Monthly Security Webinar

業界唯一に更に進化した、シスコ SSE 最新アップデート

シスコシステムズ合同会社　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
ソリューションズ エンジニア　坂川 健太

2024.6.28

超分散環境が新たな現実に

組織はサイバーセキュリティの脅威に対処する準備が十分でない

セキュリティ・ツールの多さが複雑さを招いているとの報告

IT leaders report that users bypass their current VPN solution

多様な IT ランドスケープがセキュアな接続を困難に

Source: Cybersecurity Readiness Index – Cisco: March, 2023
Source: Keys to Successful SSE, ESG global survey. June 2023
Source: Keys to Successful SSE, ESG global survey. June 2023

既存 SSE における課題とは

1. ゼロトラストとしてのカバレージ（限定的なネットワークの対応にとどまる）
2. 不十分なセキュリティ機能または柔軟ではないセキュリティ機能適用
3. 単一ではないエージェントによるエンドユーザ側での VPN と ZTNA の使い分け
4. ZTNA への移行が困難（ユーザの協力を前提）
5. 進まないアプリケーションのゼロトラスト対応（ VPN でしか救えない実情）
6. ネットワーク（LAN、DC など）と連動しないセキュリティ設計（例：セグメンテーション）
7. 端末と SSE 間のネットワークにおける不可視性と解決手法の不在
8. 買収リスク、値上げリスク

Cisco Secure Access で防御を近代化

ゼロトラストに基づくクラウドネイティブ・セキュリティの融合

Cisco Secure Access とは

実証済みのクラウドネイティブなセキュリティを1つのサービスに集

Umbrella DNS >12 years

Umbrella SWG >5 years

Duo Posture >4 years

Umbrella CASB >5 years

RBI >5 years

ZTNA >4 years

Secure Client >3 years

VPN Termination >10 years

Cloud Firewall >5 years

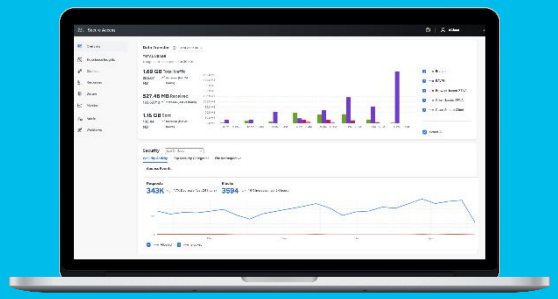
Umbrella DLP >5 years

Umbrella Advanced Malware Protection >7 years

Experience Insights/DEM (ThousandEyes) >3 years

70,000 社以上のお客様を保護 | 2億2000万以上のエンドポイント

Cisco Secure Access



- シングルコンソール
- 単一クライアント
- 統一ポリシー

コンソール、ポリシー、
クライアントの統一

高度なゼロ・トラス
ト・プロテクション

優れたユーザー
体験

Cisco
Secure Access

業界をリードする
SSE

ITオペレーション
の簡素化

セキュア インターネット アクセス

セキュア プライベート アクセス

AI による脅威の防御と管理

ユーザーにとってよりよい

シームレスなアクセス経験

ユーザーからアプリへのシームレスなゼロ・トラスト

ステップ 1
ログイン

ステップ 2
安全に仕事を開始

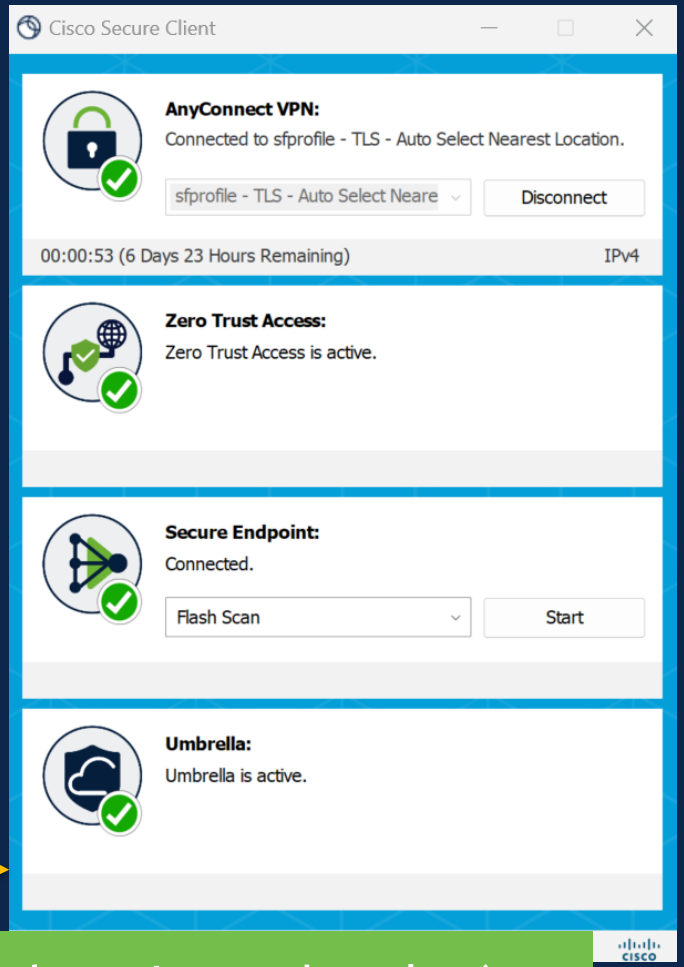
コネクティビティ、アクセス・コントロール、セキュリティはお任せください

ユーザは最小限の手間で仕事を開始

Cisco Secure Client

一連のセキュリティ・サービス実現モジュール

- AnyConnect VPN (Core)
- ZTA Module
- Secure Endpoint (AMP)
- Roaming Module
- Thousand Eyes (No UI)
- Cloud Management Module (No UI)
- Diagnostic and Reporting (DART)

