

BGOUG Conference Nov-2011, Hissarya

Building defensive perimeter with Oracle Database Firewall

Nikolay Manchev

About me

Oracle ACE

- Oracle OCP 10g, 11g
- SCJP
- VMware VCP VI3, vSphere
- LPIC-1

Visit my website at <http://manchev.org>

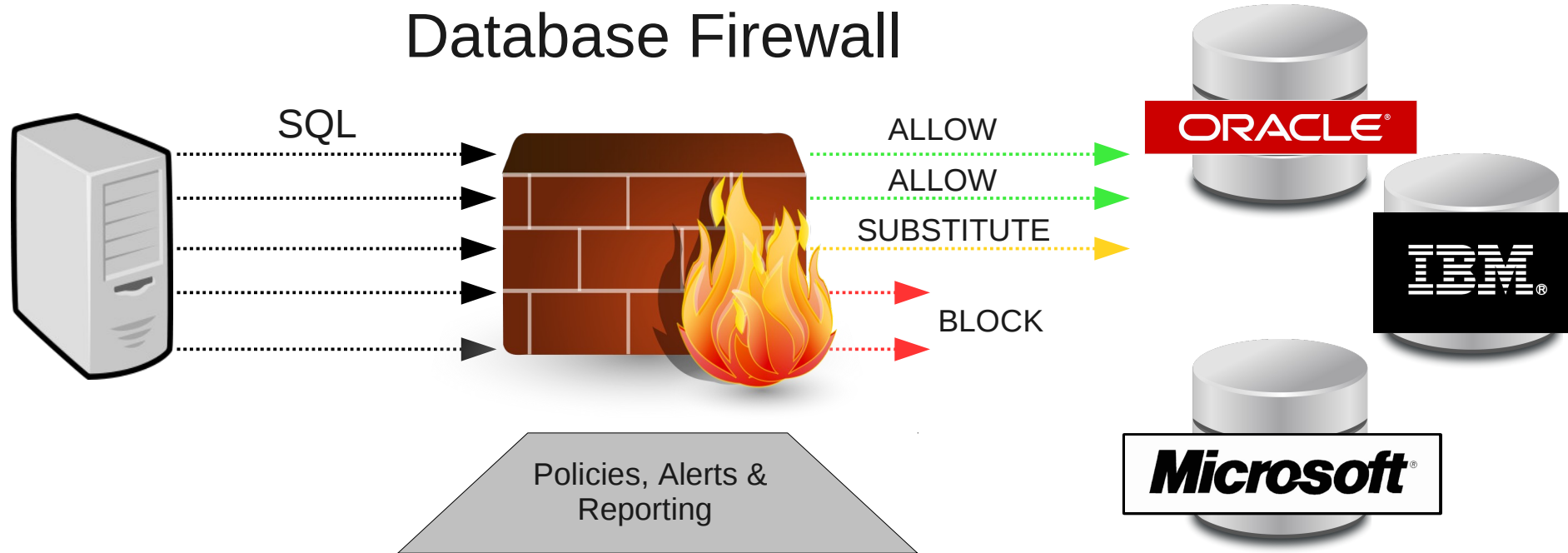
Introduction

Why Database Firewall

- 2010 Data Breach Investigation Report
 - 98% of data breached came from servers
 - 86% of records stolen via SQL injection
 - Most common techniques – privilege misuse and hacking
- Traditional solutions **do not** monitor SQL traffic sent over trusted path

Database Firewall Overview

- Active, real-time database firewall



Protection Levels

- **Database Activity Monitoring (DAM)**
 - Detects & logs unusual activities
 - Produces warnings
 - Does not block potential threats (useful in early stage deployments)
- **Database Policy Enforcement (DPE)**
 - Detects, logs & blocks potential attacks
- **Stored Procedure Auditing**
- **User Role Auditing**

Logs

- Traffic Log
 - SQL statements, login & logout events
 - Database username
 - OS username
 - IP address of the client
 - Client program name
- Event Log
 - System events not related to the database (OS level warnings)
- Administration Log
 - Configuration changes (shutdowns, restarts, policy changes in Admin Console)

