

**网络安全项目实训大作业**

**专业方向： 网络安全技术**

**成 员： 1740224167 蔡展鸿**

**1740224132 邓锋**

**指导老师： 周伟**

摘要

报告中介绍了校园网信息系统安全的现状，结合校园网信息系统的特点和安全要素分析，提出了合适校园网环境下的信息系统安全评估流程，并针对校园网网络信息系统安全评估报告，提出校园网网络信息系统加固的流程和实施系统加固的内容和方法。随着数学化校园建设的不断推进，如何构建可靠的校园网络安全防范成为不可忽视的问题 ，所以我们要不断发现校园网的安全，保护我们校园网必须建立完备的校园网安全防护体系，加强校园网的安全管理体制，保证校园网的正常运行及内部信息资源不受非法访问获取

关键字：校园网、风险评估、安全设计

目录

[摘要 2](#_Toc43843982)

[引言 4](#_Toc43843983)

[第一章 校园网概况 4](#_Toc43843984)

[1.1网络结构 4](#_Toc43843985)

[1.2网络拓扑图 5](#_Toc43843986)

[1.3带宽 5](#_Toc43843987)

[1.4核心交换机 6](#_Toc43843988)

[1.5交换机配置情况 7](#_Toc43843989)

[1.6学校各个网段 8](#_Toc43843990)

[第二章 等保2.0保护对象等级划分 8](#_Toc43843991)

[2.1等级划分 8](#_Toc43843992)

[2.2等保2.0基本框架 9](#_Toc43843993)

[2.3定级流程 10](#_Toc43843994)

[第三章 华软校园网的安全问题 11](#_Toc43843995)

[3.1物理安全 11](#_Toc43843996)

[3.1.1重要信息点的物理保护 11](#_Toc43843997)

[3.2主机安全 11](#_Toc43843998)

[3.3数据链路层安全 11](#_Toc43843999)

[3.4网络安全 11](#_Toc43844000)

[3.4.1网络系统安全 11](#_Toc43844001)

[3.4.2网络病毒 12](#_Toc43844002)

[3.5应用安全 12](#_Toc43844003)

[3.5.1 可能存在的SQL注入漏洞 12](#_Toc43844004)

[3.5.2 SNMP漏洞 12](#_Toc43844005)

[3.5.3home.sise.cn漏洞： 13](#_Toc43844006)

[第四章 整改依据 13](#_Toc43844007)

[4.1安全管理中心 14](#_Toc43844008)

[4.2安全通信网络 14](#_Toc43844009)

[4.3安全区域边界 14](#_Toc43844010)

[4.4安全计算环境 14](#_Toc43844011)

[4.5安全计算环境设计 15](#_Toc43844012)

[4.6安全管理规划 15](#_Toc43844013)

[第五章整改实施 16](#_Toc43844014)

[5.1基本需求 16](#_Toc43844015)

[5.2物理环境方面的整改 16](#_Toc43844016)

[5.2.1物理访问控制 16](#_Toc43844017)

[5.2.2防火、防雷击、防水和防潮 17](#_Toc43844018)

[5.2.3防盗窃和防破坏 17](#_Toc43844019)

[5.2.4温湿度控制 17](#_Toc43844020)

[5.3 技术方面的整改 17](#_Toc43844021)

[5.3.1 修改路由器密码 17](#_Toc43844022)

[5.3.2网络设备攻击防范 18](#_Toc43844023)

[5.3.3 DHCP常见问题及DHCP Snooping 19](#_Toc43844024)

[5.3.4漏洞扫描系统 22](#_Toc43844025)

[5.3.5日志服务器配置 22](#_Toc43844026)

[5.3.6 证书服务器配置（https） 25](#_Toc43844027)

[5.3.7 ipsec通信加密 29](#_Toc43844028)

[5.3.8数据备份与灾难恢复备份 32](#_Toc43844029)

[5.3.9 防病毒网关 37](#_Toc43844030)

[5.4管理制度方面的整改 40](#_Toc43844031)

[5.4.1管理制度 40](#_Toc43844032)

[第六章 总结 40](#_Toc43844033)

引言

随着校园网和数字化校园等信息化建设不断深入，校园网络系统已经成为了高校重要的现代化基础措施，为了教学，科研和现代化管理等提供现金、可靠、安全、快捷的计算机网络环境。而诸如：教学管理系统，高校财务系统、校园一卡通、远程教育系统、网络协作学习平台等应用也将校园网信息安全问题逐渐突显出来，如何对校园网络系统进行安全评估和分析，合理构建安全体系结，保障校园网网络信息安全越来越成为一个需要重视的问题。

1. 校园网概况

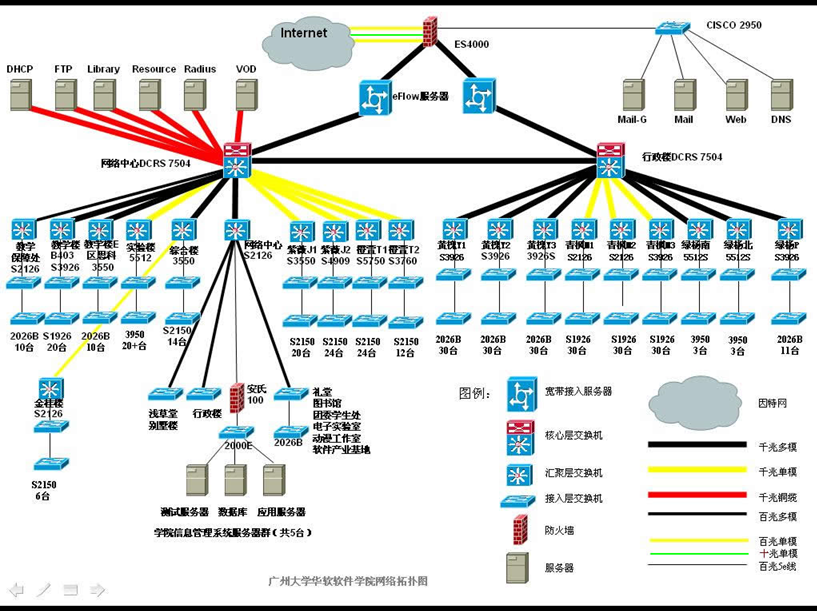
1.1网络结构

·采用层次化的网络设计

·主干设备以光纤互联

·核心层与汇聚层采用三层交换机（部分汇聚层交换机为二层交换机），提供高速交换及路由功能；接入层采用二层交换机提供高密度接入

1.2网络拓扑图



1.3带宽

**（1）外网带宽**

·两条100M电信光纤接入防火墙

·一条10M教育网光纤单独接入

**（2）内网带宽**

·防火墙与宽带服务器、核心交换机之间通过1000M光纤互联

·核心、汇聚层交换机为1000M光纤互联

·接入层（楼层）交换机与终端PC之间的线路带宽为100M

·校园服务器通过1000M铜缆直接连接核心层交换机

1.4核心交换机

**（1）核心交换机介绍**

·目前学院网络的核心交换机有两台（网络中心及行政楼各一台），通过1000M多模光纤互联

·由于学院网络主要为星型拓扑结构，大部分线路均无冗余，因此没有使用RIP、OSPF等动态IP路由协议。而采用IP静态路由来联通各个网络，同时通过应用access list来阻断一些不安全的流量，降低网络风险

**（2）核心交换机负载**

·网络中心交换机负责教学区、校园服务器及少数宿舍的网络接入，接入点较少，IP负载较低

·行政楼交换机负责电视转播服务器及大多数宿舍区的网络接入，由于接入点较多，而且需要执行汇聚层功能，IP负载相对较高

1.5交换机配置情况

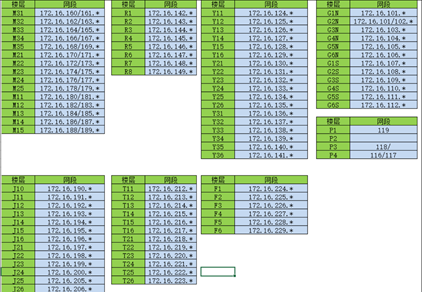
· 每台接入层（楼层）交换机根据需求不同，划分为一个或多个VLAN，指定默认网关，并通过trunk接入汇聚层的三层交换机；少数交换机以级联的方式接入其他交换机，再通过其它交换机接入汇聚层

·在具有三层功能的汇聚层交换机中配置网关、DHCP服务器，并设置默认路由用以与核心交换机通讯，部分access list也这层交换机中配置

·核心交换机中除了配置静态路由连接全网之外，还为部分二层汇聚交换机提供网关，DHCP中转发功能，同时也配置有access list与访问策略

·所有交换机均进行了multicast相关配置以优化内网的电视直播服务

1.6学校各个网段



# 第二章 等保2.0保护对象等级划分

## 2.1等级划分

第一级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对国家安全造成严重损害。

第五级，等级保护对象受到破坏后，会对国家安全造成特别严重损害。

|  |  |  |  |
| --- | --- | --- | --- |
| 受侵害的客体 | 对相应客体的侵害程度 | | |
| 一般损害 | 严重损害 | 特别严重损害 |
| 公民、法人和其他组织的合法权益 | 第一级 | 第二级 | 第三级 |
| 社会秩序、公共利益 | 第二级 | 第三级 | 第四级 |
| 国家安全 | 第三级 | 第四级 | 第五级 |

## 2.2等保2.0基本框架



## 2.3定级流程

[](https://image.3001.net/images/20190428/1556448847_5cc5864f78a1a.png)

**根据等保2.0**

|  |  |
| --- | --- |
| **区域** | **等级划分** |
| **宿舍区** | **第一级** |
| **实验区，图书馆** | **第二级** |
| **网络中心，财务区** | **第三级** |

