ALIBABA CLOUD

阿里云

Web应用防火墙

常见问题

文档版本：20220429

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.WAF常见问题

本文汇总了您在购买和使用Web应用防火墙（Web Application Firewall，简称WAF）时的常见问题。

概览

非阿里云服务器能否使用WAF？

可以，WAF支持云外机房用户接入。WAF可以保护任何公网路由可达的服务器，不论是阿里云服务、其他的云服务、IDC机房等环境，都可以使用WAF。

> **注意** 要接入中国内地WAF实例的域名必须按照工信部要求完成ICP备案，否则不支持接入。

WAF支持云虚拟主机吗？

支持，WAF的所有版本都支持独享虚拟主机，直接开通WAF进行配置即可。

对于共享虚拟主机，由于使用的是共享IP，源站由多个用户共同使用，不建议单独配置WAF。

WAF是否支持防护HTTPS业务？

支持，WAF的所有版本都支持HTTPS业务，并且支持泛域名接入。

只需根据提示将SSL证书及私钥上传，WAF即可防护HTTPS业务流量。配置HTTPS业务接入后，WAF会先解密访问请求，检查请求包，再重新加密，并转发正常的请求到源站。

WAF是否支持自定义端口？

WAF企业版及旗舰版支持自定义非标准端口。企业版最多支持10个非标准端口，旗舰版最多支持50个非标准端口。

> **注意** 不是任意端口都支持自定义。非标准端口必须在支持范围内。更多信息，请参见WAF支持的端口。

WAF是否对接入端口有限制？

根据接入方式不同，具体说明如下：

- CNAME接入：

  WAF只支持接入通过指定端口提供HTTP/HTTPS服务的域名。关于WAF不同版本支持接入的端口范围，请参见各版本支持的端口。

- 透明接入：

  WAF对接入端口没有限制，您可以将80~65535范围内任意端口的Web业务，通过透明接入方式接入WAF进行防护。更多信息，请参见透明接入。

除了上述WAF对接入端口的限制，根据当前网络访问验证结果，互联网运营商侧或因部分高危端口存在安全隐患，会拦截针对高危端口的业务流量。相关的高危TCP端口包括：42、135、137、138、139、445、593、1025、1434、1068、3127、3128、3129、3130、4444、5554、5800、5900、9996。如果您的Web业务使用了上述高危端口，则业务接入WAF后，可能出现业务在部分地域无法被访问的问题。因此，建议您将业务接入WAF前，确保Web业务使用其他非高危端口。

WAF的QPS限制规格是针对整个WAF实例汇总的QPS，还是配置的单个域名的QPS上限？

WAF的QPS限制规格针对整个WAF实例。

例如，您在WAF实例上配置防护了3个域名，则这3个域名累加的QPS不能超过规定上限。如果超过已购买的WAF实例的QPS限制，将触发限速，可能导致随机丢包。

WAF是否支持HTTPS双向认证？

WAF暂时不支持HTTPS双向认证。

WAF是否支持Websocket、HTTP 2.0或SPDY协议？

WAF支持WebSocket协议，且企业版及以上规格支持HTTP 2.0。目前暂不支持SPDY协议。

HTTP 2.0业务接入WAF防护是否会对源站有影响？

有影响。HTTP 2.0业务接入WAF防护表示WAF可以处理客户端的HTTP 2.0请求，而WAF目前仅支持以HTTP 1.0/1.1协议转发回源请求，即WAF与源站间暂不支持HTTP 2.0。因此，如果您将HTTP 2.0业务接入WAF防护，则源站的HTTP 2.0特性将会受到影响，例如，源站HTTP 2.0的多路复用特性可能失效，造成源站业务带宽上升。

WAF支持哪些TLS协议？

中国内地WAF实例默认支持TLS 1.0、TLS 1.1、TLS 1.2，海外地区WAF实例默认支持TLS 1.1、TLS 1.2。

如果您有个性化需求（例如，不需要TLS 1.0版本、希望开启TLS 1.3等），可以自定义TLS配置。相关操作，请参见自定义TLS配置。

WAF是否支持接入采用NTLM协议认证的网站？

不支持。如果网站使用NTLM协议认证，经WAF转发的访问请求可能无法通过源站服务器的NTLM认证，客户端将反复出现认证提示。建议您使用其他方式进行网站认证。

WAF中的源站IP可以填写ECS内网IP吗？

不可以。WAF通过公网进行回源，不支持直接填写内网IP。

WAF能够保护在一个域名下的多个源站IP吗？

可以，一个WAF域名配置中最多支持配置20个源站IP地址。

WAF配置多个源站时如何负载？

如果您配置了多个源站IP地址，WAF默认使用IP Hash的方式对访问请求进行负载均衡。您也可以根据需要自定义负载均衡算法。更多信息，请参见添加域名。

WAF是否支持健康检查？

WAF默认启用健康检查。WAF会对所有源站IP进行接入状态检测，如果某个源站IP没有响应，WAF会将访问请求转发至其他源站IP。

> **说明** 源站IP无法响应时，WAF将为该源站IP自动设置一个静默时间。静默时间结束后，新的访问请求可能仍然会被转发至该源站IP。关于WAF的健康检查工作原理，请参见健康检查概述。

WAF是否支持会话保持？

WAF支持会话保持，但是默认不开启。如果您需要使用会话保持，请提交工单联系技术支持团队，申请开启会话保持。

修改WAF的源站IP是否有延迟？

有。修改WAF已防护的源站IP后，大约需要一分钟生效。

WAF的回源IP段是多少？

您可以在Web应用防火墙控制台的**系统管理 > 产品信息**页面查询WAF的回源IP段。更多信息，请参见放行WAF回源IP段。

WAF是否会自动将WAF回源IP段加入安全组？

WAF不会自动将WAF回源IP段添加到安全组。如果您的源站部署了其他防火墙或主机安全防护软件，建议您将WAF回源IP段添加至相应的白名单中。

建议您配置源站保护策略，对您的源站进行安全防护。详细信息，请参见设置源站保护。

WAF回源是否需要放行所有客户端IP？

根据您的业务情况，您可以只放行WAF回源IP段，也可以放行所有客户端IP。对于Web业务，建议您只放行WAF回源IP，实现源站保护。

WAF的独享IP是否能够防御DDoS攻击？

可以。

WAF为每个用户提供独立的IP，该IP同样适用DDoS防护的黑洞策略，和ECS、SLB服务器一致。WAF的黑洞阈值和当前地区ECS的默认阈值相同。

WAF能和CDN或DDoS高防一起接入吗？

WAF完全兼容CDN和DDoS高防服务。同时接入WAF、CDN和DDoS高防的最佳部署架构为：客户端 > DDoS高防 > CDN > WAF > 负载均衡 > 源站。

WAF与DDoS高防或CDN一起接入时，只要将WAF提供的CNAME地址配置为DDoS高防或CDN的源站即可。这样就可以实现流量在经过DDoS高防或CDN之后，被转发到WAF，再通过WAF最终转发至源站，从而对源站进行全面的安全防护。更多信息，请参见通过联合部署DDoS高防和WAF提升网站防护能力、同时部署WAF和CDN。

WAF是否支持跨账号使用CDN+高防+WAF的架构？

支持，您可以跨账号使用CDN、高防、WAF产品组合成抵御DDoS攻击和Web应用攻击的安全架构。

WAF如何保证上传证书及密钥的安全性？是否会解密HTTPS流量并记录访问请求的内容？

阿里云Web应用防火墙在防护HTTPS业务时，需要您上传对应的SSL证书及密钥，用于解密HTTPS流量并检测流量中的攻击特征。我们使用了专用的证书服务器（Key Server）来存储和管理密钥。Key Server依托于阿里云密钥管理系统KMS（Key Management Service），能够保护证书和密钥的数据安全性、完整性和可用性，符合监管和等保合规要求。关于KMS的详细介绍，请参见什么是密钥管理服务。

WAF使用您上传的SSL证书及密钥解密HTTPS业务流量，只用于实时检测。我们只会记录包含攻击特征（payload）的部分请求内容，用于攻击报表展示、数据统计等，不会在您未授权的情况下，记录全量的请求或响应内容。

阿里云Web应用防火墙已通过ISO 9001、ISO 20000、ISO 22301、ISO 27001、ISO 27017、ISO 27018、ISO 27701、ISO 29151、BS 10012、CSA STAR、等保三级、SOC 1/2/3、C5、HK金融、OSPAR、PCI DSS等多项国际权威认证，且作为标准的阿里云云产品，在云平台层面具备与阿里云同等水平的安全合规资质。详细内容，请参见阿里云信任中心。

> **说明** 使用WAF防护HTTPS业务时，您也可以选择双证书方案，即在WAF上使用一套证书及密钥，在源站服务器上使用另一套证书及密钥（两套证书及密钥必须都是合法的），以便将上传到WAF的证书及密钥与源站服务器的证书及密钥分开管理。

网站已接入WAF防护，为什么在域名列表中查询不到？

您的网站备案信息可能已经失效，导致域名不符合接入要求，已被WAF自动清除。您需要为该域名完成ICP备案，并重新将网站接入WAF防护。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** 您在将网站接入中国内地WAF实例（包括包年包月实例和按量计费实例）防护前，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。

WAF如何防御CC攻击？

WAF提供多种CC安全防护模式，您可以根据实际情况进行选择。更多信息，请参见设置CC安全防护。

如果您希望同时有好的防护效果和低误杀率，建议您选择WAF企业版和旗舰版，由安全专家定制针对性的防护算法。详细信息，请参见设置自定义防护策略。

在WAF管理控制台更改配置后大约需要多久生效？

一般情况下，更改后的配置在一分钟内即可生效。

WAF自定义防护策略（ACL访问控制）中的IP字段是否支持填写网段？

支持。

为什么URL匹配字段包含双斜杠（//）的自定义防护策略规则不会生效？

由于WAF的规则引擎在处理URL匹配字段时会进行标准化处理，默认将连续的正斜杠（/）进行压缩，因此无法正确匹配包含双斜杠（//）URL的自定义防护策略规则。

如果您需要对包含双斜杠（//）的URL设置ACL访问控制，您可以直接设置该URL对应的单斜杠路径作为匹配条件。例如，如果需要将 `//api/sms/request` 作为URL匹配字段的条件值，您只需在匹配内容中填写 `/api/sms/request` ，WAF即可针对包含该内容的请求进行访问控制。

WAF管理控制台中能查看CC攻击的攻击者IP吗？

可以。您可以开通WAF日志服务，然后使用日志查询功能查询CC攻击的攻击者IP信息。更多信息，请参见步骤1：开通WAF日志服务、日志查询。

如何查询WAF使用的带宽流量？

您可以在Web应用防火墙控制台的**总览**页面查看已使用的带宽流量情况。

2.证书与密钥不匹配问题排查

问题描述

您在DDoS高防控制台、WAF控制台上传网站HTTPS证书后，收到了**证书和密钥不匹配**的提示。

解决方案

可能原因	排查及修复建议

您上传的证书与私钥内容不匹配	验证证书和私钥文件的MD5值是否一致。如果不一致，表示证书文件和私钥文件关联了不同的域名，证书和私钥内容不匹配。
	您可以执行以下命令，分别查看证书和私钥文件的MD5值：
	`openssl x509 -noout -modulus -in <证书文件>|openssl md5`
	`openssl rsa -noout -modulus -in <私钥文件>|openssl md5`
	如果确认证书和私钥文件内容不匹配，建议您重新上传正确的证书和私钥文件。