Deployment considerations

- Location
 - Database Firewall must be connected to a network point that is close to the database
 - Alternative: Database Firewall connected behind client application
- Statement blocking
 - Not used: spanning port to direct traffic to an Oracle Database Firewall port
 - Used: Database Firewall placed in between clients and database
- Direct database access
 - Local monitoring of traffic originating on the DB server

Deployment scenarios

- Database Firewall and Management Server – same host
- 1 or more Database Firewall (dedicated hosts), 1 Management Server (dedicated host)
- Redundant Database Firewall servers, 2 Management Servers – high availability configuration
- Local monitoring
 - Local connections on the DB server
- Remote monitoring
 - Installed on DB host, sends data to Database Firewall
 - No SQL blocking

Hardware considerations

- Database Firewall requires a dedicated x86 server
 - Installation **wipes out** the entire machine
- Database network should be separate from the network that runs Database Firewall applications
- Database Firewall requires 3 network ports
- Management Server requires 1 network port
- In blocking mode Database Firewall **blocks all** IPv6 traffic

Hardware requirements

- Database Firewall & Management Server
 - 1 GB RAM (minimum)
 - 80 GB of disk space
 - Three network ports

Supported databases

| Database | Direct DB Interrogation | User Role Auditing | Stored Procedure Auditing | Local Monitor |
|--------------------------------|-------------------------|--------------------|---------------------------|---------------|
| Oracle Database 8i | | | | |
| Oracle Database 9i | | ● | ● | ● |
| Oracle Database 10g | | ● | ● | ● |
| Oracle Database 11g | | ● | ● | ● |
| SQL Server 2000 | | ● | ● | ● |
| SQL Server 2005 | ● | ● | ● | ● |
| SQL Server 2008 | ● | ● | ● | ● |
| Sybase ASE 12.5.4/15.0.x | | ● | ● | ● |
| Sybase SQL Anywhere 10.0.1 | ● | ● | ● | ● |
| DB2 9.x (Linux, Unix, Windows) | | ● | ● | ● |

Installation

Enterprise Linux

ORACLE®

- To install or upgrade in graphical mode, press the <ENTER> key.
- To install or upgrade in text mode, type: linux text <ENTER>.
- Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: _

Welcome to Enterprise Linux

Root Password

Pick a root password. You must type it twice to ensure you know what it is and didn't make a mistake in typing. Remember that the root password is a critical part of system security!

Password: *****
Password (confirm): *****

OK Back

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Welcome to Enterprise Linux

Package Installation

Name : nash-5.1.19.6-61.0.1-i386
Size : 2368k
Summary: nash shell

24%

| | Packages | Bytes | Time |
|------------|----------|-------|---------|
| Total : | 320 | 770M | 0:02:59 |
| Completed: | 7 | 73M | 0:00:17 |
| Remaining: | 313 | 697M | 0:02:42 |

9%

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Please enter password for OS user "support"

< OK >

<Cancel>

Please enter password for DB user "sys"

< OK >

<Cancel>

Network Devices

```
eth0 Management, Link: yes, 00:0C:29:85:C1:7E, PCI 0000:02:01.0
eth1 br0, Link: yes, 00:0C:29:85:C1:88, PCI 0000:02:02.0
eth2 br0, Link: yes, 00:0C:29:85:C1:92, PCI 0000:02:03.0
-
Actions Save, refresh, ...
```

<Select>

<Cancel>

Welcome to Enterprise Linux

Complete

Congratulations, your Enterprise Linux installation is complete.

Remove any media used during the installation process and press
<Enter> to reboot your system.

