阿里云
Web应用防火墙

快速入门

文档版本：20200221

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 步骤2：修改DNS解析

通过DNS配置模式接入WAF时，当您成功添加网站配置后，Web应用防火墙（WAF）为网站生成一个专用的CNAME地址。您可以使用该CNAME地址更新域名的CNAME解析记录值，将网站的Web请求转发至WAF进行监控，完成WAF接入。

前提条件

- 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。本示例中，要修改的解析记录应托管在已开通WAF的阿里云账号下的云解析DNS服务中。

背景信息

- 如果在步骤1：自动添加网站配置中已自动更新DNS解析记录，且DNS解析状态正常，请直接执行步骤3：配置WAF防护策略。

- 如果在步骤1：自动添加网站配置中收到提示，需要手动修改DNS解析或者DNS解析状态异常，请参见下文手动修改DNS解析。

  下文以阿里云云解析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。

  > **说明:**
  > WAF通常采用CNAME解析的方式将网站接入进行防护，也支持以A记录解析的方式接入。如果您必须使用A记录解析的方式接入（例如，CNAME记录与MX记录冲突等情况），您可以Ping WAF CNAME地址，获取对应的WAF IP，并参见#unique_6进行后续操作。一般情况下，防护该域名的WAF IP不会频繁变更。

操作步骤

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*#unique_6*，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。

人工配置服务

如果您在添加网站配置时遇到问题或者配置后域名DNS解析状态异常，您可以购买人工配置服务。由安全工程师为您提供一对一专人支持服务，帮助您将网站域名接入Web应用防火墙进行防护，解决配置问题。

2 步骤1：自动添加网站配置

开通Web应用防火墙（WAF）后，您需要在WAF控制台上配置要防护的网站信息。本文介绍通过DNS配置模式接入WAF时，如何使用自动添加的方式创建网站配置。

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。

背景信息

> **说明:**
> 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。本快速入门根据DNS配置模式向您介绍相关操作。关于透明代理模式，请参见使用透明代理模式接入*WAF*。

通过DNS配置模式接入WAF时，当您选择添加网站配置，WAF会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也会自动更新域名的解析记录（即步骤2：修改*DNS*解析的操作），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。

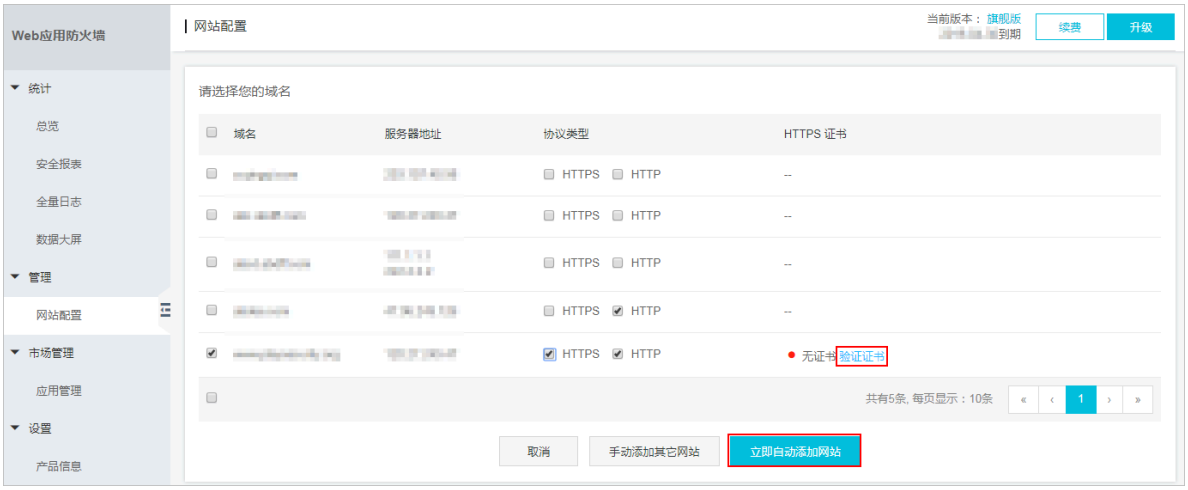
操作步骤

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。

人工配置服务

如果您在添加网站配置时遇到问题或者配置后域名DNS解析状态异常，您可以购买人工配置服务。由安全工程师为您提供一对一专人支持服务，帮助您将网站域名接入Web应用防火墙进行防护，解决配置问题。

3 WAF快速入门概览

本文将指导您在开通Web应用防火墙（WAF）后，快速部署和使用WAF。您只需要完成网站接入和WAF防护配置，即可为网站部署WAF防护。然后，您可以通过WAF安全防护记录和统计信息，实时掌握您的业务安全状况。

> 说明:
> 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。本快速入门根据DNS配置模式向您介绍相关操作。关于透明代理模式，请参考使用透明代理模式接入*WAF*。

WAF快速入门步骤

任务名	任务描述	推荐方法	前提条件
1. 自动添加网站配置	在WAF控制台添加要防护的网站信息。	自动添加网站。	· 要防护的网站使用阿里云云解析DNS进行域名解析，且在云解析DNS中存在解析A记录。 · （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。 · （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。
（可选）2. 修改*DNS*解析	修改网站的DNS解析记录，将网站收到的Web请求转发给WAF进行监控。 说明: 自动添加网站配置时收到“要手动修改DNS解析”的提示，或者手动添加网站配置时，需要执行该任务。	通过修改网站CNAME解析记录接入WAF。	· 获取WAF CNAME地址。 · 具有在域名的DNS服务商处更新DNS记录的权限。
3. 配置*WAF*防护策略	在WAF控制台调整WAF安全防护功能和策略。	使用默认防护设置。	已完成网站接入且网站配置的DNS解析状态正常。

