【第十一期】渠道技术培训资料

2021年11月

目录

01 下一代防火墙基础功能介绍

下一代防火墙产品概述

大洲智创下一代防火墙提供L2-L7 层安全可视的全面防护，通过双向检测网络流量，有效识别来自网络层和应用层的风险，提供比同时部署传统防火墙、IPS 和WAF 等多种安全设备更强的安全防护能力，可以抵御来源更广泛、操作更简便、危害更明显的应用层攻击。此外，还提供基于业务的风险报表，内容丰富直观，用户可实时了解网络和业务系统的安全状况，有效提升管理效率、降低运维成本。

全状态检测防火墙　网络应用协议分析　Web应用防护

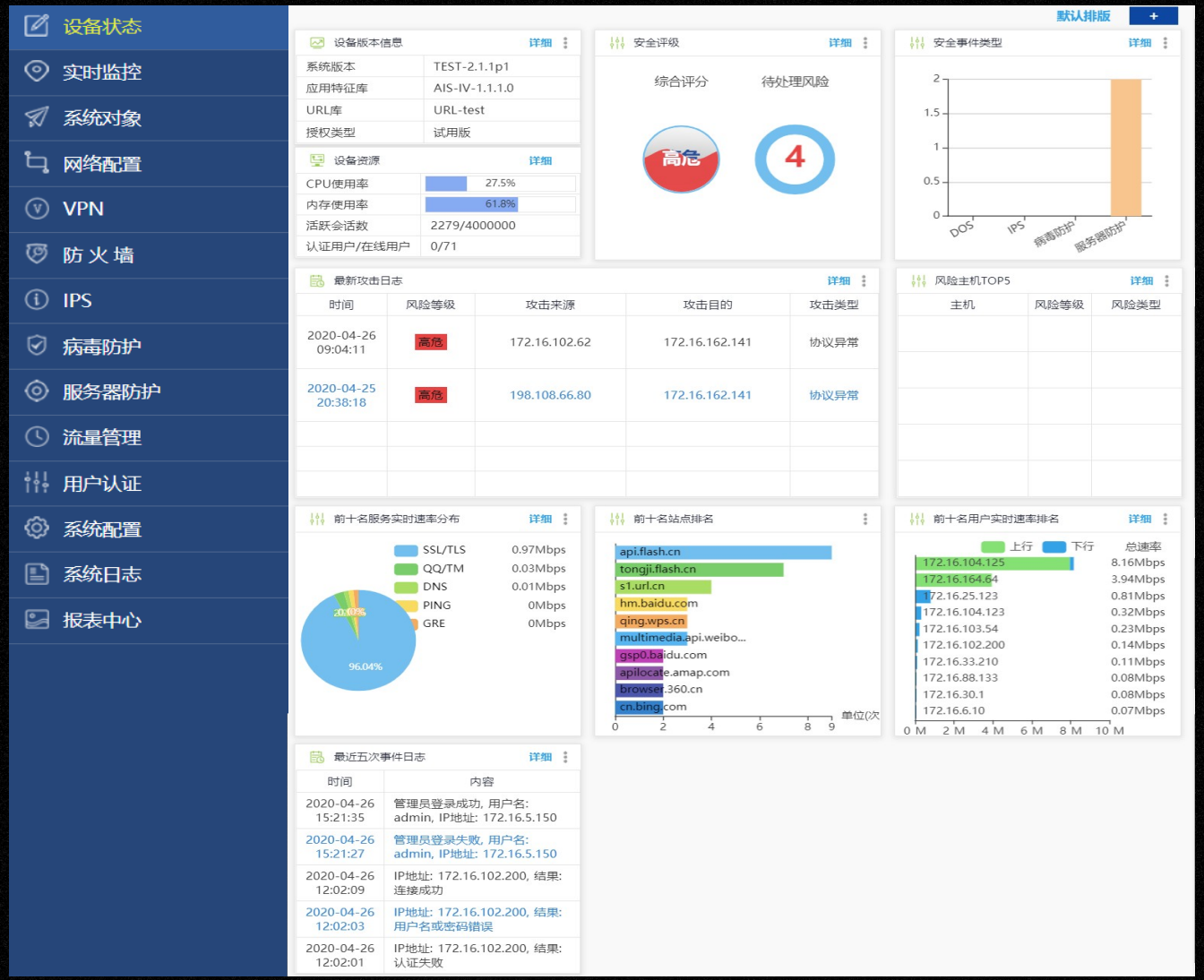
IPS入侵防御　网络防病毒　流量控制

特色技术

- 完备的基本防火墙特性
- 针对APT攻击和僵尸网络的检测
- 全方位应用洞察与控制
- 直观呈现业务系统安全风险

下一代防火墙主要功能

- 网络服务
- VPN功能
- 防火墙功能
- 高级防护
- 流量控制
- 用户认证
- 日志与报表



02 下一代防火墙基本上线配置（路由&网桥）

初始登录方式

设备默认使用ETH0作为网管口，ETH0出厂地址为192.168.0.1/24。设备默认使用安全的HTTPS方式登录Web UI，默认端口9090，初始登录 URL 为：https://192.168.0.1:9090

