SSL ルールの使用を開始するには

ここでは、SSL ルールの作成、設定、管理、トラブルシューティングの概要を示します。

SSL ルールの概要

SSL ポリシー内に各種の *SSL* ルールを設定することで、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、トラフィックを復号せずにアクセス コントロールで検査する、あるいはアクセス コントロールの分析用にトラフィックを復号するなど、複数の管理対象デバイスをカバーしたきめ細かな暗号化トラフィックの処理メソッドを構築できます。

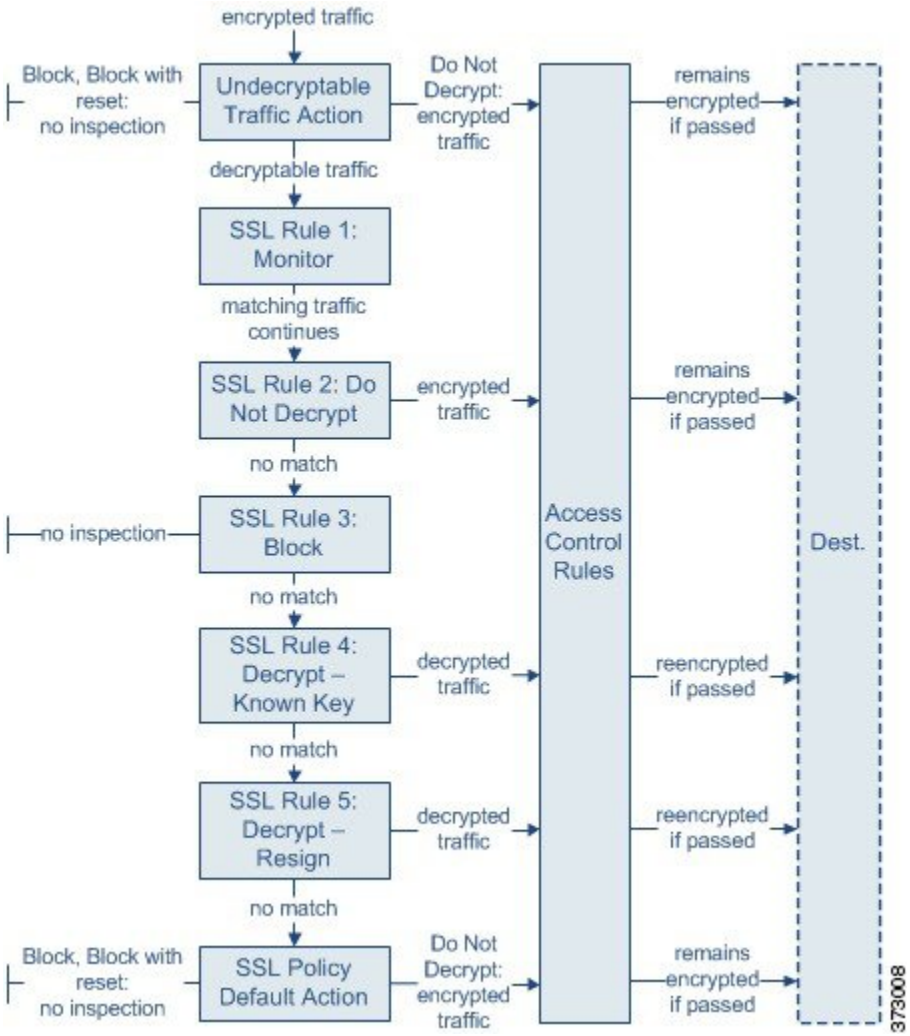
SSL ルールのトラフィック処理

システムは指定した順序で SSL ルールをトラフィックと照合します。ほとんどの場合、システムによる暗号化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 SSL ルールに従って行われます。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できないトラフィックは、アクセス コントロールを使用して検査します。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。

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。
- **SSL ルール 1：モニタ（SSL 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。

- **SSL ルール 2**：**復号しない（SSL 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。一致しないトラフィックは、引き続き次のルールと照合されます。
- **SSL ルール 3**：**ブロック（SSL 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。
- **SSL ルール 4**：**復号 - 既知のキー（SSL 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 ルール 5**：**復号 - 再署名（SSL 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 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。

暗号化トラフィック インスペクションの設定

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号には、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の SSL ポリシーへのアップロード時、SSLルール条件の作成時、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

証明書とキー ペアによる暗号化トラフィックの復号

セッション暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておくと、システムは着信する暗号化トラフィックを復号できます。[復号 - 既知

