Dépannage des applications non-navigateur dans Umbrella

Table des matières

Introduction

Ce document décrit comment dépanner des applications qui ne sont pas des navigateurs dans Cisco Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Cet article explique les meilleures pratiques et les étapes de dépannage pour configurer les applications non-navigateur pour qu'elles fonctionnent avec la passerelle Web sécurisée Umbrella. Dans la plupart des cas, aucune modification de configuration n'est requise. Cependant, certaines

applications ne fonctionnent pas bien avec les fonctions de sécurité/inspection (telles que le déchiffrement SSL) et des exceptions doivent être ajoutées pour que l'application fonctionne avec un proxy Web. Cela s'applique à Umbrella SWG ainsi qu'à d'autres solutions de proxy Web.

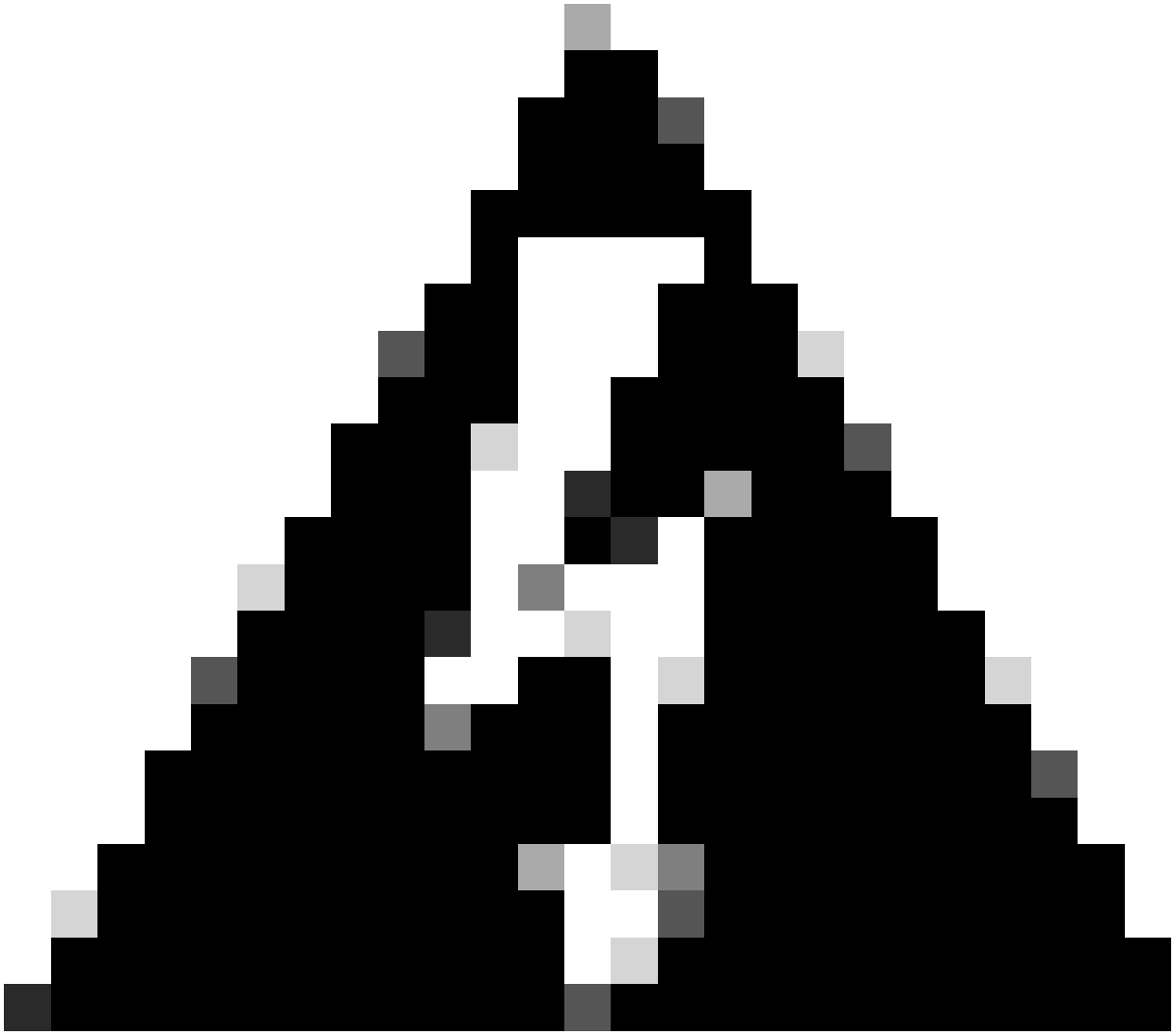
Cela est utile dans les cas où la version site Web/navigateur d'une application fonctionne, mais pas la version bureau/mobile de l'application.

