検証済みソリューション：大学業界

改訂：2023 年 12 月 14 日

大学ソリューションの概要

このドキュメントの目的は、Cisco DNA Center と Cisco Software-Defined Access ソリューションを使用した大学での導入のガイダンスを示し、検証のための参考資料として提供することです。

スマートキャンパスと自動化、ハイブリッド学習スペース、セキュアな遠隔学習など、教育業界では大きな変化が起こっています。ネットワークに接続するエンドポイントの数が急増しており、学生や教職員が各自のデバイスをキャンパスに持ち込んでいます。大学の学生や教職員は、世界中の他の大学を訪れ、研究資料にすぐにアクセスできる必要があります。教育ネットワーク環境は、他の業界と同様に、強化されたネットワークサービス、シームレスなモビリティ、ネットワークの高可用性、および効率的なネットワーク管理を必要としています。また、大学のネットワークには、個人用サービス、ワイヤレス負荷の高いネットワーク、ワイヤレスモビリティに対応するセキュリティ強化など、特殊なニーズがあります。

教育業界のニーズを念頭に置いて、次のセクションでは、大学業界の主な考慮事項について説明します。

Bonjour 向け Cisco DNA サービス

Bonjour 向け Cisco DNA サービス は、ソフトウェア定義のコントローラベースのソリューションで開発され、ネットワーク全体に分散されたデバイスがレイヤ 3 ネットワーク境界を越えて Bonjour サービスをアドバタイズおよび検出できるようにします。分散サービス指向アーキテクチャは、ネットワークエッジにおけるサービスポリシーの適用ポイントでフラッド境界を分離し、エンドツーエンドのサービス管理を実現できるように設計されています。このソリューションは、モバイル印刷、画面共有、ファイル共有、および自宅と大学のネットワーク間でのその他のサービスについて、エンドユーザー体験を維持しながら、既存の複雑なエンタープライズ ネットワーク設計に完全にシームレスに統合します。

教育用ローミング（Eduroam）

Eduroam は、海外の教育機関を訪問する際に、研究者、教職員、および学生にネットワークアクセスを提供します。ユーザーは世界中のどこからでも Eduroam Wi-Fi ネットワークに接続し、所属する教育機関のログイン情報を使用して認証します。認証に成功すると、ビジターはすぐにネットワークにアクセスできるようになります。Eduroam は、ゲストサービスに代わるものとも見なされています。教育機関では、ゲストアクセスの認証と管理のオーバーヘッドがなくなるため、管理オーバーヘッドが大幅に削減されます。

個人所有デバイスの持ち込み（BYOD）

大学のキャンパスで個人デバイスが普及するにつれて、学生はこれらのデバイスを使用して、セキュリティで保護されたリソースやアプリケーションにアクセスし、日常のアクティビティを行っています。Cisco Identity Services Engine（ISE）は BYOD 機能を提供します。学生は、ネイティブ サプリカント プロビジョニングを実行するか、またはデバイスをデバイスポータルに追加して、個人デバイスをネットワークに追加できます。大学の管理者は、BYOD デバイスにポスチャポリシーを適用することで、ネットワークのセキュリティを確保できます。

マルチサイト リモート ボーダーを使用したゲストサービス

大学のネットワーク設計は、ほとんどのキャンパスネットワーク設計と非常によく似ています。大学は、ネットワークに同時に接続している何千人もの学生全員をサポートできる必要があります。学生と教職員以外に、ゲストユーザーがネットワークにアクセスする必要もあります。ビジター、イベント参加者などには、ゲストアクセスが必要です。

ほとんどのゲストは、キャンパス ネットワーク サービスにワイヤレスでアクセスし、公開されているサービスのみに制限されます。ゲスト用に別の仮想ネットワーク（VN）を設定することで、アクセスは通常、DMZ を介したインターネットに制限されます。大学ではサイトの数が多い場合があります。設計を最適化するには、複数のサイトにまたがるすべてのゲスト仮想ネットワークを DMZ で終端します。この設計は、アンカー VN 機能（マルチサイト リモート ボーダー機能とも呼ばれます）を使用して実現されます。この機能により、VN ごとに出力設定が可能になります。複数のサイトにまたがるすべてのゲストトラフィックを 1 つの VN に収容し、共通のリモートボーダーで終端できます。

サービスとネットワークの復元力

大学のネットワークでは、ダウンタイムは許容されません。そのため、これらのネットワークには、厳密なネットワークレベルおよびサービスレベルの復元力が必要です。ネットワークレベルの復元力は、デュアル ファブリック ボーダー ノード、デュアル ファブリック コントロール プレーン ノード、デュアルアンカーボーダーおよびコントロールプレーンノード、デュアル ワイヤレス コントローラ、ハードウェアスタックを備えたファブリックスイッチ、デュアル ファブリック トランジット コントロール プレーン ノード（該当する場合）を含む堅牢なファブリックネットワーク設計で実現できます。サービスレベルの復元力は、Cisco DNA Center 3 ノードクラスタ、および複数のポリシー管理ノード（PAN）、モニタリングノード（MNT）、アクティブとスタンバイの Platform Exchange Grid（pxGrid）、ポリシーサービスノード（PSN）を備えた分散型 Cisco ISE クラスタで実現されます。

ネットワーク管理と可視性

ネットワーク管理者は、教育機関ネットワークの動的なニーズに迅速に対応するために、ネットワークを効率的に管理およびモニターできる必要があります。テレメトリを使用して、ネットワーク関連やセキュリティ関連のリスクをプロアクティブに予測し、ネットワーク、デバイス、アプリケーションのパフォーマンスを向上させる必要があります。Cisco DNA アシュアランス は、Cisco AI Network Analytics を使用して、テレメトリデータを収集し、ネットワークデバイスのパフォーマンスと正常性をモニターし、検出された問題にフラグを付け、修復手順を提示します。

Cisco DNA アシュアランス を使用すると、管理者は、ネットワークデバイスと接続されたエンドポイント（有線とワイヤレスの両方）の全体的な正常性をモニターできます。また、ネットワークおよびアプリケーション アシュアランスを使用して、デバイス、エンドポイント、アプリケーションの個々の正常性を確認できます。この詳細レベルの 360 度分析により、管理者は、ネットワーク内のエンドポイントの接続の問題など、ネットワーク要素が抱えている個々の問題を特定できます。

セキュリティとネットワークのセグメンテーション

教育機関は、他の業界と同様に、学生や教職員の情報、大学の研究データ、財務情報などを保護する必要があります。大学は、必要なセキュリティ構造を実現し、重要なデータと共通データを分離するために、ネットワークを効率的に展開およびセグメント化する必要があります。

Cisco DNA Center と Cisco ISE は、Cisco 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、Cisco 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。

Cisco SD-Access は、マクロセグメンテーションを使用することで、データプレーンとコントロールプレーンを完全に分離するニーズに対応します。ユーザーとデバイスを作成して、異なるオーバーレイ仮想ネットワーク（VN）に配置することで、大学における完全なデータの分離を実現し、さまざまな部門やユーザーにセキュリティを適用できます。

WAN の障害などが原因で、ファブリックエッジが設定された RADIUS サーバーに到達できない状況に対処するために、クリティカル VLAN が追加されました。この障害の発生中は、新しく接続するエンドポイントの認証はできません。クリティカル VLAN 機能はフォールバック VLAN を作成します。これにより、エンドポイントは正常にオンボーディングし、一時的な障害時に緊急サービスなどのアクセスのレベルを受信できます。

Cisco SD-Access は、グループベースポリシー（GBP）にスケーラブルグループタグ（SGT）によるマイクロセグメンテーションを使用して、同じ VN 内のエンドポイント間のデータプレーンの分離にさらに細かく対応できます。IT 管理者は、Cisco DNA Center でグループを作成し、ユーザー、デバイス、および IoT デバイスをロールに基づいてグループに分けることができます。IT 管理者は、これらのグループが相互に、またはグループ間でどのように相互作用するかを制御するポリシーを定義できます。

Cisco AI エンドポイント分析

最新のセキュリティ脅威は、企業ネットワークデータ全体を悪用するための脆弱な侵入ポイントを探します。侵入ポイントが侵害されると、わずか数秒でデバイスからデバイスへと侵害が拡大していきます。大学のネットワークには、複数の場所にまたがって、さまざまなデバイスが存在するため、ネットワーク上のすべてのデバイスを検索して識別するのは時間のかかる面倒な作業です。Cisco AI エンドポイント分析 では、タイプ、製造元、モデル、OS タイプ、通信プロトコル、およびポート別にデバイスを識別することで、この問題に対処します。パッシブ ネットワーク テレメトリ モニタリングとディープ パケット インスペクションを使用して、Cisco DNA Center はネットワークをスキャンし、管理者がこれらの属性に基づいてデバイスを分類するためのプロファイリングルールを作成できるようにします。機械学習と組み合わせることで、Cisco DNA Center はスプーフィングされたエンドポイントを検出し、管理者がスプーフィングされたエンドポイントに対して効果的なアクションを実行できるようにします。

