

Fase 5 da solução de problemas de caminho de dados do Firepower: Política SSL

Contents

[Introduction](#)

[Prerequisites](#)

[Troubleshooting da Fase de Política SSL](#)

[Verificar campos SSL nos eventos de conexão](#)

[Depurar a política SSL](#)

[Gerar uma captura de pacotecriptografado](#)

[Procurar Modificações de Hello do Cliente \(CHMod\)](#)

[Certifique-se de que o cliente confie na reassinatura da CA para descriptografar/reassinar](#)

[Etapas de mitigação](#)

[Adicionar Regras Não Descriptografar \(DnD\)](#)

[Ajuste de Modificação de Hello do Cliente](#)

[Dados a fornecer ao TAC](#)

[Próxima etapa](#)

Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o [artigo Visão geral](#) para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de solução de problemas de caminho de dados.

Este artigo abrange o quinto estágio da solução de problemas de caminho de dados do Firepower, o recurso de política SSL (Secure Sockets Layer).



Prerequisites

- As informações neste artigo se aplicam a qualquer plataforma Firepower Descriptografia SSL para o Adaptive Security Appliance (ASA) com FirePOWER Services (módulo SFR) disponível somente em 6.0+O recurso Modificação de Hello do cliente está disponível somente em 6.1+
- Confirme se a política SSL está sendo usada na política de controle de acesso

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 se o registro está ativado para todas as regras, incluindo a 'Ação padrão'

#	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

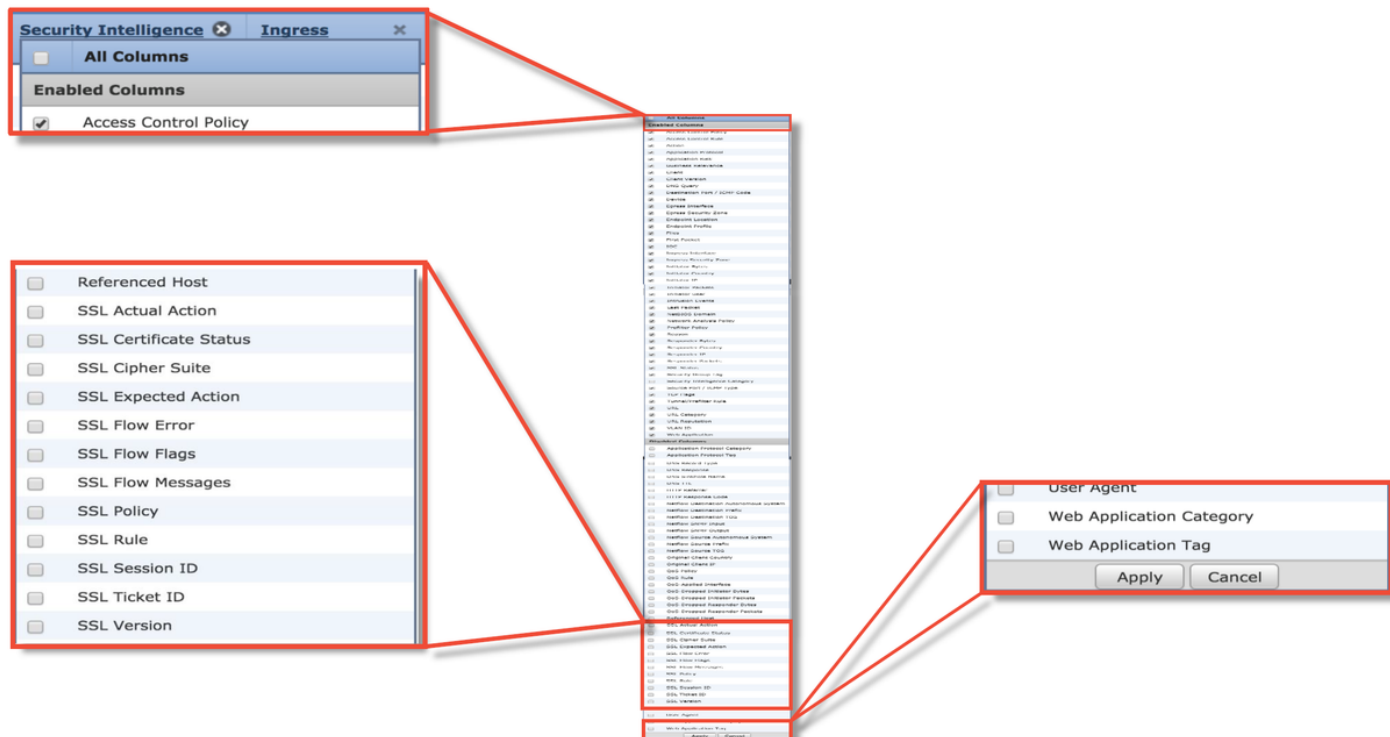
Log at End of Connection **Enable Logging**