Problèmes de compatibilité

Les applications peuvent être incompatibles pour les raisons suivantes :

Installation CA racine Umbrella	L'autorité de certification Cisco Umbrella Root doit toujours être approuvée pour les connexions TLS sans erreur. • Solution : Pour les applications non Web, assurez-vous que l'autorité de certification Cisco Umbrella Root est approuvée dans le magasin de certificats du système / de la machine locale.
Épinglage du certificat	L'épinglage de certificat (PKP) est le moment où l'application s'attend à recevoir un leaf précis (ou un certificat CA) pour valider la connexion TLS. L'application ne peut pas accepter un certificat généré par un proxy Web et n'est pas compatible avec les fonctions de décodage SSL. • Solution : Ignorer l'application ou le domaine du déchiffrement SSL à l'aide d'une liste de déchiffrement sélectif (voir Avertissement après le tableau) Pour plus d'informations sur les applications affectées par l'épinglage de certificat, cliquez ici : Épinglage de clé publique/épinglage de certificat
Prise en charge des versions TLS	L'application peut utiliser une ancienne version de TLS / Chiffre qui n'est pas prise en charge par SWG pour des raisons de sécurité. • Solution : Évitez que le trafic ne soit envoyé à Umbrella à l'aide de la fonctionnalité External Domains (PAC / AnyConnect) ou des exclusions VPN (Tunnel) (voir Avertissement après le tableau).
Protocole non Web	Certaines applications utilisent des protocoles autres que http(s), mais envoient toujours ces données sur des ports Web communs qui sont interceptés par SWG. SWG ne peut pas comprendre ce trafic. • Solution : Consultez le fournisseur d'applications pour déterminer les adresses de destination / plages IP utilisées par le logiciel. Ce logiciel doit être exclu de SWG à l'aide de Domaines externes (PAC / AnyConnect) ou d'Exclusions VPN (Tunnel) (voir Avertissement après le tableau).

