# 目 录

# 1 连接限制配置命令

## 1.1 连接限制配置命令

### 1.1.1 connection-limit apply policy (System view)

【命令】

**connection-limit apply policy** *policy-number*

**undo connection-limit apply policy** *policy-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

*policy-number*：指定连接限制策略编号，取值为 0。该连接限制策略必须已经存在。

【描述】

**connection-limit apply policy** 命令用来应用连接限制策略。**undo connection-limit apply policy** 命令用来取消连接限制策略的应用。

需要注意的是：

- 连接限制策略被应用后，就不能在连接限制策略视图下进行添加、删除、修改连接限制规则的操作。
- 应用的连接限制策略中必须至少存在一个连接限制规则。

相关配置可参考命令 **connection-limit policy**。

【举例】

# 应用连接限制策略 0。

```
<Sysname> system-view
[Sysname] connection-limit apply policy 0
```

### 1.1.2 connection-limit policy

【命令】

**connection-limit policy** *policy-number*

**undo connection-limit policy** *policy-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

*policy-number*：连接限制策略编号，取值为 0。

【描述】

**connection-limit policy** 命令用来创建一个连接限制策略，并进入连接限制策略视图。**undo connection-limit policy** 命令用来删除一个或全部连接限制策略。

需要注意的是：

- 一个连接限制策略由一系列的连接限制规则组成，在规则中指明了对指定用户的连接数进行限制。
- 创建一个连接限制策略需要指定策略的编号，此编号用来唯一标识此策略。
- 如果连接限制策略已经在系统视图下被应用，则不允许修改、删除策略中已经配置的连接限制规则，也不能添加新的连接限制规则。

【举例】

# 创建编号为 0 的连接限制策略，并进入连接限制策略视图。

```
<Sysname> system-view
[Sysname] connection-limit policy 0
[Sysname-connection-limit-policy-0]
```

### 1.1.3 display connection-limit policy

【命令】

**display connection-limit policy** { *policy-number* | **all** } [ **|** { **begin** | **exclude** | **include** } *regular-expression* ]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

*policy-number*：显示指定编号的连接限制策略，取值为 0。

**all**：显示所有的策略。

**|**：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

**begin**：从包含指定正则表达式的行开始显示。

**exclude**：只显示不包含指定正则表达式的行。

**include**：只显示包含指定正则表达式的行。

*regular-expression*：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

**display connection-limit policy** 命令用来显示连接限制策略的配置信息。

相关配置可参考命令 **limit**。

【举例】

# 显示所有连接限制策略的配置信息。

```
<Sysname> display connection-limit policy all
 There is 1 policy:
 Connection-limit policy 0, refcount 0 ,3 limits
  limit 1 acl 2000 per-source amount 1111 10
  limit 2 acl 2001 per-destination amount 300 20
  limit 3 acl 2002 per-service amount 400 50
```

表1-1 display connection-limit policy all 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Connection-limit policy | 连接限制策略编号 |
| refcount 0, 3 limits | 策略被引用的次数及策略中包含的规则数目 |
| limit | 策略下配置的连接限制规则，规则的具体含义请参考连接限制策略视图下的命令 **limit** |

## 1.1.4 limit

【命令】

**limit** *limit-id* { **source ip** { *ip-address mask-length* | **any** } [ **source-vpn** *src-vpn-name* ] | **destination ip** { *ip-address mask-length* | **any** } [ **destination-vpn** *dst-vpn-name* ] } * **protocol** { **dns** | **http** | **ip** | **tcp** | **udp** } **max-connections** *max-num* [ **per-destination** | **per-source** | **per-source-destination** ]

**undo limit** *limit-id*

【视图】

连接限制策略视图

【缺省级别】

2：系统级

【参数】

*limit-id*：连接限制策略的规则编号，取值范围为 0～255。

**source ip**：表示按照源 IP 地址信息来进行连接限制。

*ip-address mask-length*：指定连接的 IP 地址及掩码长度，*mask-length* 的取值范围为 1～32。

**any**：表示对指定网络的所有主机进行连接限制。例如，**source ip any** 表示所有源网络的主机。

**source-vpn** *src-vpn-name*：表示要限制连接的源 VPN 信息。其中，*src-vpn-name* 表示源 IP 地址所属的 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示连接限制的源 IP 地址位于公网中。