Send Connection Events to:

- Event Viewer
- Syslog
- SNMP Trap

Save Cancel

- Verifique a guia Ações não descriptografáveis para ver se há alguma opção definida para bloquear o tráfego
- Nos eventos do Connection, quando você estiver na exibição de tabela de eventos de conexão, ative todos os campos com 'SSL' no nome
A maioria é desativada por padrão e precisa ser ativada no visualizador de Eventos de Conexão



Troubleshooting da Fase de Política SSL

As etapas específicas podem ser seguidas para ajudar a entender por que a política SSL pode estar descartando o tráfego que se espera que seja permitido.

Verificar campos SSL nos eventos de conexão

Se houver suspeita de que a Política SSL está causando problemas de tráfego, o primeiro lugar a verificar é a seção Eventos de Conexão (em **Análise > Conexões > Eventos**) depois de habilitar todos os campos SSL, conforme descrito acima.

Se a política SSL estiver bloqueando o tráfego, o campo **Razão** exibirá "SSL Block". A coluna **Erro de fluxo SSL** tem informações úteis sobre o motivo do bloqueio. Os outros campos SSL têm informações sobre os dados SSL detectados pelo Firepower no fluxo.

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

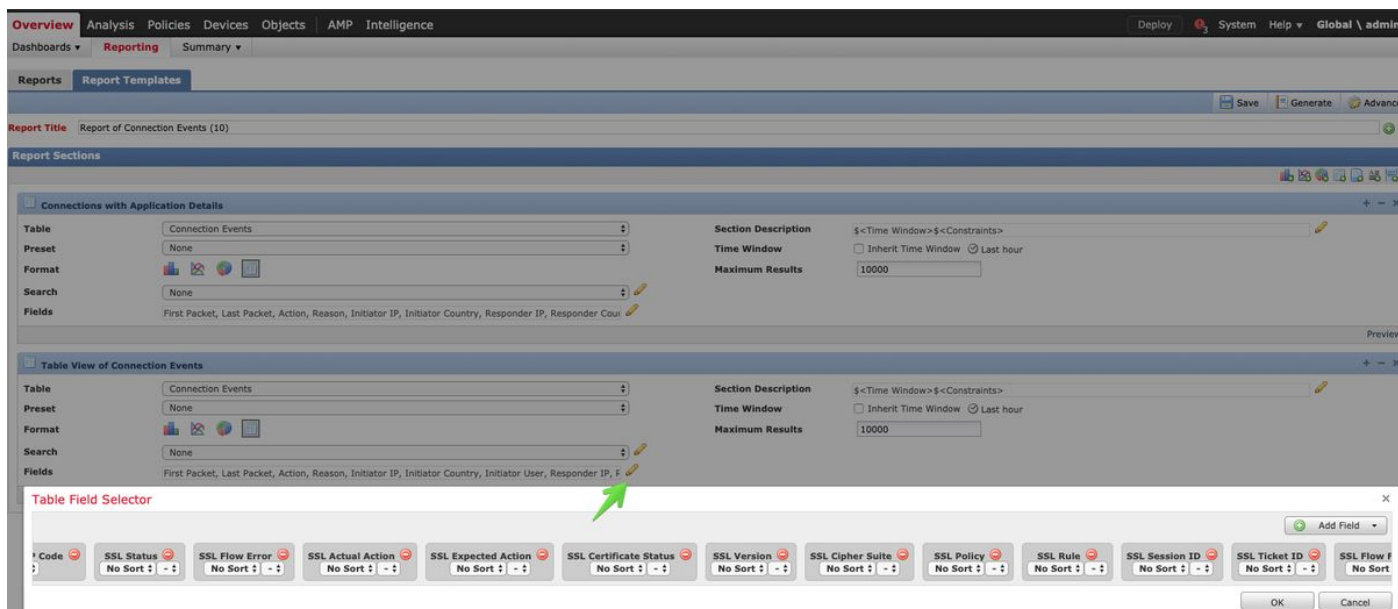
Esses dados podem ser fornecidos ao Cisco Technical Assistance Center (TAC) ao abrir um caso para a política SSL. Para exportar essas informações com facilidade, o botão **Report Designer** no canto superior direito pode ser usado.

