ゼットスケーラーの クラウドファイアウォール

セキュアなクラウドへ移行するためのガイド

zscaler™

ゼットスケーラーのクラウドファイアウォールを活用してクラウドへの移行を加速する

アプリケーションのクラウドへの移行、そしてWebプロトコルの利用が拡大したのは今に始まったことではありません。ゼットスケーラーは2008年に、この変化を予想し、セキュリティクラウドの構築を開始しました。そして今、ゼットスケーラーのクラウドはより大規模かつスケーラブルになり、HTTPとHTTPSのセッションのトラフィックがインスペクションされ、データの動きを確認できるようになりました。

中央のデータセンタからのアプリケーションの移行によって、コストが高くなるだけでなく、ユーザエクスペリエンスのレイテンシが増えてしまうといった、集中型のバックホールモデルによる問題が発生しています。中央のサイトに置かれた従来型のファイアウォール経由でDNSをルーティングする場合、そのレスポンスはユーザではなくファイアウォールに対してローカルであるため、リアルタイムのアプリケーションパフォーマンスに影響することになります。

クラウドアプリケーションは強力なビジネスイネーブラですが、固有の課題も存在します。たとえば、Office 365によって、ユーザごとに複数の接続が開き、帯域幅が増え、従来型のファイアウォールのポートやスループットの容量を使い果たしてしまうという問題があります。ゼットスケーラーの依頼によって実施されたOffice 365の導入に関する最近の調査では、多くの組織が、ネットワークやレイテンシの問題に直面していることがわかりました。導入前にファイアウォールをアップグレードしたにもかかわらず、69%の組織が導入後にレイテンシ発生していると回答しています。また、バックホールされるトラフィックの帯域幅を増やす方法でも問題は解決されず、69%が毎週問題が発生していると回答し、30%がパフォーマンスの問題が毎日発生していると回答しています。

ゼットスケーラーのクラウドファイアウォールによるメリット

ゼットスケーラーのクラウドファイアウォールは、クラウドプロキシによるWebベースのトラフィックの問題の解決と同じ方法で、これらの問題を解決します。一元管理によって、すべてのポートとプロトコルの高速かつ安全なローカルインターネットブレークアウトが可能になり、アプライアンスをアップグレードしたり導入する必要はありません。ゼットスケーラーのクラウドファイアウォールは、ゼットスケーラーのプラットフォームの他の部分と同様に拡張が可能であり、ユーザ数に基づく従量制で利用できます。

ゼットスケーラーの場合、ポリシーが物理的な場所に関連付けられないため、ポリシーがユーザを追従し、使用するデバイスや接続先に関係なく、同一の保護が提供されます。本社、ブランチオフィス、あるいは世界中のさまざまな出張先のいずれで働く場合も、同一のアクセスと保護が提供されます。

ゼットスケーラーは、「Standard（標準）」と「Advanced（高度）」の2種類のクラウドファイアウォールを提供しています。前者は、すべてのZscaler Internet Access（ZIA）サブスクリプションに含まれおり、後者は、トランスフォーメーションバンドルに含まれていますが、個別のアップグレードとして購入することもできます。

「Standard（標準）」と「Advanced（高度）」の相違点

「Standard（標準）」のクラウドファイアウォールは、ZIAサービスのサブスクリプションに含まれており、以下に説明するポリシー機能の一部をすぐにご利用いただけます。「Advanced（高度）」のクラウドファイアウォールは、トランスフォーメーションバンドルの一部として利用できるサービスで、個別のアップグレードとして購入することもできます。

2種類のクラウドファイアウォールで提供されるポリシー

Standard（標準）	Advanced（高度）
送信元と送信先のIPアドレス、ポート、プロトコルに基づき、許可 /ブロックのセキュリティポリシーを適用。すべてのアウトバウンドトラフィックで以下の機能の利用が可能。 • 統一ポリシー（場所ごとに5組） • 単一の管理コンソール • すべてのサイトとユーザに1 セットのログ	ディープパケットインスペクション（DPI）エンジンを使用し、アプリケーションに基づくきめ細かい許可 /ブロックセキュリティポリシーを適用 • 標準的なゼットスケーラークラウドファイアウォールのすべての機能 • 次世代ファイアウォール（NGFW）のすべての機能とゼットスケーラーのクラウドインテリジェンスと管理が提供され、高価なアプライアンスの購入やメンテナンスは不要 • DNSのセキュリティとコントロール：DNS解決を最適化し、きめ細かいコントロールによってDNSトンネリングの検知と防止が可能 • NGFWとコンテキスト対応のポリシー：アクセスのきめ細かい許可 /ブロックとアプリケーション、ユーザアイデンティティ、グループ、場所に基づくセキュリティポリシー • 完全修飾ドメイン名ポリシー：複数のIPでホスティングされるアプリケーションに対するアクセスポリシー • 包括的ダッシュボード：ユーザ、グループ、場所ごとのトラフィックの使用状況、脅威、アプリケーションをリアルタイムで可視化 • セッションごとの完全ログとレポート • クラウド IPS：接続のタイプや場所に関係なく、常時オンのIPS脅威保護と完全な可視性を提供し、すべてのユーザのインターネットトラフィック（SSLも含む）をインスペクション • 非標準ポートの自動プロキシ転送：非標準のポートとプロトコルを使用するアプリケーションを自動的に特定して保護

