

Umbrella에서 비 브라우저 애플리케이션 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[호환성 문제](#)

[Microsoft 365 애플리케이션](#)

[인증서 피닝 바이패스](#)

[TLS 호환성 우회](#)

[문제 해결\(고급\)](#)

[인증서 피닝에 대한 제외 항목 식별](#)

[호환되지 않는 TLS 버전에 대한 제외 항목 식별](#)

소개

이 문서에서는 Cisco Umbrella에서 브라우저 이외의 애플리케이션을 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 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.

개요

이 문서에서는 Umbrella Secure Web Gateway에서 작동하도록 비 브라우저 애플리케이션을 구성하는 모범 사례 및 문제 해결 단계에 대해 설명합니다. 대부분의 경우 컨피그레이션을 변경할 필요가 없습니다. 그러나 특정 애플리케이션은 보안/검사 기능(예: SSL 암호 해독)에서 제대로 작동하지

않으며, 웹 프록시를 사용하여 애플리케이션 기능을 수행하려면 예외를 추가해야 합니다. 이는 Umbrella SWG 및 기타 웹 프록시 솔루션에 적용됩니다.

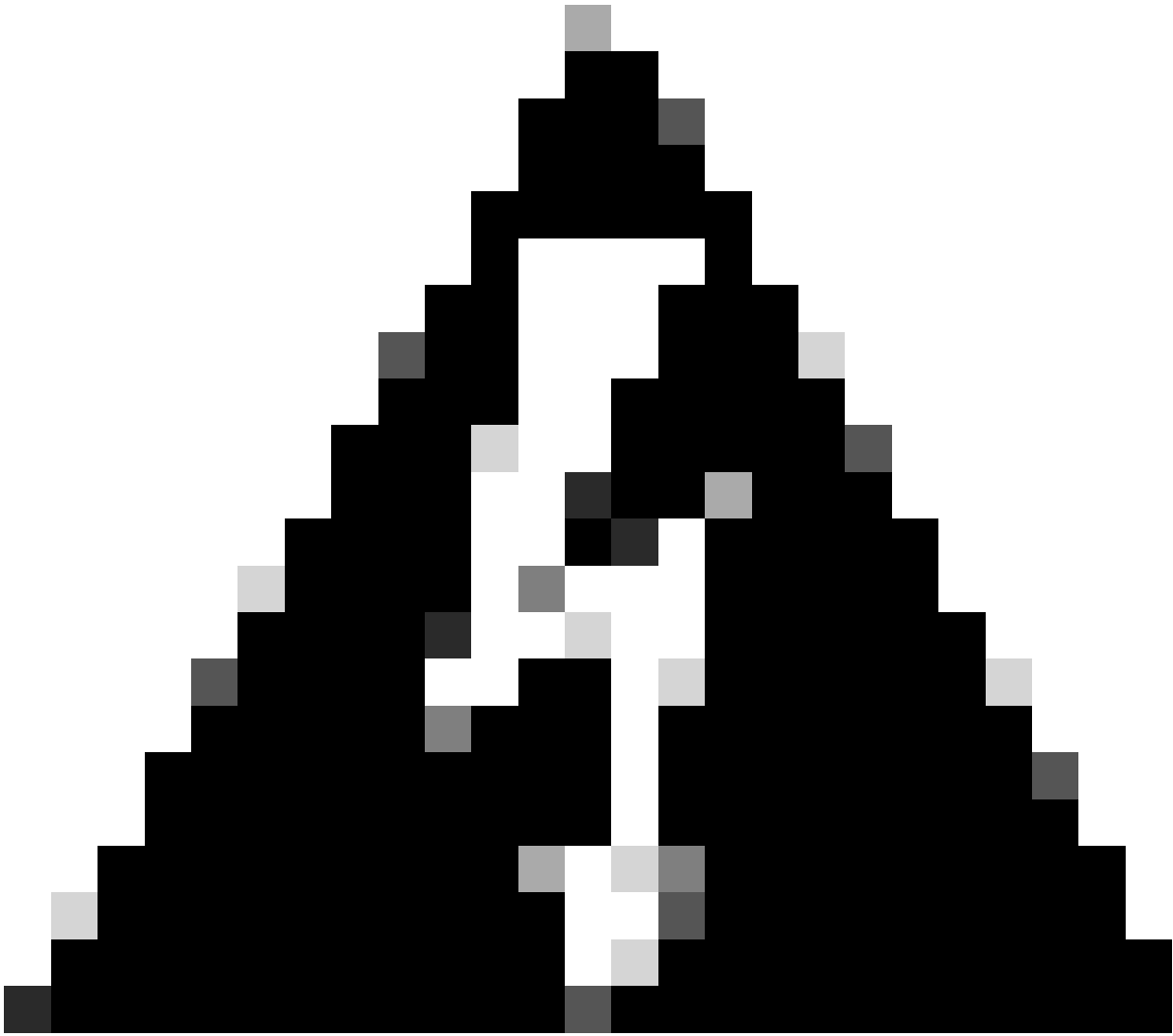
이 기능은 응용 프로그램의 웹 사이트/브라우저 버전은 작동하지만 응용 프로그램의 데스크톱/모바일 버전은 작동하지 않는 경우에 유용합니다.

