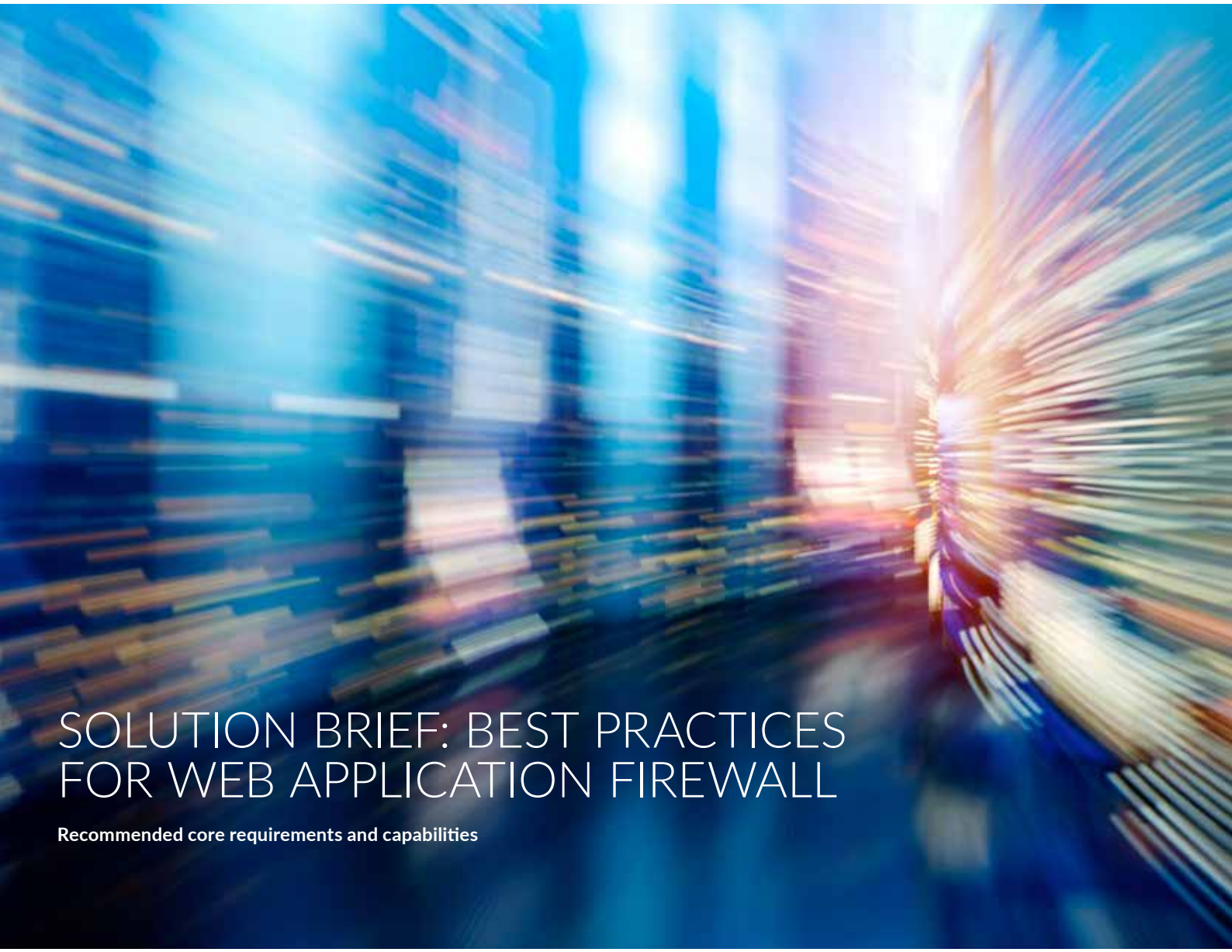
SONICWALL®



SOLUTION BRIEF: BEST PRACTICES FOR WEB APPLICATION FIREWALL

Recommended core requirements and capabilities

Abstract

The ideal WAF solution requires a comprehensive foundation for application security, data leak prevention, performance and management. This brief explores:

- Recommended core requirements
- Best-practice capabilities to consider

Introduction

Because most web servers remain vulnerable to a wide spectrum of web-based exploits on a daily basis, organizations need a dynamic web application firewall (WAF) to provide continuous real-time protection for web properties, whether they are hosted on-premises or in the public cloud. Regulations for safe data exchange over the Internet demand IT to employ a WAF solution that can prevent data theft while meeting various web security regulatory compliance and audit requirements.

Recommended core requirements

The ideal WAF solution requires a comprehensive foundation for application security, data leak prevention, performance and management:

Application Security

An effective WAF must protect against the latest web attacks that focus on leveraging the top ten vulnerabilities for web applications as defined by the Open Web Application Security Project (OWASP)[1].

A WAF should intelligently detect and alert on anomalies in web behavior, by understanding web application logic beyond just protocol behavior, and interrogating the behavior and logic of what is requested and returned within web communication. Full management and control of application traffic can decrease the attack surface. This includes forbidding invalidated redirects that send victims to unsafe webpage and unauthorized page forward to restricted pages.

