阿里云
Web应用防火墙

网站接入

文档版本：20200330

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. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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:** 重置操作将丢失用户配置数据。
	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。
	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。
	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。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	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 资产管理

Web应用防火墙提供资产管理功能，通过获取阿里云平台上的SSL证书、云解析DNS、Web应用防火墙等云产品的配置信息和站点通信流量中的网站信息，主动发现您云平台上的网络资产，同时提供一键接入防护功能帮助您的企业实现全面的网络资产管理和安全防护。

背景信息

网络应用资产是安全管理体系中最基础最重要的载体，同时也是业务系统中最基本的组成单元。随着企业业务的高速发展，各类业务系统平台逐年增多，同时也存在着员工私建站点、测试环境未及时回收等情况，可能产生大量“僵尸”资产。信息安全是很典型的木桶效应，安全防护的水位由企业最薄弱的一环决定。由于无人管理，“僵尸”资产往往使用了低版本的开源系统、组件、Web框架等，导致一些薄弱环节暴露在攻击者的视野下，攻击者可以利用这些站点作为“跳板”绕过企业的网络边界防护，进而使得整个企业内网沦陷。

Web应用防火墙（WAF）的资产管理功能旨在协助您发现阿里云上的应用资产、监控资产变化，避免在安全防护中出现资产遗漏， 提高整体安全防护水位线。资产管理为您提供云上资产识别、一键自动接入防护、0day漏洞影响范围评估等功能，为企业网络域名资产的安全管理决策提供事实依据以及将网络资产快速接入安全防护的能力，全面保障企业云上网络资产的安全。

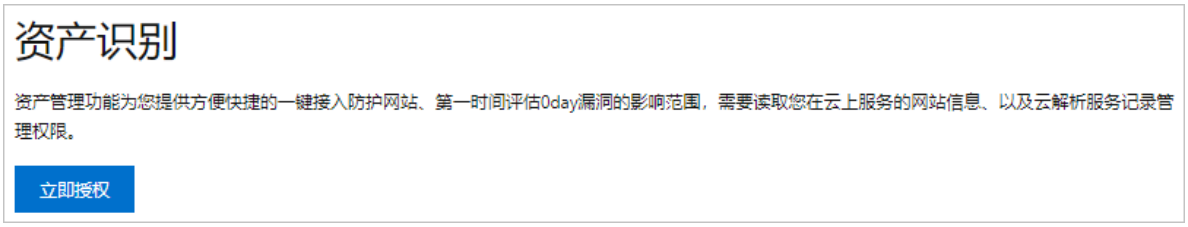
在得到您的授权后，WAF将基于所获取的您阿里云账号中的SSL证书、云解析DNS、Web应用防火墙等云产品的配置信息和阿里云上站点通信流量中的网站（Host）信息，综合发现您在阿里云平台中的所有域名资产信息，包括域名和子域名信息、服务器IP地址、端口、协议、Web防护状态等。

授权WAF访问云资源

为实现网络资产的主动发现，您需要授予WAF读取您云账号中相关云服务的网站信息和管理云解析服务的域名解析记录的权限。

1. 登录云盾Web应用防火墙控制台。
2. 在左侧导航栏，单击管理 > 资产管理。

   若您首次访问资产管理页面，您将收到云资源访问授权提示。



3. 单击授权，前往访问控制平台授权页面。

4. 单击同意授权，授权WAF访问您账号中相关云产品服务的资源。

   授权完成后，WAF将主动发现您云账号中的网络域名资产。

查看域名资产

您可以在WAF控制台的资产管理页面，查看WAF主动发现的您账号中的所有域名资产。

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择WAF实例所在地区（中国大陆、海外地区）。
3. 定位到资产管理页面，查看您的域名资产。

   WAF根据一级域名将所发现的域名资产进行聚合展示，您可以展开指定一级域名查看所发现的具体的域名资产信息，包括服务器地址、端口号、访问协议、防护状态等信息。

   说明:

   - 资产管理页面仅展示近期有流量的云上域名资产。
   - 如果域名资产的服务器地址、端口号、协议等信息未显示，表示该IP资产不属于当前的阿里云账号。

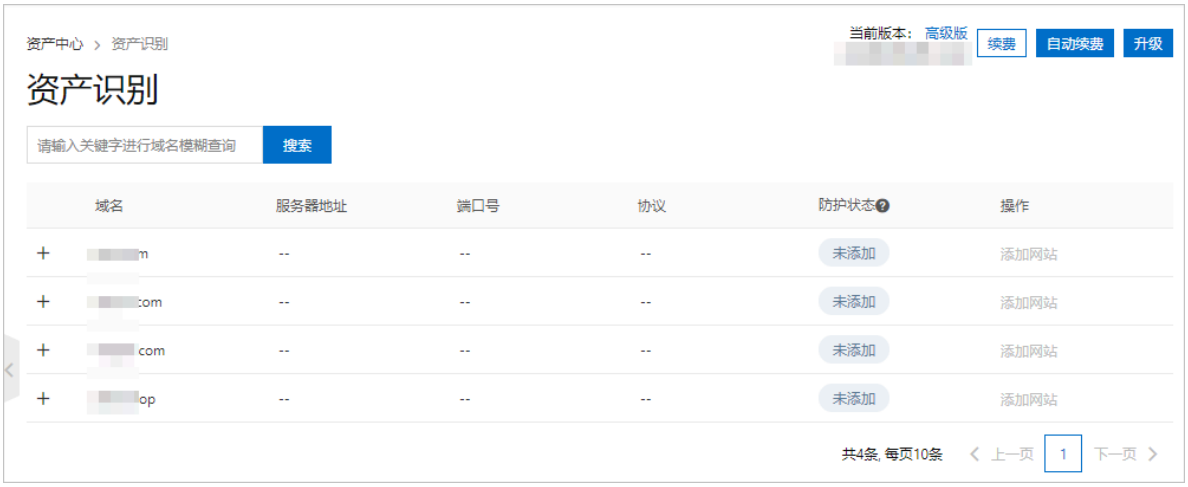
   其中，防护状态表示是否已接入WAF进行全面防护：

   - 未添加：网站资产未接入WAF防护
   - 已添加未接入：已在WAF中添加网站资产接入配置，但WAF未检测到网站流量
   - 防护中：网站资产已接入WAF防护，检测到网站流量，提供全面防护

   说明:

对于尚未接入WAF的域名资产（防护状态为未添加），建议您通过自动添加网站配置一键接入WAF进行防护，实现域名资产的全面防护。

您也可以在域名资产列表上方的搜索框中输入任意关键字，单击搜索查找指定域名资产。



查看资产详情

您可以在资产管理页面，单击资产详情查看已接入WAF防护域名资产的站点树详细信息。

说明:

对于WAF高级版，您必须升级到企业版或旗舰版，才能使用域名资产站点树功能。具体操作请参见*#unique_5*。

URL资产作为网站域名资产的详细信息，WAF根据全量日志功能采集的域名访问流量大小和流量特征对已接入防护的域名进行URL站点树分析，识别URL类型进行分类。同时，站点树使用大数据泛化聚合算法（归一化算法）对URL和参数进行聚合展示。例如，系统会将以下新闻站点的具体URL聚合为`/{字符+数字}.html`的URL形式：

- **/news1234.html**
- **/oldnews1223.html**
- **/news1224.html**
- **/news124.html**

1. **登录云盾*Web*应用防火墙控制台。**
2. **在页面上方选择WAF实例所在地区（中国大陆、海外地区）。**
3. **定位到资产管理页面，选择域名资产，单击资产详情。**

4. 在站点树区域，您可以查看该域名资产聚合后的URL、参数名、参数值类型和近一天内URL的请求次数。

> **说明:**
> 为了避免展示的URL数量过多，站点树中的URL仅展示到路径级别。默认展示最多三级并按照URL的请求次数排序，优先展示重要的资产。

- 您可以通过选择URL查询或扩展名并输入关键字，搜索特定的URL情况。
- 在URL列中，对于带有文件夹图标的URL，您可以单击URL进行展开或折叠展示URL信息。
- 在参数名|值类型列中，您可以查看URL涉及的参数名和参数值类型。

> **说明:**
> 与URL相同，所展示的参数信息也经过大数据归一化算法进行泛化聚合。默认展示三个聚合后的参数名和对应的值类型，您可以将鼠标移至其右下角的更多图标查看所有参数。

2 使用透明代理模式接入WAF

WAF透明代理模式向您提供一种简便的接入阿里云Web应用防火墙（WAF）的方法。本文介绍了使用透明代理模式接入WAF的具体操作。

前提条件

只有满足以下条件才能使用WAF透明代理模式：

- 您的WAF实例为包年包月模式。
- 源站服务器部署在阿里云ECS，且ECS实例所在地域为华北2（北京）。
- 源站ECS实例拥有公网IP或已绑定弹性公网IP（EIP）。

> **说明:**
> WAF透明代理接入模式暂不支持通过负载均衡SLB的公网IP牵引源站ECS实例的流量。

背景信息

您可以使用透明代理模式或DNS配置模式将网站接入WAF进行防护。

> **注意:**
> 透明代理模式和DNS配置模式只能选择一种，即如果要使用透明代理模式，必须先清空DNS配置模式下的域名配置记录，反之亦然。

- 透明代理模式：将所配置的源站服务器公网IP的80端口接收到的HTTP协议的流量直接牵引到WAF，经WAF处理后再将正常的访问流量回注给源站服务器。

  该方式需要您授权WAF读取您的ECS实例信息。配置过程中只用在WAF控制台添加域名和勾选相应的服务器IP。具体操作见本文操作步骤。
- DNS配置模式：通过修改域名解析的方式，将被防护域名的访问流量指向WAF；WAF根据域名配置的源站服务器地址，将处理后的请求转发回源站服务器。

  该方式需要您在WAF控制台添加一个网站配置并更新域名的DNS设置。具体操作请参见网站配置、业务接入*WAF*配置。

透明代理模式优势

- 自动支持基于目标ECS、EIP（源站服务器）的全流量防护，避免因未配置源站保护而导致的潜在安全风险。
- 自动透明的流量迁移，无需修改域名DNS记录，避免对业务造成影响。

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. 选择透明代理模式。

4. （可选） 单击立即授权。

> **说明:**
> 首次使用透明代理时，您需要授权阿里云Web应用防火墙访问您的ECS实例信息。若已完成过授权，请直接执行步骤6。

5. （可选） 在云资源访问授权页面，单击同意授权。

完成授权后直接跳转到添加域名页面，请直接执行步骤7。

6. （可选） 单击添加域名。
7. 在添加域名页面，输入要防护的域名，并从左侧WAF读取到的当前云账号中符合前提条件的ECS服务器IP中，选择域名对应的源站IP地址。

> **说明:**

选择服务器IP表示允许将该IP的80端口接收到的HTTP协议访问流量牵引至WAF进行分析、处理；WAF将根据为该域名所配置的防护策略检测访问请求，并将处理后的请求回注到源站服务器。

8. 确认其他配置，并单击确认，完成域名添加。

添加域名后自动触发流量牵引，您可以在服务器IP管理中查看已配置IP的牵引状态。

流量牵引状态包括：

- 已牵引：表示该服务器IP 80端口接收到的所有HTTP协议流量都将自动牵引至WAF进行监控。

- 牵引中：表示正在牵引流量。
- 牵引失败：表示流量牵引失败。
- 删除中：表示正在移除该IP。

对于不再需要流量牵引的服务器IP，您可以在服务器IP管理中删除对应记录。

说明:

在删除网站配置时，对应的服务器IP流量牵引不会随之删除，您需要在服务器IP管理中执行删除操作。

后续步骤

使用透明代理模式成功接入WAF后，请参见*WAF*防护配置，为域名配置防护策略。

3 使用DNS配置模式接入WAF

3.1 网站配置

网站配置指在Web应用防火墙（WAF）控制台上配置启用WAF防护的网站的转发信息。本文介绍了通过DNS配置模式接入WAF时，如何添加和管理网站配置。

背景信息

> **说明:**
> 如果您通过包年包月方式开通WAF，且您的源站服务器部署在阿里云ECS（华北2地域），同时ECS实例拥有公网IP或已绑定弹性公网IP（EIP），则您可以使用透明代理模式接入WAF。
>
> - 透明代理模式：将所配置的源站服务器公网IP的80端口接收到的HTTP协议的流量直接牵引到WAF，经WAF处理后再将正常的访问流量回注给源站服务器。
>
> 该方式需要您授权WAF读取您的ECS实例信息。配置过程中只用在WAF控制台添加域名和勾选相应的服务器IP。具体操作请参见使用透明代理模式接入*WAF*。
> - DNS配置模式：通过修改域名解析的方式，将被防护域名的访问流量指向WAF；WAF根据域名配置的源站服务器地址，将处理后的请求转发回源站服务器。
>
> 该方式需要您在WAF控制台添加网站配置并更新域名的DNS设置。

使用DNS配置模式接入WAF时，您可以选择自动添加网站配置或手动添加网站配置。

- 自动添加网站配置。添加网站配置时，WAF可以自动读取阿里云云解析*DNS*控制台中的解析A记录，获取网站域名和源站服务器IP地址，帮助您自动添加网站配置。自动添加网站配置后，WAF将尝试自动更新域名的解析记录，完成网站接入。

  > **说明:**
  > 自动添加网站配置默认使用共享集群共享IP防护资源。如果您的网站配置需要使用独享集群或独享IP防护资源，请在自动添加网站配置后，在网站配置页面修改防护资源。
- 手动添加网站配置。如果域名的DNS解析没有托管在阿里云云解析DNS上，您只能手动添加网站配置，并在域名的DNS服务商处手动修改DNS解析，将网站收到的Web请求转发至WAF进行监控，完成网站接入。

  关于手动修改DNS解析的方法，请参见业务接入*WAF*配置。

> **说明:**

允许添加的网站配置数量由WAF实例规格和扩展域名包数量决定，具体请参见扩展域名包。

如果网站配置中的源站服务器地址、服务协议、端口等信息发生变化，或者您需要调整HTTPS高级设置功能，您可以编辑网站配置。

对于不再需要WAF防护的域名，您可以在恢复其DNS解析后，删除网站配置。

自动添加网站配置

前提条件

- 要防护的网站的DNS解析托管在阿里云云解析DNS，且其解析记录中存在至少一条生效的A记录。

  推荐您使用阿里云云解析DNS，相关操作请参见设置域名解析。

  如果您暂时无法使用阿里云云解析DNS，建议您参见网站配置，手动添加网站配置。
- （仅针对中国大陆地域）网站已经通过中华人民共和国工业和信息化部ICP备案。

  推荐您使用阿里云备案服务，相关操作请参见备案导航。

  注意：
  如果您添加的网站域名尚未通过工信部域名备案，请务必尽快完成备案。WAF将不定期自动释放未通过备案的域名配置记录。
- （仅针对支持HTTPS协议的网站）获取网站的HTTPS证书和私钥文件，或者已将证书托管在阿里云证书服务。

  推荐您使用阿里云SSL证书服务对云上证书进行统一管理，相关操作请参见证书服务快速入门。

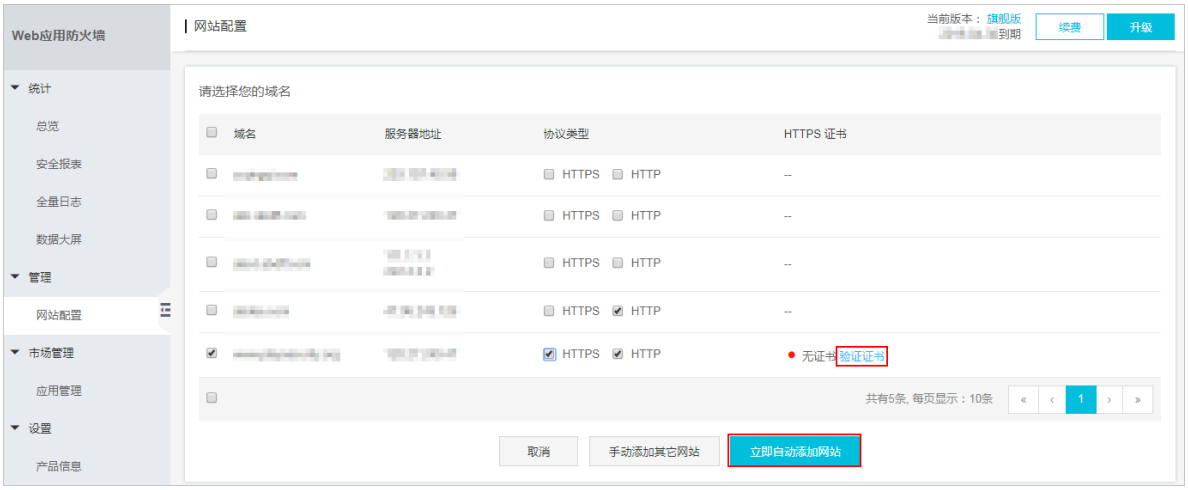
操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，选择DNS配置模式。

4. 单击添加网站。

   WAF自动罗列出当前阿里云账号在云解析DNS中已添加过解析A记录的域名。如果云解析DNS中无任何解析A记录，则不会出现请选择您的域名页面，建议您参见网站配置，手动添加网站配置。

   > **说明:**
   > 如果您添加的网站域名尚未通过工信部域名备案，请务必尽快完成备案。WAF将不定期自动释放未通过备案的域名配置记录。



5. 在请选择您的域名页面勾选要防护的域名及协议类型。

6. （可选）如果协议类型包括HTTPS，您必须先完成证书验证，才能添加网站。

   > **说明:**
   > 您也可以先不勾选HTTPS，在完成网站配置后，参见更新HTTPS证书上传证书。

   a) 单击验证证书。

   b) 在验证证书对话框中上传证书和私钥文件。

   - 如果您已将网站的证书托管在阿里云证书服务控制台，则可以在验证证书对话框中单击选择已有证书，并选择一个与要防护的域名绑定的证书。
   - 手动上传证书。单击手动上传，填写证书名称，并将该域名所绑定的证书文件和私钥文件中的文本内容分别复制粘贴到证书文件和私钥文件文本框中。

