由於握手失敗或證書驗證錯誤，NGFW服務模組TLS中止錯誤

目錄

簡介

本文說明如何解決通過啟用解密的思科下一代防火牆(NGFW)服務模組訪問基於HTTPS的網站的特定問題。

必要條件

需求

思科建議您瞭解以下主題：

- 安全套接字層(SSL)握手過程
- SSL證書

採用元件

本檔案中的資訊是根據採用Cisco Prime安全管理員(PRSM)版本9.2.1.2(52)的思科NGFW服務模組。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

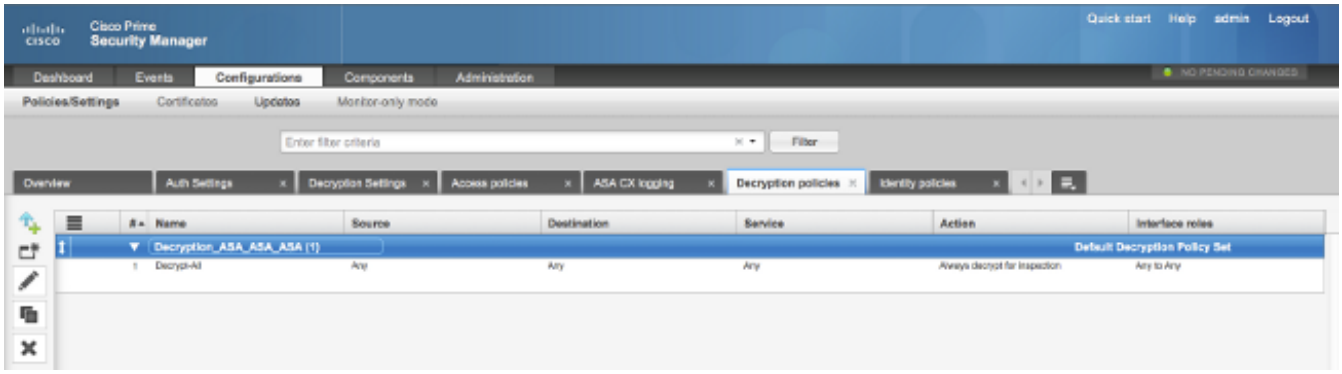
背景資訊

解密是一種功能，可讓NGFW服務模組對SSL加密的流進行解密（並檢查以其他方式加密的會話）並對流量實施策略。為了配置此功能，管理員必須在NGFW模組上配置解密證書，該證書提供給客戶端訪問基於HTTPS的網站，而不是原始伺服器證書。

為使解密起作用，NGFW模組必須信任伺服器提供的證書。本檔案將說明在NGFW服務模組與伺服器之間的SSL交握失敗時的案例，這些案例會導致您嘗試連線某些基於HTTPS的網站失敗。

