DPtech WAF3000
Web Application Firewall

Product Brochure
WAF3000 Series

杭州迪普科技股份有限公司

Overview

The rocketing development of IT technology and network applications has spawned a growing number of Web-based applications in terms of types and quantities. A variety of attacks, such as SQL injection, cross-site scripting, and webpage Trojan, pose tremendous threats to Web applications, while raising higher requirements for the protection capabilities of Web application firewalls.

DPtech's WAF3000 Series Web Application Firewall is designed to provide comprehensive security protection for web applications. It is capable of fully protecting web applications by implementing pertinent protection policies for scanning before attacks, in-process attacks, and page tampering and information theft after attacks. In this way, it helps users address Web application threats with ease.

Product Features

- **Web Vulnerability Scanning Protection**

Behavior and fingerprint detection technologies are adopted to effectively detect the scanning behavior and the fingerprints of scanning tools before hacking. In addition, to prevent hackers from collecting Web server information for further Web attacks, a series of protection methods for sensitive information have been put in place, including hidden server version information, server response status code masking, and leakage protection for website directories, source code, and database information, thus cutting off attacks at the source.

- **Accurate Detection of Webshell**

The original Webshell risk engine allows risk assignment to key functions. When the threshold is reached, it is identified as a Webshell risk and an alarm or blocking action is triggered. Compared with traditional file suffix-based detection, Webshell detection can reduce false negatives effectively and increase accuracy.

- **Smart Generation of Policies**

Interactions with vulnerability scanning help generate reports on Web vulnerability scanning and import them into WAF, automatically generating policies. In addition, it supports website self-learning and automatic site detection. Through automatic learning about the protected websites, whitelist policies are established and automatic optimization of the objects specified by the protection policies is realized.

- **Geo-location Access Control**

It provides access control based on geographic location, either at a province in China or in a specific foreign country. As requested by users, it is possible to block overseas addresses or

certain regional addresses from accessing websites, effectively eliminating website attacks from overseas addresses during major conferences.

- **Smart Status Monitoring**

It can monitor CPU usage, memory usage, concurrent connections, new connections and other states in real time through smart status monitoring. When the threshold is reached, an alarm is issued and the forwarding mode is trigged to ensure the device is working properly and the network will not be paralyzed due to overload.

- **Strategy Tuning Services**

In order to strengthen the adaptability of equipment strategies to business scenarios, DPtech provides users with strategy tuning services: DP first-line after-sales personnel go to the user's site to collect device-related security logs and submit them to headquarters security experts to analyze the logs. The user's current network situation gives corresponding strategy optimization suggestions, and at the same time, the after-sales personnel will assist the user to complete the specific strategy optimization operation to enhance the user's sense of product experience.

Product Series

WAF3000-Blade-AI

WAF3000-TS-A

WAF3000-ME-X

WAF3000-GC-X

WAF3000-GE-X

WAF3000-TM-X

Function Descriptions

Product Functions	Function Descriptions
Web Scanning Protection	Behavior and fingerprint detection technologies are adopted to accurately detect any possible Web scanning behavior.
Web Attack Protection	Effective protection against various web attacks is enabled, such as SQL injection, cross-site scripting, session hijacking, etc.
Accurate Detection of Webshell	Webshell risk engine facilitates accurate detection of Webshell uploads and connections.
Hide Sensitive Data	A series of protection methods for sensitive information have been put in place, including hidden server version information, server response status code masking, and leakage protection for website directories, source code, database information, and account

	information (bank card numbers and ID card numbers).
Geo-location-based Access Control	Geo-location-based access control is activated to keep control of access at either a province in China or in a specific foreign country.
Webpage Tamper-proof	It prevents webpage parameters from malicious tampering, effectively guaranteeing data security and integrity during interactions. A tamper-proof whitelist is established, based on which users can configure policies as needed and implement an organic combination of dynamic and static tamper-proof policies.
Web-layer DDoS Protection	It supports denial of service attack defense (DDoS) against application-layer DDoS attacks, such as CC attacks, slow DDoS, etc.
Reinforced HTTP Protocol	Reinforced HTTP Protocol is available, including non-standard protocol filtering, Cookie normalization and buffer overflow protection
Web Application Optimization	Web application optimization includes server load balancing, web acceleration, and SSL offload.
Smart Mode	It can monitor CPU usage, memory usage, concurrent connections, new connections and other states in real time. When the threshold is reached, an alarm is issued and the forwarding mode is trigged.
Website Self-learning	Website self-learning function enables learning of website directory structure, website content, request frequency, cookies and other information, creating whitelist policies.
Automatic Site Detection	Automatic site detection function supports learning the hit policy after it is generated, and automatically adding newly learned port, IP address, and URL address into the policy.
Interactions with Vulnerability Scanning	Interactions with vulnerability scanning products help generate reports on Web vulnerability scanning and import them into WAF, automatically generating policies.
Graphic Management	A user friendly graphical management interface, which supports Web GUI, SSH and serial console. Centralized management through UMC network management is also made possible.
Logs and Reports	An independent log server is provided, on which regular automatic backups can be performed. With its built-in multi-dimensional reports, functions such as graphic inquiry, audit, statistics and retrieval of various network behavior logs on the intranet are enabled to facilitate the management in understanding and controlling the network. A number of visualized reports incorporating multiple metrics, including time, attack, and business system, are available.
High Reliability	Equipped with a multiple guarantee mechanism of high reliability, it supports key component redundancy and hot-plug, application of Bypass and PFP Power Fail Safeguards, and dual-system hot standby. Truly seamless switching is thus enabled to guarantee highly stable and reliable Network Security operations.
Deployments	It supports deployments in transparent mode, reverse proxy, and side by side mode.

Hangzhou DPtech Technologies Co., Ltd.

Address：6th Floor, Zhongcai Building, No. 68 Tonghe Road, Binjiang District, Hangzhou City, Zhejiang Province

Postcode：310051

Official Website：*www.dptech.com*

Service Hotline：400-6100-598