



环回接口

本部分介绍如何配置环回接口。

- [关于环回接口，第 1 页](#)
- [环回接口准则，第 2 页](#)
- [配置环回接口，第 2 页](#)
- [对流向环回接口的流量进行速率限制，第 3 页](#)
- [环回接口历史记录，第 7 页](#)

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
- 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 依次选择 **配置 > 设备设置 > 接口设置 > 接口**。

步骤 2 依次选择 **添加 > 回环接口**。

系统将显示 **添加回环接口** 对话框。

步骤 3 在 **环回 ID** 字段中，输入一个介于 0 和 10413 之间的整数。

步骤 4 如果该接口尚未启用，请选中 **Enable Interface** 复选框。

默认情况下，该接口已启用。

步骤 5 （可选）在 **说明** 字段中输入说明。

步骤 6 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 7 点击**确定 (OK)**。

系统将返回到 **Interfaces** 窗格。

步骤 8 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 3 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** 选择配置 (Configuration) > 防火墙 (Firewall) > 服务策略 (Service Policy)，然后单击添加 (Add) > 添加服务策略规则 (Add Service Policy Rule)。
- 步骤 2** 选择全局 (Global) 策略，然后单击下一步 (Next)。

图 1: 服务政策

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:

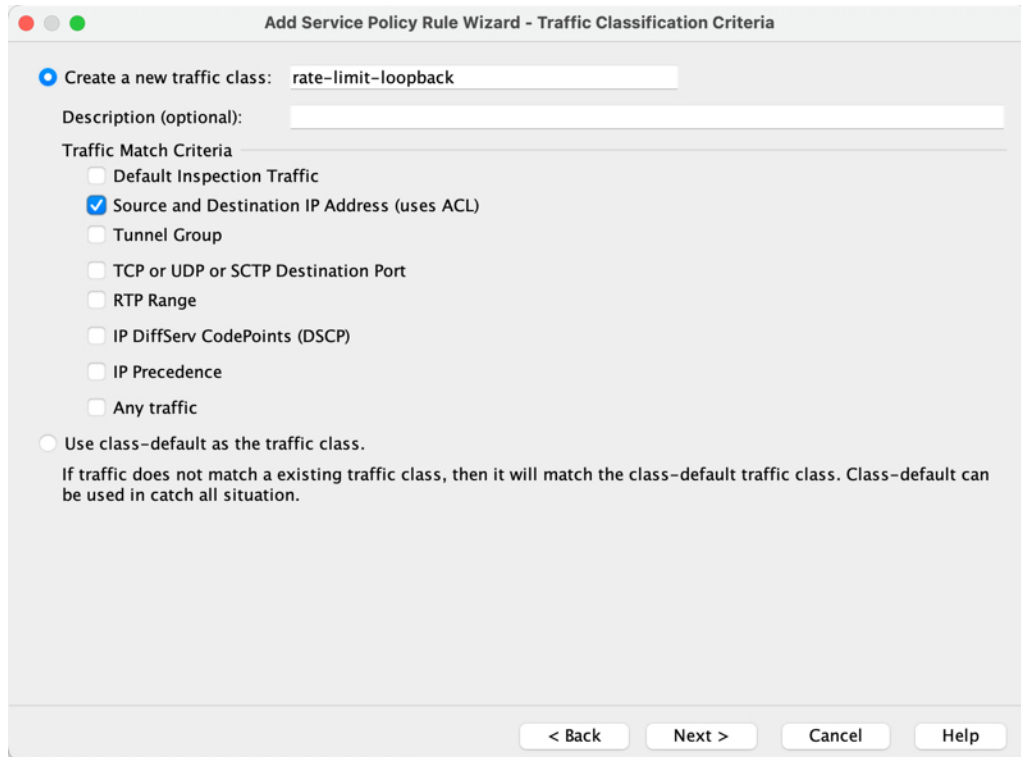
Drop and log unsupported IPv6 to IPv6 traffic

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

< Back Next > Cancel Help

- 步骤 3** 在流量分类条件 (Traffic Classification Criteria) 页面上设置以下值，然后单击下一步 (Next)。

图 2: 流量分类标准



- 创建新流量类 (Create a new traffic class) - 为环回流量类命名。
- 源和目标 IP 地址 (使用 ACL)

步骤 4 在流量匹配 - 源和目标地址 (Traffic Match - Source and Destination Address) 页面上, 定义访问控制列表以指定流向环回 IP 地址的所有 IP 流量, 然后点击下一步 (Next)。

