

HCIE-Security 备考指南

策略路由



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 策略路由需要掌握的知识点.....	1
策略路由简介.....	1
策略路由原理描述.....	2
配置策略路由-Web.....	4
举例：基于源地址的策略路由.....	11
HCIE-Security 模拟面试问题及面试建议.....	15

HCIE-Security 策略路由需要掌握的知识点

■ 掌握 PBR 的配置

策略路由简介

介绍策略路由的定义和应用场景。

定义和目的

NGFW 转发数据报文时，会查找路由表，并根据目的地址来进行报文的转发。在这种机制下，只能根据报文的地址为用户提供转发服务，无法提供有差别的服务。

策略路由是在路由表已经产生的情况下，不按照现有的路由表进行转发，而是根据用户制定的策略进行路由选择的机制，从更多的维度（入接口、源/目的安全区域、源/目的 IP 地址、用户、服务、应用）来决定报文如何转发，增加了在报文转发控制上的灵活度。策略路由并没有替代路由表机制，而是优先于路由表生效，为某些特殊业务指定转发方向。

应用场景

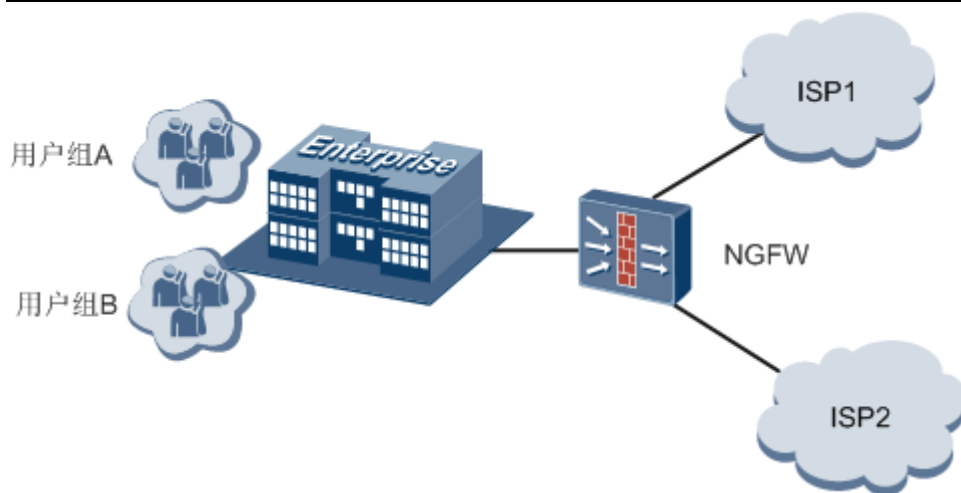
策略路由通常应用于多出口组网中，以图 1 为例，NGFW 作为出口网关，存在两个网络出口：

- ISP1：上网速度快，但付费较高。
- ISP2：价格低廉，但网速比较慢。

通过策略路由，可以实现下述功能，用户可以根据需要进行选配。

- 基于用户的选路：指定用户/用户组只能通过指定的链路访问互联网。例如，用户组 A 权限高，享受快速网络，可以通过链路 ISP1 访问互联网，用户组 B 权限低，通过链路 ISP2 访问互联网。
- 基于应用、协议类型的选路。例如，配置语音与视频等应用走带宽高线路，数据应用走带宽小的线路。

图 1 策略路由在多出口组网的应用



策略路由原理描述

介绍策略路由的实现原理。

策略路由组成

一条策略路由规则包括匹配条件和动作两部分内容。

匹配条件

匹配条件可以将要做策略路由的流量区分开来，NGFW 支持下述几种类型的匹配条件：

- 源安全区域：基于报文的源安全区域进行流量识别。
- 入接口：基于报文的接收接口来进行流量识别。
- IP 地址/MAC 地址：基于报文的源 IP/源 MAC 或目的 IP/目的 MAC 进行流量识别。
- 服务类型：基于报文所属的服务类型进行流量识别。
- 应用类型：基于报文所属的应用类型进行流量识别。
- 用户：在对应的用户通过设备的身份认证后，基于报文所属的用户进行流量识别。

在一个策略路由规则中，可以包含多个匹配条件，各匹配条件之间是“与”的关系，报文必须同时满足所有匹配条件，才可以执行后续定义的转发动作。服务类型、应用类型、用户作为匹配条件时，可以同时指定多个服务/服务组、应用/应用组、用户/用户组，只要与其中一个相同，就算满足该匹配条件。

