第 1 章 chapter 1

网络安全规划

随着计算机应用的日益普及，网络已经成为大多数企业的重要组成部分，许多常规办公应用已经开始转向网络，例如企业办公、视频会议、合作伙伴沟通等。随之而来的网络安全问题，也就成为制约企业生存与发展的命脉。网络安全建设的总体思路是：以信息资产为核心，以安全战略为指导，根据安全需求逐步完善安全基础设施，为网络应用提供安全能力支持。

1.1 项目背景

某高新产品研发企业拥有员工 2000 余人，公司总部坐落在省会城市高新技术开发区，包括 4 个生产车间和两栋职工宿舍楼，产品展示、技术开发与企业办公均在智能大厦中进行。该企业在外地另开设有两家分公司，由总公司进行统一管理和部署。目前，该企业网络的拓扑结构如图 1-1 所示，基本情况如下。

(1) 公司局域网已经基本覆盖整个厂区，中心机房位于智能大厦的第 3 层(共 15 层)，职工宿舍楼和生产车间均有网络覆盖。

(2) 网络拓扑结构为“星型＋树型”，接入层交换机为 Cisco Catalyst 2960，汇聚层交换机为 Cisco Catalyst 3750，核心层交换机为 Cisco Catalyst 6509。

(3) 现有接入用户数量为 500 个，客户端均使用私有 IP 地址，通过防火墙或代理服务器接入 Internet。部分服务器 IP 地址为共有 IP 地址。

(4) Internet 接入区的防火墙主要提供 VPN 接入功能，用于为远程移动用户或子公司网络提供远程安全访问。

(5) 会议室、产品展示大厅等公共场所部署无线接入点，实现随时随地无线漫游接入。

(6) 服务器操作系统平台多为 Windows Server 2003 和 Windows Server 2008 系统。客户端系统为 Windows XP Professional 和 Windows Vista。

