Zscaler Zero Trust Firewall

Web トラフィックと非 Web トラフィックに対する安全な適応型ゼロトラスト保護を 100% クラウドネイティブで実現

データシート

Zscaler Zero Trust Firewall は、業界で最も包括的なクラウドネイティブ セキュリティ サービス エッジ (SSE) プラットフォームですべてのユーザー、アプリケーション、場所の Web トラフィックと非 Web トラフィックを保護します。

現在、組織の業務環境では、分散化やモバイル化が進んでいます。アプリケーションはデータ センターからクラウドに移行し、新しいデジタル ワークロードはクラウド上にネイティブな形で展開されるようになってきています。さらに、ユーザーはホーム オフィス、共有ワークスペース、支店オフィス、外出先などさまざまな場所で業務を行い、インターネットから直接ビジネス アプリケーションにアクセスしています。

その結果、ユーザーやクラウド アプリケーションから大量のトラフィックが発生し、ネットワーク中心の従来のセキュリティ アプライアンスにバックホールされています。これによって、生産性への悪影響や接続のボトルネックが発生し、ビジネス リスクが高まっています。しかし、SSL で暗号化されたトラフィックを完全に検査しなければ、暗号化と非標準ポートで検出を回避するステルス攻撃に対処することはできません。このような問題を解決するために、仮想化ファイアウォールが使用される場合もありますが、この方法ではネットワークがクラウド リソースに拡張されるうえ、従来のセキュリティ アプライアンスと同様のキャパシティーの限界が生じます。

相互接続が可能な環境を確保しながらワークロードを保護するには、やはり適切な管理を行うための専用のリソースが必要であり、そのリソースを確保できなければ設定ミスのリスクにつながります。

Zscaler Zero Trust Firewall

Zscaler Zero Trust Firewall は、ユーザーやデバイスがどこから接続していても、Web トラフィック (HTTP/HTTPS) と非 Web トラフィック (FTP、DNS、RDP、Telnet など) に対してクラウドベースの保護を提供します。ローカル インターネット ブレイクアウトを活用してトラフィックを安全に転送することで、接続性と可用性を向上させます。VPN を通じたバックホールや拠点毎のセキュリティ アプライアンス スタックの複製は必要ありません。インターネットと SaaS への接続を Zscaler にルーティングすることで、SSL で暗号化されたトラフィックを含むすべてのユーザー トラフィックを検査し、弾力的な拡張によって大量かつ長時間にわたる接続を処理します。

Zero Trust Firewall は、規制上の基準に簡単に準拠できるよう組織を支援するとともに、一元的なポリシー管理コンソールを通じて、ユーザー / アプリケーション認識型の脅威対策およびリスクベースのポリシーを組織全体で構成、管理、施行し、ネットワークとアプリケーションの可視性を確保します。Firewall as a Service (FWaaS) ソリューションであるため、アップデート、アップグレード、パッチに関する責任は、拡張性の要件も含めてすべて Zscaler が負います。アプライアンスを廃止することでコストを大幅に削減し、物理的な場所に紐付く複雑なポリシーやネットワーク構成を排除できます。

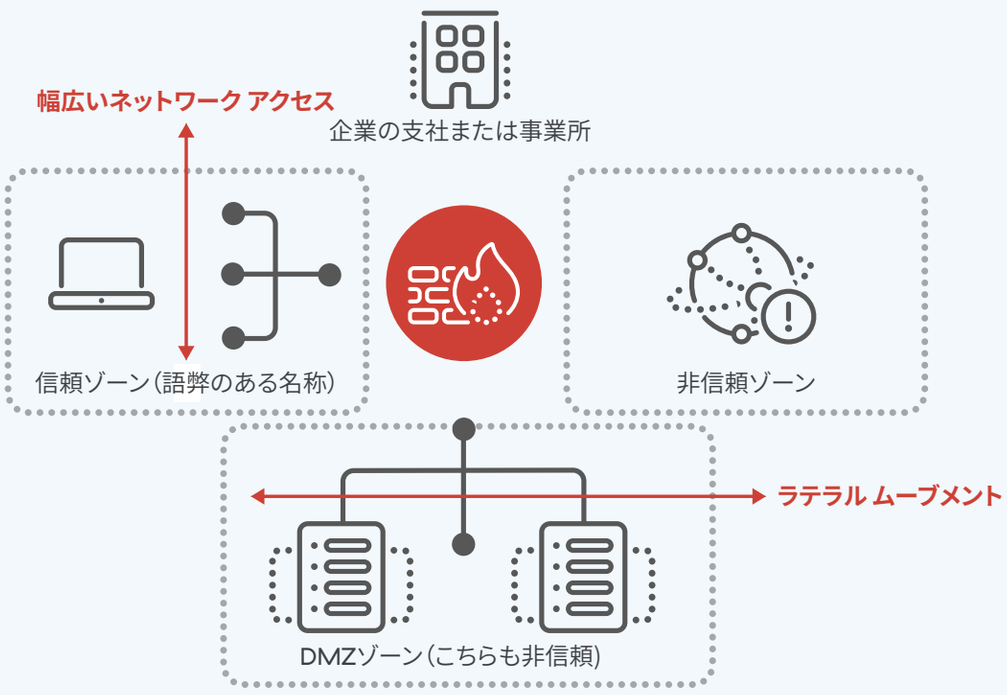
Zscaler Zero Trust Firewall によって、すべてのセッションがログに記録され、すべてのユーザーと場所が可視化されるため、必要な情報にいつでもアクセスできます。ハイブリッド環境や拠点の接続を刷新し、現代のパフォーマンスやセキュリティ上のニーズに対処することで、Zscaler は組織のクラウド トランスフォーメーションのニーズに沿った支援と拡張性を提供し、Microsoft 365 などのクラウドネイティブ アプリケーションへの移行などをサポートします。

