

# Fehlerbehebung für FirePOWER-Datenpfad

## Phase 5: SSL-Richtlinie

### Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Fehlerbehebung in der SSL-Richtlinienphase](#)

[Überprüfen von SSL-Feldern in Verbindungsereignissen](#)

[Debuggen der SSL-Richtlinie](#)

[Erstellen einer entschlüsselten Paketerfassung](#)

[Suchen Sie nach Client Hello Modifications \(CHMod\).](#)

[Vergewissern Sie sich, dass Client-Trusts CA für Entschlüsselung/Rücktritt zurückweisen](#)

[Schritte zur Risikominimierung](#)

[Nicht entschlüsseln \(DND\)-Regeln hinzufügen](#)

[Optimierung von Client-Hello-Änderungen](#)

[Daten für TAC](#)

[Nächster Schritt](#)

### Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im [Übersichtsartikel](#).

Dieser Artikel behandelt die fünfte Phase der Fehlerbehebung bei Firepower-Datenpfaden, die SSL-Richtlinienfunktion (Secure Sockets Layer).



### Voraussetzungen

- Die Informationen in diesem Artikel gelten für alle Firepower-Plattformen SSL-Entschlüsselung für die Adaptive Security Appliance (ASA) mit FirePOWER-Services (SFR-Modul) nur ab Version 6.0 verfügbar. Die Funktion "Client Hello Modification" ist nur in Version 6.1+ verfügbar.
- Bestätigen Sie, dass die SSL-Richtlinie in der Zugriffskontrollrichtlinie verwendet wird.

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions ▼

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	<b>TEST_SSL_POLICY</b>
--	------------------------

- Überprüfen Sie, ob die Protokollierung für alle Regeln aktiviert ist, einschließlich der Standardaktion.

#	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:

**Log at End of Connection** Enable Logging

Send Connection Events to:

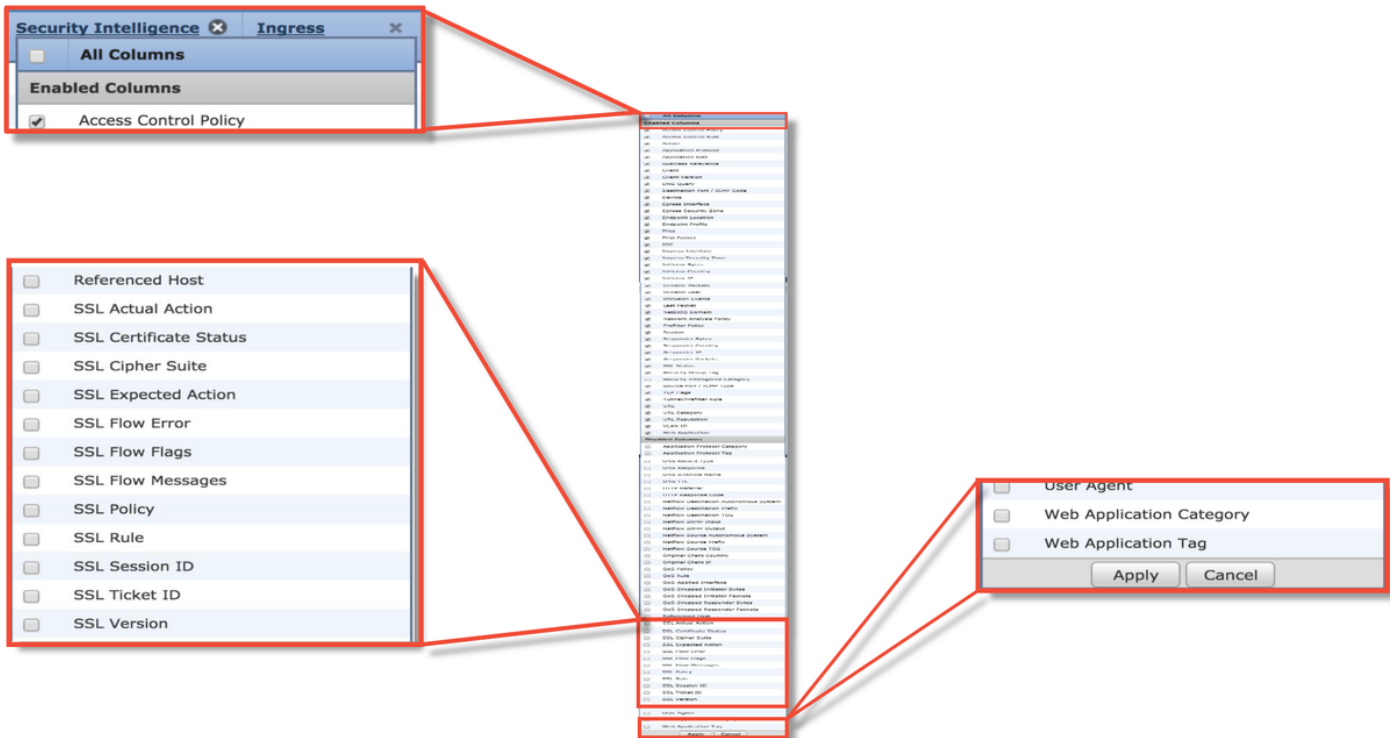
Event Viewer

Syslog

SNMP Trap

Save Cancel

- Überprüfen Sie die Registerkarte Unentschlüsselbare Aktionen, um festzustellen, ob eine Option zum Blockieren des Datenverkehrs festgelegt ist.
  - Aktivieren Sie in den Connection-Ereignissen, wenn Sie sich in der Tabellenansicht von Verbindungsereignissen befinden, alle Felder mit dem Namen 'SSL'
- Die meisten sind standardmäßig deaktiviert und müssen im Connection Events Viewer aktiviert werden.



## Fehlerbehebung in der SSL-Richtlinienphase

Es können bestimmte Schritte ausgeführt werden, um zu ermitteln, warum die SSL-Richtlinie möglicherweise Datenverkehr verwirft, der zugelassen werden soll.

### Überprüfen von SSL-Feldern in Verbindungsereignissen

Wenn der Verdacht besteht, dass die SSL-Richtlinie Datenverkehrsprobleme verursacht, sollten Sie zuerst den Abschnitt "Connection Events" (Verbindungsereignisse) (unter **Analysis > Connections > Events**) überprüfen, nachdem Sie alle SSL-Felder wie oben beschrieben aktiviert haben.

Wenn die SSL-Richtlinie den Datenverkehr blockiert, wird im Feld **Grund** "SSL-Block" angezeigt. Die Spalte **SSL Flow Error** enthält nützliche Informationen darüber, warum der Block aufgetreten ist. Die anderen SSL-Felder enthalten Informationen über SSL-Daten, die FirePOWER im Fluss erkannt hat.

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

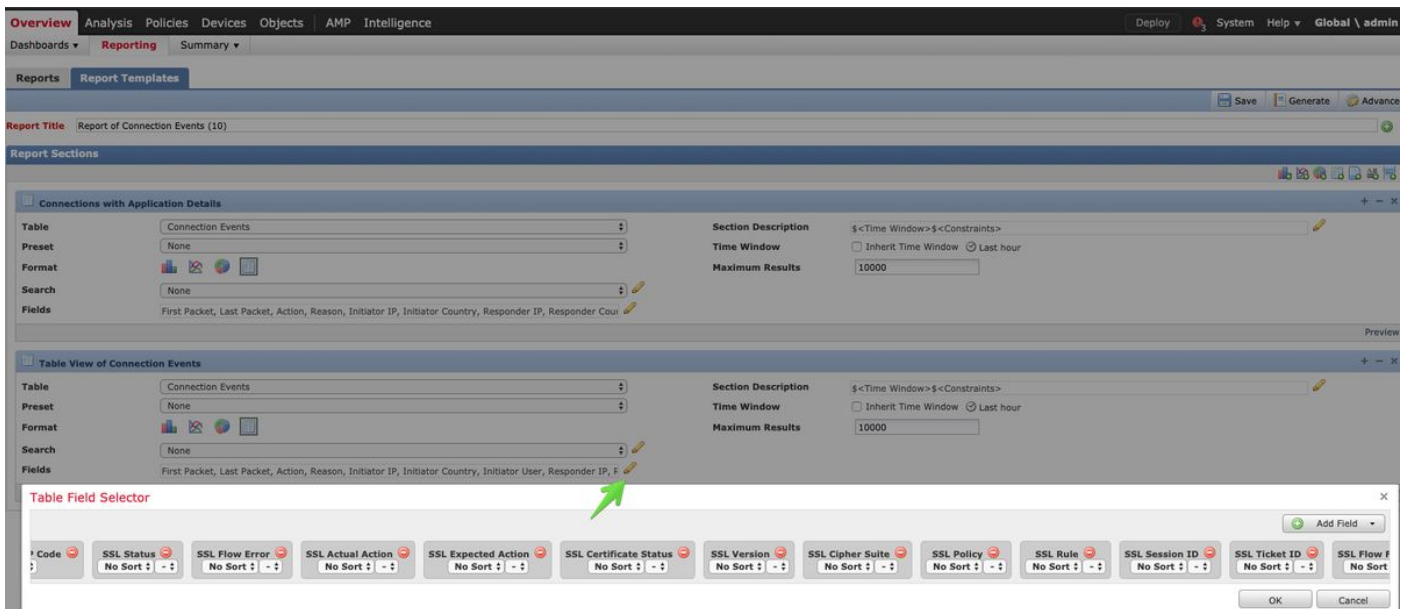
Diese Daten können dem Cisco Technical Assistance Center (TAC) zur Verfügung gestellt werden, wenn ein Ticket für eine SSL-Richtlinie geöffnet wird. Um diese Informationen einfach zu exportieren, können Sie die Schaltfläche **Berichts-Designer** oben rechts verwenden.

Wenn Sie auf diese Schaltfläche im Bereich Verbindungsereignisse klicken, werden die Filter und Optionen des Zeitfensters automatisch in die Berichtsvorlage kopiert.

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

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

Stellen Sie sicher, dass alle genannten SSL-Felder im Bereich 'Field' hinzugefügt werden.



Klicken Sie auf **Generieren**, um einen Bericht im PDF- oder CSV-Format zu erstellen.

## Debuggen der SSL-Richtlinie

Wenn die Connection-Ereignisse nicht genügend Informationen über den Fluss enthalten, kann das SSL-Debuggen über die FirePOWER-Befehlszeilenschnittstelle (CLI) ausgeführt werden.

**Hinweis:** Der gesamte folgende Debuginhalt basiert auf der SSL-Entschlüsselung, die in der Software der x86-Architektur erfolgt. Dieser Inhalt enthält keine Debugger von SSL-Hardware-Offload-Features, die in Version 6.2.3 und in Version 6.2.3 hinzugefügt wurden, die sich voneinander unterscheiden.

**Hinweis:** Auf den Firepower 9300- und 4100-Plattformen kann über die folgenden Befehle auf die betreffende Shell zugegriffen werden:

```
# Connect-Modul 1-Konsole
Firepower-module1> connect ftd
>
```

Bei mehreren Instanzen kann mit den folgenden Befehlen auf die CLI des logischen Geräts zugegriffen werden.

```
# Connect Module 1 Telnet
FirePOWER-module1> connect ftd ftd1
Herstellen einer Verbindung zur Containerkonsole ftd(ftd1) ... Geben Sie "exit" ein, um zur
Boot CLI zurückzukehren.
>
```

Der Befehl **systemsupport ssl-debug debug\_policy\_all** kann ausgeführt werden, um Debuginformationen für jeden von der SSL-Richtlinie verarbeiteten Datenfluss zu generieren.

**Vorsicht:** Der Snort-Prozess muss vor und nach der Ausführung des SSL-Debuggens neu gestartet werden. Dies kann dazu führen, dass je nach den verwendeten Snort-Down-Richtlinien und der verwendeten Bereitstellung einige Pakete verworfen werden. Der TCP-Datenverkehr wird erneut übertragen, aber der UDP-Datenverkehr kann beeinträchtigt

werden, wenn die Anwendungen, die die Firewall passieren, keinen minimalen Paketverlust tolerieren.

```
> 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

**Warnung:** Vergessen Sie nicht, das Debugging zu deaktivieren, nachdem die notwendigen Daten mit dem Befehl **ssl-debug-reset** gesammelt wurden.

Für jeden Snort-Prozess, der auf dem FirePOWER-Gerät ausgeführt wird, wird eine Datei geschrieben. Der Speicherort der Dateien ist:

- /var/common für Plattformen ohne FTD
- /ngfw/var/common für FTD-Plattformen

Debug files location

Snort PID

```
> 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 != 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

Dies sind einige der hilfreichen Felder in den Debug-Protokollen.



```

...
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;


```

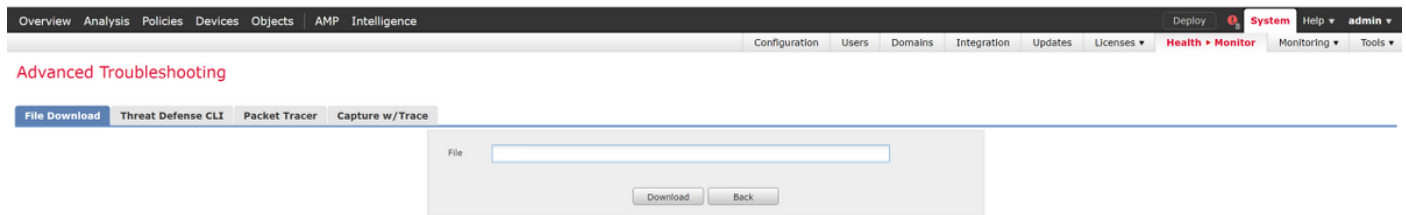
SSL Errors potentially causing drop

**Hinweis:** Wenn nach Beginn der Entschlüsselung durch Firepower ein Entschlüsselungsfehler auftritt, muss der Datenverkehr fallen gelassen werden, da die

Firewall die Sitzung bereits geändert/Man-in-the-Middle geändert hat. Daher ist es für den Client und den Server nicht möglich, die Kommunikation wieder aufzunehmen, da sie über verschiedene TCP-Stacks sowie verschiedene Verschlüsselungsschlüssel verfügen, die im Fluss verwendet werden.

Die Debugdateien können mithilfe der Anweisungen in diesem [Artikel](#) von der Eingabeaufforderung > aus vom FirePOWER-Gerät kopiert werden.

Alternativ gibt es eine Option auf dem FMC in Firepower Version 6.2.0 und höher. Um auf dieses Dienstprogramm der Benutzeroberfläche im FMC zuzugreifen, navigieren Sie zu **Devices > Device Management (Geräte > Geräteverwaltung)**. Klicken Sie anschließend auf die Schaltfläche  neben dem betreffenden Gerät, gefolgt von **Advanced Troubleshooting > File Download**. Sie können dann den Namen einer Datei eingeben und auf Herunterladen klicken.



## Erstellen einer entschlüsselten Paketerfassung

Es ist möglich, eine unverschlüsselte Paketerfassung für Sitzungen zu sammeln, die von FirePOWER entschlüsselt werden. Der Befehl lautet **Systemsupport debug-DAQ debug\_daq\_write\_pcap**.

**Vorsicht:** Der Snort-Prozess muss neu gestartet werden, bevor die entschlüsselte Paketerfassung generiert wird. Dies kann dazu führen, dass einige Pakete verworfen werden. Stateful-Protokolle wie TCP-Datenverkehr werden erneut übertragen, aber anderer Datenverkehr, z. B. UDP, kann negativ beeinflusst werden.

```
> 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_*
```



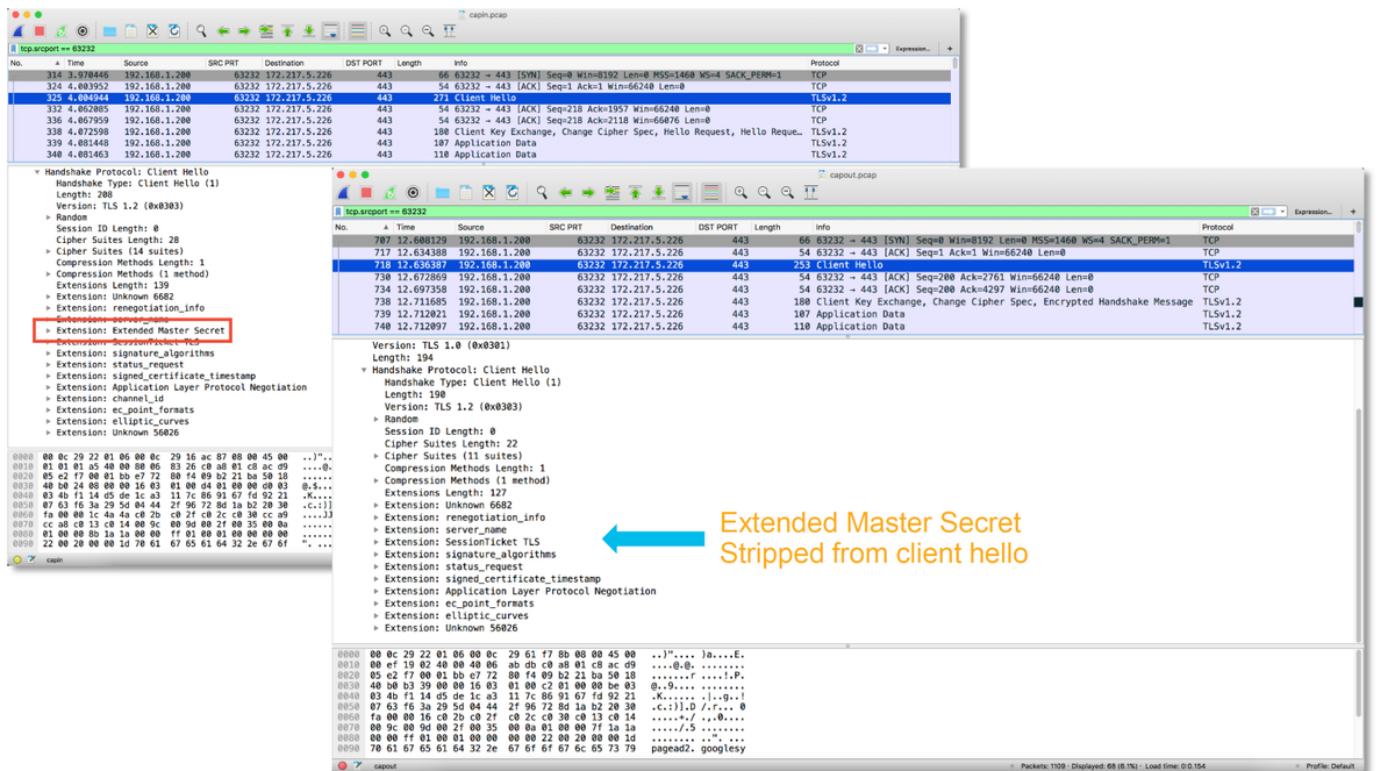
The top screenshot shows a network capture with a red arrow pointing to the error message "SSL Decryption fails". The bottom screenshot shows a network capture with a blue arrow pointing to the decrypted data, including a "POST /comet HTTP/1.1" request.

**Vorsicht:** Vor der Übermittlung einer entschlüsselten PCAP-Erfassung an das TAC wird empfohlen, die Erfassungsdatei herauszufiltern und auf die problematischen Datenflüsse zu beschränken, um zu vermeiden, dass vertrauliche Daten unnötig preisgegeben werden.

## Suchen Sie nach Client Hello Modifications (CHMod).

Die Paketerfassung kann auch ausgewertet werden, um festzustellen, ob eine Client-Hello-Änderung stattfindet.

Die Paketerfassung links zeigt den ursprünglichen Client hello. Das rechte zeigt die serverseitigen Pakete. Beachten Sie, dass der erweiterte Master-geheim über die CHMod-Funktion in Firepower entfernt wurde.



## Vergewissern Sie sich, dass Client-Trusts CA für Entschlüsselung/Rücktritt zurückweisen

Bei SSL-Richtlinienregeln mit der Aktion "Entschlüsseln - Zurücktreten" müssen Sie sicherstellen, dass der Client-Host der Zertifizierungsstelle (Certificate Authority, CA) vertraut, die als die ausscheidende Zertifizierungsstelle verwendet wird. Die Endbenutzer sollten keine Anzeichen dafür haben, dass sie von der Firewall in der Mitte sitzen. Sie sollten der signierenden CA vertrauen. Dies wird in der Regel durch Active Directory (AD)-Gruppenrichtlinien durchgesetzt, hängt jedoch von der Unternehmensrichtlinie und der AD-Infrastruktur ab.