既知のプロトコル番号を使用するプロトコルベースの攻撃をブロックしたい場合は、「Standard」のゼットスケーラーファイアウォールで対応できます。たとえば、ポート 53をブロックすることで、代替 DNSサーバの使用を防止することが可能です。

しかし、アプリケーションがポート番号とは一致するものの、想定したアプリケーションではない場合はどうでしょうか。HTTPとHTTPSで動作するアプリケーションでプロキシが重要になったのと同様、より詳細な情報が必要となる場合、また、オープンしたポートで何が動作し、どのユーザが何をしようとしているのかを知る必要がある場合は、高度なゼットスケーラークラウドファイアウォールが必要になります。

ポリシーの再考

これまでは、業界がアクセスコントロールリスト（ACL）からステートフルファイアウォール、NGFWへと移行した場合でも、運用は基本的に同じでした。ファイアウォールに「穴を開ける」ことで許容できるトラフィックを許可し、それ以外をすべてをブロックするという考え方です。デフォルトの「すべて拒否」するルールは、これまでほとんどのファイアウォールルールにおいて、最後に位置付けられていました。

有効な設計パターンではありますが、到着するトラフィックではなく、組織から外部へのトラフィックを考慮する場合、パターンを再考する必要があるでしょう。最後のルールを変更し、「すべて許可」するルールへ切り替えた方が、望ましくないものをブロックし、それ以外の許可されたトラフィックを通常どおりに流すことができます。

セキュリティエキスパートが数十年にわたって推奨してきた機能を変更するのは、この20年間で我々の仕事の進め方が大きく変化し、インターネットとのやりとりの方法が根本的に変わったためです。

組織の要件はポリシーあるいは法規制によって異なります。それらの要件によって、すべてのトラフィックをブロックするのか、あるいは許可するのか、判断をすることになります。判断の基準となるのは、どのようにサービスを運用し、どのようなサービスを提供しているかという点です。

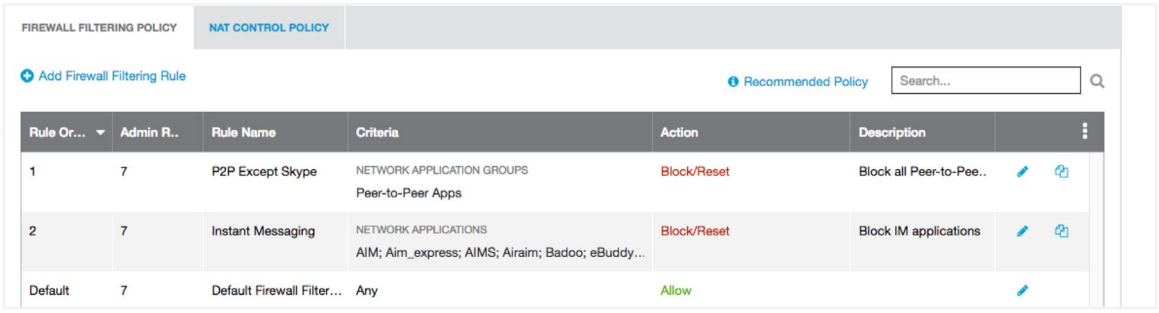
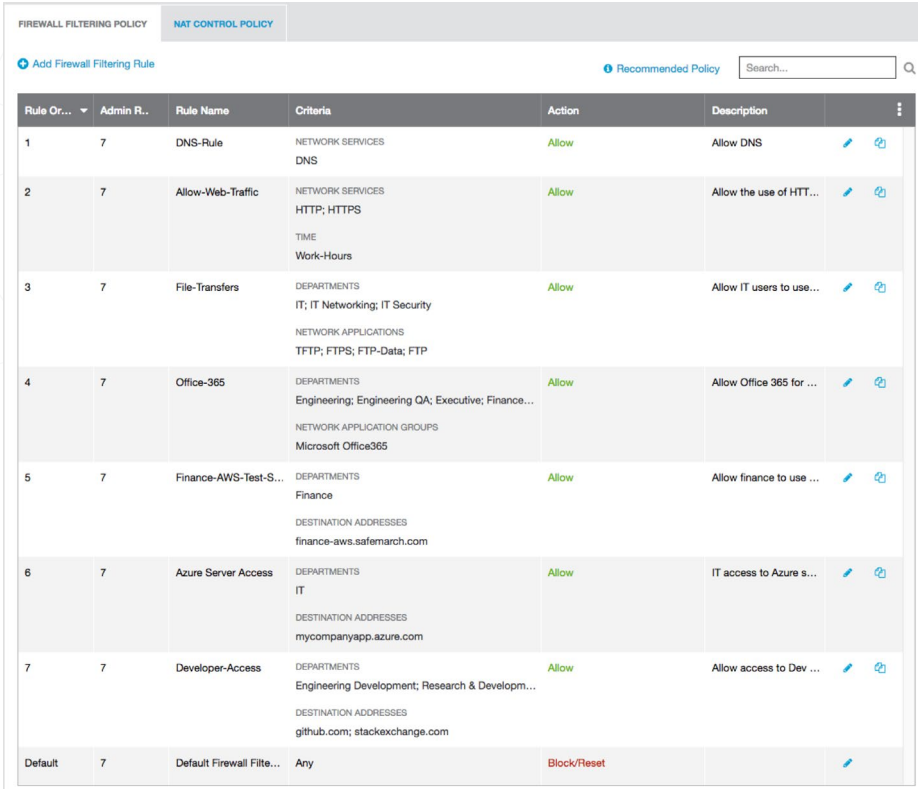


