防火墙基础组网配置典型配置案例

NAT NAT444 PPPoE DHCP 设备部署方式 **只会安装的工程师** 2024-08-23 发表

组网及说明

防火墙当前是我们经常使用到的网络安全设备，通常我们会将防火墙部署在网络的出口处作为内网与外网的隔离设备。

部署模式

1、路由部署

路由部署的模式中，防火墙墙通常需要配置出口IP地址、内网接口IP地址、安全策略、出口NAT、NAT端口映射、NAT回流、IP路由表等配置；

2、透明部署

透明部署向较于路由部署，就相对简单，通常只需要配置接口模式和配置安全策略即可；

路由模式举例

1、拓扑

配置步骤

3、配置步骤

拓扑展示了当前小型局域网的典型拓扑结构，通常比较复杂的配置都在出口防火墙上，对于核心交换机和接入交换而言通常的配置一般也只有创建vlan和vlan虚拟IP的配置通常相对简单，案例中不做解释；

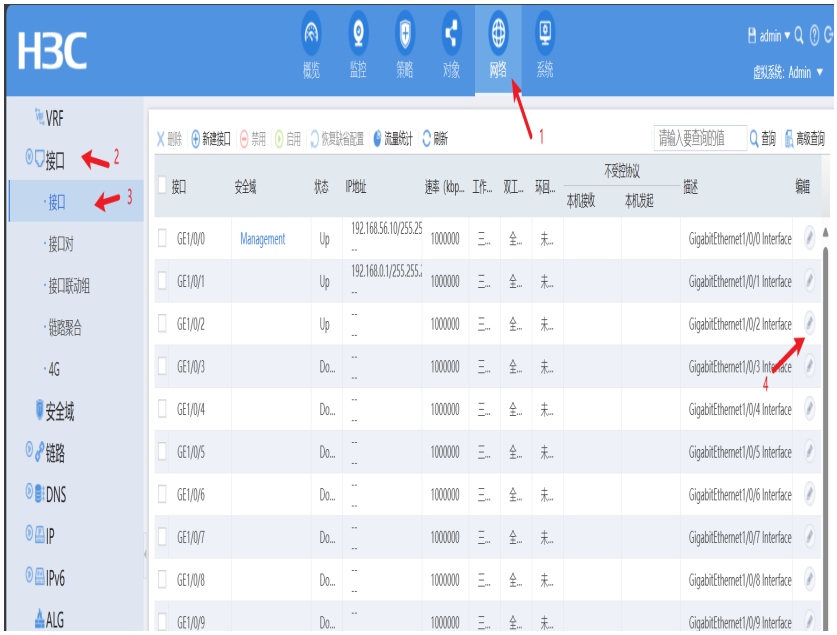
1、防火墙配置IP地址

小型组网中出口上网通常只有三种模式

1.1固定IP上网如拓扑所示，运营商会提供上网的固定IP地址、掩码、网关等信息，我们需要做的就是将网线或光纤插入防火墙上对应的端口就行；

注意:防火墙一般会有一个默认管理接口和默认管理地址，将调试电脑用网线插入默认管理口电脑配置和默认管理地址同网端的地址即可通过网页登录防火墙


不安全 | https://192.168.56.10/web/frame/login.html?ssl=false
办公lite
书签工具栏
第0章 咱们先来谈谈...
EVE | Login
QQ邮箱 - 写信
子网划分工具--子网...
流程日志
H3C
数字化解决方案领导者
安全产品管理平台
admin
记住用户名
中文
登录
其他登录方式


H3C
概览
监控
策略
对象
网络
系统
admin
虚拟系统: Admin
VRF
接口
接口
接口对
接口联动组
链路聚合
4G
安全域
链路
DNS
IP
IPv6
ALG
新建接口
禁用
启用
恢复缺省配置
流量统计
刷新
请输入要查询的值
查询
高级查询
接口
安全域
状态
IP地址
速率 (kbp...
工作...
双工...
环回...
不受控协议
本机接收
本机发送
描述
编辑
1
2
3
4

1.2DHCP上网通常指的的是在防火墙外网口处还有网关设备。可能是其他的网关设备或者是已经拨了号的光猫设备，

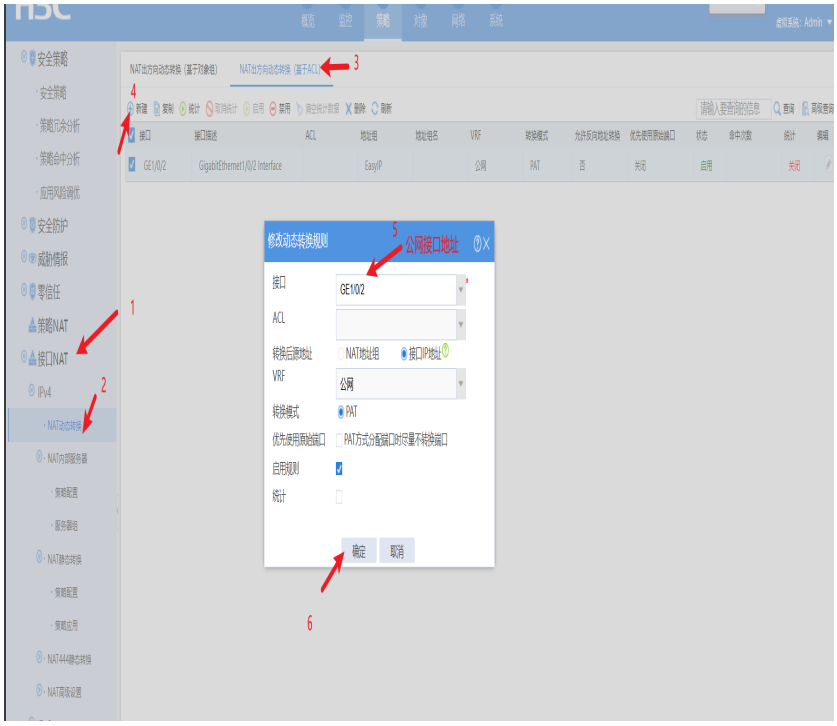
1.3PPPOE通常是我们说的拨号上网，我们只需要填入拨号的账号密码即可

1.4内网通常都是固定IP配置和出口地址配置方法相同

2、配置出口NAT和路由表

2.1NAT又叫地址转换是目前上网的强制配置华三的防火墙有两种配置方式 策略NAT 和接口NAT 但是两者不能公用，一般建议用接口NAT方式

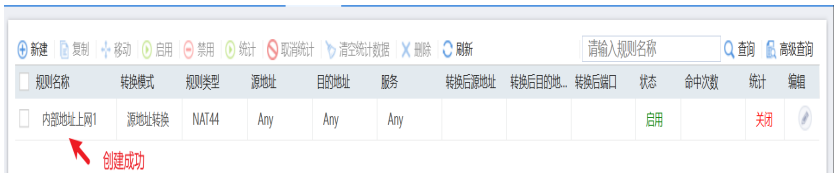
2.2.1接口NAT方式


修改动态转换规则
接口
GE1/0/2
ACL
转换后源地址
NAT地址组
接口IP地址
VRF
公网
转换模式
PAT
优先使用原始端口
PAT方式分配端口时尽量不转换端口
启用规则
统计
确定
取消
1
2
3
4
5 公网接口地址
6

