

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 حيصت](#)

[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 تاوطخ](#)

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

[ليمعلا HELLO ليدعت طبض](#)

[TAC ىلا اهميدقت متيس يتلا تانايبلا](#)

[ةيلاتلا ةوطخللا](#)

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 ىجري. رورملا ةكرح ىلع تانايبلا تاراسم عاڤخأ فاشكتسأ" تالاقم ب اهتاطابترا و FirePOWER ةيساسألا ةمظنألا ىرخألا "اهالصل او

FirePOWER تانايب راسم عاڤخأ فاشكتسأ نم ةسماخللا 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 تامولعمللا قبطنت يف طقف رفوتم (SFR ةدحو) FirePOWER تامدخ عم (ASA) فيكتلل لباقلا نامألا زاوجل 6.1+ يف ال "ليمعلا بيحرت ليدعت" ةزيم رفوتت ال 6.0+ رادصللا
- لوصوللا يف مكحتلا جهن يف SSL جهن مادختس اديكأت

test

Enter Description

Prefilter Policy: [Default Prefilter Policy](#)

SSL Policy: [TEST_SSL_POLICY](#)

Rules Security Intelligence HTTP Responses **Advanced**

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 فال اءارءال" كلذ ي ف ام ب ،ءع او ق ال ع ي مء ل ل ي ء س ت ال ن ي ء م ت ن م ق قء ء ت

#	Name	Sour... Zones	Dest Zones	Source Netw...	Dest Netw...	VLA...	Us...	Appli...	Sour...	Dest ...	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DnD banking	any	any	any	any	any	any	any	any	any	Financial Services (Any Reputatio	any	Do not decrypt
2	decrypt outbound suspicious	inside	outside	any	any	any	any	any	any	any	Any (Reputations 1-2)	any	Decrypt - Resign

Editing Rule - DnD banking

Name: Enabled Move

Action:

Logging

Log at End of Connection Enable Logging

Send Connection Events to:

