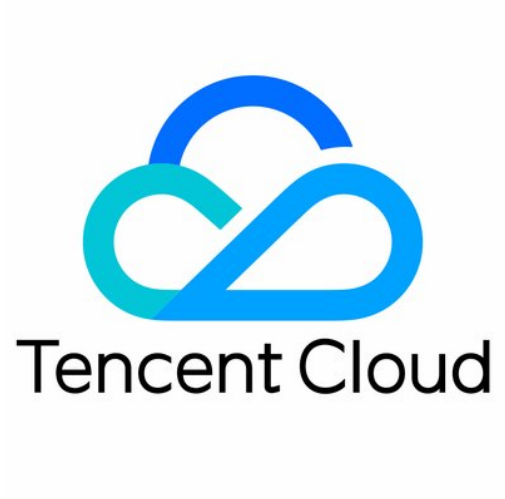
Anti-DDoS Advanced

Best Practices

Product Documentation



Contents

Best Practices
Migrating Applications to Anti-DDoS Advanced

Last updated：2020-05-09 18:03:48

Background

There could be many special configurations and restrictions for currently running online applications, and service downtime may have negative impact on business. Therefore, you are recommended to follow the suggestions below to adopt appropriate switching mode and avoid possible risks before integrating Anti-DDoS Advanced to your online applications.

Suggestions

Please note that the following suggestions are based on what we have learned from serving other Tencent Cloud customers. You are recommended to adjust or improve the scheme according to your actual situation to minimize risks.

Technical suggestions

- Modify local hosts file instead of the DNS A record. The testing team should locally test and measure relevant performance metrics such as availability and latency.
- With an intelligent DNS product, you can change the A record for specified ISPs or regions, redirect a little amount of traffic to Anti-DDoS Advanced IP for test before fully applying Anti-DDoS Advanced to your business applications.
- Shorten the TTL of the DNS record for faster disaster recovery.
- Prepare a rollback plan in advance and back off as soon as any problem arises.

Priority

- Migrate standby and non-critical business applications first.
- Migrate the applications during off-hours.

In Case of Real Server IP Exposed

Last updated：2020-04-03 14:35:44

Some attackers may record real server IP history, and the exposed IPs allow them to bypass Anti-DDoS Advanced and directly attack your real server. In this case, you are recommended to change the actual real server IP.
If you don't want to change the IP of your real server or have already done so but the IP is still exposed, in order to prevent attacker from bypassing Anti-DDoS and directly attack your real server IP, please follow the steps below:

- To prevent attackers from scanning C range or other similar IP ranges, do not use the same IP or an IP similar to the old IP as the new real server IP.
- Prepare the standby linkage and standby IP in advance.
- Set the scope of access sources to prevent malicious scans.
- Follow the instructions in Real Server-Based Defense Scheduling Solution and apply the solution based on your actual needs.

> Before changing the real server IP, be sure to confirm that all factors that may expose the IP have been eliminated.

You can refer to the following steps before changing the real server IP to check the risk factors and prevent the new IP from disclosure.

Checklist

Checking DNS resolution history

Check all the DNS resolution records of the attacked real server IP, including resolution records of sub-domain names, MX (Mail Exchanger) records of mail servers, and NS (Name Server) records. Make sure that all those records are configured for protection by Anti-DDoS Advanced, so that none of them will be resolved to the new real server IP.

Checking for information disclosure and command execution vulnerabilities

- Check your websites or business systems for possible information disclosure vulnerabilities, such as phpinfo() disclosure and sensitive information leakage on GitHub.
- Check your websites or business systems for command execution vulnerabilities.

Checking for trojans and backdoors

Check your real server for potential trojans, backdoors, and other hidden risks.

Obtaining Real Client IP

Last updated：2020-04-21 11:34:57

Using Non-Website Traffic Forwarding Rules

When Anti-DDoS Advanced uses non-website traffic forwarding rules, the real server needs to get the real client IP through the TOA module.
After the business request is forwarded through layer 4 of the protective IP, the source IP address that the business server sees after receiving the packet is the egress IP address of the protective IP. In order for the server to get the real client IP, you can use the following TOA scheme. On the Linux server of the business, install the corresponding TOA kernel package and reboot the server. Then, the server can get the real client IP.

How TOA works

Once forwarded, the data packet will undergo SNAT and DNAT at the same time, and its source and destination addresses will be modified.
Under the TCP protocol, in order to pass the client IP to the server, the client's IP and port are placed in the custom `tcp option` field during forwarding.

```
#define TCPOPT_ADDR 200
#define TCPOLEN_ADDR 8 /* |opcode|size|ip+port| = 1 + 1 + 6 */

/*
*insert client ip in tcp option, now only support IPV4,
*must be 4 bytes alignment.
*/
struct ip_vs_tcpo_addr {
__u8 opcode;
__u8 opsize;
__u16 port;
__u32 addr;
};
```

The Linux kernel's state transits from `SYN_REVC` to `TCP_ESTABLISHED` after the listening socket receives the ACK packet of three-way handshake. At this point, the kernel will invoke the `tcp_v4_syn_recv_sock` function. The Hook function `tcp_v4_syn_recv_sock_toa` will first invoke the original `tcp_v4_syn_recv_sock` function, then invoke the `get_toa_data` function to extract the `TOA OPTION` from the `TCP OPTION` , and store it in the `sk_user_data` field.

