デバイスに、その宛先のエンドポイントの IP-SGT マッピング情報が存在する必要があります。宛先に接続されているネットワーク デバイスで適用する場合は、エンドポイントが「分類済み」であるか、SGT に関連付けられている必要があります。IP-SGT マッピング情報の分類または作成は、プラットフォームの機能に応じて、802.1x または MAB を利用してローカルのネットワーク デバイスで動的に実行するか、IP-SGT、サブネット -SGT、VLAN-SGT、またはポート -SGT マッピング情報を利用してデバイス CLI で静的に実行できます。または、ISE で宛先マッピング情報を作成し、SXP で宛先スイッチにアドバタイズすることもできます。宛先までのパス上のネットワーク デバイスで適用する必要がある場合は、中間デバイスで SXP または静的分類が必要になります。

読者へのヒント

Cisco TrustSec 分類の詳細については、『User-to-Data-Center Access Control Using TrustSec Deployment Guide（TrustSec を利用したユーザからデータセンターへのアクセス制御導入ガイド）』[英語] または『User-to-Data-Center Control Using TrustSec Design Guide（TrustSec を利用したユーザからデータセンターへのアクセス制御設計ガイド）』[英語] を参照してください。

2 番目のオプションでは、宛先 IP-SGT マッピング情報に加えて、SD-Access ファブリック エンドポイントの SGT が適用ポイントに伝播されることを前提としています。フュージョン ファイアウォールからの出力で Cisco TrustSec インライン タギングを有効にするか、SXP を使用して送信元のファブリック エンドポイントの SGT を宛先または適用ポイントに伝播させる必要があります。

インライン タギングは、宛先へのトラフィックのイーサネット ヘッダーに SGT が組み込まれるため、常に最もスケーラブルなアプローチになります。SGT のすべての処理がハードウェアで行われる一方、SXP ではマッピング情報の保存と更新にメモリとプロセッサが消費されます。インライン タギングをサポートするために、フュージョン ファイアウォールと、宛先に対する適用ポイントとの間のリンクは、すべて TrustSec 用に手動で有効にする必要があります。その場合は、各デバイスで、ホップバイホップで有効にします。

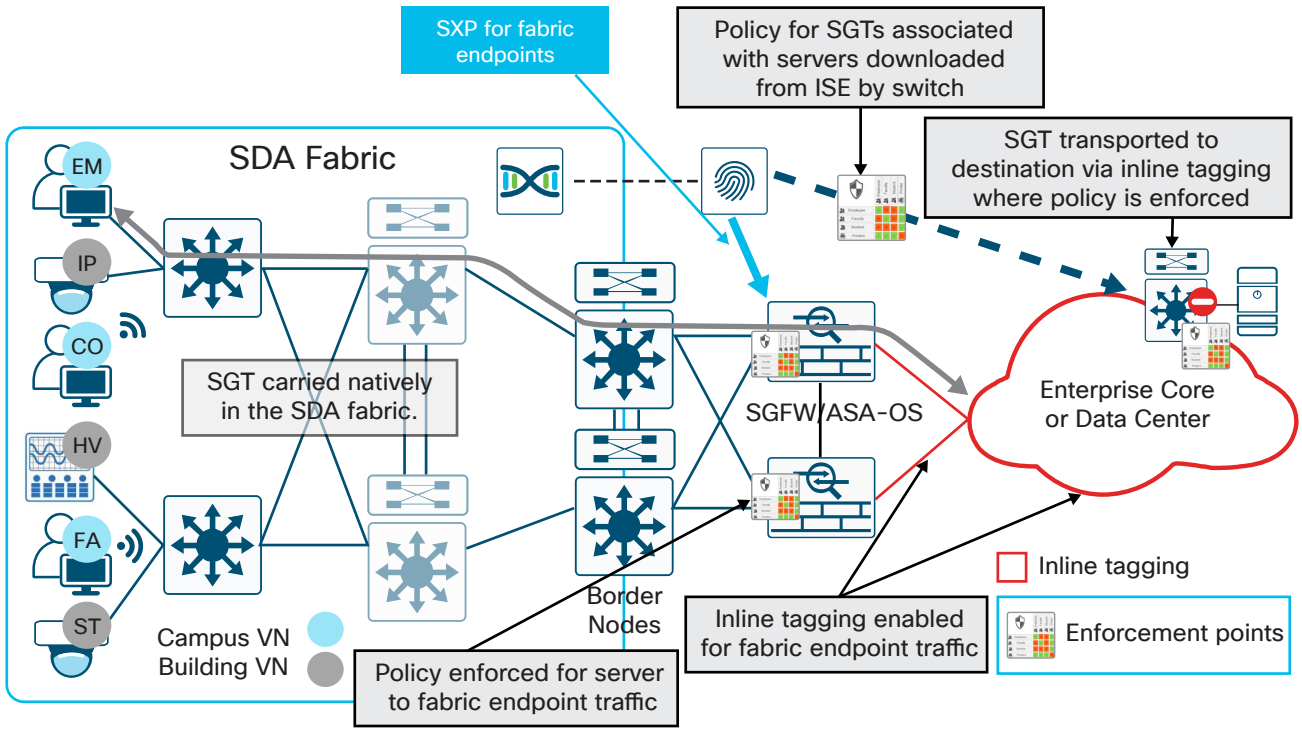
インライン タギングを有効にした場合に 1 つポイントとなる点は、ファブリックから送信されるトラフィックに対する TrustSec のグループベースのポリシーを外部の宛先で適用できるだけでなく、サーバからファブリック エンドポイントに向けたインバウンド トラフィックを制限するポリシーをフュージョン ファイアウォールで適用することもできるということです。これは、先に説明したように、サーバまたはその他の外部の宛先が SGT によってローカルで分類され、リモートでタグが付与されたトラフィックが、インライン タギングが有効化されている非ファブリック インフラストラクチャ経由でファブリックに戻る場合にのみ可能です。この構成を図 6 に示します。

読者へのヒント

TrustSec インライン タギング設定の詳細については、『User-to-Data-Center Access Control Using TrustSec Deployment Guide（TrustSec を利用したユーザからデータセンターへのアクセス制御導入ガイド）』[英語] と『User-to-Data-Center Control Using TrustSec Design Guide（TrustSec を利用したユーザからデータセンターへのアクセス制御設計ガイド）』[英語] を参照してください。

プラットフォームでのインライン タギングのサポートの詳細については、「TrustSec Platform Support Matrix（TrustSec プラットフォーム サポート マトリックス）」[英語] を参照してください。

図 6. 非 SD-Access インフラストラクチャで有効化された TrustSec インライン タギング



フュージョン ファイアウォールからのインライン タギングではなく、ISE と SXP を使用する場合は、すでに説明したように、ネットワークに対するファブリック エンドポイントの AAA 認可の際に作成された IP-SGT マッピング情報をアドバタイズするように、ISE を設定する必要があります。続いて、ポリシーを適用するネットワーク デバイスを選択し、そのデバイスと ISE との間に SXP を設定します。ルータやスイッチなどのネットワーク デバイスで IP-SGT マッピング情報を学習するように SXP を有効化することについて、先に 2 つのポイントを指摘しました。これは重要なので、さらに詳細に説明します。

- TrustSec ポリシー適用のために ISE でネットワーク デバイスを定義すると、ネットワーク デバイスは SGT のマッピング情報を学習した時点で ISE と通信し、宛先 SGT に関連付けられたポリシーを取得します。ルータまたはスイッチの場合、ダウンロードされた SGACL は、それぞれメモリまたは TCAM を消費します。SGT とそれに関連付けられたポリシーが多いと、ルータではメモリの使用量が過大になり、スイッチでは TCAM が枯渇する場合があります。その結果、一部の SGACL がインストールされない可能性があります。
- ネットワーク デバイスでは、保存できる IP-SGT マッピングの数が明確に制限されています。マッピング数が増加すれば、消費されるメモリも増大します。サポートされている数を超えると、マッピング情報がメモリにインストールされず、それらのマッピングに固有のポリシーが適用されなくなります。

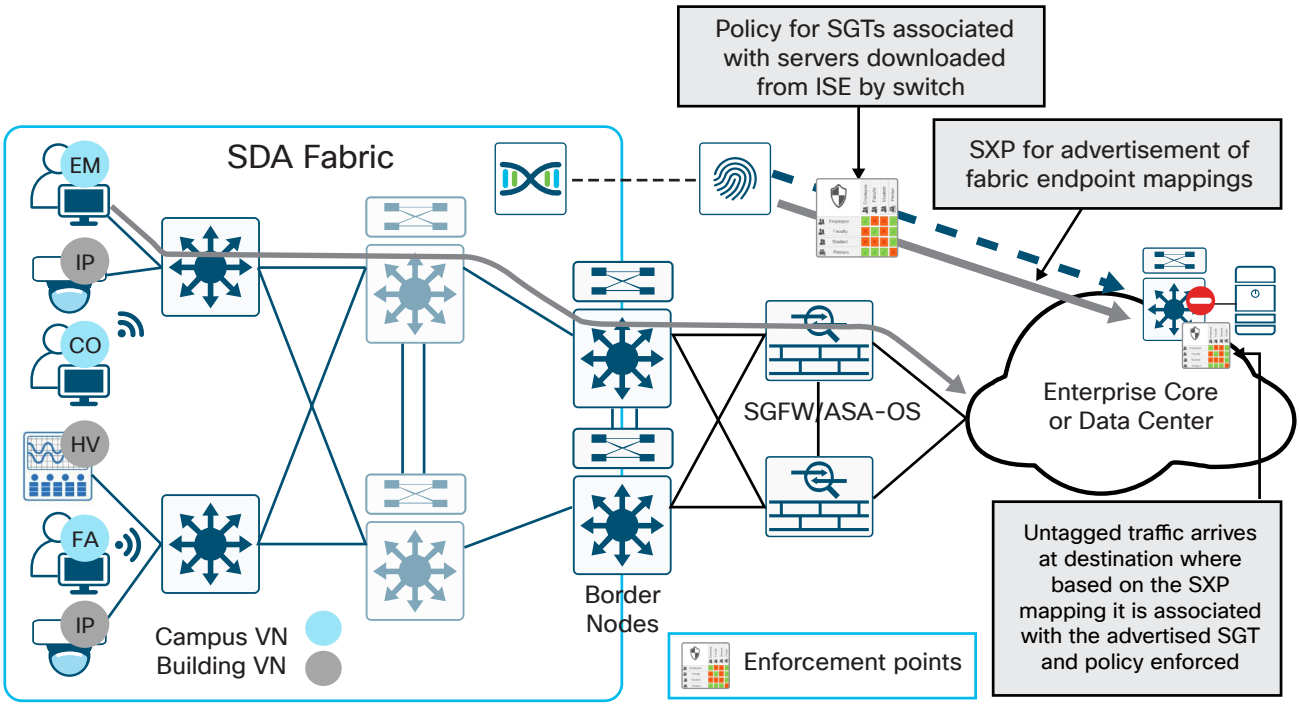
ポリシー適用に SXP マッピングを必要とするデバイスを選択する場合は、こうした点を考慮する必要があります。また前述のように、適用ポイントとして選択したシスコ ファイアウォールは、非常にスケーラブルです。図 7 に、SD-Access ファブリック外部のネットワーク デバイスでの SXP 適用を示します。

