【シスコ エンタープライズ企業向けマンスリーウェビナー】

ネットワーク セグメンテーションを実現するソリューションとユースケース

セキュリティ事業　サイバーセキュリティ製品担当　福留 康修
エンタープライズネットワーキング事業　プロダクト・セールス・スペシャリスト　次藤 則兼

2024.12.18

セグメンテーションの種類

マクロとマイクロの 2 種類

1. マクロ セグメンテーション

- 仮想ネットワークのレベル
- VRF ベース
- 異なる仮想ネットワークに存在するホストは通信不可

2. マイクロ セグメンテーション

- 仮想ネットワーク内
- タグ（SGT)にもとづく
- ロールベースでの許可にもとづきホストは通信可能

なぜマイクロ セグメンテーションなのか？

- East-West トラフィックに対するセグメンテーション
- アタック サーフェスを減らしより安心できる環境の構築
- 監査、コンプライアンス、および適合性

セグメンテーションの基本

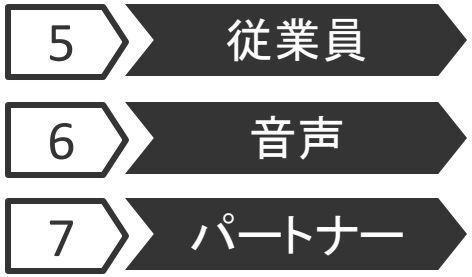
- デバイス / ユーザをベースに許可されるネットワーク
  - ユーザは信頼でき管理対象の端末を利用しているか？
  - 管理対象外の端末によるネットワークへのアクセスは許可されるか？
  - デバイスにはパッチが適用されコンプライアンス上問題ない状態か？
  - セグメントの割り当て
    - VLAN、VRF、SGT（タグ）
  - セグメント間で許可する通信やプロトコル

エンド・ツー・エンドのセグメンテーションはチャレンジ

1. **VLAN および ACL**
   - スタティックかつデバイス毎の管理
   - IP ベース
2. **VRF**
   - プライベート ネットワーク越しの Multi VRF は高価になりがち
   - インターネット越しの Multi VRF はオーバーレイ型で複雑な設計
3. **セキュリティ グループ タグ (SGT)**
   - エンド・ツー・エンドでのマーキング管理は手間
   - IP to SGT バインディングのスケーラビリティ

マイクロセグメンテーションには自動化されたタグ付与の仕組みが重要

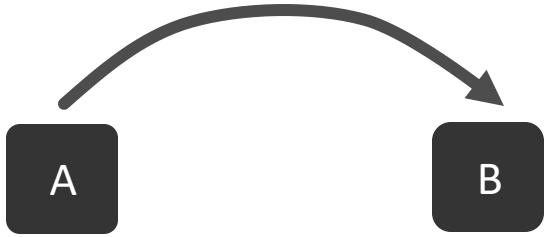
ご参考 : “タグ” 制御を行うための3つの構成要素



分類 Classification

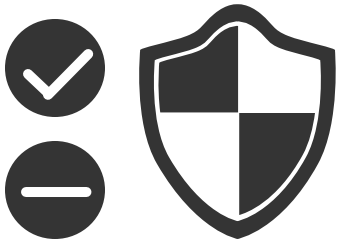
（タグ の割り当て）

- スタティック割り当て
- ダイナミック割り当て



伝播 Propagate

- インライン SGT
- SXP
- WAN オプション



適用 Enforcement

- セキュリティ グループ ACL
- SG ファイアウォール

シスコ ソリューションにおける様々なタグのユースケース

Meraki

オンプレSecurity
(Firewall)

インター
ネット

クラウドSecurity
(SSE)

マルチクラウド
(IaaS)

SD-Access

SD-WAN

データセンタ

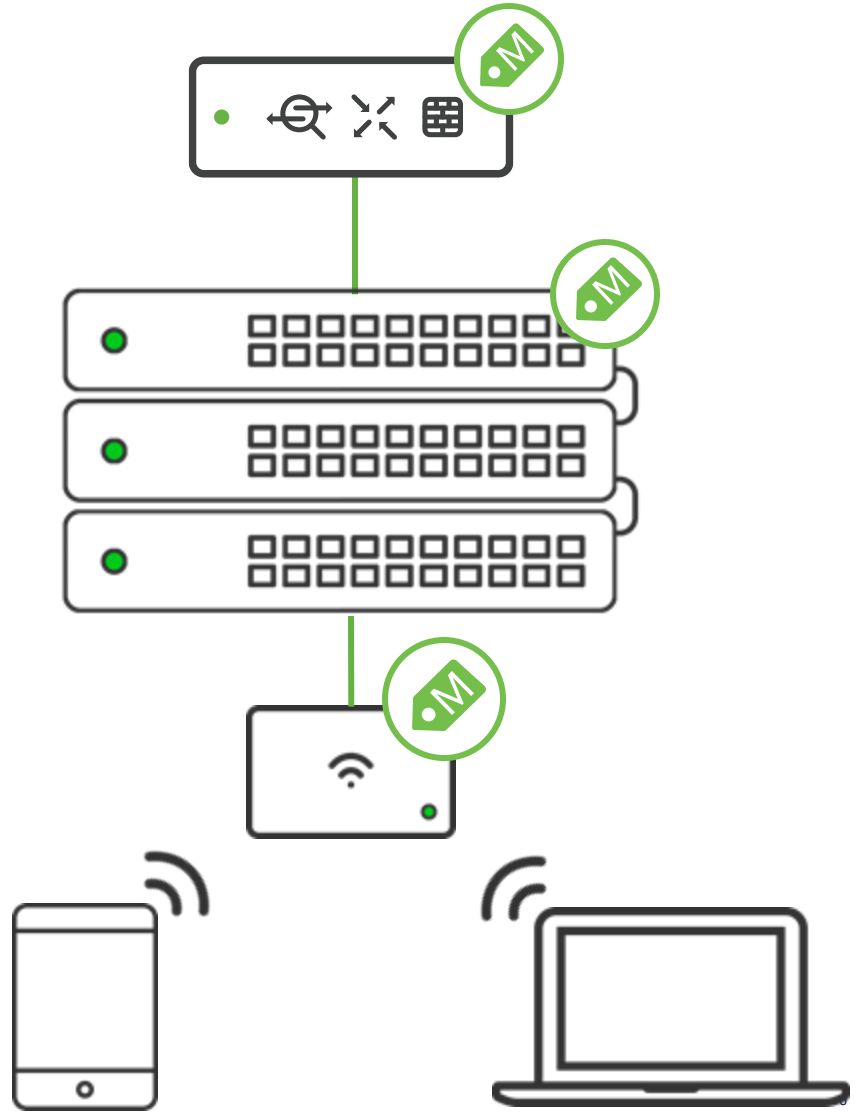
Meraki Adaptive Policy

セキュリティグループタグを使用したマイクロセグメンテーションとコンテキスト

オーガナイゼーション全体の
インテントベースのポリシー

インライン セキュリティ グループ タグ (SGT) の利用

有線、ワイヤレスアクセスだけではなく、
Auto-VPN を介した全拠点に同一のポリシーを提供



サポートされる分類 (Classification)

