关于DNS查询的性能上的差异和在不同的Oss的域名解决方法

目录

简介

本文描述不同的操作系统(Oss)如何处理域名系统(DNS)查询和影响在域名解决方法与思科AnyConnect和分开或全双工隧道。

已分解与英文虎报DNS

当您使用时请已分解包括隧道，那里是DNS:的三个选项

1. **分割DNS** -匹配域名的DNS查询，在思科可适应安全工具(ASA)配置。他们通过通道移动例如(到在ASA定义的DNS服务器)，而其他不。

2. 对由ASA定义的DNS服务器的通道所有**DNS**唯一的DNS流量允许。此设置在组策略配置。

3. **英文虎报DNS** -所有DNS查询通过由ASA定义的DNS服务器移动。一旦否定答复， DNS查询

也许也去在物理适配器配置的DNS服务器。

注意：**已分解通道所有dns**命令是在ASA版本8.2(5)实现的第一。在此版本前，您可能只执行分割DNS或标准DNS。

在任何情况下，定义通过通道移动的DNS查询，去由ASA定义的所有DNS服务器。如果没有ASA定义的DNS服务器，则DNS设置为通道是空白的。如果不安排分割DNS定义，则所有DNS查询被发送到由ASA定义的DNS服务器。然而，在本文描述的行为可以是不同的，根据操作系统(OS)。

注意：当您测试在客户端时的名字解析请避免使用Nslookup。反而，请取决于在浏览器或请使用**ping命令**。这是因为Nslookup不依靠OS DNS解析程序。AnyConnect不通过一个某一界面强制DNS请求，然而允许它或拒绝它从属在分割DNS配置。为了强制DNS解析程序尝试请求的一个可接受DNS服务器，重要的是分割DNS测试用例如依靠域名解决方法的应用程序只执行(除了Nslookup、开掘和独自处理DNS解析的相似的应用程序的所有应用程序本地DNS解析程序)。

真与最佳效果分割DNS

AnyConnect版本2.4支持分割DNS Fallback (最佳效果分割DNS)，不是真的分割DNS和被找到在传统IPSec客户端。如果请求匹配分割DNS域， AnyConnect允许请求被建立隧道到ASA。如果服务器不能解析主机名， DNS解析程序继续并且发送同一查询到被映射对物理接口的DNS服务器。

另一方面，如果请求不匹配其中任一个分割DNS域， AnyConnect不建立隧道它到ASA。反而，它建立DNS答复，以便DNS解析程序后退并且发送查询到被映射对物理接口的DNS服务器。所以此功能没有呼叫分割DNS，然而DNS fallback分割隧道的。不仅AnyConnect保证瞄准分割DNS域仅的请求被建立隧道，它也取决于在主机名字解析的客户端OS DNS解析程序行为。

这提出安全性问题由于潜在的私有域名泄漏。例如，当VPN DNS名名称服务器不可能解决DNS查询，本地DNS客户端能特定发送一个私有域名的一查询到一个公共DNS服务器。

*参考*在仅Microsoft Windows CSCtn14578，当前解决的Cisco Bug ID，自版本3.0(4235)。解决方案实现真的分割DNS，配比的严格查询已配置的域名和允许到VPN DNS服务器。其他查询只允许到其他DNS服务器，例如在物理适配器配置的那些。

建立隧道所有并且建立隧道所有DNS

当分割隧道禁用(**通道所有**配置)， DNS流量通过通道严格允许。**通道所有DNS**配置(配置在组策略)通过通道发送流量通过通道严格允许的所有DNS查找，与某种分割隧道一起和DNS。

这在平台间是一致与在Microsoft Windows的一个警告：当所有**通道全部**或**建立隧道所有DNS**配置，AnyConnect严格允许DNS流量到在安全网关配置的DNS服务器(应用对VPN适配器)。这是与以前被提及的真的分割DNS解决方案一起实现的安全性增强。

