Fehlerbehebung bei Nicht-Browser-Anwendungen in Umbrella

Inhalt

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.

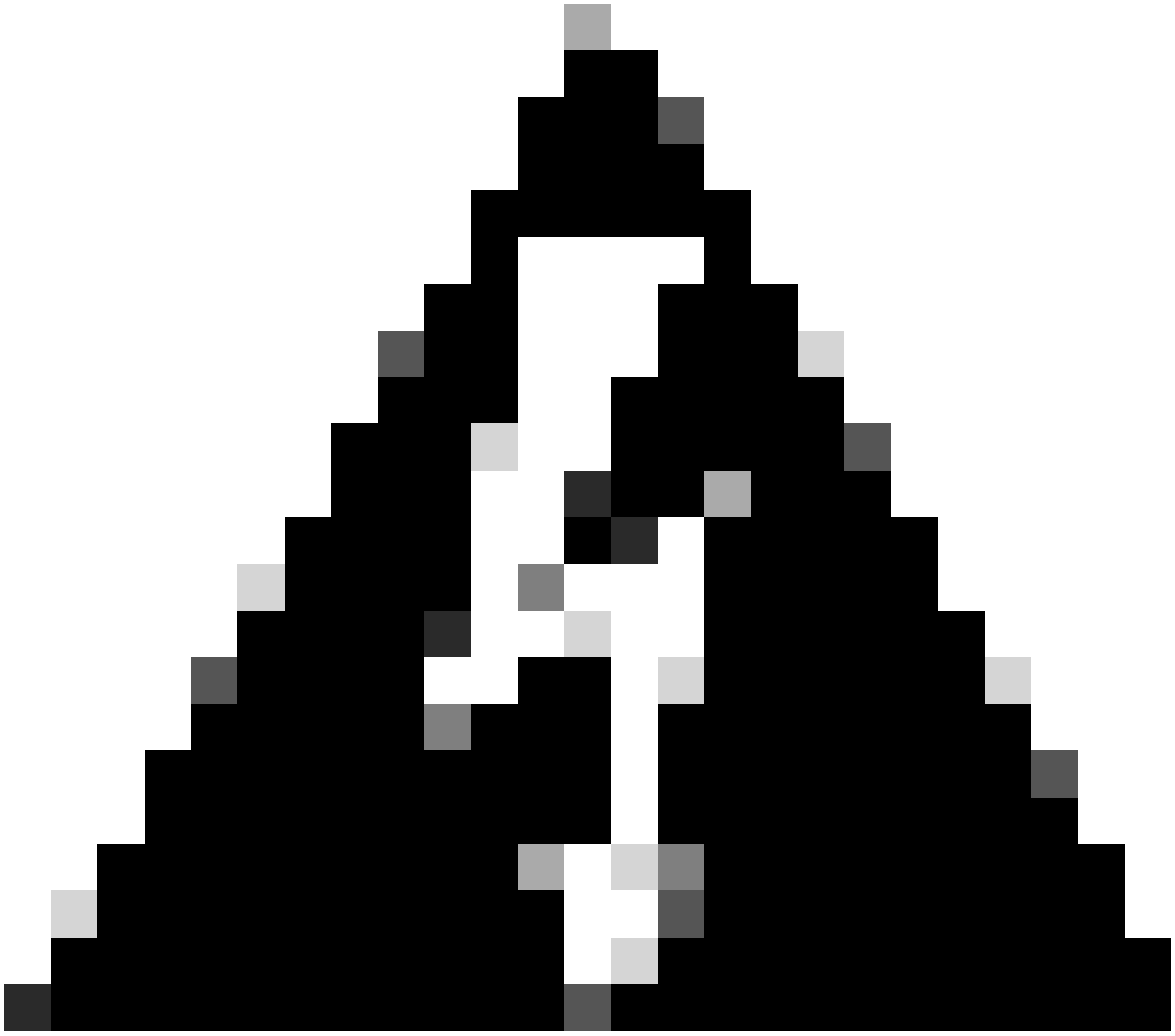
Dies ist nützlich, wenn die Website-/Browserversion einer Anwendung funktioniert, die Desktop-/Mobilversion der Anwendung jedoch nicht.