ZSCALER ZERO TRUST FIREWALL のメリット

- **あらゆる場所で働くユーザーの完全な保護。**リスクベースの動的なセキュリティ ポリシーをあらゆる場所のユーザーに適用します。複雑なポリシーやネットワーク構成は必要ありません。
- **隠れた攻撃を検出する完全な検査。**無制限のインライン トラフィック検査とネイティブな SSL 復号により、ステルス性の高い脅威を防ぎ、悪意のある接続を終了させます。
- **非標準ポートの回避型 Web トラフィックの検出。**非標準ポートを使用する回避型のサイバー脅威や暗号化されたサイバー脅威をすばやく特定、阻止します。
- **クラウド型ローカル インターネット ブレイクアウト。**インターネットへの高速かつ安全な直接接続を、ハイブリッド環境や拠点のすべてのトラフィックに適用し、弾力的な拡張とユーザー エクスペリエンスの改善を実現します。
- **常時オンのクラウド侵入防止システム (IPS)。**Zscaler ThreatLabz によって管理される振る舞いベースの適応型 IPS シグネチャーがリアルタイムで機能し、SecOps ワークフローを強化します。
- **パフォーマンスを損なわない DNS 保護。**地理的に近い場所での名前解決によって優れたパフォーマンスを維持しながら、悪意のあるサイトや DNS トンネリングからユーザーとエンドポイントを保護します。
- **グローバルに展開されたエッジを通じたクラウド型の保護。**Zscaler Zero Trust Firewall は、Zscaler Internet Access™ と完全統合され、Zscaler Zero Trust Exchange™ の一部として機能し、優れたセキュリティとユーザー エクスペリエンスを提供します。

従来のアーキテクチャーから Zscaler Zero Trust Firewall への移行

従来型ファイアウォールの ゾーンベースのアーキテクチャー



Zscalerのゼロトラスト プラットフォーム

従来のファイアウォールも次世代ファイアウォールも、NIST 800-207 に定められたゼロトラストの原則を満たすことができません。境界ベースのセキュリティ アーキテクチャーは、保護されていないネットワークやデバイス上で暗号化されたトラフィックを大規模に検査できるようには設計されていません。厳格なユーザー認証や段階ごとの継続的なポリシー チェックを行っていなければ、侵害されたサーバーやデバイスを通じて、攻撃者にネットワークへの広範なアクセスやラテラル ムーブメントを許してしまう可能性があります。さらに、従来のファイアウォールをゲートウェイとして仮想プライベート ネットワーク (VPN) を展開することで、組織のパブリック ネットワークとプライベート ネットワークが露出することになります。Zero Trust Firewall は、動的な最小特権アクセスを提供し、ネットワークとセキュリティのトランスフォーメーションを推進するための唯一のソリューションです。

クラウドネイティブな ファイアウォールのメリット

現代のデジタル環境向けに構築された Zscaler Zero Trust Firewall は、優れた弾力性を有したスケーラビリティーとパフォーマンスで、インターネットへのセキュアなアクセスを実現すると同時に、すべてのポートやプロトコルで Web および非 Web のトラフィックを処理できるようにします。自宅、本社や支店、外出先など、どのような場所でどのようなデバイスを使用しているユーザーに対しても一貫した保護を提供するとともに、従来のネットワーク セキュリティや次世代ファイアウォール アプライアンスに付きまとうコスト、複雑さ、パフォーマンスの制約を排除します。

適応型ゼロトラスト プラットフォームを活用

静的検査、パフォーマンス低下、物理的なファイアウォール アプライアンスの容量制限に妥協する必要がなくなります。完全統合型のクラウド ネイティブ プラットフォームを基盤とする Zscaler Zero Trust Firewall は、弾力的な拡張性を通じて、長期間の接続を必要とするクラウド アプリケーション トラフィックを処理すると同時に、SSL/TLS トラフィックをネイティブに傍受および検査し、暗号化されたトラフィックに潜むマルウェアを大規模に検出します。

