SSL通信の可視化とTrend Micro Deep Discovery

SSLトラフィックに隠されたサイバー攻撃を検出

課題：

SSLトラフィックに隠されたマルウェアとサイバー攻撃を阻止するため、Trend Micro Deep Discoveryには暗号化トラフィックを完全に可視化する機能が必要です。

ソリューション：

A10 Thunder ADCをトレンドマイクロのお客様が使用すると、SSLトラフィックをインターセプトおよび復号化して、Trend Micro Deep Discoveryに転送して脅威を検出して阻止できるため、防御におけるSSLの盲点が排除されます。

利点：

- SSL暗号化トラフィックを高速で復号化して脅威を特定
- ローカルとグローバルの脅威情報とカスタムのサンドボックスを組み合わせ、データ侵害とそれに伴うコスト上昇を防止
- 高度なフォレンジックとIOC（情報オブジェクトクラス）情報共有によるインシデントへの迅速な対応
- クラス最高の負荷分散とクラスタリングによるアップタイムと規模の最大化

A10 Networksとトレンドマイクロは、コラボレーションを通じて、パフォーマンスを犠牲にせずに暗号化トラフィックに隠された高度な標的型攻撃を検出しブロックするソリューションを実現しています。アプリケーションデリバリーコントローラーの製品ラインA10 Networks® Thunder® ADCがSSLトラフィックをインターセプトおよび復号化した後、Trend Micro Deep Discoveryは高度な脅威を検出しブロックします。このコラボレーションによって暗号化トラフィックを含むすべてのネットワークアクティビティを可視化して、攻撃と侵入を検出することが可能です。また、コンピューター、モバイルデバイスおよび仮想環境をマルウェアから防御し、セキュリティで保護された安全なユーザーエクスペリエンスを提供できます。

課題

暗号化が作り出す防御の盲点

第三者が機密情報にアクセスするのを防ぐために、データを暗号化するアプリケーションはますます増えています。このようなアプリケーションの所有者は、SSL（Secure Sockets Layer）とSSLを継承するTLS（Transport Layer Security）を活用してWebトラフィックを暗号化しています。現在、人気のあるWebサイトの多くでは、すべてのリクエストと応答が暗号化されています。2016年までに、北米のインターネットトラフィックの3分の2は暗号化される見込みです。[1]

アプリケーションとデータを保護するために、組織は暗号化されたすべてのトラフィックを検査する必要があります。残念ながら、多くのセキュリティデバイスでは暗号化トラフィックは検査できません。また、SSLの復号化が可能なわずかなデバイスも帯域幅のニーズの増加に追いつくことができません。そのため、企業の防御に危険なセキュリティギャップと盲点が作り出されています。

A10ネットワークスのSSLインサイトソリューション

暗号化トラフィックに隠された脅威の検出

A10はトレンドマイクロとの連携を通じて、パフォーマンスを犠牲にせずに暗号化トラフィックに隠された攻撃を効率的に防御しています。Trend Micro Deep Discoveryを使用すると、最新の巧妙な標的型攻撃をリアルタイムで検出、分析および対応できます。Deep Discoveryは、すべてのトラフィックとプロトコルを全方向から監視して、あらゆるタイプの標的型攻撃を検出することのできるネットワークアプライアンスです。

Trend Micro Deep DiscoveryをA10 Thunder ADCと連携させて導入することにより、高度な脅威やマルウェアを可視化して制御することが可能です。A10 Thunder ADCでSSLとTLSのトラフィックを復号化する一方、トレンドマイクロのネットワークセキュリティソリューションではすべての通信、ユーザー、アプリケーション、デバイスを検査して、脅威を特定します。

