DenyAll 2015 Newsletter

Based on Web Application Firewalls Are Worth the Investment for Enterprises

February 2015

denyall

NEXT GENERATION APPLICATION SECURITY

Summary

1. Editorial

Not all organizations have invested in Web Application Firewalls (WAF) yet, but those who have clearly understand the value. Especially those who rely on DenyAll's time-tested expertise in that field. According to Gartner, "*at the end of 2018, less than 20% of enterprises will rely only on firewalls or intrusion prevention systems to protect their Web applications – down from 40% today*" (Gartner Research Note G00259365 Magic Quadrant for Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Greg Young, Joseph Feiman, 17 June 2014).

Gartner's report "*Web Application Firewalls Are Worth the Investment for Enterprises*" is excellent reading material, especially if you are unsure about the differences between WAFs and Next Generation Firewalls (NGFW) or Intrusion Prevention Systems (IPS). DenyAll is delighted to give you complimentary access to that research.

Not all WAFs were created equal. In this newsletter, we explain how we are reinventing the category and creating a Next Generation Web Application Firewall.

Following the acquisition of BeeWare, in May 2014, we are combining the innovative features of both our WAFs to build a product capable of solving the real-life problems you are encountering to protect your web-enabled IT.

Our NextGen WAF combines advanced technologies such as application discovery and testing, advanced filtering, user reputation evaluation, web single sign on and great policy management capabilities. It surpasses everything you've seen so far.

Once you're done reading, please contact us. The 600+ large and mid-size organizations who trust us never make the headline news because of data security breaches. We'd be delighted to help yours as well!

Stéphane de Saint Albin

Chief Marketing Officer

DenyAll

2. Introducing the Next Generation WAF

DenyAll Web Application Firewall redefines the industry standard.

WAFs have been around for 15 years or so. The initial filtering techniques – based on regular expression signatures and white listing – proved to be efficient at protecting early day web sites. Applications have evolved a lot since then and application security vendors have had to come up with **alternative filtering** methods and **advanced management** features, to meet the need for application availability while minimizing intrusions and false positives.

15 years later, several technologies need to be **mastered and integrated** to turn application security into a true business enabler, which meets the growing demand for automation and simplicity, combined with lower cost of ownership and greater security effectiveness.

With its application security technology portfolio and focused expertise, DenyAll is ideally positioned to bring to market the **first Next Generation WAF**, which combines the following capabilities:

- Application discovery and testing,
- Innovative filtering methods for http/https and XML traffic,
- The ability to simplify users' safe access to applications,
- An ergonomic work environment ensuring WAF administrator productivity.

DenyAll Web Application Firewall defines a new standard, because:

- It can automatically **discover** unprotected applications, **profile** them, identify their vulnerabilities and **provision** ad hoc policies, to ease the burden of administrators;

- It **learns** how applications work, identifies how attacks could be carried out and provides **guidance** to administrators on how to fine-tune the security policy;

- It uses **grammatical analysis** and **sandboxing** technologies to identify the nature of incoming requests, ahead of eventually interpreting their content using signatures and heuristics (scoring) technology, in order to **block** complex, zero day attacks and **evasion** techniques;

- It combines XML data flow routing with superior **web services security**;

- It can handle various methods of **authentication** and simplify security for users with **single sign on**, to simplify and secure access to web applications;

- It can analyze **user behavior** to identify and block abnormal activity, and it will soon be able to evaluate **user reputation** and restrict the access of likely hackers;

- It can ensure in-session **browser security** to prevent compromised devices from turning into data leakage vectors;

- Its workflow-based **visual representation of policy** provides a productive environment for administrators who need to manage applications, optimize data flows and adjust policy to every changing applications;

- It will **scale** automatically as traffic grows, using a modular architecture, APIs and cloud orchestration technology.

For more information on our Next Generation WAF, please read our white paper “Introducing the Next Generation Web Application Firewall".

