SSL/TLSトラフィックを大規模に収集し可視化、セッションを再現し暗号化通信に隠れた脅威の検知やフォレンジックを実現

RSA NetWitness® Packets と A10 SSL インサイトの連携ソリューション

課題：
脅威を完全に可視化するためには、暗号化トラフィックを含む全てのトラフィックを大規模に蓄積し、検査や調査を可能にする必要がある。

解決策：
A10 Thunder®シリーズが提供するSSLインサイトソリューションがSSL/TLS通信をインターセプトし復号されたトラフィックをRSA NetWitness Packetsに送ることにより、暗号化トラフィックの大規模な蓄積と可視化やセッション再現が可能になり、脅威の検知・問題発生時のフォレンジックを実現できる。

メリット：

- A10 Thunderが専用ハードウェアを活用してSSL/TLS通信を高速で復号することで、暗号化通信に隠れた脅威を暴き出すことができる
- RSA NetWitness Packetsの持つ高度なメタデータ付与機能により、これまでにない正確さと速さでインシデントの調査・優先度付け・修正を行うことができる
- RSA Liveが常に最新の解析用パーサーを提供し、最も先進的な攻撃であっても、ビジネスへの影響が及ぶ前に検知し分析することができる
- A10 Thunderの提供する負荷分散機能によりRSA NetWitness Packetsのスケールが可能になる

通信の暗号化により脅威の可視化が困難に

サイバー攻撃の脅威は日々継続して拡大しています。攻撃者はターゲットとする組織に大掛かりな偵察を行い、従業員の名前やe-mailアドレス、ビジネスアプリケーションなどを特定しています。セキュリティチームは攻撃者の先を行くために新しい状況に適応しなくてはなりませんが、不幸にして、多くのセキュリティチームは攻撃を検知しそこなうか、新しい攻撃手法に対して追従するための十分な専門性を持ち合わせていません。

これらの脅威を認識した上で、組織は拡大しつつあるSSL/TLS通信の通信量にも対処しなくてはなりません。スヌーピングや改ざん、データの窃盗を防ぐために、SSL/TLSを用いてデータを暗号化するアプリケーションは増加しています。多くのWebアプリケーションは当初、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を暗号化していましたが、近年は全てのWebリクエストとレスポンスを暗号化しています。実際、NSS Labsの調査では2019年までに75%のエンタープライズのトラフィックが暗号化されると予測されています。[*1]

アプリケーションとデータを保護するためには、組織は暗号化通信を含む全てのトラフィックを蓄積し検査しなくてはなりません。その一方で、多くのセキュリティデバイス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数少ないデバイスも、急増するSSL/TLS通信量のペースに追いつく性能を持っておらず、組織の防御に深刻なギャップがあります。

SSL インサイトと RSA NetWitness Packets

A10ネットワークスは、SSL/TLS通信に隠れた不正なアクティビティを検知するために、EMCのセキュリティ部門であるRSAと提携しました。A10 ThunderシリーズによるSSLインサイトソリューションは、SSL/TLS通信を終端し高速に復号します。復号したトラフィックをRSA NetWitness Packetsに送ることで、データの大規模な蓄積と、トラフィック可視化やセッション再現が可能になり、脅威の検査と分析が実現できます。

A10 ThunderによるSSLインサイトではフォワードプロキシとしてSSL/TLS通信をインターセプトします。RSA NetWitness PacketsとSSLインサイトソリューションの連携を行う場合、Thunderアプライアンスを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インストールする必要があります。

図1での通信の流れは以下のようになります。

1. ThunderがSSL/TLSトラフィックをインターセプトし、トラフィックを復号して平文のトラフィックのコピーをRSA NetWitness Packetsに送信し、データの蓄積および検査と分析を実施
2. Thunderがトラフィックを再暗号化しWebサーバーにフォワード
3. Webサーバーはリクエストを受信し、暗号化されたレスポンスをクライアントに送信

[*1] https://www.nsslabs.com/company/news/press-releases/nss-labs-predicts-75-of-web-traffic-will-be-encrypted-by-2019/

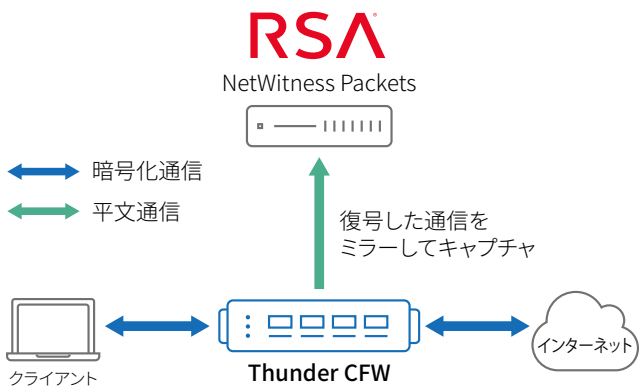


図 1：Thunder CFW による SSL/TLS 通信の可視化と RSA NetWitness Packets との連携

4. 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、復号して平文のトラフィックのコピーを RSA NetWitness Packets に送信し、データの蓄積および検査と分析を実施
5. Thunder が Web サーバーのレスポンスを再暗号化しクライアントに送信