Cisco AI エンドポイント分析 は、複数の方法を使用して悪意のあるエンドポイントを検出します。また、プロファイルラベルの変更、NAT モードの検出、同時 MAC アドレス識別、ポスチャ、認証方式、および機械学習を使用して、偽のエンドポイントを識別してフラグを立てます。全体的な信頼スコアは、すべてのエンドポイントに対して生成されます。信頼スコアは、複数のリスクスコアの加重平均です。信頼スコアが低いほど、エンドポイントのリスクが高いことを意味します。

さらに、Cisco DNA Center はエンドポイントの分類属性を Cisco ISE と共有します。アイデンティティベースの認証で新しいデバイスがオンボーディングされると、製造元とタイプに基づいて自動的に識別され、該当するグループに追加されます。セキュリティポリシーの定義と適用は、個々のエンドポイントではなくグループに適用した方が簡単です。グループベースポリシーは、エンドポイントによるセキュリティ侵害などの新しい状況に合わせてさらに簡単に編集でき、ネットワーク全体にグローバルに適用できます。

ファブリック外のレイヤ 2 ゲスト終端

お客様は、ネットワークを使用しているゲストに対してレイヤ 2 レベルのトラフィック インスペクションを必要とする場合があります。この要件は、すべてのゲストトラフィックのファーストホップがファブリックの外部にある必要があることを意味します。この実装は、Cisco DNA Center と手動のデバイス設定の組み合わせを使用して実現されます。ゲストトラフィックは VXLAN でカプセル化され、ファブリックを通過しますが、ゲストトラフィックのファーストホップまたはゲートウェイはファブリックの外部にあります。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアでテストされています。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。

ロール	モデル名	ハードウェア プラットフォーム	ソフトウェア バージョン	ソフトウェア バージョン
Cisco DNA Center アプライアンス	DN2-HW-APL-XL	Cisco DNA Center 3 ノード ハイ アベイラビリティ クラスタ	2.3.3.7	2.3.5.4
アイデンティティ管理、RADIUS サーバー	ISE-VM-K9	Cisco Identity Services Engine 仮想アプライアンス	3.0 パッチ 6 3.1 パッチ 3	3.0 パッチ 6 3.1 パッチ 3
Cisco SD-Access ファブリック コントロール プレーン ノード	ASR1001-X	Cisco 1000 シリーズ アグリゲーション サービス ルータ	17.6.4、17.9.2a	17.6.5、17.9.4
	C9500-24Y4C C9500-24Q	Cisco Catalyst 9500 シリーズ スイッチ	17.6.4、17.9.3	17.6.5、17.9.4
Cisco SD-Access ファブリック ボーダー ノード	ASR1006-X（RP3）	Cisco 1000 シリーズ アグリゲーション サービス ルータ（ASR）プロセッサ	17.6.4、17.9.2a	17.6.5、17.9.4
	C9500-24Y4C C9500-40X C9500-24Q	Cisco Catalyst 9500 シリーズ スイッチ	17.6.4、17.9.3	17.6.5、17.9.4
Cisco SD-Access ファブリック エッジ ノード	C9300-48P C9300-24P	Cisco Catalyst 9300 シリーズ スイッチ	17.6.4、17.9.3	17.6.5、17.9.4
Cisco SD-Access ワイヤレスコントローラ	C9800-80 C9800-CL	Cisco Catalyst 9800-80 ワイヤレスコントローラ Cisco Catalyst 9800-CL ワイヤレスコントローラ	17.6.4、17.9.3	17.6.5、17.9.4
Cisco SD-Access 拡張ノード	WS-C3560CX-8XPD-S Cisco IE-4000	Cisco Catalyst 3560-CX Cisco IE 4000 シリーズ	15.2(7)E3	15.2(7)E3

ソリューションの導入例のシナリオ

大学業界のプロファイルについて、図 1 に示すトポロジを使用して次のユースケースを実施しています。

Cisco DNA Center を使用するインテントベース ネットワーク

管理者は次のことを実行できます。

- グローバルネットワーク階層とグローバルおよびサイトレベルのネットワーク設定を設計します。
- デバイスを自動的にプロビジョニングします。
- 冗長性と拡張性を考慮して、デュアルボーダーとデュアル コントロールプレーン ノードを備えたメイン キャンパス ネットワークを展開します。
- 次のタイプの新しいデバイスをオンボーディングすることで、メインキャンパスとサテライトキャンパスのサイトを柔軟に拡張します。
  - ファブリックエッジは、ゼロタッチ プラグアンドプレイの LAN 自動化を使用するか、既存の IP/MPLS インフラストラクチャを使用してアンダーレイの到達可能性を確保します。
  - クラシック拡張ノードをゼロタッチ プラグアンドプレイを使用して IoT デバイス接続用のファブリックに追加します。
  - ポリシー拡張ノードを SGT を直接サポートして拡張トラフィックが適用されたファブリックに追加します。
- 分散キャンパスサイトを、共有のデータセンターやインターネットサービス用の Cisco SD-Access トランジットを使用して接続します。

機密性の高い教育機関データを保護する多層セキュリティ

管理者は次のことを実行できます。

- 学生、教職員、ゲスト、IoT、キャンパスデバイスを適切な論理ネットワークにセグメント化し、ネットワーク内の脅威の移動を制限します。
- 不正アクセスを防ぐために、有線およびワイヤレスのエンドポイントに対してクローズド認証オンボーディング（dot1x）または MAC 認証バイパス（MAB）を有効にします。
- セキュリティを強化します。Cisco DNA Center の管理者は信頼できる CA FQDN ベースの証明書を適用できます。
- グループを作成し、ユーザーやエンドポイントを（アイデンティティに基づいて）グループに分け、グループ間のトラフィックを制御するグループベースのポリシーを定義します。
- 監査ログを使用して Cisco DNA Center のアクティビティをモニターします。監査ログには、発生したシステムイベント、発生した時刻と場所、開始したユーザーが記録されます。
- Cisco DNA Center へのアクセス権限が異なる詳細なロールベースのユーザーを作成します。

Eduroam

管理者は次のことを実行できます。

- Cisco DNA Center を使用して、WPA2-Enterprise 対応で 802.1X を使用する Eduroam Wi-Fi SSID をプロビジョニングします。
- 外部 Eduroam サーバーからの認証要求を処理し、外部ユーザー認証要求を Eduroam サーバーに転送するように Cisco ISE を設定します。
- 海外の大学の外部ユーザーが、ローカルキャンパスの Eduroam SSID に接続し、認証が成功したときにネットワークにアクセスできるようにします。
- 現地の大学から旅行中のユーザーが、海外の大学の Eduroam SSID に接続してネットワークにアクセスできるようにします。

Cisco Wide Area Bonjour

管理者は次のことを実行できます。

- SDG エージェントとネットワーク情報を設定して、サービスルーティングを有効にします。
- サービスポリシーベースの ZeroConf サービス管理と、Cisco Wide Area Bonjour アプリケーションを使用したエンドユーザーデバイスからの共通 Bonjour サービス配信を設定します。
- 大学ネットワークのユーザーが、レイヤ 3 ドメイン間での印刷や画面共有などの Bonjour サービスを利用できるようにします。
- Cisco Wide Area Bonjour ダッシュボードを使用して、サブドメインレベルのサービス数およびポリシーの動作ステータスごとの SDG エージェント統計を確認します。

個人所有デバイスの持ち込み（BYOD）

管理者は次のことを実行できます。

- 大学ネットワーク内の個人デバイスに特権アクセスを付与するように Cisco ISE を設定します。
- Cisco DNA Center を使用して BYOD エンドポイントの WPA-2 エンタープライズ SSID をプロビジョニングします。
- 学生または教職員が自分の個人デバイスを大学ネットワークに接続し、特権アクセスを取得できるようにします。
- Cisco ISE のデバイスポータルを使用して、BYOD エンドポイントを管理します。

Cisco AI エンドポイント分析

管理者は次のことを実行できます。

- 分類と動作モデルの学習に基づいてスプーフィングされたエンドポイントを検出するように Cisco AI エンドポイント分析 を設定します。
- 侵害されたエンドポイントを検出してフラグを立てるように Cisco DNA Center を設定します。設定された影響パラメータに基づいて、エンドポイントの包括的な信頼スコアが計算されます。

- 信頼スコアと脅威のタイプを表示し、修正処置を実行するか、悪意のあるエンドポイントを隔離します。

マルチサイト リモート ボーダーを使用したゲストサービス

管理者は次のことを実行できます。

- ゲスト VN を設定し、複数のサイトで共有します。この VN は、アンカーサイトのリモートボーダーでアンカーできます。ゲストトラフィックはゲスト VN 内で分離され、インターネットアクセスのためにアンカーリングボーダーにトンネリングされます。
- アンカーサイトと継承されたファブリックサイト全体でゲストユーザーをオンボーディングするように、共通ゲストサブネットを設定します。
- Cisco DNA Center を使用して CWA でゲスト SSID をプロビジョニングします。ゲスト SSID はすべてのサイトで共通です。
- ネットワーク障害が発生した場合に冗長性を提供するために、物理的に異なる場所にデュアルアンカーボーダーとコントロールプレーンを備えたアンカーサイトを実装します。