Kompatibilitätsprobleme

Anwendungen können aus folgenden Gründen inkompatibel sein:

Installation der Umbrella Root CA	Die Cisco Umbrella Root CA muss für fehlerfreie TLS-Verbindungen immer vertrauenswürdig sein. • Lösung: Stellen Sie bei Nicht-Webanwendungen sicher, dass die Cisco Umbrella Root CA im Zertifikatspeicher des Systems/lokalen Computers vertrauenswürdig ist.
Zertifikat-Pinning	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. • Lösung: Umgehen der Anwendung oder Domäne von der SSL-Entschlüsselung mithilfe einer selektiven Entschlüsselungsliste (siehe Warnung nach Tabelle) Weitere Informationen zu Anwendungen, von denen bekannt ist, dass sie von der Zertifikatpinning betroffen sind, finden Sie hier: Pinning für öffentlichen Schlüssel/Zertifikatpinning
Unterstützung von TLS-Versionen	Die Anwendung kann eine ältere TLS Version / Cipher verwenden, die von SWG aus Sicherheitsgründen nicht unterstützt wird. • Lösung: Umgehen Sie den Datenverkehr, der nicht an Umbrella gesendet wird, mithilfe der Funktion für externe Domänen (PAC/AnyConnect) oder VPN-Ausschlüsse (Tunnel) (siehe Warnung nach Tabelle).
Nicht-Webprotokoll	Einige Anwendungen verwenden Protokolle, die nicht HTTP(s) sind, senden diese Daten aber dennoch über gängige Web-Ports, die von der

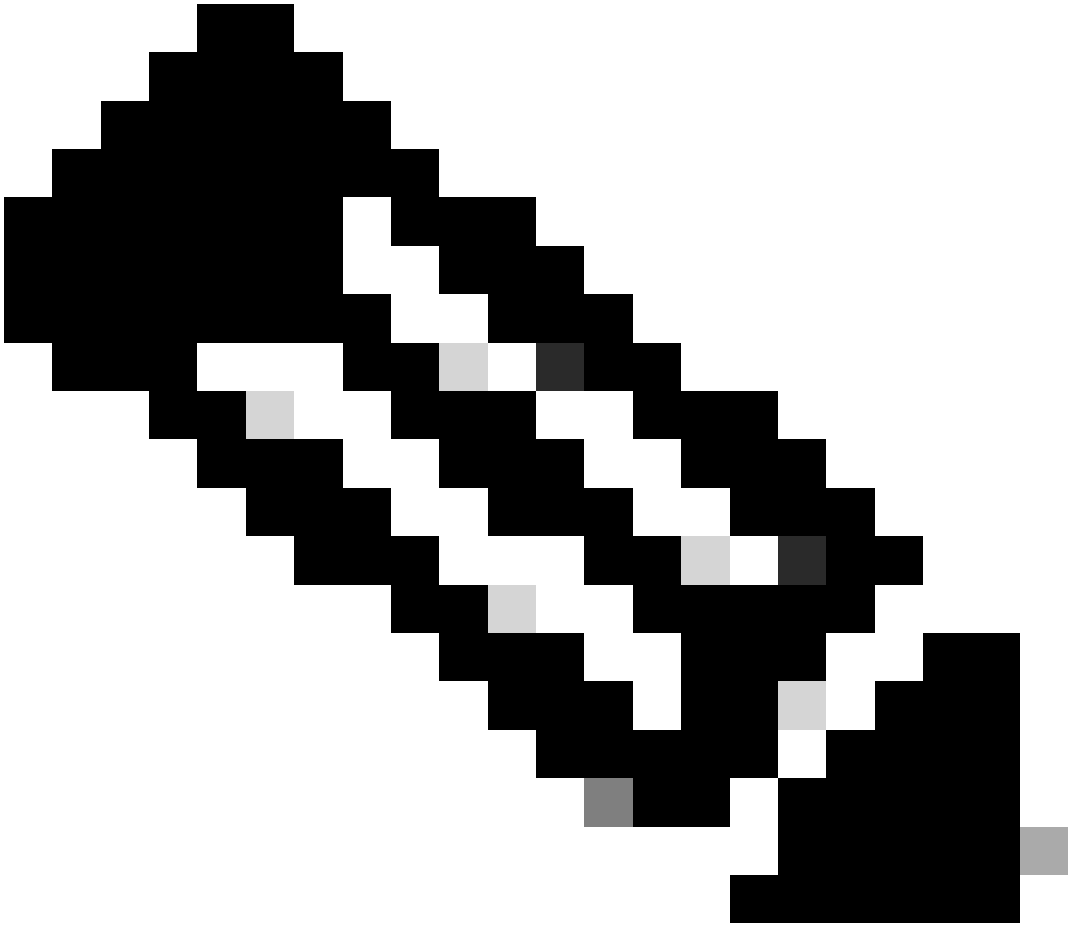
	SWG abgefangen werden. Die SWG kann diesen Datenverkehr nicht verstehen. • Lösung: Wenden Sie sich an den Anwendungsanbieter, um die Zieladressen/IP-Bereiche zu ermitteln, die von der Software verwendet werden. Diese Software muss mithilfe von externen Domänen (PAC/AnyConnect) oder VPN-Ausschlüssen (Tunnel) von der SWG ausgeschlossen werden (siehe Warnung nach Tabelle).
SAML-Authentifizierung	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. • Lösung: Aktivieren Sie die Funktion IP-Surrogate, damit Benutzerinformationen für Nicht-Browser-Anwendungen zwischengespeichert werden können. • Alternativ: Lassen Sie die Anwendung/Domäne in einer Webregel basierend auf Netzwerk- oder Tunnellidentitäten (nicht Benutzer/Gruppen) zu.
HTTP-Bereichsanforderungen	Einige Anwendungen verwenden HTTP-"Byte-Range"-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. • Lösung (HTTPS): Umgehen der Anwendung oder Domäne von der SSL-Entschlüsselung* in Umbrella mit selektiven Entschlüsselungslisten. • Lösung (HTTP): Umgehen der Anwendung oder Domäne vom Anti-Virus-Scanning* mithilfe einer Webregel mit der Option Sicherheit außer Kraft setzen. • Alternativ: Wenden Sie sich an den Umbrella-Support, wenn für Ihre Organisation standardmäßig* Range-Anfragen aktiviert sein sollen.
Explizite Proxy-Kompatibilität	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. • 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.



