Zscaler™による Microsoft 365へのアクセスを 実装するためのベストプラクティス

著者：

Naresh Kumar
ゼットスケーラー　プロダクトマネジメント担当ディレクタ

Misha Kuperman
ゼットスケーラー　クラウドオペレーション担当シニアバイスプレジデント

zscaler™

本書はゼットスケーラーが提供するものです。すべてのベストプラクティスおよび技術的推奨事項は、Microsoftプロダクトグループとの緊密な連携とレビューを通じて、Microsoft 365の接続（https://aka.ms/pnc）に関してMicrosoftが推奨する原則に基づいて策定されています。

目次

はじめに

目的

本書では、Microsoft 365のパフォーマンス、セキュリティ、およびユーザエクスペリエンスを最適化することを目的に、Zscaler Internet Access™ (ZIA™) ソリューションの構成方法に関するベストプラクティスと推奨事項を紹介しています。この推奨事項は、Microsoft 365の接続 (https://aka.ms/pnc) に関してMicrosoftが推奨する原則に基づいて策定されています。

対象読者

本書は、Microsoft 365とZIAを組み合わせた使用を検討しているIT管理者を対象としています。ZIAおよび、Webセキュリティ、ネットワークセキュリティ、Active Directory、アイデンティティ管理、ディレクトリサービスといったいくつかのテクノロジに関する十分な知識があることを前提とします。

Microsoft 365について

Microsoft 365 (旧称 Office 365) は、クラウドベースサービスの製品群として、堅牢なセキュリティ、信頼性、ユーザの生産性のニーズを満たしています。アップグレード時の新バージョンの購入とインストールは不要で、Microsoft 365の構成製品は自動的に更新され、常に最新バージョンが使用可能です。Microsoft 365のアプリケーション製品は、クラウドからブラウザを経由して提供されます。Microsoft 365のライセンスは、ユーザに対して付与され複数デバイスをカバーすることができ、オフライン / オンラインを問わず、すべてのサポート対象デバイスに一貫したエクスペリエンスを提供します。Microsoft 365には、一般的なOffice製品 (Word、Excel、PowerPoint、Outlook) に加えて、OneDrive、Microsoft Teams、SharePoint、Yammer、およびOneNoteが含まれます。

詳細については、「Microsoft 365について」および「Microsoft 365のサポート」の章を参照してください。

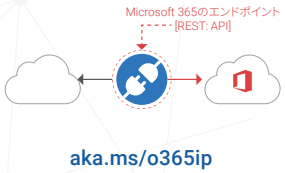
注：Microsoft 365は、World-Wide Commercial Cloud、U.S. Government Cloud、Germany Cloud、China Cloudなど、お客様向けに複数のクラウドサービスが提供されています。本書の内容は、Zscaler for Microsoft 365 World-Wide Commercial Cloudを対象とします。

Microsoftの接続に関する原則

Microsoft 365は、規模に関わらず世界中のほとんどの企業にとって、標準の生産性向上プラットフォームとなっています。Microsoft 365は、柔軟なコラボレーション機能を備えた使いやすく費用対効果の高いソリューションのため、多くの企業にとって最適な選択肢です。

以降の章で示すMicrosoftが推奨している原則は、Microsoft 365の接続とパフォーマンスを最適化することを目的としています。本書に記載しているMicrosoft 365の接続に関する原則に従ってトラフィックを管理して、Microsoft 365への接続時のパフォーマンスを最大限に高めるようにしてください。

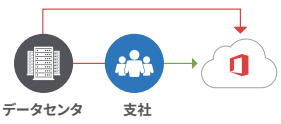
Microsoft 365のネットワーク接続に関する原則



aka.ms/o365ip

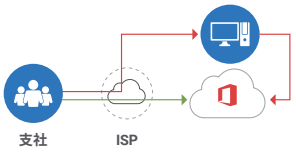
Microsoft 365トラフィックの最適化

エンドポイントのカテゴリを使用してMicrosoft 365のトラフィックを区別することで、ルーティングの効率を高めます。



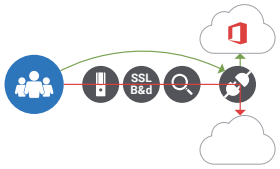
ローカルEgress（出口）の有効化

適合するDNS解決によって、インターネットを介したMicrosoft 365のデータ接続の出口をできるだけユーザの近くに配置します。



ダイレクト接続の有効化

Microsoft 365の接続に対してダイレクトEgress（出口）を有効にします。ネットワークヘアピンを回避して、Microsoftグローバルネットワークに対するネットワークレーテンシ（RTT）を最小化します。



SaaS向けセキュリティの最新化

Microsoft 365の接続に対する干渉的なネットワークセキュリティを回避します。バイパスプロキシ、トラフィックインスペクションデバイス、Microsoft 365で既に利用できる重複セキュリティを検証します。

Microsoft 365 ネットワーキングパートナープログラム

Zscaler Internet Access（ZIA）は、Microsoft 365との連携が確認済みです。ZIAはMicrosoft 365 ネットワーキングパートナープログラムの認定を取得しており、パフォーマンスや動作に関する既定の最適化内容の提供を受けています。本書で紹介しているベストプラクティスと組み合わせることで、最適な構成のための適切な導入方法を選択することができます。Microsoft 365 ネットワーキングパートナープログラムの詳細については、こちらを参照してください。

Zscaler Internet Access（ZIA）について

ZIAは、専用に構築された世界最大のセキュリティクラウドからサービスとして提供されるセキュアなインターネット /Webゲートウェイです。ZIAは、あらゆる規模の企業で必要とされる、細部にまでわたる保護機能を備えた、包括的なセキュリティスタックを提供します。ZIAは、Zscaler Zero Trust Exchange™ の主要コンポーネントであり、Zscaler Zero Trust Exchangeは、ユーザ、アプリケーション、デバイスをあらゆるネットワークを介して、あらゆるロケーションから安全に接続するクラウドネイティブプラットフォームです。各種のビジネスポリシーを適用することで、ユーザの生産性向上、ビジネスリスクの低減、コストの削減、ITの簡素化を実現します。

ゼットスケーラーはMicrosoftと協力して、さまざまな企業がオンプレミスの導入環境からMicrosoft 365 クラウドに移行することを支援してきました。ゼットスケーラーとの細部にわたる統合は、Microsoftが推奨するネットワーク関連の原則に従っています。これらの原則は、シンプルなワンクリック構成を通じて、最適なユーザエクスペリエンスとセキュアな接続の実現を目的としています。

Microsoft 365に対応するゼットスケーラーのワンクリック構成

ゼットスケーラーのワンクリック構成によって、Microsoft 365 アクティビティの可視性を高めて、管理を簡易化して、制御を強化することができます。

ゼットスケーラーのワンクリック構成

Microsoft 365の管理を簡素化

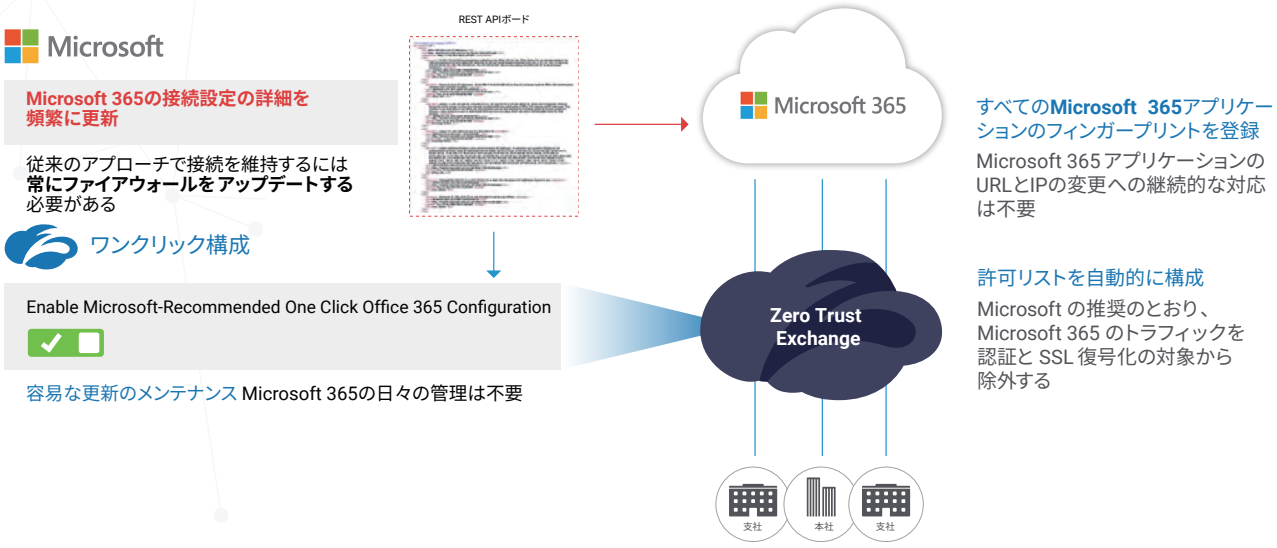


図2–Microsoft 365に対応するゼットスケーラーのワンクリック構成

ゼットスケーラーとMicrosoft 365を使用するメリット

ゼットスケーラーのワンクリック構成は、Microsoft 365を使用するうえで次のようなメリットをもたらします。

1. 導入

a. Microsoft 365とインターネットのトラフィックにどこからでもローカルでアクセスでき、オンプレミスのネットワークセキュリティハードウェアの導入や管理が不要です。

