在FMC管理的FTD上配置AnyConnect动态拆分隧道

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 限制

配置

- 步骤1.编辑组策略以使用动态拆分隧道
- 步骤2.配置AnyConnect自定义属性
- 步骤3.检验配置，保存并部署

验证

故障排除

- 问题
- 解决方案

相关信息

简介

本文档介绍如何在Firepower管理中心管理的Firepower威胁防御(FTD)上配置AnyConnect动态拆分隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco AnyConnect
- Firepower管理中心(FMC)基础知识

使用的组件

本文档中的信息基于以下软件版本：

- FMC版本7.0
- FTD版本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

由FMC管理的FTD上的AnyConnect动态拆分隧道配置在FMC 7.0版及更高版本上完全可用。如果运行较旧版本，则需要按照使用FMC进行Firepower威胁防御的高级AnyConnect VPN部署中的说明通过FlexConfig对其进行配置。

使用动态拆分隧道配置，您可以根据DNS域名微调拆分隧道配置。由于与完全限定域名(FQDN)关联的IP地址可以更改，因此基于DNS名称的分割隧道配置可提供更动态的定义，说明哪些流量是包括在远程访问虚拟专用网络(VPN)隧道中，哪些流量不是。如果为排除的域名返回的任何地址在VPN包含的地址池内，则这些地址将被排除。不阻止排除的域。相反，流向这些域的流量保留在VPN隧道之外。

注意：您还可以配置动态拆分隧道，以定义要包含在隧道中的域，否则将基于IP地址排除这些域。

限制

目前，仍不支持以下功能：

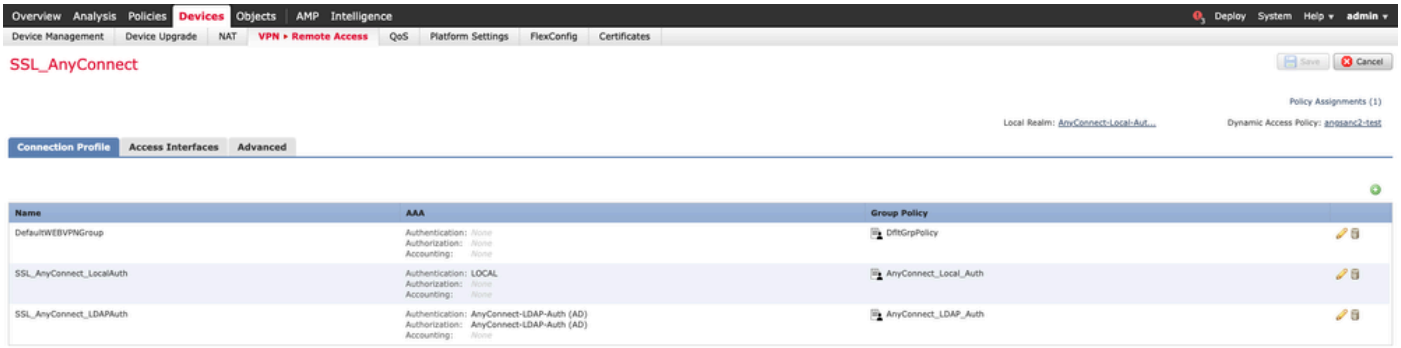
- Cisco iOS设备不支持动态拆分隧道。请参阅Cisco Bug ID CSCvr54798
- AnyConnect Linux客户端不支持动态拆分隧道。请参阅Cisco Bug ID CSCvt64988