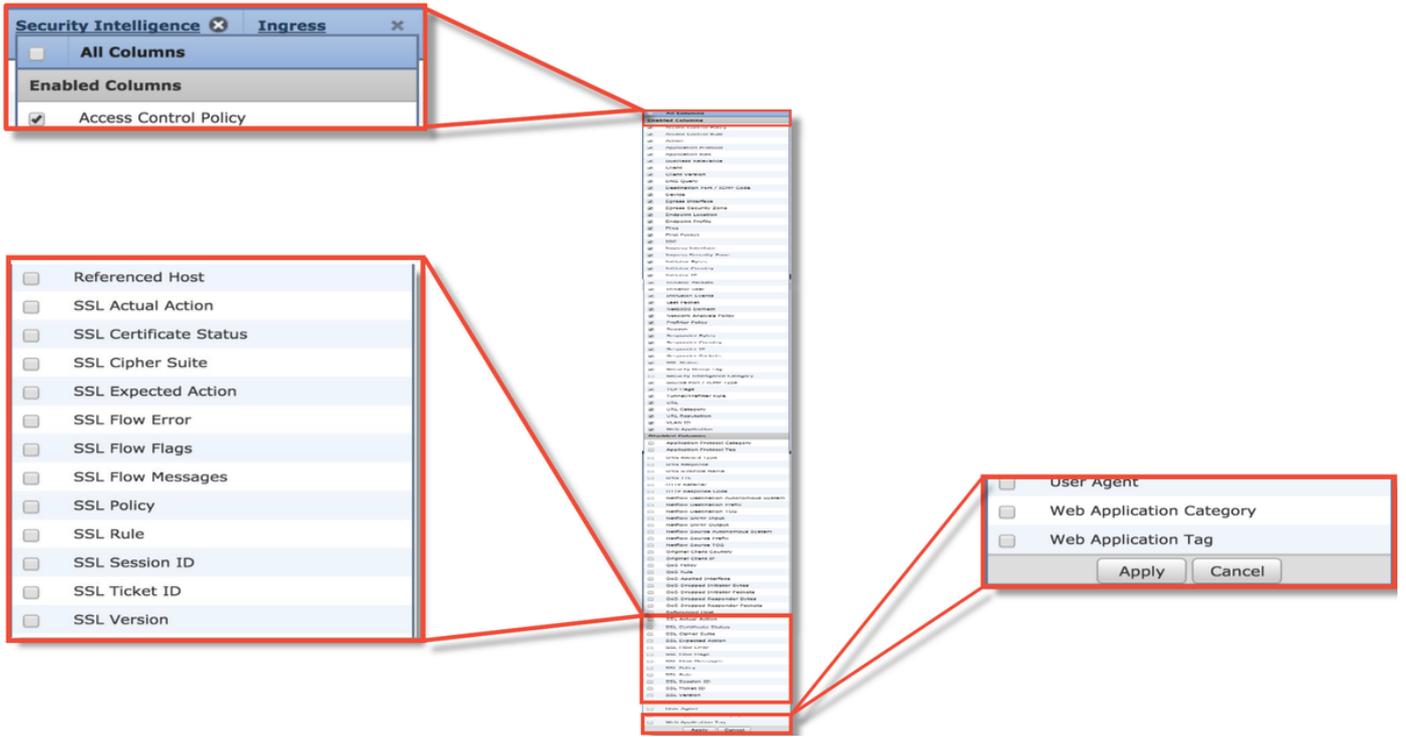
Event Viewer

Syslog

SNMP Trap

Save Cancel

- رءءل راء ء ي أ ن ي ء ء م ت اءا ام ء ء ر ء م ل ر ي ء ش ت ال اءارء ب ي و ب ت ال ء م ال ع ن م ق قء ء ت رور م ال ء ء ء
- ن ي ء م ت ب م ق ، ل ا ص ت ال اء اء ال ل وءء ال ء ر ع ء ق ي ر ط ي ف ن وء ت ام ء ن ع ، ل ا ص ت ال اء اء ء ي ف م س ال ا ي ف 'SSL' ت اء ل و قء ال ء ف اء ء اء ء ض ر اء ي ف اء ن ي ء م ت ب ء ي و ي ض ا ر ت ف ا ل ء ش ب ت ام ءء ال ء ذ ء م ط م ل ي ط ء ت م ت ي ل ا ص ت ال



اهال الصا و SSL جهن ةل حرم ااطخا فاشكتسا

ةكرح طاقسا ب SSL ةسايس موقت دق اذامل مهف يف ةدعاس ملل ةدحما تاوطخ عابتا نكمي اهاب حامسلا عقوتملا رورملا

لاصتالا اادحا يف SSL لوقح نم ققحتلا

لوالا ناكلما نإف ،رورملا ةكرح يف لكاشم يف ببستت SSL ةسايس نأ يف هبتشي ناك اذا نيكمت دعب (اادحالا > تالاصتالا > ليلحتلا تحت) لاصتالا اادحا مسق وه هصحف بجي يذلا هالعأ حضوم وه امك ، SSL لوقح عيجم

قفدت ااطخ دومع يوتحي " SSL ةلتك" ببسلا لوقح ضرعي ،رورملا ةكرح عنمي SSL جهن ناك اذا لوقح تامولعم ىلع ىرخالا SSL لوقح يوتحت .ةلتكلا شودح ببس لوح ةديفم تامولعم ىلع SSL قفدتلا يف FirePOWER اهفشتكا يتلا SSL تانايب

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) ةينقتللا ةدعاسملا زكرم ىلإ تانايبلل هذه ريفوت نكمي ريرقتللا ممصم رزمادختسا نكمي، ةلوهسب تامولعملل هذه ريدصت لجا نم. SSL ةسايسل نم.يال يولعلل نكرلا يف دوجوملا