のキー（Decrypt - Known Key）] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはアップロードされた秘密キーを使用してセッションを復号します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、システムは発信トラフィックの復号もできます。[復号 - 再署名（Decrypt - Resign）] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはクライアント ブラウザに渡されたサーバ証明書を再署名した後、中間者（man-in-the-middle）としてセッションを復号します。オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

暗号化セッションの特性に基づいたトラフィック制御

システムによる暗号化トラフィックの制御は、セッション ネゴシエートに使用されたサーバ証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、SSL ルール条件でオブジェクトを参照してトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使用される暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する。
組織が信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する。 • CA が証明書を直接発行した。 • サーバ証明書を発行した中間 CA に CA が証明書を発行した。
サーバ証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する。
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名と一致する。

関連トピック

暗号スイート リスト
識別名オブジェクト
PKI オブジェクト

SSL ルールのコンポーネント

各 SSL ルールには、一意の名前以外にも、次の基本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（Position）

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、ルールが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。

ヒント 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

SSL ルールの作成および変更

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
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]**を選択します。

ステップ 2 SSL ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 次の選択肢があります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（）をクリックします。

ステップ 4 名前を入力します。

ステップ 5 上記に要約されるようにルール コンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを**有効**にするかどうかを指定します。
- ルールの位置を指定します。SSL ルールの順序の評価 （7 ページ） を参照してください。
- [アクション（Action）] で、ルールのアクションを選択します。SSL ルール アクションの設定 （16 ページ）を参照してください。
- ルールの条件を設定します。SSL ルールの条件タイプ （9 ページ） を参照してください。

- [ログ（Logging）] オプションを指定します。SSL ルールによる復号可能接続のロギングを参照してください。

ステップ 6 [保存（Save）] をクリックします。

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。

SSL ルールの順序の評価

SSL ルールを最初に作成するときに、ルール エディタの [挿入（Insert）] ドロップダウン リストを使用して、その位置を指定します。SSL ポリシーの SSL 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、SSL ルールを上から順に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 SSL 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**。

ヒント 適切な 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

ルールのパフォーマンスに関するガイドライン

ルール カテゴリへの SSL ルールの追加

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）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタの [挿入（Insert）] ドロップダウン リストで [カテゴリ（Into Category）] を選択し、使用するカテゴリを選択します。

ステップ 2 [保存（Save）] をクリックします。

ヒント ルールを保存すると、そのカテゴリの最後に配置されます。

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。

番号による SSL ルールの配置

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）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタの [挿入（Insert）] ドロップダウンリストで、[ルールの上（above rule）] または [ルールの下（below rule）] を選択して、適切なルール番号を入力します。

ステップ 2 [保存（Save）] をクリックします。

ヒント ルールを保存すると、指定した場所に配置されます。

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。

SSL ルール条件

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、証明書の条件が設定され、バージョンの条件が設定されていないルールは、セッションSSLまたはTLSのバージョンにかかわりなく、セッションのネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価します。

すべてのSSLルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理：最も重要なこととして、ルール アクションはルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号を行うかどうかを判定します。
- ロギング：ルールアクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

SSLインスペクション設定では、次のように復号されたトラフィックの処理、検査、ログ記録を行います。

- SSLポリシーの復号できないアクションは、システムが復号できないトラフィックを処理します。
- ポリシーのデフォルト アクションは、モニタ以外のどの SSL ルールの条件にも一致しないトラフィックを処理します。

システムが暗号化セッションを信頼またはブロックしたときに、接続イベント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。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- 信頼された接続（Do not decrypt）の場合、システムはセッション終了時にイベントを生成します。

SSL ルールの条件タイプ

SSLルールを追加および編集するときは、ルールエディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。

表 *1 : SSL* ルールの条件タイプ

条件	一致する暗号化トラフィック	詳細（**Details**）
ゾーン	特定のセキュリティゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信	セキュリティゾーンは、ご使用の導入ポリシーおよびセキュリティポリシーに準じた 1 つ以上のインターフェイスの論理グループです。ゾーン内のインターフェイスは、複数のデバイスにまたがって配置される場合があります。
ネットワーク	その送信元または宛先 IP アドレス、国、または大陸による	IP アドレスを明示的に指定できます。位置情報機能を使用して、その送信元または宛先の国または大陸に基づいてトラフィックを制御できます。
VLAN タグ	VLAN のタグ	システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。
ポート	その送信元または宛先ポートによる	TCP ポートに基づいて暗号化トラフィックを制御できます。
Users	セッションに関与するユーザによる	暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化トラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。
アプリケーション	セッションで検出されたアプリケーションによる	タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタ アクセスまたは暗号化セッションの各アプリケーションへのアクセスを制御できます。
カテゴリ	証明書サブジェクトの識別名に基づいてセッションで要求される URL	URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。
識別名	暗号化セッションのネゴシエートに使用されたサーバ証明書のサブジェクトまたは発行元の識別名	サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。

