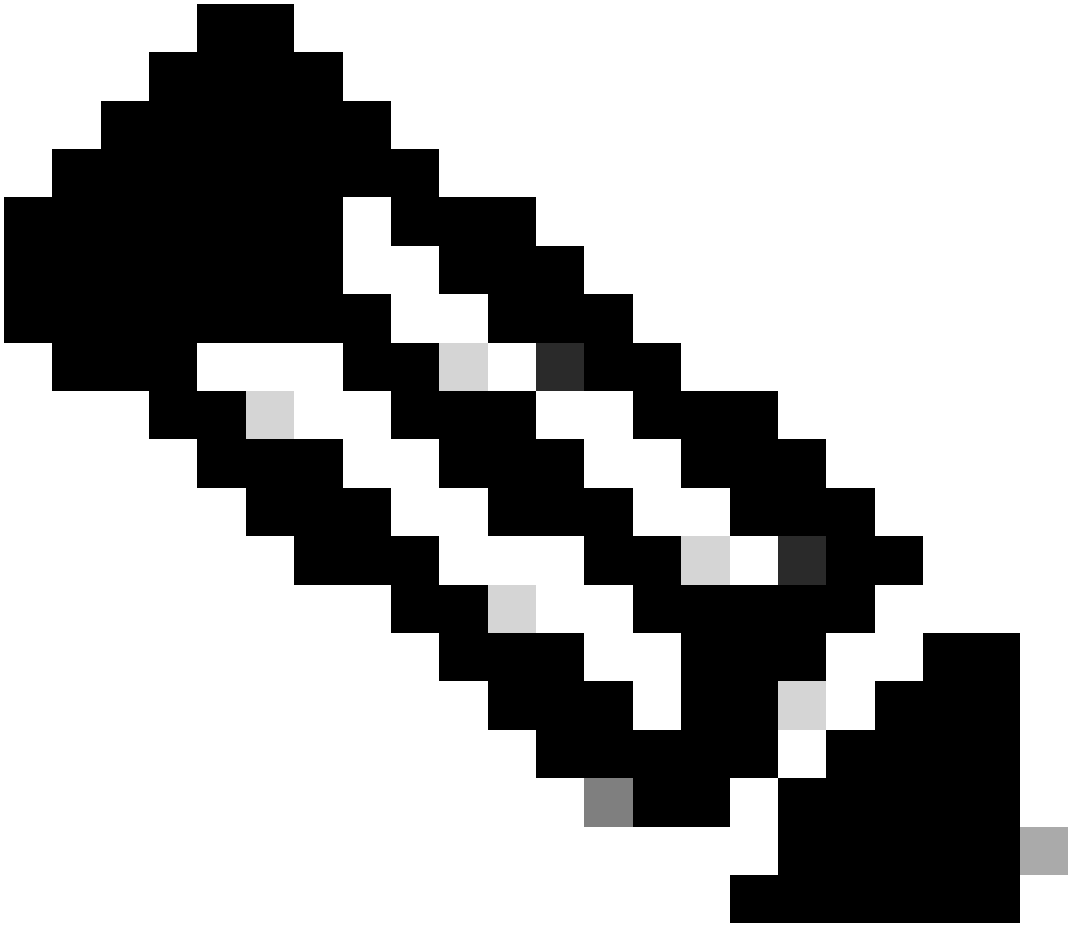
Externe Domänen im SWG-Modul für sichere Clients

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie das Cisco Secure Client (CSC) (ehemals AnyConnect) Secure Web Gateway (SWG)-Modul die Liste der konfigurierten externen Domänen anwendet und welche Auswirkungen dies hat.



Anmerkung: Cisco hat das Ende seiner Lebensdauer für Cisco AnyConnect im Jahr 2023 und für den Umbrella Roaming Client im Jahr 2024 angekündigt. Viele Kunden von Cisco Umbrella profitieren bereits von der Migration auf den Cisco Secure Client, und wir empfehlen Ihnen, die Migration so bald wie möglich zu beginnen, um ein besseres Roaming-Erlebnis zu erhalten. Weitere Informationen finden Sie in diesem Knowledge Base-Artikel: Wie installiere ich Cisco Secure Client mit dem Umbrella-Modul?

