A 集团综合网络信息系统技术方案提议书

（硬件集成部分）

第一章 总则.....4

1.1 相关本方案提议书.....4

1.2A 集团综合信息系统现实状况.....4

1.3A 集团综合信息系统建设目标.....4

第二章 建设标准.....5

2.1 优异性.....5

2.2 标准性.....5

2.3 兼容性.....6

2.4 可升级和可扩展性.....6

2.5 安全性.....6

2.6 可靠性.....6

2.7 易操作性.....6

第三章 网络系统方案.....7

3.1 广域网设计.....7

3.1.1 需求分析.....7

3.1.2 广域网计划.....8

3.1.3 网络互连设计.....9

3.1.2.1 带宽分配.....9

3.1.2.2 QOS 设计.....10

3.1.2.3 网络设备选型.....12

3.1.2.4 网络布署.....12

3.1.2.5VPN 设计.....14

3.1.2.6 网络管理.....15

第四章 网络安全方案.....16

4.1 安全设计.....16

4.1.1 防火墙技术.....*17*
4.2.1.1 防火墙选型.....17
4.2.1.2 技术细节.....17
4.2.1.3 防火墙布署.....24
4.2.2 入侵检测.....*24*
4.2.2.1 入侵检测技术.....25
4.2.3 防病毒设计.....*27*
4.2.4.1 产品选型.....30
4.2.4.2 防病毒布署.....32
第五章 主机方案.....36
5.1 主机选型标准.....36
5.2 小型机选型和设计.....37
5.2.1IBM P650 介绍.....*37*
5.3 双机热备.....43
5.3.1 系统故障分析.....*44*
5.3.2 HACMP 功效及双机原理.....*44*
5.4PC 服务器选型.....47
第六章 工程管理和实施.....47
6.1 工程督导.....47
6.1.1 工作目标.....*47*
6.1.2 内容.....*48*
6.1.2.1 具体工程计划.....48
6.1.2.2 基于工程计划协调工程进展.....48
6.1.2.3 工程管理.....48
6.1.2.4 人力资源和设备资源统一管理.....48
6.1.2.5 统一协调.....49

6.1.3 工程管理计划.....*49*
6.1.4 工程协调会.....*49*
6.2 工程实施进度一览表.....50
6.3 每一个具体工程阶段具体描述.....51
6.3.1 开箱验收.....*51*
6.3.2 安装环境验收.....*51*
6.3.3 设备现场安装.....*51*
6.3.3.1 硬件安装.....51
6.3.3.2 软件安装.....52
6.3.3.3 参数配置.....52
6.3.3.4 现场故障维修.....52
6.3.3.5 网络升级技术支持.....52
6.3.4 单节点测试和验收.....*52*
6.3.5 系统初验和系统试运行.....*53*
6.3.6 系统终验.....*53*
6.3.7 在协议设备保修期内技术支持.....*54*
6.3.7.1 技术支持概念.....54
6.3.7.2 技术人员培养.....54
6.3.7.3 技术支持构架.....54
6.3.7.4 灵活有效技术支持通信环境.....55
6.3.7.5 有效技术支持方法.....55
第七章 网络培训计划.....**56**
7.1 培训计划.....57
7.2 培训目标.....57
7.3 培训方法.....57
7.4 培训对象.....58

7.5 培训老师.....58
7.6 培训课程.....58
7.6.1 课程列表.....*58*
第八章 维护和支持.....61
8.1 服务等级.....61
8.2 硬件支持服务.....62
第九章 结束语.....63

第一章 总则

1.1 相关本方案提议书

然而“功欲善其事，必先利其器”，A 集团深刻认识到业务要发展、必需提升企业内部关键竞争力、而建立一个方便快捷安全通信网络综合信息支撑系统，已迫在眉睫，A 企业作为一个致力于企业信息化和系统集成高科技企业很荣幸参与 A 集团综合网络信息系统建设，期望能尽自己全力来施展我们专长来实现 A 集团网络信息系统建设。

1.2A 集团综合信息系统现实状况

现在，A 集团还未在全企业建立统一企业信息管理系统，关键是在总企业及七大区域性企业之间经过远程异步数据传动方法（Modem 对拔）进行数据采集和邮件传输，共有二十余个基于 Lotus Domino/Notes4.6 开发数据模块在应用。

A 集团拟建企业信息系统将是覆盖整个 A 集团专业化网络信息管理系统。该系统将建立一个统一企业办公、协同运作及管理支撑综合平台，提升办公效率、提升信息综合利用和提升企业管理水平，从而提升企业经济效益。

A 集团信息系统建设最终将达成以下目标：

(1)以优异成熟计算机技术和建筑技术为关键手段，把 A 集团信息系统建成一个覆盖全集团包含综合办公和各专业管理系统在内支撑建筑行业辅助管理系统，建立一个统一企业办公及运作支撑综合平台，以提升办公效率和企业管理水平，提升信息分析处理能力，从而提升企业经济效益。

(2)为 A 集团职员、用户、合作伙伴提供多种方便快捷交流形式，提升服务质量，增强 A 集团竞争力。

(3)加强知识管理，建立企业本身知识库。

1.3A 集团综合信息系统建设目标

A集团信息系统关键提供电子邮件服务、日常办公管理、财务管理、行业业务步骤处理和知识管理功效。依据A集团现在发展情况，估计到 年底共有上网职员约为1000名，底约为名。

A 集团综合信息系统建设，本着“实用、优异、升级简便、扩充性好、开放性好”五项基础标准进行。 依据企业实际情况和具体应用需求及行业特点，采取分期分阶段实施。 在项目实施过程中，以少花钱多办事为标准，每期投资全部应有继承性。 本期项目标目标是建立以下系统：

（1）建立连通 A 集团内部各组织机构网络平台；

（2）建立一个安全、稳定、高效网络运行空间；

（3）建立通用办公系统及邮件系统；

（4）建立财务管理系统；

（5）内部网站、网络视频会议、BBS 交流协作环境建设；

（6）建立适合建筑行业综合业务管理系统；

（7）加强知识管理，建立企业本身知识库；

本系统建设能满足未来 5 年内业务需求升级，

第二章　建设标准

多业务网络系统方案以实现以上功效为基础要求，在设计上努力争取做到既要采取国际上优异技术，又要确保系统安全可靠性和实用性。具体来讲，其设计遵照以下标准：

2.1 优异性

系统主机系统、网络平台、数据库系统、应用软件均应使用现在国际上较优异、较成熟技术，符合国际标准和规范；

2.2 标准性

所采取技术标准化，能够确保网络发展一致性，增强网络兼容性，以达成网络互连和开放。为确保未来不一样厂家设备、不一样应用、不一样协议连接，整个网络从设计、技术和设备选择，必需支持国际标准网络接口和协议，以提供高度开放性。

全方面支持 IEEE 工业标准：802.1d，802.1p，802.1q，802.1x，802.3，802.3u，802.3z；支持路由协议：IP RIP V1/2，OSPF，BGP-4；信令标准：H.323,RTP/CRTP.

支持：IPsec、L2TP、GRE、MPLS-VPN 规范。

支持多址广播协议：IGMP，DVMRP，PIM-DM，PIM-SM；

网络管理协议：SNMP，RMON，RMON2；

2.3 兼容性

跟踪世界科技发展动态，网络计划和现有光纤传输网及将要改造分配网有良好兼容，在采取优异技术前提下，最大可能地保护已经有投资，并能在已经有网络上扩展多个业务。

2.4 可升级和可扩展性

伴随技术不停发展，新标准和功效不停增加，网络设备必需能够经过网络进行升级，以提供更优异、更多功效。在网络建成后，伴随应用和用户增加，关键骨干网络设备交换能力和容量必需能作出线性增加。设备应能提供高端口

密度、模块化设计和多个类接口、技术选择，以方便未来更灵活扩展。

2.5 安全性

因为系统和其它系统连接，所以，考虑系统安全性是一个很关键方面。应采取设有安全控制网关设备相连，使用 VPN 技术和防火墙等。

2.6 可靠性

本系统是 7x 二十四小时连续运行系统，从硬件和软件两方面来确保系统高可靠性。

硬件可靠性

系统关键部件采取冗余结构，如：传输方法备份，提供备份组网结构；关键计算机设备（如数据库服务器），采取 CLUSTER 技术,支持双机或多机高可用结构；配置不间断电源等。

软件可靠性

充足考虑异常情况处理，含有强容错能力、错误恢复能力、错误统计及预警能力并给用户以提醒；并含有进程监控管理功效，确保各进程可靠运行数据库系统应。

网络结构稳定性

当增加/扩充应用子系统时，不影响网络整体结构和整体性能，对关键网络连接采取主备方法，已确保数据传输可靠性。

本系统应含有较强容灾容错能力，含有完善系统恢复和安全机制；

2.7 易操作性

提供汉字方法图形用户界面，简单易学，方便实用。

优良性能价格比。

系统应着重考虑和满足以上设计要求。

第三章　网络系统方案

该系统包含：36 个网络节点互连方案、线路备份、内部局域网建设。

3.1 广域网设计

现在 A 集团在全国有 36 处企业极其分支机构，能够分为 3 类：1 企业总部（数量 1）、2 区域性企业及本部（数量 7）、3 分企业及事业部（数量 28）。

