DDoS 高防 IP 专业版

最佳实践

产品文档

腾讯云

文档目录

最佳实践
平滑切换线上业务至 DDoS 高防 IP 专业版

最近更新时间：2020-03-10 18:35:33

需求背景

已上线的业务可能存在较多的特定设置和限制条件，且业务中断影响较大。因此建议用户将已上线运行的业务切换到本产品之前，参考本节相关建议，采用合适的切换方式，规避可能存在的风险。

建议

> 注意：
> 以下建议是基于腾讯云过往线上业务切换而总结的相关经验，用户需结合自身实际业务情况进行完善和补充，确保将切换过程中的风险降至最低。

技术维度

1. 通过本地修改 hosts 文件来替代直接修改 DNS A 记录，由测试人员本地进行业务测试，验证可用性，测试延时等相关指标。
2. 若已使用智能域名解析产品，可基于部分运营商或部分地域进行 DNS A 记录修改，先小范围将流量牵引到高防 IP 灰度上线再逐步完成全部业务切换。
3. 减小 DNS 的 TTL，一旦出现问题可尽快切回。
4. 提前准备回退方案，一旦出现问题可根据回退方案有序操作。

业务维度

1. 选取备份业务、非重要业务、非关键业务先进行迁移。
2. 选择业务较少的时段进行迁移。

源站 IP 暴露的解决方法

最近更新时间：2019-12-23 15:44:20

由于部分攻击者会记录源站使用过的 IP，因此在使用 DDoS 高防 IP 专业版 后，如果还存在绕过高防直接攻击源站 IP 的情况，建议更换源站 IP。
如不想更换源站 IP 或已经更换过 IP但仍存在 IP 暴露情况，为防止出现攻击绕过高防直接攻击源站 IP 的情况，强烈参考下面方法以保护源站 IP：

- 不使用与旧源站 IP 相同或相近网段的 IP 作为新的源站 IP，避免攻击者对 C 段或相近网段进行猜测和扫描。
- 提前准备备份链路和备份 IP。
- 设置访问来源范围，避免攻击者的恶意扫描。
- 参考 与源站结合的防护调度方案，结合实际情况进行应用。

> 说明：
> 更换源站 IP 之前，请务必确认已消除所有可能暴露源站 IP 的因素。

在更换源站 IP 前可参考下列检查方法，对暴露源站 IP 的可能因素进行逐一排查，避免新更换的源站 IP 继续暴露。

检查方法

DNS 解析记录检查

检查该遭到攻击的旧源站 IP 上所有 DNS 解析记录，如子域名的解析记录、邮件服务器 MX（Mail Exchanger）记录以及 NS（Name Server）记录等，确保全部配置到 DDoS 高防 IP 专业版，避免部分解析记录直接解析成新更换的源站 IP。

信息泄露及命令执行类漏洞检查

- 检查网站或业务系统是否存在信息泄露的漏洞，如 phpinfo() 泄露、GitHub 信息泄露等。
- 检查网站或业务系统是否存在命令执行类漏洞。

木马、后门检查

检查源站服务器是否存在木马、后门等隐患。

获取客户端真实 IP

最近更新时间：2020-03-05 17:11:01

DDoS 高防 IP 专业版使用非网站业务转发规则，源站需使用 toa 模块获取客户端的真实 IP。

业务请求经过高防 IP 的 4 层转发后，业务服务器端接收到报文后，其看到的源 IP 地址是高防 IP 的出口 IP 地址。为了让服务器端能够获取到用户端实际的 IP 地址，可以使用如下 TOA 的方案。在业务服务的 Linux 服务器上，安装对应的 TOA 内核包，并重启服务器后。业务侧就可以获取到用户端实际的 IP 地址。

TOA 原理

高防转发后，数据包同时会做 SNAT 和 DNAT，数据包的源地址和目标地址均修改。
TCP 协议下，为了将客户端 IP 传给服务器，会将客户端的 IP，port 在转发时放入了自定义的 tcp option 字段。

```
#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;
};
```