     更多信息，请参见更新HTTPS证书。

   c) 单击验证，完成证书验证。

7. 单击立即自动添加网站。

   自动添加网站后，WAF将自动为您更新该域名的DNS CNAME解析记录，将网站Web请求转发到WAF进行监控。一键添加及解析的过程一般需要10-15分钟。

   > 说明:
   > 如果您收到提示，需要手动更新DNS解析记录，请参见步骤2：修改DNS解析完成WAF接入。

8. 在管理 > 网站配置页面查看新添加的域名及其DNS解析状态。

   - DNS解析状态正常表示该网站已正常接入WAF。您可以参见步骤3：配置WAF防护策略，完成后续任务。
   - 刚添加完网站配置后，该域名的DNS解析状态也可能显示为异常。建议您稍等一会儿再来查看，或者在DNS供应商处检查域名的DNS设置。

     如果DNS设置不正确，请参见步骤2：修改DNS解析。关于DNS解析状态的判断标准，请参见DNS解析状态说明。

手动添加网站配置

前提条件

- 获取要防护的网站的域名。
- 获取网站的源站服务器地址。
- 确认网站是否已接入或需要接入CDN、高防IP等其它代理型系统。
- （仅针对中国大陆地域）网站已经通过中华人民共和国工业和信息化部ICP备案。

  推荐您使用阿里云备案服务，相关操作请参见备案导航。
- （仅针对网站支持HTTPS协议）获取网站的HTTPS证书和私钥文件，或者已将证书托管在阿里云证书服务。

  推荐您使用阿里云SSL证书服务对云上证书进行统一管理，相关操作请参见证书服务快速入门。

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，并在页面上方选择地域：中国大陆、海外地区。
3. （可选） 选择DNS配置模式。
4. 单击添加网站。

   WAF自动罗列出当前阿里云账号在云解析DNS中已添加过解析A记录的域名。如果云解析DNS中无任何解析A记录，则请选择您的域名页面不会出现。
5. （可选） 在请选择您的域名页面，单击手动添加其它网站。
6. 在填写网站信息任务中，完成以下配置。

配置项	配置说明
域名	填写要防护的域名。 说明: · 支持填写泛域名，如`*.aliyun.com`。WAF将自动匹配该泛域名对应的子域名。 · 如果同时存在泛域名和精确域名配置（如`*.aliyun.com`和`www.aliyun.com`），WAF优先使用精确域名所配置的转发规则和防护策略。 · 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	默认使用公共集群防护资源。如果您的WAF实例已升级至独享版，可选择将域名接入独享集群进行防护，支持定制化业务需求。关于独享集群的详细信息，请参见*#unique_20*。
协议类型	勾选网站支持的协议类型，可选值：HTTP、HTTPS、HTTP2.0。 说明: · 如果网站支持HTTPS加密认证，请勾选HTTPS，并在添加网站后参见**更新*HTTPS*证书**上传证书和私钥文件。 · 勾选HTTPS后，可使用高级设置实现HTTP强制跳转和HTTP回源等功能，保证访问平滑。更多信息，请参见*HTTPS*高级配置。 · 使用HTTP2.0协议，需要符合以下要求： - 您的WAF实例已升级至企业版或旗舰版。 - 您已勾选HTTPS协议。

配置项	配置说明
服务器地址	填写网站的源站服务器地址，支持IP地址和其它地址格式。网站接入WAF后，WAF将过滤后的访问请求转发至该地址。 · （推荐）勾选IP，并填写源站服务器的公网IP地址（如云服务器ECS实例的IP、负载均衡SLB实例的IP等）。 说明: - 多个地址间以逗号分隔。最多支持添加20个源站IP。 - 如果配置多个IP地址，WAF将在这些地址间自动进行健康检查和负载均衡。更多信息，请参见源站负载均衡。 · 勾选其它地址，填写服务器回源域名（如对象存储OSS的CNAME等）。 说明: - 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，在WAF控制台中完成域名接入配置后，需要在OSS控制台中为该OSS域名绑定自定义域名，具体操作请参见管理域名。
服务器端口	配置网站的协议端口。WAF通过所配置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所配置的服务端口进行转发；对于未配置的端口，WAF不会转发任何该端口的访问请求流量到源站服务器，因此这些端口的启用和漏洞不会对源站服务器造成任何安全威胁。 注意: 配置的协议和端口必须与您所接入的网站业务源站IP（在WAF中配置的服务器IP地址）的协议和端口（在WAF中配置的服务器端口）一致，不支持端口转换功能。 · 勾选HTTP协议后，默认HTTP端口为80。 · 参见勾选HTTPS协议后，默认HTTPS端口为443。 · 如果要使用其它端口，单击自定义进行添加。 说明: - 公共集群支持的详细端口列表，请参见非标端口支持。 - 如果您选择独享集群，则自定义端口仅可选择独享集群设置页面中设定的服务器端口范围。 · HTTP2.0协议的端口与HTTPS端口保持一致。
WAF前是否有七层代理（高防/CDN等）	根据该网站业务的实际情况勾选。如果在WAF前需要配置其它七层代理进行转发，请务必勾选是，否则WAF将无法获取访问该网站的客户端真实IP。

配置项	配置说明
负载均衡算法	如果配置了多个源站IP，勾选IP hash或轮询。WAF将根据所选择的方式在多个源站IP间分发访问请求，实现负载均衡。
流量标记	填写一个空闲的Header字段名称和自定义Header字段值，用来标识经过WAF转发到源站的Web请求。流量经过WAF后，WAF在请求中添加此处指定的字段，方便您的后端服务统计信息。 **说明:** 如果Web请求中本身包含此处定义的头部字段，WAF将用此处的设定值覆盖原Web请求中对应字段的内容。

7. 完成配置后，单击下一步，成功添加网站配置。

   成功添加网站配置后，您可以选择执行以下任务：

   - 根据页面提示，完成修改DNS解析任务。具体操作请参见业务接入WAF配置。
   - （已勾选HTTPS协议）上传网站HTTPS证书和私钥。具体操作请参见更新HTTPS证书。
   - 回到管理 > 网站配置页面，查看新添加的网站配置，根据需要进行编辑或删除。

   > **注意：**
   > 如果您添加的网站域名尚未通过工信部域名备案，请务必尽快完成备案。WAF将不定期自动释放未通过备案的域名配置记录。

编辑网站配置

已添加的网站配置若发生变化，例如源站服务器地址、协议类型（高级HTTPS功能）、监听端口等变化，您可以编辑网站配置。

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，在DNS配置模式下，选择要操作的网站配置，单击其操作列下的编辑。
4. 在编辑页面，参见手动添加网站步骤6，修改相应配置。

   > **说明：**
   > 域名不支持调整。若要防护其他域名，建议您新增一个网站配置，并删除不需要的网站配置。

5. 单击确定，成功编辑网站配置。

删除网站配置

若网站不再需要WAF防护，您可以先恢复其DNS解析（即将DNS指回服务器源站IP），然后删除网站配置。

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，在DNS配置模式下，选择要删除的网站配置，单击其操作列下的删除。

   > **说明：**
   > 确认删除前，请先恢复网站DNS解析；否则在删除配置后，该域名的流量将无法正常转发。

4. 在提示信息对话框中，单击确定，成功删除网站配置。

跨账号网站配置迁移说明

为了防止网站配置迁移误操作导致业务流量转发出现问题，在您删除网站配置后，有一段时间的域名保护期。如果您需要将WAF的网站配置迁移到另一个账号下，在原账号中删除网站配置后，您需要等待30分钟后才能在另一个账号的WAF实例中添加该域名的网站配置。

如果您需要快速添加该网站配置，请提交工单或在钉钉服务群中申请解除该域名的保护期。待保护期解除后，您就可以在新的账号中添加该域名的网站配置。

3.2 业务接入WAF配置

本文介绍通过DNS配置模式接入WAF时，如何在已添加网站配置后，配置域名解析，实现业务接入。

背景信息

说明:

如果您通过包年包月方式开通WAF，且您的源站服务器部署在阿里云ECS（华北2地域），同时ECS实例拥有公网IP或已绑定弹性公网IP（EIP），则您可以使用透明代理模式接入WAF。

- 透明代理模式：将所配置的源站服务器公网IP的80端口接收到的HTTP协议的流量直接牵引到WAF，经WAF处理后再将正常的访问流量回注给源站服务器。

  该方式需要您授权WAF读取您的ECS实例信息。配置过程中只用在WAF控制台添加域名和勾选相应的服务器IP。具体操作请参见使用透明代理模式接入WAF。
- DNS配置模式：通过修改域名解析的方式，将被防护域名的访问流量指向WAF；WAF根据域名配置的源站服务器地址，将处理后的请求转发回源站服务器。

  该方式需要您在WAF控制台添加网站配置并更新域名的DNS设置。

通过DNS配置模式接入WAF时，您需要先添加网站配置；成功添加网站配置后，您可以选择通过（推荐）CNAME接入和A记录接入的方式更新域名DNS解析，将网站访问流量转发到WAF进行监控。

说明:

推荐您采用CNAME接入。在某些极端情况下（如节点故障、机房故障等），通过CNAME解析方式接入WAF，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。