2. 管理

a. Microsoft 365のIPとURLの変更の管理を自動化することで、接続がブロックされることを防止したり、Microsoft 365の接続に関する原則に従って接続をインスペクションしたりできます。

3. 最適化

a. Zscaler Cloudは、Microsoftのグローバルネットワークおよび世界中の主要ISPとピアリングすることで、Microsoft 365のフロントドア宛てのエンドユーザトラフィックを最適化します。

b. ゼットスケーラーの高速なローカル DNSサービスによってレイテンシを低減して、ユーザを最寄りのMicrosoft 365 フロントドアに接続します。

ゼットスケーラーでは、上記のほかにも、帯域幅制御、Zscaler Client Connector、TCPウィンドウシェーピング、UDPサポート、ダッシュボード可視化など各種機能を提供しており、これらはすべてエンドユーザエクスペリエンスを向上させます。

ネットワークトランスフォーメーション

ローカルインターネットブレイクアウト

Microsoft 365の需要はこれまで以上に高まっていますが、Microsoft 365をこれから導入しようとしている多くの企業は、Microsoft 365が提供するクラウドネイティブのアプリケーションとサービスを最大限に活用するための適切なネットワークアーキテクチャを持っていません。

多くの企業は、ハブ&スポーク方式のネットワークを利用しており、アプリケーションがホストされてセキュリティ防御策が施されている中央のデータセンタを経由して、支社からトラフィックをルーティングしています。このようなアーキテクチャでは、レイテンシが大幅に増加して、Microsoft 365のようなアプリケーションのユーザエクスペリエンスが損なわれることになります。Microsoft 365は分散型クラウドサービスであり、地理的 / ネットワーク的にユーザに近接してフロントドアが分散配置されています。このような状況下でハブ&スポーク方式のネットワークを使用すれば、多大なレイテンシが加わり、ユーザエクスペリエンスとアプリケーションパフォーマンスの低下につながります。

Microsoftとゼットスケーラーはどちらも、できるだけユーザに近接してローカルネットワークのEgress（出口）を配置することを推奨しています。**Office 365の接続に関する主要原則**の1つである「ネットワーク接続の出口をローカルに配置する」という原則に従うことで、ユーザトラフィックのレイテンシを最小化できます。そのためには、企業ネットワークの内外にいるユーザに対してローカルのEgress（出口）とDNSを有効にします。レイテンシを低減すると、Microsoft 365のユーザエクスペリエンスが最適化されるため、企業ネットワーク、VPN、DNSのヘアピンを避けて、ユーザが可能な限り素早くEgress（出口）にアクセスできるようにすることができます。

ローカルインターネットブレイクアウトに関する検討事項

- ゼットスケーラーは、複数のデータセンタを世界各地に配備することで、レイテンシを低減して、ローカルエンドユーザ群との障害に強い接続を実現しています。
- お客様はデータセンタの地理的位置を考慮するだけでなく、業務時間中の往復遅延とパケット損失に関する指標も検討する必要があります。

最適なロケーションを検証するには、https://config.zscaler.com/を参照して、プライマリサイト、バックアップサイト、3次サイトに対する現地業務時間中のレイテンシと損失に関するデータを確認してください。詳細については、お客様の担当アカウントチームまたはサポートにお問い合わせください。ゼットスケーラーは、管理ポータルを通じてGREトンネルをセットアップするためのセルフプロビジョニング機能もサポートしています。

最適化された接続を確保するために、Zscaler Cloudに対する接続を、お客様のすべての支社でセットアップしてください。

Microsoftとのルーティング / ピアリングの最適化

ゼットスケーラーは、世界中の主要データセンタでMicrosoftとピアリングしています。

ゼットスケーラーは、ピアリングを必要としたり希望したりするすべてのお客様向けの標準対応の一環として、インターネットエクスチェンジに接続され、Microsoftネットワークとダイレクトされているデータセンタを指定しています。

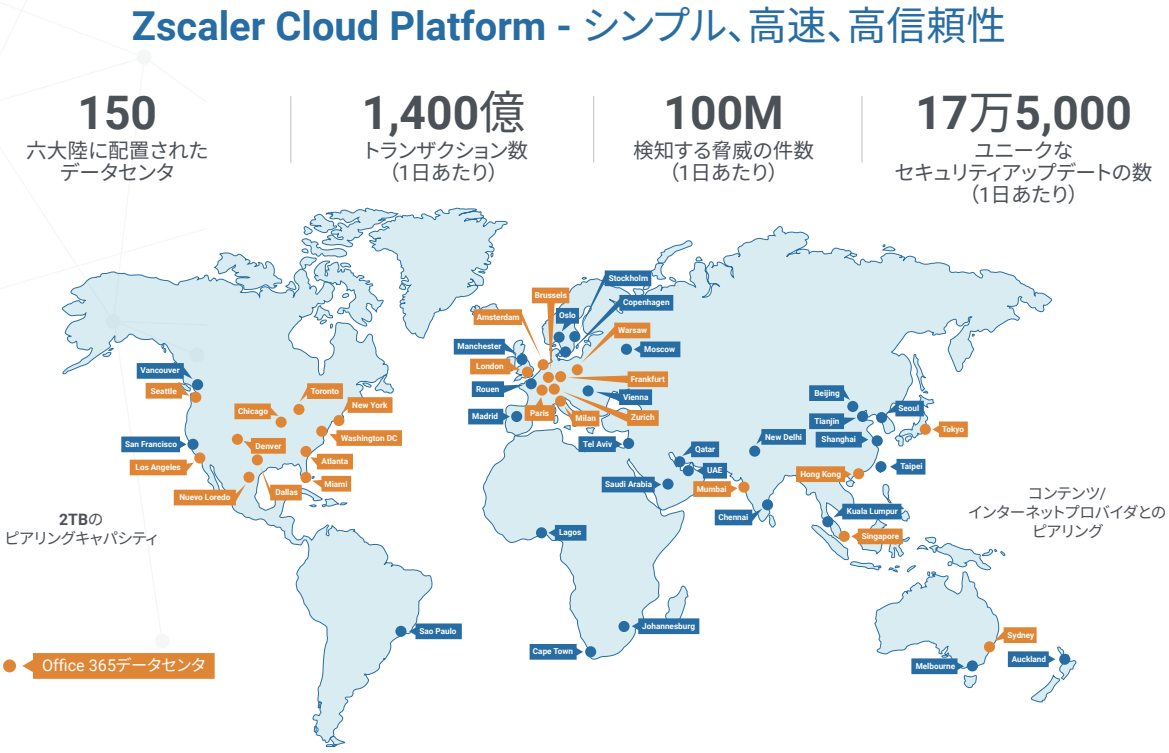


図3–グローバルに配備されたZscaler CLoud

ゼットスケーラーはオープンピアリングポリシーを定めており、これは、あらゆるプロバイダとピアリングする可能性を意味し、この性能は他の主要サービスに拡張されることがあります。

ローカルインターネットブレイクアウトを可能にするための主な推奨事項を3点あげます。

- ロケーション / サイトの識別：多くの企業が自社ネットワークを設計する際に採用しているハブ &スポーク方式のモデルでは、トラフィックをインターネットに直接転送するロケーションの数は限られています。ローカルインターネットブレイクアウトについて計画する際は、トラフィック量が特に多いロケーションと、プライベートネットワーク経由のバックホール距離が特に長いロケーションを優先してください。
- ゼットスケーラーに対して正しいトラフィック転送方式を選択してください。
- Microsoft 365のワンクリック構成を有効にして、Microsoft 365のアプリケーションとサービス宛ての推奨される信頼性の高い接続を確保してください。

