网络与信息安全保障措施

一、 网络安全保障措施

为了全面确保本公司网络安全, 在本公司网络平台解决方案设计中, 主要将基于以下设计原则：

1、安全性

在本方案的设计中, 我们将从网络、 系统、 应用、 运行管理、 系统冗余等角度综合分析, 采用先进的安全技术，如防火墙、加密技术，为热点网站提供系统、完整的安全体系。确保系统安全运行。

2、高性能

考虑本公司网络平台未来业务量的增长，在本方案的设计中，我们将从网络、服务器、软件、 应用等角度综合分析，合理设计结构与配置，以确保大量用户并发访问峰值时段，系统仍然具有足够的处理能力，保障服务质量。

3、可靠性

本公司网络平台作为 B2C平台，设计中将做到可靠简单操作，从系统结构、网络结构、技术措施、设施选型等方面综合考虑，以尽量减少系统中的单故障节点，实现 7×24小时的不间断服务。

4、可扩展性

优良的体系结构 （包括硬件、 软件体系结构） 设计对于系统是否能够适应未来业务的发展至关重要。 在本系统的设计中, 硬件系统 （如服务器、 存贮设计等） 将遵循可扩充的原则, 以确保系统随着业务量的不断增长, 在不停止服务的前提下无缝平滑扩展； 同时软件体系结构的设计也

将遵循可扩充的原则，适应新业务增长的需要。

5、开放性

考虑到本系统中将涉及不同厂商的设备技术, 以及不断扩展的系统需求, 在本项目的产品技术选型中，全部采用国际标准 / 工业标准，使本系统具有良好的开放性。

6、先进性

本系统中的软硬件平台建设、 应用系统的设计开发以及系统的维护管理所采用的产品技术均综合考虑当今互联网发展趋势, 采用相对先进同时市场相对成熟的产品技术, 以满足未来热点网站的发展需求。

7、系统集成性

在本方案中的软硬件系统包括我公司以及第三方厂商的优秀产品。 我们将为广大客户提供完整的应用集成服务, 使客户网站将更多的资源集中在业务的开拓与运营中, 而不是具体的集成工作中。

8、硬件设施保障措施：

我公司的信息服务器设备符合电子商务网络平台的各项技术接口指标和终端交易的技

术标准，不会影响公网的安全。 本公司租用新疆电信的 IDC 放置信息服务器的标准机房环境，包括：空调、照明、湿度、不间断电源、防静电地板等。新疆电信为本公司服务器提供一条高速数据端口用以接入 CHINANET网络。系统主机系统的应用模式决定了系统将面向大量的用户和面对大量的并发访问， 系统要求是高可靠性的关键性应用系统， 要求系统避免任何可能的停机和数据的破坏与丢失。 系统要求采用最新的应用服务器技术实现负载均衡和避免单点故障。

1）、系统主机硬件技术

CPU：32位长以上 CPU，支持多 CPU结构，并支持平滑升级。

服务器具有高可靠性， 具有长时间工作能力， 系统整机平均无故障时间 (MTBF)不低于 100000 小时， 系统提供强大的诊断软件，对系统进行诊断。服务器具有镜象容错功能，采用双盘容错，双机容错。 主机系统具有强大的总线带宽和 I/O 吞吐能力， 并具有灵活强大的可扩充能力

2)、配置原则

(1) 处理器的负荷峰值为 75%；

(2) 处理器、内存和磁盘需要配置平衡以提供好效果；

(3) 磁盘 (以镜像为佳) 应有 30-40%冗余量应付高峰。

(4) 内存配置应配合数据库指标。

(5)I/O 与处理器同样重要。

3)、系统主机软件技术：

服务器平台的系统软件符合开放系统互连标准和协议。操作系统选用通用的多用户、多任务 ubuntu server 操作系统， 系统应具有高度可靠性、 开放性， 支持对称多重处理 （SMP）功能，支持包括 TCP/IP 在内的多种网络协议。符合 C2级安全标准：提供完善的操作系统监控、报警和故障处理。应支持当前流行的数据库系统和开发工具。

4)、系统的存储设备的技术

RAID5的磁盘阵列等措施保证系统的安全和可靠。

I/O 能力可达 6M/s。

提供足够的扩充槽位。

5)、系统的存储能力设计

系统的存储能力主要考虑用户等数据的存储空间、 文件系统、 备份空间、测试系统空间、数据库管理空间和系统的扩展空间。 服务器系统的扩容能力系统主机的扩容能力主要包括三个方面：性能、 处理能力的扩充－包括 CPU及内存的扩充存储容量的扩充－磁盘存储空间的扩展 I/O 能力的扩充 , 包括网络适配器的扩充 (如 FDDI 卡和 ATM卡) 及外部设备的扩充 （如外接磁带库、光盘机等）

