H3C SecPath 入侵防御系统

带宽管理配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W204-20190429
产品版本：

T5010/T5020	R8514
T5030/T5060/T5080/T5000-S/T5000-C	R8501
T1020/T1030/T1050/T1060/T1080	R8514
T1000-AK340/AK350	R8514
LSWM1IPSD0/LSQM1IPSDSC0/IM-IPSX-IV	R8512

前 言

本配置指导主要介绍带宽管理相关的特性。

前言部分包含如下内容：

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 带宽管理简介

带宽管理是指对通过设备的流量实现基于源/目的安全域、源/目的 IP 地址、用户/用户组、应用/应用组、DSCP 优先级和时间段等，进行精细化的管理和控制。目前，带宽管理功能仅支持对基于 TCP（Transmission Control Protocol，传输控制协议）、UDP（User Data Protocol，用户数据报文协议）和 ICMP（Internet Control Message Protocol，互联网控制消息协议）协议的信息进行带宽管理。

带宽管理的典型应用场景如下：

- 企业内网用户所需的带宽远大于从运营商租用的出口带宽，这时网络出口就会存在带宽瓶颈的问题。
- 网络出口中 P2P 业务类型的数据流量消耗了绝大部分的带宽资源，致使企业的关键业务得不到带宽保证。

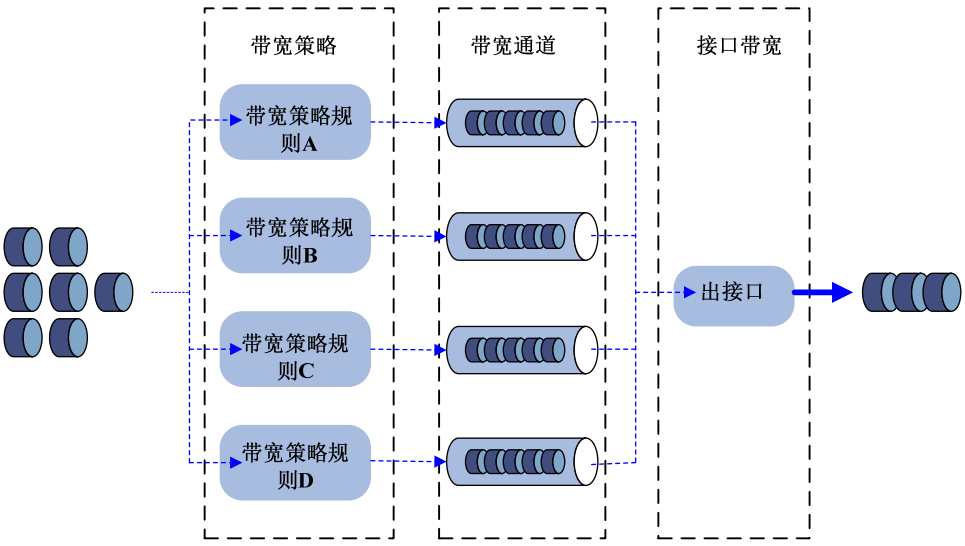
为了解决以上问题，可以在网络出口设备上部署带宽管理，针对不同的内网业务流量应用不同的带宽策略规则，实现合理分配出口带宽和保证关键业务正常运行的目的。

1.1.1 带宽管理工作原理

1. 带宽管理实现流程

带宽策略可以对符合匹配条件的流量应用带宽通道，在带宽通道中可以配置带宽保证和带宽限制功能，进而提高带宽利用率以及在线路拥堵时保证关键业务的正常运行。

图1-1 带宽管理实现流程图



带宽管理实现流程如下：

(1) 流量匹配上带宽策略中的某条规则后，如果此规则的动作中引用了带宽通道，则流量继续进入相应的带宽通道进行后续的处理，否则设备不对该流量进行带宽管理。

(2) 流量进入带宽通道后，设备会根据此带宽通道中配置的带宽限制策略对流量进行相应的处理。

(3) 如果出接口出方向上应用了QoS业务，则对流量先进行带宽策略处理，再进行QoS业务处理。

(4) 流量从出接口发送时受该接口带宽的限制。

2. 带宽策略规则

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。

带宽策略的每个规则中可以配置多种类型的匹配项，具体包括：源/目的安全域、源/目的 IP 地址、用户/用户组、应用/应用组、DSCP 优先级和时间段，规则被匹配成功的条件是：规则中已配置的所有匹配项必须均被匹配成功，但是对于用户和用户组只需匹配一项即可，应用和应用组也是只需匹配一项即可。

