

تانايب راسم عاڤخأ فاشكتسأ نم 5 ةلحرمل SSL جهن :اهالصل او Firepower

تايتو حمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[اهالصل او SSL جهن ةلحرمل عاڤخأ فاشكتسأ](#)

[لاصلتالا ثادحأ يف SSL لوقح نم ققحتلا](#)

[SSL جهن حيحصت](#)

[اهرفشت ك ف مت ةمزح طاقتلا عاشنا](#)

[\(CHMod\) ليمعلا بيحرت تاليدعت نع ثحبلا](#)

[ةلاقستسالا/ري فشتلا كفل ليقستسمل اقدصملا عجرملا يف قثي ليمعلا نأ نم دكأت](#)

[في فختلا تاوڤخ](#)

[\(DNd\) ريفشتلا ك ف مدع دعاوق ةفاضا](#)

[ليمعلا HELLO ليدعت طبض](#)

[TAC ىلا اهميدقت متيس يتلا تانايبلا](#)

[ةيلتلا ةوڤخلا](#)

ةمدقملا

يف تانايب راسم فاشكتسأ ةيفيك حضوت تالاقم ةلسلس نم عزج يه ةلاقملا هذه رثؤت دق FirePOWER تانوكم تناك اذإ ام ديدحتل يجهنم لكشب اهالصل او FirePOWER ةمظنأ ةينب لوح تامولعم ىلع لوصحلل "ةماع قرظن" ةلاقم ىلا عوجرلا يجرى. رورملا ةكرح ىلع تانايبلا تاراسم عاڤخأ فاشكتسأ" تالاقم ب اهتاطابترا و FirePOWER ةيساسألا ةمظنألا ىرخألا "اهالصل او

FirePOWER تانايب راسم عاڤخأ فاشكتسأ نم ةسماخل ةلحرمل ةلاقملا هذه يظغت (SSL) ةنمألا لىصوتلا ذخأم ةقبط جهن ةزيم يه و، اهالصل او



ةيساسألا تابلطتملا

- SSL ريفشت ك ف Firepower ةصنم يأ ىلع ةلاقملا هذه يف ةدراولا تامولعمل قبطنت يف طقف رفوتم (SFR ةدحو) FirePOWER تامدخ عم (ASA) فيكتلل لباقل نامألا زاوجل 6.1+ يف ال "ليمعلا بيحرت ليدعت" ةزيم رفوتت ال 6.0+ رادصلإا
- لوصولا يف مكحتلا جهن يف SSL جهن مادختس اديكأت

test

Enter Description

Prefilter Policy: [Default Prefilter Policy](#)

SSL Policy: [TEST_SSL_POLICY](#)

General Settings

| | |
|---|------|
| Maximum URL characters to store in connection events | 1024 |
| Allow an Interactive Block to bypass blocking for (seconds) | 600 |
| Retry URL cache miss lookup | Yes |
| Enable Threat Intelligence Director | Yes |
| Inspect traffic during policy apply | Yes |

Identity Policy Settings

| | |
|-----------------|------|
| Identity Policy | None |
|-----------------|------|

