檢查DNS查詢和域名解析的行為

目錄

簡介

本文檔介紹Cisco OS®如何處理DNS查詢以及使用Cisco AnyConnect和分割或完全隧道解決方案對域名解析的影響。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

拆分與標準DNS

使用分離包括項通道時，下列是您網域名稱系統(DNS)的三個選項：

1. 拆分DNS -在思科自適應安全裝置(ASA)上配置與域名匹配的DNS查詢。它們透過隧道（例如，到ASA上定義的DNS伺服器），而其他伺服器則不通過。

2. Tunnel-all-DNS -僅允許發往ASA定義的DNS伺服器的DNS流量。這個設定是在群組原則中設定的。

3. 標準DNS -所有DNS查詢透過ASA定義的DNS伺服器。在否定回應的情況下，DNS查詢也可以移至實體介面卡上設定的DNS伺服器。

注意：split-tunnel-all-dns命令首先在ASA版本8.2(5)中實施。在此版本之前，您只能執行分割DNS或標準DNS。

在任何情況下，定義為透過隧道的DNS查詢都會轉到由ASA定義的任何DNS伺服器。如果ASA未定義DNS伺服器，則隧道的DNS設定為空。如果您未定義拆分DNS，則所有DNS查詢都將傳送到ASA定義的DNS伺服器。但是，本文檔中描述的行為可能會因作業系統(OS)而異。

注意：在客戶端上測試名稱解析時，請避免使用NSLookup。請依賴瀏覽器或使用ping 命令。這是因為NSLookup不依賴於作業系統DNS解析器。AnyConnect不會透過特定介面強制DNS請求，但根據拆分DNS配置允許或拒絕該請求。要強制DNS解析器嘗試可接受的DNS伺服器進行請求，必須僅對依賴本地DNS解析器進行域名解析的應用程式（例如，除NSLookup、Dig和自身處理DNS解析的類似應用程式之外的所有應用程式）執行拆分DNS測試。