默认的管理员账号是admin，密码是admin*PWD。正确输入用户名和密码后，点击<登录>按钮即可进入管理界面。

路由部署的典型应用环境是将防火墙设备以路由模式部署在公网出口，代理内网上网，类似于一个路由器一样部署在网络中。外网口接ADSL拨号或者公网线路，内网口接内网交换机。

路由模式配置-静态IP

第一步：设置接口/安全区域

登录防火墙设备，进入【网络配置】>【安全区域】，本图中使用ETH2作为内网口，ETH3作为外网口。

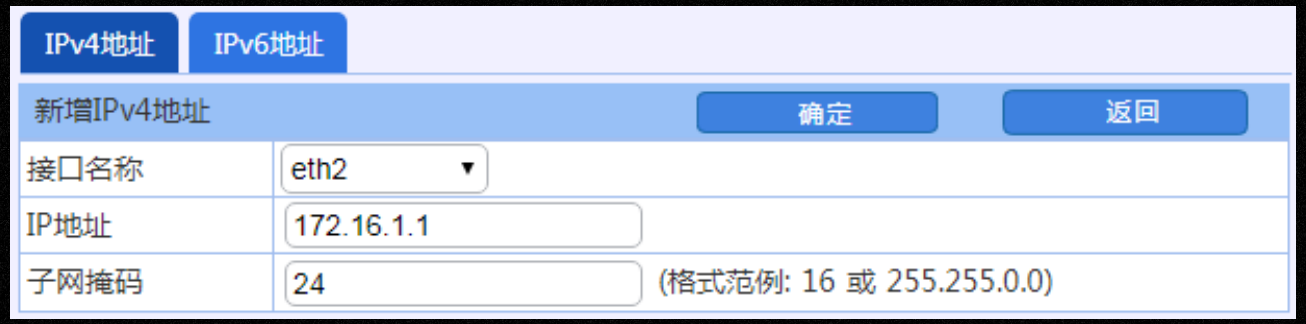
配置如下图：

配置ETH2

