AnyConnect と OpenDNS ローミング クライアントとの相互運用

目次

概要

この資料はいくつかの現在の制限を記述したもので、AnyConnect および OpenDNS ローミング クライアントを作る利用可能な回避策は協力します。 Cisco カスタマは社内ネットワークにセキュアおよび暗号化された通信のための AnyConnect VPN クライアントに頼ります。 同様に、OpenDNS ローミング クライアントはユーザに安全に OpenDNS パブリックサーバの助けによって DNS サービスを利用する機能を与えます。 これらのクライアントは両方ともエンド ポイントにセキュリティ機能の豊富なセットを追加し、従ってそれらが互いに相互運用することは重要で

す。

前提条件

AnyConnect および OpenDNS ローミング クライアントの実際上の知識。

AnyConnect VPN に ASA または IOS/IOS-XE ヘッドエンド設定（トンネル グループ/グループ ポリシー）を行った場合習熟度。

要件

次の項目に関する知識が推奨されます。

- ASA または IOS/IOS-XE ヘッドエンド
- AnyConnect VPN クライアントおよび OpenDNS ローミング クライアントを実行するエンドポイント

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- リリース 9.4 を実行する ASA ヘッドエンド
- Windows 7
- AnyConnect クライアント 4.2.00096
- OpenDNS ローミング クライアント 2.0.154

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

OpenDNS は利用可能であるために Cisco AnyConnect チームとの AnyConnect プラグインを将来開発しています。 日付が設定されない間、この統合はローミング クライアントがアドレス指定された回避策なしで AnyConnect クライアントとはたらくことを可能にします。 これはまたローミング クライアントのための送達 機構であることを AnyConnect が可能にします。

機能

AnyConnect DNS 処理

VPN ヘッドエンドは AnyConnect クライアントからのトラフィックを処理するカップルさまざまな方法で設定することができます。

1. 完全なトンネル設定（トンネルすべての）: これは暗号化されるエンド ポイントからのすべてのトラフィックを VPN トンネルを渡って送信 されるために強制し従ってトラフィックは

クリアテキストで決してパブリックインターフェイス アダプタを出て行きません

2. スプリットトンネル設定:

a. トンネリングを分割含んで下さい: 特定のサブネットにだけ向かうトラフィックまたは VPN ヘッドエンドで定義されるホストはクリアテキストのトンネルの外部でトンネルを渡って、他のすべてのトラフィック送信 されます 送信 されます

b. トンネリングを分割除いて下さい: 特定のサブネットにだけ向かうトラフィックまたは VPN ヘッドエンドで定義されるホストは暗号化から除外され、クリアテキストにパブリックインターフェイスを残します、他のトラフィックはすべてトンネルを渡ってだけ暗号化され、送信 されます

これらの設定のそれぞれは DNS 解決が AnyConnect クライアントによってどのように処理されるか判別しますエンド ポイントのオペレーティング システムによって。 CSCuf07885 のための修正の後にリリース 4.2 の Windows のための AnyConnect の DNS 処理機構の動作に変更が、ずっとあります。

Windows 7+

トンネルすべての設定 (およびトンネルすべての DNS がイネーブルの状態で分割トンネリング)

前に AnyConnect 4.2:

グループ ポリシー (トンネル DNSサーバ) の下で設定される DNSサーバへの DNS 要求だけ許可されます。 AnyConnect ドライバは「そのようなネーム」応答の他のすべての要求に応答しません。 その結果、DNS 解決はトンネル DNSサーバを使用してしか実行されたことができません。

AnyConnect 4.2 +

あらゆる DNSサーバへの DNS 要求は VPN アダプタから起き、トンネルを渡って送信 される限り、許可されます。 他の要求はすべて「そのようなネーム」応答と応答されないし、DNS 解決は VPN トンネルでしか実行されたことができません

CSCuf07885 修正前に、AC はどのネットワークアダプタが DNS 要求を始めることができるか CSCuf07885 のための修正と、制限するどんなに、ターゲット DNSサーバを制限します。

分割含んで無し下さい設定 (ディセーブルにされるトンネルすべての DNS および分割DNS を)

AnyConnect ドライバはネイティブ DNS リゾルバと干渉しません。 従って、DNS 解決はネットワークアダプタの発注に基づいていました実行された、VPN が接続されるとき AnyConnect は好まれたアダプタ常にです。 従って DNS クエリはトンネルで最初に送信され、解決される得なければ、リゾルバはパブリックインターフェイスによってそれを解決するように試みます。 分割含 access-list はトンネル DNS サーバをカバーするサブネットを含まなければなりません。 AnyConnect 4.2 から開始して、トンネル DNS サーバのためのホスト ルーティングは AnyConnect クライアントによって自動的にように分割含んでいますネットワーク (ルーティン