RSA私钥格式错误	生成新的私钥并重新上传。 您可以执行以下命令，生成一个新的私钥： `openssl rsa -in <私钥文件> -out <新私钥文件>`

其他：修复证书链

购买SSL证书后，证书服务商一般会为您提供中间证书和域名证书。如果您只有域名证书，而没有中间证书，建议您使用证书修复工具进行修复。

您可以在服务器上执行以下命令，检查证书链的完整性：

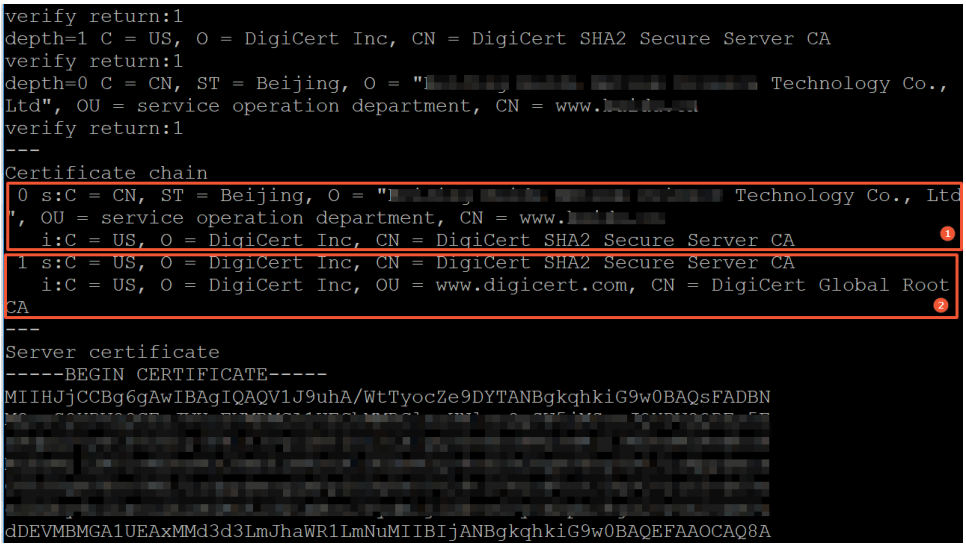
```
openssl s_client -connect <server ip>:443 -servername <domain name>
```

变量说明：

- `<server ip>`：需要替换成服务器IP地址。
- `<domain name>`：需要替换成网站域名。

> **说明** 该操作可以直接在服务器上执行，无需等待网站接入完成。

返回结果中，如果Certificate chain区域同时包含域名证书（图示①）和CA中间证书（图示②），表示证书链完整。



如果只有域名证书，没有CA中间证书，表示证书链不完整。这种情况下，建议您使用证书链修复工具修复证书链。例如，您可以使用myssl.com提供的证书链修复工具，下载域名的完整证书链，并使用下载的证书链替换您的证书文件。

一般证书文件的内容格式如下图所示，其中前半部分（图示①）是域名证书，后半部分（图示②）是中间证书。

> **注意** 内容中不能包含空格或回车字符。

3.按量计费常见问题

本文列举了按量计费模式Web应用防火墙（WAF）服务相关的常见问题。

> **注意** 开通按量计费WAF实例后，如果WAF实例连续五天不存在业务流量且未产生后付费账单，实例将会自动释放。

通过按量计费模式开通WAF后，如果没有实际使用，是否每天仍会产生费用？

按量计费模式WAF根据所配置的网站域名的实际流量进行计费，如果没有实际将网站域名接入WAF进行防护，一般情况是不会产生任何费用的。您只需关闭所配置的网站域名的所有WAF防护配置，WAF不会产生相关费用。

如果您仍然担心可能产生的费用，您可以将WAF的网站配置页面的所有网站域名配置记录删除，确保WAF不会产生任何相关费用。

如果确定不再继续使用按量计费模式的WAF，您可以在Web应用防火墙控制台单击**关闭WAF**。具体操作，请参见关闭WAF。

已经删除WAF所有的域名配置记录，DNS解析也已经切换回源站，为何仍然产生费用？

按量计费模式的WAF一般在次日生成账单并进行扣费。例如，您在3月21日删除了WAF所有的域名配置记录，则3月22日将生成最后一次的账单（3月21日的账单）并进行扣费，账单时间为2018-03-21 00:00:00至2018-03-22 00:00:00。此后，WAF将不会产生任何相关费用。

只在WAF中添加了域名配置记录，尚未将域名的DNS解析切换至分配的CNAME，为什么WAF还会产生费用？

由于互联网中存在各种爬虫脚本，当WAF检测到对应请求（可能是爬虫脚本对WAF所生成的CNAME地址的请求），就会产生费用。因此，如果您想要确保WAF不产生任何费用，请删除WAF网站配置页面中的所有域名配置记录。

WAF的按量计费模式和包年包月模式间如何切换？

- 如果您需要从按量计费模式切换至包年包月模式，您可以在Web应用防火墙控制台单击**关闭WAF**关闭按量计费模式，然后重新购买包年包月模式的WAF版本。
- 如果您需要从包年包月模式切换至按量计费模式，您可以在当前WAF实例到期后，在Web应用防火墙控制台单击**关闭WAF**释放当前WAF实例，然后重新开通按量计费模式的WAF服务。

试用按量计费模式的WAF一段时间后，如果不想继续使用，如何关闭WAF停止计费？

如果确定不再继续使用按量计费模式的WAF，您需要将您网站域名的DNS解析切换回源站，删除WAF中所有网站域名配置记录，并在Web应用防火墙控制台单击**关闭WAF**，从下个计费周期开始WAF将不再扣费。

> **说明** 关闭WAF后，您在第二天可能仍将收到关闭服务当日所产生的费用账单。例如，您在3月21日确定不再使用WAF并进行了关闭WAF操作，在3月22日您将收到最后一次的账单（即3月21日的账单）并进行扣费，账单时间为2018-03-21 00:00:00至2018-03-22 00:00:00。此后，WAF将不会产生任何相关费用。

按量计费模式的WAF是免费使用的吗？开通的时候显示每小时0元，为什么又显示最低消费4元/天？

开通按量计费模式的WAF后，如果您不配置任何网站域名WAF将不产生任何费用。当您在WAF中添加网站域名配置并启用防护功能后，WAF将根据当日网站的QPS（访问网站的每秒请求数）峰值和功能规格系数进行计费。例如，当所配置的网站当日的QPS峰值不超过5且仅启用基础防护功能规格时，WAF当天将仅产生4元的服务费用。

什么是QPS？按量计费模式的WAF如何计算网站当日的QPS峰值？

WAF中的网站QPS指的是当日00:00:00到23:59:59之间访问该网站的每秒请求数。

WAF每隔10秒统计一次该网站的QPS峰值，因此一天中共统计8,640（24*60*60/10）个QPS峰值点。根据QPS峰值大小排序，去除前1%（即86）个QPS峰值点，选取第87个最高QPS峰值点，作为当日该网站的QPS峰值，计算当日所产生的防护费用。

> **说明** 只要该网站当日存在访问请求，则QPS峰值最小为1。

建议您根据您网站的一般业务情况预估该网站的QPS峰值，计算WAF可能产生的防护费用。

如果已防护的网站遭受攻击导致出现当日网站QPS暴涨的情况，WAF是否会产生巨额的防护费用？

为了避免因遭受攻击导致QPS暴涨而产生巨额防护费用的情况，按量计费模式的WAF当日单个网站最多根据500 QPS峰值进行计费。

为何在规格设置页面显示的预估费用与实际账单费用不一致？

WAF管理控制台中的设置预估费用是为了方便您计算在对应的功能规格和预估的QPS基础上可能产生的账单费用，仅供参考。

当日实际账单的费用将根据网站实际的QPS峰值与所启用的规格功能系数计算生成。

如何开通海外地区的按量计费模式WAF服务？

按量计费模式WAF服务暂不支持海外地区，建议您购买海外地区的包年包月模式WAF版本。

在按量计费模式WAF中如何取消“支持非标准端口业务防护”功能项？

按量计费模式WAF暂时不支持非标端口降配操作。如果您已经启用了**支持非标准端口业务防护**功能项，将无法禁用该功能。您需要在WAF管理控制台单击关闭WAF关闭当前WAF实例后，重新开通按量计费模式的WAF服务。

> **警告** 关闭WAF实例将删除您当前WAF实例中的所有配置，请谨慎操作。

在按量计费模式WAF中如何取消已添加的扩展域名包/独享IP包？

按量计费模式WAF暂时不支持扩展域名包和独享IP包的降配操作。如果您已经添加了扩展域名包或独享IP包，将无法取消。

按量计费模式WAF支持哪些非标端口？

按量计费模式WAF默认支持HTTP的80和8080标准端口，HTTPS的443和8443标准端口。开启**支持非标准端口业务防护**功能项后，可支持更多非标端口，请参见WAF支持的端口。

按量计费模式WAF已开启防护开关，为何防护效果不明显？

为已配置的网站开启防护开关后，WAF将根据默认防护规则拦截恶意请求。您可以在自定义防护策略中配置防护规则，为您的网站实行针对性的防护。更多信息，请参见设置自定义防护策略。

4.按量计费2.0版本常见问题

本文汇总了WAF按量计费2.0版本的常见问题。

我已使用了旧版按量计费实例，如何切换到2.0版本实例？

您可以从以下切换方案中选择一种：

- 主动切换。您需要先把接入旧版按量计费实例的网站流量切回到源站（即将域名解析指向源站），关闭旧版按量计费WAF实例后，重新购买2.0版本按量计费实例，然后再将网站流量接入到按量计费2.0版本实例。
- 统一切换。阿里云WAF团队后续会将旧版按量计费实例统一切换到2.0版本，具体切换时间请等待通知。统一切换方案确定之前，旧版按量计费用户默认仍使用旧版按量计费模式，没有变化。如果您有切换到2.0版本的强烈诉求，可以提交工单联系我们，咨询是否可以提前切换。

旧版按量计费模式如果切换成2.0版本后，是否能够选择切换回旧版？

不能。

已经购买的按量计费资源包，是否可以用于抵扣按量计费2.0版本产生的费用？

可以。

按量计费2.0版本实例中开启某个防护功能后，会立即计费吗？

会的。防护功能即开即用，并会作为当天已开通功能进行计费，算在次日的账单中。

是不是所有防护功能都可以随时关闭（降配）？

不一定。防护功能均支持降配，但在降配操作时会进行校验。如果该防护功能在使用中或者配置了防护规则，则不允许降配。您必须先关闭对应防护功能或者删除对应规则之后才可以降配。

关闭某个防护功能后，当天还会对该功能计费吗？

会的。关闭防护功能时立即生效，但当天关闭的防护功能仍算作当天已开通功能，会被计算在次日的账单中。如果您在次日未重新开启该防护功能，则第三天的账单中不会包含该防护功能的费用。

