Solução de problemas de aplicativos que não são navegadores no Umbrella

Contents

Introdução

Este documento descreve como solucionar problemas de aplicativos que não são navegadores no Cisco Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Este artigo explica as práticas recomendadas e as etapas de solução de problemas para configurar aplicativos que não são navegadores para funcionarem com o Umbrella Secure Web

Gateway. Na maioria dos casos, nenhuma alteração de configuração é necessária. No entanto, alguns aplicativos não funcionam bem com funções de segurança/inspeção (como Descriptografia SSL) e devem ser adicionadas exceções para fazer com que o aplicativo funcione com um proxy da Web. Isso se aplica ao Umbrella SWG, bem como a outras soluções de proxy da Web.

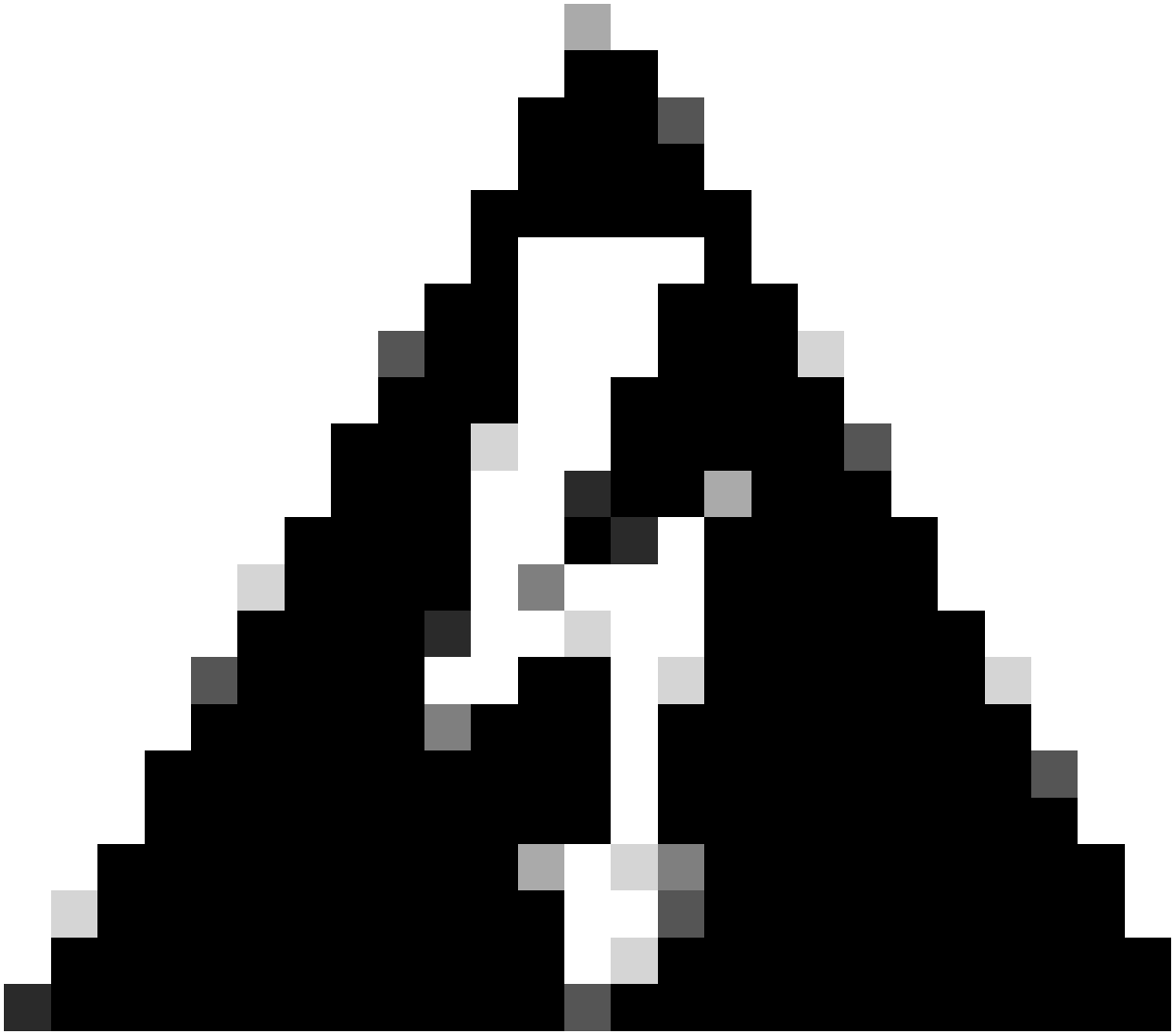
Isso é útil em circunstâncias em que a versão do site/navegador de um aplicativo funciona, mas a versão do desktop/móvel do aplicativo não.