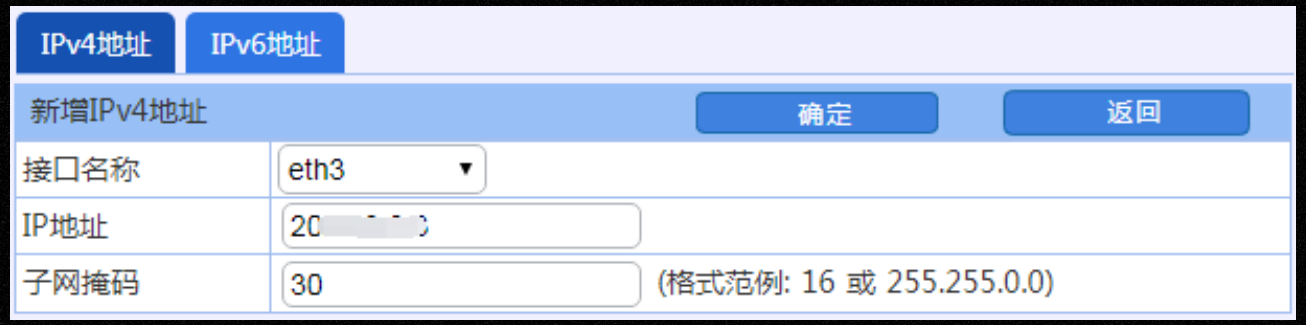
配置ETH3

第二步：配置IP地址。

进入【网络配置】>【配置IP地址】，配置如下图：



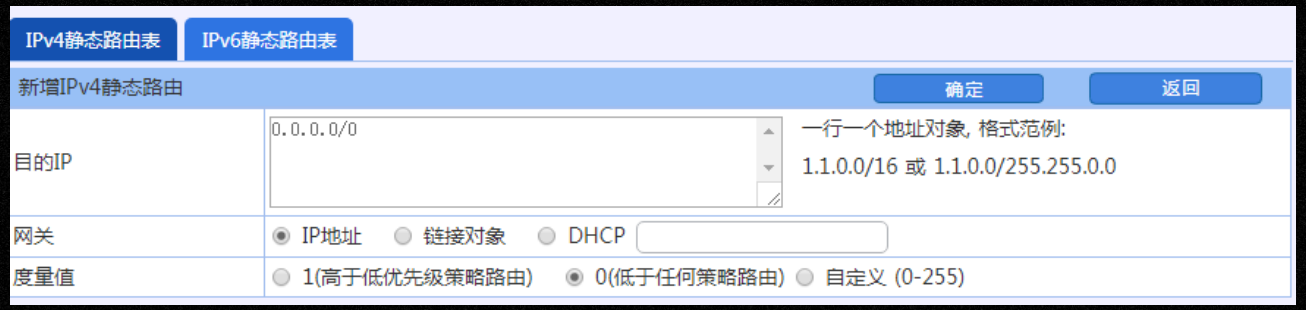
配置ETH2 IP地址



配置ETH3 IP地址

第三步：设置缺省路由

进入【网络设置】>【静态路由】，新增IPv4静态路由，目的IP默认全部，网关为下一跳IP地址，度量值默认。配置如下图：



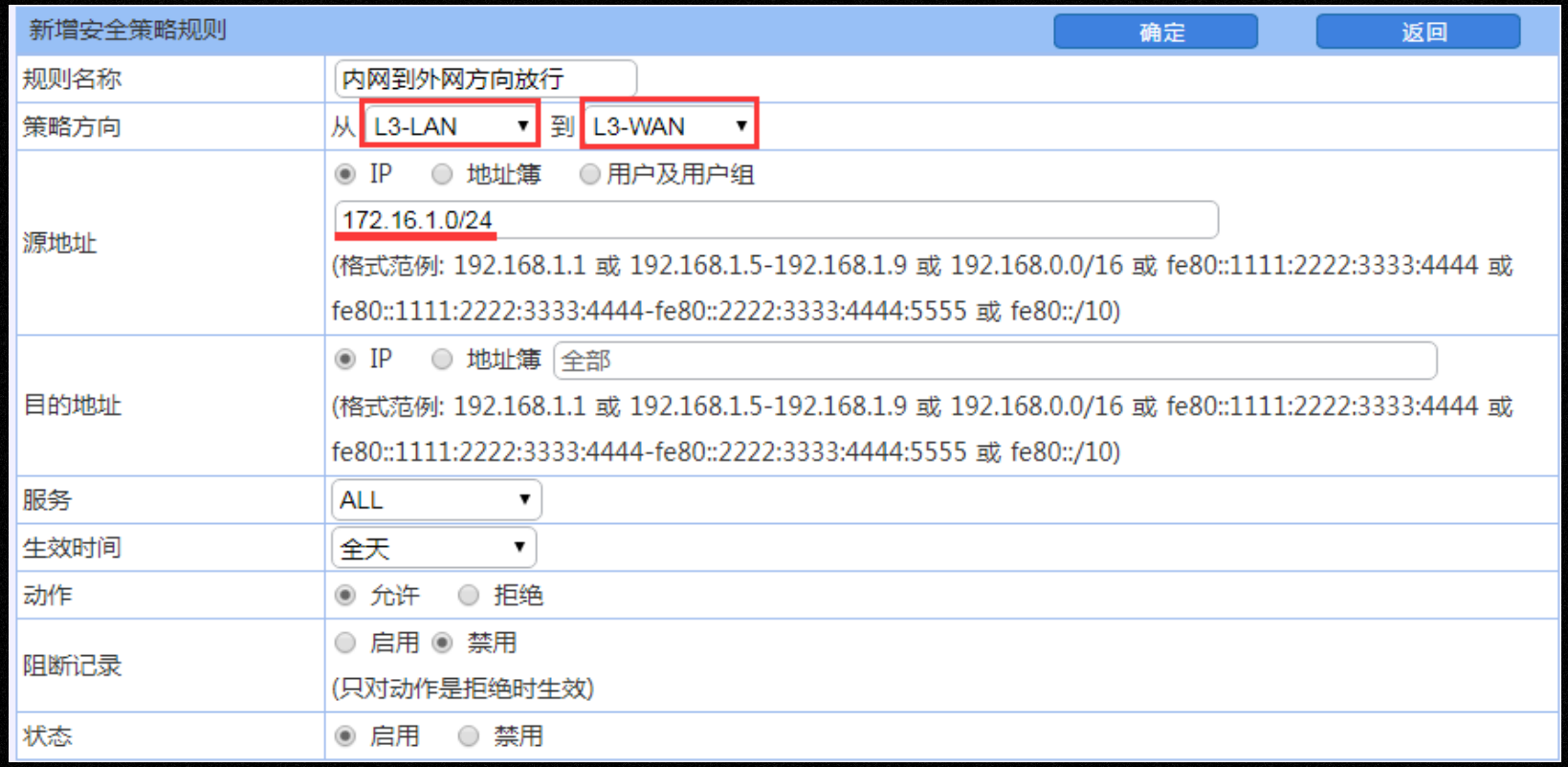
配置静态路由

提示：

