目录

第1步：添加域名

本文档介绍了开通Web应用防火墙(WAF)实例后，如何将您要防护的网站域名接入WAF进行防护。目前WAF产品处于新旧两个版本并行状态，旧版WAF预计在新版WAF公测结束后，逐步下线。

前提条件

1. 已开通WAF实例，且当前实例支持接入的域名数量未超过限制。
2. 您要接入的域名已完成ICP备案。

新版WAF操作指导 旧版WAF操作指导

新版WAF

操作步骤

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**网站接入**，点击**添加域名**按钮。
3. 在 **网站接入** > **域名**页面，完成**添加域名**、**源站设置**、**健康检查**三项配置。

添加域名

参数	说明
域名	要防护的域名，支持一级域名和二级域名，支持泛域名
协议类型	选择网站使用的网络协议类型。可选HTTP、HTTPS
服务端口	添加网站使用的转发服务端口
转发方式	设置了多个源站IP地址时，选择多源站IP间的转发方式。可选轮询、最小连接数
前置代理	网站业务在接入WAF前是否开启了其他七层代理服务。可选是、否
项目组	选择当前域名所属项目
流量标记	设置自定义的HTTP头部标记字段，对经过WAF的请求进行标记

源站设置

设置网站的源站服务器地址，支持IP地址格式。您可添加多个源站IP，完成接入后，WAF将过滤后的访问请求转发到此处设置的服务器地址。WAF将在您配置的多个IP之间，按您选择的转发方式及权重设置进行负载均衡。

健康检查

一键开启健康检查，对所有源站IP及配置端口进行接入状态检测。

4. 点击**确定**，完成域名接入流程。

网站接入相关说明

- DNS解析状态 添加域名成功后，系统将定时检测源站的DNS解析状态，在您修改将域名DNS解析至WAF的Cname之前，解析状态将显示失败。若您添加的域名为泛域名，对应的DNS解析状态显示未知。
- CC防护状态 添加域名成功后，Web攻击防护默认开启，若您未添加CC防护规则，CC防护状态显示关闭。

旧版WAF

背景信息

1. SLB_WAF实例需绑定弹性EIP后才可添加域名，请确认您的SLB_WAF实例已经绑定弹性IP。
2. 一个域名包支持添加十个域名的防护，仅限一个一级域名，支持添加泛域名。
3. 域名将进行备案检查，您的域名需先进行备案。

操作步骤

1. 选择待添加域名的WAF实例，
2. 在底部菜单栏中，点击**添加域名**。

a. SLB_WAF所需填写参数及其说明

参数	说明
填写域名	填写要防护的网站域名，支持填写泛域名
勾选协议	选择要支持的协议类型，HTTPS协议需选择安全证书
回源设置	可选择SLB_WAF实例绑定VPC内的可用弹性IP或内网服务器，建议回源到内网IP，过期或被删除的弹性IP，将从WAF回源记录中删除
健康检查	默认开启回源健康检查，若源站只有1个建议关闭，请务必保证回源检查的请求可被访问，否则可能导致WAF回源失败

b. 云WAF所需填写参数及其说明

参数	说明
填写域名	填写要防护的网站域名，支持填写泛域名
勾选协议	选择要支持的协议类型，HTTPS协议需选择安全证书
回源设置	填写要防护的公网源站IP，多个IP换行输入
健康检查	默认开启回源健康检查，若源站只有1个建议关闭，请务必保证回源检查的请求可被访问，否则可能导致WAF回源失败

