appgate

ユニバーサルZTNAの投資収益率分析

本書は、ダイレクトルートとクラウドルートのアーキテクチャアプローチの違い、主要な検討事項、およびユニバーサルゼロトラストネットワークアクセス（ZTNA）の潜在的な直接的および間接的な投資利益率（ROI）についての分析に関するホワイトペーパーである。

ゼロ・トラスト・ネットワーク・アクセス・ホワイトペーパー

ユニバーサルZTNAのROI分析
目次

はじめに

リモートワークやハイブリッドワーク環境が新たなワークモデルとして確立される中、従来のネットワーク・セキュリティ・ソリューションでは、ユーザーに安全なアクセスを提供する効果がないことが実証されている。昨今の働き方の変化により、ゼロトラスト・ネットワーク・アクセス（ZTNA）に対する需要が高まっている。

ZTNAは当初、リスクが高く、時代遅れのVPNテクノロジーに代わる、現代的で安全性の高いリモートアクセスとして導入された。ユニバーサルZTNAのコンセプトは、VPNの代替という主要なユースケースを超え、勤務場所を問わず、あらゆるデバイスから、あらゆるユーザーに対して、複雑なハイブリッドIT環境全体で、統一されたポリシーモデルによるセキュアなアクセスを提供するものである。

ユニバーサルZTNAは、ゼロトラスト・セキュリティ原則を一貫して実施し、場所に関係なく、すべてのアイデンティティとすべての保護対象リソースへのアクセスを保護する。ユニバーサルZTNAを導入することで、ベンダーとツールの統合が可能になり、企業は強固なセキュリティ体制を維持しながら、財政的責任のバランスを取ることができる。このホワイトペーパーでは、ダイレクトルート型ZTNAとクラウド ルート型ZTNAのアーキテクチャアプローチの違い、主な検討事項、リモートアクセスの代替えとしてVPNのみを適用した場合と、企業のあらゆるユースケースに汎用的に拡張した場合の潜在的な直接的・間接的投資収益率（ROI）の分析を行っている。企業が専用に構築されたユニバーサルZTNAソリューションを採用することで、ビジネスクリティカルなユースケースをどのように解き放ち、大規模で大幅なコスト効率を達成できるかを示している。

> “ユニバーサル **ZTNA**は、既存の **ZTNA**技術をリモートアクセス以外のユースケースに拡張し、オンプレミスのキャンパスや支店でのローカル業務をサポートする。（「ユニバーサル **ZTNA**」はマーケティング用語であり、**ZTNA**の本来の定義はリモートアクセスのユースケースに限定されるものではないからである）。ユニバーサル **ZTNA**は、デバイスとエンドユーザーのゼロ・トラスト・アクセス・ポリシーを一元化し、単一のアクセス・ポリシー定義を可能にする。”
>
> ガートナー2023年ZTNA市場ガイド

ユニバーサルZTNAを推進するユースケース

- 完全なVPNリプレース：すべてのユースケースにおいて、従来のVPNからZTNAへ移行
- 第三者アクセス：ネットワークの完全性を損なうことなく、外部エンティティが接続できるように
- MPLSからインターネットへのトラフィック移行：コストのかかるMPLS接続からパブリック・インターネットへのネットワーク・トラフィックの移行
- ソフトウェア定義の広域ネットワーク（SD-WAN）を排除：従来のSD-WANの複雑さや潜在的な脆弱性に依存することなく、リソースへのセキュアなアクセスを提供
- ネットワークアクセス制御（NAC）の置き換え：高価なNACソリューションを、すべてのユーザー、デバイス、場所に対する一貫したアクセス制御メカニズムに置き換え
- ゼロ・トラスト・ブランチ・コネクティビティ：支店の拠点から企業のリソースにアクセスするすべてのユーザーとデバイスの継続的な確認と承認

ユニバーサルZTNAに不可欠な能力

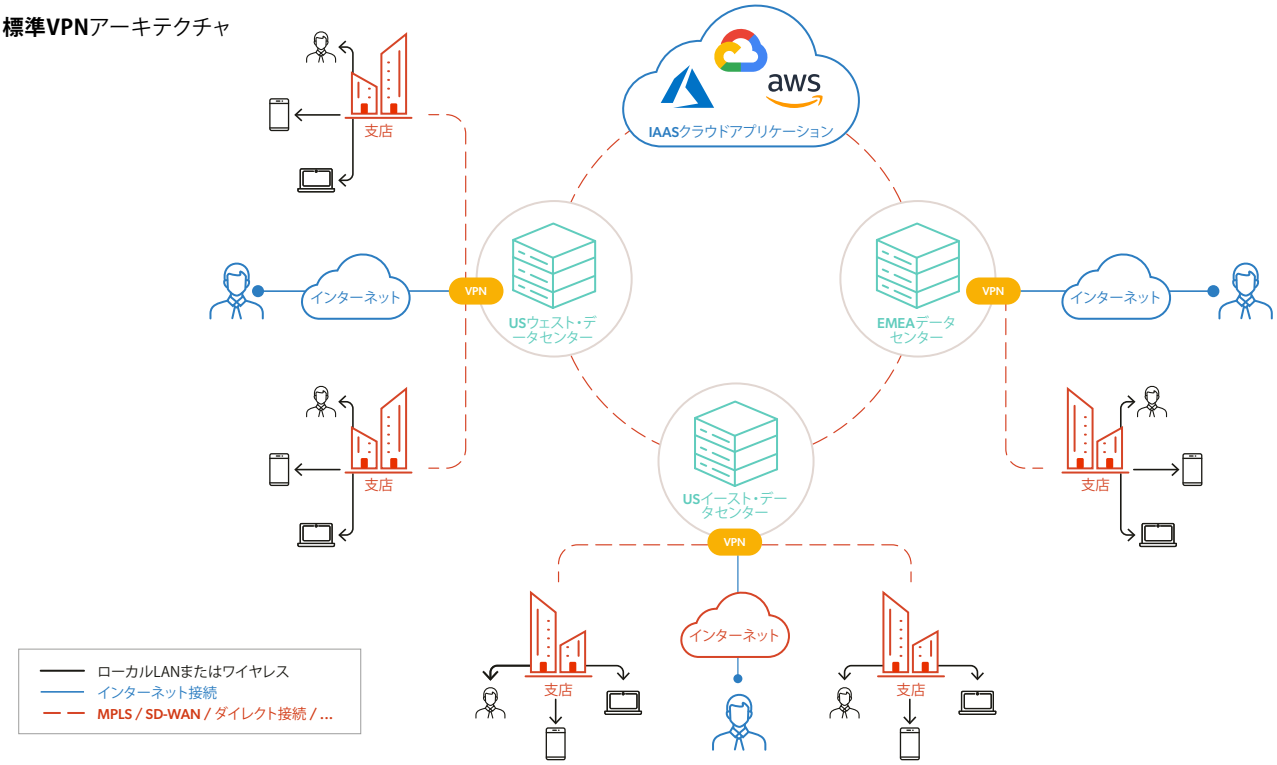
- アイデンティティ中心のセキュリティ：許可され認証されたエンティティのみが特定のネットワーク・リソースにアクセスできることを保証
- アプリケーション層毎のアクセス制御：ユーザーのタスク実行に必要な最小限のアクセスを保証
- ダイナミック・アクセス・ポリシー：ユーザーとデバイスの特定のコンテキストに基づいたアクセス権の付与
- 適応型認証：ユーザーの行動やコンテクスト要因の変化に対応し、アクセス権限が現在のセキュリティ態勢に適切であることを保証
- 拡張性と高性能：ダイナミックなスケーラビリティを拡張し、ユーザーやデバイスの増加に対応しながら、最適なパフォーマンスを維持