配置

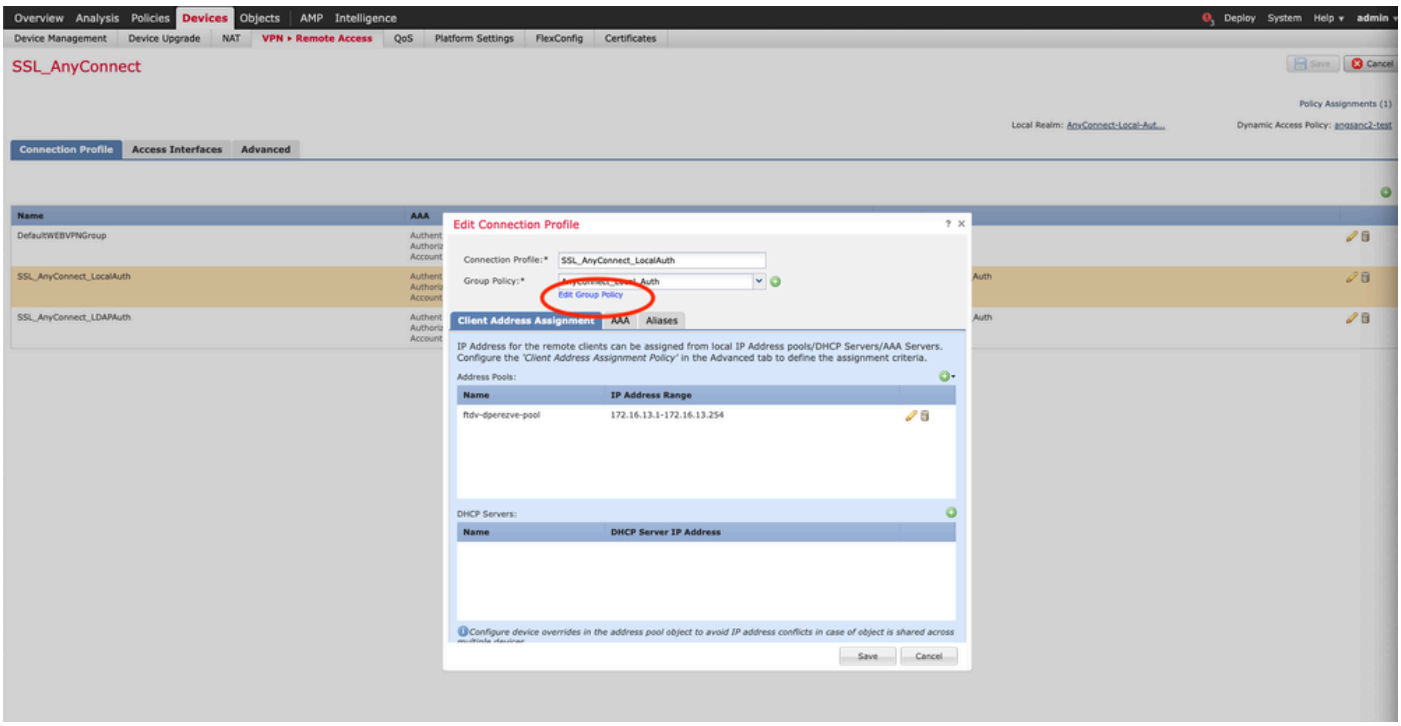
本节介绍如何在FMC管理的FTD上配置AnyConnect动态拆分隧道。

步骤1.编辑组策略以使用动态拆分隧道

1.在FMC上，导航到设备> VPN >远程访问，然后选择您要应用配置的连接配置文件:

