H3C SecPath 防火墙产品

上网行为管理配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W303-20190927

前 言

本配置指导介绍了各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《上网行为管理配置指导》主要介绍带宽管理配置、应用审计与管理配置和共享上网管理配置。

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

带宽管理对通过设备的流量实现基于 SSID（Service Set Identifier，服务集标识符）、源/目的安全域、源/目的 IP 地址、服务、用户/用户组、应用、DSCP 优先级和时间段等，实现精细化的管理和控制。

1.1.1 带宽管理应用场景

带宽管理的应用场景如下：

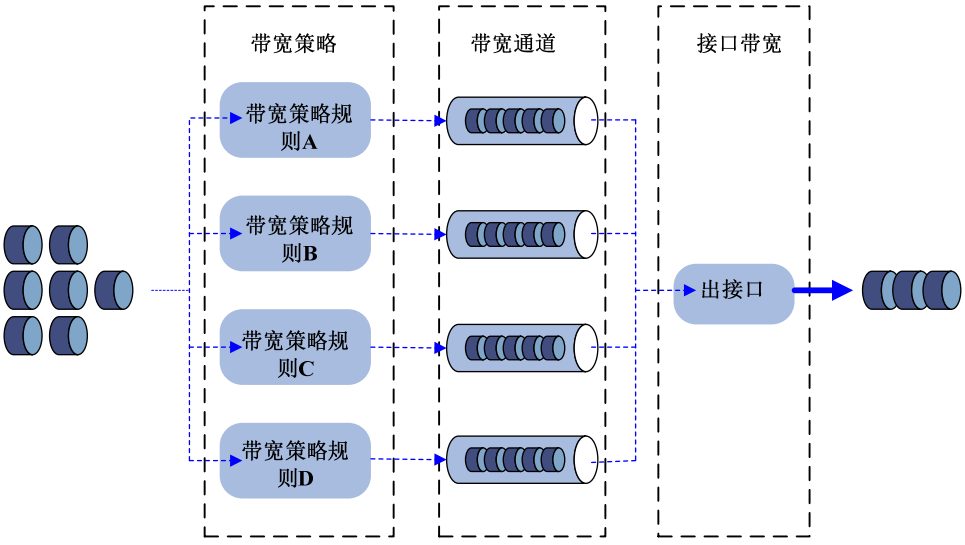
- 企业内网用户所需的带宽远大于从运营商租用的出口带宽，这时网络出口就会存在带宽瓶颈的问题。
- 网络出口中 P2P 业务类型的数据流量消耗了绝大部分的带宽资源，致使企业的关键业务得不到带宽保证。

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。

1.1.2 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) 将报文的属性信息与带宽策略规则中的过滤条件进行匹配。每种过滤条件的多个匹配项之间是或的关系，即报文与某一个过滤条件中的任意一项匹配成功，则报文与此条过滤条件匹配成功；若报文与某一个过滤条件中的所有项都匹配失败，则报文与此条过滤条件匹配失败。

(2) 若报文与某条带宽策略规则中的所有过滤条件都匹配成功（用户与用户组、应用与应用组各匹配一项即可），则报文与此条带宽策略规则匹配成功。若有一个过滤条件不匹配，则报文与此条带宽策略规则匹配失败，报文继续匹配下一条带宽策略规则。以此类推，直到最后一条带宽策略规则，若报文还未与规则匹配成功，则不对报文进行带宽管理。

(3) 报文与某条带宽策略规则匹配成功后便结束此匹配过程，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。

(4) 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。

(5) 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。

(6) 流量从出接口发送时受该接口带宽的限制。

1.1.3 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过滤条件以及流量控制的动作。带宽策略规则支持四级嵌套关系，即一个规则中可以指定一个父规则，最多支持嵌套四级。

1. 带宽策略规则过滤条件

每条带宽策略规则中可以配置多种过滤条件，具体包括：SSID（Service Set Identifier，服务集标识符）、源/目的安全域、源/目的 IP 地址、服务、用户/用户组、应用和 DSCP 优先级。每种过滤条件中均可以配置多个匹配项，比如源安全域过滤条件中可以指定多个源安全域等。

2. 带宽策略规则动作

在带宽策略规则动作中引用带宽通道后，设备将根据此带宽通道对此流量进行限流。

3. 嵌套规则匹配原则

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，先执行子规则中指定的动作，再执行父规则中指定的动作，如果父子规则对同一个带宽资源限制参数或流量优先级参数进行限制，则执行最严格的动作。如果子规则没有匹配上但父规则匹配上了，则执行父规则中指定的动作。

1.1.4 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：

1. 带宽通道限流方式

带宽通道中对流量的限制方式，包括如下两种：

- 分别设置上下行带宽：对带宽通道中的上下行流量分别限制。
- 设置总带宽：对带宽通道中的上下行流量整体限制。

2. 每规则带宽限制

每规则的保证带宽：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。

每规则的最大带宽：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。

3. 每IP或每用户带宽限制

每 IP 或每用户的保证带宽：设备除了支持配置每规则的保证带宽之外，还支持基于 IP 地址和用户的保证带宽，实现更加精细化的带宽管理。

每 IP 或每用户的最大带宽：设备除了支持配置每规则的最大带宽之外，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。

4. 连接数限制

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。

5. 流量优先级限制

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：修改报文中 DSCP（Differentiated Services Code Point）字段的值，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，能够通过 DSCP 优先级来区分流量，因此可以便于上下行设备依据修改后的 DSCP 优先级对流量采取差异化处理。

1.2 带宽管理配置限制和指导

- 配置带宽管理策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。
- 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。

1.3 带宽管理配置准备

在配置带宽管理策略之前，需完成以下任务：

- 配置时间段（请参见“ACL 和 QoS 配置指导”中的“时间段”）。
- 配置 IP 地址对象组和服务对象组（请参见“安全配置指导”中的“对象组”）。
- 配置应用（请参见“安全配置指导”中的“APR”）。
- 配置用户和用户组（请参见“安全配置指导”中的“用户身份识别与管理”）。
- 配置安全域（请参见“安全配置指导”中的“安全域”）。

1.4 带宽管理配置任务简介

带宽管理配置任务如下：

(1) 配置带宽通道

- 创建带宽通道
- 配置带宽通道参数
- 配置带宽通道引用方式
- （可选）重命名带宽通道

(2) 配置带宽策略规则

- 创建带宽策略规则
- 配置带宽策略规则过滤条件
- 配置带宽策略规则动作
- （可选）配置带宽策略规则生效时间

(3) （可选）管理和维护带宽策略规则

- 复制带宽策略规则
- 重命名带宽策略规则
- 移动带宽策略规则
- 禁用带宽策略规则
- （可选）开启带宽管理统计功能

1.5 配置带宽通道

1.5.1 创建带宽通道

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 创建带宽通道，并进入带宽通道视图。

profile name *profile-name*

1.5.2 配置带宽通道参数

1. 功能简介

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。

2. 配置限制和指导

每 IP 最大带宽、每用户最大带宽和最大带宽动态均分功能三种控制方式不能同时存在，会相互替换，最后一次配置的控制方式生效。

每 IP 保证带宽与每用户保证带宽两种控制方式不能同时存在，会相互替换，最后一次配置的控制方式生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽通道视图。

profile name *profile-name*

(4) 配置带宽参数。

- 配置每规则的保证带宽和最大带宽。

  bandwidth { **downstream** | **total** | **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。

  如需开启最大带宽的动态均分功能，则必须配置每规则的最大带宽。

- 配置每 IP 或每用户的保证带宽和最大带宽。

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

  缺省情况下，未配置每 IP 或每用户的保证带宽和最大带宽。

- 开启最大带宽动态均分功能。

  bandwidth average enable

  缺省情况下，最大带宽动态均分功能处于关闭状态。

(5) 配置连接数限制参数。

- 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。

(6) 配置优先级参数。

- 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。

1.5.3 配置带宽通道引用方式

1. 功能简介

多个带宽策略规则引用同一个带宽通道的方式，包括如下两种：

- 策略独占：表示与带宽策略规则匹配成功的流量，独享带宽通道中的带宽限制和连接数限制。
- 策略共享：表示与多条带宽策略规则匹配成功的多条流量，共享带宽通道中的带宽限制和连接数限制。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 并进入带宽通道视图。

profile name *profile-name*

(4) 配置带宽通道的引用方式。

profile reference-mode { **per-rule** | **rule-shared** }

缺省情况下，带宽通道的引用方式为策略独占。

1.5.4 重命名带宽通道

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 重命名带宽通道。

profile rename *old-name new-name*

1.6 配置带宽策略规则

1.6.1 创建带宽策略规则

1. 功能简介

一个带宽策略中可以创建多个带宽策略规则，这些规则可以独立定义，也可以继承其它规则。继承其他带宽策略规则是通过在创建带宽策略规则时为其指定父带宽策略规则实现的。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。

2. 配置限制和指导

第四级带宽策略规则不能再作为父带宽策略规则。

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。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 创建带宽策略规则，并进入该带宽策略规则视图。未配置作为带宽策略规则过滤条件的安全域

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

1.6.2 配置带宽策略规则过滤条件

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

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

(4) 配置作为带宽策略规则过滤条件的安全域。

- 配置作为带宽策略规则过滤条件的目的安全域。

  destination-zone *destination-zone-name*

- 配置作为带宽策略规则过滤条件的源安全域。

  source-zone *source-zone-name*

缺省情况下，未配置作为带宽策略规则过滤条件的安全域。

(5) 配置作为带宽策略规则过滤条件的地址对象组。

- 配置作为带宽策略规则过滤条件目的 IP 地址。

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

- 配置作为带宽策略规则过滤条件的源 IP 地址。

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

缺省情况下，未配置作为带宽策略规则过滤条件的地址对象组。

(6) 配置作为带宽策略规则过滤条件的服务。

service *object-group-name*

缺省情况下，未配置作为带宽策略规则过滤条件的服务。

(7) 配置作为带宽策略规则过滤条件的应用。

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

缺省情况下，未配置作为带宽策略规则过滤条件的应用。

(8) 配置作为带宽策略规则过滤条件的用户和用户组。

- 配置作为带宽策略规则过滤条件的用户。

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

- 配置作为带宽策略规则过滤条件的用户组。

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

缺省情况下，未配置作为带宽策略规则过滤条件的用户和用户组。

(9) 配置作为带宽策略规则过滤条件的 DSCP 优先级。

dscp *dscp-value*

缺省情况下，未配置作为带宽策略规则过滤条件的 DSCP 优先级。

(10) 配置作为带宽策略规则过滤条件的 SSID。

wlan ssid *ssid-name*

缺省情况下，未配置作为带宽策略规则过滤条件的 SSID。

本命令的支持情况与设备的型号有关，具体请参见命令参考。

1.6.3 配置带宽策略规则动作

1. 功能简介

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。

2. 配置限制和指导

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。

子规则与父规则不能引用同一个带宽通道。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

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

(4) 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。

1.6.4 配置带宽策略规则生效时间

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

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

(4) 配置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。

1.7 管理和维护带宽策略规则

1.7.1 复制带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 复制带宽策略规则。

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

1.7.2 重命名带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 重命名带宽策略规则。

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

1.7.3 移动带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 移动带宽策略规则的排列顺序。

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

1.7.4 禁用带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

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

(4) 禁用带宽策略规则。

disable

缺省情况下，带宽策略规则处于开启状态。

1.8 开启带宽管理统计功能

1. 功能简介

设备支持如下带宽管理统计功能：

- 流量统计功能：带宽管理业务将对匹配带宽策略规则的流量进行统计。
- 连接数限制统计功能：带宽管理业务将对匹配带宽策略规则的连接数限制信息进行统计。
- 规则命中统计功能：带宽管理业务将对带宽策略规则的命中情况进行统计。

2. 配置限制和指导

开启统计功能将对设备处理性能产生影响，建议仅在需要查看统计信息时开启。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 开启带宽管理统计功能。

- 开启带宽管理流量统计功能。

  statistics bandwidth enable

  缺省情况下，带宽管理流量统计功能处于关闭状态。
- 开启带宽管理连接数限制统计功能。

  statistics connection-limit enable

  缺省情况下，带宽管理连接数限制统计功能处于关闭状态。
- 开启带宽管理规则命中统计功能。

  statistics rule-hit enable

  缺省情况下，带宽管理规则命中统计功能处于关闭状态。

1.9 带宽管理显示和维护

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1-1 带宽管理显示和维护

操作	命令
显示带宽管理的流量统计信息	**display traffic-policy statistics bandwidth** { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } [**slot** *slot-number*]
显示带宽管理的连接数限制统计信息	**display traffic-policy statistics connection-limit** { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } [**slot** *slot-number*]
显示带宽策略规则的命中统计信息	**display traffic-policy statistics rule-hit** [**rule** *rule-name*] [**slot** *slot-number*]

操作	命令
清除带宽管理的流量统计信息	**reset traffic-policy statistics bandwidth** { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } [**slot** *slot-number*]
清除带宽管理的连接数限制统计信息	**reset traffic-policy statistics connection-limit** { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } [**slot** *slot-number*]
清除带宽策略规则被命中次数的统计信息	**reset traffic-policy statistics rule-hit** [**rule** *rule-name*] [**slot** *slot-number*]

1.10 带宽管理典型配置举例

1.10.1 单通道模式带宽管理配置举例

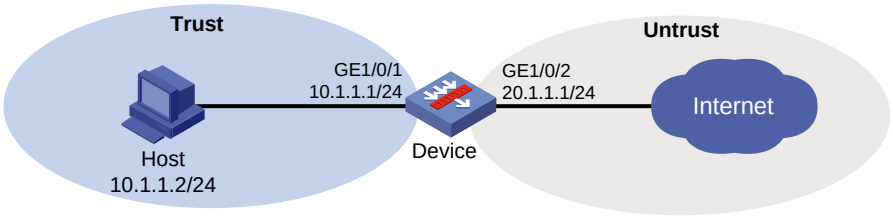
1. 组网需求

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 102400kbps。

2. 组网图

图1-2 单通道模式带宽管理配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略

(2) 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
```

(3) 配置出接口的最大带宽

配置接口 GigabitEthernet1/0/2 的期望带宽为 102400kbps。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] bandwidth 102400
[Device-GigabitEthernet1/0/2] quit
```

(4) 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-1-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-1-aiqiyi] action qos profile aiqiyi
[Device-traffic-policy-rule-1-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-2-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-2-ruleFTP] action qos profile profileFTP
[Device-traffic-policy-rule-2-ruleFTP] quit
[Device-traffic-policy] quit
```

4. 验证配置

配置完成后，当出接口 GigabitEthernet1/0/2 的流量达到 102400kbps 后，爱奇艺应用的流量最大只能达到 30720kbps，FTP 应用的流量能够保证最少达到 30720kbps。

1.10.2 父子通道模式带宽管理配置举例

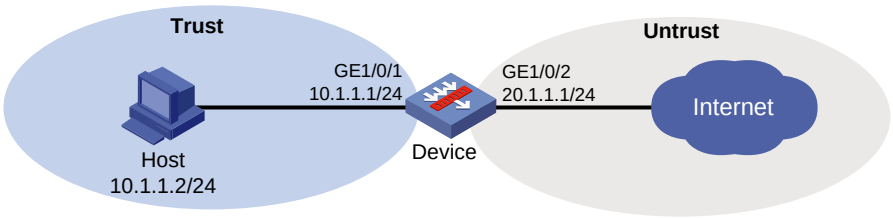
1. 组网需求

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 40960kbps。

2. 组网图

图1-3 父子通道模式带宽管理配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略

(2) 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 40960kbps。

```
[Device-traffic-policy-profile-profile] bandwidth upstream maximum 40960
[Device-traffic-policy-profile-profile] bandwidth downstream maximum 40960
[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
```

(3) 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-1-rule] action qos profile profile
[Device-traffic-policy-rule-1-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-2-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-2-aiqiyi] action qos profile aiqiyi
[Device-traffic-policy-rule-2-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-3-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-3-ruleFTP] action qos profile profileFTP
[Device-traffic-policy-rule-3-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 40960kbps，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。

1.10.3 基于用户限速带宽管理配置举例

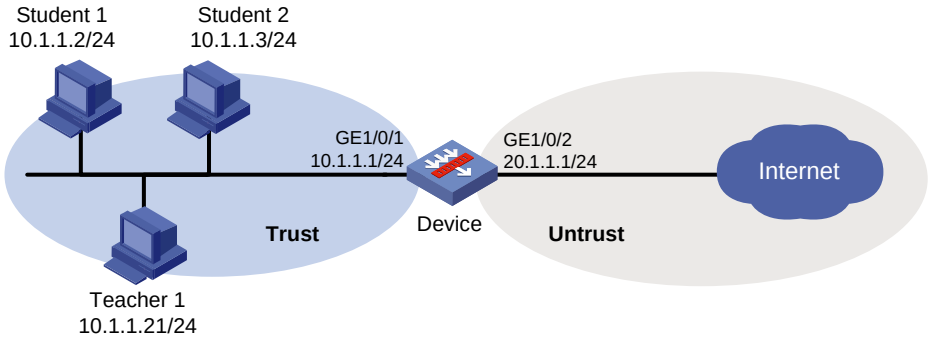
1. 组网需求

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。教师使用的带宽通道转发优先级为较低。
- 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。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配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略

(2) 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
```

(3) 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较低（2）。

```
[Device-traffic-policy-profile-profile-teacher] traffic-priority 2
[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
[Device-traffic-policy-profile-profile-student] quit
```

(4) 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-1-rule-teacher] user-group teacher
[Device-traffic-policy-rule-1-rule-teacher] action qos profile profile-teacher
[Device-traffic-policy-rule-1-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-2-rule-student] user-group student
[Device-traffic-policy-rule-2-rule-student] action qos profile profile-student
[Device-traffic-policy-rule-2-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。两位教师限速均为 10000kbps，每位学生限速为 2000kbps，且会话新建连接数都会受到限制。

目 录

1 应用审计与管理

1.1 应用审计与管理简介

应用审计与管理是在 APR（Application Recognition，应用层协议识别）的基础上进一步识别出应用的具体行为（比如 IM 聊天软件的用户登录、发消息等）和行为对象（比如 IM 聊天软件登录的行为对象是账号信息等），据此对用户的上网行为进行审计和记录。

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。

1.1.1 应用审计与管理策略

在应用审计与管理策略中通过配置过滤条件、审计规则和审计动作，可以实现对符合过滤条件的报文进行审计处理。

1. 策略类型

应用审计与管理策略分为如下三种类型：

- 审计策略：对匹配策略中所有过滤条件的报文进行审计。
- 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。

2. 过滤条件

应用审计与管理策略中可以配置多种过滤条件，具体包括：源安全域、目的安全域、源 IP 地址、目的 IP 地址、服务、用户、用户组、应用。每种过滤条件中均可以配置多个匹配项，比如源安全域过滤条件中可以指定多个源安全域等。

3. 审计规则

在审计类型的应用审计与管理策略中可以配置一系列的审计规则对某一应用的具体行为和行为对象进行精细化审计，并输出审计信息。

审计规则的匹配模式分为顺序匹配和全匹配两种，不同模式下审计规则的匹配原则如下：

- 顺序匹配：按照审计规则 ID 从小到大的顺序进行匹配，一旦报文与某条审计规则匹配成功便结束此匹配过程，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：按照审计规则 ID 从小到大的顺序进行匹配，若报文与某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；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）对此报文进行处理。

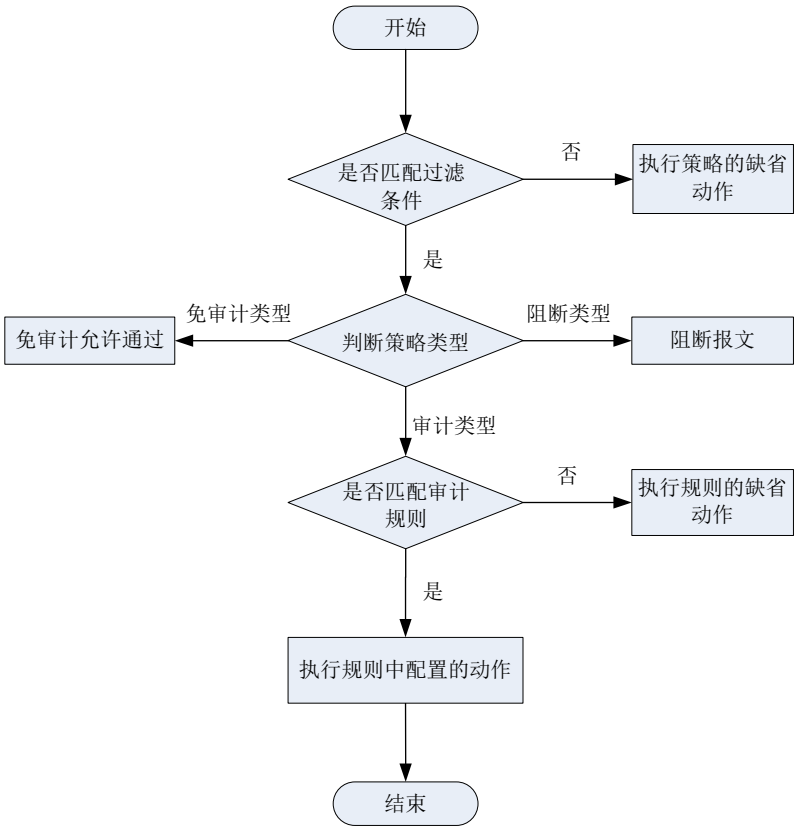
4. 审计日志

设备可以对匹配审计规则的报文输出审计日志，其输出方式包括：系统日志和快速日志。

1.1.2 应用审计与管理的报文处理流程

应用审计与管理对报文的处理流程如下图所示：

图1-1 应用审计与管理的报文处理流程图



应用审计与管理对报文的处理流程如下：

(1) 将报文的属性信息与应用审计与管理策略中的过滤条件进行匹配。每种过滤条件的多个匹配项之间是或的关系，即报文与某一个过滤条件中的任意一项匹配成功，则报文与此条过滤条件匹配成功；若报文与某一个过滤条件中的所有项都匹配失败，则报文与此条过滤条件匹配失败。

(2) 若报文与某条策略中的所有过滤条件都匹配成功（用户与用户组匹配一项即可），则报文与此条策略匹配成功。若有一个过滤条件不匹配，则报文与此条策略匹配失败，报文继续匹配下一条策略。以此类推，直到最后一条策略，若报文还未与策略匹配成功，则对报文执行策略的缺省动作。

(3) 报文与某条策略匹配成功后便结束此匹配过程，并根据此策略的类型对报文进行如下处理：

- 若策略类型为免审计类型，则允许报文通过；
- 若策略类型为阻断类型，则阻断报文；
- 若策略类型为审计类型，则继续将报文与此策略中的审计规则进行详细匹配。

(4) 若报文与审计规则匹配成功，则对报文执行审计规则中配置的动作；若匹配失败，则对报文执行审计规则的缺省动作。

1.2 应用审计与管理配置限制和指导

配置应用审计与管理策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

1.3 应用审计与管理配置准备

在配置应用审计与管理策略之前，需完成以下任务：

- 升级 APR 特征库到最新版本（请参见“安全配置指导”中的“APR”）。
- 配置时间段（请参见“ACL 和 QoS 配置指导”中的“时间段”）。
- 配置 IP 地址对象组和服务对象组（请参见“安全配置指导”中的“对象组”）。
- 配置应用（请参见“安全配置指导”中的“APR”）。
- 配置用户和用户组（请参见“安全配置指导”中的“用户身份识别与管理”）。
- 配置安全域（请参见“安全配置指导”中的“安全域”）。

1.4 应用审计与管理配置任务简介

应用审计与管理配置任务如下：

(1) 创建应用审计与管理策略

(2) 配置策略过滤条件

(3) （可选）配置策略生效时间

(4) 配置策略审计规则

(5) 配置审计规则关键字

(6) （可选）管理和维护应用审计与管理策略

(7) 激活应用审计与管理的策略和规则配置

1.5 创建应用审计与管理策略

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 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。

policy name *policy-name* { **audit** | **deny** | **noaudit** }

(4) 配置应用审计与管理策略的缺省动作。

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

缺省情况下，应用审计与管理策略的缺省动作是允许。

1.6 配置策略过滤条件

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 进入应用审计与管理策略视图。

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

(4) 配置作为应用审计与管理策略过滤条件的安全域。

- 配置作为应用审计与管理策略过滤条件的源安全域。

  source-zone *source-zone-name*

- 配置作为应用审计与管理策略过滤条件的目的安全域。

  destination-zone *destination-zone-name*

缺省情况下，未配置作为应用审计与管理策略过滤条件的安全域。

(5) 配置作为应用审计与管理策略过滤条件的地址对象组。

- 配置作为应用审计与管理策略过滤条件的源 IP 地址。

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

- 配置作为应用审计与管理策略过滤条件的目的 IP 地址。

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

缺省情况下，未配置作为应用审计与管理策略过滤条件的地址对象组。

(6) 配置作为应用审计与管理策略过滤条件的服务。

service *service-name*

缺省情况下，未配置作为应用审计与管理策略过滤条件的服务。

(7) 配置作为应用审计与管理策略过滤条件的用户和用户组。

- 配置作为应用审计与管理策略过滤条件的用户。

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

- 配置作为应用审计与管理策略过滤条件的用户组。

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

缺省情况下，未配置作为应用审计与管理策略过滤条件的用户和用户组。

(8) 配置作为应用审计与管理策略过滤条件的应用。

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

仅在免审计和阻断类型的应用审计与管理策略中可配置应用。

缺省情况下，未配置作为应用审计与管理策略过滤条件的应用。

1.7 配置策略生效时间

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 进入应用审计与管理策略视图。

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

(4) 配置应用审计与管理策略的生效时间。

time-range *time-range-name*

缺省情况下，应用审计与管理策略在任何时间都生效。

1.8 配置策略审计规则

1. 使用限制和指导

审计规则的功能仅支持在审计类型的应用审计与管理策略中配置。

在审计规则中配置 **audit-logging** 参数后：

- 缺省情况下，设备使用普通日志方式输出审计日志。有关普通日志的详细介绍，请参见“网络管理和监控配置指导”中的“信息中心”。
- 若为 DPI 业务开启了快速日志输出功能（通过在系统视图下执行 **customlog format dpi** 命令），则设备使用快速日志方式输出审计日志。有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

对于微信和 QQ，仅支持对整个应用进行阻断，不支持对指定的行为和内容进行阻断。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 进入审计类型的应用审计与管理策略视图。

policy name *policy-name* [**audit**]

(4) 配置应用审计与管理策略的审计规则。

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** | **greater-equal** | **less** | **less-equal** | **unequal** } { *number* } } **action** { **deny** | **permit** } [**audit-logging**]

缺省情况下，未配置应用审计与管理策略的审计规则。

(5) 配置审计规则的匹配模式。

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

缺省情况下，审计规则的匹配模式为顺序匹配。

(6) 配置审计规则的缺省动作。

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

缺省情况下，审计规则的缺省动作为允许。

1.9 配置审计规则关键字

1. 功能简介

配置关键字可实现对某一具体信息的匹配和审计。

4 配置步骤

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 创建关键字组，并进入关键字组视图。

keyword-group name *keyword-group-name*

(4) （可选）配置关键字组的描述信息。

description *text*

缺省情况下，未配置关键字组的描述信息。

(5) 配置审计关键字。

keyword *keyword-value*

缺省情况下，未配置审计关键字。

1.10 管理和维护应用审计与管理策略

1.10.1 复制应用审计与管理策略

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 复制应用审计与管理策略。

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

1.10.2 重命名应用审计与管理策略

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 重命名应用审计与管理策略。

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

1.10.3 移动应用审计与管理策略的位置

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 移动应用审计与管理策略的位置。

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

1.10.4 禁用应用审计与管理策略

(1) 进入系统视图。

system-view

(2) 进入应用审计与管理视图。

uapp-control

(3) 进入应用审计与管理策略视图。

policy name *policy-name*

(4) 禁用应用审计与管理策略。

disable

缺省情况下，应用审计与管理策略处于开启状态。

1.11 激活应用审计与管理的策略和规则配置

1. 功能简介

当应用审计与管理的策略和规则被创建、修改和删除后，需要配置此功能使其策略和规则配置生效。有关此功能的详细介绍请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

2. 配置限制和指导

配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一配置此功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 激活应用审计与管理的策略和规则配置。

inspect activate

缺省情况下，应用审计与管理的策略被创建、修改和删除时不生效。

1.12 应用审计与管理策略典型配置举例

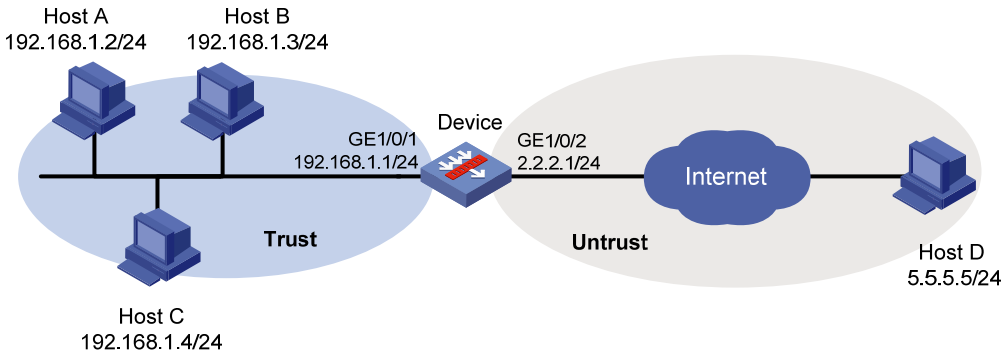
1.12.1 应用审计与管理策略审计账号登录配置举例

1. 组网需求

- 某公司内的各部门通过 Device 与 Internet 连接，该公司的工作时间为每周工作日的 8 点到 18 点。
- 通过配置应用审计与管理策略，对在上班时间登录的 QQ 账号均进行审计，并记录日志。

2. 组网图

图1-2 应用审计与管理策略审计账号登录配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略

(2) 配置时间段

创建名为 work 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<Device> system-view
[Device] time-range work 08:00 to 18:00 working-day
```

(3) 配置应用审计与管理策略

进入应用审计与管理视图。

```
[Device] uapp-control
```

创建一个名称为 audit-qq 的应用审计与管理策略，其类型为审计，并进入应用审计与管理策略视图。