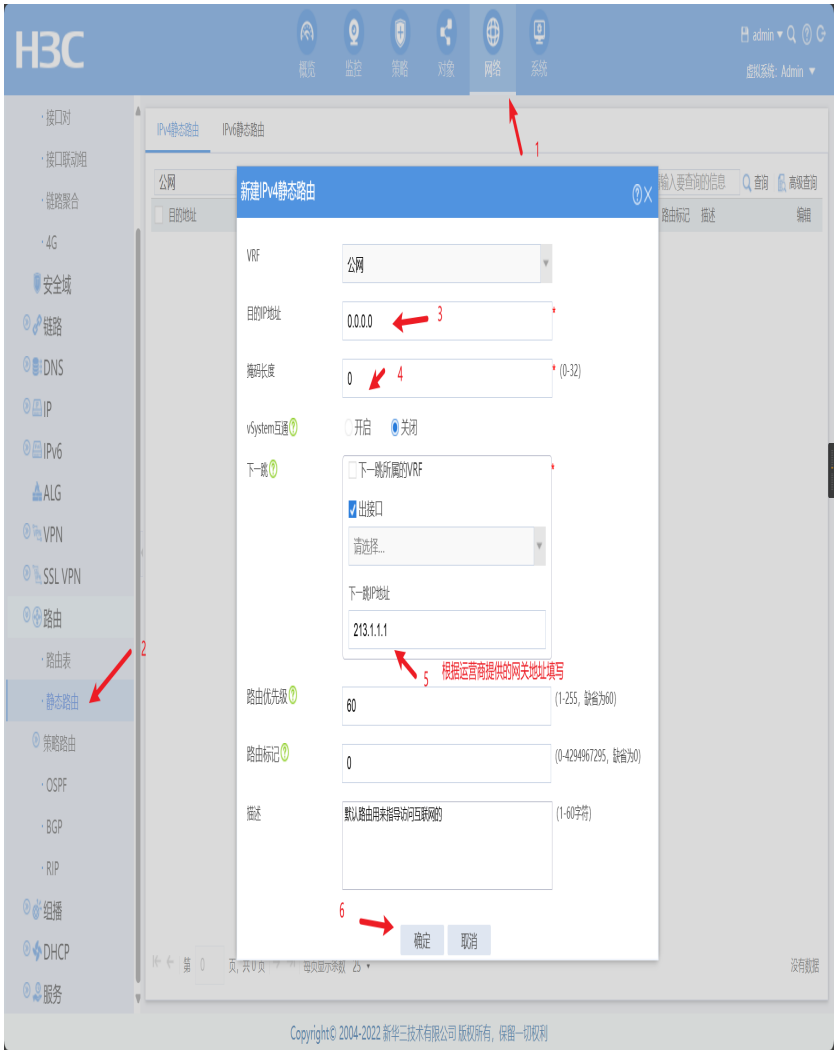

NAT出方向动态转换（基于对象组）
NAT出方向动态转换（基于ACL）
GE1/0/2
GigabitEthernet1/0/2 Interface
EasyIP
公网
PAT
否
关闭
启用
关闭
配置成功

2.2.2策略NAT方式


H3C
概览
监控
策略
对象
网络
系统
admin
虚拟系统: Admin
安全策略
策略NAT
接口NAT
新建策略NAT
规则名称
内部地址上网1
手工指定名称
规则描述
规则类型
NAT44
NAT64
NAT66
转换模式
源地址转换
5 选择可以上网的区域
源安全域
Trust, Local
目的安全域
Untrust
源地址
地址
地址对象组
目的地址
可以手动指定
也可以默认不指定
服务
请选择服务
转换方式
确定
取消
1
2
3
4
5
6
7
Copyright© 2004-2022 新华三技术有限公司 版权所有，保留一切权利



2.2网络通信处理需要IP地址以外还需要路由表信息来指导数据转发，根据拓扑所示我们需要添加两条静态路由(实际情况根据规划地址写路由)


H3C
概览
监控
策略
对象
网络
系统
admin
虚拟系统: Admin
接口对
接口联动组
链路聚合
4G
安全域
链路
DNS
IP
IPv6
ALG
VPN
SSL VPN
路由
路由表
静态路由
策略路由
OSPF
BGP
RIP
组播
DHCP
服务
IPv4静态路由
IPv6静态路由
公网
目的地址
输入要查询的信息
查询
高级查询
路由标记
描述
编辑
新建IPv4静态路由
VRF
公网
目的IP地址
0.0.0.0
掩码长度
0
(0-32)
vSystem互通
开启
关闭
下一跳
下一跳所属的VRF
出接口
请选择...
下一跳IP地址
213.1.1.1
根据运营商提供的网关地址填写
路由优先级
60
(1-255, 缺省为60)
路由标记
0
(0-4294967295, 缺省为0)
描述
默认路由用来指导访问互联网的
(1-60字符)
确定
取消
1
2
3
4
5
6
第 0 页, 共 0 页
每页显示条数
没有数据
Copyright© 2004-2022 新华三技术有限公司 版权所有, 保留一切权利

