Risoluzione dei problemi relativi alle applicazioni non browser in Umbrella

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Panoramica

Problemi di compatibilità

Applicazioni Microsoft 365

Bypass associazione certificato

Bypass compatibilità TLS

Risoluzione dei problemi (avanzata)

Identifica le esclusioni per il blocco del certificato

Identifica le esclusioni per le versioni TLS non compatibili

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alle applicazioni diverse dai browser in Cisco Umbrella.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

In questo articolo vengono illustrate le procedure ottimali e la procedura di risoluzione dei problemi per la configurazione di applicazioni non basate su browser per il funzionamento con Umbrella

Secure Web Gateway. Nella maggior parte dei casi, non è necessario apportare modifiche alla configurazione. Alcune applicazioni, tuttavia, non funzionano correttamente con le funzioni di sicurezza/ispezione (come la decrittografia SSL) ed è necessario aggiungere delle eccezioni per fare in modo che l'applicazione funzioni con un proxy Web. Ciò vale sia per Umbrella SWG che per altre soluzioni di proxy Web.

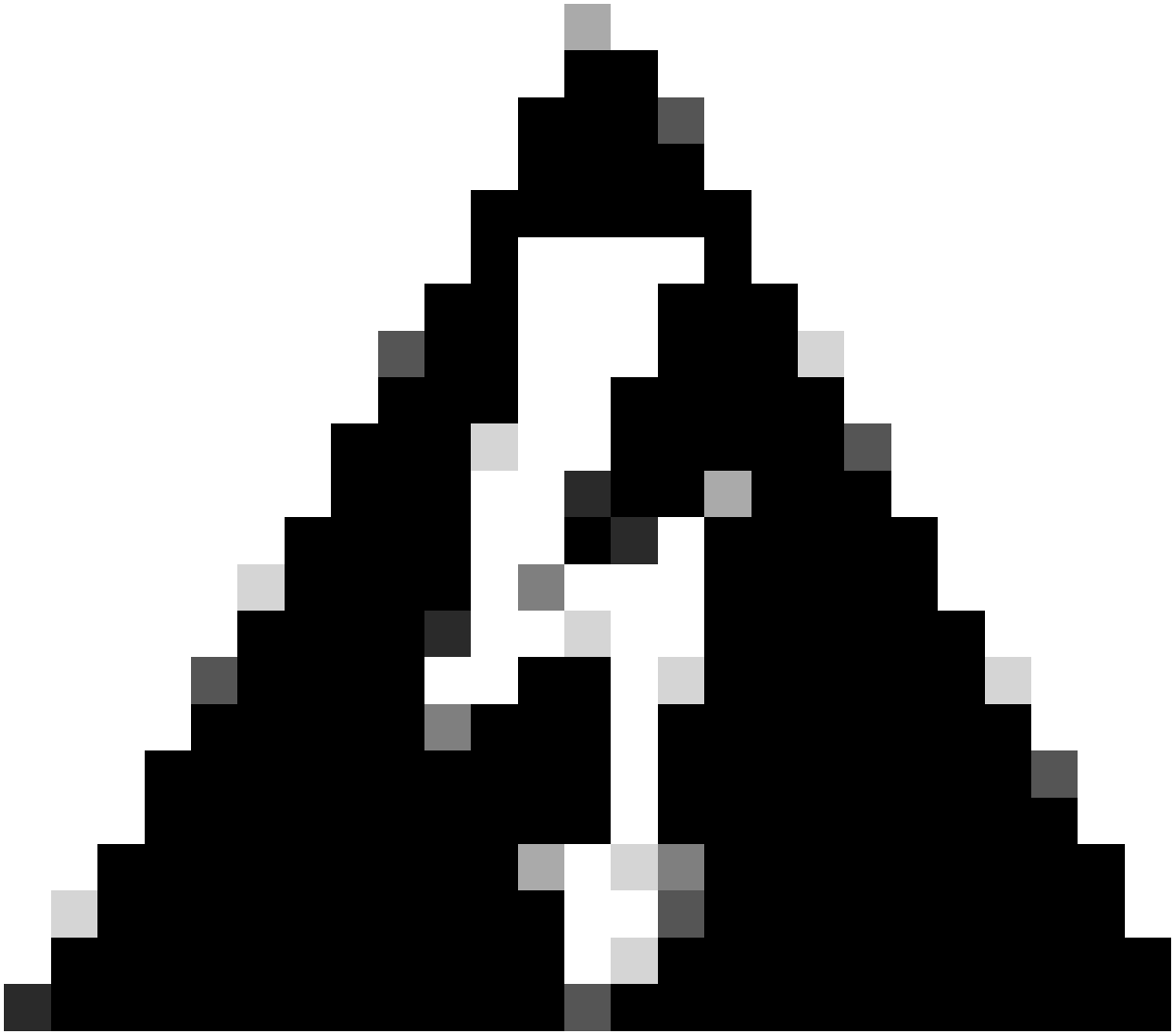
Ciò è utile nei casi in cui funziona la versione del sito Web/browser di un'applicazione, ma non la versione desktop/mobile dell'applicazione.

