ソリューションブリーフ

高機能ネットワークフォレンジックサーバによるSSL/TLS通信の解析

トーテックアメニティのNetRAPTORとA10のSSLインサイトソリューションの連携

SSL/TLS通信の増大とセキュリティの盲点

近年、Webアクセスなどを中心に第三者からの通信傍受を防ぎ安全な通信経路を確保するために、SSL/TLSを用いた通信経路の暗号化が広く行われるようになってきています。サーバ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。

一方で、SSL/TLS通信で保護される通信の内容は組織のネットワーク管理者でも確認できず、SSL/TLS通信を通じたデータの漏洩やサイバー攻撃を検知することができません。通信パケットを記録し、情報セキュリティインシデント発生時の原因究明を行うことを目的としてネットワークフォレンジック製品を利用していても、SSL/TLS通信の詳細を確認できず、情報セキュリティインシデント発生時の原因究明が十分に行えなくなるリスクがあります。

SSL/TLS通信を可視化するSSLインサイトソリューションと高機能ネットワークフォレンジックサーバNetRAPTORとの連携

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、通信パフォーマンスを落とすことなくSSL/TLS通信を可視化できます。このソリューションを導入する際には、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やSMTPSなどのSSL/TLS通信をインターセプトして復号し、復号して平文化した通信データをインライン型・パッシブ型・ICAPサーバ型のセキュリティ機器に転送して検査できます。トラフィック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。

トーテックアメニティ株式会社のネットワークフォレンジック製品NetRAPTORをこのSSLインサイトソリューションと連携させることで、SSL/TLS通信に対する詳細なパケットキャプチャとフォレンジックが実現できます。図1にあるように、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NetRAPTORに送ることで、SSL/TLS通信は復号された状態でNetRAPTORに記録されます。

NetRAPTORは通信の証跡保存とセキュリティ事故が発生した際の証跡分析を迅速に行うためのネットワークフォレンジック製品です。大量の通信データであっても取りこぼすことがないよう、独自の制御技術を用いたギガビット・フルワイヤキャプチャに完全対応しており、ネットワーク内に流れるすべてのパケットを漏れなく捕捉できます。また、通信データのキャプチャ／解析／検索インデックス作成をリアルタイムに処理する強力なフォレンジックエンジンと強力な日本語全文検索機能を持ち、あらかじめ用意された項目を入力する「簡易検索」と、論理演算を駆使することで複雑な検索が可能な「論理演算式検索」の2種類に対応、捕捉されたパケットから目的の情報へ素早く辿りつくことができます。利用頻度の高い条件を事前に登録しておくことで、リアルタイムなアラート条件として活用できます。

課題：

- HTTPSやSMTPS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への対策
- 情報セキュリティインシデント発生時の、SSL/TLSで暗号化された通信データの内容も含めた原因調査の実現

解決策：

- A10 ThunderのSSLインサイトソリューションによるSSL/TLS通信の高速な可視化（復号）
- トーテックアメニティの高機能ネットワークフォレンジックサーバNetRAPTORによる、SSLインサイトソリューションにより可視化（復号）されたSSL/TLS通信の記録とそれに基づくフォレンジック

メリット：

- NetRAPTORとThunderの組み合わせにより、SSL/TLS通信を復号した状態で記録でき、情報セキュリティインシデント発生時のフォレンジックが容易に
- 大規模なセッションを処理可能なA10 ThunderによるSSL/TLS通信の高速な復号/再暗号化における高い通信パフォーマンスの維持と、高負荷にも対応できるNetRAPTORによる大容量通信データの記録
- HTTPSやSMTPSも含むすべてのポートにおけるSSL/TLS通信の復号と記録
- リアルタイムの検索・検知が可能なフォレンジックエンジンによる迅速なインシデント対応

TOTEC AMENITY LIMITED

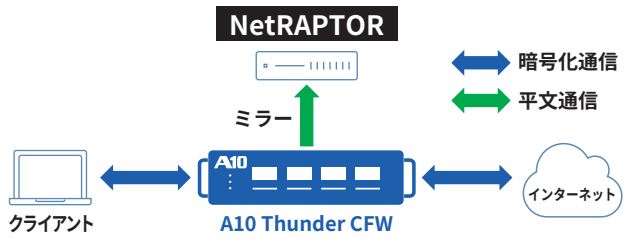

図1：A10 Thunderによる SSL インサイトソリューションと トーテックアメニティ NetRAPTOR との連携

NetRAPTORはミラーポートで通信パケットをキャプチャすることから、通常はSSL/TLS通信を復号できず、暗号化された通信内容を完全に記録して分析することができません。SSL/TLS通信に潜む脅威を可視化するためには、図1のようにSSL/TLS可視化ソリューションと連携したパケットキャプチャが必要になります。A10 Thunderは企業の内部にあるクライアントとインターネットの間で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NetRAPTORに復号した通信を送信します。SSL/TLS通信の可視化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NetRAPTORに送信し、NetRAPTORが復号されたパケットをキャプチャ
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にフォワード
3. サーバ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NetRAPTORに送信、NetRAPTORが復号されたパケットをキャプチャ
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ミラーポートを通じてNetRAPTORに送信、NetRAPTORがパケットをキャプチャ

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NetRAPTORに渡すことで、これまで通信データの内容が把握できなかったSSL/TLS通信に対しても、平文の通信と同様の、通信内容を含めたフォレンジックが可能になります。特にSSL/TLS通信で送受信されたファイルの内容や、HTTPSでアクセスしたURLなどを全て記録できるようになり、通信内容の再現や、いつどのようなサイバー攻撃を受けたかの確認、情報漏えいの検査、URLや通信内容も含めた不正アクセスの調査が可能になります。

クライアントとA10 Thunderの間、およびA10 Thunderと通信先サーバとの間のコネクションは暗号化され、なりすましやデータ窃盗は防止されます。

SSLインサイトソリューションを用いると、一度復号した通信を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やICAP連携可能な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、他のセキュリティ製品との連携も併せて行うことができます。一度の復号で複数の機器での検査を行うことができるため、復号/再暗号化に伴う通信遅延を最小にすることができます。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NetRAPTOR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での導入
- 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

トーテックアメニティ株式会社について

トーテックアメニティ株式会社は、「Let's New Value！」をコーポレートビジョンとして、お客様の新たなる価値創造のための情報化戦略・技術戦略・人財戦略を実現する、IT・エンジニアリングソリューション企業です。国内のサイバーセキュリティ関連組織との技術連携を通して、純国産のサイバーセキュリティ対策製品を自社で企画、開発、販売しています。本連携のように、自社開発の強みを活かした他製品連携にも取り組み、新しいセキュリティソリューションの提供を、積極的に行ってまいります。NetRAPTORはトーテックアメニティ株式会社の登録商標です。

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

Learn More

About A10 Networks

お問い合わせ
a10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp
a10networks.co.jp/contact

©2020 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networksは米国およびその他各国におけるA10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。商標について詳しくはホームページをご覧ください。www.a10networks.com/a10-trademarks

Part Number: A10_SB_Totec_NetRAPTOR_and_A10　Nov 2020