サービスとネットワークの復元力

管理者は次のことを実行できます。

- デュアル Cisco SD-Access ボーダー、デュアル コントロール プレーン ノード、ボーダー/エッジスタック、アンダーレイのポートチャネル、およびトランジットネットワークのデュアル トランジット コントロール プレーンにより、ネットワーク全体で高可用性を実現します。ネットワーク障害のフェールオーバーとリカバリで、トラフィックフローがまったく中断されないか、中断が最小限にとどまります。
- 既存のアプリケーション、トラフィック、ユーザーへの影響を最小限に抑えて、デバイスやリンクの障害から自動的に回復可能なネットワークを実装します。
- 3 ノード ハイ アベイラビリティ モードで Cisco DNA Center を設定します。これにより、サービスまたはノードに障害が発生した場合、Cisco DNA Center クラスタは管理者の介入なしでリカバリできます。
- PAN、PSN、pxGrid サービスのフェールオーバーを備えた分散型展開モデルで Cisco ISE を設定します。
- Cisco DNA Center 設定とデータをオンデマンドまたはスケジュールでバックアップします。バックアップファイルを Cisco DNA Center に復元して、以前の Cisco DNA Center 設定を再開できます。

シンプルな管理

管理者は次のことを実行できます。

- Cisco DNA Center により、IP、ソフトウェアリリース、プロビジョニングステータス、インベントリインサイトなどのデバイス情報を使用して、デバイスインベントリを集中管理します。
- 組織横断の VN を作成して、一貫したマクロセグメンテーションを実現します。
- 単一の VN に複数の SGT を適用し、VN 内にマイクロ セグメンテーション トラフィック用のグループベースのアクセスポリシーを作成します。

- VNの追加/削除機能を使用して新しいユーザーグループを追加または削除し、IPゲートウェイをVNに関連付けまたは関連付け解除します。
- Cisco DNA Centerのソフトウェアイメージ管理（SWIM）機能を使用して、スイッチ、ルータ、およびワイヤレスコントローラを選択したゴールデンイメージにアップグレードします。
- 拡張マルチサイト環境でVLANの割り当ての柔軟性を確保するように、サイトボーダーのレイヤ3ハンドオフのVLAN消費と最適化を設定します。

Cisco DNAアシュアランスと分析を使用したネットワークとクライアントのモニター

管理者は次のことを実行できます。

- Cisco DNAアシュアランスを使用してネットワークの正常性をモニターし、ネットワークの問題を特定します。Cisco DNAアシュアランスは、リンクのダウン、APのダウン、スイッチスタックメンバーのダウンなど、さまざまなネットワーク障害に起因する問題を報告できます。
- Cisco DNAアシュアランスを使用して有線クライアントとワイヤレスクライアントの正常性をモニターし、クライアントのオンボーディングの問題を特定します。
- 100,000の同時エンドポイントと250,000の一時エンドポイントを表示するCisco DNAアシュアランスチャートを使用して、多数のワイヤレスエンドポイントをモニターします。
- Cisco DNAアシュアランスで不正APを表示し、不正APレポートを生成します。

ファブリック外のレイヤ2ゲスト終端

管理者は次のことを実行できます。

- Cisco DNA Centerを使用してゲストネットワークを設定します。
- デバイス設定を手動でいくつか変更するだけで、レイヤ2レベルのトラフィック検査用にファブリック外部のゲストトラフィックを終端します。

ソリューション環境

ソリューションテスト環境には、トポロジとスケールの両方が含まれます。

トポロジ

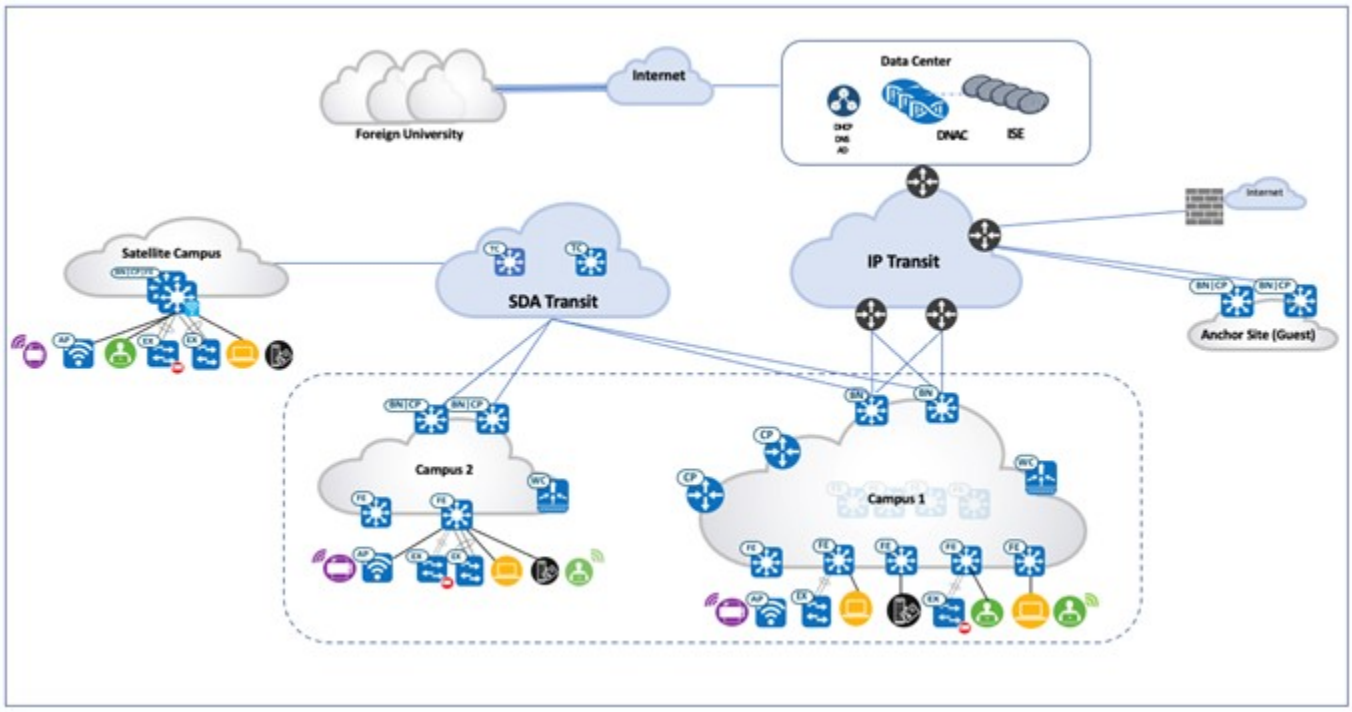
大学業界向けテストトポロジには、大規模メインキャンパスサイト、中規模キャンパスサイト、アンカーサイトぞれぞれ1つを管理するための3ノードCisco DNA Centerクラスタが含まれています。Cisco SD-Accessトランジットは、これらの分散キャンパスを接続するために展開されます。次の図は、大学業界向けソリューションのテストベッドの論理トポロジを示しています。

テストベッドのセットアップには、次のコンポーネントがあります。

- Campus 1サイトには、デュアルボーダー、専用のデュアルコントロールプレーンノード、デュアルWLC、1000のファブリックエッジがあります。

- Campus 2 サイトには、デュアル共存ボーダーおよびコントロールプレーンノード、WLC、ファブリックエッジ、拡張ノードがあります。
- サテライトキャンパスサイトは、組み込み WLC と拡張ノードを備えたハードウェアスタック上の一体型ファブリックを備えた小規模サイトです。
- アンカーサイトには、デュアル共存アンカーボーダーおよびコントロールプレーンノードがあり、複数のファブリックサイトにアンカーゲストサービスを提供します。
- SD-Access トランジットは、デュアル トランジット コントロール プレーン ノードで実装されます。大規模キャンパスサイトボーダーは、SD-Access トランジットを介して他のキャンパスサイトにインターネットアクセスを提供するように設定されています。

図 *1*: ソリューションのテスト論理トポロジ



スケール

次の表に、テストされたスケール値を示します。ハードウェアキャパシティについては、Cisco DNA Center のデータシートを参照してください。

カテゴリ	値
デバイス インベントリ	2000
ファブリックサイトごとのデバイス	600
建物とフロア	3000

カテゴリ	値
ファブリックサイトごとの VN	64
ファブリックサイトごとの IP プール	500
ファブリックサイトごとの WLC	2
ファブリックサイト	4
インベントリの AP	8000
エンドポイント	100,000（ワイヤレス 80,000、有線 20,000）
SSID	8
SDG	25
Bonjour サービスインスタンス	16000

ソリューションの重要事項

このセクションでは、大学業界プロファイルのソリューションの検証に関する主なテクニカルノートについて説明します。

Cisco Wide Area Bonjour

Cisco Wide Area Bonjour アプリケーションは、コントローラベースのソフトウェアデファインド ソリューションです。デバイスがレイヤ 2 ドメイン全体で Bonjour サービスをアドバタイズおよび検出できるようにし、それらのサービスをさまざまな有線およびワイヤレス企業ネットワークに適用できるようにします。Cisco Wide Area Bonjour アプリケーションは、大規模なセキュリティ、ポリシーの適用、サービス管理に関連する問題にも対処します。この新しい分散型アーキテクチャは、mDNS フラッド境界を排除して、ユニキャストベースのサービスルーティングに移行するように設計されており、サービスポリシー適用ポイントを提供し、Bonjour サービスの管理を可能にします。Cisco Wide Area Bonjour アプリケーションを使用すると、既存のネットワーク設計や設定を変更することなく、既存の企業環境に新しいサービスをシームレスに導入できます。

