ScaleArc

Technical Brief

Securing the Database Stack

How ScaleArc Benefits the Security Team

Introduction

Relational databases store some of the world's most valuable information, including financial transactions, personal user data, business performance data, and valuable reports. As a result, such databases are frequently the target of attacks by those who wish to gain access to that valuable data for illegitimate purposes.

Databases are frequently the target of attacks by those who wish to gain access to that valuable data for illegitimate purposes

Traditionally, most aggregation devices at the network layer – routers, firewalls, web load balancers, for example – have provided features and controls as well as information such as logs to prevent unwanted access. Since most of these devices aren't database-protocol aware, however, they really can't help much when it comes to securing the database. Also, as databases are accessed through a multitude of applications, and as more and more applications share common data sources, it is becoming extremely critical to ensure that data access patterns can be deeply monitored and controlled to prevent compromising the security of the database.

The 3 A's of network security are Authentication, Authorization and Accounting. ScaleArc allows you to significantly improve database security with strong features that expand on all three of those properties. Among the features ScaleArc supports to improve database security are:

- Traffic aggregation and control
- Database access auditing
- Database query firewall
- Zero downtime patching

Traffic Aggregation and Control

Because ScaleArc is a complete database proxy / Layer 7 routing engine with support for database authentication offload (ScaleArc can authenticate a database connection before sending any traffic to the database servers), you can use it to create a database architecture that allows for extremely granular, application-specific, secure access to the databases.

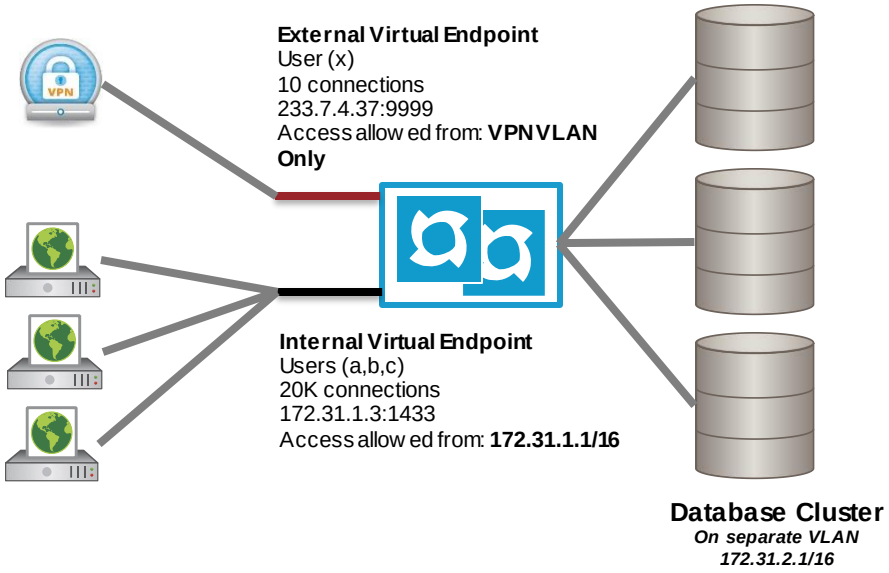

Figure 1. ScaleArc is a complete database proxy / Layer 7 routing engine with support for database authentication offload.

ScaleArc can represent the same database cluster as many different virtual endpoints. Each endpoint can have its own IP address / DNS Name and TCP Port; can be assigned to a separate network interface / VLAN; and can have its own set of IP and SQL query firewall policies, connection limits, and a restricted set of usernames that can access it. The database servers themselves can also be placed in their own private network, with ScaleArc acting as a bridge between all applications and clients and their respective databases.

These constructs let you create a significantly tighter database access policy that allows you to define different applications and teams as their own individual database access endpoints, so you can control and monitor database access more granularly. For example, you could create a single highly available "Logistics" database cluster and create two separate virtual endpoints for this cluster. One endpoint could support your own internal applications and provide access only from within your internal network. It could allow any username to connect to the database for any database access with a connection limit of 50,000 connections to accommodate for any and all workload you may have. You could use the second endpoint to support an external supplier who needs access to the same database. That supplier could connect via a bridged VPN network, which allows only a specific read-only user to authenticate and access the database limits the maximum connections to no more than 10, and doesn't allow queries that use the "SELECT *" query method to prevent easy access to full table dumps.

