息外，还会附带有该漏洞的常见解决方法，有利于更高效的排除漏洞。

2.2 入侵检测技术

入侵检测技术是指计算机网络遭受入侵行为攻击时可以检测并识别入侵行为，入侵检测技术可以配合防火墙联动实现对入侵行为的拦截，入侵检测可以分为基于主机的入侵检测、基于网络的入侵检测及混合式分布入侵检测。基于主机的入侵检测通过安装在主机上的相关入侵检测程序，分析主机操作系统端口访问、程序调用、行为日志，将这些数据与攻击签名进行分析，检测二者的匹配度。基于主机的入侵检测可以在不改变网络结构的前提下，实现对入侵行为的检测和防御，缺点是由于检测和分析在主机侧进行，对主机的系统性能有一定影响。基于网络的入侵检测系统主要设置于重要的网段内，对网络数据包进行持续性检测，对每个数据包展开特征分析，如果分析结果与某些规则相符则发出切断网络的警报，该技术可用于检测未成功的攻击，且经济性更高。混合式分布入侵检测是前两种入侵检测技术的结合，不仅能够发现攻击信息，而且能够分析系统的异常信息，具有良好的可操作性及可融合性等优点，因此应用比较广泛[1-3]。

2.3 沙箱防御技术

沙箱技术 APT 攻击防御的一种核心技术，这种技术在启用时能够创建一种虚拟环境用来隔离本地系统中的注册表、内存以及对象，而需要系统访问、文件观察等操作时可以通过虚拟环境调用来实现，同时沙箱能够利用定向技术在特定文件夹中锁定文件的修改和生成，防止核心数据以及真实注册表遭到篡改，一旦系统受到 APT 攻击，沙箱的虚拟环境能够对攻击行为进行分析并比对特征代码，从而有效防御 APT 渗透攻击。在实际生产环境中，沙箱技术能够充分发挥防御作用，但由于需要分析比对攻击特征、虚拟环境本身也需要额外消耗资源，导致沙箱环境下系统整体性能有所下降，对此要进一步优化沙箱环境效率，从提升命令与数据处理速度，有效识别并防御 APT 攻击。

2.4 端点检测与响应软件

端点检测与响应技术也是近来出现的一种终端安全防御新思路。该技术与传统的端点安全防护技术不同，其主要以大数据和人工智能的威胁分析来赋能终端防御软件，解决仅依赖传统杀毒软件、防火墙所无法解决的新型 APT 攻击。该技术框架基于终端资产的趋势预警、行为检测、攻击预防、APT 渗透防御的可视化、自适应、持续闭环的端点防御系统。面对高级威胁、业务异常、内部威胁、外部威胁等终端风险闭环管理，能进行实时的检测分析，通过已有的大数据特征库比对整个系统当前的访问流量、行为数据、不同等级的风险问题，使用机器学习模型加工比对结果最终生产当前系统最佳安全策略，实现智能化自动化处理攻击、提前预警防范并及时响应对应的安全策略，并且能够取证分析追溯攻击链。端点检测与响应技术基于企业杀毒软件、资产管理系统、安全管理平台和威胁检测与响应体系的融合，能够更好识别防御安全风险，通过平台化管理，终端之间互相联动更高效的保护信息化资产防御的安全威胁。

2.5 VPN 技术

虚拟专用网络（VPN）的功能是：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问[4]。在虚拟专用网中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的[5]。

2.6 堡垒机技术

堡垒主机是一个闭环的合规控制系统，用于审计和管理生产环境中，信息资产的各类维护操作。它通过集中管理维护信息资产、维护员账户，建立“人-资产-堡垒机账户”之间的对应关系。对维护人员与信息资产统进行不同颗粒度权限授权，同时记录维护员授权账号对不同信息资产的操作行为，堡垒机与主机之间通行加密，支持不通操作系统远程管理，对高危操作可实现拦截或者审批。帮助维护工作再有监控有管理的情况下合规开展，同时能提供操作员行为跟踪与回放，对事故可实现追溯。实现内部监督管理闭环，消除传统审计盲点，避免关键信息资产遭到内部破坏和盗取。

