Firepowerデータパスのトラブルシューティングフェーズ5:SSLポリシー

内容

概要

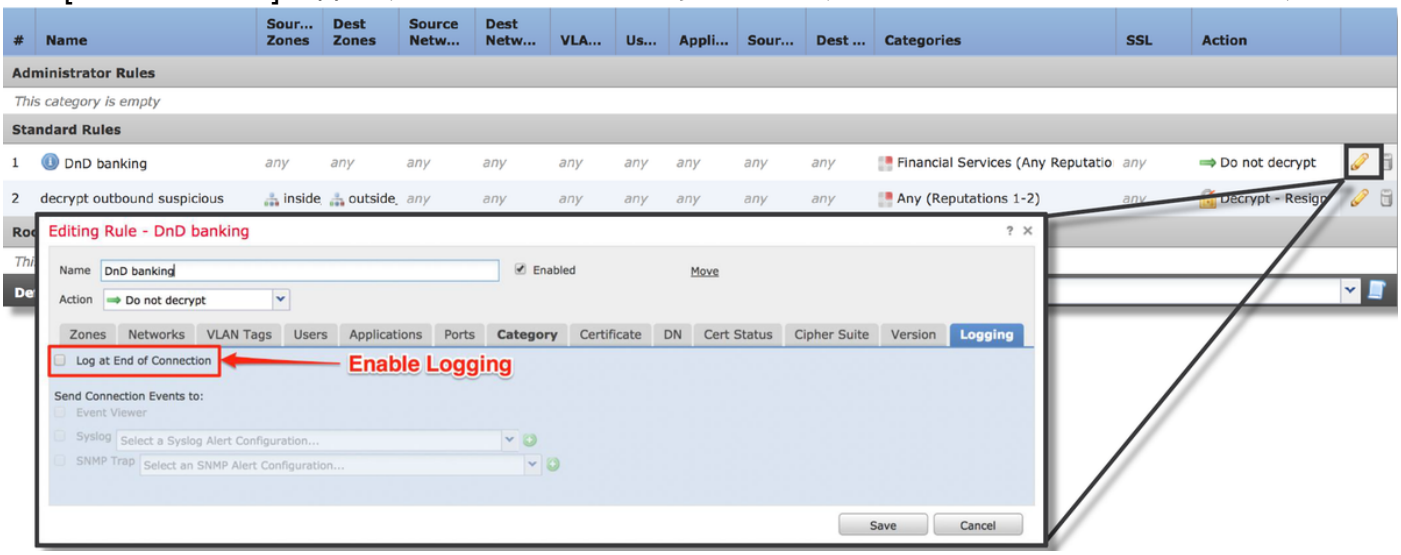
この記事は、Firepowerシステムのデータパスを体系的にトラブルシューティングし、Firepowerのコンポーネントがトラフィックに影響を与えているかどうかを判断する方法を説明する一連の記事の一部です。Firepowerプラットフォームのアーキテクチャに関する情報や、その他のデータパスのトラブルシューティングに関する記事へのリンクについては、概要記事を参照してください。