(7) 网络中部署有 Web 服务器，为企业网站提供运行平台。

(8) 企业网络办公平台为 WSS，文件服务器可以为智能大厦的办公用户提供文件共享、存储与访问。

(9) E-mail 用于员工之间的彼此交流，以及企业与外界的通信联络。

(10) 打印服务和传真服务主要满足智能大厦用户网络办公的应用。

(11) 企业分支结构通过 VPN 方式远程接入总部局域网，并且可以访问网络中的共享资源。

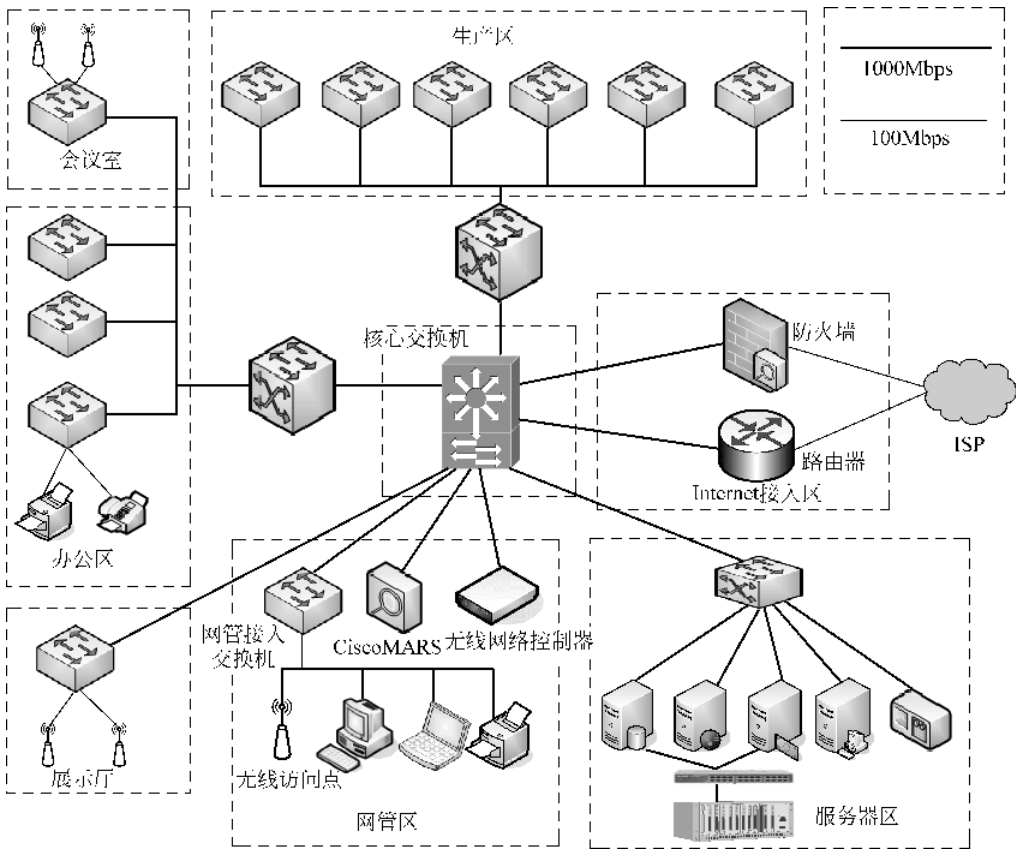

图 1-1 项目背景

1.2 项目分析

在普通小型局域网中，最常用的安全防护手段就是在路由器后部署一道防火墙，甚至安全需求较低的网络并无硬件防火墙，只是在路由器和交换机上进行简单的访问控制与数据包筛选机制就可以了。但是，在该企业网络中，许多重要应用都要依赖网络，势必对网络安全性的要求要高一些，在部署网络安全设备的同时，必须辅助多种访问控制与安全配置措施，加固网络安全。

1.2.1 安全设备分布

1. 防火墙

由于企业局域网采用以太网接入方式，所以直接使用防火墙充当接入设备，部署在网络边缘，防火墙连接的内网路由器上配置访问列表和静态路由信息。另外，在会议室、产品展示厅等公共环境中的汇聚交换机和核心交换机之间部署硬件防火墙，防止公共环境中可能存在的安全风险通过核心设备传播到整个网络。

2. IPS

IPS(Intrusion Prevention System，入侵防御系统)部署在 Internet 接入区的路由器和

核心交换机之间，用于扫描所有来自 Internet 的信息，以便及时发现网络攻击和制定解决方案。

3. IDS

IDS(Intrusion Detection System，入侵检测系统)本身是一个典型的探测设备，类似于网络嗅探器，无须转发任何流量，而只需要在网络上被动地、无声息地收集相应的报文即可。IDS 无法跨越物理网段收集信息，只能收集所在交换机的某个端口上的所有数据信息。该网络中的 IDS 部署在安全需求最高的服务器区，用于实时侦测服务器区交换机转发的所有信息。对收集来的报文，IDS 将提取相应的流量统计特征值，并利用内置的入侵知识库，与这些流量特征进行智能分析比较匹配。根据默认的阈值，匹配耦合度较高的报文流量将被认为是进攻，IDS 将根据相应的配置进行报警或进行有限度的反击。

4. Cisco Security MARS

Cisco Security MARS(Monitoring Analysis and Response System)是基于设备的全方位解决方案，是网络安全管理的关键组成部分。MARS 可以自动识别、管理并抵御安全威胁，它能与现有网络和安全部署协作，自动识别并隔离网络威胁，同时提供准确的清除建议。在本例企业网络中，MARS 直接连接在核心交换机上，用于收集经过核心交换机的所有数据信息，自动生成状态日志，供管理员调阅。

1.2.2 网络设备安全现状

当前网络中的交换机、路由器等网络设备全部都是可网管的智能设备，并且提供 Web 管理方式，同时配置了基本的安全防御措施，如登录密码、用户账户权限等。

1. 交换机和路由器安全配置

交换机的主要功能就是提供网络接入所需的接口。目前，该网络中基于交换机的安全管理仅限于 VLAN 划分、Enable 密码和 Telnet 密码等基本安全措施，并未进行任何高级安全配置，如流量控制、远程监控、IEEE 802.1x 安全认证等，存在较大的安全隐患。

企业网络采用以太网接入 Internet，而网络中部署的网络防火墙已具备接入功能，所以该网络中的路由器上只配置了简单的静态路由、访问控制列表和网络地址转换，可以满足基本的安全需求。