出於本文檔的目的，這些策略在帶有PRSM的NGFW服務模組上定義：

- **身份策略**:沒有已定義的身份策略。
- **解密策略**:**Decrypt-All**策略使用以下配置：

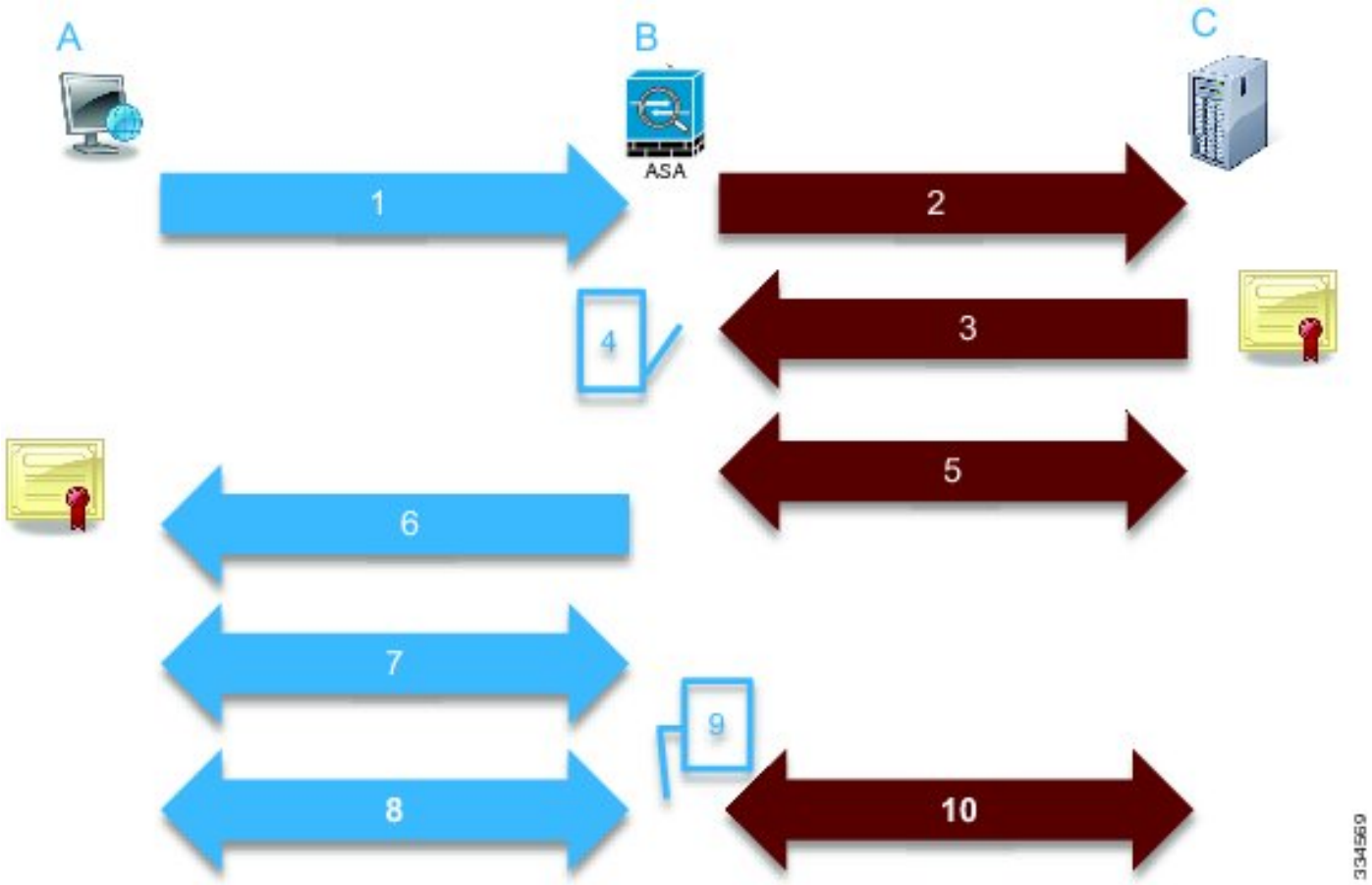


- **訪問策略**:沒有已定義的訪問策略。
- **解密設定**:本檔案假設NGFW服務模組上設定了**解密憑證**，且使用者端信任該憑證。

在NGFW服務模組上定義解密策略並按照前面所述進行配置時，NGFW服務模組會嘗試攔截通過模組的所有SSL加密流量並進行解密。

