トラフィック復号の概要

以下のトピックでは TLS/SSL（Transport Layer Security/Secure Sockets Layer）インスペクションの概要を示し、TLS/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。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

例外は SSL ポリシーです。FMC 設定オプションは **[Policies]** > **[Access Control]** > **[SSL]** となるため、これらのポリシーは TLS および SSL のトラフィックのルールを定義するために使用されますが、「SSL ポリシー」という用語を使用します。

SSL プロトコルと TLS プロトコルの詳細については、「SSL と TLS：その違いとは（SSL vs. TLS - What's the Difference?）」を参照してください。

トラフィック復号について

デフォルトでは、Firepower システムは SSL（Secure Socket Layer）プロトコルまたはその後継である TLS（Transport Layer Security）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。*TLS/SSL* インスペクションを使用すると、暗号化トラフィックを検査せずにブロックしたり、暗号化または復号化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することができます。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。

TLS/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、サブポリシーと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ると、システムでは、この SSL ポリシーを使用して暗号化セッションを処理し、その後でそれらの暗号化セッションをアクセス コントロール ルールで評価します。TLS/SSL インスペクションを設定していない場合、またはデバイスで SSL インスペクションをサポートしていない場合は、アクセス コントロール ルールですべての暗号化トラフィックが処理されます。

TLS/SSL インスペクションの設定で暗号化トラフィックの通過が許可されている場合、アクセス コントロール ルールによっても暗号化トラフィックが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。

システムで TCP 接続での TLS/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化する。外部ホストがネットワーク上のサーバとの TLS/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 TLS/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。

（注） 管理対象デバイスが暗号化されたトラフィックを処理する場合にのみ、復号ルールをセットアップします。復号ルールには、パフォーマンスに影響を及ぼす可能性があるオーバーヘッドの処理が必要です。

Firepower システムは現在、TLS バージョン 1.3 の暗号化または復号化をサポートしていません。ユーザが TLS 1.3 暗号化をネゴシエートする Web サイトにアクセスすると、Web ブラウザに次のようなエラーが表示されることがあります。

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

この動作を制御する方法の詳細については、Cisco TAC にお問い合わせください。

TLS/SSL ハンドシェイク処理

このマニュアルでは、*TLS/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。

インライン展開では、Firepower システムは TLS/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。TLS/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。

TLS/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 TLS/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。

TLS/SSL 復号化を設定した場合、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 TLS/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 : TLS/SSL* ルールの条件のデータの可用性

TLS/SSL ルール条件	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）
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 TLS/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）。
- 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、Cisco TAC 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、TLS/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 TLS/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。

（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、TLS/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。復号できる暗号スイートの現在のリストについては、Cisco TAC 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
インライン展開での再署名証明書を使用した暗号化トラフィック インスペクション （30 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 TLS/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、TLS/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 TLS/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）
TLS/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、TLS/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）
TLS/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、TLS/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。

アクション：復号 - 既知のキー（Decrypt - Known Key）

管理対象デバイスは、以前に Firepower Management Center にインポートした内部証明書オブジェクトをサーバ証明書データに一致させようとします。内部証明書オブジェクトは作成できないため、また、秘密キーを所有する必要があるため、既知のキー復号化を使用しているサーバを所有していることを想定しています。

証明書が既知の証明書と一致した場合、TLS/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、TLS/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。

クライアントとの初回接続と後続の接続の間でサーバが証明書を変更した場合、将来の接続を復号化するには、Firepower Management Center に新しいサーバ証明書をインポートする必要があります。

（注） Firepower システムは RFC 7627 で定義されている Extended Master Secret 拡張機能をサポートしていないため、既知のキーを使用して復号を行うサーバ上ではこの拡張機能を無効にする必要があります。そうしないと、復号中に接続がリセットされ、接続エラーとなります。

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、サーバ証明書に以前にインポートまたは生成した認証局（CA）で再署名します。TLS/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、TLS/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。

TLS/SSLハードウェアの加速

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 Transport Layer Security/Secure Sockets Layer（TLS/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。

TLS/SSL のハードウェア アクセラレーションは、サポートするすべてのデバイスで自動的に有効になっています（FTD コンテナ インスタンス が有効になっているデバイスを除く）。ネイティブ インスタンスのみが TLS/SSL ハードウェア アクセラレーションをサポートします。

サポート対象ハードウェア

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

- Firepower Threat Defense を搭載した Firepower 2100
- Firepower Threat Defense を搭載した Firepower 4100/9300

Firepower 4100/9300 FTD コンテナ インスタンスでの のサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

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 TLS/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。

サポートしている機能 TLS/SSL ハードウェア アクセラレーション

TLS/SSL ハードウェア アクセラレーション でサポートしている機能は次のとおりです。

- IPv4-in-IPv4 tunneled protocols only are supported; other tunneled IP protocols are *not* supported.
- Generic Routing Encapsulation（GRE）トンネルでカプセル化された TLS/SSL トラフィックの復号化

サポートしていない機能 TLS/SSL ハードウェア アクセラレーション

TLS/SSL ハードウェア アクセラレーション でサポートしていない機能は次のとおりです。

- Managed devices where FTD コンテナ インスタンス is enabled.
- インスペクション エンジンが接続を維持するように設定されていて、インスペクション 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 TLS/SSL トラフィックはドロップされます。

  この動作はによって制御されます、**configure snort preserve-connection {enable | disable}** コマンド。

上記のいずれかの機能を使用する必要がある場合は、TLS/SSL ハードウェア アクセラレーションを無効にすることができます。

Enable または Disable TLS/SSLハードウェアの加速

管理対象デバイスで TLS/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	TLS/SSL ハードウェア アクセラレーションを有効にします。デバイスを再起動するように求められます。（デフォルトでは、イネーブル）。
ssl-hw-offload disable	TLS/SSL ハードウェア アクセラレーションを無効にします。デバイスを再起動するように求められます。

