Firepower資料路徑故障排除第5階段：SSL策略

目錄

簡介

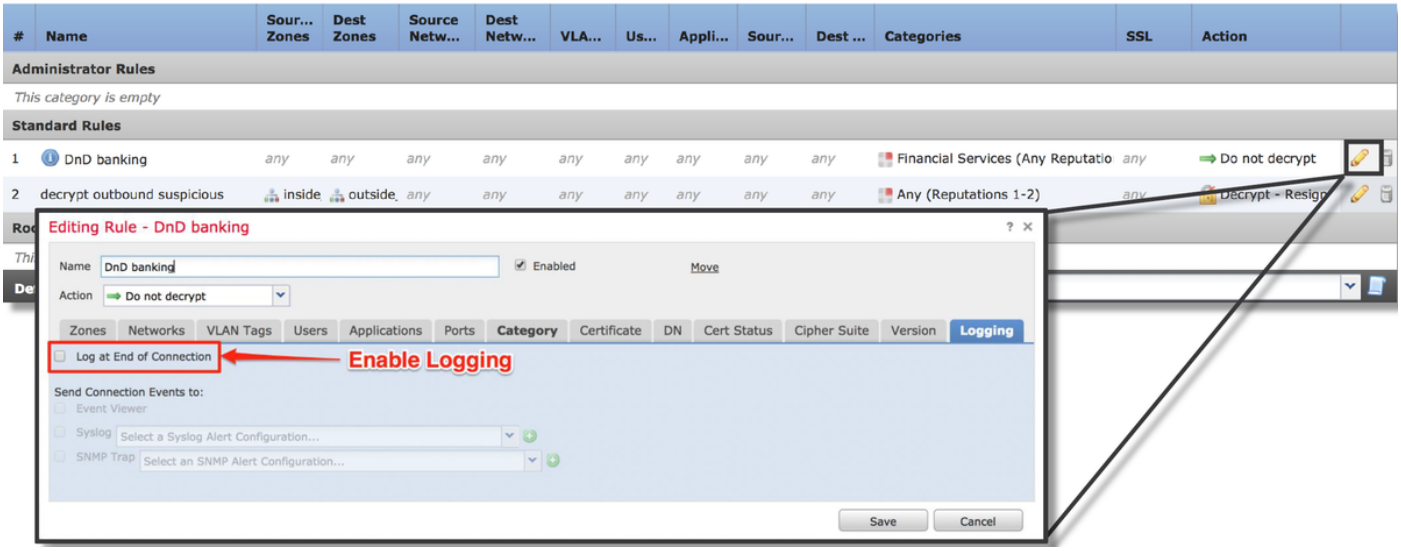
本文是一系列文章的一部分，這些文章介紹了如何對Firepower系統的資料路徑進行系統故障排除，以確定Firepower的元件是否影響流量。請參閱概述文章，瞭解有關Firepower平台架構的資訊，以及指向其他資料路徑故障排除文章的連結。

