Alibaba Cloud Web Application Firewall

Best Practices

Issue: 20190404

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Web vulnerability protection suggestion

1.1 Jenkins arbitrary file read vulnerability (CVE-2018-1999002)

On July 18, 2018, Jenkins released the latest security advisory and announced multiple vulnerabilities. SECURITY-914 is an arbitrary file read vulnerability reported by *Orange*.

Attackers can exploit this vulnerability to read any file on a Window server and under specific conditions, read files on a Linux server. Attackers can also obtain credential information in Jenkins systems and therefore expose sensitive user information. Some credentials may be user passwords, which enable the attackers to log on to Jenkins systems and execute commands.

CVE number

CVE-2018-1999002

Vulnerability name

Jenkins arbitrary file read

Description

The Stapler Web framework used by Jenkins contains an arbitrary file read vulnerability. Unauthenticated attackers can send crafted HTTP requests to read the contents of any file on the Jenkins master file system that the Jenkins master process has access to.

For more information about this vulnerability, see *Jenkins security advisory*.

Affected versions

- Jenkins weekly 2.132 and earlier versions
- Jenkins LTS 2.121.1 and earlier versions

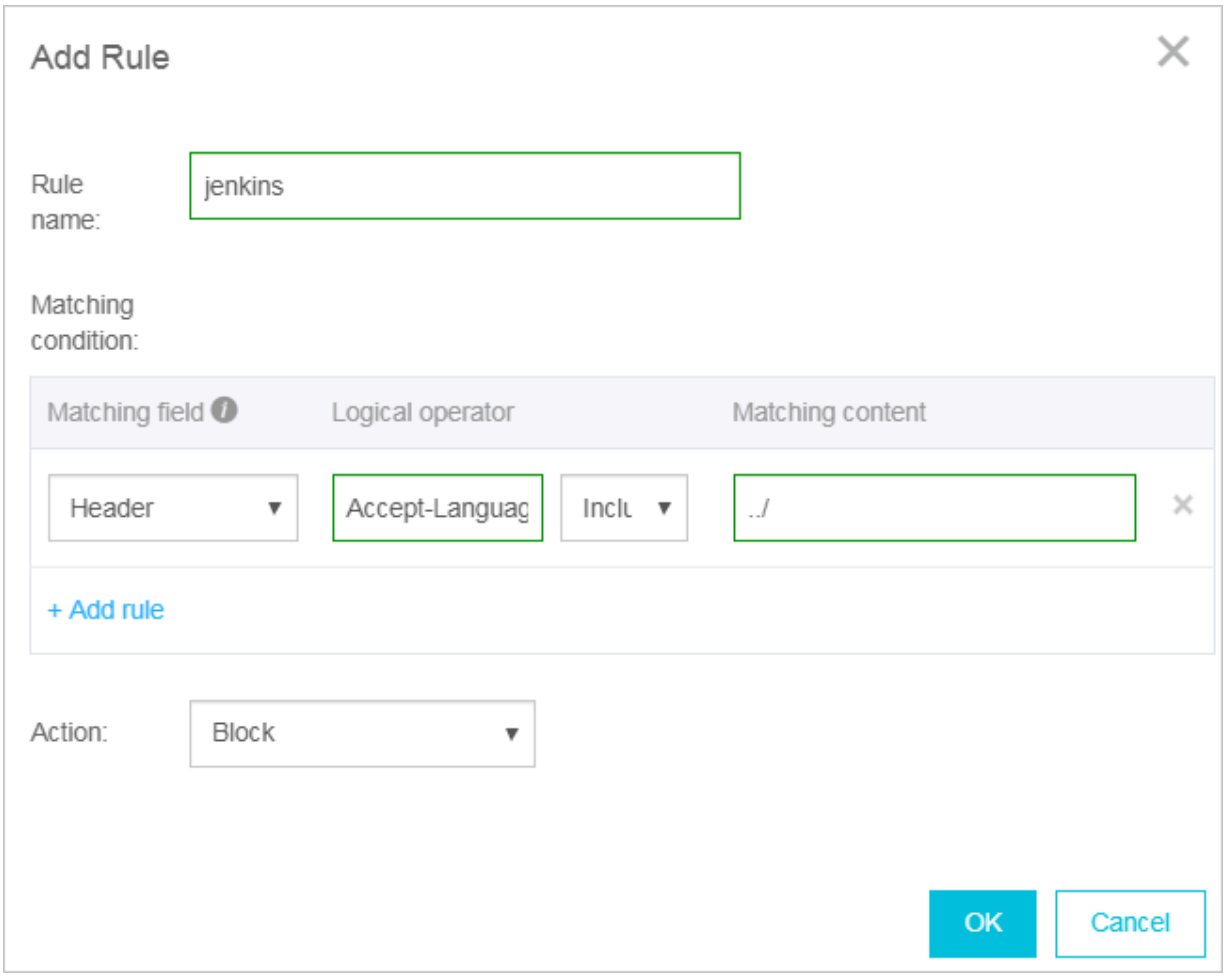
Fix

- Upgrade Jenkins weekly to version 2.133.
- Upgrade Jenkins LTS to 2.121.2.

Protection tips