# 第三章 华软校园网的安全问题

## 3.1物理安全

### 3.1.1重要信息点的物理保护

华软校园网各级网络内部存在重要的信息点，如内部核心应用系统，环境等都问题，它包括两个方面：

1. 环境安全：暴雨天容易引发潮湿及线路不稳定。此问题存在较大威胁，需要进行处理。
2. 设备安全：学校内部分楼层内主机没有上锁，可引发盗窃和毁坏等。此问题存在较大威胁，需要进行处理。

## 3.2主机安全

1）根据软校园网内主机的安全防护现状，从扫描的多台主机发现部分存在漏洞。此问题存在较大威胁，需要进行处理。

## 3.3数据链路层安全

二层交换机DHCP服务器的欺骗威胁，导致网段主机无法联网，DHCP Sproofing是一种中间人攻击方式。DHCP是提供IP地址分配的服务。当局域网中的计算机设置为自动获取IP，就会在启动后发送广播包请求IP地址。DHCP服务器（如路由器）会分配一个IP地址给计算机。在分配的时候，会提供DNS服务器地址。此问题存在威胁，需要进行处理。

## 3.4网络安全

3.4.1网络系统安全

作为校园网系统的承载平台，网络系统的安全显得非常重要。因为需要重要的信息都通过网络进行交换。由于外网连接校园网不需要通过验证，黑客可以直接进入校园网，而且校园网未给网站装安全防护软件，此类问题存在威胁，需要进行处理。

### 3.4.2网络病毒

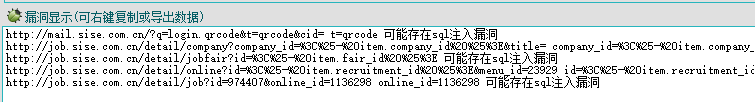
部分主机未更新病毒库及未更新系统打补丁，导致类似永恒之蓝等病毒对其进行攻击。此类问题存在较大威胁，需要进行处理。

## 3.5应用安全

华软校园网的服务器及网站漏洞存在中高风险的漏洞。

采用safe3工具对<https://www.sise.edu.cn/index.html>检测

### 3.5.1 可能存在的SQL注入漏洞





http://mail.sise.edu.cn/?q=login.qrcode&t=qrcode&cid= cid= 可能存在sql注入漏洞

http://job.sise.edu.cn/detail/jobfair?id=%3C%25-%20item.fair\_id%20%25%3E 可能存在sql注入漏洞

http://job.sise.edu.cn/detail/jobfair?id=%3C%25-%20item.fair\_id%20%25%3E 可能存在sql注入漏洞

http://mail.sise.edu.cn/tpl/public/js/ APC\_UPLOAD\_PROGRESS=88952634&=88952634 可能存在POST sql注入漏洞

http://job.sise.edu.cn/detail/company?company\_id=%3C%25-%20item.company\_id%20%25%3E&title= company\_id=%3C%25-%20item.company\_id%20%25%3E 可能存在sql注入漏洞

http://mail.sise.edu.cn/tpl/public/js/a+%22mobile/?q=change&type=%22+c+%22&module=%22+b%7D;var type=%22+c+%22 可能存在sql注入漏洞

http://job.sise.edu.cn/detail/online?id=%3C%25-%20item.recruitment\_id%20%25%3E&menu\_id=23929 id=%3C%25-%20item.recruitment\_id%20%25%3E 可能存在sql注入漏洞

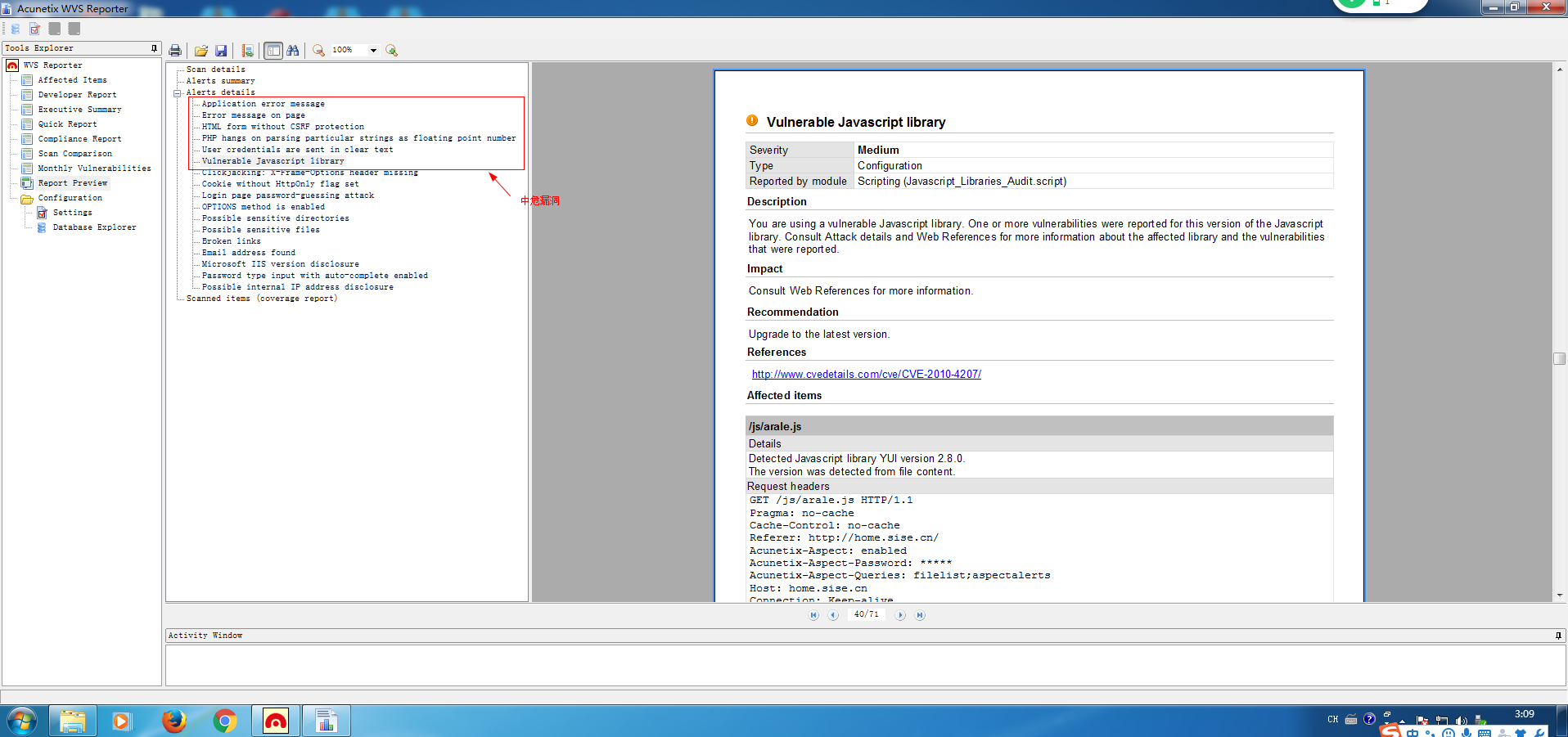
### 3.5.2 SNMP漏洞



弱口令漏洞起信息泄漏，此类漏洞导致与SNMP服务器连接的主机信息泄露。此问题存在威

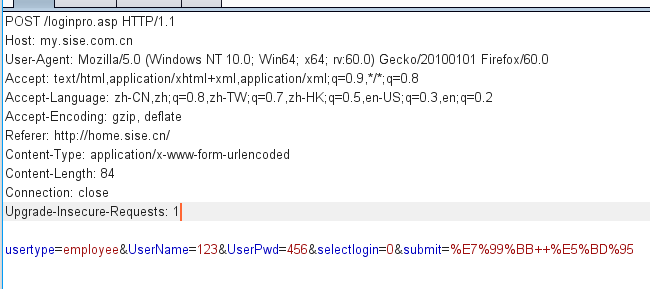
胁，需要进行处理。

### 3.5.3home.sise.cn漏洞：



Application error message 和 Error message on page

在程序出现500错误时，有关服务器的问题，会展现在浏览器的页面上weblogic的路径，这样就会把服务器的路径暴露在攻击者面前。此问题存在威胁，需要进行处理。



User cerdentials are sent in clear text

使用者的账号与密码会以明文的方式传到给网站。此问题存在较大威胁，需要进行处理。

# 第四章 整改依据

## 4.1安全管理中心

|  |  |  |  |
| --- | --- | --- | --- |
| 大数据安全 | IT运维管理 | 堡垒机 | 漏洞扫描 |
| 网站监测预警 | 等保安全一体机 | 等保建设咨询服务 |  |

建设要点

对安全进行统一管理与把控,集中分析与审计,定期识别漏洞与隐患

## 4.2安全通信网络

|  |  |  |  |
| --- | --- | --- | --- |
| 下一代防火墙 | VPN | 路由器 | 交换机 |

建设要点

构建安全的网络通信架构

保障信息传输安全

## 4.3安全区域边界

|  |  |  |  |
| --- | --- | --- | --- |
| 下一代防火墙 | 入侵检测/防御 | 上网行为管理 | 安全沙箱 |
| 动态防御系统 | 身份认证管理 | 流量安全分析 | WEB应用防护 |
| 准入控制系统 |  |  |  |

建设要点

强化安全边界防护及入侵防护

优化访问控制策略

## 4.4安全计算环境

|  |  |  |  |
| --- | --- | --- | --- |
| 入侵检测/防御 | 数据库审计 | 动态防御系统 | 网页防篡改 |
| 漏洞风险评估 | 数据备份 | 终端安全 |  |