Microsoft 365のネットワーク導入オプション

Microsoft 365は、多様なアプリケーションとマイクロサービスを通じて生産性向上とコラボレーションのためのサービスを提供する分散型 SaaS (Software-as-a-Service) クラウドです。これらのアプリケーションとサービスの多くは、エンドユーザとデータセンタの間で独自の方法で連携して、それぞれのアプリケーションやサービスの目標を達成します。このことを念頭に置いて、信頼性と速度に関するエンドユーザエクスペリエンスの水準を維持するために、導入手法は変化する可能性があります。

Microsoft 365 ネットワーキングの目標

Microsoft 365 ネットワーキングの最終目標は、エンドユーザエクスペリエンスを最適化することです。そのための手段として、最短距離のMicrosoftネットワーク POPを通じて、クライアントと最寄りのMicrosoft 365 フロントドアの間で最も高速かつ最も直接的な接続を確立します。エンドユーザエクスペリエンスの品質は、クラウドアプリケーションをサポートしている接続のパフォーマンスと即応性に直接関係します。例えば、Microsoft Teamsは、ユーザの通話、会議、共有画面コラボレーションで問題が発生しないように低レイテンシを必要としている一方で、Outlookは、サーバー側のインデックス作成機能とAI機能を活用するインスタント検索機能をサポートするために、高品質なネットワーク接続を必要としています。

そのため、ネットワーク設計における第1目標は、クライアントマシンからMicrosoftグローバルネットワークまでの往復時間（RTT：round-trip time）を短縮化することでレイテンシを最小化することです。Microsoftグローバルネットワークは、Microsoftのパブリックネットワークバックボーンとして、世界中に分散された低レイテンシかつ高可用のクラウドアプリケーションエントリポイントによってMicrosoftの全データセンタを相互接続しています。

この低レイテンシという目標を達成するために、**Microsoftは、Microsoft 365 ネットワーキング接続に関する原則を策定しました。** さらに、Microsoft 365 ネットワーキングパートナープログラムでは、お客様がMicrosoft 365のエクスペリエンスを向上させるための性能強化を支援しています。この目的の達成のために、お客様の導入環境でMicrosoft 365の接続を最適化するための主要な原則に一貫して従っていることを示す、検証済みのパートナーソリューションを簡単に照会できるようにしています。ゼットスケーラーは、Microsoft 365 ネットワーキングパートナープログラムに参加している数少ないセキュリティベンダーのうちの1社です。

Zscaler for Microsoft 365を使用した導入のベストプラクティス

トラフィック転送：

Zscaler Internet Accessにトラフィックを転送するには、主に次の4つの方法があります。

- GREトンネル
- IPsecトンネル
- Zscaler Client Connector
- PACファイル

企業ロケーション（データセンタや支社など）からのトラフィック転送

ゼットスケーラーのサービスにトラフィックを送信するには、送信元クライアントまたは中間ノード（ゲートウェイ）のどちらかが、ポリシー適用のためにゼットスケーラーのデータセンタ（Zscaler Public Service EdgeまたはZscaler Private Service Edge）と直接通信する必要があります。

企業のロケーションからゼットスケーラーのデータセンタへ多様なトンネルを構築し、ゼットスケーラーセキュリティプラットフォームを通じてインターネット宛てのトラフィックを伝送する必要があります。ゼットスケーラープラットフォームにトラフィックを転送するロケーションでは、VPNトンネリングオプションとしてGREとIPsecがサポートされています。ゼットスケーラーでは、特に大規模な企業ロケーション向けにGREトンネルを推奨しています。

詳細については、**https://help.zscaler.com/zia/best-practices-deploying-gre-tunnels**を参照してください。

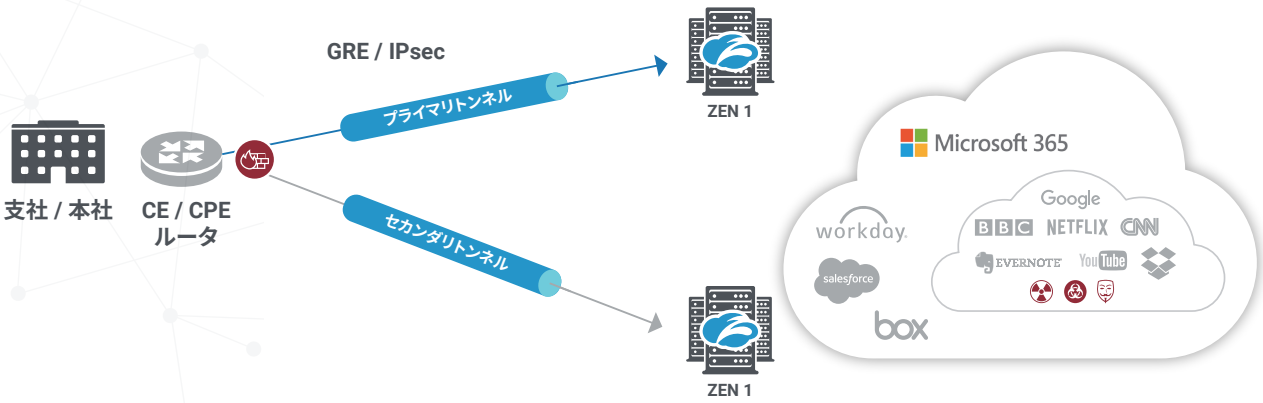


図4–トラフィック転送

一般的な推奨事項として、きめ細かいトラフィックルーティングの実現のために、トンネル構成はZscaler Client Connector（旧称 Zscaler App）などのクライアントベースのトラフィック転送手段と同じサイトに存在することが推奨されます。これにより、送信元 IPが制限されたアプリケーションなどに対する制御メカニズムが適用できると共に、冗長なDNS解決を可能な範囲で低減できます。

MTU/MSSの設定：

GREまたはIPsecを使用する場合は、ゼットスケーラーのサービスにトラフィックを送信する際の基本となる伝送メカニズムを理解することが重要です。トンネルを介してトラフィックを送信する際は、MTU（Maximum Transmission Unit - 最大パケットサイズ）やMSS（Maximum Segment Size - 1つのパケットで送信されるデータ量）などの設定値が重要になります。どちらかのケースでパケットが大きすぎると、通常 TCPは継続して機能しますがパケットのフラグメント化が発生します。

ゼットスケーラーのサービスへのトンネル作成時は、企業において値を適切に算出することが重要です。ゼットスケーラーが公開している構成と計算の例については、**https://help.zscaler.com/zia/determining-the-optimal-mtu-for-gre-or-ipsec-tunnels**をご確認ください。ただし、企業にとっての最適なTCPエクスペリエンスを確保するためには、トンネル作成時に計算することが求められます。

トンネルの監視：

トンネルの監視は当然のことながら推奨されます。クラウドサービスという特性上、トンネルはレイヤ 7で監視される必要があります。IPアドレスによる監視は、クラウドアーキテクチャを構成している一部のマシンによるサービスの参加や離脱がサービス全体に影響を与えない可能性もあり、効果的ではありません。これらのマシンのIPを確認した場合、サービスが正常に稼働している場合でも、何らかのダウンが誤認識される可能性があります。

ゼットスケーラーでは、トンネル自体のIP SLAチェックに加えて、**http://gateway.zscalerone.net/vpntest**までのトンネルを介したレイヤ 7のヘルスチェックを推奨しています。詳細については、次のリンクを参照してください：**https://help.zscaler.com/zia/best-practices-deploying-gre-tunnels**

小規模サイトの場合は、クライアントベースで転送することも可能ですが、より好ましい方法としてトンネルが推奨されます。インターネット宛てトラフィック全般に対して推奨されるベストプラクティスを以下にいくつか紹介します。

トンネリングが使用されるロケーション:

- 企業オフィスにあるすべてのクライアントデバイスから送信されるTCP/UDP/ICMPトラフィックはすべて、GREまたはIPsecのトンネルを介してゼットスケーラーに転送されることが推奨されます。
- 認証、SSL復号化、帯域幅制御を有効にします。
- そのロケーションに対してサロゲート IPを有効にします。
- 企業環境に出入りするラップトップなどのインテリジェントデバイスでZscaler Client Connectorを使用して、信頼できるネットワークの検出やトラフィック転送の制御を行うことが推奨されます。