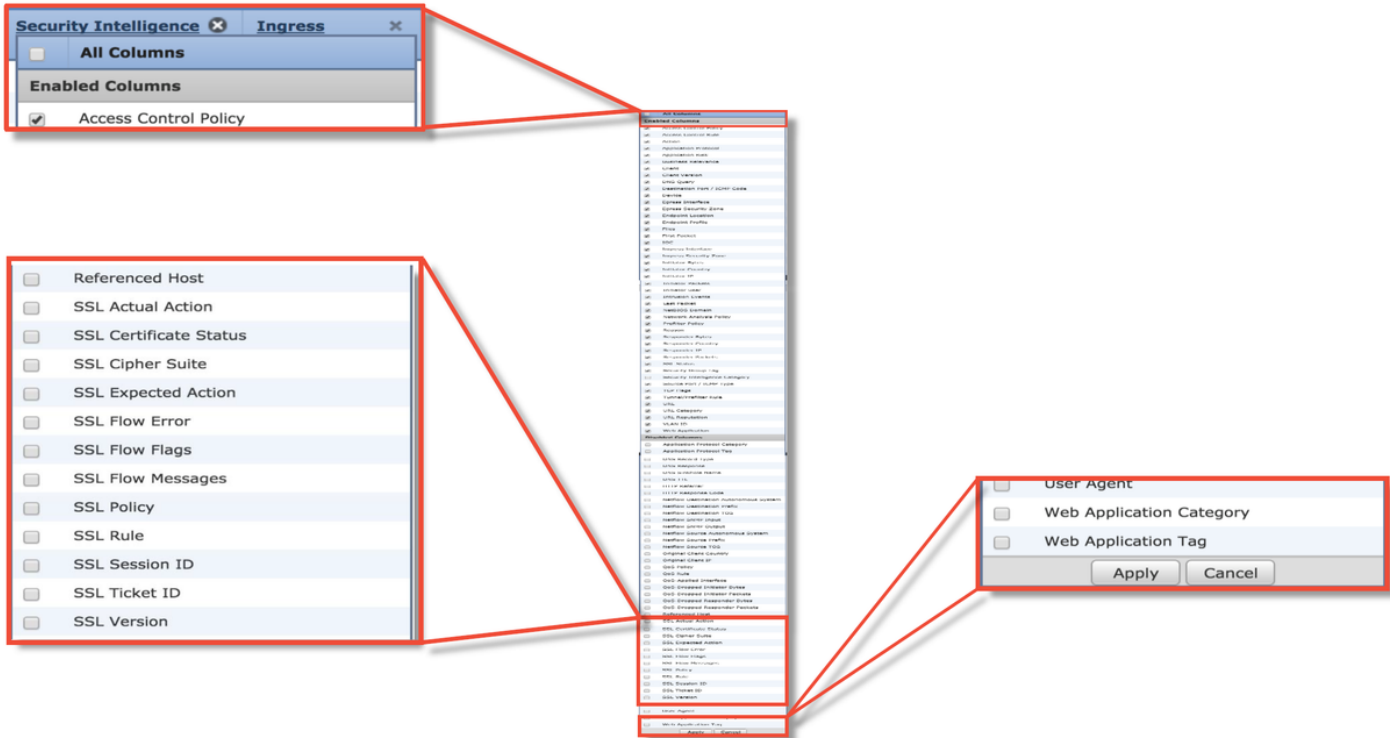
SSL Policy Settings

| | |
|--|---------------------------------|
| SSL Policy to use for inspecting encrypted connections | TEST_SSL_POLICY |
|--|---------------------------------|

• "يضا رت ف ال ا ع ا ر ج ال" ك ل ذ ي ف ا م ب ، د ع ا و ق ل ا ع ي م ج ل ل ي ج س ت ل ا ن ي ك م ت ن م ق ق ح ت

The screenshot shows the 'Editing Rule - DnD banking' dialog box. The 'Log at End of Connection' checkbox is checked and highlighted with a red arrow and the text 'Enable Logging'. The rule name is 'DnD banking', it is enabled, and the action is 'Do not decrypt'. The 'Logging' tab is selected, showing options for sending connection events to the Event Viewer, Syslog, and SNMP Trap.

- ر ط ح ل ر ا ي خ ي ا ن ي ي ع ت م ت ا ذ ا م ا ف ر ع م ل ر ي ف ش ت ل ا ع ا ر ج ا ب ي و ب ت ل ا م ا ل ع ن م ق ق ح ت ر و ر م ل ا ك ر ح
- ن ي ك م ت ب م ق ، ل ا ص ت ا ل ا ث ا د ح ا ل ل و د ج ل ا ض ر ع ق ي ر ط ي ف ن و ك ت ا م د ن ع ، ل ا ص ت ا ل ا ث ا د ح ا ي ف م س ا ل ا ي ف 'SSL' ت ا ذ ل و ق ح ل ا ف ا ك ث ا د ح ا ض ر ا ع ي ف ا ه ن ي ك م ت ب ج ي و ي ض ا ر ت ف ا ل ك ش ب ت ا م د خ ل ا ه ذ ه م ط ع م ل ي ط ع ت م ت ي ل ا ص ت ا ل ا



اهال الصا و SSL جهن ةل حرم ءاطخا فاشكتسا

ةكرح طاقسا ب SSL ةسايس موقت دق اذامل مهف يف ةدعاس ملل ةددم تاوطخ ءاب تا نكمي اءب ءامسلا ءقوتملا رورملا

لاصتالا ءاءءا يف SSL لوقء نم ققءءالا

لوالا ناكملا نإف ،رورملا ةكرء يف لكاشم يف ببستت SSL ةسايس نا يف هبءشې ناك اءا نيكمت دءب (ءاءءالا > ءالا صءالا > لئلءءالا ءءء) لاصءالا ءاءءا مسق وه هصءف بءي يءلا هالءا ءضوم وه امك ، SSL لوقء ءيمء