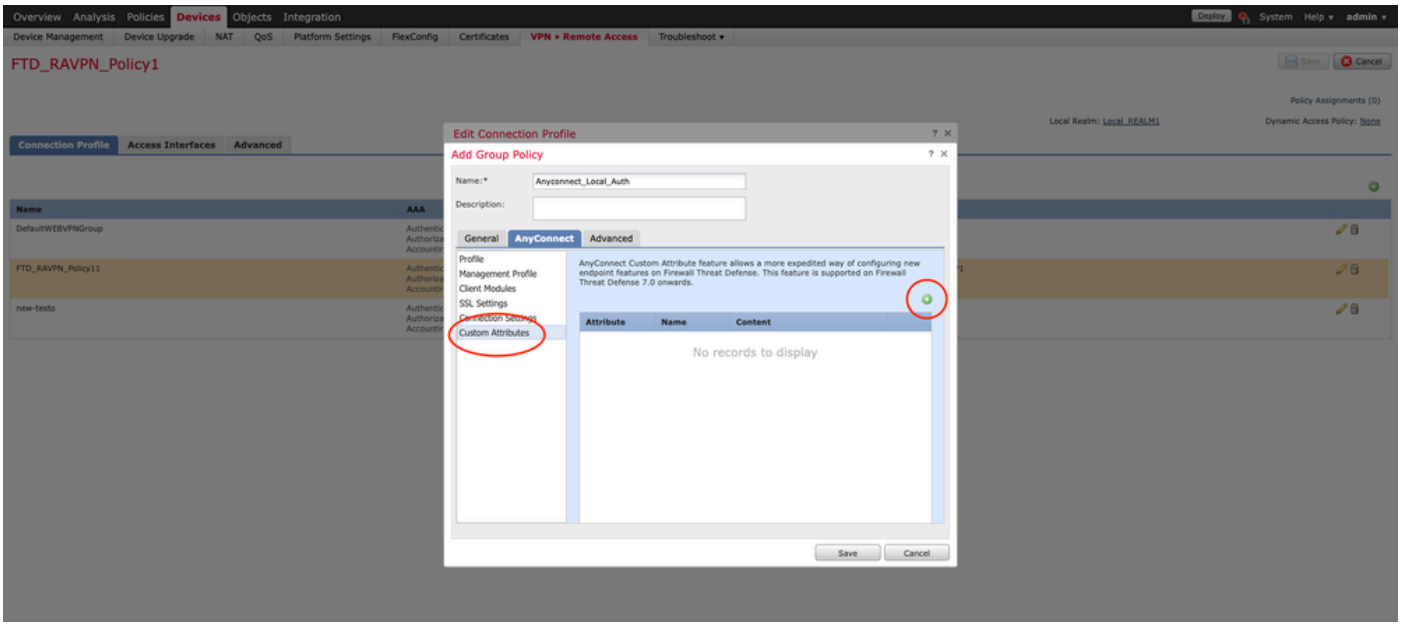


2.选择Edit Group Policy以修改已创建的一个组策略。

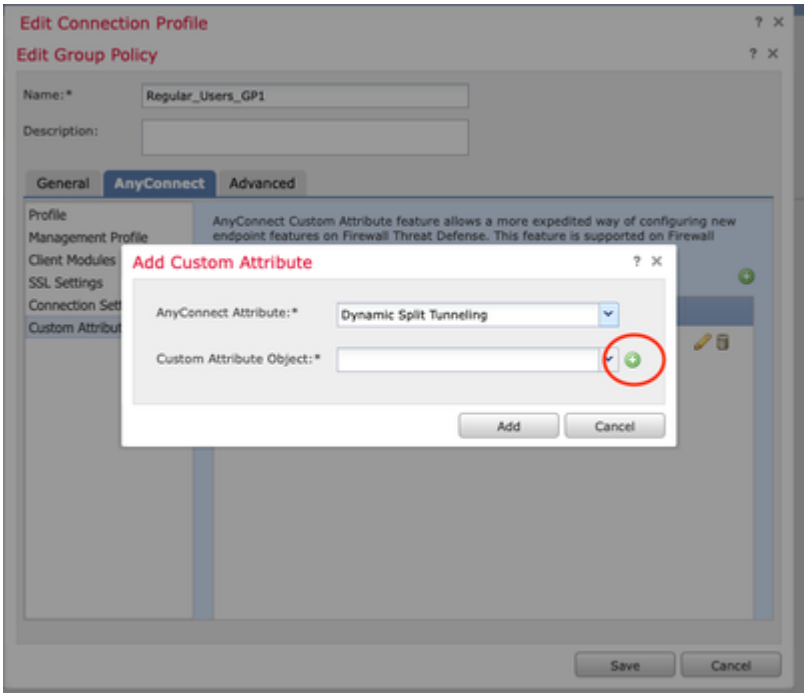


步骤2.配置AnyConnect自定义属性

1.在“组策略配置”下，导航到AnyConnect >自定义属性，点击添加(+)按钮：

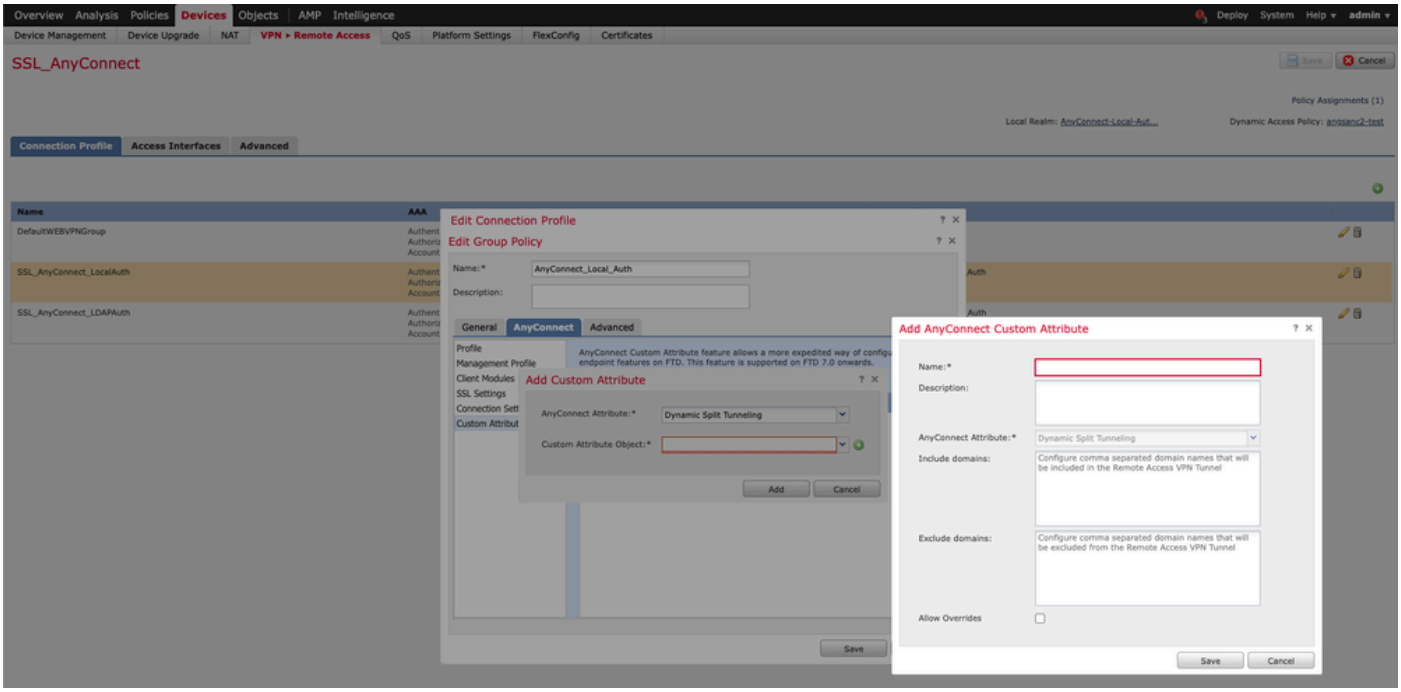


2.选择Dynamic Split Tunneling AnyConnect属性，然后单击Add(+)按钮以创建新的自定义属性对象：

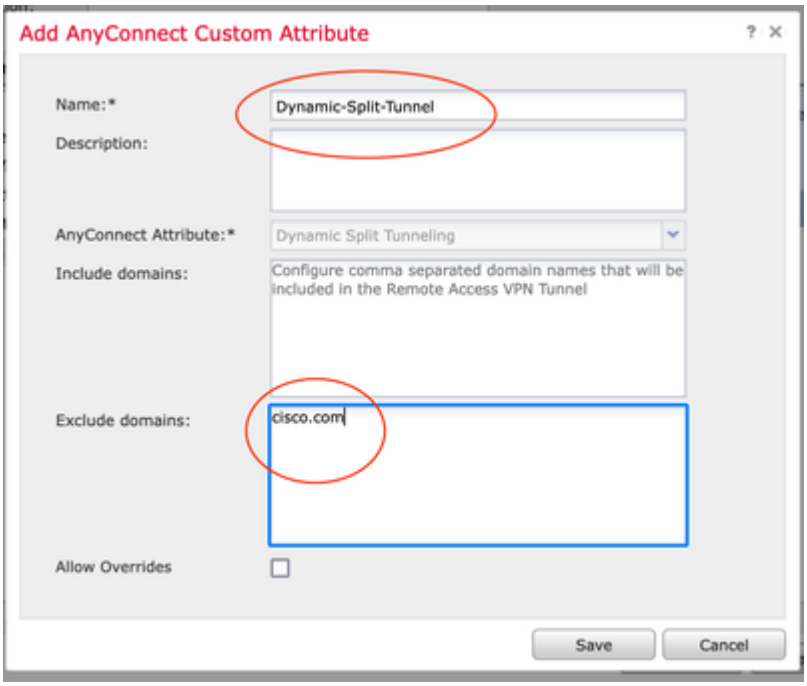


3.输入AnyConnect自定义属性的名称，并配置要动态包含或排除的域。