静的ポート割り当て

サプリカントのない
固定有線デバイス

静的 SSID 割り当て

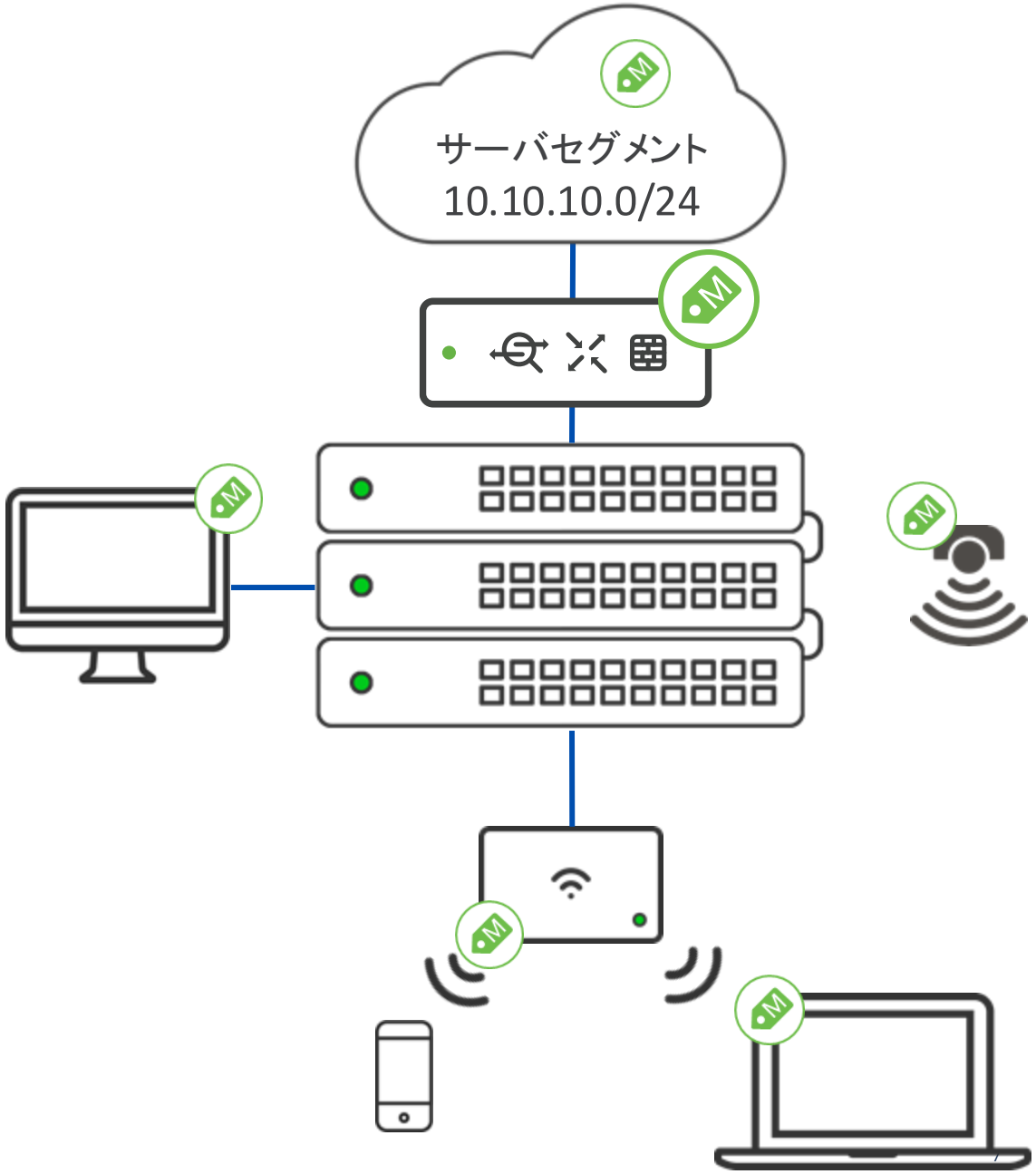
ゲストアクセス等の SSID 単位へ
割り当て

RADIUS (ダイナミック)

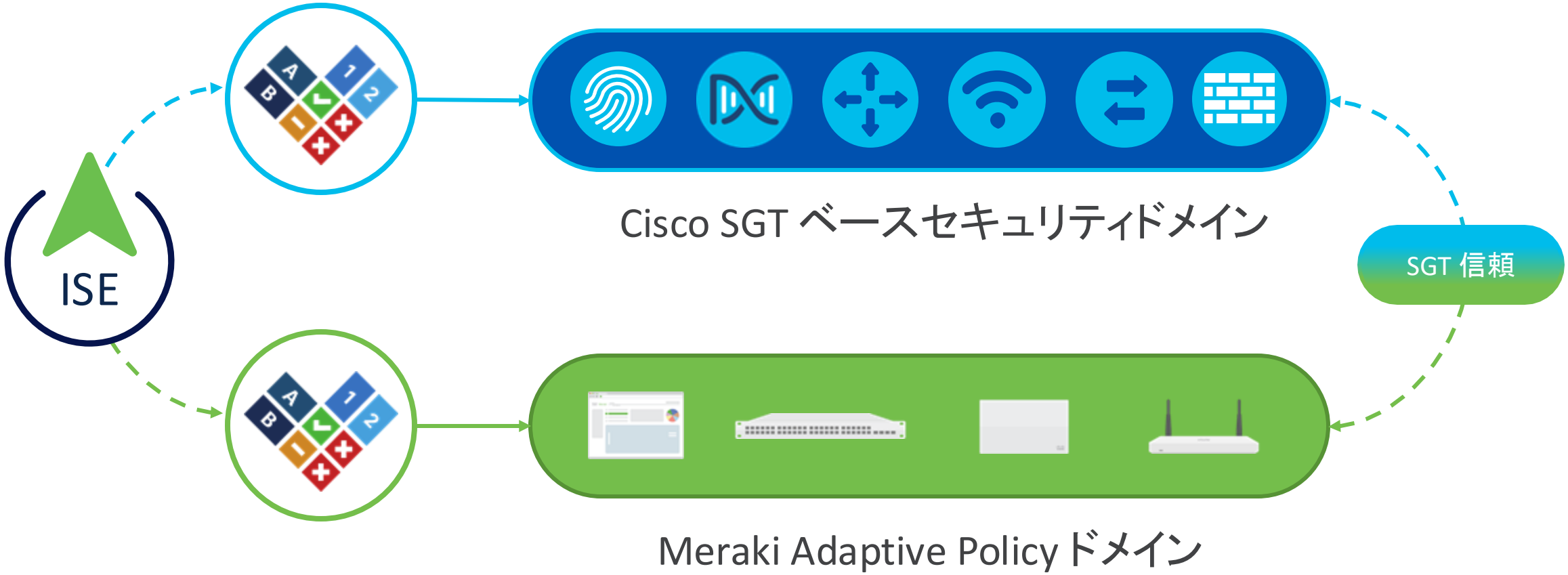
有線およびワイヤレス
MAB/802.1X および
iPSK w/ RADIUS

IP プレフィックスから SGT マップへ

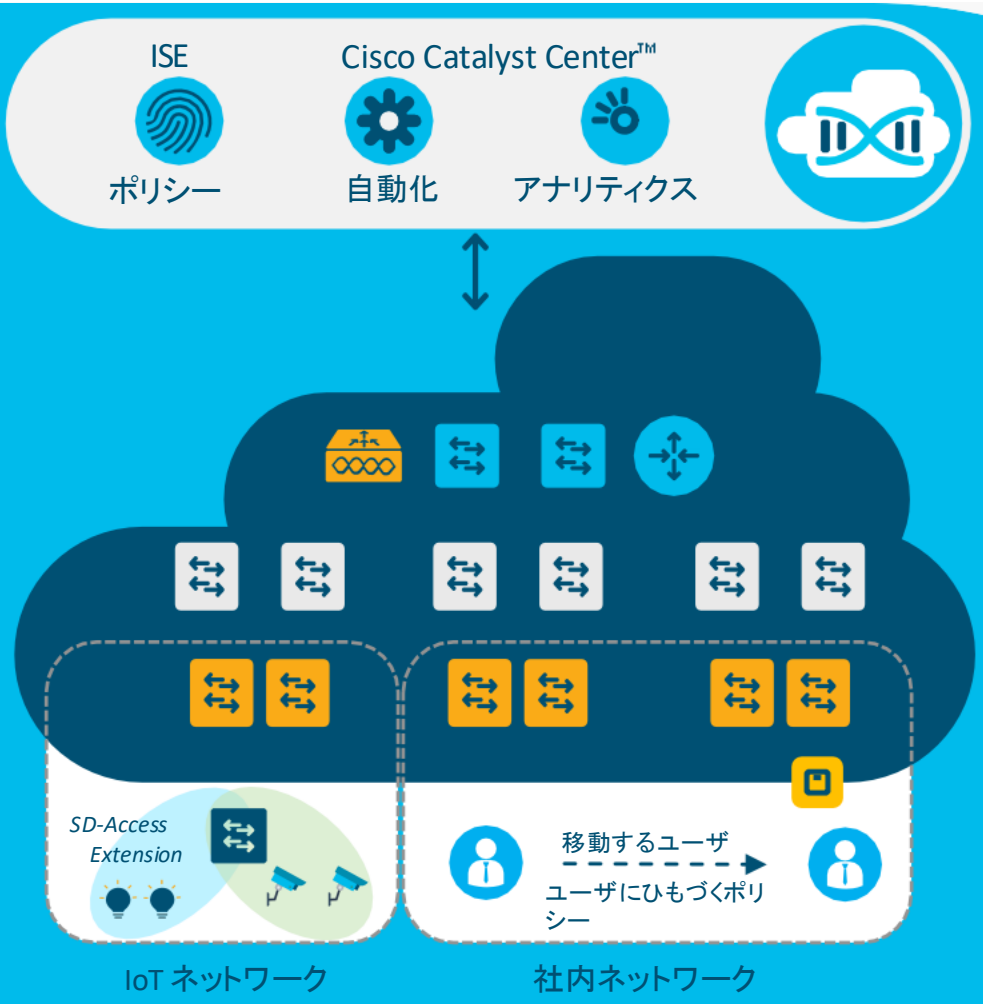
IP/Subnet に基づいた割り当て
MS : VLAN 単位に SGT 割り当て(ロードマップ)



