超高性能なデータセンター保護をコンパクトなアプライアンスで実現

Thunder Convergent Firewall のパフォーマンスと拡張性

課題：

高まるトラフィック需要に応じて拡張可能な高性能なソリューションを提供するのと同時に、ますます高度化する脅威からデータセンターのサービスや資産を保護します。

ソリューション：

A10 Thunder CFWに搭載されたデータセンターファイアウォール（DCFW）機能は、これまでにないパフォーマンスと拡張性を発揮して、高度な脅威、Webアプリケーション攻撃、およびDDoS攻撃から防御します。A10 Thunder CFWは、一連の高度な機能を単一のアプライアンスに統合する柔軟なセキュリティソリューションです。

利点：

- 包括的なセキュリティ機能セット
- セキュアなトラフィック経路の隔離を実現するマルチテナントサポート
- 複数のポート構成オプションが用意され、コンパクトでスペース効率のよいデザイン
- 単一のインターフェイスから複数のセキュリティ機能セットを管理可能
- データインターフェイスと管理インターフェイスの両方でIPv4/IPv6同等機能を完全にサポート
- データプレーンとコントロールプレーンの完全な分離

データセンターファイアウォールは、貴重なデータセンター資産の保護に不可欠な要素であり、組織の総合的なセキュリティポリシーの最も重要な構成要素の1つです。データセンターファイアウォールのパフォーマンスと安定性は、様々なサービスの中断を防止して、待ち時間に起因する応答速度の低下を防止するために非常に重要です。応答速度の低下は、アプリケーションのパフォーマンスに影響を与える可能性があります。アプリケーション遅延やパケット喪失などパフォーマンス低下の要因は、多大な経済的損失をもたらす可能性もあります。

A10 Networks® Thunder® Convergent Firewall（CFW）は、包括的なセキュリティの機能セットによって超高性能なデータセンターを実現します。含まれている機能としては、ステートフルなデータセンターファイアウォール（DCFW）、Webアプリケーションファイアウォール（WAF）、DNSアプリケーションファイアウォール（DAF）、アプリケーションアクセス管理（AAM）、アプリケーションレイヤーゲートウェイ（ALG）のサポート、分散型サービス拒否（DDoS）攻撃からの防御、高度なレイヤー4/レイヤー7サーバーロードバランシングなどが挙げられます。

課題

企業ネットワークの境界を保護するためのファイアウォールを実装する場合とは異なり、データセンターファイアウォールの実装時には、いくつかの指標を考慮する必要があります。企業ネットワークの境界でインターネットアクセスを保護する場合と比べて、トラフィック量がはるかに多いため、データセンターファイアウォールのパフォーマンス特性は非常に重要です。企業ネットワークの場合と比較してトラフィックパターンとポリシー施行が異なるということは、高負荷時のデータセンターファイアウォールのパケット検査プロセスに影響を与えます。クライアントとデータセンター間の従来のNorth-South型トラフィックパターンが進化した結果、アプリケーションサーバーとデータベースサーバー間でやり取りされるEast-West型トラフィックや、データセンターとパブリック/プライベートクラウド間でやり取りされるデータセンター間トラフィックも、North-South型トラフィックに含まれるようになりました。

ファイアウォールは、データセンター内のさまざまなトラフィックフローを検査して適切なポリシーを適用する必要があり、組織はトラフィックの経路を最適化するという課題を抱えています。これが特に当てはまるのは、VM間トラフィックへの移行が進んでいるハイブリッドデータセンター環境内です。データセンター内の複数のフロー方向に対処するためには、特定のセキュリティポリシーを施行してデータ機密性を確保するための別個の分類ゾーンを実装することが望ましい場合があります。このためには、データセンターファイアウォールはフローを分割および分離するための柔軟性を備えている必要があります。この場合、各ゾーンには独自のセキュリティポリシーおよびインターフェイスを格納できるものとします。データセンターのトラフィックを隔離することで、既存のNorth-South型ファイアウォールインターフェイスにEast-West型トラフィックをリダイレクトしたり、ヘアピン転送したりするなどの手法を回避し、最適なトラフィック経路を利用することが可能です。このような機能を使用すると、別個のファイアウォールを実装することなく、部門ごとにトラフィックを隔離することもできます。

データセンターファイアウォールには、高スループットを維持できること、サーバーファームにアクセスする数十万のセッションをサポートできること、およびアプリケーションサーバー接続の頻繁な開始と終了に起因する高いTCP接続レートを処理できることといった機能が必須です。

