SOPHOS
Cybersecurity evolved.

ZTNA の 6つのメリット

リモートアクセス VPN との比較

ソフォス ホワイトペーパー2021年 10月

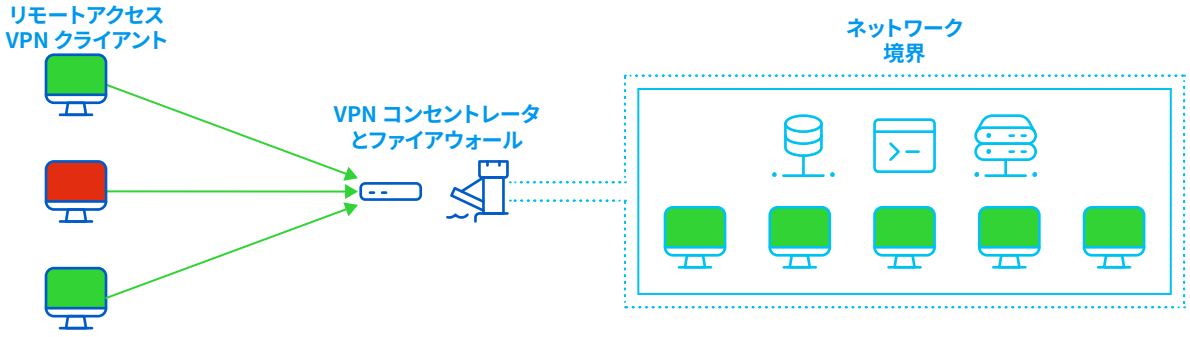
リモートアクセス VPN は長年、十分な機能を提供してきましたが、最近、リモートワークが増加したことで、この老朽化したテクノロジーの制限に焦点が当たりました。VPN を最大限に活用し続けている組織もありますが、多くの組織は、リモートアクセス VPN の課題に対処する、より優れた代替ソリューションを探しています。いくつかの組織は、次世代型リモートアクセス テクノロジーの全面的な採用を開始しています。それは、ZTNA (Zero Trust Network Access) です。ZTNA は、従来のリモートアクセス VPN と比較して、より優れたセキュリティ、より詳細な制御、可視性の向上、および透過的なユーザーエクスペリエンスを提供します。

この ZTNA ホワイトペーパーでは、従来のリモートアクセス VPN の制限と課題、および Zero Trust Network Access のメリットについて説明し、新しい ZTNA ソリューションに求めるべき重要な機能をまとめています。

リモートアクセス VPN の課題

リモートアクセス VPN は、何十年にも渡って、ほとんどのネットワークで不可欠な存在であり、ネットワーク上のシステムやリソースにリモートアクセスする際の安全な方法を提供してきました。しかし、これは、中世の城壁や堀のように、セキュリティ対策で企業ネットワークを囲んで、境界内のネットワークリソースを保護する対策をとった時代に開発された技術です。VPN は、承認されたユーザーが安全な境界内に入れるといった、保護されたゲートハウスと同等の役割を果たし、一旦アクセスが許可されると、ユーザーは境界内のすべての機能にフルアクセスできました。

従来のリモートアクセス VPN



もちろん、ネットワークは大きな進化を遂げており、これまで以上に分散されています。アプリケーションとデータはクラウドに存在し、ユーザーはリモートで作業しています。また、悪用する弱点を探している攻撃者やハッカーによってネットワークは包囲されています。

どのような最新の環境であっても、従来の VPN (IPSec/SSL) ベースのリモート アクセス ソリューションを管理することは、非常に困難になる可能性があります。IP 管理、トラフィックフローとルーティング、ファイアウォール アクセス ルール、およびクライアントと証明書のインストールと設定に対処する必要があります。ノードの数が数個を超え、ユーザーの数が数十人を超えるだけで、VPN の運用にかかる時間が増大します。それ以外にも、セキュリティを監視、制御することは、まさに悪夢のような作業になります。

