ゼロトラストネットワーク アクセスサービスを導入するための ネットワークアーキテクトガイド

VPN のリプレースとして ZTNA を
使用するためのベストプラクティス

zscaler™

プライベートアプリケーションをクラウドに移行し、ユーザのリモートワークを推進するためには、企業は円滑なユーザエクスペリエンスとプライベートアプリへのセキュアアクセスを可能にするサービスが必要です。ゼロトラストセキュリティが大きな盛り上がりを見せる現状においても、一部の企業は、アプリケーションへのユーザ接続を制限する方法として、ネットワークアクセスを前提とした次世代ファイアウォールに依存する、既存のネットワーク中心のアーキテクチャを採用しようとしています。これらの既存のアーキテクチャでは、今日のニーズに対応できず、承認されたユーザを特定のアプリに接続することを前提に設計されていません。このようなアーキテクチャは、ユーザをネットワークにアクセスさせる事になるため、多くの場合に他のアプリへのアクセスが可能となる水平移動のリスクが発生するだけでなく、IPアドレスがインターネットに公開されるため、ネットワークのエッジに置かれてインバウンドの ping をリスンする VPN コンセントレータ経由の DDoS 攻撃の標的になる恐れもあります。

VPN に代わるソリューションとして、ゼロトラストネットワークアクセス（ZTNA）サービスを検討する企業が増えており、ガートナーの予測によれば、60％の企業が2021年までに既存の VPN を段階的に廃止し、ZTNAサービスに移行するとされています。しかしながら、大規模（グローバルな）組織においては、ユーザによるアプリケーションへのアクセス方法の些細な変更であっても、大きな負担になることがあります。本書では、迅速かつビジネスを中断することなく ZTNA を導入するために知っておくべきヒントを紹介します。

本ガイドの主な内容は以下のとおりです。

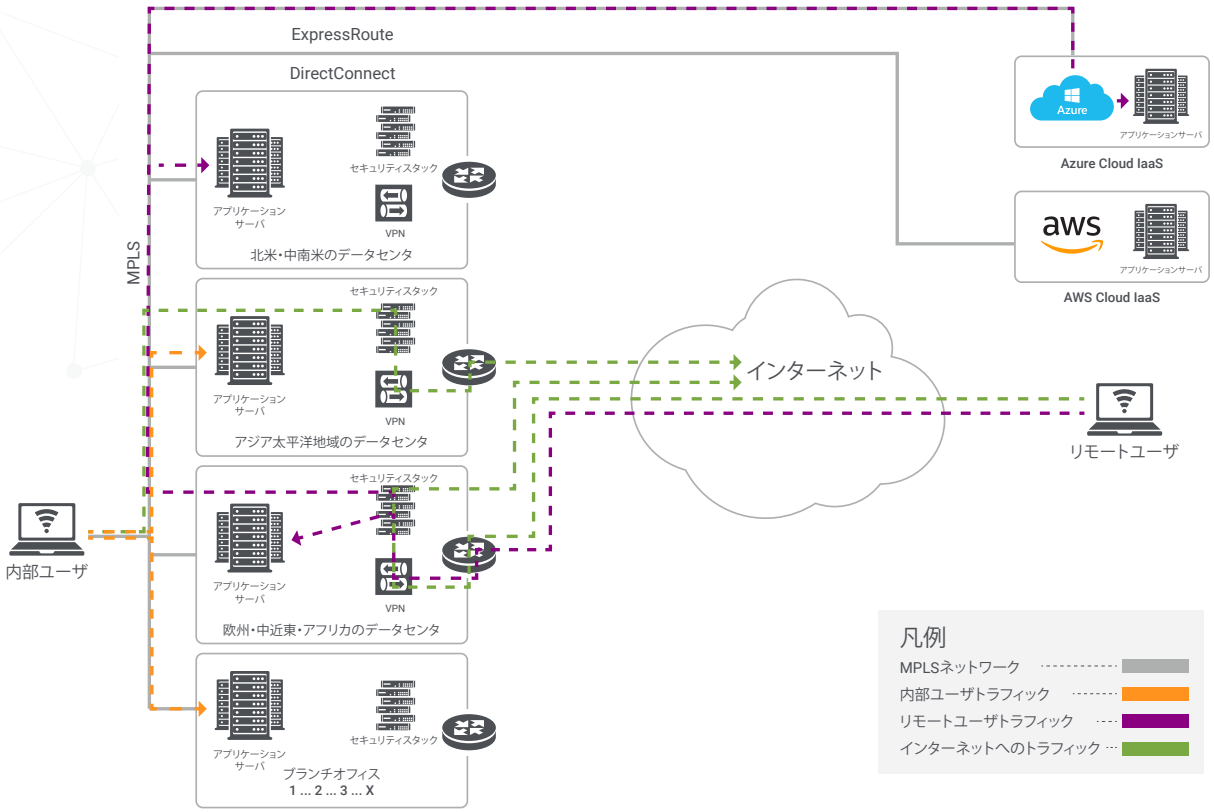
- 既存のアクセステクノロジと ZTNA のアーキテクチャの相違点
- ZTNA導入のための参照アーキテクチャ
- ZTNA の導入にあたって考慮すべき3つのフェーズ
- ZTNA を最大限に活用するためのヒントと考慮すべき点