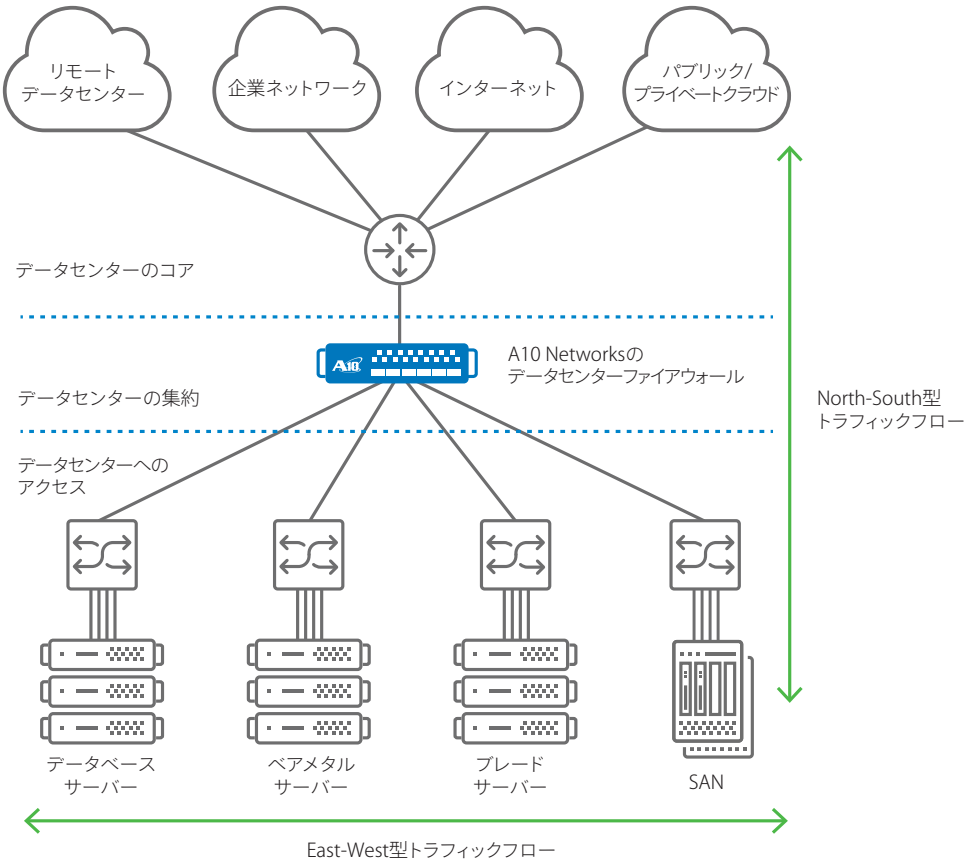

図1：データセンター内のトラフィックフロー

A10 ネットワークスのデータセンターファイアウォール ソリューション

A10 Networks のデータセンターファイアウォール（DCFW）機能は非常に高性能なステートフルファイアウォールであり、最大 220 Gbps のスループットを実現し、650 万接続 / 秒（CPS）をサポートし、大規模なデータセンターアプリケーション向けに最大 2 億 5600 万件の同時セッションに対応できる接続テーブルをサポートしています。A10 の DCFW は、大規模なマルチテナント環境に対応する、最大 128,000 件のファイアウォールルールもサポートしています。

A10 Thunder CFW 製品ラインには、DCFW が標準機能として組み込まれているだけでなく、Web アプリケーションファイアウォール（WAF）や DNS アプリケーションファイアウォール（DAF）などの他のセキュリティ機能も組み込まれています。A10 Thunder CFW でサポートされているアプリケーションデリバリーパーティション（ADP）機能を使用すると、A10 Thunder CFW を複数の独立したレイヤー 3 ドメインに論理的に分割してトラフィックフローを隔離、個別のセキュリティ機能セットをさまざまなトラフィックタイプに適用できます。

マルチテナント環境を保護

世界中の組織がクラウドコンピューティングを導入し、データセンターを仮想化して運用効率や俊敏性を向上し、規模を拡大しています。継続的なアプリケーション導入、ネットワーク機能の仮想化（NFV）、ソフトウェア定義ネットワーキング（SDN）などのトレンドはいずれも自動化を必要としており、そのためには完全なプログラミング機能が必要です。データセンターファイアウォールはこの新しいパラダイムに順応して、仮想導入、オンデマンドスケーラビリティ、クラウドオーケストレーションに対応する必要があります。データセンターファイアウォール機能が統合された A10 Thunder CFW は、A10 Harmony™ アーキテクチャーによって、完全にプログラミング可能なデータセンターセキュリティを実現します。A10 Harmony はポリシーコントロールを統合し、これまでにない優れたテレメトリーを提供し、RESTful API に完全に対応しています。

