

# ゼットスケラーとSD-WANによるソリューション

インターネットのみのブランチの保護

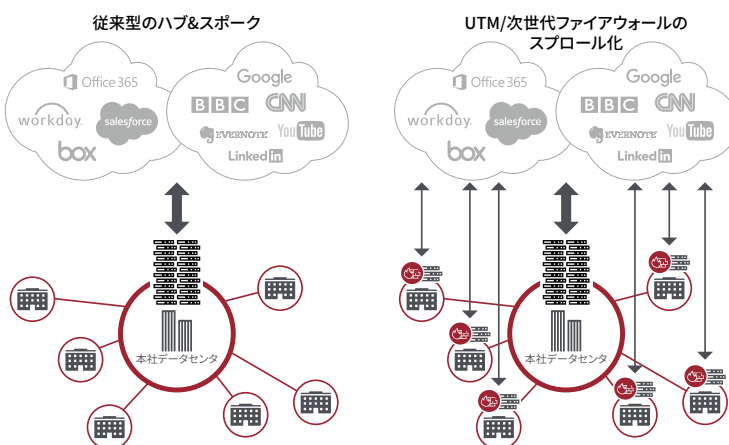


ゼットスケラーとSD-WANを活用してセキュアローカルインターネットブレイクアウトを有効にすることで、ハブ&スポークネットワークからインターネットのみのブランチアーキテクチャへの移行が容易になります。

## クラウドアプリで明らかになった従来型アーキテクチャの問題点

Office 365などのクラウドアプリケーションを導入する組織にとって、古いアプローチによるトラフィックのルーティング、すなわち、ハブ&スポークアーキテクチャを採用し、MPLS経由でトラフィックを中央のインターネットゲートウェイにバックホールする方法は、あまりに非効率的です。高速のユーザエクスペリエンスを提供し、クラウドのアプリケーションやサービスをサポートするには、インターネットトラフィックをローカルでルーティングする必要があります。

しかし、一元化されたインターネットゲートウェイと同レベルのセキュリティを実現するには、同じセキュリティアプライアンスのスタックをブランチごとに置く必要があります。その購入、導入、管理には多大なコストを要します。従来型のファイアウォールやUTMでは、SSLで暗号化されたトラフィックや非標準のポートやプロトコルを処理できないため、代替手段とし十分ではありません。これらの課題に直面した多くの組織が、ローカルインターネットのブレイクアウトを確立し、高速のユーザエクスペリエンスを提供する手段として、SD-WANに注目するようになりました。



- MPLS経由のバックホールはコストが高い
- 不要なレイテンシが発生する
- ユーザエクスペリエンスが低下する
- 導入にあたって多くのコストが発生する
- アプライアンスのスプロール化を招く
- 管理が複雑になる
- 支社のセキュリティが脅かされる
- SSLインスペクションと追加のセキュリティサービスによってパフォーマンスが低下する

## SD-WANとローカルインターネットブレイクアウト

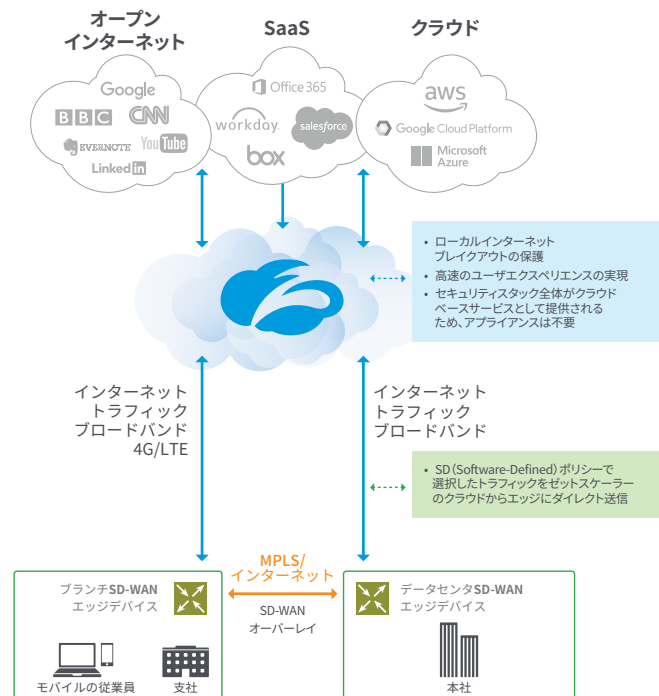
SD-WAN (Software-Defined Wide Area Networking) は、ブランチにおけるトラフィックのルーティングを簡素化し、ローカルインターネットブレイクアウトの確立を容易にします。SD (Software-Defined) ポリシーは、ブランチをインターネット、クラウドアプリケーション、データセンタに接続するトラフィックをルーティングする最適パスの選択に使用されます。すべてのブランチのポリシーを単一のインタフェースを利用してクラウドに定義することで、新しいアプリケーションやサービスの展開はもちろん、多くの場所のポリシーの管理も容易になります。忘れてはいけないのは、これらのローカルブレイクアウトを保護する必要性です。