読者へのヒント

サポートされているマッピング数、SGACL 数、SXP など、TrustSec プラットフォームのスケーラビリティに関する最新情報については、「TrustSec システム速報」[英語] を参照してください。

SXP の詳細については、シスコ TrustSec コミュニティの「Using SXP and SXP Reflectors（SXP および SXP リフレクタの使用方法）」[英語] を参照してください。

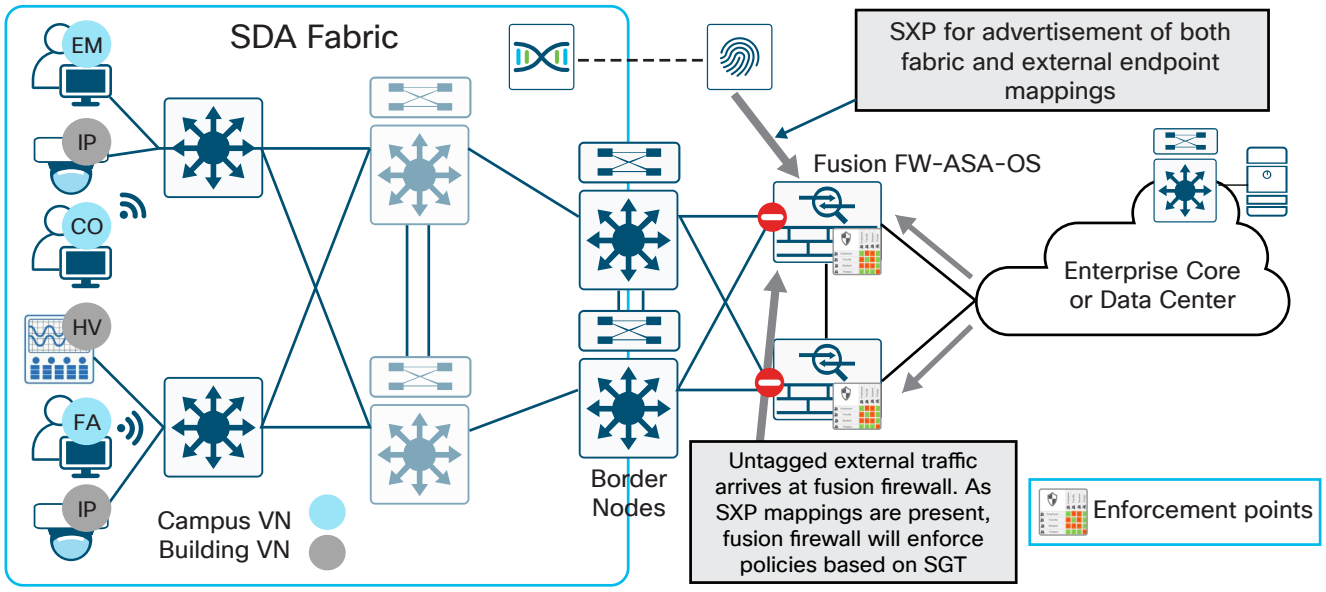
図 7. ファブリック外部の適用ポイントに対する SXP



インライン タギングではなく SXP を使用する場合の違いの 1 つは、前述の設定以外の追加設定を行わない場合、サーバまたはその他の外部エンドポイントからファブリック エンドポイントへのトラフィックに対して、SGT に基づいてポリシーを適用できないことです。この追加設定が必要なのは、外部トラフィックが SGT なしでフュージョン ファイアウォールに到達するため、SGT ベースのポリシーを適用できないからです。

追加設定を行うには、外部デバイスに関する IP-SGT マッピング情報をフュージョン ファイアウォールに伝播させ、送信元 SGT として使用できるようにする必要があります。それにより、図 8 に示すように、送信元がファブリックの外部にあり、宛先がファブリック エンドポイントである場合に、ポリシーを適用できます。

図 8. ファブリックを宛先とする外部トラフィックにポリシーを適用



仮想ネットワーク内および仮想ネットワーク間のトラフィックに対するポリシー適用

各 VN 内では、1 つ以上の拡張可能グループを定義して、その VN 内で SGT ベースのマイクロセグメンテーションを行うことができます。各 VN 内の SGT 間の通信を定義するポリシーは DNA-C で定義され、REST API を通じて ISE に送信されます。その後 ISE によって、SD-Access ファブリックのエッジ ノードに配布されます。エンドポイントをエッジ ノードに接続すると、エッジ ノードは SGT に該当するポリシーを要求し（まだ取得していない場合）、TCAM にインストールします。VN 内に適用する場合に必要なことは、VN に対してポリシーおよび関連するコントラクトを作成し、SGT 間のどの通信を許可またはドロップするかを定義することだけです。

SGT を使用してポリシーを適用し、VN 間のトラフィックを許可または拒否することもできます。VN を作成すると、その VN に拡張可能グループを割り当てることもできます。DNA-C でポリシーを構築する場合は、送信元および宛先 SGT を指定します。作成中のポリシーで別の VN の SGT を使用する場合は、以下に示すように、SGT が VN に依存しないように定義する必要があります。

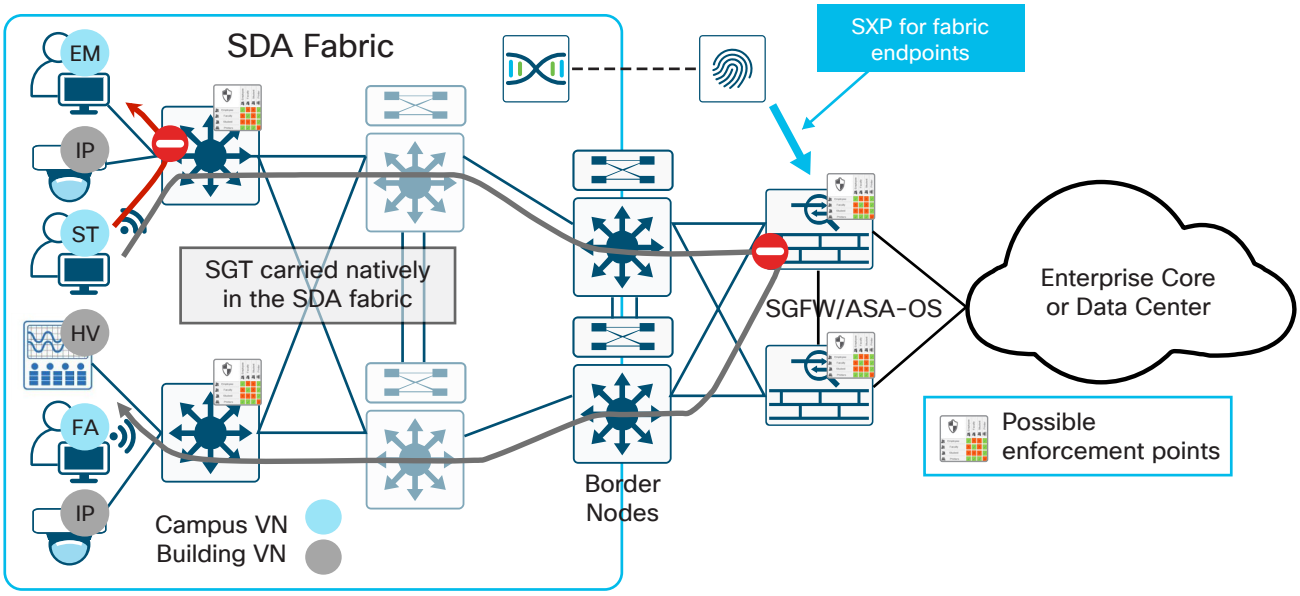
ファブリック エンドポイントと外部の宛先の間でポリシーを適用する場合、VN 間のトラフィックにポリシーを適用する際に、次の 2 つのオプションがあります。

1. SGFW として機能しているフュージョン ファイアウォールで適用する。
2. 宛先エッジ ノードで適用する

現在、拡張可能グループを割り当てることができる VN は 1 つだけであるため、1 つの VN の送信元または宛先 SGT が別の VN にも存在する DNA-C では、VN ポリシーを作成することができません。

フュージョン ファイアウォールを使用して VN 間に適用する場合は、前述のように、ファブリック エンドポイントの認可中に取得した IP-SGT マッピング情報をアドバタイズするように ISE を設定します。これらのマッピング情報は、ルール作成時に、SGFW でポリシーを適用するために使用されます。ここでも、ASA または Firepower SGFW で ASA OS を使用している場合は、SGT と IP アドレスを送信元または宛先として任意に組み合わせてルールを作成できます。ただし Firepower FTD を使用している場合は、ルールで宛先 IP アドレスを使用する必要があります。図 9 に、説明したシナリオを示します。

図 9. 仮想ネットワーク内および仮想ネットワーク間のトラフィックに対するポリシー適用



ネットワーク セグメントの定義

ネットワーク セグメントを作成するかどうかを判断する際は、仮想ネットワークでも論理ネットワークでも、組織のビジネス要件に従う必要があります。しかしこれは、実際には何を意味しているのでしょうか。ネットワークのセグメント化には、第一にどのような目的があるのでしょうか。

ネットワークをセグメント化することで、仮想的（仮想ネットワーク）または論理的（SGT）に、セキュリティ上の理由から特定のビジネス アプリケーションまたは機能専用のセグメントを定義できます。これらのセグメントでは、セグメントに対するアクセスを制御するために明確に定義したポリシーを適用し、セグメント間の通信を制限することができます。セグメント化する際、仮想ネットワークの場合はネットワーク セグメントの内外でセキュリティ ポリシーを定義し、SGT の場合は論理セグメント間および論理セグメント内でセキュリティ ポリシーを定義し、ネットワークの攻撃対象領域をそのセグメントに限定するようにします。

前述のように、SD-Access では、仮想ネットワークを使用したネットワーク セグメンテーションと、各仮想ネットワーク内で SGT を使用した「論理的な」セグメンテーションの両方が可能です。現実的には、各仮想ネットワークで拡張可能グループを 1 つずつ設定してすべての仮想ネットワークを使用するか、1 つの「ユーザ」仮想ネットワークで複数の拡張可能グループを設定するかを選択することになります。

どちらのアプローチを選択するかは、アプリケーションまたはビジネス機能を完全に分離する必要があるかどうかに大きく左右されます。Payment Card Industry（PCI; クレジット カード業界）やゲスト ネットワークなどの場合は、仮想ネットワークで完全に分離することが最適だと思われます。仮想ネットワークを使用する場合、たとえば法規制遵守の対象は、仮想ネットワークへのアクセスと仮想ネットワーク内の通信に限定されます。または、タグ間の通信を制御するポリシーを適用した拡張可能グループによって、POS マシンやカード リーダー用に必要なセグメンテーションを「論理的に」実現できます。ただし PCI の場合は、その仮想ネットワークに属する PCI タグとその他の SGT 間を分離できなければなりません。1 つの正解はなく、ほとんどの場合は複数の方法を組み合わせることになります。