建设要点

强调系统及应用安全

加强身份鉴别机制与入侵防范

## 4.5安全计算环境设计

1.个人信息保护和数据保密性

myscse系统登陆时账号密码明文显示，ftp，myscse明文传输

2．数据备份和恢复

没有本地 灾难异地实时备份

3.入侵防范

可能会受到icmp泛洪攻击、DHCP伪造 MAC地址欺骗

4.安全审计

没有日志服务功能

## 4.6安全管理规划

1.安全管理机构

没有定期检查和审核安全策略和安全管理制度

2．安全管理人员

没有考核录用人员专业技能，签署保密协议

没有对工作人员定期进行安全技术考核

3．安全建设管理

没有进行定期等保测评

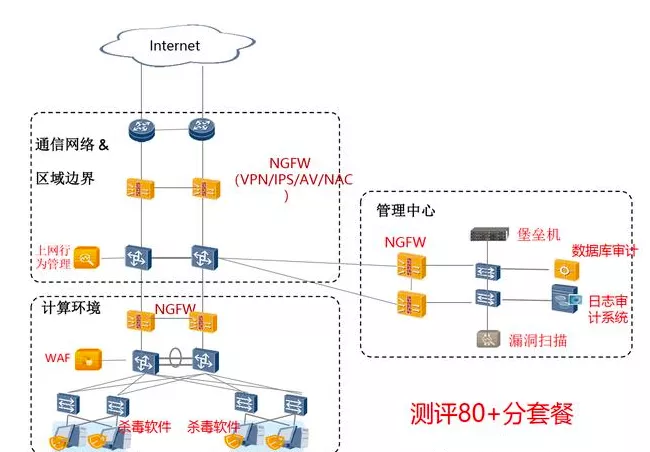
4．安全运维管理

恶意代码防范管理弱

总体上需要整改的地方还有添加防病毒网关防范病毒、路由器设备密码、网络设备防范攻击、DHCP防伪造

（ipsec）保护 IP 数据包的内容，信息管理系统登录界面为使用https进行加密，保证选课系统能力满足业务高峰期需要； 保证网络各个部分的带宽满足业务高峰期需要上外网得到保障，增加日志服务器监控重要服务器日志

根据等保2.0 三级保护部署



2-1三级等保（基础版）拓扑图

# 第五章整改实施

## 5.1基本需求

学校应升级服务器设备能同时容纳更多用户，宽带升级加快上网需求，让上网达到保障每周定期测试宽带速度与稳定，避免有网络异常。

## 5.2物理环境方面的整改

### 5.2.1物理访问控制

学校内的机房出入口应该配置电子门禁系统，控制、鉴别，或招募勤工俭学的学生值班轮守

### 5.2.2防火、防雷击、防水和防潮

1. 机房内都要有全套的防火设备，建议使用粉未灭火器，不建议配备有液体的灭火设备。安装各种检测器（co2,co,温度检测器...）
2. 将各类机柜、设施和设备等通过接地系统安全接地，还可以在机房楼顶安装避雷针。
3. 机房不建议设立在底楼和大量水源附件，机房应该及时通风，设备上应该添加防水装置。

### 5.2.3防盗窃和防破坏

将大型或贵重的设备进行固定上锁并安装警报器，机房也应进行上锁。

### 5.2.4温湿度控制

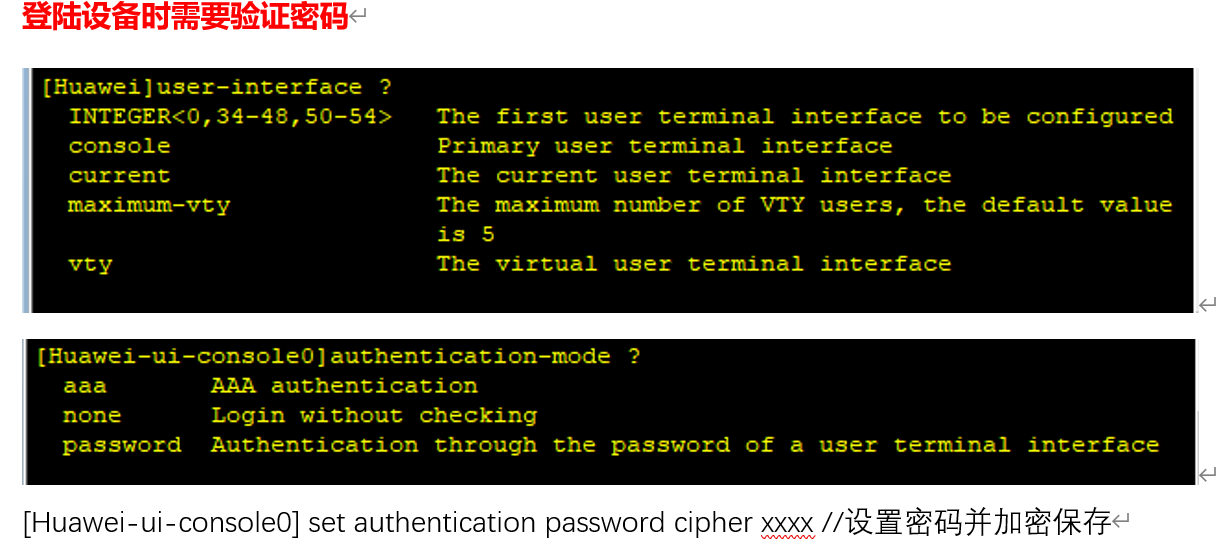
（1）应该装一个温湿度测量工具，根据不同的温湿度进行有效的调节，使机房温湿度的变化在设备运行所允许的范围内。

（2）在大型且常用的设备上添加个大型散热器。

## 5.3 技术方面的整改

### 5.3.1 修改路由器密码

现在路由器基本都设有web界面（网关ip）管理发现学校由于部分路由器是默认用户默认登录密码，所以需要修改密码防止有人登录路由器web界面修改路由器配置，



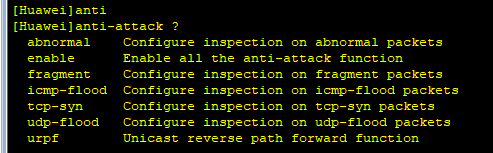
4-1设置密码

设置登录失败锁定用户处理

[HUAWEI-aaa] local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5

### 5.3.2网络设备攻击防范

1网络设备需要开启防范攻击 可防范的攻击有（华为设备为例）



4-2防范攻击选择

示例：Icmp泛洪攻击 防止有人恶意无限ping命令来攻击

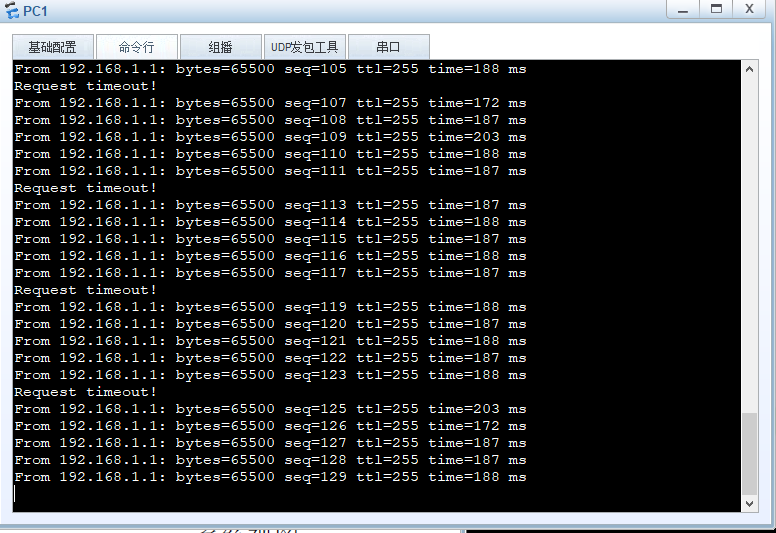
anti-attack icmp-flood enable命令用来使能ICMP泛洪攻击防范功能。（默认开启）

anti-attack icmp-flood car命令用来配置ICMP泛洪攻击报文的限制速率。

如：anti-attack icmp-flood car cir 8000

缺省情况下，ICMP泛洪攻击报文的限制速率为155000000bit/s

开启ICMP泛洪攻击后的ping结果



4-3 ping测试

### 5.3.3 DHCP常见问题及DHCP Snooping

一DHCP服务的常见问题

架设DHCP服务器可以为客户端自动分配IP地址、掩码、默认网关、DNS服务器等网络参数，简化了网络配置，提高了管理效率。但在DHCP服务的管理上存在一些问题，常见的有：

DHCP Server的冒充

DHCP Server的DOS攻击，如DHCP耗竭攻击

某些用户随便指定IP地址，造成IP地址冲突

1 DHCP Server的冒充

由于DHCP服务器和客户端之间没有认证机制，所以如果在网络上随意添加一台DHCP服务器，它就可以为客户端分配IP地址以及其他网络参数。只要让该DHCP服务器分配错误的IP地址和其他网络参数，那就会对网络造成非常大的危害。

2 DHCP Server的拒绝服务攻击

通常DHCP服务器通过检查客户端发送的DHCP请

求报文中的CHADDR（也就Client MAC address）字段来判断客户端的MAC地址。正常情况下该CHADDR字和发送请求报文的客户端真实的MAC地址是相同的。