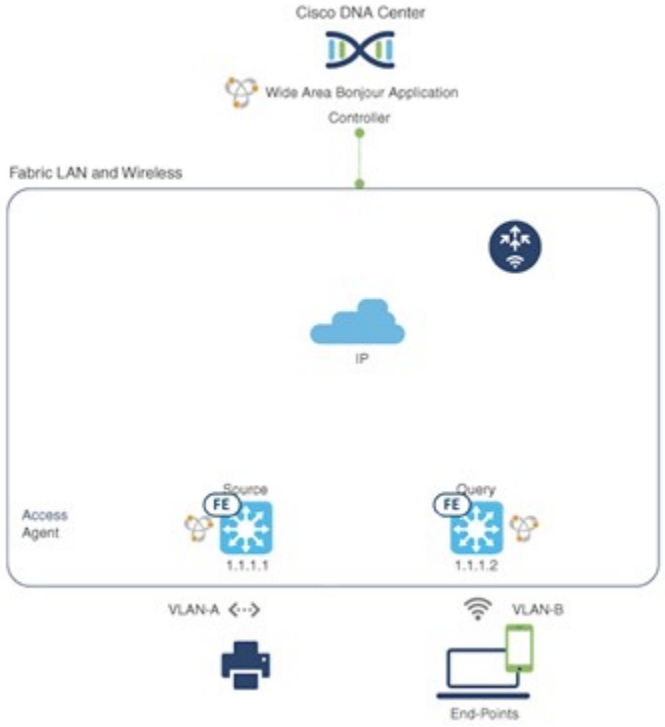
Cisco Wide Area Bonjour は、Cisco DNA Center のデフォルトアプリケーションではありません。このアプリケーションは、シスコのカタログサーバーからダウンロードしてインストールします。Cisco Wide Area Bonjour アプリケーションを正常にインストールしたら、Cisco DNA Center ホームページからメニューアイコンをクリックし、[Tools] をクリックしてアクセスできます。

Cisco DNA Center の Cisco Wide Area Bonjour アプリケーションは、Service Discovery Gateway（SDG）エージェントスイッチやサービスピアデバイスに設定をプッシュしません。SDG エージェントとサービスピアは、手動で設定するか、Cisco DNA Center のテンプレートエディタで作成されたテンプレートを使用して設定する必要があります。

このセクションでは、ファブリックエッジスイッチがファブリック対応ワイヤレスネットワークを介してリモート接続されたワイヤレスユーザーにプリンタサービスを提供する大学における Cisco Wide Area Bonjour の使用例を示します。ワイヤレスエンドポイントは、別の建物またはキャンパスサイトに存在するプリンタサービスを検出できます。学生ま

たは教職員は、プリンタが設置されている建物に物理的にいなくても、遠隔地から印刷サービス要求を開始できます。次の図に Cisco Wide Area Bonjour ソリューションの例を示します。このネットワークトポロジには、Cisco SD-Access LAN とファブリックモードのワイヤレスネットワークがあります。仮想ネットワーク環境内に Bonjour の送信元とレシーバがあります。

図 *2 : Cisco Wide Area Bonjour* ソリューション



最初のステップは、IP ネットワーク全体の信頼できる Cisco Catalyst SDG エージェントスイッチ間でサービス情報を動的に検出し配信することを Cisco Wide Area Bonjour アプリケーションに許可するグローバルサービスフィルタを実装することです。

[Create Service Filter]：Cisco Wide Area Bonjour アプリケーションから、管理者がサービスフィルタを追加するサービスドメインを選択し、アナウンスとクエリを許可するサービスタイプを選択します。管理者は、作成後にこの設定を編集、有効化、または無効化できます。

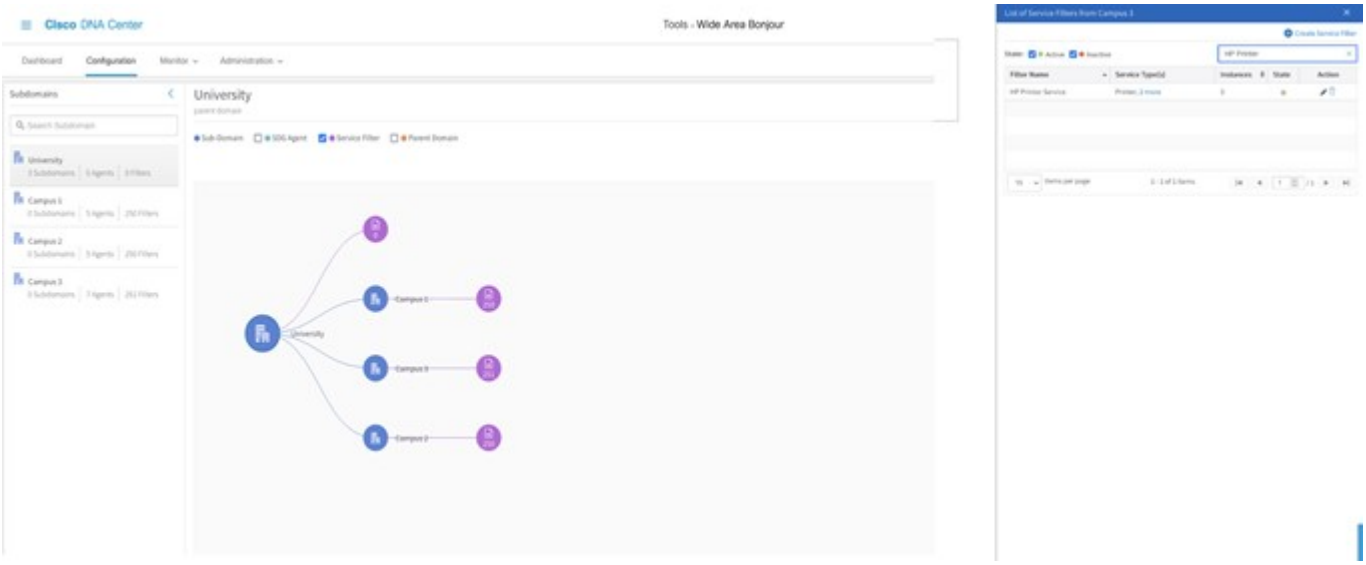
[Configure Source SDG Agents]：Cisco Wide Area Bonjour アプリケーションから、サービスをアナウンスする SDG エージェントと VLAN を選択します。管理者は、IPv4 または IPv6 ネットワークのサービスを有効または無効にすることができます。

[Configure Query SDG Agent]：Cisco Wide Area Bonjour アプリケーションから、サービス（プリンタ）のクエリを受信する SDG エージェントと VLAN を選択します。管理者は、IPv4 または IPv6 ネットワークのサービスを有効または無効にすることができます。

（注） Cisco Catalyst 9800 シリーズ WLC でグローバル ワイヤレス マルチキャスト モードを有効にする必要があります。Cisco WLC およびアクセスポイントは、デフォルトで、ワイヤレス ネットワーク インフラストラクチャと有線ネットワーク インフラストラクチャ間でレイヤ2またはレイヤ3のマルチキャスフレームを転送しません。

サービスフィルタのステータスが緑色の場合、ポリシーはアクティブです。ユーザーのラップトップが VLAN-B の任意のリモートロケーションからオンボーディングすると、VLAN-A のプリンタサービスを検出して使用できます。次の図は、Cisco DNA Center の Cisco Wide Area Bonjour ダッシュボードを示しています。