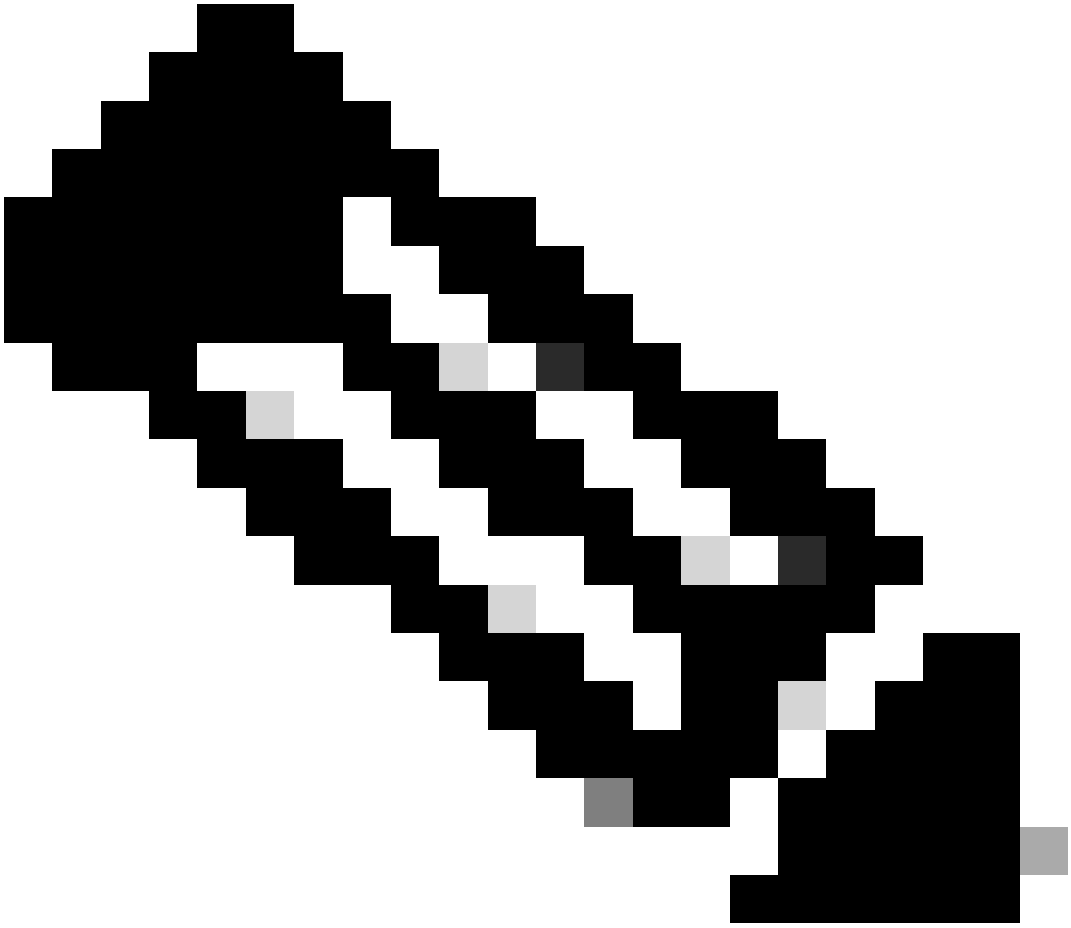
Authentification SAML	La plupart des applications autres que les navigateurs ne sont pas en mesure d'effectuer l'authentification SAML. Umbrella ne conteste pas les applications non-navigateur pour SAML et par conséquent les stratégies de filtrage basées sur l'utilisateur/le groupe ne peuvent pas correspondre. • Solution : Activez la fonctionnalité IP Surrogates afin que les informations utilisateur puissent être mises en cache pour une utilisation avec des applications non-navigateur. • Alternative : Autoriser l'application/le domaine dans une règle Web basée sur les identités de réseau ou de tunnel (et non sur les utilisateurs/groupes).
Requêtes de plage HTTP	Certaines applications utilisent des requêtes HTTP « Plage d'octets » lors du téléchargement de données ; ce qui signifie que seul un petit morceau du fichier est téléchargé à la fois. Ces requêtes sont désactivées pour des raisons de sécurité dans SWG, car cette technique peut également être utilisée pour contourner la détection antivirus. • Solution (HTTPS) : Ignorez l'application ou le domaine du décodage SSL* dans Umbrella à l'aide de listes de décodage sélectives. • Solution (HTTP) : Ignorer l'application ou le domaine de l'analyse antivirus* à l'aide d'une règle Web avec l'option Remplacer la sécurité. • Alternative : Contactez l'assistance Umbrella si vous souhaitez que les requêtes Range soient activées par défaut* pour votre organisation.
Compatibilité proxy explicite	Certaines applications ne respectent pas les paramètres du proxy système (par ex. fichiers PAC) et ne sont généralement pas compatibles avec les proxies Web explicites. Ces applications ne sont pas acheminées via Umbrella SWG dans un déploiement de fichiers PAC. • Solution : L'application doit être autorisée via le pare-feu du réseau local. Consultez le fournisseur de l'application pour obtenir des détails sur les destinations/ports autorisés.



Avertissement : La création de ces exceptions peut désactiver les fonctions d'inspection de sécurité, notamment l'analyse antivirus, l'analyse DLP, les contrôles de locataire, le contrôle de type de fichier et l'inspection d'URL. Ne le faites que si vous êtes prêt à faire confiance à la source de ces fichiers. Les besoins de l'entreprise pour l'application doivent être évalués en fonction de l'impact de la désactivation de ces fonctionnalités sur la sécurité.

Applications Microsoft 365

La fonctionnalité de compatibilité de Microsoft 365 exclut automatiquement un certain nombre de domaines Microsoft des fonctions de décodage SSL et d'application des stratégies. Cette fonctionnalité peut être activée pour résoudre les problèmes liés à la version Desktop des applications Microsoft. Pour plus d'informations, voir Gérer les paramètres globaux.

