Firepower 데이터 경로 문제 해결 5단계: SSL 정책

목차

소개

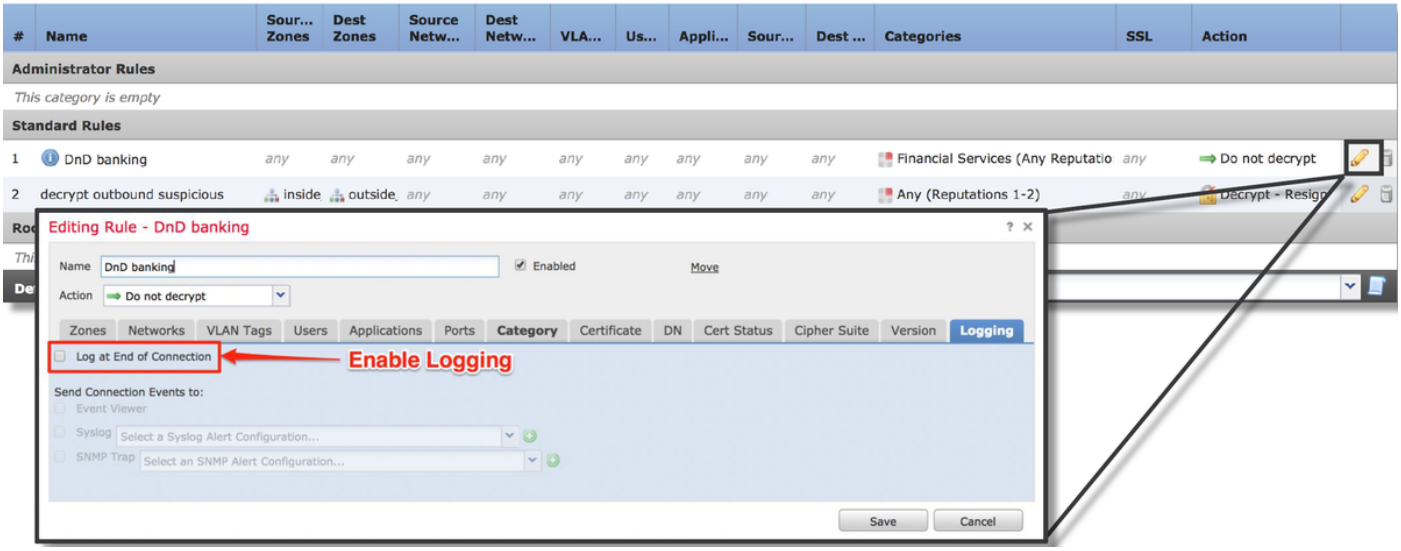
이 문서는 Firepower 시스템의 데이터 경로 문제를 체계적으로 해결하여 Firepower의 구성 요소가 트래픽에 영향을 미치는지 여부를 확인하는 방법을 설명하는 일련의 문서 중 일부입니다. Firepower 플랫폼의 아키텍처에 대한 자세한 내용은 개요 문서를 참조하고 다른 데이터 경로 문제 해결 문서에 대한 링크를 참조하십시오.

이 문서에서는 Firepower 데이터 경로 문제 해결의 5단계인 SSL(Secure Sockets Layer) 정책 기능을 다룹니다.

