

HCIE-Security 备考指南

带宽管理



HCIE 只是一个开始....

HCIE 仅是一个证书...懂得做人和处事比证书和技能更重要...

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 带宽管理需要掌握的知识点.....1

带宽管理简介.....1

总体流程.....1

带宽通道.....2

带宽策略.....5

接口带宽.....7

应用场景.....7

配置带宽通道.....10

配置带宽策略.....12

举例：在网络边界安全防护的场景中实施带宽管理.....15

HCIE-Security 模拟面试问题及面试建议.....25

HCIE-Security 带宽管理需要掌握的知识点

- 掌握防火墙带宽管理原理及配置

带宽管理简介

介绍带宽管理的定义和目的。

定义

带宽管理指的是 NGFW 基于源安全区域/入接口、目的安全区域/出接口、源地址/地区、目的地址/地区、用户、应用、服务、时间段和报文 DSCP 优先级信息，对通过自身的流量进行管理和控制。

目的

带宽管理提供带宽保证、带宽限制和连接数限制功能，可以提高带宽利用率，避免带宽耗尽。

- 带宽保证

保证网络中关键业务所需的带宽，当线路繁忙时，确保此类业务不受影响。

- 带宽限制

限制网络中非关键业务占用的带宽，避免此类业务消耗大量带宽资源，影响其他业务。

- 连接数限制

限制业务的连接数，有利于降低该业务占用的带宽，还可以节省设备的会话资源。

在 NGFW 上部署带宽管理，可以帮助网络管理员合理分配带宽资源，从而提升网络运营质量。

总体流程

了解 NGFW 实现带宽管理的整体流程，有助于后续配置。

NGFW 通过带宽策略、带宽通道和接口带宽来实现带宽管理功能，如[图 1](#)所示。

- [带宽通道](#)

带宽通道定义了被管理的对象所能够使用的带宽资源，将被带宽策略引用。

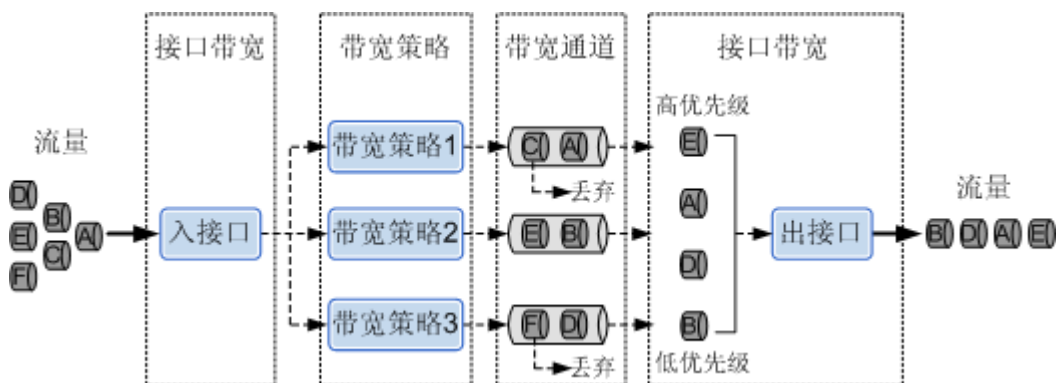
- [带宽策略](#)

带宽策略定义了被管理的对象和动作，并引用带宽通道。

- [接口带宽](#)

接口带宽定义了接口入方向和出方向的实际带宽，出方向上的流量发生拥塞时，启用队列调度机制。

图 1 带宽管理实现流程



整体的处理流程如下：

1. 流量从入接口进入时，受接口带宽的限制，然后进行带宽策略的处理。
2. 流量匹配带宽策略，经过带宽策略的分流后，进入相应的带宽通道进行处理。带宽通道的处理包括：
 - 丢弃超过了预先定义的最大带宽的流量、限制业务的连接数。
 - 标记流量的优先级，作为后续队列调度的依据。
3. 流量从出接口发送时，受接口带宽的限制。如果流量大于接口带宽，将根据转发优先级对流量进行队列调度，保证高优先级的报文被优先发送。

带宽通道

流量匹配带宽策略后进入带宽通道，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资源。带宽通道使用多个参数来对带宽资源进行描述和控制，包括整体的保证带宽和最大带宽、每 IP/每用户的保证带宽和最大带宽、连接数限制和优先级重标记。此外，带宽通道还可以实现带宽资源的闲时复用。

整体的保证带宽和最大带宽

整体的保证带宽是指进入带宽通道的流量可获得的最小带宽资源，整体的最大带宽是指进入带宽通道的流量可获得的最大带宽资源。流量进入带宽通道后，NGFW 将当前流量与带宽通道中设置的保证带宽/最大带宽进行比较，采取不同的处理方式：

- 如果流量小于保证带宽，这部分流量在出接口发送环节能够确保被转发。
- 如果流量大于最大带宽，则直接丢弃超出最大带宽的流量。
- 超出保证带宽的流量，在出接口发送环节将会与其它带宽通道中同类型的流量自由竞争带宽资源。带宽通道的优先级越高，就会更优先获得剩余带宽资源。获得带宽资源后发送流量，否则丢弃流量。

带宽通道被带宽策略引用后，最大带宽就会在带宽策略中起作用，其工作方式包括策略独占和策略共享两种：

- 策略独占

每一个引用带宽通道的带宽策略都独自受到该带宽通道的约束，即符合该带宽策略匹配条件的流量，独享最大带宽资源。

- 策略共享

所有引用带宽通道的带宽策略都共同受到该带宽通道的约束，即符合多条带宽策略匹配条件的流量，共享最大带宽资源。

每 IP/每用户的保证带宽和最大带宽

除了设置整体的保证带宽和最大带宽之外，还可以在带宽通道中定义针对 IP 或用户的保证带宽和最大带宽，实现粒度更加细化的带宽限制。

当带宽通道被带宽策略引用后，NGFW 会基于 IP 地址或用户，对符合带宽策略匹配条件的流量进行统计，保证带宽和最大带宽的作用与整体带宽类似，只是作用范围细化至每 IP/用户范围。