攻击者可以利用伪造MAC的方式发送DHCP请求，但这种攻击可以使用交换机的端口安全特性来防止。端口安全特性（Port Security）可以限制每个端口只使用唯一的MAC地址。但是如果攻击者不修改DHCP请求报文的源MAC地址，而是修改DHCP报文中的CHADDR字段来实施攻击，那端口安全就不起作用了。由于DHCP服务器认为不同的CHADDR值表示请求来自不同的客户端，所以攻击者可以通过大量发送伪造CHADDR的DHCP请求，导致DHCP服务器上的地址池被耗尽，从而无法为其他正常用户提供网络地址，这是一种DHCP耗竭攻击。DHCP耗竭攻击可以是纯粹的DOS攻击，也可以与伪造的DHCP服务器配合使用。当正常的DHCP服务器瘫痪时，攻击者就可以建立伪造的DHCP服务器来为局域网

中的客户端提供地址，使它们将信息转发给准备截取的恶意计算机。甚至即使DHCP请求报文的

源MAC地址和CHADDR字段都是正确的，但由于DHCP请求报文是广播报文，如果大量发送的话也会耗尽网络带宽，形成另一种拒绝服务攻击。

3、客户端随意指定IP地址

客户端并非一定要使用DHCP服务，它可以通过静态指定的方式来设置IP地址。如果随便指定的话，将会大大提高网络IP地址冲突的可能性。

二、DHCP Snooping技术介绍

DHCP监听（DHCP Snooping）是一种DHCP安全特性。在每个VLAN基础上启用DHCP监听特性，通过这种特性，交换机能够拦截第二层VLAN域内的所有DHCP报文。

DHCP监听将交换机端口划分为两类：

●非信任端口：通常为连接终端设备的端口，如PC，网络打印机等

●信任端口：连接合法DHCP服务器的端口或者连接汇聚交换机的上行端口

通过开启DHCP监听特性，交换机限制用户端口（非信任端口）只能够发送

DHCP请求，丢弃来自用户端口的所有其它DHCP报文，例如DHCP Offer报文等。而且，并非所有来自用户端口的DHCP请求都被允许通过，交换机还会比较DHCP 请求报文的（报文头里的）源MAC地址和（报文内容里的）DHCP客户机的硬件地址（即CHADDR字段），只有这两者相同的请求报文才会被转发，否则将被丢弃。这样就防止了DHCP耗竭攻击。

信任端口可以接收所有的DHCP报文。通过只将交换机连接到合法DHCP服务的

端口设置为信任端口，其他端口设置为非信任端口，就可以防止用户伪造DHCP服务器来攻击网络

DHCP监听特性还可以对端口的DHCP报文进行限速。通过在每个非信任端口下进行限速，将可以阻止合法DHCP请求报文的广播攻击。

DHCP监听还有一个非常重要的作用

就是建立一张DHCP监听绑定表（DHCP Snooping

Binding）。一旦一个连接在非信任端口的客户端获得一个合法的DHCP Offer，交换

机就会自动在DHCP监听绑定表里添加一个绑定条目，内容包括了该非信任端口的

客户端IP地址、MAC地址、端口号、VLAN编号、租期等信息

三、 DHCP Snooping的配置

前置命令：

[Huawei]dhcp enable

[Huawei]dhcp snooping enable

[Huawei]dhcp snooping enable vlan 1

使能DHCP Snooping功能的顺序是先使能全局下的DHCP Snooping功能，再使能接口或

VLAN下的DHCP Snooping功能。

安全功能1：日志记录所有dhcp服务器（包括伪冒的）

命令：[HUAWEI] dhcp server detect

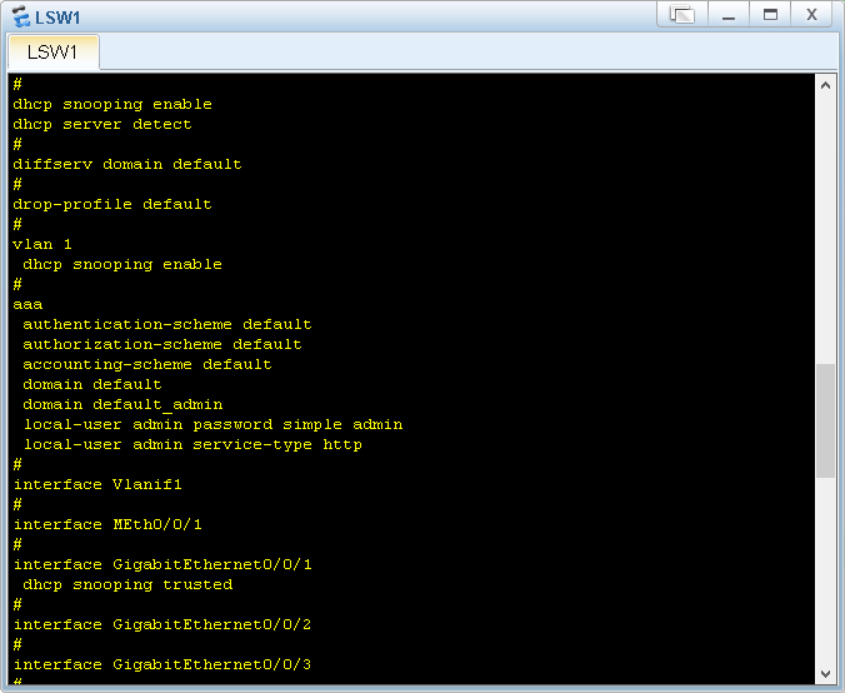
应用场景

当网络中存在伪DHCP Server时，伪DHCP Server将会回应给DHCP Client仿冒信息，如错误的网关地址、错误的DNS服务器、错误的IP等，从而使Client无法正常访问网络或访问到不正确的网络。

DHCP Snooping设备在使能DHCP Server探测功能之后，将会检查并在日志中记录所有DHCP Reply报文中携带的DHCP Server地址与接口等信息。此后网络管理员可根据日志来判定网络中是否存在伪DHCP Server进而对网络进行维护。

安全功能2：防止假冒dhcp服务器

命令：dhcp snooping trusted （接口模式下）



4-4 查询交换配置信息

四 、应用场景

为了使DHCP客户端能通过合法的DHCP服务器获取IP地址，DHCP Snooping安全机制允许将接口设置为信任接口和非信任接口，信任接口正常转发接收到的DHCP报文，非信任接口接收到DHCP服务器响应的DHCP ACK和DHCP OFFER报文后，将丢弃该报文。直接或间接连接管理员信任的DHCP服务器的接口需要设置为信任接口，其他接口设置为非信任接口，从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址，私自架设的DHCP Server仿冒者无法为DHCP客户端分配IP地址

### 5.3.4漏洞扫描系统

**功能：**基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞，根据自身漏洞库对目标进行脆弱性检测，并生产相关报告，提供漏洞修复意见

**部署：**进行旁路部署，通常旁路部署在核心交换机上，需与检测目标网络可达

### 5.3.5日志服务器配置

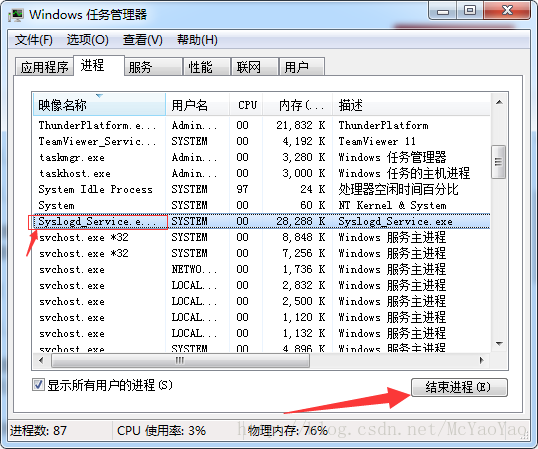
部署日志服务器。为了监控学校重要服务器还有网络设备路由器等

1、日志服务器 安装日志服务软件



4-5安装kiwi server

2、安装完成后在任务管理器中先结束掉syslogd\_service的进程



4-6结束进程

日志服务软件的配置

A点击左上角的File>>Setup

B选择左侧Log to file ，

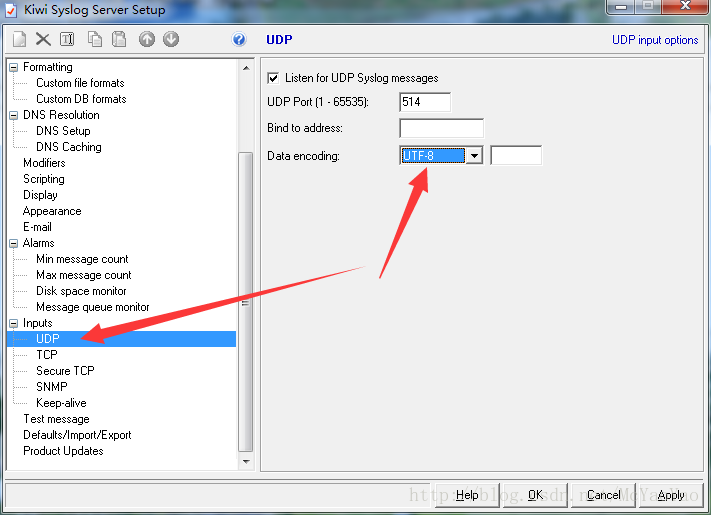
C设置日志存放位置和格式再点击左侧Shedules，然后点击左上角的“新建”进行配置计划任务。