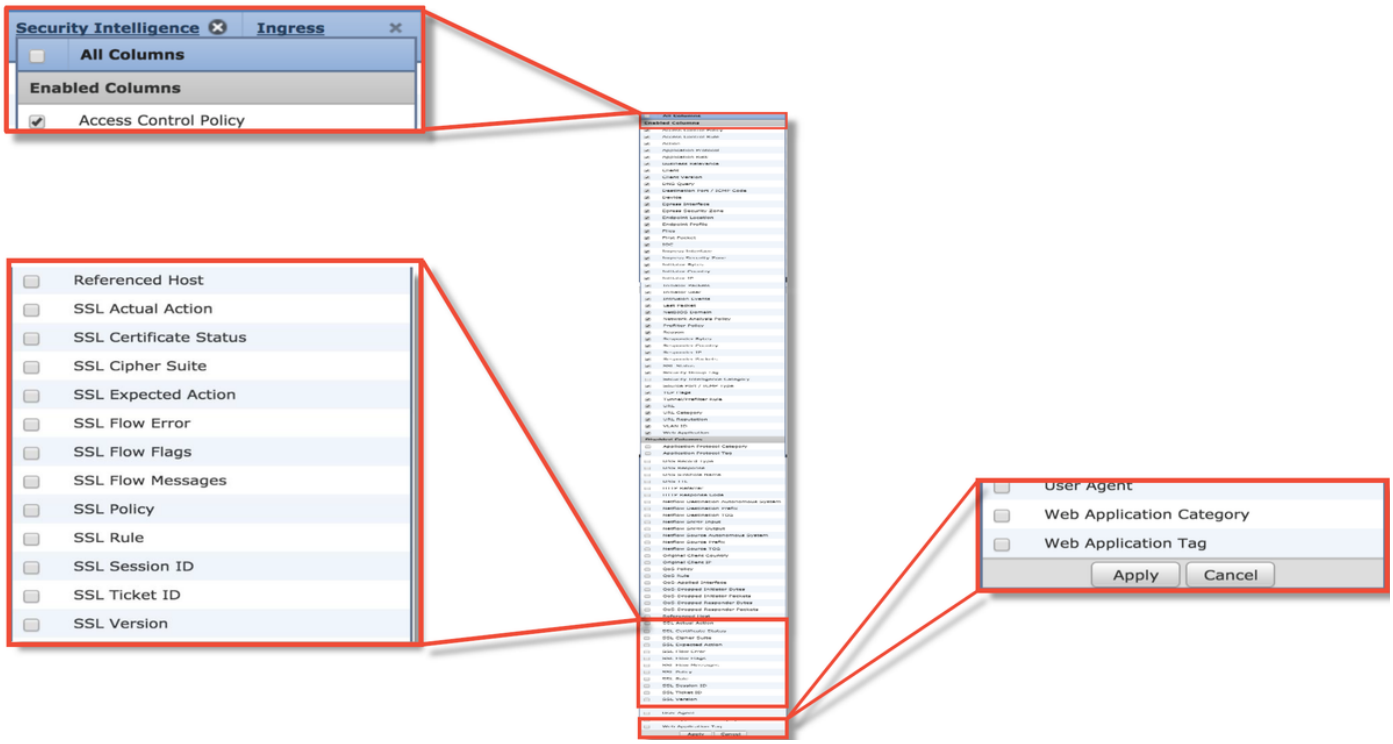
사전 요구 사항

- 이 문서의 정보는 모든 Firepower 플랫폼에 적용됩니다. FirePOWER 서비스(SFR 모듈)가 설치된 ASA(Adaptive Security Appliance)에 대한 SSL 암호 해독은 6.0 이상에서만 사용 가능클라이언트 Hello 수정 기능은 6.1 이상에서만 사용 가능
- 액세스 제어 정책에서 SSL 정책이 사용되고 있는지 확인합니다.

- '기본 작업'을 포함하여 모든 규칙에 대해 로깅이 활성화되어 있는지 확인합니다.



- 암호 해독 불가 작업 탭에서 트래픽 차단 옵션이 설정되어 있는지 확인합니다.
- 연결 이벤트에서, 연결 이벤트의 테이블 보기 상태인 경우 이름에 'SSL'이 포함된 모든 필드를 활성화합니다.
  대부분은 기본적으로 비활성화되어 있으며 연결 이벤트 뷰어에서 활성화해야 합니다.



