配置ASA/AnyConnect動態分割隧道

目錄

簡介

本文檔介紹如何透過ASDM為動態分割排除隧道配置AnyConnect安全移動客戶端。

必要條件

需求

思科建議您瞭解以下主題：

- ASA基礎知識。
- Cisco AnyConnect安全移動客戶端的基本知識。

採用元件

本檔案中的資訊是根據以下軟體版本：

- ASA 9.12(3)9
- 調適型安全裝置管理器(ASDM) 7.13(1)
- AnyConnect 4.7.0

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。

背景資訊

AnyConnect分割隧道允許Cisco AnyConnect安全移動客戶端透過IKEV2或安全套接字層(SSL)安全訪問企業資源。

在AnyConnect版本4.5之前，根據自適應安全裝置(ASA)上配置的策略，分割隧道行為可以是指定隧道、全部隧道或排除指定。

隨著雲託管電腦資源的出現，服務有時會根據使用者位置或雲託管資源的負載解析為不同的IP地址。

由於AnyConnect安全移動客戶端提供到IPV4或IPV6的靜態子網範圍、主機或池的分割隧道，網路管理員在配置AnyConnect時很難排除域/FQDN。

例如，網路管理員希望將Cisco.com域從拆分隧道配置中排除，但是Cisco.com的DNS對映會更改，因為它是由雲託管的。

使用動態分割排除隧道，AnyConnect動態解析託管應用的IPv4/IPv6地址，並對路由表和過濾器進行必要的更改，以允許隧道外部進行連線。

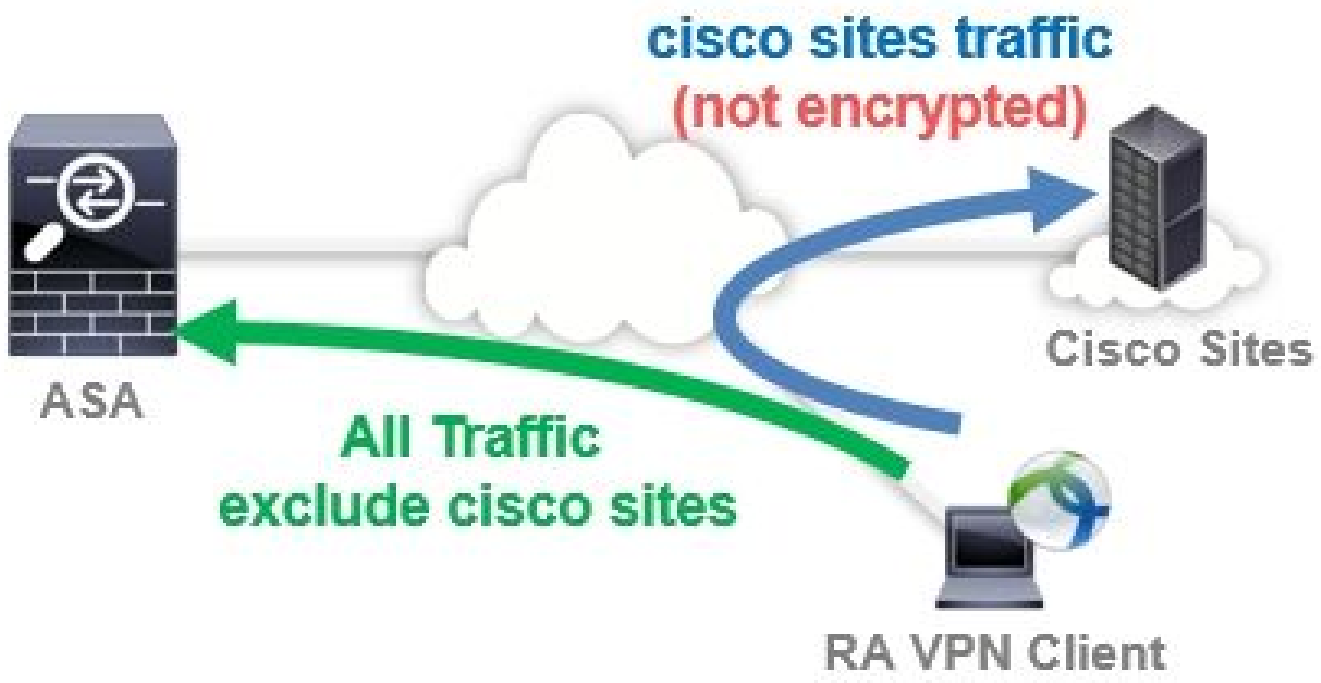
從AnyConnect 4.5開始，可以使用動態交換隧道，其中AnyConnect動態解析託管應用的IPv4/IPv6地址，並對路由表和過濾器進行必要的更改以允許隧道外部進行連線

