

Firepower Data Path Problemen opsporen en verhelpen fase 5: SSL-beleid

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Probleemoplossing voor de SSL-beleidsfase](#)

[Controleer SSL-velden in de verbindingsebeurtenissen](#)

[Afbreken van het SSL-beleid](#)

[Een decryptie pakketvastlegging genereren](#)

[Zoek naar ClientHalo-wijzigingen \(CHMod\)](#)

[Zorg ervoor dat de client vertrouwen heeft in CA voor decryptie/afschrijving](#)

[Beperkingsstappen](#)

[Voeg geen decrypt \(DND\) regels toe](#)

[Aanpassing van client-Hallo](#)

[Gegevens om te leveren aan TAC](#)

[Volgende stap](#)

Inleiding

Dit artikel maakt deel uit van een reeks artikelen waarin wordt uitgelegd hoe u het gegevenspad op FirePOWER-systemen systematisch moet oplossen om te bepalen of onderdelen van Firepower invloed kunnen hebben op het verkeer. Raadpleeg het [gedeelte Overzicht](#) voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

Dit artikel bestrijkt de vijfde fase van de probleemoplossing bij het FirePOWER-gegevenspad, de Secure Socket Layer (SSL) Policy optie.



Voorwaarden

- De informatie in dit artikel is van toepassing op elk FirePOWER-platform SSL-decryptie voor de adaptieve security applicatie (ASA) met FirePOWER Services (SFR-module) alleen beschikbaar in 6.0+De optie voor aanpassing aan client is alleen beschikbaar in 6.1+
- Bevestig dat SSL-beleid in het toegangscontrolbeleid wordt gebruikt

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
--	-----------------

- Controleer dat houtkap is ingeschakeld voor alle regels, inclusief de 'actie standaard'

