SWG 웹 사이트 액세스 문제 해결

목차

소개

배경 정보

업스트림 블록으로 인한 "액세스 거부 403" 오류

Java 문제로 인한 "액세스 거부 403" 오류

문제의 상위 레벨 근본 원인

- MPS의 Java 관련 문제는 무엇입니까?
  - 해결

502 Bad Gateway란 무엇입니까?

502 불량 게이트웨이의 공통 요인

- 지원되지 않는 SWG 암호 그룹
  - 해결
- 클라이언트 인증서 인증 요청
- 프록시에서 추가된 헤더
  - 해결

소개

이 문서에서는 Umbrella SWG(Secure Web Gateway) 프록시에 나타나는 웹 사이트 액세스 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

www.xyz.com 웹 사이트는 SWG 프록시를 통해 액세스할 수 없으며 사용자가 인터넷에 직접 액세스하려고 할 때(그림에 Umbrella SWG가 없는 경우) 정상적으로 작동합니다. SWG를 통해 웹 사이트에 액세스할 수 없을 때 보고된 다양한 증상과 다양한 유형의 오류 메시지를 검토해 보겠습니다. 가장 일반적인 게이트웨이는 502 불량 게이트웨이, 502 메시지 업스트림 오류를 릴레이할 수 없음, 업스트림 인증서가 취소됨, 액세스 거부 403 금지, 업스트림 암호가 일치하지 않음, 웹 사이트가 잠시 동안 회전한 후 시간 초과되었습니다.

업스트림 블록으로 인한 "액세스 거부 403" 오류

웹 서버 또는 업스트림 측에서 SWG 프록시 이그레스 IP 범위를 차단 또는 제한하고 있습니다. 예를 들어, Akamai WAF는 2개의 SWG 이그레스 IP 범위를 차단했습니다. 이 문제를 해결하려면 웹 사이트 관리자에게 연락하여 IP 범위 차단을 해제하도록 하는 옵션뿐입니다. 그때까지는 Anyconnect SWG 및 PAC 파일 구축을 위해 외부 도메인 관리 목록을 사용하여 SWG를 우회합니다. 간단히 말해, 이러한 유형의 문제는 프록시 자체가 아니라 프록시와 웹 서버 간의 비호환성 때문입니다. 이그레스 IP 블록으로 인한 "액세스 거부 403" 오류에 대해 KB를 구체적으로 참조하기 위한 링크입니다.

또한 Akamai가 차단 목록 IP 주소를 보유한 몇 가지 이유를 설명하는 링크도 있습니다.

Java 문제로 인한 "액세스 거부 403" 오류

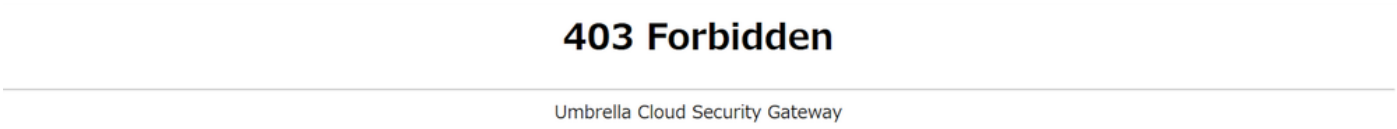
웹 사이트에 액세스할 수 없으며 파일 검사 설정이 활성화된 상태에서 SWG MPS 프록시를 통해 요청이 전송되면 "액세스 거부 또는 403 금지 - Umbrella 클라우드 보안 게이트웨이 오류"가 발생합니다. 그러나 File Inspection(파일 검사)이 비활성화되면 웹 사이트가 성공적으로 로드됩니다. 또는 웹 사이트를 우회 암호 해독에 넣으면 웹사이트가 성공적으로 로드됩니다.

문제의 상위 레벨 근본 원인

MPS의 Java 관련 문제는 무엇입니까?

프록시에서 서버에 연결을 시도한 후 해당 사이트 또는 웹 서버가 SNI 또는 SSL 경고에 대한 TLS 경고를 프록시에 다시 반환합니다. 기본적으로 이것은 고객 hello가 전송된 이후에 발생합니다. MPS 프록시(Java를 기반으로 함)는 기본적으로 설명 필드에 "Unrecognized Name"이 있는 TLS 알림을 SNI 구문 분석 중 오류로 처리하고 트랜잭션을 종료합니다. 자세한 내용은 여기를 참조하십시오.

