SSL 復号

HTTPS など一部のプロトコルは、セキュア ソケット レイヤ（SSL）またはその後継バージョンである Transport Layer Security（TLS）を使用して、セキュアな転送のためにトラフィックを暗号化します。システムでは暗号化された接続を検査できないため、アクセス判断のために上位層のトラフィック特性を考慮したアクセスルールを適用する場合は、暗号化された接続を復号する必要があります。

- SSL 復号について （1 ページ）
- SSL 復号のためのライセンス要件 （5 ページ）
- SSL 復号のガイドライン （5 ページ）
- SSL 復号ポリシーの実装および管理方法 （6 ページ）
- SSL 復号ポリシーの設定 （8 ページ）
- 例：ネットワークからの古い SSL/TLS バージョンのブロック （23 ページ）
- SSL 復号のモニタリングとトラブルシューティング （25 ページ）

SSL 復号について

通常、接続は、許可されるかブロックされるかを決定するアクセス コントロール ポリシーを経由します。ただし、SSL復号ポリシーを有効にする場合、暗号化された接続は最初にSSL復号ポリシー経由で送信され、復号化するかブロックする必要があるかが判断されます。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/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。

（注） アイデンティティ ポリシーでアクティブな認証ルールを実装するためには、SSL復号ポリシーを有効にする必要があります。SSL復号を有効にしてアイデンティティ ポリシーを有効にするが、SSL 復号は実装しない場合、デフォルトのアクションに [復号しない（Do Not Decrypt）] を選択し、追加のSSL復号ルールは作成しないでください。アイデンティティ ポリシーでは、必要なルールを自動的に生成します。

ここでは、暗号化トラフィック フロー管理と復号化についてさらに詳しく説明します。

SSL 復号を実装する理由

HTTPS 接続などの暗号化されたトラフィックは検査することができません。

銀行や他の金融機関への接続など、多くの接続は合法的に暗号化されます。多くの Web サイトでは、プライバシーや機密性の高いデータを保護するために暗号化を使用します。たとえば、Firepower Device Manager への接続は暗号化されます。

ただし、暗号化された接続の中ではユーザが望ましくないトラフィックを隠すこともできます。

SSL復号を実装することによって、接続を復号して脅威またはその他の望ましくないトラフィックが含まれていないかを確認するために検査し、再度暗号化してから接続の続行を許可できます。（復号されたトラフィックは、アクセス制御ポリシーを通過し、暗号化された特性ではなく、復号された接続の検査特性に基づいたルールに一致します。）これは、機密情報を保護するために、アクセス制御ポリシーを適用する必要性とユーザの必要性との間でバランスをとります。

ネットワークを利用させたくない種類の暗号化されたトラフィックをブロックする SSL 復号ルールを構成することもできます。

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。

暗号化されたトラフィックに適用できるアクション

SSL復号ルールを設定する場合は、次のトピックで説明しているアクションを適用できます。これらのアクションは、明示的なルールと一致しないすべてのトラフィックに適用されるデフォルトのアクションにも使用できます。

（注） SSL 復号ポリシーを経由するすべてのトラフィックは、アクセス コントロール ポリシーを経由する必要があります。SSL復号ポリシーにドロップするトラフィックを除き、許可またはドロップの最終的な決定はアクセス コントロール ポリシーに委ねられます。

再署名の復号

トラフィックを復号し再署名する場合、システムは中間者として機能します。

たとえば、ユーザがブラウザで https://www.cisco.com と入力します。トラフィックが FTD デバイスに達すると、デバイスはルールで指定された CA 証明書を使用するユーザと交渉し、ユーザと 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 https://www.cisco.com 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、ユーザには、www.cisco.com からの証明書ではなく、SSL 復号ルールで設定された CA 証明書が表示されます。ユーザは、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、ユーザと宛先サーバ間のトラフィックで両方向に復号/再暗号化を実行します。

（注） サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザに出されます。これを防止するには、クライアントの信用できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。

再署名の復号アクションでルールを設定する場合、設定されているルールの条件に加え、参照される内部 CA 証明書の署名アルゴリズムの種類に基づいてルールがトラフィックと一致します。SSL 復号ポリシーに 1 つの再署名証明書を選択できるため、これによって再署名ルールのトラフィック一致を制限できます。

たとえば、楕円曲線（EC）アルゴリズムで暗号化された発信トラフィックは、再署名証明書が EC ベースの CA 証明書の場合にのみ、再署名の復号ルールと一致します。同様に、RSA アルゴリズムで暗号化されたトラフィックは、グローバル再署名証明書が RSA の場合にのみ、再署名の復号ルールと一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されたその他すべてのルール条件が一致していても、このルールとは一致しません。

既知のキーの復号

宛先サーバを所有している場合、既知のキーで復号化を実装できます。この場合、ユーザが https://www.cisco.com への接続を開くと、それが証明書を提示している FTD デバイスであっても、www.cisco.com の実際の証明書がユーザに表示されます。

ドメインおよび証明書の所有者は、所属組織でなければなりません。cisco.com を例として取り上げると、エンドユーザにシスコの証明書が表示されるのは、組織が実際にドメイン cisco.com の所有者であり（つまり、所属企業が Cisco Systems であること）、パブリック CA によって署名された cisco.com 証明書の所有権を持っている場合のみです。復号できるのは、所属組織が所有するサイトの既存のキーを使用する場合のみです。

既知のキーを使用して復号する主な目的は、HTTPS サーバへのトラフィックを復号して、社内サーバを外部の攻撃から保護することです。外部 HTTPS サイトへのクライアント側のトラ

フィックを検査する場合は、サーバを所有していないので、再署名の復号を使用する必要があります。

（注） 既知のキーの復号を使用するには、サーバの証明書およびキーを内部アイデンティティ証明書としてアップロードし、SSL復号ポリシー設定で既知のキーの証明書一覧に追加する必要があります。その後は、宛先アドレスとしてサーバのアドレスを使用して既知のキーの復号化のルールを作成できます。SSL復号ポリシーに証明書を追加する方法については、既知のキーと復号の再署名の証明書の設定 （20 ページ）を参照してください。

復号禁止

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。暗号化されたトラフィックはアクセス コントロール ポリシーに渡され、一致するアクセス制御ルールに基づいて許可またはドロップされます。

ブロック

単にSSL復号ルールと一致する暗号化されたトラフィックをブロックできます。SSL復号ポリシーのブロックでは、アクセス コントロール ポリシーに接続が達することを防ぎます。

