Problemen oplossen met niet-browsertoepassingen in Umbrella

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met niet-browsertoepassingen in Cisco Umbrella.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

In dit artikel worden best practices en stappen voor probleemoplossing uitgelegd voor het configureren van niet-browsertoepassingen om te functioneren met Umbrella Secure Web

Gateway. In de meeste gevallen zijn er geen configuratiewijzigingen nodig. Bepaalde toepassingen werken echter niet goed met beveiligings-/inspectiefuncties (zoals SSL-decodering) en er moeten uitzonderingen worden toegevoegd om de toepassing te laten functioneren met een webproxy. Dit geldt voor Umbrella SWG en andere web proxy-oplossingen.

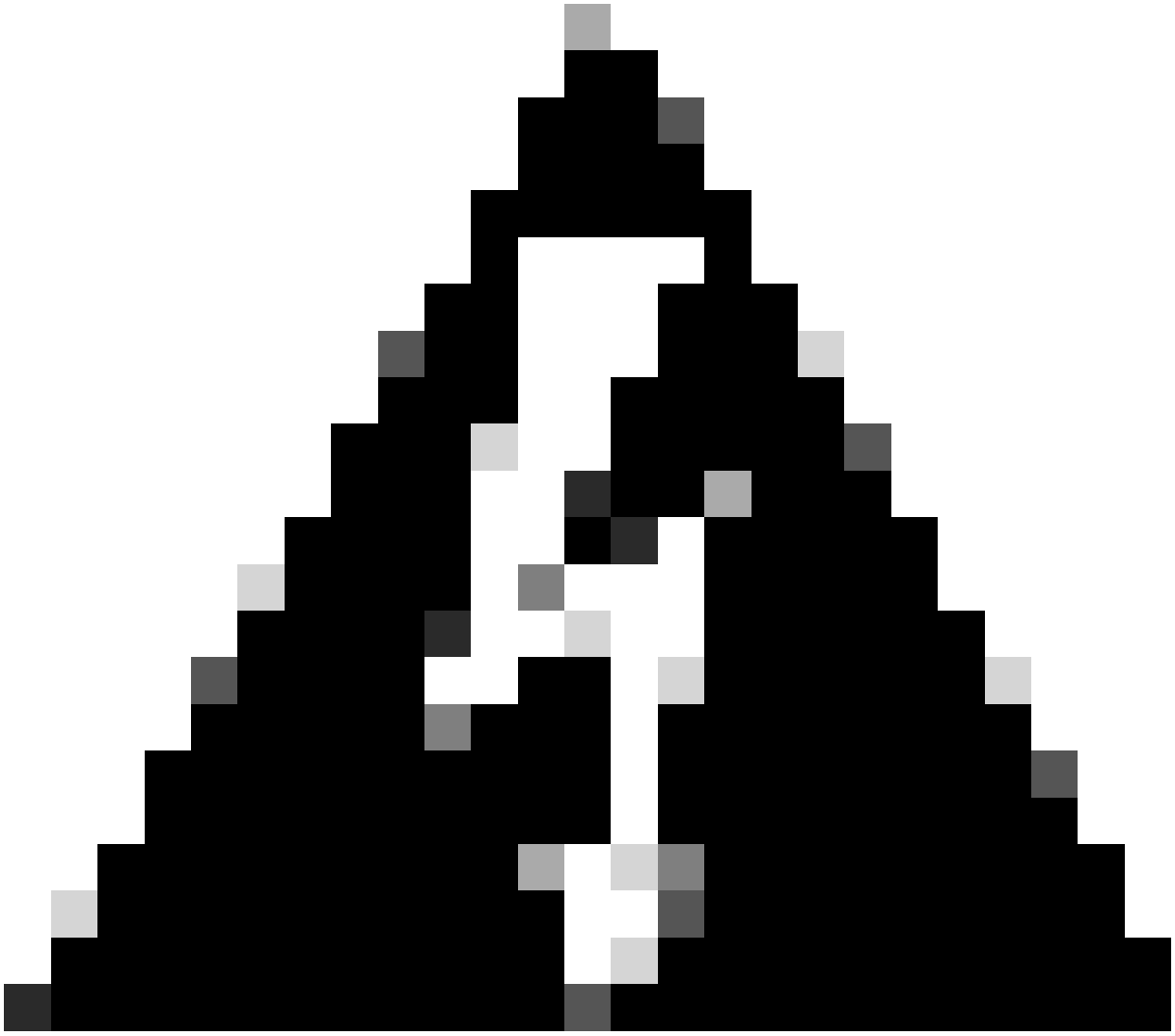
Dit is handig in omstandigheden waarin de website / browserversie van een toepassing werkt, maar de desktop / mobiele versie van de toepassing niet.

