**海南大学网络空间安全学院**

**信息安全专业**

**《计算机与网络安全》实验报告**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **姓名** | 甄五四 | **学号** | 20213006839 | **专业班级** | 信息安全(密码学方向)理科实验班 | **成绩** |  |
| **实验报告题目** | | **实验01\_防火墙（标准、扩展ACL）** | | | | | |
| **教师评语** | |  | | | | | |

实验报告内容如下：

|  |
| --- |
| 1. 在初始环境下，验证网络的连通性，并说明各路由器的转发过程 |
| 1. R1 ping R3 |
| 截屏： |
|  |
| 过程：  R1要把在数据发给R3，但R1和R3不在同一网络，R1和R2的S0/0/0接口在同一网络。所以，R1将数据包先发送给它的静态默认路由R2(12.1.1.2)。R2的和R3在同一网络，R2将数据包从其S0/0/0传递到S0/0/1，R2通过S0/0/1接口(23.1.1.2)直接把数据包送到R3。 |
|  |
| 二、创建ACL表项:“拒绝12.1.1.0网络的数据包进入R3” |
| 1. R1 ping R3 |
| 截屏：    原因：  R1发出ping请求并将数据包发送到R3的S0/0/0接口。但是，R3上的ACL 1已经配置为拒绝来自12.1.1.0/24网络的流量。因此，ACL会丢弃来自12.1.1.0/24的ping请求，所以R3不会响应R1发出的ping请求。 |
| 2. R2的S0/0/1 ping R3 |
| 截屏：    原因：R2的S0/0/1接口ping R3。数据包先匹配规则1，因为规则1不匹配所以不能对该数据包进行限制，然后对下一条的规则匹配，下一条规则为隐式默认规则。按照ACL的隐式默认规则，R3路由器拒绝所有流量进入，所以该数据包不能通过，R2的S0/0/1无法ping通R3。 |
|  |
| 三、追加ACL表项:“允许任意网络的数据包进入R3” |
| 1. R2的S0/0/1 ping R3 |
| 截屏：    原因：当R2的S0/0/1接口尝试ping R3时，ping请求会成功。追加了ACL表项：access-list 1 permit any，意味着允许除规则1以外的任意网络的数据包进入R3。R2的S0/0/1接口在网络23.1.1.0，与规则1不匹配所以能ping通。 |
| 2. R2的S0/0/0 ping R3 |
| 截屏：    原因：当R2的S0/0/0接口尝试ping R3时，ping请求会失败。虽然追加了ACL表项：access-list 1 permit any，但原有的规则1还存在。R2的S0/0/0接口在网络12.1.1.0，与规则1匹配所以不能ping通。 |
|  |
| 四、创建ACL表项:“仅拒绝12.1.1.1的数据包进入R3” |
| 1. R1 ping R3 |
| 截屏：    原因：删除ACL原有编号1及其规则后，重新创建了ACL编号1，并添加了一项拒绝规则。拒绝规则拒绝了IP地址12.1.1.1的数据包，拒绝规则重新应用到接口R3的**s0/0/0接口**的进入方向，R3拒绝来自12.1.1.1的流量进入，所以R1不能ping通R3。 |
| 2. R2的S0/0/0 ping R3 |
| 截屏：    原因：拒绝规则拒绝了IP地址12.1.1.1的数据包，之后添加的允许规则允许任何其他数据包通过，R2的S0/0/0的IP地址为12.1.1.2，不匹配拒绝规则，匹配允许规则，所以可以ping通。 |
|  |
| 五、将ACL表应用于R2的S0/0/0接口 |
| 1. R1 ping R2 |
| 截屏：    原因：将ACL表应用于R2的S0/0/0接口，则R2的S0/0/0接口拒绝来自12.1.1.1的流量，所以无法ping通12.1.1.2，而R2的S0/0/1接口想要接收来自12.1.1.1的流量，需要由S0/0/0接收来转发，所以也无法ping通23.1.1.2。 |
|  |
| 六、将ACL表应用于R1的S0/0/1接口 |
| 1. R1 ping R3 |
| 截屏：    原因：防火墙只对通过自身的流量进行过滤，而不干涉自身发送的流量。R1可以ping通R3，因为ACL应用在R1的S0/0/1接口，R1 ping R3流量从该接口流出，防火墙允许从R1到R3的流量通过。 |
|  |
| 七、将扩展的ACL表项:“拒绝12.1.1.1 telnet 23.1.1.3”应用于R3 |
| 1. R1 ping R3 |
| 截屏：    原因：根据ACL 100配置，Telnet流量从12.1.1.1到23.1.1.3被拒绝，但ping数据包不匹配这个规则，因为它们使用的是不同的协议（ICMP），接着匹配access-list 100 permit ip any any，允许任何流量进入，所以R1可以ping通R3. |
| 2. R1 telnet R3 |
| 截屏：    原因：根据ACL 100配置，Telnet流量从12.1.1.1到23.1.1.3被拒绝，R1 telnet R3匹配拒绝规则，所以R1 telnet R3不通过。 |
|  |
| 八、将扩展的ACL表项应用于R2的S0/0/0接口 |
| 1. R1 telnet R3 |
| 截屏：    原因：数据包先发送到R2的S0/0/0时，从R1发来的数据包与ACL 100拒绝规则匹配，所以数据包被丢弃，不再转发给R3，R3没有收到数据包，无法做出回应，导致连接超时。 |
| 2. R1 telnet R2 |
| 截屏：    原因：R1发送的数据包发送到R2的S0/0/0，与ACL100的拒绝规则匹配，接着匹配允许规则，匹配成功，所以R1能telnet通R2的S0/0/0,R2的S0/0/1从R2的S0/0/0转发过来，所以R1也能telnet通R2的S0/0/1。 |
|  |
| 九、实验总结 |
| 1. 一个ACL可以由多条“**deny** | **permit**”语句组成，每一条语句描述了一条规则。设备收到数据流量后，会逐条匹配ACL规则，看其是否匹配。如果不匹配，则匹配下一条。一旦找到一条匹配的规则，则执行规则中定义的动作，并不再继续与后续规则进行匹配。如果都不匹配则会执行默认规则，思科中默认规则为拒绝。 2. 子网掩码是一种用来指明一个IP地址的哪些位标识的是主机所在的子网，以及哪些位标识的是主机的掩码。子网掩码不能单独存在，它必须结合IP地址一起使用。子网掩码只有一个作用，就是将某个IP地址划分成网络地址和主机地址两部分。路由器使用的通配符掩码与源或目标地址一起来分辨匹配的地址范围，它与子网掩码不同。它不像子网掩码告诉路由器IP地址的哪一位属于网络号一样，通配符掩码告诉路由器为了判断出匹配，它需要检查IP地址中的多少位。 3. 在修改或者在其他路由器上添加ACL,需要将已经添加过的无关ACL及时删除，否则会影响后续结果。 4. 当数据流经防火墙时，防火墙会根据其配置的规则和策略来检查流量，并根据这些规则来决定是否允许或拒绝数据包通过。防火墙不会主动干涉网络上设备发出的流量，只有在流量尝试穿越防火墙时，才会进行过滤和检查。自身发送的流量通常不需要通过防火墙进行过滤，因为防火墙的主要任务是保护网络免受外部威胁。 |