If you do not want to upgrade Jenkins to resolve this vulnerability, we recommend that you use the HTTP ACL Policy feature provided by WAF to protect your business.

You can create a rule to block requests whose header field Accept-Language contains `../`. This prevents attackers from launching directory traversal attacks to read arbitrary files on your servers.



Result

Based on the access control rule, WAF blocks the request that attempts to exploit the vulnerability.

Note:
For more information about access control rules, see *Precise access control*.

1.2 Apache Struts2 REST plug-in DoS vulnerability (CVE-2018-1327)

Security experts Yevgeniy Grushka and Alvaro Munoz from HPE discovered a DoS vulnerability in the Apache Strust2 REST plug-in. The Strust REST plug-in uses the XStream library, which is vulnerable to DoS attacks launched through malicious XML requests.

CVE number

CVE-2018-1327

Vulnerability name

Apache Struts2 REST plug-in DoS vulnerability (S2-056)

Description

The S2-056 vulnerability exists in the Apache Struts2 REST plug-in. When you use the XStream handler to deserialize XML data without proper input validation, attackers can submit malicious XML data to launch DoS attacks on your application.

When malicious attackers flood your server with superfluous requests, your CPU resources can be exhausted rapidly.

For more information about this vulnerability, see the *official security bulletins*.

Affected versions

Struts 2.1.1 to Struts 2.5.14.1.

