ORACLE®

Oracle Database Firewall

Suvad Sahovic
Senior Systemberater
suvad.sahovic@oracle.com

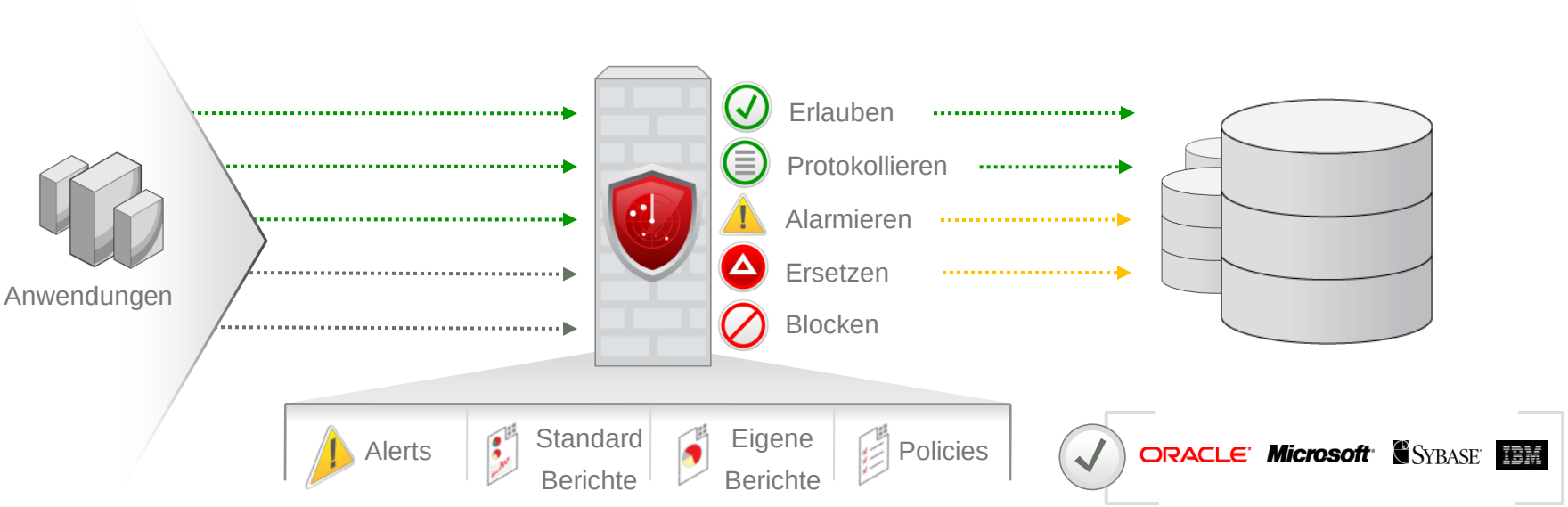
Agenda

- Oracle Database Firewall im Überblick
- Oracle Database Firewall im Einsatz
- Verfügbarkeit und Grenzen

Agenda

- Oracle Database Firewall im Überblick
- Oracle Database Firewall im Einsatz
- Verfügbarkeit und Grenzen

Oracle Database Firewall im Überblick



- Monitoring der DB Aktivitäten
- Effiziente Analyse des SQL in Echtzeit
- Genauigkeit ist von zentraler Bedeutung