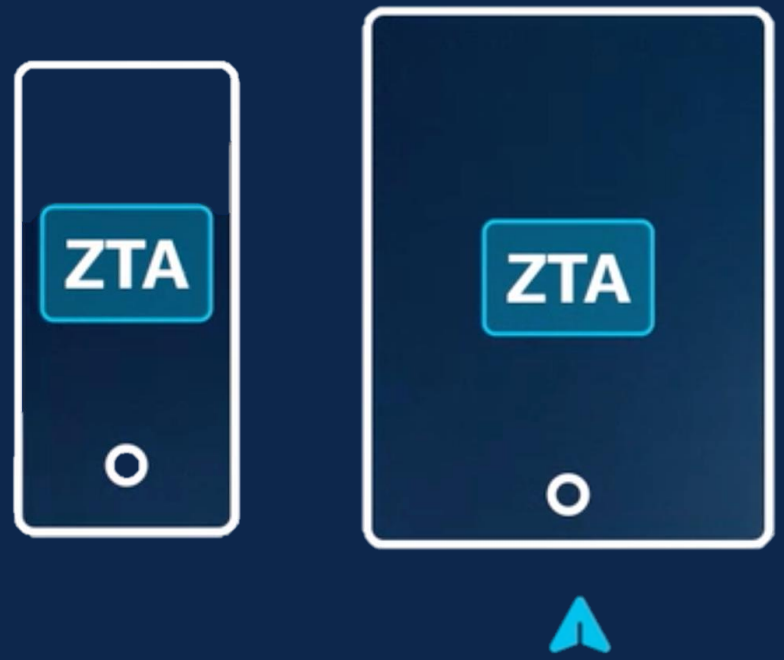


一つのエージェントで VPN、ZTNA からインターネット セキュリティまでカバー

モバイルデバイスでのシームレスでセキュアなアクセス

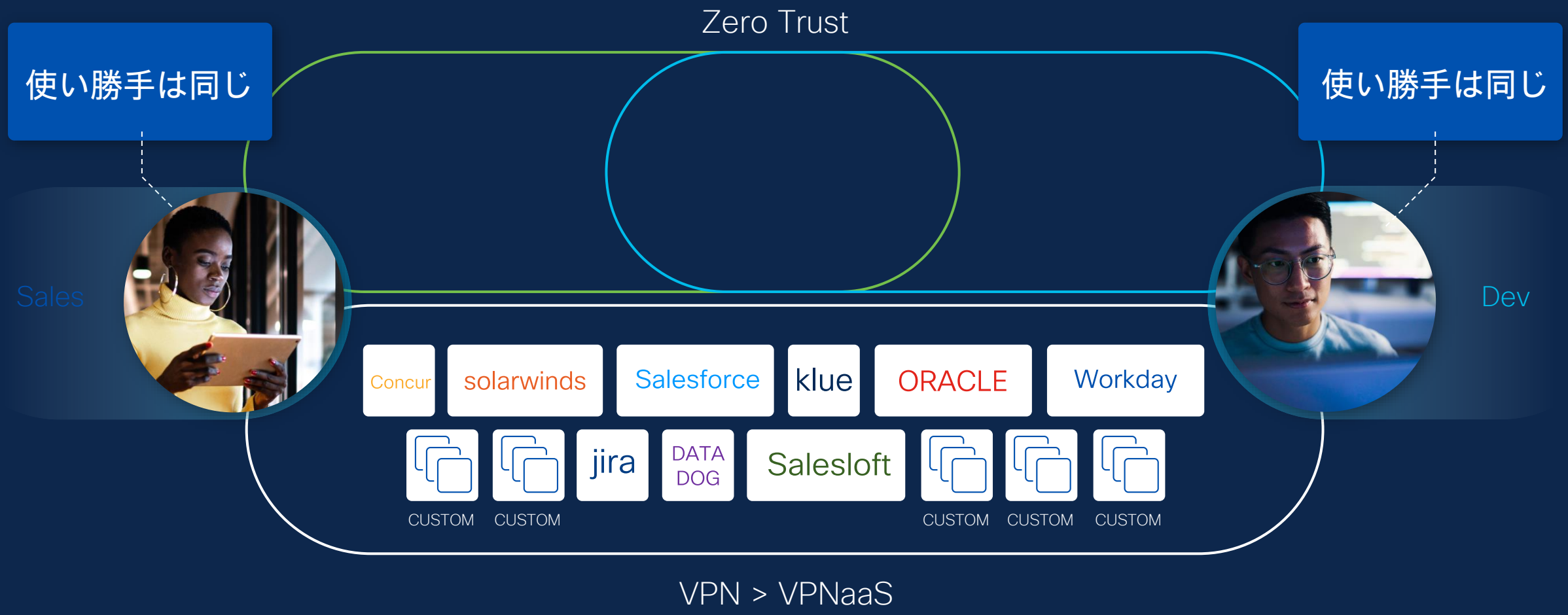
シスコと大手モバイルプロバイダーが共同で、業界初のモバイル機器向けゼロトラスト・アーキテクチャを開発

