



トラフィック復号の概要

以下のトピックではSSLインスペクションの概要を示し、SSLインスペクション設定の前提条件と詳細な導入シナリオについて説明します。

- [トラフィック復号について \(1 ページ\)](#)
- [SSL ハンドシェイク処理 \(2 ページ\)](#)
- [SSL ハードウェア アクセラレーション \(7 ページ\)](#)
- [SSL インスペクションの要件 \(8 ページ\)](#)
- [SSL インスペクションアプライアンス導入シナリオ \(9 ページ\)](#)
- [SSL の履歴 \(23 ページ\)](#)

トラフィック復号について

Firepower システムは、デフォルトではセキュア ソケット レイヤ (SSL) プロトコルまたはその後継である Transport Layer Security (TLS) プロトコルで暗号化されたトラフィックを検査できません。SSL インスペクション (検査) 機能を使用すると、暗号化トラフィックのインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセスコントロール (制御) を使用して検査したりできます。暗号化されたセッションをシステムが処理するときは、トラフィックの詳細がログに記録されます。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、ネットワーク内の暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

SSL インスペクションは、ポリシーベースの機能です。FirePOWER システムでは、アクセスコントロールポリシーは、SSL ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。アクセスコントロールと SSL ポリシーを関連付ければ、システムはアクセスコントロールルールで評価する前に、その SSL ポリシーを使用して暗号化セッションを処理します。SSL インスペクションを設定していない場合、またはデバイスがサポートしていない場合、アクセスコントロールルールは、すべての暗号化トラフィックを処理します。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、そのトラフィックがアクセスコントロールルールによって処理されることにも注意してください。ただし、一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイルインスペクションを

無効にしています。これにより、侵入およびファイルインスペクションが設定されたアクセスコントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムで TCP 接続での SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうか判定されます。復号できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化トラフィックをブロックする
- 暗号化トラフィックをブロックし、TCP 接続をリセットする
- 暗号化トラフィックを復号しない

システムによるトラフィックの復号が可能な場合は、それ以上のインスペクションなしでトラフィックをブロックするか、復号されていないトラフィックをアクセスコントロールによって評価するか、あるいは次のいずれかの方法を使用して復号します。

- 既知の秘密キーを使用して復号する。外部ホストがネットワーク上のサーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書とシステムにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。
- サーバ証明書の再署名によって復号する。ネットワーク上のホストが外部サーバとの SSL ハンドシェイクを開始すると、システムによって、交換されたサーバ証明書が、アップロード済みの認証局 (CA) 証明書で再署名されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。

復号されたトラフィックに対しては、はじめから暗号化されていないトラフィックと同じトラフィックの処理と分析 (ネットワーク、レピュテーション、およびユーザベースの各アクセスコントロール、侵入検知と防御、Cisco Advanced Malware Protection (Cisco AMP)、およびディスクバリエーション (検出)) が実行されます。システムで、復号されたトラフィックのポスト分析をブロックしない場合、トラフィックを再暗号化してから宛先ホストに渡します。

SSL ハンドシェイク処理

このマニュアルでは、SSL ハンドシェイクという用語は SSL プロトコルとその後継プロトコルである TLS の両方の暗号化セッションを開始する、2 ウェイ ハンドシェイクを表します。

パッシブ展開では、FirePOWER システムはハンドシェイクのコピーを確認しますが、実際のハンドシェイクを処理しません。インライン展開では、FirePOWER システムは SSL ハンドシェイクを処理し、ClientHello メッセージを修正する可能性があり、セッションの TCP プロキシサーバとして機能します。

(正常に TCP 3 ウェイ ハンドシェイクが完了した後) クライアントがサーバとの TCP 接続を確立すると、管理対象デバイスは TCP セッションでの暗号化されたセッションの開始の試行をモニタします。SSL ハンドシェイクは、クライアントとサーバ間の特殊なパケットの交換によって、暗号化セッションを確立します。SSL と TLS プロトコルでは、これらの特殊なパケッ

トはハンドシェイク メッセージと呼ばれます。ハンドシェイク メッセージは、クライアントとサーバの両方がサポートする暗号化属性を伝えます。

- **ClientHello** : クライアントは各暗号化属性に複数のサポートされる値を指定します。
- **ServerHello** : サーバはシステムがセキュリティで保護されたセッション中に使用する暗号化方式を決定する、各暗号化属性に 1 つのサポートされる値を指定します。

セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッションデータをキャッシュに保存し、それによりフルハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバ証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

ClientHello メッセージ処理

セキュアな接続が確立できる場合、クライアントはパケットの宛先として機能するサーバに ClientHello メッセージを送信します。クライアントは SSL ハンドシェイクを開始するメッセージを送信するか、または宛先サーバからの Hello Request メッセージへの応答に含めます。

SSL インспекションを設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを [復号 - 再署名 (Decrypt - Resign)] アクションを含む SSL ルールと照合しようとします。照合は ClientHello メッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。考えられるデータには次のものがあります。

表 1: SSL ルールの条件のデータの可用性

| SSL ルールの条件 | データの存在場所 |
|------------|-------------------------------|
| ゾーン | ClientHello |
| ネットワーク | ClientHello |
| VLAN タグ | ClientHello |
| ポート | ClientHello |
| Users | ClientHello |
| アプリケーション | ClientHello (サーバ名インジケータの拡張機能) |
| カテゴリ | ClientHello (サーバ名インジケータの拡張機能) |
| 証明書 | サーバ証明書 (キャッシュされている可能性あり) |

| SSL ルールの条件 | データの存在場所 |
|-------------------------------|-------------------------|
| 識別名 | サーバ証明書（キャッシュされている可能性あり） |
| 証明書のステータス（Certificate Status） | サーバ証明書（キャッシュされている可能性あり） |
| 暗号スイート | ServerHello |
| バージョン | ServerHello |

ClientHello メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致しない場合、システムはメッセージを変更しません。次に、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）で合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致したら、システムは ClientHello メッセージを次のように変更します。