Compatibiliteitsproblemen

Aanvragen kunnen om deze redenen onverenigbaar zijn:

CA-installatie met parapluwortel	De Cisco Umbrella Root CA moet altijd worden vertrouwd voor foutloze TLS-verbindingen. • Oplossing: voor niet-webtoepassingen moet u ervoor zorgen dat de Cisco Umbrella Root CA wordt vertrouwd in het certificaatarchief van het systeem/de lokale machine.
certificaatvastlegging	Certificate Pinning (PKP) is wanneer de toepassing verwacht een nauwkeurig blad (of CA-certificaat) te ontvangen om de TLS-handshake te valideren. De toepassing kan geen certificaat accepteren dat is gegenereerd door een webproxy en is niet compatibel met SSL-decoderingsfuncties. • Oplossing: omzeil de toepassing of het domein van SSL-decodering met behulp van een selectieve decoderingslijst (zie Waarschuwing na tabel) Meer details over toepassingen waarvan bekend is dat ze worden beïnvloed door certificaatpinning zijn hier beschikbaar: Public Key Pinning / Certificate Pinning
Ondersteuning voor TLS-versies	De toepassing kan een oudere TLS-versie / -codering gebruiken die om veiligheidsredenen niet wordt ondersteund door SWG. • Oplossing: omzeil het verkeer van verzending naar Umbrella met behulp van de functie Externe domeinen (PAC / AnyConnect) of VPN-uitsluitingen (Tunnel) (zie Waarschuwing na tabel).
niet-webprotocol	Sommige toepassingen gebruiken niet-http(s)-protocollen, maar verzenden deze gegevens nog steeds via algemene webpoorten die worden onderschept door SWG. SWG kan dit verkeer niet begrijpen. • Oplossing: raadpleeg de leverancier van de toepassing om de

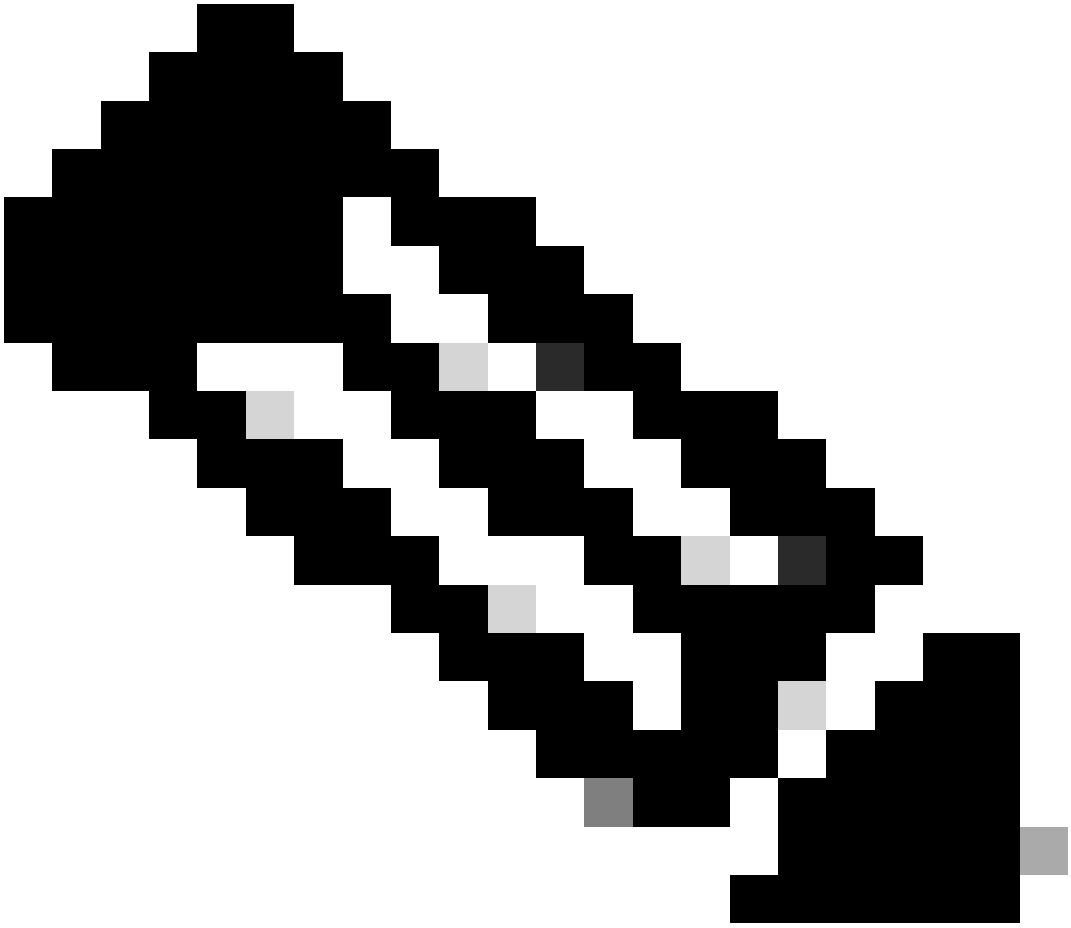
	bestemmingsadressen / IP-bereiken te bepalen die door de software worden gebruikt. Deze software moet worden uitgesloten van SWG met behulp van Externe domeinen (PAC / AnyConnect) of VPN-uitsluitingen (Tunnel) (zie Waarschuwing na tabel).