図 *3 : Cisco DNA Center の Cisco Wide Area Bonjour ダッシュボード*



Eduroam

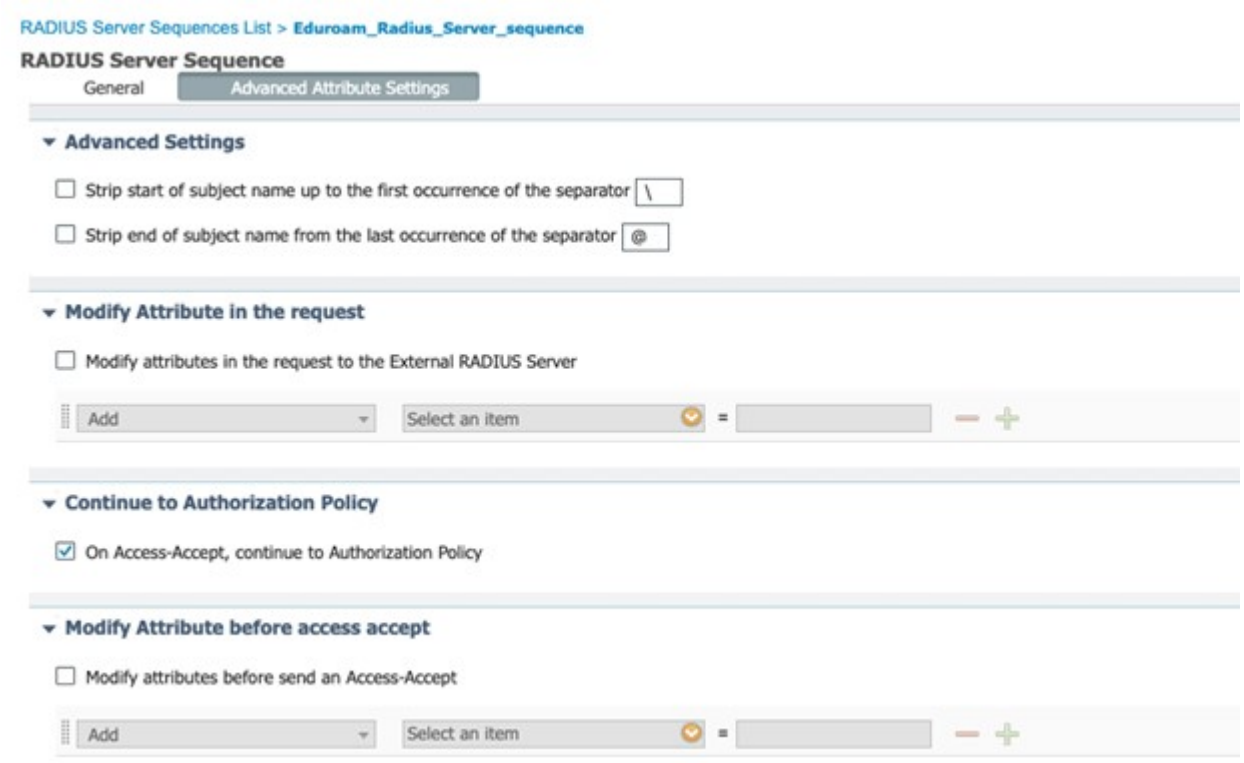
Eduroam は、研究および教育向けのグローバル ワイヤレス ネットワーク アクセス サービスです。Eduroam は、海外の教育機関を訪問する際に、研究者、教職員、および学生にネットワークアクセスを提供します。Eduroam サービスは、認証方式および参加 RADIUS サーバーの階層型システムとして IEEE 802.1X を使用します。所属教育機関および海外の教育機関の RADIUS サーバーを、参加 Eduroam サーバーのネットワークに登録する必要があります。

学生は世界中のどこからでも Eduroam Wi-Fi ネットワークに接続し、所属教育機関のログイン情報を使用して認証します。インターネットやその他のリソースへのアクセスの承認は、訪問先の教育機関によって処理されます。

Eduroam Wi-Fi SSID は WPA2-Enterprise 対応になっており、802.1X は Cisco DNA Center を使用してプロビジョニングされます。Eduroam の実装の設定は、Cisco ISE と Cisco DNA Center の両方で行う必要があります。Eduroam ポリシーセットと外部 RADIUS サーバーの設定は、Cisco ISE で行います。図 4 と図 5 に、Eduroam 外部サーバー設定を示します。

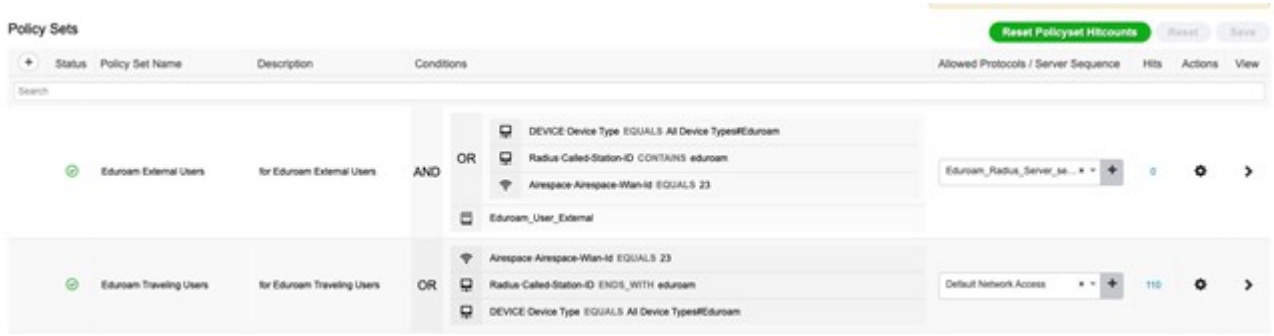
図 *4 :* 外部 ***RADIUS*** サーバー：設定 *1*

図 *5 :* 外部 *RADIUS* サーバー：設定 *2*



次の図は、Eduroam ポリシーセットの設定を示しています。

図 *6 : Cisco ISE* での *Eduroam* ポリシーセットの設定



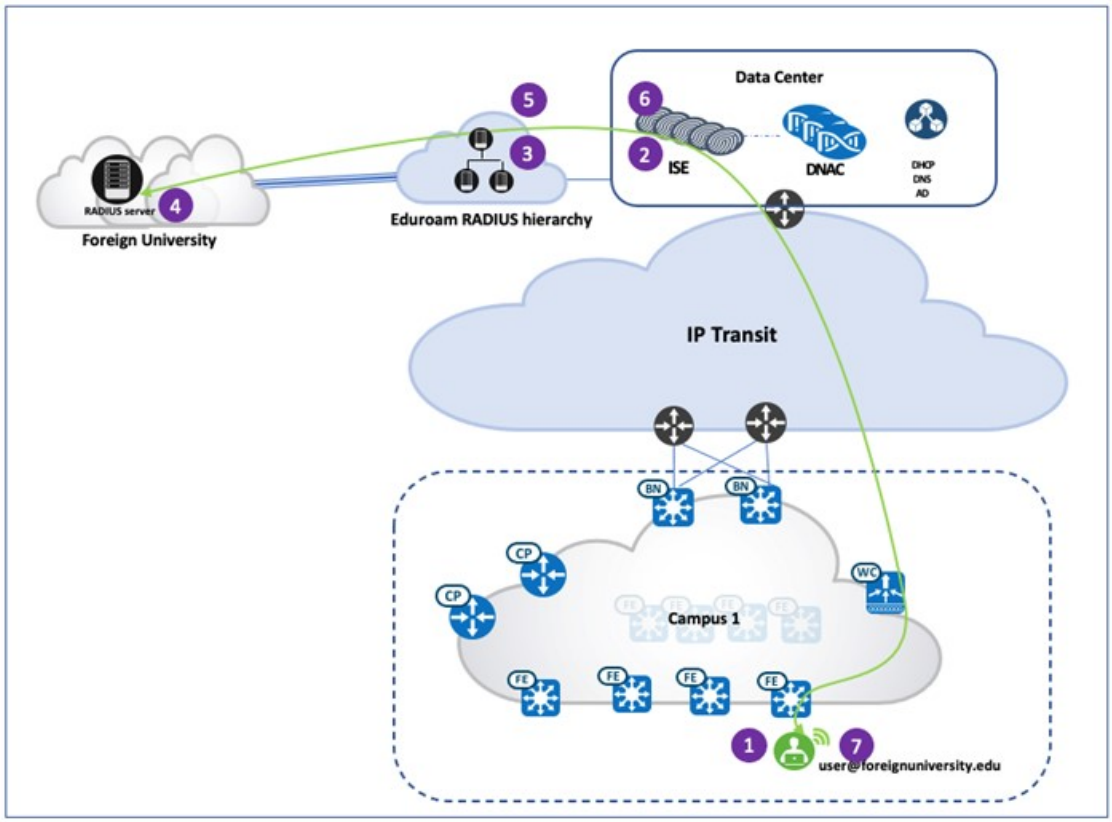
次の図は、Cisco DNA Center での Eduroam SSID の設定を示しています。

図 *7 : Cisco DNA Center* での *Eduroam SSID* 設定

Eduroam には、次の 2 つの主な使用例があります。

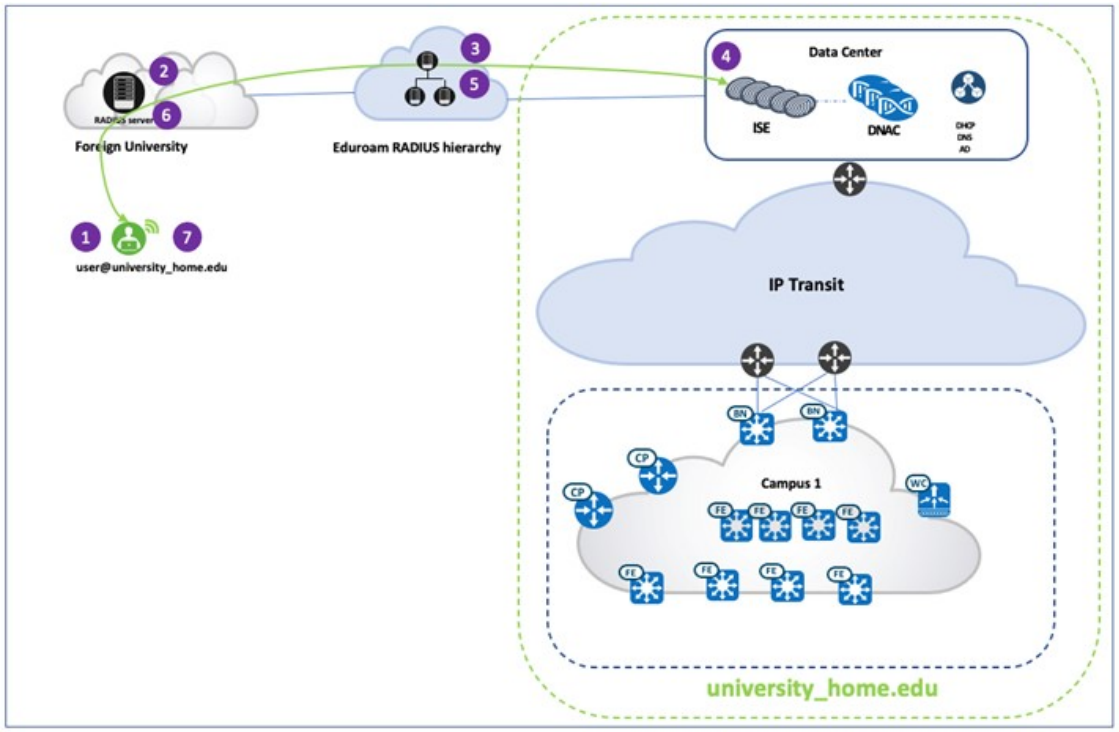
- **外部ユーザー**：このシナリオでは、学生または教職員は海外の大学に所属し、ローカルキャンパスにアクセスします。ユーザーはその Eduroam SSID に接続し、所属教育機関のログイン情報を入力します。認証要求は Eduroam サーバーにプロキシされ、次にその要求がユーザーの所属教育機関に転送されます。認証に成功すると、ユーザーはネットワークアクセスを許可されます。次の図に、認証フローを示します。