在某些情况下如果这证明有问题(例如，必须发送DNS更新/注册请求到Non-VPN DNS服务器)，则请完成这些步骤：

1. 如果当前配置是**通道全部**，则enable (event)已分解**排除隧道**。所有单个主机，已分解排除网络是可接受为使用，例如链路本地地址。

2. 保证在组策略**建立隧道所有DNS没有**配置。

在AnyConnect版本3.0(4235)解决的DNS性能问题

在这些条件下此Microsoft Windows问题主要流行：

- 使用家庭路由器设置， DNS和DHCP服务器分配同样IP地址(AnyConnect创建必要路由对DHCP服务器)。
- 很大数量的DNS域在组策略。
- 使用通道**所有**配置。
- 名字解析由一个不符合条件的主机名执行，暗示解析程序必须尝试在所有的一定数量的DNS后缀可用的DNS服务器，直到那个与被查询的主机名有关尝试。

此问题归结于尝试通过物理适配器发送DNS查询， AnyConnect阻塞的本地DNS客户端(给通道**所有**配置)。这导致可以是重大的名字解析延迟，特别是如果很大数量的DNS后缀由头端推送。DNS客户端必须通过所有查询和联机DNS服务器走，直到它收到肯定答复。

此问题在AnyConnect版本3.0(4235)被解决。与介绍一起参考Cisco Bug ID CSCtq02141和CSCtn14578，对早先被提及的真的分割DNS解决方案，欲知更多信息。

如果升级不可能实现，则这些是可能的应急方案：

- Enable (event)已分解**排除**IP地址的**隧道**，允许本地DNS请求流经物理适配器。您能使用从linklocal子网**169.254.0.0/16的**一个地址，因为不太可能任何设备发送流量到在VPN的那些IP地址之一。在您启用已分解**排除隧道后**，请启用本地LAN访问在客户端配置文件或在客户端，并且禁用**通道所有DNS**。

  在ASA，请做这些配置更改：

  ```
  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
  ```

  在客户端配置文件，您必须添加此线路：

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

  您能也启用此根据在AnyConnect客户端GUI的一个每客户端基本类型。导航对**AnyConnect首选**菜单，并且检查**Enable (event)本地LAN访问**复选框。

- 请使用完全合格的域名(FQDN)而不是不够资格的主机名名字解析。
- 请使用一个不同的IP地址在物理接口的DNS服务器。

有分割隧道的DNS在不同的Oss

另外Oss把柄DNS搜索用不同的方式，当使用与分割隧道(没有分割DNS) AnyConnect。此部分描述那些差异。

Microsoft Windows

在Microsoft Windows系统上， DNS设置单个接口的。如果使用分割隧道， DNS查询能下跌回到物理适配器DNS服务器，在他们在VPN通道适配器后失效。如果没有分割DNS的分割隧道定义，则内部和外部DNS解析工作，因为下跌回到外部DNS服务器。

有在行为上的一个变化在AnyConnect的DNS处理机制Windows的，在版本4.2在CSCuf07885的修正以后。

Windows 7+

通道所有配置(和分割隧道用启用的通道所有DNS)

前AnyConnect 4.2 ：

对根据组政策配置的DNS服务器的仅DNS请求(通道DNS服务器)允许。AnyConnect驱动程序回答与“没有这样命名”答复的其他请求。结果，使用通道DNS服务器， DNS解析可能只执行。

AnyConnect 4.2 +

只要他们起源于VPN适配器和在通道间，发送对所有DNS服务器的DNS请求允许。其他请求响应与“没有这样命名”答复，并且DNS解析可能通过VPN通道只执行

在CSCuf07885修正之前， AC限制目标DNS服务器，然而以CSCuf07885的修正，限制哪些网络适配器可以启动DNS请求。

已分解包括配置(禁用的通道所有DNS和split-dns)