Fix

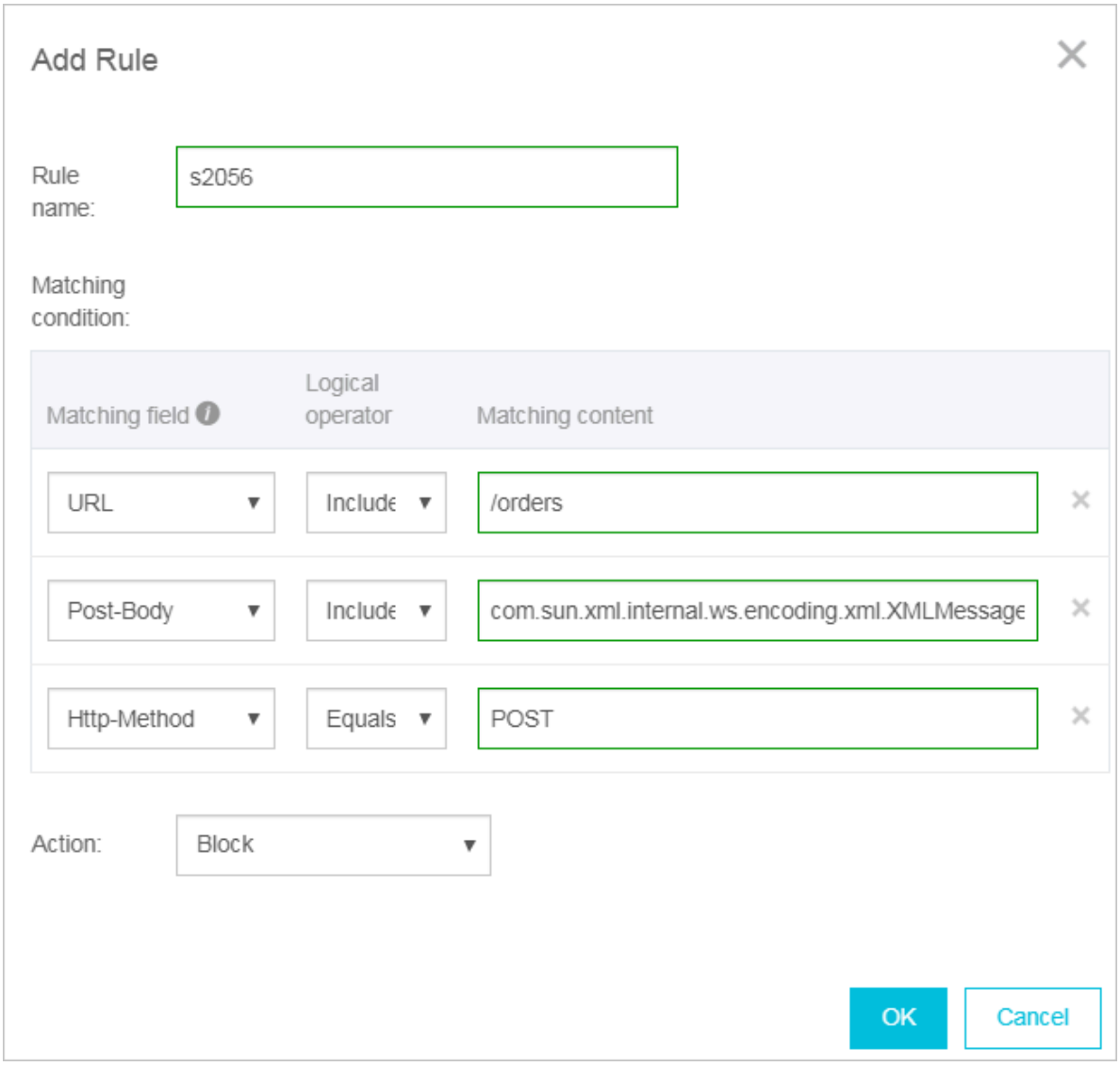
Upgrade to Apache Struts version 2.5.16.

Protection tips

If you do not want to upgrade Apache Struts to resolve this vulnerability, we recommend that you use HTTP ACL policies and custom HTTP flood protection provided by WAF to protect your business.