Schedule字段添加日志计划频率（按分钟、小时）

Source字段（设置临时存储日志的路径）

Destination字段（设置最终日志存储目录）

D点击左侧Input>UDP修改Date encoding的值为Utf-8防止部分带有汉字的日志为乱码



4-7配置信息

3、监控的客户端配置

下载安装Evtsys，解压后，先选择对应的系统文件

然后将文件夹里的全部文件拷贝到“C:\Windows\System32”目录

打开Windows命令提示符

输入 evtsys.exe -i -h 日志服务器的ip地址；

启动服务net start evtsys



4-8启动服务

5在监控的计算机操作一下文件 看日志服务器是否监控成功获取日志

如果成功获取



4-9获取客户端日志

6 Huawei设备路由器日志

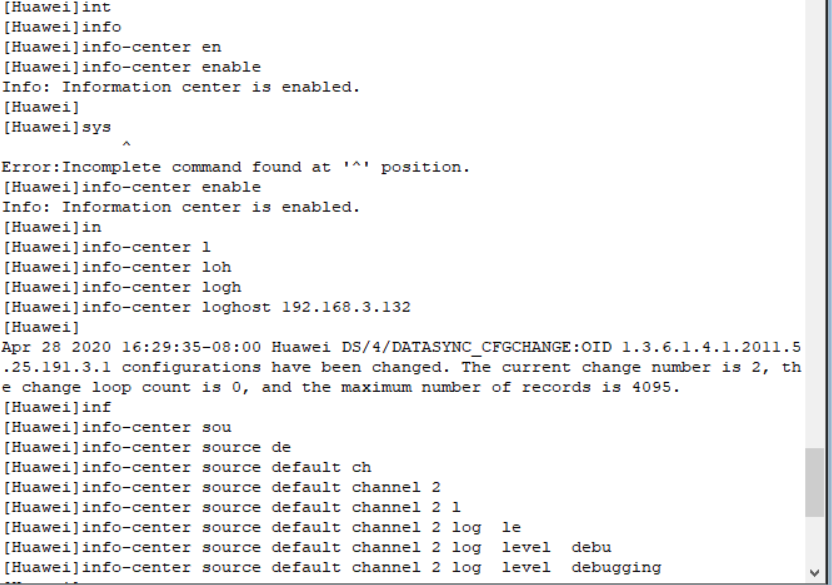
system-view

[Sysname] info-center enable #开启信息中心

[Sysname] info-center loghost x.X.X.X （192.168.3.132） #指定向日志主机输出日志信息

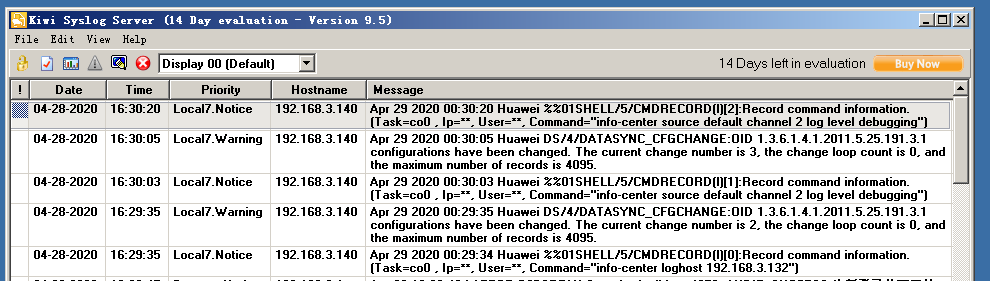
[Sysname] info-center source default channel 2 log level debugging #指定发送消息基本，表示从0-7都发送

[Sysname] info-center loghost source Vlanif1#指定从哪个接口发送



4-10配置命令

华为路由器上的配置信息日志同步到服务器



4-11获取路由器日志

### 5.3.6 证书服务器配置（https）

1 myscse系统登陆时账号密码明文显示，ftp，myscse明文传输所以我们需要配置加密，

Myscse系统是web界面所以我们采用https加密 配置http是采用用证书服务器

采用SSL

SSL原理：SSL（Security Socket Layer）全称是加密套接字协议层，它位于HTTP协议层和TCP协议层之间，用于建立用户与服务器之间的加密通信，确保所传递信息的安全性，同时SSL安全机制是依靠数字证书来实现的。

①浏览器请求与WWW服务器建立安全会话

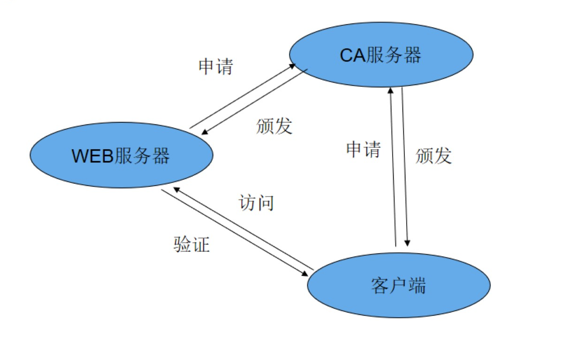
②WWW服务器将自己的公钥发给浏览器

③WWW服务器与浏览器协商密钥位数（40位或128位）

④浏览器产生会话使用的秘密密钥，并用WWW服务器的公钥加密传给WWW服务器

⑤WWW服务器用自己的私钥解密

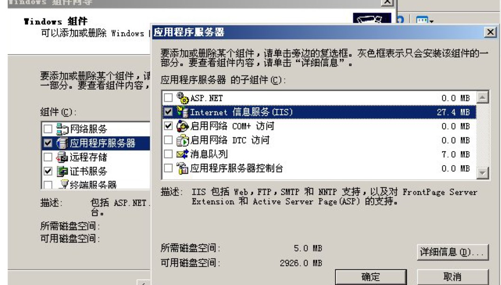
⑥WWW服务器和浏览器用会话密钥加密和解密，实现加密传输



4-13 SSL加密过程

配置过程

win2008安装证书服务器 另外一台安装web服务器



4-14安装web服务



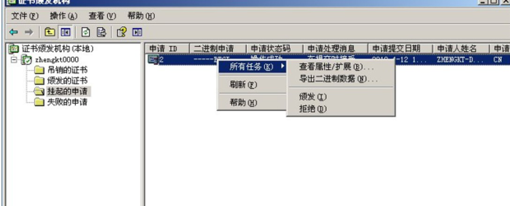
4-15 安装证书服务

win2008 web服务器申请证书(准备请求信息→提交申请)



4-16申请证书

证书服务器审查颁发证书



4-17颁发证书

web服务器下载颁发的证书下载

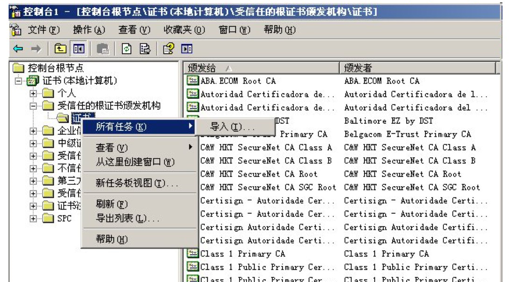


4-18下载证书

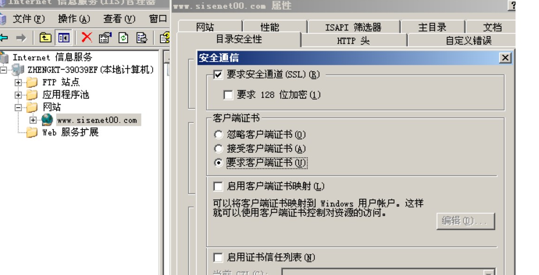
在IIS-WEB服务器上安装证书,使该站点变为SSL站点，切还需要一个CA证书添加到信任的证书机构



4-19下载CA证书

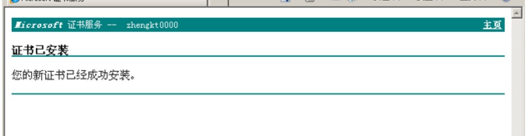


4-20导入CA证书



4-21选择要求客户端证书

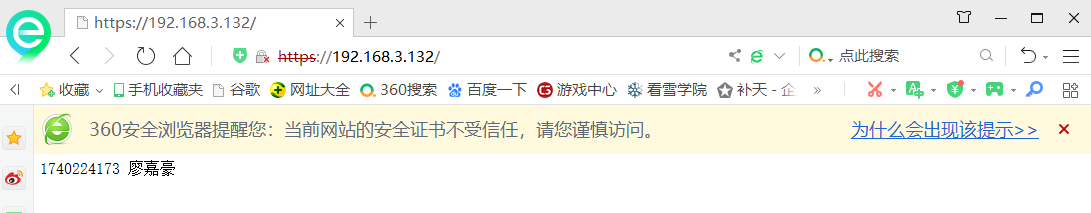
客户端 需要向证书服务器申请证书 证书服务器办法 然后在下载才能用https协议实现web数据的安全浏览



4-22 证书安装成功

登录网址

显示为HTTPS



4-23登录页面

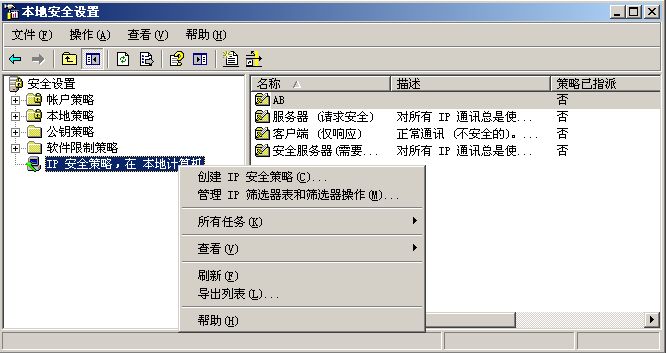
### 5.3.7 ipsec通信加密

与FTP服务器我们可以采用ipsec来实现机密

采用ipsec隧道方式进行加密连接

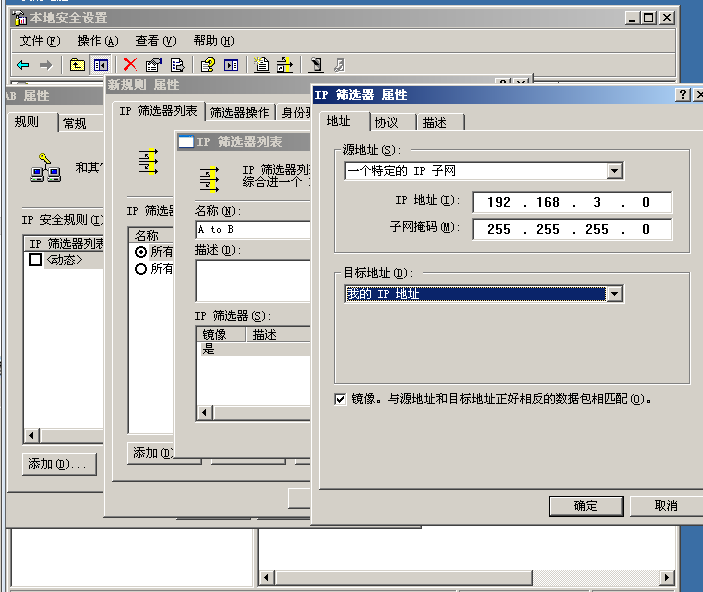
SEVERA————————Client （192.168.3.0网段）

在FTP server上创建ipsec策略



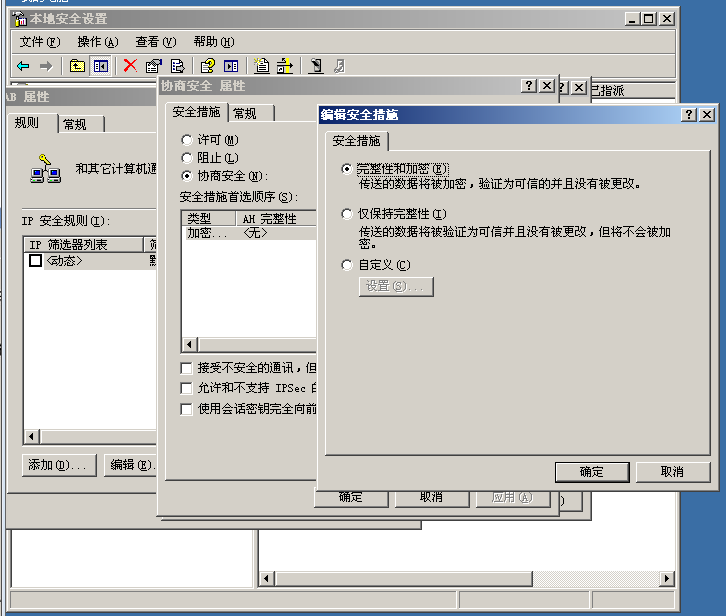
4-23创建策略

添加ip安全策略AB（勾选镜像）并指派

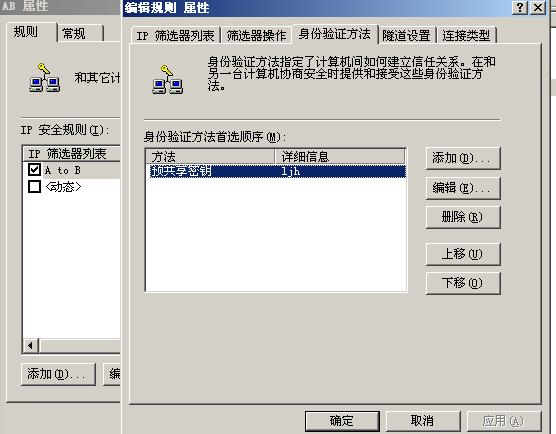


5-24设置网段

设置共享密钥，并勾完整性加密



5-25设置协商安全



4-26这是共享密钥

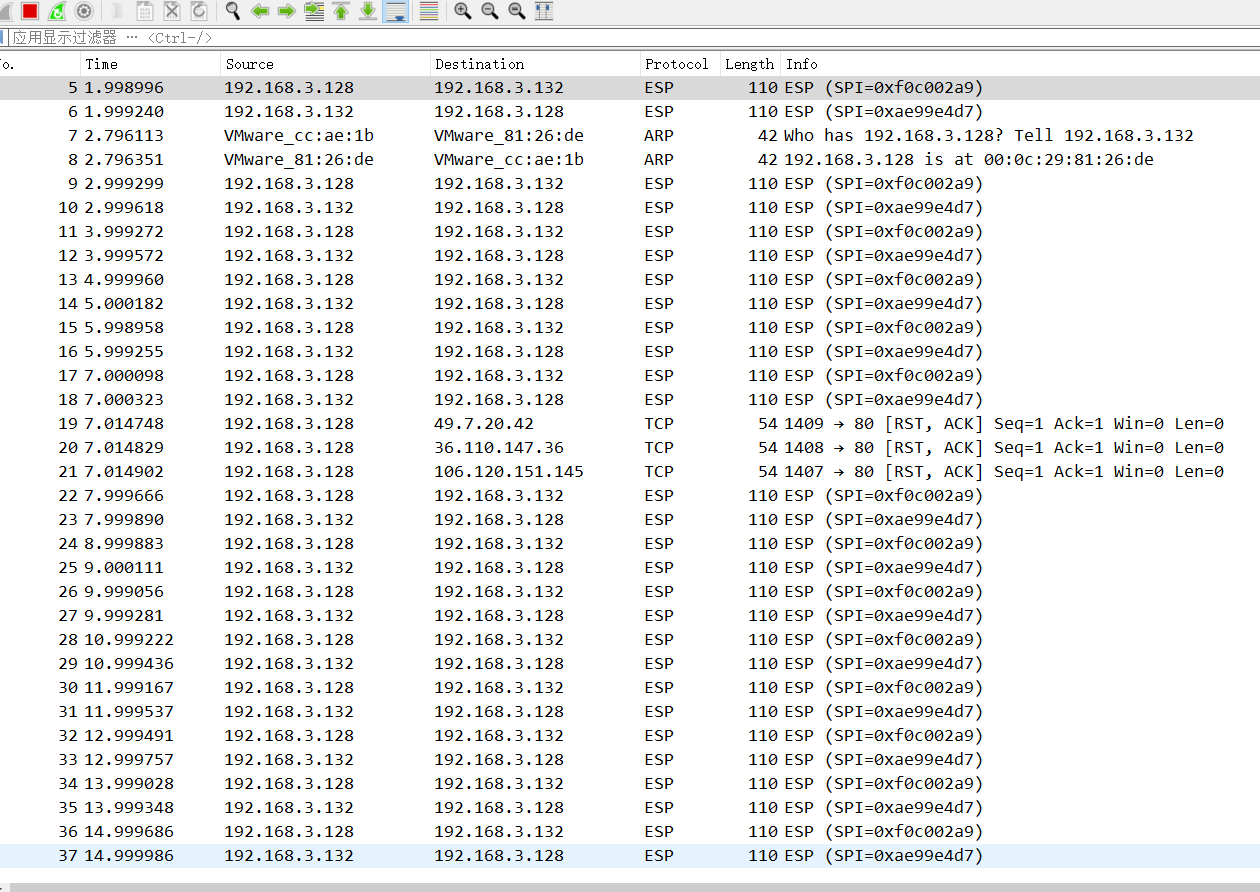
在FTP客户端上创建ipsec策略（同上）

设置共享密钥并勾完整性加密 （同上）

Ljh 两次密钥必须相同不然无法协商通信

添加ip安全策略BA（勾选镜像）并指派 如果一方指派另一方不指派是无法通信的

FTP SERVERA和FTP 客户端实现加密通信 运行协议分析软件，分析通信数据包确定有加密看不到敏感信息



5-27数据包分析

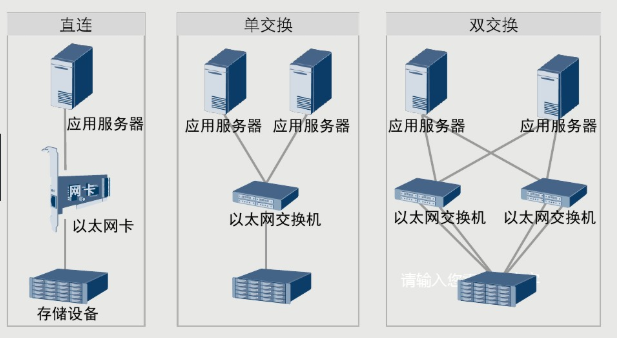
### 5.3.8数据备份与灾难恢复备份

#### 5.3.8.1备份方案

完全备份备份时间周期分为大小两类，一般为周和天完全备份是指每天都对系统进行完整意义的备份。增量备份策略是指每周作一次完全备份，每天只对当天新的或被修改过的数据进行备份。差异备份是指每周对系统作一次完全备份（比如在周日），然后在接下来每天中，只再将当天所有与星期日不同的数据（新的或修改过的）备份到磁带上

因此FTP服务器数据，信息系统数据备份方案 每周二进行完全备份，每一天进行差异备份。

我们需要采用 ISCSI创建存储区域网络（SAN）完成备份储存



4-28 Ip SAN 模型

#### 5.3.8.2 Ip SAN

以2008window作为存储设备win10为服务器

A服务器中安装服务端

B、单击开始菜单\管理工具中出现的Microsoft iSCSI Software Target ，打开iSCSI Target 控制台

C、右键单击iSCSI目标，然后单击创建iSCSI目标，下一步中设置能够访问这个iSCSI目标的IQN标示，单击高级——添加（这里可以使用DNS域名、IP地址、MAC地址和IQN标示符，实验中我们使用IP地址即要使用这个存储服务器的客户端的ip地址）。

接下来为这个iSCSI目标添加磁盘。

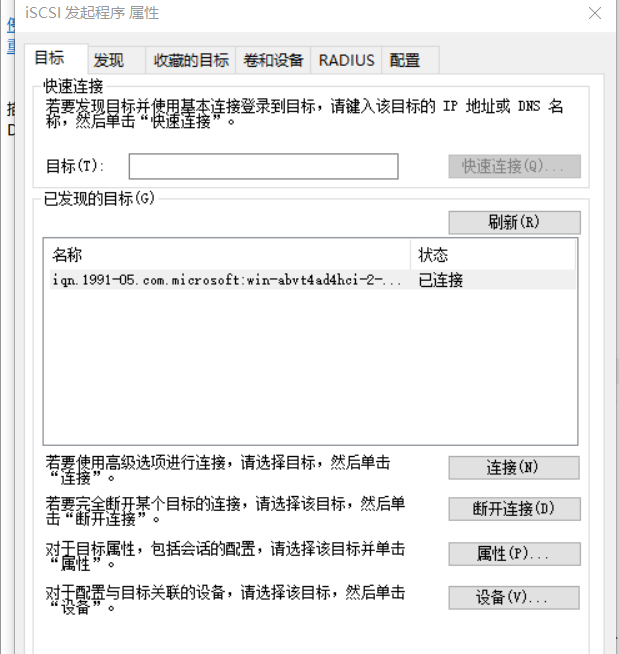
D、右键单击刚刚创建的iSCSI目标，然后单击“为iSCSI目标创建虚拟磁盘”

完成后，配好了ip-san的服务端

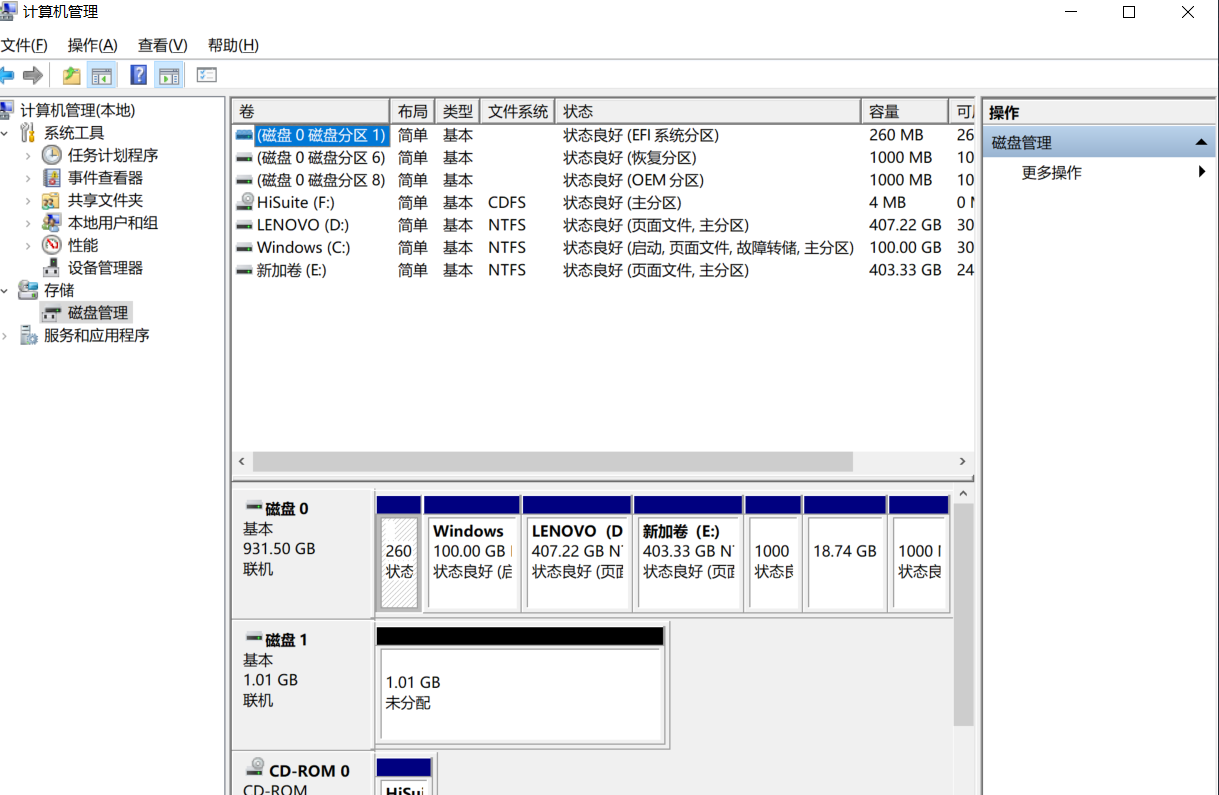
客户端配置：

E Win7以后系统不再需要安装客户端软件，在发现选项中搜索ISISC连接 输入服务端计算机的ip地址点击连接

F打开系统的磁盘管理器，就可看到新增的储存设备了



4-29建立连接



4-30连接磁盘成功后

做为存储服务器在[存储服务器](https://www.idcbest.com/datanews/11002029.html)硬件设备里最重要的肯定是硬盘了所以我们要对服务器的硬盘进行关键设备的硬件冗余

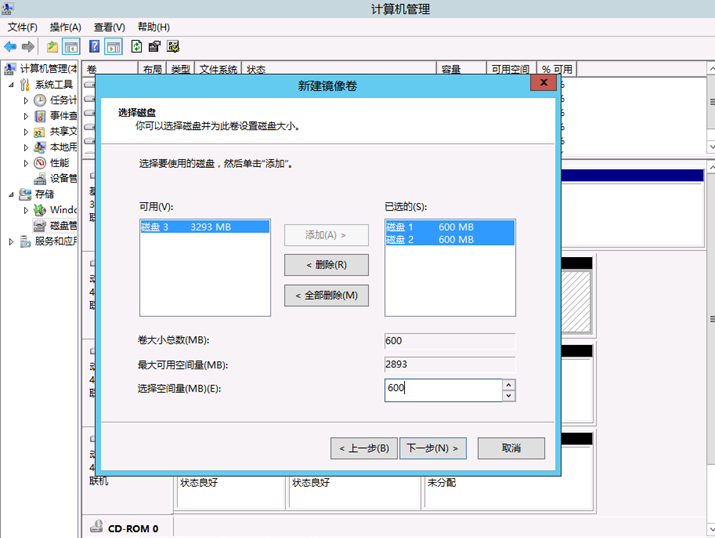
设备的硬件冗余 不直接进行数据的备份，而是把磁盘设备的数据奇偶校验信息保存到出自身以外的每一块磁盘设备中；如果其中一块磁盘出现故障，需要利用剩下的数据和校验信息可以恢复数据

虽然我们可以做阵列来提高安全性，但一般的RAID5、RAID6只能保证1到2块盘损坏的情况下数据是完整的，再损坏数据就要丢失了，所以选择性能好寿命长的硬盘才是解决问题的关键。

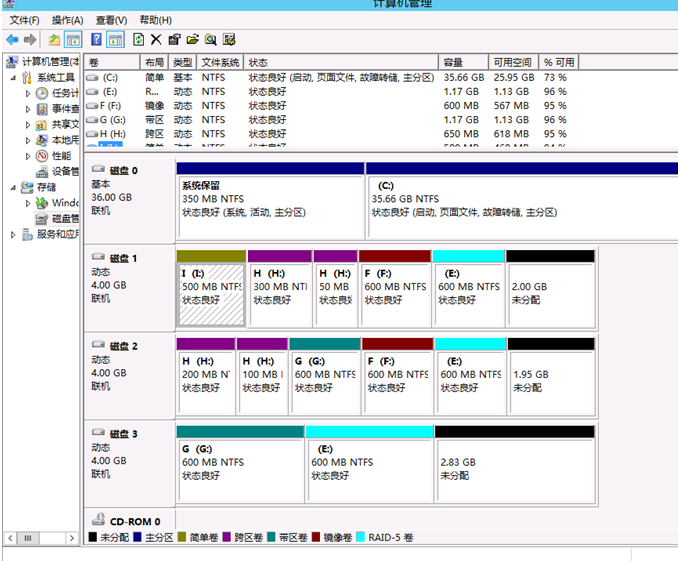
#### 5.3.8.3 RAID-5卷配置

。

，1打开磁盘管理创建先将磁盘转化为动态磁盘，创建RAID-5卷 磁盘1 磁盘2磁 3 大小容量是一样的



4-32选择三个磁盘



4-33磁盘建立成功后

当磁盘其中1块或者2块磁盘损坏我们都可以进行修复磁盘恢复文件

#### 5.3.8.4 灾难恢复备份

一 容灾备份的定义

利用技术、管理手段及相关资源确保关键数据、关键数据处理信息系统、关键业务在灾难发生后可以恢复和重续运营的过程，数据零丢失、业务连续性

灾难

地震、火灾、水灾、战争、恐怖袭击、设备系统故障、人为破坏等无法预料的突发事件。

二 容灾备份系统的种类

数据容灾

建立一个异地的数据系统，该系统是本地关键应用数据的一个可用复制 ，也可比本地数据略微滞后。

应用容灾

是在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的备份应用系统 不仅需要一份可用的数据复制，还要有包括网络、主机、应用、甚至IP等资源的复制或更高层次的容灾系统。

三 容灾备份系统的评价指标

RTO（Recovery Time Objective）恢复时间目标，是指在灾难发生后，信息系统或业务功能从停止到必须恢复的时间要求。

RPO（Recovery Point Objective）恢复点目标，即在灾难发生时，系统和数据必须恢复到的时间点要求。

RTO代表可接受的系统停顿时间，RPO代表可以接受的数据损失程度。

四 容灾备份系统等级

根据对灾难的容忍能力、系统恢复所用时间以及数据丢失的程度，《信息系统灾难恢复规范》（GB/T 20988-2007）将容灾划分为6个等级：

|  |  |  |  |
| --- | --- | --- | --- |
| 等级 | 内容 | RTO | RPO |
| 1 | 基本支持 | 2天以上 | 1至7天 |
| 2 | 备用场地支持 | 24小时以后 | 1至7天 |
| 3 | 电子传输和设备支持 | 12小时以上 | 数小时至1天 |
| 4 | 电子传输及完整设备支持 | 数小时至2天 | 数小时至1天 |
| 5 | 实时数据传输及完整数据支持 | 数分钟至2天 | 0至30分钟 |
| 6 | 数据零丢失和远程集群支持 | 数分钟 | 0 |

五 学校容灾等级选择

根据资金条件切学校情况应该选择三级，保护重要数据和重要文件为主要，

|  |  |  |
| --- | --- | --- |
| 等级 | 备份方式 | 恢复 |
| 第3级  电子链接 | 在相隔较远的地方分别建立两个数据中心，都处于工作状态，通过网络传输备份数据 | 热备中心处于待命状态，网  络传输备份数据有延迟 |

可用到的技术有

存储区域网络SAN(Storage Area Nerwork)（ip san）

远程镜像技术

将数据实时或准实时复制到异地节点

按请求镜像的主机是否需要远程镜像站点的确认信息，又可分为同步远程镜像和异步远程镜像

六 备份方案

A：在1号Server系统中安装，设置成主站。

B：在2号Server上安装，设置成从站

C：正常运行后，2号Server能够实时备份1号Serve中的数据库的数据

D：在1号Server宕机的情况下，2号Serve能接管主服务器的IP和机器名，对外提供所有的服务，保证业务不间断

D：当1号Server修复后，能快速将2号Server上数据恢复到1号Server中。

能实现的效果及主要功能：

（1) 将主服务器上的数据实时智能的备份到从站备份服务器里

（2）如果数据库遭到病毒破坏或者误删除可用数据回退进行解决；回复的任意时间

点的数据

（3）主站宕机或者磁盘柜损坏，备份服务器可接管主站服务器对外服务，保证客户端的正常运行

### 5.3.9 防病毒网关

#### 5.3.9.1概念

防病毒网关就是针对网络安全所面临的新挑战应运而生的。对病毒等恶意软件进行防御的硬件网络防护设备，可以协助企业防护各类病毒和恶意软件，对其进行隔离和清除。当企业在网络的Internet出口部署防病毒网关系统后，可大幅度降低因恶意软件传播带来的安全威胁，及时发现并限制网络病毒爆发疫情，同时它还集成了完备的防火墙，为用户构建立体的网络安全保护机制提供了完善的技术手段。广泛适用于政府、公安、军队、金融、证券、保险等多个领域。

#### 5.3.9.2防病毒网关部署

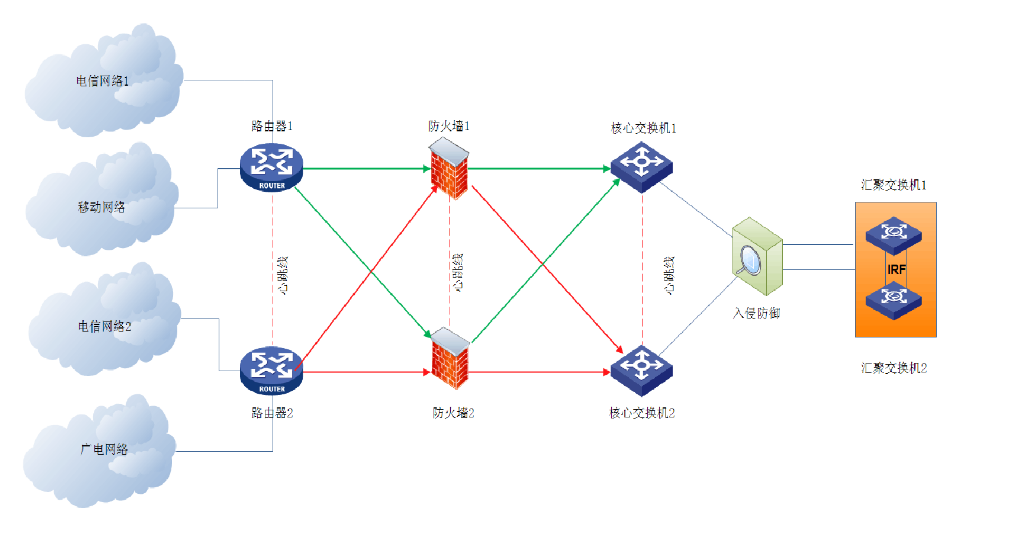
FTP服务器与邮件服务器，出去外网的设置防病毒网关，防止恶意上传病毒破环服务器谁坏数据库，如何部署防病毒网关

防病毒网关的部署位置

建议将防病毒网关部署在入侵和汇聚交换机之间，有以下两点原因1防火墙可以阻断非法改用户访问网络资源，入侵防御可以在线攻击防御，将防病毒网关部署在IPS之后可以大大减轻防病毒网关的负载，提高了防病毒网关的工作效率，

防病毒网关部署在防火墙或者路由器后面都需要连接4根线，而防病毒网关只有两根进线，由于入侵防御的部署模式是两个两出，所以选择部署在入侵防御之后的

防病毒部署的拓扑图：



防病毒网关接线图：



二 .防病毒网关查杀内容的选取，

充分发挥防病毒网关的性能，减少不必要的性能损耗，建议防病毒网关与防火墙协同工作，根据需要防病毒网关主要针对HTTP协议FTP smtp pop3协议报文的查杀，根据实际应用的需要，再做相应的配置

三. 防病毒网关的查杀方式

防病毒网关发现病毒后有四钟处理方式:包括删除文件、隔离文件、清除病毒和记录日志。如果在第一次策略处理失败的情况下，可以设置第二次策略正确的处理病毒。建议设置清除病毒的方式，清除病毒失败后采取隔离文件的方式。

四.蠕虫的防护

防病毒关需开启蠕虫过滤功能，系统默认就会自动添加一些流行蠕虫的查杀规则，其他蠕虫的防护规则可以根据各自应用系统的实际应用情况来设置阈值，其中阈值的设定需防病毒网关与各业务系统之间不断的磨合，才可以达到最佳防护效果，防止系统漏洞类的蠕虫病毒，最好的办法是更新好操作系统的补丁，因此蠕虫的防护需与服务器操作系统补丁更新配合措施

五．防毒库 的升级方式

病毒库的升级模式分为三种：自动升级，手动升级和离线升级，考虑到网络上的病毒每天每时都有新的，变种的病毒，选用自动升级的方法，因为手动升级和离线升级无法做到病毒库的升级的及时性，可能，会造成漏啥的情况对系统造成不良影响，为了保证安全。防火墙配置访问控制策略，处断所有的服务器主动发动访问外网，仅限于个别业务系统有特别需求的，可以访问指定的域名或地址，防火墙开启URP过滤策略，仅允许防病毒网关访问病毒库的升级地址

## 5.4管理制度方面的整改

### 5.4.1管理制度

1. 对管理人员和操作人员执行的日常管理操作建立操作规程
2. 使用者必须妥善保管好自己的用户名和密码，严防被盗窃而导致泄密
3. 设立超级管理员，未经许可，其他工作人员不可删除重要数据
4. 未经许可，任何工作人员不可向外透露内部机密
5. 重要数据应有多份备份，预防数据丢失

### 5.4.2 办公区域管理规程

* 办公区域网络管理规程

1. 各部门应经常检查本部门电脑使用情况，负责电脑的安全使用、密码管理、电子邮件管理等，发现问题及时纠正
2. 网络管理员对区域的所有电脑及信息进行统筹管理，对软件系统维护和改造
3. 爱护室内仪器设备，不随意更改设备位置，按规定操作设备
4. 各部门的重要操作系统，须由专人进行维护管理
5. 未经管理人员允许，不得随意取用磁盘，不得安装异常软件
6. 区域内电脑应安装防病毒软件并及时升级
7. 禁止私自更改、天机计算机设置，不得擅自盗用他人的IP地址或自设置IP地址
8. 禁止将上网端口供未授权用户使用，不得设置上网代理服务器

### 5.4.3 宿舍区域管理规程

* 宿舍区域网络管理规程

1. 学生用户上网必须向网络中心申请，填写用户入网信息表，交纳网费
2. 用户入网前，自行安装相关硬件以及软件
3. 学生用户账户属于个人所有，不得转让，不得借用
4. 学生宿舍网络仅适用于学习、科研、教学及日常个人事务使用，未经许可不得向其他商业用户提供商务服务
5. 设立宿舍区域学生网络管理员，维护学生上网服务

学生不得擅自更改交换机设置，不得破坏

第六章 总结

通过这次项目实训，我了解到做一个解决校园网网络安全解决方案的复杂。在我经过网上和书上查资料的过程中，我只是完成了凤毛麟角，对于一个整体的校园网络来说，理论终究只是理论，需要时间验证，而且在应用中面临的各种各样的问题，还有很多更好更实际的方案没有得到考虑，甚至不了解，在整体的方案设计的方面我需要学习的知识还有很多。