A WAF requires strong session management and authentication capabilities to enhance the authorization requirements such as One-Time Password, Two-factor Authentication, Single Sign-On, and client certificate authentication. Plus, the WAF should protect against known and zero-day vulnerabilities with automated virtual patching and custom rules.

Data Leak Prevention

A WAF should stop attackers from performing malicious actions such as spreading malware, executing operating system commands, browsing the file system on the web server, and initiating a connect-back shell session. It should also prevent theft of PCI compliance data such as credit card numbers and tax IDs.

Best practices also recommend that a WAF must be able to block brute-force attacks from acquiring authentication credential such as usernames and passwords. It needs to bar attackers from gaining full access to users' accounts and all accounts in the system. In addition, it needs to obstruct attackers from gaining full control of web applications and connecting to associated database(s), and restrict access to internal resources based on host, subnet, protocol, URL path, and port with comprehensive access security controls.

Performance

Optimally, the WAF should deliver web applications to users safely and reliably without disruption. It must preserve web servers' integrity and uptime with robust defense mechanisms against all types of DoS/DDoS attacks, including protocol and application layer attacks.

A robust WAF should also maintain system performance and elasticity with built-in application delivery capabilities. These should enable application-aware load balancing, SSL offloading, content caching, compression and connection multiplexing and acceleration, for resilience and an enhanced digital experience.

Management

The WAF solution should give administrators complete traffic visualization, analytic and reporting tools for making well-informed security policy decisions. It needs to have a streamlined dashboard that provides an easy-to-use, web-based management interface, featuring a status page overview of all monitoring and blocking activities. These include signature database status information and threats detected and prevented.

Best-practice capabilities to consider

To attain these goals, a best-practices WAF solution requires feature-rich web security tools and services to keep web properties safe, undisrupted and in peak performance every single day. When selecting a WAF solution, evaluate whether it provides the following feature sets.

1. **Defense against the OSWAP Top 10 web vulnerabilities**
   Provide anti-evasive protection against the latest web attacks that focus on leveraging the Top 10 vulnerabilities for web applications as defined by the Open Web Application Security Project (OWASP).
2. **Session management controls**
   Offer strong session management and authentication capabilities to enhance the authorization requirements such One-Time Password, Two-factor Authentication, Single Sign-On, and client certificate authentication.
3. **Web form input validation**
   Inspect and validate client requests for possible malicious code to protect the backend servers from transactions that could allow hackers to bypass security defenses.
4. **Session hijacking monitoring**
   Detect eavesdropping, intrusion and even theft of a web sessions to help prevent malicious actions taken by the attacker.
5. **Perfect Forward Secrecy (PFS) prevention**
   Protect past sessions against future compromises of secret keys or passwords.
6. **Cross-Site Request Forgery (CSRF) attack denial**
   Recognize and prohibit malicious websites from sending illegitimate requests to a web application that a user is already authenticated against from a different website.
7. **Block code injection or remote code-inclusion attacks**
   Identify and disrupt attacks that exploit a web application's interface to the underlying operating system and results in the unwanted execution of arbitrary code or harmful commands, such as downloading a malicious payload.

[1] https://www.owasp.org/index.php/Top_10-2017_Top_10

8. **Data Loss Prevention (DLP)**
Ensure that compliance data such as credit card numbers, tax IDs, and credentials are not leaked within web pages.

9. **Dynamic application profiling**
Enable the administrator to generate custom rules in an automated manner based on a trusted set of inputs. It should then enable the administrator to develop a profile of what inputs are acceptable by the application while everything else is denied, providing positive security enforcement.

10. **Cookie tampering protection and encryption**
Protect against cookie theft, poisoning, inaccuracies, and cross-site cookie tampering via encryption and exclusion.

11. **Offloaded web application protection**
Protect an offloaded web application (a special-purpose web app created to provide seamless access to a web application running on a server).

12. **Rate limiting for custom rules**
Track the rate at which a custom rule, or rule chain, is being matched to block dictionary attacks or brute force attacks.

13. **Compliance with industry and government regulations**
Satisfy PCI DSS Requirements 6.5 and 6.6 addressing application code vulnerabilities.

14. **Botnet detection and application layer DDoS protection**
Protect against flood attacks that can degrade, disrupt or crash the web server.

15. **Web server fingerprint protection**
Defend against web server fingerprinting attacks that identify web application software, its version and the platform that help hackers exploit vulnerabilities reported in the software.

16. **Web services/API protection**
Prevent exposure of the valuable information contain within web services and APIs.

17. **CMS platform protection**
Use custom rules with virtual patching to neutralize new vulnerabilities found in popular CMS tools, such as WordPress, Joomla, and Documentum.

18. **Web Application delivery control**
Provide application session management, load-balancing and web application acceleration with SSL/TLS support that ensures negligible impact to a legitimate user's digital experience, while provide advanced protection for the web application.

19. **Flexible deployment options**
Be deployable as a virtual appliance in private clouds based on VMWare or Microsoft Hyper-V; or in AWS or Microsoft Azure public cloud environments.

Conclusion

Today's businesses need a WAF solution that meets best practices to protect their public and internal web properties.

Learn more about SonicWall Web Application Firewall at www.sonicwall.com/web-application-firewall.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com