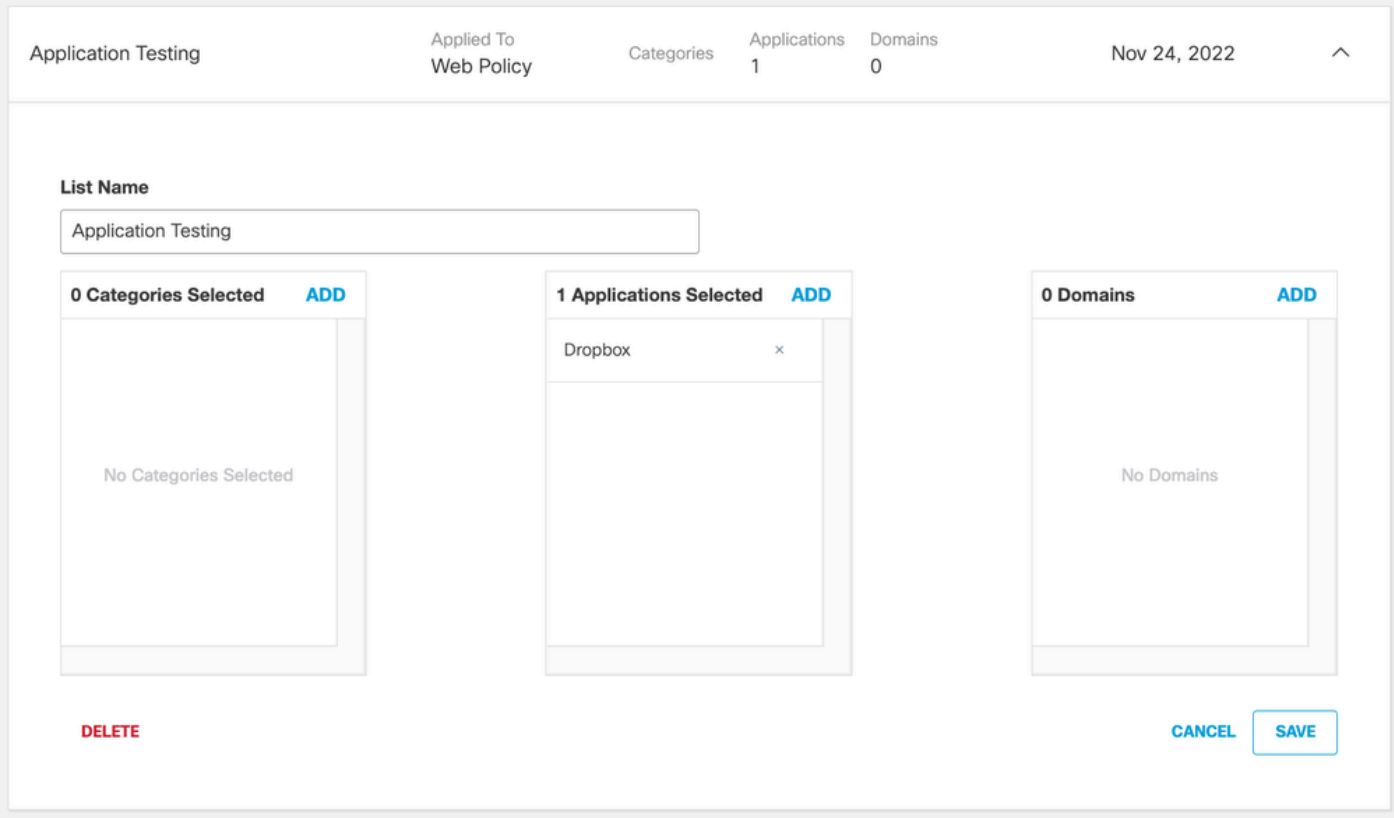


Remarque : La fonctionnalité de compatibilité de Microsoft 365 n'exclut pas tous les domaines Microsoft. Umbrella utilise les recommandations de Microsoft pour la liste des domaines qui doivent être exclus du filtrage. Pour plus d'informations, consultez Nouvelles catégories de terminaux Office365.

Contournement de l'épinglage du certificat

L'épinglage de certificat (PKP) est une cause courante de problèmes de compatibilité des applications. Cisco fournit une liste complète d'applications nommées qui peuvent être configurées pour contourner le décryptage SSL. Le décodage sélectif peut être configuré dans Politiques > Listes de décodage sélectif.

