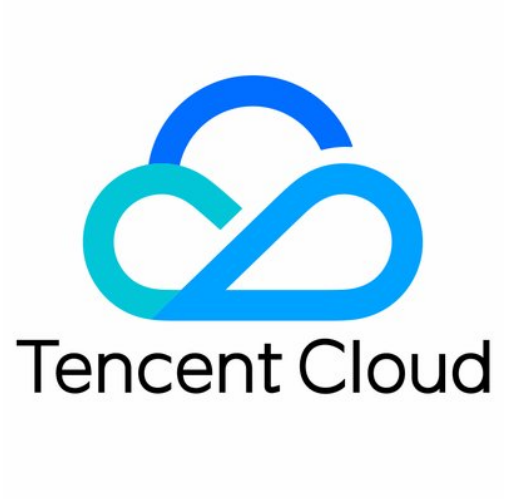
Anti-DDoS Advanced

Getting Started

Product Documentation



Contents

Getting Started
Accessing Non-website Applications

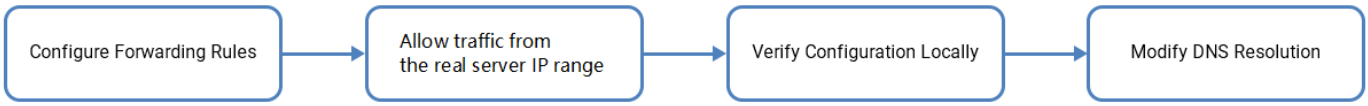
Last updated：2021-11-17 10:39:43

This document shows you how to connect non-website applications to Anti-DDoS Advanced instances and verify forwarding configurations.

Prerequisites

- Purchase an Anti-DDoS Advanced instance before adding a forwarding rule.
- Purchase a domain name resolution service before modifying the DNS information of your business domain name.

Process



Directions

Configuring a forwarding rule

1. Log in to the Anti-DDoS console and click **Anti-DDoS Advanced** -> **Access Configuration** on the left sidebar.

2. Open the **Non-website Scenarios** tab, find and select the target Anti-DDoS Advanced instance, and add a forwarding rule.

   - Create a single forwarding rule:

     a. Click **Create**.
     b. On the **Add forwarding rule** page, configure the following parameters as needed and click **OK**.

- Forwarding protocol: TCP and UDP are supported.
- Forwarding port: this is the Anti-DDoS Advanced port used for access. We recommend choosing the same port as that of the real server.
- Real server port: the real port of the business website.
- Forwarding method: **Forwarding via IP** and **Forwarding via domain name** are supported.
- Load balancing mode: only weighted polling is supported currently.
- Real server IP + weight/real server domain name: enter the real server IP + weight or real server domain name based on the **forwarding method**. Up to 20 pairs of IP + weight or domain name are supported.
  - If you tick **Forwarding via IP**, enter the real server IP address + weight, such as `1.1.1.1 50`. If a domain name corresponds to multiple pairs of real server IP + weight, you can enter all of them and separate them with carriage return. Up to 20 entries are supported.
  - If you tick **Forwarding via domain name**, enter the forwarding domain name. If a domain name corresponds to multiple real server domain names, you can enter all of them and separate them with carriage return. Up to 20 entries are supported.
    - Create multiple forwarding rules in batches:

      a. Click **Batch import** -> **Import forwarding rules**.
      b. Paste rules in the rule input box.

Note：

- From left to right, paste the forwarding protocol, forwarding port, real server port, real server IP, and weight (or forwarding domain name); separate each one with a space; only one forwarding rule can be entered per line.
- The number of forwarding rule entries added in batches cannot exceed the current quota. Within the quota limit, up to 30 entries can be imported at a time.

Allowing the forwarding IP range

To prevent the service unavailability that occurs when the real server blocks Anti-DDoS Advanced's forwarding IP, we recommend configuring allowlist policies for the real server infrastructure, including firewall, Web Application Firewall,

intrusion prevention system (IPS), and traffic management, and disabling the protection feature of the host firewall and other security software (such as Safedog) or setting allowlist policies, so that the forwarding IP will not be affected by the security policies of the real server.

To view the detailed Anti-DDoS Advanced forwarding IP range, you can log in to the Anti-DDoS console, click **Anti-DDoS Advanced** -> **Resource List** on the left sidebar, find the row of the target Anti-DDoS Advanced instance, and click its **ID/Name**.

Verifying the configuration locally

After the forwarding configuration is completed, the Anti-DDoS Advanced IP will forward the packets from the relevant port to the corresponding real server port by following the forwarding rules.