3、配置安全策略

安全策略是防火墙的核心功能，防火墙的的数据转发除了需要IP路由来指导转发以外还需要安全策略来指导数据的流向，并对不通的流量进行访问控制等精细化操作流程

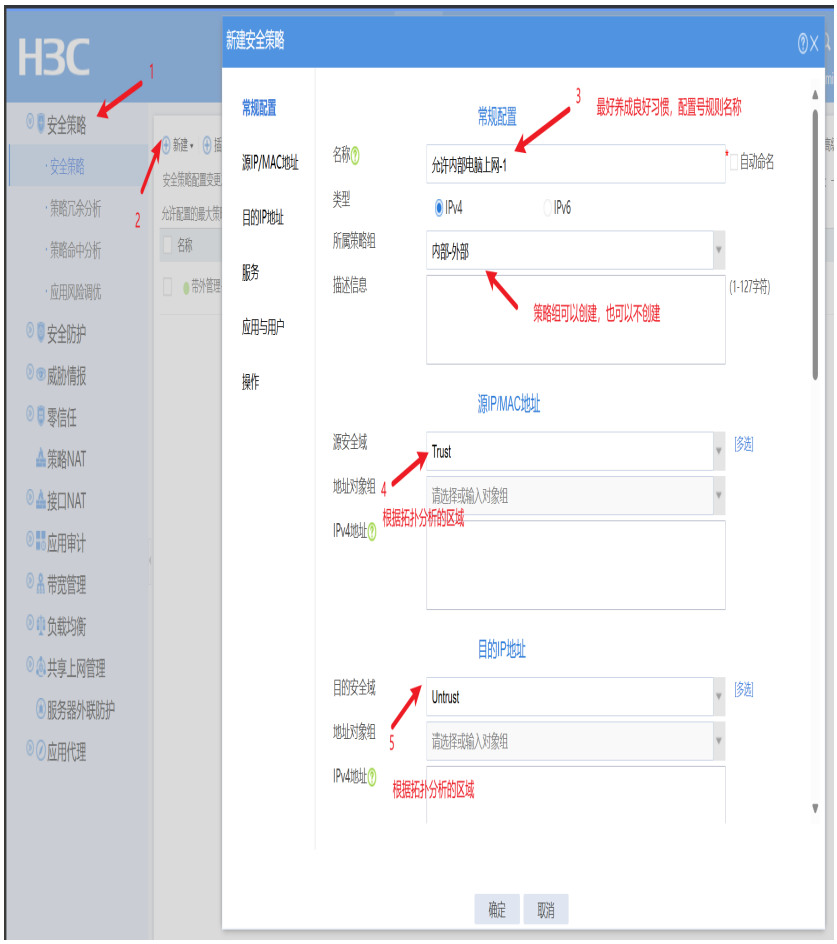
3.1安全策略

安全策略的匹配规则是从上到下匹配，第一条匹配不通过时匹配下一条，如果数据所有策略都没有匹配上的话那就不放行这这个流向的数据；

3.2允许电脑上网

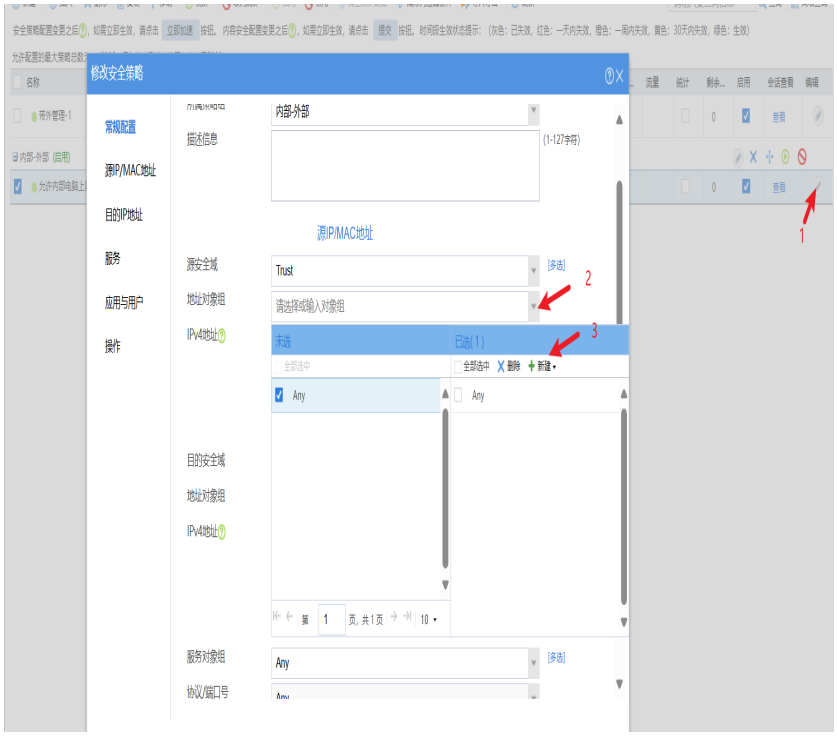
根据流量的分析，内部电脑上网的流量方向时trust到Untrust 的流量方向，所以我根据这个方向来编写策略；

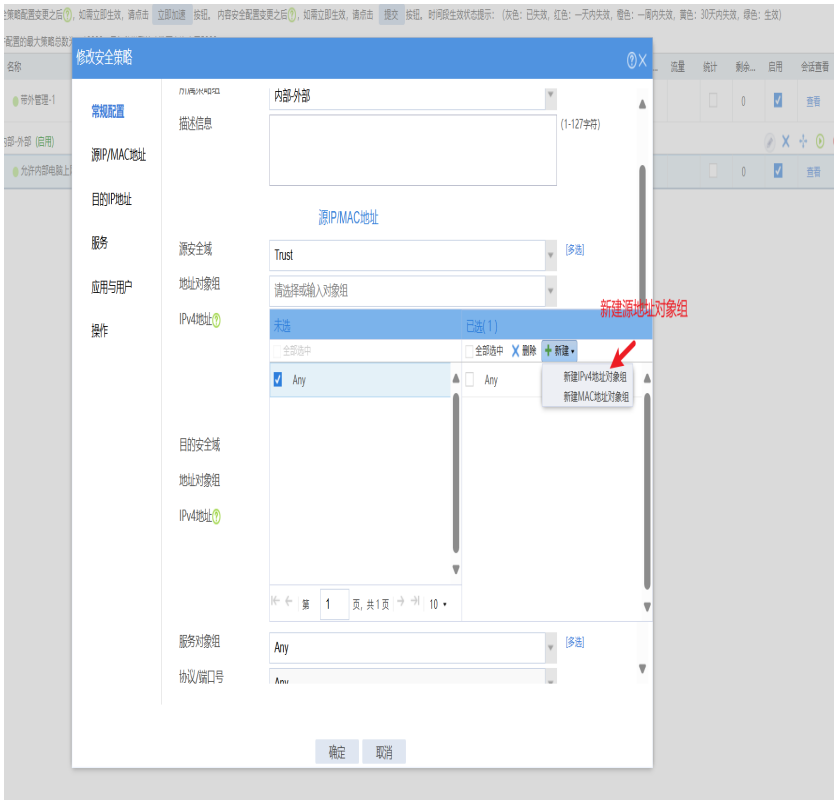

运营商网关设备
运营商网关地址：213.1.1.1 255.255.255.0
防火墙出口地址：213.1.1.2 255.255.255.0
出口路由器
防火内网地址：192.168.1.1 255.255.255.0
核心交换机与防火墙通信地址
192.168.1.2 255.255.255.0
电脑网关vlan 10
电脑网关 192.168.10.1 255.255.255.0
核心交换机
电脑上外网需求配置策略
接入交换机
电脑地址 192.168.10.2 255.255.255.0
用户电脑


