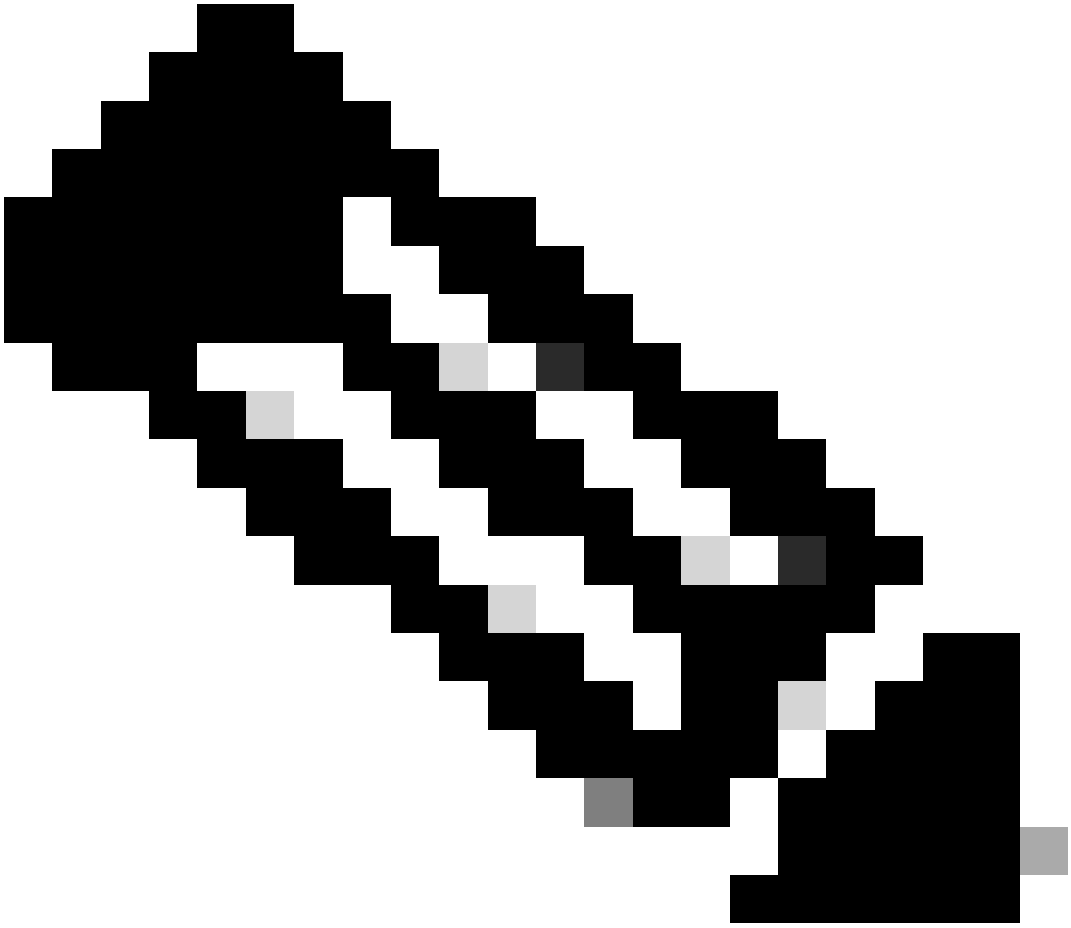
Secure Client SWG 모듈의 외부 도메인

목차

소개

이 문서에서는 CSC(Cisco Secure Client)(이전의 AnyConnect) SWG(Secure Web Gateway) 모듈이 구성된 외부 도메인 목록을 적용하는 방법 및 이에 따른 영향에 대해 설명합니다.



참고: Cisco는 2023년에 Cisco AnyConnect의 End-of-Life를, 2024년에 Umbrella Roaming Client를 발표했습니다. 많은 Cisco Umbrella 고객이 이미 Cisco Secure Client로의 마이그레이션을 통해 혜택을 누리고 있으며, 더 나은 로밍 경험을 얻으려면 최대한 빨리 마이그레이션을 시작하는 것이 좋습니다. 이 Knowledge Base 문서에서 자세히 읽기: Umbrella 모듈과 함께 Cisco Secure Client를 설치하려면 어떻게 해야 합니까?

개요

Cisco Umbrella External Domains(Cisco Umbrella 외부 도메인) 목록에는 도메인과 IP 주소가 모두 수락됩니다. 그러나 두 경우 모두 CSC SWG 모듈은 IP 주소에 기반한 제외 결정만 적용할 수 있습니다.

상위 레벨에서 SWG 모듈이 External Domains(외부 도메인) 목록의 도메인에 대한 트래픽을 식별하는 데 사용하는 메커니즘은 다음과 같습니다.