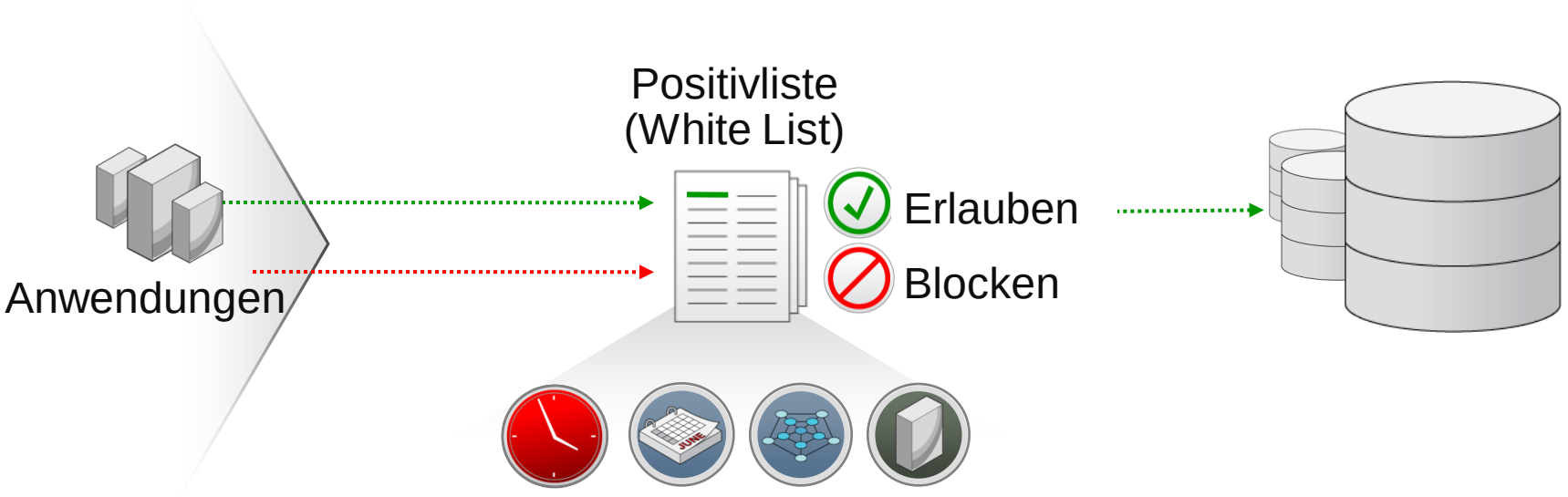
Genauigkeit zählt

- Die Firewall muss erkennen können, was das SQL in der Datenbank bewirkt
  - DML, SELECT, DCL, DDL, TCL, Stored Procedure, RPC ?
  - Wer veranlasst die Aktion und von wo?
  - Mit welchen Schemaobjekten wird gearbeitet?
  - War die Aktion erfolgreich?
- Anders als alle vergleichbaren Produkte verwendet die Oracle Database Firewall zur Analyse von SQL keine regulären Ausdrücke oder Zeichenkettenvergleiche
  - SQL ist über Vergleichsoperationen nicht zu interpretieren
  - Vergleichsoperationen sind ungenau und wenig effektiv

