Web 应用防火墙

故障排查

文档版本	01
发布日期	2024-07-11

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 网站接入异常排查

1.1 域名/IP 接入状态显示“未接入”，如何处理?

故障现象

添加防护域名或IP后，域名或IP接入WAF失败，即防护网站“接入状态”显示“未接入”。

须知

- WAF每隔一小时就会自动检测防护网站的 接入状态，当WAF统计防护网站在5分钟内达到20次访问请求时，将认定该防护网站已成功接入WAF。
- WAF默认只检测两周内新增或更新的域名的接入状态，如果域名创建时间在两周前，且最近两周内没有任何修改，您可以在“接入状态”栏，单击，手动刷新接入状态。

WAF支持云模式-CNAME接入、云模式-ELB接入和独享模式三种部署模式，各部署模式支持防护的对象说明如下：

- 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
- 云模式-ELB接入：域名或IP，华为云的Web业务
- 独享模式：域名或IP，华为云的Web业务

云模式排查思路和处理建议

防护网站的“部署模式”为“云模式”时，请参考**图1-1**和**表1-1**进行排查处理。

图 1-1 云模式排查思路

表 1-1 接入 WAF 失败问题处理

可能原因	处理建议
原因一：**域名“接入状态”未刷新**	在防护网站“接入状态”栏，单击刷新状态。
原因二：**访问流量未达到WAF统计要求** **须知** 防护网站接入WAF后，当WAF统计防护网站在5分钟内有20次请求时，将认定该防护网站已接入WAF。	1. 在1分钟内多次访问防护网站。 2. 在防护网站“接入状态”栏，单击刷新状态。

可能原因	处理建议
原因三：**域名参数配置错误**	**须知** WAF支持防护以下类型域名： • 一级域名，例如，example.com • 单域名/二级域名等子域名，例如，www.example.com • 泛域名，例如，*.example.com example.com与www.example.com是不同的域名，请确认“防护域名”配置正确。 请参照以下步骤确保域名参数配置正确。 1. 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”，进入命令提示符窗口。 2. 运行**ping** *域名在WAF对应的CNAME值*（例如ping e59e684e2278043ae98a5423aef8ee329.vip.huaweicloudwaf.com），获取WAF的IP。 3. 用文本编辑器打开hosts文件，hosts文件一般位于“C:\Windows\System32\drivers\etc\”路径下。 4. 在hosts文件添加记录：***防护域名 域名对应的WAF的IP***。 5. 修改hosts文件后保存，在命令提示符窗口中运行**ping** *防护域名*（例如ping www.example.com）。 如果回显信息中的IP地址为**2**中的WAFIP地址，说明域名参数配置正确。 如果域名参数配置错误，删除该域名后重新添加防护网站。
原因四：**未配置域名解析或代理回源地址**	确认接入WAF的网站是否使用高防、CDN、云加速等代理。 • 是：确保网站的“是否已使用代理”已配置为“四层代理”或“七层代理”。 – 将CDN等代理回源地址修改为WAF的“CNAME”。 – （可选）在DNS服务商处添加一条WAF的“子域名”和“TXT记录”。 • 否：到该域名的DNS服务商处，配置防护域名的别名解析。 详细操作请参见**域名接入WAF**。

可能原因	处理建议
原因五：**域名解析或代理回源地址配置错误**	请参照以下步骤验证域名的CNAME是否配置成功。 1. 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”，进入命令提示符窗口。 2. 执行**nslookup**命令，查询CNAME。如果回显信息的域名在WAF上的CNAME，则表示配置成功。 以域名www.example.com为例。 **nslookup** www.example.com 如果CNAME配置失败，请参见**域名接入WAF**重新修改DNS解析或代理服务的回源地址。

独享模式排查思路和处理建议

防护网站的“部署模式”为“独享模式”时，请参考**图1-2**和**表1-2**进行排查处理。

图 1-2 独享模式排查思路

表 1-2 独享模式接入 WAF 失败问题处理

可能原因	处理建议
原因一：**域名/IP“接入状态”未刷新**	在防护网站“接入状态”栏，单击刷新状态。
原因二：**访问流量未达到WAF统计要求** **须知** 防护网站接入WAF后，当WAF统计防护网站在5分钟内有20次请求时，将认定该防护网站已接入WAF。	1. 在1分钟内多次访问防护网站。 2. 在防护网站“接入状态”栏，单击刷新状态。

可能原因	处理建议
原因三：**域名/IP参数配置错误**	查看基本信息，检查域名/IP参数是否正确。 如果域名/IP配置错误，删除该域名/IP后重新添加防护网站。
原因四：**没有为独享模式实例配置负载均衡，配置的负载均衡未绑定弹性公网IP**	1. 为独享引擎实例配置负载均衡。 2. 为弹性负载均衡绑定弹性公网IP。
原因五：**独享模式实例负载均衡配置错误或负载均衡绑定弹性公网IP错误**	• 配置负载均衡后，当WAF独享引擎实例的“健康检查结果”为“正常”时，说明弹性负载均衡配置成功。健康检查异常的排查思路请参见健康检查异常。 • 为弹性负载均衡绑定弹性公网IP后，可以查看绑定的弹性公网IP，说明绑定成功。

云模式-ELB 接入排查思路和处理建议

防护网站的“部署模式”为“云模式-ELB接入”时，请参考图1-3和表1-3进行排查处理。

图 1-3 ELB 模式排查思路

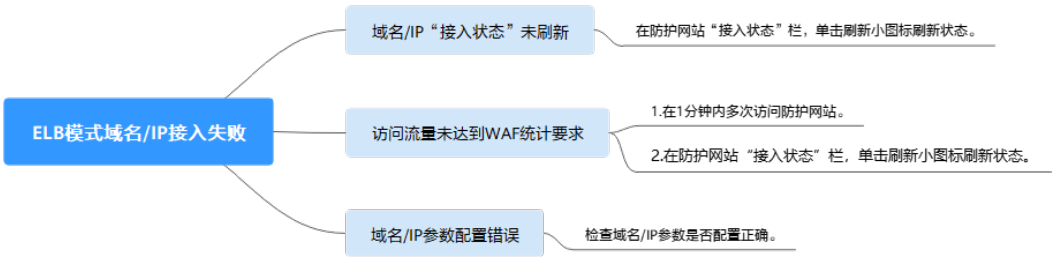


表 1-3 ELB 模式接入 WAF 失败问题处理

可能原因	处理建议
原因一：**域名/IP“接入状态”未刷新**	在防护网站“接入状态”栏，单击刷新状态。
原因二：**访问流量未达到WAF统计要求** **须知** 防护网站接入WAF后，当WAF统计防护网站在5分钟内有20次请求时，将认定该防护网站已接入WAF。	1. 在1分钟内多次访问防护网站。 2. 在防护网站“接入状态”栏，单击刷新状态。

可能原因	处理建议
原因三：**域名/IP参数配置错误**	**查看域名基本信息**，检查域名/IP参数是否正确。 如果域名/IP配置错误，删除该域名/IP后重新添加防护网站。

1.2 如何解决网站接入 WAF 后程序访问页面卡顿?