マルチドメイン対応 ゼロトラストフレームワーク



Cisco Software-Defined Access (SD-Access)
インテント・ベース・ネットワーキング



- アイデンティティ・ベース
- ポリシーとセグメンテーション
- VLAN や IP アドレスから切り離されたセキュリティ・ポリシー定義

- 自動化されたネットワーク・ファブリック
- ワークフローベースの自動化により、有線および無線用の単一ファブリックを実現

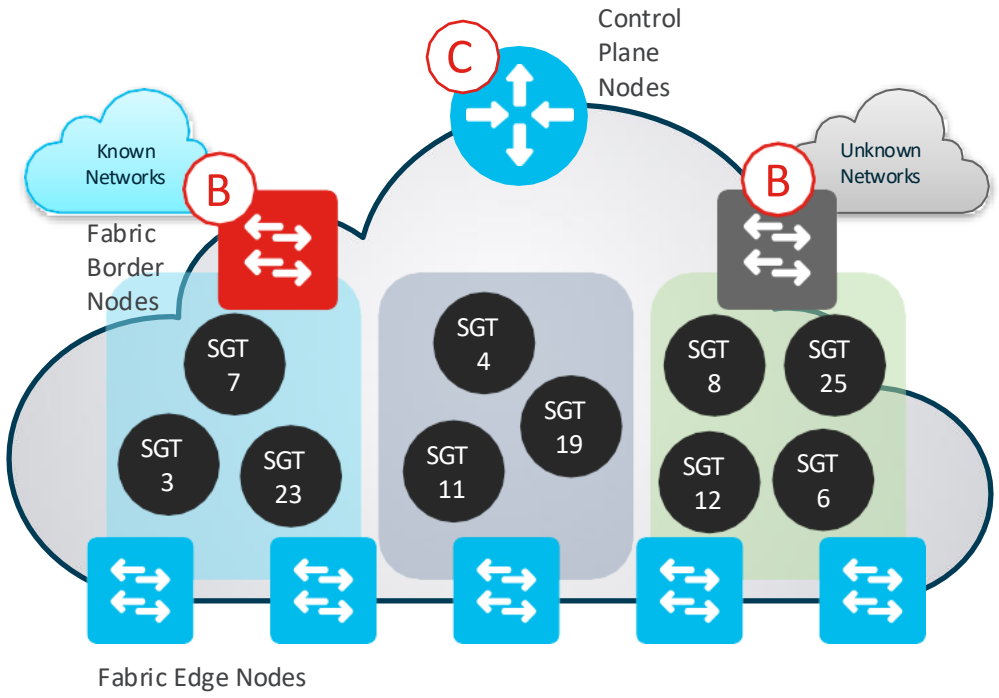
- インサイトと遠隔測定
- ユーザーとアプリケーションのアプリケーション体験

一貫したエクスペリエンスを提供するためのシンプルなオペレーション

SD-Access Scalable Group Tag (SGT)

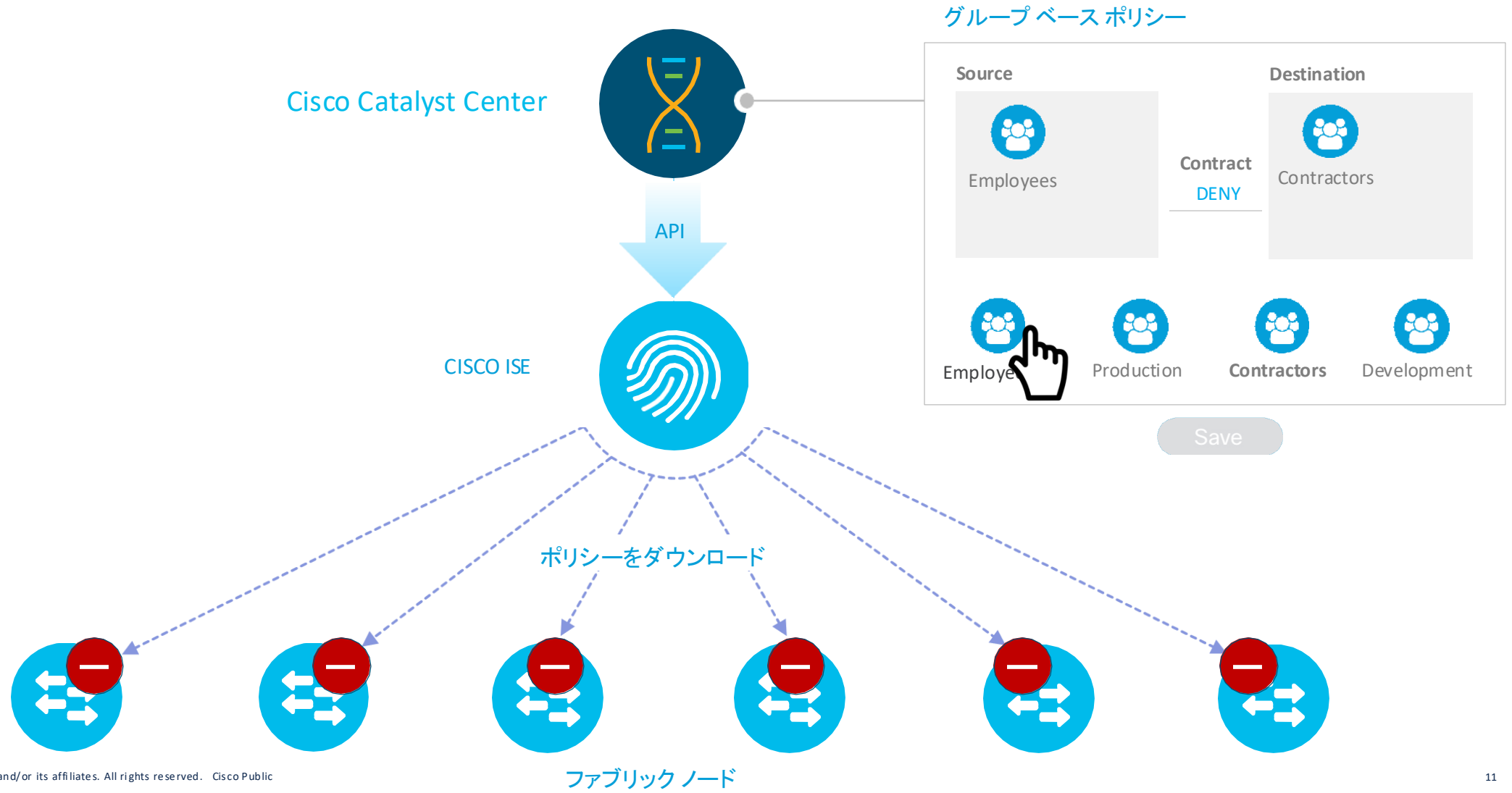
スケーラブルグループは、ユーザやデバイスを「グループ化」するための論理 ID オブジェクト

- 「スケーラブル・グループ」を使用し、エンドポイントに一意のスケーラブル・グループ・タグ（SGT）を割り当て
- ノードはファブリックのカプセル化に際し SGT を追加
- SGT は IP アドレスに依存しない「グループベースのポリシー 」を管理するために使用
- エッジノードまたはボーダーノードは、SGT を使用してローカルの Scalable Group ACL（SGACL）を適用
- SGT を利用するユースケースは「マイクロ セグメンテーション」として知られる



