CHAPTER 21

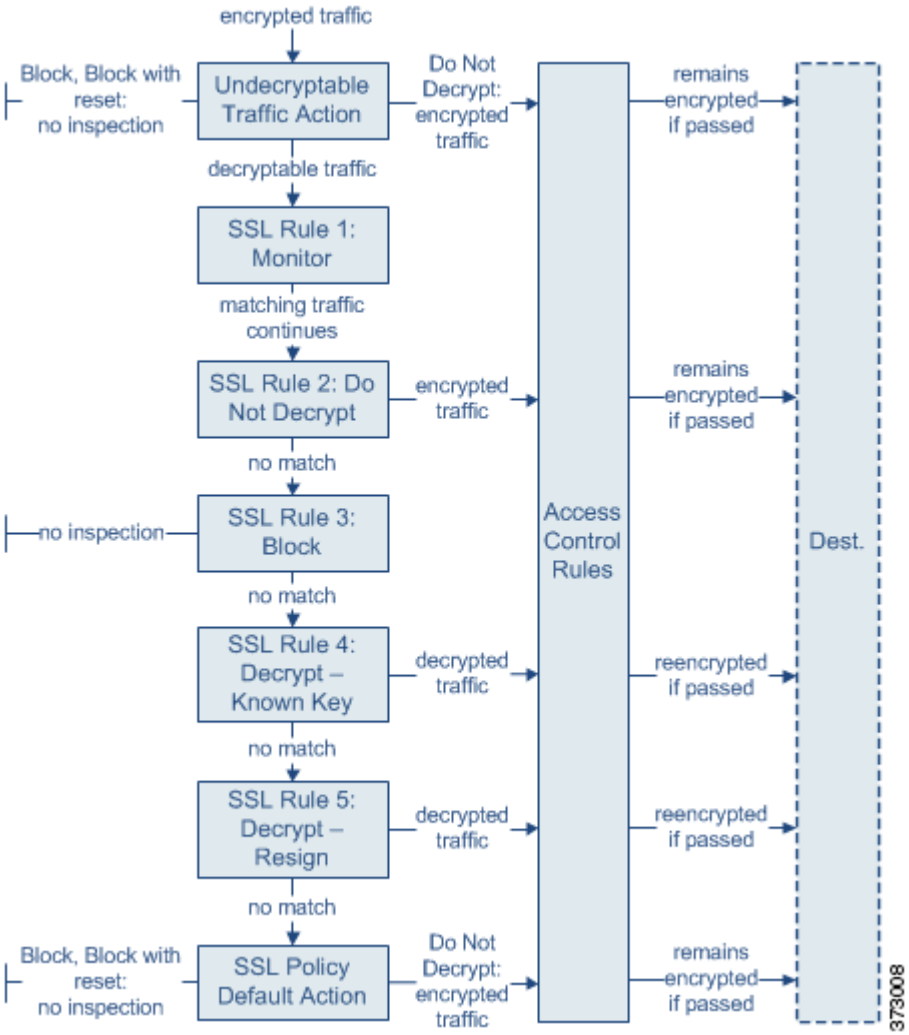
SSL ルールの準備

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。

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。

また、各ルールには 1 つの *アクション*があり、一致するトラフィックの復号後にオプションでモニタするか、ブロックするか、または一致したトラフィックをアクセス コントロールで検査するかを決定します。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。この追加インスペクションの結果、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。この追加インスペクションの結果、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。

詳細については、次の項を参照してください。

- サポートする検査情報の設定(21-3 ページ)
- SSL ルールの概要と作成(21-4 ページ)
- ポリシー内の SSL ルールの管理(21-14 ページ)

サポートする検査情報の設定

ライセンス:任意(Any)

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。

詳細については、次の各項を参照してください。

- 内部証明書オブジェクトの使用（3-57 ページ）
- 内部認証局オブジェクトの使用（3-49 ページ）

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。

詳細については、次の各項を参照してください。

- 暗号スイート リストの操作（3-45 ページ）
- 信頼できる認証局オブジェクトの使用（3-54 ページ）
- 外部証明書オブジェクトの使用（3-56 ページ）
- 識別名オブジェクトの操作（3-46 ページ）

SSL ルールの概要と作成

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

SSL ポリシー内で、SSL ルールによって複数の管理対象デバイスにわたるネットワーク トラフィックを処理するためのきめ細かなメソッドが提供されます。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。条件には、単純なものと複雑なものがあり、ターゲット デバイスのライセンスによって用途が異なります。