HTTPS 接続をブロックすると、ユーザにはシステムのデフォルトのブロック応答ページが表示されません。代わりに、ブラウザのセキュアな接続の障害時のデフォルトページが表示されます。エラー メッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

自動的に生成された SSL 復号ルール

SSL復号ポリシーを有効にしてもしなくても、システムはアクティブな認証を実装する各アイデンティティ ポリシー ルールに対して再署名の復号ルールを自動的に生成します。これは、HTTPS 接続でアクティブな認証を有効にするために必要です。

SSL復号ポリシーを有効にすると、アイデンティティ ポリシーのアクティブな認証ルールの見出しの下にこれらのルールが表示されます。これらのルールは、SSL復号ポリシーの上部にグループ化されます。ルールは読み取り専用です。アイデンティティ ポリシーを変更することによってのみ変更できます。

復号できないトラフィックの処理

接続が復号できなくなる特性は複数あります。接続に次の特性のいずれかがある場合、接続で一致するルールがあっても接続にはデフォルトのアクションが適用されます。（[復号しない（Do Not Decrypt）] ではなく）デフォルト アクションとしてブロックを選択する場合、正当なトラフィックの過剰なドロップなどの問題があることがあります。

- 圧縮されたセッション：データ圧縮が接続に適用されています。

- SSLv2 セッション：サポートされている最下位の SSL バージョンは SSLv3 です。
- 不明な暗号スイート：システムで接続の暗号スイートが認識されません。
- サポート外の暗号スイート：システムで、検出された暗号スイートに基づく復号化がサポートされません。
- キャッシュされないセッション：SSL セッションにおいてセッションの再利用が可能になっていて、クライアントとサーバがセッション ID でセッションを再確立したときに、システムがそのセッション ID をキャッシュに入れなかったことを意味します。
- ハンドシェイク エラー：SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。
- 復号エラー：復号処理中にエラーが発生しました。
- パッシブ インターフェイス トラフィック：パッシブ インターフェイス（パッシブ セキュリティ ゾーン）のすべてのトラフィックが復号不能です。

SSL 復号のためのライセンス要件

SSL 復号ポリシーを使用するのに特別なライセンスは必要ありません。

ただし、URL カテゴリおよびレピュテーションを一致基準として使用するルールを作成するには、**URL フィルタリング** ライセンスが必要です。ライセンスの設定については、オプション ライセンスの有効化と無効化を参照してください。

SSL 復号のガイドライン

SSL 復号ポリシーを設定してモニタする場合は、次の点に注意してください。

- SSL 復号ポリシーは、次のようなアクセス制御ルールがトラフィックを信頼またはブロックするように設定されている場合に、それらのルールに一致する接続に関してバイパスされます。
  - セキュリティ ゾーン、ネットワーク、地理位置情報、およびポートだけをトラフィック照合基準として使用する。
  - 検査を必要とする他のルール（アプリケーションまたは URL に基づいて接続を照合するルールなど）に先立つか、侵入またはファイル検査を適用するルールを許可する。
- URL カテゴリのマッチングを使用するときは、サイトのログイン ページがサイトそのものと異なるカテゴリにある場合に注意してください。たとえば、Gmail は「Web ベースの電子メール」カテゴリにあり、ログイン ページは「インターネット ポータル」カテゴリにあります。これらのサイトへの接続を復号するには、両方のカテゴリをルールに含める必要があります。

- 脆弱性データベース（VDB）の更新によってアプリケーションが削除（廃止）される場合は、削除されたアプリケーションを使用するSSL復号ルールまたはアプリケーション フィルタに変更を加える必要があります。これらのルールを修正するまで、変更を展開することはできません。また、問題を修正する前にシステム ソフトウェア アップデートをインストールすることはできません。[アプリケーションフィルタ（Application Filters）] オブジェクト ページ、またはルールの[アプリケーション（Application）]タブでは、これらのアプリケーション名の後に「（廃止）（Deprecated）」と表示されます。
- アクティブ認証ルールを使用している場合は、SSL復号ポリシーを無効にすることができません。SSL 復号ポリシーを無効にするには、アイデンティティ ポリシーを無効にするか、またはアクティブ認証を使用するアイデンティティ ルールを削除する必要があります。

SSL 復号ポリシーの実装および管理方法

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーン テキスト トラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。

他のセキュリティ ポリシーの場合とは異なり、SSL復号ポリシーは、監視して積極的に保守する必要があります。これは、証明書の期限が切れたり、宛先サーバで変更されたりするためです。さらに、クライアント ソフトウェアの変更により特定の接続を復号する能力が変わる場合もあります。これは、再署名の復号アクションを中間者攻撃と区別できないためです。

次の手順では、SSL 復号ポリシーの実装と保守のエンドツーエンド プロセスを説明します。

手順

ステップ 1 再署名の復号ルールを実装する場合は、必要な内部 CA 証明書を作成します。

内部認証局（CA）証明書を使用する必要があります。次の選択肢があります。ユーザは証明書を信頼する必要があるため、すでに信頼されると設定されているクライアントブラウザに証明書をアップロードするか、またはアップロードする証明書がブラウザの信頼ストアに追加されるようにします。

- デバイス自体によって署名される自己署名内部 CA 証明書を作成します。自己署名内部および内部 CA 証明書の生成を参照してください。
- 外部の信頼できる CA または組織内部の CA によって署名される内部 CA 証明書およびキーをアップロードします。内部および内部 CA 証明書のアップロードを参照してください。

ステップ 2 既知のキーの復号ルールを実装する場合は、各内部サーバから証明書とキーを収集します。

サーバから証明書とキーを取得する必要があるため、既知のキーの復号は自分で制御しているサーバでのみ使用できます。これらの証明書とキーを内部証明書（内部 CA 証明書ではない）としてアップロードします。内部および内部 CA 証明書のアップロードを参照してください。

ステップ 3 SSL 復号ポリシーの有効化 （9 ページ）。

ポリシーを有効にする際に、いくつかの基本的な設定も構成します。

ステップ 4 SSL 復号のデフォルト アクションの設定 （10 ページ）。

不確かな場合は、デフォルトアクションとして [復号しない（Do not decrypt）] を選択します。この場合でも、アクセス コントロール ポリシーは、デフォルトの SSL 復号ルールに一致するトラフィックを適切であればドロップできます。