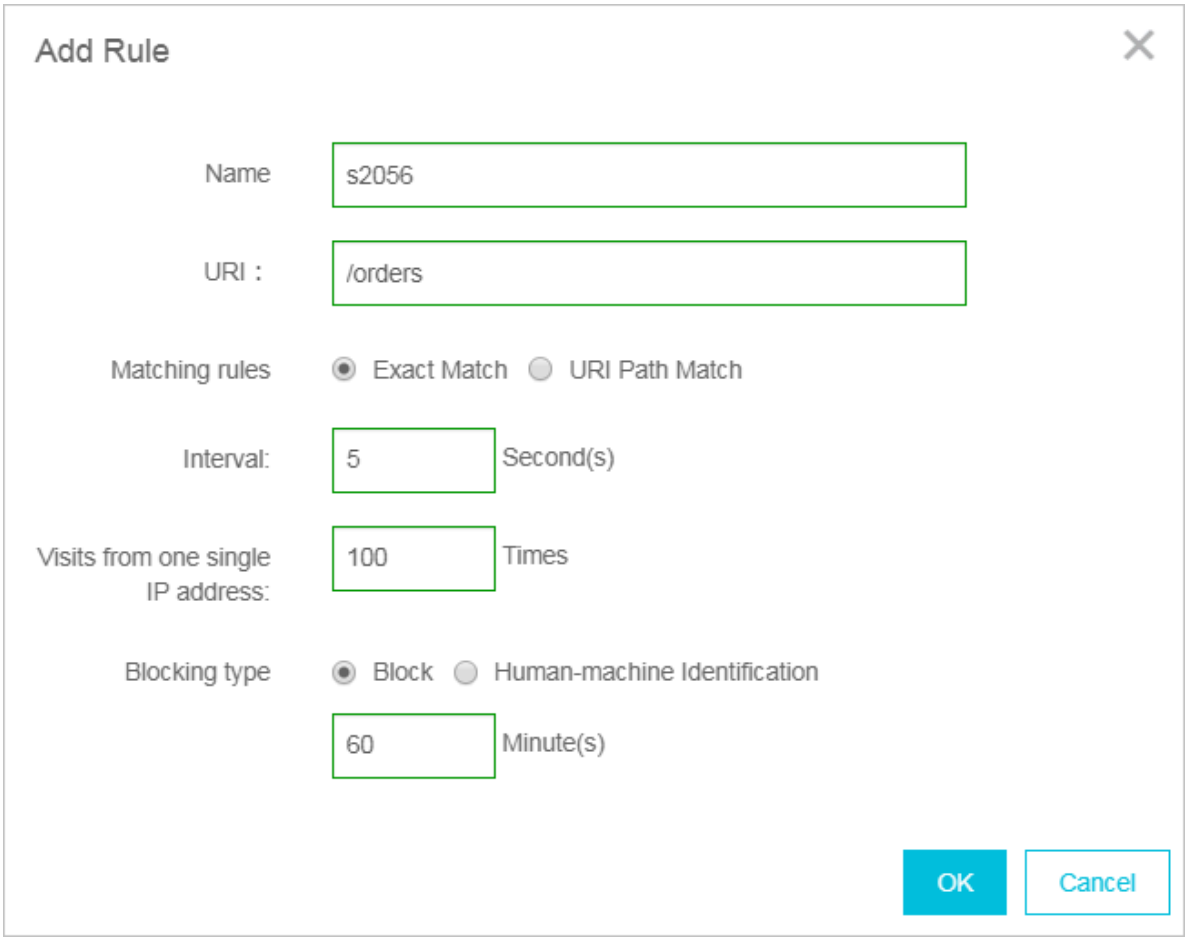
- You can add access control rules to block POST requests that contain specific XML data, such as `com . sun . xml . internal . ws . encoding . xml . XMLMessage $ XmlDataSou rce`. This can prevent DoS attacks from exploiting this vulnerability. For example, you can add the following rule to block malicious

requests sent to pages where the XStream handler is used in the Apache Strust REST plug-in.



- You can also use custom HTTP flood protection to restrict the frequency at which IP addresses send requests to pages where the XStream handler is used in the Apache Strust REST plug-in. For example, you can add the following rule to restrict

the frequency at which requests are sent to specific pages to 100 times per 5 seconds.



For more information about access control rules and custom HTTP flood protection, see *HTTP ACL Policy* and *Custom HTTP flood protection*.

1.3 WordPress DoS vulnerability (CVE-2018-6389)

On February 5, 2018, security researchers disclosed a DoS vulnerability affecting all 3.x-4.x versions of WordPress. A malicious attacker can consume server resources by having WordPress load multiple JavaScript files in a single request, which causes a DoS attack on the target server.

WAF is not affected by this vulnerability. However, if your website uses WordPress, we recommend that you add protection rules to increase the security of your business .

Description

This vulnerability is found in the *load-scripts.php* file. *load-scripts.php* is a built-in script in the WordPress CMS. The *load-scripts.php* file selectively calls required JavaScript files by passing their `names` into the `load` parameter. The `names` are separated with commas (,).

For example, in this request: `https://example.com/wp-admin/load-scripts.php?c=1&load[]=jquery-ui-core,editor&ver=4.9.1`, JavaScript files *jquery-ui-core* and *editor* are loaded.

