DTCC2013

基于网络监听的数据库安全审计

袁志永

捷骅（大连）数码科技有限公司

公司简介

Jawasoft
捷骅（大连）数码科技有限公司
JAWA Dalian Digital Technology Co,.Ltd

www.jawasoft.net

捷骅 (大连)数码科技有限公司，是专门从事软件开发、数码产品开发的民营高科技研发型企业，主营业务包括系统研发、系统集成、技术咨询服务等。

公司历经数年的发展，形成了由资深的业务专家、项目管理团队和开发队伍所组成的人才结构。

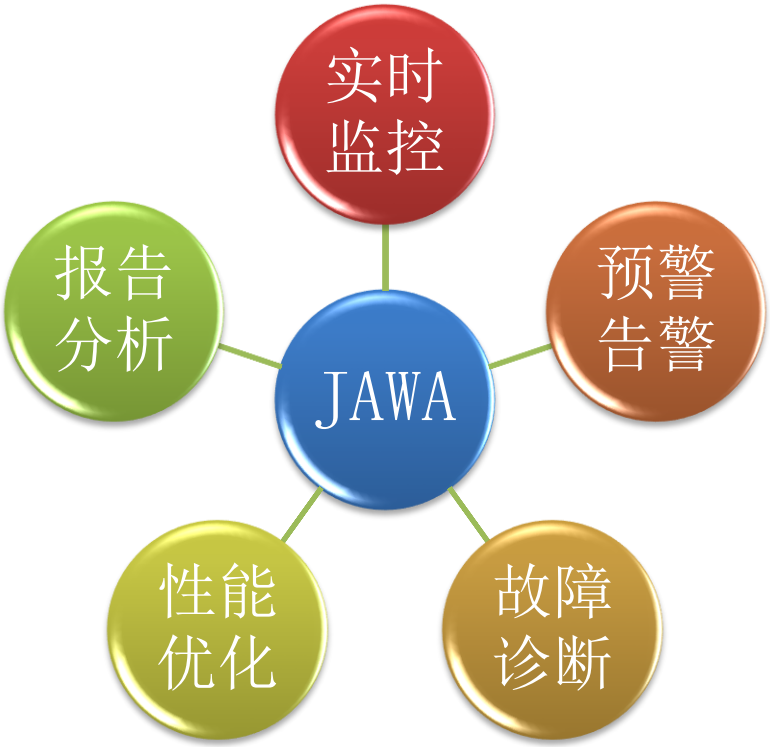
公司拥有强大的研发和运营实力，能快速响应客户需求，提供保障IT业务稳定、高效、安全运行的管理软件和解决方案。

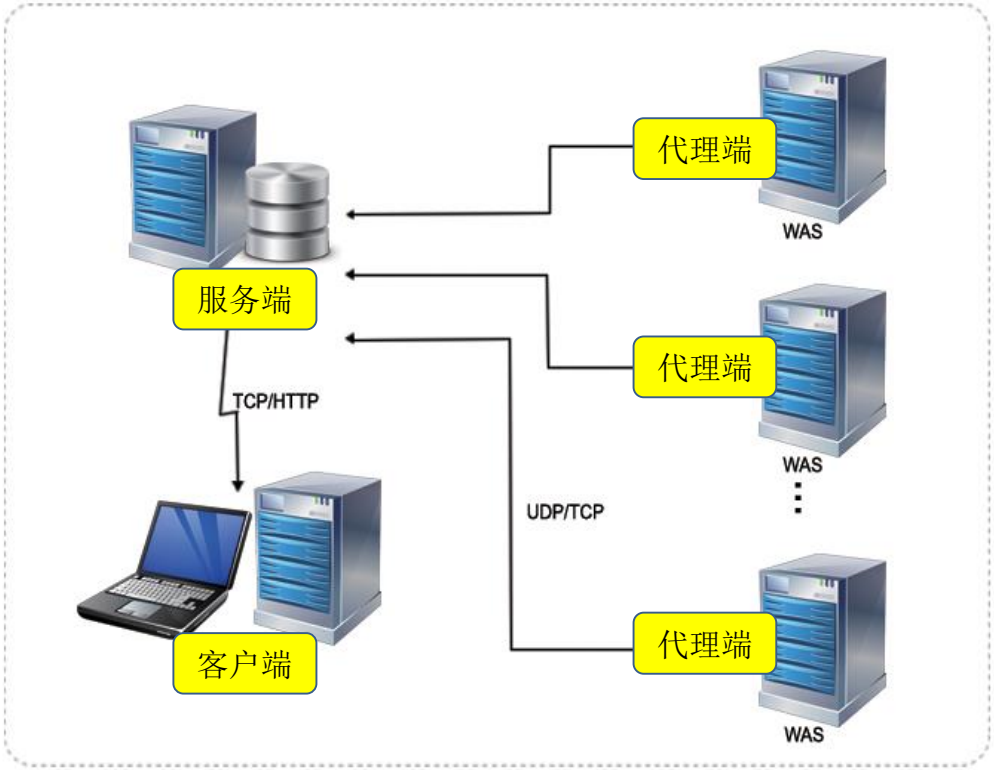
产品因需而变 服务恒久不变

捷骅应用程序性能监控系统

DTCC2013

捷骅应用程序性能监控系统致力于保障业务系统运行的稳定性和安全性，通过实时监控提供实际服务的应用程序的各项指标，准确把握业务系统的运行现状，为故障分析和性能调优提供依据，强化内部维护方面的问题处理及分析能力，规避系统运行风险，实现业务系统运维管理的“可视、可防、可管、可控”。

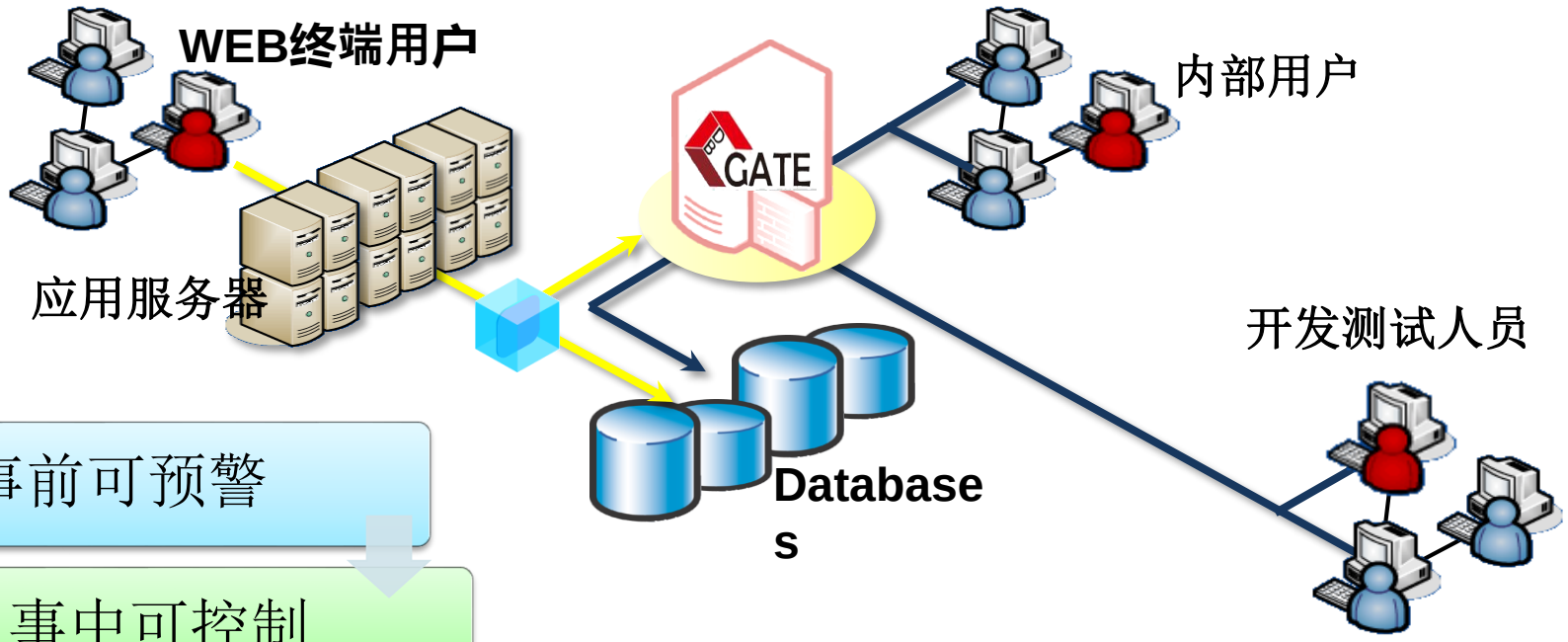




捷骅数据库审计与风险控制系统

DTCC2013

捷骅数据库安全审计与风险控制系统，通过有效监控数据库访问行为，准确掌握数据库系统的安全状态，及时发现违反数据库安全策略的事件，并实时告警、记录、防御、阻断，从而实现安全事件定位分析，事后追查取证，保障数据库安全。