説明に入る前に、「Mitigating Risk via the Software-defined Perimeter（SDP [Software-Defined Perimeter] によるリスクの軽減）」をお読みください。このブログでは、ゼロトラストネットワークアクセスサービスとは何かをわかりやすく解説しています。

それでは次に、ZTNAアーキテクチャを採用し、ユーザを企業ネットワークに接続させることなく、許可したユーザを特定のプライベートアプリケーションのみに接続する方法を詳しく見ていくことにしましょう。

現状を理解する - 企業における VPN の利用

多くの組織で広く採用されている極めて一般的なアーキテクチャを簡単な図にまとめると、次のようになります。ご覧のように、データセンタ、ルータ、ファイアウォール、VPNコンセントレータ、MPLSネットワークが存在し、それぞれの数や場所は組織によって異なるものの、この図に示したようなコンポーネントが構成されているはずです。これ以外にも、インラインプロキシ、サンドボックス、L7 ファイアウォール、AV や DLPソリューションといった、ネットワークやセキュリティの多数のデバイスも導入されているはずです。図を見やすくするため、ここでは、インターネット接続に関連するセキュリティをまとめてセキュリティスタックとして図式化しています。



この種の従来型アーキテクチャに関して、指摘しておくべき点がいくつかあります。

01 リモートユーザが VPN を使用してデータセンタに接続すると、同時に企業ネットワークにアクセス可能となります。多くの組織でのこれまでの経験から、ネットワークは比較的フラットで、 ACL がかなり制限されるため、その会社のすべてのデータセンタ環境と企業ネットワークがリモートユーザに公開されることになります。

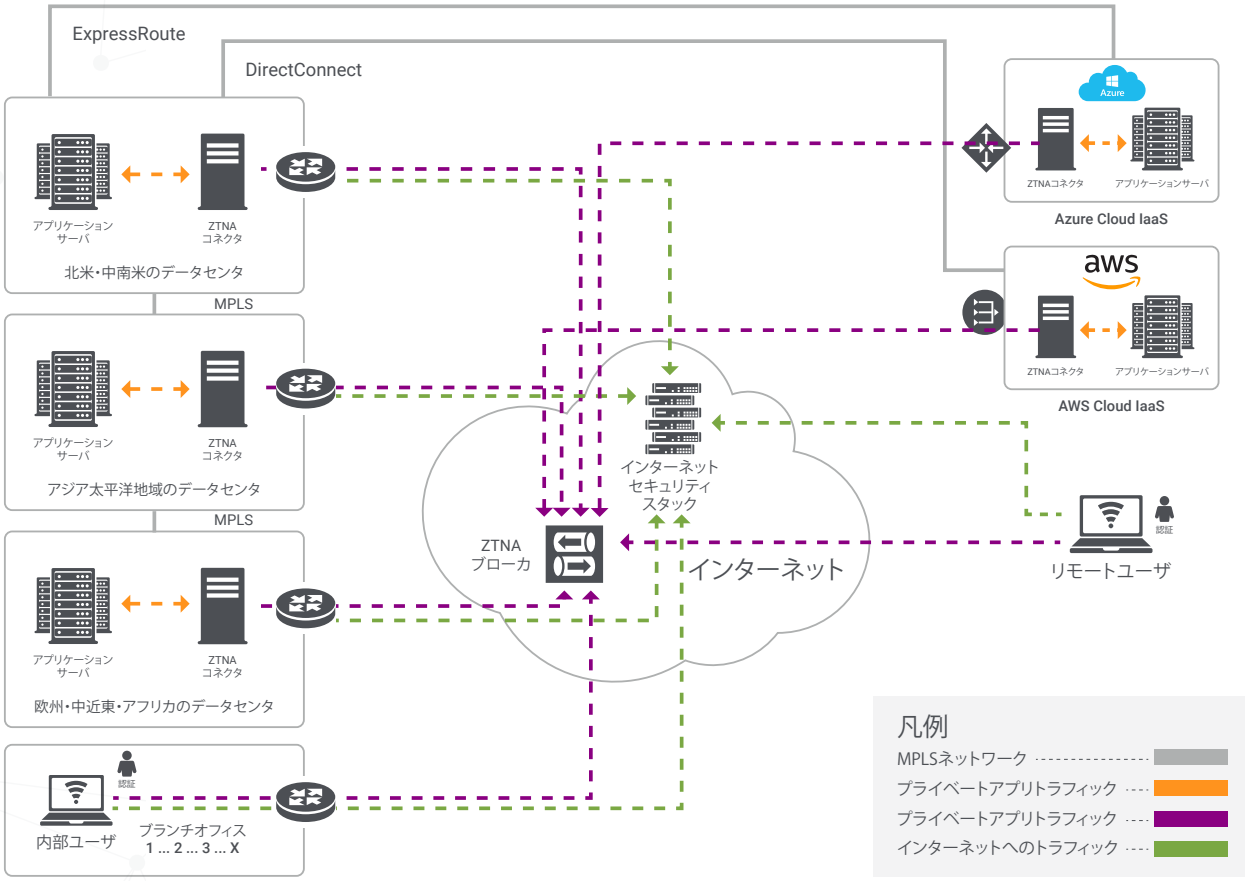
02 リモートユーザのインターネットへのすべてのトラフィックがデータセンタにバックホールされ、組織が所有する（ハードウェア）セキュリティスタックを使用してインスペクションされます。これはフルトンネル VPN と呼ばれる方法で、ユーザがネットワーク外にいる場合、ユーザを保護する必要があるセキュリティチームにとっては最適な手段です。しかし、すべてのインターネット、あるいは SaaSアプリケーションに対して、ローカルからそのままインターネットに送信されるのではなくバックホールされることになるため、ユーザエクスペリエンスが低下する恐れがあります。今では、企業側で用いる WANパイプより自宅のブロードバンドインターネット接続の方が高速である（地方であっても、 ISP経由で1Gbps のファイバ接続を利用可能）として、そちらの方を利用するユーザが増えています。

