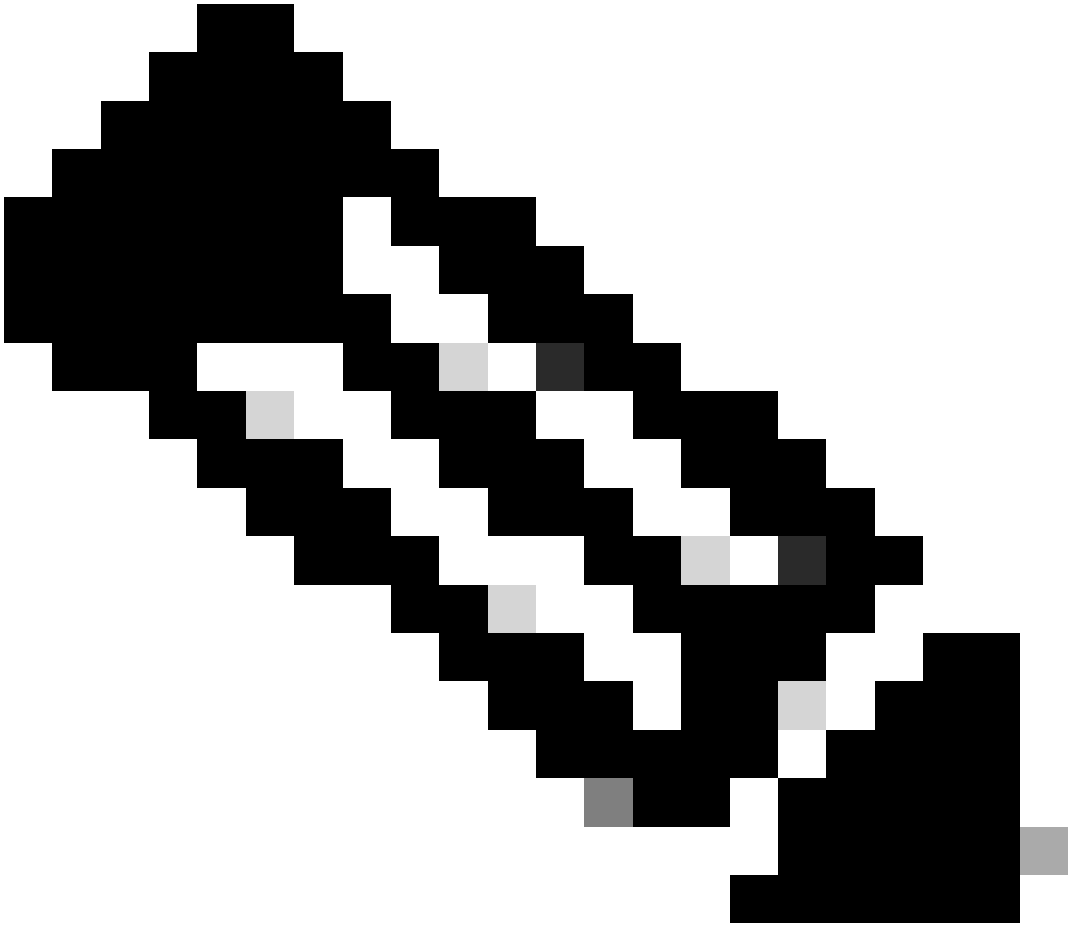
セキュアクライアントSWGモジュールの外部ドメイン

内容

はじめに

このドキュメントでは、Cisco Secure Client(CSC)（以前のAnyConnect）Secure Web Gateway(SWG)モジュールが設定済みの外部ドメインリストをどのように適用するかと、その影響について説明します。



注：シスコは2023年にCisco AnyConnectのサポート終了を、2024年にUmbrellaローミングクライアントを発表しました。Cisco Umbrellaをご利用のお客様の多くは、すでにCisco Secure Clientへの移行のメリットを享受しています。より良いローミング環境を得るために、できるだけ早く移行を開始することをお勧めします。ナレッジベース記事「How do I install Cisco Secure Client with the Umbrella Module?」の詳細を参照してください。

概要

Cisco Umbrellaの外部ドメインリストには、ドメインとIPアドレスの両方を指定できます。ただし、どちらの場合も、CSC SWGモジュールはIPアドレスに基づく除外決定だけを適用できます。

