ソリューションブリーフ

仮想化されたネットワーク上での暗号化通信に対する脅威検知・防御の強化とスケール性 / 高可用性の実現

トレンドマイクロの Virtual Network Suite™（TM VNFS）と A10 Thunder CFW の連携

課題：

- IoT におけるデバイス側からの脅威侵入とインターネット側からの脅威侵入を防ぐためのネットワークレイヤーでのセキュリティの強化
- SSL/TLS により暗号化された通信に潜む脅威への対応
- 大規模な通信に対するネットワークセキュリティのスケール性と高可用性

解決策：

不正な侵入行為・異常な通信・不正サイトへのアクセスなどのセキュリティ脅威に対する検知・防御機能を提供するトレンドマイクロ社の Trend Micro Virtual Network Function Suite（TM VNFS）と、SSL インサイト（可視化）機能および高度な負荷分散機能を有する A10 Thunder CFW との連携により、SSL/TLS 通信に隠れた脅威に対するセキュリティの強化と高いスケール性・高可用性を実現

メリット：

- 仮想化されたネットワークセキュリティ機能を提供する TM VNFS により、通信サービス利用者の通信サービスの利用状況（利用アプリケーション、利用デバイス、通信量など）やセキュリティの脅威状況に応じて必要なセキュリティ機能を適切なタイミングで提供可能に
- A10 Thunder CFW による SSL/TLS 通信の高速な復号 / 再暗号化により高い通信パフォーマンスを維持したまま、SSL/TLS 通信に対して低遅延で効率的なセキュリティ検査を実現
- 大規模なセッションを処理可能な A10 Thunder CFW による高度な負荷分散機能により、TM VNFS のスケール性と高可用性を実現

IoT（Internet of Things）時代のセキュリティとネットワーク仮想化

近年、パソコンやスマートフォンのような情報通信機器だけでなく、多くのモノがインターネットなどのネットワークに接続される、IoT 化が進んでいます。IoT 化を進めることにより、モノから得られる情報を活用した迅速なフィードバックに基づいて大幅な生産性の向上や新たなサービスの創出を実現できる一方で、ホテルのカードキーシステムがハッキングされて宿泊客が締め出されたり、公共の警報システムがハッキングされて警報が鳴り続けたり、電力システムへのサイバー攻撃で停電が発生したりする等、IoT を利用することによるセキュリティリスクも顕在化しています。全てのモノがインターネットに接続することで、あらゆるモノが脅威の対象となり、世界中からの攻撃にさらされ、影響はデジタル世界だけでなく物理世界にも及びます。ネットワークの各レイヤーを移動する IoT のデータを守るためには、デバイスに備わったセキュリティだけでなく、IoT システムに向けたデバイス側からの脅威侵入とインターネット側からの脅威侵入を防ぐためのネットワークレイヤーでのセキュリティも含めたフルレイヤーに渡るセキュリティが重要になります。

このような IoT 時代のセキュリティにおいては、従来の境界防御とエンドポイントセキュリティに留まらず、防御する IoT のユースケースに応じて、ネットワーク内に機能分散する形でサービスごとに必要なセキュリティ機能を動的に提供できることが効果的です。このような動的分散型のネットワークセキュリティを実現するためには、柔軟な設備設計が可能な SDN（Software Defined Network）/NFV（Network Function Virtualization）ベースの仮想化されたネットワークインフラが適しています。ソフトウェアで提供されるネットワーク機能を汎用のハードウェア上で利用することができるネットワークの仮想化は、企業ネットワークの柔軟性向上とコストパフォーマンス向上のためだけでなく、4G/5G のモバイルネットワークを始めとする通信インフラ事業者のネットワークでの活用が進んでおり、一般的なネットワークインフラに留まらず、今後の IoT サービスを支える基盤としての利用が進むと考えられます。

SSL/TLS 暗号化通信に潜む脅威

またセキュリティ強化の一環として、多様化するサイバー犯罪への対処や通信の盗聴、スヌーピングや改ざん、データの窃盗を防ぐために、パソコンやスマートフォンからの Web サイトへのアクセスを SSL（Secure Socket Layer）/ TLS（Transport Layer Security）により暗号化する流れが進んでおり、IoT デバイスとデータプラットフォームとのやり取りも同様に暗号化される傾向にあります。現状でも IoT デバイスとクラウドサービスを連携させる際にインターネットを通過するトラフィックにおいては、HTTP や MQTT を SSL/TLS 暗号化した HTTPS や MQTTS が用いられることが多く、また TLS のバージョン 1.3 は、IoT デバイスによる通信暗号化を想定して標準が策定されています。

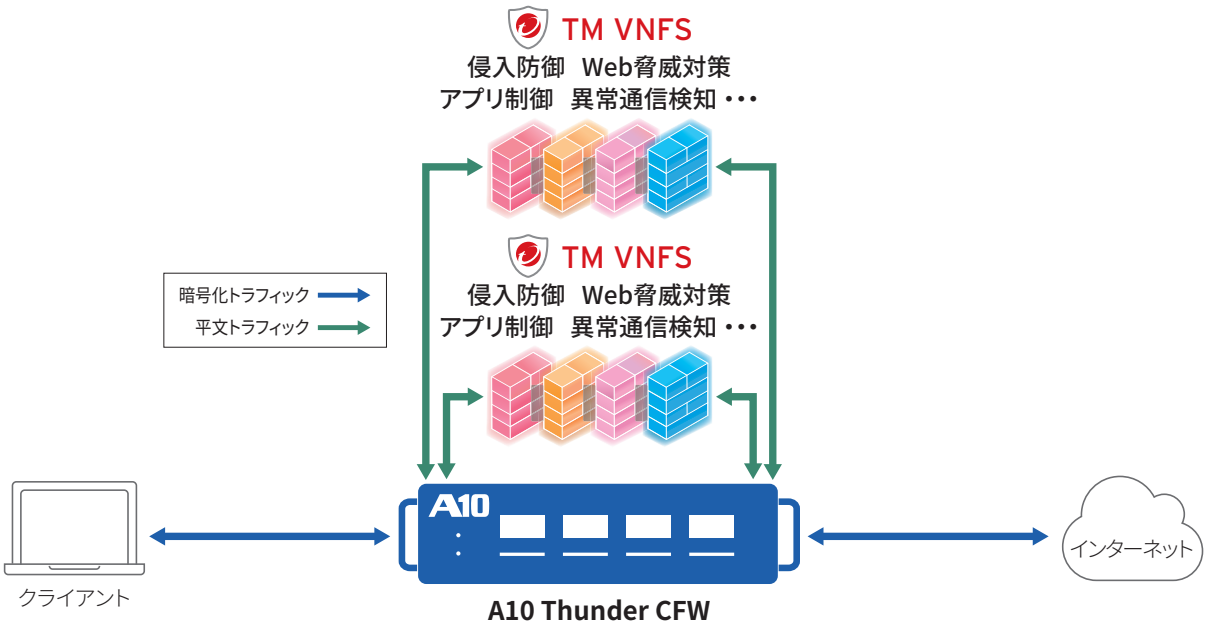

図1：TM VNFSとA10 Thunder CFWとの連携
（SSL/TLS通信の可視化によるセキュリティ強化とTM VNFSの負荷分散によるスケール性/可用性の向上）

その一方で、悪意のあるWebサイトもHTTPSなどで暗号化されていたり、暗号化通信を通じて端末にマルウェアが仕込まれたり、感染した端末から暗号化通信を利用して機密情報をアップロードさせるなど、SSL/TLS通信がサイバー攻撃の隠れ蓑や情報漏洩の抜け道として悪用されることが増えています。多くのネットワークセキュリティ機器ではSSL/TLS通信の復号と検査を行うための十分な性能や機能を持っておらず、SSL/TLS通信に隠れた脅威への対応が十分にできません。

NFV/クラウド向けネットワークセキュリティソリューション：Trend Micro Virtual Network Function Suite（TM VNFS）

トレンドマイクロ社のTrend Micro Virtual Network Function Suite（以下、TM VNFS）は、不正な侵入行為・異常な通信・不正サイトへのアクセスなどのセキュリティ脅威に対する検知・防御を始めとする細分化されたさまざまなネットワークセキュリティ機能を仮想マシンベースのソフトウェア上で提供します。セキュリティ脅威対策に加え、使用しているアプリケーションやデバイス情報を識別し、使用を許可するアプリケーションの通信を制御したり、GUIを用いて各種情報を可視化したりすることも可能です。IoTレピュテーション機能を用いてセキュリティ脅威への感染が疑われるIoTデバイスの情報を収集、当該デバイスからの通信を検知・ブロックすることもできます。ネットワーク上に配置されたTM VNFSのセキュリティ機能を用いることで、通信サービスの利用者のサービス利用状況（利用アプリケーション、利用デバイス、通信量など）や脅威状況に応じて必要なセキュリティ機能を適切なタイミングで利用者に提供することが可能です。

SSL/TLS通信に潜む脅威への対応

A10 Thunder CFWは、SSL/TLS通信に隠れた攻撃や未知の不正ファイル、URLに含まれる脅威を検出・分析するために、SSL/TLS通信を可視化するSSLインサイトソリューションを提供しています。SSLインサイトにより可視化された通信をTM VNFSと連携することで詳細な情報に基づく脅威検知を実現し、セキュリティを強化できます。

SSLインサイトを利用する際には内部ネットワークとインターネットの間にA10 Thunder CFWを設置します。A10 Thunder CFWはクライアントからみると透過型/明示型のプロキシサーバーとして動作します。SSL/TLS通信をインターセプトして復号した通信を、ミラーポートまたはインラインの通信を介してTM VNFSに送信して通信の内容を検査します。通信の流れは以下のようになります。（図1）

