Firepower Data Path Troubleshooting Phase 5: SSL Policy

Contents

Introduction

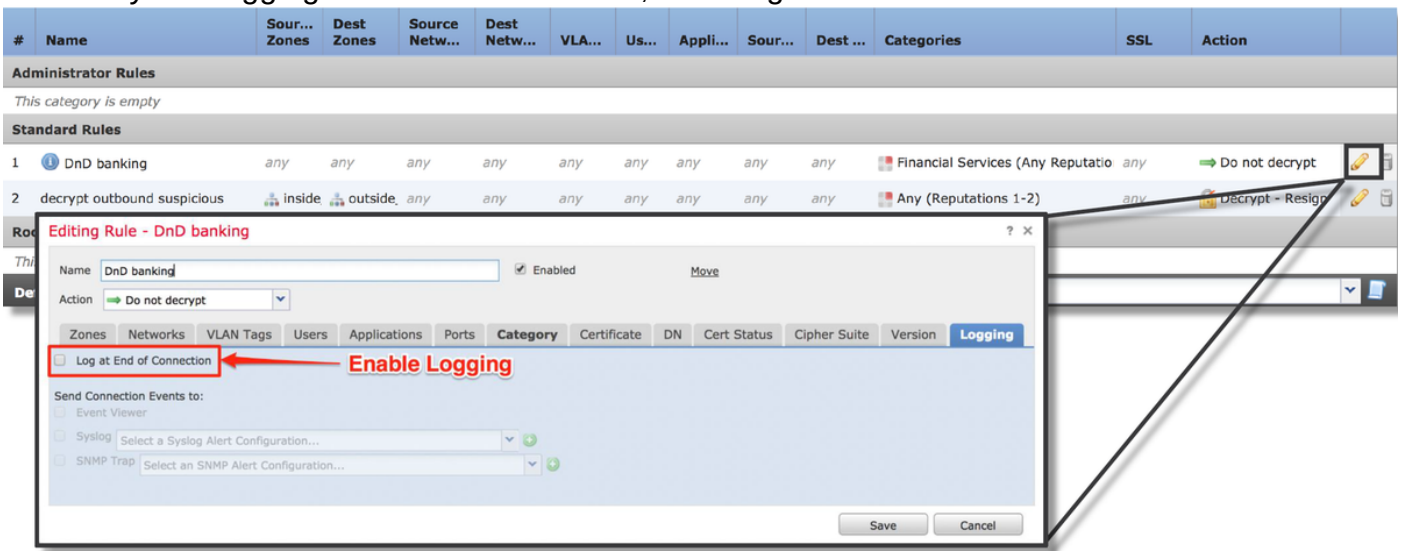
This article is part of a series of articles which explain how to systematically troubleshoot the data path on Firepower systems to determine whether components of Firepower may be affecting traffic. Please refer to the Overview article for information about the architecture of Firepower platforms and links to the other Data Path Troubleshooting articles.

This article covers the fifth stage of the Firepower data path troubleshooting, the Secure Sockets Layer (SSL) Policy feature.