Warnung: Durch das Erstellen dieser Ausnahmen können Sicherheitsüberprüfungsfunktionen wie Anti-Virus-Scanning, SvD-Scanning, Tenant-Steuerelemente, 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-Kompatibilitätsfunktion 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.

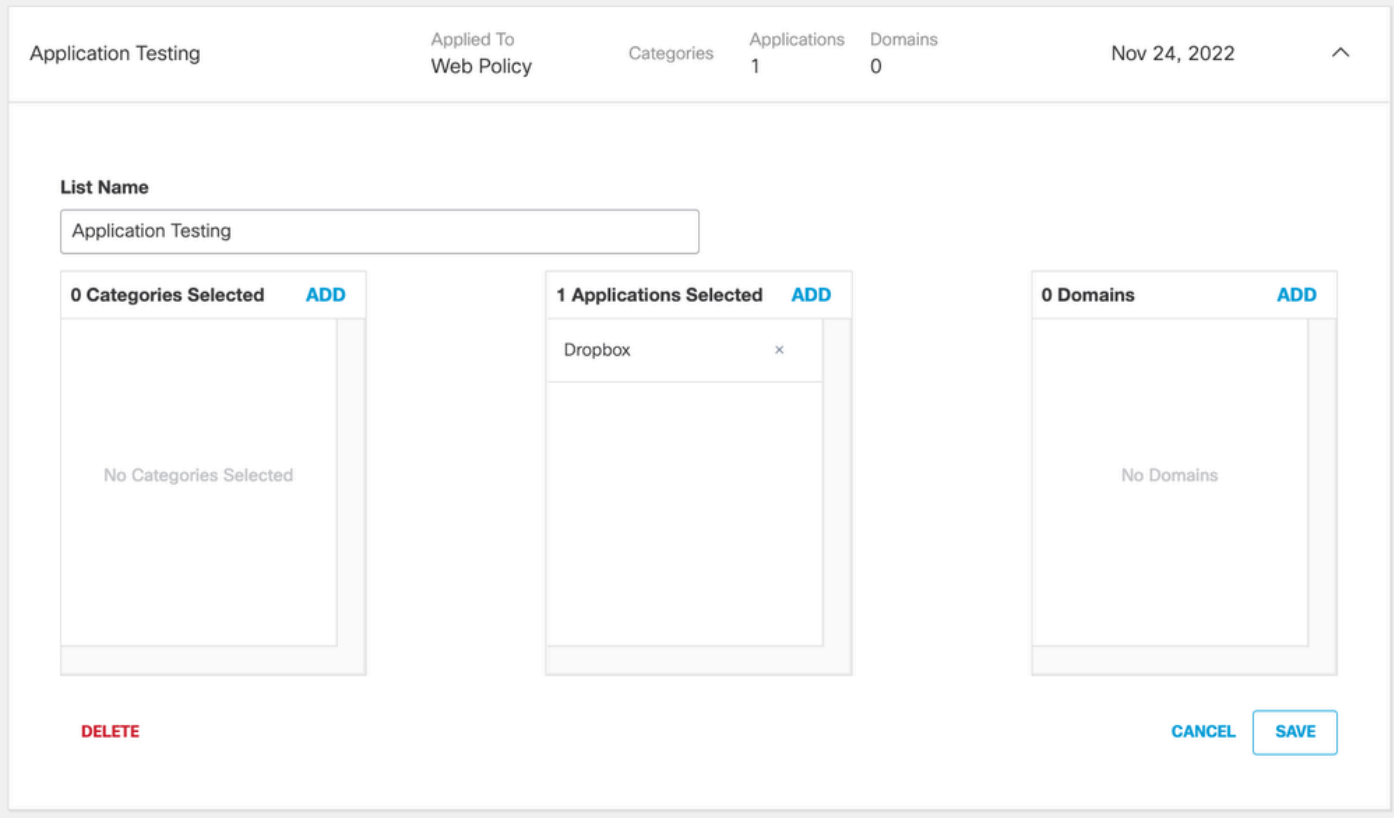


Anmerkung: Die Microsoft 365-Kompatibilitätsfunktion schließt nicht alle Microsoft-Domänen aus. Umbrella verwendet die Empfehlungen von Microsoft für die Liste der Domänen, die von der Filterung ausgeschlossen werden müssen. Weitere Informationen finden Sie unter Neue Office365-Endpunktkategorien.

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.

