山东网络安全风险评估报告编制编写公司

产品名称	山东网络安全风险评估报告编制编写公司
公司名称	河南世耀诚实业集团有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:文案定制 服务方向:专业领域
公司地址	南阳市卧龙区工业路华龙广告二楼
联系电话	13140513661 18338218580

产品详情

《网络安全法》的第二十一条明确规定，要求网络运营者应当按照网络安全等级保护制度，履行相应安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。《网络安全法》第三十一条规定，对于“ 关键信息基础设施 ”，要在网络安全等级保护制度的基础上实行重点保护。

依据等保的测评范围和内容，参考即将从由1.0时代转变到2.0时代的等级保护，由被动防御变成主动防御，以前被动防御的，要求防火墙、杀病毒、IDS，现在要上升到主动防御。到底如何做好基础安全防护建立一套完善规范的安全防御体系呢？下面让我们逐一解析：

基础安全设备包含哪些？

基础安全设备包含构造业务安全防御系统的常用安全设备，能够搭建深度防御体系的各种安全设备、安全软件。大型的互联网结构不太一样，主要为数据流量很大，普通安全厂家的设备很难满足需求，因此攻击检测和防护会自己开发。本文内容还是围绕以传统业务网络为主，传统业务网络包含的安全设备一般有以下几种：

1.1 检测告警类

网络入侵检测——入侵防御设备

用于检测网络入侵事件，常见部署在核心交换上，用于收集核心交换机的镜像流量，通过检测攻击特征形成告警事件。

网络流量分析——上网行为管理

镜像流量分析，通常也是连接到核心交换，可以分析流量，可以回溯流量，遇到分析安全事件的时候可以通过回溯流量分析攻击过程。

1.2 安全防护类

安全防护类产品同样有检测攻击的能力，检测出攻击才能进行防护，也常见防护类的产品只做检测用。

抗拒绝服务产品

部署在主链路上，内部网络的抗D设备可以处理低于出口带宽的 DDoS 流量，超过的一般用云抗D服务。

防火墙——第二代防火墙

用于做网络边界区分，虽然下一代防火墙有很多花哨的功能，但是在实际应用中比较有用的还是网络访问控制。常见部署在核心路由和核心交换机之间，或者在应用服务器和数据库服务器之间，或者不同的业务之间，有边界隔离需求的都可以部署。 在此，对有些进行等保建设急需要购买防火墙的单位，提些建议:前些年的传统防火墙已无法有效分辨和检测出当今网络中出现的各种复杂应用，更无法准确识别和拦截各类应用中的安全风险。因此防火墙的选择上一定要格外注意。可以选择一款能精 确分类与识别低、高风险应用，并根据应用不同风险等级分别进行不同等级的安全扫描，具备及时准确识别和拦截各种威胁攻击功能的防火墙。尽可能选择具备新技术的，多看功能配置和产品参数，道理就跟我们买手机是一样，都是手机，却不是所有手机都跟苹果，华为一样那么好用耐用。

WAF（Web应用防火墙）

现在几乎所有的应用都使用Web的方式提供，相比较传统防火墙设备，Web应用防火墙提供了应用层的防护能力，更专 业一些。常见部署在应用服务器与核心交换之间，或者核心交换与核心防火墙之间。

也有的业务系统比较复杂，WAF已旁路镜像流量的方式作为Web的入侵检测设备存在，只检测Web攻击事件。

网络入侵防御——入侵防御设备

入侵检测防护系统(简称：IPS)能够对网络、系统的运行状况进行监视，进而发现各种攻击企图、攻击行为或者攻击结果，保证网络系统资源的机密性、完整性和可用性，并能够及时发现网络层的攻击和入侵

行为，使用户能够及时发现攻击与入侵事件，制定相关防御措施。对内外网的入侵行为进行检测和报警，防止入侵，保证整个服务器区的安全。

企业版杀毒软件

目前普遍部署在企业网络的杀毒软件都是基于 Windows 版的，使用统一管理，可以从整体查看病毒在组织网络中的感染情况。企业网策略比较保守，发现病毒只是告警，不直接删除或清除，有可能导致系统文件出错。越来越多的组织使用 Linux 作为主要操作系统，很少有合适的杀毒软件部署。还有种 APT 的产品，杀毒是其中的一个组件或模块。众所周知国产杀毒软件排行第 一的就是360了，该产品的全称:360天擎终端安全管理系统。据市场调查反馈，去年爆发的勒索的病毒，几乎凡是安装过360天擎的单位都安好无事。

1.3 监管评估类

配置核查工具

实现统一的安全配置标准以便规范日常的安全配置操作，快速有效地对网络中种类、数量繁多的设备和软件进行安全配置检测，集中收集核查结果，快速出报告。

网站安全监控

可以对网站漏洞、网站内容、网站可用性监控的设备，属于主动扫描类的工具。漏扫、配置检查、网站监控都是属于主动扫描的设备。

堡垒机——IT运维安全审计

有时候也叫运维审计系统，可以配合 Windows 域或其他认证系统，对运维人员的操作进行审计。网络的访问控制做的好的话，个人认为堡垒机是安全运维里面比较有用的设备之一。很多厂家都有，这里不做推荐。还是那句话，从安全产品稳定性和后期维保角度考虑，尽量选择知 名的厂家是没错的。

日志审计——上网行为管理

传统日志审计，后台使用关系型数据库的，局限性很大，相当于各种日志数据处理后放到一个数据库中，安全事件发生后可以用作做事件回溯查询。数据量大了后表现就是查询速度很慢。另外一般设备是一个盒子，保存的数据量也有限。《网络安全法》第二十一条规定中明确指出采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不得少于六个月。因此日志审计是各单位在等保建设方案中，必须考虑要配备的。即便眼下没买，过后公安网警在进行相关的检查时，也会在责令整改通知书中提出来。

数据库审计

镜像应用到数据库的流量，可以获得所有的数据库操作请求，通过设定一定的规则也能检测针对数据库的攻击。

有些适合政府、企业办公网使用的安全设备，如上网行为管理、网络准入系统等都是常规必买的基础产品，不在这里介绍了。