AnyConnect驱动程序不干涉本地DNS解析程序。所以， DNS解析执行根据大约AnyConnect总是首选的适配器的网络适配器，当VPN连接时。而且， DNS查询通过通道首先被发送，并且，如果没获得解决，解析程序尝试通过公共接口解决它。已分解包括access-list包括包括通道DNS服务器的子网。从AnyConnect 4.2要启动，通道DNS服务器的主机路由由AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且已分解包括access-list不再要求通道DNS服务器子网的明确新增内容。

已分解排除配置(禁用的通道所有DNS和split-dns)

AnyConnect驱动程序不干涉本地DNS解析程序。所以， DNS解析执行根据大约AnyConnect总是首选的适配器的网络适配器，当VPN连接时。而且， DNS查询通过通道首先被发送，并且，如果没获得解决，解析程序尝试通过公共接口解决它。已分解排除access-list不应该包括包括通道DNS服务器的子网。从AnyConnect 4.2要启动，通道DNS服务器的主机路由由AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且防止在已分解排除的误配置access-list。

Split-dns (禁用的通道所有DNS，已分解包括已配置的)

前AnyConnect 4.2

DNS请求，配比与split-dns域允许建立隧道DNS服务器，但是没有允许到其他DNS服务器。如果查询被发送到其他DNS服务器，要防止这样内部DNS查询泄漏通道， AnyConnect驱动程序回应“没有这样名称”。所以， split-dns域可以只是解决的通过通道DNS服务器。

DNS请求，不配比与split-dns域允许到其他DNS服务器，但是没有允许建立隧道DNS服务器。如果非split-dns域的一查询通过通道，尝试在这种情况下， AnyConnect驱动程序回应“没有这样名称”。所以，非split-dns域可以只是解决的通过公共DNS服务器通道的外部。

AnyConnect 4.2 +

DNS请求，配比与split-dns域允许到所有DNS服务器，只要他们起源于VPN适配器。如果查询由公共接口产生， AnyConnect驱动程序回应“没有这样名称”强制解析程序总是使用通道名字解析。所以， split-dns域可以只是解决的通过通道。

DNS请求，不配比与split-dns域允许到所有DNS服务器，只要他们起源于物理适配器。如果查询由VPN适配器产生， AnyConnect回应“没有这样名称”强制解析程序通过公共接口始终尝试名字解析。所以，非split-dns域可以只是解决的通过公共接口。

Mac OSx

在Macintosh PC机系统上， DNS设置全局。如果使用分割隧道，但是没有使用分割DNS，到达DNS服务器在通道外面DNS查询是不可能的。您能只解决内部地，不外部。

这在Cisco Bug ID CSCtf20226和CSCtz86314描述。在两种情况下，此应急方案应该解决问题：

- 根据组策略指定一个外部DNS服务器IP地址并且请使用FQDN内部DNS查询。
- 如果外部名称通过通道是可解决，则请导航对**先进>分割隧道**并且通过在组策略配置DNS名的删除禁用分割DNS。这要求使用内部DNS查询的FQDN。

分割DNS盒在AnyConnect版本3.1被解决。然而，您必须保证一个这些情况符合：

- 必须为两个IP协议启用分割DNS，要求Cisco ASA版本9.0或以上。
- 必须为一个IP协议启用分割DNS。如果运行Cisco ASA版本9.0或以上，则请使用客户端旁路协议另一个IP协议。例如，请保证没有地址池，并且**客户端旁路协议**在组策略启用。或者，如果运行早于版本9.0的ASA版本，请保证没有为另一个IP协议配置的地址池。这暗示另一个IP协议是IPv6。

注意：AnyConnect不更换在Macintosh OS X的**resolv.conf文件**，然而相当更改OS X特定DNS设置。Macintosh OS X保持resolv.conffile当前为兼容性原因。请使用scutil**--dns发出命令**为了查看在Macintosh OS X的DNS设置。

通道所有配置(和分割隧道用启用的通道所有DNS)