每个匹配项中可以配置多个条件，比如一个源 IP 地址中可以指定多个地址对象组等，匹配项被匹配成功的条件是：某匹配项中的任何一个条件被匹配成功即可。

带宽策略规则支持嵌套关系，即一个规则中可以指定一个父规则。流量与存在父规则的带宽策略规则进行匹配时，遵守如下原则：

- 首先匹配父规则，如果父规则匹配上了再匹配子规则。如果父规则没有匹配上，也不会进行后续的子规则匹配，该匹配过程失败。
- 如果子规则匹配上了，就执行子规则中指定的动作；如果子规则没有匹配上但父规则匹配上了就执行父规则中指定的动作。

3. 带宽通道

带宽通道定义了具体的带宽资源，是进行带宽管理的基础。通过带宽通道，可以将物理的带宽资源从逻辑上划分为多个虚拟的带宽通道，每个带宽通道中都可自定义相应的带宽资源限制参数和流量优先级参数。目前，带宽通道中支持的带宽资源限制参数和流量优先级参数包括以下如下几种：

- 整体的保证带宽：是指保证业务的最小带宽，在线路拥堵时，可以保证公司关键业务所需的带宽，确保此类业务不受影响。
- 整体的最大带宽：是指限制业务的最大带宽，比如限制网络中非关键业务占用的带宽资源，避免该类业务消耗大量的带宽，影响其他关键业务的正常运行。
- 每 IP 或每用户的最大带宽：设备除了支持配置整体的最大带宽之外，还支持基于 IP 地址和用户的最大带宽，实现更加精细化的带宽管理。
- 每规则、每 IP 或每用户的最大连接数和最大新建连接速率限制：通常在出现以下两类网络问题的组网环境中需要在设备上配置最大连接数和最大新建连接速率限制：某内网用户在短时间内经过设备向外部网络发起大量连接，导致设备系统资源迅速消耗，其它内网用户无法正常使用网络资源；某内部服务器在短时间内接收到大量的连接请求，导致该服务器忙于处理这些连接请求，以至于不能再接受其它客户端的正常连接请求。
- 流量优先级：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。

- 重标记报文的 DSCP 优先级：是指修改报文中 DSCP（Differentiated Services Code Point）字段的值，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。

1.2 带宽管理配置任务简介

表1-1 带宽管理配置任务简介

配置任务	说明	详细配置
配置带宽通道	必选	1.3.1
创建带宽策略规则	必选	1.3.2
配置带宽策略规则中的匹配项	可选	1.3.3
配置带宽策略规则中的动作	可选	1.3.4
管理和维护带宽策略规则	可选	1.3.5

1.3 配置带宽管理

1.3.1 配置带宽通道

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后生效。

表1-2 创建带宽通道

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入带宽策略视图	**traffic-policy**	-
创建带宽通道，并进入带宽通道视图	**profile name** *profile-name*	缺省情况下，不存在带宽通道
配置带宽通道的保证带宽和最大带宽	**bandwidth** { **downstream** | **upstream** } { **guaranteed** | **maximum** } *bandwidth-value*	缺省情况下，未配置带宽通道的保证带宽和最大带宽 请保证最大带宽不小于保证带宽
配置每IP或每用户的最大带宽	**bandwidth** { **upstream** | **downstream** } **maximum** { **per-ip** | **per-user** } *bandwidth-value*	缺省情况下，未配置每IP或每用户的最大带宽
配置最大连接数	**connection-limit count** { **per-rule** | **per-ip** | **per-user** } *connection-number*	缺省情况下，未配置最大连接数
配置最大新建连接速率	**connection-limit rate** { **per-rule** | **per-ip** | **per-user** } *connection-rate*	缺省情况下，未配置最大新建连接速率限制
配置流量优先级	**traffic-priority** *priority-value*	缺省情况下，流量优先级为1
重标记报文的DSCP优先级	**remark dscp** *dscp-value*	缺省情况下，不修改报文的DSCP优先级