事前可预警

事中可控制

事后可追查

建立完善的数据安全事件响应机制

数据库安全状况

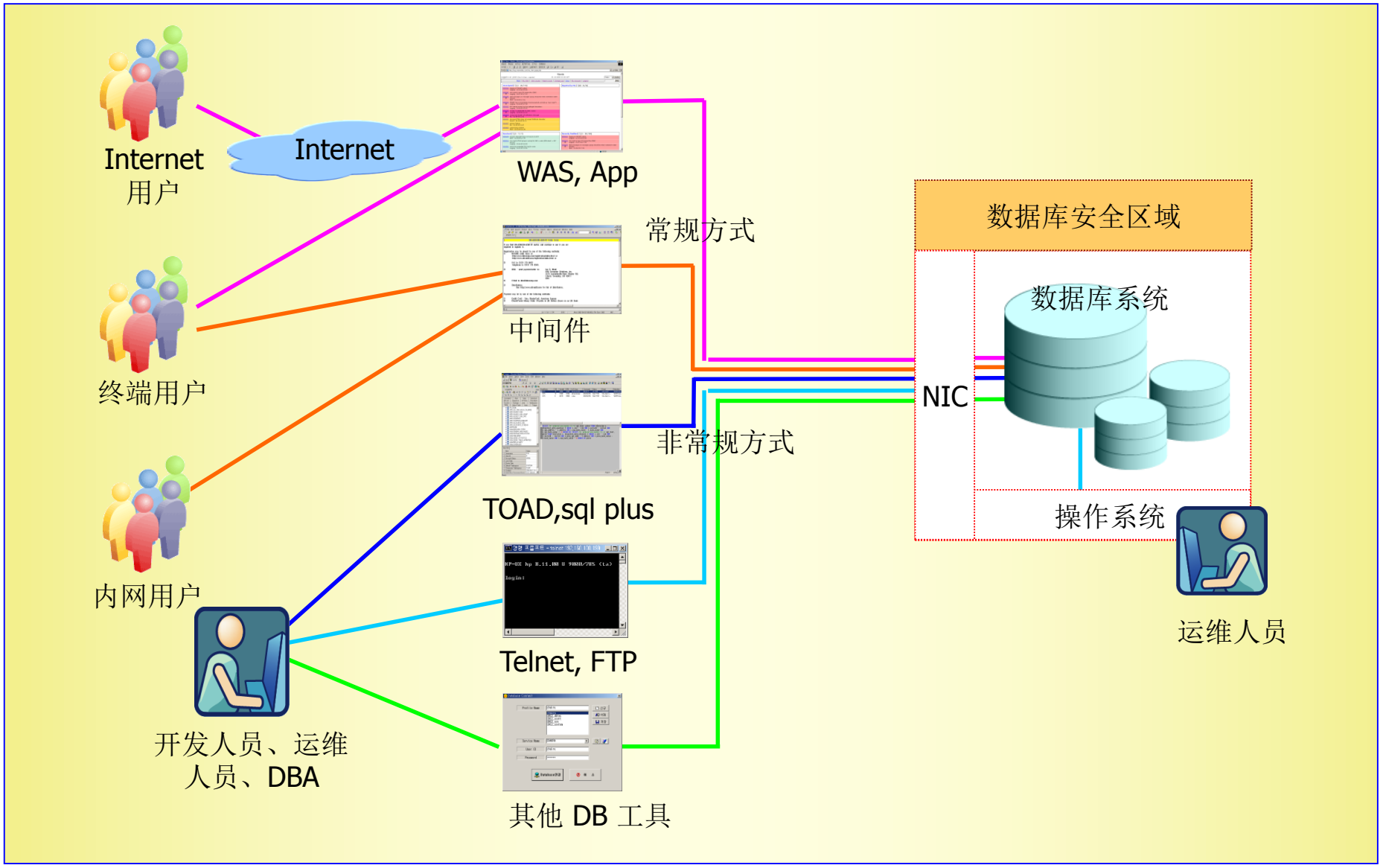
近年期，各种数据安全事件层出不穷，一旦发生数据泄露或者篡改，其影响和损失必将是十分巨大的，同时监管部门的处罚也会非常严厉，如何防止数据泄露和篡改已经成为了各大数据中心亟需应对的关键问题之一。

1. CISSPs (Certified Information Systems Security professionals)： 数据库安全在所有安全问题里居于**第一位**。
2. 所有发放信用卡的银行，必须遵守PCI-DSS (Payment Card Industry Data Security Standard) 。
3. 防火墙/IDS等对数据安全的保护有效率不到10%，**90%以上**的安全威胁需要数据库本身以及专业产品的防护。
4. 数据库安全威胁**80%**来自于内部用户的误操作和恶意操作。

----来自Forrester

ORACLE IBM SYBASE MySQL Microsoft TERADATA Raising Intelligence

数据库访问来源


Internet
用户
Internet
WAS, App
常规方式
终端用户
中间件
数据库安全区域
数据库系统
NIC
非常规方式
TOAD,sql plus
内网用户
操作系统
运维人员
Telnet, FTP
开发人员、运维
人员、DBA
其他 DB 工具