ZTNA：リモートユーザーアクセスのVPNからの代替

リモート・ユーザー・アクセスのサポートをVPN技術からZTNAに置き換えることがZTNA導入の始めのユースケースとして多くある。従来のVPNテクノロジーは、企業の境界をリモートデバイスまで拡張する。しかし、そのデバイスが侵害された場合、攻撃者は境界を突破し、永続性を確立し、偵察を行い、環境全体を横方向に移動して攻撃を成功させることができる。VPNを経由してVPNアカウントに侵入されたり、VPNコンセントレータを悪用されたりする多くの事例が、VPNがもはや最新のセキュリティ基準を満たしていないことを証明している。

企業の境界ネットワークは通常、1つまたは複数の地域のデータ・センターや、コア・アプリケーションやセキュリティ・スタックがホストされている場所に存在する。その場所はローカル・サーバー・ルームであったり、商用データ・センターであったり、あるいはインフラストラクチャー・アズ・ア・サービス（IaaS）を介してクラウド上にある場合もある。サービス（IaaS）経由のクラウドであることもある。これらのロケーションは通常、電気通信サービスが提供するセキュアな専用接続（MPLS、SD-WAN、ダイレクトコネクト、専用ファイバーなど）によって相互接続されている。これらの接続は、従来のインターネット帯域幅よりもかなり高価である。しかし、接続は暗号化され、専用で、インターネット上のどんな悪意のある人物からも見られない。

標準VPNアーキテクチャ



近年のCVEはVPNの脆弱性を露呈

2023年6月フォーティネットは、CVE-2023-27997（CVSS：9.2）として追跡されている、Fortinet FortiGate SSL VPNに影響を及ぼす重大なゼロデイ脆弱性の存在を確認した。この脆弱性を悪用すると、リモートで認証されていない脅威行為者が脆弱性のあるデバイス上でコードを実行することが可能になる。この脆弱性は認証前のものであるため、攻撃は多要素認証（MFA）をバイパスする。

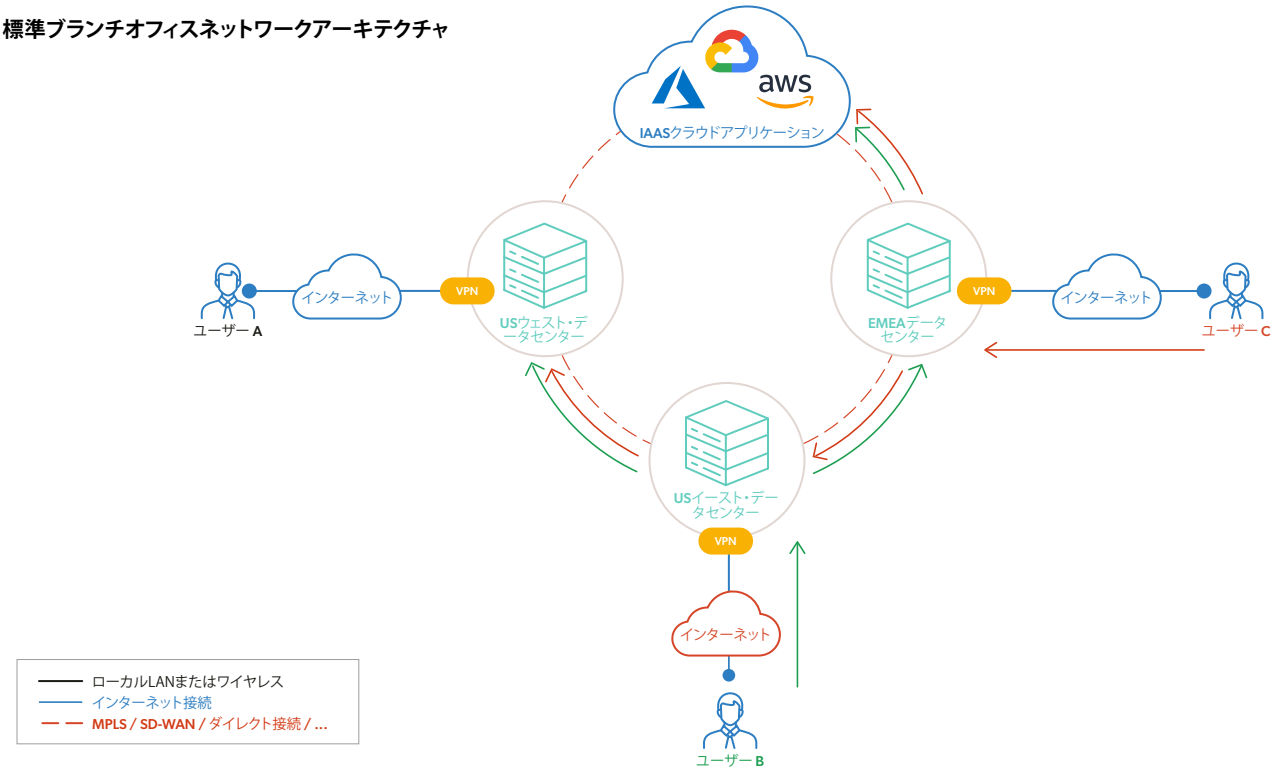
2023年9月 Ciscoは、Adaptive Security Appliance Software および Firepower Threat Defense Software のリモートアクセス VPN 機能にゼロデイ脆弱性を確認し、CVE-2023-20269 として追跡された。この脆弱性を悪用することで、攻撃者は有効な認証情報を特定することができ、この認証情報を使用して不正なリモートアクセス VPN セッションやクライアントレス SSL VPN セッションを確立することができる。