SAML-verificatie	De meeste niet-browsertoepassingen kunnen geen SAML-verificatie uitvoeren. Umbrella daagt niet-browsertoepassingen voor SAML niet uit en daarom kan het filterbeleid op basis van gebruikers/groepen niet overeenkomen. • Oplossing: schakel de IP Surrogates-functie in zodat gebruikersinformatie in de cache kan worden opgeslagen voor gebruik met niet-browsertoepassingen. • Alternatief: de toepassing/het domein toestaan in een webregel op basis van netwerk- of tunnelidentiteiten (geen gebruikers/groepen).
HTTP-bereikaanvragen	Sommige applicaties gebruiken HTTP "Byte-Range" verzoeken bij het downloaden van gegevens; wat betekent dat slechts een klein deel van het bestand wordt gedownload op een moment. Deze verzoeken zijn om veiligheidsredenen uitgeschakeld in SWG omdat deze techniek ook kan worden gebruikt om antivirusdetectie te omzeilen. • Oplossing (HTTPS): omzeil de toepassing of het domein van SSL-decodering* in Umbrella met behulp van selectieve decoderingslijsten. • Oplossing (HTTP): omzeil de toepassing of het domein van antivirusscanning* met behulp van een webregel met de optie Beveiliging overschrijven. • Alternatief: Neem contact op met Umbrella Support als u standaard* Range-verzoeken voor uw organisatie wilt hebben ingeschakeld.
Expliciete proxycompatibiliteit	Sommige toepassingen respecteren de proxy-instellingen van het systeem niet (bijvoorbeeld PAC-bestanden) en zijn over het algemeen niet compatibel met expliciete webproxies. Deze toepassingen routeren niet via Umbrella SWG in een PAC-bestandsimplementatie. • Oplossing: de toepassing moet zijn toegestaan via de firewall van het lokale netwerk. Raadpleeg de applicatieverkoper voor details over bestemmingen/havens die zijn toegestaan.