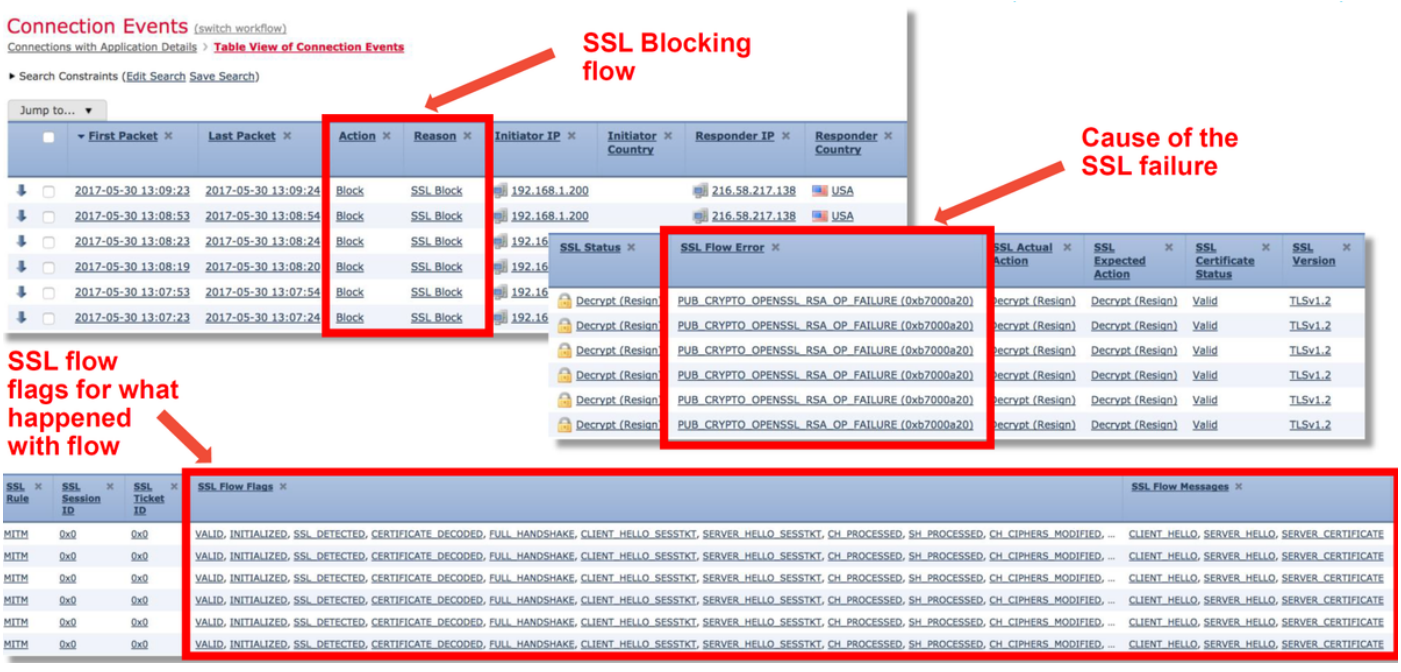
SSL 정책 문제 해결 단계

특정 단계를 수행하여 허용될 것으로 예상되는 트래픽을 SSL 정책에서 삭제하는 이유를 파악할 수 있습니다.

연결 이벤트에서 SSL 필드 확인

SSL 정책이 트래픽 문제를 일으키는 것으로 의심되는 경우, 위에서 설명한 대로 모든 SSL 필드를 활성화한 후 **분석 > 연결 > 이벤트** 아래에 있는 연결 이벤트 섹션을 먼저 확인해야 합니다.

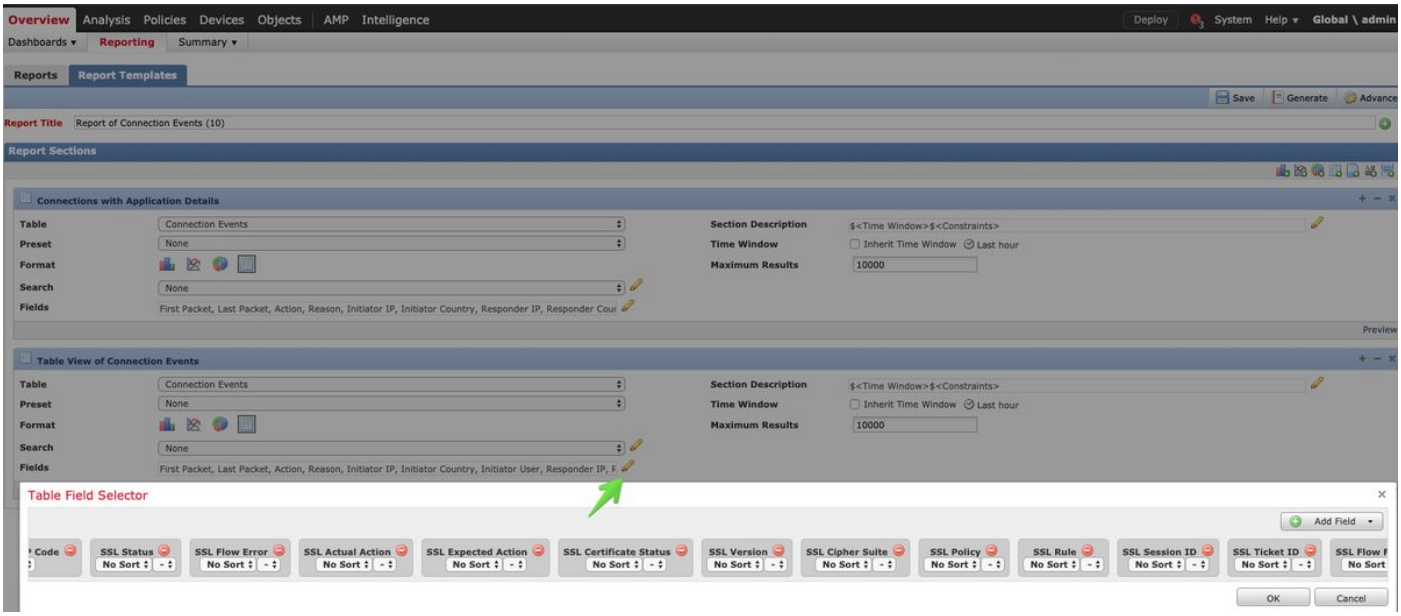
SSL 정책이 트래픽을 차단하는 경우 **이유** 필드에 "SSL 차단"이 표시됩니다. **SSL 플로우 오류** 열에는 차단이 발생한 이유에 대한 유용한 정보가 있습니다. 다른 SSL 필드에는 Firepower가 플로우에서 탐지한 SSL 데이터에 대한 정보가 있습니다.



SSL 정책에 대한 케이스를 열 때 이 데이터를 Cisco TAC(Technical Assistance Center)에 제공할 수 있습니다. 이 정보를 쉽게 내보내려면 오른쪽 상단에 있는 **보고서 디자이너** 버튼을 사용하면 됩니다.

연결 이벤트 섹션에서 이 버튼을 클릭하면 필터 및 타임 윈도우 옵션이 보고서 템플릿에 자동으로 복사됩니다.

언급된 모든 SSL 필드가 '필드' 섹션에 추가되었는지 확인합니다.



PDF 또는 CSV 형식의 보고서를 생성하려면 **생성**을 클릭합니다.