호환성 문제

다음과 같은 이유로 응용 프로그램이 호환되지 않을 수 있습니다.

Umbrella Root CA 설치	Cisco Umbrella Root CA는 오류 없는 TLS 연결에 대해 항상 신뢰되어야 합니다. • 해결책: 웹 애플리케이션이 아닌 애플리케이션의 경우 시스템/로컬 머신 인증서 저장소에서 Cisco Umbrella Root CA를 신뢰해야 합니다.
인증서 피닝	PKP(Certificate Pinning)는 애플리케이션이 TLS 핸드셰이크의 유효성을 검사하기 위해 정확한 리프(또는 CA 인증서)를 받아야 하는 경우입니다. 응용 프로그램이 웹 프록시에서 생성된 인증서를 수락할 수 없으며 SSL 암호 해독 기능과 호환되지 않습니다. • 해결책: 선택적 암호 해독 목록을 사용하여 SSL 암호 해독에서 애플리케이션 또는 도메인 우회(표 다음 경고 참조) 인증서 피닝의 영향을 받는 것으로 알려진 애플리케이션에 대한 자세한 내용은 여기를 참조하십시오. 공개 키 고정/인증서 고정
TLS 버전 지원	응용 프로그램은 보안상의 이유로 SWG에서 지원되지 않는 이전 TLS 버전/암호를 사용할 수 있습니다. • 해결책: 외부 도메인 기능(PAC/AnyConnect) 또는 VPN 제외(터널)를 사용하여 Umbrella로 전송되는 트래픽을 우회합니다(표 후 경고 참조).
비 웹 프로토콜	일부 애플리케이션은 비 http(s) 프로토콜을 사용하지만 SWG에서 가로채는 일반 웹 포트를 통해 이 데이터를 전송합니다. SWG가 이 트래픽을 인식할 수 없습니다. • 해결책: 소프트웨어에서 사용하는 대상 주소/IP 범위를 확인하려면 애플리케이션 공급업체에 문의하십시오. 이 소프트웨어는 외부 도메인(PAC/AnyConnect) 또는 VPN 제외(터널)를 사용하여 SWG에서 제외해야 합니다(표 후 경고 참조).
SAML 인증	대부분의 비 브라우저 애플리케이션은 SAML 인증을 수행할 수 없습니다. Umbrella는 SAML에 대한 비 브라우저 애플리케이션에 도전하지 않으므로 사용자/그룹 기반 필터링 정책이 일치하지 않습니다. • 해결책: 비 브라우저 애플리케이션에서 사용하기 위해 사용자 정보를 캐시할 수 있도록 IP 서로게이트 기능을 활성화합니다.

