ソリューションブリーフ

モバイルネットワーク向け GI/SGIファイアウォールプロテクション

サービスプロバイダのモバイルおよびクラウドネットワークの構築を先進のセキュリティでサポート

概要

モバイルデバイスの急速な普及と過去に類を見ないモバイルデータの増加に加え、新たなデジタルコンテンツやアプリケーションの需要により、モバイル通信事業者はすべてIPベースで構成されたモバイルネットワークに巨額の投資を行っています。

これにより、モバイル通信事業者が直面していた多くの課題が解決されるだけでなく、これまで不可能だった新しい種類のアプリケーションやサービス（ビデオ通話、高解像度コンテンツストリーミングなど）の可能性の扉が開かれました。

IoTを想定して設計される次世代のネットワークや規格は、モバイルブロードバンドをスムーズに5Gに進化させ、スケーラブルかつハイパーコネクトされた幅広いユースケースに対応します。

課題

LTEなどすべてIPベースのモバイル通信システムは増え続ける攻撃の対策が必要です。DDoSフラッド攻撃、アプリケーション層への攻撃、DNSの脆弱性をつく攻撃などは、ボットネットに感染したモバイル端末やIoTデバイス、さらにはインターネットや外部のパケットデータネットワーク（PDN）ゲートウェイ内のどこからでも発生し、サービスの可用性を脅かしています。

モバイルコアに対するDDoS攻撃が増加しているため、サービスプロバイダ各社は、進化するマルチベクトル型攻撃を含む大規模DDoS攻撃の検知と防御や、加入者のセッションを検査するステートフルファイアウォールなど、包括的なセキュリティソリューションの導入が急務となっています。

A10のキャリアグレードネットワークソリューションは、ネットワークインフラの延命の目的のために導入することもできます。接続性の維持と高いネットワーク可用性を可能にし、最高のユーザ体験を提供することができます。

eNodeBをLTEモバイルコアに接続するには、モバイル通信事業者のインフラストラクチャにおいてIPsecによる暗号化されたセキュアな通信が必要です。これにより、キャリアグレードのWi-Fi構築において、安全でないアクセスネットワーク上のトラフィックを保護します。

課題

サービスプロバイダは脅威やマルチベクトル型攻撃からモバイルネットワークインフラ、アプリケーション、および加入者を保護しながら、常時利用可能な可用性の高いネットワークを維持し、可能な限り最高のユーザ体験を提供する必要があります。

ソリューション

A10 Thunder CFWに搭載されたGi/SGiファイアウォール機能は、モバイルコアインフラや加入者をマルチベクトル型攻撃から保護し、アプリケーションを高可用性、高速、高セキュリティの状態に保ちます。モバイルネットワーク上の戦略的な場所で、スケーラブルで柔軟かつ高性能のセキュリティ機能を提供します。

特長

- キャリアグレードNAT(CGNAT)、ステートフルファイアウォール、およびDDoS防御機能を統合することにより、運用タスクを簡素化し、CAPEXおよびOPEXを削減
- クラス最高のパフォーマンスと拡張性をコンパクトな筐体で提供
- 高性能なIPsec VPNとトラフィックの検査で、データセンターやハイブリッドクラウドを保護
- IoTやM2Mネットワークをサポートする5Gや4G LTE、3Gネットワーク向けのIPsec機能により、リモートサイトとの安全な相互接続環境を実現

IoTの導入においては外部環境にあるデバイスをインターネット経由でバックエンドのサーバーに接続することができます。サービスプロバイダは進化するPDNベースの攻撃からモバイルネットワークコアおよび加入者を保護し、大規模なIPsec VPNトンネルとスループットを提供できるソリューションが必要です。

A10のGi/SGiファイアウォールソリューション

Gi/SGiファイアウォール機能を搭載したA10 Thunder® CFWは、モバイルキャリアがネットワークを拡張および保護するために必要なパフォーマンスを提供します。Thunder CFWは毎秒600万以上のコネクション数(CPS)と、2億5000万以上の同時セッション数をサポートし、最大で220 Gbpsのスループットを提供することが可能です。そのため、あらゆるサービスプロバイダの現在そして将来増加するトラフィックの要求条件を見越した導入が可能です。