組態

本節介紹如何在ASA上配置Cisco AnyConnect安全移動客戶端。

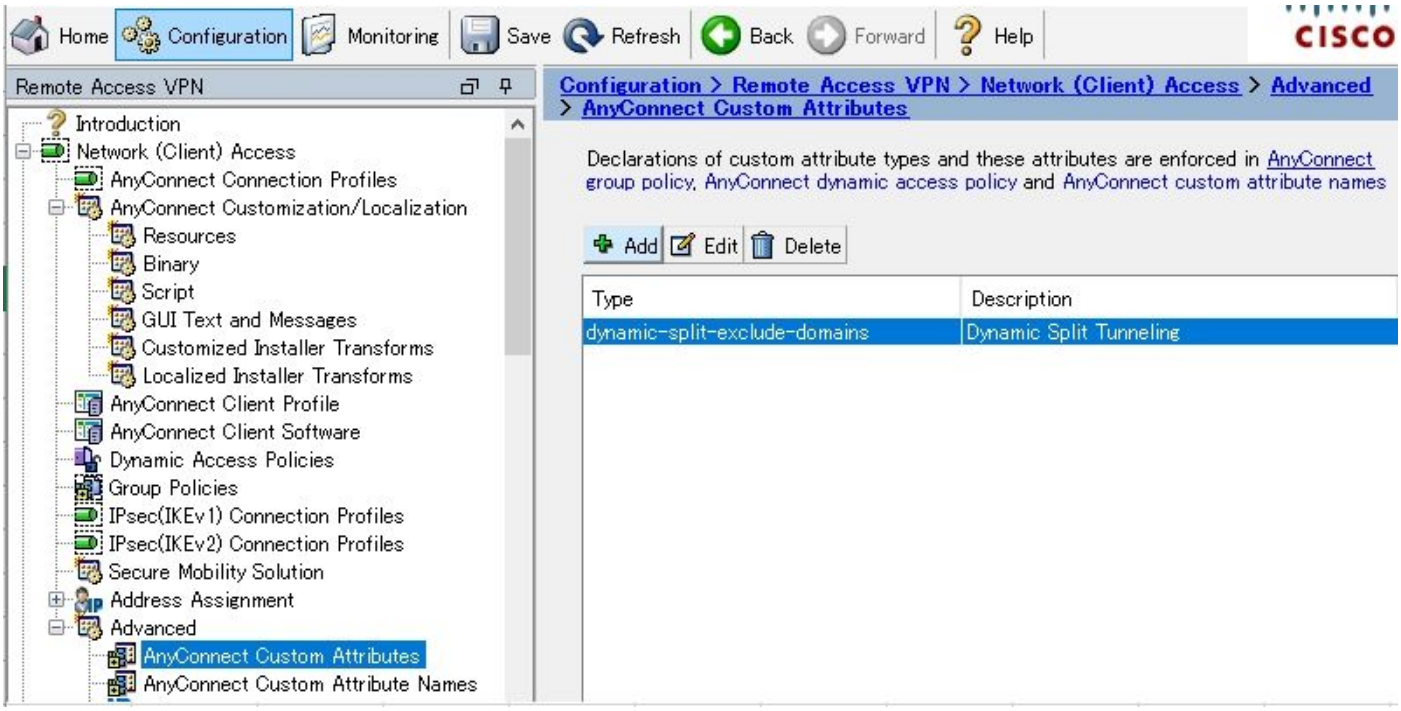
網路圖表

下圖顯示本文檔示例中使用的拓撲。



步驟 1.建立AnyConnect自定義屬性

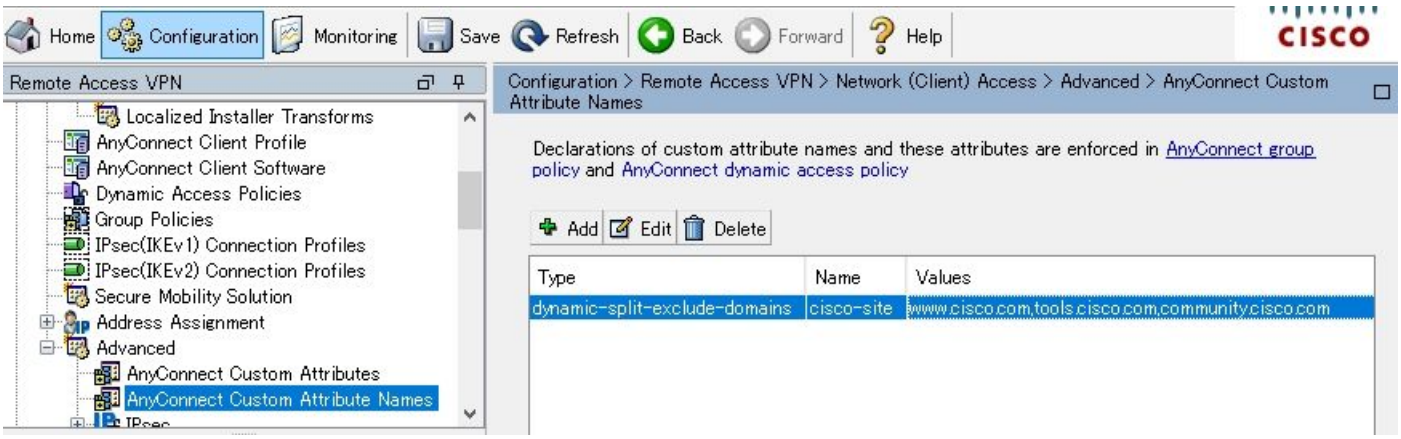
導航到**Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes**。