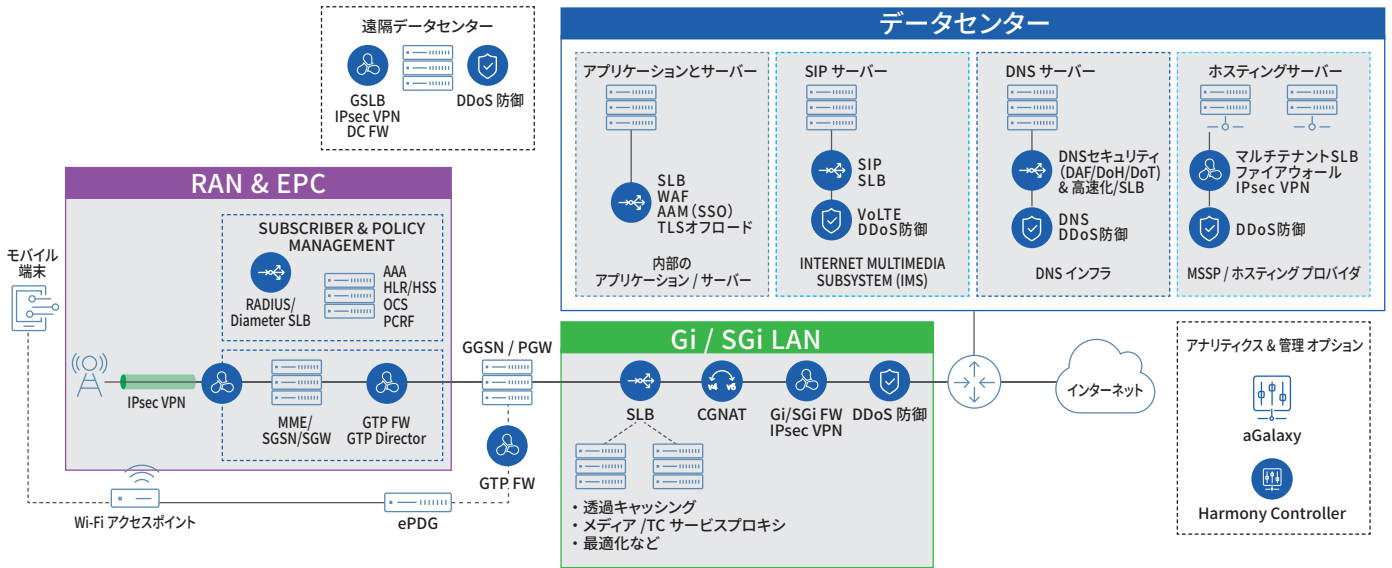
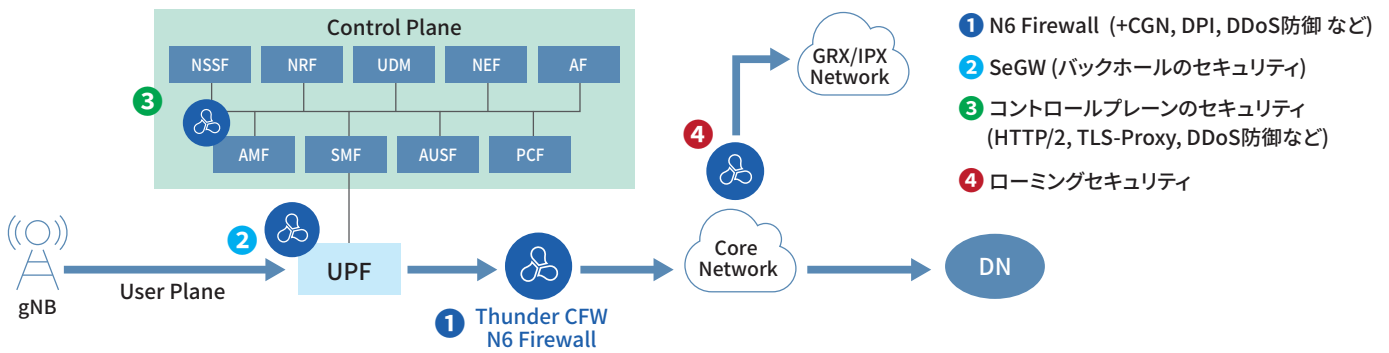