راطلال تاراخي و تاحشرملا خسن متي، "لاصتالا ثادحأ" مسق نم رزلا اذه قوف رقنلا مت اذا اياقلا ريرقتللا بلال 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


```
> 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 حيحصت لئغشت فاقئ سئنا ال :رئذحت
 system support ssl-debug-reset رمألا مادختساب

نوئي س. FirePOWER زاخ ىلع لئغشتلا دي ق ريخش ةي لمع لك لبوتكم فلم كانه نوئي س
 اتا فللمل اعقوم:

- /VAR/رئغ ةي ساسألا 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 حيحصت تالچس ي ف ةدي فللمل لوقحلل ضع ب 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_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;
...

```

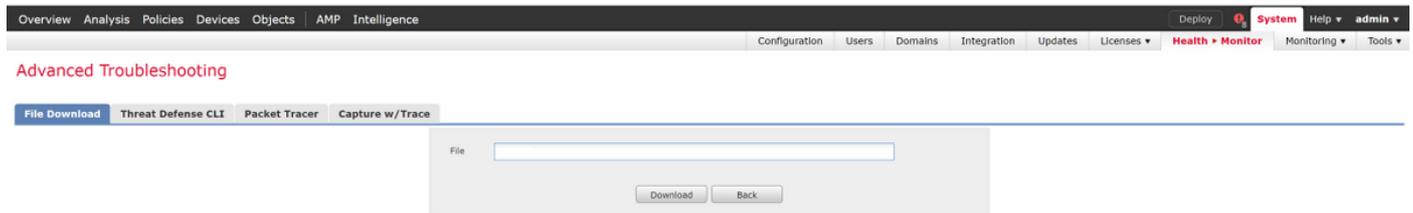
SSL Errors potentially causing drop

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

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

تاهاجتالامادختساب > رمالاهجوم نم FirePOWER زاغنم عاطخالا حيصتتافلمخسن نكمي [ةلاقملا](#) هذه يفةدراول.

ال اءاى لولل ركبأو 6.2.0 رادصال FirePOWER يفة FMC لىل رايخان، كلذ نم ال دب دوجوملا زمرلا قوف رقنا مثةزهجالا ةرادا > ةزهجالا لىل لقتنا، FMC لىل هذه ةدعاسملا كنكمي. فللملا ليزنت > مدقتملا اءالصال عاطخالافاشكتسا هعبتي، ينعمل زاغال راجب ليزنت قوف رقنلاو لؤاستلالحم فللملا مسا لاءل كلذ دب.