この記事では、Firepowerデータパスのトラブルシューティングの5番目の段階であるセキュアソケットレイヤ(SSL)ポリシー機能について説明します。

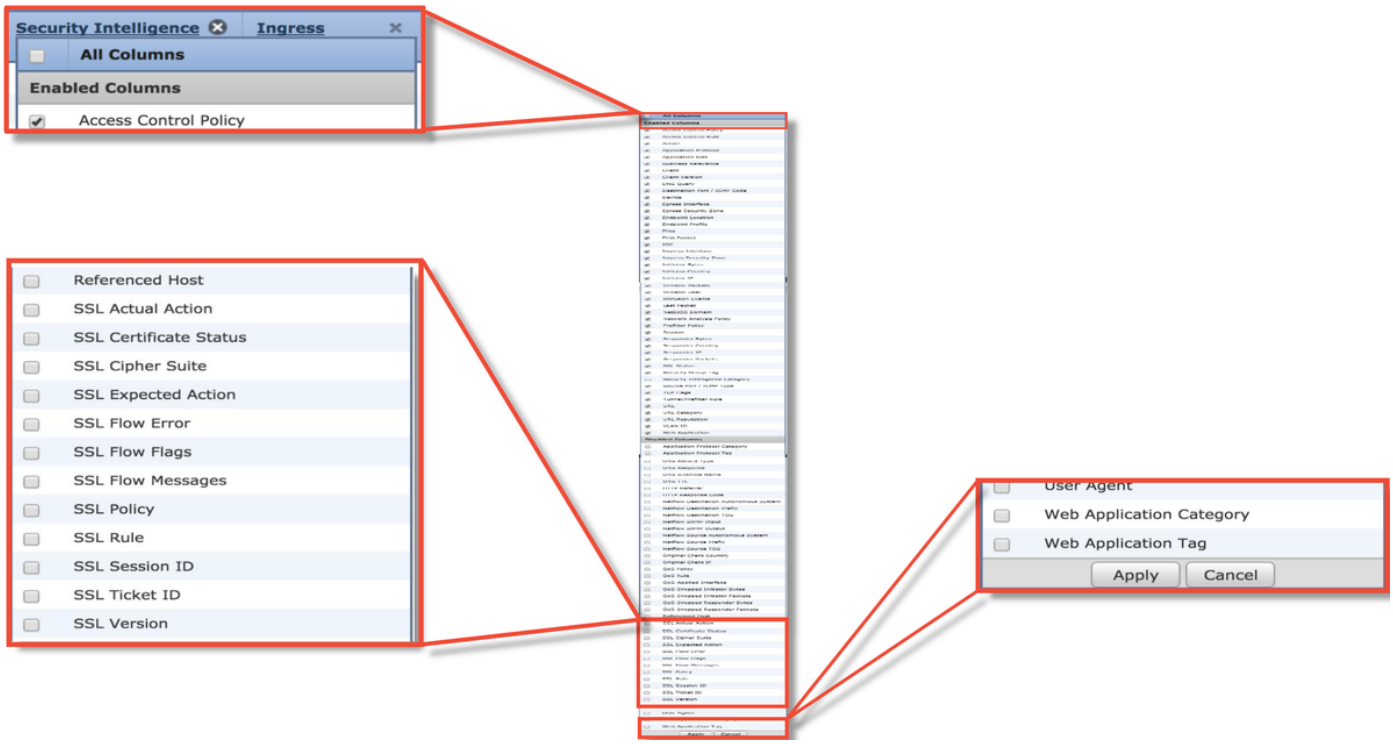
前提条件

- この記事の情報は、すべてのFirepowerプラットフォームに適用されます 適応型セキュリティアプライアンス(ASA)とFirePOWERサービス（SFRモジュール）のSSL復号化は6.0以降でのみ使用可能Client Hello Modification機能は6.1+でのみ使用できます
- アクセスコントロールポリシーでSSLポリシーが使用されていることを確認します

- [Default Action]を含むすべてのルールでロギングが有効になっていることを確認します



- [Undecryptable Actions]タブで、トラフィックをブロックするオプションが設定されているかどうかを確認します
- 接続イベントで、接続イベントのテーブルビューにいる場合は、名前に「SSL」を含むすべてのフィールドを有効にします
  ほとんどの機能はデフォルトで無効になっており、接続イベントビューアで有効にする必要があります