モバイルキャリアは、自社モバイルネットワークインフラの各所にThunder CFWを戦略的に配置することにより、EPC(EvolvedPacket Core)のGGSN(Gateway GPRS Support Node)やPGW(PDNゲートウェイ)など、自社インフラのセキュリティを効果的に確保することができます。

IPv4の延命とIPv6への移行

Thunder CFWに搭載されたキャリアグレードNAT(CGNAT)機能により、モバイルキャリアは現行のIPv4ベースのインフラを延命することができます。さらに、NAT64/DNS64などの実績あるIPv6移行技術もサポートしており、IPv6ネットワークへのスムーズな移行をアシストします。加入者は、どちらのアドレスからでも各リソースへシームレスにアクセスすることができます。

アプリケーションレイヤーゲートウェイ(ALG)により、IPアドレス変換した場合でもアプリケーションの動作と透過性を維持します。Thunder CFWは、IPv4延命とIPv6移行ソリューションを同時にサポートできるため、運用タスクの簡素化と、システムにかかるコスト削減を実現します。

モバイルネットワークのセキュリティ

Thunder CFWのGi/SGiファイアウォールは、ネットワークリソースをきめ細かく制御し、モバイルキャリアがネットワーク攻撃を阻止して、不正アクセスを防止できるようにします。豊富な機能を持つステートフルファイアウォールによって加入者を保護し、複数の脅威からモバイルのデータプレーンとコントロールプレーンサービスを守ります。

A10 Thunder CFWには、以下のモバイル通信向けセキュリティ機能が含まれます。

- CGNAT、ファイアウォール、アプリケーションの可視化などのL4-L7のサービスを統合したGi-LANソリューション
- 詳細なSCTPフィルタリングが可能なGTPファイアウォール
- DPIベースのアプリケーション可視化、制御
- マルチベクトル型のボリューム攻撃を防御し、NAT IPプールなどのリソースのセキュリティを確保して、侵入を阻止する、統合型DDoS防御機能

モバイルネットワークの導入オプション

❶ Gi/SGiインターフェイス

あらゆる脅威が進化し、インターネット、パブリックおよびプライベートクラウド、データセンターのインフラやその他のPDNゲートウェイからGi/SGiインターフェイスへの攻撃が増加しています。これにより、モバイルコアインフラは攻撃に対して脆弱な状態に置かれています。こうした攻撃にはGiインターフェイスの帯域を飽和させる攻撃、ファイアウォールへの攻撃、マルチベクトル型DDoS攻撃などが含まれます。

UEとPDNゲートウェイ間のデータプレーントラフィックはIPsecまたはGTPトンネルでカプセル化されますが、PDN(内部および外部の両方)から外部インターネットへのGiインターフェイスはカプセル化されていないため、マルチベクトル型攻撃に対して最も脆弱になっています。Gi/SGiファイアウォールを導入し、Gi/SGiのセキュリティを確保することが必要です。

❷ セキュアかつ相互接続可能なローミングの実現

サービスプロバイダにおいて、加入者にローミングサービスを提供する必要性が高まっています。これにはLTEと3Gローミング加入者の間の接続性の確保も含まれます。そのようなローミングサービスを構築する際、サービスプロバイダは自社ネットワーク上の自身の顧客を危険にさらすことなく、しかもローミング時のサービスの継続性を確保する必要があります。

きめ細かいSCTPフィルタリング機能を備えたGTPファイアウォールは、セキュリティと拡張性を提供しながら、GTPベースの脅威(情報漏洩、不審なパケット攻撃、アクセスネットワークやGRX/IPXの相互接続などから侵入するDDoS攻撃など)からモバイルコアを保護し、サービス中断のない運用をサポートします。