问题现象

网站接入WAF后程序访问页面卡顿。

可能的原因

一般是由于您在服务器后端配置了HTTP强制跳转HTTPS，在WAF上只配置了一条HTTPS（对外协议）到HTTP（源站协议）的转发，强制WAF将用户的请求进行跳转，所以造成死循环。

解决办法

请添加HTTP到HTTP和HTTPS到HTTPS这2条转发协议规则。具体操作如下：

步骤1 登录WAF控制台。

步骤2 在左侧导航栏中，选择“网站设置”，进入网站设置页面。

步骤3 在“源站服务器”栏中，单击“编辑”。

步骤4 在“修改服务器信息”页面，添加HTTP到HTTP和HTTPS到HTTPS这2条转发协议规则。

图 1-4 配置示例

----结束

有关配置转发规则的详细操作，请参见**如何解决重定向次数过多？**。

1.3 如何处理网站接入 WAF 后，文件不能上传?

将网站接入WAF后，网站的文件上传请求限制为10G 。

如果需要上传超过10G的文件、视频，建议不使用WAF防护的域名上传，可采用以下三种方式上传：

- 直接通过IP上传。
- 使用没有被WAF防护的域名上传。
- 采用FTP协议上传。

1.4 域名接入 WAF 后，漏扫工具为什么扫不到用户真实的业务?

将域名以云模式-CNAME方式接入WAF后，使用漏洞扫描工具扫描网站域名时，扫描不到网站的真实业务，只能扫描到WAF的IP。

解决方案

方案一：在WAF控制台，将工作模式切换为Bypass，具体操作请参见**切换工作模式**。

须知

Bypass后，该域名的请求直接到达其后端服务器，不再经过WAF，此时需要先放通源站业务的安全策略端口，才能保证模式切换后，业务运行正常。

方案二：将网站IP添加到漏洞扫描工具进行扫描。以漏洞管理服务为例，将网站IP添加到漏洞管理服务进行扫描。

2 证书/加密套件问题排查

2.1 如何解决证书链不完整?

如果证书机构提供的证书在用户平台内置信任库中查询不到，且证书链中没有颁发机构，则证明该证书是不完整的证书。使用不完整的证书，当用户访问防护域名对应的浏览器时，因不受信任而不能正常访问防护域名对应的浏览器。

按以下两种方法可解决此问题：

- 手动构造完整证书链，并上传证书。
- 重新上传正确的证书。

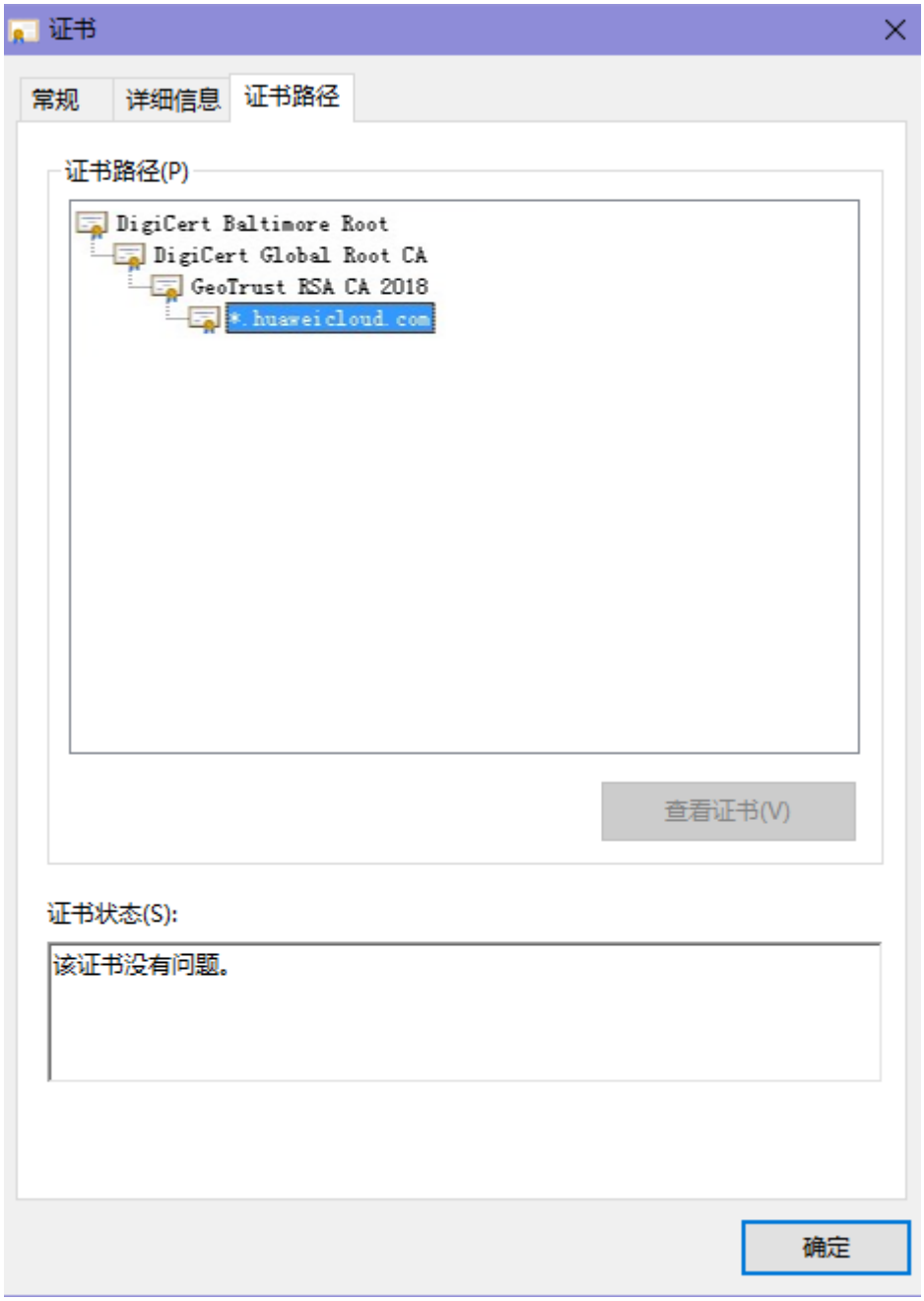
Chrome最新版本一般是支持自动验证信任链，以华为的证书为例，手工构造完整的证书链步骤如下：