内网接口接的跨三层的多个网段，需要在下一代防火墙上添加到各网段的静态路由到三层交换机。

第四步：安全策略放行

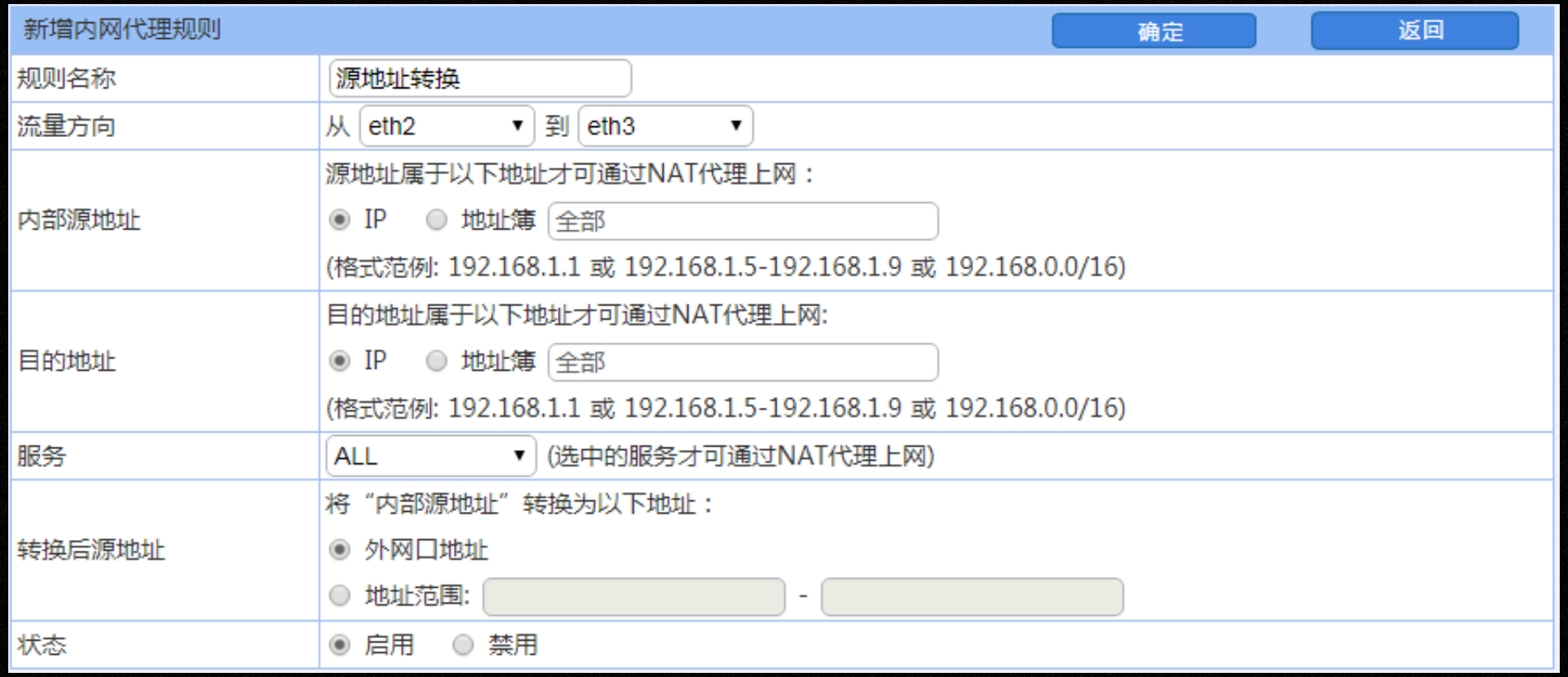
防火墙系统默认拒绝所有流量（阻挡规则在页面不显示），按需指定放行规则。进入【防火墙】>【安全策略】，策略方向L3-LAN→L3-WAN，源地址推荐配置内网口网段，目的地址默认全部。配置如下图：



配置安全策略

第五步：配置NAT规则，即源地址转换

进入【防火墙】>【NAT规则】>【内网代理】，流量方向为内网口到外网口，本文流量方向ETH2→ETH3，源目地址（也可指定源地址范围）以及其它参数均可默认，配置如下图：