```
[Device-uapp-control] policy name audit-qq audit
```

配置应用审计与管理审计策略 audit-qq 过滤条件的源安全域为 Trust。

```
[Device-uapp-control-policy-audit-qq] source-zone trust
```

配置应用审计与管理审计策略 audit-qq 过滤条件的目的安全域为 Untrust。

```
[Device-uapp-control-policy-audit-qq] destination-zone untrust
```

配置应用审计与管理审计策略 audit-qq 的生效时间段为 work。

```
[Device-uapp-control-policy-audit-qq] time-range work
```

配置审计规则，对在上班时间登录的 QQ 账号均进行审计允许登录，并记录日志。

```
[Device-uapp-control-policy-audit-qq] rule 1 app QQ behavior Login bhcontent any
keyword equal any action permit audit-logging
[Device-uapp-control-policy-audit-qq] quit
[Device-uapp-control] quit
```

(4) 激活应用审计与管理的策略和规则配置。

```
[Device] inspect activate
```

4. 验证配置

以上配置完成后，若内网主机上有 QQ 登录，则设备会对 QQ 账号登录进行审计，并会有审计日志信息输出。

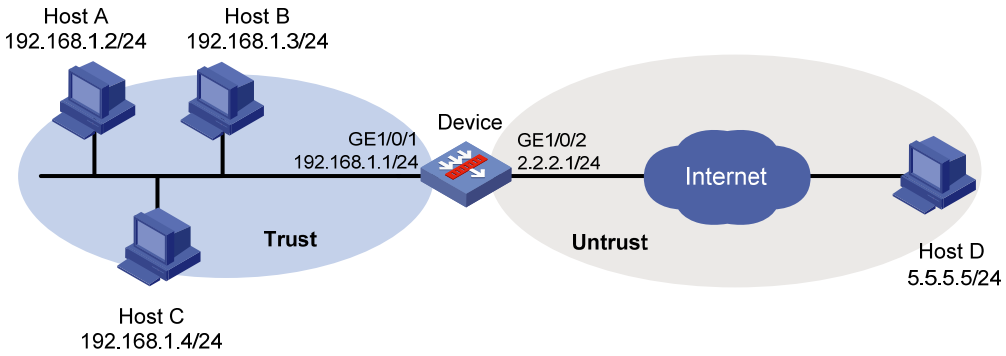
1.12.2 应用审计与管理策略审计敏感信息配置举例

1. 组网需求

某公司内的各部门通过 Device 与 Internet 连接，通过配置应用审计与管理策略，当内网用户使用微软必应搜索查找的信息中包含“机密”或“恐怖袭击”关键字时，拒绝此次搜索，并记录日志。

2. 组网图

图1-3 应用审计与管理策略审计敏感信息配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略

(2) 配置应用审计与管理策略

进入应用审计与管理视图。

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

配置名称为 keyword-bing 的关键字组，用于审计敏感信息。

```
[Device-uapp-control] keyword-group name keyword-bing
```

在关键字组 keyword-bing 中，添加关键字“机密”和“恐怖袭击”。

```
[Device-uapp-control-keyword-group-keyword-bing] keyword 机密
[Device-uapp-control-keyword-group-keyword-bing] keyword 恐怖袭击
[Device-uapp-control-keyword-group-keyword-bing] quit
```

创建一个名称为 audit-bing 的应用审计与管理策略，其类型为审计，并进入应用审计与管理策略视图。

```
[Device-uapp-control] policy name audit-bing audit
```

配置应用审计与管理审计策略 audit-bing 过滤条件的源安全域为 Trust。

```
[Device-uapp-control-policy-audit-bing] source-zone trust
```

配置应用审计与管理审计策略 audit-bing 过滤条件的目的安全域为 Untrust。

```
[Device-uapp-control-policy-audit-bing] destination-zone untrust
```

配置审计规则，当内网用户使用微软必应搜索查找的信息中包含“机密”或“恐怖袭击”关键字时，拒绝此次搜索，并记录日志。

```
[Device-uapp-control-policy-audit-bing] rule 2 app Bing behavior Search bhcontent
Keyword keyword include keyword-bing action deny audit-logging
[Device-uapp-control-policy-audit-bing] quit
[Device-uapp-control] quit
```

(3) 激活应用审计与管理的策略和规则配置。