H3C
新建安全策略
常规配置
源IP/MAC地址
目的IP地址
服务
应用与用户
操作
安全策略
策略冗余分析
策略命中分析
应用风险调优
安全防护
威胁情报
零信任
策略NAT
接口NAT
应用审计
带宽管理
负载均衡
共享上网管理
服务器外联防护
应用代理
1
2
3
最好养成良好习惯，配置号规则名称
名称
允许内部电脑上网-1
自动命名
类型
IPv4
IPv6
所属策略组
内部-外部
描述信息
(1-127字符)
策略组可以创建，也可以不创建
源IP/MAC地址
源安全域
Trust
[多选]
地址对象组
4
请选择或输入对象组
根据拓扑分析的区域
IPv4地址
目的IP地址
目的安全域
Untrust
[多选]
地址对象组
5
请选择或输入对象组
IPv4地址
根据拓扑分析的区域
确定
取消

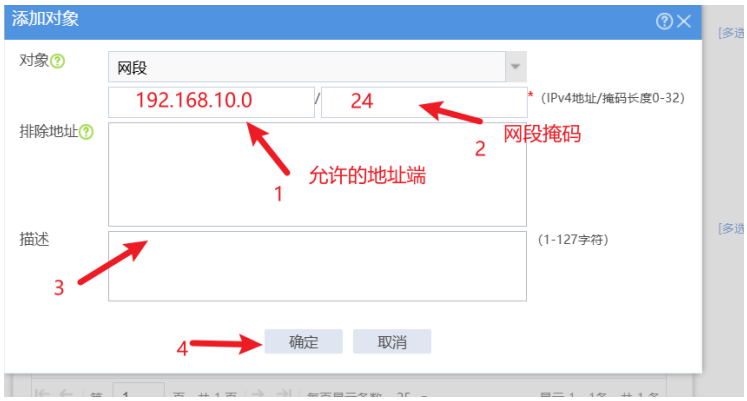
3.3通过对象设置，允许指定地址上网不在指定地址的地址则不能上网

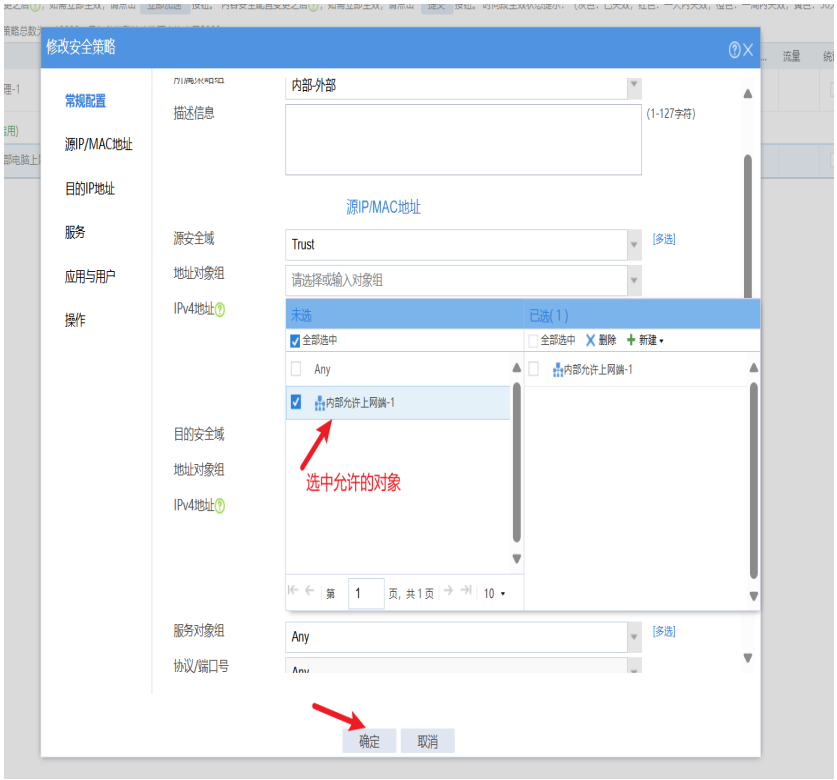
根据拓扑分析我们只需要允许源地址 192.168.10.0/24 网段目的网段为any 服务也any ,因为上互联网的所有不能指定目的地址和目的服务器类型；


修改安全策略
常规配置
源IP/MAC地址
目的IP地址
服务
应用与用户
操作
内部-外部
描述信息
(1-127字符)
源IP/MAC地址
源安全域
Trust
[多选]
地址对象组
请选择或输入对象组
IPv4地址
未选
已选(1)
全部选中
删除
新建
Any
目的安全域
地址对象组
IPv4地址
服务对象组
Any
协议/端口号
1
2
3


修改安全策略
常规配置
源IP/MAC地址
目的IP地址
服务
应用与用户
操作
内部-外部
描述信息
(1-127字符)
源IP/MAC地址
源安全域
Trust
[多选]
地址对象组
请选择或输入对象组
IPv4地址
未选
已选(1)
全部选中
删除
新建
新建源地址对象组
新建IPv4地址对象组
新建MAC地址对象组
Any
目的安全域
地址对象组
IPv4地址
服务对象组
Any
协议/端口号
确定
取消


新建IPv4地址对象组
建议养成良好习惯做好名称
对象组名称
内部允许上网端-1
(1-63字符)
描述
(1-127字符)
安全域
区域建议不选 选空
添加
删除
请输入要查询的信息
查询
类型
内容
排除地址
描述
编辑
网段
19.168.10.0/255.2...
办公一楼一层
添加允许的我网段
第 1 页，共 1 页
每页显示条数 25
显示 1 - 1条，共 1 条
确定
取消

