第 5 章　信息安全管理华为典型实例

导入语：本章系统地介绍了华为内网安全的解决方案、终端安全管理解决方案和 H3C 终端接入控制解决方案。

本章主要知识结构如图 5.1 所示。

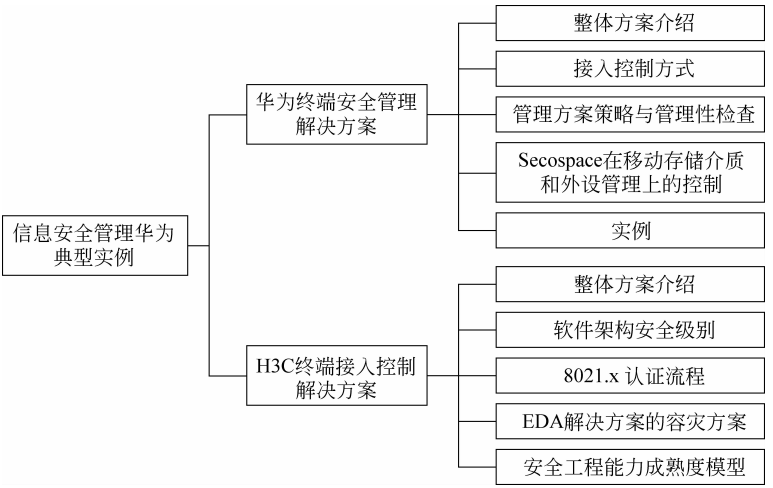

图 5.1　本章主要知识结构框图

在创新无处不在的 IT 世界里，从要求可用性到安全性再到高效率，只经历了短短的几年时间。而在 IT 管理概念中，时至今日终端管理无疑已经成为最重要的内容之一，它同样遵循着从可用性到安全性再到追求效率的发展规律。萨班斯-奥克斯利法案（Sarbanes-Oxley Act of 2002）对维护网络信息的安全性、保密性和完整性就提出了相关要求，而要达到这些要求，对终端的有效管理是解决问题的根本之道。是否能有一套完整的管理方案可同时解决终端的可用性、安全性和高效率呢？为了解决这个问题，H3C 推出了 H3C EAD（H3C End user Admission Domination）终端准入控制解决方案。H3C EAD 解决方案伴随着 IT 管理的发展，从最早实现用户身份认证，到实现网络安全认证，再到实现终端高效管理，也完成了从保障网络的可用性到安全性再到高效率的变化。H3C EAD 解决方案截至 2008 年 5 月，在现网中使用的用户数已经突破 40 万，这个变化不仅是一个数字的变化，更是代表了业界终端管理水平在质的方面的飞跃。

考核目标：熟悉并掌握华为的内网安全解决方案，终端安全管理解决方案和 H3C 终端接入控制解决方案。

5.1　内网安全危机

互联网的迅速普及，网络应用已成为企业发展中必不可少的一部分。然而，企业在感受网络所带来便利的同时，也面临着各种各样的进攻和威胁，如机密泄露、数据丢失、网络滥

用、身份冒用、非法入侵等。目前有些企业建立了相应的网络安全系统，并制定了相应的网络安全使用制度。但在实际使用中，由于用户对操作系统安全使用策略的配置及各种技术选项意义不明确，各种安全工具得不到正确的使用，系统漏洞、违规软件、病毒、恶意代码入侵等现象层出不穷，导致用户计算机操作系统达不到等级标准要求的安全等级。

5.1.1 内网安全危机

在今天的信息时代，基于网络的威胁潜伏在企业的每一个角落。随着企业和组织网络规模的增大，分支机构、移动办公、访客等增加了网络中的接入点，使存在于各层的网络漏洞成倍增加，病毒泛滥、未及时安装补丁招致恶意攻击、员工及合作伙伴盗窃机密数据等问题，成为企业面临的首要安全威胁。

5.1.2 内部威胁为首的主要安全问题

据 ISCA 统计，全球每年仅仅由于信息安全问题导致的损失高达数百亿美元，其中来自于内部的威胁高达 60%，来自内部的威胁已经成为企业首要的安全问题。企业面临的威胁复杂多样，其中主要有以下 3 个方面：