قفءءا ءطء دومع يوءءي . " SSL ةلءء " ببسلا لقق ضرءي ،رورملا ةكرء ءنمي SSL ءهن ناك اءا لوقء ءامولءم ىلء ىرءالا SSL لوقء يوءءء . ةلءءالا ءوءء ببس لوقء ةءيم ءامولءم ىلء SSL قفءءالا يف FirePOWER اهفءءءا يءلا SSL ءانايب

Connection Events (switch workflow)
 Connections with Application Details > **Table View of Connection Events**
 Search Constraints (Edit Search Save Search)

Jump to...

| First Packet | Last Packet | Action | Reason | Initiator IP | Initiator Country | Responder IP | Responder Country |
|---------------------|---------------------|--------|-----------|---------------|-------------------|----------------|-------------------|
| 2017-05-30 13:09:23 | 2017-05-30 13:09:24 | Block | SSL Block | 192.168.1.200 | | 216.58.217.138 | USA |
| 2017-05-30 13:08:53 | 2017-05-30 13:08:54 | Block | SSL Block | 192.168.1.200 | | 216.58.217.138 | USA |
| 2017-05-30 13:08:23 | 2017-05-30 13:08:24 | Block | SSL Block | 192.168.1.200 | | 216.58.217.138 | USA |
| 2017-05-30 13:08:19 | 2017-05-30 13:08:20 | Block | SSL Block | 192.168.1.200 | | 216.58.217.138 | USA |
| 2017-05-30 13:07:53 | 2017-05-30 13:07:54 | Block | SSL Block | 192.168.1.200 | | 216.58.217.138 | USA |
| 2017-05-30 13:07:23 | 2017-05-30 13:07:24 | Block | SSL Block | 192.168.1.200 | | 216.58.217.138 | USA |

SSL Blocking flow

Cause of the SSL failure

| SSL Status | SSL Flow Error | SSL Actual Action | SSL Expected Action | SSL Certificate Status | SSL Version |
|------------------|--|-------------------|---------------------|------------------------|-------------|
| Decrypt (Resign) | PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20) | Decrypt (Resign) | Decrypt (Resign) | Valid | TLSv1.2 |
| Decrypt (Resign) | PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20) | Decrypt (Resign) | Decrypt (Resign) | Valid | TLSv1.2 |
| Decrypt (Resign) | PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20) | Decrypt (Resign) | Decrypt (Resign) | Valid | TLSv1.2 |
| Decrypt (Resign) | PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20) | Decrypt (Resign) | Decrypt (Resign) | Valid | TLSv1.2 |
| Decrypt (Resign) | PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20) | Decrypt (Resign) | Decrypt (Resign) | Valid | TLSv1.2 |
| Decrypt (Resign) | PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20) | Decrypt (Resign) | Decrypt (Resign) | Valid | TLSv1.2 |

SSL flow flags for what happened with flow

| SSL Rule | SSL Session ID | SSL Ticket ID | SSL Flow Flags | SSL Flow Messages |
|----------|----------------|---------------|---|--|
| MITM | 0x0 | 0x0 | VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ... | CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE |
| MITM | 0x0 | 0x0 | VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ... | CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE |
| MITM | 0x0 | 0x0 | VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ... | CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE |
| MITM | 0x0 | 0x0 | VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ... | CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE |
| MITM | 0x0 | 0x0 | VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ... | CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE |
| MITM | 0x0 | 0x0 | VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ... | CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE |

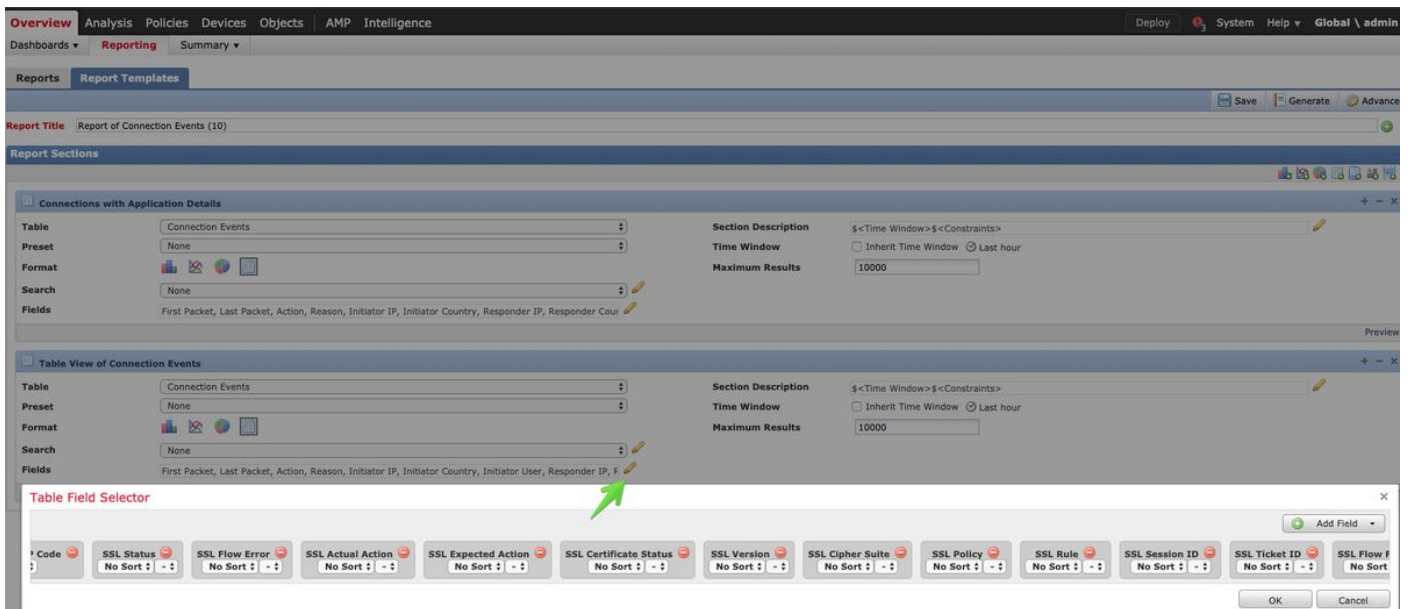
ةلاح حتف دنع Cisco نم (TAC) ةينقتلا ةدعاسملا زكرم ىلإ تانايبل هذه ريفوت نكمي ريرقتلا ممصم رزمادختسا نكمي، ةلوه سب تامولعمل هذه ريدصت لجا نم. SSL ةسايسل نم. اىل يولعل نكرلا يف دوجوملا

راطال تاراىخو تاحشرملا خسن متي، "لاصتالا ثادحأ" مسق نم رزلا اذه قوف رقنلا مت اذا اىئاقلت ريرقتلا بلاق ىلإ ينمزللا

Bookmark This Page Report Designer Dashboard View Bookmarks Search ▼

2019-06-28 09:54:40 - 2019-06-28 11:02:22 Expanding

"لقحلا" مسقلا يف ةروكذملا SSL لوقح ةفاك ةفاضلا نم دكأت



PDF وأ CSV. تاقيسنت ن ع ريرقت عاشنإل عاشنإل ع رقنا

SSL جهن حيحصت

SSL حيحصت لايغشت نكمي، قفدتال لوح ةيفاك تامولعم لىع لاصتالال اىوتحت مل اذإ Firepower (CLI) رم اوأ رطس ةهجاو لىع

يف ثدحي يذلا SSL ريفشت ك ف لىل اهاندا عااخالال حيحصت يوتحم لك دن تسى: **ةظحال** لىمحت ااعل انايم نم عااخالال حيحصت يوتحم لال اذه نمضتي ال x86 ةينب لىع چمانرب لال فلتخت يتلاو، هذعب امو 6.2.3 رادصلال يف اهتفاضل اتمت يتلا SSL ةزهجأ

قرشقلال لىل لوصول نكمي، 4100 و 9300 Firepower ساسالال ماظنلال يف: **ةظحال** لال ةينبالال رم اوأ لال لىع نم ةينعم لال

Connect 1 ةيظمنلال ةدحولال مكحت ةدحو

```
Firepower-module1> Connect ftd
>
```

ةصاخالال (CLI) رم اوأ رطس ةهجاو لىل لوصول نكمي، ةددعتمالال تاليتاملال ةبسنلاب ةينبالال رم اوأ لال مادختساب يقطنمالال زاخجالاب

Connect Module 1 telnet

```
Firepower-module1> Connect ftd ftd1
```

رطس ةهجاو لىل ةدوعلل "exit" لخدأ... ةيولالال ftd(ftd1) مكحت ةدحولال لاصتالال نالال متي ديهمتلاب ةصاخالال (CLI) رم اوأ لال

حيحصت تامولعم عاشنإل `System support ssl-debug debug_policy_all` رمألال لايغشت نكمي SSL جهن ةطساوب هتجالع ممت قفدت لك ل عااخالال

