ALIBABA CLOUD

阿里云

Web应用防火墙

接入WAF

文档版本：20220512

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 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。	`switch {active|stand}`

目录

1.使用教程

使用Web应用防火墙（Web Application Firewall，简称WAF）防护您的Web业务前，您必须将要防护的网站接入WAF。未完成接入操作，您的Web应用防火墙防护将无法生效。

网站接入流程

WAF支持使用CNAME接入和透明接入模式，为您的网站流量提供WAF防护。

- **CNAME接入**
  您在WAF控制台添加需要防护的网站域名后，通过修改域名的DNS解析设置，将网站流量解析到WAF，使访问网站的流量经过WAF并受到WAF的防护。WAF将过滤和处理后的请求转发回该域名的源站服务器。WAF支持自动添加网站（即域名一键接入）和手动添加网站两种方式。
  CNAME接入流程：
  i. 添加域名：介绍自动添加网站和手动添加网站的相关操作。

  > 注意
  > - 如果网站使用HTTPS协议，您必须在添加域名后上传正确、有效的HTTPS证书，保证WAF正常处理HTTPS协议流量。更多信息，请参见上传HTTPS证书。
  > - 如果源站服务器使用HTTP 80端口、HTTPS 443端口以外的端口，您可以在WAF支持的端口范围中自定义服务器端口。更多信息，请参见WAF支持的端口。

  ii. 放行WAF回源IP段：WAF使用特定的回源IP段将经过防护引擎检测后的正常流量转发回网站域名的源站服务器。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。
  iii. 本地验证：添加域名后，在本地电脑上搭建简易的模拟环境，验证网站流量转发设置已经生效，避免转发设置未生效时修改域名的DNS解析设置，导致业务访问异常。
  iv. 修改域名DNS：手动修改域名的DNS解析设置，将网站流量解析到WAF进行防护。
- **透明接入**
  透明接入模式无需修改域名的DNS解析设置，完成域名接入后，可以将源站ALB实例、CLB实例上的HTTP或HTTPS请求流量直接牵引到WAF，经WAF处理后再将正常的请求流量转发回源站服务器。
  关于透明接入的具体内容及操作，请参见：透明接入。

完成接入流程后，网站访问流量将经过WAF保护。WAF包含多种防护检测模块，帮助网站应对不同类型的安全威胁，其中**规则防护引擎**和**CC安全防护**模块默认开启，分别用于防御常见的Web应用攻击（例如SQL注入、XSS跨站、webshell上传等）和CC攻击，其他防护模块需要您手动开启并配置具体防护规则。更多信息，请参见网站防护配置概述。

最佳实践

- 设置源站保护：源站服务器部署在ECS时，通过设置ECS或SLB的安全组策略，只放行WAF的入方向请求，避免攻击者绕过WAF直接对源站服务器发起攻击。
- 获取客户端真实IP：接入WAF后，源站收到的所有请求都经过WAF代理，您必须通过X-Forwarded-For获取访问请求的真实来源IP。

云产品接入WAF

- 通过联合部署DDoS高防和WAF提升网站防护能力：网站需要同时防御Web应用攻击和DDoS攻击时，您可以在源站前依次部署DDoS高防和WAF。
- 同时部署WAF和CDN：网站需要防御Web应用攻击，同时部署CDN加速时，您可以在源站前依次部署CDN和WAF。

2.CNAME接入

2.1. 添加域名

本文介绍了开通Web应用防火墙（Web Application Firewall，简称 WAF）后，如何通过CNAME接入方式将您要防护的域名接入WAF进行防护。

前提条件

- 已购买WAF实例，且当前实例支持接入的域名数量未超过限制。

  > **说明** 支持接入的域名数量由WAF的实例规格和扩展域名包数量决定。更多信息，请参见域名扩展包。

- 如果您已购买中国内地的WAF实例，您必须先为域名完成ICP备案，才可以将网站接入WAF防护。否则，您在WAF中添加该网站时，将会收到报错，提示您需要完成备案。关于阿里云ICP备案的更多信息，请参见ICP备案流程概述。

  > **注意** 您将网站接入WAF防护后，还必须保证域名备案信息的有效性。为符合相关法律法规要求，中国内地WAF实例会定期清除备案失效的域名。关于相关法律法规，请参见未备案不得提供非经营性互联网信息服务。

背景信息

CNAME接入指您在WAF控制台添加要接入WAF防护的网站信息，并修改网站域名的DNS解析（设置CNAME解析记录），将网站的Web请求转发到WAF进行防护。该方式支持云上、云下的公网服务器地址接入。下文将会具体介绍CNAME接入的操作步骤。

> **说明** 除了CNAME接入，您还可以选择透明接入。透明接入无需修改网站域名的DNS解析及源站配置，即可将网站的Web请求接入WAF进行防护。该方式是云上公网资产的最佳接入方式。相关操作，请参见透明接入。

CNAME接入支持以下两种方式：

- 一键接入域名：WAF自动读取当前阿里云账号关联的网站资产信息，您只需从**一键接入**列表选择需要接入的网站域名和协议类型，即可自动添加网站信息，包括网站域名、服务器地址、80和443标准协议端口，并自动修改域名的DNS解析。

  > **注意** 自动修改域名解析需要执行网站接入的阿里云账号拥有操作云解析DNS的权限，否则自动修改域名解析会失败。这种情况下，您可以在自动添加网站后手动修改域名的DNS解析。

- 手动接入域名：如果您要接入的网站不支持自动添加，您可以手动添加网站信息，例如网站域名、网络协议、服务器地址、服务器端口等。手动添加网站信息后，您需要手动修改网站域名的DNS解析，将网站的Web请求转发到WAF进行防护。

视频教程

推荐您观看以下操作演示视频。该视频以CNAME接入为例，介绍了手动接入网站域名到WAF进行防护的完整操作。

一键接入域名

在添加网站时，如果您的阿里云账号下存在满足条件的网站域名，您可以直接从**一键接入**列表选择要添加的网站，完成自动添加网站。

支持自动添加的网站域名需要满足以下条件：

- 如果您已完成资产识别授权，则支持自动添加的域名和资产识别结果一致。更多信息，请参见资产识别。
- 如果您未执行过资产识别授权，则支持自动添加的网站域名仅包含云解析DNS中配置生效的网站域名。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 在**域名列表**页签，单击**网站接入**。

   > **说明** 进入**添加域名**页面后，**接入模式**默认为**Cname接入**。CNAME接入场景下，您无需再修改**接入模式**。

5. 在**一键接入**页签，从域名列表选中要添加的**域名**和对应的**协议类型**，并单击**立即自动添加网站**。

   > **说明** 如果**一键接入**列表为空，表示没有满足条件的域名，建议您手动添加网站。更多信息，请参见添加域名配置向导。

   如果域名使用HTTPS协议，则在选中**https**协议类型后，您必须先完成证书验证才可以添加网站。验证证书的操作步骤如下：

   i. 选中某个域名和**https**协议类型后，单击域名**HTTPS证书**列的**验证证书**。
   ii. 在**验证证书**对话框，选择一种**上传方式**，并按照页面提示上传该域名绑定的证书。

   具体操作，请参见上传HTTPS证书。

   iii. 完成证书上传后，单击**确定**。
   WAF会自动验证您上传的证书是否正确，可能结果如下：
   - 如果证书验证顺利通过，您可以单击**立即自动添加网站**。
   - 如果证书验证失败，请根据错误提示（例如**证书与密钥不匹配**）重新验证证书，直到验证通过。

     更多信息，请参见证书与密钥不匹配问题排查。

   WAF将自动添加网站信息，包括网站域名、服务器地址、80和443标准协议端口，并自动修改域名的DNS解析。

   > **说明** 如果您需要添加80和443以外的端口，建议您在自动添加网站后，手动编辑域名进行调整。更多信息，请参见相关操作。

可能出现的异常结果及后续操作

- **域名添加成功，但需要手动接入DNS**

可能原因：执行添加域名的云账号不具有操作云解析DNS的权限、上传的HTTPS证书与网站域名不匹配。

> **说明** 网站支持https协议且证书验证通过的情况下，如果上传的证书与网站不匹配，则证书检测失败，不会自动修改DNS解析。这种情况下，您必须重新上传合法、正确的证书再手动修改DNS。更多信息，请参见上传HTTPS证书。

单击**手动接入DNS**，根据**手动修改**对话框的操作引导，完成DNS修改。更多信息，请参见修改域名DNS。

- **当前已达到主域名个数限制**

单击**扩展域名包**，查看购买扩展域名包的操作引导。根据需要购买扩展域名包后，再尝试添加域名。

- **该域名未检测到ICP备案信息**

如果您购买的是中国内地的WAF实例，您必须先对域名完成ICP备案，否则您的网站将无法接入WAF防护。建议您先完成ICP备案再尝试添加域名。更多信息，请参见ICP备案流程概述。

手动接入域名

以下操作步骤介绍了使用CNAME接入模式手动添加网站的具体操作。

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 在**域名列表**页签，单击**网站接入**。

> **说明** 进入**添加域名**页面后，**接入模式**默认为**Cname接入**。CNAME接入场景下，您无需再修改**接入模式**。

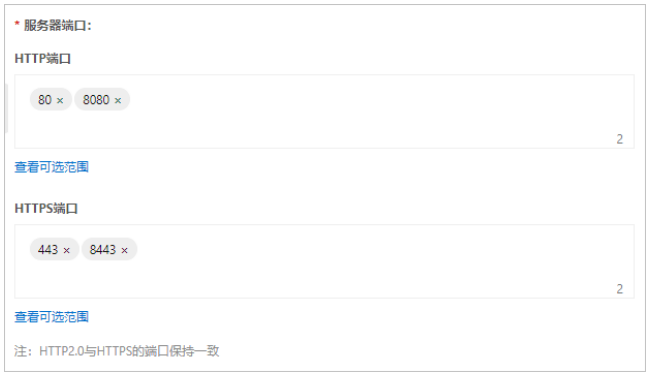
5. 单击**手动接入**页签，并根据配置向导完成相关任务。
   i. **填写网站信息**。
      填写下表描述的网站信息，并单击**下一步**。


一键接入
手动接入
1
填写网站信息
2
修改DNS解析
* 域名:
www.example.com
支持一级域名（例如：com）和二级域名（例如：www.com），二者互不影响，请根据实际情况填写。
* 防护资源
公共集群
* 协议类型:
HTTP
HTTPS
HTTP2
高级设置
* 服务器地址:
IP
域名（如CNAME）
请输入要保护的服务器公网IP，如1.1.1.1，1
7A等，每输入一个地址后按回车保存，最多输入20个
0
请确保在域名添加完毕后在"网站接入"的域名列表中打开IPv6开关，否则IPv6回源配置将不生效。
IPv4/IPv6回源协议跟随
* 服务器端口:
HTTP端口
80 ×
1
查看可选范围
HTTPS端口
443 ×
1
查看可选范围
注：HTTP2.0与HTTPS的端口保持一致
负载均衡算法:
IP hash
轮询
Least time
WAF前是否有七层代理（高防/CDN等）:
是
否
启用流量标记
资源组
默认资源组
下一步
取消

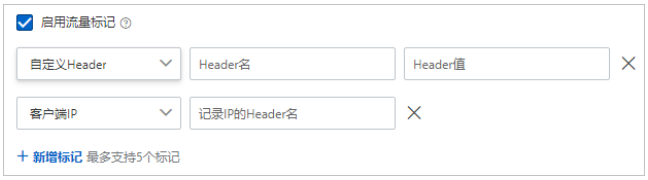
参数	说明
域名	填写网站域名。域名需要满足以下要求： ■ 支持使用精确域名（例如，`www.aliyun.com`）和泛域名（例如，`*.aliyun.com`）格式。具体说明如下： ■ 使用泛域名后，WAF将自动匹配该泛域名对应的所有子域名（例如，`*.aliyun.com` 能够匹配 `www.aliyun.com`、`test.aliyun.com` 等）。 **注意** 泛域名不支持匹配对应的主域名（例如，`*.aliyun.com` 不能够匹配 `aliyun.com`）。如果您需要将主域名接入WAF进行防护，您需要单独添加对应的域名配置（例如，单独添加 `aliyun.com`）。 ■ 如果同时存在泛域名和精确域名配置，则精确域名的转发规则和防护策略优先生效。 ■ 暂不支持添加 `.edu` 域名。如果您需要添加 `.edu` 域名，请提交工单联系售后技术支持。
防护资源	选择要使用的防护资源类型。可选项： ■ **公共集群**：默认选择。 ■ **独享集群**：只有使用独享版WAF实例时，才支持该选项。独享集群支持定制化业务需求。更多信息，请参见独享集群最佳实践。 ■ **混合云集群**：只有使用混合云接入时，需要选择该选型。更多信息，请参见网站接入（混合云WAF）。
	选择网站使用的协议类型。可选项： ■ **HTTP**

参数	说明
协议类型	■ HTTPS **注意** 如果网站支持HTTPS加密认证，请选择**HTTPS**协议并在添加域名后上传域名的证书和私钥文件。更多信息，请参见上传HTTPS证书。 选中**HTTPS**后，还支持启用以下功能：  ■ **（高级设置）开启HTTPS的强制跳转** HTTPS强制跳转表示将客户端的HTTP请求强制转换为HTTPS请求，默认跳转到443端口。如果您需要强制客户端使用HTTPS请求访问网站以提高安全性，则可以开启该设置。 **注意** ■ 只有在未选中**HTTP**协议时，支持开启该设置。 ■ 请确保网站支持HTTPS业务再开启该设置。开启该设置后，部分浏览器将被强制设置为使用HTTPS请求访问网站。 ■ **（高级设置）开启HTTP回源** HTTP回源表示WAF使用HTTP协议向源站转发回源请求，默认回源端口是80。开启HTTP回源可以在无需改动源站服务器的前提下，通过WAF实现HTTPS访问，帮助您降低网站的负载损耗。 **注意** 如果您的网站不支持HTTPS回源，请务必开启该设置。 ■ **启用回源SNI** 回源SNI表示WAF转发客户端请求到源站服务器，在与源站进行TLS握手时，通过SNI扩展字段（Server Name Indicator extension）指定要访问的主机，并与该主机建立HTTPS连接。如果您的源站服务器有多个虚拟主机（对应不同域名），则您需要开启该设置。 选中**启用回源SNI**后，您可以进一步设置SNI扩展字段的值。可选项：
	设置网站的源站服务器地址，支持IP地址格式和域名（如CNAME）格式。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。设置说明： ■ **与实际请求host保持一致**（默认）：表示WAF回源请求中SNI扩展字段的值与请求头中Host字段的值保持一致。 例如，您配置的网站域名为 `*.aliyundoc.com` ，客户端实际请求了 `www.aliyundoc.com` （即Host字段值），则WAF回源请求中SNI扩展字段的值为 `www.aliyundoc.com` 。 ■ **自定义**：表示您自定义WAF回源请求中SNI扩展字段的值。 一般情况无需自定义SNI，除非您的业务有特殊配置要求，希望WAF在回源请求中使用与实际请求Host不一致的SNI（即此处设置的自定义SNI）。

参数	说明
服务器地址	■ **IP**地址格式：填写源站的公网IP地址。需要为公网可达的IP地址。 支持填写多个IP地址，每填写一个IP地址，按回车进行确认。最多支持添加20个源站IP。 **说明** 如果设置了多个IP地址，WAF将在这些地址间自动进行健康检查和负载均衡。 海外地区WAF实例仅支持配置IPv4地址。中国内地WAF实例支持同时配置IPv4和IPv6地址，或者只配置IPv4地址，暂不支持只配置IPv6地址。区别如下： ■ 同时配置IPv4和IPv6地址时，如果开启**IPv4/IPv6协议跟随**，则来自IPv6地址的请求将被转发到IPv6源站，来自IPv4地址的请求将被转发到IPv4源站。如果不开启**IPv4/IPv6协议跟随**，则不做区分，执行混合回源（即IPv4和IPv6请求都有可能回源到IPv4或IPv6源站）。 **注意** 使用IPv6回源时，您必须确保**网站接入**列表中域名的**IPv6状态**为已开启。更多信息，请参见开启IPv6防护。 ■ 只配置IPv4地址时，IPv4和IPv6请求都将通过IPv4回源，即WAF将请求转发到您设置的IPv4源站地址。 服务器IP地址填写说明 ■ 如果源站在阿里云，一般填写ECS的公网IP地址。 ■ 当ECS前面有SLB时，则填写SLB的公网IP地址。 ■ 当源站在阿里云外的IDC机房或者其他云服务商时，建议您PING域名查询域名的公网IP地址，再填写域名的公网IP地址。 ■ **域名（如CNAME）**格式：填写服务器回源域名，例如，对象存储OSS的CNAME等。 使用域名格式时，仅支持IPv4回源（暂不支持IPv6回源），即WAF只会将客户端请求转发到回源域名解析出来的IPv4地址（WAF不解析回源域名的IPv6地址）。 **注意** ■ 服务器回源域名不应和要防护的网站域名相同。 ■ 如果您的源站服务器地址为OSS域名，则完成网站接入后，您必须前往OSS控制台中为该OSS域名绑定自定义域名。具体操作，请参见绑定自定义域名。