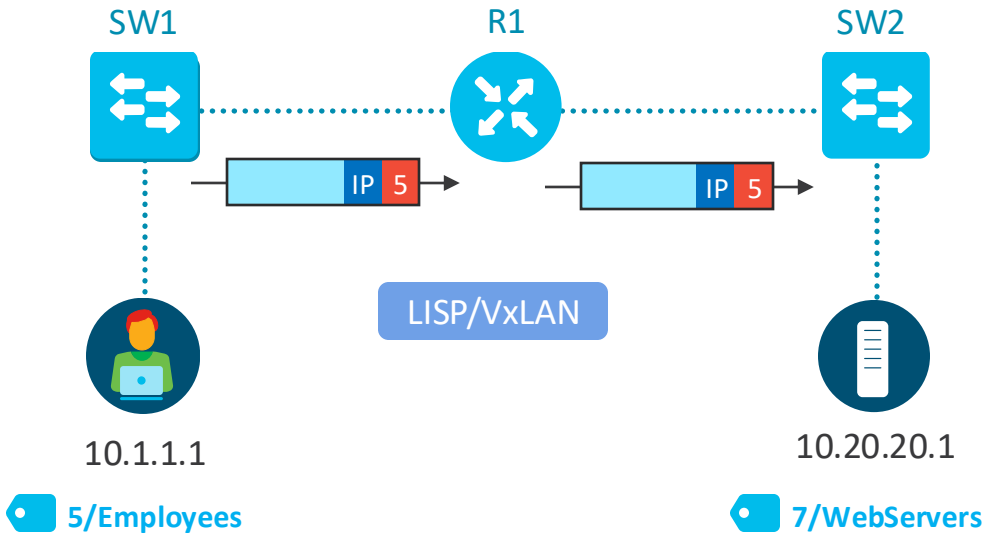
Cisco Catalyst Center

SD-Access を自動化された Fabric Campus へ



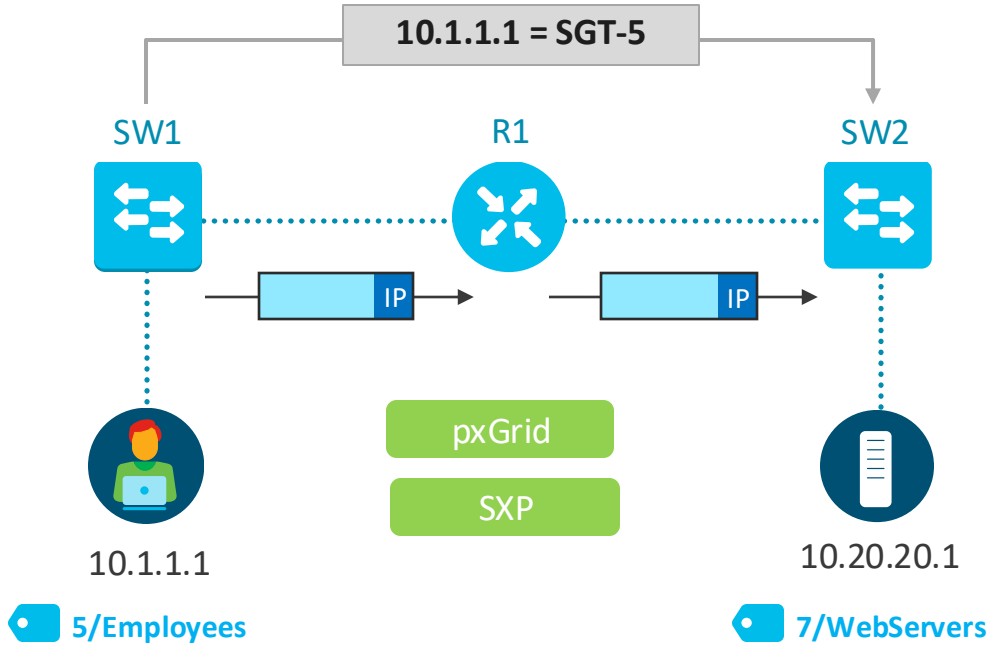
ご参考 : 伝播 (propagate) を行う 2 つの方法

データプレーンにおける伝播



SGT はデータトラフィックのインラインで伝送される

コントロール プレーンにおける伝播



IP-to-SGT データは制御プロトコル上で共有される

ファイアウォールにおける、タグにもとづく制御

ネットワークと投資を活用

- 40 を超えるシスコ製品ファミリで利用されている、拡張性/俊敏性に優れたセグメンテーション技術
- ネットワーク上のどこでもロールベースのポリシーを動的に適用可能
- SRC と DST の SGT をマッチングすることで、Firepower Threat Defense を介して TrustSec ポリシーを拡張

シンプルなアクセス管理

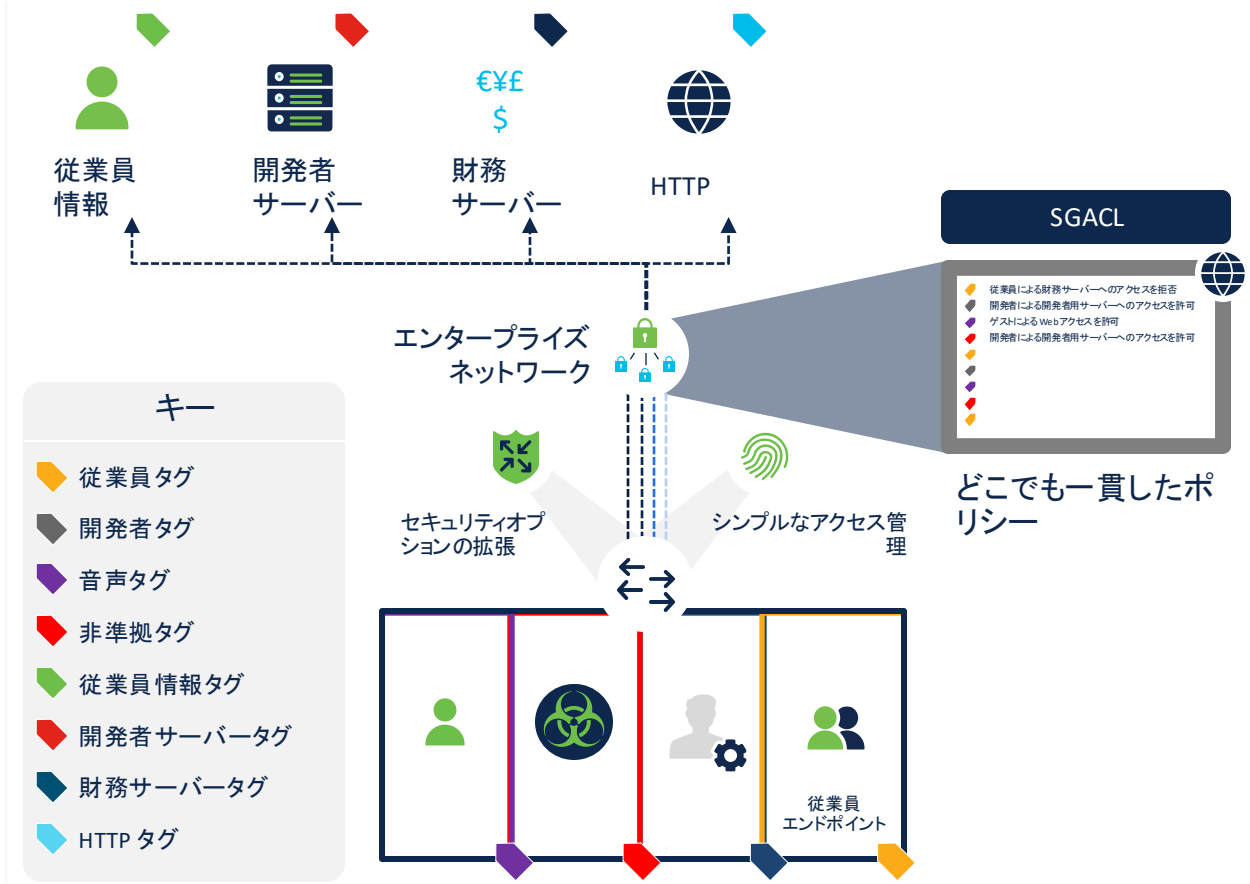
わかりやすい言葉でポリシーを管理し、ビジネスロールに基づいたアクセス制御でコンプライアンスを維持