Weitere Informationen finden Sie im folgenden [Artikel](#), in dem das Erstellen einer SSL-Richtlinie beschrieben wird.

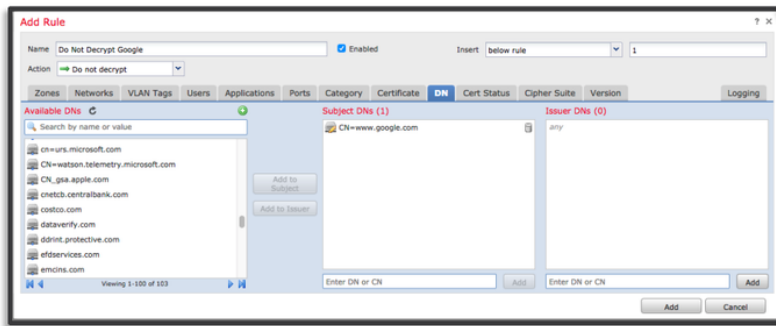
## Schritte zur Risikominimierung

Es können einige grundlegende Eindämmungsschritte befolgt werden, um:

- Konfigurieren Sie die SSL-Richtlinie erneut, um bestimmten Datenverkehr nicht zu entschlüsseln.
- Entfernen bestimmter Daten aus einem Client-Hello-Paket, damit die Entschlüsselung erfolgreich durchgeführt werden kann

## Nicht entschlüsseln (DND)-Regeln hinzufügen

Im folgenden Beispielszenario wurde festgestellt, dass der Datenverkehr zu google.com beim Durchlaufen der SSL Policy Inspection unterbrochen wird. Es wird eine Regel hinzugefügt, die auf dem Common Name (CN) im Serverzertifikat basiert, sodass der Datenverkehr zu google.com nicht entschlüsselt wird.



#	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

Nach dem Speichern und Bereitstellen der Richtlinie können die oben beschriebenen Schritte zur Fehlerbehebung erneut befolgt werden, um zu sehen, was FirePOWER mit dem Datenverkehr macht.

## Optimierung von Client-Hello-Änderungen

In einigen Fällen kann die Fehlerbehebung ergeben, dass die FirePOWER-Lösung bei der Entschlüsselung von bestimmtem Datenverkehr auf ein Problem trifft. Das **System-Support-**Dienstprogramm **ssl-client-hello-Tuning** kann auf der CLI ausgeführt werden, damit FirePOWER bestimmte Daten aus einem Client-Hello-Paket entfernt.

Im folgenden Beispiel wird eine Konfiguration hinzugefügt, sodass bestimmte TLS-Erweiterungen entfernt werden. Die numerischen IDs werden durch die Suche nach Informationen zu TLS-Erweiterungen und -Standards ermittelt.

**Vorsicht:** Der Snort-Prozess muss neu gestartet werden, bevor die Änderungen an der Client-Hello-Änderung wirksam werden, wodurch einige Pakete verworfen werden können. Stateful-Protokolle wie TCP-Datenverkehr werden erneut übertragen, aber anderer Datenverkehr, z. B. UDP, kann negativ beeinflusst werden.

```
> 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



Um Änderungen an den Einstellungen für die Client-Hello-Änderung rückgängig zu machen, kann der Befehl **ssl-client-hello-reset** implementiert werden.

## Daten für TAC

### Daten

Fehlerbehebung für  
Dateien vom  
FirePOWER  
Management Center  
(FMC) und  
FirePOWER-Geräten  
SSL-Debugger  
Erfassung von  
Sitzungspaketen  
(clientseitig,  
FirePOWER-Gerät  
selbst und, wenn  
möglich, serverseitig)  
Screenshots oder  
Berichte zu  
Verbindungsereignissen

### Anweisungen

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/11>

Anweisungen hierzu finden Sie in diesem Artikel

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

Anweisungen hierzu finden Sie in diesem Artikel

## Nächster Schritt

Wenn festgestellt wurde, dass die Komponente SSL Policy nicht die Ursache des Problems ist, besteht der nächste Schritt darin, eine Fehlerbehebung für die Funktion Active Authentication (Aktive Authentifizierung) durchzuführen.

Klicken Sie [hier](#), um mit dem nächsten Artikel fortzufahren.