SSL 정책 디버그

연결 이벤트에 플로우에 대한 충분한 정보가 포함되어 있지 않으면 Firepower CLI(Command Line Interface)에서 SSL 디버깅을 실행할 수 있습니다.

> **참고**: 아래의 모든 디버그 콘텐츠는 x86 아키텍처의 소프트웨어에서 발생하는 SSL 암호 해독을 기반으로 합니다. 이 콘텐츠에는 버전 6.2.3 이상에 추가된 SSL 하드웨어 오프로드 기능의 디버그가 포함되어 있지 않습니다(서로 다름).

> **참고**: Firepower 9300 및 4100 플랫폼에서는 다음 명령을 통해 해당 쉘(shell)에 액세스할 수 있습니다.

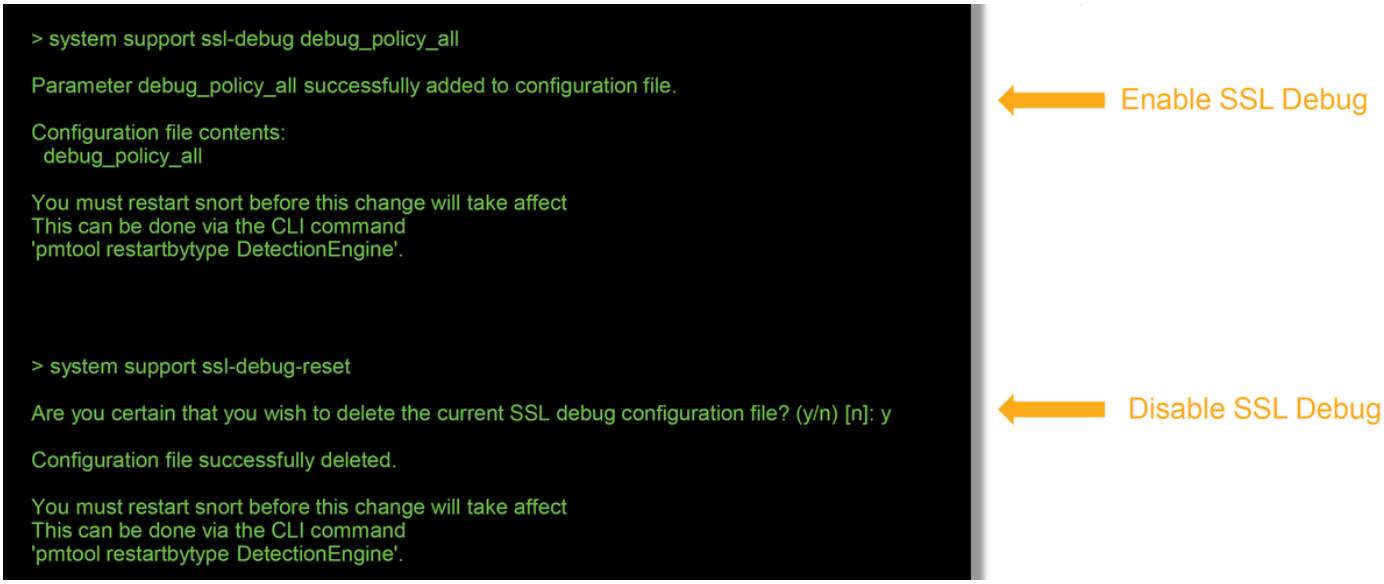
```
# connect module 1 console
Firepower-module1> connect ftd
>
```

다중 인스턴스의 경우 다음 명령을 사용하여 논리적 디바이스 CLI에 액세스할 수 있습니다.

```
# connect module 1 telnet
Firepower-module1> ftd ftd 1 연결
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>
```

system support ssl-debug debug_policy_all 명령을 실행하여 SSL 정책에 의해 처리되는 모든 플로우에 대한 디버깅 정보를 생성할 수 있습니다.

