毕业设计说明书(论文)

设计(论文)题目:网络平安系统部署

专　　业:计算机网络技术

班　　级:

学　　号:

姓　　名:

指导教师:

2015 年 10 月　　日

摘要

在计算机网络化的今天，计算机网络正飞速的开展，信息网络已经成为社会开展的重要保证。但是有利必有弊，计算机网络在带来各种利益的同时，却也存在各种技术漏洞，所以其平安性显得格外重要。本文将对计算机网络、网络信息平安的概念进行解读，对网络信息平安存在的问题和重要性进行探讨。对于最近的出现的一些平安的问题，国家渐渐的走向了平安的道路，先后棱镜门事件、中国互联网 DNS 解析故障等等问题的出现，让国家领导相当重视，慢慢地国外厂商 Cisco 网络退出中国市场，国内的厂商也得到飞速的开展。

关键词：计算机网络；信息平安；访问控制；漏洞扫描。

目录

第 1 章 绪论 1
1.1 工程背景 1
1.2 平安加固的作用 2
第 2 章 网络规划 3
2.1 拓扑设计 3
2.2 IP 地址规划表 4
第 3 章 平台搭建与配置 5
3.1 网络平台搭建 5
3.1.1 平台搭建需求 5
3.1.2 WEB_WAF 接口配置信息 6
3.1.3 DCRS 接口配置信息 6
3.1.4 DCFW 接口配置信息 7
3.1.5 DCFS 接口配置信息 7
3.1.6 DCRS 的 vlan 信息 7
3.1.7 DCS 的 VLAN 信息 8
3.1.8 DCRS 静态路由信息 9
3.2 网络平安设备配置与防护 9
3.2.1 DCFW 增强防护机制 9
3.2.2 DCFW 配置 SNAT 10
3.2.3 DCFS 对 PC 带宽控制 11
3.2.4 DCFS 访问控制 13
3.2.5 DCFS 对 BT 流量限速 13
3.2.6 DCFW 设置访问管理限制 16
3.2.7 Web_Waf 平安配置 17
第 4 章 网络设备管理 19
4.1 网络的监控 19
4.1.1 Cacti 配置需求 19
4.1.2 配置 SNMP 协议 19
4.1.3 配置日志效劳器 21
4.2 漏洞分析 22
系统漏洞扫描需求 22
4.2.2 扫描 PC 的开放端口 23
4.2.3 扫描系统的危险漏洞 24
网站漏洞扫描 26
4.3 弱口令密码的猜解 27
第 5 章 设备清单 29
总 结 30
参考文献 31

第 1 章 绪论

1.1 工程背景

建设银行广元支行根据现在的情况需要进行网络升级改造，重新规划拓扑和 IP 地址的分配，平台的搭建与配置，网络设备调试，流量的监控，以及后期存在的平安隐患问题，需要进行工作机系统漏洞扫描，网络系统加固，网络攻击防护，访问控制策略等一系列的工作。

这一次的升级中，最关键的是增加了监控日志系统和云平台的测试，应对各种系统漏洞做出的措施，不仅如此，同时还要考虑员工平安意识的培训，要让员工对信息平安的重要性有所认识，这样才能杜绝平安系统中社会工程学这样的一个环节。

信息系统平安的实现是一个过程而不是目标，信息平安风险是由于资产的重要性，人为或自然的威胁利用信息系统及其管理体系的脆弱性，导致平安事件一旦发生所造成的影响。信息系统的平安性可以通过风险的大小来度量，通过科学地分析系统在保密性、完整性、可用性等方面所面临的威胁，发现系统平安的主要问题和矛盾，就能够在平安风险的预防、减少、转移、补偿和分散等之间做出决策，最大限度地控制和化解平安威胁。

信息平安加固是解决如何确切掌握网络和信息系统的平安程度、分析平安威胁来自何方、平安的风险有多大，加强信息平安保障工作应采取哪些措施，要投入多少人力、财力和物力，确定已采取的信息平安措施是否有效以及提出按照相应信息平安等级进行平安建设和管理的依据等一系列具体问题的重要方法和根底性工作。