Problemi di compatibilità

Le applicazioni possono essere incompatibili per i seguenti motivi:

Installazione CA radice Umbrella	La CA radice Cisco Umbrella deve essere sempre considerata attendibile per le connessioni TLS senza errori. • Soluzione: Per le applicazioni non Web, verificare che la CA radice Cisco Umbrella sia attendibile nell'archivio certificati del sistema/computer locale.
Blocco certificato	Il PKP (Certificate Pinning) si verifica quando l'applicazione si aspetta di ricevere una foglia precisa (o certificato CA) per convalidare l'handshake TLS. L'applicazione non può accettare un certificato generato da un proxy Web e non è compatibile con le funzioni di decrittografia SSL. • Soluzione: Ignorare l'applicazione o il dominio dalla decrittografia SSL utilizzando un elenco di decrittografia selettiva (vedere Avviso dopo la tabella) Per ulteriori informazioni sulle applicazioni notoriamente interessate dall'associazione dei certificati, vedere: Pinning chiave pubblica/Pinning certificato
Supporto versione TLS	L'applicazione può utilizzare una versione / crittografia TLS precedente non supportata da SWG per motivi di sicurezza. • Soluzione: Evitare che il traffico venga inviato a Umbrella usando la funzionalità Domini esterni (PAC/AnyConnect) o le esclusioni VPN (Tunnel) (vedere la sezione Avviso dopo la tabella).
Protocollo non Web	Alcune applicazioni utilizzano protocolli non http(s), ma inviano comunque questi dati su porte Web comuni intercettate da SWG. Il gruppo SWG non riesce a capire questo traffico. • Soluzione: Consultare il fornitore dell'applicazione per determinare gli indirizzi di destinazione / gli intervalli IP utilizzati dal software. Questo