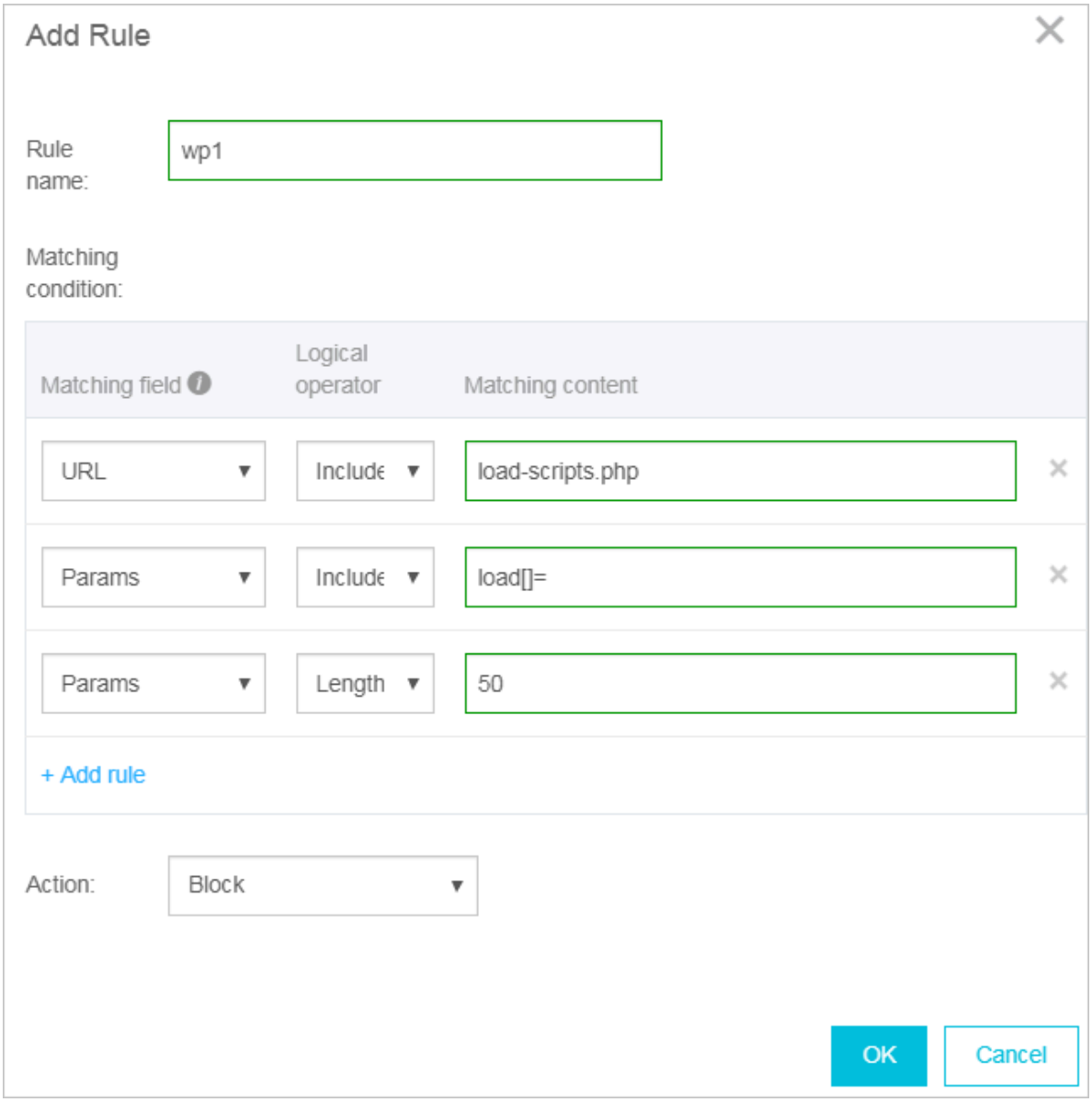
Therefore, all 181 JavaScript files defined in the *script-loader.php* file can be loaded in a single request. A malicious attacker can send a large number of requests without authorization, which results in increased server load and DoS attacks.

Protection tips

We recommend that you use HTTP ACL policies and custom HTTP flood protection to protect your WordPress website.