[1]「Global Internet Phenomena Spotlight, Sandvine」2015年

A10 Thunder ADCは、業界をリードするハイパフォーマンスなアプリケーションデリバリーコントローラーの製品ファミリーです。A10のSSLインサイトテクノロジーが統合されたThunder ADCでは、SSLトラフィックを復号化して、Trend Micro Deep Discoveryで検査します。検査後、トラフィックは再度暗号化されて、目的の宛先に転送されます。A10のSSLインサイトテクノロジーでは、Trend Micro Deep Discoveryアプライアンスのネットワーク保護機能を100%活用でき、CPUを集中的に使用するSSL暗号化と復号化のプロセスを実行する必要はありません。

Thunder ADCは、SSLトラフィックをインターセプトするトランスペアレントなSSLプロキシとして機能します。クライアントとサーバー間の暗号化された端末間のセッションでは、クライアントのネットワークの保護された環境でのみ復号化されます。

負荷分散機能の統合によるセキュリティの拡張

負荷分散機能を備えたThunder ADCでは高可用性と拡張性も提供されるため、複数のTrend Micro Deep Discoveryアプライアンスを導入できます。また、トラフィック処理の増加に対応するため、セキュリティブレードを増設してセキュリティを簡単に拡張できます。

ラウンドロビン、重み付けラウンドロビン、最少コネクションと最速応答時間を含め、多様な負荷分散のアルゴリズムをサポートしているThunder ADCは、Trend Micro Deep Discoveryのセキュリティ機能を拡張し、帯域幅のニーズの増加にも対応できます。

境界とデータセンター保護のシナリオ

Trend Micro Deep DiscoveryとA10 Thunder ADCには、多様な使用例とセキュリティニーズをサポートする豊富な導入オプションが用意されています。企業が所有するサーバーの受信トラフィックと社内ユーザーからの送信トラフィックの両方をTrend Micro Deep DiscoveryとA10 Thunder ADCの1組のアプライアンスで保護できるため、効率を最大化します。

典型的なシナリオでは、1組のThunder ADC高可用性アプライアンスでSSLトラフィックを復号化して、多層保護のためにTrend Micro Deep Discoveryアプライアンスに転送し、その後、Thunder ADCで再度暗号化します。図1の通り、SSLの各セッションは以下のように処理されます。

1. A10 Thunder ADCでSSLトラフィックが復号化され、1台または複数のTrend Micro Deep Discoveryアプライアンスに送信
2. Trend Micro Deep Discoveryアプライアンスでそのトラフィックの不正なアクティビティが検査され、セキュリティポリシーに違反しないことが確認された場合はA10 Thunder ADCに返送
3. A10 Thunder ADCでデータが復号化され、目的のサーバーまたはユーザーに送信

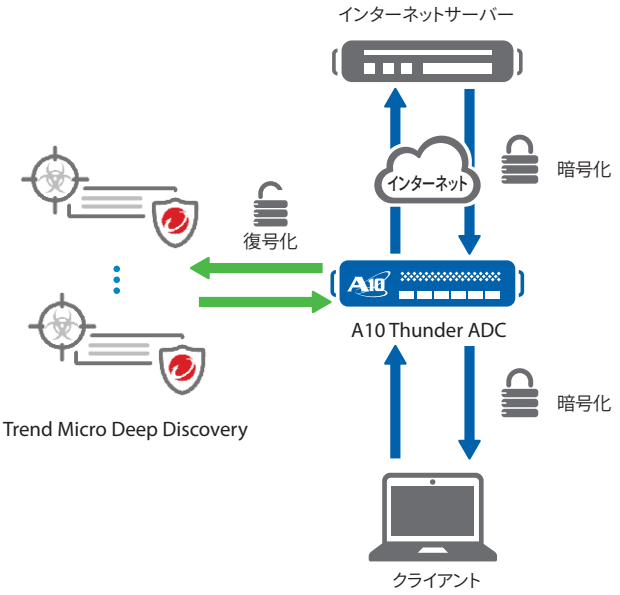

図1：データセンター内でセグメント化されたネットワークに設置されたTrend Micro Deep DiscoveryアプライアンスとA10 Thunder ADCの連携。復号化トラフィックを直接サーバーに送信して、アプリケーションサーバーの負荷を分散することも可能

