计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(3):279−282 [doi: 10.15888/j.cnki.csa.006060]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于主备模式的堡垒机网络架构①

龚文涛[1], 郎颖莹[2]

[1](中国石油大学 (华东) 信息化建设处, 青岛 266580)
[2](中国石油大学 (华东) 教育发展中心, 青岛 266580)

摘　要: 伴随网络信息科技迅猛发展, 信息网络安全等级保护制度日益被各个高校所重视和落实, 如何加强园区网的网络信息资源的安全管理变成一个研究热点和难点. 提出一种基于主、备机冗余的堡垒机网络架构设计, 将堡垒机引入到高校网络信息安全管理中, 总结高校面临的各种安全管理问题. 本文分析堡垒机的各个核心管理功能, 并将堡垒机引入到学校核心与数据中心之间的 WAF 防护体系中, 给出核心配置环节和代码, 最终总结全文.

关键词: 堡垒机; 网络; 设计; 模式; 安全

引用格式: 龚文涛,郎颖莹.基于主备模式的堡垒机网络架构.计算机系统应用,2018,27(3):279–282. http://www.c-s-a.org.cn/1003-3254/6060.html

Network Architecture of Fortress Machine Based on Main Standby Mode

GONG Wen-Tao[1], LANG Ying-Ying[2]

[1](Information Construction Department, China University of Petroleum (East China), Qingdao 266580, China)
[2](Education Development Center, China University of Petroleum (East China), Qingdao 266580, China)

Abstract: With the rapid development of network information technology, its security protection system is increasingly being valued by various colleges and universities. How to strengthen the safety management of network information resources of campus network has become a research hotspot and difficulty. This study proposes a design of the fortress machine network architecture based on the main and standby redundancy, and takes the fortress machine into the management work of the university network information security. We also summarize the security management problems. The paper analyzes various fortress machine core management functions, and the fortress machine is introduced to the WAF protection system between the school and the core of the data center. It gives the core link configuration and code as well as the summary in the end.

Key words: fortress machine; network; design; mode; security

伴随网络信息科技的突飞猛进发展, 信息网络安全等级保护制度[1]的日益被社会的各个企事业单位重视和落实, 针对企事业单位内部的局域网络中存在的各种安全性问题[2], 有诸多企事业单位采取诸多先进的信息科技管理理念和技术来加强单位的网络安全管理[3]. 针对高校来说, 需要防护和保护的系统众多, 包括学校主页、教务系统、财务系统、人事系统、资产设备管理系统、图书管理系统、档案管理系统等诸多业务应用系统[4].

除开保护这些信息系统本身之外, 还需对各个负责应用信息系统运维二级单位的网络系统管理员和相配套的公司技术人员加强管理. 堡垒机[5]作为其中一种重要的技术手段和解决方案, 能够较好满足企事业单位内部各个安全维度的安全管理需求.

堡垒机[6], 又称之为访问控制网关, 其主要是用来防护特定区域网络内的网络信息系统的一种设备, 堡垒机主要是保护两个层面, 一个是外部的用户访问入侵和恶意破坏, 另一个层面是防护内部用户对网络信

① 收稿时间: 2017-02-20; 修改时间: 2017-03-20; 采用时间: 2017-04-05; csa 在线出版时间: 2018-02-09

息资源的访问入侵和恶意破坏, 依托多种技术措施和手段来实时监控和搜集堡垒机防护范围内的网络环境下的每个组成元素的使用状况、系统实况、操作流程、网络时间、网络行为等, 为网络信息化建设者和网络安全管理人员提供行为审计、操作备案, 以便后期的规范管理.

堡垒机的分类多种多样, 从功能角度看, 堡垒机主要具备如下两个功能[4–6]:

(1) 安全设计管理和控制功能: 依托堡垒机能够起到一定的安全审计功能, 包括事前防御、事中预警的各种有效风险控制策略, 也是事后追溯偶的重要证据源头.

(2) 核心系统运维管理功能: 通过切断和阻隔普通终端用户对核心网络信息系统和服务器的直接访问, 而是需要首先登录堡垒机, 再依托堡垒机登录和管理其他的服务器, 终端用户会依托协议代理的模式协助终端用对核心网络信息系统和服务器的访问和操作.

