CHAPTER 19

トラフィック復号の概要

デフォルトでは、セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックは検査されません。アクセス コントロールの一部として *SSL インスペクション*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 コントロールで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。

システムで TCP 接続での SSL または TLS ハンドシェイクが検出されると、そのトラフィックを復号化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。

- 暗号化されたトラフィックをブロックし、オプションで 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

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、または SSL インスペクションが設定されていない場合は、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。詳細については、アクセス コントロール ルールの作成および編集（14-3 ページ）およびSSL プリプロセッサの使用（27-77 ページ）を参照してください。

システムによるトラフィックの復号化が可能な場合は、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、復号化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化します。

- 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、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。

復号化されたトラフィックに対しては、暗号化されていないトラフィックと同じ処理と分析が施されます。これには、ネットワーク、レピュテーション、ユーザ ベースのアクセス コントロール、侵入の検知と防止、高度なマルウェア防御、およびディスカバリが該当します。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、トラフィックは再暗号化されて宛先ホストに渡されます。

(注)　トラフィックのブロックや発信トラフィックの復号など、いくつかの SSL インスペクション アクションはトラフィックのフローを変更します。これらのアクションを実行できるのは、インラインに配置されたデバイスです。パッシブまたはタップ モードで配置されたデバイスは、トラフィック フローを変更できません。ただし、これらのデバイスでも着信トラフィックを復号することは可能です。詳細については、例: パッシブ展開でのトラフィック復号（19-6 ページ）を参照してください。

詳細については、次の項を参照してください。

- SSL インスペクションの要件（19-2 ページ）
- SSL インスペクション アプライアンス展開の分析（19-5 ページ）

SSL インスペクションの要件

ライセンス： 機能に応じて異なる

サポートされるデバイス： シリーズ 3

SSL インスペクションは、特定のアプライアンス モデルでのみサポートされます。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。

SSL インスペクションの設定に使用できる機能やアクションは、各自のユーザ ロールに依存します。さまざまな管理者やアナリスト用のユーザ ロールが事前定義されていますが、それ以外にも特殊なアクセス権限を持たせたカスタム ユーザ ロールを作成できます。

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 防御センターにアップロードする必要があります。

詳細については、次の項を参照してください。

- SSL インスペクションをサポートするアプライアンスの展開（19-3 ページ）
- SSL インスペクションに必要なライセンスの特定（19-3 ページ）
- カスタム ユーザ ロールによる SSL インスペクション展開の管理（19-4 ページ）
- SSL ルールを設定するために必要な情報の収集（19-5 ページ）

SSL インスペクションをサポートするアプライアンスの展開

ライセンス： 任意（Any）

サポートされるデバイス： シリーズ 3

SSL インスペクションにはシリーズ 3 デバイスが必要です。

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。

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。詳細については、SSL インスペクション アプライアンス展開の分析（19-5 ページ）を参照してください。

SSL インスペクションに必要なライセンスの特定

ライセンス： 機能に応じて異なる

ライセンスによっては、いくつかの条件を組み合わせて暗号化トラフィックの処理方法を決定できます。防御センターでのライセンスに関係なく SSL ポリシーを作成できますが、一部の SSL インスペクションに関しては、ポリシーを適用する前に特定のライセンスが必要な機能をターゲット デバイス上で有効にしておく必要があります。防御センターでは、ご使用の展開環境でサポートされない機能を示すために、警告アイコン（⚠）および確認ダイアログ ボックスを使用します。警告アイコンの上にポインタを置くと詳細が表示されます。

アクセス コントロール ポリシーの一部として管理対象デバイスに SSL ポリシーを適用すると、SSL ポリシーで復号化されたトラフィックがこのアクセス コントロール ポリシーにより検査されます。アクセス コントロールのライセンスの詳細については、アクセス コントロールのライセンスおよびロール要件（12-2 ページ）を参照してください。

次の表に、アクセス コントロール ポリシーの一部として SSL ポリシーを適用するためのライセンス要件を示します。

表 19-1　SSL インスペクションのライセンスとモデルの要件

SSL ポリシーの機能	ライセンス	サポートされる防御センター	サポートされるデバイス
ゾーン、ネットワーク、VLAN、ポート、または SSL 関連の条件に基づいて暗号化トラフィックを処理する	任意（Any）	任意（Any）	シリーズ 3
位置情報のデータを使用して暗号化トラフィックを処理する	FireSIGHT	任意（DC500 を除く）	シリーズ 3

