

# Firepower Management Center에서 보안 인텔리전스 피드 업데이트 실패 문제 해결

## 목차

[소개](#)

[배경](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[웹 GUI에서 문제 확인](#)

[CLI에서 문제 확인](#)

[솔루션](#)

[관련 정보](#)

## 소개

이 문서에서는 보안 인텔리전스 피드 업데이트 관련 문제를 해결하는 방법에 대해 설명합니다.

## 배경

보안 인텔리전스 피드는 Cisco Talos Security Intelligence and Research Group(Talos)에서 확인한 바와 같이 평판이 나쁜 여러 개의 정기적으로 업데이트되는 IP 주소 목록으로 구성됩니다. Cisco Firepower System에서 네트워크 트래픽을 필터링하기 위해 최신 정보를 사용할 수 있도록 인텔리전스 피드를 정기적으로 업데이트해야 합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Firepower Management Center
- 보안 인텔리전스 피드

### 사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 5.2 이상을 실행하는 Cisco Firepower Management Center를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

# 문제

보안 인텔리전스 피드 업데이트 실패가 발생합니다. 웹 GUI 또는 CLI를 통해 오류를 확인할 수 있습니다(다음 섹션에서 자세히 설명).

## 웹 GUI에서 문제 확인

보안 인텔리전스 피드 업데이트 오류가 발생하면 Firepower Management Center에 상태 알림이 표시됩니다.

## CLI에서 문제 확인

보안 인텔리전스 피드를 사용한 업데이트 실패의 근본 원인을 확인하려면 Firepower Management Center의 CLI에 다음 명령을 입력합니다.

```
admin@Sourcefire3D:~$ cat /var/log/messages  
메시지에서 다음 경고 중 하나를 검색합니다.
```

```
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download  
Sourcefire_Intelligence_Feed
```

```
Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download  
unsuccessful: Failure when receiving data from the peer
```

## 솔루션

문제를 해결하려면 다음 단계를 완료하십시오.

1. 다음을 확인합니다. [intelligence.sourcefire.com](https://intelligence.sourcefire.com) 사이트가 활성 상태입니다.  
<https://intelligence.sourcefire.com>으로 [이동합니다](#). 브라우저를 엽니다.
2. SSH(Secure Shell)로 Firepower Management Center의 CLI에 액세스합니다.
3. 핑 [intelligence.sourcefire.com](https://intelligence.sourcefire.com) Firepower Management Center에서

```
admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.verify  
you receive an output similar to this:
```

```
64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05  
if you do not receive a response similar to that shown, then you can have an outbound connectivity issue, or you do not have a route to intelligence.sourcefire.com.
```

4. 의 호스트 이름 확인 [intelligence.sourcefire.com](https://intelligence.sourcefire.com):

```
admin@Firepower:~$ sudo nslookup intelligence.sourcefire.com  
다음과 유사한 응답을 수신했는지 확인합니다.
```

Server: 8.8.8.8  
Address: 8.8.8.8#53

Name: intelligence.sourcefire.com  
Address: xxx.xxx.xx.x

**참고:** 앞서 설명한 출력에서는 Google DNS(Public Domain Name System) 서버를 예로 사용합니다. 출력은 System(시스템) > Local(로컬) > Configuration(컨피그레이션)에서 구성한 DNS 설정에 따라 달라집니다. Network 섹션을 참조하십시오. 표시된 것과 유사한 응답을 받지 못한 경우 DNS 설정이 올바른지 확인합니다.주의: 서버는 로드 밸런싱, 내결함성 및 업타임을 위해 라운드 로빈 IP 주소 스키마를 사용합니다. 따라서 IP 주소가 변경될 수 있으며, 방화벽은 CNAME IP 주소 대신 사용됩니다.