Problemas de compatibilidade

Os aplicativos podem ser incompatíveis pelas seguintes razões:

Instalação da CA raiz do Umbrella	A CA raiz do Cisco Umbrella sempre deve ser confiável para conexões TLS sem erros. • Solução: Para aplicativos que não são da Web, verifique se a CA raiz do guarda-chuva Cisco é confiável no armazenamento de certificados do sistema/computador local.
Fixação de Certificado	A Fixação de Certificado (PKP) é quando o aplicativo espera receber uma folha precisa (ou certificado CA) para validar o handshake TLS. O aplicativo não pode aceitar um certificado gerado por um proxy da Web e não é compatível com funções de Descriptografia SSL. • Solução: Ignorar o Aplicativo ou Domínio da Descriptografia SSL usando uma Lista de Descriptografia Seletiva (consulte Aviso após a tabela) Mais detalhes sobre os aplicativos conhecidos por serem afetados pela fixação de certificado estão disponíveis aqui: Fixação de chave pública/Fixação de certificado
Suporte à versão TLS	O aplicativo pode usar uma versão TLS/codificação mais antiga que não é suportada pelo SWG por motivos de segurança. • Solução: Evite que o tráfego seja enviado para o Umbrella usando o recurso Domínios externos (PAC / AnyConnect) ou exclusões de VPN (Túnel) (consulte Aviso após a tabela).
Protocolo não-Web	Alguns aplicativos usam protocolos não-http(s), mas ainda enviam esses dados por portas da Web comuns interceptadas pelo SWG. O SWG não consegue entender esse tráfego. • Solução: Consulte o Fornecedor do aplicativo para determinar os endereços de destino/intervalos de IP usados pelo software. Este software precisa ser excluído do SWG usando External Domains (PAC /

