H3C M9000 系列多业务安全网关

上网行为管理命令参考(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W201-20190315

前 言

本命令参考介绍了 M9000 系列产品各软件命令的命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《上网行为管理命令参考》主要介绍带宽管理和应用审计与管理命令。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 资料意见反馈

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 带宽管理 1-1

1.1 带宽管理配置命令 1-1

1.1.1 action 1-1

1.1.2 application 1-2

1.1.3 bandwidth 1-2

1.1.4 bandwidth maximum 1-4

1.1.5 connection-limit count 1-4

1.1.6 connection-limit rate 1-5

1.1.7 destination-address 1-6

1.1.8 destination-zone 1-7

1.1.9 disable 1-8

1.1.10 display traffic-policy statistics bandwidth 1-9

1.1.11 display traffic-policy statistics connection-limit maximum 1-10

1.1.12 dscp 1-14

1.1.13 profile name 1-15

1.1.14 profile rename 1-15

1.1.15 remark dscp 1-16

1.1.16 rule copy 1-17

1.1.17 rule move 1-18

1.1.18 rule name 1-19

1.1.19 rule rename 1-20

1.1.20 source-address 1-21

1.1.21 source-zone 1-21

1.1.22 time-range 1-22

1.1.23 traffic-policy 1-23

1.1.24 traffic-priority 1-23

1.1.25 user 1-24

1.1.26 user-group 1-25

1 带宽管理

1.1 带宽管理配置命令

1.1.1 action

action 命令用来配置带宽策略规则的动作。

undo action 命令用来恢复缺省情况。

【命令】

action qos profile *profile-name*

undo action

【缺省情况】

带宽策略规则中没有配置动作，即对匹配上该规则的流量不进行带宽管理，直接允许通过。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

profile-name：表示对匹配成功的流量进行限流，即对此流量应用带宽通道，进而对该流量进行带宽管理。*profile-name* 是带宽通道的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

如果流量成功匹配了某条带宽策略规则，则设备将会根据该带宽策略规则中指定的动作对此流量进行控制和管理，即按照引用的带宽通道对此流量进行限流。

配置带宽策略规则的动作时，需要注意的是：

- 子规则引用的带宽通道中的最大带宽不能大于父规则引用的带宽通道中的的最大带宽。
- 父规则引用的带宽通道中的保证带宽不能小于子规则引用的带宽通道中的保证带宽之和。
- 子规则与父规则不能引用同一个带宽通道。

【举例】

在带宽策略规则 rule1 中，配置动作为应用带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] action qos profile profile1
```

【相关命令】

- **profile name**

- **rule name**

1.1.2 application

application 命令用来指定匹配报文的应用或应用组。

undo application 命令用来取消使用指定的应用或应用组作为匹配条件。

【命令】

application { **app** *application-name* | **app-group** *application-group-name* }

undo application { **app** *application-name* | **app-group** *application-group-name* }

【缺省情况】

带宽策略规则下不存在应用或应用组作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

app *application-name*：是应用的名称，为 1～63 个字符的字符串，不区分大小写。

app-group *application-group-name*：是应用组的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

在一个带宽策略规则中可以同时指定多个应用或应用组作为匹配报文的参数或依据，配置本参数后，设备可以根据业务的应用类型来对流量进行带宽管理。例如，可以根据邮箱、P2P 下载、即时通讯和 Web 等应用对流经设备的流量实施带宽管理。

若指定传输层协议类型为 **dccp/sctp/udp-lite** 的自定义应用，带宽管理功能对这些自定义应用将不进行任何限制。有关自定义应用的详细介绍请参见“安全命令参考”中的“APR”。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的应用为 P2P_General_TCP_Communications。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] application app P2P_General_TCP_Communications
```

【相关命令】

- **app-group**（安全命令参考/APR）
- **nbar application**（安全命令参考/APR）
- **port-mapping**（安全命令参考/APR）

1.1.3 bandwidth

bandwidth 命令用来配置带宽通道的保证带宽和最大带宽。

undo bandwidth 命令用来删除带宽通道的保证带宽和最大带宽。

【命令】

bandwidth { **downstream** | **upstream** } { **guaranteed** | **maximum** } *bandwidth-value*

undo bandwidth { **downstream** | **upstream** } { **guaranteed** | **maximum** }

【缺省情况】

未配置带宽通道的保证带宽和最大带宽。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

downstream：表示对下行流量进行控制，即对 Server 访问 Client 的流量进行控制。

upstream：表示对上行流量进行控制，即对 Client 访问 Server 的流量进行控制。

guaranteed：表示设置保证带宽。

maximum：表示设置最大带宽，最大带宽不小于保证带宽。

bandwidth-value：表示带宽值，取值范围为 8～100000000，单位为 kbps。

【使用指导】

为父子规则配置带宽通道时，应遵循如下原则：

- 子规则引用的带宽通道中的的最大带宽不能大于父规则引用的带宽通道中的的最大带宽。
- 父规则引用的带宽通道中的保证带宽不能小于子规则引用的带宽通道中的保证带宽之和。
- 子规则与父规则不能引用同一个带宽通道。

接口期望带宽的缺省值较小时，在流量较大的情况下，很容易出现丢包现象，这时可以将此接口的期望带宽值调大。比如 Tunnel 口的默认带宽是 64kbps，流量比较大的情况下，易出现丢包现象，这时可将 Tunnel 接口的期望带宽值调大。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
```

配置带宽通道的上行流量的最大带宽为 10000kbps、下行流量的最大带宽为 10000kbps、上行流量的保证带宽为 5000kbps、下行流量的保证带宽为 5000kbps。

```
[Sysname-traffic-policy-profile-profile1] bandwidth upstream maximum 10000
[Sysname-traffic-policy-profile-profile1] bandwidth downstream maximum 10000
[Sysname-traffic-policy-profile-profile1] bandwidth upstream guaranteed 5000
[Sysname-traffic-policy-profile-profile1] bandwidth downstream guaranteed 5000
```

【相关命令】

- **profile name**

1.1.4 bandwidth maximum

bandwidth maximum { **per-ip** | **per-user** }命令用来配置每 IP 或每用户的最大带宽。

undo bandwidth maximum { **per-ip** | **per-user** }命令用来删除指定的最大带宽。

【命令】

bandwidth { **downstream** | **upstream** } **maximum** { **per-ip** | **per-user** } *bandwidth-value*

undo bandwidth { **downstream** | **upstream** } **maximum** { **per-ip** | **per-user** }

【缺省情况】

未配置每 IP 或每用户的最大带宽。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

downstream：表示对下行流量进行控制，即对 Server 访问 Client 的流量进行控制。

upstream：表示对上行流量进行控制，即对 Client 访问 Server 的流量进行控制。

maximum：表示设置最大带宽。

per-ip：指定每 IP 的最大带宽。

per-user：指定每用户的最大带宽。

bandwidth-value：表示带宽值，取值范围为 8～100000000，单位为 kbps。

【使用指导】

此命令可以用来对带宽通道中的每 IP 或每用户进行最大带宽限制，实现更加精细化的带宽管理。

配置的每 IP 或每用户的最大带宽不能大于带宽通道整体的最大带宽。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
```