3. 点击**确定**添加域名成功。
4. 点击实例，查看添加的防护域名。

说明：

1. 服务状态将检查是否配置回源信息和CNAME解析是否成功。
2. 域名防护默认为开启状态。

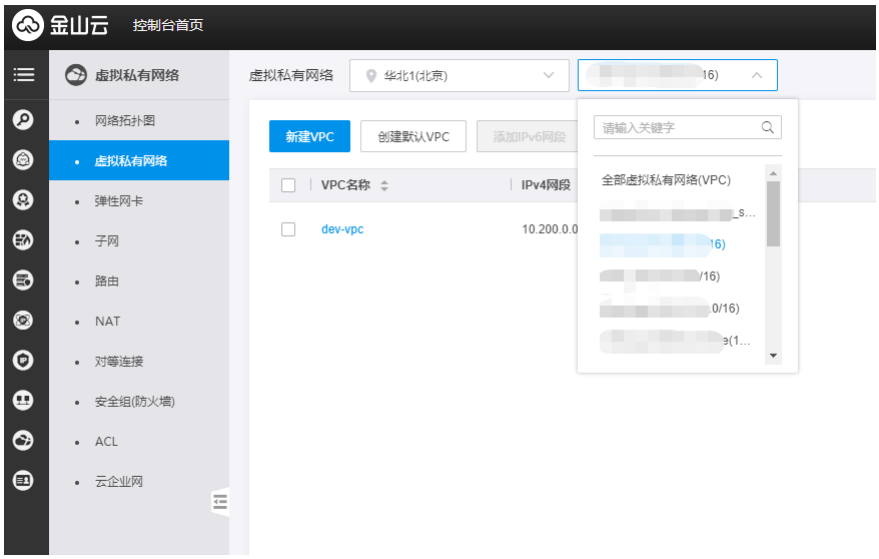
第2步：放行WAF IP段

网站接入WAF进行防护时，您需要设置源站服务器的安全软件或访问控制策略，放行WAF回源IP段的入方向流量。本文档以源站在金山云内为例，介绍了如何放行WAF回源IP段。

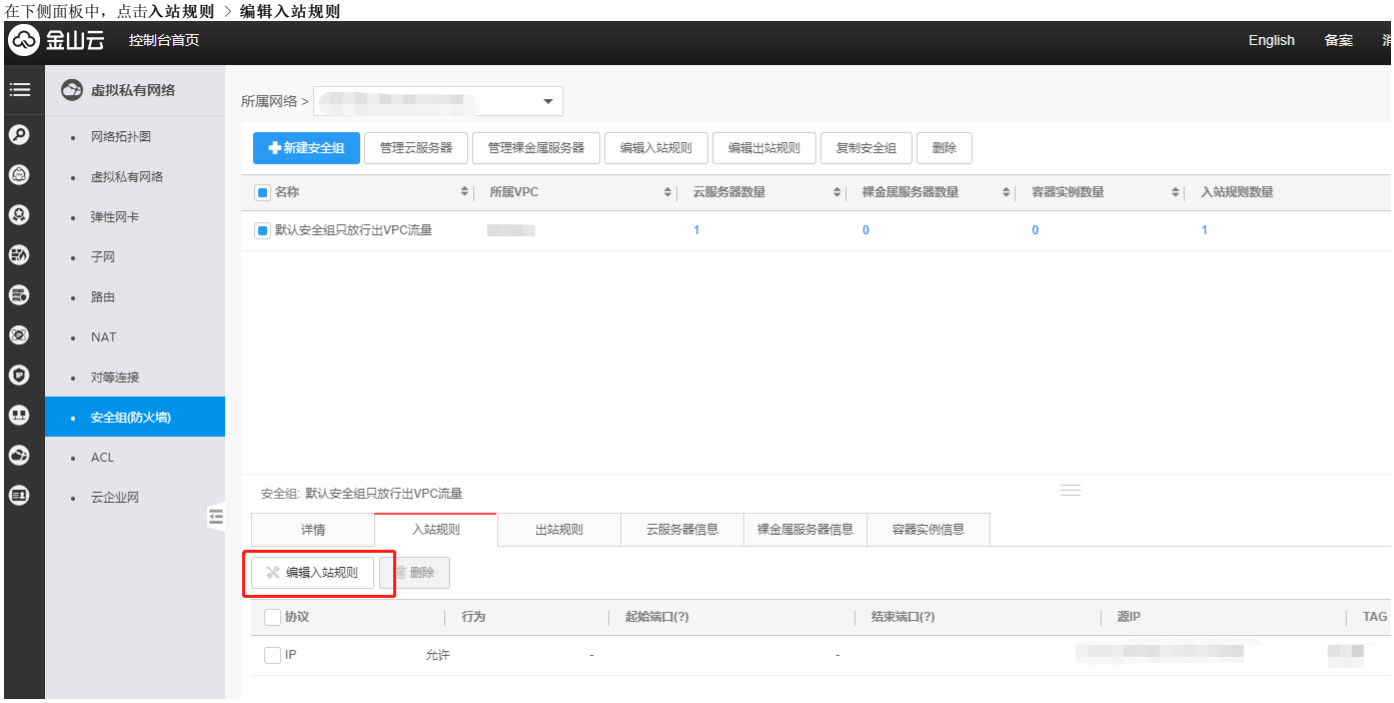
WAF回源IP段

110.43.76.96/28 110.43.76.112/28 110.43.129.96/28 110.43.129.112/28 110.43.43.48/29 110.43.43.56/29 **您需要将回源IP段添加到源站安全软件的白名单中。**