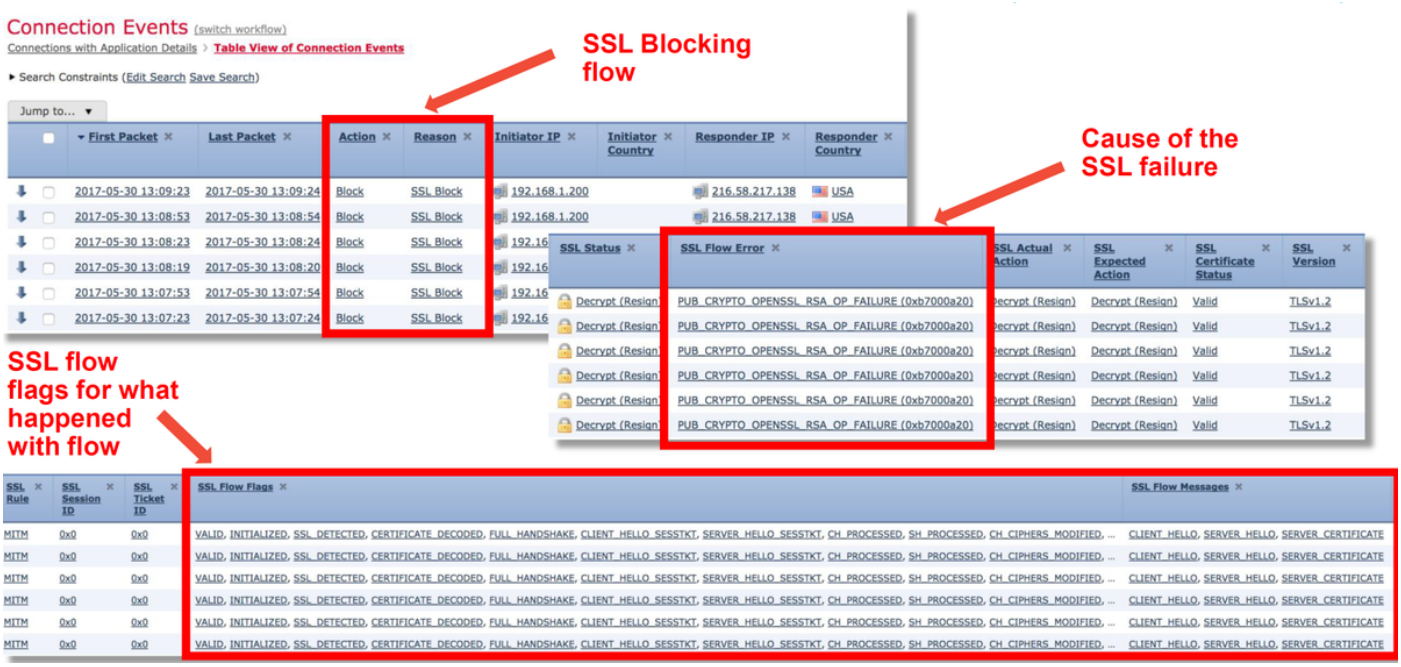
SSLポリシーフェーズのトラブルシューティング

SSLポリシーが許可されると予想されるトラフィックをドロップする理由を理解するために、特定の手順に従うことができます。

接続イベントのSSLフィールドをチェックする

SSLポリシーでトラフィックの問題が発生している疑いがある場合、最初に確認する場所は、上記のように、すべてのSSLフィールドを有効にした後の[Connection Events]セクション(**[Analysis] > [Connections] > [Events]**)です。

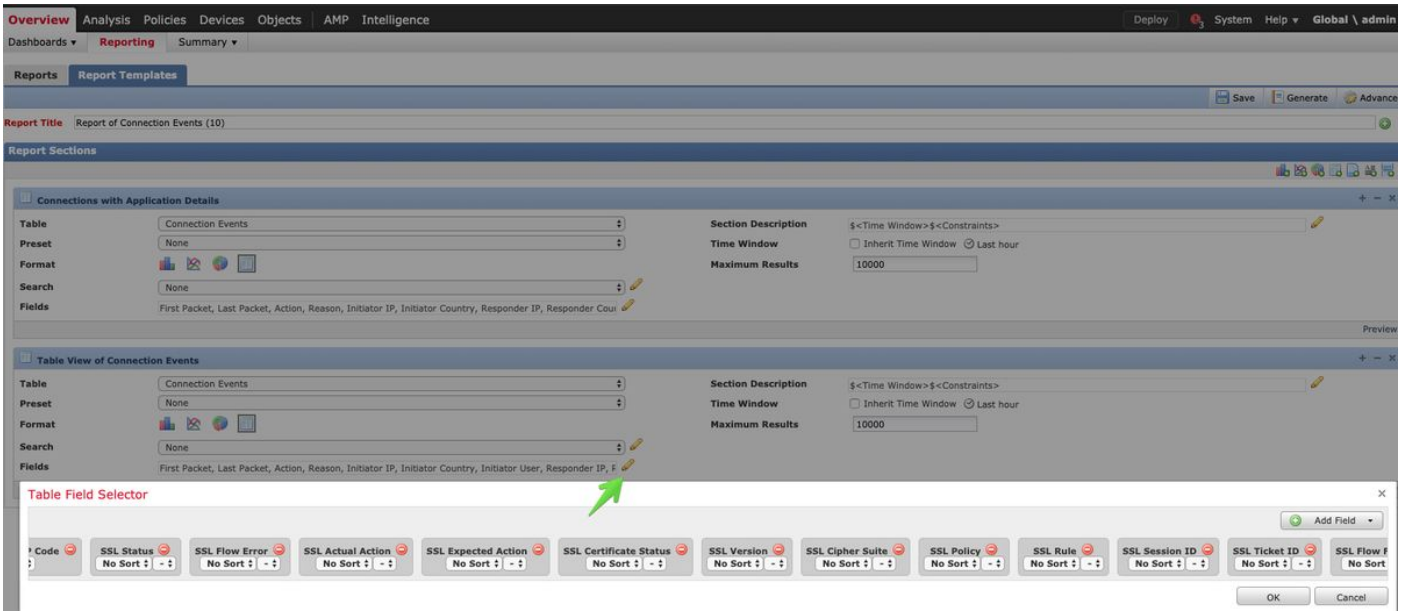
SSLポリシーがトラフィックをブロックしている場合、**[Reason]**フィールドには「SSL Block」と表示されます。「**SSL Flow Error**」列**には、ブロック**が発生した理由に関する有用な情報が表示されます。他のSSLフィールドには、Firepowerがフローで検出したSSLデータに関する情報が含まれています。



このデータは、SSLポリシーのケースをオープンする際にCisco Technical Assistance Center(TAC)に提供できます。この情報を簡単にエクスポートするには、右上**の[レポート**デザイナ]ボタンを使用できます。

[接続イベント(Connection Events)]セクションからこのボタンをクリックすると、フィルタとタイムウィンドウのオプションがレポートテンプレートに自動的にコピーされます。

[Field]セクションで、言及されているすべてのSSLフィールドが追加されていることを確認します。



「生成」をクリックして、PDFまたはCSV形式のレポートを作成します。

SSLポリシーのデバッグ

接続イベントにフローに関する十分な情報が含まれていない場合は、Firepowerコマンドラインインターフェイス(CLI)でSSLデバッグを実行できます。

> **注**：次のデバッグ内容はすべて、x86アーキテクチャ上のソフトウェアで発生するSSL復号化に基づいています。このコンテンツには、バージョン6.2.3以降で追加された、異なるSSLハードウェアオフロード機能からのデバッグは含まれていません。

