Technical White Paper on Web Application Firewall

Keywords: Server, WAF, Gateway, HTTP

Abstract: This White Paper introduces the application background of WAF technology, its implementation and operation mechanism of WAF, and its application scenarios.

Abbreviations:

Abbreviations	Full Name in English
WAF	Web Application Firewall
HTTP	HyperText Transfer Protocol
XSS(CSS)	Cross Site Script
SQL	Structured Query Language

CONTENTS

1 Overview

1.1 Web Security Status

In the World Wide Web (www, or commonly known as the Web) age, the Web service platform has become a pillar of information-based development, on which many enterprises have built service applications. While facilitating enterprises and users, the Web application platforms also put the enterprise's service systems under severe challenges. The diversification of service systems and the rapid development of the Internet draw great attention from network enthusiasts and hackers, who have gradually shifted their focus of attack from traditional Web servers to Web services, leading to a rapid increase in the potential threats of Web application platforms.

The recent years saw numerous network enthusiasts and hackers launched attacks on Web services for various purposes. In the meanwhile, a huge number of attacks launched by hackers by exploiting Web security vulnerabilities have affected government websites, Tieba, and online communities in China, causing great inconvenience to the business of enterprises and individuals at all levels.

1.2 Web Application Firewall

Web Application Firewall is launched in response to the rising number of Web security issues. In a broad sense, Web Application Firewall is designed to improve the security of Web applications. Generally deployed at hardware and devices, Web application protection is built on the front end of the Web application platforms, acting as a reliable security guard for the Web application platforms.

In summary, Web Application Firewall should feature the following advantages:

1）Audit: Audit and count the number of HTTP packets and sessions passing through the device, analyze the problems and put forward analysis reports;

2）Access Control: Perform access control on Web application platform, including active access control and passive access;

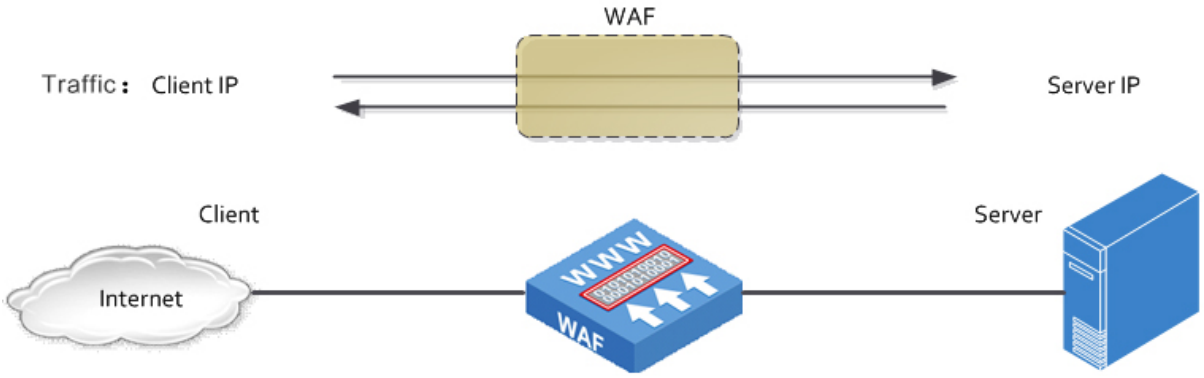
3） Network Management: Functions such as reverse proxy mode, forwarding control, and diagnostic tools are available;

4）Web Attack Protection: As the core function of Web Application Firewall, it provides security protection for Web application platforms to prevent unnecessary losses to the application platforms caused by attacks.

