

思科防火墙销售指南 之成功案例篇

思科为“杭州国家软件产业基地”顺利实施一体化网络安全解决方案

目前我国拥有国家级的软件产业基地11个,如何给这些软件产业基地中的企业提供安全可靠的网络环境,是每个软件产业基地非常关心的问题。杭州国家软件产业基地在解决园区城域网的网络安全问题时,既没有购买大量的防火墙、IDS等网络安全设备,也没有对网络结构进行任何改变,而是采用了思科简单有效的一体化网络安全解决方案,通过给网络中的Catalyst 6509交换机集成各种网络安全模块,一举消除了软件产业基地城域网的各种安全隐患。杭州国家软件产业基地的作法为其它软件产业基地的网络安全建设提供有益的借鉴。

杭州国家软件产业基地是我国重点发展的11个国家级软件产业基地之一,在杭州政府“构筑天堂硅谷,建设科技新城”方针的指引下,杭州国家软件产业基地发展迅速,并在短期内形成了自己鲜明的专业化的特色。

截止2002年11月底,杭州国家软件产业基地已经有软件企业620家,软件园企业89家,科技部认定的骨干软件企业10家。为了更好地服务于这些企业并吸引更多的软件企业来软件产业基地发展,杭州国家软件产业基地有限公司经国家发展计划委员会批

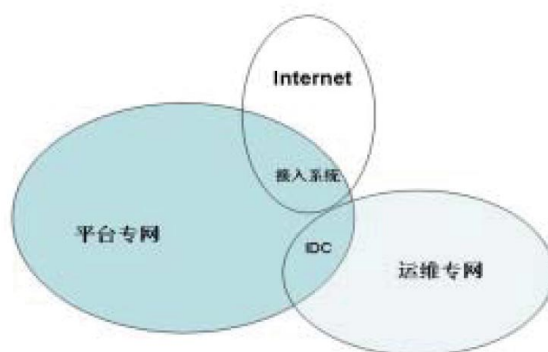
准,开始了“国家软件产业基地(杭州)网络建设项目”。其中“公共服务与技术支持平台”的建设最终将建成环绕杭州城的高速双向光纤专网,把坐落在市区范围内的各软件园区、企业聚集的商务楼宇及相关高校科研机构等联接起来。

支撑平台作用重要 网络安全需求突出

作为杭州国家软件产业基地的IP城域网,公共服务与技术支持平台的作用非常重要,不但要为软件园区、企业单位、学校等提供高速的接入服务,同时还要提供网络测试专业实验室、VPN连接、IDC主机托管、电子教学、企业邮局系统、基地封闭式开发实验室等增值服务。

国家软件产业基地网络系统逻辑图如下:

国软基地平台网络系统逻辑结构图





从系统逻辑图可看出，公共服务与技术支持平台是三个系统中规模最大、最基础的系统，大部分系统及设备都在支撑平台专网运行。由于所有的数据都要通过支撑平台的骨干网络进行转发，如果支撑平台出现安全问题，那么整个软件基地的网络系统将会有瘫痪的危险，所以支撑平台必须具备极高的安全性和可靠性。另外随着支撑平台网络的不断扩展以及接入支撑平台的软件企业的迅速增加，可以预见，支撑平台网络系统的安全风险也将会变得日益严重和复杂。基于以上考虑，杭州国家软件产业基地有限公司对支撑平台的网络安全建设提出了非常高的要求，把可靠性和安全性作为整个支撑平台网络建设的最高原则。

思科一体化网络安全解决方案获得一致认可

为了确保整个网络系统建成后的安全和稳定，杭州国家软件产业基地有限公司进行了严格的招标活动，经过认真的比较和分析，最后杭州国家软件产业基地有限公司决定全面采用思科系统公司这种独具特色的一体化网络安全方案。思科系统公司是全球知名的互联网设备和解决方案供应商，同时也是业界领先的网络安全设备和解决方案供应商。思科系统公司在透彻研究网络的基础上，通过在所有产品中都集成安全特性来打造一体化的网络安全。具体地说，就是思科公司除了提供防火墙等专用的安全产品外，还在路由器、交换机、无线网络设备等产品中都集成安全特性，从而保护网络上每个节点的安全。一体化网络安全解决方案可以做到融安全于网络中，不会在网络中留下安全死角，同时还具有实施方便、扩展灵活、保护投资等特点。思科一体化网络安全解决方案先进的安全理念得到了负责招标的专家和领导的一致好评。

思科为杭州国家软件产业基地实施的一体化网络安全方案主要是借助思科先进的交换机产品Catalyst 6509实现的。Catalyst 6509 是思科公司最新的交换机产品，作为业界领先的交换机平台，Catalyst 6509 交换机可以高度集成思科各种网络安全硬件模块，包括防火墙服务模块、IP 安全虚拟专用网（IPSecVPN）服务模块、入侵检测系统模块和网络分析模块（NAM）。如果将这些安全模块结合在一起使用，客户将能够在交换机上部署综合安全性，而无需分别管理的不同设备。

自上而下、层次鲜明，思科一体化网络安全解决方案顺利实施

思科根据软件产业基地网络系统的结构，制定了“自上而下”的方案实施原则，首先确保运维系统内网的安全，其次保证 IDC 机房、实验室及公共服务系统的安全，最后保证外网接入的安全。

为了保证运维系统的独立性及安全性，在网络建设后期从浙江通信单独租用 SDH 线路，连接世导、国软及联合，形成一个独立的内网。运维专网采用单独的 IP 地址与路由设计，保证安全。另外，在运维系统中安装 VMS 安全策略管理服务器，对全网的安全策略进行统一管理及监控。在世导 Catalyst 6509 交换机上安装 VPN 模块，提供外网的 VPN 接入终结。同时安装一台 ACS 身份认证服务器，提供对 VPN 拨入用户的认证、记账及权限策略分配。

在世导 Catalyst 6509 交换机上配置防火墙模块 FWSM，将 IDC 主机托管系统、平台骨干网连接、运维内网连接及 Internet 接入进行安全隔离。将 6509 交换机上的 5 个千兆及百兆接口配置为防火墙端口，同时分配名称，其中 Outside 口连接世导的 Internet 接入，Dmz1 口连接平台骨干网络、Dmz2 连接 IDC 机房的

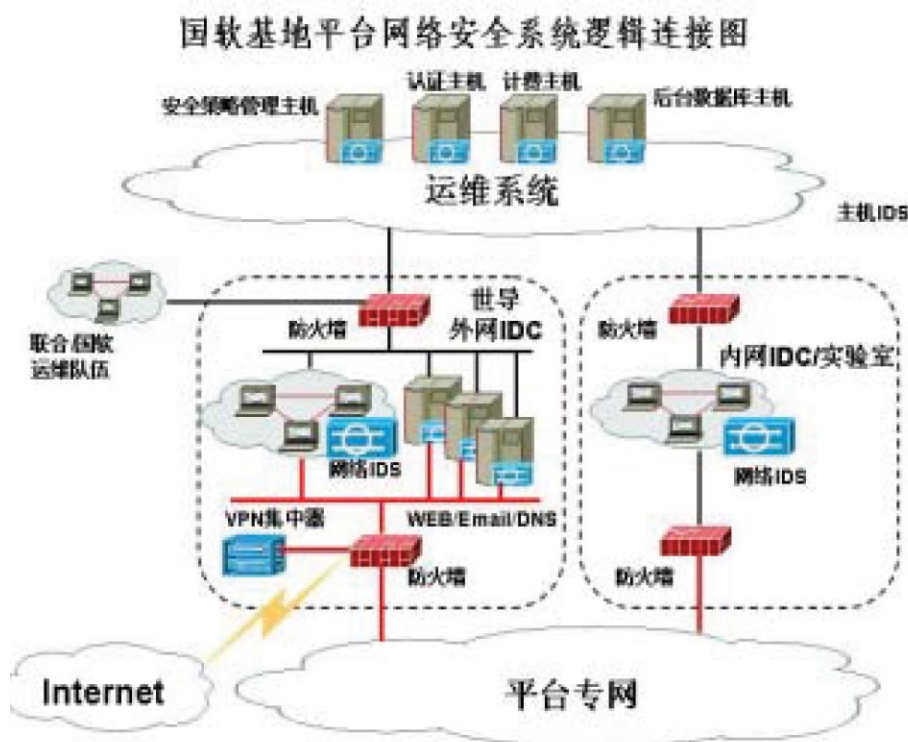


服务器群、DMZ3连接身份认证系统，Inside口连接运维内网接入。将5个四个接口权限设置为：Outside为0、dmz1为40、dmz2为60、dmz3为80、Inside为100（最高）。在国软6509上配置防火墙模块FWSM，将综合测试实验室及公共服务平台、平台骨干网连接、运维内网连接进行安全隔离。为分别连接四个区域的3个千兆及百兆接口分配名称，其中Outside口连接平台网络接入，Dmz1口连接综合实验室，Inside口连接运维内网接入。将3个四个以太网权限设置为：Outside为0、dmz1为50、Inside为100（最高）。

在世导及国软的6509交换机上安装网络入侵检测IDS模块，提供对多个网络的入侵检测。同时与防火墙模块实现联动，一旦发现网络中存在攻击行为或是非正常数据包，立即报告安全管理中心，同时在防火墙上动态增加安全策略，对攻击行为进行隔离。

在接入网系统上，利用分布到各大楼的3550交换机提供的PrivateVLAN技术和安全访问控制列表ACL等安全交换技术，同时通过合理的IP地址分配策略和路由策略，提供对接入企业的安全控制。

方案实施的拓扑图如下：





思科的网络安全发展之路

思科一体化网络安全解决方案得到了国家软件产业基地的认可，可是作为设备供应商的思科公司，能够担任起网络安全的重任呢？

2003年堪称计算机病毒年，可是令人感到尴尬的是，对那些专业信息安全厂商来说，虽然自己一再声称能帮助用户解决网络攻击问题，但在新型攻击面前，自己却基本上无能为力，架设的防线形同虚设。就在人们困惑担忧的时候，一些老牌但却属于新生的力量站了起来。就像思科，众所周知，思科是全球著名的网络设备和解决方案的提供商，相对于专业信息安全厂商对网络理解的匮乏，思科则是这方面的专家，它掌握着网络底层协议和关键技术，从而能够做到操作系统、网络基础架构牢不可破，坚如磐石！

2003年11月，思科在全球发布了网络准入控制(Network Admission Control)计划，该计划是思科自防御网络计划(Self-Defending Network, SDN)的重要组成部分，是一套高度集成的一体化网络解决方案。思科自防御网络计划是一个创新的、多侧面的网络安全战略，其目标是提高网络发现、防御和对抗安全威胁的能力。网络准入控制(Network Admission Control)是思科自防御网络计划的重要组成部分。其核心思想是，控制访问权限，有效阻止不符合安全条件的设备及访问进入网络，并将其置于某个隔离区域之外，或者仅获得对计算资源的有限访问权限。网络接入控制与思科公司关于网络安全的其它技术，如入侵检测、防火墙、网络管理与流量分析、VPN等加在一起，就构成了自防御网络的全部内涵。

思科网络接入控制是通过与业内厂商合作来实现的，2003年11月，思科宣布与NAI、Symantec、Trend Micro三家国际反病毒软件厂商合作，通过思科安全代理软件(Cisco Security Agent)与防病毒软件的配合，将思科对网络恶意行为的防御能力延伸到服务器和PC端点上。2004年2月，思科又与IBM达成类似的合作，IBM将在其笔记本电脑和Tivoli网络软件两端支持自防御网络计划。思科今后还将把网络接入控制计划向更多的厂商和机构开放，与业界广泛合作，共同编织出一张抵御任何恶意行为的防护网。

思科在你身边 世界由此改变



思科系统 (中国) 网络技术有限公司

北京

北京市东城区东长安街一
号东方广场东一办公楼
19-21 层
邮政编码: 100738
电话: (8610) 65267777
传真: (8610) 85181881

广州

广州市天河北路 233 号中信
广场 43 楼
邮政编码: 510620
电话: (8620) 87007000
传真: (8620) 38770077

上海

上海市淮海中路 222 号力宝
广场 32-33 层
邮政编码: 200021
电话: (8621) 33104777
传真: (8621) 53966750

成都

成都市顺城大街 308 号冠城
广场 23 层
邮政编码: 610017
电话: (8628) 86758000
传真: (8628) 86528999

如需了解思科公司的更多信息, 请浏览 <http://www.cisco.com>

2003 年思科系统 (中国) 网络技术有限公司北京印刷, 版权所有。

2003© 思科系统公司版权所有。该版权和 / 或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS 标识, Cisco Systems, Cisco Systems 标识, Cisco Systems Cisco Press 标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌、名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。