检查DNS查询和域名解析的行为

目录

简介

先决条件

- 要求
- 使用的组件

分割与标准DNS

- 测试DNS — 重要信息

True与尽力而为拆分DNS

Tunnel-all和Tunnel-all DNS

- 全通道DNS和思科安全客户端Umbrella模块

AnyConnect版本3.0(4235)中已解决的DNS性能问题

- 解决方法（如果无法升级）

在不同客户端操作系统上使用分割隧道的DNS

- Microsoft Windows（Windows 10和Windows 11）
  - 全隧道配置（和启用全隧道DNS的分割隧道）
  - Split-include配置（禁用全DNS隧道，不拆分DNS）
  - Split-exclude Configuration（禁用所有DNS隧道，不启用拆分DNS）
  - Split-DNS（禁用所有DNS隧道，已配置拆分 — 包含）
  - 使用分割排除隧道的分割DNS（安全客户端5.x）
  - Windows上的加密DNS(DoH/DoT)
- macOS
  - 全隧道配置（和启用全隧道DNS的分割隧道）
  - Split-include / Split-exclude（禁用所有DNS隧道，无拆分DNS）
  - Split-DNS（禁用所有DNS隧道，已配置拆分 — 包含）
- Linux
  - 全隧道配置（和启用全隧道DNS的分割隧道）
  - Split-include / Split-exclude（禁用所有DNS隧道，不拆分DNS）
  - Split-DNS（禁用所有DNS隧道，已配置拆分 — 包含）
  - Linux VM和容器
- Apple iOS（iPhone和iPad）

动态分割隧道和DNS（安全客户端4.5+）

历史客户端版本（参考）

相关Bug信息

相关信息

修订历史纪录

文档应用于

简介

本文档介绍客户端操作系统如何处理DNS查询，以及使用Cisco IOS®安全客户端对域名解析的影响。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。实验示例使用Windows、macOS、Linux和Apple iOS上的安全防火墙ASA/FTD组策略和Cisco安全客户端。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

分割与标准DNS

本文档介绍客户端操作系统如何处理DNS查询，以及在使用具有拆分或全隧道的Cisco安全客户端（以前称为Cisco AnyConnect）时对域名解析的影响。所讨论的VPN头端包括思科安全防火墙ASA和FTD（以前称为ASA）；除非另有说明，否则组策略设置（例如split-dns、dns-server和split-tunnel-all-dns）适用于这两者。

如果部分明确引用了较早的客户端版本，则适用于安全客户端4.2及更高版本（包括当前安全客户端5.x版本）中描述的行为。Cisco AnyConnect 4.x已停产；迁移到Cisco安全客户端，以获得支持的DNS和隧道功能。

DNS解析行为取决于三个因素：

- VPN DNS策略：在头端上配置（拆分DNS、全隧道DNS或标准DNS）

- 分割隧道模式：Tunnel-all、split-include或split-exclude
- 客户端操作系统：DNS解析器架构（每个接口与全局）

当您运行split-include隧道命令时，以下是组策略中可用的三个DNS选项：

模式	描述
分割DNS	与头端上配置的域名(split-dns)匹配的DNS查询通过隧道发送到VPN DNS服务器(dns-server)。 所有其他查询都使用客户端操作系统解析器和物理适配器DNS服务器。
全通道DNS	只允许发往前端定义的DNS服务器的DNS流量。在组策略中配置了split-tunnel-all-dns enable。
标准DNS	所有DNS查询首先发送到由头端定义的VPN DNS服务器。在否定（NXDOMAIN或无响应）响应时，解析程序还可以尝试使用物理适配器上的DNS服务器。



注意：split-tunnel-all-dns命令首先在ASA版本8.2(5)中实施。 在此版本之前，只有拆分DNS或标准DNS可用。在所有情况下，定义为通过隧道移动的DNS查询都会传递到头端定义的任何DNS服务器。如果在头端上未定义DNS服务器，则隧道的DNS设置为空。