Reboot

<Enter> to reboot

Network Settings Console

Current settings


```
IP Address: 192.168.0.200
Network Mask: 255.255.255.0
Default Gateway: 192.168.0.254
```

Change

```
- IP Address
  Network Mask
  Default Gateway
```

Administration Tools

Administration console

Dashboard Appliances Monitoring Reporting Archiving System Logout

Oracle Database Firewall Management Server Administration Console Welcome. You are logged in as *psmith* | Version: 5.0 | 15:59:15

Threat Status: OK

Known Blocked: 0
Unseen Blocked: 0
Known Warned: 0
Unseen Warned: 0

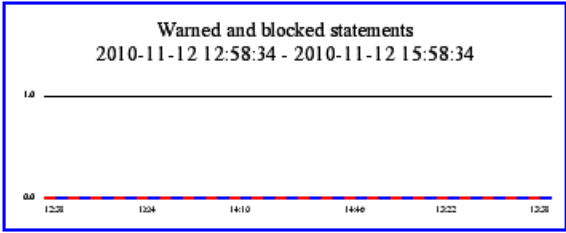
Throughput Status: OK

Statement Rate: 0
Total Statements: 0
(In Last Hour)

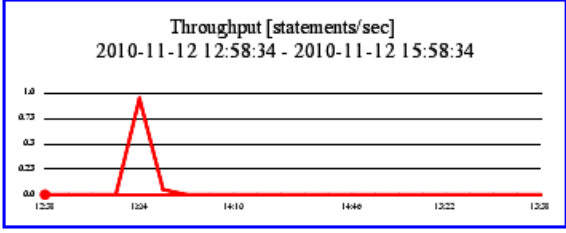
Traffic Snapshot at 2010-11-12 15:59

Filter (no filter active)

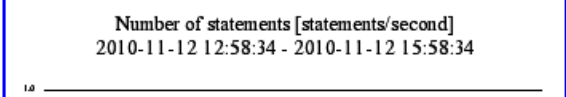
Warned and blocked statements
2010-11-12 12:58:34 - 2010-11-12 15:58:34



Throughput [statements/sec]
2010-11-12 12:58:34 - 2010-11-12 15:58:34



Number of statements [statements/second]
2010-11-12 12:58:34 - 2010-11-12 15:58:34



Quick Start

Monitor databases System settings

Top Ten Threats (Last Week)

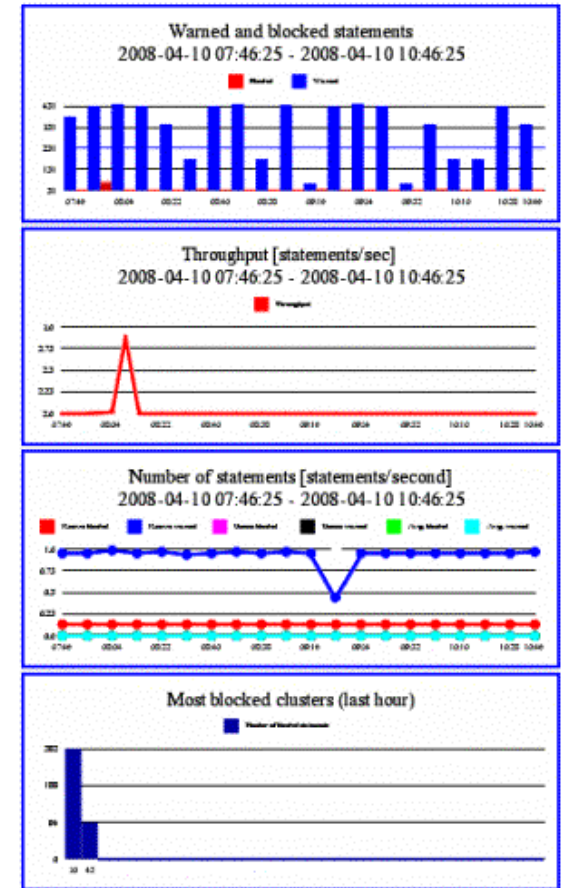
| Count | Status | Statement | Seen | Log Level | Source | Destination |
|-------------------|--------|-----------|------|-----------|--------|-------------|
| No data available | | | | | | |

Enforcement Points


| Name | Appliance | IP Address |
|---------|-----------|---------------|
| DB Demo | app83 | 10.167.147.84 |

Administration console

- Number of SQL statements that were blocked or caused a warning over the last three hours
- Number of SQL statements processed per second over the last three hours
- SQL cluster IDs that were most blocked in the last hour