配置NAT规则

路由模式配置-PPPoE拨号

第一步：设置接口/安全区域

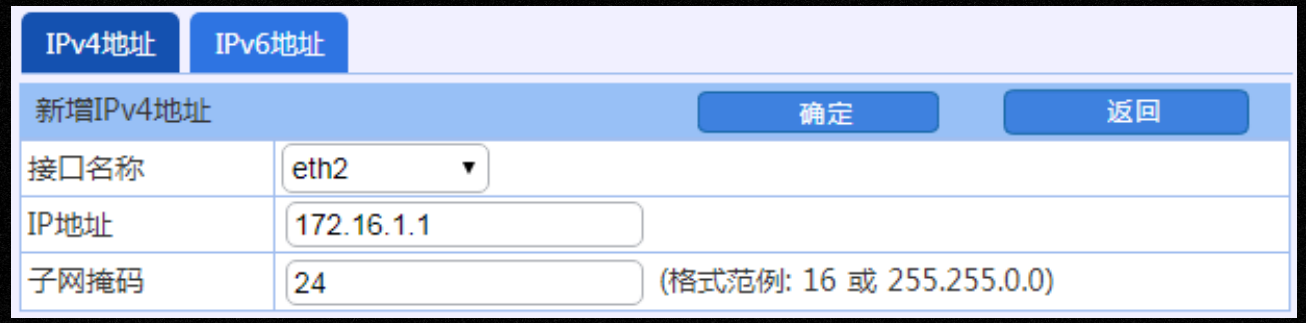
进入【网络配置】>【安全区域】，本图中使用ETH2作为内网接口，ETH3作为外网口，配置如下：

