SSL ポリシーの作成の開始

ここでは、SSL ポリシーの作成、設定、管理、およびロギングの概要を示します。

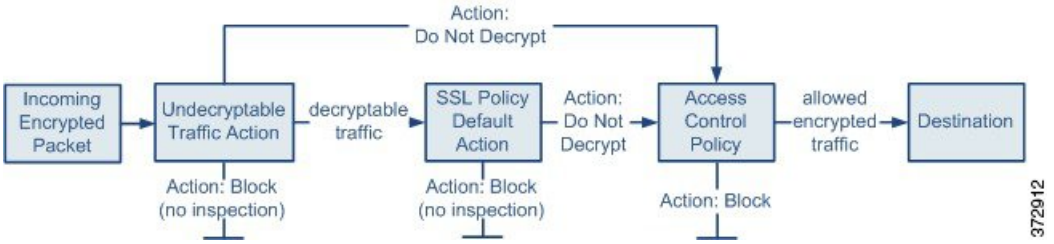
SSL ポリシーの概要

SSL ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。1 つ以上の SSL ポリシーを設定し、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から、そのアクセス コントロール ポリシーを管理対象デバイスに展開することができます。デバイスで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックを処理して検査します。次に TCP 接続上で TLS/SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号を行います。

注意 SSL ポリシーを追加または削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作を参照してください。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルト アクションで暗号化トラフィックを処理するように展開先のデバイスに指示します。デフォルト アクションの設定では、それ以上のインスペクションなしで復号可能トラフィックをブロックするか、復号されていない復号可能トラフィックをアクセスコントロールで検査するように指定できます。システ

ムは、暗号化されたトラフィックを許可するか、またはブロックできます。デバイスは復号できないトラフィックを検出すると、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ままにして、アクセス コントロールによる検査を行います。



より複雑なSSLポリシーでは、各種の復号できないトラフィックをさまざまなアクションで処理できます。また、認証局（CA）が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSLルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。

（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

TLS/SSL ルール条件

SSL ポリシーのデフォルト アクション

SSLポリシーのデフォルトアクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。TLS/SSLルールがまったく含まれないSSLポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルト アクションが決定します。デフォルト アクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

表 *1 : SSL* ポリシーのデフォルト アクション

デフォルト アクション	暗号化トラフィックに対して行う処理
ブロック（Block）	それ以上のインスペクションは行わずに TLS/SSL セッションをブロックします。
Block with reset	それ以上のインスペクションは行わずに TLS/SSL セッションをブロックし、TCP 接続をリセットします。トラフィックに UDP のようなコネクションレス型プロトコルが使用される場合は、このオプションを選択します。この場合、コネクションレス型プロトコルにより、リセットされるまで接続の再確立が試みられます。 また、このアクションでは、ブラウザの接続リセット エラーも表示されるため、接続がブロックされたことがユーザに通知されます。
復号しない（Do not decrypt）	アクセス コントロールを使用して暗号化トラフィックを検査します。

関連トピック

基本的な SSL ポリシーの作成 （6 ページ）

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

表 *2 :* 復号できないトラフィック タイプ

タイプ（Type）	説明	デフォルト アクション	使用可能なアクション
圧縮されたセッション（Compressed Session）	TLS/SSL セッションはデータ圧縮メソッドを適用します。	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） デフォルト アクションを継承する（Inherit default action）

タイプ（Type）	説明	デフォルト アクション	使用可能なアクション
SSLv2 セッション（SSLv2 Session）	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、ClientHello メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 であることに注意してください。	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） デフォルト アクションを継承する（Inherit default action）
不明な暗号スイート（Unknown Cipher Suite）	システムが認識できない暗号スイートです。	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） デフォルト アクションを継承する（Inherit default action）
サポートされていない暗号スイート（Unsupported Cipher Suite）	検出された暗号スイートに基づく復号を、システムはサポートしていません。	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） デフォルト アクションを継承する（Inherit default action）
セッションが未キャッシュ（Session not cached）	TLS/SSL セッションでセッションの再利用が有効化されており、クライアントとサーバがセッション識別子を使ってセッションを再確立しているのに、システムでセッション識別子がキャッシュされていません。	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） デフォルト アクションを継承する（Inherit default action）