5. 연결 확인 intelligence.sourcefire.com Telnet을 사용하는 경우:

```
admin@Firepower:~$ sudo telnet intelligence.sourcefire.com 443
```

다음과 유사한 출력을 수신했는지 확인합니다.

```
Trying xxx.xxx.xx.x...  
Connected to intelligence.sourcefire.com.  
Escape character is '^]'.  
intelligence.sourcefire.com
```

**참고:** 두 번째 단계를 성공적으로 완료할 수 있지만 텔넷을 통해 다음을 수행할 수 없는 경우 intelligence.sourcefire.com 포트 443을 통해 포트 443 아웃바운드를 차단하는 방화벽 규칙이 있을 수 있습니다. intelligence.sourcefire.com.

6. System(시스템) > Local(로컬) > Configuration(컨피그레이션)으로 이동하고 의 프록시 설정을 확인합니다. Manual Proxy 구성 Network 섹션을 참조하십시오.

**참고:** 이 프록시가 SSL(Secure Sockets Layer) 검사를 수행하는 경우 다음에 대한 프록시를 우회하는 우회 규칙을 적용해야 합니다. intelligence.sourcefire.com.

7. 다음을 수행할 수 있는지 테스트 HTTP GET 다음에 대한 요청 intelligence.sourcefire.com:

```
admin@Firepower:~$ sudo curl -vvk https://intelligence.sourcefire.com
```

\* About to connect() to intelligence.sourcefire.com port 443 (#0)  
\* Trying 198.148.79.58...  
\* Adding handle: conn: 0xec5630  
\* Adding handle: send: 0  
\* Adding handle: recv: 0  
\* Curl\_addHandleToPipeline: length: 1  
\* - Conn 0 (0xec5630) send\_pipe: 1, recv\_pipe: 0  
\* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)  
\* SSLv3, TLS handshake, Client hello (1):  
\* SSLv3, TLS handshake, Server hello (2):  
\* SSLv3, TLS handshake, CERT (11):  
\* SSLv3, TLS handshake, Server key exchange (12):  
\* SSLv3, TLS handshake, Server finished (14):  
\* SSLv3, TLS handshake, Client key exchange (16):  
\* SSLv3, TLS change cipher, Client hello (1):  
\* SSLv3, TLS handshake, Finished (20):  
\* SSLv3, TLS change cipher, Client hello (1):  
\* SSLv3, TLS handshake, Finished (20):  
\* SSL connection using DHE-RSA-AES256-SHA  
\* Server certificate:  
\* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;  
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;  
CN=intelligence.sourcefire.com

```

* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
: )
* Connection #0 to host intelligence.sourcefire.com left intact

```

**참고:** curl 명령 출력은 성공적인 연결을 나타냅니다. **참고:** 프록시를 사용하는 경우 curl 명령에는 사용자 이름이 필요합니다. 이 명령은 **curl -U <user> -vbk <https://intelligence.sourcefire.com>**입니다. 또한 명령을 입력한 후 프록시 비밀번호를 입력하라는 프롬프트가 표시됩니다.

- 보안 인텔리전스 피드를 다운로드하는 데 사용된 HTTPS 트래픽이 SSL 해독기를 통과하지 않는지 확인합니다. SSL 암호 해독이 발생하지 않는지 확인하려면 6단계의 출력에서 서버 인증서 정보를 검증합니다. 서버 인증서가 다음 예에 표시된 것과 일치하지 않을 경우 인증서를 폐기하는 SSL 해독기를 보유할 수 있습니다. 트래픽이 SSL 해독기를 통과하는 경우로 이동하는 모든 트래픽을 우회해야 합니다 intelligence.sourcefire.com.

```

admin@Firepower:~$ sudo curl -vbk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com

```

```
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

**참고:** SSL 해독기가 SSL 핸드셰이크의 알 수 없는 인증서를 Firepower Management Center에 전송하므로 보안 인텔리전스 피드에 대해 SSL 해독을 우회해야 합니다. Firepower Management Center로 전송된 인증서가 Sourcefire의 신뢰할 수 있는 CA에서 서명되지 않았으므로 연결을 신뢰할 수 없습니다.

## 관련 정보

- [자동매틱 Firepower Management Center에서 업데이트 다운로드 실패](#)
- [AMP\(Advanced Malware Protection\) 작업에 필요한 서버 주소](#)
- [Firepower 시스템 작업에 필요한 통신 포트](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.