Anti-DDoS Pro

Quickstart (Non-website)

Quickstart (Non-website)

Purpose

This guide introduces how to quickly set up **non-website protection** (for example APP, gaming, FTP, VOIP etc.) of Anti-DDoS Pro via Alibaba Cloud’ s console, and verify its configuration and protection.

Attention: compared with website protection, non-website protection provides only layer 4 port protection such as SYN/ACK/ICMP/UDP floods. It cannot mitigate layer 7 attacks such as HTTP floods, or web application attacks like SQL injection, XSS.

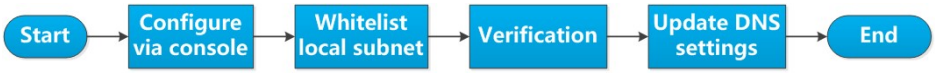
Target Readers

This guide is for the following users:

- Those who are interested in learning how Anti-DDoS Pro works
- Those who have purchased Anti-DDoS Pro and need to know how to set up Anti-DDoS Pro
- Those who want to test, verify, modify or delete Anti-DDoS Pro configuration

If you still have questions after reading this guide, refer to our online help center.

Quickstart Flowchart



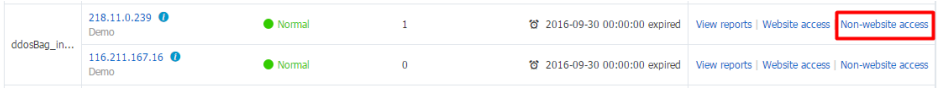
Basically non-website protection is set up as the procedures below:

1. Set up layer 4 port (non-website) protection.
2. Whitelist local IP addresses in the original server.
3. Verify local settings.
4. Update DNS settings and reroute traffic to Anti-DDoS Pro.

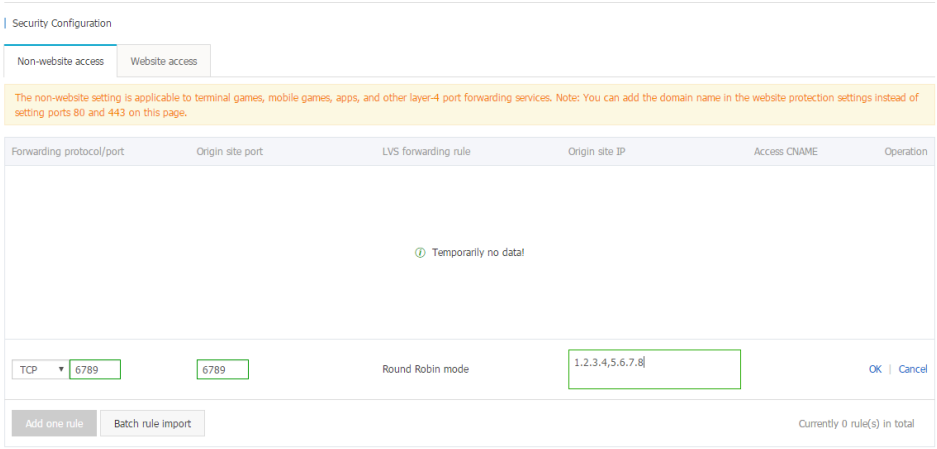
Log on to Alibaba Cloud console and go to **Anti-DDoS Service Pro**.

Operation procedure:

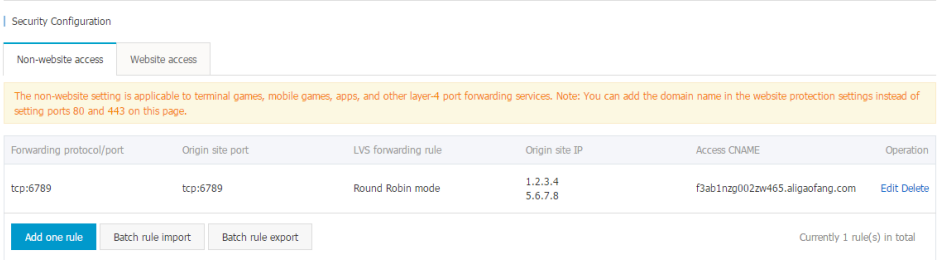
Click **Non-website access**, and then click **Add one rule** to add a layer 4 port forwarding rule.



