UNIS 防火墙产品

带宽管理配置指导(V7)

北京紫光恒越网络科技有限公司
http://www.unis-hy.com

资料版本：5P100-20160616

前 言

UNIS 防火墙产品配置指导(V7)介绍了防火墙产品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。《带宽管理配置指导》主要介绍带宽管理相关的特性。

前言部分包含如下内容：

适用款型

防火墙产品款型较多，形态丰富，本手册所描述的内容适用于如下产品款型：

表1 手册适用的产品款型

款型	形态
UNIS F5000-M06防火墙	分布式设备，可以运行在： • 独立运行模式 • IRF 模式
UNIS F5000-G20防火墙	集中式IRF设备
UNIS F1000-G20/G50/G60/G80防火墙	集中式IRF设备

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. 端口编号示例约定

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。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unis-hy.com

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：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 带宽管理

说明

对于本节命令中的 CPU 参数，仅 F5000-M06 产品支持。

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。

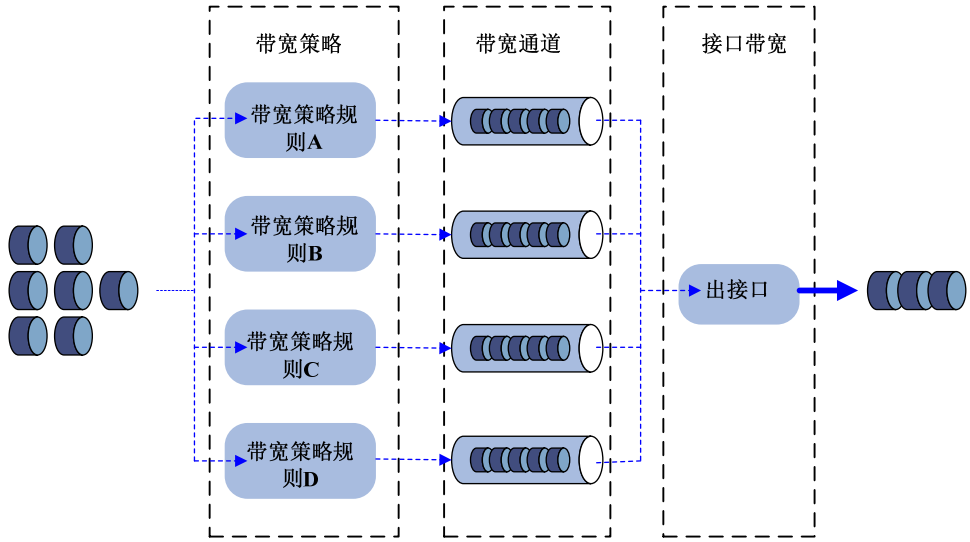
为了解决以上问题，可以在网络出口设备上部署带宽管理，针对不同的内网业务流量应用不同的带宽策略规则，实现合理分配出口带宽和保证关键业务正常运行的目的。

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) 如果接口上应用了 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。

一个带宽策略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。每类匹配项中可以配置多个条件，比如一个带宽策略规则中可以指定多个目的安全域、多个用户或多个应用组等。

判断一个带宽策略规则是否被匹配上的原则如下：

- 只有带宽策略规则中已配置的所有匹配项都被匹配上，该带宽策略规则才算匹配成功。
- 只要匹配项中的任何一个条件被匹配上则该匹配项被匹配成功。

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
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*	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*	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

为了方面用户的管理和维护，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（分布式设备-独立运行模式/集中式IRF设备）	**display traffic-policy statistic 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*]]
显示最大连接数限制的统计信息（分布式设备-IRF设备）	**display traffic-policy statistic 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*]]
显示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/集中式IRF设备）	**display traffic-policy statistic bandwidth rule** { *rule-name* | **all** } [**slot** *slot-number* [**cpu** *cpu-number*]]
显示带宽策略规则下流量速率的统计信息（分布式设备-IRF设备）	**display traffic-policy statistic bandwidth rule** { *rule-name* | **all** } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

1.5 带宽管理典型配置举例

1.5.1 配置基于应用的带宽管理典型配置举例

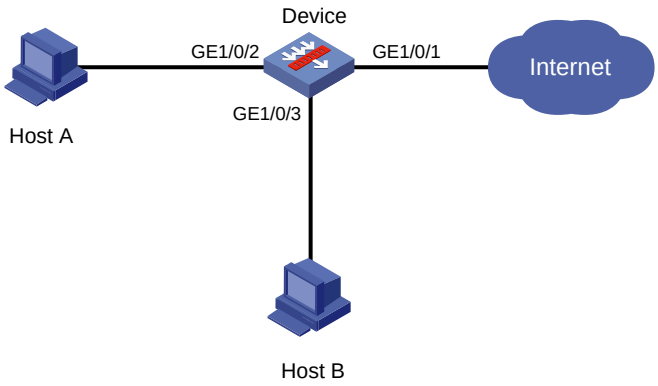
1. 组网需求

主机 A 和主机 B 通过 Device 与外网相连，通过在 Device 上配置基于应用的带宽管理功能，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 P2P 应用流量的上行最大带宽和下行最大带宽均为 30720kbit/s。
- 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 30720kbit/s
- 限制外网出接口的最大带宽为 30720kbit/s。

2. 组网图

图1-2 配置基于应用的带宽管理典型配置组网图



3. 配置步骤

说明

- 配置该功能前请确保内网主机与外网已路由可达。
- 配置该功能前请确保带宽策略规则中引用的应用或应用组在设备上已存在。有关应用或应用组的详细配置请参见“安全配置指导”中的“APR”。

(1) 配置带宽通道

创建名为 profileP2P 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 profileP2P
```

配置上/下行最大带宽均为 30720kbit/s。

```
[Device-traffic-policy-profile-profileP2P] bandwidth upstream maximum 30720
[Device-traffic-policy-profile-profileP2P] bandwidth downstream maximum 30720
[Device-traffic-policy-profile-profileP2P] 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 30720kbit/s。

```
[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
```

(2) 配置出接口的最大带宽

配置接口 GigabitEthernet1/0/1 的期望带宽为 30720kbit/s。

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

(3) 配置带宽策略规则

进入带宽策略视图。

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

创建名为 ruleP2P 的带宽策略规则，并进入该带宽策略规则视图。

```
[Device-traffic-policy] rule name ruleP2P
```

在带宽策略规则 ruleP2P 中引用自定义的应用 P2P。

```
[Device-traffic-policy-rule-ruleP2P] application app p2p
```

配置带宽策略规则 ruleP2P 中的动作为限流并应用带宽通道 profileP2P。

```
[Device-traffic-policy-rule-ruleP2P] action qos profile profileP2P
[Device-traffic-policy-rule-ruleP2P] 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 A 的 P2P 的流量达到 30720kbit/s，主机 B 的 FTP 流量也达到 30720kbit/s 时，出接口 GigabitEthernet1/0/1 仅允许 FTP 应用的流量通过。