TLS/SSL ルールのトラブルシューティング

接続イベントを使用して、さまざまなエラー状態を診断できます。たとえば、TLS/SSL トラフィックにより管理対象デバイスが過負荷状態になっていることや、アプリケーションが TLS/SSL ピニングまたは TLS ハートビートを使用していることがあります。このような場合は、SSL ルールの調整や、ネットワークの通常の動作を復元するためのその他のアクションが必要になることがあります。

TLS/SSL オーバーサブスクリプションについて

TLS/SSL オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS/SSL ハードウェア アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS/SSL ハードウェア アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、SSL ポリシーの [復号化不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定に従います。

- 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）

SSL ポリシーの [復号化不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定が [復号しない（Do Not decrypt）] で、関連付けられたアクセス コントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

TLS/SSL オーバーサブスクリプションのトラブルシューティング

管理対象デバイスで TLS/SSL ハードウェア アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスに SSL オーバーサブスクリプションが発生しているかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] イベントを追加する必要があります。

始める前に

- 管理対象デバイスで SSL ハードウェア アクセラレーションを有効にします。
- [復号できないアクション（Undecryptable Actions）] タブ ページの [ハンドシェイクエラー（Handshake Error）] の設定で、SSL ポリシーを設定します。

  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を設定するを参照してください。
- SSL ルールによる復号可能接続のロギングの説明に従って、SSL ルールのログを有効にします。

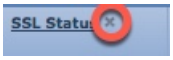
手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

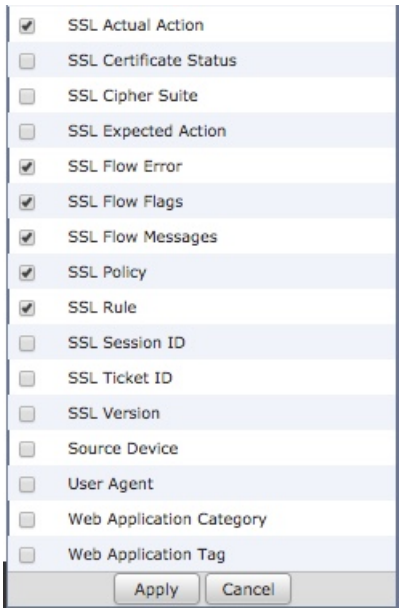
ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントのテーブル ビューで、任意の列の [x] をクリックして、少なくとも [SSLフローフラグ（SSL Flow Flags）] 列をテーブルに追加します。



次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。



接続イベントとセキュリティ インテリジェンス イベントのフィールドで説明した順序で列が追加されます。

ステップ 5 [適用（Apply）] をクリックします。
TLS/SSL オーバーサブスクライブは、[SSL Flow Flags] 列の `ERROR_EVENT_TRIGGERED` および `OVER_SUBSCRIBED` の値で示されます。

次の図は例を示しています。

SSL Flow Error	SSL Actual Action	SSL Flow Flags
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED

ステップ 6 TLS/SSL オーバーサブスクライブが発生している場合は、管理対象デバイスにログインして、次のコマンドのいずれかを入力します。

コマンド（Command）	結果
show counters	**TCP_PRX BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。
show snort tls-offload	**BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。

関連トピック

接続およびセキュリティ インテリジェンス イベント テーブルの使用
接続イベントとセキュリティ インテリジェンス イベントのフィールド
接続イベント フィールドで利用可能な情報
イベントの検索

TLS ハートビートについて

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。

TLS/SSL ハードウェア アクセラレーションが有効になっている管理対象デバイスが TLS ハートビート エクステンションを使用するパケットを扱うときは、管理対象デバイスは SSL ポリシーの [復号化不可のアクション（Undecryptable Actions）] の [復号化エラー（Decryption Errors）] の設定で指定されたアクションを行います。

- ブロック（Block）
- リセットしてブロック（Block with reset）

関連トピック

TLS ハートビートのトラブルシューティング （5 ページ）

TLS ハートビートのトラブルシューティング

管理対象デバイスで TLS/SSL ハードウェア アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスが TLS ハートビート エクステンションを使用してトラフィックを監視しているかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローメッセージ（SSL Flow Messages）] イベントを追加する必要があります。

始める前に

SSL ハートビートは、接続イベント テーブル ビューの [SSLフローメッセージ（SSL Flow Messages）] 列の `HEARTBEAT` の値で示されます。ネットワーク内のアプリケーションが SSL ハートビートを使用しているかどうかを確認するには、最初に次のタスクを実行します。