仮想ネットワークが使用される場所としては、次のような例が挙げられます。

- PCI：POS マシン、カード リーダー、クレジット カード ゲートウェイ
- 電力：発電、送電、社内ネットワークの分離
- 建物の制御：暖房、冷房、照明、およびセキュリティ システム
- 製造現場：社内ネットワークと現場の分離
- トレーディング フロア
- ネットワーク インフラストラクチャの管理
- 研究開発：社内ネットワークから研究環境を分離する
- 大学の寮：キャンパス ネットワークおよびアプリケーションから分離
- 医療機関の臨床環境：ベッドサイド モニタ、輸液ポンプ、MRI、超音波、X 線
- ゲスト ネットワーク

次に SGT が使用される例を示します。

- PCI：インベントリ スキャナ、カード リーダー、POS
- 医療機関の臨床環境：ベッドサイド モニタ、輸液ポンプ、MRI、超音波、X 線、医師、看護師、建物制御
- 大学：学生、教授、ゲスト、建物制御、セキュリティ システム
- 人事や財務などのビジネス機能
- セキュリティ システムおよびその他のビジネス コントロール

- ゲスト アクセス
- 請負業者のアクセス
- ビジネス パートナー
- 検疫および修復
- ネットワーク管理

上の例からわかるように、ネットワークのセグメント化のために、仮想ネットワーク、SGT、またはその組み合わせが大幅に重複して使用される可能性があります。したがって、セグメンテーションについて検討する場合は、どの方法であれば、設計を必要以上に複雑にすることなく、ビジネス上のセキュリティ要件に対応できるかを、明確にする必要があります。

仮想ネットワークまたは拡張可能グループ タグ

これまでのセクションでは、SD-Access を使用する場合としない場合の両方に関して、さまざまなセグメンテーション テクノロジーを見てきました。セグメンテーションが必要になるのは、どのようなビジネス要件でしょうか。

仮想ネットワーク

仮想ネットワークや VRF のように、組織でセグメント間を完全に分離することが必要な要件は、多くの場合簡単に特定できます。通常この要件は、さまざまなタイプのビジネス上の通信でセキュリティ制御を維持して、法規制を遵守するために必要となります。特定のビジネス機能またはアプリケーションで仮想ネットワークが必要かどうかを判断する際には、次の基準が重要になります。

- アプリケーションまたはビジネス機能、およびそれにアクセスするデバイスは、ネットワーク エッジからコアに拡張されるか。
- ユーザとデバイスの通信は主に仮想ネットワークに制限され、仮想ネットワーク内またはネットワーク外でアクセスを限定することが必要か。
- 仮想ネットワーク内でデバイス間の通信は許可されるか。
- 法規制の遵守に関するネットワーク監査の範囲は、仮想ネットワークまたは VRF で分離することで縮小されるか。

一般的に、上のすべてに該当する場合は、これらのアプリケーションや機能に対する仮想ネットワークまたは VRF の定義に影響する可能性があります。SD-Access を導入すると、オーバーレイの VXLAN データ プレーンと LISP コントロール プレーンによって、ファブリック内のルーティングがシンプルになります。ルーティングに関しては、ファブリック エッジで考慮することになります。ファブリック ボーダーでは、SD-Access 仮想ネットワークと外部ネットワーク間で必要なルート リークのために、依然としてフュージョン ルータまたはファイアウォールを使用する必要があります。

仮想ネットワークによる分離が有効な例としては、PCI DSS（クレジットカード データ保護基準）への対応があります。その場合は、カード所有者データと伝送に対するすべてのアクセスを制限するセキュリティ制御を導入する必要があります。クレジットカード トランザクションを収集、保存、または送信するすべてのデバイスを仮想ネットワーク内に配置することで、適切なポリシー適用ロギング機能を備えた環境に対するアクセスが制限され、PCI 監査の範囲が大幅に限定されます。

仮想ネットワークを使用する 2 番目の例としては、電力業界が挙げられます。この業界では、不可欠なインフラストラクチャである発電および送電用のネットワークと、通常業務用のネットワークを常に完全に分離することが求められます。この例では、ネットワーク間で必要とされる非常に限定された通信だけが、ステートフル ファイアウォールを通じてのみ許容されます。

仮想ネットワークを使用し、そのネットワーク間の通信を分離する必要がある例としては、他にも製造現場、ビル システム、ゲスト ネットワークなどがあります。製造業の観点からは、知的財産喪失の脅威が大きな問題になりますが、同じように重要なのが、製造現場の分離の必要性です。Internet of Things（IoT）がマルウェアに対して脆弱になったことで、企業の製造能力が文字どおり人質に取られる可能性があるからです。同様に、HVAC、セキュア エントリ、ビデオ監視などのビル システムも、組織のネットワーク内の他の部分から分離して、メンテナンスまたはセキュリティ対象のシステムに対するアクセスを制限すべきです。最後に、組織は、ゲスト ネットワークを促進し、仮想ネットワークを使用して分離することで、インターネット アクセス以外のアクセスを許可しない状態を実現できます。

これらすべての例で明らかなのは、仮想ネットワークを使用することで、セキュリティ ポリシーの適用がシンプルになることです。それは、特定のプロトコルだけを使用して、必要なユーザだけにアクセスを戦略的に制限すると同時に、ファイアウォールをフュージョン デバイスとして使用し、仮想ネットワーク間、または SD-Access ファブリック外部へのトラフィックを制御して、豊富なロギング機能を提供することによって実現されます。

定義する仮想ネットワークの数を検討する場合、最も重要になるのは、SD-Access ファブリックを構成するネットワーク デバイス全体でサポートされる仮想ネットワークの数です。複数の仮想ネットワークで 1 つのファブリック全体が構成されます。そのため、たとえば 15 の仮想ネットワークを定義すると、エッジ ノードまたはボーダー ノードのいずれかとして定義されたすべてのファブリック デバイスで、15 の仮想ネットワークがサポートされなければなりません。これは一般的に、Catalyst 3850 または 3650 を組み合わせたエッジ ノードに該当します。したがって、たとえば、DNA Center 1.1.3 では最大 64、Catalyst 9300 ではさらに多数の仮想ネットワークがサポートされますが、Catalyst 3850 および 3650 スイッチでサポートされる仮想ネットワークの数は最大 32 です。そのため DNA Center 1.1.3 を実行しているファブリックにインストールされている Catalyst 3850 では、仮想ネットワークの数が 32 に制限されます。

また、定義する必要がある仮想ネットワークの数を検討する場合にもう 1 つ重要な事項は、仮想ネットワーク間の通信が必要な場合には、何らかの形式のルート リークが必要になることです。たとえば、ある仮想ネットワークが従業員のデバイス専用であり、コラボレーション デバイス専用に 2 つ目の仮想ネットワークを確立した場合には、従業員デバイスの Cisco Jabber® や Cisco Spark™ などのコラボレーション アプリケーションが、IP フォン、Cisco Spark Board、ビデオ エンドポイントなどと通信するためには、ルート リークの方法を用意する必要があります。基本的に、該当するアドレス範囲に対してルート リークを有効にするだけでなく、ポリシーの観点から、適切な通信のために許可する必要があるすべての UDP ポートを特定することが重要です。同様に、HR、財務、会計などのビジネス機能や、学生、教職員、管理者などのユーザのタイプに基づいて別々の仮想ネットワークを作成し、関連するルート リークを定義するのは、非常に面倒になる可能性があります。このような例では、1 つの仮想ネットワーク内で拡張可能グループを使用してユーザをセグメント化することも検討すべきです。

SD-Access によるルーティングを考慮する際に、アンダーレイ ネットワークを作成し、作成する各仮想ネットワーク内で使用するために、新しい IP アドレッシング戦略を導入することも重要になります。

専用の仮想ネットワークを作成するための最適なアプローチは、最初は小規模から開始し、順次拡張していくことです。上記の例では、セグメントに対するアクセスを最小にするために、厳格に分離することが必要なことがわかります。

拡張可能グループ タグ

同じ仮想ネットワーク内のデバイス間で通信を許可し、セキュリティ ポリシー制御を行う必要はあるが、ネットワーク レイヤで分離する必要はないその他のアプリケーションやビジネスでは、SGT を使用することで効果的なセグメンテーション戦略を実行できます。仮想ネットワークを単独で使用せず、SGT を使用する主な利点の 1 つは、SD-Access 内の仮想ネットワーク内を含め、ネットワークのマイクロセグメンテーションが可能になることです。その場合はたとえば、同じスイッチに接続されたデバイスについても、SGT が同じか異なっているかに応じてデバイス間の通信を制限するポリシーとコントラクトを作成できます。この機能により、コントラクトまたは SGACL、あるいはポリシー内のレイヤ 4 アクセス制御エントリに基づいて、拡張可能グループ間だけでなく同じグループのメンバー間でも、マルウェアの水平方向の拡散が制限され、攻撃対象領域が限定されます。

セグメンテーションに SGT を使用する環境としては、たとえば大学が挙げられます。大学は、教職員、従業員、学生、プリンタ、さらにキャンパス設備やセキュリティ機器など、さまざまなタイプのユーザとデバイスで構成されています。学生とキャンパス設備やセキュリティ機器の間にもセグメンテーションが必要になりますが、拡張可能グループで分離することで対応できます。

もう 1 つは、企業が従業員、インターン、請負業者、ベンダー、人事、財務、経営幹部を SGT を使用してセグメント化する例が挙げられます。従業員の一般的なグループを SGT によって簡単に識別し、企業の会計データや従業員データから分離できます。

企業の合併買収の際に、新しい従業員が参加したり、事業の部分的な再編成に伴う従業員の異動があったりした場合にも、拡張可能グループを利用すれば容易に対応が可能です。さらに、対象の従業員を対象外の従業員から分離しながら、必要なアプリケーションとリソースへのアクセスを許可するポリシーを作成することで、機密情報へのアクセスを制限するために必要なポリシーベースの制御が可能になります。

これらの例からわかるように、仮想ネットワークを使用してネットワークを分離する必要がないことがあります。これらすべての例で、拡張可能グループに基づいたグループベースのポリシーによるセキュリティ制御で、セグメンテーション要件に十分に対応することができます。前述のように、実際には仮想ネットワークまたはレガシー VRF 内で拡張可能グループを利用するだけで、同じ仮想ネットワークまたは拡張可能グループのメンバー間での水平方向の攻撃対象領域を最小限にすることができます。

仮想ネットワークの作成に関する、SD-Access ファブリックにおけるセグメンテーション戦略と、仮想ネットワークに割り当てる拡張可能グループを評価する場合、1 つの拡張可能グループを複数の仮想ネットワークに割り当てることも、すべての拡張可能グループを 1 つの仮想ネットワークに割り当てることもできます。これは、セグメンテーション戦略に応じて現在何を導入しているかによって決まります。

SD-Access 仮想ネットワーク内で拡張可能グループを使用する場合は、考慮すべき要因がいくつかあります。

- 送信元/宛先ペア（ポリシー マトリックスにおける x:y 軸の交わったセル）に多数のレイヤ 4 ベースのアクセス制御エントリを適用するポリシーは、標準ではなく例外とすべきです。
- 現在、SD-Access ファブリックの仮想ネットワーク内にはファイアウォールを導入できないため、SGT 間のステートフル パケット インスペクションは実行できません。SGT ベースのポリシーと、関連するコントラクトを使用します。
- 独自の SGT を必要とする基準と、サポートする SGT の合計数を慎重に検討して定義する必要があります。