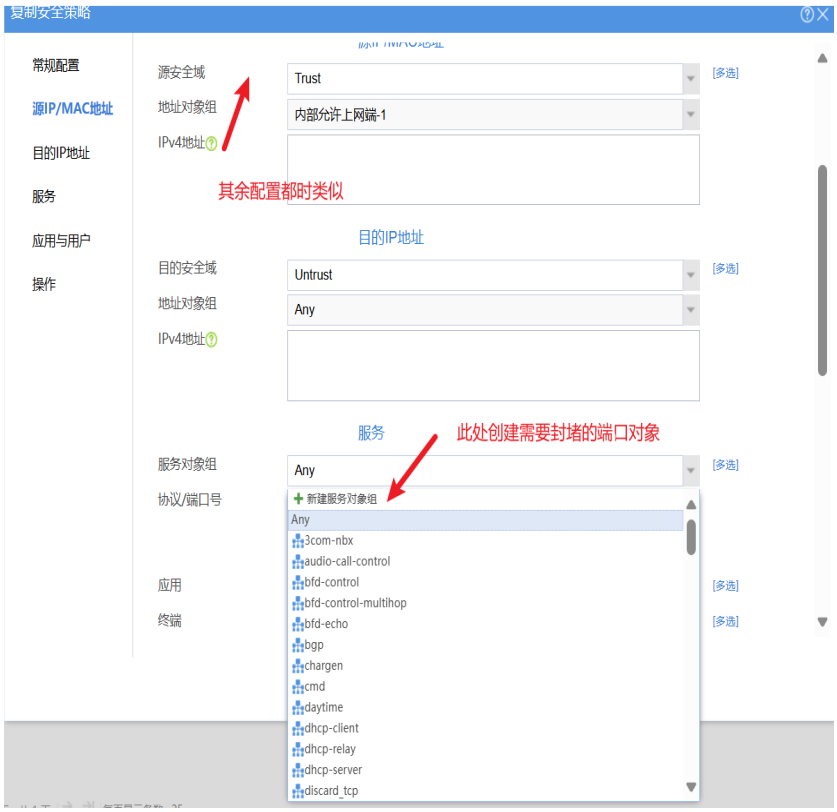

添加对象
对象
网段
192.168.10.0
/
24
(IPv4地址/掩码长度0-32)
排除地址
网段掩码
2
允许的地址端
1
描述
(1-127字符)
3
4
确定
取消

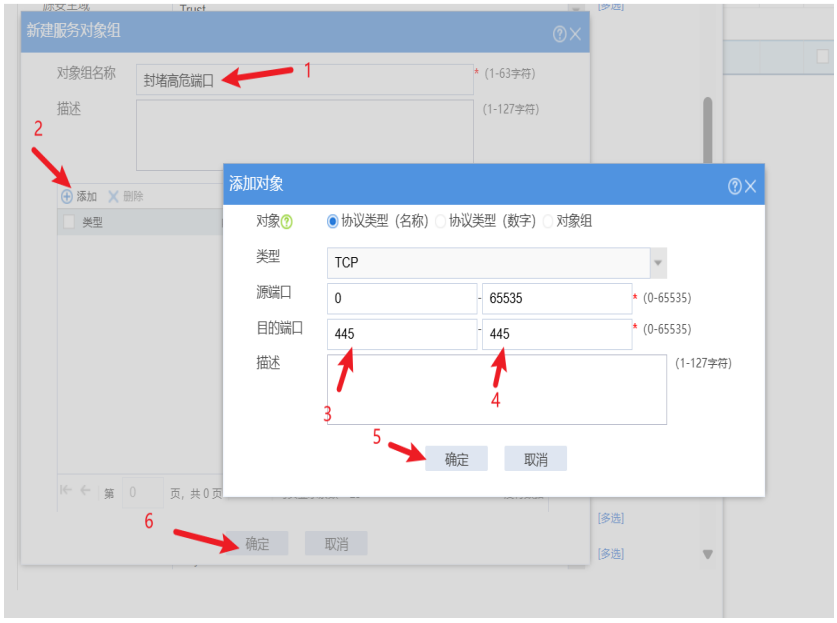

修改安全策略
常规配置
源IP/MAC地址
目的IP地址
服务
应用与用户
操作
内部-外部
描述信息
(1-127字符)
源IP/MAC地址
源安全域
Trust
[多选]
地址对象组
请选择或输入对象组
IPv4地址
未选
已选(1)
全部选中
删除
新建
Any
内部允许上网端-1
目的安全域
地址对象组
IPv4地址
选中允许的对象
第 1 页，共 1 页
10
服务对象组
Any
协议/端口号
确定
取消

3.4封堵高危端口

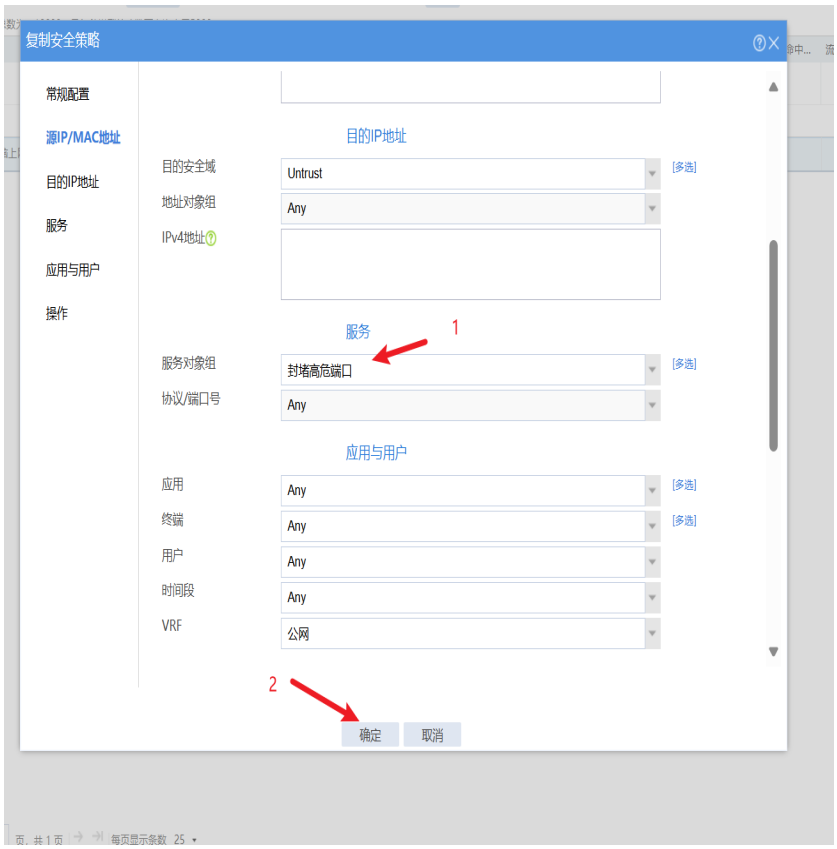
实际使用过程中通常会要求封堵一些服务和端口，但是我们要灵活分析编写规则。此处做几个举例配置