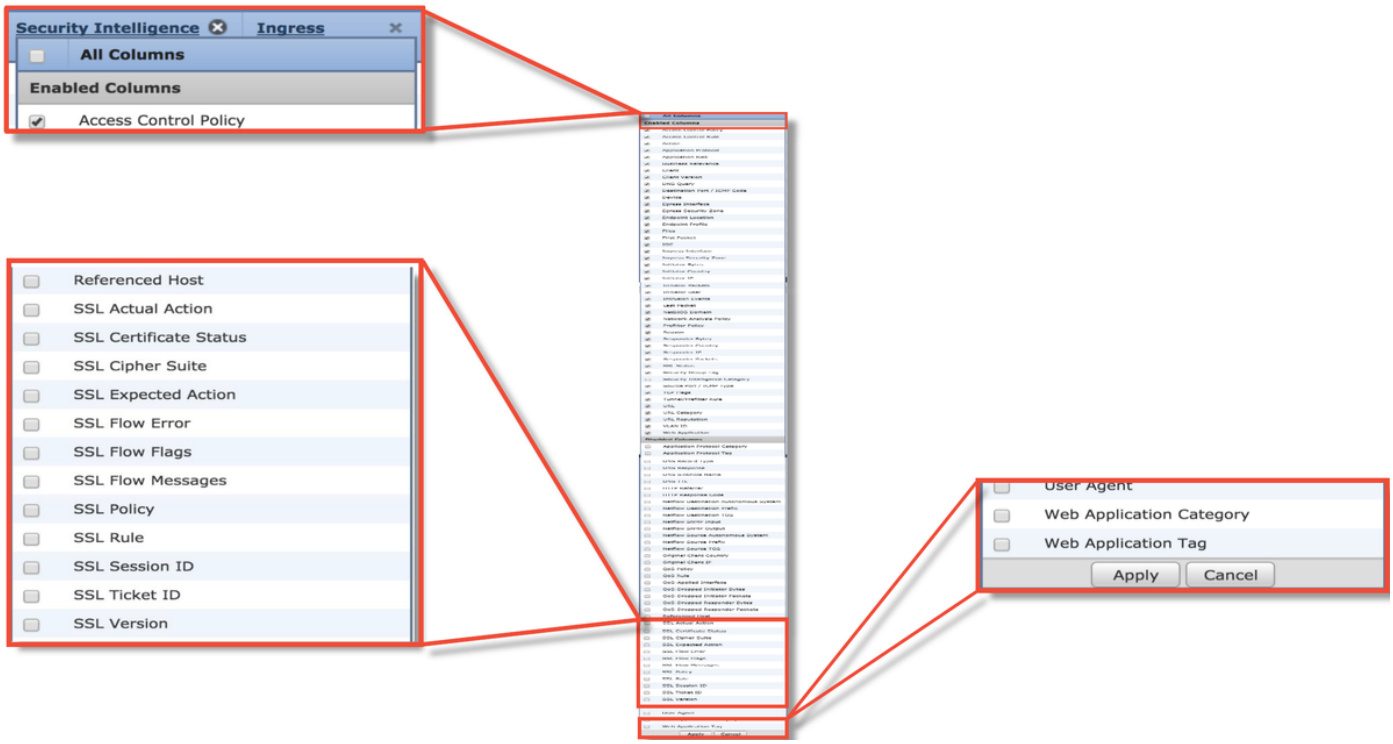
Prerequisites

- The information in this article applies to any Firepower platform SSL decryption for the Adaptive Security Appliance (ASA) with FirePOWER services (SFR module) only available in 6.0+Client Hello Modification feature is only available in 6.1+
- Confirm that SSL Policy is being used in the Access Control Policy

- Verify that logging is enabled for all rules, including the 'Default Action'



- Check the Undecryptable Actions tab to see if any option is set to block traffic
- In the Connection events, when you are in the table view of connection events, enable all of the fields with 'SSL' in the name
  Most are disabled by default and need to be enabled in the Connection Events viewer