6)、软件系统保证措施：

操作系统： ubuntu SERVER 网络操作系统

防火墙： CISCOPIX 硬件防火墙 ubuntu SERVER操作系统 具有庞大的社区力量用户可以方便

地从社区 升级站点保持数据联系，确保操作系统修补现已知的漏洞。

利用 NTFS分区技术严格控制用户对服务器数据访问权限。

操作系统上建立了严格的安全策略和日志访问记录 . 保障了用户安全、 密码安全、 以及网络对系统的访问控制安全、 并且记录了网络对系统的一切访问以及动作。 系统实现上采用标准的基于 WEB中间件技术的三层体系结构， 即：所有基于 WEB的应用都采用 WEB应用服务器技术来实现。

7）中间件平台的性能设计：

可伸缩性：允许用户开发系统和应用程序，以简单的方式满足不断增长的业务需求。

安全性：利用各种加密技术，身份和授权控制及会话安全技术，以及 Web安全性技术， 避免用户信息免受非法入侵的损害。

完整性：通过中间件实现可靠、高性能的分布式交易功能，确保准确的数据更新。

可维护性：能方便地利用新技术升级现有应用程序，满足不断增长的企业发展需要。

互操作性和开放性：中间件技术应基于开放标准的体系，提供开发分布交易应用程序功能，可跨异构环境实现现有系统的互操作性。能支持多种硬件和操作系统平台环境。

8）网络安全方面：

多层防火墙： 根据用户的不同需求， 采用多层高性能的硬件防火墙对客户托管的主机进行全面的保护。

异构防火墙：同时采用业界最先进成熟的 Cisco PIX 硬件防火墙进行保护，不同厂家不同结构的防火墙更进一步保障了用户网络和主机的安全。

防病毒扫描：专业的防病毒扫描软件，杜绝病毒对客户主机的感染。

入侵检测：专业的安全软件，提供基于网络、主机、数据库、应用程序的入侵检测服务，在防火墙的基础上又增加了几道安全措施，确保用户

9）系统的高度安全。

漏洞扫描： 定期对用户主机及应用系统进行安全漏洞扫描和分析， 排除安全隐患， 做到安全防患于未然。 CISCOPIX 硬件防火墙运行在 CISCO交换机上层提供了专门的主机上监视所有网络上流过的数据包， 发现能够正确识别攻击在进行的攻击特征。 攻击的识别是实时的， 用户可定义报警和一旦攻击被检测到的响应。此处，我们有如下保护措施：

a、全部事件监控策略 此项策略用于测试目的，监视报告所有安全事件。在现实环境下面，此项策略将严重影响检测服务器的性能。

b、攻击检测策略 此策略重点防范来自网络上的恶意攻击， 适合管理员了解网络上的重要的网络事件。

c、协议分析 此策略与攻击检测策略不同， 将会对网络的会话进行协议分析， 适合安全管理员了解网络的使用情况。

d、网站保护 此策略用于监视网络上对 HTTP流量的监视， 而且只对 HTTP攻击敏感。 适合安全管理员了解和监视网络上的网站访问情况。

ubuntu 网络保护 此策略重点防护 ubuntu 网络环境。

e、会话复制 此项策略提供了复制 Telnet， FTP，SMTP会话的功能。此功能用于安全策略的

定制。

DMZ监控此项策略重点保护在防火墙外的 DMZ区域的网络活动。 这个策略监视网络攻击和典型的互联网协议弱点攻击, 例如（HTTP,FTP,SMTP,POP和 DNS）, 适合安全管理员监视企业防火墙以外的网络事件。

f 、防火墙内监控 此项策略重点针对穿越防火墙的网络应用的攻击和协议弱点利用, 适合防火墙内部安全事件的监视。

10）数据库服务器平台

数据库平台是应用系统的基础 , 直接关系到整个应用系统的性能表现及数据的准确性和安全可靠性以及数据的处理效率等多个方面。本系统对数据库平台的设计包括：

数据库系统应具有高度的可靠性，支持分布式数据处理；

支持包括 TCP/IP 协议及 IPX/SPX 协议在内的多种网络协议；

支持 UNIX和 MS NT等多种操作系统，支持客户机 / 服务器体系结构，具备开放式的客户编程接口，支持汉字操作；具有支持并行操作所需的技术（如： 多服务器协同技术和事务处理的完整性控制技术等） ；支持联机分析处理（ OLAP）和联机事务处理（ OLTP），支持数据仓库的建立；

要求能够实现数据的快速装载，以及高效的并发处理和交互式查询；支持 C2级安全标准和多级安全控制，提供 WEB服务接口模块，对客户端输出协议支持 HTTP2.0 、SSL3.0等；支持联机备份，具有自动备份和日志管理功能。