點選**Add** 按鈕，設定 **dynamic-split-exclude-domains** 屬性和可選說明，如圖所示：



步驟 2.建立AnyConnect自定義名稱和配置值

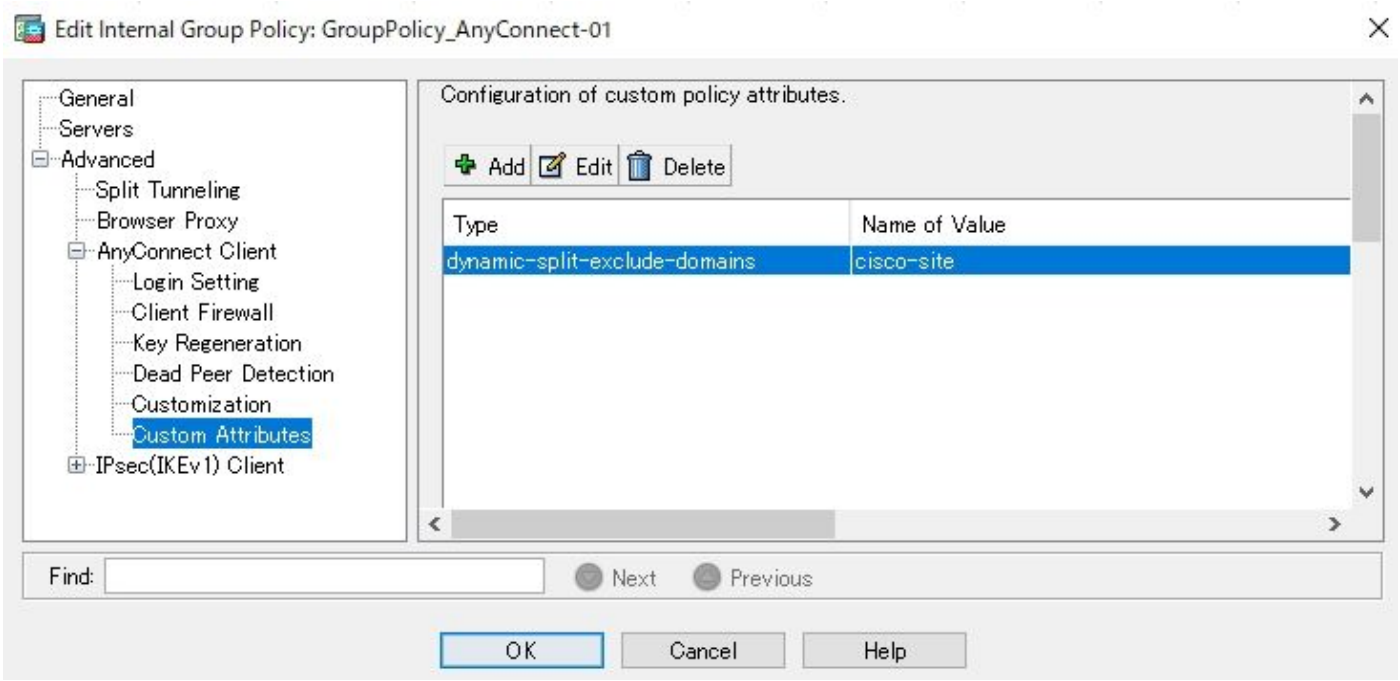
導航到 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names。按一下 **Add** 按鈕，然後設定以前從「型別」建立的屬 **dynamic-split-exclude-domains** 性，即任意名稱和值，如下圖所示：