つまり、従来のリモートアクセス VPN には、不必要な制限と課題が複数あります。

1. **暗黙的な信頼** – リモートアクセス VPN は、企業内でアクセスしたかのように、境界を通過して企業ネットワークへのリモート接続を提供するのに適しています。しかし、通過した時点でユーザーは暗黙的に信頼され、そのネットワーク上のリソースへの広範なアクセス権が与えられるため、不必要で膨大なセキュリティリスクが発生する可能性があります。
2. **潜在的な攻撃手法** – リモートアクセス VPN は、企業ネットワークに接続したデバイスのセキュリティ状態を識別できません。このため、侵害された可能性のあるデバイスが経路となって、脅威がネットワークに侵入する可能性があります。
3. **非効率的なバックホール** – リモートアクセス VPN は、ネットワークで単一の接続点となるので、リモートアクセス VPN トンネルを介して、複数の場所、データセンター、アプリケーションからのトラフィックをバックホールする必要が生じる可能性があります。
4. **可視性の欠如** – リモートアクセス VPN は、アクセスを許可するトラフィックや使用パターンを識別できないため、ユーザーのアクティビティとアプリケーションの使用状況の可視化が困難になります。
5. **ユーザーエクスペリエンス** – リモートアクセス VPN クライアントは、ユーザーエクスペリエンスが悪いことで知られています。遅延の増加、パフォーマンスの低下、接続問題の発生、一般にヘルプデスクに負担をもたらす、などがあります。
6. **管理、導入、登録** – リモートアクセス VPN クライアントのセットアップ、展開、新規ユーザーの登録、離職したユーザーの登録解除には手間がかかり、困難です。また VPN のファイアウォールやゲートウェイ側の管理も困難です。特に、複数のノード、ファイアウォール アクセス ルール、IP 管理、トラフィックフローとルーティングなどに対処する必要があります。それには、一日の仕事時間の大半をその作業で費やすこととなってしまいます。

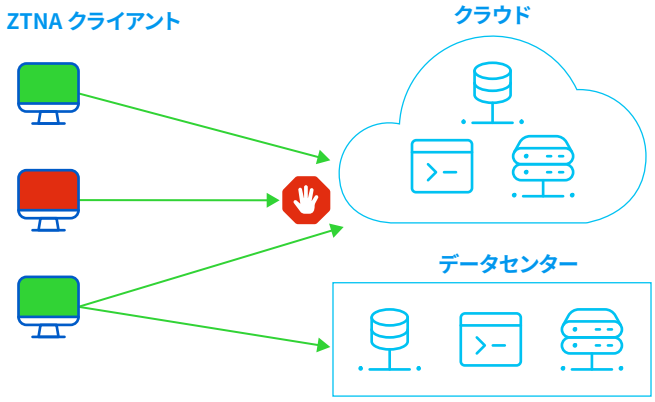
ZTNA とその仕組み

ZTNA (Zero Trust Network Access) は、リモートアクセス VPN の課題と制限に対処するように最初から設計されました。仕事に必要なアプリケーションやデータのみに安全に接続することで、場所を問わずにユーザーにより優れたソリューションを提供します。ZTNA には、ZTNA とリモートアクセス VPN を区別する、いくつかの基本的な違いがあります。

ZTNA は、その名前からわかるように、「何も信頼せず、すべてを検証する」というゼロトラストの原則に基づいています。つまり、ゼロトラストは「中世の城壁や堀」の概念を排除し、各ユーザー、デバイス、ネットワークアプリケーションをそれぞれの境界として扱い、認証情報の検証、デバイスのセキュリティ状態の検証、アクセスポリシーの確認を実行した後のみに相互接続を許可します。これによって、セキュリティ、セグメンテーション、制御が大幅に向上します。