A10 Thunder CFW がサポートするレイヤー 3 仮想化（L3V）機能を使用すると、各パーティション独自のネットワーキングリソースやアプリケーションリソースに直接アクセス可能な、独立したアプリケーションデリバリーパーティション（ADP）を作成できます。それぞれの L3V ADP は、マルチテナント環境で完全なトラフィック経路の分離を可能にする独立した L3 ドメインであり、セキュリティポリシーやトラフィックポリシーに従って、独自のセキュリティプロファイルを作成できます。たとえば、ある ADP では DDoS 攻撃を緩和するステートフルファイアウォールをサポートする一方で、別の ADP では HTTP トラフィックの検査と規制のために WAF をサポートすることができます。A10 Thunder CFW が持つ負荷分散機能は、ADP を、DNS アプリケーションファイアウォール（DAF）を有効にした DNS サーバーロードバランシングなどの特定用途専用に使用可能です。

それぞれの ADP は別々に管理できるため、組織内の異なるグループが独自のリソースを管理可能です。A10 Thunder CFW による L3V ADP のサポートにより、単一のセキュリティプラットフォームを使ってマルチテナントデータセンター環境でさまざまなセキュリティ要件に対応するための柔軟性を得ることができます。

Web アプリケーションファイアウォール（WAF）

A10 の Web アプリケーションファイアウォール（WAF）機能は、Web ベースのアプリケーションサーバーをターゲットにした OWASP（オープン Web アプリケーションセキュリティプロジェクト）の上位 10 位を占める重大な脅威から Web サーバーを防御します。WAF 機能は、Web アプリケーション宛てのトラフィックと Web アプリケーションからの応答トラフィックの両方を検査します。WAF 機能では、Web アプリケーションインフラストラク

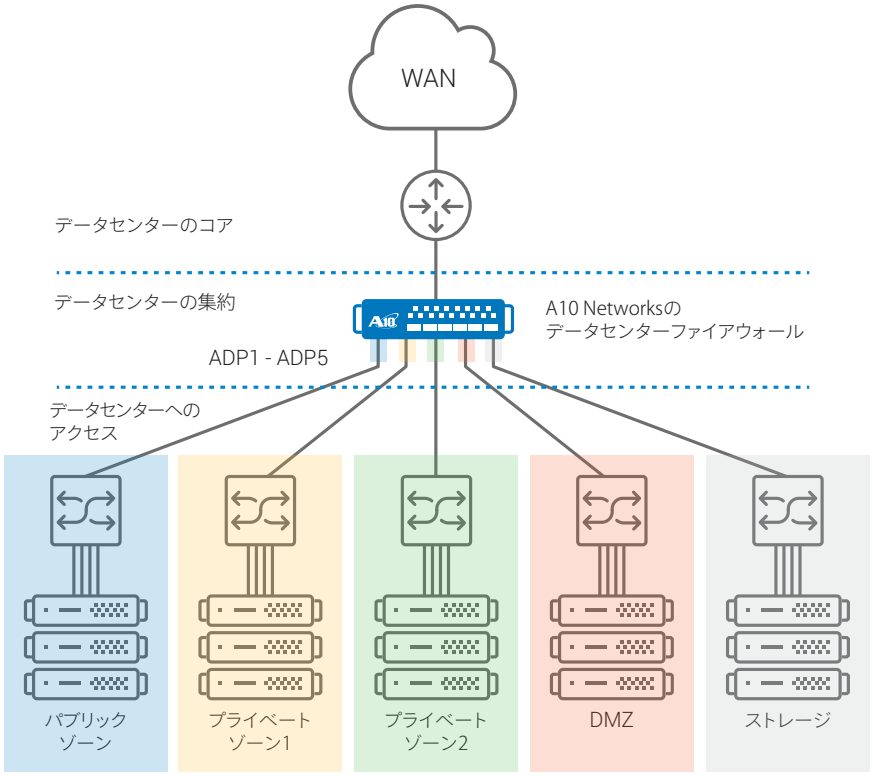

図2：データセントートラフィック分類ゾーン

チャーとアプリケーションユーザーの両方を保護することで、DCFW機能を補完し、より細かいレベルの防御を追加で実現します。

A10のWAF機能は現在の多くの脅威を認識し、柔軟なカスタマイズによって新たな脅威にも対応するよう設計されています。A10のWAF機能は、他の多くのベンダーのようにサードパーティーのWAFコードを統合するのではなく、A10ネットワークスのAdvanced Core Operating System（ACOS®）専用に開発されています。このようなアプローチの結果、高度なスケーラビリティとパフォーマンスを発揮するセキュリティソリューションが得られます。