配置每个 IP 的上行/下行最大流量带宽。

```
[Sysname-traffic-policy-profile-profile1] bandwidth upstream maximum per-ip 10000
[Sysname-traffic-policy-profile-profile1] bandwidth downstream maximum per-ip 10000
```

【相关命令】

- **profile name**

1.1.5 connection-limit count

connection-limit count 命令用来配置最大连接数。

undo connection-limit count 命令用来删除指定的最大连接数。

【命令】

connection-limit count { **per-rule** | **per-ip** | **per-user** } *connection-number*

undo connection-limit count { **per-rule** | **per-ip** | **per-user** }

【缺省情况】

未配置最大连接数。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

per-rule *connection-number*：指定带宽策略规则的最大连接数。

per-ip：指定每 IP 的最大连接数。

per-user：指定每用户的最大连接数。

connection-number：表示最大连接数，取值范围为 1～12000000。

【使用指导】

带宽通道中即可以配置整体的最大连接数限制，也可以配置基于每 IP 或每用户的最大连接数限制。每 IP 或每用户的最大连接数不能大于带宽通道整体的最大连接数。

在同一个带宽通道视图下对于 **per-ip** 和 **per-user** 不可以同时存在，但是 **per-rule** 可以与 **per-ip** 或 **per-user** 同时存在。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
```

配置带宽策略规则的最大连接数为 1000。

```
[Sysname-traffic-policy-profile-profile1] connection-limit count per-rule 1000
```

配置每 IP 的最大连接数为 500。

```
[Sysname-traffic-policy-profile-profile1] connection-limit count per-ip 500
```

【相关命令】

- **profile name**

1.1.6 connection-limit rate

connection-limit rate 命令用来配置最大新建连接速率。

undo connection-limit rate 命令用来删除指定的最大新建连接速率。

【命令】

connection-limit rate { **per-rule** | **per-ip** | **per-user** } *connection-rate*

undo connection-limit rate { **per-rule** | **per-ip** | **per-user** }

【缺省情况】

未配置最大新建连接速率限制。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

per-rule *connection-rate*：指定带宽策略规则的最大新建连接速率。

per-ip：指定每 IP 的最大新建连接速率。

per-user：指定每用户的最大新建连接速率。

connection-rate：表示最大新建连接速率，取值范围为 1～12000000，单位为每秒连接数。

【使用指导】

带宽通道中即可以配置整体的最大新建连接速率，也可以配置基于每 IP 或每用户的最大新建连接速率。

每 IP 或每用户的最大新建连接速率不能大于带宽通道整体的最大新建连接速率。

在同一个带宽通道视图下对于 **per-ip** 和 **per-user** 不可以同时存在，但是 **per-rule** 可以与 **per-ip** 或 **per-user** 同时存在。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
```

配置带宽策略规则的最大新建连接速率为 1000。

```
[Sysname-traffic-policy-profile-profile1] connection-limit rate per-rule 1000
```

配置每用户的最大新建连接速率为 500。

```
[Sysname-traffic-policy-profile-profile1] connection-limit rate per-user 500
```

【相关命令】

- **profile name**

1.1.7 destination-address

destination-address 命令用来指定匹配报文的目的 IP 地址。

undo destination-address 命令用来取消使用指定的目的 IP 地址作为匹配条件。

【命令】

destination-address address-set *object-group-name*

undo destination-address address-set *object-group-name*

【缺省情况】

带宽策略规则下不存在目的 IP 地址作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name：IPv4/IPv6 地址对象组的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

可以引用多个 IPv4 或 IPv6 地址对象组中指定的 IP 地址或网段来作为匹配报文目的 IP 地址的参数或依据。

在进行配置回滚前，请检查带宽策略规则引用的地址对象组的配置。若与回滚配置中的地址对象组名称相同但类型不同，将导致该配置回滚失败。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的目的 IP 地址为 IPv4 地址对象组 obgroup2 中指定的 IP 地址。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] destination-address address-set obgroup2
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.8 destination-zone

destination-zone 命令用来指定匹配报文的目的安全域。

undo destination-zone 命令用来取消使用指定的目的安全域作为匹配条件。

【命令】

destination-zone *destination-zone-name*

undo destination-zone *destination-zone-name*

【缺省情况】

带宽策略规则下不存在目的安全域作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

destination-zone-name：表示安全域的名称，为 1～31 个字符的字符串，不区分大小写，不能包含字符“-”。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的目的安全域为 zone2。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] destination-zone zone2
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.9 disable

disable 命令用来关闭带宽策略规则。

undo disable 命令用来恢复缺省情况。

【命令】

disable

undo disable

【缺省情况】

带宽策略规则处于开启状态。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果在某些组网环境中某条带宽策略规则暂时不会被用到，则可以使用此命令来关闭此条带宽策略规则。关闭带宽策略规则后，此规则不参与对流量的匹配，但依然可以对其进行复制、重命名和移动。

【举例】

关闭带宽策略规则 rule1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] disable
```

【相关命令】

- **rule name**

1.1.10 display traffic-policy statistics bandwidth

display traffic-policy statistics bandwidth 命令用来显示带宽策略规则下流量速率的统计信息。

【命令】

分布式设备－独立运行模式：

display traffic-policy statistics bandwidth { **all | rule** *rule-name* } [**slot** *slot-number* [**cpu** *cpu-number*]]

分布式设备－IRF 模式：

display traffic-policy statistics bandwidth { **all | rule** *rule-name* } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

all：表示显示所有带宽策略规则下流量速率的统计信息。

rule *rule-name*：表示显示指定带宽策略规则下流量速率的统计信息。*rule-name* 表示带宽策略规则名称，为 1～63 个字符的字符串，不区分大小写。

slot *slot-number*：显示指定单板上带宽策略规则下流量速率的统计信息。*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示所有单板上带宽策略规则下流量速率的统计信息。（分布式设备－独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上带宽策略规则下流量速率的统计信息。*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示所有单板上带宽策略规则下流量速率的统计信息。

cpu *cpu-number*：显示指定 CPU 上宽策略规则的流量统计信息。*cpu-number* 表示 CPU 编号，只有指定的 **slot** 支持多 CPU 时，才能配置该参数。（分布式设备－IRF 模式）

【举例】

显示所有带宽策略规则下流量速率的统计信息。（分布式设备－独立运行模式）

