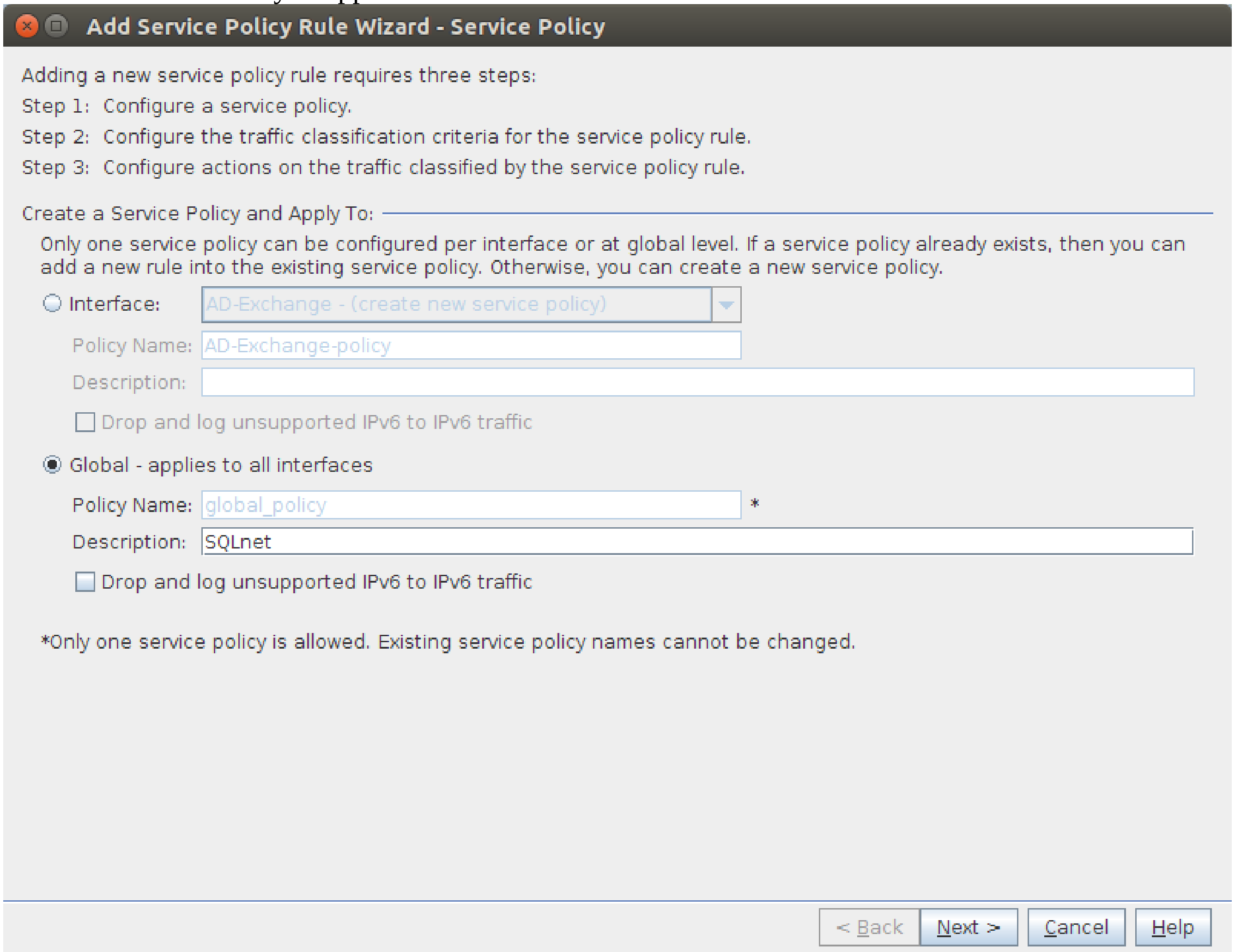
Add New Global Policy – Applies to ALL interfaces.