Wie Oracle Database Firewall Genauigkeit erreicht

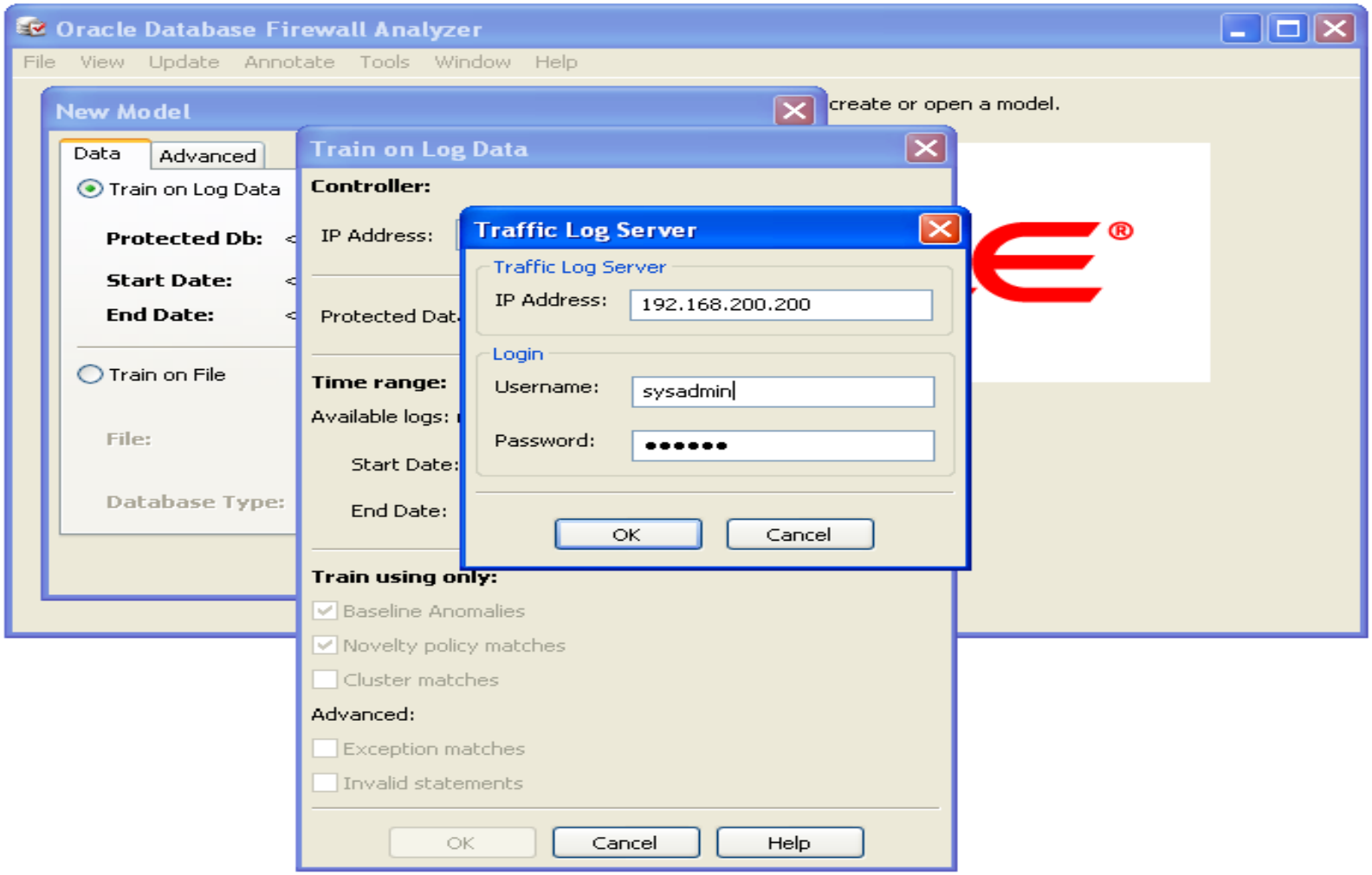
- Patentiertes Verfahren entwickelt an der Universität in Oxford
  - SynoptiQ Engine - Semantic Clustering - Intent Based Models
    - Genaue Kenntnisse der Grammatik von SQL führen zum 'Verständnis' einer Aktion
    - Durch die semantische Analyse der Grammatik und Struktur eines SQL Befehls werden alle relevanten Aspekte des Befehls erfasst
    - Es können auch Attribute aus der Umgebung der Aktion zur Analyse hinzugezogen werden
      - Zeitpunkt
      - IP Adresse des Client
      - ...