> **附註**：有關此過程的逐步說明，請參閱ASA CX和Cisco Prime安全管理器9.2使用手冊的解密流量部分。

此圖說明事件順序：



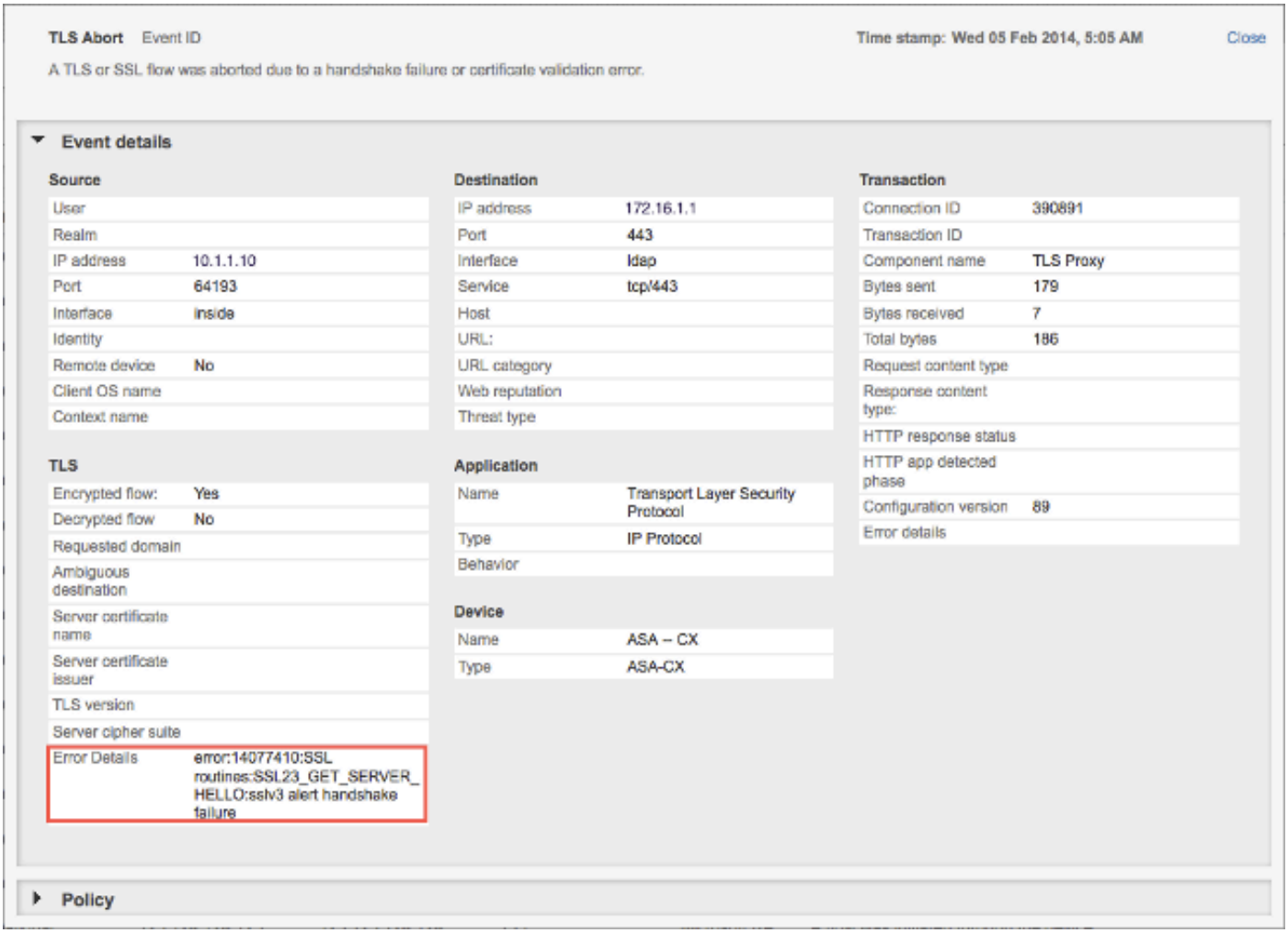
在此圖中，A 是使用者端，B是NGFW服務模組，C 是HTTPS伺服器。對於本文檔中提供的示例，基於HTTPS的伺服器是思科自適應安全裝置(ASA)上的思科自適應安全裝置管理器(ASDM)。

