□□
目前公司已经确定，数据库应用层和中间键应用层。而服务器的安全是从两个方面来保障的。一个是网络安全方面，另一个是程序安全方面。当程序没有漏洞，但是网络安全没有保障，那么所有的程序和数据都可能被丢失或破解。如果程序留有漏洞和后门，就算网络配置的再安全，也是枉然。这两个安全得到了保障才能真正的保证服务器的安全，仅仅采用网络安全配置是没有作用的。下面对于公司的Linux服务器安全设置和程序开发及安全应用措施如下：一、网络安全配置

□□1、服务器系统的安全配置

□□Linux操作系统的防火墙设置

□□选择软件：由于公司采用的是Ubuntu Server 64bit Linux
操作系统。在这种操作系统下，有一个高级别安全性能的防火墙IPFire最新版，IPFire是基于状态检测的防火墙，采用了内容过滤引擎，通讯服务质量(QoS
：解决网络延迟，阻塞，丢失数据包，传输顺序出错等问题的一种技术，确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。)，虚拟专用网络技术(VPN
：主要功能是：信息包分类，带宽管理，通信量管理，公平带宽，传输保证)和大量的检测记录。而且设置简单，上手快。

□□设置：

□□
a、开启数据库的端口，这个是可以根据公司的要求设置的，比如，3306，4580，8868等等从1000-65535之间，一个终端只开放一个端口；

□□b、开放22端口，即SSH远程管理端口，只针对某个终端开放；

□□c、ubuntu service
版linux的最高权限用户root不要设置使用固定密码(系统会在每隔5分钟自动生成一个密码，连服务器管理员都不可能知道的)；

□□安装杀毒软件

目前网络上用的比较多的杀毒软件，像avast、卡巴斯基都有linux版本的。我这里推荐使用能够avast，因为其是免费的。在杀毒方面也比较强，下面是国内检测杀毒软件的2011年的数据：

国内常用杀毒软件测试结果：

产品	认证	总分	防护	修复	性能
BitDefender	通过	15.5	6.0	4.0	5.5
F-Secure	通过	15.5	5.5	4.5	5.5
Symantec	通过	15.0	5.5	5.0	4.5
卡巴斯基	通过	14.0	5.5	4.5	4.0
熊猫Panda	通过	14.0	5.0	4.5	4.5
AVG	通过	14.0	5.0	4.5	4.5
Eset Nod32	通过	12.5	3.0	4.0	5.5
Trend Micro	通过	12.5	3.5	3.5	5.5
Webroot	通过	12.5	4.5	5.0	3.0
Avast Free	通过	11.5	3.5	2.5	5.5
Avira	通过	11.5	4.0	3.5	4.0
MSE2.0	通过	11.5	2.5	3.5	5.5
Comodo	未通过	10.5	4.0	3.0	3.5
PC Tools	未通过	10.5	4.0	3.5	3.0
McAfee	未通过	8.5	3.0	2.0	3.5
Norman	未通过	8.5	3.0	3.0	2.5

□□多终端应用

□□
Linux是可以多终端独立应用的，为了保障服务器和数据的安全。在这里采用的是多终端多库应用，进行权限分级。如：

□□
在Linux系统下增加一个终端用户，名为SSH，设置密码为：xxxxxxxx，在该用户下安装SSH服务端，并开放22端口。

□□同样的数据库也可以采用这个方式设置，端口是由公司内部指定，比如：
TJW(添健网)用户的密码是yyyyyy，在这个用户下安装MYSQL5.0，并设置端口为3306，数据库里面只针对添健网的数据库操作。

□□
JDW(机电网)用户的密码是sssssss，同样独立安装或者配置MYSQL5.0，设置端口为3307，通过这个用户进去只能操作机电网的数据库

□□让服务器定期更新漏洞

□□操作系统可以设置为定期更新漏洞，这些漏洞往往成为黑客攻击的目标。
不必要担心系统会下载病毒，应为系统只会指定到官方网站上去现在更新。
如果等到服务器能下载非法更新包时，操作系统早已经崩溃。 设置一些傀儡服务器

□□
这个是雅虎的做法，设置几台傀儡服务器(也可以叫中继服务器)具有程序自我回复和还原功能。每台服务器的系统和端口不一。由于系统设置了自我恢复功能和恢复时间。就算黑客攻击掉了其中一台，也可以保证网络系统不会停止运营。