注意：只能配置Include domains或Exclude domains。

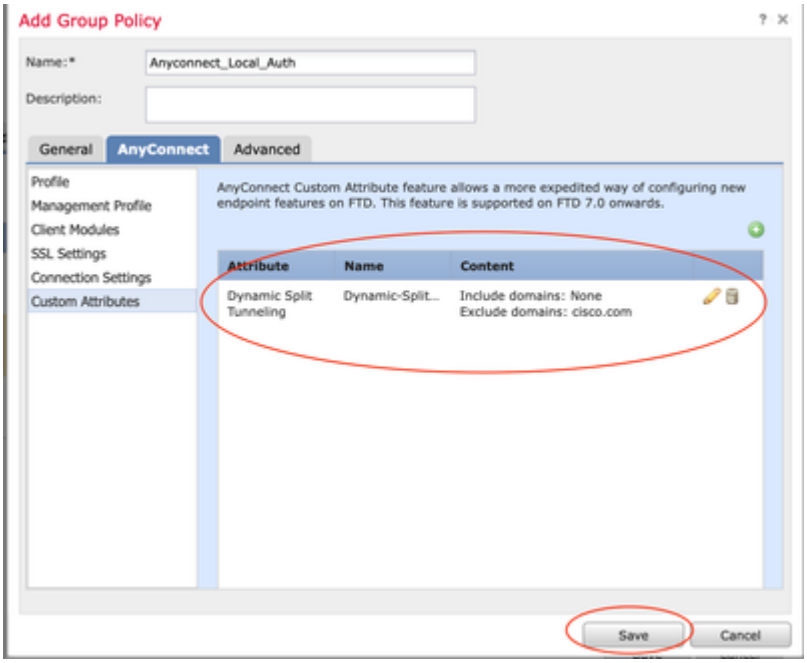


在本示例中，您将cisco.com配置为要排除的域，并将自定义属性命名为Dynamic-Split-Tunnel，如图所示：



步骤3.检验配置，保存并部署

验证已配置的自定义属性是否正确，保存配置并将更改部署到FTD。



验证

您可以通过命令行界面(CLI)在FTD上运行以下命令，以确认动态拆分隧道配置：

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy <group-policy的名称>

在本示例中，配置为：

<#root>

ftd# show run group-policy AnyConnect_Local_Auth

```