数据库安全风险


风险
内部人员
错误操作
内部人员
攻击
开发测试
数据管理
缺失
数据库配
置缺陷
未打补丁
的漏洞
专业数据
窃取组织
攻击风险
监管部门
的政策合
规性

数据库安全审计和风险控制的需求

1、数据库访问审计

2、服务器远程连接审计

3、违规操作告警和响应

4、日志查询、统计分析

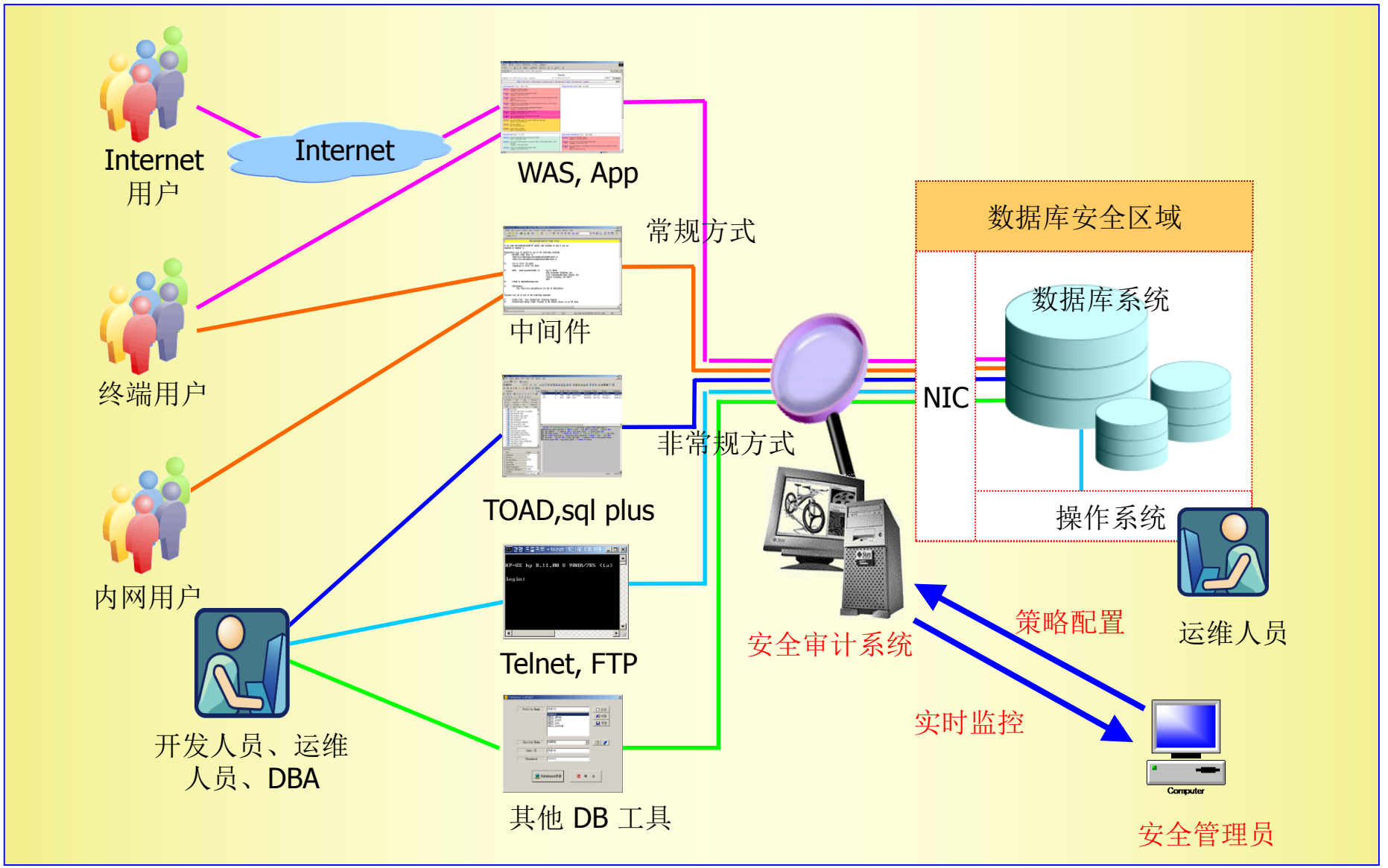
5、隐私数据掩码保护

6、高危操作审批执行

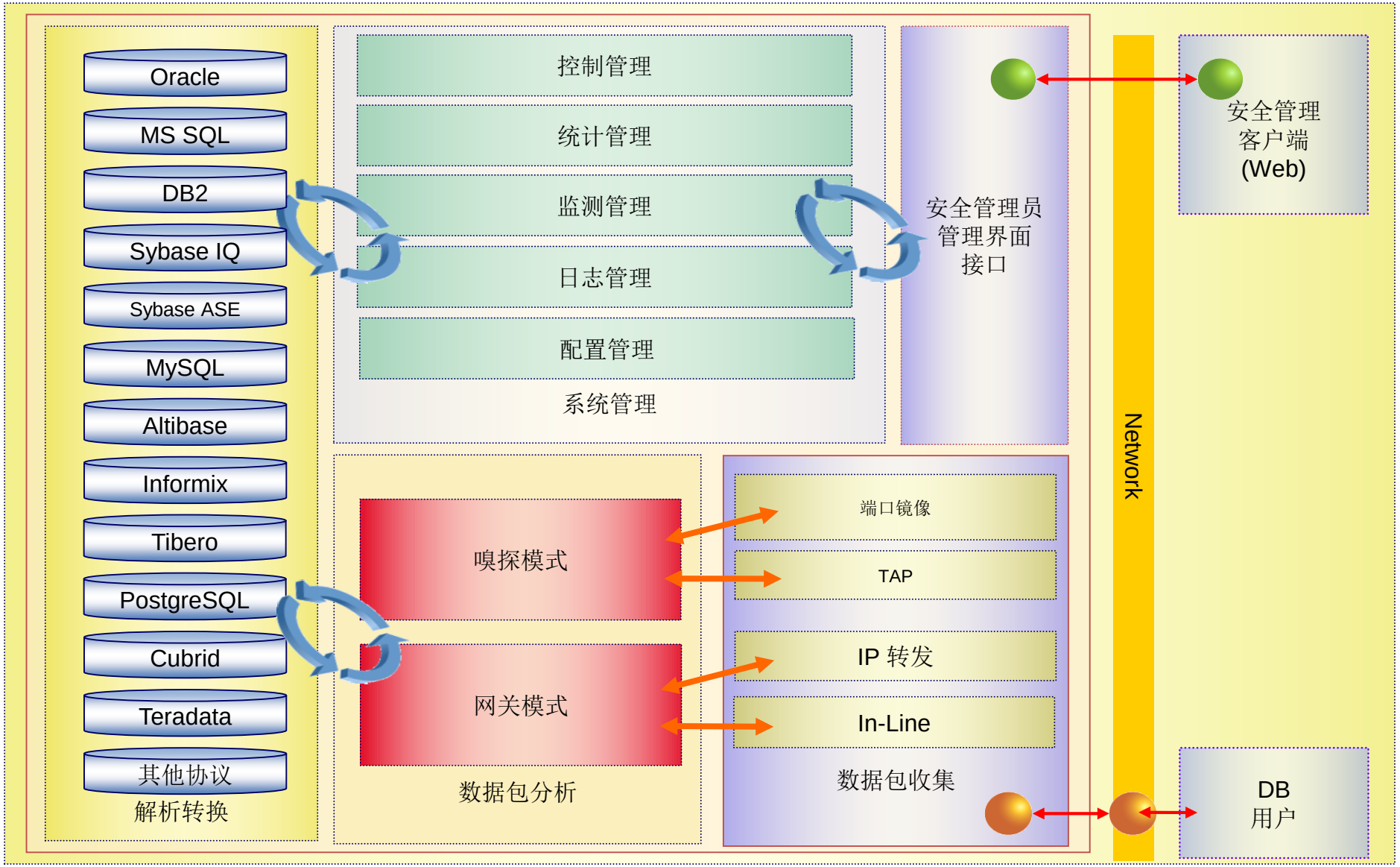
7、二层用户客户端连接认证

8、本地主机操作审计

另外一种方式的安全审计技术

