堡垒机及 VPN 技术在远程处置突发信息系统故障中的应用

卢伟开 车濡均

（南方电网数字电网研究院有限公司 510000）

摘要：随着信息时代的到来，在企业信息安全管理中，重要信息系统的业务连续性能力及突发故障处置能力愈发重要。在信息管理系统的实际运行过程中，在某些时段，当系统运行出现故障时，系统运行维护人员无法在第一时间到达现场，对系统故障进行处理，对于系统正常工作效率与企业的信息安全管理工作带来无法估量的损失。基于这一情况，借助互联网技术，构建一条安全可靠的远程网络通道成为缩短系统恢复时间的关键。本次研究中，将借助堡垒机设备雨季 VPN 技术构建企业信息安全管理的远程控制的系统运行维护的平台，并进一步优化系统运行的安全管理工作策略与手段，更充分的提升系统运行过程中的安全防卫性能，让系统运行维护工作人员能够通过新构建的高度安全的系统运行维护通路，第一时间进行系统运行故障处理，保证系统正常的工作秩序，为企业信息安全管理工作的开展提供更充分的保障。

关键词：堡垒机；VPN；远程处置

企业信息安全管理系统的运行稳定，对于保证企业信息安全管理工作的有序展开有着至关重要的作用。在系统的实际操作过程中，当系统在非工作时间出现故障时，系统运行维护工作人员会由于各种不可抗力的原因，无法在第一时间感到现象，对系统运行故障进行处置，这就使得系统的实际应用过程会出现一定的中断，对企业信息安全管理工作的连续性造成不利的影响。针对这一点，本次研究中借助 VPN 及堡垒机技术在互联网中建立应急处置网络，实现对系统运行故障的远程处置，规避掉系统日常运行维护工作中的各种不可抗力因素，让系统在出现故障时，第一时间得到有效的故障处置，更快的恢复运行。

1. 堡垒机与 VPN 技术的基本内容

堡垒机是一种比较常见的运维安全审计设备，这一设备的主要能够包括核心系统的运行维护以及信息安全的审核与管控。另外，堡垒机还能够实现对相关人员的身份认证，系统用户的账号与授权监管以及系统用户的异地登录等智能。堡垒机的应用，使得系统运行维护人员能够与具体管理的目标设备实现远程的互联，通过堡垒机，相关的工作人员可以在异地登录堡垒机，由堡垒机将登录信息转接到系统登录，完成各项具体的操作任务[1]。而 VPN 技术具体指通过加密通信技术，在公用网络上建立私有专用网络。VPN 技术的主要内容包括加密与解密的技术、隧道技术、密钥管理技术和身份认证技术等。现阶段有关 VPN 技术应用相对比较广泛的是 SSL VPN 协议以及 IPSec 等。而堡垒机设备应用中，通过与 VPN 技术的结合，真正实现了系统运行维护工作人员对系统的远程访问，相关工作人员可以通过其他的 PC 端以及移动手机终端，利用互联网对系统运行进行远程的监控，并在发现问题时，第一时间做出反应，展开问题检查与处理[2]。

2. 堡垒机与 VPN 技术结合实现系统故障远程处置的系统设计

2.1 系统设计的根本性原则

堡垒机与 VPN 技术结合的新型运行维护工作系统的设计中，由于应用这一系统的企业内部网络与外部互联网保持隔离的状态，以此保证企业内部信息管理的安全，因此在运行维护系统的设计构建中，需要为此专门建立一个企业信息管理网布网络与外部广域互联网的网络通路，才能够真正实现对于企业信息管理系统运行故障的远程发现与处置。根据企业信息管理工作中的实际应用需要，堡垒机与 VPN 技术结合构建的运行维系统的设计与构建中，需要严格遵守以下几点原则：

①这一系统的设计构建要与企业当前应用的信息管理系统实现高度的兼容，运行维护系统的运行能够与信息管理系统同步运行，并且两个系统运行的过程中不能对彼此造成干扰，以避免不可预知的网络信息安全风险，给企业日常的信息安全管理工作带来[3]；

②新型运行维护系统的应用，要充分保证企业内部信息管理网络的安全性。在企业信息安全管理工作中，内部网络的构建是为了防止外部网络信息对企业内信息安全管理工作正常秩序造成的不利影响，是企业信息安全管理工作中最重要的信息安全保障手段。基于这一点，基于堡垒机设备与VPN技术结构设计构建的运行维护系统不得对企业原有的内部网络的安全性造成一心概念股，必须要具备充分的网络安全防护的能力；

③要严格规定系统运行维护工作人员对企业内部网络访问的权限。为了有效避免外部网络信号对企业内部信息安全的威胁，减少VPN技术被恶意使用，给企业的日常信息安全管理工作带来损失，在系统权限的分配过程中，要坚持运行维护工作人员系统使用权限最小化的原则。给相关工作人员的系统使用设置多道权限，以提高对于相关人员系统使用的甄别效率，保证系统使用过程中的网络安全[4]。

2.2 系统的具体构成

本次研究中，针对企业信息安全管理工作的实际需要，降低VPN技术运用对于企业内部网络安全性的影响，可以设置两道防火墙，将企业信息管理的内部网络分割成内网区、DMZ区以及外网区三个部分。其中的堡垒机设备以及VPN技术的硬件设备解题采用分层部署的方式进行具体部署。具体的部署方式如下图所示：

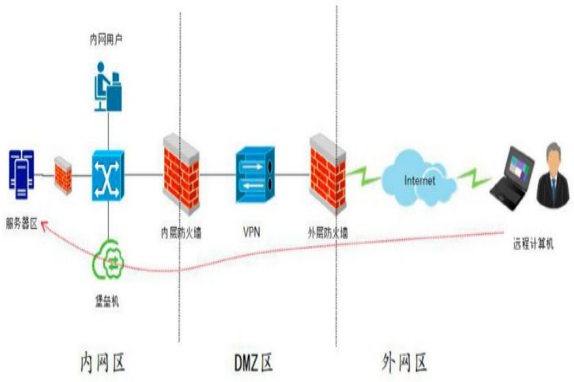

图 1.堡垒机设备与VPN技术设备的具体部署

在具体的部署中，堡垒机设备设置于内网区，通过旁路介入的方式与企业内部网络进行互联；而VPN技术设备设置于DMZ区，以串联的方式接入到两个防火墙之间的位置，而设备的内外网络通信会在经过网络时被转化成为NAT，以便将企业内部网络隐藏，保证企业内部网络的安全。而各种远程终端与系统的连接通道同样由VPN提供技术支持，相关工作人员可以通过WEB方式进行堡垒机登陆，并由堡垒机完成跳转，从而进行各项所需要进行的工作[5]。

3. 堡垒机与VPN技术运行维护系统的安全管理

3.1 安全管理中的系统配置策略

在企业日常信息安全管理工作中，为了能够最大程度上保证企业内部网络的安全，避免企业的各项具体业务系统运行中受到外部网络信号的干扰与攻击，在运行维护系统登录的设置上，可以采取系统用户多因子身份认证的方式，让系统用户经过多道认证程序登录的策略[6]。除此之外，外部互联网与系统的VPN保持连接，而VPN又与系统中的堡垒机设备保持连接，对此，系统配置策略中，堡垒机与企业信息管理系统的服务器连接需要通过防火墙装置，对网络信号进行细粒度的访问控制。同时，还要利用堡垒机设备，即时监测相关工作人员的具体操作，当出现危险操作时，要通过堡垒机设备对操作过程加以阻断处理，进一步保证系统运行安全。

而在系统用户的身份认证过程中，当相关工作人员与VPN进行连接时，可以采用用户名及口令+远端计算机硬件特征码+USBKey的认证方式进行登录验证。而在后续登陆堡垒机设备的过程中，则需要采用用户名及口令+动态口令牌的方式进行用户的验证，以防止系统非授权登陆问题的出现，保障系统应用安全。

在系统实际应用中的网络信号访问控制当中，系统外层的防火墙装置要对外部网络到DMZ区的连接流程加以更为严格的控制，在系统实际运行过程中，外部网络信号要想对系统中的VPN进行访问，只能够为其提供访问设备的5566端口的权限，这一权限具体在登录VPN设备，建立VPN与系统用户的连接中使用，实质上讲就是系统用户的注册程序，而这一过程也需要得到企业方面的许可才能进行；而系统中的内层防火墙装置也只能允许VPN设备对堡垒机设备的443等特定端口进行访问。除此之外，系统服务器部分设置的防火墙只能为堡垒机提供访问服务器3389端口（RDP方式）及22端口（SSH方式）的权限，在这一过程中还要将其他网络信号对服务器的远程控制连接进行阻断处理[7]。

3.2 具体安全管理措施

运行维护系统中堡垒机设备与VPN技术的互联，一

定程度上会导致企业信息安全管理内部网络与外部网络连接的过程中，企业内部网络与外部网络的个例被一定程度上打破，由此带来企业内部信息的泄露风险。为了在堡垒机设备与VPN技术实际应用中对这一问题的有效规避，需要对企业信息安全管理运行维护系统的实际应用加以进一步的完善，执行更具有针对性的网络安全管理手段。

①VPN设备自身就存在一定的网络安全隐患，对此，在日常对系统应用的管理中，需要定期对系统中的VPN设备进行安全扫描，及时检查设备运行过程中存在的漏洞，第一时间进行设备运行的补丁升级，以此方式进一步降低VPN设备应用过程中有可能出现的网络安全风险[8]；

②在系统实际应用的过程中，鉴于VPN设备自身存在的网络安全风险，还要尽可能缩短VPN设备在外部互联网中暴露的时间。在实际工作中，当不需要使用VPN设备的时候，可以将VPN设备设置成开机断网的状态，当需要使用这一设备的时候，再恢复其网络连接，以此方式实现设备与外部网络的充分隔离。而在使用结束之后，就需要断开设备的网络连接，让设备回到开机断网的状态，保障系统使用过程中的网络安全；

③在实际工作中，需要进一步加强远程登陆设备的安全管理。系统的远程控制中，由于系统本身的安全防护已经十分到位，对于外部网络攻击形成了强大的防御能力，在这种情况下，工作人员个人的PC端设备以及移动设备就成为外部网络攻击的突破口。为此，在实际工作中，要进一步加强对这些个人设备的安全防护系统建设，最好的办法就是为工作人员提供专门的外部连接设备，充分规范外部连接设备的使用，避免工作人员日常使用电子设备过程中由于安装外部程序等引起的外部网络攻击，从而对系统安全形成威胁；

④要进一步加强对工作人员对系统应用的管理，详细记录统计各个工作人员系统使用的各项信息，以便发现工作人员在系统使用过程中的违规操作，第一时间进行处理，保证系统使用的安全[9]。

结束语：本次研究中，针对企业信息安全管理工作的实际开展，针对企业信息安全管理工作系统的安全保护，提出了堡垒机结合VPN技术的信心运行维护系统的构建，并对围绕这一系统运行的安全管理策略与具体措施进行了一定的论述。希望本次研究能够切实帮助到企业信息安全管理系统的运行维护工作的开展，积极推动企业信息安全管理体系的充分完善。

参考文献：

[1]曾丽娟,杨平,徐浈基,吴双.基于防火墙双机热备IPsec VPN穿越仿真实验设计[J].现代信息科技,2022,6(16):96-99+103.

[2]夏永辉. 铁路GSM-R和5G-R移动通信系统运维技术的研究[D].中国铁道科学研究院,2022.

[3]陶骏,刘晴晴,佘星星.基于GRE隧道和BFFH模式的MPLS VPN网络构建[J].湖南文理学院学报(自然科学版),2022,34(02):17-22.

[4]李懂晓. 基于ITIL的S公司港口信息系统运维管理优化研究[D].广东工业大学,2022.

[5]孔生,赵胜,于祥周.VPN网络在水厂井群控制和水池调蓄中的闭环应用[J].城镇供水,2022(02):63-65+75.

[6]匡石磊.基于堡垒机的屏幕录像系统的运维操作审计研究与实践[J].网络安全技术与应用,2021(06):7-10.

[7]刘爱明,张春霞.信息安全防护系统运维模式优化研究[J].网络安全技术与应用,2020(10):40-41.

[8]赵超. 高铁运营系统韧性影响因素及提升策略研究[D].东南大学,2020.

[9]黄剑韬,黄志中,王琳琳,路程伊,金鹏,吕飞,孙娜娜,王伟,侯瑞峰.基于堡垒机的智能综合运维管理系统的设计与思考[J].中国数字医学,2018,13(08):68-69+21.