group-policy AnyConnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
```

anyconnect-custom dynamic-split-exclude-domains value cisco.com

```
anyconnect-custom dynamic-split-include-domains none
```

ftd# show run webvpn

```
webvpn
enable outside
```

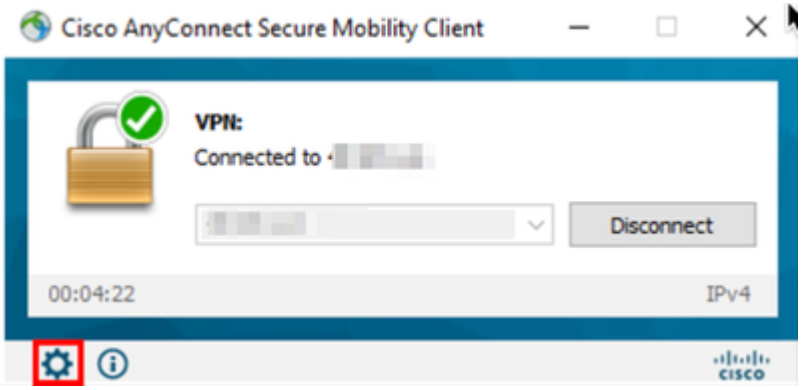
anyconnect-custom-attr dynamic-split-exclude-domains

```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
```