1 堡垒机技术原理和功能分析

1.1 网络信息资源监管问题分析

伴随网络信息技术的日益深入应用, 各种网络信息系统越来越多, 园区网的规模越来越大, 数量 越来越多, 数量庞大和业务繁杂的网络信息系统为园区网的网络建设者和网络安全管理员带来各种如下的压力和风险:

(1) 多个用户使用同一套账号和密码: 系统构建之处, 因为业务部署需要和人力资源有限, 仅有的系统超级管理员账号唯一, 而需要使用的运维管理用户众多, 使得这些管理员共同这一套超级管理员的账号和密码, 使得后期监管出现真空地带, 没法对账号的具体使用人员进行限定和控制, 进而存在实名认证不严的风险.

(2) 一个用户使用多套账号和密码: 因为信息系统规模大、数量多, 而运维的人员有限, 有的用户需要身兼数职, 包括系统管理员、运维员、安全管理员、审计员、数据库操作员等多重身份和角色重叠, 需要从多套网络设备和网络信息系统之间多重的切换, 增加管理员的记忆负担, 并降低工作效率, 并带来多套用户和密码的泄露隐患.

(3) 缺乏统一标准化的授权管理系统: 业务的众多带来的就是管理环节和业务操作次数频繁, 使得权限分配难度加大, 难以做到精细化的管理控制, 对核心的业务系统只能实现粗放似管理, 难以对某一个用户对某一个系统的某一项操作做到细粒度的访问控制授权.

(4) 无法做到访问控制内容审计: 传统的网络安全审计设备无法对用户常见的 SSH 和 RDP 等加密和图形化的操作协议执行内容审计操作, 使得各项核心的主要操作无据可查, 对核心信息系统的管理带来巨大的风险和隐患.

1.2 堡垒机技术原理分析

“堡垒”寓意一般是用于防守的坚固建筑物或形容难于攻破的物体, “堡垒机”则寓意为专门预防攻击而设定的主机, 通过将用于堡垒防护用的主机安全加固后, 使其足以防御一般, 网络攻击, 并将其布设在核心网络信息资源的前端, 使其作为坚强的“堡垒”, 在提供正常服务前提下, 确保其防护的资源安全.

结合堡垒机的概念和应用需求分析, 堡垒机实现的技术原理一般如下: 堡垒机需要搜集和保存运维人员对核心网络资源的操作行为, 分析其操作内容来实现精细化的权限控制和后台操作行为审计, 一般堡垒机还可以通过代理技术完成堡垒机如下管理机制:

首先是运维员登录和连接到堡垒机, 并向堡垒机提出操作申请; 其次是堡垒机通过核验操作员的身份和权限之后, 依托堡垒机自备的代理模块将替用户连接到核心的网络信息资源, 并提供操作平台; 最后, 核心网络信息资源将操作结果反馈给堡垒机, 操作完成.

依托堡垒机管理机制, 完成了逻辑上面运维管理人员和核心网络信息资源的分离, 构建基于网络管理员、堡垒机账号、授权访问控制、目标设备的管理机制, 解决图形协议和加密协议无法通过协议还原审计的难题.

1.3 堡垒机核心功能概述

堡垒机的核心功能很多, 有代表性的主要体现在如下方面:

(1) 支持账号和权限的细粒度管理, 对账号能够配置详细和精确的访问控制策略, 对网络设备、服务器设备、主机设备及安全账号之间进行集中管理和细粒度关联, 使得用户与系统和操作之间做到一一对应, 以满足细粒度访问控制授权的安全需求.

(2) 支持用户运维全生命周期的操作审计, 用户依托账号登入堡垒机后, 能够借助堡垒机管理平台, 登入管理员分配给他的网络信息系统资源, 配置相关的协议要求, 实现核心服务器资源的访问控制, 这个访问控

制过程将被堡垒机全生命周期记录和备案.

(3) 灵活的资源授权管理: 堡垒机为设备提供各种灵活的细粒度资源管理功能, 包括对服务器资源的对象 IP、操作协议类型、协议端口进行设定, 并且依据对账号的 IP 限制和账号有效期的设定, 可以实现对访问控制主体的灵活控制, 确保访问控制中网络信息系统的安全.

2 基于主备模式的堡垒机网络架构

2.1 基于主备模式的堡垒机网络架构设计

常见的单机堡垒机部署适合小规模的园区网, 主要网络架构包括堡垒机单机一台、园区网核心、用户及服务器区. 这种布局模式适应用户规模小、服务器数量少的应用场景, 对堡垒机的双机冗余与服务连续性要求不高, 这种网络架构部署的优点是成本低, 部署快, 对网络架构影响小, 不足之处是存在单点故障.

针对较大规模的园区网安全需求, 基于单点模式下堡垒机网络架构的无法满足, 故此, 需要部署基于主机、备用机等双机模式和冗余网络架构. 以某高校为例, 经过多年的信息化建设, 已建成五百余台服务器, 且已建成独立初具规模的数据中心, 但是存在运维人员规模大、对堡垒机实时性服务和持续性服务要求高等部署需求, 故此需要部署双机模式.

结合主备模式堡垒机网络架构部署要求, 考虑到有数据中心、学校核心、应用防火墙等要素, 特此设计主备模式堡垒机网络架构, 如图 1 所示.

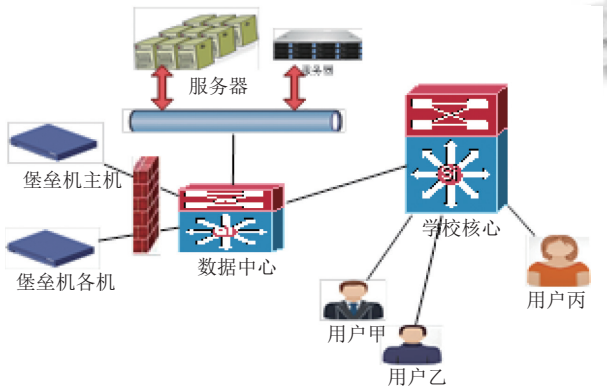

图 1 基于主备模式的堡垒机构拓扑图

堡垒机位于数据中心辖区内, 与需要保护的机器路由可达, 并无缝衔接到现有的 WEB 应用防火墙 WAF 的防护体系之内, 故此, 需要将堡垒机的网络架构嵌套应用防火墙之内, 为数据中心和外界网络构筑安全防护框架, 所有途径堡垒机的流量需要经过 WAF 进行分析和保护, 提升堡垒机的安全防护水平.

堡垒机双机的配置, 最好是配置专属的单独局域网, 从数量层面来说, 部署基于冗余主、备的堡垒机系统至少需要三个 IP 地址资源, 以此来配置主机 IP、备机 IP、浮动 IP. 主机 IP 和备机 IP 需要配置之前确保 IP 接入交换机分配的端口和 Vlan 配置正确, 且需要保证 IP 地址资源没有被占用.

2.2 基于主备模式的堡垒机网络配置分析

基于主备模式堡垒机主要部署在数据中心下, 但是需要通过学校核心和数据中心之间的应用防火墙之中, 故此, 主要的配置步骤需要一方面在学校核心上配置静态路由, 一边需要在数据中心层面配置策略路由, 并要考虑冗余. 数据中心包括核心 1 和核心 2, 网络配置如下:

在数据中心 1 上配置堡垒机网络:

```
vlan 2024
interface Vlan2024
  no shutdown
  no ip redirects
  ip address 10.10.110.11/28
  hsrp version 2
  hsrp 2024
    preempt
    ip 10.10.110.14
```

在数据中心 2 上配置堡垒机网络:

```
vlan 2024
interface Vlan2024
  no shutdown
  no ip redirects
  ip address 10.10.110.12/28
  hsrp version 2
  hsrp 2024
    preempt
    ip 10.10.110.14
```

学校核心需要为堡垒机的三个核心 IP 配置静态路由, 主机 IP 为 10.10.110.1; 备机 IP 为 10.10.110.2; 虚拟 IP 为 10.10.110.3, 第一 IP 的静态路由配置如下:

```
ip route-static 10.10.110.1 32 Vlan-interface2010
172.22.0.122 preference 200
```

ip route-static 10.10.110.1 32 Vlan-interface2009 172.22.0.90 preference 250

2.3 基于主备模式的堡垒机操作权限设计

堡垒机操作的角色分类包括 3 类: 堡垒机审计员、堡垒机操作员、堡垒机系统管理员, 各个操作角色定位如下:

堡垒机审计员: 记录和审计各个堡垒机中操作的日志, 确保对堡垒机所有的操作有记录并可追溯.

堡垒机操作员: 堡垒机操作员依据堡垒机管理员给其分配的网络信息系统资源进行运维管理, 确保在堡垒机防护体系下对网络信息系统按照要求和规则运维, 确保业务是在堡垒机的监管范围内.

堡垒机系统管理员: 堡垒机系统管理主要有如下几个核心功能, 一个是对堡垒机操作员的管理, 包括新增、删除、修改所有操作员的属性.

综上所述, 在堡垒机操作的角色分类之中, 权限最复杂和应用最广泛的就是堡垒机系统管理员, 其还可以对操作资源进行管理, 包括新增网络信息系统资源, 并且对其中的操作方式和协议进行配置, 比如对 Windows 操作系统来说, 主要是配置其远程桌面协议 (RDP, Remote Desktop Protocol), RDP 协议是一个多通道 (multi-channel) 的协议, 能够为堡垒机提供远程桌面服务. 对 Linux 操作系统来说, 主要是配置其 Secure Shell 服务, 简称 SSH 协议, 其由 IETF(互联网工程任务组, Internet Engineering Task Force) 的网络小组 (Network Working Group) 所制定, SSH 为建立在应用层基础上的安全协议, 能够为 Linux 类操作系统提供操作和管理 Linux 系统的相关服务.

2.4 基于主备模式的堡垒机测试案例

测试案例一. 堡垒机的对操作行为的审计功能测试. 通过堡垒机的审计功能模块, 能够方便对近期操作的堡垒机行为审计展示和追溯, 如图 2 所示, 能方便展示出堡垒机操作员的登录时间、登录 ip 地址、登录的资源、操作的策略等元素信息, 较好解决网络信息安全的监管不到位的问题, 方便对堡垒机的行为审计.

测试案例二. 堡垒机单机故障.

测试过程: 假设一台堡垒机出现故障, 网络不通, 业务不通, 交替测试的结果显示, 另一台工作正常, 并不影响堡垒机的整体业务, 足以证实其主备机的稳定.

主备堡垒机单点故障时到虚 IP 的网络测试如下:

C:\Users\administrator>tracert 10.10.110.3

通过最多 30 个跃点跟踪:

到 baoleiji [10.10.110.3] 的路由:

1 <1 毫秒 <1 毫秒 54 ms 本地网关

2 * <1 毫秒 <1 毫秒 172.22.0.17

3 <1 毫秒 <1 毫秒 <1 毫秒 172.22.0.122

4 <1 毫秒 <1 毫秒 <1 毫秒 10.10.110.3

通过 tracert 的网络测试可验证在单台堡垒机出现故障时, 虚 IP 的网络一直畅通, 业务不受影响.

图 2 堡垒机操作行为审计界面

3 总结

本文分析和总结了堡垒机相关的概念和功能定位, 探讨堡垒机的工作机理, 对堡垒机增强高校园区网内的各项有力措施进行分析和阐述, 分析和讨论基于单点的堡垒机架构和基于主备的堡垒机架构优缺点, 并对基于主机、备机的堡垒机网络架构进行设计和配置, 给出基于冗余的堡垒机网络架构设计核心环节, 并给出数据中心、学校核心的配置代码, 最终分析和总结堡垒机中三种常见角色及角色功能定位.

参考文献

1 王栋, 来风刚, 李静. 数据中心 IT 运维审计体系研究. 电力信息化, 2012, 10(1): 20–23.

2 杜宁宁, 赵庆亮. 浅谈信息安全审计在金融行业的实践. 中国内部审计, 2012, (4): 66–68.

3 蔡蔚. “互联网+”时代网络安全分析与管理策略研究. 信息安全与技术, 2015, (9): 8–11.

4 韩荣杰, 于晓谊. 基于堡垒主机概念的运维审计系统. 信息化建设, 2012, (1): 56–59.

5 钟平, 王会林. 高校网络安全实验室建设探索. 实验室科学, 2010, 13(1): 122–124.

6 洪允德, 高强. 计算机网络安全课程实验教学探索. 中国教育技术装备, 2014, (22): 146–148. [doi: 10.3969/j.issn.1671-489X.2014.22.146]