2024年1月：Ivantiは、CVE-2023-46805とCVE-2024-21887として追跡されている2つのゼロデイ脆弱性が悪用されていることを確認した。一つ目は認証バイパスで、制限された資料へのリモートアクセスが可能となった。もうひとつはコマンドインジェクションの脆弱性で、認証された管理者が独自のリクエストを送信し、任意のコマンドを実行できるようにするものだ。さらに多くのCVEが2024年2月に公表された。

支店やキャンパスのネットワークは通常、類似の専用接続を使用して、1つまたは複数の地域データセンターまたはクラウド拠点にリンクされている。地域データセンターが企業のインターネットの出入り口となるのは一般的である。VPNコンセントレータは通常ここでホストされ、リモート・ユーザーに地域アクセスを提供し、必要に応じてアプリケーション・トラフィックを内部ネットワーク経由で各拠点にルーティングする。

リモート・ユーザーのVPNトラフィックを可視化すると、ユーザーからのすべてのトラフィックは、1つの場所（通常は地域のVPNコンセントレータ）で企業ネットワークに入る。例えば、ユーザーCはVPNを地域のEMEAデータセンターに接続し、すべてのVPNトラフィックはその場所に到着する。また、米国東部のデータセンターにあるローカル・アプリケーションや、他の地域のデータセンターにあるアプリケーションに接続する場合もある。この場合、リモートユーザーは、これらのデータセンター間の異なるプライベート接続の帯域幅を消費する。プライベート接続で消費される帯域幅は、インター ネットの帯域幅よりもかなり高価である。さらに、ユーザーがアプリケーションに到達するために複数のリンクを通過しなければならない場合、関連するコストと遅延はさらに高くなる。

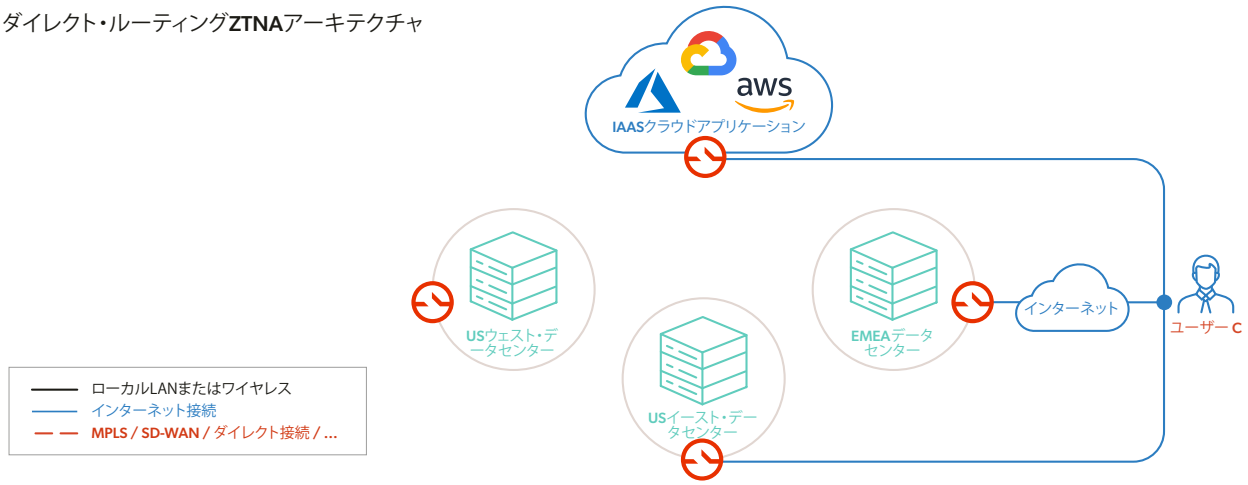
標準ブランチオフィスネットワークアーキテクチャ



ダイレクトルートZTNAアーキテクチャによるVPNの置き換え

同じ例で、VPNソリューションをダイレクト・ルーティングのZTNAに置き換えてみよう。企業ネットワークへの単一のエントリー・ポイントの代わりに、各拠点にゲートウェイがある。ユーザーは、アプリケーションやネットワーク権限のある各拠点に相互TLS（mTLS）トンネルを作成する。ゲートウェイは、シングルパケットオーソライゼーション（SPA）を使用することで、インターネット上では見えないようになっている。この認可はネットワークソケットがクライアントに、ゲートウェイに接続する前に特別なパケットを送信することを要求する。この技術は、VPN技術では対応できない分散型サービス拒否（DDoS）やゼロデイ攻撃のリスクを軽減する。この例のユーザーCは、標準的なインターネット帯域幅を活用して、3つのデータセンター間で直接mTLSトンネルを確立している。下の画像に示すように、リモートユーザーCは、VPNテクノロジーでは対応できないMPLS/SD-WAN接続から完全にオフロードさ れている。。

ダイレクト・ルーティング**ZTNA**アーキテクチャ



直接的なROI：ダイレクトルートZTNAによるVPNの置き換え

MPLS/SD-WAN接続コストの削減：

VPNユーザーが消費するMPLS/SD-WAN帯域幅の量は、VPNコンセントレーターの設置場所や、企業ネットワーク上のアプリケーションの分散状況によって異なる。クラウド中心の組織であっても、オンプレミスの VPN を活用してクラウド環境に接続している場合は、高価な MPLS/SD-WAN 帯域幅から標準的なインターネット接続に移行することで、すべてのリモート・ユーザーがすぐに節約できる。リモートアクセスにおけるVPNユーザーをダイレクトルートZTNAに移行することで、一般的に、MPLS/SD-WAN接続コストが全体の10%から20%削減されると予想される。

ハードウェアコストの削減：

ダイレクト・ルーティングZTNAは、VPNコンセントレーターを純粋なソフトウェア・ソリューションに置き換えることで、高価なハードウェアVPNアプライアンスを追加購入したり保守したりすることなく、エントリー・ポイントを簡単に追加できる。さらに、自動化されたクラウド・スケーリングが容易になり、需要の変動に応じてリソースのプロビジョニングとデプロビジョニングが可能になる。さらに、世界的なパンデミックや、特定の地域に影響を及ぼす悪天候などの重大なイベントの際にも、すべてのユーザーのリモートワークへの突然のシフトを、混乱なくサポートすることができる。Ciscoの価格体系からも明らかなように、ハードウェア・ベースのVPNバンドルは、75ユーザーで$4,700～、10,000ユーザーで$300,000～と幅があることを考慮する必要がある。ロードバランシングや冗長性を考慮したネットワーク中心の企業では、ハードウェアの資本支出は、アプライアンスのメンテナンスコストを加えると、さらに高くなる可能性がある。