ステップ 5 SSL 復号ルールの設定 （11 ページ）。

復号するトラフィック、および適用する復号のタイプを識別します。

ステップ 6 既知のキーでの復号を設定する場合は、これらの証明書を含めるように SSL 復号ポリシー設定を編集します。既知のキーと復号の再署名の証明書の設定 （20 ページ）を参照してください。

ステップ 7 必要に応じて、再署名の復号ルールに使用する CA 証明書をダウンロードして、クライアントワークステーションのブラウザにアップロードします。

証明書のダウンロードおよびクライアントへの配布については、再署名の復号ルールの CA 証明書のダウンロード （21 ページ）を参照してください。

ステップ 8 定期的に、再署名証明書および既知のキーの証明書を更新します。

- 再署名証明書：期限切れになる前にこの証明書を更新します。Firepower Device Manager を使用して証明書を生成する場合は、5 年間有効です。証明書の有効期間を確認するには、**[オブジェクト（Objects）] > [証明書（Certificates）]** を選択し、リスト内で証明書を見つけて [アクション（Actions）] 列の[情報]（information） アイコン（ ）をクリックします。情報ダイアログボックスに、有効期間およびその他の特性が表示されます。このページから代替証明書をアップロードすることもできます。
- 既知のキーの証明書：既知のキーによる復号ルールの場合、宛先サーバの現在の証明書とキーがアップロードされていることを確認する必要があります。サポートされるサーバで証明書およびキーが変更されるたびに、新しい証明書およびキーを（内部証明書として）アップロードし、新しい証明書を使用するように SSL 復号設定を更新する必要があります。

ステップ 9 外部サーバで不足している信頼できる CA 証明書をアップロードします。

システムには、サードパーティによって発行された、広範な信頼できる CA ルート証明書および信頼できる CA 中間証明書が含まれています。これらは、FTD と再署名の復号ルールの宛先サーバの間で接続をネゴシエートするときに必要です。

信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になり

ます。**[オブジェクト（Objects）] > [証明書（Certificates）]** ページで証明書をアップロードします。信頼できる CA 証明書のアップロードを参照してください。

SSL 復号ポリシーの設定

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーン テキスト トラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。

（注） VPN トンネルは SSL 復号ポリシーが評価される前に復号されるので、トンネル自体にはポリシーは適用されません。ただし、トンネル内で暗号化された接続はSSL復号ポリシーによる評価の対象となります。

以下の手順で、SSL 復号ポリシーを設定する方法を説明します。SSL 復号を作成および管理するエンドツーエンド プロセスの説明については、SSL 復号ポリシーの実装および管理方法 （6 ページ）を参照してください。

始める前に

SSL 復号ルール テーブルには、2 つのセクションが含まれています。

- [アイデンティティポリシーアクティブ認証ルール（Identity Policy Active Authentication Rules）]：アイデンティティ ポリシーを有効にしてアクティブ認証を使用するルールを作成すると、システムがこれらのポリシーの動作に必要なSSL復号ルールを自動的に作成します。これらのルールは、常に自分で作成したSSL復号ルールの前に評価されます。アイデンティティ ポリシーに変更することによって、間接的にのみこれらのルール変更できます。
- [SSLネイティブルール（SSL Native Rules）]：これらは自分で構成したルールです。このセクションにのみルールを追加できます。

手順

ステップ 1 **[ポリシー（Policies）] > [SSL復号（SSL Decryption）]** の順に選択します。

ポリシーをまだ有効化していない場合は、[SSL復号の有効化（Enable SSL Decryption）] をクリックし、「SSL 復号ポリシーの有効化 （9 ページ）」の説明に従ってポリシーを設定します。

ステップ 2 ポリシーのデフォルト アクションを設定します。

最も安全な選択肢は、[復号しない（Do Not Decrypt）] です。詳細については、SSL 復号のデフォルト アクションの設定 （10 ページ）を参照してください。

ステップ 3 SSL 復号ポリシーを管理します。

SSL復号を設定した後、このページにすべてのルールが順番に一覧表示されます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- ポリシーを無効にするには、[SSL復号ポリシー（SSL Decryption Policy）] トグルをクリックします。[SSL複合を有効化（Enable SSL Decryption）] をクリックすると再度有効にできます。
- ポリシーで使用する証明書のリストを含むポリシー設定を編集するには、[SSL復号設定（SSL Decryption Settings）] ボタン（⚙）をクリックします。また、クライアントに配布できるように、再署名の復号ルールで使用する証明書をダウンロードできます。次のトピックを参照してください。
  - 既知のキーと復号の再署名の証明書の設定 （20 ページ）
  - 再署名の復号ルールの CA 証明書のダウンロード （21 ページ）
- ルールを設定するには、次の手順を実行します。
  - 新しいルールを作成するには、[+] ボタンをクリックします。SSL 復号ルールの設定（11 ページ）を参照してください。
  - 既存のルールを編集する場合は、（[操作（Actions）] 列の）対象のルールの編集アイコン（✎）をクリックします。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。
  - 不要になったルールを削除する場合は、（[操作（Actions）] 列の）対象のルールの [削除（delete）] アイコン（🗑）をクリックします。
- ルールを移動するには、編集して [順序（Order）] ドロップダウン リストから新しい場所を選択します。

SSL 復号ポリシーの有効化

SSL復号ルールを設定する前に、ポリシーを有効にして、いくつかの基本的な設定を構成する必要があります。以下の手順で、ポリシーを直接有効にする方法を説明します。アイデンティティ ポリシーを有効にするときにこのポリシーを有効にすることもできます。アイデンティティ ポリシーでは、SSL 復号ポリシーを有効にする必要があります。

始める前に

SSL復号ポリシーを持たないリリースからアップグレードし、アクティブな認証ルールを使用してアイデンティティ ポリシーを設定した場合、SSL復号ポリシーはすでに有効になっています。必ず使用する再署名の復号証明書を選択し、必要に応じて事前定義されたルールを有効にします。

手順

ステップ 1 **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [SSL復号の有効化（Enable SSL Decryption）] をクリックしてポリシー設定を構成します。

- このポリシーを初めて有効にする場合は、[SSL復号設定（SSL Decryption Configuration）] ダイアログ ボックスが開きます。次の手順に進みます。
- 以前にこのポリシーを設定した後で無効にした場合は、前の設定とルールを使用してポリシーが再度有効になります。[SSL復号設定（SSL Decryption Configuration）] ボタン（⚙）をクリックし、既知のキーと復号の再署名の証明書の設定 （20 ページ）で説明されているように設定します。

