# 阿里云
# Web应用防火墙

## 最佳实践

文档版本：20181213

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式 | 说明 | 样例 |
| --- | --- | --- |
|  | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。 |  **禁止：**<br>重置操作将丢失用户配置数据。 |
|  | 该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。 |  **警告：**<br>重启操作将导致业务中断，恢复业务所需时间约10分钟。 |
|  | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 |  **说明：**<br>您也可以通过按**Ctrl** + **A**选中全部文件。 |
| > | 多级菜单递进。 | 设置 > 网络 > 设置网络类型 |
| 粗体 | 表示按键、菜单、页面名称等UI元素。 | 单击 **确定**。 |
| `courier` 字体 | 命令。 | 执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。 |
| 斜体 | 表示参数、变量。 | `bae log list --instanceid` *`Instance_ID`* |
| []或者[a\|b] | 表示可选项，至多选择一个。 | `ipconfig` *`[-all\|-t]`* |
| {}或者{a\|b} | 表示必选项，至多选择一个。 | `swich` *`{stand \| slave}`* |

# 目录

# 1 源站保护

正确配置源站ECS的安全组和SLB的白名单，可以防止黑客直接攻击您的源站IP。本文介绍了相关配置方法。

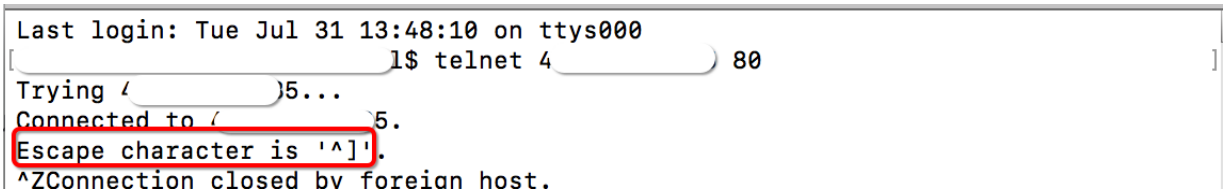
## 背景信息

> 说明：
> 源站保护不是必须的。没有配置源站保护不会影响正常业务转发，但可能导致攻击者在源站IP暴露的情况下，绕过Web应用防火墙直接攻击您的源站。

### 如何确认源站泄露

您可以在非阿里云环境直接使用Telnet工具连接源站公网IP地址的业务端口，观察是否建立连接成功。如果可以连通，表示源站存在泄露风险，如果黑客获取到源站公网IP就可以绕过WAF直接访问；如果无法连通，则表示当前不存在源站泄露风险。

例如，测试已接入WAF防护的源站IP 80端口和800端口是否能成功建立连接，测试结果显示端口可连通，说明存在源站泄露风险。




### 注意事项

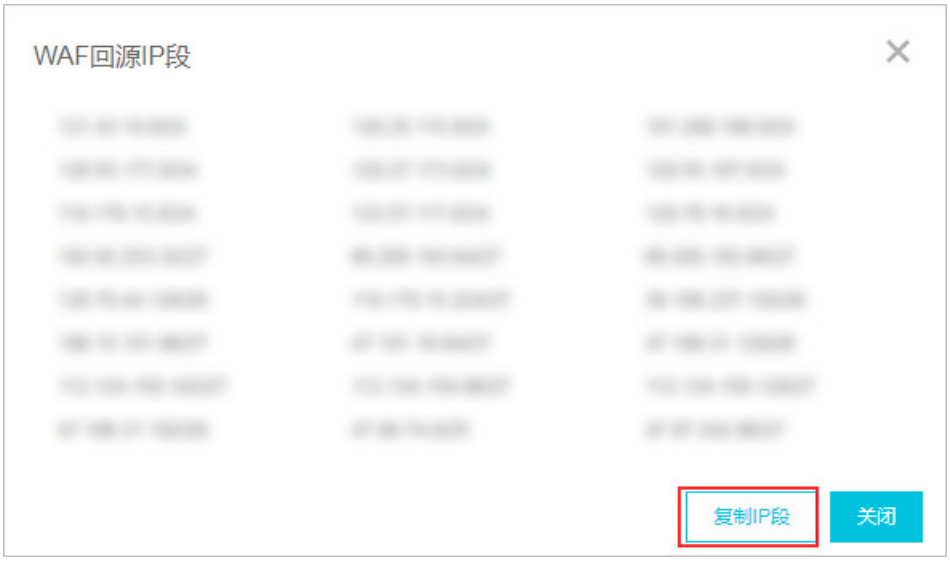
配置安全组存在一定风险。在配置源站保护前，请注意以下事项：

- 请确保该ECS或SLB实例上的所有域名都已经接入Web应用防火墙。
- 当Web应用防火墙集群出现故障时，可能会将域名访问请求旁路回源至源站，这种情况下，如果源站已配置安全组防护，可能会导致源站无法从公网访问。
- 当Web应用防火墙集群扩容新的回源网段时，如果源站已配置安全组防护，可能会导致频繁出现5xx错误。