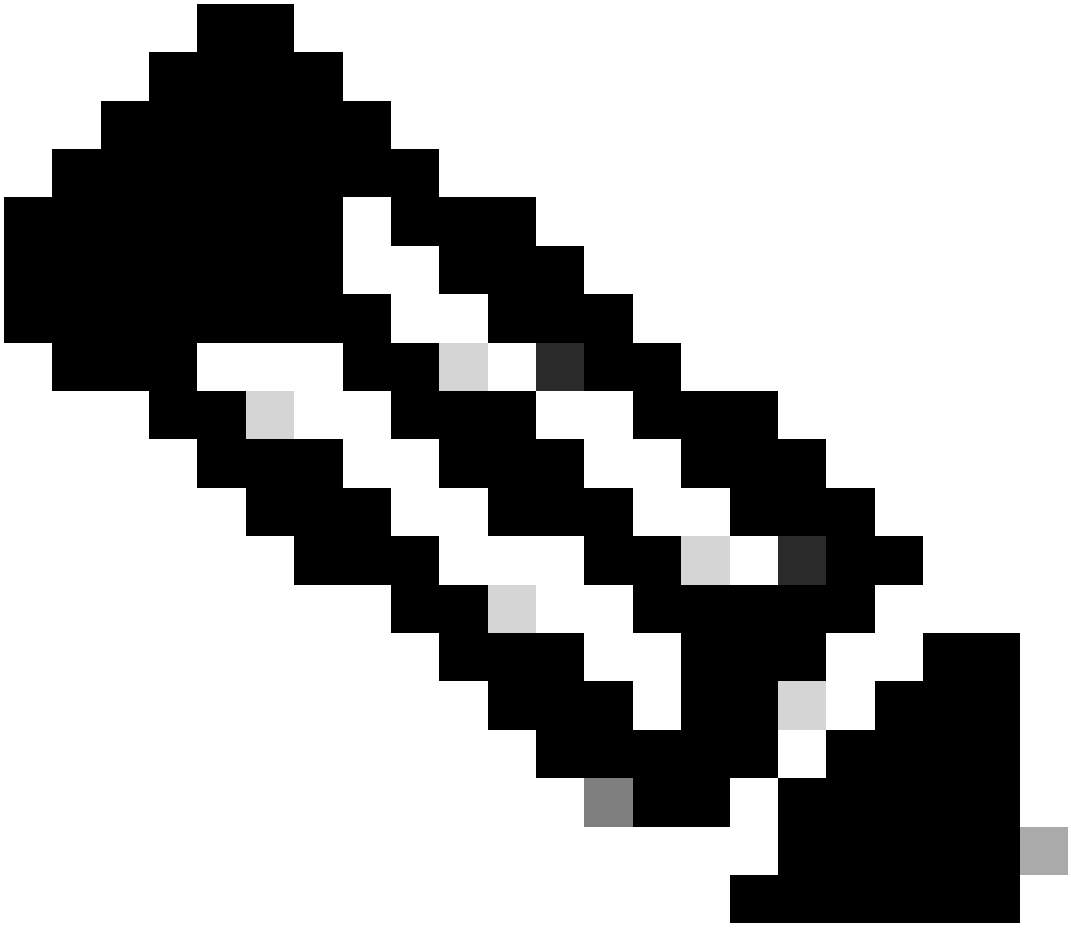
	AnyConnect) ou VPN Exclusions (Tunnel) (consulte Warning após a tabela).
Autenticação SAML	A maioria dos aplicativos que não são navegadores não consegue executar a autenticação SAML. O Umbrella não desafia aplicativos que não sejam navegadores para SAML e, portanto, as políticas de filtragem baseadas em Usuário/Grupo não podem ser correspondentes. • Solução: Habilite o recurso IP Surrogates para que as informações do usuário possam ser armazenadas em cache para uso com aplicativos que não sejam navegadores. • Alternativa: Permitir o Aplicativo/Domínio em uma regra da Web com base nas Identidades da Rede ou do Túnel (não usuários/grupos).
Solicitações de Intervalo HTTP	Alguns aplicativos usam solicitações HTTP "Byte-Range" ao fazer download de dados; o que significa que apenas uma pequena parte do arquivo é baixada de cada vez. Essas solicitações são desabilitadas por motivos de segurança no SWG, pois essa técnica também pode ser usada para ignorar a detecção de antivírus. • Solução (HTTPS): Ignore o aplicativo ou domínio da descriptografia SSL* no Umbrella usando listas de descriptografia seletivas. • Solução (HTTP): Ignore o aplicativo ou domínio da varredura de antivírus* usando uma regra da Web com a opção Sobrepor segurança. • Alternativa: Entre em contato com o suporte Umbrella se desejar que as solicitações de intervalo sejam habilitadas por padrão* para sua organização.
Compatibilidade explícita de proxy	Alguns aplicativos não respeitam as configurações de proxy do sistema (por exemplo, arquivos PAC) e geralmente não são compatíveis com proxies da Web explícitos. Esses aplicativos não fazem o roteamento através do Umbrella SWG em uma implantação de arquivo PAC. • Solução: O aplicativo deve ser permitido através do firewall de rede local. Consulte o fornecedor do aplicativo para obter detalhes sobre destinos/portas a serem permitidos.



aviso: A criação dessas exceções pode desabilitar as funções de inspeção de segurança, incluindo verificação de antivírus, verificação de DLP, Controles de usuário, Controle de tipo de arquivo e inspeção de URL. Só faça isso se você estiver feliz em confiar na fonte desses arquivos. A necessidade comercial do aplicativo deve ser avaliada em relação ao impacto de segurança da desativação desses recursos.

Aplicativos Microsoft 365

O recurso de compatibilidade do Microsoft 365 exclui automaticamente vários domínios da Microsoft das funções de decodificação SSL e aplicação de políticas. Este recurso pode ser habilitado para resolver problemas com a versão Desktop dos aplicativos da Microsoft. Para obter mais informações, consulte Gerenciar configurações globais.