按量计费2.0版本是否支持域名扩展包？对接入域名的个数有什么限制？

按量计费2.0版本不支持域名扩展包，按照实际接入的域名个数计费。

目前，默认允许接入的一级域名个数最多是30个。如果您需要接入更多的一级域名，可以提交工单联系我们。 允许接入的二级或者多级域名的个数没有限制，按照您实际接入的域名数量执行阶梯价格累加收费。关于定价的更多信息，请参见按量计费2.0版本计费方式。

按量计费2.0版本是否支持独享IP？具体如何计费？

支持。在按量计费2.0版本中，您无需预先购买独享IP包，可以直接为域名开启独享IP。按量计费2.0版本按照您开启使用的独享IP的个数进行计费，单价为20元/个/天。

> **说明** 独享IP开启后，会被计入当日费用。为了避免资源浪费和非预期费用的产生，请按实际需要选择使用。

按量计费2.0版本是否支持存储超过7天的日志？

不支持。按量计费2.0版本的日志服务功能目前只支持存储最近7天的日志。

开通日志服务时，如何选择存储容量？

开通日志服务时，您可以根据要记录日志的域名业务的QPS，选择对应的日志存储容量。建议如下：

- 需要记录日志的域名业务的QPS在700以内，日志存储容量设置为1 T即可。
- 如果QPS大于700，建议您按照1 T/700 QPS的对应关系，选择存储容量。

如果将日志存储容量降配到0 T，已经记录的日志是否会被立即删除？

不会。日志存储容量降配到0 T以后，日志会立即停止写入。由于日志存储时长固定为7天，因此当前已存储日志不会被立即删除，但会在7天后被完全清除。

购买按量计费2.0版本，是否能够帮助我通过信息安全等级保护（等保）？

不能。由于按量计费2.0版本的日志存储时长固定为7天，不满足等保规定中180天日志存储时长的要求。推荐您购买预付费的WAF高级版实例，以完成等保评审。

WAF控制台的账单和费用中心的金额是什么关系？为什么会有数据对不上的情况？

一般情况下，WAF控制台的账单和费用中心的数据是一致的。

WAF控制台的账单是根据按量计费方式，在产品页面直观展示当前配置下的费用，属于账单理论值。费用中心则在账号、实例维度，展示根据计费规则产生的详细出账记录，包含账单上叠加的折扣、优惠、资源包抵扣等情况。因此，如果在实际出账时存在特殊的折扣、优惠等，可能会使WAF控制台和费用中心的数据不一样。

5.WAF日志服务常见问题

本文汇总了WAF日志服务的常见问题。

如何开启WAF日志服务？

如果您使用的是包年包月WAF实例（高级版及以上规格），您可以在购买WAF实例时选择开启日志服务。如果您在购买WAF实例时未开启日志服务，购买实例后需要开启日志服务，则可以通过升级实例来开启日志服务。具体操作，请参见包年包月实例操作步骤。

如果您使用的是WAF按量计费实例，您需要在Web应用防火墙控制台的**系统管理 > 账单与套餐中心**页面，通过**修改套餐**，将**系统规格**下的**日志存储容量**设置为大于0的值。具体操作，请参见按量计费实例。

WAF日志会记录什么内容？

WAF日志主要记录客户端向已接入WAF进行防护的域名发起的HTTP/HTTPS请求。您为域名开启日志采集后，则客户端请求只要经过WAF，都会保留对应日志。如果域名未开启日志采集，则WAF不会记录对应的客户端请求。

关于如何为域名开启、关闭日志采集，请参见步骤2：开启日志采集。

如何评估我需要的日志存储容量？

您可以根据日志存储配置和网站业务的日常QPS，选择您需要的日志存储容量。

日志存储配置包括：

- 日志存储类型：分为存储全量日志、只存储攻击拦截日志。存储全量日志所需日志存储容量更大。
- 日志存储时长：存储时长越长，所需日志存储容量越大。
- 日志包含的字段：WAF日志字段分为必选字段（日志中必须包含的字段）和可选字段（日志中可以自定义是否包含的字段）。启用的可选字段越多，所需日志存储容量越大。

首次开通WAF日志服务后，默认日志存储配置为：存储全量日志、存储时长为180天、日志只包含必选字段。您可以通过**日志设置**功能修改日志存储配置。相关操作，请参见修改日志设置。

以默认日志存储配置为例，您可以参考以下信息，根据网站业务的日常QPS，选择所需日志存储容量：

- 日均QPS不大于80的业务防护场景，推荐选择3 TB存储容量。
- 日均QPS在80~120范围的业务防护场景，推荐选择5 TB存储容量。
- 日均QPS在120~260范围的业务防护场景，推荐选择10 TB存储容量。
- 日均QPS在260~350范围的业务防护场景，推荐选择15 TB存储容量。
- 日均QPS在350~500范围的业务防护场景，推荐选择20 TB存储容量。
- 日均QPS在500~1200范围的业务防护场景，推荐选择50 TB存储容量。

> **说明** 如果您需要自定义日志存储配置，可以在以上信息基础上估算需要的日志存储容量。

WAF日志服务是否支持修改日志存储时长？

只有包年包月WAF实例支持在30~360天范围内，修改日志存储时长。WAF按量计费实例仅支持存储最近7天的日志，不支持修改日志存储时长。

如果您使用的是包年包月WAF实例（企业版及以上规格），且已开启WAF日志服务，则可以在Web应用防火墙控制台的**日志管理 > 日志服务**页面，通过**日志设置**，修改日志存储时长。具体操作，请参见修改日志设置。

6.网站访问异常

本文介绍了已经接入Web应用防火墙进行防护的网站出现访问异常问题时，如何排查和修复问题。

排查流程

网站接入Web应用防火墙后，如果出现访问异常，您可以按照以下流程排查问题：

1. 检查是否为源站问题：通过旁路Web应用防火墙，判断是否为源站服务器的响应问题。
2. 检查是否为WAF误拦截：通过手动关闭防护模块，判断是否为WAF误拦截问题。
3. 排查常见访问错误：对照常见访问异常错误，分析和排查问题。

> **说明** 如果上述方法都不能帮助您解决问题，您可以工单联系阿里云技术工程师。

关于排查问题中可能用到的工具，请参见附录：常用工具介绍。

检查是否为源站问题

您可以参照以下步骤旁路Web应用防火墙，判断源站服务器响应是否有问题：

1. 禁用源站上的安全组、黑白名单、防火墙、安全狗、云锁等应用，防止WAF回源IP被拉入黑名单。
2. 修改本地计算机的*hosts*文件，将问题域名的解析指向对应的ECS实例、SLB实例、服务器公网IP（即在WAF上填写的源站IP地址）。
3. 通过本地计算机的浏览器访问问题域名，查看访问请求不经过Web应用防火墙时，是否能复现问题。
   - 如果问题复现，说明可能是源站服务器的响应异常，建议您及时检查源站服务器的工作状态（例如进程、CPU、内存、Web日志等）是否有异常并修复异常。
   - 如果问题没有复现，说明不是源站服务器的响应异常，请参见检查是否为WAF误拦截。

检查是否为WAF误拦截

您可以参照以下步骤关闭WAF的拦截功能，判断是否是WAF误拦截：

1. 为域名关闭**正则防护引擎**（具体操作请参见设置规则防护引擎），查看问题是否仍然存在。

   如果问题消失，建议您将**正则防护引擎**的**防护规则组**设置为**宽松规则组**（默认为**中等规则组**），或者您可以通过日志服务分析有问题的URL，并添加一条自定义防护策略（具体操作请参见设置自定义防护策略），放行访问该URL的请求。

2. 如果关闭**正则防护引擎**后问题仍然存在，您可以为域名关闭**CC安全防护**（具体操作请参见设置CC安全防护），查看问题是否仍然存在。

   如果问题消失，建议您将**CC安全防护**的模式设置为**防护**（如果本来就是**防护**模式，请忽略），或者您可以通过日志服务分析有问题的URL，并添加一条自定义防护策略（具体操作请参见设置自定义防护策略），放行访问该URL的请求。

   如果关闭**CC安全防护**后问题仍然存在，说明不是WAF误拦截，请参见排查常见访问错误。

排查常见访问错误

如果发现不经过Web应用防火墙问题会消失，而接入Web应用防火墙后，问题稳定复现，您可以按照以下方式进行排查。

问题	现象	原因	解决方案
405访问阻断	出现405阻断页面或者HTTP返回码为405。	请求被自定义防护策略或者正则防护引擎阻断。	1. 为域名关闭自定义防护策略（具体操作请参见设置自定义防护策略），查看是否还有405页面。 如果不再出现，说明您所配置的自定义防护规则误拦截了请求，需要您找到对应规则并将其删除。 2. 如果关闭自定义防护策略开关后问题仍然存在，您可以为域名关闭**正则防护引擎**（具体操作请参见设置规则防护引擎），查看问题是否仍然存在。 如果问题消失，建议您将**正则防护引擎**的**防护规则组**设置为**宽松规则组**（默认为**中等规则组**），或者您可以通过日志服务分析有问题的URL，并添加一条自定义防护策略（具体操作请参见设置自定义防护策略），放行访问该URL的请求。
302连接重置	某些IP在访问网站时显示连接被重置，HTTP返回码为302，且在请求头获得Set-Cookie。	IP访问触发了CC防御规则。	为域名关闭**CC安全防护**（具体操作请参见设置CC安全防护），查看问题是否仍然存在。 如果关闭防护后访问恢复正常，说明是CC防护规则误拦截，建议您将**CC安全防护**的模式设置为**防护**（如果本来就是**防护**模式，请忽略），或者您可以通过日志服务分析有问题的URL，并添加一条自定义防护策略（具体操作请参见设置自定义防护策略），放行访问该URL的请求。
HTTPS访问异常	客户端的HTTPS请求返回证书为 `www.notexist.com` 。	Web应用防火墙需要浏览器支持SNI，而客户端的浏览器可能不支持SNI。	一般苹果系统默认支持SNI，而Windows、Android系统需要做SNI兼容，具体请参见SNI兼容性导致HTTPS访问异常（服务器证书不可信）。
502访问白屏	网站显示白屏，同时HTTP返回码为502。	当源站（指ECS、SLB或服务器）出现丢包或者不可达的时候，Web应用防火墙会返回白屏。	1. 检查源站是否有黑名单、iptables、防火墙、安全狗、云锁等安全软件或策略。如果有，停用或卸载相关服务并清空黑名单，查看问题是否消失。 2. 绕过WAF测试访问（参见检查是否为源站问题），检查是否正常。如果仍然无法正常访问，可检查源站的进程、CPU、内存、Web日志等是否有异常。
域名ping不通	域名ping不通，且收到短信提示，WAF受DDoS攻击，进入了黑洞。	DDoS流量攻击不在Web应用防火墙的防护范围内。	开通DDoS防护服务，抵御DDoS攻击。更多信息，请参见概述。
服务器负载不均	后端多台服务器负载不均。	Web防火墙使用四层IP哈希。因此，当DDoS高防串联Web应用防火墙或SLB使用四层转发时，ECS可能出现负载不均。	Web应用防火墙和ECS直接使用SLB负载均衡，即使用7层转发，并打开cookie会话保持或负载均衡。