## 操作步骤

1. 登录云盾*Web*应用防火墙控制台。
2. 前往**管理** > **网站配置**页面。
3. 单击**Web应用防火墙回源IP网段列表**，查看Web应用防火墙所有回源IP段。


4. 在**WAF回源IP段**对话框，单击**复制IP段**，复制所有回源IP。




5. 参照以下步骤，配置源站只允许WAF回源IP进行访问。

   - **源站是ECS**

     1. 前往*ECS* 实例列表，定位到需要配置安全组的ECS实例，单击其操作列下的**管理**。
     2. 切换到**本实例安全组**页面。
     3. 选择目标安全组，并单击其操作列下的**配置规则**。
     4. 单击**添加安全组规则**，并配置如下安全组规则：
        - **网卡类型**：公网
        - **规则方向**：入方向
        - **授权策略**：允许
        - **协议类型**：TCP
        - **授权类型**：地址段访问
        - **端口范围**：80/443
        - **授权对象**：粘贴步骤4中复制的所有Web应用防火墙回源IP段

- 优先级：1

5. 为所有Web应用防火墙回源IP段添加安全组规则后，再添加如下安全组规则，拒绝公网入方向的所有IP段访问，优先级为100。

   - 网卡类型：公网
   - 规则方向：入方向
   - 授权策略：拒绝
   - 协议类型：TCP
   - 端口范围：80/443
   - 授权类型：地址段访问
   - 授权对象：0.0.0.0/0
   - 优先级：100

   **说明：**

   如果本安全组防护的服务器还与其他的IP或应用存在交互，需要将这些交互的IP和端口通过安全组一并加白放行，或者在最后添加一条优先级最低的全端口放行策略。

- **源站是SLB**

  通过类似的方式，将Web应用防火墙的回源IP加入相应负载均衡实例的白名单，具体设置方法请参考设置负载均衡白名单访问控制。

  - 建立访问控制白名单
  - 添加WAF回源IP段
  - 选择配置的白名单

# 2 获取访问者真实IP

**在启用Web应用防火墙后，怎样获取访问者真实 IP**

很多时候，网站访问并不是简单地从用户的浏览器直达服务器，中间可能部署有CDN、WAF、高防。例如，采用这样的架构：用户 > CDN/WAF/高防 > 源站服务器。那么，在经过多层加速后，服务器如何获取发起请求的真实客户端 IP 呢？

一个透明的代理服务器在把用户的请求转到下一环节的服务器时，会在HTTP的头中加入一条**X-Forwarded-For**记录，用来记录用户的真实IP，其形式为`X-Forwarded-For:用户IP`。如果中间经历了多个代理服务器，那么X-Forwarded-For会表现为以下形式：`X-Forwarded-For:用户IP, 代理服务器1-IP, 代理服务器2-IP, 代理服务器3-IP, ……`。

因此，常见的应用服务器可以使用**X-Forwarded-For的方式获取访问者真实IP**。以下分别针对Nginx，IIS 6，IIS 7，Apache和Tomcat 服务器，介绍相应的X-Forwarded-For配置方案。

**Nginx配置方案**

**1. 确认http_realip_module模块已安装**

作为负载均衡，Nginx使用**http_realip_module**来获取真实IP。使用一键安装包安装的Nginx，默认没有安装该模块。您可以执行`# nginx -V | grep http_realip_module`命令查看该模块是否已安装。如果没有安装，则需要重新编译Nginx并加装该模块。

参考以下方法，安装**http_realip_module**模块：

```
wget http://nginx.org/download/nginx-1.12.2.tar.gz
tar zxvf nginx-1.12.2.tar.gz
cd nginx-1.12.2
./configure --user=www --group=www --prefix=/alidata/server/nginx --
with-http_stub_status_module --without-http-cache --with-http_ssl_m
odule --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

**2. 修改Nginx对应server的配置**

打开`default.conf`，在`location / {}`中添加如下内容：

```
set_real_ip_from ip_range1;
set_real_ip_from ip_range2;
...
set_real_ip_from ip_rangex;
```