- 圧縮方法：クライアントがサポートする圧縮方法を指定する、`compression_methods` 要素を削除します。Firepower システムは圧縮されたセッションを復号できません。この変更により、復号できないトラフィックの圧縮されたセッションタイプが削減されます。
- 暗号スイート：Firepower システムがサポートしない場合、`cipher_suites` 要素から暗号スイートを削除します。Firepower システムが指定した暗号スイートのいずれもサポートしない場合、システムは、元の変更されていない要素を送信します。この変更により、復号できないトラフィックの、サポートされない暗号スイートと不明な暗号スイートが削減されます。
- セッション識別子：キャッシュされたセッションデータと一致しない `SessionTicket` 拡張機能と `Session Identifier` 要素から値を削除します。ClientHello 値がキャッシュされたデータと一致した場合、一時停止したセッションは、クライアントとサーバが完全な SSL ハンドシェイクを実行せずに、中断したセッションを再開できます。この変更は、セッション再開の可能性を高め、復号できないトラフィックの、セッションが未キャッシュのタイプを削減します。
- 楕円曲線：Firepower システムがサポートしない場合、サポートされる楕円曲線拡張機能から楕円曲線を削除します。Firepower システムが指定した楕円曲線のいずれもサポートしない場合、管理対象デバイスは拡張機能を削除し、`cipher_suites` 要素から関連する暗号スイートを削除します。
- ALPN 拡張機能：Firepower システムでサポートされていないアプリケーション層プロトコルネゴシエーション（ALPN）拡張機能から値を削除します（たとえば、SPDY と HTTP/2 プロトコル）。この変更は、メッセージがコンテンツ制限機能に関連付けられた SSL ルールに一致した場合にのみ実行されます。詳細については、[コンテンツ制限について](#)を参照してください。

- 他の拡張機能：Extended Master Secret、Next Protocol Negotiation（NPN）、および TLS チャネル ID 拡張機能を削除します。



- (注) システムはデフォルトで ClientHello の変更を実行します。SSL ポリシーが正しく設定されていると、このデフォルトの動作により、トラフィックの復号がより頻繁に発生します。各ネットワークにおけるデフォルトの動作を調整するには、サポートにお問い合わせください。

システムが ClientHello メッセージを変更した後、メッセージがアクセスコントロール評価（ディープインスペクションを含めることができる）で合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージを変更した後はクライアントおよびサーバで計算されたメッセージ認証コード（MAC）が一致しなくなるため、SSL ハンドシェイク時のクライアントとサーバの間の直接通信はできなくなります。すべての後続のハンドシェイクメッセージ（および一度設定された暗号化セッションに対し）、管理対象デバイスは、中間者（MITM）として機能します。ここでは 2 つの SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。その結果、暗号化セッションの詳細はセッションごとに異なります。



- (注) Firepower システムが復号できる暗号スイートは頻繁に更新されるので、SSL ルールの条件で使用可能な暗号スイートと直接対応しません。現在、復号できる暗号スイートのリストについては、サポートに連絡してください。

関連トピック

[復号できないトラフィックのデフォルト処理オプション](#)

[オンライン展開での暗号化トラフィックの再署名済み証明書による検査](#) (21 ページ)

ServerHello とサーバ証明書メッセージの処理

ServerHello メッセージは、正常な SSL ハンドシェイクの ClientHello メッセージへの応答です。

管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式が認証に証明書を使用する場合、サーバ証明書メッセージはすぐに ServerHello メッセージに続きます。

管理対象デバイスがこれらのメッセージを受信すると、SSL ルールとの一致を試みます。これらのメッセージには、ClientHello メッセージまたはセッションデータ キャッシュにはなかった情報が含まれます。具体的には、システムは、識別名、証明書のステータス、暗号スイート、およびバージョン条件で、これらのメッセージと一致させる可能性があります。

メッセージがSSLルールと一致しない場合、管理対象デバイスは、SSLポリシーのデフォルトのアクションを実行します。詳細については、[SSLポリシーのデフォルトアクション](#)を参照してください。

メッセージがSSLルールに一致する場合、管理対象デバイスは、必要に応じて次に進みます。

アクション：モニタ (Monitor)

SSLハンドシェイクは完了に進みます。管理対象デバイスは追跡およびログに記録しますが、暗号化トラフィックを復号しません。

アクション：ブロック (Block)、またはリセットしてブロック (Block with Reset)

管理対象デバイスは、SSLセッションをブロックします。必要に応じて、TCP接続もリセットします。

アクション：復号しない (Do Not Decrypt)

SSLハンドシェイクは完了に進みます。管理対象デバイスは、SSLセッションの間で交換されるアプリケーションデータを復号しません。

まれに、システムではClientHelloメッセージと[復号-再署名 (Decrypt - Resign)]ルールが一致してメッセージを変更しますが、関連するServerHelloメッセージは[復号しない (Do Not Decrypt)]ルールに一致することがあります。このような場合、クライアントから更新されたハンドシェイクをトリガーするために、システムはTCP接続をリセットします。更新されたClientHelloメッセージは[復号-再署名 (Decrypt - Resign)]ルールに一致しなくなり、SSLセッションは復号せずに進みます。

アクション：復号 - 既知のキー (Decrypt - Known Key)

管理対象デバイスは、サーバ証明書データを以前にアップロードされたサーバ証明書と照合しようとします。

証明書が以前に生成された証明書と一致した場合、SSLハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSLセッション中に交換されたアプリケーションデータを復号および再暗号化します。

まれに、システムでは、サーバ証明書メッセージが以前に生成された証明書と一致しないことがあります。たとえば、サーバはクライアントとの最初の接続と後続の接続の間に証明書を変更することがあります。この場合、システムはSSL接続をブロックし、クライアントが再接続して、システムが新しい証明書データとのハンドシェイクを処理できるようにします。

アクション：復号 - 再署名 (Decrypt - Resign)

管理対象デバイスは、サーバ証明書メッセージを処理し、以前にアップロードされた認証局 (CA) 証明書で交換されるサーバ証明書を再署名します。SSLハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSLセッション中に交換されたアプリケーションデータを復号および再暗号化します。

ServerHello および証明書メッセージの処理中、管理対象デバイスは識別名と証明書データをキャッシュし、再確立されたセッションと、後続のSSLセッションの両方でハンドシェイクが高速で処理されるようにします。

SSL ハードウェア アクセラレーション

特定の FirePOWER 管理対象デバイス モデルでは、パフォーマンスが大幅に向上する、ハードウェアでの SSL 暗号化および復号化のアクセラレーションをサポートしています。

SSL ハードウェア アクセラレーションは、デフォルトでは無効になっています。

サポート対象のハードウェア (Supported Hardware)