```
<Sysname> display traffic-policy statistics bandwidth all
CPU 1 on slot 2:
AVC bandwidth statistic:
-------------------------------------------------------------------------------
--
 Rule                State    Profile
-------------------------------------------------------------------------------
--
 rule1               Enable   abc
```

```
now bandwidth of rule rule1 is 0.0 B/s
 ------------------------------------------------------------------------------
--
 rule2                Enable   profile1
now bandwidth of rule rule2 is 0.0 B/s
------------------------------------------------------------------------------
--
------------------------------------------------------------------------------
--
```

显示所有带宽策略规则下流量速率的统计信息。（分布式设备—IRF 模式）

```
<Sysname> display traffic-policy statistics bandwidth all
CPU 1 on slot 2 in chassis 1:
AVC bandwidth statistic:
------------------------------------------------------------------------------
--
 Rule                 State    Profile
------------------------------------------------------------------------------
--
 rule1                Enable   abc
now bandwidth of rule rule1 is 0.0 B/s
------------------------------------------------------------------------------
--
 rule2                Enable   profile1
now bandwidth of rule rule2 is 0.0 B/s
------------------------------------------------------------------------------
--
------------------------------------------------------------------------------
--
```

表1-1 display traffic-policy statistics bandwidth rule 命令显示信息描述表

字段	描述
Rule	带宽策略规则的名称
State	带宽策略规则的状态，取值包括： • Enable：表示此规则已启用 • Disable：表示此规则已禁用
Profile	带宽策略规则中引用的带宽通道
now bandwidth of rule *xxx xxx* is *xxx* B/s	当前每带宽策略规则的实时带宽，单位为字节每秒

1.1.11 display traffic-policy statistics connection-limit maximum

display traffic-policy statistics connection-limit maximum 命令用来显示最大连接数限制的统计信息。

【命令】

分布式设备－独立运行模式：

display traffic-policy statistics connection-limit maximum { { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } | **per-user** [**user** *user-name*] } **rule** *rule-name* } | **per-rule** { *rule-name* | **all** } } [**slot** *slot-number* [**cpu** *cpu-number*]]

分布式设备－IRF 模式：

display traffic-policy statistics connection-limit maximum { { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } | **per-user** [**user** *user-name*] } **rule** *rule-name* } | **per-rule** { *rule-name* | **all** } } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

per-ip：显示指定带宽策略规则中每 IP 的最大连接数统计信息。

ipv4：显示指定带宽策略规则中 IPv4 类型的每 IP 的最大连接数统计信息。

ipv4-address：显示指定 IP 的最大连接数统计信息，若不指定本参数，则显示指定带宽策略规则中所有 IPv4 类型的每 IP 的最大连接数统计信息。

ipv6：显示指定带宽策略规则中 IPv6 类型的每 IP 的最大连接数统计信息。

ipv6-address：显示指定 IP 的最大连接数统计信息，若不指定本参数，则显示指定带宽策略规则中所有 IPv6 类型的每 IP 的最大连接数统计信息。

per-user：显示指定带宽策略规则中每用户的最大连接数统计信息。

user *user-name*：显示指定用户的最大连接数统计信息。*user-name* 为用户的名称，取值范围为 1～55 个字符的字符串，不区分大小写。若不指定本参数，则显示指定带宽策略规则中所有用户的最大连接数统计信息。

rule *rule-name*：显示指定带宽策略规则中符合条件的最大连接数统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写。

per-rule：显示带宽策略规则的最大连接数统计信息。

all：显示所有带宽策略规则的最大连接数统计信息。

rule-name：显示指定带宽策略规则的最大连接数统计信息，带宽策略规则的名称为 1～63 个字符的字符串，不区分大小写。

slot *slot-number*：显示指定单板上的最大连接数限制的统计信息。*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示所有单板上的最大连接数限制的统计信息。（分布式设备－独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的最大连接数限制的统计信息。*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示所有单板上的最大连接数限制的统计信息。（分布式设备－IRF 模式）

cpu *cpu-number*：显示指定 CPU 的最大连接数限制的统计信息。*cpu-number* 表示 CPU 编号，只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

【举例】

#显示带宽策略中所有规则的最大连接数统计信息。（分布式设备－独立运行模式）

```
<Sysname> display traffic-policy statistics connection-limit maximum per-rule all
CPU 1 on slot 2:
Connection-limit for maximum statistic:
Codes: CC(Current Connection), RC(Rejective Connection), CL(Current Limit)
------------------------------------------------------------------------------
--
 Policy              State    Profile             CC         RC         CL

------------------------------------------------------------------------------
--
 rule1               Enable   abc                 0          0          0

------------------------------------------------------------------------------
--
------------------------------------------------------------------------------
--
```

#显示带宽策略规则 rule1 中所有用户的最大连接数统计信息。（分布式设备－独立运行模式）

```
<Sysname> display traffic-policy statistics connection-limit maximum per-user rule rule1
CPU 1 on slot 2:
Connection-limit for maximum statistic:
Codes: CC(Current Connection), RC(Rejective Connection)
------------------------------------------------------------------------------
--
 Policy           State    Profile          User               CC         RC

------------------------------------------------------------------------------
--
 rule1            Enable   profile1         user1              1          0
------------------------------------------------------------------------------
--
```

显示带宽策略规则 rule1 中所有 IPv4 类型的每 IP 的最大连接数统计信息。（分布式设备－独立运行模式）

```
<Sysname> display traffic-policy statistics connection-limit maximum per-ip ipv4 rule rule1
CPU 1 on slot 2:
Connection-limit for maximum statistic:
Codes: CC(Current Connection), RC(Rejective Connection)
------------------------------------------------------------------------------
--
 Policy           State    Profile          IP                 CC         RC
```

```
------------------------------------------------------------------------------
--
 rule1            Enable   profile1         111.8.92.43      1          0
------------------------------------------------------------------------------
--
```

#显示带宽策略中所有规则的最大连接数统计信息。（分布式设备－IRF 模式）

```
<Sysname> display traffic-policy statistics connection-limit maximum per-rule all
CPU 1 on slot 2 in chassis 1:
Connection-limit for maximum statistic:
Codes: CC(Current Connection), RC(Rejective Connection), CL(Current Limit)
------------------------------------------------------------------------------
--
 Policy              State    Profile             CC         RC         CL

------------------------------------------------------------------------------
--
 rule1               Enable   abc                 0          0          0

------------------------------------------------------------------------------
--
------------------------------------------------------------------------------
--
```

#显示带宽策略规则 rule1 中所有用户的最大连接数统计信息。（分布式设备－IRF 模式）

```
<Sysname> display traffic-policy statistics connection-limit maximum per-user rule rule1
CPU 1 on slot 2 in chassis 1:
Connection-limit for maximum statistic:
Codes: CC(Current Connection), RC(Rejective Connection)
------------------------------------------------------------------------------
--
 Policy           State    Profile          User               CC         RC

