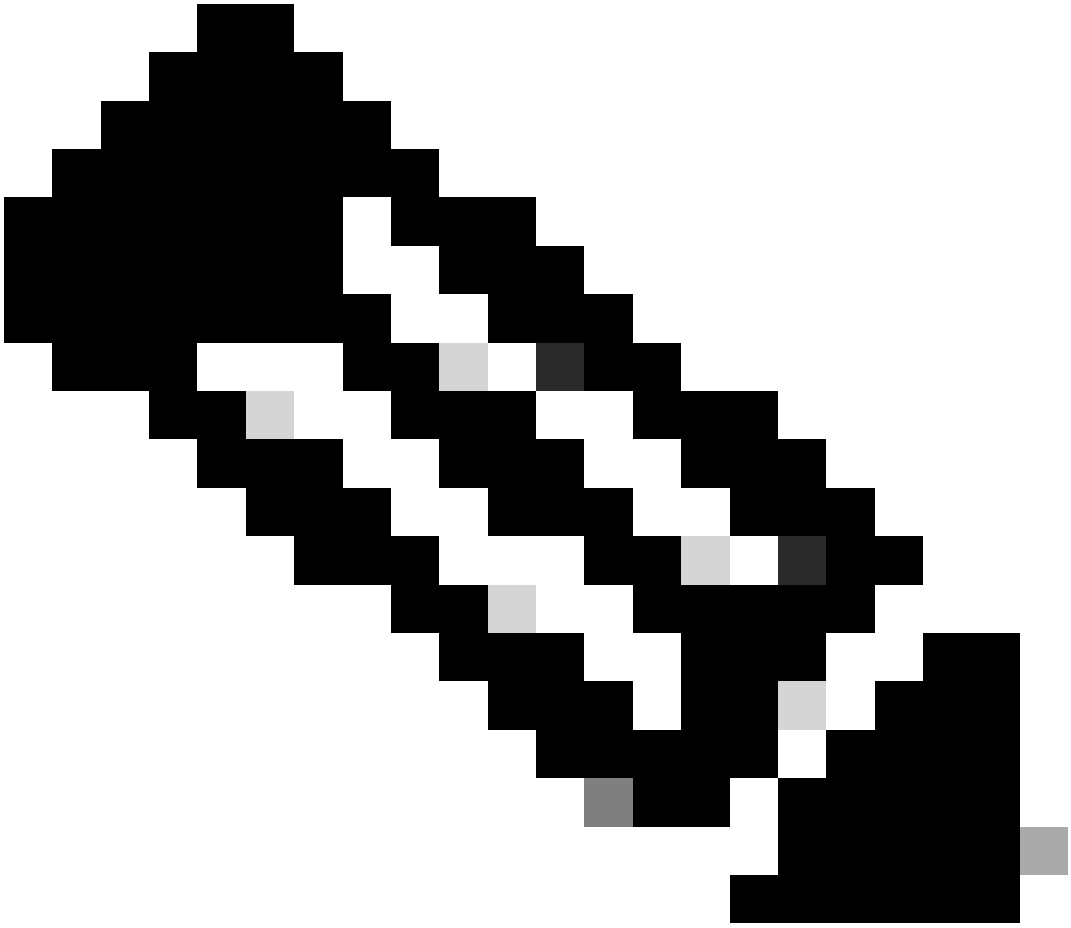
Domínios externos no módulo SWG de cliente seguro

Contents

Introdução

Este documento descreve como o módulo Cisco Secure Client (CSC) (anteriormente AnyConnect) Secure Web Gateway (SWG) aplica a lista de domínios externos configurados e as implicações disso.



Note: A Cisco anunciou o fim da vida útil do Cisco AnyConnect em 2023 e do Umbrella Roaming Client em 2024. Muitos clientes do Cisco Umbrella já estão se beneficiando da migração para o Cisco Secure Client, e você é encorajado a iniciar a migração o mais rápido possível para obter uma melhor experiência de roaming. Leia mais neste artigo da Base de conhecimento: Como instalo o Cisco Secure Client com o Umbrella Module?

Overview

A lista de domínios externos do Cisco Umbrella aceita domínios e endereços IP. No entanto, em ambos os casos, o módulo CSC SWG só pode aplicar a decisão de exclusão com base no endereço IP.

Em um alto nível, o mecanismo que o módulo SWG usa para identificar o tráfego para domínios na lista Domínios externos é o seguinte:

- O módulo SWG monitora pesquisas DNS da máquina cliente para identificar pesquisas dos domínios na lista de domínios externos

- Esses domínios e seus endereços IP correspondentes são adicionados a um cache DNS local
- A decisão de ignorar o SWG é então aplicada a qualquer tráfego destinado a um IP que corresponda a um Domínio externo dentro do cache DNS local. A decisão não é baseada no domínio usado na Solicitação HTTP.

Por que ele funciona dessa maneira?