ステップ 3 [再署名証明書の復号（Decrypt Re-Sign Certificate）] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成（Create Internal CA）] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（⬇）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールのCA証明書のダウンロード （21 ページ）も参照してください。

ステップ 4 初期 SSL 復号ルールを選択します。

システムには以下の事前定義ルールが含まれており、役立つ場合があります。

- [Sensitive_Data]：このルールでは、金融サービスまたは健康と医療の URL カテゴリ（銀行、医療機関、ヘルスケア サービスなど）内の Web サイトに一致するトラフィックは復号しません。このルールを実装するには、URL ライセンスを有効にする必要があります。

ステップ 5 [有効（Enable）] をクリックします。

SSL 復号のデフォルト アクションの設定

暗号化された接続が特定のSSL復号ルールに一致しない場合、SSL復号ポリシーのデフォルトアクションに基づいて処理されます。

手順

ステップ 1 **[ポリシー（Policies）] > [SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [デフォルトアクション（Default Action）] フィールドの任意の場所をクリックします。

ステップ 3 一致するトラフィックに適用するアクションを選択します。

- [復号しない（Do Not Decrypt）]：暗号化された接続を許可します。次にアクセス制御ポリシーは、暗号化された接続を評価し、アクセス制御ルールに基づいてドロップまたは許可します。
- [ブロック（Block）]：接続をすぐに切断します。接続はアクセス制御ポリシーに渡されません。

ステップ 4 （オプション）デフォルト アクションのロギングを設定します。

デフォルトアクションに一致するトラフィックのロギングをダッシュボードのデータまたはイベント ビューアに記載されるようにするには、トラフィックのロギングを有効にする必要があります。次のオプションから選択します。

- [接続終了時（At End of Connection）]：接続の終了時にイベントを生成します。
  - [接続イベントの送信先（Send Connection Events To）]：外部の syslog サーバにイベントのコピーを送信するには、syslogサーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成（Create New Syslog Server）] をクリックして作成します（syslog サーバへのロギングを無効にするには、サーバ リストから [任意（Any）] を選択します）。

    デバイスのイベント ストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。
- [ロギングなし（No Logging）]：イベントを生成しません。

ステップ 5 [保存（Save）] をクリックします。

SSL 復号ルールの設定

SSL 復号ルールを使用して、暗号化された接続を処理する方法を決定します。SSL 復号ポリシーに設定されたルールは、上から下への順に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

[SSLネイティブルール（SSL Native Rules）] セクションでのみルールを作成し、編集できます。

（注） SSL 復号ポリシーが接続を評価する前に、VPN 接続（サイト間とリモート アクセスの両方）のトラフィックが復号されます。したがって、SSL 復号ルールが VPN 接続に適用されることはなく、これらのルールを作成するときに VPN 接続を考慮する必要はありません。ただし、VPN トンネル内で暗号化された接続を使用する場合は評価されます。たとえば、RA VPN トンネル自体は（すでに復号されているので）評価されなくても、RA VPN 接続経由の内部サーバへの HTTPS 接続は、SSL 復号ルールによって評価されます。

始める前に

既知のキーの復号ルールを作成する場合は、宛先サーバのための証明書とキーを（内部証明書として）アップロードし、証明書を使用するためにSSL復号ポリシーの設定も編集します。既知のキーのルールは通常、ルールの宛先ネットワークの条件で宛先サーバを指定します。詳細については、既知のキーと復号の再署名の証明書の設定 （20 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [SSL復号（SSL Decryption）]** の順に選択します。

（アクティブ認証アイデンティティ ルール用に自動的に生成されたもの以外に）任意の SSL 復号ルールを構成していない場合、[事前定義済みルールを追加（Add Pre-Defined Rules）] をクリックして、事前定義済みのルールを追加できます。ルールを選択するように要求されます。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（ ）をクリックします。

不要になったルールを削除するには、ルールの [削除（delete）] アイコン（ ）をクリックします。

ステップ 3 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

[SSLネイティブルール（SSL Native Rules）] セクションにのみルールを挿入できます。アイデンティティ ポリシーアクティブ認証ルールはアイデンティティ ポリシーから自動的に生成され、読み取り専用です。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル（Title）] にルールの名前を入力します。

この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます：+ . _ -

ステップ 5 一致するトラフィックに適用するアクションを選択します。

各オプションの詳細については、次を参照してください。

- 再署名の復号 （2 ページ）
- 既知のキーの復号 （3 ページ）
- 復号禁止 （4 ページ）
- ブロック （4 ページ）

ステップ 6 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/送信先（Source/Destination）]：トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的ロケーション）、トラフィックで使用されている TCP ポート。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。SSL 復号ルールの送信元/送信先基準 （14 ページ）を参照してください。
- [アプリケーション（Application）]：アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトは任意の暗号化されたアプリケーションです。SSL 復号ルールのアプリケーション基準 （16 ページ）を参照してください。
- [URL]：Web 要求の URL カテゴリ。デフォルトでは URL カテゴリおよびレピュテーションはマッチングの目的では考慮されません。SSL 復号ルールの URL 基準 （17 ページ）を参照してください。
- [ユーザ（Users）]：アイデンティティ ソース、ユーザまたはユーザ グループ。アイデンティティ ポリシーは、ユーザとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティ ポリシーを設定する必要があります。SSL 復号ルールのユーザ基準 （18 ページ）を参照してください。
- [拡張（Advanced）]：SSL/TLS バージョンや証明書のステータスなどの接続に使用する証明書に由来する特性。SSL 復号ルールの詳細条件 （19 ページ）を参照してください。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、 ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

条件を SSL 復号ルールに追加する際は、以下のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、URL カテゴリに基づいて復号するために単一のルールを使用できます。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはア

プリケーション フィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。

- URL カテゴリのマッチングには、URL フィルタ リング機能のライセンスが必要です。

ステップ 7 （オプション）ルールのロギングを設定します。

ルールと一致するトラフィックをダッシュボード データまたはイベント ビューアに含めるには、ロギングを有効にする必要があります。次のオプションから選択します。

- [接続終了時（At End of Connection）]：接続の終了時にイベントを生成します。
  - [接続イベントの送信先（Send Connection Events To）]：外部の syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成（Create New Syslog Server）] をクリックして作成します（syslog サーバへのロギングを無効化するには、サーバのリストから [任意（Any）] を選択します）。