步骤1 查看证书并导出证书。

1. 单击浏览器前的锁，可查看证书状况。
2. 在“连接是安全的”所在行，单击 ›，并单击“证书有效”。
3. 选择“详细信息”页签，在页面右下角单击“导出”，将证书导出到本地。

步骤2 查看证书链。在本地打开导出的证书，并选中“证书路径”页签，可单击证书名称查看证书状态，如图2-1所示。

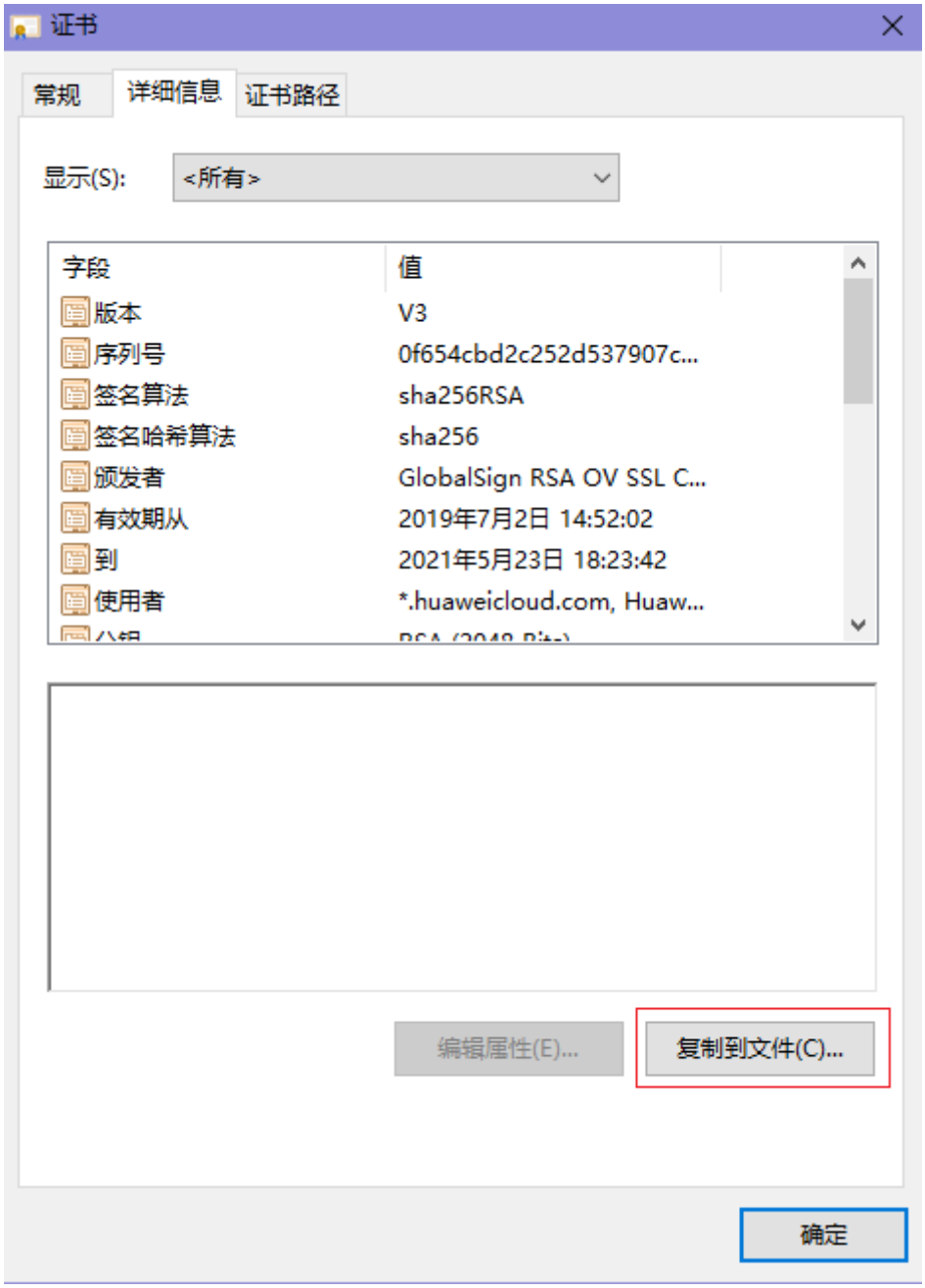
图 2-1 查看证书链



步骤3 逐一将证书另存到本地。

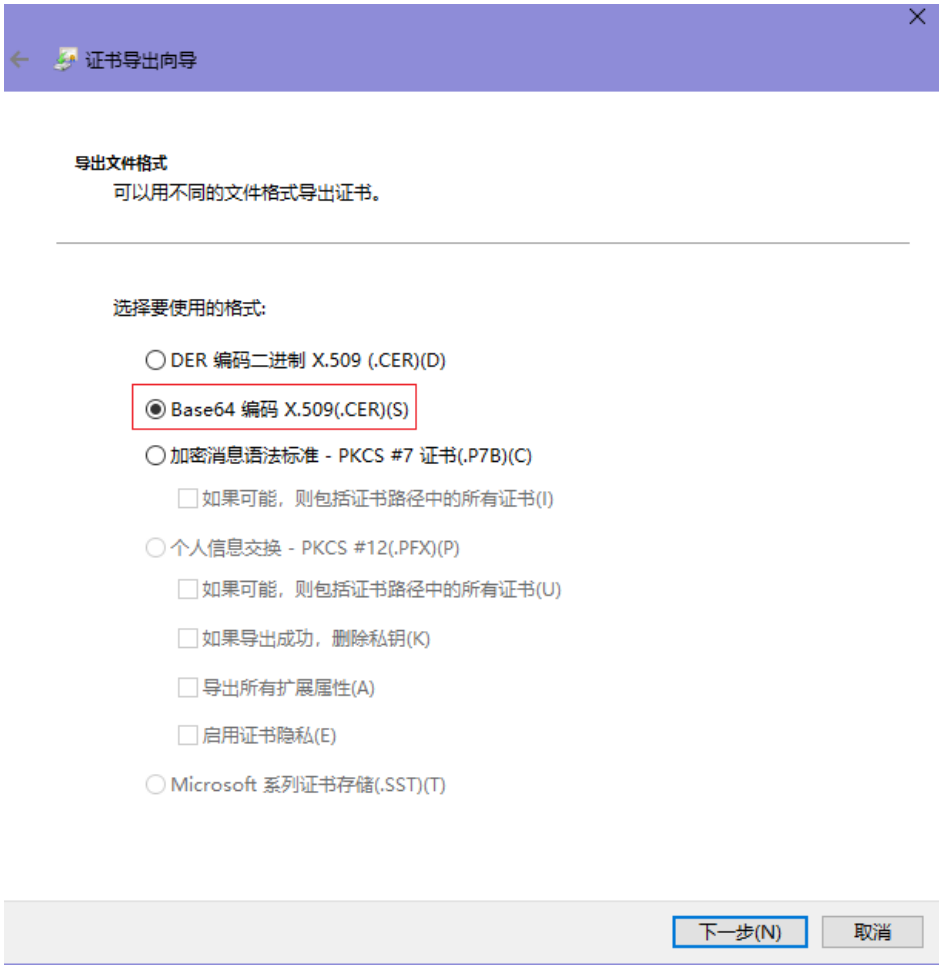
1. 选中证书名称，单击“详细信息”页签，如图2-2所示。

图 2-2 详细信息



2. 单击“复制到文件”，按照界面提示，单击“下一步”。
3. 选择“Base64编码”，单击“下一步”，如图2-3所示。

图 2-3 证书导出向导



步骤4 **证书重构**。证书全部导出到本地后，用记事本打开证书文件，按图2-4重组证书顺序，完成证书重构。

图 2-4 证书重构

步骤5 重新上传证书。

----结束

2.2 如何解决证书与密钥不匹配问题?

在DDos高防控制台、WAF控制台上传HTTPS证书后，收到证书和密钥不匹配的提示。

解决方案

可能的原因	修复建议

您上传的证书与私钥内容不匹配	1. 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`
	2. 判断证书和私钥文件的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。
	3. 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	1. 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>` 2. 重新上传私钥。