(1) 企业内网面临复杂多样的威胁。

非法用户随意接入公司内部网络；内部合法用户滥用权限；员工私自安装软件、开启危险服务；员工私自访问与工作无关网站；员工绕过防火墙访问互联网；员工未安装防病毒软件；员工忘记设置必要的口令等。

(2) 现有安全设备难以有效保护网络。

无法检查网络内计算机的安全状况；缺乏对合法终端滥用网络资源的安全管理；无法防止恶意终端的蓄意破坏。

(3) 终端数量大系统复杂、员工行为难以管理。

企业内网缺乏有效安全监控、审计手段；系统缺乏行之有效的管理及紧急响应手段；无法跟踪恶意员工泄露企业信息；员工上网等行为难以审计与管理；无法及时掌握终端的更新和变化。

5.1.3 确保企业内网安全，解决安全威胁问题

为确保企业内网的安全，必须强化内防内控，从终端入手强化弱点管理，着力解决终端接入控制；终端访问授权；终端安全健康性检查与策略管理；员工行为管理与违规审计等安全威胁问题。

(1) 终端接入控制。防止非法终端的接入，降低不安全终端的威胁。

(2) 终端访问授权。防止合法终端越权访问，保护企业核心资源。

(3) 终端安全健康性检查与策略管理。帮助企业落实安全管理制度。

(4) 员工行为管理与违规审计。强化行为审计，防止恶意终端破坏。

5.2 华为终端安全管理解决方案分析

5.2.1 华为终端安全管理解决方案

1. 信息安全策略的目标

信息安全策略的目标是为信息安全提供管理指导和支持，并与业务要求和相关的法律

法规保持一致。本策略主要包含以下 4 个方面：

(1) 策略下发。必须得到管理层批准，并向所有员工和相关第三方传达，全体人员必须履行相关的义务，享受相应的权利，承担相关的责任。

(2) 策略维护。信息安全策略通过以下方式进行文档的维护工作：

必须每年按照《风险评估管理程序》进行例行的风险评估，如遇以下情况必须及时进行风险评估。例如，发生重大安全事故；组织或技术基础结构发生重大变更；安全管理小组认为应当进行风险评估的；其他应当进行安全风险评估的情形，风险评估之后根据需要进行安全策略条目修订，并公布传达。

(3) 策略评审。每年必须参照《管理评审程序》执行公司管理评审。

(4) 适用范围。信息管理策略使用和涵盖的对象，包括现有的业务系统、硬件资产、软件资产、信息、通用服务、物理安全区域等。

2. 华为终端安全管理的解决方案

华为终端安全管理解决方案采取未雨绸缪的方式在端点接入网络之前进行安全状态评估，并提供系统漏洞修复，从而将病毒屏蔽在网络之外，同时强制应用级的安全策略，持续监控用户网络行为，包括移动存储设备管理，并对重要数据进行主动加密和严格的访问权限控制，最后还提供必要的系统应用管理，包括软件分发和资产管理。

根据终端安全管理模型，该方案采用了包括定制策略—检查控制—修复加固—统计汇总—持续审计的整体解决思路。

该方案还通过一体化、多层次和全面内网安全管理，实现企业从被动响应到有预见性、主动性的防御方式转变。

3. 终端安全管理带来的价值

终端安全管理给管理带来的价值有以下 4 个方面。

(1) 通过身份和安全双重认证、隔离、修复、授权、审计的接入控制模式，保障企业网络内部终端安全性，提高企业网络内部终端安全水平。

(2) 丰富的可灵活配置的终端管理策略，将终端管理经验融入其中，帮助企业快速部署和实现适合自身的终端管理。

(3) 强制安全检查，用户行为审计，确保企业管理制度的落实；实现细粒度的基于用户的访问控制，严格控制终端对业务系统的访问范围，保护业务系统的安全。

(4) 灵活的部署，方便的管理，丰富的报表，友好的界面，在有效提高企业终端管理水平的同时降低企业维护成本。

4. Secospace 终端安全管理系统的组成部分

Secospace 终端安全管理系统由安全代理(SA)、安全管理器(SM)、安全控制器(SC)、安全准入控制网关(SACG)、TSM 管理中心(TMC)五部分组成。每部分功能如下。