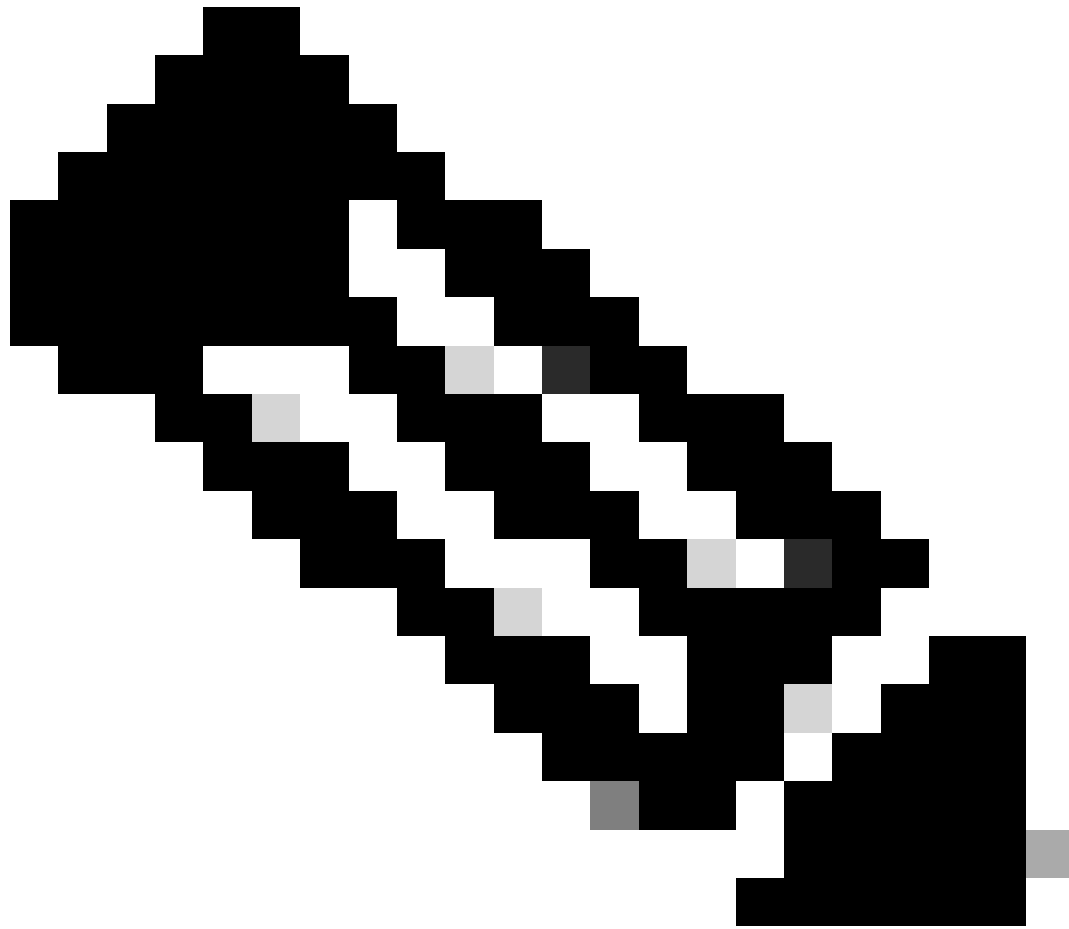
	대체: 네트워크 또는 터널 ID(사용자/그룹 아님)를 기반으로 웹 규칙에서 애플리케이션/도메인을 허용합니다.
HTTP 범위 요청	일부 애플리케이션은 데이터를 다운로드할 때 HTTP "Byte-Range" 요청을 사용합니다. 즉, 한 번에 파일의 작은 청크만 다운로드됩니다. 이러한 요청은 SWG에서 보안상의 이유로 비활성화됩니다. 이 기술을 사용하여 안티바이러스 탐지를 우회할 수도 있기 때문입니다. - 솔루션(HTTPS): 선택적 암호 해독 목록을 사용하여 Umbrella의 SSL 암호 해독*에서 애플리케이션 또는 도메인을 우회합니다. - 솔루션(HTTP): Override Security(보안 재정의) 옵션이 있는 웹 규칙을 사용하여 안티바이러스 검사에서 애플리케이션 또는 도메인 을 우회합니다. - 대체: 기사에 대해 Range(범위) 요청을 기본적으로 활성화하려면 Umbrella 지원에 문의하십시오*.
명시적 프록시 호환성	일부 응용 프로그램은 시스템 프록시 설정(예: PAC 파일) 및 는 일반적으로 명시적 웹 프록시와 호환되지 않습니다. 이러한 애플리케이션은 PAC 파일 구축에서 Umbrella SWG를 통해 라우팅되지 않습니다. 해결책: 로컬 네트워크 방화벽을 통해 애플리케이션을 허용해야 합니다. 허용할 대상/포트에 대한 자세한 내용은 애플리케이션 공급업체에 문의하십시오.



경고: 이러한 예외를 생성하면 안티바이러스 검사, DLP 검사, 테넌트 제어, 파일 유형 제어 및 URL 검사를 비롯한 보안 검사 기능을 비활성화할 수 있습니다. 이 파일의 소스를 신뢰할 수 있는 경우에만 이 작업을 수행합니다. 애플리케이션에 대한 비즈니스 요구는 이러한 기능을 비활성화할 때의 보안 영향과 비교해야 합니다.

