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。

トラフィックの復号の概要

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。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。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が判定されます。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
- 暗号化された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、システムでは、それ以上のインスペクションを行わずに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、また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アプライアンス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）、およびディスカバリ（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 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 *1*：*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 *2*：*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 ヵ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。

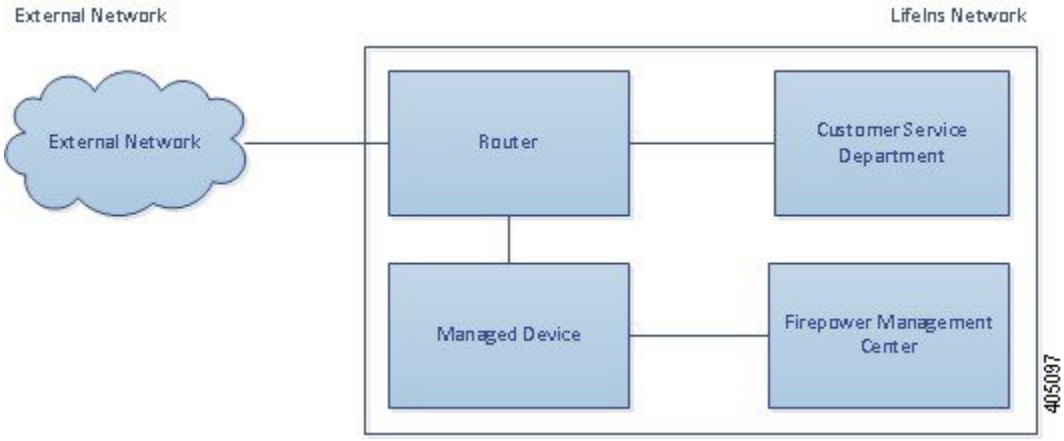
パッシブ展開でのトラフィックの復号

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ミラーリングします。

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 インスペクションの設定を次のように行います。

- 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

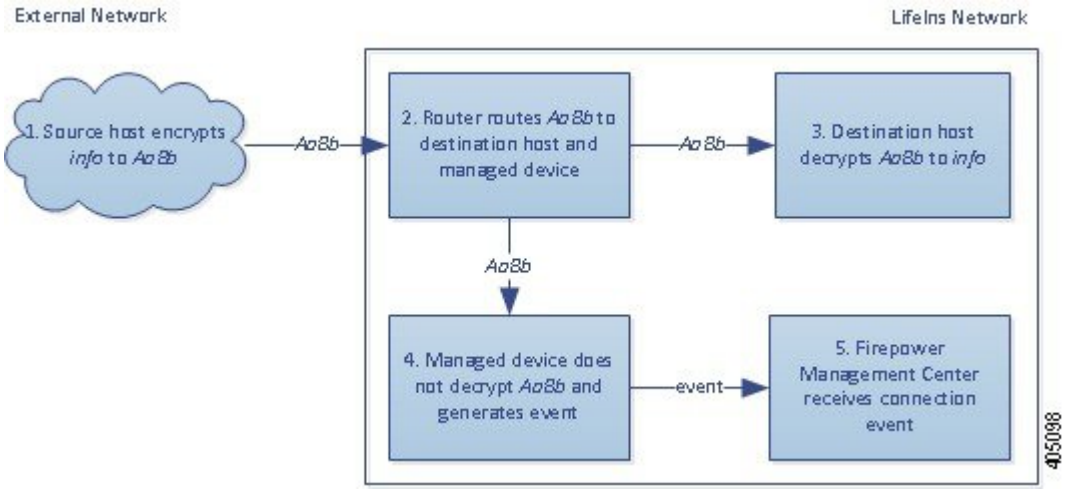
さらに、復号された申請フォーム トラフィック中に偽の申請データが含まれていないかを検査し、検出された場合はログに記録するためのアクセス コントロールも設定します。

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。管理対象デバイスが、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。