下文内容适用于为网站单独开启WAF防护，即该网站不接入CDN、DDoS高防等其它代理型服务。如果您需要将WAF与其它代理型服务结合部署，请参见以下文档：

- 同时部署WAF和CDN：介绍同时为网站部署CDN和Web应用防火墙的配置方法。
- 同时部署WAF和DDoS高防：介绍同时为网站部署DDoS高防和Web应用防火墙的配置方法。

（推荐）CNAME接入

前提条件

- 已添加网站配置。具体请参见网站配置。
- 获取WAF CNAME地址。
  1. 登录云盾Web应用防火墙控制台。
  2. 在页面上方选择地域：中国大陆、海外地区。
  3. 前往管理 > 网站配置页面，在DNS配置模式下，选择已添加的网站配置，将鼠标放置在域名上，即可出现复制CName按钮。

  4. 单击复制CName，将该CNAME复制到剪贴板中。
- 具有在域名的DNS服务商处更新DNS记录的权限。
- （可选）放行WAF回源段IP。源站服务器上已启用非阿里云安全软件（如安全狗、云锁）时，您需要在这些软件上设置放行WAF回源段IP，防止由WAF转发到源站的正常业务流量被拦截。具体请参见放行WAF回源段IP。
- （可选）进行本地验证。通过本地验证确保WAF转发规则配置正常后，再修改网站域名的DNS解析记录，防止因配置错误导致业务中断。具体请参见本地验证。

操作步骤

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

下文也提供了花生壳配置示例，介绍在花生壳修改域名解析的方法。

1. 登录云解析DNS控制台。
2. 选择要操作的域名，单击其操作列下的解析设置。

3. 选择要操作的主机记录，单击其操作列下的修改。

   关于域名的主机记录，以域名`abc.com`为例：

   - www：用于精确匹配www开头的域名，如`www.abc.com`。
   - @：用于匹配根域名`abc.com`。
   - *：用于匹配泛域名，包括根域名和所有子域名，如`blog.abc.com`、`www.abc.com`、`abc.com`等。

4. 在修改记录对话框中，完成以下操作：

   - 记录类型：修改为CNAME。
   - 记录值：修改为已复制的WAF CNAME地址。
   - 其他设置保持不变。TTL值一般建议设置为10分钟。TTL值越大，则DNS记录的同步和更新越慢。

   关于修改解析记录：

   - 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。

     > **说明:**
     > 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。

     关于DNS解析记录互斥的详细说明，请参见解析记录冲突的规则。
   - 如果必须保留MX记录（邮件服务器记录），您可以参见业务接入WAF配置，使用A记录解析的方式将域名解析到WAF IP。

5. 单击确定，完成DNS配置，等待DNS解析记录生效。
6. 验证DNS配置。您可以Ping网站域名或使用17ce等工具验证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分钟后重新检查。

7. 查看DNS解析状态。

a) 登录云盾Web应用防火墙控制台。

b) 前往管理 > 网站配置页面，在DNS配置模式下，查看域名的DNS解析状态。

- 正常：表示网站已成功接入WAF，网站访问流量由WAF监控。
- 异常：如果DNS解析状态为异常，且收到未检测到CNAME接入、无流量、检测失败等提示，说明网站未正确接入WAF。

  如果您确认已将网站域名解析到WAF CNAME地址，可在一小时后再次查看DNS解析状态或者参见DNS解析状态异常排查异常原因。

> **说明:**
> 该提示仅说明网站是否正确接入WAF，不代表您的网站访问异常。

花生壳配置示例

如果您的域名DNS托管在花生壳，您可以参照下图修改DNS解析设置。

启用源站保护

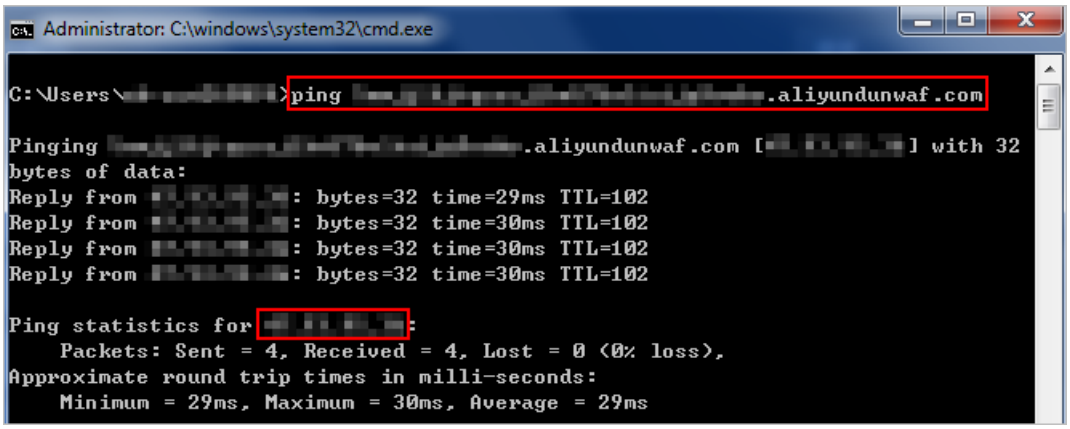
启用源站保护可以防止攻击者在获取源站服务器的真实IP后，绕过WAF直接攻击您的源站。建议您通过配置源站ECS的安全组或源站SLB的白名单，防止恶意攻击者直接攻击您的源站。具体请参见源站保护配置。

A记录接入

A记录接入和CNAME接入的流程大体相同，区别在于以下两点：

- 前提条件：获取WAF CNAME后，执行以下步骤，获取WAF IP地址。

  1. 在Windows操作系统中，打开cmd命令行工具。
  2. 执行以下命令：`ping "已复制的WAF Cname地址"`。



  3. 在返回结果中，记录WAF IP地址。

- 操作步骤：在步骤4修改记录时，执行以下操作，修改记录类型和记录值。
  - 记录类型：修改为A。
  - 记录值：修改为已获得的WAF IP地址。
  - 其他设置保持不变。

3.3 放行WAF回源IP段

网站成功接入WAF后，所有网站访问请求将先流转到WAF进行监控，经WAF实例过滤后再返回到源站服务器。流量经WAF实例返回源站的过程称为回源。

WAF实例的IP数量有限，且源站服务器收到的所有请求都来自这些IP。在源站服务器上的安全软件（如安全狗、云锁）看来，这种行为很可疑，有可能触发屏蔽WAF回源IP的操作。因此，在接入WAF防护后，您需要在源站服务器的安全软件上设置放行所有WAF回源IP。

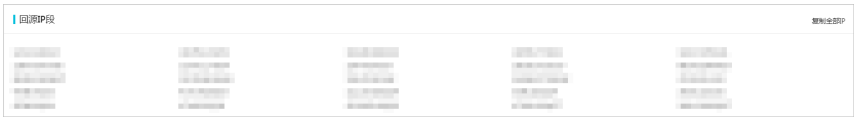
> **说明:**
> 强烈推荐您在接入WAF防护后，卸载源站服务器上的其他安全软件。

操作步骤

WAF控制台提供了最新的回源IP段列表，您可以参照以下步骤进行操作：

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方，选择地域：中国大陆、海外地区。
3. 前往设置 > 产品信息页面。

4. 在产品信息页面底部，查看和复制所有WAF回源IP段。

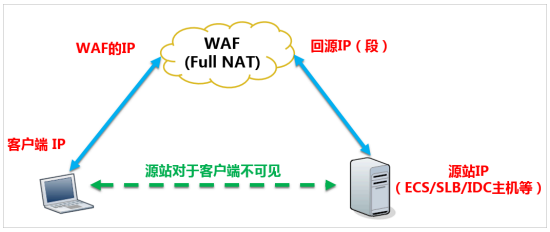


5. 打开源站服务器上的安全软件，将复制的IP段添加到白名单。

常见问题

什么是回源IP?

回源IP是WAF用来代理客户端请求服务器时用的源IP，在服务器看来，接入WAF后所有源IP都会变成WAF的回源IP，而真实的客户端地址会被加在HTTP头部的XFF字段中。



为何要放行回源IP段?

