**奇安信安域**

**网站云防护实施方案**

目录

[1 准备 3](#_Toc12540199)

[2 接入测试 3](#_Toc12540200)

[2.1 绑定host 3](#_Toc12540201)

[3 IP加白 4](#_Toc12540202)

[4 防护接入 4](#_Toc12540203)

[4.1 CNAME接入 5](#_Toc12540204)

[4.2 NS接入 5](#_Toc12540205)

[4.3 防护接入验证 5](#_Toc12540206)

[5 退出防护 6](#_Toc12540207)

[6 修改DNS解析记录示例 6](#_Toc12540208)

[7 网站接入安域后，如何获取客户端真实IP 11](#_Toc12540209)

[ASP 11](#_Toc12540210)

[PHP 12](#_Toc12540211)

[JSP 12](#_Toc12540212)

[Tomcat 12](#_Toc12540213)

# 准备

1. PC机或笔记本电脑，需能连接互联网；
2. 需拥有网站的DNS修改权限；
3. 需拥有数据中心防火墙、WAF等网关类设备的管理配置权限；
4. 如安装主机防护软件，需有该软件的管理配置权限。

# 接入测试

## 绑定host

通过在业务电脑上修改本机的hosts文件绑定域名指向安域节点，从而事先测试可否正常访问，方法如下:

修改了本机的hosts文件就是通过本机DNS强制指向这个节点，并通过节点去访问网站。前提是用户服务器上没有对IP做限制，可以用来确定通过节点IP访问源站是否有问题。

**第一步：**Windows环境hosts文件：C:\Windows\System32\drivers\etc\

**第二步：**hosts文件打开与编辑：hosts文件是一个纯文本的文件，用普通的文本编辑软件如记事本等都能打开和编辑。

绑定以下IP地址进行测试：

|  |  |
| --- | --- |
| **链路性质** | **IP地址** |
| 福州移动 |  112.49.21.33 |
| 武汉联通 | 122.190.204.33 |
| 江苏电信 | 61.160.224.32 |

**第三步：**绑定安域测试节点IP测试：新起一行添加安域测试节点IP地址与需要接入防护的网站地址，例如（可以ping CNAME值，返回得IP可以绑定hosts测试）



确认后保存、退出。（注意：没有#号）

**第四步：**验证绑定后：通过ping命令，探测网站解析情况，当ping返回的结果是之前绑定的网站IP地址，说明绑定成功。



**第五步：**hosts文件绑定成功后，可在浏览器内输入网站地址模拟网站接入防护后访问页面是否正常,如若浏览器访问网站以及各项功能测试正常后可在域名解析商处修改解析。

# IP加白

该IP列表为安域的防护节点IP，接入安域之后，这些IP将与源站进行交互。当源站服务器或源站服务器所在的机房存在WAF及防火墙设备（包括安全软件）时，在相应安全设备（安全软件）上加白所用，接入安域后源站会收到来自相同IP的大量请求，会触发拦截规则，为避免安域的节点IP被源站设备拦截，导致节点回源站服务器取数据失败，产生快照或者502报错页面。安域IP段列表如下（包含重保镜像功能的爬虫IP）：

|  |  |
| --- | --- |
| 61.160.224.0-61.160.224.255223.111.128.0-223.111.128.255123.6.81.0-123.6.81.25542.81.56.2-42.81.56.11112.49.21.1-112.49.21.128117.139.143.128-117.139.143.255122.190.204.0-122.190.204.128111.206.216.0-111.206.216.255101.227.92.0-101.227.92.255121.32.243.0-121.32.243.255219.153.112.0-219.153.112.255223.95.33.0-223.95.33.15124.232.185.0-124.232.185.128120.201.117.128-120.201.117.255101.66.188.16-101.66.188.312409:8C14:F1A:8702::/120240e:978:0303::/48 | 183.131.156.208-183.131.156.223113.105.224.32-113.105.224.39120.83.13.176-120.83.13.183183.232.204.160-183.232.204.16743.247.89.32-43.247.89.3936.27.212.0-36.27.212.25561.174.41.0-61.174.41.128101.227.27.69, 101.227.27.84101.227.27.92,101.227.27.94210.52.224.184,210.52.224.186210.52.224.188,210.52.224.189210.52.224.143, 211.95.50.4211.95.50.5, 211.95.50.7211.95.50.8 |