- 管理対象デバイスで SSL ハードウェア アクセラレーションを有効にします。
- [復号できないアクション（Undecryptable Actions）] タブ ページの [復号化エラー（Decryption Error）] の設定で、SSL ポリシーを設定します。

  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を設定するを参照してください。
- SSL ルールによる復号可能接続のロギングの説明に従って、SSL ルールのログを有効にします。

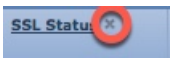
手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

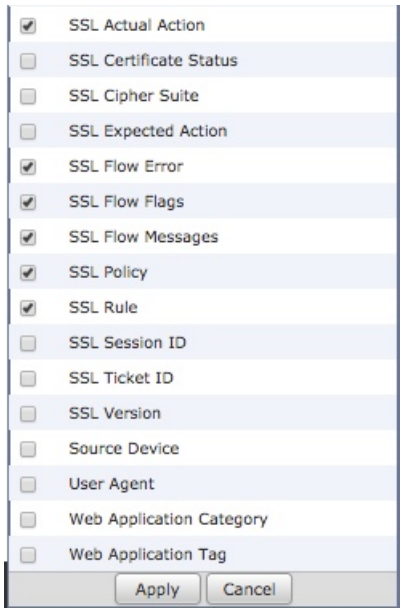
ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントのテーブル ビューで、任意の列の [x] をクリックして、少なくとも [SSLフローメッセージ（SSL Flow Messages）] 列をテーブルに追加します。



次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。



接続イベントとセキュリティ インテリジェンス イベントのフィールドで説明した順序で列が追加されます。

ステップ 5 [適用（Apply）] をクリックします。
TLS ハートビートは、[SSLフローメッセージ（SSL Flow Messages）] 列の `HEARTBEAT` の値で示されます。

ステップ 6 ネットワーク上のアプリケーションでSSLハートビートを使用する場合は、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

- TLS ハートビートのトラブルシューティング （5 ページ）
- TLS ハートビートについて （4 ページ）
- 接続およびセキュリティ インテリジェンス イベント テーブルの使用
- 接続イベントとセキュリティ インテリジェンス イベントのフィールド
- 接続イベント フィールドで利用可能な情報
- イベントの検索

TLS/SSL のピニングについて

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 ピニングが行われていることを確認するには、Facebook などのモバイル アプリケーションへのログインを試みます。ネットワーク接続エラーが表示された場合は、Web ブラウザを使用してログインします。（たとえば、Facebook のモバイル アプリケーションにログインすることはできませんが、Safari または Chrome を使用して Facebook にログインすることはできます）。Firepower Management Center の接続イベントは、TLS/SSL ピニングのさらなる証明として使用できます

（注） TLS/SSL ピニングはモバイル アプリケーションに限定されません。

ネットワーク上のアプリケーションで SSL ピニングを使用する場合は、次を参照してください。 TLS/SSL ルールのガイドラインと制限事項

関連トピック

TLS/SSL ピニングのトラブルシューティング （7 ページ）

TLS/SSL ピニングのトラブルシューティング

デバイスで SSL ピニングが発生しているかどうかを確認するには、接続イベントを表示します。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を追加する必要があります。

始める前に

- 管理対象デバイスで SSL ハードウェア アクセラレーションを有効にします。
- SSL ルールによる復号可能接続のロギングの説明に従って、TLS/SSL ルールのログを有効にします。
- Facebook のようなモバイル アプリケーションにログインします。ネットワーク接続エラーが表示されたら、Chrome または Safari を使用して Facebook にログインします。Web ブラウザを使用してログインできても、ネイティブ アプリケーションではできない場合は、SSL ピニングが発生している可能性があります。

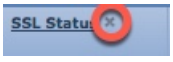
手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

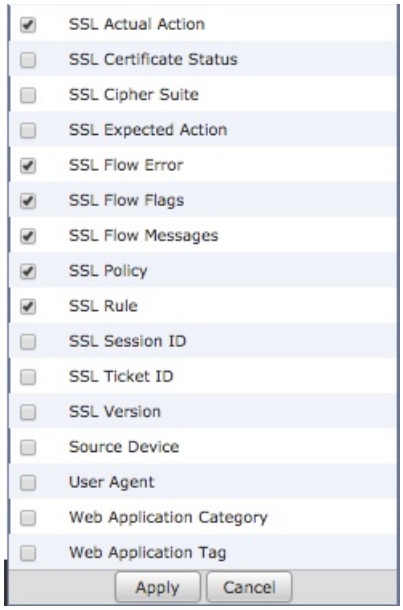
ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 任意の列の [x] をクリックして、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を接続イベント テーブルに追加します。