ZTNA 機能のもう 1つの大きな違いは、単に、ユーザーにネットワークへのアクセスが許可されて、ネットワーク内を自由に移動できるようになるわけではない、ということです。代わりに、ユーザーとアクセスが承認されているアプリケーション用の特定のゲートウェイとの間に限って、個別のトンネルが確立されます。これによって、はるかに安全なマイクロセグメンテーションが実現します。これには、セキュリティ、制御、可視性、効率性、およびパフォーマンスにおいて、複数のメリットがあります。たとえば、リモートアクセス VPN では、ユーザーがアクセスしているアプリケーションを把握することはできません。一方 ZTNA では、すべてのアプリケーションの状態とアクティビティをリアルタイムで提供することが可能で、潜在的な問題を検出したり、ライセンスの監査を実行したりする際に役立ちます。さらに、ZTNA で提供されるマイクロセグメンテーションによって、ネットワーク上のリソース間で、デバイスやユーザーアクセスによるラテラルムーブメントが発生しなくなります。各ユーザー、デバイス、アプリケーションやリソースは、まさにそれぞれの安全な境界であり、暗黙的な信頼という概念はもはや存在しません。

Zero Trust Network Access



また、ZTNA は本質的にダイナミックかつ透過的で、初期のユーザー検証以外は、ユーザーの操作を必要とせず、バックグラウンドで動作します。このユーザーエクスペリエンスは非常にスムーズかつシームレスで、ユーザーは安全かつ暗号化されたトンネルを介してアプリケーションに接続していること気付くことさえありません。

ZTNA のメリット

Zero Trust Network Access は、さまざまな点で大きなメリットをもたらしますが、主に次のような理由で導入されています。

- **在宅勤務：**ZTNA ソリューションは、在宅勤務中の従業員のリモートアクセスを、より簡単に管理できるソリューションです。より簡単かつフレキシブルに導入と登録を実行でき、VPN の運用を、一日分作業量を必要とする作業から、少ない時間で行える作業に変えます。また、リモートで作業する従業員にとっても、より透明性が高く、よりシンプルになります。
- **アプリケーションのマイクロセグメンテーション：**ZTNA ソリューションは、マイクロセグメンテーション、アクセスポリシーへのデバイスのセキュリティ状態の統合、継続的な認証の検証、および暗黙的な信頼と VPN に伴うラテラルムーブメントの排除などによって、より優れたアプリケーションセキュリティを提供します。
- **ランサムウェア対策：**ZTNA ソリューションは、ランサムウェアやその他のネットワーク侵入攻撃の一般的な攻撃手法を排除します。ZTNA ユーザーは、もはや「ネットワーク上」にないため、VPN を介して足がかりを得ることのできる脅威は、ZTNA 環境では拡散することができません。
- **新しいアプリケーションや新しいユーザーを迅速に利用可能にする：**ZTNA は、ユーザーが入れ替わる、急速に変化する環境において、より優れたセキュリティと俊敏性を実現します。新しいアプリケーションを迅速かつ安全に立ち上げたり、ユーザーやデバイスを簡単に登録または登録解除したり、アプリケーションの状態や使用状況を把握したりできます。