    デバイスのイベント ストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

- [ロギングなし（No Logging）]：イベントを生成しません。

ステップ 8 [OK] をクリックします。

SSL 復号ルールの送信元/送信先基準

SSL 復号ルールの [送信元/送信先（Source/Destination）] 基準で、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的ロケーション）、トラフィックで使用されている TCP ポートを定義します。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。TCP は、SSL 復号ルールに一致する唯一のプロトコルです。

条件を変更するには、その条件内の [+] ボタンをクリックして、目的のオブジェクトまたは要素を選択し、[OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1 つの基準を定義する 、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、外部ホストから内部ホストへのすべてのトラフィックが復号されたことを確認したい場合、[送信元ゾーン（Source Zones）] で外部ゾーンを選択し、[送信先ゾーン（Destination Zones）] で内部ゾーンを選択します。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）] : 制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。

（注） 既知のキーの復号ルールの場合、証明書とアップロードしたキーを使用する送信先サーバの IP アドレスを持つオブジェクトを選択します。

- [地理位置情報（Geolocation）] : 位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポートオブジェクト。SSL 復号ルールに対してのみ TCP プロトコルとポートを指定できます。

- TCP ポートからのトラフィックを一致させるには、[送信元ポート（Source Ports）] を設定します。
- TCP ポートへのトラフィックを一致させるには、[送信先ポート/プロトコル（Destination Ports/Protocols）] を設定します。
- 特定の TCP ポートから特定の TCP ポートへ発信されるトラフィックを一致させるには、両方のポートを設定します。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

SSL 復号ルールのアプリケーション基準

SSL 復号ルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタ処理が定義されます。デフォルトは、SSL プロトコル タグを持つアプリケーションです。暗号化されていないアプリケーションは SSL 復号ルールと一致できません。

ルールで個別のアプリケーションを指定できますが、アプリケーション フィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高くビジネスとの関連性が低いすべてのアプリケーションを復号またはブロックする SSL 復号ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションが復号またはブロックされます。

また、シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーション ディテクタを更新し追加します。これにより、リスクの高いアプリケーションのルールが新しいアプリケーションに自動的に適用される可能性があり、手動でルールを更新する必要がなくなります。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーションフィルタ オブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が 基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタ リストを変更するには、条件内の [+] ボタンをクリックし、別のタブに表示される目的のアプリケーションまたはアプリケーション フィルタ オブジェクトを選択してから、ポップアップ表示されるダイアログボックスで [OK] をクリックします。いずれかのタブで [詳細フィルタ（Advanced Filte）] をクリックするか、またはフィルタ条件を選択して特定のアプリケーションを検索します。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x] をクリックします。[フィルタとして保存（Save As Filter）] リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーション フィルタ オブジェクトとして保存します。

アプリケーション基準と、高度なフィルタを設定してアプリケーションを選択する方法の詳細については、アプリケーション フィルタ オブジェクトの設定を参照してください。

SSL 復号ルールでアプリケーション基準を使用する場合は、次のヒントを考慮してください。

- このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS ClientHello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。
- システムは、サーバ証明書の交換後にのみアプリケーションを識別できます。SSL ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。システムによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。
- 選択したアプリケーションが VDB の更新によって削除されていた場合は、アプリケーション名の後ろに「（廃止（Deprecated））」と表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システムソフトウェアのアップグレードがブロックされます。

SSL 復号ルールの URL 基準

SSL 復号ルールの URL の基準は、Web 要求の URL が属するカテゴリを定義します。また、復号、ブロック、または復号せずに許可するサイトの相対的なレピュテーションも指定できます。デフォルトでは、URL カテゴリに基づき接続と一致しません。

たとえば、すべての暗号化されたギャンブルサイトをブロックしたり、リスクの高いすべてのソーシャル ネットワーキング サイトを復号できます。該当するカテゴリとレピュテーションの URL をユーザが参照しようとすると、セッションがブロックされるか、または復号されます。URL カテゴリの照合の詳細については、カテゴリ別とレピュテーション別の URL のフィルタリングを参照してください。

[カテゴリ（Categories）] タブ

[+] をクリックし、目的のカテゴリを選択して、[OK] をクリックします。ポリシーからカテゴリやオブジェクトを削除するには、該当する [x] をクリックします。

デフォルトでは、レピュテーションに関係なく、選択した各カテゴリ内のすべての URL にルールが適用されます。レピュテーションに基づいてルールを制限するには、各カテゴリの下矢印をクリックして、[任意（Any）] チェックボックスを選択解除し、[レピュテーション（Reputation）] スライダを使用してレピュテーション レベルを選択します。レピュテーション スライダの左側に復号なしで許可されるサイトが示され、右側に復号またはブロックされるサイトが示されます。レピュテーションがどのように使用されるかは、ルール アクションによって異なります。

- ルールで接続が復号またはブロックされる場合は、レピュテーション レベルを選択すると、そのレベルよりも重大度が高いすべてのレピュテーションも選択されます。たとえば、**[疑わしいサイト（Suspicious sites）]**（レベル2）を復号またはブロックする

ようにルールを設定した場合、**[高リスク（High risk）]**（レベル 1）サイトも自動的に復号またはブロックします。

- ルールで復号なし（復号しない）で接続が許可される場合は、レピュテーション レベルを選択すると、そのレベルよりも重大度が低いすべてのレピュテーションも選択されます。たとえば、**[無害なサイト（Benign sites）]**（レベル 4）を復号しないルールを設定した場合、**[既知（Well known）]**（レベル 5）サイトも自動的に復号されません。

SSL 復号ルールのユーザ基準

SSL 復号ルールのユーザ基準は、IP 接続のユーザまたはユーザ グループを定義します。ルールにユーザまたはユーザ グループの基準を含めるように、アイデンティティ ポリシーと関連ディレクトリ サーバを設定する必要があります。

アイデンティティ ポリシーは、特定の接続に関してユーザ アイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストのIPアドレスに識別されたユーザが関連付けられます。したがって、送信元 IP アドレスがユーザにマッピングされているトラフィックは、そのユーザからのものとみなされます。IP パケット自体にはユーザ アイデンティティ情報は含まれていないため、この IP アドレスとユーザ間のマッピングが使用可能な中での最良近似となります。

1 つのルールに最大 50 のユーザまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザを選択するより有意義です。たとえば、外部ネットワークからエンジニアリング グループへのトラフィックを復号化するルールを作成し、そのグループからの発信トラフィックを復号化しない別のルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバのエンジニアリング グループに追加するだけです。