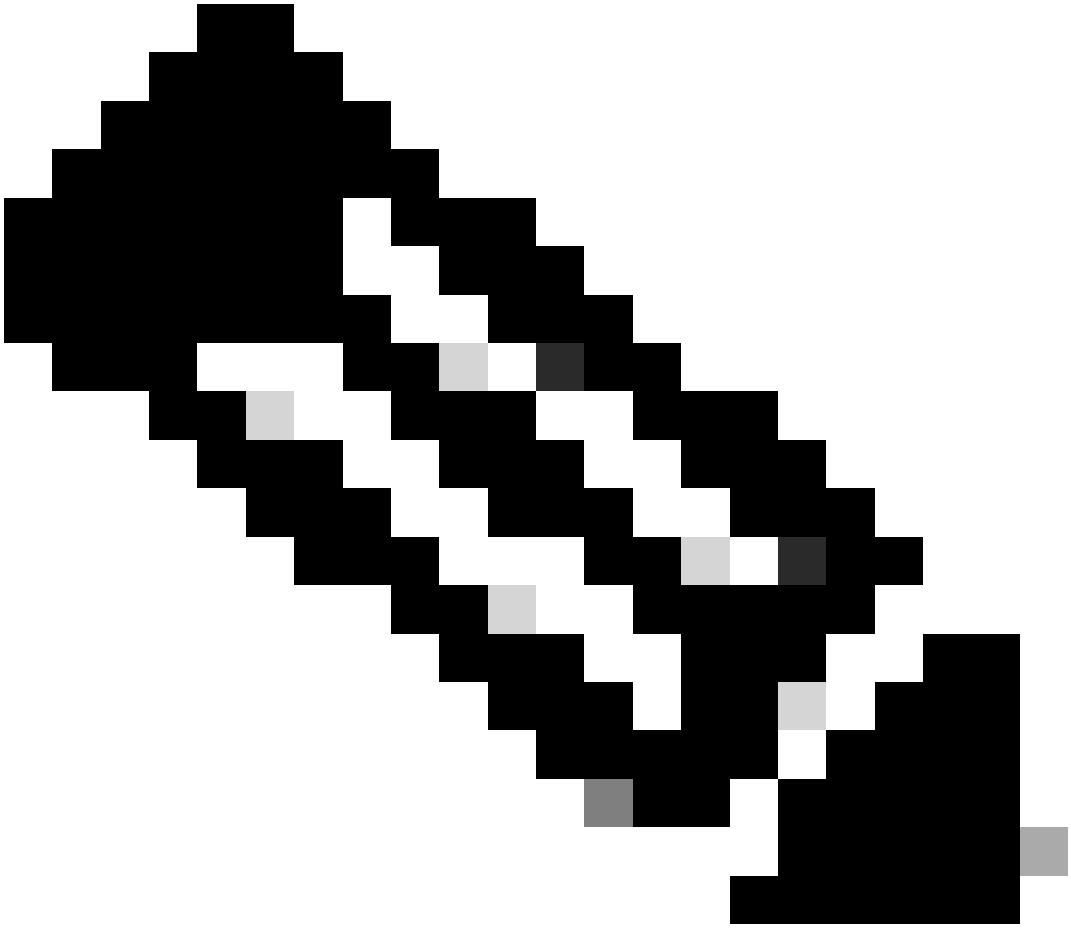
True與Best Effort Split DNS

AnyConnect 2.4版支援分割DNS後退（盡力分割DNS），這不是真正的分割DNS，可在傳統IPsec客戶端中找到。如果請求匹配拆分DNS域，則AnyConnect允許透過隧道將請求傳輸到ASA。如果伺服器無法解析主機名，則DNS解析器會繼續將相同的查詢傳送到對映到物理介面的DNS伺服器。

另一方面，如果請求與任何拆分DNS域都不匹配，則AnyConnect不會將其隧道連線到ASA。相反，它會構建DNS響應，以便DNS解析器回退，並將查詢傳送到對映到物理介面的DNS伺服器。因此，此功能不是稱為分割DNS，而是用於分割隧道的DNS後援。AnyConnect不僅確保只有目標分離DNS域的請求才能通過隧道連線，還依賴客戶端作業系統DNS解析器行為進行主機名解析。

這引起了安全方面的擔憂，因為可能存在私有域名洩漏。例如，本地DNS客戶端可以傳送私用域名查詢到公共DNS伺服器，特別是當VPN DNS名稱伺服器無法解析DNS查詢時。

請參閱當前僅在Microsoft Windows上解決的思科漏洞ID CSCtn14578(自版本3.0(4235)起)。該解決方案實現了真正的分離DNS，它嚴格查詢與VPN DNS伺服器匹配且允許其訪問的已配置域名。所有其他查詢僅允許到其他DNS伺服器，例如物理介面卡上配置的DNS伺服器。



附註：只有完成註冊的思科使用者有權存取思科內部工具與資訊。

全部使用隧道和全部使用隧道DNS

當停用分割隧道時(Tunnel-all 配置)，DNS資料流嚴格透過隧道允許。全部使用隧道DNS配置（在組策略中配置）透過隧道傳送所有DNS查詢，以及某種型別的分割隧道，並且嚴格允許DNS流量透過隧道。

在Microsoft Windows中，每個平台都存在一條警告：當配置任何全部使用隧道或全部使用隧道DNS時，AnyConnect會嚴格允許DNS流量流向安全網關（應用於VPN介面卡）上配置的DNS伺服

器。這是與前面提到的真正分離DNS解決方案一起實施的安全增強功能。

如果在某些情況下出現問題（例如，DNS更新/註冊請求必須傳送到非VPN DNS伺服器），請完成以下步驟：

1. 如果當前配置為Tunnel-all，則啟用split-exclude tunneling。任何單主機、拆分-排除網路都可被使用，例如本地鏈路地址。

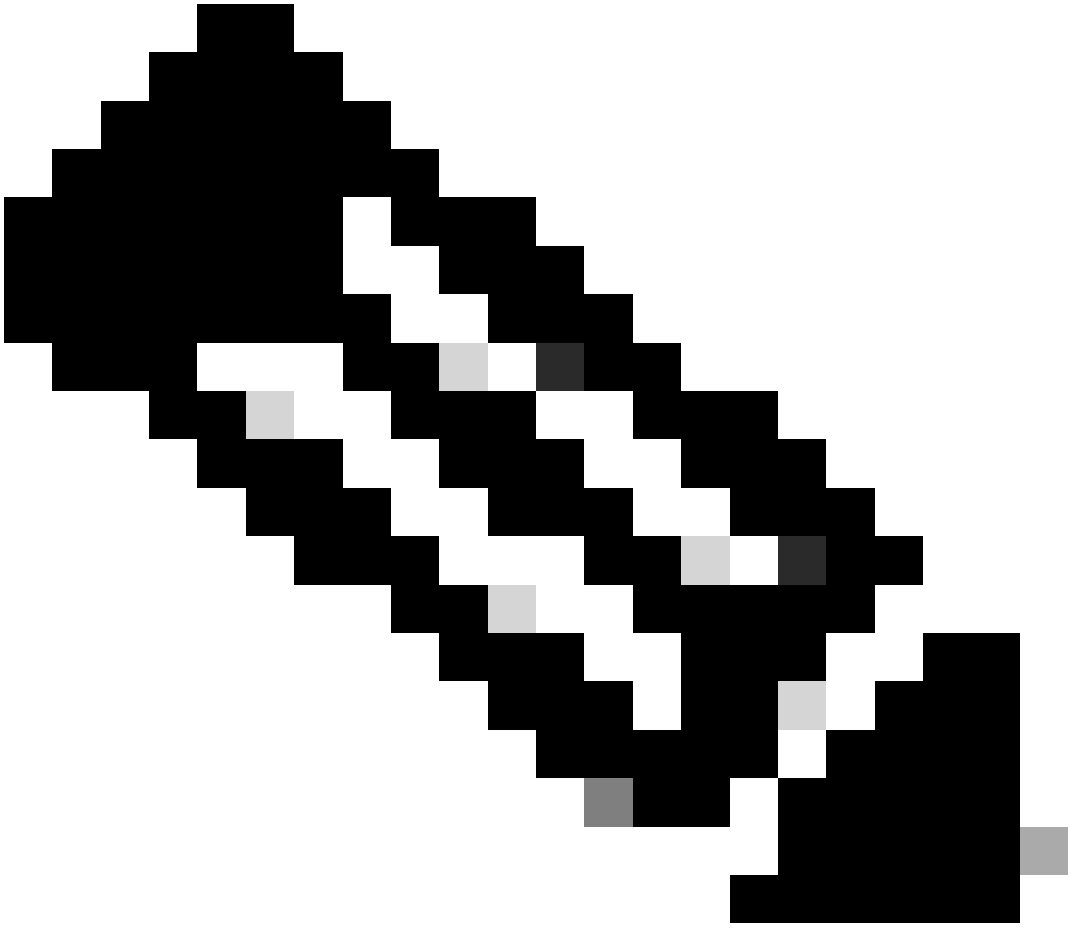
2. 請確保組策略中未配置Tunnel-all DNS。

AnyConnect版本3.0(4235)中已解決DNS效能問題

此Microsoft Windows問題在下列情況下最為普遍：

- 透過設定家庭路由器，DNS和DHCP伺服器被分配了相同的IP地址（AnyConnect會建立通往DHCP伺服器的必要路由）。
- 組策略中有大量DNS域。
- 使用了Tunnel-all配置。
- 名稱解析由不合格的主機名稱執行，這表示解析程式必須在所有可用的DNS伺服器上嘗試許多DNS尾碼，直到嘗試與查詢的主機名稱相關的伺服器為止。此問題是由於嘗試透過物理介面卡傳送DNS查詢的本地DNS客戶端引起的，AnyConnect會阻止物理介面卡(假設Tunnel-all配置)。這會導致嚴重的名稱解析延遲，尤其是在頭端推送大量DNS尾碼時。DNS客戶端必須瀏覽所有查詢和可用的DNS伺服器，直到收到肯定響應。

此問題已在AnyConnect版本3.0(4235)中解決。有關詳細資訊，請參閱思科漏洞ID CSCtq02141和思科漏洞ID CSCtn14578，以及前面提到的真正分離DNS解決方案的簡介。



附註：只有完成註冊的思科使用者有權存取思科內部工具與資訊。

如果無法實施升級，則可能的解決方法如下：

- 為IP地址啟用split-exclude tunneling，允許本地DNS請求透過物理介面卡。您可以使用linklocal子網169.254.0.0/16中的地址，因為不太可能有任何裝置透過VPN將資料流傳送到其中一個IP地址。啟用split-exclude tunnelingd後，在客戶端配置檔案上或客戶端自身上啟用本地LAN訪問，並停用Tunnel-all dDNS。

  在ASA上，進行以下配置更改：

```
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
```

在客戶端配置檔案上，必須增加以下行：

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

您也可以在AnyConnect客戶端GUI中針對每個客戶端啟用此功能。導航到AnyConnect Preference選單，然後選中Enable local LAN access覈取方塊。

- 使用完全限定域名(FQDN)而不是不限定的主機名進行名稱解析。
- 為物理介面上的DNS伺服器使用不同的IP地址。

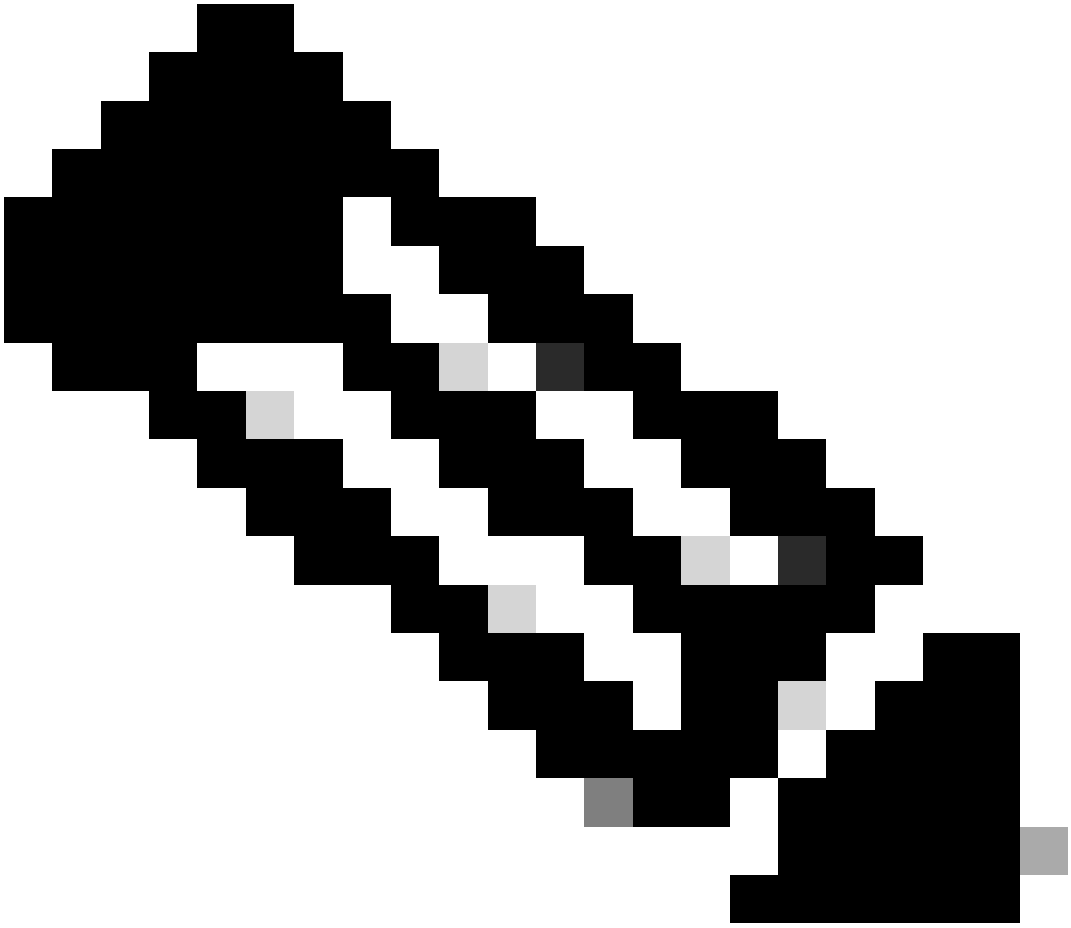
不同Cisco作業系統上使用分割通道的DNS

當用於AnyConnect的分割隧道（無分割DNS）時，不同的思科作業系統以不同方式處理DNS搜尋。本節將說明這些差異。

Microsoft Windows

在Microsoft Windows系統上，DNS設定是每個介面的。如果使用分割隧道，則DNS查詢可能會在VPN隧道介面卡上失敗後回退到物理介面卡DNS伺服器。如果定義了沒有分割DNS的分割隧道，則內部和外部DNS解析都會起作用，因為它會回退到外部DNS伺服器。

在修復思科漏洞ID CSCuf07885之後，版本4.2中處理AnyConnect for Windows問題的DNS機制的行為發生了更改。



附註：只有完成註冊的思科使用者有權存取思科內部工具與資訊。

Windows 7+

全隧道配置（以及已啟用全隧道DNS的分割隧道）

AnyConnect 4.2之前的版本：

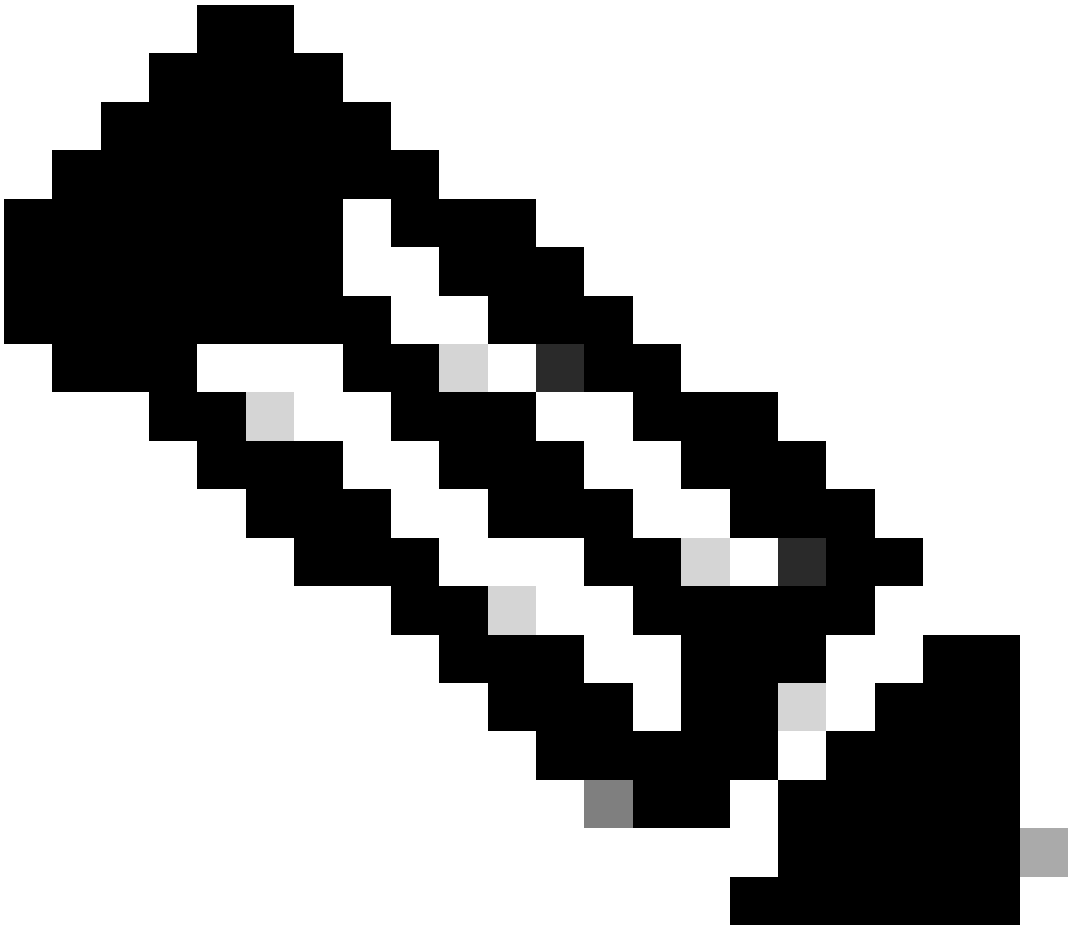
只允許向組策略下配置的DNS伺服器（隧道DNS伺服器）發出DNS請求。AnyConnect驅動程式以「無此名稱」響應響應所有其他請求。因此，只能使用隧道DNS伺服器執行DNS解析。

AnyConnect 4.2 +

允許對任何DNS伺服器的DNS請求，只要這些請求源自VPN介面卡並透過隧道傳送。所有其他請求

都以無此名稱進行響應，並且DNS解析只能透過VPN隧道執行。

在修復思科漏洞ID CSCuf07885之前，AC限制目標DNS伺服器，但透過修復此漏洞，它現在可限制哪些網路介面卡可以啟動DNS請求。



附註：只有完成註冊的思科使用者有權存取思科內部工具與資訊。

分離包括配置（停用所有DNS隧道，不分離DNS）

AnyConnect驅動程式不會干擾本地DNS解析程式。因此，DNS解析根據網路介面卡的順序執行，其中AnyConnect在VPN連線時始終是首選介面卡。此外，DNS查詢首先會透過隧道傳送，如果未得到解析，解析器會嘗試透過公共介面解析它。分離包括的訪問清單包括涵蓋隧道DNS伺服器的子網。從AnyConnect 4.2開始，隧道DNS伺服器的主機路由由AnyConnect客戶端自動增加為分離包括網路（安全路由），因此，分離包括訪問清單不再需要明確增加隧道DNS伺服器子網。

分離排除配置（停用所有DNS隧道，不分離DNS）

AnyConnect驅動程式不會干擾本地DNS解析程式。因此，DNS解析根據網路介面卡的順序執行，其中AnyConnect在VPN連線時始終是首選介面卡。此外，DNS查詢首先會透過隧道傳送，如果未得到解析，解析器會嘗試透過公共介面解析它。split-exclude access-list不能包含涵蓋隧道DNS伺服器的子網。從AnyConnect 4.2開始，隧道DNS伺服器的主機路由由AnyConnect客戶端自動增加為分離包括網路（安全路由），從而防止分離排除訪問清單中的錯誤配置。

分割DNS （停用所有通道的DNS，已設定分割DNS）

AnyConnect 4.2之前的版本

允許與分離DNS域匹配的DNS請求透過DNS伺服器隧道，但不允許其連線到其他DNS伺服器。為了防止此類內部DNS查詢從隧道中洩漏，如果向其他DNS伺服器傳送查詢，AnyConnect驅動程式將以「無此名稱」做出響應。因此，分離DNS的域只能透過隧道DNS伺服器進行解析。

允許與分離DNS域不匹配的DNS請求連線到其他DNS伺服器，但不允許透過DNS伺服器進行傳輸。即使在這種情況下，如果透過隧道嘗試查詢非拆分DNS域，AnyConnect驅動程式也會以「無此名稱」進行響應。因此，只能透過隧道外部的公共DNS伺服器解析非分離DNS域。

AnyConnect 4.2 +

允許與分離DNS域匹配的DNS請求傳送到任何DNS伺服器，只要這些請求源自VPN介面卡。如果查詢是由公共介面發起的，則AnyConnect驅動程式會以「無此名稱」作出響應，以強制解析器始終使用隧道進行名稱解析。因此，拆分DNS域只能透過隧道進行解析。

只要來自實體介面卡的DNS要求與分割DNS網域不相符，就允許這些要求傳送給任何DNS伺服器。如果查詢由VPN介面卡發起，AnyConnect將以「無此名稱」作出響應，以強制解析器始終嘗試透過公共介面解析名稱。因此，只能透過公共介面解析非分離dns域。

Mac OSx

在Macintosh系統上，DNS設定是全域的。如果使用分割隧道，但未使用分割DNS，則DNS查詢無法到達隧道外部的DNS伺服器。您只能從內部解決，不能從外部解決。

思科漏洞ID CSCtf20226和思科漏洞ID CSCtz86314中說明了此問題。在這兩種情況下，此解決方法都必須解決以下問題：

- 在組策略下指定外部DNS伺服器IP地址，並為內部DNS查詢使用FQDN。
- 如果外部名稱可以透過隧道進行解析，請導航到高級>分割隧道，並透過刪除組策略中配置的DNS名稱來停用分割DNS。這要求內部DNS查詢使用FQDN。

在AnyConnect版本3.1中解決了拆分DNS案例。但是，必須確保滿足以下條件之一：

- 必須為兩個IP協定啟用分割DNS，這需要Cisco ASA版本9.0或更高版本。
- 必須為一個IP協定啟用分割DNS。如果運行的是Cisco ASA版本9.0或更高版本，請對其他IP協定使用客戶端旁路協定。例如，請確保沒有地址池，並且組策略中啟用了Client Bypass Protocol。或者，如果您運行的ASA版本早於版本9.0，請確保沒有為其他IP協定配置地址池。這意味著另一個IP協定是IPv6。

注意：AnyConnect不會更改Macintosh OS X上的resolv.conf檔案，而是更改特定於OS X的DNS設定。Macintosh OS X基於相容性原因使resolv.conf檔案保持最新。使用scutil —dns 命令可檢視Macintosh OS X上的DNS設定。

全隧道配置（以及已啟用全隧道DNS的分割隧道）

連線AnyConnect後，系統DNS配置中僅維護隧道DNS伺服器，因此DNS請求只能傳送到隧道DNS伺服器。

分離包括配置（停用所有DNS隧道，不分離DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器被配置為首選解析器，其優先順序高於公共DNS伺服器，因此可以確保名稱解析的初始DNS請求透過隧道傳送。由於Mac OS X上的DNS設定是全局性的，因此DNS查詢不可能使用思科漏洞ID CSCtf20226（僅限註冊使用者）中所述的隧道之外的公共DNS伺服器。從AnyConnect 4.2開始，隧道DNS伺服器的主機路由由AnyConnect客戶端自動增加為分離包括網路（安全路由），因此，分離包括訪問清單不再需要明確增加隧道DNS伺服器子網。

分離排除配置（停用所有DNS隧道，不分離DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器被配置為首選解析器，它們優先於公共DNS伺服器，因此可以確保名稱解析的初始DNS請求透過隧道傳送。由於Mac OS X上的DNS設定是全局性的，因此DNS查詢不可能使用思科漏洞ID CSCtf20226（僅限註冊使用者）中所述的隧道之外的公共DNS伺服器。從AnyConnect 4.2開始，隧道DNS伺服器的主機路由由AnyConnect客戶端自動增加為分離包括網路（安全路由），因此，分離包括訪問清單不再需要明確增加隧道DNS伺服器子網。

分割DNS （停用所有通道的DNS，已設定分割DNS）

如果為兩個IP通訊協定（IPv4和IPv6）都啟用分割DNS，或它只為一個通訊協定啟用，且沒有為另一個通訊協定設定位址集區：
實施與Windows類似的真正分離DNS。真正的拆分DNS意味著與拆分DNS域匹配的請求僅透過隧道進行解析，不會洩漏給隧道外部的DNS伺服器。

如果只對一種協定啟用分割DNS，並為另一種協定分配客戶端地址，則只會對分割隧道實施DNS後退。這意味著AC僅允許透過隧道與拆分DNS域匹配的DNS請求（其他請求由AC以「拒絕」響應進行響應，以強制故障切換至公共DNS伺服器），但無法強制使用與未通過公共介面卡以明文形式傳送的拆分DNS域匹配的請求。

Linux

全隧道配置（以及已啟用全隧道DNS的分割隧道）

連線AnyConnect後，系統DNS配置中僅維護隧道DNS伺服器，因此DNS請求只能傳送到隧道DNS伺服器。

分離包括配置（停用所有DNS隧道，不分離DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器被配置為首選解析器，其優先順序高於公共DNS伺服器，因此可以確保名稱解析的初始DNS請求透過隧道傳送。

分離排除配置（停用所有DNS隧道，不分離DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器被配置為首選解析器，其優先順序高於公共DNS伺服器，因此可以確保名稱解析的初始DNS請求透過隧道傳送。