通信事業者様向けソリューション

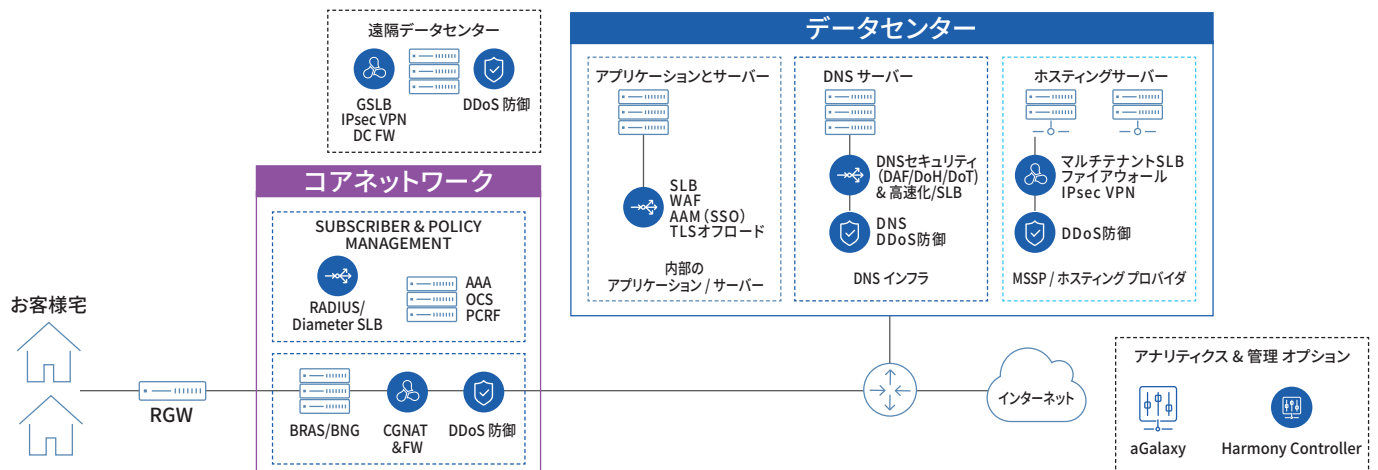
モバイル事業者様向けソリューションマップ (LTE/5G-NSA 向け)



モバイル事業者様向けソリューションマップ (5G-SA 向け)



ISP/CATV 事業者様向けソリューションマップ



IPv4 枯渇対策と IPv6 移行

A10 のキャリアグレード NAT (CGN) ソリューションを利用することにより、IPv4 アドレスの枯渇に対応しつつ、IPv6 への移行を進めることができます。Thunder CGN シリーズは、パフォーマンスに優れたトランスペアレントなアドレス・プロトコル変換を提供するキャリアグレードのネットワークゲートウェイであり、1.5U の専用ハードウェアアプライアンス 1 台で最大 370Gbps 以上のスループットを実現できます。

Thunder CGN は、CGN、DS-Lite、NAT64/DNS64、6rd、464XLAT、LW4o6、MAP-T、MAP-E などの様々な IPv6 移行技術を標準で提供し、NAT プールに対する DDoS 防御機能も持ちます。

CGN 機能などに各種セキュリティ機能が統合された Thunder CFW シリーズでは、IPv4/IPv6 双方の通信セッションに対するファイアウォール機能を提供する Gi/SGi ファイアウォール機能などを利用でき、インターネットからの攻撃からモバイルネットワークや加入者を防御したり、加入者の IPv6 端末間での攻撃や不正アクセスを防御することもできます。