条件	一致する暗号化トラフィック	詳細（Details）
証明書（Certificates）	暗号化セッションのネゴシエートに使用されるサーバ証明書	暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。
証明書のステータス（Certificate Status）	暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ	サーバ証明書のステータスに基づいて、暗号化トラフィックを制御できます。
暗号スイート	暗号化セッションのネゴシエートに使用する暗号スイート	暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。
バージョン	セッションの暗号化に使用される SSL または TLS のバージョン	セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。

関連トピック

ネットワーク ベースの SSL ルールの条件
ユーザベースの SSL ルールの条件
暗号化トラフィックでのレピュテーションベースの URL ブロッキング
サーバ証明書ベースの SSL ルール条件
ClientHello メッセージ処理

SSL ルールのアクション

SSL ルール：モニタ アクション

[モニタ（Monitor）] アクションは暗号化トラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号するかが決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタ ルールの主要な目的はネットワーク トラフィックを追跡することであるため、ルールのロギング設定や、あとで接続を処理するデフォルトのアクションにかかわらず、システムはモニタ対象トラフィックの接続終了イベントを自動的に Firepower Management Center データベースに記録します。

SSL ルール：復号しないアクション

[復号しない（Do not decrypt）] アクションは、アクセス コントロール ポリシーのルールおよびデフォルトアクションに従って暗号化トラフィックを評価するため転送します。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、こうし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。暗号化トラフィックに対しては、侵入やファイル インスペクションなどのディープ インスペクションを行うことはできません。

[復号しない（Do not decrypt）] ルールの一般的な理由は、以下のとおりです。

- SSL トラフィックの復号が法律によって禁止されている。
- 信頼できると判明しているサイトである。
- トラフィックを調べることによって中断できるサイト（Windows Update など）である。
- SSL フィールドの値を表示するには、接続イベントを使用します。（接続イベント フィールドを表示するためにトラフィックを復号化する必要はありません。）詳細については、接続イベント フィールドの入力の要件を参照してください。

詳細については、次を参照してください。 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：ブロッキング アクション

[ブロック（Block）] および [リセットしてブロック（Block with reset）] アクションは、アクセス コントロール ルールの [ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションに類似しています。これらのアクションは、クライアントとサーバによる SSL 暗号化セッションの確立と暗号化トラフィックの転送を防止します。リセット付きブロック ルールでは接続のリセットも行います。

ブロックされた暗号化トラフィックについては、設定された応答ページが表示されないので注意してください。その代わりに、ユーザの要求する禁止された URL の接続は、リセットされるか、またはタイムアウトになります。

ヒント パッシブまたはインライン（タップ モード）展開では、デバイスがトラフィックを直接検査しないので、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用できないことに注意してください。パッシブまたはインライン（タップ モード）インターフェイスを含むセキュリティ ゾーン条件内で、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用したルールを作成すると、ポリシー エディタでルールの横に警告アイコン（）が表示されます。

関連トピック

HTTP 応答ページについて

SSL ルール：復号アクション

[復号 - 既知のキー（Decrypt - Known Key）] および [復号 - 再署名（Decrypt - Resign）] アクションは、暗号化トラフィックを復号します。復号されたトラフィックは、アクセス制御を使用して検査されます。アクセス コントロール ルールは、復号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。ここではデータの確認に加えて、侵入、禁止ファイル、マルウェアを検出およびブロックできます。システムは、許可されたトラフィックを再暗号化してから宛先に渡します。

信頼できる認証局（CA）の証明書を使用してトラフィックを復号化することをお勧めします。これにより、Web ブラウザに「接続がプライベートではありません（Your connection is not private）」、「無効な証明書発行者（Invalid Certificate Issuer）」、または「ERR_CERT_AUTHORITY_INVALID」などのエラーが表示されることを防ぎます。これにより、Firepower Management Center でのこれらのエラーのロギングも低減します。