迅速なセキュリティ管理

シンプルなファイアウォール管理によってサーバーのオンボーディングが迅速になり、追加、移行、変更に要する時間が短縮

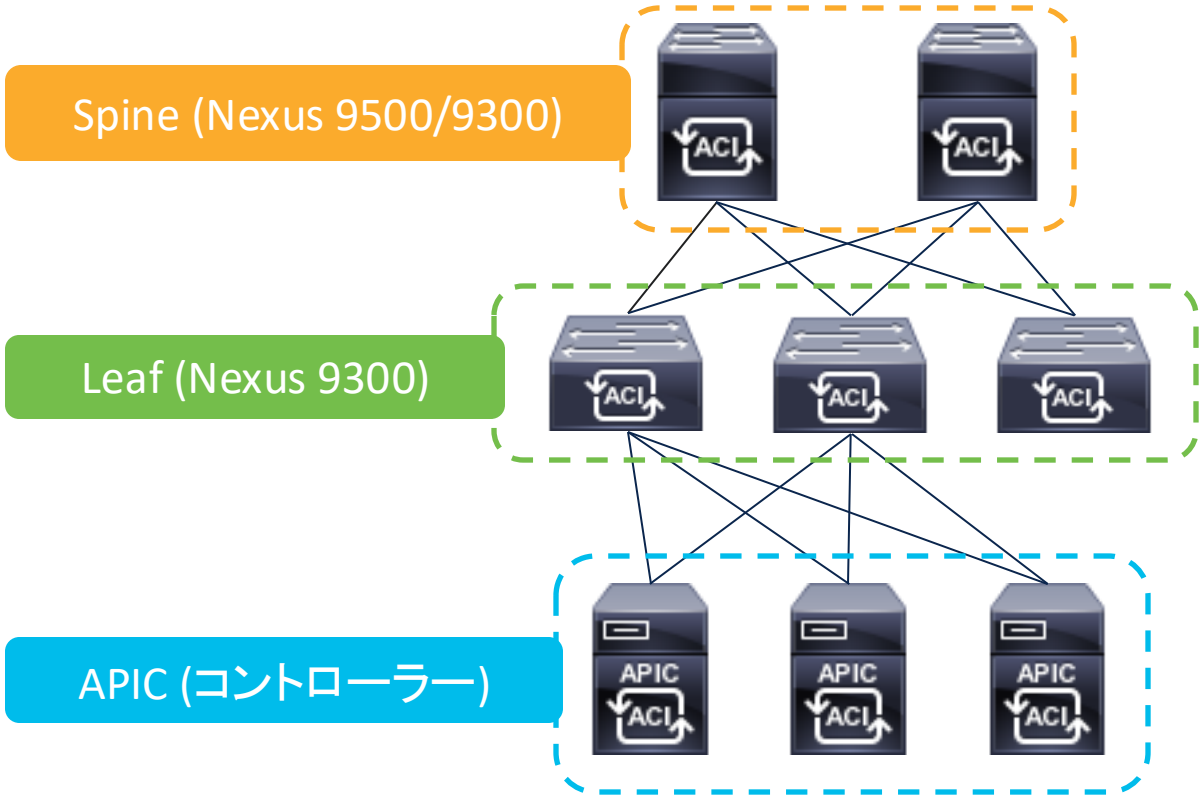
どこでも一貫したポリシー

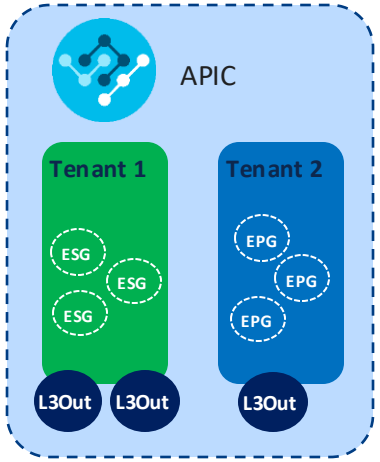
デバイスの接続が有線、ワイヤレス、VPN のいずれであっても、すべてのネットワークセグメントを一元管理可能



ACI によるセグメンテーション

IP ファブリック ネットワークを基盤として、APIC（Application Policy Infrastructure Controller）というコントローラで全体を制御するソリューション





オーバーレイ

- ACI 独自の概念(Tenant/VRF/BD etc…)を使って定義する

アンダーレイ

- ACIでは自動的に構成され、基本的にユーザが設定を行う必要がない

広帯域
- 10/40/100/400G Uplinkをサポート
- Spineを最大6台まで拡張可能

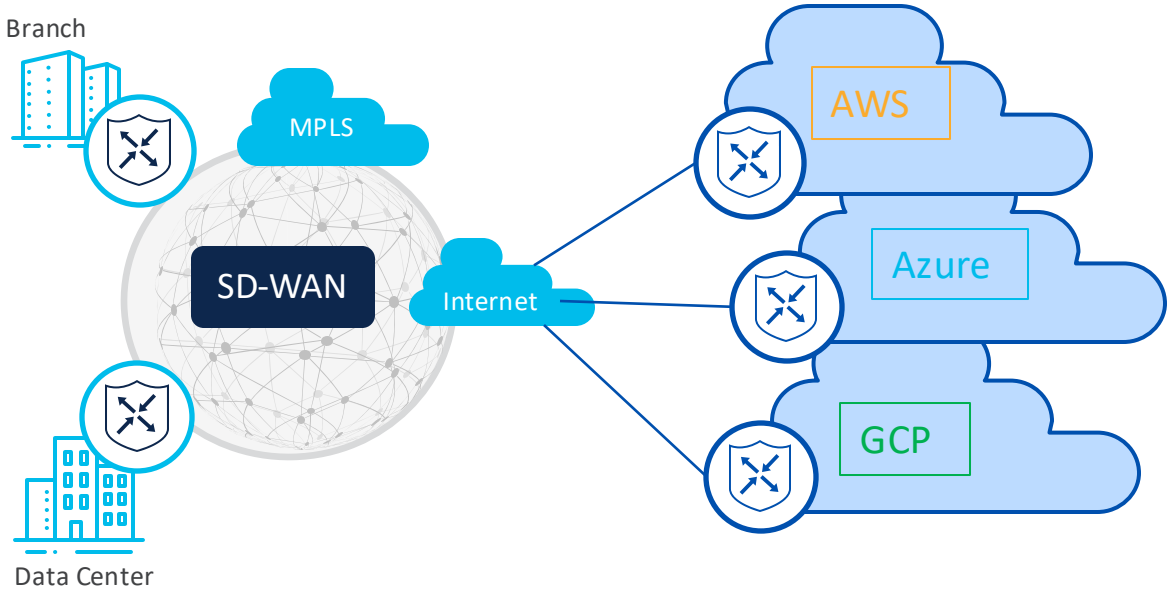
高可用性
- 数ミリ秒でのUplink障害切り替わり

拡張性
- ポートが足りなくなったらLeafを増設
- 帯域が足りなくなったらSpineを増設

柔軟性
- APICによる集中管理
- VXLANを使用して論理ネットワークを構成

パブリッククラウドへの SD-WAN 拡張の自動化

Cloud OnRamp によるマルチ クラウド対応



利点

- CSPへのSD-WANファブリックの自動化
- ポリシーの枠組みをクラウドに拡張
- ダイナミック・ルーティングのためのコントロール・プレーン統一
- 1つの管理プレーンで運用を簡素化
- デバイスと回線の可視性を高める
- 複数のクラウドプロバイダーを統合

Cisco Secure Access 概要

ゼロトラストを実現する統合型クラウドセキュリティ

ユーザーにとってより快適に
スムーズなユーザー
エクスペリエンスで仕事を支援

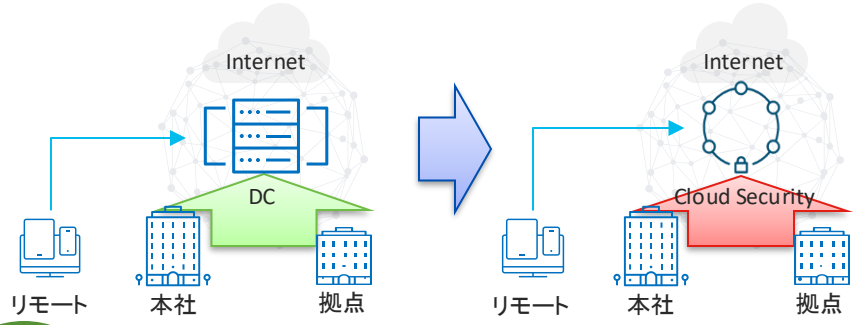
IT をより使いやすく
コストを削減し効率を向上

すべての人にとってより安全に
リスクを緩和しビジネスのレジリエンスを強化

Cisco SASE : Secure Access & Catalyst SD-WAN

現状 DC・Cloud Security 一極集中

- ✓ SaaSアプリケーションの増加によりネットワークトラフィック急増
- ✓ データセンター一極集中からCloud Securityへとシフト
- ✓ Cloud Securityによる一元的なセキュリティ対策
- ✓ リモートワーカーのVPN接続も、データセンターからCloud Securityへシフト



一極集中による問題点
- ➢ トラフィック増によるコストUp
- ➢ 期待しているスピードが出ない
  →特にSaaS, 拠点間通信
- ➢ Single Point of Failure:単一障害点

課題 アプリケーション毎に経路と行き先をコントロール

- ✓ アプリケーションの種別と重要度、トラフィック量を把握
  - ● 切れると業務に大きく影響する通信 → OT/生産系, Web会議, 勘定系
  - ● 侵害されると困る通信 → R&D, 機密情報・パテント
  - ● 多くの人が定常的に利用する通信 → Officeアプリ, 業務アプリ
  - ● **リスクの多い一般的なInternet通信** → Web閲覧、ライブラリ参照