トンネリングをサポートできないロケーション: トンネリングを使用できないオフィスでは、Zscaler Client Connectorを使用してゼットスケーラーにトラフィックを転送することが推奨されます。Client Connectorを使用することが難しい場合は、スタンドアロンのPACファイルを代わりに使用できます（ただし推奨されません）。

リモートユーザのトラフィック転送

多くのユーザがラップトップやiOS/Androidデバイスといったモバイルテクノロジを活用している状況の中で、Zscaler Client Connectorは、デバイスのロケーションにかかわらずトラフィックをZscaler Cloudに確実に転送するための推奨手段となっています。

Zscaler Client Connectorは、信頼できるネットワークのステータスを検知して、ユーザの所在に基づいてトラフィックをゼットスケーラーに適切に転送します。つまり、ユーザが企業ネットワーク上にいるのか、従来のVPN上にいるのか、または企業インフラストラクチャから完全に離れているのかに基づいてトラフィックが転送されます。Zscaler Client Connectorには、PACファイルにはない以下のようなメリットがいくつかあります。

- キャプティブポータルの検出
- 信頼できるネットワークの検出
- ユーザの識別と認証はブラウザではなくZscaler Client Connectorによって処理される

Client Connectorの使用が難しい場合は、代わりにスタンドアロンのPACファイルを使用できます（ただし推奨されません）。

VPN上：

フルトンネル：

- フルトンネル（ゼットスケーラーのスプリットなし）：インターネットトラフィックを強制的にトンネル経由で転送させたい場合は、Zscaler Client Connectorは信頼できるネットワーク上で動作するように構成し、すべてのトラフィックが企業ネットワークに接続されているかのようにデータセンタに転送されるようにします。当然ながらZscaler Client Connectorの代わりにPACファイルを使用している場合は、PACファイルはトンネル上でも継続して機能します。
- フルトンネル（ゼットスケーラーのスプリットあり）：必要に応じて、ゼットスケーラーのサブネットをトンネル構成から除外することで、Zscaler Client Connectorのトラフィックをトンネル経由の転送から除外できます。この結果、Zscaler Client Connectorはインターネットトラフィックをデータセンタに転送する代わりに、エンドユーザに最も近いゼットスケーラーのデータセンタでポリシー制御を直接適用できるようになります。PACファイルが使用されている場合、そのPACファイルはZscaler Client Connectorと同様に機能します。

スプリットトンネル：

- スプリットトンネリングが既に許可されている場合は、Zscaler Client Connectorを使用してゼットスケーラーにトラフィックを転送してください。Zscaler Client Connectorを使用することが難しい場合は、スタンドアロンのPACファイルを代わりに使用できます。

VPN外：Zscaler Client Connectorを使用してゼットスケーラーにトラフィックを転送してください。

モバイル / リモートユーザを対象にしたMicrosoft 365/TeamsとZscaler Client Connectorの組み合わせ：

Microsoftは、VPNトンネルからの最適化された接続を必要とする、WFA（Work From Anywhere）ユーザ向けのガイドラインと、パフォーマンスが非常に重視されるMicrosoft 365 アプリケーションを分割するための手法を公開しています。これらのアプリケーションには、Microsoft Teams、Exchange Online、SharePointOnlineなどがあります。

（https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide）

最適なユーザエクスペリエンスを実現するために、ゼットスケーラーでは、Zscaler Client Connectorから送信されるTeamsトラフィックのスプリットトンネリングのIPアドレスの範囲をWFAユーザのみにすることを推奨しています。ロケーショントラフィックについては、Zscaler Public Edge Connectorに対して構成されたトンネルを介してトラフィックへの転送がベストプラクティスとなります。

WFAユーザ向けの特定トラフィックを分割する手順は次のとおりです。

- すべてのWFAユーザに対してZscaler Client Connector（バージョン 2.0以降とZ-Tunnel 2.0の組み合わせ）を導入します。導入の詳細については、次のリンクを参照してください：**https://help.zscaler.com/z-app/best-practices-deploying-z-tunnel-2.0**
- ゼットスケーラーの管理ポータルにログインして、Zscaler Client Connectorポータルにアクセスします：[Policy（ポリシー）]->[Zscaler Client Connector portal（Zscaler Client Connectorポータル）]
- 次に示すように、[Application bypass（アプリケーションバイパス）]でMicrosoft Teamsを追加します：[App Profile（アプリケーションプロファイル）]->[Windows]->[Add Windows Policy（Windowsポリシーの追加）]（既存のプロファイルを必要に応じて変更します）[Z-Tunnel 2.0 configuration（Z-Tunnel 2.0の構成）]で->[Application bypass（アプリケーションバイパス）]->[selected（選択対象）]

次に示すようにMicrosoft Teamsを追加します：

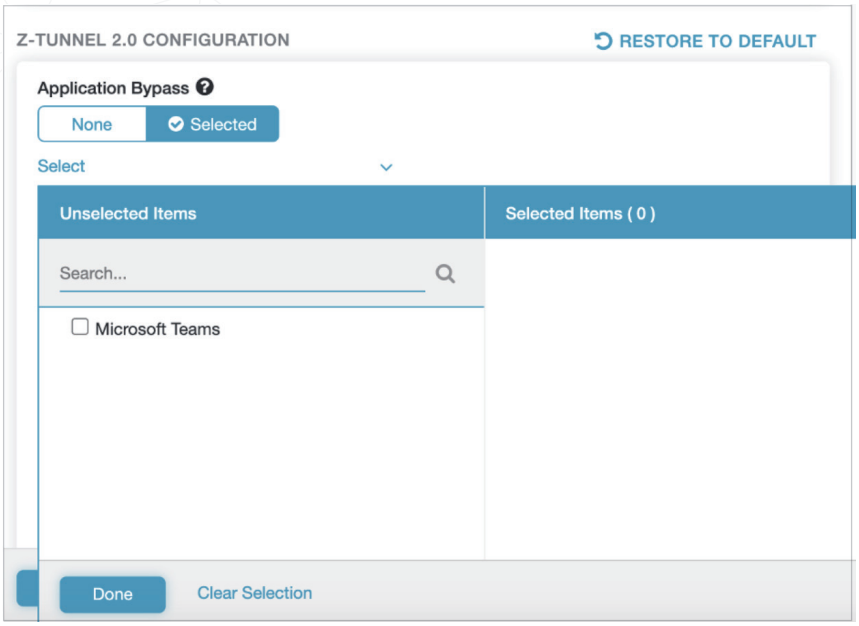


図5–Client ConnectorへのMicrosoft Teamsの追加

注：ゼットスケーラーでは、Microsoft Teamsサービス用のIPアドレスの範囲とポートを保持しています。以下に、上記のバイパス選択でカバーされているMicrosoft 365専用のIPアドレス範囲とUDPポートを示します。

13.107.64.0/18

52.112.0.0/14

52.120.0.0/14

UDP 3478、3479、3480、3481

お客様がMicrosoft Teamsサービス以外もバイパスすることを選択した場合は、以下の構成を使用して、エンドポイントの最適化されたIPアドレスの範囲とポートを手動でさらに追加できます。

注：この操作を行う場合は、関連する除外リストを定期的に見直すよう計画してください。

[App Profile（アプリケーションプロファイル）]->[Windows]->[Add Windows Policy（Windowsポリシーの追加）]（既存のプロファイルを必要に応じて変更します）

[Z-Tunnel 2.0 configuration（Z-Tunnel 2.0の構成）]で->[Destination exclusion（宛先の除外）]、IPアドレス範囲を追加します