TLS/SSLハードウェアの加速 注意事項と制約事項

管理対象デバイスで TLS/SSL ハードウェア アクセラレーションが有効になっている場合は、次の点に留意してください。

HTTP のみのパフォーマンス

トラフィックを復号しない管理対象デバイスで TLS/SSL ハードウェア アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。トラフィックを復号しないデバイスでは TLS/SSL ハードウェア アクセラレーションを無効にすることをお勧めします。

Federal Information Processing Standards（FIPS）

TLS/SSL ハードウェア アクセラレーションと連邦情報処理標準（FIPS）が両方とも有効になっている場合は、次のオプションの接続が失敗します。

- サイズが 2048 バイト未満の RSA キー
- Rivest 暗号 4（RC4）
- Single Data Encryption Standard (single DES)
- Merkle–Damgard 5（MD5）
- SSL v3

セキュリティ認定準拠モードで動作するように Firepower Management Center と管理対象デバイスを設定すると、FIPS が有効になります。このモードで動作しているときに接続を許可するには、TLS/SSL ハードウェア アクセラレーションを無効にするか、よりセキュアなオプションを採用するように Web ブラウザを設定します。

詳細については、次を参照してください。

- TLS/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：TLS/SSLハードウェアの加速 （7 ページ）。
- FIPS でサポートされている暗号方式：SSL 設定について。
- セキュリティ認定準拠のモード。
- コモン クライテリア。

ハイ アベイラビリティ（HA）

ハイ アベイラビリティ（HA）の管理対象デバイスまたはクラスタ化管理対象デバイスがある場合は、管理対象デバイスごとに TLS/SSL ハードウェア アクセラレーションを有効にする必要があります。1 つのデバイスの TLS/SSL ハードウェア アクセラレーション構成は、HA ペアの他のデバイスとは共有されません。

TLS ハートビート

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS/SSL ハードウェア アクセラレーションが有効になっている管理対象デバイスが TLS ハートビート エクステンションを使用するパケットを扱うときは、管理対象デバイスは SSL ポリシーの [復号化不可のアクション（Undecryptable Actions）] の [復号化エラー（Decryption Errors）] の設定で指定されたアクションを行います。

- ブロック（Block）
- リセットしてブロック（Block with reset）

詳細については、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を参照してください。

アプリケーションが TLS ハートビートを使用しているかどうかを判断するには、TLS ハートビートのトラブルシューティングを参照してください。

管理対象デバイスが TLS/SSL ハードウェア アクセラレーションをサポートしていない場合、または が無効になっている場合は、ネットワーク分析ポリシー（NAP）で [最大ハートビート長（Max Heartbeat Length）] を設定して TLS ハートビートの処理方法を決定できます。詳細については、SSL プリプロセッサを参照してください。

TLS/SSL オーバーサブスクリプション

TLS/SSL オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS/SSL ハードウェア アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS/SSL ハードウェア アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、SSL ポリシーの [復号化不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定に従います。

- デフォルト アクションを継承する（Inherit default action）
- 復号しない（Do not decrypt）
- ブロック（Block）
- リセットしてブロック（Block with reset）

SSL ポリシーの [復号化不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定が [復号しない（Do Not decrypt）] で、関連付けられたアクセス コントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

大量のオーバーサブスクリプションが発生している場合は、次のオプションがあります。

- 管理対象デバイスをアップグレードして、TLS/SSL の処理能力を向上させます。
- SSL ポリシーを変更して、復号の優先順位が高くないトラフィック用に [復号しない（Do Not Decrypt）] ルールを追加します。

のステータスの表示 TLS/SSLハードウェアの加速

このトピックでは、TLS/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、TLS/SSLハードウェアの加速 （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。ステータスは [全般（General）] セクションに表示されます。

TLS/SSL ベスト プラクティス

ここでは、復号化ポリシーとルールの作成時に注意する必要がある情報について説明します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

例外は SSL ポリシーです。FMC 設定オプションは **[Policies]** > **[Access Control]** > **[SSL]** となるため、これらのポリシーは TLS および SSL のトラフィックのルールを定義するために使用されますが、「SSL ポリシー」という用語を使用します。

SSL プロトコルと TLS プロトコルの詳細については、「SSL と TLS：その違いとは（SSL vs. TLS - What's the Difference?）」を参照してください。

関連トピック

復号化のケース （12 ページ）
トラフィックを復号化する場合としない場合 （12 ページ）
TLS/SSL のその他のルール アクション （14 ページ）
TLS/SSL ルールのコンポーネント （16 ページ）
TLS/SSL ルールの順序の評価 （18 ページ）

復号化のケース

Firepower システムの脅威に対する防御およびポリシーの適用機能を利用できるのは、復号化されたトラフィックのみです。Firepower システムを通過するときに暗号化されたトラフィックは許可またはブロックできるだけで、ディープインスペクションまたはすべての範囲のポリシー適用（侵入防御など）を対象にすることはできません。

すべての暗号化された接続は次のように処理されます。

- 復号化またはブロックする必要があるかどうかを判断するために、TLS/SSL 復号化ポリシーを介して送信されます。

  また、TLS/SSL の復号化ルールを設定し、非セキュアな SSL プロトコルを使用するトラフィックや、期限切れまたは無効な証明書を使用するトラフィックなど、ネットワークに必要ないとわかっているタイプの暗号化トラフィックをブロックすることもできます。

- ブロックされていない接続は、復号化されているかどうかにかかわらず、許可またはブロックの最終的な決定のためアクセス コントロール ポリシーを経由します。

トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

次に要約を示します。

- 暗号化されたトラフィックはポリシーで許可またはブロックすることができます。暗号化されたトラフィックは検査できません
- 復号化されたトラフィックは脅威に対する防御とポリシーの適用に従います。復号化されたトラフィックはポリシーで許可またはブロックできます。