3. Informations related to Gartner's report

This is DenyAll's views on some of the topics covered in Gartner's report and why you should entrust the security of your applications to DenyAll.

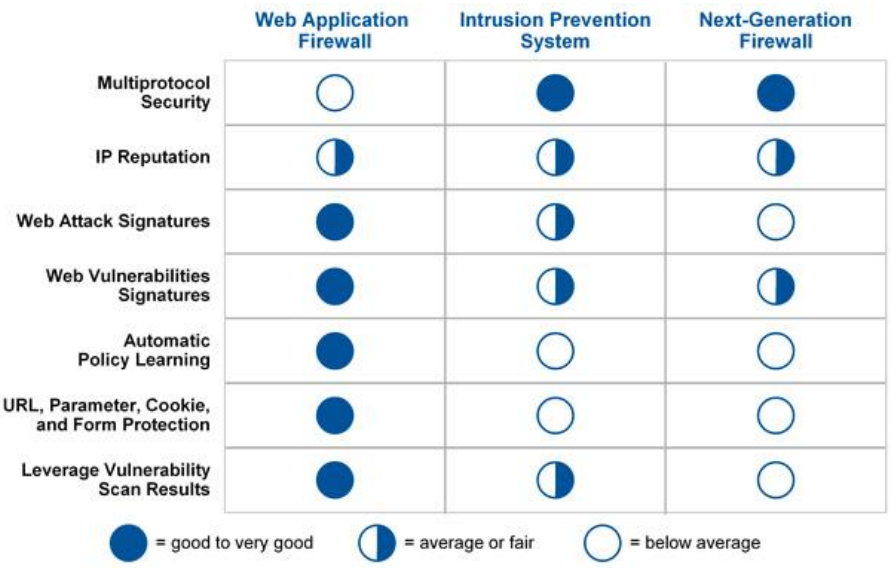
3.1 WAFs complement network security devices

In their February 2014 research note, Gartner analysts Jeremy D'Hoinne and Adam Hills did a great job at clarifying the differences between WAF and NGFW/IPS technologies, and at highlighting the complementary nature of these security controls.

They listed some of the advanced capabilities found in best-of-breed WAFs, which are required to protect modern applications from targeted attacks and evasion techniques, while reducing false positives, the archenemy of application security professionals. These include:

- Contextualized Web traffic inspection
- Automatic policy learning
- Virtual patching
- Anti-automation
- Business logic defense
- Anti-DDOS
- SSL/TLS decryption & offloading
- Web content modification
- Authentication services

The summary table below captures the most important differences.



Read the Gartner report for more details, including on how the signature-based filtering functions of basic WAFs, NGFWs and IPSs, are not up to the task of protection your applications while reducing false positives.

3.2 Applying your WAF expertise to all your applications.

WAFs have historically been deployed to secure Internet-facing applications. As the Gartner report notes, "*Enterprises tend to focus their WAF efforts on compliance or protecting public-facing custom Web applications, but often neglect equally important internal applications*" This begs the question of the scope of your application security strategy: **which applications should you place behind a WAF?**

A logical approach to answering that question is to **identify** all the web applications in your IT, **evaluate** their risk exposure and consider the business impact of any attacks on these applications and the data they serve being successful. DenyAll's experience shows that **all web applications and services eventually need to be protected**. In a web and mobile enabled world, even the smallest, most insignificant, vulnerable web application can become a vector for attackers looking to gather intelligence and eventually gain access to critical data.

Internal applications absolutely need to be placed behind a WAF. That is relatively obvious for mission critical corporate applications. Half of our customers are actually protecting SAP portals, Webmail and SharePoint environments with a DenyAll WAF. It may be less obvious but it is also true nonetheless for custom applications, including XML-based **Service Oriented Applications**, which automate the exchange of data between your organization and its business partners. Can you trust them to ensure these data feeds are free of any attack? Probably not...