ポリシーとコントラクト、またはそれらで構成される SGACL は、スイッチ TCAM を消費することを理解しておく必要があります。多数のアクセス制御エントリが設定されたコントラクトまたは SGACL を使用すると、TCAM が枯渇し、その後新しいポリシーのプログラミングができなくなる可能性があります。ポリシーは、可能な限りシンプルなものにすべきです。また、グループベースのポリシーでは、ファイアウォールと同等のステートフル パケット インスペクション機能や詳細なロギング機能を実現できないことも理解しておく必要もあります。

とは言え、ほとんどの場合、拡張可能グループによるセグメンテーションによって、同じ仮想ネットワーク内のユーザとデバイス間で優れたセキュリティ制御を実現できるこも事実です。これまでに多くの組織と政府機関が、セグメンテーション戦略に対応する単独のテクノロジー、または主要なテクノロジーとして Cisco TrustSec を導入しています。

実際多くの監査担当者は、POS マシンやカード リーダーのための効果的なセキュリティ制御として、PCI デバイス専用の SGT を使用することの効果を認識しています。それにより、拡張ネットワークにおける監査範囲が限定されます。これも、セキュアなセグメンテーション戦略策定に対する、仮想ネットワークまたは SGT というアプローチの利点を示しています。

読者へのヒント

POS マシンやカード リーダーのセキュリティ制御として SGT の使用が認められるかどうかは、PCI の監査担当者の判断によりますが、これまでの監査では、SGT の使用は、セキュリティ制御の証拠として認められていますPCI 監査に備える組織は、監査担当者と事前に話し合っておく必要があります。事例については、https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec_pci_validation.pdf [英語] を参照してください。

拡張可能グループを使用せずに SD-Access ファブリックで仮想ネットワークを展開することは可能ですが、拡張可能グループが存在する仮想ネットワークが少なくとも 1 つ存在する必要があります。デフォルトでは、これが DEFAULT_VN です。

仮想ネットワーク内に拡張可能グループを導入する場合、グループベース ポリシーの作成に SGT を使用することは、SD-Access ファブリックとボーダーに限定されます。トラフィックがボーダー ノードで仮想ネットワークから送信される場合には、プラットフォームに応じて、ボーダー、またはボーダー ノードに隣接するデバイスで、外部の宛先にグループベースのポリシーを適用できます。SGT と Cisco TrustSec をネットワーク内の他の場所でも使用する場合は、外部の非ファブリック ネットワークにタグ情報を伝播させるために、Cisco TrustSec インライン タギングと SXP のいずれか、または両方が必要になります。

SD-Access 中継サイトを使用して構成された SD-Access 分散キャンパスを導入する場合は、Cisco TrustSec インライン タギングや SXP を使用せずに、シームレスに SGT を送信できます。これは SGT が、各ファブリックのボーダー ノード間で VXLAN ヘッダーに挿入されて送信されるためです。

読者へのヒント

SD-Access 分散キャンパス導入の詳細については、SD-Access e-book（https://www.cisco.com/c/dam/en/us/products/se/2018/1/Collateral/nb-06-software-defined-access-ebook-en.pdf [英語]）を参照してください。

SD-Access の移行の詳細については、『SD-Access Migration Guide（SD-Access 移行ガイド）』（https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-739524.html [英語]）を参照してください。

もう 1 つ重要なことは、作成された仮想ネットワークの数と同様に、作成する拡張可能グループの数を評価することです。組織内の主要な各部門に SGT を割り当てるのは正常なことですが、部門をさらに各種の役割まで分割すべきではありません。

たとえば大学の環境で、「教授」に対して SGT を定義するとします。次に、数学、物理学、生物学、言語などの部門に分割することを考えます。ここで考えるべきことは、教授について、固有のポリシーが適用される複数の SGT を部門ごとに本当に作成する必要があるのか、それとも、すべての部門が、サーバや各種のデータに同じようにアクセスできる 1 つの SGT を共有すればよいのか、ということです。

拡張可能グループを定義する最良のアプローチは、すべてのロール、機能、デバイス タイプなどについて、事前にそれぞれグループを作成しないことです。グループを作成してしまうと、膨大なポリシー作成が必要になるだけでなく、スイッチやルータの SGACL ストレージ用に、さらに多くの TCAM やメモリ リソースが必要になります。ほとんどの場合、膨大なグループ定義とポリシー作成によって、セグメンテーション プロジェクトは停滞します。関係者すべてが、各ポリシー固有の利点を意識し始め、決定できなくなるからです。これは「分析まひ」と呼ばれます。さらに、グループとポリシーについて早い段階で合意ができても、ポリシーを適用すれば、見落としに対応するための変更は避けられません。それによってサービス妨害の可能性や、ポリシー変更による影響も発生します。

VN 戦略を評価する場合と同様に、まずはゆっくりと小規模で開始すべきです。特定のアプリケーションやデータへのアクセス制限によって、ただちに具体的な利点が得られるグループを特定します。初回のポリシーの効果が判定されれば、必要に応じてポリシーを簡単に変更し、また、グループ定義の追加が必要であるかどうかを判断できます。

使用例

以下の使用例は、仮想ネットワークと拡張可能グループを使用して SD-Access ファブリック内でセグメンテーションを導入する例を示しています。前述のように、仮想ネットワークは、ネットワーク セグメンテーションの第 1 レイヤ、またはマクロ レベルとして、1 つの仮想ネットワークのトラフィックを他のトラフィックから完全に分離します。次に拡張可能グループを使用して、セグメンテーションの第 2 レイヤまたはマイクロ レベルを、仮想ネットワーク内のトラフィックに適用できます。仮想ネットワーク内で拡張可能グループを使用するかどうかは任意ですが、異なる拡張可能グループ内のエンドポイント間でトラフィックを制限でき、さらに Cisco TrustSec のグループベース ポリシーを使用して、同じグループのメンバー間の通信も制限できるため、セキュリティはさらに向上します。

注意

以下に示すのは例にすぎません。各シナリオのネットワーク セグメンテーションに関する検証済みのアプローチを示すものではありません。どの組織にも、セグメンテーションの導入について独自の要件および目標があります。これらの使用例は検討材料として捉えてください。

大学

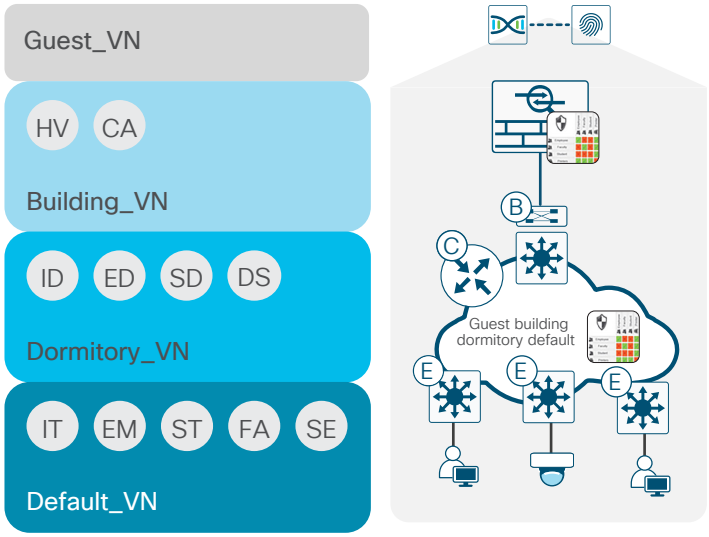
大学のキャンパスは、セキュリティの実施が特に困難な環境であるかもしれません。多数の個人用デバイスがキャンパスに持ち込まれ、寮ではストリーミングやゲーム アプリケーションが使用され、侵害されたインターネット サイトに学生がアクセスすることもあれば、学生が意図的にマルウェアを実行する可能性さえあるため、大学の環境のセキュリティ保護は非常にむずかしくなります。

大学にセグメンテーションを導入することで、トラフィックの分離が可能になり、セキュリティの新たなレイヤが追加されます。寮とキャンパス内の教室、講堂、研究室などにそれぞれ仮想ネットワークを導入することで、管理者は各環境を分離できます。その上で、各仮想ネットワーク内の拡張可能グループによるマイクロセグメンテーションを行えば、Cisco TrustSec ポリシーを適用して、各仮想ネットワーク内のグループ間の通信をさらに制限できるようになります。

図 10 に、ある大学のキャンパスに SD-Access を導入してセグメンテーションを行った例を示します。

図 10. 高等教育機関でのセグメンテーション

Label	Name
HV	HVAC
CA	Campus Security
ID	IT_Dorm
ED	Employee_Dorm
DS	Dorm_Services
SD	Student_Dorm
FA	Faculty
IT	Information Technology
EM	Employee
SE	Services
ST	Student



大学の例では、4 つの仮想ネットワークが導入されています。この例では、キャンパス環境内のほとんどの拡張可能グループについて Default_VN を使用しています。ここでは、学生（ST; Students）、教職員（FA; Faculty）、管理スタッフ（EM; Employee）用にそれぞれ拡張可能グループが設定されています。さらに、IT スタッフ用の IT グループと、デジタル サイネージ、スマート ボード、プリンタなどに使用するサービス（SE; Services）グループがあります。

Dormitory VN は、寮で使用される仮想ネットワークです。この VN では、使用されている一部の拡張可能グループが、名前は異なりますが、Default VN のグループと重複していることがわかります。これは、1.3 で VN-Agnostic SGT が利用可能になったときに更新する必要があります。詳細についてはこのドキュメントの対象外ですが、デバイスの認可中に、エンドポイントが接続されるネットワーク デバイスの場所をポリシーで使用して、一意の拡張可能グループを割り当てることができます。したがって、ネットワーク デバイスが寮にあり、学生が SD SGT に関連付けられていても、他の場所で認証された場合には、ST SGT が割り当てられます。

最後に、Guest VN と Building VN があります。Building VN は、標準の建物の制御と、ビデオおよびエントランスのセキュリティに使用されます。

この例で使用されている仮想ネットワークが導入された大学の環境では、仮想ネットワーク間のトラフィックを完全に許可しないことが可能です。その場合、図内のファイアウォールは、外部の非ファブリック ネットワークとの間で必要な相互接続だけを許可します。ただし必要に応じて、仮想ネットワーク間にグループベース ポリシーを適用する SGFW としても機能できます。

この例のファイアウォールは、Cisco ISE とのピアリングによって、認可されたユーザ用に SXP または pxGrid 経由でマッピング情報を受信し、グループベースのポリシー、またはネットワーク内の他の場所での伝播に使用できます。

製造業

製造業では、社内とプラントの両方のセキュリティが重視されています。産業スパイと知的財産喪失の脅威がある一方で、サイバー攻撃は製造工程の妨害に注力しています。製造業はサイバー攻撃の対象として、年間の上位 3 つの業界に入っています。2017 年シスコ セキュリティ機能ベンチマーク調査では、「製造業の 28 % の企業で、昨年 1 年間に 1 回以上の攻撃によって損失が発生している」と報告されています。

ISA99（International Society of Automation）規格委員会は、産業界の自動化および制御システムに関する新たなセキュリティ規格の策定に、継続的に取り組んでいます。この規格では、ソフトウェアやモニタリング システムのセキュリティだけでなく、製造工程や制御のセキュリティも対象とされています。

