高速公路网络安全管理规划

林泽山

福建省漳州高速公路有限公司 福建漳州

【摘要】高速公路网络基于网络安全管理应用研究，采用主备双链路，在区域联网中心出口边界部署与省联网中心连接的防火墙；省联网中心系统网络对收费业务服务区、数据服务区等业务区进行划分，对收费业务区、边界防火墙等业务区进行业务边界隔离；运维管理区部署终端管理服务器、漏洞扫描系统，对网络流量进行审计，收集日志信息，对网络中的风险进行提前预知，避免可能出现的安全问题，旨在提高高速公路收费网络安全和网络应用的可靠性，以及对网络安全管理的重要性。

【关键词】安全策略；防火墙；堡垒；安全意识

【收稿日期】2022 年 11 月 12 日 【出刊日期】2022 年 12 月 22 日 【DOI】10.12208/j.aics.20220083

The Highway network safety management planning

Zeshan Lin

Fujian Zhangzhou Expressway Co. LTD Fujian Zhangzhou

【**Abstract**】Based on the research of network security management application, the highway network adopts active and standby dual links, and the firewall is deployed on the border of the regional network center to connect the provincial network center. The central system network of the provincial network is divided into fee-paying service area, data service area and other business area. The fee-paying service area and other business area boundary firewall is used to isolate the business boundary. Operational administrative zone deployment server terminal management, vulnerability scanning system, for the audit, log network traffic information collection, to predict the network risk in advance, to avoid possible security problems, the purpose of this study was to improve network security and reliability of the network application of the expressway toll collection, and for the importance of network security management.

【**Keywords**】The security policy; firewall; The fortress; Safety awareness

1 网络链路路由策略的制定

通过选择相关路由协议，制定特定的路由接收和发布策略。在相同的网络结构下，通过各种路由协议，修改各项相应 规则的参数设置，从而改变路由的选择、发布和接收。基于高效，环保，清新的原则，为降低网络运行费用，且合理的制止因为单条链路断裂导致全网通信中断的情况发生，在现阶段存在的最优路由的情况下，选用多出口网络，再根据特定的路由选择特定的网址，强制完成路由转发，营造出不同的网络用户走相对应的出口，避免网络拥挤事故的发生，不仅提高了网络运行效率及网络运行的稳定性，为所有网络用户提供了更加便捷可靠的网络访问路径，且大大的降低了网络运行费用。

2 下一代防火墙设备的投入使用

作为将各类用于安全管理和筛选的软硬件设备有机结合的技术，防火墙技术能够有效地帮助计算机网络在其内外网络之间构建起一道相对隔离的保护屏障，从而保护用户数据和信息安全的一种技术。为了保障计算机网络的安全运行，提供更加高效、安全的网络运行体验，同时保障网络用户的信息资料的隐私性和完整性，防火墙有效的对计算机网络

作者简介：林泽山，男，福建平和，本科，福建省漳州高速公路有限公司，网络工程师。

安全运行中的各项操作进行合理的检测和记录，对计算机网络运行中可能出现的安全隐患及数据传输中出现的各项问题进行隔离和保护，保障计算机网络用户良好的使用体验。

防火墙技术的应用，可以实时监控和保护计算机中的重要数据，有效掌握计算机网络通信信息，实现良好的计算机防护功能。通过防火墙技术的开发和应用，可以有效地提高网络信息传输工作中的安全性，防止外部环境中的非法病毒软件或者是非法入侵访问个人计算机的行为，有效地保障用户计算机系统的安全，确保重要数据的安全。[1]

我们通过防火墙接口配置来编辑和改变其接口的地址，并根据网络中具体的应用访问地址资源来定义各种网络地址，如可以定义主机地址(即单独的一个 IP 地址)，也可以定义网络地址范围，定义子网，还可以根据业务访问定义组的相同来定义不同的地址；其次，我们根据网络中的特定应用开放端口定义防火墙端口，可以定义单个端口，也可以定义多个，或者是多个端口范围，甚至服务组。我们再一次定义配置防火墙的入侵防御策略，确定访问控制策略，使之成为防火墙的核心配置部分，根据安全性的要求对相关网络流量进行限制和放行，根据业务的需要配置相应的安全策略，包括源地址、目的地址、服务等。

我们通过选择病毒处理的方式进行病毒防御策略，通过日志设置来收到网络日志警告和管理，了解防火墙的整体使用情况。如图 1 所示。

最后我们通过选择病毒处理的方式进行病毒防御策略，通过日志设置来收到网络日志警告和管理，了解防火墙的整体使用情况。

3 通过堡垒机加强对网络信息资源管理

堡垒机，顾名思义，就是在特定的网络环境下，为了保证网络和数据不受外部和内部用户的侵入和破坏，利用各种技术手段对网络环境中各组成部分的系统状态、安全事件、网络活动的服务器进行实时的收集和监控，以便集中报警、及时处理和审计定责。其在功能上综合了核心系统运维和安全审计管控两大主干功能，能够对主机、服务器、网络设备、安全设备等的管理和维护进行安全、有效、直观的操作审计，详细记录策略配置、系统维护、内部访问、提供细微粒度审计，支持全程回放操作过程。[2]从技术实现上说，通过切断终端电脑对网络和服务器资源的直接访问，而采取协议代理的方式，接管终端电脑对网络和服务器的访问。运维安全审计则扮演着看门者的角色，所有对网络设备和服务器的请求都要经过这个闸机。因此，运维安全审计可以拦截非法访问和恶意攻击，对不合法命令进行命令阻断，对目标设备的所有非法访问行为进行过滤，并审计监控内部人员的误操作和违规操作，以便事后追责。作为企业信息安全建设不可或缺的一环，安全审计逐渐被用户所关注，是企业安全体系中的重要一环。同时，安全审计是一种有效的事前防范、事中预警的风险控制手段，也是一种可靠的事后追溯证据来源。

我们通过堡垒机的界面配置，选择需要配置的上网卡，对界面地址进行修改；通过路线配置，根据需要增加路线；通过用户管理，选择相对应的目录树，对新用户进行增补；通过再资源管理，选择需要添加的资源类型和对应的目录树，按照所需资料进行资源添加，如图 2 所示。

图 1 日志设置

图 2 堡垒机的界面配置

然后根据岗位需求，将管理资源的权限分配给单个用户或将相同的管理资源权限添加给多个用户，根据岗位所需资源，将岗位绑定在用户管理处，最后将普通用户账号分配为堡垒机普通用户的日常运维使用，通过管理账号来审核报表行为，查看所有用户的操作情况。为了加强对网络信息资源的安全管理和运用。

4 安全准入设备的加强防护

安全准入也就是通过 WEB 的方式对企业内部网络进行安全管理，加强网络管理员对计算机终端从进入到注册到监测再到修复整个周期的安全管理。首先对访问用户从接入层进行最小授权控制，严格按照用户身份对内部网络访问范围进行控制，确保企业内部网络资源安全。

其次，通过身份认证的用户还必须通过终端的诚信检查，查看补丁、杀毒等连接系统的功能是否已经及时升级，是否存在安全隐患。对通过身份认证但不符合安检的终端不予入网，强制引导移至隔离修复区，提示用户安装相关补丁、防病毒软件、配置操作系统相关安全设置等。及时发现并制止未授权终端访问内网资源，减少非法终端攻击、窃密内网等安全威胁，保障内网安全。

我们通过人工添加认证用户选择在组织结构中的根节点下创建新的单元，选择添加按钮，如图，登录用户名和姓名直接用门架，如电脑、IPC、高清摄像机、其他网络安全设备等接入设备名称，但登录名和姓名不能重复。

其次，通过人工添加资产信息，进入认证用户管理，选择在组织架构中建立的节点后面的资产明细，输入相应的内容，可信选择可信选项，保存下来，这样就成功填入了资产。当然也可以通过登录设备，https://IP/system/admin,输入用户名密码。认证用户和资产支持界面手动添加和 EXCEL 表格模板批量导入，如果用户量大，可以先在导入模板中统一采集，再批量导入，也可以采用资产扫描的方式。但选择导入时，要选择组织机构中建立的节点的名称，且注意 excel 表信息填写事项，如单位，部门，登录名，用户名，邮箱，mac 地址，ip 地址，设备是否可信，交换机 ip 及端口，终端设备类型等，即可可完成认证用户的批量导入。

最后我们通过登录设备，https://IP/system/admin,输入用户名密码，查看终端认证日志以及时了解安全准入设备的使用情况。

5 提高网络管理者安全意识，不断提高计算机网络系统的安全性

当安全事件发生后，由于安全威胁的程度不同，不同的资产受到的影响程度也不同，而这些影响又通过各种安全属性的损害程度、机密性、完整性、可用性、可控性以及对资产的不可否认等因素来体现。[3]网络安全不可避免地会受到来自外界各方面的网络安全隐患的不利影响，首先必须不断提高网管人员的安全管理意识。这不仅要求广大网络用户

要树立强烈的安全管理意识，网络安全管理人员也要清醒地认识到网络安全管理工作的重要性和必要性，能够以严谨、科学的态度，定期对计算机网络系统进行安全检测，做好计算机的日常管理和维护工作。在计算机与网络连接开始时，应加强安全管理工作，确保在重新安装计算机主机系统后，可先对整个计算机网络的病毒进行整体查杀，在开始运行前尽可能消除计算机网络病毒。其次，每台电脑都要安装合适的杀毒软件，并且要及时更新、升级杀毒软件和病毒资源库，保证能及时检测和消灭电脑病毒，使电脑处于安全使用状态。《基于网络安全管理应用的研究》主要对内外部网络安全系统进行了分析，由于当前信息技术的发展使得网络信息资源不断扩大，同时网络资源中也出现了一些不良插件带有非法占有网络资源的病毒，严重影响了网络资源的安全。

6 结论

通过结合具体业务需求，合理应用网络安全技术，对不同地理位置的用户、服务器以及网络对象进行合理分组，并结合不同的网络安全设备，设置相应的接入权限和安全权限，既有利于提高网络数据传输速度，保证计算机系统安全，又有利于网络安全管理工作的开展。高度重视网络安全管理工作，利用各种网络安全防护技术，为网络运行营造健康、安全、可靠的环境。

参考文献

[1] 刘浩然.分析计算机网络的安全隐患及防范措施[J].科技创新与应用，2019（36）：147-148

[2] 艾奇昆. 部署堡垒机保障运维安全[J].网络安全技术与应用，2017(2):27-29

[3] 曹阳，张维明.信息系统安全需求分析方法研究[J].计算机科学，2003（04）:121-124