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]；