タイプ（Type）	説明	デフォルト アクション	使用可能なアクション
ハンドシェイク エラー（Handshake Errors）	TLS/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。	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） デフォルト アクションを継承する（Inherit default action）
復号エラー（Decryption Errors）	トラフィックの復号中にエラーが発生しました。	ブロック（Block）	ブロック（Block） リセットしてブロック（Block With Reset）

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。復号できないトラフィックの処理ではデフォルトアクションのログ設定も適用されるため、復号できないトラフィックのアクションで処理される接続のログは、デフォルトでは無効化されています。

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ないことに注意してください。詳細については、TLS/SSL ルールのガイドラインと制限事項を参照してください。

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を設定する （7 ページ）

SSL ポリシーの管理

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

SSL ポリシー エディタでは、次の操作を実行できます。

- ポリシーを設定する。
- TLS/SSL ルールを追加、編集、削除、有効化、無効化、および編成する。
- 信頼できる CA 証明書を追加する。
- システムが復号できない暗号化トラフィックに対する処理を決定する。
- デフォルト アクションおよび復号できないトラフィック アクションで処理されるトラフィックのログを記録する。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[Policies]** > **[Access Control]** > **[SSL]**を選択します。

ステップ 2 SSL ポリシーを管理します。

- 関連付け：アクセス コントロール ポリシーに SSL ポリシーを関連付ける場合は、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。
- [比較（Compare）]：[ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較 を参照）。
- コピー：コピー アイコン（  ）をクリックします。
- 作成：[新規ポリシー（New Policy）] をクリックします。基本的な SSL ポリシーの作成 （6 ページ）を参照してください。
- 削除：削除アイコン（  ）をクリックします。コントロールが淡色表示されている場合、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。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 を参照）。
- 編集：編集アイコン（  ）をクリックします。SSL ポリシーの編集 （9 ページ）を参照してください。 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。
- インポート/エクスポート：コンフィギュレーションのインポート/エクスポートについてを参照してください。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成 を参照）。

基本的な SSL ポリシーの作成

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

SSL ポリシーの設定では、ポリシーに一意の名前を付け、デフォルト アクションを指定する必要があります。

手順

ステップ 1 **[Policies]** > **[Access Control]** > **[SSL]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

ステップ 4 [デフォルト アクション（Default Action）] を指定します。SSL ポリシーのデフォルト アクション （2 ページ）を参照してください。

ステップ 5 ポリシーのデフォルト アクションによる接続のロギングの説明に従って、デフォルト アクションのロギング オプションを設定します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- SSL ポリシーに追加するルールを設定します。TLS/SSL ルールの作成と変更を参照してください。
- 復号化できないトラフィックのデフォルト処理を設定します。復号できないトラフィックのデフォルト処理を設定する （7 ページ）を参照してください。
- 復号化できないトラフィックのデフォルト処理のロギング オプションを設定します。ポリシーのデフォルト アクションによる接続のロギングを参照してください。
- アクセス制御への他のポリシーの関連付けの説明に従って、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。
- 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。

復号できないトラフィックのデフォルト処理を設定する

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

システムによる復号や検査ができない特定タイプの暗号化トラフィックの処理については、SSL ポリシー レベルで、復号できないトラフィックのアクションを設定できます。TLS/SSL ルールが含まれない SSL ポリシーを展開する場合、ネットワーク上のすべての復号できない暗

号化トラフィックの処理方法は、復号できないトラフィックのアクションによって決定されます。

復号できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロック。
- 接続をブロックした後でリセットする。接続がブロックされるまで接続を試行し続ける UDP などのコネクションレス型プロトコルの場合、このオプションをお勧めします。
- アクセス コントロールを使用して暗号化トラフィックを検査します。
- SSL ポリシーのデフォルト アクションを継承する。

