ソリューションブリーフ

SSL/TLS通信に隠れた脅威の検知と不正サイトへのアクセスのブロック

トレンドマイクロのDeep Discovery Inspector/TippingPoint/Deep Discovery AnalyzerとA10のSSLインサイトソリューションの連携

課題：

- HTTPSをはじめとするSSL/TLS通信を悪用した脅威の検知とそれを実現する高速なSSL/TLS通信の可視化と検査
- 社内クライアントの不正な活動や通信の検知とアクセス制御
- SSL/TLS通信に含まれる未知の不正ファイルやURLの解析と脅威防御

解決策：

A10 Thunder CFWによるSSLインサイト（可視化）ソリューションと、トレンドマイクロ社製品との連携により、SSL/TLS通信に隠れた脅威に対して以下の防御を実現

- 標的型サイバー攻撃対策製品Deep Discovery Inspector（DDI）で検査し脅威を検知。DDIで検知された脅威情報に基づき、A10 Thunder CFWでクライアントからの脅威のあるURLへのアクセスをブロック
- 次世代型IPS製品TippingPoint Threat Protection System（TippingPoint）による不正な活動や通信の検知と脆弱性攻撃への防御
- サンドボックス製品Deep Discovery Analyzer（DDAN）による未知の不正ファイルやURLの解析と脅威防御を実現可能

メリット：

- 大規模なセッションを処理可能な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、一度の復号処理でDDI、TippingPoint、DDANでの解析を併せて実施でき低遅延で効率的な検査を実現
- DDIにより、SSL/TLS通信に隠れた標的型攻撃やゼロデイ攻撃を動的に検知し、A10 Thunder CFW上で不正URLへのアクセスをブロックして脅威の拡大を阻止
- TippingPointによりSSL/TLS通信に隠れた脆弱性攻撃や不正な活動・通信の検知と防御を実現、DDIとの連携も可能
- DDANによりSSL/TLS通信に隠れた未知の不正ファイルやURLの解析を実施し、脅威防御を実現

暗号化の加速とSSL/TLS通信に潜む脅威

近年、多様化するサイバー犯罪への対処や情報機関からの盗聴、スヌーピングや改ざん、データの窃盗を防ぐために、通信データのSSL/TLSによる暗号化の流れが進んでいます。従来はクレジットカードでの取引やユーザーログイン情報など、機密性の高いデータ通信のみが暗号化されていましたが、サーバー証明書の発行が容易になったことに加え、Webサイトの HTTPS対応が検索ランキングに反映されることやブラウザにWebサイトの暗号化への対応状況が表示されるようになったこと、多くのクラウドサービスがHTTPSでの接続を前提としていることなどにより、現在では通信の大部分がSSL/TLSにより暗号化されています。

その一方で、悪意のあるWebサイトがHTTPS化されていたり、HTTPSポータルサイトに表示される広告にマルウェアが仕込まれたり、HTTPS通信を利用するSNSやクラウドストレージ経由でボット化したクライアントへの指令を行ったりするなど、SSL/TLS通信が情報漏えいの抜け道やサイバー攻撃の隠れ蓑として悪用されることも増えてきています。日々継続して新しくなるサイバー攻撃の手法に追従し、企業のセキュリティを担保するにはSSL/TLS通信に隠れた脅威の対策が必須となっています。

しかし、従来のセキュリティ機器の多くは暗号化トラフィックを検査できず、SSL/TLS通信を復号し検査できるセキュリティ機器も、多くの場合急増するSSL/TLS通信量のペースに追いつく性能を持っていません。Ponemon Institute社によるレポート（*1）では、暗号化通信の検査が行えない主な理由として、「暗号化通信を検査可能なセキュリティ機器がない」「リソースが不十分」「通信パフォーマンスの低下」の3点が挙げられています。