#	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:

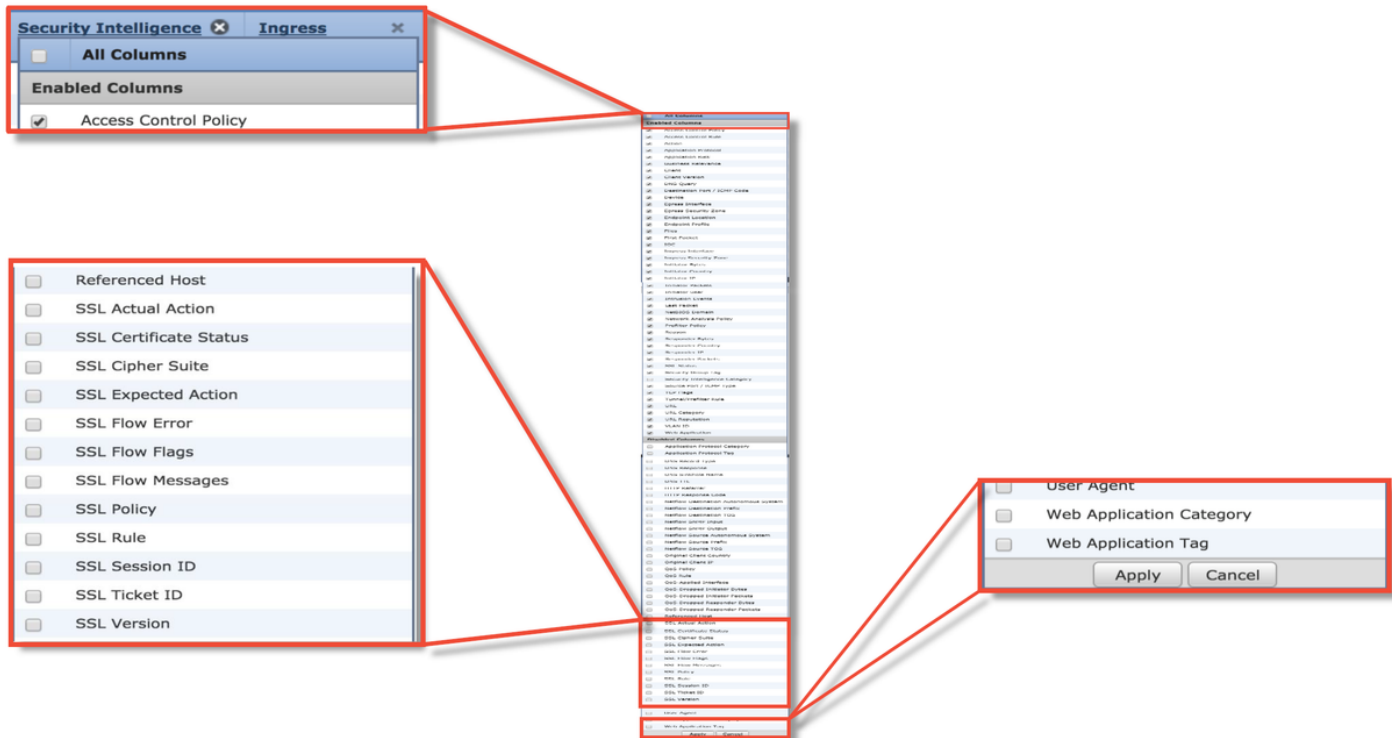
Event Viewer

Syslog

SNMP Trap

Save Cancel

- Controleer het tabblad Undecryptable Actions om te zien of er een optie is ingesteld om verkeer te blokkeren
- In de Connection gebeurtenissen, wanneer u in de tabelweergave van verbindingsebeurtenissen bent, schakelt u alle velden met 'SSL' in de naam in. De meeste zijn standaard uitgeschakeld en moeten worden ingeschakeld in de viewer Connection Events



Probleemoplossing voor de SSL-beleidsfase

Specifieke stappen kunnen worden gevolgd om te begrijpen waarom SSL Policy het verkeer dat naar verwachting is toegestaan, kan laten vallen.

Controleer SSL-velden in de verbindingsebeurtenissen

Als het SSL-beleid vermoed wordt dat u verkeersproblemen veroorzaakt, is de eerste plaats om te controleren de sectie van de gebeurtenis van de verbinding (onder **Analyse > Verbonden > Gebeurtenissen**) na het inschakelen van alle SSL velden, zoals hierboven beschreven.

Als SSL Policy het verkeer blokkeert, geeft het veld **Reason** "SSL Block" (het "SSL blok") weer. De kolom **SSL Flow Error** heeft nuttige informatie over waarom het blok optrad. De andere SSL velden hebben informatie over SSL gegevens die Firepower in de stroom wordt gedetecteerd.

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 (points to Reason column)

Cause of the SSL failure (points to SSL Flow Error table)

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 (points to SSL Flow Flags table)

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

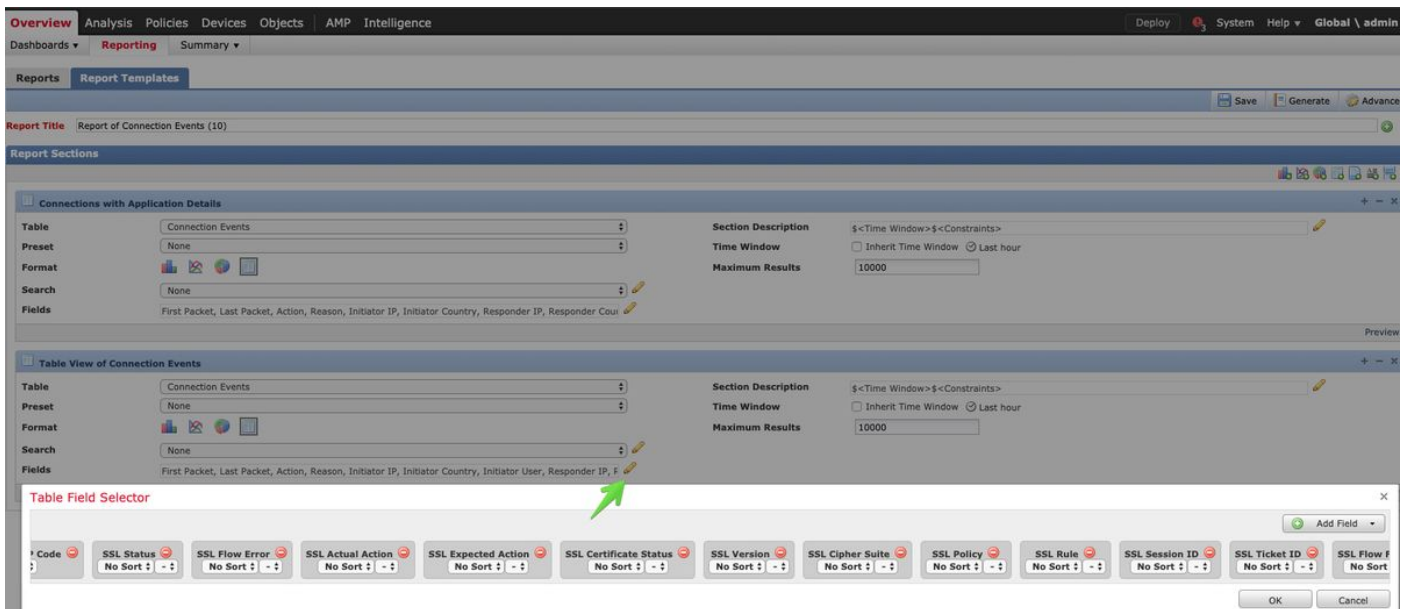
Deze gegevens kunnen aan het Cisco Technical Assistance Center (TAC) worden geleverd wanneer u een case opent voor SSL-beleid. Om deze informatie gemakkelijk te exporteren kan de knop **Ontwerper** van het **Rapport** in de rechterbovenhoek worden gebruikt.

Als op deze knop wordt gedrukt in het gedeelte Connection-gebeurtenissen, worden de opties van de filters en het tijdvenster automatisch naar de rapportsjabloon gekopieerd.

Bookmark This Page **Report Designer** Dashboard View Bookmarks Search ▼

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

Zorg ervoor dat alle vermelde SSL-velden in het vak 'Veld' zijn toegevoegd.



Klik op **Generate** om een Rapport over PDF- of CSV-indelingen te maken.

Afbreken van het SSL-beleid

Als de verbindingsebeurtenissen niet genoeg informatie over de stroom bevatten, kan het debuggen van SSL uitgevoerd worden op de Firepower Opmacht Line Interface (CLI).

Opmerking: Alle debug-inhoud hieronder is gebaseerd op de SSL-decryptie die in software op de x86-architectuur gebeurt. Deze inhoud bevat geen debugs van SSL hardware offload-functies die in versie 6.2.3 en on zijn toegevoegd en die anders zijn.

Opmerking: Op de platforms Firepower 9300 en 4100 kan de shell in kwestie worden benaderd via de volgende opdrachten:

```
# sluit module 1 console aan
Firepower-module1> verbinding-ftd
>
```

Voor meerdere instellingen kan het logische apparaat CLI worden benaderd met de volgende opdrachten.

```
# connect module 1 telnet
Firepower-module1> verbinding ftd1
Vet "exit" in om terug te keren naar CLI voor Opstarten
>
```

De opdracht **system support ssl-debug_policy_all** kan worden uitgevoerd om te zorgen voor zuiveringsinformatie voor elke stroom die door het SSL-beleid wordt verwerkt.

Voorzichtig: Het gekorte proces moet voor en na het uitvoeren van SSL debug opnieuw begonnen worden, wat een paar pakketten kan veroorzaken om te worden geworpen afhankelijk van het gekorte-down beleid en de gebruikte plaatsing. Het TCP-verkeer wordt opnieuw verzonden, maar het UDP-verkeer kan negatief worden beïnvloed als de toepassingen die door de firewall passeren geen minimaal pakketverlies verdragen.

```

> 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

Waarschuwing: Vergeet niet het foutoptreden uit te schakelen nadat de benodigde gegevens zijn verzameld met de opdracht **voor systeemondersteuning**.

Er wordt een bestand geschreven voor elk afzonderlijk proces dat op het FirePOWER-apparaat wordt uitgevoerd. De locatie van de bestanden is:

- /var/common voor niet-FTD-platforms
- /ngfw/var/common voor FTD-platforms

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

Dit zijn een aantal van de behulpzame velden in de debug-logbestanden.

```

...
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;


```

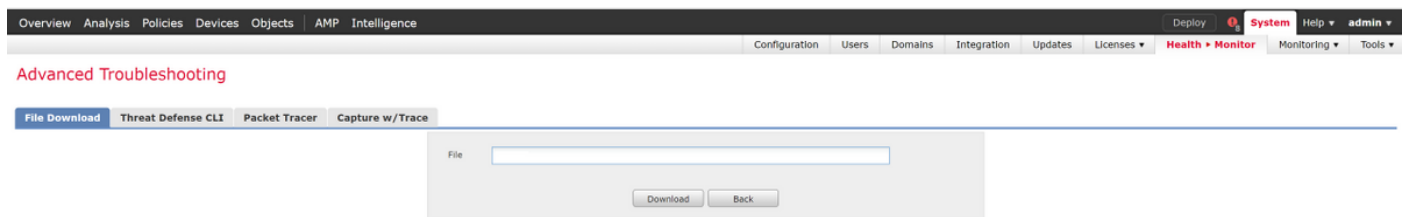
SSL Errors potentially causing drop

Opmerking: Als er een fout met decryptie is die optreedt nadat Firepower begint te decrypteren, moet het verkeer worden gedropt aangezien de firewall de sessie al

aangepast/man-in-the-middle heeft, dus het is niet mogelijk voor de client en server om communicatie te hervatten aangezien ze verschillende TCP stapels hebben evenals verschillende encryptiesleutels die in de flow gebruikt worden.

U kunt de debug-bestanden van het FirePOWER-apparaat uit de >-melding kopiëren met behulp van de aanwijzingen in dit [artikel](#).

U kunt ook een optie op het FMC instellen in Firepower versie 6.2.0 en hoger. Om toegang te hebben tot dit UI-hulpprogramma op het FMC, navigeer naar **Apparaten > Apparaatbeheer**. Klik vervolgens op de  pictogram naast het apparaat in kwestie, gevolgd door **Advanced Problemen opsporen en verhelpen > Bestand downloaden**. U kunt vervolgens de naam van een bestand in kwestie invoeren en op Downloaden klikken.



Een decryptie pakketvastlegging genereren

Het is mogelijk om een niet-versleutelde pakketvastlegging te verzamelen voor sessies die door Firepower worden versleuteld. Deze opdracht is **steemondersteuning voor debug-DAQ**
debug_daq_schrijf_pcap

Voorzichtig: Het gekleurde proces moet opnieuw worden opgestart voordat u het gedecrypteerde pakketvastlegging genereert, waardoor een paar pakketten kunnen worden gedropt. Stateful protocollen zoals TCP-verkeer worden opnieuw verzonden, maar ander verkeer, zoals UDP, kan negatief worden beïnvloed.

```
> 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 top screenshot shows a network capture with a red arrow pointing to the error message "SSL Decryption fails". The bottom screenshot shows a network capture with a blue arrow pointing to the decrypted data, including a "POST /comet HTTP/1.1" request.

Voorzichtig: Alvorens een gedecrypteerde PCAP-opname naar TAC te verzenden, wordt aanbevolen het opnamebestand te filteren en te beperken tot de problematische stromen, om te voorkomen dat gevoelige gegevens onnodig worden blootgelegd.

Zoek naar ClientHallo-wijzigingen (CHMod)

De pakketvastlegging kan ook worden geëvalueerd om te zien of om het even welke client hallo verandering plaatsvindt.

De pakketvastlegging links toont de oorspronkelijke client hallo. Rechts zie je dat server-side pakketten. Merk op dat het uitgebreide hoofdgeheim is verwijderd via de CHMod optie in Firepower.

The top screenshot shows a network capture of a TLSv1.2 Client Hello packet. The packet details pane lists several extensions, including 'Extended Master Secret', which is highlighted with a red box. The packet bytes pane shows the raw data of the Client Hello.

The bottom screenshot shows another network capture of a TLSv1.2 Client Hello packet. The 'Extended Master Secret' extension is highlighted with a red box, and a blue arrow points to it from the text 'Extended Master Secret Stripped from client hello'.

Zorg ervoor dat de client vertrouwen heeft in CA voor decryptie/afschrijving

Voor SSL Policy regels met een actie van "Ontslutelen - Aftreden", zorg er dan voor dat de clienthosts vertrouwen hebben op de certificaatautoriteit (CA) die wordt gebruikt als de afzender CA. De eindgebruikers moeten geen indicatie hebben dat zij door de firewall worden gedemoniseerd. Ze moeten de ondertekenende CA vertrouwen. Dit wordt meestal afgedwongen via Active Directory (AD) Group Policy, maar het is afhankelijk van het bedrijfsbeleid en de AD-infrastructuur.

Voor meer informatie kunt u het volgende [artikel](#) bekijken, dat beschrijft hoe u een SSL Beleid kunt creëren.

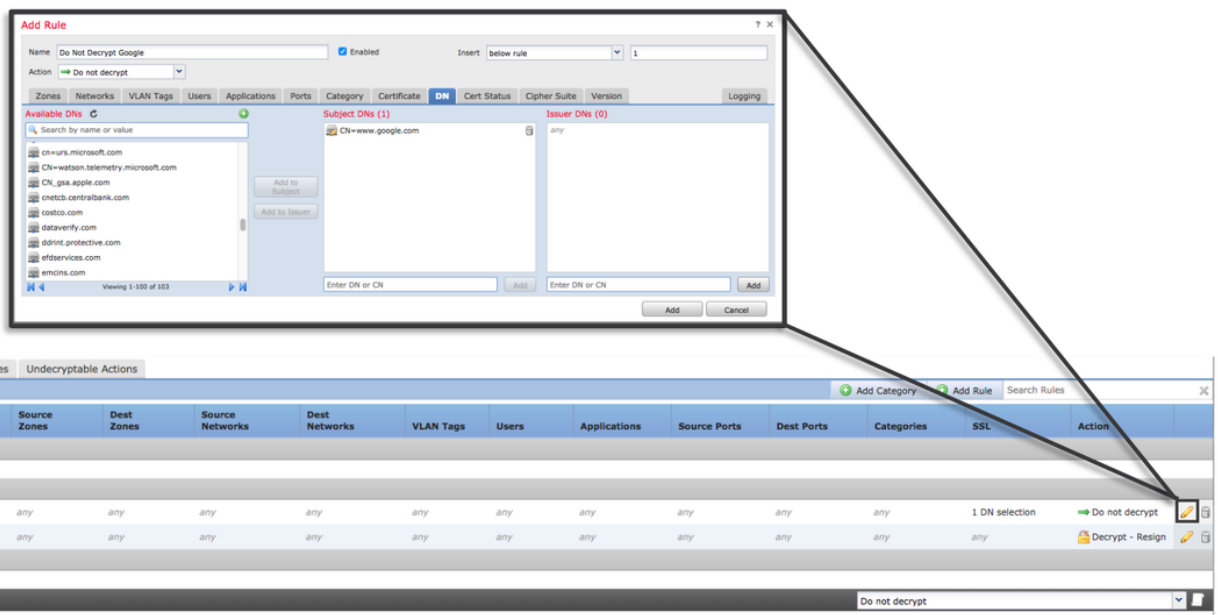
Beperkingsstappen

Er kunnen een aantal basismaatregelen worden genomen om:

- Configureer het SSL-beleid om bepaald verkeer niet te decrypteren
- Neem bepaalde gegevens uit een pakket van de klant hallo op zodat decryptie zal slagen

Voeg geen decrypt (DND) regels toe

In het volgende voorbeeldscenario is bepaald dat het verkeer naar google.com breekt wanneer het door SSL Policy inspectie passeert. Er wordt een regel toegevoegd, gebaseerd op de Gemeenschappelijke Naam (CN) in het servercertificaat, zodat het verkeer naar google.com niet wordt gedecripteerd.



Na het opslaan en implementeren van het beleid, kunnen de hierboven beschreven stappen voor het oplossen van problemen opnieuw worden gevolgd om te zien wat Firepower met het verkeer doet.

Aanpassing van client-Hallo

In bepaalde gevallen kan het oplossen van problemen onthullen dat Firepower in een probleem loopt met het decrypteren van bepaald verkeer. Het **stelsel ondersteuning** kan **SL-client-hallo-tuning** hulpprogramma op CLI worden uitgevoerd om Firepower te veroorzaken om bepaalde gegevens van een client hallo-pakket te verwijderen.

In het onderstaande voorbeeld wordt een configuratie toegevoegd zodat bepaalde TLS-uitbreidingen worden verwijderd. De numerieke ID's worden gevonden door te zoeken naar informatie over TLS-uitbreidingen en -normen.

Voorzichtig: Het snaarproces moet opnieuw opgestart worden voordat de wijzigingen in de groeten van de client van kracht worden, waardoor een paar pakketten kunnen worden geworpen. Stateful protocollen zoals TCP-verkeer worden opnieuw verzonden, maar ander verkeer, zoals UDP, kan negatief worden beïnvloed.

```
> 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

Om alle wijzigingen om te zetten die zijn aangebracht in de instellingen voor de hallo van de client, kan de **systemondersteuning** worden geïmplementeerd.

Gegevens om te leveren aan TAC

Gegevens

Probleemoplossing van bestanden van het FireSIGHT Management Center (FMC) en FirePOWER-apparaten
SSL-debugg
Volledige sessiepakket neemt van de clientkant, het apparaat zelf en de serverkant, indien mogelijk, op
Screenshots van verbidingsgebeurtenissen of rapporten

Instructies

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

Zie dit artikel voor instructies

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

Volgende stap

Als is vastgesteld dat de SSL Policy component niet de oorzaak van de kwestie is, dan zou de volgende stap de actieve optie Verificatie oplossen zijn.

Klik [hier](#) om verder te gaan met het volgende artikel.