SM 作为系统的核心管理服务器，管理多个 SC。SM 采用 B/S 架构，系统管理员可通过 Web 界面配置和修改用户信息、访问权限和策略等，并完成报表输出。

SC：SC 作为与 SA 交互的控制点，是系统管理功能的实施者。完成用户身份认证、安全策略下发和软件下发等任务。并与 802.1X 或 SACG 联动在完成身份认证和安全策略检查后，开放端口或匹配 ACL 规则授权用户访问网络资源。

SA：SA 安装于客户的 PC 上，向服务器获取安全策略参数，根据这些参数执行本地计算机的安全策略检查；实施监控终端的行为，并且把审计的结果上报服务器，作为审计的

证据。

SACG：SACG 是在华为电信级防火墙硬件平台上开发的专用的接入控制网关，是实现硬件网关接入控制方式的核心设备。

TMC：TSM 的快速恢复服务器和 TSM 快速恢复客户端可通过 TSM 管理中心以最快的速度进行托管。通过一个单一的用户界面，可以管理端到端的数据保护和恢复。TSM 服务器 hztsmserver1 默认是自动启动的，并且每次机器重启后都是自动启动的。自动功能是通过/etc/inittab 文件中的启动脚本来实现的。

据专业的网络安全评估专家建议，对网络内部终端和公共可访问的服务器到 Internet 或其他不可信网络的外出流量都应该进行过滤，以阻止黑客和蠕虫的“抓钩”攻击。SACG 对终端的所有上行流量进行过滤，将网络分为可信、非受信和 DMZ（Trusted、Untrusted 和 DMZ）3 个域，用户在没有通过身份认证和安全检查前只能访问 DMZ，即受限的认证前域。通过后才能基于用户角色开放相应可以访问的认证后域，提供有效的内网接入保护。安全接入控制网关 SACG 方式的拓扑结构如图 5.2 所示。

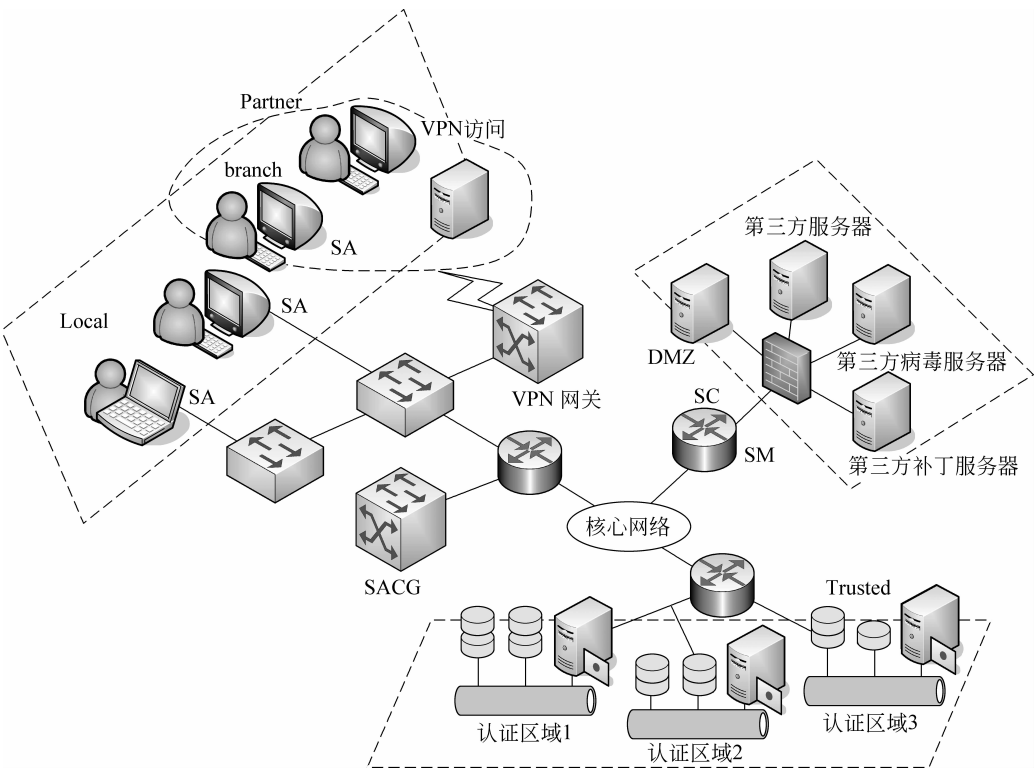

图 5.2　Secospace 终端安全管理的系统组成

网络中的资源被划分为前域、隔离域和后域。前域是指身份认证前可以访问的资源，如 DNS 服务器、外部认证源、业务控制器。隔离域是指用户通过了身份认证但未通过安全认证时允许访问的区域，如补丁服务器、防病毒服务器。后域是指用户通过安全认证后才能访问的区域，如 ERP 系统、财务系统、数据库系统。