03 社内のユーザは一般的に、有線または無線のいずれであっても、ネットワーク内でデバイスを利用しますが、これらのネットワークは従来から「信頼されている」ものであるため、通常はすべてのデータセンタネットワークにもルーティング・接続できます。内部アプリケーションへのアクセスは LAN経由でルーティングされ、インターネット・SaaSアプリケーションはセキュリティスタックを通ってから ISP へと送られます。このような状況で問題なのは、ネットワークが自分たちの「所有物」であり、コントロールしているという理由だけで、企業ネットワーク上のすべてのユーザとデバイスを自動的に信頼すべきだとしてしまう、誤った認識です。

インターネット（VPN）からリモートアクセスする際にインバウンドアクセスが必要になります。また、内部ユーザがアイデンティティを問わず、すべてのアプリケーションサーバとダイレクト通信可能であるという点についても注意が必要です。

リスクを増大させることなく、企業アプリへのアクセスを提供するためのアーキテクチャ

SD（Software-Defined）アーキテクチャの最終的な目標は、アプリケーションへのアクセスをネットワークアクセスから分離することにあります。ユーザを企業ネットワークに接続させる必要がなくなり、承認されたユーザだけがプライベートアプリケーションにアクセスでき、IPアドレスがインターネットに公開されることはなく、ネットワークセグメント、ファイアウォールポリシー、ACLの管理の複雑さが解消されます。これを簡素化してまとめたものを、以下の図に示します。



この新しいSD（Software-Defined）アーキテクチャでは、データセンタ・アプリケーションネットワーク、リモートユーザ、内部ユーザが明確に分離されている事がわかります。たとえば、米国の2箇所のみにデータセンタがある、グローバルの10数箇所にデータセンタが存在する、あるいはAzure、AWS、GCPなどの環境などがあるといったことは問題ではなく、いずれの場合も次のようなかなり単純な構成になります。

01

MPLSやサイト間VPNなどのプライベートネットワーキングが必要とされるのは、データセンタとクラウドIaaS環境の間だけであり、このような環境では、サーバからサーバへの通信が必要です。wwwサイトのWeb層をAWSに移動したものの、バックエンドのSQLデータベースが物理的なデータセンタに残されている場合も、それらの場所を結ぶプライベート接続（低レイテンシ、高帯域幅）が必要です。

02

vpn.company.com というようなインバウンド接続をリモートアクセスに必要はありません。このアーキテクチャでは、オーケストレーション (コントロール) プレーンがクラウドに置かれ、ユーザからの通信がそこを終端として処理されます。 Zscaler の環境の ZPA App Connector と呼ばれるゲートウェイには、インバウンドのリスニングポート、パブリック IP/DNSレコードは必要ありません。これらのコネクタは、 TLS経由でSaaSベースのオーケストレーションプレーンとアウトバウンドで通信します。ユーザ ID のインスペクションが完了し、アクセスポリシーと照合されてから、内部アプリケーションが仲介されます。