ダイレクトルートZTNAとは？

ダイレクト・ルーティングZTNAアーキテクチャは、企業内の プライベート・アプリケーションとネットワーク・インフラストラクチャのユニークなセット に対応するために、目的に 応じた柔軟なアプローチを提供する。こ のモデルは、データがネットワークを どのように通過するか を完全に制御し、あらゆる場所に配置されたハイブリッドインフラストラクチャのどこからでも、すべてのユーザー間接続とリソース間接続へのセキュア なアクセスを提供する。主な 利点は、ダイレクトルートアーキテクチャの拡張性 とパフォーマンスで、企業は最適なネットワークパフォーマンスを維持しながらビジネスを拡張できる。ダイレクトルート型ZTNAに関連する価格モデルは透明性が高く、理解しやすく、隠された料金がないため、企業は予測可能で管理しやすいコスト構造を実現できる。

間接的なROI：ダイレクトルートZTNAによるVPNの置き換え 情報漏洩のリスクを低減し、事業継続性を維持：

シングル・パケット認証（SPA）により、重要な企業ネットワーク・トラフィックの標準インターネットを活用することができる。SPAはエッジポイントを不可視にするため、DDoS攻撃、VPN脆弱性パッチ、ゼロデイ攻撃の可能性が排除される。SecurityWeek誌が報告しているように、アプリケーションDDoS攻撃の成功によるダウンタイムのコストは、1分あたり平均6,000ドルである。その結果、ダイレクトルートのZTNAソリューションによって、DDoS管理および運用コストとリスクの削減が実現し、ビジネスの継続性が維持される。

攻撃対象の最小化：

ユニバーサルZTNAのきめ細かなポリシーは、ユーザーに広範なネットワークアクセスが付与されないことを保証し、特に悪意のあるユーザーやデバイスが遠隔地から接続を試みた場合の攻撃対象領域を大幅に削減する。さらに、きめ細かなポリシーにより、コンテキスト要因に基づいてアクセス権限を調整できるため、悪意のある不正アクセスの試みを防止しながら、ユーザーに安全なアクセスを提供する組織の能力が強化される。

生産性の向上：

ユニバーサルZTNAは、許可されたユーザーが必要なリソースにアクセスするプロセ スを合理化し、ビジネスオーナーがアプリケーションを本番環境に迅速に展開で きるようにする。また、ITセキュリティチームは、HVACシステムや製造ロボット などの重要なシステムへの正確なアクセスをサードパーティに提供し、サードパーティによる攻撃のリスクを効果的に低減することができる。ROIは、会社の リソースへの安全なアクセスを必要とする従業員や請負業者の生産性と効率の向上に反映される。

コンプライアンスの簡素化：

ダイレクトルートのZTNAは、組織がさまざまな規制や標準に準拠するのに役立ち、従来のネットワーク・ファイアウォールのルールやログと比較して監査が容易なIDベースのポリシーを提供する。従来のセキュアアクセスソリューションではしばしば手作業が必要だったデータ収集とレポート作成の自動化により、ROIを測定することができる。ZTNAは、コンプライアンス報告の範囲を縮小し、業界規制への不適合を回避するのに役立つ。

トラフィックをMPLSからインターネットに移行するためのAppgate SDPのROIが証明された：

フォーチュン500に入るグローバルITサービス・プロバイダーは、13万人のユーザー・ベースにユニバーサルZTNAを導入した。ダイレクトルートアーキテクチャを採用したことで、それまで共有のプライベートMPLS接続を利用していた代わりに、すべてのユーザーが組織の6つの主要データセンターに接続する個別の暗号化インターネットトンネルを確立できるようになった。これ以前は、世界6カ所の主要データセンター間の相互接続として、10ギガビットのMPLS接続が必要だった。同社は、600を超えるサイトからMPLSを排除し、全体の接続コストを67%削減し、より低い帯域幅の契約を可能にした。その結果、年間数千万ドル（同社がユニバーサルZTNAソリューションに毎年支払う金額の10倍）の節約につながった。

Appgate SDPまたはゼロ・トラスト支店間接続にて実証されたROI：

ある世界的な食品・健康企業は、その広大なネットワーク内のすべてのユーザーに安全なアクセスを提供するため、ユニバーサルZTNAを採用した。導入後、支店内のユーザーはゲスト用Wifiネットワークから操作できるようになり、同社は従来のネットワーク・セキュリティ機器のほとんどを撤去することができた。同社は、世界14ヶ所の支店の機器更新費用を75万ドル節約した。これにより、運用経費が合理化され、各拠点で異なるセキュリティ・ソリューションを維持・更新する必要がなくなった。ユニバーサルZTNAを導入したことで、従業員は社内勤務かリモート勤務かにかかわらず、一貫した統一されたユーザー・エクスペリエンスを確保できるようになった。