------------------------------------------------------------------------------
--
 rule1            Enable   profile1         user1              1          0
------------------------------------------------------------------------------
--
```

显示带宽策略规则 rule1 中所有 IPv4 类型的每 IP 的最大连接数统计信息。（分布式设备－IRF 模式）

```
<Sysname> display traffic-policy statistics connection-limit maximum per-ip ipv4 rule rule1
CPU 1 on slot 2 in chassis 1:
Connection-limit for maximum statistic:
Codes: CC(Current Connection), RC(Rejective Connection)
------------------------------------------------------------------------------
--
 Policy           State    Profile          IP               CC         RC
```

```
-------------------------------------------------------------------------------
--
 rule1            Enable   profile1         111.8.92.43      1          0
-------------------------------------------------------------------------------
--
```

表1-2 display traffic-policy statistics connection-limit maximum 命令显示信息描述表

字段	描述
Policy	带宽策略规则的名称
State	带宽策略规则的状态，取值包括： • Enable：表示此规则已启用 • Disable：表示此规则已禁用
Profile	带宽策略规则中引用的带宽通道
User	用户的名称
IP	IP地址
Codes	代码缩写的表示，取值包括： • CC (current connections)：当前连接数 • RC (rejected connections)：拒绝的连接数 • CL (connection limit)：配置的连接数限制

1.1.12 dscp

dscp 命令用来指定匹配报文的 DSCP 优先级。

undo dscp 命令用来取消使用指定的 DSCP 优先级作为匹配条件。

【命令】

dscp *dscp-value*

undo dscp

【缺省情况】

带宽策略规则下不存在 DSCP 优先级作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value：表示报文DSCP优先级，取值仅可以是关键字，关键字如 表 1-3 所示。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的 DSCP 优先级为 af11。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] dscp af11
```

1.1.13 profile name

profile name 命令用来创建带宽通道，并进入带宽通道视图。如果指定的带宽通道已经存在，则直接进入带宽通道视图。

undo profile name 命令用来删除指定的带宽通道。

【命令】

profile name *profile-name*

undo profile name *profile-name*

【缺省情况】

不存在带宽通道。

【视图】

带宽策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

profile-name：带宽通道的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

带宽通道定义了实施带宽管理的对象所能够使用的带宽资源，带宽通道将被带宽策略规则引用。

【举例】

创建一个名为 profile1 的带宽通道，并进入该带宽通道视图。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1]
```

【相关命令】

- **action**

1.1.14 profile rename

profile rename 命令用来重命名带宽通道

【命令】

profile rename *old-name new-name*

【视图】

带宽策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-name：表示带宽通道原来的名称，为 1～63 个字符的字符串，不区分大小写。

new-name：表示带宽通道新的名称，为 1～63 个字符的字符串，不区分大小写。新的名称不能为设备中已存在的带宽通道名称。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] quit
```

把带宽通道 profile1 重命名为 profile2。

```
[Sysname-traffic-policy] profile rename profile1 profile2
```

1.1.15 remark dscp

remark dscp 命令用来重标记报文的 DSCP 优先级。

undo remark dscp 命令用来恢复缺省情况。

【命令】

remark dscp *dscp-value*

undo remark dscp

【缺省情况】

不修改报文的 DSCP 优先级。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value：表示报文DSCP优先级，取值仅可以是关键字，关键字如 表 1-3 所示。

表1-3 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
default	000000	0
af11	001010	10

关键字	DSCP 值（二进制）	DSCP 值（十进制）
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

【使用指导】

优先级重标记是指修改报文中 DSCP（Differentiated Services Code Point）字段的值。DSCP 字段也称为 DSCP 优先级，是网络设备进行流量分类的依据。位于报文传输路径上的各个网络设备，可以通过 DSCP 优先级来区分流量，进而对不同 DSCP 优先级的流量采取差异化的处理。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
```

重标记报文的 DSCP 优先级为 af22

```
[Sysname-traffic-policy-profile-profile1] remark dscp af22
```

【相关命令】

- **profile name**

1.1.16 rule copy

rule copy 命令用来复制带宽策略规则。

【命令】

rule copy *rule-name new-rule-name*

【视图】

带宽策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-name：表示被复制带宽策略规则的名称，为 1～63 个字符的字符串，不区分大小写。

new-rule-name：表示新建带宽策略规则的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

当新建的带宽策略规则和已存在的带宽策略规则比较相似时，可通过复制已经存在的带宽策略规则来创建新的带宽策略规则。

复制带宽策略规则时，需要注意的是：

- 如果被复制的带宽策略规则中含有子带宽策略规则，则只会复制父带宽策略规则的内容。
- 通过复制创建的新策略规则紧跟在被复制的带宽策略规则之后。

【举例】

通过复制带宽策略规则 rule1，创建一个新的带宽策略规则 rule2。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule copy rule1 rule2
```

1.1.17 rule move

rule move 命令用来移动带宽策略规则的排列顺序。

【命令】

rule move *rule-name1* { **after** | **before** } *rule-name2*

【视图】

带宽策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-name1：表示需要被移动的带宽策略规则的名称，为 1～63 个字符的字符串，不区分大小写。

after：表示把带宽策略规则 *rule-name1* 移动到带宽策略规则 *rule-name2* 的后面。

before：表示把带宽策略规则 *rule-name1* 移动到带宽策略规则 *rule-name2* 的前面。

rule-name2：表示移动目标的带宽策略规则的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

设备根据带宽策略规则在设备上显示的顺序从上到下对流量进行匹配，一旦匹配上某个带宽策略规则便结束此匹配过程，并根据该规则中指定的动作对此流量进行处理；如果流量没有匹配上任何规则，则允许该流量通过。为了使设备上部署的带宽管理功能达到更好、更严谨的效果，因此配置带宽策略规则时要遵循“先精细后宽泛”的原则。如果发现设备中已配置的带宽策略规则之间的顺序不符合这个原则，则可以使用 **rule move** 命令来调整带宽策略规则之间的顺序。

只有不同父带宽策略规则和相同父带宽策略规则下的子带宽策略规则之间才可以相互调整顺序。

【举例】

创建带宽策略规则 rule1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] quit
```

创建带宽策略规则 rule2。

```
[Sysname-traffic-policy] rule name rule2
[Sysname-traffic-policy-rule-rule2] quit
```

将带宽策略规则 rule1 的配置顺序移动到带宽策略规则 rule2 之后。