دعبو SSL عااخالال حيحصت لايغشت لبق ةجذمنلال ةيلمع لايغشت ةداعل بجي: **ريذحت** ةجذمنلال اساسلال اقفومزجالل ضعب طاقس لىل ببستى نأ نكمي امم، هلايغشت رورم ةكرح رثأت نأ نكمي نكلو، TCP رورم ةكرح لاسرل ةداعل متي س. ةمدختس مال رشنلالو دجال عم ةياملال رادج ربع رمت يتلا تاقيبطتلال حماستت مل اذإ يبللس لكشب UDP ةمزجالال نادقف نم ىندالال

```
> system support ssl-debug debug_policy_all
Parameter debug_policy_all successfully added to configuration file.
Configuration file contents:
debug_policy_all
```

← Enable SSL Debug

```
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
```

← Disable SSL Debug

```
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'.
```

ةرورضلا تانايبلا عيمجت دعب ءاطخألا حيصت لئغشت فاقئ سئت ال :رئذحت
 system support ssl-debug-reset رمألا مادختساب

نوئي س. FirePOWER زاخ ىلع لئغشتلا دئق رئخش ةئلم عم لك لبوتكم فلم كانه نوئي س
 تافلملا عوم:

- /VAR/رئغ ةئسسألا ةمظنألل عئاش/
- /NGFW/VAR/ةمظنأل كرتشم/

Debug files location

Snort PID

```
SHELL
> expert
#root@ciscoasa:/ngfw/var/common# more ssl_debug_24383
2017-05-30 04:02:05.855 ssl_policy_log_statistics:149 log_statistics, Not yet time to write out stats: Tue
May 30 04:02:05 2017
2017-05-30 04:02:05.855 ssl_client_hello_decision:740 Called for ctx 68479712
2017-05-30 04:02:05.855 ssl_client_hello_decision:743 Handshake len is 16, starts with e0dddf02
2017-05-30 04:02:05.855 ruleLoop:707 (M) Evaluating rule 1 (MITM)
2017-05-30 04:02:05.855 decryptResignBlockHandler:569 (M) Rule eval info available
2017-05-30 04:02:05.855 doRuleConditionsMatch:514 (M) Rule conditions match
2017-05-30 04:02:05.855 getCHDigestToSCFingerprintMapping:192 Digest starting with E0DDDF02
gave fingerprint starting with 9EB737B6
2017-05-30 04:02:05.855 tryToLoadServerCert:217 (M) ssl_cache_retrieve_orig_cert returned a good
certificate
2017-05-30 04:02:05.855 ruleLoop:719 (CH) [57.0] Rule #1 (MITM) caused verdict of modify. stripHTTP2
is false
2017-05-30 04:02:05.856 store_server_name:413 In store_server_name, flowid=0x80000039,
flow_context=0x414eae0, server name: len=19, ajax.googleapis.com, _server_name_hash && name &&
(fid.id32 l = 0)=1
2017-05-30 04:02:05.893 ssl_policy_decision:2881 In ssl_policy_decision, session_id_len=0,
session_tkt_len=0.
2017-05-30 04:02:05.893 match_application:1325 In match_application.
2017-05-30 04:02:05.893 ssl_policy_decision:3318 (M) Rule 1 matched.
2017-05-30 04:02:05.893 set_verdict:2553 set_verdict: rule->action: 1, passive mode=0
```

← CHMod invoked

← Rule matched/verdict reached

ءاطخألا حيصت تالئس ئف ةئفملا لوقحلل ضعب هذ.

```

...
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_HELLO,
SESSTKT,SERVER_HELLO_SESSTKT,CH_PROCESSED,SH_PROCESSED,CH_CIPHERS_MODIFIED,
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;

```

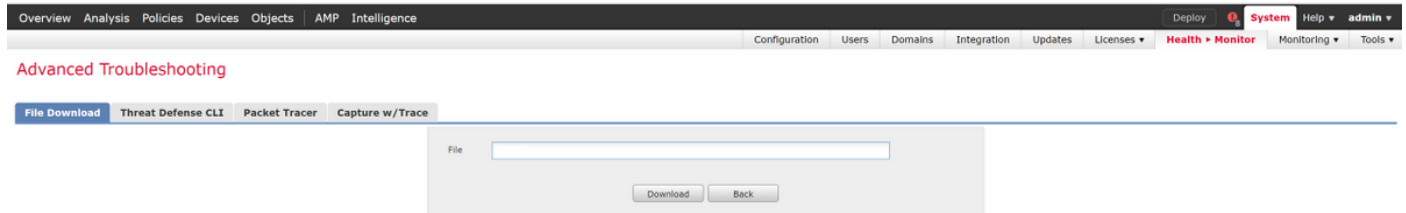
SSL Errors potentially causing drop

ري فشتلا ك ف في FirePOWER ءدب دع ب ري فشتلا ك ف في أطخ ثودح ة لاج في ف : ة طاح الم ف اقي/لي دع تب لع فلاب ماق دق ة ي امحل راج نال ارظن تانا ي بل رورم ة كرح طاقس ا ب جي

ارظن لاصتالافانئتسإمدخالاوليملل نكمي ال اذل ،دعب نع لمعلال نع لمعلال ةسلج يفةمدختسم ةفلتخم ريفشت حيتافم كلذكو مهيدل ةفلتخم TCP تاسدكم دوجول قفدتل.