3.1.1 需求分析

以下表在全国 A 集团有 36 个节点，其分布以下：

企业名称	所属类别	所在地	用户数	备注
集团总部	总企业	杭州	100	总部
A 一建	区域性企业	东阳	50	区域性企业
A 二建	区域性企业	杭州	100	区域性企业
A 三建	区域性企业	上海	100	区域性企业
A 四建	区域性企业	北京	50	区域性企业
A 五建	区域性企业	西安	100	区域性企业
A 六建	区域性企业	武汉	50	区域性企业
A 七建	区域性企业	广州	50	区域性企业
集团本部	总企业	东阳	50	同 A 一建共
金华分企业	分企业	金华		隶属 A 一建
义东分企业	分企业	义乌		隶属 A 一建
温州分企业	分企业	温州		隶属 A 一建
衢州分企业	分企业	衢州		隶属 A 一建
宁波分企业	分企业	宁波		隶属 A 二建
嘉兴分企业	分企业	嘉兴		隶属 A 二建
南京分企业	分企业	南京		隶属 A 三建
合肥分企业	分企业	合肥		隶属 A 三建

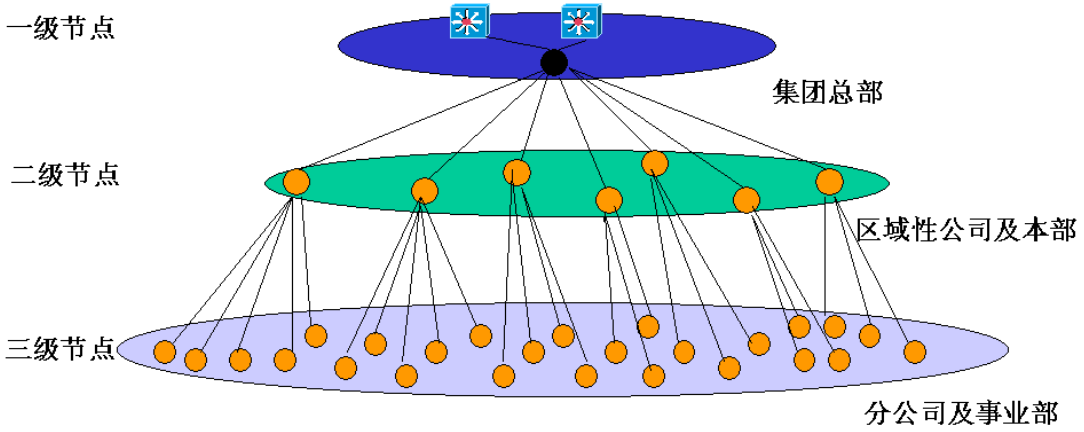
天津分企业	分企业	天津		隶属 A 四建

内蒙分企业	分企业	呼和浩特		隶属 A 四建
青海分企业	分企业	西宁		隶属 A 五建
甘肃分企业	分企业	酒泉		隶属 A 五建
湖南分企业	分企业	长沙		隶属 A 六建
江西分企业	分企业	南昌		隶属 A 六建
A 高级中学	子企业	东阳		子企业
杭州天翔房产企业	子企业	杭州		子企业
A 房产开发企业	子企业	东阳		子企业
西安亚东房产企业	子企业	西安		子企业
湖南天翔房产企业	子企业	长沙		子企业
上海亚东房产企业	子企业	上海		子企业
华天装饰	子企业	杭州		子企业
安装工程	子企业	杭州		子企业
海外工程事业部	事业部	北京		隶属总企业
装饰事业部	事业部	杭州		隶属总企业
房地产投资事业部	事业部	上海		隶属总企业
交通工程事业部	事业部	杭州		隶属总企业
项目部	项目部	分布各地		在建项目约 500 个

3.1.2 广域网计划

依据前面需求分析,考虑到网络收敛性,经济和安全等原因,我们提议采取星型结构拓扑,这么能够充足利用带宽资源,整个网络采取 3 级结构：一级节点为：

集团总部共 1 个，二级节点为：区域性企业及本部共 7 个，三级节点为其它分企业及事业部共 28 个，广域网计划以下：



在对应一级节点和二级节点对应局域网内布署入侵检测和防火墙，来确保系统安全。

3.1.3 网络互连设计

依据网络互连需求分析，和广域网计划，我们提议从以下多个方面来考虑网络设计：带宽分配、QOS 设计、路由设计、IP 地址分配、网络布署等。

3.1.2.1 带宽分配

为了支持 A 集团多业务系统可连续发展，考虑经济组网标准，我们来分析该集团现在和未来业务属性、和业务逻辑等原因对网络链路需求，同时也是设备选型一个依据。

A 集团现在有或将要有业务有全企业上网需求、财务系统、视频会议、企业办公自动化系统、建筑行业综合业务管理系统、邮件系统、知识库系统建设等建设。以上数据包含到保密、实时流媒体等数据传输要求，我们从链路选型、带宽计算两方面来确定所需带宽。

链路选型：

现在比较常使用数据链路业务能够是：DDN、FR、ISDN：

DDN 专线接入向用户提供是永久性数字连接，沿途不进行复杂软件处理，所以延时较短，避免了传统分组网中传输协议复杂、传输时延长且不固定缺点；DDN 专线接入采取交叉连接装置，可依据用户需要，在约定时间内接通所需带宽线路，信道容量分配和接续均在计算机控制下进行，含有极大灵活性和可靠性，使用户能够开通多种信息业务，传输任何适宜信息，所以，DDN 专线接入在多个接入方法中深受用户青睐。

DDN 专线接入关键优点：

能提供高性能点到点通信。通信保密性强，尤其适合金融、保险等保密性要求高用户需要；

传输质量高，网络时延小，通信速率可依据用户需要按 N＊64Kbps 选择 ；信道固定分配，充足确保了通信可靠性，确保用户带宽不会受其它用户影响 ；用户经过这条高速国际互联网通道，可构筑自己 Internet、E-mail 等应用系统 ；用户网络整体接入使局域网内 PC 均可共享互联网资源； 用户可无偿得到多个 Internet 正当 IP 地址及域名 ；用户可实现天天二十四小时全天候信息公布，即用户可建立自己 Web 站点，向国际互联网公布自己信息或提供信息服务 ；用户可经过防火墙等技术保护内部网络免受不良侵害 。

本期 A 集团要实现业务当中，有数据业务（邮件、公文流转、互联网、内部系统、数据查询）和流媒体业务（视频会议等）。

因为整个网络环境为 TCP/IP 框架下，对于数据业务这类非实时业务来讲，网络本身能够实现数据重传恢复机制，对带宽需求不是很大，而流媒体业务这类实时业务来讲，必需含有两个原因才能够在 IP 环境下实现比很好：（1）含有一定带宽，达成理想传输环境，理论上传输一路 MPEG 视频为 384K，假如采取双向视频会议必需含有大于 2*384=768K 带宽。（2）网络含有一定 QOS 机制（相关 QOS 在 QOS 设计里具体介绍）。

从**一级节点到二级节点带宽**计算以下（按两路视频会议和人上网计算）：

二级节点平均分配人数为：/7=286 人；

依据 Gartner 统计数据分析，一个企业通常只有 10%-20%人并发上网或发邮件，我们按 15%计算，即：

二级节点并发上传或下载数据人数为：286*15%=43 人；

通常 24K/秒速度数据能确保 2 秒钟正常打开网页，即：

二级节点需要广域网链路基础带宽为：**43*24K=1028K**。

因为视频会议不是常常开，当视频会议必需是能够经过 QOS 优先等级抢占 1028K 带宽中 768K。我们提议采取 **1024K** 带宽为一级节点到二级节点带宽，能够满足到未来需求。假如需要额外视频带宽能够即使方便向电信申请，而无须更换网络设备模块。

从一级节点到互联网带宽计算以下：（人上网计算）：

到，上网人数将达成人，依据 Gartner 统计数据分析，一个企业通常只有 10%-20%人并发上网或发邮件，我们按 15%计算，即：

二级节点并发上传或下载数据人数为：*15%=300 人；

通常 24K/秒速度数据能确保 2 秒钟正常打开网页，即：

二级节点需要广域网链路基础带宽为：**300*24K=7200K**。在左右能够申请 **10M** 电路，而不会添加用户端设备，完全满足需求，现在我们能够考虑 2M 电路就能够满足了。

3.1.2.2 QOS 设计

因为考虑到整个综合业务网络信息系统可靠性和可用性，那么一个质量确保体系结构是必需含有，这也是一个设备选型必需考虑地方，

要实现网络稳定质量，最先考虑就是什么业务对整个网络系统服务质量最关心，在这里最关键就是视频会议和数据语音，这两种业务才是最关心服务质量，视频会议系统通常全方面支持 H.323 和 T.120 标准来完成视频、音频、数据集中和转发。一样，在我们国家，像联通等语音电话采取是 H.323

