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
- 検知された脅威に基づく、社内クライアントのアクセス制御（脅威となるURLへのアクセスのブロック）

解決策：

A10 ThunderのSSLインサイトソリューションによりSSL/TLS通信を高速に可視化（復号）し、トレンドマイクロ社の標的型サイバー攻撃対策製品Deep Discovery Inspector（DDI）で検査することで、SSL/TLS通信に隠れた脅威を検知。DDIで検知された脅威情報に基づき、A10 Thunder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

メリット：

- 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サンドボックスや脅威情報、ネットワーク上の振る舞いから動的に検知
- 大規模なセッションを処理可能なA10 ThunderによるHTTPS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
- DDIで検知した脅威情報に基づき、A10 Thunder上で不正URLへのアクセスをブロックすることで、脅威の拡大を阻止

SSL/TLSによる暗号化の流れと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へ影響するようになったことやブラウザに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2016年のレポート[*1]では、36%の組織しか暗号化通信の検査を行っておらず、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ネットワークスのA10 Thunderシリーズで利用できる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することができます。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で実現できます。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

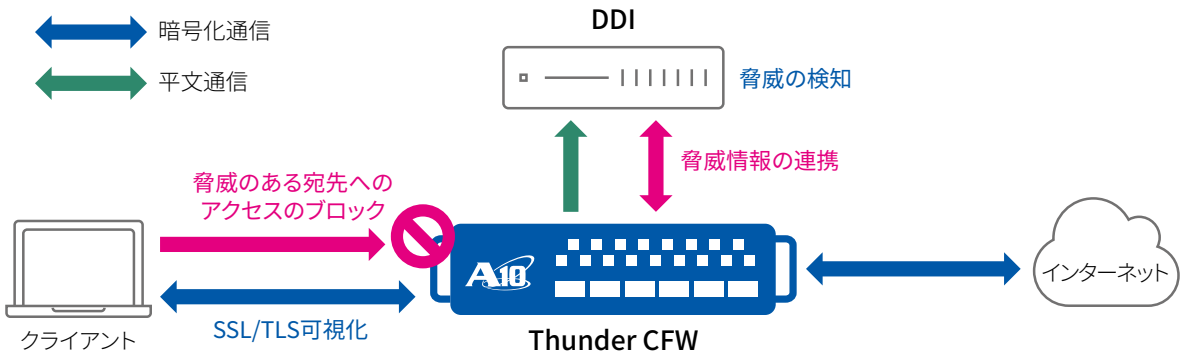

図1：A10 ThunderによるSSLインサイトソリューションとDeep Discovery Inspector（DDI）との連携

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ネットワークスのSSLインサイトと、トレンドマイクロのDeep Discovery Inspectorとの連携

A10 Thunderは、SSL/TLS通信に隠れた巧妙な標的型攻撃を検出・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Deep Discovery Inspector（DDI）と連携することができます。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で検査することで、通信パケットに含まれるより詳細な情報に基づいた脅威検知を実現し、SSL/TLS通信に対する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、世界中の主要な組織と政府機関の要件を満たすために開発された脅威管理ソリューションで、気づくことが難しい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から見つけ出し、早期に対処して被害の深刻化を防ぐことができるように設計されています。攻撃の初期段階から外部への通信に至る一連の攻撃フェーズにおいて、不正なファイルや通信の検知に加え、管理ツールを悪用した攻撃まで発見します。管理者権限を奪取された上で実行されるアクションなどを多面的に分析して異常を検出したり、サンドボックスと通信やファイルの振る舞いなどからパターンファイルだけでは検出できない攻撃を検出したりできます。利用者の環境により近いカスタムサンドボックスも利用可能です。検出した脅威については、重要なセキュリティ情報・警告・レポートをIT管理者に提供できます。通信機器のミラーポートに接続することで、ネットワークに影響を与えない形での導入ができます。

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シリーズは、クライアントから見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可能です。A10 ThunderはSSL/TLS通信をインターセプトし、SSL/TLS通信を復号して、ミラーポートを通じてDDIに平文で送信します。SSL/TLS通信の流れは以下のようになります。（図1）

1. A10 Thunder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
2. 平文化されたSSL/TLSトラフィックをA10 Thunderが再暗号化し通信先サーバーにフォワード
3. 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、復号した後ミラーポートを通じてDDIに送信
5. 復号された通信を再暗号化しクライアントに送信

※ 平文通信の場合は復号せずにそのままミラーポートを通じてDDI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クライアントがA10 Thunderを信頼する必要があるため、A10 Thunderにはクライアントが信頼できる証明書がインストールされていなくてはなりません（または、クライアント側にA10 Thunderと同じ証明書が信頼できる証明書としてインストールされている必要があります）。Thunderには任意の証明書をインストールして利用することができます。

SSL/TLS通信に含まれるリクエスト/レスポンスを平文でDDI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を実現できます。クライアントとA10 Thunderの間、およびA10 Thunder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るため、なりすましやデータ窃盗は防止されます。

上記に加え、A10 Thunder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の利用と冗長構成も可能です。A10 Thunder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。

不正サイトへのアクセスのブロック

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と連携することが可能です。この連携を用いることで、クライアントからの脅威のあるURLへのアクセスをA10 Thunder上でブロックすることができ、攻撃に対する被害拡大の阻止につながります。

この連携は、DDIが自身の上で公開する脅威インテリジェンスの情報をA10 Thunderが定期的にポーリングし、脅威URLがリストされたらそれを読み込んでA10 Thunder上のURLリストを更新することにより実現されます。A10 Thunder上で該当のURLリストに対するアクセス制御ポリシーを事前に設定しておくことで、該当URLリストに対するアクセスのドロップやアクセスログの取得が可能になります。DDI上で脅威インテリジェンスの変更が行われると、動的にその情報に追随します。これにより、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までを自動化できます。

DDIはさらに他のトレンドマイクロ社の製品と連携し、エンドポイントでの検知・ブロック・隔離なども実現できます。これらとの併用により、エンドポイントだけでの検知が難しい攻撃に対しても有効な防御を実現できます。

特長とメリット

A10 ThunderシリーズによるSSLインサイトソリューションとDDIの連携ソリューションの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（1台で最大25Gbps、2台で最大50Gbps）
- 全てのポートに渡るSSL/TLSトラフィックの復号
- 1度の復号でDDI以外にもパッシブ型・インライン型・ICAPサーバー型の複数のセキュリティ機器での検査が可能
- 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
- SSL/TLS通信に隠れた標的型攻撃やゼロデイ攻撃に対する、ネットワーク上の振る舞いやサンドボックスを用いた高度な脅威検知の実現
- 複数のDDIへの復号データの送信と負荷分散と冗長化
- DDIが検知した脅威に基づくA10 Thunderでの動的なアクセスブロックや、他のトレンドマイクロ製品との自動連携によるセキュリティの強化

結論

多くのトラフィックのSSL/TLSによる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シリーズの提供するSSLインサイトソリューションを、高度な攻撃やゼロデイ攻撃に対する検知が可能な標的型サイバー攻撃対策製品であるDDI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、DDIで検知された脅威URLの情報をA10 Thunderに連携して動的にアクセスを制御することで、より効果的にセキュリティを強化できます。

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 June 2019