夯实网络基础，加快前进步伐
——广东发展银行携手思科建设立体的网络安全防御体系

根据WTO的有关条款，中国银行业在进入WTO后拥有五年的过渡期。毋庸质疑，在五年过渡期结束后，中国银行业的竞争将会异常激烈。巨大的冲击，要求中国银行业在有限的时间内作好与国际银行业进行全面竞争的准备。为了应对竞争，目前国内各大商业银行纷纷加强自身的信息化建设，通过建立新一代的通信网络平台，来提高服务水平和管理水平，以迎接未来的挑战。广东发展银行自1988年正式成立以来，一直非常重视银行的信息化建设。经过多年的努力，目前广东发展银行已经逐步建立起基于IP技术的业务骨干网，实现了数据集中化，应用、系统、网络统一化。

从1998年开始，广东发展银行就一直选择思科系统公司来进行自身的网络建设，多年来的成功合作，已经使得思科公司与广东发展银行成为了网络领域内的紧密合作伙伴。广东发展银行最初的网络安全体系就是依据思科SAFE蓝图部署的。由于SAFE主张网络安全建设不能一蹴而就，而应该是一个动态的过程。所以在最初的部署中，思科主要协助广东发展银行解决了最突出的网络安全问题——网络对外连接出口的安全问题。具体地说就是在广东发展银行的总行和分行都设有思科的PIX防火墙，这些防火墙在各自的管理员的管理下，分别把守网络对外连接的出口，确保各自出口的边缘网络安全。

网上业务迅速增长，安全体系急需加强

随着广东发展银行业务的迅速发展，尤其是近年来，用户纷纷把业务转移到网上进行，广东发展银行的网上业务呈几何数字增长。在这种情况下，广东发展银行提出，为了更好地抵御网上的非法访问，作好关键用户的网上认证，确保能够给用户提供不间断的高质量金融服务，必须要在原有的基础上进一步加强银行在网络安全方面的部署。具体地说就是要尽快为全行制定一个统一的、立体的网络安全策略，来应对潜在的网上风险。

广东发展银行网络安全体系的改造吸引了国内外各大安全厂商参与竞标，最后广东发展银行再次选择思科作为改造的承建方。思科的再次胜出主要有两个原因：首先是广东发展银行对以前思科依照SAFE构筑的安全体系和思科的网络安全产品感到非常满意。另外一个原因是，广东发展银行非常认可思科的SAFE蓝图。因为依据SAFE蓝图，思科所提出的改建方案既能满足广东发展银行当前的安全需求，又为未来网络扩展作好了准备，而且还对以前的投资提供

了有利的保护。

各个网段分兵布守，关键网段重兵设防

通过分析广东发展银行的具体业务流程和网络结构，思科在SAFE蓝图指导下，针对广东发展银行的不同网段，分别实施了可以统一管理的不同的安全措施，具体措施如下。

分网段的立体防御

总行数据中心部署了双冗余的PIX535放火墙，把总行网络分成多个隔离网段：企业内部各功能网、外联网、INTERNET等。通过防火墙的隔离，防止了跨网攻击、网络间干扰等安全问题，同时病毒的感染范围也可以得到有效控制，使各网段的安全性大大提高。

业务网的核心交换机采用两台带有IDS模块的Catalyst6500高性能交换机，通过IDS模块增强对业务网的安全监控。

OA网是安全的关键部分，也是产生内部安全隐患的主要环节，所以OA网采用两台带有IDS和Firewall模块的Catalyst6500高性能交换机。Firewall模块可以实现虚拟局域网（VLAN）之间的安全隔离，这对于大型的OA网络来说是非常重要的。

广东发展银行的网络系统，包括总行数据中心和分行网络中心，都需要与Internet、网上银行、税银通、银券通及人行清算等多个公共信息网的互连，由于这些公共信息网是一个完全对外开放的信息资源，因此与这些网络的接口成为最易受到“黑客”攻击的环节，需要进行特别的安全控制，提供可靠的安全保障。因此，思科采用了当前业界先进的Cisco PIX防火墙产品和先进、可靠的防火墙技术，为整个网络系统提供可靠的安全防护。PIX所具有的NAT(Network Address Translation)功能可为广东发展银行内部网各工作站提供动态或静态的地址转换，获得合法的外部地址，这样既可对外隐藏内部网络，又能够节省地址资源。

为了提高网络的可靠性，消除单点故障，思科采用两台PIX防火墙用一条Failover电缆相连的措施，执行双机热备份。防火墙作为银行内部网络的唯一出口，提供与Internet等公共信息网互连的安全控制，同时为内部网络各工作站访问外部信息网提供地址转换(NAT)功能。交换机使用MAC地址过滤功能进行安全控制，只允许特定的主机进入PIX。路由器通过多个广域网端口对外连接，并提供一定的安全控制，防止非法的访问和操作。

为了加强对整个网络的控制和管理，思科又为广东发展银行部署了ACS访问控制服务器和安全策

略管理器（Cisco Secure Policy Manager），利用CSPM强大的策略管理基础设施，用户可以对银行网络上的安全产品进行可扩展的、统一的管理。

分层次的一体化的防御

思科SAFE认为，成功的安全解决方案应该在整个网络基础设施上采用集成化保护，而不能只考虑某些专用安全性设备。因此思科在他的各种网络产品上都集成了安全性能，从而确保整个网络实现立体的集成化的安全防御。广东发展银行就实施了这样的立体的集成化的安全防御。以广东发展银行外联网络系统为例，这个网段就采用了包括路由器、防火墙和交换机在内的三层的集成化的安全防御。

1、第一层安全防护由路由器实现

路由器提供于Internet/外联网等公共信息网的广域连接，与广东发展银行的DNS服务器、WWW服务器和E-Mail服务器等一起位于PIX防火墙的外部，这些服务器作为对外开放的一部分，对内部和外部用户提供相应的服务，其本身也成为公共信息网的一部分。为了对这些服务器提供有效的安全保障，防止外部的用户对服务器进行非法操作，对服务器的内容进行删除、修改等破坏，必须对外部访问所能的操作进行严格的控制。利用Cisco路由器所具有的防火墙功能，可限制外部用户对各服务器所进行的操作从而可防止各服务器受到来自外部的破坏。

2、第二层安全防护由PIX防火墙保障

PIX防火墙将企业内部网和外部完全分开，PIX是内部各网络子系统对外的唯一出口。通过使用PIX防火墙隔离内、外网络，更进一步保障了内部网络的安全。

PIX对所有的访问都可提供完整的记录，包括非法入侵尝试。PIX实现了从网络层到应用层的安全保护，可通过对数据包源点地址、目的地址、TCP端口号和包长等因素对通信进行控制，禁止任何非法访问。

3、第三层安全防护由局域网交换机提供

Catalyst 6500核心交换机部署了IDS和防火墙模块，对复杂的内部网进行有效的安全监控，是抵御外部攻击防止的第三道屏障，也是防止内部攻击的有利手段。

另外Catalyst系列交换机具有MAC地址过滤功能，因此可根据需要对交换机的每个端口进行定义，只允许特定MAC地址的工作站通过特定的端口进行访问，与连接PIX的端口进行通信。由于MAC地址的唯一性和不可配置，这种控制实际上是从硬件上对特定的机器进行控制，与对IP地址的过滤相比，这种防护具有更高的安全性。

通过以上三层安全保护，广东发展银行的网络系统实现了从链路层到应用层的可靠的安全控制，有效地防止了外部的非法访问，具有很高的安全性。

服务周到，后顾无忧

为了确保整个网络安全解决方案的顺利实施和运行，思科为广东发展银行提供了周到细致的服务。这些服务包括为安全产品提供长达三年的售后服务，为广东发展银行的有关技术人员提供培训等。尤其值得一提的是，思科还专门为广东发展银行组织了一支由网络安全工程师和金融专家组成的咨询团队，定期到广东发展银行检测整个网络的安全情况并解决具体应用中出现的问题。思科的这种周到细致的服务完全解除了广东的后顾之忧。

在广东发展银行和思科的通力合作下，广东发展银行的网络安全体系改造顺利完成。广东发展银行的网络安全体系由原来的“兵力薄弱且分散”的防御体系，一举越升为一个立体的、可以进行统一管理的大型网络安全防御体系。广东发展银行的有关领导对改建工作给予了很高的评价，表示改建后的网络安全性更高、管理性更强，可以更好地满足广东发展银行开展新型业务及为用户提供24×7×365(366)可靠服务的需要。广东发展银行还进一步表示，思科安全产品的良好扩展性和兼容性，以及思科SAFE蓝图的一贯性，为广东发展银行和思科将来进一步的合作打下了一个很好的基础。

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
23层
邮政编码：610017
电话：(8628)86758000
传真：(8628)6528999

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