## ゼットスケラー：クラウドを利用してSD-WANを保護

ゼットスケラーは、アウトバウンドインターネットトラフィックを保護し、高速のユーザエクスペリエンスを実現します。バックホールは不要です。拠点ごとに同じセキュリティアプライアンスのスタックを置く必要もありません。

ゼットスケラーのクラウドセキュリティプラットフォームはセキュリティスタック全体をクラウドサービスとして提供するため、セキュリティに関して妥協を迫られることはありません。また、ポリシーが物理的な特定の場所に関連付けられることはなく、あらゆる場所から接続するユーザを追いかけ、同一の保護を提供します。

インターネット経由のトラフィックをゼットスケラーにルーティングするだけで、すべてのトラフィック (SSLを含むすべてのポートとプロトコル) のインスペクションが直ちに開始されます。単一コンソールから、アクセスポリシーとセキュリティポリシーを定義し、すべての場所に瞬時に適用できます。さらには、クラウドサービスの柔軟なスケラビリティにより、帯域幅コントロールなどの新しいサービスを数回のクリックで導入でき、パフォーマンスに影響を与えることも、高価なアプライアンスのアップグレードが必要になることもありません。



## SSLインスペクションをSLA保証のパフォーマンスで実現

SSLがデフォルトの通信プロトコルとして利用されるようになり、ランサムウェアなどの多くの脅威が、SSLや時には他のポートさえ使用するようになった今、すべてのトラフィックのインスペクションが不可欠となりました。しかし、SSLインスペクションは今なおセキュリティアプライアンスにとって大きな課題であり、トラフィックの復号化とインスペクションを行い、再び暗号化するという作業によって、ファイアウォールのパフォーマンスが低下することは周知の事実です<sup>2</sup>。ゼットスケラーのサービスプラットフォームの一部であるクラウドファイアウォールは、SSLを含むすべてのポートとプロトコルのトラフィックをほとんどゼロのレイテンシでインスペクションします。



<sup>1</sup> 透明性レポート - Google, <https://www.google.com/transparencyreport/https/?hl=en>

<sup>2</sup> Pirc, John W. 著、「SSL Performance Problems: Significant SSL Performance Loss Leaves Much Room for Improvement」、NSS Labs (<https://www.nsslabs.com/linkserverid/13C7BD87-5056-9046-93FB736663C0B07A/>)

## ZscalerとSD-WAN

### コストと複雑さの軽減

ゼットスケラーとSD-WANによって、従来型のネットワークやセキュリティのアプライアンスのコストや複雑さから解放され、インターネットのみのブランチが実現

#### SD-WAN

- SD (Software-Defined) ポリシーを使用することで、ブランチのインターネット接続を簡素化し、従来型アプライアンスに関連する複雑なアクセスコントロールリストを排除
- 複数のブランチ接続タイプ（ブロードバンド、ブロードバンドVPN、LTE、MPLS）を活用することで、ハブ & スポークアーキテクチャからのシームレスな移行を実現

#### ZSCALER

- セキュリティスタック全体がクラウドサービスとして提供されることでローカルインターネットブレイクアウトの保護が可能になり、ブランチのファイアウォールやUTMも不要に
- アプライアンスの導入や管理の手間を省き、セキュアローカルインターネットブレイクアウトを実現
- MPLSバックホールのコストを削減

### 運用を簡素化

ゼットスケラーとSD-WANは、セキュリティをクラウドサービスとして提供し、トラフィックをルーティングするSD (Software-Defined) ポリシーを使用することで、ブランチの運用を簡素化

#### SD-WAN

- 単一のクラウド管理コンソールで定義されたソフトウェアポリシーを使用して、トラフィックのルーティング方法を判断

#### ZSCALER

- すべてのブランチへのセキュリティアプライアンスのスタックの購入、導入、管理は不要に
- 単一のコンソールによるセキュリティポリシーとアクセスポリシーの一元的な定義が可能
- ポリシーの変更をすべてのロケーションに直ちに適用
- 数分の作業で、数回のクリックで、すべての場所への新しいセキュリティサービスの導入が可能
- インターネットトラフィックをローカルにルーティングすることで、高速のユーザエクスペリエンスを実現
- 80と443だけでなく、すべてのポートでアウトバウンドインターネットトラフィックにセキュリティとアクセスコントロールを提供することで、高度な脅威から保護

### セキュリティとスケーラビリティ

ゼットスケラーは、セキュリティスタック全体をクラウドサービスとして提供し、コーヒーショップ、本社、ブランチなどのあらゆる場所から接続するユーザに同一の保護を提供

#### ZSCALER

- セキュリティとアクセスコントロールの完全セットを、セキュリティを低下させることなく、専用のクラウドベースのサービスとして提供
- 完全インラインコンテンツインスペクションとすべてのポートとプロトコルのアクセスコントロールを実行し、完全ログ機能にも対応
- SSLトラフィックをネイティブにインスペクション
- 高い柔軟性とスケーラビリティにより、パフォーマンスへの影響や、アプライアンスの入れ替えを要することなく、新しい機能（帯域幅コントロールやデータ損失防止など）の迅速な導入が可能
- セキュリティスタック全体をユーザに近づけることで、あらゆる場所から接続するユーザに同一の保護を提供