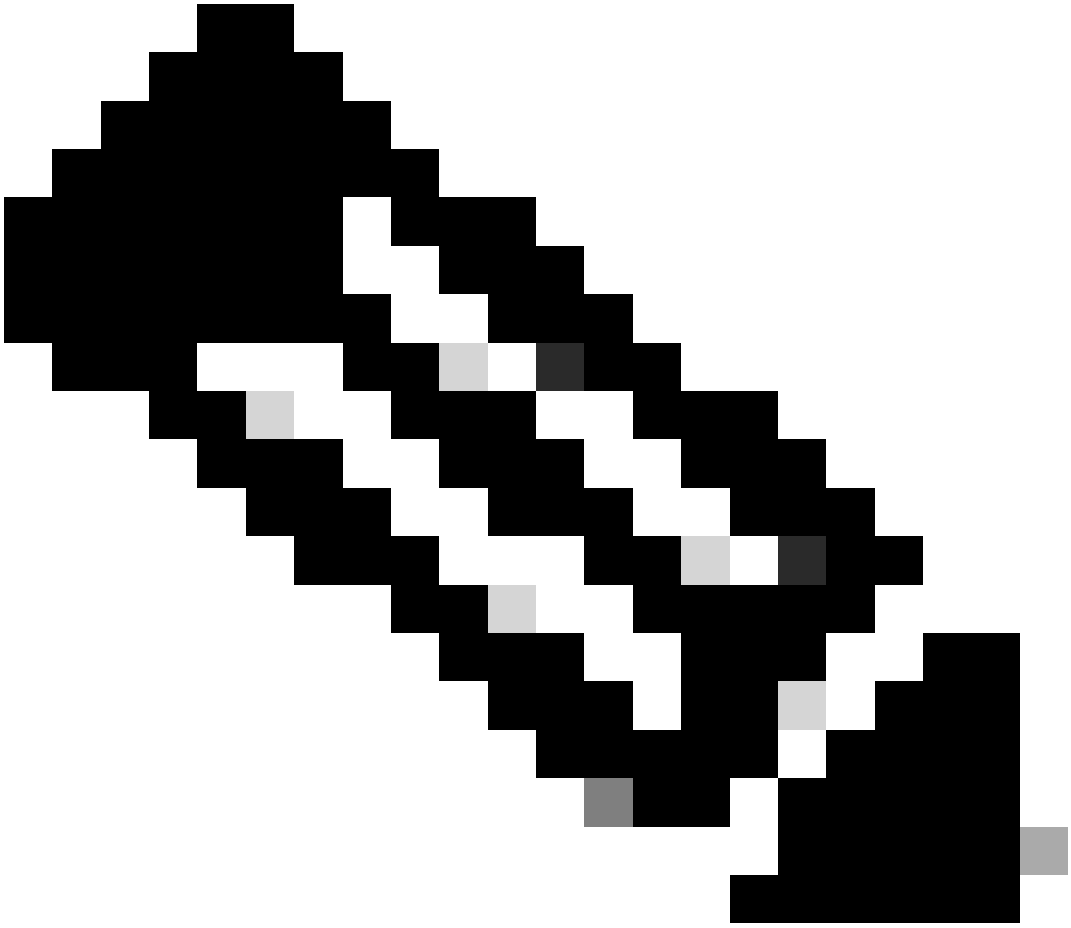
	software deve essere escluso da SWG con domini esterni (PAC/AnyConnect) o esclusioni VPN (tunnel) (vedere la tabella Avviso dopo).
autenticazione SAML	La maggior parte delle applicazioni non basate su browser non è in grado di eseguire l'autenticazione SAML. Umbrella non contesta le applicazioni non browser per SAML e pertanto i criteri di filtro basati su User/Group non possono corrispondere. • Soluzione: Abilitare la funzione IP Surrogates in modo che le informazioni utente possano essere memorizzate nella cache per l'utilizzo con applicazioni non browser. • Alternativa: Consenti applicazione/dominio in una regola Web basata sulle identità di rete o tunnel (non utenti/gruppi).
Richieste intervallo HTTP	Alcune applicazioni utilizzano le richieste HTTP "Byte-Range" per il download dei dati; significa che viene scaricata solo una piccola parte del file alla volta. Queste richieste sono disabilitate per motivi di sicurezza in SWG perché questa tecnica può essere utilizzata anche per evitare il rilevamento antivirus. • Soluzione (HTTPS): Ignora l'applicazione o il dominio dalla decrittografia SSL* in Umbrella utilizzando gli elenchi di decrittografia selettiva. • Soluzione (HTTP): Ignorare l'applicazione o il dominio da Anti-Virus scanning* utilizzando una regola Web con l'opzione Override Security. • Alternativa: Contatta il supporto Umbrella se desideri che le richieste Range siano abilitate per impostazione predefinita* per la tua organizzazione.
Compatibilità proxy esplicita	Alcune applicazioni non rispettano le impostazioni del proxy di sistema (ad es. file PAC) e non sono generalmente compatibili con proxy Web espliciti. Queste applicazioni non eseguono il routing attraverso Umbrella SWG in una distribuzione di file PAC. • Soluzione: L'applicazione deve essere consentita tramite il firewall della rete locale. Consultare il fornitore dell'applicazione per i dettagli sulle destinazioni/porte da consentire.



Avviso: La creazione di queste eccezioni può disabilitare le funzioni di ispezione della sicurezza, tra cui la scansione antivirus, la scansione DLP, i controlli tenant, il controllo del tipo di file e l'ispezione URL. Eseguire questa operazione solo se si desidera considerare attendibile l'origine di questi file. La necessità aziendale dell'applicazione deve essere valutata in base all'impatto sulla sicurezza della disattivazione di queste funzionalità.

Applicazioni Microsoft 365

La funzionalità Compatibilità di Microsoft 365 esclude automaticamente alcuni domini Microsoft dalle funzioni di decrittografia SSL e di applicazione delle policy. Questa funzionalità può essere abilitata per risolvere i problemi con la versione Desktop delle app Microsoft. Per ulteriori informazioni, vedere Gestire le impostazioni globali.