以下のハードウェア モデルは、SSL アクセラレーションをサポートしています。

- FirePOWER 9300 シリーズ セキュリティ アプライアンス
- Cisco Firepower 4100 シリーズ

仮想アプライアンス上および上記以外のハードウェアでの SSL ハードウェア アクセラレーションはサポートされていません。

ハードウェア アクセラレーションによってサポートされていない機能

SSL ハードウェア アクセラレーションによってサポートされていない機能は、次のとおりです。

- Camellia 暗号方式の復号化
- パッシブ ネットワークまたはインライン タップ モード インターフェイスを使用した SSL トラフィックの復号化
- Generic Routing Encapsulation (GRE) や IP トンネルでの IP など、トンネルでカプセル化された SSL トラフィックの復号化
- インспекション エンジンが接続を維持するように設定されていて、インспекション エンジンが予期せず失敗した場合は、エンジンが再起動されるまで SSL トラフィックはドロップされます。

この動作は、`configure snort preserve-connection {enable | disable}` コマンドにより制御されます。

SSL ハードウェア アクセラレーションの有効化または無効化

管理対象デバイスで SSL ハードウェア アクセラレーションを有効化または無効化するには、次のコマンドを使用します。

`system support {ssl-hw-offload enable | ssl-hw-offload disable}`

構文の説明


`ssl-hw-offload enable` ハードウェア アクセラレーションを有効化します。デバイスを再起動するように求められます。

ssl-hw-offload disable SSLハードウェアアクセラレーションを無効化します。デバイスを再起動するように求められます。

SSLハードウェアアクセラレーションのステータスの表示

このトピックでは、SSLハードウェアアクセラレーションが管理対象デバイスで有効になっているかどうかを確認する方法について説明します。特定の管理対象デバイスでのみ、この機能がサポートされます。詳細については、[SSLハードウェアアクセラレーション \(7ページ\)](#)を参照してください。

手順

-
- ステップ 1** Firepower Management Center にログインします。
 - ステップ 2** [デバイス (Devices)] > [デバイス管理 (Device Management)] をクリックします。
 - ステップ 3**  (編集) をクリックして、管理対象デバイスを編集します。
 - ステップ 4** [デバイス (Device)] タブ ページをクリックします。SSLハードウェアアクセラレーションステータスは、[全般 (General)] セクションに表示されます。
-

SSLインスペクションの要件

構成時の設定やライセンスに加え、アプライアンスをネットワーク上にどのように展開しているかにより、暗号化トラフィックの制御や復号化に適用できるアクションが異なります。最適な展開タイプを決定するときは、マッピングされたアクション、既存のネットワーク展開、および全体的な要件のリストを確認してください。

インライン、ルーティング、スイッチド、またはハイブリッドのインターフェイスで設定および展開されたデバイスでは、トラフィックフローの変更が可能です。これらのデバイスでは、着信および発信トラフィックのモニタリング、ブロック、許可、および復号を行うことができます。

パッシブまたはインライン (タップモード) のインターフェイスで設定および展開されたデバイスでは、トラフィックフローを変更することはできません。これらのデバイスで行えるのは、着信トラフィックのモニタリング、許可、および復号だけです。パッシブ展開では、一時 Diffie-Hellman (DHE) および楕円曲線 Diffie-Hellman (ECDHE) の暗号スイートを使用した暗号化トラフィックの復号はサポートされません。

SSLインスペクションの一部の機能では、公開キー証明書と秘密キーのペアが必要です。暗号化セッションの特性に応じてトラフィックを復号したり制御したりするためには、証明書および秘密キーのペアを Firepower Management Center にアップロードする必要があります。

SSL ルール設定の前提条件に関する情報

SSL インスペクションは、サポートする公開キー インフラストラクチャ (PKI) の多くの情報に依存しています。照合ルールの条件を設定するときは、その組織におけるトラフィック パターンについて検討する必要があります。

表 2: SSL ルール条件の設定に必要な情報

| 一致対象 | 必要な情報 |
|---------------------------|----------------------------|
| 自己署名サーバ証明書を含む、検出されたサーバ証明書 | サーバ証明書 |
| 信頼できるサーバ証明書 | CA 証明書 |
| 検出されたサーバ証明書のサブジェクトまたは発行元 | サーバ証明書のサブジェクト DN または発行元 DN |

ルールの適用先となる暗号化トラフィックの復号、ブロック、モニタリングが不要かどうか、または復号が必要かどうかについて検討します。その結果を、SSL ルールのアクション、復号できないトラフィックのアクション、および SSL ポリシーのデフォルトアクションに反映させます。

表 3: SSL 復号に必要な情報

| 復号の対象 | 必要な情報 |
|--------------------|--|
| 制御対象のサーバへの着信トラフィック | サーバ証明書のファイルと秘密キー ファイルのペア |
| 外部サーバへの発信トラフィック | CA 証明書のファイルと秘密キー ファイルのペア CA 証明書と秘密キーを生成することもできます。 |

これらの情報を収集したら、システムにアップロードして、再利用可能なオブジェクトを設定します。

関連トピック

- [識別名オブジェクト](#)
- [PKI オブジェクト](#)

SSL インスペクション アプライアンス 導入シナリオ

ここでは Life Insurance Example, Inc. (LifeIns) という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インスペクションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- カスタマー サービス部門では、単一の 7000 または 8000 シリーズ デバイスをパッシブ展開する

- 契約審査部門では、単一の 7000 または 8000 シリーズ デバイスをインライン展開する
- 上記の両方のデバイスを単一の Firepower Management Center で管理する

カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する見込み顧客からの暗号化された質問や要求を、Web サイトや電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクトメトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマー サービスでは、オンライン フォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。

契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC (MedRepo) という医療データリポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング（なりすまし）応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと考えています。

LifeIns では、経験の浅い契約審査担当者に対して 6 カ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