信頼できるオブジェクトを追加する方法の詳細については、信頼できる認証局オブジェクトを参照してください。

SSL ルールの復号メカニズムとガイドライン

[復号 - 既知のキー（Decrypt - Known Key）] アクションを設定した場合は、1 つまたは複数のサーバ証明書と秘密キーペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、システムは適切な秘密キーを使用してセッションの暗号化と復号キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号する場合です。

同様に [復号 - 再署名（Decrypt - Resign）] アクションには、1 つの認証局証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、システムは 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。各セッションにはさまざまな暗号セッションの詳細が含まれており、システムはこれを使用することでトラフィックの復号化と再暗号化が行えます。このアクションは、証明書の秘密キーを各自の管理下にあるキーに置き換えてセッション キーを取得するため、発信トラフィックに適しています。

サーバ証明書の再署名では、証明書の公開キーを CA 証明書の公開キーに置き換えるか、あるいは証明書全体が置き換えられます。通常、サーバ証明書全体を置き換える場合は、SSL 接続が確立された時点で、証明書が信頼できる認証局によって署名されていないことがクライアント ブラウザで警告されます。ただし、その CA をクライアント ブラウザで信頼できることがポリシーに設定されている場合、ブラウザは証明書が信頼できないことについて警告しません。オリジナルのサーバ証明書が自己署名の場合、システムは証明書全体を置き換えて再署名する CA を信頼しますが、ユーザのブラウザは証明書が自己署名されていることを警告しません。この場合、サーバ証明書の公開キーを交換するだけで、クライアントブラウザは証明書が自己署名であることを警告します。

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部 CA 証明書の署名アルゴ

リズム タイプに基づいて実施されます。各 [復号 - 再署名（Decrypt - Resign）] アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、異なる署名アルゴリズムで暗号化された複数のタイプの発信トラフィックを復号化する SSL ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが [復号 - 再署名（Decrypt - Resign）] ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成する場合は、EC ベースの外部証明書と暗号スイートをルールに追加する必要があります。同様に、RSA ベースの CA 証明書を参照する [復号 - 再署名（Decrypt - Resign）] ルールは、RSA アルゴリズムで暗号化された発信トラフィックとのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

次の点に注意してください。

- SSL 接続の確立に使用される暗号スイートが Diffie-Hellman Ephemeral（DHE）または楕円曲線 Diffie-Hellman Ephemeral（ECDHE）キー交換アルゴリズムを適用している場合、パッシブ展開では [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。SSL ポリシーのターゲット デバイスにパッシブまたはインライン（タップ モード）インターフェイスがあり、そこに含まれる [復号 - 既知のキー（Decrypt - Known Key）] ルールで DHE または ECDHE の暗号スイート条件が使われている場合、ルールの横に情報アイコン（[]）が表示されます。パッシブまたはインライン（タップモード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン（  ）が表示されます。

- デバイスはトラフィックを直接検査しないため、パッシブまたはインライン（タップモード）展開では [復号 - 再署名（Decrypt - Resign）] アクションを使用できません。セキュリティ ゾーン内にパッシブまたはインライン（タップ モード）インターフェイスを含む [復号 - 再署名（Decrypt - Resign）] アクションを指定してルールを作成すると、ポリシー エディタでルールの横に警告アイコン（  ）が表示されます。

  SSL ポリシーのターゲット デバイスにパッシブまたはインライン（タップ モード）インターフェイスがあり、そこに [復号 - 再署名（Decrypt - Resign）] ルールが含まれる場合、ルールの横に情報アイコン（  ）が表示されます。パッシブまたはインライン（タップモード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン（[]）が表示されます。パッシブまたはインライン（タップモード）インターフェイスを含むデバイスに、[復号 - 再署名（Decrypt - Resign）] ルールを含む SSL ポリシーを適用した場合、このルールに一致する SSL セッションはすべて失敗します。

- 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。これを防ぐには、クライアントの信頼できる 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により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。