相关操作

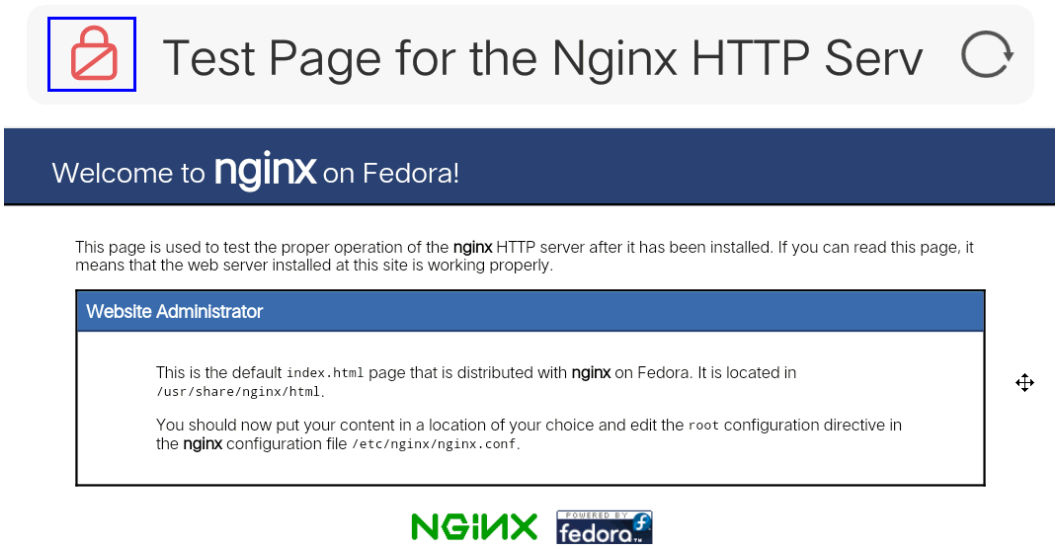
- **如何解决证书链不完整?**
- **如何解决HTTPS请求在部分手机访问异常?**

2.3 如何解决 HTTPS 请求在部分手机访问异常?

问题现象

打开手机浏览器，访问防护域名，如果出现类似如**图2-5**所示的页面，则表示该手机上HTTPS请求访问异常。

图 2-5 访问异常



原因

该问题是由于上传的证书链不完整，

解决办法

可参照**如何解决证书链不完整?** 解决。

2.4 如何处理“协议不受支持，客户端和服务器不支持一般 SSL 协议版本或加密套件”？

现象

域名接入WAF后，不能正常访问网站，提示“协议不受支持，客户端和服务器不支持一般 SSL 协议版本或加密套件”。

解决办法

建议您在TLS配置里，将“加密套件”切换为“默认加密套件”，具体操作请参见**配置PCI DSS/3DS合规与TLS**。

图 2-6 TLS 配置

2.5 如何解决“网站被检测到：SSL/TLS 存在 Bar Mitzvah Attack 漏洞”？

SSL/TLS 存在Bar Mitzvah Attack漏洞是由RC4加密算法中一个问题所导致的。该问题能够在某些情况下泄露SSL/TLS加密流量中的密文，从而将账户用户密码、信用卡数据和其他敏感信息泄露给黑客。

解决办法

建议您在TLS配置里，将“最低TLS版本”配置为“TLS v1.2”，“加密套件”配置为“加密套件2”，具体操作如请参见**配置PCI DSS/3DS合规与TLS**。

3 流量转发异常排查

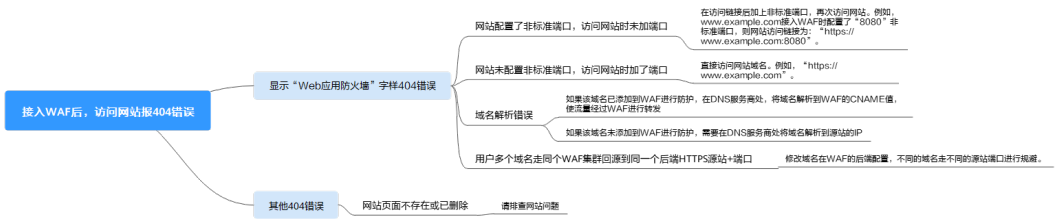
3.1 如何排查 404/502/504 错误?

