方案名称：某证券公司等级保护解决方案

个人信息：王子彦-北京昆仑联通科技发展股份有限公司

背景介绍—某证券公司网络现状

单点

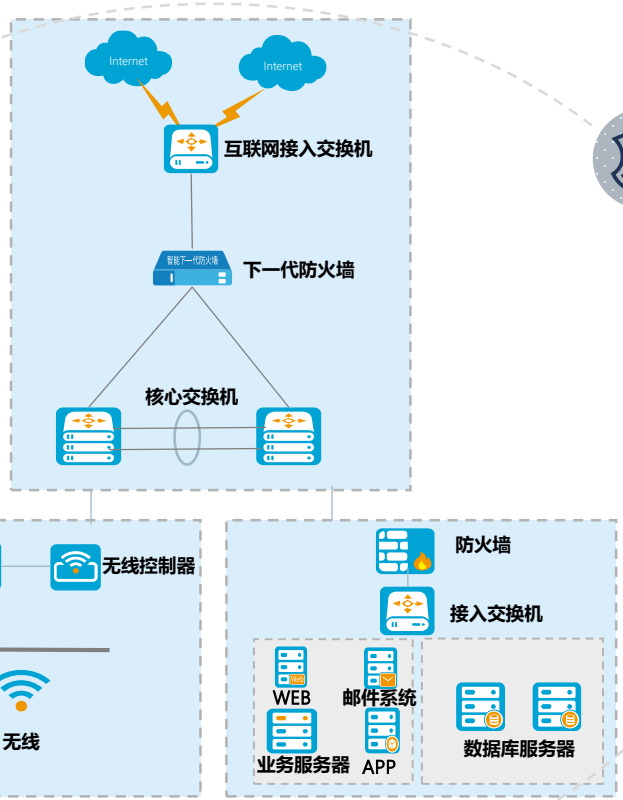
网络中设备均为单点设备，当出现单点故障时，存在业务中断风险

上网规范

网络中无流控设备，大量带宽被占用，导致工作效率低下

主机安全

未安装防病毒，无脆弱性管理机制



边界安全

客户处防火墙使用时限较长，无法做到L4-L7层深度安全监测

安全管理

客户处网络未分区域划分，导致运维管理员运维困难

计算环境安全

业务服务器均“挤”在一个区域，无法实现安全保障

需求分析—合规建设等级保护系统

01.加强设备防护，补齐安全防护短板

这是开展网络与信息安全的基础。利用各种现代化的网络与信息安全防护设备对各种信息化活动进行甄别与防范，可以有效地处理绝大多数非法攻击，必须按照国家等级保护的要求做好各项设备防护工作。

02.优化安全策略

所有的设备防护和安全管理都是基于一定策略的，策略过紧则防范工作量剧增且不利于正常开展信息化工作，策略过松则相当于不设防，起不到相应的作用，因此根据客户具体情况制定相应的策略是安全工作的重要环节之一。

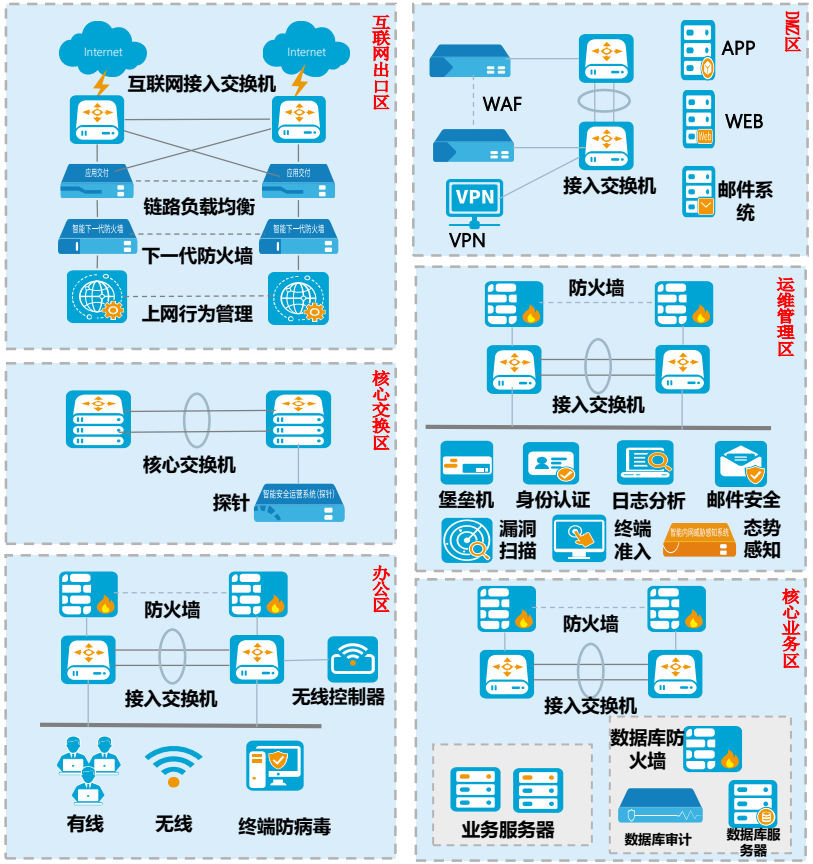
03.加强安全管理

这是开展网络与信息安全的保障。只有建立了立体有效的网络与信息安全管理体系，将职责明确划分、将责任落实到位、将奖惩清晰告知，从而充分落实各项安全工作，确保安全管理稳步开展。

04.定期安全检查，保障业务安全

在安全管理中含有安全检查一部分内容，多为自查。但安全检查不仅仅局限于自查，也不局限于单一的手段，应该是从管理、渗透、测试等多方面开展，目的是及时发现存在的问题并加以弥补。

解决方案-证券公司等保解决方案



方案设计理念阐述

1. 分区分域、层次清晰、架构合理
2. 满足架构先进要求
3. 满足高可用要求
4. 满足安全可控要求
5. 满足可扩展性要求
6. 满足安全可视要求
7. 满足监管合规要求
8. 满足三级等保要求

优势价值—等保方案价值

01 .安全可视

可视是安全的基础，网络安全等级保护解决方案给用户带来全网安全可视、预警及响应，高效感知内部高级安全风险；在外部，通过大量的外部威胁情报，辅助高级安全事件的分析； 在网络内部，在各个子域的关键节点上，通过探针或安全设备，精准的采集有效检测信息。

02.潜在威胁及风险感知

实时汇集漏洞扫描信息，感知漏洞分别及危害情况；对绕过边界防御的进入到内网的攻击进行检测，以弥补静态防御的不足。

03 .异常行为感知

对内部用户、业务资产的异常行为进行持续的检测，发现潜在风险以降低可能的损失。网络安全等级保护解决方案给用户带来动态感知和持续检测的能力，可不间断的感知业务风险。

04 .安全事件感知

对内部重要业务资产已发生的安全事件进行持续检测，第一时间发现已发生的安全事件。