

# Fehlerbehebung bei Nicht-Browser-Anwendungen in Umbrella

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Kompatibilitätsprobleme](#)

[Microsoft 365-Anwendungen](#)

[Umgehung der Zertifikatsanheftung](#)

[TLS-Kompatibilitätsüberbrückung](#)

[Fehlerbehebung \(Erweitert\)](#)

[Identifizieren von Ausschlüssen für die Zertifikatsauslagerung](#)

[Identifizieren von Ausschlüssen für inkompatible TLS-Versionen](#)

---

## Einleitung

In diesem Dokument wird die Fehlerbehebung für nicht-browserbasierte Anwendungen in Cisco Umbrella beschrieben.

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Überblick

In diesem Artikel werden die Best Practices und die Schritte zur Fehlerbehebung erläutert, mit denen nicht-browserbasierte Anwendungen so konfiguriert werden können, dass sie mit Umbrella

Secure Web Gateway funktionieren. In den meisten Fällen sind keine Konfigurationsänderungen erforderlich. Bestimmte Anwendungen funktionieren jedoch nicht gut mit Sicherheits-/Prüffunktionen (z. B. SSL-Verschlüsselung), und es müssen Ausnahmen hinzugefügt werden, damit die Anwendung mit einem Webproxy funktioniert. Dies gilt für die Umbrella SWG sowie andere Web-Proxy-Lösungen.

Dies ist nützlich, wenn die Website-/Browserversion einer Anwendung funktioniert, die Desktop-/Mobilversion der Anwendung jedoch nicht.

## Kompatibilitätsprobleme

Anwendungen können aus folgenden Gründen inkompatibel sein:

<p>Installation der Umbrella Root CA</p>	<p>Die Cisco Umbrella Root CA muss für fehlerfreie TLS-Verbindungen immer vertrauenswürdig sein.</p> <ul style="list-style-type: none"> <li>• Lösung: Stellen Sie bei Nicht-Webanwendungen sicher, dass die <a href="#">Cisco Umbrella Root CA</a> im Zertifikatspeicher des Systems/lokalen Computers vertrauenswürdig ist.</li> </ul>
<p>Zertifikat-Pinning</p>	<p>Certificate Pinning (PKP) ist der Zeitpunkt, an dem die Anwendung erwartet, ein präzises Leaf (oder CA-Zertifikat) zur Validierung des TLS-Handshakes zu erhalten. Die Anwendung kann ein von einem Webproxy generiertes Zertifikat nicht akzeptieren und ist nicht mit SSL-Verschlüsselungsfunktionen kompatibel.</p> <ul style="list-style-type: none"> <li>• Lösung: Umgehen der Anwendung oder Domäne von der SSL-Entschlüsselung mithilfe einer <a href="#">selektiven Entschlüsselungsliste</a> (siehe Warnung nach Tabelle)</li> </ul> <p>Weitere Informationen zu Anwendungen, von denen bekannt ist, dass sie von der Zertifikatpinning betroffen sind, finden Sie hier: <a href="#">Pinning für öffentlichen Schlüssel/Zertifikatpinning</a></p>
<p>Unterstützung von TLS-Versionen</p>	<p>Die Anwendung kann eine ältere TLS Version / Cipher verwenden, die von SWG aus Sicherheitsgründen nicht unterstützt wird.</p> <ul style="list-style-type: none"> <li>• Lösung: Umgehen Sie den Datenverkehr, der nicht an Umbrella gesendet wird, mithilfe der Funktion für <a href="#">externe Domänen</a> (PAC/AnyConnect) oder VPN-Ausschlüsse (Tunnel) (siehe Warnung nach Tabelle).</li> </ul>
<p>Nicht-Webprotokoll</p>	<p>Einige Anwendungen verwenden Protokolle, die nicht HTTP(s) sind, senden diese Daten aber dennoch über gängige Web-Ports, die von der</p>