- ユーザに内部アプリケーションもしくはリソースへのアクセスが許可されている場合は、オーケストレーションプレーンによって、コネクタとユーザデバイスの間のアウトバウンド TLS接続が連結しますが、このユーザが企業ネットワーク上でアクセス可能になることはないため、 DNSベースのアプリケーションは難読化されます。すなわち、アプリケーションサーバの本当のプライベート IPアドレスがユーザデバイスに公開されることはなく、ユーザがアクセスするアプリごとに合成された IPアドレスがクライアントで動的に作成されます。

- ユーザに内部アプリケーションへのアクセスが許可されていない場合、ネットワークトラフィックがデータセンタに到達することはありません。要求がクラウドでブロックされるため、ユーザが重要なアプリケーションサーバの「入口」にたどりつくリスクも排除されます。これを理解する最も簡単な方法は、サーバへの SSH または RDP のセッションを確立する前にクラウドでユーザを切断することです。(総当たり攻撃や認証情報の不正取得を除けば) ユーザが SSH/RDPセッションを認証できない可能性が高い場合であっても、このアーキテクチャによってこのリスクが排除されます。最大のメリットは何かと言えば、これらのすべての試行がログに記録されるため、ユーザが何をしようとしているかをセキュリティ部門が事前に (および事後に) 監視できる点にあります。たとえば、すべてのログを Splunk などの SIEM に送信し、1人のユーザが X分間に同じサーバ /ポートに対して何かを X回試行してポリシーによってブロックされたら (具体例としては、同じユーザが5分間に sap.company.com に対して SSH を20回試行したら) アラートが作成されるようにすることができます。ユーザがポリシーによってブロックされれば、セキュリティは保たれ、そのユーザのデバイスが感染したのか、あるいはユーザが意図的にそのような行為を実行したのかどうかをプロアクティブに判断できます。ユーザがポリシーによってブロックされなかった場合は、おそらくは SSHセッションは仲介されたものの、認証情報が正しくないためにサーバが却下したことになり、すなわち、このユーザは承認されたものの、管理 (root) パスワードを忘れたことを意味します。

03

すべてのユーザネットワークをインターネットカフェやゲスト WiFiネットワークの場合と同じように処理する必要があります。ユーザの場所が本社の敷地内、ブランチオフィス、工場、あるいは外出先であったとしても、ネットワークに接続させてしまえばアプリケーションサーバやデータセンタにアクセス、もしくはルーティングが可能となるため、特例扱いはできません。一部のブランチサイトでは、ユーザがアプリにアクセスする際の条件が異なる場合もあることに注意することが重要です。その場合、 IoTデバイスやサーバ同士などの通信にプライベートネットワーク接続が必要になることもあるでしょう。そのような条件を要するネットワークでも、ユーザネットワークから分離することをお勧めします。

04

最高のセキュリティとユーザエクスペリエンスを実現するには、インターネットアクセス、すなわちセキュリティスタックにもモダナイゼーションが必要です。ユーザを企業ネットワークから切り離すには、トラフィックを中央のデータセンターでインスペクションするのではなく、ユーザから直接送信する方法に切り替えることが必要です。例えば、ブランチオフィスで使っているルータやファイアウォール、 SD-WANデバイスを Zscaler Internet Access プラットフォームなどのクラウドセキュリティソリューションに接続するといった単純な方法で、インターネットのすべてのトラフィックを検知できます。ゼットスケーラーのソリューションは完全なセキュリティスタックを備えた SEaaS (Security-as-a-Service) であることに加え、世界中に150箇所以上のロケーションがあるため、最も近い Zscaler サイトに送信してインスペクションすることが可能です。外出先であっても、ユーザのモバイルデバイスやノート PC にインストールされた軽量のエージェントである Zscaler App クライアントによって、優れたユーザエクスペリエンスが提供され流だけでなく (バックホールではなく、最も近い Zscalerノードにローカルでインターネットトラフィックが送信されます)、そのような状況でも、 ITチームが必要とするセキュリティコントロールや可視性が提供されます。

