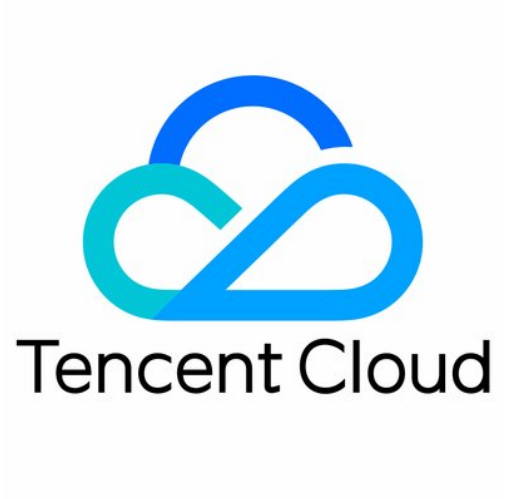
Anti-DDoS Pro

Best Practice

Product Documentation



Contents

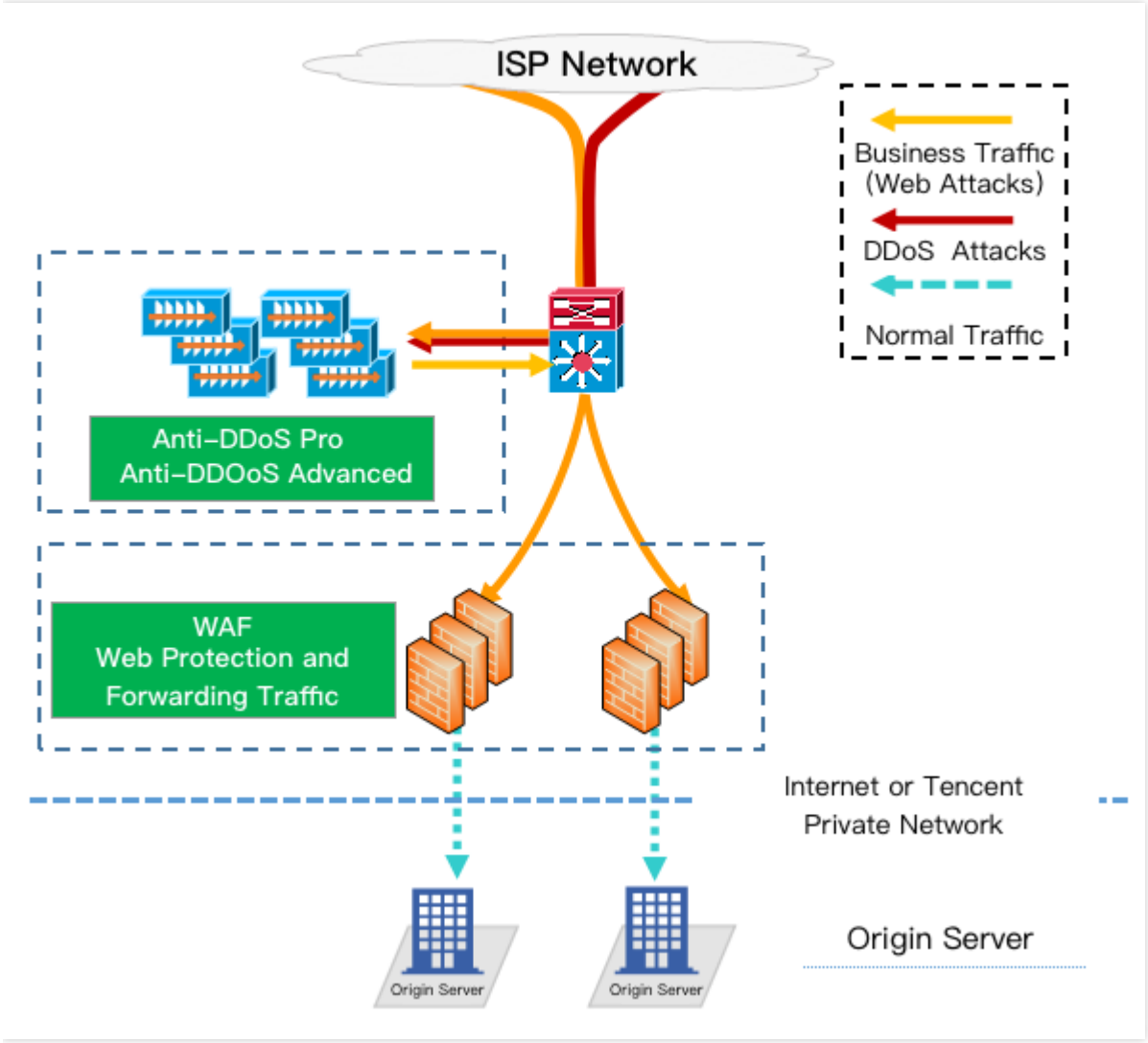
Best Practice
Combination of Anti-DDoS Pro and Web Application Firewall

