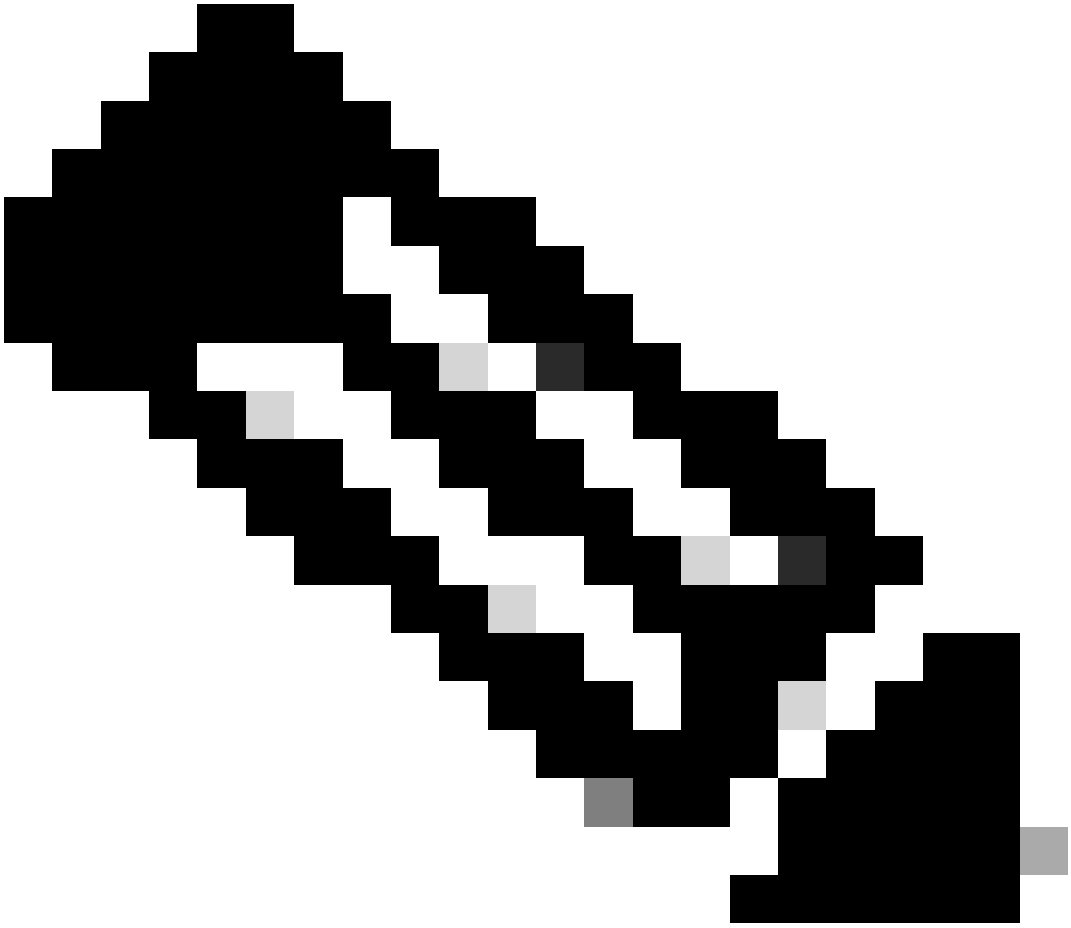
Domini esterni nel modulo Secure Client SWG

Sommario

Introduzione

In questo documento viene descritto come il modulo Cisco Secure Client (CSC) (in precedenza AnyConnect) Secure Web Gateway (SWG) applica l'elenco dei domini esterni configurati e le relative implicazioni.



Nota: Cisco ha annunciato la fine del ciclo di vita di Cisco AnyConnect nel 2023 e del client di roaming Umbrella nel 2024. Molti clienti Cisco Umbrella stanno già beneficiando della migrazione a Cisco Secure Client e si è incoraggiati ad avviare la migrazione il prima possibile per ottenere un'esperienza di roaming migliore. Ulteriori informazioni in questo articolo della Knowledge Base: Come installare Cisco Secure Client con il modulo Umbrella?

Panoramica

L'elenco dei domini esterni Cisco Umbrella accetta sia domini che indirizzi IP. Tuttavia, in entrambi i casi, il modulo CSC SWG può applicare la decisione di esclusione solo in base all'indirizzo IP.

Ad alto livello, il meccanismo utilizzato dal modulo SWG per identificare il traffico diretto ai domini nell'elenco dei domini esterni è il seguente:

- Il modulo SWG monitora le ricerche DNS dal computer client per identificare le ricerche dei domini nell'elenco dei domini esterni

- Questi domini e i relativi indirizzi IP corrispondenti vengono aggiunti a una cache DNS locale
- La decisione di ignorare SWG viene quindi applicata a tutto il traffico destinato a un IP che corrisponde a un dominio esterno all'interno della cache DNS locale. La decisione non è basata sul dominio utilizzato nella richiesta HTTP.

Perché funziona in questo modo?

Il modulo CSC SWG opera sul layer 3/layer 4, in quanto ha visibilità solo sulle intestazioni TCP/IP in cui sono memorizzati i dettagli della connessione a 5 tuple (DestinationIP:Port, SourceIP:Port e Protocol) su cui può basare le proprie regole di bypass del traffico.

