

Firepowerデータパスのトラブルシューティング フェーズ5:SSLポリシー

内容

[概要](#)

[前提条件](#)

[SSLポリシーフェーズのトラブルシューティング](#)

[接続イベントのSSLフィールドをチェックする](#)

[SSLポリシーのデバッグ](#)

[復号化されたパケットキャプチャの生成](#)

[クライアントのHelloの変更\(CHMod\)を探します](#)

[クライアントがCAの再署名を信頼して復号化/再署名を行うことを確認する](#)

[緩和手順](#)

[Do Not Decrypt\(DnD\)ルールの追加](#)

[クライアントのHello変更の調整](#)

[TACに提供するデータ](#)

[次のステップ](#)

概要

この記事は、Firepowerシステムのデータパスを体系的にトラブルシューティングし、Firepowerのコンポーネントがトラフィックに影響を与えているかどうかを判断する方法を説明する一連の記事の一部です。Firepowerプラットフォームの[アーキテクチャ](#)に関する情報や、その他のデータパスのトラブルシューティングに関する記事へのリンクについては、概要記事を参照してください。

この記事では、Firepowerデータパスのトラブルシューティングの5番目の段階であるセキュアソケットレイヤ(SSL)ポリシー機能について説明します。



前提条件

- この記事の情報は、すべてのFirepowerプラットフォームに適用されます 適応型セキュリティアプライアンス(ASA)とFirePOWERサービス (SFRモジュール) のSSL復号化は6.0以降でのみ使用可能Client Hello Modification機能は6.1+でのみ使用できます
- アクセスコントロールポリシーでSSLポリシーが使用されていることを確認します