Überblick

Die Liste der externen Cisco Umbrella-Domänen akzeptiert sowohl Domänen als auch IP-Adressen. In beiden Fällen kann das CSC-SWG-Modul jedoch nur die Ausschlussentscheidung auf Basis der IP-Adresse anwenden.

Im Allgemeinen verwendet das SWG-Modul den folgenden Mechanismus, um Datenverkehr zu Domänen in der Liste der externen Domänen zu identifizieren:

- Das SWG-Modul überwacht DNS-Lookups vom Client-Computer, um die Lookups der

Domänen in der Liste der externen Domänen zu identifizieren.
- Diese Domänen und die zugehörigen IP-Adressen werden einem lokalen DNS-Cache hinzugefügt
- Die Entscheidung, die SWG dann zu umgehen, wird auf den Datenverkehr angewendet, der für eine IP-Adresse bestimmt ist, die einer externen Domäne im lokalen DNS-Cache entspricht. Die Entscheidung basiert nicht auf der Domäne, die innerhalb der HTTP-Anforderung verwendet wird.

Warum funktioniert es so?

Das CSC-SWG-Modul wird auf Layer 3/Layer 4 ausgeführt, sodass nur die TCP/IP-Header sichtbar sind, in denen die 5-Tupel-Verbindungsdetails (DestinationIP:Port, SourceIP:Port und Protocol) gespeichert sind, auf denen die Regeln für die Umgehung des Datenverkehrs basieren können.

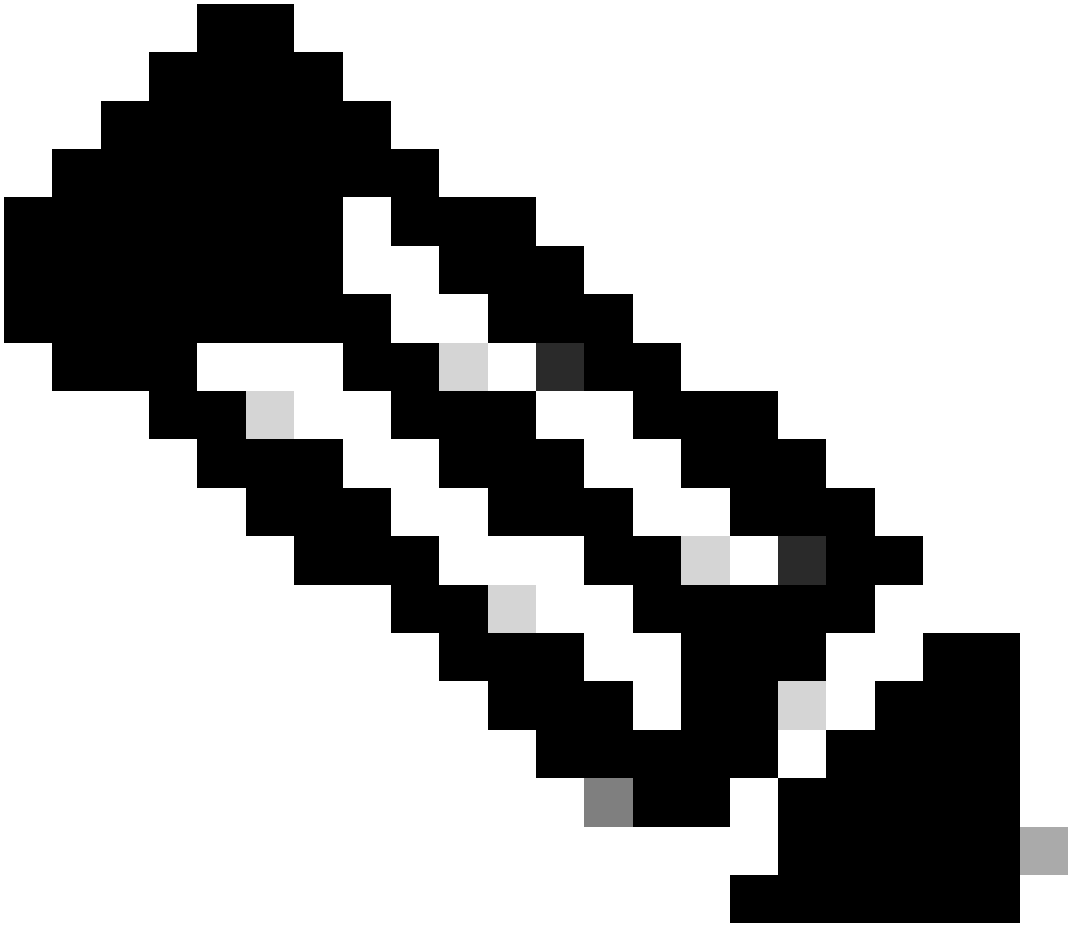
Daher benötigt die CSC SWG für domänenbasierte Umgehungen eine Möglichkeit, die Domänen in der Liste in IP-Adressen zu übersetzen, die dann mit dem Datenverkehr auf dem Client-Computer übereinstimmen können. Zu diesem Zweck generiert er den DNS-Cache aus den vom Client gesendeten DNS-Lookups, der DNS-Cache listet die IP-Adresse entsprechend den Domänen in der Liste der externen Domänen auf