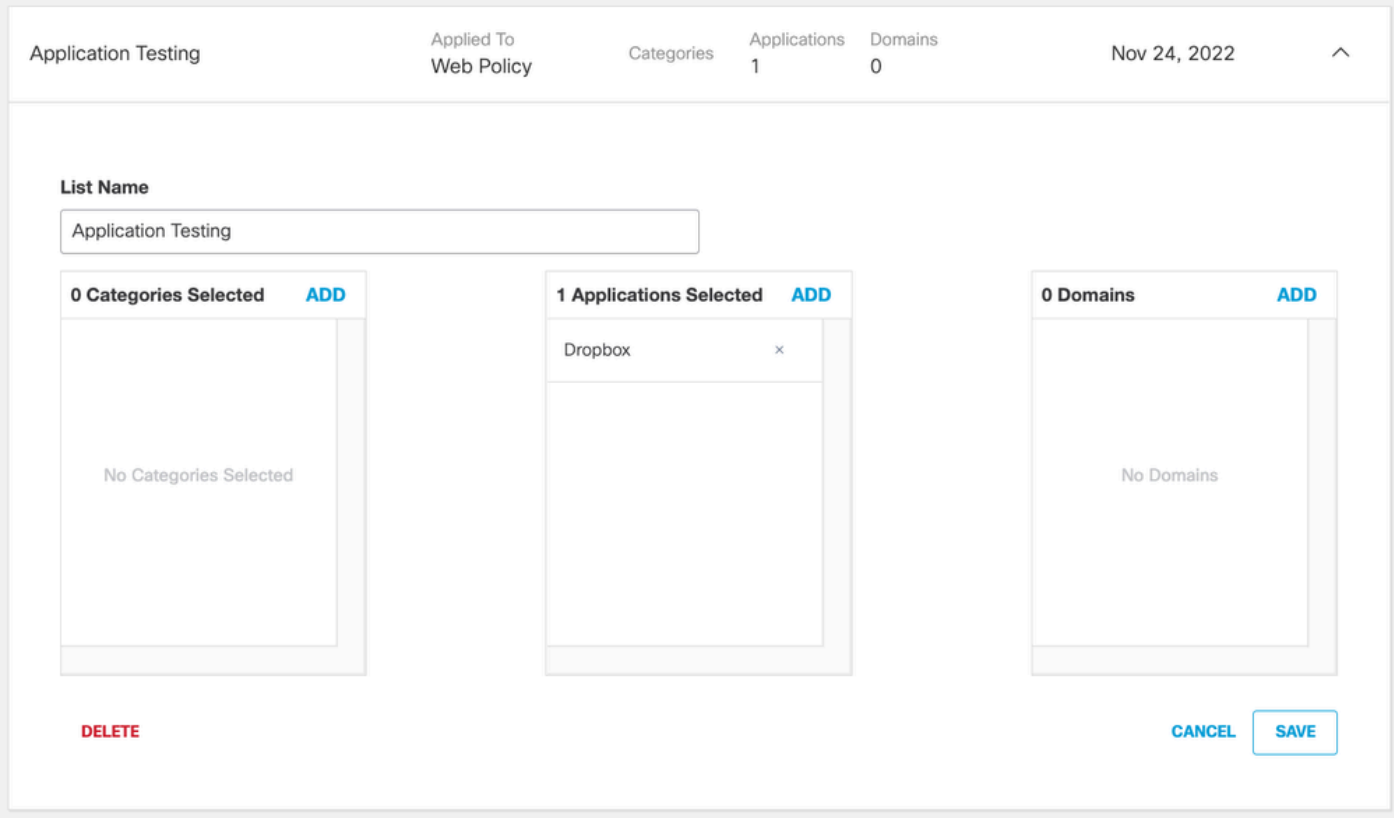


Note: O recurso de Compatibilidade do Microsoft 365 não exclui todos os domínios da Microsoft. O Umbrella usa as recomendações da Microsoft para a lista de domínios que devem ser excluídos da filtragem. Para obter mais informações, consulte Novas categorias de endpoint do Office365.

Desvio de Fixação de Certificado

A Fixação de Certificado (PKP) é uma causa comum de problemas de compatibilidade de aplicativos. A Cisco fornece uma lista abrangente de aplicativos nomeados que podem ser configurados para ignorar a descriptografia SSL para solucionar o problema. A descriptografia seletiva pode ser configurada em Policies > Selective Decryption Lists.

