F100-G2-A如何映射

NAT zhiliao_46394 2017-12-18 发表

组网及说明

防火墙+路由：H3C F100-G2-A（工作在三层），三层交互机：H3C S5500. 接入层交换机（2层）：s3110

网络结构： Internet——防火墙()——s5500（所有网关所在）——s3110——终端（服务器接5500下面）

防火墙网络配置：

网络为移动网络，有固定ip地址（以1.1.1.1为例）。

防火墙接口： G0/0/1 为到外网的接口 地址：1.1.1.1/255.255.255.128

G0/0/2 为到内网接口，也就是到5500的接口，地址为：192.168.10.2/24（以这个为例，这个用来和5500通信）

静态路由：0.0.0.0下一跳为1.1.1.254（移动的网关以这个地址为例）

192.168.11.0下一跳 192.168.10.1（这是5500上的地址用来和防火墙通信）

192.168.12.0下一跳 192.168.10.1

192.168.13.0下一跳 192.168.10.1

.....（总之所有的vlan在防火墙里面的静态路由都是路由到10这个网段上，也就是5500上面）

NAT： 动态转换，接口为 G/0/0/1 到外网，ACL 3000， 地址组 Easy IP ,转换模式PAT

ACL: 所有vlan的地址到目标地址any 都是允许的。

安全域：trust 里有 G0/0/2 内网的口，untrust 里有 G0/0/1外网的口

安全策略：源域 trust 到目标域 untrust 所有的源地址（各个vlan）到目标地址any都是允许的。

到此 内部访问外网没有问提

那么192.168.13.2和192.168.13.3这里两台服务器怎么才能让外放访问呢？？？？？

问题描述

问题：：：内网有2台服务器需要让外网用户访问，其中一台是web服务器有固定端口（以地址192.168.13.2端口8080为例），另外一台是sip服务器（端口随着外部用户变化而变化，地址以192.168.13.3为例）。应该如何做？(防火墙web登录)。

解决方法

做nat映射： to接口：选择外网接口

协议：根据需求选udp 或tcp 或tls

外网地址： 运营商的地址

端口：需要被访问的服务器的服务端口

内网地址： 需要被访问的服务器地址

端口：需要被访问的服务器的服务端口

然后把 外网接口所在的 安全域（应该是属于untrust的）到需要被访问的服务器所在的vlan所在的接口的安全域（应该是trust） 放通，也就是any到目标（需要被访问的地址）是允许的。就可以了，最好把需要映射的服务器都放在DMZ里面。

答案来自于 **鬧忒**