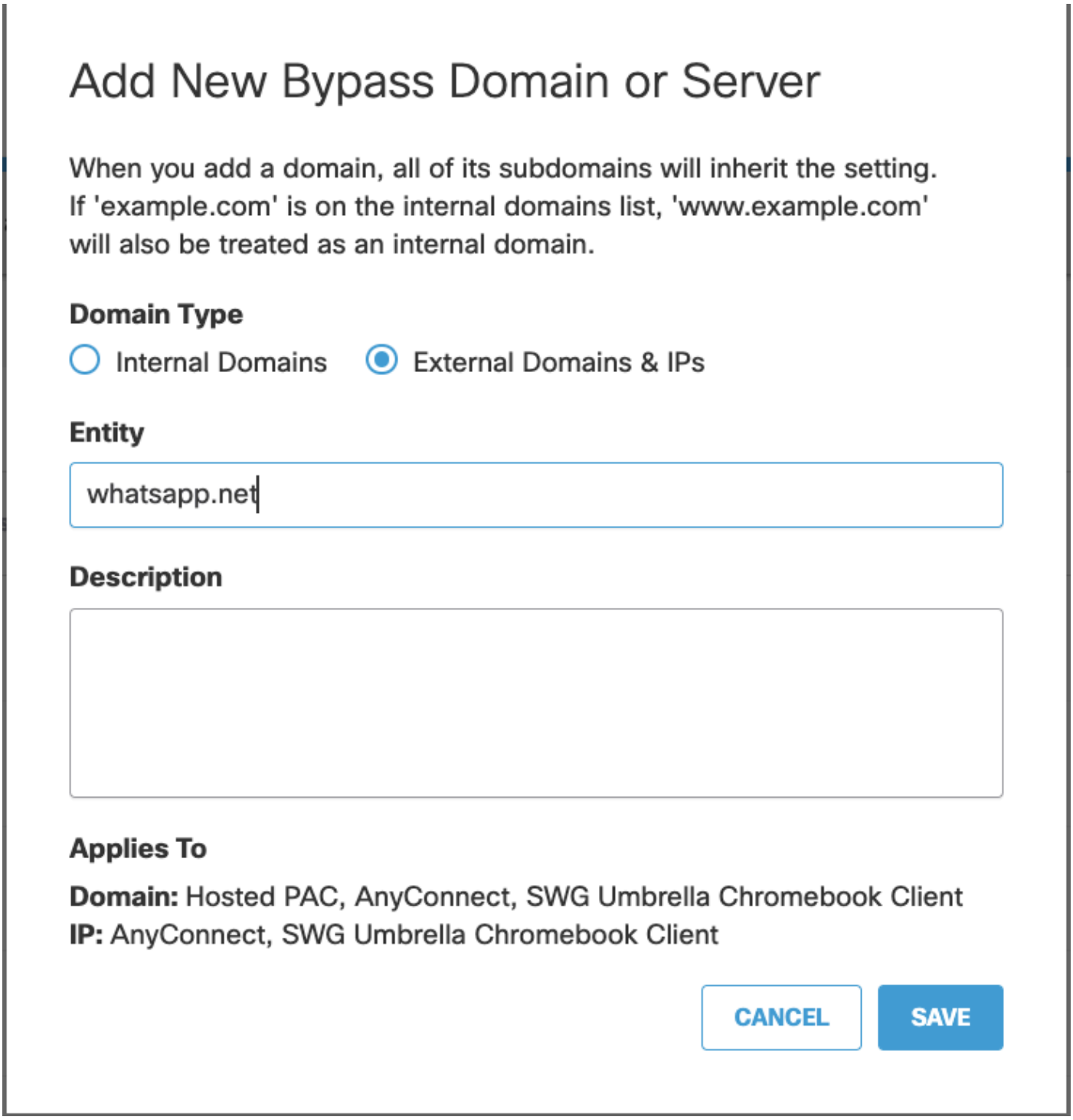
In den meisten Fällen kann der Administrator Probleme mit der Zertifikatsanheftung lösen, indem er die Anwendung einfach durch ihren Namen ausschließt. Das bedeutet, dass diese Probleme gelöst werden können, ohne dass eine Liste von Domänen gelernt oder gepflegt werden muss.



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.



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)