アクション（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。一致したトラフィックに対して行うことができ処理は、モニタ、信頼、ブロック、または復号です。復号したトラフィックには、さらにインスペクションが適用されます。システムは、ブロックされた暗号化トラフィックと信頼された暗号化トラフィックに対して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、あるいはインスペクション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、Defense Center 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て順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。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。詳細については、SSL ルールのトラブルシューティング（21-18 ページ）を参照してください。

SSL ルールを作成または変更する手順:

アクセス: Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [SSL] を選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

手順 2　ルールを追加する SSL ポリシーの横にある編集アイコン（ ）をクリックします。

SSL ポリシー エディタが表示され、[ルール（Rules）] タブにフォーカスが移動します。

手順 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、そのルールの横にある編集アイコン（）をクリックします。

SSL ルール エディタが表示されます。

手順 4　ルールの**名前**を入力します。

各ルールには固有の名前が必要です。30 文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン(:)は使用できません。

手順 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 ルールの評価順序の指定(21-6 ページ)を参照してください。
- ルールの [アクション(Action)] を選択します。ルール アクションを使用した暗号化トラフィックの処理と検査の決定(21-9 ページ)を参照してください。
- ルールの条件を設定します。条件を使用した、ルールによる暗号化トラフィックの処理の指定(21-7 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(38-15 ページ)を参照してください。

手順 6　[保存(Save)] をクリックしてルールを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります(アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください)。

SSL ルールの評価順序の指定

ライセンス: 任意(Any)

サポートされるデバイス: シリーズ 3

SSL 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、システムが、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。詳細については、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避(21-21 ページ)を参照してください。

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。既存のルールの位置またはカテゴリの変更の詳細については、SSL ルールの位置またはカテゴリの変更(21-16 ページ)を参照してください。

ルールの編集または作成時にルールをカテゴリに追加するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 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。

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。

ルールの編集または作成時にルールを番号別に配置するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 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、適切なルール番号を入力します。

ルールを保存すると、指定した場所に配置されます。

条件を使用した、ルールによる暗号化トラフィックの処理の指定

ライセンス：機能に応じて異なる

サポートされるデバイス：シリーズ 3

SSL 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。

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。SSL ルールに追加できる条件を次の表に示します。

表 21-1　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。ゾーン条件を作成するには、ネットワーク ゾーンによる暗号化トラフィックの制御（22-2 ページ）を参照してください。
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。ネットワーク条件を作成するには、ネットワークまたは地理的位置による暗号化トラフィックの制御（22-4 ページ）を参照してください。

表 21-1　SSL ルールの条件タイプ(続き)

条件	一致する暗号化トラフィック	詳細(Details)
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。VLAN 条件の作成については、暗号化された VLAN トラフィックの制御(22-6 ページ)を参照してください。
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。ポート条件を作成するには、ポートによる暗号化トラフィックの制御(22-7 ページ) を参照してください。
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。ユーザ条件を作成するには、ユーザ ベースの暗号化トラフィックの制御(22-9 ページ)を参照してください。
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。アプリケーション条件の作成については、アプリケーション ベースの暗号化トラフィックの制御(22-11 ページ)を参照してください。
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。URL 条件の作成については、URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御(22-17 ページ)を参照してください。 ⚠ **注意**　SSL ルールの URL カテゴリとレピュテーション基準を追加または削除すると、アクセス コントロール ポリシーの適用時に Snort プロセスが再開され、一時的にトラフィック インスペクション(検査)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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響(1-9 ページ)を参照してください。
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。識別名条件の作成については、証明書の識別名による暗号化トラフィックの制御(22-22 ページ)を参照してください。
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。証明書条件の作成については、証明書ステータスによる暗号化トラフィックの制御(22-26 ページ)を参照してください。

表 21-1　SSL ルールの条件タイプ(続き)

条件	一致する暗号化トラフィック	詳細(Details)
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。証明書ステータス条件の作成については、証明書ステータスによる暗号化トラフィックの制御(22-26 ページ)を参照してください。
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。暗号スイート条件の作成については、暗号スイートによる暗号化トラフィックの制御(22-30 ページ)を参照してください。
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。バージョン条件の作成については、暗号化プロトコルのバージョンによるトラフィックの制御(22-32 ページ)を参照してください。