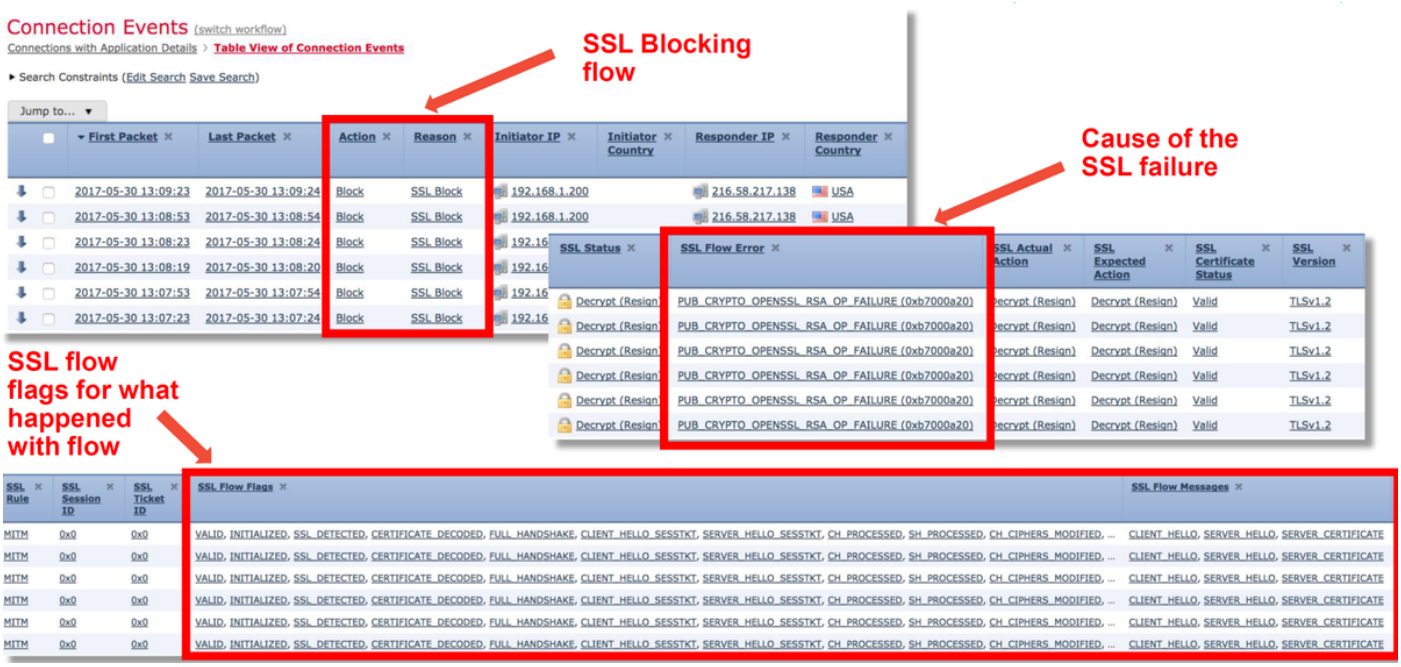
Troubleshooting the SSL Policy Phase

Specific steps can be followed to help understand why SSL Policy may be dropping traffic that is expected to be allowed.

Check SSL Fields in the Connection Events

If the SSL Policy is suspected of causing traffic issues, the first place to check is the Connection Events section (under **Analysis > Connections > Events**) after enabling all the SSL fields, as outlined above.

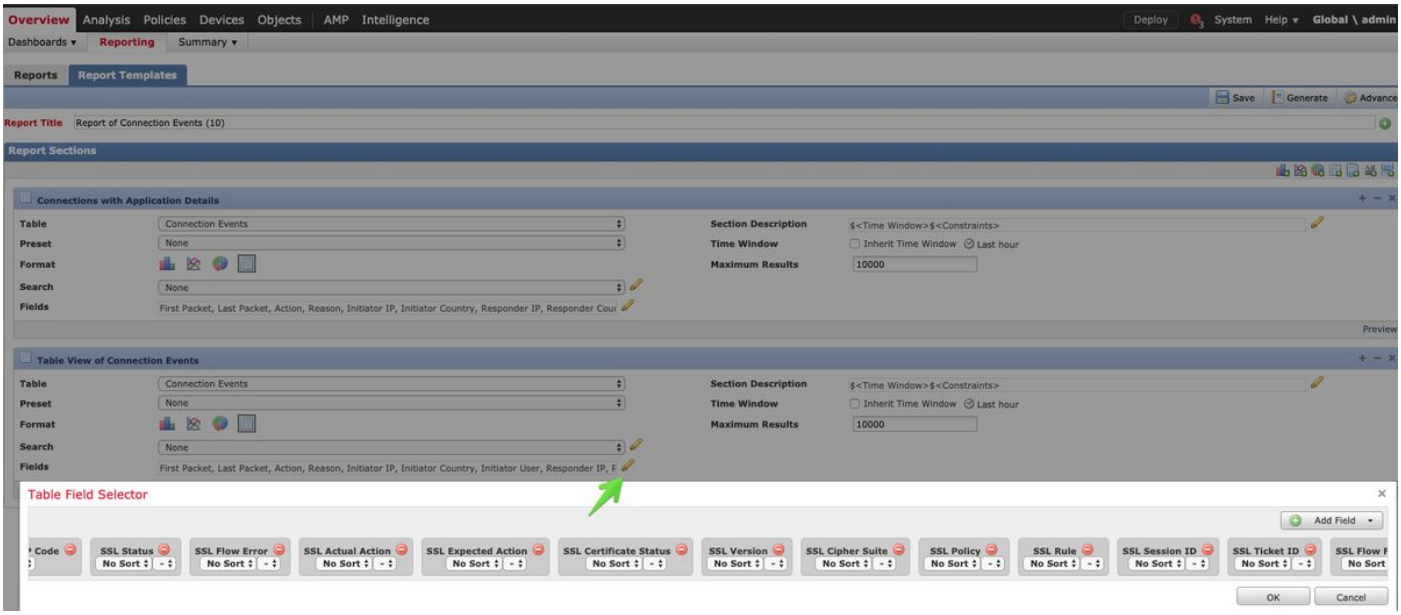
If SSL Policy is blocking traffic, the **Reason** field displays "SSL Block". The **SSL Flow Error** column has useful information about why the block occurred. The other SSL fields have information about SSL data that Firepower detected in the flow.