関連トピック

ディープ インスペクションについて

トラフィックを復号化する場合としない場合

ここでは、トラフィックを復号する場合と暗号化されたファイアウォールの通過を許可する場合のガイドラインを示します。

トラフィックを復号化しない場合

次によって禁止されている場合は、トラフィックを復号してはいけません。

- 法律：たとえば、一部の法域では、財務情報の復号化が禁止されています
- 会社のポリシー：たとえば、会社によって特権的な通信の復号化が禁止されている場合があります
- プライバシー規制
- 証明書のピン留め（*TLS/SSL* ピニングとも呼ばれる）を使用するトラフィックは、接続の切断を防ぐため、暗号化されたままにする必要があります

特定の種類のトラフィックで復号をバイパスする場合、トラフィックの処理は行われません。暗号化トラフィックは最初に SSL ポリシーによって評価され、次にアクセス コントロール ポリシーに進みます。この場合、最終的な許可またはブロックの決定が行われます。暗号化されたトラフィックは、次のものを含むがこれらに限定されない任意の TLS/SSL ルール条件で許可またはブロックできます。

- 証明書のステータス（期限切れまたは無効な証明書など）
- プロトコル（セキュアでない SSL プロトコルなど）
- ネットワーク（セキュリティ ゾーン、IP アドレス、VLAN タグなど）
- 正確な URL または URL カテゴリ
- [ポート（Port）]
- ユーザ グループ

SSL ポリシーは、このトラフィックに対して [復号しない（Do not Decrypt）] アクションを提供します。詳細については、TLS/SSL ルール：復号しないアクションを参照してください。

（注） このトピックの最後にある関連情報リンクでは、ルール評価のいくつかの側面について説明します。URL やアプリケーション フィルタリングなどの条件には、暗号化されたトラフィックに関する制限があります。これらの制限事項を必ず確認してください。

トラフィックを復号化する場合

Firepower システムの脅威に対する防御とポリシーの適用機能を利用できるのは、暗号化されたすべてのトラフィックです。管理対象デバイスでトラフィックの復号化を許可する場合（メモリと処理能力に基づいて）、法律または規制によって保護されていないトラフィックを復号化する必要があります。復号化するトラフィックを決定する必要がある場合は、ネットワーク上のトラフィックを許可するリスクに基づいて決定します。Firepower システムは、URL の評価、暗号スイート、プロトコル、その他多くの要因を含む、ルール条件を使用してトラフィックを分類するための柔軟なフレームワークを提供します。

Firepower システムには 2 つの復号方式があります。これについては次の項で説明します。

関連トピック

復号と再署名（発信トラフィック） （14 ページ）
既知のキーでの復号（着信トラフィック） （14 ページ）
TLS/SSL ルールのガイドラインと制限事項
SSL ルールの順序
URL 条件（URL フィルタリング）
アプリケーション ルールの順序

復号と再署名（発信トラフィック）

[復号と再署名（Decrypt - Resign）] TLS/SSLルール アクションでは、Firepower システムは中間者となり、傍受、復号化、および検査（トラフィックが許可されている場合）し、再暗号化することができます。[復号と再署名（Decrypt - Resign）] ルール アクションは発信トラフィックで使用されます。つまり、宛先サーバは保護ネットワーク外にあります。

FTD デバイスは、ルールで指定された内部認証局（CA）オブジェクトを使用してクライアントとネゴシエートし、クライアントと FTD デバイス間に SSL トンネルを構築します。同時に、デバイスは宛先 web サイトに接続し、サーバと FTD デバイス間に SSL トンネルを作成します。

このため、クライアントには、宛先サーバからの証明書ではなく、SSL 復号化ルールで設定された CA 証明書が表示されます。クライアントは、接続を完了するために証明書を信頼する必要があります。FTD デバイスは、クライアントと宛先サーバ間のトラフィックで両方向に復号化/再暗号化を実行します。

前提条件

[復号と再署名（Decrypt - Resign）] ルール アクションを使用するには、CA ファイルとペアの秘密キー ファイルを使用して、内部 CA オブジェクトを作成する必要があります。CA と秘密キーをまだ使用していない場合は、Firepower システムで生成できます。

関連トピック

TLS/SSL ルールの復号アクション
外部証明書オブジェクト

既知のキーでの復号（着信トラフィック）

[複合と既知のキー（Decrypt - Known Key）] TLS/SSLルール アクションでは、サーバの秘密キーを使用してトラフィックを復号化します。[複合と既知のキー（Decrypt - Known Key）] ルールアクションは着信トラフィックで使用されます。つまり、宛先サーバは保護ネットワーク内にあります。

既知のキーを使用して復号化する主な目的は、社内サーバを外部の攻撃から保護することです。

前提条件

[復号 - 既知のキー（Decrypt - Known Key）] ルール アクションを使用するには、サーバの証明書ファイルとペアの秘密キー ファイルを使用して、内部証明書オブジェクトを作成する必要があります。

関連トピック

TLS/SSL ルールの復号アクション
内部証明書オブジェクト

TLS/SSL のその他のルール アクション

次の項では、TLS/SSL のその他のルール アクションについて説明します。

関連トピック

TLS/SSL ルールのブロック アクション
TLS/SSL ルールのモニタ アクション

TLS/SSL ルールの例

次の項では、TLS/SSL の推奨ルールの設定例を示します。

関連トピック

非セキュアなプロトコルのブロック （15 ページ）

非セキュアなプロトコルのブロック

この例では、TLS 1.0、TLS 1.1、SSLv3 などのセキュアと見なされなくなったネットワーク上の TLS および SSL プロトコルをブロックする方法を示します。

非セキュアなプロトコルはすべてエクスプロイト可能なため、ネットワークから除外する必要があります。この例では、次のようになります。

- SSL ルールの [バージョン（Version）] タブ ページを使用して、一部のプロトコルをブロックすることができます。
- Firepower システムでは SSLv2 が復号化できないと見なされるため、SSL ポリシーの [復号不可のアクション（Undecryptable Actions）] を使用してブロックできます。

手順

ステップ 1 まだ Firepower 管理システムにログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [SSL]** の順にクリックします。

