DBAplus

数据库年终盘点大会-上海站

Oracle数据库防火墙使用经验及数据库安全管理的思考

刘佳

1、 Oracle数据库防火墙使用经验

2、数据库安全管理的思考

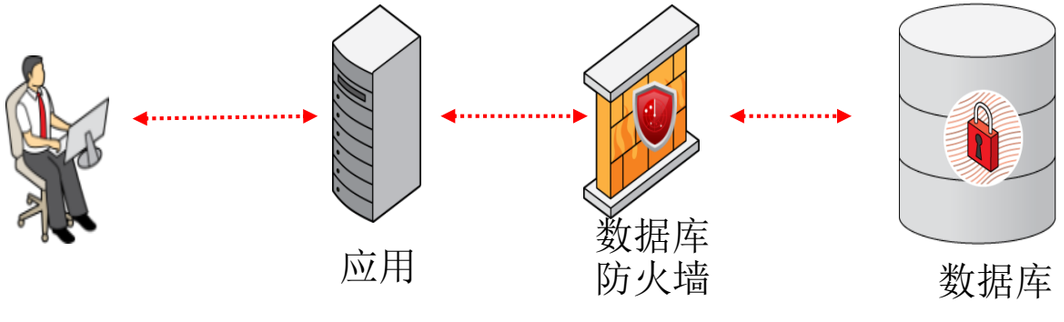
3、讨论

1、 Oracle数据库防火墙使用经验

1、 Oracle数据库防火墙使用经验

为何需要数据库防火墙?

- 数据库存在被恶意访问、攻击、甚至遭到数据偷窃的可能。
- 不了解数据使用者对数据库的访问细节， 谁（Who）用什么方法（What）在什么地方 （Where），什么时间（When），对数据库做什么事情(How)。
- 当数据库正在遭受恶意访问或攻击时，不能及时地追踪并堵截这些恶意操作。
- 数据库遭受恶意攻击、访问后，不能追踪到足够的证据。
- 来自内部的威胁，特权用户修改配置、改变或偷窃数据。

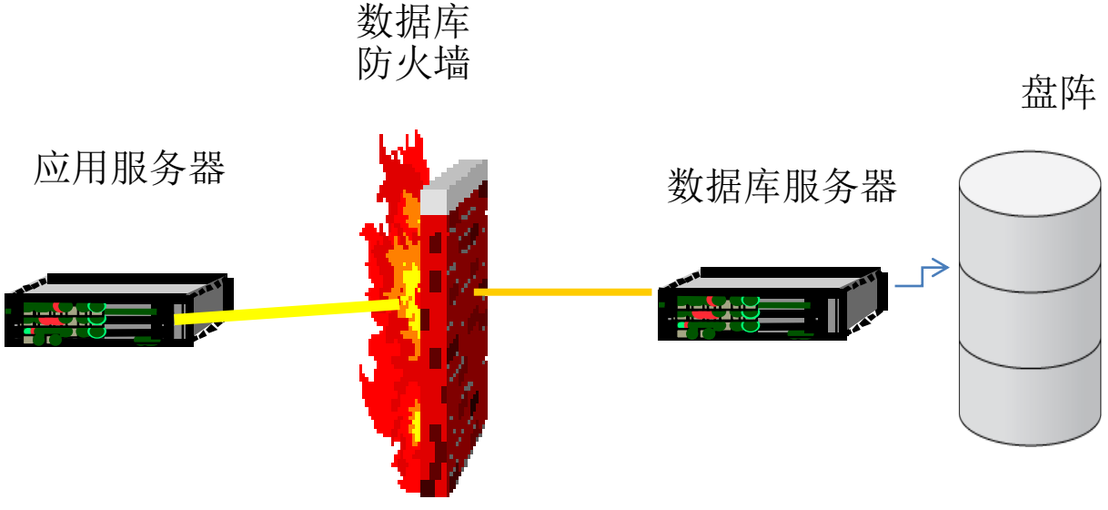


1、 Oracle数据库防火墙使用经验

- Oracle产品
  - Oracle database firewall
    - ✓ Oracle Database Firewall
    - ✓ Oracle Database Firewall Management Server
    - ✓ Oracle Database Firewall Analyzer
  - Oracle AVDF
- 其他产品
  - Improva
  - 国产软件（安恒等）