	<p>SWG abgefangen werden. Die SWG kann diesen Datenverkehr nicht verstehen.</p> <ul style="list-style-type: none"> <li>• Lösung: Wenden Sie sich an den Anwendungsanbieter, um die Zieladressen/IP-Bereiche zu ermitteln, die von der Software verwendet werden. Diese Software muss mithilfe von <a href="#">externen Domänen</a> (PAC/AnyConnect) oder VPN-Ausschlüssen (Tunnel) von der SWG ausgeschlossen werden (siehe Warnung nach Tabelle).</li> </ul>
SAML-Authentifizierung	<p>Die meisten Nicht-Browser-Anwendungen können keine SAML-Authentifizierung durchführen. Umbrella stellt keine nicht browserbasierten Anwendungen für SAML in Frage, daher können benutzer-/gruppenbasierte Filterrichtlinien nicht übereinstimmen.</p> <ul style="list-style-type: none"> <li>• Lösung: Aktivieren Sie die Funktion <a href="#">IP-Surrogate</a>, damit Benutzerinformationen für Nicht-Browser-Anwendungen zwischengespeichert werden können.</li> <li>• Alternativ: Lassen Sie die Anwendung/Domäne in einer <a href="#">Webregel</a> basierend auf Netzwerk- oder Tunnellidentitäten (nicht Benutzer/Gruppen) zu.</li> </ul>
HTTP-Bereichsanforderungen	<p>Einige Anwendungen verwenden HTTP-"<a href="#">Byte-Range</a>"-Anforderungen beim Herunterladen von Daten. Das bedeutet, dass nur ein kleiner Teil der Datei gleichzeitig heruntergeladen wird. Diese Anfragen werden aus Sicherheitsgründen in der SWG deaktiviert, da diese Technik auch verwendet werden kann, um die Anti-Virus-Erkennung zu umgehen.</p> <ul style="list-style-type: none"> <li>• Lösung (HTTPS): Umgehen der Anwendung oder Domäne von der SSL-Entschlüsselung* in Umbrella mit <a href="#">selektiven Entschlüsselungslisten</a>.</li> <li>• Lösung (HTTP): Umgehen der Anwendung oder Domäne vom Anti-Virus-Scanning* mithilfe einer Webregel mit der Option <a href="#">Sicherheit außer Kraft setzen</a>.</li> <li>• Alternativ: Wenden Sie sich an den Umbrella-Support, wenn für Ihre Organisation standardmäßig* Range-Anfragen aktiviert sein sollen.</li> </ul>
Explizite Proxy-Kompatibilität	<p>Einige Anwendungen respektieren die System-Proxy-Einstellungen nicht (z. B. PAC-Dateien) und sind im Allgemeinen nicht mit expliziten Webproxys kompatibel. Diese Anwendungen leiten Umbrella SWG in einer PAC-Dateibereitstellung nicht weiter.</p> <ul style="list-style-type: none"> <li>• Lösung: Die Anwendung muss über die lokale Netzwerk-Firewall zugelassen werden. Wenden Sie sich an den Anwendungsanbieter, um Details zu den zulässigen Zielen/Ports zu erhalten.</li> </ul>



Warnung: Durch das Erstellen dieser Ausnahmen können Sicherheitsüberprüfungsfunktionen wie Anti-Virus-Scanning, SvD-Scanning, Tenant-Steuer-elemente, Dateitypkontrolle und URL-Überprüfung deaktiviert werden. Führen Sie dies nur dann aus, wenn Sie der Quelle dieser Dateien vertrauen. Die geschäftlichen Anforderungen der Anwendung müssen mit den Auswirkungen abgewogen werden, die eine Deaktivierung dieser Funktionen auf die Sicherheit hat.

---

## Microsoft 365-Anwendungen

Die Microsoft 365-Kompatibilität-funktion schließt automatisch eine Reihe von Microsoft-Domänen von der SSL-Verschlüsselung und den Funktionen zur Richtliniendurchsetzung aus. Diese Funktion kann aktiviert werden, um Probleme mit der Desktop-Version von Microsoft-Anwendungen zu beheben. Weitere Informationen finden Sie unter [Globale Einstellungen verwalten](#).



Anmerkung: Die Microsoft 365-Kompatibilitätstfunktion schließt nicht alle Microsoft-Domänen aus. Umbrella verwendet die Empfehlungen von Microsoft für die Liste der Domänen, die von der Filterung ausgeschlossen werden müssen. Weitere Informationen finden Sie unter [Neue Office365-Endpunktkategorien](#).

---

## Umgehung der Zertifikatsanheftung

Die Zertifikatsanheftung (Certificate Pinning, PKP) ist eine häufige Ursache für Probleme mit der Anwendungskompatibilität. Cisco stellt eine umfassende Liste benannter Anwendungen bereit, die so konfiguriert werden können, dass die SSL-Verschlüsselung umgangen wird. Die selektive Entschlüsselung kann unter Richtlinien > Selektive Entschlüsselungslisten konfiguriert werden.

