Comprendre les domaines externes dans le module Secure Client SWG

Table des matières

Introduction

Aperçu

Pourquoi fonctionne-t-il de cette manière ?

Pourquoi est-ce important pour moi ?

Comment puis-je résoudre ce problème ?

- Exemple d'entrées de journal KDF

Introduction

Ce document décrit comment le module Cisco Secure Client (CSC) Secure Web Gateway (SWG) applique la liste de domaines externes configurée.



Remarque : Cisco a annoncé la fin de vie de Cisco AnyConnect en 2023 et du client d'itinérance Umbrella en 2024. De nombreux utilisateurs de Cisco Umbrella bénéficient déjà de la migration vers Cisco Secure Client et nous vous encourageons à commencer la migration dès que possible pour bénéficier d'une meilleure expérience d'itinérance. Pour en savoir plus, lisez cet article de la Base de connaissances : Comment puis-je installer Cisco Secure Client avec le module Umbrella ?

Aperçu

La liste des domaines externes Cisco Umbrella accepte les domaines et les adresses IP. Cependant, dans les deux cas, le module CSC (anciennement AnyConnect) SWG peut uniquement appliquer la décision d'exclusion basée sur l'adresse IP.

À un niveau élevé, le mécanisme utilisé par le module SWG pour identifier le trafic vers les domaines de la liste des domaines externes est le suivant :

- Le module SWG surveille les recherches DNS à partir de la machine client pour identifier les recherches des domaines de la liste des domaines externes
- Ces domaines et leurs adresses IP correspondantes sont ajoutés à un cache DNS local

- La décision de contourner ensuite SWG est ensuite appliquée à tout trafic destiné à une adresse IP qui correspond à un domaine externe dans le cache DNS local. La décision n'est pas basée sur le domaine utilisé dans la requête HTTP.

Pourquoi fonctionne-t-il de cette manière ?

Le module CSC SWG fonctionne au niveau de la couche 3/couche 4, de sorte qu'il n'a de visibilité que sur les en-têtes TCP/IP stockant les détails de la connexion à 5-tuple (DestinationIP:Port, SourceIP:Port et Protocol) sur lesquels il peut baser ses règles de contournement du trafic.

Par conséquent, pour les contournements basés sur les domaines, CSC SWG nécessite un moyen de traduire les domaines de la liste en adresses IP qu'il peut ensuite faire correspondre au trafic sur l'ordinateur client. A cet effet, il génère le cache DNS à partir des recherches DNS envoyées par le client, le cache DNS répertorie l'adresse IP correspondant aux domaines de la liste des domaines externes

La décision de contourner SWG est ensuite appliquée au trafic intercepté (par défaut 80/443) destiné à ces adresses IP.

Pourquoi est-ce important pour moi ?

Il y a quelques problèmes courants que cela peut causer :

1. Étant donné que la décision de contournement est finalement basée sur une adresse IP, le trafic pour d'autres domaines qui partagent la même adresse IP est également contourné à partir de Cisco Umbrella, ce qui vous permet d'observer le trafic inattendu sortant directement du client et de ne pas avoir de stratégie SWG appliquée ou apparaissant dans Activity Search.
2. Si, pour une raison quelconque, le module SWG ne peut pas voir la recherche DNS pour le domaine (comme dans, il y a une entrée localhost pour le domaine), alors l'IP n'est pas ajoutée au cache, et par conséquent le trafic est envoyé de manière inattendue à SWG.



Remarque : Le pilote KDF surveille uniquement les recherches DNS UDP. Si, pour une raison quelconque, la recherche DNS est effectuée via TCP, l'adresse IP n'est pas ajoutée au cache et le domaine externe n'est pas appliqué. Ceci est publié dans la recherche de bogues de Cisco.



Remarque : Nous avons résolu un problème avec le module SWG Domaines externes allant à Umbrella lorsque DNS a résolu sur TCP (CSCxxYYYY) (Windows et MacOS) dans Cisco Secure Client 5.1.4.74 (MR4)

Comment puis-je résoudre ce problème ?

Le processus du module SWG consistant à observer les recherches DNS, à ajouter des entrées au cache DNS et à appliquer l'action de contournement au trafic destiné aux adresses IP peut être suivi dans les journaux KDF. Cela nécessite que la journalisation KDF soit activée et ne puisse être activée que pendant une courte période lors du dépannage en raison du niveau de détail des journaux.

Exemple d'entrées de journal KDF

Recherche DNS d'un domaine ajouté au cache 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
```

Connexion HTTPS observée, domaine ne figurant pas dans la liste des domaines externes, requête envoyée 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: 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
```

Connexion HTTPS observée, entrée pour IP trouvée dans le cache, action de contournement appliquée :

```
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
```

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.