Waarschuwing: als u deze uitzonderingen maakt, kunt u beveiligingsinspectiefuncties uitschakelen, zoals antivirusscannen, DLP-scannen, huurderscontroles, bestandstypecontrole en URL-inspectie. Doe dit alleen als u de bron van deze bestanden vertrouwt. De zakelijke behoefte aan de toepassing moet worden afgewogen tegen de gevolgen voor de veiligheid van het uitschakelen van deze functies.

Microsoft 365-toepassingen

De Microsoft 365 Compatibility-functie sluit automatisch een aantal Microsoft-domeinen uit van SSL-decodering en beleidshandhavingsfuncties. Deze functie kan worden ingeschakeld om problemen met de desktopversie van Microsoft-apps op te lossen. Zie Globale instellingen beheren voor meer informatie.

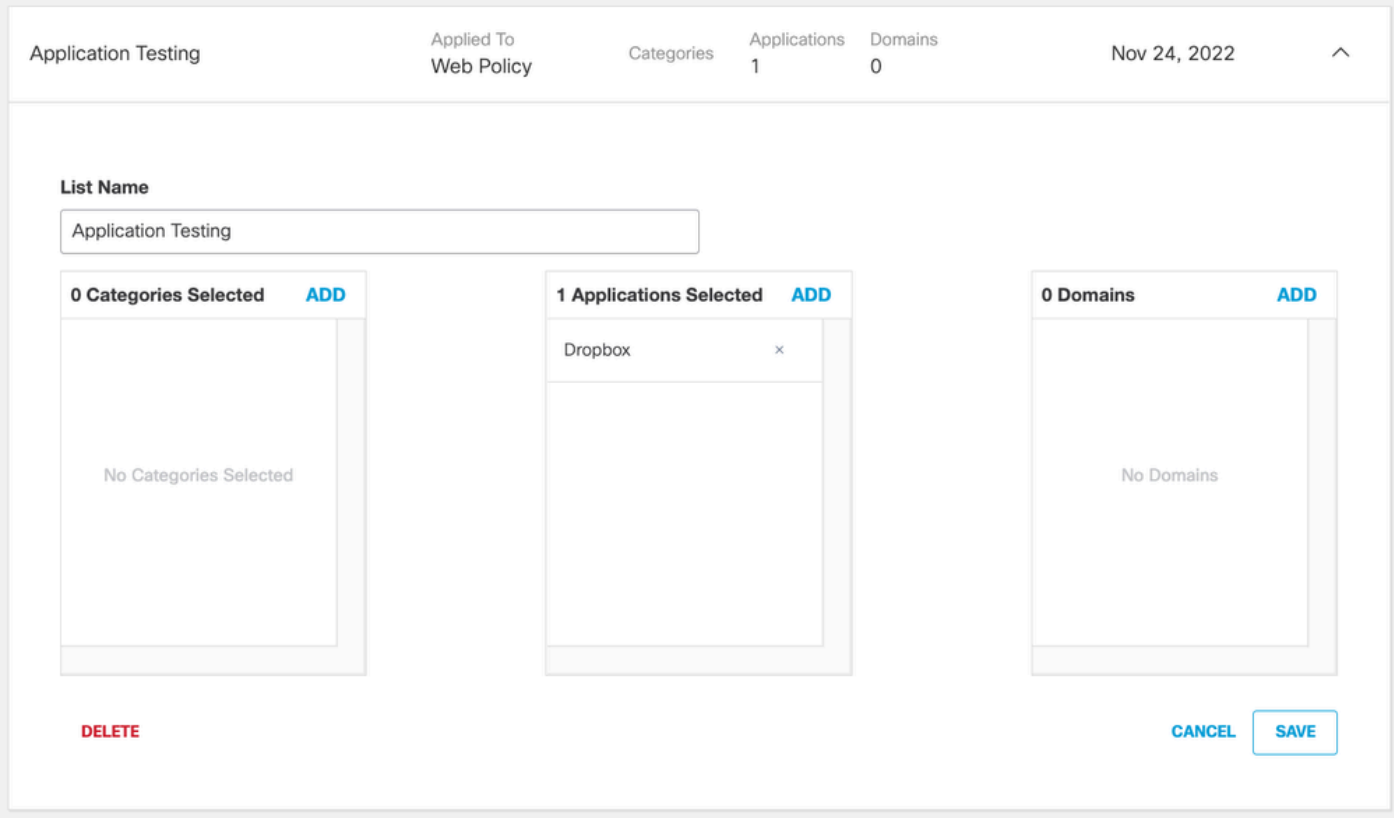


Opmerking: Microsoft 365 Compatibility sluit niet alle Microsoft-domeinen uit. Umbrella gebruikt de aanbevelingen van Microsoft voor de lijst met domeinen die moeten worden uitgesloten van filtering. Zie Nieuwe Office 365-eindpuntcategorieën voor meer informatie.

Bypass voor certificaatvastlegging

Certificate Pinning (PKP) is een veel voorkomende oorzaak van compatibiliteitsproblemen met apps. Cisco biedt een uitgebreide lijst met benoemde toepassingen die kunnen worden geconfigureerd om SSL-decryptie te omzeilen om een oplossing te vinden. De selectieve decodering kan worden geconfigureerd in Beleid > Selectieve decoderingslijsten.