本文涵蓋Firepower資料路徑故障排除的第五階段，即安全套接字層(SSL)策略功能。

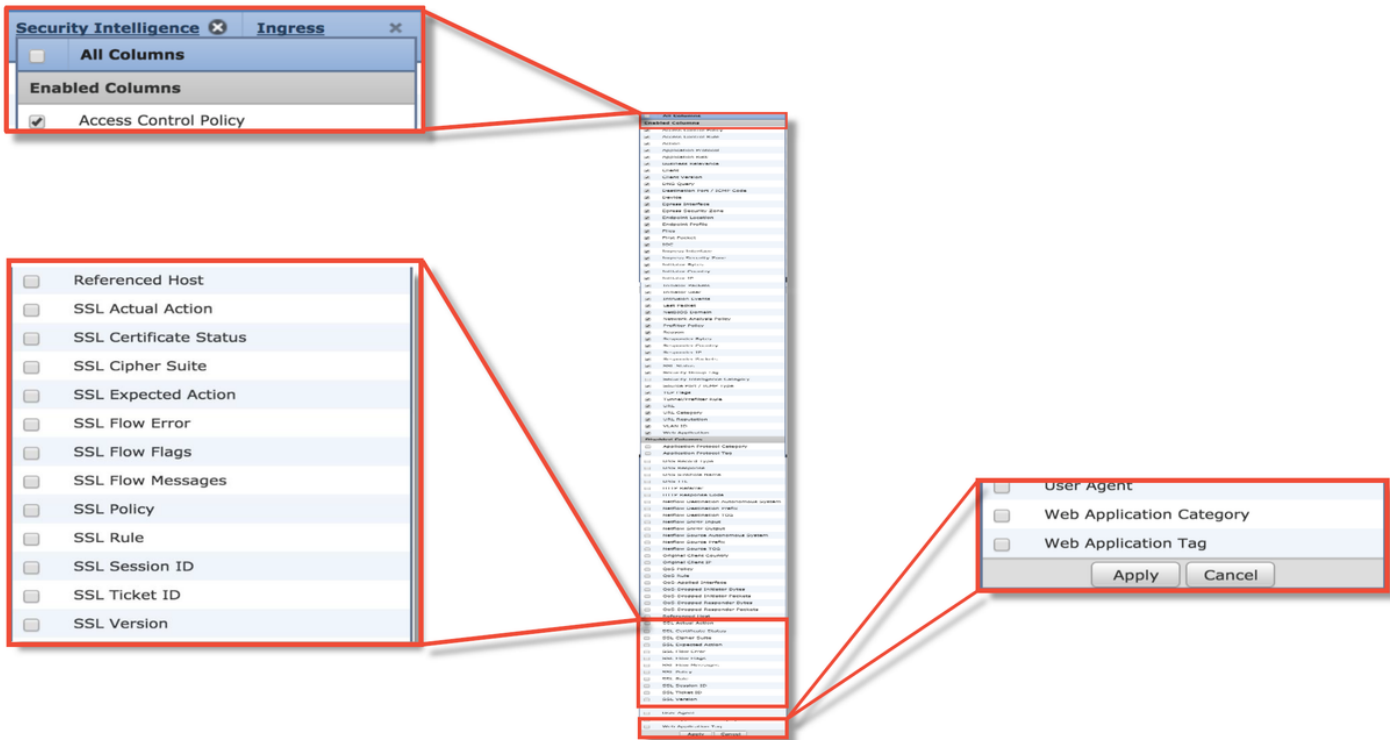
必要條件

- 本文中的資訊適用於任何Firepower平台 適用於具備FirePOWER服務（SFR模組）的自適應安全裝置(ASA)的SSL解密僅在6.0+中可用客戶端Hello修改功能僅在6.1+中可用
- 確認訪問控制策略中正在使用SSL策略

- 驗證是否已為所有規則啟用日誌記錄，包括「預設操作」



- 檢查Undecryptable Actions頁籤，檢視是否有選項設定為阻止流量
- 在連線事件中，當您處於連線事件的表檢視時，啟用名稱中帶有「SSL」的所有欄位大多數預設情況下處於禁用狀態，需要在連線事件檢視器中啟用



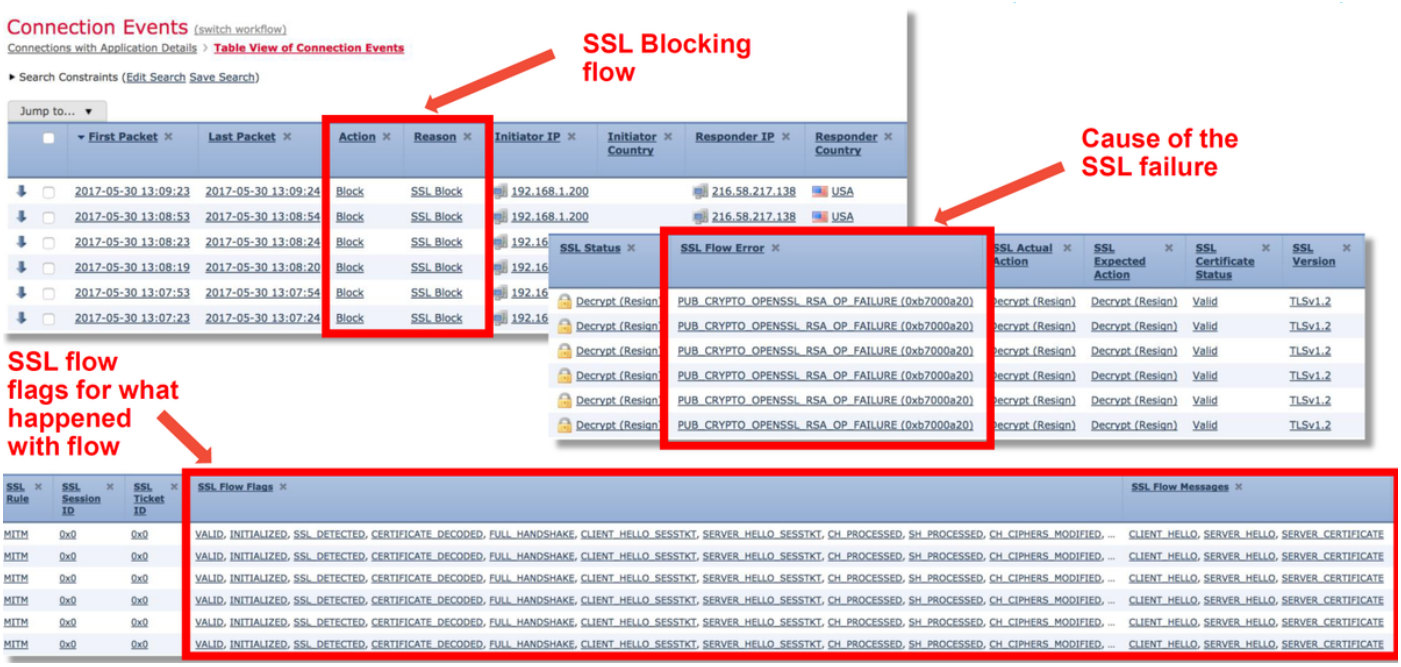
SSL策略階段故障排除

可以按照特定步驟操作，以幫助瞭解為什麼SSL策略會丟棄預期允許的流量。

檢查連線事件中的SSL欄位

如果SSL策略懷疑導致流量問題，則首先要檢查的是啟用所有SSL欄位後的Connection Events部分(在**Analysis > Connections > Events**下)，如上所述。