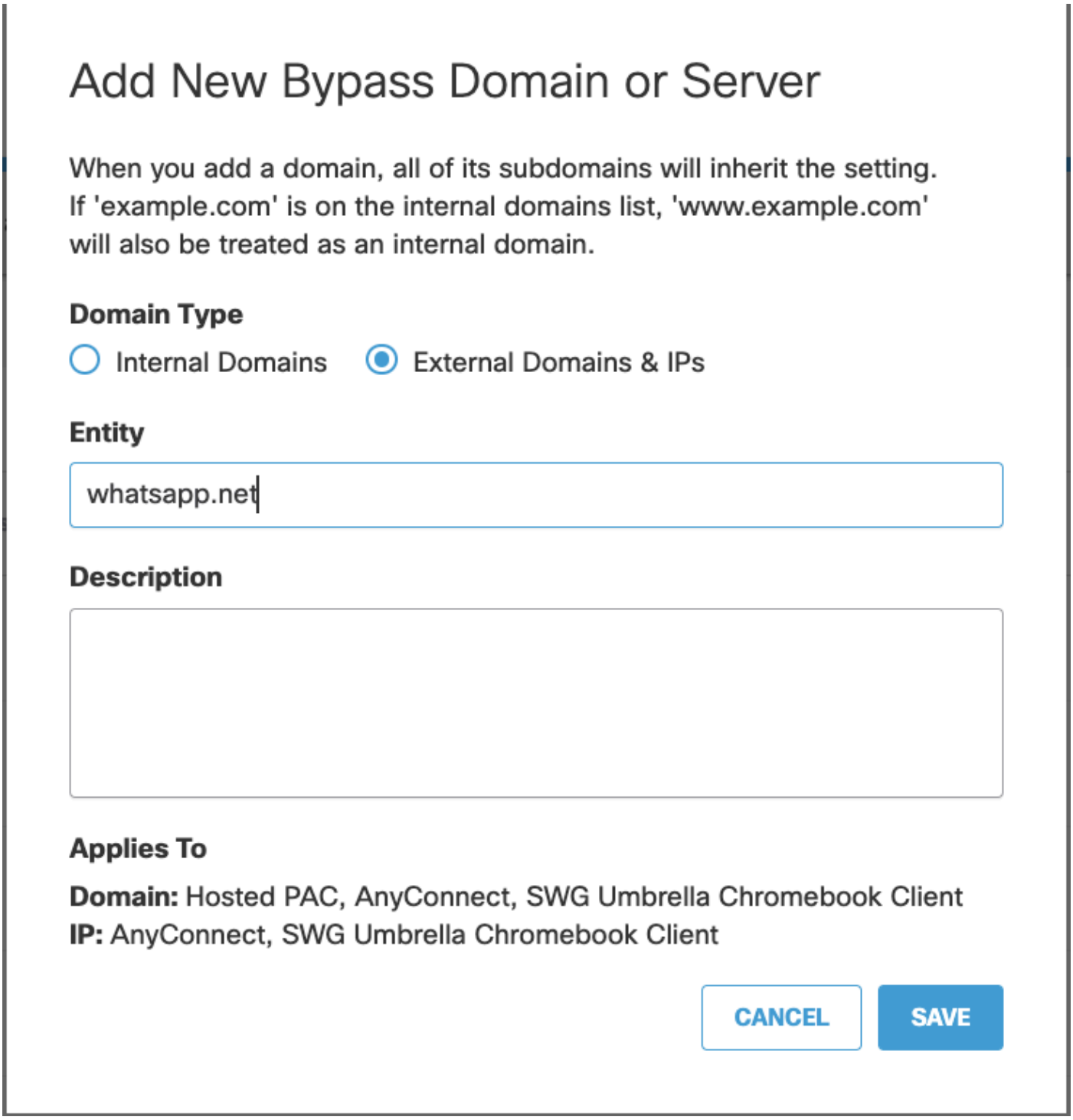
Dans la plupart des cas, l'administrateur peut résoudre les problèmes d'épinglage de certificat en excluant simplement l'application par son nom. Cela signifie que ces problèmes peuvent être résolus sans avoir à apprendre ou à tenir à jour des listes de domaines.



Les applications peuvent également être contournées en fonction du domaine de destination/de l'adresse IP. Contactez le fournisseur de l'application pour déterminer la liste applicable des domaines/IP ou consultez la section Identifier les exclusions pour l'épinglage de certificat.

Contournement de compatibilité TLS

Les versions TLS héritées ou personnalisées sont souvent à l'origine de problèmes de compatibilité des applications. Ces problèmes peuvent être résolus en excluant le trafic d'Umbrella dans Déploiements > Gestion des domaines > Domaines externes et IP. Dans un déploiement de tunnel, le trafic ne peut être exclu qu'en ajoutant des exceptions dans votre configuration VPN.



Contactez le fournisseur de l'application pour déterminer la liste applicable des domaines/IP à exclure ou consultez la section « Identification des exclusions pour les versions TLS incompatibles » (plus loin dans cet article).

Dépannage (avancé)