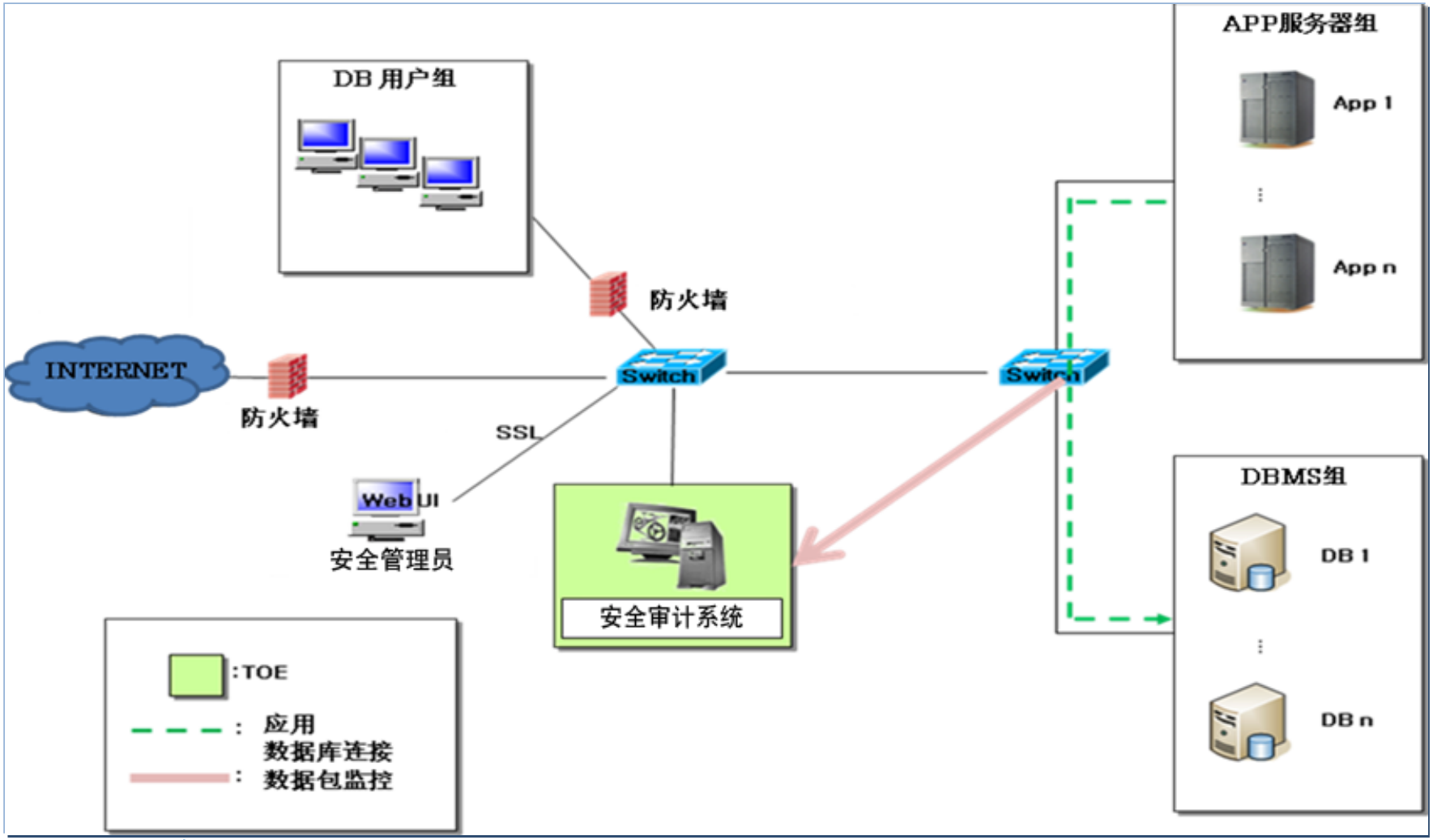


基本流程结构

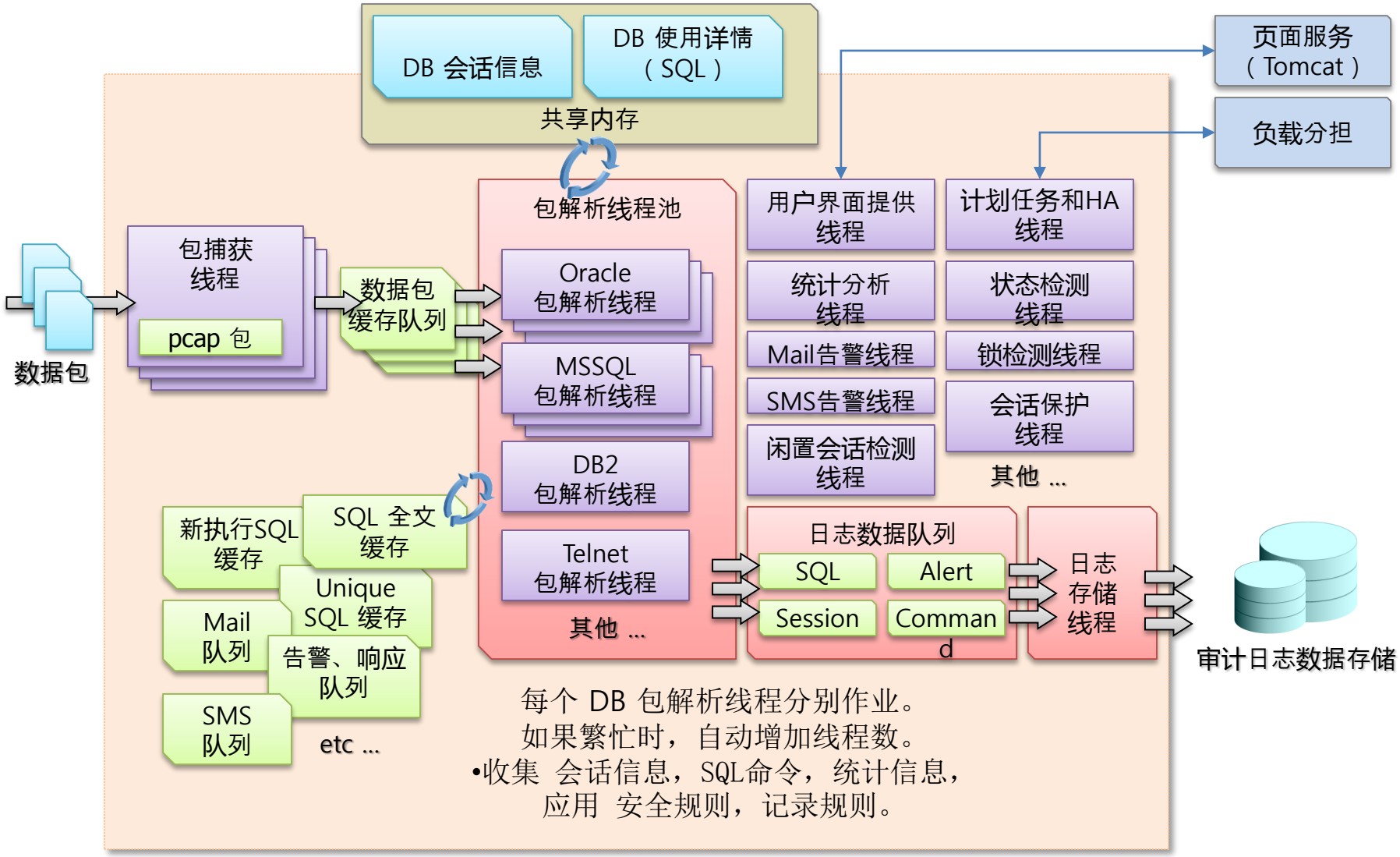

Oracle
MS SQL
DB2
Sybase IQ
Sybase ASE
MySQL
Altibase
Informix
Tibero
PostgreSQL
Cubrid
Teradata
其他协议
解析转换
控制管理
统计管理
监测管理
日志管理
配置管理
系统管理
安全管理员
管理界面
接口
安全管理
客户端
(Web)
Network
嗅探模式
网关模式
数据包分析
端口镜像
TAP
IP 转发
In-Line
数据包收集
DB
用户