グを保護して下さい）追加され、従って分割含 access-list はもはやトンネル DNSサーバ サブネットの明示的な付加を必要としません。

分割除いて無し下さい設定（ディセーブルにされるトンネルすべての DNS および分割DNS を）

AnyConnect ドライバはネイティブ DNS リゾルバと干渉しません。 従って、DNS 解決はネットワークアダプタの発注に基づいていました実行された、VPN が接続されるとき AnyConnect は好まれたアダプタ常にです。 従って DNS クエリはトンネルで最初に送信され、解決される得なければ、リゾルバはパブリックインターフェイスによってそれを解決するように試みます。 分割除 access-list はトンネル DNS サーバをカバーするサブネットを含むべきではありません。 AnyConnect 4.2 から開始して、トンネル DNS サーバのためのホスト ルーティングは分割除 access-list のミスコンフィギュレーションを防ぐ AnyConnect クライアントによって自動的にように分割含んでいますネットワーク（ルーティングを保護して下さい）、および従って追加されます。

分割DNS（ディセーブルにされるトンネルすべての DNS は設定されて分割含んでいます）

前に AnyConnect 4.2

分割DNS ドメインと一致する DNS 要求は DNSサーバをトンネル伝送することができますが他の DNSサーバに許可されません。 クエリが他の DNSサーバに送られる場合そのような内部 DNS クエリが「そのような名前」とトンネルをリークさせないことを、AnyConnect ドライバが応答する防ぐために。 つまり分割DNS ドメインはトンネル DNSサーバによって解決されますただ。

DNS はドメインが他の DNSサーバに許可される分割DNS の一致を、DNSサーバをトンネル伝送することができなくて要求します。 この場合、AnyConnect ドライバは「そのような名前」と非分割DNS ドメインのためのクエリがトンネルで試みられる場合応答しません。 そう非分割DNS ドメインはトンネルの外部の公共 DNSサーバによって解決されますただ。

AnyConnect 4.2 +

分割DNS ドメインと一致する DNS 要求はあらゆる DNSサーバに VPN アダプタから起きる限り、許可されます。 クエリがパブリックインターフェイスによって起きる場合ネーム・リゾリューションのためにトンネルを常に使用するためにリゾルバを強制するために、AnyConnect ドライバは「そのような名前と」応答しません。 つまり分割DNS ドメインはトンネルで解決されますただ。

DNS は物理的なアダプタから起きる限りドメインがあらゆる DNSサーバに許可される分割DNS の一致を要求します。 クエリが VPN アダプタによって起きる場合パブリックインターフェイスによってネーム・リゾリューションを常に試みるためにリゾルバを強制するために、AnyConnect は「そのような名前と」応答しません。 そう非分割DNS ドメインはパブリックインターフェイスによって解決されますただ。

Mac OS X

トンネルすべての設定（およびトンネルすべての DNS がイネーブルの状態で分割トンネリング

）

AnyConnect が接続されるとき、トンネル DNSサーバだけがシステム DNS 設定および従って維持されます DNS 要求でしかトンネル DNS サーバに送信 することができません。

分割含んで無し下さい設定（ディセーブルにされるトンネルすべての DNS および分割DNS を）

AnyConnect はネイティブ DNS リゾルバと干渉しません。 従ってトンネル DNSサーバは公共 DNSサーバに優先する好まれたリゾルバでネーム・リゾリューションのための最初の DNS 要求がトンネルに送信 されるようにします設定され。 DNS 設定が Mac OS X でグローバルであるので、DNS クエリが CSCtf20226 で文書化されているようにトンネルの外部の公共 DNSサーバを使用することは可能性のあるではないです。 AnyConnect 4.2 から開始して、トンネル DNS サーバのためのホスト ルーティングは AnyConnect クライアントによって自動的にように分割含んでいますネットワーク（ルーティングを保護して下さい）追加され、従って分割含 access-list はもはやトンネル DNSサーバ サブネットの明示的な付加を必要としません。