```
[Device] inspect activate
```

4. 验证配置

以上配置完成后，当内网用户使用微软必应搜索查找的信息中包含“机密”或“恐怖袭击”关键字时，此次搜索会没有响应，并会有审计日志信息输出。

目 录

1 共享上网管理

1.1 共享上网管理简介

共享上网管理功能可对共享上网行为进行检测和管理。

1.1.1 共享上网检测方式

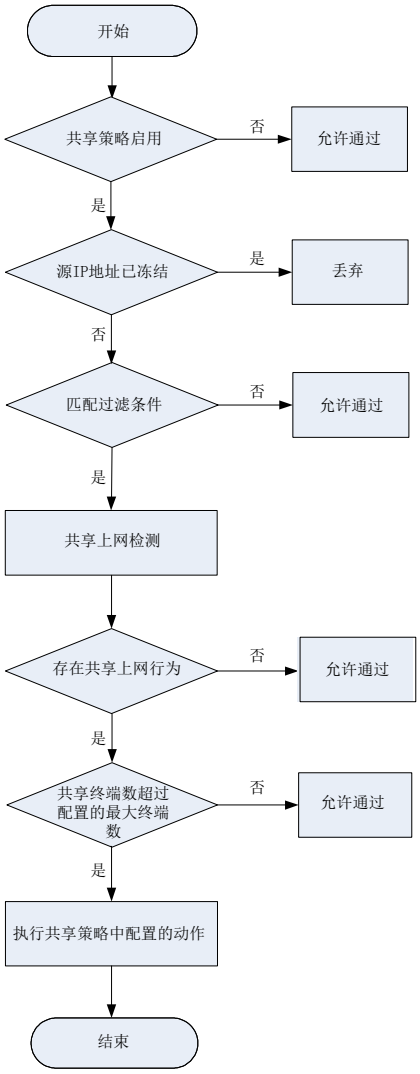
共享上网管理通过如下方式对报文的源 IP 地址是否存在共享上网行为进行检测：

- 应用特征检测方式：设备通过在 APR（Application Recognition，应用层协议识别）的基础上分析应用层的相关特征来检测终端的共享上网行为。有关 APR 的详细介绍，请参见“安全配置指导”中的“APR”。
- IPID 轨迹检测方式：设备可通过对报文的 IPID 字段的变化情况进行分析来检测终端的共享上网行为。

1.1.2 共享上网管理实现流程

共享上网管理对报文的处理流程如下图所示：

图1-1 共享上网管理的实现流程图



共享上网管理对报文的处理过程如下：

(1) 设备收到报文后，如果未启用共享策略，则允许报文通过；如果共享策略处于启用状态，则进入步骤（2）处理。

(2) 判断报文的源 IP 地址是否已经处于冻结状态。如果已冻结，则丢弃报文；如果未冻结，则进入步骤（3）处理。

(3) 报文与共享策略中的过滤条件进行匹配。如果匹配失败，则允许报文通过；如果匹配成功，则进行共享上网检测。

(4) 如果未检测到报文的源 IP 地址存在共享行为，则允许报文通过；如果检测到报文的源 IP 地址存在共享行为，则将该 IP 地址下共享的终端数量与共享上网管理策略中配置的每个 IP 地址允许的最大共享终端数进行比较：

- 如果未超过，则允许报文通过。
- 如果超过配置的最大终端数，则对报文执行共享上网管理策略中配置的动作，有关共享上网管理策略动作的详细介绍，请参见 1.9 配置共享上网管理策略动作。

1.2 共享上网管理配置任务简介

共享上网管理配置任务如下：

(1) 创建共享上网管理策略

(2) 配置共享上网管理策略过滤条件

(3) （可选）开启应用特征检测功能

(4) （可选）开启IPID轨迹检测功能

(5) 配置每个IP地址可被共享的最大终端数

(6) 配置共享上网管理策略动作

(7) 激活共享上网管理策略配置

(8) （可选）禁用共享上网管理策略

(9) （可选）手工冻结和解冻源IP地址

1.3 共享上网管理配置准备

在配置共享上网管理策略之前，需完成以下任务：

- 升级 APR 特征库到最新版本。
- 配置 IP 地址对象组（请参见“安全配置指导/对象组”）。
- 配置用户和用户组（请参见“安全配置指导/用户身份识别与管理”）。
- 配置安全域（请参见“安全配置指导/安全域”）。

1.4 创建共享上网管理策略

1. 配置限制和指导

目前，仅支持创建一个共享上网管理策略。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 创建共享上网管理策略，并进入共享上网管理策略视图。

policy name *policy-name*

(4) 配置策略的描述（可选）。

description *text*

缺省情况下，未配置共享上网管理策略的描述信息。

1.5 配置共享上网管理策略过滤条件

1. 功能简介

共享上网管理策略支持配置多种过滤条件，每种过滤条件支持配置多个匹配项，且多个匹配项之间是或的关系，即如果报文与某一个过滤条件中的任意一项匹配成功，则报文与此条过滤条件匹配成功；若报文与某一个过滤条件中的所有项都匹配失败，则报文与此条过滤条件匹配失败。

如果报文与某条策略中的所有过滤条件都匹配成功（用户与用户组匹配一项即可），则报文与此条策略匹配成功。如果有一个过滤条件匹配失败，则报文与此条策略匹配失败。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 进入共享上网管理策略视图。

policy name *policy-name*

(4) 配置作为共享上网管理策略过滤条件的安全域。

- 配置作为共享上网管理策略过滤条件的源安全域。

  source-zone *source-zone-name*

  缺省情况下，未配置作为共享上网管理策略过滤条件的源安全域。

- 配置作为共享上网管理策略过滤条件的目的安全域。

  destination-zone *destination-zone-name*

  缺省情况下，未配置作为共享上网管理策略过滤条件的目的安全域。

(5) 配置作为共享上网管理策略过滤条件的地址对象组。

- 配置作为共享上网管理策略过滤条件的源 IP 地址。

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

  缺省情况下，未配置作为共享上网管理策略过滤条件的源 IP 地址。

- 配置作为共享上网管理策略过滤条件的目的 IP 地址。

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

  缺省情况下，未配置作为共享上网管理策略过滤条件的目的 IP 地址。

(6) 配置作为共享上网管理策略过滤条件的用户和用户组。

- 配置作为共享上网管理策略过滤条件的用户。

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

  缺省情况下，未配置作为共享上网管理策略过滤条件的用户。

- 配置作为共享上网管理策略过滤条件的用户组。

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

  缺省情况下，未配置作为共享上网管理策略过滤条件的用户组。

1.6 开启应用特征检测功能

1. 功能简介

开启本功能后，设备将针对用户特定应用（包括 QQ、微信、58 同城和美团）的共享上网状态进行检测。建议在不需要对特定应用进行检测的场景下关闭本功能。

2. 配置限制和指导

应用检测功能与 IPID 轨迹检测功能互不影响，可同时开启，请管理员根据实际场景进行配置。

如果应用本身进行了加密处理，则应用检测功能无法对其进行共享上网行为检测。

开启本功能后，将对设备业务处理性能产生影响，请管理员根据设备实际情况进行配置。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 进入共享上网管理策略视图。

policy name *policy-name*

(4) 开启共享上网管理策略的应用特征检测功能。

application-inspect enable

缺省情况下，应用检测功能处于开启状态。

1.7 开启IPID轨迹检测功能

1. 功能简介

缺省情况下，设备使用应用特征检测方式对共享上网行为进行检测，但是，该检测方式只对特征库中的特定应用有效。为了满足更多场景的需求，可使用 IPID 轨迹检测功能对共享上网状态进行检测。

2. 配置限制和指导

应用检测功能与 IPID 轨迹检测功能互不影响，可同时开启，请管理员根据实际场景进行配置。

本功能仅支持检测 Windows 系统的终端，且报文 IPID 呈规律性变化。

本功能仅支持检测 IPv4 类型地址。

本功能不支持对移动终端进行共享上网行为检测。

