解决方案：华为3Com金融业端点准入防御解决方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/202/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_202923.htm 端点准入防御(EAD，Endpoint Admission Defense)解决方案从网络接入端点的安全控制入手，通过安全客户端、安全策略服务器、网络设备以及第三方软件的联动，对接入网络的用户终端强制实施企业安全策略，加强网络用户终端的主动防御能力，并严格控制终端用户的网络使用行为，保护网络安全。 概述 在互联网技术的发展应用过程中，伴随着网络应用软硬件技术的快速发展，网络信息安全问题日益严重，新的安全威胁不断涌现，特别是金融行业、其数据的特殊性和重要性、更成为黑客们攻击的重要对象，针对目前金融系统计算机犯罪频率越来越高，手段越来越复杂，银行损失金额越来越大。 目前金融系统网络安全威胁主要有： 1.通过攻击接口进行非法入侵 ：根据各级局域网、广域网、及服务器接口的情况，可以通过下面几种方式进行攻击：业务系统拒绝服务；通过猜测获得内部主机其他服务的访问权限；内部网络拓扑信息外泄；局域网中数据的截获。 2.针对系统自身存在缺陷进行攻击：利用系统(包括操作系统、支撑软件及应用系统)固有的或系统配置及管理过程中的安全漏洞，穿透或绕过安全设施的防护策略，达到非法访问直至控制系统的目的，并以此为跳板，继续攻击其他系统。此类攻击手段包括隐通道攻击、特洛伊木马、口令猜测、缓冲区溢出等。 网络安全问题的解决，三分靠技术，七分靠管理，严格管理是金融机构及用户免受网络安全问题威胁的重要措施。根据调查表明，网络安全的威

胁60%来自网络内部，网络用户不及时升级系统补丁、升级病毒库的现象普遍存在；私设代理服务器、私自访问外部网络、使用网络管理员禁止使用的软件等行为在金融系统内部网络中也比比皆是。如果只是通过防火墙和在网络设备上配置一系列访问控制策略是无法完全避免各种安全威胁的，而必须从用户接入终端-网络设备-中心服务器提供一系列端到端的安全解决方案。所以首先要从网络接入端点的安全控制入手，对接入网络的用户终端强制实施企业安全策略，加强网络用户终端的主动防御能力。 针对接入层用户的安全威胁，特别是来自应用层面的安全隐患，防止黑客对核心层设备及服务器的攻击，我们必须在接入层设置强大的安全屏障，华为3Com公司推出了端点准入防御(EAD)解决方案，该方案从网络用户终端准入控制入手，整合网络接入控制与终端安全产品，通过安全客户端、安全策略服务器、网络设备以及第三方软件的联动，对接入网络的用户终端强制实施企业安全策略，严格控制终端用户的网络使用行为，加强网络用户终端的主动防御能力，保护网络安全。 EAD简介 原理 EAD解决方案提供企业网络安全管理的平台，通过整合孤立的单点防御系统，加强对用户的集中管理，统一实施企业网络安全策略，提高网络终端的主动抵抗能力。其基本原理图如下：EAD系统由四部分组成，具体包括安全策略服务器、安全客户端平台、安全联动设备和第三方服务器。 安全策略服务器是EAD方案中的管理与控制中心，是EAD解决方案的核心组成部分，实现用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能。目前华为3Com公司的CAMS产品实现了安全策略服务器的功能，该系统在全面

管理网络用户信息的基础上，支持多种网络认证方式，支持针对用户的安全策略设置，以标准协议与网络设备联动，实现对用户接入行为的控制，同时，该系统可详细记录用户上网信息和安全事件信息，审计用户上网行为和安全事件。 安全客户端平台是安装在用户终端系统上的软件，该平台可集成各种安全厂商的安全产品插件，对用户终端进行身份认证、安全状态评估以及实施网络安全策略。 安全联动设备是企业网络中安全策略的实施点，起到强制用户准入认证、隔离不合格终端、为合法用户提供网络服务的作用。CAMS综合接入管理平台作为安全策略服务器，提供标准的协议接口，支持同交换机、路由器等各类网络设备的安全联动。 第三方服务器为病毒服务器、补丁服务器等第三方网络安全产品，通过安全策略的设置实施，第三方安全产品的功能集成至EAD解决方案种，实现安全产品功能的整合。 EAD原理图示意了应用EAD系统实现终端安全准入的流程： 1. 用户终端试图接入网络时，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用户身份认证，非法用户将被拒绝接入网络；2. 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补丁版本、病毒库版本等信息是否合格，不合格用户将被安全联动设备隔离到隔离区；3. 进入隔离区的用户可以根据企业网络安全策略，通过第三方服务器进行安装系统补丁、升级病毒库、检查终端系统信息等操作，直到接入终端符合企业网络安全策略；4. 安全状态合格的用户将实施由安全策略服务器下发的安全设置，并由安全联动设备提供基于身份的网络服务。 