1. **高防验证配置生效**

在云盾DDoS防护管理控制台配置完成后，DDoS高防预期可以把请求高防IP对应端口的报文转发到源站（真实服务器）的对应端口。为了最大程度保证业务的稳定，我们建议在全面切换业务之前先进行本地的测试。

1. **直接用IP访问（不需要域名）的业务**

有的四层业务（如游戏业务）可能不需要域名，是直接通过IP来进行交互的。

例如，高防IP是99.99.99.99，配置了端口1234的转发，源站IP是11.11.11.11，对应服务端口也是1234。在完成前两步的配置后，可以直接本地通过telnet命令访问高防IP 99.99.99.99的1234端口，telnet命令能连通则说明转发成功。

或者，如果能在本地客户端直接填写服务器IP，也可以直接填入高防IP进行测试。

1. **需要用域名访问的四层业务**

对于需要通过域名来访问的业务（如客户端中使用的服务器地址是域名而不是IP），可通过以下两种方法来验证配置是否生效：

* 修改本地hosts文件

1. 首先修改本地hosts文件 ，使本地对于被防护站点的请求经过高防。

以Windows操作系统为例：

1. 找到Hosts文件。一般Hosts文件在 C:\Windows\System32\drivers\etc\ 文件夹中。
2. 用记事本或Notepad++等文本编辑器，打开hosts文件。
3. 在最后一行添加如下内容：高防IP地址 网站域名。 以“www.aliyundemo.com”为例，在hosts文件最后一行添加如下内容：



1. 修改hosts文件后保存。
2. 在本地计算机对被防护的域名运行Ping命令。

预期解析到的IP地址是在hosts文件中绑定的高防IP地址。如果依然是源站地址，可尝试刷新本地的DNS缓存（在Windows的命令提示符中运行ipconfig/flushdns命令。）

1. 确认本地解析已经切换到高防IP以后，使用原来的域名进行测试，如果能正常访问则说明配置已经生效。

* 直接通过CNAME地址访问服务器

如果客户端支持填写服务器域名，可以把原来的域名替换成DDoS高防服务已分配的接入CNAME地址，测试访问是否正常。

如果无法正常访问，请确认步骤1、步骤2中的配置是否正确。如问题依然存在，请联系阿里云售后支持。