- SSL ルールの**暗号スイート**条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - ClientHello 処理中に自動的に匿名の暗号スイートが削除されます。ルールを使用するシステムでは、ClientHello の処理を防止するために SSL ルールを設定する必要があります。詳細については、SSL ルールの順序を参照してください。
  - システムは匿名の暗号スイートで暗号化されたトラフィックを復号化できないため、ルールで [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションは使用できません。
- クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。システムによるこのトラフィックの処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号できないアクションが決定します。
- システムは、管理対象デバイス上のキャプティブ ポータルのユーザの Web ブラウザとキャプティブ ポータルのデーモン間のキャプティブ ポータルの認証接続でトラフィックを復号化できません。
- [復号 - 既知のキー（Decrypt - Known Key）] アクションを指定して SSL ルールを作成した場合は、[識別名（Distinguished Name）] や [証明書（Certificate）] 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。
- 内部 CA オブジェクトを作成して証明書署名要求（CSR）の生成を選択した場合は、オブジェクトに署名付き証明書をアップロードするまで、この CA を [復号 - 再署名（Decrypt - Resign）] アクションに使用できません。
- [復号 - 再署名（Decrypt - Resign）] アクションをルールに設定し、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシー エディタでルールの横に情報アイコン（  ）が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン（[]）が表示され、SSL ポリシーに関連付けたアクセス コントロール ポリシーは適用できなくなります。
- ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して SSL ルールを設定します。
- [インタラクティブ ブロック（Interactive Block）] または [リセット付きインタラクティブ ブロック（Interactive Block with reset）] アクション付きのアクセス コントロール ルールと復号化トラフィックが一致する場合、システムは応答ページを表示します。
- インライン正規化プリプロセッサで [余剰ペイロードの正規化（Normalize Excess Payload）] オプションを有効にすると、プリプロセッサによる復号トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。こ

れによりSSLセッションは終了しません。トラフィックが許可された場合、トリミングされたパケットはSSLセッションの一部として暗号化されます。

関連トピック

PKI オブジェクト

SSL ルール アクションの設定

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
任意（Any）	任意（Any）	すべて（NGIPSvを除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ポリシー エディタには、次のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（  ）をクリックします。

ステップ 2 [アクション（Action）] ドロップダウン リストからルール アクションを選択します。

- 暗号化トラフィックをブロックするには、[ブロック（Block）] を選択します。
- 暗号化トラフィックをブロックし、接続をリセットするには、[リセットでブロック（Block with reset）] を選択します。
- 着信トラフィックの復号の詳細については、復号 - 既知のキー アクションの設定 （17ページ）を参照してください。
- 発信トラフィックの復号の詳細については、復号 - 再署名アクションの設定 （17ページ）を参照してください。
- 暗号化トラフィックを記録するには、[モニタ（Monitor）] を選択します。
- 暗号化トラフィックを復号しない場合は、[復号化しない（Do Not Decrypt）] を選択します。

ステップ 3 [追加（Add）] をクリックします。

次のタスク

- ネットワーク ベースの SSL ルールの条件、ユーザベースの SSL ルールの条件、レピュテーション ベースの SSL ルール条件、およびサーバ証明書ベースの SSL ルール条件の説明に従ってルール条件を設定します。
- 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。

復号 - 再署名アクションの設定

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
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタで、[アクション（Action）] リストから [復号 - 再署名（Decrypt - Resign）] を選択します。

ステップ 2 リストから内部 CA 証明書のオブジェクトを選択します。

ステップ 3 証明書全体ではなく証明書公開キーのみを置き換えるには、**[キー置換のみ（Replace Key Only）]** をオンにする必要があります。公開キーのみを置き換えようとしているため、自己署名証明書の通知がユーザのブラウザに表示されます。

ステップ 4 [追加（Add）] をクリックします。

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。

復号 - 既知のキー アクションの設定

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）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

始める前に

[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、Firepower Management Center（**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** >

[PKI] > [信頼できる CA（Trusted CAs）]）で信頼できる CA を定義している必要があります。詳細については、信頼できる CA オブジェクトの追加を参照してください。

手順

ステップ 1 SSL ルール エディタで、[アクション（Action）] ドロップダウン リストから、[復号 - 既知のキー（Decrypt - Known Key）] を選択します。

ステップ 2 [クリックして復号証明書を選択（Click to select decryption certs）] フィールドをクリックします。

ステップ 3 [使用可能な証明書（Available Certificates）] リストの 1 つ以上の内部証明書のオブジェクトを選択し、[ルールに追加（Add to Rule）] をクリックします。

ステップ 4 [OK] をクリックします。

ステップ 5 [追加（Add）] をクリックします。

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。

SSL ルールの管理

SSL ポリシー エディタの [ルール（Rules）] タブでは、ポリシー内の SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、およびその他の管理を行うことができます。

SSL ルール検索

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、SSL ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、`100Bao` という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションが追加された各ルールの [アプリケーション（Applications）] 列が強調表示されます。`100Bao` という名前のルールもある場合は、[名前（Name）] 列と [アプリケーション（Applications）] 列の両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

SSL ルールの検索

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
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ポリシー エディタで、[検索ルール（Search Rules）] プロンプトをクリックし、検索文字列を入力してから Enter キーを押します。