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: AD-Exchange - (create new service policy)

Policy Name: AD-Exchange-policy

Description:

□ Drop and log unsupported IPv6 to IPv6 traffic

● Global - applies to all interfaces

Policy Name: global_policy *

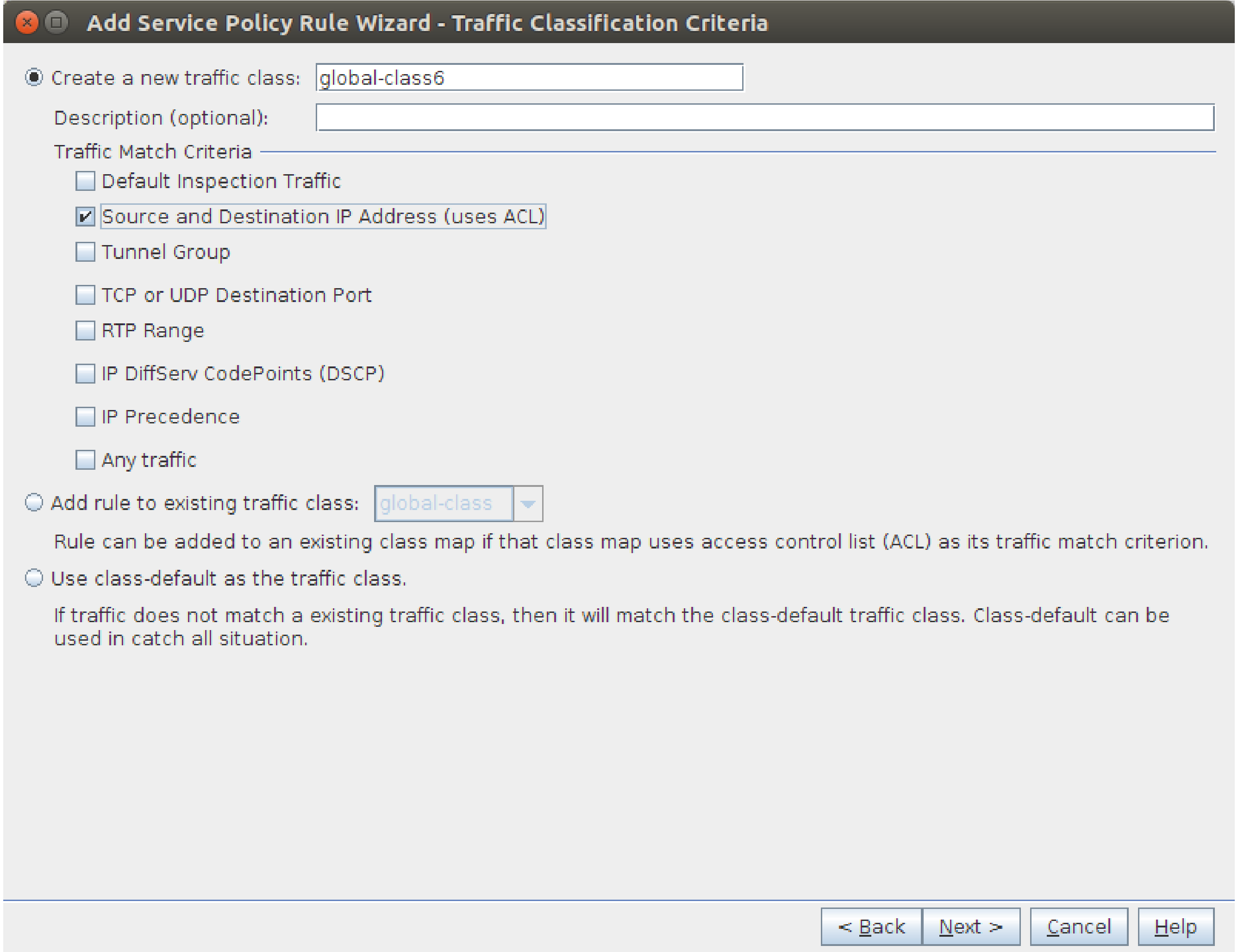
Description: SQLnet

□ Drop and log unsupported IPv6 to IPv6 traffic

*Only one service policy is allowed. Existing service policy names cannot be changed.

Hit Next

Select the ACL Option



Add Service Policy Rule Wizard - Traffic Classification Criteria

● Create a new traffic class: global-class6

Description (optional):

Traffic Match Criteria

□ Default Inspection Traffic

☑ Source and Destination IP Address (uses ACL)

□ Tunnel Group

□ TCP or UDP Destination Port

□ RTP Range

□ IP DiffServ CodePoints (DSCP)

□ IP Precedence

□ Any traffic

○ Add rule to existing traffic class: global-class

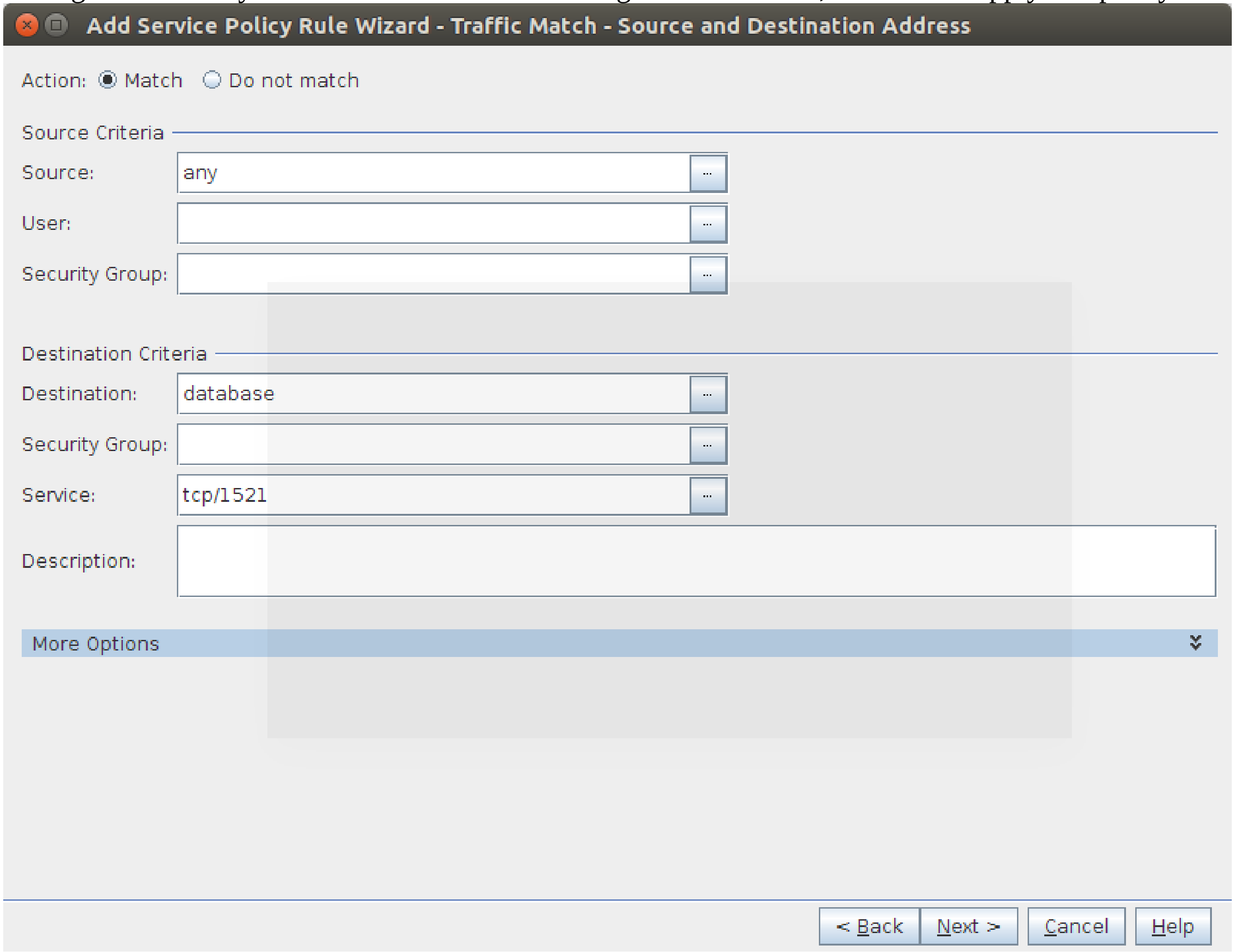
Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match criterion.

○ 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.

Hit next

Configure the ACL you want to match for interesting database traffic, that we can apply this policy to



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

Action: ● Match ○ Do not match

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: database

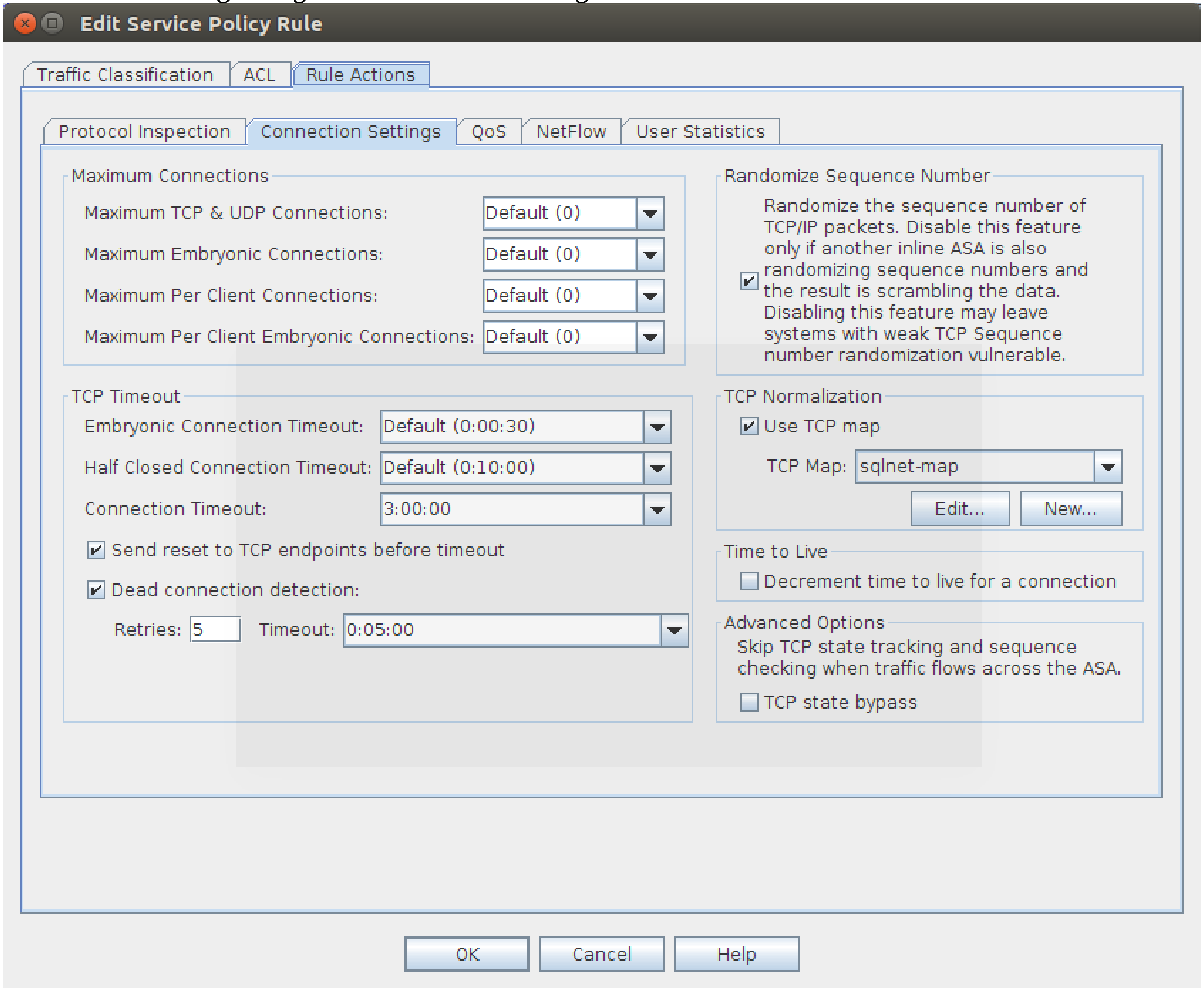
Security Group:

Service: tcp/1521

Description:

Hit next

Make the following changes to Connection Settings



Maximum Connections

Maximum TCP & UDP Connections: Default (0)

Maximum Embryonic Connections: Default (0)

Maximum Per Client Connections: Default (0)

Maximum Per Client Embryonic Connections: Default (0)

TCP Timeout

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

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

Connection Timeout: 3:00:00

☑ Send reset to TCP endpoints before timeout

☑ Dead connection detection:

Retries: 5 Timeout: 0:05:00

Randomize Sequence Number

☑ Randomize the sequence number of TCP/IP packets. Disable this feature only if another inline ASA is also randomizing sequence numbers and the result is scrambling the data. Disabling this feature may leave systems with weak TCP Sequence number randomization vulnerable.