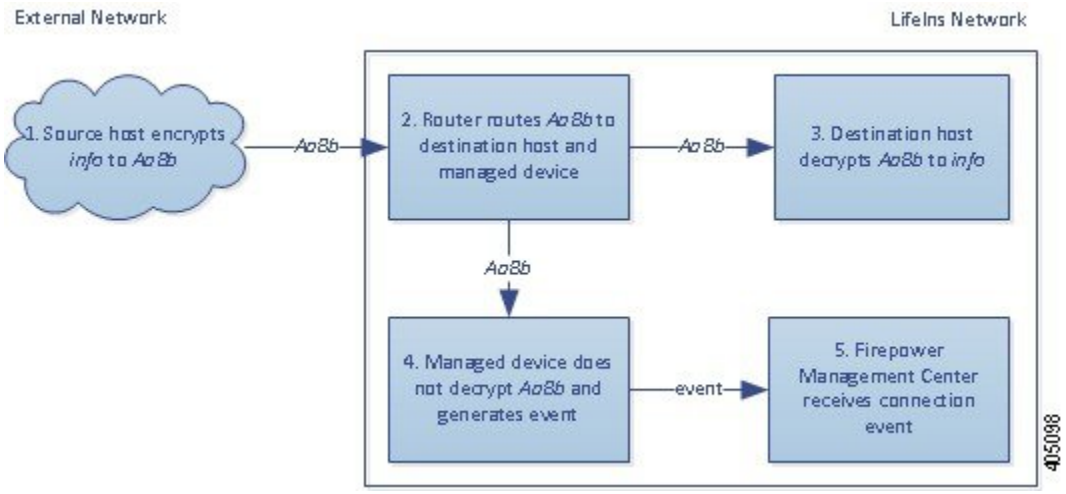
次のステップが実行されます。

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（`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. 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（`AaBb`）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（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. 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（AaBb）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。

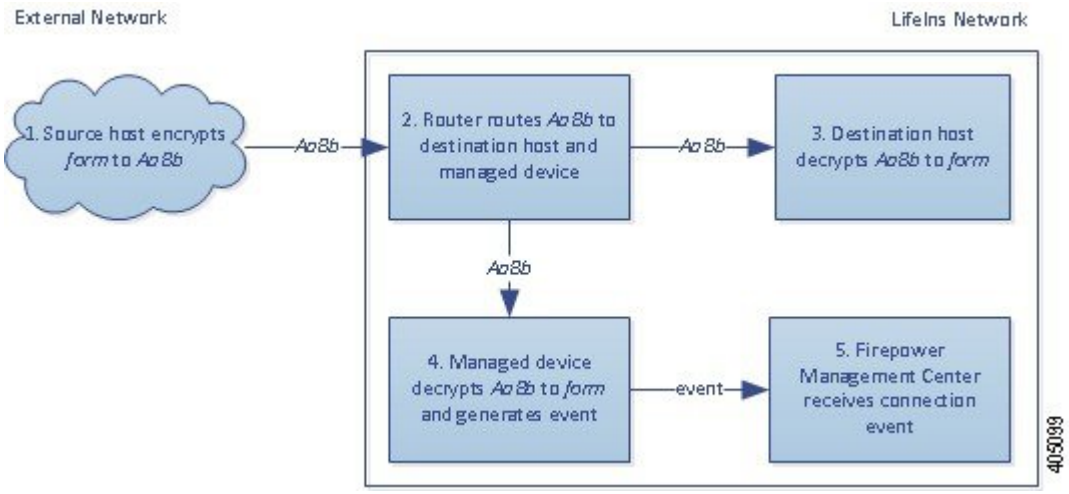
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerが接続イベントを受信します。