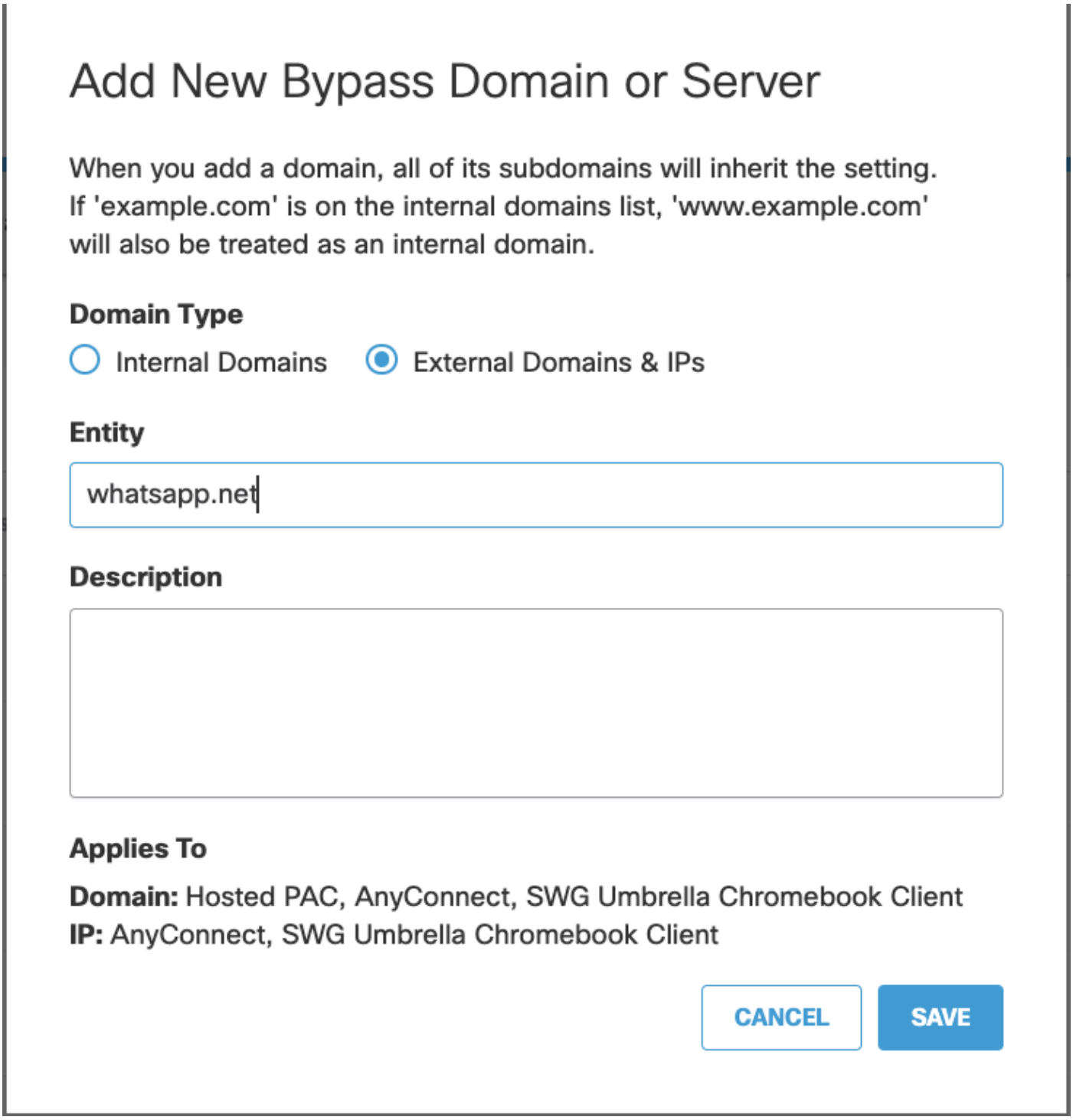
Na maioria dos casos, o administrador pode resolver problemas de fixação de certificado simplesmente excluindo o aplicativo por seu nome. Isso significa que esses problemas podem ser resolvidos sem a necessidade de aprender ou manter listas de domínios.



Como alternativa, os aplicativos podem ser ignorados com base no domínio de destino/endereço IP. Entre em contato com o fornecedor do aplicativo para determinar a lista aplicável de domínios/IPs ou consulte Identificar exclusões para fixação de certificado.

Desvio de compatibilidade TLS

As versões TLS legadas ou personalizadas são uma causa comum de problemas de compatibilidade de aplicativos. Esses problemas podem ser resolvidos excluindo o tráfego do Umbrella em Implantações > Gerenciamento de domínio > Domínios externos e IPs. Em uma implantação de túnel, o tráfego só pode ser excluído adicionando exceções em sua configuração de VPN.



Entre em contato com o fornecedor do aplicativo para determinar a lista aplicável de domínios/IPs a serem excluídos ou consulte "Identificar exclusões para versões TLS incompatíveis" (mais adiante neste artigo).

Solução de problemas (Avançado)