請注意不要在名稱中輸入空格。（例如：可能為cisco-site，不可能為cisco site）當在Values中註冊多個域或FQDN時，請使用逗號(，)分隔它們。



步驟 3.將型別和名稱增加到組策略

導航到 **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** 並選擇組策略。之後，導航到**Advanced> AnyConnect Client> Custom Attributes** 並增加已配置的 **Type** 和 **Name**，如下圖所示：



CLI組態範例

本節提供動態分割隧道的CLI配置以供參考之用。

<#root>

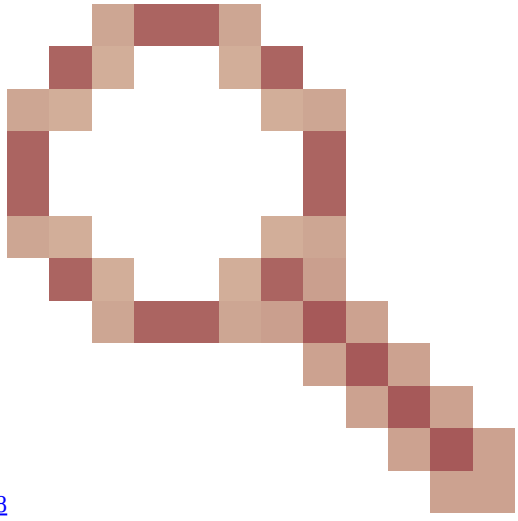
ASAv10# show run
--- snip ---

webvpn

```
 enable outside
 AnyConnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling

 hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 AnyConnect image disk0:/AnyConnect-win-4.7.04056-webdeploy-k9.pkg 1
 AnyConnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
AnyConnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.

group-policy GroupPolicy_AnyConnect-01 internal
group-policy GroupPolicy_AnyConnect-01 attributes

 wins-server none
 dns-server value 10.0.0.0
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 split-tunnel-network-list value SplitACL
 default-domain value cisco.com
 AnyConnect-custom dynamic-split-exclude-domains value cisco-site
```