つまり、従来のリモートアクセス VPN ソリューションと比較した場合の ZTNA のメリットは次のとおりです。

1. **ゼロトラスト** – ZTNA は、「何も信頼せず、すべてを検証する」というゼロトラストの原則に基づいています。これによって、より優れたセキュリティとマイクロセグメンテーションが提供されます。各ユーザーやデバイスをそれぞれの境界のように事実上処理し、企業アプリケーションとデータへのアクセスを許可するために、ID とセキュリティ状態を常に評価・検証します。ユーザーは、ポリシーによって明示的に定義されたアプリケーションやデータのみにアクセスできるため、ラテラルムーブメントやそれに伴うリスクを削減できます。
2. **デバイスのセキュリティ状態** – ZTNA は、デバイスのコンプライアンスとセキュリティ状態をアクセスポリシーに統合します。これによって、非準拠 /感染したシステム、または侵害されたシステムが企業のアプリケーションやデータにアクセスすることを阻止したり、重要な攻撃手法を排除したり、データの盗難や漏洩のリスクを削減したりすることが可能になります。
3. **どこからでも利用** – ZTNA はネットワークに依存せず、自宅、ホテル、カフェ、オフィスなど、あらゆるネットワークから同じように安全に利用できます。接続の管理は、ユーザーやデバイスの場所を問わず安全かつ透過的に行われ、ユーザーがどこで作業していても、シームレスなユーザーエクスペリエンスを提供します。
4. **より透過的** – ZTNA は、必要に応じて、バックグラウンドでセキュアな接続を自動的に確立することで、スムーズでシームレスなユーザーエクスペリエンスを提供します。ほとんどのユーザーは、データを保護している ZTNA ソリューションの存在に気付くことさえありません。
5. **可視性の向上** – ZTNA は、アプリケーションの状態の監視、容量の計画、ライセンス管理と監査などを行うために重要な、アプリケーションのアクティビティの可視性を向上することができます。
6. **簡単な管理** - ZTNA ソリューションは、多くの場合、無駄が少なく、すっきりしているため、導入と管理が簡単です。また、頻繁にユーザーが入れ替わる環境で俊敏性を高めることができ、日々の管理作業を、一日分の作業量を必要とする作業から、迅速で手間のかからない作業にします。

バイヤーズガイド：ZTNA ソリューションに求めるべき機能

対応しているクライアント、ゲートウェイ、IdP のリストを確認することはもちろんですが、さまざまなベンダーの ZTNA ソリューションを比較する際には、次の重要な機能を考慮してください。

クラウドで提供、クラウドで管理

クラウド管理には、すぐに利用を開始できることから、管理インフラの削減、簡単な導入・登録、場所を問わないアクセスに至るまで、大きなメリットがあります。クラウド管理の主なメリットの 1つは、管理サーバーやインフラを追加することなく、ログインしてすぐに利用を開始できることです。また、クラウド管理により、あらゆるデバイスから場所を問わず安全な即時アクセスが可能になり、さまざまな働き方に対応できます。また、ユーザーが世界のどこにいる場合であっても、新規ユーザーを簡単に登録できます。

他のサイバー セキュリティ ソリューションとの統合

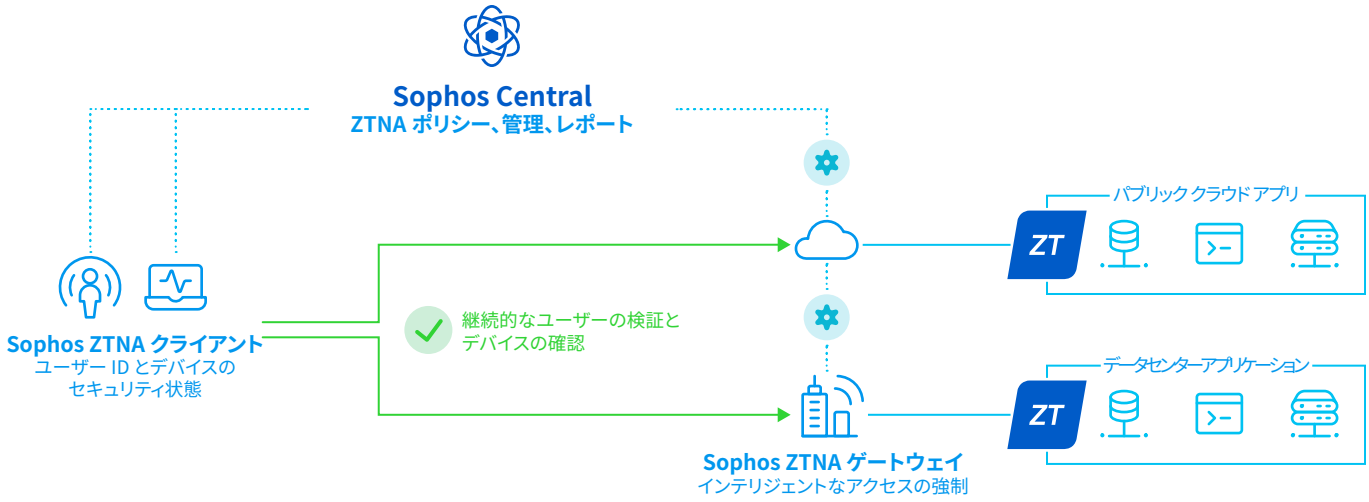
たいていの ZTNA ソリューションはスタンドアロン製品として完全に機能しますが、ファイアウォールやエンドポイントなど、他のサイバーセキュリティ製品と緊密に統合されたソリューションを使用することで大きなメリットが得られます。共通の統合されたクラウド管理コンソールは、管理者やチームの力を倍増させることができます。ZTNA を含むすべての IT セキュリティを単一の画面で一括管理することで、トレーニング時間や日々の管理負荷を削減できます。また、さまざまな IT セキュリティ製品に関する独自の分析を提供することもできます。特に、使用状況データを共有している場合はセキュリティが大幅に強化され、侵害されたデバイスや脅威がネットワークに接続 / 侵入した場合にはリアルタイムで対応できます。互いに連携して、検出された攻撃や脅威に即座に対応して、ラテラルムーブメント、拡散、データの盗難などを阻止できます。