次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および[SSLルール（SSL Rule）]列を追加します。



接続イベントとセキュリティ インテリジェンス イベントのフィールドで説明した順序で列が追加されます。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 次に SSL ピニングの動作を特定する方法について説明します。

ステップ 7 ネットワーク内のアプリケーションでSSL ピニングが使用されていることを確認する場合は、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。

次のタスク

TLS/SSL 接続イベントを使用して、次のいずれかが表示されれば、TLS/SSL ピニングの発生を確認できます。

- クライアントがサーバから SERVER_HELLO、SERVER_CERTIFICATE、SERVER_HELLO_DONE メッセージを受信した後に TCP Reset を受信すると、SSL ALERT メッセージを送信するアプリケーションの場合、次のように表示されます。（パケット キャプチャを使用すると、アラート `Unknown CA (48)` が表示される場合があります）。
  - [SSLフローフラグ（SSL Flow Flags）] 列に `ALERT_SEEN` は表示されますが、`APP_DATA_C2S` や `APP_DATA_S2C` は表示されません。
  - 管理対象デバイスでSSL ハードウェア アクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、`CLIENT_ALERT`、

CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE が表示されます。

- 管理対象デバイスが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か、機能が無効になっている場合は、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE が表示されます。
- [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

- SSL ハンドシェイク終了後にアラートではなく TCP Reset を送信するアプリケーションの場合は、次のように表示されます。
  - [SSLフローフラグ（SSL Flow Flags）] 列に ALERT_SEEN、APP_DATA_C2S、APP_DATA_S2C は表示されません。
  - 管理対象デバイスでSSLハードウェアアクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、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 が表示されます。
  - 管理対象デバイスが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か、機能が無効になっている場合は、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、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 が表示されます。
  - [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

関連トピック

接続およびセキュリティ インテリジェンス イベント テーブルの使用
接続イベントとセキュリティ インテリジェンス イベントのフィールド
接続イベント フィールドで利用可能な情報
イベントの検索

TLS/SSL 暗号スイートの確認

始める前に

このトピックでは、暗号スイートの条件を持つ TLS/SSL ルールを保存する際に次のエラーが表示された場合に実行する必要があるアクションについて説明します。

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature

algorithm that the resigning CA's signature algorithm
```

エラーは、TLS/SSL ルールの条件として選択した 1 つ以上の暗号スイーツが TLS/SSL ルールに使用されている証明書と互換性がないことを示します。この問題を解決するには、使用している証明書へのアクセス権が必要です。

（注） このトピックでのタスクには、TLS/SSL 暗号化がどのように機能するかの知識が必要です。

手順

ステップ 1 指定した暗号スイーツで [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のいずれかを持つ SSL ルールを保存しようとしたときに次のエラーが表示されます。

例：

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

ステップ 2 トラフィックの復号に使用している証明書を見つけ、必要に応じて、openssl コマンドを実行できるシステムにその総名所をコピーします。

ステップ 3 次のコマンドを実行し、証明書で使用されている署名アルゴリズムを表示します。

openssl x509 -in *CertificateName* **-text -noout**

出力の最初に次のような数行が表示されます。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

ステップ 4 **Signature algorithm** によって次が通知されます。

- 使用されている暗号化関数（前の例では、**ECDSA** は楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）を意味します）。
- 暗号化されたメッセージのダイジェストの作成に使用されたハッシュ関数（前の例では **SHA256**）。

ステップ 5 それらの値に一致する暗号スイーツのリソース（OpenSSL at University of Utah など）を検索します。暗号スイートは RFC 形式である必要があります。
また、その他のさまざまなサイト（Mozilla wiki の Server Side TLS や RFC 5246 の Appendix C など）も検索できます。マイクロソフトのドキュメントの Cipher Suites in TLS/SSL（Schannel SSP）[英語] には、暗号スイーツの詳細な説明があります。

ステップ 6 必要に応じて、OpenSSL 名を Firepower Management システムが使用している RFC 名に変換します。
`https://testssl.sh` サイトの『RFC mapping list』を参照してください。

ステップ 7 前の例の **ecdsa-with-SHA256** では、Mozilla wiki で『Modern Compatibility List』を参照できます。

a) 名前に **ECDSA** または **SHA-256** を持つ暗号スイートのみを選択します。これらの暗号スイートは次のように動作します。

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) 対応する RFC 暗号スイートを RFC マッピング リストで検索します。これらの暗号スイートは次のように動作します。

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

ステップ 8 前述の暗号スイートを TLS/SSL ルールに追加します。