Last updated：2019-09-26 18:33:27

Anti-DDoS Pro supports coupling Web application firewall to provide users with comprehensive security and protection.

- Anti-DDoS Pro provides hundreds of Gbps anti-DDoS protection capability at one-click to deal with DDoS attacks easily and ensure stable operation of your business.
- Web application firewall provides real-time protection to block Web attacks effectively, ensuring the security of your business data and information.

Deployment Plan

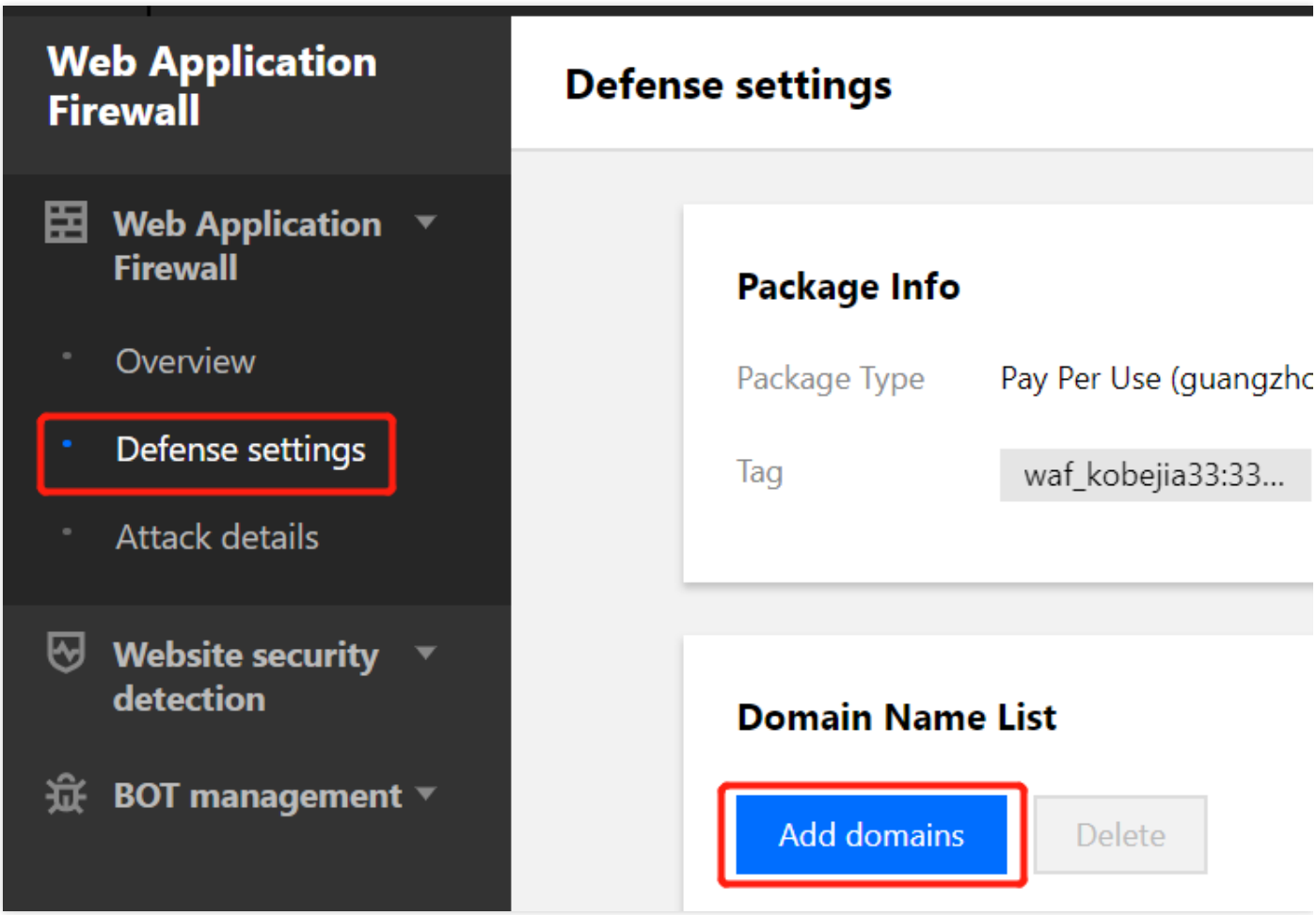


Configuration Procedure

Configuring the Web Application Firewall

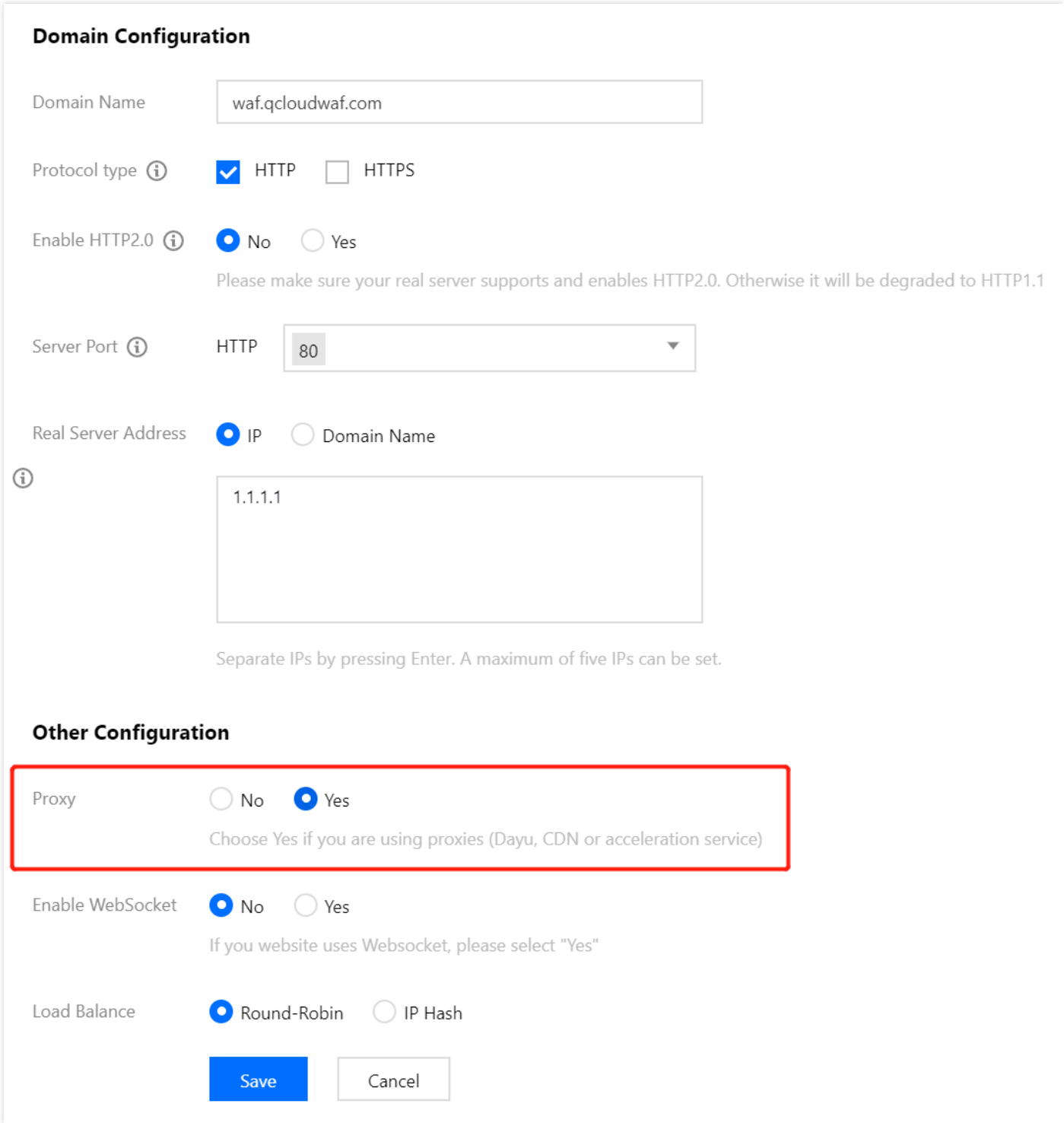
1. Log in to the Web Application Firewall Console.

2. Choose **Web Application Firewall** -> **Protection Settings**.



3. Click **Add Domain Name** and set the following parameters according to the actual condition:

- **Domain Name Configuration**
  - Domain Name: Enter the domain name to protect.
  - Protocol Type: Select according to the actual condition.
  - Enable HTTP 2.0: Select according to the actual condition.
  - Server Port: Select according to the actual condition.
  - Origin server address: Enter the real origin server IP address of the website to be protected, which is the public network IP address of the origin server.
- **Other Configurations**
  - For proxy, please select **Yes**.
  - Enable WebSocket and Cloud Load Balancer Strategies: Select according to the actual condition.



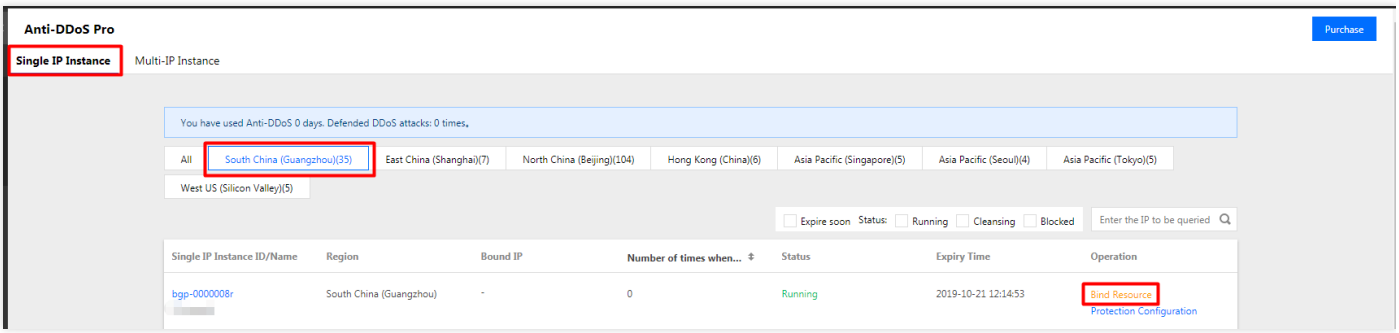
4. Click **Save**.

Configuring Anti-DDoS Pro

1. Log in to Anti-DDoS Console and choose **Anti-DDoS Pro** -> **Resource List**.

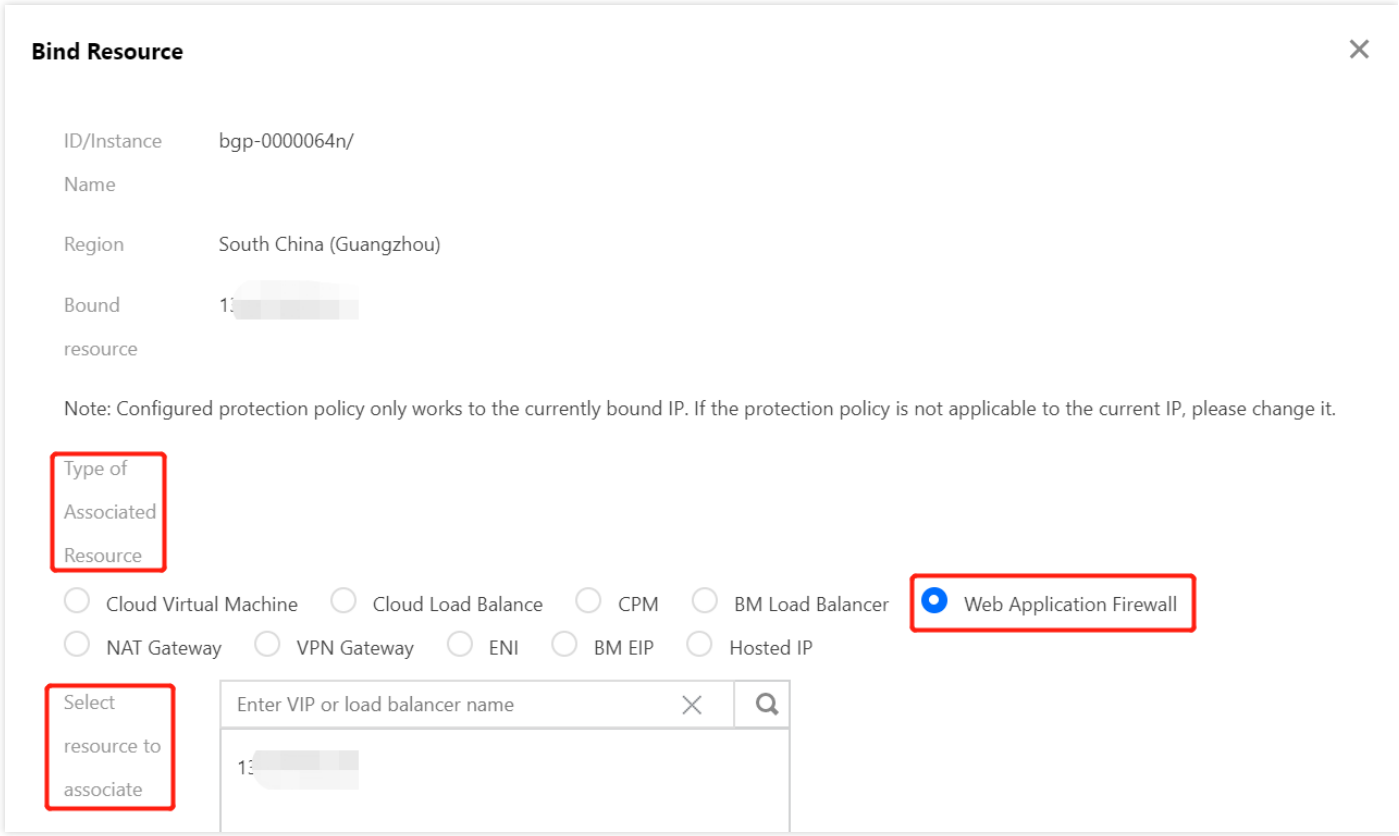
- For Single IP instance, please select the **Single IP Instance** tab.
- For Multi-IP instance, please select the **Multi-IP Instance** tab.

2. Select the region of the target Anti-DDoS Pro instance and click **Bind Resource** in the line of the instance.



3. On the **Bind Resource** page, set **Associate Resource Type** as **WAF**, and then set **Associated Resource** as the protected IP of WAF.

> You can bind multiple protected IPs of WAF to a Multi-IP instance.



4. Click **OK**.

Anti-DDoS Pro Remote Protection Scheme

Last updated：2019-09-26 18:33:35

Background

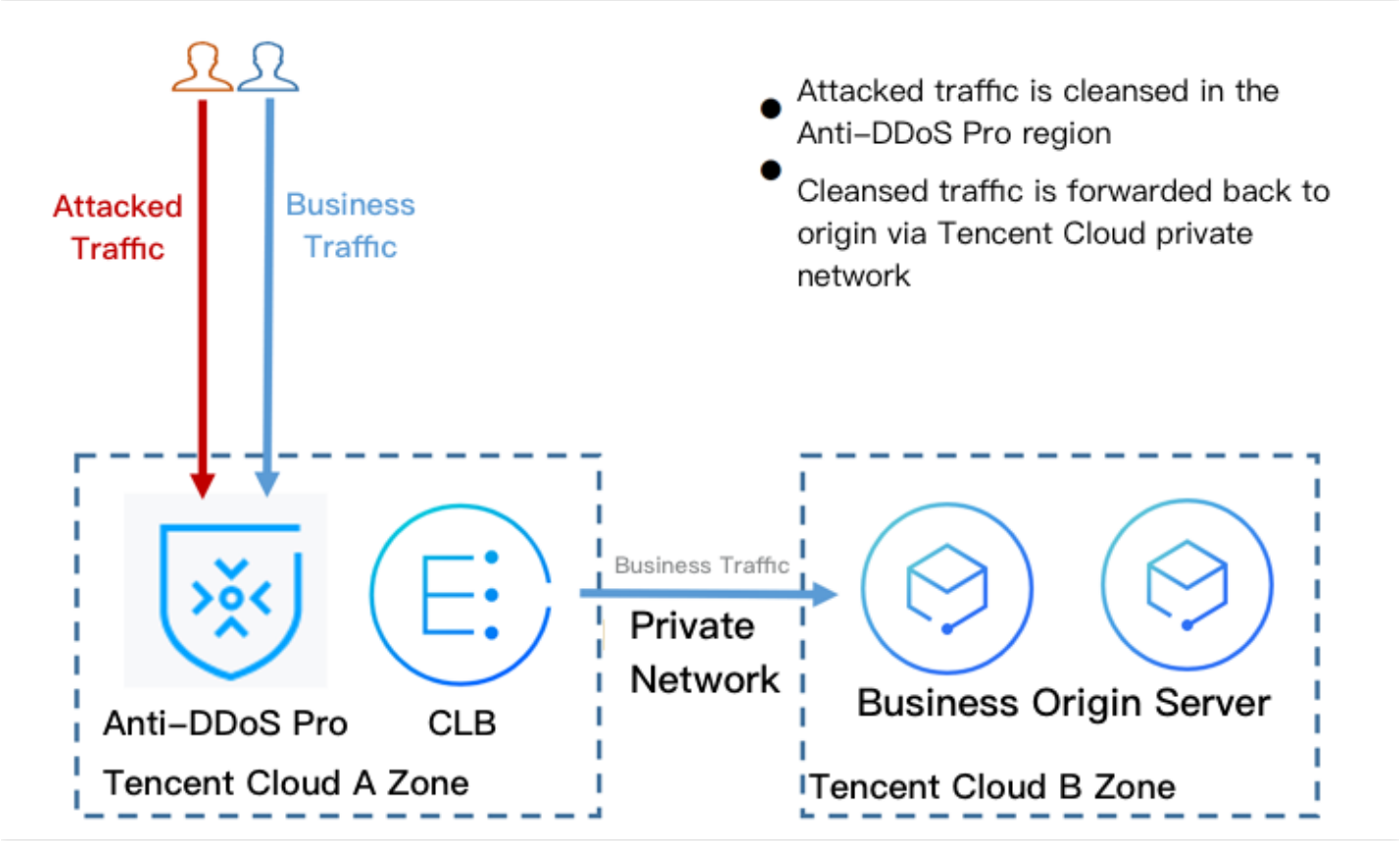
Due to objective factors, Anti-DDoS Pro provides up to 300 Gpbs of protection bandwidth in Shanghai and a lower bandwidth in Guangzhou and Beijing. In addition, Anti-DDoS Pro is not available in Chengdu, Chongqing, and other regions in China.
If your business origin servers are deployed on Tencent Cloud and you require DDoS protection in regions other than the region where Tencent Cloud origin servers locate, you can refer to this plan.

Protection Solution

This plan consists of Anti-DDoS Pro, Cloud Load Balancer (CLB), and customer originservers. Deploy a CLB in the regions with Anti-DDoS Pro resources and bind the CLB to the Anti-DDoS Pro instance. Configure the private network forwarding rules for the CLB to ensure that the public network IPs can access business through the CLB.

- In normal status, business IP can be parsed to the public network IPs of the origin server (or directly to CLB public network IPs in other regions). The business traffic accesses the nearby origin server.
- If attacks occur, the business IP is parsed to CLB IPs for DDoS attack traffic cleansing. After cleansing, the CLB forwards the traffic to the origin server via a private direct connect.

The following figure shows the detailed plan.



Solution Results

- The protection is no longer limited by regions and provides up to 300 Gpbs of Anti-DDoS Pro protection.
- The business traffic is forwarded by Tencent Cloud through direct connection to the private network with high reliability and a short delay time.
- Enjoy all the advantages of the Tencent Cloud BGP network, where all public network IPs belong to the BGP network lowering delay times.

Suggestions and Notes

- Deploy Anti-DDoS Pro and CLB in advance.
- Establish a business availability monitoring regime to discover and handle swiftly any exceptional access to the origin server when the automatic switching regime is not deployed.
- Conduct regular tests and practice drills to familiarize yourself with solutions and to solve potential problems.

Stress Test Advice for Business Systems

Last updated：2019-09-26 18:33:46

Stress testing is designed for mimicking DDoS attacks. To ensure the quality of the test, you are advised to read this document carefully before conducting a stress test and formulating an implementation plan.

> The following suggestions are based on the influence of anti-DDoS protection on stress testing. Other test-related factors, such as network bandwidth, linkage loads, or other basic resources, are subject to circumstance.

Adjusting Protection Policies

- Disable CC protection policies, or set the HTTP request threshold for CC protection to a value higher than the maximum value for stress testing.
- Disable anti-DDoS protection policies, or set the cleansing threshold for anti-DDoS protection to a value higher than the maximum value for stress testing.

Controlling Stress Testing Traffic and Request Number

- The bandwidth of stress testing should be slower than 1 Gbps, otherwise the attack defense may be triggered.
- The number of HTTP requests in the stress testing should be no more than 20,000 requests per second (QPS), otherwise the attack defense may be triggered.
- The number of new connections per second, total connections, and inbound packets per second should be less than 50,000, 2,000,000, and 200,000 respectively.

> If the stress testing requirements exceed the above ranges, please contact Tencent Cloud Technical Support. The after-sales team will offer support during stress testing.

Assessing Stress Testing in Advance

Contact Tencent cloud architectural engineers or Tencent Cloud Technical Support before the stress testing to comprehensively assess the possible consequences involved and to formulate risk aversion measures.