配置步骤	命令	说明
退回带宽策略视图	**quit**	-
重命名带宽通道	**profile rename** *old-name new-name*	-

1.3.2 创建带宽策略规则

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。在父带宽策略规则和子带宽策略规则中均可以引用带宽通道。

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。

表1-3 创建带宽策略规则

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入带宽策略视图	**traffic-policy**	-
创建带宽策略规则，并进入该带宽策略规则视图	**rule name** *rule-name* [**parent** *parent-rule-name*]	缺省情况下，不存在带宽策略规则

1.3.3 配置带宽策略规则中的匹配项

通过在带宽策略规则中引用一个或多个匹配项来作为匹配报文的参数或依据。带宽策略规则支持的匹配项包括：

- 源/目的安全域
- 源/目的 IP 地址
- 应用/应用组
- 用户/用户组
- 时间段
- DSCP 优先级

表1-4 配置带宽策略规则中的匹配项

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入带宽策略视图	**traffic-policy**	-
进入带宽策略规则	**rule name** *rule-name* [**parent** *parent-rule-name*]	-
指定匹配报文的目的安全域	**destination-zone** *destination-zone-name*	缺省情况下，带宽策略规则下不

配置步骤	命令	说明
		存在目的安全域作为匹配条件
指定匹配报文的源安全域	**source-zone** *source-zone-name*	缺省情况下，带宽策略规则下不存在源安全域作为匹配条件
指定匹配报文的目的IP地址	**destination-address address-set** *object-group-name*	缺省情况下，带宽策略规则下不存在目的IP地址作为匹配条件
指定匹配报文的源IP地址	**source-address address-set** *object-group-name*	缺省情况下，带宽策略规则下不存在源IP地址作为匹配条件
指定匹配报文的应用或应用组	**application** { **app** *application-name* | **app-group** *application-group-name* }	缺省情况下，带宽策略规则下不存在应用或应用组作为匹配条件
指定匹配报文的用户名	**user** *user-name* [**domain** *domain-name*]	缺省情况下，带宽策略规则下不存在用户名作为匹配条件
指定匹配报文的用户组	**user-group** *user-group-name* [**domain** *domain-name*]	缺省情况下，带宽策略规则下不存在用户组作为匹配条件
指定带宽策略规则的生效时间	**time-range** *time-range-name*	缺省情况下，带宽策略规则在任何时间下都生效
指定匹配报文的DSCP优先级	**dscp**	缺省情况下，带宽策略规则下不存在DSCP优先级作为匹配条件
关闭带宽策略规则	**disable**	缺省情况下，带宽策略规则处于开启状态

1.3.4 配置带宽策略规则中的动作

如果流量成功匹配了某个带宽策略规则，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。

表1-5 配置带宽策略规则中的动作

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入带宽策略视图	**traffic-policy**	-
进入带宽策略规则视图	**rule name** *rule-name* [**parent** *parent-rule-name*]	-
配置带宽策略规则中的动作	**action qos profile** *profile-name*	缺省情况下，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

1.3.5 管理和维护带宽策略规则

为了方便用户的管理和维护，带宽策略规则创建后，可以对其进行如下操作：

- 复制
- 重命名
- 移动
- 关闭

表1-6 管理和维护带宽策略规则

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入带宽策略视图	**traffic-policy**	-
复制带宽策略规则	**rule copy** *rule-name new-rule-name*	-
重命名带宽策略规则	**rule rename** *old-rule-name new-rule-name*	-
移动带宽策略规则的排列顺序	**rule move** *rule-name1* { **after** | **before** } *rule-name2*	-