This data can be provided to the Cisco Technical Assistance Center (TAC) when opening a case for SSL Policy. In order to easily export this information, **Report Designer** button at the top right corner can be used.

If this button is clicked from the Connection Events section, the filters and time window options are copied to the report template automatically.

Make sure all mentioned SSL Fields are added at the 'Field' section.



Click on **Generate** to create a Report on PDF or CSV formats.

Debug the SSL Policy

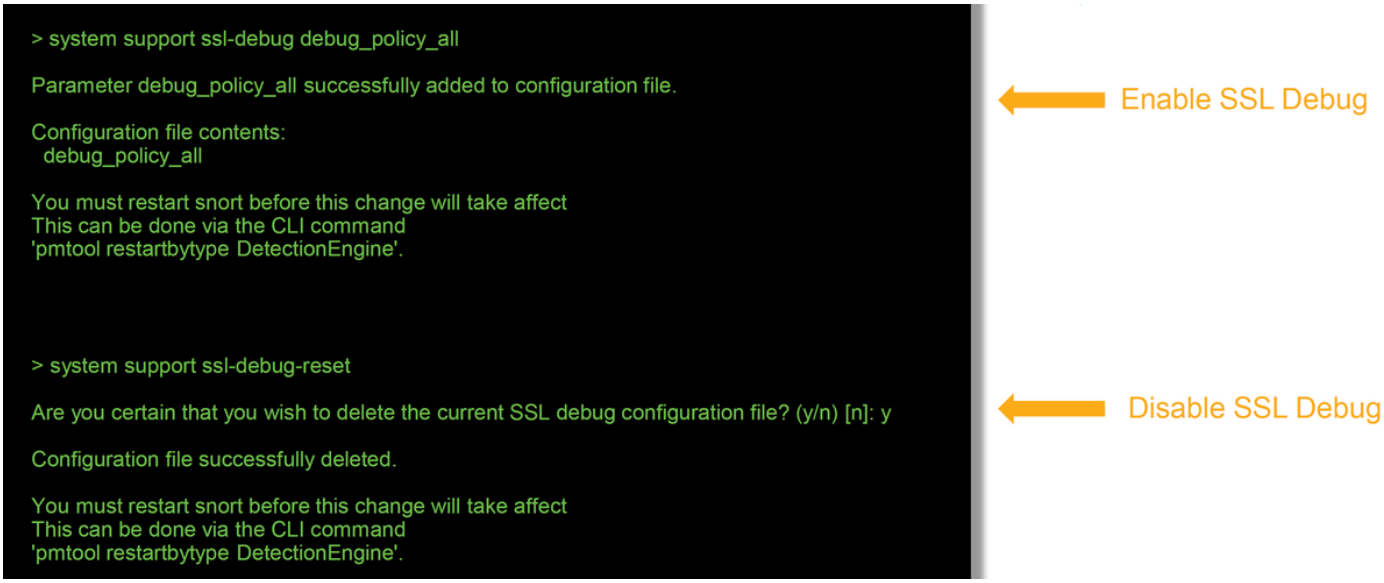
If the Connection Events do not contain enough information about the flow, SSL debugging can be run on the Firepower Command Line Interface (CLI).

> **Note**: All of the debug content below is based on the SSL decryption that happens in software on the x86 architecture. This content does not include debugs from SSL hardware offload features that were added in version 6.2.3 and on, which are different.

> **Note**: On the Firepower 9300 and 4100 platforms, the shell in question can be accessed via the following commands:
>
> # **connect module 1 console**
> Firepower-module1> **connect ftd**
> >
>
> For multi-instances, the logical device CLI can be accessed with the following commands.
> **# connect module 1 telnet**
> Firepower-module1> **connect ftd ftd1**
> Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
> >

The **system support ssl-debug debug_policy_all** command can be run to generate debugging information for every flow processed by the SSL Policy.