手順

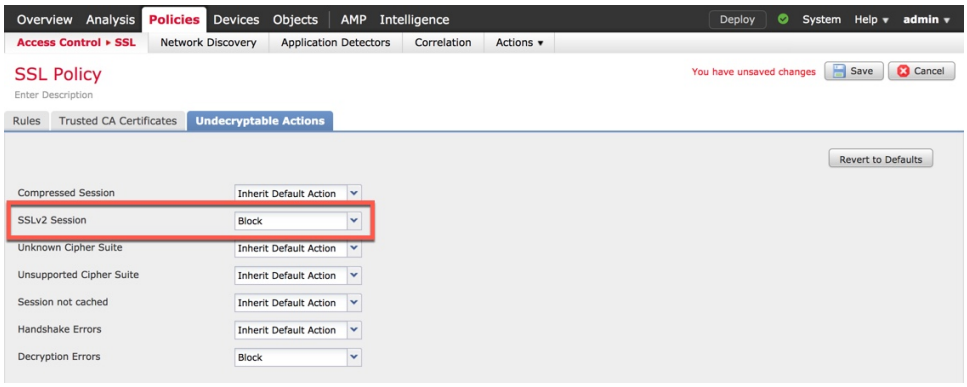
ステップ 1 SSL ポリシー エディタで、[復号できないアクション（Undecryptable Actions）] タブをクリックします。

ステップ 2 各フィールドで、SSL ポリシーのデフォルトアクションを選択するか、復号できないタイプのトラフィックに対して実行する別のアクションを選択します。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 （3 ページ）と SSL ポリシーのデフォルト アクション （2 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックしてポリシーを保存します。

例

たとえば、すべての SSLv2 トラフィックをブロックするには、次のようにオプションを設定します。



次のタスク

- 復号できないトラフィックのアクションで処理される接続に関するデフォルトロギングを設定します。ポリシーのデフォルト アクションによる接続のロギングを参照してください。
- 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 ポリシーの編集

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

ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 **[Policies]** > **[Access Control]** > **[SSL]**を選択します。

ステップ 2 設定する 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 SSL ポリシーを設定します。

- 説明：SSL ポリシーの説明を更新するには、[説明（Description）] フィールドをクリックし、新しい説明を入力します。
- ログ：復号できないトラフィックの処理および SSL ルールに一致しないトラフィックについて接続を記録するには、ポリシーのデフォルトアクションによる接続のロギングを参照してください。
- 名前の変更：SSL ポリシーの名前を変更するには、[名前（Name）] フィールドをクリックし、新しい名前を入力します。
- デフォルト アクションの設定：SSL ポリシーが SSL ルールに一致しないトラフィックをどのように処理するかを設定するには、SSL ポリシーのデフォルト アクション （2 ページ）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アクションの設定：SSL ポリシーが復号できないトラフィックをどのように処理するかを設定するには、復号できないトラフィックのデフォルト処理を設定する （7 ページ）を参照してください。
- 信頼：SSL ポリシーに信頼された CA 証明書を追加するには、外部認証局の信頼を参照してください。

ステップ 4 SSL ポリシー内のルールを編集します。

- 追加：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。
- コピー：ルールをコピーするには、選択したルールを右クリックして、[コピー（Copy）] を選択します。
- 切り取り：ルールを切り取るには、選択したルールを右クリックして、[切り取り（Cut）] を選択します。
- 削除：ルールを削除するには、ルールの横にある削除アイコン（  ）をクリックして、[OK] をクリックします。
- 無効化：有効なルールを無効にするには、選択したルールを右クリックして、[状態（State）] を選択し、[無効（Disable）] を選択します。
- 表示：特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク（Source Networks）] カラムに示されている名前または値をクリックすると、選択したルールの [ネットワーク（Networks）] ページが表示されます。詳細については、TLS/SSL のルールの条件を参照してください。
- 編集：ルールを編集するには、ルールの横にある編集アイコン（  ）をクリックします。
- 有効化：無効なルールを有効にするには、選択したルールを右クリックして、[状態（State）] を選択し、[有効（Enable）] を選択します。無効なルールはグレー表示され、ルール名の下に [（無効）（(disabled)）] というマークが付きます。
- 貼り付け：切り取られたルールまたはコピーされたルールを貼り付けるには、選択したルールを右クリックして、[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。

ステップ 5 設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[保存（Save）] をクリックします。
- 変更を廃棄する場合は、[キャンセル（Cancel）]をクリックし、プロンプトが出たら [OK] をクリックします。

次のタスク

- SSL ポリシーがアクセス コントロール ポリシーにまだ関連付けられていない場合は、アクセス制御への他のポリシーの関連付けの説明に従って関連付けます。
- 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。

関連トピック

TLS/SSL ルールの作成と変更