使用ASDM为ASA上的特定流量配置连接超时

目录

简介

本文档介绍为特定应用协议（如HTTP、HTTPS、FTP或任何其他协议）配置ASA和ASDM上的连接超时。连接超时是指防火墙或网络设备在闲置连接终止之前可以释放资源并增强安全性的非活动时间。首先，第一个问题是：此配置有什么要求？如果应用具有正确的TCP保持连接设置，则通常不需要在防火墙上配置连接超时。但是，如果应用缺乏正确的Keepalive设置或超时配置，在这种情况下，在防火墙上配置连接超时对于管理资源、增强安全性、提高网络性能、确保合规性和优化用户体验至关重要。

要求

Cisco 建议您了解以下主题：

- 访问控制列表(ACL)
- 服务策略
- 连接超时

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA9.17(1)
- ASDM 7.17(1)

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。

默认设置

注意：默认超时

默认embryonic超时为30秒。

默认半关闭空闲超时为10分钟。

默认dcd max_retries值为5。

默认dcd retry_interval值为15秒。

默认tcp空闲超时为1小时。

默认udp空闲超时为2分钟。

默认icmp空闲超时为2秒。

默认sip空闲超时为30分钟。

默认sip_media空闲超时为2分钟。

默认esp和ha空闲超时为30秒。

对于所有其他协议，默认空闲超时为2分钟。

要永不超时，请输入0:0：0。

配置连接超时

ASDM

如果特定流量具有连接表，则该流量具有特定的空闲超时；例如，在本文中，我们将更改DNS流量的连接超时。

考虑到特定流量的网络图，以下许多选项可用于配置该流量的连接超时：

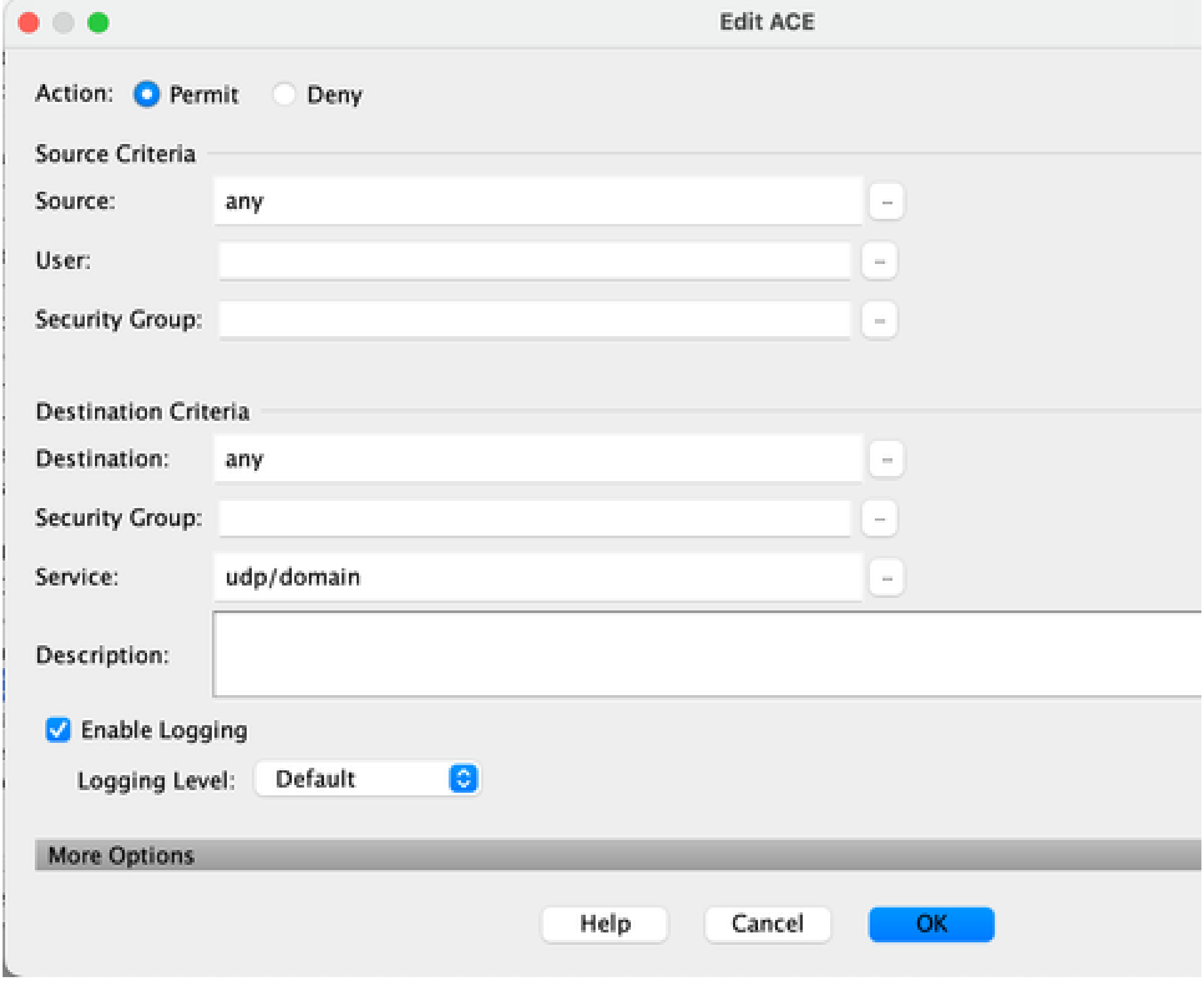
Client ----- [接口：MNG] Firewall [接口：OUT] ----- 服务器