Choose a protocol (TCP or UDP), and enter the forwarding port and the original site port. You can use commas to separate multiple original site IP addresses if needed.



Click **OK** to finish your configuration.



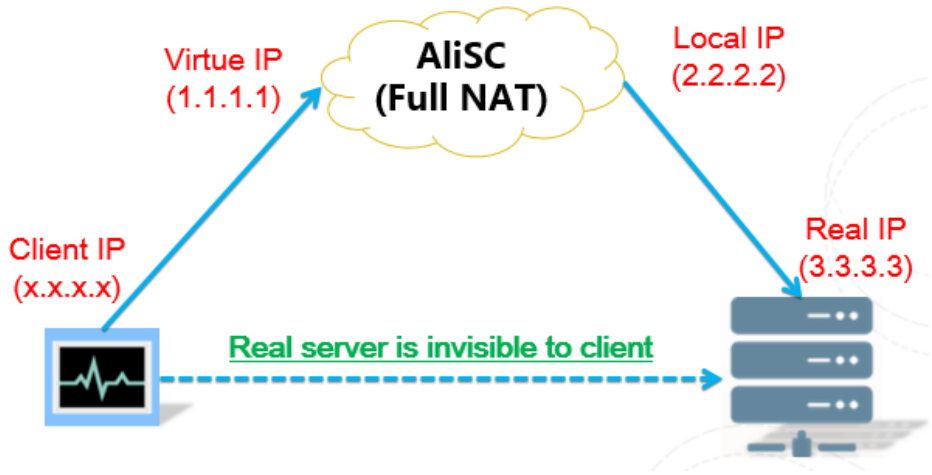
A CNAME record will also be generated here, which can be used to replace the DNS record.

Tips:

- Up to 50 layer 4 port forwarding rules are supported.
- Up to 20 original site IP addresses can be added to a layer 4 port forwarding rule. HTTPS requests will be load balanced to multiple original sites using round-robin method.
- UDP port 53 and TCP port 80 are not supported here.

The Alibaba scrubbing center works as a reverse proxy of the original server, taking over all the traffic (including both malicious and legitimate traffic), mitigating it and then forwarding it back to the original server. As a result, malicious traffic will be mitigated when going through the Anti-DDoS Pro service.

Anti-DDoS Pro uses a local IP address as the source IP address to establish a connection with the original server, as shown in the below (AliSC stands for Alibaba Scrubbing Center).



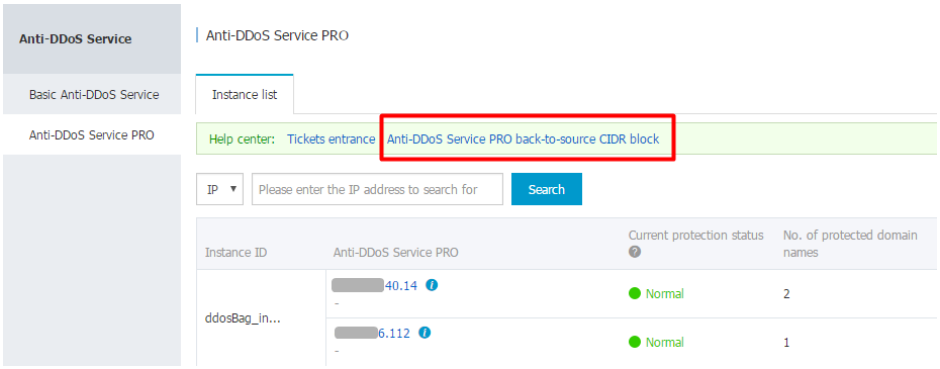
- There’ re more than one local IP addresses since AliSC has a bunch of physical servers.
- In this full NAT mode, every packet’ s source IP address is a local IP address.
- A list of local IP addresses are provided, which are fixed and needed to be whitelisted by the real server.
- AliSC uses Local IP addresses to visit IDC network and keeps the real client IP address in the HTTP/HTTPS header’ s X-forwarded-for field.

