DNS クエリに関する動作の違いおよび異なる OS でのドメイン名解決

目次

概要

このドキュメントでは、異なるオペレーティング システム（OS）がドメイン ネーム システム（DNS）のクエリを処理する方法と、Cisco AnyConnect およびスプリット トンネリングまたは完全トンネリングによるドメイン ネーム解決への影響について説明します。

スプリット DNS 対標準 DNS

使用するときトンネリングを、そこにです DNS のための 3 つのオプション分割含んで下さい:

1. **分割DNS** - DNS クエリはでドメイン名と一致する、Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア設定されます（ASA）。 それらはトンネルを通って移動します（ASA で定義される DNSサーバに他はが、たとえば）。

2. ASA によって定義される DNSサーバへのトンネルすべて **DNS** だけ DNS トラフィックは許可されます。 この設定は、グループ ポリシーで設定されます。

3. **標準 DNS** - DNS クエリすべては ASA によって定義される DNSサーバを通って移動します。 否定応答の場合には、DNS クエリはまた物理的なアダプタで設定される DNSサーバに行くかもしれません。

注: split-tunnel-all-dns コマンドは、ASA バージョン 8.2(5) で初めて実装されました。 このバージョンよりも前は、スプリット DNS または標準 DNS のみが可能でした。

いずれの場合も、トンネルを通って移動するために定義される DNS クエリは ASA によって定義されるあらゆる DNSサーバに行きます。 ASA によって定義される DNSサーバがない場合 DNS 設定はトンネルのためにブランクです。 分割DNS を定義してもらわない場合 DNS クエリすべては ASA によって定義される DNSサーバに送られます。 ただし、この資料に説明がある動作は Operating System（OS）によって異なります。

注: クライアントの名前解決をテストするときに NSLookup を使用しないでください。 代わりに、ブラウザを利用するか、**ping コマンド**を使用してください。 これは NSLookup が OS の DNS リゾルバに依存しないためです。 AnyConnect は、特定のインターフェイスを介した DNS 要求を強制しませんが、スプリット DNS の設定によっては、これを許可したり拒否したりします。 DNS リゾルバに対し、要求について任意の受け入れ可能な DNS サーバの試行を強制するには、スプリット DNS のテストをドメイン名解決についてネイティブ DNS レゾルバに依存するアプリケーション（NLSLookup、Dig、および DNS 解決をアプリケーション自身で処理する類似のアプリケーションなどを除く、すべてのアプリケーション）でのみ実行することが重要です。

真のスプリット DNS とベスト エフォートのスプリット DNS

AnyConnect リリース 2.4 は本当分割DNS ではないし、レガシー IPSecクライアントにある分割 DNS フォールバック（最もよい努力 分割DNS）をサポートします。 要求が分割DNS ドメインと一致する場合、AnyConnect は要求が ASA にトンネル伝送されるようにします。 サーバがホスト名を解決できない場合、DNS リゾルバは処理を続行し、物理インターフェイスにマッピングされた DNS サーバに同じクエリを送信します。

一方では、要求が分割DNS ドメインのうちのどれも一致する、AnyConnect は ASA にそれをトンネル伝送しません。 その代わりに、AnyConnect は DNS 応答を作成することで、DNS リゾルバがフォールバックして、物理インターフェイスにマッピングされた DNS サーバにクエリを送信します。 この機能がスプリット DNS ではなく、スプリット トンネリング用の DNS フォールバックと呼ばれるのはこのためです。 AnyConnect は、スプリット DNS ドメインに対する要求のみがトンネリングされることを保証するだけではなく、ホスト名解決に対するクライアント OS の DNS リゾルバの動作も使用します。

こうすると、非公開ドメイン名が漏えいする可能性があるため、セキュリティ上の問題となります。 たとえば、ネイティブ DNS クライアントが公開 DNS サーバに対して非公開ドメイン名を求めるクエリを送信する可能性があります（特に、VPN DNS 名前サーバが DNS クエリを解決できなかった場合）。

Cisco バグ ID CSCtn14578（現行バージョン 3.0(4235) の時点では Microsoft Windows でのみ解

決されています）を参照してください。 ソリューションは本当分割DNS を設定します、一致する問い合わせ、VPN DNSサーバに許されます厳しく設定されたドメイン名を。 その他のすべてのクエリは、物理アダプタ上で構成されたものなど、他の DNS サーバでのみ許可されます。

Tunnel All と Tunnel All DNS

スプリット トンネリングが無効（**トンネルすべての**設定）である時、DNS トラフィックはトンネルで厳しく許可されます。 **すべての DNS** 設定（グループ ポリシーで設定される）、ある種のスプリット トンネリングと共に、トンネルを通して DNS ルックアップすべておよび DNS トラフィックを送信 する**トンネルは**トンネルで厳しく許可されます。

これはすべてのプラットフォームで一貫していますが、Microsoft Windows の場合は 1 つ、注意点があります。 **tunnel all** または **tunnel all DNS** が設定された場合、AnyConnect は、セキュア ゲートウェイ上で設定された DNS サーバへの DNS トラフィックのみ許可します（VPN アダプタに適用）。 これは、先に述べた真のスプリット DNS ソリューションと一緒に実装されたセキュリティの機能強化です。