To ensure the stability of your business, a local test is recommended. The verification methods are as follows:

- **For applications accessed via IPs**
  For applications accessed via IPs (such as games), run `telnet` to check whether the Anti-DDoS Advanced port is accessible. You can also enter the Anti-DDoS Advanced IP as the server IP in your local client (if available) to check whether the local client can access the Anti-DDoS Advanced IP.
  For example, the Anti-DDoS Advanced IP is `10.1.1.1` with the forwarding port 1234. And the real server IP is `10.2.2.2` with the real server port 1234. Run `telnet` on your local client to connect to `10.1.1.1:1234` . If the address can be accessed, it means that the forwarding is successful.

- **For applications accessed via domain names**
  For applications accessed via domain names, please try the followings:

  i. Modify your local `hosts` file to direct local requests to the protected website to the Anti-DDoS Advanced IP.
  Take Windows operating system as an example:

  a. Open the `hosts` file in `C:\Windows\System32\drivers\etc` , and add the following content at the end of the text:
  `<anti-ddos advanced="" ip="" address=""> <domain name="" of="" the="" protected="" website="">`
  For example, if the Anti-DDoS Advanced IP is `10.1.1.1` and the domain name is `[www.qq.com](www.qq.com)` , add:
  `10.1.1.1 www.qq.com`
  b. Save the `hosts` file.

  ii. Run the `ping` command on the local computer to test the protected domain name.
  If the resolved IP address is the Anti-DDoS Advanced IP address bound in the `hosts` file, the forwarding is successful.

> Note：
> If the resolved IP address is still the real server IP address, try running the `ipconfig/flushdns` command in the Windows Command Prompt to clear the local DNS cache.

iii. After successful configuration of `hosts`, check whether the domain name can be accessed.
If yes, the configuration has taken effect.

> Note：
> If the verification still fails with the correct method, please log in to the Anti-DDoS console and check whether the configuration is correct. If the problem persists after you fix any incorrect configuration items, please contact Tencent Cloud technical support.

Modifying the DNS resolution of the business domain name

Before using Anti-DDoS Advanced, you need to configure the A record of your business domain name's DNS with an Anti-DDoS Advanced IP, so that all user access requests to your site will pass through Anti-DDoS Advanced first before arriving at the real server (that is, all traffic will be first directed to Anti-DDoS Advanced before getting to the real server).

> Note：
> The principle of domain name resolution configuration is consistent, but the configuration methods in different service providers may be different. Here the Tencent Cloud DNSPod is used.

1. Log in to the DNSPod console, click **Domain Name Resolution List** on the left sidebar, and click **Resolve** on the right of a domain name.
2. Open the **Record Management** tab, click **Add Records** to modify the IP address pointed to by the A record to the Anti-DDoS Advanced IP address, and click **Save**.

Accessing Website Applications

Last updated：2021-01-25 12:18:17

This document shows you how to connect website applications to Anti-DDoS Advanced instances and verify forwarding configurations.

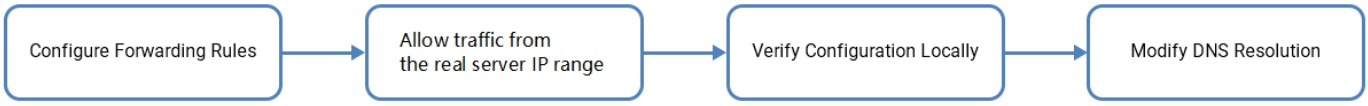
Note：

It currently supports connecting website applications in Beijing, Shanghai, and Guangzhou, while regions outside the Chinese mainland are not supported.

Prerequisites

- Purchase an Anti-DDoS Advanced instance before adding a forwarding rule.
- Purchase a domain name resolution service before modifying the DNS information of your business domain name.

Process



Directions

Configuring-a-forwarding-rule">

Configuring a forwarding rule

1. Log in to the Anti-DDoS console and click **Anti-DDoS Advanced** -> **Access Configuration** on the left sidebar.
2. Open the **Website Scenario** tab, find and select the target Anti-DDoS Advanced instance, and add a forwarding rule.
   - Create a single forwarding rule:

a. Click **Create**.

3. On the **Add forwarding rule** page, configure the following parameters as needed and click **OK**.

```
Parameter description:
```

- Domain: enter the domain name to be protected.
- Protocol: HTTP and HTTPS are supported, you can tick one as needed.

