Introduction to Network Access Control

网络准入控制概论

聂元铭　董建锋　周小平　著

科学出版社

网络准入控制概论

聂元铭　董建锋　周小平　著

科学出版社

内 容 简 介

本书系统研究了网络准入控制技术（NAC）的基本原理、主要技术手段、体系架构和解决方案，探讨了下一代网络准入控制技术的发展方向，提出了建设NAC项目的实施方法和关键要素，给出了颇具代表性的实际应用案例。

本书适合信息网络安全技术研发和应用人员使用，亦可供信息网络安全管理和维护人员学习参考，并可作为大学相关专业教材。

图书在版编目(CIP)数据

网络准入控制概论/聂元铭，董建锋，周小平著. —北京：科学出版社，2012

ISBN 978-7-03-035257-6

Ⅰ.①网… Ⅱ.①聂…②董…③周… Ⅲ.①计算机网络-安全技术-研究 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字（2012）第182812号

责任编辑：王淑兰/责任校对：王万红

责任印制：吕春珉/封面设计：耕者设计工作室

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2012年8月第 一 版 开本：B5（720×1000）

2012年8月第一次印刷 印张：14 1/2

字数：285 000

定价：48.00元

（如有印装质量问题，我社负责调换<双青>）

销售部电话 010-62136131 编辑部电话 010-62130750

前　言

伴随着社会信息化步伐的不断提速，网络正全方位地改变着我们的工作、生活以及娱乐方式。发展初期的网络注重设备的互通性、链路的可靠性，从而达到信息共享的通畅。经过多年的应用与发展，伴随着人们对网络软硬件技术认识的深入，网络安全已经超过人们对网络可靠性、交换能力和服务质量的需求，而网络的可信接入更成为网络安全的最重要环节，因此研究网络安全准入控制技术具有非常重要的现实意义。

在内网中，新的安全威胁不断涌现，任何一台终端的安全状态，都将直接影响到整个网络的安全。不符合企业安全策略的终端，如防病毒库版本低、补丁未升级、非法终端接入和违规外联等情况，最终的结果可能是全网瘫痪，所有终端都无法正常工作。如何确保网络中的终端安全状态符合企业安全策略，防止内部网络系统遭受非法入侵，防止终端身份伪造，成为构建可信网络的一大难题。通过网络准入控制系统对内网终端边界进行防护，可实现“身份认证—安全检查—隔离修复—访问授权”的一体化终端入网流程管理，对接入网络的终端实现安全准入控制，使每个入网终端均满足安全管理的基准线是网络准入控制技术的重要作用。

本书共有 7 章。从基本概念、技术原理和运行机制等方面，阐述了网络准入控制技术所涵盖的内容，并深入研究分析了网络准入控制技术的主要手段、技术架构、解决方案和网络准入控制项目的建设实践，旨在使读者了解网络准入控制技术的内涵与外延，掌握网络安全准入控制实用技术，解决网络安全管理问题，提高信息网络安全的效益和效率。

本书技术数据在盈高科技网络准入控制实验室通过验证，并在第 7 章列举了盈高科技实施的工程案例。本书写作过程中，得到了孙桂芝、常明、叶启平、翟寅川、杨军、罗治华、张婧、张优扬、汪丽娟、刘璇、韩金龙的大力支持，特别是参与本书部分章节资料整理和文字校对工作的李力、何俊、龙杨、袁宏宇、张明、王建鑫、赵思成等人为完成书稿做出了突出贡献，在此表示真诚的感谢。

由于作者水平所限，书中错误和疏漏在所难免，诚请读者予以指正。

作　者

2012 年 8 月

目　录

第 1 章　网络准入控制技术基础

网络准入控制（Network Access Control，NAC）是目前一种新型的安全防御技术，它通过对终端实施安全防护，可以有效地解决因不安全终端接入网络而引起的安全威胁，将病毒、蠕虫等各类攻击拒绝于网络之外，从而真正保障网络的安全。目前，对网络准入控制还没有一个权威、统一的定义，甚至其名称也有各种叫法，如网络接入控制、终端准入控制、终端安全接入、安全接入控制，等等。专业人员普遍认为，网络准入控制是一套可用于定义在节点访问网络之前，如何保障网络及节点安全的协议集合。该技术的核心概念是从网络终端的安全控制入手，通过消除终端的不安全因素或将其减少到最小，从而保护网络和终端的安全。

网络准入控制的主要思路是：终端接入网络之前应根据预定安全策略对其进行检查，只允许符合安全策略的终端接入网络，而将不安全的终端隔离于网络之外，自动拒绝不安全的主机接入受保护网络，直到这些主机符合网络内的安全策略为止。

具体来说，网络准入控制技术是通过使用用户身份认证手段，对用户的接入设备进行状态评估，实现对用户属性、在线状态、流量限制的全面管理与掌握。在企业、机构网络环境中，由于缺乏有效的管理与控制，网络安全形势日趋严峻，即使部署了防火墙、漏洞扫描系统、入侵检测系统和防病毒软件等安全防线，攻击网络的现象仍然层出不穷，网络的可用性难以保证。在众多的网络安全事件背后，普遍存在的事实是管理者不能及时掌握用户属性、在线状态、流量使用情况等，网络用户若没有及时安装系统补丁和升级病毒库，每个网络用户都可能成为网络攻击的发起者，同时也是受害者。因此，只有采用网络准入控制技术，通过用户身份认证手段，对用户的接入设备进行安全状态评估，使每个接入点都具有较高的可信身份和基本的安全条件，才能达到高效、安全、全方位地保护内部网络安全的目的。

1.1　网络准入控制技术背景

随着 IT 技术的不断进步，信息一体化带给人们的双刃剑效应也越来越明显，人们在体验到信息高速公路的便捷高效的同时，也会遭受到各种各样的威胁和风险带来的损失，信息安全问题越来越显得突出。据 CSI/FBI 安全报告称，虽然安全技术多年来一直在发展，且安全技术的实施更是耗资数百万美元，但病毒、蠕虫、间谍软件和其他形式的恶意软件仍然是各机构现在面临的主要问题。每年遭

遇的大量安全事故造成系统中断、收入损失、数据损坏或毁坏以及生产率降低等问题，给企业和机构带来了巨大的经济影响。

在当今这个多样化的、动态的全球网络环境中，对于试图接入企事业单位网络的可管理或不可管理的设备，网络管理员根本无法在其接入网络前知晓它们的来源。面对手段高明、资金雄厚的黑客，用户设备很可能在不知不觉间已经感染致命的恶意软件。随后，用户设备就作为一种传输媒介，在网络上传播病毒、间谍软件、广告软件、特洛伊木马、蠕虫、木马后门、bots、rootkits 和其他形式的恶意应用，或将它们直接传染给不设防的其他用户设备。感染任何此类恶意应用都将威胁到企事业单位的信息资产安全，使企业付出惨重的代价。

与此同时，随着 Internet 的快速发展，在电子政务和电子商务应用快速发展的今天，Intranet 作为 Internet 技术运用于单位、部门和企业专用网的产物，也得到迅速普及发展。这些单位、部门和企业的办公和生产对信息化的依赖程度越来越高，对信息网络安全要求也越来越高。众所周知，Intranet 并非是地域上的概念，而是在信息空间上的虚拟网络概念，如一个国家外交系统的内域网用户可能分布全球。它在原有专用网的基础上增加了服务器、服务器软件、Web 内容制作工具和浏览器，与 Internet 连通，从而使内域网充满了生机和活力。随着信息网络的迅速发展，企业的信息网络规模越来越庞大，信息接入点就越来越多。内域网为公司和单位信息的散播和利用提供了极为便利的条件。浏览器为网上用户提供信息，服务器对网络进行管理、组织和存储信息，并提供必要的安全服务。通常情况下，Intranet 中存有大量的单位内部的敏感信息，具有极高的商务、政治和军事价值。

因此，Intranet 应该说是一种半封闭甚至是全封闭的集中式可控网，所以其安全保密是至关重要的。要保证内域网不被非法入侵和破坏，网中的敏感信息不被非法窃取和篡改，同时还要保证网内用户和网外用户之间正常连通，并向他们提供应有的服务。但是从当前的实际情况来看，内网中技术手段和有效的安全机制相对落后或缺乏，这必然造成难以杜绝不符合安全规范的终端接入网络中情况的发生，这些终端都将成为传播病毒的源头和被病毒感染的对象，影响内部信息网络和终端的可利用率。

目前，大部分网络的安全管理重点是放在了防范来自外部的攻击上面，主要依赖于防火墙、入侵检测、防病毒软件等。事实证明，企事业单位内部的不安全因素远比外部危害更恐怖。据权威统计显示，83%的信息安全事故是由内部人员和内外人员勾结所为，80%以上的企事业单位内部网络曾遭受过病毒的肆虐，60%以上的企事业网站受过黑客的攻击，从这一些数字足见内部网络安全管理问题的重要性。可以说，网络内部漏洞给重要资源造成的威胁远远大于从互联网穿越防火墙造成的入侵，而传统的防护技术，如防火墙、IDS 等均无法有效地对内部漏洞进行防范。显然，如果不能相信所有的用户都能正确、合法地使用网络，这就有必要进行适当的访问控制，最基本的要求就是采用确定的机制对通信实体

和网络用户进行可靠的认证和控制。这些安全业务都需要建立健全一个完善的网络准入控制机制。

正如上面所说，对于政府机关、金融机构、各种企事业单位，虽然其内部网络基本上与互联网隔开，但仍会受到病毒、黑客等网络危害的影响，而且一旦其信息系统受到破坏，产生的经济以及社会影响相当巨大，甚至会波及到每个人的切身利益。对于这种网络覆盖面广、应用复杂、计算机终端数量众多的内网来说，很大一部分安全隐患来自内部。网络安全管理上往往面临以下这些问题。

1. 单位资产，员工私产——资产管理失控

网络中终端用户随意增减调换，每个终端硬件配备（CPU、硬盘、内存等）肆意组装拆卸、操作系统随意更换、各类应用软件胡乱安装卸载，各种外设（软驱、光驱、U 盘、打印机、Modem 等）无节制使用。

2. 网络无限，自由无限——网络资源滥用

IP 地址滥用，流量滥用，甚至工作时间聊天、游戏、赌博、疯狂下载、登录色情反动网站等行为影响工作效率，影响网络正常使用。

3. 蠕虫泛滥，业务瘫痪——病毒蠕虫入侵

由于补丁不及时，网络滥用，非法接入等因素导致网络内病毒蠕虫泛滥、网络阻塞、数据损坏丢失，而且无法快速查找定位和隔离感染病毒或表现异常的计算机终端，无法找到灾难的源头以迅速采取隔离等处理措施，导致处理病毒和异常事件效率不高，从而为正常业务带来灾难性的、持续性的影响。

4. 脆弱防线，外强中干——终端安全隐患

内部网用户计算机终端的安全补丁和杀毒软件病毒库更新缺乏有效的检查和管理手段，无法有效地防范病毒入侵内部网；每个终端漏洞密布、口令简陋且经年不改，管理员无法时刻检查、提醒或强制解决，为蠕虫、泄密等灾难埋下了各种隐患。

5. 门户大开，长驱直入——外部非法接入

移动设备（笔记本电脑等）和新增设备未经过安全检查和处理违规接入或者入侵内部网络，带来病毒传播、黑客入侵等不安全因素；对用户计算机终端接入内部网缺乏有效的管理和控制，致使外来笔记本等不安全设备可随意接入内部网，对内部网的安全造成威胁。

6. 外贼好治，家贼难防——内部非法外联

内部网络用户计算机终端通过调制解调器、双网卡、无线网卡等设备进行在

线违规拨号上网、违规离线上网等，将企业内部网与外部不安全的网络系统（如互联网）联在一起，可能会使黑客进入到内部网，并使计算机感染病毒；或违反规定将专网专用计算机带出内网进入到其他网络。

7. 网络无界，一损俱损——重要信息泄密

因系统漏洞、病毒入侵、非法接入、非法外联、网络滥用、外设滥用等各种原因与管理不善导致组织内部重要信息泄露或毁灭，造成不可弥补的重大损失。

8. 千里之堤，毁于蚁穴——补丁管理混乱

终端用户不了解系统补丁状态，不及时打补丁，也没有办法统一进行补丁的下载、分析、测试和分发，从而为蠕虫与黑客入侵保留了通道。

因此，大家应该看到，网络中连接的各个用户终端设备已成为影响当前网络安全的重要因素。这一点在国内的网络安全行业中同样十分明显，从以下的几点安全动态中就可见一斑。

1.1.1 安全动态

1. 安全动态之一

上海某上市企业（全球 500 强合资公司），生产基地包括 4 个工厂，网络内有超过 1000 台终端设备，经常发生网内 ARP 攻击事件，导致业务系统中断。后查明是机器不受管控的随意接入，其自身由于感染 ARP 病毒，影响和攻击到了全网内正常工作的机器，造成重大安全事故。

2. 安全动态之二

国家电网某省分支机构，购买了某品牌的终端管理软件，并从单位层面规定必须安装此软件后入网。但由于各种原因（用户私自卸载、重装系统、与其他软件冲突等）导致全网的软件部署率极低，并曾由于此系统与某安全软件冲突而无法运行，导致大部分用户无法入网。

3. 安全动态之三

2010 年 3 月，微软 IE 浏览器出现“零日漏洞”——KB981374，该漏洞被大量挂马网站利用，漏洞影响范围包括 IE6、IE7。未安装相关安全补丁的用户电脑一旦被攻击成功，将会感染木马下载器、黑客后门，使得电脑无法正常工作，并导致个人账号密码等隐私信息被窃取。

4. 安全动态之四

2011 年 2 月，某省厅级单位有效阻断**木马病毒风险百余次，阻断入侵攻击**

1700 余次。

1.1.2　风险分析

上述的安全事件表明，对于各机构的内网而言，现在存在的十分常见（或应该引起重视的）的网络安全风险点包括以下几个方面。

1. 入网设备及人员控制（参见安全动态之一）

如果对于单位的网络接入无法进行控制，非法机器插上网线后能随意接入网络，就会**造成进入网络窃取机密信息的危险，这将对网络中的涉密信息造成严重威胁**；另外，如果非法机器带毒入网，极有可能成为木马或蠕虫病毒威胁内网的跳板并造成重大安全事件。

2. 入网规范性控制（参见安全动态之二）

许多单位已经制定了一套内部网络管理规范，如禁止私自修改 IP 地址，禁止安装游戏或非业务软件，禁止随意保存或修改某些涉密文档等，但规范无法真正落到实处，许多用户依然我行我素，网络管理员无法对接入计算机的使用和软件安装情况进行整体管理，网络中的各类违规行为增加了管理的难度，甚至有可能造成涉密的安全风险。

3. 补丁、杀毒软件等漏洞控制（参见安全动态之三、四）

由于机构分散，部分员工整体安全意识不足又无法及时得到培训和管理，接入终端不及时升级系统补丁、不安装杀毒软件或杀毒软件不及时升级病毒库的现象普遍存在，无法对这些安全规范进行统一强制管理，这种情况下，安全性低下的单台终端同样容易成为影响全网的威胁来源和跳板（如 ARP 病毒攻击），或无法对入侵及病毒威胁进行有效的抵御，从而带来潜在的安全风险。

另外，员工计算机水平参差不齐，许多人面对计算机出现的故障无法进行及时修复。由于网点数多、范围分散，计算机出现问题后管理员需要频繁奔赴现场进行维护，工作效率低下。

4. 全网安全性审计——报告及审计需要

如果无法对入网设备进行安全性的整体评估，网络管理者就无法整体了解内网的安全性。由于无法确定设备安全性，造成无法确定和定位网络中的风险点，在安全事故发生时就无法明确相应的责任人，网络管理及维护者往往成为普通用户计算机安全漏洞的责任承担者。

由计算机安全协会（Computer Security Institute）与美国联邦调查局（FBI）联合进行的计算机安全报告显示，目前内网遭遇的主要威胁有病毒、蠕虫、间谍软件和其他形式的恶意软件，而这些威胁大都由不安全终端接入所引起。终端安

全接入是目前一种新型的安全防御技术，它通过对终端实施安全防护，可以有效地解决因不安全终端接入网络而引起的安全威胁事件，将病毒、蠕虫等各类攻击拒绝于网络之外，从而真正保障网络的安全。

在国内，直到近几年上述问题才逐渐引起管理者的重视，作为网络安全防范的源头，如何阻止非法用户接入网络，如何限制用户的安全行为，如何加强内部用户的网络接入控制已成为各个部门建立信息网络安全防御体系必须重点考虑的问题。目前，解决这一问题的有效方法就是利用交换机自身带有的功能，通过一定的配置，将网络准入控制应用到网络中，从而达到控制效果。解决这一类内网安全问题的方法被称为网络准入控制（Network Access Control，NAC）。

1.1.3 实施意义

网络准入控制体现了病毒防治、补丁修复、系统维护等终端安全防护措施与接入控制、身份认证、权限控制等网络准入控制手段的结合，体现了主动防御、整体安全的理念。网络准入控制解决方案可提供广泛而深入的功能，因此不仅涉及整个内网，而且还适用于内部组织机构和职能部门。网络准入控制技术的部署从桌面系统管理到桌面系统安全性、从网络基础设施到网络管理，几乎跨越整个IT领域。实施网络准入控制需要部署网络接入控制机制，网络策略通常基于用户身份、设备标识、设备运行状况以及设备位置等的制订。

实施网络准入控制不仅可同时确保用户和设备以适当方式通过适当连接接入适当网络，还可确保用户满足验证策略的要求、用户设备满足验证和安全策略的要求，以及用户和设备同时满足企事业单位制订的任何其他策略的要求。最直接的一个实施效果就是通过对接入企业局域网用户的认证，可以有效地拒绝不合法用户进入局域网内。例如，当有外来人员来到该企业后打算上网，他直接用网线链接网口将无法连接网络，即使他参照上网的计算机设置IP地址，由于得不到认证也不能连接网络。他必须向网管员申请后，由网管员对该计算机进行接入认证后，才能连接网络，同时也对分配的账户设置了限制权限，实现了控制源头和接入管理，从而能够更好地保障企事业网络的信息安全。

网络安全事件的源头产生于内网的情况越来越多，保障内网安全的前提和基础是网络准入控制技术。这里通过一个实例来说明网络准入控制系统都能够解决哪些具体问题。图1-1所示的是一个典型的中型企业内网的拓扑结构。

通过图1-1可以看出，该企业内网划分为多个VLAN，各VLAN的终端主机通过接入交换机接入网络，各VLAN之间通过三层交换机互连。同时，用户内网通过防火墙与广域网互联，实现外网与内网的逻辑隔离与访问控制。这样典型的网络结构虽然具有一定程度的安全性，但对于来自于内网的威胁没有很好的防范措施。

针对以上典型网络，网络准入控制解决方案可以解决用户的如下需求。

（1）防止有安全隐患的电脑或者非法电脑直接访问内部网络，发现并限制非

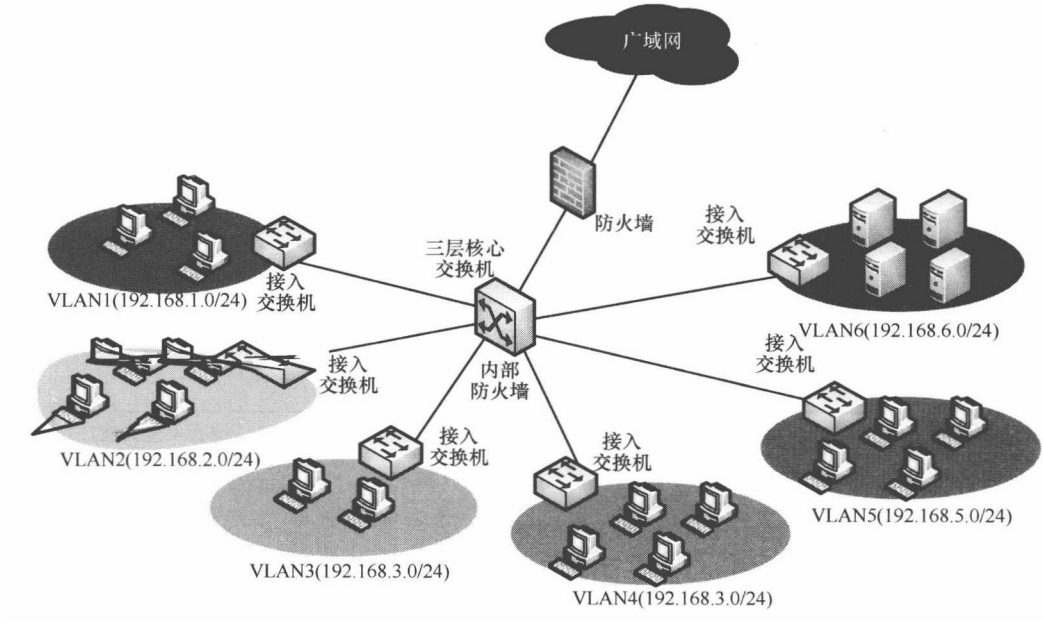

图 1-1　典型中型企业内网拓扑结构图

法外来主机接入内部网络，以免对内部网络造成危害。

（2）自行定义多种准入控制策略，加强内网接入设备的管理，合法主机的注册与审批入网，提供审批流程。

（3）内网 IP 地址管理，IP 与 MAC 地址的绑定，可依据 IP/MAC/主机名以及资产的配置对接入设备快速定位，以及防止地址冲突、网络扫描、ARP 欺骗等攻击对内网的危害。

（4）对合法主机的身份认证，以及接入后的访问控制，防止对网络资源的非授权访问和滥用。

（5）自动发现网络上的所有接入设备，对合法主机安全状态实时检测，如果发现主机存在安全风险或者用户进行了违规操作，可以隔离违规主机。

（6）检查桌面 PC 是否安装了非法软件，不允许禁止运行非法进程等；对 Modem 拨号、同时使用内外网卡等非法操作的监控、审计和禁止使用。

（7）及时发现安全设置不完善或存在安全隐患的 PC 机，对被存在风险的被隔离主机提供补丁漏洞自动修复、操作系统补丁和 MS 应用软件补丁自动更新和针对登录口令强度、Guest 账户、屏幕保护检测，加固主机安全性等必要的加固措施等。并能够形成报表，用于提示系统管理员和用户要采取的弥补措施。

总体而言，网络准入控制作为内网网络边界的第一道防线，为构建可信、安全、高效的内部网络环境提供了必要的基础支撑。

随着对网络安全问题的日益重视，网络准入控制采用的技术手段正在不断发展和更新，安全防范理念也在不断完善。目前，实现网络准入有多种方法，从这

些方法出发，不同的 IT 厂商各自推出了不同的实现方案。这些方法与方案还在不断完善中。网络准入控制技术今后的发展方向将是适应各种不同的复杂的网络环境，以及在准入过程中结合其他的网络管理要求，实现灵活的网络安全控制策略。研究新型终端安全接入技术对于新一代可信网络设备的研制，可信网络软件的设计，以及新一代网络安全防护技术的研发都具有重要的意义。

1.1.4 技术特点

网络准入控制技术主要解决网络终端合规性控制及其可信接入问题，与其他传统网络安全产品对比详见表 1-1。

表 1-1 NAC 系统与传统安全产品对比表

对比项目	网络准入控制系统	防火墙	入侵防御	桌面安全管理
简介	为解决内网中，各种类型的设备入网身份认证、安全状态检测、修复而建设的系统平台。 网络准入控制系统提供了一整套覆盖全网端点的安全管理平台，从设备入网、安全检查、隔离、修复等整个周期进行安全管理	防火墙英文名称为 FireWall，是指位于计算机和它所连接的网络之间的硬件或软件，也可以位于两个或多个网络之间，比如局域网和互联网之间，网络之间的所有数据流都经过防火墙。通过防火墙可以对网络之间的通信进行扫描，关闭不安全的端口，阻止外来的 DoS 攻击，封锁特洛伊木马等，以保证网络和计算机的安全	网络入侵防御系统作为一种在线部署的产品，提供主动的、实时的防护，其设计目标旨在准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是简单地在监测到恶意流量的同时或之后才发出告警	为解决桌面安全管理而设立的一套软件系统（硬件很少）。 桌面安全管理功能点很多，主要从资产管理、软件和补丁分发、应用软件管理、网络行为管理、行为审计等多个功能模块组成
定位	随着政策法规的要求，以及内网中各种安全事件的不断增加，在政府、电力、金融、电信及大型企事业单位日益成为迫切建设平台	作为网络安全建设的重要组成部分，防火墙系统是必须要建设的。 然而防火墙只能解决网关级的特定需求，网络安全建设决不仅仅是买几台防火墙	已成为网络安全建设的重要组成部分，在政府及高端行业以成为普遍配备的系统	作为终端安全管理的重要手段之一，桌面安全管理已越来越重要，但由于研发门槛不高，导致产品品牌众多，产品质量良莠不齐，因此，选择一款真正稳定、可靠的产品是最重要的
性能要求	主要从控制容量：200、500、1500、3000、5000 等每分钟上线率等来考虑，对可靠性、稳定性要求很高。 高端产品一般采用硬件级解决方案，在多协议支持、双机热备、无单点故障、大容量支撑上有重点解决	主要从安全性、网络性能：百兆、千兆等两方面来考虑，对可靠性、稳定性要求很高。	主要从安全性、网络性能：百兆、千兆等两方面来考虑，对可靠性、稳定性要求很高	主要从服务器承载终端数进行考量，还有客户端的性能。 由于桌面安全产品尚无相应的标准，一般采用纯软件形式，并且客户端所处的环境千差万别，各个厂商的研发实力差别很大，因此，相对而言，该系列产品的稳定性、可靠性要较弱

续表

对比项目	网络准入控制系统	防火墙	入侵防御	桌面安全管理
功能要求	解决网络层面上，所有入网设备的身份认证，安全状态的检查、隔离，以及不安全设备的修复等功能	重点解决内外网交换数据上的端口控制、访问控制等功能，实现如：地址转换、IP/MAC 绑定、静态和动态路由、源地址路由、代理、透明代理、ADSL 拨号、VPN 接入等功能	重点实现内外网交换数据上的入侵行为检测、防护，提供应用层的防护，以及对于内容级的管理，如阻断间谍软件、木马、P2P 下载等	桌面安全管理实现的功能非常多，基本上跟桌面相关的功能，都可以归入该系统，由此带来另一个问题，即功能很难达到精细、专业的标准。如资产管理很难和一套专业的资产管理平台相比，上网行为审计很难和专业的审计平台相比，甚至桌面管理平台还带有桌面准入、桌面防火墙、桌面 IPS 等功能，但其功能、性能不能和专业设备相比
发展趋势	随着等级保护、SOX 法案及内网安全管理需求的日益提升，网络安全准入控制系统已成为网络安全建设的重要组成部分，且为内网安全系统建设最为迫切的要求	防火墙已是一个成熟的市场，正常发展	IPS 市场是一个快速发展中的市场	市场需求虽然不断增加，但是桌面产品普遍功能模块太多，总体可靠性和专业性不高，和准入控制、防火墙、IPS 等专业性产品差距较大

1.2　网络准入控制技术发展

近年来，在网络安全管理实践中人们发现，安全事件的源头产生于网络内部的情况越来越多。比如，不明身份计算机的随意接入网络导致关键数据的外泄，一台染有 ARP 欺骗类病毒的计算机造成整个局域网的瘫痪，移动存储造成病毒的传播等。因此，如何确保网络内部的安全已经越来越受到人们的重视。作为内网安全保障的前提和基础，网络准入技术成为研究、应用与实践的热点。

随着对网络安全问题的日益重视，用户接入控制采用的技术手段在不断发展和更新，安全防范理念也在不断完善，市场上实现准入控制的技术方法很多，从这些技术方法出发，各 IT 厂商研发了很多各具特色的方案。这些技术方法与应用方案各适合于不同的网络环境和应用要求，还没有哪一种处于绝对领先的状态。从国外的 NAC 技术发展分析，以思科为主导的 NAC 领导产商，提出了更先进的技术框架与实现模型。目前，从控制层次的角度来分析网络准入控制技术主要分为两类：基于网络层的用户控制和基于应用的综合接入控制。总的来说，

随着网络应用技术的不断发展，企业用户正在逐步加强各自的信息网络安全建设，用户接入控制作为信息网络安全防范的源头，随着信息安全理念和技术的日益深入，其实施方法已经从原先的简单基于网络层的接入控制向基于应用的综合接入控制转变，实施手段从原来的单一的安全手段向一套整体的网络安全防御体系解决方案转变，在网络安全体系建设中起到越来越重要的作用。

而在网络准入控制发展的过程中，由于各家厂商利用标准的或私有的各种准入控制协议（标准的如 ARP 技术、DHCP 技术，私有的如 Cisco 的 EOU 技术），并且在整个准入控制的框架中利用了多种组成成分（如交换机、路由器、客户端、各种功能定位的服务器），因此整个网络准入控制行业的阵营逐渐得到了划分。

国际权威的评测机构 Forrester 对整个 NAC 行业按照核心技术的选择划分为 3 大阵营。

（1）Software-Based NAC（基于端点 Endpoint 技术协议的 NAC 系统架构）。

（2）Infrastructure-Based NAC（基于基础网络设备的 NAC 系统架构）。

（3）Appliance-Based NAC（基于应用设备理念的 NAC 系统架构）。

在 2008 年第三季度的独立调查报告“The Forrester Wave：Network Access Control，Q3 2008”中，Appliance NAC 解决方案被评价成网络访问控制领域的领跑者。Forrester 重点集中在不同的访问控制场景中进行评估，总共在 12 个不同场景中评估了各个供应商的解决方案，同时还在技术、战略和市场表现方面进行了对比。

Forrester Wave 的版权属于 Forrester Research Inc.。Forrester 和 Forrester Wave 是 Forrester Research Inc. 的商标。Forrester Wave 是 Forrester 的一个关于某一市场的图示分析，其中通过详细的电子表格列出了评分、权重和注释。Forrester 并不会为任何在 Forrester Wave 中描述到的供应商、产品或服务做宣传或广告。信息都来自于最容易获取的资源。其中的观点是当时的判断，可能随时间的发展而发生变化。图 1-2 是 Forrester 对国外主流 NAC 产商从技术框架、产品战略和市场表现等方面做的集中对比分析。

总体上看，Software-Based NAC 属于利用网络中的接入终端自行实施控制的准入架构，符合此类技术架构比较常见的是 ARP 欺骗技术；Infrastructure-Based NAC 是较为传统，也是应用范围最广的准入架构，其经典的实现方式就是 802.1x；而 Appliance-Based NAC 则属于行业领导厂商掌握的技术架构，其核心理念是用单台设备完成 90%以上的 NAC 所具备的功能，这种前沿性技术带来的益处十分明显，包括大大缩短部署时间、降低维护成本、增强对接入用户的友好性等。

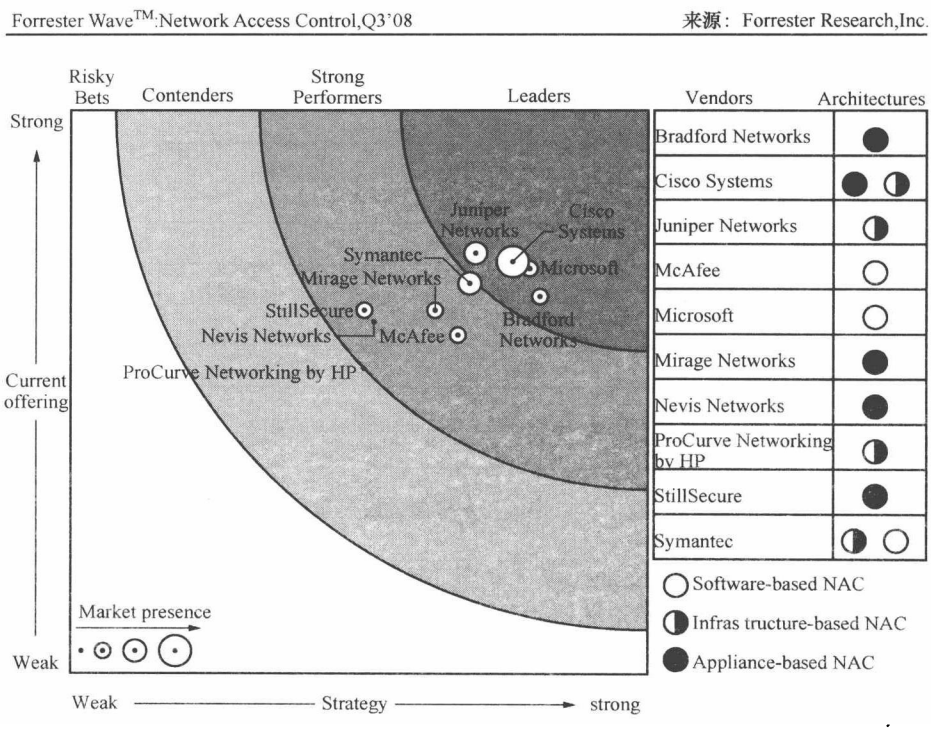

图 1-2　集中对比分析示意图

1.2.1　三代技术框架的发展

网络准入控制技术也是随时网络技术的发展，信息安全技术的发展，经历了几代技术框架的变迁。如图 1-3 所示。从早期的完全基于 Agent-Based 框架的 NAC，主要采用类似 ARP 欺骗技术、主机防火墙（TDI、NDIS）技术、DNS 协议拦截技术等，这种基于 Software-based 的 NAC 相对来说最具有伸缩性，也是最低廉的方案。但是对于如果无法安装 Agent 的网络设备就无法控制，并且如果不安装Agent也很容易绕开 NAC 的控制接入网络，同时不能很好地给用户提供友好的体验，无法对来宾做管理。

随着网络技术的发展，很多网络交换厂商为了让他们提供的基础网络方案增值，发展了基于网络交换设备的网络准入控制技术框架（Infrastructure-based NAC)。此方案主要是网络设备（交换机、路由器或者防火墙）联动，整合 Radius 服务，设备启用相关协议由设备进行控制。具有代表性的是 802.1x，EOU（EAP over UDP 的简称，是 Cisco 的专有协议)，像 802.1x 技术安全性还不错并且也可以分范围部署，但是部署复杂，部署周期也比较长，并且日常维护也十分的麻烦。由于目前这种方案相对而言还算较成熟，所以有很多客户选择以这种技术框架建设 NAC 系统。