APPLICATION AWARENESS

DEEP PACKET INSPECTION FOR WEB APPLICATION SECURITY

Indigo Software strengthens its web application firewalls with R&S®PACE 2 to enhance network protection and management capabilities

ROHDE&SCHWARZ

Make ideas real

Indigo Software utilizes R&S®PACE 2 to strengthen its web application security solution in order to analyze, filter and block network traffic to protect customers from generic web attacks.

SUMMARY

Area of business

- Network security vendor, supplier of technology for network management and protection

Challenge

- Gain deeper insights into network traffic in order to trace and identify malicious activities
- Protect customers' web servers against application-level attacks
- Develop a high-performance DPI engine that receives regular application and protocol signature updates

Solution

- Embedding the DPI engine R&S®PACE 2 into the web application firewall for granular insights into applications and protocols in real time

Benefits

- By means of traffic filtering, attacks are stopped before they reach a web server
- A fast and reliable detection of application vulnerabilities is provided
- The performance and manageability of the network traffic is improved
- By licensing R&S®PACE 2, return on investment (ROI) is boosted, time-to-market is sped up and costs are reduced

CHALLENGE

While the internet has brought about tremendous advan- ces in innovation and efficiency, it also entails countless risks that perimeter security solutions cannot protect against because they only secure the network level and control access to it. These solutions do not focus on layer 7 of the OSI model that supports application and end-user processes such as HTTP and SMTP. Attacks on this layer, such as SQL injection, cross-site scripting (XSS) and DDoS attacks, present an enormous challenge, as malicious code can masquerade as valid client requests and normal application data. This is why websites, web applications and web servers are increasingly becoming prime targets for cyberattacks.

Consequently, web application firewalls (WAF) as provided by Indigo Software have become an indispensable component in the application delivery infrastructure. Indigo Software firewalls offer layer 7 web application security on a more refined level to help organizations provide a fast, reliable and secure delivery of mission-critical web applications. Its WAF detects and blocks malicious activities behind inconspicuous website traffic that may slip through traditional security solutions.

In order to provide customers with a strong and reliable solution, Indigo Software was in need of a high-performance deep packet inspection (DPI) engine that would enable its firewalls to analyze HTTP requests and responses to detect malicious behavior. Furthermore, a DPI technology was required that would not impact their throughput and receive regular application and protocol signature updates without needing extensive custom development and maintenance.

SOLUTION

After evaluating several open source technologies, Indigo Software approached Rohde & Schwarz to embed the DPI engine R&S®PACE 2 into its firewalls for a more refined visibility of network traffic. As a result, Indigo Software is now able to accept or deny specific application requests or commands, to detect malicious activity and to block threats by analyzing web traffic and associated formats such as HTML and Javascript.

Granular control over network traffic

R&S®PACE 2 provides strong and highly reliable detection and classification of thousands of applications and protocols by combining DPI and behavioral traffic analysis even if protocols use advanced obfuscation, port hopping techniques or encryption. With the embedded DPI technology, the Indigo Software WAF is now able to reach beyond network addresses and ports to carefully examine the entire communication between clients and web applications, making it more secure.

High performance delivered
Indigo Software was looking for a DPI solution to meet its increasing need for fast performance, high application and protocol classification accuracy as well as a DPI engine with a very low memory footprint. With R&S®PACE 2, they found an easy-to-integrate software library that operates in real time at a speed of multiple Gbps. R&S®PACE 2 also receives weekly protocol and application signature updates, which ensure that Indigo Software firewalls can rely on up-to-date classifications when filtering traffic.

Unique features of R&S®PACE 2

- Weekly signature updates
- Highest classification accuracy on the DPI market
- Metadata extraction
- Fast performance with low memory footprint
- Service and technical support tailored to the customer's individual needs
- On-demand protocol and application development

RESULT

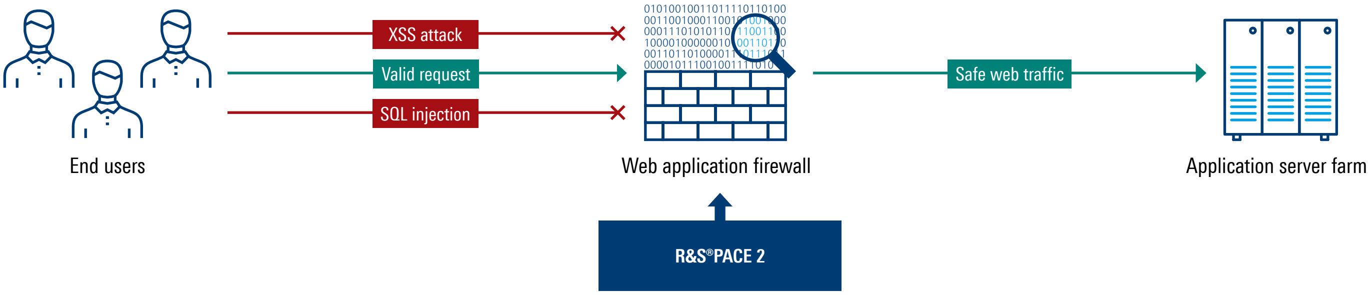
After Indigo Software integrated the DPI engine R&S®PACE 2 into its WAF, customer satisfaction increased greatly as customers instantly saw significant improvements in application performance and availability as well as a reduction in lag time. Vulnerabilities in customers' apps are now eliminated before threat actors can exploit them. Thus, data loss, application-layer DDoS, zero-day application-layer attacks and other threats are efficiently averted. Before Indigo Software deployed the new solution, an unacceptable number of false positives in previous vendors' products had made it difficult for its customers to manage and control applications within their networks. With the DPI engine's superior throughput and real-time DPI capability, customers experience no degradation of network performance.

The reliable DPI technology provided by Rohde&Schwarz also enables Indigo Software to operate in highly regulated industries and to expand its business to markets previously considered too highly policed.

By sourcing R&S®PACE 2 instead of building its own DPI, Indigo Software not only sped up its time-to-market but also reduced development time, cost and resource requirements whilst focusing on its core competencies.

> "We had evaluated open source alternatives as the core of our web application firewall, however, they did not offer the performance and reliability required for our customers. The Rohde&Schwarz DPI engine gave us what we needed – from carrier-class performance and reliability to detection of applications, protocols and even encrypted applications to excellent developer documentation and sample code."
>
> **Adam Murad, CTO at Indigo Software**

DPI-ENABLED WEB APPLICATION FIREWALL



ipoque

ipoque, a Rohde & Schwarz company, is a global leader in the world of network analytics software. We leverage our deep domain expertise to create customized software solutions that empower our customers to transform raw IP data into network intelligence. As a subsidiary of Rohde & Schwarz, we take advantage of potential synergies.

Rohde & Schwarz

The Rohde & Schwarz technology group is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test & measurement, technology systems and networks & cybersecurity. Founded more than 85 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

ipoque GmbH
Augustusplatz 9 | 04109 Leipzig
Info: + 49 (0)341 59403 0
E-Mail: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 5216.0809.52 | Version 02.00 | October 2021
White paper | Deep packet inspection for web application security
Data without tolerance limits is not binding | Subject to change