部署示意–嗅探模式

嗅探（sniffer）模式，是一种旁路模式，一般利用交换机的端口镜像方式，或者使用TAP设备实现，将数据库的进出流量复制到审计设备的数据采集网卡中。

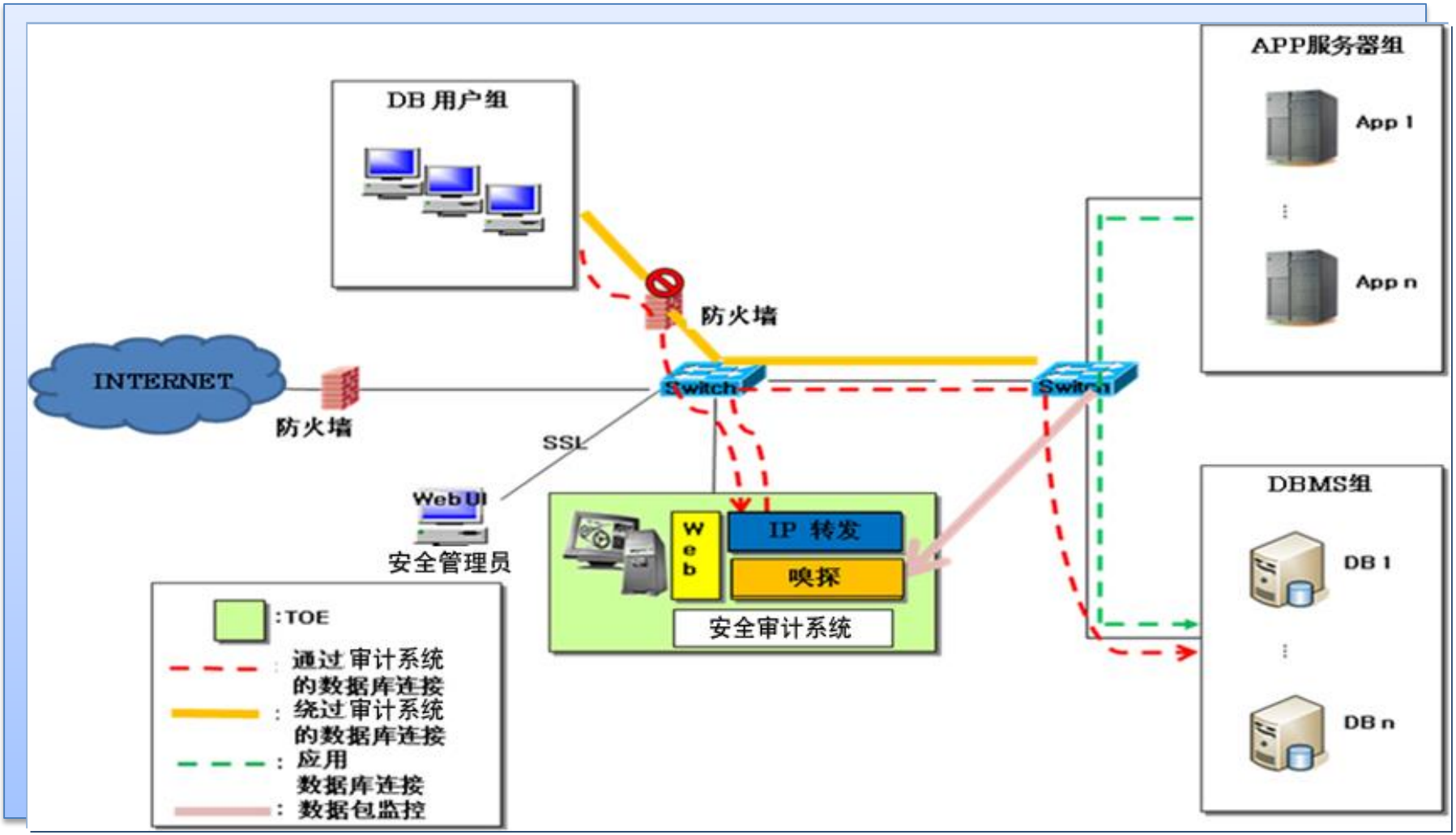


工作机制–嗅探模式

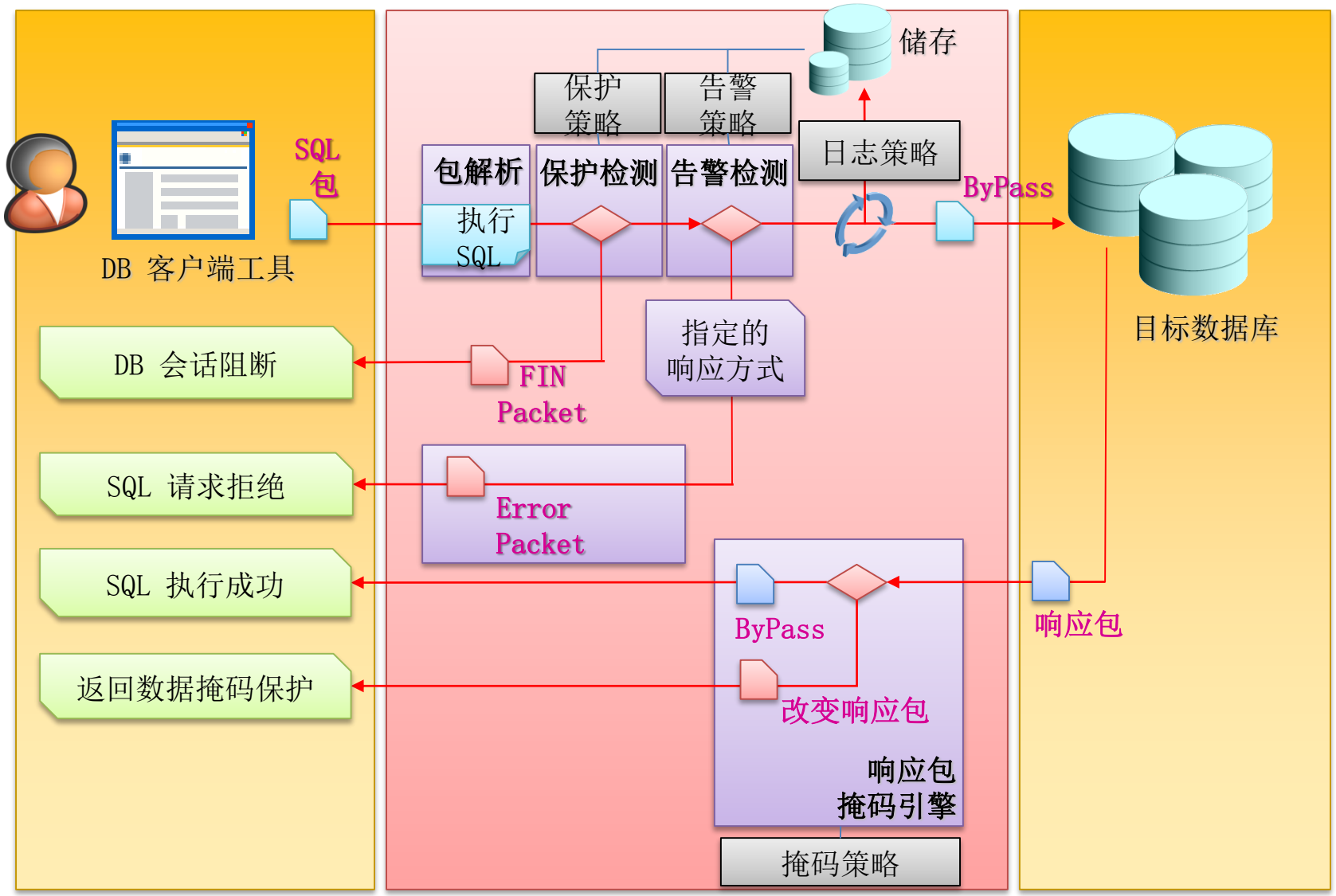

DB 会话信息
DB 使用详情（SQL）
共享内存
页面服务（Tomcat）
负载分担
包解析线程池
用户界面提供线程
计划任务和HA线程
统计分析线程
状态检测线程
Mail告警线程
锁检测线程
SMS告警线程
会话保护线程
闲置会话检测线程
其他 ...
包捕获线程
pcap 包
数据包
数据包缓存队列
Oracle 包解析线程
MSSQL 包解析线程
DB2 包解析线程
Telnet 包解析线程
其他 ...
新执行SQL缓存
SQL 全文缓存
Unique SQL 缓存
Mail 队列
告警、响应队列
SMS 队列
etc ...
日志数据队列
SQL
Alert
Session
Command
日志存储线程
审计日志数据存储
每个 DB 包解析线程分别作业。
如果繁忙时，自动增加线程数。
•收集 会话信息，SQL命令，统计信息，
应用 安全规则，记录规则。

部署示意-混合模式

混合模式是嗅探模式和网关模式的综合运用，网关模式，是在审计系统上配置一个代理网关，对数据库的访问强制通过网关，一般用于二层用户访问审计和控制。



工作机制-网关模式


储存
保护策略
告警策略
日志策略
SQL包
包解析
保护检测
告警检测
执行SQL
ByPass
DB 客户端工具
目标数据库
指定的响应方式
DB 会话阻断
FIN Packet
SQL 请求拒绝
Error Packet
SQL 执行成功
ByPass
响应包
返回数据掩码保护
改变响应包
响应包掩码引擎
掩码策略

数据库安全审计和风险控制的需求

1、数据库访问审计

2、服务器远程连接审计

3、违规操作告警和响应

4、日志查询、统计分析

5、隐私数据掩码保护

6、高危操作审批执行

7、二层用户客户端连接认证

8、本地主机操作审计

1、数据库访问审计

在嗅探模式下，通过协议解析线程，对捕获包数据进行解析还原，能够准确定位到连接的来源、用户信息、时间、操作的类型、操作语句、返回结果，以及响应时间和返回行数等信息。

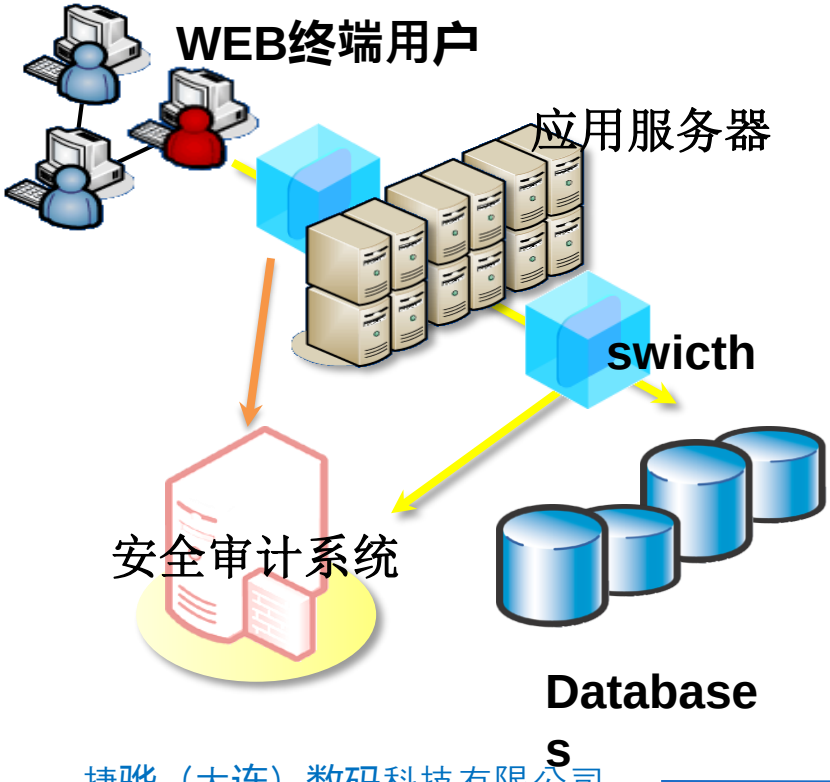
跟踪数据库访问信息

- ✓客户端信息：IP地址，主机名，应用程序名，MAC 地址等。
- ✓会话信息:时间（连接开始时间、结束时间、最后执行操作时间），DB 用户，OS 用户。
- ✓执行操作的类型（Query、DML、DDL、DCL等），SQL个数和执行成功情况。
- ✓每个连接的执行的详细SQL 命令、绑定变量和执行结果信息。
- ✓SQL 性能信息：响应时间，阈值，返回行数，网络包大小等信息。