> **注**：Firepower 9300および4100プラットフォームでは、問題のシェルに次のコマンドでアクセスできます。
>
> **# connect module 1 console**
> Firepower-module1> **connect ftd**
> **>**
>
> マルチインスタンスの場合、論理デバイスのCLIには次のコマンドでアクセスできます。
> **# connect module 1 telnet**
> Firepower-module1> **connect ftd ftd1**
> コンテナftd(ftd1)コンソールに接続しています... 「exit」と入力してブートCLIに戻ります
> **>**

system support ssl-debug debug_policy_allコマンドを実行**すると、SSLポリシーによって処理される各フローのデバッグ情報を生成できます。**

> **注意**：Snortプロセスは、SSLデバッグの実行前と実行後に再起動する必要があります。これにより、使用されるSnortダウンポリシーと展開に応じて、いくつかのパケットがドロップされる可能性があります。TCPトラフィックは再送信されますが、ファイアウォールを通過するアプリケーションが最小パケット損失を許容しない場合、UDPトラフィックは悪影響を受ける可能性があります。

```
> system support ssl-debug debug_policy_all

Parameter debug_policy_all successfully added to configuration file.

Configuration file contents:
  debug_policy_all

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



> system support ssl-debug-reset

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

Configuration file successfully deleted.

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

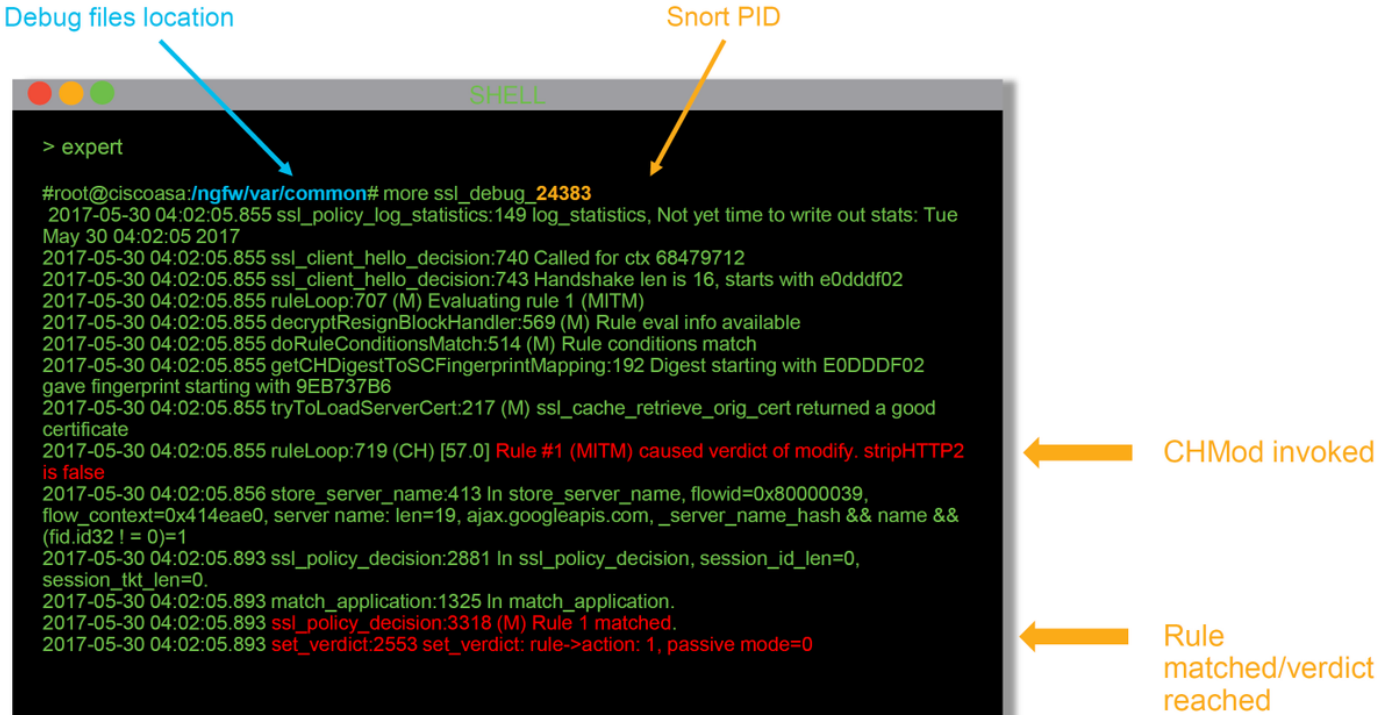
Enable SSL Debug

Disable SSL Debug

警告：system support ssl-debug-resetコマンドを使用して必要なデータを収集した後は、デバッグを必ずオフにします。

Firepowerデバイスで実行されている各Snortプロセスに対して書き込まれたファイルがあります。ファイルの場所：

- **/var/common**をFTD以外のプラットフォーム
- **/ngfw/var/common for** FTD platforms



デバッグログの有用なフィールドを次に示します。

