敏行产品安全架构说明书

发布日期：2014 年 9 月

版本：V3.0

目　　录

1 引言 2
2 安全架构组成 2
2.1. 网络拓扑 2
2.2. 软件组成 3
3 整体安全设计 3
3.1. 信息安全 3
3.2. 入侵防范 4
3.3. 高可用架构 5
3.4. 系统备份和恢复 6
4 结论 6

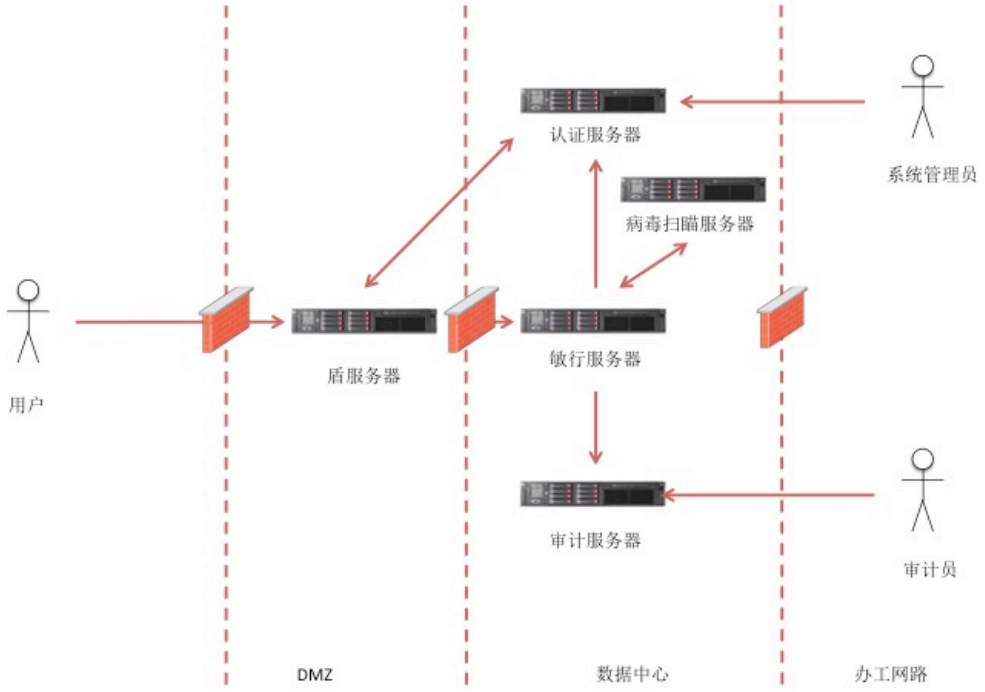
1 引言

敏行平台在系统的最初设计时，就非常注重产品的安全性。为了保护用户的数据，敏行平台使用了多种安全策略来进行防护，同时在架构上也建立完善的安全防护体系。本文档从安全架构层次讲述了敏行平台的的网络拓扑、入侵防范、高可用、系统备份与恢复的方案，

2 安全架构组成

2.1. 网络拓扑

敏行平台的安全防护架构由一系列的服务组成，包括应用防火墙、认证服务、审计系统、入侵检测系统、反病毒系统构成，架构图如下：



- 认证服务器负责对用户提交的凭证信息进行验证，敏行平台除了可以使用自身的安全认证之外，还可以利用企业内已经存在的 4A 认证服务，确保用户的

认证可以被系统管理员集中控制。

- 敏行服务器在系统授权和用户访问时，都会留存访问和审计日志，产生的审计日志可以和已有的入侵监测服务器集成。审计人员可以通过审计平台发现系统中的异常行为，可以指导系统管理人员完成对入侵行为的阻断操作。
- 盾服务器可以使用第三方厂商的应用防火墙或者基于 Redis、Nginx 构建。在管理员识别入侵或者攻击者的 IP 时，发出阻断命令，将非法的访问请求阻挡在外。
- 对于用户上传的文档数据，还可以使用病毒扫瞄服务进行发现、隔离，将危险的文件、网络地址在用户接触前进行阻挡。

2.2. 软件组成

敏行平台的安全架构软件由下列构成：

- 操作系统 Debain Linux 6.0.10 版本
- 盾服务器 Nginx 1.4.7 Redis 2.6.16
- 网络入侵检测 Suricata 2.0.4 elasticsearch 1.3.2 logstash 1.4.2 kibana 3.1.0
- 系统入侵检测 OSSEC 2.8.1
- 认证服务 LDAP V3 或第三方认真服务器
- 病毒防护 ClamAV 0.98.4 或者第三方服务器

3 整体安全设计

3.1. 信息安全

在信息的存储和传输上，敏行平台采用了多种方式保证信息的安全：

- 针对用户上传的文件，敏行平台使用 Gluster 来存放这些文件，为了保证文件的安全行，敏行平台使用了卷管理软件 LVM 来创建 Gluster 的分区并依靠