□□2、常见的服务器攻击手段即网络配置

□□

□□拒绝服务(DDOS攻击) 攻击方式：

□□
SYN(DDOS攻击)是最常见又最容易被利用的一种攻击手法，利用TCP协议缺陷，发送了大量伪造的TCP连接请求(由于服务器TCP被请求，但是得不到客户机的确认，就会尝试3次)，使得被攻击方资源耗尽，无法及时回应或处理正常的服务请求。

□□判断方法：

□□输入命令：netstat –n –p TCP | grep SYN_RECV | grep:22 | wc –L
其中22是指端口，如果显示的是10以下则是正常的，显示为10-
30可能被攻击，30以上是绝对被攻击。

□□防范配置：

□□
由于这种攻击是来源于TCP/IP协议的先天漏洞，完全规避是不可能的。只能通过一些手段减轻攻击产生的后果。

□□A、通过物理防火墙和过滤网关防护

□□
这个与IDC机房有关，判断IDC机房是否具备防火墙。通过防火墙代理接收和发送请求来减少对服务器本身的攻击压力。

□□B、加固TCP/IP协议

□□设置请求时间和连接次数，这个调整需要注意的是，如果修改了相关的值。

□□
可能造成操作系统其他的功能毁坏。在没有十足的把握前请不要去设置。下面是Linux下的基础设置不会影响到其他功能：

□□1)
防止各种端口扫描，因为请求和接收是与端口有关。首先要屏蔽扫描端口，这样限制外部计算机通过Ping和扫描端口来判定哪些端口是开放。

□□iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit

□□--limit 1/s –j ACCEPT

□□2)禁止使用ping，同时防止ping云攻击

□□iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit

□□--limit 1/s –j ACCEPT

□□3)开启Linux的syncookies功能，防范部分SYN攻击; sysctl -w net.ipv4.tcp_syncookies=1;

□□4)设置最大半连接数量，修改tcp_max_syn_backlog=2048 sysctl -w net.ipv4.tcp_max_syn_backlog=2048; 5)调整重试次数(默认是重试5次)

□□sysctl -w net.ipv4.tcp_synack_retries=3 sysctl -w net.ipv4.tcp_syn_retries=3

□□
6)开启截流阀功能，设置每秒钟只允许发送一次半连接请求。1秒后自动恢复，如果已经连接上的是不受影响的

□□iptables -I INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT iptables -I FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT

□□C、定期巡检

□□定期让工作人员检查系统日志，查看是否正常。检查方法见 判断方法

□□信息炸弹

□□攻击手段:

□□
信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。一般这种攻击分为:信息炸弹和逻辑炸弹。

□□
信息炸弹主要是短时间内，向数据库中添加大量的数据。使数据库表大小达到文件系统的最高限制，造成数据库表文件损坏。

□□
逻辑炸弹是通过书写一些死循环代码自我数据累加，最后使服务器或应用程序变慢或则文件损坏。

□□判断方法：

□□信息炸弹通常是攻击应用程序和数据库，判断方法

□□
数据库：检查是否较短时间内添加了大量的数据。而且所有的数据是相似的或相同的。同时检查数据管理软件的日志文件。

□□查看系统日志，看是否有程序执行过程中的异常。

□□防范配置：

□□
对于数据库可以采用本身的触发器功能进行判断是否为有效插入，屏蔽掉代码的Web关键字符例如尖括号<>。因为这样的代码是可执行的，可能引起服务器和其他客户电脑中毒。

□□对操作系统设置多端口，多用户权限。一般开放较低的权限用户对外。
这个可以通过服务器的安全配置杜绝。

□□

□□网络监听

□□攻击手段：

□□由于B/S结构的系统，从用户浏览器提交信息到服务器只有两种方法：
Get和Post方法，然后就是在线上传和FTP

□□
这些方法提交信息时有一个网络包，对于服务器来讲是这个包是安全的。而这个包是可以在本机电脑上通过网络嗅敏器监听来获取。

□□
有了包的数据，然后再通过一些注入软件，重复提交或者伪装一些木马后提交。这种工具网络上是有很多的。尤其是在一些文件上传和图片上传最容易挂马。

□□判断方法：

□□
通常这样攻击web服务器是无法检测和判断的。一般需要一个有经验的程序员来规避程序上的问题，然后通过中继服务器验证判断后再最终提交数据和信息。

□□防范配置:

□□1、安装服务器版的杀毒软件，实时监控端口接收到的数据。
2、通过中继服务器程序判断提交的数据，

□□
1)、如果是基本信息提交，就通过验证码、数字证书、ActiveX控件来加密信息。这样监听出来的数据本身是加密的。而且只能通过SSL安全通道提交。

□□
2)、如果提交的是图片，限制图片上传的种类。上传图片后在中继服务器上通过JAVA程序对图片像素无损压缩或转换格式为统一标准。如果JAVA程序在处理过程中异常，则删除这个图片并返回用户上传非法图片和需要重新上传。因为挂马的图片已经不是一张图片格式了，是无法通过程序验证处理。

□□
3)、如果上传的是视频，也要通过专门的压缩程序转换成网站能识别的视频格式。和图片一样。

□□
4)、Word文档或其他文本文档，上传后通过中继服务器压缩成压缩包再转存到最终服务器上。

□□
由于用户所监听的是本机与中继服务器的交互，并不知道中继服务器和最终数据服务器的交互。所以用户无法远程引发病毒程序。

□□

□□破解密码

□□攻击手段:

□□
黑客最喜欢做的事就是破解密码，而且这个破解有很多方法，通常这些方法主要用在客户自己的电脑上。

□□
比如通过木马获取按键循序;采用IE和火狐里面的密码保护程序进行反编译破解;使用既有的一些破解算法比如MD5、Base64等加密算法进行反向加密;使用查看Password属性输入框查看工具等等

□□
服务器方面很少，除非已经攻入进去，否则是拿不到密码的。如果已经攻入进去了就不会再有必要去破解密码了。密码外泄一般是内贼。

□□判断方法：

□□
这个往往主要在于客户自己的电脑上，所以我们无法去判断。不过程序上可以实现在IP段上提醒用户。

□□防范配置：

□□
WEB程序上设计一个ActiveX控件，不采用Password输入框，而是通过ActiveX来提交密码并自主加密。

□□设计一个专门的数字证书，对网页通讯进行加密。

□□二、程序开发及数据安全应用措施

□□1、程序安全

□□
服务器的安全不能只在网络和设备方面，程序也是最重要的一个环节。服务器的操作系统本身的安全系数就比较搞，再加上一些物理防火墙等一个黑客想攻击进如一台服务器是有难度的。但是如果程序具有后门和漏洞，就算服务器安全保护的再强，也是没有用的。

□□1)、开发程序时，应该使用一些必要的工具来检测程序的漏洞和后门;

□□2)、采用中继服务器接口技术，隔开用户直接访问最终服务器;

□□3)、对用户提交和上传的任何文件和信息必须通过转换后再保存;

□□
4)、检查程序的执行速度和资源消耗情况，并且做好优化。防止通过大量的程序执行造成当机(死机)。

□□2、数据安全

□□
主要是指数据库，数据库管理软件具有权限管理和用户管理。最高权限是root用户，这个用户具有所有的增删改查(库、表、字段)的权限。保障数据的安全可以通过下面方式进行：

□□
1)、针对不同的中继服务器接口开放不同的用户和权限，比如：注册新用户时，只开放一个用户为register;这个用户的权限为增加数据的权限，屏蔽掉库、表、字段信息的删改查功能。

□□
2)、多采用存储过程和触发器，这两样功能是通过数据库管理软件自主运行的，与外部程序无关。这样做的好处是，建立一些备份数据库，当用户插入一条数据时自动通过触发器备份

到备份数据库中。对于一些与资金有关的业务逻辑也可以通过触发器计算验证数据的唯一和真实性，然后更新到资金流表中。这样外部程序是不能直接操作资金流表的。并且可以通过存储过程和触发器对某些字段进行专门的加密。

□□

3)、数据库服务器采用磁盘整列，保证文件数据的长期保存;不会因为磁盘坏道造成数据丢失。

□□4)、设置数据库管理然间设置成自动更新，防止因为软件漏洞造成攻击。

□□

5)、采用异地多机热备份，保证数据的安全和完整，同时规避当机风险造成整个系统停运。