另外，NGFW 还提供了基于整体保证带宽和在线 IP 数量，为每一个 IP 实现带宽动态均分的控制方式，充分利用了闲置的带宽资源。

上下行带宽独立控制和整体控制

在上面提到的最大带宽和保证带宽，均支持上下行分别配置。在带宽通道中，上下行代表的含义跟带宽策略本身有关：与带宽策略同向时，定义为上行；与带宽策略反向时，定义为下行。

换言之，数据流命中带宽策略，定义为上行流量；将带宽策略中的源和目的互换进行反向查询，命中的流量定义为下行流量。

此外，对于上下行带宽独立控制这种细粒度的管控方式，NGFW 还提供了基于上行和下行流量之和的带宽管控方式，大大增加了管理的灵活性。

连接数限制

通信双方建立的连接在 NGFW 上体现为会话，一条会话对应一个连接。NGFW 通过限制自身生成的会话数量，来实现连接数限制功能，主要作用包括：

- P2P（Point to Point）业务会产生大量的连接，限制其连接数有利于减少 P2P 业务的流量，降低带宽占用。
- 在部署了内网服务器的场景中，连接数限制功能可以辅助 NGFW 防范针对内网服务器的 DDoS（Distributed Denial Of Service）攻击。
- 节省 NGFW 上的会话资源。

带宽通道中可以设置整体的最大连接数，也可以设置针对源 IP 或用户的最大连接数，实现更加细化的连接数限制。

优先级重标记

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。

NGFW 支持在带宽策略中配置 DSCP 作为匹配条件，也可以在带宽通道中对符合条件的报文修改其 DSCP 字段值，便于 NGFW 的上下行设备根据修改后的 DSCP 优先级来区分流量。

带宽复用

带宽复用是带宽通道的重要特征，指的是多条流量进入同一个带宽通道后，带宽通道内带宽资源的动态分配方式。当带宽通道中某一条流量没有使用带宽资源时，该空闲的带宽资源可以借给其它流量使用；如果有流量需要使用带宽资源时，可以压缩其它流量的带宽，从而将带宽资源抢占回来。

带宽复用包括下面几种情况：

- 多条流量匹配到了同一个带宽策略，多条流量之间可以实现带宽复用。
- 多个带宽策略以策略共享的方式引用带宽通道，则匹配了带宽策略的多条流量之间可以实现带宽复用。
- 匹配了父子策略中的多个子策略的多条流量之间可以实现带宽复用。

带宽策略

带宽策略决定了对网络中的哪些流量进行带宽管理，以及如何进行带宽管理。

带宽策略中引用带宽通道，所有符合带宽策略匹配条件的流量，都只能使用该带宽通道所定义的带宽资源。

规则的组成信息

带宽策略是多个带宽策略规则的集合，带宽策略规则由条件和动作组成。

条件指的是 NGFW 匹配报文的依据，包括：

- 源安全区域/入接口
- 目的安全区域/出接口
- 源地址/地区
- 目的地址/地区
- 用户
- 应用
- 服务
- 时间段
- 报文 DSCP 优先级

动作指的是 NGFW 对报文采取的处理方式，包括：

- 限流

对符合条件的流量进行管理。当动作为限流时，还需在带宽策略中引用带宽通道，对流量的具体管理措施由该带宽通道决定。

- 不限流

对符合条件的流量不进行管理。

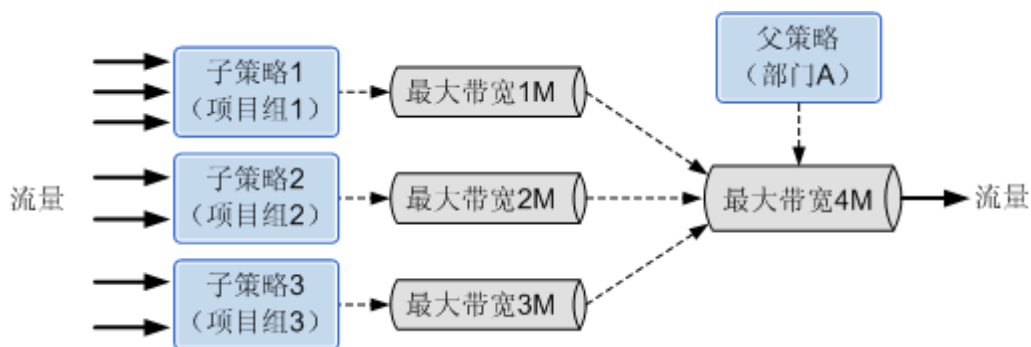
默认情况下，NGFW 上存在一条缺省的带宽策略，所有匹配条件均为任意（any），动作为不限流。

多级策略

NGFW 的带宽管理功能支持多级策略的配置方式，在一条带宽策略下，还可以继续配置多条带宽子策略。目前 NGFW 支持四级策略，对于多条同级策略，NGFW 按照界面上的排列顺序从上到下依次匹配，只要匹配了一条策略的所有条件，则执行带宽通道的动作，不再继续匹配剩下的规则；对于多级策略，流量先匹配父策略，再去匹配子策略，直到匹配到最后一级可以匹配到的子策略为止。

在进行带宽限制时使用多级策略，与使用独立的带宽策略相比，可以达到更好的带宽复用效果。例如，部门 A 中包括三个项目组：项目组 1、项目组 2 和项目组 3，使用父策略限制部门 A 的最大带宽，同时使用三条子策略限制三个项目组的最大带宽，如[图 1](#)所示。

