SSL/TLS 通信に隠れた既知および未知の脅威検知

Juniper Advanced Threat Prevention 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 通信を悪用したネットワーク上の脅威検知
- 検知された脅威に対するリスク分析や優先順位付けと迅速な対応

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）
- Juniper ATP の先進的な分析とリスク分析により、SSL インサイトソリューションで可視化（復号）された SSL/TLS 通信内の脅威を検知し優先順位付け

メリット：

- Juniper ATP と A10 Thunder の組み合わせにより、SSL/TLS 通信に隠れた脅威を振る舞い検知サンドボックス、機械学習機能、レピュテーションなどを用いて検知
- 大規模なセッションを処理可能な A10 Thunder により HTTPS 通信を高速に復号 / 再暗号化し、高い通信パフォーマンスを維持

SSL/TLS 通信に潜む脅威

近年、データの盗聴・改ざん・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。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から、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、SSL/TLS により通信内容が暗号化されることから、情報漏えいの抜け道やサイバー攻撃の隠れ蓑として SSL/TLS 通信が悪用されることも増えており、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、従来のネットワークセキュリティ機器のうち、通信をミラーポートで検査するものは、SSL/TLS による暗号化トラフィックを検査できず、HTTPS 通信などに対しては宛先のチェックや通信の振る舞いなどを用いた検査に留まり、通信内容そのものを確認することができません。

SSL/TLS 通信を可視化する A10 の SSL インサイトソリューションと Juniper Advanced Threat Protection の連携

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の精度を高めることができます。このソリューションを導入する際には、A10 Thunder アプライアンスを組織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。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、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・ICAP サーバー型のセキュリティ機器に転送して検査することができ、通信データに含まれる脅威の検査と分析を高精度で実現できます。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。

この SSL インサイトソリューションと連携できるパッシブ型のセキュリティ機器として、Juniper Networks 社の Advanced Threat Protection（Juniper ATP）があります。SSL インサイトにより可視化された通信をミラーポートで Juniper ATP に送ることで、SSL/TLS 通信に隠れた脅威の検知をより高精度に行うことができるようになります。（図 1）

Juniper ATP はサンドボックス、機械学習、SIEM の機能を統合したセキュリティソリューションです。自らが提供するセンサー（Collector）だけでなく多様なサードパーティ製品のログを統合的に収集することができ、ふるまい検知サンドボックス・静的検知・レピュテーションに加えて機械学習機能を持つことで、既知の脅威だけでなく未知の脅威に対しても高い検知率と低い誤検知率を実現しています。自動的にマルウェアの感染範囲を特定し、分析結果を基づき自社製品だけでなくサードパーティ製品に対しても防御ポリシーを自動的に適用することができ、検知された脅威に対する迅速な対応を実現します。

Juniper ATP はミラーポートで通信を検査することから、通常は HTTPS を始めとする SSL/TLS 通信を復号できず、通信内容を完全に検査することができません。SSL/TLS 通信に潜む脅威を検知するためには、図 1 のように SSL/TLS 可視化ソリューションとの連携が必要になります。

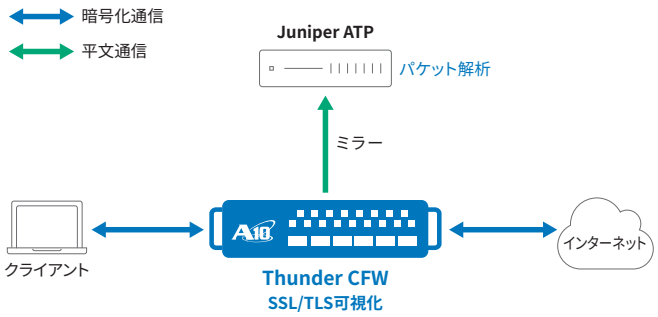

図1：A10 Thunderによる SSL インサイトソリューションと Juniper Advanced Threat Protection（ATP）との連携

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Juniper ATP に復号した通信を送信します。

SSL/TLS 通信の流れは以下のようになります。

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 Juniper ATP に送信し、Juniper ATP が脅威の検知を実施
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 Juniper ATP 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
   ※HTTP などの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 Juniper ATP 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るか、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 Juniper ATP 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、特に暗号化通信に含まれるマルウェアのダウンロードやC2サーバとの通信などに対し、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。

1台のThunderから複数の Juniper ATP に平文をミラーして検査することも可能です。一度復号するとミラーポートだけでなくインライン型のファイアウォールなどのセキュリティ機器にも復号した通信を送ることができるため、サードパーティ製品から Juniper ATP が得られるログの高度化も可能になります。また、Thunder 自身を冗長化して可用性を高めることもできます。

その他のA10 Thunderによる SSL インサイトと Juniper ATP 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
- 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
- Juniper ATP が検知した脅威に基づく、セキュリティ製品との自動連携によるセキュリティの強化

Juniper Networks について

ジュニパーネットワークスは、人々のつながり方、働き方、生活に変革をもたらす製品、ソリューション、サービスを通じて、マルチクラウド時代に伴うネットワークの複雑性に挑戦します。セキュアで自動化されたマルチクラウド環境への移行プロセスを簡素化することで、世界をつなぐAIドリブンネットワークを実現します。ジュニパーネットワークスに関する詳細な情報は、以下をご覧ください。
http://www.juniper.net/jp/

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

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: A10_SB_Juniper_and_A10 Apr 2020