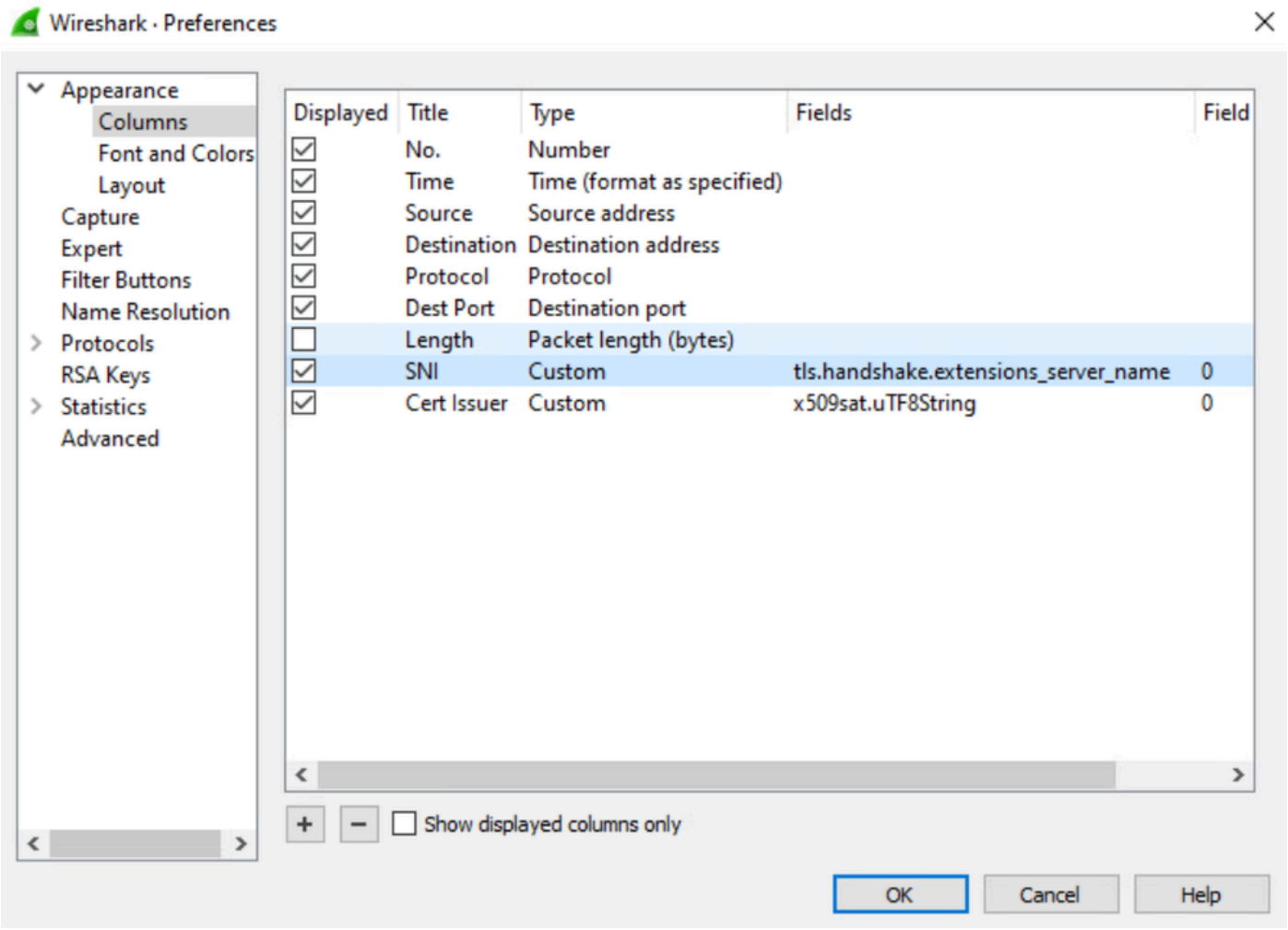
Die verbleibenden Anweisungen in diesem Artikel verwenden Wireshark (www.wireshark.org)-Paketerfassungen für die Fehlerbehebung. Wireshark kann bei der Identifizierung von Domänen helfen, die von Anwendungen verwendet werden, um beim Implementieren benutzerdefinierter Ausschlüsse zu helfen. Fügen Sie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

1. Laden Sie Wireshark von [www.wireshark.org herunter.](http://www.wireshark.org)

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.

