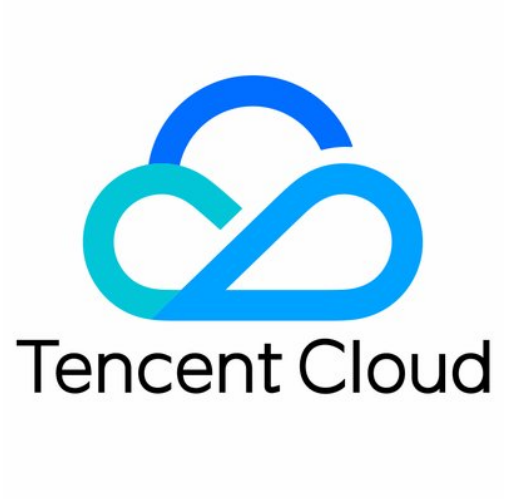
Web Application Firewall

Best Practice

Product Documentation



©2013-2019 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

©2013-2019 Tencent Cloud. All rights reserved.

Best Practice
Using WAF and Anti-DDoS Pro Together

Last updated : 2020-12-15 15:20:26

Use Cases

WAF features CC protection capabilities. For non-HTTP requests, it can work with Anti-DDoS Pro to protect your security in an all-round manner.

- Providing DDoS protection capability of hundreds of Gbps at one click, Anti-DDoS Pro can easily defend against DDoS attacks and ensure the smooth operation of your business.
- WAF can block web attacks in real time to ensure the security of your business data and information.

Directions

Step 1. Configure WAF

1. Log in to the WAF Console and select **Web Application Firewall** > **Defense settings** on the left sidebar.

2. On the defense settings page, click **Add domains** and set the following parameters as needed:
   - **Domain Configuration**
     - Domain Name: enter the domain name to be protected.
     - Web server configurations: select a protocol type and port as needed.
     - Enable HTTP2.0: select an option as needed.
     - Server Port: select an option as needed.
     - Real Server Address: enter the actual IP address of the real server of the website to be protected, i.e., public IP address of the real server.
   - **Other Configuration**
     - For proxy, please select **Yes**.
     - Enable WebSocket, Load Balance: select an option as needed.

> **Note :**

©2013-2019 Tencent Cloud. All rights reserved.

If the real server has multiple intermediate IPs, you can select a forwarding load balancing policy as needed. Currently, available policies include Round-Robin by user requests (requests from the same access source IP will be forwarded to different real servers in sequence) and IP hash (requests from the same access source IP will be forwarded to the same real server). The default policy is Round-Robin.

3. After completing the configuration, click **OK**.

Step 2. Configure Anti-DDoS Pro

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Pro** > **Resource List** on the left sidebar.

2. Select the region of the target Anti-DDoS Pro instance and click **Manage Protected Object** in the "Operation" column on the right of the instance.

3. On the **Manage Protected Object** page, set **Resource Type** as **WAF**, and select IP addresses protected by WAF in the **Resources to Associate** section.

Note :

If the WAF instance is in CLB type, then on the resource binding page, set "Resource Type" as "CLB", and select the public IP address of the corresponding CLB instance in the "Resources to Associate" section.

4. After completing the configuration, click **OK**.

©2013-2019 Tencent Cloud. All rights reserved.

Applying for and Using Free HTTPS Certificates

Last updated : 2020-08-18 17:35:37

Prerequisites

WAF supports configuration and protection of HTTPS access to domain names. If your website has not been altered for the HTTPS protocol, you can apply for a DV certificate free of charge in the SSL Certificate Service Console. After the application is approved, you can associate the certificate in the WAF Console; then, you can easily implement access and client connection to the entire website over HTTPS without modifying the real server.

Associating HTTPS Certificate

1. Log in to the WAF Console and select **Web Application Firewall** > **Protection Settings** on the left sidebar.
2. On the protection settings page, click **Add Domain Name** to enter the domain name adding page.
3. In server configuration on the page, select **HTTPS**. In certificate configuration, click **Associate Certificate**.
4. Select "Tencent Cloud-hosted Certificate" as the certificate source. Then, WAF will automatically associate an available certificate of the domain name. After the configuration is completed, click **Save**.
5. Enable forced HTTPS redirect, select the **HTTP** access protocol above, select "HTTP" as the "HTTPS Origin-pull Method", and set other parameters as needed; then, your website will support HTTPS access.

> To enable forced HTTPS redirect, you need to select both HTTP and HTTPS access protocols.

©2013-2019 Tencent Cloud. All rights reserved.

WAF Security Protection for API Gateway

Last updated : 2020-12-15 15:30:57

This document describes how to configure WAF to protect the security of APIs in API Gateway.

Prerequisites

- You have activated WAF.
- You have published the API in API Gateway as instructed in Getting Started.

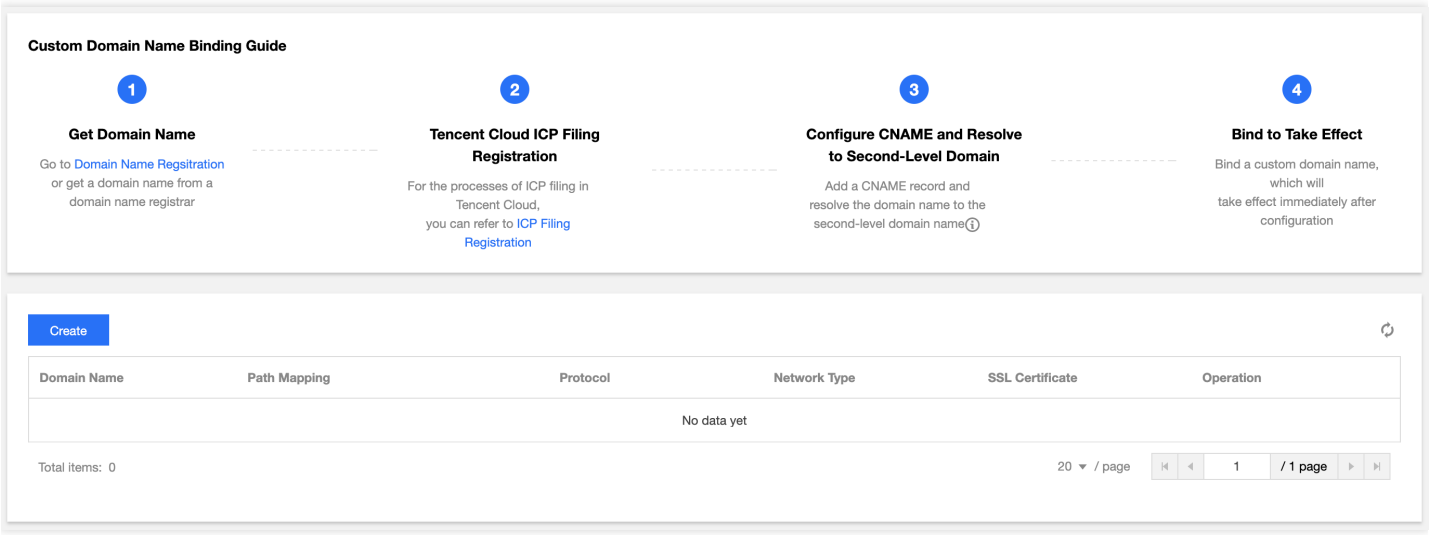
Directions

Step 1. Bind a custom domain name in the API Gateway Console

Bind a custom domain name in the API Gateway Console as instructed in Custom Domain Name and Certificate.

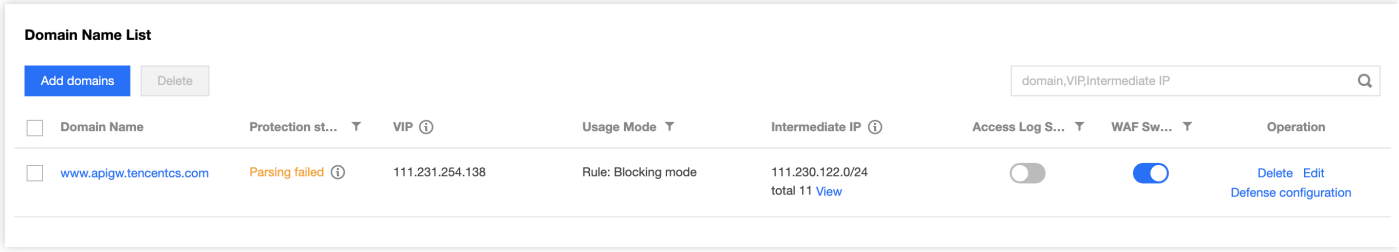
> ⚠ **Note :**
>
> When you bind the custom domain name in API Gateway, the system will verify whether the domain name is resolved (through a CNAME record) to a subdomain name of the API Gateway service. Therefore, you should resolve the custom domain name (through a CNAME record) to a subdomain name of the service first, bind it, and then modify the CNAME record to point it to the CNAME domain name of WAF.

©2013-2019 Tencent Cloud. All rights reserved.



Step 2. Configure WAF

1. Log in to the WAF Console.
2. Select **Web Application Firewall** > **Protection Settings** on the left sidebar to enter the protection settings page.
3. Click **Add Domain** above the domain name list to enter the domain name configuration page.
4. On the "Domain Configuration" page, fill in the relevant fields based on the actual conditions. Here, select "Domain Name" as the real server address, enter the subdomain name of the API Gateway service, and click **Save**.
5. After the configuration is completed, the domain name access status will become "CNAME record not configured".



Step 3. Modify the CNAME record

1. Modify the CNAME record at your DNS provider and point the custom domain name to the CNAME domain name of WAF.
2. Log in to the WAF Console and select **Web Application Firewall** > **Protection Settings** to enter the protection settings page.
3. In the domain name list, click the refresh button next to the access status, and you can see that the access status becomes "Normal protection". At this point, the access configuration is

©2013-2019 Tencent Cloud. All rights reserved.

completed.

©2013-2019 Tencent Cloud. All rights reserved.