革新的なハイブリッド接続と拠点接続

ネットワーク中心の高コストのインフラから、クラウド型の真のローカル インターネット ブレイクアウトに移行できます。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して、クラウドへの直接接続で常に高速な接続を実現しながら、すべてのポートとプロトコルにセキュリティとアクセス制御を提供します。アプライアンスの導入や管理が必要ないため、MPLS によるバックホールのコストを削減できるほか、高額で時間のかかるパッチ管理、サービス停止期間の調整、ポリシー管理が不要になります。

現代の働き方を支えるユビキタス セキュリティ

1 日あたり 300 兆のシグナルに基づいたリアルタイムのセキュリティ アップデートを活用し、毎日クラウド全体で共有することで、ユーザーの接続元の場所やデバイスを問わず同水準の保護を提供します。
セキュリティ スタック全体をユーザーの近くに配置し、組織のネットワーク内外でユーザーに動的なポリシーを適用することで、ユーザーやアプリを認識する優れた脅威対策を実現します。

既知の攻撃に対する常時オンの防御

従来のソリューションでは対応できなかった領域に、Zscaler ThreatLabz が管理しクラウドで提供されるコンテキスト認識型侵入防止システム (IPS) による脅威対策を適用できます。IoT/OT やネットワーク内外の暗号化されたトラフィックにも対応する無制限のインライン トラフィック検査により、接続の種類や場所を問わず、数千の Web アプリケーションおよび非 Web アプリケーションへのアクセスに際して、振る舞いベースの IPS シグネチャーがリアルタイムで適用されます。

DNS パフォーマンスの最適化とセキュリティ強化を両立

地理的に近いアプリを結び付けることで解決を迅速化し、ユーザー エクスペリエンスとクラウド アプリのパフォーマンスを向上させながら、ドメイン ネーム システム (DNS) セキュリティと制御ポリシーを実装します。大規模な SSL インスペクションによって可視性を取り戻し、攻撃者による DNS-over-HTTPS (DoH) の悪用を阻止することで、ユーザーと従業員が悪意のあるドメインにアクセスしたり、組織のポリシーを回避したりすることをより適切に防止します。Zscaler は DNS をサービスとして提供することで、レイテンシーを最小限に抑えるとともに、すべての DNS トラフィックに対してフル プロキシを使用してローカル インターネット ブレイクアウトを保護します。また、トンネルを通じたデータの持ち出しを、機械学習を活用して検出およびブロックします。

わかりやすいポリシー管理

単一のコンソールから、すべての場所のすべてのユーザーに対してポリシーを定義、展開し、すぐに施行できます。Zero Trust Firewall はユーザー、アプリケーション、場所、グループ、部門に基づくきめ細かいファイアウォール ルールを一元化することで、ポリシー管理を簡素化します。複雑なポリシーやネットワーク構成、ファイアウォールの設置場所単位でのポリシーの再作成は必要ありません。さらに、管理者はユーザーの詳細、要求、応答、使用サービスなどを網羅したフォレンジック的に完全なログを SIEM と XDR のツールに送信し、セキュリティ調査とインシデント対応を強化できます。

Gartner

Zscaler は、Gartner® セキュリティ・サービス・エッジ (SSE) の Magic Quadrant™ でリーダーの 1 社と評価され、実行能力において最も高いポジションに位置付けられました。

詳細はこちら →

Zscaler Zero Trust Firewallの主な機能

ポリシーの一元管理	すべての場所に対するポリシーを定義してすぐに施行できるため、場所ごとのポリシーを再作成する必要はありません。
完全統合されたセキュリティサービス	コンテキスト情報は DLP、APT、サンドボックス、その他のサービスの間で共有され、保護と可視性が強化されます。
リアルタイムのきめ細かな制御、ログ記録、可視性	6 か月分の無制限のグローバル統合ログを活用して、豊富なフォレンジックデータによる詳細な可視性を確保し、トレンド検出、生産性分析、トラブルシューティングのための分析と関連付けを可能にします。
ユーザー認識型の脅威対策	グループ、部門、ロケーションによってユーザーを定義し (在宅勤務またはリモートのユーザーをロケーションとして設定する場合も含む)、アイデンティティー プロバイダーおよびローカル ユーザー データベースと統合することで、ユーザーの物理的な場所を問わず一貫したポリシーを適用します。

Zscaler Zero Trust Firewallの主な機能(続き)