Microsoft 365 애플리케이션

Microsoft 365 호환성 기능은 SSL 암호 해독 및 정책 시행 기능에서 여러 Microsoft 도메인을 자동으로 제외합니다. 이 기능을 활성화하여 Microsoft 앱의 데스크톱 버전 문제를 해결할 수 있습니다. 자세한 내용은 전역 설정 [관리를 참조하십시오](#).



참고: Microsoft 365 호환성 기능에서 모든 Microsoft 도메인을 제외하는 것은 아닙니다. Umbrella는 필터링에서 제외해야 하는 도메인 목록에 대해 Microsoft의 권장 사항을 사용합니다. 자세한 내용은 [새 Office365 끝점 범주를 참조하십시오](#).

인증서 피닝 바이패스

PKP(Certificate Pinning)는 앱 호환성 문제의 일반적인 원인입니다. Cisco는 SSL 암호 해독을 우회하여 문제를 해결하도록 구성할 수 있는 명명된 애플리케이션의 포괄적인 목록을 제공합니다. 선택적 해독은 Policies(정책) > Selective Decryption Lists(선택적 해독 목록)에서 구성할 수 있습니다.

대부분의 경우 관리자는 이름별로 애플리케이션을 제외하는 것만으로 인증서 피닝 문제를 해결할 수 있습니다. 이는 도메인 목록을 학습하거나 유지 관리할 필요 없이 이러한 문제를 해결할 수 있음을 의미합니다.

Application Testing

Applied To
Web Policy

Categories

Applications
1

Domains
0

Nov 24, 2022

^

List Name

Application Testing

0 Categories Selected

ADD

No Categories Selected

1 Applications Selected

ADD

Dropbox

0 Domains

ADD

No Domains

DELETE

CANCEL

SAVE

또는 대상 도메인/IP 주소를 기반으로 애플리케이션을 우회할 수 있습니다. 적용 가능한 도메인/IP 목록을 확인하려면 애플리케이션 공급업체에 문의하거나 인증서 피닝에 대한 제외 항목 식별을 참조하십시오.

TLS 호환성 우회

레거시 또는 사용자 지정 TLS 버전은 앱 호환성 문제의 일반적인 원인입니다. 이러한 문제는 Deployments(구축) > Domain Management(도메인 관리) > External Domains & IPs(외부 도메인 및 IPs)에서 Umbrella에서 트래픽을 제외하여 해결할 수 있습니다. 터널 구축에서는 VPN 구성에 예외를 추가하여 트래픽을 제외할 수 있습니다.

Add New Bypass Domain or Server

When you add a domain, all of its subdomains will inherit the setting. If 'example.com' is on the internal domains list, 'www.example.com' will also be treated as an internal domain.

Domain Type

☐ Internal Domains ☒ External Domains & IPs

Entity

whatsapp.net

Description

Applies To

Domain: Hosted PAC, AnyConnect, SWG Umbrella Chromebook Client

IP: AnyConnect, SWG Umbrella Chromebook Client

CANCEL

SAVE

제외할 도메인/IP의 적용 가능한 목록을 확인하려면 애플리케이션 공급업체에 문의하거나 "Identify Exclusions for Uncompatible TLS Versions(호환되지 않는 TLS 버전에 대한 제외 식별)"(이 문서의 뒷부분 참조)를 참조하십시오.

문제 해결(고급)