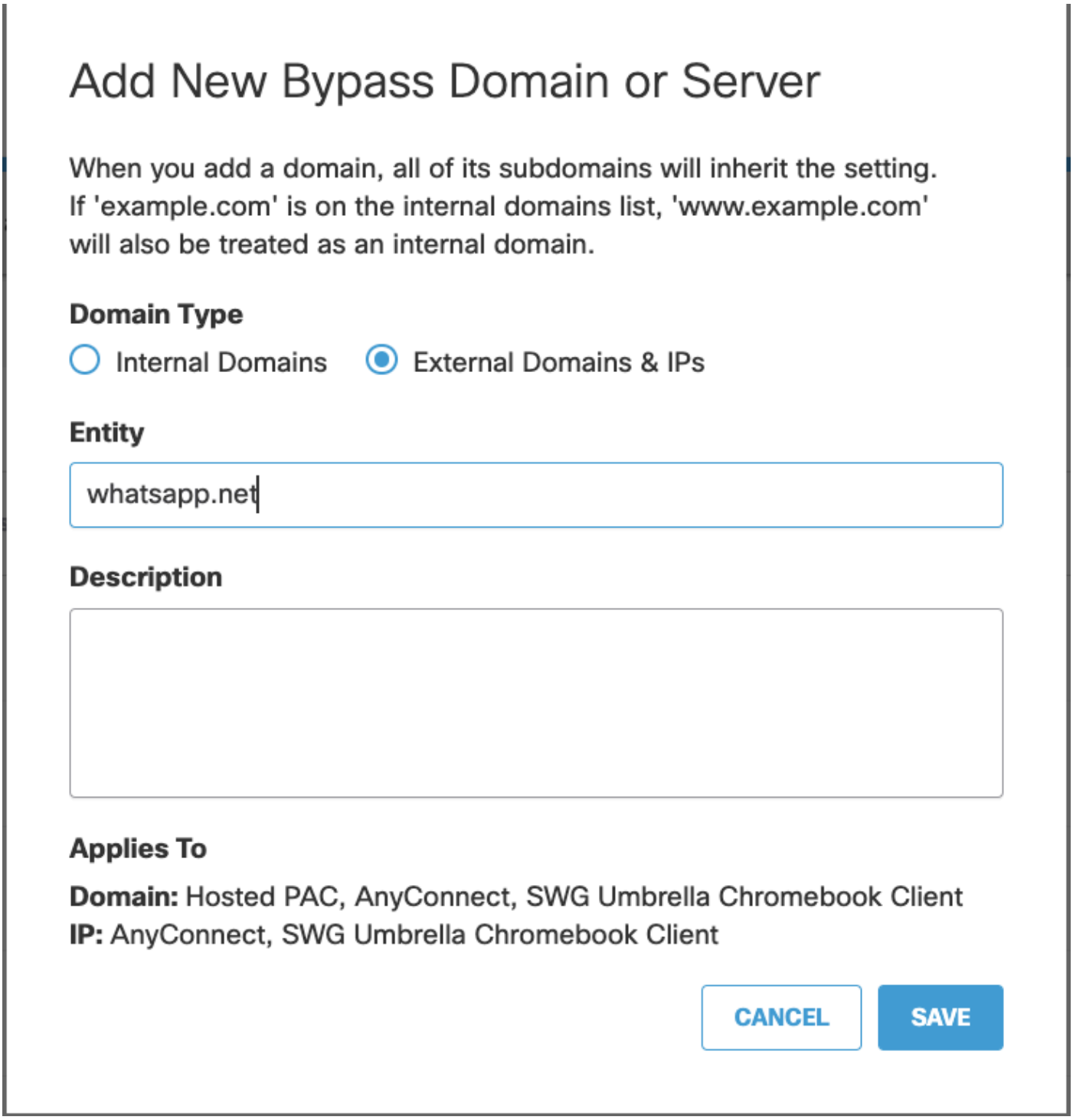
In de meeste gevallen kan de beheerder problemen met het vastzetten van certificaten oplossen door de toepassing simpelweg bij de naam uit te sluiten. Dit betekent dat deze problemen kunnen worden opgelost zonder dat u lijsten met domeinen hoeft te leren of bij te houden.



Als alternatief kunnen toepassingen worden omzeild op basis van het bestemmingsdomein / IP-adres. Neem contact op met de leverancier van de toepassing om de toepasselijke lijst met domeinen/IP's te bepalen of zie Uitsluitingen voor certificaatvastlegging identificeren.

TLS-compatibiliteitsbypass

Bestaande of aangepaste TLS-versies zijn een veelvoorkomende oorzaak van compatibiliteitsproblemen met apps. Deze problemen kunnen worden opgelost door het verkeer uit te sluiten van Umbrella in Implementaties > Domeinbeheer > Externe domeinen en IP's. In een tunnelimplementatie kan het verkeer alleen worden uitgesloten door uitzonderingen toe te voegen aan uw VPN-configuratie.



Neem contact op met de leverancier van de toepassing om de toepasselijke lijst met domeinen/IP's te bepalen om uitsluitingen voor incompatibele TLS-versies uit te sluiten of zie "Uitsluitingen identificeren voor incompatibele TLS-versies" (verderop in dit artikel).

Problemen oplossen (geavanceerd)

