目录

使用高防会影响网站SEO吗？

不会，使用高防IP不会影响网站的SEO。高防IP帮助用户免受因流量攻击导致的网站服务中断，将SEO波动的风险降到最低。相反，若不采取积的防御手段，当遭遇大规模流量攻击时，网站的访问响应延迟或服务器宕机，会对网站SEO、排名产生非常大的影响。

使用高防会影响网站备案吗？

不会，高防为网络在线业务提供安全防御，不影响用户网站所在的机房，不会影响网站的备案。

高防的CC防护会产生额外费用吗？

不会，每一个购买了高防IP的域名都默认具有CC防护的功能，用户可以在控制台选择开启或关闭CC防护。

高防过期后可以续费吗？

高防2.0过期后7天内仍可续费，超过7天金山云会释放用户在此IP下的数据。

域名能否直接A记录指向高防？

请勿通过A记录方式直接将域名指向高防IP，此种方法风险极高，为保障您的网站业务正常运行，请谨慎选择。

为何开通高防后ping出来的不是源站IP？

如果站点接入了高防IP，那么PING网站的站点域名显示出来的IP会是高防云端节点的IP，网站真实IP被隐藏，提高安全性。

如何在服务器获取用户真实IP？

使用高防IP后，网站服务器访问日志中的IP地址都将记录为高防的IP地址，无法取得客户端的真实IP地址。

网站业务获取用户真实IP

在高防IP转发的HTTP头信息中增加 header头信息，这时web服务器的日志就可以记录远程客户端的真实IP。

Nginx格式如下：

```
'$http_x_forwarded_for - $remote_user [$time_local] "$request" ''$status $body_bytes_sent "$http_referer"'
 '"$http_user_agent" ';
```

Apache格式如下：

```
LogFormat "%{X-FORWARDED_FOR}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
```

—— ASP

```
Request.ServerVariables("X_FORWARDED_FOR")
```

——PHP

```
$_SERVER["HTTP_X_FORWARDED_FOR"]
```

——JSP

```
request.getHeader("X_FORWARDED_FOR")
```

非网站业务获取用户真实IP

以下方法支持操作系统为 CentOS 或 Fedora 的源站服务器获取真实访问IP，其他操作系统请联系技术支持确认

1.uname -r 查看主机内核版本

```
[root@vm172-31-120-8 ~]# uname -r
2.6.32-696.18.7.el6.x86_64
```

2.下载内核对应的rpm包

2.6.32_358

2.6.32_504

2.6.32_696

3.10.0_229

3.10.0_327

3.10.0_514

3.10.0_693

- 安装rpm包

```
[root@vm172-31-120-8 ~]# rpm -ivh kmod-kgwttm-1.0-nogit.2.6.32_696.x86_64.rpm
```

若您的内核版本不在以上列表中，可通过源码编译安装，Centos安装步骤参考如下(其他操作系统请联系售后技术人员)：

第一步，查看系统内核版本

例如内核版本为3.10.0-957.1.3.el7.x86_64

```
# uname -r
# 3.10.0-957.1.3.el7.x86_64
```

第二步，下载对应的内核RPM包

下载centosrpm包，从中找到对应内核版本的RPM

如未找到可从centos官方获取 https://wiki.centos.org/HowTos/I_need_the_Kernel_Source

```
# rpm -ivh kernel-devel-3.10.0-327.el7.x86_64.rpm
```

第三步，安装依赖环境

```
# sudo yum install rpm-build redhat-rpm-config asciidoc hmaccalc perl-ExtUtils-Embed pesign xmlto
$ sudo yum install audit-libs-devel binutils-devel elfutils-devel elfutils-libelf-devel gcc
$ sudo yum install ncurses-devel newt-devel numactl-devel pciutils-devel python-devel zlib-devel
```

第四步，编译&安装TTM模块

下载ttm源码

```
# unzip centos-kgwttm_v4.zip
# cd kgwttm
# ./build.sh
# rpm -ivh *.rpm
# sh /usr/local/bin/kgwttm-insmod.sh
# lsmod |grep kgwttm
```

基础防护防护规则

1. **若金山云监控到用户使用的金山云产品遭受DDoS攻击：**

- 攻击流量峰值在5Gbps以下时，将为用户提供不超过15分钟的基础防护，超出15分钟后攻击流量仍然存在的，将对受攻击的服务器的EIP进行黑洞；
- 攻击流量峰值在5Gbps以上时，将立即进行流量黑洞操作，黑洞时长至少24小时，具体时长依据攻击流量大小而定；
- 若同一产品一周内遭受两次或两次以上的DDoS攻击，将禁止用户更换绑定此产品的EIP。若用户坚持继续更换EIP，金山云将强制进行EIP解绑操作，或针对遭受攻击的云服务器进行黑洞操作。用户更换EIP的行为若影响到金山云服务可用性或影响贵方之外的金山云其他客户，金山云保留向贵方追责的权利。

2. **若金山云监控到用户的云服务器被入侵：**

- 若攻击者入侵云服务器或入侵后利用该服务器对外实施攻击行为（包括但不限于扫描破解、发送垃圾邮件等），金山云将立即通知用户，请用户务必在一小时内自行采取措施进行处理，如一小时后该云服务器仍未停止被入侵，金山云将对该云服务器进行强制EIP解绑操作；
- 若攻击者入侵云服务器或入侵后利用该服务器对外发起DDoS攻击，金山云将直接强制关闭用户的该云服务器，并在强制关闭后通知用户。

详情请参考《金山云基础防护服务使用协议》