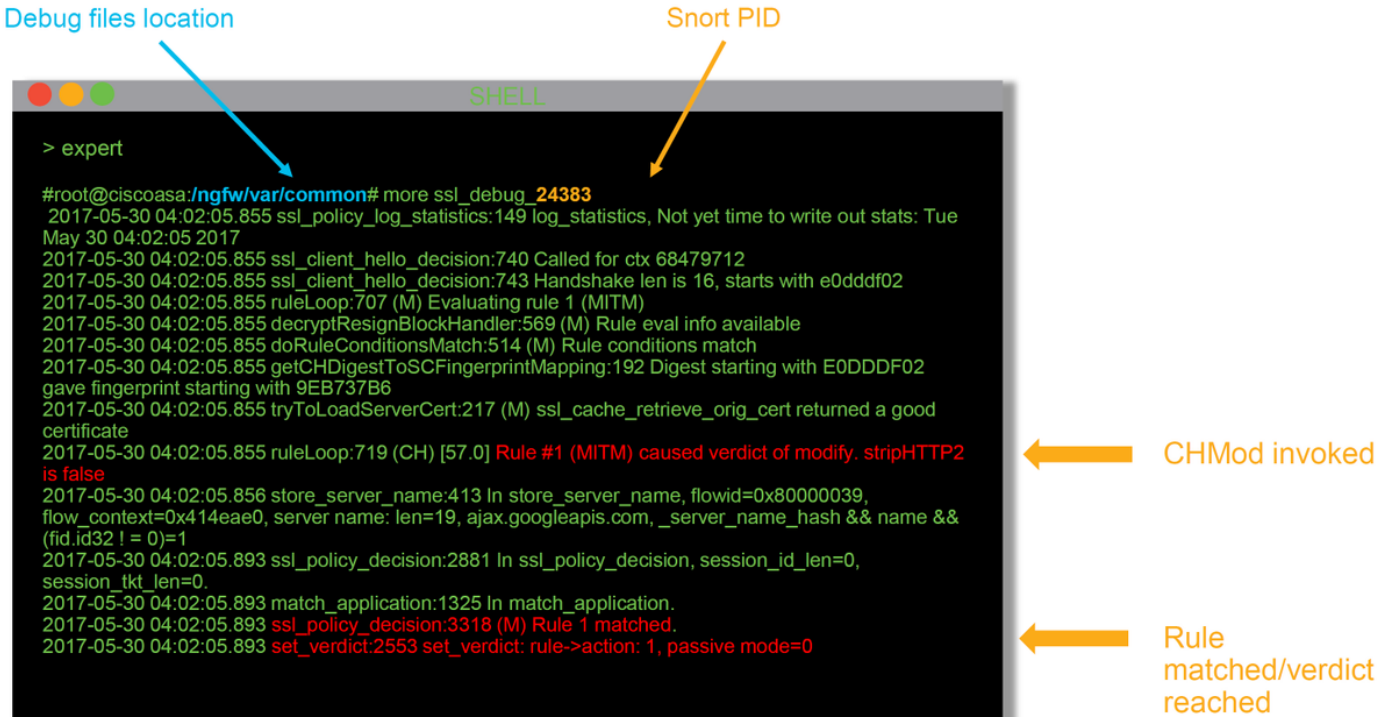
> **Caution**: The snort process must be restarted before and after running the SSL debug, which can cause a few packets to be dropped depending on the snort-down policies and deployment used. TCP traffic will be retransmitted, but UDP traffic can be negatively affected if the applications passing through the firewall don't tolerate minimum packet loss.



> **Warning**: Do not forget to turn off debugging after the necessary data is collected with the **system suport ssl-debug-reset** command.

There will be a file written for each snort process running on the Firepower device. The location of the files will be:

- **/var/common** for non-FTD platforms
- **/ngfw/var/common** for FTD platforms



These are some of the helpful fields in the debug logs.

```
...
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;
...
```

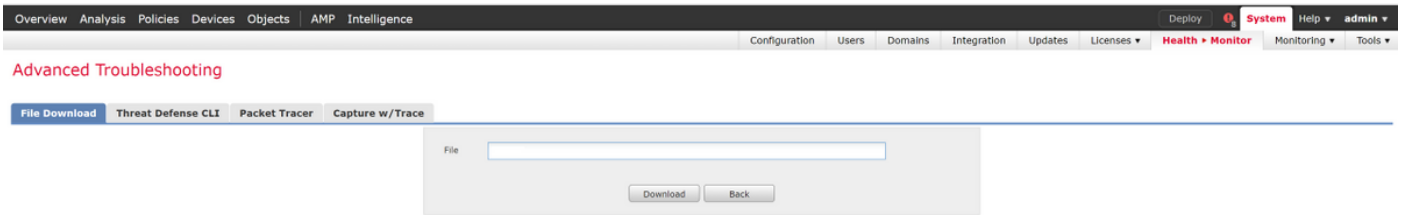
SSL Errors potentially causing drop

Note: If there is an error with decryption which occurs after Firepower begins decrypting, the traffic must be dropped since the firewall have already modified/man-in-the-middled the

session, so it is not possible for the client and server to resume communication as they have different TCP stacks as well as different encryption keys used in the flow.

