<<网络准入控制概论>>

图书基本信息

书名：<<网络准入控制概论>>

13位ISBN编号：9787030352576

10位ISBN编号：7030352572

出版时间：2012-8

出版时间：科学出版社

作者：聂元铭，董建锋，周小平　著

页数：224

字数：285000

<<网络准入控制概论>>

内容概要

《网络准入控制概论》系统研究了网络准人控制技术(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人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。

《网络准入控制概论》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。

<<网络准入控制概论>>

书籍目录

章节摘录

Web认证同802.1x认证相比，具有应用简单的优势。
但是，在EAD解决方案中，需要使用客户端进行终端的安全状态检测和控制，因此在Web认证的基础上，扩展了PORTAL协议，使之不仅能够处理Http协议，还可以控制其他协议的数据流，使EAD解决方案也支持PORTAL认证方式下的端点准入控制。
这种方式和NAC系统的NAC Appliance基本类似。
4.4.2 EAD的工作流程 如上所述，EAD准入控制系统，通过安全客户端、安全策略服务器、网络设备以及第三方安全系统的协同，对接入网络的用户终端实施安全策略管理。
以下为实现终端安全准入的流程。
Step1：用户终端试图接入网络时，终端计算机首先通过安全客户端上传用户信息至安全策略服务器进行身份认证，非法用户将被拒绝接入网络。
Step2：合法用户将被要求进行安全状态认证，由安全策略服务器验证用户终端安全状态是否符合基于用户账号预定义的安全策略，包括补丁版本、病毒库版本是否合格，软件安装允许是否合格、是否使用代理服务器等信息，不合格用户将被智能联动设备隔离到隔离区。
Step3：进入嗝离区的用户可以根据安全策略，通过第三方服务器进行安装系统补丁、升级病毒库、检查终端系统信息、卸载非法程序、取消代理设置等操作，直到接入终端符合安全策略。
Step4：安全状态合格的用户将实施由安全策略服务器根据不同用户的角色下发不同的安全设置，并由安全联动设备提供基于身份的网络服务。
从EAD的主要工作流程和基本原理可以看出，EAD将终端防病毒、补丁修复等终端安全措施与网络接入控制、访问权限控制等网络安全措施整合为一个联动的安全体系，通过对网络接人终端的检查、隔离、修复、管理和监控，使整个网络变被动防御为主动防御；变单点防御为全面防御；变分散管理为集中策略管理，提升了网络对病毒、蠕虫等新兴安全威胁的整体防御能力。
4.4.3 EAD的主要特点 以下阐述EAD系统的主要特点。
1.严格的身份认证 除基于用户名和密码的身份认证外，EAD还支持身份与接人终端的MAC地址、IP地址、所在VLAN、接人设备IP、接人设备端口号等信息进行绑定，支持智能卡、数字证书认证，增强身份认证的安全性。
2.完备的安全状态评估 根据管理员配置的安全策略，用户可以进行的安全认证检查包括终端病毒库版本检查、终端补丁检查、终端安装的应用软件检查、是否有代理、拨号配置等；为了更好地满足客户的需求，EAD客户端支持和微软SMS、LANDesk、BigFix等业界桌面安全产品的配合使用，支持和瑞星、江民、金山、Symantec、Maeafee、Trend Micro、Ahn等国内外主流病毒厂商联动。
例如EAD可充分利用微软成熟的桌面管理工具，由SMS实现各种Windows环境下用户的桌面管理需求：资产管理、补丁管理、软件分发和安装等。

<<网络准入控制概论>>

版权说明