تاهاجتالامادختساب > رمالاهجوم نم FirePOWER زاهج نم عاطخالا حيصت تافلنم خسن نكمي [ةلاقملا](#) هذه يفةدراول.

ال اءادال لوصولل ربكأو 6.2.0 رادصال FirePOWER يفة FMC لعل رايخ كانه ،كلذ نم ال دب دوجوملا زمرلا قوف رقنا مثةزهجالا ةرادا > ةزهجالا للاقنتا ، FMC لعل هذه ةدعاسملا كنكمي .فلملا ليزنت > مدقتملا اهالصالو عاطخالافاشكتسا هعبت ي ،ينعمل زاهجالا راجب ليزنت قوف رقنلاو لؤاستلالحم فلملا مسا لاخلالذدعب



اهريفشت كفةمزع طاقتلالاشنإ

اهريفشت كفةمتي يتاللمعلال تاسلجل رفشم ريغ ةمزع طاقتلال عيمجت نكمملا نم debug-DAQ debug_daq_write_pcap ماطنلال معد وه رمالال FirePOWER ةطساوب

كفةمتي يتاللةمزال طاقتلالاشنإ لبق ريخشلال ةيلمع ليعشت ةداعإ بجي :ريذحت لاسرا ةداعإ متي .مزالاضعب طاقسإ يفة ببيت ي نكمي يذلاو ،اهريفشت رورمالا ةكرح رثات نأ نكمي نكلو ،TCP رورمة كرح لثم ةلالال نع ةربعملال تالوكوتوربالا .ابللس ، UDP لثم ، يرخال

```
> 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_*
```