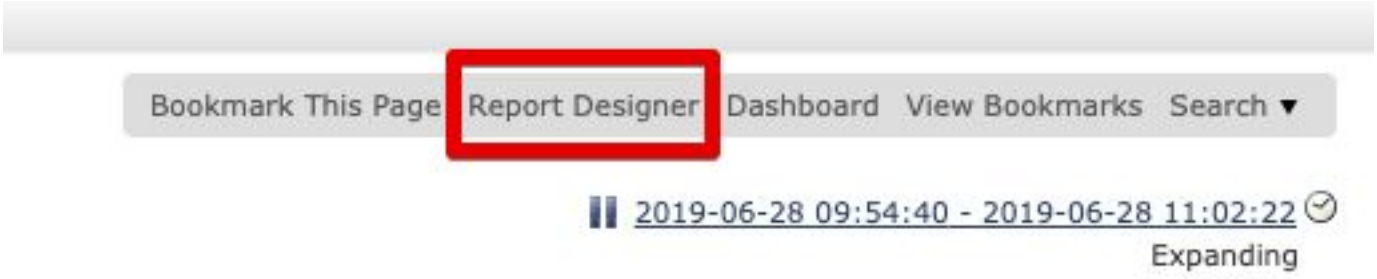
如果SSL策略阻止流量，則**Reason**欄位顯示「SSL Block」。 **SSL Flow Error**列包含有關發生阻止的原因的有用資訊。其他SSL欄位包含有關Firepower在流中檢測到的SSL資料的資訊。



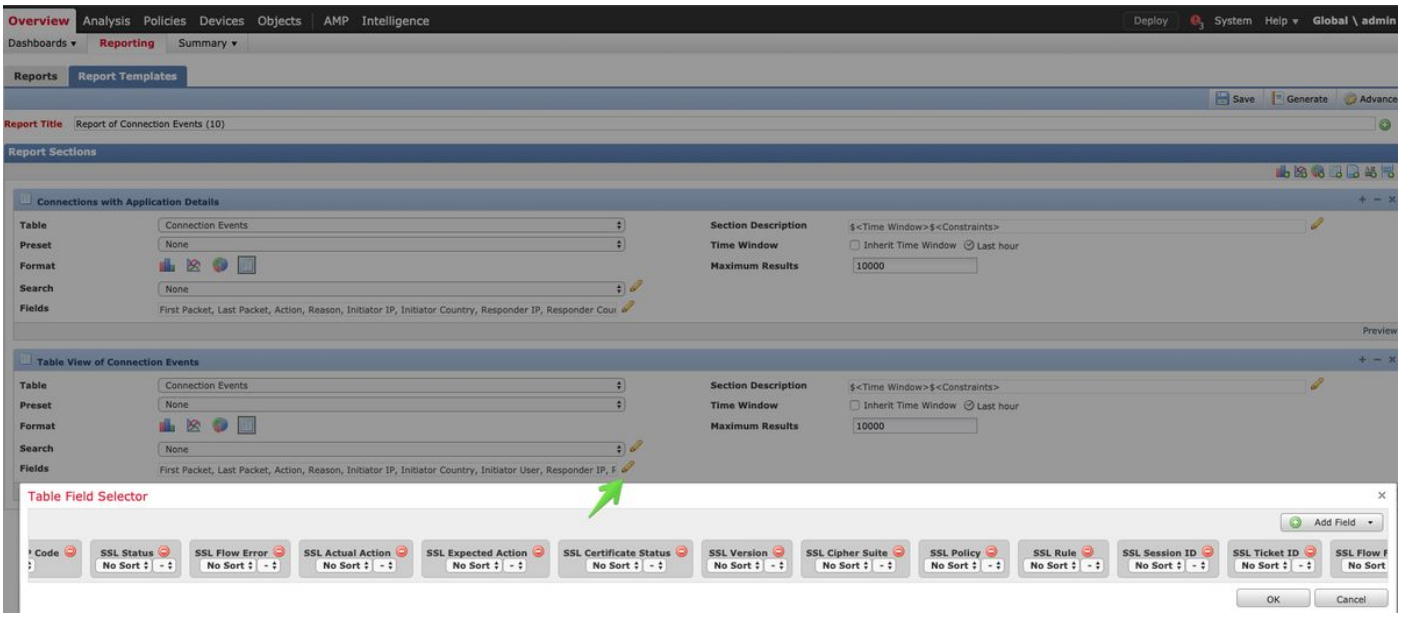
開啟SSL原則案件時，可向思科技術協助中心(TAC)提供此資料。為了輕鬆匯出此資訊，可使用**右上**

角的「報表設計器」按鈕。

如果從Connection Events部分按一下此按鈕，則會自動將篩選器和時間視窗選項複製到報告模板中。



確保在「Field」部分新增了所有提到的SSL欄位。



按一下**Generate**建立PDF或CSV格式的報告。

調試SSL策略

如果連線事件不包含有關流的足夠資訊，則可以在Firepower命令列介面(CLI)上運行SSL調試。

> **附註**：以下所有調試內容均基於x86架構軟體中發生的SSL解密。此內容不包括版本6.2.3和版本中新增的SSL硬體解除安裝功能的調試，這些功能是不同的。