动作

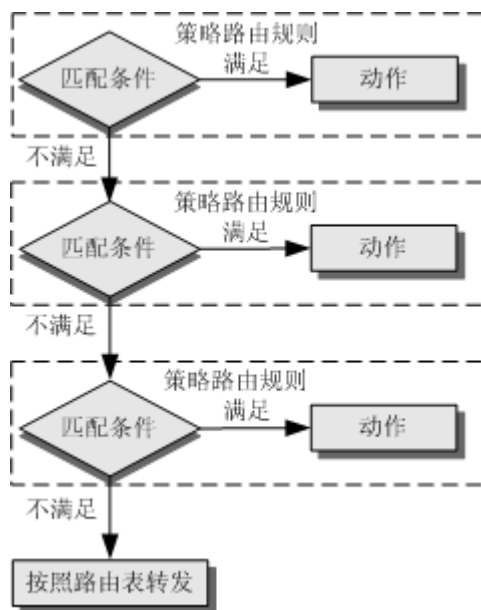
NGFW 可以对符合匹配条件的流量采取下述动作：

- 实施策略路由
 - 把报文发送到指定的下一跳设备。
 - 从指定出接口发送报文。
 - 利用智能选路功能，从多个出接口中选择一个出接口发送报文。
 - 把报文发送到指定的虚拟系统。
- 不做策略路由，按照现有的路由表进行转发。

策略路由规则匹配过程

当 NGFW 配置了多条策略路由规则时，NGFW 会按照匹配顺序，先寻找第一条规则，如果满足第一条策略路由规则的匹配条件，则按照指定动作处理报文。如果不满足第一条规则的匹配条件，则会寻找下一条策略路由规则。如果所有的策略路由规则的匹配条件都无法满足，报文按照路由表进行转发。

图 1 策略路由规则匹配过程



当策略路由为单出口时，如果动作里指定的下一跳或出接口不可达，报文会被 NGFW 直接丢弃。为了提高可靠性，可以配置 NGFW 监测下一跳或者目的 IP 的可达性，即使下一跳或目的 IP 不可达，也可以继续查找路由表，避免报文被直接丢弃。

策略路由规则匹配顺序

NGFW 可以配置多条策略路由规则，在图 2 所示的策略路由列表中，排在列表最上面的策略路由规则“abc_1”先执行，策略路由规则“abc_2”后执行。

图 2 策略路由规则匹配顺序

策略路由列表												
<div>新建 删除 复制 移动 插入 列定制</div> <div>请输入策略名称 查询 高级查询</div>												
名称	源安全区域/接口	源地址	目的地址	用户	服务	应用	时间段	动作	虚拟系统	出接口	下一跳	监控状态
<input type="checkbox"/> abc_1	GE1/0/2	any	any	any	any	any	any	转发		GE1/0/3		<input checked="" type="checkbox"/>
<input type="checkbox"/> abc_2	GE1/0/3	any	any	any	any	any	any	转发		GE1/0/2		<input checked="" type="checkbox"/>
<input type="checkbox"/> default	any	any	any	any	any	any	any	不做策略...				<input checked="" type="checkbox"/>

窍门：

当 NGFW 配置了多条策略路由规则时，将按照规则在界面上的排列顺序从上到下依次匹配，只要匹配了一条规则的所有条件，则按照动作与选项进行处理，不再继续匹配剩下的规则。所以在配置时，建议将条件更精确的规则配置在前面，条件更宽泛的规则配置在后面，这样就不会因为前面规则的条件包含了后面规则的条件，而导致后面的规则无法被匹配了，从而提高匹配的精确度。

配置策略路由-Web

介绍如何通过 Web 配置策略路由。

前提条件

- 配置[用户或用户组](#)。
- 配置[服务或服务组](#)。
- 配置[应用或应用组](#)。

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。


操作步骤

1. 选择“网络 > 路由 > 智能选路”。
2. 选择进入“策略路由”页签，单击“新建”。
3. 配置策略路由规则的名称和描述。

参数	描述
名称	输入策略路由规则的名称。名称必须是唯一的。
描述	输入策略路由规则的描述信息。合理填写描述信息有助于管理员正确理解策略路由规则的功能，使策略路由规则变得方便选择、查找和维护。