強力なSSLセキュリティプロセッサーによる高パフォーマンス

SSL通信の最初のハンドシェークはSSL暗号化の中でも最も多くCPUを消費します。セッションにおけるバルクデータの暗号化と復号化もCPUにとって大きな負荷になりますが、程度はそれほど高くありません。A10 Thunder ADCのアーキテクチャーでは、多数の保護された接続を同時に管理できます。

64ビットのA10 Networks Advanced Core Operating System（ACOS®）で強化されたThunder ADCではリニアな拡張性が提供されるため、汎用CPUと専用セキュリティプロセッサーのパフォーマンスが最大化されます。すべてのアプライアンス（ハードウェア、ハイブリッドまたはローカル）でSSLオフロードがサポートされますが、専用の高パフォーマンスセキュリティプロセッサーを含むモデルを選択すると、多数のSSLセッションの同時管理で最高のパフォーマンスが得られます。

機能と利点

SSLインサイトテクノロジーとTrend Micro Deep Discovery：

- SSL暗号化トラフィックを高速で復号化して脅威を特定
- リアルタイムの状況認識とフルスタックの可視化の統合により、高コストのデータ侵害を防止
- コンピューター、モバイルデバイス、仮想環境をマルウェアから保護
- クラス最高の負荷分散とクラスタリングによるアップタイムと拡張性の最大化

A10 Thunder ADCには強力なSSLインサイト機能が標準装備されており以下の利点をもたらします。

- 暗号化トラフィックを含むネットワークアクティビティを完全に可視化することにより、攻撃と侵入を検出して、セキュリティで保護された安全なユーザーエクスペリエンスを提供
- A10 Thunder ADCを負荷分散と復号化の集中ポイントとして使用して、SSLトラフィックをインターセプトして、セキュリティ分析、情報漏えい防止（DLP）、脅威保護、侵入検知アプライアンスなどの複数のセキュリティデバイスに検査のために送信
- トラフィックをバンキングや医療のサイトへの通信など、機密のWebサイトのトラフィックを迂回させ、機密データの復号化を回避（オプション）
- 投資を将来も活用できるよう、SSLの使用の拡大と暗号鍵の鍵長の増加に対応

まとめ – A10とトレンドマイクロの連携による暗号化トラフィックに隠された攻撃からの保護

ネットワークを移動するデータを暗号化するアプリケーションが増加し、SSLによって企業の防御に危険な盲点が作り出されています。A10 Thunder ADCとTrend Micro Deep Discoveryを組み合わせることで、容易な導入と優れた拡張性により暗号化トラフィックのインターセプトと保護を可能にするソリューションを活用できます。A10 Thunder ADCと、Trend Micro Deep Discoveryが提供するセキュリティソリューション間の相互運用性はA10が検証して、有効性を確認しています。

A10のSSLインサイトテクノロジーによって、以下が可能になります。

- A10の64ビットAdvanced Core Operating Systemと専用セキュリティプロセッサーによる、パフォーマンス、可用性、拡張性の最大化
- A10 Thunder ADCとTrend Micro Deep Discoveryなどの高度なネットワークセキュリティプラットフォームの統合による、サイバー攻撃とマルウェアの特定と阻止
- 統合されたリアルタイムの状況認識と優れたセキュリティ自動化機能の活用により、ネットワークを高度な脅威から保護

次のステップ

詳細については、A10の営業窓口にお問合せいただくか、
http://www.a10networks.co.jp/products/thunderseries/thunder-adc.html
をご覧ください。

トレンドマイクロについて

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。企業が持つデータセンターやクラウド資源、および、エンドユーザを保護し、巧妙な標的型攻撃の脅威から情報資産を守ります。

詳しい情報はホームページ（http://www.trendmicro.co.jp）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）はアプリケーションネットワーキング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、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-19152-JA-01
Mar 2016