- SWG 모듈은 클라이언트 머신의 DNS 조회를 모니터링하여 외부 도메인 목록의 도메인 조회를 식별합니다

- 이러한 도메인 및 해당 IP 주소는 로컬 DNS 캐시에 추가됩니다
- 그런 다음 SWG를 우회하는 결정은 로컬 DNS 캐시 내의 외부 도메인에 해당하는 IP로 향하는 모든 트래픽에 적용됩니다. 결정은 HTTP 요청 내에서 사용되는 도메인을 기반으로 하지 않습니다.

왜 이런 식으로 작동할까요?

CSC SWG 모듈은 레이어 3/레이어 4에서 작동하며, 트래픽 우회 규칙의 기반이 될 수 있는 5-튜플 연결 세부사항(DestinationIP:Port, SourceIP:Port 및 Protocol)을 저장하는 TCP/IP 헤더에 대한 가시성만 갖습니다.

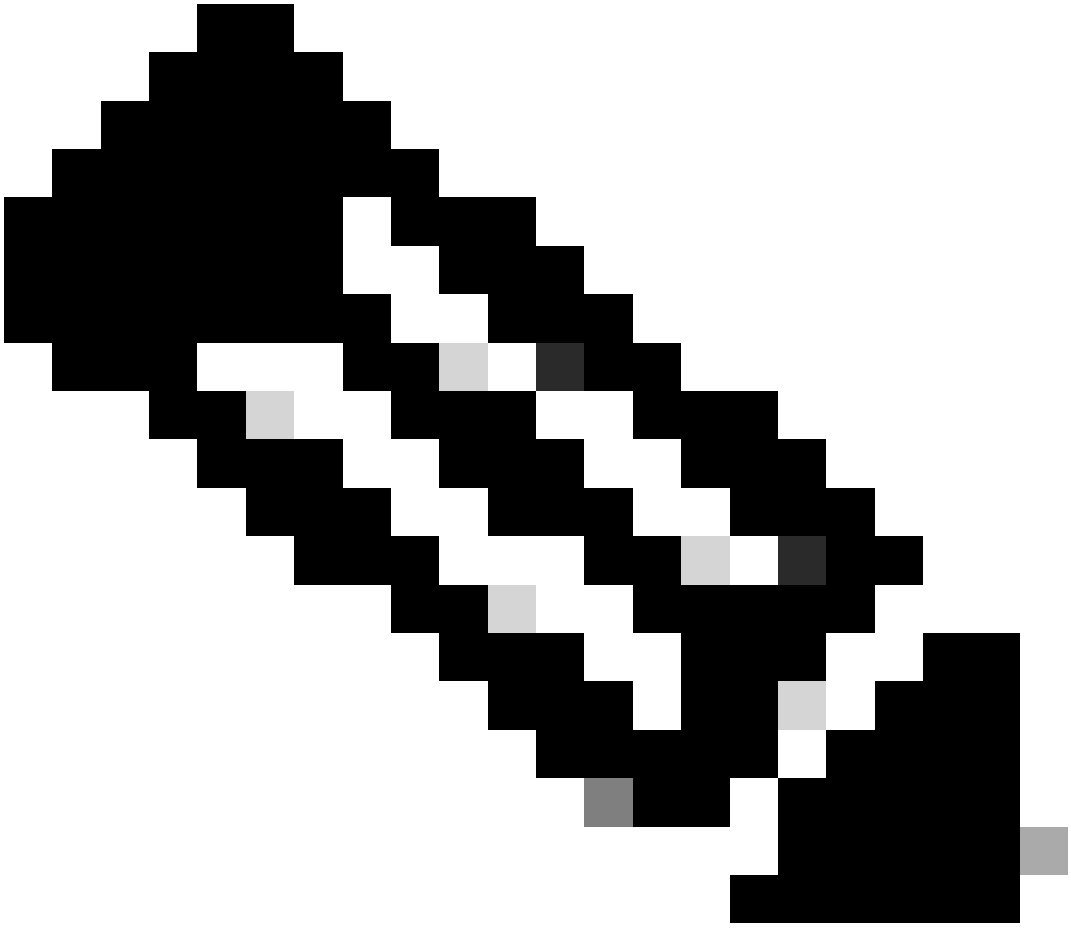
따라서 도메인 기반 우회의 경우 CSC SWG는 목록의 도메인을 IP 주소로 변환한 다음 클라이언트 시스템의 트래픽과 일치시킬 수 있는 방법이 필요합니다. 이를 위해 클라이언트에서 보낸 DNS 조회에서 DNS 캐시를 생성하며, DNS 캐시는 외부 도메인 목록의 도메인에 해당하는 IP 주소를 나열합니다

그런 다음 SWG를 우회하는 결정은 이러한 IP 주소로 향하는 차단된 트래픽(기본적으로 80/443)에 적용됩니다.