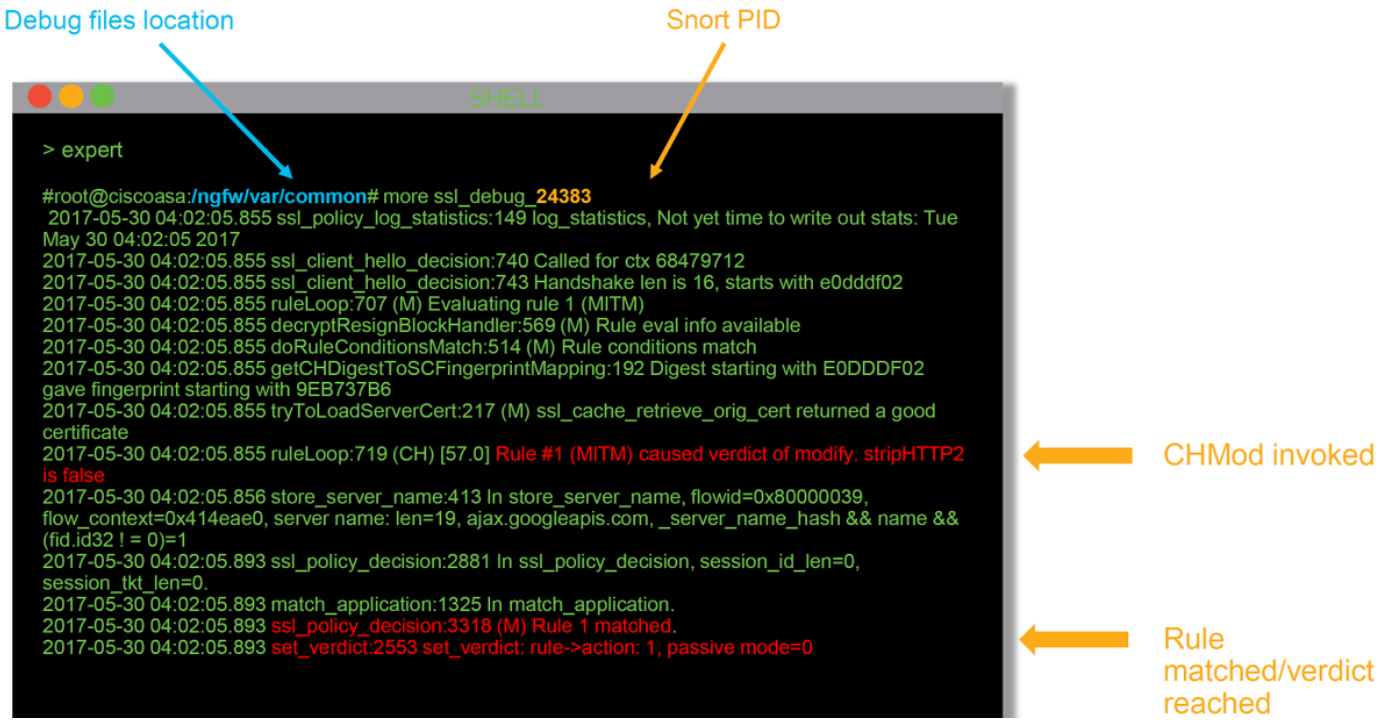
주의: SSL 디버그를 실행하기 전후에 Snort 프로세스를 재시작해야 하는데, 이 경우 사용된 snort-down 정책 및 구축에 따라 일부 패킷이 삭제될 수 있습니다. TCP 트래픽은 재전송되지만, 방화벽을 통과하는 애플리케이션이 최소 패킷 손실을 허용하지 않는 경우 UDP 트래픽이 부정적인 영향을 받을 수 있습니다.



경고: **system suport ssl-debug-reset** 명령을 사용하여 필요한 데이터를 수집한 후 디버깅을 끄는 것을 잊지 마십시오.

Firepower 디바이스에서 실행 중인 각 Snort 프로세스에 대해 파일이 작성됩니다. 파일의 위치는 다음과 같습니다.

- **비 FTD 플랫폼의 경우 /var/common**
- **FTD 플랫폼의 경우 /ngfw/var/common**



다음은 디버그 로그의 몇 가지 유용한 필드입니다.

```
...
   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

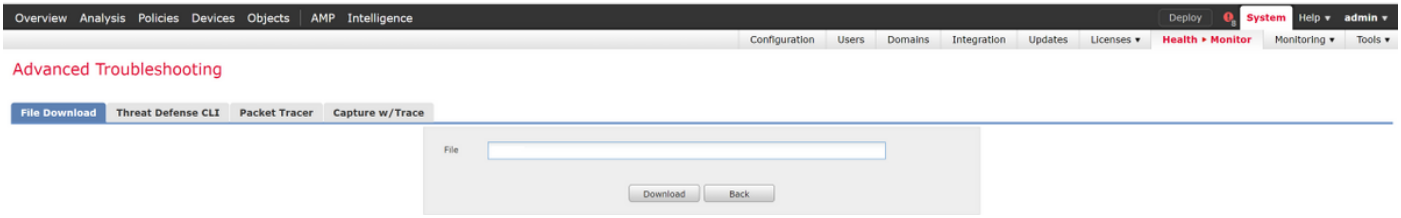
```
...
2017-05-30 04:02:05.894  Error callback.
 Logstr: ssl_policy_error_callback
  Process ID: 24383
  Flow context: 0x414eae0
  Flow info: 0x7ffea4b8d3a0
     flowid: 0x80000039
     error: 0xb7000a20
     FLOW ERROR FOUND:
         - NSE:PubCrypto [0xb7000a20;code:32;sub:10] OpenSSL RSA operation 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

> **참고**: Firepower가 암호 해독을 시작한 후 암호 해독에 오류가 발생하는 경우, 방화벽에서는 이미 세션을 수정/끼어들기했기 때문에 해당 트래픽을 삭제해야 합니다. 따라서 플로우에서 사용되는 암호화 키뿐만 아니라 TCP 스택이 서로 달라 클라이언트와 서버가 통신을 재개할 수 없습니다.

이 문서의 지침에 따라 > 프롬프트에서 Firepower 디바이스 외부로 디버그 파일을 복사할 수 있습니다.

