

Configure Connection Timeout for Specific Traffic on ASA with ASDM

Contents

[Introduction](#)

- [Requirements](#)
- [Components Used](#)
- [Defaults](#)

[Configure Connection Timeout](#)

- [ASDM](#)
- [ASA CLI](#)

[Verify](#)

[References](#)

Introduction

This document describes configuring Connection timeout on ASA and ASDM for a specific application protocol such as HTTP, HTTPS, FTP, or any other protocols. Connection timeout is the period of inactivity after which a firewall or network device terminates an idle connection to free up resources and enhance security. In advance, the first question is: What is the requirement for this configuration? If applications have proper TCP keepalive settings, configuring connection timeout on a firewall is often unnecessary. However, if applications lack proper keepalive settings or timeout configurations, in that case configuring connection timeout on a firewall is crucial for managing resources, enhancing security, improving network performance, ensuring compliance, and optimizing user experience.

Requirements

Cisco recommends that you have knowledge of these topics:

- Access Control List (ACL)
- Service Policy
- Connection Timeout

Components Used

The information in this document is based on these software and hardware versions:

- ASA 9.17(1)

- ASDM 7.17(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Defaults

 **Note:** Default timeout

The default **embryonic** timeout is 30 seconds.

The default **half-closed** idle timeout is 10 minutes.

The default **dcd** *max_retries* value is 5.

The default **dcd** *retry_interval* value is 15 seconds.

The default **tcp** idle timeout is 1 hour.

The default **udp** idle timeout is 2 minutes.

The default **icmp** idle timeout is 2 seconds.

The default **sip** idle timeout is 30 minutes.

The default **sip_media** idle timeout is 2 minutes.

The default **esp** and **ha** idle timeout is 30 seconds.

For all other protocols, the default idle timeout is 2 minutes.

To never time out, enter 0:0:0.

Configure Connection Timeout

ASDM

If a particular traffic has a connection table, it has a specific idle timeout; for example, in this article, we change the connection timeout for DNS traffic.

Here are many options to configure the Connection Timeout for specific traffic, considering the network diagram of this traffic:

Client ----- [Interface: MNG] **Firewall** [Interface: OUT] ----- **Server**

There is the possibility of assigning an ACL to the interface.

Step1: Create an ACL

We can assign Source, Destination, or Service

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

More Options

Help Cancel OK

Step2: Create Service Policy rule

You can skip the last step if you already have your ACL, or you can assign one of those parameters (source, Destination, or Service) to the Service Policy to the Interface.

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:

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

Global - applies to all interfaces

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

Step3: Create traffic class

There is a possibility to choose **Source and Destination IP Address (uses ACL)**

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic 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:

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.


< Back Next > Cancel Help

Step4: Assign ACL


In this step, you can assign the existing ACL or select match conditions (source, Destination, or Service)


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


Action: Match Do not match

Existing ACL: ExistingACL 


Source Criteria


Source: 


User: 

Security Group: 

Destination Criteria

Destination: 

Security Group: 

