



Loopback Interfaces

This chapter tells how to configure loopback interfaces.

- [About Loopback Interfaces, on page 1](#)
- [Guidelines for Loopback Interfaces, on page 2](#)
- [Configure a Loopback Interface, on page 2](#)
- [Rate-Limit Traffic to the Loopback Interface, on page 3](#)
- [History for Loopback Interfaces, on page 7](#)

About Loopback Interfaces

A loopback interface is a software-only interface that emulates a physical interface. This interface is reachable on IPv4 and IPv6 through multiple physical interfaces. The loopback interface helps to overcome path failures; it is accessible from any physical interface, so if one goes down, you can access the loopback interface from another.

Loopback interfaces can be used for:

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- Static and dynamic VTI tunnels
- Syslog
- Telnet

The ASA can distribute the loopback address using dynamic routing protocols, or you can configure a static route on the peer device to reach the loopback IP address through one of the ASA's physical interfaces. You cannot configure a static route on the ASA that specifies the loopback interface.

Guidelines for Loopback Interfaces

Failover and Clustering

- No clustering support.

Context Mode

- VTI is supported in single context mode only. Other loopback uses are supported in multiple context mode.

Additional Guidelines and Limitations

- TCP sequence randomization is always disabled for traffic from the physical interface to the loopback interface.

Configure a Loopback Interface

Add a loopback interface.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Choose Configuration > Device Setup > Interface Settings > Interfaces . |
| Step 2 | Choose Add > Loopback Interface .
The Add Loopback Interface dialog box appears. |
| Step 3 | In the Loopback ID field, enter an integer between 0 and 10413. |
| Step 4 | If the interface is not already enabled, check the Enable Interface check box.
The interface is enabled by default. |
| Step 5 | (Optional) Enter a description in the Description field. |
| Step 6 | Configure the name and IP address. See Routed and Transparent Mode Interfaces . |
| Step 7 | Click OK .
You return to the Interfaces pane. |
| Step 8 | Configure rate-limiting for loopback traffic. See Rate-Limit Traffic to the Loopback Interface, on page 3 . |
-

Rate-Limit Traffic to the Loopback Interface

You should rate-limit traffic going to the loopback interface IP address to prevent excessive load on the system. You can add a connection limit rule to the global service policy. This procedure shows adding to the default global policy (global_policy).

Procedure

Step 1 Choose **Configuration > Firewall > Service Policy**, and click **Add > Add Service Policy Rule**.

Step 2 Choose the **Global** policy and click **Next**.

Figure 1: Service Policy

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:** inside - (create new service policy)

Policy Name: inside-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

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

< Back Next > Cancel Help

Step 3 On the **Traffic Classification Criteria** page, set the following values and click **Next**.

Figure 2: Traffic Classification Criteria

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 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

- **Create a new traffic class**—Name the loopback traffic class.
- **Source and Destination IP Address (uses ACL)**

Step 4 On the **Traffic Match - Source and Destination Address** page, define the access control list to specify all IP traffic going to the loopback IP address, and click **Next**.

Figure 3: Traffic Match - Source and Destination Address

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

Action: ☒ Match ☐ Do not match

Existing ACL: ☐ ExistingACL

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: loopback1, loopback2

Security Group:

Service: ip

Description:

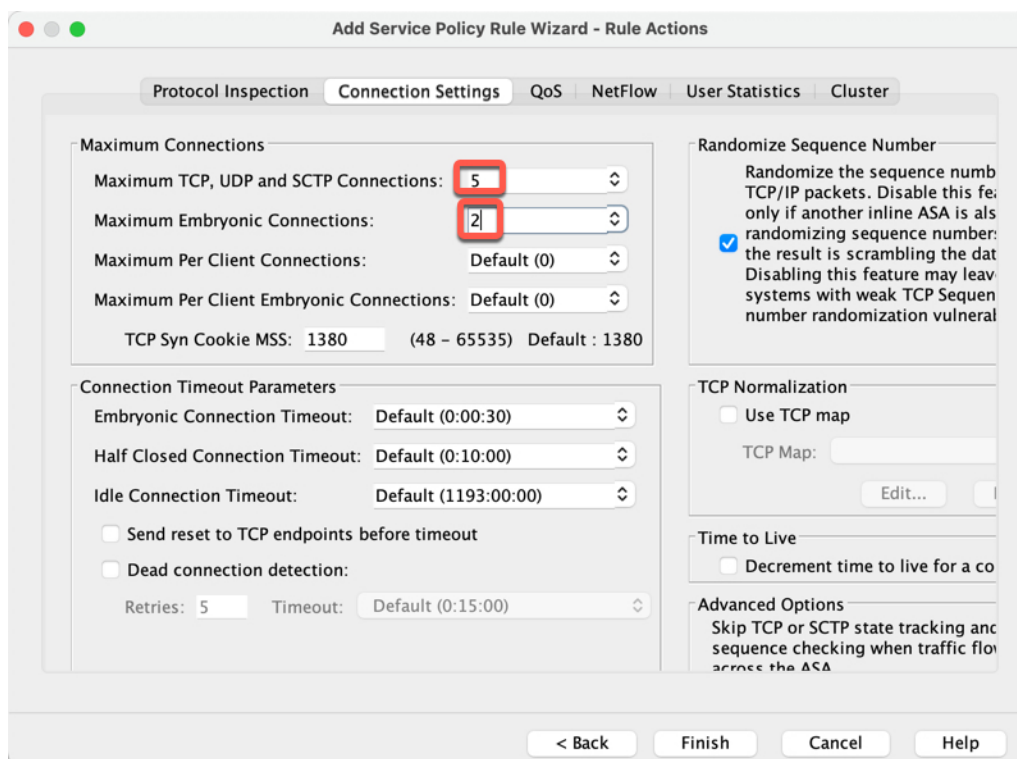
More Options

< Back Next > Cancel Help

- **Action:** Match
- **Source**—any. You can also narrow this access list by specifying the source IP addresses instead of **any**.
- **Destination**—The loopback interface IP addresses
- **Service**—ip

Step 5 On the **Rule Actions** page, click the **Connection Settings** tab, and in the **Maximum Connections** area, set the following values.

Figure 4: Rule Actions



- **Maximum TCP, UDP and SCTP Connections**—Set the maximum connections to the expected number of connections for the loopback interface, and the embryonic connections to a lower number. For example, you can set it to 5/2, or 10/5, or 1024/512, depending on the expected loopback interface sessions you need.
- **Embryonic Connections**—Setting the embryonic connection limit enables TCP Intercept, which protects the system from a DoS attack perpetrated by flooding an interface with TCP SYN packets.

Step 6 Click **Finish**.

The rule is added to the global policy.

Figure 5: Service Policy Rules Table

Configuration > Firewall > Service Policy Rules										
Add Edit Delete Find Diagram Packet Trace										
Traffic Classification	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions
Global; Policy: global_policy										
inspection_default			Match	any		any		default-in...		Inspect DNS Map p... Inspect ESMT... (12 more inspect actio..
rate-limit-loopback	1	✓	Match	any		loopback1 loopback2		ip		Max TCP/UDP Con... Max Embryonic Co...

Step 7 Click **Apply**.

History for Loopback Interfaces

Table 1: History for Loopback Interfaces

Feature Name	Version	Feature Information
Loopback interface support for DNS, HTTP, ICMP, and IPsec Flow Offload	9.2(1)	<p>You can now add a loopback interface and use it for:</p> <ul style="list-style-type: none"> • DNS • HTTP • ICMP • IPsec Flow Offload
Loopback interface support for VTI	9.1(1)	<p>A loopback interface provides redundancy of static and dynamic VTI VPN tunnels. You can now set a loopback interface as the source interface for a VTI. The VTI interface can also inherit the IP address of a loopback interface instead of a statically configured IP address. The loopback interface helps to overcome path failures. If an interface goes down, you can access all interfaces through the IP address of the loopback interface.</p> <p>New/Modified screens: Configuration > Device Setup > Interface Settings > Interfaces > Add VTI Interface > Advanced</p>
ASDM support for loopback interfaces	9.1(1)	<p>ASDM now supports loopback interfaces.</p> <p>New/Modified screens: Configuration > Device Setup > Interface Settings > Interfaces > Add Loopback Interface</p>
Support for loopback interface	9.1(2)	<p>You can now add a loopback interface and use it for:</p> <ul style="list-style-type: none"> • BGP • AAA • SNMP • Syslog • SSH • Telnet <p>New/Modified commands: interface loopback, logging host, neighbor update-source, snmp-server host, ssh, telnet</p> <p>No ASDM support.</p>