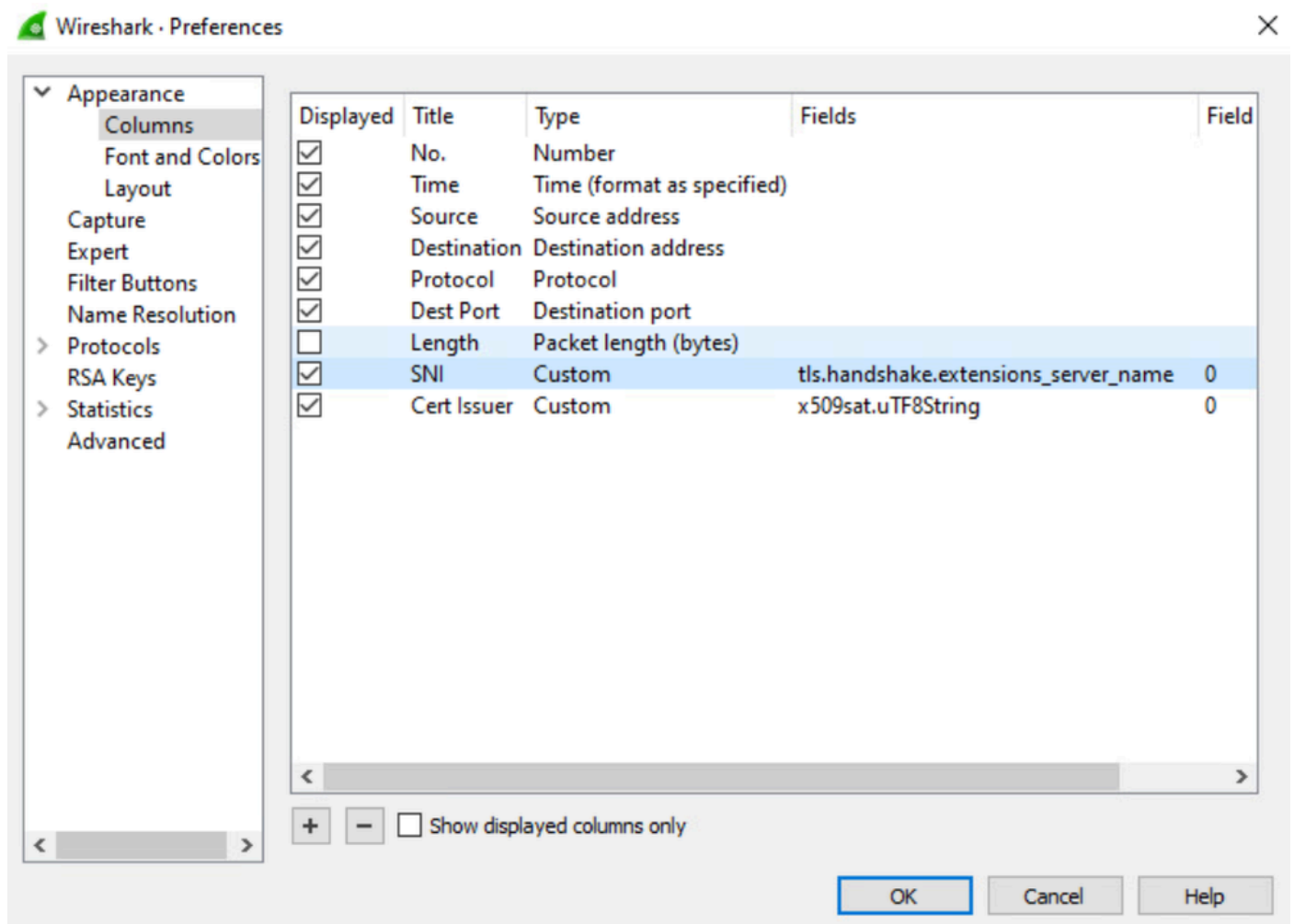
이 문서의 나머지 지침은 문제 해결을 위해 Wireshark(www.wireshark.org) 패킷 캡처를 사용합니다. Wireshark는 사용자 지정 제외 구현 지원을 위해 애플리케이션에서 사용하는 도메인을 식별하는데 도움이 될 수 있습니다. 시작하기 전에 Wireshark에서 다음 사용자 지정 열을 추가하십시오.

1. www.wireshark.org에서 Wireshark를 [다운로드합니다](#).

2. 편집 > 환경설정 > 열로 이동합니다.

3. 다음 필드로 사용자 정의 유형의 열을 생성합니다.

http.host
tls.handshake.extensions_server_name
x509sat.uTF8String



패킷 캡처를 수행하려면 다음 지침을 완료하거나 Wireshark로 네트워크 트래픽 캡처를 참조하십시오.

1. Wireshark를 관리자로 실행합니다.

2. [캡처] > [옵션]에서 관련 네트워크 인터페이스를 선택합니다.

- PAC/터널 구축의 경우 일반 LAN 네트워크 인터페이스에서 캡처합니다.
- AnyConnect 구축의 경우 LAN 네트워크 인터페이스 및 루프백 인터페이스에서 캡처합니다.

3. 문제 응용 프로그램을 제외한 다른 응용 프로그램을 모두 닫습니다.

4. DNS 캐시를 플러시합니다. ipconfig /flushdns

5. Wireshark 캡처 시작

6. 문제를 신속하게 복제하고 Wireshark 캡처를 중지합니다.