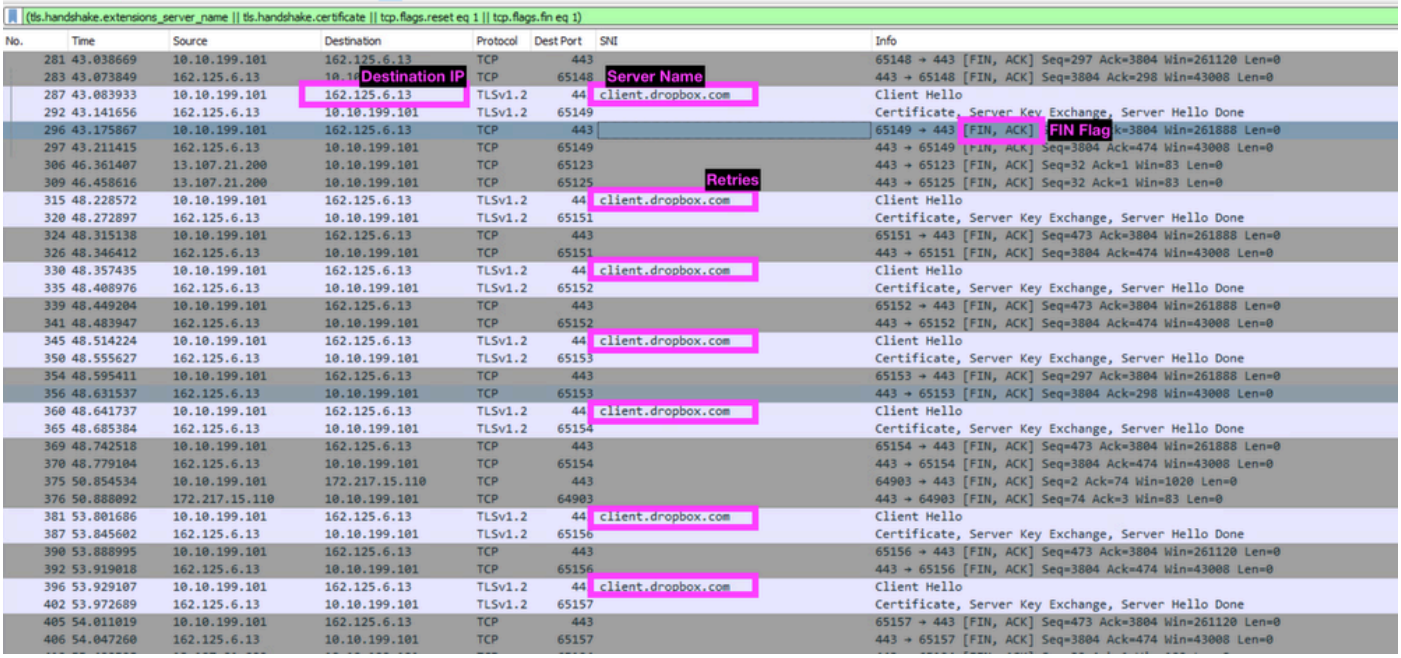
Tunnel/AnyConnect

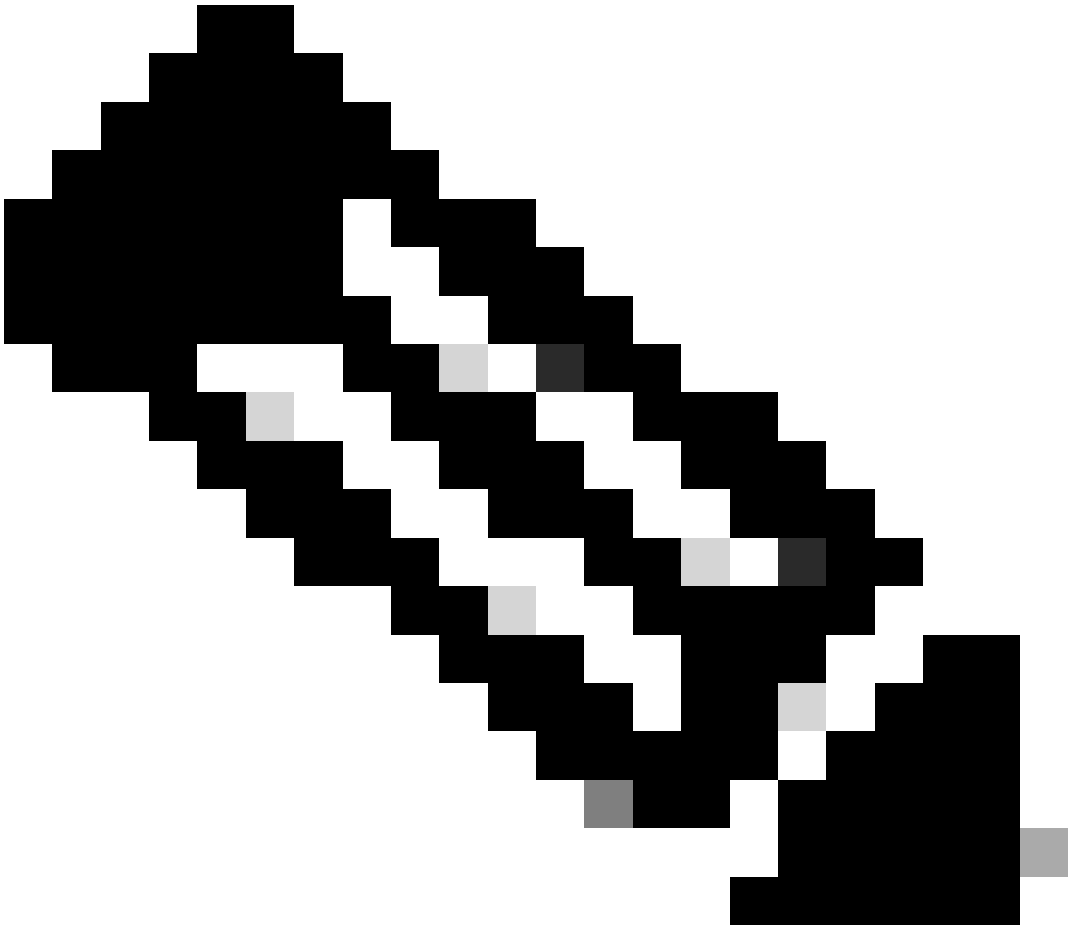
```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.rese
```

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.