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

- [Default Action]を含むすべてのルールでロギングが有効になっていることを確認します

#	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:

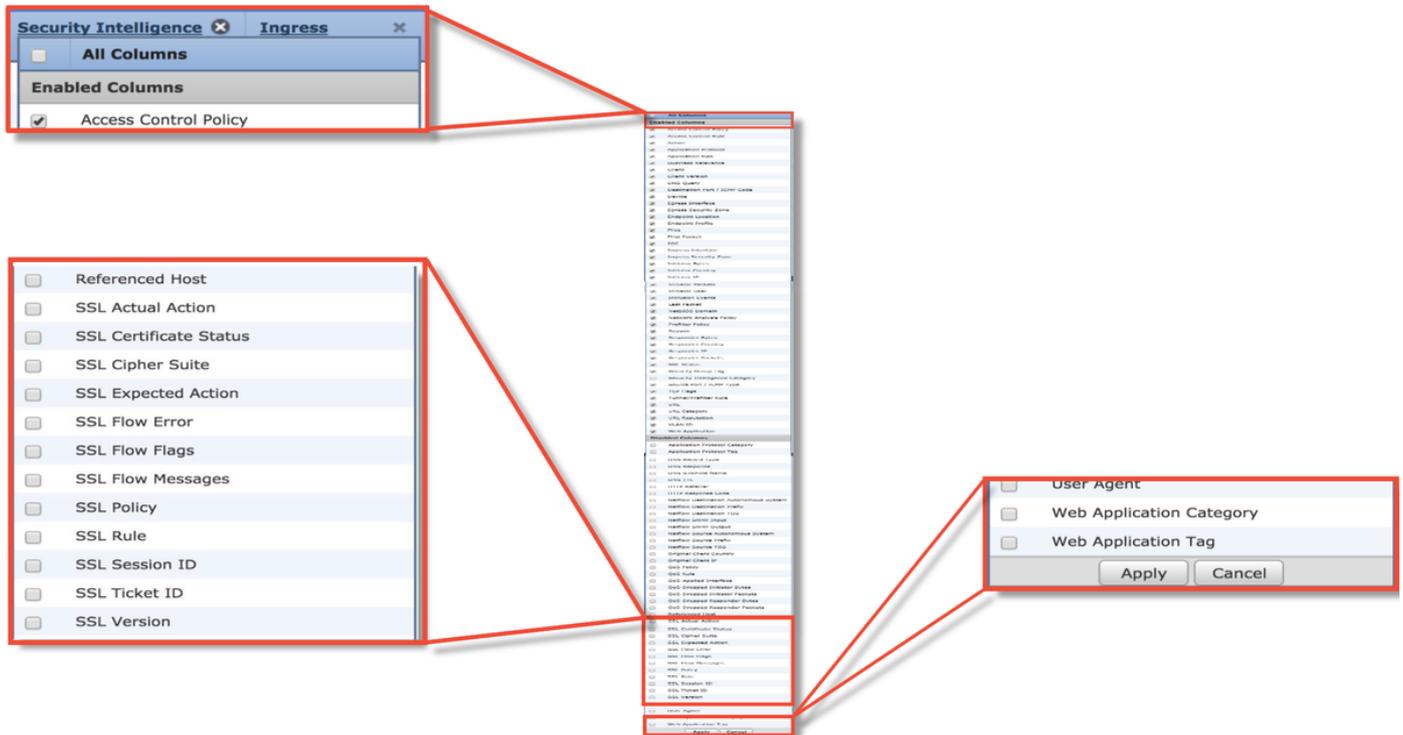
Event Viewer

Syslog

SNMP Trap

Save Cancel

- [Undecryptable Actions]タブで、トラフィックをブロックするオプションが設定されているかどうかを確認します
- 接続イベントで、接続イベントのテーブルビューにいる場合は、名前に「SSL」を含むすべてのフィールドを有効にします
ほとんどの機能はデフォルトで無効になっており、接続イベントビューアで有効にする必要があります



SSLポリシーフェーズのトラブルシューティング

SSLポリシーが許可されると予想されるトラフィックをドロップする理由を理解するために、特定の手順に従うことができます。

接続イベントのSSLフィールドをチェックする

SSLポリシーでトラフィックの問題が発生している疑いがある場合、最初に確認する場所は、上記のように、すべてのSSLフィールドを有効にした後の[Connection Events]セクション([Analysis] > [Connections] > [Events])です。

SSLポリシーがトラフィックをブロックしている場合、[Reason]フィールドには「SSL Block」と表示されます。「SSL Flow Error」列には、ブロックが発生した理由に関する有用な情報が表示されます。他のSSLフィールドには、Firepowerがフローで検出したSSLデータに関する情報が含まれています。

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

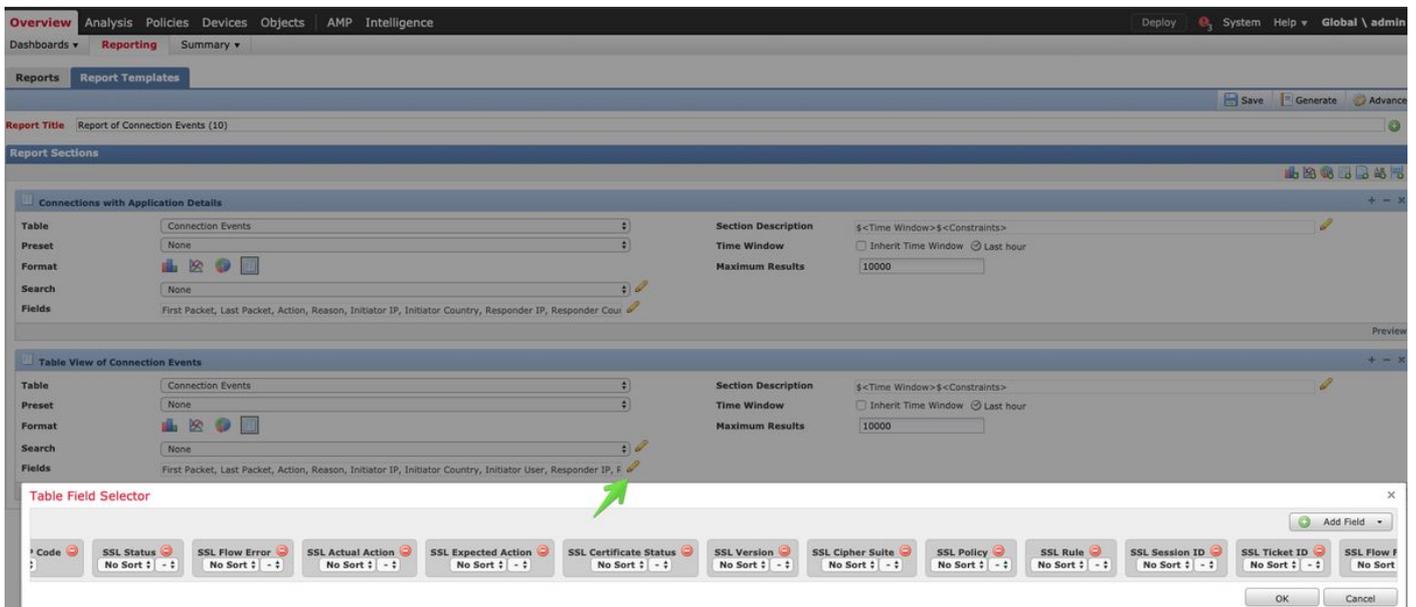
このデータは、SSLポリシーのケースをオープンする際にCisco Technical Assistance Center(TAC)に提供できます。この情報を簡単にエクスポートするには、右上の[レポートデザイナー]ボタンを使用できます。