Linux 内核在监听套接字收到三次握手的 ACK 包之后，会从 `SYN_REVC` 状态进入到 `TCP_ESTABLISHED` 状态。这时内核会调用 `tcp_v4_syn_recv_sock` 函数。 Hook 函数 `tcp_v4_syn_recv_sock_toa` 首先调用原有的 `tcp_v4_syn_recv_sock` 函数，然后调用 `get_toa_data` 函数从 TCP OPTION 中提取出 TOA OPTION，并存储在 `sk_user_data` 字段中。

然后用 `inet_getname_toa hook inet_getname` ，在获取源 IP 地址和端口时，首先调用原来的 `inet_getname` ，然后判断 `sk_user_data` 是否为空，如果有数据从其中提取真实的 IP 和 port，替换 `inet_getname` 的返回。

客户端程序在用户态调用 getpeername，返回的 IP 和 port 即为客户端的原始 IP。

内核包安装步骤

Centos 6.x/7.x

安装步骤

1. 下载安装包
   (1) Centos 6.x 下载
   (2) Centos 7.x 下载

2. 安装包文件

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

3. 安装完成之后重启主机

```
reboot
```

4. 执行命令检查 toa 模块是否加载成功

```
lsmod | grep toa
```

5. 没有加载的话手工开启

```
modprobe toa
```

6. 可用下面的命令开启自动加载 toa 模块

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

Ubuntu 16.04

下载安装包：
(1) 内核包下载
(2) 内核 header 包下载
安装步骤：

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

Headers 包可不装，如需要做相关开发则安装。
安装完成之后重启主机，然后 lsmod | grep toa 检查 toa 模块是否加载 没有加载的话 modprobe toa 开启。
可用下面的命令开启加载 toa 模块

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

Debian 8

(1) 内核包下载
(2) 内核 header 包下载

安装方法与 Ubuntu 相同。

请根据业务服务器 Linux 操作系统的类型和版本下载对应的内核包，按如下步骤操作。如果没有和用户操作系统一致的内核包，用户还可以参考下面 TOA 源代码安装指引操作。

TOA 源代码内核安装指引

源码安装

1. 下载打好 toa 补丁 的源码包，单击 toa 补丁即可下载安装包。
2. 解压。
3. 编辑 .config，将 CONFIG_IPV6=M 改成 CONFIG_IPV6=y 。
4. 如果需要加上一些自定义说明，可以编辑 Makefile。
5. make -jn (n 为线程数)。
6. make modules_install 。
7. make install 。
8. 修改 /boot/grub/menu.lst 将 default 改为新安装的内核（title 顺序从 0 开始）。
9. Reboot 重启后即为 toa 内核。
0. lsmode | grep toa 检查 toa 模块是否加载 没有加载的话 modprobe toa 开启。

内核包制作

可自己制作 rpm 包，也可由我们提供。

1. 安装 kernel-2.6.32-220.23.1.el6.src.rpm

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

2. 生成内核源码目录

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

3. 复制一份源码目录

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

4. 在复制出来的源码目录中打 toa 补丁

```
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-2.6.32-220.23.1.el6.patch
```

5. 编辑.config 并拷贝到 SOURCE 目录

```
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. 删除原始源码中的.config