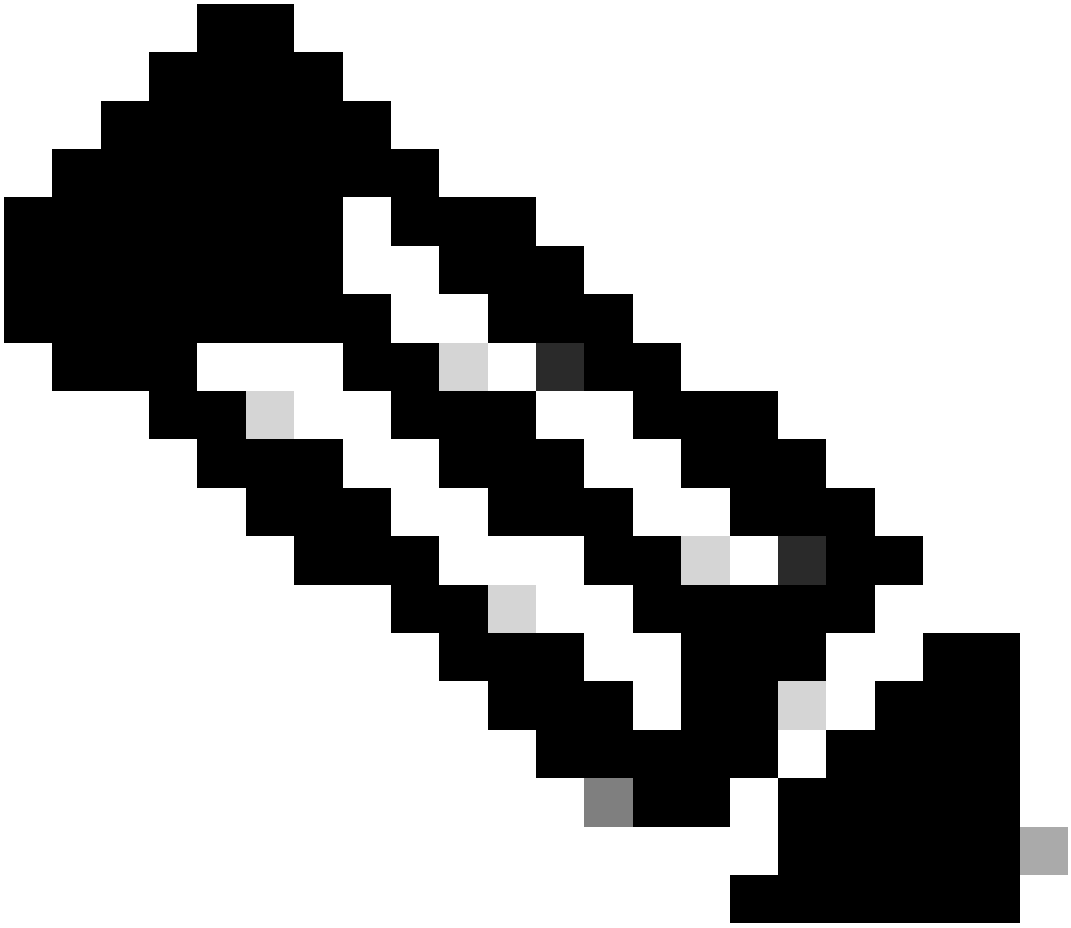
Pertanto, per le bypass basate su dominio, CSC SWG richiede un modo per convertire i domini nell'elenco in indirizzi IP che possono quindi corrispondere al traffico sul computer client. A tale scopo, genera la cache DNS dalle ricerche DNS inviate dal client, la cache DNS elenca l'indirizzo IP corrispondente ai domini nell'elenco dei domini esterni

La decisione di ignorare SWG viene quindi applicata al traffico intercettato (per impostazione predefinita 80/443) destinato a questi indirizzi IP.

Perché questo ha importanza per me?

Ciò può causare un paio di problemi comuni:

1. Poiché la decisione di bypass si basa in ultima analisi su un IP, anche il traffico di altri domini che condividono lo stesso IP viene ignorato da Cisco Umbrella, con la conseguenza che il cliente osserva un traffico imprevisto che proviene direttamente dal client e non ha la policy SWG applicata o visualizzata in Activity Search.
2. Se per qualche motivo il modulo SWG non riesce a vedere la ricerca DNS per il dominio (come in, c'è una voce localhost per il dominio), allora l'IP non viene aggiunto alla cache e quindi il traffico viene inaspettatamente inviato al gruppo SWG.



Nota: Il driver KDF esegue il monitoraggio solo delle ricerche DNS UDP. Se per qualsiasi motivo la ricerca DNS viene eseguita tramite TCP, l'indirizzo IP non viene aggiunto alla cache e il dominio esterno non viene applicato. L'indirizzo viene pubblicato in Cisco Bug Search.

Nota: È stato risolto un problema con il modulo SWG Domini esterni indirizzati a Umbrella

quando il DNS è stato risolto tramite TCP (CSCwe48679
) (Windows e MacOS) in Cisco Secure Client 5.1.4.74 (MR4)

Come risolvere i problemi relativi a questo processo?

Il processo del modulo SWG che osserva le ricerche DNS, aggiunge voci alla cache DNS e applica l'azione di bypass al traffico destinato agli IP può essere seguito nei registri KDF. È quindi necessario che la registrazione KDF sia attivata e possa essere attivata solo per un breve periodo durante la risoluzione dei problemi a causa del livello di dettaglio dei registri.

Voci di log KDF di esempio

Ricerca DNS di un dominio aggiunto alla 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
```

Osservata connessione HTTPS, dominio non presente nell'elenco dei domini esterni, richiesta inviata tramite 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
```

Rilevata connessione HTTPS, voce per IP trovata nella cache, azione di bypass applicata:

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).