问题	现象	原因	解决方案
微信或支付宝回调失败	微信或支付宝回调失败。	可能是高频访问被CC防护规则拦截，或者使用了HTTPS方式回调，且微信和支付宝不支持SNI。	• CC安全防护问题： i. 为域名关闭**CC安全防护**（具体操作请参见设置CC安全防护），查看问题是否仍然存在。 ii. 如果关闭防护后恢复正常，说明是CC防护规则误拦截，建议您将**CC安全防护**的模式设置为**防护**（如果本来就是**防护**模式，请忽略），或者您可以通过日志服务分析有问题的URL，并添加一条自定义防护策略（具体操作请参见设置自定义防护策略），放行访问该URL的请求。 • SNI问题：设置让微信或支付宝直接调用ECS或者SLB IP，不要经过Web应用防火墙。更多信息，请参见SNI兼容性导致HTTPS访问异常（服务器证书不可信）。

附录：常用工具介绍

- Chrome浏览器-开发者工具：Chrome浏览器自带开发者工具，可以用来查看页面元素的加载情况。按**F12**打开工具，切换至**Network**标签。
- ping：Windows和Linux操作系统自带的网络测试工具，可以用来分析和判定网络故障。Windows系统按Win+R，输入CMD打开工具。用法：`ping 域名或IP`。
- traceroute（Linux）、tracert（Windows）：链路追踪工具，可以检测在哪一跳发生丢包。Windows系统按CTRL+R，输入*cmd*打开工具。用法：`tracert -d 域名或IP`。
- nslookup：用于检测域名解析的工具，可以检查域名解析是否生效。Windows系统按CTRL+R，输入*cmd*打开工具。用法：`nslookup 域名`。
- 17测网站：用于探测全国访问质量、DNS解析和丢包情况。

7.HTTPS访问异常问题

接入WAF后出现HTTPS访问异常（HTTP是正常的），例如页面打不开、提示证书不可信、部分接口调用失败、部分机型、操作系统、App访问报错等问题，您可以参照本文提供的排错方法来排查问题。

确认控制台已选中HTTPS并已上传证书

使用WAF防护HTTPS业务时，必须在WAF控制台上选中HTTPS，并且上传与服务器完全一样的证书和密钥。即使WAF与高防、SLB、CDN等其他产品一起使用时，也要在WAF上传证书和密钥。WAF的证书是独立于其他产品。

> **说明** 在控制台上传证书成功后，可能需要最多5分钟的时间来使配置完全生效，在此期间可能出现访问异常的现象。您可以绑定hosts（相关操作，请参见本地验证），确保配置已经生效之后，再将DNS解析切换过来。

确认证书链完整（常见错误）

多数情况下，证书服务商会提供给您多个证书（其中包含服务器的证书以及一个或多个CA根证书），这些证书组合成一个完整的证书链。以阿里云的证书为例，您收到的证书链如下图所示。

请确保在WAF中上传了完整的证书链而不是只有部分证书。请将多个证书文本内容联合到一起，并确保服务器证书在上面，根证书在下面。以下是您需要上传的证书内容的一个样例。

```
-----BEGIN CERTIFICATE-----
……
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
……
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
……
-----END CERTIFICATE-----
```

如果证书链不完整，可能会出现打开页面提示证书不可信，某些安卓手机、操作系统或App访问报错、异常等情况（可能部分环境下访问是正常的）。

您也可以借助网上的第三方检测工具（例如GeoCerts SSL Checker）来检查当前的证书链是否完整。

> **说明** 这种方式只能检测当前解析到的域名状态。假如您已经将解析回源而没有解析到WAF，是无法检测WAF上的证书状态的。

SNI问题

如果出现特定的一些客户端或应用程序不能正常访问HTTPS业务，提示“SSL handshake failed/error”或者证书不可信，则很可能是客户端不支持SNI引起的。这些客户端或应用程序可能是旧版本的安卓，低版本Java开发的一些调用程序（特别是使用SSL协商的程序）、XP系统的IE浏览器、某些老款手机，以及第三方的支付回调接口等。

目前绝大部分的浏览器和应用程序、微信、支付宝回调接口等都已全面支持SNI。如果您将解析切换回源站就恢复正常，切换到WAF就异常，则可能是这个问题。建议升级相关的客户端，或者将回调接口直接解析回源。

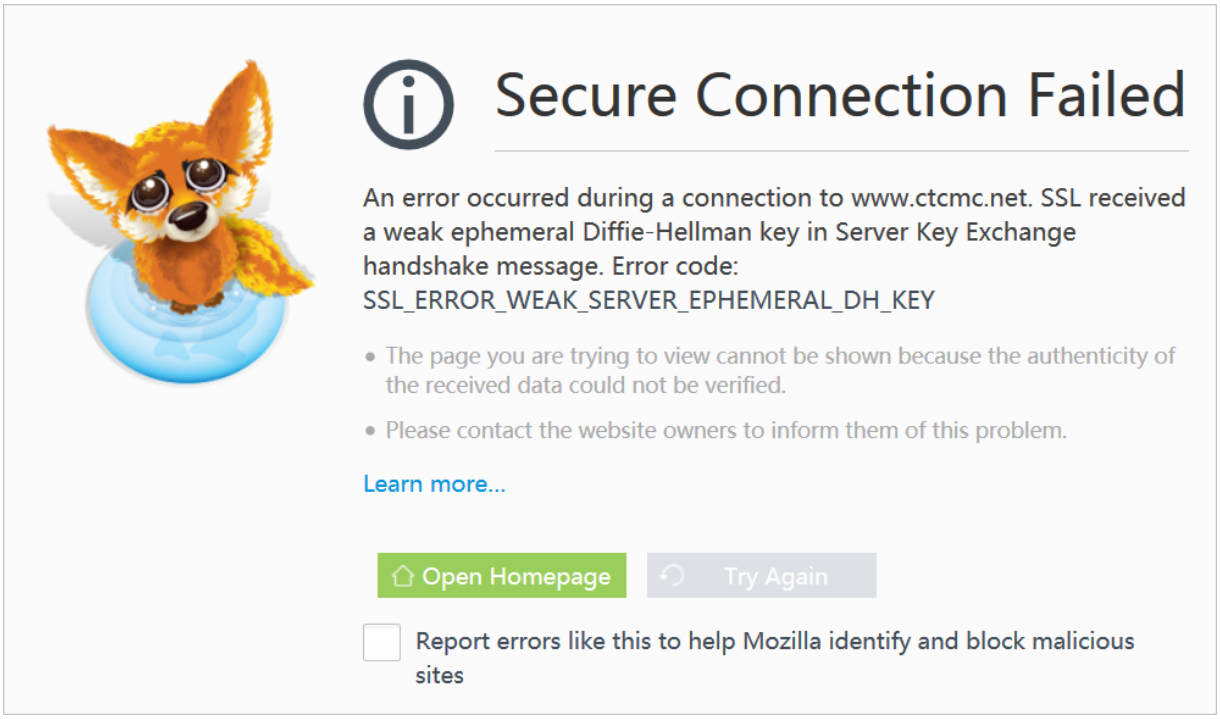
更多信息，请参见SNI兼容性导致HTTPS访问异常（服务器证书不可信）。

Windows Server 2003、IIS6服务器

Windows Server 2003、IIS6服务器在接入WAF后，访问HTTPS业务会出现白屏和502现象。这是因为系统TLS版本和加密套件过旧，安全性太弱，与WAF默认的HTTPS回源算法不兼容。目前，我们不再支持对2003系统的HTTPS回源，微软官方也已不建议使用2003系统搭建HTTPS站点。为了您的通信安全，请升级至2008或以上的操作系统。

DH密钥太短导致连接失败

因为过短的DH（Diffie-Hellman）密钥存在安全问题，WAF已经停止对短密钥的支持。同样的，当您使用较新版本的火狐浏览器（例如51.0.1）不经过WAF访问源站，也会看到相应的报错信息。



请升级相关组件（例如JDK版本），确保服务器DH算法的key位数为2048比特或更大。

说明 Key的长度是服务器加密算法决定的，与证书无关。如果您不知道如何操作，请联系您的服务器开发人员，或搜索相关的解决方案。您可以根据以下报错信息来查找相关解决方案：`SSL routines:ssl3_check_cert_and_algorithm:dh key too small`。

需要HTTP跳转的业务也需要选中HTTP

如在源站服务器做了访问HTTP强制跳转到HTTPS的设置，则必须在WAF上选中HTTP和HTTPS。否则，HTTP请求到了WAF后，无法正常转发回源站，也会报错。

8.SNI兼容性导致HTTPS访问异常（服务器证书不可信）

本文介绍了因客户端不兼容SNI，导致业务接入Web应用防火墙后出现HTTPS访问异常的解决方法。

背景介绍

随着IPv4地址的短缺，为了让多个域名复用一个IP地址，在HTTP服务器上引入了虚拟主机的概念。服务器可以根据客户端请求中不同的Host，将请求分配给不同的域名（虚拟主机）来处理。在一个被多个域名（虚拟主机）共享IP的HTTPS服务器中，当浏览器访问一个HTTPS站点时，会首先与服务器建立SSL连接。建立SSL连接的第一步是请求服务器的证书。服务器在发送证书时，不知道浏览器访问的是哪个域名，所以不能根据不同域名发送不同的证书。

SNI（Server Name Indication）是为了解决一个服务器使用多个域名和证书的SSL/TLS扩展。它的工作原理是：在与服务器建立SSL连接之前，先发送要访问站点的域名（Hostname），这样服务器会根据这个域名返回一个合适的证书。

目前，大多数操作系统和浏览器都已经很好地支持SNI扩展。OpenSSL 0.9.8 已经内置这一功能，新版的Nginx也支持SNI。

问题描述

在接入Web应用防火墙后，如果您出现HTTPS访问异常问题，可能是由于客户端不支持SNI导致的。

当使用不支持SNI的浏览器访问Web应用防火墙的网站时，Web应用防火墙因不知道客户端请求的是哪个域名，无法调取对应的虚拟主机证书来跟客户端交互，只能使用内置的一个缺省证书去跟客户端握手，这时在客户端浏览器上会提示“服务器证书不可信”。