参数	说明
服务器端口	添加网站使用的转发服务端口。 WAF通过此处添加的端口为网站提供流量的接入与转发服务，网站域名的业务流量只通过已添加的服务端口进行转发。对于未添加的端口，WAF不会转发任何该端口的访问请求流量到源站服务器，因此这些端口的启用不会对源站服务器造成任何安全威胁。 **注意** 网站信息中设置的**协议类型**和**服务器端口**必须是源站服务器提供Web业务的协议和端口，不支持端口转换。例如，源站服务器提供Web服务的是80端口HTTP协议，域名配置也必须是一致的，设置其他端口则无法正常转发。 默认端口： ■ **HTTP 80**：选中HTTP协议后默认设置。 ■ **HTTPS 443**：选中HTTPS协议后默认设置。 **说明** HTTP 2.0协议的端口与HTTPS协议的端口保持一致。 自定义端口：在**HTTP端口**输入框、**HTTPS端口**输入框输入端口并按回车进行添加。单击**查看可选范围**可以查询所有支持使用的端口。  **说明** ■ WAF旗舰版和独享版实例最多支持接入50个不同的服务器端口（包含80、8080、443、8443端口在内）；企业版和高级版实例最多支持接入10个服务器端口（包含80、8080、443、8443端口在内）。 ■ 关于公共集群支持的详细端口列表，请参见WAF支持的端口。 ■ 如果您要接入WAF独享集群，则自定义端口仅支持从**独享设置**页面中设置的**服务器端口**范围中选择。更多信息，请参见设置独享集群。

参数	说明
负载均衡算法	设置了多个源站服务器地址时，选择多源站服务器间的负载均衡算法。可选项： ■ **IP hash**（默认）：将某个IP的请求定向到同一个源站服务器。 **说明** 使用IP hash时，如果源站服务器的IP地址不够分散，可能会出现负载不均的情况。 ■ **轮询**：将所有请求轮流分配给源站服务器。 ■ **Least time**：通过智能DNS解析能力和升级后的Least-time回源算法，保证业务流量从接入防护节点到转发回源站服务器整个链路的时延最短。 **说明** Least time仅在开通智能负载均衡后支持使用。更多信息，请参见智能负载均衡。 设置生效后，WAF将根据设置的负载均衡算法向多个源站地址分发回源请求，实现负载均衡。
WAF前是否有七层代理（高防/CDN等）	选择网站业务在接入WAF前是否开启了其他七层代理服务（例如，DDoS高防、CDN等）。可选项： ■ **否**：表示WAF收到的业务请求来自发起请求的客户端。WAF直接取与WAF建立连接的IP（来自 `REMOTE_ADDR` 字段）作为客户端IP。 ■ **是**：表示WAF收到的业务请求来自其他七层代理服务转发，而非直接来自发起请求的客户端。为了保证WAF可以获取真实的客户端IP进行安全分析，您需要进一步设置**客户端IP判定方式**。 WAF默认读取请求Header字段 `X-Forwarded-For`（XFF）中的第一个IP地址作为客户端IP。  如果您的网站业务已通过其他代理服务的设置，规定将客户端源IP放置在某个自定义的Header字段（例如，X-Client-IP、X-Real-IP），则您需要选择**取指定Header字段中的第一个IP作为客户端源IP，避免XFF伪造**，并在**指定Header字段**框中输入对应的Header字段。 **说明** 推荐您在业务中使用自定义Header存放客户端IP，并在WAF中配置对应Header字段。该方式可以避免攻击者伪造XFF字段，躲避WAF的检测规则，提高业务的安全性。 支持输入多个Header字段。每输入完一个Header字段，需要按半角逗号（,）确认。设置了多个Header时，WAF将按顺序尝试读取客户端IP。如果第一个Header不存在，则读取第二个，以此类推。如果所有指定Header都不存在，则读取XFF中第一个IP地址作为客户端IP。

参数	说明
启用流量标记	设置是否启用WAF流量标记功能。 流量标记表示WAF在转发客户端请求到源站服务器时，在请求头中添加或修改由您指定的自定义字段，用于标记该请求经过WAF转发、记录该请求的客户端IP。 选中**启用流量标记**后，您需要设置标记字段。  标记字段分为以下类型： ■ **自定义Header**：需要设置**Header名**和**Header值**，使WAF在回源请求中添加该Header信息，标记请求经过WAF（区分没有经过WAF的请求，便于您的后端服务统计分析）。 例如，您可以使用 `ALIWAF-TAG: Yes` 标记经过WAF的请求，其中，`ALIWAF-TAG` 为Header名，`Yes` 为Header值。 **注意** 请不要填写标准的HTTP头部字段（例如User-Agent等），否则会导致标准头部字段内容被自定义的字段值覆盖。 ■ **客户端IP**：设置**记录IP的Header名**，使WAF在回源请求中，将该Header的值修改为客户端IP。关于WAF判定客户端IP的具体规则，请参见**WAF前是否有七层代理（高防/CDN等）**参数的描述。 如果您的后端服务需要从指定的自定义Header（例如，example-client-ip）中获取客户端IP进行业务分析，则您可以将该Header设置为**记录IP的Header名**。 **注意** 请不要填写标准的HTTP头部字段（例如User-Agent等），否则会导致标准头部字段内容被自定义的字段值覆盖。 单击**新增标记**，可以增加标记字段。最多支持设置5个标记字段。
资源组	从资源组列表中选择该域名所属资源组。 **说明** 您可以使用资源管理服务创建资源组，根据业务部门、项目等维度对云资源进行分组管理。更多信息，请参见创建资源组。

ii. **修改DNS解析**。

根据页面提示修改域名的DNS解析，将网站域名解析到WAF进行防护，完成后单击**下一步**。更多信息，请参见修改域名DNS。

iii. **添加完成**。

根据页面提示设置放行WAF回源IP段，完成后单击**完成，返回网站列表**，返回**网站接入**页面。更多信息，请参见放行WAF回源IP段。

上传HTTPS证书

如果您添加的网站信息的**协议类型**中包含**HTTPS**，您必须在Web应用防火墙控制台上传与该网站域名关联的HTTPS证书，且证书必须正确、有效，才能保证WAF正常防护网站的HTTPS协议访问请求。

上传HTTPS证书支持以下方式：

- 手动上传证书：您需要提前准备好网站的证书文件和私钥文件。
  需要准备的证书相关内容如下（上传时请确保证书有完整的证书链）：
  - *.crt（公钥文件）或*.pem（证书文件）
  - *.key（私钥文件）
- 选择已有证书：您可以直接从阿里云SSL证书服务已有证书中选择与域名关联的证书。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 在**域名列表**中定位到要操作的域名，单击**源站信息**列下的

   图标。

   > **说明** 只有在添加域名时选择了HTTPS协议类型，**源站信息**列下才会出现
   >
   > 
   >
   > 图标。

5. 在**上传证书**（或**更新证书**）对话框，选择一种**上传方式**上传HTTPS证书。

   > **说明** 如果您已经上传过证书，则显示**更新证书**对话框。**更新证书**对话框中的配置内容和**上传证书**对话框一致。

   - **手动上传**：填写**证书名称**，并将与域名关联的证书文件和私钥文件的文本内容分别复制粘贴到**证书文件**和**私钥文件**。

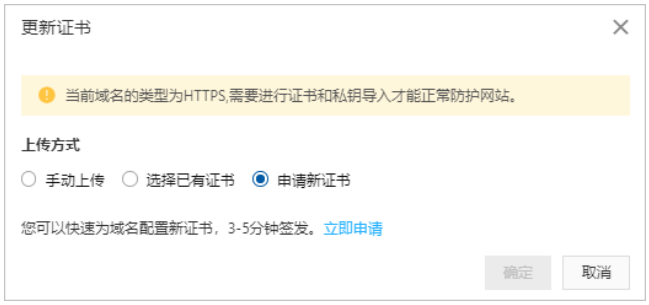
关于**证书文件**的说明如下：

- 如果证书是PEM、CER、CRT格式，您可以使用文本编辑器直接打开证书文件并复制其中的文本内容。
- 如果证书是除PEM、CER、CRT外的其他格式，例如PFX、P7B等，您需要将证书文件转换成PEM格式后，才可以使用文本编辑器打开并复制其中的文本内容。 关于证书格式的转换方法，请参见HTTPS证书转换成PEM格式。
- 请确保上传完整的证书链。如果域名关联了多个证书文件，您需要先将证书文件中的文本内容拼接合并，再粘贴到**证书文件**。

- **选择已有证书**：从**证书**列表选择要上传的证书。

证书列表罗列了SSL证书服务中已签发的证书，您可以从列表中选择与当前域名关联的证书。单击**云盾-证书服务**，可以跳转到SSL证书管理控制台管理证书。

- **申请新证书**：单击**立即申请**，跳转到SSL证书申请页面为域名快速申请证书。



按照页面提示为域名配置证书后，已配置证书将默认上传到Web应用防火墙。

> **说明** 快速申请证书仅支持申请收费型DV证书。如果您需要申请其他类型的证书，请前往SSL证书购买页面进行操作。更多信息，请参见选择购买方式购买SSL证书。

6. 单击**确定**。

后续配置

完成域名接入流程后，网站访问流量将经过WAF保护，您还需要完善以下配置，才能更好地防护网站安全。

配置类型	说明	相关文档
网站防护配置	WAF包含多种防护检测模块，帮助网站应对不同类型的安全威胁，其中**规则防护引擎**和**CC安全防护**模块默认开启，分别用于防御常见的Web应用攻击（例如，SQL注入、XSS跨站、Webshell上传等）和CC攻击，其他防护模块需要您手动开启并配置具体防护规则。	网站防护配置概述
告警配置	通过配置告警规则，您可以使WAF在网站请求流量中检测到攻击事件、异常流量时，向您发送告警通知，帮助您及时掌握业务的安全状态。	告警设置
日志服务配置	通过启用日志服务，您可以使WAF采集并存储网站业务的日志数据，供您进行业务查询与分析。WAF日志服务默认存储180天内的网站全量日志，帮助您满足等保合规要求。	日志服务概述

相关操作

成功添加域名后，您可以在**网站接入**页面的**域名列表**中查看已接入的域名并根据需要执行以下操作：

- 上传HTTPS证书：如果网站支持HTTPS协议，请务必确保在WAF上传正确的证书和私钥，保证正常防护HTTPS业务流量。您可以在**源站信息**列下单击上传域名的HTTPS证书和私钥。

  更多信息，请参见上传HTTPS证书。
- 开启IPv6防护：如果网站有IPv6协议业务流量需要防护，您可以在**快捷操作**列下为域名开启**IPV6**开关。更多信息，请参见开启IPv6防护。

- 开启日志服务：在**快捷操作**列下为域名开启**日志服务**后，WAF日志服务将采集网站的全量日志，支持用作查询分析、仪表盘展示、设置告警等功能。
  更多信息，请参见步骤2：开启日志采集。

  > 注意 日志服务是WAF提供的增值服务，必须开通后才能使用。更多信息，请参见步骤1：开通WAF日志服务。

- 设置防护资源：在**快捷操作**列下单击**防护资源**后的，为域名设置防护资源。
  支持的防护资源类型包括：
  - **共享集群共享IP**（默认）
  - **共享集群独享IP**：关于独享IP的介绍，请参见域名独享资源包。
  - **共享集群全局负载均衡防护**：关于全局负载均衡的介绍，请参见智能负载均衡。
  - **独享集群**：关于独享集群的介绍，请参见设置独享集群。
- 查看攻击监控报表：单击**攻击监控**列下的**查看报表**，跳转到**安全报表**页面，查看域名的防护报表。更多信息，请参见WAF安全报表。
- 设置防护策略：单击**操作**列下的**防护配置**，跳转到**网站防护**页面，设置**Web安全**、**Bot管理**、**访问控制/限流**防护模块的防护策略。更多信息，请参见网站防护配置概述。
- 编辑域名：单击**操作**列下的**编辑**，修改网站信息，例如，协议类型、服务器地址、服务器端口等。不支持修改域名。
- 删除域名：单击**操作**列下的**删除**，删除域名。

  > 警告 在删除域名前，请将域名DNS解析回服务器源站IP。否则，在删除域名后，域名的流量将无法正常转发。

相关问题

请参见常见问题中的**网站接入配置问题**。

2.2. 本地验证

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，建议您通过修改本地计算机的DNS解析，在本地计算机上验证WAF的域名接入设置正确有效。本文以Windows操作系统为例，介绍了在本地计算机验证域名接入设置的操作步骤。

前提条件

已通过CNAME接入模式手动添加网站域名。更多信息，请参见手动添加网站。

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. 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>
```

其中 `<被防护域名>` 表示已在WAF添加的域名，`<WAF IP地址>` 表示域名对应的WAF IP地址。`<WAF IP地址>` 和 `<域名>` 之间使用空格分隔。
获取WAF IP地址的操作步骤如下：

i. 登录Web应用防火墙控制台。

ii. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。

iii. 在左侧导航栏，选择**资产中心 > 网站接入**。

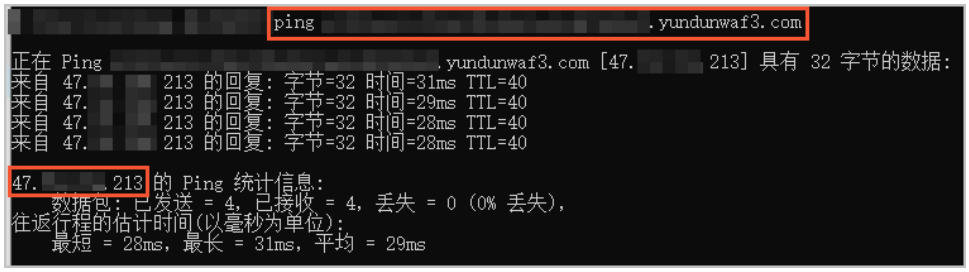
iv. 在**域名列表**中，定位到已添加的域名，将光标放置在域名上，然后单击

，复制域名对应的WAF **Cname**地址。

v. 在Windows操作系统中，打开cmd命令行工具。

vi. 执行以下命令：

```
ping <已复制的WAF Cname地址>
```



vii. 在 `ping` 命令的返回结果中，记录域名对应的WAF IP地址。

示例：假设已在WAF添加的域名是 `test.aliyundoc.com`，域名对应的WAF IP地址是 `47.XX.XX.213`，则在*hosts*文件最后一行添加以下内容：