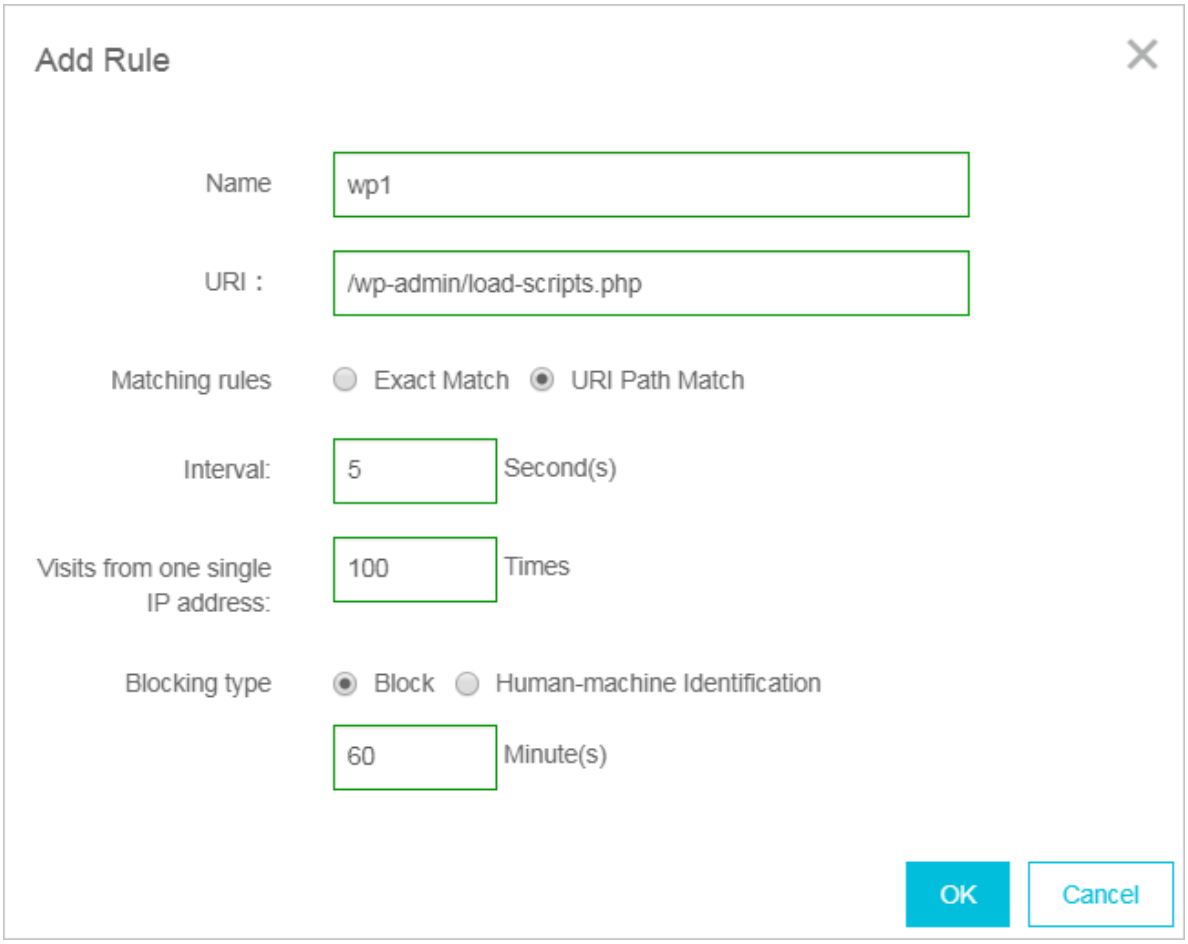
- You can add access control rules to restrict the number of parameters passed to the *load-scripts.php* file. For example, you can add the following rule to

restrict the length of the parameter passed to `load-scripts.php` to up to 50 characters.



- You can also use custom HTTP flood protection to restrict the frequency at which IP addresses can send requests to the `load-scripts.php`. For example, you

can add the following rule to restrict the frequency at which an IP address sends requests to `load-scripts.php` to up to 100 times per 5 seconds.