2 Deployments

2.1Transparent Mode

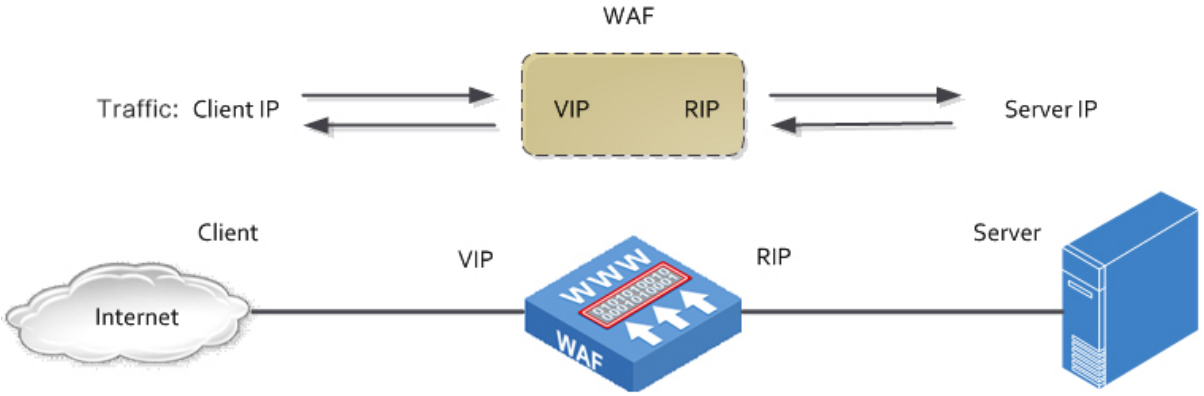
As shown in the figure, in Transparent Mode, the uplink and downlink configurations of WAF device will remain unchanged, i.e., between two running devices. As there is no need to adjust the existing network structure in Transparent mode, plug-and-play deployment can be realized.



Deployment features: Fast, easy and plug-and-play. Deployment before configuration.

2.2 Reverse Proxy Mode

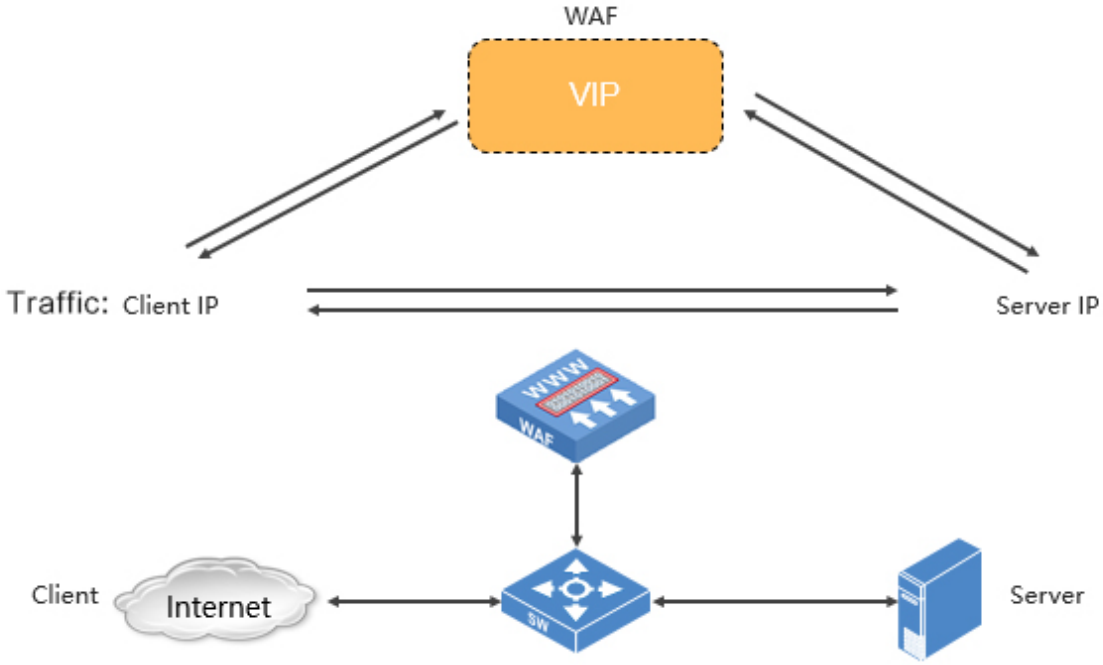
As shown in the figure, in the Reverse proxy mode, WAF device is deployed in the network backbone, and the client accesses to the back-end server using virtual IP as a proxy.



Deployment features: Network deployment structure needs to be planned in advance; functions available include load balancing.

2.3 Bypass Mode

As shown in the figure, in Bypass mode, the WAF device is connected side by side to the router, rather than acting as router between the back-end server and the client.



Deployment features: Seamless connection with the original services without changing the existing network topology; optimized services include load balancing and others.