또는 Firepower 버전 6.2.0 이상의 FMC에 옵션이 있습니다. FMC의 이 UI 유틸리티에 액세스하려면 **디바이스 > 디바이스 관리**로 이동합니다. 그런 다음 해당 디바이스 옆의 아이콘과 **Advanced Troubleshooting(고급 문제 해결) > File Download(파일 다운로드)가 차례로 나타납니다**. 그런 다음 해당 파일의 이름을 입력하고 다운로드를 클릭할 수 있습니다.

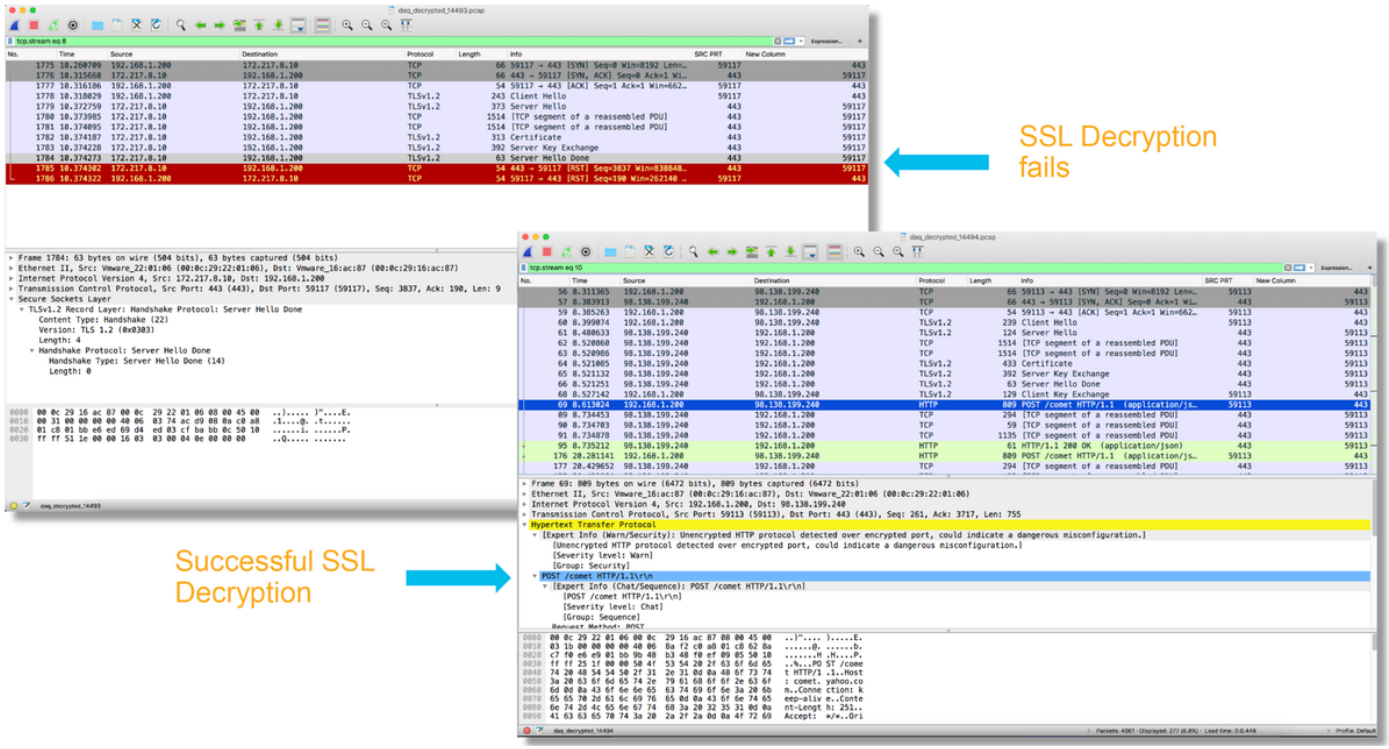


암호 해독된 패킷 캡처 생성

Firepower에서 암호 해독되는 세션에 대해 암호화되지 않은 패킷 캡처를 수집할 수 있습니다. 명령은 **system support debug-daq debug_daq_write_pcap입니다.**

> **주의**: 암호 해독된 패킷 캡처를 생성하기 전에 Snort 프로세스를 재시작할 수 있는데, 그러면 일부 패킷이 삭제될 수 있습니다. TCP 트래픽과 같은 상태 저장 프로토콜은 재전송되지만, UDP와 같은 다른 트래픽은 부정적인 영향을 받을 수 있습니다.

```
> 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_*
```

