配置ASA/AnyConnect动态拆分隧道

目录

简介

本文档介绍如何通过ASDM为动态拆分排除隧道配置AnyConnect安全移动客户端。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA基础知识。
- Cisco AnyConnect安全移动客户端基础知识。

使用的组件

本文档中的信息基于以下软件版本：

- ASA 9.12(3)9
- 自适应安全设备管理器(ASDM)7.13(1)
- AnyConnect 4.7.0

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。

背景信息

AnyConnect分割隧道允许Cisco AnyConnect安全移动客户端通过IKEV2或安全套接字层(SSL)安全访问企业资源。

在AnyConnect版本4.5之前，根据在自适应安全设备(ASA)上配置的策略，拆分隧道行为可以是Tunnel Specified、Tunnel All或Exclude Specified。

随着云托管计算机资源的出现，服务有时会根据用户的位置或云托管资源的负载解析到不同的IP地址。

由于AnyConnect安全移动客户端提供到IPV4或IPV6的静态子网范围、主机或池的分割隧道，因此网络管理员在配置AnyConnect时很难排除域/FQDN。

例如，网络管理员希望将Cisco.com域从拆分隧道配置中排除，但Cisco.com的DNS映射会更改，因为它是云托管的。

使用动态拆分排除隧道，AnyConnect动态解析托管应用的IPv4/IPv6地址，并对路由表和过滤器进行必要的更改，以允许隧道外部进行连接。

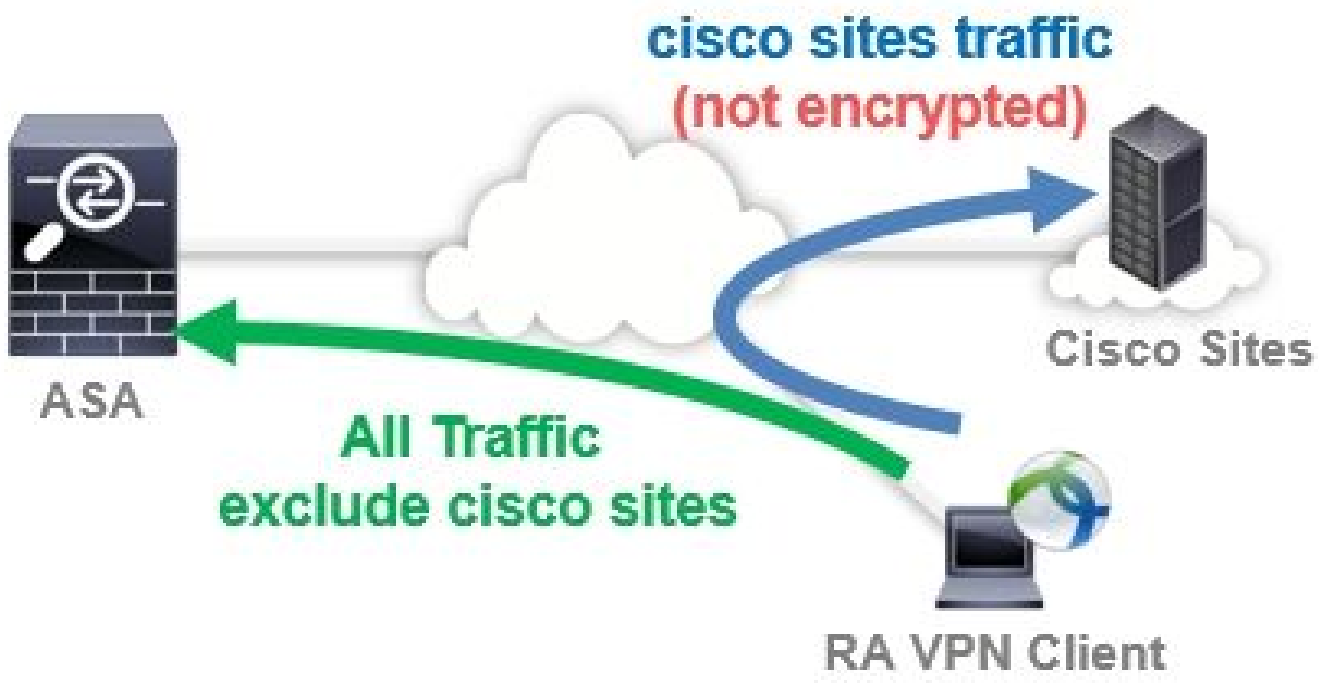
从AnyConnect 4.5开始，可以使用动态拆分隧道，其中AnyConnect动态解析托管应用的IPv4/IPv6地址，并对路由表和过滤器进行必要的更改，以允许隧道外部进行连接