信息平安风险加固是信息系统平安保障机制建立过程中的一种评价方法，其结果为信息平安管理提供依据。风险加固将导出信息系统的平安需求，因此，所有信息平安建设都应该以风险加固为起点。信息平安建设的最终目的是效劳于信息化，但其直接目的是为了控制平安风险。

指导该支行信息系统平安技术体系与管理体系的建设。对银行进行信息平安加固后，可以制定企业网络和系统的平安策略及平安解决方案，从而指导银行信息系统平安技术体系〔如部署防火墙、入侵检测与漏洞扫描系统、防病毒系统、数据备份系统、防洪水攻击等〕与管理体系〔平安组织保证、平安管理制度及平安培训机制等〕的建设。

1.2 平安加固的作用

随着现代计算机网络技术和经济社会的不断开展，人们对计算机网络技术的应用提出了更高的要求。系统化、多元化及集成化是现代计算机网络信息管理技术开展的根本趋势。计算机网络技术的蓬勃开展给社会带来了很大的经济效益，与此同时，其自身也有一些平安隐患存在，而怎样才能够将这些平安隐患彻底去除对于计算机网络的平安十分重要。计算机网络信息平安防范技术是一门综合性的学科，其主要是对外部非法用户的攻击进行防范来确保网络的平安的。

明确企业信息系统的平安现状。进行信息平安加固后，可以让企业准确地了解自身的网络、各种应用系统以及管理制度标准的平安现状，从而明晰企业的平安需求。

确定企业信息系统的主要平安风险。在对网络和应用系统进行信息平安加固并进行风险分级后，可以确定企业信息系统的主要平安风险，并让企业选择防止、降低、接受等风险处置措施。