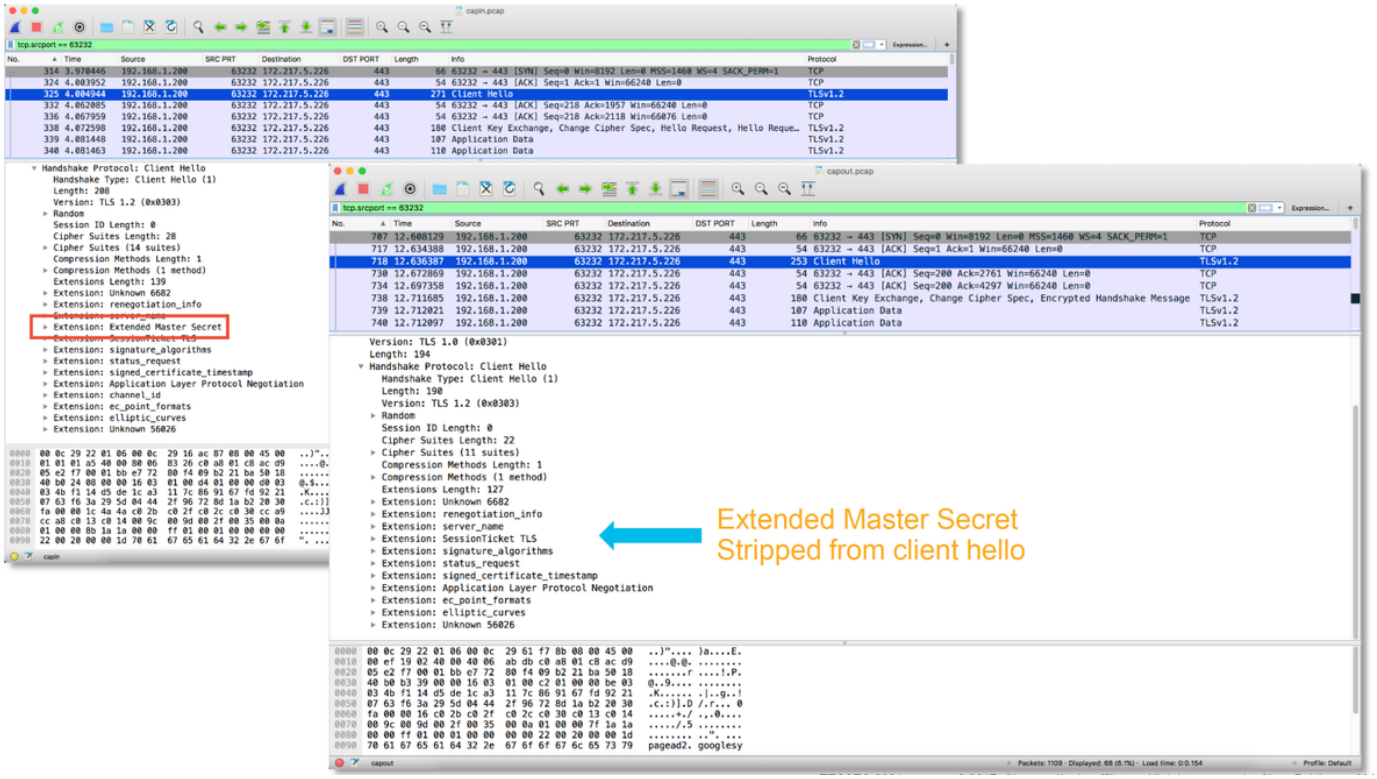


> **주의**: 암호 해독된 PCAP 캡처를 TAC에 제출하기 전에, 민감한 데이터가 불필요하게 노출되지 않도록 캡처 파일을 필터링하여 문제가 있는 플로우로 제한하는 것이 좋습니다.

클라이언트 Hello 수정 찾기(CHMod)

패킷 캡처를 평가하여 클라이언트 hello 수정이 발생하는지 확인할 수도 있습니다.

왼쪽의 패킷 캡처는 원래 클라이언트 hello를 나타냅니다. 오른쪽의 패킷 캡처는 해당 서버측 패킷을 보여줍니다. Firepower의 CHMod 기능을 통해 확장된 마스터 암호가 제거되었음을 확인할 수 있습니다.



암호 해독/재서명을 위해 클라이언트가 재서명 CA를 신뢰하는지 확인

"암호 해독 - 재서명" 작업이 포함된 SSL 정책 규칙의 경우, 클라이언트 호스트가 재서명 CA로 사용되는 CA(Certificate Authority)를 신뢰하는지 확인합니다. 최종 사용자에게는 방화벽의 끼어들기가 표시되지 않아야 합니다. 서명 CA를 신뢰해야 합니다. 이는 일반적으로 AD(Active Directory) 그룹 정책을 통해 적용되지만, 회사 정책 및 AD 인프라에 따라 달라집니다.

자세한 내용은 SSL 정책을 생성하는 방법을 설명하는 다음 문서를 참조하십시오.