Positivlisten

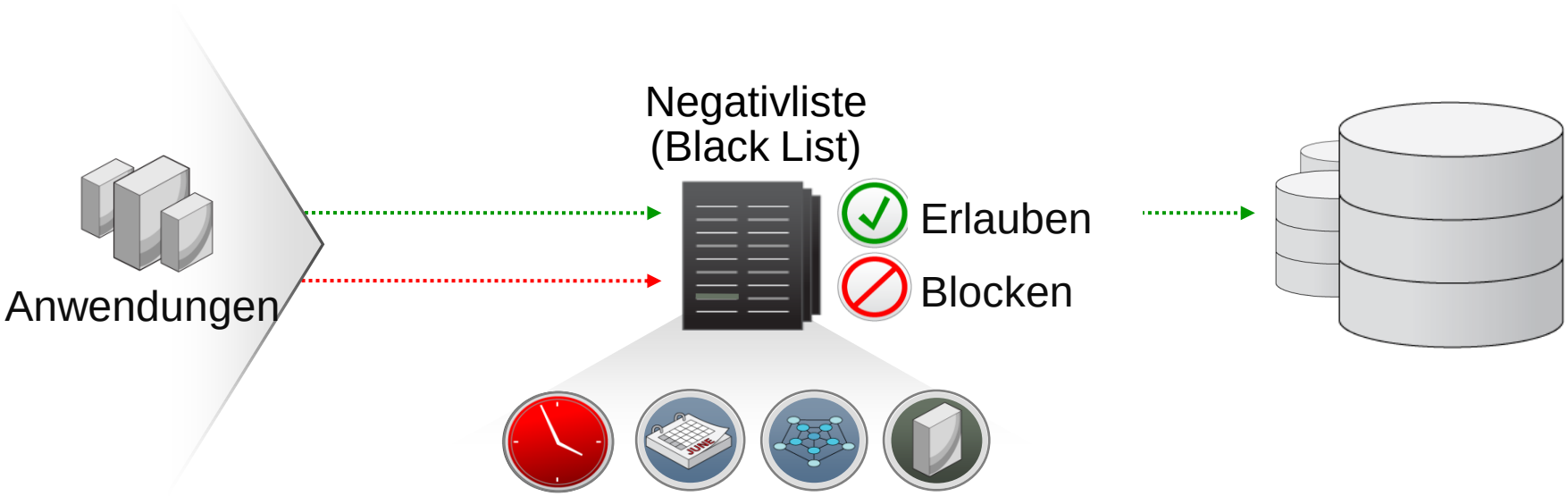


- Positivlisten können automatisch generiert werden
- Für jede Anwendung oder Applikation zu definieren
- Faktoren wie Tageszeit, Wochentag, Netzwerk, Anwendung, ... können berücksichtigt werden