シリーズ 3デバイスでの暗号化トラフィックの制御と検査は可能ですが、トラフィックの制御に、検出されたアプリケーション、URL カテゴリ、またはユーザを使用するには追加ライセンスが必要です。また過度に複雑なルールは、多くのリソースを消費し、状況によってはポリシーを適用できなくなる場合があります。詳細については、SSL ルールのトラブルシューティング(21-18 ページ)を参照してください。

ルール アクションを使用した暗号化トラフィックの処理と検査の決定

ライセンス:任意(Any)

サポートされるデバイス:シリーズ 3

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:まず第一に、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。「復号できないトラフィックのデフォルト処理の設定(20-5 ページ)」を参照してください。
- 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。暗号化トラフィックに対するデフォルトの処理とインスペクションの設定(20-4 ページ)を参照してください。

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。

ルール アクションの詳細および、ルール アクションが処理とログに与える影響の詳細については、次のセクションを参照してください。

- [モニタ（Monitor）] アクション：アクションの遅延とログの確保（21-10 ページ）
- [復号しない（Do Not Decrypt）] アクション：暗号化トラフィックを検査なしで転送（21-11 ページ）
- [ブロック（Block）] アクション：検査なしで暗号化トラフィックをブロック（21-11 ページ）
- [復号（Decrypt）] アクション：さらに検査するためにトラフィックを復号（21-11 ページ）
- ポリシー内の SSL ルールの管理（21-14 ページ）

[モニタ（Monitor）] アクション：アクションの遅延とログの確保

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

[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 ルールの主な目的はネットワーク トラフィックのトラッキングなので、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ログに記録します。つまり、ルールのロギング設定または後で接続を処理するデフォルト アクションとは無関係に、システムは Defense Center データベース接続の終了時に常にログに記録します。言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールに一致すれば必ず接続がログに記録されます。

[復号しない(Do Not Decrypt)] アクション:暗号化トラフィックを検査なしで転送

ライセンス:任意(Any)

サポートされるデバイス:シリーズ 3

[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。侵入やファイル インスペクションなど、暗号化トラフィックのディープ インスペクションは実行できません。

[ブロック(Block)] アクション:検査なしで暗号化トラフィックをブロック

ライセンス:任意(Any)

サポートされるデバイス:シリーズ 3

[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。詳細については、ブロックされた URL のカスタム Web ページの表示(16-21 ページ)を参照してください。

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。

[復号(Decrypt)] アクション:さらに検査するためにトラフィックを復号

ライセンス:任意(Any)

サポートされるデバイス:シリーズ 3

[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 コントロール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。ここではデータの検査に加えて、侵入、禁止ファイル、マルウェアの検出とブロックができます。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。

[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、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間をつなぐ、2 つの SSL セッションが作成されます。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。

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。
- 匿名の暗号スイートで暗号化されたトラフィックは復号化できません。匿名の暗号スイートを **Cipher Suite** 条件に追加した場合、SSL ルールに [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。
- 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。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の設定（20-5 ページ）を参照してください。
- [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。詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（21-9 ページ）を参照してください。
- 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。詳細については、新しい署名付き証明書の取得およびアップロード（3-52 ページ）を参照してください。
- [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。詳細については、証明書による暗号化トラフィックの制御（22-24 ページ）および暗号スイートによる暗号化トラフィックの制御（22-30 ページ）を参照してください。
- [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションのアクセス コントロール ルールと復号トラフィックが一致する場合、システムは一致する接続をインタラクションなしでブロックし、応答ページを表示**しません**。