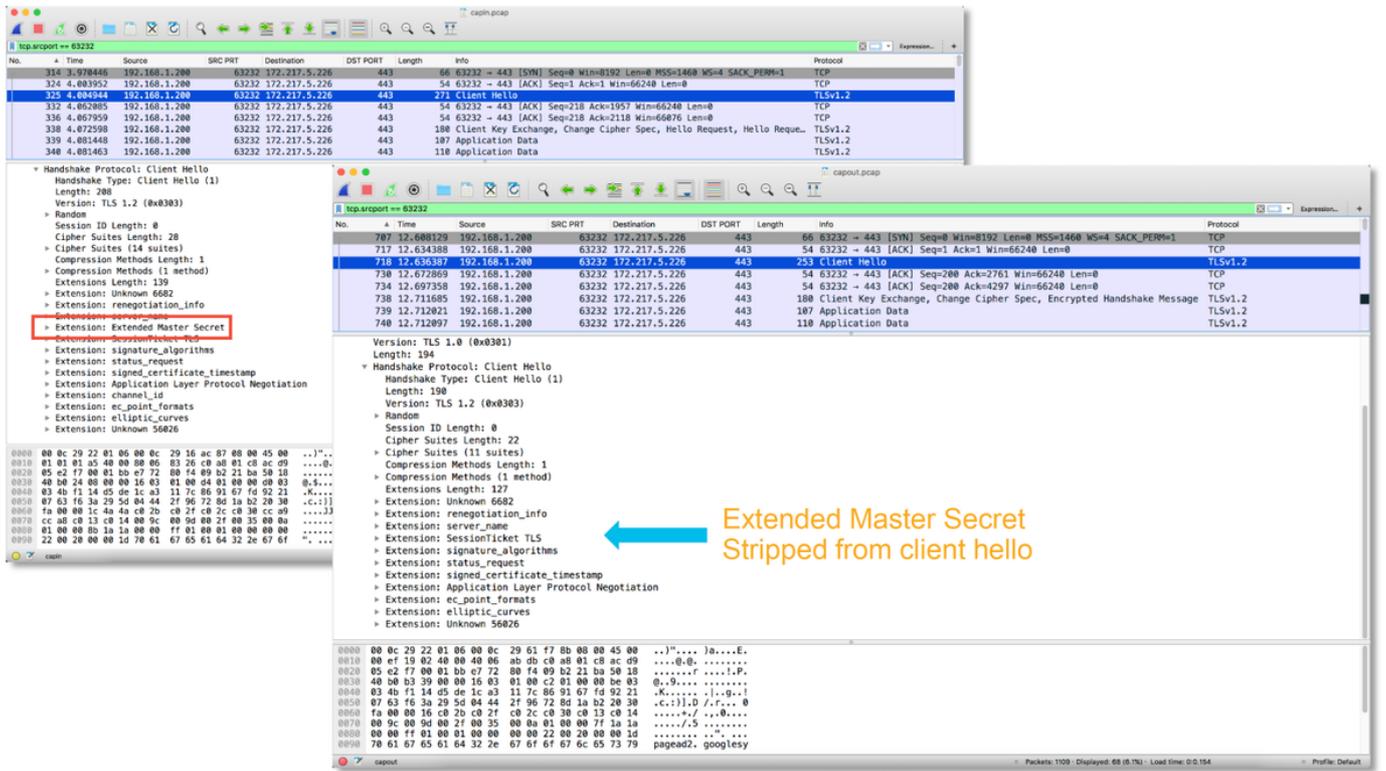


اهريفشت كفةمزع طاقتلالاشنإ

اهريفشت كفةمتي يتاللمعلال تاسلجل رفشم ريغه مزع طاقتلال عيمجت نكمملا نم `debug-DAQ debug_daq_write_pcap` ماطنلال معد وه رمالال FirePOWER ةطساوب

كفةم تي تاللامزع طاقتلالاشنإ لبق ريخشلال ةيلمع لىلغشت ةءاعإ بجي: ريدحت لاسرا ةءاعإ متي. مزجالاضعب طاقسإ يفة ببيتى نا نكمي يذلاو، اهريفشت رورملا ةكرح رثات نا نكمي نكلو، TCP رورم ةكرح لثم ةلالال نع ةربعملال تالوكوتوربالا. ابللس، UDP لثم، ىرخال.

```
> 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_*
```

كفل لي قسما ق دصملا عجرملا يف قثي ليمعلا نأ نم دكأت ةلاق سالا/ر ي ف شتلا

يفي ضم نأ نم دكأت ، "ةلاق سالا - ر ي ف شت ك ف" ءارجا عم SSL ةسايس دعاوقل ةبسنلاب نأ يف بنو الو . ليق سالا CA ك مدخت سالا (CA) "ق دصملا عجرملا" يف نوقثي ليمعلا نم راوح يف لوخدلا كشو يلع او حبصأ مهنا ىلى ءراشا ي ن ي ئا ه ن لا ن ي مدخت سالا ىدل نو ك ي جهن لال خ نم ءئاش لكش ب كل ذ صرف متي . عي قوتلا CA ب اوقثي نأ بجي . ةيامحلا راج لال خ AD . ةيساسالا ةينبالاو ءكرشلا ةسايس ىلع دمتعي هنكلو (AD) ءومجم