Apple 社および Samsung 社に対応



モバイルデバイスからのシームレスなプライベート アプリ アクセス

ゼロトラストへの道のりを簡素化



IT 管理者にとって使いやすく

単一のクラウドプラットフォームにおけるセキュリティの融合

トラフィックの把握、リスク分析、アクセス管理

シングル コンソール

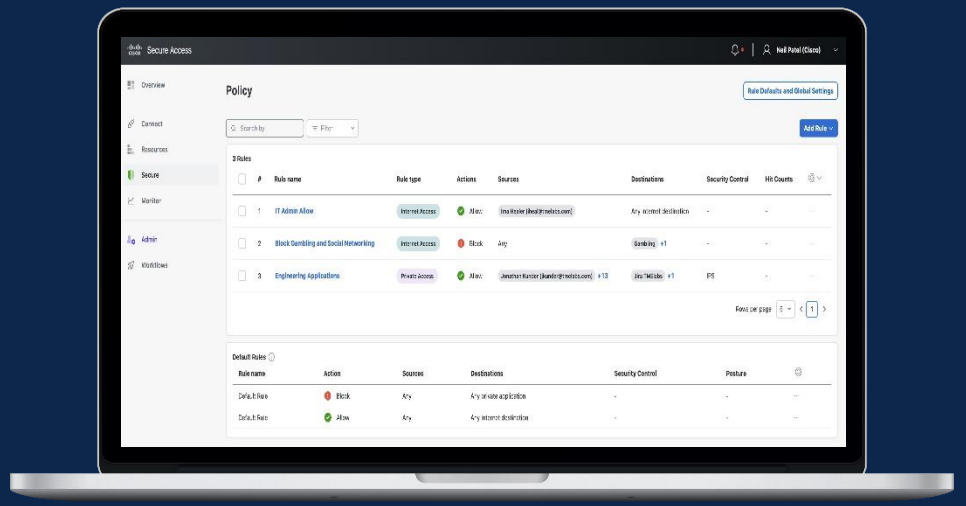
統合ポリシー管理
全体的な脅威の可視化
集約されたレポート

ユニファイド エージェント

シームレスなユーザー体験
オンボーディングの迅速化
メンテナンスの合理化

シングル サブスクリプション

ベンダー/ライセンスの統合
展開の最適化
コスト効率化

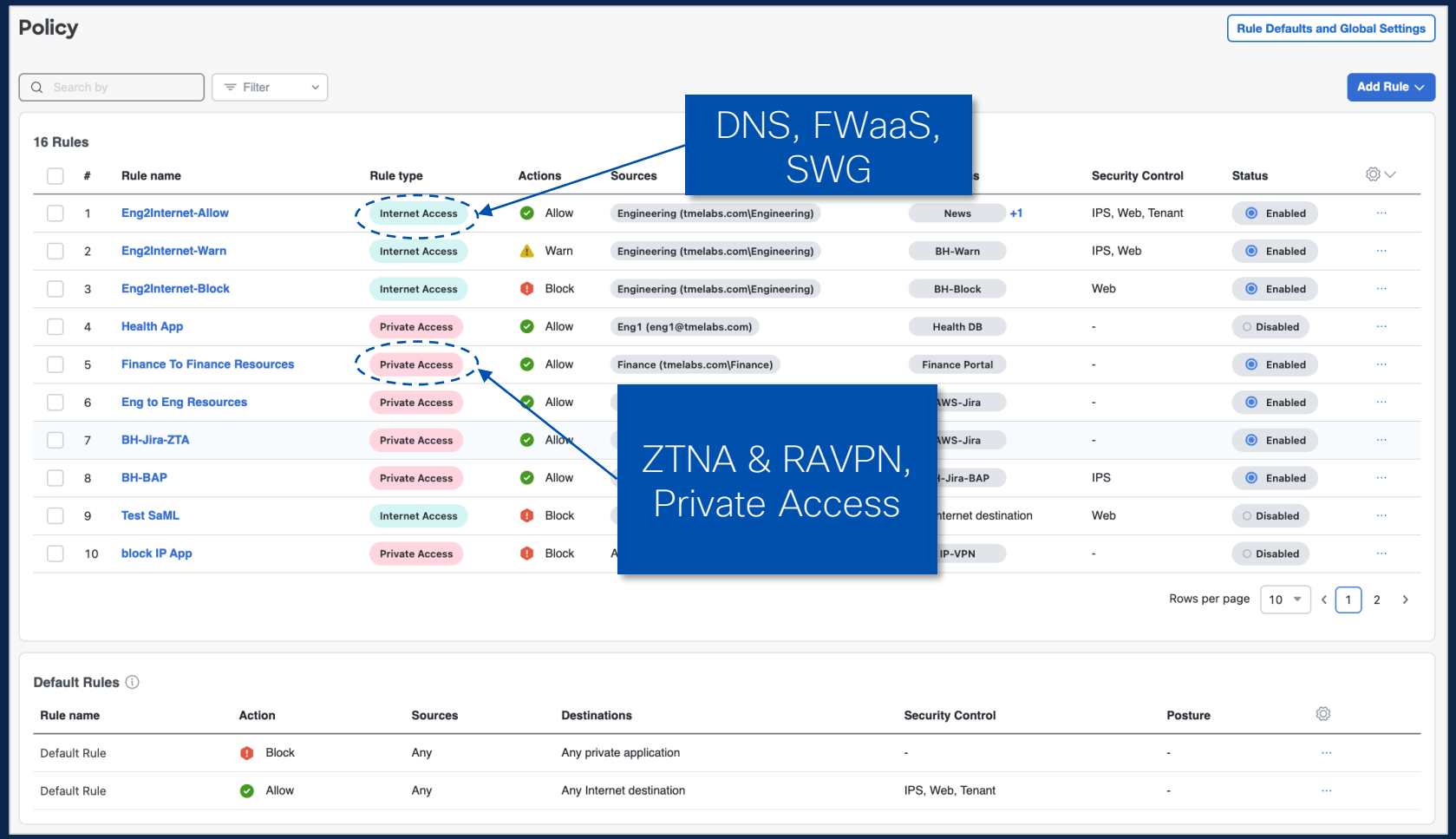


クラウドセキュリティの統合によるコスト削減と効率性の向上

ユニファイド ポリシー

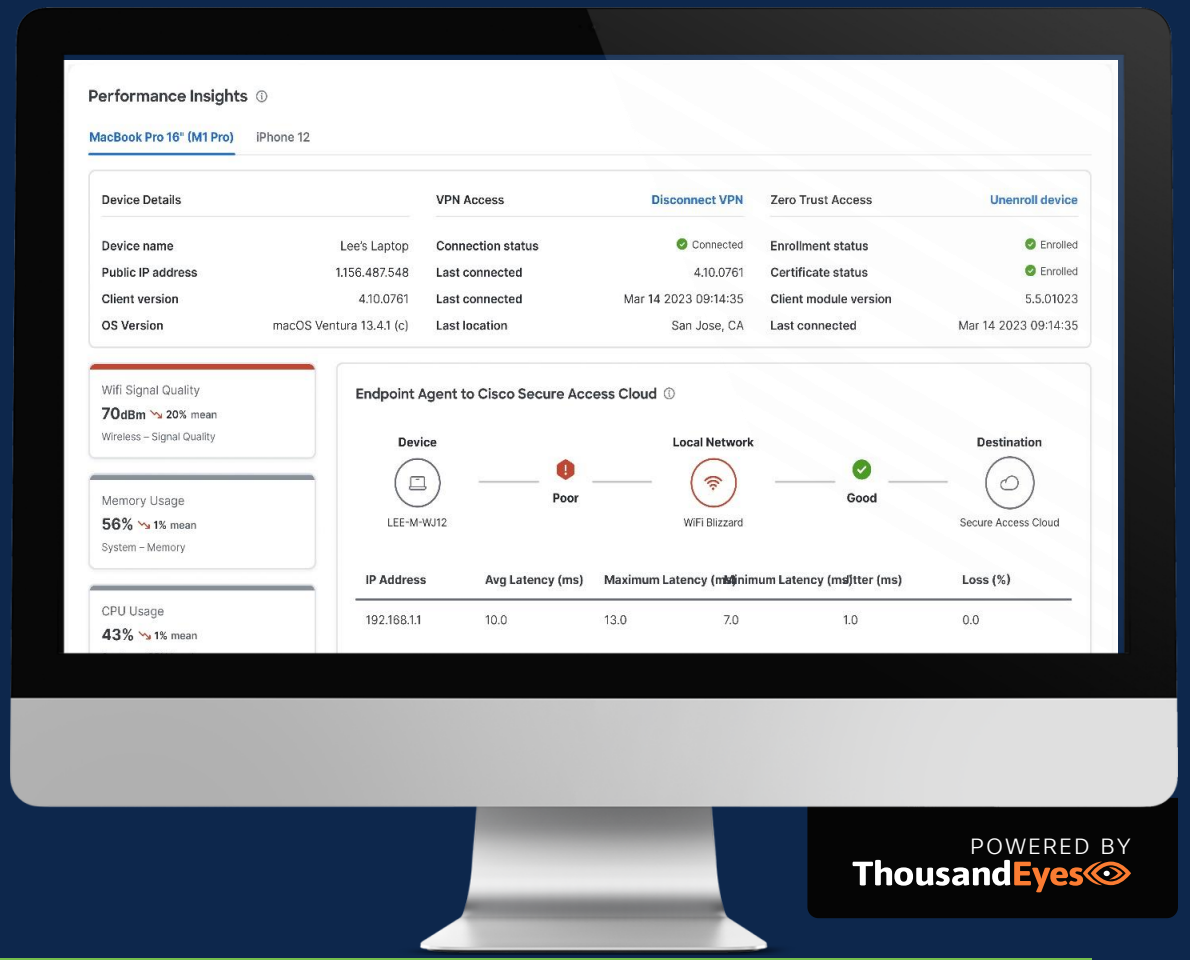
インターネットからプライベート アプリケーション アクセス までまとめてポリシーを設定・管理

- SSE のポリシーは以下のように構成
  - パブリック・インターネット/SaaSアクセス・コントロール・ポリシー
  - プライベート・アクセス・コントロール・ポリシー
- 各ルールには明示的な「ルール・タイプ」が定義付けされ、ポリシー設定を統一したビュー
- ルールは各実施エンジンで順番に評価



エクスペリエンス インサイト

- エンドポイントのパフォーマンス – CPU 、メモリ、Wi-Fi
- ネットワーク・パフォーマンス – エンドポイントと Secure Access 間
- SaaSアプリケーション・パフォーマンス（トップ20）
- ビデオおよびテキスト（UCaaS）のパフォーマンス・モニタリング
- ユーザー固有のイベント



POWERED BY ThousandEyes

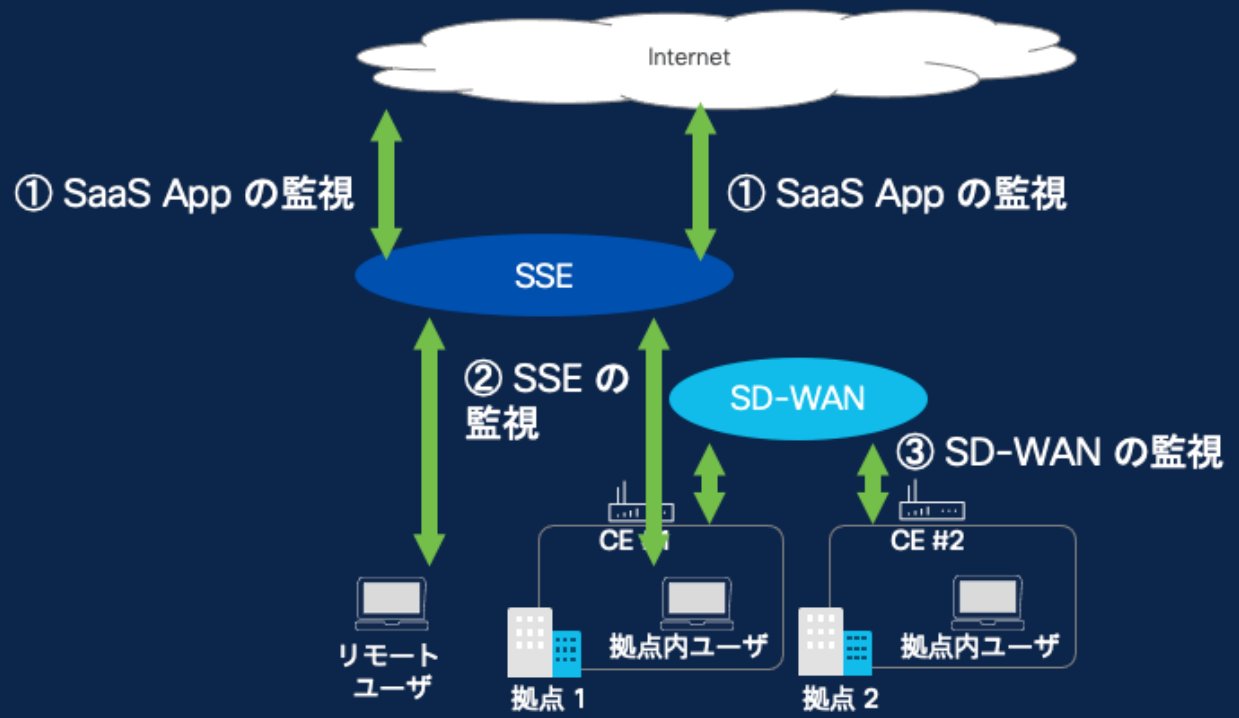
ユーザーからアプリケーションへのアクセスの健全性とパフォーマンスを監視

Dashboard visual is for illustrative purposes only

Endpoints Performance

All | Unhealthy | At risk | Healthy

ご参考）シスコ SASE に含まれる監視



cisco ThousandEyes

User name

Anna Mariano

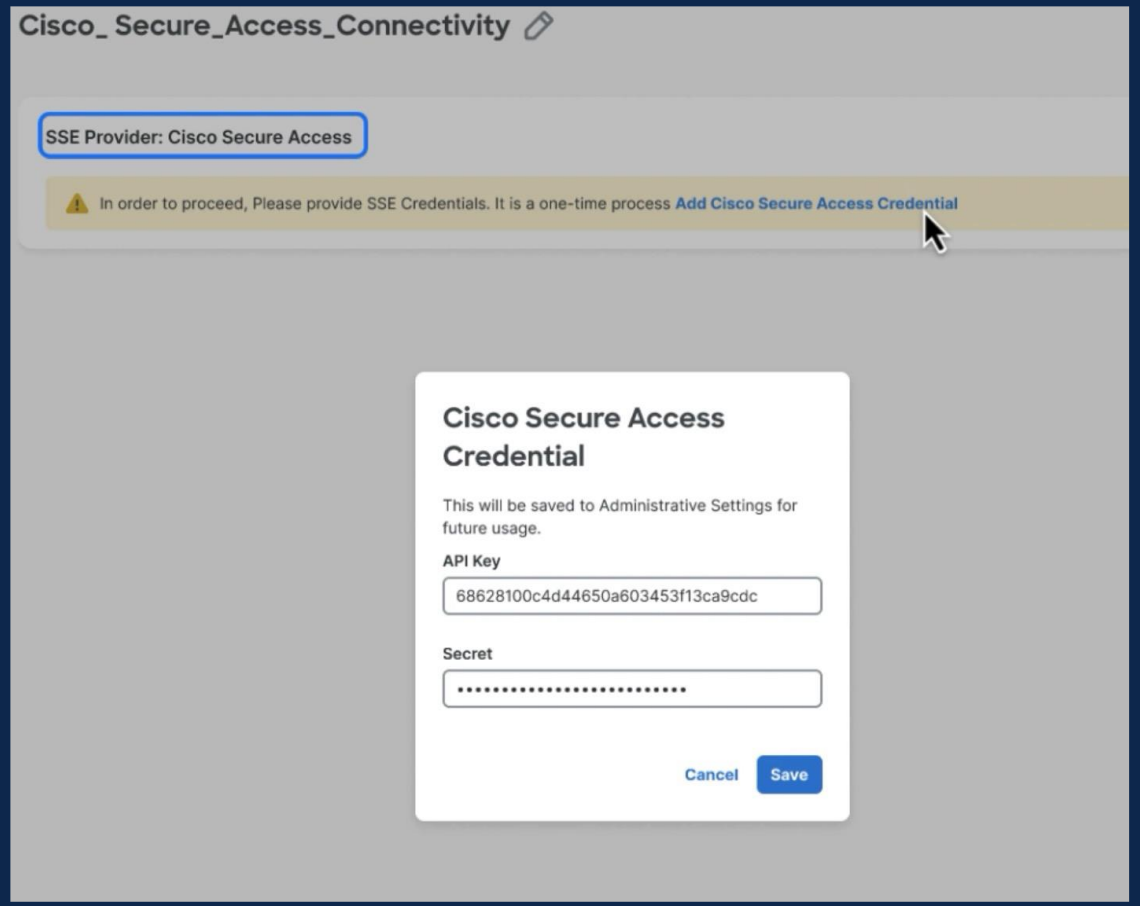
Karah Thornton

Ryan Campbell

Google Workspace	workspace.google.com	44 ms	200	OK	Feb 4, 2024 4:46PM	US (Pacific North

SDWAN – Secure Internet Access

簡単なステップでセキュアなブランチ・アクセスを実現



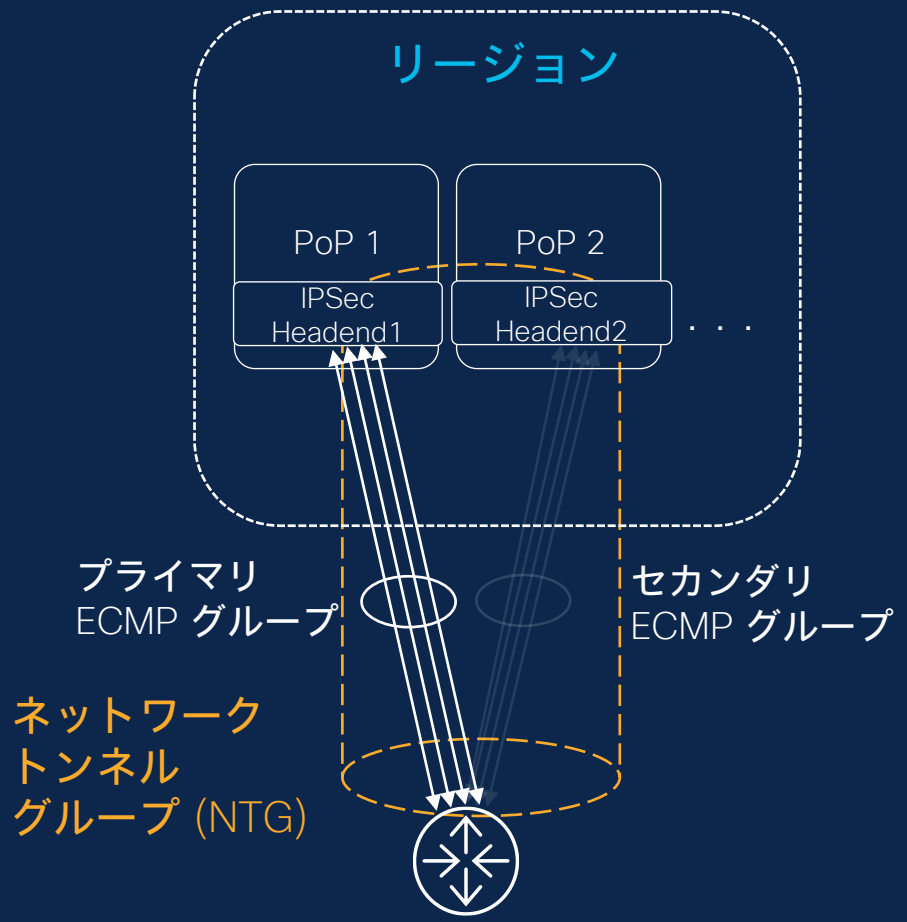
ブランチを Cisco Secure Access に接続し、セキュアなインターネット・アクセスを実現

機能:

- Catalyst SD-WAN によるトンネルの自動化
- トンネルのグループ化による帯域幅の拡大
- vManage ダッシュボードへの組み込み
- すべてのデバイスで一貫したインターネット・セキュリティ・ポリシー
- ネットワーク・セグメントベースのポリシーと ISE タグ

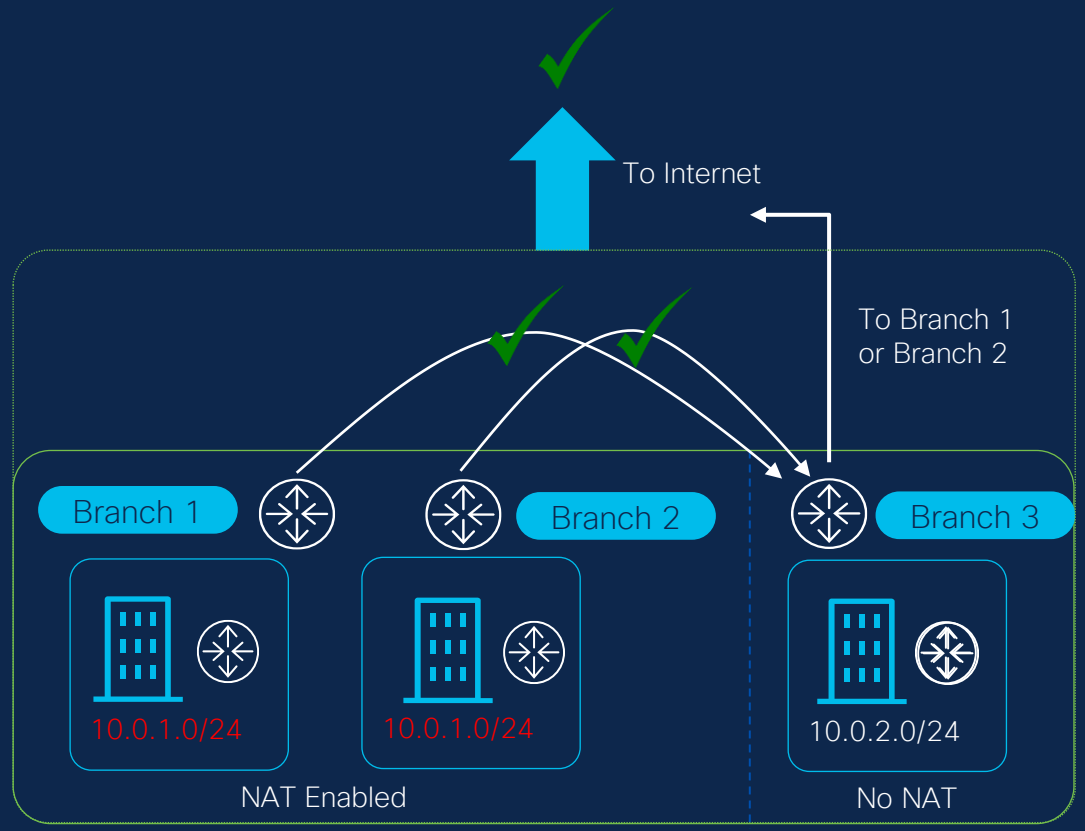
ECMP による拡張性と IP オーバーラッピング対応

ECMP によるネットワーク拡張性



お客様環境に設置のルータ

IP オーバーラッピング対応



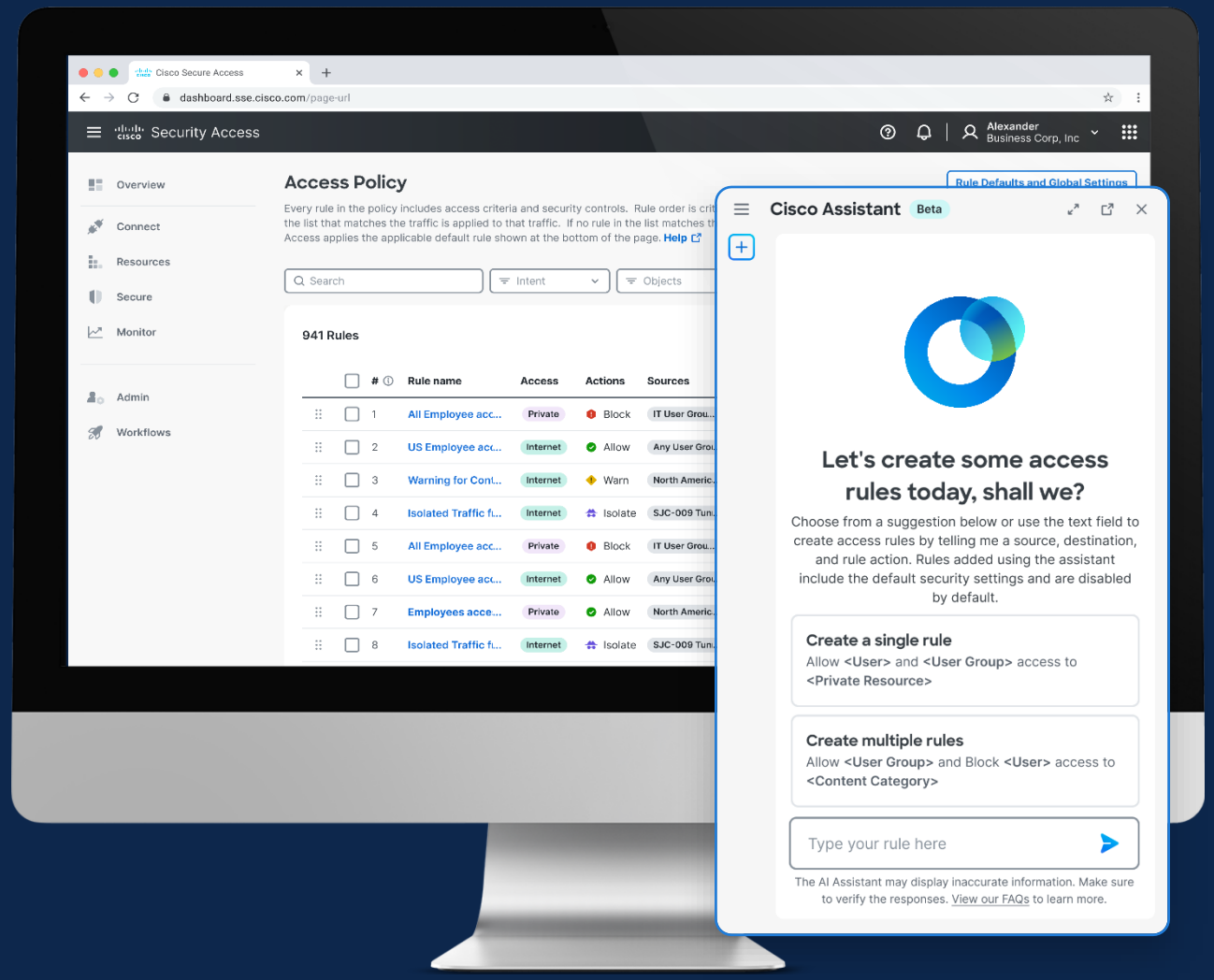
セキュアアクセスにおけるシスコ AI アシスタントの導入

生成 AI の自然言語で構築:

ポリシー管理の簡素化とスピードアップを最大 70% 実現

人的ミスの削減

業務効率の向上



Dashboard visual is for illustrative purposes only

誰にとってもより安全

現代のゼロ トラスト エンフォースメント

Cisco Secure Access 機能

基本のセキュアサービスエッジ（SSE）の一歩先を行くサービスで快適な接続を実現しビジネスを強力に保護

基本となる SSE

- セキュア Web ゲートウェイ（SWG）
- クラウド アクセス セキュリティ ブローカ（CASB）と DLP
- ゼロトラスト ネットワーク アクセス（ZTNA）
- サービスとしてのファイアウォール（FWaaS）と IPS