This level of control and isolation of workload, users, and applications not only lets you monitor and audit access very accurately but also lets you very quickly shut down access for specific endpoints or access groups in case of a breach. It also ensures no one within your organization can ever access the database through a direct administrative client connection without an audit trail.

Database Access Auditing

ScaleArc is the only technology that can provide full, granular database access logging for all connections, reads, writes, and transactions without any additional performance overhead on the database stack. ScaleArc also processes these logs into very easy to understand usage patterns, which lets you analyze and compare data access patterns across a very wide time range very quickly and discover anomalies in a fraction of the time it takes to do so via conventional log-based analysis methods – if such a log is present at all, since most databases don't store connection and read logs but only write logs.

ScaleArc is the only technology that can provide full, granular database access logging for all connections, reads, writes, and transactions without any additional performance overhead on the database stack.

This ability to quickly compare access patterns is particularly critical when a data leak or breach occurs, since the time it takes to discover the usage pattern of how the breach occurred is directly correlated with the time it takes to close the hole that led to the breach. The faster you close the breach, the less risk you have.

Though ScaleArc provides very detailed logs, they ability to store many months of data can be impacted if you're limited on storage capacity. ScaleArc's de-duplicated analytics conserve storage space by storing the analyzed, reduced-pattern data in easy-to-access, hourly patterns while still preserving many details about the database traffic, such as what type of query patterns were executed, how frequently, and by which users and what IP addresses. If storage is limited, the logs may be rotated, but this data is preserved. It isn't uncommon for ScaleArc customers to be able to see such details for usage patterns for time periods spanning a few months even if they're constrained on storage space.

ScaleArc's unique patterns comparison tool lets you quickly see what new query methods or patterns have been used in a time band when compared with another. You can easily find new query patterns that may correspond to SQL injection attacks or new, unique data-access patterns that have never been seen before. This tool lets you quickly find errant query behavior and block it using ScaleArc's database query firewall. In the future, ScaleArc will include tools to automatically scan and analyze database traffic patterns for signs of SQL injection attacks and proactively alert you of the same.

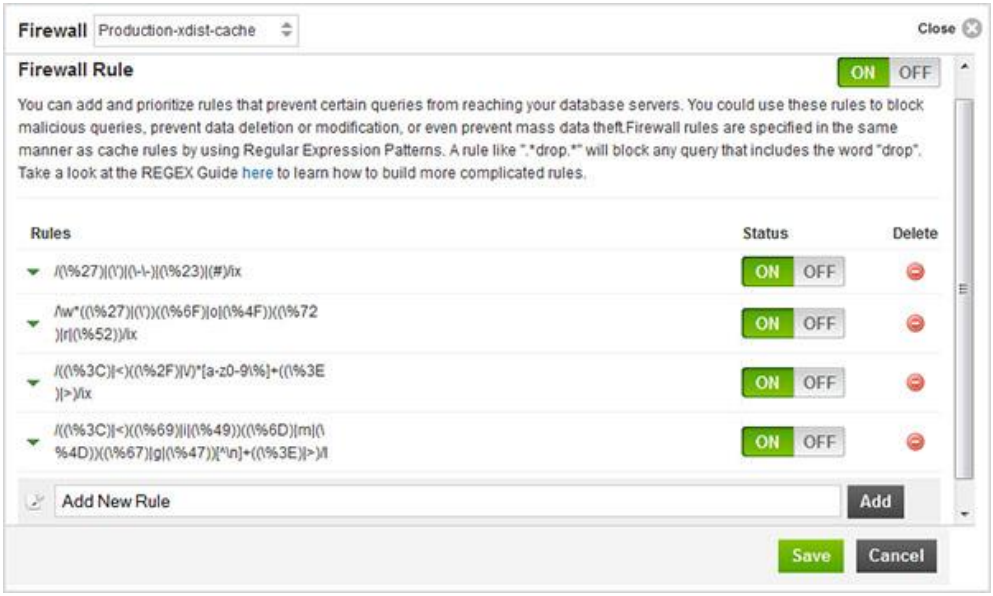

Figure 2. ScaleArc's SQL query firewall lets you simply block any unwanted SQL queries with simple Regex patterns that can be automatically generated from ScaleArc's analytics or custom crafted to suit certain specific use cases.