TCP Normalization

☑ Use TCP map

TCP Map: sqlnet-map

Time to Live

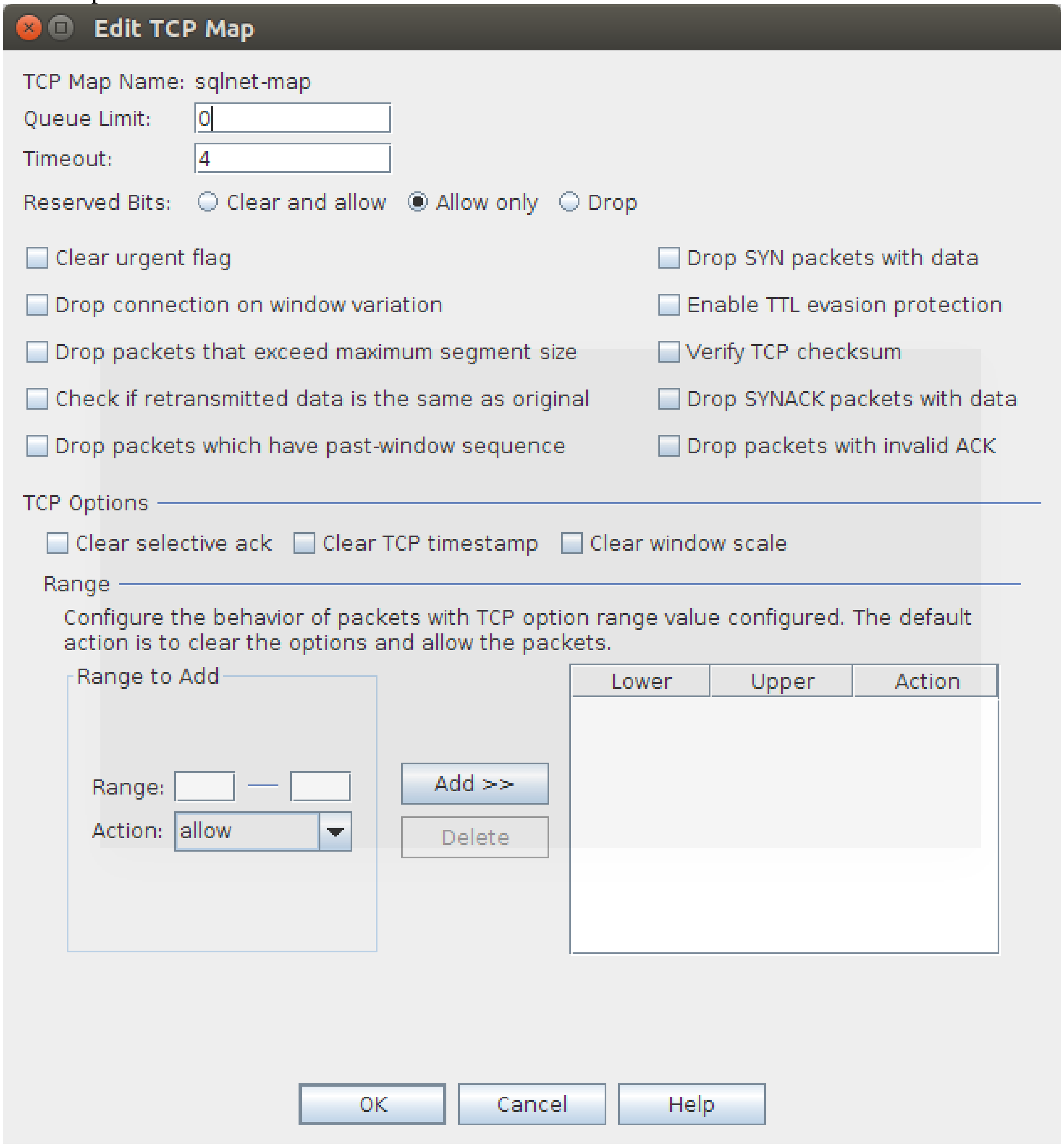
☐ Decrement time to live for a connection

Advanced Options

Skip TCP state tracking and sequence checking when traffic flows across the ASA.

☐ TCP state bypass

TCP Map should look like this:



Edit TCP Map

TCP Map Name: sqlnet-map

Queue Limit: 0

Timeout: 4

Reserved Bits: ○ Clear and allow ● Allow only ○ Drop

□ Clear urgent flag

□ Drop connection on window variation

□ Drop packets that exceed maximum segment size

□ Check if retransmitted data is the same as original

□ Drop packets which have past-window sequence

□ Drop SYN packets with data

□ Enable TTL evasion protection

□ Verify TCP checksum

□ Drop SYNACK packets with data

□ Drop packets with invalid ACK

TCP Options

□ Clear selective ack □ Clear TCP timestamp □ Clear window scale

Range

Configure the behavior of packets with TCP option range value configured. The default action is to clear the options and allow the packets.

Range to Add

Range: —

Action: allow

Lower	Upper	Action