ヒント 一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ステップ 2 目的のルールを見つけます。

- 照合ルールの間を移動する場合は、次の一致アイコン（▼）または前の一致アイコン（▲）をクリックします。
- ページを更新し、検索文字列および強調表示をクリアするには、クリア アイコン（✖）をクリックします。

SSL ルールの有効化と無効化

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
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

作成したSSLルールは、デフォルトで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。SSLポリシーのルール リストを表示すると、無効なルールはグレー

表示されますが、変更は可能です。またはルール エディタを使用して SSL ルールを有効または無効にできることに注意してください。

手順

ステップ 1 SSL ポリシー エディタで、ルールを右クリックしてルール状態を選択します。

ステップ 2 [保存（Save）] をクリックします。

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。

SSL ルールの移動

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
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ポリシー エディタで、各ルールの空白部分をクリックしてルールを選択します。

ステップ 2 ルールを右クリックして、[切り取り（Cut）] を選択します。

ステップ 3 切り取ったルールを貼り付けたい位置に隣接するルールの空白部分を右クリックし、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。

ヒント 2 つの異なる SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできません。

ステップ 4 [保存（Save）] をクリックします。

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。

新しい SSL ルール カテゴリの追加

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
任意（Any）	任意（Any）	すべて（NGIPSvを除く）	任意（Any）	Admin/Access Admin/Network Admin

余計なポリシーを作成することなくルールをさらに整理するため、標準ルールとルート ルールのカテゴリの間にカスタム カテゴリを作成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

手順

ステップ 1 SSL ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入（Insert new category）] を選択することもできます。

ステップ 2 [名前（Name）] を入力します。

ステップ 3 次の選択肢があります。

- 最初の [挿入（Insert）] ドロップダウン リストから [カテゴリの上（above Category）] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- ドロップダウン リストから [ルールの下（below rule）] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- ドロップダウン リストから [ルールの上（above rule）] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4 [OK] をクリックします。

ヒント 削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5 [保存（Save）] をクリックします。

SSL ルールのトラブルシューティング

SSL ルールを適切に設定するのは複雑なタスクですが、暗号化トラフィックを処理する有効な導入には不可欠のタスクです。ルールが互いをプリエンプトしたり、追加ライセンスが必要になったりすることがあります。また、ルールに無効な設定が含まれる可能性もあります。慎重に設定された SSL ルールは、ネットワーク トラフィックの処理に必要なリソースの軽減にも寄与します。過度に複雑なルールを作成し、ルールを誤って順序付けすると、パフォーマンスに悪影響を与える可能性があります。詳細については、ルールのパフォーマンスに関するガイドラインを参照してください。

SSL ルールの無効な設定に対する警告

SSL ポリシーが依存する外部の設定は変更される可能性があるため、有効であった SSL ポリシー設定が無効になる場合があります。次の例について考えてみます。

- URL カテゴリ条件を含むルールで、それまで有効であったものが、URL フィルタリング ライセンスを持たないデバイスをターゲットにすることで無効になる場合があります。その時点で、ルールの横にエラーアイコンが表示され、ポリシーをそのデバイスに展開できなくなります。展開可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- [復号 - 再署名（Decrypt-Resign）] ルールを作成し、後でパッシブ インターフェイスでセキュリティ ゾーンを条件として追加した場合、ルールの横に警告アイコンが表示されます。パッシブ展開では証明書の再署名によるトラフィックの復号はできないので、パッシブインターフェイスをルールから削除するか、またはルールアクションを変更するまで、このルールには効果がありません。
- ルールにユーザまたはグループを追加した後、そのユーザまたはグループを除外するようにレルムの設定を変更すると、ルールは適用されなくなります。（レルムを無効にする場合も同様です。）
- ServerHello またはサーバ証明書条件（証明書、識別名、証明書のステータス、暗号スイート、バージョン）と一致する [復号しない（Do Not Decrypt）] ルールを、ClientHello 条件（ゾーン、ネットワーク、VLAN タグ、ポート、ユーザ、アプリケーション、カテゴリ）で照合する [復号 - 再署名（Decrypt - Resign）] ルールの前に配置する場合、ClientHello の変更をプリエンプション処理して、復号されないセッションの数を増やすことができます。

  システムがこの設定に含まれるルールを識別すると、ServerHello またはサーバ証明書条件を使用するルールの横に警告アイコンが表示されます。

関連トピック

ルールとその他のポリシーの警告
ルールのパフォーマンスに関するガイドライン