VPNをクラウドルートのZTNAアーキテクチャへ置き換え

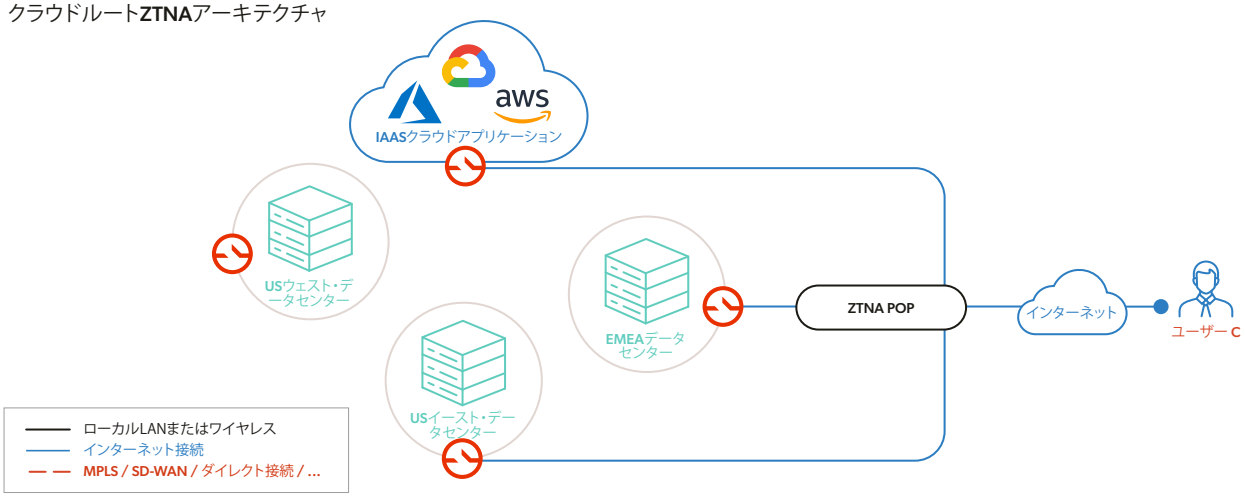
VPN技術をクラウドルート型ZTNAアーキテクチャに置き換えた場合、ダイレクトルート型アーキテクチャと同様のコスト削減とメリットが適用される。ただし、このアーキテクチャでは、ユーザーと最も近いZTNAのPOP（Point of Presence）間、およびPOPと地域のデータセンター間の接続が必要になるため、インターネット帯域幅のコストが2倍になり、待ち時間も追加される。クラウドルートされたZTNA POPと各データセンター間の接続は通常、暗号化された共有接続であり、システム全体のパフォーマンスに大きな影響を与える。トラフィックの実行はクラウドで行われ、組織のデータセンター内の共有オープントンネルを利用する。もしクラウドが侵害された場合、組織のすべての重要なサイトへのバックドアが存在することになる。

さらに、クラウドルーティングされたZTNAアーキテクチャでは、すべてのプロトコルをサポートしたり、下方向へのトラフィックを処理したりすることに限界があることが多い。これは、VoIP（Voice Over Internet Protocol）の使用ケースや、デバイスのパッチ適用、管理、サポートを必要とするIT運用ツールセットに対応する上で重要である。この制限により、顧客は購入後に、入手したクラウドルート型ZTNAソリューションに何が含まれ、何が含まれないかを判断するという、困難な意思決定を迫られる可能性がある。そうなると、組織はアプリケーションを、クラウドルート型ZTNAソリューションで保護されるものと、そうでないものに二分しなければならず、侵害に対して脆弱なままになってしまう。

クラウドルートZTNAとは？

一般にID認識プロキシ（IAP）と呼ばれるクラウドルート型ZTNAアーキテクチャは、その迅速な開発と市場投入の速さから、市場では一般的なものとなっている。このモデルでは、データトラフィックはマルチテナントのクラウド環境を経由する。このようなアーキテクチャには、ネットワーク・プロトコルのサポートに制限があること、オンプレミスのリソースに制約があること、レイテンシーやヘアピンの制限があること、効率的に拡張できないことなど、多くの欠点がある。さらに、ベンダーのマルチテナント型クラウドのセキュリティ、可用性、拡張性には暗黙の信頼が置かれている。包括的なコントロールと予測可能性を求める企業にとっては、ダイレクトルートのZTNAソリューションの方が有利な場合が多い。

クラウドルート**ZTNA**アーキテクチャ



ユニバーサルZTNA：すべてのユーザーに安全なアクセスを提供

ZTNAがリモート・ユーザーのアクセスを可能にするVPNの代替に限定されている場合、IT管理チームはしばしば、リモート・ユーザーと社内ユーザーのセキュリティ・ルールを別々に管理する必要に迫られる。このようなセキュリティプロトコルの断片化は、ネットワークインフラの複雑性と潜在的な脆弱性の増大につながる。ユニバーサルZTNAに移行すると、リモートユーザーと社内ユーザーの区別がなくなり、一貫したセキュリティプロトコルが保証され、すべてのユーザーに対して均一なレイテンシーとパフォーマンスが保証される。なぜ複雑さが増すのか、その例を検討し、ダイレクトルートとクラウドルートの両アーキテクチャを紹介する。

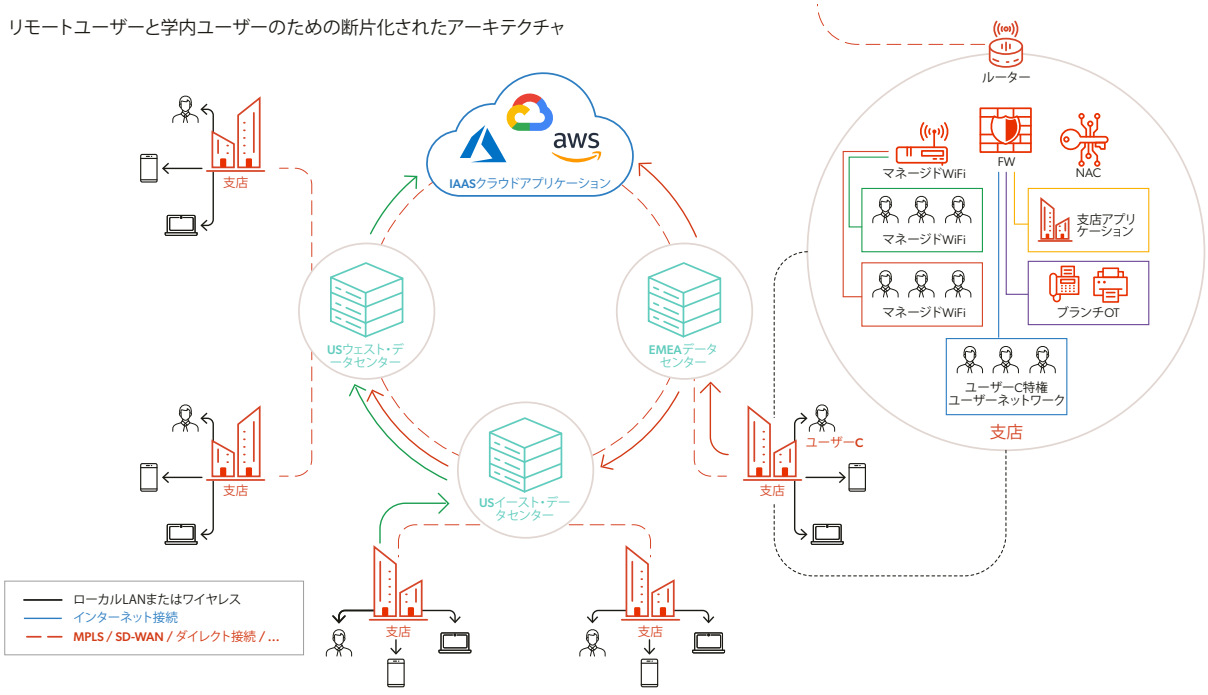
例として、ユーザーCは特権ユーザー（IT管理者/オペレーション）で、EMEAの支店からデスクトップを使って作業する必要があるとする。特権ユーザーは、多数の機密システムやアプリケーションに広くアクセスするので、他のオフィス・ユーザーから保護するために、特権ユーザー・ネットワークに配置されることがよくある。これを実現するために、企業はネットワーク・アクセス制御（NAC）ソリューション、無線管理システム、特権ユーザーのデバイスを識別するための特別なイーサネット・スイッチを必要としている。

