Cisco FMC(Secure Firewall Management Center)에서 프록시 트러블슈팅

목차

소개

이 문서에서는 사용자가 중간 서버를 통해 인터넷에 연결할 수 있도록 FMC에서 프록시를 구성하여 보안을 강화하고 때로는 성능을 개선하는 방법에 대해 설명합니다. 이 문서에서는 FMC에서 프록시를 구성하는 단계를 안내하고 일반적인 문제에 대한 트러블슈팅 팁을 제공합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Secure Firewall Management Center)
- 프록시

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMC 7.4.x

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.

설정

FMC GUI에서 네트워크 http-proxy를 구성합니다.

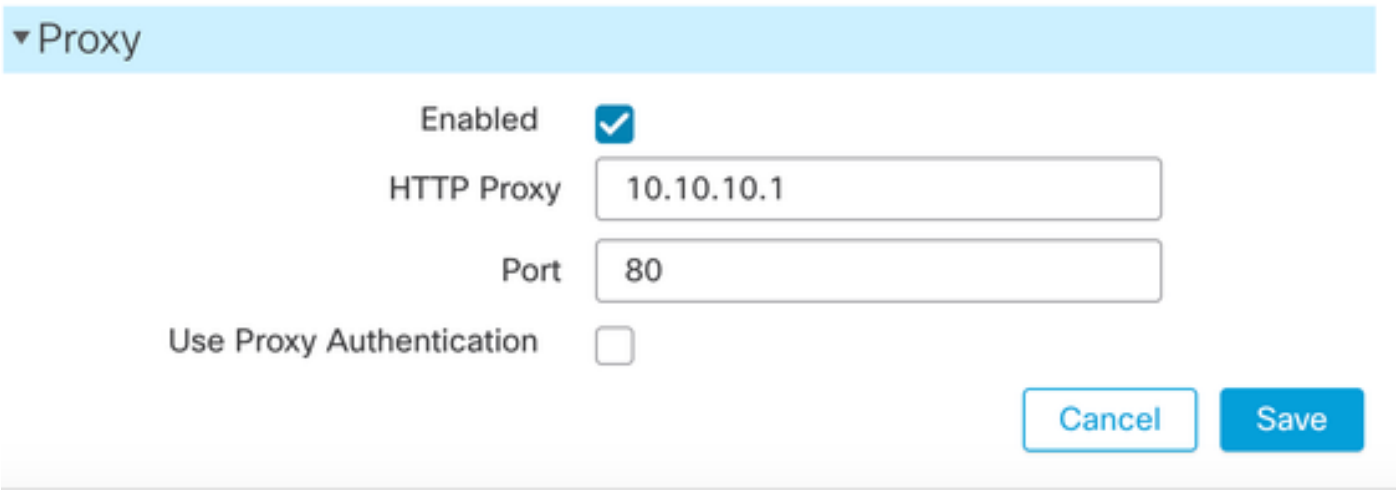
Login FMC GUI(FMC GUI) > System(시스템) > Configuration(컨피그레이션)을 선택한 다음 Management Interfaces(관리 인터페이스)를 선택합니다.

참고: NTLM(NT LAN Manager) 인증을 사용하는 프록시는 지원되지 않습니다. Smart Licensing을 사용하는 경우 프록시 FQDN은 64자를 초과할 수 없습니다.

Proxy(프록시) 영역에서 HTTP 프록시 설정을 구성합니다.

관리 센터는 포트 TCP/443(HTTPS) 및 TCP/80(HTTP)에서 인터넷에 직접 연결하도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다.

- Enabled(활성화됨) 확인란을 선택합니다.
- HTTP Proxyfield(HTTP 프록시 필드)에 프록시 서버의 IP 주소 또는 정규화된 도메인 이름을 입력합니다.
- 포트 필드에 포트 번호를 입력합니다.
- Use Proxy Authentication(프록시 인증 사용)을 선택하여 인증 자격 증명을 제공한 다음 사용자 이름과 비밀번호를 제공합니다.
- 저장을 클릭합니다.



참고: 프록시 비밀번호에는 A-Z, a-z, 0-9 및 특수 문자를 사용할 수 있습니다.

문제 해결

FMC CLI 및 expert 모드에 액세스한 다음 iprep_proxy.conf를 확인하여 프록시 설정이 올바른지 확인합니다.

<#root>

admin@fmc:~$

cat /etc/sf/iprep_proxy.conf

iprep_proxy {
PROXY_HOST 10.10.10.1;
PROXY_PORT 80;
}

활성 프록시 연결을 확인하려면 활성 연결을 확인합니다.

