

SDN网络服务 最佳实践

产品版本: v6.4.1

发布日期: 2024-06-05

目录

1 最佳实践	1
1.1 通过Keepalived与虚拟IP结合配置云主机网络 高可用	1
1.2 配置多活网络方案	5
1.3 配置路由器连接多个外网	11
1.4 配置云内对等连接	15
1.5 同VPC下限制子网间互访	18
1.6 限制VPC的出口流量	21
1.7 同VPC下云主机间通过配置无状态安全组实现S SH	23

1 最佳实践

1.1 通过Keepalived与虚拟IP结合配置云主机网络高可用

背景描述

通过为多个云主机的多个虚拟网卡配置同一虚拟IP（VIP），可以自定义其作为高可用服务的可漂移网络入口，保障业务应用的高可用性。典型的应用场景是将此虚拟IP与Keepalived相结合使用。

本文将以在两个CentOS 7云主机中配置Keepalived虚拟IP为例，详细介绍如何在该平台中配置Keepalived与虚拟IP结合使用，以保障业务连续性。

前提条件

- 已参考“计算”帮助中“云主机”的相关内容，完成两个CentOS 7云主机的创建。

操作步骤

1. 分别为各云主机的虚拟网卡配置同一虚拟IP。

- 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[虚拟网卡]，进入“虚拟网卡”页面。
- 勾选待操作虚拟网卡后， **更多** - **管理虚拟IP** ，弹出“管理虚拟IP”对话框。
- 如果虚拟IP不存在，则点击 **创建虚拟IP** 完成虚拟IP的创建，如果虚拟IP已存在，直接选择即可。

2. 在各云主机中安装Keepalived。

- 下载keepalived的rpm安装包。具体命令如下::

```
wget
http://www.rpmfind.net/linux/centos/7.6.1810/os/x86_64/Packages/keepalived-1.3.5-6.el7.x86_64.rpm
```

2. 配置EPEL源。

通过yum命令，配置EPEL源。具体命令如下::

```
yum -y
install http://dl.fedoraproject.org/pub/epel/7Server/x86_64/e/epel-
release-7-8.noarch.rpm
```

3. 安装keepalived的rpm安装包。具体命令如下::

```
yum localinstall keepalived-1.3.5-6.el7.x86_64.rpm -y
```

3. 配置各云主机的Keepalived。

1. 通过VIM编辑器，打开并编辑各云主机的Keepalived配置文件（即/etc/keepalived/keepalived.conf文件）。

Master云主机Instance A（**node 1**）的配置示例::

```
global_defs {
    router_id rt1
}
vrrp_instance VI_1 {
    state MASTER
    interface eth0
    unicast_peer {
        $node2    #Fixed IP for Instance B.
    }
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1234
    }
    virtual_ipaddress {
        $vip dev eth0    #Use the VIP address you configured.
    }
}
```

Backup云主机Instance B (**node 2**) 的配置示例::

```
global_defs {
    router_id rt1
}
vrrp_instance VI_1 {
    state BACKUP
    interface eth0
    unicast_peer {
        $node1    #Fixed IP for Instance A.
    }
    virtual_router_id 51
    priority 80
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1234
    }
    virtual_ipaddress {
        $vip dev eth0    #Use the VIP address you configured.
    }
}
```

2. 启动Keepalived服务。具体命令如下::

```
service keepalived start
```

结果验证

1. 在Master云主机 (**node 1**) 中, 查询其IP信息, 确认虚拟IP已配置成功。查询IP信息的具体命令如下::

```
ip a
```

2. 停止Master云主机 (**node 1**) 的Keepalived服务。具体命令如下::

```
service keepalived stop
```

3. 查询Master云主机 (**node 1**) 和Backup云主机 (**node 2**) 的IP信息, 确认虚拟IP成功漂移到Backup云主机 (**node 2**) 上。

