构筑纵深的智能网络安全防御体系思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E6_9E_84_E7_AD_91_E7_BA_B5_E6_c101_644244.htm GSN全局安全解决方案通过软硬件的联动、计算机层面与网络层面的结合，从入网身份、客户端PC、网络通信等多个角度对网络安全进行监控、检测、防御和处理，帮助用户构建起具有战略纵深的全局安全网络防线，保障金融企业的网络安全。 在战争中，一条没有纵深的防线在出现单点突破后就会土崩瓦解。而构建了多重防线也有可能由于缺乏防线之间及时智能的协调，抵御攻击的效率大打折扣。因为各个防线上的士兵各自为战，在一条防线被突破后不能组织有效的反击. 网络安全挑战 近年来，随着业务量的不断增长和新兴业务的持续涌现，金融企业网络内部的应用行为趋向复杂。同时，随着频频变种的病毒、木马、恶意攻击的层出不穷，我们与这些威胁的战争也一直在进行。划分安全区域，部署防火墙进行边界防护的传统做法已经被大部分企业采用.应对终端PC的病毒，部署防病毒软件和防毒墙等设备.针对网络内部的安全事件审计，又部署了大量的IDS设备.为了实现客户端PC的应用管理，又要求安装Windows AD或者专业桌面管理软件……企业在网络安全建设方面，投入大量的精力和资金，在各级机构部署了大量系统，构筑起越来越多的防线。 在日趋复杂的安全威胁面前，我们采取的措施的确可以面面俱到。但是应用的各个产品和方案通常是“ 自扫门前雪 ”，异构等问题也导致构成的多重防线很难得到统一的调度管理。一旦遇到单一产品/方案处理不力，就会造成管理失控，甚至给业务造成严重影响

，给网络管理者带来巨大的管理压力。 例如，在某金融企业的某个局域网中，一次ARP欺骗攻击的发生造成某个区域局域网用户大面积业务中断。由于病毒脚本的隐蔽性，防病毒软件无法有效地进行处理，交换机的CPU占用率在大量异常ARP报文涌入后急剧升高造成了管理困难，防毒墙和防火墙部署在边界无法发挥作用，IDS相关报告的事件数量达到了天文数字却无法进行处理，网络管理者守着一堆的安全系统和设备，却只能一再重复地进行手工查找处理，“ 望毒兴叹 ”。 如何综合现有的网络安全方案和手段，构建一道既有战略纵深、又能进行智能联动的网络安全方案呢? 锐捷GSN方案概述 锐捷网络基于多年服务于金融行业网络规划和建设的经验，以及在网络准入安全方面的深入研究和成熟应用，应对金融行业网络安全挑战，推出了 GSN(Global Security Network)全局安全网络解决方案。该方案采用用户身份管理体系，端点安全防护体系和网络通信防护体系三道防线的构筑，实现了网络安全的战略纵深，确保了金融企业的网络安全。 为了实现传统网络设备与专业安全系统的统一联动，锐捷网络GSN全局安全解决方案，融合软硬件于一体，通过软件与硬件的联动、计算机领域与网络领域的结合，帮助用户实现全局安全。GSN是一套由软件和硬件联动的解决方案，它由后台的管理系统、网络接入设备、入侵检测设备以及安全客户端共同构成。 