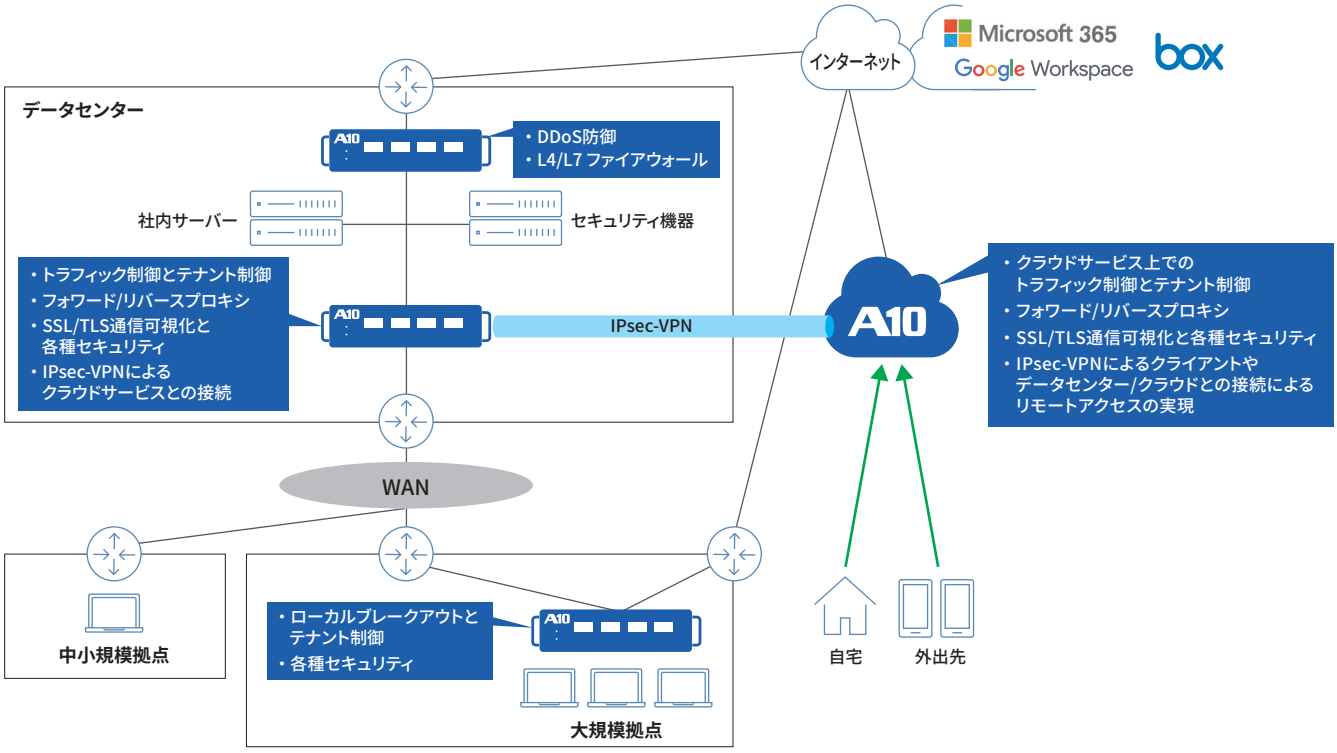
A10
Always Secure. Always Available.

企業・自治体情報セキュリティ対策向けソリューション

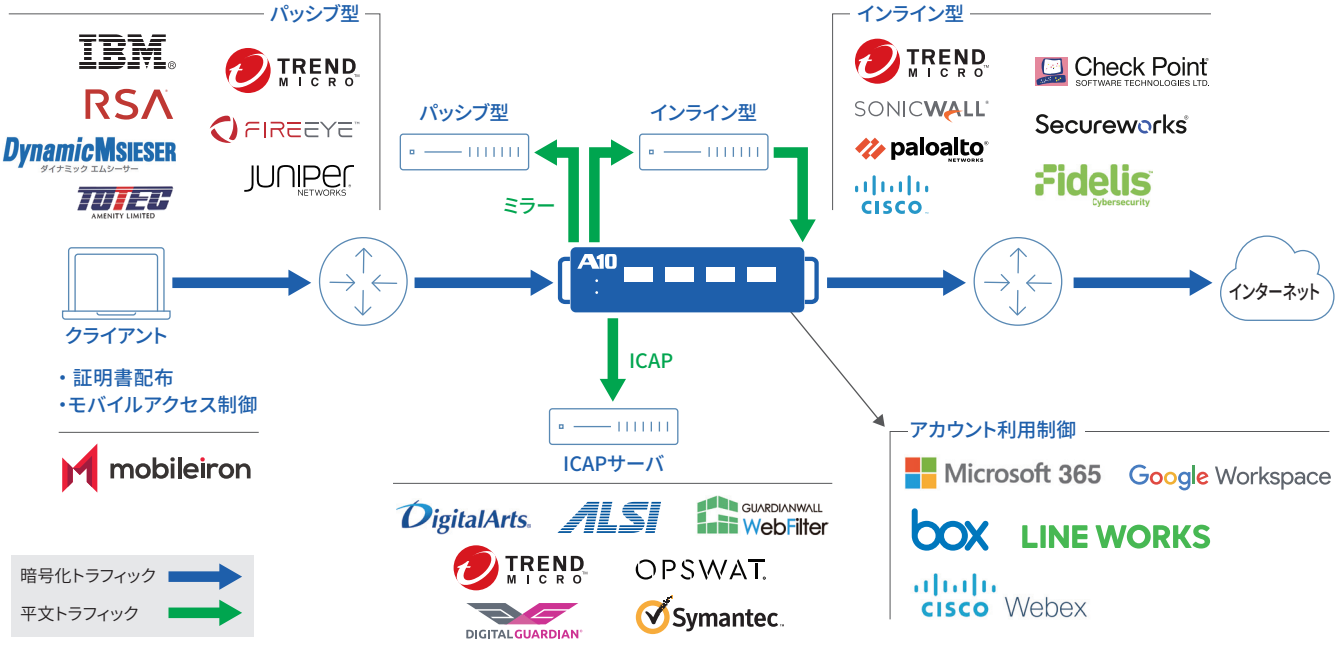
エンタープライズネットワーク向けソリューションマップ

データセンター／拠点／クラウドの各ポイントで通信トラフィックを最適化しセキュリティを強化



SSL/TLS通信可視化と連携ソリューション

SSL/TLS通信を高速に復号し多様なセキュリティ製品と連携、暗号化通信に隠れた脅威を検知し防御



Always Secure. Always Available.