**destination ip**：表示按照目的 IP 地址信息来进行连接限制。

**destination-vpn** *dst-vpn-name*：表示要限制连接的目的 VPN 信息。其中，*dst-vpn-name* 表示目的 IP 地址所属的 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示连接限制的目的 IP 地址位于公网中。

**protocol**：表示对指定协议类型的连接进行连接限制。

- **dns**：表示对 DNS 协议的连接进行连接限制。
- **http**：表示对 HTTP 协议的连接进行连接限制。
- **ip**：表示对 IP 协议的连接进行连接限制。
- **tcp**：表示对 TCP 协议的连接进行连接限制。
- **udp**：表示对 UDP 协议的连接进行连接限制。

**max-connections** *max-num*：表示允许的最大连接数。其中，*max-num* 为连接数阈值。集中式设备取值范围为 1～1000000，分布式设备取值范围为 1～2000000。当设备工作在网关模式时，取值范围为 1～500000。

**per-destination**：表示按照每个目的 IP 地址的方式进行统计和限制。

**per-source**：表示按照每个源 IP 地址的方式进行统计和限制。

**per-source-destination**：表示按照每个源到目的 IP 地址对的方式进行统计和限制。

【描述】

**limit** 命令用来配置基于 IP 地址的连接限制规则。**undo limit** 命令用来删除指定的连接限制规则。

需要注意的是：

- 不能配置内容完全相同的连接限制规则。
- 删除连接限制规则中所指定的 VPN 实例时，将会使得所有与该 VPN 相关的连接限制规则不能生效。
- 连接限制规则的匹配顺序为：按照连接限制规则编号从小到大的顺序进行匹配。如果两条规则的源网段、目的网段或协议存在包含关系，则按匹配到的第一条规则进行限制。因此在配置连接限制规则时，需要从整体策略考虑，根据各规则的内容来合理安排规则的编号顺序，推荐按照限制粒度和范围由小到大的顺序来设置规则序号。

相关配置可参考命令 **connection-limit policy** 和 **display connection-limit policy**。

【举例】

# 配置编号为 1 的连接限制规则，对源 IP 地址为 1.1.1.1 的 TCP 连接数进行限制，连接数上限值为 200。

```
<Sysname> system-view
[Sysname] connection-limit policy 0
[Sysname-connection-limit-policy-0] limit 1 source ip 1.1.1.1 32 protocol tcp max-connections 200
```

# 配置编号为 2 的连接限制规则，对目的 IP 地址为 2.2.2.2 的 UDP 连接数进行限制，连接数上限值为 200。

```
[Sysname-connection-limit-policy-0] limit 2 destination ip 2.2.2.2 32 protocol udp max-connections 200
```

# 配置编号为 3 的连接限制规则，对源网段 1.1.1.0/24 中的每个用户的 IP 连接数进行限制，连接数上限值为 200。

```
[Sysname-connection-limit-policy-0] limit 3 source ip 1.1.1.0 24 protocol ip max-connections 200 per-source
```

# 配置编号为 4 的连接限制规则，对目的网段 2.2.2.0/24 中的每个用户的 IP 连接数进行限制，连接数上限值为 200。

```
[Sysname-connection-limit-policy-0] limit 4 destination ip 2.2.2.0 24 protocol ip max-connections 200 per-destination
```

# 配置编号为 5 的连接限制规则，对从 vpn1 到 vpn2 的所有 IP 连接数进行限制，连接数上限值为 200。

```
[Sysname-connection-limit-policy-0] limit 5 source ip any source-vpn vpn1 destination ip any
destination-vpn vpn2 protocol ip max-connections 200
```