Database Query Firewall

ScaleArc's SQL query firewall lets you simply block any unwanted SQL queries with simple Regex patterns that can be automatically generated from ScaleArc's analytics or custom crafted to suit certain specific use cases. Here are a few examples of the kind of traffic you could potentially block.

- Malicious SQL queries that contain SQL injection attacks, or other usage patterns that may have been specially crafted to overburden the database (e.g., queries crafted with SLEEP calls in them, or queries requesting very large ranges of data due to certain holes in application design that permit user-defined ranges). Blocking them in ScaleArc will let all legitimate SQL traffic go through but return errors to those attempting to exploit the apps or database.
- Queries that are sapping performance but whose source can't be easily traced in the application. The moment you block such queries, the application logs themselves will return a very specific error which will help you trace which part of the application was sending those queries.
- Query patterns you don't wish to allow to be used in your applications. For example, a development lead at a customer didn't want his team writing code that required JOINs, but he had no means to enforce that rule in the database. With ScaleArc, enforcing such rules is as simple as blocking keywords including "INNER JOIN" and others.

Zero Downtime Patching

The number of extreme risk database and operating system exploits that require urgent patching has been going up at a very rapid rate in recent years. Recent examples such as the SSL Heartbleed bug or the Shellshock exploit were extremely risky as they left almost every server in many large networks vulnerable, and were exploited by hackers almost immediately at mass scale and used to spread malware, which led to many other attacks.

The increasing breadth and rate of vulnerabilities is leading to mandates by security teams that patches to alleviate such exploits should be installed as soon as possible. As a result, you likely need more frequent, almost ad-hoc, maintenance activity that may require you to bring down database servers and, in turn, the application. This type of maintenance activity is complex and tedious and requires resources outside of normal business hours. It may also require application re-deployment to add alert messages and maintenance window pages, it takes time to perform the actual maintenance operation, and then you must ensure the environment is healthy after the maintenance operation and bring up the app again.

The increasing breadth and rate of vulnerabilities is leading to mandates by security teams that patches to alleviate such exploits should be installed as soon as possible.

ScaleArc lets you avoid these maintenance windows, simplifying the process of keeping your database stack on the latest security patches – without any application interruptions without the need to perform maintenance outside business hours, and without needing to involve application developers.

Reduce Your Business Risk

Database firewalls are great at analyzing traffic flows in real time, alerting on malicious events and then taking action to block them. They are not built for logging all traffic for historical analysis. ScaleArc does not have full firewall capabilities and so cannot be compared directly to firewalls such as those from Imperva or Palo Alto Networks. However, ScaleArc's software complements existing database firewalls and greatly strengthens and enhances the security of the database environment in the following ways:

- ScaleArc creates an "air gap" between the applications and databases. Applications connect to ScaleArc, not to the databases, and ScaleArc provides granular access controls on a per-tenant (i.e., per app) basis to provide much tighter lockdown of the database environment.
- ScaleArc logs every single query in great detail and provides tools for historical or real-time analysis on those logs, enabling audit-quality analysis and other capabilities.
    - For example, you can quickly compare a certain hour of query traffic to the same hour the day before to see what unique queries accessed the database environment, helping to isolate unique traffic that could be malicious or unauthorized.
- Query-filtering capabilities are available to transparently block specific query patterns at ScaleArc without having to touch the application code. You can block queries with a single click of the mouse button or through the ScaleArc API.
- ScaleArc can support end-to-end SSL encryption from the application to the database, to ensure query transmissions that utilize SSL can gain full access to the ScaleArc functionality while maintaining an SSL environment.

ScaleArc

2901 Tasman Drive, Suite 205
Santa Clara, CA 95054
Phone: 1-408-780-2040
Fax: 1-408-427-3748
www.scalearc.com

ScaleArc is the leading provider of database load balancing software. The ScaleArc software inserts transparently between applications and databases, creating an agile data tier that provides continuous availability and increased performance for all apps. With ScaleArc, enterprises also gain instant database scalability and a new level of real-time visibility for their application environments, both on prem and in the cloud. Learn more about ScaleArc, our customers, and our partners at www.ScaleArc.com.

02/13/15