由于来源的IP变得更加集中，频率会变得更快，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，从而将其拉黑。一旦拉黑，WAF的请求将无法得到源站的正常响应。因此，在接入WAF后，您应确保源站已将WAF的全部回源IP放行（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。

建议在部署WAF后，您在源站上只允许来自WAF的访问请求，这样既可保证访问不受影响，又能防止源站IP暴露后被黑客直接攻击。更多信息，请参考源站保护。

3.4 本地验证

在把业务流量切到WAF之前，建议您先通过本地验证确保一切配置正常，WAF转发正常。本地验证需要在本地模拟接入WAF，然后访问被防护网站，验证WAF正常转发。

本地接入WAF

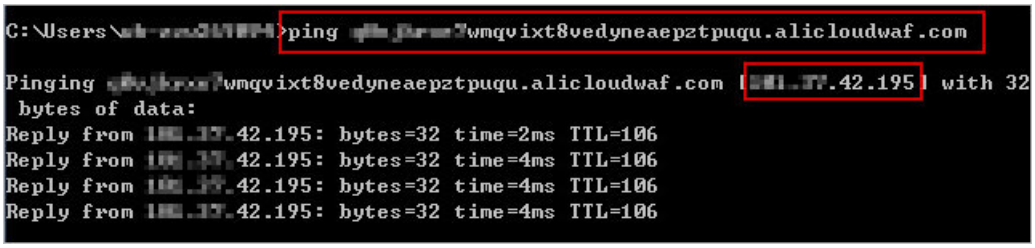
通过修改本地*hosts*文件（什么是*hosts*文件）模拟接入WAF，将从本地访问被防护站点的请求导向WAF。以Windows操作系统为例，

1. 用记事本或notepad++等文本编辑器打开*hosts*文件，*hosts*文件一般位于*C:\Windows\System32\drivers\etc\hosts*路径。

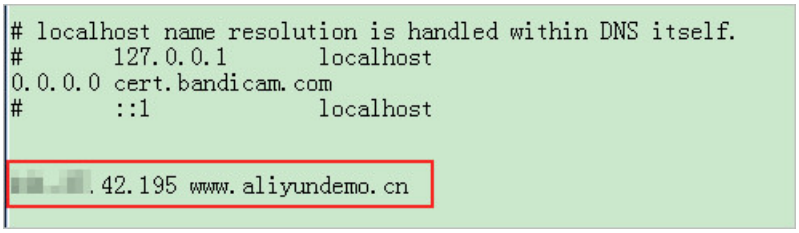
2. 在最后一行添加如下内容：`WAF的IP 被防护的域名`。

   以域名`www.aliyundemo.cn`为例，该域名已添加到WAF的网站配置中，且WAF为其分配了以下CNAME值：`xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`

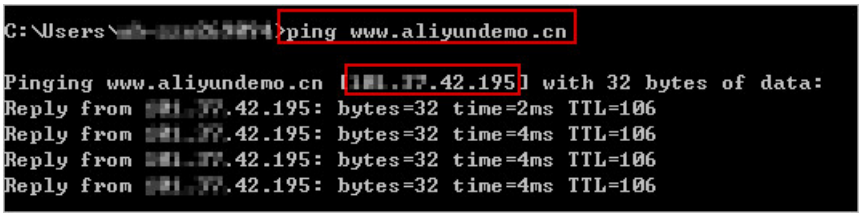
   a. 在Windows中打开cmd命令行工具，运行`ping xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`获取WAF IP。如下图所示，在响应结果中可以看到用来防护您的域名的WAF IP。

   b. 在`hosts`文件添加如下内容，前面的IP地址即上一步获取的WAF IP地址，后面的域名即被防护的域名。

3. 修改`hosts`文件后保存。然后本地ping一下被防护的域名。

   预期此时解析到的IP地址应该是刚才绑定的WAF IP地址。如果依然是源站地址，可尝试刷新本地的DNS缓存（Windows的cmd下可以使用`ipconfig/flushdns`命令）。

验证WAF转发正常

确认hosts绑定已经生效（域名已经本地解析为WAF IP）后，打开浏览器，输入该域名进行访问，如果WAF的配置正确，预期网站能够正常打开。

同时也可以尝试手动模拟一些简单的web攻击命令。例如，您可以在URL后面加`/alert(xss)`（这是一个用作测试的Web攻击请求），访问`www.aliyundemo.cn/alert(xss)`。

预期WAF会弹出如下阻拦页面。

3.5 更新HTTPS证书

要使Web应用防护墙（WAF）帮助您监控HTTPS业务流量，您必须在网站配置中勾选HTTPS协议，并上传HTTPS证书，保证HTTPS协议状态正常。如果证书发生变化，您也要在WAF控制台及时更新证书。

背景信息

如果您已将证书文件上传到云盾SSL证书服务进行统一管理，那么在以下步骤中，您可以选择一个已有证书进行更新。

否则，您需要准备好网站的证书和私钥文件，以完成以下操作。

一般情况下，您所需准备的证书相关内容包括：

- ***.crt（公钥文件）或*.pem（证书文件）**
- ***.key（私钥文件）**

操作步骤

1. **登录云盾Web应用防火墙控制台。**
2. **在页面上方选择地域：中国大陆、海外地区。**
3. **在管理 > 网站配置页面，选择要操作的域名，单击其HTTPS协议状态右侧的上传按钮（ ）。**

4. 在更新证书对话框中，选择上传方式并上传证书。

- 如果该域名所绑定的HTTPS证书已添加至云盾SSL证书服务进行管理，您可以单击选择已有证书，直接选择想要上传的证书。

- 手动上传证书。单击手动上传，填写证书名称，并将该域名所绑定的证书文件和私钥文件中的文本内容分别复制粘贴到证书文件和私钥文件文本框中。

> **说明:**
>
> - 对于.pem、.cer、.crt格式的证书，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；对于其他格式（如.pfx、.p7b等）的证书，则需要将证书文件转换成.pem格式后，才能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式，请参考HTTPS证书转换成PEM格式。
> - 如果该HTTPS证书有多个证书文件（如证书链），需要将证书文件中的文本内容拼接合并后粘贴至证书文件文本框中。

证书文件文本内容样例：

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx8ixZJ4krc+1M+
j2kcubVpsE2
cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOk
jgvhlqt9vc
65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9
nIrHsPl8YKk
vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