O módulo CSC SWG opera na Camada 3/Camada 4, dessa forma, ele só tem visibilidade dos cabeçalhos TCP/IP que armazenam os detalhes de conexão de 5 tuplas (DestinationIP:Port, SourceIP:Port e Protocol) nos quais pode basear suas regras de desvio de tráfego.

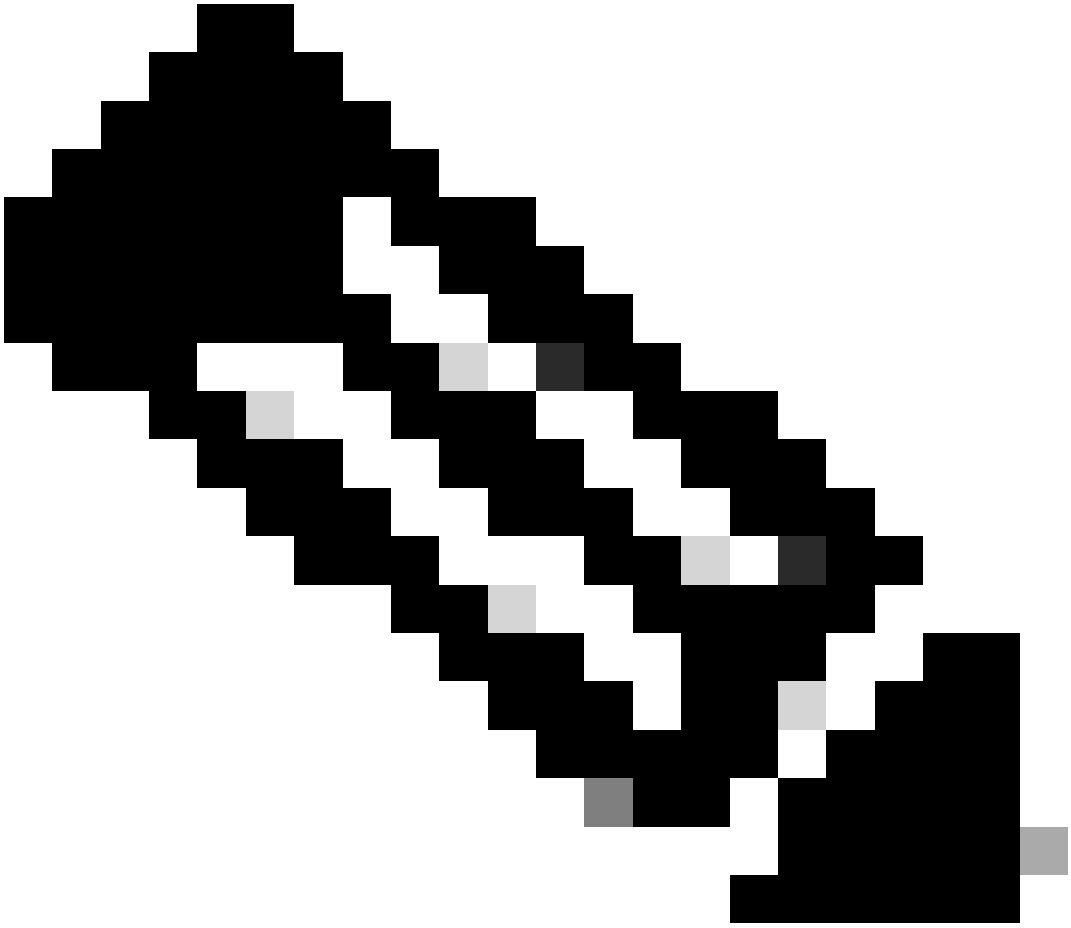
Portanto, para desvios baseados em domínio, o CSC SWG requer uma maneira de converter os domínios na lista em endereços IP que podem ser correspondidos ao tráfego na máquina cliente. Para isso, ele gera o cache DNS a partir das pesquisas de DNS enviadas do cliente, o cache DNS lista o endereço IP correspondente aos domínios na lista de domínios externos

A decisão de ignorar o SWG é então aplicada ao tráfego interceptado (por padrão 80/443) destinado a esses endereços IP.