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.

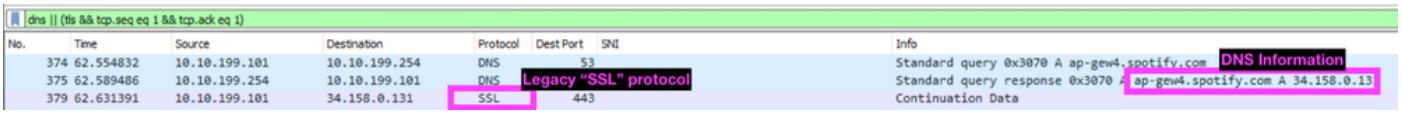
Tunnel/AnyConnect

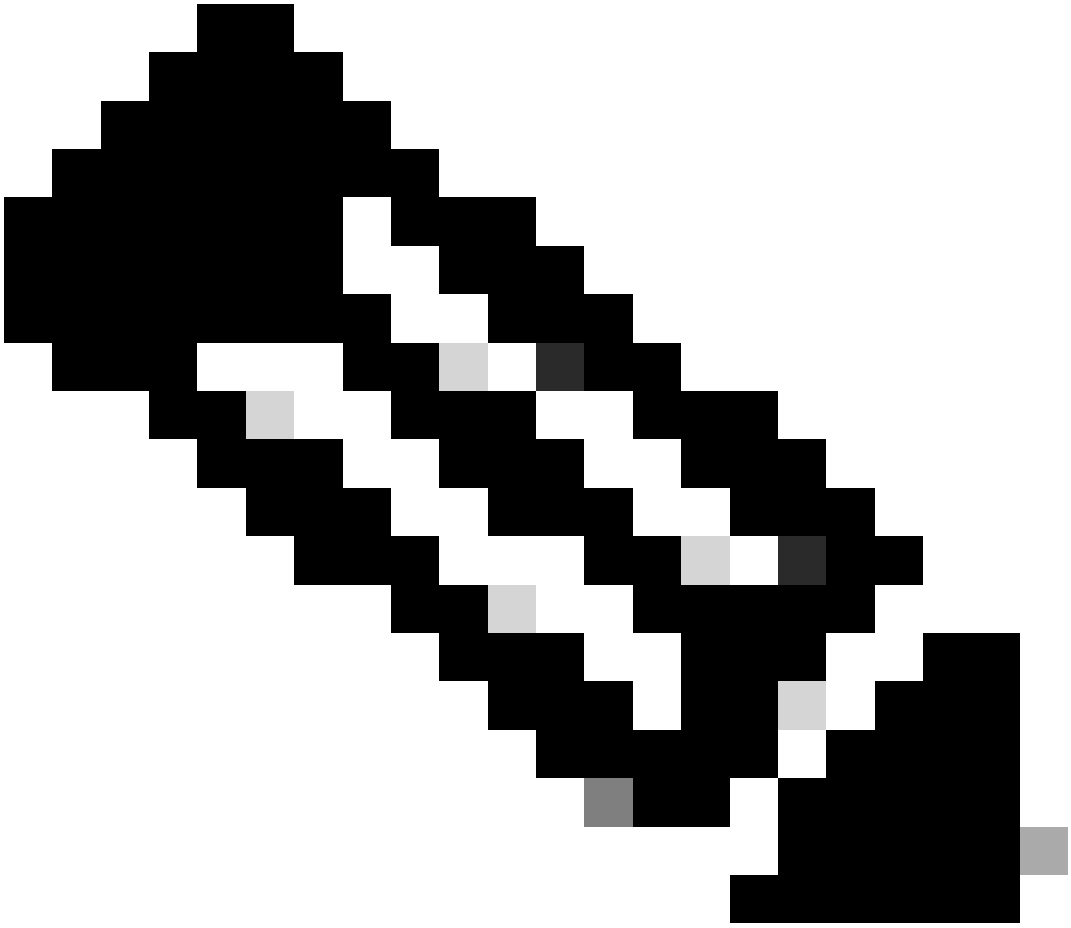
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

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.





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.