私钥文件文本内容样例：

```
-----BEGIN RSA PRIVATE KEY-----
DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQ
```

```
Cr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJ
aiygoIYo
aMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDz
FdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

5. 单击保存，成功上传证书和私钥文件。

预期结果

HTTPS协议状态显示为正常。

3.6 HTTPS高级配置

WAF提供灵活的HTTPS配置功能，帮助您在不改造源站的情况下，一键实现全站HTTPS和强制客户端使用HTTPS连接。

前提条件

如果您使用按量付费模式WAF，您必须在功能与规格中勾选支持HTTPS相关业务，才能使用HTTPS高级配置。更多信息，请参见功能与规格配置。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 在管理 > 网站配置页面，选择要操作的域名，单击其操作列下的编辑。
4. 在协议类型下勾选HTTPS，并单击打开高级设置菜单。

- 开启HTTP回源

  如果您的网站不支持HTTPS回源，请开启HTTP回源（默认回源端口是80端口），通过WAF实现HTTPS访问。使用该设置后，客户端可以通过HTTP和HTTPS方式访问站点。

  说明:

使用HTTP回源，可以无需在源站服务器上做任何改动，也不需要配置HTTPS。但是，该配置的前提是在WAF上传正确的证书和私钥（证书可以在阿里云证书免费申请）。

- 开启HTTPS的强制跳转

  如果您需要强制客户端使用HTTPS来访问（从安全性考虑，推荐这样做），您可以开启HTTPS的强制跳转。

  说明:
  开启HTTPS强制跳转前必须先取消HTTP协议。

  选择开启HTTPS的强制跳转后，部分浏览器将被缓存设置为使用HTTPS请求访问网站，请确保您的网站支持HTTPS业务。

  开启HTTPS强制跳转后，HTTP请求将显示为HTTPS，默认跳转到443端口。

3.7 非标端口支持

WAF默认支持以下端口：80/8080（HTTP）和443/8443（HTTPS）。企业版和旗舰版WAF实例支持更多的非标端口，且对被防护域名使用的不同端口的总数有相应限制。

如果您使用按量付费模式WAF，您必须在功能与规格中勾选支持非标端口业务防护，才能使用非标端口接入WAF。具体操作请参见功能与规格配置。

不同端口总数限制

针对每个阿里云账号（即每个WAF实例），由WAF防护的全部域名所使用的不同端口的总数有以下限制：

- **每个企业版用户支持最多10个不同的端口（包含80/8080/443/8443端口）**
- **每个旗舰版用户支持最多50个不同的端口（包含80/8080/443/8443端口）**
- **按量付费开通的WAF支持最多50个不同的端口（包含80/8080/443/8443端口）**

说明:
独享版支持更大范围的非标端口的接入防护，且支持基于HTTP、HTTPS和HTTP 2.0协议的自定义回源端口配置。更多详细信息，请参见*#unique_20*。

支持的端口

WAF仅防护支持的端口，对于不支持的端口WAF既不会防护，也不会转发。例如，4444端口的业务请求到达WAF后，请求会被直接丢弃。

说明:
具体端口支持情况，请以控制台显示为准。

- **在企业版和旗舰版WAF中，HTTP协议支持以下端口：**

  80、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、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8080、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:
其中，48800端口仅在中国大陆地区WAF实例中支持，海外地区实例暂不支持该端口。

- 在企业版和旗舰版WAF中，HTTPS协议支持以下端口：

  443、4443、5443、6443、7443、8443、8553、8663、9443、9553、9663、18980

注意:
其中，18980端口仅在中国大陆地区WAF实例中支持，海外地区实例暂不支持该端口。

- 按量付费的WAF实例在开启支持非标端口业务防护后，支持上述HTTP和HTTPS端口。

3.8 标记WAF回源流量

在将网站域名接入Web应用防火墙进行防护时，您可以为网站域名设置流量标记。当该网站域名的流量经过WAF时，WAF将在请求中添加对应的流量标记，便于后端的源站服务器统计相关信息。

根据您在流量标记中设置的HTTP Header字段名称和字段值，当流量经过WAF时，WAF将在所有请求头中添加对应的字段和字段值。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）、防护效果分析等。

说明:
如果所设置的HTTP自定义头部字段已存在，WAF仍将用您设置的流量标记字段值覆盖该请求中的原本存在的字段值。

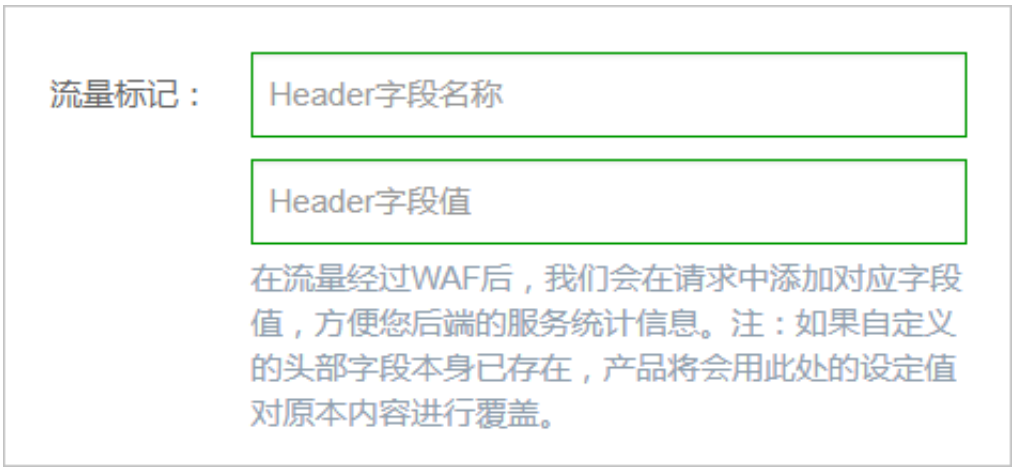
操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，选择域名配置记录，单击编辑。

说明:
您也可以在添加网站域名配置时，设置流量标记。

4. 在流量标记配置项中，填写Header字段名称和字段值。

> **说明:**
> 请勿填写已经被使用的自定义Header字段，否则请求中该字段的值将被WAF的流量标记字段值所覆盖。



5. 单击确定。配置生效后，WAF将在转发该网站域名的请求时添加对应的HTTP Header字段和字段值。

3.9 WAF源站负载均衡

如果您的源站有多个服务器，在为域名接入WAF防护时，您可以添加多个源站IP。配置多源站IP后，WAF在将过滤后的访问请求回源时，按照IP Hash或轮询的方式去做负载均衡。同时，WAF也会对多个源站进行健康检查。

配置示例

假设源站IP有3个（1.1.1.1、2.2.2.2、3.3.3.3）。您可以添加网站配置或编辑已有网站配置（具体操作参见网站配置），在服务器地址中添加多个源站IP（下图示例中包括1.1.1.1、2.2.2.2、3.3.3.3）。一个域名最多支持添加20个源站IP。

添加多个源站IP后，您需要指定负载均衡算法：IP hash、轮询。

> **说明:**
> 使用IP HASH时，如果源IP不够分散，可能会出现负载不均。

3.10 同时部署WAF和DDoS高防

Web应用防火墙本身仅拥有阿里云默认提供的最大5Gbps的DDoS基础防护能力，如果您希望同时为业务接入Web攻击防护和DDoS高级防护，我们推荐您组合使用阿里云Web应用防火墙（WAF）和DDoS高防。本文介绍了为业务同时部署WAF和DDoS高防的配置方法。

前提条件

- **开通*Web*应用防火墙**
- **开通*DDoS*高防**

背景信息

WAF的核心能力是防护应用层的攻击，典型的是一些由恶意攻击者精心构造的攻击请求，而WAF本身不具备DDoS高级防护能力。DDoS高防的核心能力在于防护DDoS攻击，偏向于流量攻击。更多信息，请参见*#unique_35*。

网络攻击者往往不会仅用单一的攻击方式发起攻击，多采用混合型的攻击方式，既有流量型攻击，又混杂精巧的Web应用层攻击等其他攻击方式。因此，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，一般建议您根据遭受的攻击进行分析来选择适合的防护手段。

WAF与DDoS高防完全兼容。您可以参照以下架构为网站业务同时部署WAF和DDoS高防：DDoS高防（入口层，实现DDoS防护）> Web应用防火墙（中间层，实现应用层防护）> 源站。

操作步骤

1. 在Web应用防火墙中添加网站配置。
   a) 登录云盾Web应用防火墙控制台
   b) 在管理 > 网站配置页面，单击添加网站。
   c) 添加新的网站，并在网站信息中完成以下配置。
      - 域名：填写被防护网站的域名。
      - 服务器地址：勾选IP并填写ECS公网IP、SLB公网IP、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。

      说明:
      更多信息，请参见网站配置。

      成功添加网站配置。
   d) 在网站配置列表中复制网站的WAF Cname地址。
2. 在DDoS高防中添加网站配置。
   a) 登录云盾DDoS高防（新BGP）控制台。
   b) 在管理 > 网站配置页面，单击添加网站。
   c) 在填写域名信息任务中， 完成以下配置，并单击添加。
      - 功能套餐和实例：选择要使用的DDoS高防实例。
      - 网站：填写被防护网站的域名。
      - 协议类型：勾选源站支持的协议类型。
      - 服务器地址：勾选源站域名并填写步骤1中获得的WAF Cname地址。

      说明:

更多信息，请参见添加网站配置。

成功添加网站配置，获得DDoS高防Cname地址。

3. 更新域名的DNS解析。前往域名的DNS服务商处，设置域名解析，添加一条CNAME记录，将网站域名的解析地址指向步骤2获得的DDoS高防Cname地址。

说明:

更多信息，请参见业务接入*DDoS*高防配置。

预期结果

完成上述配置后，网站流量先经过DDoS高防，再转发到Web应用防火墙。

3.11 同时部署WAF和CDN

云盾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。

a) 登录阿里云CDN控制台。

b) 在域名管理页面，选择要操作的域名，单击管理。

c) 在源站信息下，单击修改配置。

d) 修改源站信息。

- 类型：选择源站域名。
- 域名：填写WAF生成的CNAME地址。
- 端口：选择80端口。

e) 前往回源配置页面，在回源配置页签下，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。**

4 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。本文介绍了源站服务器保护的相关配置方法。

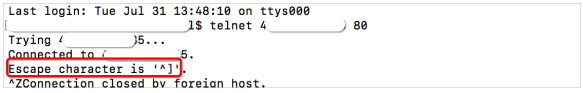
背景信息

> **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，一旦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:**
> 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实例上的所有网站域名都已经接入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，确保网站正常访问。这种情况下，如果源站已配置安全组防护，则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，选择WAF实例所在的地区。
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。

> **说明:**

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

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

     a. 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。

     b. 切换到本实例安全组页面。

     c. 选择目标安全组，并单击其操作列下的配置规则。

     d. 单击添加安全组规则，并配置如下安全组规则：

     说明:
     安全组规则授权对象支持输入“10.x.x.x/32”格式的IP网段，且支持添加多组授权对象（以“,”隔开），最多支持添加10组授权对象。

     - 网卡类型：内网

       说明:

如果ECS实例的网络类型为经典网络，则网卡类型需设置为公网。

- 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

e. 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：内网

说明:

如果ECS实例的网络类型为经典网络，则网卡类型需设置为公网。

- 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小的全端口放行策略。

- 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，具体设置方法请参见*#unique_42*。

  a. 登录负载均衡管理控制台，前往访问控制页面，单击创建访问控制策略组。
  b. 填写策略组名称，添加WAF回源IP网段，单击确定。
  c. 在实例管理页面，选择相应的负载均衡实例。
  d. 在监听页签中，选择端口监听记录，单击更多 > 设置访问控制。
  e. 启用访问控制，选择访问控制方式为白名单，并选择所创建的WAF回源IP网段的访问控制策略组，单击确定。

后续步骤

源站保护配置完成后，您可以通过测试已接入WAF防护的源站IP80端口和8080端口是否能成功建立连接验证配置是否生效。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示源站保护配置成功。

5 获取访问者真实IP

本文介绍了业务接入Web应用防火墙（WAF）后，如何获取访问者的真实IP地址。

在大部分实际业务场景中，网站访问请求并不是简单地从用户（访问者）的浏览器直达网站的源站服务器，中间可能经过所部署的CDN、DDoS高防、WAF等代理服务器。例如，网站可能采用这样的部署架构：用户 > CDN/DDoS高防/WAF > 源站服务器。这种情况下，访问请求在经过多层加速或代理转发后，源站服务器该如何获取发起请求的真实客户端IP?

一般情况下，透明的代理服务器在将用户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，用于记录用户的真实IP，其记录格式为`X-Forwarded-For:用户IP`。如果期间经历多个代理服务器，则X-Forwarded-For将以该格式记录用户真实IP和所经过的代理服务器IP：`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Web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。

注意:
在开始配置前，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

1. 确认已安装http_realip_module模块。

   为实现负载均衡，Nginx使用http_realip_module模块来获取真实IP。

   您可以通过执行`# nginx -V | grep http_realip_module`命令查看是否已安装该模块。如未安装，则需要重新编译Nginx服务并加装该模块。

   说明:
   一般情况下，如果您通过一键安装包安装Nginx服务器，默认不安装该模块。

   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服务配置文件。**

   打开default.conf配置文件，在location / {}中添加以下内容：

   说明：

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