如果未定义拆分DNS，则所有DNS查询都将发送到由头端定义的DNS服务器（受本文档后面介绍的操作系统特定行为的约束）。 但是，本文档中描述的行为可能会因操作系统(OS)而异。

测试DNS — 重要信息



注意：在客户端上测试名称解析时，请避免使用NSLookup或dig。而应使用Web浏览器或运行ping命令。NSLookup和dig与大多数应用使用操作系统的DNS解析器末节的方式不同。安全客户端不会强制每个DNS请求通过特定接口；它根据拆分DNS和全通道DNS策略允许或拒绝请求。

要观察正确的故障切换行为，请仅对依赖本地操作系统DNS解析程序的应用程序（浏览器、ping和大多数业务应用程序）进行测试。 执行自身DNS解析的工具（NSLookup、dig和某些自定义应用）即使在客户端正常工作的情况下也会显示误导性故障。

True与尽力而为拆分DNS

AnyConnect版本2.4引入了分割DNS回退（尽力分割DNS），这不是真正的分割DNS，也可在传统IPsec客户端中找到。

尽力而为（回退）行为：

- 如果请求与拆分DNS域匹配，则安全客户端允许通过隧道将请求传送到前端。
- 如果VPN DNS服务器无法解析主机名，OS DNS解析器将继续，并且可以将相同的查询发送到物理接口上的DNS服务器。
- 如果请求与任何拆分DNS域都不匹配，则安全客户端不会通过隧道传输该请求。它可以合成响应，因此解析器会回退到物理接口DNS服务器。

这就是为什么传统功能称为拆分隧道的DNS回退，这不是真正的拆分DNS。安全客户端确保只有匹配的拆分DNS域查询才能进入隧道，但仍依赖操作系统解析程序行为进行最终解析。

安全问题:当VPN DNS服务器返回NXDOMAIN或解析失败时，私有域名会泄漏到公共DNS服务器；解析程序会重试物理适配器。

真正的拆分DNS:Cisco Bug ID CSCtn14578

在Microsoft Windows的AnyConnect 3.0(4235)中解决，并保留在Secure Client 4.2+中：

- 仅允许通过VPN路径（隧道DNS服务器/VPN适配器，具体取决于平台和版本）查询已配置的拆分DNS域。
- 所有其他查询仅允许通过非VPN DNS服务器（物理适配器）。



注意：只有注册的思科用户才能访问内部思科漏洞工具和详细的漏洞信息。

Tunnel-all和Tunnel-all DNS

当禁用分割隧道（tunnel-all配置）时，DNS流量将严格通过隧道进行允许。

tunnel-all-DNS配置（split-tunnel-all-dns enable在组策略中）通过隧道发送所有DNS查找，同时还配置了某种形式的拆分隧道，并且严格允许DNS流量通过隧道接口。

在Microsoft Windows上有一个警告的平台之间是一致的，当配置了tunnel-all或tunnel-all-DNS时，安全客户端会严格允许DNS流量流向安全网关上配置的DNS服务器（应用于VPN适配器）。 此安全增强通过真正的分离DNS实现。如果存在问题（例如，DNS更新/注册必须到达非VPN DNS服务器），请完成以下步骤：

1. 如果当前配置为tunnel-all，请启用split-exclude隧道。任何单主机拆分 — 排除网络都是可接受的，例如本地链路地址。
2. 确保组策略中未启用tunnel-all-DNS(split-tunnel-all-dns disable)。

全通道DNS和思科安全客户端Umbrella模块

当同时启用拆分隧道和隧道全DNS时，DNS会在内核级别被拦截，如果它没有传出正确的VPN接口，则会被拦截。在加密DNS不可用的网络中，安全客户端Umbrella模块（以前称为AnyConnect漫游安全）可能会受到影响。这是因为模块可以尝试通过LAN接口使用标准DNS，而tunnel-all-DNS需要通过VPN使用DNS。