In den meisten Fällen kann der Administrator Probleme mit der Zertifikatsanheftung lösen, indem er die Anwendung einfach durch ihren Namen ausschließt. Das bedeutet, dass diese Probleme gelöst werden können, ohne dass eine Liste von Domänen gelernt oder gepflegt werden muss.

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 x

No Domains

0 Domains **ADD**

No Domains

**DELETE** **CANCEL** **SAVE**

Alternativ können Anwendungen basierend auf der Zieldomäne/IP-Adresse umgangen werden. Wenden Sie sich an den Anwendungsanbieter, um die entsprechende Liste der Domänen/IPs zu ermitteln, oder lesen Sie die Informationen unter Identify exclusions for certificate pinning (Ausschlüsse für Zertifikatpinning identifizieren).

## TLS-Kompatibilitätsüberbrückung

Ältere oder benutzerdefinierte TLS-Versionen sind eine häufige Ursache für Probleme mit der Anwendungskompatibilität. Diese Probleme können gelöst werden, indem der Datenverkehr aus Umbrella in Bereitstellungen > Domänenmanagement > Externe Domänen und IPs ausgeschlossen wird. In einer Tunnelbereitstellung kann der Datenverkehr nur durch Hinzufügen von Ausnahmen in der VPN-Konfiguration ausgeschlossen werden.

## 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

### Description

### Applies To

**Domain:** Hosted PAC, AnyConnect, SWG Umbrella Chromebook Client

**IP:** AnyConnect, SWG Umbrella Chromebook Client

CANCEL

SAVE

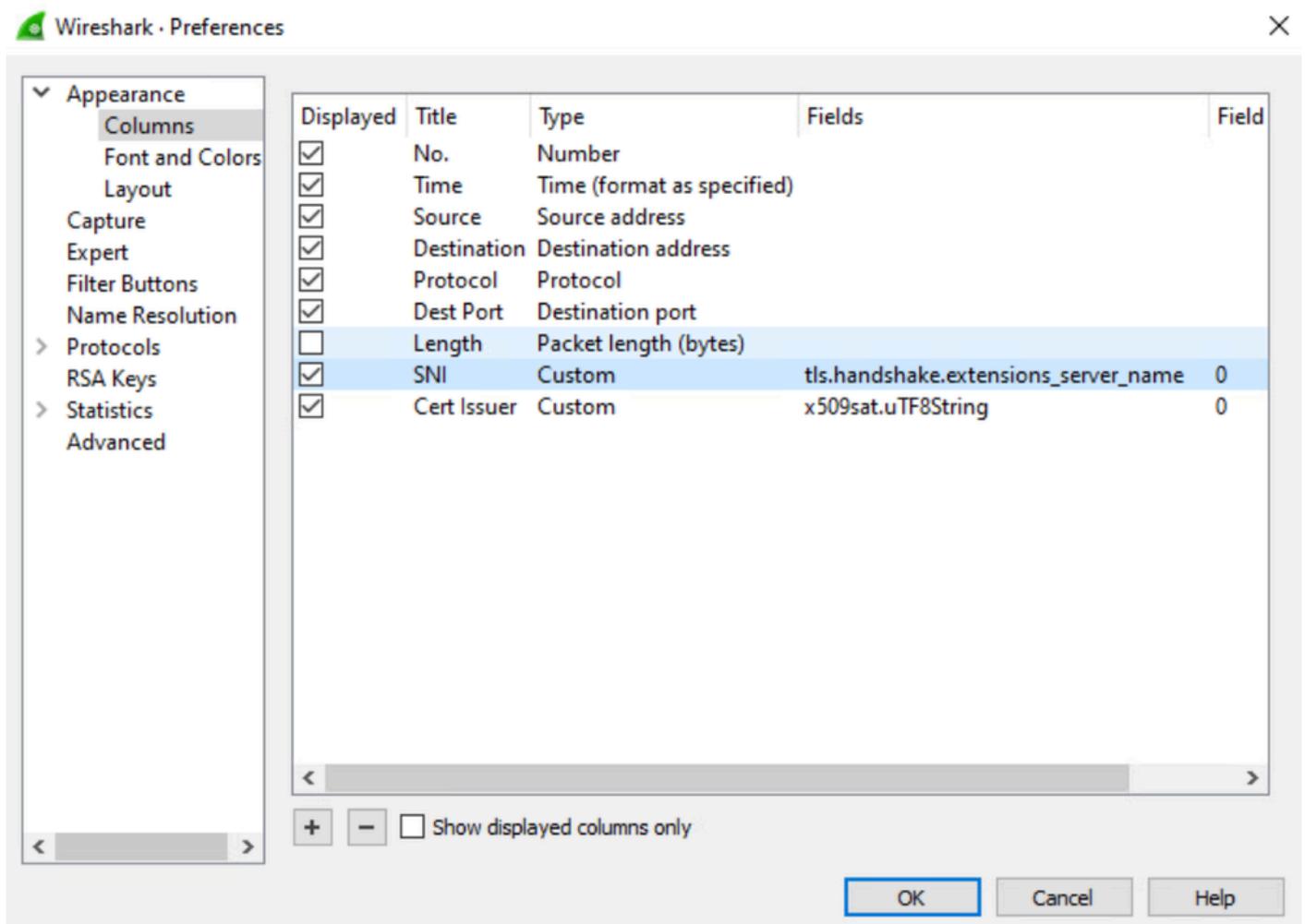
Wenden Sie sich an den Anwendungsanbieter, um die Liste der auszuschließenden Domänen/IP-Adressen zu ermitteln, oder lesen Sie "Identify Exclusions for Incompatible TLS Versions" (weiter unten in diesem Artikel).