图 1 带宽限制时使用多级策略示意图



假设项目组 3（子策略 3）中只有 1M 的流量，项目组 1（子策略 1）和项目组 2（子策略 2）就可以复用部门 A（父策略）中剩余的 3M 带宽资源。如果不使用多级策略，而使用三条引用了不同带宽通道的独立的带宽策略，这三条带宽策略之间无法共用带宽通道，三个项目组之间也就无法实现带宽资源的复用。

接口带宽

配置接口带宽，限制 NGFW 的接口在入方向和出方向上能够使用的带宽资源。

NGFW 作为大中型企业的出口网关时，企业向运营商申请的带宽资源一般都小于 NGFW 出接口的物理带宽。如果 NGFW 无法感知出接口上所能够使用的最大带宽资源，导致发出去的流量到达对端设备后产生拥塞，严重的话将会造成丢包。

通过配置接口出方向上的带宽限制功能，可以使出接口的实际带宽与运营商所提供的带宽资源相匹配。当流量超过接口可以使用的实际带宽时，NGFW 可以感知拥塞，触发队列调度机制，优先转发关键业务的流量。

此外，也可以配置接口入方向上的实际带宽，当 NGFW 接收其它设备发送的流量时，限制进入接口的流量。

应用场景

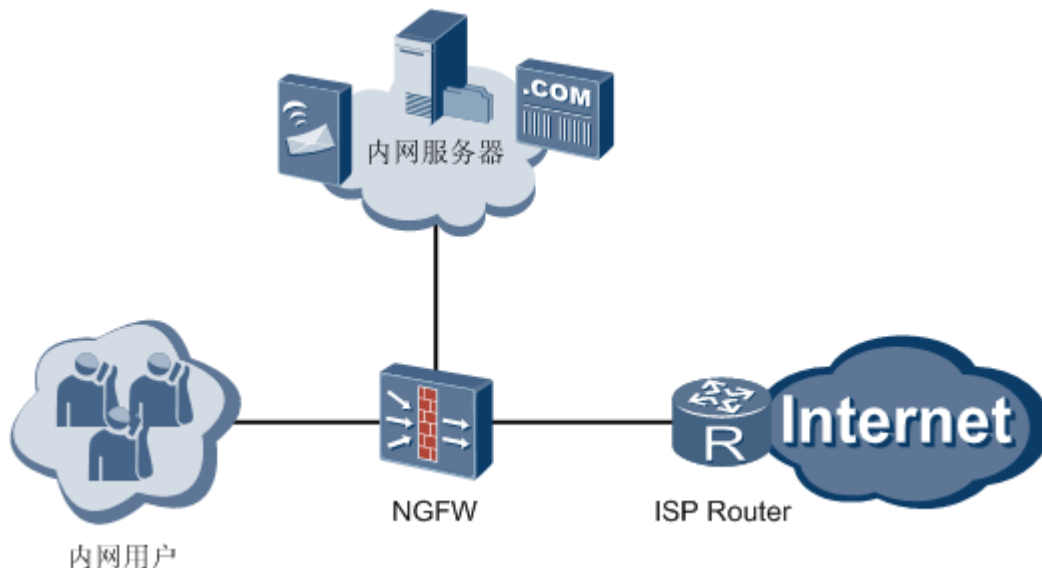
介绍带宽管理的应用场景。

在网络边界安全防护的场景中实施带宽管理

如[图 1](#)所示，NGFW 作为大中型企业的出口网关，部署在网络边界处。在该场景中，对于带宽资源的使用，通常会面临如下问题：

- 内网用户访问 Internet 时，所需的带宽远大于企业从运营商租用的带宽，存在带宽瓶颈。另外，P2P 业务类型的流量消耗了绝大部分的带宽资源，致使关键业务得不到带宽保证。
- Internet 用户访问内网服务器时，大量的针对内网服务器的访问需求导致服务器性能降低，无法正常提供服务。

图 1 在网络边界安全防护的场景中实施带宽管理



针对上述问题，NGFW 提供带宽管理功能，实现如下目的：

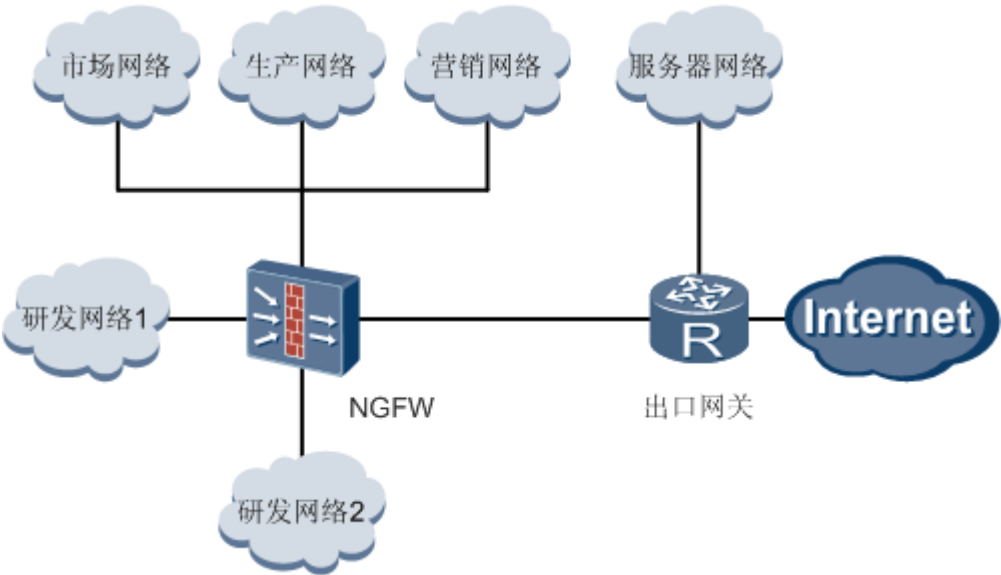
- 对于内网用户访问 Internet 的情况，设置出接口的接口带宽，发生拥塞时优先调度关键业务的流量。同时，对 P2P 业务类型的流量进行限制，避免该类业务占用大量带宽。此外，还可以基于不同用户/部门实施差异化的带宽管理。
- 对于 Internet 用户访问内网服务器的情况，限制 Internet 用户访问内网服务器的连接数，确保服务器正常运行，辅助防范针对内网服务器的 DDoS（Distributed Denial Of Service）攻击。

