业务配置DDoS高防后，如果存在攻击绕过DDoS高防直接攻击源站的情况，说明源站IP地址可能已经暴露，需要您更换源站服务器的IP地址。

**排查源站IP暴露的原因**

更换源站服务器的IP地址前，请务必确认您已经消除了所有可能暴露源站IP的因素，避免源站IP更换后再次暴露。您可以从以下方面进行排查：

* 源站服务器上是否存在木马、后门等安全隐患。

推荐您使用阿里云云安全中心服务检查和修复服务器的安全漏洞。更多信息，请参见[什么是云安全中心](https://help.aliyun.com/document_detail/42302.html#concept-bjv-y5w-ydb)。

* 源站服务器上是否存在没有配置DDoS高防的其他服务，例如邮件服务器的MX记录、BBS记录等除Web记录以外的记录。

**注意** 请仔细检查网站域名的DNS解析记录，确认没有任何记录直接解析到源站服务器的IP地址。

* 是否存在网站源码信息泄露。例如phpinfo()指令中可能包含的IP地址等泄露。
* 是否存在恶意扫描。您可以在配置DDoS高防后设置源站保护，在源站服务器上只放行DDoS高防回源IP的入方向流量。具体操作请参见[配置DDoS高防后设置源站保护](https://help.aliyun.com/document_detail/40525.html#concept-40525-zh)。

**更换源站IP**

确认已消除所有可能暴露源站IP的因素后，您可以更换源站服务器的IP地址。具体操作请参见[更换 ECS IP](https://help.aliyun.com/document_detail/51004.html?spm=a2c4g.11186623.2.14.252c74a62CbybC#task650)。

如果您不想更换源站IP或已经更换过源站IP但是仍存在IP暴露的情况，建议您在后端ECS服务器前部署一台负载均衡SLB服务器（具体操作请参见[负载均衡快速入门](https://help.aliyun.com/document_detail/86456.html#concept-ybd-pfl-vdb)）。您可以使用以下网络架构：客户端->DDoS高防->SLB->ECS。

采用这种架构后，即使攻击者直接攻击源站，导致源站IP被黑洞，通过DDoS高防访问服务器依然不受影响。因为负载均衡服务器到源站的访问流量通过内网传输，即使源站IP被黑洞，DDoS高防实例的IP仍然可以通过负载均衡服务器访问源站。