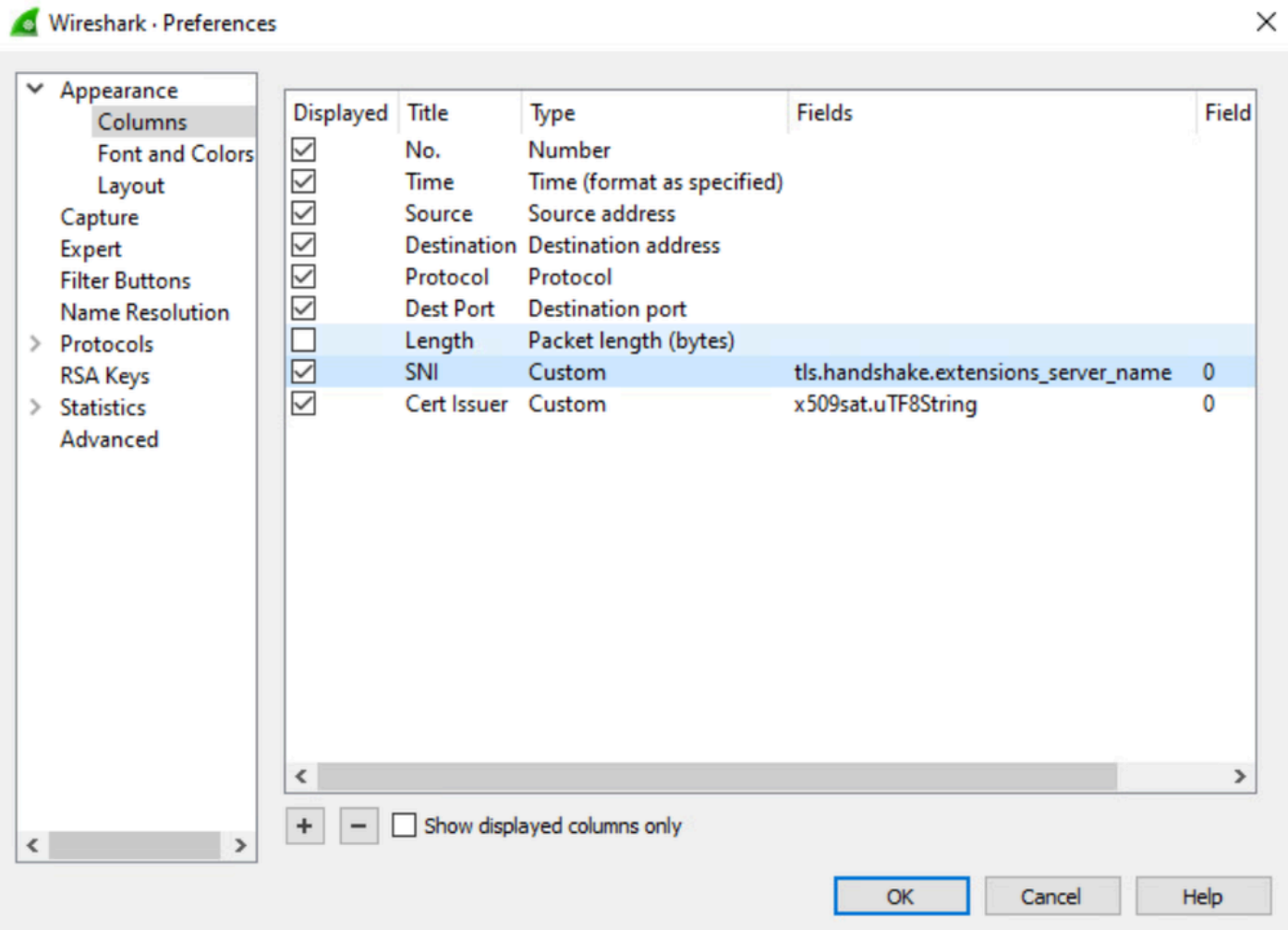
De overige instructies in dit artikel gebruiken Wireshark (www.wireshark.org) pakketopnames voor het oplossen van problemen. Wireshark kan helpen om te identificeren welke domeinen worden gebruikt door applicaties voor hulp bij het implementeren van aangepaste uitsluitingen. Voordat u begint, voegt u deze aangepaste kolommen toe in Wireshark:

1. Download Wireshark van [www.wireshark.org.](http://www.wireshark.org)

2. Ga naar Bewerken > Voorkeuren > Kolommen.

3. Maak kolommen van het type Aangepast met deze velden:

```
http.host
tls.handshake.extensions_server_name
x509sat.uTF8String
```



Als u een pakketopname wilt uitvoeren, vult u deze instructies in of raadpleegt u Netwerkverkeer vastleggen met Wireshark.

1. Voer Wireshark uit als beheerder.

2. Selecteer de relevante netwerkinterfaces in Vastleggen > Opties.

- Voor PAC-/tunnelimplementaties kunt u gegevens vastleggen op uw normale LAN-netwerkinterface.
- Leg voor AnyConnect-implementaties gegevens vast op uw LAN-netwerkinterface en de loopback-interface.

3. Sluit alle andere toepassingen behalve de probleemtoepassing.

4. Spoel uw DNS-cache door: `ipconfig /flushdns`

5. Start de wireshark-vangst.

6. Repliceer het probleem snel en stop de wireshark-vangst.

Uitsluitingen voor certificaatvastlegging identificeren

Certificaat pinning wordt afgedwongen op de client, wat betekent dat het exacte gedrag en de resolutie stappen verschilt voor elke toepassing. Zoek in de vastleguitvoer naar veelbetekenende tekenen dat een TLS-verbinding faalt:

- Een TLS-verbinding wordt snel gesloten of opnieuw ingesteld (RST of FIN).
- Een TLS-verbinding wordt herhaaldelijk opnieuw geprobeerd.
- Het certificaat voor de TLS-verbinding wordt uitgegeven door Cisco Umbrella en wordt daarom gedecodeerd.

