

Fase 5 de Troubleshooting de Trayectoria de Datos de Firepower: Política SSL

Contenido

[Introducción](#)

[Prerequisites](#)

[Solución de problemas de la fase de política SSL](#)

[Compruebe los campos SSL en los eventos de conexión](#)

[Depurar la política SSL](#)

[Generar una captura de paquetes descifrados](#)

[Buscar modificaciones de saludo de cliente \(CHMod\)](#)

[Asegúrese De Que El Cliente Confía En Renunciar A CA Para Descifrar/Renunciar](#)

[Pasos de mitigación](#)

[Agregar reglas No descifrar \(DnD\)](#)

[Ajuste de modificación de saludo del cliente](#)

[Datos que se deben proporcionar al TAC](#)

[Siguiete paso](#)

Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el [artículo Descripción general](#) para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a otros artículos de Troubleshooting de Trayectoria de Datos.

En este artículo se describe la quinta etapa de la solución de problemas de la ruta de datos de Firepower, la función Secure Sockets Layer (SSL) Policy.



Prerequisites

- La información de este artículo se aplica a cualquier plataforma Firepower Descifrado SSL para Adaptive Security Appliance (ASA) con FirePOWER Services (módulo SFR) solo disponible en más de 6.0La función de modificación de saludo del cliente sólo está disponible en 6.1+
- Confirme que la política SSL se está utilizando en la política de control de acceso

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 **TEST_SSL_POLICY**

- Verifique que el registro esté habilitado para todas las reglas, incluida la 'Acción predeterminada'

| # | 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:

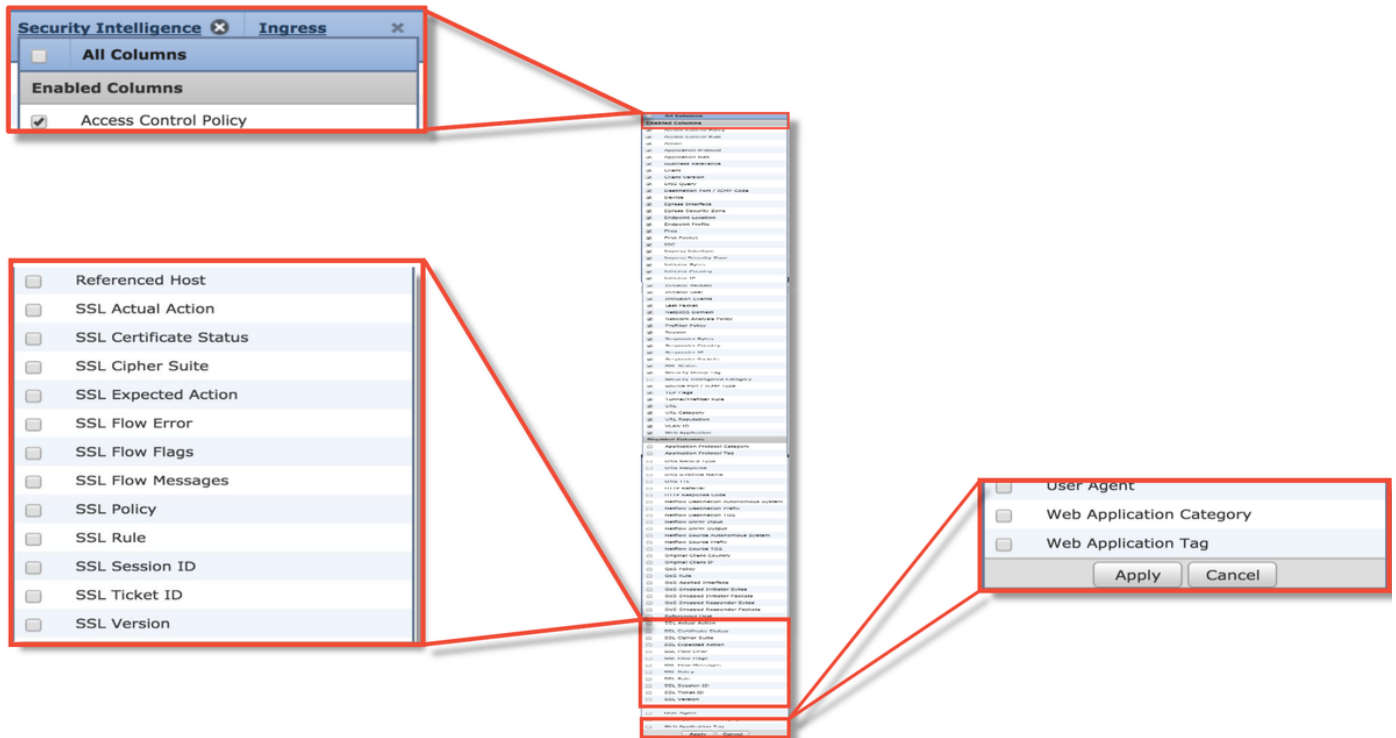
Log at End of Connection Enable Logging

Send Connection Events to:

- Event Viewer
- Syslog Select a Syslog Alert Configuration...
- SNMP Trap Select an SNMP Alert Configuration...

Save Cancel

- Verifique la ficha Undecryptable Actions (Acciones descifrables) para ver si hay alguna opción configurada para bloquear el tráfico
- En los eventos Connection, cuando se encuentre en la vista de tabla de los eventos de conexión, active todos los campos con 'SSL' en el nombre
La mayoría de ellas están desactivadas de forma predeterminada y deben habilitarse en el visor de eventos de conexión



Solución de problemas de la fase de política SSL

Se pueden seguir pasos específicos para ayudar a entender por qué la política SSL puede estar descartando el tráfico que se espera que se permita.

Compruebe los campos SSL en los eventos de conexión

Si se sospecha que la política SSL causa problemas de tráfico, el primer lugar para verificar es la sección Eventos de conexión (en **Análisis > Conexiones > Eventos**) después de habilitar todos los campos SSL, como se ha descrito anteriormente.

Si la política SSL está bloqueando el tráfico, el campo **Motivo** muestra "Bloque SSL". La columna **SSL Flow Error** contiene información útil sobre el motivo del bloqueo. Los otros campos SSL tienen información sobre los datos SSL que Firepower detectó en el flujo.

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 | 192.16 | | | |
| 2017-05-30 13:08:19 | 2017-05-30 13:08:20 | Block | SSL Block | 192.16 | | | |
| 2017-05-30 13:07:53 | 2017-05-30 13:07:54 | Block | SSL Block | 192.16 | | | |
| 2017-05-30 13:07:23 | 2017-05-30 13:07:24 | Block | SSL Block | 192.16 | | | |

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 |

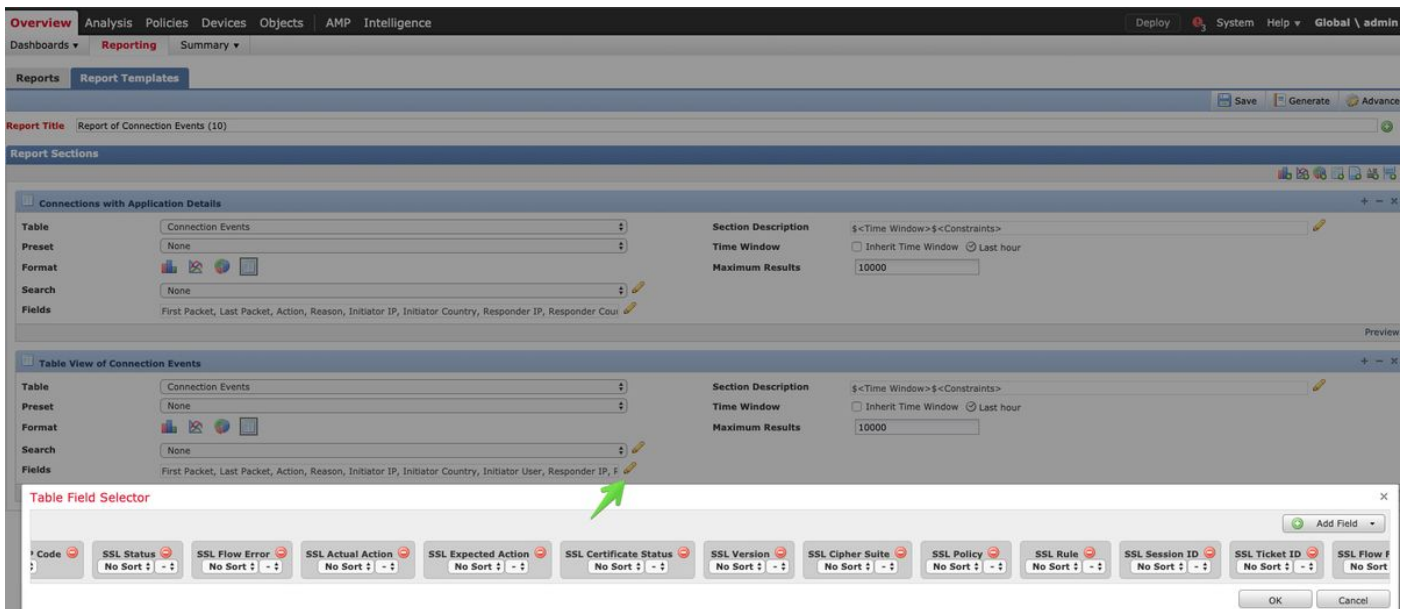
Estos datos se pueden proporcionar al centro de asistencia técnica Cisco Technical Assistance Center (TAC) al abrir un caso para la política SSL. Para exportar fácilmente esta información, se puede utilizar el botón **Diseñador de informes** de la esquina superior derecha.

Si se hace clic en este botón en la sección Eventos de conexión, las opciones de los filtros y de la ventana de tiempo se copiarán automáticamente en la plantilla de informe.

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

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

Asegúrese de que todos los campos SSL mencionados se agregan en la sección "Campo".



Haga clic en **Generar** para crear un informe en formatos PDF o CSV.

Depurar la política SSL

Si los eventos de conexión no contienen suficiente información sobre el flujo, la depuración SSL se puede ejecutar en la interfaz de línea de comandos (CLI) de Firepower.

Nota: Todo el contenido de depuración que se muestra a continuación se basa en el descifrado SSL que ocurre en el software en la arquitectura x86. Este contenido no incluye las depuraciones de las funciones de descarga de hardware SSL que se agregaron en la versión 6.2.3 y en versiones posteriores, que son diferentes.

Nota: En las plataformas Firepower 9300 y 4100, se puede acceder al shell en cuestión a través de los siguientes comandos:

```
# connect module 1 console
Firepower-module1> connect ftd
>
```

Para múltiples instancias, se puede acceder a la CLI del dispositivo lógico con los siguientes comandos.

```
# connect module 1 telnet
Firepower-module1> connect ftd1
Conectando con la consola ftd(ftd1) del contenedor... introduzca "exit" para volver a Boot
CLI
>
```

El comando **system support ssl-debug debug debug_policy_all** se puede ejecutar para generar información de depuración para cada flujo procesado por la política SSL.

Precaución: El proceso snort debe reiniciarse antes y después de ejecutar el debug SSL, lo que puede hacer que se descarten algunos paquetes según las políticas de snort-down y la implementación utilizada. El tráfico TCP se retransmitirá, pero el tráfico UDP puede verse afectado negativamente si las aplicaciones que pasan a través del firewall no toleran la

pérdida mínima de paquetes.

```
> 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

Advertencia: No olvide apagar la depuración después de que se recopile los datos necesarios con el comando **system support ssl-debug-reset**.

Habrà un archivo escrito para cada proceso de sondeo que se ejecute en el dispositivo Firepower. La ubicación de los archivos será:

- /var/common para plataformas que no son FTD
- /ngfw/var/common para las plataformas FTD

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 getCHDDigestToSCFingerprintMapping: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

Estos son algunos de los campos útiles en los registros de depuración.


```

...
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;
...


```

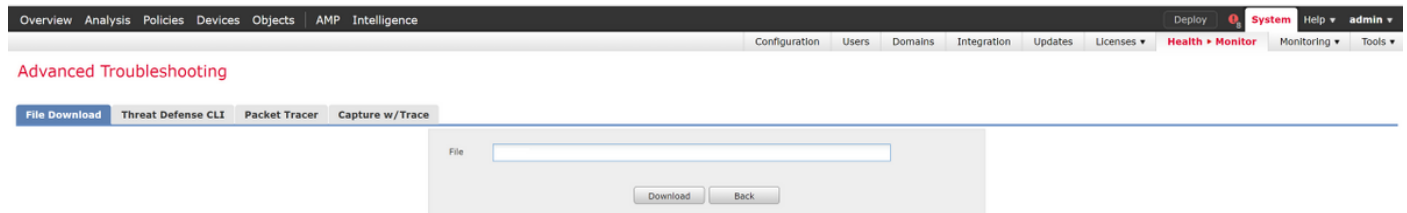
SSL Errors potentially causing drop

Nota: Si hay un error con el descifrado que ocurre después de que Firepower comience a descifrar, el tráfico debe descartarse ya que el firewall ya ha modificado/man-in-the-middle

la sesión, por lo que no es posible que el cliente y el servidor reanuden la comunicación ya que tienen diferentes pilas TCP así como diferentes claves de cifrado utilizadas en el flujo.

Los archivos de depuración se pueden copiar del dispositivo Firepower desde el mensaje > utilizando las instrucciones de este [artículo](#).

Alternativamente, hay una opción en el FMC en Firepower versión 6.2.0 y posterior. Para acceder a esta utilidad de interfaz de usuario en el FMC, navegue hasta **Dispositivos > Administración de dispositivos**. A continuación, haga clic en el botón  junto al dispositivo en cuestión, seguido de **Resolución de problemas avanzada > Descarga de archivos**. A continuación, puede introducir el nombre de un archivo en cuestión y hacer clic en Descargar.



Generar una captura de paquetes descifrados

Es posible recopilar una captura de paquetes sin cifrar para las sesiones que se descifran mediante Firepower. El comando es **system support debug-DAQ debug_daq_write_pcap**

Precaución: El proceso snort debe reiniciarse antes de generar la captura de paquetes descifrados, lo que puede hacer que se descarten algunos paquetes. Los protocolos de estado como el tráfico TCP se retransmiten, pero otro tráfico, como UDP, puede verse afectado 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_*
```


SSL Decryption fails

Successful SSL Decryption

Warning: [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 [x] [x]
 [Expert Info (Chat/Sequence): POST /comet HTTP/1.1 [x] [x]
 [Group: Security]
 * POST /comet HTTP/1.1 [x] [x]
 [Severity level: Chat]
 [Group: Sequence]
 [Banner: Method: POST
 0000 00 00 20 16 ac 87 00 0c 29 22 01 06 00 45 80].....E
 0010 00 31 00 00 00 00 00 83 74 ac 09 08 0a c8 80].....P
 0020 01 c8 01 00 00 e0 00 04 e0 83 cf ba 00 0c 50 10].....P
 0030 ff ff 31 5e 00 00 10 03 03 00 04 0e 00 00 00].....

Precaución: Antes de enviar una captura PCAP descifrada al TAC, se recomienda filtrar y limitar el archivo de captura a los flujos problemáticos, a fin de evitar la revelación innecesaria de cualquier dato sensible.

Buscar modificaciones de saludo de cliente (CHMod)

La captura de paquetes también se puede evaluar para ver si se está produciendo alguna modificación de saludo del cliente.

La captura de paquetes a la izquierda representa el hello del cliente original. El de la derecha muestra los paquetes del lado del servidor. Observe que el secreto maestro extendido se ha eliminado a través de la función CHMod en Firepower.

The image displays two screenshots of Wireshark network traffic analysis. The top screenshot shows a TLSv1.2 Client Hello packet with the 'Extended Master Secret' extension highlighted in red. The bottom screenshot shows a TLSv1.2 Client Hello packet with the 'Extended Master Secret' extension highlighted in orange and a blue arrow pointing to it from the text 'Extended Master Secret Stripped from client hello'.

Asegúrese De Que El Cliente Confía En Renunciar A CA Para Descifrar/Renunciar

Para las reglas de política SSL con una acción de "Descifrar - Renuncia", asegúrese de que los hosts del cliente confían en la Autoridad de Certificados (CA) utilizada como la CA que renuncia. Los usuarios finales no deben tener ninguna indicación de que el firewall los está metiendo. Deben confiar en la CA firmante. Esto suele aplicarse a través de la política de grupo de Active Directory (AD), pero depende de la política de la empresa y de la infraestructura de AD.

Para obtener más información, puede revisar el siguiente [artículo](#), que describe cómo crear una política SSL.

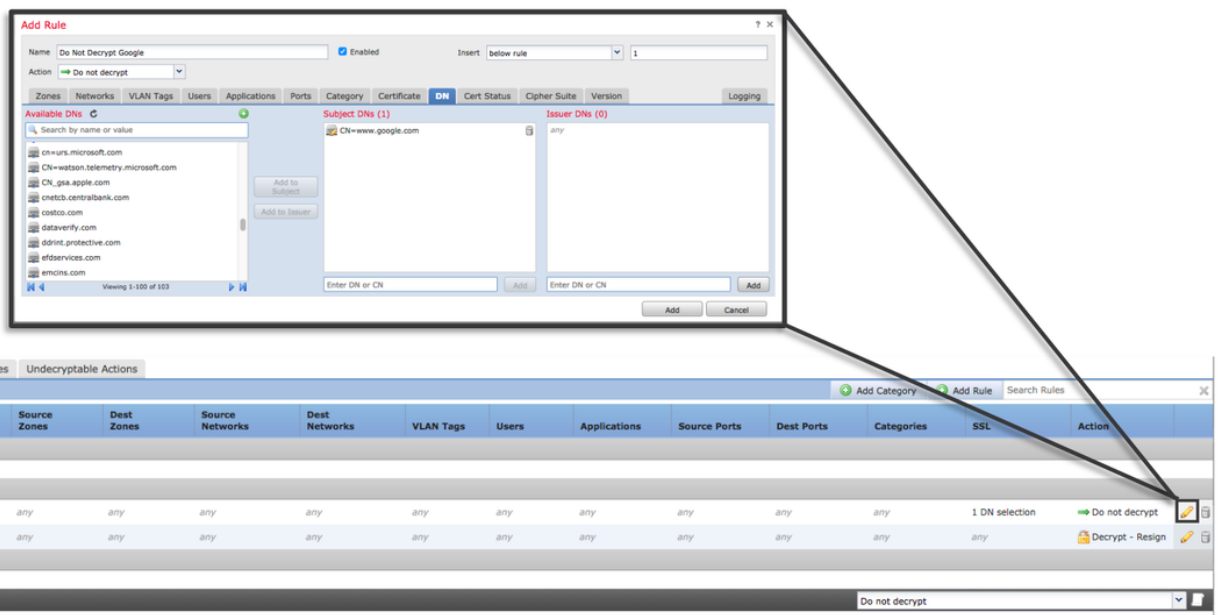
Pasos de mitigación

Se pueden seguir algunos pasos básicos de mitigación para:

- Vuelva a configurar la política SSL para no descifrar cierto tráfico
- Quitar ciertos datos de un paquete hello del cliente para que el descifrado se realice correctamente

Agregar reglas No descifrar (DnD)

En el siguiente escenario de ejemplo, se ha determinado que el tráfico a google.com se interrumpe al pasar por la inspección de la política SSL. Se agrega una regla basada en el nombre común (CN) en el certificado del servidor para que el tráfico a google.com no sea descifrado.



Después de guardar e implementar la política, los pasos de solución de problemas descritos anteriormente se pueden seguir de nuevo para ver lo que Firepower está haciendo con el tráfico.

Ajuste de modificación de saludo del cliente

En algunos casos, la resolución de problemas puede revelar que Firepower se está topando con un problema con el descifrado de cierto tráfico. La utilidad **system support ssl-client-hello-tune** se puede ejecutar en la CLI para hacer que Firepower elimine ciertos datos de un paquete hello de cliente.

En el siguiente ejemplo, se agrega una configuración para que se quiten ciertas extensiones TLS. Los ID numéricos se encuentran buscando información sobre las extensiones y estándares de TLS.

Precaución: El proceso snort debe reiniciarse antes de que los cambios de la modificación hello del cliente entren en vigor, lo que puede hacer que se descarten algunos paquetes. Los protocolos de estado como el tráfico TCP se retransmiten, pero otro tráfico, como UDP, puede verse afectado 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

Para revertir cualquier cambio realizado en la configuración de modificación hello del cliente, se puede implementar el comando **system support ssl-client-hello-reset**.

Datos que se deben proporcionar al TAC

Datos Instrucciones

Solución de
problemas de
archivos de
Firepower
Management
Center (FMC)
y dispositivos

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

Firepower
Depuraciones
SSL

Consulte este artículo para obtener instrucciones

Capturas de
paquetes de
sesión
completa (del
lado del
cliente, del
dispositivo

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

Firepower y
del lado del
servidor
cuando sea
posible)

Capturas de
pantalla o
informes de
eventos de
conexión

Consulte este artículo para obtener instrucciones

Siguiente paso

Si se ha determinado que el componente de política SSL no es la causa del problema, el siguiente paso sería resolver el problema de la función de autenticación activa.

Haga clic [aquí](#) para continuar con el siguiente artículo.