❸ モバイルバックホールの保護

E-UTRANとEPCの間にセキュリティゲートウェイ(SEG)を導入することにより、S1(コントロールプレーンおよびデータプ

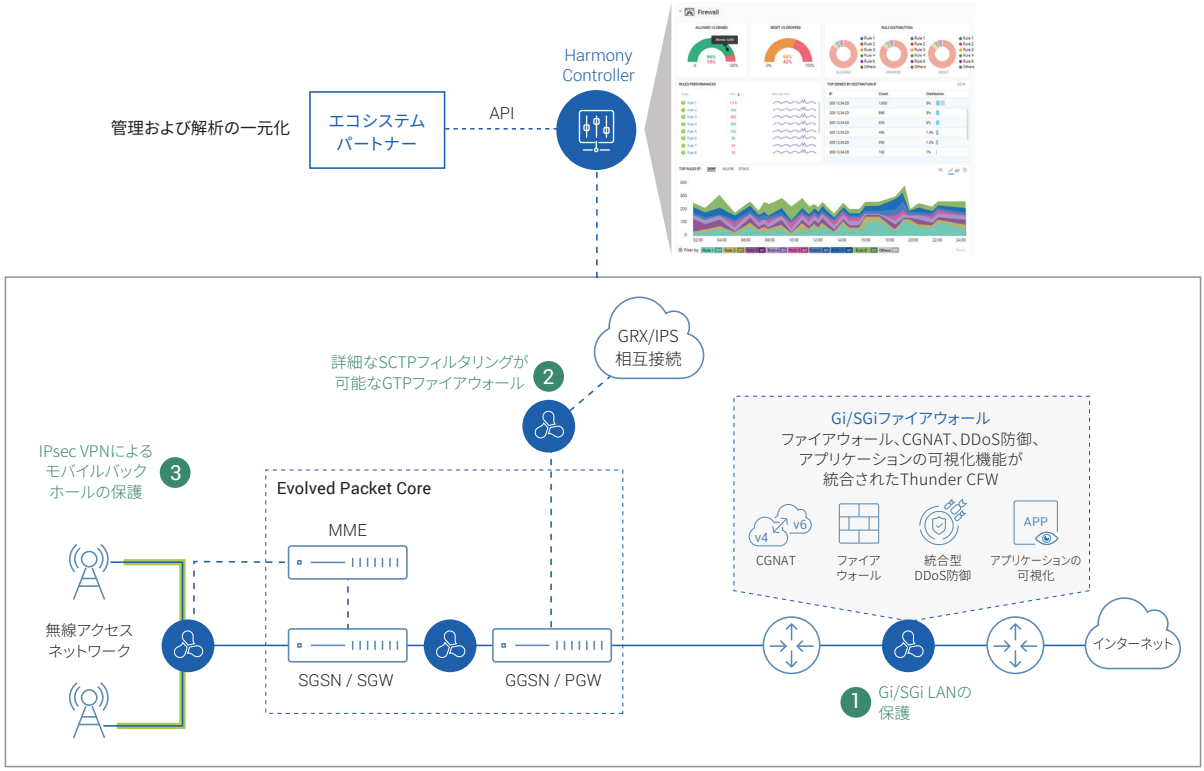

図1： A10 Thunder CFW Gi/SGiファイアウォールの導入シナリオ

レーン）インターフェイスを流れるバックホールトラフィックの秘匿性保護および整合性維持を実現することができます。通常、eNodeBとSEGの間にIPsecトンネルが構築され、大規模な終端処理を行うことが想定されます。この戦略的な展開により、無線アクセスネットワーク、VASエンジン、およびモバイルコアを標的とするモバイルデバイスのリスクを緩和することができます。

❹ アプリケーションの可視化と制御

ディープパケットインスペクションベースのアプリケーション可視化機能は暗号化トラフィックを含むトラフィックに対してきめ細かい分析を行い、40を超える数のカテゴリ、3000件を超えるアプリケーションに分類します。ネットワークおよびアプリケーションのトラフィックの傾向を理解することにより、効果的なネットワーク設備の計画、より深いビジネスインテリジェンス、法律執行機関（LEA）へのコンプライアンスの向上、サービスの収益化などにつなげることが可能です。