4. 配置策略路由规则的匹配条件。

参数	描述
类型	配置基于报文来源的匹配条件，有两个选项，二者只能选择其一： <ul style="list-style-type: none"> • 入接口：基于报文的接收接口来进行流量识别。 • 源安全区域：基于报文的源安全区域进行流量识别。
入接口	将报文的入接口设置为策略路由的匹配条件。 窍门： 除了物理口，NGFW 还支持将 VLAN 接口、以太网子接口、Eth-Trunk 接口、Loopback 接口这四种类型的逻辑接口配置为入接口： <ul style="list-style-type: none"> • 将 VLAN 接口配置为入接口，可以对指定 VLAN 的流量实施策略路由。 • 将以太网子接口配置为入接口时，可以对指定子接口的流量实施策略路由。 • 将 Eth-Trunk 接口配置为入接口时，可以对来自指定 Eth-Trunk 链路的流量实施策略路由。
源安全区域	将源安全区域设置为策略路由的匹配条件。
源地址	将报文的源 IP 地址/MAC 地址设置为策略路由的匹配条件。
目的地址	将报文的目的 IP 地址/MAC 地址设置为策略路由的匹配条件。
用户	将报文所属的用户或用户组设置为策略路由的匹配条件。
服务	将报文所属的服务类型设置为策略路由的匹配条件。 有关“服务”的详细解释请参考 服务和应用组 。
应用	将报文所属的应用类型设置为策略路由的匹配条件。 有关“应用”的详细解释请参考 应用和应用组 。 窍门： 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：

参数	描述
	<p>f. 单击“多选”。</p> <p>g. 在搜索框中输入全部或部分应用名称。</p> <p>h. 单击，在下拉列表中会显示搜索到的应用名称。</p> <p>i. 选中需要的应用名称，添加此应用。</p>
时间段	配置策略路由的生效时间。

5. 配置策略路由规则的动作。

参数	描述
动作	<p>对满足匹配条件的报文，采取何种转发动作，有两种选项：</p> <ul style="list-style-type: none"> 转发(PBR)：报文满足匹配条件，按照策略路由转发。 转发其他虚拟系统：报文满足匹配条件，按照策略路由将流量转发至其他虚拟系统。 不做策略路由(NO PBR)：报文满足匹配条件，按照普通路由表转发。 <p>窍门：</p> <p>“不做策略路由(NO PBR)”动作主要用于满足一些特殊需求。例如需要对 10.1.1.0/24 网段内除 10.1.1.2 以外的所有主机进行策略路由，可以利用规则的匹配优先级，先配置一条对 10.1.1.2 主机不做策略路由的规则，再配置一条对 10.1.1.0/24 网段做策略路由的规则。</p>
出接口类型	<p>策略路由支持配置单个出接口或多个出接口。</p> <ul style="list-style-type: none"> 单出口 <p>如果下一跳或者出接口不可达，报文将被 NGFW 直接丢弃；为了提高可靠性，可以通过监控功能监测下一跳或者目的 IP 的可达性，即使下一跳或目的 IP 不可达，也可以继续查找路由表，避免报文被直接丢弃。</p> 多出口 <p>当策略路由有多个出接口时，需要利用策略路由智能选路功能选择最佳的出接口。智能选路是指到达目的网络有多条链路可选时，NGFW 可以根据管理员设置的链路带宽、权重、优先级或者自动探测到的链路质量动态地选择出接口，实现链路资源的合理利用和用户体验的提升。</p> <p>说明：</p> <p>策略路由智能选路和全局智能选路统称为智能选路，前者解决的是流量命中策略路由时，如果有多个出接口如何进行选路的问题；后者解决的是流量命中缺省路由时，如果有多条缺省路由如何进行选路的问题。智能选路功能的原理和相关技术请参考智能选路，此处不进行详细介绍。</p>

- 单出口配置

参数	描述
出接口	选择按照策略路由转发时，设置报文的发送接口。 说明： <ul style="list-style-type: none"> 可以同时配置出接口和下一跳，但是出接口和下一跳二者必须配置一个。 当配置的“出接口”为非点到点类型网络接口（例如以太网接口）时，由于同一出接口可能连接到多个网络设备，所以建议同时配置“下一跳”以保证路由的正确性。
下一跳	选择按照策略路由转发时，设置报文发送的下一跳。

- 配置单出口后，可以通过监控功能监测到下一跳或某个目的 IP 的可达性，并根据链路状态来决定是否按照策略路由转发报文。

- 单击“监控”对应的“启用”复选框。
- “监控 IP 地址/域名”文本框中输入要监控的 IP 地址或域名。

“监控 IP 地址/域名”输入直连下一跳或者非直连下一跳的 IP 地址后，NGFW 会实时监测到目的 IP 的可达性，如果发现目的 IP 不可达，策略路由失效，报文按照路由表来转发。

当启用“监控”功能时，由于可能通过多个出接口到达同一“监控 IP 地址/域名”，为了保证监控的有效性，建议在配置策略路由时同时配置“出接口”，监控指定“出接口”到指定地址的路由连通性。

- 多出口配置



说明：

此处仅介绍不同智能选路方式下的相关配置，接口下的相关配置请参考[配置全局选路策略](#)。

在“智能选路方式”下拉菜单中选择不同的选路方式：

- “智能选路方式”为“根据链路带宽负载分担”时，如[图 1](#)所示，具体参数解释请参见[表 1](#)。

图 1 配置根据链路带宽负载分担

智能选路方式 根据链路带宽负载分担

出接口列表

+ 新建

✖ 删除

<input type="checkbox"/> 链路接口/运营商/接口组	过载保护阈值	
	入方向	出方向
<input type="checkbox"/> GE1/0/0	95	95
<input type="checkbox"/> GE1/0/1	95	95

共 2 条

表 1 配置根据链路带宽负载分担参数解释

参数	说明
链路接口/运营商/接口组	参与智能选路的成员接口。 单击“新建”后，可以在下拉菜单中选择成员接口。单个出接口、普通接口组、ISP 接口组都可以作为成员接口，接口组实际上就是一个或多个智能选路成员接口的集合。接口组不能嵌套，即多个接口组不能组成一个新的接口组。
过载保护阈值	接口链路的带宽利用率。 此处不可配置，在接口下配置。
入方向	入方向的过载保护阈值。 此处不可配置，在接口下配置。
出方向	出方向的过载保护阈值。 此处不可配置，在接口下配置。

- “智能选路方式”为“根据链路质量负载分担”时，如[图 2](#)所示，具体参数解释请参见[表 2](#)。

图 2 配置根据链路质量负载分担

智能选路方式 根据链路质量负载分担

链路质量参数 ☒ 丢包率 ☒ 时延 ☒ 时延抖动

永久探测 ☐ 启用

出接口列表

+ 新建

✖ 删除

<input type="checkbox"/> 链路接口/运营商/接口组	过载保护阈值	
	入方向	出方向
<input type="checkbox"/> GE1/0/1	95	95
<input type="checkbox"/> GE1/0/0	95	95

共 2 条

表 2 配置根据链路质量负载分担参数解释

参数	说明
链路质量参数	<p>当选路方式为根据链路质量负载分担时，管理员可以选择一个或多个链路质量参数来衡量链路的质量。NGFW 支持以下三个链路质量参数：</p> <ul style="list-style-type: none"> 丢包率：丢包率是缺省的链路质量参数。NGFW 发送若干个探测报文后，将统计丢包的个数，丢包率等于回应报文个数除以探测报文个数。丢包率是最重要的参数，对链路质量的判定起决定性作用。 时延：回应报文的接收时间减去探测报文的发送时间即为时延，NGFW 发送 N 个探测报文后，将分别计算每次探测的时延，并取 N 次探测的平均值作为最终结果。 时延抖动：相邻两次探测的时延之差取绝对值即为时延抖动。NGFW 发送 N 个探测报文后，将分别计算相邻两次探测的时延之差并取绝对值，然后取所有时延抖动的平均值作为最终结果。
永久探测	开启永久探测后，NGFW 会定时探测链路的质量，并刷新链路质量探测表。
链路接口/运营商/接口组	<p>参与智能选路的成员接口。</p> <p>单击“新建”后，可以在下拉菜单中选择成员接口。单个出接口、普通接口组、ISP 接口组都可以作为成员接口，接口组实际上就是一个或多个智能选路成员接口的集合。接口组不能嵌套，即多个接口组不能组成一个新的接口组。</p>
过载保护阈值	<p>接口链路的带宽利用率。</p> <p>此处不可配置，在接口下配置。</p>
入方向	<p>入方向的过载保护阈值。</p> <p>此处不可配置，在接口下配置。</p>
出方向	<p>出方向的过载保护阈值。</p> <p>此处不可配置，在接口下配置。</p>

- “智能选路方式”为“根据链路权重负载分担”时，如[图 3](#)所示，具体参数解释请参见[表 3](#)。

图 3 配置根据链路权重负载分担

智能选路方式: 根据链路权重负载分担

出接口列表

+ 新建 - 删除

链路接口/运营商/接口组	过载保护阈值		权重
	入方向	出方向	
<input type="checkbox"/> GE1/0/1	95	95	2
<input type="checkbox"/> GE1/0/0	95	95	1

共 2 条

表 3 配置根据链路权重负载分担参数解释

参数	说明
链路接口/运营商/接口组	参与智能选路的成员接口。 单击“新建”后，可以在下拉菜单中选择成员接口。单个出接口、普通接口组、ISP 接口组都可以作为成员接口，接口组实际上就是一个或多个智能选路成员接口的集合。接口组不能嵌套，即多个接口组不能组成一个新的接口组。
过载保护阈值	接口链路的带宽利用率。 此处不可配置，在接口下配置。
入方向	入方向的过载保护阈值。 此处不可配置，在接口下配置。
出方向	出方向的过载保护阈值。 此处不可配置，在接口下配置。
权重	成员接口的权重值。 NGFW 进行智能选路时，将按照权重值的比例分配流量，所以权重大的链路转发较多的流量，权重小的链路转发较少的流量。

- “智能选路方式”为“根据链路优先级主备备份”时，如[图 4](#)所示，具体参数解释请参见[表 4](#)。

图 4 配置根据链路优先级主备备份

智能选路方式: 根据链路优先级主备备份

备份接口自动关闭功能: ☐ 启用

出接口列表

+ 新建 - 删除

链路接口/运营商/接口组	过载保护阈值		优先级
	入方向	出方向	
<input type="checkbox"/> GE1/0/1	95	95	2
<input checked="" type="checkbox"/> GE1/0/0	95	95	1

共 2 条

表 4 配置根据链路优先级主备备份参数解释

参数	说明
备份接口自动关闭功能	启用此功能后，所有备份接口的状态变为 DOWN ，只有当主接口过载（需要配置接口过载保护）或状态为 DOWN 时，优先级最高的备份接口状态才变为 UP ，其他备份接口的状态仍为 DOWN 。当主接口和优先级最高的备份接口均过载或状态均为 DOWN 时，优先级第二高的备份接口状态才变为 UP ，以此类推。
链路接口/运营商/接口组	参与智能选路的成员接口。

表 4 配置根据链路优先级主备备份参数解释

参数	说明
	单击“新建”后，可以在下拉菜单中选择成员接口。单个出接口、普通接口组、ISP 接口组都可以作为成员接口，接口组实际上就是一个或多个智能选路成员接口的集合。接口组不能嵌套，即多个接口组不能组成一个新的接口组。
过载保护阈值	接口链路的带宽利用率。 此处不可配置，在接口下配置。
入方向	入方向的过载保护阈值。 此处不可配置，在接口下配置。
出方向	出方向的过载保护阈值。 此处不可配置，在接口下配置。
优先级	成员接口的优先级。 数值越大，优先级越高。

后续处理

当策略路由有多个出接口时，如果“智能选路方式”设置为“根据链路质量负载分担”，则可以通过链路质量探测表查看各链路的质量。

1. 选择“网络 > 路由 > 智能选路”。
2. 选择进入“链路质量探测表”页签，单击“刷新”可以查看到最新的信息。

举例：基于源地址的策略路由

通过配置策略路由实现不同源地址数据通过不同的链路转发。

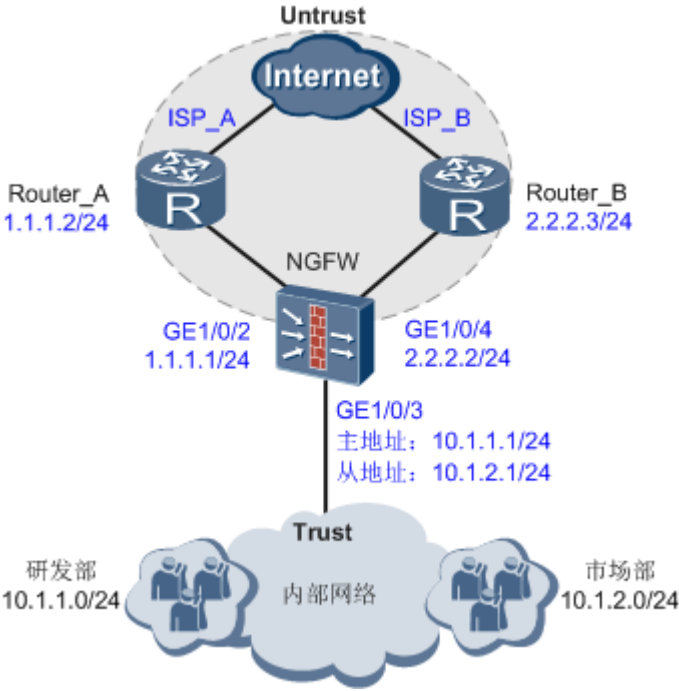
组网需求

某企业主要分为市场部和研发部两个部门，组网如[图 1](#)所示，NGFW 位于企业网出口，该企业部署了两条接入 Internet 的链路 ISP-A、ISP-B。ISP-A 上网速度快、网络速度稳定但费用较高，ISP-B 上网费用低廉，但是网速相对慢一些。


需求如下：

- 市场部对网速要求比较高，通过链路 ISP-A 访问 Internet。
- 研发部对网速要求不高，通过链路 ISP-B 来访问 Internet。

图 1 基于源地址的策略路由



操作步骤

- 1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
 - a. 将接口 GE1/0/3 加入 Trust 区域。
 - 1. 选择“网络 > 接口”。
 - 2. 选择 GE1/0/3 对应的 , 按如下参数配置。

安全区域	trust
IP 地址	10.1.1.1/24
	10.1.2.1/24

- b. 参考上述步骤，将接口 GE1/0/2 加入 Untrust 区域。

GE1/0/2 接口配置如下。

安全区域	untrust
IP 地址	1.1.1.1/24

- c. 参考上述步骤，将接口 GE1/0/4 加入 Untrust 区域。

GE1/0/4 接口配置如下。

安全区域	untrust
IP 地址	2.2.2.2/24

2. 配置 Trust 区域和 Untrust 区域之间的安全策略。

- a. 选择“策略 > 安全策略 > 安全策略”。
- b. 单击“新建”，按如下参数配置从 Trust 到 Untrust 的域间策略。

名称	policy_sec_trust_untrust
源安全区域	trust
目的安全区域	untrust
动作	permit

- c. 单击“应用”。

3. 创建策略路由“pbr_1”，从 Trust 区域接收的属于市场部的报文发送到下一跳 1.1.1.2。

- a. 选择“策略 > 策略路由”。
- b. 单击“新建”，按如下参数配置。

名称	pbr_1
描述	pbr_1
类型	源安全区域
源安全区域	trust
源地址/地区	10.1.1.0/24
出接口类型	单出口
下一跳	1.1.1.2
监控	启用 监控 IP 地址/域名：1.1.1.2

- c. 单击“确定”。

4. 创建策略路由“pbr_2”，从 Trust 区域接收的属于研发部的报文发送到下一跳 2.2.2.3。

- a. 单击“新建”，按如下参数配置。

名称	pbr_2
描述	pbr_2
类型	源安全区域
源安全区域	trust

源地址/地区	10.1.2.0/24
出接口类型	单出口
下一跳	2.2.2.3
监控	启用 监控 IP 地址/域名: 2.2.2.3

b. 单击“确定”。

配置脚本

```
#
interface GigabitEthernet1/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 ip address 10.1.1.1 255.255.255.0
 ip address 10.1.2.1 255.255.255.0 sub
#
interface GigabitEthernet1/0/4
 ip address 2.2.2.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/3
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/2
 add interface GigabitEthernet1/0/4
#
security-policy
 rule name policy_sec_trust_untrust
 source-zone trust
 destination-zone untrust
 action permit
#
ip-link check enable
 ip-link 1 destination 1.1.1.2 mode icmp
 ip-link 2 destination 2.2.2.3 mode icmp
#
rule name pbr_1
 description pbr_1
```



```
source-zone trust
source-address 10.1.1.0 24
track ip-link 1
action pbr next-hop 1.1.1.2
rule name pbr_2
description pbr_2
source-zone trust
source-address 10.1.2.0 24
track ip-link 2
action pbr next-hop 2.2.2.3
#
return
```

HCIE-Security 模拟面试问题及面试建议

1. 策略路由有哪些匹配条件，哪些策略路由规则的动作？
2. 策略路由智能选路和全局智能选路有什么区别？