From the original server’ s perspective, source IP addresses will be much more concentrated, and the packets from them will be sent faster than before.

This could be more suspicious to the original server’ s firewall or security software (if there is one), which may block or limit the local IP addresses. So make sure all the local IP addresses are whitelisted after they are diverted to Alibaba Cloud.

For enhanced safety concern, it is recommended to block all the requests from other IP addresses (besides the local IP addresses) to the original server, so that the original server is better protected even if its real IP address is disclosed.

Latest local IP subnets (generally fixed subnets) are provided in the console, as shown in the below:



You can verify the forwarding setting to make sure it works well. This is not always necessary. However, it is recommended to do verification before updating your IP/DNS settings and rerouting all the traffic.

Manually bind the virtual IP address provided by Anti-DDoS Pro with the domain name in your local host file (for example C:\Windows\System32\drivers\etc\hosts). This way, the domain name will be resolved to the IP address only in your local device. Anti-DDoS Pro flushes your local DNS cache (for example ipconfig/flushdns in Windows CMD) and loads this domain name in your browser.

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

[redacted].0.239 www.aaa.com
```

If your protected service doesn't have a domain name (for example an IP address will be enough), you can directly replace the server's IP address with the virtual IP address provided in a local testing environment.

If you can access to the service normally, your configuration is well done. Otherwise, check your configuration again or contact our support for help.

All the settings have been done. Now let's reroute the traffic to Anti-DDoS Pro.

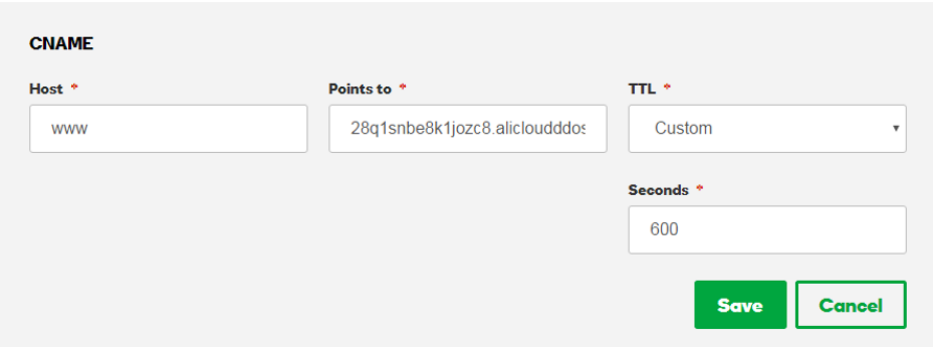
If your service does not need a domain name, you can directly update the server's IP address by replacing it with the virtual IP address provided by Anti-DDoS Pro.

If your service needs a domain name, go to your DNS configuration panel and update the former DNS record using CNAME record or A record, depending on your DNS service provider's configuration.

Although both CNAME record and A record are supported for rerouting traffic, it is strongly recommended that you use CNAME record instead of A record, because something goes wrong with a specific virtual IP address. The traffic can be switched to another virtual IP address (for example backup IP address) or even original site to avoid further problems. For more details, refer to **CNAME Access Configuration**.

- **CNAME record**

Update the former DNS record with the CNAME record generated. The former A Record can be deleted. The recommended TTL value is 10 minutes.



- **A Record**

Update the former A record with the virtual IP address provided by Anti-DDoS Pro. You can resolve the domain name to a different virtual IP address (if more than one virtual IP address are available, depending on different ISPs). The recommended TTL value is 10 minutes.