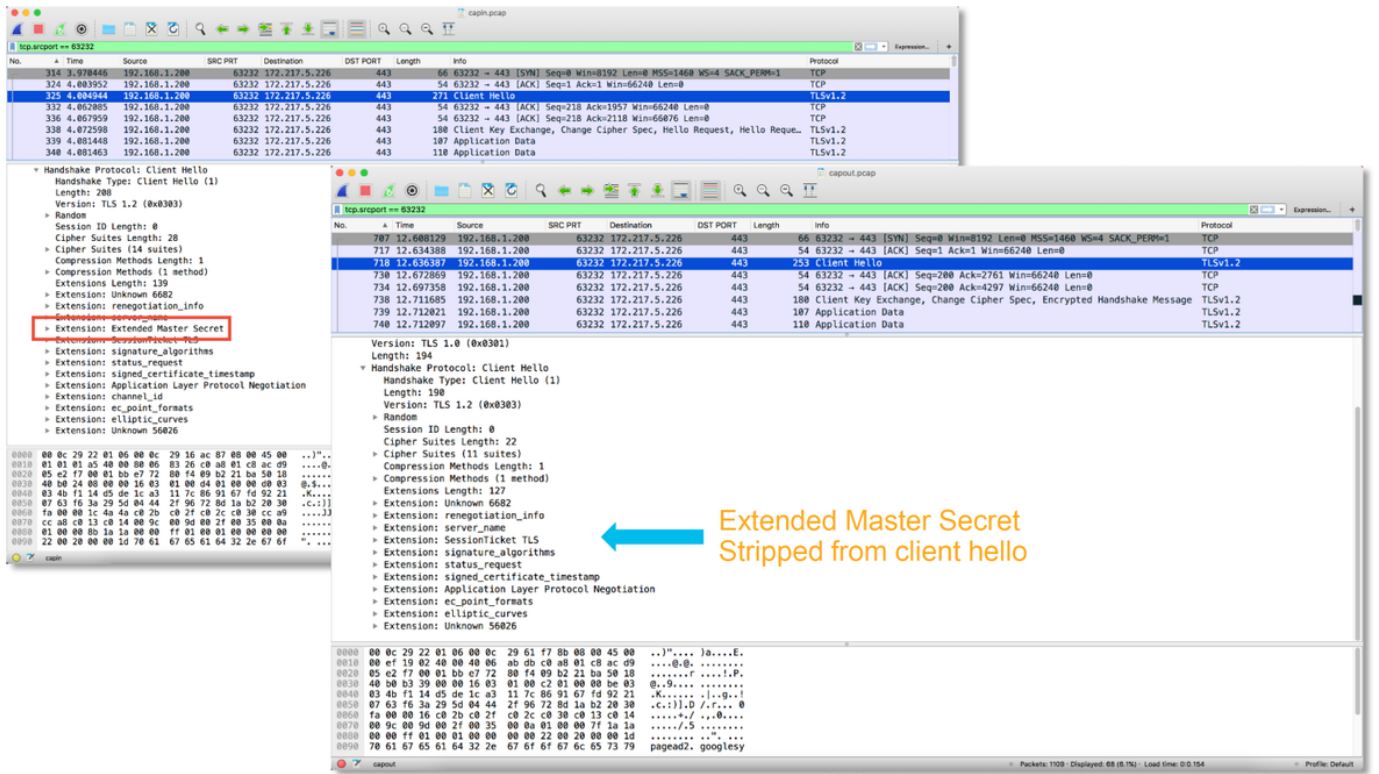

The image displays two screenshots of Wireshark network traffic analysis. The top screenshot shows a list of packets where the last few are highlighted in red, indicating a failure in SSL decryption. A blue arrow points to these packets with the text "SSL Decryption fails". The bottom screenshot shows a detailed view of a packet where the payload is successfully decrypted and displayed in ASCII. A blue arrow points to this section with the text "Successful SSL Decryption".

فلم ةي فصتب ي صوي ،TAC إلى اهرى فشت ك فم PCAP طاقن ل لاسرا ل بق :ريذحت
 تانايب ي أ نع فشكل بنجتل ،لكاشم لل ةبسمل اتاقفدتل إلى هدحو طاقنلالا
 عاد نود ةساسح

لعمال بيحرت تاليدت نع شحبال (CHMod)

شده لعمال بيحرت يلع ليدت ي اناك اذا ام ةفرعمل ةمزل طاقنل ميقت اضي انكمي

نمي ل يلع ةدوجومل كلت رهظت .ي لصلأل لعمال بيحرت راسي ل يلع ةمزل طاقنل روصي
 في CHMod ةزيم ربع عسومل يسيئرل رسلا ةلازاتمت دق هنا طحال .مداخل بناج نم مزل
 FirePOWER.



كفل لي قسما ق دصملا عجرملا يف قثي ليمعلا نأ نم دكأت ةلاق تسال/اريفش التا

يفيضم نأ نم دكأت ،"ةلاق تسال" - ريفش ت ك ف " اراج | عم SSL ةسايس دعاوقل ةبسنلاب نأ يفغ بني الو . ليق تسملا CA ك مدختسملا (CA) "ق دصملا عجرملا" يف نوقثي ليمعلا نم راوح يف لوخدلا كشو يلع اوحبصأ مهنا ىلى اراش | ي نيفئاهنلا نيمدختسملا ىدل نوكي جهن لالخنم عئاش لكش ب كلذ صرف متي . عيقوتللا CA ب اوقثي نأ بجي . ةيامحل راج لالخنم AD . ةيساسالا ةينبالاو ةكرشللا ةسايس ىلع دمتعي هنكلو (AD) ةومجم

ةسايس ءاشن ةيفي ك ددحت يتلاو ، ةيلاتلا [ةلاقملا](#) ةعجارم كنكمي ، تامولعمل نم ديزمل SSL .

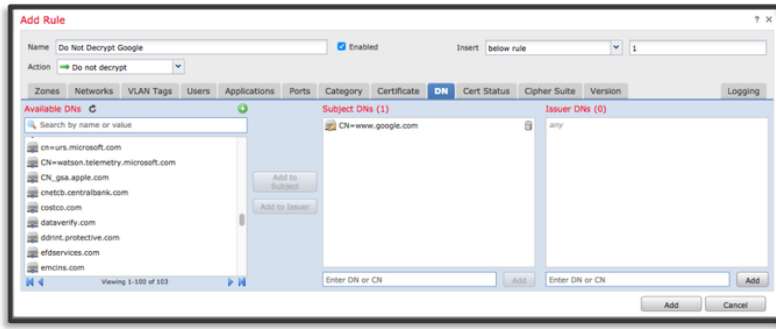
فيفختلا تاوطخ

لجأ نم ةيساسالا فيفختلا تاوطخ ضعب عابتا نكمي

- نعيم رورم ةكرح ريفش ت ك ف مدعل SSL جهن نيوكت ةداع |
- ريفش ت ك ف حجني ىتح ليمعلا بيحرت ةمزح نم ةنيعم تانايب اراج |