SSL/TLS通信の可視化：SSLインサイトソリューション

A10 Thunder CFWで提供するSSLインサイトソリューションを利用することで、SSL/TLS通信に隠れた脅威を可視化し、通信パフォーマンスを落とすことなく、セキュリティ機器での脅威検知と防御を実現できます。SSLインサイトソリューションはクライアントとインターネット間のHTTPS通信をはじめとするSSL/TLS通信をインターセプトし高速に復号します。復号したトラフィックをセキュリティ機器に送ることで、通信データに含まれる脅威の検査と分析をハイパフォーマンスに実現できます。トラフィックの分析のために復号された通信データは再暗号化され、目的のアドレスに転送されます。

A10 Thunder CFWによるSSLインサイトを導入する際には、Thunderアプライアンスを自組織の内部にあるクライアントとインターネットの間に設置する必要があります。復号して平文化した通信データはインライン型・パッシブ型のセキュリティ機器に転送して検査することが出来るとともに、ICAPを通じて外部のICAPサーバーとの連携を行うことができます。

*1 Hidden Threats in Encrypted Traffic: A Study of North America & EMEA, Ponemon Institute

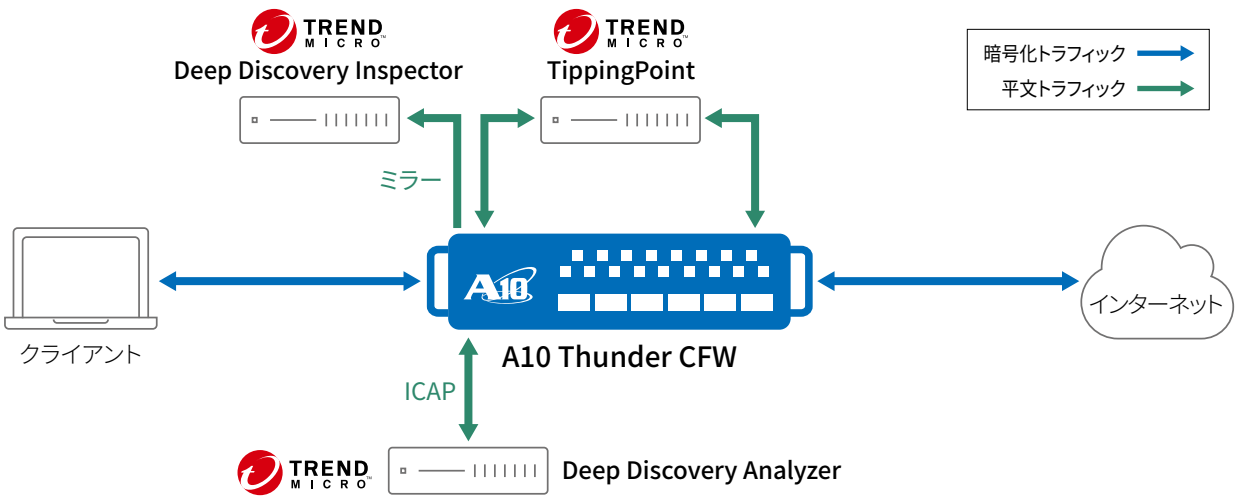

図1：A10 Thunder CFWによるSSLインサイトソリューションと各種トレンドマイクロ製品との連携

SSL/TLS通信に隠れた脅威の検知と不正サイトへのアクセスのブロック

A10 Thunder CFWは、SSL/TLS通信に隠れた巧妙な標的型攻撃や脆弱性攻撃、未知の不正ファイルやURLに含まれる脅威を検出・分析するために、トレンドマイクロ社の標的型サイバー攻撃対策製品DDIや次世代型IPS製品TippingPoint、サンドボックス製品DDANと連携できます。SSLインサイトソリューションにより復号したSSL/TLS通信をDDI/TippingPoint/DDANで検査することで、通信パケットに含まれる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。