1.4 带宽管理显示维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后带宽管理的运行情况，以及带宽管理处理业务的统计信息。

表1-7 应用层检测引擎显示和维护

操作	命令
显示最大连接数限制的统计信息	**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*]
显示带宽策略规则下流量速率的统计信息	**display traffic-policy statistics bandwidth** { **all | rule** *rule-name* } [**slot** *slot-number*]

1.5 带宽管理典型配置举例

1.5.1 单通道模式带宽管理典型配置举例

1. 组网需求

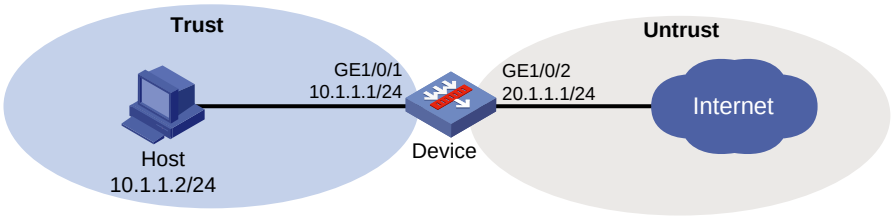
内网主机通过 Device 与外网相连，通过在 Device 上配置带宽管理功能，实现当内网流量的出口发生拥塞时优先保证 FTP 业务的需求。具体要求如下：

- 限制内网用户，访问外网爱奇艺（iQiYiPPS）应用流量的上行最大带宽和下行最大带宽均为30720kbps。

- 保证内网用户，访问外网 FTP 应用流量的上行保证带宽和下行保证带宽均为 30720kbps。
- 限制外网出接口的最大带宽为 30720kbps。

2. 组网图

图1-2 单通道模式带宽管理典型配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域（略）

(3) 配置相关的路由和安全策略，保证 Trust 安全域中的主机可以正常访 Internet（略）

(4) 配置带宽通道

创建名为 aiqiyi 的带宽通道，并进入该带宽通道视图。

```
<Device> system-view
[Device] traffic-policy
[Device-traffic-policy] profile name aiqiyi
```

配置上/下行最大带宽均为 30720kbps。

```
[Device-traffic-policy-profile-aiqiyi] bandwidth upstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] bandwidth downstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] quit
```

创建名为 profileFTP 的带宽通道，并进入该带宽通道视图。

```
[Device-traffic-policy] profile name profileFTP
```

配置上/下行保证带宽均为 30720kbps。

```
[Device-traffic-policy-profile-profileFTP] bandwidth upstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] bandwidth downstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] quit
[Device-traffic-policy] quit
```

(5) 配置出接口的最大带宽

配置接口 GigabitEthernet1/0/2 的期望带宽为 30720kbps。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] bandwidth 30720
[Device-GigabitEthernet1/0/2] quit
```

(6) 配置带宽策略规则

进入带宽策略视图。

```
[Device] traffic-policy
```

创建名为 aiqiyi 的带宽策略规则，并进入该带宽策略规则视图。

```
[Device-traffic-policy] rule name aiqiyi
```

在带宽策略规则 aiqiyi 中引用预定义应用 iQiYiPPS。

```
[Device-traffic-policy-rule-aiqiyi] application app iQiYiPPS
```

配置带宽策略规则 aiqiyi 中的动作为限流并应用带宽通道 aiqiyi。

```
[Device-traffic-policy-rule-aiqiyi] action qos profile aiqiyi
[Device-traffic-policy-rule-aiqiyi] quit
```

创建名为 ruleFTP 的带宽策略规则，并进入该带宽策略规则视图。

```
[Device-traffic-policy] rule name ruleFTP
```

配置带宽策略规则 ruleFTP 中引用预定义的应用 ftp。

```
[Device-traffic-policy-rule-ruleFTP] application app ftp
```

配置带宽策略规则 ruleFTP 中的动作为限流并应用带宽通道 profileFTP。