3　网络安全技术应用

以我省某高职院校网络安全升级改造为例。在校园网中添加漏洞扫描设备、入侵检测设备、硬件沙箱设备、端点检测与响应软件、VPN 设备、硬件堡垒机。并设置以下安全策略：

（1）每天 0 点通过漏洞扫描设备定期扫描内网重要信息化资产，根据漏扫报告及时修复相关漏洞。（2）对现有信息化业务梳理，校内使用的业务原则上不开通公网接口，必须公网访问的业务只开放必要端口，并对公网访问端口配置入侵检测策略。（3）对校园网内部计算机统一安装端点检测与响应软件，避免出现内网电脑被渗透后作为跳板攻击服务器的情况出现。（4）配置堡垒机，将不同维护人员账号与相关服务器绑定，不同维护员之间访问互相隔离，实现日常维护管理审计闭环。（5）配置 VPN 服务，对校外使用有需求但通过公网开放访问不安全的业务使用 VPN 方式访问，在保障系统安全的前提下实现远程办公。

4　结语

高职院校信息化的推进，离不开高职院校网络安全技术的应用与升级，只有有效利用相关网络安全技术，推进信息化建设与网络安全建设同步规划实施，高职院校信息化才能实现健康和可持续发展。

参考文献：

[1]王鲁华，李宇波，赵阳.基于数据挖掘的网络入侵检测方法[J].信息安全研究，2017，3（9）：810-816.

[2]林国庆.数据挖掘算法在入侵检测系统中的应用研究[J].电脑知识与技术，2017，13（8）：49-51.

[3]赵婉彤.入侵检测技术在网络安全中的具体运用[J].信息与电脑（理论版），2017（4）：192-193.

[4]李飞，吴春旺，王敏.信息安全理论与技术：西安电子科技大学出版社，2016.03：190.

[5]肖佳，杨科.基于 SSL VPN 协议的安全浏览系统的设计实现及复合应用方案[J].信息网络安全，2012（11）：66-70.

VPN 技术在校园网络安全体系的应用

◆王真

（邢台技师学院　河北　054000）

摘要：当前，我国科技发展愈发的成熟，校园信息化管理模式也成了时代发展的必然。院校内会相继构建不同的校园网络，借助校园网络，让老师和学生之间的关系变得更加的密切，保障了师生之间的友好沟通状态。学校的规模不断扩张，校区在不断发展，一些院校的分校会在不同的地区构建，想要保障分校发展的协调性，就应当借助 VPN 技术进行管理，这样就可以处理校园网络地区限制管理的问题，同时还会起到改善校园网络应用及管理的作用。

关键词：VPN 技术；校园网络安全体系；应用

VPN 技术主要是以网络运营商供给的互联网为基准，创建出虚拟性私有通道的网络安全防护技术。其技术的应用可以供给用户高质量的服务，在一个开放性的网络环境当中，临时性的建立专用数据传输渠道，加密隧道当中传递的信息，实现专网专用的目的。但是随着高校信息化建设的发展和推进，校园网络的安全稳定性要求越来越高，需要创建出更为简洁且实用性较强的安全体系，这样才能够让校园网络保持良好正常的运行状态，分析 VPN 技术在校园网络安全体系中的应用要点，设计出合理的应用方案，提升其技术应用的实践价值。

1 VPN 概念及关键技术

1.1 数据加密技术

通常状况下，数据加密技术隐藏或者加密数据信息是数据包在虚拟专用网络当中主要的传输方式。若数据包处于一种安全性较差的网络环境当中，其在传输的过程中哪怕已经通过了用户身份验证，也无法确保 VPN 的安全可靠性。所以，在数据发送隧道的一端，需要加密用户的身份认证，保障加密数据的传输状态。在数据接收隧道的另一端，已经完成认证的用户应当解密加密的数据信息，得到相应的原始数据，这类技术可以大致划分成为两类，其分别为非对称加密以及对称加密。对称加密是使用频率较高的一类数据加密技术，其技术可以针对一些机密性的数据采取公钥密码的方式进行管理[1]。

1.2 访问控制技术

访问控制技术功能会对用户访问系统以及使用系统的资源进行管理，能够保障用户可以访问特定的系统资源，拒绝没有授权的用户去访问该系统，从而实现系统资源访问控制的目的。

1.3 用户认证技术

在构建虚拟专用隧道传输数据之前，通常需要使用用户认证技术去辨别用户真实身份，对网络资源的访问，进行合理化管控。用户认证协议摘要技术主要是以哈希函数变换数据报文的长度，使得其得到长度相同，固定不变的报文摘要。但是这类函数会受到自身特性的影响，控制难度较大，想要在众多的数据报文当中找到长度相同，固定不变的报文摘要，需要损耗大量的时间和精力，整体工作难度较高。

1.4 隧道技术

隧道技术是 VPN 传输的重要技术，该技术主要是借助某协议实现另外一类协议传输数据的技术，这一技术的应用本质就是以隧道协议为主，该技术大致分成乘客协议、传输协议以及隧道协议。其中，传输协议是结合隧道的定义完成数据传输任务；乘客协议是对数据进行封装，其对于数据帧以及数据包的协议会有所差异，需要把数据帧和数据包进行封装处理，之后再进行传输，这些封装之后的数据帧以及数据包可以较为精确地到达其目的地的地址，最后进行解封的处理，得到原始的数据帧以及数据报；隧道协议的功能就是拆除、保持以及建立数据传输渠道。

2 VPN 技术在校园网络安全体系的应用

2.1 应用原则

想要将 VPN 技术投入到校园当中，就需要考虑该校园网络的使用需求范围，同时还需要遵守 VPN 技术的应用原则。VPN 网络技术投入到高校应用功能当中，其模块主要分为四类：首先是后台管理，后台创设的作用就是用来收集和 VPN 技术服务器相关的访问记录，将这些记录内容进行整合，重新传输给安全审计进行管理，在后台去总结用户的各项操作行为以及详细情况。其次是浏览控制模块，其模块创设的主要作用就是结合 VPN 浏览控制的方案，保障其技术系统设定的有效度，精确的供给客户方案服务。再次是身份验证，要验证客户端，服务端和客户端的认证方式有所差异，将数字认证技术投入到内网当中，将用户以及用户密码结合的形式投入到外网验证当中[2]。最后是数据传输，数据传输模块也被称之为核心的网络体系分支，其模块存在的作用就是加密、转发数据。在现阶段，我国大部分高校对于 VPN 技术的应用要求都会比较高，特别是后勤以及财务部门，校园在连接网络的阶段，会使用二层隔离的方式，之后进行重心交换机的传输，以该种形式完成分校信息之间的传递任务。一些用户的安全级别会比较低，这就会适当降低安全级别的要求，需要提高 VPN 技术服务器的性能。比如，在移动客户浏览阶段，可以借助 Access VPN 方案进行作业，将其服务器增设到校园网络内，移动客户应用专门的 VPN 客户端和校园网络连接，这类网络连接的形式仅需要 ISP 提供宽带费用或者支付费用即可，并不需要再次支付其他额外的费用。在构建高校 VPN 服务器阶段，以基础环境方向为主，选择 LINUX 网络系统，对其进行实践和证明，其系统的拓展性会比较强，也不需要服务等任何的费用，和 Windows Server 平台进行比较，其系统的性能会更加的优越。

2.2 分析安全体系需求

VPN 校园网络安全体系需求可以大致划分为三类：首先是远程网络对校内网络站点所发起的访问，大部分分校区的老师和学生都要远程访问该数据库，查询学生的个人成绩/查看校内通知等，这部分功能需求往往需要借助用户远程访问的形式来实现。其次是分校区和主校区网络互联访问的需求，要将分校区和主校区的业务服务整合在一起，实行校园一卡通或者创建专门的网络通道，使得这些机密数据信息可以安全性的传输在分校区和主校区之间。最后是远程用户访问高校图书馆资源的需求，安全性认证用户，远程用户对图书馆的资源进行分配，让其构成用户管理、安全防护功能融合一体的系统[3]。