配置ETH2

配置ETH3

第二步：配置IP地址

进入【网络配置】>【配置IP地址】，配置如下图：



配置ETH2 IP地址

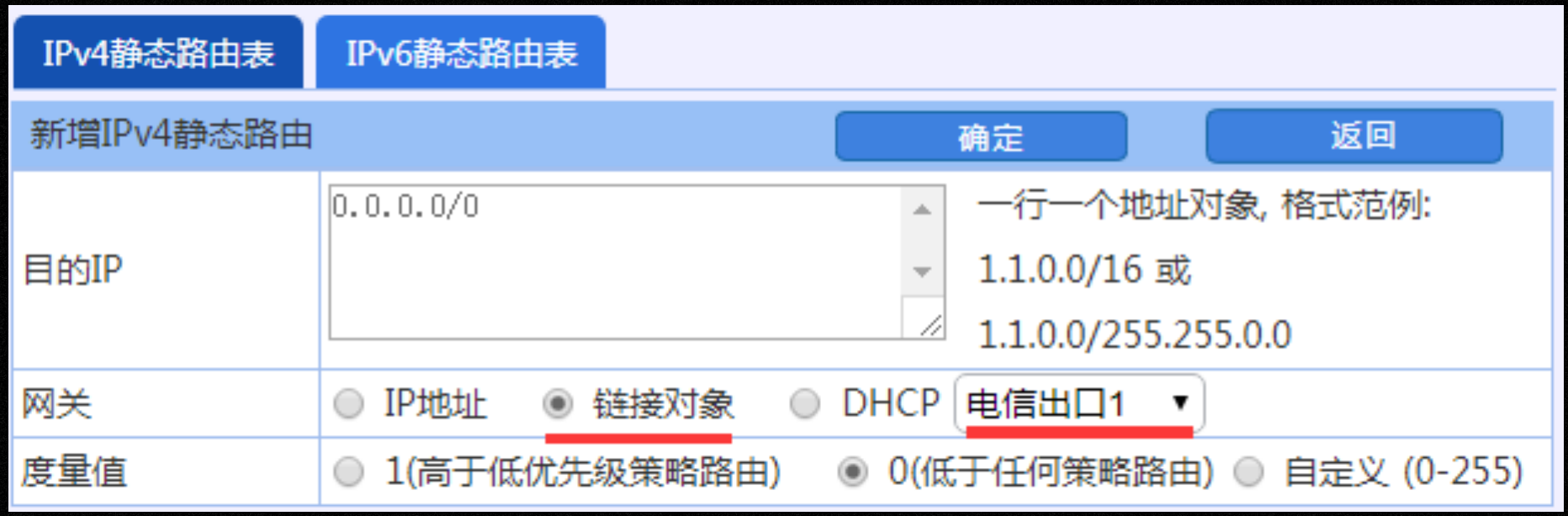
第三步：配置PPPoE拨号参数

进入【网络配置】>【链接对象】，配置如下图：

配置PPPoE参数

第四步：配置缺省路由

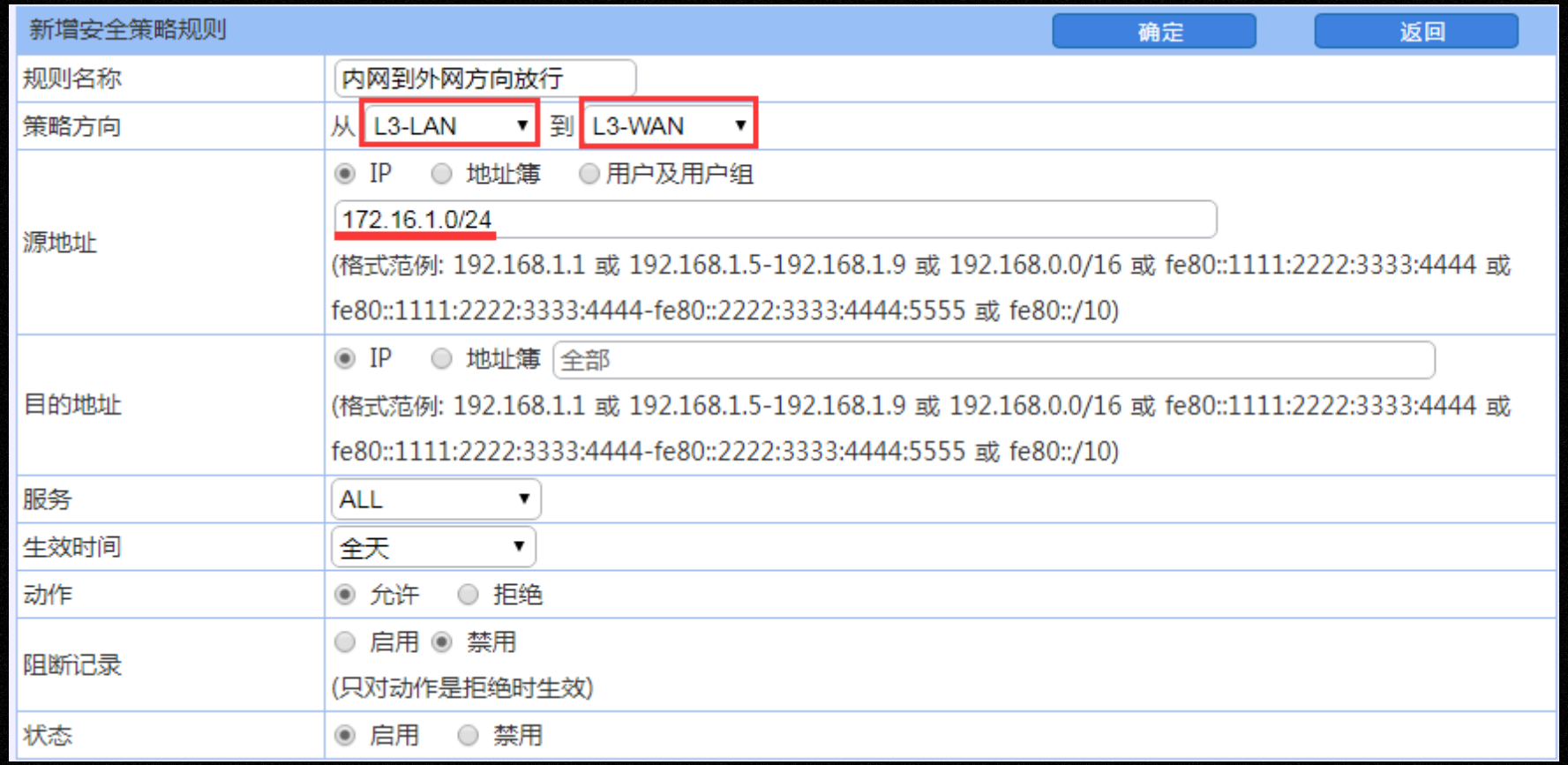
进入【网络配置】>【静态路由】，目的IP默认全部，网关选择链接对象，下拉框选择PPPoE规则名称“电信出口1”，度量值默认即可。