ステップ 3 SSL ポリシーを追加または編集します。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

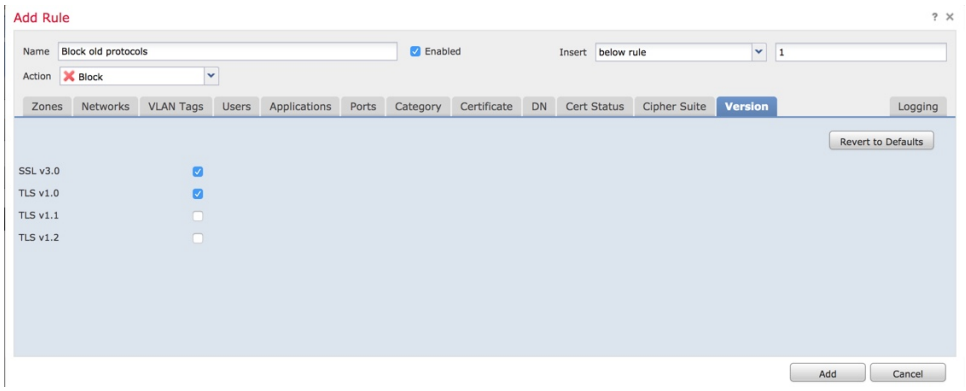
ステップ 5 [名前（Name）] フィールドにルールの名前を入力します。

ステップ 6 [アクション（Action）] リストから [ブロック（Block）] または [リセットしてブロック（Block with reset）] をクリックします。

ステップ 7 [バージョン（Version）] タブ ページをクリックします。

ステップ 8 **SSL v3.0**、**TLS 1.0**、**TLS 1.1** など、セキュアでなくなったプロトコルのチェックボックスをオンにします。引き続きセキュアと見なされているプロトコルのチェックボックスをオフにします。

次の図は例を示しています。

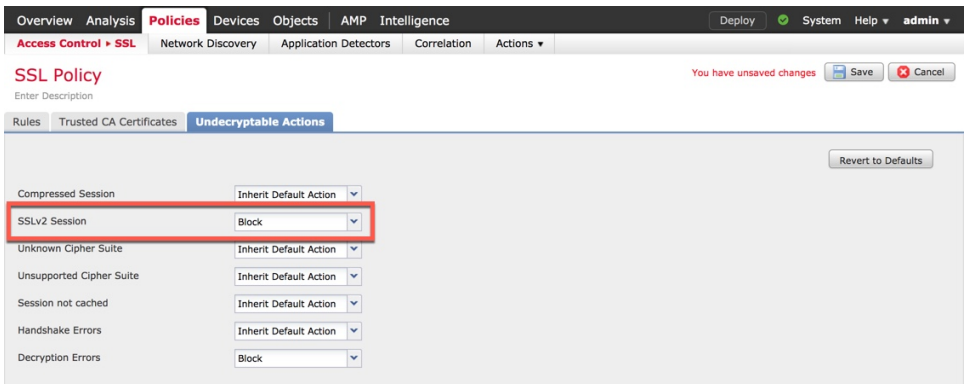


ステップ 9 必要に応じて他のルール条件を選択します。

ステップ 10 ルールを保存します。

ステップ 11 SSL ポリシー ページで [復号できないアクション（Undecryptable Actions）] をクリックします。

ステップ 12 [SSLv2セッション（SSLv2 Session）] リストから [ブロック（Block）] または [リセットしてブロック（Block with reset）] をクリックします。次の図は例を示しています。



ステップ 13 [保存（Save）] をクリックします。

ステップ 14 これは特定のルールであるため、アプリケーション一致ルールなどの一般的なルールよりもポリシー内で上位に配置します。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

関連トピック

TLS/SSL ルール条件

TLS/SSL ルールのコンポーネント

各 TLS/SSL ルールには、次のコンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

SSL ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

条件（Conditions）

条件は、ルールで処理する特定のトラフィックを指定します。こうした条件では、セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを照合できます。使用する条件は、ターゲット デバイスのライセンスによって異なります。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。暗号化された一致したトラフィックは、モニタ、許可、ブロック、または復号できます。復号および許可された暗号化トラフィックは、さらなる検査の影響下に置かれます。システムは、ブロックされた暗号化トラフィックに対してはインスペクションを実行**しない**ことに注意してください。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1 つのルールに一致するトラフィックのレコードを 1 つ保持できます。SSL ポリシーでの設定に従って、システムが暗号化セッションをブロックするか、あるいは復号なしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。接続のログは、Firepower Management Center のデータベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

ログ方法の詳細については、接続のロギングのベスト プラクティスを参照してください。

ヒント　TLS/SSL ルールを適切に作成し順序付けするのは複雑なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。予期したとおりにトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

関連トピック

- インターフェイス条件
- ネットワーク条件
- VLAN 条件
- ポートおよび ICMP コードの条件
- アプリケーション条件（アプリケーション制御）
- URL 条件（URL フィルタリング）
- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）
- ルールのパフォーマンスに関するガイドライン
- TLS/SSL ルールのガイドラインと制限事項

TLS/SSL ルールの順序の評価

SSL ポリシーで TLS/SSL ルールを作成する場合、ルール エディタの [挿入（Insert）] リストを使用してその位置を指定します。SSL ポリシー内の TLS/SSL ルールには、1 から始まる番号が付けられています。システムは、ルール番号の昇順で上から順に、TLS/SSL ルールをトラフィックと照合します。

ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の TLS/SSLSSL ルールに従って行われます。モニタ ルール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。こうした条件には、単純なものと複雑なものがあります。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号化トラフィックに対してモニタ、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号化できないトラフィックはアクセス コントロールの対象です。ただし、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ります。