配置

本节介绍如何在ASA上配置Cisco AnyConnect安全移动客户端。

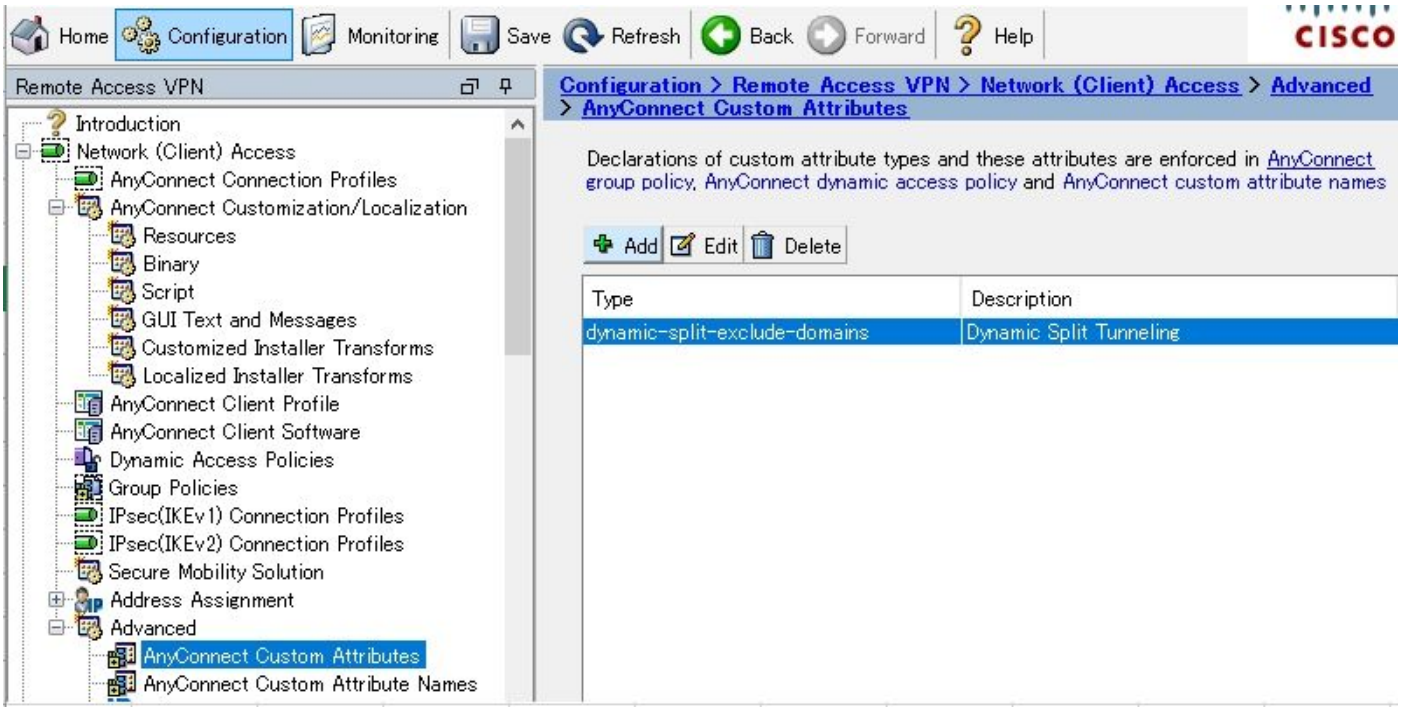
网络图

下图显示了用于本文档示例的拓扑。



步骤1:创建AnyConnect自定义属性

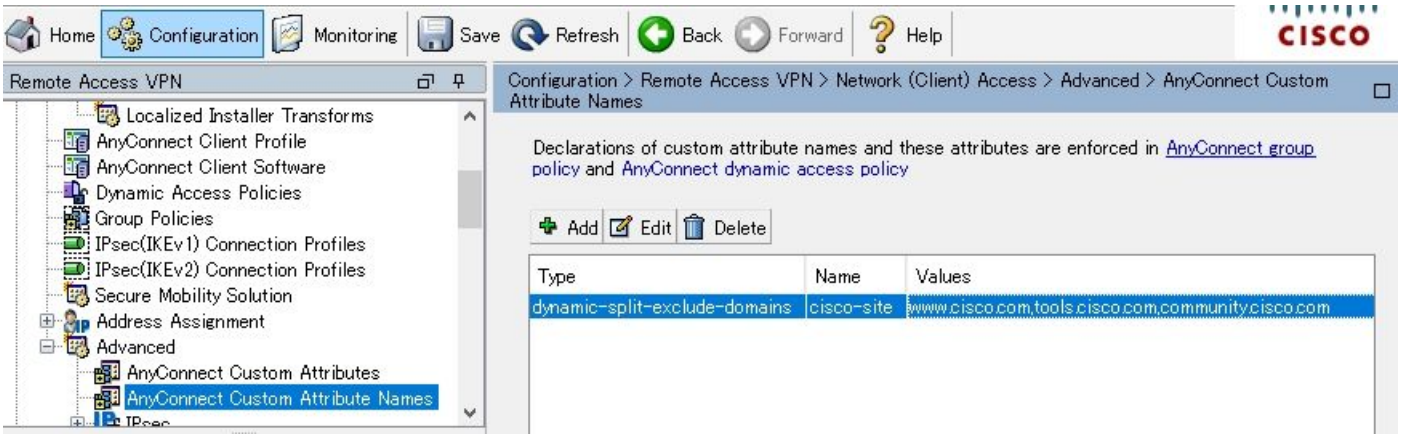
导航至 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.