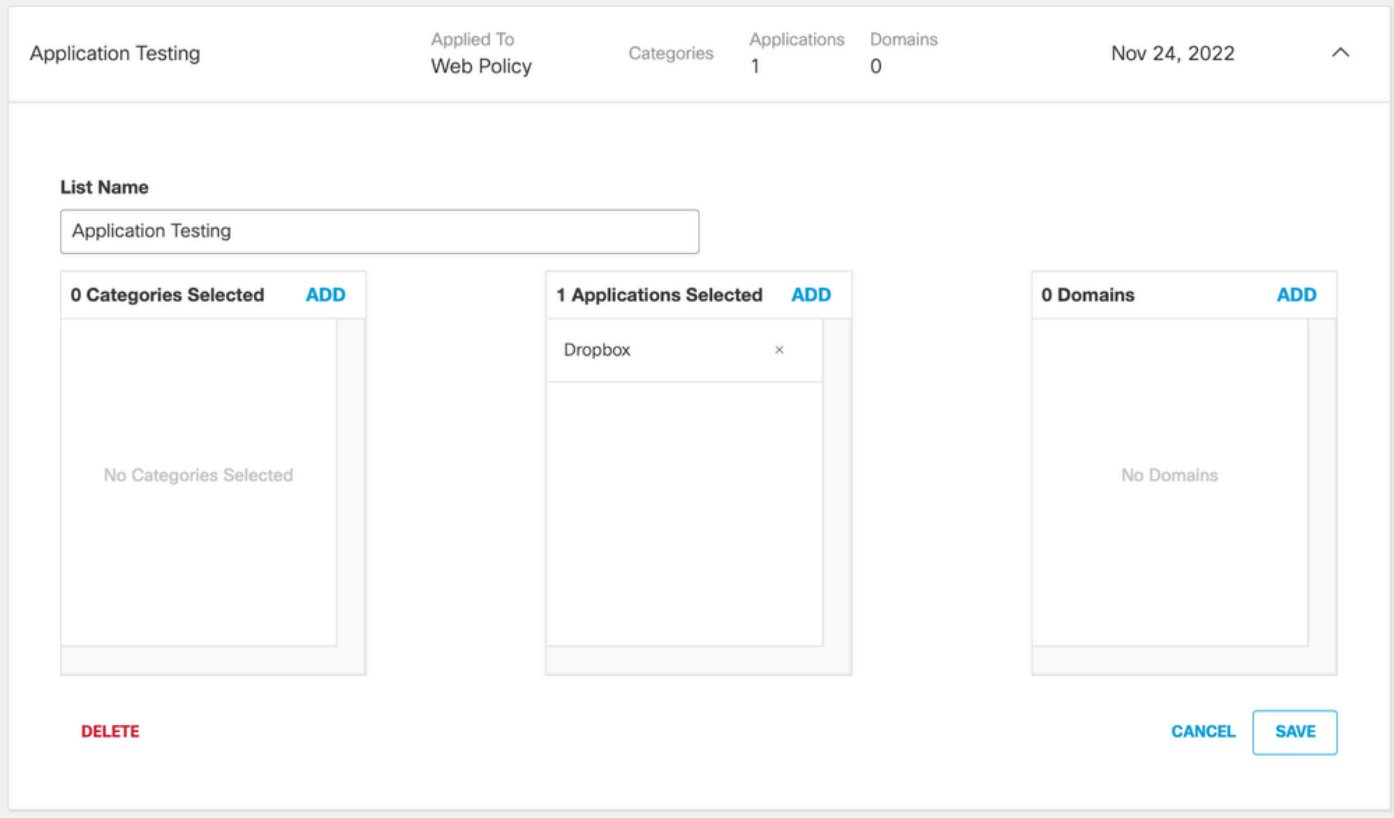


Nota: La caratteristica di compatibilità di Microsoft 365 non esclude tutti i domini Microsoft. Umbrella utilizza i suggerimenti di Microsoft per l'elenco dei domini che devono essere esclusi dal filtro. Per ulteriori informazioni, vedere Nuove categorie di endpoint di Office 365.

Bypass associazione certificato

Il Pinning del certificato (PKP) è una causa comune di problemi di compatibilità delle app. Cisco fornisce un elenco completo delle applicazioni denominate che possono essere configurate in modo da ignorare la decrittografia SSL e risolvere il problema. La decrittografia selettiva può essere configurata in Criteri > Elenchi di decrittografia selettiva.