表 19-1　SSL インスペクションのライセンスとモデルの要件（続き）

SSL ポリシーの機能	ライセンス	サポートされる防御センター	サポートされるデバイス
アプリケーションまたはユーザの条件を使用して暗号化トラフィックを処理する	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーションデータを使用して暗号化されたトラフィックをフィルタ処理する	URL フィルタリング	DC500 を除くいずれか	シリーズ 3

カスタム ユーザ ロールによる SSL インスペクション展開の管理

ライセンス： 任意（Any）

カスタム ユーザ ロールの管理（61-57 ページ）で説明しているように、カスタム ユーザ ロールを作成して専用のカスタム特権を割り当てることができます。カスタム ユーザ ロールには、メニューベースのアクセス許可およびシステム アクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザ ロールを基に作成したりできます。次の表は、SSL インスペクションの設定と展開を行うためのユーザ権限を決定するロール アクセス許可を示しています。

表 19-2　SSL インスペクション関連のユーザ ロールのアクセス許可

ユーザのアクセス許可	説明
オブジェクト マネージャ（Object Manager）	SSL インスペクション関連のオブジェクトを作成、変更、削除できます
SSL	SSL ポリシーのレポートを生成し、SSL ポリシーまたはポリシー リビジョンの比較ができます
SSL ポリシーの変更（Modify SSL Policy）	SSL ポリシーを表示、作成、変更、削除でき、管理者ルール カテゴリやルート ルール カテゴリに含まれない SSL ルールを作成、変更、削除できます
管理者ルールの変更（Modify Administrator Rules）	管理者ルール カテゴリの SSL ルールを作成、変更、削除できます
ルート ルールの変更（Modify Root Rules）	ルート ルール カテゴリの SSL ルールを作成、変更、削除できます
SSL ポリシーの適用（Apply SSL Policy）	アクセス コントロール ポリシーの適用時に、関連付けられた SSL ポリシーを適用できます
アクセス コントロール リスト（Access Control List）	アクセス コントロール ポリシーの一覧を表示できます
アクセス コントロール ポリシーの変更（Modify Access Control Policy）	アクセス コントロール ポリシーに SSL ポリシーを関連付けることができます
アクセス コントロール ポリシーの適用（Apply Access Control Policies）	SSL ポリシーが関連付けられたアクセス コントロール ポリシーを適用できます

詳細については、アクセス コントロールのライセンスおよびロール要件（12-2 ページ）を参照してください。

SSL ルールを設定するために必要な情報の収集

ライセンス： 機能に依存

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。次の表に示す情報を収集しておく必要があります。

表 19-3　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

詳細については、SSL ルールを使用したトラフィック復号の調整（22-1 ページ）を参照してください。

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。トラフィックを復号する場合は、次の表に示す情報を収集しておく必要があります。

表 19-4　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。

詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（21-9 ページ）を参照してください。

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。詳細については、再利用可能なオブジェクトの管理（3-1 ページ）を参照してください。

SSL インスペクション アプライアンス展開の分析

ライセンス： 機能に依存

サポートされるデバイス： シリーズ 3

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、単一のシリーズ 3 管理対象デバイスをパッシブ展開する。
- 契約審査部門では、単一のシリーズ 3 管理対象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防御センターで管理する

