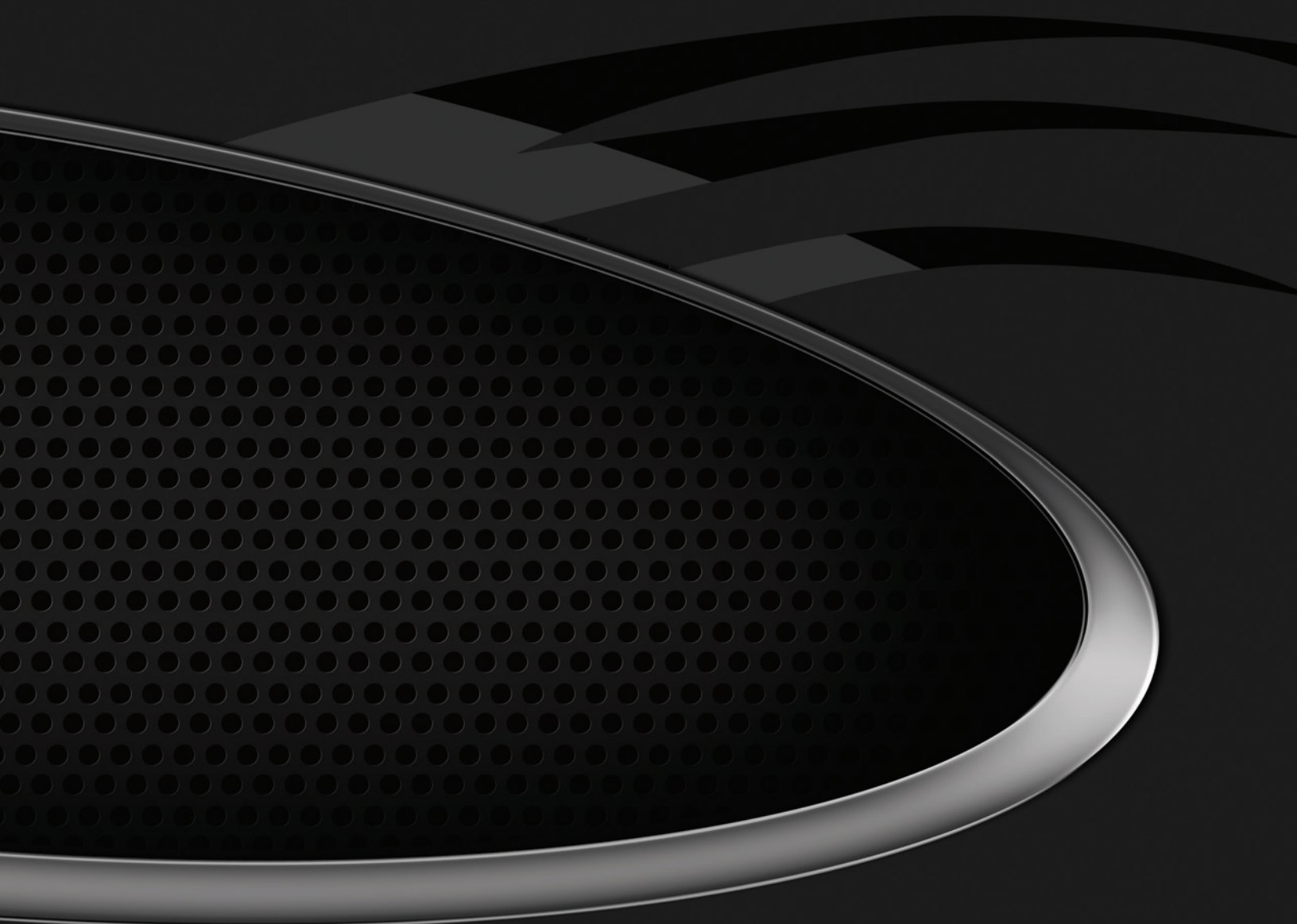# Riverbed Stingray Application Firewall

riverbed®

Overview

Attacks against web applications are increasing in sophistication, and automation makes them increasingly common. These attacks are geared toward discovering and exploiting weak points, not at the network level, but in the application code and framework itself. However, the target of the attacks remains the same – confidential information.