アプリ認識型の脅威対策	最初のパケットでアプリケーション サービスを特定および分類して、ファイアウォールのフィルタリング ポリシーと転送ポリシーを有効にし、コンテキストを認識する適応型ポリシーで優先度の高いアクションを迅速に実行します。 すべてのネットワーク サービス (ポートとプロトコル)、ネットワーク アプリケーション (SNI (ホスト名)、DPI ベース)、アプリケーション サービス (最初のパケットによる識別、IP、FQDN グループ、その他のヒューリスティックベースの検出技術に基づく UCaaS) のアプリケーション タイプに対応しています。
適応型の IPS セキュリティと制御	カスタム IPS シグネチャー、適応型および振る舞いベースの数千の IPS シグネチャーを活用して、すべてのユーザーのインターネット トラフィックを検査します。これにより、接続の種類や場所を問わず、あらゆるポートとプロトコルで常時オンのクラウド型脅威対策を提供します。ThreatLabz が管理する IPS シグネチャーの一覧は、こちらからご確認いただけます。
高度なセキュリティ検査	FTP、DNS、RDP、Telnet などの非 Web プロトコルに高度な DPI を適用し、非標準ポート上の回避型のトラフィックを特定、防止します。

Zscaler Zero Trust Firewallの主な機能(続き)

DNS のセキュリティと制御	クラウド アプリケーションのパフォーマンスを最適化し、レイテンシーを最小限に抑えながら、Zscaler ですべての DNS をプロキシすることで優れたセキュリティを実現します。ユーザー、アプリ、場所、解決された IP の国に基づいてポリシーを有効にすることで、悪意のあるドメインからのユーザーを自動的にブロックし、DNS トンネリングを検出、防止します。 • **解決：**サービスとしての DNS によって、地理的な最適化、テナントの最適化、レイテンシーの最小化を通じた最適な解決を実現します。 • **DNS フィルタリング：**カスタム DNS フィルタリング ルールを作成して、既知の宛先や悪意のある宛先に対するさまざまな種類の DNS リクエストをブロック、許可、リダイレクトできます。 • **セキュリティとデータの持ち出し：**機械学習を活用してマルウェア、フィッシング、DNS トンネリング、データの持ち出しを検出します。 • **DNS over HTTPS (DoH):** 一般的な HTTPS トラフィックで DNS 接続を暗号化する際に、DoH の死角と組織の制御のバイパスを防ぎます。
完全修飾ドメイン名 (FQDN) ポリシー	複数の IP でホストされるアプリケーションのアクセス ポリシーを簡単に構成、管理できます。
ファイル転送プロトコル (FTP) の制御およびネットワーク アドレス変換 (NAT) のサポート	FTP と FTP over HTTP のアクセス制御、および NAT の宛先プロキシと NAT 転送をサポートします。
プライバシーおよびコンプライアンスの認定	グローバル企業および政府機関の厳格なリスク、プライバシー、コンプライアンス要件に準拠
業界および国のデータ プライバシー規制	業界固有および各国のデータ プライバシー規制に準拠しています。
世界規模で共有される保護	クラウド効果を活かし、Zscaler クラウドで処理される 1 日あたり数千億件のリクエストから特定された新たな脅威を、あらゆる場所のすべての Zscaler ユーザーにおいてブロックします。

Zscaler Zero Trust Firewall は、Zscaler Internet Access に完全に統合されており、ZIA、Zscaler for Users の Essentials および Business エディションに含まれています。Zscaler Zero Trust Firewall の高度な機能は、ZIA、Zscaler for Users の Transformation および Unlimited エディションに含まれているほか、アドオン モジュールとして、Essentials および Business エディションでも利用できます。

	Standard	Advanced
ZERO TRUST FIREWALL のポリシー基準		
ネットワークとアプリケーション サービス	✓ 最大 10 ルール	✓
FQDN フィルタリング チェック		✓
場所の認識		✓
ユーザーの認識 – チェック	–	✓
ネットワーク アプリケーション (DPI)	–	✓
動的なリスクベースのポリシー	–	✓
ファイアウォール ルール	✓ 最大 10 ルール	✓ 最大 1000 ルール以上
DNS 制御		
信頼できる DNS リゾルバー	✓	✓
DNS フィルタリングとセキュリティ	✓ 最大 64 ルール	✓
DNS トンネルとアプリの検出	–	✓
IPS 制御	–	✓
FTP 制御	✓	✓
NAT 制御	✓	✓

プラットフォームの特長		
すべての SSL 通信を分析	✓	✓
リアルタイム ロギング	✓ 完全な DNS ログを含む、ファイアウォールの許可アクションに関する集約ログおよびブロック アクションに関する詳細ログ Essentials および Platform ライセンスに含まれる	✓ ユーザー ID、アプリ ID、IPS を含む、すべてのアクションと機能に関するログ 追加のアドオン ライセンスが必要

Zscaler について
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange™ は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/jp**

zscaler™

Zero Trust Everywhere