<#root>

admin@fmc:~$

netstat -na | grep 10.10.10.1

tcp 0 0 10.40.40.1:40220 10.10.10.1:80

ESTABLISHED

curl 명령을 사용하여 요청 세부사항과 프록시의 응답을 모두 확인합니다. 응답을 수신할 경우: HTTP/1.1 200 Connection established(HTTP/1.1 200 연결 설정), 이는 FMC가 프록시를 통해 트래픽을 성공적으로 전송 및 수신하고 있음을 나타냅니다.

<#root>

admin@fmc:~$

curl -x http://10.10.10.1:80 -I https://tools.cisco.com

HTTP/1.1 200 Connection established

프록시에 대한 사용자 이름 및 비밀번호를 구성한 경우 인증 및 프록시 응답을 확인합니다.

```
curl -u proxyuser:proxypass --proxy http://proxy.example.com:80 https://example.com
```

확인

프록시를 통한 연결 설정 성공

프록시와 함께 curl 명령을 실행할 때(예: curl -x http://proxy:80 -I https://tools.cisco.com) 일련의 예상 네트워크 상호 작용이 발생하며, 이는 패킷 캡처(tcpdump)를 통해 관찰할 수 있습니다. 이것은 실제 tcpdump 출력으로 보강된 프로세스의 상위 레벨 개요입니다.

TCP 핸드셰이크 시작:
클라이언트(FMC)는 SYN 패킷을 전송하여 포트 80의 프록시 서버에 대한 TCP 연결을 시작합니다. 프록시가 SYN-ACK로 응답하고 클라이언트가 ACK로 핸드셰이크를 완료합니다. 이렇게 하면 HTTP 통신이 진행되는 TCP 세션이 설정됩니다.

tcpdump 출력 예:

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

HTTP 연결 요청:
TCP 연결이 설정되면 클라이언트는 대상 HTTPS 서버(tools.cisco.com:443)에 터널을 만들도록 지시하는 HTTP CONNECT 요청을 프록시에 전송합니다. 이 요청을 통해 클라이언트는 프록시를 통해 엔드 투 엔드 TLS 세션을 협상할 수 있습니다.

예 tcpdump(디코딩된 HTTP):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

연결 설정 승인:
프록시가 HTTP/1.1 200 Connection established 응답으로 응답하며, 이는 대상 서버에 대한 터널이 성공적으로 생성되었음을 나타냅니다. 즉, 이제 프록시가 릴레이 역할을 하며 클라이언트와

tools.cisco.com 간에 암호화된 트래픽을 전달합니다.

예: tcpdump

<#root>

```
HTTP/1.1

200

 Connection established
```

터널을 통한 HTTPS 통신:
성공적인 CONNECT 응답 후 클라이언트는 설정된 터널을 통해 tools.cisco.com과 직접 SSL/TLS 핸드셰이크를 시작합니다. 이 트래픽은 암호화되므로 tcpdump에서 내용을 볼 수 없지만 TLS 클라이언트 Hello 및 서버 Hello 패킷을 비롯한 패킷 길이 및 시간이 표시됩니다.

예: tcpdump

```
10:20:59.123456 IP client.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > client.54321: Flags [P.], length 1514 (Server Hello)
```

HTTP 리디렉션 처리(302 찾음):
HTTPS 통신의 일환으로 클라이언트는 tools.cisco.com에서 리소스를 요청합니다. 서버는 HTTP/1.1 302 Found redirect to another URL(https://tools.cisco.com/healthcheck)로 응답하며, 클라이언트는 curl 매개 변수 및 요청의 목적에 따라 이를 따를 수 있습니다. 이 리디렉션은 암호화된 TLS 세션 내에서 발생하며 직접 표시되지 않지만, 예상된 동작이며 TLS 트래픽의 암호를 해독하는 경우 관찰될 수 있습니다.

