目　录

第一章 前言

随着我国金融改革的进行，各个银行纷纷将竞争的焦点集中到服务手段上，不断加大电子化建设投入，扩大计算机网络规模和应用范围。但是，应该看到，电子化在给银行带来利益的同时，也给银行带来了新的安全问题，并且，这个问题现在显得越来越紧迫。原因主要有三个:

- 是伴随我国经济体制改革，特别是金融体制改革的深入、对外开放的扩大，金融风险迅速增大。防范和化解金融风险成了各级政府和金融部门非常关注的问题。

- 二是当前计算机应用日益广泛、计算机日趋网络化，系统的安全性漏洞也随之增加。多年以来，银行迫于竞争的压力，不断扩大电子化网点、推出电子化新品种，忽略了计算机管理制度和安全措施的建设，使计算机安全问题日益突出。

- 三是计算机知识日益普及，金融网络向国际化发展，计算机犯罪技术也在不断提高，利用计算机犯罪的案件呈逐年上升趋势，这也迫切要求银行信息系统具有更高的安全防范体系。

银行信息系统安全性总的原则应该是：制度防范内，技术防范外。所谓“制度防内”，是要建立严密的计算机管理规章制度、运行规程，形成内部各层人员、各职能部门、各系统的相互制约关系，杜绝内部作案的可能性，并建立良好的故障处理反应机制，保障银行信息系统的安全正常运行；“技术防外”主要是指从技术手段上加强安全措施，防止外部黑客的入侵。我们在不影响中国工商银行正常业务与应用的基础上建立安全防护体系，从而满足中国工商银行的网络安全要求，为中国工商银行的网络保驾护航!

第二章 安全的概念

当前基于银行内部网的业务系统已全面运行。随着工行业务范围的不断扩大和对网络与系统要求的不断提高，安全风险亦随之增加。与此同时，与合作伙伴的网络相连提供代理服务（中间业务）、为客户提供网上服务，也成为工行业务发展的一个重点。面对这些要求，如何更好地使用网络资源？如何更好地管理系统和网络？如何全面地提高工行信息系统的安全指数？如何更好地为客户提供网上服务？都是亟待解决的问题。非常复杂，也给网络的安全带来极大的隐患。

建设功能强大和安全可靠的网络化信息管理系统是工行网络实现现代化管理的必要手段。如何构建工行安全可靠的网络系统是本方案的目的。本方案将根据工行网络的网络结构特点提出工行网络安全系统的设计方案。

（本方案是本公司为工行网络提出的“网络安全系统－防火墙分系统”的设计建议，将不涉及其他部分的内容，如“入侵检测系统”、“数据安全系统”等）

2.1 信息安全的内涵

长期以来，人们把信息安全理解为对信息的机密性、完整性和可获性的保护，这固然是对的，但它是面向单机、面向数据的。八十年代进入了微机和局域网时代，计算机已从专用机房内解放到分散的办公桌面乃至家庭，由于它的用户/网络结构比较简单、对称，所以既要依靠技术措施保护，还要制定人人必须遵守的规定。因此，这个时代的信息安全是面向网管、面向规约的。

九十年代进入了互联网时代，每个用户都可以联接、使用乃至控制散布在世界上各个角落的上网计算机，因此 Internet 的信息安全内容更多，更为强调面向连接、面向用户。因为在这个新的信息世界里，人与计算机的关系发生了质的变化。人、网、环境相结合，形成了一个复杂的巨系统。在这个复杂的巨系统中，"人"以资源使用者的身份出现，是系统的主体，处于主导地位，而系统的资源(包括硬软件、通讯网、数据、信息内容等)则是客体，它是为主体即"人"服务的，

与此相适应，信息安全的主体也是"人"（包括用户、团体、社会和国家），其目的主要是保证主体对信息资源的控制。可以这样说：面向数据的安全概念是前述的保密性、完整性和可靠性， 而面向使用者的安全概念则是鉴别、授权、访问控制、抗否认性和可服务性以及在于内容的个人隐私、知识产权等的保护。这两者结合就是信息安全体系结构中的安全服务功能，而这些安全问题又要依靠密码、数字签名、身份验证技术、防火墙、安全审计、灾难恢复、防病毒、防黑客入侵等安全机制（措施）加以解决。其中密码技术和管理是信息安全的核心，安全标准和系统评估是信息安全的基础。总之，从系统的概念出发，现代的信息安全是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共、国家信息安全的总和。信息安全系统是一个多维、多因素、多层次、多目标的系统。

我们在一个大系统的安全建设方面，要从系统复杂性的观点理解和解决整个系统安全问题：信息安全是过程、策略、标准、管理、指导、监控、法规、培训和工具技术的有机总和。这需要在不同层面上面向目标，用定性与定量相结合、技术措施与专家经验相结合的综合集成方法加以解决。对信息内容的管理则要从源头、传递、网关、服务网站和用户层面进行综合管理控制。

2.2 安全方案的设计原则

网络安全体系的核心目标是实现对网络系统和应用操作过程的有效控制和管理。任何安全系统必须建立在技术、组织和制度这三个基础之上。

在设计工行网络的网络安全系统时，我们将遵循以下原则：

全局性、综合性、整体性设计原则

工行网络的安全方案将运用系统工程的观点、方法，从工行的网络整体角度出发，分析工行网络的安全问题，提出切合工行需求的行之有效的安全解决方案。

需求、风险、代价平衡分析的原则

对各个网络来说，绝对安全难以达到，也不一定必要。对一个网络要进行

实际分析，对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定本系统的安全策略。保护成本、被保护信息的价值必须平衡。

在设计工行安全方案时，将均衡考虑各种安全措施的效果，提供具有最优的性能价格比的安全解决方案。安全需要付出代价(资金、性能损失等)，但是任何单纯为了安全而不考虑代价的安全方案都是不切实际的。方案设计同时提供了可操作的分步实施计划。

可行性、可靠性、安全性

作为一个工程项目，可行性是设计工行安全方案的根本，它将直接影响到网络通信平台的畅通；可靠性是安全系统和网络通信平台正常运行的保证；而安全性是设计安全方案的最终目的。

多重保护原则

任何安全保护措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其它保护仍可保护信息的安全。

没有任何一个安全系统可以做到绝对的安全，因此在做安全方案设计时不能把整个系统的安全寄托在单一的安全措施或安全产品上，应该采取多级防护原则，确保信息系统安全。

一致性原则

主要是指网络安全问题应与整个网络的工作周期(或生命周期)同时存在，制定的安全体系结构必须与网络的安全需求相一致。在设计工行安全方案时就充分考虑在实施中的风险及实施周期和成本，对潜在的风险做了充分的分析并给出相应的解决对策。

可管理、易操作原则

安全措施要由人来完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，采用的措施不能影响系统正常运行。

设计方案应该尽量采用最新的安全技术，实现安全管理的自动化，以减轻安全管理的负担。同时减小因为管理上的疏漏而系统的安全造成的威胁。

适应性、灵活性原则

安全措施必须能随着网络性能及安全需求的变化而变化，要容易适应、容易修改。

2.3 网络安全系统的技术实施

构筑网络安全系统的最终目的是对网络资源或者说是保护对象实施最有效的安全保护。从网络的系统和应用平台对网络协议层次的依赖关系不难看出，只有对网络协议结构层次的所有层次实施相应有效的技术措施，才能实现对网络资源的安全保护。

针对一般网络系统的结构和应用要求，为了达到保护网络资源的目的，必须在网络协议层次实施相应的安全措施，如下表 1。

表 1 （ * 表示需要实施）

	物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
			※	※		※	※
访问控制			※	※		※	※
数据保密	※	※	※	※		※	※
数据完整性			※	※		※	
不可抵赖性						※	
审计			※	※	※		※
可用性	※	※	※	※			

在本方案中，我们建议工行网络系统通过防火墙系统、防病毒网关完成表 1 中的安全手段实施。

2.4 主要的安全技术

由于 TCP/IP 协议本身的安全问题，使现在的网络存在大量的安全问题，如缺少足够的访问控制机制、缺少足够的身份认证机制、边界缺少安全防护、网络结构不合理、缺少 QoS 管理、缺少审计等安全问题。安全防护技术就是为了解决这些安全问题。目前常用的安全技术有:

- 密码技术

密码技术的基本思想是伪装信息。所谓加密是指将信息经过加密密钥及加密函数转换，变成无意义的密文；而解密则是将此密文经过解密函数、解密密钥的处理还原成明文。密码技术是网络安全技术的基础。

- 身份验证技术

身份识别是指用户向系统出示自己的身份证明过程。身份认证是系统查核用户的身份证明过程。通常把这两项工作统称为身份验证，是判明和确认通信双方真实身份的两个重要环节。常用的验证技术有以下三种: 报文鉴别; 身份鉴别，包括口令鉴别、磁卡鉴别、生物特征鉴别；数字签名。

- 访问控制技术

在计算机系统中，安全机制的核心是访问控制。访问控制技术是计算机网络系统中要确定合法用户对哪些系统资源享有何种权限、可进行什么类型的访问操作，防止非法用户进入计算机系统和合法用户对系统资源的非法使用。它包括有关策略、模型、机制的基础理论与实现方法。实施访问控制是维护系统运行安全、保护系统资源的重要技术手段。

- 防火墙技术

防火墙就是一个或一组网络设备，用来在两个或多个网络间加强访问控制，其目的是保护一个网络不受来自另一个网络的攻击。防火墙应该是不同网络之间的唯一出入口，并能根据制定的安全策略对出入网络的信息流进行控制。防火墙总体可分为三大类: 分组过滤、应用代理和状态检测型。

- 安全内核技术

在操作系统的层次上进行安全性的增强。通过对操作系统内核的裁剪、加固和改造，删除了内核中可能引起安全性问题的部分，大大加强了系统内部的安全性和抗攻击能力。

- 网络反病毒技术

计算机病毒是将自身纳入其它程序中的一段小程序，它可以自我隐蔽、自我生成，利用其它合法程序不断传播和进行破坏。从广义上讲，它还包括逻辑炸弹、木马和系统陷阱入口等。计算机病毒攻击网络的途径主要是通过软盘拷贝、互联网上的文件传输、硬件设备中的固化病毒的程序等。网络病毒可以突破网络的安全防御，侵入到网络主机上，破坏资源、甚至造成网络的瘫痪。网络反病毒技术主要包括预防病毒、检测病毒和杀病毒三种技术。

- 信息泄露防治技术

信息泄漏的两种情况：① 通过地线、电源线、信号线传播出去；② 通过空间传播。泄漏信息易被故意方接收并重显出来，从而造成失密。

- 网络安全漏洞扫描技术

计算机系统安全与否取决于它的软硬件的设计，而实际系统安全取决于设备的使用。在用户和系统管理的操作中，最能影响系统安全性的是系统或用户的工作参数设置。系统遭受入侵的最主要原因是系统特性的错误使用，而这种错误发生概率极高。利用安全漏洞扫描技术可以发现许多常见的问题。安全漏洞扫描技术通过对系统当前的状况进行扫描、分析，找出可能威胁系统的异常系统配置。

- 入侵检测技术

入侵检测是根据用户的历史行为，基于用户的当前操作，完成对攻击的决策并留下攻击证据，为数据恢复和事故处理提供依据。入侵检测过程是一个机器(检测工具)与人(黑客)对抗的决策分析过程，其技术基础是基于知识的智能推理。入侵检测可分为实时入侵检测和事后入侵检测两种。

- 冗余及备份技术

冗余及备份技术是保证网络系统持续运营的一项保证，在网络安全的构建构成中，重要的连接点上必须考虑链路及设备的冗余及备份技术，以确保网络的高可用性。

- 日志、审计技术

早期的大、中型计算机系统中都收集审计信息来建立跟踪文件，这些审计跟踪的目的多是为了性能测试或计费，目前这些审计文件也为系统安全检

测提供了有用信息。通用的审计跟踪能提供用于攻击检测的重要信息，例如如何运行了什么程序，什么时候访问或修改过那些文件。为了使通用的审计跟踪能用于攻击检测等安全目的，必须配备自动工具对审计数据进行分析，以期尽早发现那些可疑事件或行为的线索，给出报警或对抗措施。

第三章 工商银行网络结构与应用系统分析

3.1 工商银行的网络结构

工商银行网络总体是一个银行内部业务系统，采取总行到省行及地市分行的三级网络结构。

整体网络分为三级节点：一级分行网络为一级的节点；二级分行网络为二级的节点；各支行/网点网络为三级节点。这里我们参见图 3.1 一级分行辖内网络安全设计总图所示。

我们在这里以一级分行网络为主，介绍网络安全在工商银行的网络结构和系统的应用。

3.2 网络应用

办公区、综合信息区、生产区系统应用

办公区主要是为银行内部用户办公使用。综合信息区和生产区是为内部办公用户通过局域网络互连成为办公自动化系统，通过网络不同部门或不同用户之间可以共享文件、打印机等公共资源，不同用户之间可以方便地进行信息交换。各部门或不同级别用户都有一些重要或涉密信息存放在内部网中。

网管安管区应用

网络安管区以集中控管整个一级分行辖内网络为中心的。

与合作伙伴网络互连应用

前面提到的中间业务服务器与外单位相连接，通过该中间业务服务器，与其它银行、企业如：电信、证券公司之间进行如代收电话费、证券交易等业务，中间业务服务器为银行与外单位提供一种互连接口。