配置缺省路由

第五步：安全策略配置

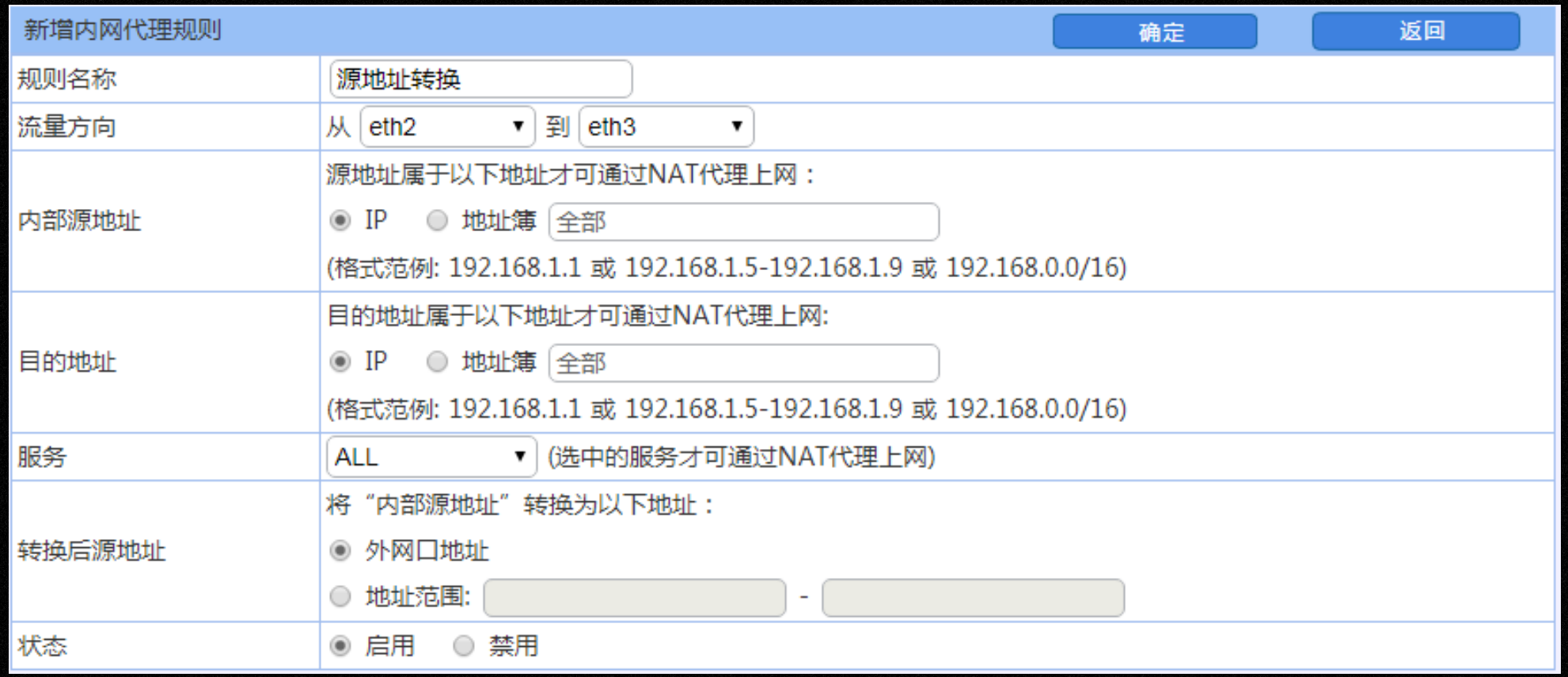
防火墙系统默认拒绝所有流量（规则在页面不显示），需指定放行规则。进入【防火墙】>【安全策略】，策略方向为L3-LAN→L3-WAN，源地址推荐配置内网网段，目的地址默认全部，配置如下图：



配置安全策略

第六步：配置NAT规则，即源地址转换

进入【防火墙】>【NAT规则】>【内网代理】，流量方向内网口到外网口，本文流量方向ETH2→ETH3，源目地址（也可指定源地址范围）以及其它参数均可默认。

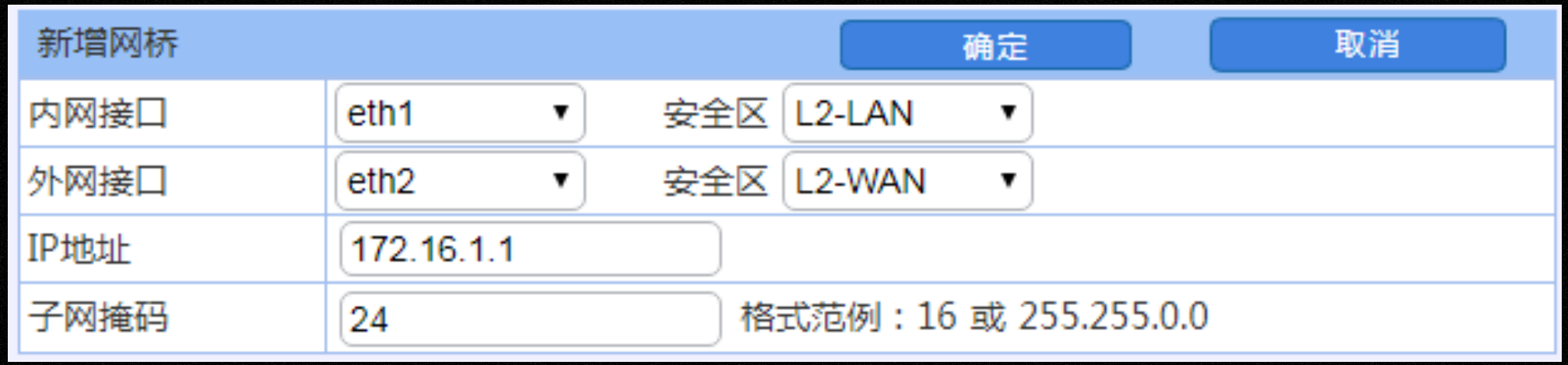


配置NAT规则

当数据进出下一代防火墙设备的网口处于网桥接口模式时，设备可视为一根带过滤功能的网线。一般在不方便更改原有网络拓扑结构的情况下使用，通常串接防火墙和核心交换机之间，不要更改原有网关及内网用户的配置，对下一代防火墙设备进行一些基本配置即可使用，网桥模式的主要特点是对用户做到完全透明。