そのソース内のすべてのユーザに適用するアイデンティティ ソースを選択することもできます。したがって、複数の Active Directory ドメインをサポートする場合は、ドメインに基づく差分復号化を提供できます。

ユーザ リストを変更するには、条件内の [+] ボタンをクリックし、次の手法のいずれかを使用して、目的のユーザまたはユーザ グループを選択します。ポリシーからユーザまたはグループを削除するには、対応する [x] をクリックします。

- [アイデンティティ ソース（Identity Sources）]：AD レルムやローカル ユーザ データベースなど、選択したソースから取得したすべてのユーザにルールを適用するアイデンティティ ソースを選択します。必要なレルムがまだ存在しない場合、[新規アイデンティティ レルムの作成（Create New Identity Realm）] をクリックして作成します。
- [グループ（Groups）]：目的のユーザ グループを選択します。グループは、ディレクトリ サーバにグループが設定されている場合のみ使用可能です。グループを選択すると、ルールはサブグループを含むグループのすべてのメンバーに適用されます。サブグループを別の方法で処理する場合は、サブグループ用の個別のアクセス ルールを作成し、それをアクセス コントロール ポリシー内で親グループのルールの上に配置する必要があります。

- [ユーザ（Users）]：個々のユーザを選択します。ユーザ名には、Realm\username などのアイデンティティ ソースがプレフィックスとして付けられます。

  Special-Identities-Realm の下にはいくつかの組み込みユーザがあります。

  - [認証失敗（Failed Authentication）]：ユーザは認証を求められましたが、最大許容試行回数内に有効なユーザ名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザのネットワークへのアクセスは妨げられませんが、これらのユーザのネットワーク アクセスを制限するためのアクセス ルールを記述できます。
  - [ゲスト（Guest）]：ゲストユーザは、これらのユーザをゲストと呼ぶようにアイデンティティ ルールが設定されている点を除き、認証失敗ユーザと同様です。ゲストユーザは認証を求められましたが、最大試行回数内に認証されることができませんでした。
  - [認証不要（No Authentication Required）]：ユーザの接続が認証なしに指定されたアイデンティティ ルールに一致したため、ユーザは認証を求められませんでした。
  - [不明（Unknown）]：IP アドレスのユーザ マッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。

SSL 復号ルールの詳細条件

詳細のトラフィックの一致条件は、接続に使用する証明書に由来する特徴に関連します。次のオプションのいずれかまたはすべてを設定できます。

証明書のプロパティ

トラフィックは、選択したプロパティのいずれかに一致する場合、ルールの証明書プロパティのオプションに一致します。次の設定を行えます。

証明書のステータス

証明書が [有効（Valid）] か [無効（Invalid）] か。証明書のステータスを気にしない場合は、[任意（Any）]（デフォルト）を選択します。

証明書は、次の条件のすべてが満たされている場合に有効とみなされ、それ以外の場合は無効とみなされます。

- ポリシーが証明書を発行した CA を信用できる。
- 証明書の署名を証明書の内容に対して正しく検証できる。
- 発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
- ポリシーの信頼できる CA のいずれも証明書を失効させていません。
- 現在の日付が証明書の [有効期間の開始（Valid From）] と [有効期間の終了（Valid To）] の期間内にある。

自己署名

サーバ証明書に同じサブジェクトおよび発行元識別名が含まれているかどうか。次のいずれかを選択します。

- [自己署名（Self-Signing）]：サーバ証明書は自己署名されています。
- [CA 署名（CA-Signing）]：サーバ証明書は認証局によって署名されています。つまり、発行元とサブジェクトは同じではありません。
- [任意（Any）]：証明書が自己署名されているかどうかを一致条件として考慮しません。

サポートされるバージョン

一致する SSL/TLS バージョン。ルールは、選択したいずれかのバージョンを使用するトラフィックにのみ適用されます。デフォルトは全バージョンです。[SSLv3.0]、[TLSv1.0]、[TLSv1.1]、[TLSv1.2] から選択します。

たとえば、TLSv1.2 の接続のみを許可する場合は、TLSv1.2 以外のバージョンにブロックルールを作成できます。

記載されていない SSL v2.0 などのバージョンを使用するトラフィックは、SSL 復号ポリシーのデフォルトのアクションによって処理されます。

既知のキーと復号の再署名の証明書の設定

再署名によってまたは既知のキーを使用して復号を実装する場合は、SSL 復号ルールが使用できる証明書を特定する必要があります。すべての証明書が有効で、期限が切れていないことを確認します。

特に既知のキーを復号する場合は、復号する接続の各宛先サーバの現在の証明書とキーがシステムにあることを確認する必要があります。既知のキーの復号ルールでは、復号の宛先サーバからの実際の証明書とキーを使用します。したがって、常に FTD デバイスに現在の証明書とキーがあることを確認する必要があります。そうでない場合復号は失敗します。

既知のキーのルールで宛先サーバの証明書またはキーを変更するたびに新しい内部証明書とキーをアップロードします。それらを内部証明書（内部 CA 証明書ではありません）としてアップロードします。次の手順の間に証明書をアップロードするか、**[オブジェクト（Objects）]**> **[証明書（Certificates）]** ページに進み、そこにアップロードします。

手順

ステップ 1 **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [SSL復号設定（SSL Decryption Settings）] ボタン（⚙）をクリックします。

ステップ 3 [再署名証明書の復号（Decrypt Re-Sign Certificate）] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成（Create Internal CA）] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールのCA証明書のダウンロード（21 ページ）も参照してください。

ステップ 4 既知のキーを使用して復号するルールごとに、宛先サーバの内部証明書とキーをアップロードします。

a) [既知のキーの証明書の復号（Decrypt Known-Key Certificates）] で [+] をクリックします。
b) 内部 ID の証明書を選択するか、[新しい内部証明書の作成（Create New Internal Certificate）] をクリックし、ここでそれをアップロードします。
c) [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

再署名の復号ルールの CA 証明書のダウンロード

トラフィックを復号する場合、ユーザは、TLS/SSL を使用するアプリケーションで信頼できるルート認証局として定義された暗号化プロセスで使用される、内部 CA 証明書を持っている必要があります。通常、証明書を生成した場合や、証明書をインポートした場合であっても、これらのアプリケーションで証明書がすでに信頼されているものとして定義されることはありません。大部分の Web ブラウザはデフォルトで、ユーザが HTTPS 要求を送信すると、Web サイトのセキュリティ証明書に問題があることを知らせる警告メッセージがクライアント アプリケーションから表示されます。通常、このエラー メッセージでは、Web サイトのセキュリティ証明書が信頼された認証局から発行されたものではないこと、または Web サイトが不明な認証局で証明されたものであることが示されますが、警告によって処理中に中間者攻撃の可能性があることが示唆される場合もあります。クライアントアプリケーションによっては、この警告メッセージがユーザに示されず、ユーザは承認されない証明書を受け入れることができません。