第四章 工商银行网络安全风险分析

随着银行外联业务的兴起以及与相关合作伙伴网络的连接,例如公安、税务、电信、电力、证券、商业等业务往来增多，地市分行的外联网也在逐步扩大，网上银行正蓬勃发展，以上种种网络环境要求银行网要有很高的可靠性、安全性和保密性。由于目前网络的应用的自由性、广泛性以及黑客的“流行”，银行面临着各种安全威胁。如：非授权访问、信息泄露、数据被篡改或丢失等。一旦信息泄露或者信息混乱，将给银行自身信誉、社会稳定、国家安全带来巨大影响。

为了便于分析网络安全风险和设计网络安全解决方案,我们采取对网络分层的方法，并且在每个层面上进行细致的分析，根据风险分析的结果设计出符合具体实际的、可行的网络安全整体解决方案。

从系统和应用出发，网络的安全因素可以划分到如下的五个安全层中，即物理层、系统层、应用层、网络层和安全管理。

4.1 物理层的安全风险分析

网络的物理安全风险主要指网络周边环境和物理特性引起的网络设备和线路不可以使用,而造成网络的不可以使用。它是整个网络安全的前提。如:

- 设备被盗、被毁坏
- 链路老化或被有意或者无意的破坏
- 因电子辐射造成信息泄露
- 设备意外故障、停电
- 地震、火灾、水灾等自然灾害

因此，银行专网在网络安全考虑时，首先要考虑物理安全。例如：设备被盗、被毁坏；设备老化、意外故障；计算机系统通过无线电辐射泄露秘密信息等。除此之外，由于银行专用网络涉及业务网核心与管理网核心两个不同的密级，因此在方案中我们将利用“物理隔离”技术，将两个网络从物理上隔断而保证逻辑上连通实现所谓的“信息摆渡”。

4.2 网络层安全风险分析

4.2.1 数据传输风险分析

1. **重要业务数据泄漏**

由于在同级局域网和上下级网络数据传输线路之间存在被窃听的威胁，同时局域网网络内部也存在着内部攻击行为，其中包括登录通行字和一些敏感信息，可能被侵袭者搭线窃取和篡改，造成泄密。

如果没有专门的软件或硬件对数据进行控制，所有的广域网通信都将不受限制地进行传输，因此任何一个对通信进行监测的人都可以对通信数据进行截取。这种形式的“攻击”是相对比较容易成功的，只要使用现在可以很容易得到的“包检测”软件即可。

2. **重要数据被破坏**

由于目前尚无安全的数据库及个人终端安全保护措施，还不能抵御来自网络上的各种对数据库及个人终端的攻击。同时一旦不法分子针对网上传输数据做出伪造、删除、窃取、窜改等攻击，都将造成十分严重的影响和损失。存储数据对于银行系统来说极为重要，如果由于通信线路的质量原因或者人为的恶意篡改，都将导致难以想象的后果，这也是网络犯罪的最大特征。

4.2.2 网络边界风险分析

4.2.2.1 银行中间业务系统安全

银行在要求扩大社会服务面的前提下，应运而生的是各项中间业务的蓬勃发展，各种各样的银行代理业务悄然出现，如代发工资、代收电费、代收水费、代收煤气费、代收电话费、代收税款、办理证券等等；银行的服务手段也从传统的柜台发展到 ATM、自助终端、电话银行等自助式的服务方式，最后发展到完全通过网络进行资金的结算，同时银行因业务需要和相关行业部门打交道的机会也在同步增长，例如在实行存款实名制后，银行可能要到公安系统网络查询身份证信息。在实行存款纳税后需要与国税网络进行数据交换等，为方便客户和中心管理，

银行都建立了中间业务平台系统。该系统灵活地与银行储蓄、信用卡和会计业务系统结合，同时保持相对的独立性，把银行的各种中间业务集中在一起统一管理，实现各种各样不同方式的中间业务应用。

由于中间业务的另一方可能处于一个较为开放的网络环境中，而且中间业务委托方的网络很可能与 INTERNET 网络进行互连，所以中间业务网络环境的复杂性和开放性成为中间业务网络潜在威胁的最大来源。

4.2.2.2 INTERNET 出口的安全

目前许多银行的网络提供与 INTERNET 连接的基于 WEB 的网上银行服务，并且，银行内部用户也有上网需求，但现有的网络安全防范措施还很薄弱，存在的安全风险主要有:

- 入侵者通过 Sniffer 等程序来探测扫描网络及操作系统存在的安全漏洞，如网络 IP 地址、应用操作系统的类型、开放哪些 TCP 端口号、系统保存用户名和口令等安全信息的关键文件等，并通过相应攻击程序对内网进行攻击。
- 入侵者通过网络监听等先进手段获得内部网用户的用户名、口令等信息，进而假冒内部合法身份进行非法登录，窃取内部网的重要信息。
- 入侵者通过发送大量 PING 数据包对内部网中重要服务器进行攻击，使得服务器超负荷工作以至拒绝服务甚至系统瘫痪。

4.2.2.3 管理系统和业务系统之间的访问控制需求

内部网中办公系统与银行业务系统之间如果没有采用相应一些访问控制，也可能造成内部重要信息泄漏或非法攻击。

银行办公系统不仅提供办公自动化，而且还可能涉及到如财务数据报表、领导决策等机密信息。银行业务系统涉存放着大量重要的数据库信息，包含无数客户的信息。因此依据银行办公系统与银行业务系统都有各自的重要信息，在通常情况下这两个系统之间是不允许随意访问的。我们知道网络安全不仅来自外部网络，同样存在于内部网，而且来自内部的攻击更严重、更难防范。如果银行办公

系统与业务系统没有采取相应安全措施，同样是内部网用户的个别员工可能访问到他本不该访问的信息。还可能通过可以访问的条件制造一些其它不安全因素（伪造、篡改数据等）。或者在别的用户关机后，盗用其 IP 进行非法操作，来隐瞒身份。

4.2.3 网络设备的安全风险

由于银行专用网络中使用大量的网络设备，如交换机、路由器等。使得这些设备的自身安全性也会直接关系的银行系统和各种网络应用的正常运转。例如，路由设备存在路由信息泄漏、交换机和路由器设备配置风险等。

4.3 系统层的安全风险

系统级的安全风险分析主要针对银行专用网络采用的操作系统、数据库、及相关商用产品的安全漏洞和病毒威胁进行分析。银行专用网络通常采用的操作系统(主要为 UNIX)本身在安全方面有一定考虑，但服务器、数据库的安全级别较低，存在一些安全隐患。

4.4 应用层安全风险分析

银行专用网络应用系统中主要存在以下安全风险：业务网和办公网之间的非法访问；中间业务的安全；用户提交的业务信息被监听或修改；用户对成功提交的业务进行事后抵赖；由于银行专用网络对外提供网上银行 WWW 服务，因此存在外部网非法用户对服务器攻击。

4.4.1 与 INTERNET 连接带来的安全隐患

为满足银行内部用户上网需求，银行网与 INETRNET 直接连接，这样网络结构信息极易为攻击者所利用，有人可能在未经授权的情况下非法访问银行的内部网络，窃取信息同时由于二者之间尚无专门的安全防护措施，服务器主机所提供的网络服务也极易被攻击者所利用，发动进一步攻击。即使采用代理服务器进行网络隔离，一旦代理服务器失控，内部网络将直接暴露在 INTERNET 上，如果银

行开通网络银行服务，内部部分业务系统还需要向公众开放，面临网络黑客攻击的威胁更大。

4.4.2 身份认证漏洞

服务系统登录和主机登录使用的是静态口令，口令在一定时间内是不变的，且在数据库中有存储记录，可重复使用。这样非法用户通过网络窃听，非法数据库访问，穷举攻击，重放攻击等手段很容易得到这种静态口令，然后，利用口令，可对资源非法访问和越权操作。

4.4.3 高速局域网服务器群安全

4.4.3.1 银行网络服务器的基本安全需求

满足基本的安全要求，是该网络服务器成功运行的必要条件，在此基础上提供强有力的安全保障，是网络安全的重要原则。

银行网络内部部署了众多的网络设备、服务器，保护这些设备的正常运行，维护主要业务系统的安全，是银行网络的基本安全需求。对于各种各样的网络攻击，如何在提供灵活且高效的网络通讯及信息服务的同时，抵御和发现网络攻击，并且提供跟踪攻击的手段，是一项需要解决的问题。

银行网络基本安全要求:

(1) 网络正常运行。在受到攻击的情况下，能够保证网络服务器继续运行。

(2) 服务器网络管理/网络部署的资料不被窃取。

(3) 具备先进的入侵检测及跟踪体系。

(4) 提供灵活而高效的内外通讯服务。

4.4.3.2 业务系统服务器的安全分析

与普通网络应用不同的是，业务系统服务器是银行网络应用的核心。对于业务系统服务器应该具有最高的网络安全措施。业务系统服务器面临以下安全问题:

- 对业务服务器的非授权访问

业务服务器是为银行应用系统提供信息数据服务，许多信息只有相应级别用户才能查阅，由于缺乏安全措施，可能会有非法用户在没有经过允许下直接访问网络资源，造成机密信息外泄。

- 对业务服务器的攻击

当有黑客利用网络漏洞对建行业务主机攻击或网络受到其它一些安全威胁时(如内部人员的违规操作等)，网络无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。使有时间要求的服务不能及时得到响应，使信息系统处于瘫痪状态。

- 业务服务器的带宽要求

业务服务器是银行应用最繁忙的网络设备，因此面临网络带宽的巨大压力，同时服务器必须响应实时的数据访问请求，保持应用的高可靠性，所以服务器群必须有优先的带宽分配请求，不能允许其他应用占用网络资源。为保证服务器可靠响应，总行与各分行之间的网络线路和设备必须保证 24 小时畅通，网络设备要有相应的冗余和备份。

银行业务系统服务器应保障:

(1) 访问控制，确保业务系统不被非法访问，业务系统资源不被其他应用非法占用。

(2) 数据安全，保证数据库软硬件系统的整体安全性和可靠性和数据传输的安全性。

(3) 入侵检测，对于试图破坏业务系统的恶意行为能够及时发现、记录和跟踪，提供非法攻击的犯罪证据。

(4) 来自网络内部其他系统的破坏，或误操作造成的安全隐患。

(5) 对业务服务器信息流应有相应的审计功能。

4.4.3.3 内部管理服务平台的安全分析

管理公用服务平台指由银行网络提供给网内客户的公共信息服务，提供公用服务一般是银行总行或省\市一级分行，公用服务平台有可能受到来自内部网络

人员资源非法占用和做攻击性测试。

公用服务平台的安全要求:

(1) 访问控制。

(2) 服务器实时安全监控。

(3) 应用系统的通讯安全。

4.5 表示层安全风险分析

最安全的网络设备离不开人的管理，再好的安全策略最终要靠人来实现，因此管理是整个网络安全中最为重要的一环,尤其是对于一个比较庞大和复杂的网络，更是如此。因此我们有必要认真的分析管理所带来的安全风险，并采取相应的安全措施。

银行系统应按照国家关于计算机和网络的一些安全管理条例，如《计算站场地安全要求》、《中华人民共和国计算机信息系统安全保护条例》等，制订安全管理制度。

责权不明，管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。责权不明，管理混乱，使得一些员工或管理员随便让一些非本地员工甚至外来人员进入银行网络机房重地,或者员工有意无意泄漏他们所知道的一些重要信息，而管理上却没有相应制度来约束。

当网络出现攻击行为或网络受到其它一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

第五章 工商银行一级网络安全解决方案

5.1 网络安全方案设计原则

网络安全建设是一个系统工程，工商银行一级网络安全体系建设应按照“统一规划、统筹安排，统一标准、相互配套”的原则进行，采用先进的“平台化”建设思想，避免重复投入、重复建设，充分考虑整体和局部的利益，坚持近期目标与远期目标相结合。

5.2 工商银行一级分行网络安全解决方案

在解决方案中，我们推荐在总行入围的 NETSCREEN 产品作为该解决方案的应用产品。

5.2.1 物理层安全解决方案

保证计算机信息系统各种设备的物理安全是保障整个网络安全的前提。物理安全是保护计算机网络设备、设施以及其它媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。它主要包括三个方面：环境安全、设备安全、线路安全。

为了将不同密级的网络隔离开，我们还要采用隔离技术将核心密和普通密两个网络在物理上隔离同时保证在逻辑上两个网络能够连通。

- 环境安全

  对系统所在环境的安全保护，如区域保护和灾难保护；（参见国家标准 GB50173－93《电子计算机机房设计规范》、国标 GB2887－89《计算站场地技术条件》、GB9361－88《计算站场地安全要求》

- 设备安全

  设备安全主要包括设备的防盗、防破坏、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等；设备冗余备份；通过严格管理及提高员工的整体安全意识来实现。

- 媒体安全

  包括媒体数据的安全及媒体本身的安全。显然，为保证银行网络的物理安全，除在网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多，在理论和技术支持下的验证工作也证实这种截取距离在几百甚至可达千米的复原显示技术给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间上的扩散，通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。

