

Fase 5 della risoluzione dei problemi del percorso dei dati di Firepower: Criterio SSL

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Risoluzione dei problemi relativi alla fase dei criteri SSL](#)

[Controllare i campi SSL negli eventi di connessione](#)

[Debug del criterio SSL](#)

[Genera acquisizione pacchetto decrittografato](#)

[Cerca modifiche Hello client \(CHMod\)](#)

[Verificare che il client sia attendibile e che la CA venga riassegnata per la decrittografia o le dimissioni](#)

[Fasi di mitigazione](#)

[Aggiungi regole Do Not Decrypt \(DnD\)](#)

[Ottimizzazione modifiche Hello client](#)

[Dati da fornire a TAC](#)

[Passaggio successivo](#)

Introduzione

Questo articolo fa parte di una serie di articoli che spiegano come risolvere in modo sistematico i problemi relativi al percorso dei dati nei sistemi Firepower per determinare se i componenti di Firepower possono influire sul traffico. Per informazioni sull'architettura delle piattaforme Firepower e per i collegamenti agli altri articoli sulla risoluzione dei problemi relativi ai percorsi di dati, consultare l'[articolo](#) di [panoramica](#).

In questo articolo viene illustrata la quinta fase della risoluzione dei problemi relativi al percorso dati di Firepower, ovvero la funzionalità dei criteri SSL (Secure Sockets Layer).



Prerequisiti

- Le informazioni di questo articolo si applicano a tutte le piattaforme Firepower Decrittografia SSL per Adaptive Security Appliance (ASA) con servizi FirePOWER (modulo SFR) disponibile solo in 6.0+La funzione Modifica Hello del client è disponibile solo in 6.1+
- Confermare l'utilizzo del criterio SSL nei criteri di controllo di accesso

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

- Verificare che la registrazione sia attivata per tutte le regole, inclusa l'azione predefinita

#	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:

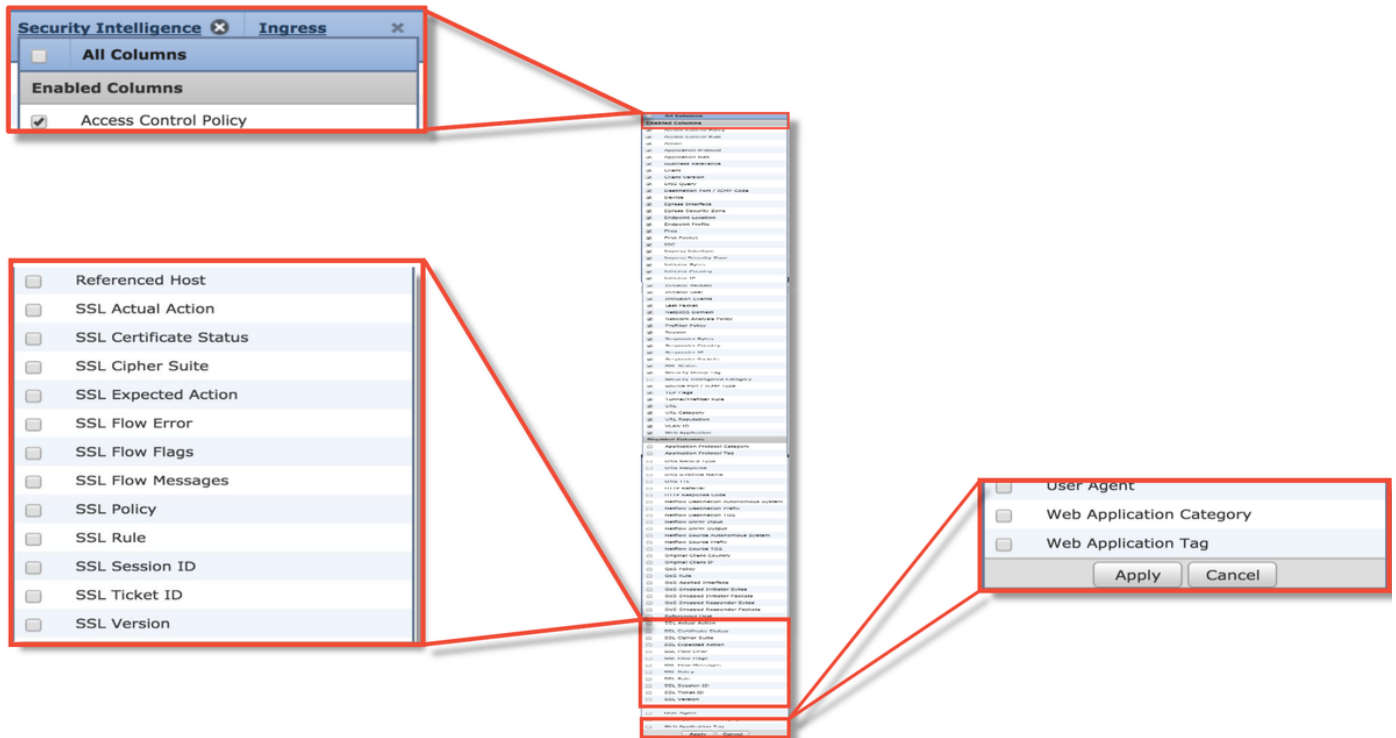
Event Viewer

Syslog

SNMP Trap

Save Cancel

- Selezionare la scheda Azioni non decrittografabili per verificare se sono impostate opzioni per bloccare il traffico
 - Negli eventi di connessione, nella visualizzazione per tabella degli eventi di connessione, abilitare tutti i campi con 'SSL' nel nome
- La maggior parte di essi è disattivata per impostazione predefinita e deve essere attivata nel visualizzatore Eventi connessione



Risoluzione dei problemi relativi alla fase dei criteri SSL

È possibile seguire passaggi specifici per comprendere perché i criteri SSL potrebbero eliminare il traffico che si prevede verrà autorizzato.

Controllare i campi SSL negli eventi di connessione

Se si sospetta che il criterio SSL causi problemi di traffico, controllare innanzitutto la sezione Eventi di connessione (in **Analisi > Connessioni > Eventi**) dopo aver abilitato tutti i campi SSL, come descritto in precedenza.

Se il criterio SSL blocca il traffico, il campo **Reason** (Motivo) visualizza "SSL Block" (Blocco SSL). La colonna **Errore di flusso SSL** contiene informazioni utili sul motivo per cui si è verificato il blocco. Gli altri campi SSL contengono informazioni sui dati SSL rilevati da Firepower nel flusso.

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

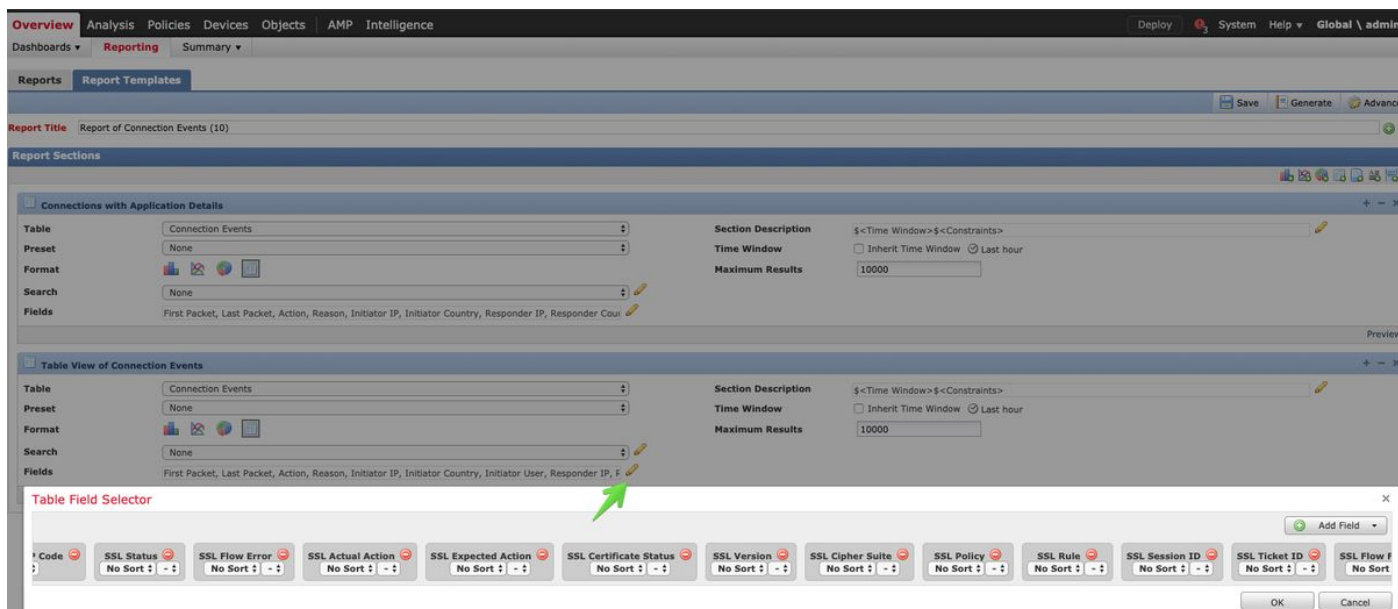
Questi dati possono essere forniti al Cisco Technical Assistance Center (TAC) quando apre una richiesta per la policy SSL. Per esportare facilmente queste informazioni, è possibile utilizzare il pulsante **Report Designer** nell'angolo superiore destro.

Se si fa clic su questo pulsante nella sezione Eventi connessione, le opzioni dei filtri e della finestra temporale vengono copiate automaticamente nel modello di report.

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

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

Accertarsi che tutti i campi SSL menzionati siano aggiunti nella sezione 'Campo'.



Fare clic su **Generate** (Genera) per creare un report sui formati PDF o CSV.

Debug del criterio SSL

Se gli eventi di connessione non contengono informazioni sufficienti sul flusso, è possibile eseguire il debug SSL nell'interfaccia CLI (Command Line Interface) di Firepower.

Nota: Tutto il contenuto di debug riportato di seguito si basa sulla decrittografia SSL eseguita nel software dell'architettura x86. Il contenuto non include i debug da funzionalità di offload hardware SSL aggiunte nella versione 6.2.3 e successive, che sono diverse.

Nota: Sulle piattaforme Firepower 9300 e 4100, è possibile accedere alla shell in questione tramite i seguenti comandi:

```
# connessi console modulo 1
Firepower-module1> connessione ftd
>
```

Per le istanze multiple, è possibile accedere alla CLI del dispositivo logico con i seguenti comandi.

```
# connect module 1 telnet
Firepower-module1> connessione ftd ftd1
Connessione alla console ftd(ftd1) del contenitore in corso... immettere "exit" per tornare alla
CLI di avvio
>
```

È possibile eseguire il comando **system support ssl-debug debug_policy_all** per generare informazioni di debug per ogni flusso elaborato dal criterio SSL.

Attenzione: Il processo di snort deve essere riavviato prima e dopo l'esecuzione del debug SSL. Ciò può causare l'eliminazione di alcuni pacchetti a seconda dei criteri di snort-down e della distribuzione utilizzati. Il traffico TCP verrà ritrasmesso, ma il traffico UDP potrebbe essere influenzato negativamente se le applicazioni che passano attraverso il firewall non tollerano la perdita minima di pacchetti.

```

> 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

Avviso: Non dimenticare di disattivare il debug dopo aver raccolto i dati necessari con il comando **system support ssl-debug-reset**.

Verrà scritto un file per ogni processo di snort in esecuzione sul dispositivo Firepower. Il percorso dei file sarà:

- **/var/common** per piattaforme non FTD
- **/ngfw/var/common** per piattaforme FTD

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

Questi sono alcuni dei campi utili nei log di debug.


```

...
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;


```

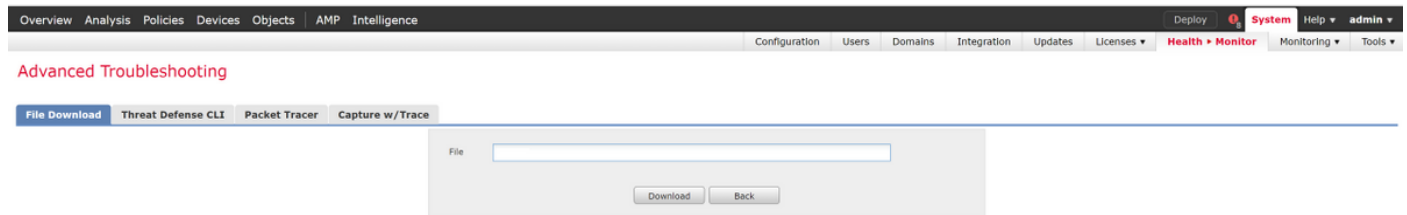
SSL Errors potentially causing drop

Nota: Se si verifica un errore di decrittografia dopo l'inizio della decrittografia da parte di Firepower, il traffico deve essere interrotto in quanto il firewall ha già modificato/man-in-the-

middled la sessione, quindi non è possibile per il client e il server riprendere la comunicazione in quanto hanno stack TCP diversi e chiavi di crittografia diverse utilizzate nel flusso.

I file di debug possono essere copiati dal prompt > del dispositivo Firepower usando le istruzioni riportate in questo [articolo](#).

In alternativa, è disponibile un'opzione sul FMC in Firepower versione 6.2.0 e successive. Per accedere all'utilità UI nel FMC, selezionare **Dispositivi > Gestione dispositivi**. Quindi, fare clic sul pulsante  accanto al dispositivo in questione, quindi selezionare **Advanced Troubleshooting > File Download**. È quindi possibile immettere il nome del file in questione e fare clic su Download.



Genera acquisizione pacchetto decrittografato

È possibile raccogliere un pacchetto non crittografato acquisito per le sessioni che vengono decrittografate da Firepower. Il comando è **system support debug-DAQ debug_daq_write_cap**

Attenzione: È necessario riavviare il processo di snort prima di generare l'acquisizione dei pacchetti decrittografati, che può causare l'eliminazione di alcuni pacchetti. I protocolli stateful, ad esempio il traffico TCP, vengono ritrasmessi, ma il traffico di altro tipo, ad esempio UDP, può essere influenzato negativamente.

```
> 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 list of network packets. A red arrow points to a packet with the following details:

- No. 1785
- Time: 18.374222
- Source: 192.168.1.200
- Destination: 172.217.8.10
- Protocol: TCP
- Length: 54
- Info: 443 → 59113 [RST] Seq=190 Win=262140
- Src Port: 59117
- Dst Port: 443

 An orange arrow points to this entry with the text "SSL Decryption fails".

The bottom screenshot shows a detailed view of a packet. A red arrow points to the "Hypertext Transfer Protocol" section, which contains the following text:


```

    * [Expert Info (Warn/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
    (Severity level: Warn)
    [Group: Security]
    * POST /comet HTTP/1.1 [URL]
    [Security level: Chat]
    [Group: Sequence]
    [Request Method]: POST
    [Request URI]: /comet HTTP/1.1 [URL]
    [Request Headers]:
    Host: 172.217.8.10
    Content-Type: application/json
    Accept: */*
    Connection: keep-alive
    
```

 An orange arrow points to this section with the text "Successful SSL Decryption".

Attenzione: Prima di inviare una cattura PCAP decrittografata a TAC, si consiglia di filtrare e limitare il file di cattura ai flussi problematici, in modo da evitare di rivelare inutilmente dati sensibili.

Cerca modifiche Hello client (CHMod)

L'acquisizione del pacchetto può anche essere valutata per verificare se sono in corso modifiche hello del client.

L'acquisizione del pacchetto a sinistra rappresenta il saluto originale del cliente. Quello a destra mostra i pacchetti sul lato server. Si noti che il master secret esteso è stato rimosso tramite la funzionalità CHMod in Firepower.

The image displays two screenshots from the Wireshark network protocol analyzer. The top screenshot shows a list of network packets. Packet 253 is highlighted, which is a 'Client Hello' message. The bottom screenshot shows the expanded details of this packet. In the 'Extensions' section, the 'Extended Master Secret' extension is highlighted with a red box. A blue arrow points from the text 'Extended Master Secret Stripped from client hello' to this extension, indicating that this extension is missing from the client's hello message.

Verificare che il client sia attendibile e che la CA venga riassegnata per la decrittografia o le dimissioni

Per le regole dei criteri SSL con un'azione "Decrittografia - Abbandona", verificare che il client ospiti l'Autorità di certificazione (CA) utilizzata come CA che si sta dimettendo. Gli utenti finali non devono avere alcuna indicazione del fatto che sono in contatto diretto con il firewall. La CA di firma deve essere considerata attendibile. Questa impostazione viene in genere applicata tramite Criteri di gruppo di Active Directory (AD), ma dipende dai criteri aziendali e dall'infrastruttura AD.

Per ulteriori informazioni, vedere [l'articolo](#) seguente, in cui viene descritto come creare un criterio SSL.

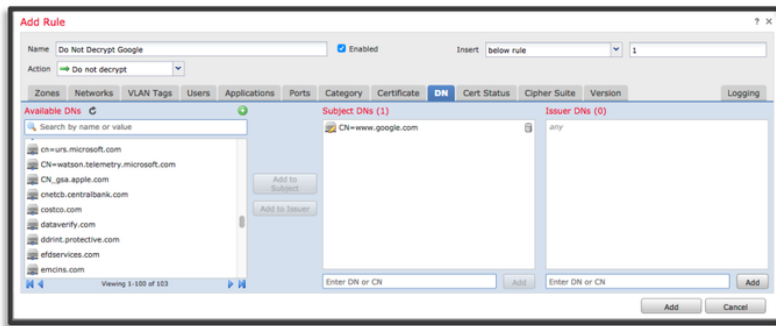
Fasi di mitigazione

È possibile eseguire alcune operazioni di mitigazione di base per:

- Riconfigurare il criterio SSL per non decrittografare determinati traffici
- Eliminare alcuni dati da un pacchetto hello client in modo che la decrittografia abbia esito positivo

Aggiungi regole Do Not Decrypt (DnD)

Nello scenario di esempio seguente è stato determinato che il traffico verso google.com si interrompe durante il passaggio attraverso l'ispezione dei criteri SSL. Viene aggiunta una regola basata sul nome comune (CN) nel certificato del server in modo che il traffico verso google.com non venga decrittografato.



#	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	MtM	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action												Do not decrypt	

Dopo aver salvato e distribuito il criterio, è possibile seguire nuovamente le procedure di risoluzione dei problemi descritte in precedenza per verificare l'azione di Firepower sul traffico.

Ottimizzazione modifiche Hello client

In alcuni casi, la risoluzione dei problemi può rivelare che Firepower sta riscontrando un problema con la decrittografia di determinati traffici. L'utilità **system support ssl-client-hello-tuning** può essere eseguita sulla CLI per fare in modo che Firepower rimuova alcuni dati da un pacchetto client hello.

Nell'esempio seguente viene aggiunta una configurazione che consente di rimuovere alcune estensioni TLS. Gli ID numerici vengono trovati cercando informazioni sulle estensioni e gli standard TLS.

Attenzione: Il processo di snort deve essere riavviato prima che le modifiche apportate alla hello del client abbiano effetto, il che può causare l'eliminazione di alcuni pacchetti. I protocolli stateful, ad esempio il traffico TCP, vengono ritrasmessi, ma il traffico di altro tipo, ad esempio UDP, può essere influenzato negativamente.

```
> 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



Per ripristinare le modifiche apportate alle impostazioni hello del client, è possibile implementare il comando **system support ssl-client-hello-reset**.

Dati da fornire a TAC

Dati Istruzioni

Risoluzione
dei problemi
dei file da

Firepower

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

(FMC) e dai
dispositivi

Firepower

Debug SSL Per istruzioni, vedere questo articolo

Acquisizione
completa dei
pacchetti

della
sessione

(dal lato

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

dispositivo

Firepower e

dal lato

server

quando

possibile)

Screenshot

o report degli
eventi di Per istruzioni, vedere questo articolo

connessione

Passaggio successivo

Se è stato determinato che il componente Criteri SSL non è la causa del problema, il passaggio successivo consiste nella risoluzione dei problemi relativi alla funzionalità Autenticazione attiva.

Fare clic [qui](#) per continuare con l'articolo successivo.