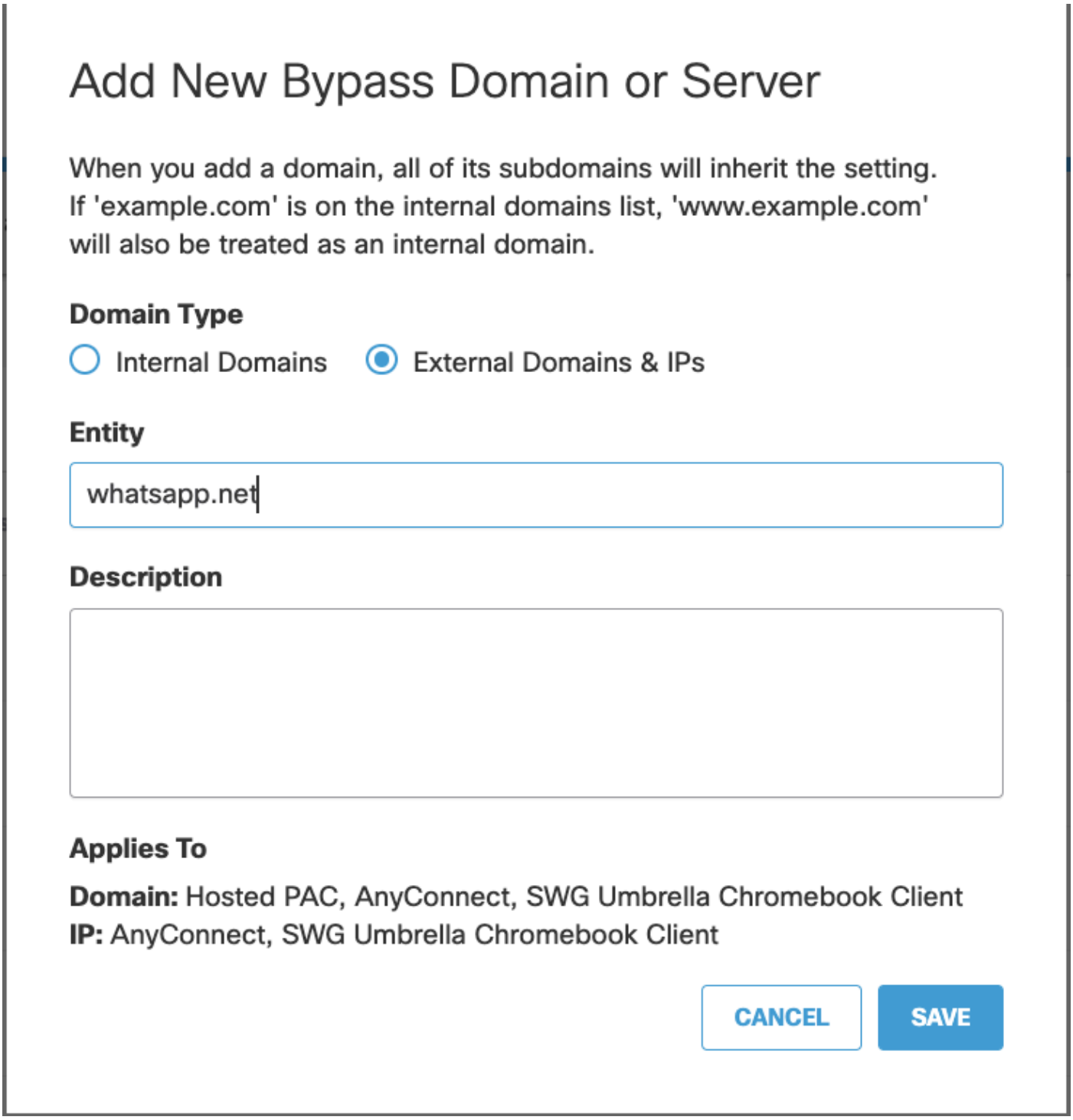
Nella maggior parte dei casi, l'amministratore può risolvere i problemi di associazione dei certificati semplicemente escludendo l'applicazione in base al nome. Questo significa che questi problemi possono essere risolti senza dover imparare o mantenere elenchi di domini.



In alternativa, è possibile ignorare le applicazioni in base al dominio o all'indirizzo IP di destinazione. Contattare il fornitore dell'applicazione per determinare l'elenco di domini/IP applicabile o vedere Identificare le esclusioni per il blocco del certificato.

Bypass compatibilità TLS

Le versioni TLS legacy o personalizzate sono una causa comune dei problemi di compatibilità delle app. Per risolvere questi problemi, è possibile escludere il traffico proveniente da Umbrella in Distribuzioni > Gestione domini > Domini esterni e IP. In una distribuzione tunnel il traffico può essere escluso solo aggiungendo eccezioni nella configurazione VPN.



Contattare il fornitore dell'applicazione per determinare l'elenco applicabile di domini/IP da escludere o vedere "Identificare le esclusioni per le versioni TLS incompatibili" (più avanti in questo articolo).

Risoluzione dei problemi (avanzata)