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。

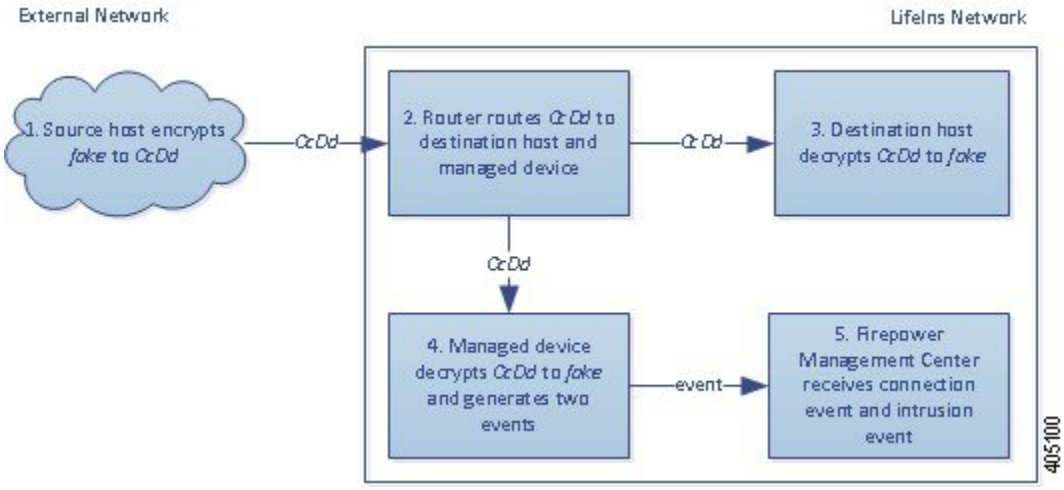


次のステップが実行されます。

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. 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（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。

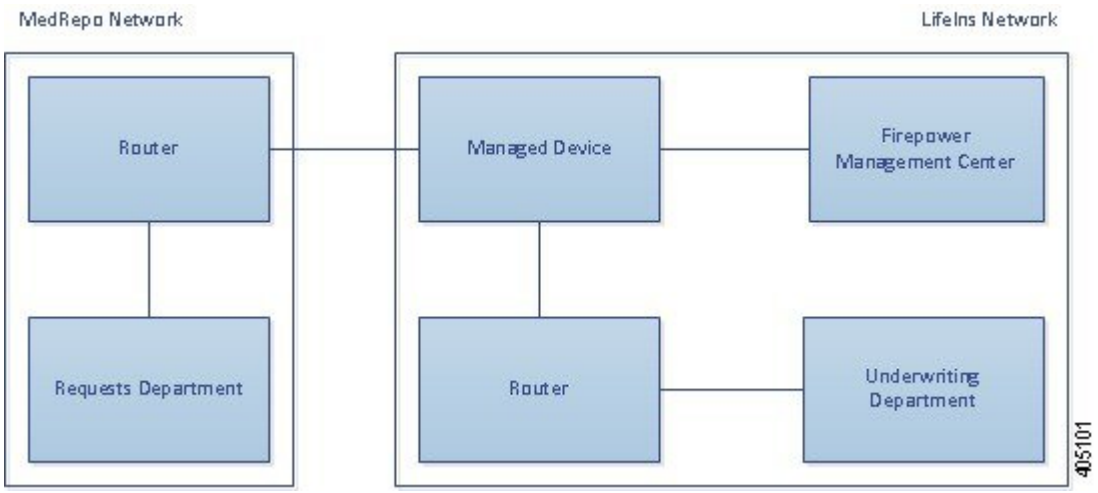
インライン展開でのトラフィックの復号

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。管理対象デバイスがその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、また管理元の 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。

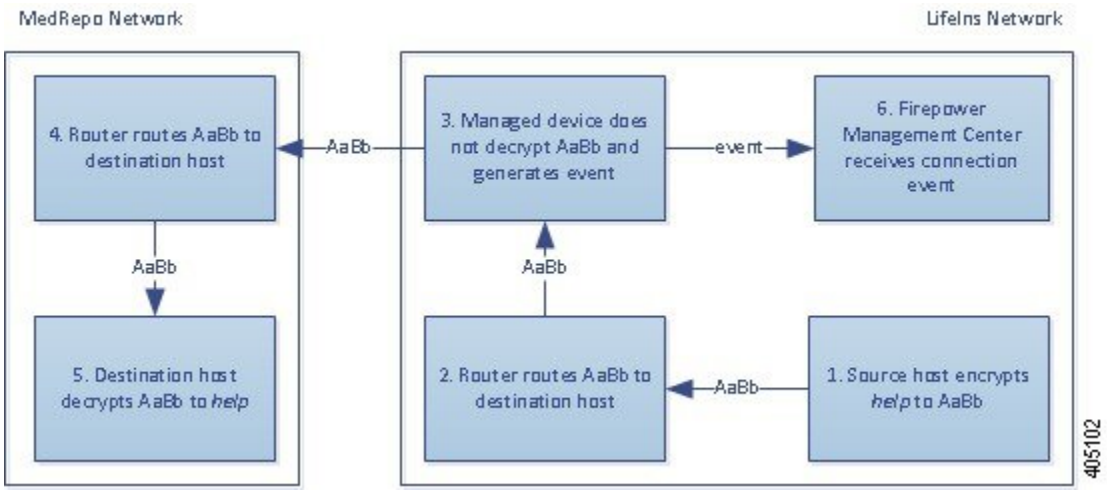
- 復号トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する
- 規制に準拠しない情報を含んでいる復号トラフィックをブロックし、不適切な情報をログに記録する
- 他の暗号化および復号されたトラフィックをすべて許可する