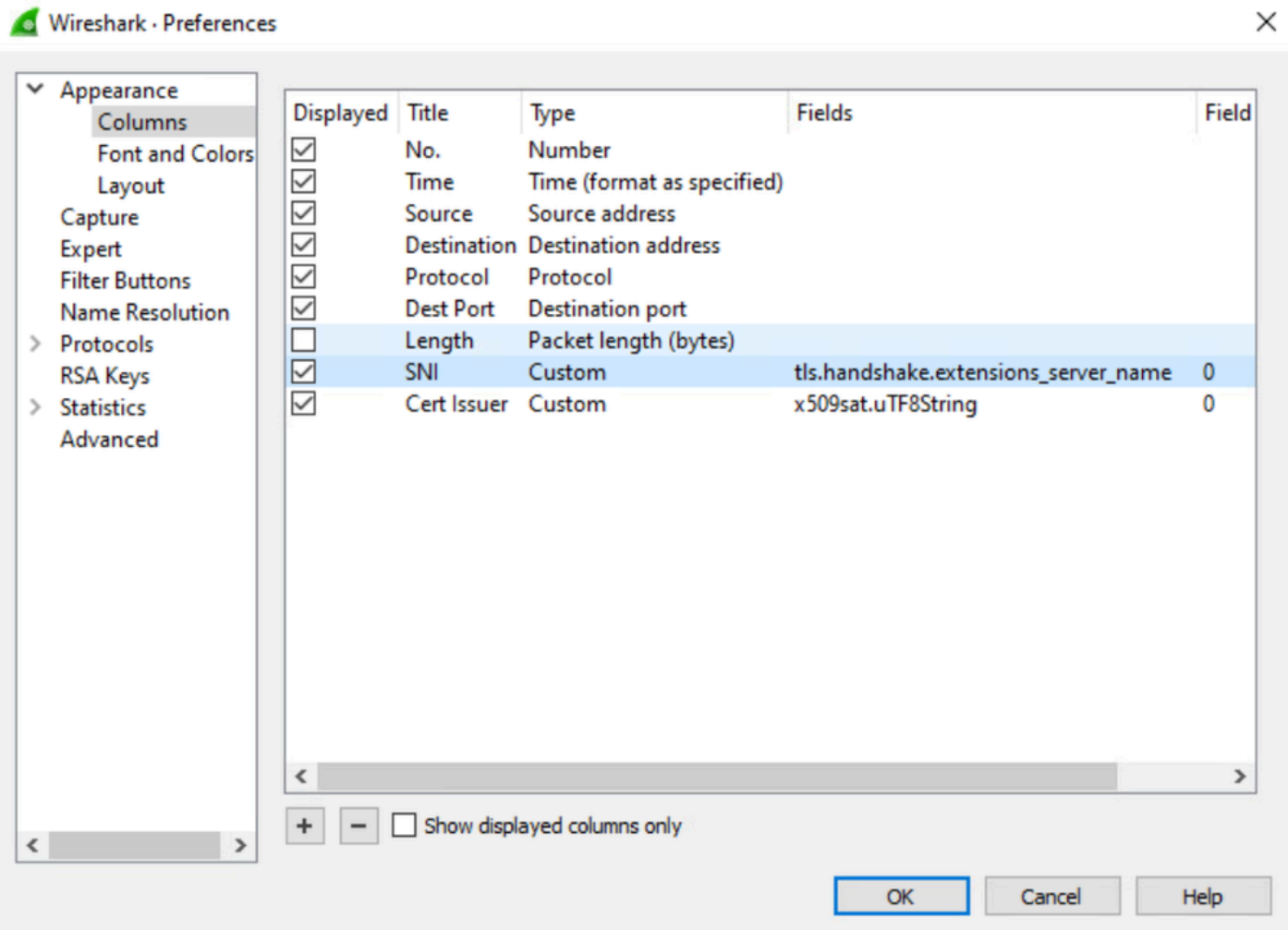
As instruções restantes neste artigo usam as capturas de pacotes do Wireshark (www.wireshark.org) para fins de solução de problemas. O Wireshark pode ajudar a identificar quais domínios são usados por aplicativos para ajudar na implementação de exclusões personalizadas. Antes de iniciar, adicione estas colunas personalizadas no Wireshark:

1. Baixe o Wireshark de [www.wireshark.org.](http://www.wireshark.org)

2. Vá para Editar > Preferências > Colunas.

3. Crie colunas do tipo Personalizado com estes campos:

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



Para executar uma captura de pacote, siga estas instruções ou consulte Capturar Tráfego de Rede com o Wireshark.

1. Execute o Wireshark como Administrador.

2. Selecione as interfaces de rede relevantes em Capturar > Opções.

- Para implantações de PAC/túnel, capture em sua interface de rede LAN normal.
- Para implantações do AnyConnect, capture em sua interface de rede LAN e na interface de loopback.

3. Feche todos os outros aplicativos, exceto o aplicativo com problema.

4. Limpe o cache DNS: `ipconfig /flushdns`

5. Inicie a captura Wireshark.

6. Replique rapidamente o problema e pare a captura Wireshark.

Identificar Exclusões para Fixação de Certificado

A fixação do certificado é aplicada no cliente, o que significa que o comportamento exato e as etapas de resolução diferem para cada aplicativo. Na saída da captura, procure sinais de aviso de que uma conexão TLS está falhando:

- Uma conexão TLS está sendo rapidamente fechada ou redefinida (RST ou FIN).
- Uma conexão TLS está sendo repetidamente repetida.
- O certificado para a conexão TLS está sendo emitido pelo Cisco Umbrella e, portanto, está sendo descriptografado.