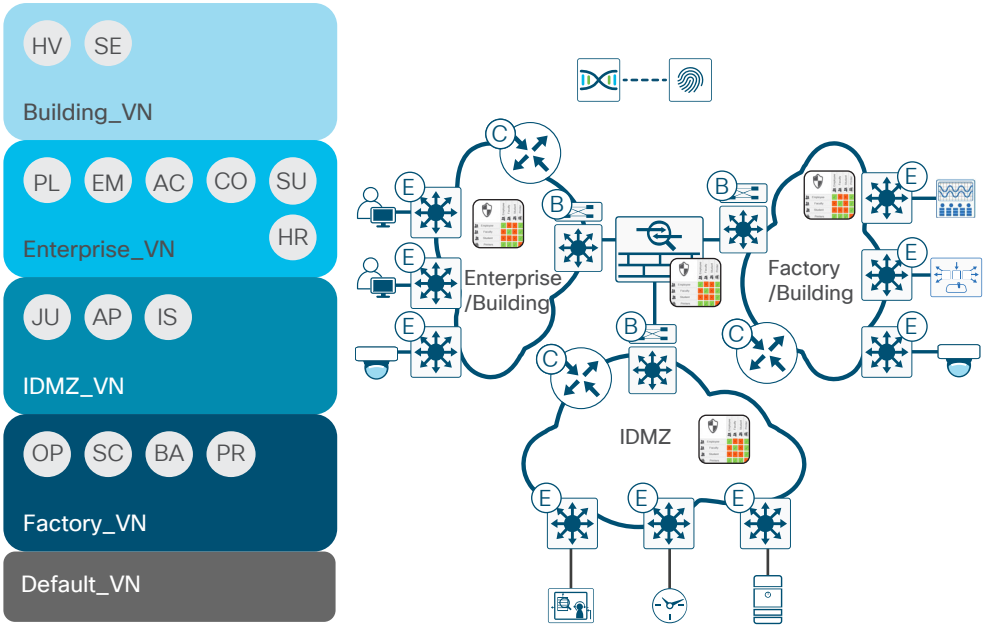
使用される通信プロトコルと、重要なプロセスへのアクセスのあらゆる側面にセキュリティを組み込むことで製造業を変革する取り組みに加え、ネットワーク セグメンテーションによってセキュリティ レイヤを追加し、さまざまなシステムへのアクセスを制御するポリシーを適用できるようになります。

図 11 に、製造業のネットワークに導入できるセグメンテーション戦略を示します。ここでは、3 つのファブリックがファイアウォールで接続されています。SD-Access ファブリックの 2 つには、それぞれ Enterprise/Building と Factory/Building の 2 つの仮想ネットワークが含まれています。この図では 1 つの例だけを示していますが、実際には、4 つすべての仮想ネットワークを定義し、それぞれをファイアウォールで接続する、1 つのファブリックを実装することが可能です。各仮想ネットワークには、仮想ネットワーク内でのマイクロセグメンテーションを実現する、複数の拡張可能グループがあります。

このセグメンテーション戦略では、Building、Enterprise、IDMZ、Factory の 4 つの仮想ネットワークが確立され、図に示すファイアウォールを通じてのみ相互接続が可能です。このファイアウォールには、4 つすべての仮想ネットワークから拡張可能グループ情報が送信されます。SGT をポリシー作成に使用することで、仮想ネットワーク間のアクセスを必要最小限に制限することができます。

図 11. 製造業でのセグメンテーション

Label	Name
HV	HVAC
SE	Security
PL	Plant Operations
EM	Employee
AC	Accounting
CO	Contractor
SU	Supplier
HR	Human Resources
JU	Jump Boxes
AP	Industrial Applications
IS	Industrial Services
OP	Site Operations
SC	Supervisory Control
BA	Basic Control
PR	Process



Enterprise VN には、さまざまなタイプのユーザについて定義された拡張可能グループがあります。各グループは、データセンターまたはその他の場所（図では示されていない）にあるリソースだけにアクセスでき、他の拡張可能グループ内のユーザやデバイスにはほとんど、または、まったくアクセスできません。仮想ネットワーク内では、グループ間で許容される通信を特定するか、すべてのアクセスを単純に拒否するポリシーを確立できます。

Building VN は文字どおり建物用であり、建物のすべての制御機能が含まれています。この例では、入口でのカード認証やロック メカニズムなどの物理的なセキュリティ、ビデオ監視、HVAC、さらに建物の照明やデジタル サイネージが設定されています。Building VN に対して唯一許可されるアクセスは、管理者または請負業者によるシステムに対するメンテナンス アクセスです。

Factory VN は工場の作業現場用であり、最高度のセキュリティ要件が適用されるセグメントです。Factory VN では、拡張可能グループ間のポリシー制御強化のために、マイクロセグメンテーションを行います。ここで定義されているグループは、一般的に監視制御に使用されます。各種のプロセスまたは作業セル間の製造プロセスをモニタおよび自動化するために使用され、他の SGT は数値制御、コンベア システム、ロボットなどで使用されます。通常、運用スタッフは、ファイアウォールの背後にある IDMZ を通じてのみ Factory VN にアクセスできます。ユーザはほとんどの場合、IDMZ にある VDI サーバ経由でのみアクセスが可能です。

最後に、IDMZ は製造現場とのすべての通信を制限します。工場の従業員または Enterprise VN の従業員が Factory VN 内のリソースにアクセスする必要がある場合、IDMZ 内の VDI ジャンプ ボックスを通じてのみ可能です。工場の運用で必要とされる Network Time Protocol や Active Directory などのサービスは、Factory VN 専用として使用され、それらも IDMZ に配置されます。製造アプリケーションは IDMZ に配置され、Factory VN エンドポイントからアクセスされます。

医療

医療業界に対する攻撃は毎年増え続けており、ランサムウェアやマルウェアによる犯罪的な攻撃が、最も一般的な攻撃ベクトルになっています。これまで医療業界では、セキュリティ制御を導入して環境を保護することが遅れていました。患者情報、財務データ、クレジット カード データ、研究データなど、ターゲットとして価値の高いデータが多くあることから、医療業界が悪意のある攻撃のターゲットになるケースが増えているのも当然です。

ネットワーク セグメンテーションは、重要なシステムや患者データへのアクセスを統制する明確に定義されたポリシーを適用してセキュリティ制御を強化する手段として、多数の医療機関で導入されています。ネットワーク セグメンテーションによって、医療機関では多様なシステムまたは機能を小規模な環境またはセグメントに分割し、セグメント間とセグメント内のアクセスを制限できます。

しかし VRF、さらには MPLS を導入している医療機関がある一方で、ほとんどの病院や医療機関のキャンパスでは、個別臨床ネットワークを構築して、ファイアウォールによって管理環境と病棟を分離しているだけです。通常、実際に運用されているセグメンテーションはこれだけです。これは、病院または大規模なキャンパスのデータセンターのサーバ ファームの外部になります。

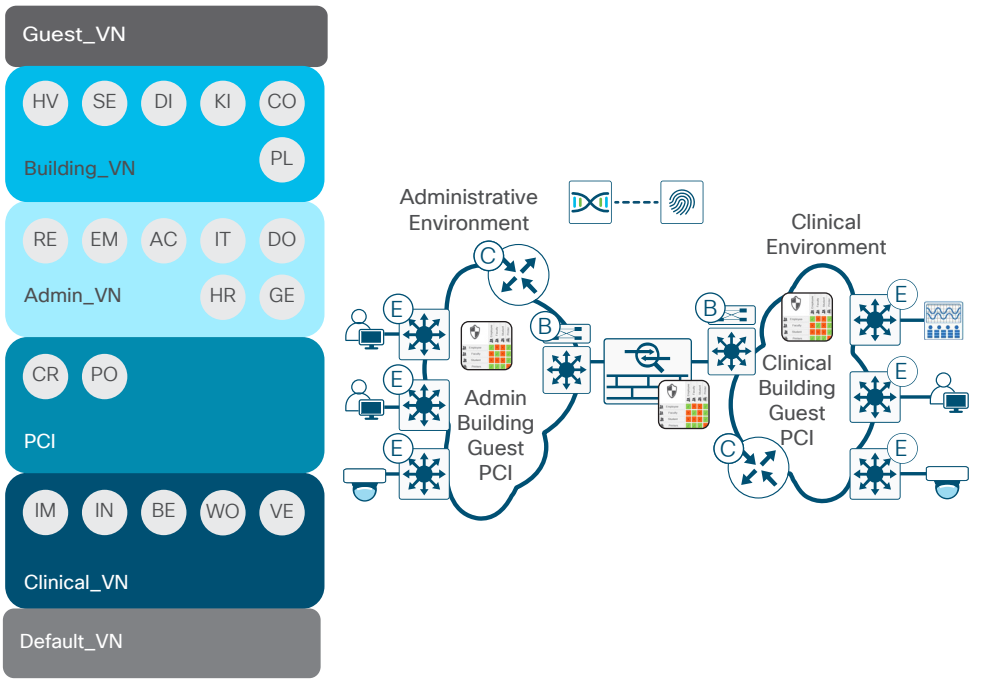
図 12 は、2 つの別のファブリックを示しています。1 つは管理機能用、もう 1 つは臨床環境用です。ここでは、各環境で 2 つの別のネットワークが維持される、確立された手法がとられています。現実的には、仮想ネットワークと SGT によってセグメント化された 1 つのファブリックでは不十分だという理由はありません。

ここに示す 2 つのファブリックでは、Admin 仮想ネットワークまたは Clinical 仮想ネットワーク内のデバイスと通信のセグメント化に、それぞれ仮想ネットワークが定義され、他のセグメント（仮想ネットワーク）がビル管理、ゲスト サービス、さらに PCI 用に確保されています。図 12 に示すように、Building、Guest、および PCI VN は、いずれの環境でも利用可能であるため、両方のファブリックにまたがっています。

Admin と Clinical の 2 つのファブリック/環境はファイアウォールによって接続され、そのファイアウォールがファブリック間のアクセスを制限しながら、各ファブリック内の 4 つの仮想ネットワークを相互接続しています。一般的ではありませんが、場合によっては仮想ネットワーク間の通信が必要になることもあります。そのような状況では、ユーザのデバイス上に存在するマルウェアが別の仮想ネットワークに移動しないように、ユーザが仮想ネットワーク専用の VDI を使用する必要が生ずる場合があります。

図 12. 医療機関でのセグメンテーション

Label	Name
HV	HVAC
SE	Security
DI	Digital Signage
KI	Kiosk_Information
CO	Contractor
PL	Plant Operations
RE	Research
EM	Employee
AC	Accounting
IT	IT Admin
DO	Doctor
HR	Human Resources
GE	General
CR	Card Reader
PO	Point of Sale
IM	Imaging
IN	Infusion Pumps
BE	Bedside Monitors
WO	Workstation/Carts
VE	Vendor



この例では、各仮想ネットワーク内の拡張可能グループによって、Cisco TrustSec ポリシーによるマイクロセグメンテーションが実現し、同じグループ内のメンバー間の通信に加え、拡張可能グループ間の通信が制限されます。そのため仮想ネットワーク内の攻撃対象領域が大幅に限定され、ユーザ間でマルウェアが水平方向に拡散する危険が最小限になります。