```
…
2017-05-30 04:02:05.893  Verdict callback.
 Logstr: ssl_policy_decision: Found matching rule.
   Process ID: 24383
   Flow context: 0x414eae0
   Flow info: 0x7ffea4b8ccf0
     flowid: 0x80000039
     error: 0x00000000
     cipher_suite: 49199 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     ssl_version: TLS1.2
     server_cert_h: 89
         cert summary: CN=*.googleapis.com;O=Google Inc;
     flags: 0x40820004048181c3/0x00000088c0000000
  Connection Event: 0x7ffea4b8c9e8 messages: 0x00000038
  Policy ID: 93a182e8-1d00-11e6-9e03-b6d00120637b
     Rule ID: 1
     Logging is on: 1
     Cipher Suite: 49199 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     SSL Version: 16 - TLS1.2
     Server Cert Status: 2 - valid ca chain,
     URL Category Matched: 0
     App ID Matched: 0
     Client Hello Server Name: (null)
     Actual Action: 6 - Decrypt and resign.
     Expected Action: 6 - Decrypt and resign.
     SSL Flow Status: 2 - success - SSL Rule successfully applied.
     SSL Flow Error: 0x00000000 - NSLIB:Logging [0x00000000;code:0;sub:0] Success;
     SSL Flow Messages: 0x00000038 - CLIENT_HELLO,SERVER_HELLO,SERVER_CERTIFICATE
```

Certificate summary can help identify the flow

Validate that Expected and Actual actions are the same

```
…
    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;
…
```

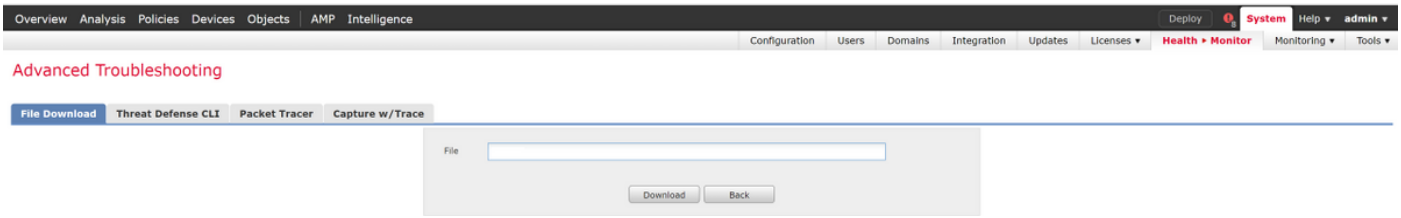
SSL Errors potentially causing drop

注：Firepowerが復号化を開始した後に復号化にエラーが発生した場合、ファイアウォールがすでにセッションを変更/man-in-the-middredしているため、トラフィックを廃棄する必要

があります。そのため、クライアントとサーバは異なるTCPスタックと異なる暗号キーをを使用します。

この記事の指示に従って、>プロンプトからFirepowerデバイスのデバッグファイルをコピーできます。

または、Firepowerバージョン6.2.0以降のFMCにオプションがあります。FMCでこのUIユーティリティにアクセスするには、[Devices] > [Device Management]に移動します。次に、 アイコンをクリックし、その後に[Advanced Troubleshooting] > [File Download]をクリックします。その後、該当するファイルの名前を入力し、[Download]をクリックします。

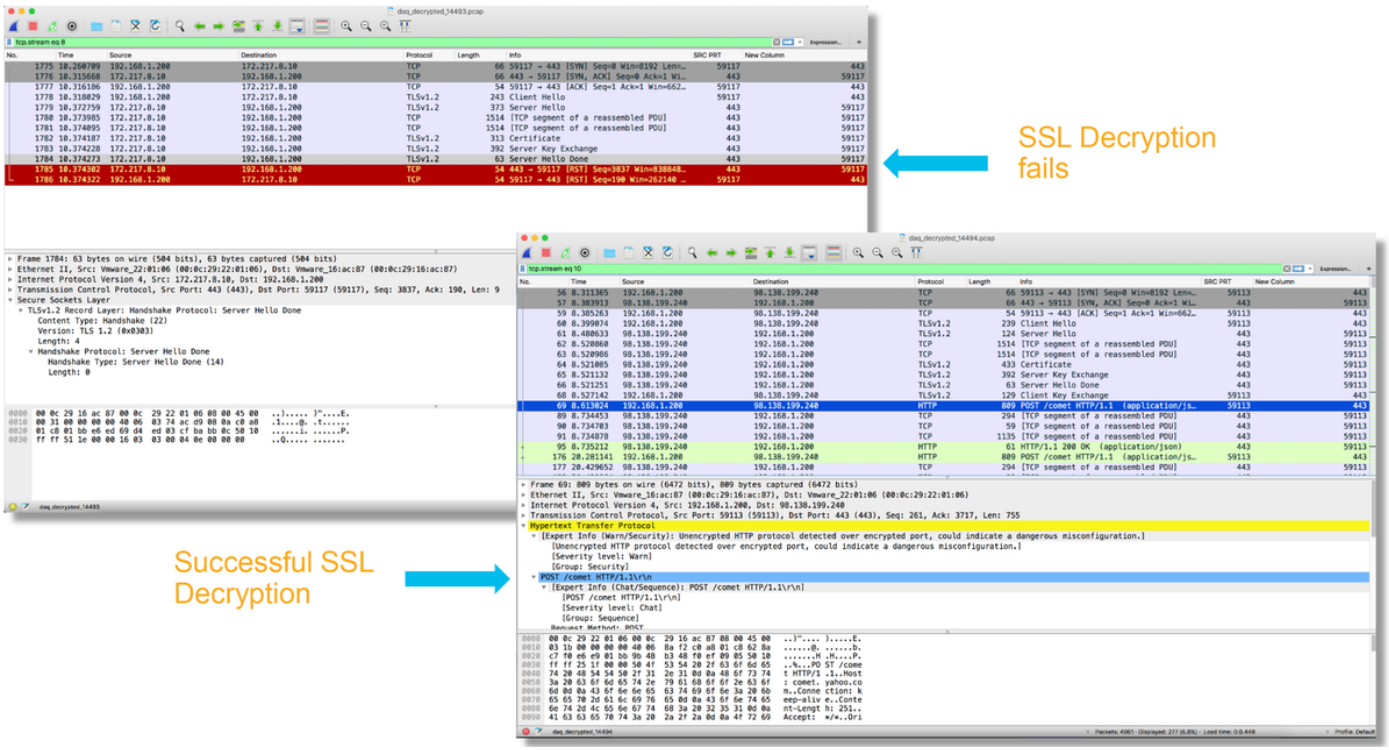


復号化されたパケットキャプチャの生成

Firepowerによって復号化されるセッションの暗号化されていないパケットキャプチャを収集できます。コマンドはsystem support debug-DAQ debug_daq_write_pcapです

注意：Snortプロセスは、復号化されたパケットキャプチャを生成する前に再起動する必要があります。これにより、いくつかのパケットが廃棄される可能性があります。TCPトラフィックなどのステートフルプロトコルは再送信されますが、UDPなどの他のトラフィックは悪影響を受ける可能性があります。