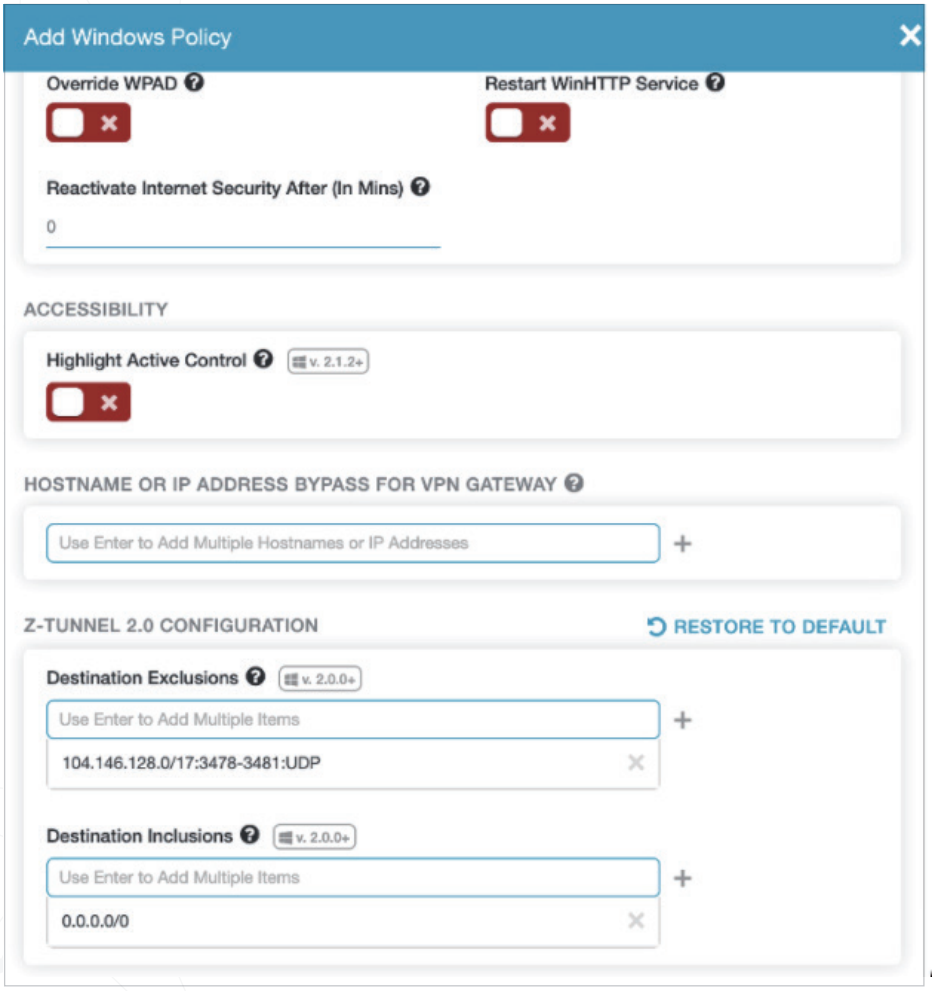


図6–IPアドレス範囲の追加

エンドポイントの最適化されたIPアドレスの範囲の詳細については、次のリンクを参照してください：

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide

PACファイルに関する問題：

PACファイルの導入においては、可視性とセキュアなアクセス制御の両方に関する多くの制限事項があります。ゼットスケーラーでは、PACファイルを用いたトラフィック転送を実施しないことを強く推奨します。PACファイルに関する問題としては、以下のものがあります。

- PACファイルの管理は、例外処理や更新が原因で非常に複雑になることがある
- PACファイルのエラーのトラブルシューティングは困難である
- PACファイルはWebトラフィックのみに適用されるため、コラボレーションアプリケーションに対してPACファイルが適切に扱われない場合は、パフォーマンス低下の可能性がある
- PACファイルが不適切に扱われた場合は（DIRECTの使用）、セキュリティリスクが生じる可能性がある

PACファイルは、セキュリティを低下させるほかにも、使用性と管理性も低下させます。Zscaler Internet AccessとMicrosoft 365を使用してパフォーマンスとセキュリティを最大限に高めるには、Zscaler Client Connectorの使用を推奨します。

Zscaler Private Service Edgeに関する検討事項

アーキテクチャ上の観点からは、組織上の制約がある場合を除いて、Zscaler Private Service Edgeの間で技術的な相違はありません。ハイブリッド環境を導入済みのお客様は、Zscaler Private Service Edgeに対して同様の配慮を持って、Zscaler Private Service EdgeをIPの範囲に追加できます。

Microsoftが推奨するワンクリック構成

Microsoft 365のアプリケーションは、ユーザエクスペリエンスを最大化しセキュリティを強化するために、Microsoft 365向けの接続とトラフィックにおいて、多様なプロトコル、接続の最適化、強力な転送時暗号化テクノロジ、高度なセキュリティチェックを採用しています。これらの接続の多くは、インラインのネットワークプロトコルとデータの処理、インスペクション、および認証前アクションの影響を受けます。このため、Microsoftは、Microsoft 365 トラフィックのインラインのネットワーク復号化とインスペクションを推奨しておらず、サポートもしていません（詳細については、https://docs.microsoft.com/en-us/office365/troubleshoot/miscellaneous/office-365-third-party-network-devicesを参照してください）。

Zscaler Internet Accessは、「Microsoft 365 ワンクリック構成」をサポートすることで、Microsoft 365のトラフィックに関する上記のMicrosoft推奨事項に完全に準拠しています。ワンクリック構成が有効になっていると（デフォルトで有効）、Microsoft 365のトラフィックはゼットスケーラーを通じて最適化されて、SSLのインスペクションレイヤと認証前レイヤをバイパスするため、パフォーマンスと相互運用性を最大限に高められます。

管理ポータルで、[Policy（ポリシー）]->[URL and Cloud App policy（URLとクラウドアプリケーションのポリシー）]->[Advanced Policy Settings（詳細ポリシー設定）]で設定を有効にします。

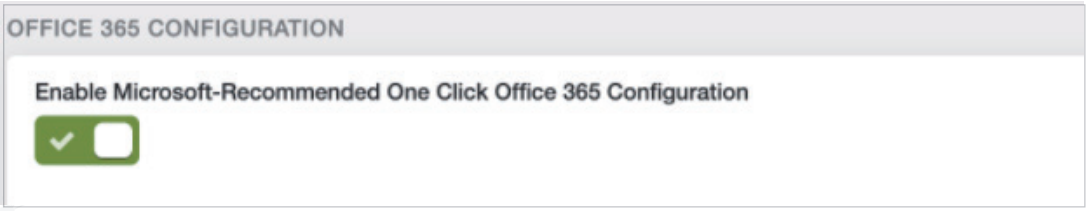


図7–ワンクリック構成の有効化

この設定を有効にしてアクティブ化すると、次の2つの自動化ポリシーがゼットスケーラーのファイアウォール内に作成されます。

1. SSLと認証を（REST APIに基づいて）識別してバイパスして、セキュリティスタックを回避することで、レイテンシを最小化するポリシー

Rule Order	Rule Name	Criteria	Action
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow

図8–SSLバイパスポリシー

2. 経路を最適化して、最も近いフロントドア・アプリケーションエンドポイントに接続するDNSポリシー

図9–DNSポリシー

推奨されるファイアウォールポリシー

ZIAを利用してすべてのWebアプリケーショントラフィックを転送しているお客様の環境において推奨されるファイアウォールポリシーを以下に示します（[Policy（ポリシー）]->[Firewall Control（ファイアウォール制御）]からアクセス可能）。ワンクリック構成によって、Microsoft 365のトラフィックを処理するためのデフォルトポリシーが自動的に取り込まれます。

注：下記のルール 1は必須ではありません。Microsoft 365はこのルールなしで動作しますが、他のWebトラフィックが正常に機能するためには、これが現在のファイアウォールに対して推奨されるポリシーです。

推奨されるポリシー

シナリオ：Auth、SSL、FWが有効化された状態でGRE/IPSecを使用して接続されたロケーション。Microsoft Office365のワンクリック構成が有効化されており、Microsoft 365専用のURLポリシーなしで、以下のようなファイアウォールポリシーのみ。

Rule Order	Rule Name	Criteria	Action
1	Zscaler Proxy Traffic	DESTINATION IP CATEGORIES Zscaler Proxy IPs NETWORK SERVICES Zscaler Proxy Network Services	Allow
2	Allow_HTTP_HTTPS_TRAFFIC	NETWORK SERVICES HTTP; HTTPS	Allow
3	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow
Default	Default Firewall Filtering Rule	Any	Block/Reset

図10–推奨されるファイアウォールポリシー

注：ZENによってすべての9440 トラフィックがプロキシに自動転送されるため、ルール 1に9440を追加する必要はありません。このため、明示的に構成する必要はありません。

結果：S4Bにログインできるとともに、オーディオ / ビデオ通話とデスクトップ共有が可能。HTTP/HTTPsからOutlook 2016、Word、putなどにログイン可能となっている。

ゼットスケーラーを使用したローカルインターネットブレイクアウトの確認

企業のローカルインターネットブレイクアウトを確認するには、以下のステップを実行します。

ステップ 1：ZIA管理ポータルで、[Administration（管理）]->[Location Management（ロケーション管理）]->[Locations（ロケーション）]にアクセスして、ロケーションの合計数を確認します。