特定の条件（ネットワークや IP アドレスなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

ヒント 適切な TLS/SSL ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

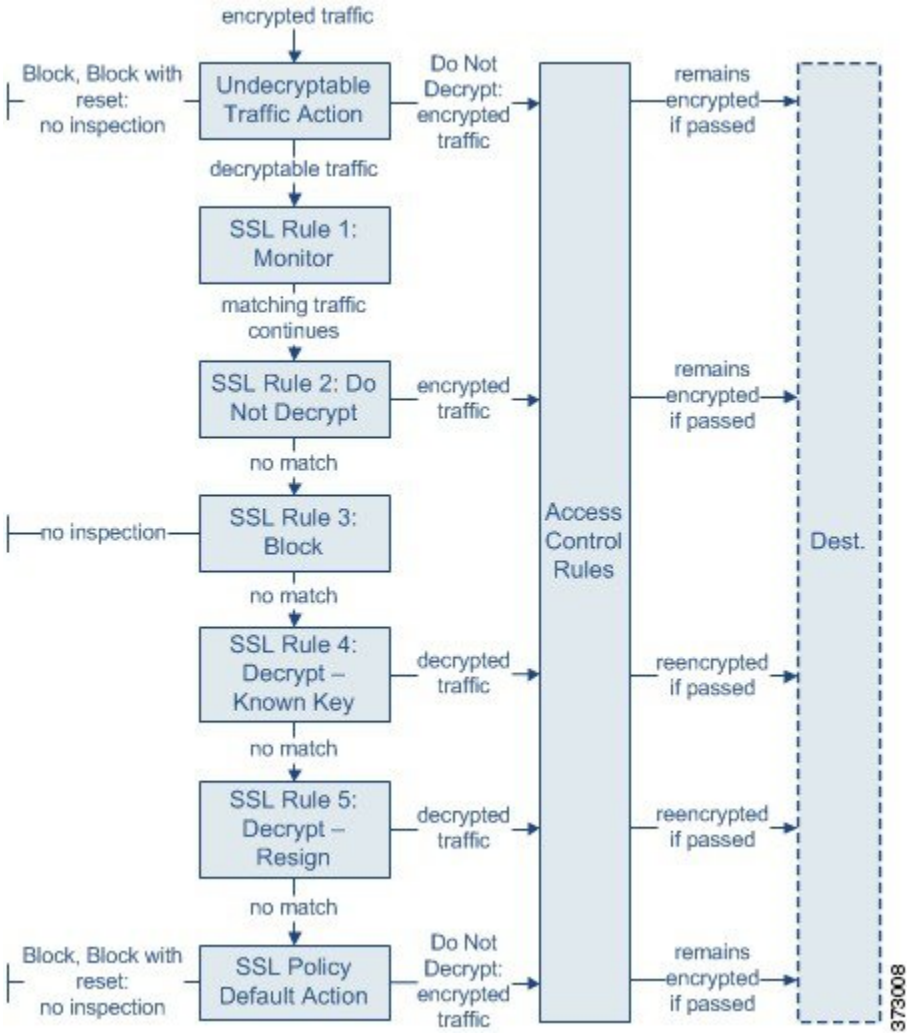
番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、3つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

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
- SSL ルールの順序
- ルールのパフォーマンスに関するガイドライン

複数ルールの例

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号化できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号できないトラフィックについてシステムは、それ以上のインスペクションなしでブロックするか、あるいはアクセス コントロールによるインスペクション用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **TLS/SSLルール 1：モニタ（Rule 1: Monitor）**は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- **TLS/SSLルール 2：復号しない（Rule 2: Do Not Decrypt）**は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。

- **TLS/SSLルール 3**：**ブロック（Rule 3: Block**）は、暗号化トラフィックを 4 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **TLS/SSLルール 4**：**復号 - 既知のキー（Rule 4: Decrypt - Known Key**）は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号されます。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **TLS/SSLルール 5**：**復号 - 再署名（Rule 5: Decrypt - Resign**）は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション（SSL Policy Default Action**）は、どの TLS/SSL ルールにも一致しなかったすべてのトラフィックを処理します。デフォルト アクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

TLS/SSL ポリシーとルールの設定方法

このトピックでは、ネットワーク上の TLS/SSL トラフィックをブロック、モニタ、または許可する SSL ポリシーとこれらのポリシーの TLS/SSL ルールを設定するために必要なタスクの概要を説明します。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

手順

	コマンドまたはアクション	目的
ステップ 1	SSL ポリシーを作成します。	SSL ポリシーは、1 つ以上のルールのコンテナです。アクセス制御のために SSL ポリシーとそのルールを使用するには、後で SSL ポリシーをアクセス コントロール ポリシーに関連付ける必要があります。基本的な SSL ポリシーの作成を参照してください。
ステップ 2	SSL ポリシーのデフォルト アクションを設定します。	デフォルト アクションは、トラフィックが SSL ポリシーによって定義されたルールに一致しない場合に実行されます。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。
ステップ 3	復号化できないトラフィックの処理方法を指定します。	トラフィックは、セキュアでないプロトコル、不明な暗号スイートの使用、またはハンドシェイクや復号化でエラーが発生した場合など、さまざまな理由で復号できなくなる可能性があります。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を参照してください。
ステップ 4	[復号-既知のキー（Decrypt - Known Key）]（ネットワーク内のサーバに着信トラフィックを復号するための）TLS/SSL ルールの場合、内部証明書オブジェクトを作成します。	内部証明書オブジェクトは、サーバの証明書と秘密キーを使用します。内部証明書オブジェクトを参照してください。
ステップ 5	[復号-再署名（Decrypt - Resign）]（ネットワーク外部のサーバに発信トラフィックを復号するための）TLS/SSL ルールの場合、内部認証局（CA）オブジェクトを作成します。	内部 CA オブジェクトは、CA と秘密キーを使用します。内部認証局オブジェクトを参照してください。
ステップ 6	TLS/SSL ルールを作成します。	• [ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive block）]：TLS/SSL ルール アクション設定。 • [復号しない（Do Not Decrypt）]：TLS/SSL ルール アクション設定を参照してください。