```
47.XX.XX.213 test.aliyundoc.com
```

4. 保存修改后的*hosts*文件，并执行 `ping <被防护域名>` 命令，验证hosts修改已生效。

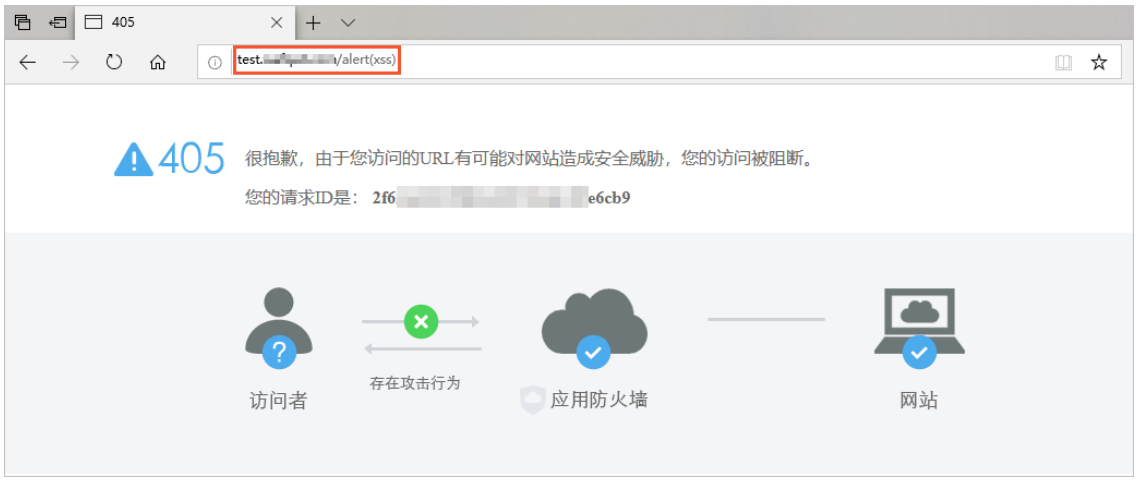
预期 `ping` 命令解析到的IP地址是域名对应的WAF IP地址，表示hosts修改已经生效。
如果解析到了源站IP地址，请刷新本地的DNS缓存（可以执行 `.\ipconfig /flushdns` 命令）并重新执行ping命令，直到验证hosts修改已经生效。

5. 打开本地计算机的浏览器，在地址栏输入被防护域名进行访问。
   - 如果网站能够正常访问，说明WAF中添加的域名设置正确有效。您可以在将*hosts*文件复原后，放心修改域名的DNS解析，将网站流量解析到WAF进行防护。更多信息，请参见修改域名DNS。
   - 如果网站访问不正常，说明WAF中添加的域名设置可能有问题，建议您检查WAF中的域名接入设置，修复问题后重新进行本地验证。更多信息，请参见添加域名。

6. （可选）本地模拟简单的Web攻击命令，查看WAF的防护效果。

例如，您可以在浏览器的地址栏输入 `<被防护域名>/alert(xss)`（这是一个用作测试的Web攻击请求），查看针对Web应用攻击的防御效果。

预期WAF会返回一个拦截页面。



7. 完成本地验证后，重新修改*hosts*文件，删除步骤3中添加的记录。

> **注意** 如果您没有及时删除对应记录，将可能导致本地计算机访问被防护域名的请求出现异常。

获取技术支持

如果您无法排查出域名接入设置的故障，需要进一步技术支持，请参考以下途径：

- 登录Web应用防火墙控制台，在左侧导航栏底部单击**有问题，找专家**，通过钉钉扫码加入钉钉群（群号：21715946），联系阿里云安全产品专家进行协助。
- 提交工单。
- 购买Web应用防火墙支持服务，获取第三方服务团队提供的专业技术支持，包括WAF接入指导和基础安全咨询等。

2.3. 放行WAF回源IP段

WAF使用特定的回源IP段将经过防护引擎检测后的正常流量转发回网站域名的源站服务器。网站接入WAF进行防护后，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。

背景信息

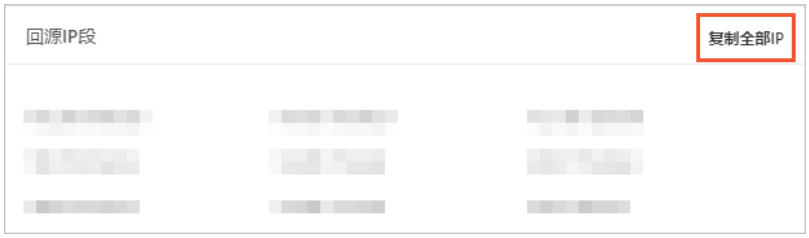
如果您的源站服务器上使用了安全狗、云锁等安全软件，您必须在源站安全软件中设置放行WAF回源IP段，避免由WAF转发回源站服务器的正常流量被误判断为异常攻击而被拦截，影响网站正常访问。

出于安全性考虑，建议您在网站流量成功接入WAF后，设置源站服务器的访问控制策略，只允许WAF回源IP段的入方向流量，避免攻击者绕过WAF直接对源站服务器发起攻击。更多信息，请参见设置源站保护。

获取WAF回源IP段

1. 登录Web应用防火墙控制台。
2.
3. 在左侧导航栏，选择**系统管理 > 产品信息**。
4. 在**产品信息**页面底部，定位到**回源IP段**区域，单击**复制全部IP**。

   回源IP段区域实时显示最新的WAF回源IP段。



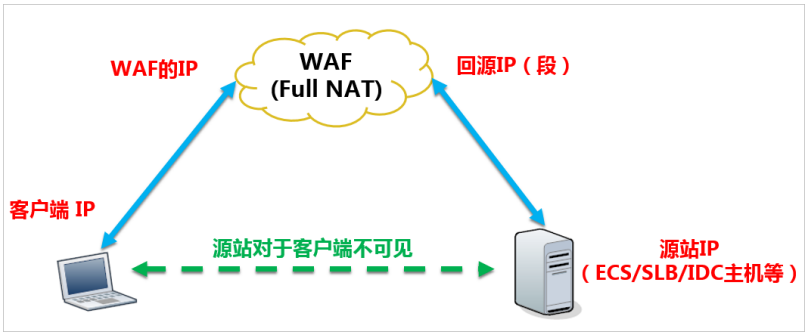
后续步骤

获取WAF回源IP段后，您需要将回源IP段添加到源站安全软件的白名单中。

> **警告** 如果您没有在源站设置放行WAF的回源IP段，则WAF转发回源站的正常业务请求可能会被误拦截，导致业务中断。

常见问题

- 什么是WAF回源IP段？
  回源IP段是WAF代理真实客户端请求源站服务器时使用的IP地址段。在源站服务器看来，网站接入WAF后，所有请求来源IP都会变成WAF的回源IP，而真实的客户端IP会被添加在HTTP头部的XFF字段中。



- 为什么要放行WAF回源IP段？
  网站接入WAF后，由于访问来源IP变得更加集中，访问频率变得更高，服务器上的防火墙或安全软件很容易认为这些IP在发起攻击，从而将WAF回源IP段拉黑。如果WAF的回源IP段被拉黑，WAF的请求将无法得到源站的正常响应。因此，在网站接入WAF后，您应确保源站服务器已将WAF的全部回源IP放行（即加入白名单），不然可能会出现网站打不开或打开极其缓慢等情况。

相关FAQ

- WAF是否会自动将WAF回源IP段加入安全组？
- WAF回源是否需要放行所有客户端IP？

2.4. 修改域名DNS

在Web应用防火墙（Web Application Firewall，简称WAF）添加网站域名后，您必须使用WAF的CNAME地址（或IP地址）修改域名的DNS解析设置，将网站的Web请求解析到WAF进行安全防护。本文介绍了修改域名DNS的相关内容。

背景信息

WAF支持通过以下两种方式接入域名的Web请求：

- CNAME接入：将域名解析到WAF的CNAME地址。
  推荐您使用CNAME接入。在某些极端情况下（例如节点故障、机房故障等），CNAME接入可以实现自动切换节点IP，甚至直接将解析切回源站，从而最大程度保证业务的稳定运行，提供高可用性和灾备能力。

- A记录接入：将域名解析到WAF的IP地址。
  建议您仅在CNAME接入与当前域名解析设置存在冲突时（例如CNAME记录与MX记录冲突且必须保留MX记录），再使用A记录接入。
  关于DNS解析记录冲突的详细说明，请参见解析记录冲突规则。

本文内容适用于为网站单独开启WAF防护，即网站不接入CDN、DDoS高防等其他代理型服务。如果您需要同时部署WAF和其他代理型服务，请参见以下文档：

- 同时部署WAF和CDN
- 通过联合部署DDoS高防和WAF提升网站防护能力

前提条件

- 已通过CNAME接入模式在WAF中手动添加要防护的网站信息。具体操作，请参见手动接入域名。
- 拥有在域名的DNS服务商处修改域名解析设置的权限。
- （可选）已在源站服务器上放行WAF回源IP段。更多信息，请参见放行WAF回源IP段。

  注意 如果源站服务器上使用了非阿里云安全软件（例如安全狗、云锁），您需要在这些软件上设置放行WAF的回源IP段，防止由WAF转发到源站的正常业务流量被拦截。

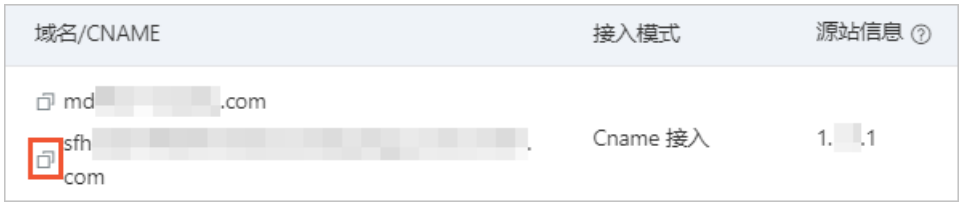
- （可选）已通过本地验证确保转发配置生效。通过本地验证确保WAF的网站转发配置正常，防止因配置错误导致业务中断。更多信息，请参见本地验证。

  警告 如果在WAF的网站转发配置未生效时修改域名DNS，可能导致业务中断。

获取WAF CNAME地址或WAF IP地址

修改域名DNS前，您必须先获取域名对应的WAF CNAME地址或WAF IP地址。如果您在添加域名时已经获得相关地址，请忽略以下步骤。

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 在**域名列表**中定位到已添加的域名，将光标悬置在域名上，查看并复制域名对应的WAF CNAME地址。



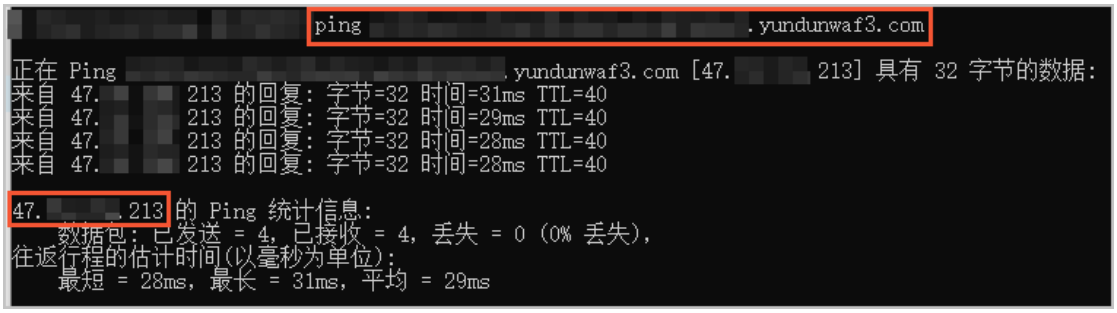
5. （可选）获取域名对应的WAF IP地址。

   说明 仅在使用A记录接入时需要获取WAF IP地址。如果您使用CNAME接入，请忽略该步骤。

   i. 在Windows操作系统中，打开cmd命令行工具。

ii. 执行以下命令：