2.3 设计方案

（1）主分校区构建校园内部虚拟专用网

使用光纤链路将分校区和主校区连接在一起，同时把网络出口增设在分校区校园网络当中，要推行学习成绩以及人事档案等相应的应用系统，这些系统在使用时，必须要经由这一光纤链路。应用 IPSec VPN 技术去加密该链路当中传输的各项数据信息，这样可以保障整体网络信息传递的安全性。如果产生访问请求的用户为普通用户，那么就可以在设计安全方式时，允许普通用户去访问分校区或者主校区的网络，让其能够感觉同处在同一个网络内。若其设置较高的安全级别，则会浪费网络系统的资源，甚至还会导致用户访问的速度越来越慢，所以并不需要设置较高的安全级别。如果用户的业务较为敏感，包含人事档案管理或者学生成绩管理等方面的内容，那么就可以使用二层协议网络隔离的形式，让校园网络和用户先连接在一起，之后再把数据信息传递到校园网络当中的核心交换机当中，保障分校区和主校区数据加密传输的状态。此外还需要在两个校区内安装网络路由器设备，不管是对方校区的网络资源请求，还是数据传输，都需要经过该路由设备。校园网络的资源量相对来说会比较大，所以在安装路由器时，必须要重视路由器的可靠性以及稳定度，尽可能减小设备的成本费用。在分校区以及主校区的位置增设 VPN 功能的网络路由设备，同时还需要对其设备进行安全的管理，创建 VPN 通道，将需要传播、传输的数据信息，结合网络路由方式传输到指定的地址[4]。

（2）校园内部网络设置 VPN 服务器

若移动用户以及远程用户都需要访问校园网络，那么就可以借助 VPN 软件系统，对其数据进行加密及封装的处理，网络运营商供给极具开放性的互联网服务，将其和校园内部网络连接在一起，构建访问虚拟专用网络，也就是 Ac -cess VPN。移动用户以及远程用户在发送请求连接校园网络的过程中，VPN 服务器要实现其连接的功能，使用 Linux 操作系统当做校园网络，配置 VPN 服务的平台，这是因为操作系统的扩展性会比较好，使用的灵活度会比较强，能够稳定进行操作。其应用优势要往往高于 Windows 平台，在其内部网络设置中增设 IBMX 366 服务器，Open VPN 软件均由 SSL 协议进行开发，所以在选择 VPN 服务器当中，应当安装 Open VPN 软件系统，这样可以创建出以 SSL 为主的 VPN 系统。SSL VPN 主要是以 SSL 协议为基准，实现访问目的 VPN 技术。该工作会在传输层上，经过

校园网络当中的各个网络地址转换设备以及防护墙设备等，使得移动用户以及远程用户可以随时随地的访问校园网络。但是移动用户以及远程用户在请求访问的过程中，往往需要借助一个校园网络 IP 地址，所以需要架构一台 DHCP 服务器，由该服务器供给移动以及远程用户 IP 地址。若远程用户想要让其和校园网络服务器连接，那么就需要得到其所配置的 VPN 服务器域名。在 DNS 服务器当中，增设该域名，保障用户请求连接的准确性，及时的解析为 DNS 服务器域名。如果远程用户发起校园内部网络资源的访问需求，那么就可以应用校园网络供给的 URL 地址，向这一服务器发起连接，在得到用户身份认证之后，结合其权限划分指相应的服务器内，这类远程访问虚拟专用网络的连接形式，能够较好避免其受到外部入侵解的攻击和干扰[5]。

3　结语

需要站在校园网络信息化建设需求的立场上进行探究，制定出更为合理的 VPN 技术校园网络安全体系应用方案，让移动用户以及远程用户均可借助 VPN 通用渠道访问校园的网络资源，加密传输各项数据信息，避免外部非法入侵者攻击校园网络，设计更适合院校发展的 VPN 安全体系，认证并分析该体系的构造过程，满足校园对于 VPN 应用的各类需求。

参考文献：

[1]费建英.VPN 技术在校园网络安全体系中的应用[J].计算机光盘软件与应用，2013（23）：22-25.

[2]刘春芝.VPN 技术在校园网络安全架构中的应用[J].企业家天地（理论版），2010（05），04-06.

[3]黄磊.基于 VPN 技术的校园网络安全体系构建[J].赤峰学院学报（自然科学版），2016（13）：14-16.

[4]陈剑.基于上网行为管理和 VPN 的校园网络安全体系的设计与实现[J].现代计算机（专业版），2010（07）：01-04.

[5]宋晓飞.基于 VPN 技术的校园网络安全建设研究[J].电子世界，2014（06）：08-09.

基于等保 2.0 标准的高校内网安全防护的探究

◆仇静

（南京工程学院　江苏　211167）

摘要：等保 2.0 标准发布以来，高校信息安全态势面临新的挑战。为更好地应对新的形势和风险，本文通过对新标准中的要求进行简要分析，结合高校内网安全现状，对内网安全防护提出新的思考，为后续高校信息化建设中网络安全保障工作提供参考。

关键词：等保 2.0；高校信息化；内网防护

在网络和信息技术飞速发展的今天，各行各业的信息化进程日新月异，网络安全形势越来越严峻，高校在信息化建设进程中也面临着多种多样的网络安全问题。2019 年，网络安全等级保护 2.0 标准的发布对高校网络安全建设提出了新的要求。为了应对愈演愈烈的网络安全风险，提升高校网络安全防护水平，本文分析等保 2.0 标准下，高校内网防护存在的常见问题，提出高校内网安全防护相关策略。

1　高校校园内网安全现状

目前国内高校校园网采用的网络安全防护策略通常是以防备外网的主动攻击为主要工作内容，而对内网终端默认为信任或者安全状态。有些高校将内网与互联网进行物理隔离，并让内网用户统一通过网关访问互联网。虽然采用了许多安全措施，网络安全事件依然在不断发生。内网一台主机出现威胁网络安全行为，其他主机将大概率会遭殃[1]。究其原因：

1.1 校园内网逻辑边界不清晰

校园内网实现资料共享、网络互通，则必须将内网主机之间建立互信关系。一方面，借智能手机为支撑的移动计算技术，传统的工作方式从固定计算机办公转变为移动化的办公方式，一些系统需随时随地进行数据访问；学校分工与对外协作越来越复杂，外部的人员也将对校内数据进行访问。另一方面，大部分高校采用了云计算和大数据技术，将大量业务和数据迁移到公有云上，这些集中数据的集中，也导致了这些内网数据逻辑边界的不清晰。

1.2 校园内网终端漏洞没有及时修复

目前国产操作系统还不成熟，计算机及服务器主要采用微软公司的 Windows 系统，根据网络安全调查结果显示，全球大约 80%以上的病毒都是基于 Windows 系统的漏洞而进行攻击的。虽然微软公司不断推出各种补丁，但对于高校，内网管理面积达，主机数量多，管理人员有限，如果漏洞没有得到及时修复，导致被黑客利用，对内网中的其他终端主机产生巨大威胁，严重时可导致整个内网瘫痪。

1.3 缺乏对虚拟网络的安全防护措施

传统数据中心的三层架构无法满足海量虚拟机的配置和不断扩大的业务需求，越来越多的高校在数据中心设计中采用虚拟化技术。服务器虚拟化导致在物理服务器内部存在多台虚拟机，每台虚拟机承载不同的应用，同时，在物理服务器内引入了虚拟交换机，这样在同一物理服务器中的虚拟机之间的通讯不需要经过物理网卡而是在虚拟交换机中直接通过链路转发，因而也不会通过外部的防火墙等安全防护设备，原有的安全防护机制变得无效[2]。加强东西流量安全防护，是目前虚拟化网络安全领域亟待解决的问题。

1.4 资源访问权限控制机制的缺失

目前高校的校园网用户一旦接入内网，就可以随意访问内网公共资源，这也造成了许多的安全问题。在资源访问权限未做分级管理的情况下，一些安全事故就在所难免。如果内网建立资源访问权限分级管理就能让用户在访问内网资源时变得可控，可管，那么就能减少一些网络安全事故的发生。

1.5 网络安全管理机制尚不健全

高校在校园网设计之初，普遍注重网络的实用和高效，建设资金重点用在关键网络、硬件设备和软件系统的投入，而忽略网络安全问题，目前很多高校网络安全技术岗位都是由其他岗位人员兼任，致使网络安全管理机制不健全，技术力量薄弱，难以高效率地预防和处理网络安全问题。

2　网络安全等级保护 2.0 的要求

2019 年 5 月，《网络安全等级保护基本要求》（“等保 2.0”）正式发布，并于 2019 年 12 月 1 日开始实施，网络安全等级保护制度建设开始进入 2.0 时代。相比旧标准体系，等保 2.0 统一了基本要求与设计要求的安全框架（通信网络、区域边界、计算环境），充分体现“一个中心，三重防护”的纵深防御思路，强化可信计算安全技术要求应用。等保 2.0 标准对通信网络、网络边界、主机设备、应用和数据、以及云计算扩展、移动互联扩展、物联网扩展和工业控制扩展等方面都有新的要求[3]。

结合新标准，高校内网安全防护时应该坚持以下原则：首先，需求和风险保持平衡。在选择网络保障的时候，要充分考虑可能存在的