```
[Device-traffic-policy-rule-ruleFTP] action qos profile profileFTP
[Device-traffic-policy-rule-ruleFTP] quit
[Device-traffic-policy] quit
```

4. 验证配置

以上配置完成后，当主机的爱奇艺的流量达到 30720kbps，主机的 FTP 流量也达到 30720kbps 时，出接口 GigabitEthernet1/0/2 仅允许 FTP 应用的流量通过。

1.5.2 父子通道模式带宽管理典型配置举例

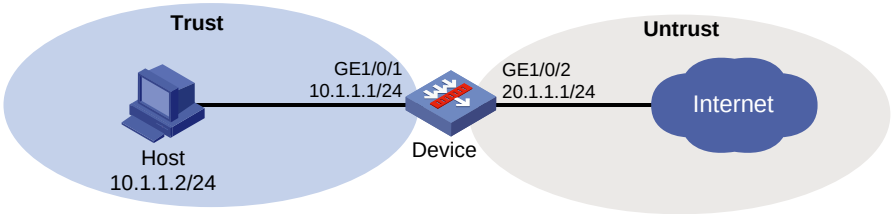
1. 组网需求

内网主机通过 Device 与外网相连，通过在 Device 上配置带宽管理功能，实现当内网流量发生拥塞时优先保证 FTP 业务的需求。具体要求如下：

- 限制内网用户，访问外网爱奇艺（iQiYiPPS）应用流量的上行最大带宽和下行最大带宽均为 30720kbps。
- 保证内网用户，访问外网 FTP 应用流量的上行保证带宽和下行保证带宽均为 30720kbps。
- 限制内网用户的最大带宽为 40000kbps。

2. 组网图

图1-3 父子通道模式带宽管理典型配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域（略）

(3) 配置相关的路由和安全策略，保证 Trust 安全域中的主机可以正常访 Internet（略）

(4) 配置带宽通道

创建名为 profile 的带宽通道，并进入该带宽通道视图。