	コマンドまたはアクション	目的
		• [復号-再署名（Decrypt - Resign）]：復号 - 再署名アクションの設定を参照してください。 • [復号-既知のキー（Decrypt - Known Key）]：復号 - 既知のキー アクションの設定を参照してください。 • [モニタ（Monitor）]：TLS/SSL ルール アクション設定を参照してください。
ステップ 7	SSL ポリシーをアクセス コントロール ポリシーに関連付けます。	SSL ポリシーをアクセス コントロール ポリシーに関連付けていない限り、SSL ポリシーの影響はありません。関連付けた後、アクセス コントロール ルールに一致するトラフィックを許可またはブロックし、その他のアクションを実行することができます。アクセス制御への他のポリシーの関連付けを参照してください。
ステップ 8	復号化されたトラフィックを許可またはブロックするようにアクセスコントロール ルールを設定します。	アクセス コントロール ポリシーのコンポーネントを参照してください。
ステップ 9	管理対象デバイスにアクセスコントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開を参照してください。

TLS/SSL インスペクション アプライアンス展開シナリオ

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。

- 契約審査部門では、単一の FTD 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。

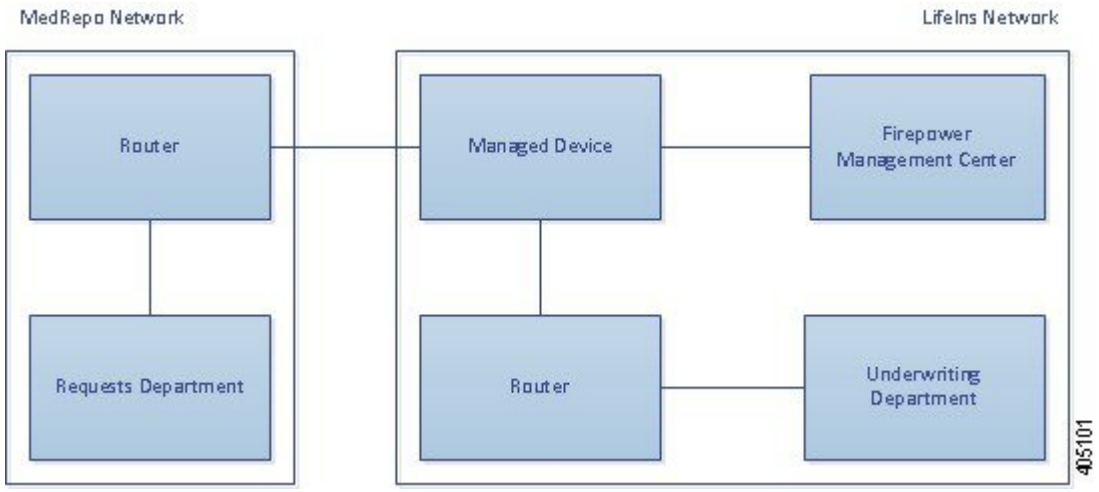
LifeIns では、経験の浅い契約審査担当者に対して 6 ヵ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

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。

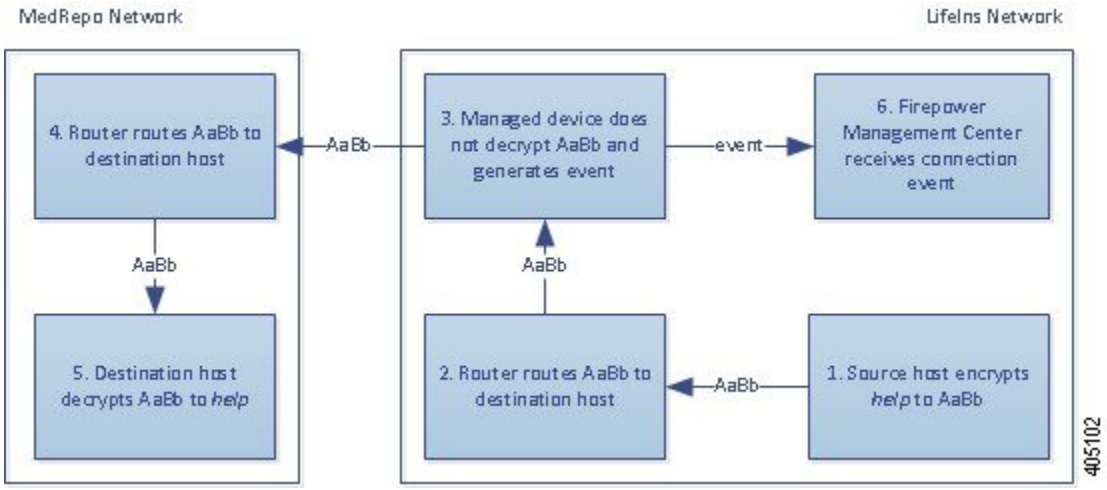
また、TLS/SSL アクセス コントロール ルールを使用して、[復号 - 再署名（Decrypt - Resign）] アクションでシステムにトラフィックを復号化して再署名させることもできます。トラフィックが TLS/SSL ルールに一致する場合、システムは ClientHello メッセージを変更した後、メッ

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、ClientHello メッセージ処理 （4 ページ）を参照してください。