Se esse botão for clicado na seção Eventos de conexão, os filtros e as opções de janela de tempo serão copiados automaticamente para o modelo de relatório.

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

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

Verifique se todos os campos SSL mencionados foram adicionados à seção 'Campo'.



Clique em **Gerar** para criar um relatório nos formatos PDF ou CSV.

Depurar a política SSL

Se os eventos de conexão não contiverem informações suficientes sobre o fluxo, a depuração SSL poderá ser executada na CLI (Command Line Interface, interface de linha de comando) do Firepower.

Note: Todo o conteúdo de depuração abaixo é baseado na descryptografia SSL que acontece no software na arquitetura x86. Este conteúdo não inclui depurações de recursos de descarga de hardware SSL adicionados na versão 6.2.3 e posteriores, que são diferentes.

Note: Nas plataformas Firepower 9300 e 4100, o shell em questão pode ser acessado por meio dos seguintes comandos:

```
# conectar o módulo 1
Firepower-module1> connect ftd
>
```

Para várias instâncias, a CLI do dispositivo lógico pode ser acessada com os seguintes comandos.

```
# connect module 1 telnet
Firepower-module1> conectar ftd ftd1
Conectando ao console do contêiner ftd(ftd1)... digite "exit" para voltar à CLI de inicialização
>
```

O comando `system support ssl-debug debug_policy_all` pode ser executado para gerar informações de depuração para cada fluxo processado pela Política SSL.

Caution: O processo de snort deve ser reiniciado antes e depois da execução da depuração SSL, o que pode fazer com que alguns pacotes sejam descartados, dependendo das políticas de snort-down e da implantação usada. O tráfego TCP será retransmitido, mas o tráfego UDP poderá ser afetado negativamente se os aplicativos que passam pelo firewall

não tolerarem a perda mínima de pacotes.

```
> 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

aviso: Não se esqueça de desativar a depuração depois que os dados necessários forem coletados com o comando **system support ssl-debug-reset**.

Haverá um arquivo gravado para cada processo de snort em execução no dispositivo Firepower. O local dos arquivos será:

- /var/comum para plataformas não-FTD
- /ngfw/var/common para 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

Estes são alguns dos campos úteis nos logs de depuração.