このセグメントは、企業ネットワーク全体の重要なシステムにアクセスできる。その結果、一般的なユーザーや、通常インターネット接続だけにアクセスが制限されているゲスト社員（請負業者やサードパーティー・ベンダーなど）から隔離される。高度で複雑なファイアウォールルールは、すべての支店に設置され、通常は中央のファイアウォール管理システムからプッシュされる。ユーザー・グループを区別するためにオフィス内に新しいユーザー・セグメントが追加されるたびに、ファイアウォールのファイアウォール・ルール、NACソリューション、無線管理システムで指数関数的な作業が発生する。そのため、ユーザーとデバイスのセグメンテーションは、通常4つから6つの異なるセグメントになり、企業ネットワークのセグメンテーションは非常に粗い粒度になる。

企 業は、スイッチング機能と NACの組み合わせによるキャンパスネットワークのセキュリティ確保に数十億ドルを費やしている。このアプローチはハイブリッドワークへの移行に伴い、破壊の機が熟している。製品リーダーは、ZTNA製品を社内環境に拡張し、収益と企業価値を向上させる必要があるが、早急に対応しなければならない。

Gartner Campus Network Security and NAC are Ripe for Market Disruption

リモートユーザーと学内ユーザーのための断片化されたアーキテクチャ



ユーザーCが支店からUS West、US East、EMEA、エンタープライズIaaSクラウド環境のすべての異なるアプリケーションに接続する場合、これらのリンクのそれぞれでMPLS/SD-WAN帯域幅を使用する。プライベート・アプリケーションとインターネット・ブラウジング・トラフィック用の帯域幅はすべて、最も近いエンタープライズ・データ・センターへの支店のプライベート接続でも消費される。

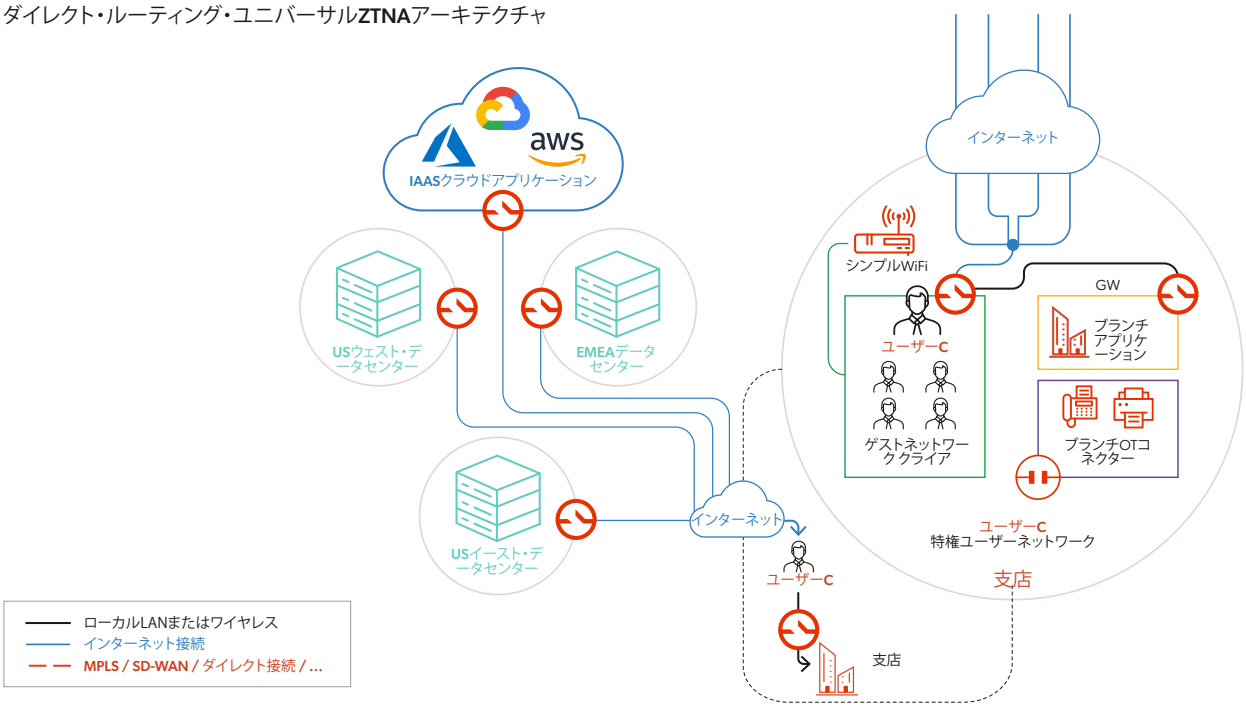
さらに、合併や買収の際には、企業のネットワーキングとセキュリティが著しく複雑になる。新たなMPLS/SD-WAN接続が必要となり、重複するサブネットを処理して企業のルーティング・テーブルを拡張しなければならない。ほとんどの場合、コア・ファイアウォールとブランチ・セキュリティ機器は異なるソリューションであるため、統合が困難であったり、企業標準による置き換えにコストがかかったりする。

ダイレクトルートアーキテクチャーのユニバーサルZTNA

ここで、ユニバーサルZTNAアプローチについて確認しておこう。このアプローチは、ZTNA接続を通じて企業アプリケーションに接続するすべてのリモートユーザーと社内ユーザーに適用される。このユースケースは、IoTデバイス、サーバー、またはZTNAクライアントがインストールできないデバイスにも拡張することができる。