Then, `inet_getname_toa hook inet_getname` will be used. When the source IP address and port is obtained, the original `inet_getname` function will be invoked first, and then it will be checked whether `sk_user_data` is empty. If real IP and port can be extracted from this field, the returned values of `inet_getname` will be replaced with these two values.

The client program calls `getpeername` in the user mode, and the client's original IP and port will be returned.

Kernel package installation steps

CentOS 6.x/7.x

1. Download the installation package:
   - Download for CentOS 6.x
   - Download for CentOS 7.x
2. Install the package file.

```
rpm -hiv kernel-2.6.32-220.23.1.el6.toa.x86_64.rpm --force
```

3. Reboot the server after the installation is completed.

```
reboot
```

4. Run the following command to check whether the TOA module is successfully loaded.

```
lsmod | grep toa
```

5. If not, manually start it.

```
modprobe toa
```

6. Run the following command to enable automatic loading of the TOA module.

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Ubuntu 16.04

1. Download the installation package:
   - Download the kernel package
   - Download the kernel header package
2. Run the following command:

```
dpkg -i linux-image-4.4.87.toa_1.0_amd64.deb
```

The header package is optional. If needed for relevant development, install it.

3. After the installation is completed, reboot the server, then run the `lsmod | grep toa` command to check whether the TOA module is loaded, and if not, start it by running the `modprobe toa` command.
   Run the following command to enable loading of the TOA module:

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Debian 8

1. Download the installation package:
   - Download the kernel package
   - Download the kernel header package
2. The installation method is the same as that for Ubuntu.
   Please download the appropriate kernel package according to the type and version of the Linux OS of your business server and follow the steps below. If there is no kernel package for your OS, please see the **TOA source code installation guide** below.

TOA source code installation guide

Source code installation

1. Download the source code package containing the TOA patch and click the TOA patch to download the installation package.
2. Decompress it.
3. Edit `.config` by changing `CONFIG_IPV6=M` to `CONFIG_IPV6=y` .
4. If you need to add some custom descriptions, you can edit `Makefile` .
5. Run `make -jn` (n is the number of threads).
6. Run `make modules_install` .
7. Run `make install` .
8. Modify `/boot/grub/menu.lst` by changing `default` to the newly installed kernel (the `title` order starts at 0).
9. Reboot and the kernel will have TOA.
0. Run `lsmode | grep toa` to check whether the TOA module is loaded, and if not, start it by running `modprobe toa` .

Kernel package production

You can make your own rpm package or use the one we provide.

1. Install `kernel-2.6.32-220.23.1.el6.src.rpm` .

```
rpm -hiv kernel-2.6.32-220.23.1.el6.src.rpm
```

2. Generate the kernel source code directory.

```
rpmbuild -bp ~/rpmbuild/SPECS/kernel.spec
```

3. Copy the source code directory.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/ cp -a linux-2.6.32-220.23.1.el
6.x86_64/ linux-2.6.32-220.23.1.el6.x86_64_new
```

4. Apply the TOA patch to the copied source directory.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64
_new/
patch -p1 < /usr/local/src/linux-2.6.32-220.23.1.el6.x86_64.rs/toa-2.6.32-220.2
3.1.el6.patch
```

5. Edit `.config` and copy it to the `SOURCE` directory.

```
sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config
echo -e '\n# toa\nCONFIG_TOA=m' >> .config
cp .config ~/rpmbuild/SOURCES/config-x86_64-generic
```

6. Delete `.config` from the original source code.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64

rm -rf .config
```

7. Generate the final patch.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/
diff -uNr linux-2.6.32-220.23.1.el6.x86_64 linux-2.6.32-220.23.1.el6.x86_64_ne
w/ >
~/rpmbuild/SOURCES/toa.patch
```

8. Edit `kernel.spec` .

```
vim ~/rpmbuild/SPECS/kernel.spec
```

Add the following lines to `ApplyOptionPath` (you can also modify the names of custom kernel packages such as `buildid`):

```
Patch999999: toa.patch
ApplyOptionalPatch toa.patch
```

9. Make an rpm package.

```
rpmbuild -bb --with baseonly --without kabichk --with firmware --without debugi
nfo --target=x86_64 ~/rpmbuild/SPECS/kernel.spec
```

0. Install the kernel rpm package.

```
rpm -hiv kernel-xxxx.rpm --force
```

1. Reboot to load the TOA module

Using Website Traffic Forwarding Rules

When Anti-DDoS Advanced uses website traffic forwarding rules, the `X-Forwarded-For` field in the HTTP header can be used to get the real client IP.

`X-Forwarded-For` is an extended field in the HTTP header used to enable the server to identify the real IP of the clients accessing the server through proxies.