快適なクラウドサービス利用と利用アカウント制御

A10 のクラウドアクセスプロキシソリューションにより、Microsoft 365 や Box などの SaaS を始めとするクラウドサービスの快適な利用を実現できます。SaaS の利用を開始すると、これまで組織内で閉じていた通信が全てインターネットに流れることから必要な通信セッション数が増大し、既存のプロキシサーバーやファイアウォールなどが通信のボトルネックとなり、十分な帯域があってもクラウドサービスの動作に影響を与えます。

Thunder CFW シリーズを導入しフォワードプロキシとして利用することで、クラウドサービスのトラフィックを識別して、ボトルネックとなる箇所をバイパスできます。クラウドサービスは基本的にドメイン名で定義されており、IP アドレスは頻繁に変化することからルーターやファイアウォール等でのトラフィック制御は困難ですが、Thunder CFW ではトラフィックに含まれるドメイン名を識別して通信を振り分けるため、適切にトラフィックを制御できます。データセンターと拠点を繋ぐ WAN がボトルネックになった場合には、拠点に Thunder シリーズを導入することで、クラウドサービス向け通信を直接インターネットに振り分けるローカルブレークアウトも実現できます。

また、情報漏えい防止の観点などから、組織内から個人アカウント等でクラウドサービスを利用されることを防ぐために、利用アカウントの制御（テナント制御）を行うことができます。SaaS 側でテナント制御の機能を提供しているものだけでなく、SSL/TLS 通信可視化を利用することで多様なクラウドサービスのテナント制御を実現できます。

認証・認可に基づく適切なアクセス制御

Thunder ADC/CFW シリーズは、リバースプロキシまたはフォワードプロキシとして動作し、Active Directory や 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を行えます。ユーザー情報や属性情報に応じてきめ細かくリソースへのアクセス制御を実現し、ユーザー情報を含めたアクセスログを記録できます。

組織内向けサービスの高速な配信と可用性の向上

さらに、Thunder ADC/CFW シリーズにより、データセンター内の組織内向けサービス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ます。Web アプリケーションファイアウォールや L4 ファイアウォールによるセキュリティの強化も実現できます。Harmony Controller を用いることでアプリケーションの利用状況やレイテンシも可視化でき、サービスの問題点などへの迅速で効率的な対処を可能にします。

暗号化された通信に対するセキュリティの強化

ネットワークトラフィックの大部分が HTTPS を始めとする SSL/TLS を用いた暗号化通信となっている一方で、多くのサイバー攻撃でも不正ファイルのダウンロードや情報の窃取に SSL/TLS 通信が利用されています。Thunder CFW シリーズで利用できる SSL/TLS 可視化（SSL インサイト）ソリューションにより、暗号化通信を高速に復号し、セキュリティ機器での高速な検査を実現できます。一度復号することでインライン型（ファイアウォールや IPS など）・パッシブ型（サンドボックスや標的型攻撃防御製品、SIEM、フォレンジック製品など）・ICAP 連携型（URL フィルタリングやウィルススキャン / コンテンツ無害化 / データ損失防止など）のセキュリティ機器で並行した検査ができ、通信遅延も最小に抑えることができます。SSL/TLS 可視化により、サブディレクトリ以下の情報やペイロードも含めた詳細なアクセスログの取得も可能です。

IPsec-VPN によるセキュアな通信の実現

Thunder CFW シリーズでは標準で IPsec-VPN を利用でき、PC 端末やモバイル端末の OS の標準機能である IPsec-VPN クライアント機能を利用することでリモートアクセス／リモートワークの環境を実現したり（Client-to-Site IPsec VPN）、データセンター間や IaaS などのクラウドサービスとの間を広帯域な IPsec-VPN で接続（Site-to-Site IPsec VPN）することができます。接続時にユーザーと端末の双方が認証され、低レイヤでの通信暗号化により、通信プロトコルを問わないセキュアな通信が実現できます。

ネットワークセキュリティの強化

Thunder CFW シリーズでは標準で高性能な L4 ステートフルファイアウォールを利用できます。また、パケットを検査することでアプリケーションを識別してトラフィック制御を行うことも可能です。送信元 / 宛先の情報やアプリケーションの情報に基づいた帯域制御やレートリミットも適用できます。また、URL のカテゴリを指定して通信トラフィックの制御（フォワードプロキシの制御や SSL/TLS 可視化の実施可否などの制御）を行ったり、URL レピュテーションスコアや IP アドレスレピュテーションに基づくトラフィック制御を行うことも可能です。

また、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。インターネットの出口に通常設置されるファイアウォールは帯域の大きくない DDoS 攻撃でも容易に停止させることができ、組織内からクラウドサービスの利用等が出来なくなってしまいます。オンプレミスでの DDoS 攻撃防御を行うことで、このような攻撃にも有効な防御を実現できます。

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：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

Part Number: A10_SB_Solutions_for_Enterprises APR 2021