```
ping <已复制的WAF CNAME地址>
```



iii. 在Ping命令的返回结果中，记录域名对应的WAF IP地址。

使用云解析DNS修改域名解析

以下操作以阿里云云解析DNS为例介绍修改域名解析记录的方法。如果您的域名解析托管在阿里云云解析DNS，您可以直接参照以下步骤进行操作。如果您使用其他服务商的DNS服务，请参照以下步骤在域名DNS服务商的系统上进行类似配置。

1. 登录云解析DNS控制台。
2. 在**域名解析**页面，定位到要设置的域名，单击其**操作**列下的**解析设置**。
3. 在**解析设置**页面，定位到要设置的**主机记录**，单击其**操作**列下的**修改**。

   关于主机记录的选择，以 `aliyun.com` 域名为例：

   - **www**：用于精确匹配www开头的域名，例如 `www.aliyun.com` 。
   - **@**：用于匹配根域名，例如 `aliyun.com` 。
   - ***：用于匹配泛域名，包括根域名和所有子域名，例如 `blog.aliyun.com` 、 `www.aliyun.com` 、 `aliyun.com` 等。
4. 在**修改记录**对话框，选择使用CNAME接入或A记录接入的方式修改记录。
   - **CNAME接入**：将**记录类型**设置为**CNAME**、**记录值**修改为WAF CNAME地址，其余设置保持不变。

     > **说明** TTL值一般建议设置为10分钟。TTL值越大，DNS记录的同步和更新越慢。

关于不同记录类型的冲突需注意以下情况：

- 对于同一个主机记录，CNAME解析记录值只能填写一个，您需要将其修改为WAF CNAME地址。
- 不同DNS解析记录类型间存在冲突。例如，对于同一个主机记录，CNAME记录与A记录、MX记录、TXT记录等其他记录互相冲突。在无法直接修改记录类型的情况下，您可以先删除存在冲突的其他记录，再添加一条新的CNAME记录。

  > **警告** 删除其他解析记录并新增CNAME解析记录的过程应尽可能在短时间内完成。如果删除A记录后长时间没有添加CNAME解析记录，可能导致域名无法正常解析。

- 如果必须保留MX记录（邮件服务器记录），建议您使用A记录接入的方式将域名解析到WAF IP。

- **A记录接入**：将**记录类型**设置为**A**、**记录值**修改为WAF IP地址，其余设置保持不变。

  > **说明** TTL值一般建议设置为10分钟。TTL值越大，DNS记录的同步和更新越慢。

5. 单击**确定**，完成解析设置修改，等待修改后的DNS解析记录生效。
6. 验证DNS解析设置。您可以ping网站域名或使用DNS检测工具验证DNS解析是否生效。

> **说明** 由于DNS解析记录生效需要一定时间，如果验证失败，您可以等待10分钟后重新验证。

相关操作

- 开启源站保护
  开启源站保护可以防止攻击者在获取源站服务器的真实IP后，绕过WAF直接攻击您的源站。建议您通过配置源站ECS的安全组或源站SLB的白名单，防止恶意攻击者直接攻击您的源站。更多信息，请参见设置源站保护。
- 获取客户端真实IP
  网站接入WAF后，源站服务器收到的回源请求全部来自WAF，您必须通过 `X-Forwarded-For` 请求头字段获取访问者的真实IP。更多信息，请参见获取客户端真实IP。

2.5. 设置端口

通过Cname接入方式将网站接入Web应用防火墙（WAF）实例防护时，您需要设置该网站使用的HTTP/HTTPS端口。设置端口并完成网站接入后，通过该端口访问网站的流量会经过WAF，并受到WAF的检测和防护。

背景信息

完成网站接入后，WAF只通过在接入网站时已添加的服务器端口，向源站服务器转发业务流量。对于未添加的端口，WAF不会转发任何来自该端口的访问请求流量到源站服务器。
WAF防护的端口包含标准端口和非标准端口，不同的版本支持的端口数量和非标准端口范围有所不同。具体差异，请参见各版本支持的端口。

应用场景

您需要在以下场景下设置端口：

- 通过Cname接入方式将网站接入WAF进行防护时，您需要设置该网站使用的HTTP/HTTPS端口号。

- 该网站使用的HTTP/HTTPS端口号有修改时，您需要更改端口设置。

操作步骤

1. 登录Web应用防火墙控制台。
2.
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 在**域名列表**中，定位到要操作的域名，单击操作列下的**编辑**。
5. 在**编辑**页面，定位到**服务器端口**区域，分别在**HTTP端口**框、**HTTPS端口**框中输入对应的端口号。

   每输入一个端口号，按回车完成添加。

   > **注意** 输入的端口必须在可选范围内，否则无法保存。您可以单击**查看可选范围**，查询某个端口是否在可选范围内。

6. 单击**确定**，保存网站接入配置。

其他相关问题

已接入网站的未配置端口是否会对源站带来安全风险？

WAF是否支持自定义端口？

非标端口业务无法接入Web应用防火墙高级版

2.6. 自定义TLS配置

已接入WAF防护的网站域名，如果网站使用的是HTTPS协议传输数据，WAF支持对该域名自定义TLS协议版本和加密套件，更灵活地满足您对于更高安全性（例如，等保合规场景）或更高的TLS通信兼容性（例如，兼容客户端旧版本的TLS协议）的需求。

背景信息

为有效保证您网站的通信安全，WAF对已接入的HTTPS域名指定默认的TLS配置，对不在指定范围内的TLS协议版本和加密套件的访问流量进行拦截。

WAF目前已支持对TLS加密套件自定义，有效避免因网站使用的加密套件和WAF默认配置的加密套件不匹配，导致访问失败的问题。您可以根据网站的实际情况，为已接入的域名修改TLS协议版本和加密套件。

前提条件

- 域名已完成网站接入。具体操作，请参见添加域名。
- 网站域名使用的是HTTPS协议且已上传了HTTPS证书。具体操作，请参见上传HTTPS证书。

配置TLS

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**资产中心 > 网站接入**。
3. 在**网站接入**页面，定位到需要配置TLS的域名，单击**操作**列的**TLS配置**。

   > 注意 只有使用了HTTPS协议的网站域名需要配置TLS。如果网站域名使用的是HTTP协议或者使用HTTPS协议但是未上传HTTPS证书，**操作**列不显示**TLS配置**。

4. 在**TLS安全策略配置**页面，对TLS协议版本和加密套件进行自定义配置。

配置项	说明
域名	需要自定义配置TLS的网站域名。此项已自动填写，无需您手动设置。
TLS协议版本	选择网站使用的TLS版本。可选项： ○ **支持TLS 1.0及以上版本，兼容性最高，安全性较低**：选择该项表示对TLS 1.0及以上所有版本生效。 ○ **支持TLS 1.1及以上版本，兼容性较好，安全性较好**：选择该项表示对TLS 1.1及以上所有版本生效，使用TLS 1.0将无法访问该网站。 ○ **支持TLS 1.2及以上版本，兼容性较好，安全性最高**：选择该项表示对TLS 1.2及以上所有版本生效，使用TLS 1.0和1.1将无法访问该网站。
开启TLS 1.3	支持同时开启TLS 1.3。

配置项	说明
加密套件	选择您需要使用的加密套件类型。可选项： ○ **全部加密套件，兼容性最高，安全性较低**，支持以下强加密套件和弱加密套件： ■ 强加密套件： ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ■ 弱加密套件： ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ■ TLS_RSA_WITH_AES_128_GCM_SHA256 ■ TLS_RSA_WITH_AES_256_GCM_SHA384 ■ TLS_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_RSA_WITH_AES_256_CBC_SHA256 ■ TLS_RSA_WITH_AES_128_CBC_SHA ■ TLS_RSA_WITH_AES_256_CBC_SHA ■ SSL_RSA_WITH_3DES_EDE_CBC_SHA ○ **协议版本的自定义加密套件，请谨慎选择，避免影响业务**

5. 单击**保存**，配置即可生效。

   WAF会拦截使用了非指定范围内的TLS协议版本和加密套件的访问流量。

2.7. 设置源站保护

通过CNAME接入方式将网站接入Web应用防火墙（WAF）防护后，您可以设置源站服务器的访问控制策略，只放行WAF回源IP段的入方向流量，防止黑客获取您的源站IP并绕过WAF直接攻击源站。本文介绍了源站服务器部署在云服务器ECS、负载均衡SLB时，如何设置对应的安全组规则和白名单策略。

前提条件

- 源站服务器部署在云服务器ECS、负载均衡SLB。
- 源站ECS实例或SLB实例上的所有域名都已经通过**CNAME接入**方式接入WAF防护。
  相关操作，请参见添加域名。

> **注意** 如果您使用**透明接入**方式，将源站SLB、ECS的业务流量接入WAF防护，则对应的引流端口默认受到保护，攻击者无法绕过WAF直接攻击源站，因此，您无需按照本文介绍去设置源站保护。更多信息，请参见透明接入。

风险须知

网站接入WAF进行防护后，无论您是否设置源站保护，都不影响正常业务的转发。设置源站保护可以帮助您预防攻击者在源站IP暴露的情况下，绕过WAF直接攻击您的源站。关于如何判断源站是否存在IP泄露风险，请参见如何检测源站是否存在IP泄露风险？。

配置源站服务器的访问控制策略存在一定风险。在设置源站保护前，请注意以下事项：

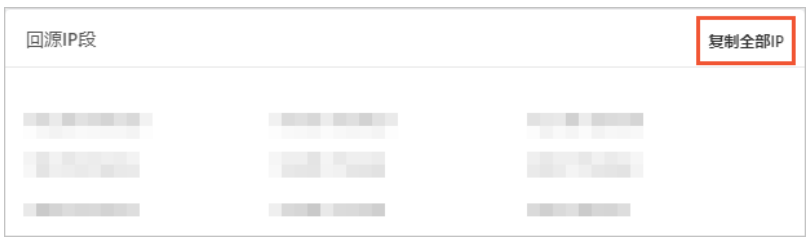
- 请确保同一源站ECS实例、SLB实例上的所有域名都已经接入WAF进行防护，避免攻击者通过未接入WAF的域名入侵源站，从而影响其他域名业务。
- WAF在集群出现故障时，可能会将域名访问请求旁路回源至源站，确保网站正常访问。这种情况下，如果源站已设置ECS安全组、SLB白名单访问控制策略，可能会导致源站暂时无法通过公网访问。
- 当WAF集群扩容增加新的回源IP段时，如果源站已设置ECS安全组、SLB白名单防护，可能会导致频繁出现5XX错误响应。建议您定期关注Web应用防火墙控制台发布的回源网段变更通知，及时更新涉及回源IP网段的访问控制策略。
- 如果您不再使用WAF，在将业务流量切回源站服务器之前，请务必先删除已添加的访问控制策略，放行所有业务流量，避免业务流量切回后出现业务中断。

获取WAF回源IP段

> **注意** WAF回源IP段会定期更新，请关注定期变更通知，及时将更新后的回源IP段添加至相应的安全组、白名单规则中，避免出现误拦截。

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**系统管理 > 产品信息**。
4. 在**产品信息**页面底部，定位到**回源IP段**区域，单击**复制全部IP**。

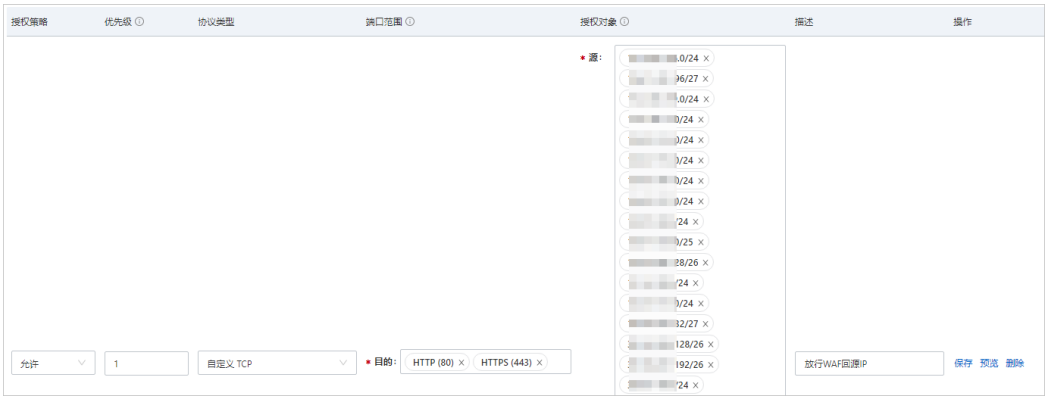
   回源IP段区域实时显示最新的WAF回源IP段。



设置ECS安全组规则

如果您的源站服务器直接部署在云服务器ECS实例，请在获取WAF回源IP段后，参照以下步骤设置源站ECS实例的安全组规则。通过设置安全组规则，只放行WAF回源IP段的入方向流量。

1. 登录云服务器ECS控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏，选择ECS实例的资源组和地域。
4. 在**实例列表**，定位到要操作的实例，在**操作**列下选择**更多 > 网络和安全组 > 安全组配置**。
5. 定位到要设置的安全组，单击**操作**列下的**配置规则**。
6. 添加一条优先级最高的安全组规则，放行WAF回源IP段的入方向流量。
   i. 在**访问规则**区域的**入方向**页签下，单击**手动添加**。
   ii. 完成以下规则配置，并单击**保存**。



配置项	说明
授权策略	选择**允许**。
优先级	输入**1**，表示优先级最高。
协议类型	选择**自定义TCP**。
端口范围	选择**HTTP（80）**和**HTTPS（443）**。
授权对象	将已复制的WAF回源IP段粘贴到**源**输入框。 您可以按Ctrl+V键进行粘贴。
描述	自定义描述信息。示例：放行WAF回源IP。

> **注意** 如果当前安全组防护的服务器与WAF回源IP以外的其他IP、HTTP/HTTPS以外的其他应用有交互，请将这些交互IP和端口通过安全组一并加白放行。

成功添加该安全组规则后，ECS实例安全组将以最高优先级放行WAF回源IP段的所有入方向流量。

> **警告** 请务必确保所有WAF回源IP段都已通过源站ECS实例的安全组规则设置了入方向的允许策略，否则可能导致网站访问异常。

7. 添加一条优先级最低的安全组规则，拒绝所有IP段的入方向流量。

i. 在**访问规则**区域的**入方向**页签下，单击**手动添加**。

ii. 完成以下规则配置，并单击**保存**。

配置项	说明
授权策略	选择**拒绝**。
优先级	输入**100**，表示优先级最低。
协议类型	选择**自定义TCP**。
端口范围	选择**HTTP（80）**和**HTTPS（443）**。
授权对象	在源输入框，输入*0.0.0.0/0*（表示所有IP段）并按回车键。
描述	自定义描述信息。示例：拒绝所有入方向流量。

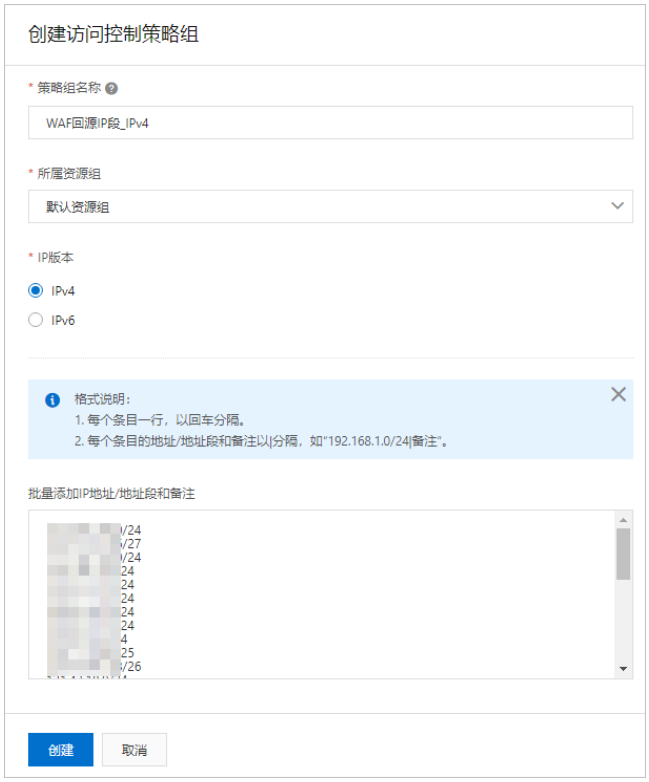
成功添加该安全组规则后，ECS实例安全组除了放行WAF回源IP段的入方向流量（步骤6定义的规则）外，还将拒绝所有其他IP段的入方向流量，保证所有业务流量都经WAF转发到源站ECS实例。

开启SLB访问控制

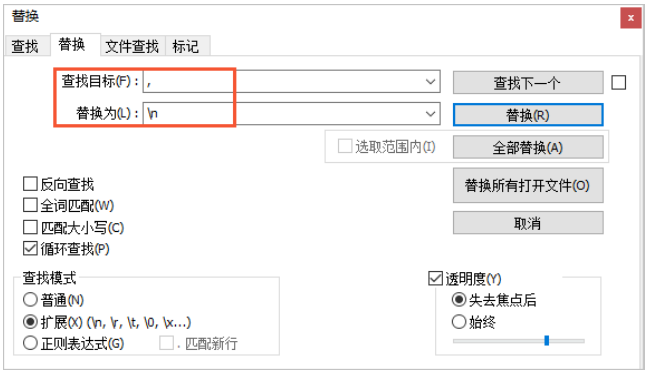
如果您的源站服务器部署了负载均衡SLB，请在获取WAF回源IP段后，参照以下步骤设置SLB实例的访问控制（白名单）策略。通过开启访问控制（白名单），只放行WAF回源IP段的入方向流量。

以下操作描述以传统型负载均衡CLB为例进行介绍。如果您使用应用型负载均衡ALB，请结合以下操作描述及ALB访问控制文档进行操作。

1. 登录负载均衡SLB控制台。
2. 在左侧导航栏，选择**传统型负载均衡CLB（原SLB）** > **访问控制**。
3. 在顶部菜单栏，选择SLB实例的资源组和地域。
4. 创建访问控制策略组。
   i. 在**访问控制**页面，单击**创建访问控制策略组**。
   ii. 在**创建访问控制策略组**面板，完成以下策略组配置，并单击**创建**。



以下配置表示为所有IPv4类型的WAF回源IP创建一个策略组。

配置项	说明
策略组名称	自定义策略组名称。示例：WAF回源IP段_IPv4。
所属资源组	选择策略组所属资源组。
IP版本	选择**IPv4**。
批量添加IP地址/地址段和备注	粘贴所有IPv4类型的WAF回源IP。 每行只允许输入一个条目。多个条目间通过回车分隔。 **说明** 由于复制获取的所有WAF回源IP段之间以半角逗号（,）分隔，建议您使用支持扩展替换的文本编辑器，将半角逗号（,）统一替换为换行符（\n）再进行粘贴。 

iii. 再次执行步骤b~c，为所有IPv6类型的WAF回源IP创建一个策略组。

与步骤c有差异的配置说明如下：

- **策略组名称**：您可以将该策略组命名为“WAF回源IP段_IPv6”。
- **IP版本**：选择**IPv6**。
- **批量添加IP地址/地址段和备注**：粘贴所有IPv6类型的WAF回源IP。

5. 为监听设置访问控制策略。

i. 在左侧导航栏，选择**传统型负载均衡CLB（原SLB）** > **实例管理**。

ii. 在**实例管理**列表，定位到要操作的实例，单击实例ID。

iii. 在**监听**列表，定位到要设置的监听，在**操作**列下单击 ⋮ 图标，然后单击**设置访问控制**。

请根据已接入WAF防护的业务类型，选择要设置的监听：

- 如果您已将HTTP业务接入WAF防护，则需要设置HTTP监听。
- 如果您已将HTTPS业务接入WAF防护，则需要设置HTTPS监听。
- 如果您已将HTTP和HTTPS业务接入WAF防护，则需要分别设置HTTP监听和HTTPS监听。

iv. 在**访问控制设置**页面，打开**启动访问控制**开关并完成以下配置。

配置项	说明
访问控制方式	选择**白名单：允许特定IP访问负载均衡SLB**。
选择访问控制策略组	根据CLB实例的IP版本，选择WAF回源IP对应的访问控制策略组： ■ IPv4类型CLB实例仅支持选择IPv4版本的策略组。 ■ IPv6类型CLB实例仅支持选择IPv6版本的策略组。

完成以上配置后，CLB实例监听将会放行WAF回源IP段的入方向流量。

后续操作

完成ECS安全组、SLB白名单设置后，您可以通过测试源站IP的80端口和8080端口是否能成功建立连接，验证设置是否已生效。

如果端口无法直接连通，但网站业务仍可正常访问，则表示源站保护已设置成功。

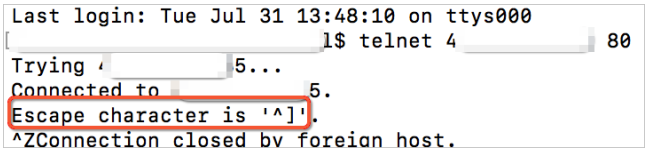
如何检测源站是否存在IP泄露风险？

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，检测是否能够成功建立连接：

- 如果可以连通，表示源站存在IP泄露风险，一旦黑客获取到源站公网IP就可以绕过WAF直接访问源站。

- 如果无法连通，表示源站当前不存在IP泄露风险。

示例：测试已接入WAF进行防护的源站IP的80端口和8080端口是否能成功建立连接。以下截图中的测试结果显示端口可以连通，说明源站存在IP泄露风险。



2.8. 获取客户端真实IP

网站部署了流量代理服务（例如Web应用防火墙、DDoS高防、CDN）后，源站服务器可以通过解析回源请求中的X-Forwarded-For记录，获取客户端的真实IP。本文介绍了不同类型的Web应用服务器（包括Nginx、IIS 6、IIS 7、Apache、Tomcat）以及容器K8s如何进行相关设置，以获取客户端的真实IP。

背景信息

在大部分实际业务场景中，网站访问请求并不是简单地从客户端（访问者）的浏览器直接到达网站的源站服务器，而是在客户端和服务器之前经过了根据业务需要部署的Web应用防火墙、DDoS高防、CDN等代理服务器。这种情况下，访问请求在到达源站服务器之前可能经过了多层安全代理转发或加速代理转发，源站服务器该如何获取发起请求的真实客户端IP?

透明的代理服务器在将客户端的访问请求转发到下一环节的服务器时，会在HTTP的请求头中添加一条X-Forwarded-For记录，用于记录客户端的IP，格式为 `X-Forwarded-For:客户端IP` 。如果客户端和服务器之间有多个代理服务器，则X-Forwarded-For记录使用以下格式记录客户端IP和依次经过的代理服务器IP： `X-Forwarded-For:客户端IP，代理服务器1的IP，代理服务器2的IP，代理服务器3的IP，……` 。

因此，常见的Web应用服务器可以通过解析X-Forwarded-For记录获取客户端真实IP。

下文分别针对Nginx、IIS 6、IIS 7、Apache和Tomcat服务器以及容器K8s，介绍相应的X-Forwarded-For配置方案。

> **注意** 开始配置之前，请务必对现有环境进行备份，包括ECS快照备份和Web应用服务器配置文件备份。

Nginx配置方案

Nginx服务器使用http_realip_module模块获取客户端IP地址。

1. 安装http_realip_module模块。

   在Nginx服务器上执行 `# nginx -V | grep http_realip_module` 命令，查看是否已安装http_realip_module模块。如果没有安装，请重新编译Nginx服务并安装该模块。

   > **说明** 一般情况下，通过一键安装包安装的Nginx服务器默认不安装http_realip_module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_stat
us_module --without-http-cache --with-http_ssl_module --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服务配置文件。
   i. 打开 `default.conf` 配置文件。
   ii. 在 `location / {}` 中添加以下内容：

   ```
   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>`、`<ip_range2>`、`<ip_rangex>`需要设置为代理服务器（即Web应用防火墙）的回源IP段。关于Web应用防火墙的回源IP段，请参见放行WAF回源IP段。
   多个回源IP段必须分行添加。假设代理服务器的回源IP段包含10.0.0.1、10.0.0.2、10.0.0.3，则使用以下格式：