网站接入WAF防护之后，如果您访问网站时出现404 Not Found、502 Bad Gateway，504 Gateway Timeout等错误，请参考以下方法解决。

404 Not Found 错误排查思路和处理建议

网站接入WAF后，访问网站时出现404 Not Found错误，请参考图3-1进行排查处理。

图 3-1 404 错误排查思路



- 如果访问网站返回如图3-2所示页面，原因和处理建议说明如下：

  图 3-2 404 页面

原因一：添加防护域名到WAF时，配置了非标准端口，例如配置了如图3-3所示的非标准端口业务，访问网站时未加端口用“https://www.example.com”或者“https://www.example.com:80”访问网站。

图 3-3 非标准端口配置

处理建议：在访问链接后加上非标准端口，再次访问源站，如“https://www.example.com:8080”。

原因二：添加防护域名到WAF时，没有配置非标准端口，访问时使用了非标准端口或者“源站端口”配置的非标准端口，例如配置了如图3-4所示的防护业务，用“http://www.example.com:8080”访问网站。

图 3-4 未配置非标准端口

说明

没有配置非标准端口的情况下，WAF默认防护80/443端口的业务。其他端口的业务不能正常访问，如果您需要防护其他非标准端口的业务，请重新进行域名配置。

处理建议：直接访问网站域名，如“https://www.example.com”。

原因三：域名解析错误。

处理建议：

- 如果该域名已添加到WAF进行防护，参照**域名解析**重新完成域名接入的操作，使流量经过WAF进行转发。
- 如果该域名未添加到WAF进行防护，需要在DNS服务商处将域名解析到源站的IP。

原因四：用户多个域名走同个WAF集群回源到同一个后端HTTPS源站+端口，由于WAF回源是长连接复用的，后端源站节点无法分辨是哪个域名（nginx通过Host和SNI分辨），会有一定几率出现A域名的请求转发到B域名的后端，所以会出现404。

处理建议：修改域名在WAF的后端配置，不同的域名走不同的源站端口进行规避。

- 如果访问网站时，返回的不是图3-2所示的404页面，原因和处理建议说明如下：
  原因：网站页面不存在或已删除。
  处理建议：请排查网站问题。

502 Bad Gateway 错误排查思路和处理建议

完成WAF配置之后网站访问正常，但过一段时间，访问页面返回502，或者大概率出现502，请参考图3-5进行排查处理。

图 3-5 502 错误排查思路

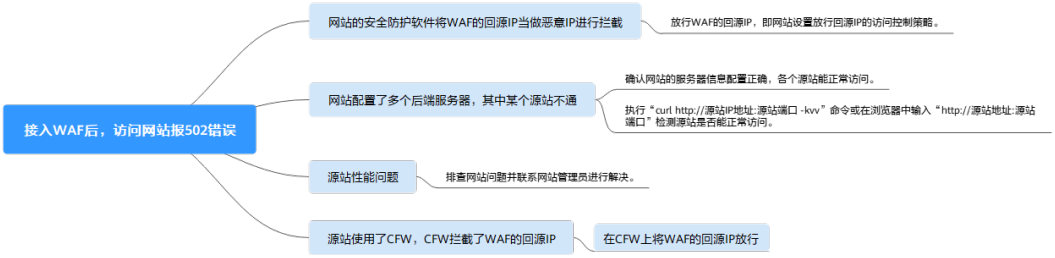


表 3-1 502 错误问题处理

可能原因	处理建议
原因一：**网站使用了其他的安全防护软件（如360、安全狗、云锁或云盾等安全防护软件），这些软件把WAF的回源IP当成了恶意IP，拦截了WAF转发的请求**	源站服务器配置放行WAF回源IP的访问控制策略。 ● 云模式：请参见**如何放行云模式WAF的回源IP段？**。 ● 独享模式：请参见**放行独享引擎回源IP**。
原因二：**网站的后端配置了多个服务器，其中某个源站不通**	请参照**步骤1~步骤8**，确保所有源站都可以正常访问。
原因三：**网站服务器性能问题**	排查网站问题并联系您的网站管理员进行解决。
原因四：**源站使用了CFW，CFW拦截了WAF的回源ip**	该问题有以下排查方法： ● 如果源站使用了CFW，在CFW的控制台查看拦截日志，排查是否有相关的事件产生。 ● 查看CFW的访问控制策略，排查是否配置了拦截WAF的回源IP 在CFW上将WAF的回源IP放行，具体操作请参见**配置访问控制策略**

当**网站的后端配置了多个服务器，其中某个源站不通**时，请参照以下操作步骤，检查网站的服务器是否配置正确。

须知

修改服务器信息，大约需要2分钟同步生效。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

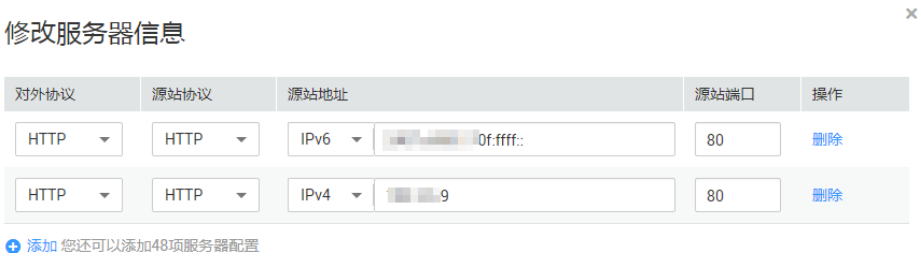
步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行中，单击目标域名，进入域名基本信息页面。

步骤6 在“源站服务器”栏中，单击编辑，进入“修改服务器信息”页面，确保对外协议、源站协议、源站地址、端口等信息配置正确。

图 3-6 服务器配置



步骤7 检测各个源站是否能正常访问。

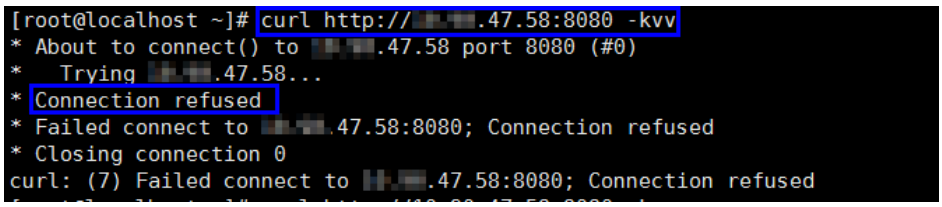
- 在主机上执行以下命令进行检测。

```
curl http://xx.xx.xx.xx:yy -kvv
```

说明

- xx.xx.xx.xx代表源站服务器的源站IP地址，yy代表源站服务器的源站端口，xx.xx.xx.xx和yy必须是同一个服务器的源站地址和端口。
- 执行curl命令的主机需要满足以下条件：
  - 网络通信正常。
  - 已安装curl命令。Windows操作系统的主机需要手动安装curl，其他操作系统自带curl。

图 3-7 检测源站



  - 如果回显信息提示连接正常表示可以正常访问网站。
  - 如果回显信息提示“connection refused”表示源站不通，不能正常访问网站，请执行步骤8。

- 在浏览器中输入“http://*源站地址*:*源站端口*”进行检测。
  - 如果可以访问，表示网站访问正常。
  - 如果不能访问，表示源站不通，不能正常访问网站，请执行步骤8。