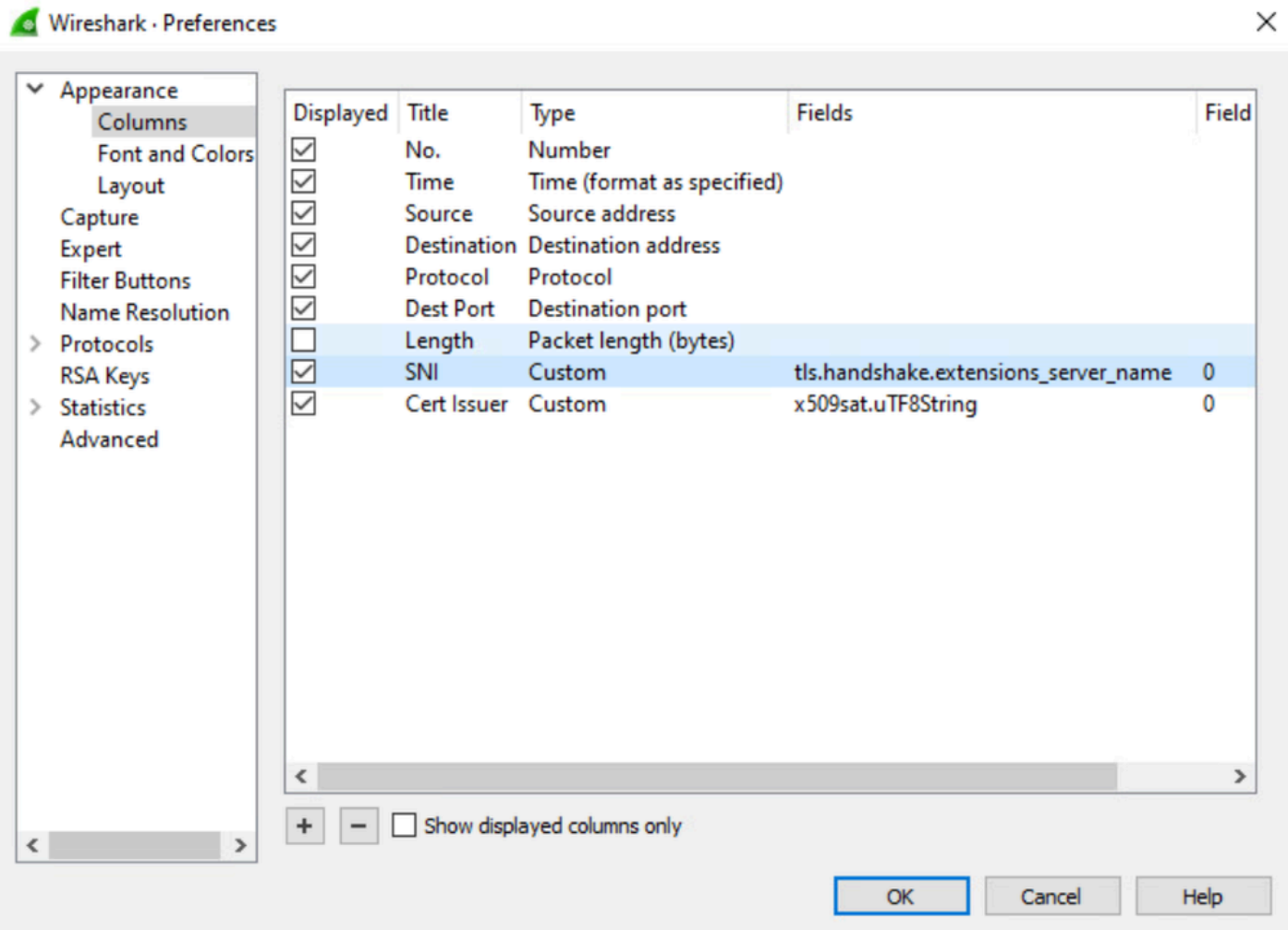
Le rimanenti istruzioni in questo articolo utilizzano le acquisizioni di pacchetti di Wireshark (www.wireshark.org) per la risoluzione dei problemi. Wireshark consente di identificare i domini utilizzati dalle applicazioni per l'implementazione di esclusioni personalizzate. Prima di iniziare, aggiungere le seguenti colonne personalizzate in Wireshark:

1. Scaricare Wireshark da [www.wireshark.org.](http://www.wireshark.org)

2. Selezionare Modifica > Preferenze > Colonne.

3. Creare colonne di tipo Personalizzato con i seguenti campi:

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



Per acquisire un pacchetto, attenersi alle seguenti istruzioni o vedere Acquisire il traffico di rete con Wireshark.

1. Eseguire Wireshark come amministratore.

2. Selezionare le interfacce di rete appropriate in Acquisizione > Opzioni.

- Per le distribuzioni PAC/tunnel, eseguire l'acquisizione sulla normale interfaccia di rete LAN.
- Per le implementazioni AnyConnect, eseguire l'acquisizione sull'interfaccia di rete LAN e sull'interfaccia di loopback.

3. Chiudere tutte le altre applicazioni ad eccezione di quella in cui si è verificato il problema.

4. Scaricare la cache DNS: `ipconfig /flushdns`

5. Avviare la cattura di Wireshark.

6. Riprodurre rapidamente il problema e fermare la cattura di Wireshark.

Identifica le esclusioni per il blocco del certificato

Il blocco del certificato viene applicato al client, pertanto il comportamento esatto e i passaggi di risoluzione differiscono per ogni applicazione. Nell'output di acquisizione, cercare i segnali rivelatori di un errore di connessione TLS:

- Una connessione TLS è stata chiusa o reimpostata rapidamente (RST o FIN).
- È in corso un tentativo ripetuto di connessione TLS.
- Il certificato per la connessione TLS è stato rilasciato da Cisco Umbrella ed è quindi in corso di decrittografia.