协议，当然也有像北电基于软交换功效语音系统，不过全部是要求对时间比较敏感协议，如 UDP，RTP，CRTP 等，所以 QOS 是一定要确保，除了数字线路服务质量以外，就是要考虑接入服务器 QOS 功效了。

1．优异先出（FIFO）

优异先出提供了基础存贮转发功效，也是现在 Internet 使用最广泛一个方法，它在网络拥塞时存贮分组，在拥塞解除时按分组抵达次序转发分组。是默认排队方法，所以不需要配置。缺点是不提供 QoS 功效，对突发数据流在传输时间要求严格时，应用程序会引发过多延迟，并对突发性存在包丢失连接公平性较差，对上层 TCP 快速恢复效率也较低。

2．优先级排队算法（priorityQueuing，PQ）

优先级排队算法是严禁其它流量前提下，授权一个类型流量经过，使用优先级排队给路由接口上传输数据分配优先级，当有空闲路由时，路由就往返扫描全部队列，将高优先队列数据发出，只有当高优先级队列空了以后，才能为低优先级服务，假如优先级队列满，则扔掉数据包，路由器不处理，优先级排队适适用于网络链路不停阻塞情况。

PQ 带宽分配独立于数据包大小。所以它在没有牺牲统计利用情况下提供另外公平性，和端到端拥塞控制机制能够很好协同，它缺点在于实现起来很复杂，需要每个数据流排队处理，每个流状态统计，数据包分类和包调度额外开销等。

3．定制排队

定制排队是为许可含有不一样最低带宽和延迟要求应用程序共享网络而设计。定制排队为不一样协议分配不一样队列空间，并以循环方法处理队列。为特定协议分配较大队列空间能够提升其优先级。定制排队比优先级更为“公平”。在可能发生拥塞地方使用定制排队能够提供确保带宽。定制排队能够确保为每一个特定通信类型得到固定部分可用带宽，同时在链路担心情况下，避免数据包企图占用超出预分配量限制可能。

4. 加权公平排队（Weight fair queuing，WFQ）

加权公平排队用于降低延迟改变，为数据流提供可估计吞吐量和响应时间。目标是为轻载网络用户和重载网络用户提供公平一致服务。确保低权值响应时间和高权值响应时间一致。

加权公平排队是一个基于数据流排队算法，它能识别交互式应用数据流，并将应用数据流调度到队列前部，以降低响应时间。WFQ 和定制排队和优先排队不一样。能自动适应不停改变网络通信环境，几乎不需要配置。

5. 随机先期检测（random early detection，RED）

前面介绍排队机制是基础拥塞控制策略。尽管这些技术对控制拥塞是必需。但它们对避免拥塞现象发生全部显得无能为力。 随机先期检测监视网上各点通信负载，假如拥塞增多，就随机丢弃部分分组，当源分布点检测到通信丢失，降低传输速率。RED 能够在各连接之间取得很好公平性，对突出业务适应性较强。

6. 加权随机先期检测（weightedrandom early detection，WRED）

加权随机先期检测是将 RED 和优先级排队结合起来，这种结合为高优先级分组提供了优先通信处理能力，当某个接口开始出现拥塞时，它有选择地丢弃较低优先级通信，而不是简单地随机丢弃分组。

总而言之，在传统 TCP 拥塞控制中，结合 IP 层拥塞控制算法，将是完善 Internet 拥塞控制最有效路径。

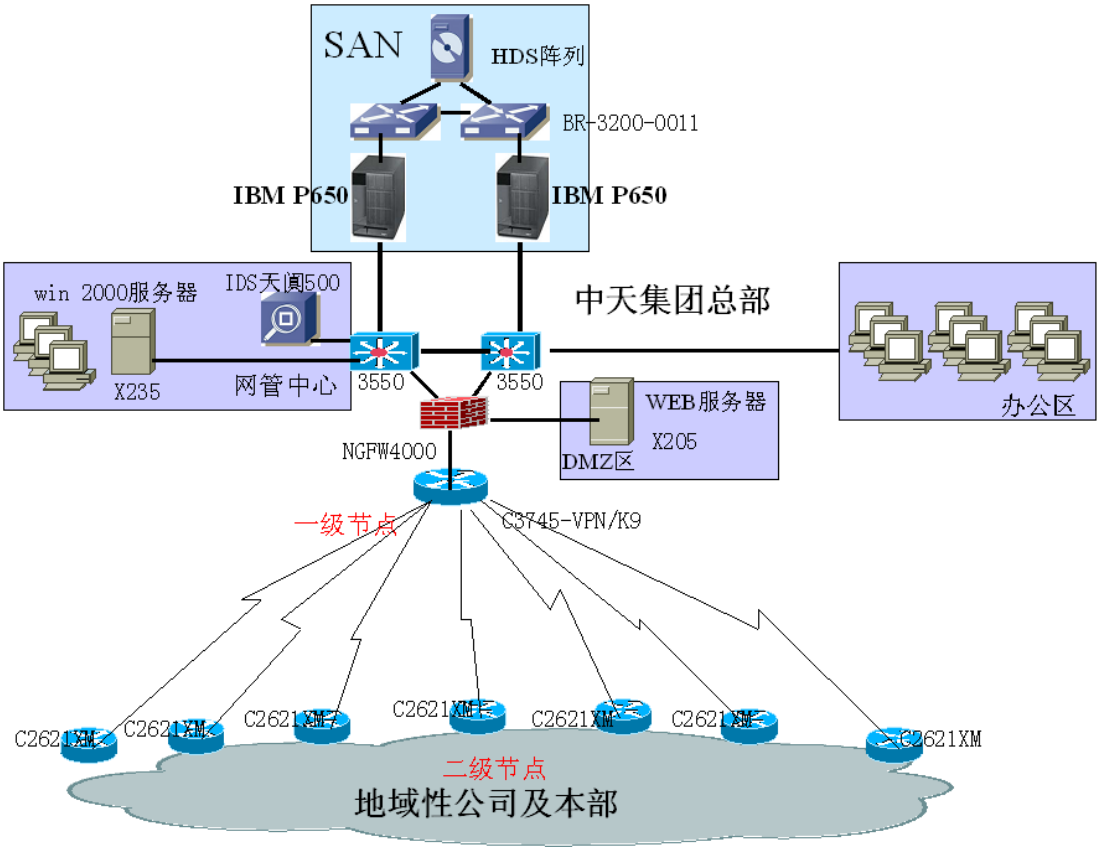
3.1.2.3 网络设备选型

设备选型对整个网络系统质量十分关键，A 企业做为一个成熟系统集成商，有一套科学而有效质量管理体系，首先，要考虑用户需求、售后服务、关键应用、特殊应用、质量确保、网络属性、现在系统系统结构等多个方面来考虑。