   ```
   set_real_ip_from 10.0.0.1;
   set_real_ip_from 10.0.0.2;
   set_real_ip_from 10.0.0.3;
   real_ip_header X-Forwarded-For;
   ```

3. 修改log_format日志记录格式。
   i. 打开 `nginx.conf` 配置文件，定位到 `http` 配置部分的 `log_format` 。
   ii. 在 `log_format` 中添加 `x-forwarded-for` 字段，替换默认的 `remote-address` 字段。
   修改后的log_format内容如下：

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

4. 执行 `nginx -s reload` 命令，重启Nginx服务。
   重启Nignx服务器后，上述配置才会生效，Nignx服务器将可以通过X-Forwarded-For记录获取客户端真实IP。

IIS 6配置方案

IIS 6服务器必须安装 `F5XForwardedFor.dll` 插件，才可以从服务器记录的访问日志中获取客户端IP地址。

1. 根据服务器操作系统版本，将 `x86\Release` 或 `x64\Release` 目录下的 `F5XForwardedFor.dll` 文件拷贝到某个自定义目录（例如 `C:\ISAPIFilters` ）。

   > **说明** 请确保IIS进程对自定义目录拥有读取权限。

如果 `x86\Release` 或 `x64\Release` 目录下没有 `F5XForwardedFor.dll` 插件，您可以手动下载F5XForwardedFor.dll。

2. 打开IIS管理器，定位到当前开启的网站，在网站上右键单击**属性**。
3. 在**属性**页切换到**ISAPI筛选器**，单击**添加**。
4. 在添加对话框，完成以下参数设置，并单击**确定**。
   - **筛选器名称**：输入 `F5XForwardedFor` 。
   - **可执行文件**：填写 `F5XForwardedFor.dll` 的完整路径，例如 `C:\ISAPIFilters\F5XForwardedFor.dll` 。
5. 重启IIS服务器，等待配置生效。

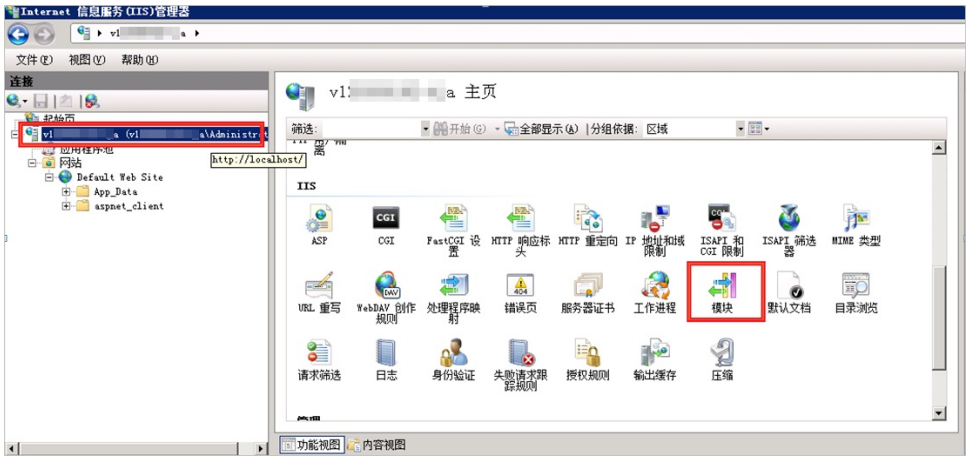
IIS 7配置方案

IIS 7服务器必须安装F5XForwardedFor模块，才可以从服务器记录的访问日志中获取客户端IP地址。

1. 根据服务器操作系统版本，将 `x86\Release` 或 `x64\Release` 目录下的 `F5XFFHttpModule.dll` 和 `F5XFFHttpModule.ini` 文件拷贝到某个自定义目录（例如 `C:\x_forwarded_for\x86` 或 `C:\x_forwarded_for\x64` ）。

   > **说明** 请确保IIS进程对自定义目录拥有读取权限。

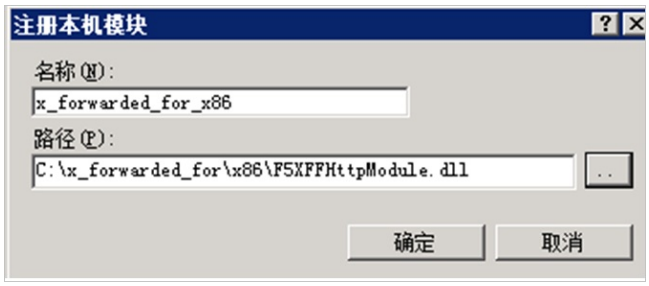
   如果 `x86\Release` 或 `x64\Release` 目录下没有 `F5XFFHttpModule.dll` 和 `F5XFFHttpModule.ini` ，您可以手动下载F5XForwardedFor模块。
2. 在IIS选项中，双击打开**模块**。



3. 单击**配置本机模块**。

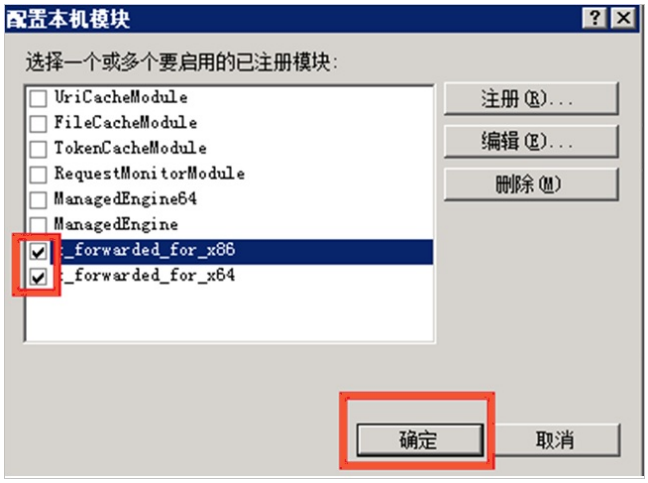
4. 在**配置本机模块**对话框，单击**注册**，服务器操作系统版本注册相关的DLL文件。
   - 32为操作系统注册x_forwarded_for_x86模块
     - **名称**：输入 `x_forwarded_for_x86` 。

- **路径**：填写 `F5XFFHttpModule.dll` 的完整路径，例如 `C:\x_forwarded_for\x86\F5XFFHttpModule.dll` 。

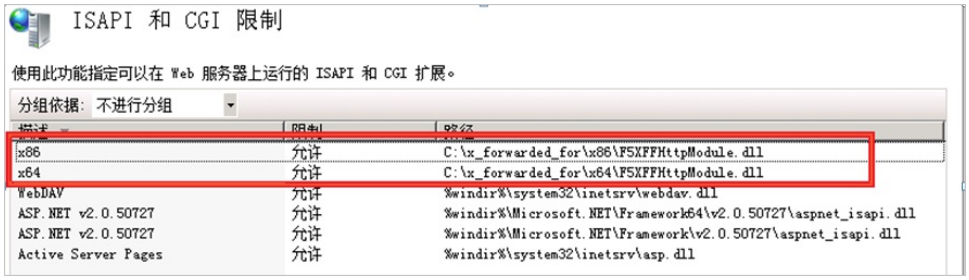


- 64为操作系统注册x_forwarded_for_x64模块
  - **名称**：输入 `x_forwarded_for_x64` 。
  - **路径**：填写 `F5XFFHttpModule.dll` 的完整路径，例如*C:\x_forwarded_for\x64\F5XFFHttpModule.dll*。

5. 在**配置本机模块**对话框，选中新注册的模块（x_forwarded_for_x86、x_forwarded_for_x64）并单击**确定**。



6. 在**ISAPI 和CGI限制**页面，添加已注册的DLL，并将**限制**设置为**允许**。



7. 重启IIS服务器，等待配置生效。

Apache配置方案

Windows操作系统

Apache 2.4及以上版本的安装包中自带remoteip_module模块文件（ `mod_remoteip.so` ），Apache服务器使用该模块获取客户端IP地址。

1. 进入Apache服务器的extra配置文件夹（ `conf/extra/` ），新建 `httpd-remoteip.conf` 配置文件。

   > **说明** 通过引入 `remoteip.conf` 配置文件的方式加载相关配置，减少直接修改 `httpd.conf` 配置文件的次数，避免因操作失误导致业务异常。

2. 编辑 `httpd-remoteip.conf` 配置文件，在文件中添加以下内容：

   ```
   # 加载mod_remoteip.so模块
   LoadModule remoteip_module modules/mod_remoteip.so
   # 设置RemoteIPHeader头部
   RemoteIPHeader X-Forwarded-For
   # 设置回源IP段
   RemoteIPInternalProxy <ip_range1> <ip_range2> …… <ip_rangex>
   ```

   其中， `<ip_range1>` 、 `<ip_range2>` 、 `<ip_rangex>` 需要设置为代理服务器（即Web应用防火墙）的回源IP段。关于Web应用防火墙的回源IP段，请参见放行WAF回源IP段。
   多个回源IP段之前使用空格分隔。假设代理服务器的回源IP段包含10.0.0.1、10.0.0.2、10.0.0.3，则使用以下格式：

   ```
   RemoteIPInternalProxy 10.0.0.1 10.0.0.2 10.0.0.3
   ```

3. 编辑*conf/httpd.conf*配置文件，在文件中添加以下内容：

   ```
   Include conf/extra/httpd-remoteip.conf
   ```

   以上命令表示在*conf/httpd.conf*中插入 `httpd-remoteip.conf` 配置文件。

4. 在 `httpd.conf` 配置文件中修改日志格式。

   ```
   LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
   LogFormat "%a %l %u %t \"%r\" %>s %b" common
   ```

5. 重启Apache服务，使配置生效。

Linux操作系统

您可以参考上述Windows操作系统服务器的配置方式，添加Apache 2.4及以上版本自带的remoteip_module模块（ `mod_remoteip.so` ）并配置日志格式，获取客户端IP地址。

如果Linux服务器使用的Apache版本低于2.4，请参照以下步骤，通过设置Apache的第三方模块（mod_rpaf），获取客户端IP地址。

1. 安装mod_rpaf模块。

   ```
   wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.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. 编辑Apache配置文件 `/alidata/server/httpd/conf/httpd.conf` ，在文件最后添加以下内容：

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

其中，`<rpaf ip地址>`不是代理服务器的公网IP地址，具体IP请通过Apache日志查询。通常包含两个IP地址，示例如下：

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 10.XX.XX.65 10.XX.XX.131
RPAFheader X-Forwarded-For
```

3. 重启Apache服务，使配置生效。

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

更多Apache相关模块的信息，请参见Apache帮助文档。

Tomcat配置方案

Tomcat服务器通过启用X-Forwarded-For功能，获取客户端IP地址。

1. 打开`tomcat/conf/server.xml`配置文件。
2. 将AccessLogValve日志记录功能部分修改为以下内容：

```
<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="f
alse"/>
```

容器K8s配置方案

如果您的服务部署在K8s上，K8s会将真实的客户端IP记录在X-Original-Forwarded-For字段中，并将WAF回源地址记录在X-Forwarded-For字段中。您需要修改容器的配置文件，使Ingress将真实的IP添加到X-Forwarded-For字段中，以便您正常获取真实的客户端IP地址。

您可以参考以下步骤，对容器配置文件进行修改。

1. 执行以下命令修改配置文件`kube-system/nginx-configuration`。

```
kubectl -n kube-system edit cm nginx-configuration
```

2. 在配置文件中添加以下内容：

```
compute-full-forwarded-for: "true"
forwarded-for-header: "X-Forwarded-For"
use-forwarded-headers: "true"
```

3. 保存配置文件。
   保存后配置即刻生效，Ingress会将真实的客户端IP添加到X-Forwarded-For字段中。
4. 将业务程序获取客户端真实IP的字段修改为X-Original-Forwarded-For。

2.9. WAF接入配置最佳实践

将网站域名接入Web应用防火墙（Web Application Firewall，简称WAF），能够帮助您的网站防御OWASP TOP10常见Web攻击和恶意CC攻击流量，避免网站遭到入侵导致数据泄露，全面保障您网站的安全性和可用性。您可以参考本文中的接入配置和防护策略最佳实践，在各类场景中使用WAF更好地保护您的网站。

正常网站业务接入场景

业务梳理

建议您对所需接入WAF进行防护的业务情况进行全面梳理，帮助您了解当前业务状况和具体数据，为后续配置WAF的防护策略提供依据。

梳理项	说明
网站和业务信息	
网站/应用业务每天的流量峰值情况，包括Mbps、QPS	判断风险时间点，并且可作为WAF实例的业务带宽和业务QPS规格的选择依据。
业务的主要用户群体（例如，访问用户的主要来源地区）	判断非法攻击来源，后续可使用地域级IP黑名单屏蔽非法来源地区。
业务是否为C/S架构	如果是C/S架构，进一步明确是否有App客户端、Windows客户端、Linux客户端、代码回调或其他环境的客户端。
源站是否部署在非中国内地地域	判断所配置的实例是否符合最佳网络架构。
源站服务器的操作系统（Linux、Windows）和所使用的Web服务中间件（Apache、Nginx、IIS等）	判断源站是否存在访问控制策略，避免源站误拦截WAF回源IP转发的流量。
域名使用协议	判断所使用的通信协议WAF是否支持。
业务端口	判断源站业务端口是否在WAF支持的端口范围内。更多信息，请参见WAF支持的端口。
业务是否有获取并校验真实源IP机制	接入WAF后，真实源IP会发生变化。请确认是否要在源站上调整获取真实源IP配置，避免影响业务。
业务是否使用TLS 1.0或弱加密套件	判断业务使用的加密套件是否支持。
业务是否需要支持IPv6协议	WAF企业版和旗舰版实例已支持IPv6协议。
（针对HTTPS业务）业务是否使用双向认证	WAF虚拟独享集群目前已支持双向认证。如果您的HTTPS业务采用双向认证，请通过工单或WAF安全专家服务钉钉群联系阿里云技术支持人员。
（针对HTTPS业务）客户端是否支持SNI标准	对于支持HTTPS协议的域名，接入WAF后，客户端和服务端都需要支持SNI标准。
（针对HTTPS业务）是否存在会话保持机制	如果业务部署了阿里云负载均衡（SLB）实例，建议开启Cookie会话保持功能。
业务交互过程	了解业务交互过程、业务处理逻辑，便于后续配置针对性防护策略。

梳理项	说明
活跃用户数量	便于后续在处理紧急攻击事件时，判断事件严重程度，以采取风险较低的应急处理措施。
业务及攻击情况	
业务类型及业务特征（例如，游戏、棋牌、网站、App等业务）	便于在后续攻防过程中分析攻击特征。
业务流量（入方向）	帮助后续判断是否包含恶意流量。例如，日均访问流量为100 Mbps，则超过100 Mbps时可能遭受攻击。
业务流量（出方向）	帮助后续判断是否遭受攻击，并且作为是否需要额外业务带宽扩展的参考依据。
单用户、单IP的入方向流量范围和连接情况	帮助后续判断是否可针对单个IP制定限速策略。
用户群体属性	例如，个人用户、网吧用户或通过代理访问的用户。
业务是否遭受过大流量攻击及攻击类型	判断是否需要增加DDoS防护服务。
业务遭受过最大的攻击流量峰值	根据攻击流量峰值判断需要的DDoS防护规格。
业务是否遭受过CC攻击（HTTP Flood）	通过分析历史攻击特征，配置预防性策略。
业务遭受过最大的CC攻击峰值QPS	通过分析历史攻击特征，配置预防性策略。
业务是否提供Web API服务	如果提供Web API服务，不建议使用CC攻击紧急防护模式。通过分析API访问特征配置自定义CC攻击防护策略，避免API正常请求被拦截。
业务是否存在注册、登录、密码找回、短信接口被刷的情况	判断是否开启数据风控防护策略，并提前开启相关测试工作。
业务是否已完成压力测试	评估源站服务器的请求处理性能，帮助后续判断是否因遭受攻击导致业务发生异常。