**点击 **Add** 按钮，并设置 **dynamic-split-exclude-domains** 属性和可选说明，如图所示：



第二步：创建AnyConnect自定义名称和配置值

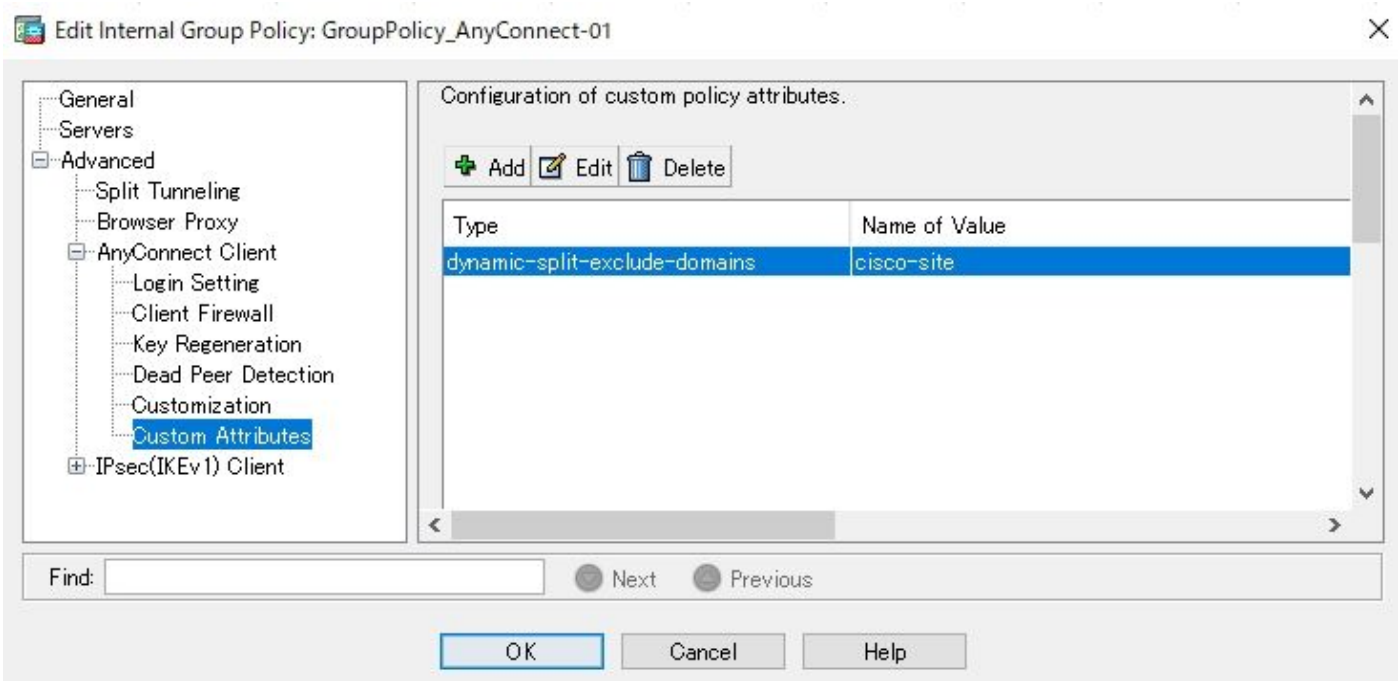
导航至 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.**点击 **Add** 按钮，并设置 **dynamic-split-exclude-domains** 先前从Type创建的属性，任意名称和值，如图所示：