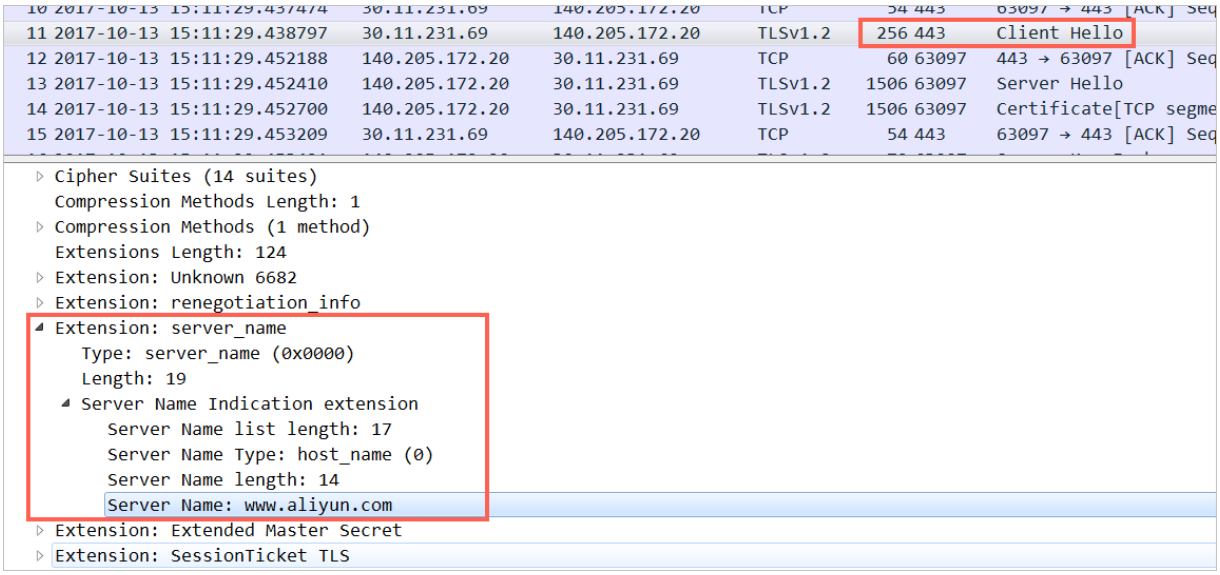
如果客户端不支持SNI，可能会出现如下现象：

- 在手机App客户端，iOS客户端可以正常访问，而Android客户端无法正常打开。
- 浏览器打开网站，显示证书不可信。

解决方案

您可以在客户端抓SSL握手的报文，来判断客户端是否支持SNI。以Chrome浏览器访问阿里云官网为例。

若在Client Hello报文里可以看到SNI扩展，则表示客户端支持SNI扩展。



否则，客户端不支持SNI扩展。对于不支持SNI的客户端有以下建议：

- 建议您升级或使用新版本的浏览器（如Chrome、Firefox等）。
- 如果是微信、支付宝第三方回调，需要让其调用源站IP，绕过Web应用防火墙。

SNI兼容性

> **说明** SNI兼容TLS1.0及以上协议，但不被SSL支持。

- SNI支持以下桌面版浏览器：
  - Chrome 5及以上版本
  - Chrome 6及以上版本（Windows XP）
  - Firefox 2及以上版本
  - IE 7及以上版本（运行在Windows Vista/Server 2008及以上版本系统中，在XP系统中任何版本的IE浏览器都不支持SNI）
  - Konqueror 4.7及以上版本
  - Opera 8及以上版本
  - Safari 3.0 on Windows Vista/Server 2008及以上版本，Mac OS X 10.5.6 及以上版本
- SNI支持以下库：
  - GNU TLS
  - Java 7及以上版本，仅作为客户端
  - HTTP client 4.3.2及以上版本
  - libcurl 7.18.1及以上版本
  - NSS 3.1.1及以上版本
  - OpenSSL 0.9.8j及以上版本
  - OpenSSL 0.9.8f及以上版本，需配置flag
  - Qt 4.8及以上版本
  - Python3、Python 2.7.9及以上版本

- SNI支持以下手机端浏览器：
  - Android Browser on 3.0 Honeycomb及以上版本
  - iOS Safari on iOS 4及以上版本
  - Windows Phone 7及以上版本
- SNI支持以下服务器：
  - Apache 2.2.12及以上版本
  - Apache Traffic Server 3.2.0及以上版本
  - HAProxy 1.5及以上版本
  - IIS 8.0及以上版本
  - lighttpd 1.4.24及以上版本
  - LiteSpeed 4.1及以上版本
  - nginx 0.5.32及以上版本
- SNI 支持以下命令行：
  - cURL 7.18.1及以上版本
  - wget 1.14及以上版本

9.已配置WAF防护的ECS源站遭受入侵的处理建议

如果您为网站配置WAF防护后，源站服务器ECS仍然被恶意攻击者入侵，请参照下表查看可能原因和对应解决方案。

序号	可能原因	解决方案
1	接入WAF之前已被入侵。	参照下文给出的方案清理您的服务器。
2	WAF配置好后，没有更改DNS解析，访问流量实际上还是直接去向服务器，没有经过WAF防御。	确保已经修改DNS解析，让网站在WAF防御之下。请参考业务接入WAF配置。
3	使用WAF之前，ECS IP已经暴露，且未配置安全组，黑客直接攻击ECS。	配置安全组，防止直接绕过WAF直接攻击ECS。请参考源站保护。
4	ECS服务器上还有其他站点，且该站点未受到WAF防护，导致服务器被“旁注”。	确保该ECS上所有HTTP业务都经过WAF防御。
5	非Web攻击方式入侵，例如暴力破解ECS SSH密码等。	确保ECS、数据库全部使用强密码。

注意 清理主机木马、病毒前，请先创建快照进行备份，避免误操作导致数据丢失无法还原。

排查病毒木马

1. 使用 `netstat` 查看网络连接，分析是否有可疑发送行为，如有则停止服务器。
2. 使用杀毒软件进行病毒查杀。

Linux中常用的木马清理命令有：

```
chattr -i /usr/bin/.sshd
rm -f /usr/bin/.sshd
chattr -i /usr/bin/.swhd
rm -f /usr/bin/.swhd
rm -f -r /usr/bin/bsd-port
cp /usr/bin/dpkgd/ps /bin/ps
cp /usr/bin/dpkgd/netstat /bin/netstat
cp /usr/bin/dpkgd/lsof /usr/sbin/lsof
cp /usr/bin/dpkgd/ss /usr/sbin/ss
rm -r -f /root/.ssh
rm -r -f /usr/bin/bsd-port
find /proc/ -name exe | xargs ls -l | grep -v task |grep deleted| awk '{print $11}' | awk -
F/ '{print $NF}' | xargs killall -9
```

排查并修复服务器漏洞

1. 查看服务器账号是否有异常。如有，则停止服务器，并删除异常账号。
2. 查看服务器是否有异地登录情况。如有，则修改登录密码为强密码。强密码由10位以上字符组成，同时

包含大小写字母、数字，和特殊符号。

3. 检查Jenkins、Tomcat、PhpMyadmin、WDCP、Weblogic等服务的后台密码，确保启用强密码。对于不使用的服务，建议关闭其8080管理端口。
4. 查看Web应用（如struts、ElasticSearch等）是否存在漏洞。确保网站在WAF防御之下，建议结合使用态势感知来查杀木马、病毒，并安装补丁。
5. 查看是否存在Jenkins管理员无密码远程执行命令漏洞。如有，请设置密码或关闭8080端口管理页面。
6. 查看是否有Redis无密码可远程写入文件漏洞。检查 `/root/` 下是否有黑客创建的SSH登录密钥文件，如有则将其删除。修改Redis为有密码访问并使用强密码。若不需要公网访问，请使用 `bind 127.0.0.1` 绑定本地访问。
7. 查看MySQL、SQLServer、FTP、WEB管理后台等其它设置密码的地方，确保启用强密码。

使用云盾服务

- 确保该ECS上所有网站都已启用WAF。
- 使用云盾态势感知，扫描主机风险和漏洞，查杀木马并修复漏洞。

重新初始化云盘

假如在排查过病毒木马及服务器漏洞，并启用云盾服务后，问题仍然存在，建议您重新初始化云盘，将作系统盘或数据盘用的云盘恢复到创建时的状态。

具体操作请参考重新初始化云盘。

> **注意** 在重新初始化云盘前，请将系统盘和数据盘的数据完全下载备份到本地保存；初始化以后，对数据进行杀毒后再上传。

重置磁盘后，重新执行排查病毒木马，排查并修复服务器漏洞，使用云盾服务。

使用云盾安全管家

如果上述方式均无法解决您的问题，或者操作过于复杂，建议您选购云盾安全管家（SOS）服务，购买付费服务，让云上专家帮助您解决问题。

10.WAF被黑洞怎么解决

本文介绍了Web应用防火墙（WAF）遭受大流量DDoS攻击后进入黑洞的影响及解决方法。

黑洞的影响

当WAF遭受到大流量DDoS攻击时，如果攻击流量超过了阿里云免费提供的DDoS防护能力，WAF实例对应的独享IP（简称WAF IP）就会进入黑洞。此时，您会在WAF控制台的**总览**页面，收到相关提示信息。

当WAF IP被黑洞后，所有转发到WAF实例的流量（包括正常请求和攻击流量）都会被丢弃。这意味着所有接入当前WAF实例防护的域名，在黑洞期间都无法访问。

如何解除黑洞和防御DDoS攻击

出现黑洞事件后，您只需等待黑洞时间结束，黑洞状态将会自动解除。默认的黑洞时间为150分钟。WAF的黑洞阈值与您的ECS所在地域的默认阈值相同。关于黑洞和阿里云黑洞策略的更多介绍，请参见阿里云黑洞策略。

> **说明** 默认情况下，每个WAF实例分配给您一个独享的IP，一旦这个WAF IP被黑洞，WAF实例上配置的所有域名都无法访问。为了避免这种情况发生，您可以为重要的域名单独购买额外的独享IP，以防重要域名受其他被DDoS攻击的域名牵连。关于独享IP的更多介绍，请参见域名独享资源包。

解决大流量DDoS攻击的根本办法是使用DDoS高防服务对您的域名进行防护。如果您已采用DDoS高防结合WAF的部署架构，但WAF仍然被攻击进入黑洞，请提交工单联系售后技术支持团队协助处理。

WAF黑洞常见问题

- WAF被黑洞了，是否能马上为我解除？

  不能。由于黑洞是阿里云向运营商购买的服务，而运营商对黑洞解除时间和频率都有严格的限制，所以黑洞状态无法人工解除，需要您耐心等待系统自动解封。

  > **说明** 即使能够立刻解除黑洞，如果WAF仍在遭受大流量DDoS攻击，还是会再次触发黑洞。

- WAF配置了多个域名，如何查看是哪个域名被攻击？

  一般情况下，黑客会解析某个已接入WAF防护的域名，在获取WAF实例的IP后，对其发起DDoS攻击。大流量的DDoS攻击都是针对WAF IP，从攻击流量中无法得知具体哪个域名被攻击。

  您可以使用域名拆分来获知哪个域名被攻击。例如，您可以将部分域名解析到WAF，部分域名解析到其他地址（ECS源站、CDN或SLB 等），如果拆分之后WAF不再被黑洞，说明黑客的攻击目标在拆分出去的部分域名。但是，这种方式操作比较复杂，且可能导致源站等其他资产的暴露，从而引发更大的安全问题。因此，除非在必要情况下，不建议您通过这种方式来判断哪个域名被攻击。

- 通过更换WAF的IP，是否就能不会被黑洞了？

更换WAF IP无法解决实际问题。如果黑客针对您的域名进行攻击，即使您更换了WAF IP，黑客只需要ping您的域名就能获取到更换后的IP，并且继续发起DDoS攻击。

- DDoS攻击和CC攻击有什么区别？WAF为什么不能防御DDoS攻击？

  大流量的DDoS攻击主要是针对IP的四层攻击，而CC攻击是针对七层应用的攻击（例如HTTP GET/POST Flood）。WAF可以防御CC攻击，但对于大流量的DDoS攻击，由于需要通过足够大的带宽资源把所有流量都硬抗下来再进行清洗，只能通过DDoS高防服务来防护。