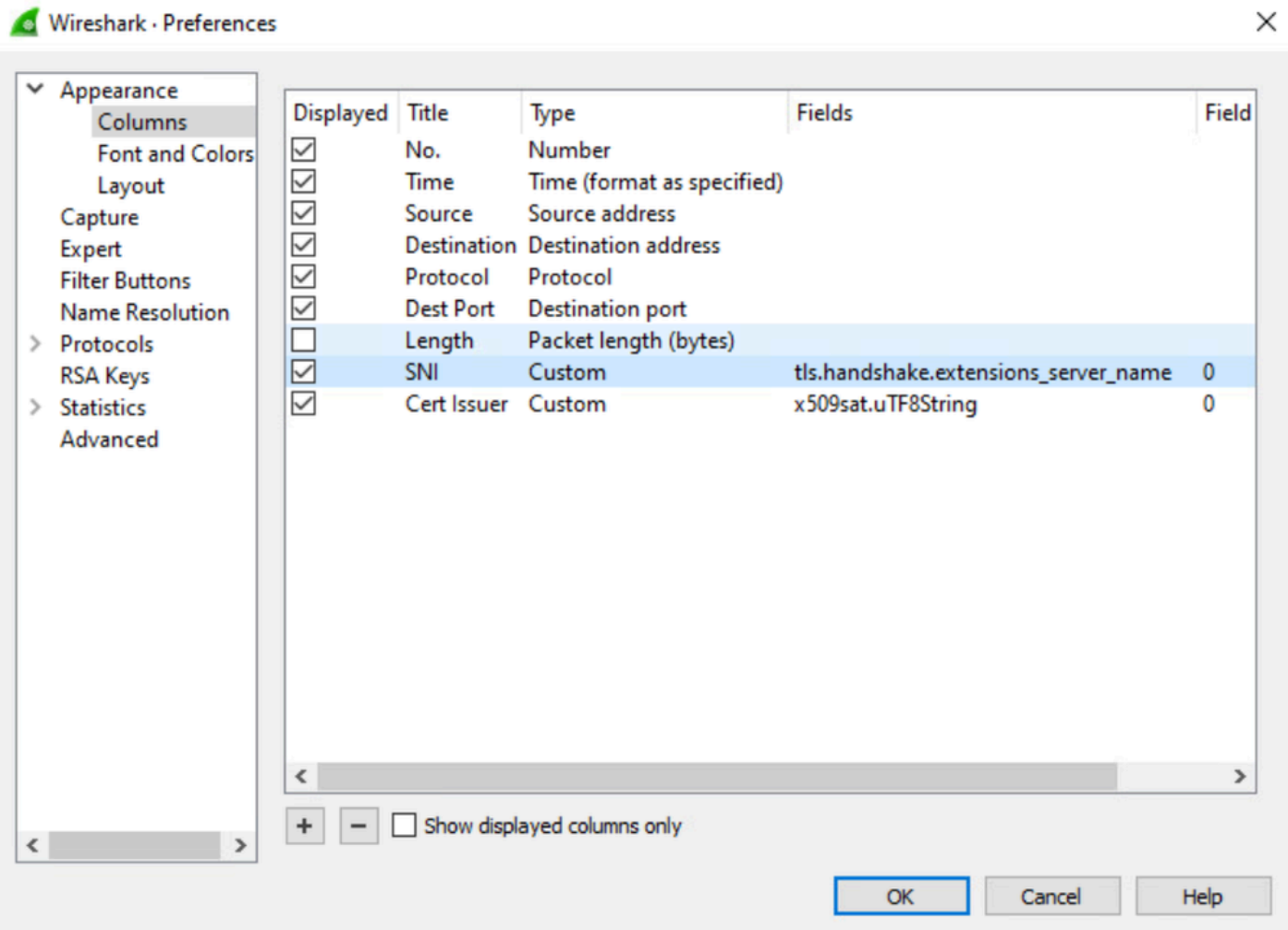
Les instructions restantes de cet article utilisent les captures de paquets Wireshark (www.wireshark.org) à des fins de dépannage. Wireshark peut aider à identifier les domaines utilisés par les applications pour mettre en oeuvre des exclusions personnalisées. Avant de commencer, ajoutez ces colonnes personnalisées dans Wireshark :

1. Téléchargez Wireshark depuis [www.wireshark.org.](http://www.wireshark.org)

2. Accédez à Modifier > Préférences > Colonnes.

3. Créez des colonnes de type Personnalisé avec ces champs :

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



Pour effectuer une capture de paquets, suivez ces instructions ou reportez-vous à la section Capture du trafic réseau avec Wireshark.

1. Exécutez Wireshark en tant qu'administrateur.

2. Sélectionnez les interfaces réseau appropriées dans Capture > Options.

- Pour les déploiements PAC / Tunnel, effectuez une capture sur votre interface réseau LAN normale.
- Pour les déploiements AnyConnect, effectuez une capture sur votre interface réseau LAN et sur l'interface de bouclage.

3. Fermez toutes les autres applications, à l'exception de l'application qui pose problème.

4. Videz votre cache DNS : `ipconfig /flushdns`

5. Démarrez la capture Wireshark.

6. Répétez rapidement le problème et arrêtez la capture Wireshark.

Identifier les exclusions pour l'épinglage des certificats

L'épinglage de certificat est appliqué au client, ce qui signifie que le comportement exact et les étapes de résolution diffèrent pour chaque application. Dans le résultat de la capture, recherchez des signes révélateurs d'échec d'une connexion TLS :

- Une connexion TLS est rapidement fermée ou réinitialisée (RST ou FIN).
- Une connexion TLS est tentée à plusieurs reprises.
- Le certificat pour la connexion TLS est émis par Cisco Umbrella et est donc en cours de déchiffrement.

Ces exemples de filtres Wireshark peuvent vous aider à afficher les détails importants des connexions TLS.

Tunnel / AnyConnect

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

Chaînage PAC/Proxy

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

Dans cet exemple, l'application de bureau Dropbox est affectée par l'épinglage de certificat lors de la tentative de connexion à client.dropbox.com.

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

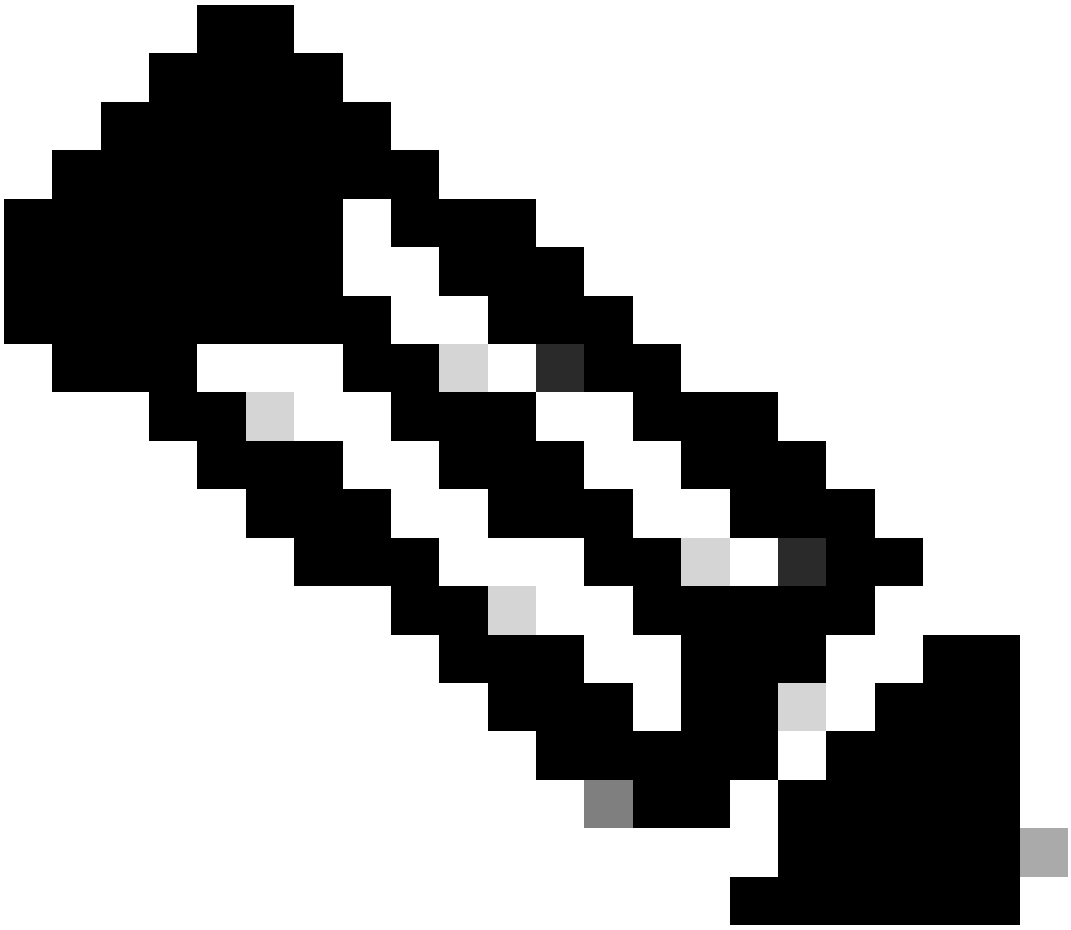
No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
281	43.038669	10.10.199.101	162.125.6.13	TCP	443		65148 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261120 Len=0
283	43.073849	162.125.6.13	10.10.199.101	TCP	65148		443 → 65148 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
287	43.083933	10.10.199.101	162.125.6.13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

FIN Flag

Retries



Remarque : Après avoir ajouté la ou les exclusions nécessaires, vous pouvez répéter ces

étapes plusieurs fois pour identifier toutes les destinations utilisées par l'application.

Identifier les exclusions pour les versions TLS incompatibles

Recherchez les connexions SSL/TLS qui n'utilisent pas les protocoles TLS1.2+ obligatoires pris en charge par Umbrella SWG. Il peut s'agir de protocoles hérités (TLS1.0 ou version antérieure) ou de protocoles personnalisés personnalisés mis en oeuvre par une application.