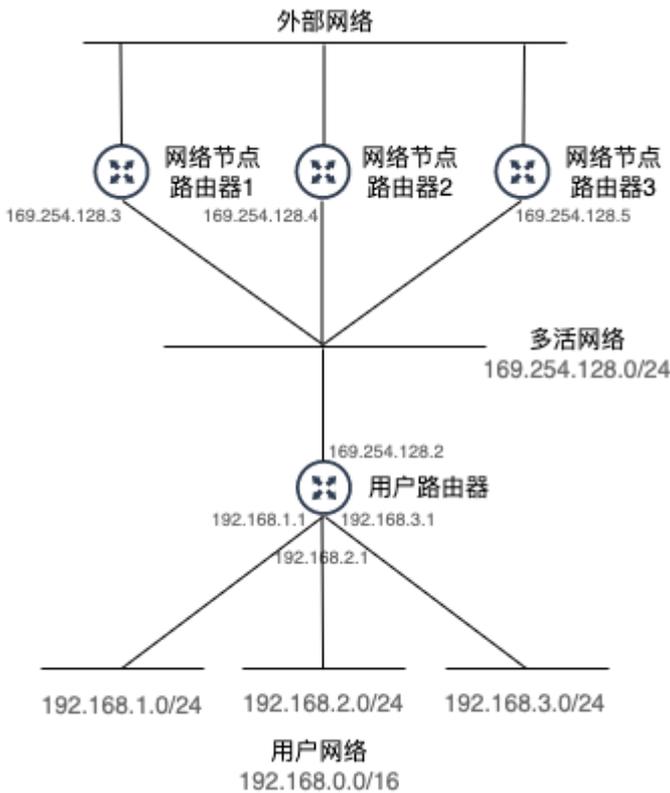
1.2 配置多活网络方案

背景描述

通过配置多活网络，可以横向提升网络性能，保障业务应用的高性能访问。本文将以配置三个网络节点路由器为例，介绍如何在该平台中配置多活网络方案，以提升业务的网络性能。

说明：

多活网络方案仅支持纯路由模式的路由器，即此方案中使用的用户路由器不支持公网IP和SNAT功能。



本实践方案中，具体网络规划信息如下：

类型	说明
----	----

类型	说明
用户网络	<ul style="list-style-type: none"> * 名称: user_network * 网络类型: 内部网络 * 网络模式: Geneve * 子网1: <ul style="list-style-type: none"> - 名称: user_network_default_ipv4_subnet - 网段: 192.168.1.0/24 - 网关地址: 设置网关 (192.168.1.1) - DHCP服务: 开启 * 子网2: <ul style="list-style-type: none"> - 名称: user_network_default_ipv4_subnet2 - 网段: 192.168.2.0/24 - 网关地址: 设置网关 (192.168.2.1) - DHCP服务: 开启 * 子网3: <ul style="list-style-type: none"> - 名称: user_network_default_ipv4_subnet3 - 网段: 192.168.3.0/24 - 网关地址: 设置网关 (192.168.3.1) - DHCP服务: 开启
多活网络	<ul style="list-style-type: none"> * 名称: multi_net_169_254_128 * 网络类型: 内部网络 * 网络模式: Geneve * 子网: <ul style="list-style-type: none"> - 名称: multi_net_169_254_128_default_ipv4_subnet - 网段: 169.254.128.0/24 - 网关地址: 不设置 - DHCP服务: 关闭