Die Entscheidung, die SWG zu umgehen, wird dann auf abgefangenen Datenverkehr (standardmäßig 80/443) angewendet, der an diese IP-Adressen gerichtet ist.

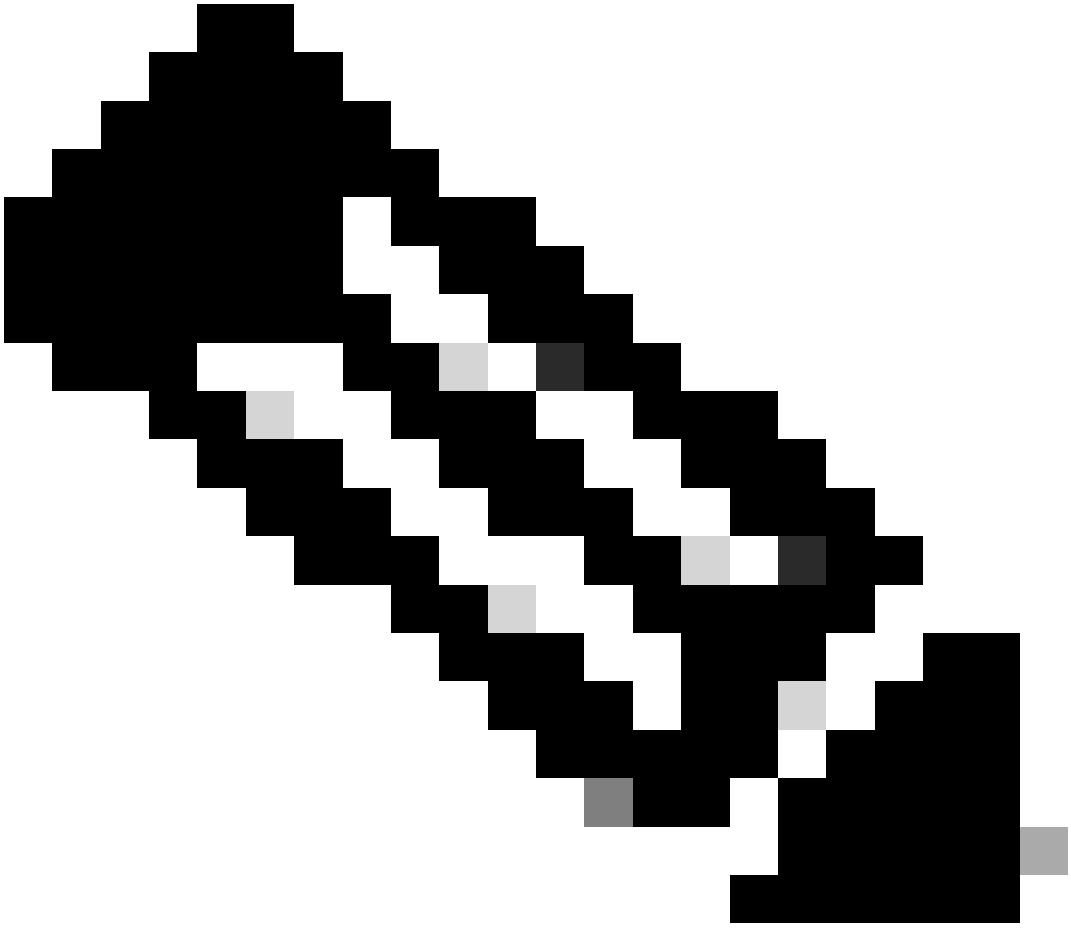
Warum ist mir das wichtig?