인증서 피닝에 대한 제외 항목 식별

인증서 피닝은 클라이언트에 적용되므로, 모든 애플리케이션에 대해 정확한 동작 및 해결 단계가 다릅니다. 캡처 출력에서 TLS 연결이 실패하고 있음을 알리는 신호를 찾습니다.

- TLS 연결이 빠르게 닫히거나 재설정되는 중입니다(RST 또는 FIN).
- TLS 연결을 반복적으로 재시도하는 중입니다.
- TLS 연결에 대한 인증서가 Cisco Umbrella에서 발급되고 있으므로 해독되고 있습니다.

이 예의 Wireshark 필터는 TLS 연결의 중요한 세부 정보를 확인하는 데 도움이 됩니다.

터널/AnyConnect

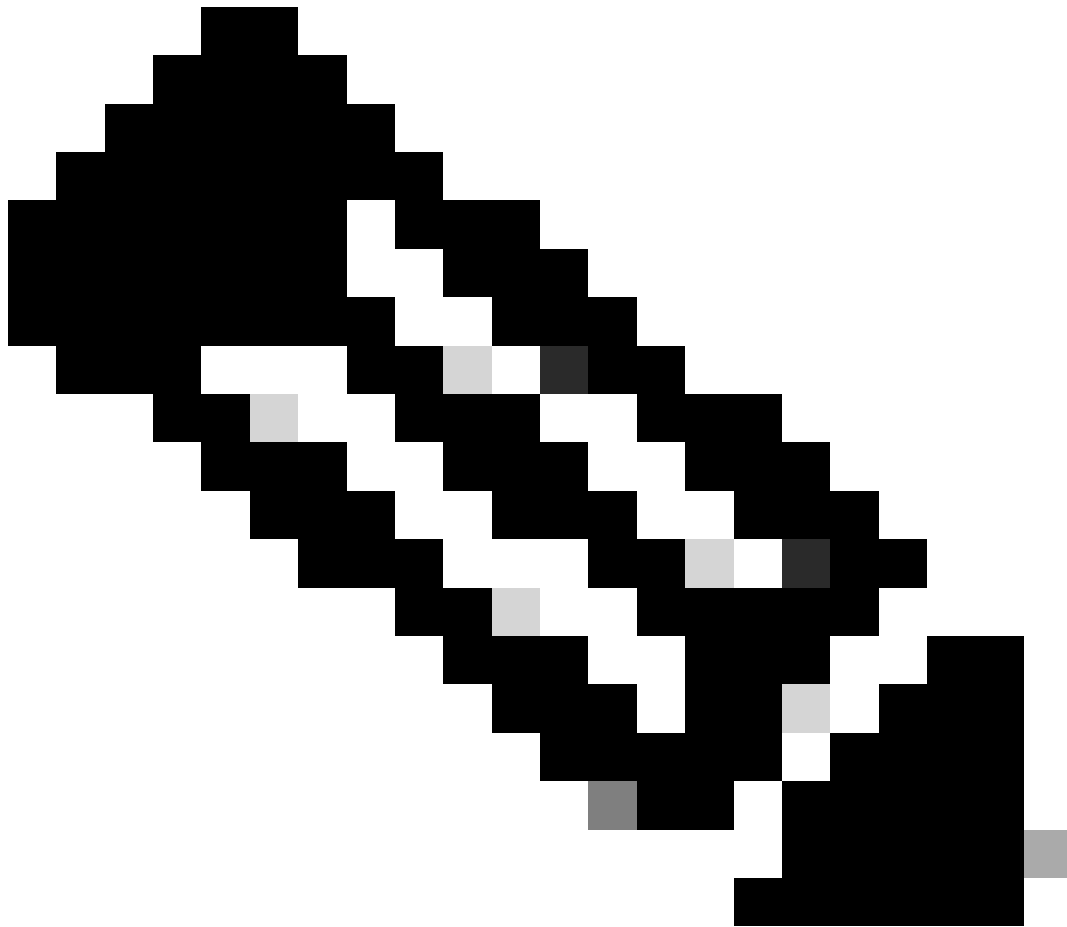
```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.reset eq 1 || tcp.flags.fin eq 1)
```

PAC/프록시 연결

```
tcp.port eq 443 && (http.request.method eq CONNECT || tcp.flags.reset eq 1)
```

이 예에서 DropBox 데스크톱 애플리케이션은 client.dropbox.com에 연결하려고 시도할 때 인증서 피닝의 영향을 받습니다.