准备工作

> **注意** 在将网站业务接入WAF时，强烈建议您先使用测试业务环境进行测试，测试通过后再正式接入生产业务环境。

在将网站业务接入WAF前，您需要完成以下准备工作：

- 所需接入的网站域名清单，包含网站的源站服务器IP、端口信息等。
- 所接入的网站域名必须已完成备案。更多信息，请参见阿里云备案。
- 如果您的网站支持HTTPS协议访问，您需要准备相应的证书和私钥信息，一般包含格式为CRT的公钥文件或格式为PEM的证书文件、格式为KEY的私钥文件。
- 具有网站DNS域名解析管理员的账号，用于修改DNS解析记录将网站流量切换至WAF。
- 推荐在将网站业务接入前，完成压力测试。
- 检查网站业务是否已有信任的访问客户端（例如，监控系统、通过内部固定IP或IP段调用的API接口、固定

的程序客户端请求等）。在将业务接入后，需要将这些信任的客户端IP加入白名单。

WAF配置

1. 域名接入配置。
   根据您的业务场景，参考以下接入配置指导，将您的网站域名接入WAF：
   - 单独使用WAF配置指导
   - 同时部署WAF和DDoS高防配置指导
   - 同时部署WAF和CDN配置指导

   > **说明** 如果在添加域名配置时，提示**您配置的域名已被其他用户使用**，建议您检查是否已在其他阿里云账号的WAF实例中添加与该域名冲突的配置记录。如果确实存在，您需要删除造成冲突的域名配置记录后再进行配置。

2. 源站保护配置：
   - 源站保护：为避免恶意攻击者绕过WAF直接攻击或入侵源站服务器，建议您完成源站保护配置。更多信息，请参见源站保护。
   - 标记WAF回源流量：将网站域名接入WAF进行防护后，您可以为网站域名设置流量标记（相关操作，请参见设置流量标记）。通过设置流量标记的方式，方便地标识经过WAF转发的流量，从而实现精准的源站保护（访问控制）、防护效果分析，有效防止流量绕过WAF请求源站。

   > **说明** 如果您接入WAF的网站域名的业务源站使用的是Windows IIS Web服务，在配置HTTPS域名时，IIS默认会启用**需要服务器名称指示**（即SNI）。这种情况下，在将域名接入WAF后可能会出现访问空白页502的错误信息，您只需禁用该配置选项即可解决该问题。

3. 防护策略配置。
   参考以下推荐防护配置对已接入的网站业务进行防护：
   - 规则防护引擎
     一般情况下，建议选用**拦截**模式，并选用**中等规则组**防护策略。

     > **说明** 业务接入WAF防护一段时间后（一般为2~3天），如果出现网站业务的正常请求被WAF误拦截的情况，您可以通过设置自定义规则组的方式提升Web防护效果。相关操作，请参见使用自定义规则组提升Web攻击防护效果。

   - CC安全防护
     业务正常运行时，建议采用系统默认配置。

> **说明** 由于CC防护的防护-紧急模式可能产生一定量的误拦截，如果您的业务为App业务或Web API服务，不建议您开启**防护-紧急**模式。如果使用CC安全防护的正常模式仍发现误拦截现象，建议您使用精准访问控制功能放行特定类型请求。

> **说明** 业务接入WAF防护一段时间后（一般为2-3天），可以通过分析业务日志数据（例如，访问URL、单个IP访问QPS情况等）评估单个IP的请求QPS峰值，提前通过自定义CC攻击防护配置限速策略，避免遭受攻击后的被动响应和临时策略配置。

当您的网站遭受大量CC攻击时，建议您开通日志服务功能。通过访问日志分析，发现恶意访问请求的特征，然后结合以下WAF的安全防护功能进行联合防御：

- 自定义CC攻击防护：针对URL设置灵活的限速策略，有效缓解CC攻击（HTTP Flood）带来的业务影响。

  > **说明** 自定义CC攻击防护的限速策略可能产生误拦截，建议您通过深度日志分析找出攻击特征，配置精准访问控制策略实现精准拦截。

- 自定义ACL访问控制：当攻击源IP比较分散时，可以通过分析访问日志，使用精准访问控制提供的丰富字段和逻辑条件组合，灵活配置访问控制策略实现精准防护，有效降低误拦截。
  - 支持IP、URL、Referer、User Agent、Params、Header等HTTP常见参数和字段的条件组合。
  - 支持包含、不包含、等于、不等于、前缀为、前缀不为等逻辑条件，设置阻断或放行策略。
- 地域级IP黑名单：针对全球来源IP地理位置进行自定义地域访问控制。您可以根据业务的用户分布情况，屏蔽不需要的访问来源地区。
- 数据风控：通过风险决策引擎和人机识别算法，有效识别和拦截欺诈行为。

  > **说明** 数据风控功能目前仅适用于网页/H5环境。

  一般来说，功能性页面遭恶意被刷的风险较低，可不配置数据风控策略。而对于注册、登录、密码找回、营销活动类等静态页面，建议您根据防护需求配置数据风控，有效识别和拦截欺诈行为。配置完成后，务必进行兼容性和业务可用性测试，避免数据风控策略配置对正常业务造成影响。

  > **说明** 部分页面前端代码与数据风控的JavaScript脚本可能存在兼容性问题。如果遇到此类问题，建议您使用指定页面插入JS功能，并在测试通过后开启防护，避免影响正常业务。如果您仍然无法解决，可以联系阿里云技术支持获得帮助。

- 日志功能
  根据您的业务和预算情况，选择启用日志服务功能。开通日志服务功能，可记录更多详细的原始日志信息，同时实现更灵活的访问日志自定义分析，发现恶意请求特征。更多信息，请参见概述。
- 监控告警

根据您的业务情况，为网站业务设置具体的QPS、4XX、5XX告警触发阈值。通过配置WAF告警监控功能，实时感知攻击事件。更多信息，请参见使用云监控设置WAF监控与告警。

4. 本地测试。
完成上述WAF配置后，建议您进行配置准确性检查和验证测试。

> **说明** 您可以通过修改本地系统Hosts文件方式进行测试。相关操作，请参见本地验证。

配置准确性检查项

编号	检查项	是否必检
1	接入配置域名是否填写正确	是
2	域名是否备案	是
3	接入配置协议是否与实际协议一致	是
4	接入配置端口是否与实际提供的服务端口一致	是
5	WAF前是否有配置其他七层代理（例如，DDoS高防、CDN等）	是
6	源站填写的IP是否是真实服务器IP，而不是错误地填写了高防IP或其他服务IP	是
7	回源算法是否与预期一致	否，建议检查
8	证书信息是否正确上传	是
9	证书是否合法（例如，加密算法不合规、错误上传其他域名的证书等）	是
10	证书链是否完整	是
11	是否配置流量标记	否，建议检查
12	告警监控配置	否，建议检查
13	是否已了解按量计费实例的计费方式 **说明** 仅适用于按量计费WAF实例。	是

业务可用性验证项

编号	检查项	是否必检
1	测试业务（包括Web、App客户端、Windows客户端、Linux客户端、其他环境的客户端）是否能够正常访问	是
2	测试业务登录会话保持功能是否正常	是

编号	检查项	是否必检
3	观察业务返回4XX和5XX响应码的次数，确保回源IP未被拦截	是
4	对于App业务，检查是否存在SNI问题	是
5	是否配置后端真实服务器获取真实源IP	否，建议检查
6	是否配置源站保护，防止攻击者绕过WAF直接入侵源站	否，建议检查

5. 正式切换业务流量。
   必要测试项均检测通过后，建议采用灰度的方式逐个域名修改DNS解析记录，将网站业务流量切换至Web应用防火墙，避免批量操作导致业务异常。修改DNS解析记录后，需要10分钟左右生效。如果切换流量过程中出现异常，请快速恢复DNS解析记录。

   > **说明** 如果您域名DNS解析存在MX记录与CNAME记录冲突的情况，建议您通过A记录方式接入WAF。或者，您可以通过创建二级域名的方式区分业务，实现使用CNAME方式接入。

   真实业务流量切换后，您需要再次根据上述业务可用性验证项进行测试，确保网站业务正常运行。
6. 日常运维。
   - 您可以参考以下最佳实践根据所需防护的具体场景，进一步配置具有针对性的防护策略：
     - 规则防护引擎最佳实践
     - CC攻击防护最佳实践
   - 如果您使用的是按量计费WAF实例，请仔细阅读WAF按量计费实例计费方式（具体内容，请参见按量计费2.0），避免出现实际产生的费用超出预算的情况。
   - 为避免WAF实例遭受大量DDoS攻击触发黑洞策略，导致网站业务无法访问的情况，建议您根据实际情况选择DDoS原生防护或DDoS高防产品，防御DDoS攻击。更多信息，请参见什么是DDoS原生防护、什么是DDoS高防（新BGP&国际）。
   - 如果出现业务访问延时或丢包的问题，参考以下建议变更部署方式：
     - 针对源站服务器在海外地区、WAF实例为中国内地地区、主要访问用户来自中国内地地区的情况，如果用户访问网站时存在延时高、丢包等现象，可能是由于回源网络链路问题，推荐您将源站服务器部署在中国内地地区。
     - 针对源站服务器在海外地区、WAF实例为海外地区、主要访问用户来自中国内地地区的情况，如果用户访问网站时存在延时高、丢包等现象，可能存在跨网络运营商导致的访问链路不稳定，推荐您使用中国内地地区的WAF实例。
   - 如果需要删除已防护的域名配置记录，确认网站业务是否已正式接入WAF。
     - 如果尚未正式切换业务流量，直接在Web应用防火墙管理控制台中删除域名配置记录即可。
     - 如果已完成业务流量切换，删除域名配置前务必前往域名DNS解析服务控制台，修改域名解析记录将业务流量切换回源站服务器。

> **说明**
> - 删除域名配置前，请务必确认域名的DNS解析已经切换至源站服务器。
> - 删除域名配置后，WAF将无法再为您的域名提供专业级安全防护。

业务遭受攻击时的紧急接入场景

如果您的网站业务已经遭受攻击，建议您在将业务接入WAF前执行以下操作：

- 遭受Web攻击入侵
  i. 为避免二次入侵，务必先清理入侵者植入的恶意文件并修复漏洞。

  > **说明** 如果您需要专业的安全运维人员帮助，请选购应急响应服务。

  ii. 已对业务系统进行安全加固。
  iii. 将网站业务接入WAF。

  > **说明** 根据实际情况将Web攻击防护策略调至高级规则，有效防御Web攻击行为导致的入侵事件。

- 遭受CC攻击或爬虫攻击
  在将网站业务接入WAF后，需要通过日志功能分析网站访问日志，判断攻击特征后进行针对性的防护策略配置。

安全专家服务

开通WAF后，您可以在管理控制台中通过钉钉扫描二维码直接联系阿里云安全服务专家。

安全专家将针对您的业务场景提供WAF接入配置指导、安全攻击分析和防御相关安全服务，基于业务实际情况帮助您更好地使用WAF对业务进行安全防护，保障您业务的网络应用安全。

> **说明** 为了便于快速分析和解决问题，在远程技术支持服务过程中，可能需要您授权阿里云安全专家查看业务数据。所有安全专家服务人员都将严格遵循服务授权和保密原则，防止您的信息泄露。

3.透明接入

Web应用防火墙（Web Application Firewall，简称WAF）提供CNAME接入和透明接入两种方式，使您的网站流量可以受到WAF的保护。如果您的源站服务器为ECS服务器或者部署在阿里云公网SLB、ALB上，那么除了使用CNAME接入，您还可以选择云原生的透明接入方式。

在透明接入模式下，WAF无需修改域名DNS解析、设置源站保护，无需改变服务器获取真实源IP，保护您的Web业务正常运转。

透明接入支持接入ALB实例、CLB实例上的Web流量。

前提条件

条件类型	描述	补充说明
WAF实例版本	已开通WAF包年包月服务的高级版、企业版、旗舰版，或者WAF按量计费服务。	详细版本介绍，请参见套餐和版本说明。
WAF实例地域	已开通中国内地地域的WAF实例。	目前，仅中国内地的WAF实例支持透明接入，海外地区的WAF实例暂不支持透明接入。
云服务实例的类型	已创建IPv4公网SLB实例。	透明接入不支持私网SLB和IPv6版本的公网SLB实例。
SLB配置	需要透明接入的SLB实例拥有公网IP，且端口未开启双向认证。	如果您使用了私网SLB+EIP，也支持使用透明接入。
域名备案	需要防护的网站域名如果托管在中国内地（大陆）的服务器上，该域名需要完成ICP备案。	无

条件类型	描述	补充说明
（可选）证书状态	**注意** 如果您要接入七层SLB实例上的Web流量，必须满足该前提条件。接入四层SLB实例或ECS源站上Web流量时，无需满足该前提条件。 由于透明接入WAF的证书同步机制的限制，要求您在七层SLB实例端口中配置的证书必须从**阿里云签发证书**列表中选择。因此，执行透明接入前，您必须对透明接入配置端口上使用的证书，完成以下操作： 1. 必须先将该证书上传到数字证书管理服务控制台进行统一管理，或直接从数字证书管理服务控制台购买和申请证书。 2. 证书上传到数字证书管理服务控制台或在数字证书管理服务控制台完成证书申请后，您需要在负载均衡SLB控制台为该透明接入配置的端口配置监听时，选择该证书并完成配置。 **说明** 以上操作顺序不可颠倒，否则会导致您无法在WAF控制台透明接入模块的**七层SLB类型**列表中看到该端口。	如果您先在SLB中完成证书配置，而没有先在数字证书管理服务控制台上传证书或申请证书，SLB无法将该证书自动同步到WAF中，您将无法在WAF控制台透明接入模块的**七层SLB类型**列表中看到该端口，最终导致您无法完成网站接入。相关内容，请参见上传证书。 下图展示了在负载均衡SLB控制台为该端口配置监听时，如何正确选择该证书： 

功能优势

透明接入模式具有以下优势：

- 无需修改DNS解析，无需设置源站保护，防护更简单、安全。
- 全透明代理防护，无需回源配置，源站即可直接获取访问者的真实IP。
- 联动阿里云数字证书管理服务对证书（支持非阿里云证书）进行统一管理，运维更便捷。
- 支持任意非标业务端口接入WAF防护。

使用限制

限制项类型	描述
SLB和ECS地域	您的公网SLB实例和ECS实例地域必须位于西南1（成都）、华北2（北京）、华北3（张家口）、华东1（杭州）、华东2（上海）、华南1（深圳）。 由于历史网络架构的原因，部分公网SLB不支持透明接入。 具体开通咨询，请使用钉钉加入阿里云WAF云原生接入咨询群聊（群号：32208925），联系我们。

限制项类型	描述
引流端口配置的数量	不同版本的WAF实例支持添加的引流端口配置的数量如下： • 高级版：不超过20条。 • 企业版：不超过50条。 • 旗舰版：不超过100条。 • 按量计费版本：不超过20条。 透明接入对指定源站服务器的具体端口生效，即您可以针对某个源站服务器（具有公网IP）的具体端口（例如80、443等）开启透明接入。开启透明接入后，该服务器端口的流量被引流到WAF进行防护。 例如，假设您同时为SLB实例A的80、443端口，以及另一个SLB实例B的80、443端口开启透明接入，则您一共添加了4个引流端口配置（SLB实例A的80端口、SLB实例A的443端口、SLB实例B的80端口、SLB实例B的443端口）。
业务同时接入DDoS高防和WAF	如果您的业务需要同时接入DDoS高防和WAF，则只有在业务通过域名接入方式（即七层接入模式）接入DDoS高防时，该业务才支持通过透明接入方式接入WAF。 如果业务通过端口接入方式（即四层接入模式）接入DDoS高防，则该业务暂不支持通过透明接入方式接入WAF。针对这种情况，推荐您使用CNAME接入方式，将该业务接入WAF进行防护。更多信息，请参见网站接入（CNAME接入）。

步骤一：添加域名

警告 域名首次透明接入WAF时，可能会导致Web业务出现秒级闪断。您可以在**总览**页面，查看到当前业务QPS有明显下降。

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**资产中心 > 网站接入**。
3. （可选）在顶部菜单栏左上角，选择**中国内地**地域。