Because the threat is not only external, internal applications which are not accessible outside of the corporate network also need to be put behind a WAF. If only to be able to find out what happened, after the fact, in a **forensics analysis** type of scenario, and understand how employees and other authorized users were the unwilling vectors of an attack or **misused** their access rights. Even if you're managing and attempting to secure them it is sound to assume that the devices used to connect to your internal applications are potentially compromised, as a result of users' hectic browsing habits. One should not underestimate the risk of a stealth **man-in-the-browser** malware inserting itself into an authorized session, taking place within the corporate network, stealing user credentials and finding the right opportunity to exfiltrate data.

Finally, DenyAll's experience shows that leveraging the **expertise** acquired in the process of deploying a WAF on select applications and applying it to the entire application infrastructure is a best practice which also helps improve the Total Cost of Ownership (TCO) of these tools. Indeed, the knowledge acquired in the process of protecting a selection of applications – as it refers to web languages and protocols, application structure and vulnerabilities, or the pitfalls associated with **false**

positive management – can be easily leveraged for all web applications and web services. The **scalability** of WAF technology can be leveraged to secure all Web applications from a central location.

3.3 Beyond virtual patching, towards automatic WAF provisioning.

As Gartner has been recommending for years, securing web applications will be best achieved by combining the deployment of a WAF with **application security testing** and secure coding practices. DenyAll shares that vision and integrated its Dynamic Application Security Testing (DAST) – **DenyAll Vulnerability Manager** – and WAF products to delivery virtual patching and a lot more: the tight integration actually opens the way towards **automatic WAF provisioning**, based on a better intelligence of the application environment.

DenyAll Vulnerability Manager can be used to test the security of web sites and applications already placed behind a WAF, with a view to **improving the efficiency** of the WAF's policy, tuning its setting to block potential exploits, until the vulnerabilities are actually remediated. Many vendors talk about this 'virtual patching' benefit but, because third-party technology integration rarely delivers the value it promises, few customers actually use it to date. At DenyAll, our implementation of the concept is a lot more **granular** and therefore **effective**, because we master both DAST and WAF technologies.

Beyond virtual patching, our scanner can also be used to **discover** the unprotected web applications and web services running in your network, **assess** the risks they pose and share that data with the WAF, to provision ad-hoc policies that are based on each applications' specific nature and set of vulnerabilities. By interpreting a scan report generated by DenyAll Vulnerability Manager, **DenyAll Web Application Firewalls** automatically generates policy recommendations for the soon-to-be-protected applications, which the administrator can refine and apply in just a few clicks.

As a result, DenyAll WAFs can be deployed to protect all your web applications and web services, wherever they are: within the **perimeter**, in the DMZ, or **inside** the network, closer to the internal applications that need to be protected, or in a public or private **cloud**, depending on the nature of the applications or their lifecycle phase. DenyAll WAFs are available as virtual or physical appliances. They are also available on Amazon Web Services and Microsoft Azure.

For more on this topic, please read our whitepaper "The Challenge of Securing Applications".

3.4 Securing complex web languages: why innovation is a must.

The Gartner report calls out the fact that new web languages, such as HTML5, JavaScript, JSON or PHP, while enabling the creation of **richer user experiences**, create **new risks** and tend to **confuse basic filtering engines**, opening the door to significant false positive and performance issues.

Our experience shows that traditional, linear filtering techniques, based on **regular expressions** matching (blacklist signatures), or **endless learning** phases (white listing), are not up to the task of securing modern applications. This is the reason why basic WAFs and NGFW/IPS cannot deal with todays' attacks like modern WAFs can. Effective application security requires a paradigm shift towards more **intelligent filtering**, based on identifying the **nature** of the requests, taking the **context** of users and their actions into consideration. DenyAll's Advanced Detection Engines use **grammatical analysis** to identify structured languages, such as SQL and JavaScript, in incoming requests and block these as a consequence. Some of these engines also use a **sandboxing** approach to identify command injection attacks, for example. These complement traditional signatures and DenyAll's original **scoring** technology, which can identify and block complex, zero day attacks and evasion techniques.

For more details on this topic, see our webinar series and read our whitepapers.

3.5 User Reputation: beyond IP reputation, how to identify hackers.

To prevent access rights misuse and denial of service attacks targeting applications, WAFs need to be able to detect abnormal yet legal behavior, both in real-time and after the fact, as part of a forensics analysis effort.

Building on our unique '**User Behavioral Tracking**' capabilities, which help prevent issues such as application flooding, site crawling, brute force attacks and cookie theft, we are working on a brand new '**User Reputation**' technology, which will be introduced in a future release of our NextGen WAF this year. DenyAll's User Reputation takes the concept to a new level, by combining user behavior and activity tracking over time, with user contextual data (device, geolocation, IP reputation, etc), and **hacker trapping** techniques (ala 'honeypot'), to assess the profile of users and allow administrators to make decisions based on users' trust scores.

For the time being, we are only providing details about these innovative features to customers and partners under Non-Disclosure Agreement. Please contact us if you are interested in learning more.

3.6 Application Security in the Cloud.

In the first Gartner Magic Quadrant for Web Application Firewalls[1], the analysts predict that "*by year-end 2020, more than 50% of public Web applications protected by a WAF will use WAFs delivered as a cloud service or Internet-hosted virtual appliance – up from less than 10% today*".

Organizations need to deploy application security wherever their applications and critical data live. Be it on premises, on hardware or software appliances, in a private cloud or hosted on a public IaaS platform. Be it temporarily, for scalability testing reasons, or more definitely. At DenyAll, we are investing to ensure you can deploy WAFs anywhere, anytime.

DenyAll WAFs are pre-instantiated on **Amazon** Web Services and Microsoft **Azure** today. Our NextGen WAF will also run on **OpenStack** soon. DenyAll's WAF-as-a-Service, Cloud Protector, is based on the same platform. We added automation and orchestration logic to create a fully **scalable** solution. New WAF instances are brought up and down automatically as required by the evolution of traffic. This capability is being built into our NextGen WAF, so your business applications can take full advantage of the cloud without taking unnecessary risks or sacrificing the integrity of your informational assets.

DenyAll's management console will allow administrators to centrally manage application security policy irrespective of the applications' location, be it on premises, in the datacenter of a hoster or service provider, in a private or public cloud.

3.7 Why entrust the security of your applications to DenyAll?

At DenyAll, we are application security experts and have been for 15 years. We have a solid track record of securing the mission critical web applications and web services of very demanding organizations, in all verticals (finance, energy, defense, manufacturing, services, government, etc). Unlike our competitors, whose core know-how is securing networks and balancing traffic, our own art is application security. If our 600+ customers make the news headlines, it's certainly not because of security breaches: we help prevent them! We have a passion for customer satisfaction and are very close to our customers and partners, adjusting to their needs quickly and in creative ways. We are innovators. We are driven by a vision of how application security needs to get simpler and more efficient, to enable safe access, communications and transactions. Give us a try!

[1] *Gartner Research Note G00259365 Magic Quadrant for Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Greg Young, Joseph Feiman, 17 June 2014*

denyall

NEXT GENERATION APPLICATION SECURITY

Germany

An der Welle 4
D-60322 Frankfurt
Deutschland

Tel: +49 (0)6233 66 75 39
Fax : +49 (0)6975 93 82 00

Montpellier

501 rue Denis Papin
34000 Montpellier
France

Tel: +33 (0)1 46 20 96 01

Headquarter

6 avenue de la Cristallerie
92310 Sèvres
France

Tel : +33 (0)1 46 20 96 00
Fax : +33 (0)1 46 20 96 02

Email : info@denyall.com

www.denyall.com