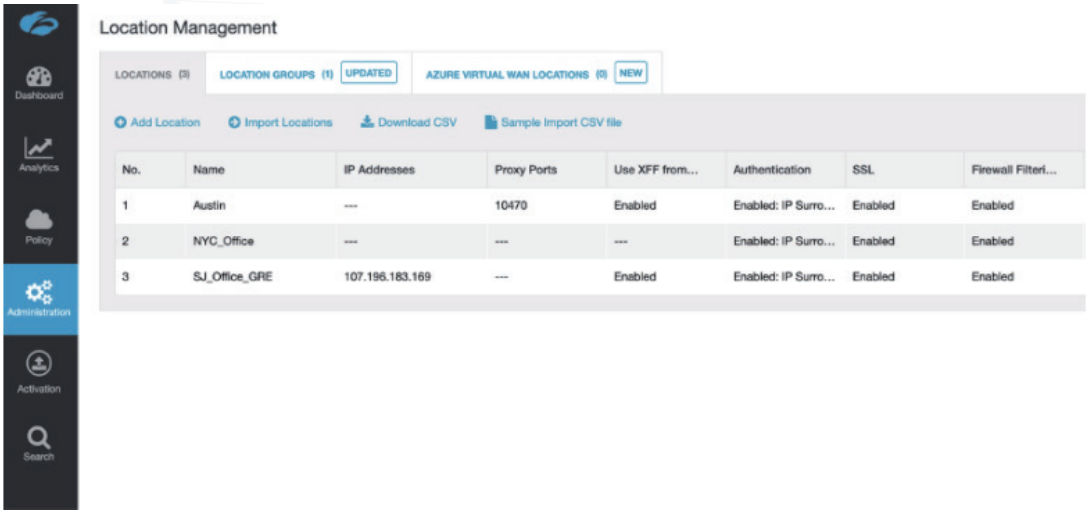


図11–管理ポータルに表示されたローカルインターネットブレイクアウト

ステップ 2：[Dashboard（ダッシュボード）]->[Microsoft 365 dashboard（Microsoft 365 ダッシュボード）]にアクセスして、[Top Office 365 Locations（上位のOffice 365 ロケーション）]ウィジェットを表示して、ローカルブレイクアウトが有効になっているロケーションの数を確認します。

図12–ローカルブレイクアウトがあるロケーション

すべてのポートとプロトコルのトラフィックの転送

Microsoft 365は、多くの企業にとってローカルインターネットブレイクアウトを用いる主な要因となっています。お客様は、ゼットスケーラーのクラウドセキュリティプラットフォームを使用して、すべてのSaaSアプリケーションとインターネット接続先を対象にして、支社や地域のロケーションでインターネットへのダイレクトアクセスを活用できます。

Skype for BusinessやMicrosoft Teamsなどのアプリケーションでユーザエクスペリエンスと通話のクオリティを高めるためには、すべてのオーディオ / メディアトラフィック（UDP）を各ロケーションからローカルインターネット Egress（出口）を介して送信することが重要です。

推奨事項：ゼットスケーラーでは、Cloud Firewall機能を利用してすべてのインターネット宛てトラフィックを送信することで、すべてのWeb/非 Webアプリケーショントラフィックを保護することを推奨しています。

ゼットスケーラーを使用した付加価値サービス

テナント制約の制御

Microsoftのテナント制約によって、企業はユーザがアクセスできるテナントのリストを指定できます。Azure ADでは、これらの許可されたテナントへのアクセス権のみを付与します。

ZIA Public Service Edgeによって、以下のドメインが受信する各要求について2つのHTTPヘッダー Restrict-Access-To-TenantsとRestrict-Access-Contextが挿入されます。

- login.microsoftonline.com
- login.microsoft.com
- login.windows.net

上記の3つのドメイン以外のドメインについては、ゼットスケーラーによって制約ヘッダーが挿入されることはありません。

管理ポータルでテナント制約を有効にするには、以下のステップを実行します。

1. 管理ポータルの[Administration（管理）]->[Tenant Profiles（テナントプロファイル）]で、テナントプロファイルを作成します。

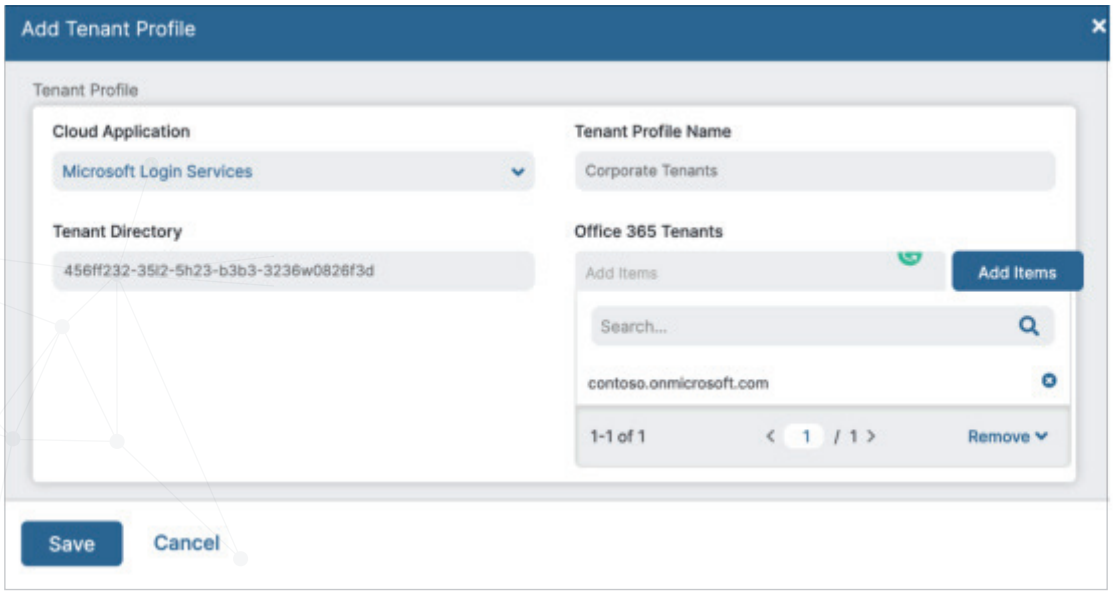
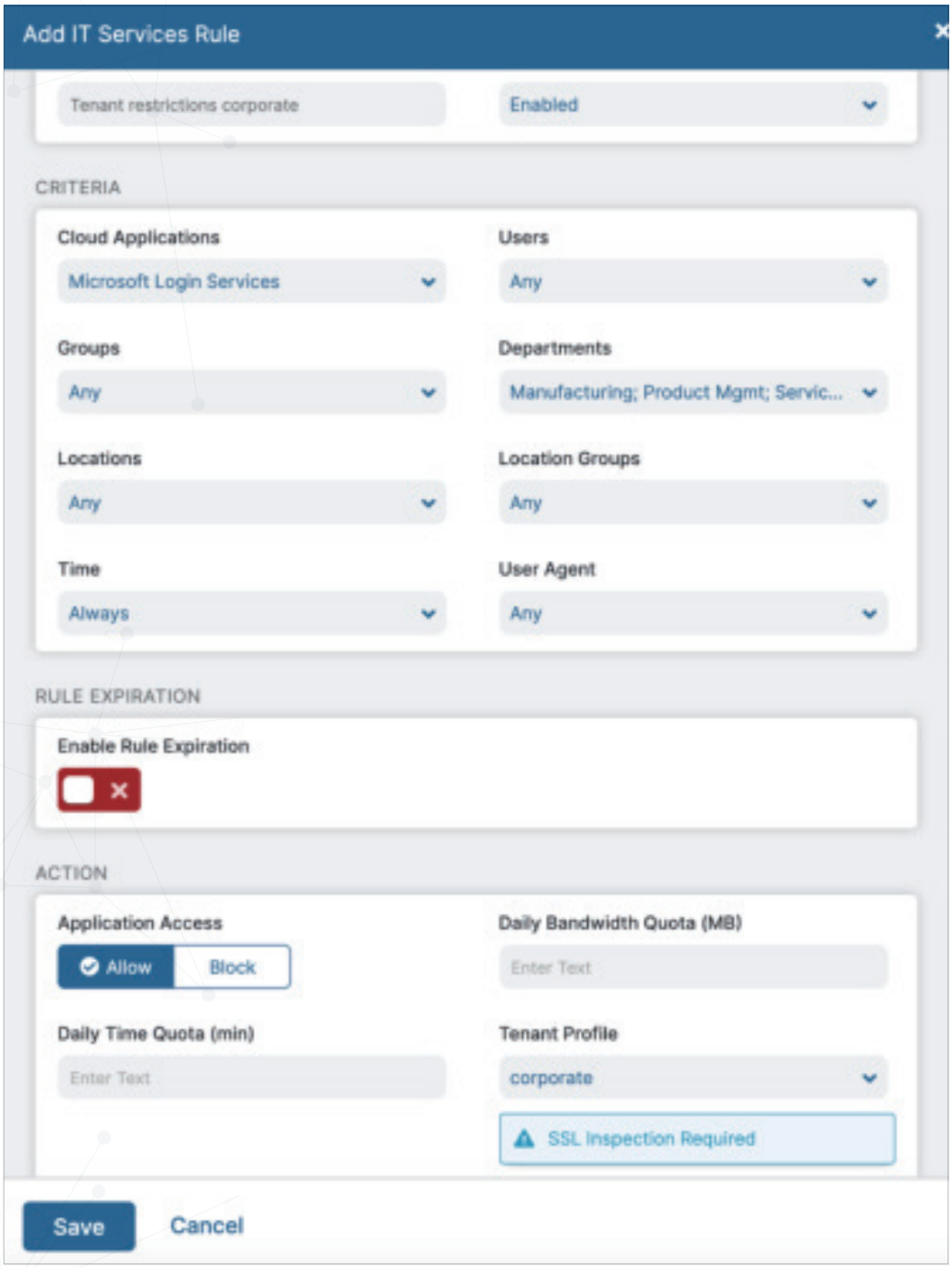