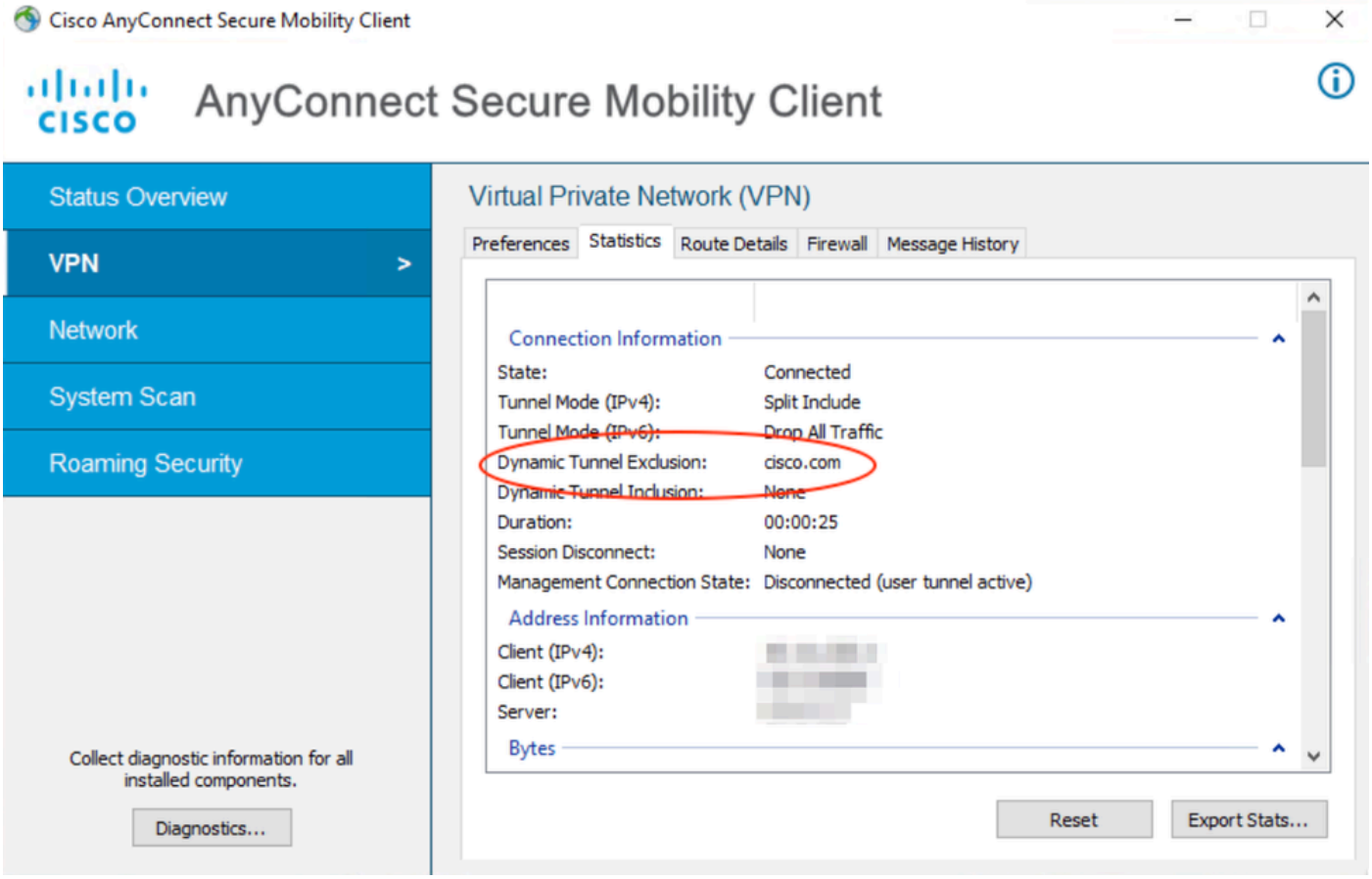
```
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

要验证客户端上配置的动态隧道排除，请执行以下操作：

1.启动AnyConnect软件并点击齿轮图标，如下图所示：



2.导航到VPN > Statistics，并确认在Dynamic Split Exclusion/Inclusion:



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 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。

问题

如果在AnyConnect自定义属性中配置了通配符（例如，*.cisco.com），则AnyConnect会话将断开连接。

解决方案

您可以使用cisco.com域值来替换通配符。此更改允许您包括或排除www.cisco.com and tools.cisco.com之类的域。

相关信息

- 如需其他帮助，请联系技术支持中心(TAC)。需要有效的支持合同：思科全球支持联系人
- 您还可以访问Cisco VPN社区。

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）。