安恒信息
DAS-security 安全中国

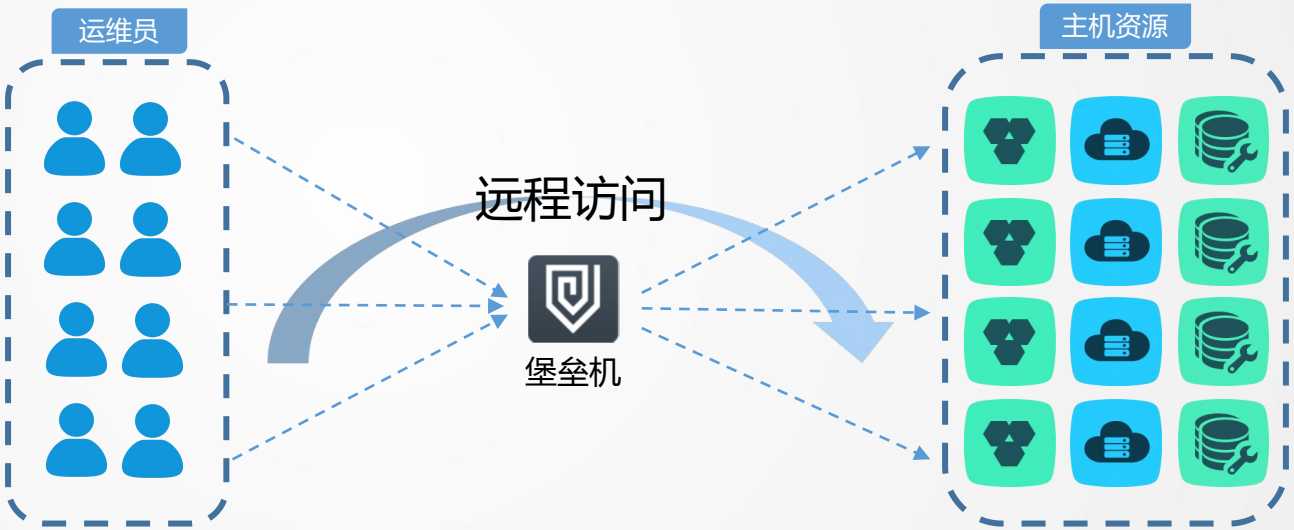
安恒堡垒机远程办公IT运维安全解决方案

演讲人：吴焱

www.dbappsecurity.com.cn

目 录
Contents

什么是堡垒机



统一认证　统一管理　权限控制　集中审计

为什么需要堡垒机

安恒信息 DAS-Security 安全中国

数据泄露严重

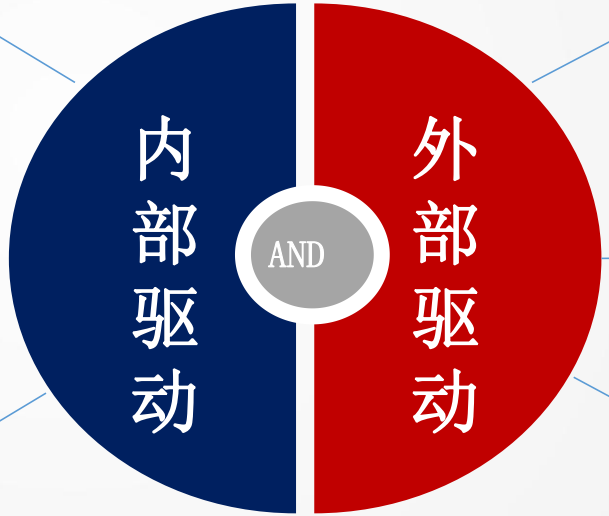
- 华住5亿开房数据泄露
- 某省公安厅住房信息泄露
- 上海某医院新生儿记录泄露

运维事故频发

- 携程网宕机事件
- 阿里云服务瘫痪
- Gitlab服务瘫痪

IT运维内控

- 共享账号泛滥
- 权限控制难
- 违规操作难审计



《网络安全法》

- 采取网络安全技术措施
- 日志留存不少于六个月
- 按照等保制度、违法处罚

《等保2.0》

- 用户身份鉴权
- 用户访问权限控制、最小化授权原则
- 运维操作完整审计、定期备份

《行业规范》

- 运营商：电信企业行业相关规定
- 金融证券：央行政策，银保监检查为主
- 上市公司：《企业内部控制基本规范》

目 录
Contents

疫情期间远程办公IT运维现状

安恒信息 DAS-security 安全中国

新型冠状病毒正在全国肆虐，企业单位纷纷响应国家号召，积极开展远程办公，但随之而来的安全问题也日益明显，尤其针对IT运维人员，需要保障企业单位内部的业务服务正常，面临诸多难题：

疫情期间，业务上线怎么办？

重点服务异常，如何紧急维护？

远程办公期间，如何保障运维合规？

中小型企业，医疗、教育等单位抗风险能力较差，现有安全合规性建设难以满足当前疫情形势下的运维安全，如何降低企业损失，并满足疫情期间的隔离要求，成为各企业单位开展远程办公IT运维安全建设的难题。