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。

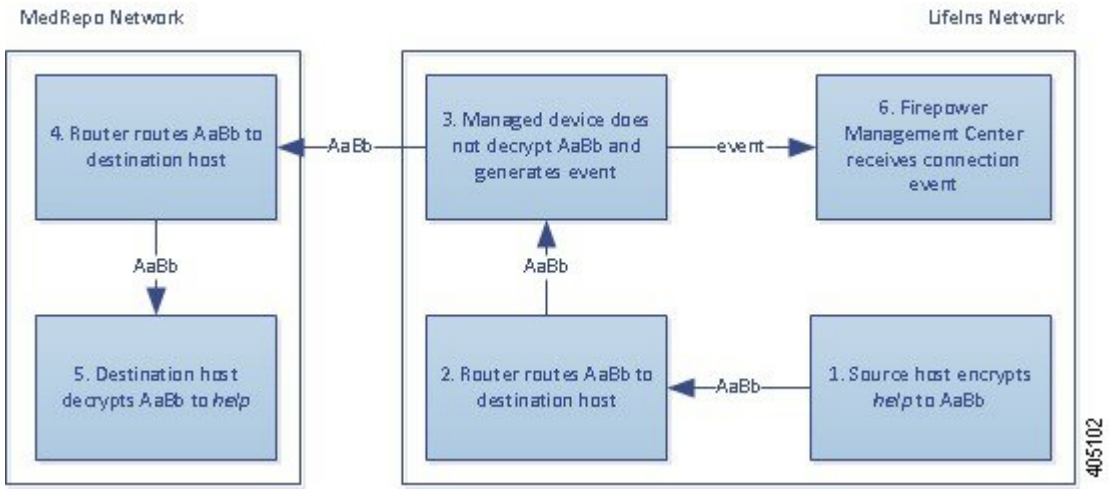
1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはトラフィックを復号化しません。

   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。

インライン展開で復号される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TLS/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。



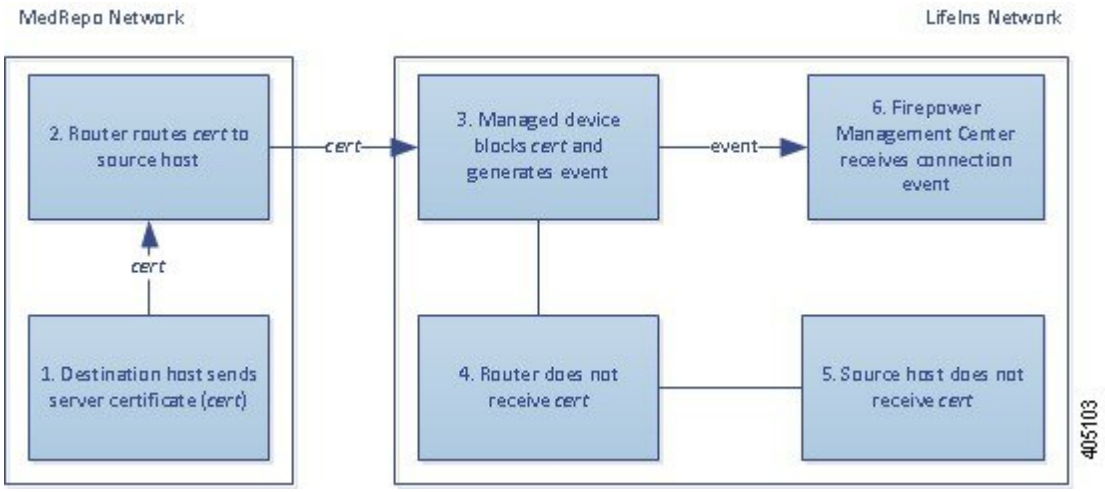
次のステップが実行されます。

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。

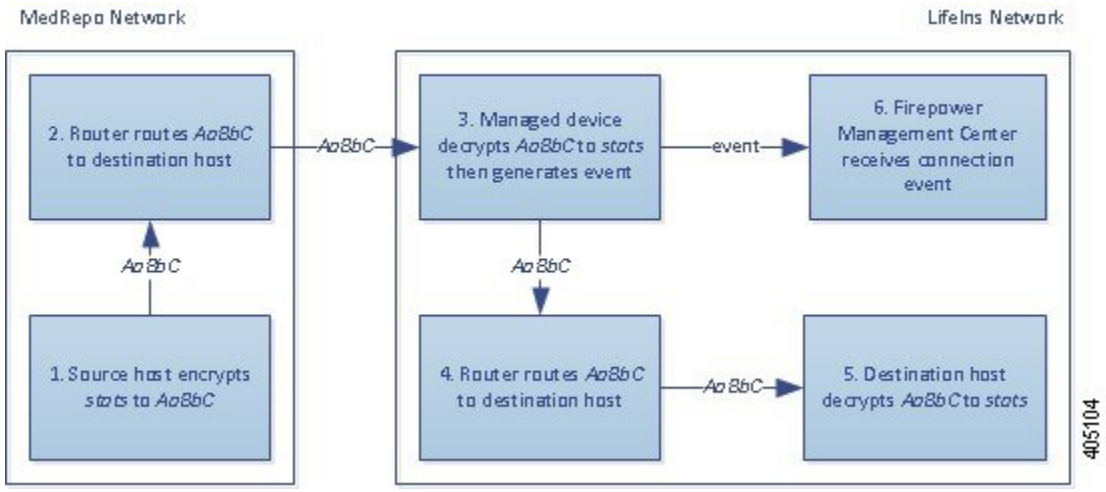


次のステップが実行されます。

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 TLS/SSL ハンドシェイクの確立要求を受信すると、TLS/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 TLS/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。

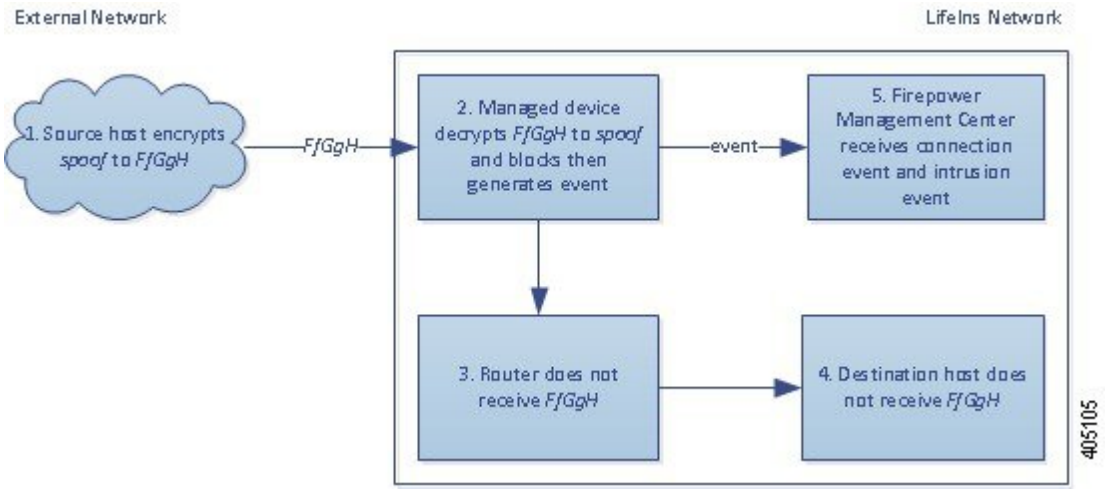


次のステップが実行されます。

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化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。

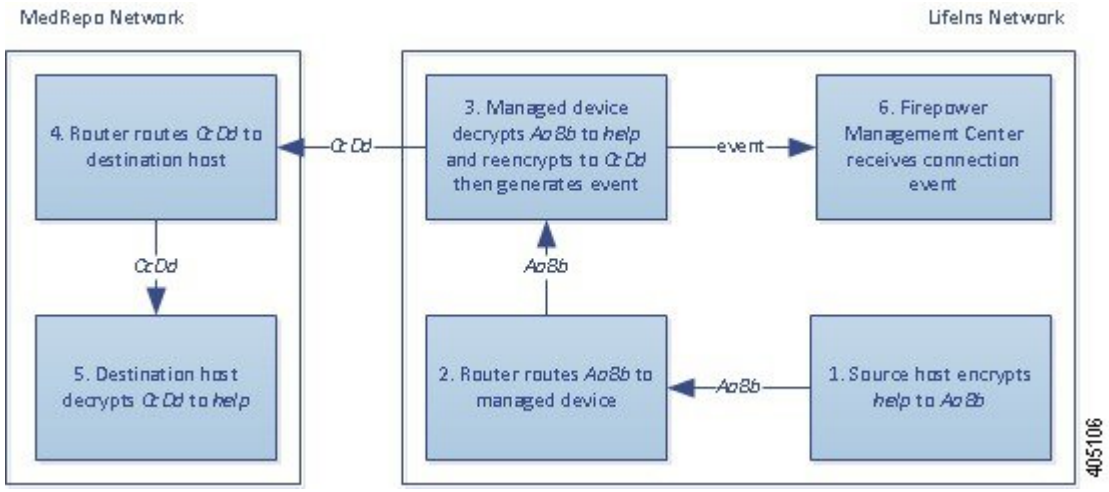
1. ユーザがプレーン テキストの要求（spoof）を送信しますが、このトラフィックは改変されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化（FfGgH）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（spoof）に復号化します。

   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. 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再署名証明書を使用した暗号化トラフィック インスペクション

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 TLS/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 TLS/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。



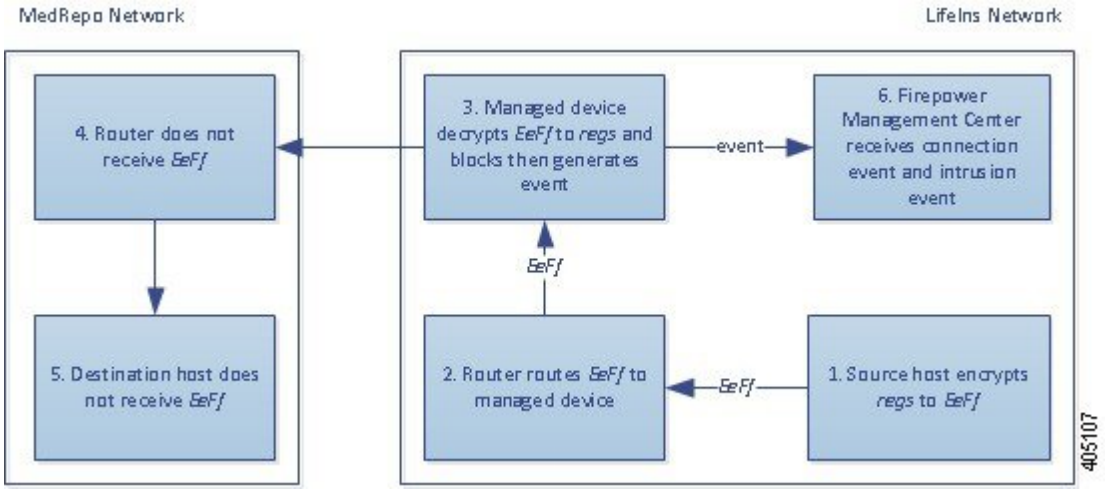
次のステップが実行されます。

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。

TLS/SSL の履歴

機能	バージョン（Version）	詳細
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）	6.3.0.1	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。

機能	バージョン（Version）	詳細
Extended Master Secret 拡張機能はサポートされていません。	6.3	拡張機能は [復号 - 再署名（Decrypt - Resign）] ルールの ClientHello 変更時に削除されます。
TLS/SSL ハードウェア アクセラレーションデフォルトでは有効になっています	6.3	TLS/SSL ハードウェア アクセラレーション デフォルトですべてのサポート対象デバイスで有効になっていますが、必要に応じて無効にすることができます。
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）	6.2.3.9	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。
アグレッシブ TLS 1.3 ダウングレード	6.2.3.7	**system support ssl-client-hello-enabled aggressive-tls13-downgrade {true|false}** CLI コマンドを使用して、TLS 1.2 への TLS 1.3 トラフィックのダウングレードの動作を決定できます。詳細については、『*Command Reference for Firepower Threat Defense*』を参照してください。
TLS/SSL ハードウェア アクセラレーション introduced	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 TLS/SSL 暗号化および復号が実行されます。デフォルトでは、この機能は有効です。 影響を受ける画面：TLS/SSL ハードウェア アクセラレーションのステータスを表示するには、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）]**、[全般（General）] タブ ページ。
カテゴリとレピュテーションの条件をサポート	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 をサポート	6.1.0	• 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。