第 2 章 网络规划

2.1 拓扑设计

拓扑如图 2-1 所示，用到了 Linux 云效劳器，PC 机 3 台，防火墙，WAF 防火墙，流量控制器，三层交换机，二层交换机。

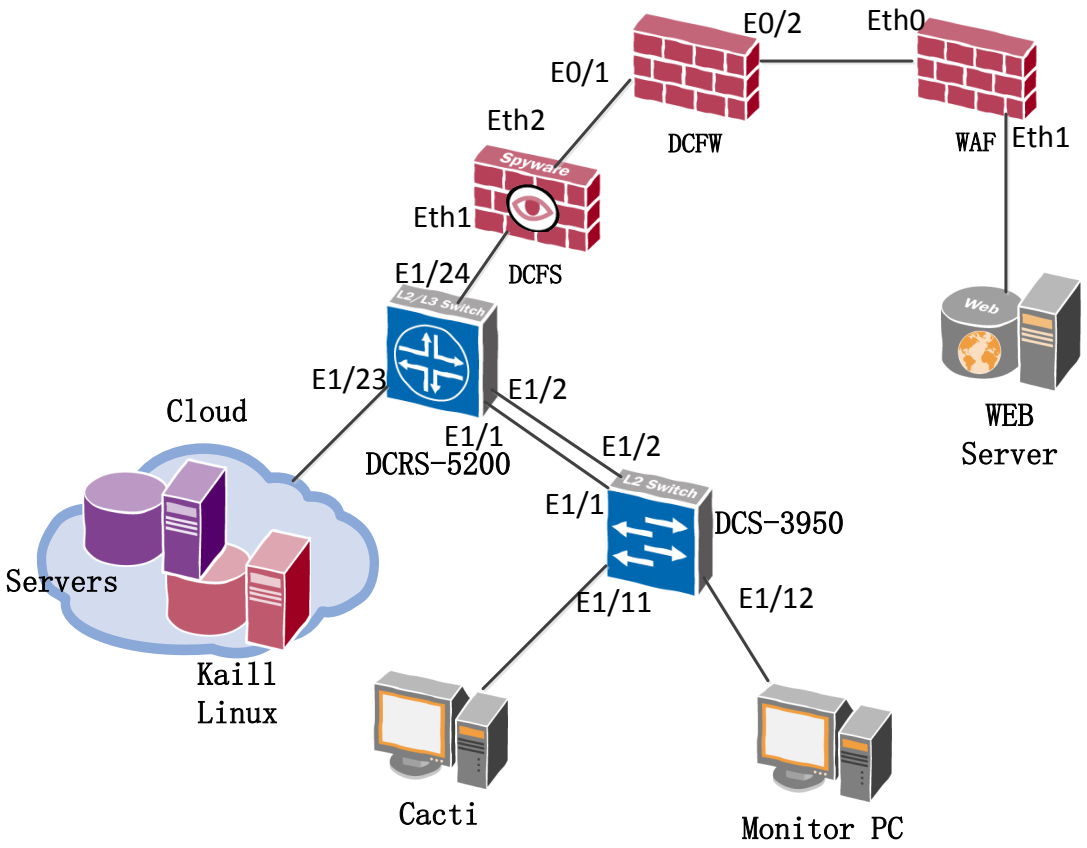

图 2-1 拓扑图

由 WAF 做 web 效劳器防护，防火墙做源目的 NAT，流控设备做内网流量监控与局部限制策略，Linux 效劳器做平安测试用，DCRS-5200 与 DCS-3950 彼此采用 e1/1 和 e1/2 互联；采用生成树〔MSTP〕 起到防环和冗余机制，DCRS-5200 为根桥；DCS-3950 的 e1/2 处于 block 状态；DCRS-5200、DCFS 采用静态路由的方式，全网络互连。

2.2 IP 地址规划表

本方案采用的地址分配方法利用 VLSM 技术,有大量预留空间,本企业网使用静态路由协议 ,在边界防火墙上可做会聚,提高网络性能。如表所示:

表 2-1　ip 地址分配表

设备名称	接口	IP 地址	说明
DCFW	E0/2		与 WAF 相连
	E0/1		与 DCFS 相连
DCFS	Eth2	无	与 DCFW 相连
	Eth1		与 DCRS-5200 相连
WAF	Eth0	193.1.1.2/24 (桥模式)	与 DCFW 相连
	Eth1	193.1.1.2/24 (桥模式)	与 Web 效劳器相连
DCRS-5200	Vlan 2		与 DCFS 相连
	E1/1	Trunk 模式〔Vlan1,3,17〕	
	Vlan 17	1	与 Cloud 相连
	Vlan 3		
DCS-3950	E1/1	Trunk 模式〔Vlan1,3,17〕	
	Vlan 17	1	与 Monitor PC 相连
	Vlan 3	1	与 Cacti 相连
Web Server			与 WAF 相连
Cacti		10.0.30.2/24	与 DCS-3950 相连
Monitor PC		1	与 DCS-3950 相连

第 3 章 平台搭建与配置

3.1 网络平台搭建

3.1.1 平台搭建需求

表 3-1 搭建需求表

序号	网络需求
1	根据网络拓扑图所示，按照 IP 地址规划表，对 WAF 的名称、各接口 IP 地址进行配置。
2	根据网络拓扑图所示，按照 IP 地址规划表，对 DCRS 的名称、各接口 IP 地址进行配置。
3	根据网络拓扑图所示，按照 IP 地址规划表，对 DCFW 的名称、各接口 IP 地址进行配置。
4	根据网络拓扑图所示，按照 IP 地址规划表，对 DCFS 的名称、各接口 IP 地址进行配置。
5	根据网络拓扑图所示，按照 IP 地址规划表，在 DCRS-5200 交换机上创立相应的 VLAN，并将相应接口划入 VLAN。
6	根据网络拓扑图所示，按照 IP 地址规划表，在 DCRS-3950 交换机上创立相应的 VLAN，并将相应接口划入 VLAN。
7	DCRS-5200、DCFS 采用静态路由的方式，全网络互连。
8	Monitor PC、Cacti、Web 效劳器全网互通。
9	DCRS-5200 与 DCS-3950 彼此采用 e1/1 和 e1/2 互联；采用生成树〔MSTP〕起到防环和冗余机制，DCRS-5200 为根桥；DCS-3950 的 e1/2 处于 block 状态。

3.1.2 WEB_WAF 接口配置信息

图 3-1 防火墙设置

3.1.3 DCRS 接口配置信息

```
Interface Ethernet0/0/1
 switchport mode trunk
 switchport trunk allowed vlan 1;3;17
!
Interface Ethernet0/0/2
 switchport mode trunk
 switchport trunk allowed vlan 1;3;17
!
Interface Ethernet0/0/23
 vlan-translation enable
 switchport access vlan 17
!
Interface Ethernet0/0/24
 switchport access vlan 20
!
interface Vlan1
!
interface Vlan17
 description cloud_monitor_gateway
 ip
!
interface Vlan20
 description to_DCFS
 ip
```

interface Vlan3

```
 description cacti_gateway
 ip
!
```

3.1.4 DCFW 接口配置信息

名称	IP地址/网络掩码	安全域	MAC	物理状态	管理状态	链路状态	协议状态	操作
ethernet0/0	0.0.0.0/0	trust	0003.0f13.b830					
ethernet0/1	10.0.2.1/24	trust	0003.0f13.b831					
ethernet0/2	193.1.1.1/24	dmz	0003.0f13.b832					
ethernet0/3	0.0.0.0/0	NULL	0003.0f13.b833					
ethernet0/4	192.168.45.1/24	trust	0003.0f13.b834					
tunnel1	0.0.0.0/0	NULL	----------					
vswitchif1	0.0.0.0/0	NULL	0003.0f13.b83d					

图 3-2 DCFW 接口设置

3.1.5 DCFS 接口配置信息

名称	类型	状态	地址	In	Out	网桥	网络区域	设置
ETH0(管理)	以太网	autoselect (1000baseTX [full-duplex])	192.168.45.1	-	-	无	外网	设置
ETH1(内网)	以太网	autoselect (100baseTX [full-duplex])	10.0.2.100	-	-	5	内网	设置
ETH2(外网)	以太网	autoselect (1000baseTX [full-duplex])		-	-	5	外网	设置
ETH3(内网)	以太网	no carrier		-	-	6	内网	设置
ETH4(外网)	以太网	no carrier		-	-	6	外网	设置

图 3-3 接口的配置信息

3.1.6 DCRS 的 vlan 信息

```
ipv4 forwarding enable
!
vlan 1
!
vlan 2
!
vlan 3
 name cacti
```

```
!
vlan 17
 name cloud_monitor
!
vlan 20
 name to_DCFS
!
Interface Ethernet0/0/1
 switchport mode trunk
 switchport trunk allowed vlan 1;3;17
!
Interface Ethernet0/0/2
 switchport mode trunk
 switchport trunk allowed vlan 1;3;17
!
Interface Ethernet0/0/23
 vlan-translation enable
 switchport access vlan 17
!
Interface Ethernet0/0/24
 switchport access vlan 20
```

3.1.7 DCS 的 VLAN 信息

```
vlan 1
!
vlan 3
 name cacti
!
vlan 17
 name monitor
!
Interface Ethernet1/1
 description to_DCFS_5200_E1/1-2
 switchport mode trunk
 switchport trunk allowed vlan 1;3;17
!
Interface Ethernet1/2
 description to_DCFS_5200_E1/1-2
 spanning-tree mst 0 cost 200000
 switchport mode trunk
 switchport trunk allowed vlan 1;3;17
!
```

```
Interface Ethernet1/11
  switchport access vlan 3
!
Interface Ethernet1/12
  switchport access vlan 17
!
```

3.1.8 DCRS 静态路由信息

ip

3.2 网络平安设备配置与防护

根据建设银行的目前需求，制定一系列的平安措施，以及一些流量的整形、上网行为控制，完善网络部署的根本形成结构。

3.2.1 DCFW 增强防护机制

需求：在 DCFW 的 trust 平安域上，开启 DDOS 攻击防护，连接 web 效劳器的接口属于 DMZ 平安域、连接内网的接口属于 trust 平安域。

步骤一：开启 DDOS 防护

图 3-4 防火墙平安设置

步骤二：定于网络的 trust 区域和 DMZ 区域

图 3-5 防火墙网络设置

3.2.2 DCFW 配置 SNAT

需求：在 DCFW 上做 SNAT，使内网用户网段和效劳器网段能访问 web 效劳器。

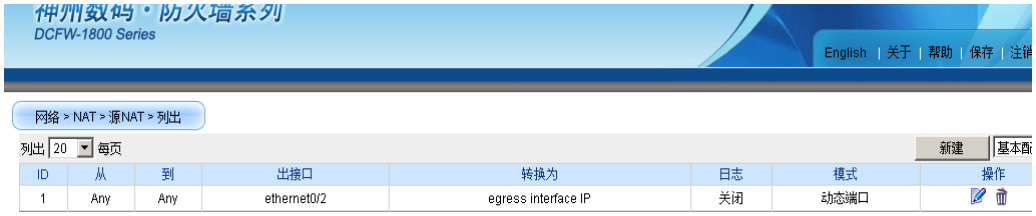

图 3-6 防火墙 NAT 设置

3.2.3 DCFS 对 PC 带宽控制

在 DCFS 上对 Monitor PC 做限速，上传带宽 1M，下载带宽 2M，禁止周一到周五访问 web 效劳器的　　和　　s 效劳。

步骤一：做策略对 monitor PC 进行限速下载带宽设置 2M，上传速度 1M。

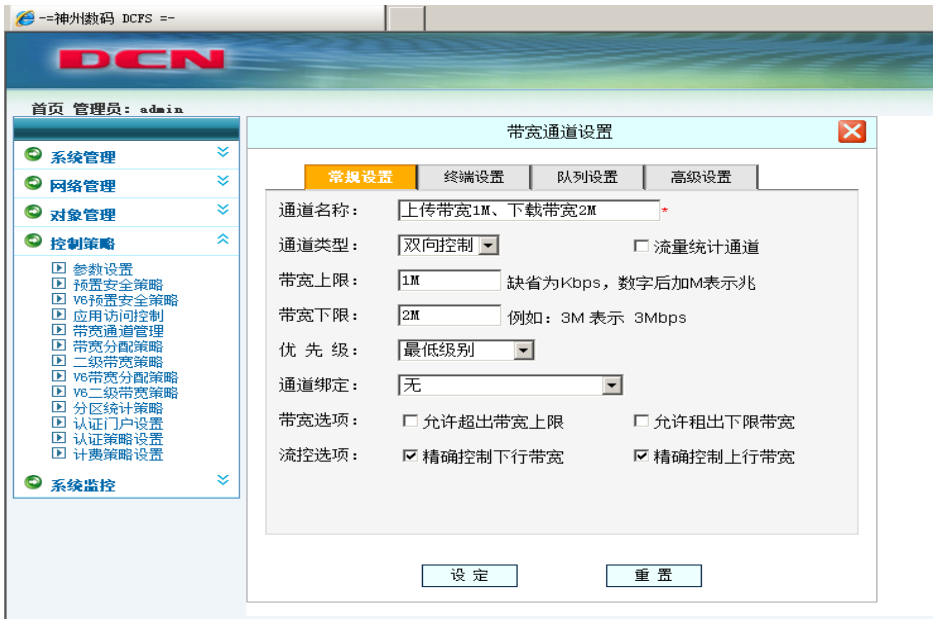

图 3-7 带宽通道设置

步骤二：带宽通道应用到规那么。

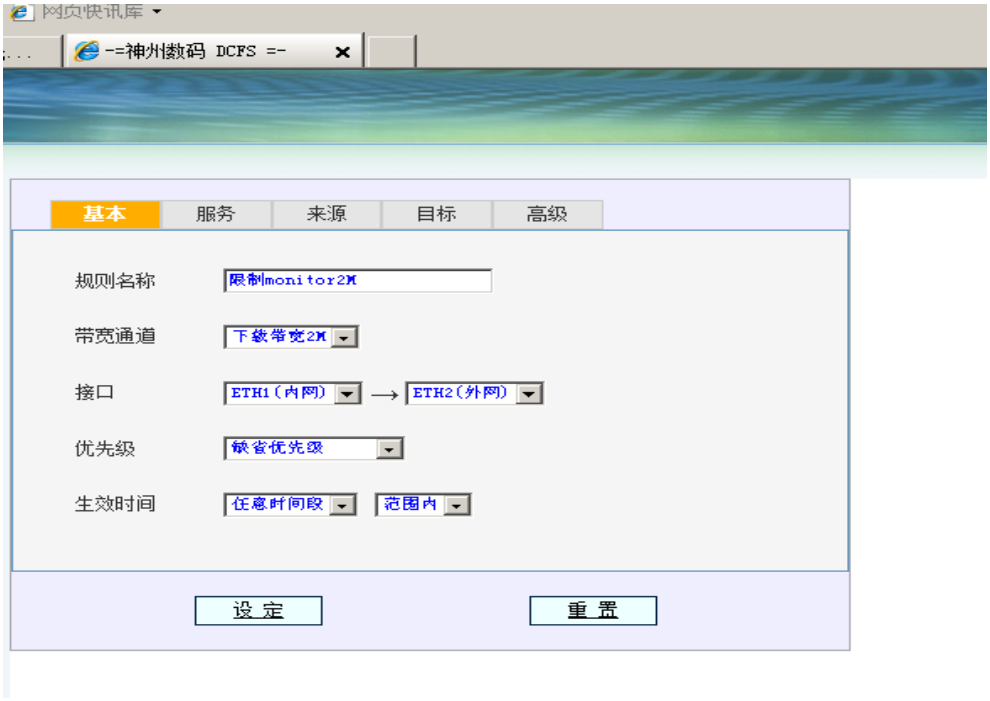

图 3-8 策略根本设置

步骤三：被限速的 MonitorPC 到 WEB 效劳器。

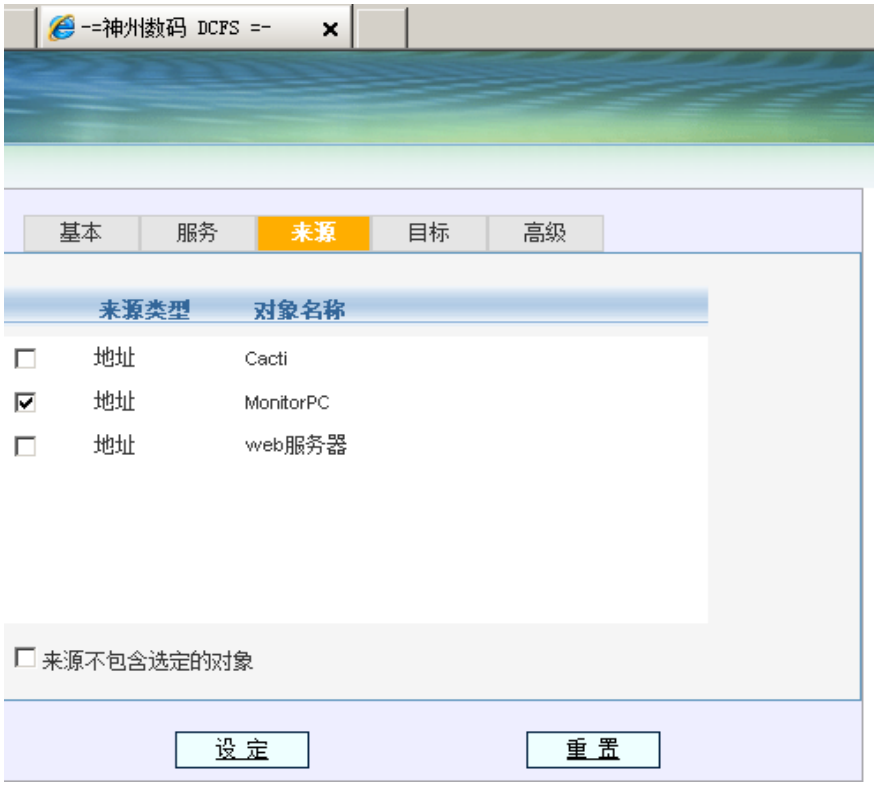

图 3-9 策略对象设置

图 3-10 策略目标设置