Dies kann zu einigen häufigen Problemen führen:

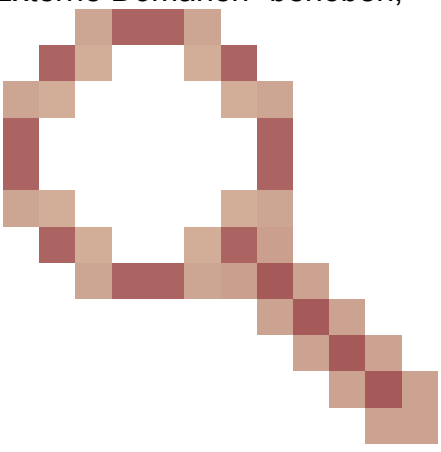
1. Da die Umgehungsentscheidung letztendlich auf einer IP basiert, wird der Datenverkehr für andere Domänen mit derselben IP ebenfalls von Cisco Umbrella umgangen. Dies führt dazu, dass der Kunde unerwarteten Datenverkehr direkt vom Client ausgeht und keine SWG-Richtlinie anwendet oder in der Aktivitätssuche erscheint.
2. Wenn das SWG-Modul aus irgendeinem Grund die DNS-Suche für die Domäne nicht sehen kann (wie in, es gibt einen lokalen Host-Eintrag für die Domäne), wird die IP nicht zum Cache hinzugefügt, und der Datenverkehr wird daher unerwartet an die SWG gesendet.



Anmerkung: Der KDF-Treiber überwacht nur UDP-DNS-Lookups. Wenn die DNS-Suche aus irgendeinem Grund über TCP durchgeführt wird, wird die IP nicht zum Cache hinzugefügt, und die externe Domäne wird nicht angewendet. Diese finden Sie in Cisco Bug Search.



Anmerkung: Wir haben ein Problem mit dem SWG-Modul "Externe Domänen" behoben,



das zu Umbrella geht, wenn DNS über TCP (CSCwe48679
) (Windows und MacOS) in Cisco Secure Client 5.1.4.74 (MR4)

Wie kann ich diesen Prozess beheben?

Der Prozess, mit dem das SWG-Modul die DNS-Abfragen beobachtet, Einträge zum DNS-Cache

hinzufügt und die Umgehungsaktion auf den Datenverkehr anwendet, der für die IPs bestimmt ist, kann in den KDF-Protokollen nachverfolgt werden. Dies erfordert, dass die KDF-Protokollierung aktiviert ist und aufgrund der Ausführlichkeit der Protokolle nur für kurze Zeit während der Fehlerbehebung aktiviert werden kann.

Beispiel für KDF-Protokolleinträge

DNS-Suche einer Domäne, die dem DNS-Cache hinzugefügt wird:

```
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-Verbindung beobachtet, Domäne nicht in Liste externer Domänen, Anfrage über SWG gesendet:

```
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-Verbindung beobachtet, Eintrag für IP im Cache gefunden, Umgehungsaktion angewendet:

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.