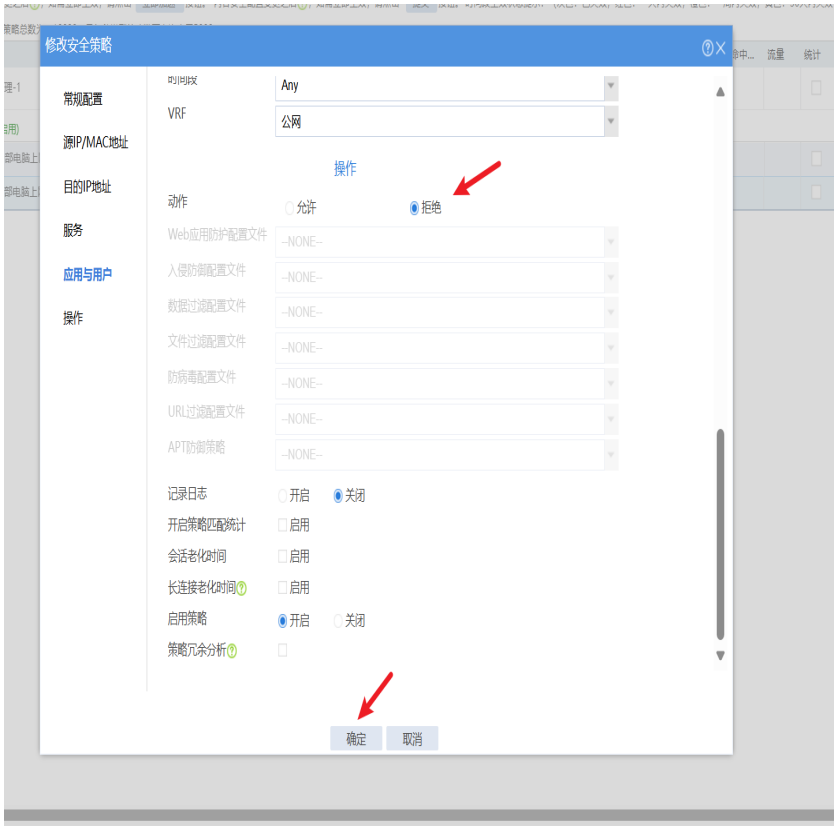
1.封堵内网到外网任意地址的445 端口





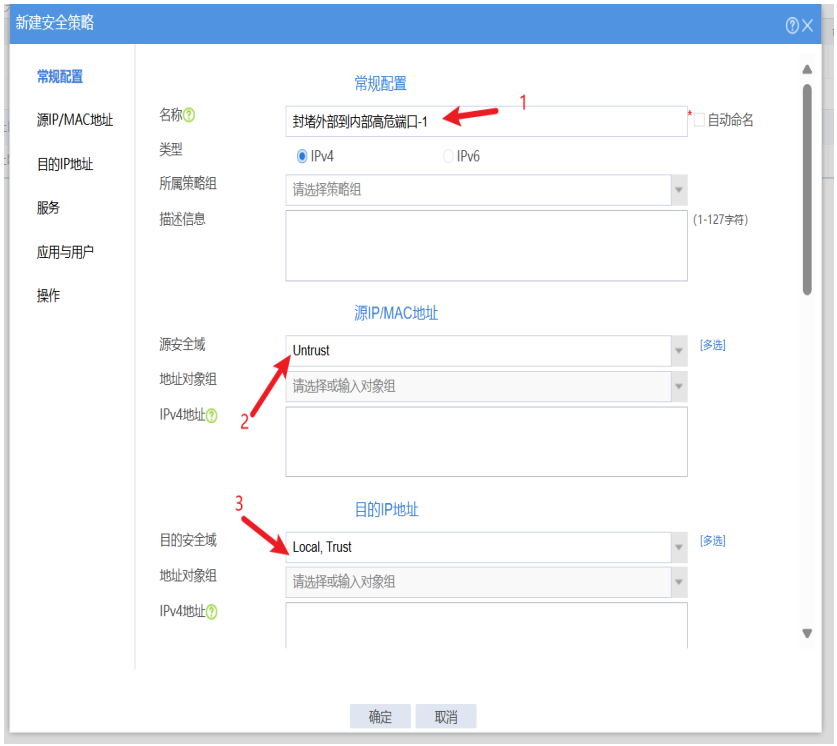

添加
删除
类型
TCP
1
添加对象
对象
协议类型（名称）
协议类型（数字）
对象组
类型
2
UDP
源端口
0
65535
(0-65535)
目的端口
445
445
(0-65535)
描述
3
4
(1-127字符)
确定
取消
5
第 1 页，共 1 页
确定
取消
[多选]
[多选]

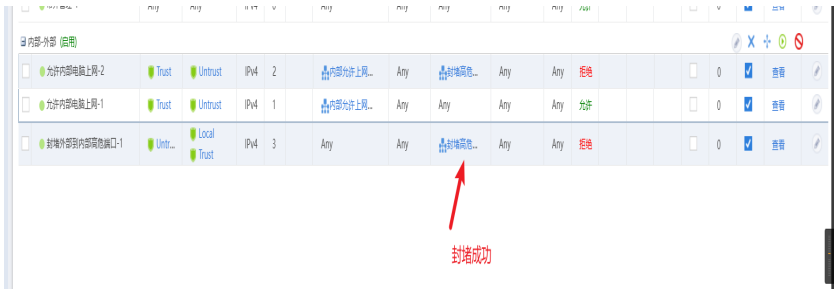

复制安全策略
常规配置
源IP/MAC地址
目的IP地址
服务
应用与用户
操作
目的IP地址
目的安全域
Untrust
[多选]
地址对象组
Any
IPv4地址
服务
1
服务对象组
封堵高危端口
[多选]
协议/端口号
Any
应用与用户
应用
Any
[多选]
终端
Any
[多选]
用户
Any
时间段
Any
VRF
公网
2
确定
取消
每页显示条数 25