1. A10 Thunder CFWがクライアントから通信先のサーバーに向けたトラフィックをインターセプトしてSSL/TLS通信を復号し、復号した通信をTM VNFSに送信して脅威検知を実施
2. TM VNFSで検査された平文のトラフィックをA10 Thunder CFWが再暗号化し通信先のサーバーにフォワード
3. 通信先のサーバーはリクエストを受信し、レスポンスをクライアントに送信

4. A10 Thunder CFWが暗号化されたサーバーからのレスポンスをインターセプトし、復号した後TM VNFSに送信し検査
5. TM VNFSで検査された平文の通信を再暗号化しクライアントに送信

SSL/TLS通信の特性上、リクエストの復号とレスポンスの再暗号化のためには、A10 Thunder CFWとクライアントに同一の信頼できる証明書がインストールされている必要があります。A10 Thunder CFWには任意の証明書をインストールして利用できます。

SSL/TLS通信に含まれるリクエスト/レスポンスを平文でTM VNFSに渡すことで、これまでネットワークセキュリティ機能単体では十分に検査ができなかったSSL/TLS通信に対しても高度な脅威検知と防御を実現できます。クライアントとA10 Thunder CFWの間、およびA10 Thunder CFWと通信先サーバーとの間のコネクションは暗号化したまま保持され、なりすましやデータ窃盗は防止されます。

その他のA10 Thunder CFWによるSSLインサイトの特長とメリットは以下になります。

- 格段に優れた処理能力（SSL/TLSコネクション数とスループット）
- 全てのポートに渡るSSL/TLSトラフィックの復号
- L2/L3の多様なネットワーク構成に対応し、既存の環境に応じた柔軟な構成が可能
- 復号対象とするSSL/TLS通信の指定などが可能な詳細なポリシー設定

TM VNFSのスケール性と高可用性の実現

上記に加え、図1に示されているように、A10 Thunder CFWに搭載されている負荷分散機能を利用することで、複数のTM VNFSの利用と冗長構成を実現できます。これにより大規模なトラフィックに対するTM VNFSのスケール性を確保すると共に、万が一のTM VNFSの障害に対する高可用性を実現できます。A10 Thunder CFWの負荷分散機能により、それぞれのTM VNFSではL2のインラインで通信を検査すると共に、同じクライアントとサーバー間の通信が必ず同じTM VNFSを通過して検査される構成を実現できます。

A10 Thunder CFW自体の障害に対応するための冗長構成も可能で、システム全体としても高い可用性を実現できます。これらの機能は、SSL/TLS通信の可視化と併せて利用できます。

結論

多様な環境変化に柔軟かつ迅速に対応できるネットワークインフラを実現するためには、ネットワーク機能の仮想化が重要です。TM VNFSは、仮想化されたネットワークセキュリティ機能により、IoTシステムや通信事業者のインフラへの柔軟なセキュリティソリューションを提供します。TM VNFSをA10 Thunder CFWの提供するSSLインサイトソリューションと共に利用することで、SSL/TLS通信に隠れた脅威に対する有効な防御を実現できます。また、A10 Thunder CFWの提供する高度な負荷分散機能により、TM VNFSのスケール性と高可用性を併せて実現できます。

トレンドマイクロ株式会社について

トレンドマイクロ株式会社は、より安全な情報社会とお客様の未来を創造する、インターネットセキュリティのグローバルリーダー企業です。最先端の技術を駆使した革新的なセキュリティ対策製品を通じて、お客様の情報資産を守ります。

トレンドマイクロのソリューションは、クラウド上のセキュリティ技術基盤「Trend Micro Smart Protection Network™」に集約されたビッグデータと、グローバルに広がる脅威解析ネットワーク、および創業以来培われてきたセキュリティインテリジェンスによって支えられています。実装や管理がシンプルで、お客様の個々の環境にフィットしたソリューションを通じ、スマートな情報保護を実現します。守るべき情報資産に着目し、モバイル端末やエンドポイント、ゲートウェイ、サーバーおよびクラウド上の情報を多層的に守ります。

詳しい情報はホームページ（http://www.trendmicro.com）をご覧ください。

A10 Networks / A10ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、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

お問い合わせ：

A10ネットワークス株式会社

www.a10networks.co.jp
a10networks.co.jp/contact

トレンドマイクロ株式会社

www.trendmicro.com

東京本社
〒151-0053 東京都渋谷区代々木2-1-1
新宿マインズタワー
TEL.03-5334-3601（法人お問い合わせ窓口）
FAX.03-5334-3639

名古屋営業所
〒460-0002 愛知県名古屋市中区丸の内3-22-24
名古屋桜通ビル7F
TEL.052-955-1221　FAX.052-963-6332

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原3-4-30
ニッセイ新大阪ビル13F
TEL.06-6350-0330　FAX.06-6350-0591

福岡営業所
〒812-0011 福岡県福岡市博多区博多駅前2-3-7
シティ21ビル7F
TEL.092-471-0562　FAX.092-471-0563

Part Number: SB_TrendMicro_VNFS_and_A10　Nov 2020