```
set_real_ip_from ip_range1;
set_real_ip_from ip_range2;
...
set_real_ip_from ip_rangex;
real_ip_header    X-Forwarded-For;
```

3. **修改日志记录格式（log_format）。**

   *log_format*一般在nginx.conf配置文件中的http配置部分。在*log_format*中，添加x-forwarded-for字段，替换默认的remote-address字段，即将*log_format*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" ';
```

4. **重启Nginx服务，使配置生效。**

   完成以上操作后，执行nginx -s reload命令重启Nginx服务。配置生效后，Nignx服务器即可通过X-Forwarded-For的方式记录访问者真实IP。

IIS 6配置方案

您可以通过安装*F5XForwardedFor.dll*插件，从IIS 6服务器记录的访问日志中获取访问者真实IP地址。

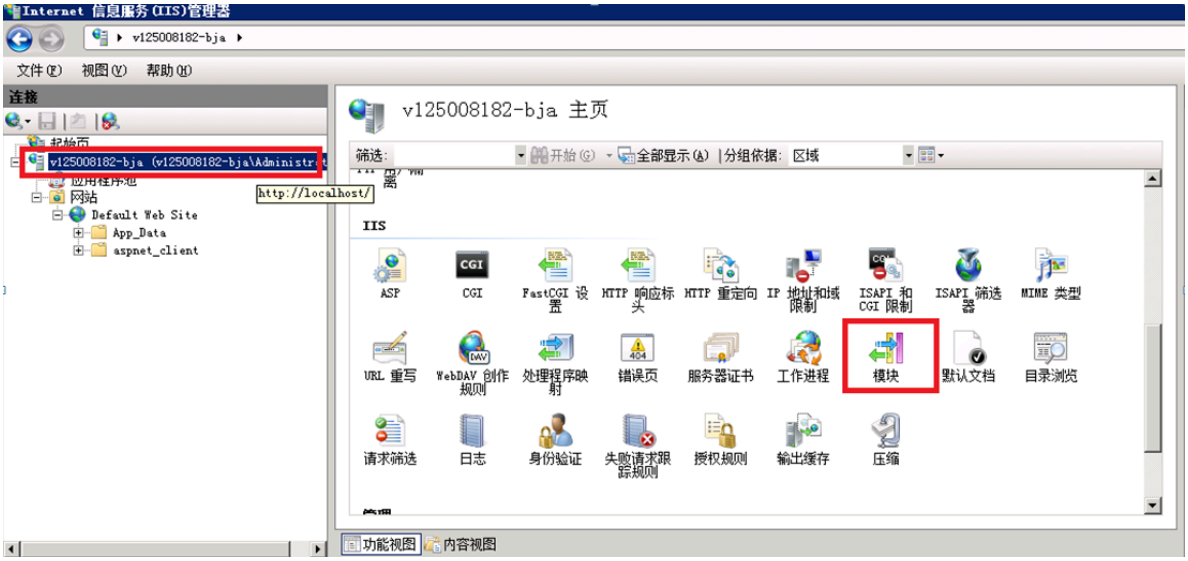
1. **根据您服务器的操作系统版本将*x86\Release*或者*x64\Release*目录中的*F5XForwardedFor.dll*文件拷贝至指定目录（例如，*C:\ISAPIFilters*），同时确保IIS进程对该目录有读取权限。**
2. **打开IIS管理器，找到当前开启的网站，在该网站上右键选择属性，打开属性页。**
3. **在属性页切换至ISAPI筛选器，单击添加。**
4. **在添加窗口下，配置以下参数，并单击确定。**
   - **筛选器名称：F5XForwardedFor**
   - **可执行文件：F5XForwardedFor.dll的完整路径，例如*C:\ISAPIFilters\F5XForwardedFor.dll***

5. **重启IIS服务器，等待配置生效。**

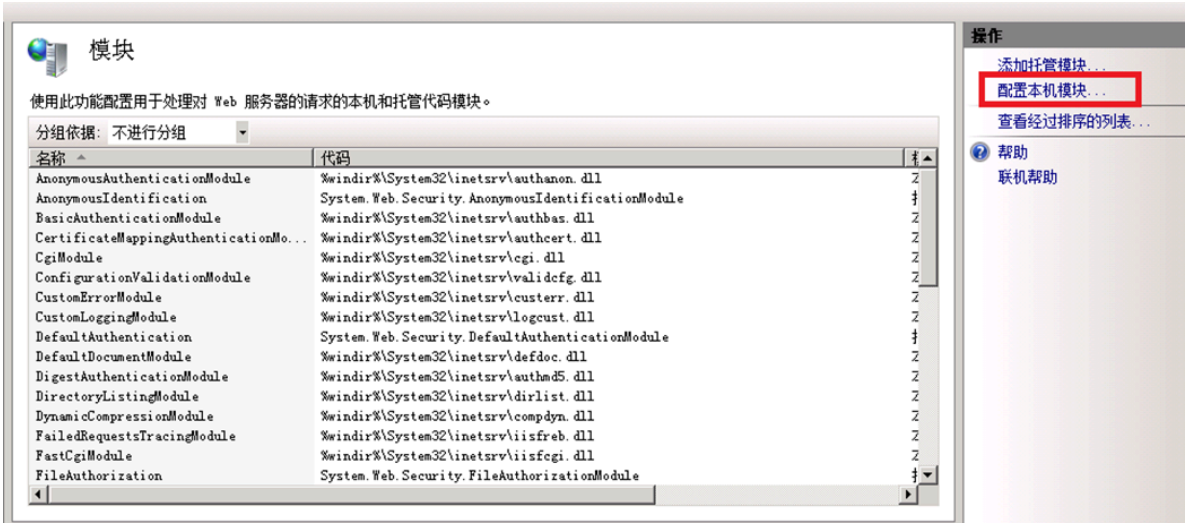
IIS 7配置方案

您可以通过安装*F5XForwardedFor*模块，获取访问者真实IP地址。

1. **根据服务器的操作系统版本将*x86\Release*或者*x64\Release*目录中的*F5XFFHttpModule.dll*和*F5XFFHttpModule.ini*文件拷贝到指定目录（例如，*C:\x_forwarded_for\x86*或*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。**