11.支持防护的域名后缀

WAF支持添加防护的域名覆盖绝大多数的域名后缀，仅个别域名后缀无法接入防护。本文列举所有WAF支持接入防护的域名后缀供您查看。

> **说明** 如果您需要配置的域名不在支持范围内，请工单联系我们。

0~9

2000.hu	5xsoft.com

a

ac	ac.cn	ac.gn	ac.id	ac.il	ac.im
accountant	adult.ht	ae	aero	aeroport.fr	af
ag	agrar.hu	ah.cn	ai	al	am
app	apps.lair.io	art.ht	as	asia	assedic.fr
asso.gp	asso.ht	at	auction	audio	auto
avocat.fr	avoues.fr	无	无	无	无

b

ba	bar	be	best	bg	bh
bi	bike	biz	biz.id	biz.pk	biz.vn
bj.cn	black	bloxcms.com	blue	bo	bolt.hu
bs	business	by	bz	无	无

c

ca	cab	cafe	camera	camp	car
cards	care	cars	cash	casino.hu	cc
cc.ua	cci.fr	cd	center	ceo	cg
ch	chambagri.fr	chat	cheap	chirurgiens-dentistes.fr	ci
city	city.hu	cl	club	cm	cn
cn.cn	cn.com	cn.net	co	co	co.at

co.cm	co.cr	co.gg	co.gg	co.gl	co.gy
co.hu	co.id	co.id	co.id	co.il	co.il
co.im	co.in	co.ir	co.jp	co.kr	co.ma
co.nl	co.nz	co.th	co.tz	co.uk	co.za
coffee	com	com.ar	com.au	com.bd	com.bo
com.br	com.bz	com.cm	com.cn	com.cn	com.co
com.de	com.ec	com.es	com.fr	com.ge	com.gh
com.gh	com.gi	com.gl	com.gl	com.gn	com.gp
com.gr	com.gt	com.gt	com.gy	com.hk	com.hk
com.hn	com.hn	com.hr	com.ht	com.im	com.im
com.kw	com.kz	com.lc	com.mo	com.mx	com.my
com.my	com.ng	com.np	com.pa	com.pe	com.ph
com.pk	com.pl	com.ps	com.pt	com.py	com.ru
com.sg	com.sg	com.so	com.sususu	com.sv	com.tr
com.tw	com.ua	com.uy	com.vc	com.ve	com.vn
company	cool	coop.ht	cq.cn	cr	credit
cricket	cu	cx	cz	无	无

d

date	dd-dns.de	de	de.com	desa.id	dev.static.land
diet	diskstation.eu	diskstation.me	diskstation.org	dj	dk
dm	do	dog	domains	download	draydns.de
dray-dns.de	dscloud.biz	dscloud.me	dscloud.mobi	dsmynas.com	dsmynas.net
dsmynas.org	dynvpn.de	dyn-vpn.de	无	无	无

e

ec	edu	edu.bi	edu.cn	edu.ge	edu.gh
edu.gi	edu.gl	edu.gl	edu.gn	edu.gp	edu.gr

edu.gt	edu.gy	edu.hk	edu.hk	edu.hn	edu.ht
edu.mo	edu.my	edu.pl	edu.rs	edu.sg	edu.tw
ee	email	erotica.hu	erotika.hu	es	eu
experts-comptables.fr	无	无	无	无	无

f

fail	faith	family	familyds.com	familyds.net	familyds.org
fans	farm	fi	film.hu	fin.ec	firm.ht
fish	fit	fj.cn	flowers	fm	forum.hu
fr	from.hr	fund	fyi	无	无

g

ga	game	games.hu	gb	gb.net	gd
gd	gd.cn	gda.pl	gdansk.pl	gdynia.pl	ge
ge	geometre-expert.fr	gf	gf	gg	gg
gh	gh	gi	gi	github.io	gl
gl	global	gm	gn	go.id	gob.gt
gob.hn	gold	gouv.fr	gouv.ht	gov	gov
gov.cn	gov.cn	gov.ge	gov.gh	gov.gi	gov.gn
gov.gr	gov.gy	gov.hk	gov.ie	gov.il	gov.my
gov.sg	gov.vn	gp	gp	gq	gr
gr	green	greta.fr	group	gs	gs.cn
gt	guide	guitars	guru	gx.cn	gy
gz.cn	无	无	无	无	无

h

ha.cn	haus	hb.cn	he.cn	help	hi.cn
hiphop	hk	hk.cn	hk.com	hk.org	hl.cn

hm	hn	hn.cn	holiday	homelink.one	host
hosting	hotel.hu	house	ht	hu	hu.com
huissier-justice.fr	无	无	无	无	无

i

i234.me	idf.il	idv.hk	idv.tw	ie	ie
il	im	im	in	in.th	inbar.int
inc.hk	ind.gt	inf.ua	info	info.ec	info.ht
info.hu	info.vn	ingatlan.hu	ink	int	io
ir	is	it	iz.hr	无	无

j

je	jl.cn	jo	jobs	jogasz.hu	jp
js.cn	jx.cn	无	无	无	无

k

k12.il	kg	ki	kim	konyvelo.hu	kr
kr.com	kz	无	无	无	无

l

la	lakas.hu	land	lc	li	lib.de.us
life	limo	link	live	lk	ln.cn
love	lt	ltd.co.im	ltd.gi	ltd.hk	ltd.ua
lu	lv	ly	无	无	无

m

ma	markets	mba	md	me	me.uk
med.ec	med.ht	med.pl	medecin.fr	media	media.hu
mein-vigor.de	men	mg	mil.ge	mil.gh	mil.gt
mil.hn	mil.id	mil.my	mk	mn	mo

mo.cn	mobi.gp	mod.gi	money	mp	ms
mu	muni.il	mw	my	my	my.id
myds.me	myfz.com	mymai.com	my-vigor.de	my-wan.de	无

n

na	name	name.hr	name.my	net	net.au
net.cn	net.cn	net.co	net.ec	net.ge	net.gg
net.gl	net.gn	net.gp	net.gr	net.gt	net.gt
net.gy	net.hk	net.hk	net.hn	net.hn	net.ht
net.id	net.il	net.im	net.in	net.kw	net.my
net.pk	net.sg	net.vc	net.vn	network	news
news.hu	nf	ningja	nl	nm.cn	no
nom.es	notaires.fr	now.sh	nr	nu	nx.cn

o

one	online	ooo	or.id	or.kr	org
org.ag	org.au	org.bz	org.cn	org.cn	org.es
org.ge	org.gg	org.gh	org.gi	org.gl	org.gn
org.gp	org.gr	org.gt	org.gt	org.gy	org.hk
org.hk	org.hn	org.hn	org.ht	org.hu	org.il
org.il	org.im	org.in	org.mo	org.my	org.nz
org.pe	org.pk	org.sg	org.uk	org.vn	无

p

pa	party	pe	per.sg	perso.ht	pet
ph	pharmacien.fr	pink	pk	pl	plc.co.im
plus	pm	pn	poker	pol.ht	port.fr
pr	press	priv.hu	pro	pro.ec	pro.ht
ps	pt	pvt.ge	pw	无	无

q

qa	qh.cn	qou.cn	无	无	无

r

racing	re	reklam.hu	rel.ht	remotewd.com	ren
rent	rest	review	rip	ro	router.management
rs	ru	run	rw	rwit.cn	无

s

sa	sale	sc	sc.cn	sch.id	school
sd	sd.cn	se	se.com	sex	sex.hu
sexy	sg	sg	sh	sh.cn	shoes
shop	shop.ht	shop.hu	show	si	site
sites.static.land	sk	sl	sn.cn	so	social
solar	sopot.pl	space	spacekit.io	sport.hu	sr
st	stackspace.space	static.land	stolos.io	store	storj.farm
studio	style	suli.hu	sususu.admstask3	sx.cn	syno-ds.de
synology.me	synology-diskstation.de	synology-ds.de	szex.hu	无	无

t

taifun-dns.de	taipei	tattoo	tax	tc	team
tech	tel	tf	tips	tj	tj.cn
tk	tl	tm	tm.hu	tn	to
today	tools	top	town	townnews-staging.com	toys
tozsde.hu	transurl.be	transurl.eu	transurl.nl	travel	tt
tt.im	tuxfamily.org	tv	tv.im	tw	tw.cn

u

ua	uber.space	ug	uk.com	us	us.com
utazas.hu	uz	无	无	无	无

v

vc	vet	veterinaire.fr	vg	video	video.hu
vin	vip	vn	vpnplus.to	vu	无

w

wang	watch	web.id	webcam	website	wf
win	wine	wmflabs.org	work	works	world
ws	wtf	wzlm.cn	无	无	无

x

xin	xj.cn	xs4all.space	xxx	xyz	xz.cn

y

ybo.faith	ybo.party	ybo.review	ybo.science	ybo.trade	yn.cn
yoga	yolasite.com	yombo.me	yt	无	无

z

za.net	za.org	zhangkj.co	zj.cn	zone	无

12.已接入网站的未配置端口是否会对源站带来安全风险？

Web应用防火墙（WAF）对外提供流量接入转发服务，防护集群会默认提供一系列端口用于您的网站接入和防护服务，每个网站的业务流量只通过网站接入时配置的HTTP/HTTPS端口进行接入业务流量转发。

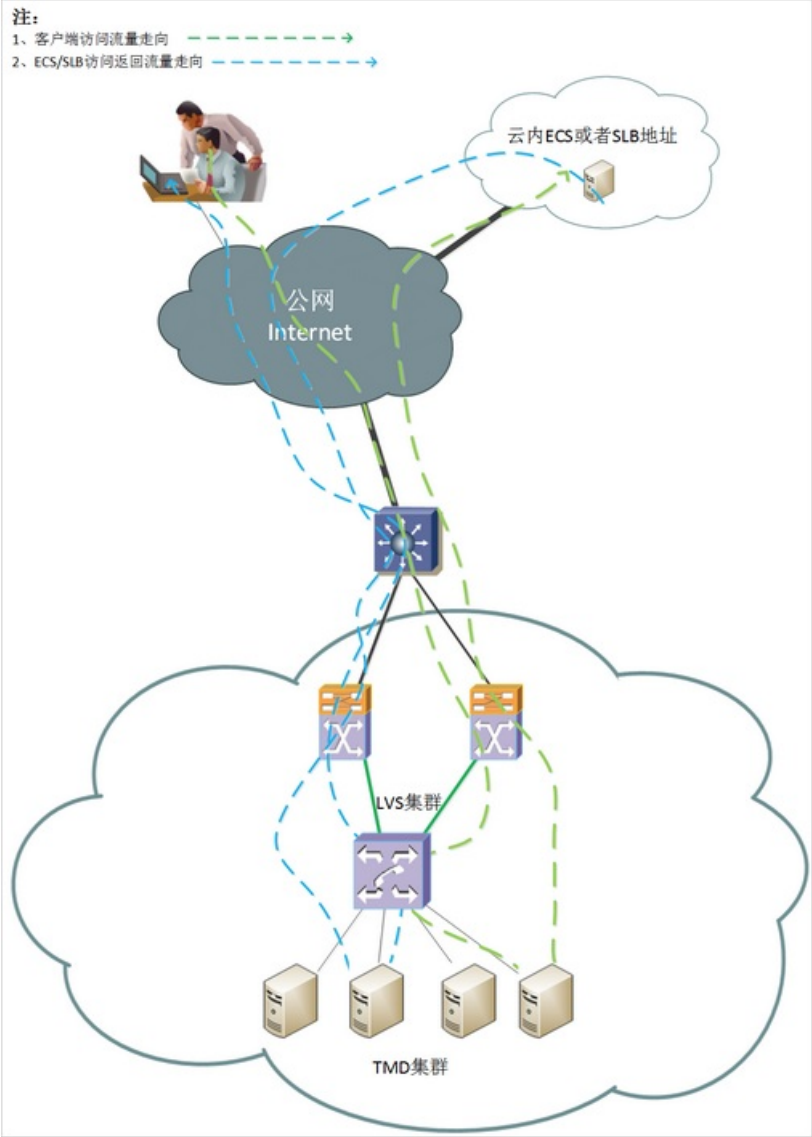
对于已接入WAF防护的网站，WAF防护集群不会转发未配置端口（无论该端口是否开启）的访问请求流量到源站服务器。因此，不会对源站服务带来任何安全风险和威胁。