> **附註**：在Firepower 9300和4100平台上，可以通過以下命令訪問有關外殼：

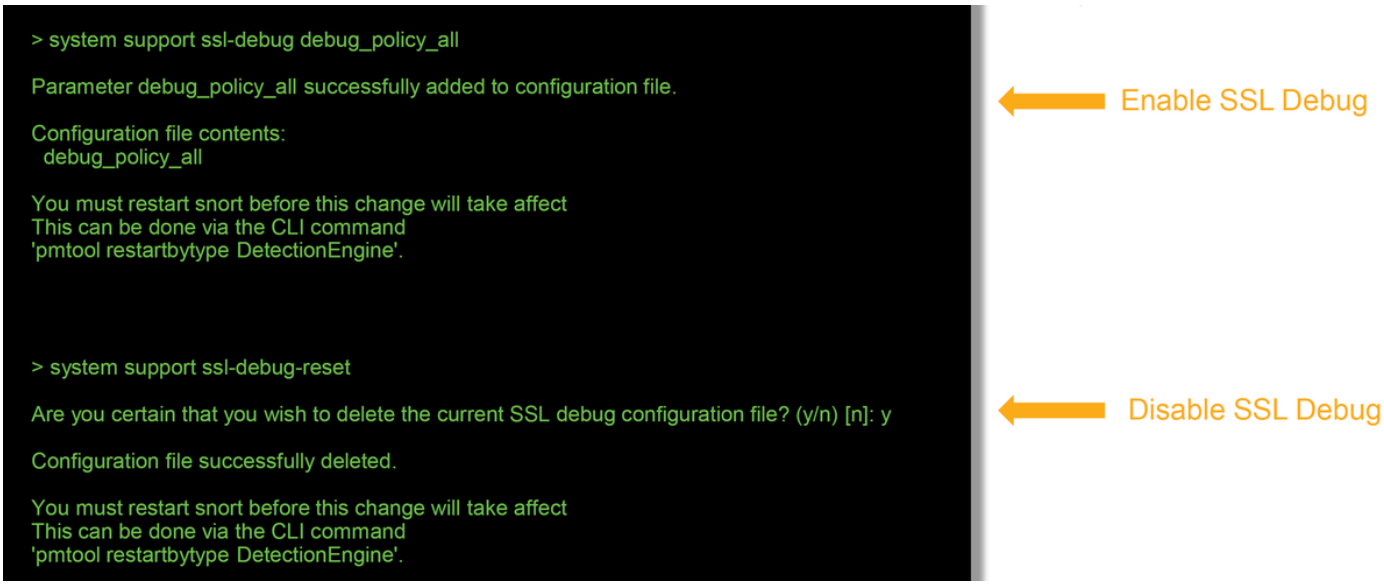
 # connect module 1主控台
Firepower-module1> **connect ftd**
>

對於多例項，可以使用以下命令訪問邏輯裝置CLI。

```
# connect module 1 telnet
Firepower-module1> connect ftd ftd1
正在連線到容器ftd(ftd1)控制檯……輸入「exit」以返回啟動CLI
>
```