# 防护接入

**以下接入方式详情请参考附件。**

温馨提示：多数域名注册商每天仅允许修改一次域名DNS，请谨慎修改，以免造成域名解析失败，网站无法访问的问题。

##  CNAME接入

接入时需要在权威DNS处（一般为域名注册商），把需要接入防护的子域名修改解析记录，做CNAME记录指向提供的记录值（见附件） (如DNS服务器有bind规则，请在记录值最后加一个点)，然后等待生效。即把原有域名对应的DNS A记录删除，新建指向安域的CNAME记录值（如果DNS解析商支持直接修改A记录为CNAME记录也可以）。

##  NS接入

需要修改域名解析DNS服务器为安域的，修改为以下地址：ns1.qaxanyu.com及ns2.qaxanyu.com。在DNS服务器修改前，所有的域名解析记录均需在安域平台进行完整配置，不能遗漏，而原域名DNS解析面板的所有解析将在DNS授权缓存到期后失效，各地解析因缓存问题可能会陆续失效，失效后将自动以安域的DNS解析为准。缓存时间大约为0-72小时。

温馨提示：CNAME与NS是两种接入方式，不需要两种方式都修改，默认是CNAME接入，只修改CNAME值即可。

##  防护接入验证

工具/命令：nslookup

通过nslookup命令查看待测域名的ns记录，成功接入后可看到如下图所示的带有qax关键字的name server。

命令格式：nslookup -qt=ns 待测具体域名



工具/命令：ping

在cmd命令行ping待测域名，可以看到解析的ip已非源站ip。



# 退出防护

可以通过两种方式退出安域防护系统，第一种方式：在安域平台-系统配置-策略配置-一键设置-选择开启一键回源，即可关闭防护，一般10分钟内生效，之后用户解析到的地址为源站IP。



第二种方式：将DNS的解析地址修改为该域名原有a记录。

# 修改DNS解析记录示例

**一 CNAME接入**

操作步骤，以阿里云作为域名提供商的域名管理系统为例。

1 登录域名控制台，进入到【云解析DNS】--【解析设置】



2 对A记录(cname记录)的zacn,点击【修改】





3 修改记录类型为CNAME，修改记录值为安域提供的cname值，



1. 修改完毕后的记录



注意，如果DNS服务器有bind规则，则需要在cname值后面加”.”

1. 验证修改是否成功

等待10分钟左右，具体时间视TTL而定，点击windows左下角的“开始”----“运行”----输入cmd,回车

在弹出的窗口内输入nslookup回车，再输入域名，非权威应答显示的为安域的CNAME值,address变为安域ip,是表示接入成功。



**二 NS接入方式**

操作步骤，以万网作为域名提供商的域名管理系统为例。

1 登录域名控制台，进入到【域名列表】--【管理】



2 点击【DNS修改】--【修改DNS服务器】



3 填写安域的DNS服务器，ns1.qaxanyu.com和ns2.qaxanyu.com。



4 确认更改成功



由于不同域名后缀的注册商缓存时间的限制，成功切换DNS服务器为安域DNS可能存在12-72小时的等待时间。

5验证修改是否成功

点击windows左下角的“开始”----“运行”----输入cmd,回车

在弹出的窗口内输入nslookup -qt=ns 域名。非权威应答显示的为ns1.qaxanyu.com以及ns2.qaxanyu.com则修改成功。



注意：由于各厂商域名管理系统不同，以上截图只针对万网，实际操作界面以用户域名管理系统为准。

# 网站接入安域后，如何获取客户端真实IP

用户的真实ip被安域放在x-forward-for里面，可以通过下面的方法来获取:

### ASP

Request.ServerVariables("HTTP\_X\_FORWARDED\_FOR")

### PHP

$\_SERVER["HTTP\_X\_FORWARDED\_FOR"]

### JSP

request.getHeader("HTTP\_X\_FORWARDED\_FOR")

### Tomcat

1.在反向代理请求中有X-Forwarded-For的前提下，tomcat的配置文件server.xml中org.apache.catalina.valves.AccessLogValve的pattern中包含%{X-Forwarded-For}i即可在access log看到客户端的真实ip;

2.pattern="%{X\_Forwarded\_For}i|%t|%s|%S|%b|%D|%q|%T|%{Referer}i|%{User-Agent}i"/>