ハンドシェイク障害または証明書検証エラーによる NGFW サービス モジュール TLS の中断

内容

概要

このドキュメントでは、復号化がイネーブルにされた Cisco Next-Generation Firewall（NGFW）のサービス モジュールを使用して、HTTPS ベースの Web サイトにアクセスする場合の特定の問題のトラブルシューティングを行う方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュア ソケット レイヤ（SSL）のハンドシェイク手順
- SSL 証明書

使用するコンポーネント

このドキュメントの情報は、Cisco Prime Security Manager（PRSM）バージョン 9.2.1.2(52) の Cisco NGFW サービス モジュールに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

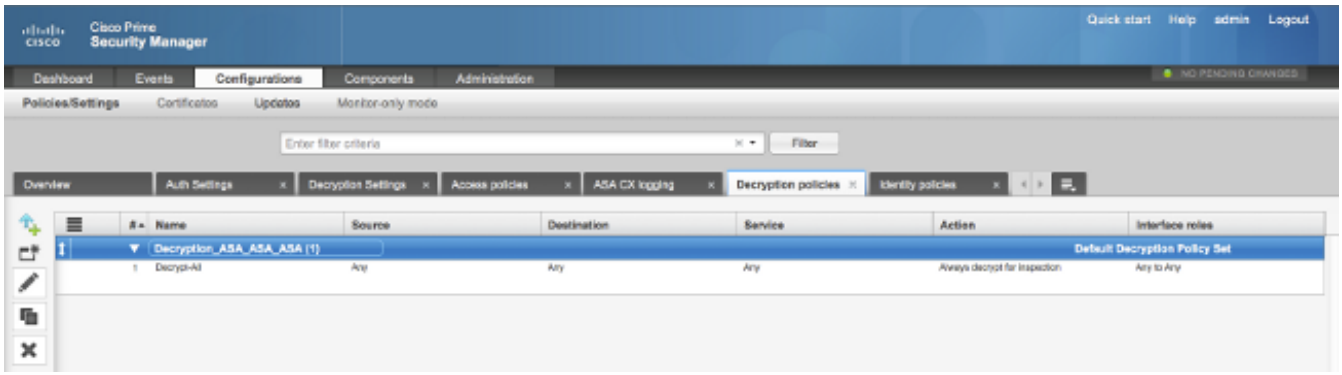
復号化は、NGFW サービス モジュールが SSL 暗号化されたフローを復号化し（他の方法で暗号

化された対話を検査して）、トラフィック上でポリシーを適用できるようにする機能です。この機能を設定するには、管理者は、元のサーバ証明書の代わりに、クライアントがアクセスする HTTPS ベースの Web サイトに提示する NGFW のモジュールの復号化証明書を設定する必要があります。

復号化が機能するには、NGFW モジュールがサーバに提示された証明書を信頼する必要があります。このドキュメントでは、NGFW サービス モジュールとサーバ間で SSL ハンドシェイクが失敗し、ユーザが特定の HTTPS ベースの Web サイトに接続しようとすると、その Web サイトが失敗するシナリオについて説明します。

このドキュメントでは、これらのポリシーは PRSM を搭載する NGFW サービス モジュールで定義されています。

- **アイデンティティ ポリシー**：定義されたアイデンティティ ポリシーはありません。
- **復号化ポリシー**この設定では、**Decrypt-All ポリシーを使用します。**