トレンドマイクロ社のDDIは、通信機器のミラーポートに接続され、組織のネットワーク内部の全方位の通信を検査し、標的型攻撃やゼロデイ攻撃をネットワーク上の振る舞いを多面的に分析することでパターンファイルだけでは検出できないような攻撃も見つけ出すことができ、IT管理者が早期に対処することで被害の深刻化を防ぐことができます。検出した脅威について、重要なセキュリティ情報・警告・レポートをIT管理者に提供します。TippingPointは脆弱性攻撃をインラインで守る次世代型IPSで、企業内におけるネットワーク接続デバイスを対象に、既知の脆弱性やゼロデイ脆弱性をネットワーク領域で防御します。脆弱性そのものを保護する仮想パッチや、IPアドレス/DNSドメイン/URLのブラックリストによる不正な通信のブロック、マルウェアの不正な活動や通信をブロックする機能を持ちます。DDANはデスクトップに類似した仮想環境であるサンドボックスを構築し、未知の不正ファイルやURLを仮想環境上で実行・解析し不正なアクセスをブロックすることもできます。サンドボックスのカスタマイズにも対応し、トレンドマイクロ社の他のセキュリティ製品との連携により高度な検出・解析・防御を提供できます。

企業の内部にあるクライアントとインターネットの間に設置したA10 Thunder CFWは、クライアントからみるとプロキシサーバーとして動作します（透過型で配置することもできます）。A10 Thunder CFWはSSL/TLS通信をインターセプトし復号した通信を、ミラーポートを通じてDDIに、インラインの通信を介してTippingPointに、ICAPを通じてDDANに送信します。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、SSL/TLS通信を復号し、ミラーポートを通じてDDIに送信し、DDIで脅威検知を実施。並行して平文の通信をインラインで配置されたTippingPointに通すことで脅威検知と制御を実施し、ICAPを通じてDDANに平文の通信を送信し、トラフィック検査と制御を実施
2. 平文化されたSSL/TLSトラフィックをA10 Thunder CFWが再暗号化し通信先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DDI/TippingPoint/DDANに送信し検査
5. 復号された通信を再暗号化しクライアントに送信

※ HTTPなどの平文通信の場合は復号せずにそのままDDI/TippingPoint/DDANに送信

SSL/TLS通信に含まれるリクエスト/レスポンスを平文でDDI/TippingPoint/DDANに渡すことで、これまで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。また、一度の復号でDDI/TippingPoint/DDANでの効率的な検査を実現でき、かつ復号/再暗号化による通信の遅延を最小化することができます。

TippingPointやDDANとの連携では脅威が検知された不正な通信をブロックすることができますが、DDIの持つ「脅威インテリジェンスの共有」機能を利用することで、検出された脅威URLの情報をA10 Thunder CFWと連携し、クライアントからの脅威のあるURLへのアクセスをA10 Thunder CFW上でブロックすることもでき、攻撃に対する被害拡大の阻止につながります。また、DDIの情報をTippingPointと連携してTippingPointで不正なURLへのアクセスをブロックしたりすることもできます。これらにより、SSL/TLS通信に含まれる脅威の検知だけでなく、検知した脅威へのアクセス制御のアクションも自動化できます。

上記に加え、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DDI/TippingPoint/DDANの利用と冗長構成も可能です。A10 Thunder CFW自体の冗長構成も可能であり、この連携ソリューションにより高可用性とスケーラビリティをともに実現できます。
その他の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SSL/TLSコネクション数の処理能力とスループット
- 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
- 復号の対象とするSSL/TLS通信の指定などが可能な詳細なポリシー設定

結論

多くのトラフィックのSSL/TLS暗号化が進むにつれ、SSL/TLS通信が企業の防御にとって危険な盲点となりつつあります。高速なSSL/TLS通信の可視化を実現できるA10 Thunder CFWの提供するSSLインサイトソリューションを、トレンドマイクロ社のDDI/TippingPoint/DDAN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。

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）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、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ています。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

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

お問い合わせ：

Part Number: SB_TrendMicro_DDI_and_A10 Nov 2019