## Fehlerbehebung (Erweitert)

Die verbleibenden Anweisungen in diesem Artikel verwenden Wireshark ([www.wireshark.org](http://www.wireshark.org))-Paketerfassungen für die Fehlerbehebung. Wireshark kann bei der Identifizierung von Domänen helfen, die von Anwendungen verwendet werden, um beim Implementieren benutzerdefinierter Ausschlüsse zu helfen. Fügen Sie vor dem Start die folgenden benutzerdefinierten Spalten in Wireshark hinzu:

1. Laden Sie Wireshark von [www.wireshark.org](http://www.wireshark.org) herunter.
2. Gehen Sie zu Bearbeiten > Voreinstellungen > Spalten.
3. Erstellen Sie Spalten vom Typ Benutzerdefiniert mit folgenden Feldern:

http.host  
 tls.handshake.extensions\_server\_name  
 x509sat.uTF8String



Um eine Paketerfassung durchzuführen, befolgen Sie diese Anweisungen, oder lesen Sie Capture Network Traffic with Wireshark.

1. Führen Sie Wireshark als Administrator aus.
2. Wählen Sie unter Capture > Options (Erfassung > Optionen) die entsprechenden Netzwerkschnittstellen aus.
  - Bei PAC/Tunnel-Bereitstellungen Erfassung auf Ihrer normalen LAN-Netzwerkschnittstelle.
  - Erfassen Sie bei AnyConnect-Bereitstellungen die Daten auf Ihrer LAN-Netzwerkschnittstelle und der Loopback-Schnittstelle.

3. Schließen Sie alle anderen Anwendungen mit Ausnahme der Problemanwendung.
4. DNS-Cache leeren: `ipconfig/flushdns`
5. Starten Sie die Erfassung von Wireshark.
6. Replizieren Sie das Problem schnell, und stoppen Sie die Erfassung von Wireshark.

## Identifizieren von Ausschlüssen für die Zertifikatauslagerung

Die Zertifikatpinning wird auf dem Client erzwungen, d. h., das genaue Verhalten und die Auflösungsschritte unterscheiden sich für jede Anwendung. Suchen Sie in der Erfassungsausgabe nach Anzeichen für den Ausfall einer TLS-Verbindung:

- Eine TLS-Verbindung wird schnell geschlossen oder zurückgesetzt (RST oder FIN).
- Eine TLS-Verbindung wird wiederholt versucht.
- Das Zertifikat für die TLS-Verbindung wird von Cisco Umbrella ausgestellt und daher entschlüsselt.

Diese Wireshark-Filter können dabei helfen, die wichtigen Details der TLS-Verbindungen anzuzeigen.