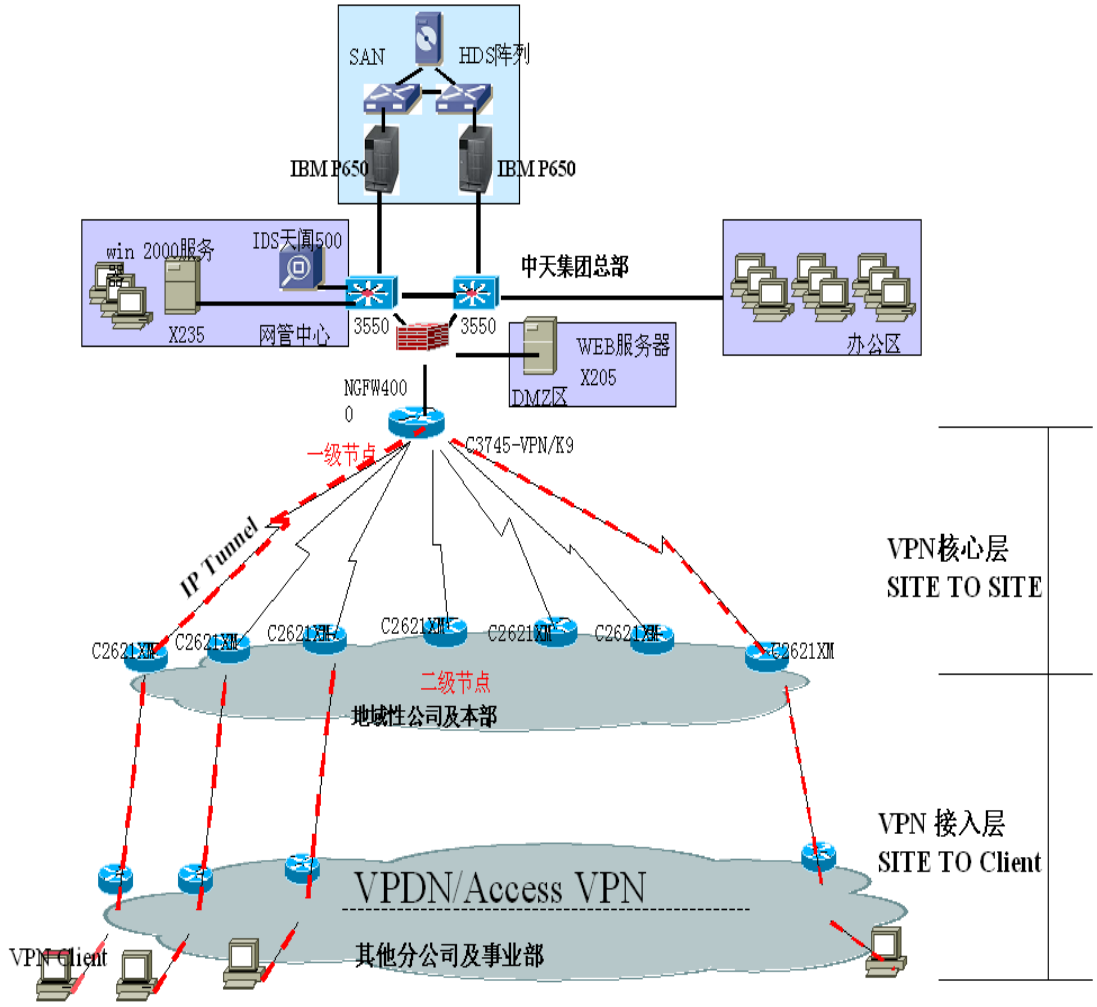
现在中国著名网络设备供给商关键有三家 Cisco,3COM 和华为。其中 3COM 路由器设备在中国使用不是十分广泛，同时网络产品以交换机为关键产品，在其它网络产品方面力量相对其它两家厂商稍弱。华为作为中国关键网络产品供给商，产品线齐全，种类多档次较齐全在，中国市场有一定拥有率，价格比较廉价，关键是通常网络应用环境，在 VPN、VOIP 和其它复杂应用中比较少。Cisco 做为全球最大网络设备供给商，在路由器和交换机领域结果有目共睹，它产品应用在世界各个角落，在中国也广为使用。Cisco 产品线齐全，从小型 SOHO 用路由器和交换机到大型骨干路由器、交换机一应俱全。同时产品端口密度高，同一产品含有多个不一样配置方案有利于产品多功效化如 VOIP、VPN 等。它拥有很多独创技术如 ISL、NetFlow、Fast EtherChannel 等，对系统以后演进和发展有很大好处，而在 IP 广域互连上，CISCO 含有最大优势，同时因为 Cisco 完整产品线为用户提供了丰富选择余地，Cisco 网络设备优异兼容性也为和其它企业产品互连提供了可靠确保。在售后方面，CISCO 也做很好，在 A 集团综合网络信息系统中原有设备大部分为 CISCO 产品，考虑到网络平滑性，和维护方便等各个原因，尤其是特殊应用 QOS 确保方面，VPN 特征方面、安全方面等，比其它两个厂家全部要成熟和更多案例，针对此次项目我们推荐 CISCO 高可用产品在实现系统网络支撑平台。

3.1.2.4 网络布署

杭州 A 集团总部一级节点,作为关键节点,含有以下功效:汇接二级 7 个节点数据,终止 VPN 隧道,我们提议采取 CISCO 最新高性能路由器 CISCO374-VPN/K9 作为关键路由器, 模块化 Cisco 3700 系列应用服务路由器充足利用了 Cisco 1700、2600 和 3600 系列路由器针对 WAN 访问、语音网关和拨号应用等而配置可选网络模块(NM)、WAN 接口卡(WIG)和高级集成模块(AIM)。另外，Cisco 3725 和 Cisco 3745 这两个 Cisco 3700 平台引进一个新、可提供更广泛接口高密度服务模块 (HDSM)。配置四个 NM 插槽 Cisco 3745 路由器取消了在每一对相邻 NM 插槽之间中心导轨，所以能够采取两个 HDSM ，而不是四个 NM。配置两个 NM 插槽 Cisco 3725 路由器可在它所配置两个 NM 插槽之一中采取一个 HDSM ，并仍可在剩下 NM 插槽内采取一个 NM 。采取新 HDSM 以后，Cisco 3700 系列路由器就能够集成更高端口密度和新高性能服务了。支持 VPN,提供 7 个广域网接口,和一个 Internet 广域网口,经过高级集成模块 AIM-VPN-HP 来实现 VPN 加密隧道提议和终止,CISCO3745 本身集成了 3 个 WIC 卡，我们能够经过提供 2 个 NM-2W 模块，配置 2 个 WIC-2T，和 1 个 WIC-1T，共 8 个，其中 7 个接入二级节点，另外一个能够作为 Internet 接驳，Internet 接驳速率临时定为 2M，未来能够经过升级到 10M。图所表示：


SAN
HDS阵列
BR-3200-0011
IBM P650
IBM P650
win 2000服务器
IDS天阗500
X235
网管中心
3550
3550
中天集团总部
办公区
WEB服务器
X205
DMZ区
NGFW4000
一级节点
C3745-VPN/K9
C2621XM
C2621XM
C2621XM
C2621XM
C2621XM
C2621XM
C2621XM
二级节点
地域性公司及本部

在此次项目中，CISCO3745-VPN/K9 最大能够同时支持个 Tunnels，即便是全体上网人数同时和总部通信，全部没有任何问题；局域网采取天融信防火墙 NGFW4000-S 来实现阻隔一些端口入侵和非法探测，提供具体日志和审计功效，该防火墙也能够跟入侵检测系统天阗 500 联动，动态检测黑客入侵并禁用对应端口，在防火墙 DMZ 布署 WEB 服务器供外部访问，具体描述见网络安全设计。对于三级节点 VPN 接入就能够支持多个方法了，最经济方法就是采取 SITE TO Client 方法，由 CISCO 自带 VPN Client（支持多个操作系统）经过拨号或经过专线、ISDN、FR 等方法访问 VPN，由对端 VPN 网关提供认证，具体方法见下面章节：VPN 设计。整体拓扑以下所表示：



3.1.2.5VPN 设计

VPN（虚拟专网）是利用公共网络资源(如公用电信网)为用户组建专用网一个技术，它经过对网络数据进行封包和加密传输，在公网上传输私有数据，达成私有网络安全等级，从而利用公网构筑专网（即 VPN）。它是一个逻辑上专用网络，向用户提供专用网络所含有功效，但本身却不是一个独立物理网络。

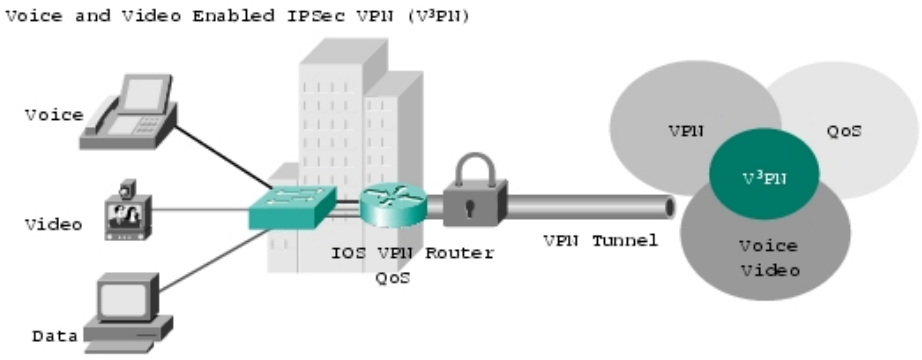
此次项目中依据前面计划：

在一级节点和二级节点之间布署端到到端 VPN：Site TO Site，结构为星型结构：HUB-SPOKE。

在二级节点和三级节点布署端到点方法 VPN：Site TO Clint。

在此次项目应用中考虑到传输有视频、语音、数据 3 类信息，各类信息对网络环境全部有一定要求，尤其是 VPN 环境下实现更是比较复杂，我们采取 CISCO3745、2621XM VPN 多应用服务器能够支持 V3PN，即能在 IPsec 隧道上实现视频、语音、数据 3 类信息封装，而确保 IP 中 QOS 特征不改变，从而确保数据 IP 连贯应用。这个过程多用户来讲是透明。

在 CISCO3745、2621XM 中，提供 12.2(13) T 或以上版本 IOS，支持 IPSec 提供 DES 和 3DES Advanced Encryption Standard (AES)，新型 AES 支持 128-bit key (default), 和 192-bit key, 或 256-bit key.提供愈加复杂愈加安全应用。图所表示：