此過程有兩個重要因素需要考慮：

- 在該過程的第二步中，伺服器必須接受NGFW服務模組提供的其中一個SSL密碼套件。
- 在該過程的第四步，NGFW服務模組必須信任伺服器提供的證書。

問題

如果伺服器無法接受NFGW服務模組提供的任何SSL密碼，您將收到類似以下內容的錯誤消息：



必須注意錯誤詳細資訊資訊（突出顯示），其中顯示：

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

在模組診斷歸檔檔案中檢視/var/log/cisco/tls_proxy.log檔案時，會顯示以下錯誤消息：

```
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
```

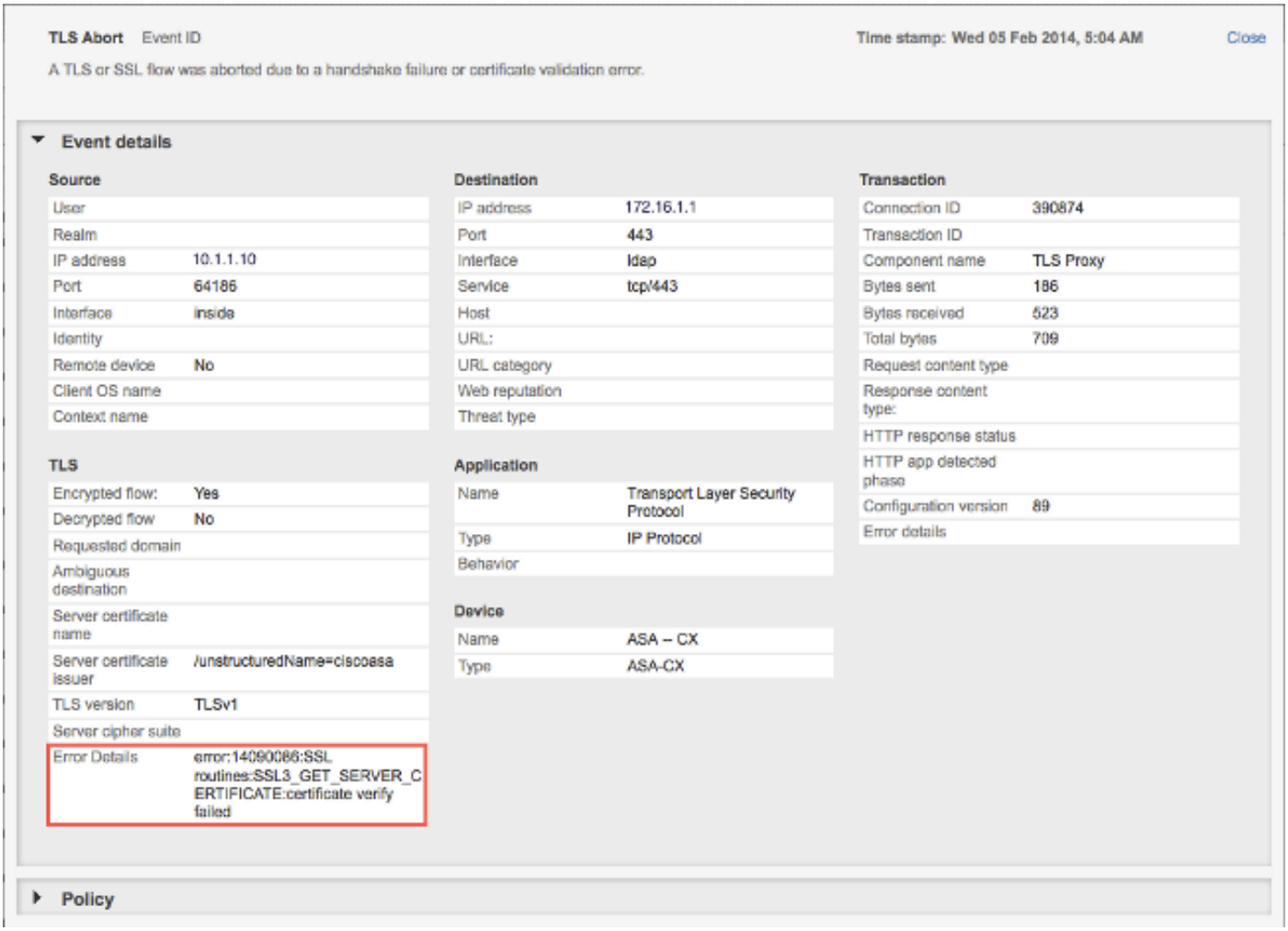
解決方案

此問題的一個可能原因是模組上未安裝三重資料加密標準/高級加密標準(3DES/AES)許可證（通常稱為K9）。您可以免費下載模組的K9許可證，並通過PRSM上傳該許可證。

如果在安裝3DES/AES許可證後問題仍然存在，請獲取NGFW服務模組和伺服器之間的SSL握手的資料包捕獲，然後與伺服器管理員聯絡以在伺服器上啟用適當的SSL密碼。

問題

如果NGFW服務模組不信任伺服器提供的證書，則會收到類似以下內容的錯誤消息：



必須注意錯誤詳細資訊資訊（突出顯示），其中顯示：

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

在模組診斷歸檔檔案中檢視/var/log/cisco/tls_proxy.log檔案時，會顯示以下錯誤消息：

```
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
```

解決方案

如果模組無法信任伺服器SSL證書，則必須使用PRSM將伺服器證書匯入模組，以確保SSL握手過程成功。

完成以下步驟以匯入伺服器證書：

1. 當您訪問伺服器以便通過瀏覽器下載證書時，請繞過NGFW服務模組。繞過模組的一種方法是建立不解密流向該特定伺服器的流量的解密策略。此影片顯示如何建立策略：

   以下步驟如影片所示：