   目前，仅中国内地WAF实例支持透明接入。如果WAF控制台已默认展示中国内地地域，则无需切换地域。
4. 在**域名列表**页签，单击**网站接入**。
5. 在**添加域名**页面，选择**接入模式**为**透明接入**。

6. （可选）完成云资源访问授权。

   首次执行透明接入时，您需要按照页面提示授权WAF访问相关的云服务；如果您已经完成过授权，则不会出现相关提示，请跳过该步骤。更多信息，请参见授权WAF访问云资源。
7. 在**添加域名信息**模块，完成域名和源站服务端口等配置。

i. 在**域名**文本框，输入您的网站域名（也支持填写源站服务器IP地址）。

> **注意** 透明接入模式下，此处设置的域名仅用于（完成网站接入后）在域名维度设置网站防护策略、查看防护总览及安全报表。此处设置的域名与实际接入WAF防护的业务流量无必然联系，只有在下一步端口配置中开启端口，才表示将对应源站服务端口的流量接入WAF防护。

域名必须已经完成备案，且不允许重复添加域名。支持的域名类型包括：

- **通配符域名**（例如，`*.example.com`）。使用通配符域名后，WAF将自动匹配该通配符域名对应的所有子域名。
- **精确域名**（例如，`www.example.com`）。如果同时存在通配符域名和精确域名配置，则精确域名的转发规则和防护策略优先生效。

ii. 设置要开启透明接入（即需要将其流量引流到WAF进行防护）的源站服务端口。

目前支持对阿里云ALB实例、SLB实例（七层监听）、SLB实例（四层监听）、ECS实例类型的源站服务端口开启透明接入。不同类型的源站服务端口开启透明接入的设置方法有差异，具体请单击以下页签，查看相关说明。如果您需要了解更详细的说明，请参见引流端口配置。

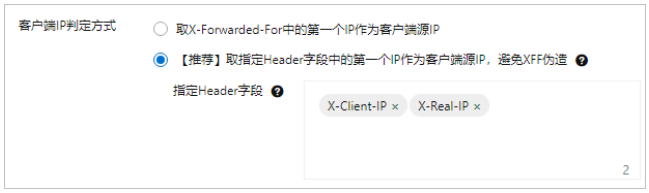
ALB类型 | 七层SLB类型 | 四层SLB类型 | ECS类型

推荐场景：您部署了应用型负载均衡（ALB）实例作为Web服务的入口，需要为ALB实例监听端口上的流量开启WAF防护。
实例列表说明：实例列表展示了负载均衡服务中已创建的公网ALB实例，**端口号**列展示了ALB实例下已创建的HTTP或HTTPS监听对应的监听端口。
为监听端口开启WAF防护的方法：
在负载均衡控制台，为ALB实例创建HTTP或HTTPS监听，并在监听配置中选中**为监听开启WAF安全防护**。如果您已经创建过HTTP或HTTPS监听，可以通过修改监听配置，为监听开启或关闭WAF安全防护。
在WAF控制台透明接入模块的ALB类型实例列表中，您只可以查看已创建的HTTP或HTTPS监听是否开启了WAF防护，不支持修改。如需修改，必须在负载均衡控制台操作。

iii. 选择**WAF前是否有七层代理（高防/CDN等）**：

- **否**：表示WAF收到的业务请求来自发起请求的客户端。WAF直接取与WAF建立连接的IP（来自`REMOTE_ADDR`字段）作为客户端IP。

- **是**：表示WAF收到的业务请求来自其他七层代理服务转发，而非直接来自发起请求的客户端。为了保证WAF可以获取真实的客户端IP进行安全分析，您需要进一步设置**客户端IP判定方式**。
  WAF默认读取请求Header字段 `X-Forwarded-For` （XFF）中的第一个IP地址作为客户端IP。



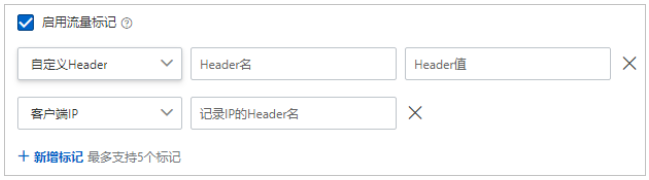
如果您的网站业务已通过其他代理服务的设置，规定将客户端源IP放置在某个自定义的Header字段（例如，X-Client-IP、X-Real-IP），则您需要选择**取指定Header字段中的第一个IP作为客户端源IP，避免XFF伪造**，并在**指定Header字段**框中输入对应的Header字段。

> **说明** 推荐您在业务中使用自定义Header存放客户端IP，并在WAF中配置对应Header字段。该方式可以避免攻击者伪造XFF字段，躲避WAF的检测规则，提高业务的安全性。

支持输入多个Header字段。每输入完一个Header字段，需要按半角逗号（,）确认。设置了多个Header时，WAF将按顺序尝试读取客户端IP。如果第一个Header不存在，则读取第二个，以此类推。如果所有指定Header都不存在，则读取XFF中第一个IP地址作为客户端IP。

iv. （可选）设置是否启用WAF流量标记功能。

流量标记表示WAF在转发客户端请求到源站服务器时，在请求头中添加或修改由您指定的自定义字段，用于标记该请求经过WAF转发、记录该请求的客户端IP。
选中**启用流量标记**后，您需要设置标记字段。



标记字段分为以下类型：

- **自定义Header**：需要设置**Header名**和**Header值**，使WAF在回源请求中添加该Header信息，标记请求经过WAF（区分没有经过WAF的请求，便于您的后端服务统计分析）。
  例如，您可以使用 `ALIWAF-TAG: Yes` 标记经过WAF的请求，其中， `ALIWAF-TAG` 为Header名， `Yes` 为Header值。

> **注意** 请不要填写标准的HTTP头部字段（例如User-Agent等），否则会导致标准头部字段内容被自定义的字段值覆盖。

- **客户端IP**：设置**记录IP的Header名**，使WAF在回源请求中，将该Header的值修改为客户端IP。
  关于WAF判定客户端IP的具体规则，请参见**WAF前是否有七层代理（高防/CDN等）**参数的描述。
  如果您的后端服务需要从指定的自定义Header（例如，example-client-ip）中获取客户端IP进行业务分析，则您可以将该Header设置为**记录IP的Header名**。

> **注意** 请不要填写标准的HTTP头部字段（例如User-Agent等），否则会导致标准头部字段内容被自定义的字段值覆盖。

v. 从**资源组**列表中选择域名所属的资源组。

> **说明** 您可以使用资源管理服务创建资源组，根据业务部门、项目等维度对云资源进行分组管理。更多信息，请参见创建资源组。

vi. 单击**下一步**。

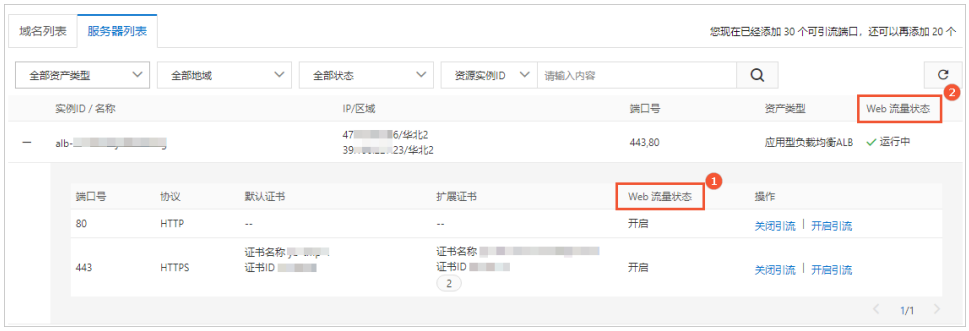
8. 在**检查并确认**模块，检查已配置的透明接入信息，并单击**下一步**。
9. 在**添加完成**模块，单击**完成，返回网站列表**。
   域名添加完成后，您可以在**域名列表**中查看已添加域名及源站信息，并可以根据需要编辑、删除域名配置。

WAF默认对您在**添加域名信息**中开启的源站服务端口上的流量进行检测，并将处理后的正常请求返回到源站服务器。您可以根据业务实际需要，在**服务器列表**页签，修改源站服务端口的流量防护状态。相关操作，请参见步骤二：查看服务器列表信息。

步骤二：查看服务器列表信息

完成域名添加后，您可以查看源站服务器的详细防护信息，以及在需要紧急容灾的情况下强制关闭引流或删除引流端口。

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**资产中心 > 网站接入**。
3. 在顶部菜单栏左上角，选择**中国内地**地域。
   目前，仅中国内地WAF实例支持透明接入。如果WAF控制台已默认展示中国内地地域，则无需切换地域。
4. 在**网站接入**页面，单击**服务器列表**页签。
5. 在**服务器列表**页签，查看已接入WAF防护的源站服务器资产（包含ALB实例、SLB实例、ECS实例）。
   您可以单击实例前的 ＋ 图标，展开查看该实例下已添加到WAF防护的端口。



Web流量状态说明：

- 端口号后的**Web流量状态**（图示①）表示该端口的流量目前是否经过WAF防护。取值说明：
  - **开启**：表示已开启防护。
  - **关闭**：表示未开启防护。

  您可以根据需要修改端口的防护状态，相关操作，请参见下一步。

- 实例后的**Web流量状态**（图示②）表示该实例下端口接入WAF防护的整体状态。取值说明：
  - **未防护**：表示该实例下端口都已关闭防护。
  - **部分防护**：表示该实例下有部分端口已开启防护。
  - **运行中**：表示该实例下端口都已开启防护。

6. （可选）修改端口引流状态及删除端口。
   - **关闭引流**、**开启引流**（适用于所有类型的服务器资产）
     - 对于已开启WAF防护的端口，如果您暂时不需要WAF对端口流量进行防护，可以单击端口**操作**列下的**关闭引流**，并在**提示**对话框中单击**确定**。
       关闭端口引流后，该服务器端口的流量将不会经过WAF防护。
     - 对于已关闭WAF防护的端口，如果您需要WAF重新对端口流量进行防护，可以单击端口**操作**列下的**开启引流**，并在**提示**对话框中单击**确定**。
   - **删除**（仅适用于四层SLB类型、ECS类型的服务器资产）
     如果您不再需要WAF对某个端口的流量进行防护，可以单击端口**操作**列下的**删除**，并在**提示**对话框中单击**确定**。
     后续如果您需要重新为该端口开启WAF防护，必须重新添加端口。

后续步骤

完成接入流程后，网站访问流量将经过WAF并受到WAF的防护。WAF包含多种防护检测模块，帮助网站防御不同类型的安全威胁，其中**规则防护引擎**和**CC安全防护**模块默认开启，分别用于防御常见的Web应用攻击（例如SQL注入、XSS跨站、webshell上传等）和CC攻击，其他防护模块需要您手动开启并配置具体防护规则。更多信息，请参见网站防护配置概述。

相关文档

CNAME接入

上传已有证书到数字证书管理服务控制台

4.透明接入常见问题

同一个域名是否支持使用透明接入和CNAME接入两种模式？

不支持。

每个域名只能使用透明接入或CNAME接入两种方式之一。如果您已通过CNAME接入开启WAF防护的域名，需要切换为透明接入，您必须先删除该域名的CNAME接入配置，然后在透明接入模式下重新接入该域名。

> **警告** 域名首次透明接入WAF时，可能会导致该域名指向的网站Web业务出现秒级闪断。

已透明接入的域名如果无需WAF转发流量和提供防护，该如何处理？

如果您确认该域名无需WAF继续提供防护，您可以在WAF控制台**资产中心 > 网站接入**页面的**服务器列表**中，定位该域名所在的源站IP，为对应端口关闭引流（具体操作，请参见修改端口引流状态）。操作完成后，该域名的访问流量将切回到域名所在的源站服务器，不再通过WAF转发。

透明接入后，源站可以获取客户端的真实IP吗？

可以。WAF会向域名所在的服务器直接提供真实的客户端IP，而不再将WAF的回源IP地址返回给源站服务器。

端口绑定的证书更新后，是否需要将证书重新上传到WAF透明接入模块中？

不同类型的源站实例所需操作不同，具体说明如下：

- 源站实例为**ALB类型**、**七层SLB类型**：不需要在WAF透明接入模块重新上传证书。您只需在负载均衡实例中更新证书，WAF透明接入模块会自动同步最新的证书。
- 源站实例为**四层SLB类型**、**ECS类型**：需要在WAF透明接入模块重新上传证书。

同一个域名如果配置到了多个SLB实例上，我需要如何完成透明接入？

这种情况下，您需要在对该域名进行透明接入配置时，同时添加这几个SLB实例的HTTP/HTTPS服务端口，实现WAF对这几个实例同时引流。

如果配置透明接入时，您仅添加了其中一个SLB实例的HTTP/HTTPS服务端口，WAF将仅转发来自该端口的访问流量并对其进行防护。来自其他SLB实例的流量将不会通过WAF转发和受到WAF的防护。

一个SLB实例配置了多个域名，如果我只对其中一个域名完成了透明接入，会有什么影响？

这种情况下，该SLB实例上其他域名也受到WAF默认防护策略（包括规则防护引擎、CC安全防护）的防护。WAF如果检测到这些域名有攻击流量，也会对攻击流量进行拦截。

> **注意** 透明接入模式下，接入WAF防护的流量只与服务器（ECS、SLB、ALB实例）的引流端口配置有关。如果您的SLB实例上配置了多个域名，且这些域名都是通过同一个端口（假设为HTTPS 443端口）提供服务，则您为其中一个域名开启透明接入时，需要将SLB实例的443端口配置为引流端口，该操作会使443端口上所有流量（包含其他域名的流量）都接入到WAF进行防护。更多信息，请参见步骤一：添加域名。

透明接入时为什么看不到我需要接入的七层SLB实例？

透明接入存在一定的限制条件。具体内容，请参见透明接入。

使用透明接入模式将SLB接入到WAF时，如果您在Web应用防火墙控制台**添加域名**页面的**七层SLB类型**列表中，无法看到您需要接入的SLB公网实例或者无法成功接入WAF，可能原因有以下几点：

原因	说明	解决方法
公网SLB实例所在的地域不在透明接入支持的范围内。	目前，仅支持位于华北2（北京）、华北3（张家口）、华东1（杭州）、华东2（上海）、华南1（深圳）或西南1（成都）地域的公网SLB实例使用透明接入模式。	使用位于华北2（北京）、华北3（张家口）、华东1（杭州）、华东2（上海）、华南1（深圳）或西南1（成都）地域的公网SLB实例接入WAF。
公网SLB实例绑定的公网IP是IPv6版本。	透明接入不支持IPv6版本的公网SLB实例。	使用IPv4版本的公网SLB实例接入WAF。
公网SLB实例中未配置监听协议。	未添加监听端口的SLB实例将无法使用透明接入。	在SLB实例控制台为SLB实例添加监听端口。
原有的公网SLB实例位于历史网络架构中的经典网络。	目前，仅支持已完成公网上移网络改造的SLB接入WAF。如果您的SLB满足其他条件但未出现透明接入列表中，可能是由于您当前的SLB未完成公网上移改造。	使用私网SLB+EIP的网络结构的SLB实例或新购公网SLB实例（新购买的公网SLB实例不存在历史网络架构中的问题）接入WAF。
透明接入时，需要配置的公网SLB实例（七层）端口使用的证书未上传到阿里云数字证书管理服务控制台进行统一管理。	公网SLB实例（七层）接入WAF时，需要配置的端口如果为HTTPS协议，但是该端口使用的证书未上传到阿里云SSL证书服务中，会导致SLB无法将该证书自动同步到WAF中，您将无法完成网站接入。	将该公网SLB实例（七层）HTTPS端口使用的证书上传到数字证书管理服务控制台。
透明接入时，需要配置的公网SLB实例端口开启了双向认证。	如果当前HTTPS协议在公网SLB中采用了双向认证，则暂时不支持透明接入。	需要在SLB控制台取消双向认证选项后，重新在Web应用防火墙控制台执行透明接入。
需要执行透明接入的公网SLB是新购的SLB实例。	新购买的SLB实例存在有一定的数据延迟，您可能在**透明接入**页面暂时无法看到新购买的SLB实例。	完成SLB购买后，建议您等待1~3分钟，再刷新Web应用防火墙控制台后执行透明接入。
透明接入时，需要配置的公网SLB实例端口不在当前WAF版本支持的范围内。	WAF包年包月服务的高级版、企业版、旗舰版支持透明接入模式。如果需要配置的公网SLB实例端口不在当前WAF版本支持的范围内，您在Web应用防火墙控制台**添加域名**页面的**七层SLB类型**列表中，添加该端口时将无法保存，从而导致无法将该公网SLB实例成功接入WAF。	使用当前WAF版本支持的端口。 **说明** 透明接入模式下，不同版本支持接入的端口不同。旗舰版支持任意非标端口接入；关于其他版本支持的端口范围，可以在**七层SLB类型**右上角单击**查看可选范围**获取。