限制

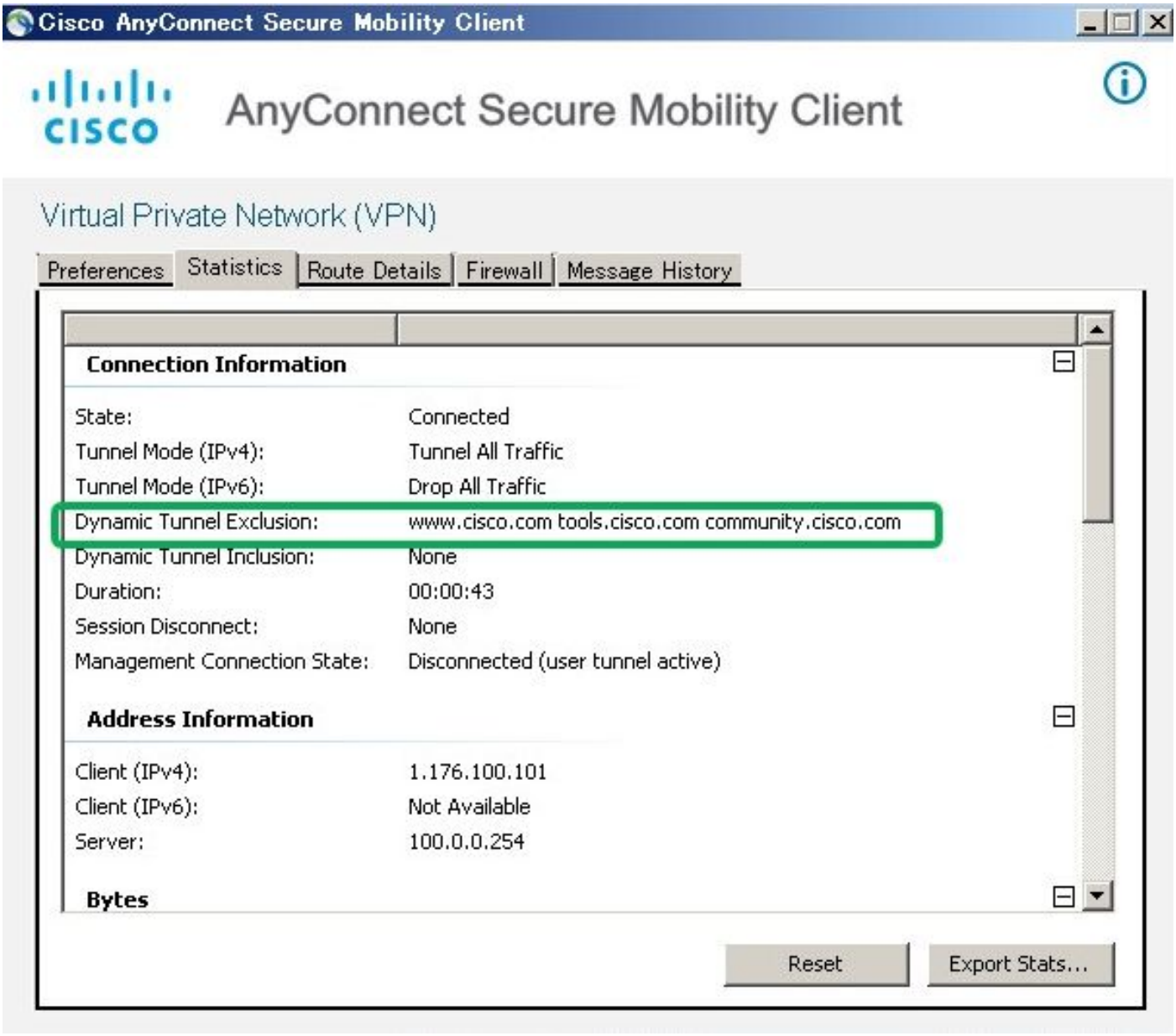
- 需要ASA版本9.0或更高版本才能使用動態分割隧道自定義屬性。
- 不支援值欄位中的萬用字元。