Automatisches Erstellen von Positivlisten



Negativlisten

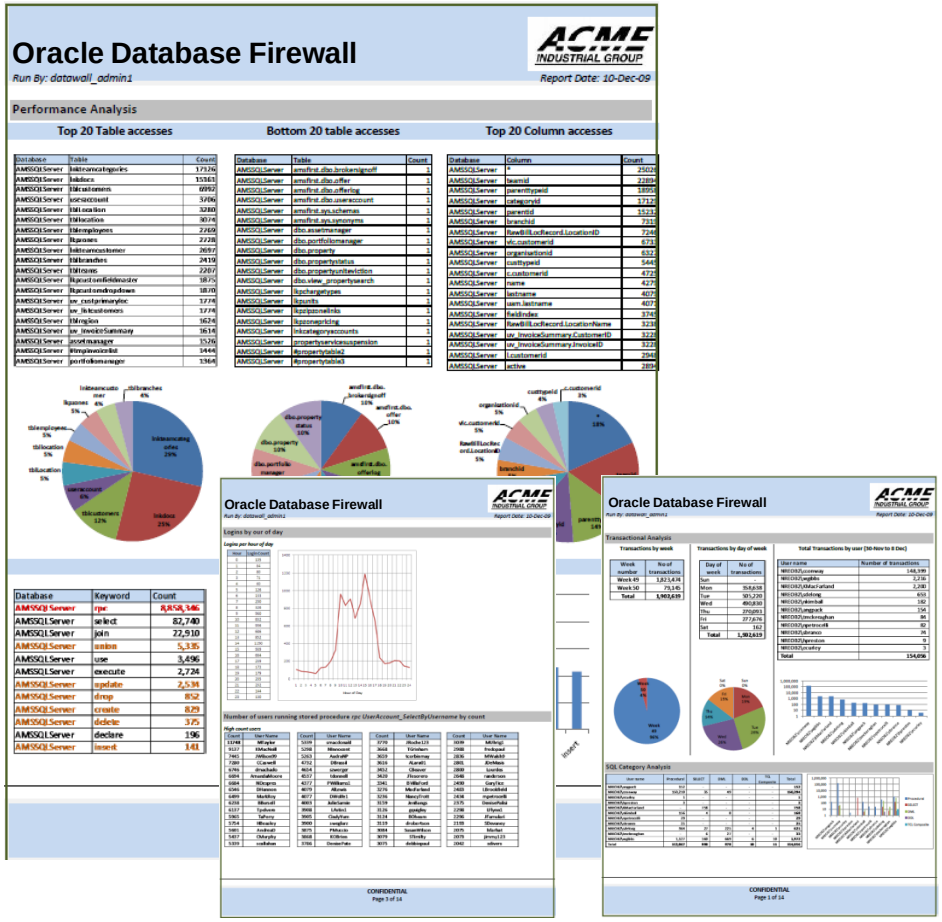


- Unterbindet unerwünschte SQL Befehle
- Kann Benutzer ausschließen, Zugriff auf Objekte verhindern
- Verhindert die Eskalation von Privilegien oder Rollen sowie nicht authorisierte Zugriffe auf sensible Daten
- Faktoren wie Tageszeit, Wochentag, Netzwerkinformationen, Anwendungsname können berücksichtigt werden

Protokollieren (Logging)

- Ergebnisse werden zur Sicherung gegen Manipulationen signiert
- Umfang der Aufzeichnungen ist konfigurierbar
  - Nur bestimmte Befehle
  - Abweichungen von Policies
  - ...

Berichte



- Database Firewall führt Protokolle in einer eigenen Datenbank
- Mehr als 130 anpassbare Berichte im Lieferumfang
  - Berechtigungslisten für eigene Kontrollen und Audits
  - Definierbare Aktionen und Aktivitäten privilegierter Benutzer
  - Unterstützt die Nachweisbarkeit von PCI-, SOX-, ... konformen Praktiken
- Bei Bedarf können sensible Daten in den Berichten maskiert werden

Integration mit anderen Produkten

- Reporting Lösung
  - Zum Erstellen von Berichten über die von den Firewalls übertragenen Ereignisse
- BIG-IP Application Security Manager (ASM 9.5.x)
  - Web Application Firewall (WAF) von f5 Networks, Inc.
- ArcSight Security Information Event Management (SIEM)
  - Zentrales System für Logging, Analyse und Management von Syslog Informationen aus unterschiedlichsten Quellen

Agenda

- Oracle Database Firewall im Überblick
- Oracle Database Firewall im Einsatz
- Verfügbarkeit und Grenzen

Die Bausteine

- Kontrolliert jeden Zugriff
- Blockt nicht autorisierte Aktionen ab

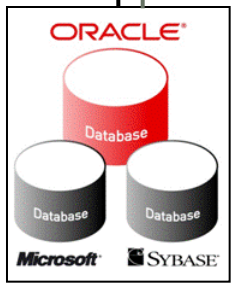
- Berichte, Archive
- Firewall, Policy Management
- Alarmieren, Integration

- Definiert Zugriffskontrollen
- Nur Windows XP oder Vista Desktop

Database Firewall

Database Firewall Management Server

Policy Analyzer



Die Bausteine - Verfügbarkeit Firewalls

- Kontrolliert jeden Zugriff
- Blockt nicht autorisierte Aktionen ab

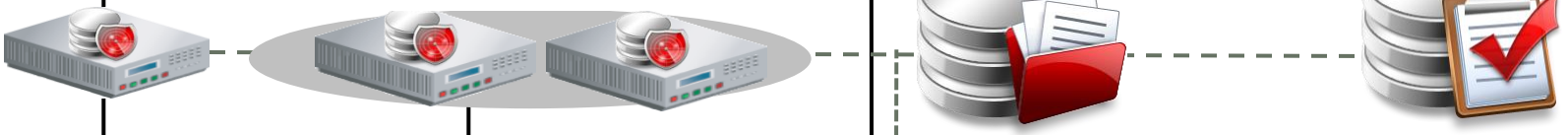
- Berichte, Archive
- Firewall, Policy Management
- Alarmieren, Integration