2、封堵外网-到内网的高危端口

通常来说没得端口映射需求，不需要编写外网到内网的策略，再次注意对于防火墙来说只要没有没有匹配的策略就是拒绝，所以当需要封堵端口时要确定号流量的方向，然后根据方向通过区域来实现端口封堵。

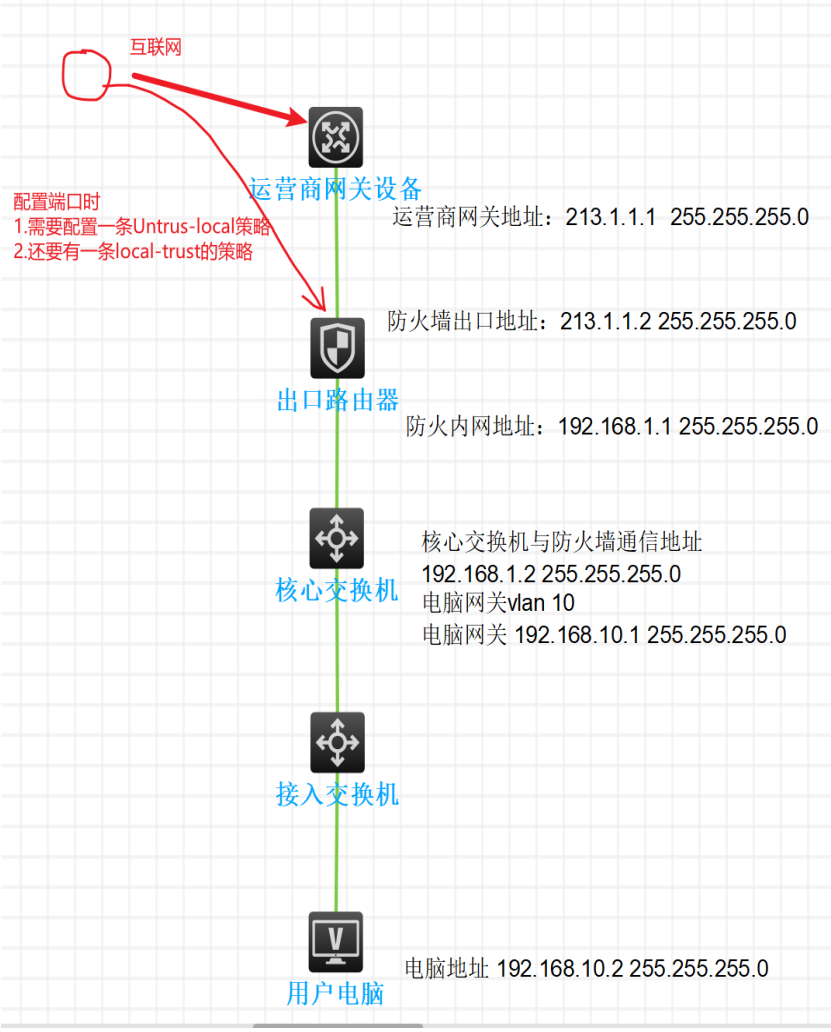




4、配置端口映射

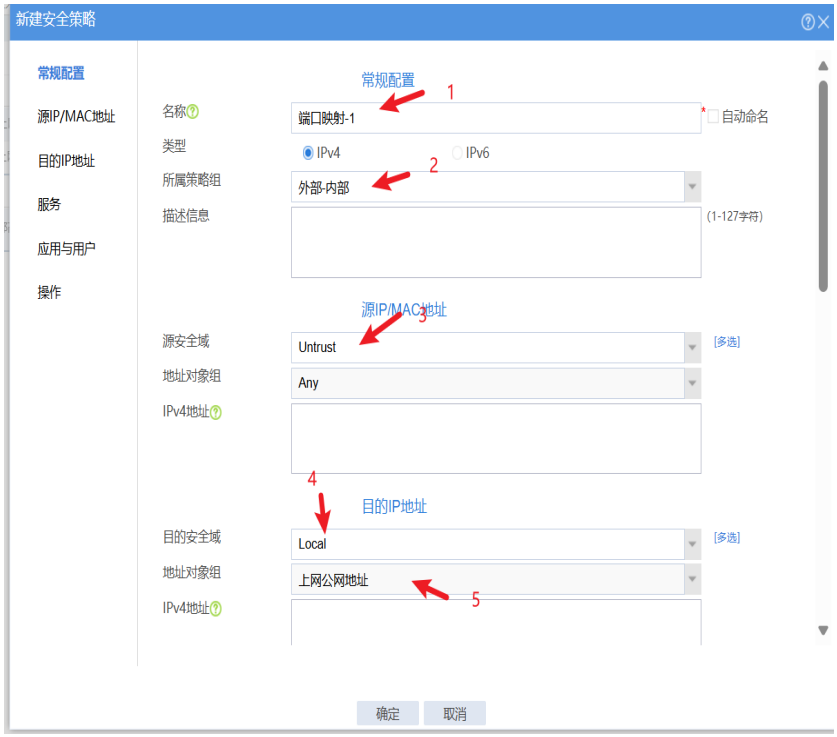
端口映射通常指的的内部办公网络有对外提供的某种服务，需要从互联网网访问

举例：映射192.168.10.2服务器的tcp 8443 端口

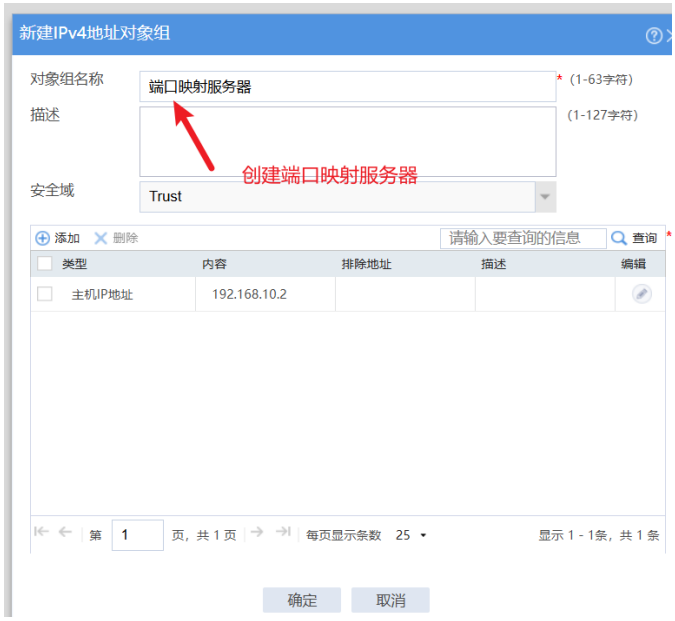


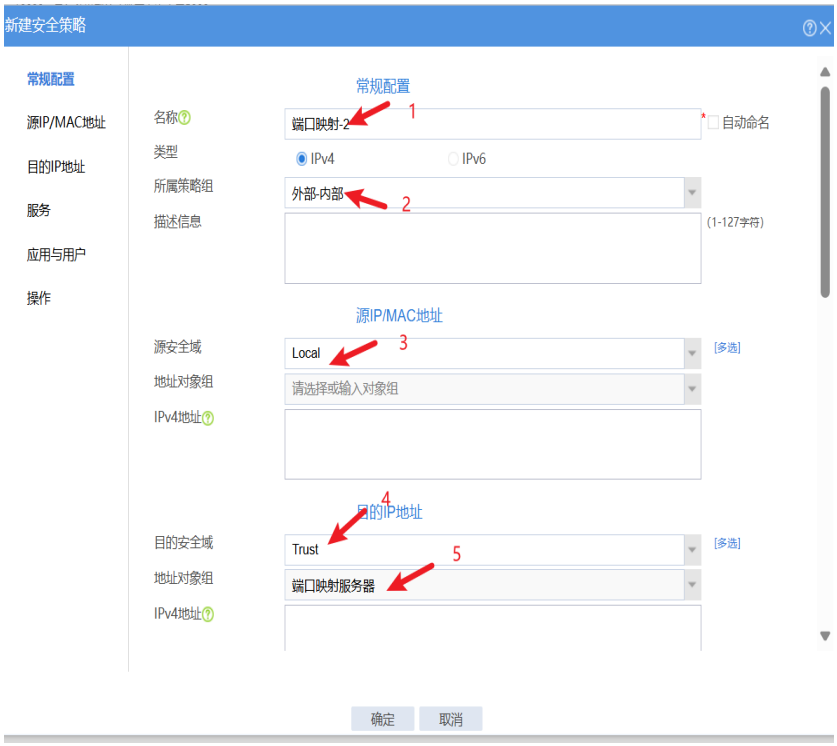
1、互访网发起的访问请求会先到防火墙本地，所以需要一条Untrus到local的安全策略


新建服务对象组
对象组名称
映射端口
(1-63字符)
描述
(1-127字符)
创建映射端口组
添加
删除
请输入要查询的信息
查询
类型
内容
描述
编辑
TCP