ZTNAアーキテクチャの導入を可能にする3つのフェーズ

アーキテクトの方々からよく受ける「何から始めればいいのか」という質問に対して、多くの場合「状況によって異なる」とお答えしています。達成できる成果はさまざまであり、具体的なニーズ、要件、構成によって異なるため、大多数のエンジニアやアーキテクトの方々がこの回答に同意してくださっています。しかし我々は、その過程で推奨されるいくつかのベストプラクティスを提示することも自分たちの責任であると考えます。このセクションでは、その過程をいくつかの段階に分けて進める方法を紹介しますが、それぞれの組織が従わなければならない手順がすべて確定しているわけではありません。これまでの多くの事例で得られた、現在の要件を満足するためのアプローチを概説したものであり、組織がゼロトラストネットワーキングのコンセプトの採用を可能にする提案でもあります。トラストとは、何らかの形で暗示されるものではなく、ユーザ、デバイス、サービスなどの管理者が設定したコンテキストによるポリシーに基づき、その都度得られるものです。

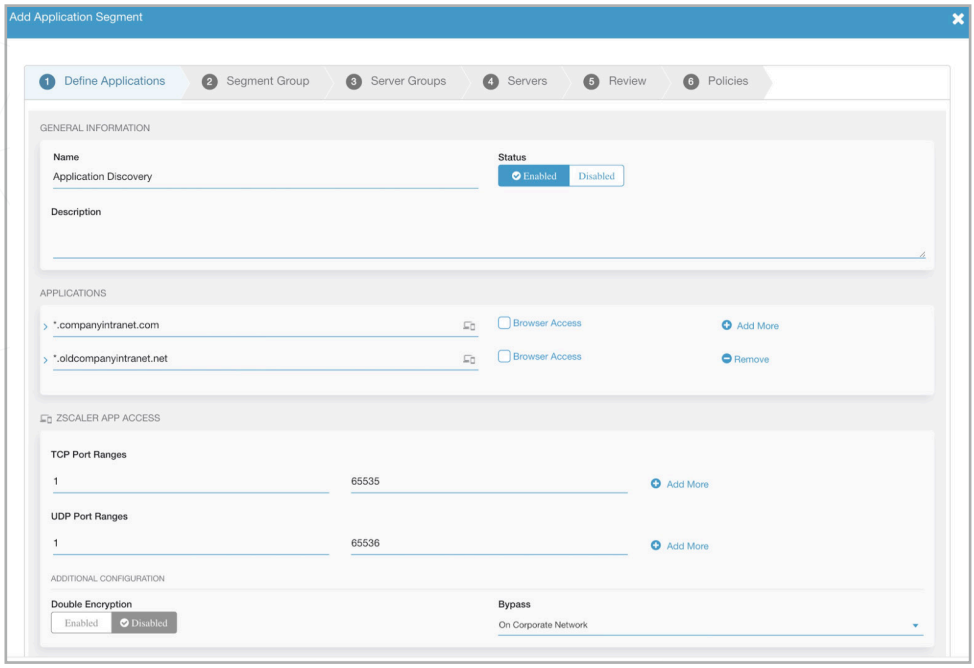
このアプローチは、喩えるなら乳児の歩みのようなものです。リモートユーザから始め、セグメントを開発した後に、ZTNA を利用してすべてのユーザが場所に関係なくプライベートアプリにアクセスできるようになったとして、その過程で、ユーザがアプリケーションやサービスにアクセスする方法、場所（データセンタ、クラウド IaaS環境、従業員の物理的な勤務地）、その配分（数やタイプ）、プロジェクトベースのタイムラインの検討が必要になるでしょう。VPN の再検討は、既存の VPN では解消できない課題が存在する「常時オン」を前提とする VPN を念頭に置いたものではなく、ZTNA の導入のきっかけとするべきです。