ريفش ت ك ف مدع دعاوق ةفاضل (DNd)

رورملا دنع رسكنت google.com ىلى رورملا ةكرح نأ ديدحت مت ، يلاتلا لاثملا ويرانيس يف مداخل ةداهش يف (CN) عئاشلا مسالا ىلع ءانب ، ةدعاوق ةفاضل مت . SSL ةسايس صحف ربع google.com ىلى رورملا ةكرح ريفش ت ك ف متي ال ىتح



| # | Name | Source Zones | Dest Zones | Source Networks | Dest Networks | VLAN Tags | Users | Applications | Source Ports | Dest Ports | Categories | SSL | Action |
|------------------------|-----------------------|--------------|------------|-----------------|---------------|-----------|-------|--------------|--------------|------------|------------|----------------|------------------|
| Administrator Rules | | | | | | | | | | | | | |
| This category is empty | | | | | | | | | | | | | |
| Standard Rules | | | | | | | | | | | | | |
| 1 | Do Not Decrypt Google | any | any | any | any | any | any | any | any | any | any | 1 DN selection | Do not decrypt |
| 2 | MIM | any | any | any | any | any | any | any | any | any | any | any | Decrypt - Resign |
| Root Rules | | | | | | | | | | | | | |
| This category is empty | | | | | | | | | | | | | |
| Default Action | | | | | | | | | | | | Do not decrypt | |

قروم هالعا ةحضوملا احوالصوا ءاطخألا فاشك تأسأ تاوطخ عابتا نكمي، هرشنو وجهنلا ظفح دعب رورملا ةكرح عم FirePOWER هب موقوي ام ةفرعمل ىرخأ.

للمعمل HELLO ليدعت طبض

يف ةلكشم دوجو نع احوالصوا ءاطخألا فاشك تأسأ فاشكي نأ نكمي، التاحل ضعب يف معدل ةدعاسملا ءادألا ليغشت نكمي. ةني عم رورم ةكرح ريفشت ك فب قلعتت FirePOWER تانايب ليزي FirePOWER لعل (CLI) رم اوألا رطس ءهجاو ىلع `ssl-client-hello-tuning` ماظنلا للمعمل ءاصألا HELLO ةمزنم ةني عم.

ىلع روثعلا متي. ةني عم TLS تاقحلم ءلازا متت ىتح نيوكت ةفاضإ متت، يلاتلا لاثملا يف اهرپي عم و TLS تاقحلم لوح تامولعم نع ثحبلا لالخنم ةيمقرلا تافرعلا.

للمعمل بيحرت ليدعت تاريغت حبصت نأ لبق رخنلا ةلمع ليغشت ءداعإ بجي: ريذحت لاسرا ءداعإ متي. مزحل ضعب طاقسإ يف ببستت نأ نكمي يتلاو، لوعفملا ءيراس رورملا ةكرح رثأت نأ نكمي نكلو، TCP رورم ةكرح لثم ءلاحلا نع ءربعملا تالوكوتوربلا ابللس، UDP لثم، ىرخألا.

```
> 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

رمأل اذيفنت نكمي، ليمع لل ابحرم ليدعت تادادع اىل ع اوارح ا مت تاريغت اى ةداعتسال
system support ssl-client-hello-reset.

TAC اىل اهم يدقت متيس يتا انايبل

تاميلعت تانايبل

فاشك تسأ

ءاطخأ

تافلما

اهحالص او

زكرم نم

ءرادإ

Firepower

(FMC)

ءزه او

FirePOWER

ححصت

ءاطخأ SSL

طاقتال

ءسلج ءمزح

ءلماك لمع

بناج نم

ليمع

زاهو

FirePOWER

هسفن

بناجو

دنع مءاخال

(نالك اىل)

تاطقل

ءءشاش

ءءر رىراقت

لاصتال

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn>

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-applian>

تاميلعت اىل ع لوصحلل ءلاقملا هذه ع لاط

ءىلاتال ءوطخال

نوكتس ةيلا ةوطخلا نإف ، ةلكشملا ببس وه سئل SSL ةسايس نوكم نأ ديدحت مت اذإ
اهال صاوة طشنلا ةقدا صملا ةزيم ءاطخأ فاشكتسا

ةيلا ةلاقملا ةعباتمل [إنه](#) رقنا

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ل ا ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا