AnyConnect和OpenDNS漫遊客戶端之間的互操作

目錄

簡介

本檔案介紹使AnyConnect和OpenDNS漫遊客戶端協同工作的一些當前限制和可用的變通辦法。思科客戶依靠AnyConnect VPN客戶端與其公司網路進行安全和加密的通訊。同樣，OpenDNS漫遊客戶端使使用者能夠在OpenDNS公共伺服器的幫助下安全地使用DNS服務。這兩個客戶端在終端上都新增了一組豐富的安全功能，因此它們相互互操作非常重要。

必要條件

有關AnyConnect和OpenDNS漫遊客戶端的工作知識。

熟悉AnyConnect VPN的ASA或IOS/IOS-XE頭端配置（隧道組/組策略）。

需求

思科建議您瞭解以下主題：

- ASA或IOS/IOS-XE頭端
- 運行AnyConnect VPN客戶端和OpenDNS漫遊客戶端的終端

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA頭端運行版本9.4
- Windows 7
- AnyConnect客戶端4.2.00096
- OpenDNS漫遊客戶端2.0.154

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

OpenDNS正在開發一個與Cisco AnyConnect團隊配合使用的AnyConnect外掛，以便將來可用。儘管尚未設定日期，但此整合將允許漫遊客戶端與AnyConnect客戶端配合使用，而不解決任何問題。這也會使AnyConnect成為漫遊客戶端的傳送機制。

功能

AnyConnect DNS處理

VPN頭端可通過多種不同方式配置，以處理來自AnyConnect客戶端的流量。

1. 全通道組態（全通道）：這會強制來自終端的所有流量通過VPN隧道進行加密，因此流量永遠不會以明文形式離開公共介面介面卡
2. 拆分隧道配置：

   a.分割包含通道：僅發往VPN前端上定義的特定子網或主機的流量通過隧道傳送，所有其他流量以明文形式傳送到隧道外部

   b.分割排除隧道：僅發往VPN頭端上定義的特定子網或主機的流量會排除在加密之外，以明文形式離開公共介面，所有其他流量會加密，並且僅通過隧道傳送

這些配置中的每一個都決定AnyConnect客戶端如何處理DNS解析，具體取決於終端上的作業系統。修復CSCuf07885後，版本4.2中的AnyConnect for Windows上DNS處理機制中的行為發生了變化。

Windows 7+

全通道組態（和已啟用全通道DNS的分割通道）

AnyConnect 4.2之前的版本：

僅允許向在組策略（隧道DNS伺服器）下配置的DNS伺服器發出DNS請求。AnyConnect驅動程式用「no these name」響應來響應所有其他請求。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介面卡並通過隧道傳送。所有其他請求都以「無此類名稱」響應進行響應，並且DNS解析只能通過VPN隧道執行

在CSCuf07885 fix之前，AC會限制目標DNS伺服器，但通過CSCuf07885的修補程式，會限制哪些網路介面卡可以啟動DNS請求。

Split-include configuration（禁用所有DNS隧道且沒有拆分DNS）

AnyConnect驅動程式不會干擾本機DNS解析程式。因此，DNS解析是根據網路介面卡的順序執行的，AnyConnect始終是連線VPN時的首選介面卡。因此，DNS查詢將首先通過隧道傳送，如果未得到解析，解析程式將嘗試通過公共介面解析它。split-include access-list必須包含覆蓋隧道DNS伺服器的子網。 從AnyConnect 4.2開始，AnyConnect客戶端會自動將隧道DNS伺服器的主機路由新增為拆分包含網路（安全路由），因此，拆分包含訪問清單不再需要顯式新增隧道DNS伺服器子網。

Split-exclude configuration（禁用所有DNS隧道且沒有拆分DNS）

AnyConnect驅動程式不會干擾本機DNS解析程式。因此，DNS解析是根據網路介面卡的順序執行的，AnyConnect始終是連線VPN時的首選介面卡。因此，DNS查詢將首先通過隧道傳送，如果未得到解析，解析程式將嘗試通過公共介面解析它。split-exclude access-list不應包含涵蓋通道DNS伺服器的子網。 從AnyConnect 4.2開始，AnyConnect客戶端會自動將隧道DNS伺服器的主機路由新增為拆分包含網路（安全路由），因此這將防止拆分排除訪問清單中的配置錯誤。

Split-DNS（已禁用所有DNS隧道，已配置split-include）

AnyConnect 4.2之前的版本

與拆分DNS域匹配的DNS請求允許通過DNS伺服器隧道，但不允許傳送到其他DNS伺服器。為了防止此類內部DNS查詢從隧道中洩漏，如果查詢被傳送到其他DNS伺服器，AnyConnect驅動程式將以「無此類名稱」進行響應。因此，只能通過隧道DNS伺服器解析拆分DNS域。

允許與拆分DNS域不匹配的DNS請求傳送到其他DNS伺服器，但不允許通過DNS伺服器隧道。

即使在這種情況下，如果通過隧道嘗試查詢非拆分DNS域，AnyConnect驅動程式也會以「no this name」進行響應。因此，只能通過隧道外部的公共DNS伺服器解析非拆分DNS域。

AnyConnect 4.2 +

與拆分DNS域匹配的DNS請求允許到任何DNS伺服器，只要它們源自VPN介面卡。如果查詢是由公共介面發起的，則AnyConnect驅動程式將以「no this name」作為響應，以強制解析程式始終使用隧道進行名稱解析。因此，拆分DNS域只能通過隧道解析。

只要來自物理介面卡，任何DNS伺服器都允許與拆分DNS域不匹配的DNS請求。如果查詢是由VPN介面卡發起的，AnyConnect將以「no this name」作為響應，以強制解析程式始終嘗試通過公共介面解析名稱。因此，只能通過公共介面解析非拆分dns域。

Mac OS X

全通道組態（和已啟用全通道DNS的分割通道）

連線AnyConnect時，在系統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。

Split-include configuration（禁用所有DNS隧道且沒有拆分DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器配置為首選解析器，優先於公共DNS伺服器，從而確保通過隧道傳送有關名稱解析的初始DNS請求。由於Mac OS X上的DNS設定是全域性設定，因此DNS查詢無法使用CSCtf2026中記錄的隧道之外的公共DNS伺服器。從AnyConnect 4.2開始，AnyConnect客戶端會自動將隧道DNS伺服器的主機路由新增為拆分包含網路（安全路由），因此，拆分包含訪問清單不再需要顯式新增隧道DNS伺服器子網。

Split-exclude configuration（禁用所有DNS隧道且沒有拆分DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器配置為首選解析器，優先於公共DNS伺服器，從而確保通過隧道傳送有關名稱解析的初始DNS請求。由於Mac OS X上的DNS設定是全域性設定，因此DNS查詢無法使用CSCtf2026中記錄的隧道之外的公共DNS伺服器。從AnyConnect 4.2開始，AnyConnect客戶端會自動將隧道DNS伺服器的主機路由新增為拆分包含網路（安全路由），因此，拆分包含訪問清單不再需要顯式新增隧道DNS伺服器子網。

Split-DNS（已禁用所有DNS隧道，已配置split-include）

如果為兩個IP協定（IPv4和IPv6）都啟用了拆分DNS，或者它只為一個協定啟用，並且沒有為另一個協定配置地址池：
實施與Windows類似的真正拆分DNS。真正的拆分DNS意味著與拆分DNS域匹配的請求只能通過隧道解析，不會洩漏到隧道外部的DNS伺服器。

如果只為一個協定啟用了拆分DNS，且為另一個協定分配了客戶端地址，則僅強制實施「用於拆分隧道的DNS回退」。這意味著AC僅允許通過隧道與拆分DNS域匹配的DNS請求（其他請求由AC以

「拒絕」響應進行響應，以強制故障轉移至公共DNS伺服器），但無法強制要求匹配拆分DNS域的請求不通過公共介面卡以明文形式傳送。

Linux

全通道組態（和已啟用全通道DNS的分割通道）

連線AnyConnect時，在系統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。

Split-include configuration（禁用所有DNS隧道且沒有拆分DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器配置為首選解析器，優先於公共DNS伺服器，從而確保通過隧道傳送有關名稱解析的初始DNS請求。

Split-exclude configuration（禁用所有DNS隧道且沒有拆分DNS）

AnyConnect不會干擾本地DNS解析程式。隧道DNS伺服器配置為首選解析器，優先於公共DNS伺服器，從而確保通過隧道傳送有關名稱解析的初始DNS請求。

Split-DNS（已禁用所有DNS隧道，已配置split-include）

如果啟用了拆分DNS，則僅強制執行「用於拆分隧道的DNS回退」。這意味著AC僅允許通過隧道與拆分DNS域匹配的DNS請求（其他請求由AC以「拒絕」響應進行響應，以強制故障轉移至公共DNS伺服器），但無法強制要求匹配拆分DNS域的請求不通過公共介面卡以明文形式傳送。

OpenDNS漫遊客戶端

漫遊客戶端是管理終端上DNS服務的軟體，它利用OpenDNS公共DNS伺服器來保護和加密DNS流量。

理想情況下，客戶端應處於受保護且加密的狀態。但是，如果客戶端無法與OpenDNS公共解析器伺服器(208.67.222.222)建立TLS會話，它將嘗試在UDP埠53上傳送未加密的DNS流量到208.67.222.222。漫遊客戶端僅使用OpenDNS的公共解析器IP地址208.67.222.222（還有幾個其它地址，如208.67.2220 220、208.67.222.220和208.67.220.222）。 漫遊客戶端安裝後，會將127.0.0.1(localhost)設定為本地DNS伺服器，並覆蓋當前的每介面DNS設定。當前DNS設定儲存在漫遊客戶端配置資料夾中的本地resolv.conf檔案中（即使在Windows上）。OpenDNS甚至會備份通過AnyConnect介面卡獲取的DNS伺服器。例如，如果192.168.92.2是公共介面卡上的DNS伺服器，OpenDNS將在以下位置建立resolv.conf:

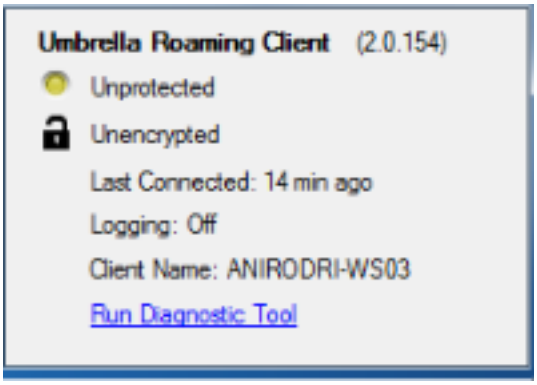
```
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
nameserver 192.168.92.2
```

漫遊使用者端會加密每個封包集至OpenDNS;但是，它不會啟動或使用到208.67.222.222的加密隧道。 漫遊客戶端具有可選的IP層實施功能，該功能將為非DNS用途開啟IPSec連線以阻止IP地址。在活動的AnyConnect連線存在時，這將自動禁用。它還繫結到127.0.0.1:53以接收在電腦上本地生成的查詢。當終端需要解析名稱時，本地查詢會由於覆蓋而被定向到127.0.0.1，然後漫遊客戶端的基礎的dnscrypt-proxy進程會通過加密通道將其轉發到OpenDNS公共伺服器。

如果DNS不允許流到127.0.0.1:53，則漫遊客戶端將無法運行，並將發生以下情況。如果客戶端無法訪問公共DNS伺服器或127.0.0.1:53繫結地址，它將轉換到失效開放狀態並還原本地介面卡上的DNS設定。在後台中，它會繼續傳送探測器到208.67.222.222，並且如果重新建立安全連線，它可以轉換到活動模式。

限制

檢視兩個客戶端的高級功能後，顯然漫遊客戶端需要能夠更改本地DNS設定並繫結到127.0.0.1:53以通過安全通道轉發查詢。連線VPN時，AnyConnect不會干擾本機DNS解析程式的唯一配置是split-include和split-exclude（禁用split-tunnel-all DNS）。 因此，當前建議在漫遊客戶端也在使用時使用這些配置之一。如果使用全隧道配置，或啟用全隧道分割DNS，漫遊客戶端將保持未保護/未加密狀態，如圖所示。



因應措施

如果目的是保護使用VPN隧道的漫遊客戶端和OpenDNS伺服器之間的通訊，則可以在VPN頭端上使用虛擬拆分 — 排除訪問清單。這是最接近全通道組態的東西。如果沒有此類要求，則可以在訪問清單不包括OpenDNS公共伺服器的情況下使用拆分包括，也可以在訪問清單包括OpenDNS公共伺服器的情況下使用拆分排除。

此外，使用漫遊客戶端時，無法使用拆分DNS模式，因為這將導致本地DNS解析丟失。分割通道所有DNS也應保持禁用狀態；但是，它部分受支援，應該允許漫遊客戶端在故障轉移後進行加密。

組態

通道OpenDNS流量

此範例在split-exclude access-list中使用虛擬IP位址。通過此配置，與208.67.222.222的所有通訊都通過VPN隧道進行，並且漫遊客戶端在加密和保護狀態下運行。

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

從VPN隧道排除OpenDNS流量

此示例使用split-exclude access-list中的OpenDNS解析程式地址。通過此配置，與208.67.222.222的所有通訊都發生在VPN隧道之外，漫遊客戶端在加密和保護狀態下運行。

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

此示例顯示內部192.168.1.0/24子網的拆分包含配置。透過此設定，漫遊使用者端仍會在加密和保護狀態下運作，因為前往208.67.222.222的流量不會透過通道傳送。

```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
```

```
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Note: Split-tunnel-all-dns must be disabled in all of the scenarios

驗證

連線VPN後，漫遊客戶端應顯示受保護且已加密，如下圖所示：