Damit nichts anbrennt: Oracle Database Firewall

Heinz-Wilhelm Fabry
ORACLE Deutschland B.V. & Co. KG
München

Schlüsselwörter:

SynoptiQ Engine, Database Firewall, SQL Injection, flexible Verteidigung, *defence in depth*, Compliance, Forensik

Einleitung

Die Anstrengungen um die Sicherheit von EDV Systemen beginnt in den Köpfen der Menschen, setzt sich fort in der Implementierung geeigneter unternehmerischer Prozesse und endet bei Produkten, die die Menschen und Prozesse wirksam unterstützen. Die Database Firewall bietet eine solche Unterstützung, indem sie unerwünschte Aktionen daran hindert, zur Datenbank vorzudringen.

Überblick

Abbildung 1 gibt einen Überblick über die Funktionalität der Oracle Database Firewall.

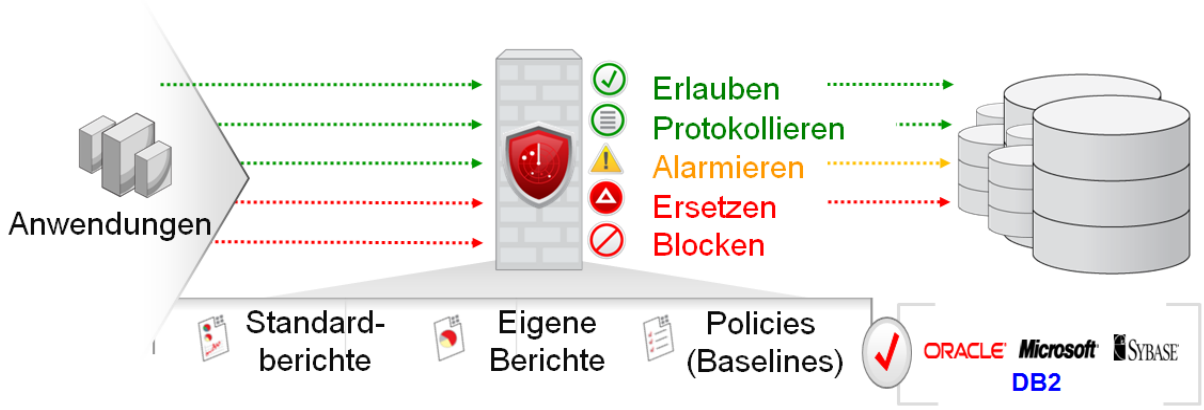

Abb. 1: Überblick

Die Firewall funktioniert wie ein Sniffer, der den Netzwerkverkehr zur Datenbank kontrolliert und je nach Konfiguration reagiert. So kann die Firewall SQL Befehle

- passieren lassen
- protokollieren
- einen Alarm auslösen lassen
- durch einen anderen Befehl ersetzen oder
- abblocken.

Die Oracle Database Firewall eignet sich ideal zum Einsatz in heterogenen Datenbankumgebungen. Das wird an der Liste der Datenbanken deutlich, die die Firewall schützen kann

- Oracle von Version 8i bis Version 11g
- Microsoft SQL Server 2000, 2005 und 2008
- Sybase ASE 12.5.3 bis 15 und SQL Anywhere 10.0.1 und
- DB2 Version 9 auf den Betriebssystemen Linux, UNIX und Windows

Weitere Datenbanken werden folgen, zum Beispiel MySQL.

Aus der Sicht von Auditoren stellt neben der Schutzfunktion der Firewall die Berichtsbibliothek mit über 130 Berichten sicherlich den größten Wert des Produkts dar. Zusätzlich können mit beliebigen Berichtsgeneratoren, die auf Oracle Datenbanken zugreifen können, auch eigene Berichte erstellt werden - z.B. mit Crystal Reports, das zwar nicht im Lieferumfang enthalten ist, aber eng mit der Database Firewall integriert ist.

Alle gespeicherten Informationen können um sensitive Daten bereinigt werden. So sind sie auch in den Berichten nicht sichtbar. Selbst das berechtigte Lesen der Berichte kann also sensitive Daten nicht kompromittieren.

Da die Oracle Database Firewall mit der Web Application Firewall der Firma f5 Networks, Inc. sowie mit dem ArcSight Security Event Management System integriert werden kann, erleichtert sie auch forensische Analysen.