The debug files can be copied off of the Firepower device from the > prompt using the directions in this article.

Alternatively, there is an option on the FMC in Firepower version 6.2.0 and greater. To access this UI utility on the FMC, navigate to **Devices > Device Management**. Then, click on the icon next to the device in question, followed by **Advanced Troubleshooting > File Download**. You can then enter the name of a file in question and click Download.

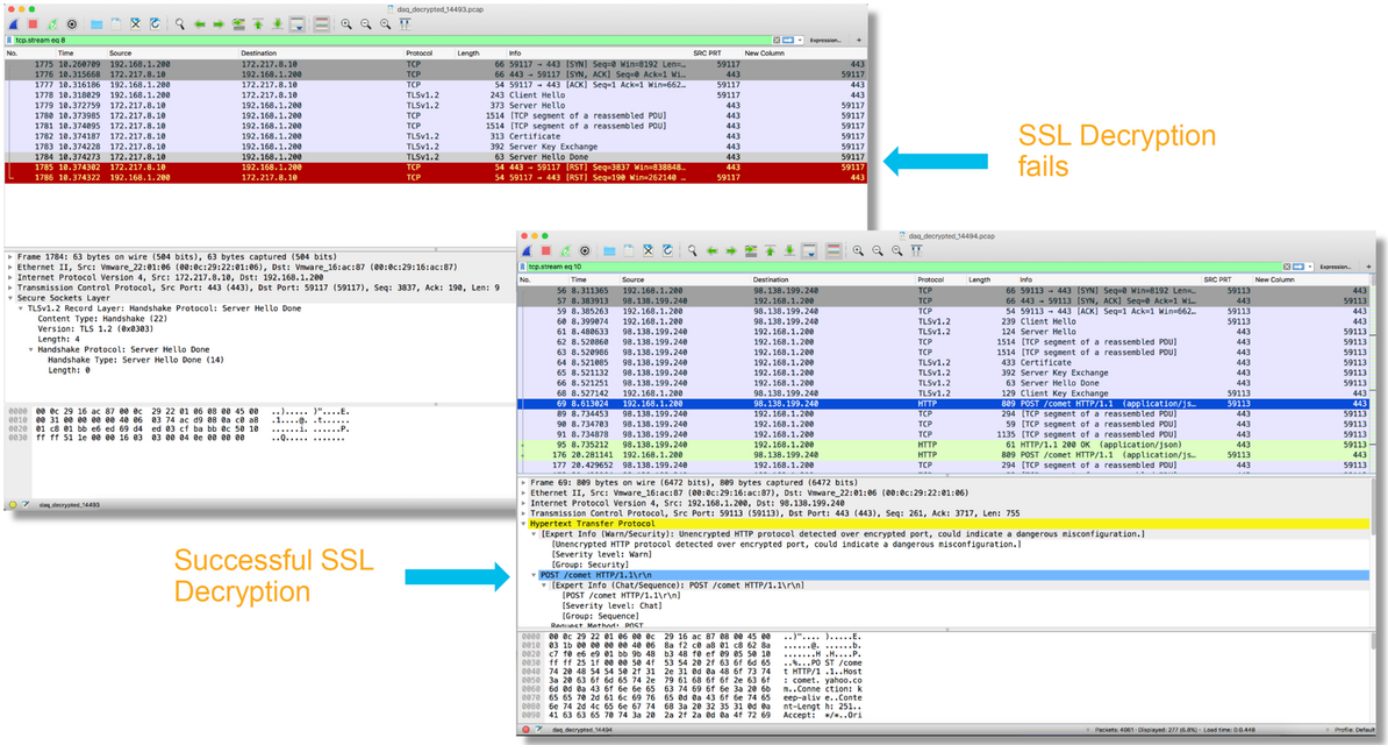


Generate a Decrypted Packet Capture

It is possible to collect an unencrypted packet capture for the sessions which get decrypted by Firepower. The command is **system support debug-DAQ debug_daq_write_pcap**

> **Caution**: The snort process must be restarted before generating the decrypted packet capture, which can cause a few packets to be dropped. Stateful protocols such as TCP traffic are retransmitted, but other traffic, such as UDP, can be negatively affected.

```
> 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_*
```