```
<Device> system-view
[Device] traffic-policy
[Device-traffic-policy] profile name profile
```
配置上/下行最大带宽均为 40000kbps。
```
[Device-traffic-policy-profile-profile] bandwidth upstream maximum 40000
[Device-traffic-policy-profile-profile] bandwidth downstream maximum 40000
[Device-traffic-policy-profile-profile] quit
```
创建名为 aiqiyi 的带宽通道，并进入该带宽通道视图。
```
[Device-traffic-policy] profile name aiqiyi
```
配置上/下行最大带宽均为 30720kbps。
```
[Device-traffic-policy-profile-aiqiyi] bandwidth upstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] bandwidth downstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] quit
```
创建名为 profileFTP 的带宽通道，并进入该带宽通道视图。
```
[Device-traffic-policy] profile name profileFTP
```
配置上/下行保证带宽均为 30720kbps。
```
[Device-traffic-policy-profile-profileFTP] bandwidth upstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] bandwidth downstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] quit
```
(5) 配置带宽策略

创建名为 rule 的带宽策略规则，并进入该带宽策略规则视图。
```
[Device-traffic-policy] rule name rule
```
配置带宽策略规则 rule 中的动作为限流并应用带宽通道 profile。
```
[Device-traffic-policy-rule-rule] action qos profile profile
[Device-traffic-policy-rule-rule] quit
```
创建名为 aiqiyi 的带宽策略规则，并进入该带宽策略规则视图，指定带宽策略规则的父规则为 rule。
```
[Device-traffic-policy] rule name aiqiyi parent rule
```
在带宽策略规则 aiqiyi 中引用预定义应用 iQiYiPPS。
```
[Device-traffic-policy-rule-aiqiyi] application app iQiYiPPS
```
配置带宽策略规则 aiqiyi 中的动作为限流并应用带宽通道 aiqiyi。
```
[Device-traffic-policy-rule-aiqiyi] action qos profile aiqiyi
[Device-traffic-policy-rule-aiqiyi] quit
```
创建名为 ruleFTP 的带宽策略规则，并进入该带宽策略规则视图，指定带宽策略规则的父规则为 rule。
```
[Device-traffic-policy] rule name ruleFTP parent rule
```
配置带宽策略规则 ruleFTP 中引用预定义的应用 ftp。
```
[Device-traffic-policy-rule-ruleFTP] application app ftp
```
配置带宽策略规则 ruleFTP 中的动作为限流并应用带宽通道 profileFTP。
```
[Device-traffic-policy-rule-ruleFTP] action qos profile profileFTP
[Device-traffic-policy-rule-ruleFTP] quit
[Device-traffic-policy] quit
```
4. 验证配置

以上配置完成后，内网用户的实际流量会限制在 40000kbps，并且爱奇艺流量被限制在 30720kbps；当网络发生拥塞时，FTP 业务基本不受影响。

1.5.3 基于用户限速带宽管理典型配置举例

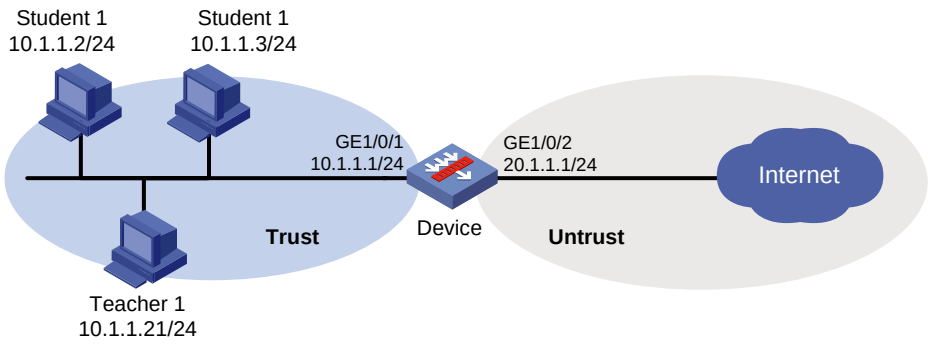
1. 组网需求

内网有两个用户组，分别为教师组 teacher 和学生组 student。teacher 组有教师 2 名，student 组有学生 5 名。通过在 Device 上配置带宽管理功能，实现基于用户进行限速带宽管理的功能。具体需求如下：

- 每个教师绑定一个 IP 地址，上行和下行均限速 10000kbps，每用户的最大连接数不超过 10000，并标记教师上网流量的 DSCP（差分服务标志）的数值为 cs7。教师使用的带宽通道转发优先级为最高。
- 每个学生绑定一个 IP 地址，上行和下行均限速 2000kbps，每用户的最大连接数不超过 10000，并标记学生上网流量的 DSCP（差分服务标志）的数值为 ef。学生使用的带宽通道转发优先级为最低。

2. 组网图

图1-4 基于用户限速带宽管理典型配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域（略）

(3) 配置相关的路由和安全策略，保证 Trust 安全域中的主机可以正常访 Internet（略）

(4) 创建网络类本地接入用户

创建名为 student1 的网络类本地接入用户。

```
<Device> system-view
[Device] local-user student1 class network
```

设置用户 student1 的密码为明文 student。

```
[Device-luser-network-student1] password simple student
```

指定用户 student1 可以使用的服务类型为 IKE、Portal 以及 SSL VPN。

```
[Device-luser-network-student1] service-type ike
[Device-luser-network-student1] service-type portal
[Device-luser-network-student1] service-type sslvpn
[Device-luser-network-student1] quit
```

创建学生用户 student1～student5，密码均为 student；教师用户 teacher1、teacher2，密码均为 teacher。教师用户和学生用户可用服务均为 IKE、Portal、SSL VPN。（具体配置步骤请参考上述学生用户 student1 的配置步骤）

创建名为 student 的用户组，并添加身份识别成员学生用户 student1～student5。

```
[Device] user-group student
[Device-ugroup-student] identity-member user student1
[Device-ugroup-student] identity-member user student2
[Device-ugroup-student] identity-member user student3
[Device-ugroup-student] identity-member user student4
[Device-ugroup-student] identity-member user student5
[Device-ugroup-student] quit
```

创建名为 teacher 的用户组，并添加身份识别成员教师用户 teacher1 和 teacher2。