Genauigkeit macht den Unterschied

Eine Database Firewall ist um so effektiver, je genauer sie berechtigte von unberechtigten Aktivitäten unterscheidet. Dazu gehören die Einbindung sowohl von Benutzerdaten als auch von Daten aus der Umgebung des Benutzers - also zum Beispiel den Zeitpunkt einer Aktion oder die IP Adresse des Systems, von dem aus versucht wird, auf die Datenbank zuzugreifen.

Vergleichbare Produkte am Markt analysieren die Zeichenketten von SQL Befehlen, um berechtigte von unberechtigten Zugriffen zu unterscheiden. Die Oracle Database Firewall verfolgt einen völlig anderen Ansatz.

Die wissenschaftlichen Grundlagen für die Oracle Database Firewall wurden von Forschern im Bereich der Linguistik an der Universität Oxford in Großbritannien gelegt. Die Erkenntnisse sind unter der Bezeichnung SynoptiQ Engine patentiert. Ausgangsbasis der Forscher war die Mitte der 1950er Jahre von Noam Chomskys vorgenommene Hierarchisierung von Sprachen. Danach kategorisierten die Forscher SQL als eine Sprache, die über Zeichenkettenvergleiche nicht ausreichend exakt interpretierbar ist. Das soll an einem Beispiel erläutert werden.

Ein SQL Befehl, der eine unsinnige WHERE Bedingung enthält, ist grundsätzlich als Gefahr einzustufen. So wird bei SQL Injection Angriffen unter anderem davon Gebrauch gemacht, den WHERE Bedingungen gegebener SQL Befehle eine eigene Bedingung der Form

```
OR 1=1
```

anzuhängen. Da die Auswertung dieser Bedingung immer den Wert TRUE liefert, führt ein so modifizierter Befehl nicht mehr nur zur Anzeige, Veränderung oder Löschung der über die WHERE Bedingung ausgewählten Datensätze, sondern zeigt, ändert oder löscht alle Datensätze.

Selbst ausgefeilte, auf Zeichenkettenvergleichen beruhende Implementierungen von Firewalls müssen daran scheitern, die Gefahr der beiden im folgenden Listing aufgeführten Bedingungen zu erkennen.

```
LEFT('catastrophe', 3) = 'cat'
'hund' <> 'katze'
```

Die unzureichende Eignung von Zeichenkettenvergleichen hat für den EDV Alltag Konsequenzen: Zum einen werden solche Vergleiche dazu führen, dass SQL Befehle zu Unrecht als gefählich klassifiziert werden. Zum anderen wird ein solches System immer wieder auch Befehle als harmlos klassifizieren, die in Wirklichkeit SQL Injection Angriffe sind.

Systemkomponenten

Ein Oracle Database Firewall System besteht immer aus drei Komponenten: Einer Firewall oder mehreren Firewalls, einem oder zwei Management Servern und einem Werkzeug namens Analyzer. Abbildung 2 zeigt schematisch diese Komponenten.