LVM 对文件系统进行加密。系统的维护人员无法通过克隆虚拟机镜像的方式来提取镜像上的内容。

- 用户的基本信息在敏行系统中是存储在数据库中的，敏行平台可以针对用户的敏感信息进行加密，防止管理人员使用维护帐户偷窥数据库中的内容。使用加密系统之后，每次数据写入数据库时进行加密。用户读取信息时，系统再根据内置的管理密钥进行解密，保证用户信息的安全性。
- 用户在敏行内设置的密码，都经过最高强度的 512 位密码加密，而且使用盐值来提高密码的强度，确保用户密码的存储安全。
- 敏行平台默认开启了全站的 SSL 的数据加密，确保用户传输的数据安全。虽然使用全站 HTTPS 的来加密数据，会消耗比较多的 CPU 计算资源，但这种方式下，数据发送更加安全，避免一些内容在传送过程中被替换，导致危险代码的注入。
- 在移动设备上，敏行的客户端会使用安全证书来校验服务器端的连接，如果中间人伪造一个站点，是无法通过客户端设备的校验的。
- 客户端软件默认会加密存储在手机上的信息，确保手机丢失后，手机上的内容资料不被非法获取。

3.2. 入侵防范

为了防止服务器被黑客入侵，敏行服务器在设计上采用了多中措施来保护服务器的安全。

- 敏行服务器默认开启了全站的 SSL 加密，使用敏行传输的数据都是加密的，并且手机在连接敏行系统时，对系统的证书进行安全校验，确保不会受到中间人的攻击。
- 在处理推送给用户手机的数据时，敏行系统也进行了双向的加密，确保所有传送的数据都是加密的。
- 敏行后台运行的程序默认都以非 root 用户身份运行，不允许 root 帐户在服务器上登陆。
- Linux 系统默认都会带有 iptables 的防火墙，可以在应用级别阻断非法的入

侵和嗅探。敏行系统默认打开了 iptables，并设定仅打开默认的端口，确保内部系统的信息不被外部所探测。

- 敏行平台中用户上传的文件会默认存储在分布式文件系统 Gluster 内，在上传后，文件的基本信息会保留在数据库中，文件名会被替换成一个安全的序号，防止文件名中被注入恶意代码而被内部处理程序所执行。为了防范用户上传恶意程序，系统默认的开放了文件存储的结构，可以配合企业内的防毒软件，进行文件内容的扫瞄，限制用户传播带有木马，蠕虫的文件。在另外一种情况下，黑客寻找到系统的漏洞后，尝试上传恶意代码，然后执行。为了防范这种形式的攻击，敏行还可以利用其他的分布式文件系统来存储文件内容，不会将文件直接存储在操作系统内，避免文件被直接执行的风险。
- 敏行服务器默认会记录系统的权限变化和敏感信息的访问记录，提供给审计平台和入侵监测程序，由入侵监测系统对异常行为进行识别和阻断。
- 为了防范代码级别的漏洞，敏行使用 Rails 的最新版本，防止系统出现 sql 注入，跨站点攻击等问题。

3.3. 高可用架构

敏行平台默认部署为双机主备模式运行，为了确保在故障发生时能快速进行故障转移，敏行对运行的主要服务都进行了冗余，采用了多种措施来保证服务的可用性。

- 最外层的 HAProxy 可以做成主备方式运行，将来自外部的请求负载均衡到两台服务器上。
- 两台服务器部署了敏行的运行环境，可以分别来自外部的请求。其中一台服务器如果出现故障，都可以被 HAProxy 识别，新的请求会被定向到另外一台正常的服务器上。
- 对于无法按照负载均衡方式运行的服务，例如 Mysql、Redis，系统将他们配置为主从复制的模式，主服务产生的数据，会实时复制到从服务器上。任何主服务器发生故障，都会被监控软件所捕获，监控软件会将服务从主服务器切换到从服务器上。
- 敏行的服务被设计在虚拟化的环境上运行，可以让用户非常容易进行服务的

扩展，迁移。故障发生时候，可以做到快速恢复，快速扩展。

- 用户上传的文件被保存在 Gluster 的分布式文件系统中，文件会在两台服务器中进行分布，任何一台服务器的存储发生故障，都可以在后续的恢复中进行修复。

3.4. 系统备份和恢复

敏行平台为了减少由于硬件故障，自然灾害为系统带来的服务中断，在系统设计的最初就让系统支持多机器，分布式运行，并且针对系统的持续运行采用了数据的冗余和实时复制的方案。

- 系统采用文件系统快照和数据库实时复制的手段为系统数据进行备份，可以做到因为故障引起的数据丢失降低到最小范围。
- 针对单独服务器的故障，系统使用 HA 软件进行自动维护，将失效的主机转移到其他可用的主机上。
- 敏行系统在部署上还可以为客户提供地理位置的数据分布，大幅降低用户因为数据中心故障带来的数据丢失风险。
- 敏行还可以为客户提供自动化的运维部署和恢复工具，大大缩短用户升级，数据恢复的时间。

4 结论

敏行平台设计了完善的安全架构，涵盖了网络、系统容灾、入侵监测、访问控制，因此可以为企业的运行提供良好的安全保护。