Web Application Firewall

Glossary

Product Documentation

Glossary

Last updated：2022-06-23 10:14:04

SSL Certificate

Secure Sockets Layer (SSL) is a security protocol designed to ensure the security and data integrity of internet communication. Based on the SSL protocol, an SSL certificate can be installed on a server to achieve encrypted data transmission.

Proxy Server

Proxy server is a core server security feature which is applicable to the session layer in the Open Systems Interconnection (OSI) model. It can improve the access speed, hide real website IPs, and enhance website security.

Domain Name Resolution

Servers on the internet communicate with each other through IP addresses. However, most people are used to remembering a domain name that can be mapped to multiple IP addresses. The conversion between a domain name and an IP address is called domain name resolution.
The following are common domain name resolution types:
A record resolution: It specifies the IPv4 address of the domain name.
Select "A" as the record type.
Enter the server IP address provided by Tencent Cloud as the record value.
MX priority does not need to be configured.
Set TTL to 600 by default.
CNAME record resolution: It is used to point a domain name to another one which will be used to provide the IP address.
Select "CNAME" as the record type.
Enter the CNAME record generated after the protected domain name is added to WAF as the record value.
MX priority does not need to be configured.
Set TTL to 600 by default.

Security Groups

A security group is a virtual firewall that features stateful data packet filtering. It is used to configure the network access control of CVM instances. You can add CVM instances with the same network security isolation requirements in the same region to the same security group to filter their inbound and outbound traffic through the network policies of the security group.

VIP Address

After you add a domain name, WAF will automatically allocate a VIP address to it accordingly, which will act as the ingress address of WAF when the real server receives access requests. The access traffic will be forwarded to the VIP after DNS resolution and then to WAF.

Intermediate IP Address

After you add a domain name, WAF will automatically allocate multiple intermediate IP addresses to it accordingly, which can be used as the egress IPs of WAF to forward filtered normal traffic to your real server.

DNS Hijacking Protection

DNS hijacking protection provides DNS hijacking detection rules for site users to avoid data theft and financial loss caused by malicious hijacking, where attackers attack the DNS server or fake a new DNS server for the client domain name to be incorrectly resolved to malicious sites.

CC Attack Protection

Challenge Collapsar (CC) attack protection refers to a protection service against CC attacks where attackers use certain tools to simulate multiple users in order to continuously send connection requests to your website and make your business unavailable. You can add CC protection rules to defend against CC attacks for webpage requests.

Tamper Protection

Tamper protection refers to a mechanism where core webpages can be cached to the cloud and those in the cache can be published instead to realize the effect of webpage substitution. When the core webpages receive requests, content stored in cloud will be returned.

Leakage Protection

Leakage protection refers to a mechanism where the responding webpages are checked for sensitive information such as ID and phone numbers and any sensitive information detected will be observed or replaced with asterisks (*) according to the preset match behaviors, which helps avoid leakage of sensitive information.

Region Blocking

Region blocking refers to a mechanism that determines the region of an attacking IP and blocks access requests from all IPs in the specific region in order to quickly block attacks.

QPS

Queries per second (QPS) is a metric measurement how much traffic is processed by a particular query server within the specified time period. On the internet, the performance of DNS servers is often measured with QPS, which corresponds to fetches/sec (responded requests per second, i.e., the maximum throughput).