
Hillstone
山 石 网 科
方案名称：集中财务信息管理系统等保三级建设方案
个人信息：龚世洋-北京九州泰岳科技开发有限公司

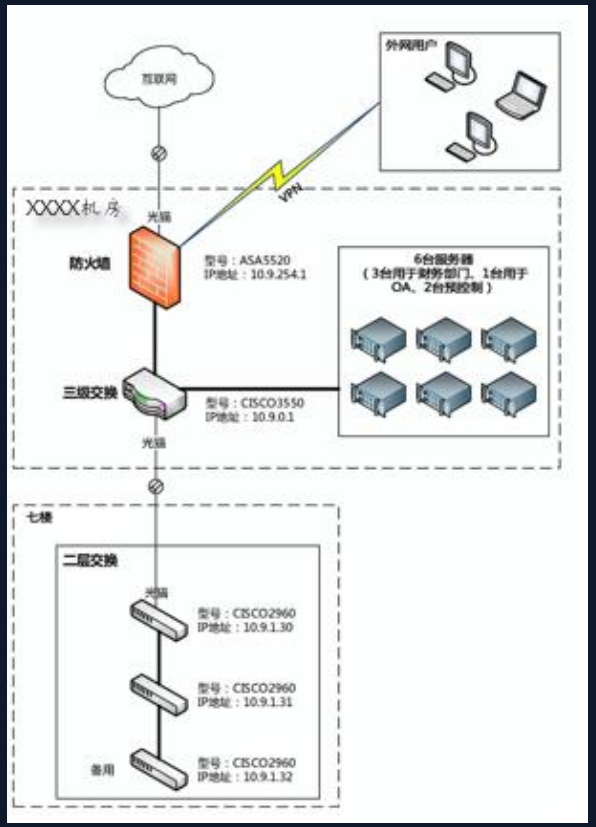
背景介绍

北京XX集团为提升集团的财务管理水平拟实施集团集中财务信息管理系统。此次推行的系统内容包括集中核算、集团报表，将使XX集团财务管理体系达到管理规范化、管控科学化、资源一体化、价值最大化的目标。

“集中财务信息管理系统”是XX集团信息化一个重要的管理系统，它的建设对提升XX集团整体管理水平具有十分重要的意义，也是XX集团的一项重要的工作。本项目主要针对XX集团集中财务信息管理系统整体解决方案和应用软件实施。

本次系统建设将采用本部加二级数据中心的模式构建XX集团集中核算系统，未来下级单位或兄弟单位将通过北京XX集团所属的XXXX做财务集中业务，因此需要在XXXX现有的网络环境中做适当的调整，在满足未来XXXX自身系统及业务要求的前提下，建立起一个稳定、可扩展、高性能、安全的财务信息管理系统环境。

需求分析



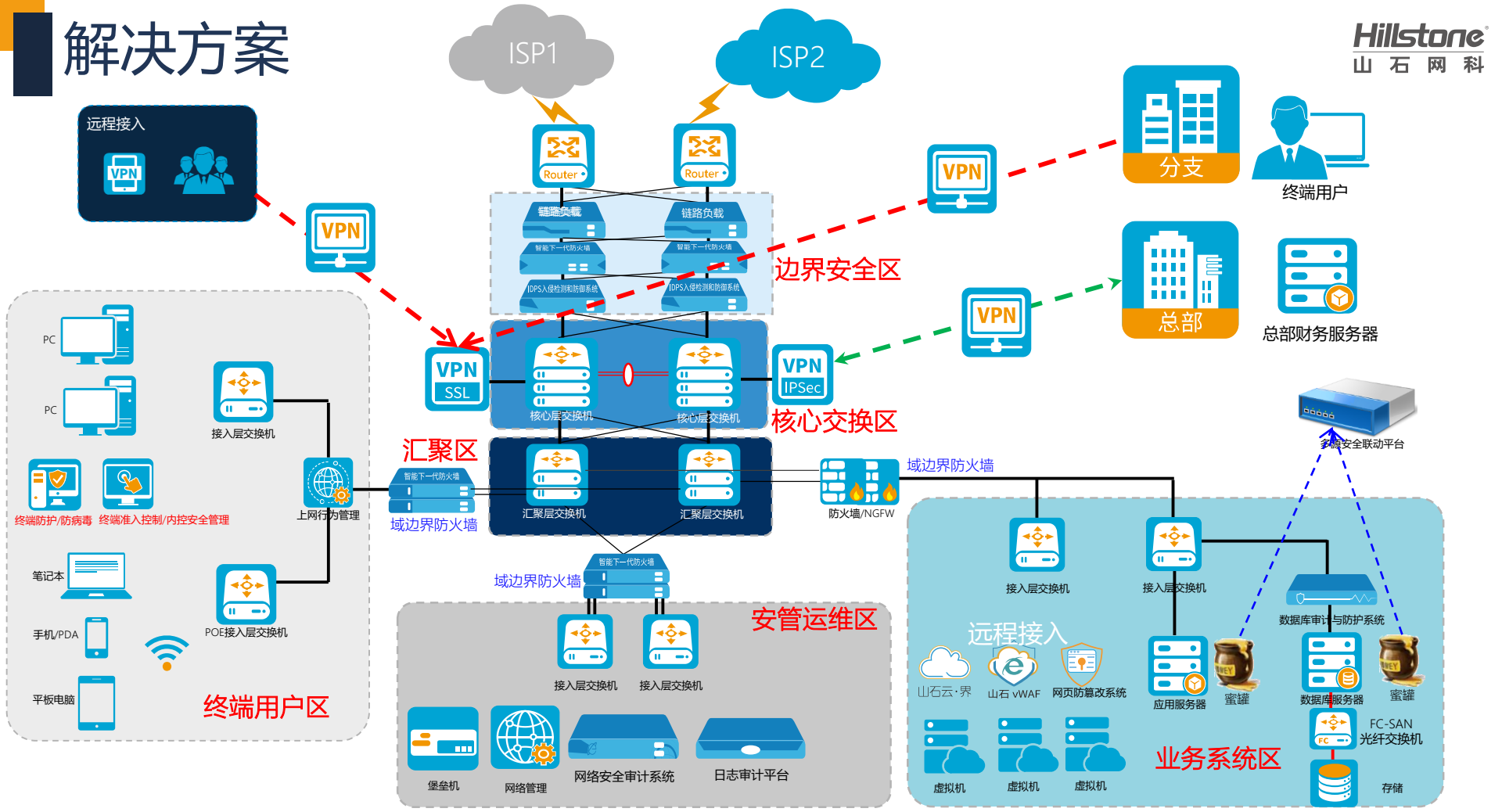
现有网络结构

本次XX集团集中财务信息管理系统建设采用本部加二级数据中心模式构建，XXXX将作为财务数据汇聚节点，其网络环境对于XX集团财务信息管理系统的建设起到关键性作用，因此XXXX的网络环境必需保障未来的财务系统及其他业务系统的安全、稳定、高效运转。

从目前XXXX的网络结构来看，主要有以下几个方面问题需要重点考虑:

- 目前XXXX的财务服务器对于新系统的性能及财务系统软件环境需要更新及增强。
- 目前XXXX通过一台CISCO 防火墙上面集成VPN模块提供下级及兄弟单位的财务系统VPN访问，首先由于CISCO防火墙使用时间及模块化VPN稳定等给财务系统的访问造成不稳定性，特别是在月底财务数据集中上报时风险更加明显，其次CISCO防火墙是一台传统的3、4层防火墙其防护能力不能达到对目前90%的应用层攻击防护，这将对财务系统的数据安全带来安全风险。第三目前XXXX仅仅通过一台防火墙实现业务的访问并作为网关部署，其单点故障风险特别明显。
- 目前网络中仅有一台防火墙设备，不能提供针对性的系统防护，并且其网络全部采用单点方式连接，网络稳定性难以保障，对于断网风险没有防护手段。
- 目前网络接入采用单线方式，对于外部下级单位及兄弟单位VPN接入的跨运营商访问慢问题、以及线路单点问题没有考虑，一旦该线路出现问题，下级单位及兄弟单位财务数据的传递以及XXXX和集团的业务将面临中断。造成的影响将不仅仅是XXXX自身上网的问题。
- 目前XXXX采用实体机构建了财务、域控等业务系统，而目前的数据量不算太大，导致硬件设备的利用率较低，从长期来看，未来新增各类业务系统或者扩容都将带来较大的硬件投资，并且由于没有统一的管理平台，目前对于各业务系统的运转情况不能进行监测，由于XXXX到目前为止也没有相应的运维系统平台所以对于硬件的监控存在空白。
- XXXX集团属于北京市国资委体系，按照相关要求，其系统建设必须满足等级保护相关要求。

解决方案

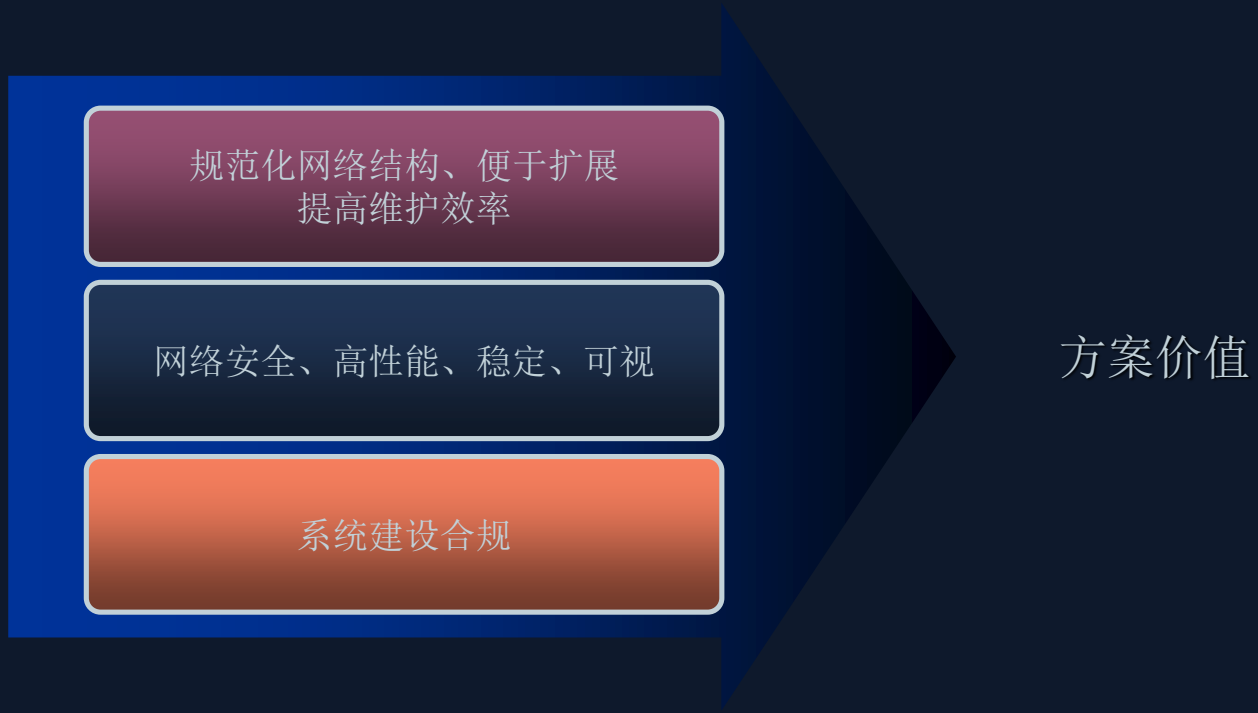

ISP1
ISP2
远程接入
VPN
Router
Router
链路负载
智能下一代防火墙
IDPS入侵检测和防御系统
边界安全区
VPN
分支
终端用户
VPN
总部
总部财务服务器
VPN
SSL
VPN
IPSec
核心层交换机
核心层交换机
核心交换区
汇聚区
汇聚层交换机
汇聚层交换机
域边界防火墙
域边界防火墙
防火墙/NGFW
多维安全联动平台
PC
PC
接入层交换机
终端防护/防病毒
终端准入控制/内控安全管理
上网行为管理
笔记本
手机/PDA
平板电脑
POE接入层交换机
终端用户区
域边界防火墙
接入层交换机
接入层交换机
安管运维区
堡垒机
网络管理
网络安全审计系统
日志审计平台
接入层交换机
接入层交换机
远程接入
山石云·界
山石 vWAF
网页防篡改系统
应用服务器
蜜罐
数据库审计与防护系统
数据库服务器
蜜罐
FC-SAN
光纤交换机
存储
虚拟机
虚拟机
虚拟机
业务系统区

解决方案

- 在该方案中我们考虑了目前XXXX通过CISCO ASA5520传统防火墙提供VPN业务的稳定性问题，由于该防火墙非专业的VPN设备，它通过业务板卡的方式对VPN进行支持，在板卡式防火墙中，首先每增加一个业务板卡其性能的下降非常明显，而且VPN的稳定性非常差，这样将导致未来财务或其他移动办公业务的稳定性及效率。因此在该方案中首要解决的问题即防火墙与VPN分离的问题。通过专业的VPN设备构建高性能、稳定的VPN接入业务。
- 考虑到目前只有一条线路，并且带宽有限，公司的内部办公上网、下级单位及合作伙伴众多，对于集中财务信息管理系统的访问效果很难得到保障，因此本方案中通过上网行为管理，对内部上网应用进行合理管理，为财务及未来的各类业务系统提供更优先的使用权限及带宽通道，从而降低一味投入带宽而应用效率不见提高的情况出现。在链路方面采用多链路负载均衡的方式实现链路的高效使用。
- 将原有的防火墙功能独立出来从而提高了CSICO ASA 5520的3、4层防火墙处理性能，但是面对目前更多的入侵都是采用应用层攻击，例如SQL注入、跨站攻击、APT攻击等其防护原有防火墙能力就显得比较薄弱，所以设计了下一代防火墙来应对这类问题。
- 在业务系统区的设计上，通过虚拟化手段，将办公OA等其他WEB应用系统等都以虚拟机的形式出现，对财务系统、数据库系统采用实体双机方式实现业务的可靠性。通过后端专业的SAN存储设备，提供对数据库、及其他业务系统的数据存储，并通过磁带库的方式实现对财务数据库中的数据进行备份。对于重要的数据库系统前端部署数据库防护设备提高安全性。
- 对于虚拟化业务系统，其安全采用山石虚拟化安全防护产品实现对虚拟环境的防护，规避传统硬件防火墙不能对虚拟化系统内部做安全的难题。
- 对于重要的业务系统，设置蜜罐产品，通过蜜罐的方式将攻击引诱到虚拟系统，同时蜜罐将信息报送多源联动平台，平台下发策略给各安全防护系统实现安全防护。
- 在安管运维区设置等保必要的堡垒机、日志审计、安全审计、运维管理等系统，在终端区设置防病毒、准入、内网安全管理等系统、在边界安全区设置防火墙、入侵检测、防御等系统。

- 方案设计按照结构化设计方式、分层、分域、分重要程度等维度考虑，适度冗余的方式，将整个网络分为接入层、汇聚层、核心层、边界安全区、终端用户区、安管运维区、业务系统区等；
- 整体网络实现主干冗余、可扩展、域边界隔离可控。

方案优势



Hillstone
山 石 网 科

为您的安全竭尽全力！

Thanks

400-828-6655

https://www.hillstonenet.com.cn