步骤8 检测服务器是否运行正常。

如果运行不正常，请尝试重启服务器。

----结束

504 Gateway Timeout 错误排查思路和处理建议

完成WAF域名接入配置之后，业务正常，但当业务量增加时，发生504错误的概率增加，直接访问源站IP也有一定概率出现504错误，请参考图3-8进行排查处理。

图 3-8 504 错误排查思路

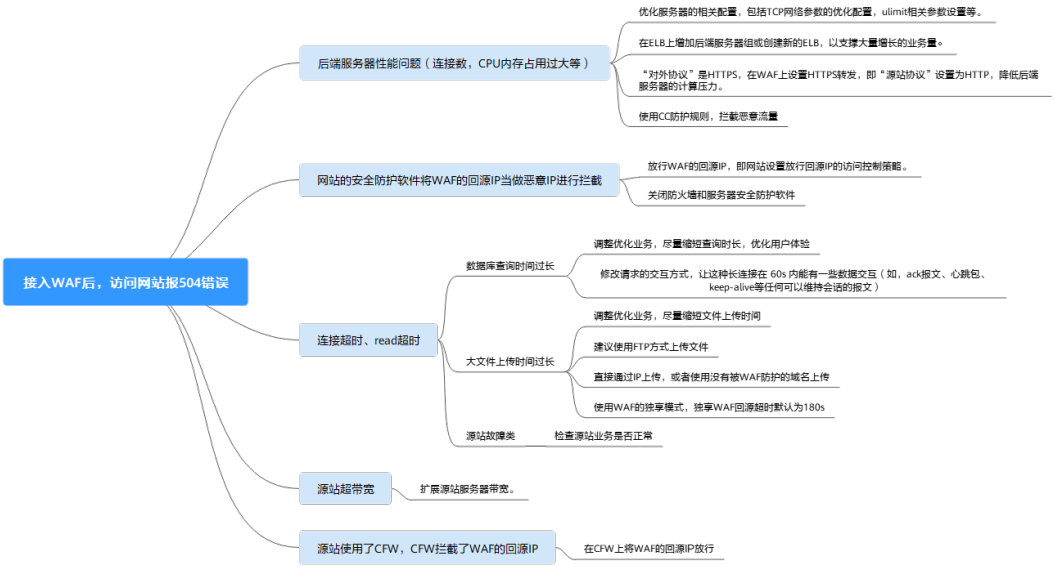


表 3-2 504 错误问题处理

可能原因	排查方法	处理建议
原因一：**后端服务器性能问题（连接数，CPU内存占用过大等）**	源站性能问题，可以排查源站访问日志以及访问流量情况，定性分析。	• 优化服务器的相关配置，包括TCP网络参数的优化配置，ulimit相关参数设置等。 • 如果是云模式部署方式，如果使用了ELB负载均衡，建议在ELB上增加后端服务器组或创建新的ELB，支撑大量增长的业务量。 – 增加后端服务器组的详细操作，请参见**添加或移除后端服务器（共享型）**。 – 配置新ELB的操作，请参考**步骤1~步骤8**。 • 如果“对外协议”是HTTPS，建议在WAF设置HTTPS转发，回源走HTTP协议即“源站协议”设置为HTTP，降低后端服务器的计算压力。 如果有重定向问题，建议参照**如何解决重定向次数过多？**解决。 修改服务器信息的详细操作，请参见**修改服务器信息**。 • 使用CC防护规则，拦截恶意流量。
原因二： • **安全组未将WAF回源IP设置为白名单或未放开端口** • **源站有防火墙设备，且该防火墙设备拦截了WAF的回源IP**	建议采用以下方法进行排查： • 排查客户源站是否有安全组，防火墙，服务器安全软件等。 • 在客户端与WAF上同时进行抓包分析，排查源站防火墙等设备对WAF的长连接是否有主动丢包的现象。	• 源站服务器配置放行WAF回源IP的访问控制策略。 – 云模式：请参见**如何放行云模式WAF的回源IP段？**。 – 独享模式：请参见**放行独享引擎回源IP**。 • 建议您关闭防火墙和服务器安全防护软件。

可能原因	排查方法	处理建议
原因三：**连接超时、read超时** **说明** • 源站响应时间过长导致504（数据库查询时间过长，大文件上传时间过长，源站故障等）。 • WAF回源到客户源站超时时间大多为60秒或180秒，如果超时则会报错504。	该问题有以下排查方法： • 绕过WAF，直接访问客户源站，查看响应时长 • 查看全量日志里面访问日志源站响应时长 • 建议客户绕过WAF测试上传功能，并检查客户上传文件大小	• 数据库查询时间过长： – 调整优化业务，尽量缩短查询时长，优化用户体验。 – 修改请求的交互方式，让这种长连接在 60s 内能有一些数据交互（如，ack报文、心跳包、keep-alive等任何可以维持会话的报文）。 • 大文件上传时间过长： – 调整优化业务，尽量缩短文件上传时间。 – 建议使用FTP方式上传文件。 – 直接通过IP上传，或者使用没有被WAF防护的域名上传。 – 使用WAF的独享模式，独享WAF回源超时默认为120s。 • 源站故障类： 检查源站业务是否正常。
原因四：**源站带宽不足，访问流量过大，带宽超限制**	该问题有以下排查方法： • 如果客户配置的WAF后端为7层ELB，则可以在ELB上查504相关日志 • 如果客户配置的WAF后端为4层ELB，则可以在ELB上查“Traffic exceeded the bandwidth threshold”相关字段日志 • 如果客户配置的WAF后端为EIP，则在504高峰查看EIP流量监控。	扩展源站服务器带宽。

可能原因	排查方法	处理建议
原因五：**源站使用了CFW，CFW拦截了WAF的回源ip**	该问题有以下排查方法： • 如果源站使用了CFW，在CFW的控制台查看拦截日志，排查是否有相关的事件产生。 • 查看CFW的访问控制策略，排查是否配置了拦截WAF的回源IP	在CFW上将WAF的回源IP放行，具体操作请参见**配置访问控制策略**

创建新的ELB，参照以下方法将ELB的EIP作为服务器的IP地址，接入WAF。

须知

修改服务器信息，大约需要2分钟同步生效。

步骤1 **创建共享型负载均衡器**。

步骤2 **登录管理控制台**。

步骤3 单击页面左上方的 ☰，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“域名”列中，单击目标域名，进入域名基本信息页面。

步骤6 在“源站服务器”栏中，单击编辑，进入“修改服务器信息”页面，单击“添加”，新增后端服务器。

图 3-9 服务器配置

步骤7 将“源站地址”设置为ELB的弹性公网IP地址。

步骤8 单击“确定”，服务器信息修改成功。

----结束

3.2 如何处理 418 错误码问题?