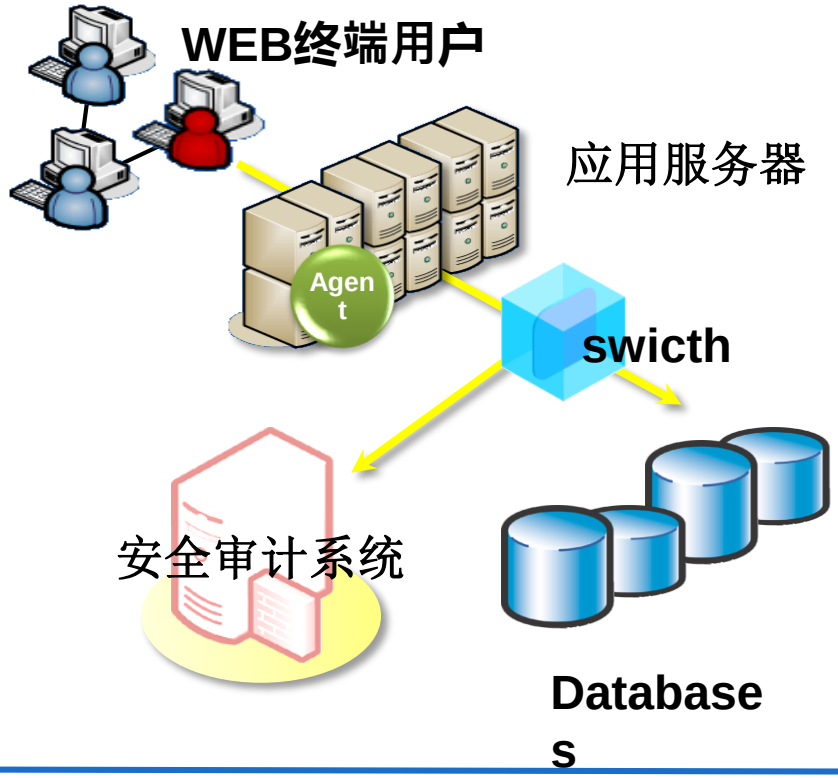
1、数据库访问审计　三用用户追踪技术

3 Tier WAS end user：对于通过应用系统进行的数据访问，在通常的审计记录中，像IP地址，会被显示为应用服务器的IP地址。如果我们需要获取终端用户信息，例如终端IP，用户名等，通常的实现方式有两种：

（1）镜像应用服务器流量
--分段匹配



（2）在应用服务器上部署代理
--JAVA Hooking技术



2、服务器远程连接审计

通过远程协议解析线程，对包数据进行解析，使之能够监测到数据库服务器的TELNET / SSH/Rlogin等远程连接会话，定位连接来源、还原操作过程以及查看执行结果等信息。

会话 ID	289
服务器名称	SVR20
协议	TELNET
客户端 IP	10.188.114.84
主机名	XP-201201091613
登陆 ID	oracle
登陆时间	2012-04-05 10:50:12

序号	时间	指令	
10	2012-04-05 10:53:48	exit	[结果]
9	2012-04-05 10:53:45	select * from dba_users;	[结果]
8	2012-04-05 10:53:37	select instance_name from v$instance;	[结果]
7	2012-04-05 10:53:13	select instance_name from dba_users;	[结果]
6	2012-04-05 10:52:57	sqlplus / as sysdba	[结果]
5	2012-04-05 10:52:52	export ORACLE_SID=gtp	[结果]
4	2012-04-05 10:52:24	ps -ef|grep ora_	[结果]
3	2012-04-05 10:51:29	ls	[结果]
2	2012-04-05 10:51:27	cd admin	[结果]

服务器远程会话信息

- ✓客户端信息：IP，主机名等
- ✓会话信息:时间，协议，登陆用户
- ✓指令序列
- ✓指令执行结果

3、违规操作告警和响应

一旦发生违反安全策略的事件时，系统可以自动发出告警、也可以根据设定自动响应。
策略配置是安全防护的灵魂，合理的制定安全策略，既要达到全面保护的目的，同时还要避免过度防护。

安全策略

- ✓**灵活：除了预置针对常见的威胁的安全策略外，可以根据客户端、时间、用户、表、列、操作类型、包含指定内容、返回行数等各种条件灵活的设定策略**
- ✓**智能：能够根据一定周期内收集的数据，区分出安全与不安全的操作，并且针对判定为不安全的操作自动告警。**
- ✓**响应动作：一般包含发送告警（声光电、短信、邮件）、丢弃数据包、会话阻断、执行本地或远程脚本等**

* 在嗅探模式下，响应动作可能会有轻微的延迟。

4、日志查询、统计分析

通过对日志的查询和深度挖掘，分析数据库存在的安全漏洞和风险等级，可以对数据库进行风险评估，在事前进行安全加固。一旦发生了安全事件，利用日志，可以快速进行追踪溯源和责任认定。
报告模块，可以生成种类丰富的报告，可以为审计、分析和决策提供依据。

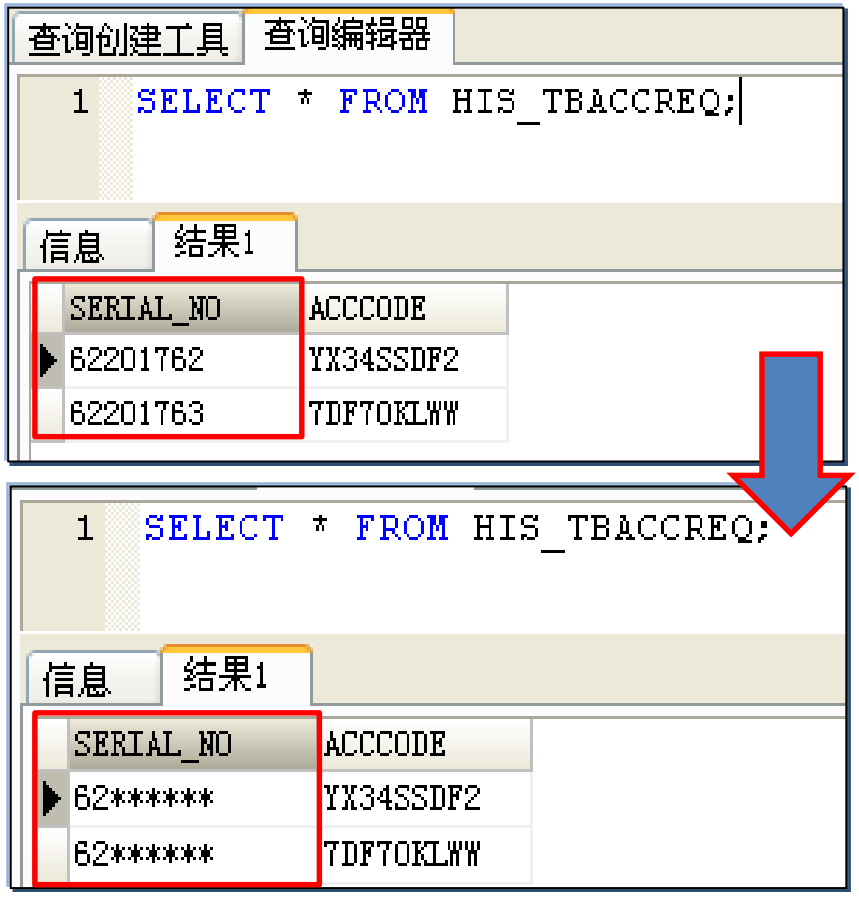
日志及报告

- ✓**告警日志**
- ✓**数据库连接日志**
- ✓**服务器远程连接日志**
- ✓**SQL日志**
- ✓**系统本身操作日志**
- ✓**具有趋势分析功能**
- ✓**能够提供行业合规性报表**
- ✓**方便的导出为常见的报表格式**

5、隐私数据掩码保护

在很多单位的开发、测试、甚至生产数据库中，可能包含隐私或者机密数据，针对二层用户（应用系统以外的访问），可以按照制定的策略对隐私数据进行全部或部分掩码变形处理，防止信息泄漏。

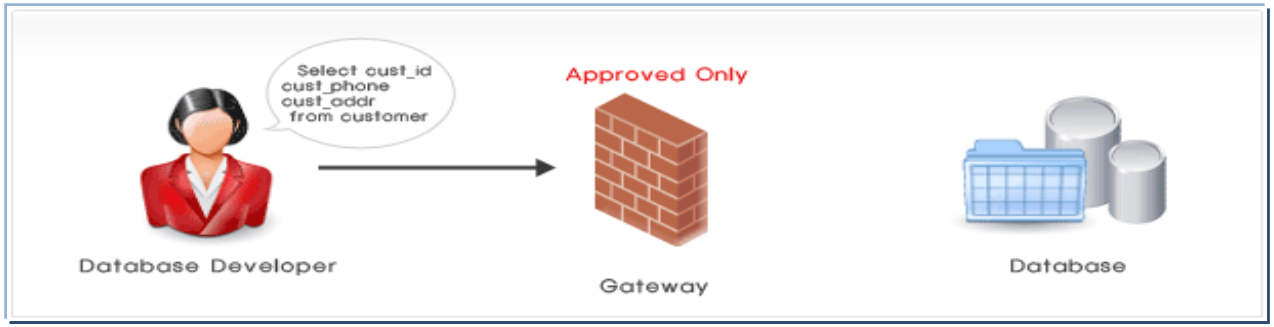
掩码变形	数据库加密
基于网络数据包掩码	数据库底层加密
DB无需安装插件	DB需要安装插件
不改变DB内数据	改变DB内数据
数据库负载0影响	数据库负载影响大
响应延迟十分小	响应延迟大