Deze voorbeeldfilters van Wireshark kunnen helpen om de belangrijke details van TLS-verbindingen te bekijken.

Tunnel / AnyConnect

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

PAC / Proxy-chaining

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

In dit voorbeeld wordt de bureaubladtoepassing van DropBox beïnvloed door certificaatpinning wanneer wordt geprobeerd verbinding te maken met client.dropbox.com.

(tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.reset eq 1 || tcp.flags.fin eq 1)

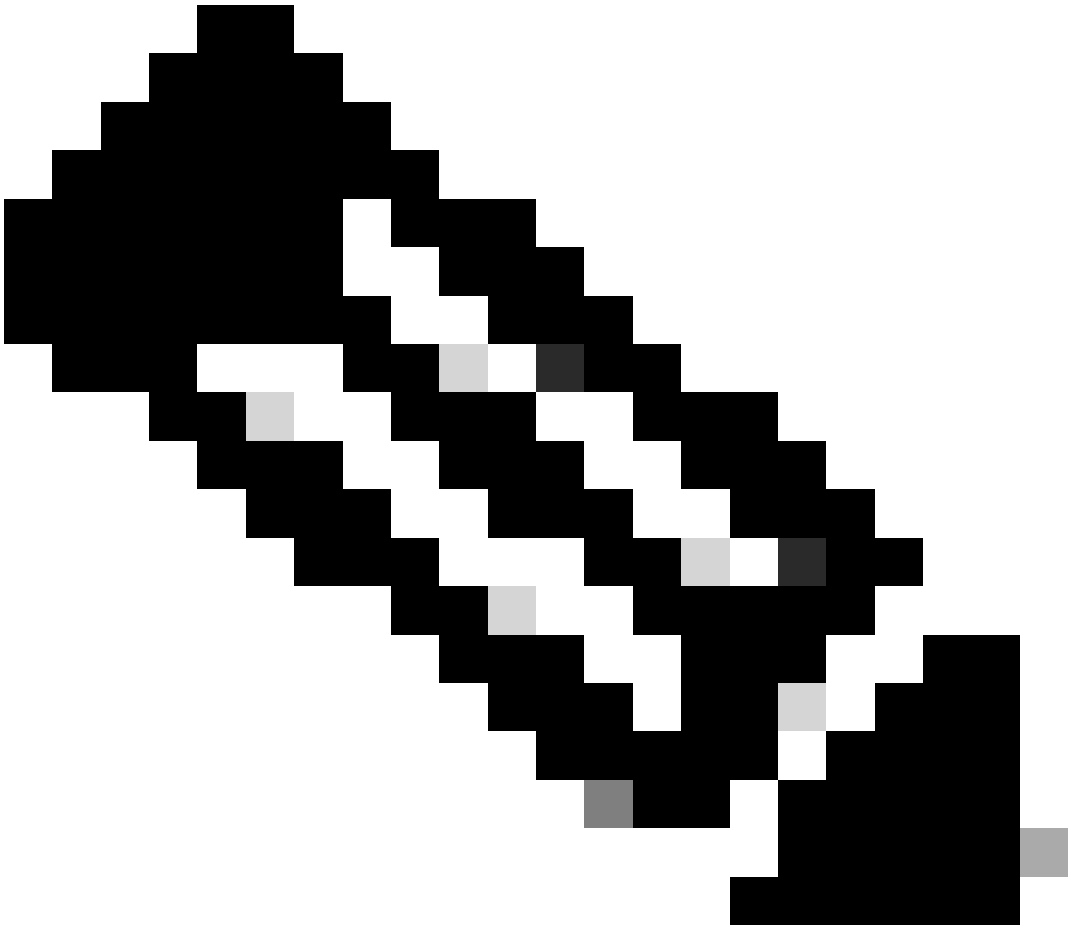
No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
281	43.038669	10.10.199.101	162.125.6.13	TCP	443		65148 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261120 Len=0
283	43.073849	162.125.6.13	10.10.199.101	TCP	65148		443 → 65148 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
287	43.083933	10.10.199.101	162.125.6.13	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]
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		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

Destination IP

Server Name

Retries

FIN Flag



Opmerking: na het toevoegen van de nodige uitsluiting(en), kunt u deze stappen

meerdere keren herhalen om alle bestemmingen te identificeren die door de toepassing worden gebruikt.

Uitsluitingen voor incompatibele TLS-versies identificeren

Zoek naar SSL/TLS-verbindingen die geen gebruik maken van de verplichte TLS1.2+-protocollen die worden ondersteund door Umbrella SWG. Dit kan bestaande protocollen (TLS1.0 of eerder) of aangepaste protocollen op maat zijn die door een toepassing worden geïmplementeerd.

