**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 邓鹏超 | **同组实验者** |  |
| **实验项目名称** | 网络访问控制与扩展包过滤配置 | | | **实验日期** | 11月7 日 |
| **实验成绩：** | | | | | |
| **一．实验目的**  通过本实验理解基于IP地址、协议和端口的包过滤原理和应用方法，掌握扩展访问控制列表的设计、配置和测试。   1. **实验任务**   1、参照拓扑图建立网络拓扑。  2、配置路由器和PC，确保网络拓扑的连通性。  3、配置扩展访问控制列表满足应用需求。  **三．实验设备**  Cisco Router 2620XM 3台  Catalyst Switch 2950-24 6台  Hub Hub-PT 1台  PC PC-PT 5台  Server Server-PT 4台  **四．实验拓扑与参数配置**  实验的参考拓扑图和参考配置参数如图所示。    图9-1 实验拓扑图  表8.1参数配置表   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 路由器配置信息（子网掩码均为255.255.255.0） | | | | | | | | | 主机名 | 类型 | | IP 地址 | | RIP路由网络 | | 时钟频率 | | InsideRouter | 2620XM | | Fa0/0: 192.168.1.2  Eth1/0: 192.168.2.1  Eth1/1: 192.168.3.1  Eth1/2: 192.168.4.1  Eth1/3: 192.168.5.1 | | 192.168.1.0  192.168.2.0  192.168.3.0  192.168.4.0  192.168.5.0 | |  | | EageRouter | 2620XM | | Fa0/0: 192.168.1.1  Ser0/0: 218.58.59.91 | | 192.168.1.0  218.58.59.0 | |  | | OutsideRouter | 2620XM | | Fa0/0: 218.58.100.1  Ser0/0: 218.58.59.90 | | 218.58.59.0  218.58.100.0 | | 9600 | | PC和Server配置信息（子网掩码均为255.255.255.0） | | | | | | | | | 主机名 | | IP 地址 | | 默认网关 | | 所属网段 | | | PC1 | | 192.168.2.2 | | 192.168.2.1 | | 192.168.2.0 | | | PC2 | | 192.168.2.3 | | 192.168.2.1 | | 192.168.2.0 | | | PC3 | | 192.168.3.2 | | 192.168.3.1 | | 192.168.3.0 | | | PC4 | | 192.168.4.2 | | 192.168.4.1 | | 192.168.4.0 | | | PC5 | | 192.168.5.2 | | 192.168.5.1 | | 192.168.5.0 | | | PC6 | | 218.58.100.2 | | 218.58.100.1 | | 218.58.100.0 | | | WWW | | 192.168.1.3 | | 192.168.1.1 | | 192.168.1.0 | | | FTP | | 192.168.1.4 | | 192.168.1.1 | | 192.168.1.0 | | | SMTP | | 192.168.1.5 | | 192.168.1.1 | | 192.168.1.0 | | | Outside WWW | | 218.58.100.3 | | 218.58.100.1 | | 218.58.100.0 | |  1. **实验步骤**   **步骤1** 按照实验拓扑图和参数配置表配置各设备  和网络访问控制与基本包过滤配置中一样，先将实验拓扑图连好，并保证能正常ping通    两两间能正常ping通  **步骤2** 配置扩展访问控制列表满足禁止宿舍网段访问FTP服务器上的ftp资源的应用需求。  **（1）** **创建访问控制列表access –list 100，将其应用到InsideRouter 的Fa0/0端口上。**    **查看建立的访问控制列表**    **（2）然后进行测试。添加多个Complex PDU进行测试**    PC5 到 FTP服务器的FTP PDU设置 PC5 到 WWW 服务器的HTTP PDU设置    PC5到SMTP服务器的SMTP PDU设置  **测试结果如下**     1. **测试结果分析**   1号PDU Successful状态说明宿舍网段可以访问WWW服务器。  2号PDU Successful状态说明宿舍网段可以访问FTP服务器。    **步骤2**  **（1）创建访问控制列表access-lists 101,将其应用到EageRouter 的Fa0/0端口上**        **查看建立的访问控制列表**       1. **然后进行测试。添加多个Complex PDU进行测试**     PC6到FTP服务器的FTP PDU设置 PC6到内网WWW服务器的HTTP PDU设置 | | | | | |
| PC6到SMTP服务器的SMTP PDU设 PC1到Outside WWW服务器的HTTP PDU设置  PC2、PC3、PC4、PC4到Outside WWW服务器的Complex PDU设置和PC1到Outside WWW服务器的Complex PDU设置一样。  **测试结果如下**      0号PDU 的Failed状态说明外网不能访问内网的FTP服务器。  1号PDU 的Successful状态说明外网能访问内网的WWW服务器。  2号PDU 的Successful状态说明外网能访问内网的SMTP服务器。  其他PDU的Successful状态说明管理网段，行政网段，教学网段，宿舍网段能访问外网的Outside WWW服务器。   1. **实验思考** 2. **思考扩展访问控制列表的进行访问控制的依据有那些？**   协议类型、源地址、目的地址、源端口、目的端口、建立连接的和IP优先级   1. **有人说在同一个Router上同一个端口的同一个方向上不能绑定多个访问控制列表， 在同一个Router上同一个端口的两个不同方向（inside、outside）能分别绑定一个访问控制列表，这个说法对吗？请做实验验证。**   验证后发现同一个端口的同一个方向上不能绑定多个访问控制列表，但是可在同一个端口的两个不同方向能分别绑定一个访问控制列表   1. **扩展访问控制列表的配置一般包括哪几步？**   配置过滤规则、配置应用端口   1. **扩展访问控制列表有什么样的应用原则？**   **最小特权原则:**只给受控对象完成任务所必须的最小的权限。也就是说被控制的总规则是各个规则的交集，只满足部分条件的是不容许通过规则的。  **最靠近受控对象原则:**所有的网络层访问权限控制。也就是说在检查规则时是采用自上而下在ACL中一条条检测的，只要发现符合条件了就立刻转发，而不继续检测下面的ACL语句。  **默认丢弃原则:**在CISCO路由交换设备中默认最后一句为ACL中加入了deny any, 也就是丢弃所有不合条件的数据包 | | | | | |