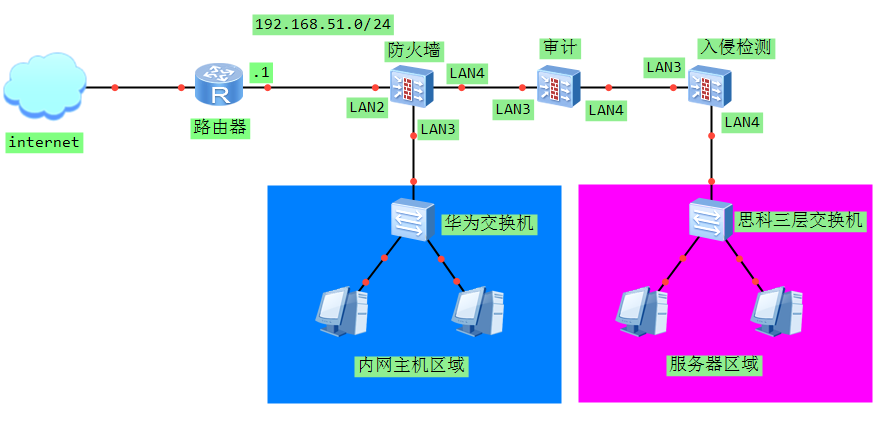
“信息安全管理与评估”实验任务书

## 赛项环境设置

赛项环境设置包含了三个竞赛阶段的基础信息：网络拓扑图、IP地址规划表、设备初始化信息。

### 网络拓扑图



### 设备初始化信息

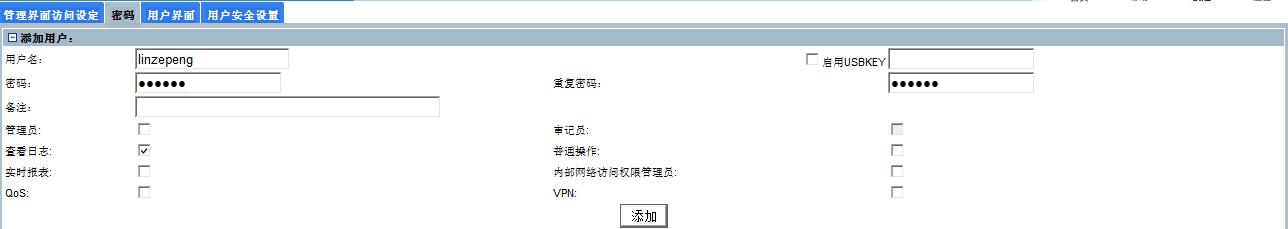
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **管理地址** | **默认管理接口** | **用户名** | **密码** |
| 防火墙 | https://192.168.0.1 | LAN1 | admin | XXXXXX |
| 安全审计 | https://192.168.18X.102 | LAN2 | root | root |
| 入侵检测 | https://192.168.18X.103 | LAN2 | admin | XXXXXX |
| 三层交换机 | 192.168.18X.7 |  |  | XXXXXX |
| 备注 | 所有设备的默认管理接口、管理IP地址不允许修改 | | | |
| 以上X为所在小组编号。密码处如你为第二组则为222222.以此类推 | | | | |

# 网络安全设备配置与防护

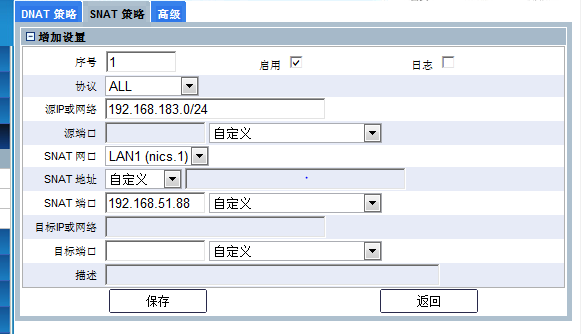
每个队伍提交的答案保存到一个WORD文档中。以下配置都要截图，截图内容为配置关键步骤以及验证结果。