默认情况下，Umbrella模块使用加密DNS（UDP端口443），它通常不会被tunnel-all-DNS阻止。问题主要出现在加密不可用和使用普通的DNS时。

建议：如果将tunnel-all-DNS与Umbrella模块配合使用，请将Cisco Umbrella解析器地址添加到拆分包含列表。或参阅为使用Umbrella模块的安全客户端启用所有DNS隧道文档(文档ID:224809。)

AnyConnect版本3.0(4235)中已解决的DNS性能问题

在以下情况下，此Microsoft Windows问题最为普遍：

- DNS和DHCP服务器共享同一IP地址的家庭路由器设置（安全客户端创建通向DHCP服务器的必要路由。）
- 组策略中有大量DNS后缀/域。
- tunnel-all配置。
- 名称解析使用不限定的主机名，因此，解析程序会尝试在所有可用的DNS服务器上使用多个DNS后缀。
- 本地DNS客户端尝试通过物理适配器发送DNS查询，安全客户端在tunnel-all下阻止该物理适配器。

这可能会导致严重的名称解析延迟，特别是在头端推送许多DNS后缀时。解析程序必须浏览后缀和服务器，直到收到肯定响应。

此问题在AnyConnect 3.0(4235)及更高版本的Secure Client中已解决。有关详细信息，请参阅Cisco Bug ID CSCtq02141和Cisco Bug ID CSCtn14578。

注意：只有注册的思科用户才有权访问内部思科漏洞工具。

解决方法（如果无法升级）

为IP地址启用切分 — 排除隧道，以便本地DNS可以使用物理适配器。来自本地链路子网169.254.0.0/16的地址通常用作通往这些地址的流量，不太可能通过VPN。

启用切分 — 排除隧道后，在客户端配置文件或客户端上启用本地LAN访问，并禁用tunnel-all-DNS。这是ASA/FTD配置示例：

```
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
```

客户端配置文件XML:

```
    true
```

也可以在安全客户端GUI中启用此功能：使用VPN启用允许本地(LAN)访问

1. 使用完全限定域名(FQDN)而不是非限定主机名。
2. 为物理接口上的DNS服务器使用不同的IP地址（与同一子网上的DHCP分开）。

在不同客户端操作系统上使用分割隧道的DNS

不同的客户端操作系统通过分割隧道（无分割DNS）以不同方式处理安全客户端的DNS;本节介绍这些差异。

Microsoft Windows（Windows 10和Windows 11）

在Windows上，DNS设置按网络接口进行。使用分割隧道，DNS查询在VPN隧道适配器上失败后，可以回退到物理适配器DNS服务器。如果使用拆分隧道而不使用拆分DNS，内部和外部解析都可以工作，因为解析程序可以回退到外部DNS服务器。在修复Cisco Bug ID CSCuf07885后，版本4.2中的Secure Client for Windows发生了重大更改。此行为在Secure Client 5.x中保持不变。



注意：只有注册的思科用户才有权访问内部思科漏洞工具。

全隧道配置（和启用全隧道DNS的分割隧道）

Pre-Secure Client 4.2（AnyConnect 4.1及更低版本）：

- 仅允许向组策略下配置的DNS服务器（隧道DNS服务器）发出DNS请求。
- 安全客户端驱动程序会响应所有其他无此类名称的请求。
- DNS解析只能使用隧道DNS服务器。

安全客户端4.2及更高版本：

- 允许发往任何DNS服务器的DNS请求，如果请求来自VPN适配器并通过隧道发送。
- 所有其他请求均未收到此类名称；仅通过VPN隧道进行解析。
- 在Cisco Bug ID CSCuf07885之前，安全客户端限制目标DNS服务器。此修复之后，它会限制哪些网络适配器可以启动DNS请求。

Split-include配置（禁用全DNS隧道，不拆分DNS）

安全客户端驱动程序不会干扰本地DNS解析程序。分辨率取决于网络适配器的顺序；连接VPN时，安全客户端是首选适配器。

DNS查询首先通过隧道发送；如果未解决，解析程序可以尝试使用公共接口。在4.2之前的版本中，拆分包含访问列表必须包括涵盖隧道DNS服务器的子网。从安全客户端4.2开始，隧道DNS服务器的主机路由会自动添加为拆分包含网络（安全路由），因此拆分包含的ACL不再需要显式隧道DNS服务器子网。

Split-exclude Configuration（禁用所有DNS隧道，不启用拆分DNS）

与拆分包含相同的解析程序行为，先建立隧道，然后是公共接口回退。split-exclude访问列表不得包含涵盖隧道DNS服务器的子网。 从安全客户端4.2开始，隧道DNS服务器的自动主机路由可防止常见的拆分 — 排除配置错误。

Split-DNS（禁用所有DNS隧道，已配置拆分 — 包含）

Windows上的拆分DNS需要拆分包含隧道（指定了拆分隧道策略隧道。）它不支持用于拆分DNS配置的仅拆分排除隧道策略。

预安全客户端4.2:

- 拆分DNS域查询：仅允许通过隧道传输DNS服务器；如果发送到其他服务器，则不会使用此类名称。
- 非拆分DNS域查询：仅允许到其他DNS服务器；如果尝试通过隧道，则不会使用此类名称。

安全客户端4.2及更高版本（在Windows上真正拆分DNS）:

- 拆分DNS域查询：仅当DNS服务器源自VPN适配器时才允许访问它们。来自公共接口的查询不会收到此类名称以强制使用隧道。
- 非拆分DNS域查询：仅允许来自物理适配器的DNS服务器访问。来自VPN适配器的查询不会收到此类名称以强制公共接口解析。

使用分割排除隧道的分割DNS（安全客户端5.x）

安全客户端5.x管理文档为拆分 — 排除配置添加拆分DNS。有关头端和策略要求，请参阅安全客户端5.x管理员指南 — 为分割排除隧道配置分割DNS。拆分DNS处于活动状态后，操作系统级实施规则仍然适用。

Windows上的加密DNS(DoH/DoT)

使用HTTPS DNS(DoH)或TLS DNS(DoT)的应用或操作系统功能可以绕过安全客户端过滤的Windows存根解析器路径。如果分离DNS对于特定应用似乎失败，但在浏览器中运行，请验证这些应用使用的是加密的DNS还是自定义的DNS。标准的拆分DNS测试应该使用操作系统解析器（浏览器、ping），而不是NSLookup/dig。

---

macOS

在macOS上，DNS设置是全局的（不是每个接口）。 如果使用拆分隧道而不使用拆分DNS，则DNS查询通常无法按预期到达隧道外部的DNS服务器，只能解析内部名称，而不能通过公共路径解析外部名称。Cisco Bug ID CSCtf20226和Cisco Bug ID CSCtz86314中记录了此错误。

解决方法:

- 在组策略下指定外部DNS服务器IP并将FQDN用于内部查询。
- 如果可以通过隧道解析外部名称，请通过从组策略中删除DNS名称在Advanced > Split Tunneling中禁用拆分DNS，并将FQDN用于内部查询。

从AnyConnect 3.1开始，MacOS上支持拆分DNS，但受以下条件限制：

- 为两个IP协议启用拆分DNS（需要ASA 9.0+/等效FTD），或；
- 为一个IP协议启用拆分DNS，为另一个IP协议启用客户端旁路协议，且没有绕过协议的地址池（或9.0之前的ASA版本上没有IPv6池）。

注意：安全客户端不主要通过macOS上的/etc/resolv.conf管理名称解析；配置操作系统级别的DNS设置。macOS可以保持resolv.conf更新以确保兼容性。运行scutil —dns以查看有