```
> 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_*
```

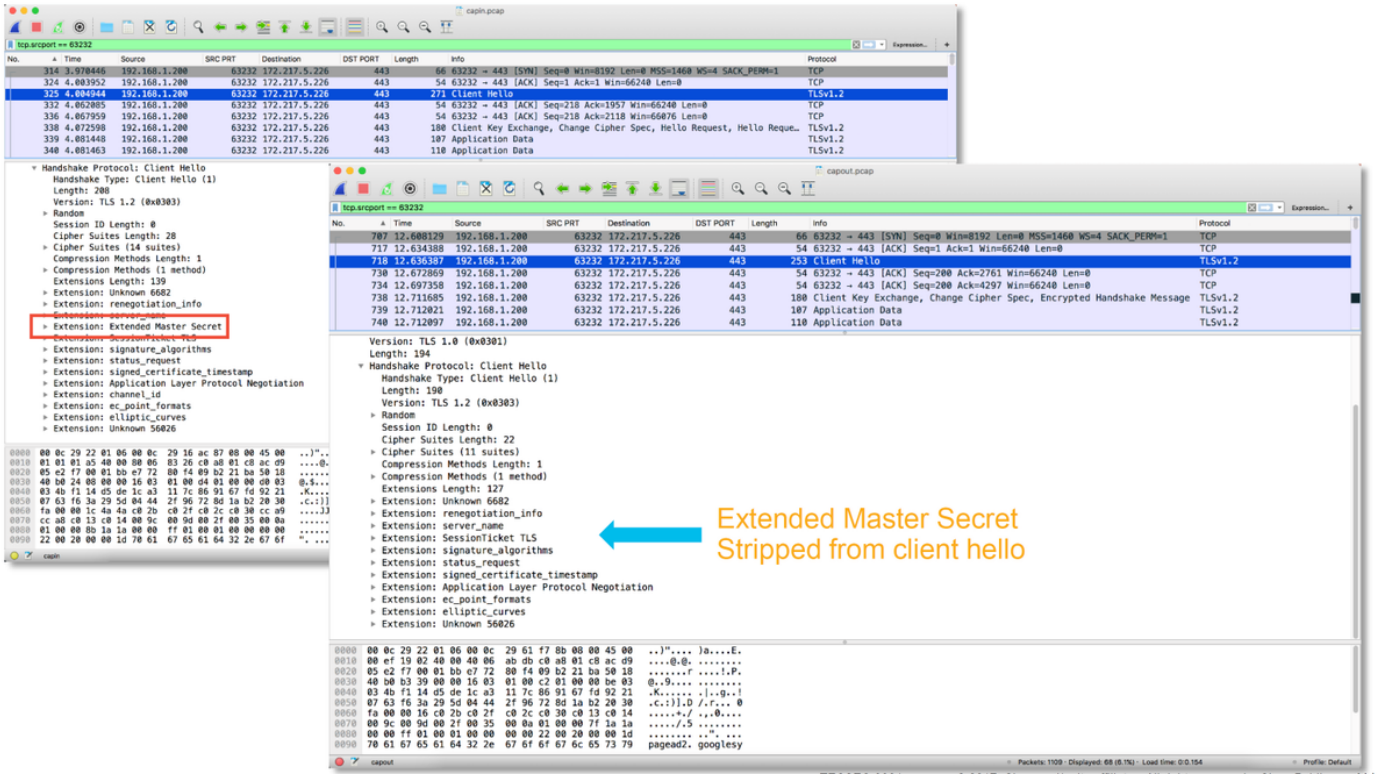


注意：復号化されたPCAPキャプチャをTACに送信する前に、問題のあるフローにキャプチャファイルを除外し、制限することを推奨します。これにより、機密データが不必要に漏洩することを回避できます。

クライアントのHelloの変更(CHMod)を探します

また、パケットキャプチャを評価して、クライアントのhello変更が行われているかどうかを確認することもできます。

左側のパケットキャプチャは、元のクライアントhelloを示しています。右側の1つは、サーバ側のパケットを示しています。拡張マスターシークレットがFirepowerのCHMod機能によって削除されていることに注意してください。



クライアントがCAの再署名を信頼して復号化/再署名を行うことを確認する

アクションが「Decrypt - Resign」のSSLポリシールールの場合、クライアントホストが再署名CAとして使用される認証局(CA)を信頼していることを確認します。エンドユーザは、ファイアウォールによってman-in-the-middredであることを示す必要はありません。署名CAを信頼する必要があります。これはActive Directory(AD)グループポリシーを通じて最も一般的に適用されますが、会社のポリシーとADインフラストラクチャによって異なります。

詳細については、次の記事を参照してください。この記事では、SSLポリシーの作成方法について説明しています。

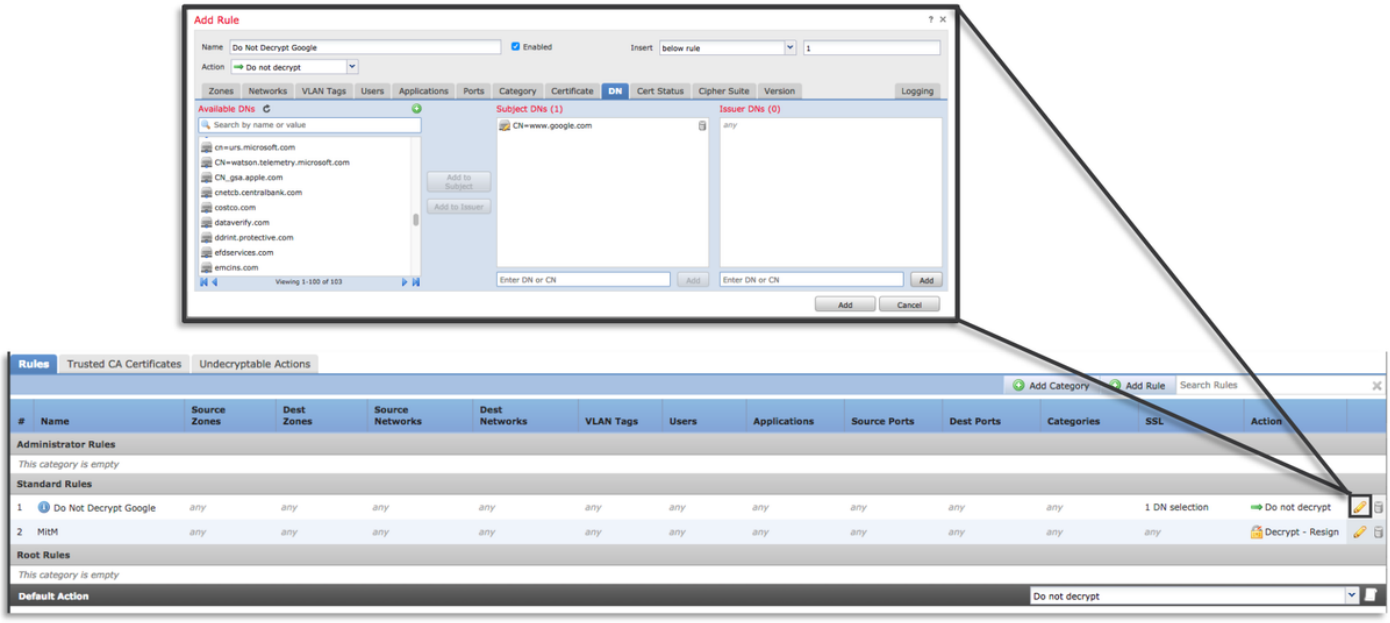
緩和手順

いくつかの基本的な緩和手順に従って、次のことを実行できます。

- 特定のトラフィックを復号化しないようにSSLポリシーを再設定する
- クライアントのhelloパケットから特定のデータを削除し、復号化が成功するようにします

Do Not Decrypt(DnD)ルールの追加