(tls.handshake.extensions_server_name tls.handshake.certificate tcp.flags.reset eq 1 tcp.flags.fin eq 1)							
No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
281	43.038669	10.10.199.101	162.125.6.13	TCP	443		65148 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261120 Len=0
283	43.073849	162.125.6.13	10.10.199.101	TCP	65148	Server Name	443 → 65148 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
287	43.083933	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
292	43.141656	162.125.6.13	10.10.199.101	TLSv1.2	65149		Certificate, Server Key Exchange, Server Hello Done
296	43.175867	10.10.199.101	162.125.6.13	TCP	443		65149 → 443 [FIN, ACK] Seq=3804 Ack=474 Win=261888 Len=0
297	43.211415	162.125.6.13	10.10.199.101	TCP	65149		443 → 65149 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
306	46.361407	13.107.21.200	10.10.199.101	TCP	65123		443 → 65123 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0
309	46.458616	13.107.21.200	10.10.199.101	TCP	65125	Retries	443 → 65125 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0
315	48.228572	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
320	48.272897	162.125.6.13	10.10.199.101	TLSv1.2	65151		Certificate, Server Key Exchange, Server Hello Done
324	48.315138	10.10.199.101	162.125.6.13	TCP	443		65151 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
326	48.346412	162.125.6.13	10.10.199.101	TCP	65151		443 → 65151 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
330	48.357435	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
335	48.408976	162.125.6.13	10.10.199.101	TLSv1.2	65152		Certificate, Server Key Exchange, Server Hello Done
339	48.449204	10.10.199.101	162.125.6.13	TCP	443		65152 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
341	48.483947	162.125.6.13	10.10.199.101	TCP	65152		443 → 65152 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
345	48.514224	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
350	48.555627	162.125.6.13	10.10.199.101	TLSv1.2	65153		Certificate, Server Key Exchange, Server Hello Done
354	48.595411	10.10.199.101	162.125.6.13	TCP	443		65153 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261888 Len=0
356	48.631537	162.125.6.13	10.10.199.101	TCP	65153		443 → 65153 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
360	48.641737	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
365	48.685384	162.125.6.13	10.10.199.101	TLSv1.2	65154		Certificate, Server Key Exchange, Server Hello Done
369	48.742518	10.10.199.101	162.125.6.13	TCP	443		65154 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
370	48.779104	162.125.6.13	10.10.199.101	TCP	65154		443 → 65154 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
375	50.854534	10.10.199.101	172.217.15.110	TCP	443		64903 → 443 [FIN, ACK] Seq=2 Ack=74 Win=1020 Len=0
376	50.888092	172.217.15.110	10.10.199.101	TCP	64903		443 → 64903 [FIN, ACK] Seq=74 Ack=3 Win=83 Len=0
381	53.801686	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
387	53.845602	162.125.6.13	10.10.199.101	TLSv1.2	65156		Certificate, Server Key Exchange, Server Hello Done
390	53.888995	10.10.199.101	162.125.6.13	TCP	443		65156 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261120 Len=0
392	53.919018	162.125.6.13	10.10.199.101	TCP	65156		443 → 65156 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
396	53.929107	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
402	53.972689	162.125.6.13	10.10.199.101	TLSv1.2	65157		Certificate, Server Key Exchange, Server Hello Done
405	54.011019	10.10.199.101	162.125.6.13	TCP	443		65157 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261120 Len=0
406	54.047260	162.125.6.13	10.10.199.101	TCP	65157		443 → 65157 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0



참고: 필요한 제외를 추가한 후 이 단계를 여러 번 반복하여 애플리케이션에서 사용하는 모든 대상을 식별할 수 있습니다.

호환되지 않는 TLS 버전에 대한 제외 항목 식별

Umbrella SWG에서 지원하는 필수 TLS1.2+ 프로토콜을 사용하지 않는 SSL/TLS 연결을 확인합니다. 여기에는 레거시 프로토콜(TLS1.0 이하) 또는 애플리케이션에 의해 구현된 맞춤형 프로토콜이 포함될 수 있습니다.

이 예제 필터는 DNS 쿼리와 함께 초기 TLS 핸드셰이크 패킷을 보여줍니다.