図 *8 :* 外部ユーザーの認証フロー



- **旅行中のユーザー**：このシナリオでは、学生または教職員は教育機関に所属していますが、物理的には海外の大学キャンパスにいます。このユーザーが海外の大学の Eduroam SSID に接続すると、認証要求が Eduroam RADIUS サーバーに送信され、次にその要求がユーザーの所属教育機関に転送されます。認証に成功すると、所属教育機関の RADIUS サーバーは Eduroam サーバーに「Access Accept」応答を送信し、Eduroam サーバーはこの応答を海外の大学に転送します。ユーザーは認証され、海外の大学でネットワークアクセスを取得します。次の図に、認証フローを示します。

図 *9:* 旅行中のユーザーの認証フロー



個人所有デバイスの持ち込み（BYOD）

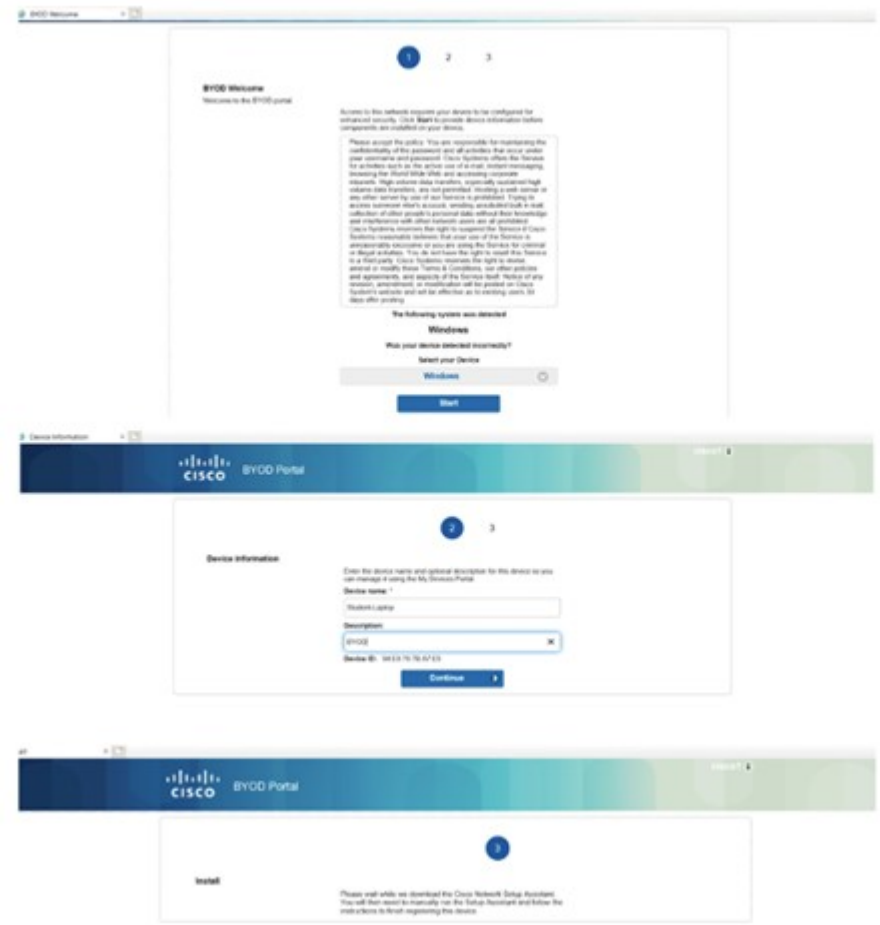
Cisco ISE は、学生や教職員がネイティブ サプリカント プロビジョニングを実行するか、デバイスをデバイスポータルに追加することで、個人デバイスをネットワークに追加できる Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）機能を提供します。大学の管理者は、ネットワークにアクセスするデバイスが安全であり、ジェイルブレイクやルート化されていないことを確認できます。ネットワークにアクセスするデバイスは、承認され、ポリシーに適合している場合にのみ、識別され、接続が許可されます。管理者は、ユーザー、デバイス、およびネットワーク上で実行されているアプリケーションを可視化できます。

シングル SSID BYOD では、エンドポイントがセキュアな WLAN に関連付けを行うと、オンボーディングされます。その後、エンドポイントが自動的に再接続すると、同じ WLAN を介してフルネットワークアクセスが付与されます。Cisco ISE BYOD 設定の主要なコンポーネントは次のとおりです。

- [Client Provisioning Policy]：このポリシーを使用して、エンドポイントタイプまたはユーザーグループに基づいて、関連付ける BYOD プロファイルを制御します。BYOD プロファイルには、証明書テンプレート、SSID 名、プロキシ設定などが含まれます。
- [Authentication and Authorization Policy]：このポリシーを使用して、ユーザーが BYOD フローを通過するときにユーザーに表示されるポータルを制御します。また、ユーザーの認証方法と、BYOD フローを通過するために必要なネットワークまたは SSID も指定します。
- [Endpoint Onboarding]：エンドポイントは複数のアクションを実行する必要があります。これらのアクションには、BYOD ポータルを介した正しい Cisco ISE ノードとの通信の開始、デジタル証明書ペアの作成、証明書署名要求の送信、ネットワークプロファイルの設定が含まれます。Windows の場合、Cisco ISE はサプリカント プロビジョニ

ング ウィザード（SPW）とも呼ばれる Network Setup Assistant（NSA）を利用して、ユーザーの BYOD フローを容易にします。エンドポイントがオンボーディングフローを完了すると、Cisco ISE は NSA をダウンロードしてインストールするようにユーザーに指示します。これによって、ユーザーは手順に沿って BYOD プロセスを完了できます。新しいバージョンの Windows が継続的に市場に導入されているため、管理者は Cisco ISE の NSA を定期的に更新して、新しい OS のサポートを確保する必要があります。次の図は、Windows 10 ラップトップでの BYOD オンボーディングを示しています。

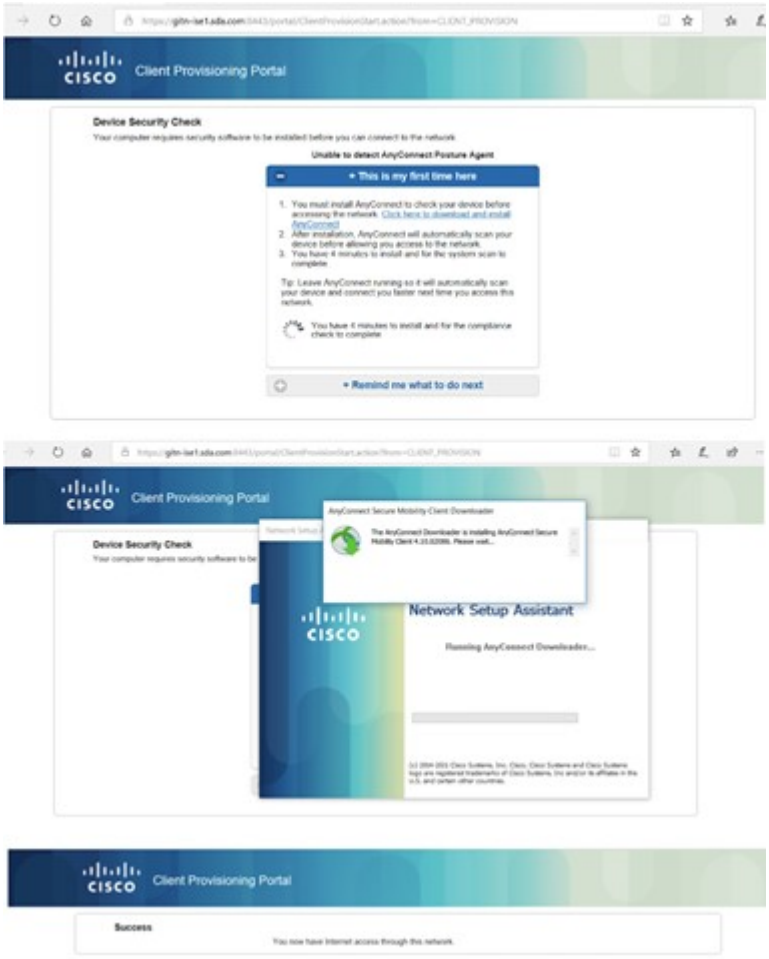
図 *10 : BYOD* オンボーディング ワークフロー



- [Posture Policy]：ポスチャは、Cisco ISE のサービスです。ポスチャを使用すると、ネットワークへの接続を許可する前に、エンドポイントのコンプライアンス（ポスチャとも呼ばれる）をチェックできます。Cisco ISE AnyConnect ポスチャエージェントなどのポスチャエージェントは、エンドポイントで実行されます。クライアント プロビジョニング サービスは、エンドポイントが適切なポスチャエージェントを受信できるようにします。