Dit voorbeeldfilter toont u de eerste TLS-handshake-pakketten samen met DNS-query's.

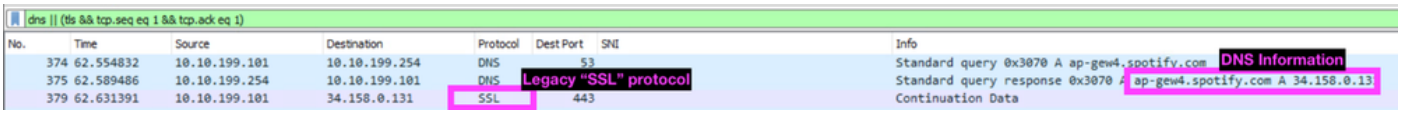
Tunnel / AnyConnect

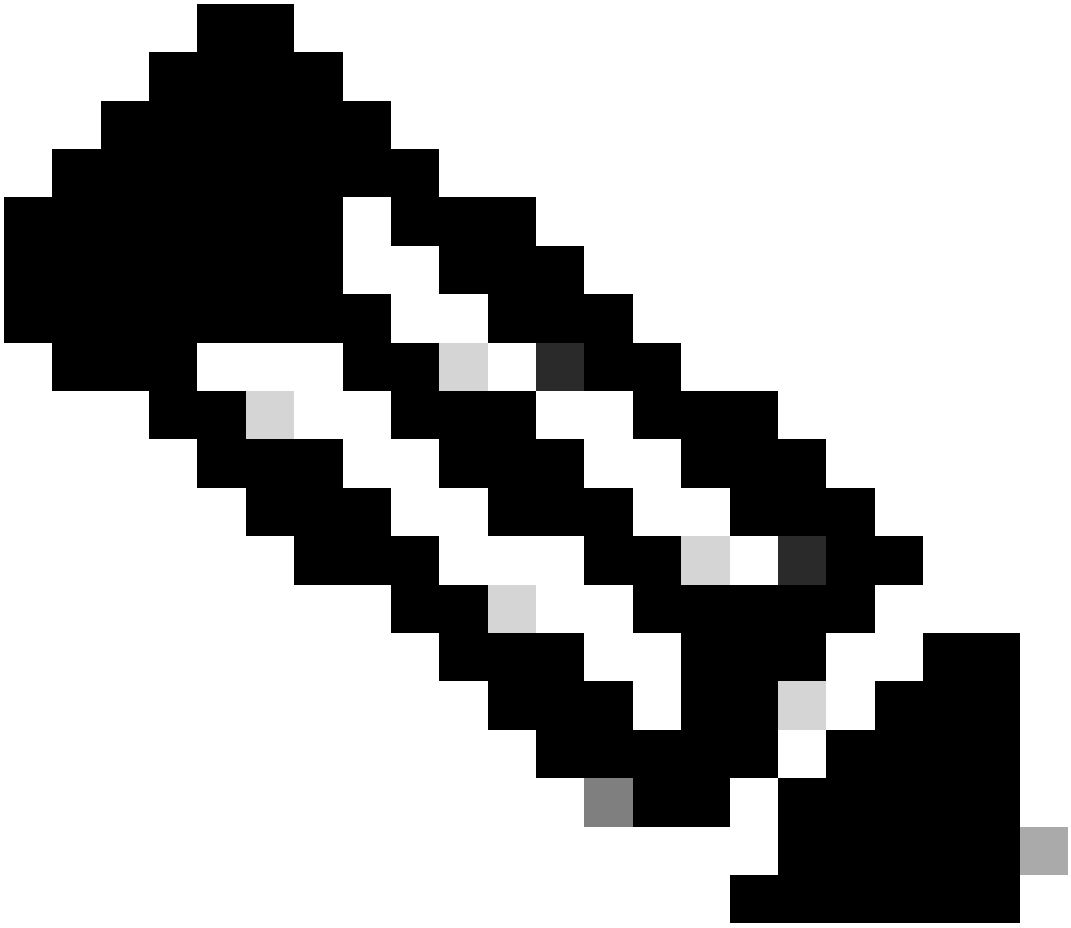
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

PAC / Proxy-chaining

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

In dit voorbeeld probeert de Spotify-desktoptoepassing verbinding te maken met ap-gew4.spotify.com met een niet-standaard of verouderd "SSL"-protocol dat niet via SWG kan worden verzonden.





Opmerking: na het toevoegen van de nodige uitsluiting(en), kunt u deze stappen meerdere keren herhalen om alle bestemmingen te identificeren die door de toepassing worden gebruikt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.