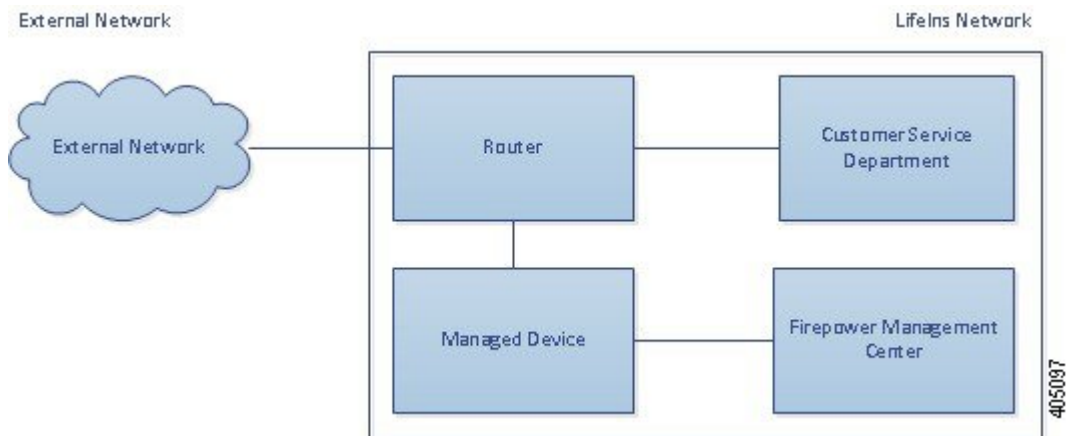
パッシブ展開でのトラフィックの復号

LifeIns のビジネス要件では、カスタマー サービスに次の要求をしています。

- すべての要求と申請書類を 24 時間以内に処理する
- 着信するコンタクトメトリックのコレクションプロセスを改善する
- 着信した不正な申請書類を特定して廃棄する

カスタマー サービス部門では、追加の監査用レビューを必要としません。

LifeIns ではカスタマー サービスの管理対象デバイスのパッシブ展開を計画しています。



外部ネットワークからのトラフィックはLifeInsのルータに送信されます。ルータはトラフィックをカスタマーサービス部門にルーティングし、検査用にトラフィックのコピーを管理対象デバイスに送信します。

管理するFirepower Management Centerでは、Access Control および SSL Editor のカスタム ロールを持つユーザにより、次の SSL インспекションの設定を行います。

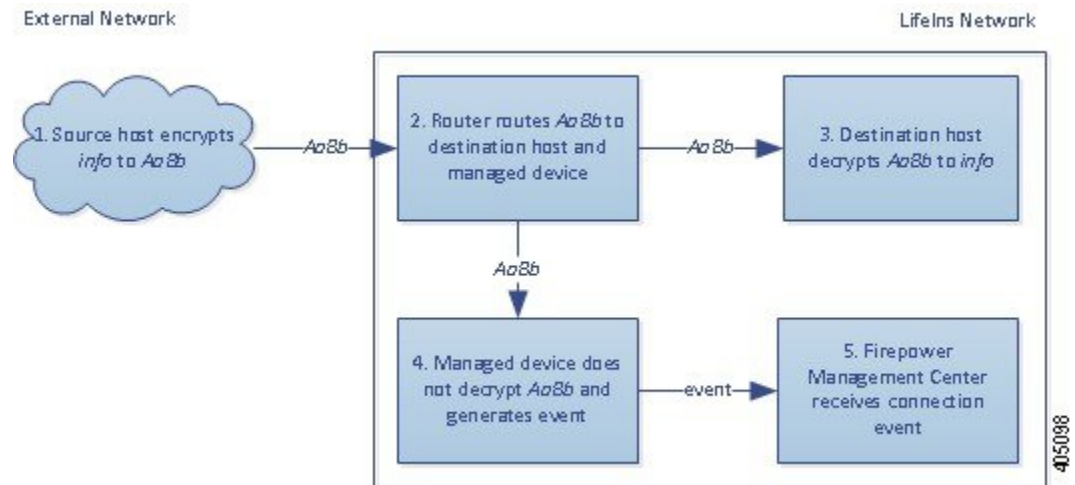
- カスタマー サービス部門に送信された暗号化トラフィックをすべてログに記録する
- オンラインの申請フォームからカスタマーサービスに送信された暗号化トラフィックを復号する
- カスタマー サービスに送信された他の暗号化トラフィックは、オンライン リクエスト フォームからのトラフィックも含め、すべて復号しない

さらに、復号された申請フォームトラフィック中に偽の申請データが含まれていないかを検査し、検出された場合はログに記録するためのアクセスコントロールも設定します。

次のシナリオでは、ユーザからカスタマー サービスにオンライン フォームが送信されます。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスは、このトラフィックのコピーを受信します。クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。システムは、ハンドシェイクと接続の詳細に応じて、接続のログを記録し、暗号化トラフィックのコピーを処理します。

パッシブ展開での暗号化トラフィック モニタリング

管理対象デバイスは、カスタマー サービスに送信されるすべての SSL 暗号化トラフィックについて、接続のログを記録します。

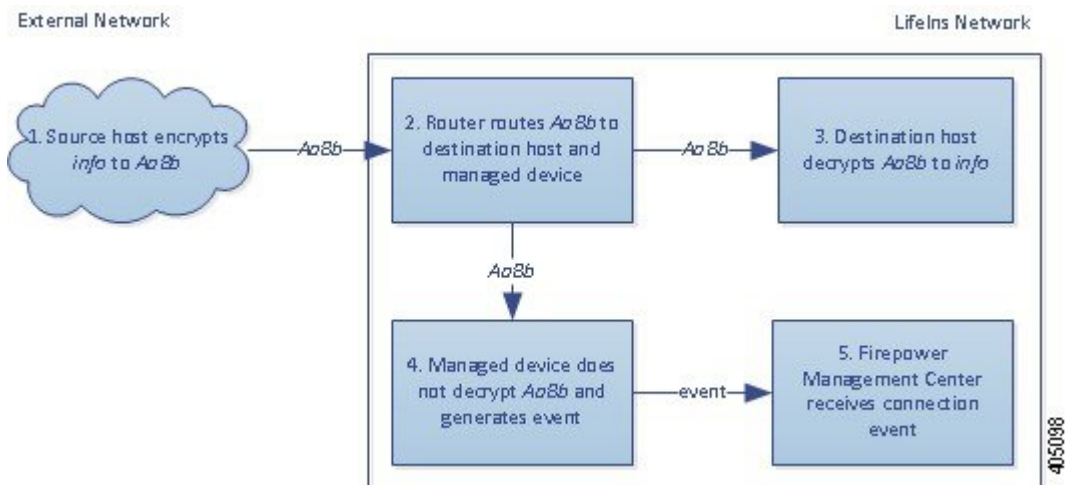


次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (info) を送信します。クライアントがこれを暗号化 (AoBb) し、カスタマー サービスに暗号化トラフィックを送信します。
2. Lifelys のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求 (AoBb) を受信し、これをプレーンテキスト (info) に復号します。
4. 管理対象デバイスはトラフィックを復号化しません。
アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerが接続イベントを受信します。

