# Oracle Database FireWall

Khái niệm:

* Oracle Database FireWall là 1 hệ thống tường lửa có thể bảo vệ tính an toàn cho các database (Oracle, MySQL, Microsoft SQL Server, Sybase Adaptive Server Enterprise (ASE), Sybase SQL Anywhere SQL, and IBM DB2 SQL ) trên nền tảng (Linux, UNIX, and Microsoft Windows)
* Nó ngăn chặn các cuộc tấn công, ghi lại log của các hoạt động, cung cấp các tool tăng cường các tính năng bảo mật của DB hiện có như mã hóa dữ liệu và xác thực người dùng

Cách tiếp cận của Database FireWall đối với vấn đề Security

* FW làm việc dựa trên việc phân tích ý nghĩa câu truy vấn mà client gửi tới. Điều này cung cấp 1 khả năng bảo vệ tốt hơn rất nhiều
* Không giới hạn độ dài độ dài của các câu truy vấn cần phải phân tích . Hiển thị 2000 ký tự đầu tiên và áp dụng cho mọi loại truy vấn ( ví dụ như ANSI SQL...)
* FW có thể ngăn chặn nhưng cuộc tấn công trước đây chưa từng xảy ra cũng như các cuộc tấn công SQL injection
* FW ko làm ảnh hưởng tới hiệu năng làm việc của hệ thống

Các thành phần chính của FireWall:

* Oracle Database Firewall Analyzer
  + Tạo các chính sách bảo mật ( policy file) đến và đi thông qua firewall
  + Firewall có khả năng tích lũy những kết quả từ trước ( lưu giữ nhưng cấu hình chính sách và kêt quả thực thi đối với những dữ liệu từ trước ) để sinh ra những chứng sách thích hợp
  + Từ đó,chúng chia những câu lệnh SQL thành các nhóm, mỗi nhóm sẽ áp dụng các chính sách riêng
* Oracle Database Firewalls :
  + Firewall sẽ dựa trên các chính sách bảo mật và thông tin của các truy vấn SQL để quyết định các hành động tiếp theo (cho phép, chặn, cảnh báo..)
* Oracle Database Firewall Management Server : quản lý các firewall kết nối với nó ( lưu trữ log file, tạo các báo cáo ), quản lý các chính sách bảo mật từ, theo dõi các chế độ ...
  + Ghi lại log để:
    - Giám sát và tạo báo cáo
    - Giúp Analyzer tạo và cải tiến các chính sách bảo mật
    - Không phụ thuộc vào log của database ( ko ảnh hưởng tới DB)
  + Các loại log bao gồm
    - Traffic log: ( user, ip, Os, client program...)
    - Event log ( các sự kiện xảy ra đối với FW)
    - Admin log ( các thao tác của admin đối vs FW)

