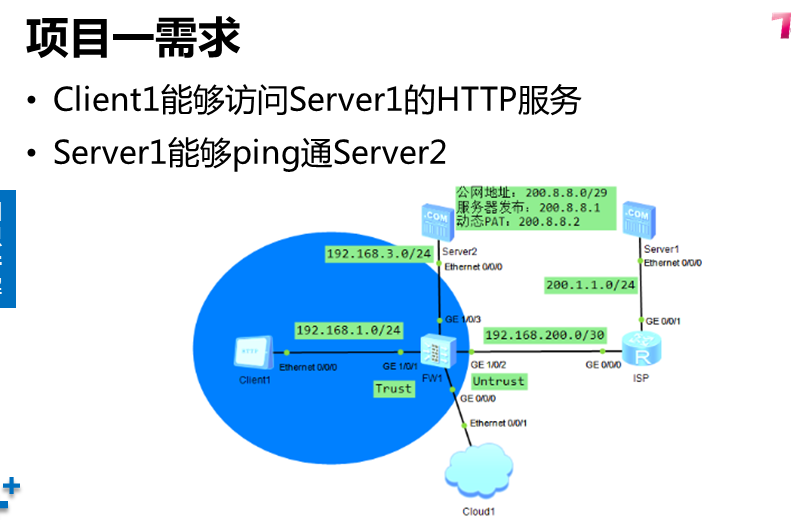
**彻底理解NAT**



配置步骤：

配置接口IP地址并将接口加入安全区域

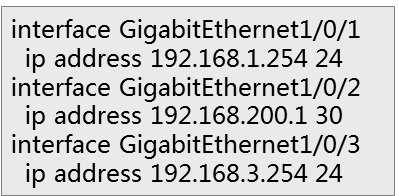
配置安全策略

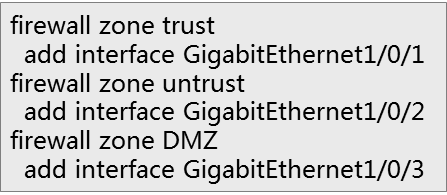
配置NAT策略

配置路由

路由环路问题

配置接口IP地址并加入安全区域







配置安全策略

Trush访问untrush

Untrush访问DMZ



配置NAT策略

配置NAPT

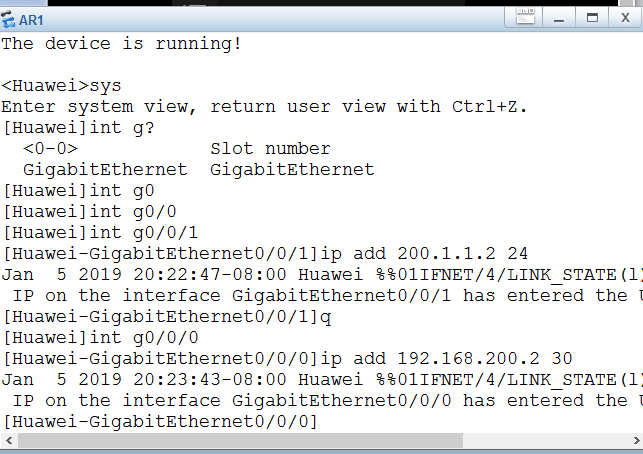




防火墙配置默认路由



ISP配置详细路由





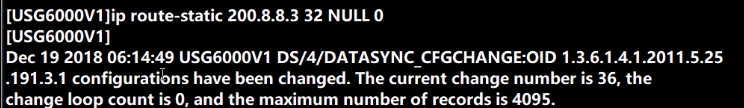
配置服务器发布



路由环路问题

G1/0/2接口抓包

防火墙配置黑洞路由

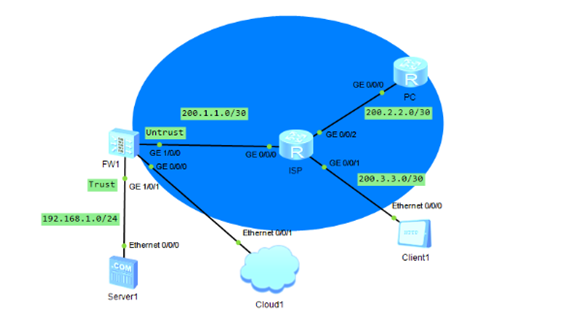


**防火墙NAT综合配置**

只有PC可以telnet到防火墙（ISP不能telnet防火墙）

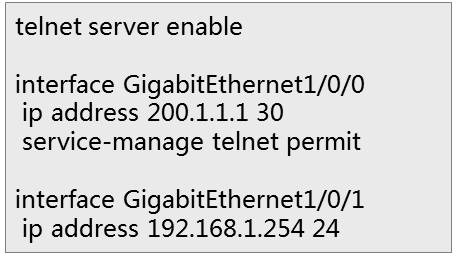
配置安全策略和服务器发布，client1可以访问server1的HTTP服务

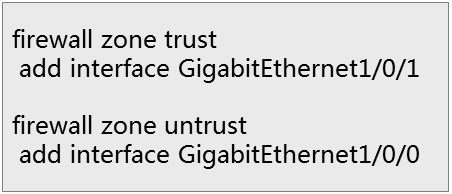
配置安全策略和easy ip，使server1通过地址转换ping通pc（模拟上网）

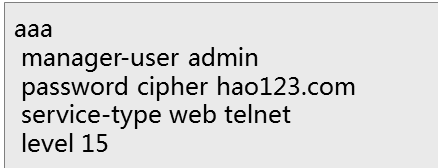


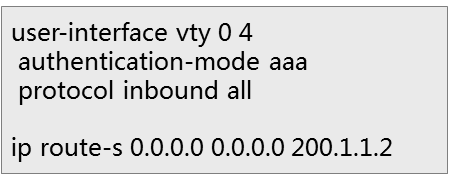


只有pc可以telnet到防火墙

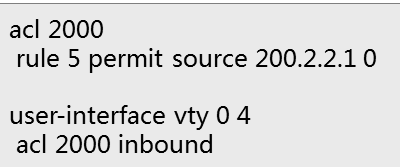






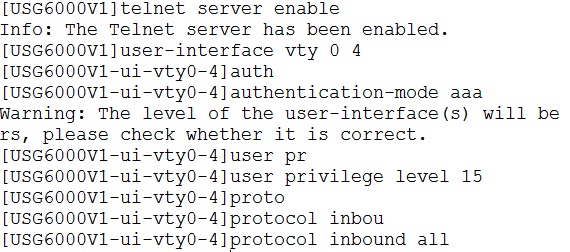


此时PC可以telnet防火墙，ISP也能telnet防火墙

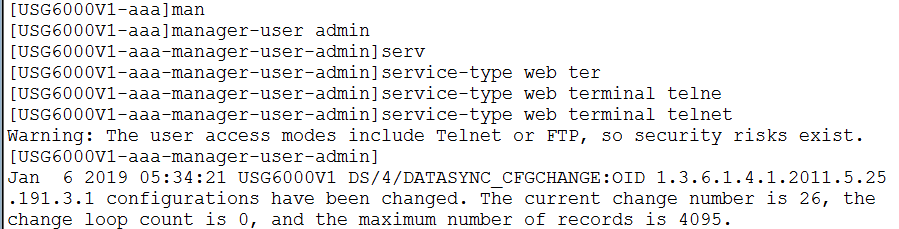


此时ISP不能telnet防火墙

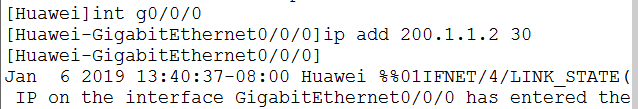
创建用户的等级和端口的开放



进入aaa视图，添加telnet服务和等级



配置路由器地址



防火墙配置telnet服务



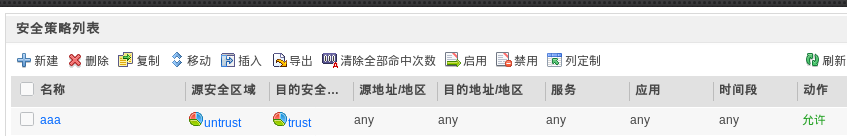


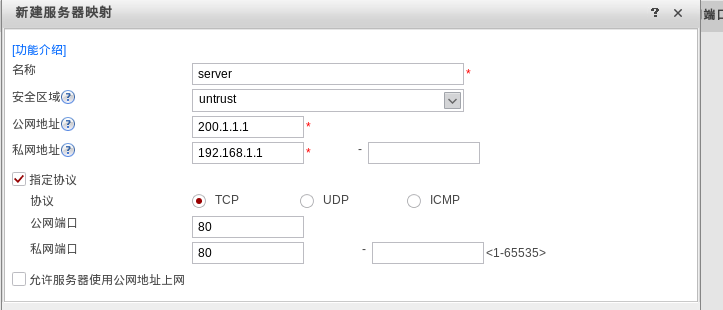
配置安全策略和服务器发布，client1可以访问server1的http服务

安全策略：trust访问untrush

服务器发布：只允许80端口

五元组抓包G1/0/接口





配置安全策略和easy ip，使server1通过地址转换ping通PC（模拟上网）

安全策略：trust访问untrush

Easy ip：使用出接口地址

五元组抓包G1/0/0接口