Stingray Application Firewall is a sophisticated, application-aware Web Application Firewall for deep application security. Now you can protect against known and unknown attacks at the application layer (such as OWASP Top10), secure your application and meet compliance requirements with confidence.
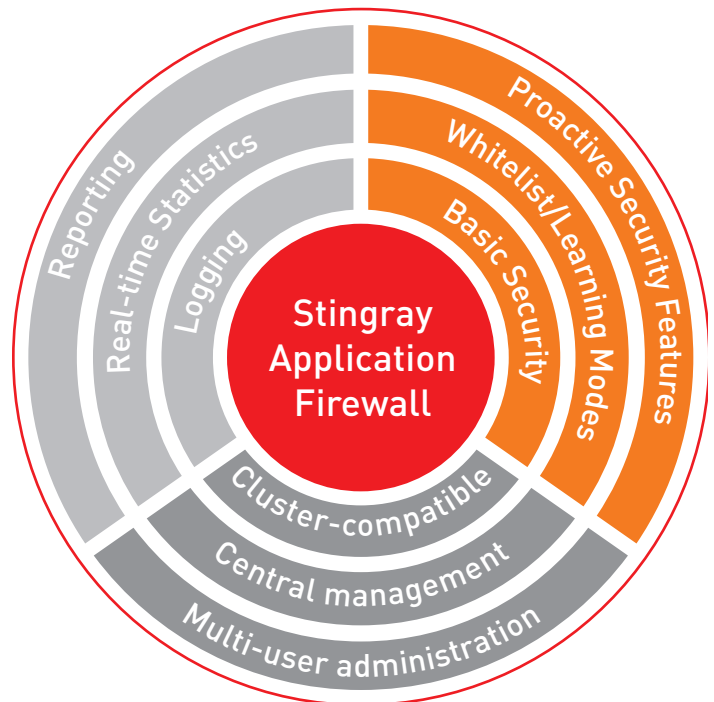
Stingray Application Firewall

A strong security layer is a necessary component for any complex web application that handles sensitive data. No matter how carefully developed and audited application code may be, it is very hard to be fully confident that no vulnerabilities exist in the application and the framework that supports it. Stingray Application Firewall adds an additional barrier of protection to increase the security of your application:

Detect and defend against common application vulnerabilities – Many attack processes seek to discover common weak points such as unchecked input data, insecure application configuration, and weak authentication. Such discoveries can then lead an attacker to draw on a library of SQL injection, cross-site scripting or session hijacking attacks. Stingray Application Firewall contains a comprehensive set of baseline signatures and identification tools to detect and block these exploratory requests.

Proactively secure your application – Stingray Application Firewall surrounds the application with a strong security perimeter that establishes a secure session identifier, proactively encrypts cookies and URLs and applies site usage enforcement to ensure that users follow appropriate journeys through the application and do not exploit the stateless nature of HTTP transactions.

Develop sophisticated security policies – No two applications are the same, and Stingray Application Firewall monitors and learns common application usage patterns. Ruleset suggestions can be inspected by the security officer, then run in 'shadow' mode for testing purposes before they are deployed to enforce user behavior. Whitelists and blacklists quickly simplify and accelerate security rules to improve performance and reduce complexity.

Monitor and Report – No security system can be deployed and managed with confidence without full audit tracking and logging. Stingray Application Firewall provides a number of reports for various purposes, ranging from immediate real-time alerts to weekly or monthly reports that outline attack trends and application behaviour.

Stingray Application Firewall is a comprehensive, scalable software solution to improve application security and inform on user behavior

PCI DSS Compliance

PCI DSS is a key standard with which organization accepting credit card details must comply. Failure to meet the requirements of PCI DSS exposes a merchant to fraud, makes the merchant liable to costs resulting from breach of cardholder data, and incurs higher processing fees from credit providers.