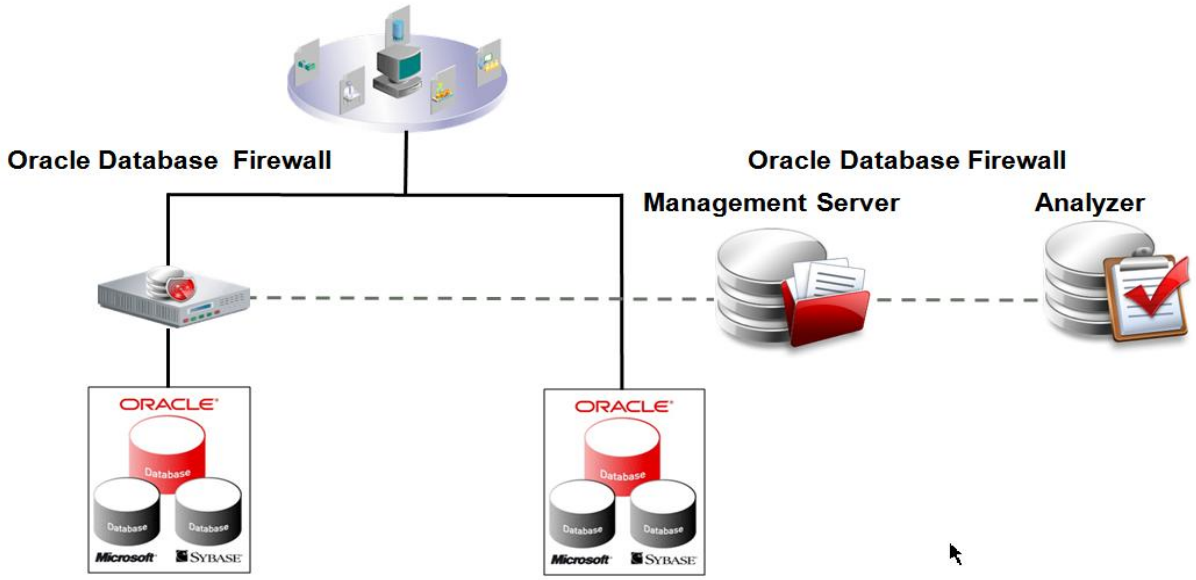

Abb. 2: Komponenten eines Systems mit der Oracle Database Firewall

Die Funktion der Firewall übernimmt die gleichnamige Produktkomponente. Sie muss auf einem eigenen Rechner laufen: Der gesamte Datenverkehr zu einer Datenbank oder zu mehreren Datenbanken mit identischen Sicherheitsvorgaben wird durch diesen Rechner geleitet und dort analysiert. Dabei kann man davon ausgehen, dass pro Core einer CPU dieses Rechners etwa 5000 SQL Befehle pro Sekunde bearbeitet werden können. Wird die Last für eine Firewall zu hoch oder um eine höhere Verfügbarkeit zu erreichen, können auch mehrere Firewalls parallel eingesetzt werden.

Die Komponente Management Server hat zwei Aufgaben. Zum einen ist sie für die Administration einer Firewall oder mehrer Firewalls zuständig. Hier sind auch die Regeln hinterlegt, die die Firewalls steuern. Andererseits dient der Management Server als Repository für alle Informationen, die die Firewalls über die von ihnen kontrollierten SQL Befehle sammeln. Der Umfang der Informationssammlung ist konfigurierbar und Basis für die oben bereits erwähnten Berichte. Die Informationen sind zum Schutz vor Manipulationen signiert.

Management Server werden über eine Browserschnittstelle verwaltet und konfiguriert, die Administration Console. Aus diesr Konsole werden auch die Berichte angestoßen. Abbildung 3 zeigt einen Ausschnitt des Eingangsbildschirm der Administration Console unmittelbar nach der Installation des Management Servers.