- 隔离技术

  隔离技术要达到以下几点关键技术:

- 物理隔断:
- 可选择数据交换：两个网络能够有选择的交换数据，好像它们直接相连一样。
- 数据是静态的：在交换数据过程中，数据是静态的（被动的），不能被执行。
- 独立决策：所有决策要求数据在一个安全的环境中处理，与不可信的网络隔断。
- 高性能：上述所有工作实时进行，最大通过量和最小延时。

5.2.2 网络层安全解决方案

5.2.2.1 防火墙安全技术建议

工商银行网络是一个由总行、省行、各地市行网络组成的三级网络体系结构，从网络安全角度上讲，他们属于不同的网络安全域，因此在各中心的网络边界，以及 Internet 边界都应安装防火墙，并需要实施相应的安全策略控制。另外，根据对外提供信息查询等服务的要求，为了控制对关键服务器的授权访问控制，建议把对外公开服务器集合起来划分为一个专门的服务器子网，设置防火墙策略来保护对它们的访问。应通过防火墙进行办公网和业务网的隔离，并对下一级分行的访问进行合理控制。

网络边界安全一般是采用防火墙等成熟产品和技术实现网络的访问控制，采用安全检测手段防范非法用户的主动入侵。

采用的 NetScreen 防火墙产品具有以下功能，能完全符合工行安全建设的标准和需求。

- 基于状态检测的分组过滤
- 多级的立体访问控制机制
- 面向对象的管理机制
- 支持多种连接方式，透明、路由、NAT（网络地址转换）
- 支持 OSPF、IPX、NETBEUI、SNMP 等协议
- 具有双向的地址转换能力
- 透明应用代理功能
- 一次性口令认证机制
- 带宽管理能力
- 内置了一定的入侵检测功能或能够与入侵检测设备联动
- 远程管理能力
- 双机冗余功能
- 负载均衡
- 支持动态 IP 地址
- 内嵌 VPN 功能支持
- 灵活的审计、日志功能

5.2.2.2 入侵检测安全技术（建议）

利用 NetScreen 防火墙技术，经过仔细的配置，通常能够在内外网之间提供安全的网络保护，降低了网络安全风险。但是，仅仅使用防火墙，网络安全还远远不够，主要表现在以下几个方面:

- 入侵者可寻找防火墙背后可能敞开的后门
- 入侵者可能就在防火墙内
- 由于性能的限制，防火墙通常不能提供实时的入侵检测能力
- 保护措施单一

入侵检测系统是近年出现的新型网络安全技术，目的是提供实时的入侵检测及采取相应的防护手段，如发现违规访问、阻断网络连接、内部越权访问等，发现更为隐蔽的攻击。

银行专用网络安全体系必须建立一个智能化的实时攻击识别和响应系统，管理和降低网络安全风险，保证网络安全防护能力能够不断增强。

目前网络入侵安全问题主要采用网络入侵监测系统等成熟产品和技术来解决。网络入侵检测系统应能满足以下要求:

- 能在网络环境下实现实时地分布协同地入侵检测，全面检测可能的入侵行为。能及时识别各种黑客攻击行为，发现攻击时，阻断弱化攻击行为、并能详细记录，生成入侵检测报告，及时向管理员报警。
- 能够按照管理者需要进行多个层次的扫描，按照特定的时间、广度和细度的需求配置多个扫描;
- 能够支持大规模并行检测，能够方便地对大的网络同时执行多个检测;
- 所采用的入侵检测产品和技术不能被绕过或旁路。
- 检测和扫描行为不能影响正常的网络连接服务和网络的效率。
- 检测的特征库要全面并能够及时更新。
- 安全检测策略可由用户自行设定，对检测强度和风险程度进行等级管理，用户可根据不同需求选择相应的检测策略。
- 能够帮助建立安全策略，具有详细的帮助数据库，帮助管理员实现网络的安全，并且制定实际的、可强制执行的网络安全策略。

5.2.2.3 网络设备安全增强技术

在漏洞扫描与风险评估的基础上对网络设备进行安全性增强配置，下面以CISCO 路由器的几个安全增强配置为例说明网络设备的安全性也是不容忽视的。

- 合作伙伴接入集中到一至二台路由器。
- 外连路由器禁止从外网的 telnet 连接。
- 外连路由器如使用 Cisco 设备，必须关闭 CDP，以免泄露网络信息。
- 启用 NAT 功能，隐藏内网的真实地址，避免泄露内网信息。
- 基于多重保护原则，外连路由器也启用 ACL，和防火墙的包过滤策略保持一

致，确保防火墙在发生故障时还保持相当的防护。

- 对合作伙伴提供的 WEB、FTP 等高风险服务的服务器应放在 DMZ 区，后台应用服务器放在内网。
- 防火墙应具备动态状态检测、NAT、代理用户认证、入侵检测等功能和足够的转发能力。
- 防火墙的软件应该易于升级。可以通过图形界面的方式，通过浏览器的方式来将目标文件导入至防火墙，随后，防火墙收到升级文件后，会自动进行升级和重新启动 NetScreenOS 系统,以确保升级的成功和应用程序的正常运行。
- Login Banner 配置：修改 login banner，隐藏路由器系统真实信息，防止真实信息的泄露。
- 用户验证配置：配置用户验证方式以增强系统访问的安全性。
- AAA 方式配置：配置 AAA 方式来增加用户访问安全性。
- 路由命令审计配置：配置 AAA 命令记账来增强系统访问安全性。

5.2.2.4 数据传输安全建议

为保证数据传输的机密性和完整性，建议在工商银行专用网络中采用安全 VPN 系统，系统部署如下，在远程前置机和 NetScreen 防火墙之间统一安装 VPN 设备。并且支持远程分布式集中统一管理功能。

5.3 防火墙系统集中管理（可选）

工商银行网络是由多个不同安全级别安全域的组成，为了保证企业内部网络的安全性，建议在相应的边界处设立相应的防火墙系统。这个分散的防火墙系统的设置和管理就显得非常重要，因为它某一处的漏同将影响整个工商银行网络分行 Intranet 的安全性。

在此防火墙系统的管理上，有分散和集中两种方式。分散方式分别管理各自的防火墙。方式在大型企业中存在较大的缺点，首先它对各处的网络管理员要求非常高，相应提高了企业的管理成本；其次，当防火墙系统部署点很多时，由于各自制定安全策略，存在安全隐患较大，同时，当出现安全问题时，由于没有实现统一监控，很难判断问题出现在何处，从而不能及时解决问题。集中方式将对

所有防火墙实现集中的管理，集中制定安全策略，这将很好的克服以上缺点。

我们推荐工商银行网络对防火墙系统实行统一的管理。

NetScreen 防火墙可实现方便的集中管理。NetScreen 的安全管理系统 NetScreen Global PRO 具有集中的设备配置、故障/事件管理、基于角色的监控、使用跟踪等功能。NetScreen-Global PRO 提供了中央配置管理功能，可以高效地把数百条、甚至数千条策略分发到各 NetScreen 设备或设备群组及 NetScreen-Remote 客户端。

NetScreen-Global PRO 系列的关键性能在它能够通过简便操作、直观的策略管理用户界面，迅速为设备完成部署。用户只需一次性地定义一条策略，然后将其映射采用到多个设备中。 换言之，NetScreen-Global PRO 为设备部署提供高度易操作性与灵活性，减少管理工作。

本方案为工商银行网络配置的 NetScreen-Global PRO Express 软件适合用于多达 25 台 NetScreen 设备部署的企业中。通过 NetScreen-Global PRO Express，工商银行网络管理员可以简便地管理 NetScreen 设备，监控整个广域网防火墙设备部署，建立网络活动图形报表及实现策略管理。

5.4 安全域的划分

5.4.1 安全域

安全域，系统内包含相同的安全要求，达到相同的安全防护等级的区域。同一个安全域，一般要求有统一的安全管理组织和制度以及统一的安全技术防护体系。安全域定义了与内部网络系统的最低安全等级，在安全域内可以包含更高安全级别的安全域。

安全域分离是指确保至少有一个安全域，对自己执行是可用的，并且该主体受保护不被不可信主体从外部干扰和篡改。域分离的具体要求如下:

通过将安全域的资源与该域外的主体及不受约束的实体分离开，使得安全域外的实体不能观察或修改安全域内的数据或编码;

域内传输是受控的，不能随意地进入或退出安全域;

按地址传到保护域的用户或应用参数，根据保护域的地址空间进行确认，而按值传到保护的域的用户或应用参数则根据保护域内所期望的值进行确认;

5.4.2 安全域划分

在确定网络安全防护边界时，首先要确定网络内安全域的划分，我们把整个工商银行的内部生产网、测试区和服务器群构成的网络看作是一个安全域，内部生产网、测试区和服务器群组则是这个安全域中拥有更高安全级别的安全域。

根据我公司对工行网络系统的经验，我们从工商银行整个网络拓扑的角度来看，可以将工商银行的网络系统依照其信息安全风险划分为以下几个安全等级和可信度，见下列图示:

	安全区域	安全级别	访问级别
1	合作伙伴网络	低级	提供网络连接，可以访问经过审核的网络资源
2	服务器群组、测试区、生产区	中级	提供一般的访问控制
3	办公区、数据中心、综合信息区、网管安管区	高级	对经过严格审核的访问开放

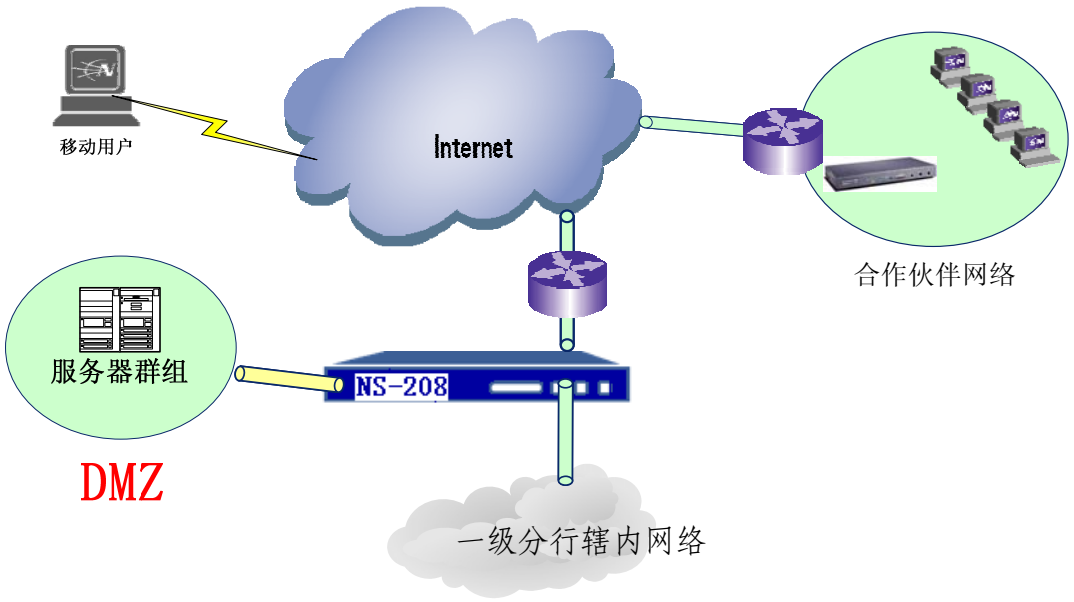


图 5.1 一级分行辖内网络安全设计总图

5.4.3 安全域分析

我们在 NetScreen 防火墙划分三个安全级别，详见上面图示。这样我们很好的将来自合作伙伴网络的威胁，降低到最低程度，将风险分为两个部分，一个是我们需要重点保护的办公区、数据中心、综合信息区、网管安管区四个区域，另一个是安全等级为中级的区域，主要包括服务器群组、测试区、生产区等几个对外发布信息的区域，在 NetScreen-204 和 NetScreen-208 中分别可以提供两个和六个独立的接口，提供给这个区域，这样可以令黑客攻击某台服务器的同时，不会威胁到其它的服务器，更不会威胁到我们定义的安全级别为高级的办公区、数据中心、综合信息区、网管安管区的区域。

5.5 防火墙的选择

5.5.1 防火墙选择要点

选择防火墙的要点在于:

- 安全性

  即是否通过了严格的入侵测试;
- 抗攻击能力

  对典型攻击的防御能力;
- 性能

  是否能够提供足够的网络吞吐能力;
- 自我完备能力，自身的安全性，Fail-close 可管理能力
- 是否支持简单方便的管理和监控
- VPN 支持
- 认证和加密特性
- 服务的类型和原理
- 网络地址转换能力
- 与网络内其它安全系统的动态适应
- 可靠性是否支持系统冗余

对于网络不同信任域，实现双向控制或有限访问原则，使受控的子网或主机访问权限和信息流向能得到有效控制。具体相对网络对象而言需要解决网络的边界的控制和网络内部的控制，对于网络资源来说保持有限访问的原则，信息流向则可根据安全需求实现单向或双向控制。访问控制最重要的设备就是防火墙，防火墙是网络安全领域的首要的，基础的设施，它对维护内部网络的安全起着重要的作用。利用防火墙可以有效的划分网络不同安全级别区域间的边界，并在边界上对不同区域间的访问实施访问控制、身份鉴别、和审计等安全功能。