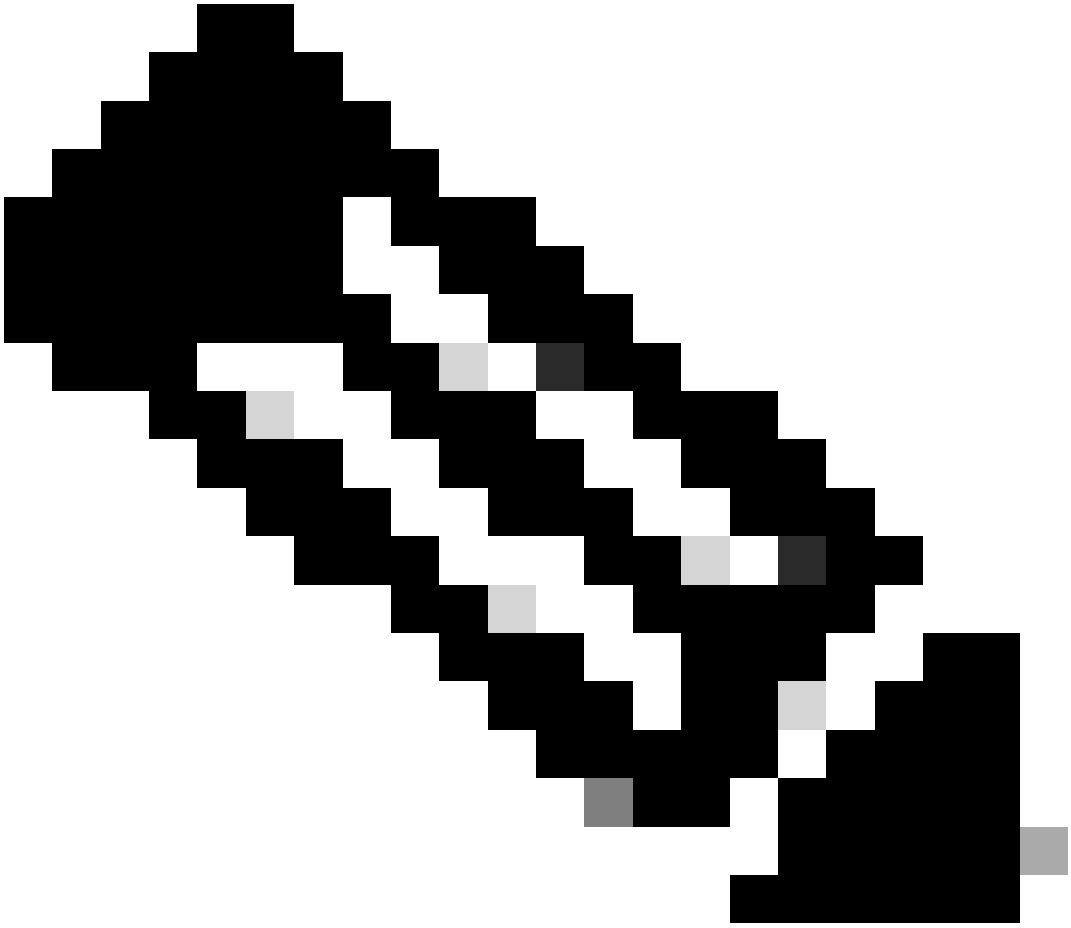
이게 왜 나한테 중요한데?

이로 인해 발생할 수 있는 몇 가지 일반적인 문제가 있습니다.