可以为该接口分配ACL。

第1步：创建ACL

我们可以分配源、目标或服务

ASDM > Configuration > Firewall > Advanced > ACL Manager



Edit ACE

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: any

Security Group:

Service: udp/domain

Description:

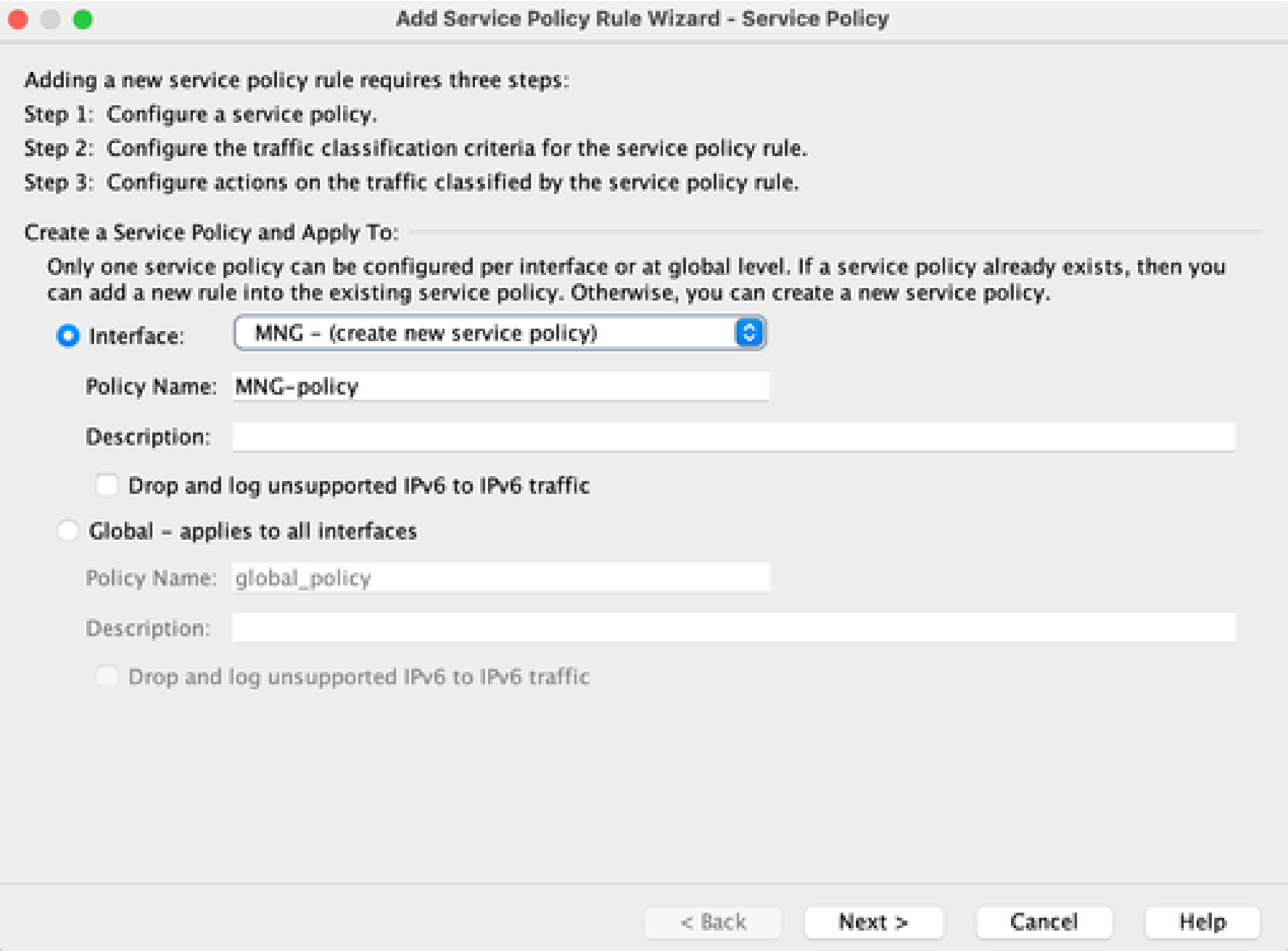
☑ Enable Logging

Logging Level: Default

第2步：创建服务策略规则

如果您已经有ACL，则可以跳过最后一步，也可以将其中一个参数（源、目标或服务）分配给接口的服务策略。

ASDM > Configuration > Firewall > Service Policy rules



Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

● Interface: MNG - (create new service policy)

Policy Name: MNG-policy

Description:

□ Drop and log unsupported IPv6 to IPv6 traffic

○ Global - applies to all interfaces

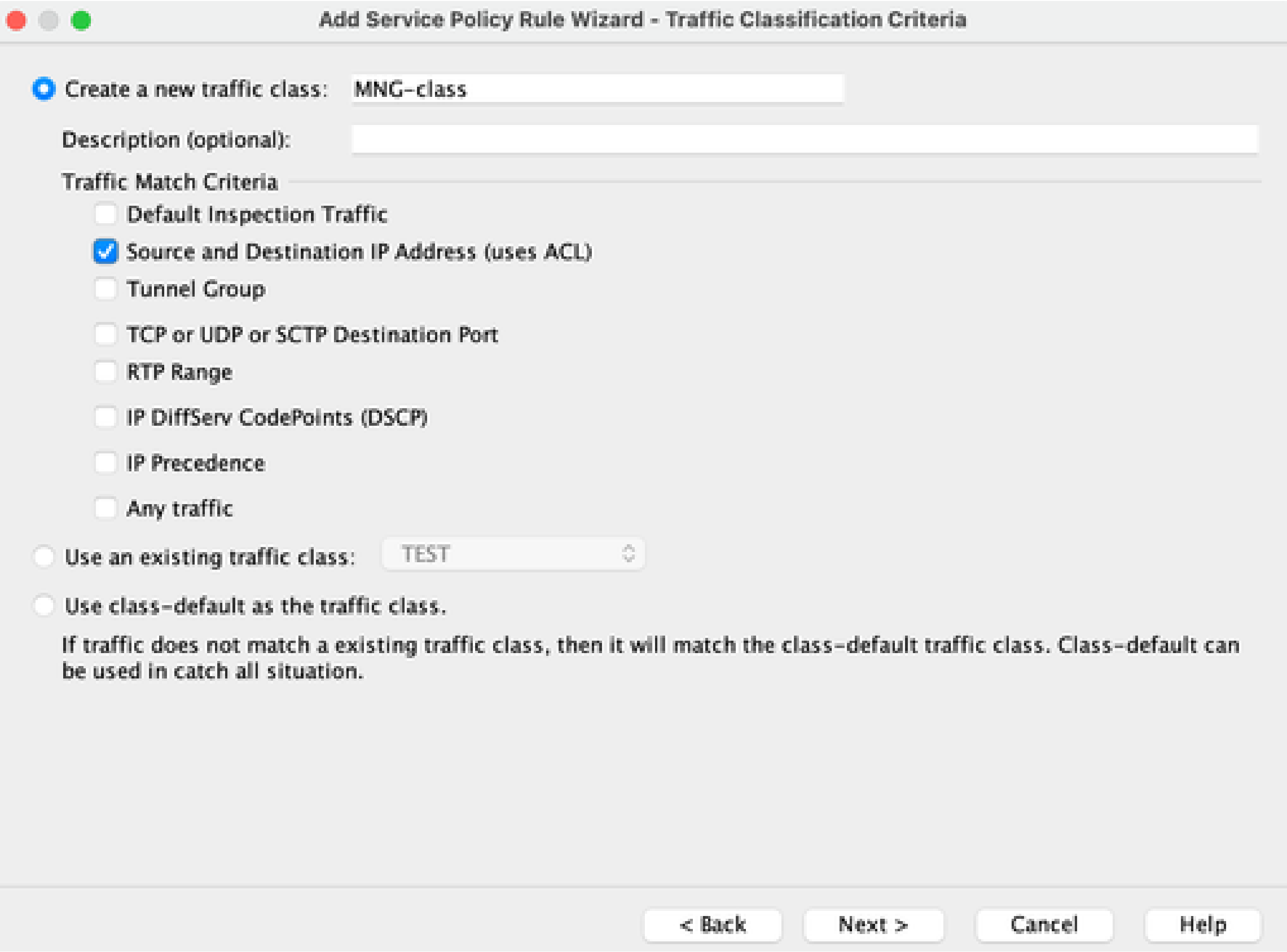
Policy Name: global_policy

Description:

□ Drop and log unsupported IPv6 to IPv6 traffic

第3步：创建流量类

可以选择源和目标IP地址（使用ACL）



Add Service Policy Rule Wizard - Traffic Classification Criteria

● Create a new traffic class: MNG-class

Description (optional):

Traffic Match Criteria

□ Default Inspection Traffic

☑ Source and Destination IP Address (uses ACL)

□ Tunnel Group

□ TCP or UDP or SCTP Destination Port

□ RTP Range

□ IP DiffServ CodePoints (DSCP)