2. 办公设备安全配置

企业网络中的集中办公设备包括打印机和传真机，均支持网络接入功能，部署在楼层的集中办公区。由于缺乏访问权限控制措施，致使网络打印机和传真机被滥用，造成不必要的资源浪费。另外，用户计算机到打印机之间的数据传输是未经加密的明文，存在一定的安全隐患。

1.2.3 服务器部署现状

网络中的应用服务器包括域控制器、DHCP 服务器、文件服务器、打印服务器、传真服务器、网络办公平台、数据库服务器等，其中有多种网络服务合用一台服务器，网络中共有服务器 10 台，通过单独的交换机高速连接至核心交换机，完全采用链路冗余结束双线连接，确保连接的可靠性。

所有服务器均已加入域中，接受域控制器的统一管理，并且已开启远程终端功能，用户

可以使用有效的管理员账户凭据远程登录服务器，实现相应的配置与管理任务。

1.2.4 客户端计算机

客户端计算机主要以 Windows 操作系统为主，极少数用户是运行 Linux 和 Mac OS 操作系统的。客户端计算机的安全防御比较薄弱，仅限于用户账户登录密码、个人防火墙、杀毒软件等。因此，由于个别客户端感染病毒而导致网络瘫痪的问题时有发生。对于 Windows 系统而言，应用最多的 Windows XP Professional 和 Windows Vista 系统已经集成了比较完善的安全防御功能，如 Internet 防火墙、Windows 防火墙、Windows Defender、Windows Update 等，客户端用户只需对这些功能进行简单配置，即可增强系统安全性。

另外，对于中型规模的企业网络而言，统一的网络管理才是最重要的。例如，统一配置客户端计算机安全功能、部署 WSUS 服务器、增强网络访问控制、部署 NAP 系统等。

1.2.5 无线局域网安全现状

在企业网络中部署无线局域网，延伸了有线局域网的覆盖范围，避免网络布线对现有整体布局和装修的破坏，既是环境需求，也是企业发展和生存的需要。用户在无线网络覆盖范围内可以自由访问网络，充分享受无线畅游的便利。但是，由于无线网络传输的特殊性，无线局域网的安全问题也是不容忽视的。该企业网络中的无限网络安全问题，主要表现在如下几个方面。

1. WEP 密钥的发布问题

802.11 本身并未规定密钥如何分发。所有安全性考虑的前提是假定密钥已通过与 802.11 无关的安全渠道送到了工作站点上，而在实际应用中，一般都是手工设置，并长期固定使用 4 个可选密钥之一。因此，当工作站点增多时，手工方法的配置和管理将十分烦琐且效率低下，而且密钥一旦丢失，WLAN 将无安全性可言。

2. WEP 用户身份认证方法的缺陷

802.11 标准规定了两种认证方式：开放系统认证和共享密钥认证。

开放系统认证是默认的认证方法，任何移动站点都可加入 BSS(Basic Service Set，基本服务集)，并可以跟 AP(Access Point，接入点)通信，能“听到”所有未加密的数据，可见，这种方法根本没有提供认证，也就不存在安全性。

共享密钥认证是一种请求响应认证机制：AP 在收到工作站点 STA(Static Timing Analysis，静态时序分析)的请求接入消息时发送询问消息，STA 对询问消息使用共享密钥进行加密并送回 AP，AP 解密并校验消息的完整性，若成功，则允许 STA 接入 WLAN。攻击者只需抓住加密前后的询问消息，加以简单的数学运算就可得到共享密钥生成的伪随机密码流，然后伪造合法的响应消息通过 AP 认证后接入 WLAN。

3. SSID 和 MAC 地址过滤

WEP 服务集标识 SSID 由 Lucent 公司提出，用于对封闭网络进行访问控制。只有与 AP 有相同的 SSID 的客户站点才允许访问 WLAN。MAC 地址过滤的想法是 AP 中存有合法客户站点的 MAC 地址列表，拒绝 MAC 地址不在列表中的站点接入被保护的网络。但由于 SSID 和 MAC 地址很容易被窃取，因此安全性较低。

