Understand External Domains in the Secure Client SWG Module

Contents

Introduction

Overview

Why does it function in this way?

Why does this matter to me?

How can I troubleshoot this process?

Example KDF log entries

Introduction

This document describes how the Cisco Secure Client (CSC) Secure Web Gateway (SWG) module applies the configured external domains list.



Note: Cisco announced the End-of-Life of Cisco AnyConnect in 2023 and the Umbrella Roaming Client in 2024. Many Cisco Umbrella users are already benefiting from migrating to Cisco Secure Client, and you are encouraged to begin migration as soon as possible to get a better roaming experience. Read more in this Knowledge Base article: How do I install Cisco Secure Client with the Umbrella Module?

Overview

The Cisco Umbrella External Domains list accepts both domains and IP addresses. However, in both cases, the CSC (formerly AnyConnect) SWG module can only apply the exclusion decision based on IP address.

At a high level, the mechanism that the SWG module uses to identify traffic to domains on the External Domains list is as follows:

- The SWG module monitors DNS lookups from the client machine to identify lookups of the domains on the external domains list
- These domains and their corresponding IP addresses are added to a local DNS cache
- The decision to then bypass SWG is then applied to any traffic destined for an IP that corresponds to an External Domain within the local DNS cache. The decision is not based on the domain used within the HTTP Request.

Why does it function in this way?

The CSC SWG module operates at Layer3/Layer4, as such it only has visibility into the TCP/IP headers storing the 5-Tuple connection details (DestinationIP:Port, SourceIP:Port and Protocol) on which it can base its traffic bypass rules.

Therefore, for domain-based bypasses, CSC SWG requires a way of translating the domains in the list to IP addresses which it can then match to the traffic on the client machine. To this end, it generates the DNS cache from the DNS lookups sent from the client, the DNS cache lists the IP address corresponding to the domains on the external domains list

The decision to bypass SWG is then applied to intercepted traffic (by default 80/443) destined to these IP addresses.

Why does this matter to me?

There are a couple of common issues that this can cause:

1. Given the bypass decision is ultimately based on an IP, traffic for other domains that share the same IP also gets bypassed from Cisco Umbrella, resulting in you observing unexpected traffic egressing from the client directly and not having SWG policy applied or appearing in Activity Search.
2. If for any reason the SWG module cannot see the DNS lookup for the domain (as in, there is a localhost entry for the domain), then the IP is not added to the cache, and therefore the traffic is unexpectedly sent to SWG.



Note: The KDF driver only monitors UDP DNS lookups. If for any reason the DNS lookup is performed via TCP, then the IP is not added to the cache and the external domain is not applied. This is published in Cisco's Bug Search.



Note: We have fixed an issue with the SWG module External domains going to Umbrella when DNS resolved over TCP (CSCxxYYYYY) (Windows and MacOS) in Cisco Secure Client 5.1.4.74 (MR4)

How can I troubleshoot this process?

The process of the SWG module observing the DNS lookups, adding entries to the DNS cache, and applying the bypass action to traffic destined for the IPs can be followed in the KDF logs. This requires that KDF logging is enabled and can only be enabled for a short period while troubleshooting due to the verbosity of the logs.

Example KDF log entries

DNS lookup of a domain being added to the DNS cache:

```
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
```

HTTPS connection observed, domain not on external domains list, request sent via 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: pa
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: pa
```

HTTPS connection observed, entry for IP found in cache, bypass action applied:

```
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 0x000000000000000
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
```