A10 ネットワークスの SSL インサイトにより、内部のクライアントと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、スヌーピングやデータ窃盗を防止できます。インバウンド / アウトバウンドのどちらのネットワークトラフィックも適切に RSA NetWitness Packets により検査・分析される状態を保ち、ネットワークアクティビティの完全な可視化を実現します。

また、負荷分散機能により、Thunder シリーズは複数の RSA NetWitness Packets の非インラインモードでの利用を可能にし、ハードウェア障害時にはネットワークデータを利用可能な RSA NetWitness Packets に送信することで、高可用性とスケーラビリティを実現します。

SSL/TLS 通信の課題

多数の SSL/TLS セッションを終端し同時に暗号化 / 復号する処理は、CPU に非常に大きな負荷がかかります。また、SSL/TLS 通信のセキュリティ強度の強化には、CPU の処理能力の大幅な増強が求められます。SSL の鍵長は暗号強度に関連します。一般的に、2,048 ビットの SSL 証明書は 1,024 ビットの証明書と比べ、暗号化時におよそ 3.4 倍、復号時には 6.3 倍の処理能力を必要とすると言われています。また、4,096 ビットの証明書は 1,024 ビットの証明書に比べ、復号処理に概算で 25 倍の処理能力を必要とします。

米国国立標準技術研究所 (NIST) の SP 800-131A によって推奨された、1,024 ビットから 2,048 ビット鍵長への移行は、SSL/TLS トラフィックの暗号化 / 復号を行うデバイスに負荷を与えています。SSL 証明書の鍵長を増やしてセキュリティ強度を上げたい場合、セキュリティアプライアンスの劇的なパフォーマンス向上が求められます。SSL トラフィックをインターセプトし検査するデバイスは、複数のセッションを同時に管理し、秒間で多数の SSL/TLS コネクションを扱い、より大きな SSL 鍵サイズを扱えるだけの処理能力を持つ必要があります。

強力なセキュリティプロセッサーによる SSL/TLS 通信の高速処理

SSL/TLS 暗号化では最初の SSL ハンドシェイクの部分で最も CPU に負荷がかかります。セッション内でのデータの暗号化 / 復号も CPU にとっての負荷となりますが、ハンドシェイクと比べると負荷は小さくなります。A10 Thunder シリーズは多数の暗号化コネクションを同時に扱うことが出来るように設計されており、格段に優れた SSL/TLS コネクション数とスループットを得ることができます。

A10 の 64bit の Advanced Core Operating System (ACOS®) により、Thunder シリーズはセキュリティ専用プロセッサーとスイッチング / ルーティングプロセッサーの能力を最大限活用し、リニアなスケーラビリティと最大限のパフォーマンスを提供することができます。

SSL/TLS コネクションを確立するために既存の CPU リソースを利用した場合、SSL の鍵長が長くなると急激にパフォーマンスが低下します。次世代のセキュリティプロセッサーを利用することで、Thunder シリーズは 1,024 ビット鍵長でも 2,048 ビット鍵長でもほぼ同等の高い性能を示し、膨大な処理能力を要する 4,096 ビット鍵長でも商用レベルでの高い性能を得ることができます。

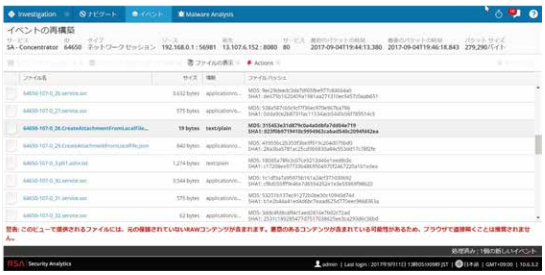
Thunder シリーズにより提供される詳細なポリシー設定により、利用者はトラフィックの種類、発信元 / 宛先 IP アドレスやその他の属性に応じてどの暗号化セッションを復号し、どのセッションを暗号化されたままにしておくかを制御することができます。

A10 の Thunder シリーズのその他の特長と利点は以下の通りです。

- 全てのポートとプロトコルにわたる、SSL/TLS 暗号化トラフィックの復号
- 最大 40Gbps 以上の SSL/TLS トラフィックに対応できる拡張性
- 全てのポートで SSL/TLS 通信を動的に検知
- SSL/TLS セッションで利用される複数の暗号スイートを制御
- SSH および STARTTLS (SMTP や XMPP など) プロトコルの復号
- PFS 暗号のサポート
- FIPS 140-2 level 3 のハードウェアセキュリティモジュールのサポート
- インライン / アウトオブバンドのセキュリティアプライアンスに対して復号と負荷分散を同時に実行
- 柔軟な導入オプション
- URL フィルタリングと復号しない通信を迂回させるための URL クラシフィケーションサービス