WAF默认提供的端口列表，请参见各版本支持的端口。

13.Web应用防火墙流量访问示意图

本文介绍了Web应用防火墙的流量访问示意流程。

下图展示了Web应用防火墙的流量访问示意流程。



流程说明如下：

> **说明** Web应用防火墙的IP均在云上，即Web应用防火墙的VIP能够通过Banff查看流量。Web应用防火墙的VIP是一个LVS集群，您可以将Web应用防火墙的VIP理解为SLB的VIP，并在VNET上查到Web应用防火墙的VIP以及VIP后端的WAF Engine的IP地址。

1. Client请求访问Web应用防火墙的VIP地址。
2. Web应用防火墙的VIP将请求转发给LVS集群后方一台服务器（A）进行处理。
3. 服务器（A）将报文解析到7层，判断是否为恶意访问或者攻击。
   - 如果是正常访问，则转发给源站。
   - 如果是恶意访问，则阻断业务，直接将报文返回给Client并结束。

4. 源站收到转发的报文后进行处理，处理完成后将报文返回给服务器（A）。

   > **说明** 请注意步骤3和4中服务器（A）的角色变化。
   > - 对于Client而言，服务器（A）为服务端。
   > - 对于源站而言， 服务器（A）为客户端。

5. 服务器（A）将报文通过LVS的IP地址，返回给Client并结束。

14.CC攻击防护攻击紧急模式

当CC攻击防护的正常防护模式不能够帮助您拦截大流量且复杂的CC攻击时，您可以选择攻击紧急模式。

默认情况下，CC攻击的防护模式是正常模式，帮助您拦截常规的CC攻击。当您发现源站CPU飙升，数据库或者应用丢包时，您可以选用攻击紧急模式。

攻击紧急模式可能导致对正常请求的误拦截。建议您购买企业版或者旗舰版Web应用防火墙，并启用自定义CC防护。

15.405状态码问题排查及处置方法

问题描述

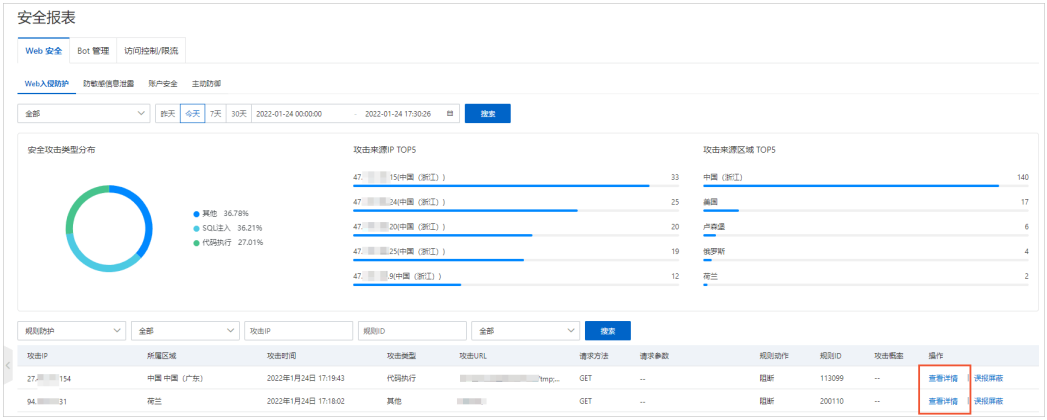
网站部署Web应用防火墙后，当用户访问有可能对网站造成安全威胁的URL时，会收到405报错，提示访问被WAF拦截。

解决方案

出现405拦截响应时，您可以使用以下方法获取攻击详情信息：

- 在Web应用防火墙控制台的**安全报表**页面，通过**Web安全 > Web入侵防护**报表，查看Web攻击的拦截记录，获取攻击详情信息。具体操作，请参见WAF安全报表。

> 注意　安全报表只支持查询规则防护引擎、深度学习引擎拦截的攻击详情。

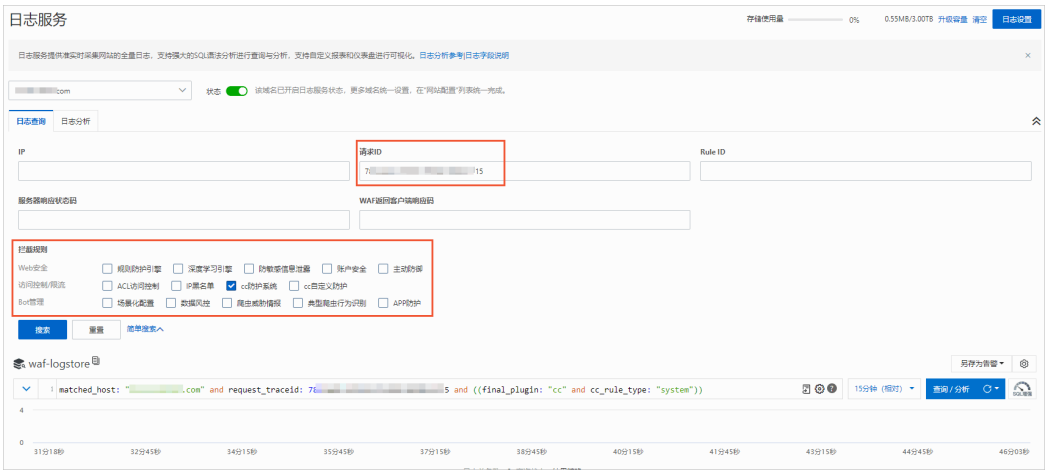


攻击详情信息示例如下图。

- 如果您已为域名开启日志采集，推荐您通过日志服务，查询攻击详情信息。日志服务支持查询所有防护模块的攻击拦截记录。

  您可以从WAF返回的拦截响应页面获取当前请求的ID，然后在Web应用防火墙控制台的**日志服务**页面，通过**日志查询**页签的快捷搜索功能，查询相关日志数据。具体操作，请参见日志查询。

  > **注意** WAF日志服务是付费功能，您必须先开通日志服务，并为域名开启日志采集，才可以查询域名的日志数据。更多信息，请参见步骤1：开通WAF日志服务、步骤2：开启日志采集。



获取并分析攻击详情后，如果您判断WAF拦截的访问是正常业务请求，您可以通过以下方法进行处理：

- 在**安全报表**页面，通过**Web安全 > Web入侵防护**报表的**误报屏蔽**功能，一键禁用触发误拦截的具体防护规则。

  具体操作，请参见Web安全报表说明。

  > **注意** **误报屏蔽**只适用于屏蔽WAF规则防护引擎内置的系统防护规则、深度学习引擎自动生成的防护规则。如果您通过攻击详情发现您自定义的防护规则对业务造成了误拦截（例如，您在自定义防护策略模块中添加的**ACL访问控制**、**CC攻击防护**规则），您需要手动删除对应规则。

- 在**网站防护**页面，手动为不同防护模块设置白名单规则，自定义在请求满足特定匹配条件（例如，访问指定URL）时，禁用指定的防护模块或防护规则。

  更多信息，请参见设置网站白名单。

16.非标端口业务无法接入Web应用防火墙高级版

问题描述

Web应用防火墙高级版仅支持接入HTTP 80、8080端口，或者HTTPS 443、8443端口的网站业务。如果您的后端业务使用了上述接口外的非标准端口，则在接入Web应用防火墙高级版时，业务接入会失败。

解决方案

- 企业版及以上规格的Web应用防火墙实例支持接入特定的非标准端口业务，详见WAF支持的端口。如果您的后端业务端口在WAF支持的端口范围内，则您可以升级Web应用防火墙高级版实例到企业版及以上规格。具体操作请参见升级。
- 针对Web应用防火墙不支持的业务端口，您可以部署负载均衡作为中间转发，网络架构为：WAF->SLB->ECS。

  使用负载均衡作为中间转发时，您可以在WAF上正常配置HTTPS业务， 端口默认为443； 负载均衡上配置HTTPS监听，前端端口为443，后端端口为业务端口。

  > **说明** 此架构要求您在WAF和SLB上均上传对应的HTTPS证书，否则无法回源。

17.上传HTTPS证书时提示“Https私钥格式错误”

问题描述

在Web应用防火墙上传HTTPS证书时提示“Https私钥格式错误”。

问题原因

证书的私钥可能被加密了。Web应用防火墙无法识别被加密的私钥。

解决方案

1. 查看私钥文件。如果私钥文件中包含如下图红框中标注的内容，则说明私钥被加密。

2. 执行以下命令并输入密码，解密私钥文件。

```
openssl rsa -in [$keyName] -text
#[$keyName]表示私钥文件名称。
```

如果返回结果如下图所示，则说明私钥解密成功。

3. 在Web应用防火墙重新上传解密后的私钥内容。

18.Web应用防火墙拦截上传文件的请求

本文介绍了业务接入Web应用防火墙后，上传文件请求被Web应用防火墙拦截的解决方法。

问题描述

在浏览器中调用POST方法上传文件时，会有一定的概率出现405错误，提示被Web应用防火墙拦截。

问题原因

因为POST方法上传文件时，文件本身的内容也会被转码放到POST请求的body中一起上传，并且同样会被Web应用防火墙检测到。当转码后的文件中出现一些关键字时，就会被Web应用防火墙误认为含有恶意代码，从而拦截。

解决方案

由于是文件转码后的误命中，暂时没有主动的解决办法，建议您将该地址加入精准访问控制的放行规则里。

19.登录状态丢失怎么解决？

本文介绍了业务接入Web应用防火墙（WAF）后，出现登录状态丢失问题的解决方法。

问题描述

部分网站在使用WAF后，可能会出现登录状态丢失，或其他和登录状态相关的异常。这些异常的主要原因有：

- 域名有多个源站（ECS），却没有做session同步，尤其是在WAF后面挂接了SLB的架构下。
- 没有从x-forwarded-for中获取真实IP进行校验。

解决方案

- 为服务器配置session同步。

  具体请参见[ASP.NET]Session在多个站点之间共享解决方案。
- 如果WAF后面挂接了SLB，可以用七层HTTP方式做转发，打开会话保持，并以cookie方式做会话保持。
- 从x-forwarded-for中获取访问者真实IP进行校验。

  具体请参见获取访问者真实IP。

20.长连接超时问题

本文介绍了在接入WAF的业务中，当客户端与服务器之间出现长连接超时响应问题的解决方法。

问题描述

在某些特定业务场景中，客户端在提交某个请求后，需要等待服务器处理超过60秒的时间才可以返回响应，并且在处理完毕之前服务器与客户端没有任何数据交互。

例如，您通过网页上传一个Excel表格，要求服务器处理其中的数据（处理时间约需3分钟），且在提交表格后120秒内，客户端与服务器之间没有任何数据交互（HTTP或者TCP报文）。这种情况下，WAF会返回一个504超时的响应给客户端，同时断开连接。