SWGモジュールがExternal Domainsリストのドメインへのトラフィックを識別するために使用するメカニズムの概要は次のとおりです。

- SWGモジュールは、クライアントマシンからのDNSルックアップを監視して、外部ドメイ

ンリストのドメインのルックアップを特定します
- これらのドメインとそれに対応するIPアドレスは、ローカルDNSキャッシュに追加されます
- 次に、SWGをバイパスするという決定は、ローカルDNSキャッシュ内の外部ドメインに対応するIP宛てのすべてのトラフィックに適用されます。この決定は、HTTP要求内で使用されるドメインに基づくものではありません。

それはなぜこのように機能するのでしょうか。

CSC SWGモジュールは、レイヤ3/レイヤ4で動作します。つまり、TCP/IPヘッダーに対する可視性だけを持ち、トラフィックバイパスルールのベースとなる5タプル接続の詳細（DestinationIP:Port、SourceIP:Port、およびProtocol）を格納します。

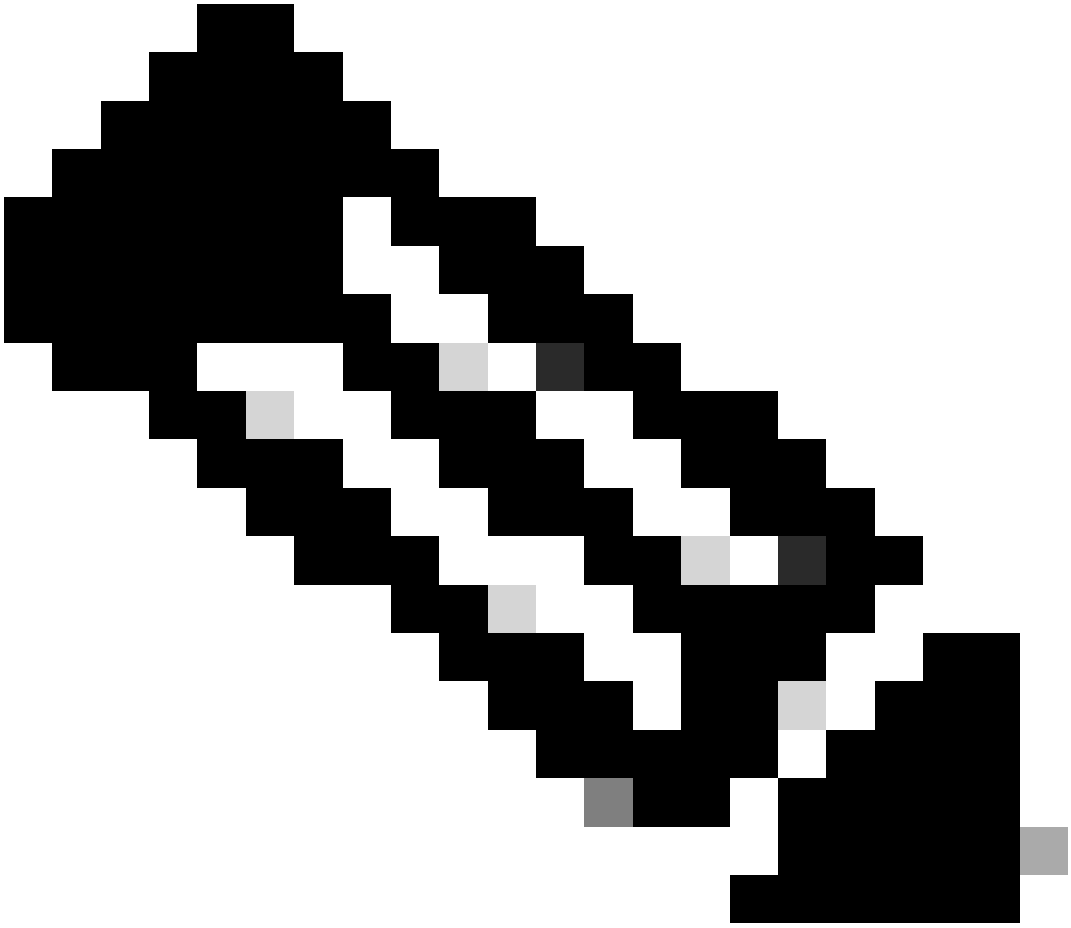
したがって、ドメインベースのバイパスの場合、CSC SWGは、リスト内のドメインをIPアドレスに変換し、クライアントマシン上のトラフィックと照合する方法を必要とします。このため、クライアントから送信されたDNSルックアップからDNSキャッシュを生成し、DNSキャッシュは外部ドメインリストのドメインに対応するIPアドレスをリストします