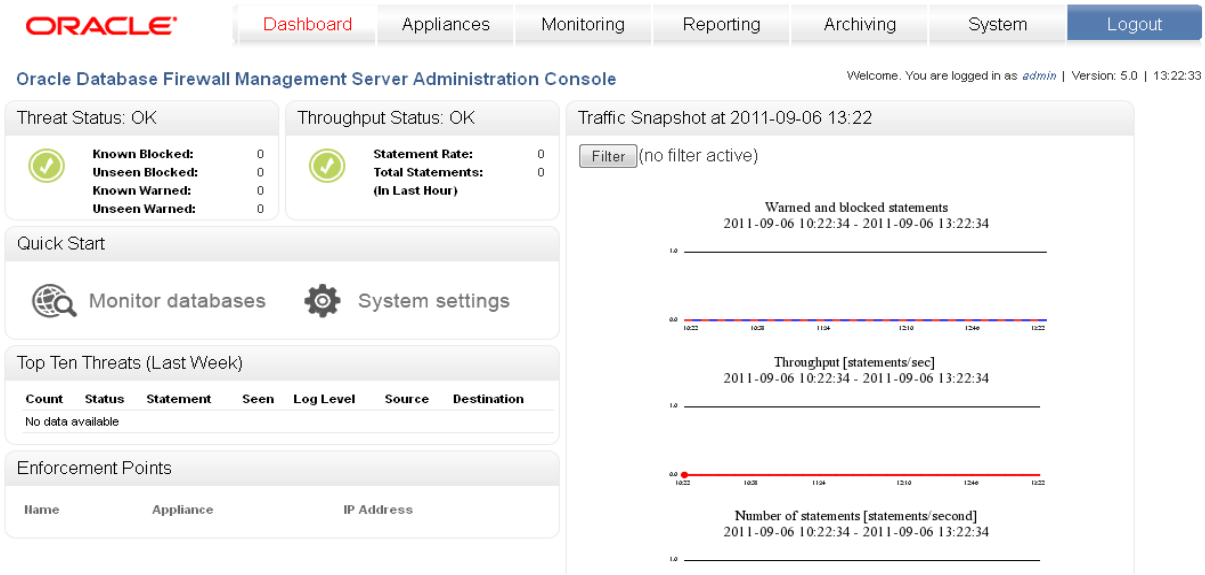

Abb. 3: Administration Console

Die Verfügbarkeit des Management Servers kann durch Hinzufügen eines zweiten Management Servers erhöht werden. Das zweite System ist dabei stets auf dem gleichen Stand wie das erste, verhält sich aber ansonsten passiv. Nur wenn der erste Management Server ausfällt, übernimmt der zweite die Rolle des aktiven Servers.

Die dritte Komponente des Systems ist der Analyzer. Es handelt sich um eine grafische Oberfläche, über die die Regeln konfiguriert werden, nach denen die Firewalls SQL Befehle analysieren. Dazu greift der Analyzer auf die Informationen zurück, die von den Firewalls im Management Server abgelegt werden.

Einrichten des Systems

Sowohl Firewall als auch Management Server sind als Appliances konzipiert. Allerdings muß der Kunde die Hardware für diese Appliances zur Verfügung stellen: Für beide Komponente wird ein X86 Rechner mit mindestens 1G Arbeitsspeicher und 80G Festplattenspeicher benötigt. Oracle hätte zwar auch die entsprechende Hardware als Teil des Produkts liefern können, aber die Trennung von Hardware und Software nimmt Rücksicht darauf, dass viele Kunden in ihren Rechenzentren ausschließlich Systeme festgelegter Anbieter verwenden.

Auf den von den Kunden gestellten Rechnern wird in einem einzigen Installationsgang zunächst als Betriebssystem ein angepasstes Oracle Enterprise Linux installiert und dann die Software für die Firewall beziehungsweise für den Management Server. Das Ergebnis ist jeweils ein Appliance, in das der Kunde nicht eingreifen darf. Alle Änderungen an den beiden Appliances dürfen ausschließlich über von Oracle gelieferte Patches vorgenommen werden.

Schließlich wird der Analyzer auf einem Windows XP oder Vista System installiert. Damit ist die Installation komplett.

Konfiguration des Systems für Netzwerkzugriffe

Jede Firewall kann individuell konfiguriert werden. Am einfachsten geschieht das, indem man sich eine sogenannte Positivliste oder Whitelist erstellen läßt, also eine Liste aller Aktionen, die keine Gefahr darstellen. Abbildung 4 zeigt den Eingangsbildschirm zum Anlegen einer solchen Liste.