```
[Device] user-group teacher
[Device-ugroup-teacher] identity-member user teacher1
[Device-ugroup-teacher] identity-member user teacher2
[Device-ugroup-teacher] quit
```

创建静态类型的身份识别用户

```
[Device] user-identity static-user student1 bind ipv4 10.1.1.2
[Device] user-identity static-user student2 bind ipv4 10.1.1.3
[Device] user-identity static-user student3 bind ipv4 10.1.1.4
[Device] user-identity static-user student4 bind ipv4 10.1.1.5
[Device] user-identity static-user student5 bind ipv4 10.1.1.6
[Device] user-identity static-user teacher1 bind ipv4 10.1.1.21
[Device] user-identity static-user teacher2 bind ipv4 10.1.1.22
```

开启身份识别功能

```
[Device] user-identity enable
```

(5) 配置带宽通道

创建名为 profile-teacher 的带宽通道，并进入该带宽通道视图。

```
[Device] traffic-policy
[Device-traffic-policy] profile name profile-teacher
```

配置上/下行最大带宽均为 10000kbps。

```
[Device-traffic-policy-profile-profile-teacher] bandwidth upstream maximum per-user 10000
[Device-traffic-policy-profile-profile-teacher] bandwidth downstream maximum per-user
10000
```

配置每用户的最大连接数为 10000。

```
[Device-traffic-policy-profile-profile-teacher] connection-limit count per-user 10000
```

配置教师使用的带宽通道转发流量优先级为最高（7）。

```
[Device-traffic-policy-profile-profile-teacher] traffic-priority 7
```

配置教师上网流量的 DSCP 值为 cs7。

```
[Device-traffic-policy-profile-profile-teacher] remark dscp cs7
[Device-traffic-policy-profile-profile-teacher] quit
```

创建名为 profile-student 的带宽通道，并进入该带宽通道视图。

```
[Device-traffic-policy] profile name profile-student
```

配置上/下行最大带宽均为 2000kbps。

```
[Device-traffic-policy-profile-profile-student] bandwidth upstream maximum per-user 2000
```

```
[Device-traffic-policy-profile-profile-student] bandwidth downstream maximum per-user 2000
```
配置每用户的最大连接数为 10000。
```
[Device-traffic-policy-profile-profile-student] connection-limit count per-user 10000
```
配置学生使用的带宽通道转发流量优先级为最低（1）。
```
[Device-traffic-policy-profile-profile-student] traffic-priority 1
```
配置教师上网流量的 DSCP 值为 ef。
```
[Device-traffic-policy-profile-profile-student] remark dscp ef
[Device-traffic-policy-profile-profile-student] quit
```
(6)　配置带宽策略

创建名为 rule-teacher 的带宽策略规则，并进入该带宽策略规则视图。
```
[Device-traffic-policy] rule name rule-teacher
```
指定匹配报文的用户组为 teacher，配置带宽策略规则 rule-teacher 中的动作为限流并应用带宽通道 profile-teacher。
```
[Device-traffic-policy-rule-rule-teacher] user-group teacher
[Device-traffic-policy-rule-rule-teacher] action qos profile profile-teacher
[Device-traffic-policy-rule-rule-teacher] quit
```
创建名为 rule-student 的带宽策略规则，并进入该带宽策略规则视图。
```
[Device-traffic-policy] rule name rule-student
```
指定匹配报文的用户组为 student，配置带宽策略规则 rule-student 中的动作为限流并应用带宽通道 profile-student。
```
[Device-traffic-policy-rule-rule-student] user-group student
[Device-traffic-policy-rule-rule-student] action qos profile profile-student
[Device-traffic-policy-rule-rule-student] quit
[Device-traffic-policy] quit
```
4. 验证配置

以上配置完成后，可以实现基于用户进行限速的功能。

- 2 位教师限速均为 10000kbps，每位学生限速为 2000kbps，且会话新建连接数都会受到限制。
- 可通过重标记 DSCP 值来区分教师和学生的上网流量，教师的上网流量会被优先转发。