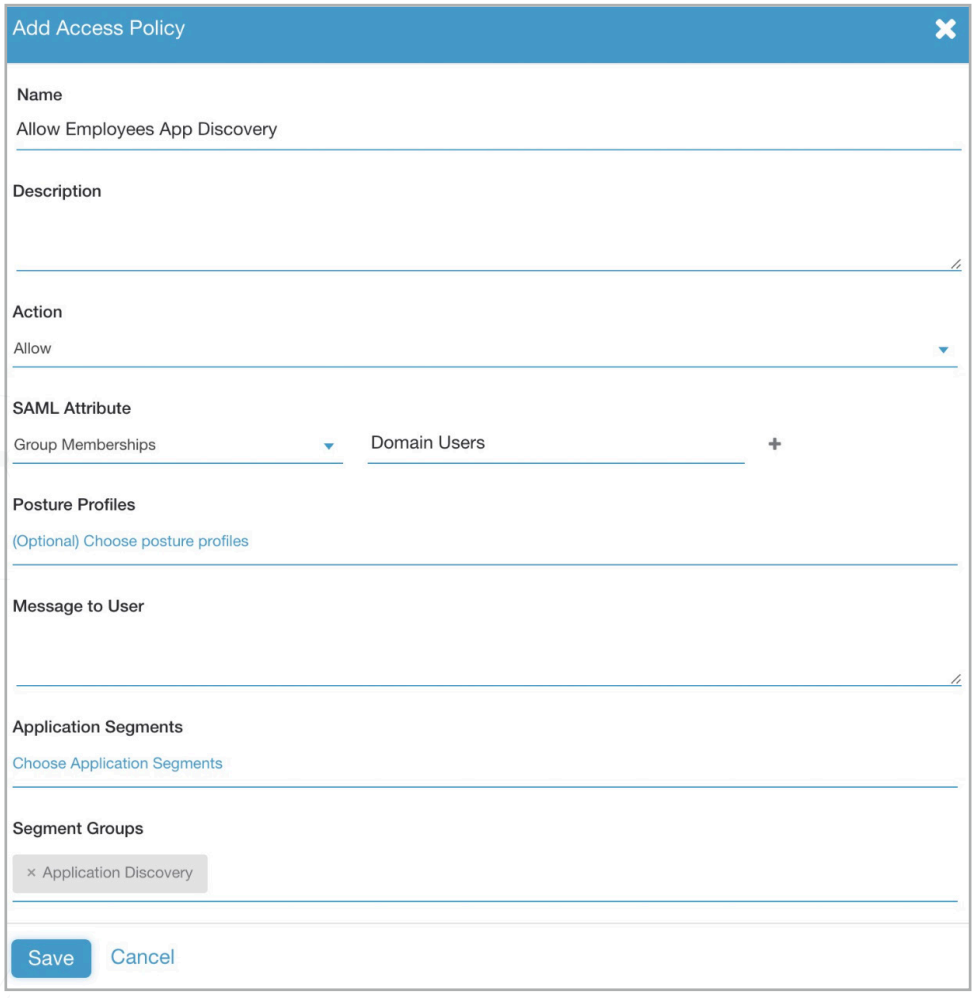
フェーズ1　ZTNAを導入し、リモートアクセスやアプリケーション検出に利用する

このフェーズでは、まず初めに、既存のリモートアクセス VPNソリューションをリプレイスします。そのために、現在のリモートアクセス VPN と同等のアクセスレベルを実現する ZTNA を導入する必要があるでしょう。これは、新しいイニシアチブによってリモートユーザの生産性が低下したと判断されないようにする上で重要なことです。

また、どのようなプライベートアプリが環境で実行中であるかを理解することで、攻撃対象領域を少なくし、シャドー IT を解消する必要もあります。想定よりはるかに多数のアプリが存在する可能性があります。Zscaler Private Access（ZPA）の「Application Discovery（アプリケーション検出）」機能でこれを解決できます。それぞれのユーザがアクセスする必要があるすべての内部アプリケーション /サービスを把握するのは不可能であるため、「Application Discovery」では、*.company.net、TCP と UDP のすべてのポートといったワイルドカードを利用できます。

ユーザのサービスへの登録が成功すると、ユーザがオフネットワークになったことをクライアントが自動的に検知し、ユーザがネットワーク外にいる状態では、すべての内部アプリケーションが ZTNA を経由するようになります。ユーザは、VPNクライアントを起動することなく、以前と同様に内部リソースにアクセスできます。これらのすべてのアクセスログに ZPA管理コンソールからアクセスできるだけでなく、任意の SIEM にほぼリアルタイムでログをストリーミングする事が可能なため、ユーザがどのアプリケーションにアクセスしているかを詳しく確認できます。