Cet exemple de filtre vous montre les paquets de connexion TLS initiaux avec les requêtes DNS.

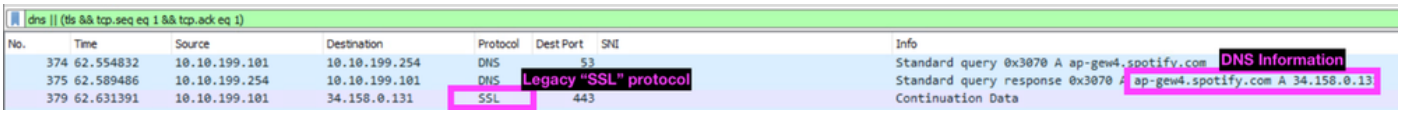
Tunnel/AnyConnect

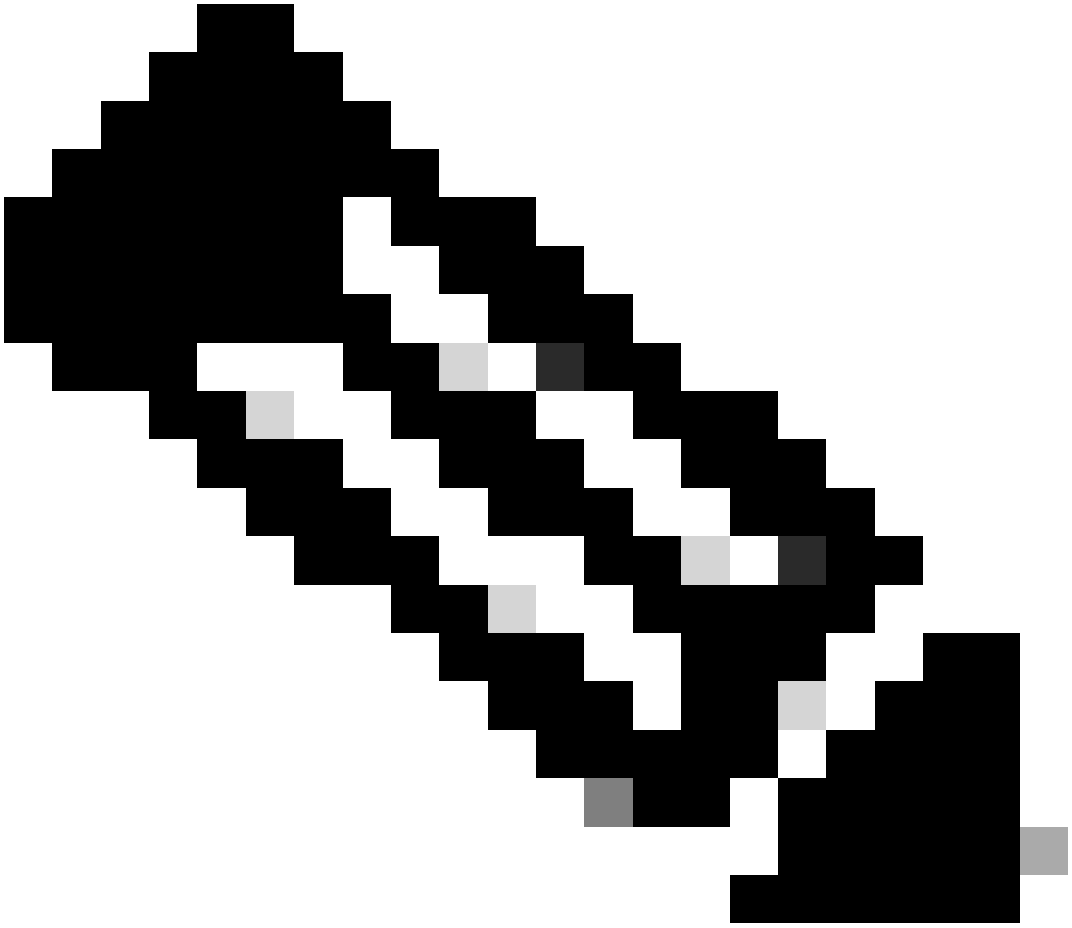
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

Chaînage PAC/Proxy

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

Dans cet exemple, l'application de bureau Spotify tente de se connecter à ap-gew4.spotify.com en utilisant un protocole "SSL" non standard ou hérité qui ne peut pas être envoyé via SWG.





Remarque : Après avoir ajouté la ou les exclusions nécessaires, vous pouvez répéter ces étapes plusieurs fois pour identifier toutes les destinations utilisées par l'application.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.