注意不要在Name中输入空格。（例如：可能的思科站点、不可能的思科站点）当在值中注册多个域或FQDN时，用逗号(,)分隔它们。



第三步：向组策略添加类型和名称

导航至 **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** 并选择组策略。之后，导航至 **Advanced> AnyConnect Client> Custom Attributes** 并添加已配置的 **Type** 和 **Name**,如图所示:



CLI配置示例

本节提供动态分割隧道的CLI配置以供参考。

<#root>

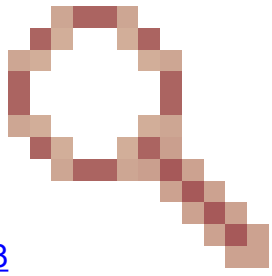
```
ASAv10# show run
  --- snip ---
```

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

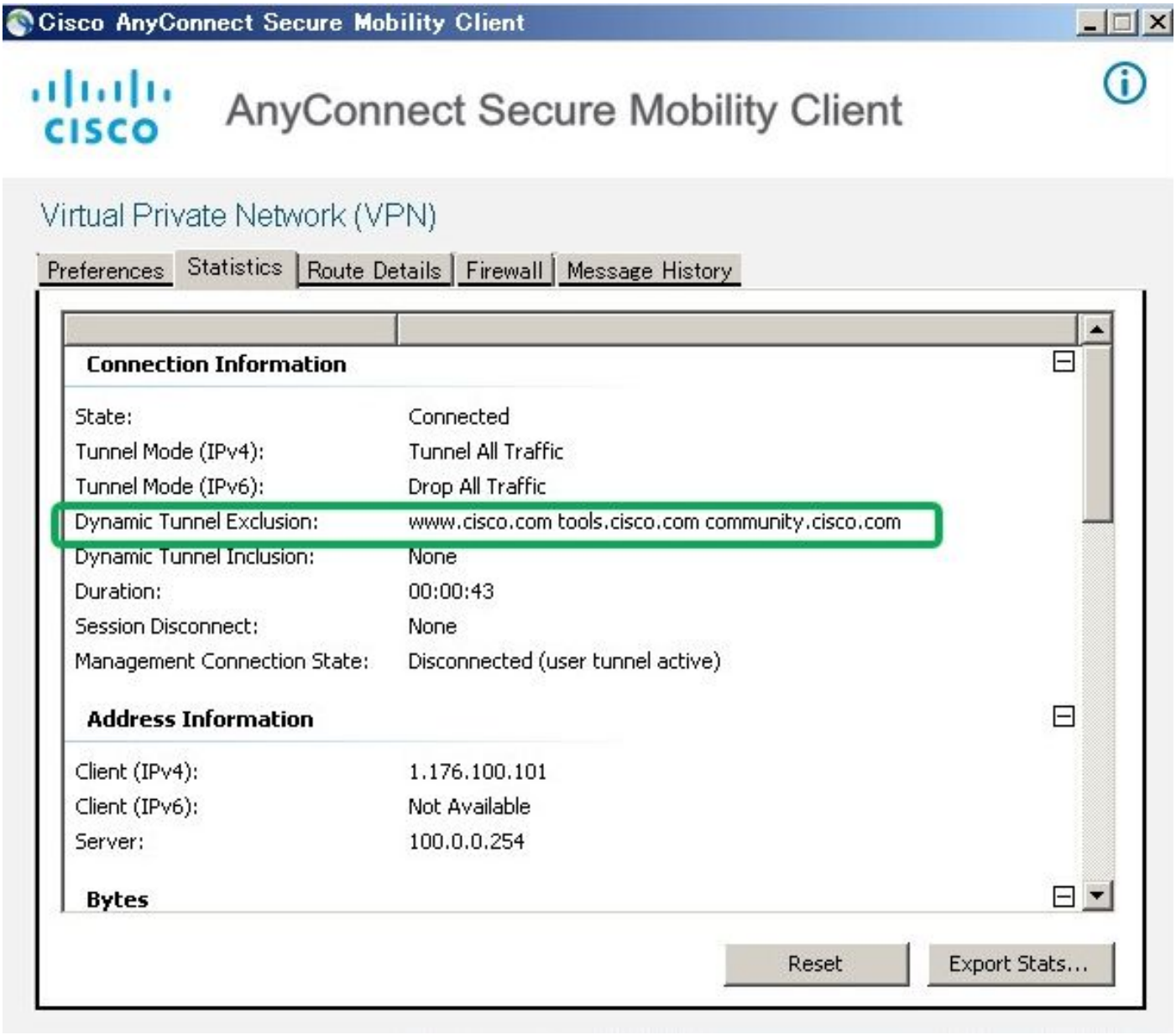
- 使用Dynamic Split Tunneling自定义属性需要ASA 9.0版或更高版本。
- 不支持值字段中的通配符。