WAF機能は、A10の他のセキュリティメカニズムと連携して、Webアプリケーションの包括的な防御、コード脆弱性からの保護、およびデータ漏えいの防止を実現することもできます。また、PCI-DSS（クレジットカード業界のデータセキュリティ基準）など、セキュリティに関する規制を遵守する上でも役立ちます。

DNSアプリケーションファイアウォール（DAF）

A10のDNSアプリケーションファイアウォール（DAF）機能は、A10 Thunder CFWに組み込まれており、DNSインフラストラクチャーを保護してDNSサーバーリソースを最適化することを目的として設計されています。A10 DAFはすべてのDNSトラフィックを検査して、正規のトラフィックであることを確認し、不正なトラフィックをブロックするか追加検査のためにリダイレクトします。

DNS攻撃（偽装されたソースIPアドレスからの不正な形式のDNSパケットの送信など）は、標準のDNSパケットタイプに一致しないトラフィックを削除することで簡単に阻止できます。IPレート制限によってトラフィック急増からの高度な保護を可能にすることで、DNSサーバーはフラッド攻撃から防御されるため、DNSトラフィックの処理や増大する高負荷時間帯への対応に貴重なリソースを利用することができます。

攻撃者は、特殊なクエリータイプや命令コードを使用して要求を送信することで、DNSサーバーを悪用することもできます。A10 Thunder CFWは、特定のDNSクエリータイプや特定のDNS命令コードを許可または拒否するように設定できます。A10のDAF機能は、クエリー動作に関するきめ細かいアプリケーションルールとIPレート制限などの対策を通じて、DNSインフラストラクチャーの悪用に対する高度な防御を実現します。

機能と利点

包括的で拡張性の高い管理

A10 Thunder CFWは業界標準のCLIやWebユーザーインターフェイス、およびサードパーティー製管理システムと統合可能なA10 Networks aXAPI® RESTベースAPIを備えており、管理を効率化および自動化することが可能です。大規模な導入の場合は、A10ネットワークスの集中管理システムaGalaxy®を使用して、物理的な場所にかかわらず、複数のA10 Thunder CFWアプライアンスで日常的なタスクを広範囲にわたって実行できます。

ロギングおよびレポート作成

A10 Thunder CFWは、トラフィック分析のための高速syslogロギングに加えて、電子メールによるアラートや、トラフィック分析のためのNetFlowとsFlowの統計情報をサポートしています。リアルタイムダッシュボードには、システム情報、メモリーとCPUの使用率、およびネットワークステータスが表示されます。

運用・設備コストを削減

A10 Thunder CFWは、複数のセキュリティサービスを単一の強力なプラットフォーム上に統合することで、データセンターのコストを削減します。これにより、必要なネットワークデバイス数を減らして、消費電力と冷却コストを低減して、貴重なラックスペースを節約できます。