터널/AnyConnect

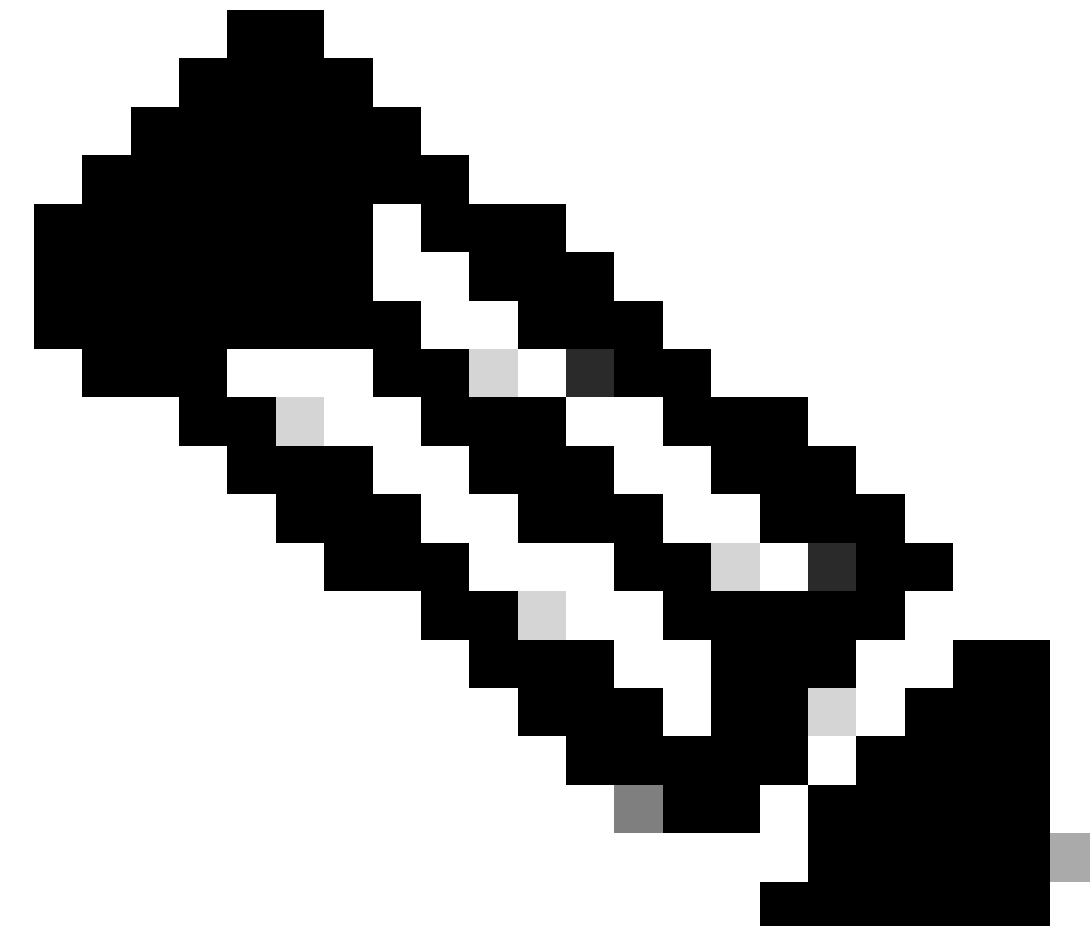
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

PAC/프록시 연결

```
dns || http.request.method eq CONNECT
```

이 예에서 Spotify 데스크톱 애플리케이션은 SWG를 통해 전송할 수 없는 비표준 또는 레거시 "SSL" 프로토콜을 사용하여 ap-gew4.spotify.com에 연결을 시도합니다.

dns (tls && tcp.seq eq 1 && tcp.ack eq 1)						
No.	Time	Source	Destination	Protocol	Dest Port	SNI
374	62.554832	10.10.199.101	10.10.199.254	DNS	53	
375	62.589486	10.10.199.254	10.10.199.101	DNS	Legacy "SSL" protocol	
379	62.631391	10.10.199.101	34.158.0.131	SSL	443	
				Info		
				Standard query 0x3070 A ap-gew4.spotify.com DNS Information		
				Standard query response 0x3070 A ap-gew4.spotify.com A 34.158.0.131		
				Continuation Data		



참고: 필요한 제외를 추가한 후 이 단계를 여러 번 반복하여 애플리케이션에서 사용하는 모든 대상을 식별할 수 있습니다.

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.