SSL インサイトで復号された通信のキャプチャ

セッションを再現して
詳細分析



暗号化された通信のキャプチャ

セッション再現不可！
内容の分析も困難

図 2：SSL/TLS 通信を復号して NetWitness Packets により詳細分析する例と暗号化通信のパケットキャプチャとの比較

RSA NetWitness による可視化と分析

RSA NetWitness Suite は組織が必要とする優れた通信の可視化機能を提供するセキュリティ監視のプラットフォームです。複数のログ、ネットワークの情報（パケットと NetFlow）、エンドポイントの状態を結合し、エンタープライズ全体にわたって起こっている事象を確認することができます。環境を全体的に俯瞰できることで、分析者はより効率的に攻撃を検知出来るようになります。

RSA NetWitness Suite は以下のいくつかのユースケースに適合するように、柔軟でモジュラーなアプローチをセキュリティチームに提供します。

- ネットワークフォレンジックを通じた完全な可視化と迅速な調査
- SIEM（Security Information and Event Management）製品以上の分析のケイパビリティとログ中心のアプローチ
- コンプライアンスの必須要件を満たすためのビルトインされた機能

RSA NetWitness Packets は、RSA NetWitness Suite の中で、可視化と分析の元となるネットワークトラフィックの収集と蓄積・メタデータ保管とインデクシング・脅威検知を行います。1 台で最大 10Gbps のパケットキャプチャをサポートし、PB 単位での大容量データの保存に対応しています。RSA Live から配信される最新の解析用パーサーを利用してネットワークセッションを解析し、得られた情報をメタデータとして作成することで、分析者は長期間かつ大容量のデータに対して非常に高速な検索を行うことができます。また、特定のセッションをテキスト・メールビュー・Web ビュー・ファイル抽出など様々な形式で再現することができます。脅威の発見に有用なメタデータや相関的なルールを使用した脅威の発見と通知を実現し、よりプロアクティブな脅威検知を実現します。

A10 の SSL インサイトソリューションを利用することで、通常は検査できない SSL/TLS 通信の内容も RSA NetWitness Packets により検査することが可能となり、脅威に対する完全な可視化と分析を実現できます（図 2）。

結論

転送中のデータを暗号化するアプリケーションが増えるにつれて、SSL/TLS 通信は企業の防御にとって危険な盲点となりつつあります。A10 Thunder シリーズを RSA NetWitness Packets と共に利用することで、暗号化通信をインターセプトし、導入が容易でスケーラブルなセキュリティ強化ソリューションを提供することができます。RSA NetWitness Packets と A10 Thunder の相互接続性は検証を通して確認されています。A10 の SSL インサイトソリューションを利用することで、以下が実現されます。

- A10 の 64 ビット OS である ACOS と専用のセキュリティプロセッサーを使うことによる、パフォーマンス、可用性、スケーラビリティの最大化
- RSA NetWitness などの先進的なセキュリティ監視プラットフォームとの統合により、イベント管理やフォレンジック、コンプライアンスを実現
- セキュリティログ、ネットワークのパケットキャプチャ、エンドポイントの状態を組み合わせて、会社全体で発生している事象を確認

A10 の強力な SSL インサイトの機能により、以下が実現されます。

- 攻撃や情報漏えいを暴くための、暗号化通信を含めたネットワーク活動の完全な可視化
- Thunder によりインターセプトして復号した SSL/TLS 通信を複数のセキュリティデバイスに転送し、セキュリティ分析や DLP、脅威防御や侵入検知を実施
- 金融やヘルスケアの Web サイトとの通信などの機密データを扱う Web サイトへのトラフィックを迂回させ復号を回避（オプション）
- SSL/TLS の鍵長が増大した場合にも対応でき、投資を保護

EMC ジャパン株式会社
RSA について

EMC ジャパンは、情報インフラの卓越したテクノロジーとソリューションの提供を通して、日本のお客様の情報インフラの課題解決をご支援し、あらゆる規模のお客様のビジネスの継続と成長、さらにビジネス価値の創造に貢献致します。RSA は、EMC ジャパンでセキュリティ、リスク、コンプライアンス管理ソリューションを提供しています。世界中の企業が抱えている組織のリスク管理やモバイルアクセスの保護と連携、コンプライアンスの証明、仮想環境やクラウド環境でのセキュリティ確保をはじめとする複雑で慎重な対処を要するセキュリティ上の課題を解決し、お客様の事業成長を支援します。
http://japan.rsa.com/

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。
URL：http://www.a10networks.co.jp/
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社
〒106-0032
東京都港区六本木三丁目2番1号
住友不動産六本木グランドタワー33階
TEL : 03-4520-5700
FAX: 03-4520-5701
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-19125-JA-02
Jan 2018