TLS/SSL ルールの使用を開始するには

ここでは、TLS/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。

（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。

TLS/SSL規則の概要

TLS/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。

TLS/SSL ルールのガイドラインと制限事項

TLS/SSL ルールを設定するときは、次の点に注意してください。TLS/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。ルールをどのように設定するかには、制御できない特定のアプリケーションの動作を含む、多くの要素が影響します。

さらに、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。

TLS/SSL ハードウェア アクセラレーションに特に関連するガイドラインについては、TLS/SSL ハードウェアの加速を参照してください。

関連トピック

TLS/SSL 復号の使用上のガイドライン

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

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使用するデバイスでトラフィックを復号化することはできません。

TLS/SSL ルールのサポートされない機能

パッシブおよびインライン タップ モードのインターフェイスはサポートされていません。

TLS/SSL トラフィックはパッシブまたはインライン タップ モードのインターフェイスでは復号できません。

TLS 1.3 はサポートされません

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

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

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

TLS/SSL 復号化禁止のガイドライン

次によって禁止されている場合は、トラフィックを復号してはいけません。

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

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

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

TLS/SSL 復号化：再署名のガイドライン

[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 TLS/SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。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、TLS/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 TLS/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。

また次の点に注意してください。

匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 のセクション A.5 を参照してください。

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

一致しない暗号スイート

証明書と一致しない暗号スイートで TLS/SSL ルールを保存しようとすると、次のエラーが表示されます。この問題を解決するには、TLS/SSL 暗号スイートの確認 を参照してください。

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

信頼できない認証局

サーバ証明書の再署名に使用する認証局（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。

HTTP プロキシの制限

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 TLS/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。

署名済み CA のアップロード

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。

TLS/SSL 復号化：既知のキーのガイドライン

[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。

また次の点に注意してください。

匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 のセクション A.5 を参照してください。

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

識別名または証明書が一致しない

[復号 - 既知のキー（Decrypt - Known Key）] アクションを指定して TLS/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。

署名アルゴリズムの不一致

[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。

証明書のピン留め

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 TLS/SSL ルールを設定します。

TLS/SSL ブロックのガイドライン

[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。

ルールでロギングを有効にすると、（**[分析（Analysis）] > [イベント（Events）] > [接続（Connections）]**で）2 つの接続イベントが表示されます。インタラクティブ ブロックのイベントと、ユーザがサイトの継続を選択したかどうかを示す別のイベントです。

TLS/SSL 証明書のピン留めのガイドライン

一部のアプリケーションでは、アプリケーション自体に元のサーバ証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで TLS/SSL ルールを設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL のピン留めは中間者攻撃を避けるために使用されるため、防止または回避する方法はありません。次の選択肢があります。

- そのアプリケーション用に、[復号-再署名（Decrypt - Resign）] ルールよりも順序が前の、[復号しない（Do Not Decrypt）] ルールを作成します。
- Web ブラウザを使用してアプリケーションにアクセスするようユーザに指示します。

ルールの順序の詳細については、SSL ルールの順序を参照してください。

アプリケーションが TLS/SSL のピン留めを使用しているかどうかを判断するには、TLS/SSL ピニングのトラブルシューティングを参照してください。

TLS/SSL ハートビートのガイドライン

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

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

詳細については、TLS ハートビートについてを参照してください。

TLS/SSL 匿名の暗号スイートの制限事項

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 のセクション A.5 を参照してください。

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

TLS/SSL ルールの [暗号スイート（Cipher Suite）] 条件に匿名の暗号スイートを追加することはできますが、システムは、ClientHello 処理中に自動的に匿名の暗号スイートを削除します。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 TLS/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。

TLS/SSL 正規化のガイドライン

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。これで TLS/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 TLS/SSL セッションの一部として暗号化されます。

TLS/SSL のその他のルールのガイドライン

ユーザとグループ

ルールにグループまたはユーザを追加した後、そのグループまたはユーザ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。）レルムの詳細については、レルムの作成を参照してください。

TLS/SSL ルールのカテゴリ

SSL ポリシーに [復号-再署名（Decrypt - Resign）] アクションがあるにもかかわらず Web サイトが復号されない場合は、そのポリシーに関連付けられているルールの [カテゴリ（Category）] タブ ページを確認します。

場合によっては、認証などの目的で Web サイトが別のサイトにリダイレクトされ、リダイレクト先のサイトの URL カテゴリが復号を試みているサイトとは異なることがあります。たとえば、`gmail.com`（[Webベース電子メール（Web based email）] カテゴリ）は認証のために `accounts.gmail.com`（[インターネットポータル（Internet Portals）] カテゴリ）にリダイレクトされます。関連するすべてのカテゴリを必ずSSLルールに含めます。

ローカル データベースにない URL のクエリ

[復号-再署名（Decrypt - Resign）] ルールを作成し、ローカル データベースにカテゴリとレピュテーションがない Web サイトをユーザが参照すると、データが復号されないことがあります。一部の Web サイトはローカル データベースで分類されません。分類されない場合、その Web サイトのデータはデフォルトでは復号されません。

この動作は **[システム（System）] > [統合（Integration）] > の設定を使用し [Cisco CSI]、[不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URLs）]** を使用して制御できます。

このオプションの詳細については、シスコ クラウドを参照してください。

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化

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化もできます。[復号 - 再署名（Decrypt - Resign）] アクションが設定された TLS/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、TLS/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