パッシブ展開での復号されていない暗号化トラフィック

保険契約に関する要求を含むすべての SSL 暗号化トラフィックについては、管理対象デバイスはそのトラフィックを復号せずに許可し、接続のログを記録します。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (info) を送信します。クライアントがこれを暗号化 (AoBb) し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求 (AoBb) を受信し、これをプレーンテキスト (info) に復号します。
4. 管理対象デバイスはトラフィックを復号化しません。
アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerが接続イベントを受信します。

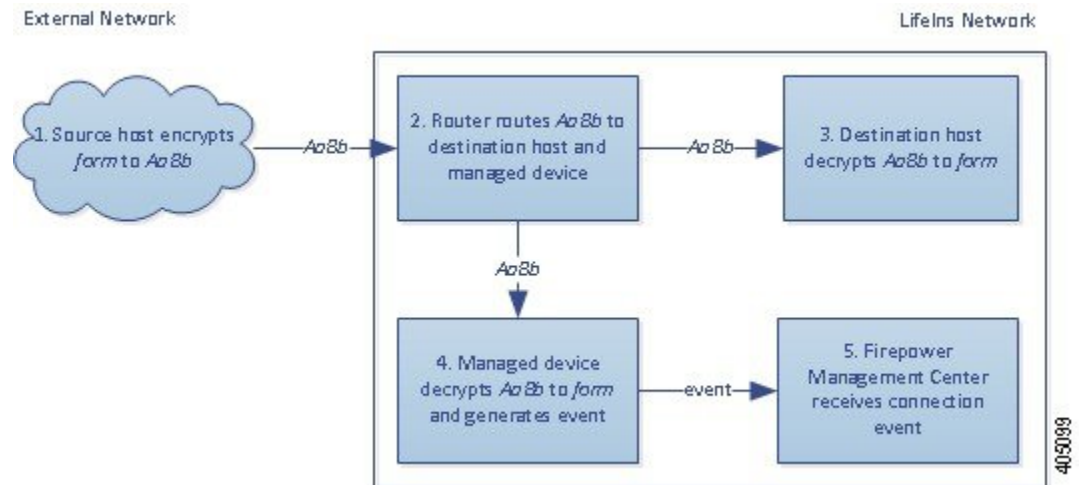
パッシブ展開での暗号化トラフィックの秘密キーによる検査

申請フォームのデータを含むすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。



(注) パッシブ展開の場合、DHE または ECDHE 暗号スイートで暗号化されたトラフィックは、既知の秘密キーを使って復号することはできません。

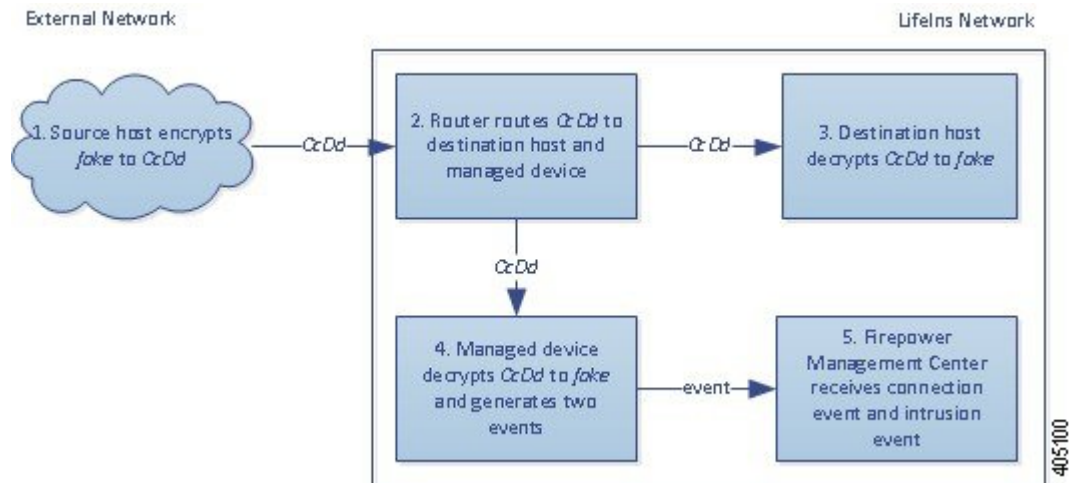
有効な申請フォームの情報を含むトラフィックについては、接続のログが記録されます。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (form) を送信します。クライアントがこれを暗号化 (AaBb) し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (form) に復号します。
4. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、暗号化トラフィックをプレーンテキスト (form) に復号化します。
アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続します。偽の申請書であることを示す情報は検出されません。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Center は、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、復号されたトラフィックに偽の申請データが含まれていた場合、接続および偽のデータについてのログが記録されます。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (*fake*) を送信します。クライアントがこれを暗号化 (*CcDd*) し、カスタマーサービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマーサービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマーサービス部門のサーバが、暗号化された情報の要求 (*CcDd*) を受信し、これをプレーンテキスト (*fake*) に復号します。
4. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、暗号化トラフィックをプレーンテキスト (*fake*) に復号化します。
 アクセスコントロールポリシーは、復号されたトラフィックの処理を継続して、偽の申請書であることを示す情報を検出します。デバイスが侵入イベントを生成します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Center は、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび偽の申請データの侵入イベントを受信します。

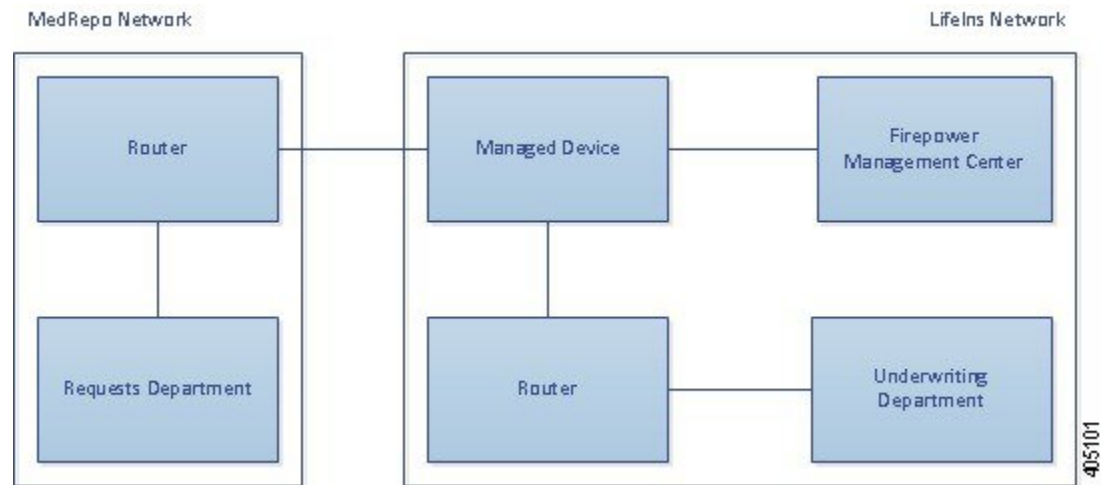
インライン展開でのトラフィックの復号

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepo への情報要求が適切なすべての規則に準じていることを検証する
- その契約審査によるメトリックコレクションプロセスを改善する
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する
- 契約審査部門から MedRepo のカスタマーサービス部門へのすべての不適切な規制要求を排除する