任务名	任务描述	推荐方法	前提条件
4. 查看安全报表	在WAF控制台查看已接入业务的安全防护数据。	· 使用总览页面查看业务和安全概况。 · 使用安全报表页面查看详细安全防护和风险记录。	已完成网站接入且网站配置的DNS解析状态正常。

更多关于WAF的部署和使用方法，请参考*WAF*功能使用概览。

4 步骤3：配置WAF防护策略

网站接入Web应用防火墙（WAF）后，WAF以默认防护策略为其过滤常见Web攻击（如SQL注入、XSS等）和CC攻击。您可以根据实际业务需求启用更多的WAF防护功能和调整WAF防护策略。

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，选择要操作的域名，单击其操作列下的防护配置。
4. 开启需要的防护功能并配置相应防护策略：

> **说明:**
>
> - 包年包月模式下，不同WAF版本支持的功能不同，下述功能不一定都包含在您的WAF实例中。关于WAF各版本间的功能差异，请参见WAF各版本功能说明。
> - 针对按量付费模式，请参见功能与规格配置，选用需要的防护功能。

功能	描述	相关文档
Web应用攻击防护	默认开启，帮助您防御SQL注入、XSS跨站攻击等常见的Web攻击。您可以根据实际业务需求选择不同强度的防护策略和模式。	Web应用攻击防护规则策略
CC安全防护	默认开启，帮助您防御针对页面请求的CC攻击。您可以根据实际业务需求选择不同强度的防护策略，或者自定义CC防护规则限制单个IP在指定时间段内的请求数量。	选择CC防护模式 自定义CC防护
大数据深度学习引擎	开启后，自动对请求做语义分析，检测经伪装或隐藏的恶意请求，帮助您防护通过攻击混淆、变种等方式发起的恶意攻击。	大数据深度学习引擎
精准访问控制	开启后，您可以自定义访问控制规则，根据请求来源IP、请求URL，以及常见的请求头字段过滤访问请求。	精准访问控制
封禁地区	开启后，帮助您一键封禁来自指定中国省份（地区）或海外地区的IP的访问请求。	封禁地区

功能	描述	相关文档
网站防篡改	开启后，您可以添加防护规则，锁定指定的网站页面，防止其信息被恶意篡改。被锁定的页面在收到请求时，返回您为其设置的缓存内容。	网站防篡改
数据风控	开启后，您可以添加防护规则，监控指定业务接口上的机器欺诈行为，如垃圾注册、账号被盗、活动作弊、垃圾消息等，并为其启用安全验证页面。	数据风控
防敏感信息泄漏	开启后，您可以添加防护规则，过滤服务器返回内容（异常页面或关键字）中的敏感信息，如身份证号、银行卡号、电话号码和敏感词汇等。	防敏感信息泄露
高频Web攻击IP自动封禁	开启后，帮助您自动封禁在短时间内进行多次Web攻击的客户端IP。	高频Web攻击IP自动封禁
目录扫描防护	开启后，帮助您自动封禁在短时间内进行多次目录遍历攻击的客户端IP。	目录扫描防护
扫描威胁情报	开启后，帮助您自动封禁来自常见扫描工具或阿里云恶意扫描攻击IP库中IP的访问请求。	扫描威胁情报
主动防御	采用自研机器学习算法学习域名合法流量，为域名自动生成定制的安全策略，防护未知攻击。	#unique_31

5 步骤4：查看安全报表

网站接入Web应用防火墙（WAF）后，您可以在WAF控制台查看网站的安全防护数据和风险信息，用于业务分析。

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. 前往统计 > 总览页面，查看业务和安全概览信息。

   支持查看的业务概览信息包括以下内容：

   - 近30天内的业务请求数量统计图（总QPS和各防护功能拦截的QPS）
   - 近30天内的业务带宽统计图（入带宽和出带宽）
   - 近30天内的业务异常响应数量统计图
   - 访问来源地域分布统计（访问来源区域TOP5、访问来源IP TOP10）
   - 访问源系统类型分布统计（移动端OS、PC端浏览器）
   - 响应时间最长的TOP5 URL
   - 被访问次数最多的TOP5 URL

   支持查看的安全概览信息包括以下内容：

   - 近30天的攻击防护统计（Web应用攻击、CC攻击、访问控制事件）
   - 风险预警信息（新发现的业务安全风险和行业安全风险）
   - WAF的安全防护规则更新消息

   具体内容，请参考总览。

4. 前往统计 > 安全报表页面，查看具体的攻击防护记录和风险预警记录。

   支持查看的攻击防护记录包括以下内容：

   - WAF阻断的所有Web攻击记录
   - WAF拦截的针对某个域名的CC攻击记录
   - 针对某个域名的访问控制事件记录

   支持查看的风险预警记录包括以下内容：

   - 来自已知的黑客的攻击记录
   - WordPress攻击记录
   - 疑似攻击记录
   - Robots脚本探测记录
   - 爬虫访问记录
   - 短信接口滥刷记录

   具体内容，请参考*WAF*安全报表。