암호화된 리디렉션 트래픽은 다음과 같이 표시됩니다.

```
10:21:00.123000 IP client.54321 > proxy.80: Flags [P.], length 517 (Encrypted Application Data)
10:21:00.123045 IP proxy.80 > client.54321: Flags [P.], length 317 (Encrypted Application Data)
```

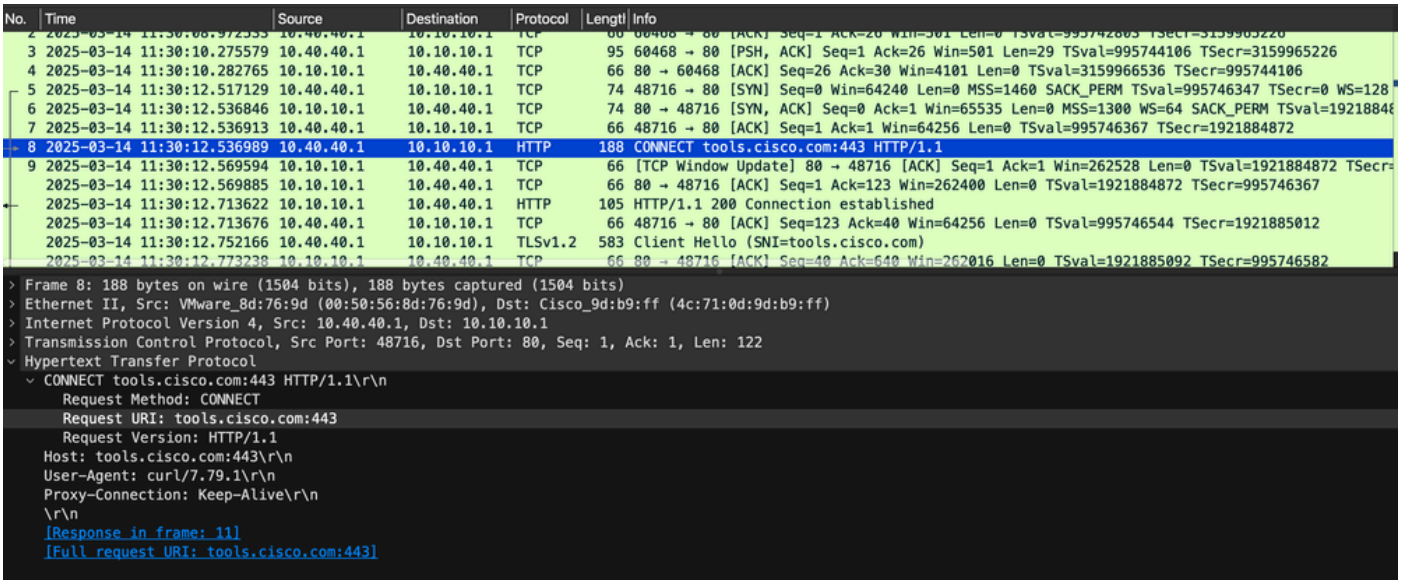
연결 해제:
교환이 완료되면 클라이언트와 프록시 모두 FIN 패킷과 ACK 패킷을 교환하여 TCP 연결을 정상적으로 닫아 적절한 세션 종료를 보장합니다.

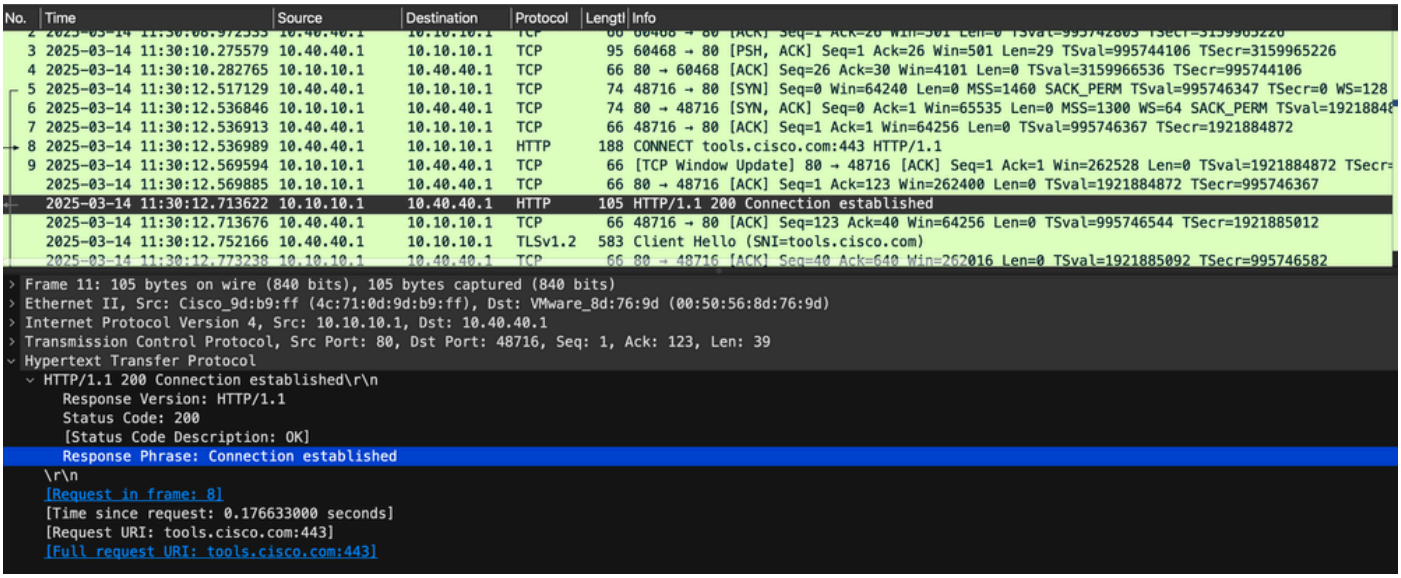
tcpdump 출력 예:

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```

팁: tcpdump 출력을 분석하면 명시적 프록시를 통한 HTTPS 요청이 예상 플로우를 따르는지 확인할 수 있습니다. TCP 핸드셰이크, CONNECT 요청, 터널 설정, TLS 핸드셰이크, 암호화된 통신(가능한 리디렉션 포함) 및 정상적인 연결 닫힘 이렇게 하면 프록시 및 클라이언트 상호 작용이 설계된 대로 작동하며 터널링 또는 SSL 협상 실패와 같은 흐름의 모든 문제를 식별할 수 있습니다.

FMC(10.40.40.1)는 포트 80에서 프록시(10.10.10.1)와의 성공적인 TCP 핸드셰이크를 설정한 다음, 포트 443에서 서버에 대한 HTTP 연결(72.163.4.161)을 설정합니다. 서버는 HTTP 200 연결 설정 메시지로 응답합니다. TLS 핸드셰이크가 완료되고 데이터가 제대로 흐릅니다. 마지막으로 TCP 연결이 정상적으로 종료됩니다(FIN).





알려진 문제

프록시 ACL 제한 사항

권한 문제(예: 프록시의 액세스 목록)가 있는 경우 패킷 캡처(tcpdump)를 통해 이를 확인할 수 있습니다. 다음은 tcpdump 출력 예와 함께 오류 시나리오에 대한 개괄적인 설명입니다.

TCP 핸드셰이크 시작:
클라이언트(Firepower)는 포트 80에서 프록시에 대한 TCP 연결을 설정하는 것으로 시작합니다. TCP 핸드셰이크(SYN, SYN-ACK, ACK)가 성공적으로 완료됩니다. 이는 프록시에 연결할 수 있음을 의미합니다.

tcpdump 출력 예:

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

HTTP 연결 요청:
일단 연결되면 클라이언트는 tools.cisco.com:443에 대한 터널을 생성하도록 요청하는 HTTP CONNECT 요청을 프록시에 전송합니다.

예 tcpdump(디코딩된 HTTP):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

프록시의 오류 응답:

이 트래픽을 허용하지 않는 ACL(Access List)로 인해 프록시가 터널을 허용하는 대신 요청을 거부합니다. 프록시가 403 Forbidden 또는 502 Bad Gateway와 같은 오류로 응답합니다.

오류를 표시하는 tcpdump 출력의 예:

<#root>

HTTP/1.1

403

```
 Forbidden
Content-Type: text/html
Content-Length: 123
Connection: close
```

연결 해제:
오류 메시지를 보낸 후 프록시가 연결을 닫고 양측이 FIN/ACK 패킷을 교환합니다.

tcpdump 출력 예:

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```


팁: tcpdump에서 TCP 연결 및 HTTP CONNECT 요청이 성공했지만 프록시에서 터널 설정을 거부했음을 확인할 수 있습니다. 이는 일반적으로 프록시에 트래픽 통과를 방해하는 ACL 또는 권한 제한이 있음을 나타냅니다.

프록시 다운로드 실패(시간 초과/전송 불완전)

이 시나리오에서 FMC는 프록시에 성공적으로 연결하고 파일 다운로드를 시작하지만 전송 시간이 초과되거나 완료되지 않습니다. 이는 일반적으로 프록시에 대한 프록시 검사, 시간 초과 또는 파일 크기 제한 때문입니다.