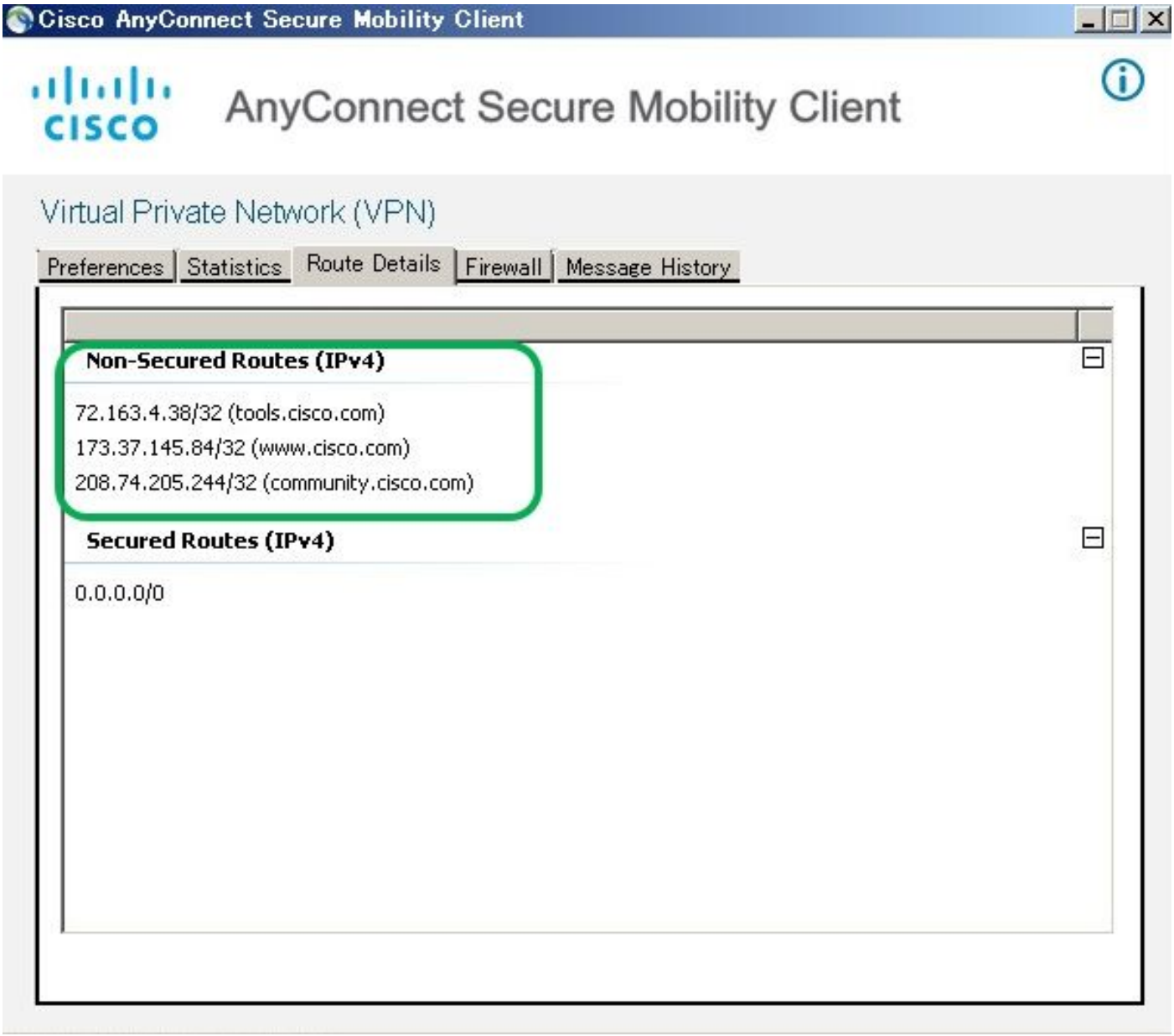
- iOS (Apple)裝置不支援動態分割隧道(增強請求：思科漏洞ID CSCvr54798)。