- 経験豊富な契約審査担当者は監査しない

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。



MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeIns のネットワークにトラフィックがルーティングされます。管理対象デバイスはトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送して、管理している Firepower Management Center にイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

管理元の Firepower Management Center で、[アクセス コントロール (Access Control)] および [SSL エディタ (SSL Editor)] のカスタム ロールを持つユーザが、SSL アクセス コントロール ルールの設定を次のように行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号する
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号しない

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号トラフィックを検査するアクセス コントロールを設定します。

- 復号トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する
- 規制に準拠しない情報を含んでいる復号トラフィックをブロックし、不適切な情報をログに記録する
- 他の暗号化および復号されたトラフィックをすべて許可する

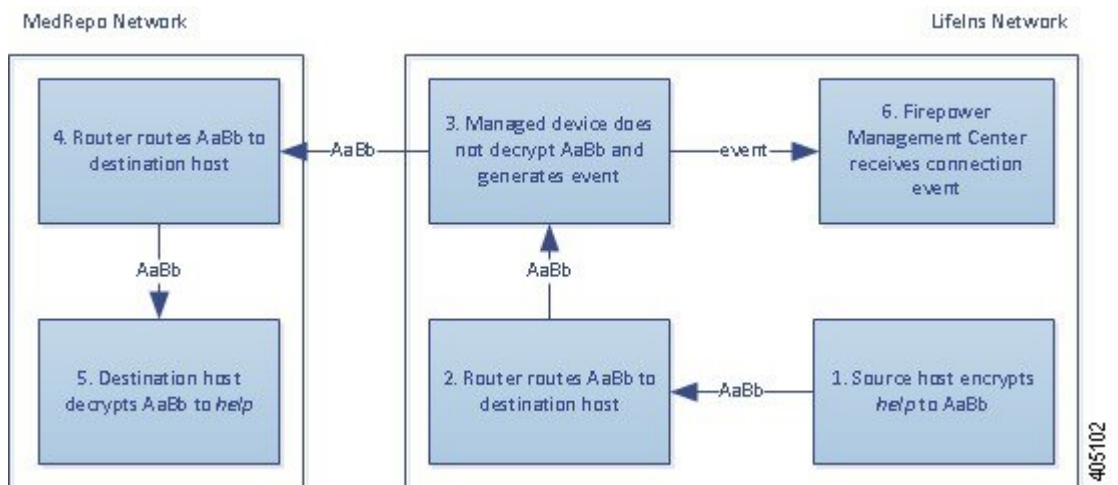
許可された復号トラフィックは、再暗号化されて宛先ホストに転送されます。

また、SSL アクセスコントロールルールを使用して、[復号 - 再署名 (Decrypt - Resign)]アクションでシステムにトラフィックを復号化して再署名させることもできます。トラフィックがSSLルールに一致する場合、システムはClientHelloメッセージを変更した後、メッセージがアクセスコントロール評価（ディープインスペクションを含めることができる）に合格するかどうかを判断します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。詳細については、次を参照してください。 [ClientHello メッセージ処理 \(3 ページ\)](#)

次のシナリオでは、ユーザが情報をオンラインでリモートサーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスはこのトラフィックを受信し、ハンドシェイクと接続の詳細に応じて、システムが接続ログの記録およびトラフィックの処理をします。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

インライン展開での暗号化トラフィック モニタリング

契約審査部門で送受信されるすべてのSSL暗号化トラフィックについて、接続のログが記録されます。



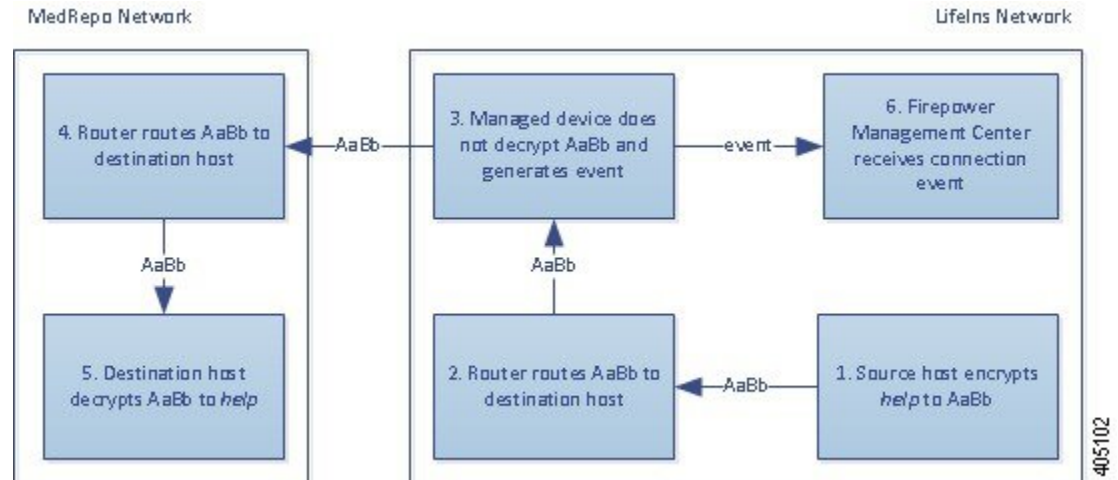
次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (help) を送信します。クライアントがこれを暗号化 (AaBb) し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはトラフィックを復号化しません。
アクセスコントロールポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。

5. 契約審査部門のサーバは、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (help) に復号します。
6. Firepower Management Centerが接続イベントを受信します。