[接続イベント(Connection Events)]セクションからこのボタンをクリックすると、フィルタとタイムウィンドウのオプションがレポートテンプレートに自動的にコピーされます。

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

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

[Field]セクションで、言及されているすべてのSSLフィールドが追加されていることを確認します。



「生成」をクリックして、PDFまたはCSV形式のレポートを作成します。

SSLポリシーのデバッグ

接続イベントにフローに関する十分な情報が含まれていない場合は、Firepowerコマンドラインインターフェイス(CLI)でSSLデバッグを実行できます。

注：次のデバッグ内容はすべて、x86アーキテクチャ上のソフトウェアで発生するSSL復号化に基づいています。このコンテンツには、バージョン6.2.3以降で追加された、異なるSSLハードウェアオフロード機能からのデバッグは含まれていません。

注：Firepower 9300および4100プラットフォームでは、問題のシェルに次のコマンドでアクセスできます。

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

マルチインスタンスの場合、論理デバイスのCLIには次のコマンドでアクセスできます。

```
# connect module 1 telnet
Firepower-module1> connect ftd ftd1
コンテナftd(ftd1)コンソールに接続しています... 「exit」と入力してブートCLIに戻ります
>
```

system support ssl-debug debug_policy_allコマンドを実行すると、SSLポリシーによって処理される各フローのデバッグ情報を生成できます。

注意：Snortプロセスは、SSLデバッグの実行前と実行後に再起動する必要があります。これにより、使用されるSnortダウンポリシーと展開に応じて、いくつかのパケットがドロップされる可能性があります。TCPトラフィックは再送信されますが、ファイアウォールを通過するアプリケーションが最小パケット損失を許容しない場合、UDPトラフィックは悪影響を受ける可能性があります。

```
> 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 : system support ssl-debug-resetコマンドを使用して必要なデータを収集した後は、デバッグを必ずオフにします。

Firepowerデバイスで実行されている各Snortプロセスに対して書き込まれたファイルがあります。ファイルの場所 :

- /var/commonをFTD以外のプラットフォーム
- /ngfw/var/common for FTD platforms

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 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

デバッグログの有用なフィールドを次に示します。

```

...
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

注：Firepowerが復号化を開始した後に復号化にエラーが発生した場合、ファイアウォールがすでにセッションを変更/man-in-the-middleしているため、トラフィックを廃棄する必要

があります。そのため、クライアントとサーバは異なるTCPスタックと異なる暗号キーを使用します。

この記事の指示に従って、>プロンプトからFirepowerデバイスのデバッグファイルをコピー[できます](#)。

または、Firepowerバージョン6.2.0以降のFMCにオプションがあります。FMCでこのUIユーティリティにアクセスするには、[Devices] > [Device Management]に移動します。次に、 アイコンをクリックし、その後に[Advanced Troubleshooting] > [File Download]をクリックします。その後、該当するファイルの名前を入力し、[Download]をクリックします。



復号化されたパケットキャプチャの生成

Firepowerによって復号化されるセッションの暗号化されていないパケットキャプチャを収集できます。コマンドはsystem support debug-DAQ debug_daq_write_pcapです