パケットコアの防御や GTP トラフィックの制御

Thunder CFW シリーズでは、GTP/SCTP ファイアウォール機能を標準で利用できます。不正な GTP/SCTP 通信の検査やレートリミットなどが可能で、不正なローミング先や端末からの GTP/SCTP を悪用した攻撃からモバイル事業者のネットワークを防御します。また、GTP トラフィックの内容に基づき通信を適切なゲートウェイに振り分けるための GTP Director の機能を併せ持ち、モバイルネットワークのスライシングなどに利用できます。

広帯域の IPsec-VPN 機能により、バックホールの通信暗号化も実現できます。

DDoS 攻撃からの防御

Thunder TPS シリーズを利用することで、ネットワーク層からアプリケーション層までのマルチレイヤーに渡る DDoS 攻撃 (マルチベクトル DDoS 攻撃) を検知・防御して正常通信のみを通すことができます。ネットワークの外側からの攻撃だけでなく、内部からの攻撃にも対応できます。

管理ソリューションである aGalaxy と連携することで、フローデータから DDoS 攻撃を検知し、自動的に防御設定を変更できます。攻撃内容を分析するためのダッシュボードや高度なレポート機能も搭載されており、攻撃の状況を確認しながら対策を変更できます。

Thunder TPS は、機械学習を用いてボリューム型 DDoS 攻撃の内容を分析し、自動的に緩和フィルターを適用できる ZAP (Zero-day Automated Protection <ゼロデイ自動保護>) 機能が搭載されており、手動での作業なく迅速な防御を実現できます。不正な IP アドレスからの攻撃を防ぐために、50 以上の提携セキュリティ機関から集めた 3,100 万以上の脅威 IP 情報を相関分析することにより、高い検知率でありながら誤検知が少なく、リアルタイムに更新される IP レピュテーション情報も利用できます。

トラフィック制御と帯域制御

Thunder CFW シリーズを利用することで、通信トラフィックを適切なネットワークサービスにチェーンするためのトラフィック制御を行ったり、送信元/宛先やアプリケーションの種別に応じた帯域制御やレートリミットを

通信トラフィックに適用できます。利用者に応じて提供するネットワークサービスへ適切にトラフィックを振り分けることが可能です。

帯域制御/レートリミット機能を用いると、P2P アプリケーションやトラフィック量の多い利用者に対するトラフィック制御を行ったり、ネットワーク攻撃を防御することができます。

アプリケーション配信の最適化

Thunder ADC/CFW シリーズを利用することで、データセンター内の自社サービス、DNS サーバー、ホスティングサーバーなどのサーバー負荷分散や TLS オフロードなどのアプリケーション配信最適化を実現できます。

HTTP/2 のサーバー負荷分散や TLS1.3 のオフロードにも対応し、高速なアプリケーション配信を実現するとともに高いサービスの可用性を実現したり、Web アプリケーションファイアウォールや L4/L7 ファイアウォールによるセキュリティの強化を実現できます。

DNS サーバーの前段に配置して DNS over HTTPS や DNS over TLS を容易に実現したり、DNS リクエストに対するアプリケーションファイアウォール機能によるセキュリティ強化も実現できます。

ユーザー認証プロキシとしては LDAP 等との連携による認証・認可だけでなく、SAML2.0 や OpenID Connect、OAuth2.0 に対応した認証・認可、CAPTCHA を利用した認証なども実現できます。

ネットワーク仮想化 / コンテナ化への対応

Thunder シリーズは専用ハードウェアアプライアンスだけでなく、サーバー仮想化プラットフォームでの利用やベアメタルでのインストール、コンテナプラットフォームでの利用、各種パブリッククラウドでの利用にも対応しています。

仮想版でも 1 インスタンスあたり最大 100Gbps、コンテナ版では最大 180Gbps のスループットに対応し、キャリアグレードの性能を提供します。また、必要な帯域をプールで購入し、通信トラフィックに応じて帯域を柔軟にインスタンスに割り当てることができるライセンス体系も提供しており、ネットワーク機能の配置を最適化できます。

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ク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 : <http://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

©2021 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networks は米国およびその他の各国における 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_Solutions_for_ServiceProviders APR 2021