

Firepower数据路径故障排除第5阶段：SSL策略

目录

[简介](#)

[先决条件](#)

[SSL策略阶段故障排除](#)

[检查连接事件中的SSL字段](#)

[调试SSL策略](#)

[生成解密的数据包捕获](#)

[查找客户端问候修改\(CHMod\)](#)

[确保客户信任辞职CA以进行解密/辞职](#)

[缓解步骤](#)

[添加不解密\(DnD\)规则](#)

[客户端Hello修改调整](#)

[向TAC提供的数据](#)

[下一步](#)

简介

本文是一系列文章的一部分，这些文章说明如何系统地排除Firepower系统上的数据路径故障，以确定Firepower的组件是否可能影响流量。有关Firepower平台架构的[信息以及指向其他数据路径故障排除](#)文章的链接，请参阅概述文章。

本文介绍Firepower数据路径故障排除的第五阶段，即安全套接字层(SSL)策略功能。



先决条件

- 本文中的信息适用于任何Firepower平台带FirePOWER服务(SFR模块)的自适应安全设备(ASA)的SSL解密仅在6.0+中提供客户端呼叫修改功能仅在6.1+中可用
- 确认SSL策略正在访问控制策略中使用

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
--	---

- 验证是否已为所有规则 (包括“默认操作”) 启用日志记录

#	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:

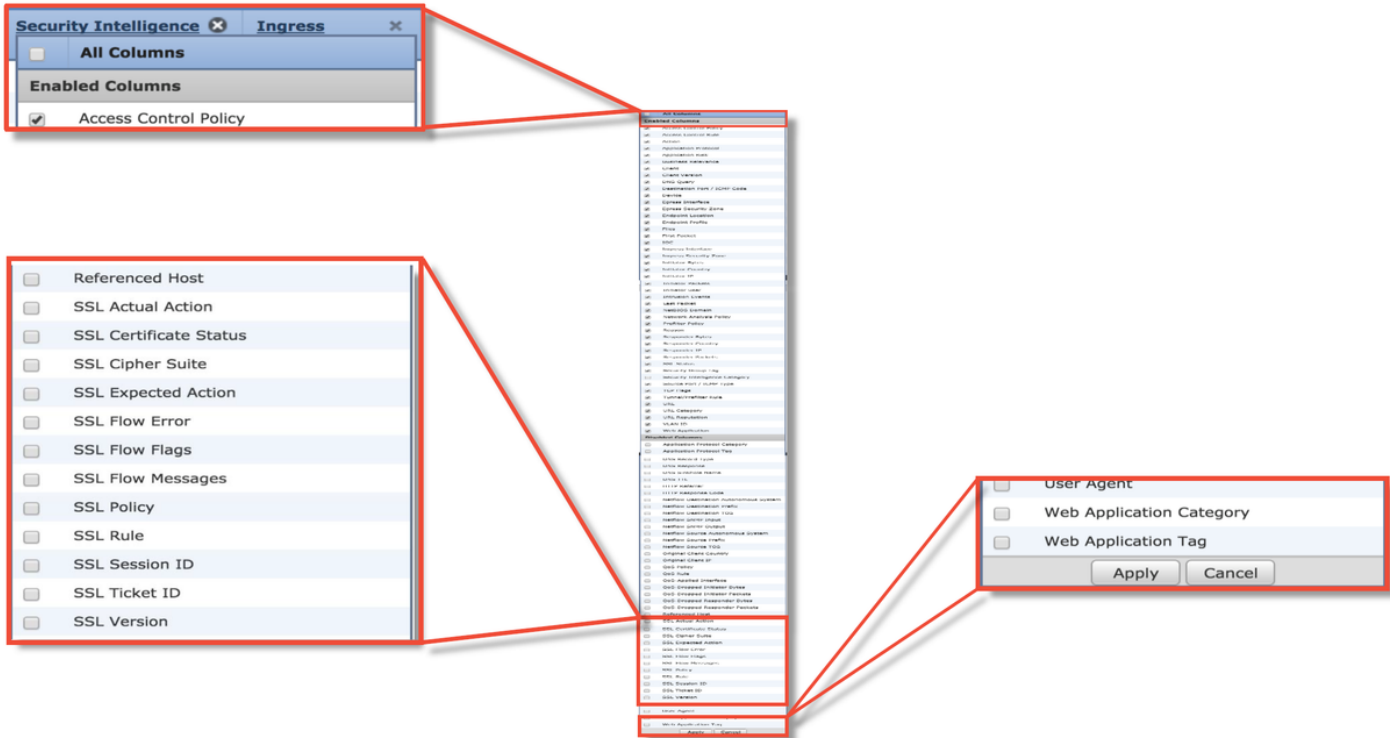
Event Viewer

Syslog

SNMP Trap

Save Cancel

- 选中Undecryptable Actions选项卡，查看是否将任何选项设置为阻止流量
- 在连接事件中，当您处于连接事件的表视图中时，启用名称中带有“SSL”的所有字段
大多数默认禁用，需要在连接事件查看器中启用



SSL策略阶段故障排除

可以执行特定步骤，以帮助了解SSL策略可能丢弃预期允许的流量的原因。

检查连接事件中的SSL字段

如果怀疑SSL策略导致流量问题，首先要检查的是启用所有SSL字段后的Connection Events部分(在Analysis > Connections > Events下)，如上所述。

