# 关于加强防范
# 勒索病毒及网络攻击的安全提示操作指引

# 目录

# 1.概述

为了确保金蝶产品能够正常运行，不出现感染勒索病毒、数据泄露等安全问题，特制定本操作指引。

# 2.操作指引

## 2.1 只开放必要的网络端口至互联网

- 对外禁止开放不安全协议，在防火墙/路由器上 DNAT（配置虚拟 IP，配置策略 ACL）中仅映射 https（默认 443 端口）协议，http（默认 80 端口）协议对外开放，即对外开放服务（协议）必须为 HTTP 或 HTTPS（见下图），禁止对外开放 RDP 协议（3389 端口）、SSH 协议（默认 22 端口）、RPC 服务（默认 135-139）、Simba（默认 445 单口）等高危协议及端口（如 FTP、SIP、MySQL、Oracle、redis 等），内部服务器开放协议默认禁止（见下图）：


图 1：配置示例（防火墙）

- 对于应用程序使用访问，内部做好访问控制（如仅财务部门办公网络可访问），运维端口/协议（RDP、SSH、Redis 等）仅对运维设备（建议：安全运维堡垒机）开放。

## 2.2 ERP 系统安全加固

确保安装 ERP 系统最新的安全稳定版本或者补丁（见下表）。

| 序号 | 产品 | 建议版本 | 获取方式 |
| --- | --- | --- | --- |
| 1 | 金蝶云苍穹/星瀚 | 建议 CONSTELLATION.V4.0.008 以上版本<br>推荐版本：<br>CONSTELLATION.V5.0.006 | 下载链接：<br>https://download.kdcloud.com/download/?code=16618263301ac37eebfacdda4a9f3d28 |
| 2 | 金蝶云星空 | PT-146922 8.0.0.20220811<br>发布时间:2022/8/11<br>（金蝶云星空 V7~V8） | https://open.kingdee.com/K3Cloud/Open/PTHistory.aspx?product=BM0JA8DBhNnPB5vdIo%2fyYEpoaTUJ%2fnngd7nZwMm9%2bcP%2fvALzQIDBpJ7s79L97TAVS%2bIBi0FoiTgaYz0u%2b5HA3If0Lt5aVvyaOzGgAZteQAa9KnQHiRUIIjAUaMNdsgI8YNK%2fslrKAEoMjSxDd4KhXzffJ%2bJQ%2fU5Y00M1PAIZdc0%3dThisIsSplit&type=A |
| 3 | EAS Cloud | 1、7.5 及以下版本已退出生命周期，无补丁修复支持，请推动升级<br>2、8.0 及以上及时安装加固补丁 | 安全修复补丁（8.0）<br>https://vip.kingdee.com/link/s/Mip4G<br>安全修复补丁（8.2）<br>https://vip.kingdee.com/link/s/Mip4y<br>安全修复补丁（8.5）<br>https://vip.kingdee.com/link/s/MiMqx<br>安全修复补丁（8.6.0）<br>https://vip.kingdee.com/link/s/Mip42<br>安全修复补丁（8.6.1）<br>https://vip.kingdee.com/link/s/MiMqT |

| | | | |
|---|---|---|---|
| 4 | KIS 云 | 使用 KIS 云产品或相关工具的私有云客户建议升级到公有云或者参照以下清单升级到安全加固版本，以便获得更强的安全防护，如 SQL 防注入、强密码策略、私有云账套自动云备份功能等<br>KIS 云安全加固系列产品<br>旗舰版 V7.0.1<br>发布日期：2022-07-21<br>专业版 V16.0.2<br>发布日期：2021-12-31<br>商贸版 V9.0<br>发布日期：2018-11-01<br>标准版 V14.0<br>发布日期：2021-11-19<br>迷你版 V14.0<br>发布日期：2021-11-19<br>KIS 云安全加固相关工具<br>KIS 云客户端 V8.6<br>KIS 云桌面服务端 V8.0.4<br>KIS 私有云服务端 V7.0.8<br>金蝶云·远程办公助手_客户端 V2.2<br>金蝶云·远程办公助手_服务端 V2.1 | KIS 云系列产品链接：<br>https://vip.kingdee.com/knowledge/specialDetail/341901700862361344<br>KIS 云相关工具链接：<br>KIS 云客户端 V8.6 获取地址：<br>https://kisyun.kingdee.com<br>KIS 云桌面服务端 V8.0.4 获取地址：<br>https://kisdoc.kingdee.com/web/#/56/880<br>KIS 私有云服务端 V7.0.8 获取地址：<br>https://kisdoc.kingdee.com/web/#/20/246<br>金蝶云·远程办公助手_客户端 V2.2<br>金蝶云·远程办公助手_服务端 V2.1<br>获取地址：<br>https://www.jdy.com/products/remote-work/ |
| 5 | s-HR | 1、金蝶 s-HR V1.5 及以下版本已退出生命周期，无补丁修复支持，请推动升级<br>2、金蝶 s-HR V8.2 及以上及时安装加固补丁 | https://pan.yunzhijia.com/edit#/507146560702775296/ |
| 6 | WISE | 15.1SP | https://k3mobile.kingdee.com/GrayscalePatch |
| 7 | 金蝶建筑房地产(EAS) | 同 EAS | 底层与 EAS 一致，安全版本参考 EAS |
| 8 | 金蝶建筑房地产(苍穹) | 同苍穹 | 底层与苍穹一致，安全版本参考苍穹 |

| | | | |
|---|---|---|---|
| 9 | 金蝶云食神餐饮 | 金蝶云食神餐饮<br>PT-001846<br>发布时间:2022/5/18 | https://open.kingdee.com/K3Cloud/Open/PTHistory.aspx?product=dFey4nX6SuD2eoW8WQvHGQBKhr3SMmPBu%2f7M0ESuBLnjaNQUexZHUo8IidGyJ5fOAndMIB4AfzgXHDVLF5DHzZA%2faxo1W7myRsEZDVnN2iIJgW7TkkKNZnu%2bvCBHTlMIHYMucrO3kmgbUs928sOrRQNdpB9o5PSd%2fEAhbSGLPpo%3dThisIsSplit&type=D<br><br>http://ksm.kingdee.com:8000/ccsp/patch!patchDownLoadMain.action |

## 2.3 做好数据备份

务必至少每天备份数据在不同存储上，且异地保存，并检查备份数据的可用性。对于云部署模式，应考虑异地或者跨云备份；对于本地机房，应离线备份至其它介质上。

## 2.4 加强密码管理，全面修改弱密码

- 遵守并严格执行符合相关技术标准和所属公司安全规范的密码要求
- 建议：所有密码必须设置强密码（数字+字母大小写+特殊字符四种中任选三种，长度不少于 8 位，建议定期（90 天-180 天）修改密码），服务器不要使用同一密码；

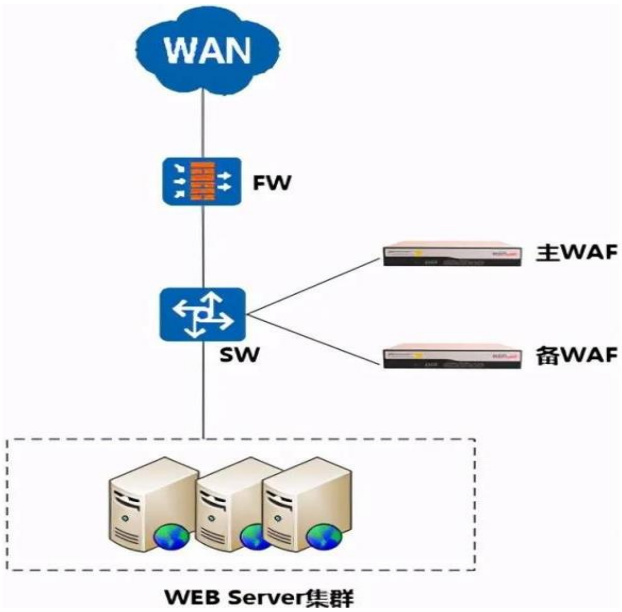
- 修改初始或默认帐号密码（服务器修改密码 linux：passwd XX 用户名 输入 2 次，windows-开始-设置-账户-登录选项-密码|域账户密码直接修改 AD 密码）。

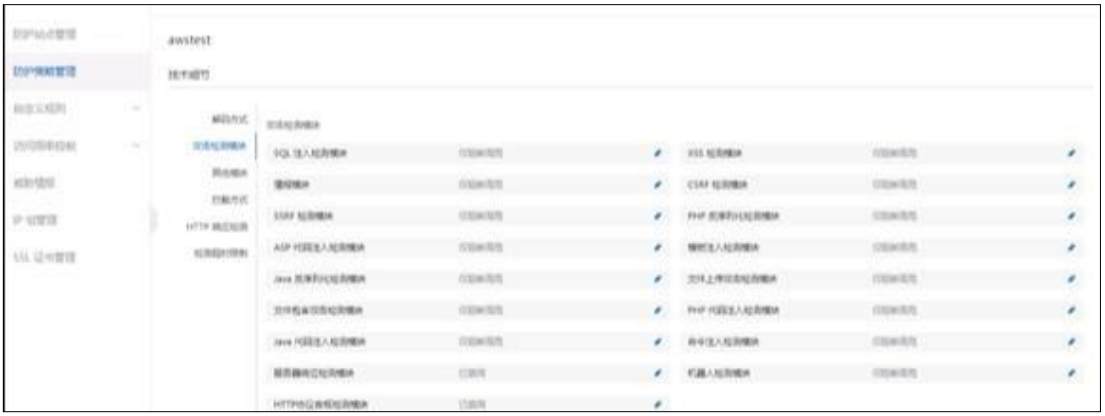


## 2.5 安装安全防御软件

为及时识别攻击，建议部署以下安全防护设备：

- 增加 WAF 设备，把 web 应用系统加入到 WAF 中进行防护，对开放的 HTTP&HTTPS 协议进行防护（串接 WAF-配置站点|上传证书-开启防护）必须开启的防护有基础防护、注入防护、XSS 等，防护策略不低于中；





- 增加主机入侵检测（HIDS）设备，对操作系统及容器进行入侵检测（部署 HIDS 管理控制台-打通网络-安装 agent-设置告警规则）；
- 在服务器上安装防病毒软件（推荐趋势、360、火绒、卡巴斯基等）（部署管理控制台-安装 agent/虚拟机-设置告警规则，定期更新病毒库）；



- 通过 WAF、防火墙等设备对安全攻击行为进行遏制（封禁 IP，黑白名单设置、频率限制等）。