アプリケーションの重要度に応じた選択
- ➢ 通信経路の選択:可用性、冗長性を重視
- ➢ 通信経路の分離:完全性、機密性
- ➢ セキュリティの適用:完全性、安全性

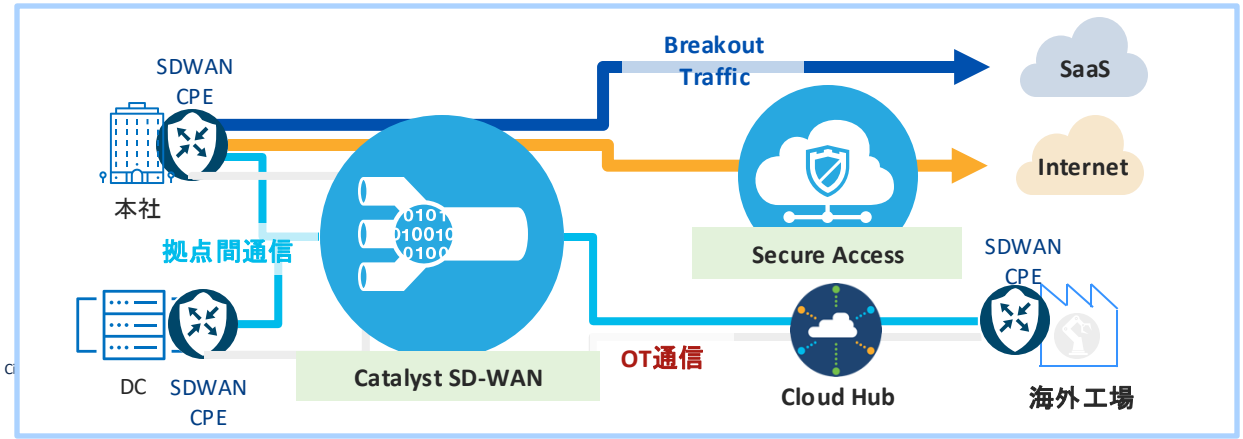
インターネットトラフィックのセキュリティ対策
- ➢ 主要なSaaS(MS365, Webexなど) → Breakout可能
- ➢ **一般的なInternet通信 → 要Cloud Security**

解決策 SSEとNetworkingをバランスよく組み合わせた アプリケーションのトラフィック量と重要度に応じた経路選択と強固なセキュリティ対策

Ciscoソリューション

Cisco Catalyst SD-WAN 特徴

- 詳細なアプリケーション振り分けによる適切な経路選択
- WANを論理分割し通信のセキュリティを確保するWANセグメンテーション機能
- ルータ・SD-WANとしての豊富な導入実績
- 高い安全性と可用性を実現するAct/Actでの冗長構成



Ciscoソリューション

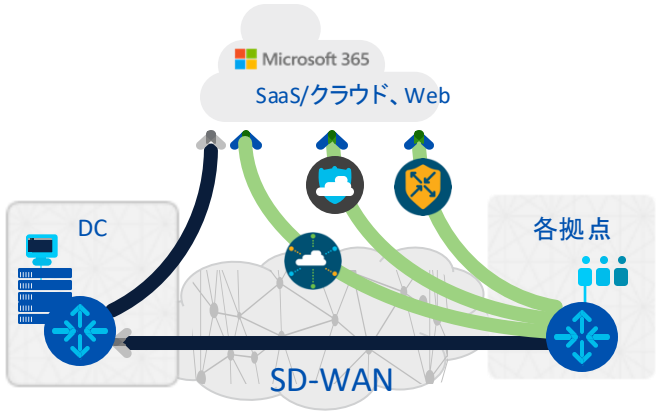
Cisco Secure Access 特徴

- 数十万User単位の大手製造業など豊富な導入実績
- Talos Intelligence 精度の高い脅威インテリジェンスの利用
- リモートアクセスではZTNA/VPNの両方を利用可能 高い利便性を実現
- SD-WANとの高い親和性による真のSASEソリューション

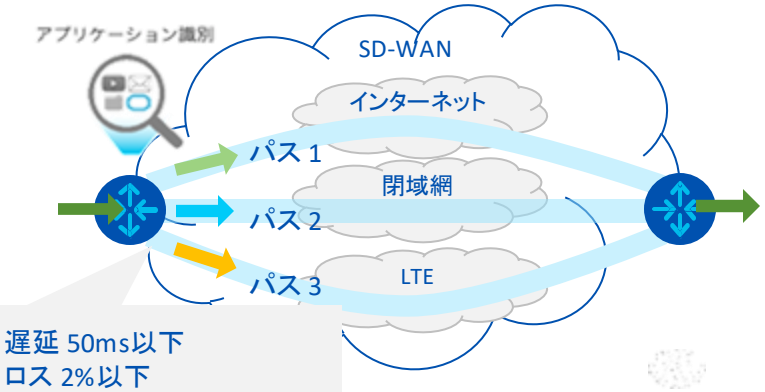
ご参考：Cisco Catalyst SD-WAN の特徴的なユースケース

Cisco Catalyst SD-WANは、クラウドベースのサービスとアプリケーションに迅速かつ安全にアクセスできるようにします。

ローカルブレイクアウト



WAN利用の最適化

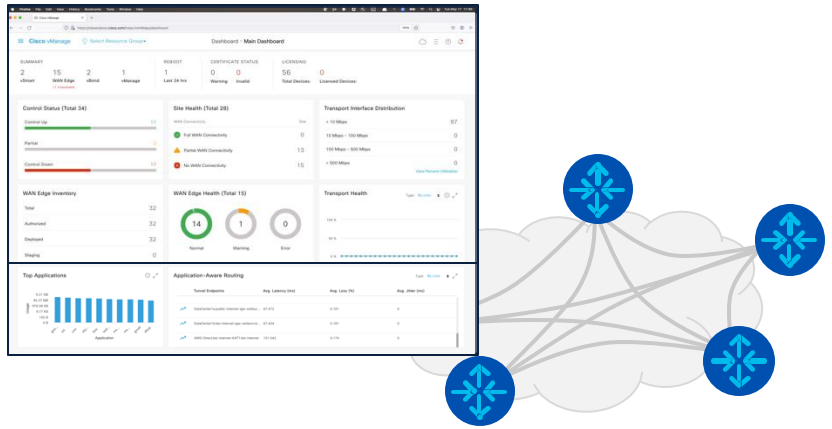


- 遅延 50ms以下
- ロス 2%以下
- ジッター 10ms以下

パブリッククラウド拡張

セグメンテーション

一元管理、可視化、分析

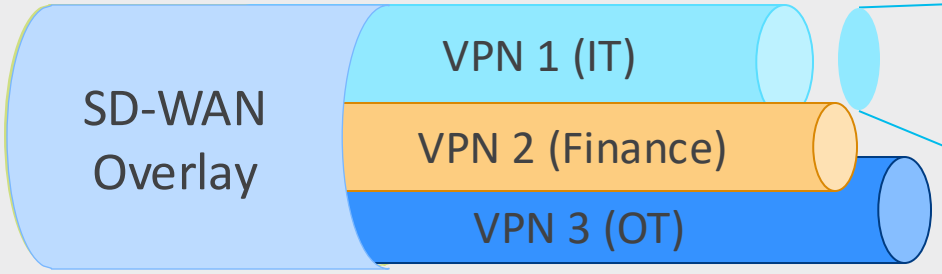


ゼロタッチプロビジョニング

Catalyst SD-WANでのセグメンテーション

セキュリティの重要な要素としてのセグメンテーション

マクロ・セグメンテーション

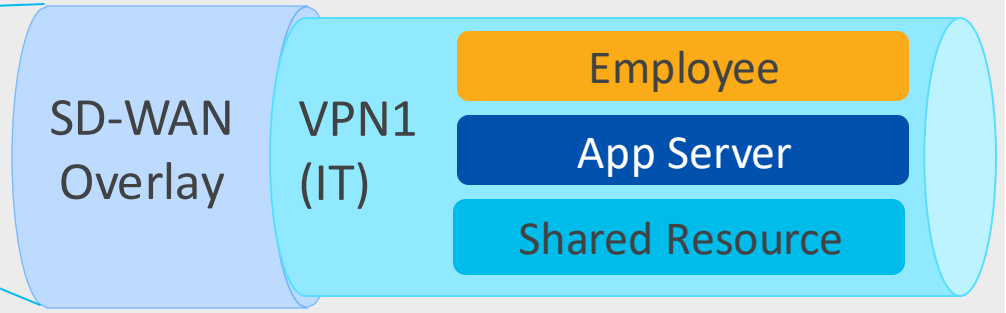


VPN Level Segmentation

- IT VPN
- Finance VPN
- OT VPN

トラフィックの流れを効率的に管理し、ネットワークの輻輳を軽減することで、システム全体のパフォーマンスが向上。
さらに、セグメントごとにトラフィックを分散させることで、重要なアプリケーションやサービスへのアクセス速度を向上させるだけでなく、回線内を論理的に分離することで、安全性の確保が可能。