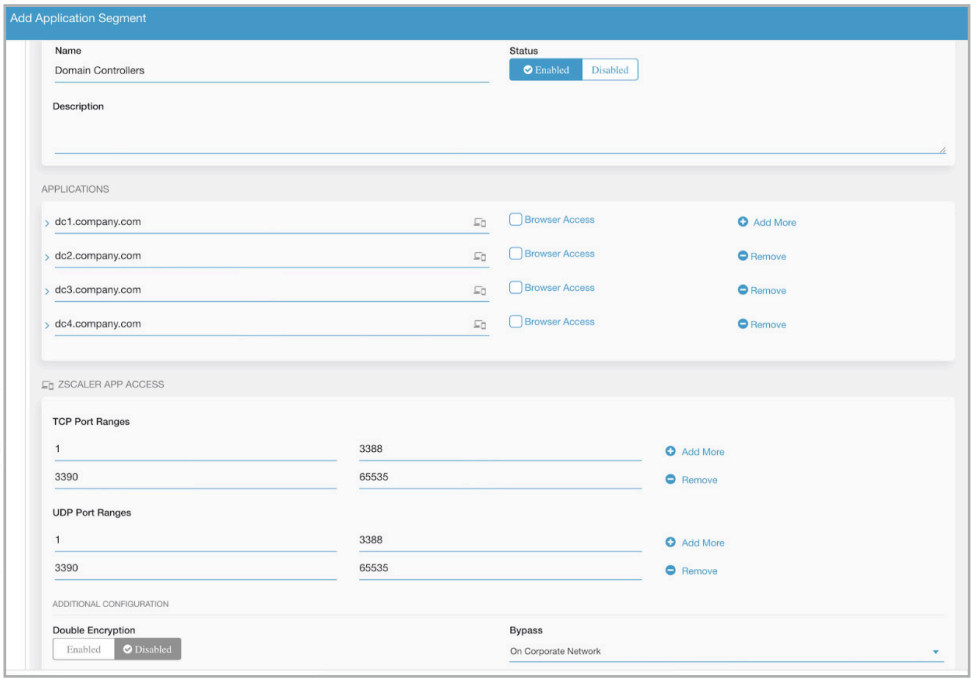


内部プライベートネットワーク（MPLS、サイト間 VPN）がまだ存在している可能性が高いため、ユーザが会社のネットワークに復帰すると、Zscaler Appクライアントによって ZPA が自動的にオフになります。この状態では、内部アプリケーションへのすべてのアクセスが、Zscalerの介在なく LAN で処理されます。

フェーズ2　マイクロセグメンテーションを活用することで、接続の権限を最小限にする

このフェーズでは、ポリシーを定義してプライベートアプリケーションをセグメントに分割し、ユーザのアイデンティティ属性によってそれらのセグメントへのアクセスが提供されるようにする必要があります。

大規模の組織には数百あるいは数千のアプリケーション /サービスが存在するため、多くの組織は、TCP 22（SSH）や TCP/UDP 3389（RDP）などの管理ポートのセグメンテーショントから始め、これらのポートへのアクセスをグローバルで ITユーザだけに提供するようにします。もちろん、1回限りの要件が発生する可能性は常にありますが、このセグメンテーションによって、アクセスするべきではないサーバにユーザが接続してしまうリスクを減らすことができます。たとえば、営業担当者が SAPアプリケーションをホスティングしている Windows Server の TCP 3389にアクセスする必要はないはずです。同じサーバを利用するとしても、ポート TCP 80/443でフロントエンドの Web の部分だけにアクセスできればよいはずです。



ドメインコントローラもしくはサービス、セキュリティソフトウェアクライアント、ソフトウェアを展開するクライアントなどのインフラストラクチャサーバであれば、ホストであることが明白であるため、簡単にセグメンテーションできます。

アプリのセグメンテーションは継続するプロセスであり、一般的な推奨事項として、ビジネスにとって最も重要で、特定のタイプのユーザだけがアクセスするアプリケーションを優先的にセグメンテーションすることをお勧めします。

アプリケーションをセグメンテーションすると、それらのアプリケーションは「Application Discovery（アプリケーション検出）」の「プール」から削除されます。これは、このような組み合わせとマッチングによって、明示的に定義していないドメイン内のアプリケーションにユーザが引き続きアクセスできるようにするだけでなく、必要なサービスポートで既知のアプリケーションにアクセスすることもできることを意味します。

インターネットセキュリティも必ず念頭に置くこと

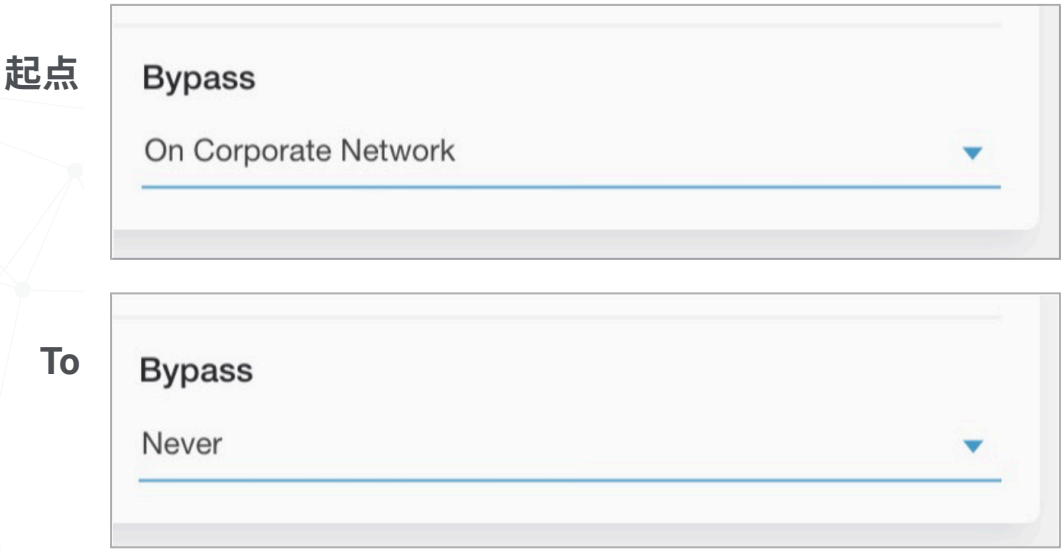
本ガイドではプライベートアプリケーションを中心に解説してきましたが、忘れてならないのは、インターネットへのトラフィックにもセキュリティスタックを提供することです。多くの組織が、アプライアンスや仮想アプライアンス（ファイアウォールなど）に頼ることのない、完全にクラウドベースのインバウンドやアウトバウンドセキュリティスタックへのモダナイゼーションを検討しています。ゼットスケーラーは、Zscaler Internet Access（ZIA）と呼ばれる、アウトバウンドクラウドセキュリティソリューションを提供しています。