- Definiert Zugriffskontrollen
- Nur Windows XP oder Vista Desktop

Database Firewall

Database Firewall Management Server

Policy Analyzer



Database Firewall

Identische HW
('Resilient Pair')

Die Bausteine - Verfügbarkeit Management Server

- Kontrolliert jeden Zugriff
- Blockt nicht autorisierte Aktionen ab

- Berichte, Archive
- Firewall, Policy Management
- Alarmieren, Integration

- Definiert Zugriffskontrollen
- Nur Windows XP oder Vista Desktop

Database Firewall

Database Firewall Management Server

Policy Analyzer

Database Firewall

Identische HW ('Resilient Pair')

Stand-by-System ('Resilient Pair')

Die Bausteine - Remote / Local Monitor

- Kontrolliert jeden Zugriff
- Blockt nicht autorisierte Aktionen ab

- Berichte, Archive
- Firewall, Policy Management
- Alarmieren, Integration

- Definiert Zugriffskontrollen
- Nur Windows XP oder Vista Desktop

Database Firewall

Database Firewall Management Server

Policy Analyzer

Database Firewall

Identische HW
('Resilient Pair')

Maximal Stand-by-System
('Resilient Pair')

Remote / Local Monitor

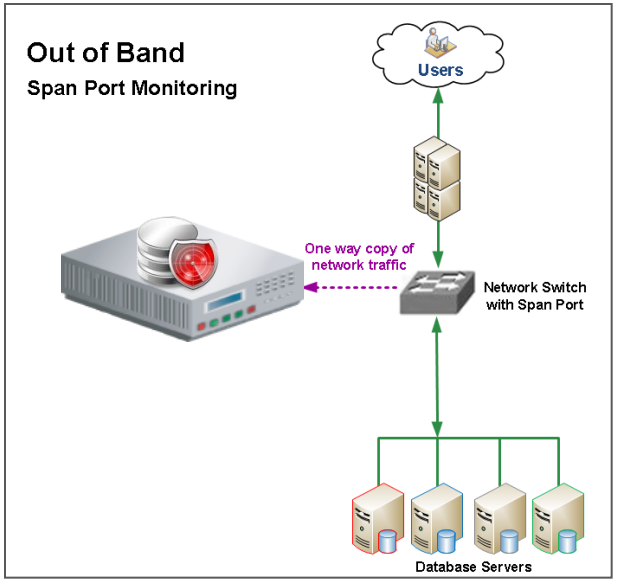
- Leiten Datenbankzugriffe an die Database Firewall weiter

Flexibel einzusetzen

- Normalerweise separate Rechner für jede Firewall und jeden Firewall Management Server
  - Oracle Enterprise Linux
  - Mindestens 1G RAM
  - Mindestens 80G Disk
- Firewall benötigt zertifizierte Netzwerkkarten, um Aktionen abblocken zu können
- Skalierung
  - Vertikal: CPU, Festspeicher oder Arbeitsspeicher hinzufügen statt mehr und mehr Rechner oder Appliances
  - Horizontal: Rechner hinzufügen, wenn Kapazitätsgrenzen erreicht sind oder aus Überlegungen zur Verfügbarkeit