Format:

`X-Forwarded-For: Client, proxy1, proxy2, proxy3……`

When forwarding the user access request to the real server, Anti-DDoS Advanced will record the real IP of the requesting user at the beginning of the `X-Forwarded-For` field. Therefore, the application on the real server only needs to get the content of the `X-Forwarded-For` field in the HTTP header.

For more information, please see How to Get Real Client IP Based on Layer-7 Forwarding Rules.

Real Server-based Defense Scheduling Solution

Last updated：2020-05-09 18:03:49

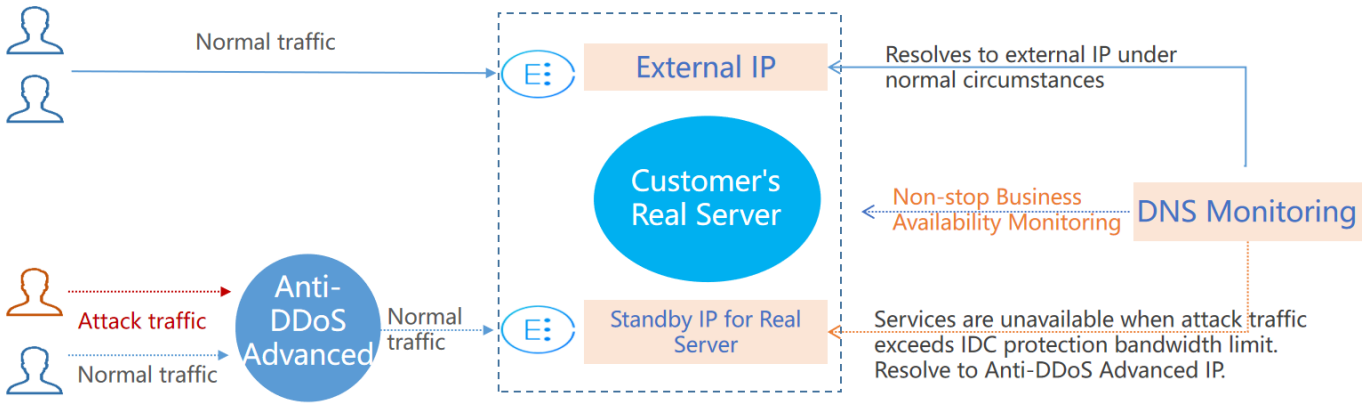
Background

You may consider real server-based protection scheduling if your customers have low tolerance for connection latency or if your business requires normal traffic to directly access the real server.
This scheme can quickly schedule protection after attacks occur, while allowing normal traffic to access the real server.

Protection Scheme

The figure below illustrates how real server-based protection scheduling works:

> This scheme requires monitoring and intelligent switching provided by DNS service providers.



Scheme Description

To implement this scheme, you need an Anti-DDoS Advanced IP, a DNS monitor, an external business IP, and a standby IP of the real server.

- Under normal circumstances, your business domain name is resolved to the outbound IP. Requests access the real server directly. DNS monitors watch over whether the applications are accessible on the real server in real time. As soon as the DNS monitor detects that the outbound IP is not accessible, DNS will resolve the business domain name to the Anti-DDoS Advanced IP according to the preset switching rules. Anti-DDoS Advanced will cleanse and remove the attack traffic and forward normal traffic to the standby IP of the real server, thus ensuring service availability.

  > To avoid faulty switching caused by uncontrollable factors such as network jitter, manual switching is recommended.

Benefits

- Meets the needs of direct access to the real server under normal circumstances.
- Applies to businesses that require very low connection latency.
- When the traffic volume is beyond the protection capability of the real server, the domain name will be automatically resolved to the Anti-DDoS Advanced IP.

Tips and Precautions

- Configure the forwarding rules of real server standby IP and Anti-DDoS Advanced IP in advance.
- Deploy the standby IP and primary IP of the real server with different physical addresses for better protection results.
- Practice and test regularly and familiarize yourself with scheme details to solve potential problems.

Suggestions on Stress Test

Last updated：2020-05-09 18:03:49

A stress test is designed to simulate DDoS attacks. To ensure the quality of the test, you are recommended to read this document carefully before conducting a stress test.

> The following suggestions are mainly about the impact of DDoS protection on stress testing. You may also need to consider other test-related factors, such as network bandwidth, linkage loads, and other basic resources.

Adjusting Protection Policies

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

Limiting Traffic and Number of Requests in Stress Test

- The bandwidth of your stress test should be lower than 1 Gbps; otherwise, attack protection may be triggered.
- The number of HTTP requests in your stress test should be no more than 20,000 requests per second (QPS); otherwise, attack protection may be triggered.
- The number of new connections established per second, the maximum number of connections, and the number of inbound packets per second in your stress test should be less than 50,000, 2,000,000, and 200,000, respectively.

> If the traffic and number of requests in your stress test will exceed the above ranges, please contact Tencent Cloud Technical Support. We will offer support during your stress test.

Evaluating Impact of Stress Test in Advance

You are recommended to contact Tencent Cloud solution architects or Tencent Cloud Technical Support before you conduct the stress test to evaluate possible consequences and develop risk aversion measures.