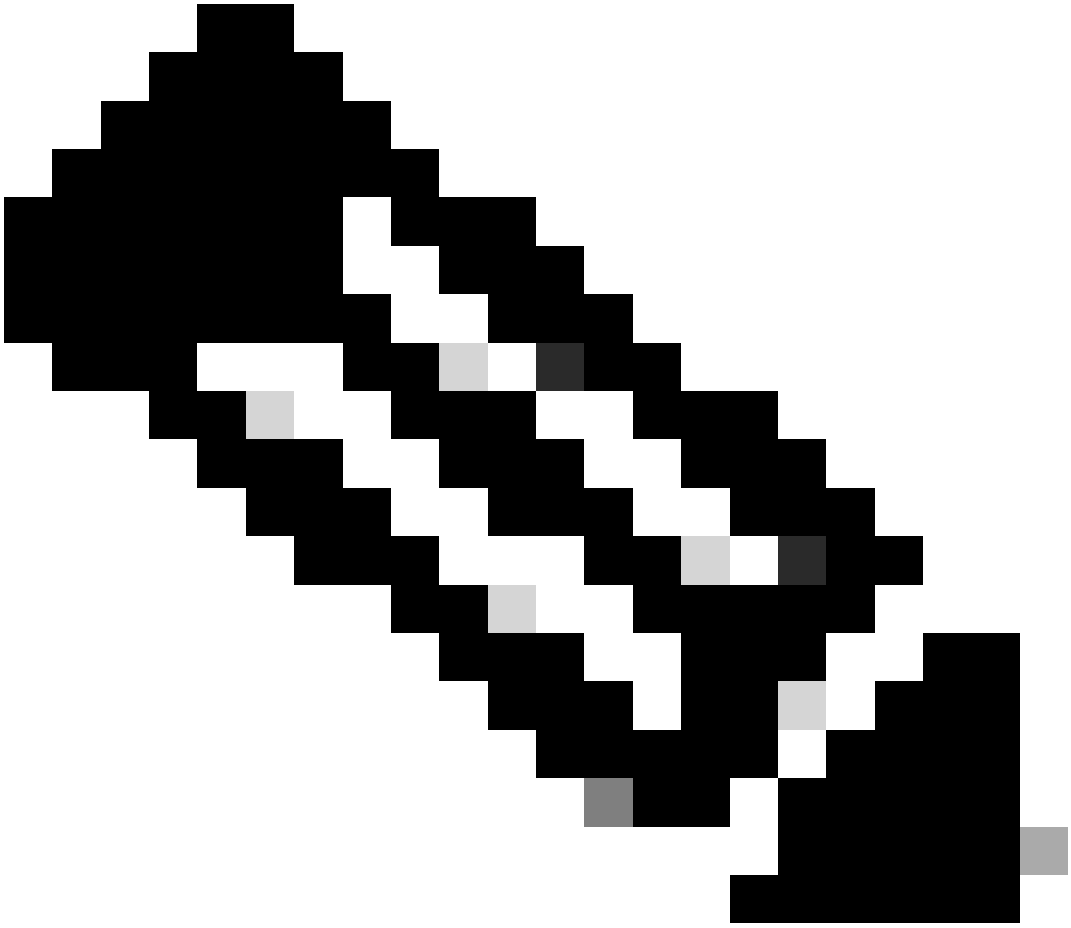
Externe domeinen in de SWG-module voor beveiligde clients

Inhoud

Inleiding

In dit document wordt beschreven hoe de Cisco Secure Client (CSC) (voorheen AnyConnect) Secure Web Gateway (SWG)-module de lijst met geconfigureerde externe domeinen toepast en wat de implicaties hiervan zijn.



Cisco kondigde het einde van de levensduur van Cisco AnyConnect in 2023 en de Umbrella Roaming Client in 2024. Veel Cisco Umbrella-klanten profiteren al van de migratie naar Cisco Secure Client en u wordt aangemoedigd om zo snel mogelijk te migreren om een betere roamingervaring te krijgen. Lees meer in dit Knowledge Base-artikel: Hoe installeer ik Cisco Secure Client met de overkoepelende module?

Overzicht

De Cisco Umbrella External Domains-lijst accepteert zowel domeinen als IP-adressen. In beide gevallen kan de SWG-module van de CSC echter alleen het uitsluitingsbesluit op basis van het IP-adres toepassen.

Op hoog niveau is het mechanisme dat de SWG-module gebruikt om verkeer naar domeinen in de lijst Externe domeinen te identificeren als volgt:

- De SWG-module bewaakt DNS-opzoekingen vanaf het clientsysteem om opzoekingen van de domeinen in de lijst met externe domeinen te identificeren

- Deze domeinen en de bijbehorende IP-adressen worden toegevoegd aan een lokale DNS-cache
- De beslissing om SWG te omzeilen wordt vervolgens toegepast op elk verkeer dat bestemd is voor een IP dat overeenkomt met een extern domein in de lokale DNS-cache. De beslissing is niet gebaseerd op het domein dat wordt gebruikt in het HTTP-verzoek.

Waarom functioneert het op deze manier?

De CSC SWG-module werkt op Layer3/Layer4, zodat deze alleen inzicht heeft in de TCP/IP-headers die de 5-Tuple-verbindingsdetails opslaan (DestinationIP:Port, SourceIP:Port en Protocol) waarop deze de verkeersregels kan baseren.

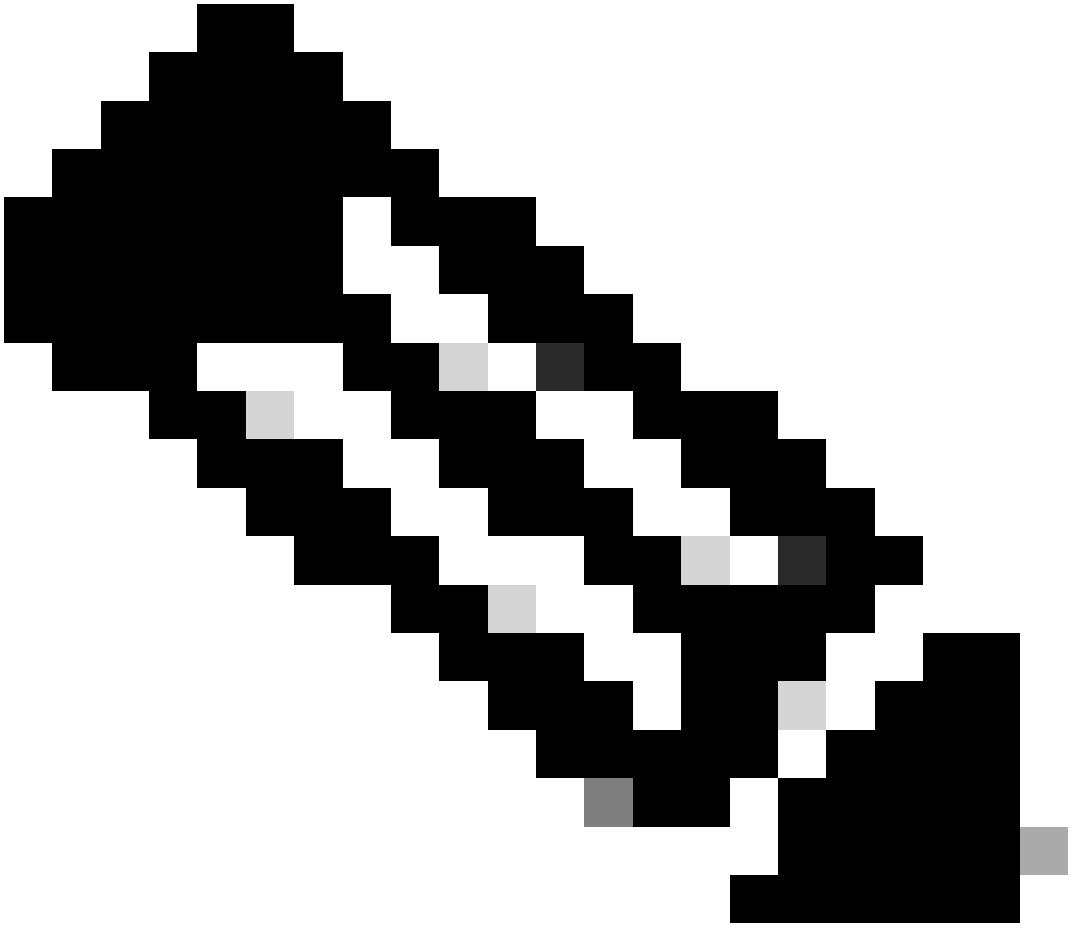
Daarom vereist CSC SWG voor domeingebaseerde bypasses een manier om de domeinen in de lijst te vertalen naar IP-adressen die vervolgens kunnen worden afgestemd op het verkeer op het clientsysteem. Hiertoe genereert het de DNS-cache van de DNS-lookups die van de client zijn verzonden, de DNS-cache vermeldt het IP-adres dat overeenkomt met de domeinen in de lijst met externe domeinen

De beslissing om SWG te omzeilen wordt vervolgens toegepast op onderschept verkeer (standaard 80/443) dat bestemd is voor deze IP-adressen.

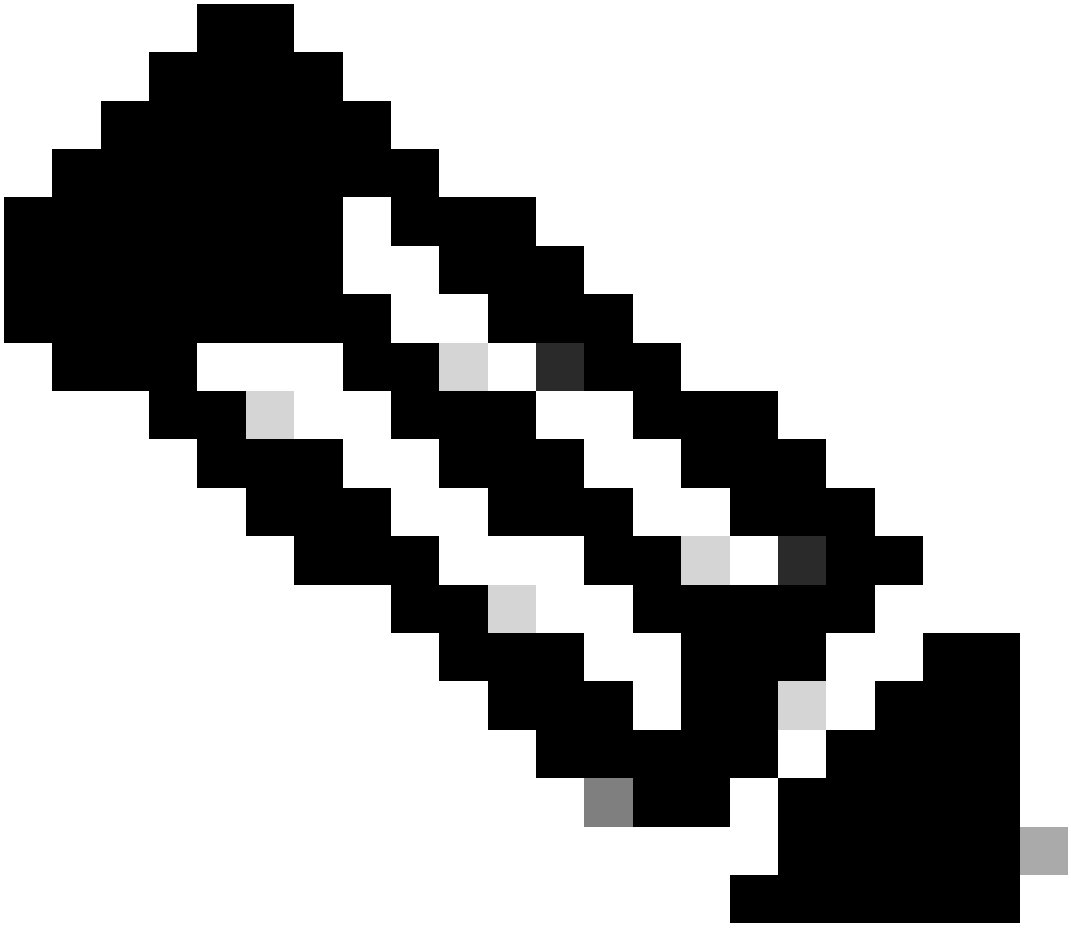
Waarom doet dit ertoe voor mij?

Er zijn een paar veel voorkomende problemen die dit kan veroorzaken:

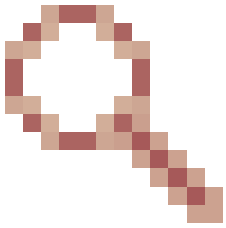
1. Aangezien de bypass-beslissing uiteindelijk is gebaseerd op een IP, wordt verkeer voor andere domeinen die hetzelfde IP delen ook omzeild van Cisco Umbrella, waardoor de klant onverwacht verkeer rechtstreeks van de client waarneemt en het SWG-beleid niet heeft toegepast of in Activity Search wordt weergegeven.
2. Als de SWG-module om welke reden dan ook de DNS-zoekopdracht voor het domein niet kan zien (zoals in, er is een localhost-vermelding voor het domein), wordt de IP niet toegevoegd aan de cache en wordt het verkeer daarom onverwacht naar SWG verzonden.



Opmerking: het KDF-stuurprogramma bewaakt alleen UDP DNS-lookups. Als om welke reden dan ook de DNS-zoekopdracht via TCP wordt uitgevoerd, wordt het IP-adres niet aan de cache toegevoegd en wordt het externe domein niet toegepast. Dit is gepubliceerd in Cisco's Bug Search.



Opmerking: we hebben een probleem opgelost met de SWG-module Externe domeinen



die naar Umbrella gaan wanneer DNS is opgelost via TCP (CSCwe48679)
) (Windows en MacOS) in Cisco Secure Client 5.1.4.74 (MR4)

Hoe kan ik dit proces oplossen?

Het proces van de SWG-module die de DNS-lookups observeert, items toevoegt aan de DNS-cache en de bypass-actie toepast op verkeer dat bestemd is voor de IP's, kan worden gevolgd in de KDF-logs. Dit vereist dat KDF-logboekregistratie is ingeschakeld en alleen gedurende een korte periode kan worden ingeschakeld tijdens het oplossen van problemen vanwege de breedheid van de logs.

Voorbeeld KDF-logboekvermeldingen

DNS-zoekopdracht van een domein dat wordt toegevoegd aan de 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-verbinding geobserveerd, domein niet op lijst met externe domeinen, verzoek verzonden 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
```

HTTPS-verbinding waargenomen, vermelding voor IP gevonden in cache, bypass-actie toegepast:

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.