集中式安全管理　助新疆移动掌控全局
——思科安全解决方案在新疆移动BOSS系统改造中的成功

业务发展呼唤高效网络

移动通信对信息网络的依赖程度之高，可能是另一些行业无法想象的，仅其业务运营支撑系统（BOSS系统）就运行着计费、结算、营业帐务和客户服务等多项核心业务，这些业务都要求有一个高度稳定、运行顺畅、安全可靠的网络。近年来，在日新月异的信息技术的大力推动下，移动通信业得到了前所未有的蓬勃发展。随着业务量的成倍增长和业务范围的迅猛扩展，中国移动通信新疆公司迫切需要将原有的网络改造，建立一个高性能、高安全性、高可用性、高可扩充性的骨干网络平台，使得它一方面可以承载未来两年（至2003年底）可预见的包括300万用户的多项业务应用，另一方面顺应“大集中”的趋势，实现对全区各州县业务的集中统一管理。

系统改造　安全先行

新疆移动通信公司业务支撑系统(BOSS--Business Operation Support System)由计费系统、结算系统、营业帐务系统、客户服务系统组成，对于这样一个密切关系到企业生存基础的系统，其安全的重要性是可想而知的。可以说，安全是部署所有系统应用和实施优质服务的前提和保障，因而BOSS系统必须有很高的安全性！

分析整个BOSS系统，所涉及的安全控制将主要有网络安全性、处理机安全性和用户安全性三种，其中每台处理机的安全性可以通过UNIX的登录过程实施控制，用户级的安全性可以通过文件的所有者和文件访问权限机构来控制，而网络的安全性将是最大的挑战。

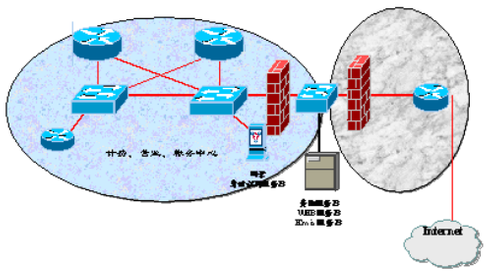
一方面网络中大量存储和传输的数据有可能被盗用、暴露或者篡改，另一方面，BOSS系统本身与Internet的连接、与其它单位系统（如银行、邮储、公安等）的接口及拨号连接等网络接口也都是易受黑客攻击的地方。

新疆移动业务运营支撑系统网络分布广、处理业务多且皆为计费、客服等核心业务，另外还要注意区中心和各地州不同的安全级别，要保障这样一个复杂的分布式网络环境的整体安全，必须首先要对网络系统有一个全面深刻的了解，并且对网络的各个环节可能存在的潜在威胁有一个清晰的认识，然后制定出相应的安全策略。

思科集中分层方案　全面解决安全难题

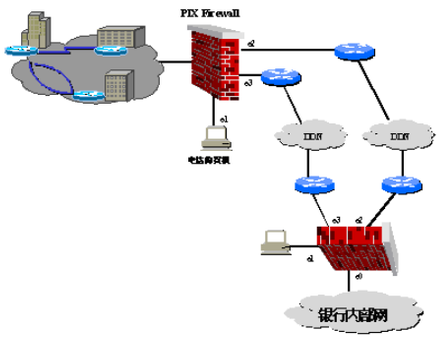
思科系统公司作为是新疆移动新BOSS系统的设计者和搭建者，不仅对BOSS系统架构集中式分布特点及多级安全性需求了如指掌，而且，作为世界领

例如在区中心与Internet的连接就设置了PIX防火墙，将内网与外网隔断，而作为用户WEB查询用的服务器则置于DMZ（Demilitarized　Zoon）中，用户访问时，不会直接进入内网，而只和查询服务器发生关联，再由查询服务器——也只能由查询服务器进入内网寻找到用户所需的数据。这样就可以基本上保证系统的安全性。如下图所示：



系统与Internet的连接

另外，BOSS系统与其它系统的网络接口（如话费代收及银行、邮储、公安之类的接口）都是在区中心采用防火墙等安全机制来集中保证网络的互相独立性。下图以银行为例说明。每家银行现在基本上都可实现通存通兑，也就是说都有一套覆盖全区的网络，而新疆移动采用的是计费、营业及综合帐务系统的集中模式，所以只要在区中国移动与各家银行的区中心作网络连接就可以实现联网了。这种方法接口单一，连接方法简单，易于管理，安全隐患小，投资节约。



二是在拨号连接安全问题上，思科除了采用回拔技术以外，也主要使用了集中的访问控制。BOSS系统的拔号用户主要是营业厅和代理点两类，对营业厅，它完成的业务多一些，因此也应具有较高的权限；对代理点，不应让其访问过多的数据。这可以通过给予不同的用户名和口令，再对这些用户名和口令作不同访问限制的方法来实现，也可以通过对地址的访问控制实现，具体选用哪一种可依实际情况而定。

可能看到，为了实现这些功能，使用集中的访问控制是必要的，它不但可以保证网络不受侵犯，也可以记录下对于网络的操作，监测各种用户的访问。

全面安全　轻松拥有

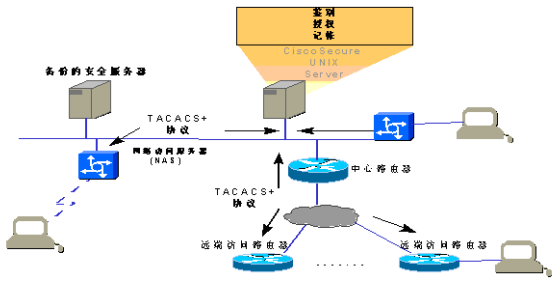
新疆移动BOSS系统通过实施思科安全方案后，整个网络的运行将可在一种可控方式下，保证其安全性；

先的整体安全解决方案最终，新疆移动选择思科作为部署系统安全的厂商。

基于BOSS系统的需求，思科在综合考虑安全性、易用性和成本之后，提出了集中分级的安全解决方案。

首先，“集中式安全管理”，即采用专门用于保证安全性的服务器对整个系统进行监测和管理。

如图所示：



(TACAS：Terminal Access Controller Access Control System--终端访问控制系统)

有了这样的服务器以后，连接在这个网络的所有用户，不管它需要以什么样的方式访问网络设备，都必须通过服务器的安全性监测。由于服务器上可以运行功能很强的安全性方面的软件，可以完全满足BOSS系统的安全需求。在路由器、拨号访问服务器和安全服务器之间传送的可以是经过加密的有关网络安全协议的数据流。

通过这种集中式的安全控制机制，我们可以实现鉴别（authentication）、授权（authorization）和记帐（accounting）的所谓“AAA”安全功能。

为了进一步提高安全数据库的可靠性，我们还可以在网络上设置不止一台的安全数据库；即使在所有的安全数据库都发生故障的情况之下，还可以设置成利用路由器中的数据库实现分散的安全控制方式。

其次，分级安全控制。新疆移动BOSS系统位于区中心和各地洲的网络重要性是不一样的，需要保护的对象也不同，因此安全实施的力度也应不同。也就是说一个好的安全体系，是应有主次之分的。思科在本次方案中根据用户系统的特点构筑了一个分层次的、采用不同厂商安全产品的异构的安全体系。具体为：在系统与外单位的接口处构建一级安全防护，针对计费中心核心的主机，核心数据库的安全构建第二层安全防护体系，并且采用不同厂商安全产品，进一步提高攻击的难度。这种分层异构安全体系，其实就是思科公司面向网络安全端到端的SAFE（Security Architecture for E-Business）解决方案中深度防御理念的具体应用。

最后，思科在具体的访问控制中，也充分利用了BOSS系统的集中模式。

一是使用了一个被广泛使用的“防火墙”的概念，即把防火墙看作是一个数据流的过滤器，只有用户所期望的数据流才能够通过这个过滤器，而其它所有的数据流都不能通过，这一控制是双向的。

不但可以通过集中控制的机制对分布全区15个地洲的网络进行安全管理,防止非授权的人员进入网络之中,还可根据具体用户的级别确定他们的访问权限,以实现分层次的安全控制机制;另外，思科通过将自身高性能的安全产品（如PIX防火墙和VPN等）以及第三方安全产品和技术部署到网络相应的位置,大大增强了网络的抗攻击能力。

在整个项目中,思科作为顶级的网络系统专家,从整个网络系统的角度综合设计整体安全的解决方案。这个方案保证了新疆移动BOSS系统整体的安全而且也实现了系统改造的初衷。

改造后的系统帮助客户解决了原来因地缘分布广造成的管理难度大、成本高、不能及时解决客户问题等问题,使得新疆移动的策略制定、实施,对客户问题的诊断、解决都可以在中心区完成。另外,由于实现了业务管理和安全管理的"大集中",整个BOSS系统的管理都变得更简单、可控，从而不仅保障了整个系统安全、持续、高效地运行,还大幅地提高了人员工作效率,节约了管理成本。思科公司认为在这个系统设计及实施过程中,有三点是保证系统成功的关键。

第一，如何在新疆移动具体地"生产"网络中运用SAFE蓝图的模块化分析方法。思科的"SAFE"蓝图倡导将企业复杂的网络环境模块化,正是这种模块化的分析方法,使得思科可以帮助新疆移动化繁为简地分析其网络各个模块内部以及相互连接处的薄弱环节和关键部分。这样,一方面可以帮助新疆移动有针对性的采取防御策略和手段,使网络系统得到经济、立体、全面的保护；另一方面,使得网络结构及安全部署都能够随着业务的发展而被便捷的推广,保证了网络结构的高可扩展性；

第二,要将国际领先的理念、解决方案本土化、客户化；

第三,在设计、实施的过程中不断与客户沟通,提供给客户一系列良好的服务。