図 12 で導入されているセグメンテーション戦略で、Clinical 仮想ネットワークは、非常に厳格なセキュリティ制御を必要とするセグメントになっています。臨床環境は、実際の病棟と、モニタリング、イメージング、患者ケア システム/デバイスで構成されています。この仮想ネットワークに対する侵害は人命に関わるため、デバイスからこの仮想ネットワークにアクセスすることは、最も制限すべきです。ここに示すように、VE SGT は、さまざまなイメージング、モニタリング、患者ケア システムの修復または調整のためにオンサイトに来るベンダー専用として利用されてきました。

ここでは、医療情報（PHI; Patient Health Information）システムと電子カルテ（EHR）システムは示されていません。通常これらのシステムは、データセンター内のセキュアなエンクレーブや、場合によってはクラウド内に置かれています。これらのシステムには多くの場合、Clinical VN（WO SGT）または Admin VN（DO SGT）からアクセスします。

Admin VN は、医療環境における臨床以外の作業用に確保されています。この環境は、医療システムの管理スタッフと IT スタッフ、さらに医師や研究者が使用します。この仮想ネットワークには、各種医療現場における実際のオフィスが含まれる場合もあります。

PCI VN は多くの場合、医療環境の中で、医療以外の専門家によって管理されています。現実には、PCI 環境は両方の環境にわたって展開され、ギフト ショップ、売店、カフェテリア、さらには部門の受付や患者の自己負担金の受領などもサポートしています。

Building VN では、施設またはキャンパス全体の建物、セキュリティ、情報システムを完全に分離できます。病室や待合室の患者やゲスト向けの情報キオスク、デジタル サイネージ、ビデオ ストリーミングも、Building VN に配置できます。

最後に、Guest VN はすべての患者とビジターによるインターネット アクセス用に用意されています。

PCI および小売

PCI 監査を受けたことがあればわかることですが、ネットワーク図の作成、カード所有者のデータ（保管中および転送中を含む）を保護する制御の証拠の提示、範囲の明確化、レポートやログのサンプルの提示には、大量の情報と時間が必要になります。カード所有者データは、ステートフル検査と脅威検出が可能なファイアウォールの背後に保存されますが、ネットワーク全体に配置された、POS マシンやカード リーダーなどその他のコンポーネントも対象になります。

データセンターに存在するカード所有者データ環境（CDE）を保護する場合、Cisco ACI や Cisco TrustSec を使用したテナントやエンドポイント グループなどのセグメンテーション戦略に加えて、NGFW を使用することで、セキュリティ制御を特定して導入することが容易になります。

ブランチ環境、さらにはキャンパス環境では制御が困難になり、POS マシンやカード リーダーが接続されたネットワークに対する PCI 監査の範囲が大幅に拡大する可能性があります。これは、セグメント化されていない場合、同じネットワークに接続されているものは、有線でもワイヤレスでも、POS マシンと合わせてすべて PCI 監査の対象になるためです。

小売、金融、医療などの分野の組織では、仮想ネットワークと VRF、また拡張可能グループに基づくセグメンテーション戦略を導入し、PCI 監査の範囲を限定することで、負担が軽減される可能性があります。他のすべてから分離された仮想ネットワークを使用することで、対象範囲を限定できるだけでなく、ファイアウォールを使用してアクセスを制限しながら、詳細なロギング機能によって、セキュアなアクセスにも対応できます。

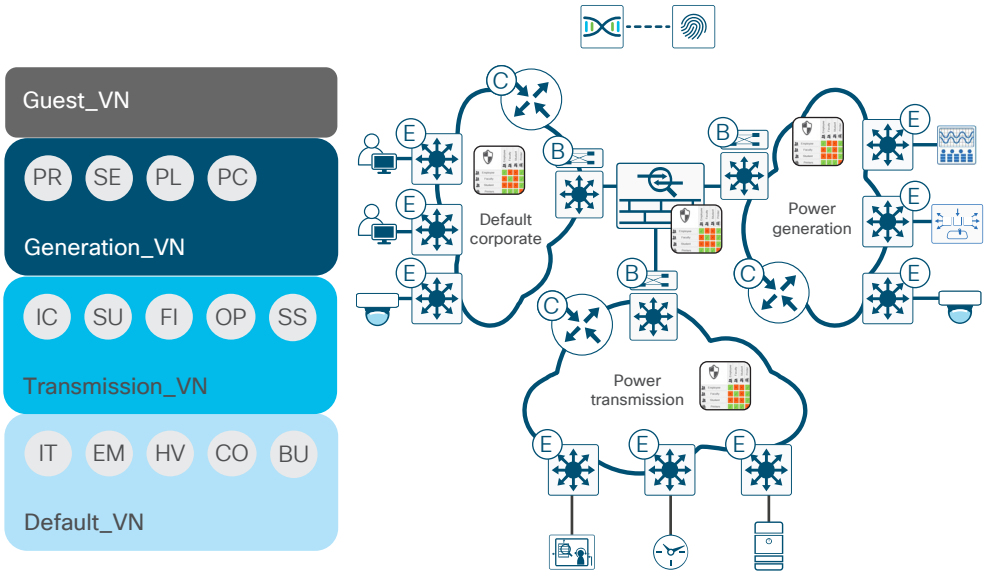
電力

北米では、North American Electric Reliability Corporation（NERC）が規制機関として、Critical Infrastructure Protection（CIP）規格の導入によって電力システムの信頼性とセキュリティを確保しています。欧州では European Union Agency for Network and Information Security（ENISA）が、Smart Grid Architecture Model（SGAM）を利用して同様の役割を果たしています。基本的な要件の 1 つは、発電、送電、社内業務を相互に分離するネットワーク境界を明確に定義することです。これらのネットワーク間のアクセスは、ファイアウォールによって制御されます。この環境では、完全な分離が必要であり、ネットワーク間ではセキュアなアクセスだけを限定的に許可するために、仮想ネットワークの使用がほとんど既定事項になっています。

図 13 は、電力会社でネットワーク セグメンテーションを使用した例を、大幅にシンプルにして示しています。この例では DEFAULT_VN に加えて、3 つの仮想ネットワークが定義されています。DEFAULT 仮想ネットワークは、従業員、請負業者、社内の全体の HVAC やセキュリティ システムを含む全設備について使用されます。Power Generation VN は発電所専用で、Power Transmission VN は変電所の装置および制御/現場作業スタッフで構成されています。最後に、Guest VN は社内設備用に定義されています。これら 3 つの仮想ネットワークでは、ファイアウォールによってアクセスを制限することで必要な分離を実現し、法規制遵守の要件に対応しています。

図 13. 電力分野におけるセグメンテーション

Label	Name
PR	Process
SE	Plant Security
PL	Plant Operations
PC	Plant Contractor
IC	Instrumentaion and Control
SU	Substation
FI	Field
OP	Operations
SS	Substation Security
IT	IT Staff
EM	Employee
HV	HVAC
CO	Contractor
BU	Building Security



個々の仮想ネットワーク内では、ネットワークでさらにマイクロセグメンテーションを実施し、仮想ネットワーク内の拡張可能グループ間のアクセスを制限する必要があります。Transmission VN がその例です。この仮想ネットワークでは、電力線の装置および制御（IC）、変電所の装置および制御（SU）、変電所のキー エントリと IP 監視のためのセキュリティ システム（SS）、変電所および電力線メンテナンスのためのフィールド エンジニアリングおよび架線作業員（FI）、システム全体の運用および制御スタッフ（OP）について、それぞれ拡張可能グループが定義されています。マイクロセグメンテーションは、送電網の監視と制御が必要な場合のアクセスに対する制限を軽減しながら、装置および制御エンドポイントとフィールド リソース間のアクセスを制限するために必要になります。

付録 A：ネットワーク セグメンテーションの概要：簡単な経緯

読者へのヒント

このセクションは、VLAN や VRF、さらには Cisco TrustSec® を含む、ネットワーク セグメンテーションにあまり詳しくない読者を対象としています。これらの概念に精通している場合は、次のセクションに進んで、現在のネットワーク セグメンテーションに関する説明をお読みください。

ネットワーク セグメンテーションは新しい概念ではありませんが、この 20 年ほどの間に大幅な進化を遂げました。当初ネットワーク セグメンテーションは、仮想 LAN（VLAN）を使用して、1 つの「フラットな」ネットワーク/ブロードキャスト ドメインを小さなセグメントに分割するプロセスとして定義されていました。当初の目的は、デバイスが処理する必要があるブロードキャスト数を最小にすることで、ネットワーク自体だけでなく、エンドポイントを含めた全体的なパフォーマンスを向上させることでした。

しかしその後、セキュリティ上の理由から VLAN を使用したネットワーク セグメンテーションが導入されました。また、アクセス コントロール リスト（ACL）を使用してセグメント間の通信を制限し、ビジネス関連のポリシーを適用するためにも使用されました。当初 VLAN は、1 つのセグメント（VLAN）とそのデバイスを分離するだけの、非常に基本的な手段でしかありませんでした。その後プライベート VLAN によって、VLAN 内の通信をさらに制限するマイクロセグメンテーションが可能になりました。

最終的に、場所にかかわらず全社的にネットワーク セグメントを拡張する必要性から、Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）インスタンスの概念が導入され、ネットワーク セグメント間のレイヤ 3 分離が実現しました。各 VRF が独自のルーティング テーブルを保持し、仮想ネットワークを作成することで分離されます。1 つの VRF に含まれるルートが別の VRF には含まれておらず、相互の通信が制限されるためです。

シスコは 10 年をかけて、Cisco TrustSec® という新しいテクノロジーを開発しました。それによって、「ネットワーク セグメンテーション」の意味が再定義されることになりました。Cisco TrustSec では、セグメンテーションは、IP アドレッシングやルーティングを使用した VLAN や VRF に基づいて実現されるものではなくなっています。IP アドレッシングに関わりなく、ロールベースまたはグループベースのメンバーシップを使用してポリシーを作成することで、ネットワークをセグメント化します。

VLAN およびプライベート VLAN

初期のネットワーキングでは、「ネットワーク セグメンテーション」という用語は、大規模でフラットな Open Systems Interconnection（OSI）レイヤ 2 ネットワークまたはブロードキャスト ドメインを、小規模なネットワーク セグメントまたは OSI レイヤ 3 サブネットに分割するプロセスを示すために使われていました。それによって、接続されたエンドポイントからのブロードキャストの範囲がサブネット内に限定されるため、エンドポイントが分離され、ネットワークの全体的なパフォーマンスが向上していました。こうした個々のレイヤ 2 セグメントの概念が最終的に IEEE 802.1Q 規格に組み込まれ、セグメントが VLAN と呼ばれるようになりました。

VLAN によって、1 つのセグメントまたは VLAN 内のデバイス トラフィックが別のトラフィックから分離されます。VLAN 間の通信はすべて、レイヤ 3 インターフェイスを通じてルーティングされる必要があるためです。このレイヤ 3 インターフェイスでは、ACL を適用することで、TCP または User Datagram Protocol（UDP）ポート番号によって特定された IP アドレスまたはアプリケーションに基づいて、転送するトラフィックとドロップするトラフィックを制御できます。現在ではルータ ACL、または RACL と呼ばれる ACL は当初、レイヤ 3 の境界でのみ適用が可能でした。しかしスイッチング製品が進化するとともに、VLAN ACL または VACL と呼ばれる ACL を VLAN に適用し、最終的に PACL と呼ばれるポート ACL を物理インターフェイスに適用できるようになりました。現在の基準から見れば初歩的なものですが、これは VLAN 内または VLAN 間でデバイス間の接続を保護する効果的な手段になりました。またこの戦略は、現在も多くの組織で、ファイアウォールによって補完されながら使用されています。