以下のいくつかの方法で、ユーザに必要な証明書を提供できます。

ルート証明書を受け入れるようにユーザに通知する

組織内のユーザに、企業の新しいポリシーについて通知し、組織が提供したルート証明書を、信頼できる認証局として受け入れるように指示できます。ユーザは証明書を受け入れ、信頼されたルート認証局のストレージエリアにそれを保存して、次にサイトにアクセスしたときにプロンプトが再度表示されないようにする必要があります。

（注） ユーザは、代替証明書を作成した CA 証明書を受け入れて、信頼する必要があります。そうではなく、単に代替サーバ証明書を信頼した場合は、異なる HTTPS サイトを訪問するたびに、警告が表示される状況が続きます。

クライアント デバイスにルート証明書を追加する

ネットワーク上のすべてのクライアントデバイスに、信頼できるルート認証局としてルート証明書を追加できます。そうすれば、クライアントアプリケーションは自動的にルート証明書を持つトランザクションを受け入れるようになります。

証明書を電子メールで送信するか、共有サイトに置くことで、ユーザが証明書を入手できるようにします。または、会社のワークステーションイメージに証明書を組み込み、アプリケーションの更新機能を使用して、ユーザに証明書を自動的に配布することもできます。

次に、内部 CA 証明書をダウンロードして、Windows クライアントにインストールする方法を説明します。

手順

ステップ 1 Firepower Device Manager から証明書をダウンロードします。

a) **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

b) [SSL復号設定（SSL Decryption Settings）] ボタン（⚙）をクリックします。

c) [ダウンロード（Download）] ボタン（⬇）をクリックします。

d) ダウンロード場所を選択して、必要に応じてファイル名を変更し（拡張子はそのまま）、[保存（Save）] をクリックします。

これで、[SSL復号設定（SSL Decryption Settings）] ダイアログ ボックスからキャンセルできます。

ステップ 2 クライアント システムの Web ブラウザにある信頼されたルート認証局のストレージ エリアに証明書をインストールするか、クライアント自体が証明書をインストールできるようにします。

プロセスは、オペレーティング システムとブラウザの種類によって異なります。たとえば、Windows 上で実行されている Internet Explorer および Chrome の場合は次のプロセスを使用できます。（Firefox の場合は、**[ツール（Tools）]** > **[オプション（Options）]** > **[詳細（Advanced）]** ページでインストールします。）

a) [スタート（Start）] メニューから、**[コントロールパネル（Control Panel）]** > **[インターネットオプション（Internet Options）]** を選択します。

b) [コンテンツ（Content）] タブを選択します。

c) [証明書（Certificates）] ボタンをクリックして、[証明書（Certificates）] ダイアログ ボックスを開きます。

d) [信頼されたルート証明機関（Trusted Root Certification Authorities）] タブを選択します。
e) [インポート（Import）] をクリックし、ウィザードに従ってダウンロードされたファイル（<uuid>_internalCA.crt）を見つけて選択し、信頼できるルート認証局のストアに追加します。
f) [終了（Finish）] をクリックします。

メッセージは、インポートが成功したことを示しているはずです。ユーザがよく知られたサードパーティの認証局から証明書を取得するのではなく自己署名証明書を生成した場合は、途中で Windows が証明書を検証できなかったことを警告するダイアログ ボックスが表示される場合があります。

[証明書（Certificates）] ダイアログ ボックスと [インターネットオプション（Internet Options）] ダイアログ ボックスを閉じることができます。

例：ネットワークからの古いSSL/TLSバージョンのブロック

組織によっては、政府の規制や会社のポリシーで、古いバージョンの SSL または TLS を使用できないように義務付けている場合があります。SSL 復号ポリシーを使用して、禁止する SSL/TLS バージョンを使用しているトラフィックをブロックできます。禁止されたトラフィックが即座に捕捉されるように、SSL 復号ポリシーの先頭にこのルールを配置することを検討してください。

次に、すべての SSL 3.0 および TLS 1.0 接続をブロックする例を示します。

始める前に

この手順では、SSL 復号ポリシーがすでに有効になっていると仮定します（SSL 復号ポリシーの有効化 （9 ページ）を参照）。

手順

ステップ 1 **[ポリシー（Policies）] > [SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [+] ボタンをクリックして、新しいルールを作成します。

ステップ 3 [順序（Order）] で、[1] を選択してルールをポリシーの先頭に配置するか、またはネットワークに最も適した数を選択します。

デフォルトでは、ルールはポリシーの最後に追加されます。

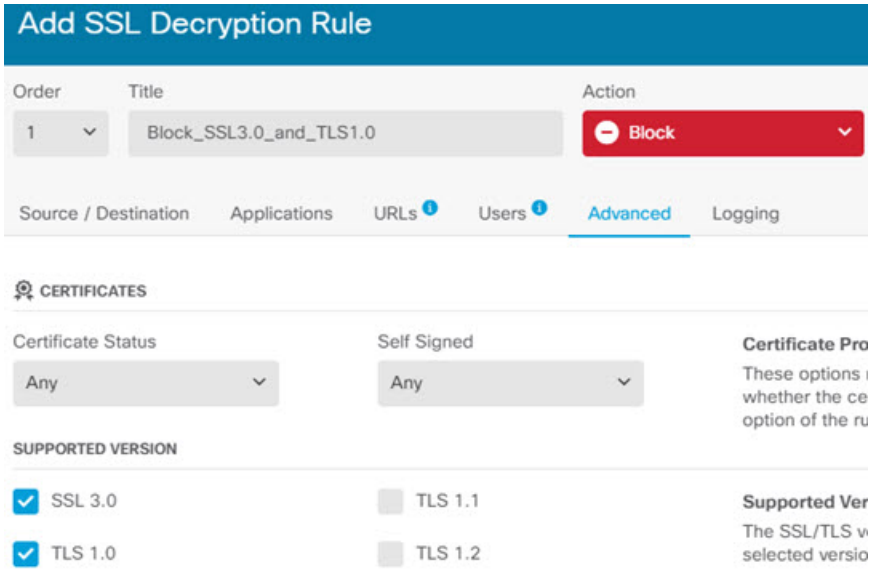
ステップ 4 [タイトル（Title）] に、ルールの名前（たとえば、Block_SSL3.0_and_TLS1.0）を入力します。