Questi filtri Wireshark di esempio possono aiutare a visualizzare i dettagli importanti delle connessioni TLS.

Tunnel/AnyConnect

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

Concatenamento PAC/proxy

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

In questo esempio, l'applicazione desktop DropBox è interessata dall'associazione del certificato quando si tenta di connettersi a client.dropbox.com.

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

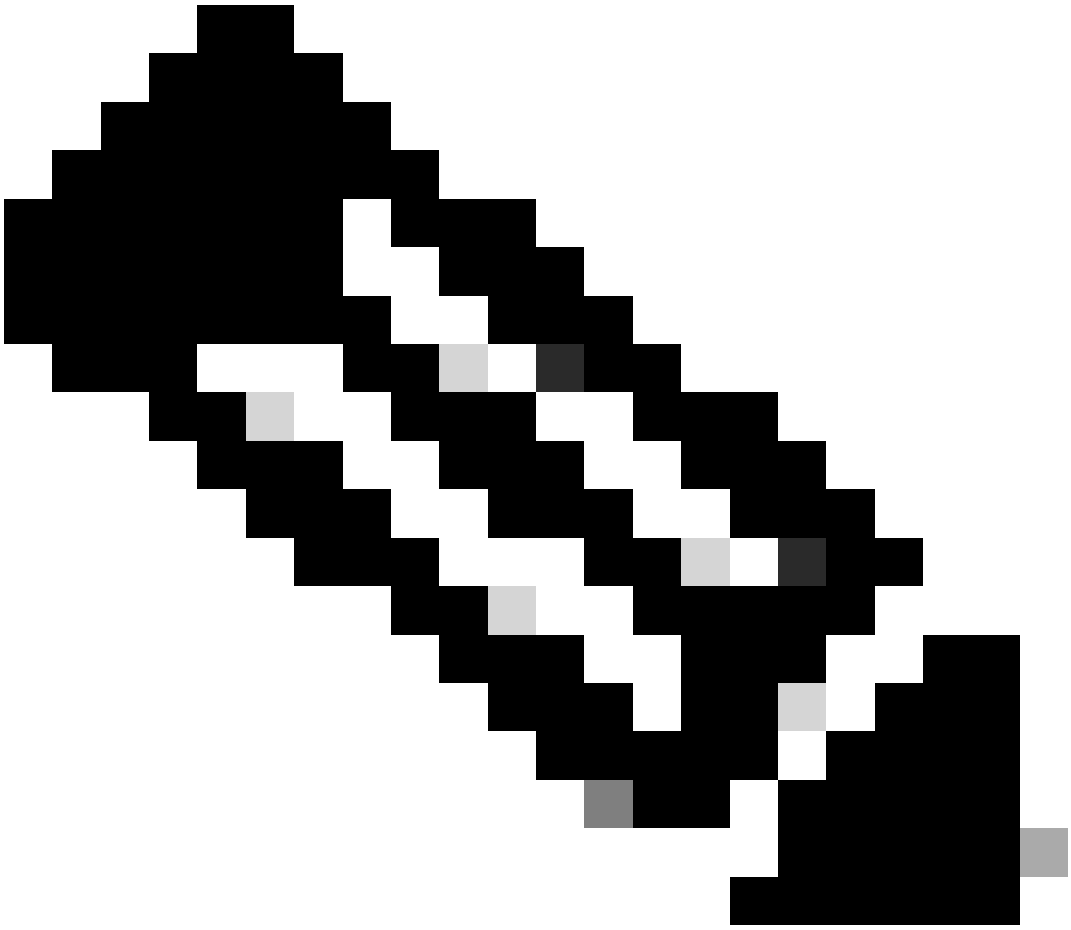
No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
281	43.038669	10.10.199.101	162.125.6.13	TCP	443		65148 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261120 Len=0
283	43.073849	162.125.6.13	10.10.199.101	TCP	65148		443 → 65148 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
287	43.083933	10.10.199.101	162.125.6.13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



Nota: Dopo aver aggiunto le esclusioni necessarie, è possibile ripetere questi passaggi

più volte per identificare tutte le destinazioni utilizzate dall'applicazione.

Identifica le esclusioni per le versioni TLS non compatibili

Cercare connessioni SSL/TLS che non utilizzano i protocolli TLS1.2+ obbligatori supportati da Umbrella SWG. Può includere protocolli legacy (TLS1.0 o versioni precedenti) o protocolli personalizzati personalizzati implementati da un'applicazione.