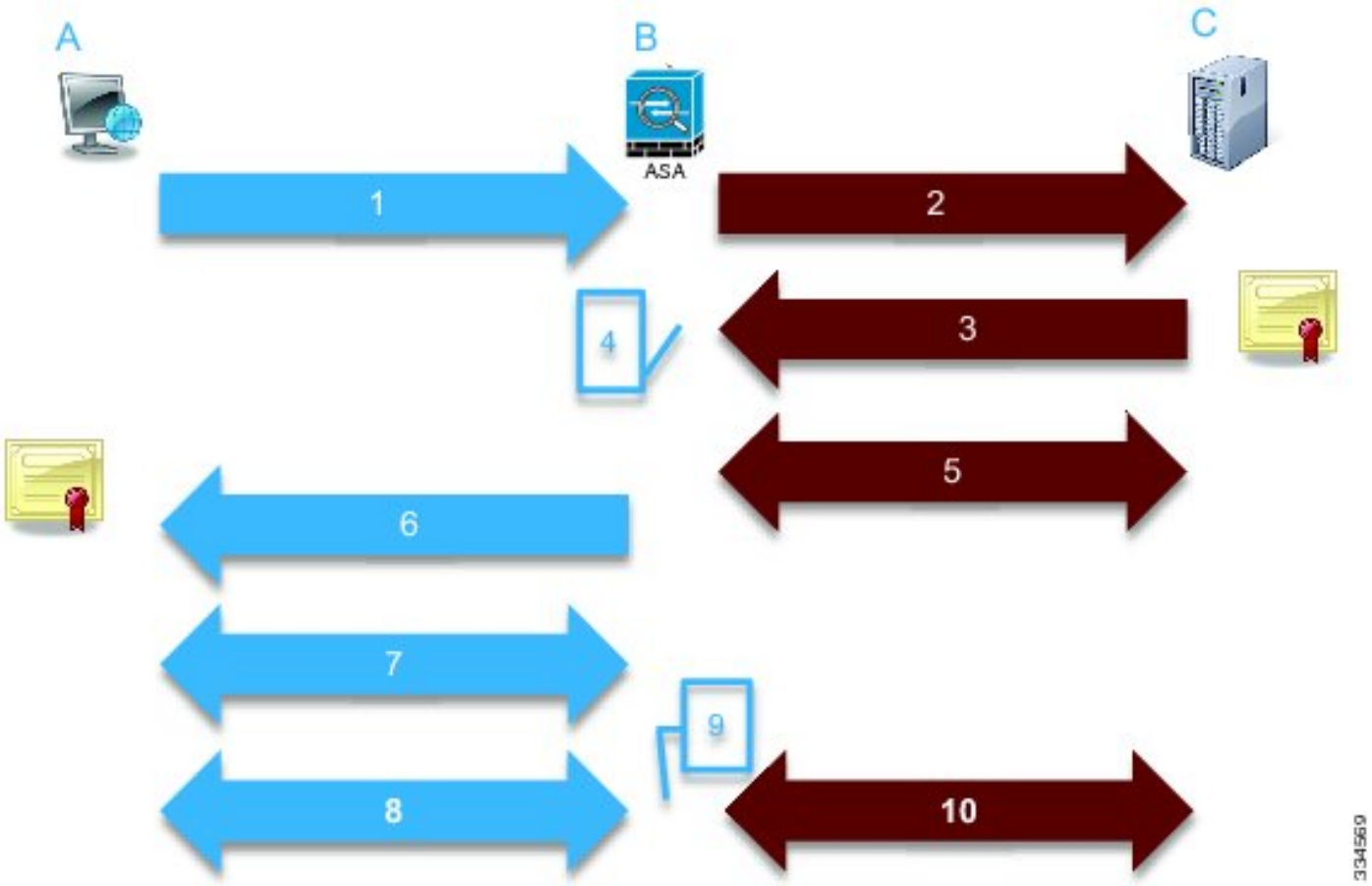


- **アクセス ポリシー**定義済みのアクセス ポリシーはありません。
- **復号化の設定**：このドキュメントでは、**復号化証明書**が NGFW サービス モジュールで設定されており、クライアントが信頼すると仮定します。

復号化ポリシーが NGFW サービス モジュールで定義され、前述のように設定されている場合、NGFW サービス モジュールは、モジュールを通じて SSL 暗号化されたトラフィックすべてを傍受して復号化しようとします。

> **注**：このプロセスの段階的な説明は、『Cisco ASA CX および Cisco Prime Security Manager ユーザ ガイド』の「復号化されたトラフィック フロー」セクションで入手できます。