图 3: 流量匹配 - 源和目标地址

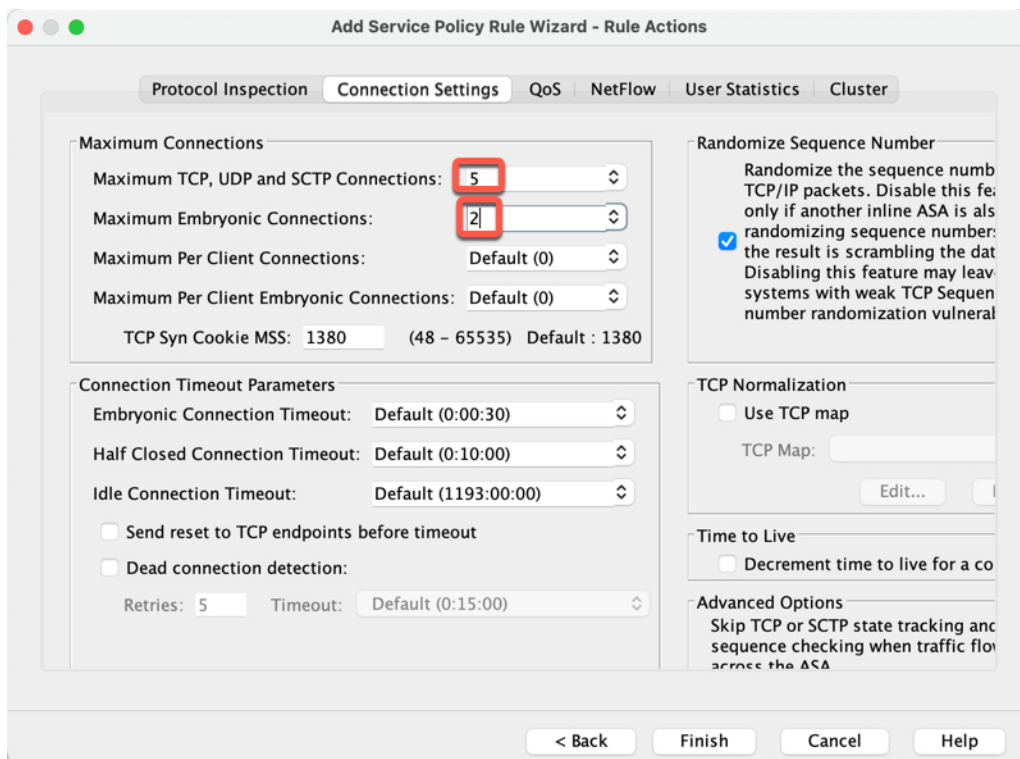
The screenshot shows a configuration window titled "Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address". It contains several sections:

- Action:** Radio buttons for "Match" (selected) and "Do not match".
- Existing ACL:** Radio button for "ExistingACL".
- Source Criteria:** Fields for "Source:" (value: any), "User:", and "Security Group:". The "Source:" field is highlighted with a red box.
- Destination Criteria:** Fields for "Destination:" (value: loopback1, loopback2), "Security Group:", and "Service:" (value: ip). The "Destination:" and "Service:" fields are highlighted with red boxes.
- Description:** An empty text area.
- More Options:** A collapsed section.
- Navigation:** Buttons for "< Back", "Next >", "Cancel", and "Help".

- 操作: 匹配
- 源 (Source) - 任意。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。
- 目标 (Destination) - 环回接口 IP 地址
- 服务 (Service) - ip

步骤 5 在规则操作 (Rule Actions) 页面上, 点击连接设置 (Connection Settings) 选项卡, 然后在最大连接数 (Maximum Connections) 区域中设置以下值。

图 4: 规则操作



- **最大 TCP、UDP 和 SCTP 连接数 (Maximum TCP, UDP and SCTP Connections)** - 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。
- **初期连接数 (Embryonic Connections)** - 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）。

步骤 6 点击完成。

规则会被添加到全局策略中。

图 5: 服务策略规则表

Traffic Classification	Name	#	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 ESMTMP (12 more inspect actio...
	rate-limit-loopback	1	✓	Match	any		loopback1 loopback2		ip		Max TCP/UDP Con... Max Embryonic Co...

步骤 7 点击 Apply。

环回接口历史记录

表 1: 环回接口历史记录

功能名称	版本	功能信息
VTI 的环回接口支持	919(1)	<p>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。</p> <p>新增/修改的屏幕：配置 > 设备设置 > 接口设置 > 接口 > 添加 VTI 接口 > 高级</p>
ASDM 支持环回接口	919(1)	<p>ASDM 现在支持环回接口。</p> <p>新增/修改的屏幕：配置 > 设备设置 > 接口设置 > 接口 > 添回环接口</p>
支持环回接口	918(2)	<p>您现在可以添加环回接口并用于：</p> <ul style="list-style-type: none"> • BGP • AAA • SNMP • 系统日志 • SSH • Telnet <p>新增/修改的命令：interface loopback、logging host、neighbor update-source、snmp-server host、ssh、telnet</p> <p>无 ASDM 支持。</p>

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。