效的DNS配置。

全隧道配置（和启用全隧道DNS的分割隧道）

当连接安全客户端时，系统DNS配置中仅保留隧道DNS服务器；请求仅继续通过隧道DNS服务器。

Split-include / Split-exclude（禁用所有DNS隧道，无拆分DNS）

安全客户端不会干扰本地解析程序。隧道DNS服务器优先于公共解析器，因此第一次查询尝试通过隧道。由于DNS在macOS上是全局的，因此查询并不总是可靠地使用隧道外部的公共DNS(Cisco bug ID: CSCtf20226)。

从安全客户端4.2开始，隧道DNS服务器的主机路由会自动添加为安全路由。

Split-DNS（禁用所有DNS隧道，已配置拆分 — 包含）

真正拆分DNS（类似于Windows）适用于以下情况：

- 为IPv4和IPv6启用拆分DNS，或者；
- 为一个协议启用了拆分DNS，而另一个协议不存在客户端地址池。

真正的拆分DNS意味着匹配的拆分DNS域仅通过隧道进行解析，不会泄漏给外部解析程序。

如果只为一个协议启用了拆分DNS，而为另一个协议分配了客户端地址，则只实施拆分隧道的DNS回退：安全客户端允许通过隧道进行匹配查询（可以拒绝其他查询以强制故障切换），但无法完全防止通过公共适配器以明文形式发送的拆分DNS域查询的泄漏。

平台支持（安全客户端管理指南）：Windows和macOS支持完全拆分DNS。Linux的支持有限（请参见Linux部分）。

Linux

全隧道配置（和启用全隧道DNS的分割隧道）

当连接安全客户端时，系统DNS配置中仅维护隧道DNS服务器。

Split-include / Split-exclude（禁用所有DNS隧道，不拆分DNS）

安全客户端不会干扰本地解析程序。首选隧道DNS服务器；初始分辨率尝试通过隧道。

Split-DNS（禁用所有DNS隧道，已配置拆分 — 包含）

如果启用了拆分DNS，则在Linux上仅对拆分隧道实施DNS回退：

- 安全客户端允许通过隧道进行拆分DNS域查询。
- 其他查询可能会收到拒绝消息，以鼓励故障切换到公共DNS。
- 安全客户端无法完全实施拆分DNS域查询，因为它们从不通过公共适配器以明文形式发送。

安全客户端管理指南记录了Linux上的有限拆分DNS:只有通过隧道传输的DNS请求完全受分离DNS策略的制约；隧道外部的一些查询不符合分离DNS策略。

Linux VM和容器

安全客户端支持tunnel-from-any-source自定义属性，因此具有任何源地址的数据包可以在VM实例或Docker容器内以拆分包含或拆分排除模式进行路由。有关配置详细信息，请参阅《安全客户端5.x管理员指南》。

Apple iOS（iPhone和iPad）

iOS行为与macOS不同，与Windows不同。如果配置了拆分隧道而不使用拆分DNS，则DNS查询通常使用为设备定义的全局DNS服务器，而不是与Windows相同的回退模式。

实际影响:在使用不带拆分DNS的分割隧道时，通常需要使用拆分DNS域条目来进行可靠的内部名称解析。

历史修正：Cisco Bug ID CSCtq09624 —（适用于iOS 2.5.4038及更高版本的AnyConnect。）当前用于iOS的安全客户端遵循相同的一般要求；在使用拆分包括/拆分和排除时，为内部域配置拆分DNS，而不依赖Windows风格的回退。

注意：iOS DNS查询忽略.local域(Cisco bug ID CSCts89292。)

苹果视之为设计行为；不要期望通过iOS上的标准拆分DNS进行本地解析。在iOS上，当拆分隧道与某些拆分DNS列表配置结合使用时，安全客户端拆分DNS行为也与其他平台不同。对于iOS特定策略组合（split-dns none、default-domain等），请参阅《安全客户端管理员指南》中的“使用拆分隧道进行拆分DNS解析的行为”部分。