Esses filtros Wireshark de exemplo podem ajudar a visualizar os detalhes importantes das conexões TLS.

Túnel / AnyConnect

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

Encadeamento de Proxy/PAC

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

Neste exemplo, o aplicativo de área de trabalho DropBox é afetado pela fixação de certificado ao tentar se conectar a client.dropbox.com.

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

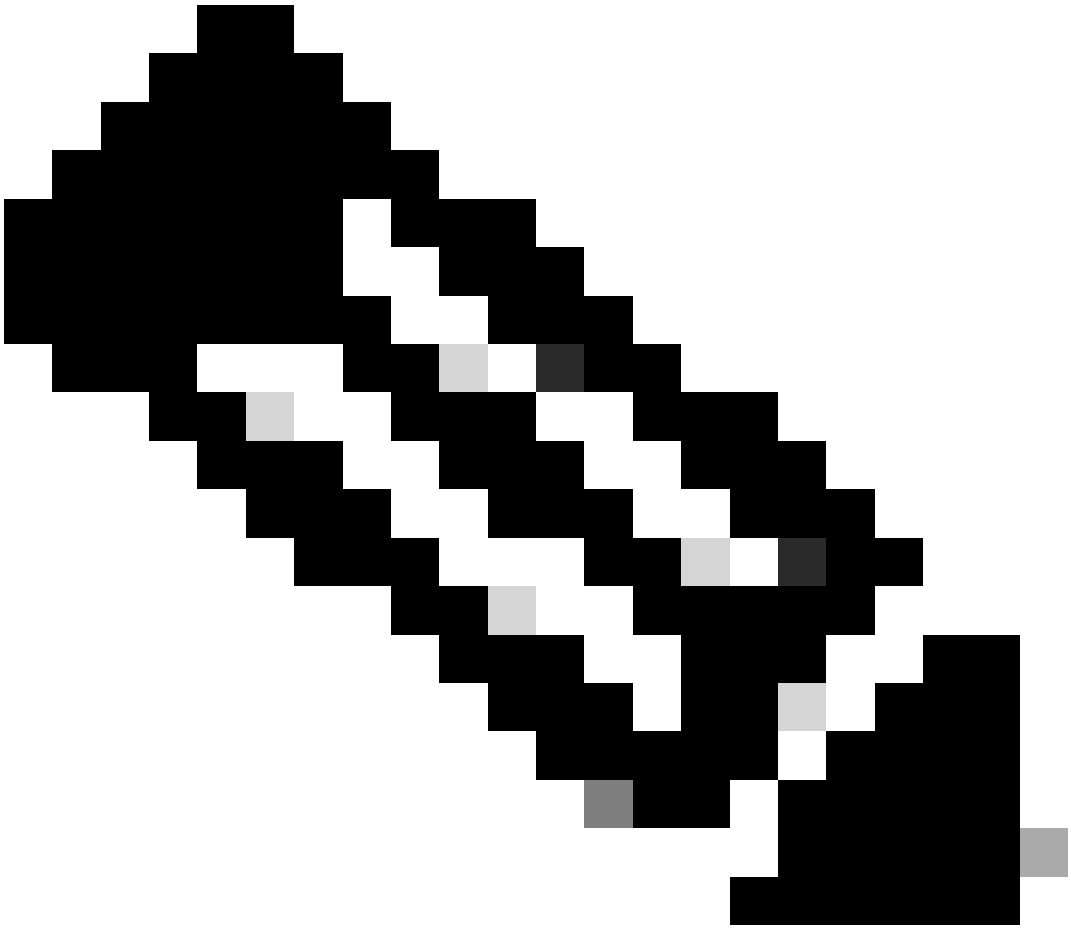
No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
281	43.038669	10.10.199.101	162.125.6.13	TCP	443		65148 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261120 Len=0
283	43.073849	162.125.6.13	10.10.199.101	TCP	65148		443 → 65148 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
287	43.083933	10.10.199.101	162.125.6.13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



Note: Depois de adicionar as exclusões necessárias, você pode repetir essas etapas

várias vezes para identificar todos os destinos usados pelo aplicativo.

Identificar exclusões para versões TLS incompatíveis

Procure conexões SSL/TLS que não usem os protocolos TLS1.2+ obrigatórios suportados pelo Umbrella SWG. Isso pode incluir protocolos legados (TLS1.0 ou anterior) ou protocolos personalizados sob medida implementados por uma aplicação.