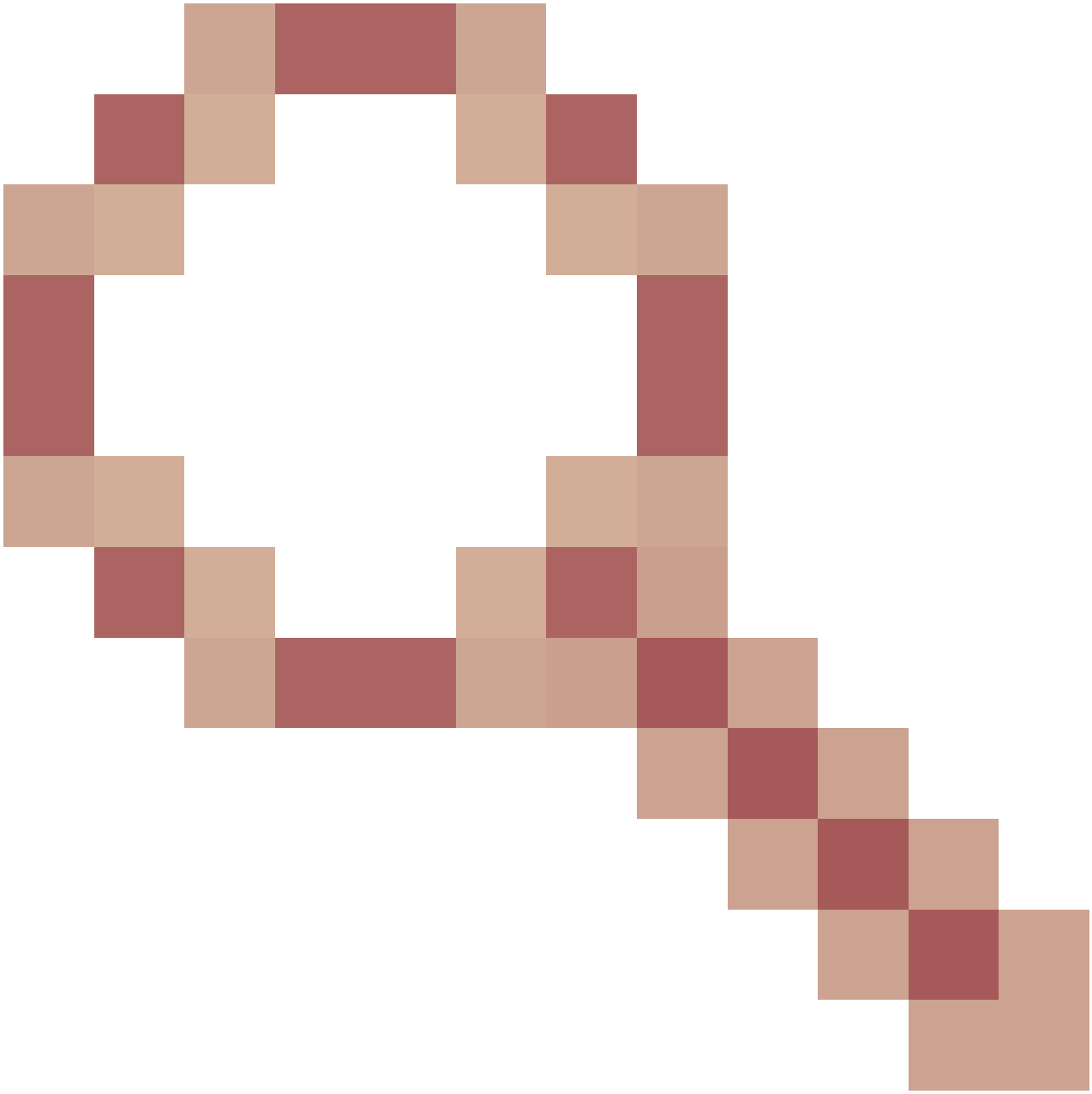
1. 우회 결정이 궁극적으로 IP를 기반으로 하는 경우, 동일한 IP를 공유하는 다른 도메인의 트래픽도 Cisco Umbrella에서 우회되므로, 고객은 클라이언트에서 직접 이동하는 예기치 않은 트래픽을 관찰할 수 있으며, SWG 정책이 적용되거나 활동 검색에 표시되지 않습니다.
2. 어떤 이유로든 SWG 모듈에서 도메인에 대한 DNS 조회를 볼 수 없는 경우(예: 도메인에 대한 localhost 항목이 있는 경우), IP가 캐시에 추가되지 않으므로 트래픽이 예기치 않게 SWG로 전송됩니다.



참고: KDF 드라이버는 UDP DNS 조회만 모니터링합니다. 어떤 이유로든 DNS 조회가 TCP를 통해 수행되는 경우 IP가 캐시에 추가되지 않고 외부 도메인이 적용되지 않습니다. 이 문서는 Cisco의 버그 검색에 게시되어 있습니다.



참고: TCP를 통해 DNS를 확인할 때 Umbrella로 이동하는 SWG 모듈 외부 도메인 문제를 해결했습니다(CSCwe48679



)(Windows 및 MacOS)(Cisco Secure Client 5.1.4.74(MR4))

이 프로세스를 트러블슈팅하려면 어떻게 해야 합니까?

SWG 모듈이 DNS 조회를 관찰하고, DNS 캐시에 엔트리를 추가하고, IP로 향하는 트래픽에 우회 작업을 적용하는 프로세스는 KDF 로그에서 따를 수 있습니다. 이를 위해서는 KDF 로깅이 활성화되어 있어야 하며, 로그의 다양성으로 인해 트러블슈팅을 수행하는 동안 잠시 동안만 활성화할 수 있습니다.

KDF 로그 항목 예

DNS 캐시에 추가되는 도메인의 DNS 조회:

```
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 연결이 관찰되었으며, 도메인이 외부 도메인 목록에 없음, SWG를 통해 요청 전송:

```
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
```

HTTPS 연결이 관찰됨, 캐시에서 IP에 대한 항목이 발견됨, 우회 작업이 적용됨:

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.