可以運行**system support ssl-debug debug_policy_all**命令來為SSL策略處理的每個流生成調試資訊。

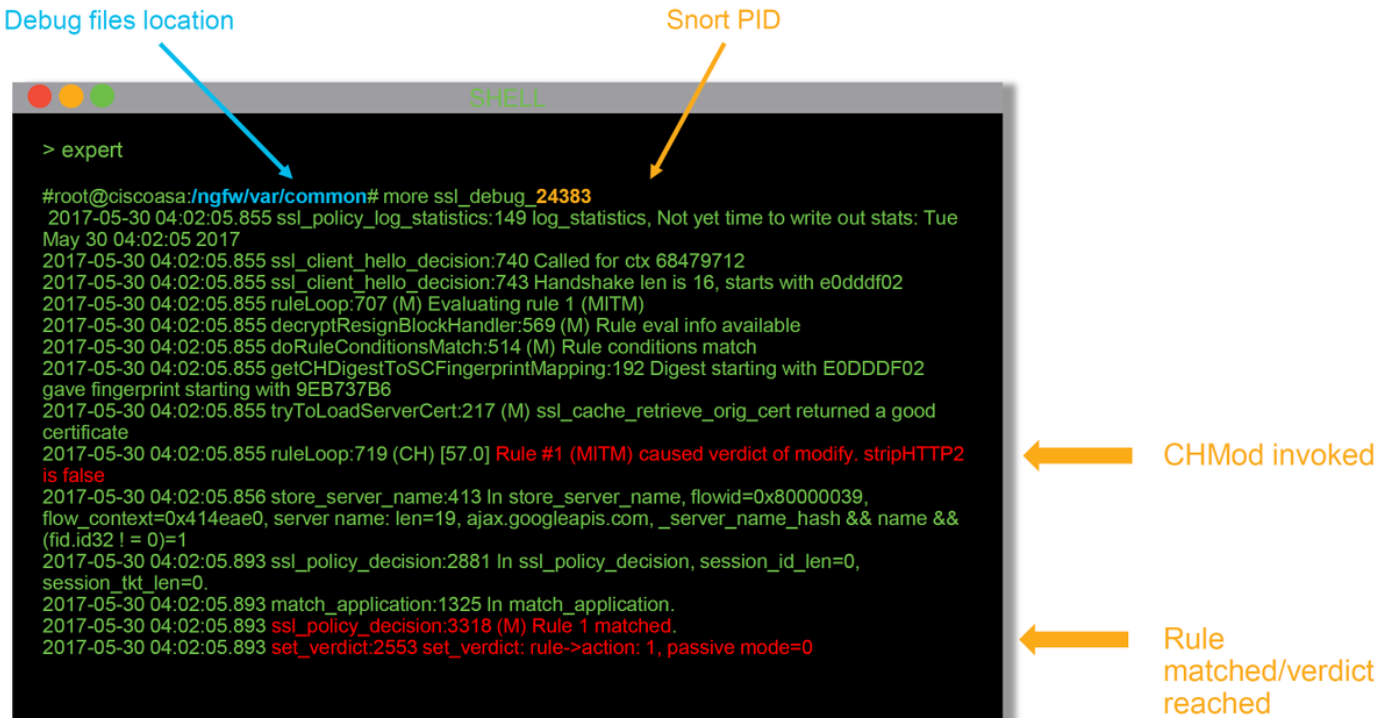
注意：在運行SSL調試之前和之後，必須重新啟動Snort進程，這可能會導致丟棄一些資料包，具體取決於所用的Snort關閉策略和部署。TCP流量將重新傳輸，但如果通過防火牆的應用程式無法容忍最小資料包丟失，則UDP流量可能會受到負面影響。



警告：使用**system support ssl-debug-reset** 命令收集必要的資料後，不要忘記關閉調試。

將為在Firepower裝置上運行的每個snort進程寫入一個檔案。檔案的位置將為：

- **/var/common**（非FTD平台）
- **/ngfw/var/common** for FTD platform



以下是偵錯日誌中的一些有用欄位。

```
...
   SSL Flow Flags: 0x00000088c48181c3 -
VALID,INITIALIZED,SSL_DETECTED,CERTIFICATE_DECODED,FULL_HANDSHAKE,CLIENT_HELL
O_SESSTKT,SERVER_HELLO_SESSTKT,CH_PROCESSED,SH_PROCESSED,CH_CIPHERS_MO
DIFIED,CH_CURVES_MODIFIED,CH_EXTENSION_REMOVED,CH_ALPN_HAS_H2
   SSL Session ID:
   SSL Session Ticket:

  Network parameters:
    src_addr: 192.168.1.200
    src_port: 55113
    src_intf: 3
    src_zone: -1
    dst_addr: 216.58.218.234
    dst_port: 443
    dst_intf: 2
    dst_zone: -1
    vlan: 0
  Matching Rule:
    ordinal rule id: 1
    rule id: 1
    rule name: MITM
  Verdict:
     Flow action: 6 - Decrypt and resign.
     Error action: 2 - Block.
```

Verdict the flow reached

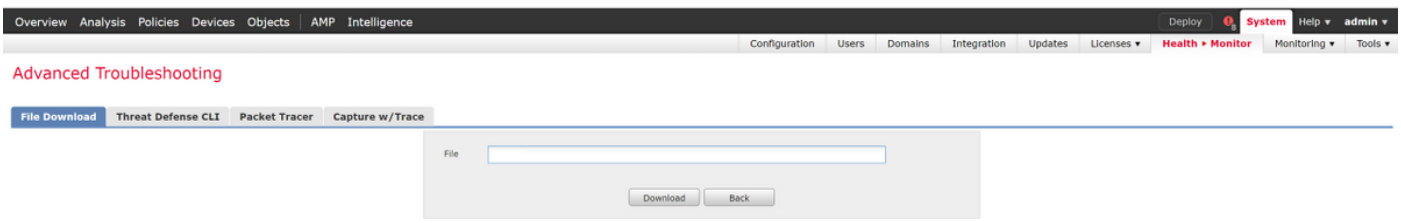
```
...
2017-05-30 04:02:05.894  Error callback.
 Logstr: ssl_policy_error_callback
  Process ID: 24383
  Flow context: 0x414eae0
  Flow info: 0x7ffea4b8d3a0
     flowid: 0x80000039
     error: 0xb7000a20
     FLOW ERROR FOUND:
         - NSE:PubCrypto [0xb7000a20;code:32;sub:10] OpenSSL RSA operation failure;
     cipher_suite: 65535 - Unknown
     ssl_version: UNKNOWN
     server_cert_h: -1
     flags: 0xca4a0407068181c5/0x00000088c0000000
    messages: 0x00000078
  Connection Event: 0x7ffea4b8d290
     Policy ID: 93a182e8-1d00-11e6-9e03-b6d00120637b
    [ ...Omitting for brevity ]
    SSL Flow Status: 10 - decryption_error - Error found during SSL flow after server certificate.
    SSL Flow Error: 0xb7000a20 - NSE:PubCrypto [0xb7000a20;code:32;sub:10] OpenSSL RSA
operation failure;
...
```