### Tunnel/AnyConnect

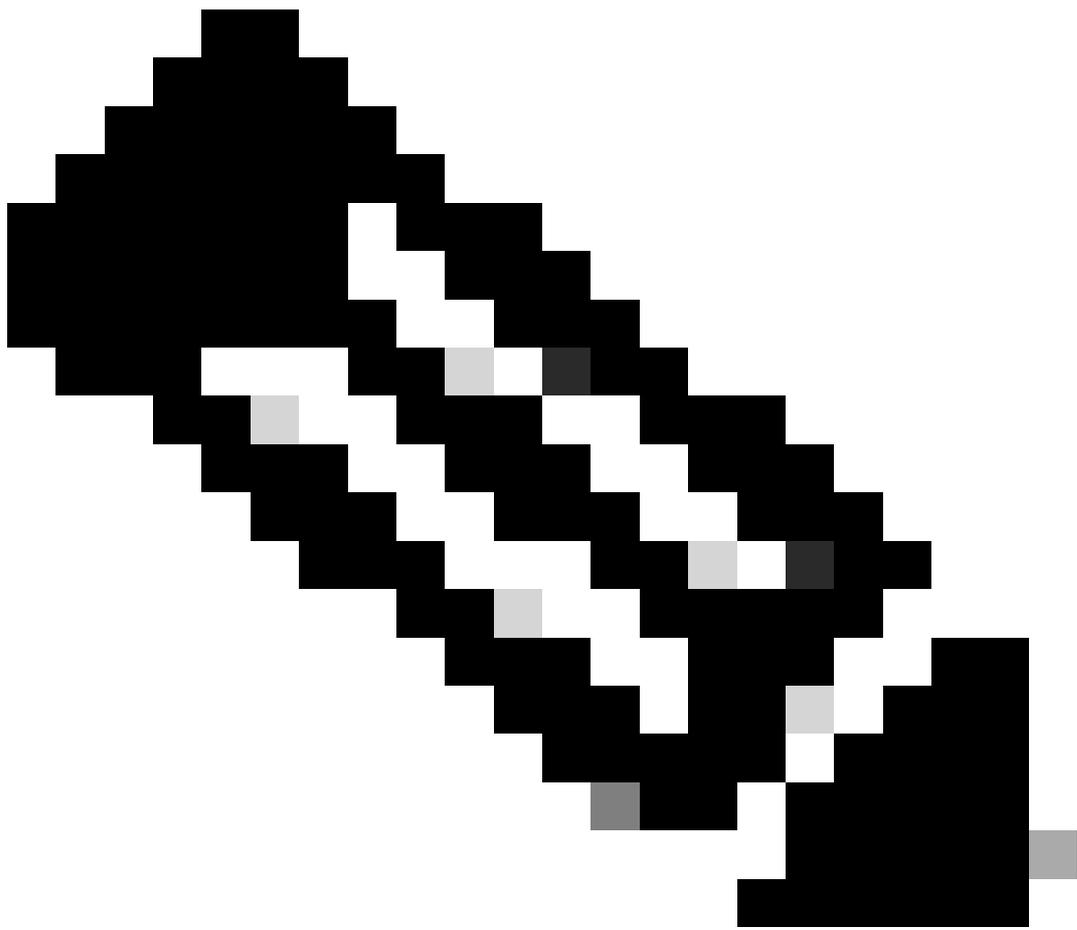
```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.reset)
```

### PAC/Proxy-Verkettung

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

In diesem Beispiel wird die DropBox-Desktopanwendung durch das Zertifikat-Pinning beeinflusst, wenn versucht wird, eine Verbindung mit `client.dropbox.com` herzustellen.

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



Anmerkung: Nachdem Sie die erforderlichen Ausschlüsse hinzugefügt haben, können Sie

diese Schritte mehrmals wiederholen, um alle von der Anwendung verwendeten Ziele zu identifizieren.

## Identifizieren von Ausschlüssen für inkompatible TLS-Versionen

Suchen Sie nach SSL/TLS-Verbindungen, die nicht die obligatorischen TLS1.2+-Protokolle verwenden, die von Umbrella SWG unterstützt werden. Dies kann Legacy-Protokolle (TLS1.0 oder frühere Versionen) oder benutzerdefinierte, von einer Anwendung implementierte Protokolle umfassen.

Dieser Beispielfilter zeigt die ersten TLS-Handshake-Pakete zusammen mit DNS-Abfragen.