The standard defines a pragmatic set of security procedures that a merchant must meet. Section 6.6 of the standard mandates that a merchant must either perform regular security reviews of the source of all public-facing applications or deploy and configure an appropriate web application firewall.

Stingray Application Firewall helps meet the requirements of PCI DSS 6.6, along with other parts of the PCI DSS standard. Stingray Application Firewall can easily be configured with additional security policies to detect and prevent attacks specific to all applications.

Using Stingray Application Firewall

Basic Mode and Expert Mode

Stingray Application Firewall configuration is performed via a multi-tenant web-based user interface. Administrators can switch between a simple basic mode to create general configurations and a powerful expert mode.

In basic mode, administrators are helped in their configuration efforts by wizards and intelligent learning algorithms. A few key basic inputs are sufficient to configure a broad security policy that configures the appropriate baseline rules and advanced handlers.

Expert mode makes it easy to customize the parameters of each handler in detail as necessary. Stingray Application Firewall can automatically propose rules based on real traffic, and individual security policies can be fine-tuned iteratively as required.

Active and Shadow rulesets

Stingray Application Firewall can run two rulesets concurrently. The active ruleset is applied to all traffic and decisions to block or redirect traffic are enforced. Simultaneously, a second ruleset can run in shadow mode; applied to traffic, but the enforcement decisions are only logged.

Active and shadow rulesets make it easy to modify an existing security policy and run it in diagnostic mode without compromising the security of the application. They are an effective tool to validate rule suggestions or baseline updates against production traffic before they are enforced.

Execution of security policies

At runtime, Stingray Application Firewall receives and analyzes each request before it is processed by the web application.

In so doing, every request is assigned to one of these classes:

- Legitimate requests are passed to the web application.

- Definite attacks are repelled when protection is activated and, at the same time, as much data as possible is saved in order to identify and trace the attacker.

- Requests whose danger cannot be definitively assessed at the local level can either be rejected or passed on, depending on the local rating and installed security policy. They are also logged internally and used to then classify subsequent requests.

For return traffic, Stingray Application Firewall also analyzes your Web application's responses. Security related information such as credit card numbers can thus be filtered out from the responses and does not escape even when the attack is successful. As it continues to analyze your Web application over a period of time, Stingray Application Firewall gathers key information about its behaviour and uses it to advise how to further optimise the protection.
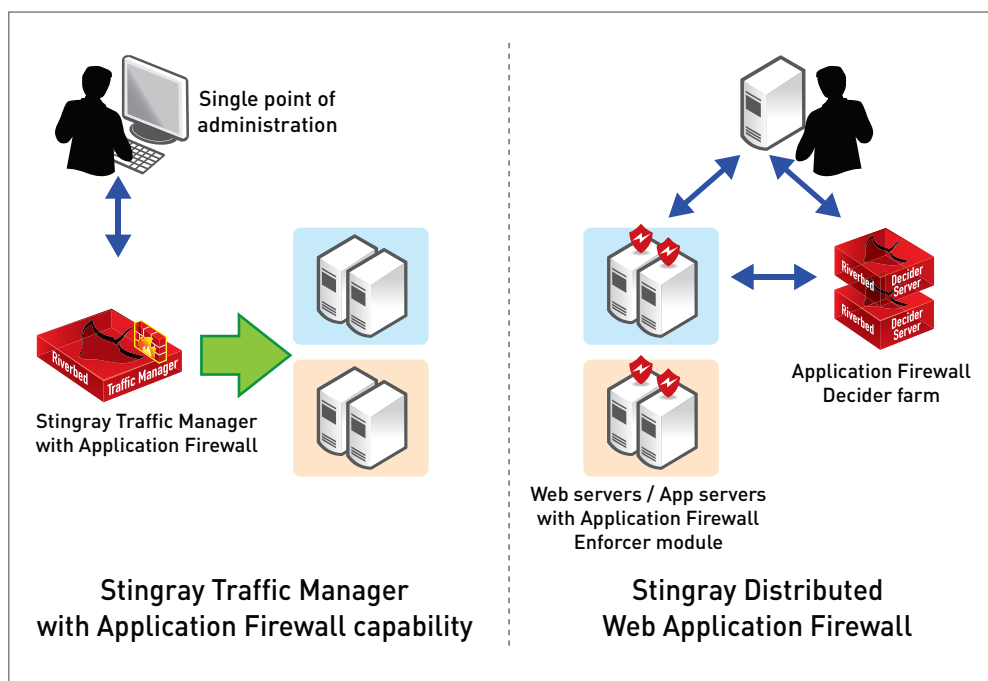
Logging, Statistics and Reporting