我使用的是私网SLB+EIP，是否支持透明接入？

支持。

5.云产品接入WAF

5.1. 同时部署WAF和CDN

Web应用防火墙（WAF）可以与CDN（如网宿、加速乐、七牛、又拍、阿里云CDN等）结合使用，为开启内容加速的域名提供Web攻击防御。

背景信息

您可以参照以下架构为源站同时部署WAF和CDN：CDN（入口层，内容加速）> Web应用防火墙（中间层，实现应用层防护）> 源站。

使用阿里云CDN

1. 参见CDN快速入门，将要防护的域名（即加速域名）接入CDN。
2. 在Web应用防火墙中创建网站配置。
   - **域名**：填写要防护的域名。
   - **服务器地址**：填写SLB公网IP、ECS公网IP，或云外机房服务器的IP。
   - **WAF前是否有七层代理（高防/CDN等）**：勾选是。

   具体操作请参见网站配置。

3. 成功创建网站配置后，Web应用防火墙为该域名生成一个专用的CNAME地址。

> **说明** 关于如何查看WAF生成的CNAME地址，请参见WAF接入指南。

4. 将CDN配置中的源站修改为Web应用防火墙分配的CNAME地址。
   i. 登录阿里云CDN控制台。
   ii. 在**域名管理**页面，选择要操作的域名，单击**管理**。
   iii. 在**源站信息**区域，单击已有源站信息后面的**编辑**，修改已有源站配置。

参数	说明

参数	说明
源站信息	选择源站的类型，并填写源站地址。 ■ **地址长度**：最长不超过67个字符。 ■ **源站数量**：每个加速域名的源站数量最多可以设置20个。 ■ **OSS域名** ■ 资源已存储在阿里云OSS中，可直接输入阿里云OSS Bucket的外网域名作为源站（不支持OSS内网域名作为源站），例如：`***.oss-cn-hangzhou.aliyundoc.com`。 ■ 查看OSS外网域名：前往OSS控制台查看，或直接选择同账号下的OSS Bucket。 ■ **IP**：支持配置多个服务器外网IP作为源站地址，不支持内网IP，阿里云ECS的外网IP可免审核。 ■ **源站域名**：支持配置域名作为源站地址，可配置多个域名。 说明 ■ 源站域名不能与加速域名相同，否则会造成循环解析，无法回源。 ■ 域名仅支持全英文小写。 ■ 如果域名包含中文（例如：阿里云.网址），请以中文形式进行相关备案，再通过第三方工具punnycode将中文域名转换成为英文域名（例如：xn--fiq****.xn--eq****）后填入。 ■ **函数计算域名**：支持将您在同一账号下的函数计算产品上配置的函数计算域名，配置为源站地址。您需要选择函数计算**区域**和**域名**。操作方法，请参见配置自定义域名。
优先级	支持设置主备，主优先级大于备优先级。用户请求通过阿里云CDN回源时，会优先回源到优先级为主的源站地址。 例如，有A、B两个源站，A源站的优先级为主，B源站的优先级为备，则用户请求通过阿里云CDN回源时会优先回源到A源站，如果A源站出现故障，将会回源到B源站，当A源站恢复正常后会从B源站切换回A源站。
权重	当多个源站的优先级相同时，阿里云CDN会按照源站的权重分配用户请求回源到不同源站的比例，实现按权重的负载均衡。您可以根据业务需求，自行设置权限值。 ■ 取值范围：1~100，数值越大，源站分配到的用户请求比例越高。 ■ 默认值：10。 示例：有A、B两个源站，两个源站的优先级都是主，A源站的权重为80，B源站的权重为20，则用户请求将会按照8:2的比例在A、B两个源站之间分配。

参数	说明
端口	即，CDN节点回到源站哪个端口请求资源。默认为80，根据您源站的支持情况，可自定义设置回源端口，允许设置的端口范围为1~65535。 ■ 默认值：80。 ■ 端口值为443时，以HTTPS协议回源；80或其他自定义端口，以HTTP协议回源。 说明 ■ 如果需要以HTTPS协议回源到其他自定义端口，请提交工单申请。 ■ 如果配置了**回源协议**功能（默认为关闭状态），这里配置的端口会失效。关闭回源协议的方法，请参见配置回源协议。 ■ 当源站选择OSS域名时，回源端口是否支持自定义端口，取决于OSS产品。

iv. 前往**回源配置**页面，在**配置**页签下，确认**回源HOST**未开启。

完成上述配置后，流量经过CDN，其中动态内容将继续通过Web应用防火墙进行安全检测防护。

使用非阿里云CDN

1. 配置CDN，将域名接入CDN。
2. 在Web应用防火墙中创建网站配置。具体请参见使用阿里云CDN步骤2。
3. 查看WAF CNAME地址。具体请参见使用阿里云CDN步骤3。
4. 将CDN配置的源站改为WAF CNAME地址。

5.2. 通过联合部署DDoS高防和WAF提升网站防护能力

如果您的网络遭受的攻击既有流量型攻击，又混杂精巧的Web应用层攻击时，单一使用一种网络安全防护产品无法起到全面的防护效果，我们推荐您组合使用阿里云DDoS高防和Web应用防火墙（Web Application Firewall，简称 WAF）。本文介绍了为业务同时部署DDoS高防和WAF时的配置指导。

前提条件

- 已开通DDoS高防（新BGP）或者DDoS高防（国际）实例。更多信息，请参见购买DDoS高防实例。
- 已开通WAF实例。更多信息，请参见开通Web应用防火墙。

背景信息

DDoS高防和WAF同时部署时采用以下网络架构：DDoS高防（入口层，防御DDoS攻击）->WAF（中间层，防御Web应用攻击）->源站服务器（ECS、SLB、VPC、IDC等）。网站业务流量会先经过DDoS高防清洗，然后转发到WAF过滤Web攻击，最后只有正常的业务流量被转发到源站服务器，保障网站的业务安全和数据安全。业务流量的转发过程如下图所示。

说明 应用上述网络架构后，访问请求将经过多层中间代理才到达源站，源站不能直接获取请求的真实来源IP。如果您需要获取访问请求的真实来源IP，请参见配置DDoS高防后获取真实的请求来源IP。

步骤一：网站业务接入WAF

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 在**域名列表**页签，单击**网站接入**。
5. 添加域名。
   - 接入模式：CNAME接入。

     说明 进入**添加域名**页面后，**接入模式**默认为**Cname接入**。CNAME接入场景下，您无需再修改**接入模式**。

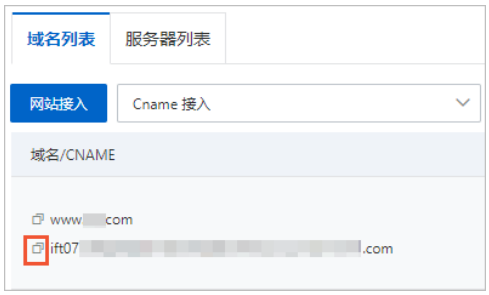
     a. 单击**手动接入**页签，在**填写网站信息**模块按以下要求配置参数。

     说明 CAME接入支持一键接入和手动接入两种方式，DDoS高防和WAF同时部署的场景下，推荐使用手动接入。

     - **域名**：填写要防护的网站域名。
     - **防护资源**：按实际情况选择要使用的防护资源类型。
     - **协议类型**：按实际情况选择网站支持的协议类型。
     - **服务器地址**：选择IP并填写源站服务器对应的SLB公网IP、ECS公网IP或云外机房服务器的IP。
     - **服务器端口**：根据已选择的**协议类型**，按实际情况设置源站提供对应服务的端口。
     - **负载均衡算法**：当设置了多个源站服务器地址时，按实际情况选择多源站服务器间的负载均衡算法。
     - **WAF前是否有七层代理（高防/CDN等）**：选择**是**。
     - **启用流量标记**：按实际情况设置是否启用WAF流量标记功能。
     - **资源组**：当需要根据业务部门、项目等维度对云资源进行分组管理时，从资源组列表中选择该域名所属资源组。

     b. 单击**下一步**。

c. 返回**域名列表**，找到新添加的域名，在**域名/CNAME**列复制WAF为该域名分配的**CNAME**地址。



- 接入模式：透明接入。
  a. 在**添加域名**页面，选择**接入模式**为**透明接入**。
  b. 在**添加域名信息**模块按以下要求配置参数。
     - **域名**：填写要防护的网站域名。
     - **ALB类型**、**七层SLB类型**、**四层SLB类型**、**ECS类型**：在标签页中选择待防护实例所属类型，勾选待防护实例对应的端口。
     - **WAF前是否有七层代理（高防/CDN等）**：选择**是**。
     - **启用流量标记**：按实际情况设置是否启用WAF流量标记功能。
     - **资源组**：当需要根据业务部门、项目等维度对云资源进行分组管理时，从资源组列表中选择该域名所属资源组。
  c. 单击**下一步**。
  d. 检查并确认配置后，单击**下一步**。
  e. 单击**完成**，返回网站列表。

步骤二：网站业务接入DDoS高防

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

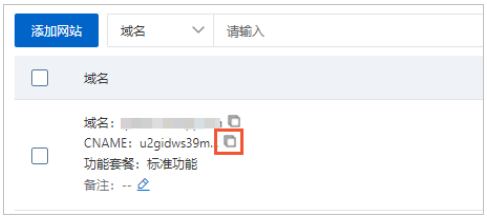
     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，单击**添加网站**。
5. 按照页面提示，完成**添加网站**配置向导。

i. 在**填写网站信息**模块按以下要求配置参数。

- **功能套餐**：按实际情况选择要关联的DDoS高防实例的功能套餐。
- **实例**：按实际情况选择要关联的DDoS高防实例。
- **网站**：填写要防护的网站域名。
- **协议类型**：按实际情况选择网站支持的协议类型。
- **启用OCSP**：按实际情况选择是否启用OCSP（Online Certificate Status Protocol）功能。
- **服务器地址**：
  - 域名在WAF上的接入模式为CNAME接入时，选择**源站域名**并填写步骤一中获取的WAF的CNAME地址。
  - 域名在WAF上的接入模式为透明接入时，选择**源站IP**并填写源站服务器的公网IP。
- **服务器端口**：根据已选择的**协议类型**，设置源站提供对应服务的端口。

ii. 单击**添加**。

iii. 返回**域名接入**页面，找到新添加的域名，在**域名**列复制DDoS高防为该域名分配的**CNAME**地址。



步骤三：修改域名的DNS解析

如果您的域名DNS托管在阿里云云解析DNS，请按照以下操作，将域名解析指向步骤二获取的DDoS高防**CNAME**地址。如果您使用其他DNS服务商的域名解析服务，请登录服务商系统修改网站域名的解析记录，下文内容仅供参考。

1. 登录阿里云云解析DNS控制台。
2. 在**域名解析**页面，找到要操作的域名，在**操作**列下单击**解析设置**。
3. 在**解析设置**页面，找到要修改的解析记录，在**操作**列下单击**修改**。

> **说明** 如果要操作的解析记录不在记录列表中，您可以单击**添加记录**。

4. 在**修改记录**（或**添加记录**）页面，选择**记录类型**为**CNAME**，并将**记录值**修改为域名对应的DDoS高防CNAME地址（即步骤二中获取到的DDoS高防**CNAME**地址）。
5. 单击**确认**，等待修改后的解析设置生效。
6. 使用浏览器测试网站访问是否正常。

   如果网站访问出现异常，请参见业务接入高防后存在卡顿、延迟、访问不通等问题。

相关文档

- 添加域名：介绍了开通WAF后，如何通过CNAME接入方式将您要防护的域名接入WAF进行防护。
- 透明接入：介绍了开通WAF后，如何通过透明接入方式将您要防护的域名接入WAF进行防护。
- 添加网站：介绍了开通DDoS高防后，添加网站配置和批量导入网站配置的操作步骤。
- 修改DNS解析接入网站业务：介绍了手动修改域名解析以接入DDoS高防的操作方法。

6.WAF支持的端口

WAF既可以防护标准端口（包括80和8080、443和8443），也可以防护由WAF指定的非标准端口。您可以在网站接入配置中自定义网站服务器端口，WAF将通过您设置的服务器端口为网站提供流量的接入与转发服务。

背景信息

完成网站接入后，WAF只通过已设置的服务器端口向源站服务器转发业务流量。对于未设置的端口，WAF不会转发任何该端口的访问请求流量到源站服务器。

注意事项

WAF防护的端口包含标准端口和非标准端口，不同的版本支持的端口数量和非标准端口范围有所不同。具体差异，请参见各版本支持的端口。请您仔细阅读以下注意事项：

- 每个WAF实例的端口限制数包含了防护的标准端口和非标准端口总和。
- 除了透明接入模式下和独享版以外，其他情况下，WAF支持的非标端口并不是指您业务中任何一个自定义的非标端口，而必须是由WAF指定的非标端口。

如何在控制台查看可选的端口范围

您可以通过控制台查询可选端口范围。操作步骤如下：

1. 打开控制台**资产中心 > 网站接入**页面。
2. 定位到需要设置端口的域名，并单击操作列的**编辑**。
3. 在**编辑**页面，定位到**服务器端口**模块，单击**自定义**，添加需要配置的端口。

详细操作，请参见设置端口。

各版本支持的端口

- 透明接入模式
  透明接入模式下，WAF实例支持防护0~65535范围内的任意非标端口。

  > **说明** 透明接入模式下，WAF实例支持添加的端口引流配置的数量有限制。相关信息，请参见使用限制。

- CNAME接入模式
  CNAME接入模式下，只有**企业版以上**包年包月WAF实例和按量计费WAF实例（必须已开启**支持非标端口**配置）支持配置非标端口。
  下表展示了CNAME接入模式下WAF各版本支持的端口信息。实际支持的端口以控制台提供的端口（在控制台查看可选端口范围）为准。

WAF版本	每个WAF实例防护的端口限制数	默认支持的标准端口	可选的非标端口范围
高级版	4个	◦ HTTP：80、8080 ◦ HTTPS：443、8443	不支持

WAF版本	每个WAF实例防护的端口限制数	默认支持的标准端口	可选的非标端口范围
企业版	10个（包含标准端口和非标端口的总和）	○ HTTP：80、8080 ○ HTTPS：443、8443	○ HTTP协议端口： 81、82、83、84、85、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800 **注意** 仅中国内地地域的WAF实例支持48800端口，海外地区WAF实例暂不支持48800端口。 ○ HTTPS协议端口： 4443、5443、6443、7443、8553、8663、9443、9553、9663、18980 **注意** 仅中国内地地域的WAF实例支持18980端口，海外地区WAF实例暂不支持18980端口。

WAF版本	每个WAF实例防护的端口限制数	默认支持的标准端口	可选的非标端口范围
旗舰版	50个（包含标准端口和非标端口的总和）	◦ HTTP：80、8080 ◦ HTTPS：443、8443	◦ HTTP协议端口： 81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800 **注意** 仅中国内地地域的WAF实例支持48800端口，海外地区WAF实例暂不支持48800端口。 ◦ HTTPS协议端口： 4443、5443、6443、7443、8553、8663、9443、9553、9663、18980 **注意** 仅中国内地地域的WAF实例支持18980端口，海外地区WAF实例暂不支持18980端口。
独享版	50个（包含标准端口和非标端口的总和）	◦ HTTP：80、8080 ◦ HTTPS：443、8443	除了不支持特定的系统端口（例如，22、53、4431、4646、4985、4986、4987、6060、8301、8600、9100、15001、56688）以外，独享版WAF支持0~65535范围内其他任意的非标端口。
按量计费	10个（包含标准端口和非标端口的总和）	◦ HTTP：80、8080 ◦ HTTPS：443、8443	您必须已开启按量计费WAF的**支持非标端口**配置，才能使用WAF指定的非标端口。 开启方法：打开WAF控制台**系统管理 > 账单与套餐中心**页面，通过**修改套餐**，开启**接入调度**下**支持非标端口**。 具体支持的端口号与本表格中**旗舰版**一致。

说明 独享版WAF实例支持除以上端口外更多的非标端口业务，且支持基于HTTP、HTTPS和HTTP 2.0协议的自定义回源端口配置。更多信息，请参见设置独享集群。

其他相关问题

已接入网站的未配置端口是否会对源站带来安全风险？

WAF是否支持自定义端口？

非标端口业务无法接入Web应用防火墙高级版