```
real_ip_header    X-Forwarded-For;
```

其中，ip_range1，2，...，x 指WAF的回源IP地址，需要分多条分别添加。

**3.** 修改日志记录格式 **log_format**

*log_format*一般在nginx.conf中的http配置下。在*log_format*中，将*x-forwarded-for*字段加进去，替换掉原来的*remote-address*，即修改为以下内容：

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

完成以上操作后，使用nginx -s reload命令重启Nginx，使配置生效。

**IIS 6**配置方案

您可以选择从IIS 6日志中获取来访者真实IP地址，但前提是您已安装插件*F5XForwardedFor.dll*。

操作步骤

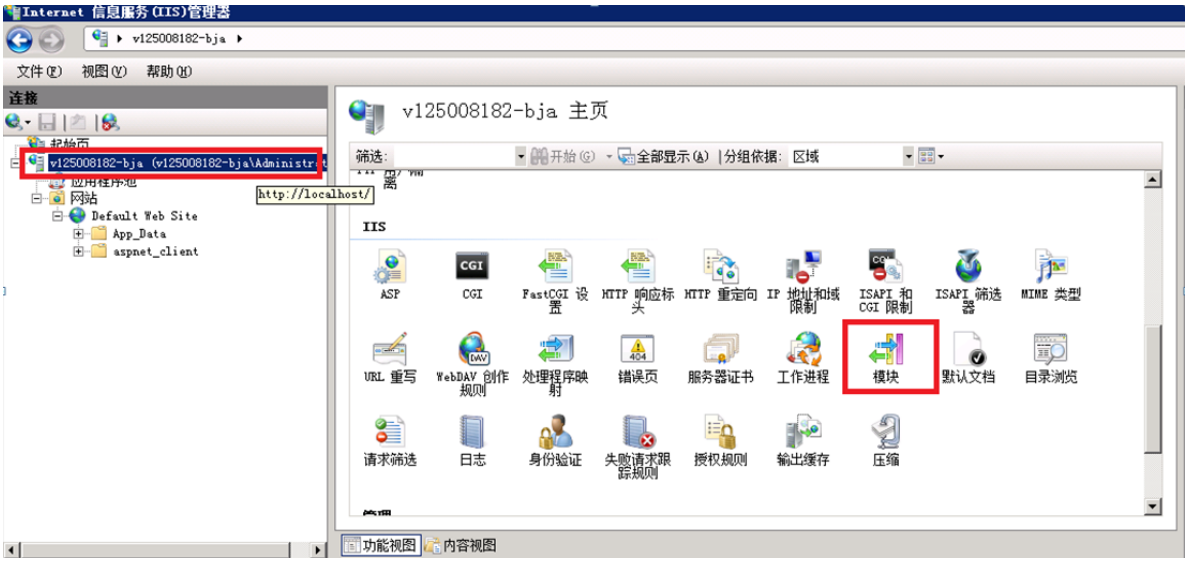
1. 根据服务器的操作系统版本将*x86\Release*或者*x64\Release*目录下的*F5XForwardedFor.dll*拷贝到某个目录（假设为*C:\ISAPIFilters*），同时确保IIS进程对该目录有读取权限。
2. 打开IIS管理器，找到当前开启的网站，在该网站上右键选择属性，打开属性页。