またプライベート VLAN の導入によって VLAN が強化され、さらに細かいセグメンテーションが可能になりました。プライベート VLAN は、プロミスキャス（P）ポートを使用したプライマリ VLAN、分離（I）ポートを使用した分離 VLAN、コミュニティ（C）ポートを使用したコミュニティ VLAN の、3 つのタイプの VLAN で構成されています。プライマリ VLAN の（P）ポートは、スイッチ仮想インターフェイス（SVI）、またはルータが接続されたポートに関連付けられています。分離 VLAN に割り当てられたポート（I）は、アップストリームでプロミスキャス（P）ポートとのみ通信でき、コミュニティ VLAN に割り当てられたポート（C）は、相互に、または（P）ポートと通信できます。それによって、分離ポート間、分離ポートとコミュニティ VLAN 間、またはコミュニティ VLAN 間のセグメンテーションが実現します。分離ポートとコミュニティ ポート間の通信は、ACL を使用してポリシーを適用できる、（P）ポートを通じて行う必要があります。

読者へのヒント

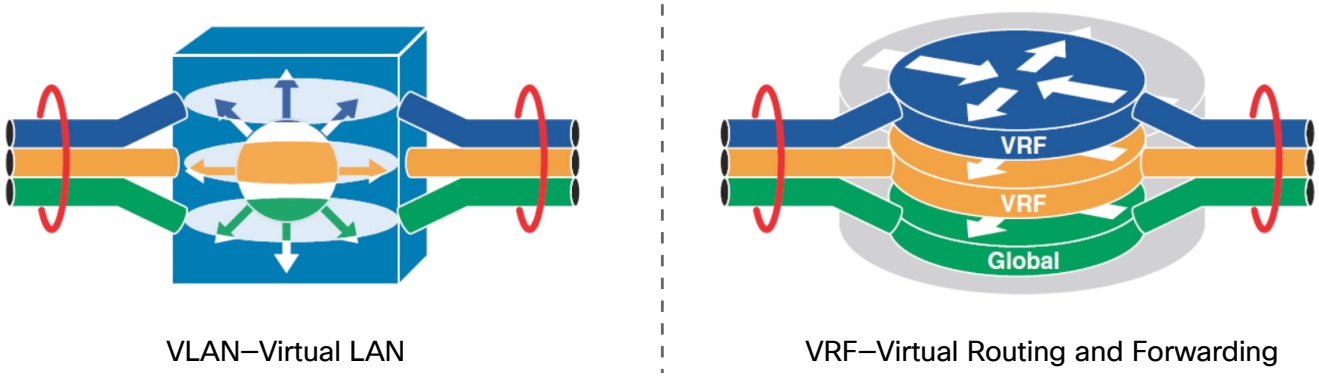
プライベート VLAN の詳細については、スイッチングに関するシスコのドキュメント、または https://learningnetwork.cisco.com/docs/DOC-16110 [英語] などのシスコ ラーニングのドキュメントを参照してください。

ネットワークで VLAN とプライベート VLAN のどちらを使用しているかにかかわらず、それらはブロードキャスト ドメインとともにネットワーク全体に拡張されるため、スパニング ツリーを戦略的に設定し、ループしない安定したネットワーク トポロジを確保する必要があります。

仮想ルーティング/フォワーディング インスタンス

前述のように、VLAN はレイヤ 2 における最も基本的なパス分離手法です。しかし、強固なネットワーク設計を行うには、ブロードキャスト ドメインの範囲とスパニングツリー ループの可能性を最小限にするために、レイヤ 2 VLAN をレイヤ 3 仮想ネットワークまたは VPN に変換する方法が必要になります。このレイヤ 3 仮想ネットワークは、独自のコントロール プレーンをサポートし、データ転送用にアドレッシング構造とルーティング テーブルを備えるとともに、そのデバイス上またはネットワーク内の他のレイヤ 3 VPN から完全に分離されていなければなりません。このタイプの機能を基本とするテクノロジーを、Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）と呼びます。図 14 では、VLAN と VRF のインスタンスの違いを示しています。

図 14. VRF と VLAN の比較



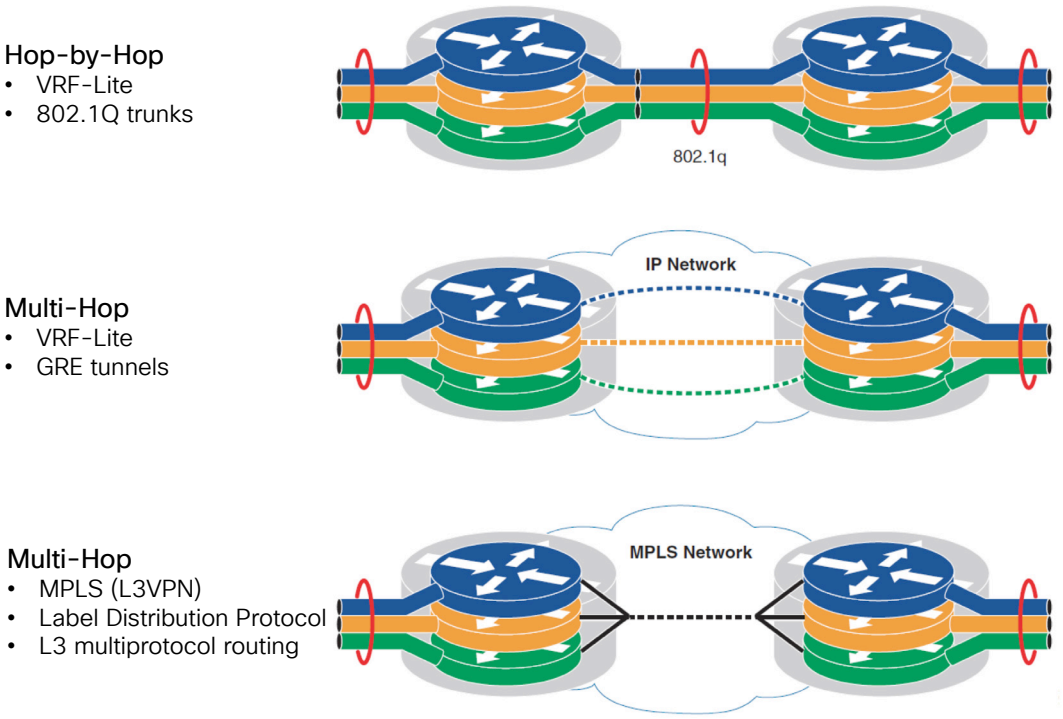
VLAN–Virtual LAN　　VRF–Virtual Routing and Forwarding

VRF は、ネットワーク デバイス上で定義され、レイヤ 2、クライアント側 VLAN、レイヤ 3 の各ネットワーク間の境界として機能します。それぞれの VRF インスタンスは、IP ルーティング テーブル、フォワーディング テーブル、そして、割り当てられた 1 つ以上のインターフェイスで構成されます。Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Border Gateway Protocol（BGP）、Routing Information Protocol（RIP）v2 などの一般的なルーティング プロトコルは、アドレス ファミリを使用して、各仮想ネットワークで固有のルーティング テーブルに登録するルートを学習してアドバタイズするために使用できます。このルーティング情報は、デバイス設定によってその VRF に割り当てられている論理的なインターフェイス（SVI）、あるいはインターフェイスとサブインターフェイスを通じて、さらに Cisco Express Forwarding テーブルに登録されます。VRF はグローバル ルーティング テーブルの上位にあり、VRF に割り当てられていない IPv4 プレフィックスおよびインターフェイスで構成されたネットワーク デバイス間で、必要なレイヤ 3 接続を提供します。

セキュリティの観点から、ネットワークのセグメント化に使用される場合、仮想ネットワークまたは VRF が定義され、IP アドレスによってエンドポイントが関連付けられ、VRF に割り当てられて VRF 内でルーティング可能になります。VRF 間のトラフィックを分離するには、デフォルトでは共有されない VRF ごとに個別にルーティング テーブルを維持します。仮想ネットワーク間でルートを「リーク」しながら、他の仮想ネットワークまたはグローバル テーブル内のリソースに対する特定のアクセスを許可することが可能です。「フュージョン」ルータまたはファイアウォールとも呼ばれるこれらのネットワーク デバイスでは、ACL を作成して、ポリシー、および、VRF とグローバル ルーティング テーブル間の通信用にリークされるルートを定義できます。

ネットワーク デバイス上の VRF インスタンスは、分離されたオブジェクトとして、ネットワーク全体の他のデバイスにある、同じ VRF の別のインスタンスに拡張する必要があります。これにはいくつかの方法があります。多数のサイト間でエニーツーエニー接続が必要な場合は、マルチプロトコル ラベル スイッチング（MPLS）が最良の方法になります。MPLS は、マルチプロトコル ルーティングと Label Distribution Protocol を組み合わせ、単一のルーティング プロセスを使用して、各 VRF 内のルートをアドバタイズすることで、エンドツーエンドの接続を実現します。ただし、ホップバイホップ、マルチホップ、またはハブアンドスポークで十分な場合は、一般に VRF-Lite と呼ばれる、MPLS 機能のサブセットを使用できます。VRF-Lite では、802.1Q、Generic Routing Encapsulation（GRE）、またはマルチポイント GRE（mGRE）を使用して、多様なネットワーク デバイスにある VRF を接続します。図 15 に、3 つすべての方法を示します。

図 15. VRF パスの分離



読者へのヒント

MPLS の詳細については、https://www.cisco.com/c/ja_jp/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html を参照してください。

Cisco TrustSec：ソフトウェアデファインド セグメンテーション

サービス プロバイダー以外の企業で VRF-Lite と MPLS が導入され、セキュリティ ポリシーを適用する方法としてネットワークがセグメント化され始めた一方、シスコは、論理コンストラクトまたはソフトウェア定義型コンストラクトを使用した Cisco TrustSec を開発しました。VRF-Lite や MPLS とは異なり、Cisco TrustSec アーキテクチャでは、IP アドレッシングや固有のルーティング インスタンスによる分離は行いません。VRF がなくても Cisco TrustSec を導入できます。TrustSec はトポロジにまったく依存しません。

Cisco TrustSec アーキテクチャの中核にあるのがセキュリティ グループ タグ（SGT）です。SGT では、任意に定義された SGT によって示される非公開ユーザ グループに任意に割り当てることで、ホストの IP アドレスの抽象化が可能です。一般的にこれらのグループは、Microsoft Active Directory または Lightweight Directory Access Protocol（LDAP）で作成されたグループと連動します。ただし IoT の場合、通常これらのエンドポイントはそれらのデータベースとの相関関係がなく、目的またはデバイスのタイプに基づいて独立して編成されます。