在内网管控与安全隔离的场景中实施带宽管理

如图 2 所示，NGFW 作为内网管控与安全隔离设备，部署在大中型企业的内部网络中。在该场景中，除了内部网络与 Internet 之间的流量之外，内部网络中的流量也会影响带宽资源的合理使用，主要体现在：

- 内部网络结构复杂，用户数量较多，不同用户/部门之间无限制占用带宽资源，降低网络质量。
- 大量的针对服务器的访问需求导致服务器无法正常工作。

图 2 在内网管控与安全隔离的场景中实施带宽管理



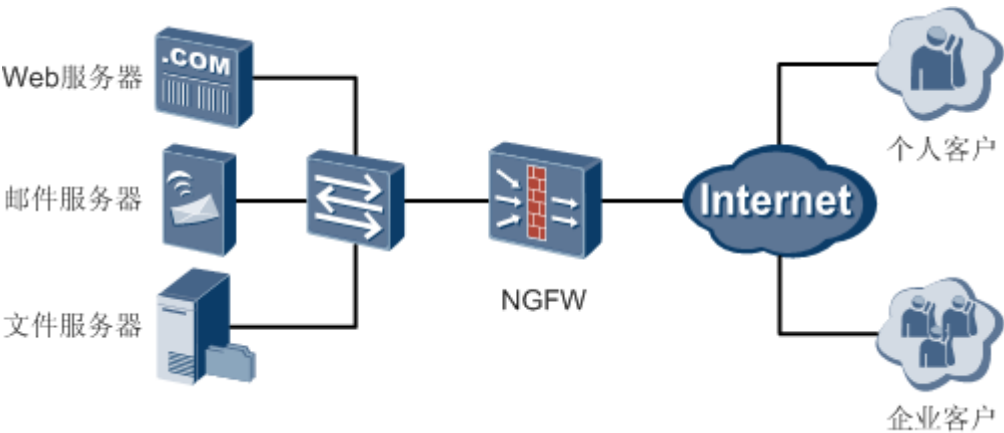
针对上述问题，通过带宽管理可以实现如下目的：

- 基于不同用户/部门配置不同的带宽策略，限制内部网络中不同用户/部门之间的业务流量，避免网络拥塞。
- 限制内部网络用户访问内网服务器的连接数，确保服务器正常运行，同时还可以节省 NGFW 的会话资源。

在数据中心安全防护的场景中实施带宽管理

如图 3 所示，数据中心（Internet Data Center，IDC）为中小型企业或个人客户提供服务器托管、虚拟域名空间等服务。NGFW 作为数据中心边界防护设备，对外部网络访问数据中心的流量进行控制。

图 3 在数据中心安全防护的场景中实施带宽管理



在该场景中，通过带宽管理功能可以实现如下目的：

- 基于 IP 和应用的流量控制，确保服务器稳定运行，避免网络出口拥塞。
- 限制外部用户访问服务器的连接数，保证服务器正常运行，同时还可以辅助防范 DDoS 攻击。

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引用。

前提条件

待实施流量管理的对象所能够使用的具体带宽资源已经确定。

背景信息

带宽通道使用多个参数来对带宽资源进行描述和控制，包括上下行整体的保证带宽和最大带宽、上下行每 IP/每用户的保证带宽和最大带宽、连接数限制和优先级重标记。

由于带宽通道最终会被带宽策略引用，所以带宽通道中的上下行与带宽策略的方向存在对应关系：与带宽策略同向时，定义为上行；与带宽策略反向时，定义为下行。在着手配置带宽通道之前，请根据您的实际情况，明确上下行所代表的真实方向（例如内网用户访问外网，习惯称为上行），再对应到带宽策略的配置（源地址为用户，目的地址为外网资源地址）。

如果配置了接口带宽，带宽通道中定义的带宽资源值要符合整体的接口带宽值的约束，关于接口带宽的配置请参见[接口和接口对](#)。



注意：

为父子策略配置带宽通道时，应遵循如下原则：

- 子策略的最大带宽不能大于父策略的最大带宽。
- 在同一组父子策略中，限流方式只能同时为“分别设置上下行带宽”或者“设置总带宽”，二者不能同时存在，否则会出现带宽控制不准等问题。
- 父策略与子策略不能引用同一个带宽通道。
- 只有子策略才能引用配置了“平均分配”功能的带宽通道，父策略引用的带宽通道不能配置“平均分配”功能。

操作步骤

1. 选择“策略 > 带宽管理 > 带宽通道”。
2. 单击“新建”。
3. 配置带宽通道的名称和限流方式。

参数	说明
名称	输入带宽通道的名称。 输入的名称不能与已经存在的带宽通道名称相同。
限流方式	<ul style="list-style-type: none"> • 分别设置上下行带宽：对于上下行带宽采取独立控制。 • 设置总带宽：基于上行和下行流量之和的整体管控。

4. 配置带宽通道的整体带宽。

参数	说明
引用方式	选择带宽通道被带宽策略引用后的工作方式。 <ul style="list-style-type: none"> • “策略独占”表示每一个引用带宽通道的带宽策略都独自受到该带宽通道的约束。 • “策略共享”表示所有引用带宽通道的带宽策略都共同受到该带宽通道的约束。
上行最大带宽/下行最大带宽	流量可获得的最大带宽资源。 设置该参数可以实现对流量的带宽限制功能。
上行保证带宽/下行保证带宽	流量可获得的最小带宽资源。 设置该参数可以实现对流量的带宽保证功能。
转发优先级	流量使用带宽资源的优先级。 如果流量大于保证带宽、小于最大带宽或者处于保证带宽和最大带宽之间，这部分流量在出接口发送环节将会与其它带宽通道中同类型的流量自由竞争带宽资源。优先级越高，就会更优先获得剩余的带宽资源。

5. 配置带宽通道的每 IP/每用户带宽。

参数	说明
限流对象	选择限流对象。 <ul style="list-style-type: none"> • “每 IP”表示对每一个 IP 地址的流量进行限制。 • “每用户”表示对每一个用户的流量进行限制。
IP 间带宽分配策略	“平均分配”表示基于整体带宽中设置的“保证带宽”，根据在线 IP 个数动态的对每一个 IP 地址的流量进行平均分配。
上行最大带宽/下行最大带宽	每 IP/每用户的流量可获得的最大带宽资源。 该参数的值不能大于整体带宽中设置的“最大带宽”。
上行保证带宽/下行保证带宽	每 IP/每用户的流量可获得的最小带宽资源。

参数	说明
	每 IP/每用户的保证带宽之和，不能大于整体保证带宽。

6. 配置带宽通道的连接数限制。

参数	说明
整体并发连接数	带宽通道整体的最大并发连接数。
限制方式	选择连接数的限制方式。 <ul style="list-style-type: none"> “每 IP”表示对每一个源 IP 地址发起的连接数进行限制。 “每用户”表示对每一个用户发起的连接数进行限制。
每 IP/每用户连接数	每 IP/每用户的最大并发连接数。 该参数的值不能大于设置的“整体并发连接数”。

7. 配置带宽通道的优先级重标记。

参数	说明
重标记 DSCP 优先级	修改报文的 DSCP 优先级。

8. 单击“确定”。

配置带宽策略

带宽策略定义了需要进行带宽管理的对象，并通过引用带宽通道来进行相应的控制。

前提条件

- 待实施流量管理的对象已经确定，可以通过源地址/地区、目的地址/地区、源安全区域/入接口、目的安全区域/出接口、服务、用户、应用、时间段和报文 DSCP 优先级信息定义该流量的特征。
- 需要引用的带宽通道已经配置完成。

背景信息

- 对于多条同级策略，NGFW 按照界面上的排列顺序从上到下依次匹配，只要匹配了一条策略的所有条件，则执行带宽通道的动作，不再继续匹配剩下的规则。
- 对于父子策略，流量先匹配父策略，再去匹配子策略，直到匹配到最后一级可以匹配到的子策略为止。
- 如果所有规则都没有匹配到，则按照缺省的带宽策略进行处理。

NGFW 上存在一条缺省的带宽策略，所有匹配条件均为任意（any），动作为不限流。



说明：

当使用 MAC 地址作为策略匹配条件时，需注意：

- 如果 NGFW 与内网之间直连或通过二层交换机相连，可以直接以 MAC 地址作为匹配条件。
- 如果 NGFW 与内网之间通过三层网络设备相连，首先需要配置 NGFW 的跨三层 MAC 识别功能，再以 MAC 地址作为匹配条件。有关跨三层 MAC 识别功能的介绍，请参见[跨三层 MAC 识别](#)。

操作步骤

1. 选择“策略 > 带宽管理 > 带宽策略”。
2. 单击“新建”。
3. 配置带宽策略规则的名称、描述和所属父策略。






参数	说明
名称	输入带宽策略规则的名称。 输入的名称不能与已经存在的带宽策略名称相同。
描述	输入带宽策略规则的描述信息。 合理填写描述信息有助于管理员正确理解带宽策略规则的功能，便于查找和维护。
所属父策略	输入带宽策略规则所属的父策略。 父策略必须是已经存在的带宽策略规则。


4. 配置带宽策略规则的匹配条件。

各个匹配条件之间是“与”的关系，报文的属性与各个条件必须全部匹配，才认为该报文匹配这条规则。而同一个匹配条件中的多个信息之间是“或”的关系，报文的属性只要匹配了其中的一个信息，就认为报文的属性匹配了这个条件。

配置多条带宽策略规则时，请先配置条件精确的规则，再配置条件宽泛的规则，即保证条件精确的规则位于条件宽泛的规则之上。

参数	说明
源类型	选择匹配条件中源信息的类型，可以是“源安全区域”或者“入接口”。
源安全区域	源安全区域是指发出流量的安全区域。 该参数只在“源类型”为“源安全区域”时需要配置。
入接口	入接口是指流量进入的接口。 该参数只在“源类型”为“入接口”时需要配置。

参数	说明
目的类型	选择匹配条件中目的信息的类型，可以是“目的安全区域”或者“出接口”。
目的安全区域	目的安全区域是指接收流量的安全区域。 该参数只在“目的类型”为“目的安全区域”时需要配置。
出接口	出接口是指发出流量的接口。 该参数只在“目的类型”为“出接口”时需要配置。
源地址/地区	<p>输入或者选择流量的源地址。</p> <ul style="list-style-type: none"> 地址和地址组：管理员可以指定一个单独的 IP/MAC 地址或者一个连续的 IP 网段，还可以通过地址组来划定不连续的或者是不方便通过掩码指定的连续的 IP 地址范围、MAC 地址集合。具体请参见地址和地址组。 域名组：管理员可以通过指定域名组，将某些域名对应的 IP 地址作为策略的匹配条件。具体参见域名组。 地区和地区组：管理员可以通过指定地区或地址地区组，将某些地区的 IP 地址作为策略的匹配条件。具体参见地区和地区组。 <p>配置时可以手动输入 IP/MAC 地址或者从下拉列表中选择已有的地址对象。下拉列表中的地址对象包含如下几类：</p> <ul style="list-style-type: none">  图标代表地址。  图标代表地址组。  图标代表域名组。  或国旗图标代表地区，先显示自定义地区再显示预定义地区。地区相当于以地区为单位的 IP 地址集合。  图标代表地区组。 <p>说明： 当使用 MAC 地址作为策略匹配条件时，需注意：</p> <ul style="list-style-type: none"> 如果 NGFW 与内网之间直连或通过二层交换机相连，可以直接以 MAC 地址作为匹配条件。 如果 NGFW 与内网之间通过三层网络设备相连，首先需要配置 NGFW 的跨三层 MAC 识别功能，再以 MAC 地址作为匹配条件。 <p>说明： 若限流方式为每 IP，当需要限流的 PC 上存在多个 IP 地址，且从这些 IP 地址访问目的网络的流量均经过 NGFW 时，需要将所有 IP 地址配置到带宽策略中，否则可能导致限流不准确。 例如，PC 同时通过 10.3.1.1 和 10.3.2.1 两个 IP 地址访问外网，要求限制 PC 的下行最大带宽为 1Mbps，则需要在带宽策略的源地址中同时配置 10.3.1.1 和 10.3.2.1 作为匹配条件，并引用整体下行带宽为 1Mbps 的带宽通道。</p>
目的地址/地区	<p>输入或者选择流量的目的地址。</p> <p>下拉列表中的地址对象类型与源地址/地区相同。</p>
用户	用户是指流量的所有者，表示“谁”发出的流量。
应用	<p>应用是指流量的应用类型，表示某个具体的应用程序产生的流量。</p> <p>窍门：</p>

参数	说明
	设备支持模糊搜索功能，能够帮助管理员快速搜索并添加需要的应用。具体操作如下： k. 单击“多选”。 l. 在搜索框中输入全部或部分应用名称。 m. 单击  ，在下拉列表中会显示搜索到的应用名称。 n. 选中需要的应用名称，添加此应用。
服务	服务是指流量的协议类型，表示某种协议产生的流量。
时间段	时间段是指带宽策略规则的生效时间。
报文优先级	报文优先级是指流量中报文的 DSCP 优先级。

5. 配置带宽策略规则的动作，并引用带宽通道。

参数	说明
动作	选择带宽策略规则的动作，可以是“限流”或者“不限流”。
带宽通道	选择带宽策略规则所引用的带宽通道。 该参数只在“动作”为“限流”时需要配置。

6. 单击“确定”。

后续处理

带宽策略配置完成后，可以在“监控 > 报表 > 流量报表”中查看流量趋势，检查带宽管理是否生效。

如果带宽管理功能没有生效，请根据本节内容调整带宽策略的参数，或者根据[带宽通道](#)中的内容，调整带宽通道的参数。

举例：在网络边界安全防护的场景中实施带宽管理

介绍了 NGFW 作为安全网关部署在企业的网络边界时，如何实施带宽管理。

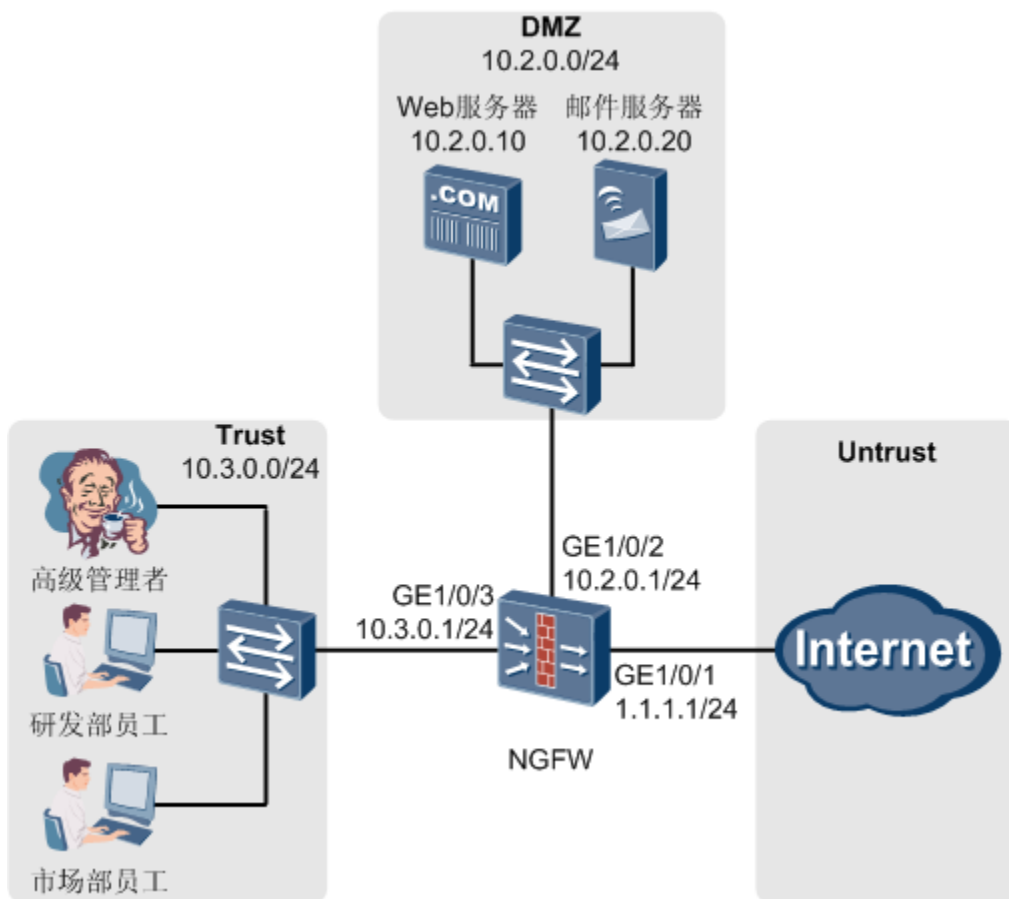
组网需求

如[图 1](#)所示，某企业将 NGFW 作为出口网关部署在网络边界处，并从运营商租用了上下行均为 100M 带宽的专线，使内部网络中的用户可以访问 Internet。

该网络环境中，内部用户访问 Internet 的流量以及 Internet 上的用户访问内部服务器的流量，都将占用 100M 的带宽资源，容易产生拥塞。为此，网络管理员希望利用 NGFW 的带宽管理功能，实现如下需求：

- 限制内部网络用户与 Internet 之间的 P2P 类型的业务流量最大不能超过 20M，避免占用大量带宽资源。
- 高级管理者访问 Internet 时可以获得 20M 的保证带宽，但最大带宽不能超过 30M。
- 研发部下设产品组 1 和产品组 2 两个项目组，研发部访问 Internet 时可以使用的最大带宽不能超过 20M，其中产品组 1 和产品组 2 访问 Internet 时可以使用的最大带宽均不能超过 15M。
- 市场部访问 Internet 时可以使用的最大带宽不能超过 30M，其中每一个员工可以使用的最大带宽不能超过 10M。
- 限制 Internet 用户访问 Web 服务器以及访问邮件服务器的并发连接数不能超过 3000，保证服务器正常运行。

图 1 在网络边界安全防护的场景中实施带宽管理组网图



配置思路

1. 配置接口 GigabitEthernet 1/0/1 的接口带宽，与运营商提供的带宽资源相匹配，当发生拥塞时，能够优先处理关键业务的流量。
2. 对于网络中的 P2P 业务，定义其能够使用的最大带宽，使用带宽策略进行流量限制。
3. 对于高级管理者，定义其能够使用的保证带宽和最大带宽，使用带宽策略实现带宽管理。

4. 对于研发部员工，使用父子策略来限制研发部以及产品组 1 和产品组 2 能够使用的最大带宽资源。
5. 对于市场部员工，定义其能够使用的整体最大带宽，并基于每用户来限制单个用户的带宽资源。
6. 配置连接数限制功能，限制目的地址为 Web 服务器和邮件服务器的会话数量。



说明：

假设接口的 IP 地址、安全区域、路由、安全策略、用户认证以及 NAT 策略都已经配置完成，在此基础上，本举例只介绍配置带宽管理的内容。

操作步骤

1. 配置接口带宽。
 - a. 选择“网络 > 接口”。
 - b. 单击 GE1/0/1 对应的 ，按如下参数配置。

入方向带宽	100Mbps
出方向带宽	100Mbps

- c. 单击“确定”。
2. 针对 P2P 业务进行带宽管理。
 - a. 选择“策略 > 带宽管理 > 带宽通道”。
 - b. 单击“新建”，按如下参数配置。

名称	profile_p2p
下行最大带宽	20Mbps

- c. 单击“确定”。
- d. 选择“策略 > 带宽管理 > 带宽策略”。
 - e. 单击“新建”，按如下参数配置。



说明：

此处仅给出了 BT、eDonkey/eMule 两种 P2P 业务作为例子，具体配置时请根据实际需求指定 P2P 业务。

名称	policy_p2p
源类型	源安全区域

源安全区域	trust
目的类型	目的安全区域
目的安全区域	untrust
应用	BT,eDonkey/eMule
动作	限流
带宽通道	profile_p2p

f. 单击“确定”。

3. 针对高级管理者进行带宽管理。

a. 选择“策略 > 带宽管理 > 带宽通道”。

b. 单击“新建”，按如下参数配置。

名称	profile_manager
下行最大带宽	30Mbps
下行保证带宽	20Mbps

c. 单击“确定”。

d. 选择“策略 > 带宽管理 > 带宽策略”。

e. 单击“新建”，按如下参数配置。

名称	policy_manager
源类型	源安全区域
源安全区域	trust
目的类型	目的安全区域
目的安全区域	untrust
用户	/default/manager
动作	限流
带宽通道	profile_manager

f. 单击“确定”。

4. 针对研发部进行带宽管理。

a. 选择“策略 > 带宽管理 > 带宽通道”。

b. 单击“新建”，按如下参数配置。

名称	profile_research
----	------------------

下行最大带宽	20Mbps
--------	--------

- c. 单击“确定”。
- d. 单击“新建”，按如下参数配置。

名称	profile_research_product1
下行最大带宽	15Mbps

- e. 单击“确定”。
- f. 单击“新建”，按如下参数配置。

名称	profile_research_product2
下行最大带宽	15Mbps

- g. 单击“确定”。
- h. 选择“策略 > 带宽管理 > 带宽策略”。
- i. 单击“新建”，按如下参数配置。

名称	policy_research
源类型	源安全区域
源安全区域	trust
目的类型	目的安全区域
目的安全区域	untrust
用户	/default/research
动作	限流
带宽通道	profile_research

- j. 单击“确定”。
- k. 单击“新建”，按如下参数配置。

名称	policy_research_product1
所属父策略	policy_research
源类型	源安全区域
源安全区域	trust
目的类型	目的安全区域
目的安全区域	untrust
用户	/default/research/research_product1
动作	限流

带宽通道	profile_research_product1
------	---------------------------

- l. 单击“确定”。
- m. 单击“新建”，按如下参数配置。

名称	policy_research_product2
所属父策略	policy_research
源类型	源安全区域
源安全区域	trust
目的类型	目的安全区域
目的安全区域	untrust
用户	/default/research/research_product2
动作	限流
带宽通道	profile_research_product2

- n. 单击“确定”。

5. 针对市场部进行带宽管理。

- a. 选择“策略 > 带宽管理 > 带宽通道”。
- b. 单击“新建”，按如下参数配置。

名称	profile_marketing
下行最大带宽	30Mbps
每 IP/每用户限流	
限流对象	每用户
下行最大带宽	10Mbps

- c. 单击“确定”。
- d. 选择“策略 > 带宽管理 > 带宽策略”。
- e. 单击“新建”，按如下参数配置。

名称	policy_marketing
源类型	源安全区域
源安全区域	trust
目的类型	目的安全区域
目的安全区域	untrust

用户	/default/marketing
动作	限流
带宽通道	profile_marketing

f. 单击“确定”。

6. 针对内网服务器的并发连接数进行限制。

a. 选择“策略 > 带宽管理 > 带宽通道”。

b. 单击“新建”，按如下参数配置。

名称	profile_connection
连接数限制	
整体并发连接数	3000

c. 单击“确定”。

d. 选择“策略 > 带宽管理 > 带宽策略”。

e. 单击“新建”，按如下参数配置。

名称	policy_connection_web
源类型	源安全区域
源安全区域	untrust
目的类型	目的安全区域
目的安全区域	dmz
目的地址/地区	10.2.0.10/32
动作	限流
带宽通道	profile_connection

f. 单击“确定”。

g. 单击“新建”，按如下参数配置。

名称	policy_connection_mail
源类型	源安全区域
源安全区域	untrust
目的类型	目的安全区域
目的安全区域	dmz
目的地址/地区	10.2.0.20/32

动作	限流
带宽通道	profile_connection

h. 单击“确定”。

结果验证

- 对于 P2P 业务的流量控制，管理员可以使用如下方法验证配置是否生效：
 - 在内部网络中使用 BT 或 eDonkey/eMule 工具从 Internet 下载文件，查看 BT 或 eDonkey/eMule 工具的下载速率最大不超过 20M。
 - 在 NGFW 上选择“监控 > 报表 > 流量报表”，按“应用”的维度来查看 P2P 业务流量的报表，P2P 业务流量不超过 20M。
- 对于不同用户的流量控制，管理员可以使用如下方法验证配置是否生效：
 - 在内部网络中依次使用高级管理者、研发部员工和市场部员工的账号登录，使用文件下载工具（如 FTP）从 Internet 下载文件，然后通过查看文件下载工具的下载速率来验证配置是否生效。
 - 在 NGFW 上选择“监控 > 报表 > 流量报表”，按“用户”的维度来查看不同用户流量的报表，验证配置是否生效。
 - 对于高级管理者，从 Internet 下载文件时可以获得 20M 的保证带宽，最大带宽不超过 30M。
 - 对于研发部员工，从 Internet 下载文件时可获得的最大带宽不超过 15M。
 - 对于市场部员工，从 Internet 下载文件时可获得的最大带宽不超过 10M。
- 对于服务器的并发连接数限制，管理员可以使用如下方法验证配置是否生效：
 - 模拟用户访问内部网络的 Web 服务器（10.2.0.10）以及邮件服务器（10.2.0.20），用户数量超过 3000 个。
 - 在 NGFW 上选择“监控 > 报表 > 流量报表”，按“目的地址”的维度来查看会话数，验证针对服务器（10.2.0.10 和 10.2.0.20）的并发连接数限制是否生效。

配置脚本

```
#
sysname NGFW
#
interface GigabitEthernet1/0/1
ip address 1.1.1.1 255.255.255.0
```



```
bandwidth ingress 100000
bandwidth egress 100000
#
interface GigabitEthernet1/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/3
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/1
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet1/0/2
#
traffic-policy
 profile profile_p2p
  bandwidth downstream maximum-bandwidth 20000
 profile profile_manager
  bandwidth downstream guaranteed-bandwidth 20000
  bandwidth downstream maximum-bandwidth 30000
 profile profile_research
  bandwidth downstream maximum-bandwidth 20000
 profile profile_research_product1
  bandwidth downstream maximum-bandwidth 15000
 profile profile_research_product2
  bandwidth downstream maximum-bandwidth 15000
 profile profile_marketing
  bandwidth downstream maximum-bandwidth 30000
  bandwidth ip-car downstream maximum-bandwidth per-user 10000
 profile profile_connection
  bandwidth connection-limit per-rule 3000
 rule name policy_p2p
  source-zone trust
  destination-zone untrust
  application app BT
```

```

application app eDonkey/eMule
action qos profile profile_p2p
rule name policy_manager
    source-zone trust
    destination-zone untrust
    user /default/manager
    action qos profile profile_manager
rule name profile_research
    source-zone trust
    destination-zone untrust
    user /default/research
    action qos profile profile_research
rule name policy_research_product1 parent profile_research
    source-zone trust
    destination-zone untrust
    user /default/research/research_product1
    action qos profile profile_research_product1
rule name policy_research_product2 parent profile_research
    source-zone trust
    destination-zone untrust
    user /default/research/research_product2
    action qos profile profile_research_product2
rule name policy_marketing
    source-zone trust
    destination-zone untrust
    user /default/marketing
    action qos profile profile_marketing
rule name policy_connection_web
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.10 32
    action qos profile profile_connection
rule name policy_connection_mail
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.20 32
    action qos profile profile_connection
#
return

```

HCIE-Security 模拟面试问题及面试建议

1. 带宽通道和带宽策略之间有什么关系？