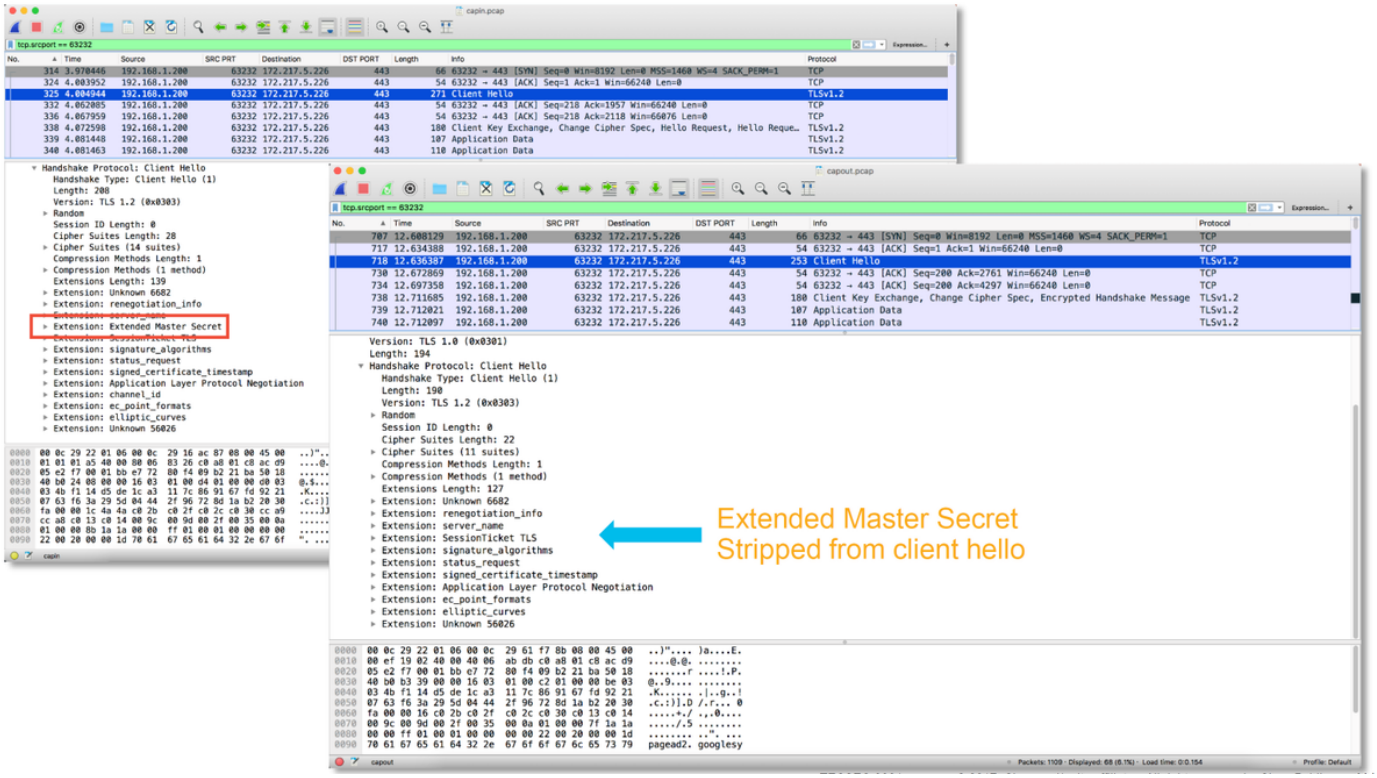


Caution: Before submitting a decrypted PCAP capture to TAC, it is recommended to filter out and limit the capture file to the problematic flows, as to avoid revealing any sensitive data unnecessarily.

Look for Client Hello Modifications (CHMod)

The packet capture can also be evaluated to see if any client hello modification is taking place.

The packet capture on the left depicts the original client hello. The one on the right shows that server-side packets. Notice that the extended master secret has been removed via the CHMod feature in Firepower.



Make Sure Client Trusts Resigning CA For Decrypt/Resign

For SSL Policy rules with an action of "Decrypt - Resign", make sure that the client hosts trust the Certificate Authority (CA) used as the resigning CA. The end users should have no indication that they are being man-in-the-middled by the firewall. They should trust the signing CA. This is most commonly enforced through Active Directory (AD) Group Policy but it depends on the company policy and AD Infrastructure.

For more information, you can review the following article, which outlines how to create an SSL Policy.