1、 Oracle数据库防火墙使用经验

数据库防火墙概念

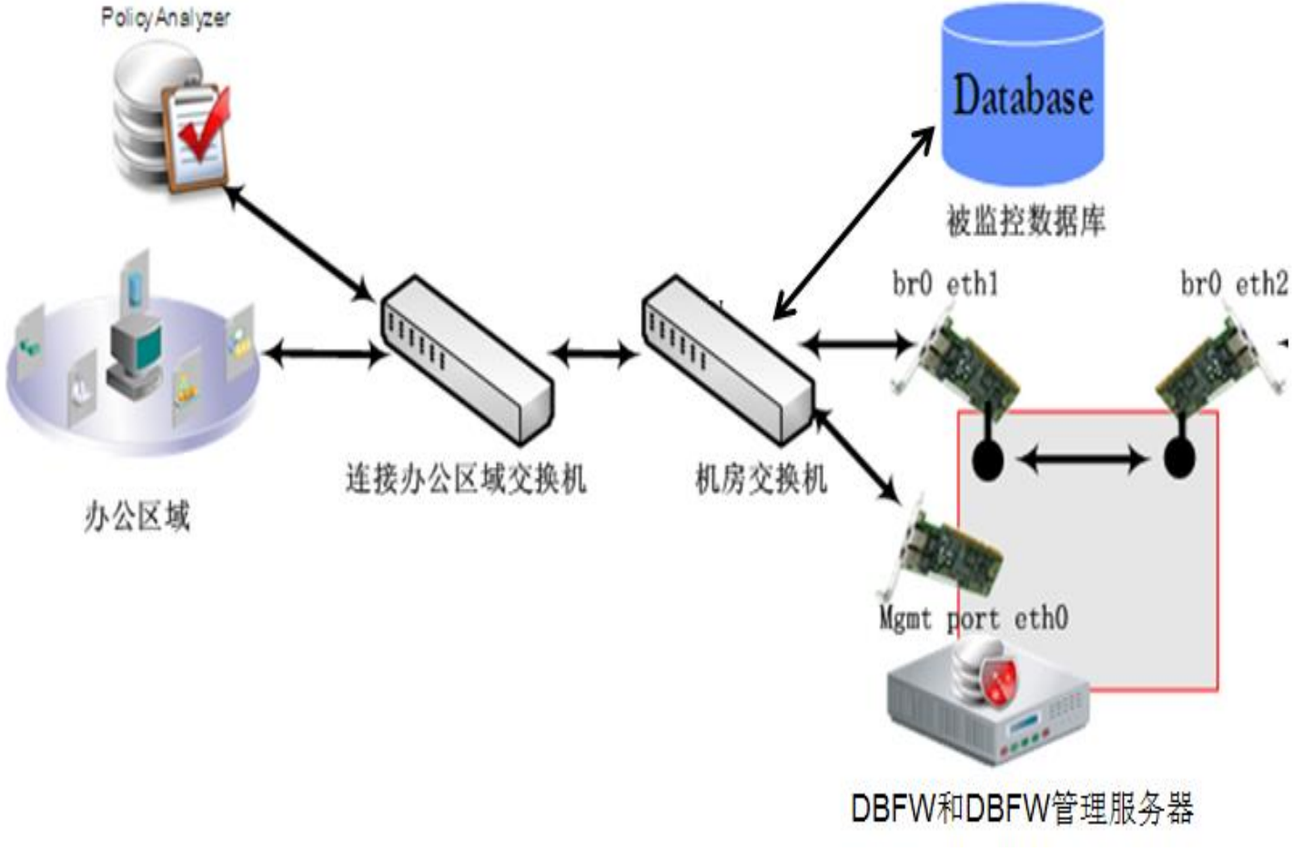


防火墙：网络层次之间设置的、用于加强访问控制的软硬件保护设施

数据库防火墙：应用和数据库之间设置的、用于加强数据库访问控制的重要保护设施

以往所说的防火墙，通常是指网络防火墙，用于TCP/IP层网络监测。
而数据库防火墙，是专门监测和审计对数据库的SQL访问

常见的部署模式


PolicyAnalyzer
Database
被监控数据库
br0 eth1
br0 eth2
办公区域
连接办公区域交换机
机房交换机
Mgmt port eth0
DBFW和DBFW管理服务器

1、 Oracle数据库防火墙使用经验

- 如何做到访问全覆盖（数据库访问的三种模式）
  - 网络协议访问（经过SQL*NET）。
  - 通过beq协议在本机上访问（bequeath协议，IPC机制，linux下的多进程通信机制）。
  - 数据库实例的共享内存访问。

DBAplus

DBFW监控模式

监控模式		功能特点
Appliance Mode	DAM	➢ 数据库处于监控、审计模式，无阻止SQL；可用于旁路模式。
	DPE	➢ 具有DAM的所有功能， 并可以阻断SQL的访问，必须用于in-line模式。
SPA		➢ 监控、审计存储过程，包含存储过程的创建、修改、删除及其中包含的SQL类型，需要在目标数据库上执行数据库脚本。
URA		➢ 监控、审计用户的权限及角色变化，需要在目标数据库上执行数据库脚本。
Local Monitor		➢ 监控、审计数据库服务器上用户的数据库访问行为， 只能监控，不阻断，需要在目标数据库上执行数据库脚本。
Remote Monitor		➢ 将包含数据库访问信息的网络流量传递给DBFW；最简单的部署方式是在数据库服务器上运行；也可以不与数据库服务器部署在一起， 在这种模式下， 需要通过SPAN方式将包含数据库访问信息的流量传递给Remote Monitor正在运行的机器上；它仅支持Linux/Unix， 不支持windows；也不阻断SQL的访问。

1、 Oracle数据库防火墙使用经验

- 优点
  - 软硬件独立。
  - 开放后台数据库，支持二次开发。
  - 部署较为简单快捷。
  - 界面比较友好。

2、数据库安全管理的思考

2、数据库安全管理的思考

- 纵向上划分好职责边界
  - 偏向于内部数据管控，不能替代外层防护措施。（OpenSSL，struts2的漏洞。）
  - 边界需明晰。
  - 内部制度健全（内部数据访问控制、内部审计制度）

2、数据库安全管理的思考

- 横向上消除薄弱环节
  - 不同的应用，数据访问限制应保持一致（如web应用和手机app应用应保持一致）。
  - 多数据中心的数据保护措施应保持一致。
  - 多个环境的数据保护措施应保持一致。

2、数据库安全管理的思考

- 数据安全制度的建立和完善
  - 对标相关制度和管理办法。
  - 加强执行力度。
  - 加强审计力度。

3、讨论

DBAplus

www.dbaplus.cn

THANK YOU !