Database Firewall Analyzer

- Used mostly for policy design
- Runs only on MSFT Windows 
- Provides functionality for clustering statements

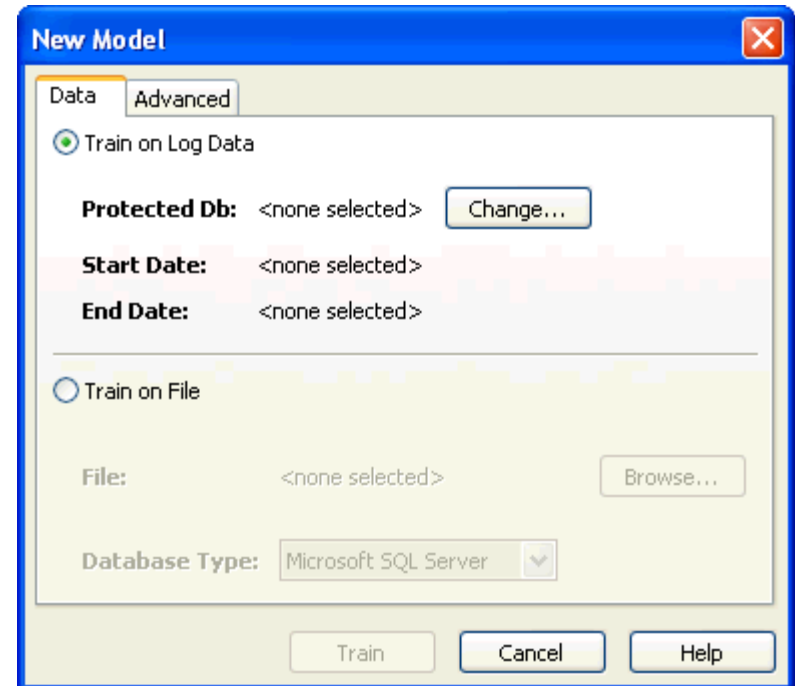
```
SELECT * FROM DEPT;  
SELECT * FROM EMP.DEPT;  
SELECT * FROM DUAL;
```



You don't want individual policies for these.

Training the analyzer

- Using Log Data from firewall
- Using Train file
 - List of SQL statements



Automatic Policy Creation

- Automatically assigns a threat severity to each cluster
- Automatically assigns logging and action levels to each cluster based on its threat severity

The screenshot displays the Oracle Database Firewall Analyzer interface. The main window is titled "Log Data Training - Oracle Database Firewall Analyzer". The interface includes a menu bar (File, View, Update, Annotate, Tools, Window, Help) and a tabbed interface with "Summary", "Details", "Baseline", "Properties", "Analysis", and "Invalid SQL" tabs. The "Summary" tab is active, showing several configuration sections:

- Exceptions:** A section with a "New Exception..." button. On the right, it shows "Action: Unassigned", "Threat: Unassigned", and "Logging Level: Unassigned".
- Statement Class Distribution:** A horizontal bar chart showing the distribution of statement classes. The legend includes: Data Manipulation Read Only (green), Data Manipulation (purple), Data Definition (yellow), Data Control (orange), Procedural (red), Transaction (blue), Composite Containing Transaction (black), and Composite (white). On the right, a table shows counts: Data manipulation (read only): 1, Data manipulation: 1, Data definition: 0, Data control: 0, Procedural: 1.
- Threat Severity Distribution:** A horizontal bar chart showing the distribution of threat severities. The legend includes: Unassigned (white), Insignificant (green), Minor (blue), Moderate (yellow), Major (orange), and Catastrophic (red). On the right, a table shows counts: Unassigned: 0, Insignificant: 0, Minor: 1, Moderate: 1, Major: 1.
- Action Distribution:** A horizontal bar chart showing the distribution of actions. The legend includes: Unassigned (blue), Pass (green), Warn (yellow), and Block (red). On the right, a table shows counts: Unassigned: 0, Passed: 1, Warned: 1, Blocked: 2.
- Policy Rules:** A section with a "New Novelty Policy..." button. On the right, it shows "Passed: 0" and "Blocked: 0".
- Default Rule for Baseline Anomalies:** A section with a "New Novelty Policy..." button. On the right, it shows "Action: Unassigned", "Threat: Unassigned", and "Logging Level: Unassigned".