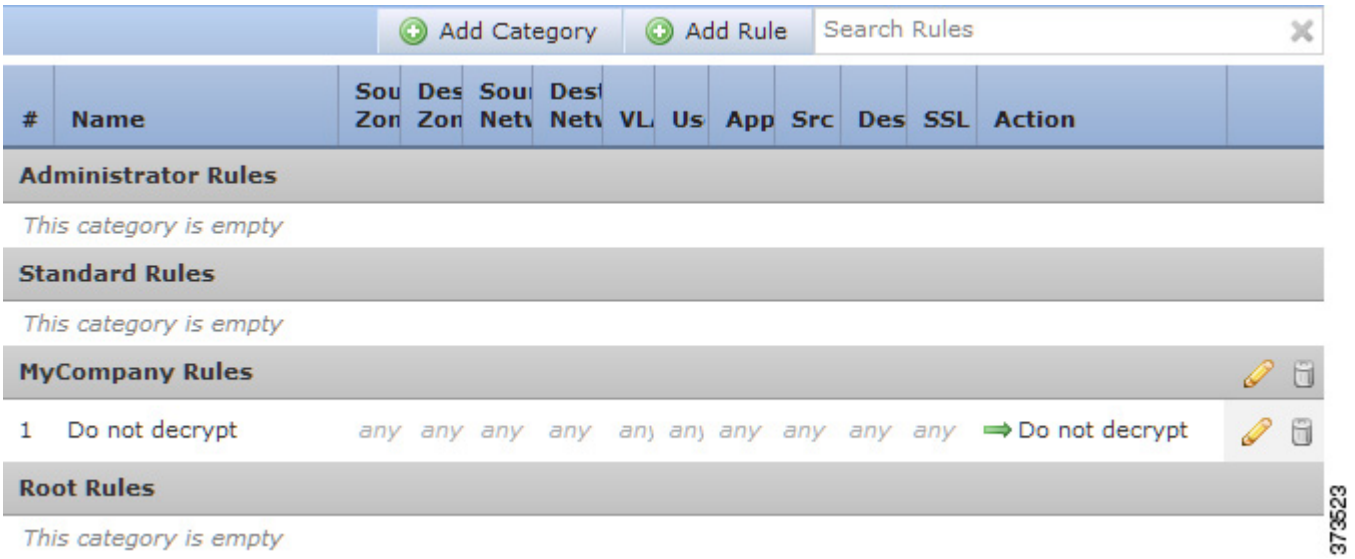
- インライン正規化プリプロセッサで [余剰ペイロードの正規化（Normalize Excess Payload）] オプションを有効にすると、プリプロセッサによる復号トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これにより SSL セッションは終了しません。トラフィックが許可された場合、トリミングされたパケットは SSL セッションの一部として暗号化されます。このオプションの詳細については、インライン トラフィックの正規化（29-7 ページ）を参照してください。
- ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サ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。

ポリシー内の SSL ルールの管理

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

SSL ポリシー エディタの [ルール（Rules）] タブでは、以下の図に示すように、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、その他の管理が行えます。



各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。警告、エラー、その他の重要な情報がアイコンで示されます。無効なルールはグレーで表示され、ルール名の下に [無効（disabled）] というマークが付きます。アイコンの詳細については、SSL ルールのトラブルシューティング（21-18 ページ）を参照してください。

SSL ルールの管理の詳細については、次を参照してください。

- SSL ルールの検索（21-15 ページ）
- SSL ルールの有効化と無効化（21-16 ページ）
- SSL ルールの位置またはカテゴリの変更（21-16 ページ）

SSL ルールの検索

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

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。

ルールを検索するには、次の手順を実行します。

アクセス: Admin/Access Admin/Network Admin

手順 1　検索するポリシーの 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 を押します。検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。

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。

手順 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

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

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 ルールを有効化または無効化できることに注意してください。SSL ルールの概要と作成（21-4 ページ）を参照してください。

SSL ルールの状態を変更するには、次の手順に従います。

アクセス：Admin/Access Admin/Network Admin

手順 1　有効または無効にするルールを含むポリシーの SSL ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

- 非アクティブなルールを有効にするには、[状態（State）] > [有効化（Enable）] を選択します。
- アクティブなルールを無効にするには、[状態（State）] > [無効（Disable）] を選択します。

手順 2　[保存（Save）] をクリックして、ポリシーを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

SSL ルールの位置またはカテゴリの変更

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

SSL ルールを編成しやすいように、SSL ポリシーには、Administrator Rules（管理者ルール）、Standard Rules（標準ルール）、Root Rules（ルート ルール）という、システムが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリは移動、削除、名前変更することはできませんが、カスタム カテゴリを作成することができます。

デフォルトでは、SSL ポリシーの変更を許可する定義済みユーザ ロールはすべて、ルール カテゴリ内およびカテゴリ間での SSL ルールの移動および変更も行えます。しかし、ユーザがルールを移動および変更することを制限するには、カスタム ロールを作成できます。