4. WEP 加密机制的天生脆弱性

WEP 加密机制的天生脆弱性是受网络攻击的最主要原因，WEP2 算法作为 802.11i 的安全标准，对现有系统改进相对较小并易于实现。

1.3 项目需求

由于该公司的主要业务为高新产品开发和生产，掌握众多行业机密信息，并且下设多个部门，所以对网络安全性和稳定性要求比较高。无论是基础网络还是客户端都必须严格做好安全防御工作。

1.3.1 网络安全需求

综合项目成本和实际应用等多方面因素，可以从如下几个方面满足用户需求。

(1) 将防火墙部署在网络边缘，用于隔离来自 Internet 的所有网络风险。

(2) 在路由器和核心交换机之间部署 IPS，对全网的所有 Internet 通信进行检测，以便可以自动阻止、调整或隔离非正常网络请求和危险信息的传输。

(3) 生产区和办公区分别通过汇聚交换机连接至核心交换机，在相应的汇聚交换机上分别进行适当的安全配置，将可能存在的风险因素隔离在网络局部。

(4) 在办公区网络中，将安全需求和应用需求不同的用户指定到不同的 VLAN 中，充分确保部门内部和部门间的信息安全。

(5) 在会议室和展示厅等移动用户比较集中的场所，部署无线接入系统，在无线接入点以及无线接入点连接的接入交换机上，分别部署相应的安全防御措施，如 IEEE 802.1x 认证、禁止广播 SSID、WEP 加密等。

(6) 网络管理区和服务器区直接连接至核心交换机，以确保网络传输的可靠性。网络管理区中部署有 MARS 系统，用于监控、分析和处理网络中所有通过核心交换机的数据通信，以便及时发现网络中存在的恶意攻击、非正常访问等情况，并协助管理员制定相应的解决方案。

(7) 为了确保服务器的安全，在服务器集中区部署 IDS，可以对服务器区网络以及系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

1.3.2 网络访问安全需求

由于公司大部分用户信息安全意识较差，因此必须对安全需求较高的部门的用户进行集中管理，防止机密信息外泄。另外，本公司在外地设有分公司，只能通过远程接入方式访问内部网络资源，可以借助 VPN 技术实现加密传输，充分确保信息安全。目前，该网络中网络访问安全需求如下。

(1) 客户端更新需要集中管理。大多数用户都已启用 Windows Update 功能，但是每个用户都从微软官方站点下载更新程序，会占用大量的网络带宽。另外，还有部分用户并未开启 Windows Update 功能，存在可能招致网络攻击的安全漏洞。

(2) 网络病毒不得不防。网络病毒和攻击是目前最主要的信息安全威胁因素。网络病

毒的防御工作绝非一蹴而就，必须从各方面严格防范。通常情况下，大部分用户都安装了杀毒软件和个人防火墙软件，可以起到一定的安全防护作用，但是未能升级病毒库同样可能感染病毒。更严重的是，部分用户不安装任何杀毒软件和防火墙就开始使用，这是非常危险的。

(3) 网络访问控制需求。网络中缺乏严格的访问控制措施，用户只需使用相应的用户账户和密码即可接入网络和访问共享资源，而对客户端系统健康程度没有任何要求和限制。如果接入用户的计算机已经感染病毒，则病毒可能通过网络快速蔓延至整个网络的所有分支。

(4) 远程访问安全的保护。远程接入是该网络中的重要应用之一，用于实现分公司网络到总公司网络的互联。远程访问 VPN 技术本身就具有一定的安全性，同时采用隧道和加密等多种技术，但是为了确保远程访问的安全，应加强远程访问的保护与控制。

1.4 项目规划

网络安全与网络应用是相互制约和影响的。网络应用需要安全措施的保护，但是如果安全措施过于严格，就会影响到应用的易用性。因此，部署网络安全措施之前，必须经过严格的规划。另外，网络安全的管理遍布网络的所有分支，包括设备安全、访问安全、服务器安全、客户端安全等。

1.4.1 服务器安全规划

服务器是企业网络的重要基础，其安全性将直接影响企业网站以及网络应用的安全，甚至会影响企业的生存与发展。服务器的大部分应用都是基于网络操作系统等软件实现的，因此，无论是应用程序出错，还是硬件故障都可能导致服务器瘫痪。若想做好服务器安全防护工作，必须从多方面入手。

1. 服务器硬件安全

服务器硬件设备的维护主要包括增加和卸载设备、更换设备、工作环境维护等。因为服务器的运行是不间断的，因此这些维护工作必须在确保服务器正常运行的状态下进行。

(1) 增加内存和硬盘容量。服务器的内存和硬盘都是支持热插拔的，建议增加与原设备同厂商、同型号、同容量的内存或硬盘，避免由于兼容性问题而导致服务器宕机。

(2) 定期为服务器除尘。很多服务器故障都是由于内部灰尘导致的，因此建议管理员每个月定期拆机打扫一次。

(3) 控制机房温度和湿度。虽然服务器对工作环境的要求比较宽泛，但是当服务器周边环境比较恶劣时同样会降低其处理速度和稳定性。

2. 操作系统安全

服务器操作系统的安全是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。对于操作系统的安全防范可以采取如下策略。

(1) 对操作系统进行安全配置，提高系统的安全性。系统内部调用不对 Internet 公开，关键性信息不直接公开，尽可能采用安全性高的操作系统。

(2) 应用系统在开发时，采用规范化的开发过程，尽可能地减少应用系统的漏洞。

(3) 网络上的服务器和网络设备尽可能不采取同一家的产品。

(4) 通过专业的安全工具(安全检测系统)定期对网络进行安全评估。

3. 网络应用服务安全

局域网中常用的网络服务包括 WWW 服务、FTP 服务、DNS 服务、DHCP 服务、Active Directory 服务等,随着服务器提供的服务越来越多,系统也容易混乱、安全性也将降低,因此,就需要对网络服务的相关参数进行设置,以增强其安全性和稳定性。通常情况下,网络应用服务安全可以分为如下 4 层。

(1) 网络与应用平台安全:主要包括网络的可靠性与生存性、信息系统的可靠性和可用性。网络的可靠性与生存性依靠环境安全、物理安全、节点安全、链路安全、拓扑安全、系统安全等方面来保障。信息系统的可靠性和可用性主要由计算机系统安全性决定。

(2) 应用服务提供安全:主要包括应用服务的可用性与可控性。服务可控性依靠服务接入安全以及服务防否认、服务防攻击、国家对应用服务的管制等方面来保障。服务可用性与承载业务网络可靠性以及维护能力等相关。

(3) 信息存储与传输安全:主要包括信息在网络传输和信息系统存储时完整性、机密性和不可否认性。信息完整性可以依靠报文鉴别机制;信息机密性可以依靠加密机制以及密钥分发等来保障;信息不可否认性可以依靠数字签名等技术来保障。

(4) 信息内容安全:主要指通过网络应用服务所传递的信息内容不涉及危害国家安全,泄露国家机密或商业秘密,侵犯国家利益、公共利益或公民合法权益,从事违法犯罪活动。

1.4.2 客户端安全规划

目前,Windows XP 和 Windows Vista 是首选客户端操作系统,为了便于统一管理,应将相对固定的客户端计算机加入域,接受域控制器的统一管理。通常情况下,可以从如下 5 方面做好客户端计算机的安全防御工作。

(1) 对于加入域的计算机可以通过组策略等工具统一部署安全策略,例如用户账户策略、密码策略、硬件设备安装限制策略等,确保客户端的安全。

(2) 对于未加入域的计算机,应提高用户网络安全的意识,通过设置登录密码、计算机锁定、防火墙等方式,确保系统安全。

(3) 在网络中部署 WSUS 服务器,负责为所有客户端计算机和服务器提供系统更新,避免系统漏洞的产生。

(4) 在所有客户端上部署 Symantec 网络防病毒客户端软件,并接受服务器端的统一管理,开启自动更新病毒库功能。

(5) 灵活部署和运用 Windows 防火墙、Windows Defender 等系统集成安全防护程序。

1.4.3 网络设备安全规划

局域网中的主要网络设备包括路由器、交换机和防火墙,分别用于提供不同的网络功能和应用。网络设备的部署方式、工作环境、配置管理等,都可能影响其安全性。

1. 网络设备的脆弱性

通常情况下,当用户按照组网规划方案购入并部署好网络设备之后,设备中的主要组成

系统即可在一段时间内保持相对稳定地运行。但是，网络设备本身就有一定的脆弱性，这也往往会成为入侵者攻击的目标。网络设备的安全脆弱性主要表现在如下 5 方面。

(1) 提供不必要的网络服务，提高了攻击者的攻击机会。

(2) 存在不安全的配置，带来不必要的安全隐患。

(3) 不适当的访问控制。

(4) 存在系统软件上的安全漏洞。

(5) 物理上没有得到安全存放，容易遭受临近攻击。

针对这些与生俱来的安全弱点，用户可以通过如下措施加固设备安全。

(1) 禁用不必要的网络服务。

(2) 修改不安全的配置。

(3) 利用最小特权原则严格对设备的访问控制。

(4) 及时对系统进行软件升级。

(5) 提供符合 IPP(Information Protection Policy，信息保护策略)要求的物理保护环境。

2. 部署网络安全设备

局域网中常见的网络安全设备包括网络防火墙、入侵检测设备、入侵防御设备等。网络防火墙是必不可少的，用于拦截处理来自 Internet 的各种攻击行为，并且可以隔离内部网络有效避免内部攻击。入侵检测设备只能用于记录入侵行为，局域网中已经很少使用。通常情况下，可以在网络中部署入侵防御系统，保护内部服务器或局域网的安全。

3. IOS 安全

IOS 就是智能网络设备的网络操作系统，主要用于提供软件管理平台。IOS 与计算机操作系统类似，难免存在系统漏洞，入侵者同样可以通过这些漏洞进入网络设备的 IOS，进行各种破坏活动，从而影响网络的正常运行。

通常情况下，用户可以从如下 6 方面实现网络设备的 IOS 安全。

(1) 配置登录密码，主要包括 Enable 密码和 Telnet 密码，必要时可以以加密方式存储密码，以确保其安全性。

(2) 配置用户访问安全级别，为不同的管理账户赋予不同的访问和管理权限。

(3) 控制终端访问安全，严格控制允许终端连接的数量，以及终端会话超时限制。

(4) 配置 SNMP 安全。SNMP 字符串用于验证用户与交换机的连接，确保其身份的有效性，类似于用户账户和密码。

(5) 及时备份 IOS 映像，以便出现误操作或遭遇攻击时可以迅速恢复。

(6) 升级 IOS 版本。IOS 的系统漏洞是不可避免的，用户可以通过安装补丁或升级 IOS 版本的方法避免由于系统漏洞导致的网络攻击。

1.4.4 无线设备安全规划

无线接入不仅是企业发展的需要，更是企业形象的代表。无线局域网是有线网络的扩展，主要用于为移动终端用户提供网络接入。该公司中的 AP(Access Point，无线接入点)主要分布在产品展示区和会议室，方便移动用户随时随地访问公司网络。如今许多笔记本电脑、掌上电脑、手机等都提供无线接入功能，在无线网络覆盖范围内“蹭网”已经成为一种

时尚，对于管理员而言，无线网络安全自然也就成了管理重点。

在无线局域网管理中，可以采用如下措施确保网络安全。

(1) 确保桌面计算机和服务器系统实现尽可能的安全。这种保护提高了攻击的门槛，即使攻击者进入了 WLAN，仍然很难渗透进用户的计算机。

(2) 启用无线 AP 和工作站所支持的最强 WEP。同时，确保拥有一个强健的 WEP 密码，这个密码应该符合有线网络中所应用的相同的密码强度规则。

(3) 确保无线网络的网络名称(SSID)不是可以轻松识别的。不要使用公司名称、自己的姓名或者地址作为 SSID。

(4) 如果无线 AP 支持 SSID 广播，应当关闭。这个措施可以创建一个封闭网络，这样，新的客户端必须在连接之前输入正确的 SSID。

(5) 使用 IEEE 802.1x 身份验证协议保护无线网络的安全。

(6) 在网络中部署无线网络控制器，统一管理和部署网络中的所有无线接入点，实时监测无线网络攻击情况。

1.4.5 安全设备规划

在安全性需求较高的网络中，网络安全设备是必不可少的。该公司网络中使用的安全设备包括网络防火墙、IDS 和 IPS。

1. 网络防火墙

防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界即采用不同安全策略的两个网络连接处，如用户和 Internet 之间、同一企业内部同部门的网络之间等。防火墙的目的就是在网络连接之间建立一个安全控制点，通过设定一定的筛选机制来决定允许或拒绝数据包通过，实现对进入网络内部的服务和访问的审计与控制。网络防火墙是内、外网络数据传输的必经之路。

2. IDS

IDS 是继“防火墙”、“信息加密”等传统安全保护方法之后的新一代安全保障技术。入侵检测技术是为保证计算机系统的安全，而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术。IDS 通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。该网络中的 IDS 部署在服务器区的接入交换机处。

IDS 能够检测到的攻击类型通常包括：系统扫描(System Scanning)、拒绝服务(Deny of Service)和系统渗透(System Penetration)。IDS 对攻击的检测方法主要包括：被动、非在线地发现和实时、在线地发现计算机网络中的攻击者。IDS 的主要优势是监听网络流量，但又不会影响网络的性能。作为对防火墙的有益补充，IDS 能够帮助网络系统快速发现网络攻击的发生，可扩展系统管理员的安全管理能力，包括安全审计、监视、进攻识别和响应等，从而提高了信息安全基础结构的完整性，被认为是继防火墙之后的第二道安全闸门。

3. IPS

网络中的 IPS 主要用于拦截和处理传统网络防火墙无法解决的网络攻击，部署在网络中的 Internet 接入区。

传统的防火墙旨在拒绝那些明显可疑的网络流量，但仍然允许某些流量通过，因此，防

火墙对于很多入侵攻击仍然无计可施，而绝大多数 IDS 系统都是被动的，不是主动的，即在攻击实际发生前，往往无法预先发出警报。而入侵防御系统 IPS 则倾向于提供主动防御，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。

IPS 是通过直接嵌入到网络流量中实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将其传送到内部系统中。此时，有问题的数据包，以及所有来自同一数据流的后续数据包，都能在 IPS 设备中被清除掉。

1.4.6 局域网接入安全规划

根据拓扑结构，可以将局域网分为核心层、汇聚层和接入层 3 个层次。接入层是最终面向用户的，是局域网用户进入网络的接入点，在该层应用保障安全的策略，能为局域网的安全运行提供保障。

1. 常规接入安全措施

在传统有线网络中，通常可以采用 802.1x 认证确保局域网接入的安全，但需要交换机支持和后台的 RADIUS 服务器，同时必须采用国内某些网络厂商提供的 802.1x 解决方案，可以实现用户名、IP 地址、MAC 地址、端口、VLAN、交换机 IP 等的绑定，从而有效避免网络设备、用户等的非法接入。除此之外，防火墙类的产品也可以控制局域网接入，但需要额外投资，并且可靠性不是很高。

在无线局域网中，管理员可以通过如下措施确保接入安全。

(1) 设置 SSID。SSID 是无线局域网的网络名称，通常用于区分不同的网络。无线设备或用户接入网络之前必须提供匹配的 SSID，否则无法接入。SSID 类似于一个简单的口令，阻止非法用户的接入，保障无线局域网的安全。另外，还需要禁止无线设备的 SSID 广播功能。

(2) 配置 MAC 地址访问控制列表。每个网络设备或计算机的网卡都有一个唯一的 MAC 地址，因此通过配置 MAC 地址访问控制列表，可以确保只有经过注册的设备才可以接入网络，阻止未经授权的无线用户接入。

(3) 配置 WEP 加密。WEP 加密主要是针对无线网络中传输的数据而言的，可以用于保护链路层数据的安全。WEP 使用 40 位密钥，采用 RSA 开发的 RC4 对称加密算法，在链路层加密数据。

(4) 配置 802.1x 认证。当无线设备或用户接入无线局域网之前，可以通过 802.1x 认证决定是否允许其继续访问。如果认证通过，则 AP 为无线工作站打开这个逻辑端口，否则不允许接入。

2. NAP 技术

NAP(Network Access Protection，网络访问保护)是 Microsoft 在 Windows Vista 和 Windows Server 2008 提供的全新系统组件，它可以在访问私有网络时提供系统平台健康校验。NAP 平台提供了一套完整性校验的方法来判断接入网络的客户端的健康状态，对不符合健康策略需求的客户端限制其网络访问权限。

为了校验访问网络的主机的健康状况，网络架构需要提供如下功能性领域。