The recording and analysis of user activity and attack profiles gives the confidence that Stingray Application Firewall is operating as configured, and helps tune rulesets to eliminate additional suspicious user behaviour and reduce any false positives. The logging, particularly the automatically generated weekly and monthly reports, assist in demonstrating compliance with any legal or contractual rules relating to the keeping of records.

Standalone Web Application firewall or optional component for Stingray Traffic Manager

Stingray Application Firewall is available as a component of Stingray Traffic Manager, providing a fully-integrated application delivery controller (ADC) and web application firewall system.

Stingray Application Firewall is also available in a uniquely-scalable clustered architecture. Security policies are managed by an administration server and pushed out to a farm of decider processes. Enforcer modules on web and application servers capture traffic bi-directionally and forward to available deciders for validation. Enforcer and decider components may be scaled as required to meet traffic requirements.

Single point of administration

Stingray Traffic Manager with Application Firewall

Application Firewall Decider farm

Web servers / App servers with Application Firewall Enforcer module

Stingray Traffic Manager with Application Firewall capability

Stingray Distributed Web Application Firewall

Key Features and Benefits

Stingray Application Firewall is a powerful security solution combining:

- Basic and expert mode configuration for rapid configuration and fine-tuning

- Simultaneous enforcement (active) and monitoring (shadow) rulesets

- Automatic basic protection, enhanced by fine-grained custom settings

- Proactive protection including secure session management, cookie protection, URL encryption and form field protection

- Regular updates to baseline protection rulesets for common vulnerabilities

- Automated ruleset suggestions based on intelligent learning algorithms

- Bidirectional HTTP inspection; full analysis of requests and responses

- Automatic configuration for protection of Microsoft Outlook Web Access

- Dashboard of a centralized, real-time overview of security status of all applications

- Comprehensive statistics and detailed log files, managed across the cluster

- Configurable alarms (email, HTTP POST, log file) when defined events occur

- Export and import functions for migration of rules from test to live systems

- Role-based management of multiple web applications

- Full auditing of all configuration and ruleset changes

- PDF reports of service activity and security alerts

About Riverbed

Riverbed delivers performance for the globally connected enterprise. With Riverbed, enterprises can successfully and intelligently implement strategic initiatives such as virtualization, consolidation, cloud computing, and disaster recovery without fear of compromising performance. By giving enterprises the platform they need to understand, optimize and consolidate their IT, Riverbed helps enterprises to build a fast, fluid and dynamic IT architecture that aligns with the business needs of the organization. Additional information about Riverbed (NASDAQ: RVBD) is available at **www.riverbed.com**.

InfoWorld
2011
TECHNOLOGY
OF THE YEAR
AWARDS

2005, 2006, 2007, 2008, 2009, 2011

NETWORKWORLD
BEST OF THE TESTS '08

2006 Network Computing
WELL-CONNECTED AWARDS
WINNER

Riverbed Technology
199 Fremont Street
San Francisco, CA 94105
Tel: +1 415 247 8800
Fax: +1 415 247 8801
www.riverbed.com

Riverbed Technology Ltd.
The Jeffreys Building
Cowley Road
Cambridge CB4 0WS
United Kingdom
Tel: +44 (0)1223 568555

Riverbed Technology Pte. Ltd.
391A Orchard Road #22-06/10
Ngee Ann City Tower A
Singapore 238873
Tel: +65 6508-7400

Riverbed Technology K.K.
Shiba-Koen Plaza Building 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990

BR-SRAF101311