```
[Sysname-traffic-policy] rule move rule1 after rule2
```

1.1.18 rule name

rule name 命令用来创建带宽策略规则，并进入带宽策略规则视图。如果指定的带宽策略规则已经存在，则直接进入带宽策略规则视图。

undo rule name 命令用来删除指定的带宽策略规则。

【命令】

rule name *rule-name* [**parent** *parent-rule-name*]

undo rule name *rule-name*

【缺省情况】

不存在带宽策略规则。

【视图】

带宽策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-name：表示带宽策略规则的名称，为 1～63 个字符的字符串，不区分大小写。

parent *parent-rule-name*：指定带宽策略规则的父规则。*parent-rule-name* 表示父规则的名称，为 1～63 个字符的字符串，不区分大小写。指定的父规则必须已经存在，否则创建该带宽策略规则时失败。

【使用指导】

带宽策略中可以配置多个带宽策略规则，这些规则用于定义匹配流量的匹配项以及流量控制的动作。不同规则之间的匹配顺序为：设备根据这些规则在设备上显示的顺序从上到下对流量进行匹配，一旦流量匹配上某条规则便结束此匹配过程，并根据该规则中指定的动作对此流量进行处理；如果流量没有匹配上任何规则，则允许该流量通过。

当创建带宽策略规则时，如果需要继承其他带宽策略规则中的匹配项属性，则可以在创建带宽策略规则时为其指定父带宽策略规则。

创建带宽策略规则时，需要注意的是：

- 如果指定的父带宽策略规则已是其他带宽策略规则的子带宽策略规则，则创建该带宽策略规则失败。
- 只能在创建带宽策略规则时指定带宽策略规则的父带宽策略规则，不能为已存在的带宽策略规则添加或修改父带宽策略规则。

【举例】

创建一个名称为 rule1 的带宽策略规则，并进入该带宽策略规则视图。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1]
```

1.1.19 rule rename

rule rename 命令用来重命名带宽策略规则。

【命令】

rule rename *old-rule-name new-rule-name*

【视图】

带宽策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-rule-name：表示带宽策略规则的原有名称，为 1～63 个字符的字符串，不区分大小写。

new-rule-name：表示带宽策略规则的新名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

创建带宽策略规则 rule1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] quit
```

把带宽策略规则 rule1 重命名为 rule2。

```
[Sysname-traffic-policy] rule rename rule1 rule2
```

1.1.20 source-address

source-address 命令用来指定匹配报文的源 IP 地址。

undo source-address 命令用来取消使用指定的源 IP 地址作为匹配条件。

【命令】

source-address address-set *object-group-name*

undo source-address address-set *object-group-name*

【缺省情况】

带宽策略规则下不存在源 IP 地址作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name：表示 IPv4/IPv6 地址对象组的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

可以引用多个 IPv4 或 IPv6 地址对象组中指定的 IP 地址来作为匹配报文源 IP 地址的参数或依据。在进行配置回滚前，请检查带宽策略规则引用的地址对象组的配置。若与回滚配置中的地址对象组名称相同但类型不同，将导致该配置回滚失败。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的源 IP 地址为 IPv4 地址对象组 obgroup1 中指定的 IP 地址。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] source-address address-set obgroup1
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.21 source-zone

source-zone 命令用来指定匹配报文的源安全域。

undo source-zone 命令用来取消使用指定的源安全域作为匹配条件。

【命令】

source-zone *source-zone-name*

undo source-zone *source-zone-name*

【缺省情况】

带宽策略规则下不存在源安全域作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

source-zone-name：表示安全域的名称，为 1～31 个字符的字符串，不区分大小写，不能包含字符“-”。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的源安全域为 zone1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] source-zone zone1
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.22 time-range

time-range 命令用来指定带宽策略规则的生效时间。

undo time-range 命令用来恢复缺省情况。

【命令】

time-range *time-range-name*

undo time-range

【缺省情况】

带宽策略规则在任何时间下都生效。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

time-range-name：指定时间段的名称，为 1～32 个字符的字符串，不区分大小写。

【举例】

在带宽策略规则 rule1 中，指定带宽策略规则的生效时间为时间段 work-time 中配置的时间。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] time-range work-time
```

【相关命令】

- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.23 traffic-policy

traffic-policy 命令用来进入带宽策略视图。

【命令】

traffic-policy

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

带宽策略视图下可以完成对带宽策略规则的创建、复制、移动和重命名等操作。

【举例】

进入带宽策略视图。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy]
```

1.1.24 traffic-priority

traffic-priority 命令用来配置流量优先级。

undo traffic-priority 命令用来恢复缺省情况。

【命令】

traffic-priority *priority-value*

undo traffic-priority

【缺省情况】

流量优先级为 1。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

priority-value：表示流量优的先级，取值范围为 1～7，数值越大优先级越高。

【使用指导】

当多个带宽通道中的流量同时从某个接口发送时，如果此接口发生阻塞，则优先级高的流量优先被发送。优先级相同的流量将会自由竞争出接口的带宽资源。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
```

配置流量优先级为 7。

```
[Sysname-traffic-policy-profile-profile1] traffic-priority 7
```

【相关命令】

- **profile name**

1.1.25 user

user 命令用来指定匹配报文的用户名。

undo user 命令用来取消使用指定的用户名作为匹配条件。

【命令】

user *user-name* [**domain** *domain-name*]

undo user *user-name* [**domain** *domain-name*]

【缺省情况】

带宽策略规则下不存在用户名作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name：指定用户的名称，为 1～55 个字符的字符串，不区分大小写。

domain *domain-name*：表示在指定的身份识别域中匹配此用户。*domain-name* 是身份识别域的名称，为 1～255 个字符的字符串，不区分大小写，不能包括字符“?”。若不指定此参数，则表示在不属于任何身份识别域的用户中匹配此用户。有关身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【使用指导】

本命令可以实现基于用户的精细化带宽管理。此功能可以有效解决在移动互联网中，用户 IP 地址不断变化带来的带宽管理不方便的问题，即以不变的用户名应对变化的 IP 地址，将流量的源 IP 地址识别为用户。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的用户名为 managers。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] user managers
```

引用用户名为 user1，身份识别域为 dpi 的用户作为带宽策略规则的匹配条件。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name myrule
[Sysname-traffic-policy-rule-myrule] user user1 domain dpi
```

【相关命令】

- **local-user**（安全命令参考/AAA）
- **user-identity enable**（安全命令参考/用户身份识别与管理）
- **user-identity static-user**（安全命令参考/用户身份识别与管理）

1.1.26 user-group

user-group 命令用来指定匹配报文的用户组。

undo user-group 命令用来取消使用指定的用户组作为匹配条件。

【命令】

user-group *user-group-name* [**domain** *domain-name*]

undo user-group *user-group-name* [**domain** *domain-name*]

【缺省情况】

带宽策略规则下不存在用户组作为匹配条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-group-name：指定用户组的名称，为 1～32 个字符的字符串，不区分大小写。

domain *domain-name*：表示在指定的身份识别域中匹配此用户组。*domain-name* 是身份识别域的名称，为 1～255 个字符的字符串，不区分大小写，不能包括字符“?”。若不指定此参数，则表示在不属于任何身份识别域的用户组中匹配此用户组。有关身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【使用指导】