5. 华为 Secospace 终端安全管理

ACG 安全接入控制网关，是实现接入控制与访问控制的核心设备，根据用户组来控制对业务服务器的访问权限，进行实时控制。

电信级的硬件平台，支持双机热备，高可靠性，实现细粒度的多认证后域划分，提供 3 个级别的设备支持不同的并发用户数(300/500/1000)。

6. Secospace 终端安全解决方案功能

Secospace 终端安全解决方案主要解决准入控制、终端安全基线管理、用户行为管理、补丁和软件的分发等功能。

准入控制是指发现并控制内部员工、外来访客和合作伙伴等对企业网络资源的访问，防止非法用户和不安全的终端接入内网，并根据用户身份授权访问指定的内网资源。

终端安全基线管理是指集中配置终端的安全基线，全面评估终端的安全状态，对不符合安全基线的终端进行隔离、修复，提高终端的安全防护水平，保证企业整网的安全。

用户行为管理是指审计并控制终端用户违反企业管理制度的行为，如 Web 访问、媒体下载、非法软件使用、非法外联、计算机外设、网络访问行为、网络异常监测等，防止计算机和网络资源的滥用和恶意破坏，规范终端用户使用 IT 资源的行为，提高企业整网的可用性和安全性。

补丁和软件分发是指提供智能、高效的补丁和软件分发功能，准确地评估系统漏洞，在最大限度降低网络带宽占用率的同时，及时帮助终端更新补丁，消除终端的安全漏洞；企业资产安全审计，动态收集企业软、硬件资产信息，跟踪企业资产变更，帮助管理员全面了解终端资产状况，提升企业整网的 IT 管理水平。

7. 安全接入控制为客户解决的问题

安全控制主要为客户解决：控制终端网络接入；访问权限管理；针对不同场景提供灵活的接入控制的问题。

(1) 控制终端网络接入，保障内部网络安全。禁止非授权的终端进入网络；禁止不安全的终端进入网络；禁止违规的终端进入网络。

(2) 访问权限管理，保护企业核心资源。安全接入控制网关提供网络层访问权限控制；支持划分多认证后域，实现细粒度访问权限管理。

(3) 针对不同场景提供灵活的接入控制方式。终端代理＋安全接入控制网关；Web＋安全接入控制网关；终端代理＋802.1X；终端代理＋802.1X＋安全接入控制网关。

5.2.2 接入控制方式

1. 安全接入控制网关方式及特点

安全接入控制网关 SACG 是 Secospace 主推的接入控制方案，该方案同 802.1X、DHCP、ARP 等方式相比优势明显。安全网关是各种技术有趣的融合，具有重要且独特的保护作用，其范围从协议级过滤到十分复杂的应用级过滤。防火墙主要有三类，分别为分组过滤、电路网关、应用网关三类。安全网关在应用层和网络层上面都有防火墙的身影，在第三层上面还能看到 VPN 作用。安全接入控制网关 SACG、电信级硬件网关设备，提供对终端的安全接入控制，部署和维护简单，安全可靠、性能卓越。

SACG 是由一个路由器和一个处理机构成的安全网关，两个部件结合在一起后，它们可以提供协议、链路和应用级保护。这种专用的网关不像其他种类的网关一样，需要提供转换

功能。作为网络边缘的网关，它们的责任是控制出入的数据流。显然，由这种网关连接的内网与外网都使用 IP 协议，因此不需要做协议转换，过滤是最重要的。保护内网不被非授权的外部网络访问的原因是显然的。控制向外访问的原因就不那么明显了。