开启此功能后，将对设备业务处理性能产生影响，请管理员根据设备实际情况进行配置。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 进入共享上网管理策略视图。

policy name *policy-name*

(4) 开启共享上网管理策略的 IPID 轨迹检测功能。

ipid-trail enable

缺省情况下，IPID 轨迹检测功能处于关闭状态。

1.8 配置每个IP地址可被共享的最大终端数

1. 功能简介

本命令用于限制可以同时使用相同 IP 地址进行共享上网的的终端数量。当设备检测到某 IP 地址下的共享终端数大于配置的最大终端数时，将对该 IP 地址执行共享上网管理策略中配置的动作；如果检测到的终端数小于配置的最大终端数，则允许此共享行为。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 进入共享上网管理策略视图。

policy name *policy-name*

(4) 配置每个 IP 地址可被共享的最大终端数。

per-ip-shared max-terminals *number*

缺省情况下，不限制每个 IP 地址可被共享的终端数。

1.9 配置共享上网管理策略动作

1. 功能简介

设备将根据本功能配置的动作对命中策略的源 IP 地址执行相应的操作：

当动作为冻结时，设备将自动冻结该 IP 地址，后续来自该 IP 地址的报文将被丢弃。当达到冻结时间后，被冻结的 IP 地址将自动解冻。

当动作为允许时，设备将允许该 IP 地址的共享上网行为。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 进入共享上网管理策略视图。

policy name *policy-name*

(4) 配置共享上网管理策略的动作。

action { **freeze** *freeze-time* | **permit** } [**logging**]

缺省情况下，动作为允许。

1.10 激活共享上网管理策略配置

1. 功能简介

当共享上网管理策略被创建和删除后，需要配置此功能使其生效。

2. 配置限制和指导

配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一配置此功能。

有关此功能的详细介绍请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 激活共享上网管理策略配置。

inspect activate

缺省情况下，共享上网管理策略被创建和删除时不生效。

1.11 禁用共享上网管理策略

1. 功能简介

如果在某些组网环境中暂时不需要启用共享上网管理策略，可以配置本功能禁用该策略。

2. 配置限制和指导

目前设备仅支持同时配置一个共享上网管理策略，禁用该策略后，共享上网管理功能将失效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 进入共享上网管理策略视图。

policy name *policy-name*

(4) 禁用共享上网管理策略。

disable

缺省情况下，共享上网管理策略处于开启状态。

1.12 手工冻结和解冻源IP地址

1. 功能简介

本功能适用于如下情况：

- 当某 IP 地址处于冻结状态且未达到冻结时间时，可通过本功能进行手工解冻。
- 当某 IP 地址处于未冻结状态时，可通过本功能进行手工冻结。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入共享上网管理视图。

netshare-control

(3) 手工冻结 IP 地址。

freeze { **ipv4** | **ipv6** } **ip-address** [**vpn-instance** *vpn-instance-name*] **time** *freeze-time*

(4) 手工解冻 IP 地址。

unfreeze { **ipv4** | **ipv6** } **ip-address** [**vpn-instance** *vpn-instance-name*]

1.13 共享上网管理显示和维护

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共享上网管理的运行情况。

表1-1 共享上网管理显示和维护

操作	命令
显示共享上网状态信息	**display netshare-control** [{ **ipv4** | **ipv6** } **ip-address** | **status** { **frozen** | **unfrozen** }] [**slot** *slot-number*]

1.14 共享上网管理策略典型配置举例

1.14.1 共享上网管理基本组网配置举例

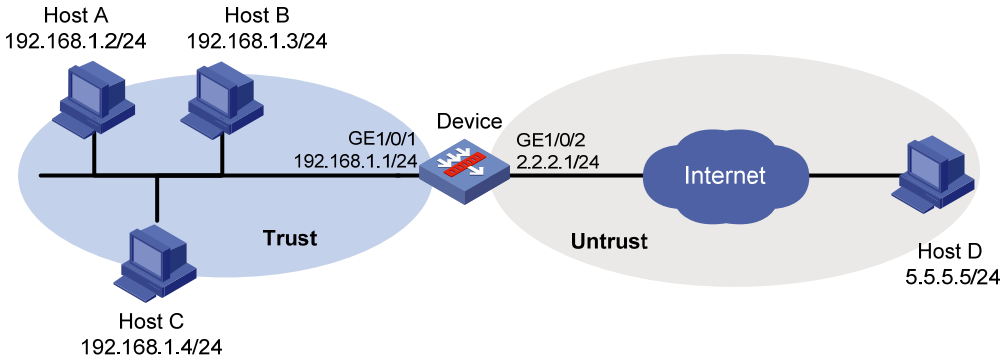
1. 组网需求

如 图 1-2 所示，Device分别通过Trust安全域和Untrust安全域与局域网和Internet相连。现有以下组网需求：

某公司内的各部门通过 Device 与 Internet 连接，管理员发现有员工在主机上开启代理软件，为其他主机共享上网。现在需要通过配置共享上网管理功能策略，禁止共享上网行为。如果检测到存在共享上网行为，则将源 IP 地址冻结 1 小时并记录日志。

2. 组网图

图1-2 共享上网管理配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略

(2) 配置共享上网管理策略

进入共享上网管理视图。

```
<Device> system-view
[Device] netshare-control
```

创建一个名称为 a 的共享上网管理策略，并进入共享上网管理策略视图。

```
[Device-netshare-control] policy name a
```

配置共享上网管理策略 a 过滤条件的源安全域为 Trust。

```
[Device-netshare-control-policy-a] source-zone trust
```

配置共享上网管理策略 a 过滤条件的目的安全域为 Untrust。

```
[Device-netshare-control-policy-a] destination-zone untrust
```

配置共享上网管理策略 a 的每个 IP 地址可被共享的最大终端数。

```
[Device-netshare-control-policy-a] per-ip-shared max-terminals 1
```

配置共享上网管理策略 a 的动作为冻结 1 小时并记录日志。

```
[Device-netshare-control-policy-a] action freeze 60 logging
[Device-netshare-control-policy-a] quit
[Device-netshare-control] quit
```

(3) 激活共享上网管理策略配置。

```
[Device] inspect active
```

4. 验证配置

以上配置完成后，如果内网有主机通过代理软件上网，就能检测到该主机的 IP 地址存在共享上网行为，并冻结该 IP 地址 1 小时并记录日志。