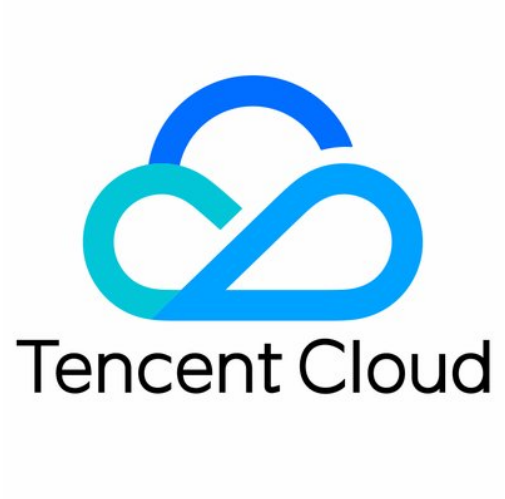
Web Application Firewall

Product Intro

Product Introduction



Contents

Product Intro
Overview

Last updated：2018-06-22 14:39:20

What Is WAF?

Tencent Cloud Web Application Firewall (WAF) is an AI-based one-stop protection solution against Web business operation risks. With strong security and big data capabilities and 19 years of Web security protection experience of Tencent, WAF provides effective security guarantee for websites.
Tencent Cloud WAF can effectively prevent SQL injection, cross-site scripting (XSS), trojan upload, unauthorized access and other OWASP attacks. In addition, it can provide all-round protection for website systems and businesses by effectively filtering CC attacks, detecting DNS linkage hijacking, providing zero-day vulnerability patches, and preventing webpage tampering.

Key Features

Feature	Description
AI+Web application firewall	With the Web attack identification based on AI+ rules, anti-bypass, low false negative and low false positive, it can precisely and effectively defend against common Web attacks, such as SQL injection, unauthorized access, XSS, cross-site request forgery (CSRF), Webshell trojan upload and other Top 10 Web security threats and attacks defined by OWASP.
Virtual patching for zero-day vulnerabilities	Tencent security team provides 24/7 monitoring to uncover vulnerabilities and make responses. It will issue virtual patches for high-risk Web vulnerabilities and zero-day vulnerabilities within 24 hours upon detection, and protected users can obtain the defense capability against emergency vulnerability and zero-day vulnerability attacks without performing any operation. The response cycle is greatly shortened.
Webpage tamper resistance	You can set it to back up core webpage contents to the cloud, and publish the backed up webpage contents to achieve webpage substitution, thus avoiding adverse impacts on your organization caused by webpage tampering.

Feature	Description
Data leakage prevention	It can prevent backend databases from being hacked by means of ex-ante server application hiding, real-time intrusion protection, and ex-post sensitive data replacement and hiding policies.
CC attack defense	Multi-dimensionally custom precise access control in combination with human-machine identification and frequency control can effectively filter junk access and mitigate CC attacks.
Crawler bot behavior management	The webpage crawler and bot management based on the AI+ rules repository can help enterprises mitigate business risks, such as website user data leakage, content infringement, competitive pricing, inventory query, black hat SEO and business strategy disclosure, caused by malicious BOT behaviors.
DNS illegal hijacking detection	It performs nationwide DNS verification on domain names submitted by users, perceives and displays the hijacking details of the protected domain names in each region, to help enterprises avoid data interception and financial loss caused by website users being maliciously hijacked.
30-line BGP IP access protection	Tencent Cloud WAF supports exclusive 30-line BGP IP linkage access for defense nodes. The nodes are scheduled intelligently, which effectively solves the access delay problem and ensures the site access speed of users in all tiers of cities, thus achieving the unaware cloud WAF security protection deployment without affecting the website access speed.

Why Is WAF Necessary?

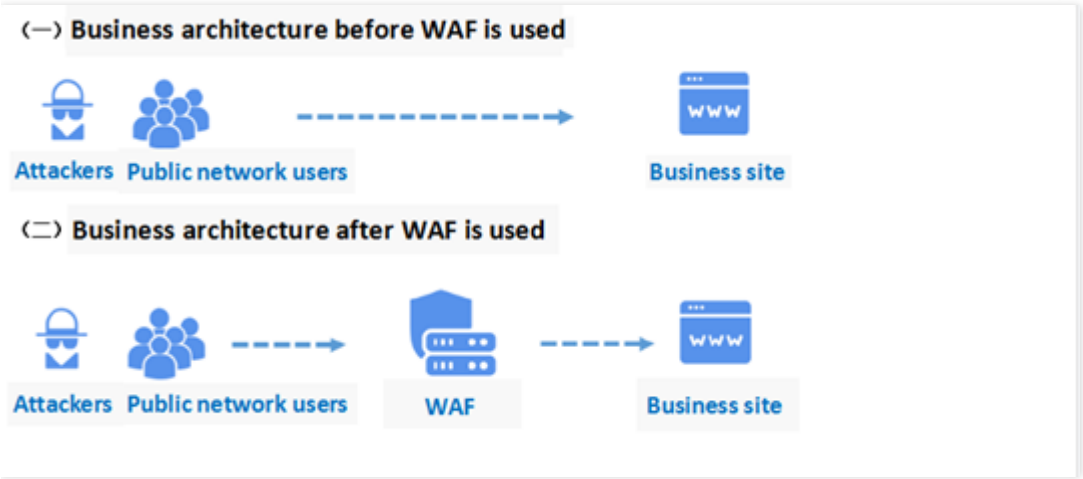
In the following scenarios, Tencent Cloud WAF can provide effective defense and prevention against risks, and ensure system and business security of enterprise websites.

- **Data leakage (core information asset is leaked)**
  As web sites are used as the entry for the information assets of many enterprises, hackers can steal enterprise information assets by means of invading web sites, resulting in incalculable losses to enterprises.
- **Malicious access and data crawling (the service is not running normally because data is leveraged by opponents)**
  Hackers controlling zombie computers launch CC attacks on the web sites, which then will be unable to provide services due to resource depletion. Malicious users capture the core content of websites (literature blogs, recruitment sites, forum sites, and e-commerce site comments) via web crawlers. Product details of e-commerce sites are gathered deliberately by competitors for research. Bonus

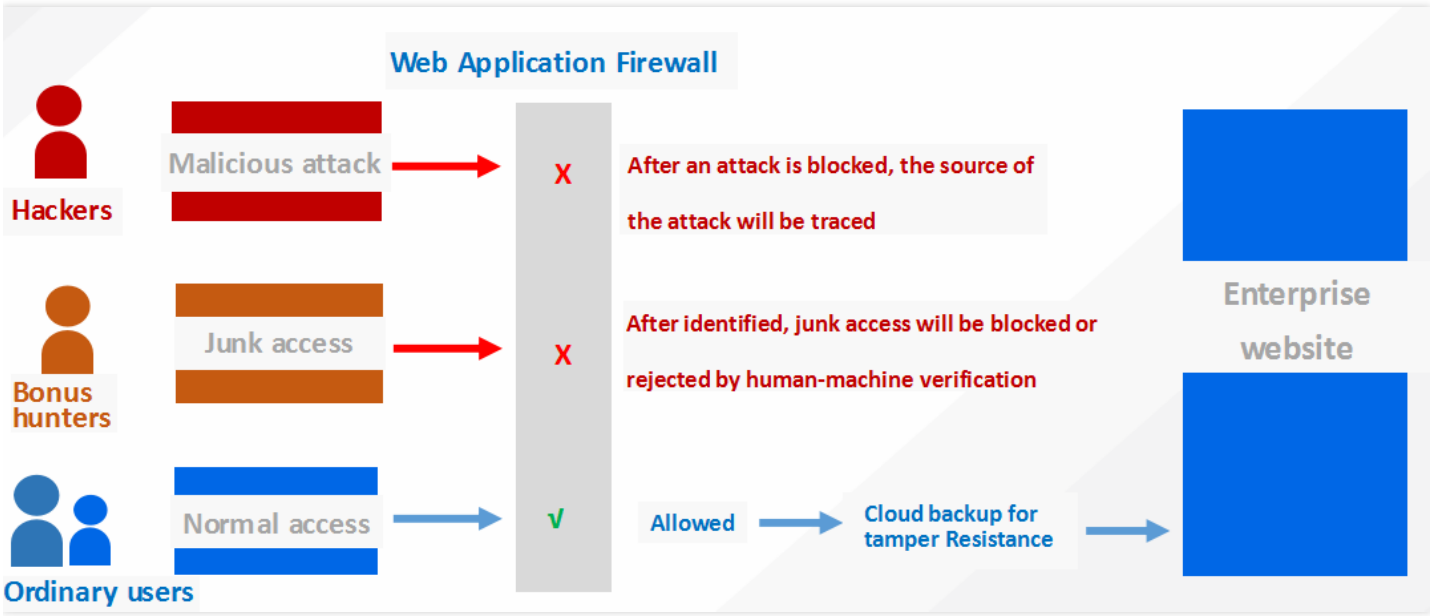
hunters seek for arbitrage by searching for low-priced product information or obtaining marketing intelligence in advance.

- **Website malicious code and tampering (affecting credibility and image)**
  After obtaining permissions of web sites or servers, attackers will inject malicious codes to make users execute malicious programs, to earn traffic, to steal accounts or to show off; insert links of pornographic, gambling, or illegal contents; and tamper with webpage images and texts. These will severely influence the operation of websites and impair the image and credibility of website operators.
- **Framework vulnerabilities (attacked during patch fixing period)**
  Many web systems are based on common open source frameworks, such as Structs2, Spring, and WordPress, which often carry security vulnerabilities. It is really a tough and dangerous period before patches are ready to use, because many attacks spring up soon after the vulnerabilities are uncovered.
- **Illegal hijacking (hijacking cannot be perceived)**
  The normal DNS requests of websites cannot be responded properly or the accessed content is maliciously modified due to the efforts of obtaining traffic or increasing advertising revenue. These are common hijacks on the Internet. Website operators generally cannot perceive these before receiving customer complaints.
- **Service interruption caused by DDoS attacks with large traffic**
  Being cheap and low-threshold, DDoS attack is often used to disrupt the operation of competitors or to make key portals inaccessible, leading to significant impact on business continuity and branding. And usually there isn't much operators can do when they are attacked.

Basic Defense Process



Tencent WAF defense diagram:



Advantages

Last updated：2018-06-22 11:18:20

Quick threat perception

By leveraging Tencent's big data threat intelligence, it can perceive threats as soon as they emerge.

Continuous threat defense

With more advanced threat defense technologies, Tencent United Security Laboratory continuously delivers top-level security protection capabilities.

Business risk defense

The exclusive BOT behavior management, DNS hijacking detection and junk access filtration capabilities can meet the protection requirements of secure business operation.

Minimum protection delay

The exclusive 30-line BGP IP linkage access protection provides the lowest service delay in the industry to guarantee the access speed of protected businesses.

Seamless scaling protection

The 100 GB anti-DDoS capability can be implemented seamlessly with only one click to defend against DDoS attacks with large traffic, thus avoiding sudden risks.

Scenarios

Last updated：2018-06-22 11:19:04

Government website protection

- WAF can be accessed with one click, and configured with ease. It can hide and protect origin servers, and prevent the website content from being stolen and tampered by hackers, ensuring correct website information, availability of government services, and satisfactory and smooth public access.

E-commerce website protection

- WAF provides continuous optimization of protection rules, precise blocking of Web attacks, and all-round protection against OWASP Top 10 Web application risks.
- In the case of highly concurrent purchases, it can intelligently filter malicious attacks and junk access to ensure smooth access to businesses.

Financial website protection

- WAF can be accessed with one click, and integrates with the large-traffic DDoS defense, and also provides web security protection.
- WAF can effectively monitor DNS linkage hijacking to avoid malicious directing of website traffic.
- WAF can effectively detect exceptional access like account credential enumeration attack to avoid user information leakage.
- With cloud resources and automatic scaling capability, WAF can easily deal with sudden business growth and large-traffic CC attacks.

Data leakage prevention

- WAF can avoid website core data leakage caused by hacker injection and intrusion attacks.
- Anti-CC attack: Anti-malicious CC (http get flood). WAF can ensure website availability by blocking massive malicious requests on layer 4 and layer 7.