詳細については、以下を参照してください。

- SSL ルールの移動（21-17 ページ）
- 新しい SSL ルール カテゴリの追加（21-17 ページ）

SSL ルールの移動

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

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。デフォルトでは、SSL ポリシーの変更を許可する定義済みユーザ ロールはすべて、ルール カテゴリ内およびカテゴリ間での SSL ルールの移動も行えます。しかし、ユーザがシステムによって提供されるカテゴリ内のルールを移動することを制限するには、カスタム ロールを作成できます。

次の手順は、SSL ポリシー エディタを使用して 1 つまたは複数のルールを同時に移動する方法を説明しています。またはルール エディタを使用して個々の SSL ルールを移動することもできます。SSL ルールの概要と作成（21-4 ページ）を参照してください。

ルールを移動するには、次の手順を実行します。

アクセス: Admin/Access Admin/Network Admin

手順 1　移動するルールを含むポリシーの SSL ポリシー エディタで、ルールごとに空白部分をクリックして、ルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。

選択したルールが強調表示されます。

手順 2　ルールを移動します。カット アンド ペーストやドラッグ アンド ドロップを使用することもできます。

新しい場所にルールをカット アンド ペーストするには、選択したルールを右クリックし、[カット（Cut）] を選択します。次に、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。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 ペーストはできないことに注意してください。

手順 3　[保存（Save）] をクリックして、ポリシーを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください）。

新しい SSL ルール カテゴリの追加

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

SSL ルールを編成しやすいように、SSL ポリシーには、Administrator Rules（管理者ルール）、Standard Rules（標準ルール）、Root Rules（ルート ルール）という、システムが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリは移動、削除、名前変更することはできませんが、標準ルールとルート ルール間でカスタム カテゴリを作成することができます。

カスタム カテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。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。

ロールに追加したユーザ権限に基づいて、システム提供のカテゴリにあるルールのユーザによる移動および変更を制限するカスタム ロールの作成も可能です。詳細については、ユーザ アカウント特権について（61-61 ページ）を参照してください。

新しいカテゴリを追加するには、次の手順を実行します。

アクセス: Admin/Access Admin/Network Admin

手順 1　ルール カテゴリを追加するポリシーの 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。

[カテゴリの追加（Add Category）] ポップアップ ウィンドウが表示されます。

手順 2　[名前（Name）] に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

手順 3　次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、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。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウン リストから [ルールの下（below rule）] を選択した後、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。
- 既存のルールの上にルールを配置する場合は、ドロップダウン リストから [ルールの上（above rule）] を選択した後、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。

手順 4　[OK] をクリックします。

カテゴリが追加されます。カテゴリ名を編集するには、カスタム カテゴリの横にある編集アイコン（ ）をクリックします。カテゴリを削除するには、削除アイコン（ ）をクリックします。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。

手順 5　[保存（Save）] をクリックして、ポリシーを保存します。

SSL ルールのトラブルシューティング

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

SSL ルールを適切に作成して順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。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。

各ルールについては、次の表に示すように、ポリシー エディタのアイコンによる警告とエラーの表示がされます。アイコンにポインタを合わせると、警告、エラー、情報の内容を示すテキストを確認できます。

表 21-2　SSL のエラー アイコン

アイコン	説明	詳細（Details）
	警告	問題によっては、ルールやその他の警告を示している SSL ポリシーに適用できる場合があります。この場合、間違いのある設定には効果がありません。たとえば、プリエンプションされたルールはトラフィックを評価しません。ただし、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題が解消されるまでそのポリシーは適用できません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。
	error	ルールまたはその他の SSL ポリシー設定にエラーがある場合、問題が解消されるまでそのポリシーは適用できません。
	情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題は重大ではなく、ポリシーの適用を妨げません。

SSL ルールを適切に設定することは、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。複雑なルールを作成したり、ルールの順番が不適切であったりすると、パフォーマンスに影響する可能性があります。

詳細については、以下を参照してください。

- SSL ルールの警告とエラーの概要（21-19 ページ）
- ルールのプリエンプションと無効な設定の警告について（21-20 ページ）
- SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避（21-21 ページ）