SACG 是在华为电信级防火墙硬件平台上开发的专用的接入控制网关，通过基于角色的 ACL 规则(UCL)动态将用户关联到可以访问的认证后域，未通过身份认证和安全检查前，使用认证前域对应的 ACL 规则进行数据包的过滤，限制用户访问的网络资源。

安全接入控制网关方案的最大优点是可实现基于角色的网络访问权限控制；而且部署和实施简单，采用侧挂或直挂的方式，不改变现网拓扑结构。

电信级的安全标准，服务器支持资源池方式，SACG 双机热备支持逃生道，SC 与 SACG 维持心跳，当服务器异常时 SACG 可自动根据业务优先或安全优先，开放或关闭所有网络权限控制。

安全接入控制网关方式的特点是：基于用户角色的访问权限控制；不改变现网拓扑结构，部署维护简单；电信级安全标准，高可靠性；支持逃生通道，可自动恢复故障。

SACG 接入认证的原理和流程如图 5.3 所示。

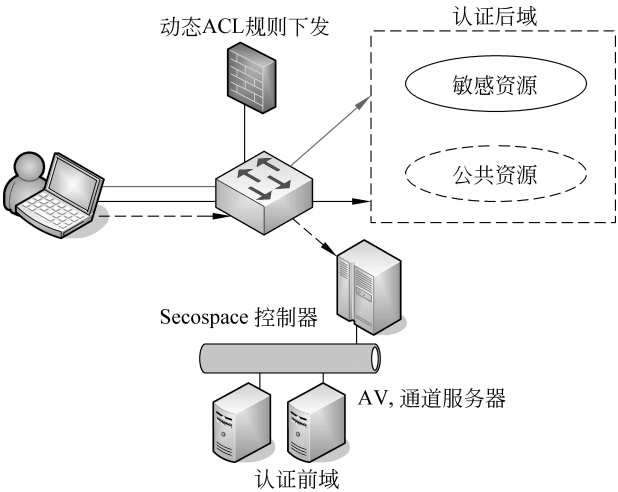

图 5.3　安全接入控制网关方式

(1) 用户终端接入企业标准网络时，Secospace 代理会与 SC 控制服务器建立一个 SSL 通道，用于保护 Secospace 代理 SA 和服务器之间的通信。

(2) SA 与服务器协商认证的参数以及 License 控制信息，进行 Liscense 验证。

(3) 执行身份认证流程。SA 根据采用的身份认证类型(用户名＋口令/AD 域集成认证等)，将用户名/口令信息上报至服务器进行身份认证；如果是域认证方式(如 AD\ED 和第三方 LADP 系统等)，Secospace 将与域管理服务器联动，使用域系统作为统一第三方认证源，用户无须再次输入用户名/口令即可成功认证。

(4) SA 向服务器请求更新安全策略，获得最新的策略信息列表，根据策略执行本地安全策略检查，最后将结果上报 SC。

(5) SC 收到安全认证的结果，判断是否符合策略规定的接入要求，如果满足，则与 SACG 联动，通过用户的身份属性匹配 ACL 规则，把对应的终端从认证前域切换到认证后

域，实现最小授权访问的目的；用于保护 Secospace 代理 SA 和服务器之间的通信。

2. 802.1X 接入控制方式

802.1X 是一种基于端口的网络接入控制技术，起源于 802.11 协议，制订 1X 协议的初衷是为了解决无线局域网用户的接入认证问题。

在它的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而可以实现业务与认证的分离，SC 和以太网交换机利用不可控的逻辑端口共同完成对用户的认证与控制，业务报文直接承载在正常的二层报文上通过可控端口进行交换。802.1X 接入控制方式简化了 PPPOE 方式中对每个数据包进行拆包和封装等烦琐的工作。所以 802.1X 封装效率高，消除了网络瓶颈，对设备的整体性能要求不高，可有效降低建网成本。

Secospace V1R2 C02 中与数通交换机联动，通过对动态 VLAN 和动态 ACL 规则下发的支持，解决不同用户角色的访问权限控制，并能隔离不安全终端到隔离域接受安全修复，解决 R1 版本 1X 方案的局限。