Este filtro de exemplo mostra os pacotes de handshake TLS iniciais junto com as consultas DNS.

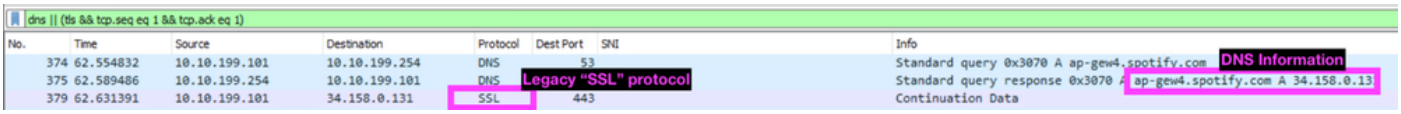
Túnel / AnyConnect

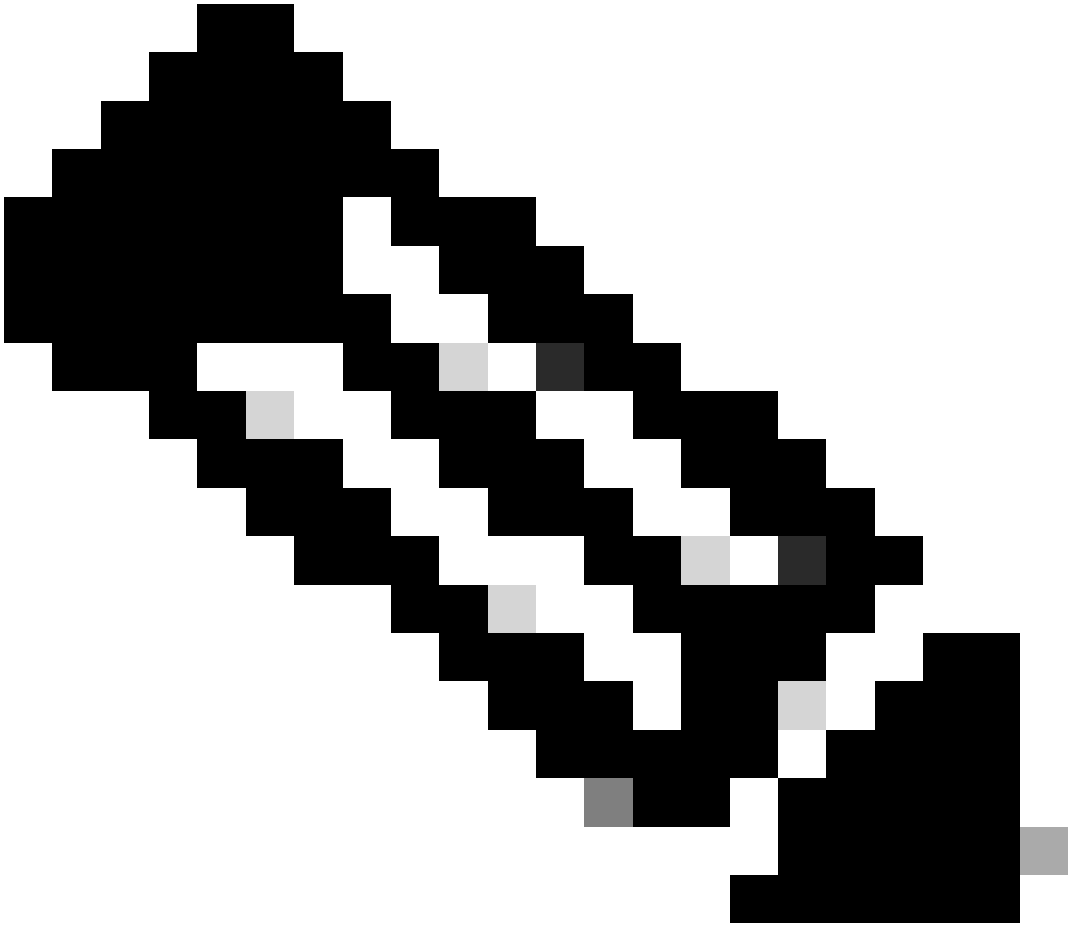
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

Encadeamento de Proxy/PAC

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

Neste exemplo, o aplicativo de desktop Spotify está tentando se conectar ao ap-gew4.spotify.com usando um protocolo "SSL" legado ou não padrão que não pode ser enviado via SWG.





Note: Depois de adicionar as exclusões necessárias, você pode repetir essas etapas várias vezes para identificar todos os destinos usados pelo aplicativo.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.