3. 在属性页切换至**ISAPI**筛选器，单击添加。
4. 在添加窗口下，配置以下参数，并单击确定。
   - 筛选器名称：F5XForwardedFor
   - 可执行文件：F5XForwardedFor.dll的完整路径，如本例中的*C:\ISAPIFilters\F5XForwardedFor.dll*
5. 重启 IIS 服务器，等待配置生效。

**IIS 7**配置方案

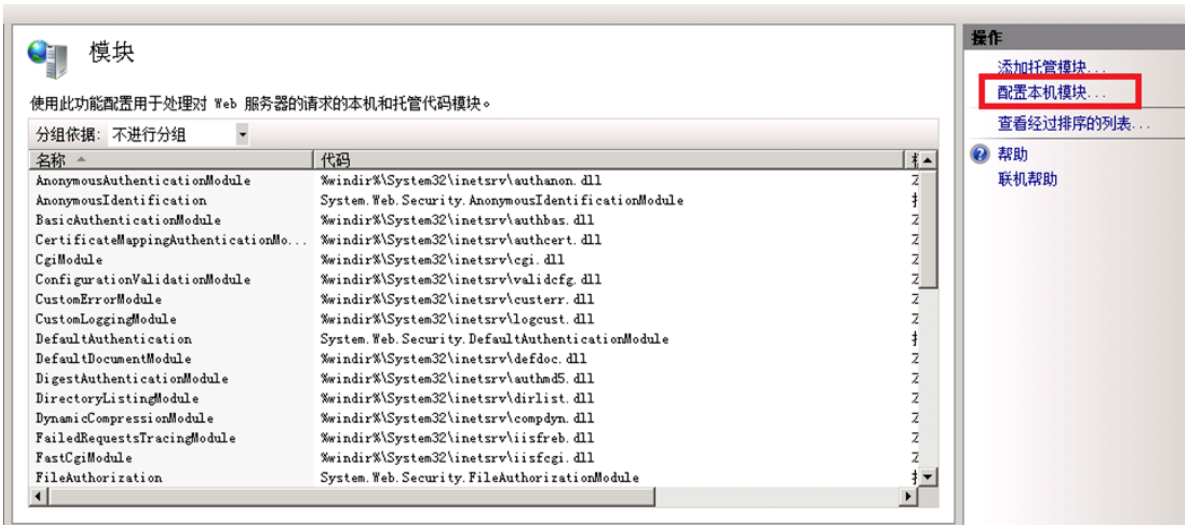
您可以通过F5XForwardedFor模块来获取来访者真实IP地址，但前提是您已安装*F5XForwardedFor*模块。

操作步骤

1. 根据服务器操作系统版本将*x86\Release*或者*x64\Release*目录下的*F5XFFHttpModule.dll*和*F5XFFHttpModule.ini*拷贝到指定目录下（假设为*C:\x_forwarded_for\x86*和*C:\x_forwarded_for\x64*），并确保IIS进程对该目录有读取权限。
2. 在**IIS**服务器选项中，双击打开模块。

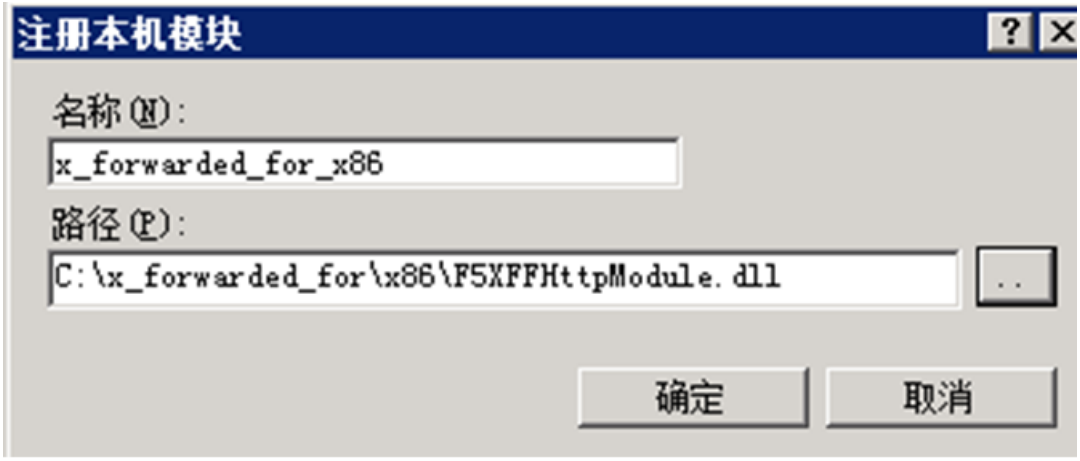



3. 选择配置本机模块。