Questo filtro di esempio mostra i pacchetti di handshake TLS iniziali insieme alle query DNS.

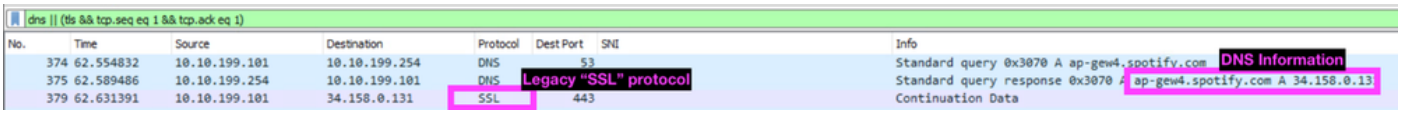
Tunnel/AnyConnect

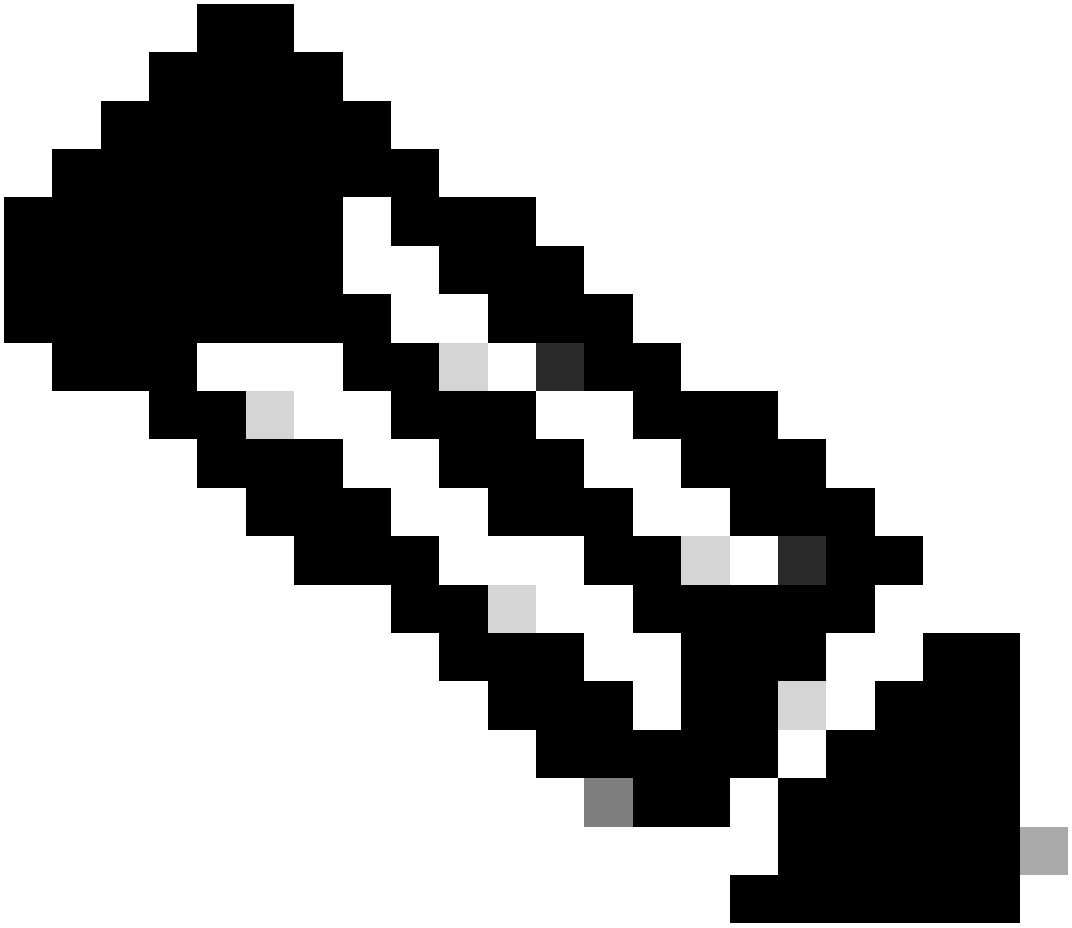
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

Concatenamento PAC/proxy

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

In questo esempio, l'applicazione desktop Spotify sta tentando di connettersi a ap-gew4.spotify.com utilizzando un protocollo "SSL" non standard o legacy che non può essere inviato tramite SWG.





Nota: Dopo aver aggiunto le esclusioni necessarie, è possibile ripetere questi passaggi più volte per identificare tutte le destinazioni utilizzate dall'applicazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).