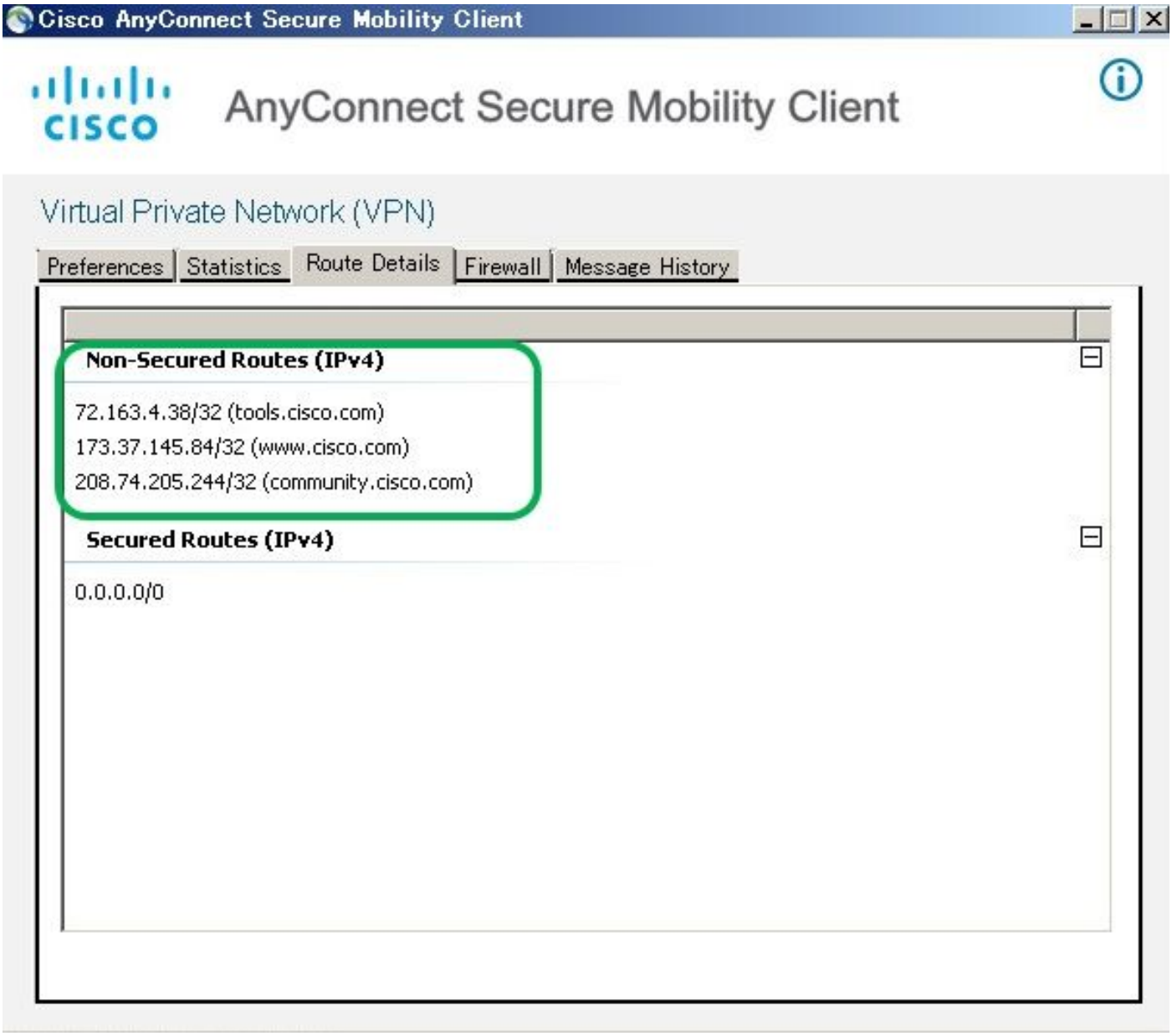
- iOS(Apple)设备不支持动态拆分隧道(增强请求：Cisco bug ID CSCvr54798 影响。