```

...
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;


```

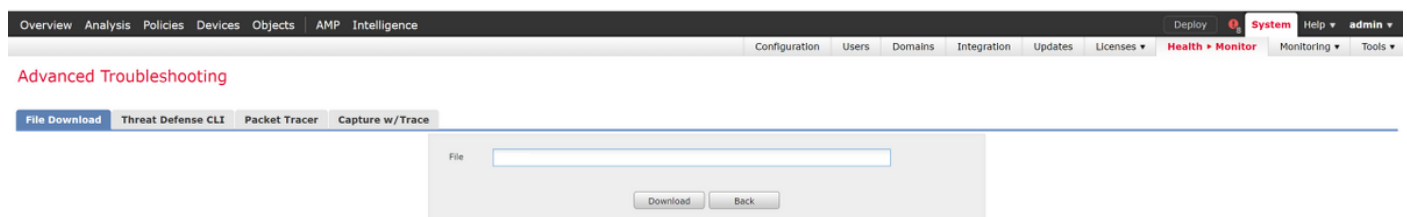
SSL Errors potentially causing drop

Note: Se houver um erro com a descriptografia que ocorre depois que o Firepower começa a descriptografar, o tráfego deve ser descartado, uma vez que o firewall já

modificou/colocou no meio da sessão, portanto, não é possível que o cliente e o servidor retomem a comunicação, pois eles têm pilhas de TCP diferentes, bem como chaves de criptografia diferentes usadas no fluxo.

Os arquivos de depuração podem ser copiados do dispositivo Firepower do prompt > usando as instruções neste [artigo](#).

Como alternativa, há uma opção no FMC no Firepower versão 6.2.0 e posterior. Para acessar este utilitário de IU no FMC, navegue para **Dispositivos > Gerenciamento de dispositivos**. Em seguida, clique no botão  ao lado do dispositivo em questão, seguido por **Advanced Troubleshooting > File Download**. Em seguida, você pode digitar o nome de um arquivo em questão e clicar em Download.



Gerar uma captura de pacote descriptografado

É possível coletar uma captura de pacote não criptografado para as sessões que são descriptografadas pelo Firepower. O comando é **system support debug-DAQ debug_daq_write_pcap**

Caution: O processo de snort deve ser reiniciado antes de gerar a captura de pacote descriptografado, o que pode fazer com que alguns pacotes sejam descartados. Os protocolos stateful, como o tráfego TCP, são retransmitidos, mas outros tráfegos, como o UDP, podem ser afetados 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: 18.374322
- Source: 192.168.1.200
- Destination: 172.217.8.10
- Protocol: TCP
- Length: 54
- Info: 59117 → 443 [ACK] Seq=190 Win=262140
- Src Port: 59117
- New Column: 443

 An orange arrow labeled "SSL Decryption fails" points to this packet.

The bottom screenshot shows a detailed view of a packet. A blue arrow labeled "Successful SSL Decryption" points to the "Hypertext Transfer Protocol" section, which contains the following information:

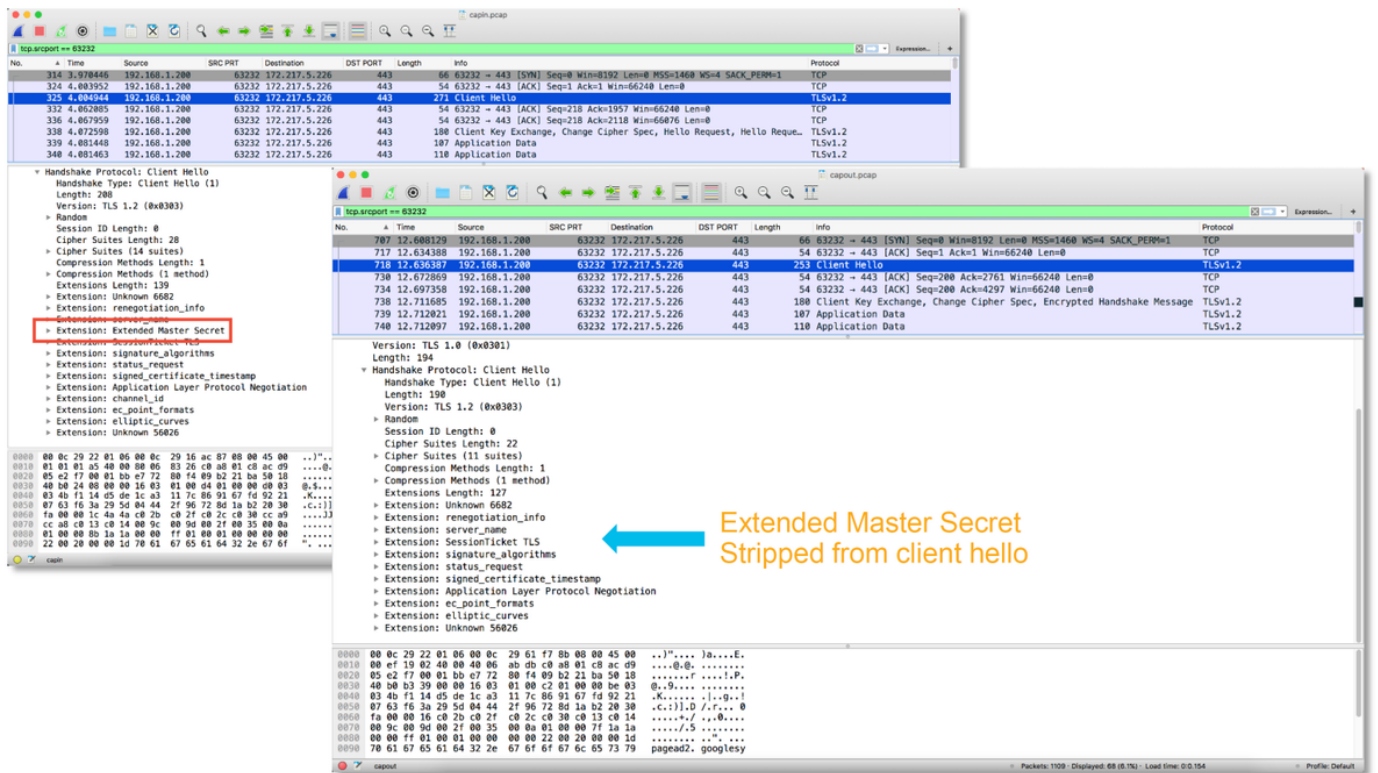
- POST /comet HTTP/1.1 [URL]
- Content-Type: application/json
- Content-Length: 889
- Host: 172.217.8.10
- User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0
- Accept: */*
- Accept-Language: pt-BR
- Accept-Encoding: gzip, deflate
- Connection: keep-alive
- Cookie: ...
- Referer: ...

Caution: Antes de enviar uma captura PCAP descriptografada para o TAC, recomenda-se filtrar e limitar o arquivo de captura aos fluxos problemáticos, para evitar revelar dados confidenciais desnecessariamente.

Procurar Modificações de Hello do Cliente (CHMod)

A captura de pacotes também pode ser avaliada para ver se alguma modificação de saudação do cliente está ocorrendo.

A captura de pacote à esquerda descreve a saudação do cliente original. O da direita mostra os pacotes do lado do servidor. Observe que o segredo mestre estendido foi removido por meio do recurso CHMod no Firepower.



Certifique-se de que o cliente confie na reassinatura da CA para descriptografar/reassinar