当AnyConnect连接时，只有通道DNS服务器在系统DNS配置并且DNS请求维护能只发送到通道DNS服务器。

已分解包括配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置，当首选的解析程序，优先于公共DNS服务器，因而保证初始DNS要求名字解析在通道发送。因为DNS设置是全局在Mac OS X，使用公共DNS服务器通道的外部如提供在CSCtf20226上DNS查询是不可能的。从AnyConnect 4.2要启动，通道DNS服务器的主机路由由AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且已分解包括access-list不再要求通道DNS服务器子网的明确新增内容。

已分解排除配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置，当首选的解析程序，优先于公共DNS服务器，因而它保证初始DNS要求名字解析在通道发送。因为DNS设置是全局在Mac OS X，使用公共DNS服务器通道的外部如提供在CSCtf20226上DNS查询是不可能的。从AnyConnect 4.2要启动，通道DNS服务器的主机路由由AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且已分解包括access-list不再要求通道DNS服务器子网的明确新增内容。

Split-dns (禁用的通道所有DNS，已分解包括已配置的)

如果split-dns为两IP协议(IPv4和IPv6)启用或为一份协议只启用，并且没有为另一份协议配置的地址池：
真的split-dns，类似于Windows，被强制执行。真的split-dns含义与split-dns域的匹配通过通道只是解决的该请求，他们没有漏到DNS服务器通道的外部。

如果split-dns为一份协议只启用，并且客户端地址为另一份协议分配，只有**分割隧道的DNS fallback**被强制执行。这意味着AC只允许通过通道匹配split-dns域的DNS请求(其他请求由与“拒绝的”答复的AC应答强制故障切换到公共DNS服务器)，但是不能强制执行配比与split-dns域无危险没有发送，通过公共适配器的请求。

Linux

通道所有配置(和分割隧道用启用的通道所有DNS)

当AnyConnect连接时，只有通道DNS服务器在系统DNS配置并且DNS请求维护能只发送到通道DNS服务器。

已分解包括配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置，当首选的解析程序，优先于公共DNS服务器，因而保证初始DNS要求名字解析在通道发送。

已分解排除配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置，当首选的解析程序，优先于公共DNS服务器，因而保证初始DNS要求名字解析在通道发送。

Split-dns (禁用的通道所有DNS，已分解包括已配置的)

如果split-dns启用，只有**分割隧道的DNS fallback**被强制执行。这意味着AC只允许配比与split-dns域通过通道的DNS请求(其他请求由与"拒绝的"答复的AC应答强制故障切换到公共DNS服务器)，但是不能强制执行配比与split-dns域无危险没有发送，通过公共适配器的该请求。

IP电话

IP电话是Macintosh PC机系统的完整对面并且不类似于Microsoft Windows.如果分割隧道定义，但是分割DNS没有定义，则DNS查询通过定义的全局DNS服务器退出。例如，分割DNS域条目对于内部解决方法是必需的。此行为在Cisco Bug ID CSCtq09624在Apple iOS AnyConnect客户端的版本2.5.4038描述和修复。

> **注意**：注意IP电话DNS查询忽略**.local域**。这在Cisco Bug ID CSCts89292描述。苹果公司工程师确认问题由OS的功能导致。这是设计的行为，并且苹果公司确认那里是它的没有更改。

相关信息

- CSCsv34395 -添加支持在代理的AnyConnect FQDN到DHCP服务器
- CSCtn14578 -支持真的分割DNS的AnyConnect;不是fallback
- CSCtq02141 - AnyConnect DNS问题，当ISP DNS在相同子网作为公有IP
- CSCtn14578 -支持真的分割DNS的AnyConnect;不是fallback
- CSCtf20226 -做有分割隧道行为的AnyConnect DNS Mac的同windows一样
- CSCtz86314 - Mac ：通过通道没不正确地被发送的DNS查询用分割DNS
- CSCtq09624 -做AnyConnect有分割隧道行为的IP电话DNS同Windows一样
- CSCts89292 - IP电话DNS查询的AC忽略.local域
- Cisco IOS 防火墙
- 技术支持和文档 - Cisco Systems