インライン展開での復号されていない暗号化トラフィック

経験豊富な契約審査担当者から送信されるすべてのSSL暗号化トラフィックについては、管理対象デバイスはそのトラフィックを復号せずに許可し、接続のログを記録します。

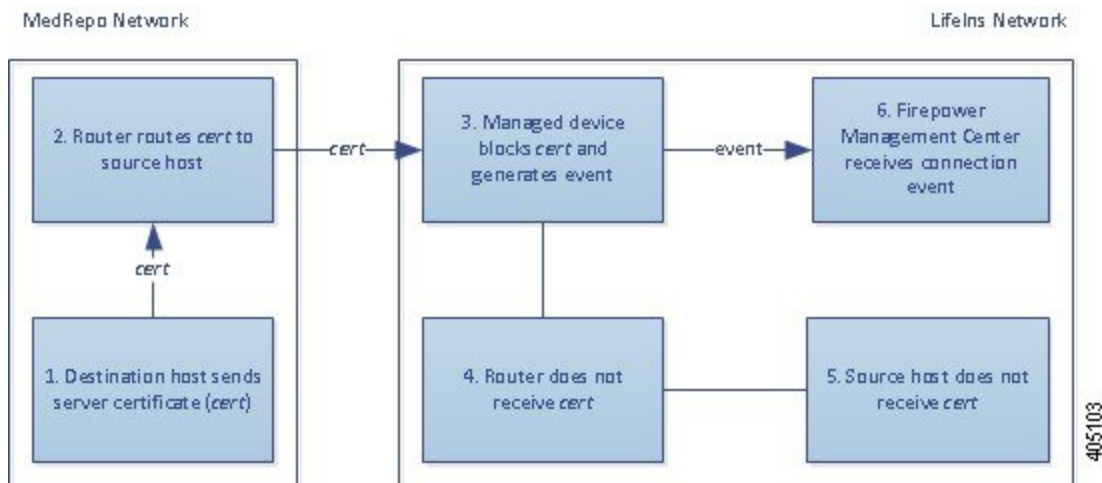


次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (help) を送信します。クライアントがこれを暗号化 (AaBb) し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはこのトラフィックを復号化しません。
アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (help) に復号します。
6. Firepower Management Centerが接続イベントを受信します。

インライン展開での暗号化トラフィックのブロック

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべての SMTPS 電子メールトラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。

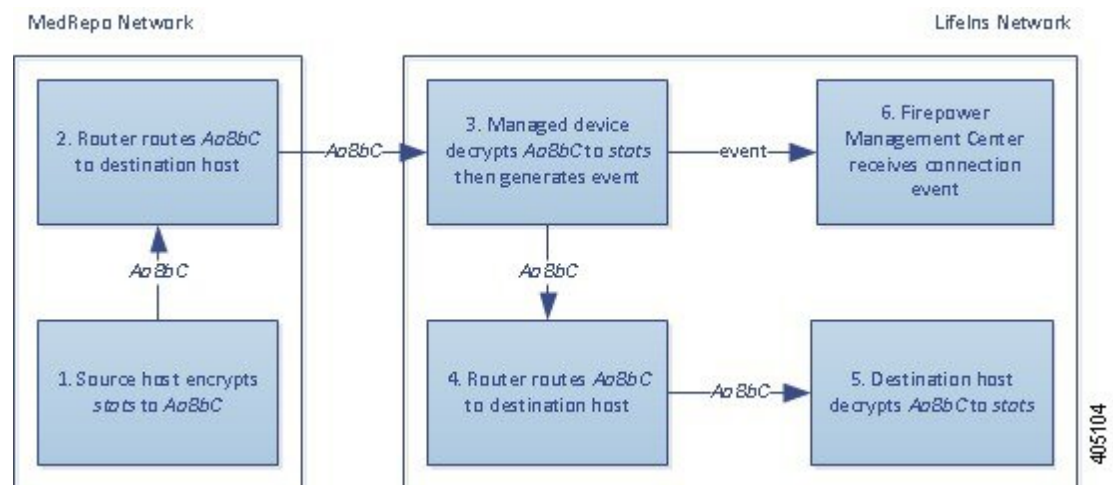


次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアントブラウザから SSL ハンドシェイクの確立要求を受信すると、SSL ハンドシェイクの次のステップとして、サーバ証明書 (cert) を LifeIns の契約審査担当者に送信します。
2. MedRepo のルータが証明書を受信し、これを LifeIns の契約審査担当者にルーティングします。
3. 管理対象デバイスは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. Firepower Management Center が接続イベントを受信します。

インライン展開での暗号化トラフィックの秘密キーによる検査

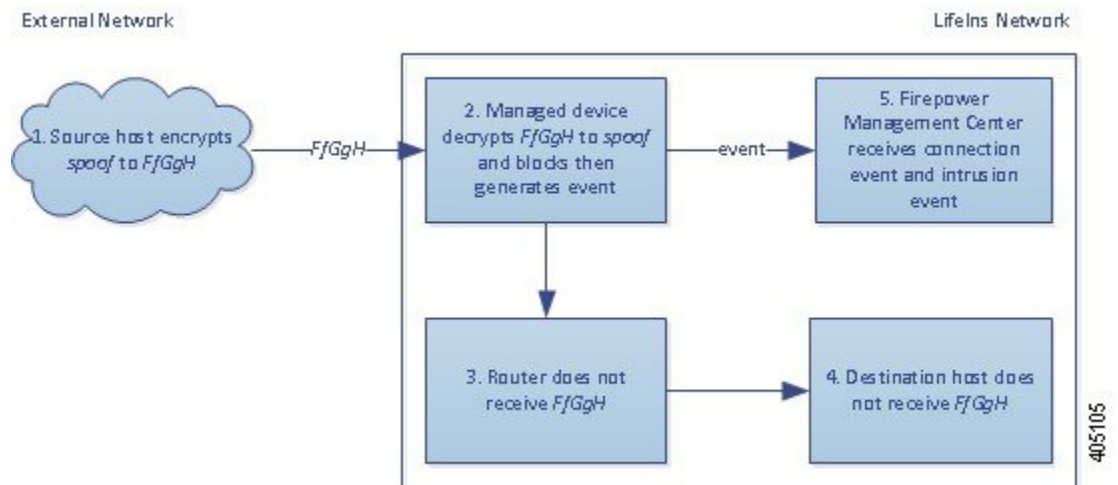
MedRepo から LifeIns の契約審査部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、アップロードされたサーバ秘密キーを使って取得されたセッションキーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (stats) を送信します。クライアントがこれを暗号化 (AaBbC) し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (stats) に復号化します。
アクセスコントロールポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック (AaBbC) を転送し、セッション終了後に接続イベントを生成します。
4. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報 (AaBbC) を受信し、これをプレーンテキスト (stats) に復号します。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。