次のシナリオ例では、SSLポリシーインスペクションを通過する際にgoogle.comへのトラフィックが切断されていることが確認されています。サーバ証明書の共通名(CN)に基づいて、google.comへのトラフィックが復号化されないようにルールが追加されます。



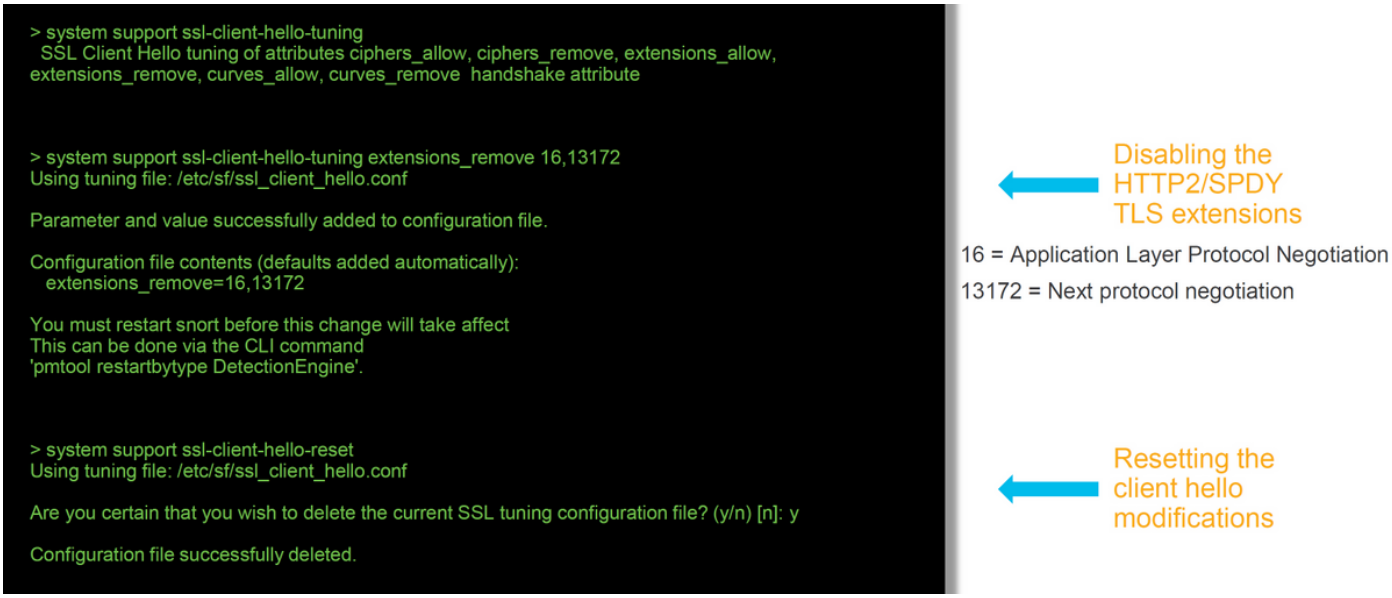
ポリシーを保存して展開した後、前述のトラブルシューティング手順に従って、Firepowerがトラフィックで何を行っているかを確認できます。

クライアントのHello変更の調整

場合によっては、トラブルシューティングによって、Firepowerで特定のトラフィックの復号化に関する問題が発生していることが明らかになることがあります。**system support ssl-client-hello-tuningユーティリティをCLIで実行する**と、Firepowerがクライアントのhelloパケットから特定のデータを削除できます。

次の例では、特定のTLS拡張が削除されるように設定が追加されています。数値IDは、TLSの拡張と標準に関する情報を検索することによって見つけることができます。

> **注意**：Snortプロセスは、クライアントのhello変更が有効になる前に再起動する必要があります。これにより、いくつかのパケットがドロップされる可能性があります。TCPトラフィックなどのステートフルプロトコルは再送信されますが、UDPなどの他のトラフィックは悪影響を受ける可能性があります。



クライアントのhello変更設定に対する変更を元に戻すには、**system support ssl-client-hello-resetコマンドを実**装できます。

TACに提供するデータ

Data
Firepower Management Center(FMC)およびFirepowerデバイスからのファイルのトラブルシューティン
SSLデバッグ
フルセッションパケットキャプチャ（可能であれば、クライアント側、Firepowerデバイス自体、および
接続イベントのスクリーンショットまたはレポート

次のステップ

SSLポリシーコンポーネントが問題の原因ではないと判断された場合は、次のステップとしてアクティブ認証機能のトラブルシューティングを行います。

次の記事に進むには、ここをクリックしてください。