ステップ 5 [アクション（Action）] で、[ブロック（Block）] を選択します。これで、ルールに一致するすべてのトラフィックがただちにドロップされます。

ステップ 6 [送信元/宛先（Source/Destination）]、[アプリケーション（Applications）]、[URLs]、[ユーザ（Users）] の各タブについては、すべてのオプションをデフォルト値のままにします。

ステップ 7 [詳細（Advanced）] タブをクリックし、[サポートされているバージョン（Supported Versions）] の下の [SSL3.0] と [TLS1.0] を選択したままにします。ただし、[TLS1.1] と [TLS1.2] はオフにします。

ポリシーは次のようになります。



ステップ 8 （任意）ブロックされた接続をダッシュボードやイベントに反映させるには、[ロギング（Logging）] タブをクリックし、[接続終了（At End of Connection）] を選択します。外部 syslog サーバを選択することもできます（使用している場合）。

ステップ 9 [OK] をクリックします。

これでポリシーを展開できます。展開すると、システムを通過するすべての SSL 3.0 または TLS 1.0 接続がドロップされます。

（注） SSL 2.0 接続は、ポリシーのデフォルト アクションによって処理されます。これらもドロップされるようにするには、デフォルト アクションを [ブロック（Block）] に変更します。

次のタスク

このルールを実装する場合は、次の推奨事項をお勧めします。

- どのタイプの復号ルールでも、[詳細（Advanced）] タブのデフォルト設定のままにします。その場合はすべての SSL/TLS オプションが選択されます。すべてのバージョンに適用することで、ハンドシェイク プロセスが簡素化されます。ただし、最初のブロック ルールでは、SSL 3.0 および TLS 1.0 接続が引き続き妨げられます。

- 通常は、ポリシーのデフォルト アクションとして [復号しない（Do Not Decrypt）] を使用することをお勧めします。しかし、SSL 2.0 接続は常にデフォルト アクションによって処理されるため、代わりに [ブロック（Block）] を使用することもできます。ただし、すべての復号可能なトラフィックのデフォルトアクションとして [復号しない（Do Not Decrypt）] を適用する場合は、ポリシーの最後に [復号しない（Do Not Decrypt）] ルールを作成し、トラフィック一致基準のすべてのデフォルト値を受け入れます。このルールならば、テーブル内の以前のルールに一致しない、すべてのサポート対象の TLS 接続に一致し、それらの TLS バージョンにおけるデフォルトとして機能します。

SSL 復号のモニタリングとトラブルシューティング

ここでは、SSL 復号ポリシーのモニタリングおよびトラブルシューティング方法について説明します。

SSL 復号のモニタリング

ダッシュボードに復号についての情報を表示でき、ログ収集を有効化したルール（またはデフォルトのアクション）に一致するトラフィックのイベントを表示できます。

SSL 復号のダッシュボード

全体的な復号の統計情報を評価するには、**[モニタリング（Monitoring）]** > **[SSL復号（SSL Decryption）]** ダッシュボードを表示します。ダッシュボードには次の情報が表示されます。

- 暗号化されたトラフィックとプレーン テキスト トラフィックの割合。
- SSL ルールに従って、暗号化されたトラフィックがどの程度復号されたか。

イベン

ダッシュボードに加えて、イベント ビューア（**[モニタリング（Monitoring）]** > **[イベント（Events）]**）には、暗号化されたトラフィックの SSL 情報が含まれています。イベントの評価についていくつかのヒントを次に示します。

- 一致するトラフィックをブロックする SSL ルール（またはデフォルトのアクション）と一致したためにドロップされた接続の場合、[アクション（Action）] は「ブロック」、[理由（Reason）] は「SSL ブロック」であることが必要です。
- [実際のSSLアクション（SSL Actual Action）] フィールドは、システムが接続に適用した実際のアクションを示します。これは、一致するルールに定義されたアクションを示す [予期されたSSLアクション（SSL Expected Action）] とは異なります。たとえば、接続が復号を適用するルールと一致しても、いくつかの理由で復号できないことがあります。

復号再署名がブラウザでは機能するがアプリでは機能しないWebサイトの処理（SSL または認証局ピニング）

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL（または認証局）ピニング」と呼ばれる手法が使用されます。SSL ピニング手法では、元のサーバ証明書のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが再署名された証明書を Firepower Threat Defense から受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Web サイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Web ブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上のブラウザでも接続できるというのが主な症状です。たとえば、Facebook の iOS または Android アプリケーションを使用すると接続に失敗しますが、Safari または Chrome で https://www.facebook.com を指定すると接続に成功します。

SSL ピニングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

- アプリケーションのユーザをサポートします。この場合は、サイトへのトラフィックを復号できません。[SSL復号（SSL Decryption）] ルールの [アプリケーション（Application）] タブで、サイトのアプリケーションの [復号しない（Do Not Decrypt）] ルールを作成し、そのルールが、接続に適用される [再署名の復号（Decrypt Re-sign）] ルールの前に適用されることを確認します。
- ユーザにブラウザだけを使用させます。サイトへのトラフィックを復号する必要がある場合は、ネットワーク経由での接続にサイトのアプリケーションを使用できないため、ブラウザのみを使用しなければならないことをユーザに通知する必要があります。

詳細

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実に SSL ピニングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用して SSL ピニングを識別できます。

アプリケーションは、次の 2 つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ 1 のアプリケーション（Facebook など）は、サーバから SH、CERT、SHD メッセージを受け取るとすぐに SSL ALERT メッセージを送信します。アラートは、通常、SSL ピニングを示す「Unknown CA (48)」アラートです。アラート メッセージの後に TCP リセットが送信されます。イベントの詳細情報で次のような症状が見られます。
  - SSL フロー フラグには ALERT_SEEN が含まれます。
  - SSL フロー フラグには APP_DATA_C2S または APP_DATA_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE です。

- グループ 2 のアプリケーション（Dropbox など）はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってから TCP リセットを送信します。イベントで次のような症状が見られます。
  - SSL フロー フラグには ALERT_SEEN、APP_DATA_C2S または APP_DATA_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED です。

復号再署名がブラウザでは機能するがアプリでは機能しない Web サイトの処理（SSL または認証局ピニング）