図13–テナント制約の制御

2. [Policy（ポリシー）]->[URL and Cloud App policy（URLとクラウドアプリケーションのポリシー）]->[IT services (category)（ITサービス（カテゴリ））]->[Microsoft Login Services（Microsoftログインサービス）]にアクセスして、クラウドアプリケーションポリシー内でテナント制約を有効にします。



個人用テナントのブロック

ゼットスケーラーで提供されているテナント制約制御機能を使用して、個人使用のOutlookアカウントやOneDriveアカウントを定義して、データ漏洩や高度な脅威から企業を保護できます。ゼットスケーラーは、個人使用のためのOutlookトラフィックやOneDriveトラフィックにインスペクションを実施して、フィッシング攻撃を防止できます。

ゼットスケーラーの管理 UIで、次のように構成してください。

[Policy（ポリシー）]->[URL and Cloud app policy（URLとクラウドアプリケーションのポリシー）]->[cloud app policy（クラウドアプリケーションポリシー）]->[File hosting（ファイルのホスティング）]（OneDrive）

[Policy（ポリシー）]->[URL and Cloud app policy（URLとクラウドアプリケーションのポリシー）]->[cloud app policy（クラウドアプリケーションポリシー）]->[Webmail（Webメール）]（Outlook）

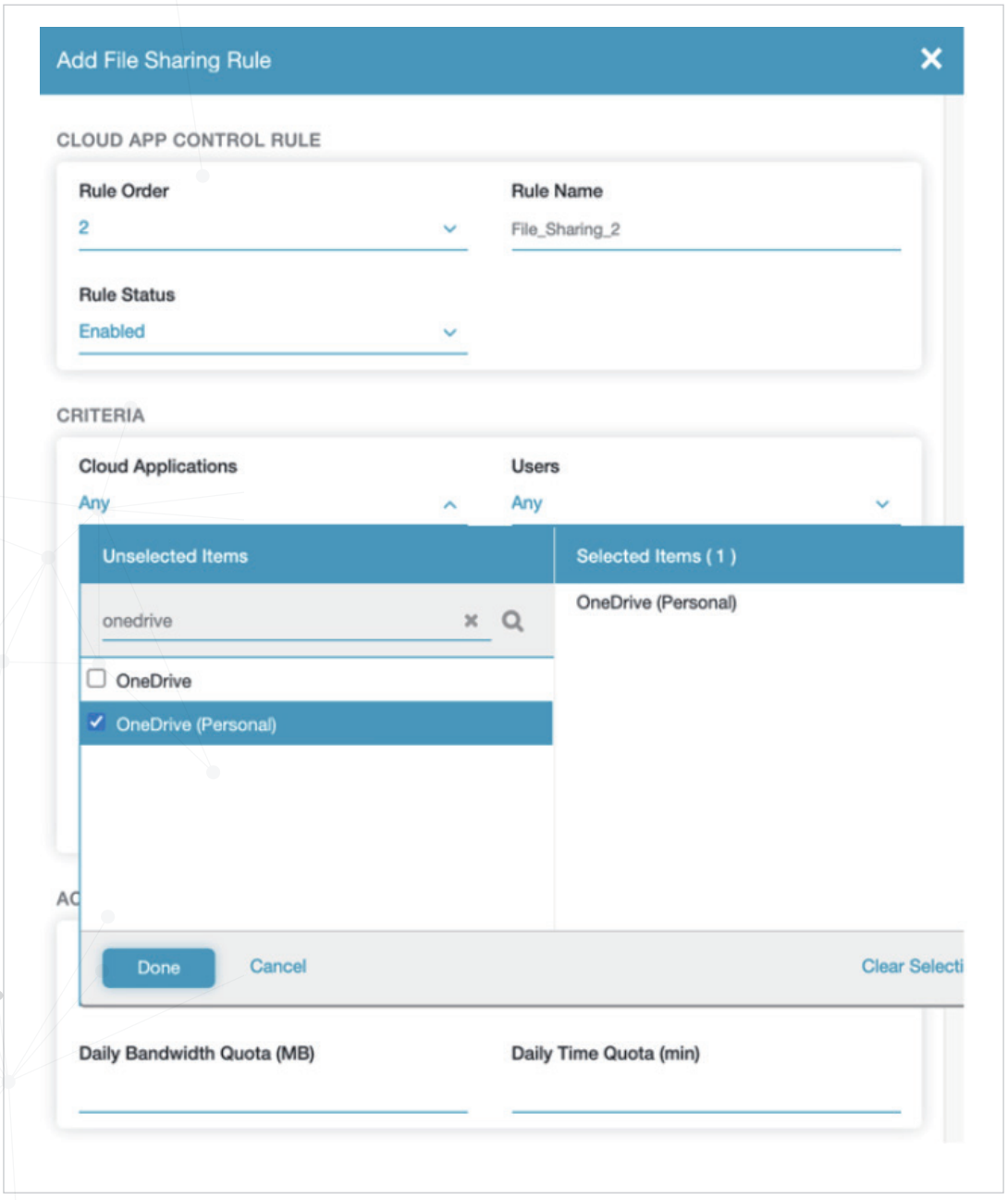


図14–個人用テナントのブロック

ゼットスケーラーを使用した条件付きアクセス

Zscaler Cloudを介してMicrosoft 365のトラフィックが転送されるため、Microsoftのネットワークでは、これらのすべてのトラフィックはゼットスケーラーのパブリック IPアドレスから送信されるトラフィックとみなされます。これらのIPアドレスは他のゼットスケーラーユーザも使用できるため、Microsoft 365 アプリケーションにアクセスする特定の制御機能をユーザのロケーションに基づいて適用することはできません。

Microsoftの条件付きアクセスでは、次の特定ホスト名を使用してセキュリティ制御が実施されます。

- login.microsoftonline.com
- login.windows.net

Microsoft 365に届くIPアドレスが企業のパブリック IPアドレスである場合は、シームレスな認証を適用できます。そうでない場合は、多要素認証が適用されます。