TCP 핸드셰이크 시작
FMC는 포트 80에서 프록시에 대한 TCP 연결을 시작하고 핸드셰이크가 성공적으로 완료됩니다.
tcpdump 출력 예:

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

HTTP CONNECT 요청
FMC는 외부 대상에 연결하기 위해 프록시에 HTTP CONNECT 요청을 보냅니다.
예 tcpdump(디코딩된 HTTP):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

터널 설정 및 TLS 핸드셰이크
프록시가 설정된 HTTP/1.1 200 연결로 응답하므로 TLS 핸드셰이크가 시작될 수 있습니다.

tcpdump 출력 예:

```
<#root>

HTTP/1.1

200

 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

시간 초과 또는 불완전한 다운로드
파일 전송을 시작한 후 다운로드가 중단되거나 완료되지 않아 시간 초과가 발생합니다. 연결이 유휴 상태로 유지됩니다.
가능한 원인은 다음과 같습니다.

- 프록시 검사 지연 또는 필터링.
- 긴 전송에 대한 프록시 시간 제한입니다.
- 프록시에서 지정한 파일 크기 제한

비활성 상태를 표시하는 tcpdump 예:

```
<#root>

10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440

# FMC sending data


# No response from proxy, connection goes idle...


# After a while, FMC may close the connection or retry.
```

팁: FMC는 다운로드를 시작하지만 프록시 필터링 또는 파일 크기 제한으로 인해 종종 발생하는 시간 초과 또는 불완전한 전송으로 인해 다운로드를 완료하지 못합니다.

프록시 파일 다운로드 실패(MTU 문제)

이 경우 FMC는 프록시에 연결하여 파일 다운로드를 시작하지만 MTU 문제로 인해 세션이 실패합니다. 이러한 문제로 인해 특히 대용량 파일 또는 SSL/TLS 핸드셰이크의 경우 패킷 조각화 또는 삭제된 패킷이 발생합니다.

TCP 핸드셰이크 시작
FMC는 프록시와 TCP 핸드셰이크를 시작하며, 이는 성공합니다.
tcpdump 출력 예:

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

HTTP CONNECT 요청 및 터널 설정
FMC가 HTTP CONNECT 요청을 전송하고 프록시가 응답하면서 터널을 설정할 수 있습니다.
예 tcpdump(디코딩된 HTTP):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

TLS 핸드셰이크 시작
FMC와 tools.cisco.com에서 SSL/TLS 협상을 시작하고 초기 패킷이 교환됩니다.
tcpdump 출력 예:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

MTU로 인한 패킷 조각화 또는 삭제
FMC 또는 서버가 대용량 패킷을 전송하려고 할 때 MTU 문제로 인해 패킷 조각화 또는 패킷 삭제로 인해 파일 전송 또는 TLS 협상 실패가 발생합니다.

이는 일반적으로 FMC와 프록시 간(또는 프록시와 인터넷 간) MTU가 잘못 설정되었거나 너무 작을 때 발생합니다.
프래그먼트화 시도를 보여 주는 tcpdump 예:

<#root>

```
10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440
# Large packet

10:21:00.456123 IP proxy.80 > fmc.54321: Flags [R], seq X, win 0, length 0
# Proxy resets connection due to MTU issue
```

팁: MTU를 실행하면 패킷이 삭제되거나 조각화되며, 이로 인해 TLS 핸드셰이크가 중단되거나 파일 다운로드가 실패합니다. 이는 잘못된 MTU 설정으로 인해 SSL 검사 또는 패킷 조각화가 발생하는 경우에 일반적으로 나타납니다.

실패 시나리오에서 FMC는 HTTP 200 없이 CONNECT를 가져오며, 재전송 및 FIN에서 TLS/데이터 교환을 확인하지 않으며, 이는 MTU 문제 또는 프록시/업스트림 문제 때문일 수 있습니다.

curl을 사용할 때 서버 측 문제 또는 인증 오류를 나타내는 다양한 HTTP 응답 코드가 나타날 수 있습니다. 다음은 가장 일반적인 오류 코드 및 그 의미의 목록입니다.

HTTP 코드	의미	원인
400	잘못된 요청	잘못된 요청 구문
401	인증되지 않음	자격 증명 누락 또는 오류
403	금지됨	액세스 거부됨
404	찾을 수 없음	리소스를 찾을 수 없음
500	내부 오류	서버 오류
502	잘못된 게이트웨이	서버 통신 오류
503	서비스를 사용할 수 없음	서버 오버로드 또는 유지 보수
504	게이트웨이 시간 초과	서버 간 시간 초과

참조

Cisco Secure Firewall Threat Defense 릴리스 노트, 버전 7.4.x

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.