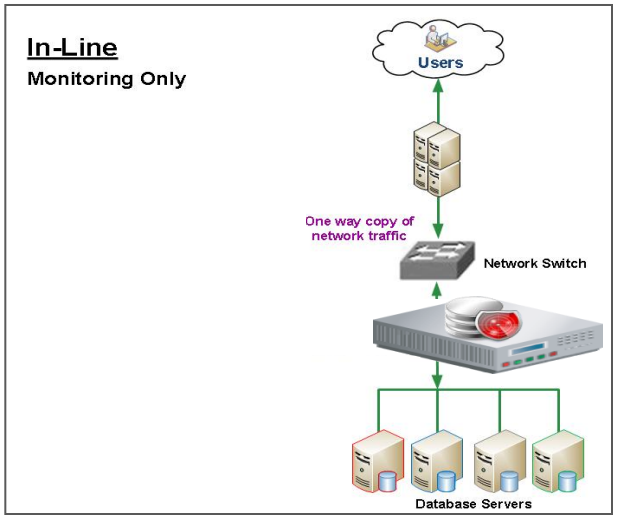
Out of Band

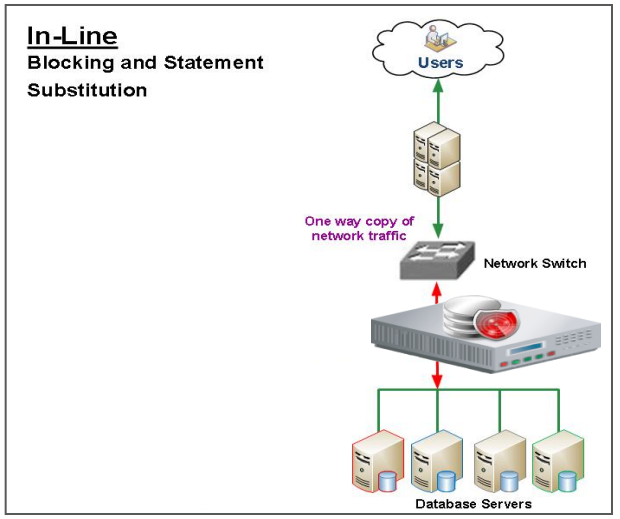
- Monitor Only Modus
  - Technisch: Wird auch als "SPAN", "Span Port", "Mirrored" oder "Tap" bezeichnet
  - Kein Abblocken von Aktionen
- Ausschließlich zur Protokollierung und für Berichte
- Kein Einfluß auf laufende Datenbanken oder Anwendungen



In-Line

- Blocking und Monitoring
  - Technisch: Wird auch als “bridge” oder “transparent bridge” bezeichnet
  - SQL wird im Hinblick auf die festgelegten Regeln überprüft
  - Durch Einsatz von Netzwerk Bypass Karten kein Ausfall der Firewall





Weitere Möglichkeiten

- Stored Procedure und User Role Auditing
  - Protokollieren Änderungen an Stored Procedures und Rollen
    - Über eigens angelegten Benutzer mit minimalen Privilegien
    - Frequenz der Überprüfung einzustellen
- Response Monitoring
  - Erfassen von Erfolg / Misserfolg von Befehlen und Logins / Logouts
- Direct Database Interrogation
  - Für SQL Server und Sybase SQL ANYWHERE
    - Zusätzliche Informationen zu Befehlen, z.B. welcher Benutzer einen Befehl ausgeführt hat

Agenda

- Oracle Database Firewall im Überblick
- Oracle Database Firewall im Einsatz
- Verfügbarkeit und Grenzen

Unterstützte Datenbanken

- Oracle
  - Oracle8i, Oracle9i, Oracle Database 10g, Oracle Database 11g
- MS-SQL Server
  - 2000, 2005, 2008
- Sybase
  - ASE 12.5.4 bis 15
  - SQL Anywhere 10.0.1
- IBM
  - DB2 9 auf Linux, UNIX, Windows

Verfügbarkeit und Grenzen

- Version 5.0 verfügbar seit 11. Januar 2011
- Produkt ist kein Newcomer im Markt
  - Oracle hat die britische Firma Secerno im Mai 2010 gekauft
  - Das bedeutendste Produkt der Firma Secerno hieß DataWall und ist der Vorläufer von Oracle Database Firewall
- Kein Appliance, sondern reine Softwarelösung
  - Spezifika zur erforderlichen Hardware beachten - zum Beispiel zertifizierte Netzwerkkarten zum Blocken
  - Performance (Version 4.1): 230.000 Transaktionen / Sekunde*
- Zur Zeit keine Unterstützung von Infiniband
- Zur Zeit kann die Firewall nicht uneingeschränkt mit verschlüsselten Netzwerken arbeiten

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®