动态分割隧道和DNS（安全客户端4.5+）

动态拆分隧道可在连接时或按需解析FQDN，并调整流向指定域的流量的路由和过滤器。这包括在隧道中或从隧道中排除，而不包含静态IP列表。

功能	描述
动态拆分排除	在应用程序解析这些名称时，会将域(example.com)从隧道中排除。
动态拆分包括	域动态包含在隧道中。
增强的动态拆分	结合使用优先级规则的包括/排除域列表（例如excluded example.com，但包括mail.example.com）。

动态分割隧道使用DNS解析来推动路由更改。它通过头端上的安全客户端自定义属性进行配置（例如dynamic-split-exclude-domains、dynamic-split-include-domains）。

动态拆分隧道适用于tunnel-all和split-exclude（动态排除）或split-include（动态包含）策略。它不会取代拆分DNS策略，但可以补充它：拆分DNS控制哪些查询通过隧道传送；动态分割隧道根据解析的名称控制哪些IP流量通过隧道传输。请参阅配置详细信息：配置动态分割隧道和《安全客户端5.x管理员指南》。

分割排除故障切换（安全客户端5.x）：当公共路径与分离排除目标无连接时，可选自定义属性SplitExcludeFailoverEnabled通过VPN路由流量。有关自定义属性设置，请参阅《管理员指南》。

历史客户端版本（参考）

下表仅适用于仍在运行过时客户端的旧部署：

version	相关性
AnyConnect 2.4	引入了尽力而为的分离DNS回退
AnyConnect 2.5(iOS)	Cisco Bug ID:CSCtq09624 iOS DNS协调
AnyConnect 3.0(4235)	在Windows上真正拆分DNS;DNS性能修复
AnyConnect 3.1(macOS)	具有IPv4/IPv6条件的拆分DNS支持
AnyConnect 4.2	思科漏洞ID:基于CSCuf07885适配器的实施；自动隧道DNS主机路由

在所有受支持的平台上部署Secure Client 5.x，以获得当前修复程序和功能。

相关Bug信息

注意：只有注册的思科用户才有权访问内部思科漏洞工具。

- 思科漏洞ID:CSCtn14578 — 真正的拆分DNS（非回退） — Windows，3.0(4235)+
- Cisco Bug ID: CSCtq02141 — 当ISP DNS与公共IP位于同一子网时的DNS延迟
- Cisco Bug ID:CSCuf07885 - Windows DNS:受适配器限制，而非目标服务器 — 4.2+
- Cisco Bug ID:CSCtf20226 - macOS拆分隧道DNS，与Windows不同
- Cisco Bug ID:CSCtz86314 - macOS拆分DNS查询不通过隧道发送
- Cisco Bug ID:CSCtq09624 - iOS拆分隧道DNS行为
- Cisco Bug ID:CSCts89292 - iOS忽略.local DNS域
- Cisco Bug ID:CSCsv34395 - DHCP服务器的FQDN代理支持

相关信息

- 检查DNS查询和域名解析的行为(Cisco.com) — 文档ID 116016
- Cisco Secure Client 5.x管理员指南 — 配置VPN访问/拆分DNS
- 配置ASA/AnyConnect动态拆分隧道 — 文档ID编215383
- 为使用Umbrella模块的安全客户端启用隧道所有DNS — 文档ID为224809
- AnyConnect和OpenDNS漫游客户端之间的互操作 — 文档ID信200395
- 思科技术支持和下载

修订历史纪录

修订版	日期	备注
4.0	2026年7月28日	全面实质性更新：安全客户端品牌、平台更新、动态拆分隧道、Umbrella/tunnel-all-DNS、输入错误和配置修复、纠正的相关链接
3.0	2024年5月23日	重新认证(Cisco.com)
1.0	2014年6月12日	首次公开发布

文档应用于

- 思科安全客户端（包括AnyConnect） — Windows、macOS、Linux、iOS
- 思科安全防火墙ASA和FTD远程访问VPN组策略

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。