

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 2
- Monitoring Loopback Interfaces, on page 4
- History for Loopback Interfaces, on page 4

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
- SNMP
- SSH
- 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 Create a loopback interface:

interface loopback *number*

The number can be between 0 and 10413.

Example:

```
ciscoasa(config)# interface loopback 10
```

Step 2 Configure the name and IP address. See Routed and Transparent Mode Interfaces.

Step 3 Configure rate-limiting for loopback traffic. See Rate-Limit Traffic to the Loopback Interface, on page 2.

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 Create an access list identifying traffic to the loopback interface IP address.

access-list *name* **extended permit ip any host** *loopback_ip*

Create an ACE for each loopback interface IP address. You can also narrow this access list by specifiying the source IP addresses instead of **any**.

Example:

```
ciscoasa(config)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
```

Step 2 Create a class map that identifies the access list.

class-map *name*

match access-list *acl_name*

Example:

```
ciscoasa(config)# class-map rate-limit-loopback
ciscoasa(config-cmap)# match access-list loop
```

Step 3 Apply maximum connections and maximum embryonic connections to the class map as part of the global policy map.

policy-map global_policy

class *class_map_name*

set connection conn-max *conns* **embryonic-conn-max** *conns*

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.

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.

Example:

```
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class rate-limit-loopback
ciscoasa(config-pmap-c)# set connection conn-max 5 embryonic-conn-max 2
```

Example

The following example sets the maximum connections and embryonic connections to 10 and 5 for the default global policy for all traffic going to two loopback interfaces at 10.1.1.1 and 10.2.1.1.

```
ciscoasa(config)# interface loopback 1
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop1
ciscoasa(config-if)# interface loopback 2
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop2
ciscoasa(config-if)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match access-list loop
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection conn-max 10 embryonic-conn-max 5
```

Monitoring Loopback Interfaces

See the following commands:

- **show interface**

  Displays interface statistics.

- **show interface ip brief**

  Displays interface IP addresses and status.

History for Loopback Interfaces

Table 1: History for Loopback Interfaces

Feature Name	Version	Feature Information
Support for loopback interface	9.18(2)	You can now add a loopback interface and use it for: • BGP • AAA • SNMP • Syslog • SSH • Telnet New/Modified commands: **interface loopback**, **logging host**, **neighbor update-source**, **snmp-server host**, **ssh**, **telnet**