＋

シスコは基本の機能も追加の機能も 1 つのサブスクリプションで提供

- DNS セキュリティ
- マルチモード DLP
- 高度なマルウェア防御
- サンドボックス
- Talos 脅威インテリジェンス
- サービスとしての VPN
- エクスペリエンス インサイト
- リモートブラウザ分離

シスコ独自のゼロトラスト アクセス

高いパフォーマンス

ネットワーク・アクセラレーションによる高速接続

OSに組み込まれたゼロ トラスト アプリへの即時アクセス

次世代インターネットプロトコルによる低遅延

より強固なセキュリティ

アイデンティティを認識するプロキシでネットワークを防御

より深いマイクロセグメンテーションによるラテラル ムーブメントからの保護

プライベート・アプリケーションの詳細の漏洩を防止

ハイパフォーマンスと高度なセキュリティを両立

Cisco Talos 脅威インテリジェンス

専門家、データ、
Gen AI を活用した、
脅威の全体像に対す
る比類なき可視性

550B セキュリティ イベント /日

~9M ブロックされた電子メール /時

~2,000 あらたなサンプル /分

~2,000 ドメインをブロック /秒

Secure Access: AI の利用を安全に

AI 利活用に際し出入りする知的財産の保護

脅威の可視性	漏洩防止	脅威の予防
アクティビティーの発見と評価	プロンプトもアップロードも検査 (DLP)	アプリのブロックとダウンロードの制御

70 以上の生成 AI アプリ（API を含む）を発見し、コントロール

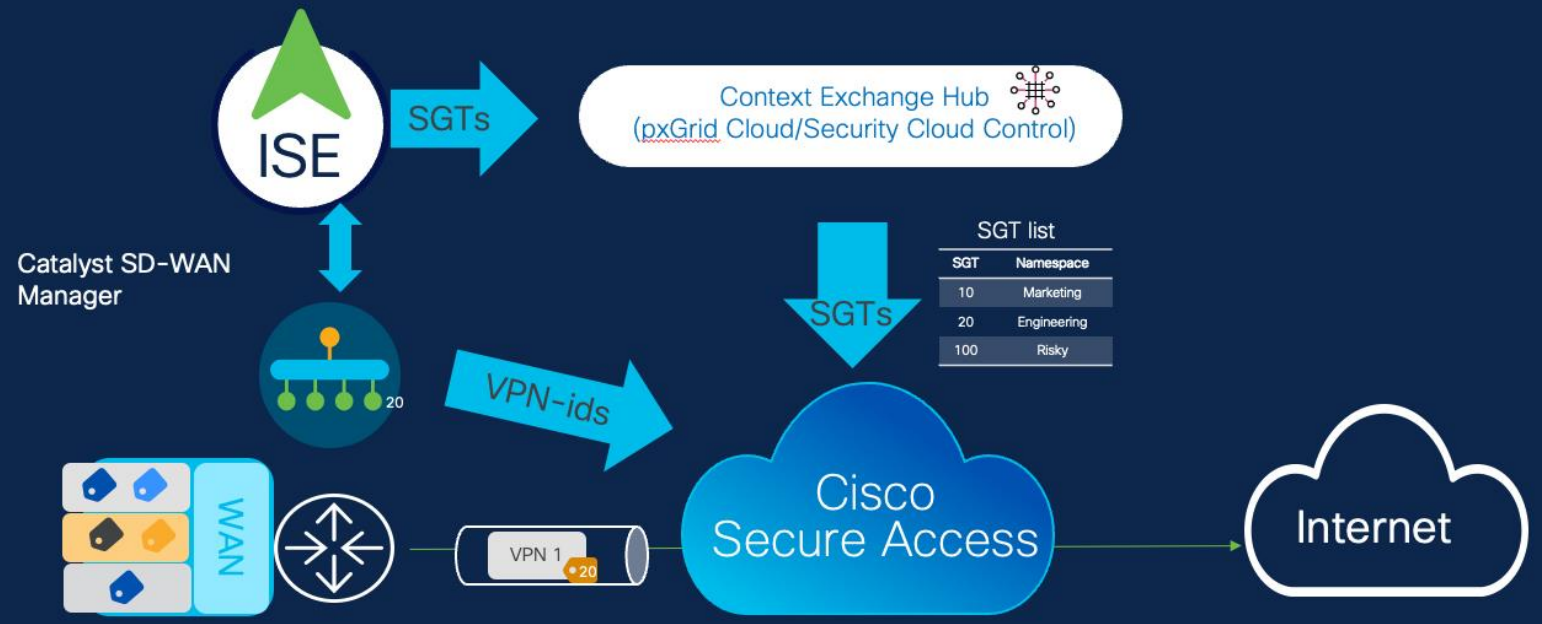
増え続ける AI 活用に安心をご提供

最近の発表とロードマップ

1.	Reserved IP for Roaming Users	EFT in May
2.	Mobile ZTA for iOS and Android	Released in May
3.	Chromebook support (DNS, SWG) for Internet Access	EFT in May
4.	Cisco SD-WAN Integration for Private Access	
5.	ISE-RADIUS for RA-VPN (AAA, Change of Authorization(COA), Posture)	Released in Mar
6.	ISE Integration for Security Group Tagging (TrustSec integration with LAN/Cloud)	Phase 1 EFT in May
7.	Unique IP pool Assignment per VPN profile	
8.	IPv6	
9.	AI Assistant	Phase 1 release in May
10.	API	Phase 1 release in May

Catalyst SD-WAN / Secure Access / Cisco ISE 間でコンテキスト共有してインターネット アクセスをセキュアに

1. Catalyst SD-WAN ブランチから発信されるインターネット接続トラフィックを保護
2. Catalyst SD-WAN は Cisco ISE と連携して、ネットワークコンテキスト（ISE Security Group Tags[SGT] および SD-WAN VRF/VPN） を Cisco Secure Access と共有
3. Cisco Secure Access は、これらのネットワークコンテキストに基づいてポリシーを適用できるようになり、SD-WAN のブランチユーザーからインターネットに接続されたトラフィックを保護
4. ISE SGT を使用することで、ポリシー施行のためにトラフィックをマイクロセグメント化可能



セグメンテーションされた環境に対するセキュアなインターネットアクセス

Cisco Secure Access パッケージ概要

リモート プライベート アクセスとダイレクト インターネット アクセスの個別のユーザ数

Cisco Secure Access Advantage

Essentials パッケージのすべての機能に加え

レイヤ 7 ファイアウォール、IPS、DLP、RBI（レベル All）、無制限サンドボックスなど*

Cisco Secure Access Essentials

Base パッケージ

安全なインターネットアクセス、安全なプライベートアクセス、SWG、ZTNA、レイヤ 3 および 4 のファイアウォール、CASB、RBI（レベル Risky）など

- ユーザー単位のライセンス
- サブスクリプションの期間
  - 1、3、5 年間のサブスクリプション
  - 契約別の非標準契約

* Private Access の DLP については以降のリリースにて対応予定

SSE および ZTNA のリーダーとして認定

FORRESTER®

Rated as Strong
Performer in Forrester
2024 SSE Wave

Gartner Peer Insights™

SSE Category 2024
4.4/5 Rating

Customer Value Leader
Global Security Services Edge

FROST & SULLIVAN
2024 BEST PRACTICES AWARD

OVERALL LEADER

ZTNA Overall Leader Award
KuppingerCole 2024

PeerSpot No.1 Ranked

Rated First in
CASB, SWG, DNS
Internet Security

Secure Access お客様事例

グローバル製造・販売会社

お客様プロフィール

- 創業 100 年以上
- 従業員 10 万人以上
- 売上高 1,500 億ドル以上
- 数十の主要ブランド

顧客ニーズ

- 即時のゼロ トラスト構想
- 完全で柔軟な SSE パスへの要望
- ベンダーの統合
- きめ細かな最小権限制御
- 効率的なリモート ユーザ エクスペリエンス
- 管理の簡素化
- IPS と RBI