这是因为WAF默认不会维持超过120秒（没有任何数据交互）的长连接。

解决方案

- WAF独享集群支持自定义连接超时时间。如果您使用独享集群防护网站业务，则可以修改网站配置，根据业务需要，在120~3600秒范围内自定义读、写连接超时时长。更多信息，请参见设置独享集群。
- 如果您使用共享集群防护资源，则目前无法支持超过120秒的长连接。

21.Web应用防火墙：产品经理、安全专家“面对面”

尊敬的Web应用防火墙用户：

针对高级版、企业版、旗舰版用户，我们提供您与WAF产品经理、安全专家直接沟通的渠道。关于Web应用防火墙的问题，您可以直接向产品经理和安全专家咨询，并得到快速响应（响应时间：5*8 标准工作时间，其他时间建议优先选择工单）。同时，我们也期待收到您对产品的吐槽和建议。

您可以通过以下方式，和我们建立直达沟通：

1. 在手机或电脑上下载钉钉聊天软件，并注册账号。
2. 使用钉钉加入WAF紧急事件处理群聊（群号：21715946），与WAF产品经理和安全专家直接在线沟通。

22.云解析版本产品规格

云盾Web应用防火墙云解析版本的产品规格下表所示。

产品参数	具体描述	云解析版
HTTP	支持HTTP（80）端口	支持
HTTPS	支持HTTPS（443）端口	不支持
云外机房	支持网站在阿里云外	支持
Web应用基础防护	防护如SQL注入、命令执行等常见Web攻击	支持
0day漏洞补丁防御	快速防护最新Web漏洞	支持
服务可用性	防护服务部署的所在机房	单机房
Web防护规则定制	针对网站定制Web防护规则	不支持
CC防护规则定制	针对特定业务接口做专家定制规则防护	不支持
CC防护阈值	每秒的攻击请求数阈值	1,000
访问控制规则	精准防护规则条数	5（支持IP/URL）
防护域名个数	可防护的域名个数	2
日常QPS阈值	每秒的正常请求数阈值	100
带宽阈值	每秒的带宽阈值（Mbps）	10（源站在云外）200（源站在云内）
回源IP个数	同一个域名最多同时回源的IP	2
定制化需求	支持各种定制化需求	不支持

如该产品规格不满足您的需求，您可在控制台升级服务。点击查看产品版本信息。

23.常见Web漏洞释义

跨站攻击

漏洞描述

跨站脚本攻击（Cross-site scripting，简称XSS攻击），通常发生在客户端，可被用于进行隐私窃取、钓鱼欺骗、密码偷取、恶意代码传播等攻击行为。XSS攻击使用到的技术主要为HTML和JavaScript脚本，也包括VBScript和ActionScript脚本等。

恶意攻击者将对客户端有危害的代码放到服务器上作为一个网页内容，用户不经意打开此网页时，这些恶意代码会注入到用户的浏览器中并执行，从而使用户受到攻击。一般而言，利用跨站脚本攻击，攻击者可窃取会话cookie，从而获得用户的隐私信息，甚至包括密码等敏感信息。

漏洞危害

XSS攻击对Web服务器本身虽无直接危害，但是它借助网站进行传播，对网站用户进行攻击，窃取网站用户账号信息等，从而也会对网站产生较严重的危害。XSS攻击可导致以下危害：

- 钓鱼欺骗：最典型的就是利用目标网站的反射型跨站脚本漏洞将目标网站重定向到钓鱼网站，或者通过注入钓鱼JavaScript脚本以监控目标网站的表单输入，甚至攻击者基于DHTML技术发起更高级的钓鱼攻击。
- 网站挂马：跨站时，攻击者利用Iframe标签嵌入隐藏的恶意网站，将被攻击者定向到恶意网站上、或弹出恶意网站窗口等方式，进行挂马攻击。
- 身份盗用：Cookie是用户对于特定网站的身份验证标志，XSS攻击可以盗取用户的cookie，从而利用该cookie盗取用户对该网站的操作权限。如果一个网站管理员用户的cookie被窃取，将会对网站引发巨大的危害。
- 盗取网站用户信息：当窃取到用户cookie从而获取到用户身份时，攻击者可以盗取到用户对网站的操作权限，从而查看用户隐私信息。
- 垃圾信息发送：在社交网站社区中，利用XSS漏洞借用被攻击者的身份发送大量的垃圾信息给特定的目标群。
- 劫持用户Web行为：一些高级的XSS攻击甚至可以劫持用户的Web行为，从而监视用户的浏览历史、发送与接收的数据等等。
- XSS蠕虫：借助XSS蠕虫病毒还可以用来打广告、刷流量、挂马、恶作剧、破坏网上数据、实施DDoS攻击等。

CRLF攻击

漏洞描述

HTTP响应拆分漏洞，也叫CRLF注入攻击。CR、LF分别对应回车、换行字符。

HTTP头信息由很多被CRLF组合分离的行构成，每行的结构都是“键：值”。如果用户输入的值部分注入了CRLF字符，它有可能改变的HTTP报头结构。

漏洞危害

攻击者通过注入自定义HTTP头信息（例如，攻击者可以注入会话cookie或HTML代码），进行XSS攻击或会话固定漏洞攻击等。

SQL注入攻击

漏洞描述

SQL注入攻击（SQL Injection，简称注入攻击），被广泛用于非法获取网站控制权，是发生在应用程序的数据库层上的安全漏洞。

在设计不良的程序当中，忽略了对输入字符串中夹带的SQL指令进行检查，导致夹带的SQL指令被数据库误认为是正常的SQL指令而运行， 从而使数据库受到攻击，导致数据被窃取、更改、或删除，甚至进一步导致网站被嵌入恶意代码、被植入后门程序等危害。

漏洞危害

SQL注入攻击可导致以下危害：

- 机密数据被窃取。
- 核心业务数据被篡改。
- 网页被篡改。
- 数据库所在的服务器被攻击变成傀儡主机，甚至企业网被入侵。

写入WebShell攻击

漏洞描述

写入WebShell攻击，是指攻击者正在往网站服务器写入网页木马程序，企图控制服务器的攻击。

漏洞危害

攻击者在用户网站上写入一个Web木马后门，进而操作用户网站上的文件、执行命令等等。

本地文件包含

漏洞描述

本地文件包含是指程序代码在处理包含文件的时候没有严格控制，攻击者可以把上传的静态文件、或网站日志文件作为代码执行。

漏洞危害

攻击者利用该漏洞，在服务器上执行命令，进而获取到服务器权限，造成网站被恶意删除、用户和交易数据被篡改等一系列恶性后果。

远程文件包含

漏洞描述

远程文件包含是指程序代码在处理包含文件的时候没有严格控制，导致攻击者可以构造参数包含远程代码在服务器上执行。

漏洞危害

攻击者利用该漏洞，在服务器上执行命令，进而获取到服务器权限，造成网站被恶意删除、用户和交易数据被篡改等一系列恶性后果。

远程代码执行

漏洞描述

远程代码执行，也叫代码注入，是指由于服务端代码漏洞导致恶意用户输入的代码在服务端被执行的一种高危安全漏洞。

漏洞危害

攻击者利用该漏洞，可以在服务器上执行拼装的代码。

FastCGI攻击

漏洞描述

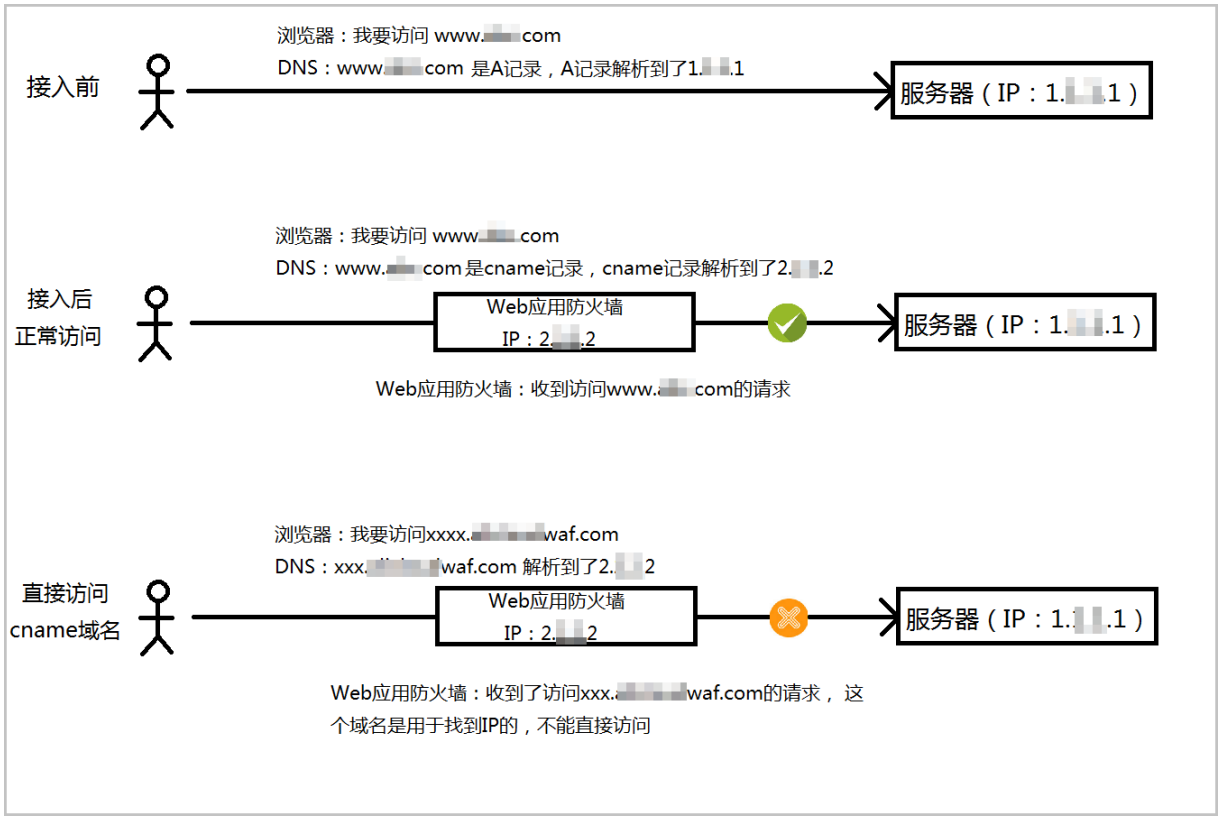
FastCGI攻击是Nginx中存在一个较为严重的安全漏洞。FastCGI模块默认情况下可能导致服务器错误地将任何类型的文件以PHP的方式进行解析。

漏洞危害

恶意的攻击者可能攻陷支持PHP的Nginx服务器。

24.为什么不能直接访问WAF生成的CNAME域名？

Web应用防火墙或高防IP生成的CNAME域名是用于DNS解析的，不能直接访问。



如果直接访问CNAME域名，可能显示504页面，或者本帮助页面。