□ IP Precedence

□ Any traffic

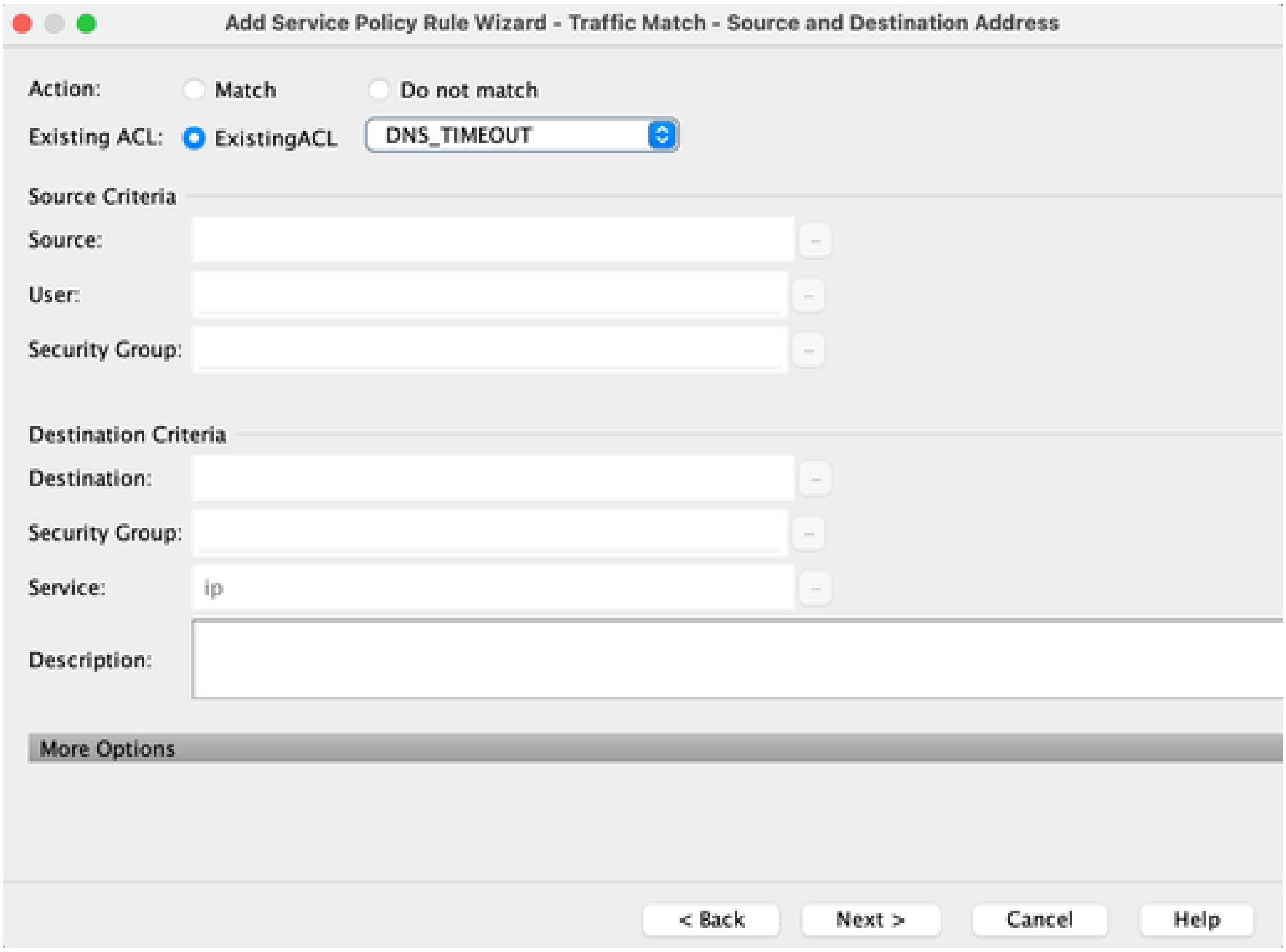
○ Use an existing traffic class: TEST

○ Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

第4步：分配ACL

在此步骤中，您可以分配现有ACL或选择匹配条件（源、目标或服务）



Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ○ Match ○ Do not match

Existing ACL: ● ExistingACL DNS_TIMEOUT

Source Criteria

Source:

User:

Security Group:

Destination Criteria

Destination:

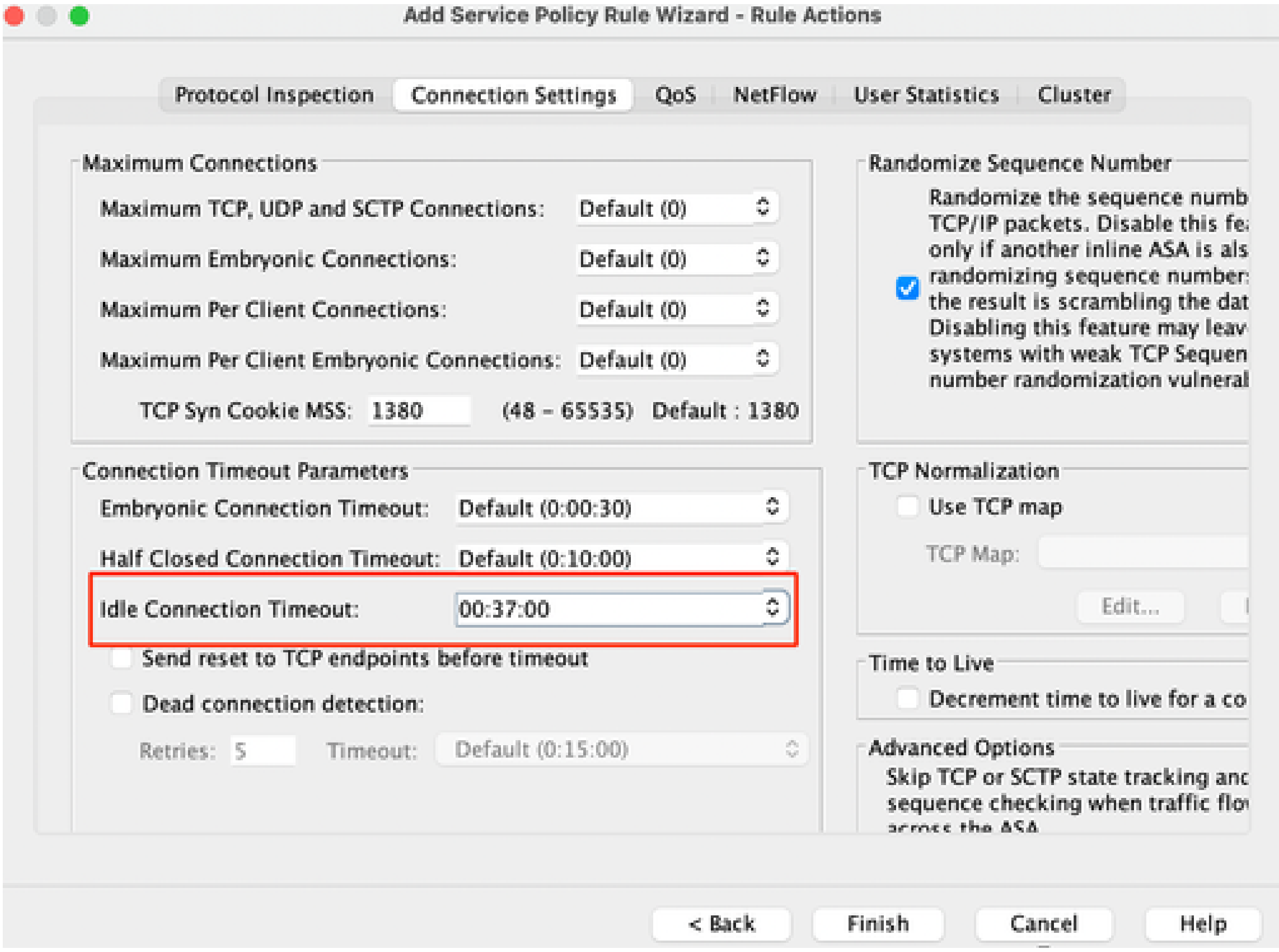
Security Group:

Service: ip

Description:

第5步：配置空闲超时参数

根据有效格式HH：MM：SS配置空闲超时。



Maximum Connections

Maximum TCP, UDP and SCTP Connections: Default (0)

Maximum Embryonic Connections: Default (0)

Maximum Per Client Connections: Default (0)

Maximum Per Client Embryonic Connections: Default (0)

TCP Syn Cookie MSS: 1380 (48 - 65535) Default : 1380

Connection Timeout Parameters

Embryonic Connection Timeout: Default (0:00:30)

Half Closed Connection Timeout: Default (0:10:00)

Idle Connection Timeout: 00:37:00

□ Send reset to TCP endpoints before timeout

□ Dead connection detection:

Retries: 5 Timeout: Default (0:15:00)

Randomize Sequence Number

☑ Randomize the sequence numb TCP/IP packets. Disable this fe only if another inline ASA is als randomizing sequence number the result is scrambling the dat Disabling this feature may leav systems with weak TCP Sequen number randomization vulneral

TCP Normalization

□ Use TCP map

TCP Map:

Edit...

Time to Live

□ Decrement time to live for a co

Advanced Options

Skip TCP or SCTP state tracking anc sequence checking when traffic flo across the ASA

清除该特定流量的连接：

```
#clear conn address输入IP地址或IP地址范围

#clear conn protocol输入此关键字以仅清除SCP/TCP/UDP连接
```

ASA CLI

您可以通过CLI配置所有这些设置：

```
ACL：

access-list DNS_TIMEOUT extended permit udp any any eq domain

Class-map:

class-map MNG-class
match access-list DNS_TIMEOUT

Policy-map:
```

```
policy-map MNG-policy
class MNG-class
set connection timeout idle 0:37:00
```

在接口上应用策略映射：

```
service-policy MNG-policy interface MNG
```

验证

提示：如果我们运行此命令，则可以确认DNS流量的连接超时：

ASA CLI > enable mode > show conn long

示例：show conn long address 192.168.1.1

```
UDP MNG：192.168.1.1/53 (192.168.1.1/53)输出：10.10.10.30/63327 (10.10.10.30/63327)，标志-，空闲17，正常运行时间17，超时2m0s，字节36

UDP MNG：192.168.1.1/53 (192.168.1.1/53)输出：10.10.10.30/62558 (10.10.10.30/62558)，标志-，空闲40，正常运行时间40，超时2m0，字节36
```

然后，在配置之后，我们可以确认空闲超时配置：

示例：show conn long address 192.168.1.1

```
UDP MNG：192.168.1.1/53 (192.168.1.1/53)输出：10.10.10.30/63044 (10.10.10.30/63044)，标志- ，空闲8秒，正常运行时间8秒，超时37m0秒，字节37

UDP MNG：192.168.1.1/53 (192.168.1.1/53)输出：10.10.10.30/63589 (10.10.10.30/63589)，标志-、空闲5s、正常运行时间5s、超时37m0s、字节41
```

参考

什么是连接设置

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）。