SSL Errors potentially causing drop

附註：如果Firepower開始解密後發生解密錯誤，則必須丟棄流量，因為防火牆已修改/中間人引導了會話，因此客戶端和伺服器無法恢復通訊，因為它們在流中使用了不同的TCP堆疊和不同的加密金鑰。

使用本文中的說明，可以從>提示符處從Firepower裝置複製調試檔案。

或者，在Firepower 6.2.0及更高版本中，FMC上有一個選項。要在FMC上訪問此UI實用程式，請導航至**Devices > Device Management**。然後，按一下 圖示位於相關裝置旁，然後是**Advanced Troubleshooting > File Download**。然後，您可以輸入有問題的檔案的名稱，然後按一下「下載」。

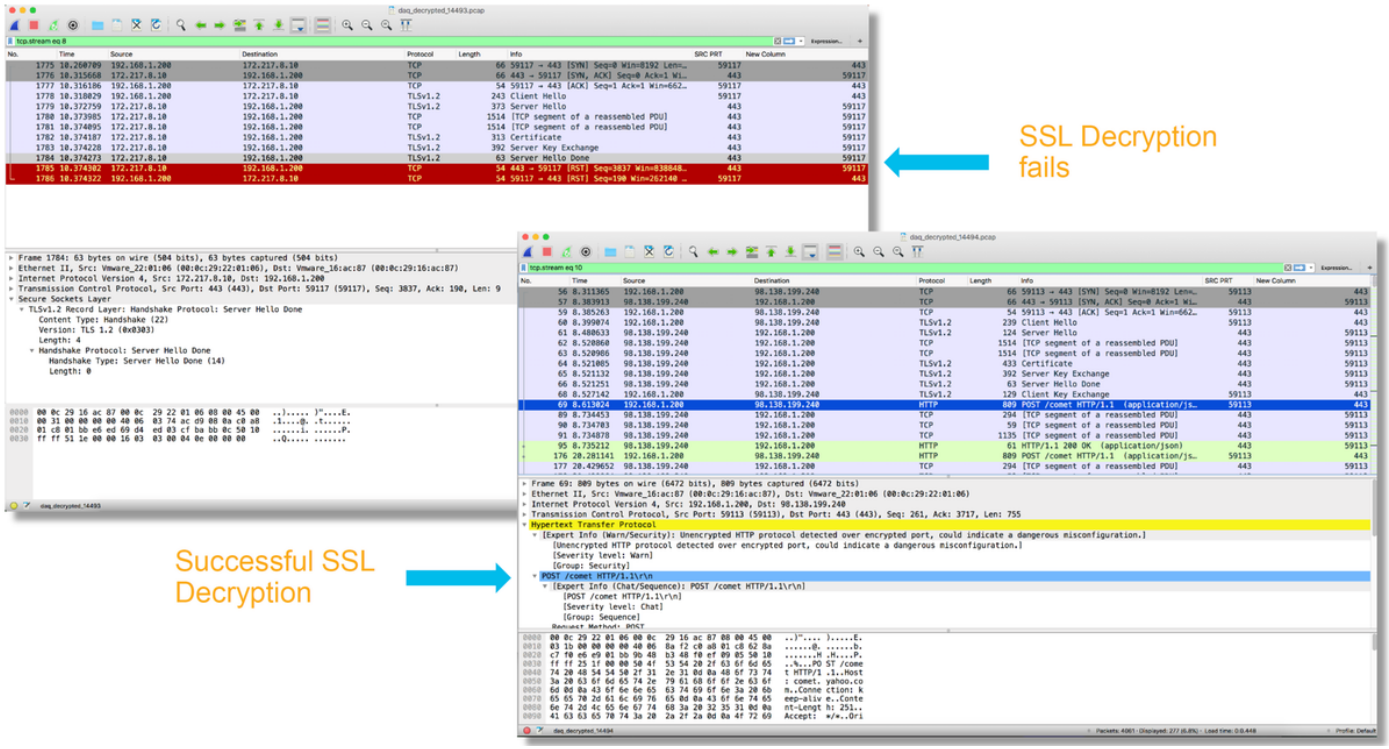


生成解密的資料包捕獲

可以為由Firepower解密的會話收集未加密的資料包捕獲。命令是**system support debug-DAQ debug_daq_write_pcap**

> **注意**：在生成解密的資料包捕獲之前，必須重新啟動snort進程，否則可能導致丟棄幾個資料包。TCP流量等有狀態通訊協定會重新傳輸，但其他流量（例如UDP）可能會受到負面影響。

```
> system support debug-DAQ debug_daq_write_pcap

Parameter debug_daq_write_pcap successfully added to configuration file.

Configuration file contents:
  debug_daq_write_pcap

You must restart snort before this change will take affect
This can be done via the CLI command
'system support pmtool restartbytype DetectionEngine'.

> system support pmtool restartbytype DetectionEngine

> expert
admin@firepower:~$ cd /var/common/
admin@firepower:/var/common$ ls
daq_decrypted_15903.pcap  daq_decrypted_15909.pcap

admin@firepower:/var/common$ tar pczf daq_pcaps.tgz daq_decrypted_*
```