如果请求本身含有恶意负载被WAF拦截，此时访问WAF防护的域名时会出现418的错误。您可以通过查看WAF的防护日志，查看拦截原因。有关查看防护日志的详细操作，请参见**查看防护日志**。

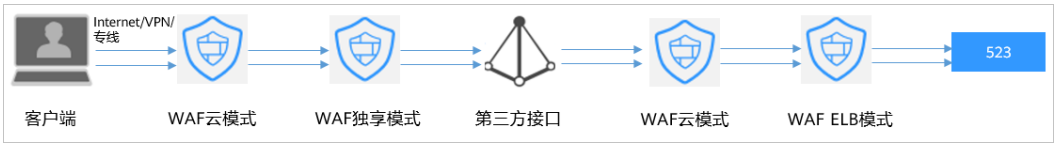
- 如果您判断该请求为业务正常请求调用，可以通过误报处理操作对该路径的对应规则进行放行处理，避免同样问题再次发生。

  有关处理误报事件的详细操作，请参见**处理误报事件**。
- 如果确认有问题，说明您的网站受到了攻击，并被WAF拦截。

3.3 如何处理 523 错误码问题?

523错误码是由于同一个访问请求四次经过了WAF引起，为了避免出现死循环现象，WAF会拦截该请求。如果您在访问网站时出现了523错误码问题，请先梳理流量图，查出流量串接多个华为云WAF的原因。

可能导致523错误码的示例流量图如下：



原因一：将同一个网站接入 WAF 4 次以上

通过WAF的各种模式（云模式-CNAME接入、云模式-ELB接入、独享模式），将同一个网站接入WAF 4次以上。

解决办法：

梳理流量图，将用户流量绕过多余WAF，具体操作如下：

步骤1 登录WAF管理控制台。

步骤2 在左侧导航树中，选择“网站设置”，进入网站设置列表。

步骤3 找到出现523问题的防护网站，保留一个配置，删除多余的防护网站，具体操作请参见**删除防护网站**。

防止删除网站后造成业务中断，在删除网站前，需要完成以下操作：

云模式：请您先到DNS服务商处将域名重新解析，指向源站服务器IP地址，否则该域名的流量将无法切回服务器，影响正常访问。

独享模式：修改ELB的后端服务器组，不再接入WAF实例节点，具体操作请参见**更换后端服务器组**。

----结束

原因二：调用了第三方接口且第三方接口也使用了华为云 WAF

将用户的请求在转发给第三方接口时仅修改了host，而header、cookie执行了原样转发，导致保留了WAF原有的计数器。

解决办法：

修改反向代理请求中的header字段，具体操作如下：

须知

用户的流量链路上，在WAF后如果有NGINX，才可用此方法。

步骤1 通过使用“proxy_set_header”来重定义发往代理服务器的请求头，执行以下命令打开nginx配置文件。

以Nginx安装在“/opt/nginx/”目录为例，具体情况需要依据实际目录调整。

vi /opt/nginx/conf/nginx.conf

步骤2 在nginx配置文件中加入**proxy_set_header X-CloudWAF-Traffic-Tag 0;**，示例如下：

```
location  ^~/test/ {
    ......
    proxy_set_header Host       $proxy_host;
    proxy_set_header X-CloudWAF-Traffic-Tag 0;
    ......
    proxy_pass http://x.x.x.x;
}
```

----结束

原因三：源站 IP 误配置为 WAF 的回源 IP 或 WAF 前代理的 IP

如果“源站地址”误配置为WAF的回源IP或WAF前代理的IP，会造成访问死循环，报523错误。

解决办法：

检测源站服务器的配置，将“源站地址”修改为正确的源站IP，具体操作请参见**修改服务器配置信息**。

图 3-10 修改源站地址

3.4 如何解决重定向次数过多？

在WAF中完成了域名接入后，请求访问目标域名时，如果提示“重定向次数过多”，一般是由于您在服务器后端配置了HTTP强制跳转HTTPS，在WAF上只配置了一条HTTPS（对外协议）到HTTP（源站协议）的转发，强制WAF将用户的请求进行跳转，所以造成死循环。

可在WAF中**修改服务器信息**，配置两条HTTP（对外协议）到HTTP（源站协议）和HTTPS（对外协议）到HTTPS（源站协议）的服务器信息。配置完成后，服务器信息如**图3-11**所示。

图 3-11 配置示例

3.5 如何处理接入 WAF 后报错 414 Request-URI Too Large?

故障现象

防护网站接入WAF后，用户不能正常访问网站，提示“414 Request-URI Too Large”错误，如**图3-12**所示。

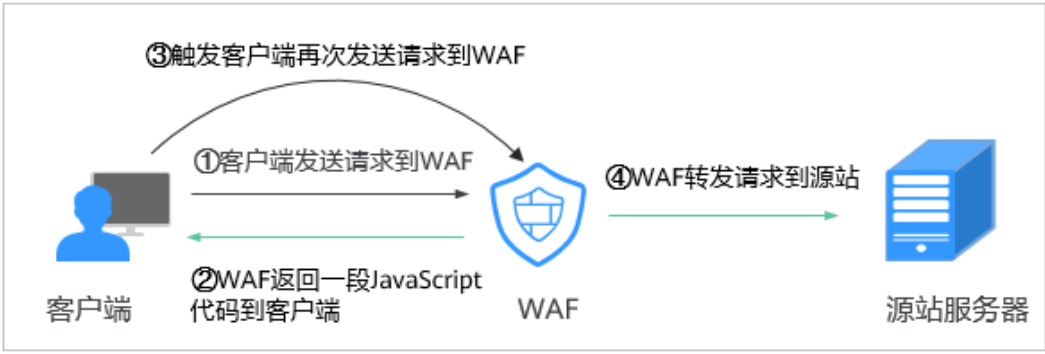
图 3-12 提示“414 Request-URI Too Large”错误

可能原因

防护网站开启了“JS脚本反爬虫”，由于用户的客户端浏览器没有JavaScript解析能力，客户端会缓存包含WAF返回JavaScript代码的页面，而用户每次访问防护网站时都会访问该缓存页面，WAF由此判定用户访问请求为非法的浏览器或爬虫工具，访问请求验证一直失败，造成无限循环，最终导致URI长度超出浏览器限制，访问网站失败。

开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成JS验证，并将该请求转发给源站，如**图3-13**所示。

图 3-13 JS 脚本反爬虫正常检测流程



- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求到WAF，即WAF无法完成js验证。
- 如果客户端爬虫伪造了WAF的认证请求，发送到WAF时，WAF将拦截该请求，js验证失败。

处理建议

当客户端的浏览器没有JavaScript解析能力时，请参照以下操作步骤关闭JS脚本反爬虫。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“网站反爬虫”配置框，用户可根据自己的需要开启或关闭网站反爬虫策略。

- ：开启状态。
- ：关闭状态。

步骤7 选择“JS脚本反爬虫”页签，关闭JS脚本反爬虫，即JS脚本反爬虫的“状态”为，如图3-14所示。

图 3-14 关闭 JS 脚本反爬虫

----结束

3.6 如何解决“源站服务器 CPU 使用率高达 100%”问题?