   要在CX上訪問PRSM，請導航到**https://<IP_ADDRESS_OF_PRSM>**。此示例使用**https://10.106.44.101**。

   在PRSM中導航到**Configurations > Policies/Settings > Decryption policies**。

   按一下位於螢幕左上角的圖示，然後選擇**Add above policy**選項以將策略新增到清單頂部。

   將策略命名為，將Source保留為**Any**，並建立**CX Network組對**象。
   附註：請記得包含基於HTTPS的伺服器的IP地址。在本示例中，使用IP地址**172.16.1.1**。為操作選擇**Do not decrypt**。

   儲存策略並提交更改。
2. 透過瀏覽器下載伺服器憑證，並透過PRSM將其上傳到NGFW服務模組，如以下影片所示：

   以下步驟如影片所示：

   定義上述策略後，使用瀏覽器導航到通過NGFW服務模組開啟的基於HTTPS的伺服器。
   附註：在本示例中，使用Mozilla Firefox版本26.0導航到帶有**https://172.16.1.1**URL的伺服器（ASA上的ASDM）。如果彈出一個安全警告，請接受該警告並新增一個安全例外。

   按一下位址列左側的小鎖狀圖示。此圖示的位置因所使用的瀏覽器和版本而異。

   選擇伺服器證書後，按一下**View Certificate**按鈕，然後按一下Details頁籤下的**Export**按鈕。

   將證書儲存在您選擇的個人電腦上。

   登入PRSM並瀏覽到**Configurations > Certificates**。

   按一下**I want to... > Import certificate**，然後選擇以前下載的伺服器證書（從步驟4）。

   儲存並提交更改。完成後，NGFW服務模組應信任伺服器提供的證書。
3. 刪除步驟1中新增的策略。NGFW服務模組現在能夠成功完成與伺服器的握手。

相關資訊

- [ASA CX和Cisco Prime安全管理器9.2使用手冊]
- [技術支援與文件 - Cisco Systems]