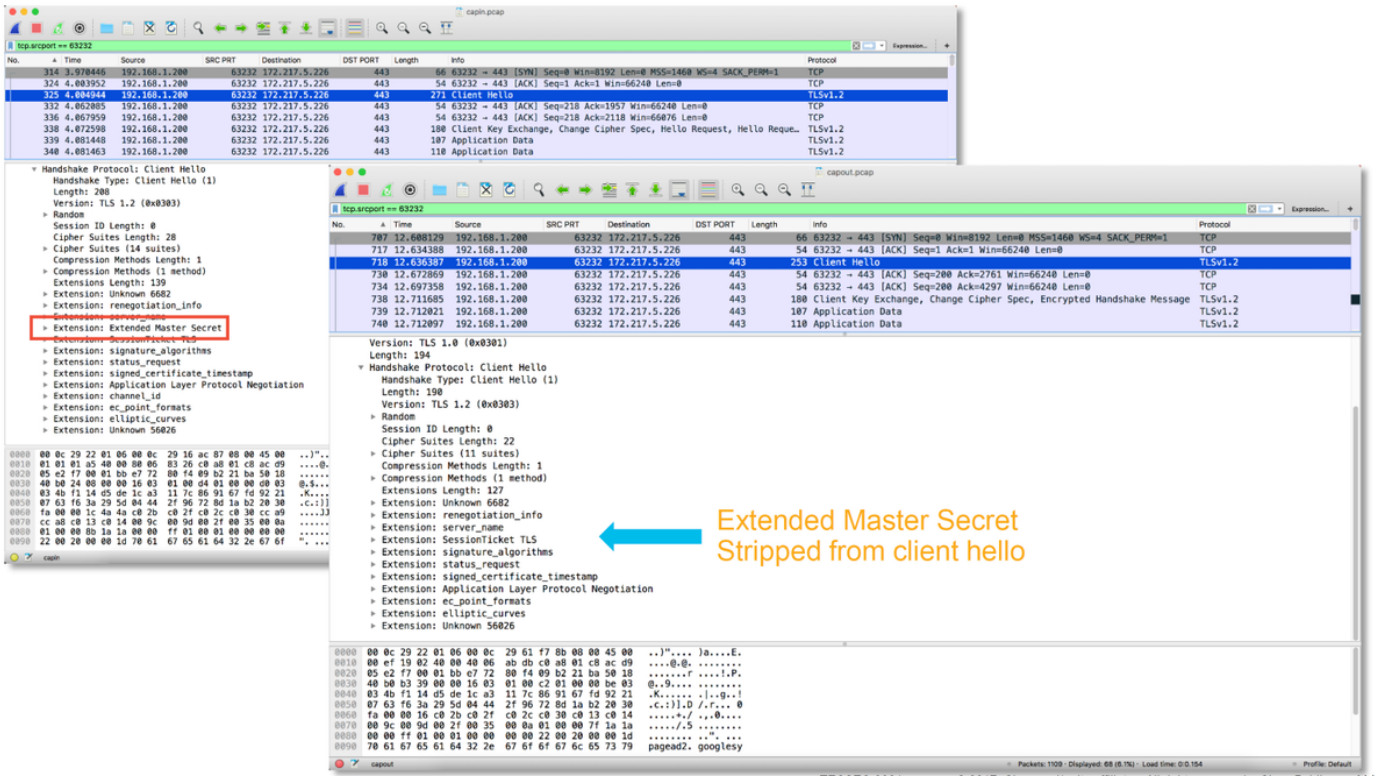


> **注意**：在將解密的PCAP捕獲提交到TAC之前，建議過濾捕獲檔案並將其限制到有問題的流，以避免不必要地洩露任何敏感資料。

查詢客戶端Hello修改(CHMod)

還可以評估資料包捕獲，檢視是否正在進行客戶端hello修改。

左側的資料包捕獲描述原始客戶端hello。右邊顯示的是伺服器端資料包。請注意，已通過Firepower中的CHMod功能刪除擴展主金鑰。



確保客戶端信任為解密/重新簽名CA

對於具有「解密 — 重新簽名」操作的SSL策略規則，請確保客戶端主機信任用作重新簽名CA的證書頒發機構(CA)。終端使用者不應有任何跡象表明他們受到防火牆的中間人控制。他們應該信任簽名CA。這通常通過Active Directory(AD)組策略實施，但取決於公司策略和AD基礎架構。