如图 5.4 所示，新的 1X 方案中增加了隔离域的概念，不仅能防止不安全终端对后域的威胁，同时能起到保护其他未通过认证终端的作用。1X 的另一个优点是安全性较高，抗攻击力强，认证通过前端口处于关闭状态，使终端无法访问认证后域。但是 1X 也有其固有的局限性，由于要在每台交换机上做配置，实施和日常维护相对复杂；因为存在单点故障，方案的可靠性不高，故障恢复需要手动关闭 1X。

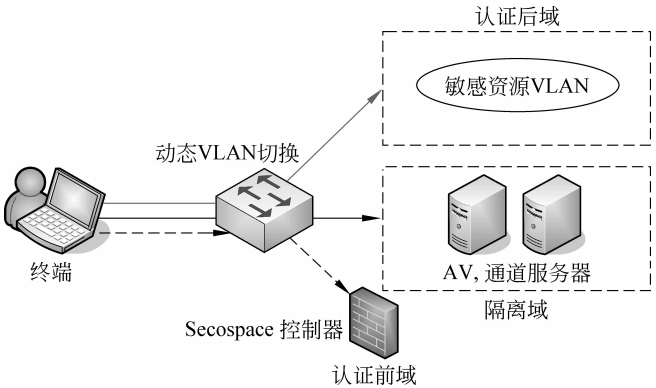

图 5.4　802.1X 接入控制方式

因此，该方案适用于网络规模较小，物理位置相对集中的场景；要求接入层设备都支持 802.1X 协议；可以满足内部员工、临时雇员和合作伙伴的接入控制；对管理员的网管水平要求高。

802.1X 接入控制方式的特点是二层协议，对设备的整体性能要求不高，可有效降低建网成本。基于用户角色的访问权限控制（动态 VLAN、ACL 下发）；认证与业务分离，安全性高，认证通过前无法访问网络；提供隔离域，防止威胁其他终端。

3. 主机防火墙接入控制方式

主机防火墙接入控制方式是 Secospace V1R2C 01 中实现的核心功能点，方案设计的应用场景是与 SACG 控制方式结合，提供有效的局域网内终端的互访控制。当然，该方案也可独当一面，通过单独部署实现独立的网络准入和终端互访保护。

主机防火墙接入控制方式适用于网络层次不太清晰、服务器分散的中小型网络。内部员工、临时雇员、合作伙伴要求部署和维护工作量投入有限，如图 5.5 所示。

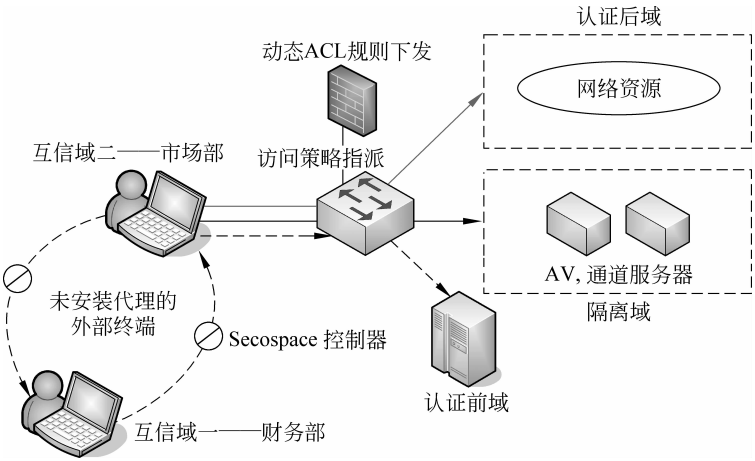

图 5.5　主机防火墙接入控制方式

主机防火墙接入控制方式的特点是有效控制局域网内终端互访行为；提供隔离域，防止威胁其他终端；纯软件控制方式，效率高，配置灵活，部署和维护简单；支持逃生通道，可自动恢复故障。

4. 不同场景和角色实现网络接入保护

主机采用硬件安全接入网关方式接入网络，旁挂在汇聚层交换机上，安装了 Secospace 代理的市场部员工，在通过身份认证和安全策略检查后可正常接入网络，访问企业的公共资源；财务部员工终端上没有安装代理，由 SACG 提供 Web 推送功能，当员工打开浏览器访问网站时，可通过 URL 重定向的方式重定向到定制的 Web 页面上下载 Secospace 代理，员工安装 SA 后即可通过接入控制流程，最终获取相应资源的访问权限，如图 5.6 所示。

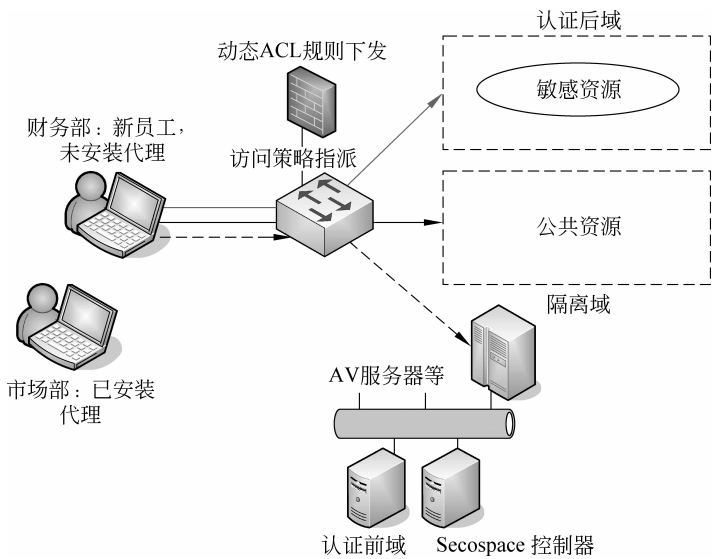

图 5.6　硬件安全接入控制网关方式

在这里了解到 Secospace V1R2 C01 中实现的又一亮点：支持 CA 认证，用于鉴别用户身份，Secospace 可支持所有遵循 X.509 标准的数字证书，可以很好地满足目前研究所、金融和涉密单位的需求。

同样，Secospace V1R2 C01 还可采用主机防火墙接入控制方式，通过指派 IPSec 策略，建立不同互信域，如财务部终端作为互信域 1、市场部作为互信域 2，即使都通过了安全检查，不同互信域间也不可互访。与此同时，对于未安装代理的外部终端或未通过身份认证和安全检查的非可信终端也不可访问通过安全检查的可信终端。这样就能有效阻止不安全终端对安全终端的互访行为，如共享目录就能够使局域网中的设备免遭病毒及蠕虫等攻击。

最后还可采用 802.1X 接入控制方式，未通过身份认证和安全检查前，交换机端口处于关闭状态，终端不可访问局域网内的领域终端，检查通过后通过交换机动态切换 VLAN，控制终端可访问的认证后域，实现基于不同用户角色的网络访问控制，如图 5.7 所示。

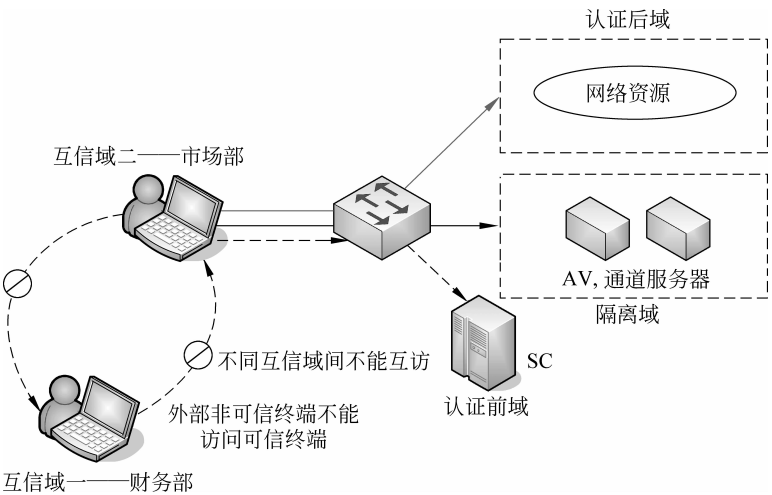

图 5.7　主机接入防火墙控制方式

下面描述用户非常关注的临时访客接入场景。这也是 Gartner 研究报告调查显示 80% NAC 项目的第一驱动因素：如何为访客提供安全的内部网络服务？

在这里推荐通过 SACG＋ActiveX 或 Web 的接入控制方式。一般临时访客的接入方式比较多样，如通过网线直接接入公司内部网口或交换机，或者通过无线网卡接入。由于临时访客往往不愿意安装代理，Secospace V1R2 C01 提供了 ActiveX 认证，用户只需要通过 SACG 提供的 URL 重定向下载 ActiveX 控件，迅速通过访客公共账号实现接入。如果用户的操作系统是 Mac 或者 Unix，也可通过 SACG 提供的 URL 重定向进行 Web 认证。但是要注意 Web 认证方式只能实现单纯的身份认证和接入控制，由于终端没有代理，安全策略检查和后面将要介绍的员工行为管理、资产管理等都无法实现。但这对于满足访客的内网接入控制需求足矣。

最后是远程办公、合作伙伴 VPN 接入场景。同样采用 SACG＋ActiveX/Web 的接入控制方式，在用户通过 VPN 接入后，SACG 分别给合作伙伴或远程办公用户提供 Web 推送，通过 URL 重定向下载 ActiveX/Secospace 代理，或直接通过 Web 认证方式接入。但要注意远程办公、合作伙伴 VPN 接入要求 VPN 没有做 NAT 网络地址转换；否则就会出现一

个用户通过认证，其他 VPN 用户都可以直接接入网络的情况。

5.2.3 华为终端管理安全管理策略与安全性检查

安全策略管理和员工行为管理也是 Secospace 相比于友商的突出优势。Secospace 提供业界最丰富的安全策略，各类检查类、网络行为监控和移动存储、外设管理等，全面评估端点安全状态，强制企业 IT 策略遵从，并持续监控，主动消除各种已知和未知威胁，如财务部由于经常访问企业敏感的财务信息，可以制定严格的安全策略模板，实行严格的策略检查和准入，防止恶意攻击。总裁办公室则可制定相对宽松的安全策略模板，满足基本的准入条件即可接入企业标准网络。

业界最丰富的安全策略是强制企业 IT 策略遵从主动评估终端安全状态，强制终端策略遵从。自动发现终端漏洞，消除已知和未知威胁。量体裁衣，基于角色的动态管理策略控制方式是根据用户角色或部门自定义不同安全规则，针对不同控制点采取的不同策略。那么安全策略管理为客户解决的问题又有哪些呢？像人性化的安全策略管理（灵活选择实施的安全策略内容；灵活选择策略执行类型为强制或非强制；灵活选择策略实施对象），全面的企业安全策略，全面提升企业信息安全水平，提高效率等。

终端安全性检查可以由审计人员通过下达审计监控任务，对用户终端的安全性状况进行检查，并生成审计报表；也可以由用户发起进行本机自检，显示出来检查结果，让用户了解本机安全状况，帮助用户提高本机安全性，防止无意泄密。

华为终端安全性检查的基本流程依次为：获取计算机终端基本配置信息、检查分区表信息、检查共享目录、获取终端硬件信息、获取终端进程信息、检查屏保设置信息、检查安装软件、检查 Windows 补丁、检查其他软件补丁。

那么，如何进行华为终端安全性检查呢？首先要获取计算机终端的基本配置信息、检查分区列表和共享目录，获取终端硬件信息和进程信息，之后再检查屏保设置信息，信息无误后安装软件和 Windows 补丁，安装完成后进行防泄密检查，并用 USB 存储设备监视，最后进行屏幕监控。下面来看一下具体的操作步骤。

（1）获取计算机终端基本配置信息。可以获得机器的 IP 地址信息、MAC 地址信息、主机名、操作系统版本信息。

（2）检查分区表信息。可以检查分区数量，分区大小，分区类型，是否隐藏分区。如果有违规分区将用红色显示。

（3）检查共享目录。可以检查共享名，共享目录路径，是否设置密码。如果有违规目录将用红色显示。

（4）获取终端硬件信息。可以获取机器的基本硬件配置信息。

（5）获取终端进程信息。可以获取机器目前的进程信息。

（6）检查屏保设置信息。可以检查屏保是否设置密码，屏保启动时间，根据策略判断启动时间是否符合要求；如果有不符合策略文件的将用红色显示。

（7）检查安装软件。可以通过注册表检查已安装的软件，根据策略文件判断软件为合法、非法等类型。如果缺少必装软件或有违规软件将用红色显示。

（8）检查 Windows 补丁。通过注册表检查已安装的 Windows 补丁，根据策略文件判断有没有没装的要求补丁。如果没有将用红色显示。