  エンドポイントがコンプライアンスに対応し、正常にオンボーディングされると、ポータルはユーザーにフルアクセスが付与されたことを通知します。Cisco ISE がエンドポイントを BYOD デバイスとして登録している間、ユーザーはブラウザを開いて他の接続先に移動できます。次の図は、クライアント プロビジョニング ワークフローを示しています。

図 *11* : クライアント プロビジョニング ワークフロー



マルチサイト リモート ボーダーを使用したゲストサービス

大学のキャンパス管理者は、多くの場合、すべてのキャンパスサイトで広範なゲストサービスを管理する必要があります。通常、ゲストユーザー（個々のファブリックサイトにバインドされます）はローカルサイトのアドレスプールから IP アドレスを取得し、すべてのトラフィックがローカルサイトのボーダーに送られます。この設定では、複数サイト間でのアドレス管理とポリシー適用が複雑になります。この課題に対処するために、Cisco DNA Center は VN アンカーを利用したマルチサイト リモート ボーダー ソリューションを提供しています。このソリューションは、マルチサイト リモート ボーダーとも呼ばれます。このソリューションでは、複数の分散サイトの指定 VN からのトラフィックを集約し、単一の共通のサブネットを使用して中央の場所（アンカーサイト）に戻すことができます。そのゲスト VN に対してサイトごとのサブネットを定義して使用する必要はありません。簡素化され一元化された共通サブネット構造により、VN アンカーサイトはサイト全体のゲストサービスの展開を大幅に簡素化し、大学環境でのゲストトラフィックに一貫した安全なセグメンテーションを提供します。

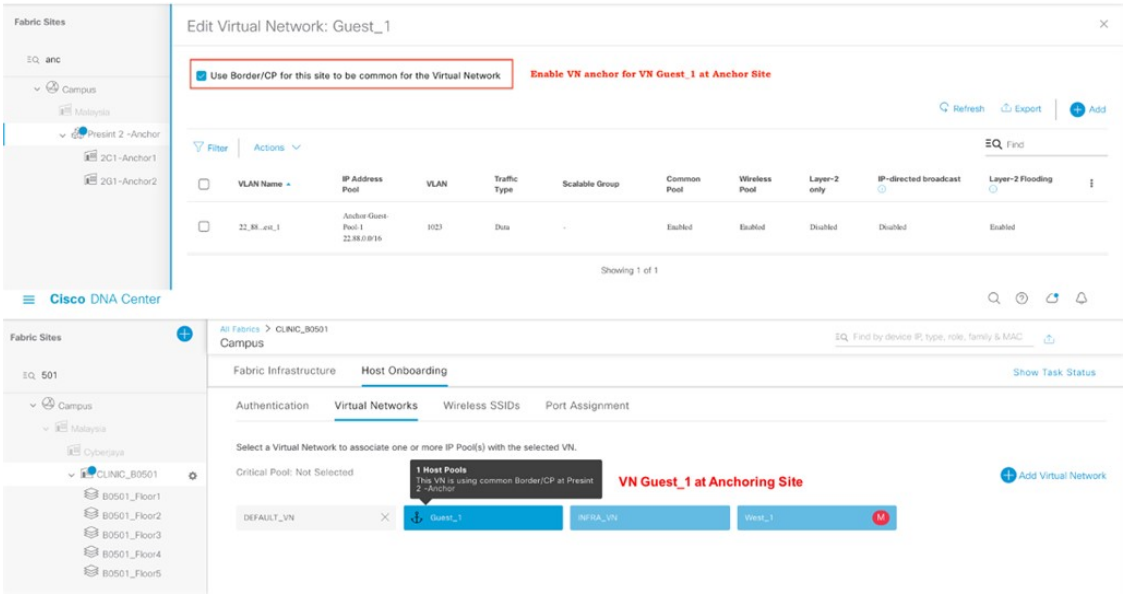
アンカーサービスを使用すると、各サイトのアンカー VN に属するエンドポイントのトラフィックが集約され、VXLAN を介してアンカーサイトにあるリモートアンカーボーダーにトンネリングされます。アンカーサイトは従来のファブリックサイトとほぼ同様に機能しますが、特定の VN にサービスを提供する仮想ファブリックサイトを形成します。こ

の仮想ファブリックサイトには独自のサイトボーダーとコントロールプレーン（CP）があり、それらがアンカーサイトに配置されます。アンカーサイトの特別な点は、そのエッジとワイヤレスコントローラが複数のファブリックサイト（アンカーリングサイト）に分散していることです。

マルチサイト リモート ボーダーは VN 単位で有効になります。アンカー VN の場合（理想的にはゲストサービスの場合）、継承されたサイトのすべてのエッジは、データプレーンと制御通信にアンカーボーダーと CP を使用します。アンカーリングサイトのワイヤレスコントローラは、ワイヤレスエンドポイントの登録のためにアンカー CP と通信します。アンカーされていない従来の VN の場合、エッジおよびワイヤレスコントローラは、今までと同様、データプレーンと制御通信に独自のサイトローカルボーダーと CP を使用します。ファブリックロールで動作するデバイスの他のルーティングロケータ（RLOC）と同様に、CP およびアンカーボーダーノードのループバック 0 アドレスは、アンカーリングサイトに配置されたエッジノードのグローバル ルーティング テーブルにある /32 ルートを介して到達可能である必要があります。アンカーボーダーの到達可能性は複数の IP ネットワークにおよぶ可能性があるため、VXLAN の 50 バイトのオーバーヘッドに対応するために、パス全体で MTU を考慮する必要があります。

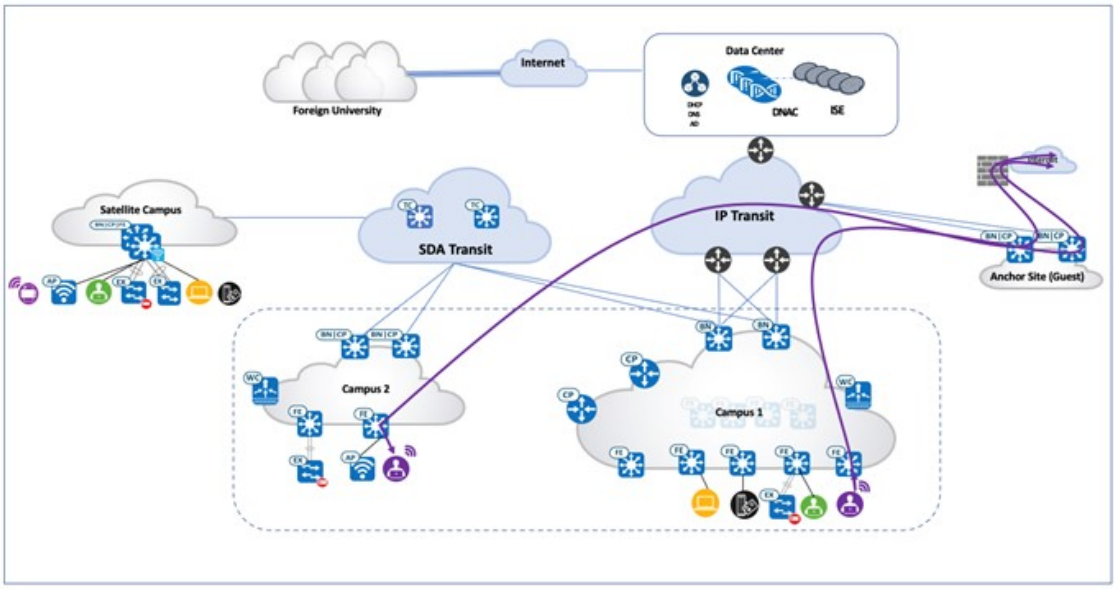
ゲスト VN は、アンカーサイトを使用するように設定されます。ゲストエンドポイントがゲスト SSID に参加し、Cisco ISE を使用して中央 Web 認証に合格すると、アンカーゲスト VN に関連付けられます。ゲストトラフィックはアンカーボーダーにトンネリングされ、ファイアウォールを介してインターネットに到達します。次の図は、Cisco DNA Center GUI で有効になっているマルチサイト リモート ボーダーを示しています。