注意：Snortプロセスは、復号化されたパケットキャプチャを生成する前に再起動する必要があります。これにより、いくつかのパケットが廃棄される可能性があります。TCPトラフィックなどのステートフルプロトコルは再送信されますが、UDPなどの他のトラフィックは悪影響を受ける可能性があります。

```
> 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_*
```

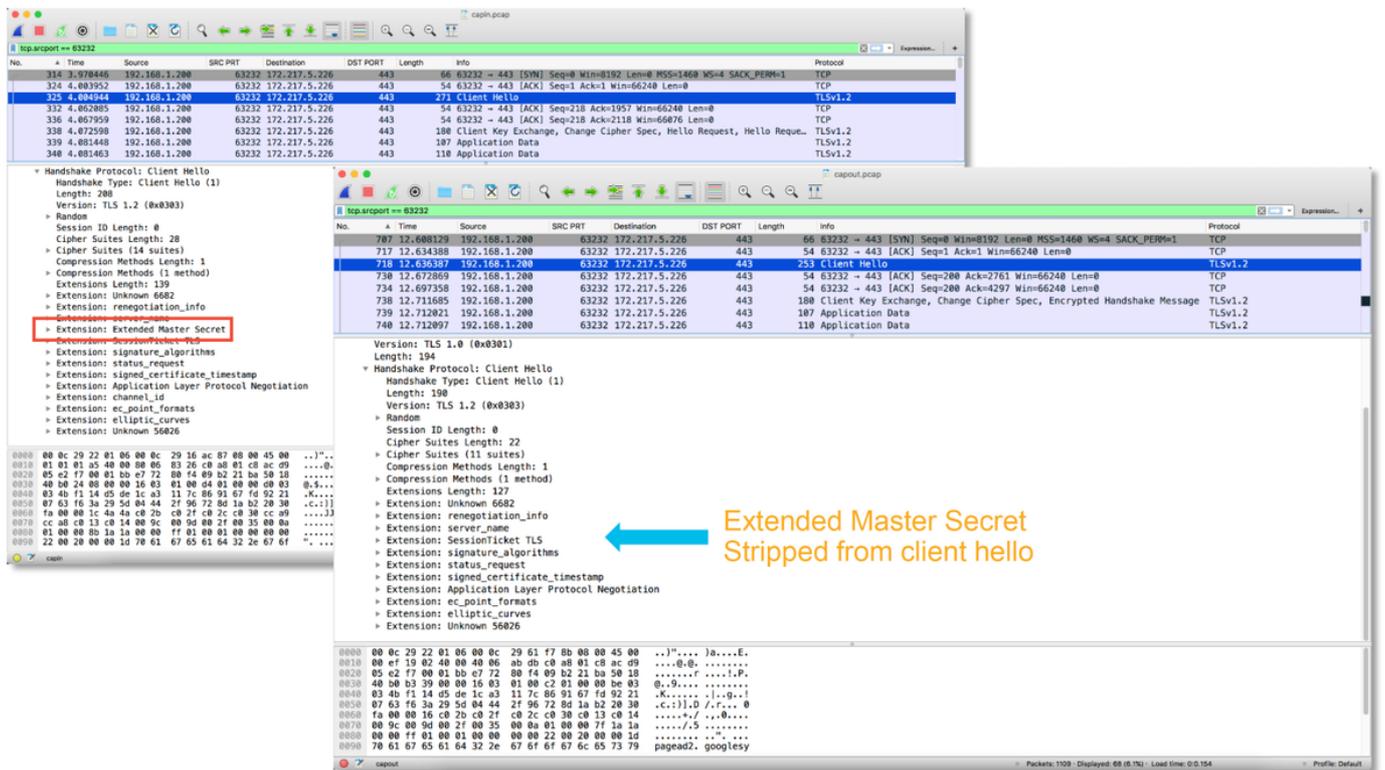
The top screenshot shows a network traffic capture with a red arrow pointing to a packet where SSL decryption failed. The bottom screenshot shows a successful SSL decryption, with a blue arrow pointing to the corresponding packet. Below the bottom screenshot, a warning message is visible: "Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration." This message is repeated for several packets, including a POST request to /comet HTTP/1.1.