防火墙是保护网络内部安全的第一道防护，使用防火墙有如下益处:

- **保护脆弱的服务**

  通过过滤不安全的服务，防火墙可以极大地提高网络安全和减少子网中主机的风险。例如，防火墙可以禁止 NIS、NFS 服务通过，防火墙同时可以拒绝源路由和 ICMP 重定向封包。

- **控制对系统的访问**

  防火墙可以提供对系统的访问控制。如允许从外部访问某些主机，同时禁止访问另外的主机。例如，防火墙允许外部访问特定的 Mail Server 和 Web Server。

- **集中的安全管理**

  防火墙对网络实现集中的安全管理，在防火墙定义的安全规则可以运行于整个内部网络，而无须在内部网每台机器上分别设立安全策略。防火墙可以定义不同的认证方法，而不需要在每台机器上分别安装特定的认证软件。外部用户也只需要经过一次认证即可访问内部网。

- **增强的保密性**

  使用防火墙可以阻止攻击者获取攻击网络的有用信息，如 Finger 和 DNS。

- **记录和统计网络**

  利用数据以及非法使用数据防火墙可以记录和统计通过防火墙的网络通讯，提供关于网络使用的统计数据，并且，防火墙可以提供统计数据，来判断可能的攻击和探测。

- **策略执行**

防火墙提供了制定和执行网络安全策略的手段。未设置防火墙时，网络安全取决于每台主机的用户。

5.5.2 防火墙的选型

根据用户的需求情况和我们的工程建设经验，我们选用了两款美国NetScreen百兆级防火墙，分别是NetScreen-204和NetScreen-208，作为工商银行一级分行辖内网络防火墙，该防火墙产品具有较高的性能，并经过了中国公安部的认证许可。

NetScreen 科技公司成立于 1997 年 10 月，总部位于美国加州的硅谷。公司致力于发展一种新型的与网络安全有关的高科技产品，把多种功能集成到一起，创造新的业界性能纪录。NetScreen创建新的体系结构并已取得了专利。该项技术能有效消除传统防火墙实现数据加盟时的性能瓶颈，能实现最高级别的IP 安全（IPSec），先进的系统级的设计允许产品提供多种功能，并且这些功能都具有无与伦比的性能。

NetScreen 科技公司已经为业界在虚拟专用网领域设立了新的安全解决系统的标准。所有的功能全部放在有关专有的硬件平台的盒子里，并且这些功能都有着无与伦比的性能。

目前公司由 Sequoia Capital 投资赞助。Sequoia 是一家领先的风险投资公司，成立于1974年，已成功地为超过350家公司提供了最初的风险投资基金，其中包括3Com 公司、Cisco 系统公司、Oracle 公司、Symantec 公司和Yahoo 公司等等。

NetScreen公司的产品NetScreen-100获得了KeyLabs工作组的“测试首选奖”，在1998年4月举行的数据通讯杂志的评测中，NetScreen-100的VPN吞吐量是获得第二名的2.5倍。1998年11月，NetScreen公司再次荣获“测试者选择奖”，这是数据通讯杂志的年度奖。在同类产品中，NetScreen 是唯一员工把防火墙、虚拟专用网（VPN）、负载均衡及流量控制结合起来，且提供100M高性能的产品。

在1998年，NetScreen 通过了ICSA (国际计算机安全协会)的防火墙认证。1998 年 9 月，NetScreen 推出了 VPN 远程存取客户端软件。1998 年 10 月，

NetScreen 宣布推出 NetScreen-1000 的产品。这是第一个支持千兆位传输的具有防火墙和 VPN 功能的产品。

国内的一些重要单位（部门）采用了 NetScreen 公司的产品:

．中国工商银行数据中心、中国人民银行济南分行及各地市支行、中国银行云南各地支行、中国建设银行、中国光大银行、国泰证券 、国家信息中心 、．天津市信息中心 ．四川省信息中心．化工部信息中心．、中国公众多媒体通讯网(169) (32 个省骨干节点防火墙)、．北京市电信局、电信总局数据局、福建漳州电信局、广东省数据局、上海市长话局、．西门子(中国)有限公司、清华产业集团、上海东方航空公司、．大通国际运输公司、上海通用汽车公司等。

5.5.2.1 产品性能

NetScreen 公司的防火墙产品线分布非常齐全， 有 NetScreen-5、NetScreen-10、NetScreen-100、NetScreen-204、NetScreen-208、NetScreen-500、NetScreen-1000 及 NetScreen 远程 VPN 客户软件等多种档次的安全产品。

通过新一代体系结构完成业界领先的性能和安全保护

- －专用加密加速 ASIC
- －ASIC 可处理 － DES, 3DES, MD5, SHA1, PKI 加速, Session 查找, TCP 头解析, 认证, NAT, 随机数产生和策略查询 (每秒 25 million 策略).
- －超级性能 single, multi, 与 parallel 处理板
- －基于需求定制，安全优化的操作系统 ScreenOS™

•核心技术高度集成

- 基于状态过滤的防火墙
- 攻击检测与保护
- VPN / PKI
- 流量管理 /带宽管理
- 端到端的解决方案提供灵活的网络结构
- 全面的设备管理方法

- 集成的安全系统
- ICSA 认证的 IPSec VPN 和状态监控，stateful inspection firewall, DoS 防御，认证，PKI，NAT 加速和流量管理
- 10Mbps 到 2Gbps Firewall
- 10Mbps 到 1Gbps 3DES IPSec VPN
- ScreenOS 安全软件 客户化实时操作系统

高可用性

- 稳定的状态，冗余的特性。
- HA 拓扑 - Active passive, Active- Active, Full Mesh
- DoS 攻击防护 (比软件解决方案快 8 到 10 倍)
- 强大的管理
- WebUI，CLI，简单的安装与管理
- 运营商的基于策略的集中管理和实时监控

5.5.2.2 NetScreen 全线安全产品简介

产品型号	性能特点	技术参数
NetScreen-1000	无用户数限制,硬、软件一体,2 个 1000M 接口,2 个 10/100M 接口,NAT、VPN 模式下 1000M 速度,PAT, NAT,高达 500,000 个链接数,负载均衡，动态过滤，图形管理，带宽控制，双机备份，VPN	
NetScreen-500	NetScreen-500 集防火墙、VPN 及流量管理等功能于一体，占用 2U 机架空间。它是一款高性能的产品，支持多个安全域。NetScreen-500 具有 NetScreen-1000 及 NetScreen-100 的所有优点。另外在功能上设有高可用性交换端口、管理端口及四个流量模块组，还有一个可编辑的 LCD 指示屏，使管理变得更加容易。	
NetScreen-208	NetScreen-208 是目前市场上功能最多的防火墙产品，可以方便地集成在许多不同的网络环境中，包括大中型企业的办公室，电子商务网站，数据中心和电信运营基础设施。它具有 8 个自适应 10/100M 以太网端口，延	

	续了 NetScreen 防火墙优秀的处理能力(550Mbps)--即使在对系统资源要求极高的应用中（诸如 VPN-3DES 加密）也能保持超过 200Mbps 的速率。	
NetScreen-204	NetScreen-204 是目前市场上功能最多的防火墙产品，可以方便地集成在许多不同的网络环境中，包括大中型企业的办公室，电子商务网站，数据中心和电信运营基础设施。它具有 4 个自适应 10/100M 以太网端口，延续了 NetScreen 防火墙优秀的处理能力(400Mbps)--即使在对系统资源要求极高的应用中（诸如 VPN-3DES 加密）也能保持超过 200Mbps 的速率。	
NetScreen-50	NetScreen-50 防火墙为中小型公司企业的办事处、远程办公室提供了一套完整的网络安全解决方案。NetScreen-50 是个高性能的安全应用方案，具有四个自适应 10/100 Base-以太网口（信任 Trust,非信任 Untrust,DMZ，另外一个留作将来使用），它能够提供 170Mbps 的防火墙数据流量和 50Mbps 的 3 倍 DES 加密 VPN 性能，保护局域网(LANs)以及建立数据交流的 mail 服务器，web 服务器和 FTP 服务器的安全。NetScreen-50 支持 8,000 个并发 TCP/IP 会话和 100 个 VPN 通道。	
NetScreen-25	NetScreen-50 防火墙为中小型公司企业的办事处、远程办公室提供了一套完整的网络安全解决方案。NetScreen-50 是个高性能的安全应用方案，具有四个自适应 10/100 Base-以太网口（信任 Trust,非信任 Untrust,DMZ，另外一个留作将来使用），它能够提供 100Mbps 的防火墙数据流量和 20Mbps 的 3 倍 DES 加密 VPN 性能，保护局域网(LANs)以及建立数据交流的 mail 服务器，web 服务器和 FTP 服务器的安全。NetScreen-25 支持 4,000 个并发 TCP/IP 会话和 25 个 VPN 通道。	
NetScreen-5XP	NetScreen-5XP 与以前的产品（NetScreen5a）相比具有运算速度更快的 CPU，千兆级的 ASIC 专用芯片和 4M 快速闪存，使 NetScreen-5XP 完全可以在对数据进行 3 倍 DES 加密的同时保证 10Mbps 的带宽，与过去的产品相比新增了一些主要功能，包括增强的拒绝 Dos 攻击和 VPN 路由功能。	

	NetScreen-5XP 支持全双工的以太网并且它的处理器运算速度比上代产品提升了 50%, 针对那些对于时间及其敏感的设备 NetScreen-5XP 全面提升了系统的吞吐量并将数据包的接收延迟降低到最少。（NetScreen-5XP 在 2001-SuperComm 展览中获得 SUPERQuest 大奖）	
NetScreen-Global Security Management 全球安全控管中心	NetScreen 提供了服务提供商和企业所需要的用来管理所有 NetScreen 产品的特性。众所周知 NetScreen Global Manager 允许安全管理者从一个中央控制台高效地管理几百台甚至上千台的设备，另外，广泛的实时信息和历史报告提供了关键的设备使用趋势，性能瓶颈和安全事件，对于管理单台 NetScreen 设备，NetScreen 提供了易用的基于 Web 的用户界面和命令行(CLI)。	暂无
NS-Remote 远程访问	NetScreen-Remote 是一种在用户主机（桌面或笔记本电脑）上运行的软件，简化了对网络、设备或公共或非信任网络中其它主机的安全远程接入。	

5.5.2.3 NetScreen 系列防火墙产品优势

- **专用集成化安全系统**

高性能安全系统，在基于 ASIC 的硬件平台上运行 NetScreen-ScreenOS 防火墙和 VPN 软件,提供了市场领先的性能,吞吐量高达 400Mbps 和 550Mbps，支持最多 1,000 条 VPN 隧道。

- **可管理安全域**

采用 NetScreen 独特的虚拟系统特性，在被管理安全服务或企业分区中可以提供最多 4 个和 8 个安全域。

- **高可用性**

固态设计、冗余的可带电热插拔电源和可带电热插拔风扇，在每个系统内部实现了最大的运行时间。高可用性软件允许在发生故障时切换到冗余系统，而不会丢失防火墙会话或 VPN 隧道。

- **灵活的配置选项，可扩展的解决方案**

多种配置，满足了单一企业部署到包括多个客户的大型互联网数据中心的要求。

NetScreen 公司提供了一系列专用的高性能系统，它把状态检测防火墙和 VPN 功能与业内领先的性能集成起来。NetScreen 的集成化安全系统是一种容错平台，为大型企业和服务供应商提供了可扩充的解决方案。所有 NetScreen 安全系统还支持虚拟系统，可以为多个安全域，提供安全保护。

NetScreen 的全功能防火墙采用状态检测技术，可以防止入侵人员和拒绝服务攻击。NetScreen 定制的 GigaScreen ASIC 在硬件中处理防火墙访问策略和加密算法，其性能明显要高于纯软件解决方案。

NetScreen-ScreenOS 是一种经过 ICSA 认证的状态检测防火墙。

全功能解决方案，采用为安全优化的硬件、操作系统和防火墙，比拼凑在一起的基于软件的解决方案提供了更高的安全水平。

基于策略的 NAT 允许实现入局地址转换。

强健的攻击防范功能，包括 SYN 攻击、ICMP flood、端口扫描等攻击防范功能。

网络地址转换(NAT)、端口地址转换(PAT)，隐藏了内部不可路由的 IP 地址；以及透明模式。

基于策略的 NAT 允许实现入局地址转换。

所有 NetScreen 安全系统中都集成了一个全功能 VPN 解决方案，它们支持站点到站点 VPN 及远程接入 VPN 应用。

为远程接入 VPN 应用和站点到站点 VPN 应用提供全面的 VPN 支持。网络设计可以采用集中星型 VPN 拓扑，实现全网状结构，简化远程办公室 VPN 的配置和管理，同时在主要站点之间提供冗余的高性能链路。

NetScreen-ScreenOS 经过 ICSA 和 VPNC 认证，提供了 IPSec 互操作能力。

3DES 和 DES 加密，带有数字证书的 IKE (PKI X.509)或预先共享 的密码或手动密钥协商。

SHA-1 和 MD5 强力认证。

基于策略的 NAT 实现了企业外部网 VPN 应用。

NetScreen 的虚拟系统允许创建多个安全域，每个安全域，都拥有自己的地址簿、策略和管理功能。虚拟系统与 802.1q VLAN 标记相结合，把安全域延伸到整个交换网络中。NetScreen-204、NetScreen-208 和相应的 VLAN 交换网络，可

以表现为一个可支持最多 4 个端口和 8 个端口的综合安全系统。

扩展了互联网数据中心提供的服务，可以在共享的硬件平台上提供托管 VPN 和防火墙。

针对多个 DMZ 对企业网络分段，或在内部部门之间提供安全保护能力。

把多个 VLAN 映射到一个虚拟系统上。

每个虚拟系统都采用单独的 WebUI、CLI 和管理访问权限。

NetScreen 的安全系统包括关键的高可用性冗余特性，包括自动化镜像配置、活动会话和容错 VPN 维护、可带电热插拔的冗余电源、风扇和处理模块。它利用 NetScreen 冗余协议实现了冗余的高可用性（HA）拓扑，该协议提供了四大功能:

在 HA 群组成员之间镜像配置，在发生故障切换时确保正确的行为。

可以在 HA 群组中维护所有活动会话和 VPN 隧道。

故障切换算法根据系统健康状态确定哪个系统是主系统，把状态与相邻系统连接起来或监控从相邻系统直到远程系统的路径。

故障检测和切换到备用单元可以在不到六秒内完成，而不管活动会话和 VPN 隧道的数量有多少。

NetScreen-ScreenOS 允许虚拟主机公司和企业为客户和贸易合作伙伴简便地建立安全边界，进而实现企业外部网 VPN。虚拟主机现在可以使用基于 NAT（网络地址转换）的技术，接收和区分各个客户的流量。这样，尽管另一个客户可以使用某个客户的专用网络地址，而流量仍可以进入一台或多台服务器。它运用安全策略，把每个客户的地址转换成中央 NetScreen 设备可以识别的不同地址，来实现这一过程。

模块化：NetScreen 系统采用模块化设计，允许定制配置和实现额外的可靠性。所有系统都提供了冗余交流或直流电源可以拆卸的风扇模块。NetScreen-1000 还配有多个处理板，提高了冗余性和性能。NetScreen-500 提供了两类接口模块和四个接口模块托架，提高了系统配置水平。

全方位管理：NetScreen 的安全系统包括强健的管理支持，允许网络管理员管理设备。由于 VPN 功能是内置的，因此可以对所有管理加密，从而实现真正的安全远程管理。

采用 NetScreen-Global Manager 或 NetScreen-Global PRO 实现菜单驱动的中央站点管理*。

通过内置 Web UI（HTTP 和 HTTPS）实现基于浏览器的管理。

通过 SSH、Telnet 和控制台端口进入命令行界面（CLI）。

电子邮件告警、SNMP 告警。

与 Syslog 或 WebTrends 相集成，实现外部登录、监视和分析。

为最多 20 个管理员提供 3 种访问权限：根管理、管理和只读。

便于安装：所有 NetScreen 系统在设计时都考虑了安装需求。它提供了所有架装设备，同时可以配置声音和可视告警，帮助现场技术人员监控设备状态。

NetScreen 产品是基于安全处理器的产品。全新的技术包括定制的专有的芯片免费加盟和策略实现。高性能的多总线体系结构、内嵌的高速 RISC CPU 和专用软件。

NetScreen 防火墙的专用 ASIC 芯片提供存取策略的功能。该功能以硬件方式实现，它比软件防火墙有着无可比拟的速度优势。CPU 可以专门负责管理数据流。(策略存取执行防火墙保护和加密解密功能)。由于做到了系统级的安全处理功能。NetScreen 消除了基于 PC 平台的防火墙的需管理多个部件所引起的性能下降的瓶颈。

NetScreen 提供了多功能和高安全性能的无缝连接。

另外，该产品允许用户在远程实现加密通信，并且这种 VPN 功能不影响性能。允许他们在自己的企业内部构筑安全体系。

NetScreen 产品动态加密保护和按优先级实时监控未来数据，它专有的独特的系统设计保证了它的高性能，ASIC 芯片可以独自处理并过滤包。先进的多总线结构比基于 PC 的平台上的防火墙产品快。同样基于系统级的安全功能设计消除了传输的瓶颈。

NetScreen 支持高性能的存取为每一个当前用户，无论是远程还是在防火墙内，支持创纪录的并行连接用户数。NetScreen-1000 创纪录地实现了 TCP/IP 并发连接(超过 500000)；策略数(多于 4000)和并发的 VPN 连接数(超过 20000)。

所有产品都支持超过 4000 个存取策略，并提供简单易用的过滤界面。

NetScreen 全功能防火墙包括了包过滤、代理服务器和动态线路级过滤器。该产品提供了高级的数据包检查和事件日志功能。

NetScreen 会集了 VPN 功能，保证了数据在传输过程中的加密和解密，但在数据被加、解密之前，首先要满足预定的策略。

NetScreen 支持业界的加密标准。包括网络密钥交换(IKE, 或以前的 ISAKMP) 通过 IP, DES, Triple DES。并且还支持数据签名(MD5)算法。NetScreen 将支持 X.509 认证公钥算法 (PKI), 可以自动地管理 VPN。

NetScreen-1000 建立了新的 VPN 性能测试基准，与其它同类产品比较，NetScreen-1000 有着更高的吞吐量，更广泛的安全性和更低的价位。

流量管理提供给网络管理员必须的信息去监控和管理网络流量。网络控制功能像带宽分配。流量优先级和负载均衡，使该产品成为 web 服务器和 ISP 的理想产品。

该产品易于安装，而且 NetScreen 产品可以远程通过网络上任何一台具有浏览器的机器来管理。

NetScreen 使用了状态检查的方法来实现动态的包过滤。这种方法也同样被其他重要的防火墙厂商 CheckPoint 和 Cisco 所采用。相比其他的两种方法简单的包过滤和复杂的应用网关来讲，它具有更快速和更安全的优点。

简单的包过滤只检查 IP 地址和端口号。它通常由路由器来实现。但它只能做到拒绝端口访问或允许端口访问。它不能了解连接的状态。一旦真正的用户完成了 TCP 的连接后，就留下了可使黑客劫持端口号的漏洞。

应用网关通过检查应用层所有的包，提供了更好的安全性。但是用户需要厂商提供所有应用的代理。而且它只能用软件实现，因此性能是很低的。

状态检查的链路层代理，另一方面，可实现硬件层。防火墙保持所有的 TCP 会话的检查。一旦一个会话结束，防火墙就结束这个连接。在不牺牲安全性的条件下，提供更高的性能。

NetScreen 也可提供网络层的 URL 过滤，并在不久的将来实现病毒扫描的功能。

NetScreen 产品也提供信息的和用户的认证。NetScreen 是通过建立 VPN 通道，由 MD5 实现的 ESP 信息的认证，并依从 IPSec 标准

用户的认证可由两种方法实现。用户可在防火墙上定义多达 2000 用户或者设置一个 Radius 服务器来存储用户认证的信息。

NetScreen 产品可连接信任端口（Trusted ）或 不信任端口（Untrusted）

然后通过web 界面来管理。并提供了跨 Internet 来实现远程管理能力。不信任端口（Untrusted）可以因安全的原因而设置为取消。如果取消它，不信任端口是不可 ping 的。(不信任端口(untrusted）在 1.60 版本以前是不可 ping 的)。

NetScreen 产品同样也可通过 console 端口，使用命令行方式进行管理。如果用户喜欢使用命令行方式或希望通过远程来管理防火墙,可在 console 口连接一个调制解调器。Console 口的访问也可因为安全原因设置为取消。

NetScreen 产品也可以通过 telnet 来管理。Telnet 和 Web 管理也可通过 VPN 通道加密，提供安全的管理。

管理方便，可通过串口管理，使用命令行方式。也可以在图形方式下用浏览器进行管理，不分硬件平台和操作系统，只要把浏览器打开就可以通过用 Web server 的方式来管理.配置简单尤其在配置三个端口的 IP 时很方便对于大型网络中多个 NetScreen 设备，可以采用 SNMP 的集中式管理，通过网络管理软件，如 Sun Net Manager 来进行管理. 而且 NetScreen 还可以提供备份的远程拨号方式的管理不仅如此，为安全起见，NetScreen 可以关闭远程的管理方式，而只使用本地的、安全的管理方式。

5.5.2.4 NetScreen-204& NetScreen-208

我们在产品选型上，分别选用了NetScreen-204和NetScreen-208的两款防火墙。

之所以选用NetScreen-204和NetScreen-208防火墙进行安全防护是基于以下原因:

NetScreen-204可以实现高达400 Mbps的防火墙吞吐量、200 Mbps的3DES VPN吞吐量，支持1,000条IPSec隧道及最多128,000个并发会话。而NetScreen-208可以实现高达550 Mbps的防火墙吞吐量、200 Mbps的3DES VPN吞吐量，支持1,000条IPSec隧道及最多128,000个并发会话。对于系统来说NetScreen-204和NetScreen-208的处理能力都很强，一台NetScreen-204或者NetScreen-208就会满足系统的应用需求（包括并发访问能力、实时性等），如采用NetScreen-208单从处理能力这方面来说会更好。

该防火墙所处的位置是系统的一个核心位置，为了避免单点故障，建议采用冗余结构。而NetScreen-208这款防火墙设备价格超过NetScreen-204防火墙，如

果采用NetScreen-208防火墙可以提供多于NetScreen-204防火墙4个独立端口。

所以我们在系统采用了一台NetScreen-204作为防火墙的具体标准配置方式。

产品概述

NetScreen-204是目前市场上功能最多的防火墙产品，可以方便地集成在许多不同的网络环境中，包括大中型企业的办公室，电子商务网站，数据中心和电信运营基础设施。它具有4个自适应10/100M以太网端口，延续了NetScreen防火墙优秀能力(400Mbps)--即使在对系统资源要求极高的应用中（诸如VPN-3DES加密）也能保持超过200Mbps的速率。

多个可灵活配置的端口

具有4个以太网端口，可以适应任何网络环境的要求，在改变了简单的内、外部网络安全区域划分后NS-200系列具有更高的安全水准，现在可以用设备具有的多个端口把网络划分成多个区域，更有效地把需要保护的特别区域与潜在威胁分离开来。

在每个端口上都可以设置防火墙保护策略

所有的端口都可防止拒绝服务式攻击和其他攻击，可以针对来自于外部和内部的攻击提供安全保护措施。每个端口都可配置针对28种攻击手段的保护策略，以便在当今不断变化的网络中增加安全防护的机动灵活性并提高了安全系数。

VPN通道可以设置在各个端口

NetScreen-204防火墙系列可以把各个端口设置为遵守IPSec协议的VPN通道的起点或终点，从而搭建功能更强的VPN网络。这个功能一个最典型的应用就是在无线局域网中：把防火墙的内部端口设为VPN通道的终点，使无线网络中的内部通讯信息得以加密而不被外界破译。NetScreen整合网络安全产品把防火墙功能和用户认证服务结合在一起，可以锁定那些没有经过授权的网络访问，并且在无线网络的通讯中通过加密提供信息的保密。

集中星型的(hub-and-spoke)

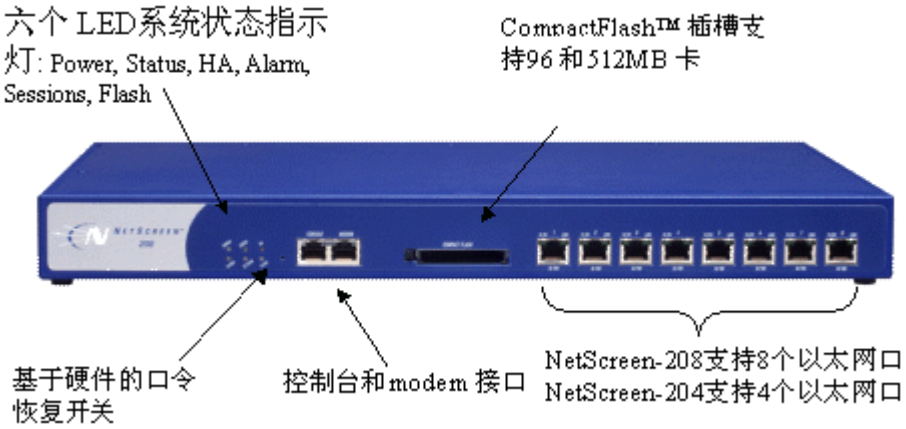
NetScreen-204适合部署集中星型(hub and spoke)VPN网络的中央站点。用户不需要为每个远程站点之间单独建立VPN通道，只需在远程和中央站点设立一个VPN通道，让中央站点把网络流量导引到正确的远程站点。NetScreen-204具有高度VPN容量和处理性能，可以更容易实现上述功能。

VPN高可用性（冗余设备）

NetScreen-204支持高可用性(HA)，维护所有对话同步，包括IPSec的安全联盟(SAs)。由于所有会话和IPSec SA都在设备之间被保存和维护，因此当主系统切换到备份系统时不会发生网络中断。

NetScreen-204防火墙系统特性-技术参数

5.5.2.5 防火墙的具体配置



其中:

产品概述

NetScreen-208是目前市场上功能最多的防火墙产品，可以方便地集成在许多不同的网络环境中，包括大中型企业的办公室，电子商务网站，数据中心和电信运营基础设施。它具有8个自适应10/100M以太网端口，延续了NetScreen防火墙优秀能力(550Mbps)--即使在对系统资源要求极高的应用中（诸如VPN-3DES加密）也能保持超过200Mbps的速率。

多个可灵活配置的端口

具有8个以太网端口，可以适应任何网络环境的要求，在改变了简单的内部和外部区域划分后NS-200系列具有更高的安全水准，现在可以用设备具有的多个端口把网络划分成多个区域，更有效地把需要保护的特别区域与潜在威胁分离开来。

在每个端口上都可以设置防火墙保护策略

所有的端口都可防止拒绝服务式攻击和其他攻击，可以针对来自于外部和内

部的攻击提供安全保护措施。每个端口都可配置针对28种攻击手段的保护策略，以便在当今不断变化的网络中增加安全防护的机动灵活性并提高了安全系数。

VPN通道可以设置在各个端口

NetScreen-208防火墙系列可以把各个端口设置为遵守IPSec协议的VPN通道的起点或终点，从而搭建功能更强的VPN网络。这个功能一个最典型的应用就是在无线局域网中：把防火墙的内部端口设为VPN通道的终点，使无线网络中的内部通讯信息得以加密而不被外界破译。NetScreen整合网络安全产品把防火墙功能和用户认证服务结合在一起，可以锁定那些没有经过授权的网络访问，并且在无线网络的通讯中通过加密提供信息的保密。

集中星型的(hub-and-spoke)

NetScreen-208适合部署星型(hub and spoke)VPN网络的中央站点。用户不需要为每个远程站点之间单独建立VPN通道，只需在远程和中央站点设立一个VPN通道，让中央站点把网络流量导引到正确的远程站点。NetScreen-208具有高度VPN容量和处理性能，可以更容易实现上述功能。

VPN高可用性（冗余设备）

NetScreen-208支持高可用性(HA)，维护所有对话同步，包括IPSec的安全联盟(SAs)。由于所有会话和IPSec SA都在设备之间被保存和维护，因此当主系统切换到备份系统时不会发生网络中断。

5.5.2.6 防火墙的连接方式

在本方案中，分别选用的两台 NetScreen-500ES 以及与网络交换设备的连接方式如下图所示

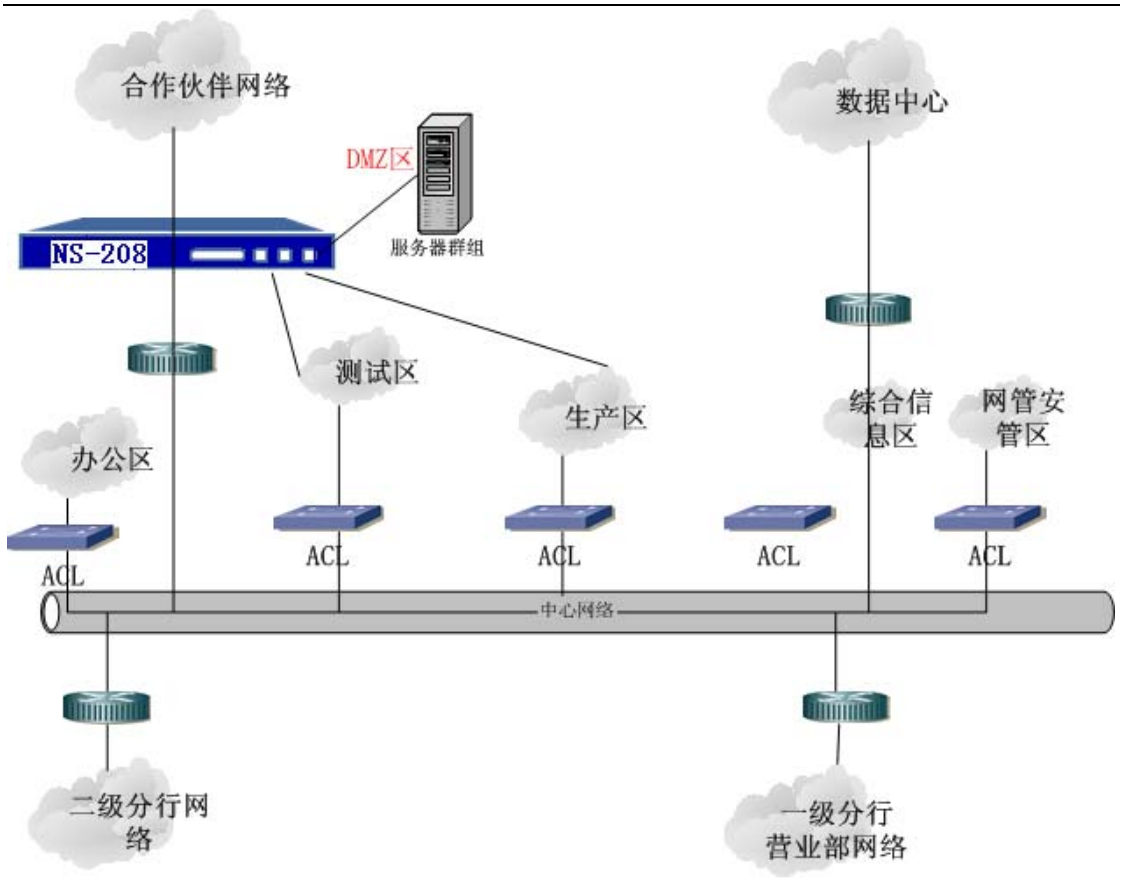


图 4.1 一级分行网络安全设计总图

第六章 剩余风险分析

本次安全方案只是对两个高风险的边界进行了安全防护设计，分别是“服务器群组、测试区、生产区”和“办公区、数据中心、综合信息区、网管安管区”，而其他边界没有采取任何安全防护措施，现在我们对安全设计后的网络进行剩余风险分析。

6.1 安全域边界的剩余风险分析

从前面安全域的分析中可以看到:

1. 合作伙伴网络与服务器群组之间有防火墙，所以目前这两个边界处的风险等级是中级。

2. 合作伙伴网络与生产区之间有防火墙，所以目前这两个边界处的风险等级是中级。

3. 合作伙伴网络与测试区之间有防火墙，所以目前这两个边界处的风险等级是中级。

4. 合作伙伴网络与办公区、数据中心、综合信息区、网管安管区之间有防火墙，并且访问方向是单向的，也就是，合作伙伴网络不能够直接访问办公区、数据中心、综合信息区、网管安管区的区域，所以目前这两个边界处的风险等级是高级。

5. 服务器群组、测试区、生产区与办公区、数据中心、综合信息区、网管安管区之间有防火墙的保护，所以目前每两个边界处的风险等级是高级。

6. 办公区、数据中心、综合信息区、网管安管区之间没有防火墙的保护，所以目前每两个边界处的风险等级是低级。

6.2 网管安管区子系统

工商银行一级安全网络是由多个不同安全级别的安全域，为了保证企业内部网络的安全性，在风险等级相对高的边界处设立相应的防火墙系统。这个分散的防火墙系统的设置和管理就显得非常重要，因为它某一处的漏同将影响整个工商银行一级网络 Intranet 的安全性。

6.3 木马程序的剩余风险分析与建议

由于新型木马程序在被入侵、感染的主机上作为客户端向外发送数据，而且使用的端口也是 HTTP 的合法端口（80），因而防火墙和 HTTP 代理服务器也无法识别这种攻击。

建议：加强防病毒的措施，及时对被感染的主机进行清除。

第七章 安全服务

建立网络安全保障体系不能仅仅依靠现有的安全机制和设备，更重要的是提供全方位的安全服务。网络安全不是几种安全产品的集合，它作为一项系统工程已经形成了自己的专业体系，没有先进科学的知识结构很难对此进行全面细致的把握；网络安全系统存在固有弱点，即使最微小的安全漏洞都可能引发整个网络

的崩溃；同时网络安全处在信息产业飞速发展的大环境下，现有的系统安全只是暂时的、静态的，所有这些问题都必须通过持续全面的安全服务来解决。完善的安全服务应包括全方位的安全咨询，整体系统安全的策划、设计，优质的工程实施、细致及时的售后服务和技术培训。除此之外，定期的网络安全风险评估，帮助客户制定特别事件应急响应方案扩充了安全服务的内涵。

7.1 技术支持体系

7.1.1 技术支持模式

本公司的技术支持模式包括两个方面:

- 直接的一线服务

向最终用户提供直接的一线服务，为用户提供技术咨询、方案设计与论证、现场安装服务以及售后服务。

- 二线技术支持

由于客观原因我们无法在规定的时限内将用户的问题确诊或解决时，我们会及时地向 NetScreen TAC 开 Case，由 NetScreen 技术支持中心进行技术支持，并最终负责排除用户网络故障。

7.2 工程实施方案

7.2.1 工程实施服务

工程实施服务是指本公司工程服务部地工程技术人员现场进行网络安装工作，具体包括如下工程内容:

1. 系统准备阶段

目的: 制定网络工程的具体任务，为系统工程的具体实施提供前期准备。

工作内容: 详细了解用户需求，对用户的网络应用情况做全面调研。为网络详细的方案设计提供依据。主要内容包括:

- 组织召开项目协调会
- 机房现场勘查和准备
- 工程实施方案的设计及审订
- 相关网络设备和线路的调整
- 确定实施的组织结构及其职责
- 确定工程实施进度

2. 详细网络方案技术实施规范

目的：形成详细的网络方案技术实施规范。

工作内容：优化网络设备配置。

3. 网络技术培训阶段

目的：充分利用合同签订到设备到货这段时间，通过专业培训，使系统管理人员熟悉将来的软硬件环境，提高工作效率，确保工作质量。

工作内容：通过教师讲解、上机操作辅导，使用户网络技术人员建立起网络技术基础知识，并且逐步积累网络安装与维护的经验。

注：NetScreen 公司可以为用户提供基础课程和高级别课程。选用的初级教材是《Implementing NetScreen Security Solution》(INSS)，高级教材是《NetScreen Management Troubleshooting and Performance-tuning》(NMTP)。设备采用用户部分到货设备或我公司 Demo 设备。

4. 现场环境准备

目的：保证客户现场条件符合网络实施要求，以保障后续工作顺利进行。

工作内容：由我公司网络工程师配合用户对网络中心现场场地条件进行测试。

在网络设备安装前，用户应为我公司的有关技术实施人员提供必要工作条件。网络设备的安装在下面几项工作完成后进行。

- 现有线缆布局和配线排布局
- 设备安装地建筑物强度（机房承重能力）

- 电路设备状况
- 机架空间和可以利用机架状况
- 电源能力和地线排布局
- 用户对设备安装所能提供的具体支持（设备支持、人力支持、管理支持、技术支持、等等）
- 具体设备安装构想和方式等等。

5. 整体工程网络设备到货验收

目的：对设备进行检验是否符合要求。

工作内容：合同设备完成通关和外包装验收之后，将会运抵工商银行分行安装地点，我公司网络工程师将在有关人员的监督下严格按照设备的验收标准对设备进行验收，如果发现设备存在型号不符、设备损坏、测试不正常、资料不全、缺少配件等影响工程实施的设备问题时，将立即给予圆满解决。设备验收清单参考设备订货合同。验收报告双方签字确认。

6. 硬件系统安装调试

目的：实现数据中心和各分支机构的网络连接。

工作内容：在现场环境准备充分后，由本公司网络工程师负责设备的安装与调试。针对网络的特点，本公司将派出最优秀的项目管理人员和技术工程实施队伍，与用户的技术人员组成专业项目组，协调资源，保证工程的顺利进行。 具体实施步骤：

- 进行回退和应急方案设计及可行性分析
- 设备上架
- 上线前准备和测试
- 具体实施

7. 网络的测试和联调

目的：检验对网络进行初步验收和测试。

工作内容：网络安装调试完成后，我们与用户一道对网络进行上线后的单系统的安全策略测试、业务流测试等。验收合格后，由用户填写网络验收报告。上线后的测试内容一般包括：

- 网络连通性
- 防火墙策略正确性
- 相关业务和应用

8. 网络试运行阶段的维护

目的：检验网络的实际运行是否符合要求。

工作内容：对网络进行三个月的试运行，检验其可靠性、安全性等，其间不断调整完善直至完全正常运行。同时考核应用软件的效率，必要时调整设备参数，以适应应用软件的有效运行。同时进行免费的现场技术培训，目的是逐步将网络工程中的技术细节和维护方式转交给用户的技术人员。

9. 系统最终验收

目的：对于系统进行最终验收测试，评定项目，形成项目文档。

工作内容：网络实际运行测试

10. 故障处理

对于用户的任何技术问题，我公司提供远程故障诊断、技术支持以及必要的现场技术支持。现场技术支持包括：

- 现场备件更换
- 现场操作系统升级
- 现场故障诊断、排除
- 现场设备替代

当用户网络出现严重故障，业务无法正常进行时，我们可以派遣工程师，携带必要的设备、工具，到用户现场排除故障，恢复网络运行。

11. 产品备件保修服务

NetScreen 的硬件防火墙产品提供一年的免费保修。

如果确认设备出现硬件故障，我们会为用户提供完善正规的返修服务。

12. 培训服务

针对网络技术人员，我公司提供多种网络安全技术培训课程，供用户客户选择，初级培训和高级培训。

13. 系统运行技术咨询服务

不管是在保修期内，还是在保修期外，我公司免费为客户提供技术咨询服务，这其中包括：新技术咨询、网络配置调整、故障解决等。我们的热线电话常年 24 小时开放，随时随地解答客户的技术询问。

7.2.2 工程实施质量保证体系

工商银行分行网络安全项目是一个非常重大的项目，我公司将按照公司 ISO9001:2000 的质量管理体系要求，结合项目实施管理方法论，严格控制该项目的工程质量。

一、工程管理组织

我公司对每个重大项目都相应配备了一名工程监理，工程监理一般对负责项目有一定的工程技术及管理经验，由公司资深具有吩咐工行网络实施经验的工程师或质量管理部成员承担，同时以项目变化需要，可以增加监理助理，配合工程监理同时监督工程的执行。

二、管理方法

1、项目经理提交所有项目实施计划、技术文档，要得到项目监理的审核批准，形式 E-mail 电子邮件通知方式

2、实施各阶段实施前，项目经理应通知项目监理检查前一阶段的实施符合计划要求，才可进入下一步骤，以项目管理日志记录方式

3、重大质量事故或隐患，质量监理有权组织协调会议，甚至要求客户停止或修改方案，撤换责任人，以会议纪要的方式

4、任何计划的修改，方案的改动，都必须得到质量监理的审核批准，以 E-mail 通知的方式

5、项目监理对于项目的隐患、事故，根据责任方，开出“纠正与预防处理单”，同时跟踪纠正措施的执行，公司质量管理部备案

三、预防纠正措施

我公司的工程监理对工程实施过程输出的信息应进行识别。当出现问题时将由工程监理负责在《纠正和预防措施处理单》中填写不合格事实内容，并确定责任部门和项目组；交责任部门和项目分析问题原因和制订纠正措施并实施，工程监理负责跟踪实施后的效果。

7.3 事件及故障处理

7.3.1 故障级别定义

我们将用户故障分为四个等级:

编号	故障级别	故障现象
P1	一级故障	现有的安全设备停机，或对最终用户的业务运作有严重影响
P2	二级故障	现有安全设备的操作性能严重下降，或由于网络性能明显下降，对最终用户的业务运作有重要影响
P3	三级故障	安全设备的操作性能受损或个别设备故障，只影响局部，不影响全局业务
P4	四级故障	安装、配置等技术难点，业务不受影响

根据对故障级别的定义，我们工程师将在严格规定的时限内，对客户进行响应和故障处理。

故障级别	电话响应	规定时限
P1	<1 小时	< 6 小时
P2	<1 小时	< 3 天
P3	<1 小时	< 5 天
P4	<1 小时	< 10 天

我公司的网络工程师将随时远程连接支持,或在服务期内的提供快速的现场支持。

7.3.2 事件处理流程

我们公司将事件的处理过程分为七个部分，包括:

1、合法性检查

2、事件的建立与分发

3、1小时回复及提醒

4、事件的处理

5、事件的升级处理过程

6、事件的查询处理

7、事件的关闭及归档

第八章 附件一 NetScreen公司简介

NetScreen Technologies Inc.以业界领先的防火墙/虚拟专用网络 (VPN) 解决方案，显着加强互联网的安全能力。NetScreen 的突破性 ASIC 安全解决方案，实现接近联机速度的数据包处理，并能充分利用其带宽，避免了其它传统安全产品所出现的瓶颈问题。

NetScreen 之全面化产品包括多种为不同应用而设计的解决方案，上至专为互联网数据中心和服务供应商设计的业界第一个千兆比特級安全系统 NetScreen-1000，下至为单一远程办公者而设计的解决方案 NetScreen-5。NetScreen 安全系统和设备之管理操作经由 NetScreen-Global PRO 进行，这是一个高可扩展的软件平台，方便系统之建置、执行和网络管制。

市场背景

目前市场上对安全、高成本效益、高性能网络连接的需求大大提升。随着互联网使用量以高速增长，防止网络受到外来攻击和保障通信隐私的需求亦不断增加。现时业界对此问题的讨论重点已经不再是围绕是否需要防火墙或 VPN，而是如何可更好地采用这些技术。NetScreen 产品不但符合多项业界安全和加密标准，而且比较其它品牌的产品更胜一筹，优点在于：入门产品的成本效益及使用简易性；以及高端产品的管理能力和性能表现。

最普遍的国际互联网的安全解决方案是防火墙和 VPN。防火墙是业界最常用的互联网的安全解决方案，可防止非法入侵者存取数据并且限制未经授权用户进入网络；而 VPN 则可保证经公共网络连接的两个或多个连接点 (如公司的不同办事处) 之间安全、专有的通信。

防火墙和 VPN 解决方案过往是以基于服务器的软件应用程序推行的，与网络业初期路由功能以软件形式提供的情形大致相同。不过，这种软件解决方案却会引致多方面的瓶颈问题。首先，最严重的问题在于计算器本身的设计并非用于处理网络信息或网络传输。

在低速传输情况下，这种软件解决方案确实还能操作良好。然而，随着互

联网连接速度的大幅度提升，通过数字用户线(DSL)、线缆调制解调器(cable modem)、T1/E1和 T3/E3线路及更高速的连接，这种软件的解决方案却变成了主要瓶颈（由于安全解决方案阻塞网络的传输，导致客户只可用到部分所购买的连接带宽。基于个人计算机的解决方案，另一个潜在问题是方案本身难以抵御网络受破坏/入侵。此外，现有复杂的软件配置也是一个问题，特别是易用性和管理方面。因此，企业客户开始急于寻找其它解决方案，在性能和透明度方面能够迎合宽带数据连接的需求。这种趋势的转变，正如过往由基于软件的网络路由器和交换机过渡到为用户定制的硬件设备。

在企业市场以外，安全解决方案的需求更为复杂。亚洲电讯行业目前正处于巨变时期，由于市场开放加上需求大幅上升，竞争的激烈程度亦不断提升，导致现今服务供应商的商业模式发生了彻底的改变。许多供应商正通过其安全管理服务或将安全作为所提供服务的一部分的方式，藉此开拓更多的收入来源和发挥品牌竞争优势。互联网公司和业务迈向网絡化的传统企业等电子商务企业也要面对自身的系統安全问题。以下为这些市场对网络安全的部分需求的扼要说明：

电子商务：安全解决方案在容许网站供外界存取的同时，亦必须保障内部的数据库资料，或为地域上分散的服务器之间进行网站内容拷贝时提供安全的连接和远端管理。

网站寄存和服务器跨域管理设施：由于网站寄存或服务器跨域管理设施可以为电子商务客户提供的高速基建设施，讓他們更能快速响应其网上客户的查询，因此他们愈来愈倾向于将其网站服务器存放于这些设施内。这些服务供应商可转售防火墙和 VPN 技术给电子商务客户，或者提供安全服务，代客户操作和控管安全技术。常见的受控服务包括以下三种：单纯的防火墙服务（传统的单一防火墙由具备防火墙功能的安全网絡所取代；单纯的 VPN 服务（采用安全的 VPN 连接会代替广域网絡设备，而毋需采用帧中继(frame-relay)或 T1/E1 的连接；而集成防火墙和 VPN 服务则将两种应用方案相结合。

应用服务供应商：应用服务供应商(ASP) 模式即将基于集中寄存的应用软件经互联网的安全传送到客户的网站。这些应用服务供应商需要经过 IPSec VPN 信道

为客户的网站提供安全连接。

可控安全供应商(ASP)：可控安全供应商的职责是代终端用户建置和管理安全技术。此类供应商包括为企业客户提供可控服务的增值转售商，以及分銷安全服务給其它服务供应商（如城域网、智能楼宇网絡和互联网服务供应商）的安全服务包销商；而服务供应商则向其终端用户提供零售的可控安全服务。

上述所有公司在安全性能和管理能力上所面对的问题，都远比一般企业为多。直至最近，众多公司仍被迫要使用由现有的企业级的安全产品「拼凑」出来的不完整解决方案。简言之，服务供应商需要提升安全的需求，以保护重要的客户数据，只有现在的解决方案却无法达到所需的性能和管理效力。

据 IDC 和 Infonetics 的统计显示，到二零零三年时，防火墙产品的全球销售额将增至十四亿美元，而 VPN 产品更高达三十三亿美元。为了抢占这个市场，新的解决方案必须具备高度严密的安全功能，并能充分发挥高速传输性能，同时可为电子商务企业提供低成本安装和运作，以及为服务供货商提供增值功能和出具保证的性能服务。

NetScreen 系列产品

NetScreen-1000: NetScreen-1000是业内性能最高、扩展能力最强的安全解决方案，也是唯一集成了防火墙和 VPN 功能于一身、同时具备千兆比特級性能的安全产品。NetScreen-1000的传输速率达一千兆比特、可同时处理五十万個並发 TCP 会话及二万五千个 IPSec 通道。该解决方案最优胜之处在于其多租户体系架构，可建立多至一百个虚拟系统，每个虚拟系统拥有自己的地址本、策略和管理的安全域。此外，NetScreen-1000还具备高可用性和备份的特点，包括在发生故障时透过自动复制设定，以及容易互换的电源供应器、风扇和插卡等，确保防火墙和 VPN 会话无间断的运作。

NetScreen-500: NetScreen-500针对公司企业面对防火墙和 VPN 不断俱增的需求，提供简易安装和管理的安全方案，同时更为他们节省整体之网絡行政和设备开支。NetScreen-500提供700Mbps 防火墙和250Mbps VPN 的传输性能，同时支援多至一万个 VPN 通道，以及拥有全面性的流量管理功能。该方案可支援多至二十五个拥

有独立安全域的虚拟系统，在组件设计上发挥高可用性和备份的特点。

NetScreen-200 系列： NetScreen-200 系列包括 NetScreen-204 和 NetScreen-208产品，两者的区别在于10/100兆以太网。它们是当今最通用的产品，可以轻松整合到不同的环境，其中包括大型至中型企业的办公室、电子商务网站、数据中心以及电信运营基础设施。NetScreen-200系列配备四到八个自适应就10/100Base-T 以太网商品，提供高效率的防火墙功能（NetScreen-208为550Mbps，而 NetScreen-204为400Mbps）。即使在3DES 加密的严苛应用上亦能提供高于200Mbps 的速率性能。

NetScreen-Global PRO: NetScreen-Global PRO 是一个专为服务供应商和大型企业而设之高度可扩展性安全管理平台，具备一个功能超卓的多层数据收集和储存架构。NetScreen-Global PRO 提供拖拉式(drag-and-drop)的简便功能，让系统管理员轻松地建立和修改 VPN，同時更拥有开放性的介面，能简易地支持第三方的管理工具。此平台提供预設定义、高性能的报告模板，让网絡主管人员可以轻易地建立特定的报告。

NetScreen-Global Manager: NetScreen-Global Manager 是专为企业和服务供应商而设，其强大功能可透过一个中央点对多个或复杂网站的网络进行安全控制。此方案可为多达一千组设备同时提供集中化配置和状态监控；网络动态的图表报告；以及所有 NetScreen 安全系统和设备的策略管理。

NetScreen-Remote: NetScreen-Remote 软件解决方案可让客户和 VPN 连接。该软件基于 IRE Inc.,的 IPSec 客户端软件。IRE Inc.，是 VPN 客户端软件主要供货商。

第九章 附 件 二 NetScreen-204& NetScreen-208 软硬件规格

9.1 NetScreen-204

NetScreen-204 产品外观

9.1.1 产品概述

NetScreen-204 是目前市场上功能最多的防火墙产品,可以方便地集成在许多不同的网络环境中，包括大中型企业的办公室，电子商务网站，数据中心和电信运营基础设施。它具有 4 个自适应 10/100M 以太网端口，延续了 NetScreen 防火墙优秀的接高速度处理能力(400Mbps)--即使在对系统资源要求极高的应用中（诸如 VPN-3DES 加密）也能保持超过 200Mbps 的速率。

9.1.2 多个可灵活配置的端口

具有 4 个以太网端口，可以适应任何网络环境的要求，在改变了简单的安全区域划分后 NS-200 系列具有更高的安全水准，现在可以用设备具有的多个端口把网络划分成多个区域，更有效地把需要保护的特别区域与潜在威胁分离开来。

9.1.3 在每个端口上都可以设置防火墙保护策略

所有的端口都可防止拒绝服务式攻击和其他攻击，可以针对来自于外部和内部的攻击提供安全保护措施。每个端口都可配置针对 28 种攻击手段的保护策略，以便在当今不断变化的网络中增加安全防护的机动灵活性并提高了安全系数。

9.1.4VPN 通道可以设置在各个端口

NetScreen-204 防火墙系列可以把各个端口设置为遵守 IPSec 协议的 VPN 通道的起点或终点，从而搭建功能更强的 VPN 网络。这个功能一个最典型的应用就是在无线局域网中：把防火墙的内部端口设为 VPN 通道的终点，使无线网络中的内部通讯信息得以加密而不被外界破译。NetScreen 网络安全产品把防火墙功能和用户认证服务结合在一起，可以锁定那些没有经过授权的网络访问，并且在无线网络的通讯中通过加密提供信息的保密。

9.1.5 集中星型的(hub-and-spoke)

NetScreen-204 适合部署在集中星型(hub and spoke)VPN 网络的中央站点。用户不需要为每个远程站点之间单独建立 VPN 通道,只需在远程和中央站点间架设一个 VPN 通道,让中央站点把网络流量导引到正确的远程站点。NetScreen-204 具有高度 VPN 容量和处理性能，可以更容易实现上述功能。

9.1.6 VPN 高可用性（冗余设备）

NetScreen-204 支持高可用性(HA)，维护所有对话同步，包括 IPSec 的安全联盟(SAS)。由于所有会话和 IPSec SA 都在设备之间被保存和维护，因此当主系统切换到备份系统时不会发生网络中断。

9.1.7 NetScreen-204 防火墙系统特性-技术参数

性能	并发会话: 128,000 每秒的新会话数: 13,000 防火墙性能: 400Mbps 三倍 DES(128 位): 200Mbps 策略: 4,000 时间表: 256 4 个自适应 10/100M Base-T 以太网口
工作模式	透明模式（所有端口）: 是 路由模式在所有端口: 是 NAT(网络地址转换)在所有端口: 是 基于策略的 NAT:是 PAT(端口地址转换): 是 虚拟 IP(Virtual IP):4 映射 IP(Mapped IP): 4,000 IP 路由--静态路由: 256 每个端口的用户数，信任端: 没有限制
IP 地址分配	静态: 均支持 DHCP client(动态 IP 分配):N/A PPPoE client:非信任端 内部 DHCP 服务器: 信任端 DHCP Relay:支持

防火墙攻击检测	同步攻击: 是 ICMP flood 检测:是 UDP flood 检测:是 检测死 ping(Ping of death):是 检测 IP 欺骗(IP spoofing):是 检测端口扫描(Port scan):是 检测陆地攻击(Land attack):是 检测撕毁攻击(Tear drop attack):是 过滤 IP 源路由选项(Filter IP source route option):是 检测 IP 地址扫描攻击(IP address sweep attack):是 检测 WinNuke attack 攻击:是 Java/ActiveX/Zip/EXE:是 默认分组拒绝(Default packet deny):是 Dos & DDoS 保护:是 用户定义的不良 URL: 48 Per-source session limiting:是 SYN fragments:是 Syn and Fin bit set:是 No flags in TCP:是 FIN with no ACK:是 ICMP fragment:是 Large ICMP:是 IP source route:是 IP record route:是 IP security options:是 IP timestamp:是 IP stream:是 IP bad options:是 Unknown protocols:是
VPN	专用隧道: 1,000 手工密钥、IKE、PKI(X.509) : 是 DES(56-bit)&三倍 DES(168bit)加密 encryption: 是 完全正向保密(DH 群组)Perfect forward secrecy(DH Groups): 1,2,5 防止回复攻击(Prevent replay attack): 是 远程接入 VPN(Remote access VPN): 是 L2TP within IPSec: 是 站点间 VPN(Site-to-site VPN): 是 集中星型 VPN 网络拓扑: 是 IPSec NAT Traversal: 是
IPSec	认证: SHA-1:是 MD5:是

	PKI 认证请求（PKCS 7& PKCS 10）：是 Automated certificate enrollment(SCEP)：是 Online Certificate Status Protocol(OCSP)：是 支持的证书服务器: Versign 认证中心:是 Entrust 认证中心:是 Microsoft 认证中心:是 RSA Keon CA 认证中心:是 iplanet(Netscape)认证中心:是 Baltimore 认证中心:是 DOD PKI 认证中心:是
防火墙和 VPN 用户 认证	内置（内部）数据库用户限额：1,500; RADIUS（外部）数据库：是; SA SecureID(外部)数据库：是; LDAP（外部）数据库：是;
流 量 管 理	有保障的带宽：适用 最大带宽：适用 优先使用带宽：适用 DiffServ 标记：适用
负 载 均 衡	轮询 Round robin：是; 加权轮询 Weighted round robin：是; 最少连接 Least connections：是; 加权最少连接 Weighted least connections：是;
高可用性(HA)	高可用性(HA)：是 防火墙和 VPN 会话保护：是 设备故障监测：是 链路故障监测：是 故障切换网络通知：是 新 HA 成员认证：是 HA 流量加密：是
系 统 管 理	网 址 浏览器 配 置 管 理（WebUI:HTTP and HTTPS）; 命令行界面--控制台（Command line interface:console, telnet）; 命令行界面(telnet); 安全命令外壳（兼容 ssh v1）Secure Command Shell(ssh v1 compatible); NetScreen Global Pro：在新版本的 Screens 发布后可实现; NetScreen Global Pro Express：在新版本的 ScreenOS 发

	布后可实现; 在任何借口上经过 VPN 通道可实现管理; SNMP 完全自定义 MIB
管理	多个管理员: 20; 远程数据库管理: RADIUS; 网络管理: 6; 根源管理、管理和只读三种用户权限(Root Admin,Admin,&Read Only user levels): 是; 软件升级和配置变动: TFTP/WebUI/Global
日志/监控	系统日志(Syslog):外部; 电子邮件(两个地址)E-mail(2 addresses):是; Web Trends:外部; SNMP:是; Traceroute:是; VPN 通道监视程序(VPN tunnel monitor): 是; Websense URL 过滤:外部
External Flash (外接存储卡)	CompactFlash: 96 或 512MB 可选 PCMCIA 闪存:无; 事件日志和告警(Event logs & alarms):是; 系统配置脚本(System config script):是; ScreenOS 软件(ScreenOS software):是
电源	AC(交流)电源: 90-264 可变 VAC(47 到 63Hz); 功率消耗: 45 瓦; DC(直流)电源: -36 to -72VDC, 功率消耗: 50 瓦
外 型 尺 寸	10.8 英寸(长) x 17.5 英寸(宽) x 1.73 英寸(高), 重量 7 磅
可堆叠	支持
支持的标准	ARP, TCP/IP, UDP, ICMP, HTTP, RADIUS, IPSec (IPESP), MD5,SHA-1, AES, DES, 3DES, IKE (ISAKMP), TFTP (client), SNMP,X.509v3, DHCP, PPPoE
安全标准认证	安全认证: FCC, UL, CE, CUL, C-Tick, VCCI, BSMI, CSA
工作环境温度	5-40°C(40 到 105F)
湿度	5%-90%, 无冷凝
平均故障间隔时间 (Bellcore model)	6.8 年

9.2 NetScreen-208

NetScreen-208 产品外观

9.2.1 产品概述

NetScreen-208 是目前市场上功能最多的防火墙产品,可以方便地集成在许多不同的网络环境中，包括大中型企业的办公室，电子商务网站，数据中心和电信运营基础设施。它具有 8 个自适应 10/100M 以太网端口，延续了 NetScreen 防火墙优秀的线速能力(550Mbps)--即使在对系统资源要求极高的应用中（诸如 VPN-3DES 加密）也能保持超过 200Mbps 的速率。

9.2.2 多个可灵活配置的端口

具有 8 个以太网端口，可以适应任何网络环境的要求，在改变了简单的安全区域划分后 NS-200 系列具有更高的安全水准，现在可以用设备具有的多个端口把网络划分成多个区域，更有效地把需要保护的特别区域与潜在威胁分离开来。

9.2.3 NetScreen-208 防火墙系统特性-技术参数

(*注意: 所有的功能特性可以在 ScreenOS3.1.0r1 上实现，在低版本的 ScreenOS 中有一些功能不支持)

能	并发会话: 128,000 每秒的新会话数: 13,000 防火墙性能: 550Mbps 三倍 DES(128 位): 200Mbps 策略: 4,000 时间表: 256 8 个自适应 10/100M Base-T 以太网口
工作模式	透明模式（所有端口）: 是 路由模式在所有端口: 是 NAT(网络地址转换)在所有端口: 是 基于策略的 NAT:是 PAT(端口地址转换): 是 虚拟 IP(Virtual IP):4 映射 IP(Mapped IP): 4,000 IP 路由--静态路由: 256 每个端口的用户数，信任端: 没有限制

IP 地址分配	静态: 均支持 DHCP client(动态 IP 分配):N/A PPPoE client:非信任端 内部 DHCP 服务器: 信任端 DHCP Relay:支持
防火墙攻击检测	同步攻击: 是 ICMP flood 检测:是 UDP flood 检测:是 检测死 ping(Ping of death):是 检测 IP 欺骗(IP spoofing):是 检测端口扫描(Port scan):是 检测陆地攻击(Land attack):是 检测撕毁攻击(Tear drop attack):是 过滤 IP 源路由选项(Filter IP source route option):是 检测 IP 地址扫描攻击(IP address sweep attack):是 检测 WinNuke attack 攻击:是 Java/ActiveX/Zip/EXE:是 默认分组拒绝(Default packet deny):是 Dos & DDoS 保护:是 用户定义的不良 URL: 48 Per-source session limiting:是 Syn fragments:是 Syn and Fin bit set:是 No flags in TCP:是 FIN with no ACK:是 ICMP fragment:是 Large ICMP:是 IP source route:是 IP record route:是 IP security options:是 IP timestamp:是 IP stream:是 IP bad options:是 Unknown protocols:是
VPN	专用隧道: 1,000 手工密匙、IKE、PKI(X.509) : 是 DES(56-bit)&三倍 DES(168bit)加密 encryption: 是 完全正向保密(DH 群组)Perfect forward secrecy(DH Groups): 1,2,5 防止回复攻击(Prevent replay attack): 是 远程接入 VPN(Remote access VPN): 是 L2TP within IPSec: 是 站点间 VPN(Site-to-site VPN): 是 集中星型 VPN 网络拓扑: 是

	IPSec NAT Traversal: 是
IPSec	认证: SHA-1:是 MD5:是 PKI 认证请求（PKCS 7& PKCS 10）: 是 Automated certificate enrollment(SCEP): 是 Online Certificate Status Protocol(OCSP): 是 支持的证书服务器: Versign 认证中心:是 Entrust 认证中心:是 Microsoft 认证中心:是 RSA Keon 认证中心:是 IPlanet(Netscape)认证中心:是 Baltimore 认证中心:是 DOD PKI 认证中心:是
防火墙和 VPN 用户 认证	内置（内部）数据库用户限额: 1,500; RADIUS（外部）数据库: 是; SA SecureID(外部)数据库: 是; LDAP（外部）数据库: 是;
流 量 管 理	有保障的带宽: 适用 最大带宽: 适用 优先使用带宽: 适用 DiffServ 标记: 适用
负 载 均 衡	轮询 Round robin: 是; 加权轮询 Weighted round robin: 是; 最少连接 Least connections: 是; 加权最少连接 Weighted least connections: 是;
高可用性(HA)	高可用性(HA): 是 防火墙和 VPN 会话保护: 是 设备故障监测: 是 链路故障监测: 是 故障切换网络通知: 是 新 HA 成员认证: 是 HA 流量加密: 是
系 统 管 理	网 址浏览器 配 置 管 理（WebUI:HTTP and HTTPS）; 命令行界面--控制台（Command line interface:console, telnet）; 命令行界面(telnet);

	NetScreen Global Pro: 在新版本的 ScreenOS 发布后可实现; NetScreen Global Pro Express: 在新版本的 ScreenOS 发布后可实现; 在任何借口上经过 VPN 通道可实现管理; SNMP 完全自定义 MIB
管理	多个管理员: 20; 远程数据库管理: RADIUS; 网络管理: 6; 根源管理、管理和只读三种用户权限(Root Admin, Admin, &Read Only user levels): 是; 软件升级和配置变动: TFTP/WebUI/Global
日志/监控	系统日志(Syslog):外部; 电子邮件(两个地址)E-mail(2 addresses):是; Web Trends:外部; SNMP:是; Traceroute:是; VPN 通道监视程序(VPN tunnel monitor): 是; Websense URL 过滤:外部
External Flash (外接存储卡)	CompactFlash: 96 或 512MB 可选 PCMCIA 闪存:无; 事件日志和告警(Event logs & alarms):是; 系统配置脚本(System config script):是; ScreenOS 软件(ScreenOS software):是
电源	AC(交流)电源: 90-264 可变 VAC(47 到 63Hz); 功率消耗: 45 瓦; DC(直流)电源: -36 to -72VDC, 功率消耗: 50 瓦
外 型 尺 寸	10.8 英寸(长) x 17.5 英寸(宽) x 1.73 英寸(高), 重量 7 磅
可堆叠	支持
支持的标准	ARP, TCP/IP, UDP, ICMP, HTTP, RADIUS, IPSec (IPESP), MD5, SHA-1, AES, DES, 3DES, IKE (ISAKMP), TFTP (client), SNMP, X.509v3, DHCP, PPPoE
安全标准认证	安全认证: FCC, UL, CE, CUL, C-Tick, VCCI, BSMI, CSA
工作环境温度	5-40°C(40 到 105F)
湿度	5%-90%, 无冷凝
平均故障间隔时间 (Bellcore model)	6.5 年