验证

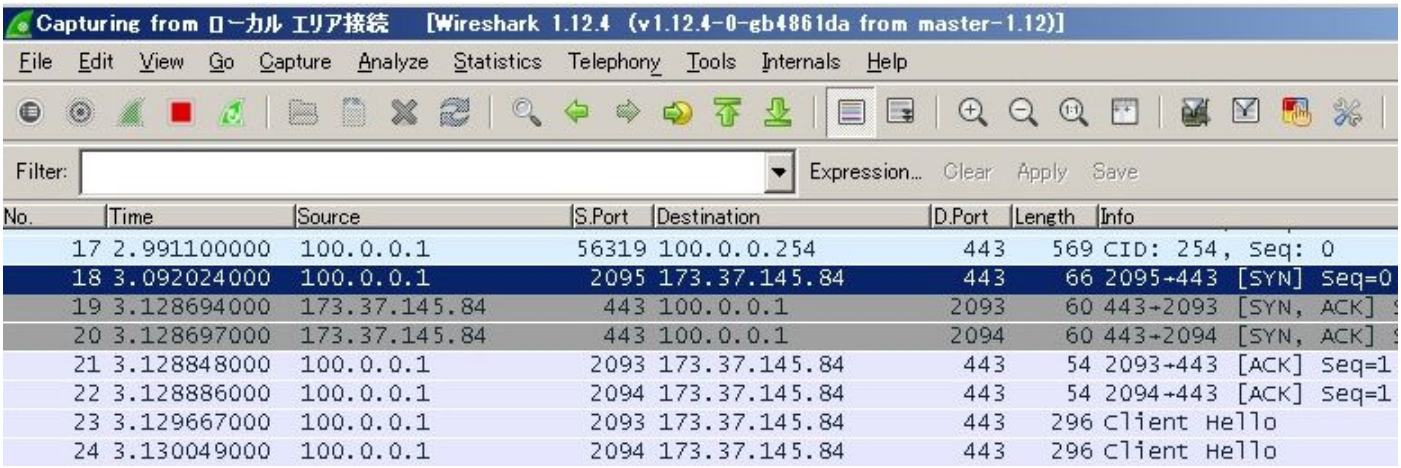
要验证已配置的 **Dynamic Tunnel Exclusions**, 启动AnyConnect软件，单击 **Advanced Window>Statistics**，如图所示：



您也可以导航至 **Advanced Window>Route Details** 选项卡中，您可以验证**Dynamic Tunnel Exclusions**列在下**Non-Secured Routes**, 如图所示.



www.cisco.com在本示例中，您已在**Dynamic Tunnel Exclusion list**并且，在AnyConnect客户端物理接口上收集的Wireshark捕获可确认到www.cisco.com(198.51.100.0)的流量未被DTLS加密。



故障排除

如果通配符用于值字段

如果在Values字段中配置了通配符，例如，在Values中配置了*.cisco.com，则AnyConnect会话将断开连接，如日志所示：

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Fir
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Cli
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (17
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Web
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session
```

注意：您也可以使用Values（值）中的cisco.com域来允许FQDN，例如www.cisco.com和tools.cisco.com。

如果Route Details选项卡中未显示非安全路由

当客户端启动排除目标的流量时，AnyConnect客户端会自动获取并添加Route Details选项卡中的IP地址和FQDN。

要验证AnyConnect用户是否已分配到正确的Anyconnect组策略，可以运行该命令 **show vpn-sessiondb anyconnect filter name**

<#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
```

一般故障排除

您可以使用AnyConnect诊断和报告工具(DART)收集有助于排除AnyConnect安装和连接问题的数据。 DART向导用于运行AnyConnect的计算机。DART 可以收集日志、状态和诊断信息供思科技术支持中心 (TAC) 执行分析，并且不需要管理员权限即可在客户端计算机上运行。

相关信息

- Cisco AnyConnect安全移动客户端管理员指南，版本4.7 — 关于动态拆分隧道
- ASDM手册3:Cisco ASA系列VPN ASDM配置指南，7.13 — 配置动态拆分隧道

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）。