

Dominios externos en el módulo SWG de Secure Client

Contenido

[Introducción](#)

[Overview](#)

[¿Por qué funciona de esta manera?](#)

[¿Por qué me importa esto?](#)

[¿Cómo se solucionan los problemas de este proceso?](#)

[Ejemplo de entradas de registro KDF](#)

Introducción

Este documento describe cómo el módulo Secure Web Gateway (SWG) de Cisco Secure Client (CSC) (anteriormente AnyConnect) aplica la lista de dominios externos configurada y las implicaciones de esto.



Nota: Cisco anunció el fin del ciclo de vida de Cisco AnyConnect en 2023 y de Umbrella Roaming Client en 2024. Muchos clientes de Cisco Umbrella ya se están beneficiando de la migración a Cisco Secure Client, por lo que le animamos a que inicie la migración lo antes posible para disfrutar de una mejor experiencia de roaming. Obtenga más información en este artículo de Knowledge Base: [¿Cómo instalo Cisco Secure Client con el módulo Umbrella?](#)

Overview

La [lista de dominios externos de Cisco Umbrella](#) acepta tanto dominios como direcciones IP. Sin embargo, en ambos casos, el módulo CSC SWG solo puede aplicar la decisión de exclusión basada en la dirección IP.

A nivel general, el mecanismo que utiliza el módulo SWG para identificar el tráfico a los dominios de la lista de dominios externos es el siguiente:

- El módulo SWG supervisa las búsquedas de DNS del equipo cliente para identificar las

búsquedas de los dominios de la lista de dominios externos

- Estos dominios y sus direcciones IP correspondientes se agregan a una caché DNS local
- La decisión de entonces omitir SWG se aplica a cualquier tráfico destinado a una IP que corresponde a un dominio externo dentro de la memoria caché DNS local. La decisión no se basa en el dominio utilizado en la solicitud HTTP.

¿Por qué funciona de esta manera?

El módulo CSC SWG funciona en la capa 3/capa 4, por lo que solo tiene visibilidad de los encabezados TCP/IP que almacenan los detalles de conexión de 5 tuplas (IP de destino:puerto, IP de origen:puerto y protocolo) en los que puede basar sus reglas de omisión del tráfico.

Por lo tanto, para las derivaciones basadas en dominios, CSC SWG requiere una forma de traducir los dominios de la lista a direcciones IP que luego puedan coincidir con el tráfico en la máquina cliente. Para este fin, genera la memoria caché DNS a partir de las búsquedas DNS enviadas desde el cliente, la memoria caché DNS muestra la dirección IP correspondiente a los dominios de la lista de dominios externos

La decisión de omitir SWG se aplica entonces al tráfico interceptado (de forma predeterminada 80/443) destinado a estas direcciones IP.

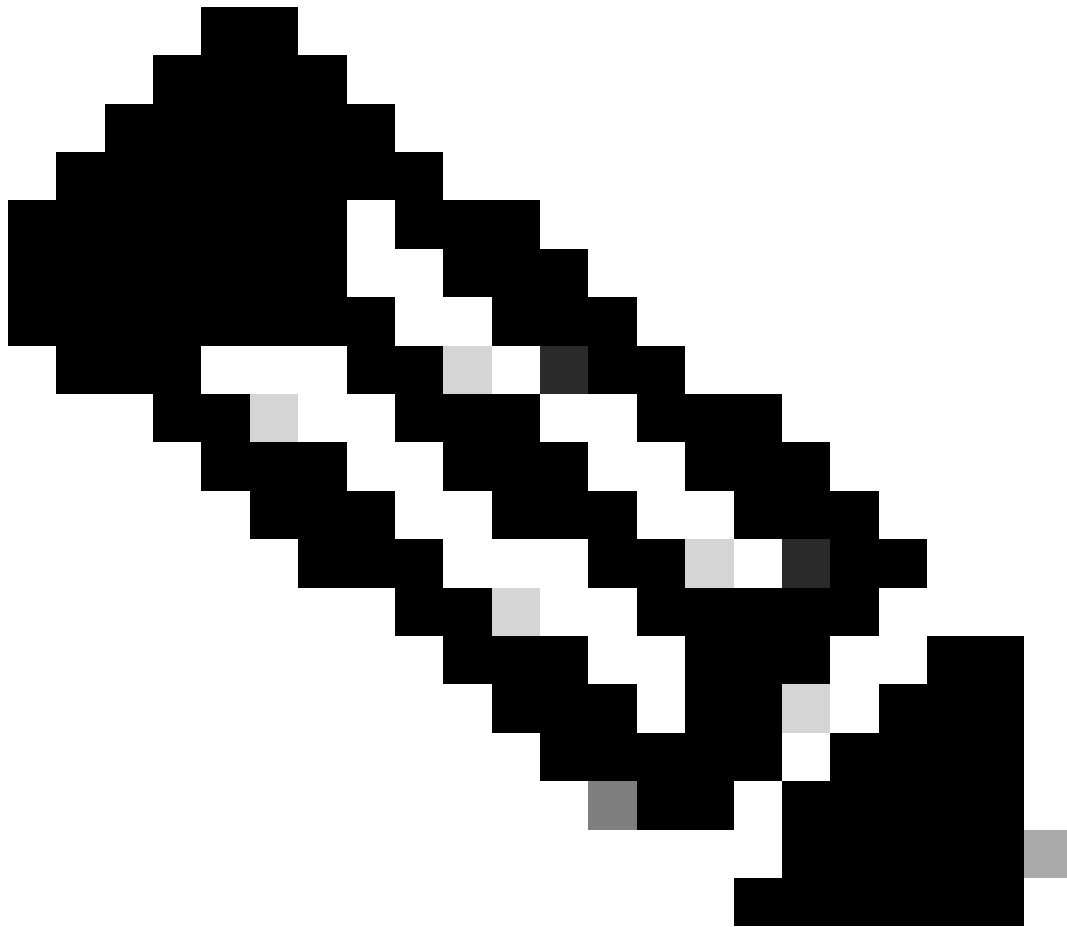
¿Por qué me importa esto?

Hay un par de problemas comunes que esto puede causar:

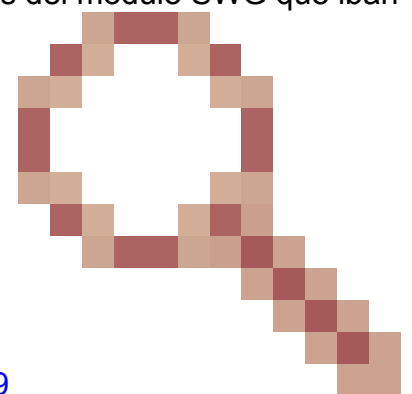
1. Dado que la decisión de desvío se basa en última instancia en una IP, el tráfico de otros dominios que comparten la misma IP también se omite en Cisco Umbrella, lo que hace que el cliente observe el tráfico inesperado que egresa directamente del cliente y no tenga la política SWG aplicada o que aparezca en la búsqueda de actividad.
2. Si por alguna razón el módulo SWG no puede ver la búsqueda de DNS para el dominio (como en, hay una entrada de host local para el dominio), entonces la IP no se agrega a la memoria caché y, por lo tanto, el tráfico se envía inesperadamente a SWG.



Nota: El controlador KDF sólo supervisa las búsquedas de DNS UDP. Si por alguna razón la búsqueda de DNS se realiza a través de TCP, entonces la IP no se agrega a la memoria caché y el dominio externo no se aplica. Esto se publica en [Búsqueda de errores de Cisco](#).



Nota: Hemos corregido un problema con los dominios externos del módulo SWG que iban



a Umbrella cuando DNS se resolvía sobre TCP ([CSCwe48679](#)) (Windows y MacOS) en Cisco Secure Client 5.1.4.74 (MR4)

¿Cómo se solucionan los problemas de este proceso?

El proceso del módulo SWG que observa las búsquedas de DNS, agrega entradas a la memoria caché de DNS y aplica la acción de omisión al tráfico destinado a las IP se puede seguir en los

registros de KDF. Esto requiere que el registro de KDF esté habilitado y solo se pueda habilitar durante un corto período de tiempo mientras se resuelve el problema debido a la verbosidad de los registros.

Ejemplo de entradas de registro KDF

Búsqueda DNS de un dominio que se agrega a la caché DNS:

```
00000283 11.60169029 acsock 11:34:57.9474385 (CDnsCachePluginImp::notify_recv): acquired safe buffer fo
00000284 11.60171318 acsock 11:34:57.9474385 (CDnsCacheMgr::AddResponseToCache): add to cache (www.club
00000285 11.60171986 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000286 11.60172462 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000287 11.60172939 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000288 11.60173225 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCache): Added entry (www.club386.com,
00000289 11.60173607 acsock 11:34:57.9474385 (CDnsCacheMgr::AddResponseToCache): add to cache (www.club
```

Conexión HTTPS observada, dominio no incluido en la lista de dominios externos, solicitud enviada mediante SWG:

```
00000840 10.69207287 acsock 12:13:50.0741618 (CNvmPlugin::notify_bind): called
00000841 10.69207764 acsock 12:13:50.0741618 (CNvmPlugin::notify_bind): nvm: cookie 0x0000000000000000:
00000842 10.69208336 acsock 12:13:50.0741618 (CSocketScanSafePluginImp::notify_bind): websec cookie FFF
00000843 10.69208908 acsock 12:13:50.0741618 (COpenDnsPluginImp::notify_bind):.opendns cookie FFFFD30F9
00000844 10.69209576 acsock 12:13:50.0741618 (CNvmPlugin::notify_send): nvm: cookie 0000000000000000: p
00000845 10.69211483 acsock 12:13:50.0741618 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by ad
00000846 10.69221306 acsock 12:13:50.0741618 (CSocketMultiplexor::notify_stream_v4): recv: protocol 6,
00000847 10.69222069 acsock 12:13:50.0741618 (CNvmPlugin::notify_recv): nvm: cookie 0000000000000000: p
```

Conexión HTTPS observada, entrada para IP encontrada en caché, acción de omisión aplicada:

```
00003163 9.63360023 acsock 15:33:48.7197706 (CNvmPlugin::notify_bind): called
00003164 9.63360405 acsock 15:33:48.7197706 (CNvmPlugin::notify_bind): nvm: cookie 0x0000000000000000:
00003165 9.63360882 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_bind): websec cookie FFFF
00003166 9.63361359 acsock 15:33:48.7197706 (COpenDnsPluginImp::notify_bind):.opendns cookie FFFF8C02C8
00003167 9.63364792 acsock 15:33:48.7197706 (CNvmPlugin::notify_connect): called
00003168 9.63365269 acsock 15:33:48.7197706 (CNvmPlugin::notify_connect): nvm: cookie 0x0000000000000000
00003169 9.63366127 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_connect): websec cookie F
00003170 9.63367081 acsock 15:33:48.7197706 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by add
00003171 9.63367558 acsock 15:33:48.7197706 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by add
00003172 9.63370323 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::getFQDN_check_domain_exception):
00003173 9.63370800 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::evaluate_rules): domain name fou
00003174 9.63371372 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_connect): cookie FFFF8C02
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).