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。

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。管理対象デバイスが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基づいて、システムが接続のログへの記録とトラフィックの処理を行います。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。



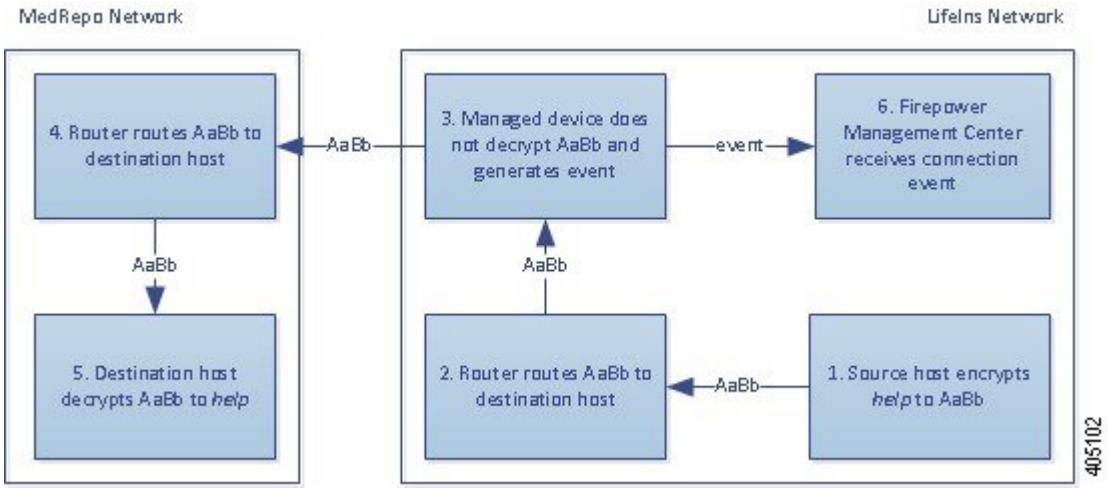
次のステップが実行されます。

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。



