环回接口

本部分介绍如何配置环回接口。

关于环回接口

环回接口是一种会模拟物理接口的纯软件接口。此接口可通过多个物理接口在IPv4和IPv6上访问。环回接口有助于克服路径故障；它可以从任何物理接口访问，因此，如果其中一个接口发生故障，您可以从另一个接口访问环回接口。

环回接口可用于：

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- 静态和动态 VTI 隧道
- 系统日志
- Telnet

ASA可以使用动态路由协议分发环回地址，也可以在对等设备上配置静态路由，以通过ASA的物理接口之一到达环回 IP 地址。不能在指定环回接口的 ASA 上配置静态路由。

环回接口准则

故障转移和集群

- 无集群支持。

情景模式

- VTI 仅支持单情景模式。在多情景模式下支持其他环回用途。

其他准则和限制

- 对于从物理接口到环回接口的流量，TCP 序列随机化始终处于禁用状态。

配置环回接口

添加环回接口。

过程

步骤 1 创建环回接口：

interface loopback 编号

数字可以介于 0 和 10413 之间。

示例：

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

步骤 2 配置名称和 IP 地址。请参阅路由模式接口和透明模式接口。

步骤 3 配置环回的速率限制。请参阅对流向环回接口的流量进行速率限制，第 2 页。

对流向环回接口的流量进行速率限制

您应该对流向环回接口 IP 地址的流量进行速率限制，以防止系统负载过大。您可以向全局服务策略添加连接限制规则。此程序会显示添加到默认全局策略 (global_policy)。

过程

步骤 1 创建用于识别流向环回接口 IP 地址的流量的访问列表。

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

为每个环回接口 IP 地址创建 ACE。您还可以通过指定源 IP 地址而不是 **任何**来缩小此访问列表的范围。

示例：

```
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
```

步骤 2 创建可标识访问列表的类映射。

class-map 名称

match access-list *acl_name*

示例：

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

步骤 3 将最大连接数和最大初期连接数作为全局策略映射的一部分应用于类映射。

policy-map global_policy

class *class_map_name*

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

将最大连接数设置为环回接口的预期连接数，并将初期 连接数设置为较低的数字。例如，您可以将其设置为 5/2、10/5 或 1024/512，具体取决于所需的预期环回接口会话。

设置初期连接限制触发 TCP 拦截，从而防止系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。

示例：

```
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
```

示例

以下示例将默认全局策略的最大连接数和初期连接数设为 10.1.1.1 和 10.2.1.1 处的两个环回接口。

```
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
```

监控环回接口

请参阅以下命令：

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

环回接口的历史记录

表 *1:* 环回接口的历史记录

功能名称	版本	功能信息
环回接口支持 DNS、HTTP、ICMP 和 IPsec 分流	9.20(1)	您现在可以添加环回接口并用于： • DNS • HTTP • ICMP • IPsec 流分流
VTI 的环回接口支持	9.19(1)	环回接口提供静态和动态 VTI VPN 隧道的冗余。现在，您可以将环回接口设置为 VTI 的源接口。VTI 接口可以从环回接口继承 IP 地址，而不是静态配置的 IP 地址。环回接口有助于克服路径故障。如果接口发生故障，您可以通过环回接口的 IP 地址来访问所有接口。 新增/修改的命令：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered**

功能名称	版本	功能信息
支持环回接口	9.18(2)	您现在可以添加环回接口并用于： • BGP • AAA • SNMP • 系统日志 • SSH • Telnet 新增/修改的命令：**interface loopback**、**logging host**、**neighbor update-source**、**snmp-server host**、**ssh**、**telnet**

环回接口的历史记录

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。