问题现象

网站遭受攻击，网站已接入WAF，但防护没起作用，源站服务器CPU使用率高达100%，怎么办?

可能原因

网站可能遭受了CC攻击。

当发现网站处理速度下降，网络带宽占用过高时，很有可能已经遭受CC攻击，此时可查看Web服务器的访问日志或网络连接数量，如果访问日志或网络连接数量显著增加，则可确定遭受CC攻击。

解决办法

步骤1 确认WAF的防护策略的配置规则都开启了拦截模式。

步骤2 配置一条“路径”包含“/”的CC策略对网站的全路径进行防护，限速频率设置严格一些，观察请求流量，确认攻击是否缓减，并根据防护效果调整策略，配置如图3-15所示。

图 3-15 全路径防护

步骤3 查看防护日志，对于攻击量大的IP，把IP加入黑名单，进行立即拦截。黑名单的配置请参见**配置IP黑白名单规则**。

----结束

3.7 连接超时时长是多少，是否可以手动设置该时长?

- 浏览器到WAF引擎的连接超时时长默认是120秒，该值取决于浏览器的配置，该值在WAF界面不可以手动设置。
- WAF到客户源站的连接超时时长默认为30秒，该值可以在WAF界面手动设置，但仅“独享模式”和“云模式”的专业版、铂金版支持手动设置连接超时时长。

  在域名的基本信息页面，开启“超时配置”并单击，设置“连接超时”、“读超时”、“写超时”的时间，并单击 保存设置。

4 误拦截正常请求排查

4.1 WAF 误拦截了正常访问请求，如何处理?

当WAF根据您配置的防护规则检测到符合规则的恶意攻击时，会按照规则中的防护动作（仅记录、拦截等），在“防护事件”页面中记录检测到的攻击事件。

须知

如果您已开通企业项目，请务必在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能处理该企业项目下的误报事件。有关企业项目的详细介绍，请参见**管理项目和企业项目**。

在误拦截事件所在行的“操作”列中，单击“详情”，查看事件详细信息。如果确认该防护事件为误报事件时，您可以参照**表4-1**对该事件进行误报处理。处理后，WAF将不再拦截该事件，即“防护事件”页面中将不再显示该攻击事件，您也不会收到该攻击事件的告警通知。

表 4-1 误报处理说明

命中规则类型	命中规则	处理方式
WAF内置防护规则	• Web基础防护规则 防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击，以及Webshell检测、深度反逃逸检测等Web基础防护。 • 网站反爬虫的“特征反爬虫”规则 可防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫。	在该攻击事件所在行的“操作”列，单击“误报处理”，详细操作请参见**处理误报事件**。

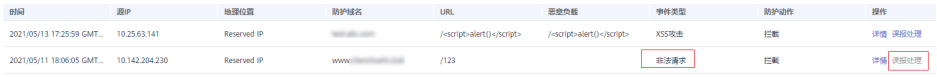
命中规则类型	命中规则	处理方式
自定义防护规则	• CC攻击防护规则 • 精准访问防护规则 • 黑白名单规则 • 地理位置访问控制规则 • 网页防篡改规则 • 网站反爬虫的“JS脚本反爬虫”规则 • 防敏感信息泄露规则 • 隐私屏蔽规则	在拦截该攻击事件的防护规则页面，删除对应的防护规则。
其他	“非法请求”访问请求 **说明** 当遇到以下情况时，WAF将判定该访问请求为非法请求并拦截该访问请求： • POST/PUT使用“form-data”时，表单的参数个数多于8192个。 • URL的参数个数多于2048个。 • Header个数超过512个。	“误报处理”按钮置灰不能使用，请参见**配置精准访问防护规则**放行该访问请求。

4.2 WAF 误拦截了“非法请求”访问请求，如何处理?

问题现象

防护网站接入WAF后，访问请求被WAF拦截，在“防护事件”页面查看防护日志，显示访问请求为“非法请求”且误报处理按钮置灰不能使用，如**图4-1**所示。

图 4-1 非法请求被 WAF 拦截



可能原因

当遇到以下情况时，WAF将判定该访问请求为非法请求并拦截该访问请求：

- POST/PUT使用“form-data”时，表单的参数个数多于8192个。
- URL的参数个数多于2048个。
- Header个数超过512个。

处理建议

当确认访问请求为正常请求时，请通过**配置精准访问防护规则**放行该访问请求。

4.3 为什么误报处理不能使用了?

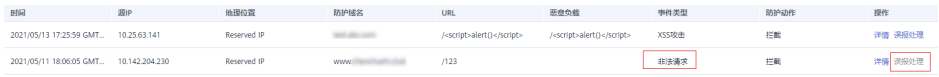
误报处理不能使用时，请先确认登录管理控制台账号是否授予了使用WAF的权限，有关WAF权限的详细介绍，请参见**WAF权限管理**。

须知

如果您已开通企业项目，处理误报事件时请在“企业项目”下拉列表中选择您所在的企业项目。

- 基于自定义规则（CC攻击防护规则、精准访问防护规则、黑白名单规则、地理位置访问控制规则等）拦截或记录的攻击事件，无法执行“误报处理”操作，如果您确认该攻击事件为误报，可在自定义规则页面，将该攻击事件对应的防护规则删除或关闭。
- 防护网站接入WAF后，当WAF检测到访问请求的以下参数超过512个时，WAF将判定该访问请求为非法请求并拦截该访问请求，且误报处理按钮置灰不能使用：
  - POST/PUT使用“form-data”时，表单的参数个数多于8192个。
  - URL的参数个数多于2048个。
  - Header个数超过512个。

图 4-2 非法请求被 WAF 拦截



有关非法请求的处理建议，请参见**WAF误拦截了“非法请求”访问请求，如何处理?** 。

5 权限异常排查

5.1 访问独享引擎页面时提示“IAM 未授权”？

问题现象

当访问“系统管理”下的“独享引擎”页面时，提示“调用IAM失败，请检查当前用户是否具有IAM权限”时。

可能的原因

登录账号未授予“IAM ReadOnly”权限。

处理办法

为您的账号授予“IAM ReadOnly”权限，具体的操作方法请参见**给IAM用户授权**。

⚠ 注意

为用户组授权时，设置最小授权范围，必须选择“所有资源”，才能授权生效。

5.2 添加防护域名时，为什么无法选择 SCM 证书?

现象

在WAF中添加防护域名时，在证书下拉框中选择SCM证书时，提示“用户角色无权限访问该接口 scm cert download”。

原因

该用户使用的账号没有“SCM Administrator”和“SCM FullAccess”这两个权限。

解决办法

在IAM中授予该账号“SCM Administrator”和“SCM FullAccess”权限，即可在添加防护域名时选择同一账号下的SCM证书。