シスコを選んだ理由

- セグメンテーションを強化でき、ラテラルムーブメントを防止
- ユーザー単位、アプリ単位のゼロトラスト接続
- ユーザーと管理者の利点を実証
- 請負業者向けのクライアントレス ZTNA
- IPS と RBI を含む

競合他社製品に対する評価結果

A 社 :インターネットとプライベート・アクセスで複数のダッシュボードとインストール。古い ZTNA アーキテクチャ
高価格 で多くのアドオン。
B 社 : 設定が難しい。古い VPN サービスのアプローチ。

Secure Access お客様事例

大規模病院

お客様プロフィール

- 大学医学部の教育病院
- 700 床以上
- 職員 80,000 人以上
- 年間患者数数万人
- 年間数千億円の研究
- 年間売上 1 兆円以上

顧客ニーズ

- 幅広いセキュリティ機能
- ベンダーの統合
- 信頼性の高い拡張性
- 柔軟な導入オプション
- セキュリティの有効性
- 機能横断的な効率的なセキュリティ管理

シスコを選んだ理由

- 統一契約 ネットワーク /SD-WAN & セキュリティ
- コスト削減
- 単一の SSE ダッシュボードとポリシーエンジン
- 導入と運用の効率化
- 実証済みのセキュリティ性能

競合他社製品に対する評価結果

A 社 : インターネットとプライベート・アクセスの分離、契約の柔軟性に欠ける、高額な料金設定
B 社 : リバース・プロキシ・アプローチで遅く、設定も複雑

Secure Access お客様事例（その他）

製造業	従業員 7,000人以上 シスコ・セキュア・アクセスに完全移行した最初のお客様	重視した点： 単一のモジュール型 Cisco Secure Client によるエンドポイントエクスペリエンスの統合機能	シスコの差別化ポイント： エンド・ツー・エンド・ポートフォリオと、Cisco XDR との強固な統合
ヘルスケア	従業員 60,000人以上 エレベート オファーを利用して Umbrella SIG からのアップグレード	重視した点： 既存のインフラとセキュリティへの投資を活用できる	シスコの差別化ポイント： 強固なセグメンテーションを可能にする ISE との統合
公安	10,000 人以上 優先セキュリティベンダーによるゼロ・トラスト戦略の強化を検討	重視した点： ノートパソコンと iPhone むけに従来の VPN サービスからの移行に際し、低リスクでスピーディーな展開が可能	シスコの差別化ポイント： ネットワーキングとセキュリティのエンド・ツー・エンドを対象にする、Cisco SD-WAN と ISE との統合

既存 SSE における課題を解決する Secure Access

1. ゼロトラストにおいて重要と言える広範なカバレージ
2. 十分なセキュリティ機能に加え、柔軟なセキュリティ機能適用
3. ユニファイドエージェントによりエンドユーザ側での VPN と ZTNA の使い分けは不要
4. ZTNA への移行がスムーズ（ユーザの協力は基本的に不要）
5. 長期的なアプリケーションのゼロトラスト化に合わせて ZTNA と VPN の両方を標準で提供
6. ネットワーク（LAN、DC など）と一貫性のあるセキュリティ設計（例：セグメンテーション）に対応
7. 端末と SSE 間、SSE と 著名な SaaS間における詳細経路可視化と解決手法の提供
8. 値上げを前提とせず、安心して長期的に利用可能

機能だけではない！
シスコ SASE (SSE + SD-WAN) をご採用頂くメリット

	Cisco (SD-WAN + Secure Access)	他社
1. 各拠点の展開工数 (機器設置、設計)	◯ (設置、設計、設定工数小)	△
2. 大規模拠点における設計の柔軟性	◯ (ECMP 対応)	△
3. SSE のメンテナンスによる影響	◯ (無し)	△ (経路の手動切り替えが必要)
4. SSE のスケールアップ時における影響	◯ (無し)	△ (停止を伴う)
5. SASE 横断的な通信経路の可視化	◯ (標準対応)	△
6. モバイル デバイス対応	◯ (追加コスト無し。Apple 社および Google 社との開発連携。)	△ (モバイル用ライセンスが必要。)
7. 特別支援体制 (プレミアム サポート)	◯ (日本語および英語)	△ (英語)
8. TAC	◯ (日本および海外で受付可)	△ (海外のみ)
9. SSE + SD-WAN 障害時の対応	◯ (シスコ)	△ (2 社以上の TAC へケースオープン必要)

Demo

DLP
ChatGPT からの保護の例

Cisco Secure Access | ChatGPT

dashboard.sse.cisco.com/org/8206399/overview

Secure Access

Kenta Sakagawa

- Overview
- Experience Insights
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

Connectivity

Last 24 Hours

Network tunnel groups 23 total

- 12 Disconnected
- 6 Warning
- 5 Connected

Resource connector groups 5 total

- 3 Disconnected
- 2 Connected

Data Transfer

Last 24 Hours

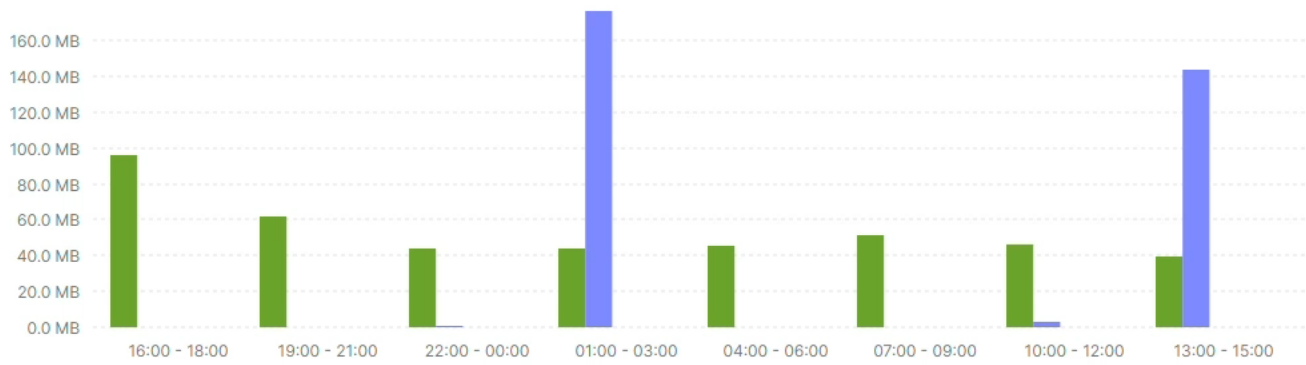
TOTAL USAGE

Usage data - delayed up to 30 min.

753.84 MB Total traffic
234.95 MB Decrease (last 24 hours)

106.62 MB Received
27.50 MB Decrease (last 24 hours)

647.23 MB Sent
207.46 MB Decrease (last 24 hours)



AI Assistant
アクセスポリシーの作成

Overview
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows

Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

Connectivity

Last 24 Hours

Network tunnel groups 23 total

- 12 Disconnected
- 6 Warning
- 5 Connected

Resource connector groups 5 total

- 3 Disconnected
- 2 Connected

Data Transfer

Last 24 Hours

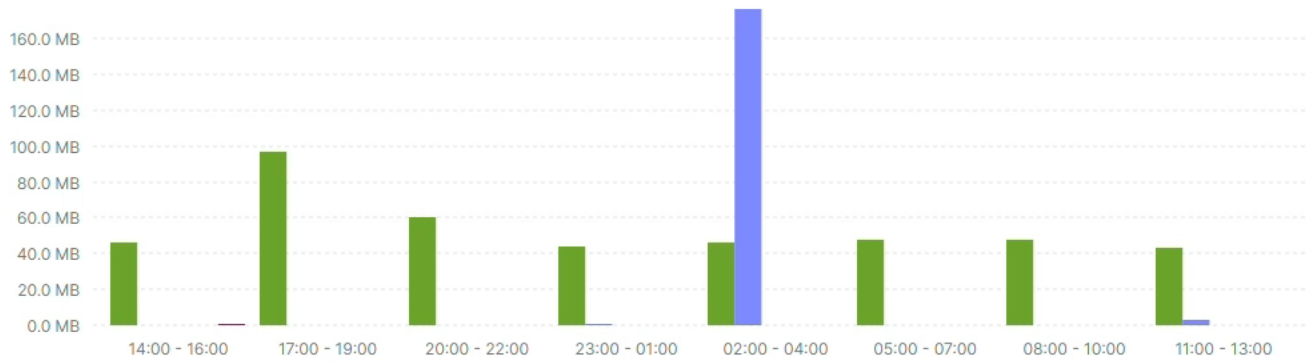
TOTAL USAGE

Usage data - delayed up to 30 min.