现有中小型企业远程IT运维场景主要有一下几类：

无VPN无堡垒机

- 不具备远程IT运维能力
- 需要将重要业务对公网开放，安全风险高
- 即使可以远程运维，也无审计不合规

有VPN无堡垒机

- 仅具备远程IT运维的网络接入
- 权限控制不足，存在越权操作风险
- 文件传输无法控制，存在数据泄露风险
- 运维操作无审计，事后难以追溯不合规

无VPN有堡垒机

- 堡垒机在内网，外网无法直接访问
- 需要将堡垒机对公网开放，端口映射存在风险
- 运维链路传输不安全

独立VPN+堡垒机

- VPN和堡垒机是不同厂商，认证体系独立，需要先拨VPN，再登堡垒机，使用过程繁琐，效率低
- 需要单独购买VPN设备和堡垒机设备，建设成本高，部署不方便

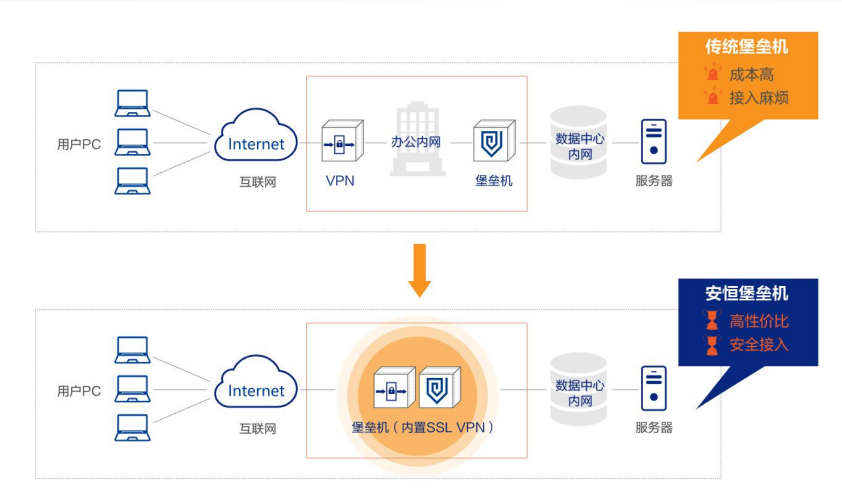
目 录
Contents

安恒堡垒机—本地部署解决方案

安恒堡垒机+内置SSL VPN交付：

安恒堡垒机集成了SSL VPN功能模块，只需将VPN服务端口映射互联网，即可实现远程IT运维，保障了远程运维接入安全性的问题，同时通过堡垒机单点登录服务器进行远程运维操作，即解决了外网接入的链路安全，同时保证运维过程的权限控制，操作审计及合规要求。

网络拓扑



核心价值

- **SSL VPN安全接入，保障远程IT运维链路安全**
- **严格的访问权限控制，降低远程IT运维风险**
- **文件传输双向控制，保证远程IT运维的数据安全**
- **远程IT运维操作全程审计，保证远程IT运维合规**
- **疫情期间，堡垒机+VPN功能免费使用**

适用场景

- **适用于需要远程IT运维的中小型企业，以及教育、医疗等行业客户**
- **适用于多数据中心，实现统一运维入口，资产统一管理**

安恒堡垒机—本地部署解决方案交付说明

同时支持硬件一体机或软件交付，在疫情期间，

1.全行业支持：均享受免费软件堡垒机服务，直至疫情结束。

2.对于医疗行业、公安、网信等监管单位，需要硬件支持的可免费提供硬件一体机（使用权）。

硬件一体机交付规格：

产品型号	DAS-USM150	DAS-USM200	DAS-USM800	DAS-USM500	DAS-USM1000
产品规格	资产数：100 并发连接数：100	资产数：200 并发连接数：200	资产数：600 并发连接数：600	资产数：500 并发连接数：500	资产数：1000 并发连接数：1000
VPN规格	可选10/20并发	可选10/20/50并发	可选10/20/50/100并发	可选10/20/50/100并发	可选10/20/50/10/200并发

软件交付规格:(支持远程部署交付，客户自行提供虚拟机环境)

产品型号	DAS-USM100-PRO	DAS-USM200-PRO	DAS-USM500-PRO	DAS-USM1000-PRO
产品规格	资产数：100 并发连接数：100	资产数：200 并发连接数：200	资产数：500 并发连接数：500	资产数：1000 并发连接数：1000
VPN规格	可选10/20并发	可选10/20/50并发	可选10/20/50/100并发	可选10/20/50/100/200并发
虚拟机最低配置要求	4核CPU，8G内存，双硬盘：100G系统盘，1T数据盘	4核CPU，8G内存，双硬盘：100G系统盘，1T数据盘	4核CPU，8G内存，双硬盘：100G系统盘，1T数据盘	8核CPU，16G内存，双硬盘：100G系统盘，2T数据盘

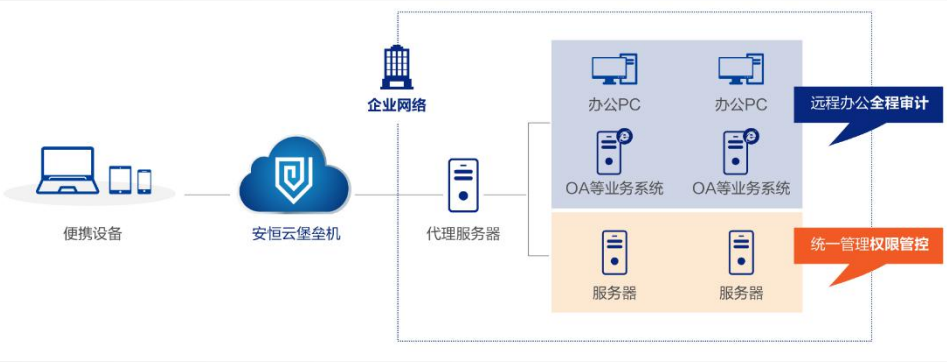
注：部署版本需升级到2.0.8.2以上版本，并申请具备VPN授权的许可，疫情期间按月提供免费授权许可

安恒堡垒机—混合云部署解决方案

安恒云堡垒+Proxy代理：

云上部署安恒云堡垒机，只需在企业内部局域网中，配置一台Proxy代理服务器，与云堡垒机服务网络互通，即可实现免费的远程IT运维使用

网络拓扑



核心价值

- **极速交付，快速部署：在阿里云、腾讯云市场搜索“安恒堡垒机”，镜像交付，一键部署。**
- **配置简单，急速上线：仅需要提供一台windows或linux服务器作为代理服务器，没有VPN也可以远程办公。**
- **使用简单，无需插件：只要您电脑上有浏览器，就可使用，无需安装任何软件。**
- **精细控制，全程审计：权限精细划分，操作全程录像审计，安全加倍。**

适用场景

- **适用于需要远程IT运维的中小型企业，允许审计数据云上存储，可按月付费**
- **适用于多云、多数据中心场景，实现统一运维入口，资产统一管理**

安恒堡垒机—混合云部署解决方案交付说明

使用流程

1. 购买免费镜像：
   - 阿里云市场购买链接：https://market.aliyun.com/products/56844019/cmjj028076.html?
   - 腾讯云市场购买链接：https://market.cloud.tencent.com/products/5735
2. 提供一台windows或linux服务器作为代理服务器（支持HTTP、SSH、SOCKS5代理即可，映射到公网供堡垒机接入）。
3. 为每个用户授权自己的办公电脑，即可通过堡垒机连接到内网办公电脑，进行日常办公。
4. 为服务器维护人员授权日常维护的主机，通过RDP，SSH，SFTP进行日常主机维护操作。

免费使用，为“战疫”出一份力

1. 抗击疫情结束前，提供免费云堡垒机服务，让您轻松远程办公，安全运维！
   - 全行业支持：均享受免费云堡垒机服务，直至疫情结束。
   - 医疗行业及相关监管单位：提供1年免费云堡垒机服务。

2. 获取免费正式许可：下单安恒云堡垒机许可，并联系客服改价。
   1. 阿里云市场购买链接：https://market.aliyun.com/products/53366009/cmfw023700.html
   2. 腾讯云市场购买链接：https://market.cloud.tencent.com/products/5635

产品规格	50资产	100资产	200资产	500资产	1000资产
规格	资产数：50 并发连接数：50	资产数：100 并发连接数：100	资产数：200 并发连接数：200	资产数：500 并发连接数：500	资产数：1000 并发连接数：1000
原价	1580元/月	2380元/月	3980元/月	5780元/月	8080元/月

安恒堡垒机远程运维方案优势

安恒信息
DAS-Security 安全中国

01 远程运维安全接入

内置SSL VPN功能，实现远程运维的安全接入，保证数据传输安全

02 统一认证，高效运维

VPN与堡垒机使用相同的账号体系，只需一次认证，即可单点登录堡垒机运维，提高运维效率

03 灵活的权限控制

用户只能运维堡垒机中已授权的服务器，降低越权操作，高危操作风险

04 运维审计满足合规

所有远程运维操作，堡垒机都可以进行审计录像，方便事后追踪溯源，满足合规建设要求

05 文件传输双向控制

堡垒机支持灵活的文件传输双向控制，可以只允许上传不允许下载，且支持传输文件留存，有效防止数据泄露风险

06 建设成本低

VPN与堡垒机二合一，方便部署，建设成本低，管理方便
云堡垒机方案急速部署，可按月付费

安恒信息
DAS-security 安全中国

谢谢观看

Thanks for watching

www.dbappsecurity.com.cn