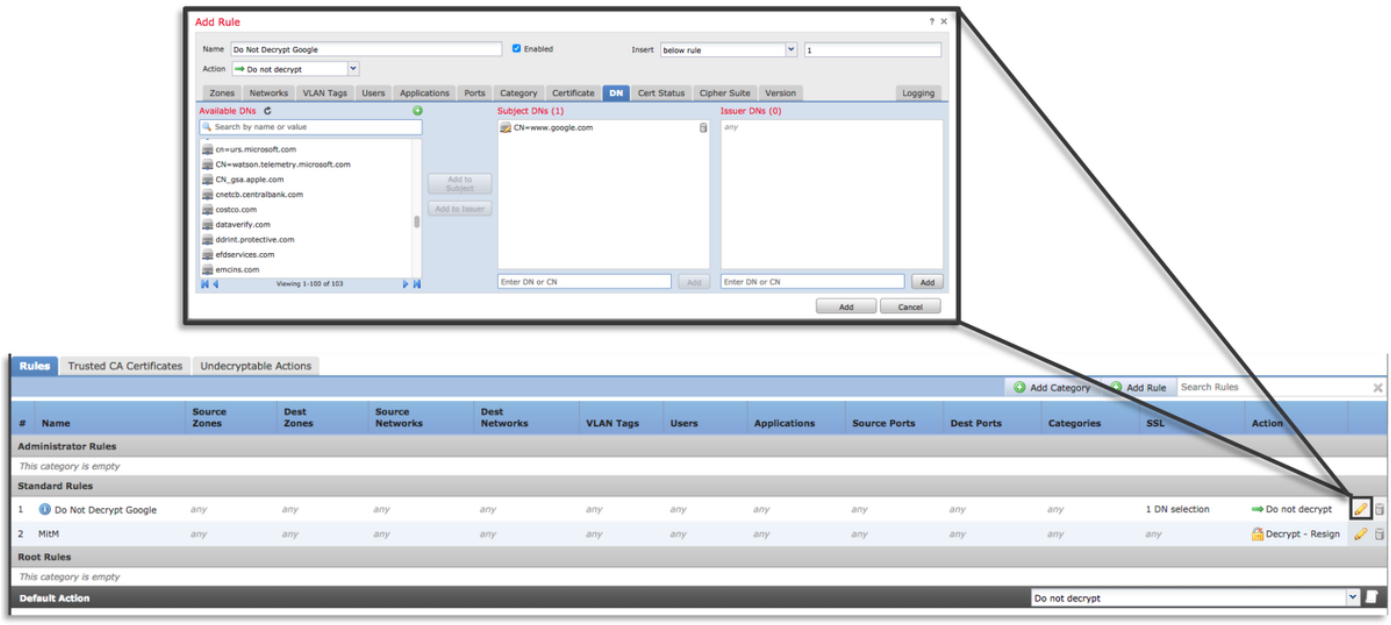
완화 단계

다음을 위해 몇 가지 기본 완화 단계를 수행할 수 있습니다.

- 특정 트래픽의 암호를 해독하지 않도록 SSL 정책 재설정
- 암호 해독에 성공하도록 클라이언트 Hello 패킷에서 특정 데이터 제거

DnD(암호 해독 안 함) 규칙 추가

다음 시나리오 예에서는 SSL 정책 검사를 통과할 때 google.com에 대한 트래픽이 중단되는 것으로 확인되었습니다. google.com에 대한 트래픽의 암호가 해독되지 않도록 서버 인증서의 CN(Common Name)을 기반으로 규칙을 추가합니다.



정책을 저장 및 구축한 후에는 위에서 설명한 문제 해결 단계를 다시 수행하여 Firepower가 해당 트래픽에 대해 수행하는 작업을 확인할 수 있습니다.

클라이언트 Hello 수정 조정

경우에 따라 문제 해결을 통해 Firepower가 특정 트래픽의 암호를 해독하는 데 문제에 있음을 확인할 수 있습니다. **system support ssl-client-hello-tuning** 유틸리티를 CLI에서 실행하면 Firepower가 클라이언트 hello 패킷에서 특정 데이터를 제거할 수 있습니다.

아래 예에서는 특정 TLS 확장이 제거되도록 설정이 추가되었습니다. 숫자 ID는 TLS 확장 및 표준에 대한 정보를 검색하여 찾을 수 있습니다.

> **주의**: 클라이언트 hello 수정 변경 사항을 적용하기 전에 Snort 프로세스를 재시작해야 하는데, 그렇게 하면 일부 패킷이 삭제될 수 있습니다. TCP 트래픽과 같은 상태 저장 프로토콜은 재전송되지만, UDP와 같은 다른 트래픽은 부정적인 영향을 받을 수 있습니다.

```
> 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

클라이언트 hello 수정 설정에 대한 변경 사항을 되돌리려면 **system support ssl-client-hello-reset** 명령을 실행하면 됩니다.

TAC에 제공할 데이터

데이터	지침
FMC(Firepower Management Center) 및 Firepower 디바이스에서 파일 문제 해결	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-te
SSL 디버그	지침은 이 문서를 참조하십시오.
전체 세션 패킷 캡처(가능한 경우 클라이언트 측, Firepower 디바이스 자체 및 서버측에서)	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-app
연결 이벤트 스크린샷 또는 보고서	지침은 이 문서를 참조하십시오.

다음 단계

SSL 정책 구성 요소가 문제의 원인이 아닌 것으로 확인된 경우, 다음 단계로 활성 인증 기능의 문제 해결을 수행합니다.

다음 문서로 이동하려면 여기를 클릭하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.