フェーズ3　ZTNAで（リモートユーザだけでなく）全ユーザにプライベートアプリへのアクセスを提供する

これで、最終フェーズへと進む準備が完了しました。すなわち、プライベートアプリケーションへのすべてのアクセスが正確に設定され、明示的で最小限の権限での接続がデフォルトで設定されたということです。

この接続は、ZPAによって、内側から外側へのセッションごとの接続としてTLSの二重に暗号化されたトンネル経由で提供され、許可されたユーザと指定されたプライベートアプリの間にセキュアセグメントが作成されます。

ここで、Zscaler Appによるネットワークの検知の方法に関する前述の説明を思い出してみましょう。すなわち、ZPAには、アプリケーションセグメントごとに、(1) ネットワーク内にいる場合 ZPAをバイパスする、(2) 常に ZPAをバイパスする、(3) ZPAをバイパスしないという構成オプションがあります。フェーズ 1では、(1) のオプションを使用してアプリセグメントを展開しましたが、リモートユーザだけでなく、全ユーザにセキュアアクセスを提供するには、どうすればよいのでしょうか？その方法は簡単で、アプリのセグメントを ZPAをバイパスしないように切り替えるだけです。つまり、ユーザがオフィスにいる場合も、内部リソースへのすべてのアクセスがこの明示的なトラストアーキテクチャソリューションによって仲介されることになり、LAN上でデータセンタのアプリケーションサーバに直接ルーティングされることはありません。



手順はとても簡単ですが、この切り替えに関連する課題がプラットフォームではない場所に残されていると言えるでしょう。前述のとおり、最終的な目標は多くの場合に、アプリケーションサーバやデータセンタネットワークをすべてのユーザネットワークから完全に削除することであり、これは、どのブランチオフィスや工場などからもデータセンタに接続できなくなることを意味します（これらの場所のユーザネットワークからの接続がなくなるという意味ではありません）。

最終的な考察とヒント

一番簡単なのは、まだネットワーク外にいる、新しい小規模のオフィスから始めることでしょう。ブロードバンドインターネット接続だけでそのオフィスを開設します。インターネットへのすべてのトラフィックがクラウドセキュリティプラットフォーム（ZIAなど）に送信されるようにし、プライベートアプリケーションのすべてのトラフィックがZPAプラットフォームに送られるようにします。

喩えるなら、インターネットカフェをオープンするようなものです。ここで重要なのは、この接続方法であっても、ユーザがアプリケーションにアクセスできるということです。センサ、IoTデバイス、サーバを利用する工場などの場所であれば、プライベートMPLSやVPNを利用してデータセンタと通信する必要があるでしょう。これらの場所のネットワークを1つのデータセンタと考え、すべてのユーザをリモートユーザと考えるようにし、すべてのユーザが「ゲストWiFi」を利用し、内部アプリアクセスが認証されたユーザに仲介されるようにします。

最終的に言えるのは、ZTNAやSDPが注目され、盛り上がりを見せていますが、これらのアーキテクチャの真の目標は、プライベートアプリへのアクセスに優れたユーザエクスペリエンスと必要とされるセキュリティを提供することです。この新しい方法を組織が採用するには時間がかかりますが、ネットワークアーキテクトであれば、それを可能にする基盤（プラットフォーム）を構築できるはずです。

ホスティング型のZPAを無料で7日間ご利用いただけます。
登録はこちらから：**https://www.zscaler.jp/zpa-interactive**

ゼットスケーラー株式会社
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ3階
www.zscaler.jp