了解安全客户端SWG模块中的外部域

目录

简介

概述

为什么它以这种方式运行？

为什么这对我来说如此重要？

如何排除此过程的故障？

KDF日志条目示例

简介

本文档介绍思科安全客户端(CSC)安全网络网关(SWG)模块如何应用配置的外部域列表。

注意：思科于2023年宣布了Cisco AnyConnect的生命周期终止，并于2024年宣布了Umbrella漫游客户端。许多Cisco Umbrella用户已经从迁移到Cisco安全客户端中受益，我们鼓励您尽快开始迁移，以获得更好的漫游体验。阅读此知识库文章的更多信息：如何安装带有Umbrella模块的思科安全客户端？

概述

Cisco Umbrella External Domains列表接受域和IP地址。但是，在这两种情况下，CSC（以前称为AnyConnect）SWG模块只能根据IP地址应用排除决策。

在较高层面上，SWG模块用于识别流向外部域列表中的域的流量的机制如下：

- SWG模块监控来自客户端计算机的DNS查找，以识别外部域列表中的域查找
- 这些域及其相应的IP地址将添加到本地DNS缓存
- 然后绕过SWG的决策将应用于发往与本地DNS缓存中的外部域对应的IP的任何流量。此决定不是基于HTTP请求中使用的域。

为什么它以这种方式运行？

CSC SWG模块在第3/第4层运行，因此，它只能查看存储5元组连接详细信息

（DestinationIP:Port、SourceIP:Port和Protocol）的TCP/IP报头，其流量旁路规则可以基于这些信息。

因此，对于基于域的旁路，CSC SWG需要将列表中的域转换为IP地址，然后可以将其与客户端计算机上的流量匹配。为此，它根据客户端发送的DNS查找生成DNS缓存，DNS缓存列出与外部域列表中的域对应的IP地址

然后，将绕过SWG的决策应用于目的地为这些IP地址的拦截流量（默认值为80/443）。

为什么这对我来说如此重要？

这可能会导致一些常见问题：

1. 鉴于绕行决策最终基于IP，共享同一IP的其他域的流量也会从Cisco Umbrella绕过，导致您观察到来自客户端的意外流量直接流出，并且未应用或出现在活动搜索中。
2. 如果由于任何原因，SWG模块无法看到该域的DNS查找（如中的，存在该域的localhost条目），则不会将IP添加到缓存，因此流量会意外发送到SWG。

注意：KDF驱动程序仅监控UDP DNS查找。如果由于任何原因通过TCP执行DNS查找，则不会将IP添加到缓存，也不会应用外部域。这在Cisco's Bug Search中发布。

注意：我们已修复了通过TCP解析DNS时SWG模块外部域进入Umbrella的问题(CSCxxYYYYY)（Windows和MacOS），在Cisco安全客户端5.1.4.74(MR4)中

如何排除此过程的故障？

SWG模块观察DNS查找、向DNS缓存添加条目以及向发往IP的流量应用旁路操作的过程可在KDF日志中执行。这要求启用KDF日志记录，并且由于日志的丰富性，只能在故障排除期间启用较短时间。

KDF日志条目示例

要添加到DNS缓存的域的DNS查找：

```
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
```

观察到的HTTPS连接、不在外部域列表中的域、通过SWG发送的请求：

```
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
```

观察到的HTTPS连接、缓存中找到的IP条目、应用的旁路操作：

```
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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。