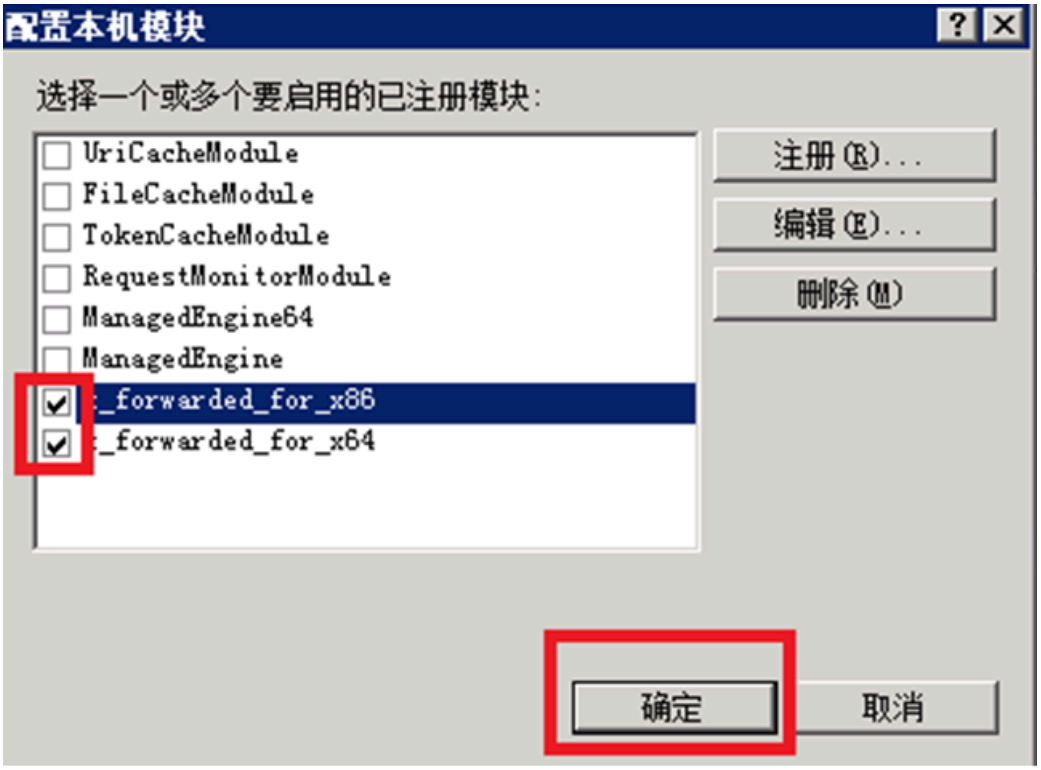
3. **单击配置本机模块。**



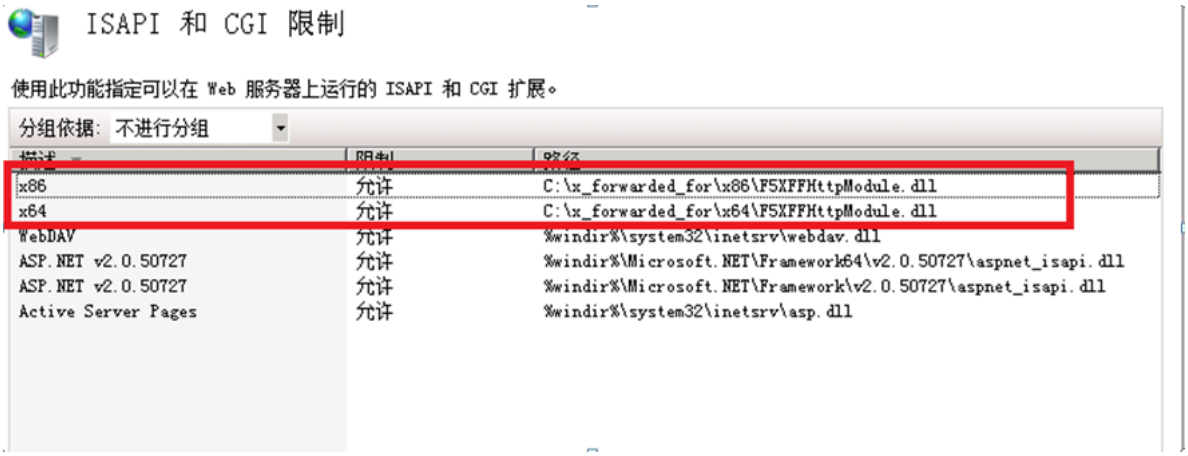
4. 在配置本机模块对话框中，单击注册，分别注册已下载的DLL文件。

- **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

Windows操作系统

在Apache 2.4及以上版本的安装包中已自带remoteip_module模块文件（mod_remoteip.so），您可以通过该模块获取访问者真实IP地址。

1. 在Apache的extra配置文件夹（*conf/extra/*）中，新建httpd-remoteip.conf配置文件。

   说明：

   为减少直接修改httpd.conf配置文件的次数，避免因操作失误而导致的业务异常，通过引入remoteip.conf配置文件的方式加载相关配置。

2. 在httpd-remoteip.conf配置文件中，添加以下访问者真实IP的获取规则。

```
#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 112.124.159.0/24 118.178.15.0/24 120.27.173.0
/24 203.107.20.0/24 203.107.21.0/24 203.107.22.0/24 203.107.23.0/24
47.97.128.0/24 47.97.129.0/24 47.97.130.0/24 47.97.131.0/24
```

3. 修改*conf/httpd.conf*配置文件，插入httpd-remoteip.conf配置文件。

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

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，获取访问者真实IP地址。

如果您服务器使用的Apache版本低于2.4，参考以下步骤通过Apache的第三方模块（mod_rpaf），获取访问者真实IP地址。

1. 执行以下命令，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. 修改Apache配置文件*/alidata/server/httpd/conf/httpd.conf*，在文件最后添加以下内容：

   说明：

其中，`RPAFproxy_ips ip`地址不是代理服务器提供的公网IP。具体IP可参考Apache的日志，通常会有两个IP地址。

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

3. 添加完成后，执行以下命令重启Apache服务，使配置生效。

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

mod_rpaf模块配置示例

```


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

通过启用Tomcat的X-Forwarded-For功能，获取访问者真实IP地址。

打开*tomcat/conf/server.xml*配置文件，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="false"/>
```

6 WAF接入配置最佳实践

将网站域名接入云盾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，在各类场景中使用云盾Web应用防火墙更好地保护您的网站。

正常网站业务接入场景

业务梳理

首先，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，后续可使用地区封禁功能屏蔽非法来源地区。
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大陆地域	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，请参见非标端口支持。
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。

梳理项	说明
（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。
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

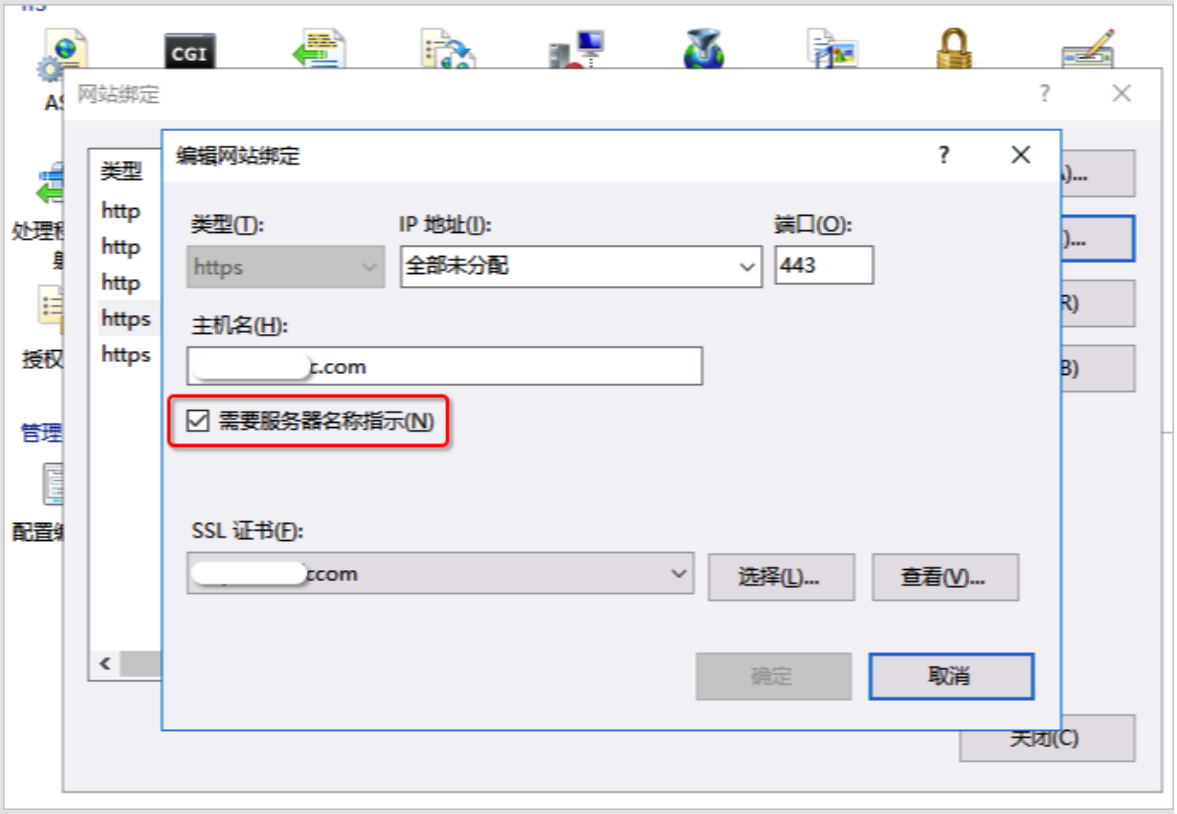
> **说明:**
> 如果在添加域名配置时，提示“您配置的域名已被其它用户使用”。建议您检查是否已在其它阿里云账号的WAF实例中添加与该域名冲突的配置记录。如果确实存在，您需要删除造成冲突的域名配置记录后再进行配置。

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。
- 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。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：

- Web攻击防护

  一般情况下，建议选用防护模式，并选用中等规则防护策略。

> 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。

- CC攻击防护

  业务正常运行时，建议采用系统默认配置。

> 说明：
> 由于CC防护的攻击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，不建议您开启攻击紧急模式。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。

- 精准访问控制：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。
- 封禁地区：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

在日志分析方面，WAF提供两大功能供您选择：

- 全量日志：建议您为网站开启全量日志功能，通过全量日志您可以对网站遭受的七层网络攻击进行分析，发现其攻击行为特征。

  说明：

全量日志功能仅支持企业版以上的WAF实例。对于按量付费WAF实例，您需要手动启用全量日志功能。

- 日志服务：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。

· 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*监控告警功能，实时感知攻击事件。

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。

表 6-1: 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前是否有配置其它七层代理（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

编号	检查项	是否必检
13	是否已了解按量付费实例的计费方式 说明: 仅适用于按量付费WAF实例。	是

表 6-2: 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
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：
  - *Web*攻击防护最佳实践
  - *CC*攻击防护最佳实践
- 如果您使用的是按量付费WAF实例，请仔细阅读*WAF*按量付费实例计费方式，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*防护包或*DDoS*高防产品防御DDoS攻击。
- 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、WAF实例为中国大陆地区、主要访问用户来自中国大陆地区的情况，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大陆地区。
  - 针对源站服务器在海外、WAF实例为海外地区、主要访问用户来自中国大陆地区的情况，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，推荐您使用中国大陆地区的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，云盾Web应用防火墙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

1. 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。

2. 已对业务系统进行安全加固。
3. 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。

> 注意:
> 如果您使用的是按量付费WAF实例，请仔细阅读*WAF*按量付费实例计费方式，避免出现实际产生的费用超出预算的情况。

安全专家服务

购买开通云盾Web应用防火墙后，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。