これが問題となる場合（たとえば、DNS の更新/登録要求を、VPN DNS サーバ以外のサーバに送信する必要がある場合など）は、次の手順を実行します。

1. 現在の設定が **tunnel all** の場合、**split-exclude tunneling** を有効にします。 すべてのシングル ホスト、スプリット除外ネットワーク（リンクローカル アドレスなど）の使用を受け入れます。

2. **tunnel all DNS** がグループ ポリシーで設定されていないことを確認します。

AnyConnect バージョン 3.0(4235) で解決された DNS の性能問題

この Microsoft Windows で発生する問題は、以下の条件で最もよく見られます。

- ホーム ルータ設定によって、DNS および DHCP サーバに同じ IP アドレスが割り当てられる（AnyConnect により、DHCP サーバへの必要なルートが作成されます）。
- 大量の DNS ドメインがグループ ポリシーにある。
- **Tunnel-all** 設定が使用される。
- 名前解決は修飾されていないホスト名によって実行されます。これは、問い合わせされたホスト名に関係するものが試行されるまで、リゾルバは選択可能なすべての DNS サーバについて大量の DNS サフィクスを試す必要があることを意味します。

この問題は、AnyConnect がブロックする物理アダプタ経由で DNS クエリを送信しようとするネイティブ DNS クライアントが原因です（**tunnel-all** 設定を指定した場合）。 これは名前解決の遅延につながり、特に大量の DNS サフィックスがヘッドエンドにより送信される場合は重大な問題になる可能性があります。 DNS クライアントは肯定応答を受信するまで、すべてのクエリと選択可能な DNS サーバを調べる必要があるからです。

この問題は AnyConnect バージョン 3.0(4235) で解決されています。 詳細については、前述の真のスプリット DNS ソリューションの概要とともに、Cisco バグ ID CSCtq02141 および

CSCtn14578 を参照してください。

アップグレードが設定されます場合これらは可能性のある 回避策です:

- IP アドレスの **split-exclude tunneling** を有効にします。これにより、ローカル DNS 要求が物理アダプタ経由で送信されることが許可されます。 何らかのデバイスがリンクローカル サブネット **169.254.0.0/16** のいずれかのアドレスに対して VPN 経由でトラフィックを送信することはほとんどないため、このサブネットのアドレスを使用できます。 **split-exclude tunneling** を有効にした後、クライアント プロファイルまたはクライアント自身のローカル LAN アドレスを有効にし、**tunnel all DNS** を無効にしてください。

  ASA では、次の設定を変更してください。

  ```
  access-list acl_linklocal_169.254.1.1 standard permit host 169.254.1.1
  group-policy gp_access-14 attributes
  split-tunnel-policy excludespecified
  split-tunnel-network-list value acl_linklocal_169.254.1.1
  split-tunnel-all-dns disable
  exit
  ```

  クライアント プロファイルで、次の行を追加してください。

  ```
  <LocalLanAccess UserControllable="true">true</LocalLanAccess>
  ```

  また、AnyConnect クライアント GUI でこれをクライアントごとに有効にすることもできます。 [AnyConnect Preference] メニューに移動し、[Enable local LAN access] チェック ボックスをオンにします。

- 名前解決には、修飾されていないホスト名でなく、完全修飾ドメイン名（FQDN）を使用します。

- 物理インターフェイスの DNS サーバに別の IP アドレスを使用します。

異なる OS でのスプリット トンネリングの DNS

AnyConnect のスプリット トンネリング（スプリット DNS なし）と併用する場合、OS によって DNS 検索を処理する方法が異なります。 このセクションではこれらの相違点について説明します。

Microsoft Windows

Microsoft Windows システムでは、DNS 設定をインターフェイスごとに行います。 スプリット トンネリングが使用される場合、DNS クエリは VPN トンネル アダプタで失敗した後に、物理アダプタの DNS サーバへフォール バックできます。 スプリット DNS を使用しないスプリット トンネリングが定義された場合、外部 DNS サーバにフォールバックするため、内部および外部の両方の DNS 解決が機能します。

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 AnyConnect が好まれたアダプタ常にであるネットワークアダプタの発注に VPN が接続されるとき基づいていました実行された。 さらに、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が含まれています。 AnyConnect 4.2 から開始するために、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 AnyConnect が好まれたアダプタ常にであるネットワークアダプタの発注に VPN が接続されるとき基づいていました実行された。 さらに、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。 従って AnyConnect 4.2 から開始するために、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、分割除 access-list のミスコンフィギュレーションを防ぎます。

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

DNS 要求は、分割DNS ドメインと一致する 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。 従って、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 要求は他の DNSサーバに、分割DNS ドメインと一致する許可されますが、DNSサーバをトンネル伝送することができません。 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。 従って、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 +

DNS 要求はあらゆる DNSサーバに、分割DNS ドメインと一致する 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。 従って、分割DNS ドメインはトンネルで解決されますただ。

