Always Secure. Always Available.

ソリューションブリーフ

クラウドサービス活用時代に適した プロキシソリューション

A10 Thunderによるセキュアサービスエッジとゼロトラストアーキテクチャの実現

プロキシの従来の利用方法と役割の変化

従業員などがインターネットアクセスをセキュアに行うためのソリューションとして、プロキシサーバ（プロキシ）は広く利用されています。従業員や組織をサイバー攻撃から保護するために、組織内にある業務用の端末からインターネットにアクセスする際に、Webプロキシがユーザー認証・認可を行ったり、URLフィルタリングによって不正なサイトや業務に無関係なサイトへのアクセスをブロックしたり、攻撃の痕跡を事後に追跡するためのアクセスログを保管できる機能が主に利用されてきました。また、インターネット接続回線の利用効率を上げるために、Webコンテンツのキャッシュ機能も活用されてきました。

その一方で、近年、従来に比べてインターネットの利用が業務に占める割合が増え、オフィススイートなどを含めたSaaS型のクラウドサービスなどを活用するようになったことから、従来のプロキシでの処理能力を上回る通信トラフィックが発生するようになりました。加えて、HTTPSなどの暗号化された通信やカスタマイズされたWebコンテンツの利用が拡大したことで、既存のセキュリティ機能やコンテンツキャッシュの機能が十分に有効でなくなっています。これに対処するために、HTTPSなどの暗号化された通信をプロキシで復号して検査しようとすると、大幅に処理能力が低下してしまう問題があります。

また、広く重要性が指摘されるようになったゼロトラストアーキテクチャにおいては、ネットワークの境界を設けて内部のネットワークにあるものを完全に信用する姿勢を排除した設計が重要となります。これを実現するには、従業員のリソースへのアクセスを認証基盤と連携して動的に認証・認可したり、内部からの不正なサイトへのアクセスを抑止したり、クラウドサービスなどを利用する際にもIDベースセキュリティで管理可能なアカウントのみでアクセスさせるように制限する必要があります。

クラウドサービス活用とゼロトラストアーキテクチャ実現に適した A10 Thunder CFWによるプロキシソリューション

A10ネットワークスのA10 Thunder CFWシリーズではクラウドサービス活用に適したプロキシ機能を提供しています（図1）。クラウドサービスの利用などで発生する大規模な通信セッションを処理できる高い性能を持ち、宛先サービスのドメイン名に応じて通信ボトルネックを回避するためのトラフィック制御や回線分散を行うことで、快適なクラウドサービス利用を実現します。また、クラウドサービスを利用する際に利用可能なアカウントを制限し、個人や利用が許可されていない法人アカウントでのログインを止めることができます（テナント制御）。クラウドサービスへログインできるアカウントをIDベースセキュリティで管理可能なアカウントに制限することで、組織のゼロトラストアーキテクチャの実現に貢献します。加えて、認証基盤と連携してユーザー認証・認可を行うことでリソースへのアクセスを柔軟に制御でき、ゼロトラストアーキテクチャにおけるポリシー実行ポイントの役割を担うことができます。

HTTPSなどのSSL/TLS通信の復号を高速に実施でき、暗号化通信に隠れた攻撃の痕跡や従業員の振る舞いの追跡を確実に行うことができます。通信の完全な可視化と通信の振る舞いの評価は、ゼロトラストアーキテクチャにおける動的な認証・認可において、非常に重要な要素となります。また、SSL/TLSを復号し、他のセキュリティ機器と連携することで、高度な攻撃の検知と防御も実現できます。

課題：

- SaaSをはじめとするクラウドサービスのセキュアで快適な利用環境の実現
- 認証・認可に基づく適切なインターネットアクセス制御
- 攻撃の痕跡や従業員の振る舞いを追跡するための詳細なアクセスログの取得
- 暗号化された通信に隠れた攻撃を含む、多様化するサイバー攻撃からの従業員の保護

解決策：

- A10 Thunder CFWによる大規模なセッション処理と通信トラフィックの制御、およびクラウドサービスを利用するアカウントの制限（テナント制御）
- 認証・認可基盤と連携した柔軟なインターネットアクセス管理とアクセス制御
- SSL/TLS通信の復号による詳細なアクセスログの記録
- SSL/TLS通信の復号、リアルタイムでの脅威からの防御を実現するURLフィルタリングやIPアドレスレピュテーション、L4/L7ファイアウォール、IPsec-VPNなどのセキュリティ機能の利用

メリット：

- 通信のボトルネック回避や回線分散による快適なクラウドサービスの利用と、テナント制御によるゼロトラストアーキテクチャ（IDベースセキュリティ）の実現、高いコストパフォーマンスによるTCOの削減
- 認証・認可による適切なリソースへのアクセス制御
- 詳細なアクセスログによる攻撃の痕跡や従業員の振る舞いの確実な追跡
- 不正なサイトへのアクセスや攻撃者からのアクセスの防止によるセキュリティ機能の強化

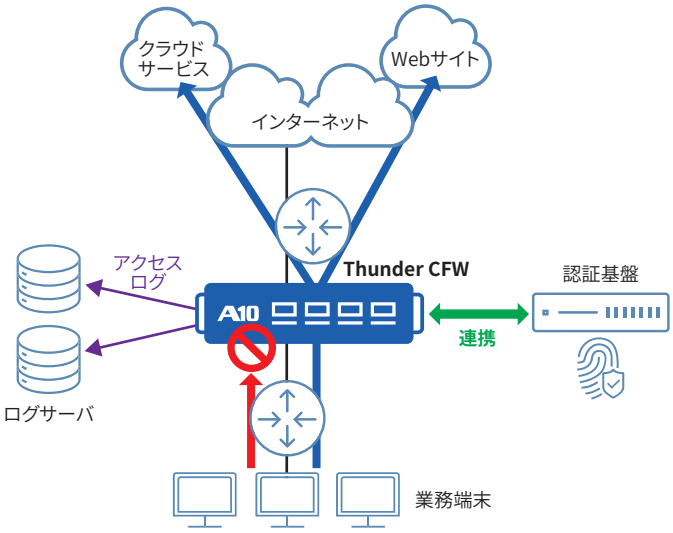

図 1： A10 Thunder CFW のプロキシ機能

多様なセキュリティ機能

A10 Thunder CFW では、プロキシ機能や SSL/TLS 通信の復号機能に加え、以下のセキュリティ機能も併せて利用できます。

URL フィルタリング・URL レピュテーションによる通信制御

通信の宛先となる URL を 80 種類以上のカテゴリに分類し、アクセスの可否や SSL/TLS 復号の実行可否を制御できます。悪意のあるカテゴリに分類されるサイトへのアクセスを拒否したり、アクセスログを取得することで、端末のボット感染を防いだり、ボット化した端末や悪意のある従業員による不正サイトへのアクセスを検知できます。URL のレピュテーションスコアに基づく通信制御やアクセスログの出力も可能です。URL のカテゴリやレピュテーションスコアはリアルタイムで更新され、最新の脅威に迅速に対応できます。

IP アドレスレピュテーションによる通信制御

リアルタイムで更新される悪意のあるサイトの IP アドレスリストを利用し、宛先 / 送信元の IP アドレスに基づいてアクセス可否を制御できます。DNS が不正に改変されている場合でも、IP アドレスでの制御により不正なサイトへのアクセスを防止できます。また、攻撃者からのアクセスの防止や、悪意のある従業員の不正な振る舞いの検知にも利用できます。

L4/L7 ファイアウォールによるセキュリティ

L4 ファイアウォールの機能がビルトインされており、組織の内部・外部への不正アクセスの制御や、組織内での攻撃の水平展開を防ぐためのマイクロセグメンテーションを実現できます。また、アプリケーション可視化によるシャドー IT の発見や利用の許可されていない Web アプリケーションの利用を制限するために、L7 ファイアウォール（アプリケーションファイアウォール）の機能を利用できます。3,500 種類を超えるアプリケーションをディープパケットインスペクション（DPI）により識別します。

IPsec VPN による通信経路の暗号化

オープンな通信回線においても通信経路を暗号化し、セキュアな通信経路を実現するために IPsec VPN 機能を利用できます。複数サイト間での広帯域な Site-to-Site IPsec VPN だけでなく、業務端末の OS にビルトインされた IPsec VPN と接続するための Client-to-Site IPsec VPN にも対応しています。

マルウェアスキャン / ファイル無害化 / データ損失防止

A10 Thunder CFW が OPSWAT 社の提供する MetaDefender Core と連携することで、最大 30 種類以上のアンチマルウェアエンジンを利用して高精度にマルウェアを検知するマルウェアスキャンや、ファイル形式を変換することなく悪意の埋め込まれる可能性のある要素を取り除くファイル無害化、機密性の高いデータのマスキングや外部漏洩を防止するデータ損失防止の機能を利用できます。SSL/TLS 復号の機能と併せて利用することで、標的型攻撃などの高度な攻撃に対し有効に防御を行うことができます。

高い通信処理性能

A10 Thunder CFW は独自のアーキテクチャに基づく OS を利用することで、コンパクトな筐体でも非常に高い性能を持ちます。同価格帯の製品でも、他社のプロキシ製品と比較して 40 倍以上の同時セッション数を処理でき、120 倍以上のスループットを実現します。ハードウェアアプライアンスだけでなく、ベアメタル、仮想アプライアンス、コンテナなどの多様なフォームファクタに対応しており、いずれのフォームファクタにおいても、同一の機能を高い性能で利用でき、環境に応じた柔軟な配置が可能です。

ハードウェアアプライアンスを利用する場合は、以下がユーザー数あたりの目安になります。

- 6,000 ユーザー未満：Thunder 1040
- 10,000 ユーザー未満：Thunder 3040
- 10,000 ユーザー以上：Thunder 3350 または Thunder 4440

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、サービス事業者やクラウド事業者および企業で利用される 5G ネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を担保します。A10 Networks は 2004 年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界 117 か国のお客様にサービスを提供しています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

www.a10networks.co.jp/
Facebook：https://www.facebook.com/A10networksjapan

Learn More
About A10 Networks

お問い合わせ
a10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp
a10networks.co.jp/contact

©2022 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networksは米国およびその他各国におけるA10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。商標について詳しくはホームページをご覧ください。www.a10networks.com/a10-trademarks

Part Number: A10_SB_Proxy　MAR 2022