IPSEC 配置说明

示例说明：

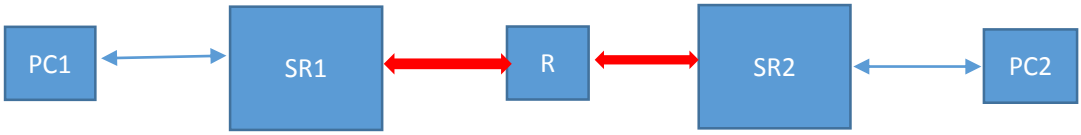
1、PC1 和 PC2 是两台终端电脑，它们的 IP 地址分别为 PC1(IP 地址：192.168.201.100 子网掩码：255.255.255.0 默认网关：192.168.201.1)；PC2(IP 地址：192.168.208.100 子网掩码：255.255.255.0 默认网关：192.168.208.1)

2、R 是一台主干路由器，它的两个网口的 IP 地址分别为 172.16.16.1 和 172.16.17.1

3、SR1 和 SR2 是我们的网络安全设备，SR1 配置为：一个 LAN 口(eth6)和一个 WAN 口(eth7)，LAN 口 IP 地址为 192.168.201.1，WAN 口 IP 地址为 172.16.16.5；SR2 配置为：一个 LAN 口(eth6)和一个 WAN 口(eth7)，LAN 口 IP 地址为 192.168.208.1，WAN 口 IP 地址为 172.16.17.3

4、网络拓扑：SR1 的 eth6 网口连接 PC1， SR1 的 eth7 网口连接 R 的 WAN3；SR2 的 eth6 网口连接 PC2， SR2 的 eth7 网口连接 R 的 LAN3

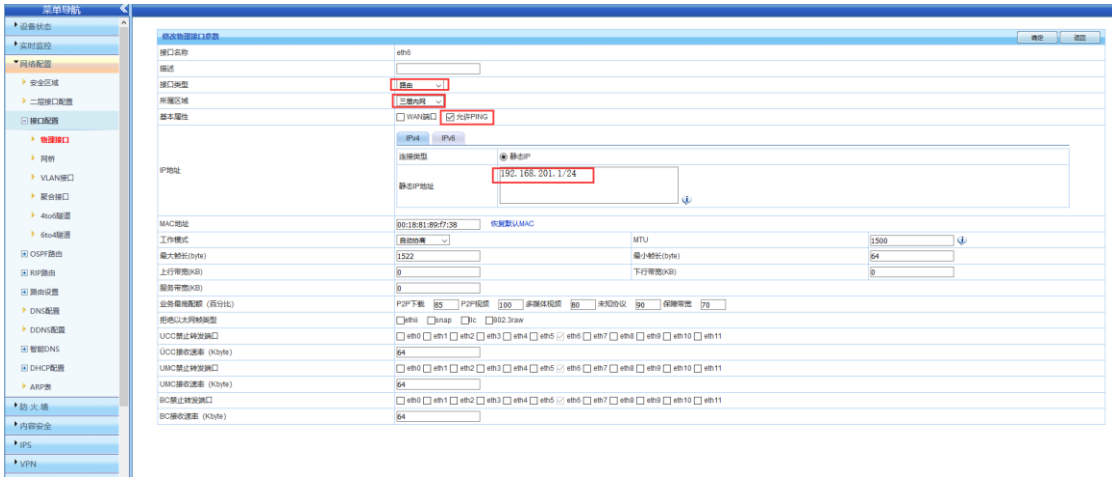
网络拓扑示意图如下



一． SR1 机器的配置

1. 配置 LAN 口

进入管理页面的【网络配置】->【接口配置】->【物理接口】，以 eth6 为例，点击 eth6 的【修改】，弹出下列修改页面：



填写 LAN 口的主要信息，

接口类型：路由

所属区域：三层内网

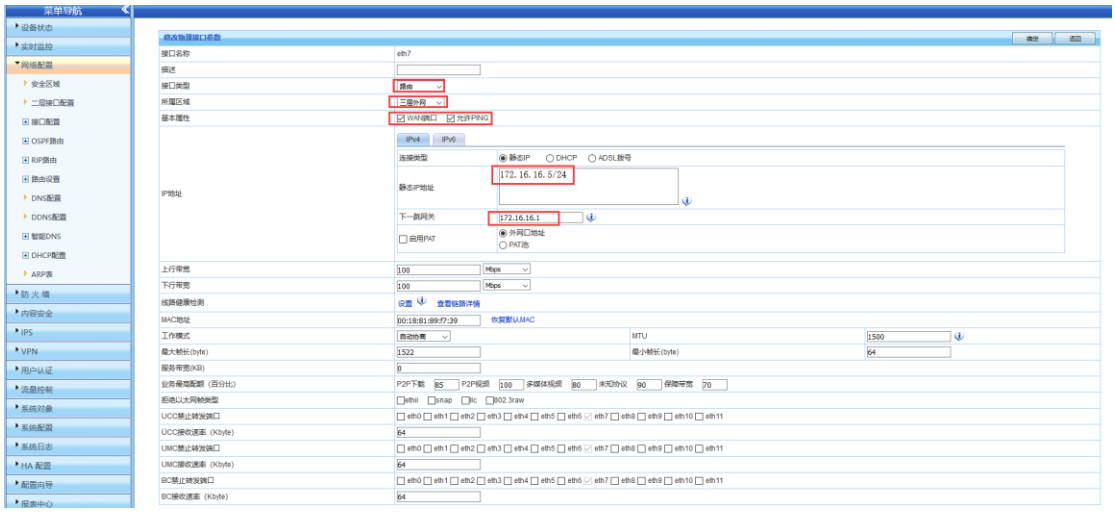
允许 PING: 勾选

静态 IP：192.168.201.1/24

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

2. 配置 WAN 口

（1）进入管理页面的【网络配置】->【接口配置】->【物理接口】，以 eth7 为例，点击 eth7 的【修改】，弹出下列修改页面：



填写 WAN 口的主要信息，

接口类型：路由

所属区域：三层外网

WAN 端口：勾选

允许 PING: 勾选

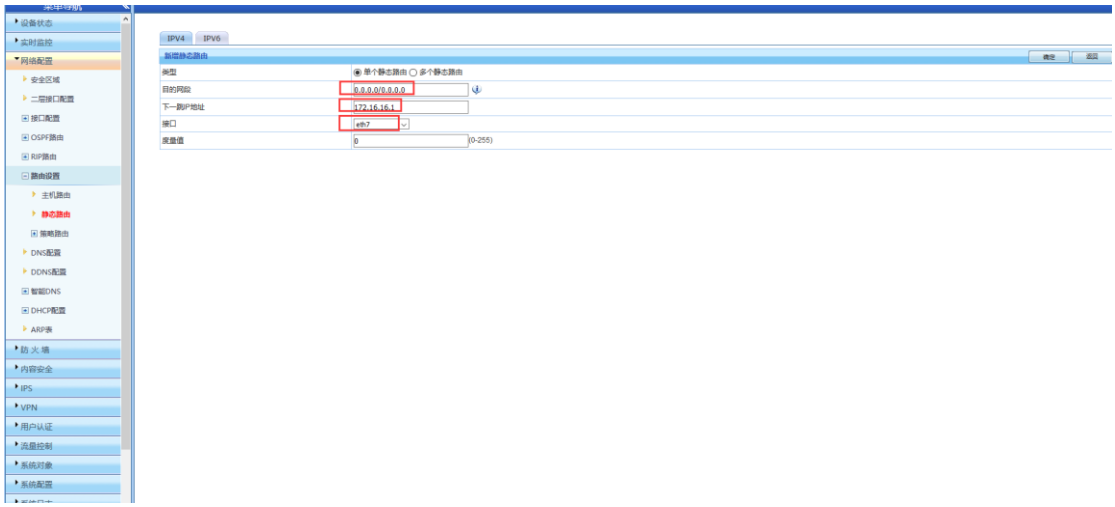
静态 IP：172.16.16.5/24

下一跳网关：172.16.16.1

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

（2） 为了跨路由访问，必须为 WAN 口设置一条静态默认路由，进入管理页面的【网络配置】->【路由设置】->【静态路由】，点击【新增】按钮，弹出如下页

面：



填写静态路由的主要信息，

目的网段：0.0.0.0/0.0.0.0

下一跳 IP 地址：172.16.16.1

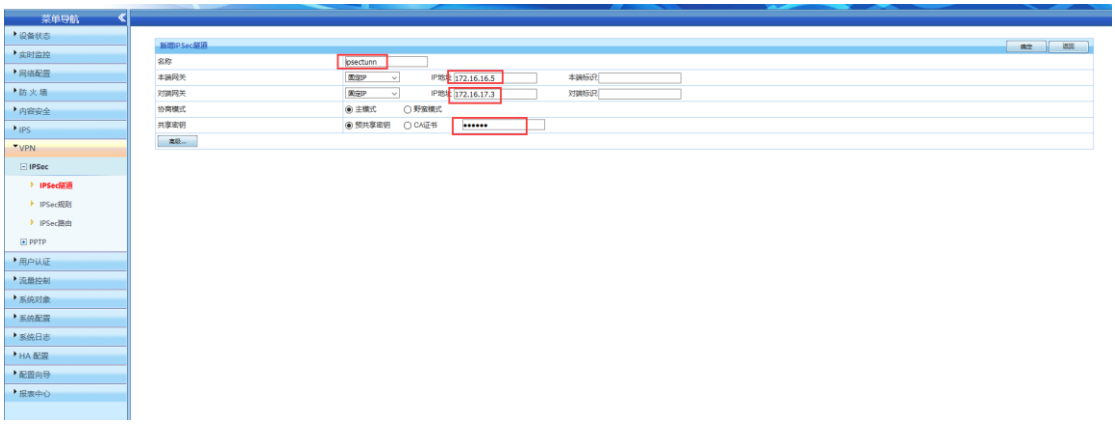
接口：eth7

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

3. 配置 IPSEC

（1）设置 IPSec 隧道

进入管理页面的【VPN】->【IPSec】->【IPSec 隧道】，点击【新增】按钮，弹出如下页面：



填写 IPSec 隧道的主要信息，

名称：ipsectunn

本端网关->固定 IP：172.16.16.5

对端网关->固定 IP：172.16.17.3

共享密钥->预共享密钥：123456

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

（2）设置 IPSec 规则

进入管理页面的【防火墙】->【安全策略】,点击【新增】按钮，弹出如下页面：

填写 IPSec 规则的主要信息，

名称：ipsecrule

源地址->IP 地址：192.168.201.0/24

目的地址->IP 地址：192.168.208.0/24

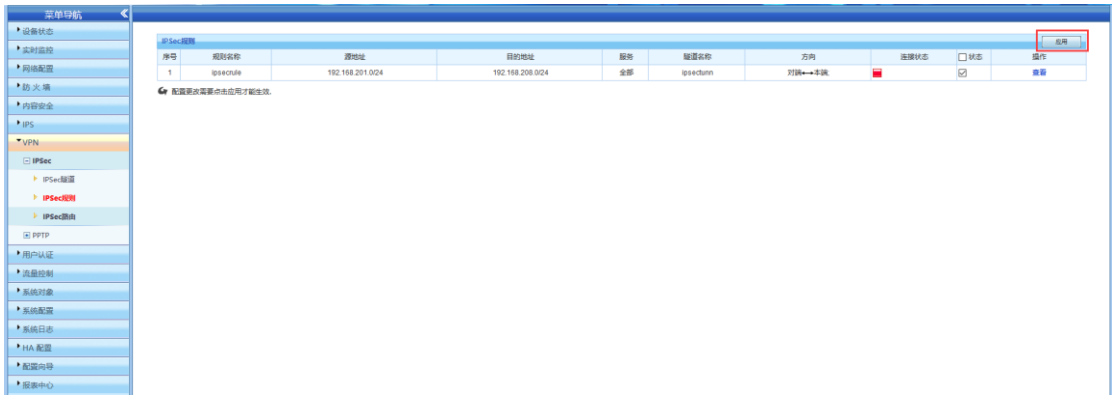
动作：VPN

隧道名称：ipsectunn

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

（3）启用 IPSec

进入管理页面的【VPN】->【IPSec】->【IPSec 规则】，如下图所示：



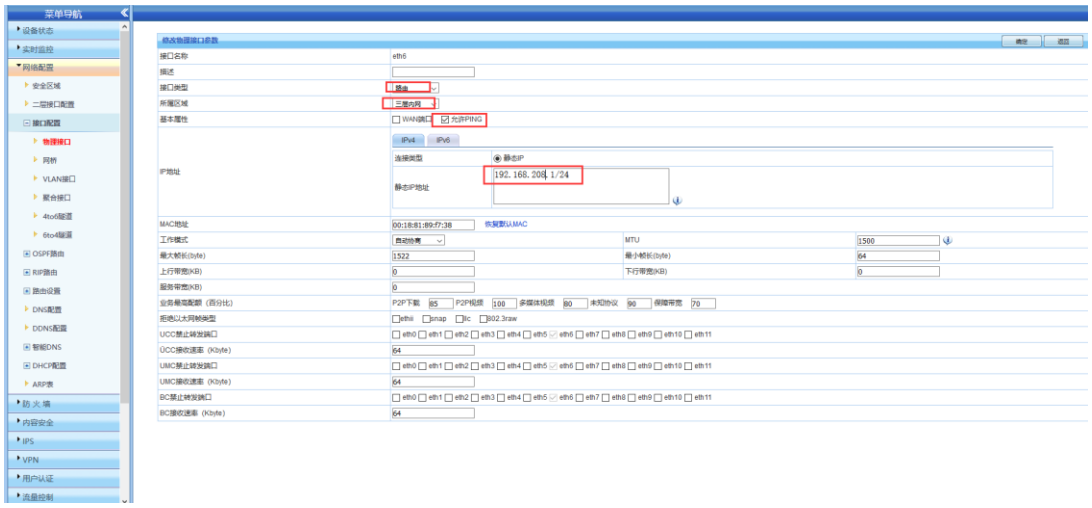
点击上图右上角的【应用】按钮，就可启用 IPSec 功能。

二． SR2 机器的配置

1. 配置 LAN 口

进入管理页面的【网络配置】->【接口配置】->【物

理接口】，以 eth6 为例，点击 eth6 的【修改】，弹出下列修改页面：



填写 LAN 口的主要信息，

接口类型：路由

所属区域：三层内网

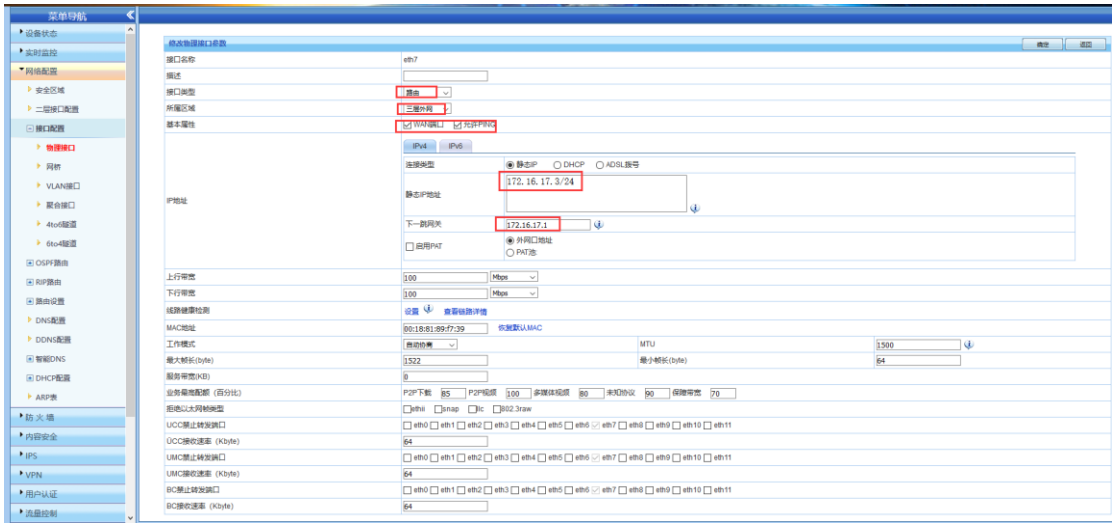
允许 PING: 勾选

静态 IP：192.168.208.1/24

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

2. 配置 WAN 口

（1）进入管理页面的【网络配置】->【接口配置】->【物理接口】，以 eth7 为例，点击 eth7 的【修改】，弹出下列修改页面：



填写 WAN 口的主要信息，

接口类型：路由

所属区域：三层外网

WAN 端口：勾选

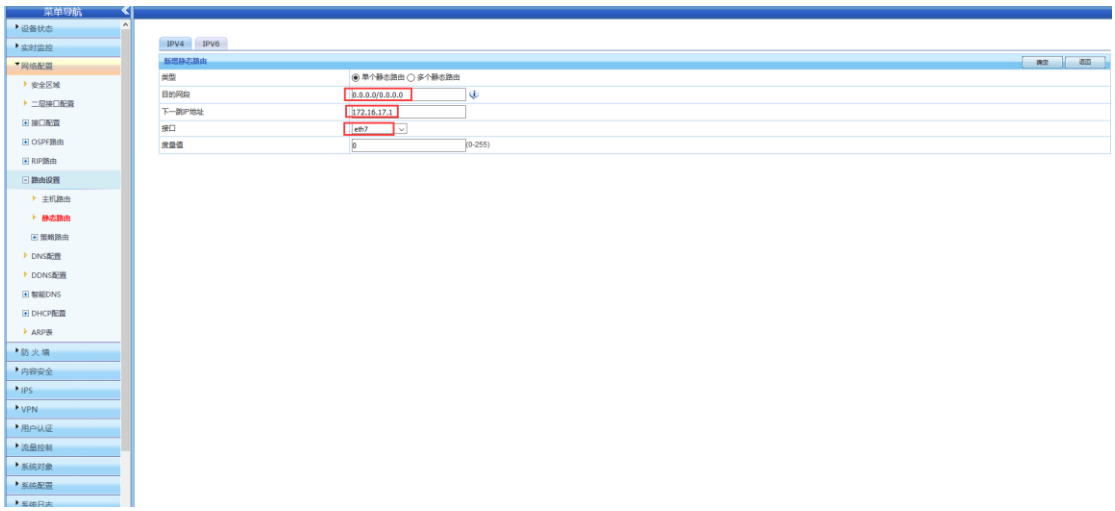
允许 PING: 勾选

静态 IP：172.16.17.3/24

下一跳网关：172.16.17.1

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

（2）为了跨路由访问，必须为 WAN 口设置一条静态默认路由，进入管理页面的【网络配置】->【路由设置】->【静态路由】，点击【新增】按钮:



填写静态路由的主要信息，

目的网段：0.0.0.0/0.0.0.0

下一跳 IP 地址：172.16.17.1

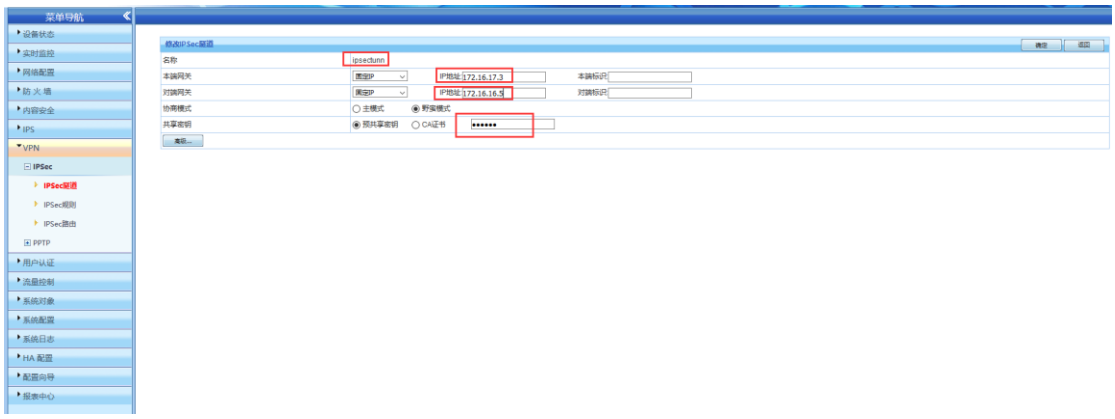
接口：eth7

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

3. 配置 IPSEC

（1）设置 IPSec 隧道

进入管理页面的【VPN】->【IPSec】->【IPSec 隧道】，点击【新增】按钮：



填写 IPSec 隧道的主要信息，

名称：ipsectunn

本端网关->固定 IP：172.16.17.3

对端网关->固定 IP：172.16.16.5

共享密钥->预共享密钥：123456

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

（2）设置 IPSec 规则

进入管理页面的【防火墙】->【安全策略】,点击【新增】按钮：

填写 IPSec 规则的主要信息，

名称：ipsecrule

源地址->IP 地址：192.168.208.0/24

目的地址->IP 地址：192.168.201.0/24

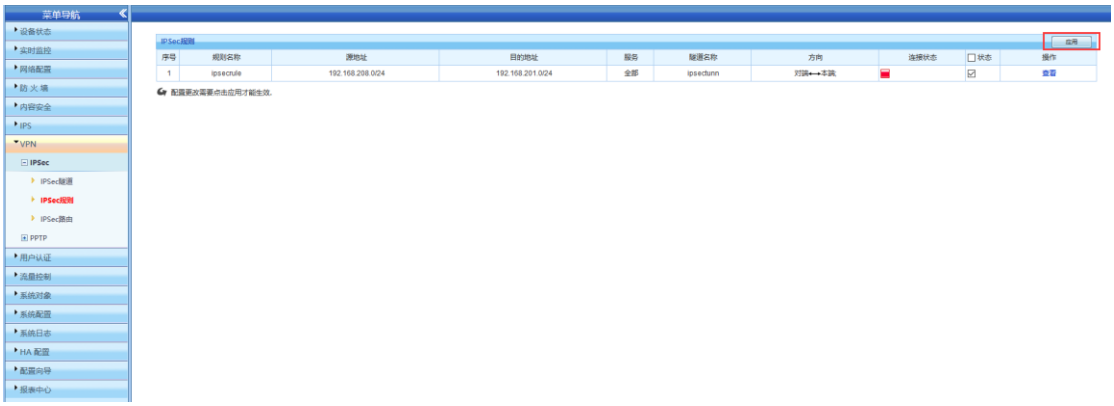
动作：VPN

隧道名称：ipsectunn

见图中的红色框。其他的次要信息保持系统默认即可。再点击【确定】按钮。

（3）启用 IPSec

进入管理页面的【VPN】->【IPSec】->【IPSec 规则】，如下图所示：



点击上图右上角的【应用】按钮，就可启用 IPSec 功能。