マイクロ・セグメンテーション



Group Level Segmentation
Example: IT VPN

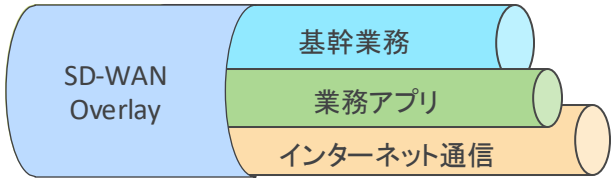
- Employee
- App Server
- Shared Resource

マクロセグメンテーションの中で、TAG付けを行い、さらに小さなセクションに分割。それぞれのセクションに独自のセキュリティポリシーを設定してアクセスできるようにする手法。従来のACLベースでは実現できない、属性やビヘイビアに応じたダイナミックかつ詳細なセグメンテーションとセキュリティ設定が可能。

Catalyst SD-WAN：マクロ・セグメンテーション

Catalyst SD-WANによる マクロ・セグメンテーション

- ✓ LANセグメントやアプリに応じたマクロ・セグメンテーション



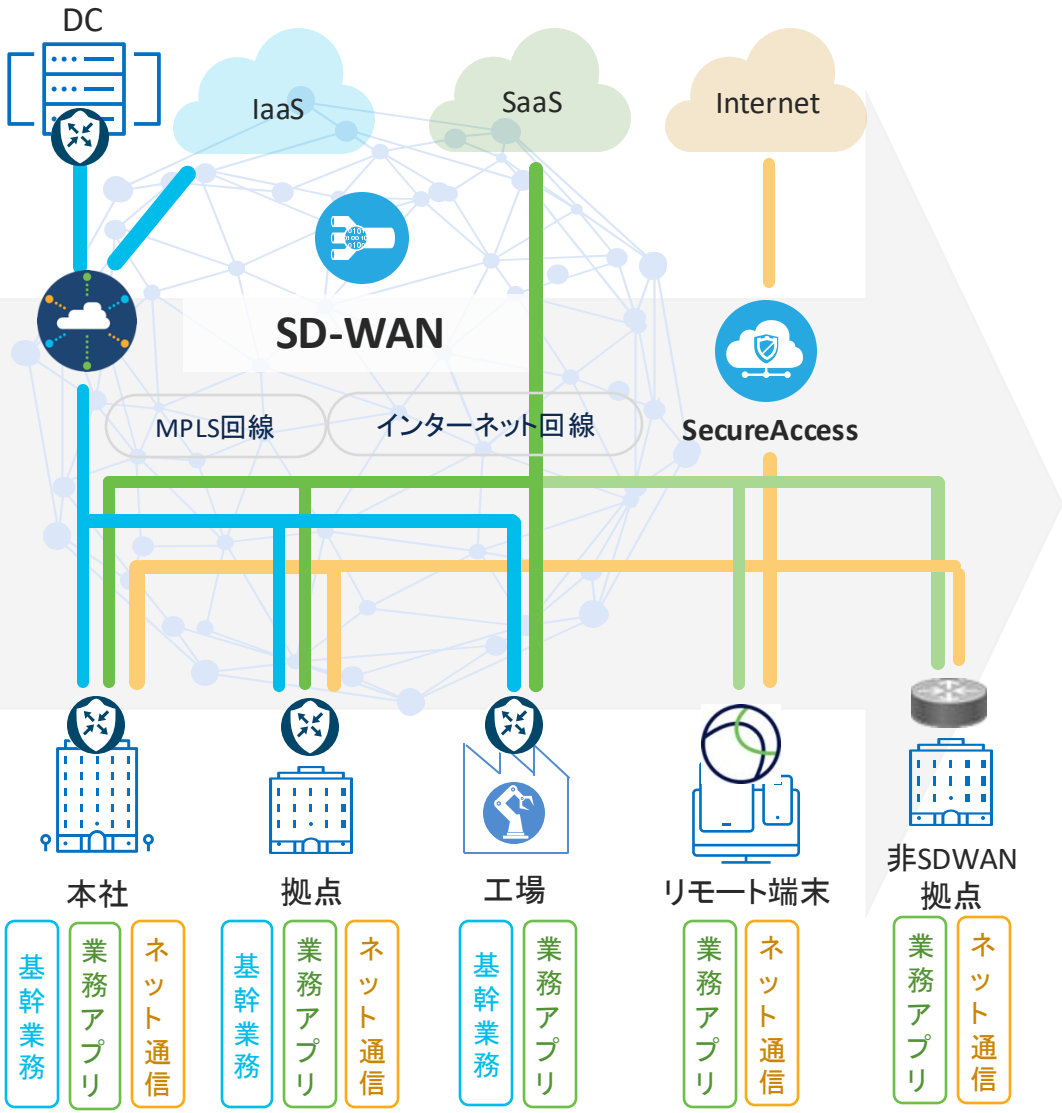
- ✓ それぞれのマクロ・セグメントで重要度に応じたセキュリティ対策

エンタープライズ ファイアウォール

侵入防御システム

URL フィルタリング

Adv. Malware Protection



柔軟性（+拡張性）

キャリア・回線種別に依存しない柔軟なWAN構築が可能。また、将来の回線の増設・増速にも柔軟に対応可能。

機密性（セキュリティ）

業務内容・事業内容に応じたWANのセグメンテーションにより、重要業務トラフィックを論理分割し安全性を確保。

安定性（品質）

アプリケーションの重要度と、回線の品質をモニターし、常に最適な経路を自動選択。常に安定したアプリケーション体験を実現可能

Catalyst SD-WAN：マイクロ・セグメンテーション

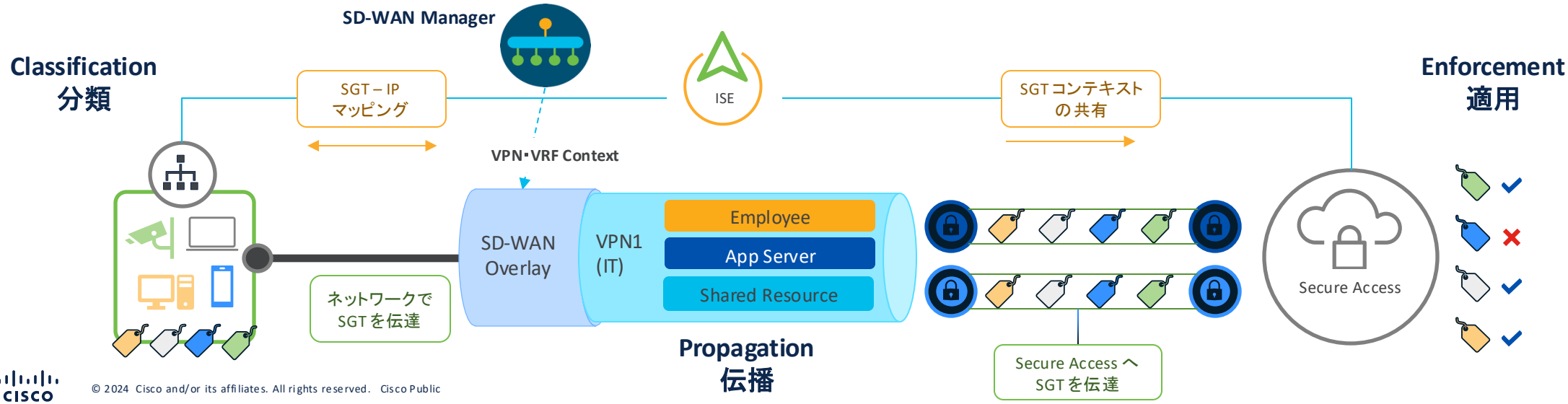
課題

- ネットワーク全域において一貫性のあるセキュリティポリシーをユーザ、デバイス、ワークロードに適用することは全てのCISOの共通認識であり、最重要課題の一つであり、ゼロトラスト実現の鍵となっている
- コンテキスト情報共有可能なセキュリティポリシーのユースケースとしては、製造拠点のCatalyst SD-WAN EdgeのLAN側にいる授業員、ゲスト、IoTデバイスがインターネット上のサービスを使用する際に、セグメンテーション情報（マクロ、マイクロ）に基づき、クラウドセキュリティ側で制御を行う必要がある。