本命令可以实现基于用户组的精细化带宽管理。此功能可以有效解决在移动互联网中，用户 IP 地址不断变化带来的带宽管理不方便的问题，即以不变的用户组应对变化的 IP 地址，将流量的源 IP 地址识别为用户组。

【举例】

在带宽策略规则 rule1 中，指定匹配报文的用户组为 mak。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] user-group mak
```

引用用户组名为 usergroup1，域为 dpi 的用户组作为带宽策略规则的匹配条件。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name myrule
[Sysname-traffic-policy-rule-myrule] user-group usergroup1 domain dpi
```

【相关命令】

- **user-group**（安全命令参考/AAA）
- **user-identity enable**（安全命令参考/用户身份识别与管理）

目 录

1 应用审计与管理 1-1
1.1 应用审计与管理配置命令 1-1
1.1.1 application 1-1
1.1.2 description 1-2
1.1.3 destination-address 1-2
1.1.4 destination-zone 1-3
1.1.5 disable 1-4
1.1.6 keyword 1-5
1.1.7 keyword-group name 1-5
1.1.8 policy copy 1-6
1.1.9 policy default-action 1-6
1.1.10 policy move 1-7
1.1.11 policy name 1-8
1.1.12 policy rename 1-9
1.1.13 rule 1-9
1.1.14 rule default-action 1-11
1.1.15 rule match-method 1-12
1.1.16 service 1-13
1.1.17 source-address 1-13
1.1.18 source-zone 1-14
1.1.19 time-range 1-15
1.1.20 uapp-control 1-15
1.1.21 user 1-16
1.1.22 user-group 1-17

1 应用审计与管理

说明

本特性会解析出用户报文中的敏感信息和私密信息，请保证将本特性仅用于合法用途。

1.1 应用审计与管理配置命令

1.1.1 application

application 命令用来配置作为应用审计与管理策略过滤条件的应用和应用组。

undo application 命令用来删除作为应用审计与管理策略过滤条件的应用和应用组。

【命令】

application { **app** *application-name* | **app-group** *application-group-name* }

undo application { **app** *application-name* | **app-group** *application-group-name* }

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

app *application-name*：表示应用的名称，为 1～63 个字符的字符串，不区分大小写。

app-group *application-group-name*：表示应用组的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

仅在免审计和阻断类型的策略中可配置此命令。

多次执行本命令，可配置多个应用和应用组作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理阻断策略 mypolicy2 过滤条件的应用为 app1 和 app2，应用组为 group1 和 group2。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy2 deny
[Sysname-uapp-control-policy-mypolicy2] application app app1
```

```
[Sysname-uapp-control-policy-mypolicy2] application app app2
[Sysname-uapp-control-policy-mypolicy2] application app-group group1
[Sysname-uapp-control-policy-mypolicy2] application app-group group2
```

【相关命令】

- **app-group**（安全命令参考/APR）
- **nbar application**（安全命令参考/APR）
- **port-mapping**（安全命令参考/APR）

1.1.2 description

description 命令用来配置关键字组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

不存在关键字组的描述信息。

【视图】

关键字组视图

【缺省用户角色】

network-admin

context-admin

【参数】

text：表示关键字组的描述信息，为 1～255 个字符的字符串，区分大小写。

【举例】

配置关键字组的描述信息为 account limit。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] keyword-group name mykeywordgroup
[Sysname-uapp-control-keyword-group-mykeywordgroup] description account limit
```

1.1.3 destination-address

destination-address 命令用来配置作为应用审计与管理策略过滤条件的目的 IP 地址。

undo destination-address 命令用来删除作为应用审计与管理策略过滤条件的目的 IP 地址。

【命令】

destination-address { **ipv4** | **ipv6** } *object-group-name*

undo destination-address { **ipv4** | **ipv6** } *object-group-name*

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4：表示指定 IPv4 地址对象组。

ipv6：表示指定 IPv6 地址对象组。

object-group-name：表示地址对象组的名称，为 1～31 个字符的字符串，不区分大小写，且必须已存在。

【使用指导】

多次执行本命令，可配置多个目的 IPv4/IPv6 地址对象组作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的目的 IPv4 地址。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] destination-address ipv4 obgroup3
[Sysname-uapp-control-policy-mypolicy1] destination-address ipv4 obgroup4
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.4 destination-zone

destination-zone 命令用来配置作为应用审计与管理策略过滤条件的目的安全域。

undo destination-zone 命令用来删除作为应用审计与管理策略过滤条件的目的安全域。

【命令】

destination-zone *destination-zone-name*

undo destination-zone *destination-zone-name*

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

destination-zone-name：表示安全域的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

多次执行本命令，可配置多个目的安全域作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的目的安全域为 zone3 和 zone4。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] destination-zone zone3
[Sysname-uapp-control-policy-mypolicy1] destination-zone zone4
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.5 disable

disable 命令用来关闭应用审计与管理策略。

undo disable 命令用来开启应用审计与管理策略。

【命令】

disable

undo disable

【缺省情况】

应用审计与管理策略处于开启状态。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果在某些组网环境中某条应用审计与管理策略暂时不会被用到，则可以使用此命令来关闭此条应用审计与管理策略。关闭应用审计与管理策略后，此策略将不能对流量进行匹配，但依然可以对其进行复制、重命名和移动的操作。

【举例】

关闭应用审计与管理策略 mypolicy1。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1
[Sysname-uapp-control-policy-mypolicy1] disable
```

1.1.6 keyword

keyword 命令用来配置关键字。

undo keyword 命令用来删除指定的关键字。

【命令】

keyword *keyword-value*

undo keyword *keyword-value*

【缺省情况】

不存在关键字。

【视图】

关键字组视图

【缺省用户角色】

network-admin

context-admin

【参数】

keyword-value：表示关键字，为 1～63 个字符的字符串，区分大小写。

【举例】

配置应用审计与管理的关键字为 keywordname。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] keyword-group name mykeywordgroup
[Sysname-uapp-control-keyword-group-mykeywordgroup] keyword keywordname
```

1.1.7 keyword-group name

keyword-group name 命令用来创建关键字组，并进入关键字组视图。如果指定的关键字组已经存在，则直接进入关键字组视图。

undo keyword-group name 命令用来删除指定的关键字组。

【命令】

keyword-group name *keyword-group-name*

undo keyword-group name *keyword-group-name*

【缺省情况】

不存在关键字组。

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

keyword-group-name：表示关键字组的名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

创建名称为 mykeywordgroup 的关键字组，并进入关键字组视图。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] keyword-group name mykeywordgroup
[Sysname-uapp-control-keyword-group-mykeywordgroup]
```

1.1.8 policy copy

policy copy 命令用来复制应用审计与管理策略。

【命令】

policy copy *policy-name new-policy-name*

【缺省情况】

不存在应用审计与管理策略。

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示被复制应用审计与管理策略的名称，为 1～63 个字符的字符串，不区分大小写。

new-policy-name：表示新建应用审计与管理策略的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

当需要新建的应用审计与管理策略和已存在的策略比较相似时，可通过复制已经存在的策略来快速的创建新的应用审计与管理策略。

【举例】

复制应用审计与管理策略 policy1，复制后的策略名称为 policy2。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy copy policy1 policy2
```