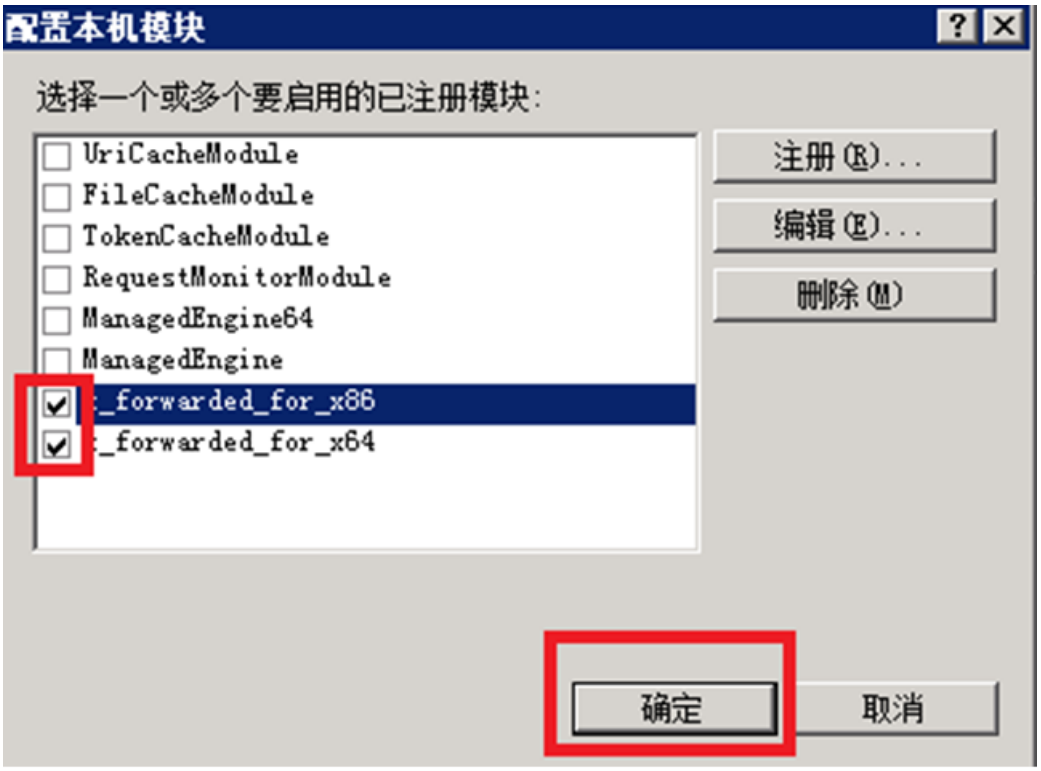

4. 在配置本机模块对话框中，单击注册，分别注册已下载的DLL文件。

   - 注册模块 x_forwarded_for_x86
     - 名称：x_forwarded_for_x86
     - 路径：*C:\x_forwarded_for\x86\F5XFFHttpModule.dll*
   - 注册模块 x_forwarded_for_x64
     - 名称：x_forwarded_for_x64
     - 路径：*C:\x_forwarded_for\x64\F5XFFHttpModule.dll*

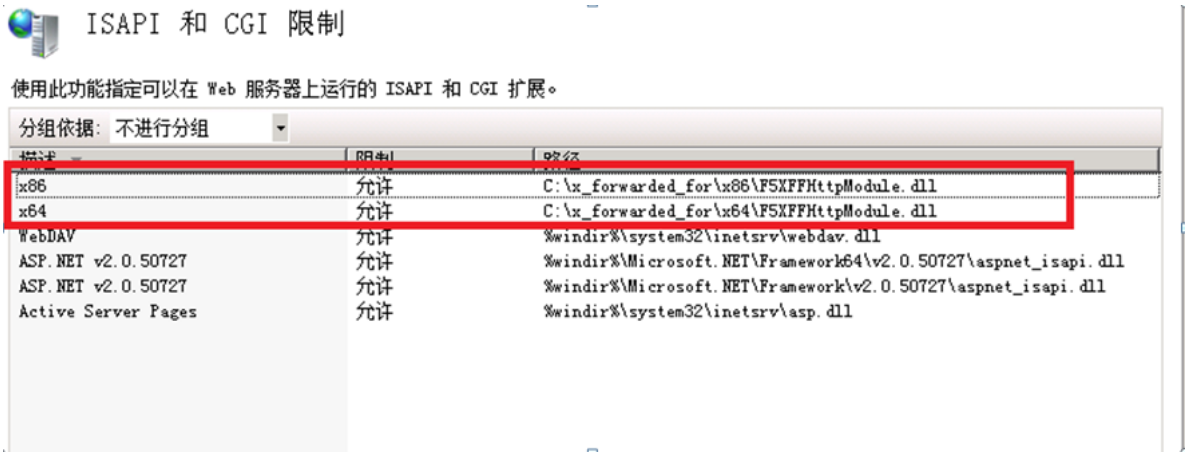




5. 注册完成后，勾选新注册的模块（x_forwarded_for_x86 和 x_forwarded_for_x64）并单击确定。




6. 在**API 和CGI限制**中，分别添加已注册的DLL，并将其限制改为允许。




7. 重启IIS服务器，等待配置生效。

**Apache配置方案**

1. 使用以下代码，安装Apache的一个第三方模块*mod_rpaf*。

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0
.c
```