TLS/SSL ルールの作成と変更

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（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 Firepower Management Center にログインします。

ステップ 2 **[Policies]** > **[Access Control]** > **[SSL]** をクリックします。

ステップ 3 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 4 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 5 ルールの [名前（Name）] を入力します。

ステップ 6 ルールを有効にするかどうか [Enabled] を指定します。

ステップ 7 ルールの位置を指定します。TLS/SSL ルールの順序の評価 を参照してください。

ステップ 8 ルールの [アクション（Action）] をクリックします。TLS/SSL ルール アクション設定 （20 ページ）を参照してください。

ステップ 9 ルールの条件を設定します。TLS/SSL ルールの条件タイプ （16 ページ） を参照してください。

ステップ 10 [保存（Save）] をクリックします。

次のエラーが表示されている場合は、TLS/SSL 暗号スイートの確認：**Traffic cannot match this rule; none of your selected cipher suites contain a signature algorithm that the resigning CA's signature algorithm**を参照してください。

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。

TLS/SSL ルールをルール カテゴリに追加する

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

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 TLS/SSL ルールの位置指定

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

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。

TLS/SSL ルールの検索

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、TLS/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。

TLS/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（**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 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。

TLS/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（Access）
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 TLS/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 TLS/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。

TLS/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（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 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 TLS/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 TLS/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（Access）
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 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。

TLS/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 TLS/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。

TLS/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 TLS/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。

TLS/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 : TLS/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 ゾーンとは、展開やセキュリティポリシーに従って1つまたは複数のインターフェイスを論理的にグループ化したものです。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。 （注） 、インラインまたはタップモードインターフェイスでトラフィックを復号することはできません。
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	送信元ポートまたは宛先ポート	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。

条件	一致する暗号化トラフィック	詳細（Details）
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	ブラウザでユーザが入力した URL が共通名（CN）と一致するか、または URL が証明書のサブジェクト代替名（SAN）に含まれています	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。
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

TLS/SSL のルールの条件
ユーザベースの TLS/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 TLS/SSL ルール条件
ClientHello メッセージ処理

TLS/SSL 規則アクション

ここでは、TLS/SSL ルールで利用可能なアクションについて説明します。

関連トピック

TLS/SSL ルールの復号アクション （19 ページ）
TLS/SSL ルールのブロック アクション （19 ページ）
TLS/SSL ルール：復号しないアクション （18 ページ）
TLS/SSL ルールのモニタ アクション （18 ページ）

TLS/SSL ルールのモニタ 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。

TLS/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 アクションの一般的な理由は、以下のとおりです。

- TLS/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。
- TLS/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、復号できないトラフィックのデフォルト処理オプションを参照してください。

TLS/SSL ルールのブロック アクション

Firepower システムは、システムを通過させないトラフィックに対して次の TLS/SSL ルール アクションを提供します。

- [ブロック（Block）] では、接続が終了するため、クライアント ブラウザにエラーが表示されます。

  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。

- [インタラクティブブロック（Interactive block）] では、宛先サーバへの接続が中断され、サーバへのアクセスが会社のポリシーに違反している可能性があることをユーザは確認する必要があります。

  デフォルトの確認応答ページを使用したり、カスタム ページを作成したりできます。

  接続イベントは、ユーザが宛先サーバの継続を選択したかどうかを示します。

- [リセットしてブロック（Block with reset）] では、接続がリセットされるため、クライアント ブラウザにエラーが表示されます。

  このエラーでは、接続がリセットされたことはわかりますが、その理由はわかりません。

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ため、[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

TLS/SSL ルールの復号アクション

[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）からの証明書を使用してトラフィックを復号することをお勧めします。これにより、**Invalid Issuer** が接続イベント内の SSL 証明書ステータス列に表示されないようにします。

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。

TLS/SSL ルール アクション設定

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

参照先：

- TLS/SSL ルールのブロック アクション （19 ページ）
- TLS/SSL ルール：復号しないアクション （18 ページ）
- TLS/SSL ルールのモニタ アクション （18 ページ）

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 （22 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 （21 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

- TLS/SSL のルールの条件、ユーザベースの TLS/SSL ルールの条件、レピュテーション ベースの TLS/SSL ルール条件、およびサーバ証明書ベースの TLS/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（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

TLS/SSL 復号化：再署名のガイドライン （4 ページ）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）] 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。

ステップ 5 オプション信頼できる CA 署名書を SSL に使用して、接続イベントの SSL 証明書ステータス列に **Invalid Issuer** が表示されるのを回避するには、証明書をポリシーに追加します。

a) SSL ポリシー エディタ ページで、[信頼できる CA 証明書（Trusted CA Certificates）] タブをクリックします。

b) 既知のキーに対応する CA 証明書を SSL ポリシーに追加します。

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

TLS/SSL 復号化：既知のキーのガイドライン （5 ページ）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。

ステップ 6 オプション信頼できる CA 署名書を SSL に使用して、接続イベントの SSL 証明書ステータス列に **Invalid Issuer** が表示されるのを回避するには、証明書をポリシーに追加します。

a) SSL ポリシー エディタ ページで、[信頼できる CA 証明書（Trusted CA Certificates）] タブをクリックします。

b) 既知のキーに対応する CA 証明書を SSL ポリシーに追加します。

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。

TLS/SSL Rules Management

SSL ポリシー エディタの [ルール（Rules）] タブ ページでは、ポリシー内の TLS/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。