SSL ルールの警告とエラーの概要

ライセンス：機能に応じて異なる

サポートされるデバイス：シリーズ 3

SSL ルールは任意のライセンスを使って作成できますが、ルール条件とインスペクション オプションによっては、ターゲット デバイスで特定のライセンス機能を有効化する必要があります。ライセンスが必要な機能を使用するポリシーを、ライセンス供与されていないデバイスに適用することはできません。ライセンス供与されていない機能については、これを示す警告アイコンおよび確認ダイアログが表示されます。警告アイコンの上にポインタを置くと詳細が表示されます。

次の表に、SSL ルールの使用に必要となるライセンスを示します。

表 21-3　SSL ルールのライセンス要件

ルールの用途	ライセンス	サポートされるDefense Center	サポートされるデバイス
ゾーン、ネットワーク、VLAN、ポート、証明書、DN、証明書ステータス、暗号スイート、またはバージョンの条件	Any	Any	シリーズ 3
位置情報データを使用するネットワーク条件	FireSIGHT	任意（DC500 を除く）	シリーズ 3
アプリケーション条件またはユーザ条件	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーション データを使用するカテゴリ条件	URL Filtering	DC500 を除くいずれか	シリーズ 3

ルールのプリエンプションと無効な設定の警告について

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

SSL ルールを適切に設定して順序付けることは、効果的な展開を構築する上で不可欠な要素です。SSL ポリシーの内部では、SSL ルールで他のルールのプリエンプションが発生したり、無効な設定が含まれたりする場合があります。これらの問題については、警告およびエラーのアイコンが表示されます。

ルールのプリエンプションの警告について

SSL ルールの条件が後続のルールよりも優先して適用され、後続のルールによるトラフィックの照合が回避される場合があります。次に例を示します。

```
Rule 1: do not decrypt Administrators
Rule 2: block Administrators
```

上記の最初のルールによってトラフィックは事前に許可されているため、2 番目のルールによってトラフィックがブロックされることはありません。

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初のルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールよりも優先して適用されることになります。

```
Rule 1: do not decrypt VLAN 22-33
Rule 2: block VLAN 27
```

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 がルール 2 をプリエンプション処理し、ルール 2 での VLAN 2 の照合は行われません。

```
Rule 1: do not decrypt Source Network 10.4.0.2/16
Rule 2: do not decrypt Source Network 10.4.0.2/16, VLAN 2
```

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。次に例を示します。

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 1 URL www.example.com
```

条件が 1 つでも異なる場合は、後続のルールが回避されることはありません。次に例を示します。

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 2 URL www.example.com
```

無効な設定の警告について

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 Filtering 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適用できなくなります。適用可能にするには、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）] ルールを作成した後からパッシブ インターフェイスでセキュリティ ゾーンをゾーン条件に追加した場合、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。
- ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセス コントロールの対象ユーザではなくなるため、そのルールは効果がなくなります。

SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

SSL 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。

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。

重要性が最も高いルールから最も低いルールへの順序付け

最初に、組織のニーズに適するルールを順序付けする必要があります。すべてのトラフィックに適用する必要がある優先順位ルールをポリシーの先頭部分付近に配置します。たとえば、ある一人のユーザからの発信トラフィックは詳細な解析用に復号するが（[復号 - 再署名（Decrypt-Resign）] ルールを使用）、その部門の他のすべてのユーザからのトラフィックは復号しない場合は（[復号しない（Do not decrypt）] ルールを使用）、この順序で 2 つの SSL ルールを配置します。

特定のルールから一般的なルールへの順序付け

特定のルール、つまり処理するトラフィックの定義を絞り込むルールを先に設定することで、パフォーマンスを向上させることができます。これは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理できるという理由からも重要です。

ここで 1 つのシナリオとして、信頼できる CA（Good CA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックはブロックしたいが、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。ここで必要となるのは、CA 証明書およびすべての中間 CA 証明書をアップロードし、その後に次のようにルールを順序付けることです。

```
Rule 1: Block issuer CN=www.badca.com
Rule 2: Do not decrypt issuer CN=www.goodca.com
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Do not decrypt issuer CN=www.goodca.com
Rule 2: Block issuer CN=www.badca.com
```

最初のルールは Good CA によって信頼されたすべてのトラフィックに一致し、その中には Bad CA によって信頼されたトラフィックも含まれます。どのトラフィックも 2 番目のルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

証明書でピニングしたサイトからのトラフィックを許可するルールの配置

証明書のピニングを行うと、SSL セッションが確立される前に、サーバの公開キー証明書が、サーバにすでに関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。[復号 - 再署名（Decrypt - Resign）] アクションにはサーバ証明書を変更してからクライアントに渡すという動作が含まれているため、ブラウザがすでにその証明書をピニングしている場合は、変更された証明書が拒否されます。