図 *12 : Cisco DNA Center* でのアンカー *VN* の作成と関連付け



次の図は、アンカーゲストトラフィックのトラフィックパスを示しています。

図 *13* : アンカー *VN* が実装されたゲストトラフィックフロー



AI エンドポイント分析

大学では、多数のユーザーとそのデバイスを管理する必要があります。BYOD では、学生または教職員は 1 人あたり 2 ～ 3 台のデバイスを使用します。規模に加えて、セキュリティの問題も発生します。最新のセキュリティ脅威は、ネットワークの有益な企業情報にアクセスするために悪用できる脆弱な侵入ポイントを探します。ネットワーク内のすべてのデバイスを特定して追跡するのは、時間がかかり、面倒な作業です。Cisco AI エンドポイント分析機能は、パッシブ ネットワーク テレメトリ モニタリングとディープ パケット インスペクションを使用して、タイプ、製造元、モデル、OS タイプ、通信プロトコル、およびポート別にデバイスを識別することで、この問題に対処します。この機能を使用すると、管理者は、属性に基づいてデバイスを分類するためのプロファイリングルールを作成できます。Cisco DNA Center は、機械学習と連携してスプーフィングされたエンドポイントを検出し、管理者が適切なアクションを判断できるようにします。

Cisco AI エンドポイント分析 は、Cisco DNA Center とともに実行される追加のアプリケーションです。このアプリケーションは、カタログサーバーからダウンロードしてインストールします。その後、Cisco DNA Center のシステム設定で有効にします。Cisco DNA Center は、最新のエンドポイント分析モデルをダウンロードするためにクラウドに接続する必要があります。Cisco AI エンドポイント分析 を正常にインストールしたら、Cisco DNA Center ホームページからメニューアイコンをクリックし、[Policy] をクリックしてアクセスできます。

Cisco AI エンドポイント分析 は、複数の方法を使用して悪意のあるエンドポイントを検出します。また、プロファイルラベルの変更、NAT モードの検出、同時 MAC アドレス、ポスチャ、認証方式、および機械学習の機能を使用して、偽のエンドポイントを識別してフラグを立てます。全体的な信頼スコアは、すべてのエンドポイントに対して生成されます。信頼スコアは、複数のリスクスコアの加重平均です。信頼スコアが低いほど、エンドポイントのリスクが高いことを意味します。

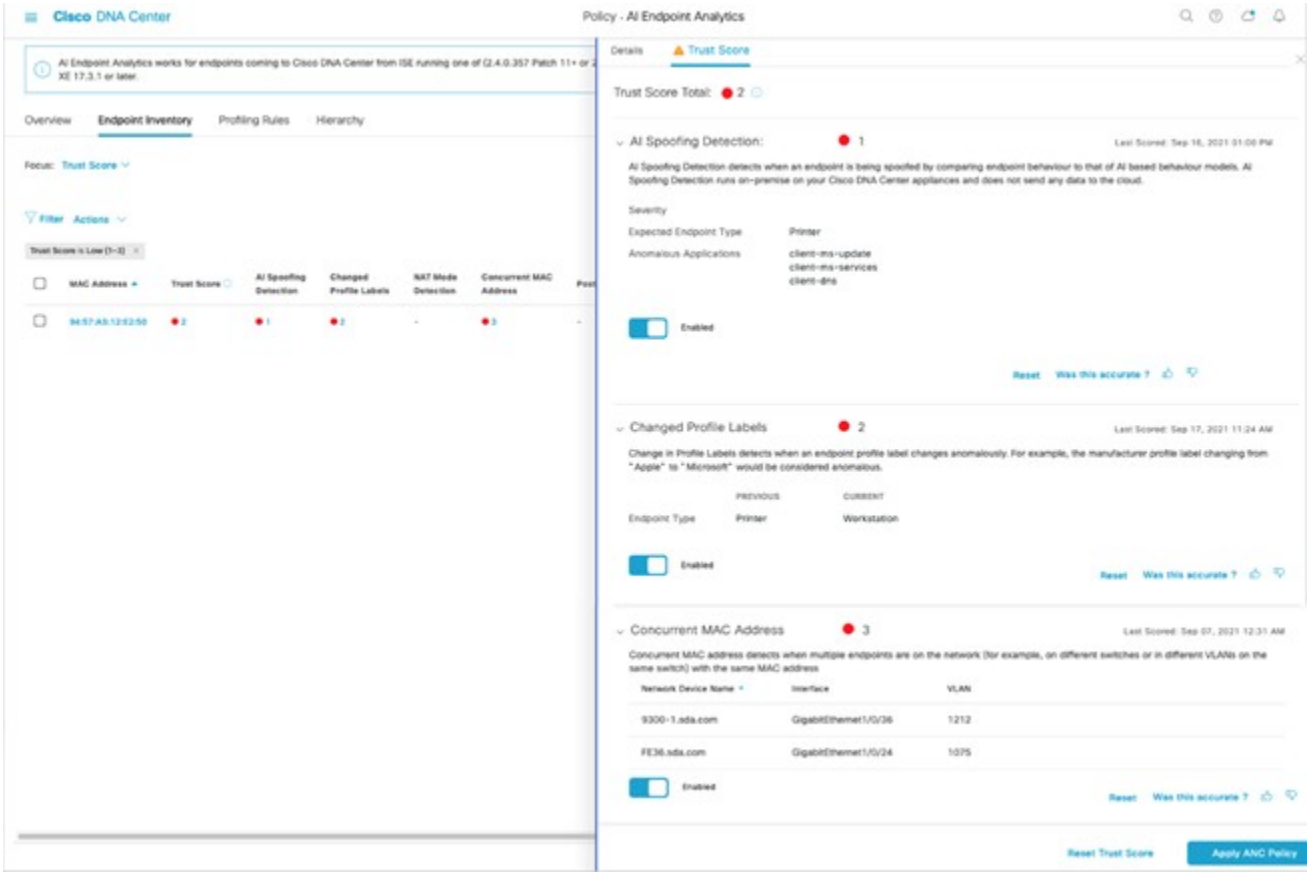
さらに、Cisco DNA Center はエンドポイントの分類属性を Cisco ISE と共有します。アイデンティティベースの認証で新しいデバイスがオンボーディングされると、製造元とタイプに基づいて自動的に識別され、該当するグループに追加されます。セキュリティポリシーの定義と適用は、個々のエンドポイントではなくグループに適用した方が簡単です。

グループベースのポリシーは、エンドポイントによるセキュリティ侵害などの新たな状況に合わせて簡単に更新でき、ネットワーク全体にグローバルに適用できます。

たとえば、学生のラップトップによって図書室のプリンタがスプーフィングされ、ネットワークにアクセスしたとします。

次の図は、悪意があるとしてフラグが立てられたプリンタ MAC アドレスと、その他の信頼スコア詳細を示しています。

図 *14 : Cisco DNA Center* の *Cisco AI* エンドポイント分析 信頼スコア詳細



Cisco DNA Center は、ネットワーク内の 2 つの場所でのプリンタ MAC アドレスの存在を特定し、悪意のあるデバイスのタイプを特定できます。また、侵害された MAC アドレスによって送信されているトラフィックのタイプを特定することもできます。

ファブリック外のレイヤ 2 ゲスト終端

お客様は、ネットワークを使用しているゲストに対してレイヤ 2 レベルのトラフィック インスペクションを必要とする場合があります。この要件は、すべてのゲストトラフィックのファーストホップがファブリックの外部にある必要があることを意味します。この実装は、Cisco DNA Center と手動のデバイス設定の組み合わせを使用して実現されます。ゲストトラフィックは VXLAN でカプセル化され、ファブリックを通過しますが、ゲストトラフィックのファーストホップまたはゲートウェイはファブリックの外部にあります。

この設定を実現するために、ゲストネットワーク/SSID は Cisco DNA Center から展開されます。また、ゲスト VN のファブリックサイトのボーダーにはレイヤ 2 ハンドオフがあります。ファイアウォールまたはレイヤ 2 終端ポイントは、レイヤ 2 ハンドオフのもう一方の端にあります。ファイアウォールには、ゲストと同じサブネット内の IP アドレスが設定されます。ゲストが IP アドレスを取得する DHCP サーバーは、ファイアウォールレイヤ 2 終端 IP としてファブリック エニーキャスト ゲートウェイ IP ではなく、ルータ IP を提供する必要があります。

これらの変更により、ファイアウォール IP はゲスト VN のクライアントのように機能します。ゲストラップトップが IP アドレスを取得してトラフィックを送信する場合、ファーストホップ（ファブリック外のレイヤ 2 終端ポイント）は L2 LISP を介して解決され、ラップトップは外部と正常に通信できます。この設定では、ファブリック外でゲストトラフィックのレイヤ 2 インスペクションをさらに実行できます。

参照

- *Cisco SD-Access Solution Design Guide (CVD)*
- *Cisco Software-Defined Access for Distributed Campus Prescriptive Deployment Guide*
- *Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide*
- *Cisco Software-Defined Access Compatibility Matrix*
- *Cisco ISE BYOD Prescriptive Deployment Guide*
- *Configure Fusion Router in SDA*
- *Cisco DNA Service for Bonjour: SD-Access Wired and Wireless Deployment Guide*
- *Cisco DNA Service for Bonjour: Quick Configuration Guide*

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。