分割DNS （停用所有通道的DNS，已設定分割DNS）

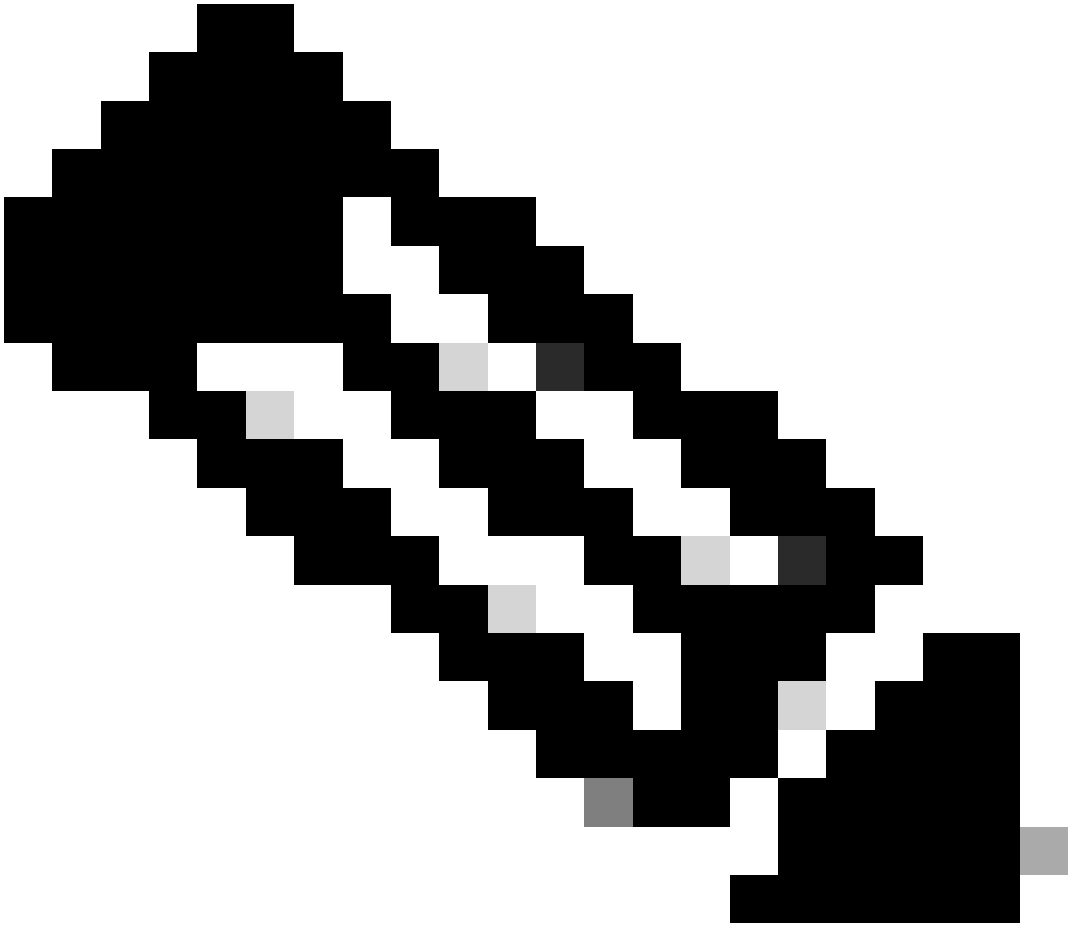
如果啟用了分割DNS，則僅對分割隧道實施DNS後退。這表示AC只允許透過通道與分割DNS網域相符的DNS要求（其他要求會由AC以「拒絕」回應回覆，以強制容錯移轉至公用DNS伺服器），但無法透過公用介面卡強制與未以明文傳送的分割DNS網域相符的要求。

iPhone

iPhone與Macintosh系統完全相反，與Microsoft Windows不同。如果定義了分割隧道，但未定義分割DNS，則DNS查詢將透過定義的全局DNS伺服器退出。例如，拆分DNS域條目對於內部解析是必需的。此行為記錄在思科漏洞ID CSCtq09624中，並在2.5.4038版中針對Apple iOS AnyConnect客戶端進行了修復。

注意：請注意，iPhone DNS查詢忽略.local域。 思科漏洞ID CSCts89292中說明了此問題。Apple工程師確認問題是由作業系統的功能引起的。這是設計好的行為，蘋果證實，它沒有改變。

相關錯誤資訊



附註：只有完成註冊的思科使用者有權存取思科內部工具與資訊。

- 思科漏洞ID CSCsv34395 -在AnyConnect中增加對FQDN代理到DHCP伺服器的支援
- 思科漏洞ID CSCtn14578 - AnyConnect支援真正的分離DNS；非後援
- 思科漏洞ID CSCtq02141 - ISP DNS與公共IP位於同一子網時，AnyConnect DNS問題
- 思科漏洞ID CSCtf20226 -使Mac的AnyConnect DNS具有與Windows相同的拆分隧道行為
- 思科漏洞ID CSCtz86314 - Mac：DNS查詢錯誤地未通過具有分割DNS的隧道傳送
- 思科漏洞ID CSCtq09624 -使具有分割隧道行為的AnyConnect iPhone DNS與Windows相同
- 思科漏洞ID CSCts89292 - iPhone的AC DNS查詢忽略.local域

相關資訊

- Cisco IOS®防火牆
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。