对于堡垒机，这些价值到底可以体现多大，还是看公司的需求及现状而定，有些公司使用堡垒机只为满足一些合规要求，比如自身行业监管对其业务系统等保三级的认证要求，用以实现等保三要求的双因素认证和操作审计等，只为合规而合规；当然也有公司真正把这个设备物尽其用，比如每个团队一个堡垒机，当然我们公司虽然没夸张到一个团队一台，但也相对用的比较深，这里跟大家唠唠细节。

简单先从堡垒机几大核心点及对应技术上要实现的效果做罗列说明：

## **背景**

### **1、用户账号**

一阶：手动倒入堡垒机新增用户账号；

二阶：通过Api推送新增用户账号；

三阶：与内部统一登录平台或AD域对接，自动化新增和回收用户账号。

### **2、认证**

一阶：静态账号密码认证；

二阶：静态口令+短信、静态口令+googleauth、静态口令+硬件key；

### **3、设备**

一阶：手动倒入目标设备；

二阶：与公司内部CMDB对接，API自动同步设备。

### **3、权限**

一阶：通过邮件发起权限的申请和变更，需直接领导及相关人员审批；

二阶：通过内部OA发起权限的申请和变更，需直接领导及相关人员审批(此处优势在于便于外审、it审计等的数据提供)；

补充：人员活水涉及到的权限变更，我采用的是开发脚本实时监控内部人力资源的接口，如识别到人员组织结构调整，自动化发送邮件给对应的人员进行二次权限确认。

### **4、系统账号的密码&密钥**

一阶：普通用户登录访问目标设备，手动输入账号密码登录；

二阶：所有设备由管理员统一批量代填，并安全需求分配给对应用户，并通过堡垒机自身密码修改功能定期修改；

补充：此处的密码管理员采用双人负责，一人负责静态密码，一人负责绑定动态密码，两人共同操作密码的备份和批量修改工作。

### **5、审计**

一阶：通过日常抽查、报表模版、命令报表等进行审计；

二阶：通过api定制化开发报表，例：监控堡垒机上的所有配置变更（人员设备的增删改茶、权限的变更）形成报表，并作可视化展现等。

### **6、rdpapp发布**

一阶：放弃此项功能；

二阶：部分人员使用此项功能，但为保证效率大量图形化操作依然通过其他方式访问实现；

三阶：全部通过此项功能访问。

补充说明：此处并非追求盲目的一刀切，部分资源虽然部署在生产网，但因其自身安全性较高且数据价值较低，可以选择放开网络至允许办公网络直接访问，安全组进行重点监控。

上述都是单纯从技术层面做的介绍，3分技术，7分管理，可以说一切可以用技术实现的问题都不是问题，但是一旦涉及到人，就需要我们有自己的套路、打法和管理手段来搞定，也是一个项目如何建设、推广、运营好的关键。

简单跟大家聊聊我司堡垒机的建设推广运营过程：

## **一、项目目标：**

堡垒机作为公司员工访问生产网的唯一途径。

## **二、产品选型和测试：**

挑选了全国最好的4家堡垒机厂商做部署测试，测试重点在于各个厂商对于应用发布的能力上，如何实现百人级别的图形化并发和用户彼此之间的数据隔离。

## **三、项目建设**

### **1.现状及需求**

公司生产网存在3000台左右机器，700人左右的用户访问，访问需求包括Linux的ssh访问，windows的rdp访问，数据库、相关分析平台及管理后台的rdpapp访问。

### **2.设备部署**

堡垒机双击HA部署，发布服务器（高内存、cpu和独立的显卡很重要）起虚拟化，网络层面部署在安全管理区，只允许办公网访问，办公网到机房存在单独的物理专线。

### **3.需求调研&试运行**

跟各个对生产网又需求的团队人员沟通访问生产网所需的图形化工具，并协调公司对生产网访问需求最复杂的团队配合访问测试，团队如：IT运维团队、安全团队、DBA、MA、BA。访问方式包括ssh、rdp、rdpapp。重点放在rdpapp这种图形化工具方面，适配包括Chrome等10几款工具。

### **4.分阶段推广**

推广期是最难的时候，意味着大量的人要陆续放弃使用便捷快速的openvpn变换到一个登录麻烦、访问受限、操作被审计的堡垒机场景，就像本来大家吃着锅唱着歌，突然就被安全团队给“劫”了。

[](https://image.3001.net/images/20190306/1551802682_5c7ea13a8175c.jpeg)

那如何让大家心甘情愿被安全组“劫”呢，方法如下：

**a、准备充足，弹药充分**

提前搭建好需求调研阶段用户所需的所有环境，准备好操作手册、操作视屏录像、试运行阶段的共识记录等。在公司内部年会、技术总结会中站台，分享安全已经做的和即将做的工作，由CEO、CTO等配合站台，为以后的安全工作推广埋下伏笔。

**b、分阶段推广，先对自己人“下手”**

推广第一阶段是对跟安全团队同属于CTO直管的所有业务技术支撑团队，项目的第一枪必须打响，且必须有个成功案例来证明和推动后面难啃的业务方。

**c、沟通、共识、协调**

沟通是拉近人与人之间最快的手段，不断与各相关团队的PO（敏捷文化）、技术总监、VP等沟通堡垒机的意义、重要性和推广安排，达成共识，协调本团队人员配合提交个人访问需求，完成堡垒机的推广工作

**d、过程和结果同样重要**

每个推广阶段都进行多次的使用培训、问题答疑、维护驻场，一个推广阶段完成会形成总结报告群发相关人及领导告知，不仅是对工作的记录总结，也是变相对相关人员的督促。

### **5.监控**

在防火墙、主机防护产品中添加策略，如出现异常登录访问进行告警，防止个人通过非堡垒机访问访问生产网的相关资源。

### **6.运维**

通过如zabbix等方式对设备进行实时监控，保证sla在4个9以上；

定期对账号、权限、操作、日志等进行检查，日常报告至少周报一份，正常报告至少每季度一份（外审、IT审计等都会用的上）；

其他运维内容可根据公司文化自行设计，如技术中提到的定制化的可视化监控等。

## **四、项目制度和方案**

管理层面建议有如下但不仅限于内容：

《堡垒机使用管理制度》

《堡垒机权限管理规定》

《堡垒机应急方案》截取自己写方案中的一段内容作为分享：

如果堡垒机设备出现故障导致无法登录时，要尽快启动应急预案，降低对运维操作的影响。具体流程如下：

当堡垒机故障无法登录时，需要运维人员为相关人员开通sslvpn权限，相关人员可以通过vpn直接登录目标设备；

如运维通过堡垒机密码托管方式访问业务，当运维堡垒机故障无法登录时，需要密码保管员在第一时间将设备密码交付给相关运维人员，运维人员凭借密码保管员提供的密码可以直接登录目标设备；