```
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. 生成最终 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_new/ >
~/rpmbuild/SOURCES/toa.patch
```

8. 编辑 kernel.spec

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

在ApplyOptionPath 下添加如下两行（还可修改 buildid 等自定义内核包名）

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

9. 制作 rpm 包

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

0. 安装内核 rpm 包

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

重启，加载 toa 模块

与源站结合的防护调度方案

最近更新时间：2020-03-10 18:34:03

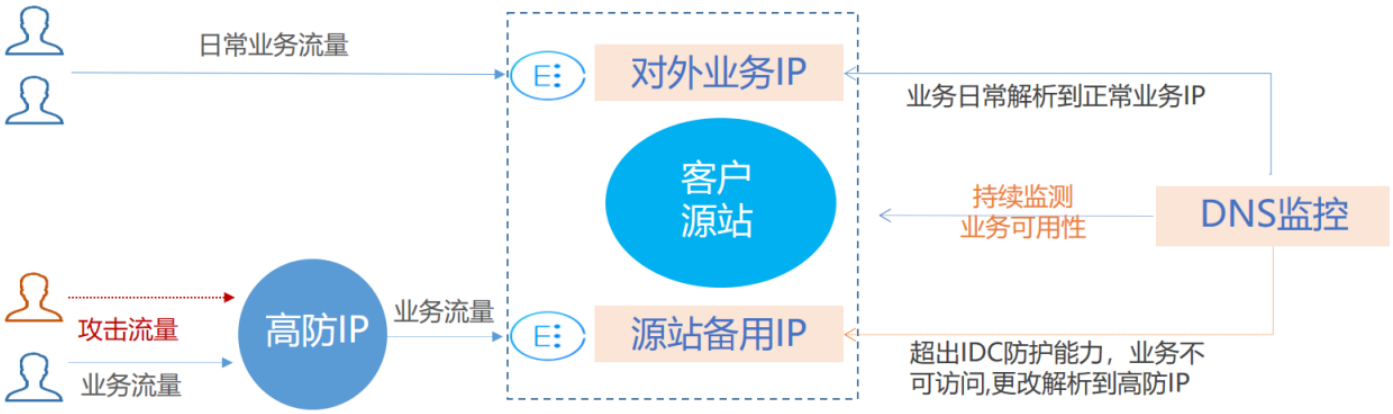
需求背景

部分用户业务对延时要求严格，或者受限于业务要求常态化情况下必须直接访问源站，此时可考虑结合源站的防护调度方案。
该方案可满足流量常态化情况下直接访问源站，但遭到攻击后可迅速具备防护能力的要求。

防护方案

与源站结合的防护调度方案如下图：

> 说明：
> 本方案依赖于 DNS 服务商，需要具备监控和智能切换功能。



方案说明

本方案主要由高防 IP、DNS 监控、客户源站的对外业务 IP 和源站备用 IP 组成。

- 常态化情况下，业务的域名解析到正常的对外业务 IP，业务流量直接访问源站。DNS 监控实时监控源站业务是否可以正常访问。
- 当 DNS 监控检测到正常的对外业务 IP 无法访问时，依据智能切换的设置规则，迅速将业务域名解析到高防 IP 上。高防 IP 对攻击流量进行清洗，将干净的业务流量转发到源站的备用 IP，从而保障业务可用。

> 注意：
> 为避免由于网络抖动等因素造成的误切换，为确保监控效果，建议进行手动切换。

方案效果

- 满足常态化情况下直接访问源站的需求。
- 适用于对延时要求非常严格的业务。
- 遭到攻击超出源站防护能力后，可自动切换到高防 IP 进行防护。

建议与注意事项

1. 需提前完成源站备用 IP、高防 IP 转发规则等配置。
2. 建议将源站备用 IP 与正常的业务 IP 分布在不同的物理线路，以获得更好的防护效果。
3. 建议定期进行验证和演练，熟悉方案细节，解决可能存在的问题。

业务系统压力测试建议

最近更新时间：2020-03-10 18:32:57

压力测试的过程在一定程度上与 DDoS 攻击类似，为确保压力测试取得相应效果，建议用户在进行压力测试前先参考本文档获取适用的建议，再拟定合适实施方案。

> 注意：
> 以下建议主要是基于 DDoS 防护对压力测试的影响而提出。其他与压力测试有关的方面，如网络带宽、链路负载或其他基础资源情况等，请用户结合实际情况考虑和补充。

调整防护策略

- 建议关闭 CC 防护策略，如存在某些客观原因不能关闭 CC 防护策略，请将 CC 攻击防护的 HTTP 请求数阈值调整到压测最大值以上。
- 建议关闭 DDoS 防护策略，如存在某些客观原因不能关闭 DDoS 防护策略，请将 DDoS 防护的清洗阈值调整到压测最大值以上。

控制压测流量及请求数

- 建议将压测流量值小于1Gbps，否则将有可能触发攻击防护。
- 建议将压测的 HTTP 请求数限制在20,000QPS以内（即 HTTP 请求数每秒不超过20,000个），否则将有可能触发攻击防护。
- 建议将压测的每秒新建连接数小于50,000个，最大连接数小于2,000,000个，每秒入包量小于200,000个。

> 注意：
> 如压测需要超出以上限制范围，请联系 腾讯云技术支持，售后团队将配合进行压测工作。

提前评估压测可能的影响

建议用户在压测前联系腾讯云架构师或 腾讯云技术支持，全面评估压测可能产生的影响及范围，制定合理的风险规避措施。