第一步：设置网桥接口

进入【网络配置】>【接口配置】>【网桥】，新增网桥，内网接口/外网接口分别为ETH1/ETH2，安全区默认，并设置IP地址，配置如下图：



配置网桥接口

第二步：安全策略配置

防火墙系统默认拒绝所有流量（规则在页面不显示），需指定放行规则。

进入【防火墙】>【安全策略】，策略方向L2-LAN→L2-WAN，源地址推荐配置内网口网段，目的地址默认全部，配置如下图：

新增安全策略规则 [确定] [返回]

规则名称	桥模式数据放行
策略方向	从 L2-LAN 到 L2-WAN
源地址	IP 地址簿 用户及用户组 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16 或 fe80::1111:2222:3333:4444 或 fe80::1111:2222:3333:4444-fe80::2222:3333:4444:5555 或 fe80::/10)
目的地址	IP 地址簿 全部 (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16 或 fe80::1111:2222:3333:4444 或 fe80::1111:2222:3333:4444-fe80::2222:3333:4444:5555 或 fe80::/10)
服务	ALL
生效时间	全天
动作	允许 拒绝
阻断记录	启用 禁用 (只对动作是拒绝时生效)
状态	启用 禁用

配置安全策略

第三步：静态路由设置

按需选择，如果防火墙设备下面有核心交换机，需要配置回执路由，下一跳指向核心交换机。配置完毕后，将设备接入网络中，ETH1口接内网设备，ETH2口接上联出口设备。

提示：

1.网桥接口设置IP，主要用途有：网管、重定向认证页面、重定向阻挡提示页面；

2.网桥接口也可以不设置IP地址，可以用管理口来做带外管理；前提是终端和防火墙管理口之间路由可达。

03 常见问题排查

常见问题点

1、当涉及到物理接口需要DHCP或者PPPoE拨号使用时，在【网络配置】>【链路对象】进行创建虚拟端口，然后绑定到指定的物理接口即可；

2、PPPoE拨号或者DHCP获取模式下，终端用户上不了网，需查看默认路由配置，是否出口路由接入配置错误，在此模式下需要将默认路由出口指定创建的虚拟接口上，而不是物理接口；

3、日志中查看不到内网用户的上网信息，全是外网IP的话，这个内外接口接反，需确认连线接口；

4、因交接或时间久远，忘记登录密码时，可使用串口线连接console口进行恢复：

1）使用console线登录设备，输入用户名：recovery　密码：root*PWD

2）登录后上下键选择菜单账号“Reset WebUI Password”，回车，

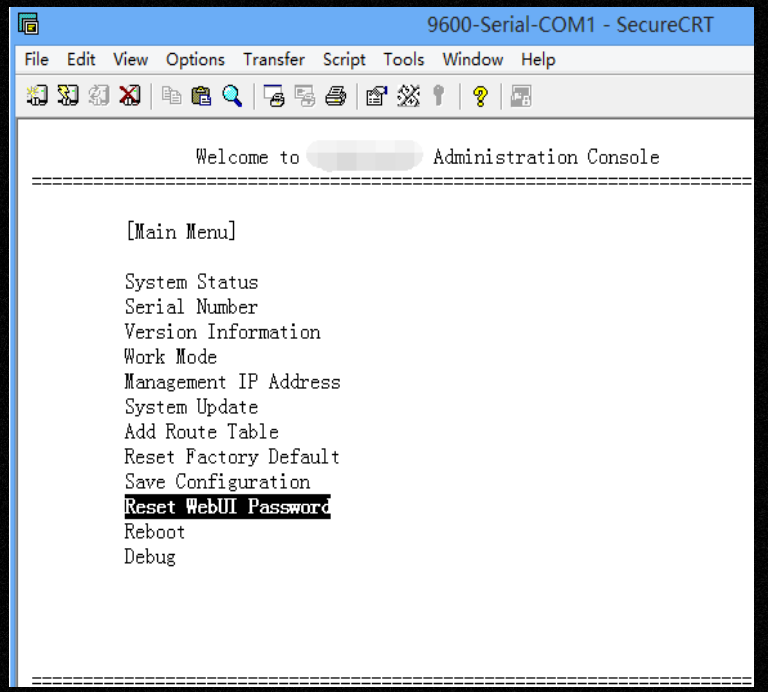
提示“Are you sure(Y-yes,N-no):”

输入Y（不区分大小写）

重置完成，提示“Note:Reset Success!”,菜单自动返回。

3）选择菜单“Save Configuration”，回车，保存配置。

4）“Reboot”重启即可。



DAZOO

www.idazoo.com 深圳市宝安区创维创新谷2A栋 400 856 0968