DNS 要求はあらゆる DNSサーバに、分割DNS ドメインと一致する物理的なアダプタから起きる限り許可されます。 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。 従って、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 OSx

Macintosh システムでは、DNS 設定はグローバルです。 スプリット トンネリングが使用されているものの、スプリット DNS は使用されない場合、DNS クエリはトンネル外部の DNS サーバに到達できません。 外部ではなく、内部でのみ解決できます。

これは Cisco バグ ID CSCtf20226 および CSCtz86314 に記載されています。 いずれの場合も、次の回避策によって問題が解決されるはずです。

- グループ ポリシーで外部 DNS サーバの IP アドレスを指定し、内部 DNS クエリに FQDN を使用します。
- 外部名がトンネルを介して解決可能である場合は、[Advanced] > [Split Tunneling] を選択して、グループ ポリシーで設定されている DNS 名を削除し、スプリット DNS を無効にします。これには、内部 DNS クエリに FQDN を使用する必要があります。

分割DNS ケースは AnyConnect バージョン 3.1 で解決されます。 ただし、次の条件のいずれかが満たされていることを確認する必要があります。

- スプリット DNS を両方の IP プロトコルに対して有効にする必要があります（Cisco ASA バ

ージョン 9.0 以降が必要）。

- スプリット DNS を 1 つの IP プロトコルに対して有効にする必要があります。 Cisco ASA バージョン 9.0 以降を実行している場合、他の IP プロトコルにクライアント バイパス プロトコルを使用します。 たとえば、アドレス プールがなく、**クライアント バイパス プロトコル**がグループ ポリシーで有効になっていることを確認します。 またバージョン 9.0 より早い ASA バージョンを実行したら、確認して下さい他の IP プロトコルのために設定されるアドレス プールがないことを。 これは、もう一方の IP プロトコルが IPv6 であることを意味します。

注: AnyConnect は、Macintosh OS X の **resolv.conf** ファイルを変更しませんが、 OS X 固有の DNS の設定を変更します。 Macintosh OS X は互換性のために resolv.conffile を最新状態で維持します。 scutil**----dns コマンド**を使用することにより、Macintosh OS X の DNS 設定を表示できます。

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。 トンネル DNSサーバは好まれたリゾルバで設定されます、従って公共 DNSサーバに優先する、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。 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 から開始するために、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。 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設定されます従ってネーム・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。 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 から開始するために、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 はトンネルの外部の DNSサーバに分割DNS ドメインが付いている一致がトンネルでだけ解決されるその要求を、リークしません意味します。

split-DNS が 1 つだけのプロトコルに対して有効になっており、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ている場合、split-tunneling 用の DNS フォールバックのみ適用されます。 これは AC トンネルで分割DNS ドメインと (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) 一致するが意味しましたり、明白に送信 されない 分割DNS ドメインとパブリックアダプターで一致する要求を実施できません割り当て DNS 要求だけ。

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。 トンネル DNSサーバは好まれたリゾルバで設定されます、従って公共 DNSサーバに優先する、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。

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。 トンネル DNSサーバは好まれたリゾルバで設定されます、従って公共 DNSサーバに優先する、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。

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 (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) 一致するが意味しましたり、明白に送信 されない 分割DNS ドメインとパブリックアダプターで一致するその要求を実施できません割り当て DNS 要求だけ。

iPhone

iPhone は Macintosh システムとはまったく異なるものであり、Microsoft Windows にも似ていま

せん。 スプリット トンネリングが定義されているものの、スプリット DNS は定義されていない場合、DNS クエリは、定義されているグローバル DNS サーバ経由で送信されます。 たとえば、スプリット DNS ドメイン エントリは内部解決のために必須です。 この動作は Cisco バグ ID CSCtq09624 に記載されており、Apple iOS AnyConnect クライアントのバージョン 2.5.4038 で修正されています。

> **注:** iPhone の DNS クエリは **.local ドメイン**を無視することに注意してください。 この問題については、Cisco バグ ID CSCts89292 に記載されています。 この問題はオペレーティング システムの機能が原因であることが、Apple のエンジニアによって確認されています。 これは設計による動作であり、変更されることがないことが Apple により確認されています。

関連情報

- CSCsv34395 - DHCP サーバへの FQDN のプロキシ実行のサポートを AnyConnect に追加する
- CSCtn14578：真のスプリット DNS をサポートする AnyConnect（フォールバックしない）
- CSCtq02141 - ISP DNS がパブリック IP と同じサブネットの場合の AnyConnect DNS の問題
- CSCtn14578：真のスプリット DNS をサポートする AnyConnect（フォールバックしない）
- CSCtf20226 - Mac でのスプリット トンネルを使用した AnyConnect DNS の動作を Windows と同じにする
- CSCtz86314 - Mac： スプリット DNS によるトンネル経由で DNS クエリが正しく送信されない
- CSCtq09624 - スプリット トンネリングを使用した AnyConnect iPhone DNS の動作を Windows と同じにする
- CSCts89292 - iPhone DNS への AC のクエリが .local domains を無視する
- Cisco IOS ファイアウォール
- テクニカル サポートとドキュメント – Cisco Systems