源端口0 - 65535, 目的端...
第 1 页，共 1 页
每页显示条数 25
显示 1 - 1条，共 1 条
确定
取消

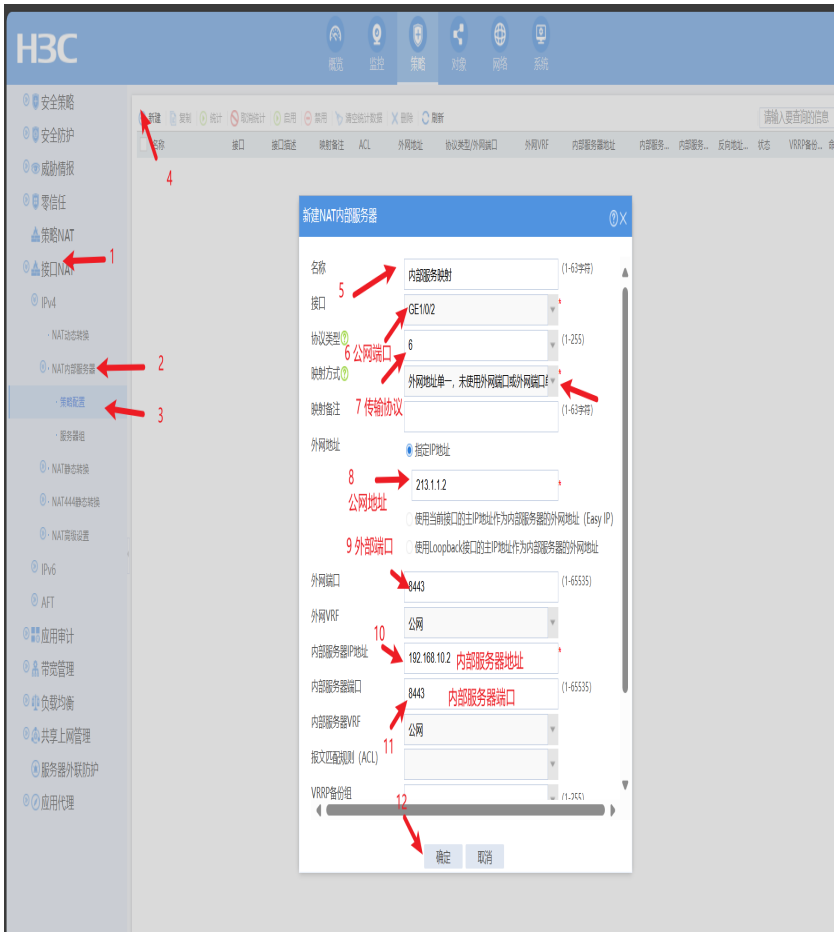

新建安全策略
常规配置
源IP/MAC地址
目的IP地址
服务
应用与用户
操作
常规配置
1
名称
端口映射-1
自动命名
类型
IPv4
IPv6
所属策略组
2
外部-内部
描述信息
(1-127字符)
源IP/MAC地址
3
源安全域
Untrust
[多选]
地址对象组
Any
IPv4地址
4
目的IP地址
目的安全域
Local
[多选]
地址对象组
上网公网地址
5
IPv4地址
确定
取消

2、流量到了防火墙时还需要有一条防火墙到内网的策略，所以要添加local-trust的策略





3.策略都添加完成后，开始配置端口映射策略,端口映射也有两种映射方式，一种只策略NAT的目的映射，另一种是接口NAT的内部服务器映射推荐应接口NAT方式



配置关键点

2、需求分析

1、配置接口IP

2、配置出口NAT和路由表

3、配置安全策略

4、配置端口映射