次の図は、イベントのシーケンスを示しています。



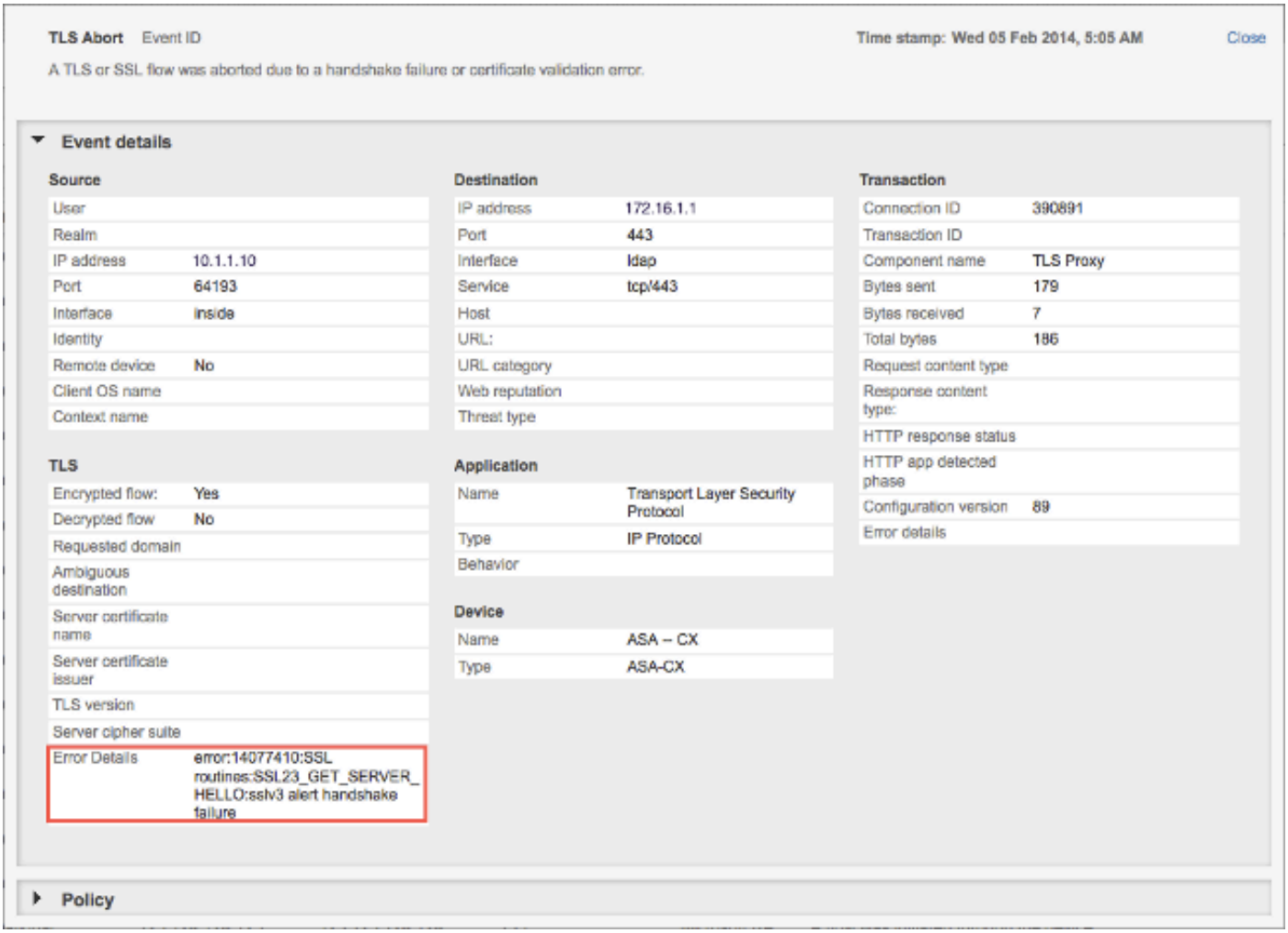
この図では、A はクライアント、**B は NGFW サービス モジュール、C は** HTTPS サーバです。このドキュメントで示されている例では、HTTPS ベースのサーバは Cisco 適応型セキュリティ アプライアンス（ASA）の Cisco Adaptive Security Device Manager（ASDM）です。

このプロセスで考慮する必要がある 2 つの重要な要素があります。

- プロセスの 2 番目の手順で、サーバは NGFW サービス モジュールによって提示される SSL 暗号化スイートの 1 つを受け入れる必要があります。
- プロセスの 4 番目の手順では、NGFW サービス モジュールはサーバに提示される証明書を信頼する必要があります。

問題

サーバが NFGW サービス モジュールによって提示されるで SSL 暗号化を受け入れることができない場合、次のような エラー メッセージが表示されます。



表示されるエラーの（ハイライトされた）詳細情報を記録することが重要です。

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

モジュール診断のアーカイブにある **/var/log/cisco/tls_proxy.log** ファイルを確認すると、次のエラー メッセージが表示されています。

```
2014-02-05 05:21:42,189 INFO  TLS_Proxy   - SSL alert message received from
 server (0x228 = "fatal : handshake failure") in Session: x2fd1f6

2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:
 SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while
 connecting to server for Session: x2fd1f6
```

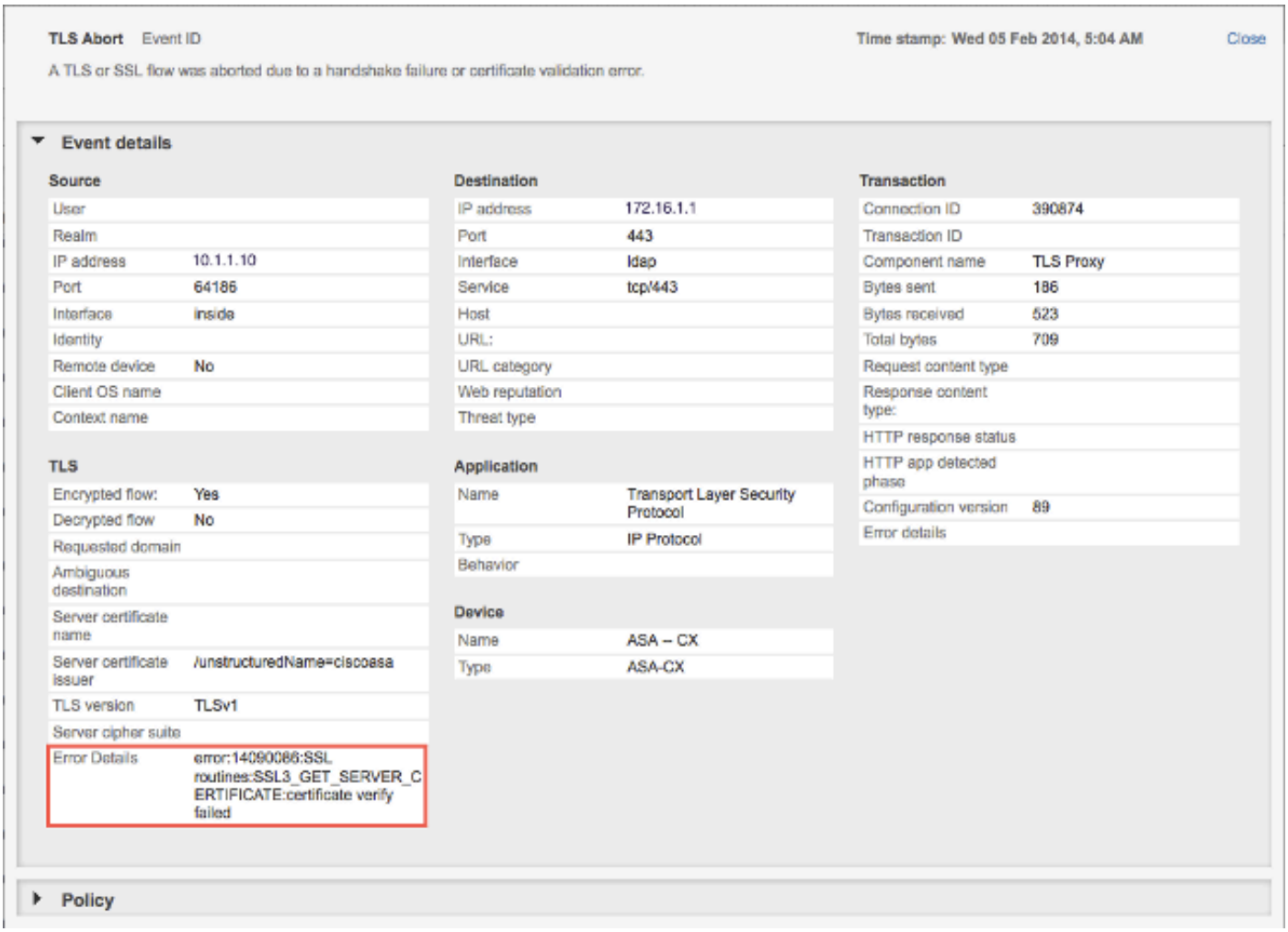
解決方法

この問題の 1 つの原因は、Triple Data Encryption Standard/高度暗号化規格（3DES/AES）ライセンス（通常 K9 と呼ばれています）がモジュールにインストールされていないことです。料金が発生するおとなく、モジュールの [K9 ライセンスをダウンロードし、PRSM 経由でアップロードできます。]