ユーザーエクスペリエンスと管理操作性

検討しているソリューションが、優れたユーザーエクスペリエンスを提供するだけでなく、運営と管理の操作性がよいことも確認してください。最近は、リモートで作業するユーザーが世界中で増えていますが、新規ユーザーができるだけ早く作業を開始できるようにするため、登録と効率的なデバイスのセットアップは重要です。ZTNA エージェントの導入方法、および新規ユーザーをポリシーに簡単に追加できるかどうかという点に注意を払ってください。また、購入するソリューションが、スムーズでシームレスなユーザーエクスペリエンスを提供するだけでなく、アプリケーションのアクティビティをリアルタイムの表示など、可視性があることも確認してください。これによって、ピーク時の負荷、容量、ライセンスの使用状況、さらにはアプリケーションの問題までをプロアクティブに検出できます。

Sophos ZTNA

Sophos ZTNA は、Zero Trust Network Access を簡単、統合型、安全にするために最初から設計されています。Sophos ZTNA はクラウドで提供・管理され、業界で最も信頼性の高い、サイバーセキュリティのクラウド管理およびレポートのプラットフォームである Sophos Central に統合されています。Sophos Central では、ZTNA だけでなく、Sophos Firewall、エンドポイントやサーバー保護、モバイルデバイス管理、クラウドセキュリティ、メール保護なども管理できます。



Sophos ZTNA はまた、Sophos Firewall および Sophos Intercept X と緊密に統合されている点でもユニークです。これにより、Synchronized Security および Security Heartbeat を活用して、ファイアウォール、デバイス、ZTNA、Sophos Central 間でデバイスのセキュリティ状態を共有し、脅威や非準拠のデバイスに自動的に対応できます。そして、クリーンアップされるまで、アクセスを制限し、侵害されたシステムを自動隔離します。

ソフォスのお客様は、完全に統合されたソフォスのサイバー セキュリティ ソリューションを使用すると、時間を大幅に節約できると報告しています。Sophos Central から管理されるソフォスの製品スイートを組み合わせて使用し、Synchronized Security を活用して脅威の自動検出と対応を実現することは、IT チームのメンバーを 2倍に増やしたことに相当すると述べています。もちろん Sophos ZTNA は、他のベンダーのセキュリティ製品とも連携しますが、ソフォスのエコシステムの他の製品と緊密に連携して、可視性、保護、対応において、実環境での明確なメリットを提供するという点でユニークです。

詳細は以下をご覧ください

sophos.com/ztna

ソフォス株式会社
営業部
Email: sales@sophos.co.jp

21-10-07 JA (DD)