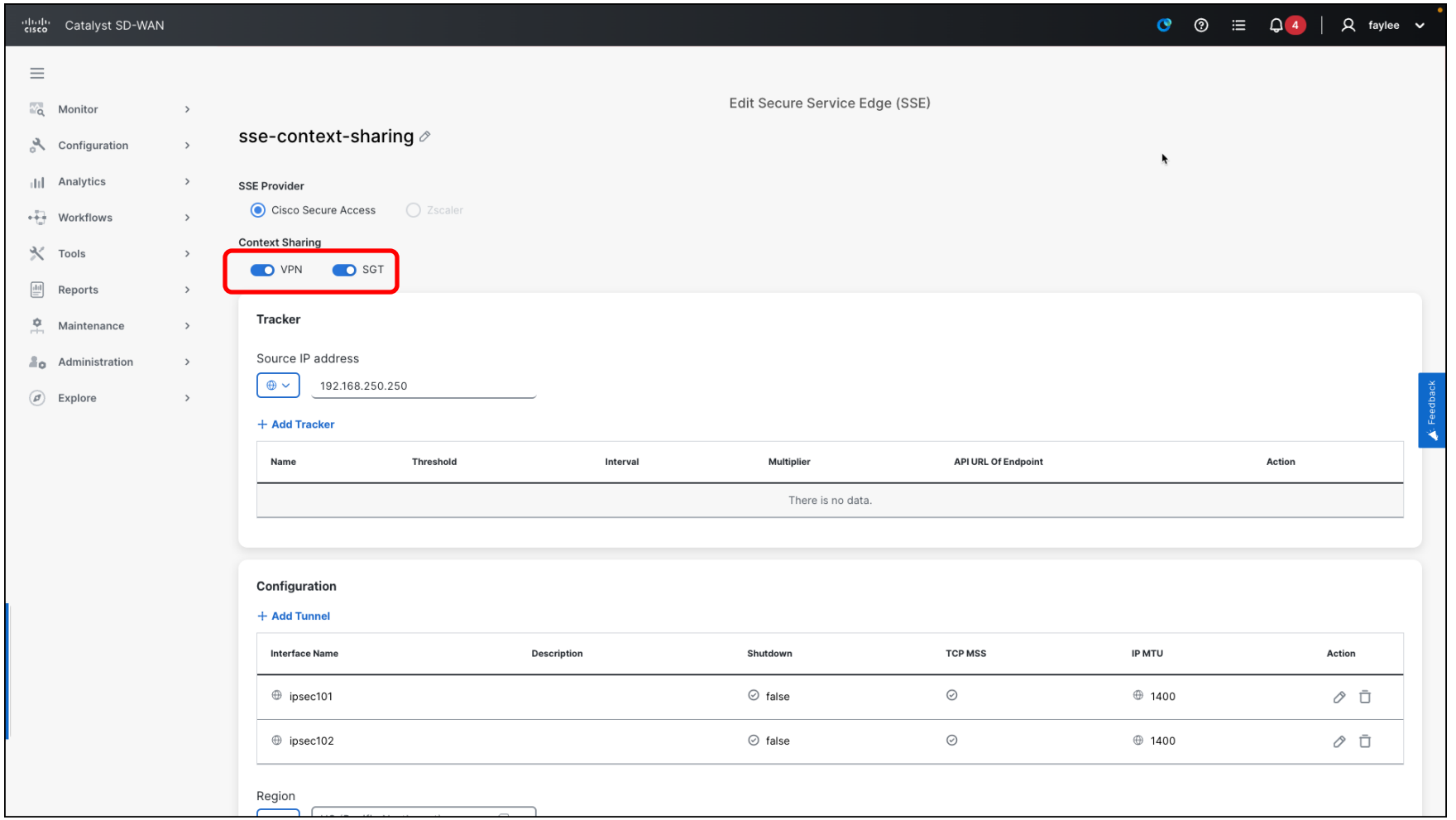
ソリューション

- 最新Verの20.15/17.15より、Catalyst SD-WANはCisco Secure Accessとコンテキスト情報を共有可能
- Catalyst SD-WANはマクロ・セグメンテーションのコンテキスト情報（VPN/VRF）、マイクロセグメンテーションのコンテキスト情報（SGT）の両方をCisco Secure Accessへ共有可能に！
- Cisco Secure Accessはこれらのコンテキスト情報をセキュリティポリシー適用に活用することが可能

- ネットワーク全体で一貫したセグメンテーションを実現する SGT -

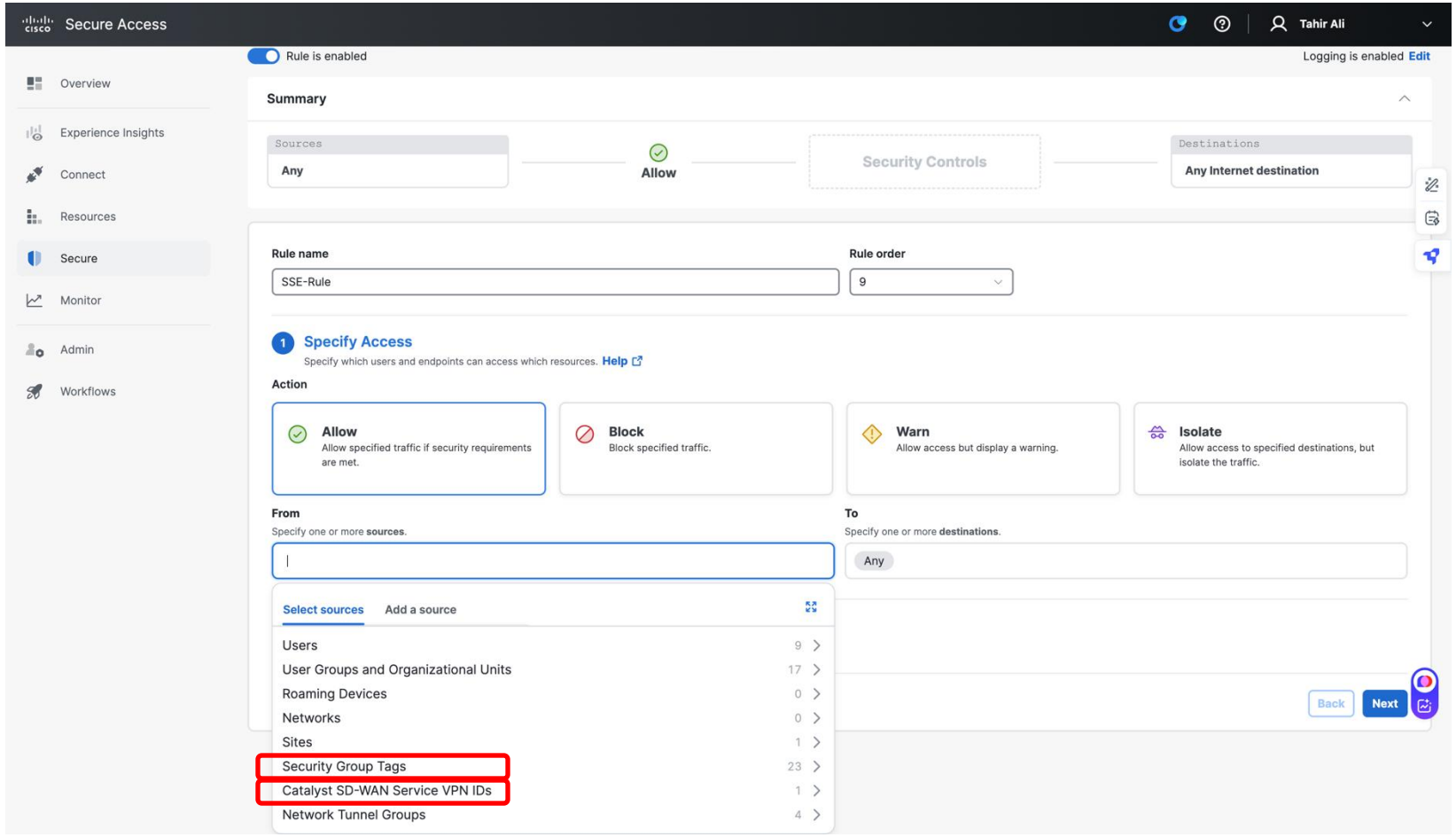


Catalyst SD-WAN Manager GUI – Context共有の設定



- VPN、SGT はそれぞれ個別に有効化可能、同時に有効化も可能
- 有効化後、IPsec のインライン情報として VPN-id/SGT-id inline が転送される

Catalyst SD-WAN：Cisco Secure Accessとの連携



- ソースオブジェクトとして、VPN や SGT が選択可能


CISCO