SD-WAN セキュリティ

シスコは、WAN 全体で、ユーザ、接続されたデバイス、アプリケーションの使用、およびすべてのトラフィックを保護します。

ビジネスは WAN で実施され、収益の 90% を生み出します。成長を加速するために、ブランチやリモート ユーザ、デバイスをデジタル化し、ネットワークのアーキテクチャを再構築して、WAN を直接インターネットやマルチクラウド アプリケーションに接続しようとしています。

お客様が WAN を保護する戦略は 3 つあります。ビジネスがインターネットに直接接続されている場合、もしくはその予定がある場合、ブランチからクラウド エッジに至るまでのセキュリティ スタックが必要となります。

1

WAN バックホール

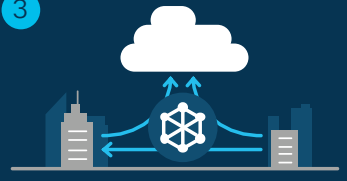
データセンターのエッジにおける既存のセキュリティ スタックにより、すべてのブランチ　ユーザ、接続されたデバイス、アプリケーションの使用をカバーします。

2

セキュリティの向上

一部のゲスト ユーザもしくはすべてのユーザ、O365 などの一部のアプリまたはすべてのアプリによる既存のダイレクト インターネット アクセス（DIA）ブレークアウトを保護しているセキュリティ スタックを更新したり、レイヤを追加したりします。

3



ソフトウェア定義型（SD）WAN およびセキュリティの導入

数十から数千箇所に及ぶ拠点において、新しい DIA ブレークアウトによってブランチを変革し、セキュリティとパフォーマンスの向上、シンプル化、コスト削減を実現します。

すべてのセキュリティ リスクを軽減

SD-WAN ベンダーの 90 % 以上は、従来のセキュリティ ベンダーではありません。

内部から外部
マルウェア感染 コマンド & コントロール フィッシング攻撃不正利用

内部
不正アクセス 水平移動 コンプライアンス違反

外部から内部 *
不正アクセス サービス妨害攻撃

* オンサイト サービスやデバイスにリモートからアクセス可能

始めるには

1. どんな WAN トポロジでも、Cisco Umbrella のセキュア インターネット ゲートウェイによって、クラウド エッジのセキュリティが向上し、場所を問わずにユーザが保護されます。
   詳細：cisco.com/jp/go/umbrella
   トライアル：signup.umbrella.com

2. ブランチ エッジと SD-WAN ファブリックを保護するための単一のエッジ デバイスを求めている、予算が限られた IT チームには、Cisco Meraki™ MX が最もシンプルな方法です。**詳細：**cs.co/MX-fw-sdwan [英語]
   デモ/トライアル：cs.co/MX-demo [英語]

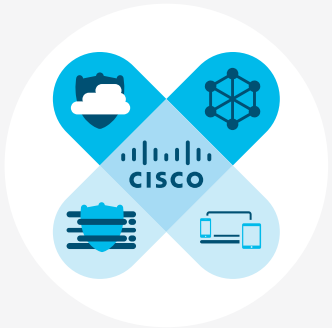
3. 複雑な WAN トポロジの対応力を最大化したいネットワーク チームには、Cisco SD-WANが最も柔軟な方法です。
   詳細：cisco.com/jp/go/sdwan

4. 業界トップクラスのシンプルさを多要素認証に求めているセキュリティ チームには、適応型のリスクベース アプリケーション アクセス ポリシーに対応した拡張可能な単一プラットフォーム経由での Cisco Duo コア コンポーネントの導入をお勧めします。
   詳細：duo.com [英語]
   トライアル：demo.duo.com [英語]

シスコのオープンな統合 SD-WAN セキュリティ アーキテクチャ

セキュア インターネット ゲートウェイ
すべてのポートを脅威から保護し、インターネットやマルチクラウド アプリケーションへの安全なアクセスを実現します。

エッジ ファイアウォールの柔軟性
次世代ファイアウォールまたはエンタープライズ ファイアウォールのオプションでオンサイト サービスやデバイスを保護し、コンプライアンスを遵守します。



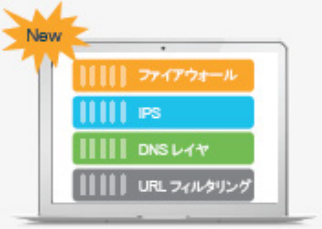
SD-WAN
クラウドによるクラウドのための柔軟かつセキュアな接続および迅速な運用を実現し、アプリケーション パフォーマンスを保証します。

ユニファイド アクセス セキュリティ
ユーザやデバイスの信頼性に基づいて、すべてのアプリケーションに、時間や場所を問わずにアクセスできます。

シスコのソリューションによって、ブランチからクラウド エッジに至るまで、隙のない安全なブランチ変革が実現します。

クラウド エッジ全体のセキュリティ
セキュアなインターネット ゲートウェイおよび**ユニファイド アクセス セキュリティ**によって外部からのセキュリティ リスクを軽減

シン、リッチ、または フルスタック ブランチエッジ
シンプルで柔軟な SD-WAN オプションで内部のセキュリティ リスクを軽減



セキュリティの有効性とネットワークの対応力向上を同時に実現

マルチベンダー ソリューションとは異なり、Cisco® Talos™ 脅威インテリジェンスを利用したシスコの脅威検知は、業界でトップクラスのスピードを誇ります。シスコの保護は、Cisco Umbrella™ の統計モデルおよび機械学習モデル、高度なマルウェア防御（AMP）のファイル レピュテーションおよび動的分析を活用して、常に学習・適応します。

ユーザ エクスペリエンスとビジネス継続性の両立

適切な導入事例が少ない新興企業とは異なり、シスコは、毎日 9,000 万超のユーザに使用されている、スピードと信頼性に優れたインフラストラクチャを構築しています。シスコのセキュア インターネット ゲートウェイによって 100 % のビジネス稼働時間を保証し、シスコの SD-WAN によってあらゆるアプリケーションの停止ゼロを保証します。

変革力

クラウド提供型のセキュリティ
効果的に学習・適応し、攻撃発動箇所を保護

インテントベースのネットワーク
継続的に学習・適応し、アプリケーション パフォーマンス問題を予防

高度な分析
アプリケーションの QoE モデルと脅威インテリジェンスによって、ビジネスや IT に関するインサイトを獲得

柔軟性

エッジ セキュリティ フルスタック
外部から内部、内部から外部、内部のセキュリティ リスクに対応するレイヤ 3 ～ 7 のポリシーベースの保護

エッジ デバイスの柔軟性
ルータおよびファイアウォールには、シン、リッチ、フルスタック オプションが用意されており、オンサイトの IT 需要や既存の導入環境に柔軟に対応可能

オープン アーキテクチャ
プログラム可能な CLI 用の API で、ノースバウンドの自動化およびサウスバウンドの統合を実現

シンプル

SaaS の管理
ブランチまたはクラウド エッジでセキュリティとネットワーキングを適用することで運用コストを削減

ゼロタッチ プロビジョニング
IaaS および SaaS アプリケーション用のクラウド導入を自動化

トランスポートの独立性
DIA またはセキュア VPN オーバーレイを使用するワークロードに対応したビジネス ポリシーを有効化

C45-741398-00 11/18