読者へのヒント

SD-Access が登場する以前、SGT という略語はセキュリティ グループ タグを意味していました。SD-Access が登場したことで、将来的に SGT が他の目的に使用される可能性があることから、SGT は現在、拡張可能グループ タグを意味するようになっています。SD-Access より前に TrustSec に導入されていた、QoS とポリシーベースのルーティングが例として挙げられます。

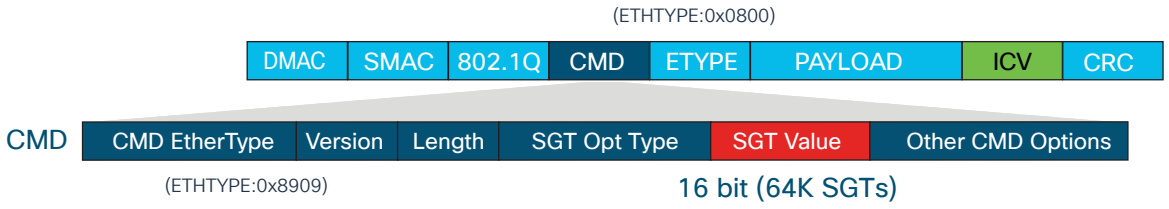
Cisco TrustSec の導入を集中管理する場合は、RADIUS ベースのアイデンティティ サービスと SGT ベースのポリシー作成用に、Cisco Identity Services Engine（ISE）が必要になります。SGT は Cisco ISE で作成され、集中管理されます。SGT の割り当ては、ネットワークに対して、802.1X、MAC Authentication Bypass（MAB）または WebAuth によって認証/認可した場合、あるいは Active Directory と Windows Management Instrumentation（WMI）を使用して認証/認可に成功した時点で行われます。認可が完了すると、ISE はそのデバイスに関連付けられている SGT を、接続しているネットワーク デバイスに RADIUS 経由で送信します。それにより、ネットワーク デバイスで、SGT に IP アドレスがマッピングされます。このマッピング情報は、デバイスの通信とポリシー適用に使用されます。Cisco Nexus® 7000 シリーズ スイッチを使用するレガシー データセンター内のサーバなど、動的な認証が適切でないか不可能であるデバイスの場合、SGT は、ポート、VLAN、サブネット、または個々の IP アドレスについて、Cisco TrustSec 対応スイッチおよびルータで手動で定義することもできます。

読者へのヒント

データセンターで TrustSec を使用する方法の詳細については、『TrustSec Data Center Segmentation Guide（TrustSec データセンター セグメンテーション ガイド）』[英語] を参照してください。

SGT は、Scalable-Group Tag Exchange Protocol（SXP）という pxGrid 経由の TCP ベースのプロトコルによって、IP アドレスと SGT のマッピング情報としてアドバタイズされるか、図 16 に示すように、イーサネット フレームに挿入される Cisco Metadata（CMD）というシスコ独自のフィールド内で 16 ビット値として送信されます。これはインライン タギングと呼ばれます。

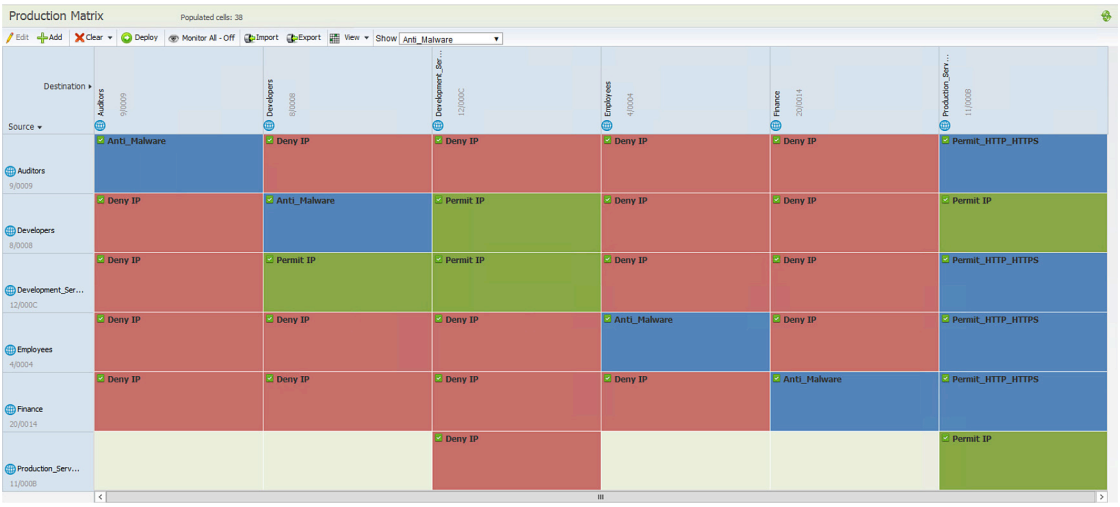
図 16. Cisco Metadata 内の SGT



インライン タギングは、Cisco TrustSec 対応スイッチとライン カードにおいて、ホップバイホップ方式で実行されます。スイッチが ISE からスタティック設定で IP-SGT マッピング情報を受け取るか、SXP 経由で学習したら、図に示す CMD をイーサネット フレームに挿入し、Cisco TrustSec 対応インターフェイスを通じてエンドポイントのトラフィックに転送します。アップストリームのスイッチに到達すると、CMD が抽出され、SGT が取得されます。この時点で、同じタグと合わせて宛先に転送されるか、タグに基づいてポリシーが適用されます。

これらの SGT に基づき、ISE でグループベースのポリシーを作成し、動的に配布することで、サポートするルータおよびスイッチで Security Group ACL（SGACL）を利用して、ポリシー適用に使用できます。図 17 に示すように、送信元と宛先に基づくマトリックスは、ISE でのポリシー作成に使用されます。さらに、Cisco 適応型セキュリティ アプライアンス（ASA）または Firepower NGFW などの Security Group Firewall（SGFW）、さらにサービス統合型ルータ（ISR）または ASR ルータの Cisco IOS® Zone-Based Firewall（ZBFW）では、SGT に基づいてローカルで作成されたファイアウォール ルールを使用して、ポリシーを決定できます。ルータおよびスイッチで設定された SGACL はステートレスであり、ファイアウォールを使用する場合にステートフル インスペクションは実行できません。

図 17. Cisco TrustSec ポリシー マトリックス



ポリシーは、イーサネット フレームに挿入されて送信されるか、SXP アドバタイズメントと宛先 IP-SGT マッピング情報により、送信元 SGT が取得される最初のネットワーク デバイスで適用されます。通常宛先のデバイスで適用されますが、送信元と宛先の間にあるデバイスで SXP またはスタティック マッピングを使用して IP-SGT マッピング情報が作成されている場合には、中間デバイスで行われる場合があります。

ポリシーが適用されるようにするには、ISE で設定される SGACL をネットワーク デバイスにダウンロードする必要があります。これらの SGACL を保存する際には、ローカル リソース（TCAM とメモリ）の制限があることを考慮して、対象の SGT に関するポリシーと、ネットワーク デバイス上のマッピング情報だけを ISE からダウンロードします。それにより、SGT マッピングがなされたデバイスを宛先とするトラフィックで使用されるポリシーだけがダウンロードされるため、ローカル リソースの消費が抑制されます。Cisco TrustSec で、ネットワークからの送信時にポリシーが適用されるのはそのためです。

VRF-Lite や MPLS とは異なり、Cisco TrustSec では、分離と制御を行う上で、複数の VLAN またはルーティング テーブルは必要ありません。すべての転送で必要なルーティング テーブルは 1 つだけであり、代わりに、グループ メンバーシップ、デバイスに割り当てられたそのグループの SGT、Cisco ISE によって集中管理されてネットワーク インフラストラクチャに配布されるグループベース ポリシーによって分離されます。

Cisco TrustSec と VRF は相互排他的ではなく、同時に使用することができます。Cisco TrustSec と VRF を同時に使用する場合は、VRF 間の分離によるマクロセグメンテーションが可能です。さらに VRF 内で Cisco TrustSec を使用することで、マイクロセグメンテーションが可能になります。

Cisco TrustSec インライン タギングは、ネットワーク接続に VRF-Lite を使用している場合にサポートされますが、Label Distribution Protocol と Cisco TrustSec の両方がインターフェイスで必要な MPLS 環境ではサポートされません。これは設定上の制限ではなく、アーキテクチャ上の制限です。標準の転送情報ベース（FIB）ではなく、ラベル転送情報ベースがネクストホップ処理に使用されるため、SGT とその IP との関連付けは学習されません。MPLS ネットワークでは、SXP を使用して、ネットワークの MPLS 部分に IP-SGT マッピング情報を伝播する必要があります。

読者へのヒント

Cisco TrustSec の詳細については、https://www.cisco.com/go/trustsec [英語] を参照してください。

TrustSec のプラットフォーム サポートの詳細については、「TrustSec Platform Support Matrix（TrustSec プラットフォーム サポート マトリックス）」[英語] を参照してください。

付録 B:リファレンス

セキュリティ グループ ファイアウォールを使用したアクセス制御:https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/access_control_using_security.pdf [英語]

APIC ポリシー モデル:https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731310.html [英語]

シスコのアーキテクチャ:https://www.cisco.com/c/ja_jp/solutions/intent-based-networking.html

シスコ インテントベース ネットワーキング ホワイト ペーパー:https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-09-intent-networking-wp-cte-en.pdf?oid=wpren006178 [英語]

SD-Access ボーダー ノードでのポリシー適用:https://communities.cisco.com/docs/DOC-77432 [英語]

SD-Access 設計ガイド:https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/software-defined-access/index.html および『Cisco Validated Design SD-Access Design Guide(SD-Access シスコ検証済みデザイン ガイド)』(https://www.cisco.com/c/ja_jp/solutions/design-zone/uc.html)

CCO の TrustSec シスコ コミュニティ:https://communities.cisco.com/community/technology/security/pa/trustsec [英語]

CCO の TrustSec:https://www.cisco.com/go/trustsec [英語]

TrustSec プラットフォーム機能マトリックス:https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/software-platform-capability-matrix.pdf [英語]

TrustSec システム速報:https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html [英語]

『TrustSec User-to-Data-Center Access Control Using TrustSec Deployment Guide(TrustSec を利用したユーザからデータセンターへのアクセス制御導入ガイド)』:https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2016/User-to-DC_Access_Control_Using_TrustSec_Deployment_April2016.pdf [英語]

『TrustSec User-to-Data-Center Access Control Using TrustSec Design Guide(TrustSec を利用したユーザからデータセンターへのアクセス制御設計ガイド)』:https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/User-to-DC_Access_Control_Using_TrustSec_Design_October2015.pdf [英語]

TrustSec:SXP および SXP リフレクタの使用方法:https://communities.cisco.com/docs/DOC-75763 [英語]

このガイドに関するコメントやご提案は、フィードバック フォームをご使用ください。

アメリカ本社
Cisco Systems, Inc.
San Jose, CA

アジア太平洋本社
Cisco Systems (USA) Pte. Ltd.
Singapore

ヨーロッパ本社
Cisco Systems International BV Amsterdam、
The Netherlands

シスコは世界各国に 200 ヵ所を超えるオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号については当社の Web サイト（www.cisco.com/go/offices/）をご覧ください。