3 Comprehensive Web Protection

3.1 Protection against Parameter Attacks

Injection attacks and XSS (Cross Site Script), both of which are closely related to HTTP request parameters, are listed as the first two risks in the “Top Ten Web Application Security Risks" released by OWASP. It sheds the light on the importance of parameter attack protection.

3.1.1 Protection against SQL Injection

SQL Injection is generally caused by the lack of application verification of the input data. Hackers generally send a piece of data containing SQL statements to the parser, which then restores the data to a command for execution. SQL Injection attacks usually lead to catastrophic consequences. All information in the entire database can be read or tampered, and access rights of even the administrator can be obtained. Usually, attackers look for SQL

injection vulnerability, determine the type of the back-end database, and obtain the relevant permissions to carry out dangerous attacks. DPtech WAF3000 provides a signature library of SQL injections, which includes injection point search, surmise of database type and permission structures, addition of new database users and system users, addition of permissions, surmise of data table structure, backup database, directory traversal, WEBSHELL upload and backup of logs. In practice, attack payload can be found in anywhere in the HTTP request, such as request string, POST data, cookie, custom or standard HTTP header, and part of the URL. DPtech enables detection of potential threats in the above locations. When an attack packet passes through the device, the system will match potential threats with the signature library. If packet is found to contain attack signatures, it will be block upon an alarm to prevent malicious requests for data tampering. The defense work is mainly carried out in the following aspects:

1）Construct dynamic SQL statements based on dynamic strings. We replace the original dynamic query statements with parameterized statements, which not only provides effective protection, but also improve the efficiency compared to modern databases;.

2） We conduct input validation to make sure its compliance with the standard process defined in the application. Validation applies to simple scenarios of taking parameter values as a data type or complex ones with regular expressions or business logic for verification. In response, we have whitelists (positive verification) and blacklists (negative verification) in place. For simple or confirmed attack statements, we use blacklist matching. For complex and potentially threatening statements, we determine whether it is a security statement by analyzing its grammar and morphology. By grammar and morphology, we are referring to the database grammar and morphology that are relatively outdated but still in use compared with new data;

3） Encode the output query statements: We performed different encoding processes for different databases to change potentially threatening codes into a part of other security codes, thus effectively preventing malicious users from exploiting SQL Injection vulnerability in specific queries;

4. We perform normalization on input encoding or multiple encoding statements. As it is impossible to refuse to receive any input containing encoded format in practice, we look for diversified encoding methods for different codes and perform one or more encodings on these statements. To eliminate any possible errors easily found in this method, we compile a great number of functions and algorithms to decode and get a final format for analysis, thus determining its security status;

3.1.2 Protection against XSS

XSS occurs when a user accesses a Web page, to which a hacker has added a piece of malicious HTML code, or triggers an event, the HTML code embedded in the Web page is called to assist the hacker in attacking. DPtech-WAF3000 builds a signature library for these attacks, which includes script keywords, tag keywords, event keywords and other signatures. We also stipulate relevant regular expressions, which decode the data submitted by the user and convert irregular characters therein to get desired formats. Then we detect the converted data, match its signatures and regular expressions, and block any request containing malicious codes or scripts. Meanwhile, we encode the data output to the Web page to disable malicious codes.

3.1.3 Protection against Command Injection

The rapid development of Web server platforms allows us to make any necessary interactions with the server's operating system using the built-in API. If used properly, these APIs can help developers access file systems, connect to other processes, and establish secure network communication. However, sometimes developers send operating system commands directly to the server. If the input command submitted by users is transmitted to the operating system, it may be subject to command injection attacks, allowing the attackers to submit specially designed inputs and modify the developer's execution commands. DPtech WAF3000 designs a large number of functions to address this issue. By searching for and matching various operating system commands and common deformation conventions, it effectively prevents command injection attacks by restricting the length of system parameters and blocking the meta characters.

3.1.4 Directory Traversal Attack

There are many Web functions that force applications to read or write data to the file system. To operate in such a potentially threatening way, hackers specially design and provide such functions so as to access security and private files set by developers, which is known as directory traversal vulnerabilities. By exploiting these vulnerabilities, hackers can initiate a series of threatening behaviors, such as reading a great amount of security information or meaningful but hidden information, and tampering with user or server information. DPtech WAF3000 is provided with a complete signature library and sophisticated algorithm analysis. Based on intelligent analysis, it determines whether the input statements contain dangers or potential threats. If yes, it further confirms their risk levels through signature matching and protocol matching. If it is found that the statements are initiating abnormal requests to access a directory, the malicious access will be blocked and protected.

3.2 Protection against Parameter Tampering

Protect the parameters of the signatures under the URL corresponding to the domain name

DPtech WAF3000 supports double protocols of signatures and parameters and specifies the range of value. By checking if the parameters corresponding to the specific features in the client packets fall within the specified range, it prevents the client from entering illegal parameter values, thereby greatly reducing the possibility of introducing potentially dangerous requests through parameters.

3.3 Protection against HTTP Protocol Attack

3.3.1 Normalization check of HTTP requests

In the constantly emerging attacks, hackers exploit protocol blind spots and launch malicious attacks through splitting and other techniques. In response, DPtech WAF3000 performs normalization verification on HTTP requests (GET, POST, PUT, OPTIONS and Custom)， its versions (HTTP/1.1, HTTP/1.0, HTTP/0.9), and protocol formats. It provides protection for packets beyond the scope of normalization, eliminating malicious attacks launched through protocol blind spots, such as splitting.

It can impose limitations on the overall length of URL according to the type of services, effective preventing server parsing load caused by malformed URLs. Limitations can also be set to protocol attributes, such as the total number, total length, parameter name, and the length of parameter values of URL requests.

3.3.2 Cookie Normalization Check

The emergence and popularization of Cookie makes it a new target of hackers. Abnormal information is added to the Cookie to modify its original values, preventing the server from using the Cookie. It is beyond doubt that such attacks will cause great trouble to the users. Therefore, DPtech WAF3000 verifies the Cookie of requests to prevent malformed Cookie from stealing the users' private information or misleading the server to make wrong judgments.

3.3.3 Request Header Normalization

With the development of information technology, each field of the header has gradually put into various applications, thus making the header field a vulnerability prone to be exploited by hackers. For instance, attacks against Referer can be used to forge and launch other types of attacks on systems originating from statistical sites. DPtech WAF3000 provides 9 custom normalization rules for normalization rules of common header domains, and is capable of performing normalization control on each field in the request header domain through up to 32 custom normalization rules. Normalization is also available for the number and length of the

header fields, which helps normalize escape attempts caused by header fields with abnormal lengths.

3.3.4 Cookie Encryption

The Cookie in the client packets sent by the server generally stores the session value generated internally. This value is the key that determines the direct connection between the client and the server, and shall not be tampered by the client or malicious user. Malicious tampering will lead to security and privacy information leakage and unnecessary losses to customers and servers. DPtech WAF3000 summarizes and encrypts the Cookie valve using the set-cookie field of the response packet. Users are not allowed to view or modify the Cookie when it passes through the httponly. The encrypted Cookie is returned to the client to prevent the latter from making any modifications. Replay the Cookie exploited by malicious users and make careful analysis on Cookie tampering to prohibit them from accessing the server. In this way, protection against related dangers is enabled.

3.3.5 HTTPS Offload

HTTP offload refers to the HTTPS services provided by DPtech WAF3000 in the external network. After checking the attacks (HTTPS detection is basically similar to the HTTP detection, only the HTTPS encryption protocol is decrypted), a session is established with the final server. This is conducive to effective reduction of server loads.

Meanwhile, HTTPS attacks are filtered to avoid attacks and damages to the security of the server caused by exploiting HTTPS vulnerabilities.

3.3.6 HTTPS Load

On the contrary of HTTPS offload, HTTP load refers to the HTTP services provided by DPtech WAF3000 in the external network. After checking the attacks, an HTTPS session is established with the final server. It is applicable to scenarios where there is a trusted link between the client and the WAF, but an untrusted link between the WAF and the server.

Meanwhile, HTTPS attacks are filtered to avoid attacks and damages to the security of the server caused by exploiting HTTPS vulnerabilities.

3.3.7 HTTPS Two-way Loading and Offloading

HTTPS two-way loading and offloading is a combination of the two methods mentioned above. DPtech WAF3000 provides HTTPS services in external network, performs attack detection at the HTTPS protocol layer to decrypt it into HTTP protocol, and continues the attack detection at the HTTP protocol layer. Finally, after the checking the attacks, it encapsulates the HPPT protocol data into HTTPS data by using HTTPS protocol shaping before sending it to the final server.

3.4 Protection against Buffer Overflow

Buffer Overflow attack refers to destructive results occurring to the running programs or systems by exploiting buffer vulnerabilities. Usually, the length of input data shall not exceed the length of the buffer. However, a majority of programs consider the data length is consistent with the applied space size, which provides a condition of traversal of overflow attacks. DPtech WAF3000 performs two-way detection of HTTP request lines and headers and keeps Web server in proper operation through

3.5 Protection against Website Directory Scanning

Some website directory scanning software initiates a request link to the server through a built-in or self-filled common path, analyzes the packet returned by the server, and judges whether the directory exists to get prepared for the launching upcoming harms. DPtech WAF3000 is provided with a sound directory dictionary which is subject to regular updates. It limits the frequency of content in the request directory dictionary through the built-in high-precision algorithm to effectively protecting the defense server directory from being scanned by hackers.

3.6 Protection against Weak Passwords and Brute Force

It happens when the user name and password of the administrator are stolen by the hacker in the back-end management, which allows the hacker's operation of the server without being identified as illegal actions by the server. DPtech WAF3000 tests the user's password through the built-in scoring algorithm. When the score is lower than the threshold, the password is identified as a weak password, and the user will be notified promptly to timely modify the password, making it more difficult to launch attacks.

DPtech WAF3000 calculates and counts the login request frequency through a precise algorithm to analyze whether there is brute force of the username and password, ensuring prompt and proper protection and preventing the username from brute force attacks.

If username and password are accidentally leaked, the attackers can still find no way to launch an attack with the back-end administrator account as they cannot obtain the second authentication password set in DPtech WAF3000.

3.7 Application-layer Anti-DDoS

DDoS is short for Denial of Service attack. Attacks of the sources as well as the server are called DDoS attacks. Application layer DDoS is special that it provides effective protection against DDoS through restricting the HTTP requests. DPtech WAF3000 provides protection against SYN flood, HTTP flood, XML DOS and other common DoS attacks. With a fast and accurate algorithm, the device calculates the times of source attacks within a specified time

period. If the threshold is exceeded, the attack sources will be blocked. We are capable of efficiently calculating the threshold with a set of professional algorithms, thus providing real-time protection against application-layer DOS attacks.

3.8 Protection of Multiple Policies

DPtech WAF3000 supports protection of multiple policies by setting up multiple blacklists and whitelists to effectively avoid a large number of attacks.

3.8.1 URL Blacklist and Whitelist Protection

URL blacklist and whitelist mechanism provide strict restrictions on the range of server paths, enabling reliable and effective protection for important Web pages.

3.8.2 usr-agent Blacklist and Whitelist Protection

It determines whether a user request is illegal or not by looking for matched user information fields and blocking illegal user requests promptly to guarantee the security the website server.

3.8.3 Granular Configuration and Protection of User Requests

DPtech WAF3000 supports protection for request methods, protocol versions, parameter range and length, request header length, and submitted data length. It enables normalization restrictions on request URL parameters through regular expressions in the protocol. By checking the header domain and the header itself, it places strict restrictions on the pre-defined and custom length of the header, the maximum number of header domains, the length of header, and the length of request and response. Through these granular configuration, it can effectively track all kinds of attacks and provide effective protections.

3.8.4 Blacklist Linkage

DPtech WAF3000 makes statistical analysis on the blocking frequency of source IP address requests and includes source IP addresses that exceed the set threshold on the blacklist. In this way, the blacklist is constantly updated automatically, which help more effectively to block any potential attacks on the Web server.

3.9 Sensitive Keyword Filtering and Server Information Protection

3.9.1 Illegal keyword filtering

Thanks to policy configuration, DPtech WAF3000 effectively hides or blocks sensitive keywords contained in user submitted information or web pages. Through matching the above information by using regular expression, it provides users with easy to use methods to prevent posting of illegal content.

3.9.2 Intelligent filtering of crawlers

Network crawlers are growing dramatically in size due to the rapid development of Web services, consuming large amounts of server resources and bringing down the speed of server. By performing classified blocking of the crawlers, DPtech WAF3000 discards unwanted crawlers to prevent them from consuming huge server resources.

3.9.3 Sensitive information protection of server

There are a large number of sniffing attacks in the network which, though may not directly affect the server, might be exploited by attackers to launch traversal attacks as they provide important information returned by the server. DPtech WAF3000 can effectively filter the basic information contained in the client packets returned by the server, such as the server version number and application type, thus preventing the hackers to launch subsequent attacks by exploiting such information.

3.9.4 Server error message replacement

To prevent sniffing attacks, DPtech WAF3000 performs filtering on the returned server error information, hides or discards the information related to server security and returns it to the client, effectively preventing attackers from collecting server error information and achieving "prior" protection against attacks.

3.9.5 Key files protection

Files with security and privacy information are often stored in servers. Although such files are strictly confidential, servers rarely provide protection for them. DPtech WAF3000 can block access and download requests involving such key files using algorithms. In this way, it prevents hackers from analyzing server vulnerabilities or stealing user information by collecting server residual test scripts, directory files, obsolete databases, etc.

3.9.6 Malicious file upload protection

Nowadays, a large number of website forums allow their users to upload files, which is dangerous but necessary. Through careful examination of uploaded files and accurate dictionary matching, DPtech WAF3000 effectively prevents hackers from uploading Trojan horses and viruses and conducting other malicious acts by bypassing authentication and other restrictions.

3.9.7 Protection against CSRF

CSRF refers to Cross-Site Request Forgery. The attack is extremely harmful. It forges a request packet in the name of the victim and sends it to the attacked object, thus capable of performing relevant operations available only to specified permissions without actually

receiving the permission. Based on careful algorithms, DPtech WAF3000 analyzes and processes the specific fields of the request packets of the access protection page to determine whether the guest is launching an attack by forging his identity. If yes, the request will be blocked to provide protection.

4 Load Balancing

DPtech WAF3000 provides the following abundant load balancing functions:

- Support multiple load balancing scheduling algorithms
- Support diversified health check methods
- Support continuity function
- Support L4~7 load balancing

5 Session Management

Session Number Limits

With session identification and counting technology, DPtech WAF3000 provides the following protection for the IP addresses for specific purposes:

- Limit of sessions per IP connection
- Limit of concurrent sessions per second
- Limit of new connections per second

6 Web page Tamper-proof

6.1 Web page Tamper-proof

For many enterprises and departments, there are some crucial web pages that do not require frequent changes. To this end, DPtech WAF3000 is designed with the web page tamper-proof function, which protects crucial web pages from being tampered while ensuring proper access through efficient implementations. Once the device detects any changes of web pages, either normal or malicious, it will send the original content to the client and issue an alarm. In this way, the user can perform validity checks on the changes to confirm whether it has been tampered with maliciously. If it is found that there is malicious tampering, the original content can be restored in time. If changes are made as needed by the developers, this web page can be updated through the device. Therefore, it effectively protects web page tampering. Traditional tamper-proof works by enabling caching on the device and comparing fingerprints

of the request page with the cache page, so as to determine whether the web page has been tampered with. For pages that are subject to constant updates, manual refreshing is required, adding to the workload of network administrators and affecting the timeliness of information acquisition due to the time interval between refresh operations. WAF3000 Tamper-proof adopts a whitelist mechanism to include content that is allowed to be changed to the whitelist policy. When the Web page changes, the device will determine whether the content changes are contained in the dynamic tags of the white list. If yes, the device cache will be automatically refreshed.

6.2 Web page Tampering Recovery

DPtech WAF3000 provides protection for the website's overall directory. Through interactions with the server, the website's overall directory structure and contents are obtained. Efficient and accurate algorithms are used to learn and memorize relevant contents, and protection is carried out as needed by the users. If the website directory or file changes abnormally, an alarm will be generated and the original directory structure and file content will be restored within the specified time. For necessary modifications made by the developers, the issue of mistaken attacks can be addressed by updating the protected objects in time. In this way, secure and reliable protection for the overall directory information is realized.