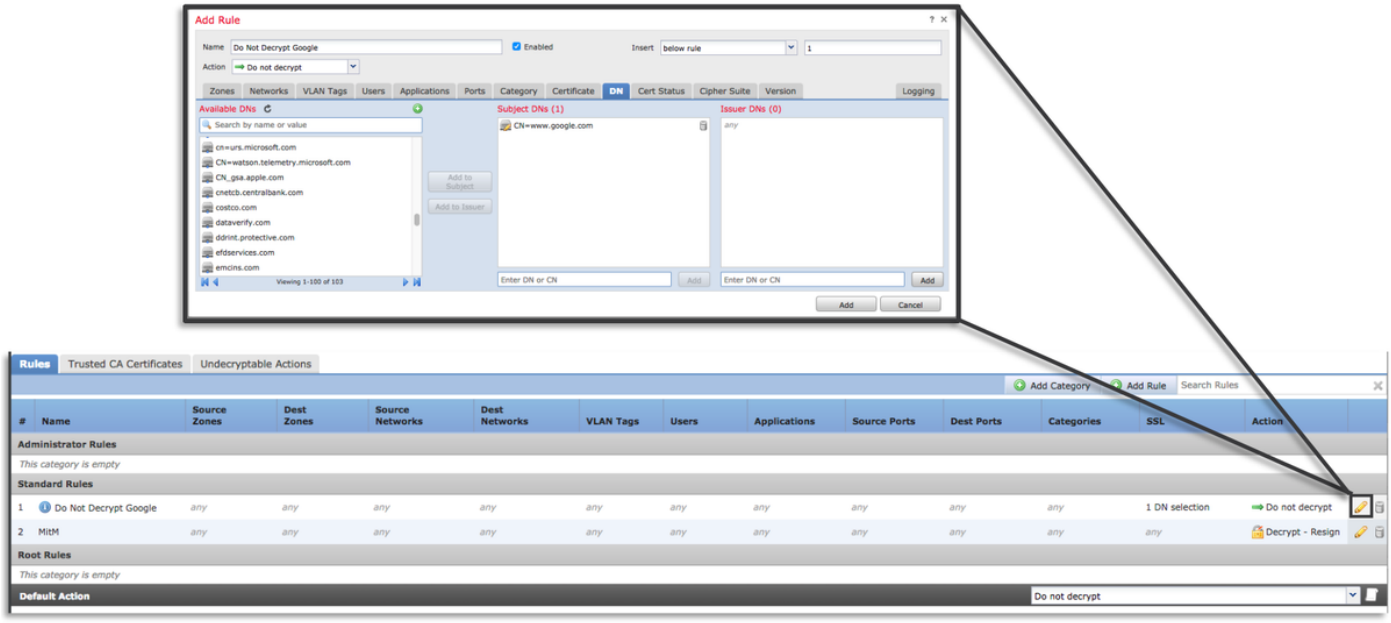
Mitigation Steps

Some basic mitigation steps can be followed in order to:

- Re-configure the SSL Policy to not decrypt certain traffic
- Strip certain data out of a client hello packet so that decryption will succeed

Add Do Not Decrypt (DnD) Rules

In the following example scenario, it has been determined that traffic to google.com is breaking when passing through SSL Policy inspection. A rule is added, based off of the Common Name (CN) in the server certificate so that traffic to google.com is not decrypted.



After saving and deploying the policy, the troubleshooting steps outlined above can be followed again to see what Firepower is doing with the traffic.

Client Hello Modification Tuning

In some cases, troubleshooting can reveal that Firepower is running into an issue with decrypting certain traffic. The **system support ssl-client-hello-tuning** utility can be run on the CLI to cause Firepower to remove certain data from a client hello packet.

In the example below, a configuration is added so that certain TLS extensions are removed. The numerical ID's are found by searching for information on TLS extensions and standards.

> **Caution**: The snort process must be restarted before the client hello modification changes take effect, which can cause a few packets to be dropped. Stateful protocols such as TCP traffic are retransmitted, but other traffic, such as UDP, can be negatively affected.

```
> 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

In order to revert any changes made to the client hello modification settings, the **system support ssl-client-hello-reset** command can be implemented.

Data to Provide to TAC

Data	Instructions
Troubleshoot files from the Firepower Management Center (FMC) and Firepower devices	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
SSL Debugs	See this article for instructions
Full session packet captures (from the client side, Firepower device itself and server side when possible)	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-applia
Connection Event screenshots or reports	See this article for instructions

Next Step

If it has been determined that the SSL Policy component is not the cause of the issue, the next step would be to troubleshoot the Active Authentication feature.

Click here to proceed with the next article.