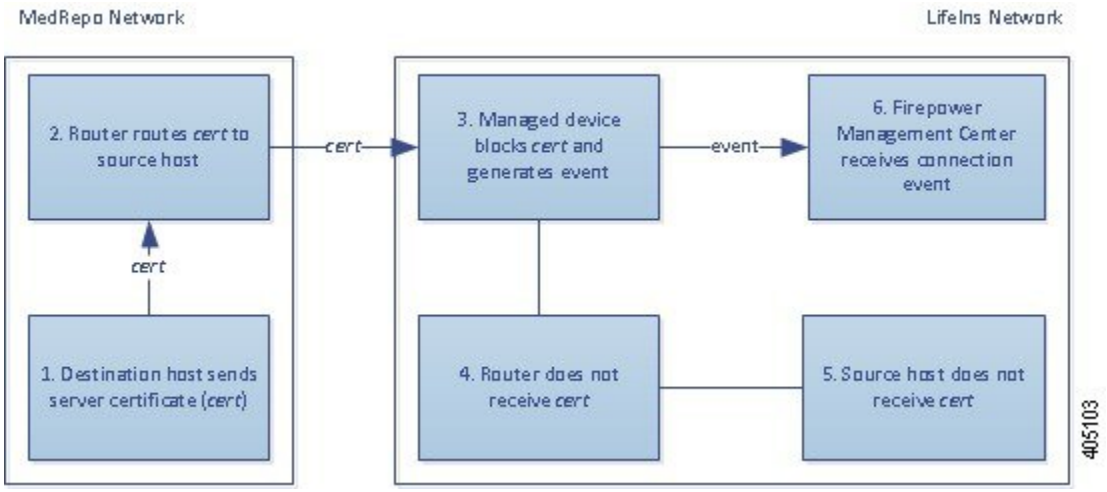
次のステップが実行されます。

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。

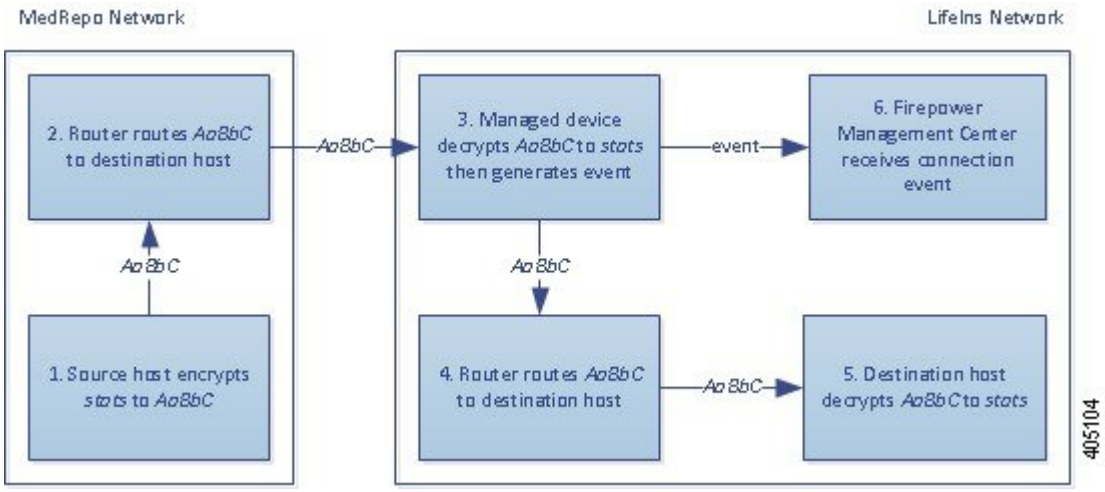


次のステップが実行されます。

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。

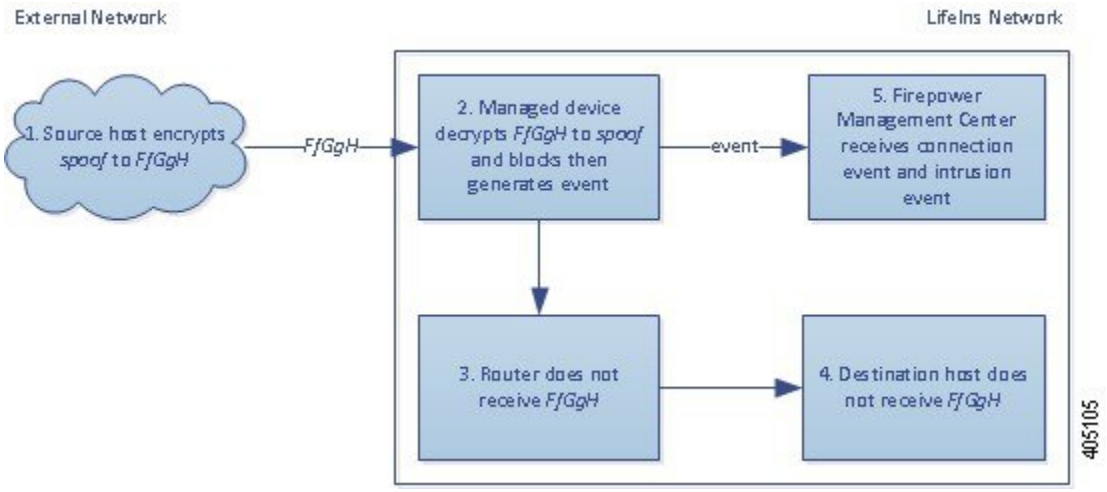


次のステップが実行されます。

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。

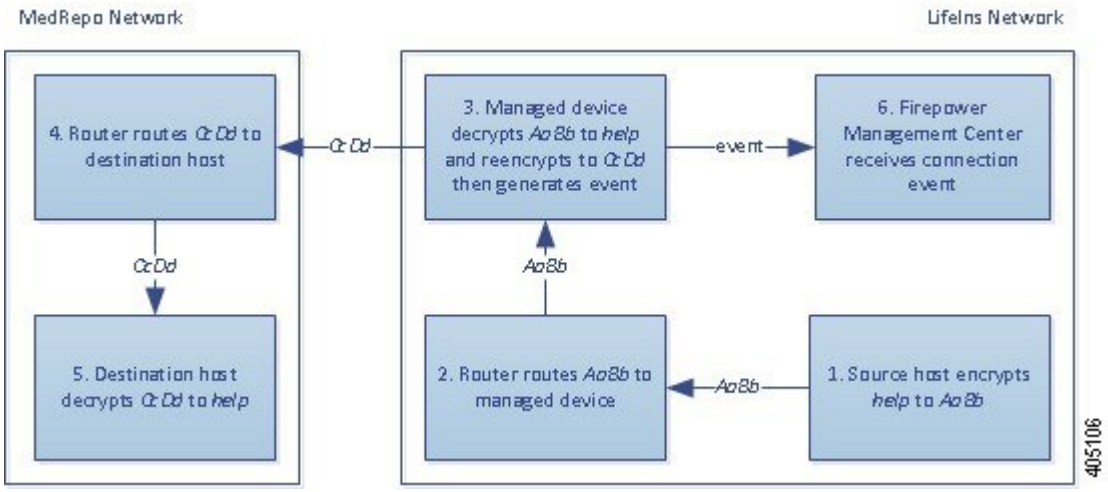
1. ユーザがプレーン テキストの要求（spoof）を送信しますが、このトラフィックは改変されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化（FfGgH）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（spoof）に復号します。

   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、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。



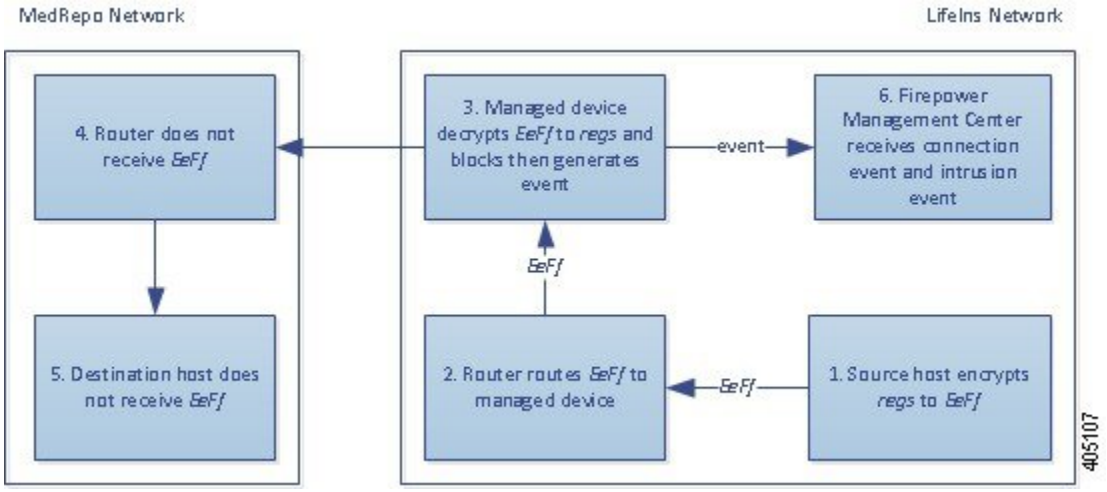
次のステップが実行されます。

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。