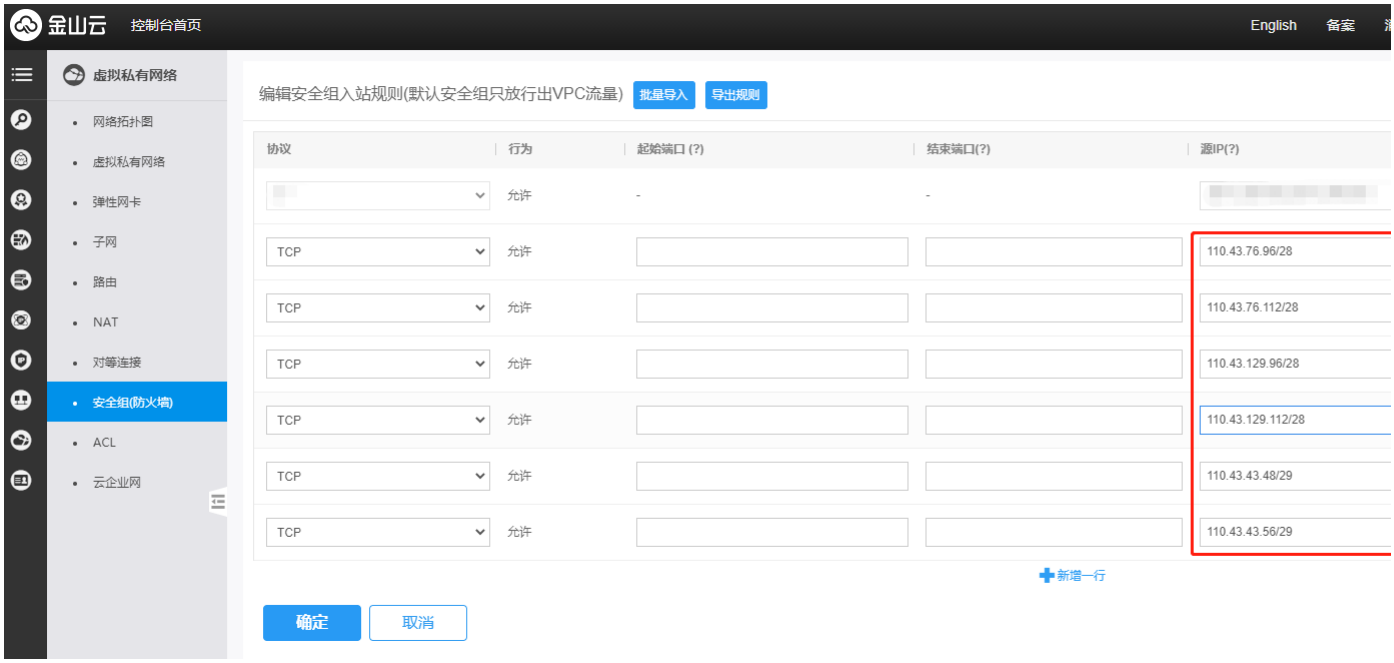
操作步骤



1. 登录虚拟私有网络控制台，选择源站云服务器所在的VPC。
2. 在左侧导航栏，点击**安全组(防火墙)**，选择需要修改的安全组。
3. 在下侧面板中，点击**入站规则** > **编辑入站规则**



4. 点击**新增一行**，输入WAF回源IP段，点击**确定**。



若您使用旧版WAF请按如下IP配置放行：

SLB_WAF	云WAF
100.64.84.0/24	
100.64.85.0/24	
100.64.195.0/24	
100.65.49.0/24	华北1(北京)：110.43.76.0/24
100.65.50.0/24	华东1(上海)：110.43.129.0/24
100.65.192.0/24	华南1(广州)：110.43.43.0/26
100.71.192.0/24	
100.71.193.0/24	
100.71.194.0/24	

第3步：验证配置生效

已在Web应用防火墙（WAF）中添加域名，但还未修改域名的DNS解析（将网站域名解析到WAF）时，为了保证业务的稳定性，建议您在修改DNS解析前在本地验证配置是否已生效。

前提条件

已为WAF实例添加要防护的网站域名。

背景信息

通过修改本地计算机的hosts文件，可以设置本地计算机的域名寻址映射，即仅对本地计算机生效的DNS解析记录。本地验证需要您在本地计算机上将网站域名的解析指向WAF的IP地址。这样就可以通过本地计算机访问被防护的域名，验证WAF中添加的域名接入设置是否正确有效，避免域名接入配置异常导致网站访问异常。

操作步骤

以下操作以本地计算机使用Windows操作系统为例进行描述。

1）获取WAF IP地址

1. 登录Web应用防火墙控制台。
2. 在左侧菜单栏，点击**网站接入**。
3. 在域名列表中，定位到已添加的域名，将光标移入到cname标签上，复制域名对应的WAF Cname地址。

4. 在Windows操作系统中，打开cmd命令行工具。
5. 执行以下命令：

   ```
   ping <已复制的WAF Cname地址>
   ```

6. 在ping命令返回的结果中，记录域名对应的WAF IP地址。

2）修改本地hosts文件

1. 打开本地计算机的文件资源管理器。
2. 在地址栏输入C:\Windows\System32\drivers\etc\hosts，并选择使用记事本或Notepad++等文本编辑器打开hosts文件。
3. 在hosts文件最后一行添加以下记录：

   〈WAF IP地址〉〈被防护域名〉

   例如： 22.111.234.12 say.hello.com，IP地址和域名之间使用空格分隔。
4. 保存修改后的hosts文件，并在cmd命令行中执行以下命令，验证配置生效。

   ping〈被防护域名〉

   说明：如果ping命令解析到了源站IP地址，请刷新本地的DNS缓存，并重新执行ping命令；如果ping命令解析到的IP地址是域名对应的WAF IP地址，表示hosts修改已经生效。
5. 通过本地浏览器访问被防护域名，如果网站能正常访问，说明WAF中添加的域名设置正确有效。
6. 本地验证通过后，您可修改域名的DNS解析，将网站流量解析到WAF进行防护，并删除步骤3中添加的记录。

第4步：修改DNS解析

在Web应用防火墙(WAF)添加网站域名，并在本地验证生效后，需在域名服务提供商进行DNS管理修改DNS解析记录，将域名请求解析到WAF实例进行安全防护。本文以金山云DNS为例，介绍了修改DNS解析的相关内容，用户可以参考此步骤修改，或咨询域名所在的服务提供商。

前提条件

1. 已添加要防护的网站域名信息。具体操作，请参见第一步：添加域名。
2. 拥有在域名的DNS服务商处修改域名解析设置的权限。
3. 已在源站放行WAF回源IP段。
4. 已通过本地验证确保转发配置生效。

获取WAF Cname地址和WAF IP地址

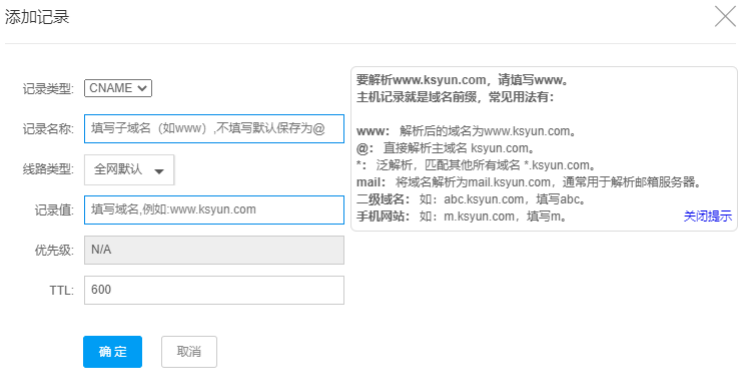
1. 登录Web应用防火墙控制台。
2. 在左侧菜单栏，点击**网站接入**。
3. 在域名列表中，定位到已添加的域名，将光标移入到cname标签上，复制域名对应的WAF Cname地址。

4. 在Windows操作系统中，打开cmd命令行工具。
5. 执行以下命令：

   ping〈已复制的WAF Cname地址〉
6. 在ping命令返回的结果中，记录域名对应的WAF IP地址。

使用云解析DNS修改域名解析

1. 登录云解析控制台。
2. 在**域名服务** > **云解析**页面，定位到要设置的域名，点击该域名。
3. 在底部菜单栏中，点击**添加记录**按钮。



4. 在**添加记录**弹窗中，添加记录信息。

   记录类型设置为**CNAME**、**记录值**修改为WAF CNAME地址、**记录名称**内容为需要防护的网站域名。
5. 点击**确定**，记录添加成功。
6. 待DNS解析生效后，回到WAF控制台，若回源实例、CNAME均已配置，且源站可访问，则会看到此条域名记录的服务状态变为**服务正常**。