1.1.9 policy default-action

policy default-action 命令用来配置应用审计与管理策略的缺省动作。

【命令】

policy default-action { **deny** | **permit** }

【缺省情况】

应用审计与管理策略的缺省动作是允许。

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

deny：表示阻断报文。

permit：表示允许报文通过。

【使用指导】

若报文未与任何一个应用审计与管理策略匹配成功，则设备将根据应用审计与管理策略的缺省动作对报文进行处理。

【举例】

配置应用审计与管理策略的缺省动作为丢弃。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy default-action deny
```

1.1.10 policy move

policy move 命令用来移动应用审计与管理策略的位置。

【命令】

policy move *policy-name1* { **after** | **before** } *policy-name2*

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name1：表示需要被移动的应用审计与管理策略的名称，为 1～63 个字符的字符串，不区分大小写。

after：表示把应用审计与管理策略 *policy-name1* 移动到应用审计与管理策略 *policy-name2* 的后面。

before：表示把应用审计与管理策略 *policy-name1* 移动到应用审计与管理策略 *policy-name2* 的前面。

policy-name2：表示移动目标的应用审计与管理策略的名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

创建应用审计与管理策略，名称为 policy1。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name policy1 audit
[Sysname-uapp-control-policy-policy1] quit
```

创建应用审计与管理策略，名称为 policy2。

```
[Sysname-uapp-control] policy name policy2 audit
[Sysname-uapp-control-policy-policy2] quit
```

移动应用审计与管理策略 policy1 到 policy2 之后

```
[Sysname-uapp-control] policy move policy1 after policy2
```

1.1.11 policy name

policy name 命令用来创建应用审计与管理策略，并进入应用审计与管理策略视图。如果指定的应用审计与管理策略已经存在，则直接进入应用审计与管理策略视图。

undo policy name 命令用来删除指定的应用审计与管理策略。

【命令】

policy name *policy-name* [**audit** | **deny** | **noaudit**]

undo policy name *policy-name*

【缺省情况】

不存在应用审计与管理策略。

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示应用审计与管理策略的名称，为 1～63 个字符的字符串，不区分大小写，且名称必须全局唯一。

audit：表示审计类型的策略。

deny：表示阻断类型的策略。

noaudit：表示免审计类型的策略。

【使用指导】

本命令用来创建应用审计与管理策略，创建策略时必须指定策略类型，应用审计与管理策略分为如下三类：

- 审计策略：对匹配策略中所有过滤条件的报文，根据审计规则对此报文进行审计。
- 免审计策略：对匹配策略中所有过滤条件的报文进行免审计。
- 阻断策略：对匹配策略中所有过滤条件的报文进行阻断。

每类策略中具体可配置的内容不同，其中 **application** 命令只能在免审计和阻断类型的策略下配置，**rule**、**rule default-action** 和 **rule match-method** 命令只能在审计类型的策略下配置。

【举例】

创建一个名称为 mypolicy1 的应用审计与管理策略，并对用户的应用行为进行审计，并进入应用审计与管理策略视图。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1]
```

1.1.12 policy rename

policy rename 命令用来重命名应用审计与管理策略。

【命令】

policy rename *old-policy-name new-policy-name*

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-policy-name：表示应用审计与管理策略的原有名称，为 1～63 个字符的字符串，不区分大小写。

new-policy-name：表示应用审计与管理策略的新名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

创建应用审计与管理策略，名称为 policy1。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name policy1 audit
[Sysname-uapp-control-policy-policy1] quit
```

修改应用审计与管理策略 policy1 的名称为 policy2

```
[Sysname-uapp-control] policy rename policy1 policy2
```

1.1.13 rule

rule 命令用来配置应用审计与管理策略的审计规则。

undo rule id 命令用来删除指定的审计规则。

【命令】

rule *rule-id* { **app** *app-name* | **app-category** *app-category-name* | **any** } **behavior** { *behavior-name* | **any** } **bhcontent** { *bhcontent-name* | **any** } { **keyword** { **equal** | **exclude** | **include** | **unequal** } { *keyword-group-name* | **any** } | **integer** { **equal** | **greater** | **less** | **unequal** } { *number* } } **action** { **deny** | **permit** } [**audit-logging**]

undo rule *rule-id*

【缺省情况】

应用审计与管理策略中不存在审计规则。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id：表示审计规则 ID，取值范围为 1～64。

app *app-name*：表示对指定的应用进行审计。

app-category *app-category-name*：表示对指定的应用分类进行审计。

any：表示对所有应用和应用分类进行审计。

behavior *behavior-name*：表示对指定应用或应用分类的某一具体行为进行审计。*behavior-name* 是行为名称，**any** 表示所有行为。

bhcontent *bhcontent-name*：表示对该行为中的某一具体内容进行审计。*bhcontent-name* 是行为内容，**any** 表示所有行为内容。

keyword：表示行为内容的匹配方式为字符串形式的关键字。

- **equal**：表示审计规则对行为内容的匹配方式为与关键字完全相等。
- **exclude**：表示审计规则对行为内容的匹配方式为不包含关键字。
- **include**：表示审计规则对行为内容的匹配方式为包含关键字。
- **unequal**：表示审计规则对行为内容的匹配方式为与关键字不相等。

keyword-group-name：表示审计规则引用的关键字组，**any** 表示对指定应用或应用分类行为的所有内容进行审计。

integer：表示行为内容的匹配方式为数字。

- **equal**：表示对等于指定数字的行为内容进行审计。
- **greater**：表示对大于指定数字的行为内容进行审计。
- **less**：表示对小于指定数字的行为内容进行审计。
- **unequal**：表示对不等于指定数字的行为内容进行审计。

number：表示审计规则使用的数字，取值范围为 1～4294967295。

action：表示审计规则的动作，即对与审计规则匹配成功的报文执行的动作。

- **deny**：表示审计规则动作为阻断报文。
- **permit**：表示审计规则动作为允许报文通过。
- **audit-logging**：表示审计规则动作为生成审计日志。若未配置本参数，则与此审计规则匹配成功的报文不会生成审计日志。

【使用指导】

审计规则用来对用户的具体应用行为进行更加精细化控制。

当报文与策略中配置的所有过滤条件均匹配成功后，会根据审计规则对此报文进行更加精细化的审计。

仅在审计类型的策略中可配置此命令。

【举例】

创建一个名称为 mypolicy1 的应用审计与管理审计策略。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
```

创建第一条审计规则：对 QQ 应用行为是登录，行为内容为账号且包含关键字 1234 的用户报文进行放行审计，并生成审计日志。