次のステップが実行されます。

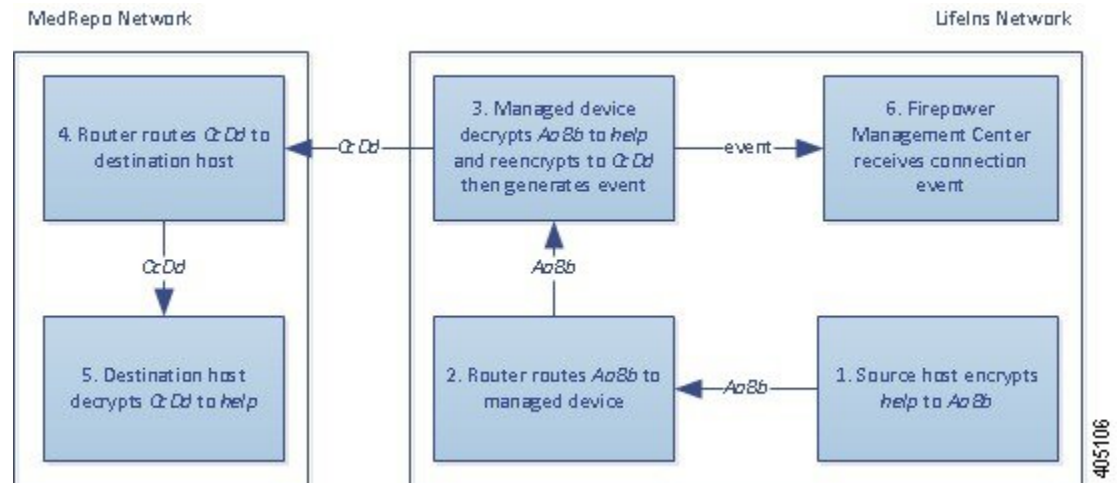
1. ユーザがプレーンテキストの要求 (spoof) を送信しますが、このトラフィックは変更されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化 (FfGgH) し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (spoof) に復号化します。
 アクセスコントロールポリシーは、カスタムの侵入ポリシーを使用して復号化されたトラフィックの処理を継続し、スプーフィング行為を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
3. 内部ルータは、ブロックされたトラフィックを受信しません。
4. 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。
5. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

インライン展開での暗号化トラフィックの再署名済み証明書による検査

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、再署名されたサーバ証明書を使って取得されたセッションキーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。



- (注) インライン展開においてサーバ証明書の再署名によりトラフィックを復号化する場合、デバイスは中間者 (man-in-the-middle) として機能します。ここでは2つの SSL セッションが作成され、1つはクライアントと管理対象デバイスの間、もう1つは管理対象デバイスとサーバの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。



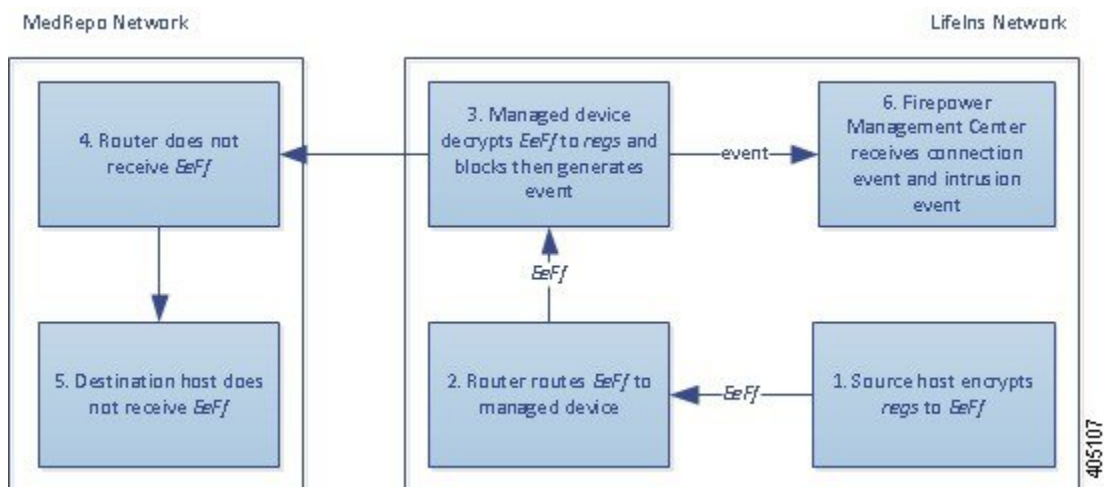
次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (help) を送信します。クライアントがこれを暗号化 (AaBb) し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (help) に復号します。
アクセスコントロールポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。不適切な要求は検出されません。デバイスはトラフィックを再暗号化 (CcDd) して、送信を許可します。セッション終了後、接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報 (CcDd) を受信し、これをプレーンテキスト (help) に復号します。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。



- (注) 再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメインルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアにCA証明書を追加します。

これに対し、規制要件を満たさない情報を含んでいる復号トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。



次のステップが実行されます。

1. ユーザが規制要件に準拠していない要求をプレーンテキスト (regs) で送信します。クライアントがこれを暗号化 (EeFf) し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (regs) に復号します。
 アクセスコントロールポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、不適切な要求を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
4. 外部ルータは、ブロックされたトラフィックを受信しません。
5. リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。

SSL の履歴

| 機能 | バージョン (Version) | 詳細 (Details) |
|--------------------|-----------------|---|
| SSLハードウェアアクセラレーション | 6.2.3 | 特定の管理対象デバイスモデルでは、パフォーマンスが向上する、ハードウェアでのSSL暗号化および復号が実行されます。 |

| 機能 | バージョン (Version) | 詳細 (Details) |
|------------------|-----------------|---|
| カテゴリとレピュテーションの条件 | 6.2.2 | カテゴリ/レピュテーションの条件を使用したアクセス コントロール ルールまたは SSL ルール。 |
| SafeSearch | 6.1.0 | <ul style="list-style-type: none"> • SSL ポリシーにより復号され、その後アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルトアクションによりブロック (またはインタラクティブにブロック) された接続については、HTTP 応答ページが表示されます。このような場合、システムは応答ページを暗号化して、再暗号化された SSL ストリームの最後にそれを送信します。 • SafeSearch により好ましくないコンテンツがフィルタリングされ、成人向けサイトの検索が停止されます。 |
| SSL | - | 導入された機能。 |