有關詳細資訊，可以查閱以下文章，其中概述了如何建立SSL策略。

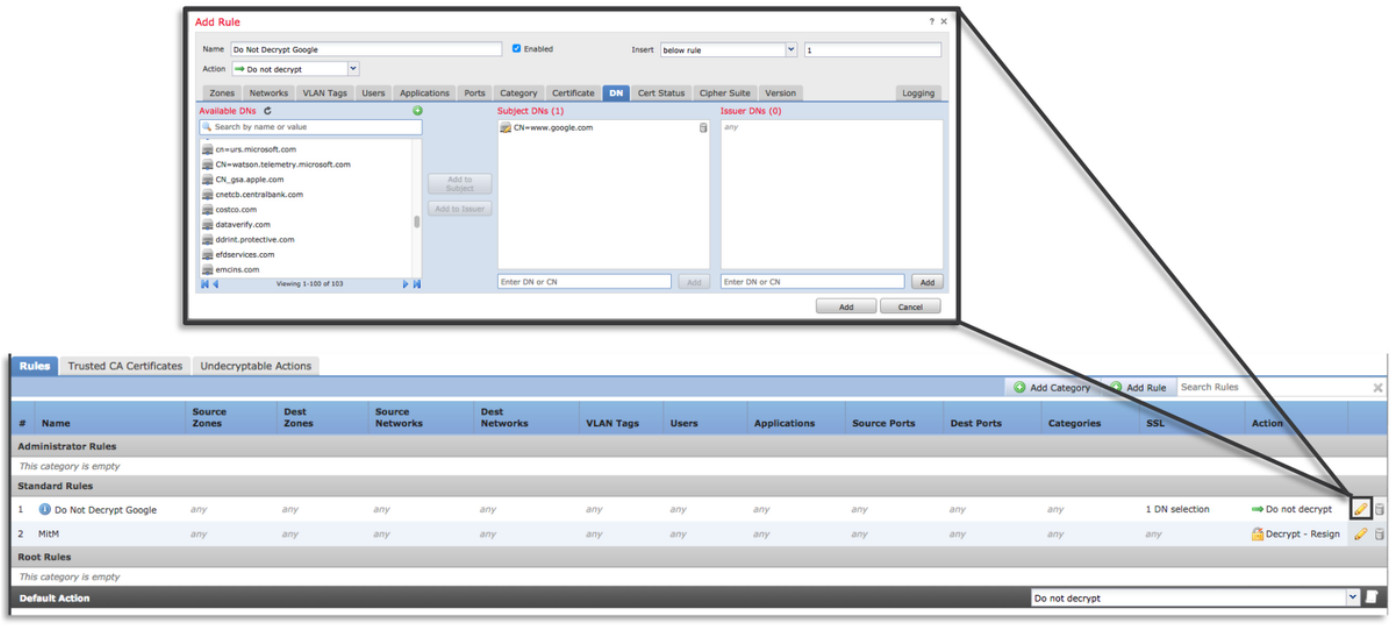
緩解步驟

可遵循一些基本緩解步驟，以便：

- 重新配置SSL策略以不解密某些流量
- 從客戶端hello資料包中去除某些資料，以便解密成功

新增不解密(DnD)規則

在以下示例場景中，確定通過SSL策略檢查時到google.com的流量中斷。根據伺服器證書中的公用名(CN)新增規則，以便不會解密到google.com的流量。



儲存並部署策略後，可以再次執行上述故障排除步驟，以檢視Firepower對流量執行的操作。

客戶端Hello修改調整

在某些情況下，故障排除可能會發現Firepower在解密某些流量時遇到了問題。**系統支援ssl-client-hello-tuning**實用程式可在CLI上運行，以使Firepower從客戶端hello資料包中刪除特定資料。

在以下示例中，新增了一個配置，以便刪除某些TLS擴展。通過搜尋TLS擴展和標準的資訊可以找到數字ID。

> **注意**：在客戶端hello修改更改生效之前，必須重新啟動snort進程，因為更改生效可能導致丟棄一些資料包。TCP流量等有狀態通訊協定會重新傳輸，但其他流量（例如UDP）可能會受到負面影響。

```
> system support ssl-client-hello-tuning
  SSL Client Hello tuning of attributes ciphers_allow, ciphers_remove, extensions_allow,
extensions_remove, curves_allow, curves_remove  handshake attribute


> system support ssl-client-hello-tuning extensions_remove 16,13172
Using tuning file: /etc/sf/ssl_client_hello.conf

Parameter and value successfully added to configuration file.

Configuration file contents (defaults added automatically):
   extensions_remove=16,13172

You must restart snort before this change will take affect
This can be done via the CLI command
'pmtool restartbytype DetectionEngine'.


> system support ssl-client-hello-reset
Using tuning file: /etc/sf/ssl_client_hello.conf

Are you certain that you wish to delete the current SSL tuning configuration file? (y/n) [n]: y

Configuration file successfully deleted.
```

Disabling the HTTP2/SPDY TLS extensions

16 = Application Layer Protocol Negotiation

13172 = Next protocol negotiation

Resetting the client hello modifications

要恢復對客戶端hello修改設定所做的任何更改，可以實施**system support ssl-client-hello-reset**命令。

要提供給TAC的資料

資料	說明
對Firepower管理中心(FMC)和Firepower裝置中的檔案進行故障排除	http://www.cisco.com/c/en/us/s
SSL調試	有關說明，請參閱本文
完整會話資料包捕獲（儘可能從客戶端、Firepower裝置本身和伺服器端）	http://www.cisco.com/c/en/us/s
連線事件螢幕截圖或報告	有關說明，請參閱本文

下一步

如果確定SSL策略元件不是問題的原因，則下一步是排除活動身份驗證功能的故障。

按一下here繼續下一篇文章。