2. 修改Apache配置文件*/alidata/server/httpd/conf/httpd.conf*，在其末尾添加以下内容。

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips ip地址
RPAFheader X-Forwarded-For
```

其中，RPAFproxy_ips ip地址不是负载均衡提供的公网IP，具体IP可以参考Apache日志，通常会有2个。

3. 添加完成后，使用以下命令重启Apache。

```
/alidata/server/httpd/bin/apachectl restart
```

案例

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 10.242.230.65 10.242.230.131
```

```
RPAFheader X-Forwarded-For
```

**Tomcat配置方案**

参照以下方法来开启Tomcat的X-Forwarded-For：

打开*tomcat/conf/server.xml*，修改AccessLogValve日志纪录功能为如下内容。

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory
="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T
" resolveHosts="false"/>
```

# 3 Web防护功能最佳实践

本文介绍了阿里云云盾Web应用防火墙的Web攻击防护最佳实践，主要从应用场景、防护策略、防护效果、规则更新四个方面进行介绍。

## 应用场景

Web应用防火墙（Web Application Firewall，简称WAF）主要提供针对Web攻击的防护，例如SQL注入、XSS、远程命令执行、Webshell上传等攻击。关于Web攻击的详细信息，请参考*OWASP 2017 Top 10*。

> **说明：**
> 主机层服务的安全问题（例如Redis、MySQL未授权访问等）导致的服务器入侵不在WAF的防护范围之内。

## 防护策略

在将网站成功接入WAF防护后，登录*Web*应用防火墙控制台，在**管理 > 网站配置**页面选择已防护的网站，并单击**防护配置**，即可查看Web应用攻击防护的防护状态，如图所示。

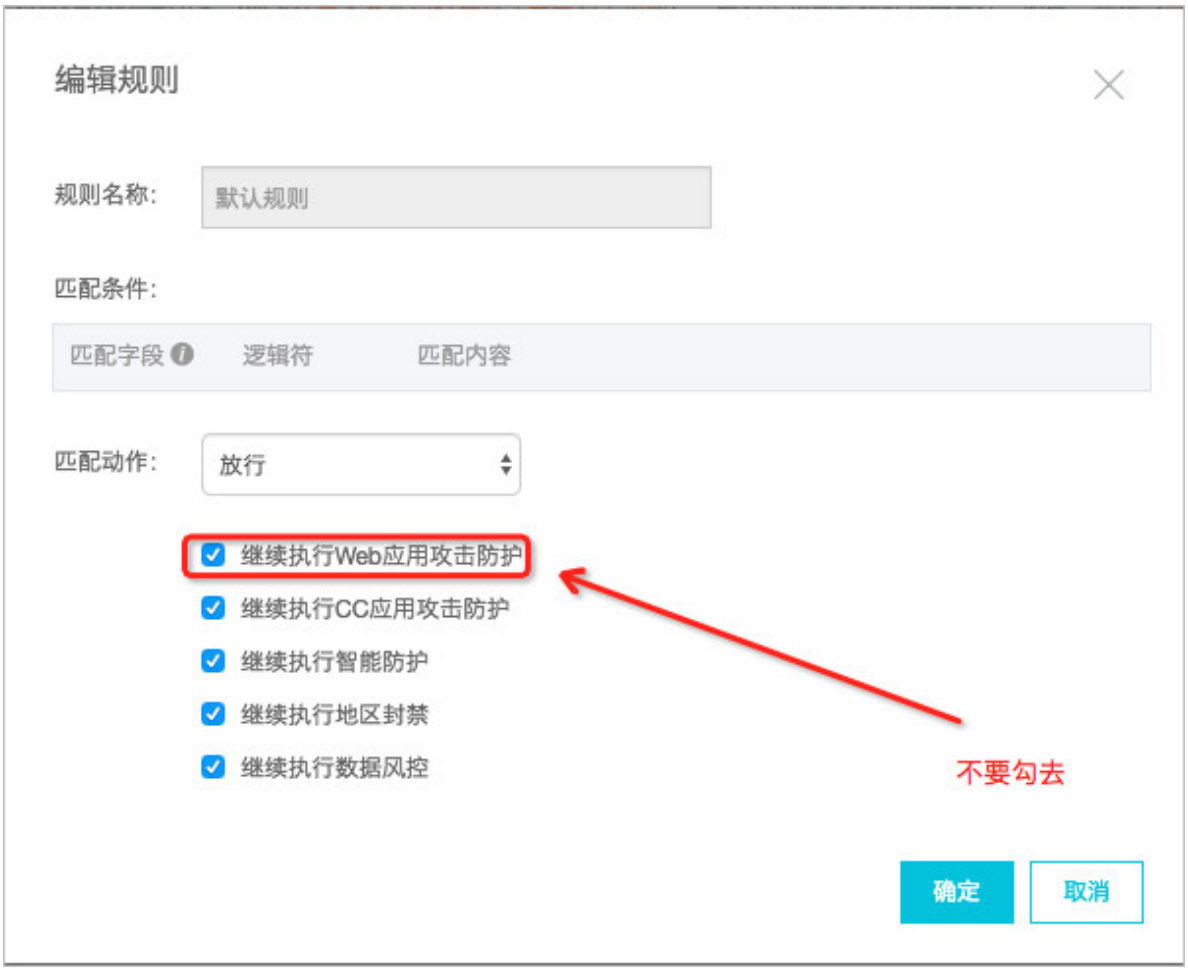

Web应用攻击防护功能默认开启，并使用正常模式的防护规则策略。其中，

- 状态
  - 开启表示WAF的Web应用攻击防护模块已开启。
  - 关闭表示该防护模块处于关闭状态。
- 模式：分为防护和预警两种模式。
  - 防护模式表示当遭受Web攻击时，WAF自动拦截攻击请求，并在后台记录攻击日志。