注意：復号化されたPCAPキャプチャをTACに送信する前に、問題のあるフローにキャプチャファイルを除外し、制限することを推奨します。これにより、機密データが不必要に漏洩することを回避できます。

クライアントのHelloの変更(CHMod)を探します

また、パケットキャプチャを評価して、クライアントのhello変更が行われているかどうかを確認することもできます。

左側のパケットキャプチャは、元のクライアントhelloを示しています。右側の1つは、サーバ側のパケットを示しています。拡張マスターシークレットがFirepowerのCHMod機能によって削除されていることに注意してください。



クライアントがCAの再署名を信頼して復号化/再署名を行うことを確認する

アクションが「Decrypt - Resign」のSSLポリシールールの場合、クライアントホストが再署名CAとして使用される認証局(CA)を信頼していることを確認します。エンドユーザは、ファイアウォールによってman-in-the-middleであることを示す必要はありません。署名CAを信頼する必要があります。これはActive Directory(AD)グループポリシーを通じて最も一般的に適用されますが、会社のポリシーとADインフラストラクチャによって異なります。

詳細については、次の記事を参照してください。この記事では、SSLポリシーの作成方法について説明しています。

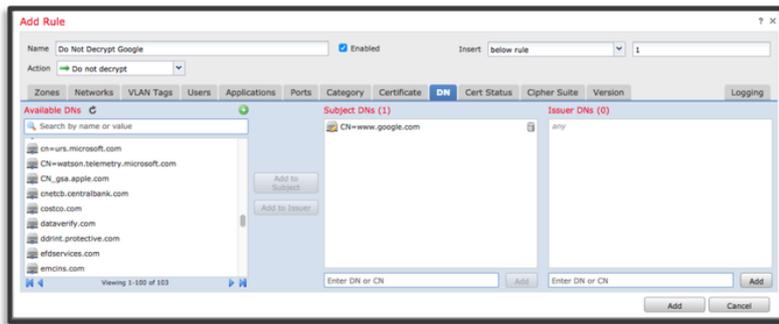
緩和手順

いくつかの基本的な緩和手順に従って、次のことを実行できます。

- 特定のトラフィックを復号化しないようにSSLポリシーを再設定する
- クライアントのhelloパケットから特定のデータを削除し、復号化が成功するようにします

Do Not Decrypt(DnD)ルールの追加

次のシナリオ例では、SSLポリシーインスペクションを通過する際にgoogle.comへのトラフィックが切断されていることが確認されています。サーバ証明書の共通名(CN)に基づいて、google.comへのトラフィックが復号化されないようにルールが追加されます。



#	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	

ポリシーを保存して展開した後、前述のトラブルシューティング手順に従って、Firepowerがトラフィックで何を行っているかを確認できます。

クライアントのHello変更の調整

場合によっては、トラブルシューティングによって、Firepowerで特定のトラフィックの復号化に関する問題が発生していることが明らかになることがあります。system support ssl-client-hello-tuningユーティリティをCLIで実行すると、Firepowerがクライアントのhelloパケットから特定のデータを削除できます。

次の例では、特定のTLS拡張が削除されるように設定が追加されています。数値IDは、TLSの拡張と標準に関する情報を検索することによって見つけることができます。

注意： Snortプロセスは、クライアントのhello変更が有効になる前に再起動する必要があります。これにより、いくつかのパケットがドロップされる可能性があります。TCPトラフィックなどのステートフルプロトコルは再送信されますが、UDPなどの他のトラフィックは悪影響を受ける可能性があります。

```
> 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

クライアントのhello変更設定に対する変更を元に戻すには、**system support ssl-client-hello-reset**コマンドを実装できます。

TACに提供するデータ

Data

Firepower Management Center(FMC)およびFirepowerデバイスからのファイルのトラブルシューティング
SSLデバッグ

フルセッションパケットキャプチャ (可能であれば、クライアント側、Firepowerデバイス自体、および
接続イベントのスクリーンショットまたはレポート

次のステップ

SSLポリシーコンポーネントが問題の原因ではないと判断された場合は、次のステップとしてアクティブ認証機能のトラブルシューティングを行います。

次の記事に進むには、[ここをクリック](#)してください。