トラフィックのほとんどを占めるペイロードトラフィックは、ゼットスケーラーを介して転送され、前述のように最適化されます。

次の図は概略的な仕組みを示したものです。

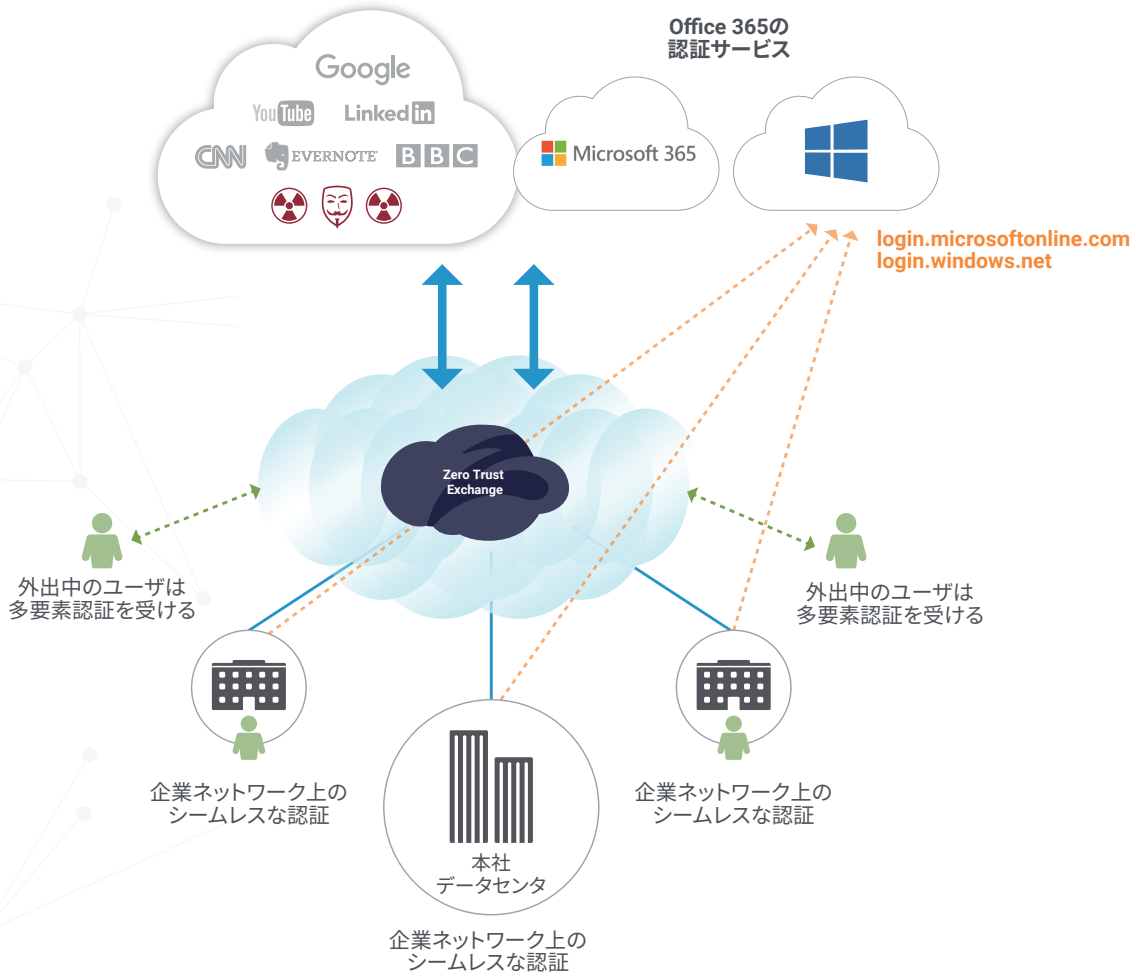


図15–ゼットスケーラーと条件付きアクセスの統合

ゼットスケーラーのIPアドレスを信頼できるIPアドレスとして追加

すべてのトラフィックにはゼットスケーラーのIPアドレスが割り当てられているため、それらのIPアドレスを信頼できるネットワークのリストとして追加できます。アドレスの詳細については、https://config.zscaler.comを参照してください。

これにより、アクセスが簡素化されて、ローミングユーザも多要素認証を用いることがなくなる一方で、ユーザが企業ネットワーク上にいるのかリモート / モバイル環境にいるのかが認識されなくなります。

PACファイルの使用

Zscaler Client Connectorは、転送プロファイルとアプリケーションプロファイルにPACファイルを使用して、ゼットスケーラーに転送されるトラフィックと、バイパスされるトラフィックを決定します。PACファイルを使用すると、Zscaler Client Connectorを使用して特定の宛先を簡単にバイパスできます。トラフィックをダイレクト送信して多要素認証の発生を判断するには、次のステートメントをPACファイルに追加する必要があります。

```
if (dnsDomainIs(host, “login.microsoftonline.com”)||

dnsDomainIs(host, “login.microsoft.com”)||

dnsDomainIs(host, “login.windows.net”))

{return “DIRECT”;}
```

これらのホスト名によって、クライアントのパブリック IPアドレスの条件付きアクセスが判定されます。

帯域幅コントロール

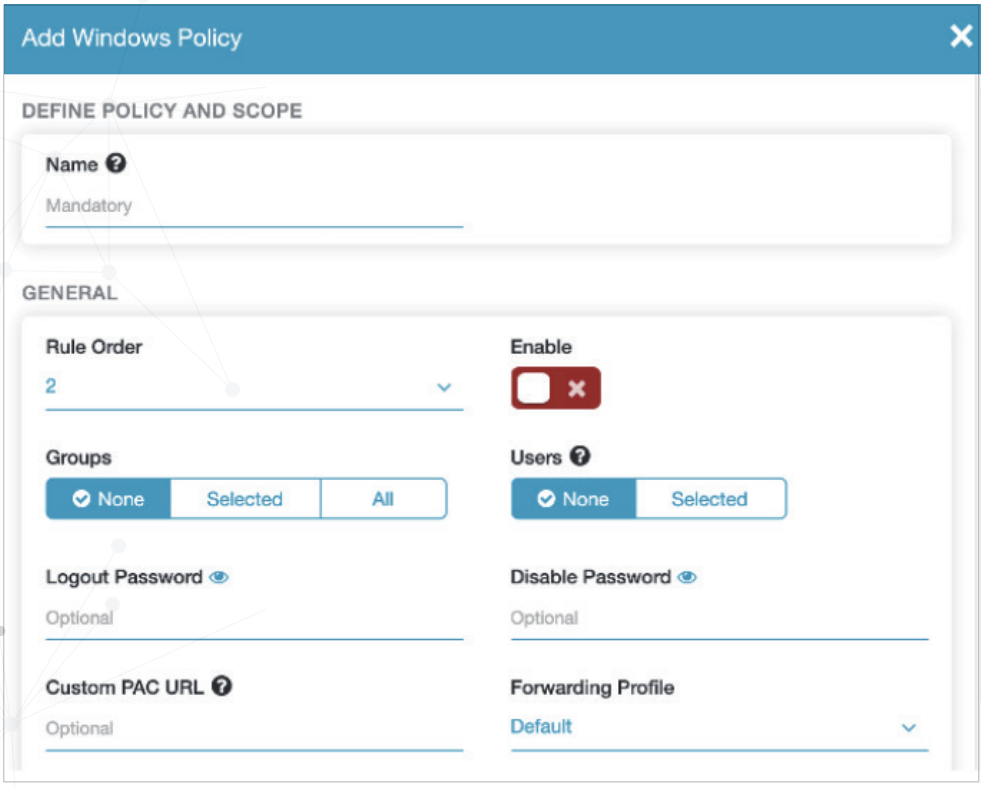


図16–アクセスポリシーの設定

Zscaler Bandwidth Controlを使用すると、インターネットの使用量にかかわらず、ビジネスに必須なMicrosoft 365アプリケーションへのアクセスを保持でき、ソーシャルメディアやストリーミングに関して通常より厳格なルールを追加で適用するなど、すべてのトラフィックフローをより細かく制御できます。例えば、帯域幅の最大10%をストリーミングとソーシャルメディアに割り当てることができます。帯域幅が制約されている場合は、ビジネスに必須のトラフィックとの競合時に、このトラフィックに帯域幅を割り当てられないようにできます。このようにして、Microsoft 365 Teams、SharePoint、OneDriveなどのビジネスに必須のアプリケーションに対して、最大限のパフォーマンスを維持するために十分な帯域幅を常に確保できます。

まとめ

ゼットスケーラーを使用すると、Microsoft 365のようなインターネットベースのアプリケーションのために、クラウドへのダイレクトアクセスが可能になります。企業は、コストのかかるMPLS回線を介してトラフィックをバックホールする代わりに、インターネットを介してアプリケーションサーバーにトラフィックをダイレクトに送信できます。ゼットスケーラーは、グローバルなクラウドに直結したネットワークを活用してMicrosoft 365の導入を簡素化し、ユーザエクスペリエンスとアプリケーションパフォーマンスを向上させることができます。

ゼットスケーラー株式会社
〒100-0004
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