たとえば、クライアント ブラウザが、証明書ピニングを使用するサイト `windowsupdate.microsoft.com` に接続されており、そのトラフィックと一致する SSL ルールを [復号 - 再署名（Decrypt - Resign）] アクションを使用して設定すると、システムはサーバ証明書に再署名してから、クライアント ブラウザに渡します。この変更されたサーバ証明書は、ブラウザでピニングした `windowsupdate.microsoft.com` の証明書と一致しないため、クライアント ブラウザは接続を拒否します。

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。SSL ポリシーでは、このルールを、トラフィックと一致するすべての [復号 - 再署名（Decrypt - Resign）] ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。また、接続が成功した場合も、失敗した場合も、ログに記録された接続イベントから証明書を表示できます。

トラフィックを復号するルールは後方に配置する

トラフィックの復号はリソースを必要とする処理なので、トラフィックの復号を実行しないルール（[復号しない（Do not decrypt）]、[ブロック（Block）]）を、実行するルール（[復号 - 既知のキー（Decrypt-Known Key）]、[復号 - 再署名（Decrypt-Resign）]）より前に配置することで、パフォーマンスが向上する可能性があります。この理由は、トラフィックの復号には多量のリソースを消費するものがあるからです。また Block ルールは、復号やインスペクションの対象となるはずのトラフィックをそらす可能性があります。他の要素がすべて同等である、つまりルールのセットで、より重要というルールがなく、プリエンプションが問題ではない場合には、次の順序でルールを配置することを考慮してください。

- 一致する接続はロギングするが、トラフィックで他のアクションは実行しないモニタ ルール
- 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 [ブロック（Block）] ルール
- 暗号化トラフィックを復号しない [復号しない（Do not decrypt）] ルール
- 既知の秘密キーを使用して着信トラフィックを復号する [復号 - 既知のキー（Decrypt-Known Key）] ルール
- サーバ証明書に再署名することによって発信トラフィックを復号する [復号 - 再署名（Decrypt-Resign）] ルール

パフォーマンスを改善する SSL インスペクション設定

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

複雑な SSL ポリシーおよびルールは、多量のリソースを消費する可能性があります。SSL ポリシーが適用されると、システムはすべてのルールをまとめて評価し、ネットワーク トラフィックの評価にターゲット デバイスが使用する 1 つの拡張セットとして一連の条件を統合します。ターゲット デバイスでサポートされる SSL ルールの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。

ルールの単純化

次のガイドラインは、SSL ルールの単純化とパフォーマンスの向上に役立ちます。

- ルールの作成時には、条件を構成する要素は可能な限り少なくします。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御および URL フィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAP ユーザ グループを使用します。

  SSL ルール条件で使用するオブジェクトに要素を結合しても、パフォーマンスは向上しないことに注意してください。たとえば、50 個の IP アドレスを 1 つのネットワーク オブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。
- できる限り、セキュリティ ゾーンごとにルールを制限します。デバイスのインターフェイスがゾーン制限されたルールのゾーンの 1 つにない場合、ルールはそのデバイスのパフォーマンスに影響を与えません。
- ルールを過度に設定しないでください。処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を使用しないでください。

トラフィック復号の設定

トラフィック復号を設定する際は、次の注意事項に従ってください。

- トラフィックの復号では、トラフィックを復号し、アクセス コントロールを使用して検査する処理のリソースを必要とします。処理対象を絞り込んだ復号ルールを作成することは、処理対象が広範な復号ルールよりも復号するトラフィック量が減るので、その結果として、トラフィック復号に必要な処理のリソースも削減されます。暗号化トラフィックは、いったん復号した後にアクセス コントロール ルールを使用して許可またはブロックするのではなく、できるだけブロックするかまたは復号しないことを選択します。
- ルート発行元 CA に基づいてトラフィックを信頼するように証明書ステータスの条件を設定する場合は、ルート CA 証明書およびルート CA 信頼チェーン内のすべての中間 CA 証明書を SSL ポリシーにアップロードするようにします。信頼できる CA の信頼チェーン内のすべてのトラフィックは復号なしで許可されるようになり、不要な復号は実施されません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。