3DES/AES ライセンスをインストールしても問題が解決しない場合は、NGFW サービス モジュールとサーバ間の SSL ハンドシェイクのパケット キャプチャを取得し、サーバ管理者に連絡して、サーバの適切な SSL 暗号化をイネーブルにします。

問題

NGFW サービス モジュールがサーバに提示されている証明書を信頼しない場合、次のような エラー メッセージが表示されます。



表示されるエラーの（ハイライトされた）詳細情報を記録することが重要です。

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

モジュール診断のアーカイブにある /var/log/cisco/tls_proxy.log ファイルを確認すると、次のエラー メッセージが表示されています。

```
2014-02-05 05:22:11,505 INFO  TLS_Proxy - Certificate verification failure:
 self signed certificate (code 18, depth 0)

2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from
 server (0x230 = "fatal : unknown CA") in Session: x148a696e

2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
 SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
 connecting to server for Session: x148a696e
```

解決方法

モジュールがサーバ SSL 証明書を信頼できない場合、SSL ハンドシェイク プロセスが正常に行えるように、PRSM を搭載するモジュールにサーバ証明書をインポートする必要があります。

サーバ証明書をインポートするには、次の手順を実行します。

1. ブラウザ経由で証明書をダウンロードするためにサーバにアクセスするときは、NGFW サービス モジュールをバイパスします。モジュールをバイパスする方法の 1 つは、特定のサーバへのトラフィックを復号化しない復号化ポリシーを作成することです。このビデオでは、ポリシーの作成方法が示されます。

   以下に、ビデオで示される手順を示します。

   https://<IP_ADDRESS_OF_PRSM> に移動して、CX の PRSM にアクセスします。この例では **https://10.106.44.101** を使用します。

   PRSM で、[Configurations] > [Policies/Settings] > [Decryption policies] **の順に選択します。**

   画面の左上隅の近くにあるアイコンをクリックして、[Add above policy] **オプションを選択して、リストの先頭にポリシーを追加します。**

   ポリシーに名前を付け、ソースを **Any** のままにして、**CX Network group オブジェクトを作成します。**
   注：HTTPS ベースのサーバの IP アドレスを含めることに注意してください。この例では、IP アドレスとして **172.16.1.1** が使用されます。操作として、**Do not decrypt を選択します。**

   ポリシーを保存して、変更を確定します。
2. このビデオに示されているように、ブラウザを使用してサーバ証明書をダウンロードし、PRSM を介して NGFW サービス モジュールにアップロードします。

   以下に、ビデオで示される手順を示します。

   上述のポリシーを定義したら、ブラウザを使用して NGFW サービス モジュールを介して開く HTTPS ベースのサーバに移動します。
   注：この例では、Mozilla Firefox バージョン 26.0 は **https://172.16.1.1** という URL を持つサーバ (ASA 上の ASDM) に移動するために使用されます。セキュリティ警告が表示されたら、それを受け入れ、セキュリティ例外を追加します。

   アドレス バーの左側にある小さいロック形状のアイコンをクリックします。このアイコンの場所は、使用するブラウザとバージョンによって異なります。

   [View Certificate] **ボタンをクリックし、サーバ証明書を選択してから、[Details] タブの下にある [Export] タンをクリックします。**

お使いの PC の任意の場所に証明書を保存します。

PRSM にログインし、[Configurations] > [Certificates] の順に選択します。

[I want to...] > [Import certificate]をクリックし、以前にダウンロードしたサーバ証明書を選択します（ステップ4から）。

変更を保存して、確定します。この手順が完全すると、NGFW サービス モジュールはサーバによって提示された証明書を信頼しているはずです。

3. ステップ1で追加したポリシーを削除します。これで、NGFWサービスモジュールはサーバとのハンドシェイクを正常に完了できます。

関連情報

- ASA CX および Cisco Prime Security Manager 9.2 ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems