金 融

ABT·安博通

看透安全 体验价值

金融安全策略运维

解决方案

方案背景

随着金融系统计算机的应用和发展，计算机网络技术为金融业的集约化经营和高速发展奠定了坚实的基础。但是随着金融科技的应用，一方面以手机银行、网上银行为代表的金融科技对银行的网络边界逐步“侵蚀”，银行的网络安全边界被彻底打破；另一方面国家监管部门从网络架构、访问控制、集中管理等几个方面对银行的网络安全合规建设要求也越来越高，因此银行在风险与合规之间面临着严峻的挑战。

银行安全现状

基础保护不到“位”

划分安全域保障是对银行生产网络环境中多平台、多网络的基础保护。随后制定严格的管理运维流程对网络及平台中的信息进行进一步的防护。然而当前网络中很难将管理制度，一一对应在工作中落实和监督。

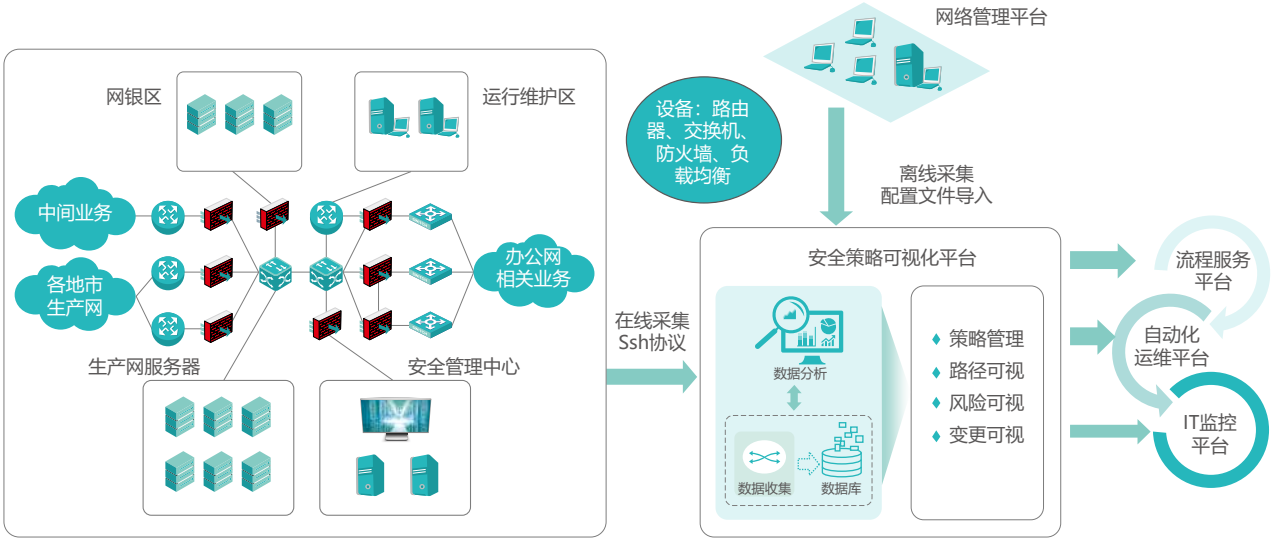
运维体系管理“难”

- 缺乏策略变更前的合规性检查；
- 缺乏策略变更风险评估；
- 缺乏对策略持续性监控且在发生威胁时响应不及时；
- 缺乏对管理制度的持续监控。

解决方案

业务架构图

针对银行的整个运维管理流程，安博通提出了银行业安全策略运维解决方案。通过对防火墙、路由器、交换机、负载均衡设备上的网络访问控制策略进行风险挖掘、建模分析、风险评估以及持续性监控等，为银行网络运维的合规性、可靠性、无间断运行提供全方位技术支持。



流程服务平台“合规化”

业务人员提出变更后结合流程服务平台，在审批前进行策略风险评估，通过挖掘原有设备上的策略信息与现有的变更策略进行比对分析，查看是否有相同策略存在，是否与现有策略造成冲突，确认变更的合规性。

自动化运维平台“更可靠”

策略变更前进行仿真测试，验证业务人员申请的变更是否达到预期要求并且无新的风险引入；根据仿真测试的结果生成变更建议，告诉用户一条最优路径进行变更并生成相应的变更参数，由自动化变更平台调用相应的参数进行变更下发，减少技术人员对变更的参与，确认变更的可靠性。

IT监控平台“无间断”

1

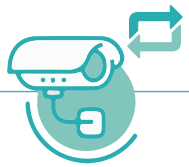
策略风险监控

对网络设备策略信息进行深度挖掘并进行持续性监控，一旦发现隐藏、冗余这些风险策略信息即把信息传送至IT监控平台，通知相关的技术人员进行策略审计。

2

动态基线监控

对银行制定的安全域与业务之间的合规基线访问关系进行持续性监控并且能精确到端口、IP、协议，一旦发生有违规策略变更，通过IT监控平台预警提示，确保基线制度落地。



3

策略变更监控

实时采集或者周期性采集策略配置文件对文件进行备份，主动及时发现变更内容，当有安全事件发生时通过对变更内容进行对比分析，快速对安全事件进行响应。

4

攻击面监控

通过数据流和业务之间的访问路径实时掌握关键数据资产的安全状态，实现核心业务威胁面的可视化分析。

5

合规审计

通过对网络设备上的策略信息进行持续性监控分析，定期对网络安全策略进行巡检，查看策略的合规性，并根据审计部门的要求生成相应的合规报告。

ABT·安博通

看透安全 体验价值

北京安博通科技股份有限公司

营销中心：北京市西城区裕民路18号北环中心2602室

电话：010-80699886

研发中心：北京市海淀区上地中关村软件园二期15号楼3层

电话：010-57649050

www.abtnetworks.com