包括的なユニバーサルZTNA機能を提供し、ダイレクトルートアーキテクチャと組み合わせたソリューションを選択することが極めて重要である。一般的にリモートユーザーアクセスだけでなく、あらゆる企業ユースケースに対応しようとすると、プロトコルとサポートされるデバイスの数がはるかに複雑になる。したがって、すべてのユーザーからリソース、リソースからリソースへの接続を保護するZTNAソリューションを選択する際には、これらの潜在的なハードルを念頭に置くことが重要である。ZTNAは、セキュアな個別のネットワークオーバーレイとして機能するソフトウェアソリューションであるため、ユーザーごとや支社ごとの移行が可能で、ほとんどの企業にとって比較的簡単で無停止の導入が可能である。唯一の要件は、すべてのユーザーまたはオフィス全体が移行を完了したら、残りの専用相互接続を削除または縮小し、特定の支店セキュリティ・ツールを削除することである。

ダイレクト・ルーティング・ユニバーサル**ZTNA**アーキテクチャ



直接的なROI：ユニバーサル・ダイレクトルートZTNA

コスト削減と未解明のユースケース：

完全に導入された場合、ユーザートラフィックはデータセンターと支社間のMPLS/SDWAN接続（プライベートリンク経由）を経由しなくなる。その代わり、支社から最寄りのデータセンターへのユーザートラフィックはすべて、通常のインターネット接続を使用することになる。さらに、オフィス内のIoTデバイスやローカルサーバーがユニバーサルZTNAで保護されている場合、接続全体をシンプルなインターネット接続に置き換えることができ、コスト効率が大幅に向上する。

前述したように、VPNコンセントレーターは純粋なソフトウェア・ソリューションに置き換えられるため、高価なハードウェアVPNアプライアンスを追加購入したり保守したりすることなく、エントリー・ポイントの追加が容易になる。さらに、自動化されたクラウド・スケーリングが容易となり、需要の変動に応じてリソースのプロビジョニングとデプロビジョニングが可能になる。さらに、特定の地域に影響を及ぼす地政学的紛争、伝染病、自然災害が発生した場合でも、全ユーザーのリモートワークへの突然の移行を支障なくサポートできる。

さらに、支店のセキュリティツールのコストも大幅に削減できる。すべてのユーザーが、カフェスタイルのワイヤレス（または有線）インターネット・ゲスト・ネットワークから仕事をすることができる。必要なのはインターネットアクセスだけで、支社ネットワークは企業アプリケーションにアクセスすることはない。ユーザーがデバイスを使用する際、ZTNAクライアントは、彼らが権限を持つすべてのロケーションに 接続し、支店内のローカルエリアネットワーク（LAN）接続でローカルアプリケーション（ローカルプリンタやVoIPサーバーなど）を使用することもできる。ユーザーが接続すると、ローカル・デバイスはリングフェンス（囲い込み）され、他のユーザーからローカル・ネットワーク上のデバイスが見えないようにすることができる。これにより、さまざまなユーザーのネットワーク・セグメンテーション、NACソリューション、複雑なマネージド・ワイヤレス設定、適切なユーザー・アクセスを保証するために必要な複雑なファイアウォール・ルールが不要となる。

合併や買収では、新しいデータセンターやクラウド・ロケーションのための追加ゲートウェイが唯一の要件となる。既存のアイデンティティ・アクセス管理（IAM）ソリューションを利用する新規ユーザーのオンボーディングは、ZTNAクライアントソフトウェアを各ユーザーに配備することで完了する。ダイレクトルートソリューションでは、各ユーザーのネットワークがポリシーエンジンによって指定された仕様に従って構築されるため、中央の企業ルーティングテーブルを必要としない。これにより、IPサブネットの重複の問題が解消される。合併や買収の統合が合理化され、最初のユーザーが数カ月や数四半期ではなく、数時間から数日で被買収企業に接続できるようになる。

コネクタを使用してIoTやその他のデバイスを包含するようにユースケースを拡大することは、コスト削減やセキュリティ上のメリット、運用効率の向上、より包括的なネットワーク管理にもつながる。IoTデバイスをZTNAフレームワークに統合することで、企業は堅牢なセキュリティとアクセス制御対策を、より広範な接続デバイスに拡張することができる。この統合により、ポリシーの一元的な実施、アクセス管理の簡素化、多様な種類のデバイス間での一貫したセキュリティ・プロトコルが可能になり、多数のエンドポイントのセキュリティ管理の複雑さが軽減される。

間接的なROI：ユニバーサル・ダイレクトルートZTNA

違反のリスクを低減：

SPAを使えば、重要な企業ネットワーク・トラフィックのための標準的なインターネットを活用することができる。エッジポイントは不可視であるため、DDoS、VPN脆弱性パッチ、ゼロデイ攻撃の可能性は排除される。SecurityWeek誌が報告しているように、アプリケーションDDoS攻撃の成功によるダウンタイムのコストは、1分あたり平均6,000ドルである。その結果、DDoSの管理コストと運用コスト、リスクの両方を削減し、ビジネスの継続性を維持することができる。

きめ細かなポリシーを導入することで、ユーザーに広範なネットワーク・アクセスが許可されないようになり、特に悪意のあるユーザーやデバイスが遠隔地から接続を試みた場合の攻撃ベクトルが大幅に減少する。さらに、きめ細かなポリシーは、コンテキスト要因に基づいてアクセス権限を調整することを可能にし、悪意のある行為者による不正アクセスの試みを防止しながら、ユーザーに安全なアクセスを提供する組織の能力を強化する。

生産性の向上：

ユニバーサルZTNAは、許可されたユーザーが必要なリソースにアクセスするプロセスを合理化し、経営者がアプリケーションを本番環境に迅速に展開できるようにする。また、ITセキュリティチームは、HVACシステムや製造ロボットなどの重要なシステムへの正確なアクセスをサードパーティに提供し、サードパーティによる攻撃のリスクを効果的に低減することができる。ROIは、会社のリソースへの安全なアクセスを必要とする従業員や請負業者の生産性と効率の向上に反映される。

コンプライアンスの簡素化：

ユニバーサル・ダイレクトルーティングZTNAは、組織がさまざまな規制や標準に準拠するのに役立ち、従来のネットワーク・ファイアウォールのルールやログと比較して監査が容易なIDベースのポリシーを提供する。ROIは、従来のアクセスセキュリティのアプローチではしばしば手作業が必要であったデータ収集とレポートを、自動化によって測定することができる。ZTNAは、コンプライアンス報告の範囲を縮小し、さまざまな業界規制への不適合を回避するのに役立つ。