如果SSL策略阻止流量，则“原因”字段显示“SSL阻止”。“SSL流错误”列包含有关阻止发生原因的有用信息。其他SSL字段包含有关Firepower在流中检测到的SSL数据的信息。

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 Action/Reason columns)

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

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	TLv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLv1.2

SSL flow flags for what happened with flow (points to SSL Flow Flags column)

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_SSESSTKT, SERVER_HELLO_SSESSTKT, 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_SSESSTKT, SERVER_HELLO_SSESSTKT, 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_SSESSTKT, SERVER_HELLO_SSESSTKT, 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_SSESSTKT, SERVER_HELLO_SSESSTKT, 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_SSESSTKT, SERVER_HELLO_SSESSTKT, 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_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE

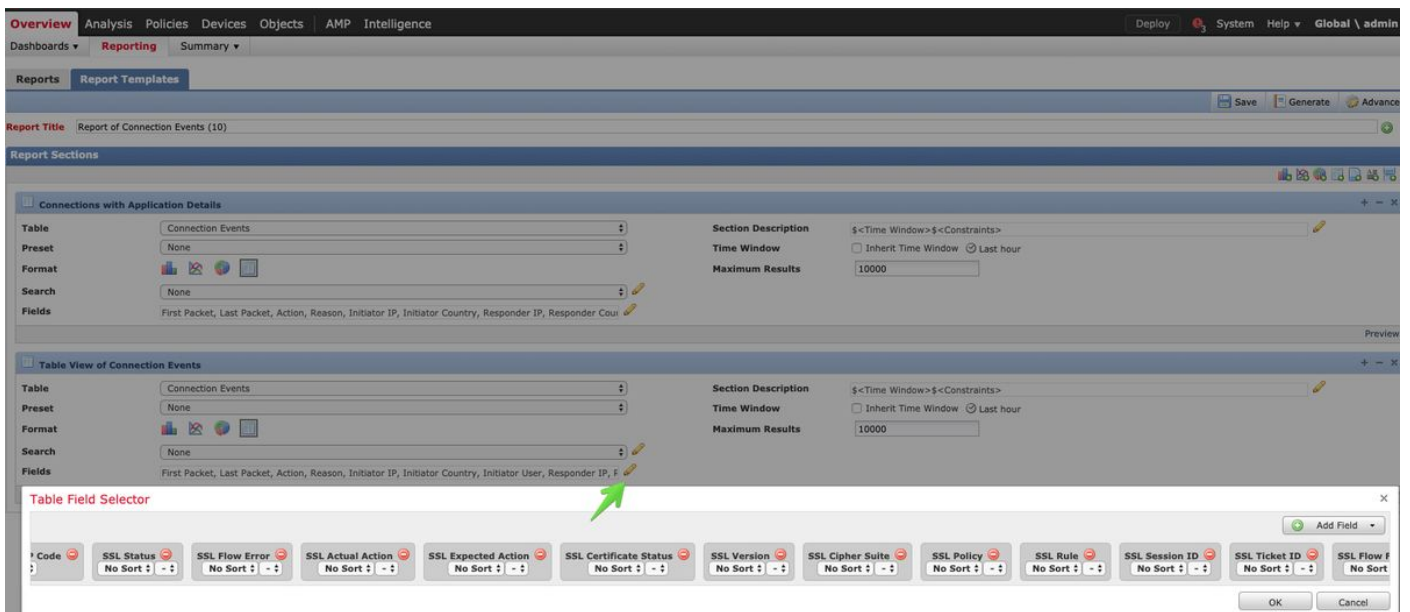
在为SSL策略创建案例时，可向思科技术支持中心(TAC)提供此数据。为了轻松导出此信息，可以使

用右上角的报表设计器按钮。

如果从“连接事件”部分单击此按钮，过滤器和时间窗口选项将自动复制到报告模板。



确保在“字段”部分添加所有提及的SSL字段。



单击“生成”以创建PDF或CSV格式的报告。

调试SSL策略

如果连接事件中没有包含有关流的足够信息，则可以在Firepower命令行界面(CLI)上运行SSL调试。

注意：以下所有调试内容均基于x86架构上软件中发生的SSL解密。此内容不包括来自6.2.3版和2.3版中添加的SSL硬件卸载功能的调试，这些功能不同。

注意：在Firepower 9300和4100平台上，可通过以下命令访问相关外壳：

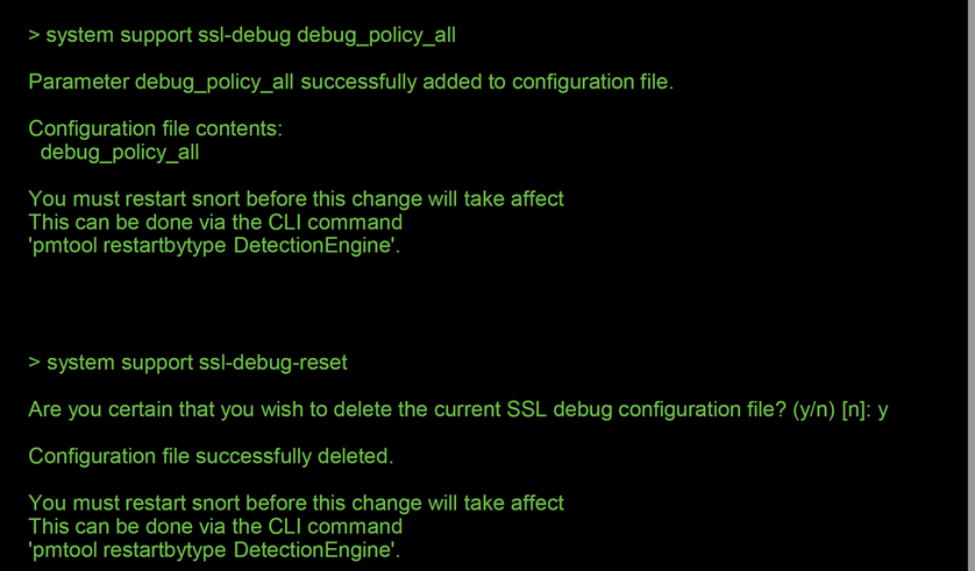
```
# connect module 1 console
Firepower-module1> connect ftd
>
```

对于多实例，可使用以下命令访问逻辑设备CLI。

```
# connect module 1 telnet
Firepower-module1> connect ftd ftd1
正在连接到容器ftd(ftd1)控制台.....输入“exit”以返回引导CLI
>
```

系统支持`ssl-debug debug_policy_all`命令可以运行，以生成SSL策略处理的每个流的调试信息。

警告：在运行SSL调试之前和之后，必须重新启动snort进程，这可能会导致一些数据包被丢弃，具体取决于使用的snort-down策略和部署。TCP流量将被重新传输，但如果通过防火墙的应用不允许最小丢包，UDP流量可能会受到负面影响。



```
> 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

警告：使用`system support ssl-debug-reset`命令收集必要数据后，不要忘记关闭调试功能。

将为Firepower设备上运行的每个snort进程编写一个文件。文件的位置将是：

- `/var/common` (适用于非FTD平台)
- `/ngfw/var/common` (适用于FTD平台)

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 e0ddd02
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

这些是调试日志中的一些有用字段。

```
...
2017-05-30 04:02:05.893 Verdict callback.
Logstr: ssl_policy_decision: Found matching rule.
Process ID: 24383
Flow context: 0x414eae0
Flow info: 0x7f6a4b8ccf0
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: 0x7f6a4b8c9e8 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,
O_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: 0x7f6ea4b8d3a0
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: 0x7f6ea4b8d290
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 ←

注意：如果在Firepower开始解密后出现解密错误，则必须丢弃流量，因为防火墙已修改/中间会话，所以客户端和服务端无法恢复通信，因为它们具有不同的TCP堆栈以及在流中使用的不同加密密钥。

使用本文中的说明，可以从>提示符中从Firepower设备复制调试文件。

或者，在Firepower版本6.2.0及更高版本中，FMC上也有一个选项。要访问FMC上的此UI实用程序，请导航至“设备”>“设备管理”。然后，单击  图标，然后是高级故障排除>文件下载。然后，可以输入有关文件的名称，然后点击Download。



生成解密的数据包捕获

可以为Firepower解密的会话收集未加密的数据包捕获。命令是system support debug-DAQ

debug_daq_write_pcap

警告：在生成解密的数据包捕获之前，必须重新启动Snort进程，这可能导致一些数据包被丢弃。TCP流量等有状态协议会重新传输，但UDP等其他流量可能会受到负面影响。

```
> 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_*
```

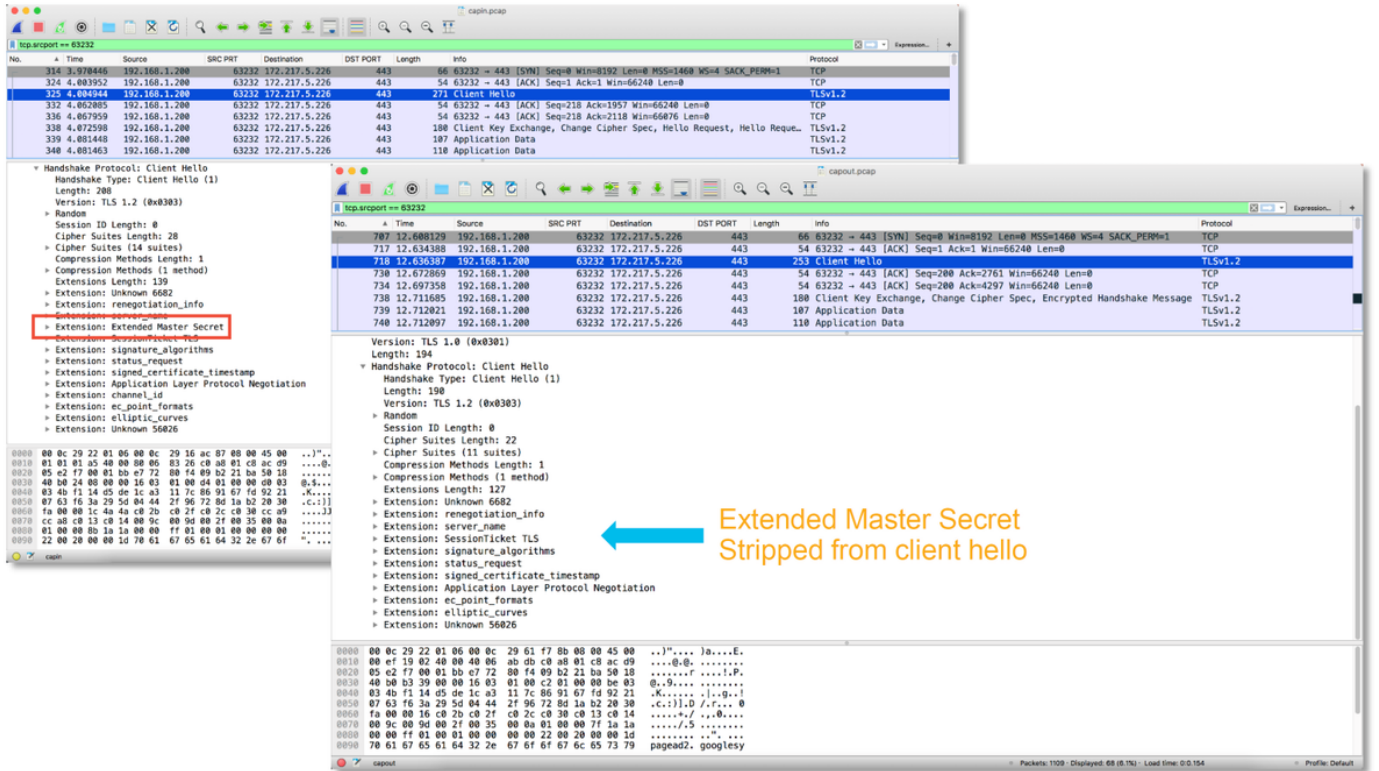
The top screenshot shows a packet capture with a red highlight on a failed SSL decryption attempt. A blue arrow points from the text "SSL Decryption fails" to the corresponding entry in the packet list. The bottom screenshot shows a packet capture with a blue highlight on a successful SSL decryption. A blue arrow points from the text "Successful SSL Decryption" to the corresponding entry in the packet list.

警告：在将解密的PCAP捕获提交到TAC之前，建议过滤并限制捕获文件到有问题的流中，以免不必要地泄露任何敏感数据。

查找客户端问候修改(CHMod)

还可以评估数据包捕获，以查看是否正在进行任何客户端hello修改。

左侧的数据包捕获描述了原始客户端hello。右侧显示的是服务器端数据包。请注意，扩展主密钥已通过Firepower中的CHMod功能删除。



确保客户信任辞职CA以进行解密/辞职

对于具有“解密 — 重新签名”(Decrypt - Resign)操作的SSL策略规则，请确保客户端主机信任用作辞职CA的证书颁发机构(CA)。最终用户不应表明他们是防火墙的中间人。他们应信任签名CA。这通常通过Active Directory(AD)组策略实施，但取决于公司策略和AD基础设施。

有关详细信息，请查看以下[文章](#)，其中概述了如何创建SSL策略。

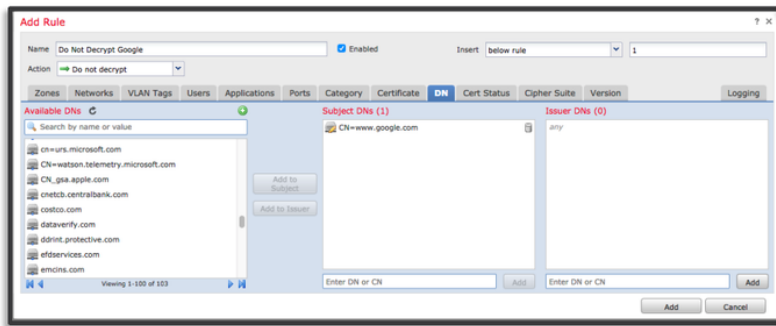
缓解步骤

可以执行一些基本的缓解步骤，以便：

- 重新配置SSL策略以不解密某些流量
- 从客户端Hello数据包中删除某些数据，以便解密成功

添加不解密(DnD)规则

在以下示例场景中，已确定通过SSL策略检查时发往google.com的流量正在中断。根据服务器证书中的公用名(CN)添加规则，以便不解密流向google.com的流量。



#	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	

保存和部署策略后，可以再次执行上述故障排除步骤，以查看Firepower对流量执行的操作。

客户端Hello修改调整

在某些情况下，故障排除可能表明Firepower在解密特定流量时遇到问题。系统支持ssl-client-hello-tuning实用程序可在CLI上运行，以使Firepower从客户端hello数据包中删除某些数据。

在以下示例中，添加了配置，以删除某些TLS扩展。通过搜索有关TLS扩展和标准的信息来找到数字ID。

警告：在客户端hello修改更改生效之前，必须重新启动snort进程，这可能导致一些数据包被丢弃。TCP流量等有状态协议会重新传输，但UDP等其他流量可能会受到负面影响。

```
> 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

要恢复对客户端hello修改设置所做的任何更改，可以实施system support ssl-client-hello-reset命令

向TAC提供的数据

数据

从Firepower管理中心(FMC)和Firepower设备排除文件故障

SSL调试

完整会话数据包捕获 (尽可能从客户端、Firepower设备本身和服务器端)

连接事件屏幕截图或报告

说明

<http://www.cisco.com/c/en/us/s>

有关说明，请参阅本文

<http://www.cisco.com/c/en/us/s>

有关说明，请参阅本文

下一步

如果已确定SSL策略组件不是问题的原因，则下一步是排除活动身份验证功能故障。

单击[此处](#)继续下一篇文章。