次に、SWGをバイパスするという決定が、これらのIPアドレスを宛先とする代行受信されたトラフィック（デフォルトでは80/443）に適用されます。

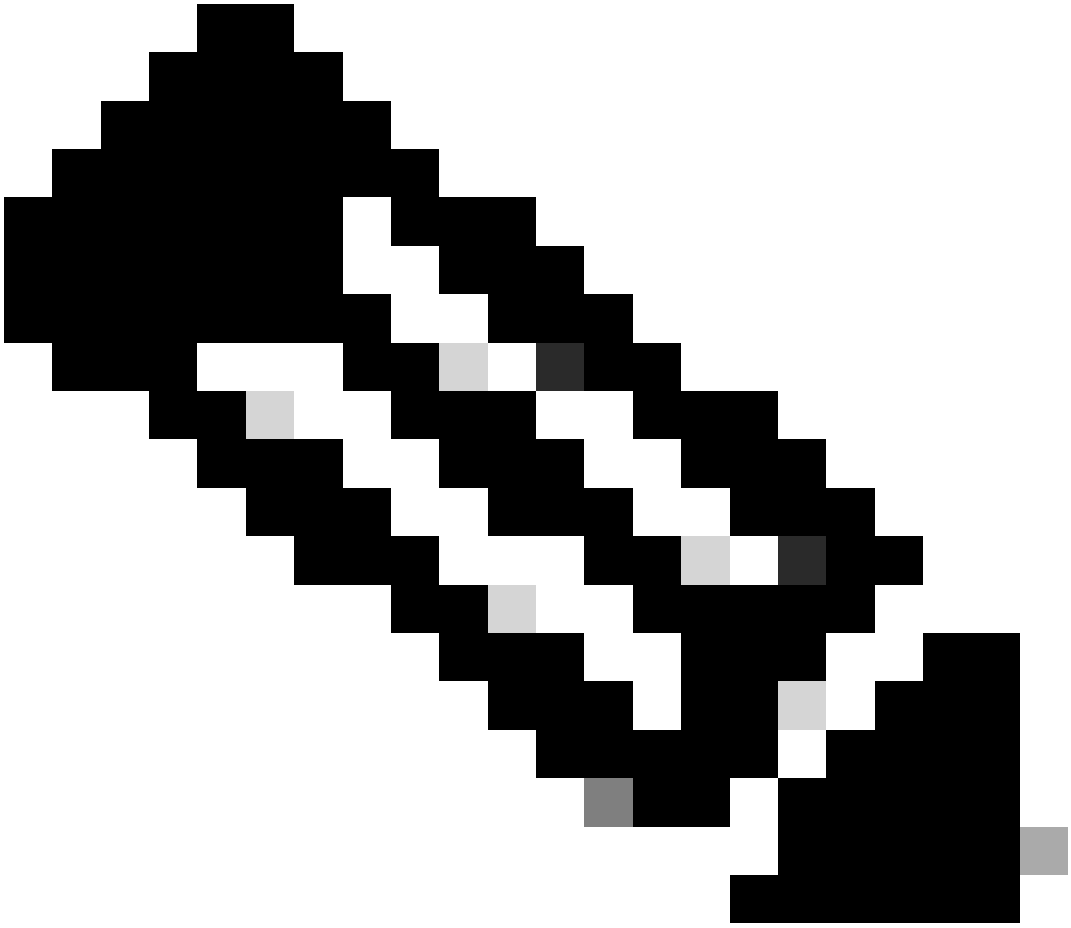
なぜこれが私にとって重要なのでしょうか？

これが原因で発生する可能性のある一般的な問題がいくつかあります。

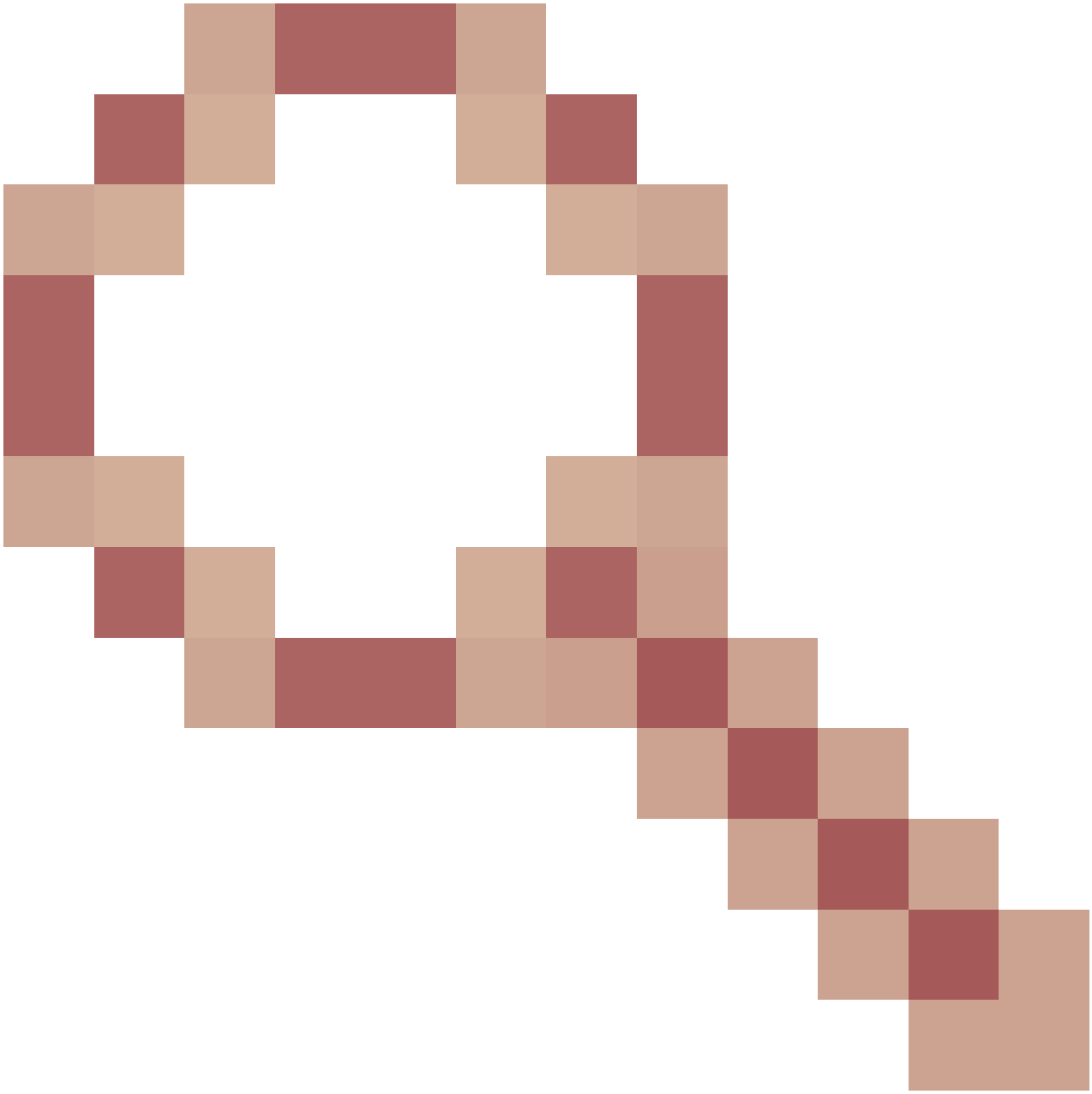
1. バイパスの決定が最終的にIPに基づくことを考えると、同じIPを共有する他のドメインのトラフィックもCisco Umbrellaからバイパスされるため、お客様はクライアントから直接送信される予期しないトラフィックを確認し、SWGポリシーが適用されていないか、アクティビティ検索に表示されません。
2. 何らかの理由でSWGモジュールがドメインのDNSルックアップを認識できない場合（のように、ドメインのlocalhost工ントリが存在する場合）、IPはキャッシュに追加されないため、トラフィックは予期せずSWGに送信されます。



注: KDFドライバはUDP DNSルックアップのみを監視します。何らかの理由でDNSルックアップがTCP経由で実行される場合、IPはキャッシュに追加されず、外部ドメインは適用されません。この問題は、Cisco Bug Searchで公開されています。



注:DNSがTCP(CSCwe48679



)（WindowsおよびMacOS）(Cisco Secure Client 5.1.4.74(MR4)

このプロセスをトラブルシューティングするにはどうすればよいですか。

DNSルックアップの監視、DNSキャッシュへのエントリの追加、およびIP宛のトラフィックへのバイパス(BYPASS)アクションの適用を行うSWGモジュールのプロセスは、KDFログで追跡できます。これには、KDFロギングが有効になっている必要があり、ログの冗長性のためにトラブルシューティングを行っている間は短時間だけ有効にできます。

KDFログエントリの例

DNSキャッシュに追加されるドメインのDNSルックアップ：

```
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接続が確認されました。ドメインが外部ドメインリストにありません。要求はSWG経由で送信されました：

```
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接続が検出されました。IPのエントリがキャッシュに見つかりました。バイパス操作が適用されました：

```
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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。