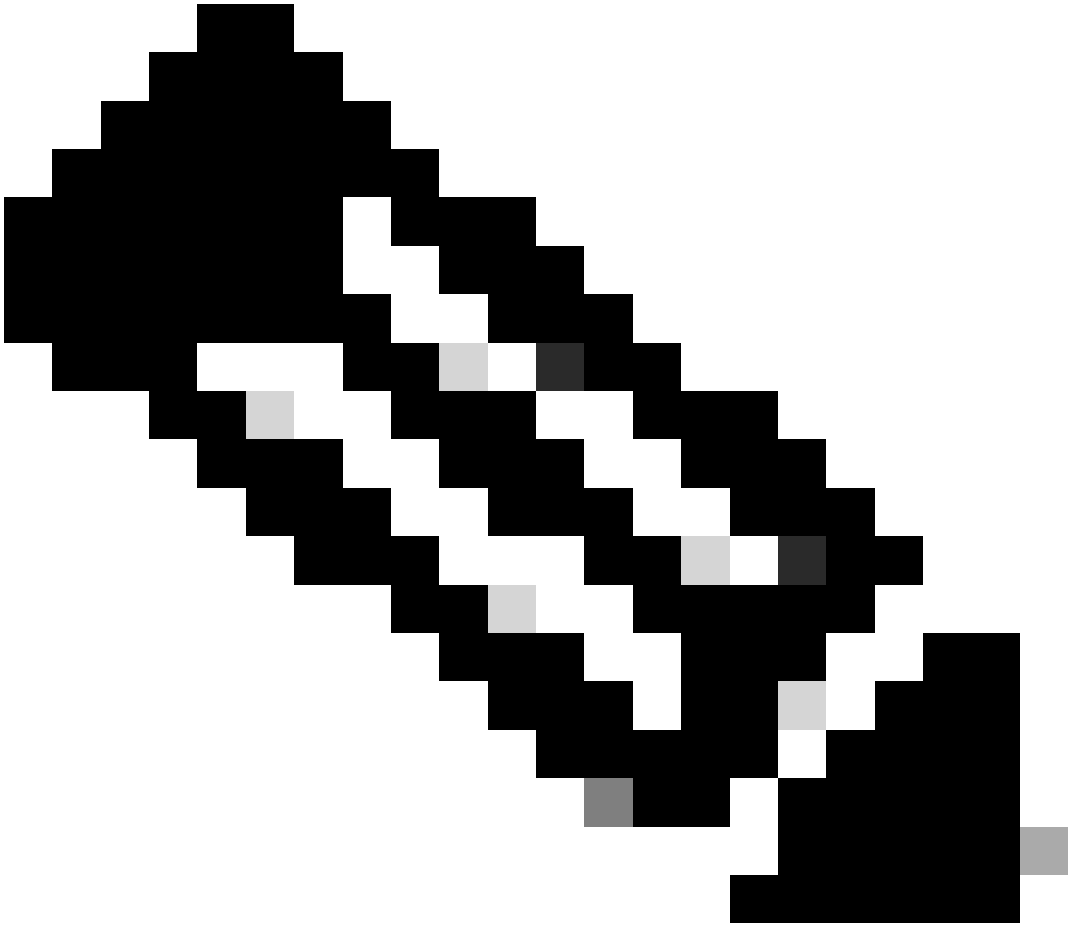
Por que isso é importante para mim?

Há alguns problemas comuns que isso pode causar:

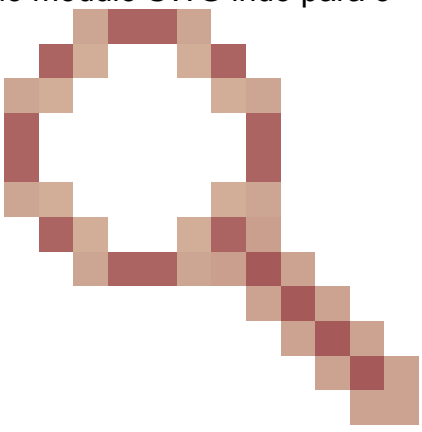
1. Como a decisão de desvio é baseada em um IP, o tráfego para outros domínios que compartilham o mesmo IP também é ignorado do Cisco Umbrella, fazendo com que o cliente observe tráfego inesperado saindo diretamente do cliente e não tenha a política SWG aplicada ou aparecendo na pesquisa de atividade.
2. Se, por algum motivo, o módulo SWG não puder ver a pesquisa DNS para o domínio (como em, há uma entrada localhost para o domínio), o IP não será adicionado ao cache e, portanto, o tráfego será enviado inesperadamente para o SWG.



Note: O driver KDF monitora apenas pesquisas UDP DNS. Se, por algum motivo, a pesquisa de DNS for realizada via TCP, o IP não será adicionado ao cache e o domínio externo não será aplicado. Isso é publicado na Bug Search da Cisco.



Note: Resolvemos um problema com os domínios externos do módulo SWG indo para o



Umbrella quando o DNS é resolvido por TCP (CSCwe48679
) (Windows e MacOS) no Cisco Secure Client 5.1.4.74 (MR4)

Como posso solucionar problemas desse processo?

O processo do módulo SWG observando as pesquisas de DNS, adicionando entradas ao cache

DNS e aplicando a ação de desvio ao tráfego destinado para os IPs pode ser seguido nos logs KDF. Isso exige que o registro KDF esteja habilitado e só possa ser habilitado por um curto período de tempo durante a solução de problemas devido ao detalhamento dos registros.

Exemplo de entradas de registro KDF

Pesquisa DNS de um domínio que está sendo adicionado ao 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
```

Conexão HTTPS observada, domínio não incluído na lista de domínios externos, solicitação enviada 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
```

Conexão HTTPS observada, entrada para IP encontrada no cache, ação de bypass aplicada:

```
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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.