类型	说明
用户路由器	<ul style="list-style-type: none"> * 名称: user_router * 路由器连接: <ul style="list-style-type: none"> - 子网: multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24; 子网IP: 169.254.128.2 - 子网: user_network_default_ipv4_subnet:192.168.1.0/24; 子网IP: 192.168.1.1 - 子网: user_network_default_ipv4_subnet2:192.168.2.0/24; 子网IP: 192.168.2.1 - 子网: user_network_default_ipv4_subnet3:192.168.3.0/24; 子网IP: 192.168.3.1 * 静态路由: <ul style="list-style-type: none"> - 目的CIDR: 0.0.0.0/0; 下一跳: 169.254.128.3 - 目的CIDR: 0.0.0.0/0; 下一跳: 169.254.128.4 - 目的CIDR: 0.0.0.0/0; 下一跳: 169.254.128.5
网络节点路由器 1	<ul style="list-style-type: none"> * 名称: multi_ex_router_lb_1 * 可用区: 与网络节点的可用区一致 * 路由器网关: 172.16.10.3 (不开启SNAT) * 路由器连接: <ul style="list-style-type: none"> - 子网: multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24; 子网IP: 169.254.128.3 * 静态路由: <ul style="list-style-type: none"> - 目的CIDR: 192.168.0.0/16; 下一跳: 169.254.128.2
网络节点路由器 2	<ul style="list-style-type: none"> * 名称: multi_ex_router_lb_2 * 可用区: 与网络节点的可用区一致 * 路由器网关: 172.16.10.4 (不开启SNAT) * 路由器连接: <ul style="list-style-type: none"> - 子网: multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24; 子网IP: 169.254.128.4 * 静态路由: <ul style="list-style-type: none"> - 目的CIDR: 192.168.0.0/16; 下一跳: 169.254.128.2

类型	说明
网络节点路由器 3	<ul style="list-style-type: none"> * 名称: multi_ex_router_lb_3 * 可用区: 与网络节点的可用区一致 * 路由器网关: 172.16.10.5 (不开启SNAT) * 路由器连接: <ul style="list-style-type: none"> - 子网: multi_net_169_254_128_default_ipv4_subnet:169.254.128.0/24; 子网IP: 169.254.128.5 * 静态路由: <ul style="list-style-type: none"> - 目的CIDR: 192.168.0.0/16; 下一跳: 169.254.128.2

操作步骤

1. 创建用户网络和多活网络。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户网络和多活网络。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
2. 单击 **创建网络** ，进入“创建网络”页面。
3. 配置参数后，单击 **创建网络** ，完成操作。其中，各参数的具体说明，请参考 [创建二层基础网络](#)。

2. 创建用户路由器和网络节点路由器。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户路由器和网络节点路由器。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，进入“路由器”页面。
2. 单击 **创建路由器** ，弹出“创建路由器”对话框。
3. 配置参数后，单击 **创建** ，完成操作。其中，各参数的具体说明，请参考 [创建路由器](#)。

3. 设置网络节点路由器的网关。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置各网络节点路由器的网关。

1. 在“路由器”页面中，勾选待操作的网络节点路由器后，单击 **更多** - **设置网关**，弹出“设置路由器网关”对话框。

2. 配置参数后，单击 **设置**，完成操作。其中，各参数的具体说明，请参考 [设置路由器网关](#)。

4. 设置用户路由器和网络节点路由器的子网连接。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和网络节点路由器的子网连接。

1. 在“路由器”页面中，单击待操作路由器的名称，进入其详情页面。

2. 在[路由器连接]页签中，单击 **连接子网**，弹出“连接子网”对话框。

3. 配置参数后，单击 **连接**，完成操作。

5. 设置用户路由器和网络节点路由器的静态路由。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和网络节点路由器的静态路由。

1. 在“路由器”页面中，单击待操作路由器的名称，进入其详情页面。

2. 在[静态路由]页签中，单击 **添加静态路由**，弹出“添加静态路由”对话框。

3. 配置参数后，单击 **连接**，完成操作。

6. 设置外网网关的ECMP静态路由。

请在外部网关处，设置从外网网关回内网的静态路由。以Linux服务器网关为例，说明本实践方案中的静态路由配置命令::

```
ip route add 192.168.1.0/24 nexthop via 172.16.10.3 weight 1 nexthop via 172.16.10.4 weight 1 nexthop via 172.16.10.5 weight 1
ip route add 192.168.2.0/24 nexthop via 172.16.10.3 weight 1 nexthop via 172.16.10.4 weight 1 nexthop via 172.16.10.5 weight 1
ip route add 192.168.3.0/24 nexthop via 172.16.10.3 weight 1 nexthop via 172.16.10.4 weight 1 nexthop via 172.16.10.5 weight 1
```

结果验证

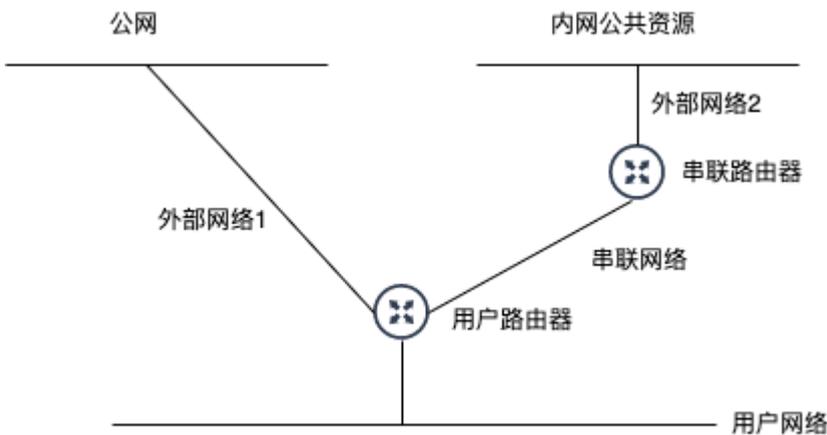
通过查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络拓扑]，进入“网络拓扑”页面。
2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图。

1.3 配置路由器连接多个外网

背景描述

通过配置路由器连接多个外部网络，可以实现云主机、容器或裸金属主机等计算资源访问安全隔离的多个网络环境，保障业务应用的安全可靠访问。本文将以配置一个用户路由器连接两个外部网络（一个用于连接公网，一个用于连接内网公共资源）为例，介绍如何在该云平台中配置路由器连接多个外部网络，以提升业务的高可靠性。



本实践方案中，具体网络规划信息如下：

类型	配置	说明
用户网络	<ul style="list-style-type: none"> * 名称: user_network * 网络类型: 内部网络 * 网络模式: Geneve * 子网: <ul style="list-style-type: none"> - 名称: user_network_default_ipv4_subnet - 网段: 10.0.0.0/24 - 网关地址: 设置网关 (10.0.0.1) - DHCP服务: 开启 	用于建立用户路由器与用户的云主机、容器或裸金属主机等计算资源之间的连接。

类型	配置	说明
外部网络1	<ul style="list-style-type: none"> * 名称: ex_net_1 * 网络类型: 外部网络 * 网络模式: VLAN * 子网: <ul style="list-style-type: none"> - 名称: ex_net_1_default_ipv4_subnet - 网段: 172.17.0.0/24 - 网关地址: 设置网关 (172.17.0.1) 	用于建立用户路由器与公网之间的连接。
外部网络2	<ul style="list-style-type: none"> * 名称: ex_net_2 * 网络类型: 外部网络 * 网络模式: VLAN * 子网: <ul style="list-style-type: none"> - 名称: ex_net_2_default_ipv4_subnet - 网段: 172.16.0.0/24 - 网关地址: 设置网关 (172.16.0.1) 	用于建立串联路由器与内网公共资源 (如对象存储、公共rpm源等) 之间的连接。
串联网络	<ul style="list-style-type: none"> * 名称: series_network * 网络类型: 内部网络 * 网络模式: Geneve * 子网: <ul style="list-style-type: none"> - 名称: series_network_default_ipv4_subnet - 网段: 169.254.128.0/24 - 网关地址: 不设置 - DHCP服务: 关闭 	用于建立用户路由器与串联路由器之间的连接。
用户路由器	<ul style="list-style-type: none"> * 名称: user_router * 路由器网关: 172.17.0.10 (开启SNAT) * 路由器连接: <ul style="list-style-type: none"> - 子网: user_network_default_ipv4_subnet:10.0.0.0/24; 子网IP: 10.0.0.1 - 子网: series_network_default_ipv4_subnet:169.254.128.0/24; 子网IP: 169.254.128.2 * 静态路由: <ul style="list-style-type: none"> - 目的CIDR: 172.16.0.0/24; 下一跳: 169.254.128.3 	用于建立用户网络、公网与内网公共资源之间的连接。

类型	配置	说明
串联路由器	* 名称: series_router * 可用区: 如需保证两个外部网络的访问物理隔离, 请指定单独的可用区, 并确保该可用区已配置独立的网络节点。 * 路由器网关: 172.16.0.10 (开启SNAT) * 路由器连接: - 子网: series_network_default_ipv4_subnet: 169.254.128.0/24; 子网IP: 169.254.128.3 * 静态路由: - 目的CIDR: 10.0.0.0/24; 下一跳: 169.254.128.2	用于建立用户网络与内网公共资源 (如对象存储、公共rpm源等) 之间的连接。

操作步骤

1. 创建用户网络、外部网络和串联网络。

请依据本实践方案中的网络规划信息, 参考以下操作步骤, 依次创建用户网络、外部网络1、外部网络2和串联网络。

1. 在云平台的顶部导航栏中, 依次选择[产品与服务]-[网络]-[网络], 进入“网络”页面。
2. 单击 **创建网络**, 进入“创建网络”页面。
3. 配置参数后, 单击 **创建网络**, 完成操作。其中, 各参数的具体说明, 请参考 [创建二层基础网络](#)。

2. 创建用户路由器和串联路由器。

请依据本实践方案中的网络规划信息, 参考以下操作步骤, 依次创建用户路由器和串联路由器。

1. 在云平台的顶部导航栏中, 依次选择[产品与服务]-[网络]-[路由器], 进入“路由器”页面。
2. 单击 **创建路由器**, 弹出“创建路由器”对话框。
3. 配置参数后, 单击 **创建**, 完成操作。其中, 各参数的具体说明, 请参考 [创建路由器](#)。

3. 设置串联路由器的网关。

请依据本实践方案中的网络规划信息，参考以下操作步骤，设置串联路由器的网关。

1. 在“路由器”页面中，勾选待操作的网络节点路由器后，单击 **更多** - **设置网关**，弹出“设置路由器网关”对话框。
 2. 配置参数后，单击 **设置**，完成操作。其中，各参数的具体说明，请参考 [设置路由器网关](#)。
4. 设置用户路由器和串联路由器的子网连接。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器和串联路由器的子网连接。

1. 在“路由器”页面中，单击待操作路由器的名称，进入其详情页面。
 2. 在[路由器连接]页签中，单击 **连接子网**，弹出“连接子网”对话框。
 3. 配置参数后，单击 **连接**，完成操作。
5. 设置用户路由器的静态路由。

请依据本实践方案中的网络规划信息，参考以下操作步骤，设置用户路由器的静态路由。

1. 在“路由器”页面中，单击待操作路由器的名称，进入其详情页面。
2. 在[静态路由]页签中，单击 **添加静态路由**，弹出“添加静态路由”对话框。
3. 配置参数后，单击 **连接**，完成操作。

结果验证

通过查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络拓扑]，进入“网络拓扑”页面。
2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图。

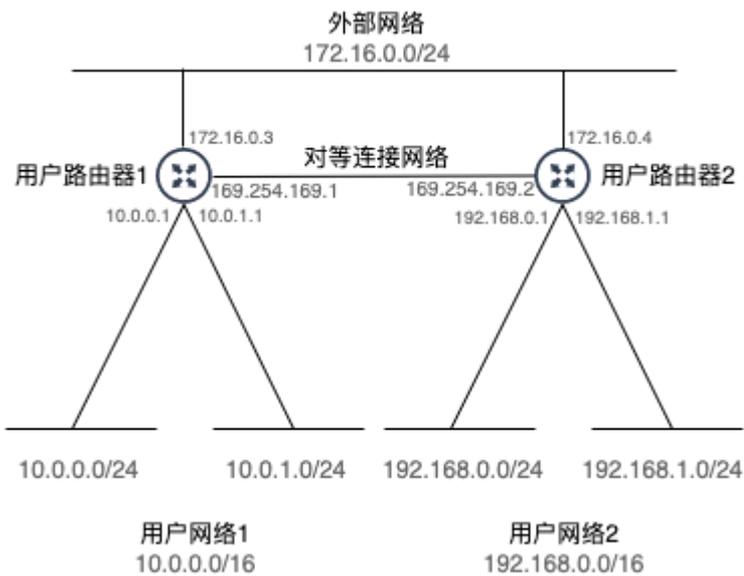
1.4 配置云内对等连接

背景描述

通过配置用户内部网络中多个路由器之间的对等连接，可以实现云内路由器下各子网之间的三层网络互通。本文将配置两个用户路由器的对等连接为例，介绍如何在该平台中配置内部网络的对等连接，实现云内三层网络互通。

警告：

在配置多个用户路由器之间的云内对等连接时，请确保各路由器的子网不发生冲突。



本实践方案中，具体网络规划信息如下（其中，用户网络与外部网络假定已完成相关配置，具体信息如上图所示，下表仅展示需另添加的信息）：

类型	配置	说明
----	----	----

类型	配置	说明
对等连接网络	* 名称: peer_network * 网络类型: 内部网络 * 网络模式: Geneve * 子网: - 名称: peer_network_default_ipv4_subnet - 网段: 169.254.169.0/29 - 网关地址: 不设置 - DHCP服务: 关闭	用于建立两个用户路由器之间的对等连接。
用户路由器1	* 名称: user_router_1 * 路由器连接: - 子网: peer_network_default_ipv4_subnet:169.254.169.0/29; 子网IP: 169.254.169.1 * 静态路由: - 目的CIDR: 192.168.0.0/16; 下一跳: 169.254.169.2	用于建立用户网络、外部网络与其他内部网络之间的连接。
用户路由器2	* 名称: user_router_2 * 路由器连接: - 子网: peer_network_default_ipv4_subnet:169.254.169.0/29; 子网IP: 169.254.169.2 * 静态路由: - 目的CIDR: 10.0.0.0/16; 下一跳: 169.254.169.1	用于建立用户网络、外部网络与其他内部网络之间的连接。

操作步骤

1. 创建对等连接网络。

请依据本实践方案中的网络规划信息，参考以下操作步骤，创建对等连接网络。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
2. 单击 **创建网络** ，进入“创建网络”页面。

3. 配置参数后，单击 **创建网络** ，完成操作。其中，各参数的具体说明，请参考 [创建二层基础网络](#)。

2. 创建用户路由器。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次创建用户路由器1和用户路由器2。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，进入“路由器”页面。

2. 单击 **创建路由器** ，弹出“创建路由器”对话框。

3. 配置参数后，单击 **创建** ，完成操作。其中，各参数的具体说明，请参考 [创建路由器](#)。

3. 设置用户路由器的子网连接。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器1和用户路由器2的子网连接。

1. 在“路由器”页面中，单击待操作路由器的名称，进入其详情页面。

2. 在[路由器连接]页签中，单击 **连接子网** ，弹出“连接子网”对话框。

3. 配置参数后，单击 **连接** ，完成操作。

4. 设置用户路由器的静态路由。

请依据本实践方案中的网络规划信息，参考以下操作步骤，依次设置用户路由器1和用户路由器2的静态路由。

1. 在“路由器”页面中，单击待操作路由器的名称，进入其详情页面。

2. 在[静态路由]页签中，单击 **添加静态路由** ，弹出“添加静态路由”对话框。

3. 配置参数后，单击 **连接** ，完成操作。

结果验证

通过查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络拓扑]，进入“网络拓扑”页面。

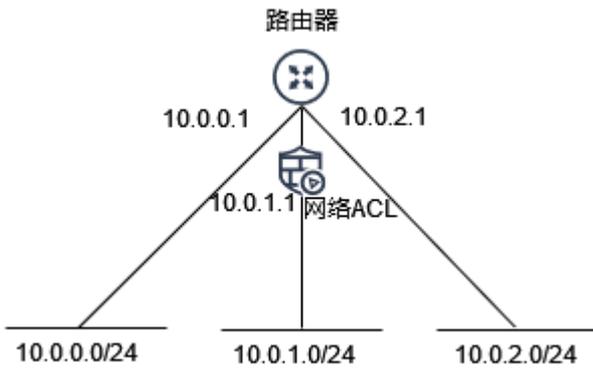
2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图。

1.5 同VPC下限制子网间互访

背景描述

在VPC没有绑定网络ACL情况下，VPC内子网可以互通。通过配置网络ACL限制同VPC下子网间流量。

如图所示拓扑，VPC内网段 `10.0.1.0/24` 禁止与除 `10.0.0.0/24` 外的其它网段互通。



本实践方案通过配置网络ACL完成上述需求。

前提条件

路由器绑定了上述网段子网，子网间的云主机可以互通。

操作步骤

1. 创建网络ACL。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[网络ACL]，进入“网络ACL列表”页面。
2. 单击 `创建网络ACL` ，弹出“创建网络ACL”对话框。
3. 配置参数后，单击 `创建` ，完成操作。

参数	说明
----	----

参数	说明
名称	网络ACL的名称。
描述	网络ACL的描述。

2. 配置网络ACL出入方向规则。

1. 在网络ACL的详情页面，单击 **入方向规则** - **添加规则** ，出现规则编辑框。
2. 添加如下规则，单击 **确认** ，完成操作。

方向	类型	策略	协议	源地址
入方向	ipv4	允许	全部	10.0.0.0/24

说明：网络ACL规则是无状态的，所以配置了一个方向的允许策略，还需要配置回复方向的允许策略，才能达到流量放行的需求。

3. 单击 **出方向规则** - **添加规则** ，出现规则编辑框。
4. 配置如下规则，单击 **确认** ，完成操作。

方向	类型	策略	协议	源地址
出方向	ipv4	允许	全部	0.0.0.0/0

3. 关联子网。

1. 点击已经创建的网络ACL，进入该网络ACL的详情页面，单击 **关联子网** - **关联** ，弹出“关联子网”对话框。
2. 选择上述网段为 **10.0.1.0/24** 的子网，单击 **关联** 。

说明：关联子网后，网络ACL默认拒绝所有出入子网网关的流量，直至添加放通规则。

结果验证

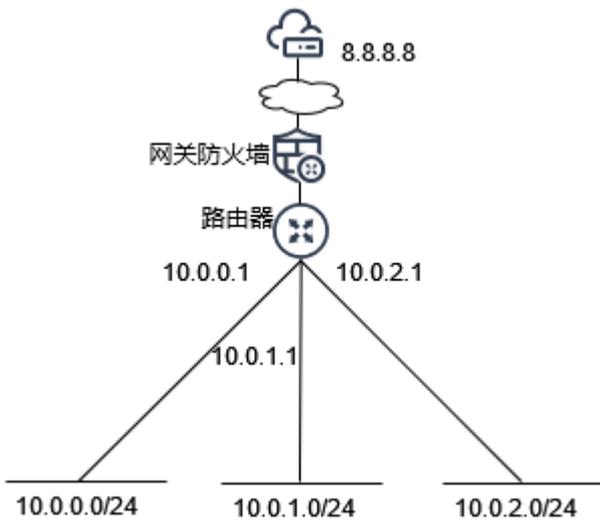
进入网段 10.0.0.0/24 的云主机，能正常访问网段 10.0.1.0/24 的云主机；进入网段 10.0.2.0/24 的云主机，无法访问网段 10.0.1.0/24 的云主机。

1.6 限制VPC的出口流量

背景描述

在VPC没有绑定网关防火墙的情况下，VPC内云主机访问外网没有限制。通过配置网关防火墙可以限制VPC下的出口流量。

如图所示拓扑，禁止VPC内所有云主机访问外网，放行所有云主机访问外网 `8.8.8.8` 的主机。



本实践方案通过配置网关防火墙完成上述需求。

前提条件

路由器绑定了外部网关，以及云主机所在的子网，并且云主机可以访问外网。

操作步骤

1. 创建网关防火墙。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[网关防火墙]，进入“网关防火墙”页面。
2. 单击 `创建网关防火墙` ，弹出“创建网关防火墙”对话框。
3. 配置参数后，单击 `创建` ，完成操作。

参数	说明
名称	网关防火墙的名称。
描述	网关防火墙的描述。

2. 配置网关防火墙出方向规则。

1. 单击 **出方向规则** - **添加规则** ，出现规则编辑框。
2. 配置如下规则，单击 **确认** ，完成操作。

说明：网关防火墙规则是带状态的，所以只需要配置一个方向的允许策略，回复报文也会被允许通过。

方向	类型	策略	协议	源地址	源
出方向	ipv4	允许	全部	0.0.0.0/0	全

3. 关联路由器。

1. 点击已经创建的网关防火墙，进入该网关防火墙的详情页面，单击 **关联路由器** - **关联** ，弹出“关联路由器”对话框。
2. 选择上述路由器，单击 **关联** 。

说明：关联路由器后，网关防火墙默认拒绝所有出入路由器网关的流量，直至添加放通规则。

结果验证

进入VPC内任意一台云主机， **ping** 访问 **114.114.114.114** 失败，能正常访问 **8.8.8.8** 。

1.7 同VPC下云主机间通过配置无状态安全组实现SSH

背景描述

安全组默认是有状态的，我们在一些场景可以使用无状态安全组，本实践方案通过配置无状态安全组完成云主机A和云主机B互相SSH。

说明：无状态安全组的典型使用场景包括

- 无状态安全组性能比有状态性能好，在裸金属场景下，如果对网络性能有要求，考虑使用无状态安全组。
- 在LVS负载均衡的DR模式下，云主机的虚拟网卡需要使用无状态安全组。

操作步骤

1. 创建无状态安全组。

- 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[安全组]，进入“安全组列表”页面。
- 单击 **创建安全组**，弹出“创建安全组”对话框。
- 选择状态为 **否**，配置完参数后，单击 **创建**，完成操作。

参数	说明
名称	安全组的名称。
描述	安全组的描述。
状态	安全组是否带状态。

说明：创建完无状态安全组后，默认会创建一条入方向放行metadata流量的规则，以及出方向放行 `0.0.0.0/0` 的规则。除非入向全部放开，无状态安全组无法做到云主机访问任意公网，因为回复包无

法添加入向的具体规则，包括源IP，目的端口都无法确定。

方向	类型	协议和端口	源地址
入方向	ipv4	TCP:全部	169.254.169.254/32
出方向	ipv4	全部	0.0.0.0/0
出方向	ipv6	全部	::/0

2. 配置安全组出入方向规则。

1. 在安全组列表，点击上述安全组的 **配置规则**，进入安全组详情页面的规则列表。
2. 添加如下规则，单击 **确认**，完成操作。

方向	类型	协议和端口	源地址
入方向	ipv4	TCP:全部	10.0.0.0/24

说明：由于无状态安全组规则是无状态的，所以配置了一个方向的允许策略，需要配置回复方向的允许策略，以达到流量放行的需求。

3. 虚拟网卡关联安全组。

1. 进入虚拟网卡列表，选择云主机A和云主机B的虚拟网卡，点击页面上方 **更多** - **编辑安全组**，弹出“编辑安全组”对话框。
2. 选择上述安全组，单击 **保存**。

结果验证

进入云主机A，能正常SSH访问云主机B；进入云主机B，能正常SSH访问云主机A。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：

北京市海淀区西北旺东路10号院东区1号楼1层107-2号

南京易捷思达软件科技有限公司：

江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：

contact@easystack.cn (业务咨询)

partners@easystack.cn(合作伙伴咨询)

marketing@easystack.cn (市场合作)