Scenario	Operation
Websites with HTTP only	Tick **HTTP**.
Websites with HTTPS only	▪ Tick **HTTPS**. ▪ Certificate source: the Tencent Cloud hosted certificate is selected by default. ▪ Certificate: select the corresponding SSL certificate.

- Forwarding method: **Forwarding via IP** and **Forwarding via domain name** are supported.
- Enter the real server IP or real server domain name based on the **forwarding method**.

```
- If you tick **Forwarding via IP**, enter the real server IP (or IP + port). If a domain name corresponds to multiple real server IPs (or multiple pairs of IP + port), you can enter all of them and separate them with carriage return. Up to 16 entries are supported.
- If you tick **Forwarding via domain name**, enter the forwarding domain name (CNAME) or domain name (CNAME) + port. If a domain name corresponds to multiple real server domain names (CNAME) or multiple pairs of domain name (CNAME) + port, you can enter all of them and separate them with carriage return. Up to 16 entries are supported.
```

- Create multiple forwarding rules in batches:

a. Click **Batch import** -> **Import forwarding rules**.

b. Paste rules in the rule input box.

> ⚠ **Note：**
>
> - From left to right, paste the domain name, protocol, real server IP (real server domain name is currently not supported), and real server port; separate the real server IP and real server port with `:` and others with spaces; only one forwarding rule can be entered per line.
> - The number of forwarding rule entries added in batches cannot exceed the current quota.

Allowing-the-forwarding-IP-range">

Allowing the forwarding IP range

To prevent the service unavailability that occurs when the real server blocks Anti-DDoS Advanced's forwarding IP, we recommend configuring allowlist policies for the real server infrastructure, including firewall, Web Application Firewall, intrusion prevention system (IPS), and traffic management, and disabling the protection feature of the host firewall and other security software (such as Safedog) or setting allowlist policies, so that the forwarding IP will not be affected by the security policies of the real server.
To view the detailed Anti-DDoS Advanced forwarding IP range, you can log in to the Anti-DDoS console, click **Anti-DDoS Advanced** -> **Resource List** on the left sidebar, find the row of the target Anti-DDoS Advanced instance, and click its **ID/Name**.

Verifying-the-configuration-locally">

Verifying the configuration locally

After the forwarding configuration is completed, the Anti-DDoS Advanced IP will forward the packets from the relevant port to the corresponding real server port by following the forwarding rules.
To ensure the stability of your business, a local test is recommended. The verification methods are as follows:

1. Modify your local `hosts` file to direct local requests to the protected website to the Anti-DDoS Advanced IP.
   Take Windows operating system as an example:
   i. Open the `hosts` file in `C:\Windows\System32\drivers\etc`, and add the following content at the end of the text:
   `<Anti-DDoS Advanced IP address> <Domain name of the protected website>`
   For example, if the Anti-DDoS Advanced IP is `10.1.1.1` and the domain name is `[www.qq.com](www.qq.com)`, add:
   `10.1.1.1 www.qq.com`
   ii. Save the `hosts` file.
2. Run the `ping` command on the local computer to test the protected domain name.
   If the resolved IP address is the Anti-DDoS Advanced IP address bound in the `hosts` file, the forwarding is successful.

> **Note：**
> If the resolved IP address is still the real server IP address, try running the `ipconfig/flushdns` command in the Windows Command Prompt to clear the local DNS cache.

3. After successful configuration of `hosts`, check whether the domain name can be accessed.
   If yes, the configuration has taken effect.

Note：

If the verification still fails with the correct method, please log in to the Anti-DDoS console and check whether the configuration is correct. If the problem persists after you fix any incorrect configuration items, please contact Tencent Cloud technical support.

Modifying-the-DNS-resolution-of-the-business-domain-name">

Modifying the DNS resolution of the business domain name

Before using Anti-DDoS Advanced, you need to configure the A record of your business domain name's DNS with an Anti-DDoS Advanced IP, so that all user access requests to your site will pass through Anti-DDoS Advanced first before arriving at the real server (that is, all traffic will be first directed to Anti-DDoS Advanced before getting to the real server).

Note：

The principle of domain name resolution configuration is consistent, but the configuration methods in different service providers may be different. Here the Tencent Cloud DNSPod is used.

1. Log in to the DNSPod console, click **Domain Name Resolution List** on the left sidebar, and click **Resolve** on the right of a domain name.
2. Open the **Record Management** tab, click **Add Records** to modify the IP address pointed to by the A record to the Anti-DDoS Advanced IP address, and click **Save**.