A10のデータセンターファイアウォール機能は、セキュリティ機能を統合するだけでなく、必要に応じてネットワーキング機能やアプリケーション

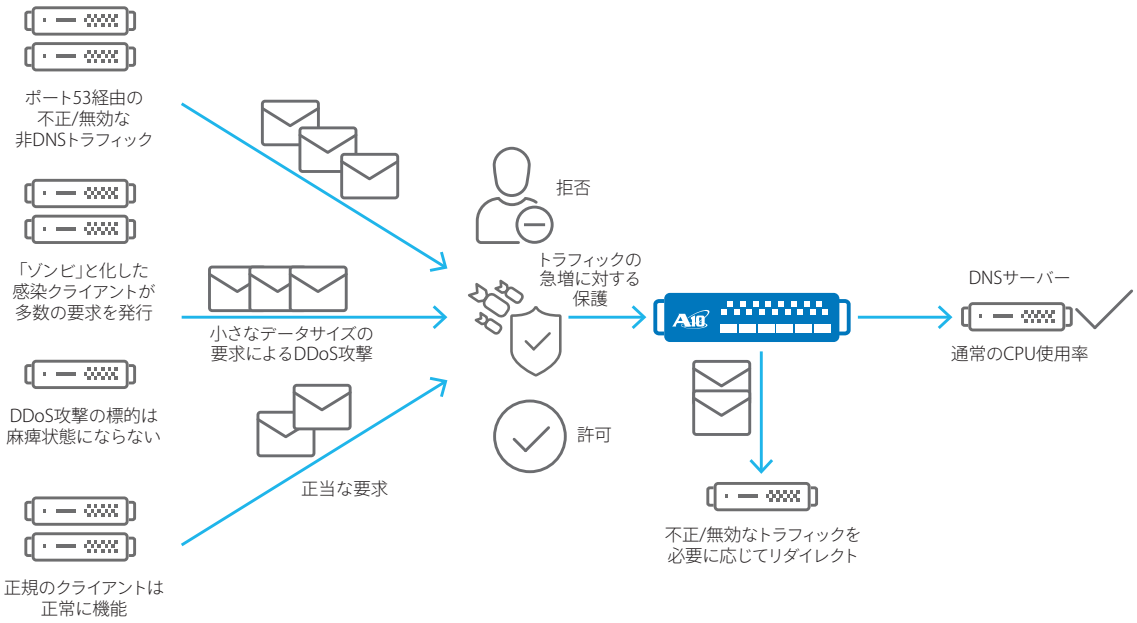

図3：DNSアプリケーションファイアウォール機能では、既知の不正なクライアントからの攻撃、非DNSトラフィック、およびDNSクエリーを検知可能

デリバリー機能も統合することで、集約化をさらに進め、データセンターから単一目的のデバイスをなくし、ハードウェアコストと運用コストを削減することを可能します。ファイアウォールポリシーはACOSオペレーティングシステムに完全に統合されるため、顧客はパフォーマンスに影響を及ぼすことなく、負荷分散とセキュリティ機能を同時に使用できます。単一の管理インターフェイスを使用して複数のセキュリティ機能とアプリケーションデリバリー機能を管理できるため、運用コストをさらに削減できます。

ソリューションのコンポーネント

- Thunder Convergent Firewall（Thunder CFW）
- データセンターファイアウォール（DCFW）
- aGalaxy® 集中管理システム
- aXAPI® REST ベース API

まとめ - コンパクトなアプライアンスによる超高性能なデータセンターの実現

データセンターファイアウォールの機能セットは、他の主要コンポーネントとともにA10 Thunder CFWに組み込まれており、強力で柔軟なセキュリティソリューションを提供します。A10 Thunder CFWは、A10のAdvanced Core Operating System（ACOS）プラットフォーム上に構築されており、Symmetric Scalable Multi-Core Processing（SSMP）ソフトウェアアーキテクチャーをベースにしています。SSMPアーキテクチャーは、現在と将来のデータセンタートラフィック負荷への対応に求められる、非常に高いパフォーマンスを実現します。

A10 Thunder CFWは、コンパクトなアプライアンスに格納された超高性能なセキュリティソリューションであり、組織が新たな脅威を広範囲にわたって阻止することが可能です。データセンターファイアウォール機能は、共有メモリーアーキテクチャーとFTA（Flexible Traffic Accelerator）テクノロジーを統合し、超高速のスループットと比類ない接続数を実現します。これにより、データセンターの資産を保護すると同時に、従来のパフォーマンスボトルネックを解消することが可能です。

次のステップ

詳細については、A10の営業窓口にお問い合わせいただくか、www.a10networks.co.jp/lp_thunder-cfwを参照してください。

A10 Networks / A10ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はアプリケーションネットワーキングおよびセキュリティ分野におけるリーダーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。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、世界各国の拠点からお客様をサポートしています。

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。詳しくはホームページをご覧ください。

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

A10ネットワークス株式会社
〒105-0001
東京都港区虎ノ門4-3-20
神谷町MTビル16階
TEL：03-5777-1995
FAX: 03-5777-1997
jinfo@a10networks.com
www.a10networks.co.jp

海外拠点

北米（A10 Networks本社）
sales@a10networks.com
ヨーロッパ
emea_sales@a10networks.com
南米
latam_sales@a10networks.com
中国
china_sales@a10networks.com
香港
HongKong@a10networks.com
台湾
taiwan@a10networks.com
韓国
korea@a10networks.com
南アジア
SouthAsia@a10networks.com
オーストラリア/ニュージーランド
anz_sales@a10networks.com

お客様のビジネスを強化するA10のアプリケーションサービスゲートウェイ、Thunderの詳細は、A10ネットワークスのWebサイト**www.a10networks.co.jp**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-SB-19157-JA-01
June 2016