驗證

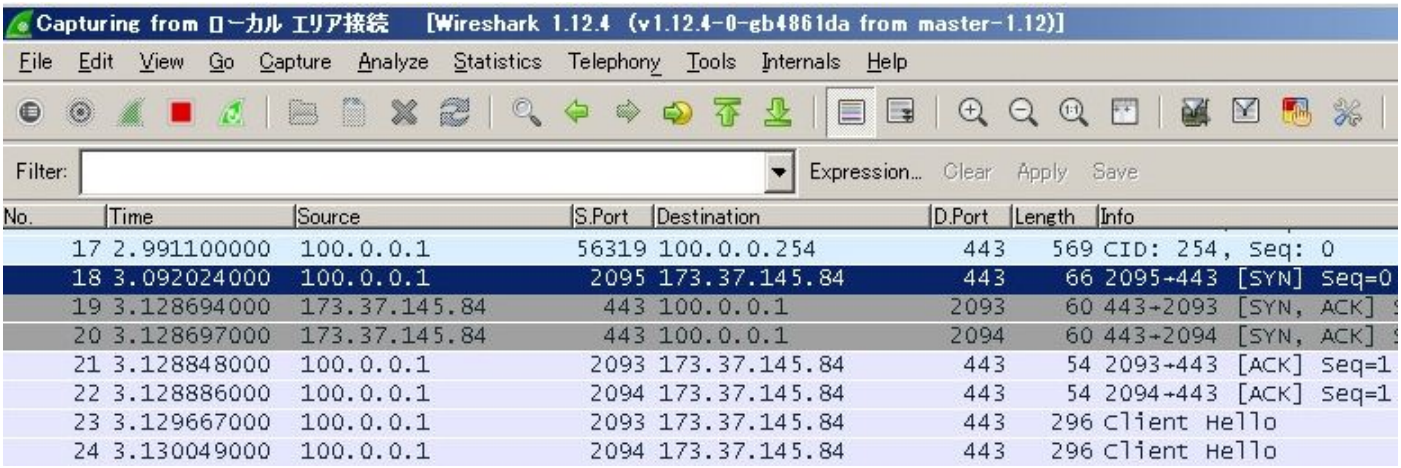
要驗證客戶端上已配置的**Dynamic Tunnel Exclusions**, AnyConnectlaunchsoftware，請按一下 **Advanced Window**>**Statistics**，如下圖所示：



您也可以導覽至**Advanced Window**>**Route Details** 索引標籤，進**Dynamic Tunnel Exclusions**行驗證，**Non-Secured Routes**, 如下圖所示。



在本示例中，您已配置www.cisco.com **Dynamic Tunnel Exclusion list**underand the Wireshark capture collected on the AnyConnect client physical interface confirm the traffic to www.cisco.com (198.51.100.0) is not encrypted by DTLS。



疑難排解

如果值欄位中使用萬用字元

如果在「值」欄位中配置了萬用字元，例如，在「值」中配置了***.cisco.com**，則AnyConnect會話將斷開連線，如日誌中所示：

Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> N
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> First TCP SVC connection established for
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP SVC connection established without
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Client Type: Cisco AnyConnect VPN Ag
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv4 Address <172.16.0.0> IPv6 address
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (172.16.0.0/44868) to identity:203.0.113.0/443
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC closing connection: Transport closin
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC Message: 16/ERROR: Configuration
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> WebVPN session terminated: User Reque
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session disconnected. Session Type: AnyConnect-

注意：或者，您也可以使用值中的**cisco.com**域來允許FQDN，例如www.cisco.com和tools.cisco.com。

如果Route Details頁籤中未顯示安全路由

當客戶端為排除的目標發起流量時，AnyConnect客戶端會自動在Route Details頁籤中獲知並增加IP地址和FQDN。

為了驗證AnyConnect使用者是否分配到正確的Anyconnect組策略，您可以運行命令 **show vpn-sessiondb anyconnect filter name <username>**

<#root>

ASAv10# show vpn-sessiondb anyconnect filter name cisco

Session Type: AnyConnect

Username : cisco Index : 7
Assigned IP : 172.16.0.0 Public IP : 10.0.0.0
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 7795373 Bytes Rx : 390956

Group Policy : GroupPolicy_AnyConnect-01

Tunnel Group : AnyConnect-01
Login Time : 13:20:48 UTC Tue Mar 31 2020
Duration : 20h:19m:47s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 019600a9000070005e8343b0
Security Grp : none

一般疑難排解

您可以使用AnyConnect診斷和報告工具(DART)來收集有助於解決AnyConnect安裝和連線問題的資料。 DART嚮導用於運行AnyConnect的電腦。DART彙編了用於思科技術支援中心(TAC)分析的日誌、狀態和診斷資訊，不需要管理員許可權便可在客戶端電腦上運行。

相關資訊

- **Cisco AnyConnect安全移動客戶端管理員指南，版本4.7 -關於動態分割隧道**
- **ASDM書3：Cisco ASA系列VPN ASDM配置指南7.13 -配置動態分割隧道**

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）。