分割除いて無し下さい設定（ディセーブルにされるトンネルすべての DNS および分割DNS を）

AnyConnect はネイティブ DNS リゾルバと干渉しません。 従ってトンネル DNSサーバは公共 DNSサーバに優先する好まれたリゾルバでネーム・リゾリューションのための最初の DNS 要求がトンネルに送信 されるようにします設定され。 DNS 設定が Mac OS X でグローバルであるので、DNS クエリが CSCtf20226 で文書化されているようにトンネルの外部の公共 DNSサーバを使用することは可能性のあるではないです。 AnyConnect 4.2 から開始して、トンネル DNS サーバのためのホスト ルーティングは AnyConnect クライアントによって自動的にように分割含んでいますネットワーク（ルーティングを保護して下さい）追加され、従って分割含 access-list はもはやトンネル DNSサーバ サブネットの明示的な付加を必要としません。

分割DNS（ディセーブルにされるトンネルすべての DNS は設定されて分割含んでいます）

分割DNS が両方の IP プロトコル（IPv4 および IPv6）のためにイネーブルになっていればまたは 1 つのプロトコルのためだけにイネーブルになって、他のプロトコルのために設定されるアドレス プールがありません:
Windows と同様に、True split-DNS が適用されます。 本当分割DNS は分割DNS ドメインと一致する要求がトンネルでだけ解決されることを、リークしません意味しますトンネルの外部の DNSサーバに。

分割DNS が 1 つのプロトコルだけのためにイネーブルになっていればおよびクライアントアドレスが他のプロトコルに割り当てられれば、「分割トンネリングのための DNS フォールバックだけ」が実施されます。 これは AC トンネルで分割DNS ドメインと一致する割り当て DNS 要求だけ（公共 DNSサーバにフェールオーバーを強制する他の要求は「拒否された」応答の AC によって答えます）意味しますが、パブリックアダプターで、分割DNS ドメインと一致する要求が明白に送信 されないこと実施できません。

Linux

トンネルすべての設定（およびトンネルすべての DNS がイネーブルの状態で分割トンネリング

）

AnyConnect が接続されるとき、トンネル DNSサーバだけがシステム DNS 設定および従って維持されます DNS 要求でしかトンネル DNS サーバに送信 することができません。

分割含んで無し下さい設定（ディセーブルにされるトンネルすべての DNS および分割DNS を）

AnyConnect はネイティブ DNS リゾルバと干渉しません。 従ってトンネル DNSサーバは公共DNSサーバに優先する好まれたリゾルバでネーム・リゾリューションのための最初の DNS 要求がトンネルに送信 されるようにします設定され。

分割除いて無し下さい設定（ディセーブルにされるトンネルすべての DNS および分割DNS を）

AnyConnect はネイティブ DNS リゾルバと干渉しません。 従ってトンネル DNSサーバは公共DNSサーバに優先する好まれたリゾルバでネーム・リゾリューションのための最初の DNS 要求がトンネルに送信 されるようにします設定され。

分割DNS（ディセーブルにされるトンネルすべての DNS は設定されて分割含んでいます）

分割DNS がイネーブルになっている場合、「分割トンネリングのための DNS フォールバックだけ」が実施されます。 これは AC トンネルで分割DNS ドメインと一致する割り当て DNS 要求だけ（公共 DNSサーバにフェールオーバーを強制する他の要求は「拒否された」応答の AC によって答えます）意味しますが、パブリックアダプターで、分割DNS ドメインと一致する要求が明白に送信 されないこと実施できません。

OpenDNS ローミング クライアント

ローミング クライアントはエンド ポイントの DNS サービスを管理するで、DNS トラフィックを保護し、暗号化するのに OpenDNS 公共 DNSサーバを利用しますソフトウェア。

理想的には、クライアントは保護され、暗号化された状態にあるはずです。 ただし、クライアントが OpenDNS 公共リゾルバ サーバとの TLS セッションを設定することができなければ（208.67.222.222）、それは UDP ポート 53 で非暗号化 208.67.222.222 に DNS トラフィックを送信 するように試みます。 ローミング クライアントは OpenDNS の公共リゾルバ IP アドレス 208.67.222.222 を特に使用します（208.67.220.220 のような少数の他が、208.67.222.220、208.67.220.222）あり。 一度インストールされるローミング クライアントはローカルDNSサーバとして 127.0.0.1（localhost）をセットし、現在のインターフェースごとの DNS 設定を無効にします。 現在の DNS 設定はローミング クライアントコンフィギュレーション フォルダ内のローカル resolv.conf ファイルで（Windows で）保存されます。 OpenDNS は AnyConnect アダプタで学習されるそれらの DNSサーバをバックアップします。 たとえば、192.168.92.2 がパブリックアダプターの DNSサーバなら、OpenDNS は次の位置で resolv.conf を作成します:

C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf

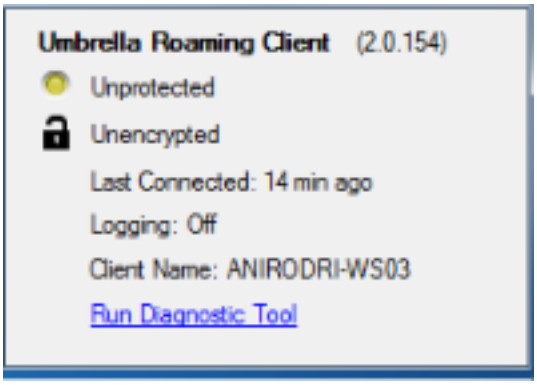
ネーム サーバ 192.168.92.2

ローミング クライアントは OpenDNS に設定された各パケットを暗号化します; ただし、それは 208.67.222.222 に暗号化トンネルを開始しませんし、使用しません。 ローミング クライアントに IP アドレスをブロックする非 DNS 目的で IPSec接続を開始するオプションの IPレイヤ適用機能があります。 これは AnyConnect アクティブな接続の前で自動的に無効に なります。 それはまた 127.0.0.1:53 にローカルでコンピュータで生成されるクエリを受信するために結合 します。 エンド ポイントが名前を変換する必要があるとき ローカル クエリは上書きするによる 127.0.0.1 に指示されそれからローミング クライアントの根本的な dnscrypt プロキシ プロセスは暗号化されたチャネル上の OpenDNS パブリックサーバにそれらを転送します。

DNS が 127.0.0.1:53 にフローすればことができない場合ローミング クライアントは機能できないし、次は発生します。 クライアントが公共 DNSサーバか 127.0.0.1:53 バインドされたアドレスに達することができない場合障害開いた状態に移行し、ローカルアダプタの DNS 設定を復元する。 バックグラウンドでは、それは信頼できる接続が回復される場合 208.67.222.222 にプローブを送信 し続け、アクティブ モードに移行できます。

制限事項

両方のクライアントの高レベル機能性を検知 して、それはローミング クライアントはローカル DNS 設定を変更し、セキュア チャネルを渡るクエリを転送するために 127.0.0.1:53 に結合 する機能がある必要があること明白です。 VPN が接続されるとき、AnyConnect がネイティブ DNS リゾルバと干渉しない唯一の設定は分割含分割除くためにであり、(分割トンネルすべての DNS がディセーブルの状態で)。 従ってローミング クライアントがまた使用中のとき、現在設定の 1 つを使用することを推奨します。 ローミング クライアントは無防備/非暗号化状態をトンネルすべての設定が使用されるか、または分割トンネルすべての DNS がイメージに示すようにイネーブルになっていれば、場合維持します。



回避策

インテントがローミング クライアント間の通信を保護することであり、VPN を使用して OpenDNS がサーバ トンネル伝送すれば、ダミーは VPN ヘッドエンドで access-list を使用することができます分割除きます。 これは完全なトンネル設定へ最も密接な事柄です。 そのような要件がない場合、access-list が OpenDNS パブリックサーバが含まれているところに access-list が OpenDNS パブリックサーバが含まれていない、または分割除きます使用することができます分割含んで下さいところに使用することができます。

これがローカル DNS 解決の損失という結果に終るのでローミング クライアントを使用した場合、分割DNS モードが使用することができない、さらに。 分割トンネルすべての DNS はまたディセーブルのままになるはずです; ただし、それは部分的にサポートされ、ローミング クライアントを暗号化された後フェールオーバーになることを許可する必要があります。

設定

トンネル OpenDNS トラフィック

この例は分割除 access-list でダミーの IP アドレスを使用します。 この設定によって、208.67.222.222 によってすべての通信は VPN トンネルを渡って起こり、ローミング クライアントは暗号化され、保護された状態で操作します。

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

VPN トンネルから OpenDNS トラフィックを除いて下さい

この例は分割除 access-list で OpenDNS リゾルバ アドレスを使用します。 この設定によって、208.67.222.222 によってすべての通信は VPN トンネルの外部で起こり、ローミング クライアントは暗号化され、保護された状態で操作します。

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

この例は内部 192.168.1.0/24 サブネットのための分割含設定を示したものです。 この設定によって、ローミング クライアントはまだ暗号化され、保護された状態で 208.67.222.222 へのトラフィックがトンネルで送信 されないので操作します。

```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#

Note: Split-tunnel-all-dns must be disabled in all of the  scenarios
```

確認

VPN が接続されるとき、ローミング クライアントはこのイメージに示すように保護され、暗号化されて示す必要があります: