Web Application Firewall

Getting Started

Product Introduction

Contents

Getting Started
Getting Started

Getting Started
Getting Started

Last updated：2018-07-30 17:25:47

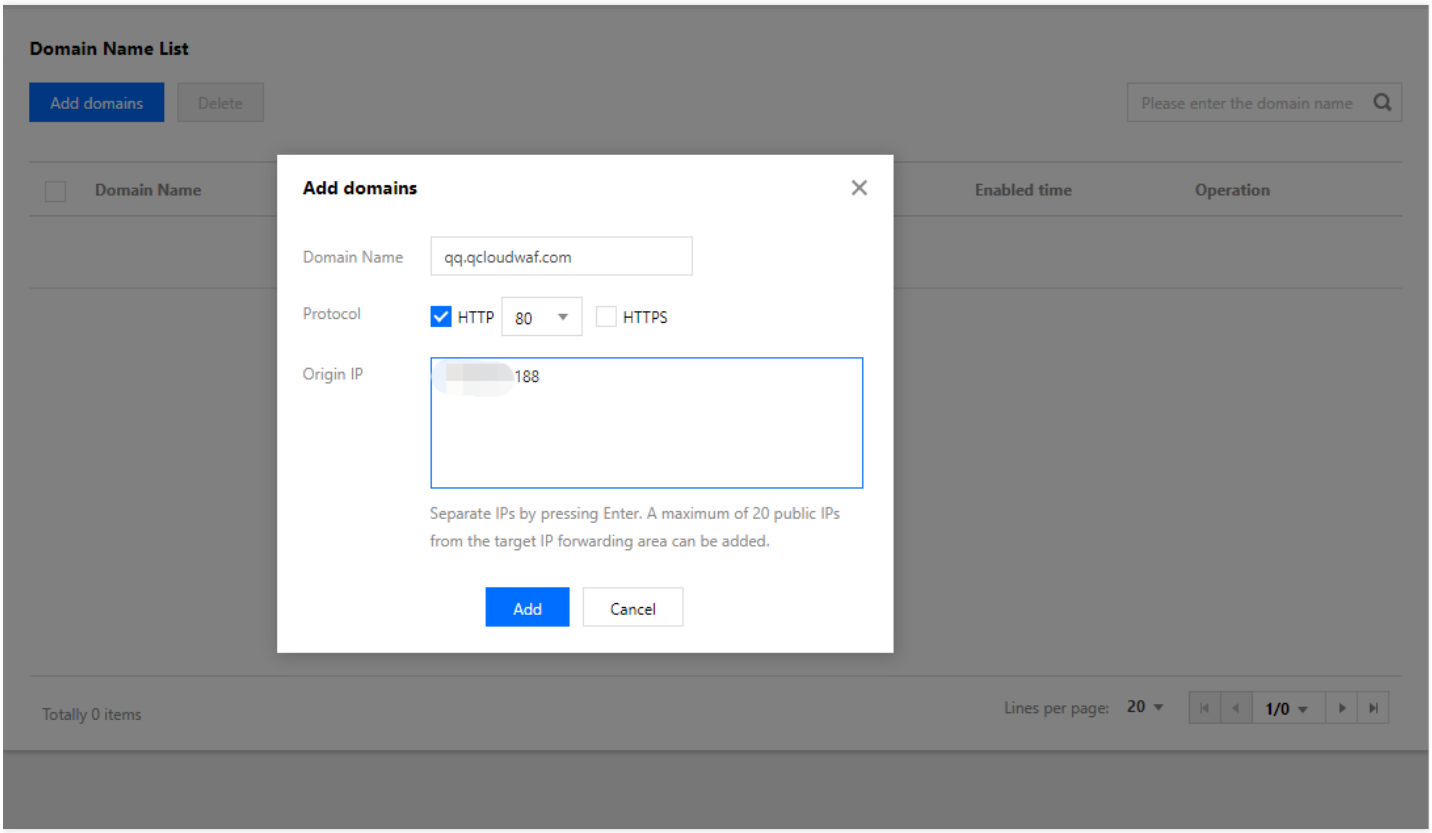
Getting Started with WAF

1. Add a domain name

To enable WAF to identify the domain names to be protected, you need to add the domain names to WAF first. For example, we will show you how to add the domain name qq.qcloudwaf.com.

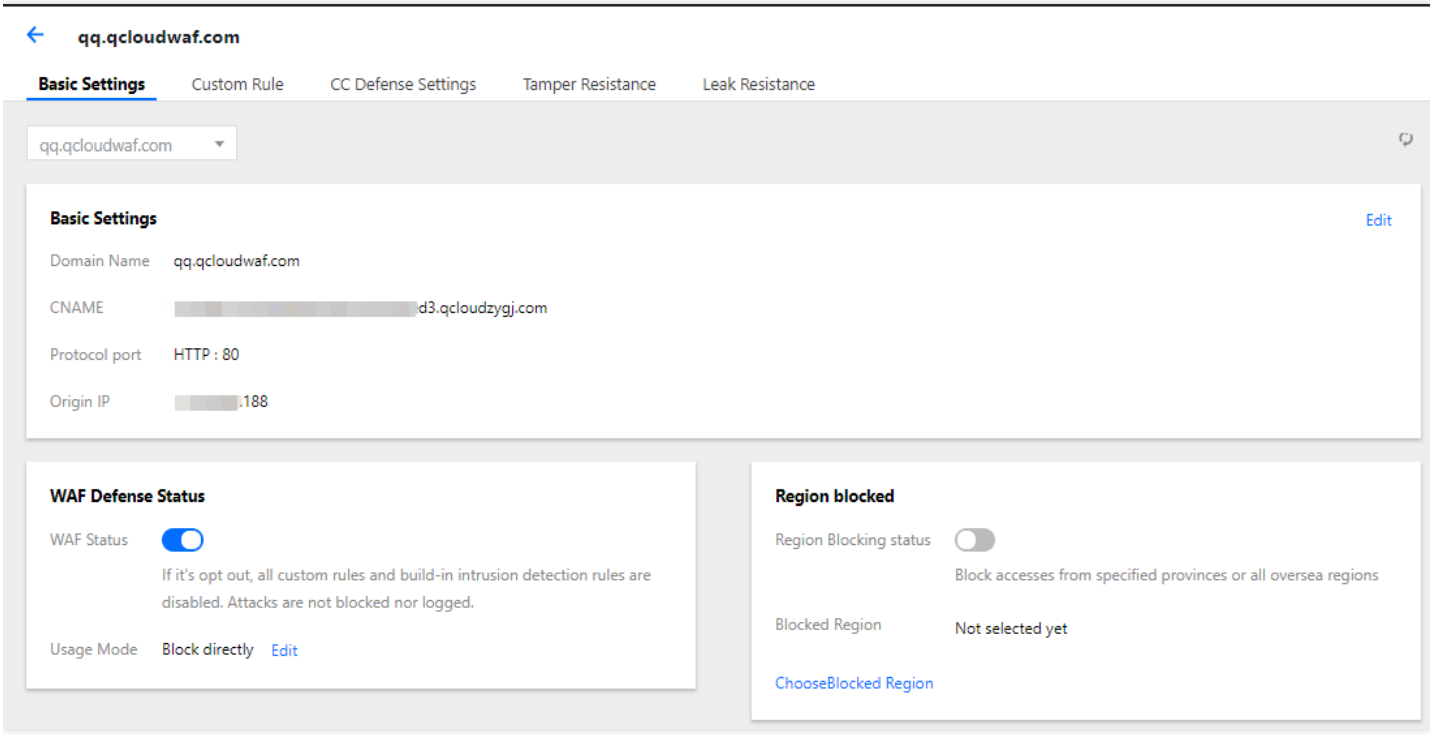
(1) Log in to the Tencent Cloud WAF console, click **Web Application Firewall** -> **Defense settings**in the navigation bar.

(2) Click **Add domains**, enter the domain name to be protected (qq.qcloudwaf.com) in the Domain Name input box, select a protocol and a port as needed (for example, HTTP and port 80), and enter the actual origin server IP of the website to be protected (i.e. the public IP of the origin server) in the Origin IP input box.



Click **Add** to complete the configuration.

(3) The added domain name is shown on the defense settings page. Double click the domain name to enter its details page, and you can see the CNAME assigned to the site by WAF.



Now, the domain name has been added successfully.

2. Local test

DNS resolution is required for local machines to access websites. Before performing DNS resolution, a local machine will obtain the IP of the target domain name from the local hosts file first. Therefore, we can direct the local access traffic to WAF by modifying the hosts file instead of directly modifying the DNS resolution record which will influence the access of public network users to websites, and test the connectivity of access to websites through WAF.

(1) Add a record of IP domain name in the local hosts file. The IP is obtained by pinging the CNAME assigned by WAF.

```
[root@centos73 ~]# ping                          37952a0ed3.qcloudzygj.com
PING                    337952a0ed3.qcloudzygj.com (119.28.174.239) 56(84) bytes of data.
64 bytes from          239 (          239): icmp_seq=1 ttl=46 time=174 ms
64 bytes from          239 (          239): icmp_seq=2 ttl=46 time=174 ms
64 bytes from          239 (          239): icmp_seq=3 ttl=46 time=175 ms
64 bytes from          239 (          239): icmp_seq=4 ttl=46 time=175 ms
64 bytes from          239 (          239): icmp_seq=5 ttl=46 time=173 ms
64 bytes from         .239 (         .239): icmp_seq=6 ttl=46 time=168 ms
^C
--- [                    37952a0ed3.qcloudzygj.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 168.867/173.663/175.837/2.350 ms
```

In Windows, modify "C:\Windows\System32\drivers\etc\hosts" by adding entries as shown in the following figure:

```
# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost


      239   qq.qcloudwaf.com
```

In Linux, modify "/etc/hosts" by adding entries as shown in the following figure:

```
                                  cat /etc/hosts
#127.0.0.1   localhost   localhost.localdomain   VM_174_185_centos
10.104.174.185  localhost   localhost.localdomain   VM_174_185_centos
#::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
#139.199.92.59 www.qcloudwaf.com

      239   qq.qcloudwaf.com
```

(2) Access a website on the local computer. If the website can be opened normally, the connectivity of access to the web origin server through WAF is normal. Then enter

```
http://qq.qcloudwaf.com/?test=alert(123)
```

in your browser. If the blocking page appears in the browser, WAF protection works properly.

3. Modify DNS resolution

To protect the public network traffic to websites with WAF, you need to modify the DNS resolution record. For example, we will show you how to modify the DNS resolution of the website qq.qcloudwaf.com on Tencent Cloud.

(1) Log in to the Tencent Cloud console, click the **Tencent Cloud DNS** tab in the navigation bar, select the

domain name qcloudwaf.com from the domain name list on the right, and then click **Resolve** to enter the resolution configuration page.

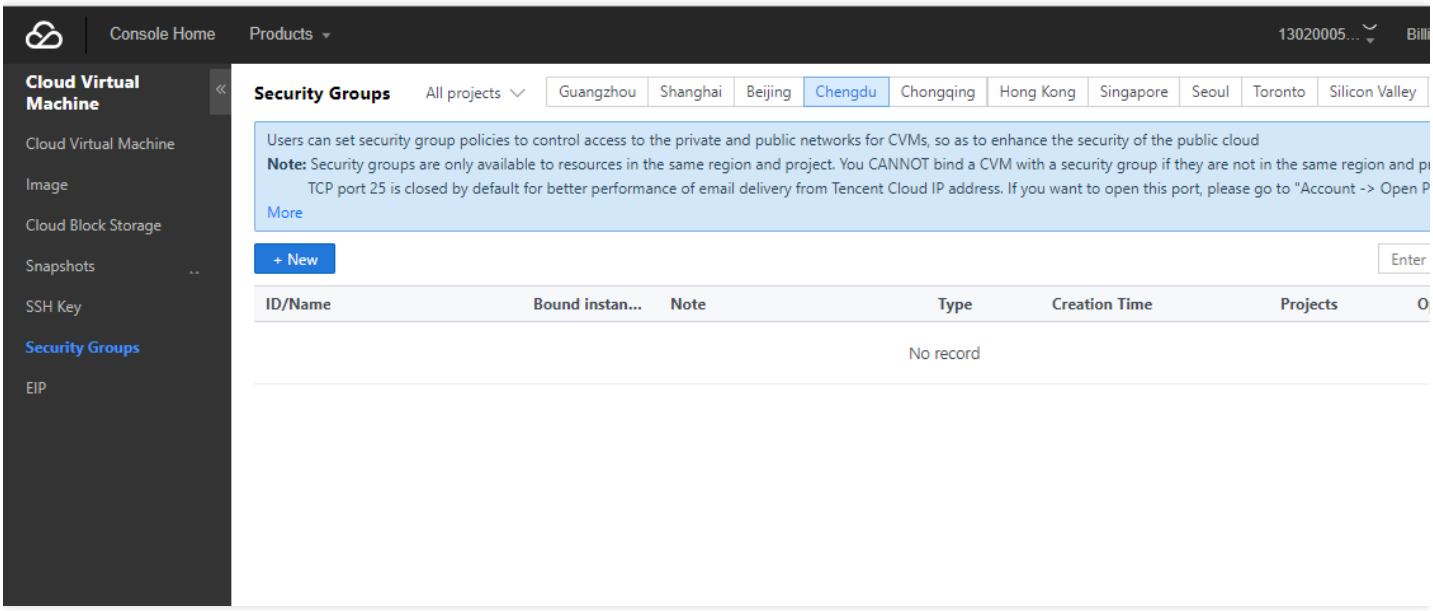
(2) Click **Add a Record**, and in the pop-up configuration window, select CNAME for Record Type, enter the host name of corresponding website for Host Name (enter qq here because qq.qcloudwaf.com is to be protected in this example), and enter the CNAME domain name `**********5e54837952a0ed3.qcloudzygj.com` assigned by WAF for Record Value.

(3) After the modified DNS record takes effect, the traffic of all Internet users accessing websites will be directed to and protected by WAF.
If WAF detects that the resolution of the protected domain name is normal, it displays **Normal Protection** in the console.

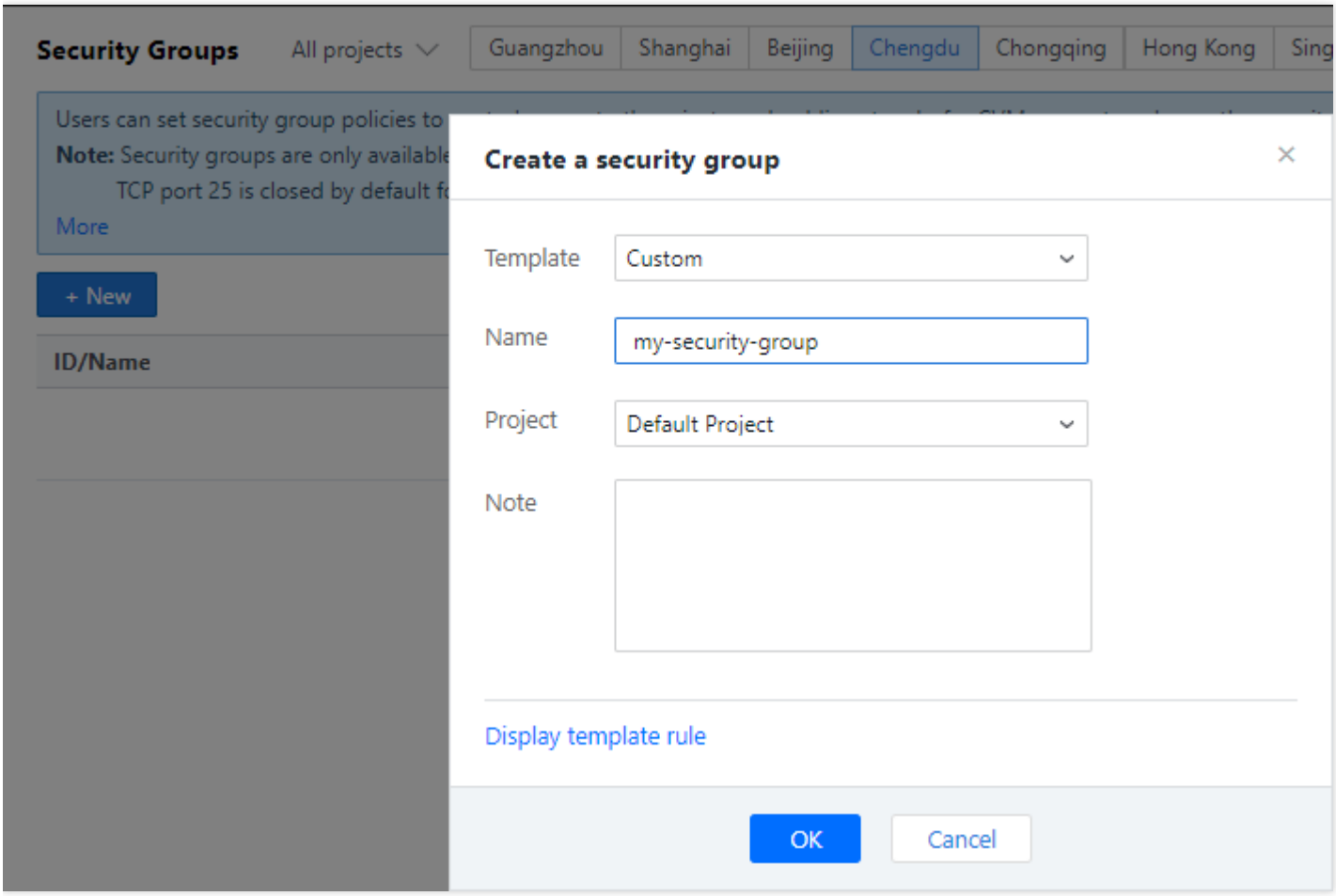
4. Set a security group

Security group, an instance-level firewall provided by Tencent Cloud, is used to control inbound/outbound traffic of CVMs. You can set to allow only traffic from WAF to access websites in the security group in order to prevent attackers from bypassing WAF and directly attacking the origin server. For example, we will show you how to allow a WAF intermediate IP (which can be viewed in the WAF console) in a security group.

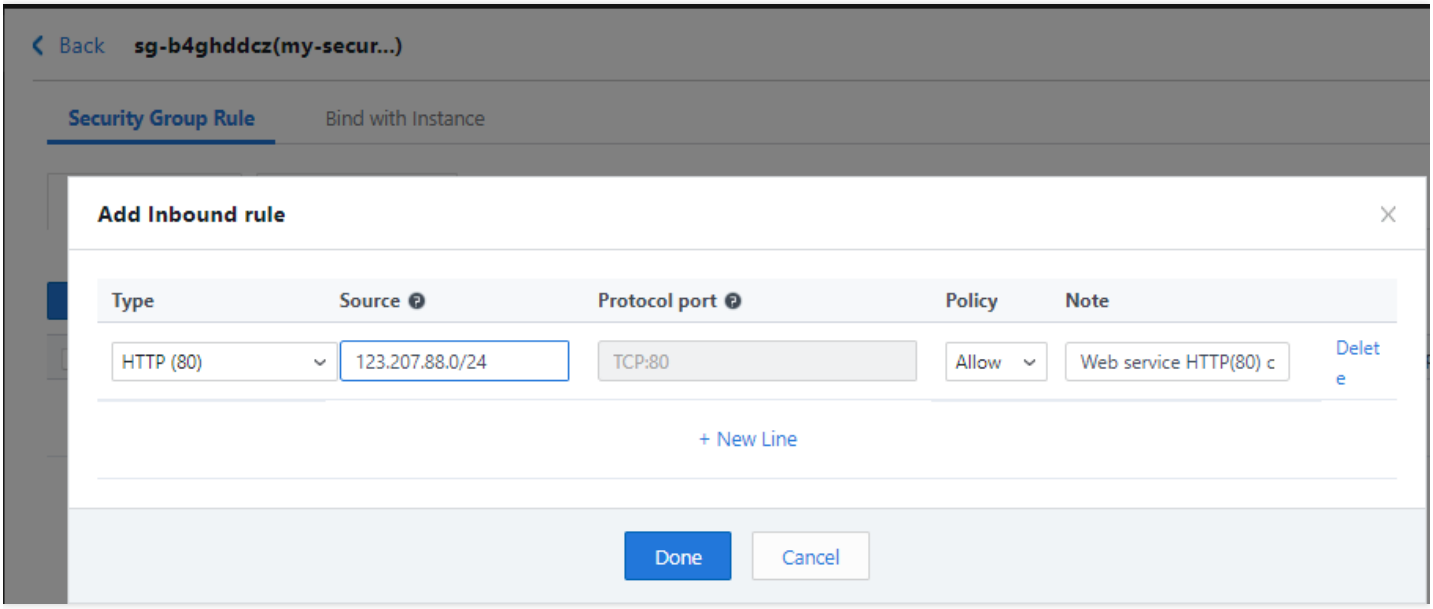
(1) Log in to the Tencent Cloud console, click **Cloud Virtual Machine** in the navigation bar, and click **Security Groups** in the left navigation pane.



(2) Click the **New** button, enter the security group name (e.g. my-security-group), select Custom for Template, and enter the relevant note.



(3) Click **+ New Line** in the inbound rule list. In the new configuration line, select HTTP for Type, and enter the intermediate IP address range 123.207.88.0/24 for Source.



Click **Done** to complete the configuration.

(4) Find the new security group in the security group list, click **Operation** -> **Add Instance**, select CVM for Binding Type, and select the CVM to be bound to complete the binding operation. You can also enter the CVM list page to view or modify the security group associated with the CVM. In the CVM list page, select the CVM for which you want to modify the security group, and click **Operation** -> **More** -> **Configure Security Group**, and then select a security group for binding.