Appgate SDPによるNACリプレースのROIが証明された：

あるマネージド・ホスティング・ソリューション・プロバイダーは、基本的なホスティングの枠を超え、ネットワーク通信とアクセス・ポイントの包括的な制御のためにユニバーサルZTNAを採用した。この導入により、ユーザーのプロビジョニングとアクセス変更にかかる時間が98%も短縮された。以前は3日かかっていたクラウド・ユーザーのプロビジョニングが、今ではわずか10分で済み、1時間かかっていたアカウントの変更も30秒で完了する。ZTNAの採用により、同組織はシステムの30%をゼロ・トラストの原則により合致したものに移行した。この組織は、ネットワークとシステムへのアクセスを改善すると同時に、ネットワーク・アクセス・イベントの可視性を強化し、その結果、セキュリティ・インシデントが大幅に減少した。今後の計画では、エンドポイントの60%を保護するスタンドアロン独立型NACを段階的に廃止し、その数をゼロにする予定である。

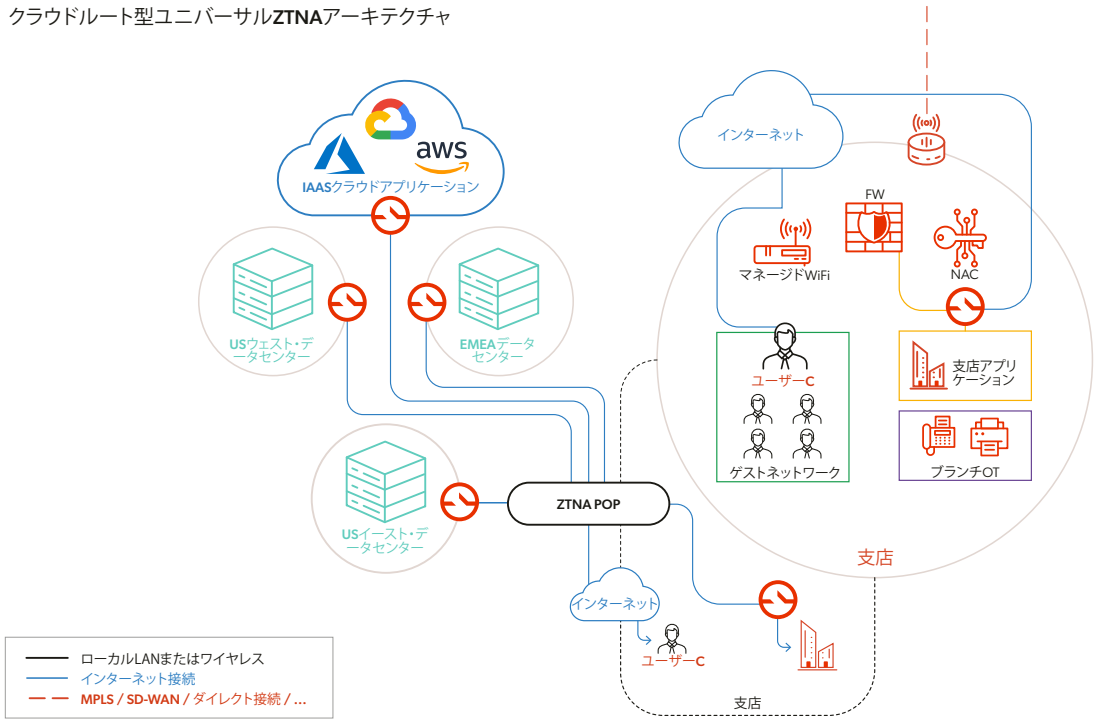
クラウドルートアーキテクチャによるユニバーサルZTNA

クラウドルーティングされたZTNAソリューションの導入は、ROIにマイナスの影響を与えるいくつかの課題をもたらす可能性がある。これらのアーキテクチャには多くのプロトコル制限があり、その多くは以下のようなもので、ダウンストリーム・トラフィックをサポートしていなかったり、IoTシナリオに対応するクライアントレス・オプションを提供していなかったりする。このため、ローカルブランチのセキュリティ・ツールを置き換えることはできない。さらに、クラウドルートのZTNAソリューションは、多くの場合、ウェブベースのアプリケーションのみに対応しし ており、ファイルサーバー、プリンター、VoIPシステムなど、ウェブ以外のローカルブランチリソースは除外されている。

この制限により、すべてのトラフィックをクラウドにリダイレクトし、ローカルブランチに戻す必要があるため、レイテンシーが増大し、インターネット帯域幅コストが2倍になり、運用コストが増加する。

さらに、クラウドルートされたZTNA POPから支店までの共有接続は、すべてのユーザーとデバイスによって一括して使用されるため、パフォーマンスが大幅に低下する。この問題を軽減するためにローカルPOPを提供するベンダーもあるが、余分なコンピューティングリソースが必要で、各支店ごとに高額なライセンス料が発生するため、ROIにさらに影響する。クラウドルートのZTNAモデルでは、トラフィックの強制はクラウドで管理されるため、さらなるリスクが生じる。もしZTNA POPが侵害された場合、攻撃者がネットワークに侵入するためのゲートウェイとして機能する可能性がある。

クラウドルート型ユニバーサル**ZTNA**アーキテクチャ



結論

ユニバーサルZTNAの採用により、特にダイレクトルートアーキテクチャでは、企業は実質的なROIを達成し、運用効率を高めることができる。すべてのユーザーとデバイスのゼロトラスト・アクセス・ポリシーを統合することで、企業全体で統一された一貫性のあるアクセス・ポリシー定義が実現する。このアプローチにより、従業員は勤務地に関係なく、より安全で一貫性のあるユーザー・エクスペリエンスを保証され、セキュリティ・チームはネットワーク全体にわたるアクセス制御とポリシーの展開と管理を合理化できる。慎重な計画と適切なベンダーとの提携により、ユニバーサルZTNAを採用することで、最も複雑な企業ネットワーク全体のセキュリティを強化するためのコスト効率の高いアプローチを提供する。

Appgateについて

Appgateはセキュアなアクセスを提供する会社である。ゼロ・トラスト・セキュリティの原則に基づいて構築されたソ リューションを提供することで、人々の働き方とつながり方を強化している。人々と定義されたセキュリティ・アプローチにより、クラウド、オンプレミス、ハイブリッド環境における、あらゆるデバイスと場所から、あらゆるITインフラストラクチャのワークロードへの迅速かつシンプルでセキュアな接続が可能になる。Appgateは、世界中の組織や政府機関が現在地からスタートし、Zero Trustの旅を加速させ、将来の計画を立てるのを支援している。詳細は appgate.com をご覧ください。

appgate