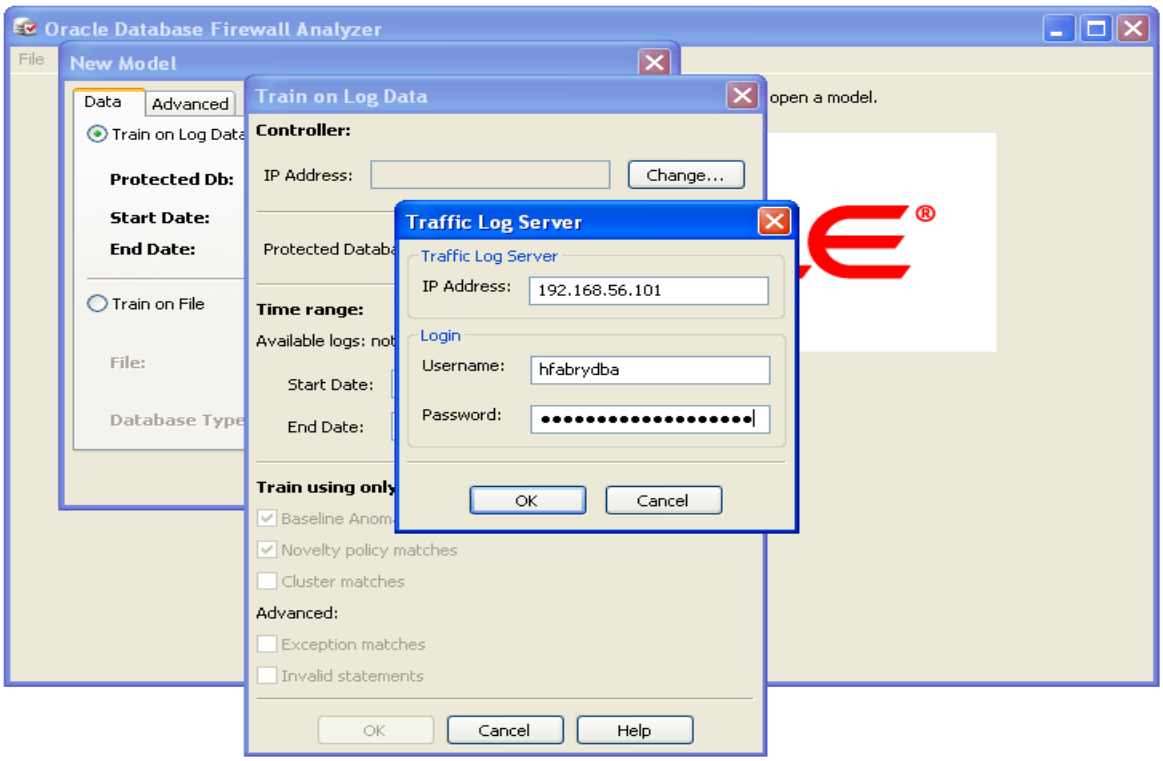

Abb. 4: Arbeiten mit dem Analyzer

Dazu wird entweder der gesamte Netzwerkverkehr zu einer Datenbank, oder es werden alle Aktivitäten einer bestimmten Anwendung aufgezeichnet. Sofern die Aktionen des Aufzeichnungszeitraums 'legal' waren, kann man die Firewall zum Beispiel anweisen diese und alle vergleichbaren Aktionen zuzulassen sowie alle anderen Aktionen abzublocken und zu protokollieren. Diese Konfigurationsvariante ist bequem und sehr flexibel. Aber auch die Verwendung von Negativlisten (Blacklists) ist möglich. So kann zum Beispiel der Zugriff auf festzulegende Objekte verhindert werden.

Konfiguration des Systems für lokale Zugriffe

Nicht alle Zugriffe auf zu schützende Datenbanken erfolgen über das Netzwerk. Häufig arbeiten zum Beispiel Administratoren lokal auf den Servern und greifen direkt mit eigenen Werkzeugen auf die Datenbanken zu. Ein Abblocken oder das Ersetzen von Statements ist dann nicht möglich.

Für den Schutz einer Oracle Datenbank wird man kompensatorisch auf das Oracle Auditing zurückgreifen. Für Datenbanken anderer Hersteller kann man auf das sogenannte lokale Monitoren

zurückgreifen. Dazu werden von der Firewall in diesen Datenbanken Hilfstabellen angelegt und die lokalen Aktionen dort mitprotokolliert.

Verfügbarkeit und Grenzen

Die Oracle Database Firewall ist kein neues Produkt. Sie wurde ursprünglich von der britischen Firma Secerno entwickelt und bis zur Version 4.2 unter dem Namen DataWall vertrieben. Oracle hat die Firma Secerno im Mai 2010 gekauft und nach einigen Änderungen und Erweiterungen das Produkt als Oracle Database Firewall Version 5.0 Anfang 2011 freigegeben.

Abschließend sei darauf hingewiesen, dass die Firewall zur Zeit bei Datenbankzugriffen über verschlüsselte Datenleitungen nicht verwendet werden kann. Dabei ist es unerheblich, ob die Verschlüsselung über SQL Net erfolgt oder über andere Verfahren. Allerdings wird vermutlich schon die nächste Version des Produkts mit der SQL Net Netzwerkverschlüsselung arbeiten können. Bis dahin kann man die Zeit nutzen und die Firewall stufenweise einführen: Zunächst schützt man schutzbedürftige Systeme, auf die unverschlüsselt zugegriffen wird. So gewinnt man erste praktische Erfahrungen in der Arbeit mit der Firewall. Sobald der Zugriff auf verschlüsselte Daten unterstützt wird, bindet man dann die Systeme ein, die die Verschlüsselung nutzen.

Kontaktadresse:

Heinz-Wilhelm Fabry
ORACLE Deutschland B.V. & Co. KG
Riesstr. 25
D-80992 München

Telefon: +49 (0) 89-1430 1534
E-Mail heinz-wilhelm.fabry@oracle.com
Internet: www.oracle.com