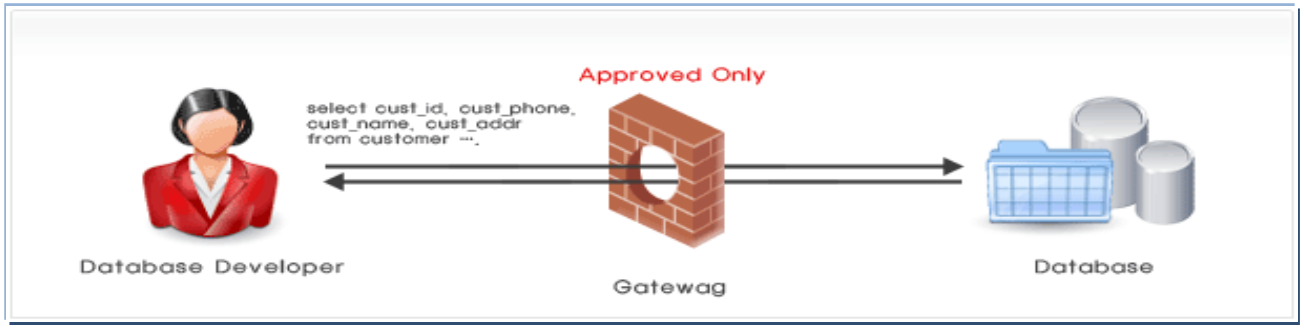


- ✓**根据策略决定哪些返回结果掩码**
- ✓**需在网关模式下实现**

6、高危操作审批执行

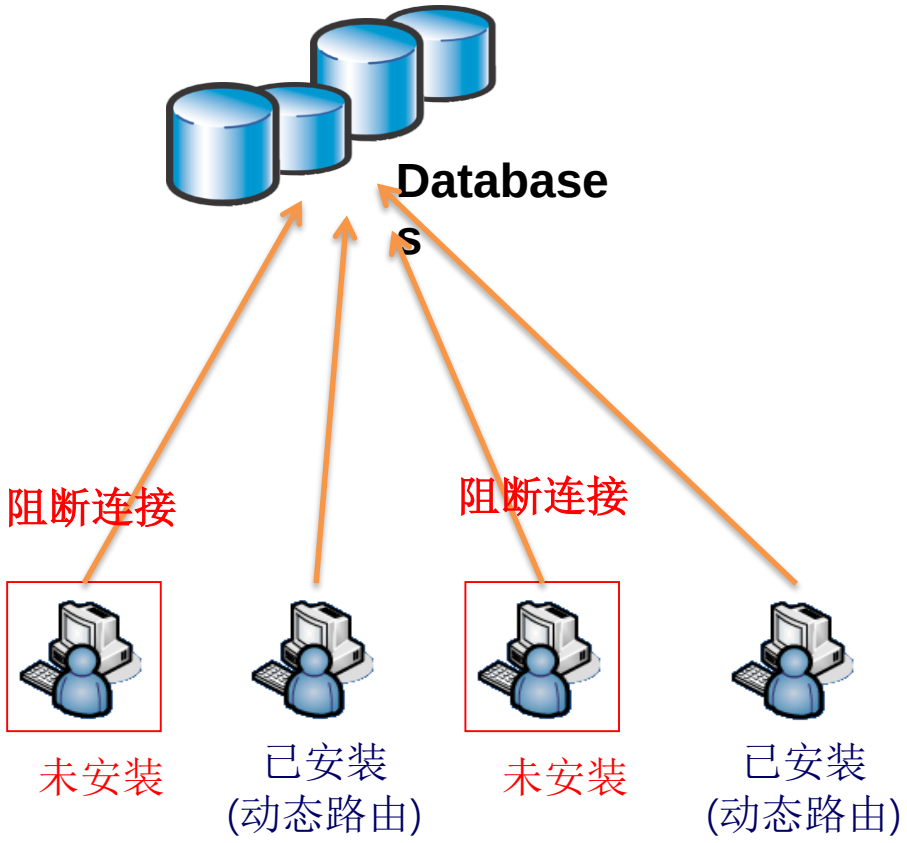
对于比较危险的数据操作，必须在安全控制责任人批准后才可以执行，为此，需要提供多样的审批过程，包括事前及事后审批，委托审批，部分自动审批等，即提供多样化的审批工作流程，同时进行数据修改前后的对比审查能力。





7、二层用户客户端连接认证

对于二层用户访问，通过客户端连接认证的方式，实现身份认证、动态路由，强制使用网关模式，并加强安全防护。即通过检测客户端PC是否安装了指定的安全认证插件和是否通过了身份认证，决定是否允许访问数据库。



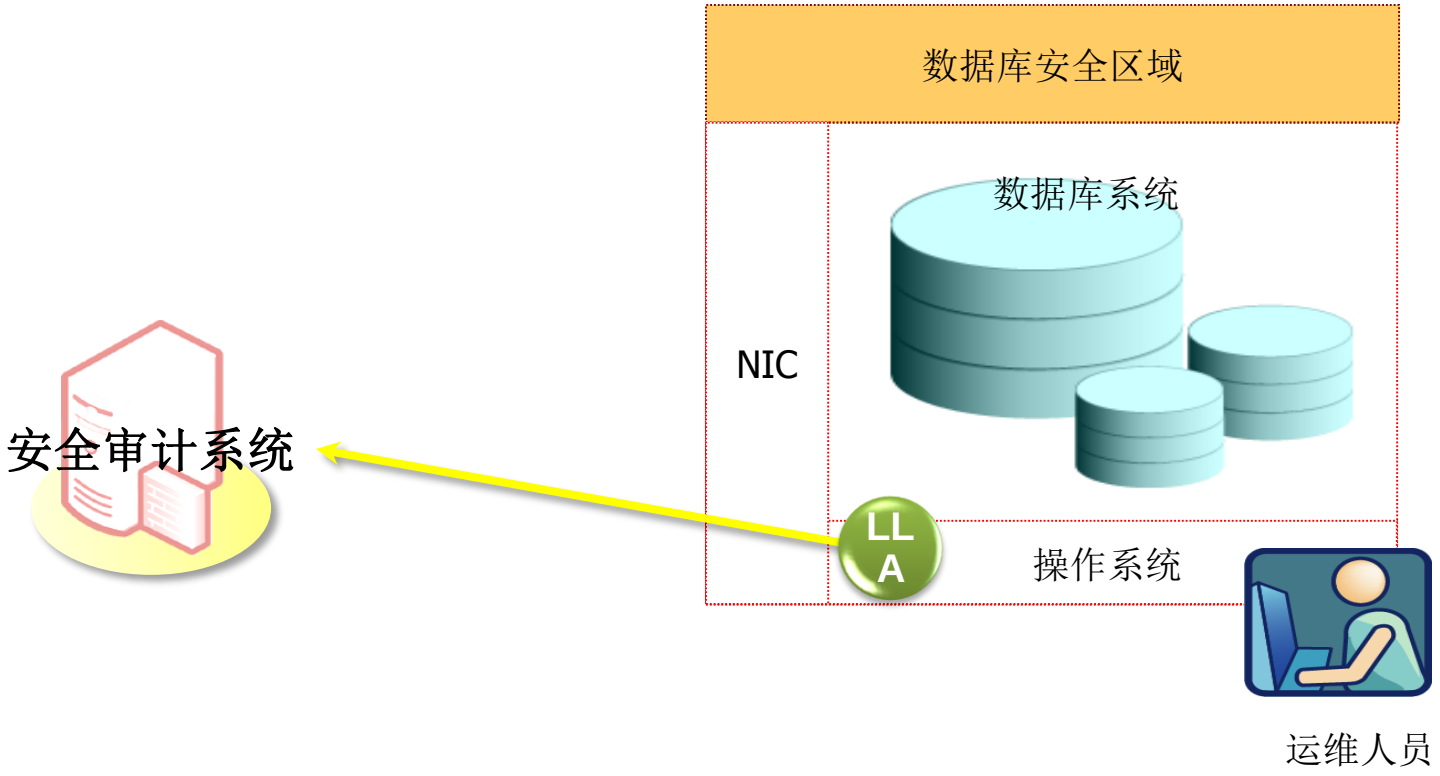
动态路由

✓网关模式：客户端需要修改tnsname

✓动态路由：客户端无需修改tnsname，插件可以自动路由到网关

8、本地主机操作审计

对于极特殊的情况下，用户直接在数据库服务器主机上进行的操作，通过在数据库服务器上安装一个本地操作日志记录的代理插件，记录用户的行为。



设备配置-内存

- 内存大小

CPU : 性能稳定要求

闲置率 > 60%

MEM :

操作系统

256 MB

审计系统

共享内存

300Mb 还原会话 NIC

SQL 监控

1 (Session) * 20 (SQL Count/Session) * 1500byte (AVG SQL Size) * 1.2 (Queue Count Compensation) → 0.035Mb