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

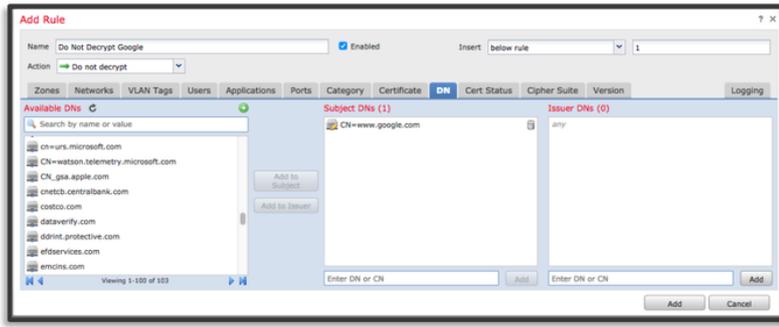
فيختلا تاو طخ

لجأ نم ةيساسالا فيختلا تاو طخ ضعب ءاب تا نكمي :

- نعيم رورم ءكرح ر ي ف شت ك ف مدعل SSL جهن نيوك ءءاعا
- ر ي ف شتلا ك ف حجني ىتح ليمعلا بيحرت ءمزح نم ءنيعم تانايب جارجا

ر ي ف شتلا ك ف مدع دعاوق ءفاضلا

رورملا دنع رسكنت google.com ىلى رورملا ءكرح نأ ديدحت مت ، يلاتلا لاثملا ويراني س يف مداخل ءءاهش يف (CN) ءئاشلا مسالا ىلع ءانب ، ءءاق ءفاضلا مت . SSL ةسايس صرحف ربع google.com ىلى رورملا ءكرح ر ي ف شت 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، تالاحل ضعب يف معدل ةدعاسملا ءادألا ليغشت نكمي. ةني عم رورم ةكرح ريفشت ك فب قلعتت FirePOWER تانايب ليزي FirePOWER لعلج (CLI) رماوالا رطس ءهجاو ىلع `ssl-client-hello-tuning` ماظنلا للمعمل ءاصخال HELLO ةمزنم ةني عم.

ىلع روثعلال متي. ةني عم TLS تاقحلم ءلازا متت ىتح نيوكت ةفاضإ متت، يلاتلا لاثملا يف اهرپي عمو TLS تاقحلم لوح تامولعم نع ثحبلا لالخنم ةيمقرلا تافرعمل.

للمعمل بيحرت ليدعت تاريغت حبصت نأ لبق رخنلا ةلمع ليغشت ءداعإ بجي: ريذحت لاسرا ءداعإ متي. مزحلل 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 ل ابحرم ليدعت تادادع اىل ع اوارح ا مت تاريغت اى ةداعتسال
system support ssl-client-hello-reset.

TAC اىل اهم يدقت متيس يتل انايبل

تاميلعت تانايبلا

فاشك س ا

ءاطخ ا

تافلما

اهال ص او

زكرم نم

ءراد ا

Firepower

(FMC)

ءزه او

FirePOWER

ححصت

ءاطخ ا SSL

طاقتلا

ءسلج ةمزح

ءلماك لمع

بناج نم

ليمعلا

زاهو

FirePOWER

هسفن

بناجو

دنع مءاخلا

(نالك اءلا

تاطقل

ءءشاش

ءءر رراقء

لاصءالا

<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 لوصح لىل ةلاقملا هءه ع لاط

ءيلاءلا ةوطخلا

نوكتس ةيلا ةوطخلا نإف ، ةلكشملا ببس وه سېل SSL ةسايس نوكم نأ دېدحت 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 اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م 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 م ل ا ح ل ا و ه
ل ا ا م ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه 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 چ ن ا ل ا دن ت س م ل ا