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。

詳細については、次の項を参照してください。

- 例:パッシブ展開でのトラフィック復号（19-6 ページ）
- 例:インライン展開でのトラフィック復号（19-11 ページ）

例:パッシブ展開でのトラフィック復号

ライセンス: 機能に依存

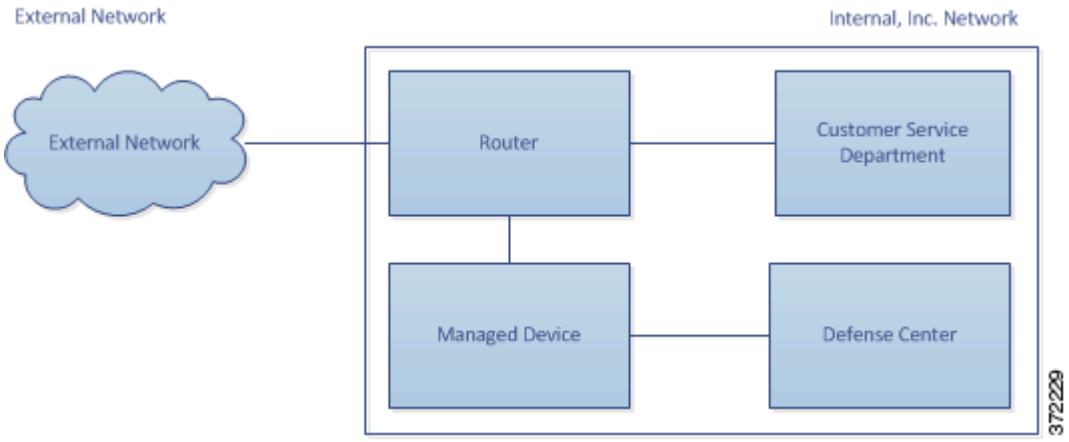
サポートされるデバイス: シリーズ 3

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 のカスタマー サービス部門では、管理対象デバイスのパッシブ展開を計画しています。次の図は、LifeIns のパッシブ展開を示しています。



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。

管理する防御センターでは、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 インスペク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。

詳細については、次のトピックを参照してください。

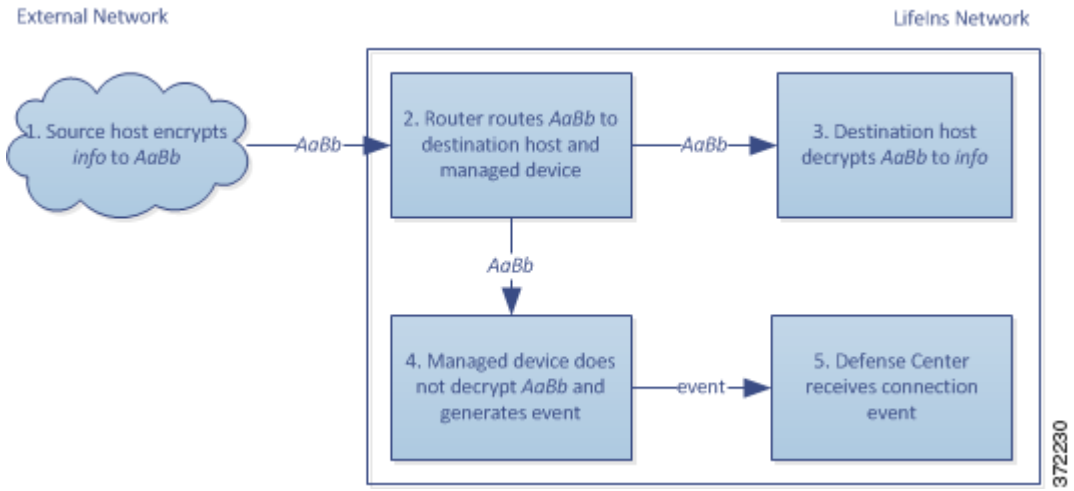
- パッシブ展開で暗号化トラフィックをモニタする（19-7 ページ）
- パッシブ展開で暗号化トラフィックを復号しない（19-8 ページ）
- パッシブ展開で暗号化トラフィックを秘密キーで検査する（19-9 ページ）

パッシブ展開で暗号化トラフィックをモニタする

ライセンス： 任意（Any）

サポートされるデバイス： シリーズ 3

システムは、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。次の図は、暗号化トラフィックをシステムがモニタする状況を示しています。



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。

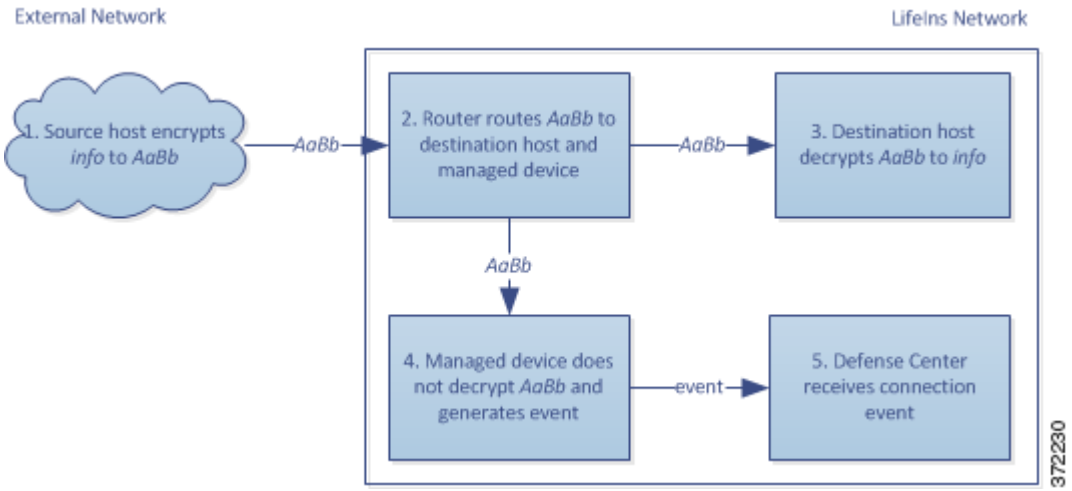
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. 防御センターが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを復号しない

ライセンス： 任意（Any）

サポートされるデバイス： シリーズ 3

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は復号されずに許可され、接続のログが記録されます。次の図は、追加の検査を行わずに暗号化トラフィックを許可する状況を示しています。



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. 防御センターが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを秘密キーで検査する

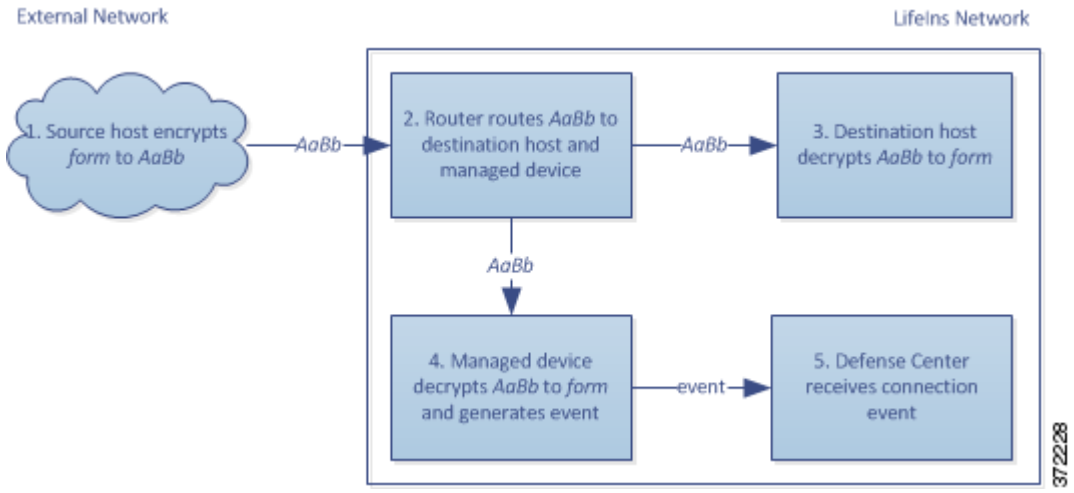
ライセンス： 任意（Any）

サポートされるデバイス： シリーズ 3

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。次の図は、既知の秘密キーによりトラフィックを復号する状況を示しています。

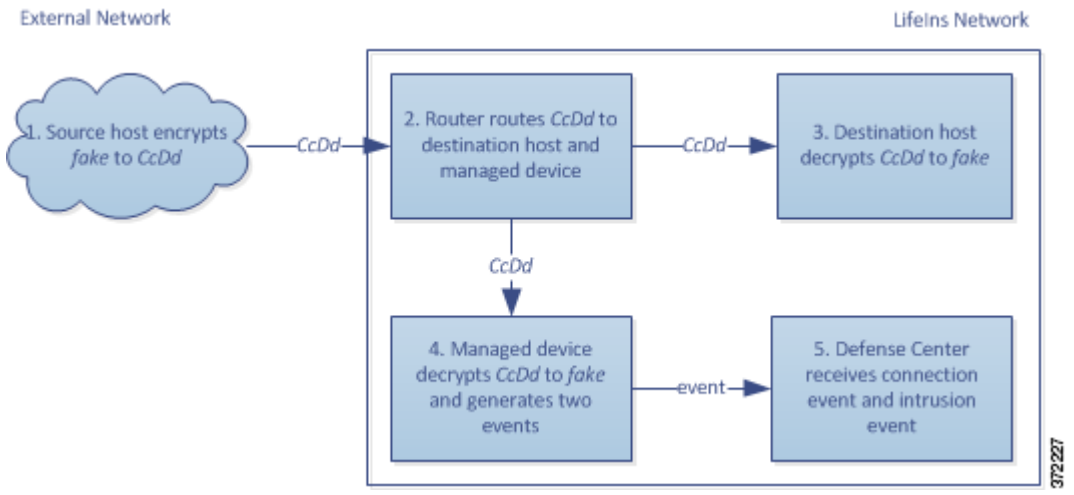


次のステップが実行されます。

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. 防御センターは、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。次の図は、既知の秘密キーにより、偽の申請データを含んでいる着信トラフィックを復号する状況を示しています。



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. 防御センターは、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。

例:インライン展開でのトラフィック復号

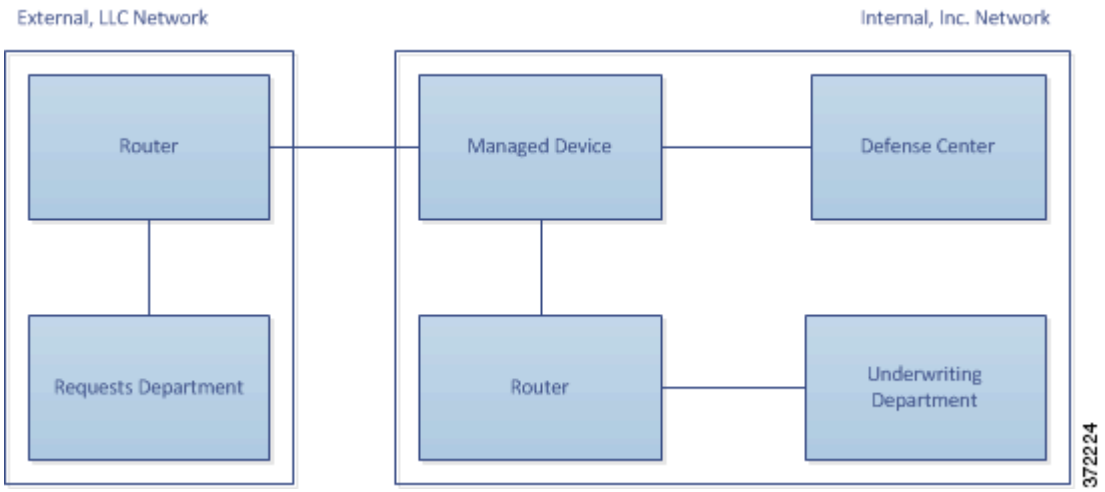
ライセンス： 機能に依存

サポートされるデバイス： シリーズ 3

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。次の図は、LifeIns のインライン展開を示しています。



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、管理している防御センター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。

管理する防御センターでは、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 インスペクションの設定を行います。

- 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。

詳細については、次のトピックを参照してください。

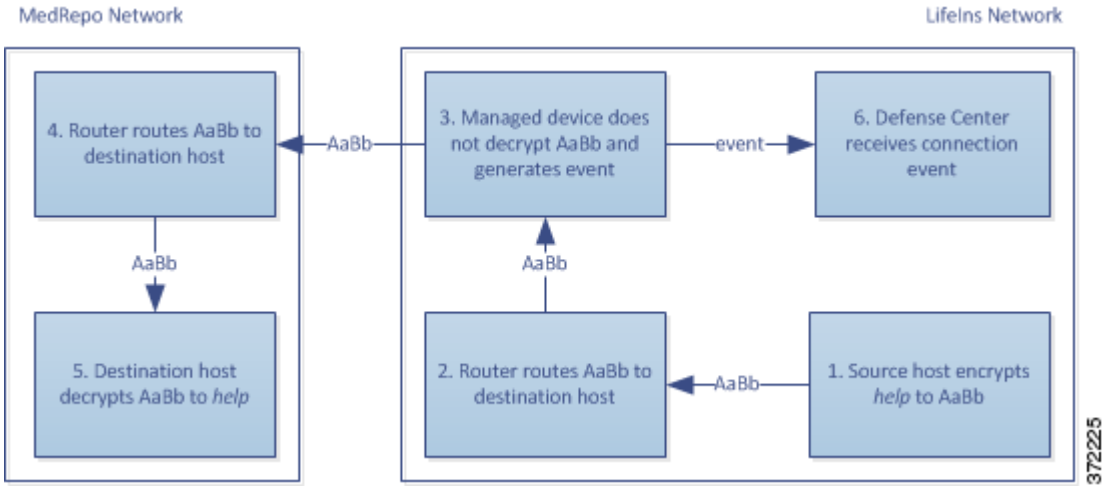
- インライン展開で暗号化トラフィックをモニタする（19-13 ページ）
- インライン展開で特定ユーザからの暗号化トラフィックを許可する（19-13 ページ）
- インライン展開で暗号化トラフィックをブロックする（19-14 ページ）
- インライン展開で暗号化トラフィックを秘密キーで検査する（19-15 ページ）
- インライン展開で特定ユーザの暗号化トラフィックを、再署名された証明書で検査する（19-17 ページ）

インライン展開で暗号化トラフィックをモニタする

ライセンス： 任意（Any）

サポートされるデバイス： シリーズ 3

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。次の図は、暗号化トラフィックをシステムがモニタする状況を示しています。



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。

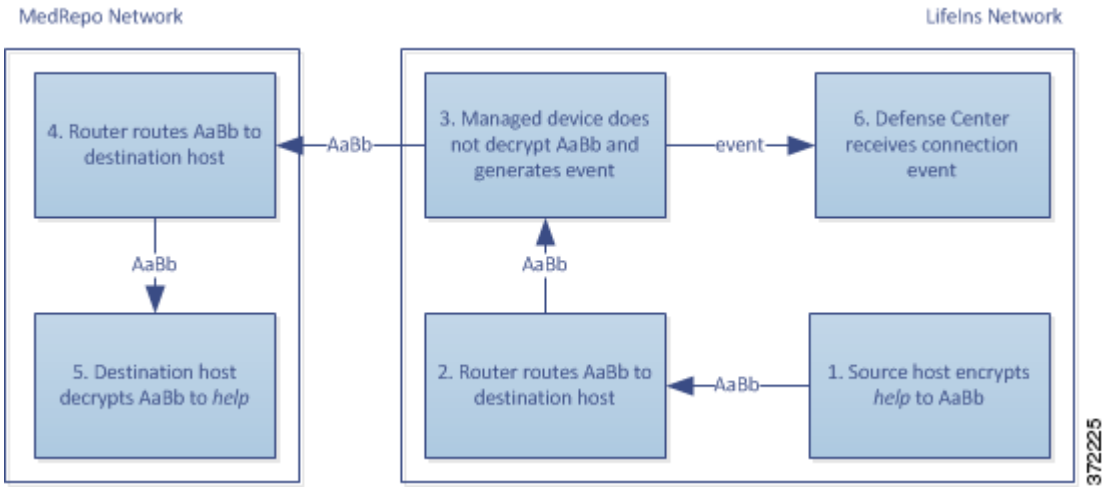
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`help`）に復号します。
6. 防御センターが接続イベントを受信します。

インライン展開で特定ユーザからの暗号化トラフィックを許可する

ライセンス： Control

サポートされるデバイス： シリーズ 3

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は復号されずに許可され、接続のログが記録されます。次の図は、暗号化トラフィックをシステムが許可する状況を示しています。



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。

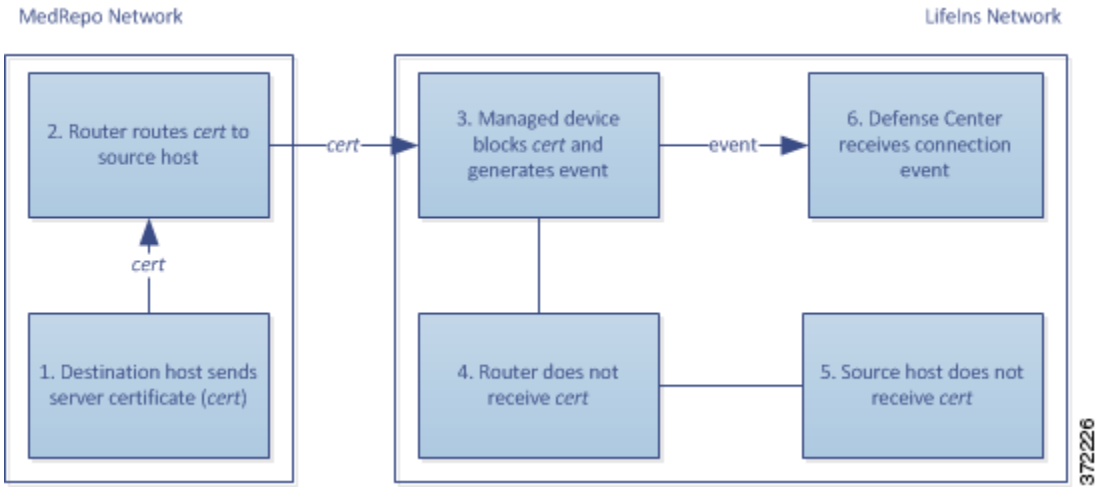
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`help`）に復号します。
6. 防御センターが接続イベントを受信します。

インライン展開で暗号化トラフィックをブロックする

ライセンス： 任意（Any）

サポートされるデバイス： シリーズ 3

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。次の図は、暗号化トラフィックをシステムがブロックする状況を示しています。



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. 防御センターが接続イベントを受信します。

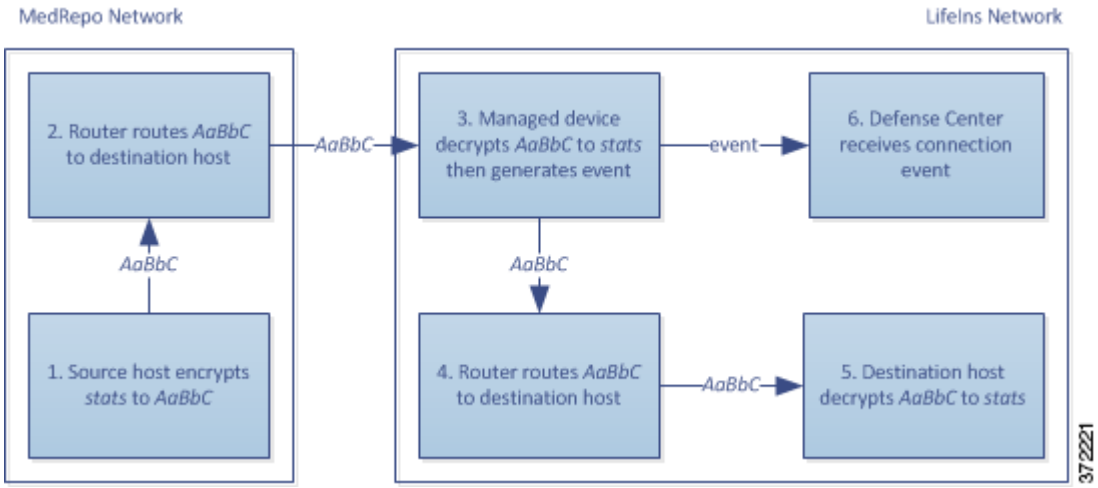
インライン展開で暗号化トラフィックを秘密キーで検査する

ライセンス： 任意（Any）

サポートされるデバイス： シリーズ 3

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。

次の図は、既知の秘密キーを使用して暗号化トラフィックを復号した後、アクセス コントロールを使用してトラフィックを検査して、復号されたトラフィックを許可する状況を示しています。

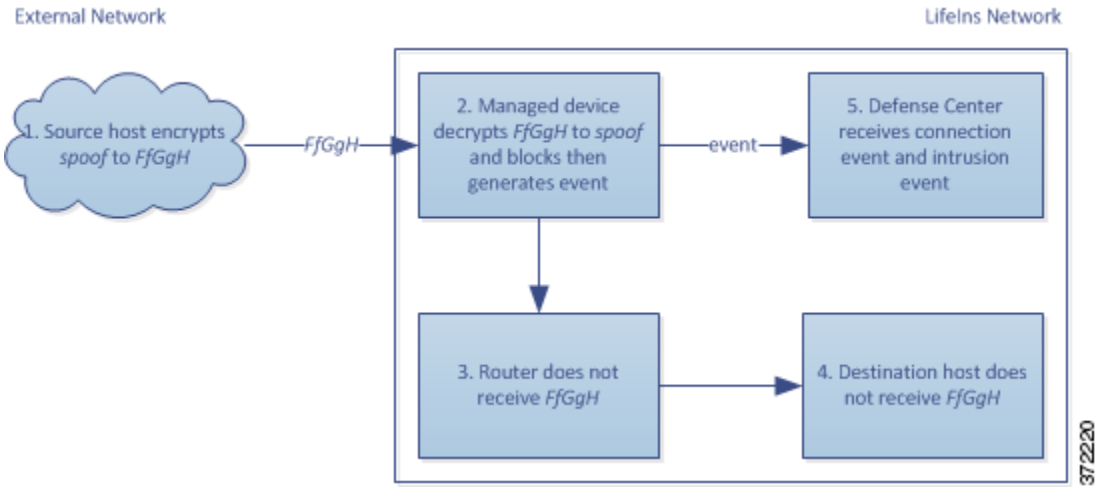


次のステップが実行されます。

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. 防御センターは、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。次の図は、既知の秘密キーを使用して暗号化トラフィックを復号した後、アクセス コントロール ポリシーを使用してトラフィックを検査して、復号されたトラフィックをブロックする状況を示しています。



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、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. 防御センターは、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。

インライン展開で特定ユーザの暗号化トラフィックを、再署名された証明書で検査する

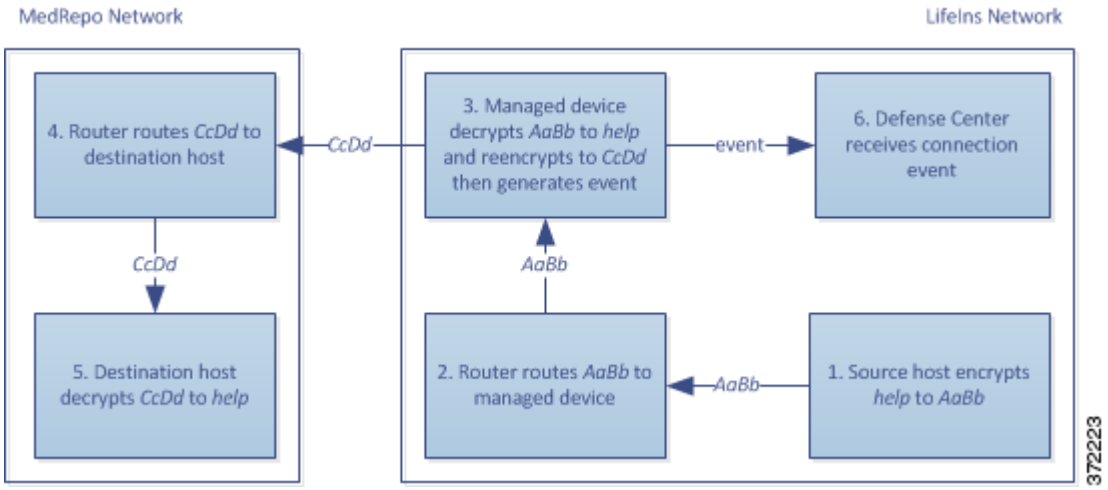
ライセンス： Control

サポートされるデバイス： シリーズ 3

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、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をつなぐ、2 つの SSL セッションが作成されます。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。

次の図は、再署名されたサーバ証明書と秘密キーを使用して暗号化トラフィックを復号化した後、アクセス コントロールを使用してトラフィックを検査して、復号化されたトラフィックを許可する状況を示しています。



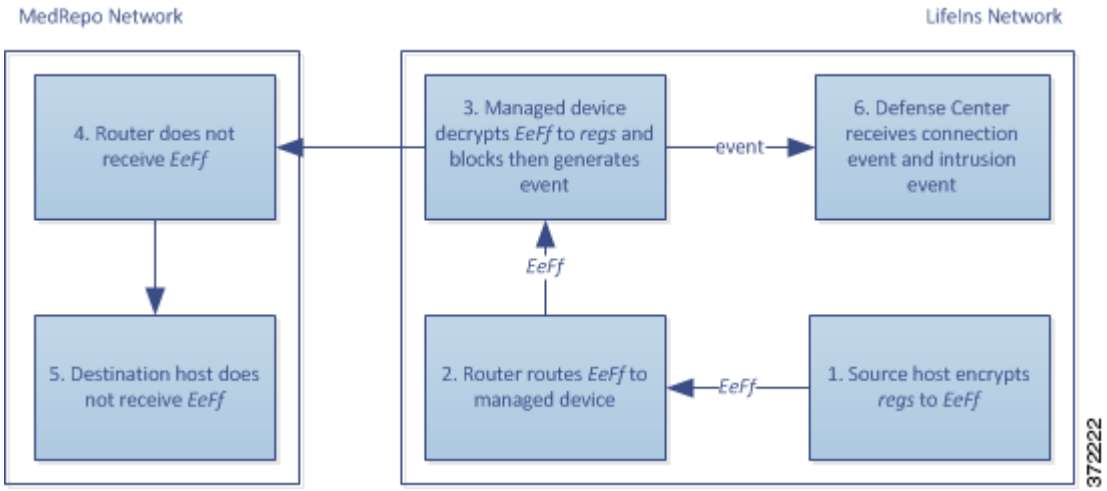
次のステップが実行されます。

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。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. 防御センターは、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。次の図は、再署名されたサーバ証明書と秘密キーを使用して暗号化トラフィックを復号した後、アクセス コントロール ポリシーを使用してトラフィックを検査して、復号されたトラフィックをブロックする状況を示しています。



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、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. 防御センターは、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。