  - 预警模式表示当遭受Web攻击时，WAF不会拦截攻击请求，仅在后台记录攻击日志。
- 防护规则策略：分为宽松、正常、严格三种模式，仅在启用防护模式后生效。
  - 宽松防护规则策略的防护粒度较粗，只拦截攻击特征比较明显的请求。

- 正常防护规则策略的防护粒度较宽松且防护规则策略精准，可以拦截常见的具有绕过特征的攻击请求。
- 严格防护规则策略的防护粒度最精细，可以拦截具有复杂的绕过特征的攻击请求。

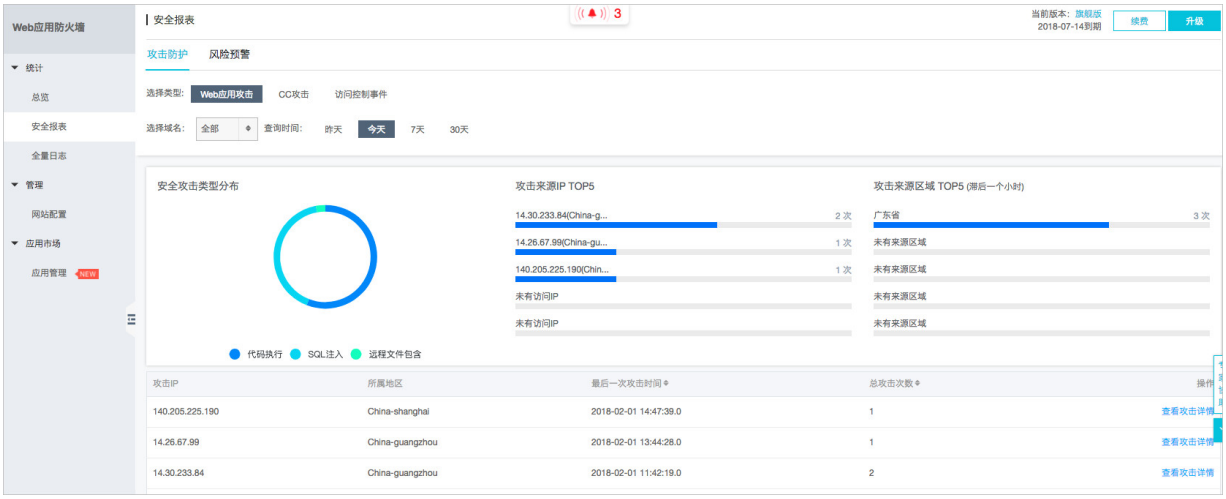
使用建议：

- 如果您对自己的业务流量特征还不完全清楚，建议先切换到预警模式进行观察。一般情况下，建议您观察一至两周，然后分析预警模式下的攻击日志。
  - 如果没有发现任何正常业务流量被拦截的记录，则可以切换到防护模式启用拦截防护。
  - 如果发现攻击日志中存在正常业务流量，可以联系阿里云安全专家沟通具体的解决方案。
- PHPMyAdmin、开发技术类论坛接入WAF防护可能会存在误拦截的问题，建议联系阿里云安全专家沟通具体的解决方案。
- 业务操作方面应注意以下问题：
  - 正常业务的HTTP请求中尽量不要直接传递原始的SQL语句、JAVA SCRIPT代码。
  - 正常业务的URL尽量不要使用一些特殊的关键字（UPDATE、SET等）作为路径，例如`www.example.com/abc/update/mod.php?set=1`。
  - 如果业务中需要上传文件，不建议直接通过Web方式上传超过50M的文件，建议使用OSS或者其他方式上传。
- 开启WAF的Web应用攻击防护功能后，不要禁用默认精准访问控制规则中的Web防护通用防护模块，如图所示。




**防护效果**

开启WAF的Web应用攻击防护功能后，您可以在**统计 > 安全报表**页面，查看攻击的拦截日志，如图所示。




在**安全报表**页面，您可以查看昨天、当天、7天以及一个月内的攻击详情。同时，单击**查看攻击详情**，可以查看具体的攻击信息，如图所示。


该截图中的拦截日志即为一条已被WAF拦截的SQL注入攻击请求。

> **说明：**
> 如果您发现WAF误拦截了正常业务流量，建议您先通过精准访问控制功能对受影响的URL配置白名单策略，然后联系阿里云安全专家沟通具体解决方案。

规则更新

对于互联网披露的已知漏洞和未披露的0day漏洞，云盾WAF将及时完成防护规则的更新，并发布防护公告。

您可以登录*Web*应用防火墙控制台，前往**总览** > **安全**页面，查看最新发布的防护公告，如图所示。


该截图中公告栏展示了针对weblogic远程命令执行漏洞的防护规则的更新公告。

> **说明：**
> Web攻击往往存在不止一种概念证明方法（Proof of Concept，简称PoC），阿里云安全专家会对漏洞原理进行深度分析从而确保发布的Web防护规则覆盖已公开和未公开的各种漏洞利用方式。

## 更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效的应对漏洞及黑客攻击，详情请关注安全管家服务。

# 4 通过设置自定义规则组提升Web防护效果

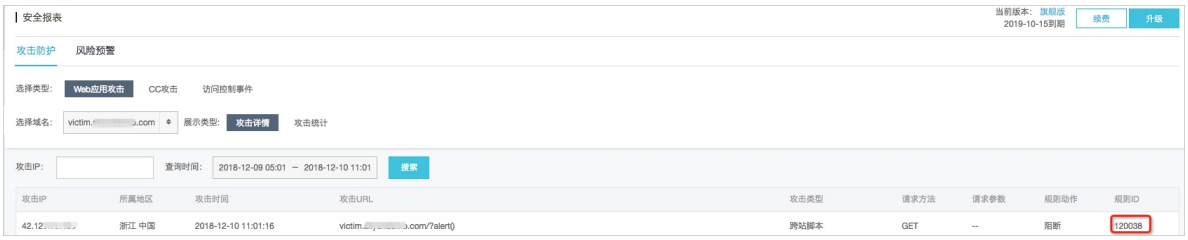
当您发现网站业务的正常请求被WAF误拦截时，您可以通过设置自定义规则组的方式避免该类误拦截。

当业务正常请求被WAF的Web应用攻击防护功能误拦截时，您可以确定触发本次拦截的Web应用防护规则，然后通过为该网站域名设置自定义规则组的方式为该网站域名移除特定规则，使WAF针对该网站业务不再拦截同样的正常请求。

> 说明：
> 在将该防护规则从自定义规则组移除时，请务必确认该类请求的针对该网站业务是正常请求。

**确定触发拦截的防护规则ID**

1. 登录*Web*应用防火墙控制台。
2. 选择中国大陆或海外地区地域。
3. 定位到统计 > 安全报表页面，在攻击防护页签。
4. 选择**Web**应用攻击类型，选择发生误拦截的网站域名，选择攻击详情展示类型。
5. 通过设置查询时间范围或访问IP的方式，找到相关的拦截记录日志。在拦截日志中，记录了拦截该请求的WAF防护规则ID。



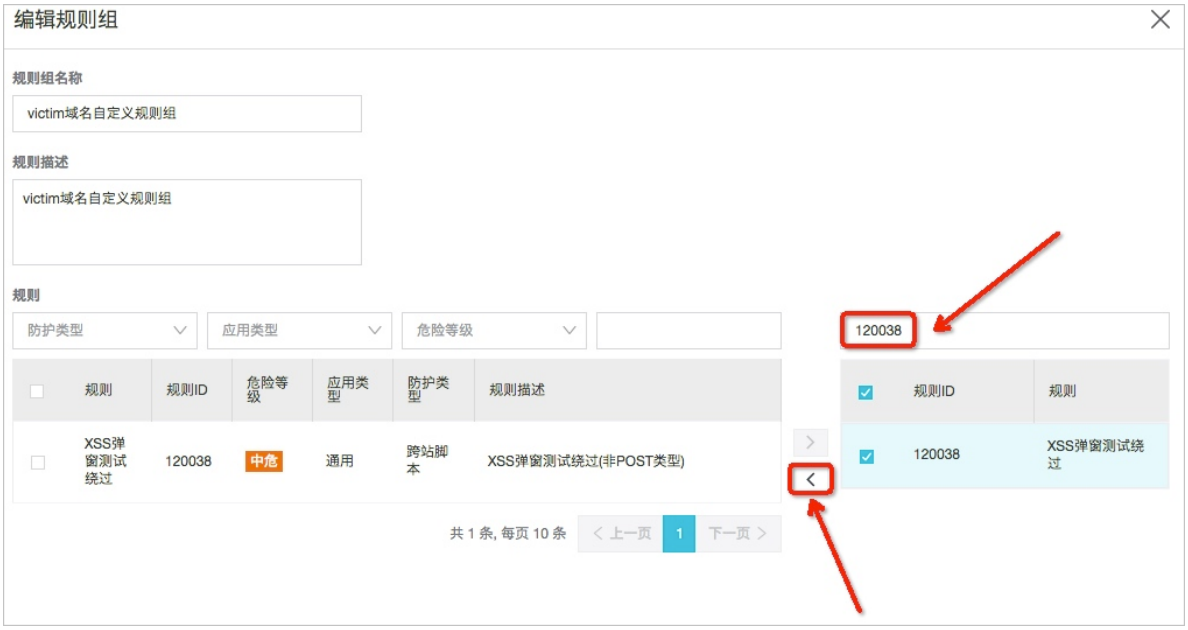

**为网站设置自定义规则组**

> 说明：
> 自定义规则组功能仅支持企业版以上的包年包月WAF实例。

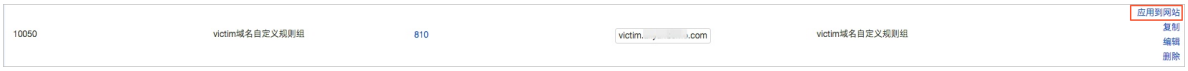
1. 在管理 > 网站配置页面，找到该网站的域名配置记录，单击防护设置，查看当前该网站采用的防护规则策略。


2. 定位到**设置 > 自定义规则组**页面，找到该网站域名当前采用的规则组，单击**复制**。
3. 填写规则组名称和规则描述，单击**确认**，创建自定义规则组。
4. 选择已创建的自定义规则组，单击**编辑**。
5. 在**编辑规则组**对话框的右侧的规则列表中，通过规则ID找到触发误拦截的规则ID，选中该规则并单击  将该规则从规则组中移除，单击**确认**。

> **说明：**
> 左侧规则列表列出的是WAF所有的Web应用防护规则，右侧则是该自定义规则组中包含的规则。




6. 在**自定义规则组**页面中，选择该自定义规则组，单击**应用到网站**并选择出现误拦截的网站域名。



自定义规则组应用完成后，该网站域名的Web应用攻击防护规则策略将变更为所应用的自定义规则组。


此时，您再次向该网站域名发送同样的请求，将不再被WAF拦截。

**说明：**

如果访问请求仍然被WAF拦截，您可以根据上述步骤再次确定本次触发拦截的防护规则ID，并在自定义规则组中将该规则移除，避免误拦截。