经过以上设计能够确保原来 QOS 机制在网络中一直启用，确保网络平滑。

考虑到网络规模变大，如未来可能需要建立新办事处或地域性分企业，这么添加路由器可能会对基于传统 IPsec 方法 VPN 造成一定影响，我们能够采取 IPsec+GRE（通用路由封装）技术来实现基于 IP 路由收敛 VPN 技术，这么，路由更新能够完全透过 2 层 VPN 来实现，这对用户来讲是完全透明，一旦 A 集团规模发生巨大改变，网络拓扑方法要改变如组成 MESH 方法或节点数大大增加，我们能够完全在不更改设备情况下建立基于 MPLS VPN，CISCO3745 完全能够设置 PE 路由器，而 CISCO2621 能够对应地设置为 CE 路由器，这么整个关键 VPN 网络就从 2 层 VPN 直接升级到 3 层 IP VPN 构架来了。

在二级节点和三级节点采取端到点方法 VPN：Site TO Client。

对于 3 级节点加入到集团 VPN 当中来，就很方便了，我们购置 CISCO3745 和 CISCO2621 VPN 路由器，随机附带了一份 CD，包含了 Client 端 IPsec 程序，该程序很简单大部分设置全部是预定义，VPN 访问策略和配置能够直接从对应所属二级或一级 VPN Gateway（这里是 3745 或 2621 路由器）直接下载，现在 VPN Client 能够支持以下系统 Windows 95(OSR2+), 98, ME, NT 4.0, , XP, Linux (Intel), Solaris (UltraSparc-32 & 64 bit) and MAC OS X 10.1 & 10.2 (Jaguar)

3.1.2.6 网络管理

在本方案中采取了 CISCO 处理方案，对于网络管理，我们提议采取 CISCOWORKS。

CiscoWorks 服务管了处理方案建构在第 3 层结构基础之上，包含可远程安装数据搜集应用、Cisco IOS 内嵌式技术和一整套融合了业界最优异评定服务和定额引擎应用软件。该处理方案构件包含：

管理引擎 1110（ME1110）——可在网络中远程安装，是含有极高扩展性和灵活性数据搜集处理方案。ME1110 是专为搜集 Cisco 设备度量数据而设计，并许可在数据搜集需求增加情况下暂停管理服务器来安装新 ME1110 设备。

服务保障代理——一个用来确定度量数据服务等级技术，以验证度量数据是否符合服务等级要求。鉴于服务保障代理技术已内嵌于 Cisco IOS 软件中，所以它是随时可用，而且对网络基础设施费用几乎不会组成任何影响。

服务等级管理器——建构于开放 XML 应用程序接口基础上，可提供给合作伙伴以用于第三方应用集成。

CiscoWorks 服务管了处理方案使网络经理能够验证她们为广域连接和网络服务提供服务等级。它将基于标准开放式管理应用程序接口、Cisco 内嵌式 IOS 代理、可扩展服务等级管理应用和第三方产品相结合，从而含有了端到端服务级检验和全方面管理能力。所以，用户现在能够完全放心地使用这些新应用，比如 VoIP、IP 电话、虚拟专网和电子商务处理方案等，可轻松地取得不一样服务和愈加好终端用户满意度，实施同时监视多个服务级协议，调试并改善网络和定制故障汇报。和此同时，第三方应用开发人员和系统集成人员能够连续地取得相关网络层数据，并对定义和搜集到服务级度量信息进行标准化。

第四章 网络安全方案

4.1 安全设计

网络面临安全威胁大致可分为两种：一是对网络数据威胁； 二是对网络设备威胁。这些威胁可能起源于多种原因：可能是源于网络外部， 也可能是内部人员造成； 总结起来，最关键威胁是来自外部和内部人员恶意攻击和入侵，这是企业信息化等顺利发展最大障碍。

基于 VPN 网络基础上安全了，不过考虑到 Internet 应用，内部人员网络入侵、资料盗取、恶意破坏，病毒入侵等原因，综合安全设计还是必需，我们提议针对这些原因提出以下安全防护方法：

1、防火墙技术

2、IDS 入侵检测系统

3、防病毒系统

4、备份（相关备份配置，我们在主机设计里描述）

4.1.1 防火墙技术

防火墙是一个成熟技术,现在防火墙功效也越来越强大,技术越来越统一,考虑到企业信息系统安全等级,在选型上重视国产,含有一定应用案例,选型标准以下:

4.2.1.1 防火墙选型

因为网络信息化系统网络安全关键性,并结合网络信息化系统信息安全工作实际条件及情况，我们确定以下选型标准：

防火墙必需含有自我系统保护能力。

防火墙必需含有强大 NAT 转换功效。

防火墙支持各类加密算法和 VPN 功效。

防火墙端口是可扩展。

防火墙产品应提供避免或严禁内外网络用户进入系统手段，即使对安全管理员而言，也应遵照对系统操作最小授权标准。

防火墙产品硬件/软件必需含有经国家授权部门测试认证安全等级。

防火墙产品遇故障工作失效，系统应自动转为缺省严禁状态。

防火墙产品必需最少含有推行所需安全服务最小能力。

防火墙产品所采取技术，不单纯追求优异、完善，而必需确保实用和成熟性，相关技术标准应采取、引用和靠近国家标准。

防火墙产品接入不影响原网络拓扑结构，防火墙产品运行最小影响原网络系统运行效率。

防火墙产品假如包含密码技术使用，必需取得国家密码管理委员会办公室立项和判定同意；防火墙产品如包含密码算法必需按国家密码委员会办公室要求进行申请和使用。

防火墙产品须经过国家信息安全产品认证机构认证。

经过以上分析，我们提议采取中国著名防火墙厂商天融信防火墙产品 NG FW4000，其强大性能处理和全方面控制规则得到很多企业和企业青睐。

4.2.1.2 技术细节

采取独创最新最优异技术

--核检测技术，即基于OS 内核会话检测技术，在OS 内核实现对应用层访问控制。它相对于包过滤和应用代理防火墙来讲，不仅愈加成功地实现了对应用层细粒度控制，同时，更有效确保了防火墙性能。

采取独创优异设计思想

--面向资源进行设计，对不一样对象具体组成资源，如文件、防火区域、节点对象、协议类型、应用行为、应用类型、管理端口协议等，直接进行控制，极大提升了安全性，并确保了配置方便性。

优异独特防火墙策略体系

--面向资源防火墙策略体系。建立独立防火区域，经过中央管理接口、管理端口协议、不一样节点对象（网络邻居、自定义网路、防火墙所在子网等）、协议类型、应用行为等不一样资源配置策略，使防火墙策略配置愈加简单，且便于维护。

分层式管理结构

防火墙管理采取集中层次管理结构，实现“防火墙—防火区--对象—资源”安全策略定义结构。配置简单、配置安全性高；管理简单、维护方便；愈加好确保了性能。

支持 TOPSEC 技术体系关键技术

支持TOPSEC技术体系关键技术，能够实现防火墙、IDS、病毒防护系统、信息审计系统等互通和联动，并支持TopsecManager综合管理系统和SAS安全审计系统。

适用更广泛网络及应用环境

支持众多网络通信协议和应用协议，如DHCP 、VLAN 、ADSL 、IPX 、RIP 、ISL 、802.1Q 、Spanning tree 、DECnet 、NETBEUI 、IPSEC 、PPTP 、AppleTalk 、H.323 、BOOTP、pppoe协议等，使4000防火墙适用网络范围愈加广泛，确保用户网络应用。方便用户扩展IP 宽带接入及IP电话、视频会议、VOD 点播等多媒体应用。

支持多个工作模式

能够支持透明、路由和混合工作模式。其中，独创混合模式源于天融信网络接口物理实现技术和天融信专用安全协议实现，并在 NGFW4000 中进行了重新设计和实现，深入得到了优化，方便适适用于复杂网络结构和应用接入。

支持远程集中管理

可经过安全认证及管理信息加密传输实现全局防火墙设备集中管理。实现统一安全政策布署，确保整个系统安全策略一致性，提升整个系统安全强度。

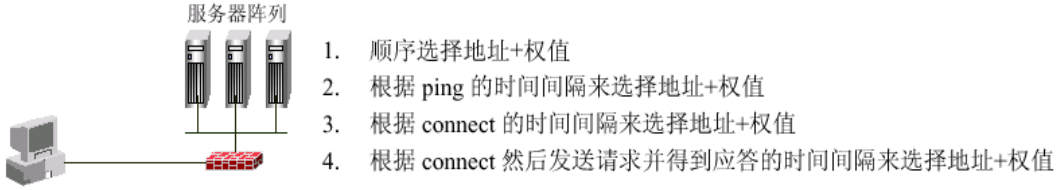
NGFW4000 关键配置和管理全部是基于 GUI（Graphic User Interface） 方法，管理主机只需安装专门管理软件，就能够在不一样操作系统平台、不一样地域对防火墙进行配置和管理。

支持负载均衡和双机备份

支持两台防火墙之间双机备份和负载均衡；支持多台服务器之间负载均衡。不仅愈加好适用不一样网络环境，且愈加好提供高性能和确保可靠性。

支持服务器负载均衡

NGFW4000 防火墙能够支持一个服务器阵列，这个阵列经过防火墙对外表现为单台机器，防火墙将外部来访问在这些服务器之间进行均衡，同时能够识别出故障服务器。



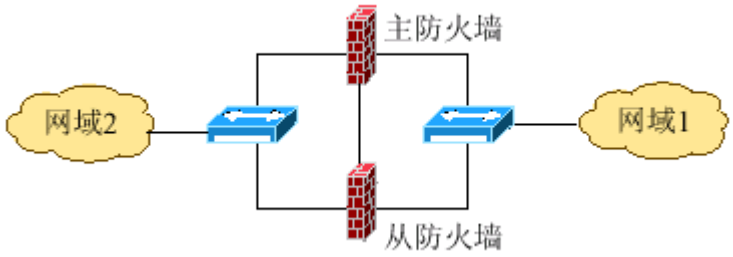
图表 1 防火墙负载均衡技术

防火墙本身负载均衡

NGFW4000 支持负载均衡功效，能够在高带宽网络环境中有效提升性能，同时负载均衡还实现了接口之间备份，当 A 机器某个接口故障时，B 机器对应接口能够接管它工作，同时 A 机器其它接口仍然正常地工作。

双机备份

为了确保网络高可用性和高可靠性，NGFW4000 提供了双机备份功效，即在同一个网络节点使用两个配置相同防火墙。正常情况下一个处于工作状态，为主防火墙，另一个处于备份状态，为从防火墙。当主防火墙发生意外 down 机、网络故障、硬件故障等情况时，主从防火墙自动切换工作状态，从防火墙替换主防火墙正常工作，从而确保了网络正常使用。切换过程不需要人为操作和其它系统参与，切换时间能够以秒计算。同时 NGFW4000 还实现了状态传送协议 STP ，当一台防火墙故障时，这台防火墙上连接不需要重新建立就能够透明地迁移到另一台防火墙上，用户不会觉察到。

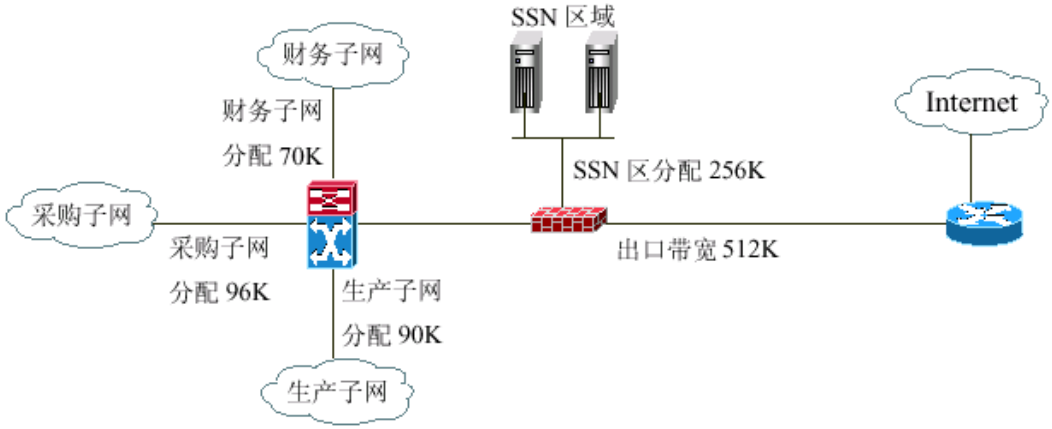


图表 2 防火墙双机备份

多层次分布式带宽管理

带宽管理完全虚拟了网络带宽应用实际环境，并实现多层次分布式管理模式，避免了单层集中管理缺点；而且，能够实现带宽分层、带宽分级、带宽分配、带宽优化等管理，优化网络资源应用，提升网络资源应用效率。

NGFW4000 能够许可管理员定义任意两个网络对象之间通信时最大带宽，而且带宽能够是分层，比如部门带宽下面有小组带宽然后是个人带宽等，能够预防带宽被滥用，确保关键通信顺畅。具体以下图所表示：



图表 3 分布式管理

支持多个身份认证

支持多个身份认证支持，如 OTP 、RADIUS 、S/KEY 、SECUREID 、TACACS/TACACS+、口令方法、数字证书（CA ），愈加好更广泛实现了用户判别和访问控制。

更强防御功效

在内核上实现对病毒防护，内容过滤（如 HTTP 、FTP 等 ）和入侵检测（IDS ）功效，其中入侵检测功效，防火墙 4000 不仅有内置 IDS 功效，还能够和 IDS 实现联动。这不仅提升了安全性，而且确保了性能。

深层日志及灵活、强大审计分析功效

提供丰富日志信息，用户可依据特定需要进行日志选项（不做日志、日志会话（即传统日志）、日志命令）。独创网络实时监测信息，可具体审计命令级操作，便于入侵行为分析和追踪。大大提升防火墙审计分析有效性。

一个安全防护体系中审计系统作用是统计安全系统发生事件、状态改变历史、经过该节点符合安全策略访问和不符合安全策略企图，使管理员能够随时审核系统安全效果、追踪危险事件、调整安全策略。进行信息审计前提是必需有足够多日志信息。NGFW4000 提供了很强大日志功效，用户能够依据需要对不一样通讯会话统计不一样日志。

NGFW4000

审计日志包含以下两个部分：日志会话、日志命令。日志会话也就是传统防火墙日志，负责统计通讯时间、源地址、目标地址、源端口、目标端口、字节数、是否许可经过。日志会话信息用来进行流量分析已经足够，不过用来进行安全性分析还远远不够；应用层日志命令在日志会话基础之上统计下各个应用层命令及其参数，比如 HTTP 请求及其要取网页名；访问日志则是在应用层命令日志基础之上统计下用户对网络资源访问，它和应用层日志命令区分是：应用层日志命令能够统计下大量数据，有些用户可能不需要，如协商通信参数过程等。比如针对 FTP 协议，日志会话只统计下读、写文件动作；日志命令则是在访问日志基础之上，统计如用户发送邮件，用户取下网页等。天融信新一代防火墙产品能够依据用户不一样需要对不一样访问策略做不一样日志，比如有一条访问策略许可外界用户取 FTP 服务器上文件，假如做命令日志，用户就能够知道到底是哪些文件被取走了。

4 .14 管理安全、方便灵活

防火墙 4000 经过简单配置即可接入网络进行通信和访问控制，GUI 管理界面提供了清楚管理结构，每一个管理结构元素包含了丰富控制元和控制模型。对全部管理加密（支持 SSL 和 SSH ），并进行严格审计，实现了真正安全远程管理。同时，能够支持 SNMP 和目前通用网络管理平台兼容，如 HP Openview 等，方便管理和维护。

优异性价比

强大完善功效、优异性能、高稳定性和可靠性，及方便扩展 VPN 、IDS 、认证、计费、审计等安全服务，表现了优异性价比，可有效地保护用户投资。

独立防火区域

NGFW4000 防火墙每个物理接口对应一个独立防火区域，每个区域安全策略只对该区域有效。每个区域能够单独设置自己默认安全策略，全部对该区域访问全部将匹配和该区域对应安全策略。也能够设定是否许可从该区域 PING 、TELNET 防火墙。

面向资源管理机制

NGFW4000

中采取面向多种对象不一样组成资源管理机制。对象是由很多个资源组成实体，规则建立在这种实体基础上。资源概念比对象控制愈加细化，简化了用户规则，使规则更为直观；同时，提升了配置管理员效率，提升了配置灵活性。NGFW4000 提供了很多个资源，如，网络节点、子网、第三方用户、用户数据库、防火区域、端口协议、文件资源、VLAN 、特殊端口。

支持透明接入

NGFW4000 支持透明接入。将 NGFW4000 配置为透明工作模式，无需更改用户网络拓扑结构就能接入用户网络中，用户网络中主机也无需更改任何网络配置就能经过防火墙进行访问（当然是要在防火墙规则许可情况下）。透明接入极大方便了防火墙接入，同时并不降低网络安全性。NGFW4000 还能工作在透明和路由混合模式下，更能适应多种不一样网络环境接入。

多级过滤立体访问控制

为确保系统安全性和提升防护能力，增强控制灵活性，NGFW4000 采取了多级过滤方法：以基于 OS 内核会话检测技术为关键，在 IP 层提供基于状态检测分组过滤，能够依据网络地址、网络协议和 TCP 、UDP 端口进行过滤；在应用层经过重写通讯会话部分或全部提供对高层应用协议命令、访问路径、内容、访问文件资源过滤；同时还直接支持第三方认证服务器提供用户级判别和过滤控制。NGFW4000 多级过滤形成了立体全方面访问控制机制。

强大地址转换能力

NGFW4000 拥有强大地址转换能力。NGFW4000 同时支持正向、反向地址转换，能为用户提供完整地址转换处理方案。

正向地址转换用于使用保留 IP 地址内部网用户经过防火墙访问公众网中地址时对源地址进行转换。NGFW4000 支持依据源或目标地址指定转换地址静态 NAT 方法和从地址缓冲池中随机选择转换地址动态 NAT 方法，两种方法总共能够有多达 32 个不一样转换地址，能够满足绝大多数网络环境需求。对公众网来说，访问全部是来自于防火墙转换后地址，并不认为是来自内部网某个地址，能够有效隐藏内部网络拓扑结构等信息。同时内部网用户共享使用这些转

换地址，本身使用保留 IP 地址就能够正常访问公众网，有效处理了全局 IP

地址不足问题。

内部网用户对公众网提供访问服务（如 Web 、FTP 服务等）服务器假如是保留 IP 地址，或想隐藏服务器真实 IP 地址，全部能够使用 NGFW4000 反向地址转换来对目标地址进行转换。公众网访问防火墙反向转换地址，由内部网使用保留 IP 地址服务器提供服务，一样既能够处理全局 IP 地址不足问题，又能有效隐藏内部服务器信息，对服务器进行保护。NGFW4000 提供端口映射和 IP 映射两种反向地址转换方法，端口映射安全性更高、更节省全局 IP 地址，IP 映射则更为灵活方便。

透明应用代理

NGFW4000 提供对常见高层应用服务（HTTP 、FTP 、SMTP 、POP3 、NNTP ）透明代理。用户不需要在自己主机上作任何相关代理服务器设置，只需管理员在防火墙上配置相关规则，用户经过防火墙进行上述应用访问就会由防火墙进行代理，这些配置对用户来说完全是透明，极大方便了用户使用代理。同时 NGFW4000 还对上述服务做了更具体控制，如 HTTP 对命令（GET 、POST 、HEAD 、DELETE 、OPTION 、PUT 、TRACE 等）和 URL 和脚本类型进行过滤，FTP 对命令（GET 、PUT ）及访问路径进行控制，SMTP 、POP3 对收发信人进行控制，NNTP 对命令（POST 、GROUP ）和新闻组进行控制，这使得用户使用代理访问 Internet 更为安全。

内嵌 VPN 功效支持

NGFW4000 内建了 VPN 关键功效。用户启用 NGFW4000 VPN 功效，就能够和 VPN 体系中其它网关 VPN 、Windows 用户端、当然也包含另外启用了 VPN 功效 NGFW4000 互通，建立加密隧道进行加密通信，形成虚拟专用网在异地局域网间经过互联网提供安全可靠网络使用环境。在功效上就相当于一台 VPN 网关 VPN 和一台 NGFW4000 两台设备组合起来，在硬件上仅为一台设备，而且因为是内建功效支持，功效间结合愈加平滑易用。

安全服务器网络（SSN ）保护

NGFW4000

采取多穴主机体系，能够定义某个接口连接网络为安全服务器网络（SSN——Security Server Network ），将提供信息访问服务服务器安装于该网络区域内，和内、外网络从物理上隔离开来，并提供专门安全保护。NGFW4000 提出 SSN 概念有别于传统所谓 DMZ 停火区模式，它是一个更为主动安全防护理念：通常情况下，SSN 主机不许可主动向内、外网提议连接请求，只许可向内、外网回应其请求数据包；外网用户也只能访问 SSN 上主机，不能访问内部网主机。即 SSN 和外部网之间受防火墙保护，同时 SSN 和内部网之间也受防火墙保护，即使 SSN 受破坏，内部网络仍处于防火墙保护之下。同时 NGFW4000 提供 SSN 保护功效针对用户最常提供 Web 访问服务进行专门保护，能定时检验 SSN 区 Web 服务器，进行校验，一旦发觉服务器被入侵修改，能够依据备份信息立即恢复服务器内容，将服务器被入侵修改造成影响减至最小。

支持 SSL 、SSH 安全管理

为了便于管理员管理，NGFW4000 除了支持当地管理以外，还提供远程登陆管理和基于 Web 方法管理。

为了确保远程管理安全性，NGFW4000 不管是对管理员还是管理过程全部采取了一系列安全方法：对远程管理员提供了基于 OTP 机制管理员认证、管理员主机限定和同时只能有一个管理员登陆限制。为了预防远程管理过程被监听和修改，还支持基于 SSH 远程登陆管理和基于 SSL Web 方法管理，将管理主机和防火墙之间通讯进行加密以确保安全。

支持 SNMP （简单网络管理协议）

现在在计算机网络中应用最为广泛网络管理标准是 SNMP （简单网络管理协议）。

防火墙作为一个网络安全访问控制基础网络设备，为它提供一个标准网络管理方法是有必需，NGFW4000 就提供了对这个标准协议支持。

为了愈加好地支持网络集中管理，NGFW4000 提供了对 SNMP v1 、v2 、v2c 、v3 等不一样版本支持，并和目前通用网络管理平台兼容，如 HP Openview 、Cisco works 等，能够经过这些管理平台对防火墙运行情况进行监控，并接收经过

SNMP TRAP 发送报警信息，帮助网络管理员找出并纠正 TCP/IP 互联网中故障。为了避免因为 SNMP 本身安全性上缺点而造成防火墙本身安全性受到威胁，系统仅许可网管系统查询信息，而不许可改变防火墙配置。

简单方便配置备份和恢复

NGFW4000 提供简单方便配置文件管理，管理员可经过 Web 界面进行配置文件备份、下载、删除、恢复和上载。用户能够随时手工备份防火墙配置文件，能够将备份结果下载到当地管理主机中保留，也能够将备份上载回防火墙进行恢复还原。

用户定制特殊功效支持

NGFW4000 使用模块化设计，用户能够依据需要，经过网络下载对应模块，经过升级程序增加新功效。还可依据用户特定安全需求定制特殊功效。

支持动态 IP 地址

NGFW4000 支持运行 DHCP 、BOOTP 等协议动态主机，让用户在管理方便同时不损失安全性。对于使用 DHCP 服务器来动态分配 IP 地址网络环境，极难使用 IP 地址来进行访问控制，因为网络中主机没有固定静态 IP 地址，此时处理方法有两种：一个是让防火墙自己来充当 DHCP 服务器进行 IP 地址分配，此时防火墙本身能够知道主机动态 IP 地址，从而进行访问控制，不过在这种方法下，防火墙内部必需开启 DHCP 服务，这不仅会增加防火墙额外负荷，更为严重是防火墙本身开启过多服务会影响本身安全性。

另一个方法是防火墙本身不充当 DHCP 服务器，而是在用户端主机上安装一个开机自动运行小软件，每次在主机开机后，自动将主机获取动态 IP 地址传输给防火墙，这么就能够对指定主机进行访问控制了。天融信新一代防火墙产品使用就是后一个方法来处理对 DHCP 环境支持。

源、目地址路由功效

天融信新一代防火墙产品采取一个特殊路由技术，通常路由技术只依据目标地址来做出路由选择，而网络卫士防火墙 4000

则依据通讯源地址和目标地址来做出路由选择。这种源目地址路由技术能够很好适应有多个网络出口环境。比如对于一些教育系统网络可能同时有两条互联网出口，一条是经过教育网线路连接到 Internet ，另外一条就是申请电信线路直接连接到互联网图所表示。对于这种环境为了愈加好利用带宽，让网络中部分终端走教育网出口，另外一部分终端走电信线路，这么能够很好利用现有带宽资源，不会造成带宽浪费，不过在这种网络环境下，假如防火墙不支持源目标地址路由技术就极难实现，因为到互联网目标地址全部是一样，只是起源不一样。

4.2.1.3 防火墙布署

采取 NG FW4000 防火墙, 支持 IP 分组管理功效，能够防御源路由攻击、IP 碎片包攻击、DNS/RIP/ICMP 攻击、SYN 等多个攻击：防火墙系统能够检测到对网络或内部主机多个拒绝服务攻击，提供透明代理功效：防火墙提供给用级代理，对常见高层应用（HTTP、FTP、SMTP、POP3、NNTP）提供具体控制。支持 IP/MAC 地址绑定，提供自动查询 MAC 地址功效。支持 IPsec 隧道,完全满足 A 集团需求,并发连接数达成 40 万,提供 3 个 10/100 端口,最大支持 6 口 10/100M 端口，同时 NG FW4000 支持负载均衡功效，能够进行多台防火墙布署，也能够单独布署，满足企业多样化需求。

4.2.2 入侵检测

此次系统建设考虑到内外网络安全，采取一个合理入侵检测系统也是对整个资源保护得到一个良好补充。

网络面临安全威胁大致可分为两种：一是对网络数据威胁； 二是对网络设备威胁。这些威胁可能起源于多种多样原因：可能是有意，也可能是无意；可能是起源于企业外部， 也可能是内部人员造成；可能是人为，也可能是自然力造成。 总结起来，大致有下面多个关键威胁：

(1) 非人为、自然力造成数据丢失、设备失效、线路阻断

(2) 人为但属于操作人员无意失误造成数据丢失

(3) 来自外部和内部人员恶意攻击和入侵

前面两种预防和传统电信网络基础相同，最终一个是目前 Internet 网络所面临最大威胁，是电子商务、企业上网工程等顺利发展最大障碍，也是企业网络安全策略最需要处理问题。

入侵检测系统(Intrusion Detection System, IDS)是一个保护自己免受黑客攻击网络安全技术。入侵检测技术能够帮助系统对付网络攻击，扩展系统管理员安全管理能力(包含安全审计、监视、进攻识别和响应)，提升信息安全基础结构完整性。它从计算机网络系统中关键点搜集信息，并分析这些信息，看看网络中是否有违反安全策略行为和遭到攻击迹象。入侵检测被认为是防火墙以后第二道安全闸门，它在不影响网络性能情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作实时保护。

同时，针对不一样用户不一样需求，IDS 不应仅提供入侵检测基础功效，它还应该涵盖到网络内容分析、网络病毒源分析、过滤不良网页等功效，处理能力应该达成千兆网络入侵检测。

IDS 从根本上作为一个网络可疑行为检测工具，其用户群是很大。其中有电信行业高速网络用户，也有一般大型企业用户，还有中小型企业和学校等小规模用户。这些用户群采取 IDS 根本目标就是为了检测网络中可疑行为而且进行告警、响应和统计。

4.2.2.1 入侵检测技术

入侵检测系统采取以下技术

强大网络访问控制功效：入侵检测系统采取了一套规则库来定义什么用户能够访问什么网络资源，确定仅有授权用户才能够访问网络资源。

大规模入侵特征库：入侵检测系统实时地在网络流量中察看是否包含入侵行为。入侵升级文件能够快速立即地进行在线升级，让特征库随时保持最新最全。

强大碎片重组能力和抗入侵能力。能够有效发觉和阻拦碎片攻击和 IDS 入侵攻击。

本身抗攻击能力。入侵检测系统能够进行隐藏 IP 设置，确保本身不会受到黑客攻击，确保本身安全性。

强大攻击特征自定义功效。管理员能够随时利用 入侵检测系统提供正则表示式对最新出现攻击方法进行特征定义和方法，很方便和灵活。

细致入微数据包分析功效。入侵检测系统能够在二进制等级对数据包进行特征定义和匹配，分析隐藏攻击手段。管理员能够采取该方法对攻击行为进行自定义。

强大网络安全设备联动能力。入侵检测系统现在能够同 Check Point Firewall-1/NG、Nokia 全系列防火墙、eTrust 防火墙、思科路由器和全部采取 OPSEC 标准防火墙进行联动。即 入侵检测系统一旦发觉入侵行为，便能够立即通知这些防火墙动态修改安全策略，对外来入侵在第一时间进行有效拦截。

高负载网络下高性能。采取专用数据处理机制让其即使在高流量下也能够正确发觉网络入侵行为。支持全交换网络环境。

网络利用情况纪录：入侵检测系统提供了基于最终用户明、应用程序等进行跟踪和统计网络使用情况功效。这大大有利于提升网络策略计划，而且提供了正确网络利用情况汇报。

入侵统计和分析：为搜集入侵信息并归纳入库分析提供了一套完整有效机制。

集成了防病毒引擎：入侵检测系统采取 KILL 防病毒引擎来检验网络流量中是否包含病毒。尤其是在现在情况下，网络病毒已经成为一个最流量病毒，而且最近又出现了新旧病毒组合，如求职信病毒和 CIH 病毒组合，结合了旧病毒强大破坏性和新病毒传输快速特点，对网络安全造成了极大威胁。网络病毒流传检测功效对网络病毒立即检测和防护是很有必需。

强大报表能力:预置上百种报表模版，提供类似于网络入侵数量统计、入侵类型统计、入侵源统计和传输网络病毒前几名和每种行为具体报表分析等内容。

采取 Crystal Reports 专业报表格式，能够生成包含 HTML、Word、Excel、Lotus

Notes、Txt 等十余种格式报表。

报表扩展能力：支持 Webtrends、Telemate 等专业报表软件接口，而且提供丰富 API 功效。

强大报警功效。能够经过电子邮件、寻呼、NT 事件日志、消息框、SNMP Trap、打印机等等预定义功效进行告警，用户还能够经过提供接口方便地自定义保警方法，如经过短消息报警。

远程管理功效：远程用户能够经过拨号方法访问、察看而且监控 入侵检测系统运行情况。在紧急情况下，管理员能够在家里对 入侵检测系统进行管理和入侵分析。

中央管理机制： 入侵检测系统提供了强大中央管理和策略分发机制。当一个网络分布于不一样地理位置时候，管理员仅仅需要在每一个位置安装对应检测引擎，就能够集中在中央管理台进行管理策略定义、分发和入侵库升级等工作。

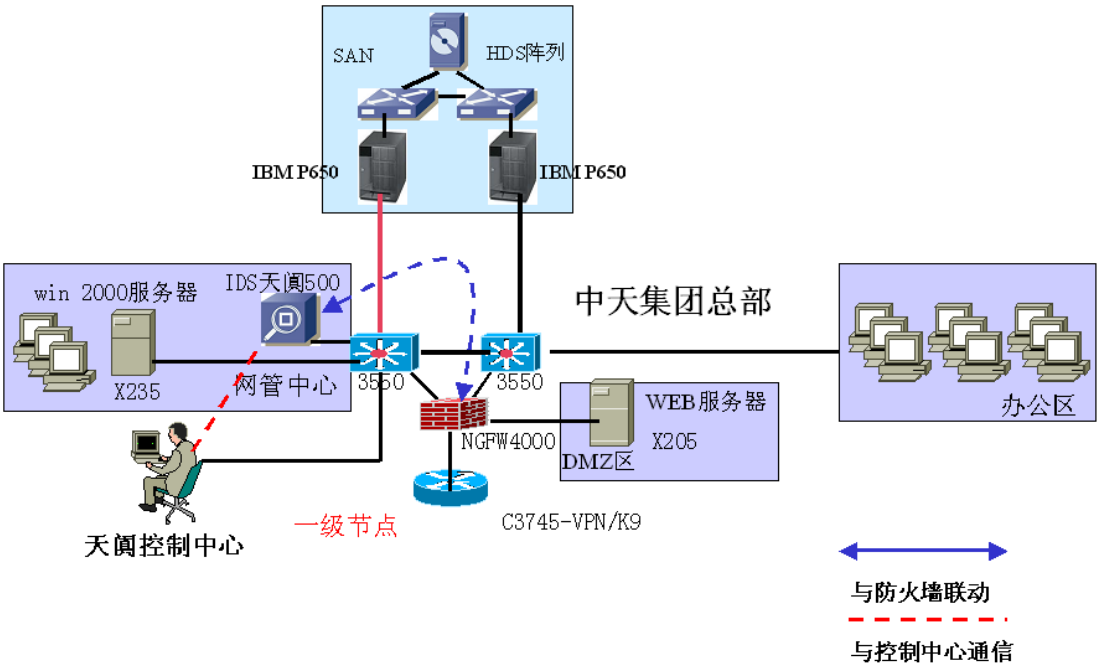
在此次项目中，我们提议在集团总部采取启明星辰入侵检测系统天阗500，在地域性企业采取天阗100，这两款设备全部是网络型入侵检测系统，经过旁路方法全方面侦听网上信息流，动态监视网络上流过全部数据包，经过检测和实时分析，立即甚至提前发觉非法或异常行为。经过采取告警、阻断和在线帮助等事件响应方法，以最快速度阻止入侵事件发生。网络型入侵检测系统能够全天候进行日志统计和管理，进行离线分析，对特殊事件进行智能判定和回放。网络型入侵检测关键优点以下：

按网段检测，方便实施和布署；

旁路方法监听，对入侵者和业务网络透明存在；

不占用网络带宽资源和其它业务主机系统资源；

能够实现和其它安全设备之间紧密配合。



在天阗控制中心能够实时和IDS通信，统计状态信息等，控制中心是个高性能管理系统，它能控制在当地或远程多个网络探测引擎活动，集中制订和配置策略，提供统一数据管理和实时告警管理。它能显示具体入侵告警信息(如入侵者IP 地址、攻击特征)，对事件响应提供在线帮助，以最快方法阻止入侵事件发生。另外，它还能全方面接收和管理日志，方便进行事后分析并形成综合汇报。

4.2.3 防病毒设计

伴随数字技术及 Internet 技术日益发展，病毒技术也在不停发展提升。它们传输路径越来越广，传输速度越来越快，造成危害越来越大，几乎到了令人防不胜防地步。很多企业机构在建立了一个完整网络平台以后，急需一个切实可行防病毒处理方案，来确保整个企业业务数据不受到病毒破坏，日常工作不受病毒侵扰。那么，怎样在做到防病毒万无一失呢？我们将从企业网络经典结构、经典应用和现代病毒利用网络特征传输趋势来处理这些问题。

一、企业网络经典结构

现代化企业

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。
如要下载或阅读全文，请访问：
https://d.book118.com/206033011235010141