检查DNS查询和域名解析的行为

目录

简介

本文档介绍Cisco OS®如何处理DNS查询以及使用Cisco AnyConnect和拆分或全隧道技术对域名解析的影响。

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。

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。

拆分与标准DNS

使用分离包括隧道时，对于域名系统(DNS)有以下三个选项：

1. 拆分DNS -在思科自适应安全设备(ASA)上配置与域名匹配的DNS查询。它们通过隧道（例如，到ASA上定义的DNS服务器），而其他服务器则不会。

2. Tunnel-all-DNS -仅允许到ASA定义的DNS服务器的DNS流量。该设置在组策略中配置。

3. 标准DNS -所有DNS查询都会通过ASA定义的DNS服务器。在否定响应的情况下，DNS查询还可以转到物理适配器上配置的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，您只能执行拆分DNS或标准DNS。

在任何情况下，定义为通过隧道传输的DNS查询都会转到由ASA定义的任何DNS服务器。如果ASA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查询都会发送到ASA定义的DNS服务器。但是，本文档中描述的行为可能因操作系统(OS)而异。

注意：在客户端上测试名称解析时，请避免使用NSLookup。请依赖浏览器或使用ping 命令。这是因为NSLookup不依赖于操作系统DNS解析器。AnyConnect不会通过特定接口强制DNS请求，但根据拆分DNS配置允许或拒绝该请求。要强制DNS解析器尝试使用可接受的DNS服务器处理请求，切记只有依靠本地DNS解析器进行域名解析的应用程序才能执行拆分DNS测试（除NSLookup、Dig和自己处理DNS解析的类似应用程序之外的所有应用程序）。

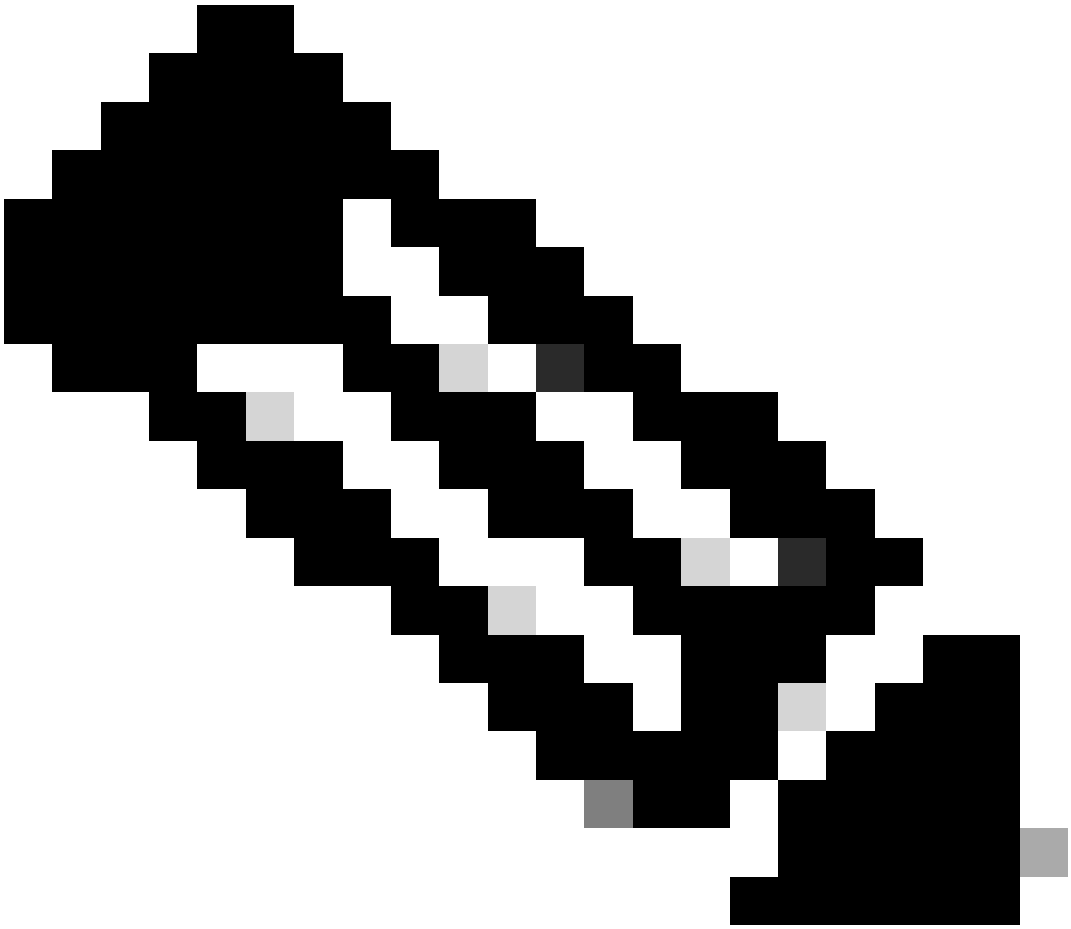
True与Best Effort Split DNS

AnyConnect版本2.4支持拆分DNS回退（尽力拆分DNS），这不是真正的拆分DNS，可在传统IPsec客户端中找到。如果请求与拆分DNS域匹配，则AnyConnect允许该请求通过隧道传输到ASA。如果服务器无法解析主机名，则DNS解析器将继续并向映射到物理接口的DNS服务器发送相同的查询。

另一方面，如果请求与任何拆分DNS域都不匹配，AnyConnect不会将其通过隧道连接至ASA。相反，它会构建DNS响应，以便DNS解析器回退并将查询发送到映射到物理接口的DNS服务器。因此，此功能不是称为拆分DNS，而是用于拆分隧道的DNS回退。AnyConnect不仅确保仅以目标拆分DNS域为目标的请求通过隧道传输，还依靠客户端操作系统DNS解析器行为进行主机名解析。

由于可能存在私有域名泄露，这引起了安全方面的担忧。例如，当VPN DNS域名服务器无法解析DNS查询时，本地DNS客户端可以向公共DNS服务器发送专用域名查询。

请参阅当前仅在Microsoft Windows上解决的思科漏洞ID CSCtn14578(自版本3.0(4235))。该解决方案实现了真正的分离DNS，它严格查询与VPN DNS服务器匹配并允许其访问的已配置域名。所有其他查询仅允许发往其他DNS服务器，例如物理适配器上配置的那些服务器。



注意：只有思科注册用户才能访问思科内部工具和信息。

全部使用隧道和全部使用隧道DNS

当禁用分割隧道(Tunnel-all配置)时，DNS流量严格限制通过隧道。全部使用隧道DNS配置（在组策略中配置）通过隧道发送所有DNS查找，以及某些类型的分割隧道，并严格允许DNS流量通过隧道。

这在Microsoft Windows的平台上所有平台之间是一致的，有一个警告：当配置任何Tunnel-all 或 Tunnel-all DNS 时，AnyConnect严格允许DNS流量流向安全网关（应用于VPN适配器）上配置的DNS服务器。这是与前面提到的真正拆分DNS解决方案一起实施的安全增强功能。

如果在某些情况下这证明是有问题的（例如，必须将DNS更新/注册请求发送到非VPN DNS服务器

），请完成以下步骤：

1. 如果当前配置是Tunnel-all，请启用split-exclude tunneling。任何单主机、拆分-排除网络均可使用，例如本地链路地址。

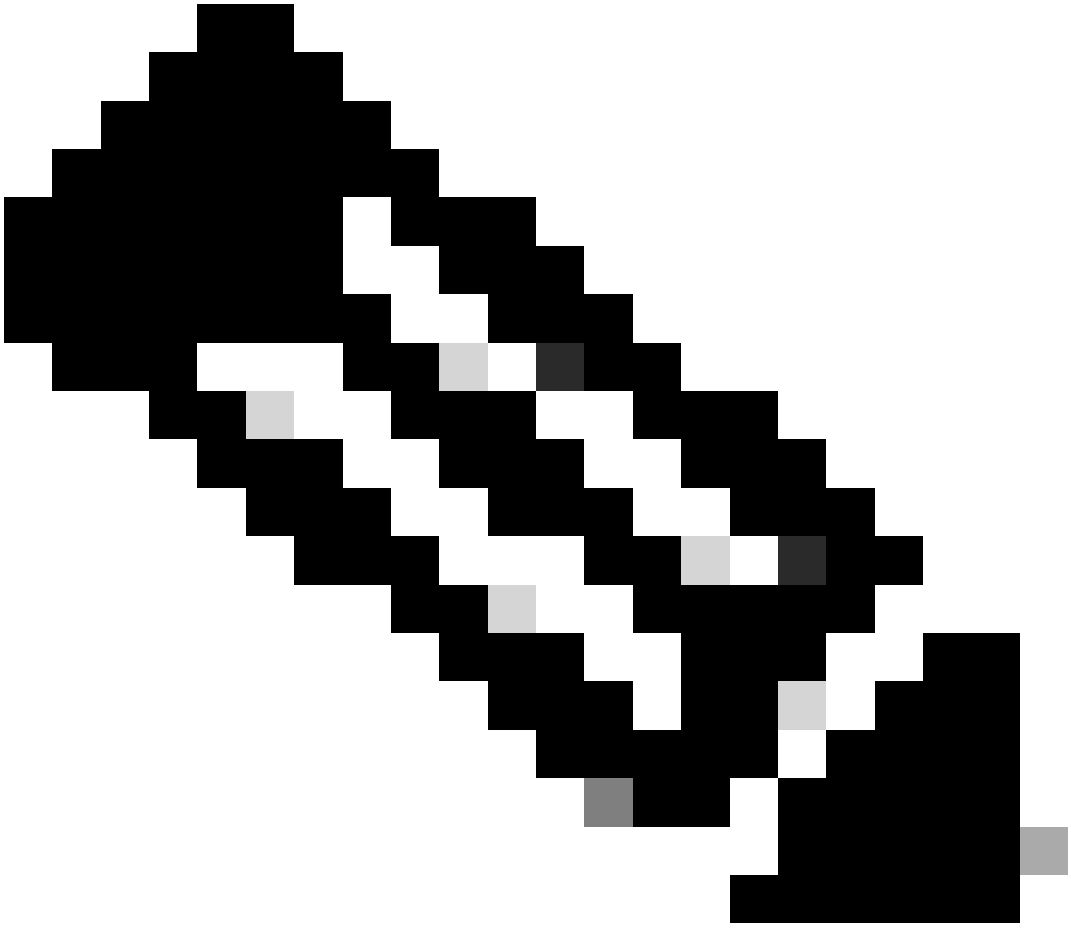
2. 确保组策略中没有配置全部隧道DNS。

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问题最常见：

- 设置家庭路由器后，DNS和DHCP服务器被分配相同的IP地址（AnyConnect创建通往DHCP服务器的必要路由）。
- 组策略中有大量DNS域。
- 使用的是Tunnel-all配置。
- 域名解析由不合格的主机名执行，这意味着解析程序必须在所有可用DNS服务器上尝试多个DNS后缀，直到尝试与查询的主机名相关的后缀。此问题是由于尝试通过物理适配器发送DNS查询的本地DNS客户端，AnyConnect会阻止该客户端(假设Tunnel-all 配置)。这会导致严重的名称解析延迟，尤其是在头端推送大量DNS后缀时。DNS客户端必须浏览所有查询和可用的DNS服务器，直到收到肯定响应。

此问题在AnyConnect版本3.0(4235)中已解决。有关详细信息，请参阅Cisco Bug ID CSCtq02141和Cisco Bug ID CSCtn14578，以及前面提到的真正分割DNS解决方案的简介。



注意：只有思科注册用户才能访问思科内部工具和信息。

如果无法实施升级，则可以采用以下解决方法：

- 为IP地址启用分离排除隧道，允许本地DNS请求通过物理适配器。您可以使用本地链路子网169.254.0.0/16中的地址，因为不可能有任何设备通过VPN将数据流发送到其中一个IP地址。启用split-exclude tunnelingd后，请在客户端配置文件上或客户端自身上启用本地LAN访问，并禁用Tunnel-all dDNS。

  在ASA上，进行以下配置更改：

```
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
```

在客户端配置文件中，必须添加以下行：

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

您还可以在AnyConnect客户端GUI中基于每个客户端启用此功能。导航到AnyConnect Preference菜单，然后选中Enable local LAN access 复选框。

- 对于名称解析，请使用完全限定域名(FQDN)，而不是非限定主机名。
- 在物理接口上为DNS服务器使用不同的IP地址。

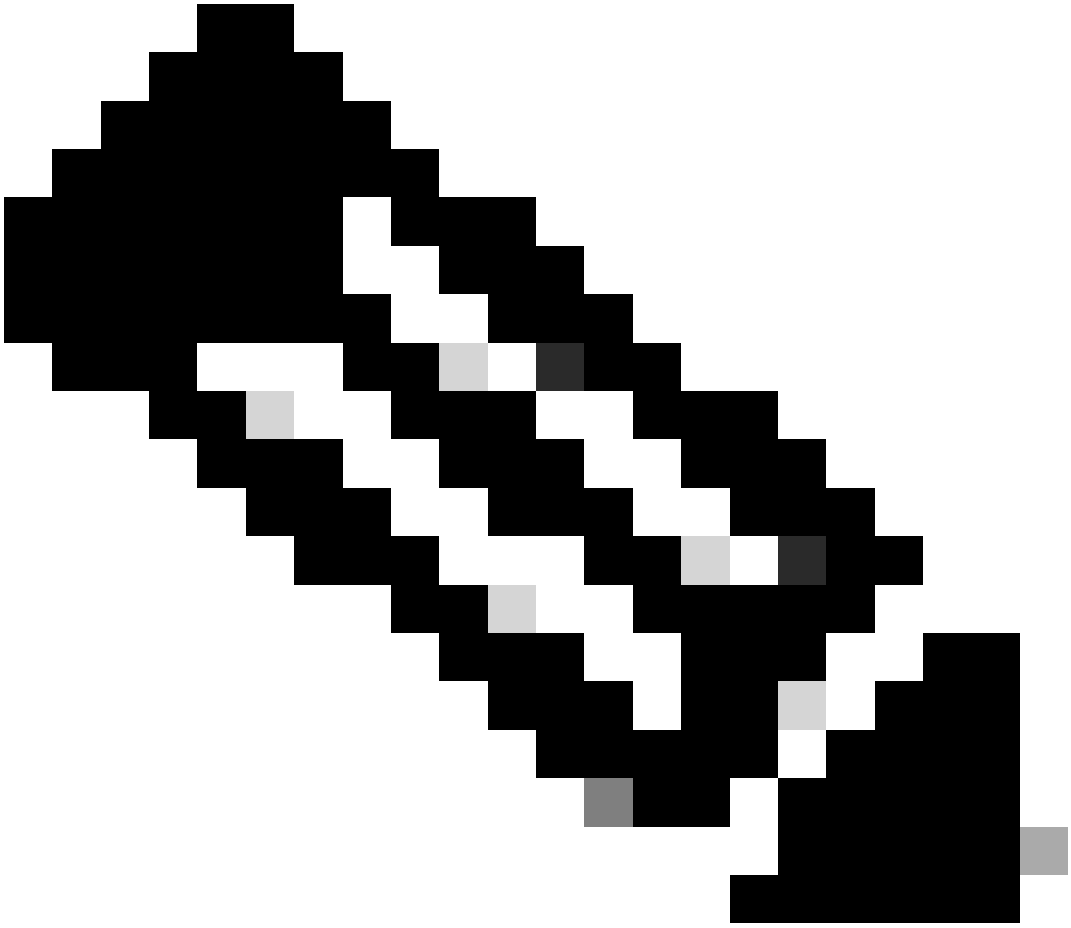
不同Cisco OS上使用分割隧道的DNS

当与AnyConnect的分割隧道（无分割DNS）配合使用时，不同的思科操作系统以不同方式处理DNS搜索。本节介绍这些差异。

Microsoft Windows

在Microsoft Windows系统上，DNS设置是按接口进行的。如果使用分割隧道，则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。如果定义了没有拆分DNS的分割隧道，则内部和外部DNS解析都会起作用，因为它会回退到外部DNS服务器。

在版本4.2中，在解决了思科漏洞ID CSCuf07885之后，在AnyConnect for Windows上处理此问题的DNS机制的行为发生了变化。



注意：只有思科注册用户才能访问思科内部工具和信息。

Windows 7+

全部使用隧道配置（以及启用了全部使用隧道DNS的分割隧道）

AnyConnect 4.2之前的版本：

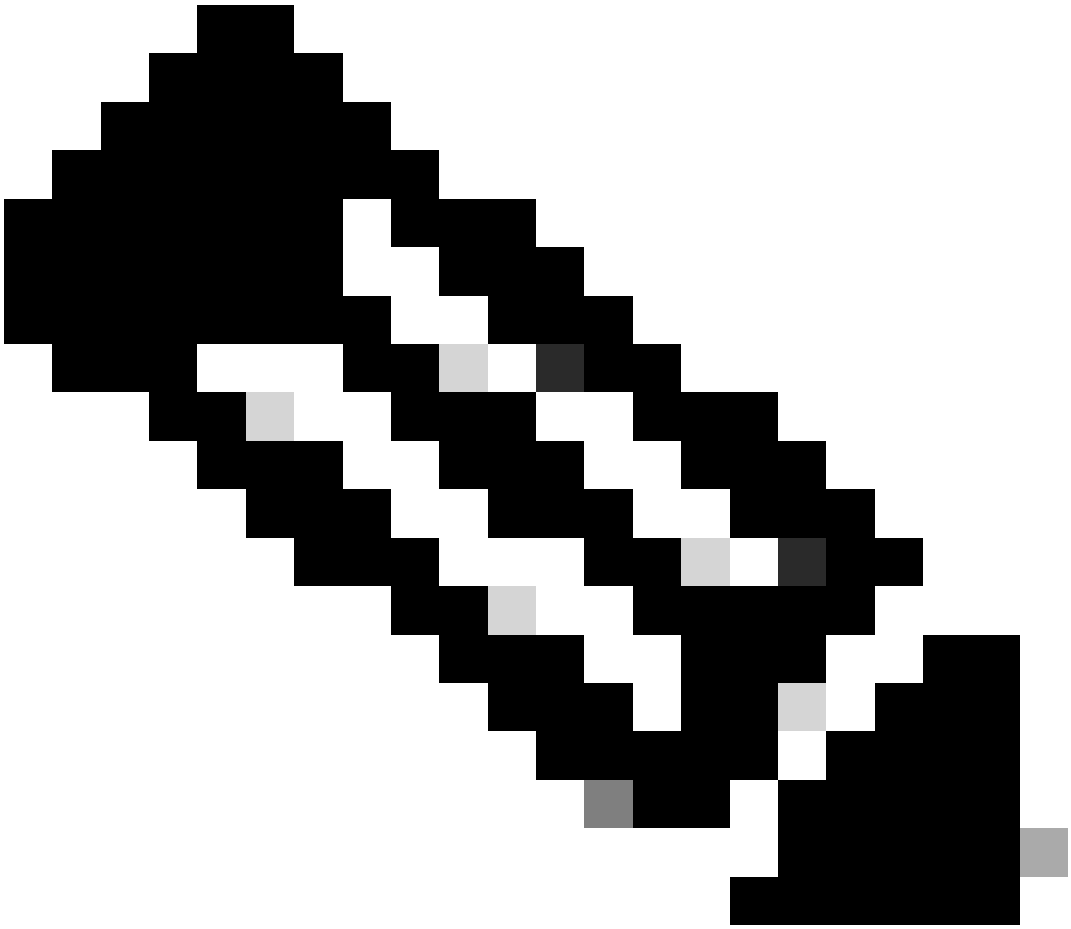
仅允许对组策略下配置的DNS服务器（隧道DNS服务器）的DNS请求。AnyConnect驱动程序使用“无此名称”响应来响应所有其他请求。因此，DNS解析只能通过隧道DNS服务器执行。

AnyConnect 4.2 +

允许发往任何DNS服务器的DNS请求，只要这些请求源自VPN适配器并通过隧道发送。所有其它请

求将以没有此类名称进行响应，并且DNS解析只能通过VPN隧道执行。

在修复思科漏洞ID CSCuf07885之前，AC限制目标DNS服务器，但通过修复此漏洞，它现在限制哪些网络适配器可以启动DNS请求。



注意：只有思科注册用户才能访问思科内部工具和信息。

拆分-包含配置（禁用所有DNS隧道，不拆分DNS）

AnyConnect驱动程序不干扰本地DNS解析器。因此，DNS解析是根据网络适配器的顺序执行的，其中AnyConnect在VPN连接时始终是首选适配器。此外，DNS查询首先会通过隧道发送，如果无法解析，解析程序会尝试通过公共接口解析它。拆分-包含访问列表包括涵盖隧道DNS服务器的子网。从AnyConnect 4.2开始，隧道DNS服务器的主机路由将由AnyConnect客户端自动添加为拆分包含网络（安全路由），因此，拆分包含访问列表不再需要显式添加隧道DNS服务器子网。

分离排除配置（禁用所有DNS隧道，不分离DNS）

AnyConnect驱动程序不干扰本地DNS解析器。因此，DNS解析是根据网络适配器的顺序执行的，其中AnyConnect在VPN连接时始终是首选适配器。此外，DNS查询首先会通过隧道发送，如果无法解析，解析程序会尝试通过公共接口解析它。split-exclude access-list不得包含涵盖隧道DNS服务器的子网。从AnyConnect 4.2开始，隧道DNS服务器的主机路由由AnyConnect客户端自动添加为分离包括网络（安全路由），从而防止分离排除访问列表中的错误配置。

Split-DNS（禁用所有DNS隧道，已配置split-include）

AnyConnect 4.2之前的版本

允许与拆分DNS域匹配的DNS请求通过DNS服务器隧道传输，但不允许传输至其他DNS服务器。为防止此类内部DNS查询泄漏隧道，如果查询发送到其他DNS服务器，AnyConnect驱动程序将以“无此名称”做出响应。因此，只能通过隧道DNS服务器解析拆分DNS域。

允许与拆分DNS域不匹配的DNS请求发送到其他DNS服务器，但不允许隧道传输DNS服务器。即使在这种情况下，如果通过隧道尝试查询非拆分DNS域，AnyConnect驱动程序也会以“无此名称”做出响应。因此，只能通过隧道外部的公共DNS服务器解析非拆分DNS域。

AnyConnect 4.2 +

允许与拆分DNS域匹配的DNS请求发送到任何DNS服务器，只要这些请求源自VPN适配器。如果查询由公共接口发起，AnyConnect驱动程序将以“no such name”做出响应，以强制解析程序始终使用隧道进行名称解析。因此，拆分DNS域只能通过隧道解析。

允许与分离dns域不匹配的DNS请求发送到任何DNS服务器，只要这些请求来自物理适配器。如果查询由VPN适配器发起，AnyConnect将以“no such name”做出响应，以强制解析器始终尝试通过公共接口解析名称。因此，只能通过公共接口解析非拆分dns域。

Mac OSx

在Macintosh系统上，DNS设置是全局的。如果使用分割隧道，但未使用分割DNS，则DNS查询无法到达隧道外部的DNS服务器。您只能在内部（而非外部）进行解析。

思科漏洞ID CSCtf20226和思科漏洞ID CSCtz86314中说明了这一点。在这两种情况下，此解决方法都必须解决以下问题：

- 在组策略下指定外部DNS服务器IP地址，并为内部DNS查询使用FQDN。
- 如果外部名称可以通过隧道进行解析，请导航到高级>分割隧道，并通过删除组策略中配置的DNS名称来禁用分割DNS。这要求内部DNS查询使用FQDN。

拆分DNS案例在AnyConnect版本3.1中已解决。但是，您必须确保满足以下条件之一：

- 必须为两个IP协议启用拆分DNS，这需要思科ASA 9.0版或更高版本。
- 必须为一个IP协议启用拆分DNS。如果运行的是Cisco ASA版本9.0或更高版本，请对其他IP协议使用客户端旁路协议。例如，请确保没有地址池并且已在组策略中启用客户端旁路协议。或者，如果您运行的ASA版本早于版本9.0，请确保没有为另一个IP协议配置地址池。这意味着另一个IP协议是IPv6。

注意：AnyConnect不会更改Macintosh OS X上的resolv.conf文件，而是更改特定于OS X的DNS设置。Macintosh OS X出于兼容性考虑，保持resolv.conf文件为最新版本。使用scutil —dns 命令可查看Macintosh OS X上的DNS设置。

全部使用隧道配置（以及启用了全部使用隧道DNS的分割隧道）

连接AnyConnect后，系统DNS配置中仅维护隧道DNS服务器，因此DNS请求只能发送到隧道DNS服务器。

拆分-包含配置（禁用所有DNS隧道，不拆分DNS）

AnyConnect不会干扰本地DNS解析器。隧道DNS服务器被配置为首选解析器，优先于公共DNS服务器，因此可以确保名称解析的初始DNS请求通过隧道发送。由于Mac OS X上的DNS设置是全局性的，因此DNS查询不可能使用隧道外的公共DNS服务器(如Cisco Bug ID CSCtf20226中所述)。从AnyConnect 4.2开始，隧道DNS服务器的主机路由将由AnyConnect客户端自动添加为拆分包含网络（安全路由），因此，拆分包含访问列表不再需要显式添加隧道DNS服务器子网。

分离排除配置（禁用所有DNS隧道，不分离DNS）

AnyConnect不会干扰本地DNS解析器。隧道DNS服务器被配置为首选解析器，它们优先于公共DNS服务器，因此可以确保名称解析的初始DNS请求通过隧道发送。由于Mac OS X上的DNS设置是全局性的，因此DNS查询不可能使用隧道外的公共DNS服务器(如Cisco Bug ID CSCtf20226中所述)。从AnyConnect 4.2开始，隧道DNS服务器的主机路由将由AnyConnect客户端自动添加为拆分包含网络（安全路由），因此，拆分包含访问列表不再需要显式添加隧道DNS服务器子网。

Split-DNS（禁用所有DNS隧道，已配置split-include）

如果为两个IP协议（IPv4和IPv6）都启用了拆分DNS，或者它只为一个协议启用，并且没有为另一个协议配置地址池：
系统将真正执行分离 DNS（与 Windows 相似）。真正的拆分DNS意味着与拆分DNS域匹配的请求仅通过隧道进行解析，而不会泄漏到隧道外部的DNS服务器。

如果只对一种 IP 协议启用分离 DNS，并且为另一种 IP 协议分配了客户端地址，则只会强制对分离

隧道执行 DNS 回退。这意味着AC仅允许通过隧道与拆分DNS域匹配的DNS请求（其他请求由AC以“拒绝”响应进行回复，以强制故障切换至公共DNS服务器），但无法通过公共适配器实施与未以明文形式发送的拆分DNS域匹配的请求。

Linux

全部使用隧道配置（以及启用了全部使用隧道DNS的分割隧道）

连接AnyConnect后，系统DNS配置中仅维护隧道DNS服务器，因此DNS请求只能发送到隧道DNS服务器。

拆分-包含配置（禁用所有DNS隧道，不拆分DNS）

AnyConnect不会干扰本地DNS解析器。隧道DNS服务器被配置为首选解析器，优先于公共DNS服务器，因此可以确保名称解析的初始DNS请求通过隧道发送。

分离排除配置（禁用所有DNS隧道，不分离DNS）

AnyConnect不会干扰本地DNS解析器。隧道DNS服务器被配置为首选解析器，优先于公共DNS服务器，因此可以确保名称解析的初始DNS请求通过隧道发送。

Split-DNS（禁用所有DNS隧道，已配置split-include）

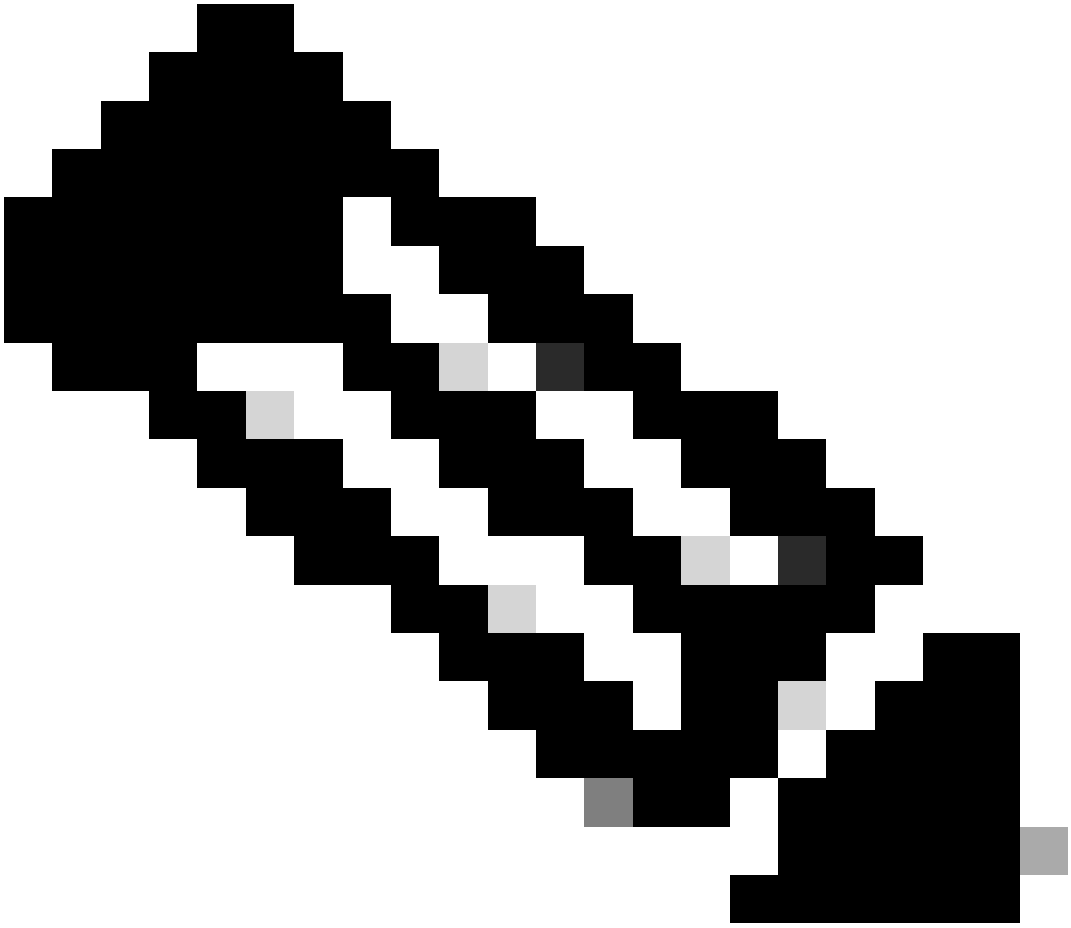
如果启用了拆分DNS，则仅强制实施拆分隧道的DNS后退。这意味着AC仅允许通过隧道与拆分DNS域匹配的DNS请求（其他请求由AC以“拒绝”响应进行响应，以强制故障切换至公共DNS服务器），但无法通过公共适配器实施与未以明文形式发送的拆分DNS域匹配的请求。

iPhone

iPhone与Macintosh系统完全相反，并且与Microsoft Windows不同。如果定义了分割隧道，但未定义分割DNS，则DNS查询将通过定义的全局DNS服务器退出。例如，拆分DNS域条目对于内部解析是必需的。此行为记录在Cisco bug ID CSCtq09624中，并在用于Apple iOS AnyConnect客户端的2.5.4038版中进行了修复。

注意：请注意，iPhone DNS查询ignore .local域。 思科漏洞ID CSCts89292中说明了这一点。Apple工程师确认问题是由操作系统的功能导致的。这是设计好的行为，苹果证实，它没有变化。

相关Bug信息



注意：只有思科注册用户才能访问思科内部工具和信息。

- 思科漏洞ID CSCsv34395 - AnyConnect中添加了对代理FQDN到DHCP服务器的支持
- 思科漏洞ID CSCtn14578 - AnyConnect支持真正拆分DNS；不退回
- 思科漏洞ID CSCtq02141 - ISP DNS与公共IP位于同一子网时的AnyConnect DNS问题
- 思科漏洞ID CSCtf20226 -使AnyConnect DNS具有与Windows相同的Mac拆分隧道行为
- 思科漏洞ID CSCtz86314 - Mac：DNS查询错误地未通过具有拆分DNS的隧道发送
- 思科漏洞ID CSCtq09624 -使AnyConnect iPhone DNS具有与Windows相同的拆分隧道行为
- 思科漏洞ID CSCts89292 - iPhone DNS查询的AC忽略.local域

相关信息

- Cisco IOS®防火墙
- 思科技术支持和下载

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）。