Para regras de Política SSL com uma ação de "Descriptografar - Resign", certifique-se de que os hosts do cliente confiem na Autoridade de Certificado (CA) usada como CA que está renunciando. Os usuários finais não devem ter nenhuma indicação de que estão sendo manipulados pelo firewall. Eles devem confiar na CA de assinatura. Isso é mais comumente aplicado por meio da Política de Grupo do Active Directory (AD), mas depende da política da empresa e da infraestrutura do AD.

Para obter mais informações, você pode rever o seguinte [artigo](#), que descreve como criar uma política SSL.

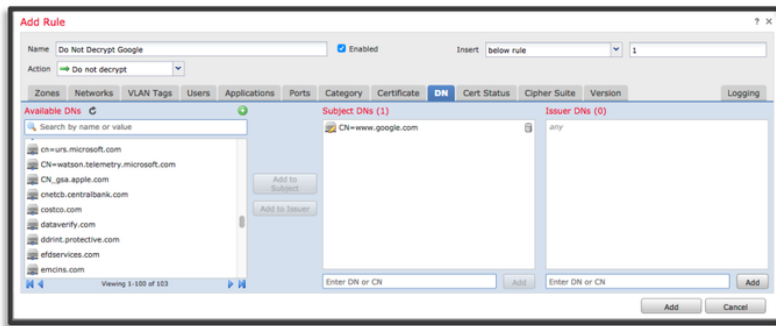
Etapas de mitigação

Algumas etapas básicas de mitigação podem ser seguidas para:

- Reconfigure a política SSL para não descriptografar determinado tráfego
- Retirar determinados dados de um pacote hello do cliente para que a descriptografia seja bem-sucedida

Adicionar Regras Não Descriptografar (DnD)

No cenário de exemplo a seguir, foi determinado que o tráfego para google.com está quebrando ao passar pela inspeção da política SSL. Uma regra é adicionada, com base no nome comum (CN) no certificado do servidor, para que o tráfego no google.com não seja descriptografado.



#	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	

Depois de salvar e implantar a política, as etapas de solução de problemas descritas acima podem ser seguidas novamente para ver o que o Firepower está fazendo com o tráfego.

Ajuste de Modificação de Hello do Cliente

Em alguns casos, a solução de problemas pode revelar que o Firepower está enfrentando um problema com a descryptografia de determinado tráfego. O utilitário `ssl-client-hello-tuning` pode ser executado na CLI para fazer com que o Firepower remova determinados dados de um pacote hello do cliente.

No exemplo abaixo, uma configuração é adicionada para que certas extensões TLS sejam removidas. Os IDs numéricos são encontrados procurando informações sobre extensões e padrões TLS.

Caution: O processo de snort deve ser reiniciado antes que as alterações de hello do cliente entrem em vigor, o que pode fazer com que alguns pacotes sejam descartados. Os protocolos stateful, como o tráfego TCP, são retransmitidos, mas outros tráfegos, como o UDP, podem ser afetados 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 reverter quaisquer alterações feitas nas configurações de modificação de saudação do cliente, o comando **system support ssl-client-hello-reset** pode ser implementado.

Dados a fornecer ao TAC

Dados Instruções

Solucionar
problemas
de arquivos
do Firepower

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

(FMC) e dos
dispositivos

Firepower

Depurações
SSL

Consulte este artigo para obter instruções

Capturas
completas
de pacotes
de sessão
(do lado do
cliente, do
próprio
dispositivo

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

Firepower e
do lado do
servidor,
quando
possível)

Capturas de
tela ou

relatórios do evento de
conexão

Consulte este artigo para obter instruções

Próxima etapa

Se for determinado que o componente de política SSL não é a causa do problema, a próxima etapa será solucionar o problema do recurso de autenticação ativa.

Clique [aqui](#) para continuar com o próximo artigo.