```
[Sysname-uapp-control-policy-mypolicy1] rule 1 app qq behavior login bhcontent account keyword include mykeywd1 action permit audit-logging
```

创建第二条审计规则：对 QQ 应用行为是登录，行为内容为账号但不等于数字 785 的用户报文进行放行审计，但不生成审计日志。

```
[Sysname-uapp-control-policy-mypolicy1] rule 2 app qq behavior login bhcontent account integer unequal 785 action permit
```

创建第三条审计规则：对 IM 应用组行为是登录，行为内容为账号且包含关键字 0 的用户报文进行阻断，并生成审计日志。

```
[Sysname-uapp-control-policy-mypolicy1] rule 3 app-category IM behavior login bhcontent account keyword include mykeywd2 action deny audit-logging
```

【相关命令】

- **keyword-group name**
- **keyword**

1.1.14 rule default-action

rule default-action 命令用来配置审计规则的缺省动作。

【命令】

rule default-action { **deny** | **permit** }

【缺省情况】

审计规则的缺省动作为允许。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

deny：表示阻断匹配审计规则的报文。

permit：表示允许匹配审计规则的报文通过。

【使用指导】

若报文所属的应用或应用组不在所有规则所需审计的应用或应用组范围内，则设备将根据该策略中审计规则的缺省动作对报文进行处理。

【举例】

配置审计规则的缺省动作为阻断。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] rule default-action deny
```

1.1.15 rule match-method

rule match-method 命令用来配置审计规则的匹配模式。

【命令】

rule match-method { **all** | **in-order** }

【缺省情况】

审计规则的匹配模式为顺序匹配。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

all：表示审计规则匹配模式为全匹配。

in-order：表示审计规则匹配模式为顺序匹配。

【使用指导】

顺序匹配表示审计规则按照规则 ID 从小到大的顺序进行逐一匹配，一旦报文与某条审计规则匹配成功就结束此匹配过程，并根据该审计规则中的动作对此报文进行相应处理。

全匹配表示审计规则按照审计规则 ID 从小到大的顺序进行匹配，若报文与其条动作为允许的规则匹配成功，则继续匹配后续规则直到最后一条规则；若报文与某条动作为阻断的规则匹配成功，则不再进行后续规则的匹配。设备将根据所有匹配成功的审计规则中优先级最高的动作（阻断的优先级高于允许）对此报文进行相应处理。

【举例】

配置审计规则的匹配模式为全匹配。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] rule match-method all
```

1.1.16 service

service 命令用来配置作为应用审计与管理策略过滤条件的服务。

undo service 命令用来删除作为应用审计与管理策略过滤条件的服务。

【命令】

service *service-name*

undo service *service-name*

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

service-name：是服务对象组的名称，为 1～31 个字符的字符串，不区分大小写，且必须已存在。

【使用指导】

多次执行本命令，可配置多个服务作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的服务为 dns-tcp 和 dns-udp。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] service dns-tcp
[Sysname-uapp-control-policy-mypolicy1] service dns-udp
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.17 source-address

source-address 命令用来配置作为应用审计与管理策略过滤条件的源 IP 地址。

undo source-address 命令用来删除作为应用审计与管理策略过滤条件的源 IP 地址。

【命令】

source-address { **ipv4** | **ipv6** } *object-group-name*

undo source-address { **ipv4** | **ipv6** } *object-group-name*

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4：表示指定 IPv4 地址对象组。

ipv6：表示指定 IPv6 地址对象组。

object-group-name：表示地址对象组的名称，为 1～31 个字符的字符串，不区分大小写，且必须已存在。

【使用指导】

多次执行本命令，可配置多个源 IP/IPv6 地址对象组作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的源 IP 地址。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy audit
[Sysname-uapp-control-policy-mypolicy] source-address ipv4 obgroup1
[Sysname-uapp-control-policy-mypolicy] source-address ipv4 obgroup2
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.18 source-zone

source-zone 命令用来配置作为应用审计与管理策略过滤条件的源安全域。

undo source-zone 命令用来删除作为应用审计与管理策略过滤条件的源安全域。

【命令】

source-zone *source-zone-name*

undo source-zone *source-zone-name*

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

source-zone-name：表示安全域的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

多次执行本命令，可配置多个源安全域作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的源安全域为 zone1 和 zone2。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] source-zone zone1
[Sysname-uapp-control-policy-mypolicy1] source-zone zone2
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.19 time-range

time-range 命令用来配置应用审计与管理策略的生效时间。

undo time-range 命令用来恢复缺省情况。

【命令】

time-range *time-range-name*

undo time-range

【缺省情况】

应用审计与管理策略在任何时间下都生效。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

time-range-name：表示时间段的名称，为 1～32 个字符的字符串，不区分大小写。

【举例】

配置应用审计与管理审计策略 mypolicy1 的生效时间段为 work-time。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] time-range work-time
```

【相关命令】

- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.20 uapp-control

uapp-control 命令用来进入应用审计与管理视图。

【命令】

uapp-control

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在应用审计与管理视图下可完成应用审计与管理策略的创建、复制、移动和重命名以及关键字组的创建。应用审计与管理策略分为三种类型：审计（audit），免审计（noaudit）和阻断（deny），其中免审计和阻断类型的策略用来做粗粒度的应用审计与管理，审计类型的策略用来做精细化的应用审计与管理。

【举例】

进入应用审计与管理视图。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control]
```

1.1.21 user

user 命令用来配置作为应用审计与管理策略过滤条件的用户。

undo user 命令用来删除作为应用审计与管理策略过滤条件的用户。

【命令】

user *user-name*

undo user *user-name*

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name：表示用户的名称，为 1～55 个字符的字符串，区分大小写。

【使用指导】

多次执行本命令，可配置多个用户作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的用户为 managers1 和 managers2。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user managers1
[Sysname-uapp-control-policy-mypolicy1] user managers2
```

【相关命令】

- **user-identity enable**（安全命令参考/用户身份识别与管理）

1.1.22 user-group

user-group 命令用来配置作为应用审计与管理策略过滤条件的用户组。

undo user-group 命令用来删除作为应用审计与管理策略过滤条件的用户组。

【命令】

user-group *user-group-name*

undo user-group *user-group-name*

【缺省情况】

应用审计与管理策略下不存在过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-group-name：表示用户组的名称，为 1～32 个字符的字符串，不区分大小写。

【使用指导】

多次执行本命令，可配置多个用户组作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的用户组为 group1 和 group2。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user-group group1
[Sysname-uapp-control-policy-mypolicy1] user-group group2
```

【相关命令】

- **user-identity enable**（安全命令参考/用户身份识别与管理）