SQL 输出

64Kb/SQL, 1 Session → 64Kb * 20 SQL = 1.25Mb/Session

UNI SQL

»(SQL length + 500)*Number of UNI SQL → AVG. 250Mb

Web(Java) : 1Gb

MySQL : 500Mb

内存 = (256Mb + (300 * N)Mb + (S * 0.035)Mb + (S * 1.25)Mb + 250Mb +1024Mb + 500Mb) * 1.2

Ex) NIC 2ea, Session 500/sec (peak time) → N = 2, S = 500

Memory = (256 + 600 + 17.5 + 625 + 250 + 1024 + 500) * 1.2 = 3927Mb

我们建议设备主内存超过4GB

设备配置–存储

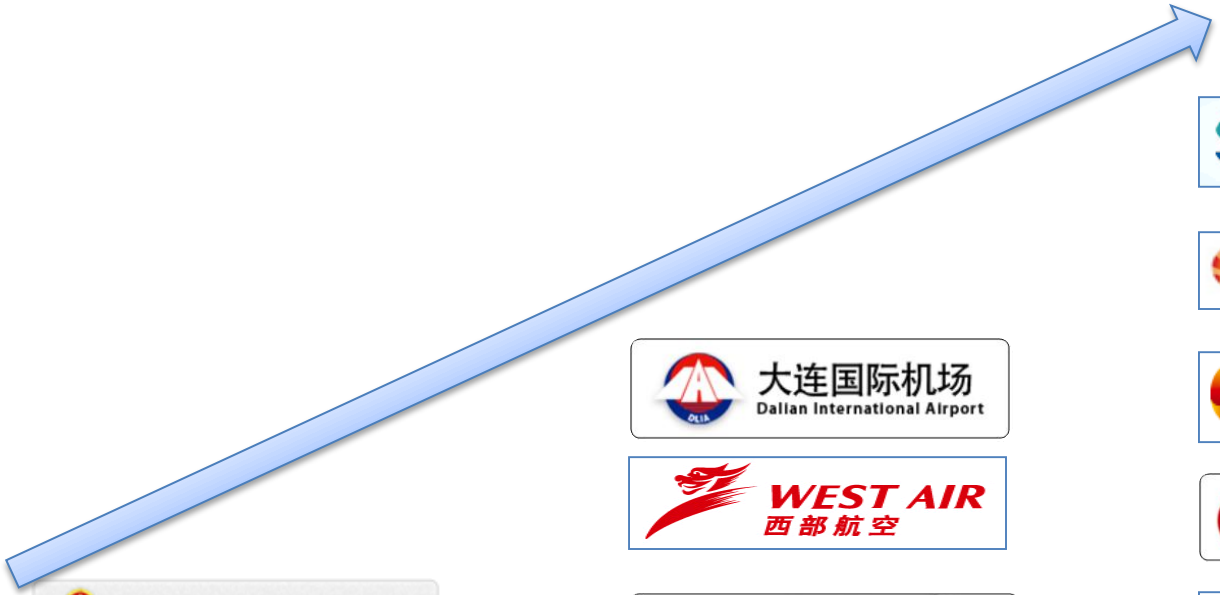
- 磁盘大小
  - OS 安装
    - 2Gb
  - Swap 内存区域
    - 2GB
  - 审计系统
    - 218Mb
  - JDK
    - 27Mb
  - MySQL（数据库）
    - 120Mb
  - SQL 日志
    - 1(Avg. Sql Count/Sec) * 1,500Byte(Avg. SQL Size) * 3600 * 24 * 1(Logging Days) = 124Mb/1天 (SQL查询结果的空间没有被列入)
  - DB 日志 (Session, UNI SQL, Etc)
    - SQL 日志 * 1/10

  Disk = 2048Mb + 2048Mb + 218Mb + 27Mb + 120Mb + ((S * 124 * D)*1.1Mb) * 1.3

  Ex) Sql Count = 1000/Sec, Logging Days = 90 Days → S = 1000, D = 90
    - Disk = 2048 + 2048 + 218 + 27 + 120 + ((1000 * 124 * 90) * 1.1) * 1.3 = 15.22TB

  Ex) Sql Count = 100/Sec, Logging Days = 90 Days → S = 100, D = 90
    - Disk = 2048 + 2048 + 218 + 27 + 120 + ((100 * 124 * 90) * 1.1) * 1.3 = 1.53TB
- NIC
  - 依赖于客户的网络环境

成功应用案例



大连市人民政府

本溪市人力资源和社会保障局 Human Resources and Social Security Bureau of Benxi

大连市人力资源和社会保障局

辽宁省地方税务局 LIAO NING LOCAL TAXATION

大连国际机场 Dalian International Airport

WEST AIR 西部航空

沈阳住房公积金管理中心 Shenyang Housing Fund Management Center

大连市公安局 INTERNET OF DALIAN PUBLIC SECURITY BUREAU

辽宁省人力资源和社会保障厅 Liaoning Provincial Department of Human Resources and Social Security

沈阳市人力资源和社会保障网 WWW.SYHRSS.GOV.CN

中国民生银行 CHINA MINSHENG BANKING CORP., LTD.

宁波银行 BANK OF NINGBO

鞍山银行 BANK OF ANSHAN

大连银行 BANK OF DALIAN

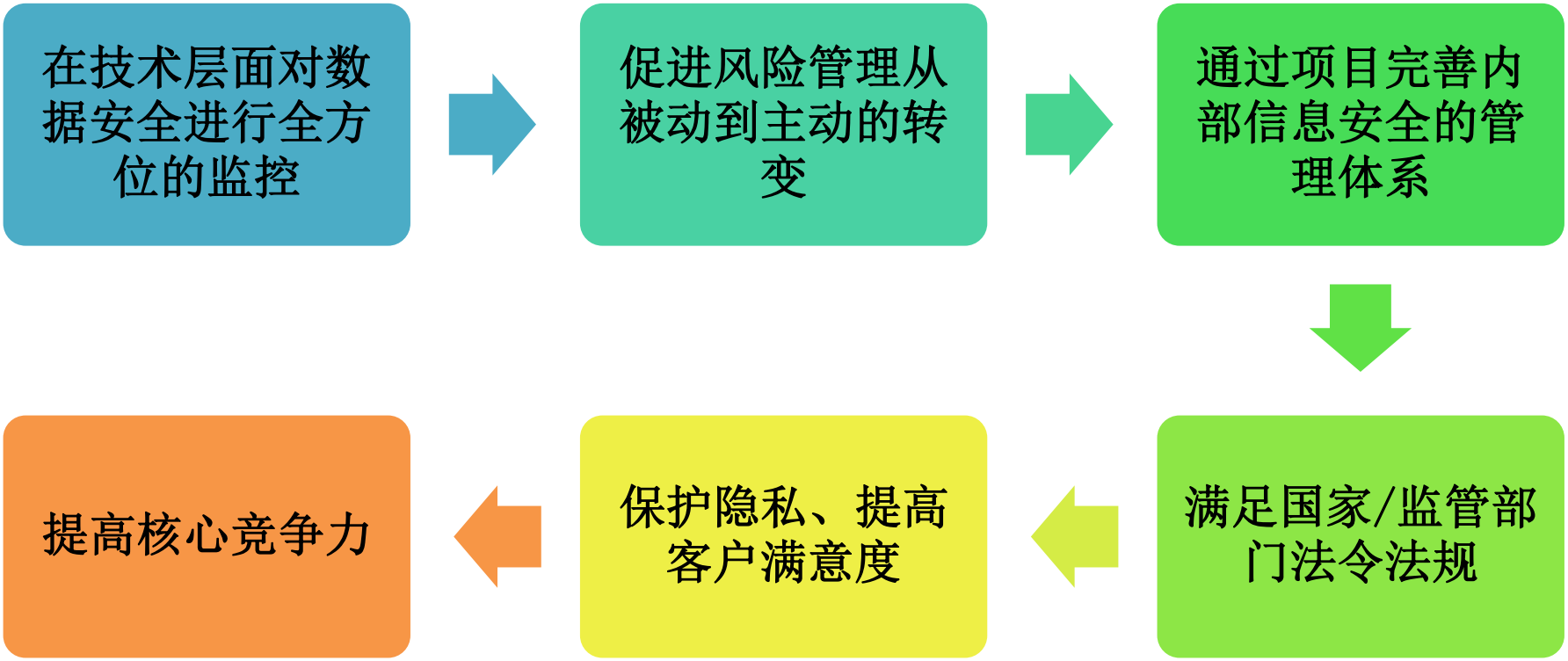
大连商品交易所 DALIAN COMMODITY EXCHANGE

ING 中荷人寿

NEC Empowered by Innovation

SAMSUNG SAMSUNG FIRE & MARINE INSURANCE

数据库审计与风险控制的意义



谢谢大家！