At the bottom of the window, there is a "Help" button.

Policy Upload

The screenshot displays the Oracle Database Firewall Management Server Administration Console. At the top left is the Oracle logo. A navigation bar contains tabs for Dashboard, Appliances, Monitoring (highlighted in red), Reporting, Archiving, and System. A Logout button is located in the top right corner. Below the navigation bar, the page title is "Oracle Database Firewall Management Server Administration Console" and the user information is "Welcome. You are logged in as mbernstein | Version: 5.0 | 19:28:50".

The main content area is divided into a left sidebar and a main panel. The sidebar contains several sections:

- Monitoring**
- Enforcement Points:**
 - List
 - Create
 - Tasks
- Protected Databases:**
 - List
 - Create
- Policies:**
 - List
 - Upload
- Resilience:**
 - Create Pair

The main panel is titled "Upload Policy" and contains the following form elements:

- Policy:** A text input field followed by a "Browse..." button.
- Description (Optional):** A larger text input field with up and down arrow buttons on the right side.
- Save:** A button located below the description field.

At the bottom right of the main panel, the copyright notice reads: "Copyright © 2006, 2010 Oracle and/or its affiliates. All Rights Reserved."

Stored Procedure Auditing

- View all additions or changes made to the stored procedures
- Determine which changes are pending approval
- Approve changes
- View all approvals made
- Examine a history of previous approvals

Pending Approvals for Stored Procedures

Filter (filter applied)
« Previous 1 2 3 4 5 6 7 8 9 ... 311 312 Next »

| Enforcement Point | Stored Procedure Name | Class | Modifications | Status | By | Last Modification Date |
|-------------------|--|-------|---------------|---------|----|------------------------|
| DB01 | AVSRCUSER1.DBMS_SRC_STREAMS_UTILITY_BODY | user | New | Pending | | 2008-09-25 21:41:28 |

User Role Auditing

- View all additions or changes made to the user roles.
- Approve the changes.
- Determine which changes are pending approval.
- View all approvals made.
- Examine a history of previous approvals.

Pending Approvals for User Roles

Filter (no filter active) Approve All

| Enforcement Point | User Role Name | Class | Modifications | Status | By | Last Modification Date | Tags |
|-------------------|----------------|-------|----------------|---------|----|------------------------|---|
| DB01 | AVSRCUSR1 | user | 1 modification | Pending | | 2010-08-26 13:46:04 | Decline Accept |
| DB01 | AVSYS | user | 1 modification | Pending | | 2010-08-26 13:46:04 | SYSTEM Decline Accept |

User Role Auditing

Difference for User Role "AVSYS"

Key: Unmodified Text **New Text** **Inserted Text** **Replaced Text** **Deleted Text**

[Print this Page](#)

Enforcement Point: DB01
User Role Name: AVSYS
Class: User
Edit Summary: 1 modification
Last Approved: 2010-08-26 13:42:41 UTC
Modified: 2010-08-26 13:46:04 UTC