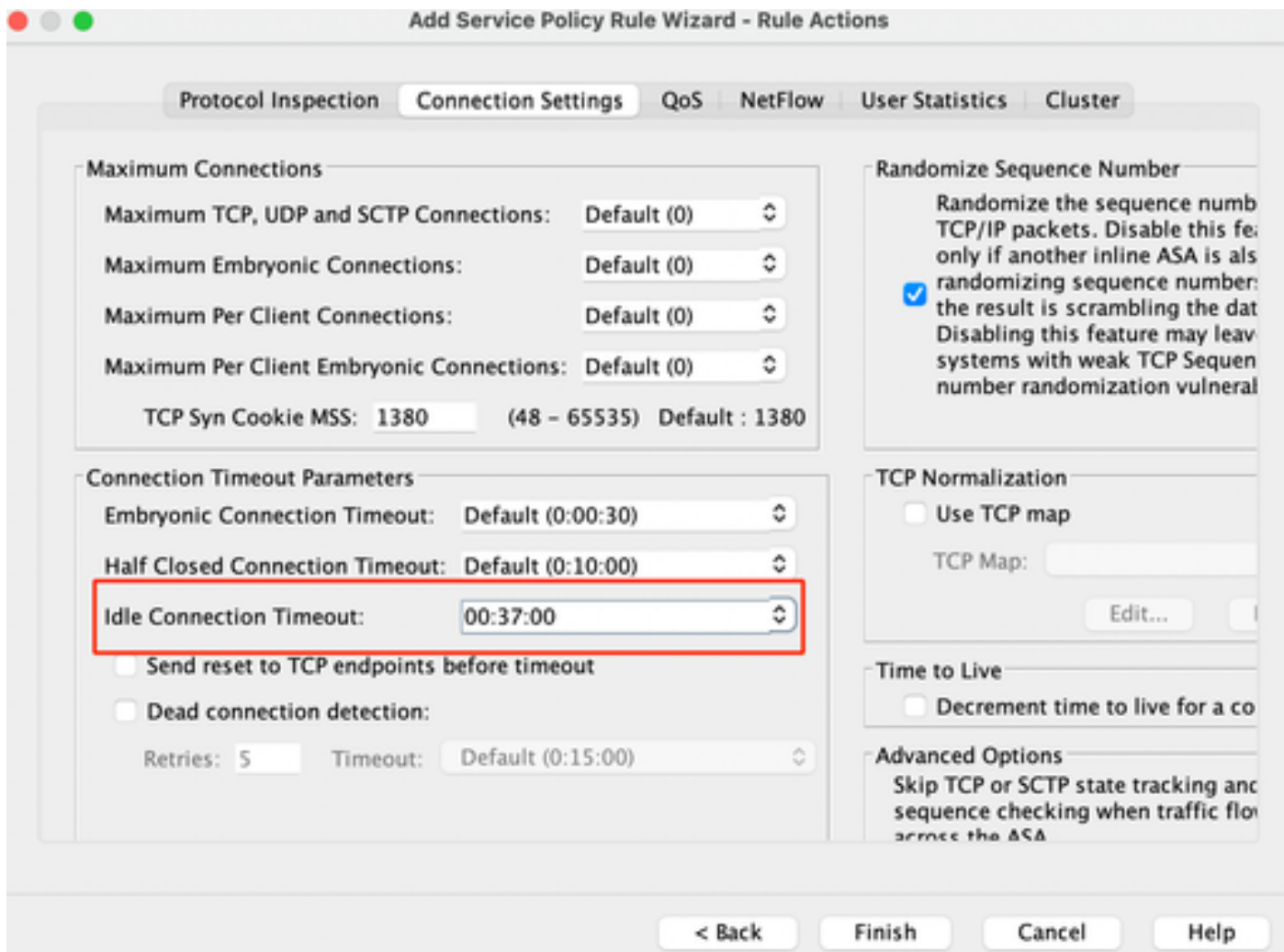
Service: 

Description:

More Options

Step5: Configure the Idle Timeout parameter

Based on valid format HH:MM:SS configure the Idle timeout.



Clear connections for that particular traffic:

```
#clear conn address Enter an IP address or a range of IP addresses
#clear conn protocol Enter this keyword to clear SCP/TCP/UDP conns only
```

ASA CLI

You can configure all these settings via the CLI:

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
```

Apply the Policy-map on the Interface:

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

Verify



Tip: If we run this command, we can confirm the connection timeout of the DNS traffic:

ASA CLI > enable mode > show conn long

Example: *show conn long address 192.168.1.1*

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flags - , idle
17s, uptime 17s, timeout 2m0s, bytes 36
```

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flags - , idle
40s, uptime 40s, timeout 2m0s, bytes 36
```

Then, after configuration, we can confirm the idle timeout configuration:

Example: *show conn long address 192.168.1.1*

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flags - , idle
8s, uptime 8s, timeout 37m0s, bytes 37
```

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flags - , idle
5s, uptime 5s, timeout 37m0s, bytes 41
```

References

[What Are Connection Settings](#)