管理と可視化の一元化

A10 Harmony™ ControllerをThunder CFWと組み合わせて導入することにより、Giファイアウォール用の分析機能とともに、アプリケーションやネットワークレベルで可視性を向上させることができます。カスタマイズ可能なドリルダウンビューに分析結果を表示することができるため、レポートを通じて必要な対策を把握することできるようになります。また分析結果をもとにトラブルシューティングを迅速に進めることができます。さらにマルチクラウド環境に配置されたGiファイアウォール全体の一元的な管理と管理ポリシーの設定が可能です。

高パフォーマンスのアーキテクチャ

Thunder CFWアプライアンスは、A10のAdvanced Core Operating System（ACOS®）をベースに構築されています。ACOSはゼロから独自に開発し、マルチコアCPUアーキテクチャのパフォーマンスを最大限に引き出すように設計されています。ACOSはCPUコア数の増加に伴いパフォーマンスをリニアにスケールアップさせることが可能で、コンパクトなフォームファクタで比類ないパフォーマンスを発揮します。

ACOSは共有メモリ（Symmetric Scalable Multi-Core Processing（SSMP））アーキテクチャにより、各CPUが完全に独立した並列処理を行います。マルチコア特有の問題であるデータコピーやロッキングをなくすことにより、CPUのパフォーマンスを最大限に発揮させることが可能です。

Thunder CFW のアプライアンスはマルチコアアーキテクチャのために最適化されたスケーラビリティの高い 64 ビット OS により包括的なセキュリティソリューションを提供し、モバイルインフラストラクチャのセキュリティを確保します。

ソリューションのコンポーネント

- Thunder Convergent Firewall（Thunder CFW）
- Security Gateway（SeGW）
- Gi/SGi ファイアウォール（Gi/SGi FW）
- 詳細な SCTP フィルタリングが可能な GTP ファイアウォール
- アプリケーションの可視化と制御
- Site-to-Site IPsec VPN
- キャリアグレードネットワーキングソリューション
- 一元管理システム A10 Defend Orchestrator
- aXAPI®（REST ベースの API）

まとめ

A10 Thunder CFW には、Gi/SGi ファイアウォールおよびセキュリティゲートウェイの機能セットのほか、レイヤー 4 ステートフルファイアウォール、L7 アプリケーションの可視化、詳細な SCTP フィルタリングが可能な GTP ファイアウォール、統合された DDoS 防御、CGNAT など、主要ないくつかのキーコンポーネントが同梱されています。この包括的かつ統合されたアプローチにより、クラス最高のパフォーマンス、効率性、および拡張性を提供し、モバイルインフラストラクチャを保護すると共に OPEX および CAPEX のコスト削減をもたらします。

Thunder CFW は、A10 の ACOS プラットフォームをベースとした共有メモリアーキテクチャで構築され、現在そして将来のモバイルおよびクラウドネットワークの導入に必要な卓越した高いパフォーマンスを提供する強力かつ包括的なセキュリティソリューションです。

Gi/SGi ファイアウォールは、共有メモリアーキテクチャと Flexible Traffic Accelerator（FTA）テクノロジとの組み合わせにより、超高速スループットと比類なき接続速度を提供し、モバイルコアのインフラ資産を保護すると同時に従来のボトルネックを解消します。

さらに、A10 Networks の仮想アプライアンス vThunder® 上で Gi/SGi ファイアウォールソリューションを活用することにより、サービスプロバイダ各社は柔軟で、展開が容易、かつオンデマンドのソフトウェアベースの展開を実現できます。

お問い合わせ

製品に関するお問い合わせは a10networks.co.jp/contact よりご連絡ください。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks は、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Web サービス事業者まで 7000 社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10 ネットワークスは 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社を置き、世界中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。
詳しくはホームページをご覧ください。
• URL：https://www.a10networks.co.jp/
• X（旧 Twitter）：https://twitter.com/a10networksjp
• 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

Part Number: A10-SB-19169-JA-04 JUN 2024