図1.「すべて許可」のデフォルトルールの例

ゲストネットワークを公共スペースに提供する場合、不適切なコンテンツをブロックし、P2Pなどのプロトコルをブロックすることで、不正あるいは違法である可能性がある活動を防止し、その後で「すべて許可」するルールを選択することになるでしょう。ゲストネットワークのユーザは、データセンタではなくインターネットにアクセスするため、それ以外のトラフィックは組織にとって許容されるものと考えられます。



Rule Or...	Admin R..	Rule Name	Criteria	Action	Description
1	7	DNS-Rule	NETWORK SERVICES DNS	Allow	Allow DNS
2	7	Allow-Web-Traffic	NETWORK SERVICES HTTP; HTTPS TIME Work-Hours	Allow	Allow the use of HTT...
3	7	File-Transfers	DEPARTMENTS IT; IT Networking; IT Security NETWORK APPLICATIONS TFTP; FTPS; FTP-Data; FTP	Allow	Allow IT users to use...
4	7	Office-365	DEPARTMENTS Engineering; Engineering QA; Executive; Finance... NETWORK APPLICATION GROUPS Microsoft Office365	Allow	Allow Office 365 for ...
5	7	Finance-AWS-Test-S...	DEPARTMENTS Finance DESTINATION ADDRESSES finance-aws.safemarch.com	Allow	Allow finance to use ...
6	7	Azure Server Access	DEPARTMENTS IT DESTINATION ADDRESSES mycompanyapp.azure.com	Allow	IT access to Azure s...
7	7	Developer-Access	DEPARTMENTS Engineering Development; Research & Developm... DESTINATION ADDRESSES github.com; stackexchange.com	Allow	Allow access to Dev ...
Default	7	Default Firewall Filte...	Any	Block/Reset	

図2.「すべて拒否」のデフォルトルールの例

ただし、医療や金融などの厳しい法規制の遵守が求められる業界の組織の場合、承認されたアプリケーションだけを許可するというのがおそらく妥当な方法です。この場合、正しいものだけの持ち出しを許可し、それ以外のすべてをローカルに置いて外部に持ち出されないようにするのが、最も適切なアプローチです。インターネットアクセスを必要とするアプリケーションのみに操作を許可し、「すべて拒否」するルールを適用させるのが最善の方法です。

クラウドファイアウォールの詳細と構成方法
https://help.zscaler.com/zia/about-firewall-control

まとめ

私たちが働く場所は急速に変化しています。将来的には、データセンタがクラウドに置かれたインフラストラクチャとサービスに置き換えられ、高価なバックホールがローカルブレイクアウトに置き換えられるようになるでしょう。オフネットワークのユーザがさらに増加し、オフィス以外の場所で働くようになるでしょう。このような未来の働く環境を保護するには、あらゆる場所でさまざまな方法で働くユーザを追従できる、サービスとポリシーが統合されたセキュリティプラットフォームが必要です。ゼットスケーラーのクラウドファイアウォールは、アプライアンスを使用することなく、すべてのポート、プロトコルの高速かつ安全なローカルインターネットブレイクアウトを可能にします。標準のクラウドファイアウォールと高度なクラウドファイアウォールを提供する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は、セキュリティスタック全体をユーザに近づけることで、あらゆる場所で働くユーザにど同一の保護を提供し、柔軟なスケーラビリティによって、すべてのクラウドアプリケーショントラフィックの処理を可能にします。

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