Tunnel/AnyConnect

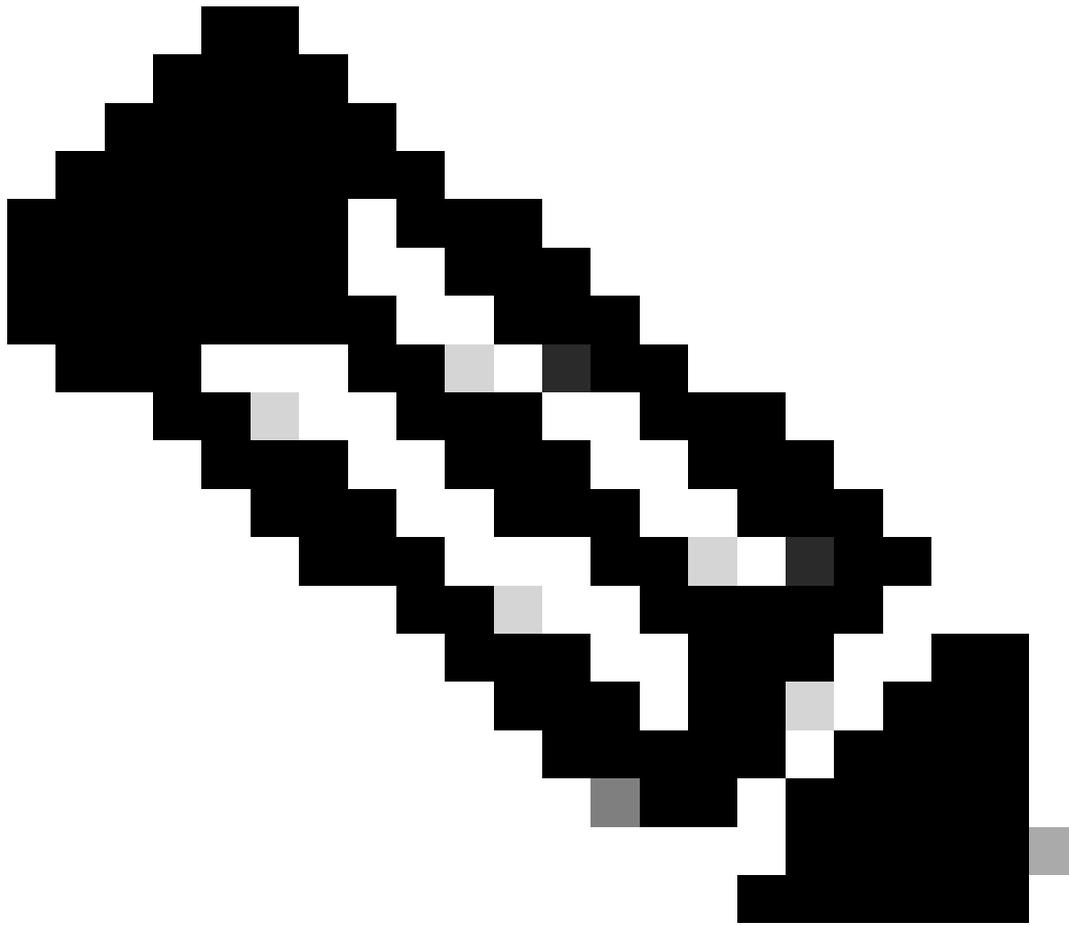
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

PAC/Proxy-Verkettung

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

In diesem Beispiel versucht die Spotify-Desktopanwendung, eine Verbindung zu ap-gew4.spotify.com mithilfe eines nicht standardmäßigen oder älteren "SSL"-Protokolls herzustellen, das nicht über SWG gesendet werden kann.

No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
374	62.554832	10.10.199.101	10.10.199.254	DNS	53		Standard query 0x3070 A ap-gew4.spotify.com <b>DNS Information</b>
375	62.589486	10.10.199.254	10.10.199.101	DNS		<b>Legacy "SSL" protocol</b>	Standard query response 0x3070 A ap-gew4.spotify.com A 34.158.0.13
379	62.631391	10.10.199.101	34.158.0.131	SSL	443		Continuation Data



Anmerkung: Nachdem Sie die erforderlichen Ausschlüsse hinzugefügt haben, können Sie diese Schritte mehrmals wiederholen, um alle von der Anwendung verwendeten Ziele zu identifizieren.

---

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.