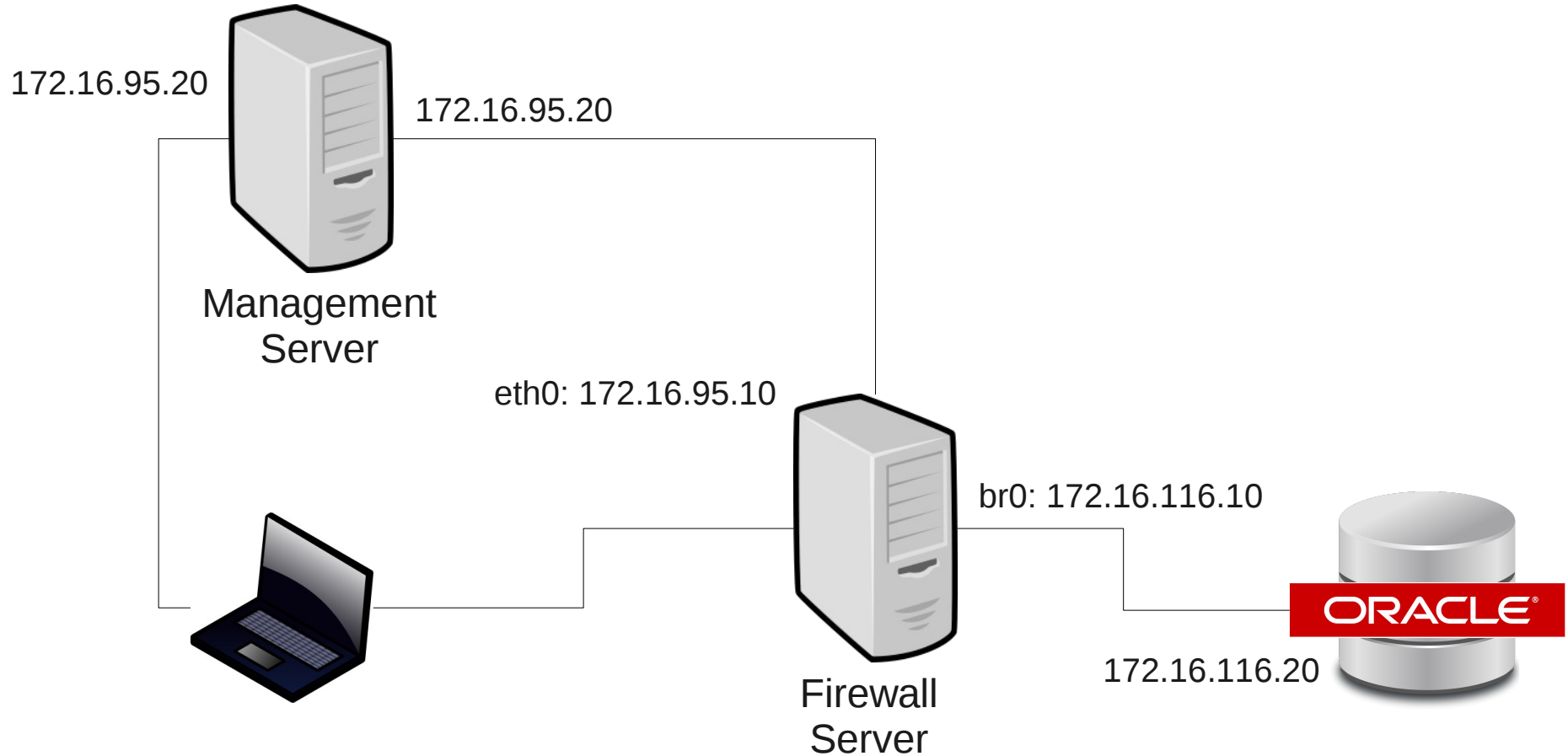
```
Username: AVSYS

Authentication method: DATABASE

Roles:
AQ_ADMINISTRATOR_ROLE : (parent: AV_ADMIN)
AQ_USER_ROLE : (parent: AV_SOURCE)
AV_ADMIN
AV_AGENT : (parent: AV_ADMIN)
AV_SOURCE
CONNECT : (parent: DV_ACCTMGR)
DV_ACCTMGR
HS_ADMIN_ROLE : (parent: SELECT_CATALOG_ROLE)
RESOURCE
SELECT_CATALOG_ROLE : (parent: AV_ADMIN)
XDBADMIN : (parent: AV_ADMIN)
XDBWEBSERVICES : (parent: XDBADMIN)

Privileges:
ALTER ANY RULE
ALTER PROFILE : (parent: DV_ACCTMGR)
ALTER SYSTEM
ALTER_USER : (parent: DV_ACCTMGR)
CREATE ANY RULE
CREATE ANY VIEW : (parent: AV_AGENT)
```

Demo Setup



Q&A

Visit my website at <http://manchev.org>