이는 SWG 또는 MPS 프록시 문제가 아닙니다. 이는 서버 측의 잘못된 컨피그레이션으로 인한 SWG 또는 기타 프록시와의 비호환성 중 하나입니다. 브라우저에서는 일반적으로 이 경고를 무시하지만 SWG 또는 기타 콘텐츠 보안 필터는 SSL 경고를 치명적인 오류로 간주하고 세션을 종료하며, 이로 인해 사용자에게 403개의 금지된 오류 페이지가 표시됩니다. 또한 502 Bad Gateway(잘못된 게이트웨이) 오류를 보고할 수 있지만, 이 그림에서 볼 수 있듯이 대부분의 예에서는 403 Forbidden(금지된 403) 오류입니다.



15151734443924

MPS는 애플리케이션 레이어에서 작동하므로 TLS 프로토콜에서 생성된 알림을 기반으로 TLS 레이어가 트랜잭션을 처리하는 방법을 거의 또는 전혀 제어할 수 없습니다. TLS 엔드포인트/인증서가 올바르게 구성되었는지 확인하는 것은 서버의 책임입니다. 이 링크를 참조하십시오.

문제를 좁히거나 트러블슈팅하기 위해 SSL Lab에서 쉽게 지적할 수 있습니다.

15152060146964

중간에 SWG 프록시 없이 웹 사이트에 액세스하거나 SWG에서 HTTPS 검사를 우회하는 경우 브라우저에서 SNI Unrecognized name(SNI 알 수 없음 이름) 알림을 무시하고 웹 서버와의 통신을 계속하기 때문에 웹 사이트가 작동합니다.

이 기사를 쓸 때, 권장되는 해결책은 우리가 여러분에게 제안할 수 있는 최고의 완화이다. 머지않아 새로운 프록시 아키텍처를 통해 이러한 문제를 더욱 원활하게 처리할 수 있게 될 것입니다.

해결

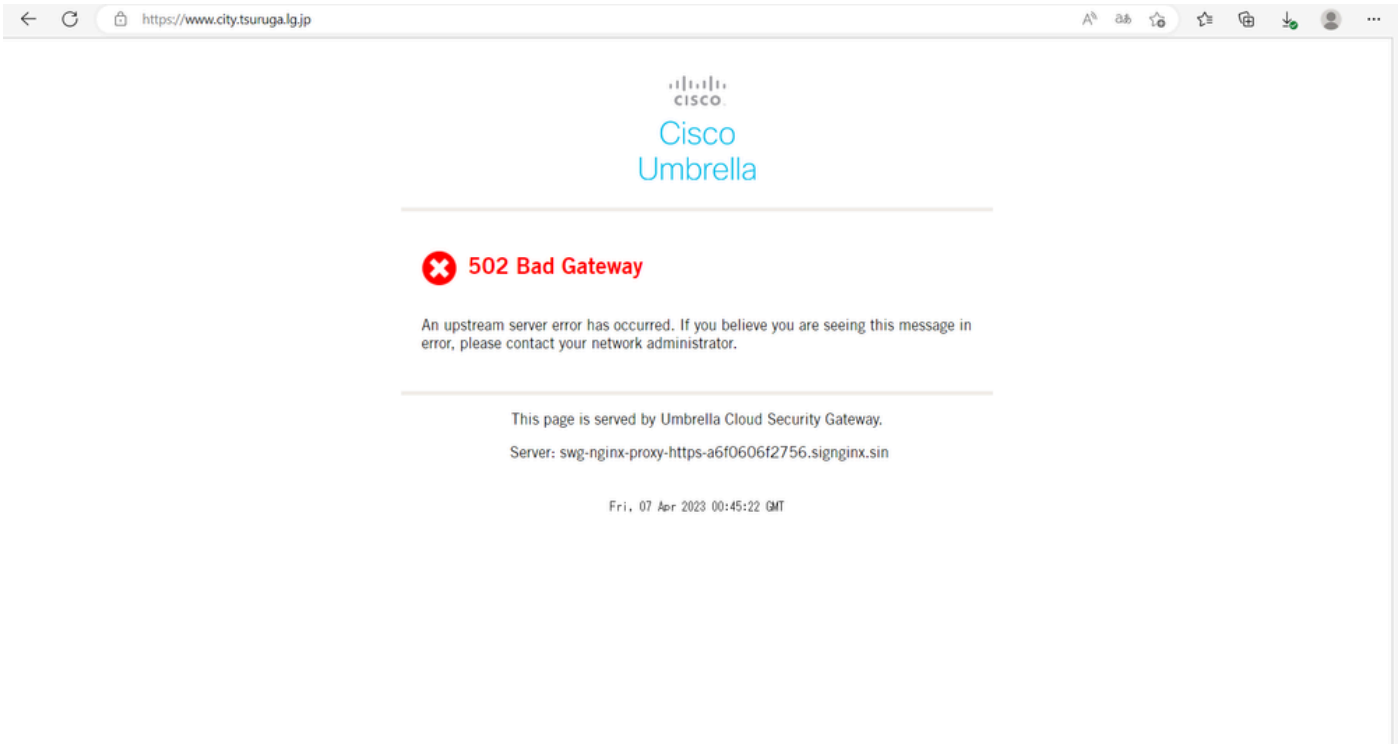
1. 영향을 받는 도메인에 대한 암호 해독 사용 안 함 - 또는
2. 도메인을 대상 목록에 추가하고 허용 규칙을 연결합니다(사이트를 신뢰하는 경우).