614.80 MB Total traffic
380.20 MB Decrease (last 24 hours)

100.75 MB Received
31.79 MB Decrease (last 24 hours)

514.05 MB Sent
348.41 MB Decrease (last 24 hours)



API
接続先リストの編集
(応用編)

Overview
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows

Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. **Help**

Connectivity

Last 24 Hours

Network tunnel groups 21 total

- 10 Disconnected
- 5 Warning
- 6 Connected

Resource connector groups 4 total

- 2 Disconnected
- 2 Connected

Data Transfer

Last 24 Hours

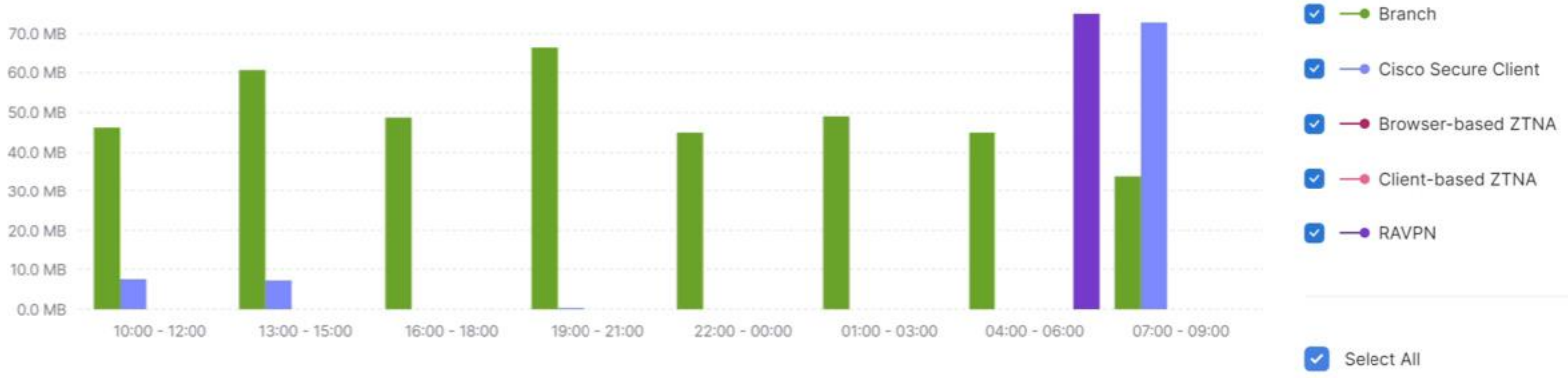
TOTAL USAGE

Usage data - delayed up to 30 min.

558.63 MB Total traffic
671.10 MB Decrease (last 24 hours)

117.29 MB Received
90.63 MB Decrease (last 24 hours)

441.34 MB Sent
580.47 MB Decrease (last 24 hours)



Security

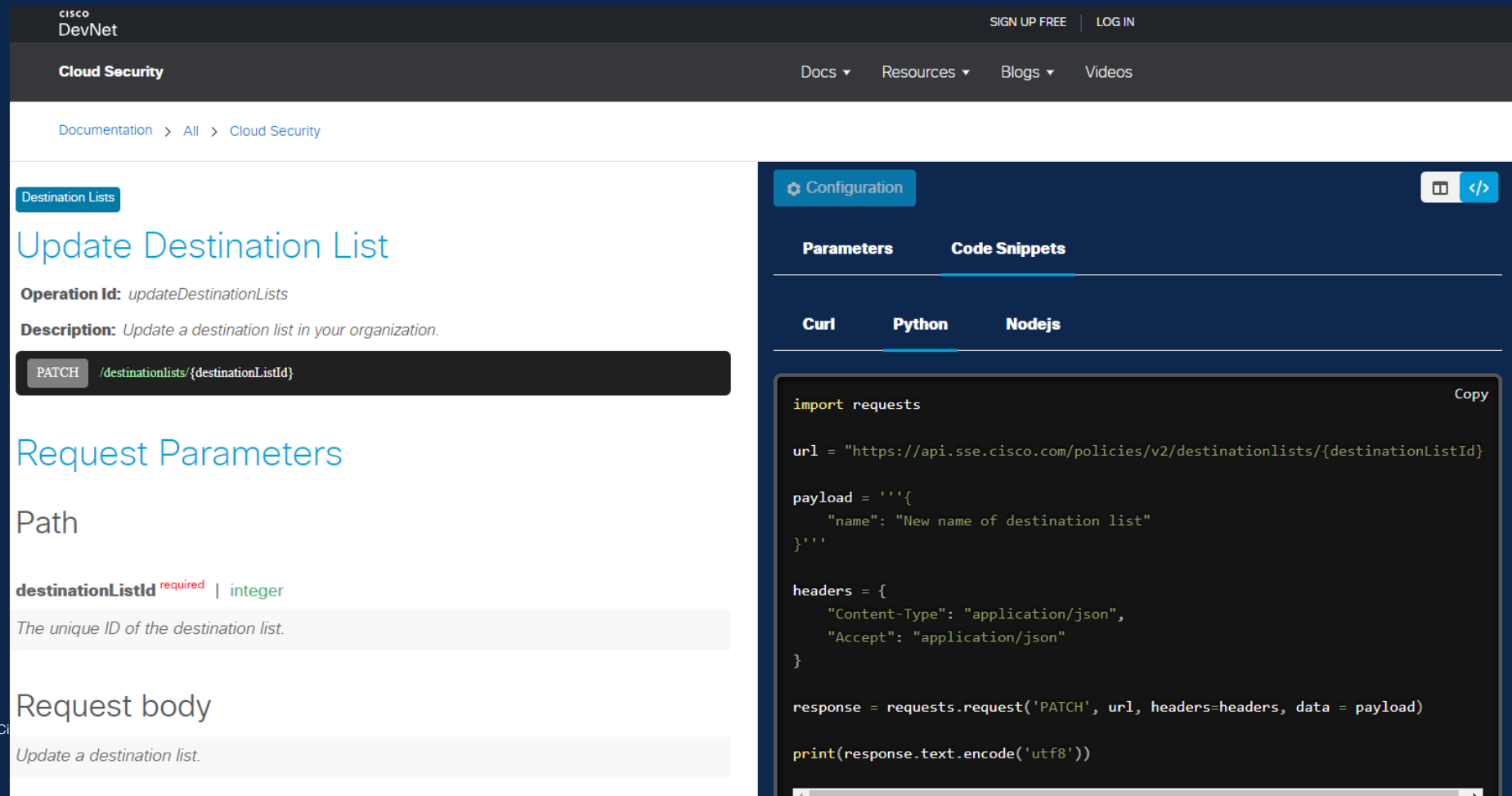
Last 24 Hours

Security Activity | Top Security Categories | File Retrospective

Cisco Secure Access API で接続先リストを編集するステップ

1. Cisco Secure Access 管理ダッシュボードよりAPI Key + Key Secret を作成します
2. API Key + Key Secret より Authorization Token を作成します
3. 接続先リスト ID を取得します
4. 接続先リスト ID を指定して、該当接続先リストに任意の宛先を追加します

Cisco Secure Access API Document




CISCO