AR系列路由器包过滤防火墙的典型配置

姚忆斌　2006-10-24 发表

AR系列路由器包过滤防火墙的典型配置

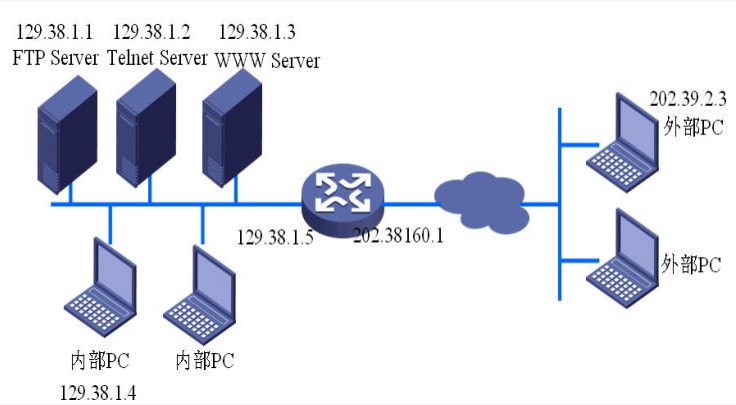
【需求】

通过一台Quidway路由器的接口Serial1/0/0访问Internet，路由器与内部网通过以太网接口Ethernet0/0/0连接。公司内部对外提供WWW、FTP和Telnet服务，公司内部子网为129.38.1.0，其中，内部FTP服务器地址为129.38.1.1，内部Telnet服务器地址为129.38.1.2，内部WWW服务器地址为129.38.1.3，公司对外地址为202.38.160.1。在路由器上配置了地址转换，这样内部PC机可以访问Internet，外部PC可以访问内部服务器,假定外部特定用户的IP地址为202.39.2.3。。通过配置防火墙，希望实现以下要求:

外部网络只有特定用户可以访问内部服务器。

内部网络只有特定主机可以访问外部网络。

【组网图】



【配置脚本】

Router配置脚本
在路由器Quidway上允许防火墙。 [Quidway] firewall enable # 设置防火墙缺省过滤方式为允许包通过。 [Quidway] firewall default permit # 创建访问控制列表3001。 [Quidway] acl number 3001 # 配置规则允许特定主机访问外部网，允许内部服务器访问外部网。 [Quidway-acl-adv-3001] rule permit ip source 129.38.1.4 0 [Quidway-acl-adv-3001] rule permit ip source 129.38.1.1 0 [Quidway-acl-adv-3001] rule permit ip source 129.38.1.2 0 [Quidway-acl-adv-3001] rule permit ip source 129.38.1.3 0 [Quidway-acl-adv-3001] rule deny ip # 创建访问控制列表3002 [Quidway] acl number 3002 # 配置规则允许特定用户从外部网访问内部服务器。 [Quidway-acl-adv-3002] rule permit tcp source 202.39.2.3 0 destination 202.38.160.1 0 # 配置规则允许特定用户从外部网取得数据（只允许端口大于1024的包）。 [Quidway-acl-adv-3002] rule permit tcp destination 202.38.160.1 0 destination-port gt 1024 # 将规则3001作用于从接口Ethernet0/0/0进入的包。 [Quidway-Ethernet0/0/0] firewall packet-filter 3001 inbound # 将规则3002作用于从接口Serial1/0/0进入的包。 [Quidway-Serial1/0/0] firewall packet-filter 3002 inbound