502 Bad Gateway란 무엇입니까?

502 Bad Gateway Error(502 잘못된 게이트웨이 오류)는 서버가 게이트웨이 또는 프록시 역할을 하며 업스트림 서버로부터 잘못된 응답을 받았음을 의미합니다. 사용자가 SWG 프록시를 통해 웹 사이트에 액세스하려고 하면 두 가지 통신 흐름이 발생합니다.

a) 클라이언트 —> 프록시 연결(다운스트림)
b) 프록시—> 웹 서버 연결 종료(업스트림)

502 SWG 프록시(MPS, Nginx)와 엔드 서버 연결 간에 잘못된 게이트웨이 오류가 발생했습니다.



15026978020884

502 불량 게이트웨이의 공통 요인

1. 지원되지 않는 SWG 암호 그룹

2. 클라이언트 인증서 인증 요청

3. SWG 프록시에서 추가 또는 제거한 헤더

지원되지 않는 SWG 암호 그룹

TLS 협상 중에 지원되지 않는 SWG 암호 그룹을 보고하는 웹 서버를 가정해 보겠습니다. SWG MPS(Modular Proxy Service) 프록시는 TLS_CHACHA20_POLY1305_SHA256 암호 그룹을 지원하지 않습니다. SWG 지원 암호 모음과 TLS를 다룬 기사가 따로 있으니 참고하시기 바랍니다. 클라이언트 hello 및 서버 hello에서 암호 그룹 교환 중에 캡처된 다른 패킷을 검토하면 이 문제를 쉽게 파악할 수 있습니다. 트러블슈팅 단계로 CURL 명령을 사용하여 특정 암호를 사용하여 문제를 좁히고 예 1 및 2와 같이 암호 그룹으로 인한 것인지 확인합니다.

Curl 명령의 예:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
 - curl -x  proxy.sig.umbrella.com:80 -v  xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Testing website without Proxy

```
: - curl -v www.xyz.com:80
```

Mac/Linux:

```
  - curl -vvv -o /dev/null -k -L www.cnn.com
```

Windows:

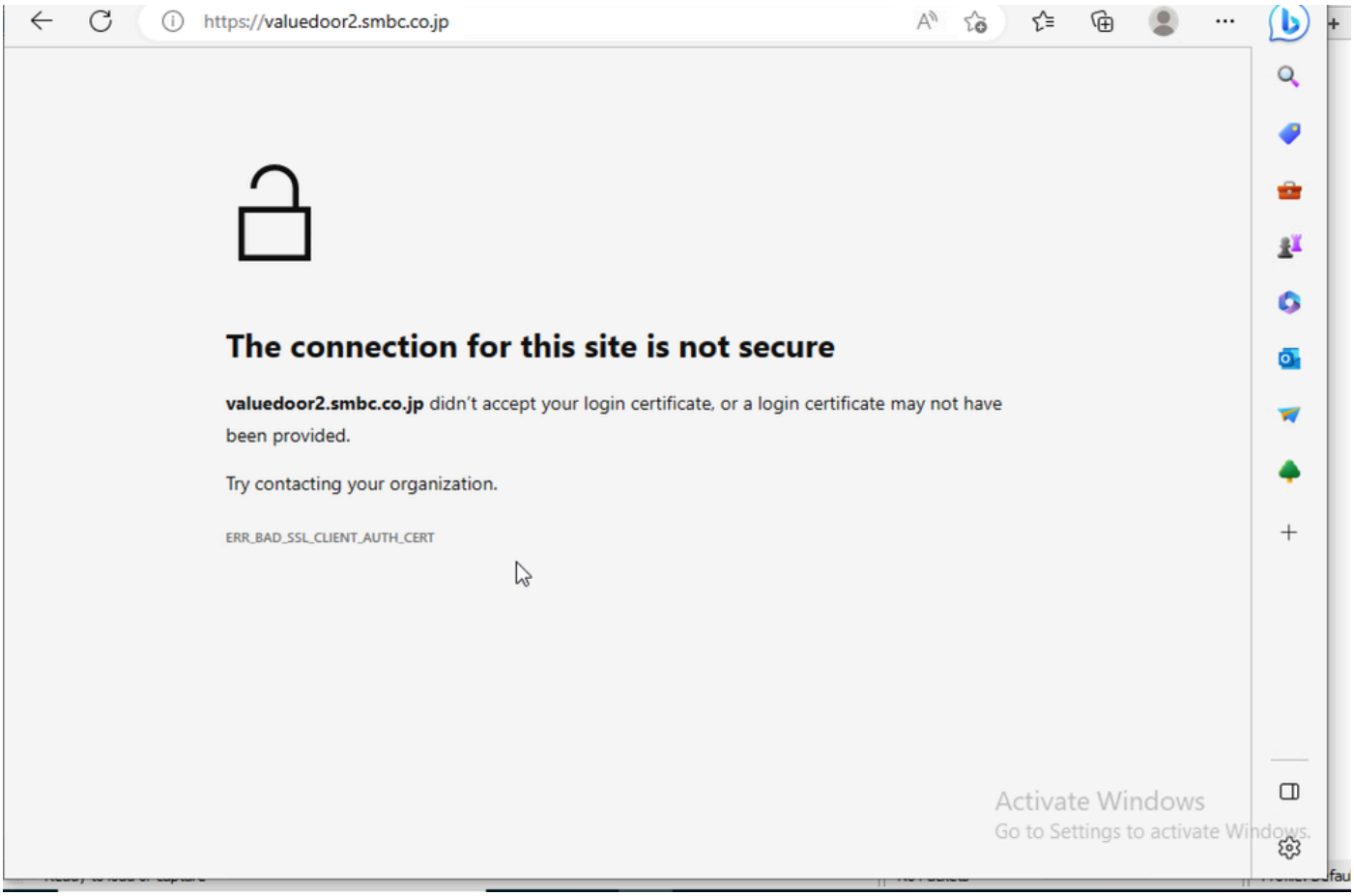
```
 - curl -vvv -o null -k -L www.cnn.com
```

해결

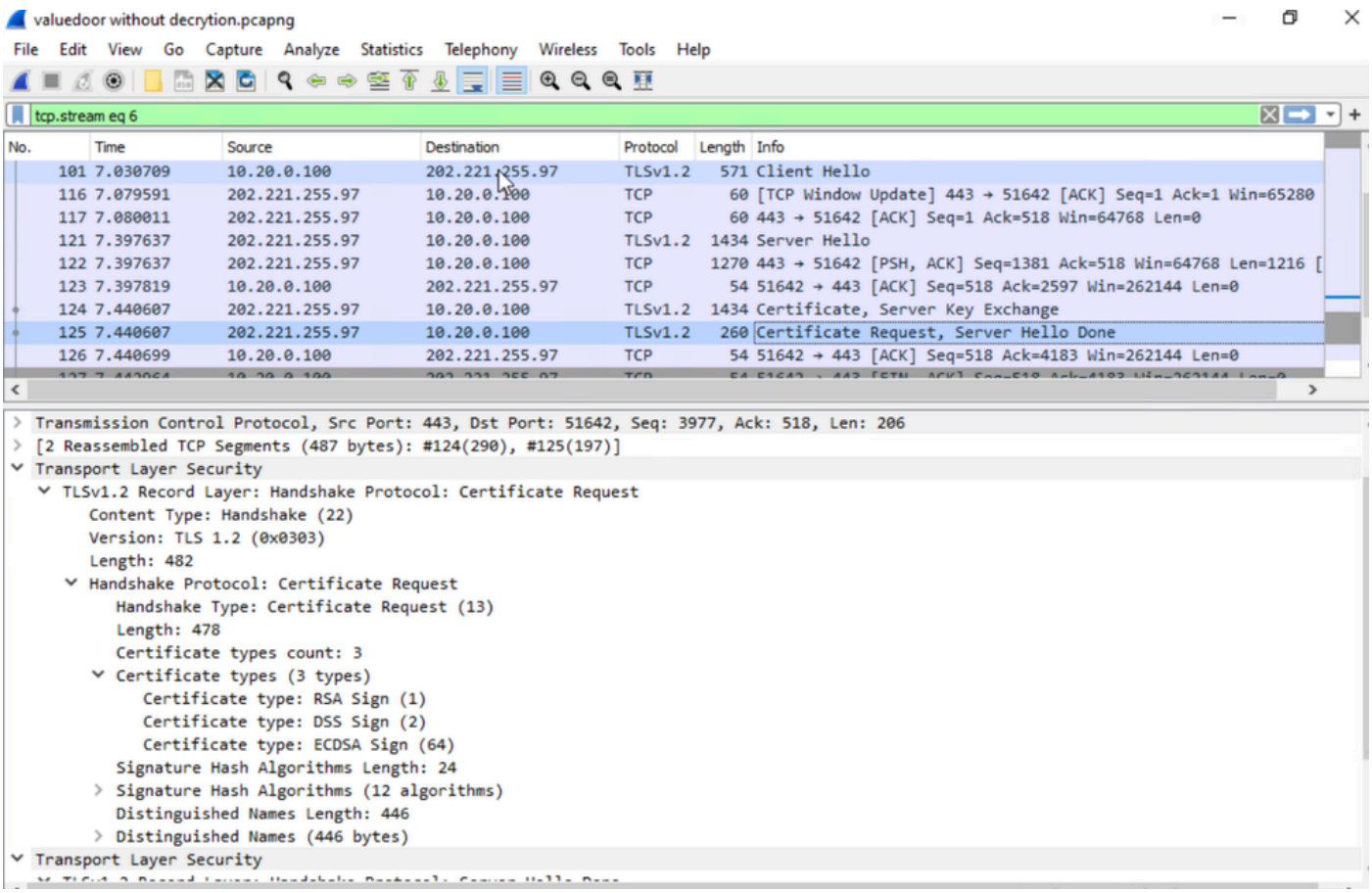
문제를 해결하려면 선택적 암호 해독 목록을 사용하여 문제가 있는 웹 사이트에 대한 검사를 건너뜁니다.

클라이언트 인증서 인증 요청

SWG 프록시와 업스트림 간의 TLS 핸드셰이크 중에 업스트림 웹 서버는 클라이언트 인증서 인증을 기대합니다. 클라이언트 인증서 인증이 지원되지 않으므로 외부 도메인 관리 목록을 사용하여 프록시에서 해당 도메인을 우회해야 하며 https 검사만 우회하는 것만으로는 충분하지 않습니다. 예를 들면 다음과 같습니다. https://valuedoor2.smbc.co.jp



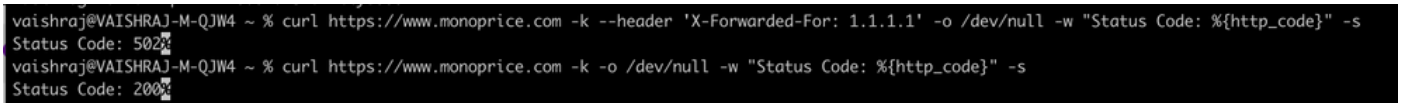
15027182308884



15027192992276

프록시에서 추가된 헤더

https 검사가 사용하도록 설정된 경우 SWG 프록시에서 XFF(X-Forward-For Header)를 추가했기 때문에 웹 서버에서 502 잘못된 게이트웨이 오류를 보고하고 있습니다. MPS 프록시를 통한 파일 검사 문제를 배제하기 위해 먼저 https 검사 사용 또는 사용 안 함, 파일 검사 사용 또는 사용 안 함 등의 문제를 해결하여 502개의 불량 게이트웨이 문제의 대부분을 쉽게 줄일 수 있습니다.



15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_co
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

HTTPS 검사가 켜져 있을 때 XFF 헤더를 사용하므로 업스트림 서버가 클라이언트 IP(사용자의 물리적 위치를 제공)를 기반으로 최적의 지리적 위치 콘텐츠를 제공할 수 있습니다.

HTTPS 검사가 활성화되지 않은 경우 이 헤더는 프록시에서 추가되지 않으므로 502 잘못된 게이트웨이 오류가 발생하지 않습니다. 이는 SWG 프록시 문제가 아닙니다. 이 오류는 업스트림 웹 서버가 표준 XFF 헤더를 지원하지 않도록 잘못 구성되었기 때문입니다.

해결

문제를 해결하려면 선택적 암호 해독 목록을 사용하여 특정 도메인에 대한 HTTPS 검사를 우회하십시오.

- 517 업스트림 인증서가 해지됨
- 인증서 및 TLS 프로토콜 오류
- 내부 테스트를 위해 수동으로 SWG DC 선택

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.