首先要使内网主机与服务器都可以访问外网并且互访。安全设备网络自行设计与搭配。如透明模式相连，lantolan等。**配置的关键步骤均到截图。**

1. 在公司总部的防火墙上配置，并且新增一个用户，用户名(队长全拼英文)，密码123456，该用户只有查看配置权限，不具有添加配置或修改配置的权限。



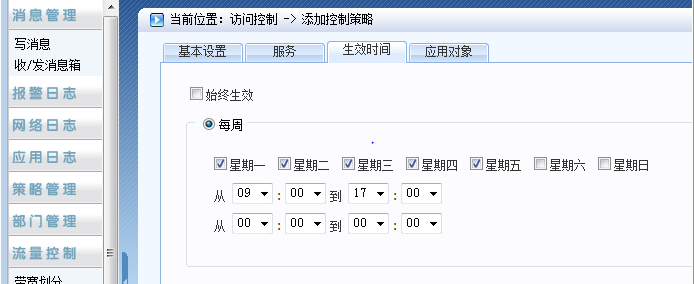
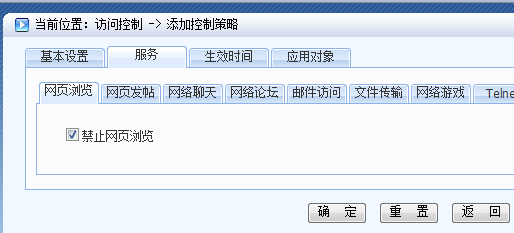
1. 在公司总部的防火墙上配置，使内网所有用户网段和服务器区网段都可以通过防火墙外网接口IP地址访问互联网。



1. 在公司总部的防火墙上配置，总的出口带宽是100M，其中LAN3与LAN4各占50M带宽。



1. 在公司总部的审计上配置，在上班时间（工作日的9:00-17:00）只不允许公司员工访问外网资源。



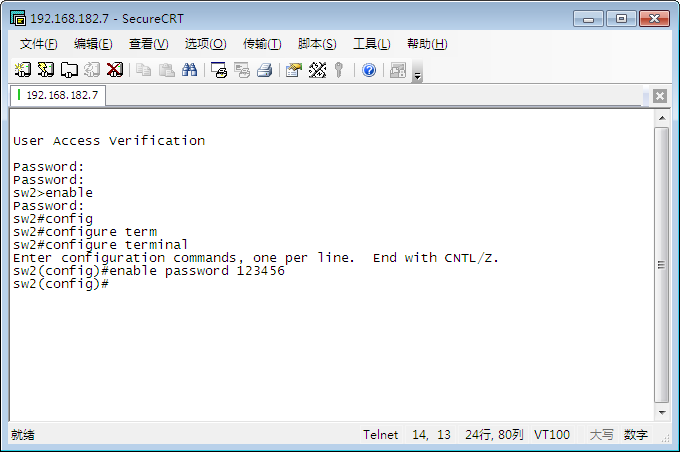
1. 在公司总部的审计系统上配置，在上班时间如有事情需要访问网络，限制只有通过审计的WEB认证后才能访问互联网



1. 在公司总部的审计系统上配置，增加非admin账户(队长全拼英文)，密码123456，该账户仅用于用户查询设备的日志信息和统计信息。

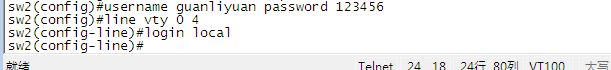


1. 在公司总部的三层交换机上配置，配置设备enable密码，并且在登录设备时必须正确输入enable密码才能进入交换机的配置模式。密码统一为123456.



1. 在公司总部的三层交换机上配置，允许使用console和telnet方式管理设备。同时telnet只允许同时在线5个用户。telnet用户名为队长全拼英文。

密码123456.



1. 在公司总部的三层交换机上配置，连接主机的端口开启广播风暴抑制功能，参数设置为400pps。



1. 在公司总部的入侵检测上配置，阻止常见的WEB攻击数据包访问到公司内网服务器。



1. 在公司总部的入侵检测系统上配置，开启入侵检测系统的DDoS防护。



# Windows server 2003 相关实验

## IIS安全加固与证书签发

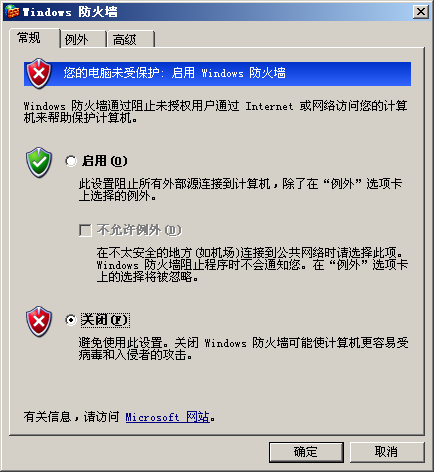
**任务环境说明：(服务器区主机开启虚拟机做本实验)**

•Web服务器操作系统：windows2003 server；

•安装服务/工具1：Web服务，版本是IIS-6.0；

•安装服务/工具2：FTP服务，版本是IIS-6.0；

1. 配置Windows 防火墙，使IIS Web服务能够被访问，对配置进行截屏。



1. 加固IIS Web服务器的安全配置，使得Web服务只能被内网用户所在的网段访问，对加固配置进行截屏。
2. 为IIS Web服务器申请服务器证书，对申请摘要进行截屏。
3. 为IIS Web服务器颁发一年期服务器证书，对颁发过程进行截屏。
4. 将IIS 服务器启用客户端证书设置。使用客户端浏览器访问该Web服务进行测试。将要求客户端提供证书的弹出页面截屏。
5. 为PC申请CA证书。颁发该证书。对申请和颁发过程截屏。
6. 在PC上安装CA证书。使用PC浏览器访问该Web服务进行测试，对操作过程截屏。

系统安全配置

|  |  |  |
| --- | --- | --- |
| **任务分类** | **序号** | **任务要求** |
| 一、文件服务器 | 1.1 | 为所有员工都创建相应用户，命名方式采用汉语拼音即可，例如“李方”的用户名为lifang，其用户口令为123456； |
| 1.2 | 创建3个组，组名采用需要使用部门名称的拼音来命名，并将相应用户加入相应组中； |
| 1.3 | 在非系统分区创建文件夹share，在share下按照部门名称创建文件夹，在部门文件夹下按照员工名字创建文件夹，结构如下： |
| 1.4 | 为每个文件夹设置合理的NTFS权限，要求如下：  外联部和产品部的员工只能对属于自己的文件夹下的内容有读、写、修改权限，无权访问其他员工的文件夹内容；  总经理室的用户不仅可以对自己的文件夹下的内容有读、写、修改权限，并且对其他部门员工的文件夹下的内容也拥有读、写、修改权限；  程美与徐雪两个用户对彼此文件夹下的内容只拥有只读的权限；  整个share的树形目录结构保持不变； |
| 1.5 | 为share目录设置合理的共享权限； |
| 1.6 | 用王波用户通过UNC方式访问徐雪的共享文件夹，验证结果； |
| 1.7 | 用徐雪用户通过UNC方式访问郭伟的共享文件夹，验证结果； |
| 1.8 | 用程美用户通过UNC方式访问徐雪的共享文件夹，验证结果； |
| 二、部署系统安全策略 | 3.1 | 增强系统账号的安全性，启用密码复杂性策略； |
| 3.2 | 增强系统账号的安全性，设置密码长度最小为8位； |
| 3.3 | 重新设置管理员的密码，并在提交文档中注明所设置的密码； |
| 3.4 | 对于密码为空的本地账户只允许通过控制台登录； |
| 3.5 | 把3389端口修改成2003端口。 |
| 3.6 | 禁用“不允许SAM账户和共享的匿名枚举” |
| 3.7 | 利用注册表禁止默认共享 |
| 3.8 | 登录系统5次失败后锁定账户30分钟 |
| 3.9 | 利用注册表禁止系统自动登录 |
| 4.0 | 利用注册表防止SYN攻击 |
| 4.1 | 利用注册表防止ICMP攻击 |
| 4.2 | 利用注册表防止SNMP攻击 |
| 4.3 | 利用注册表对AFD.SYS进行保护 |
| 4.4 | 利用注册表禁止139空连接 |
|  | 4.5 | 利用注册表禁止WebDAV |
|  | 4.6 | 利用本地策略做到关机时清理虚拟内存页面文件 |
|  | 4.7 | 利用本地策略做到不允许系统在未登录前关机 |
|  | 4.8 | 利用本地策略做到只有Administrator组可以关闭系统 |

在一些文件删除后存放在回收站内。此时用户清空了回收站后发现删除的文件中有自己需要的资料。（此时用户没有做其他操作）现在想要进行恢复。请问什么样的方法可以不用数据恢复软件恢复误删除的文件？