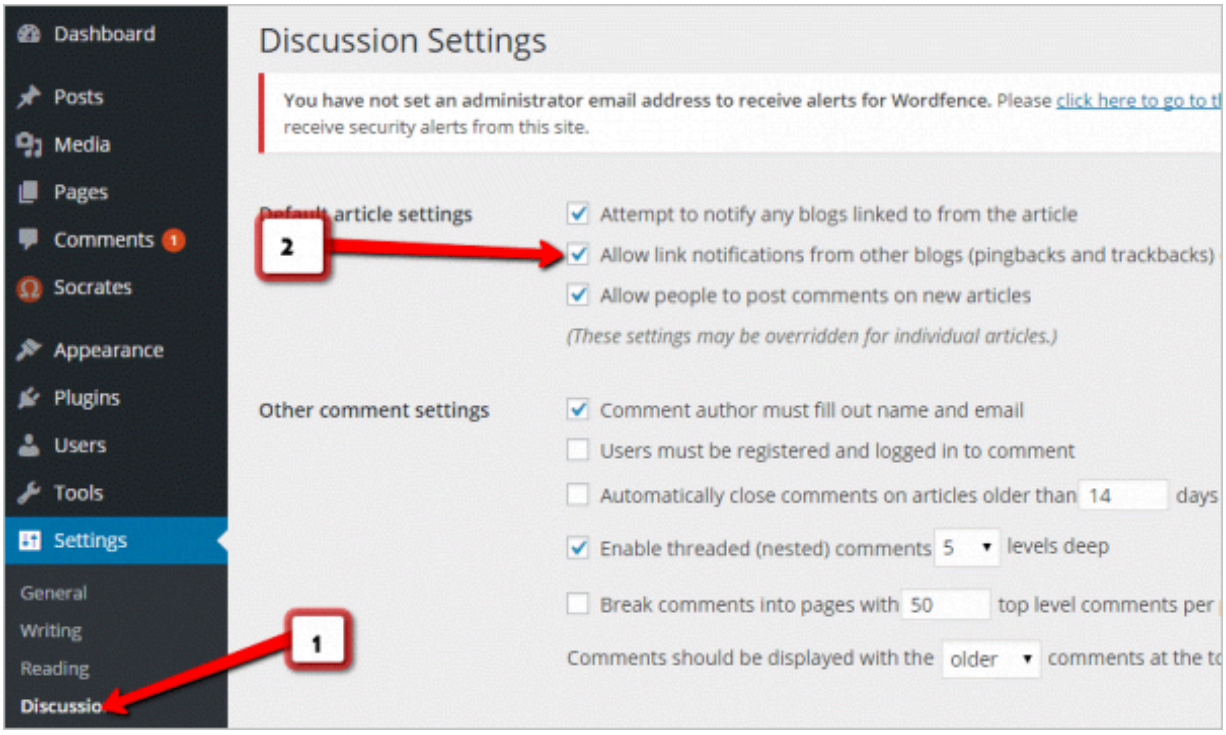
For more information about access control rules and custom HTTP flood protection, see *HTTP ACL policy* and *Custom HTTP flood protection*.

1.4 Prevent WordPress Pingback attacks

This topic describes how to prevent WordPress Pingback attacks with Alibaba Cloud WAF.

What is a WordPress Pingback attack

WordPress is a blog platform developed using the PHP language, and pingback is a plug-in of WordPress. Hackers can use pingback to initiate WordPress Pingback attacks against the website.



After suffering from the WordPress attack, you can see a lot of requests with User-Agent containing WordPress and pingback on the server log.

UA
WordPress/4.2.10; http://ascsolutions.vn; verifying pingback from 191.96.249.54
WordPress/4.0.1; http://146.148.63.90; verifying pingback from 191.96.249.54
WordPress/4.6.1; https://www.nokhostinsabt.com; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://eadastage.lib.umd.edu; verifying pingback from 191.96.249.54
WordPress/3.5.1; http://danieljromo.com
WordPress/4.2.4; http://wd.icopy.net.tw; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://kmgproje.com; verifying pingback from 191.96.249.54
WordPress/4.1.6; http://www.vv-atalanta.nl; verifying pingback from 191.96.249.54

As a variant of HTTP flood attack, WordPress Pingback attacks typically have the following symptoms: slow webpage loading, excessive server CPU consumption, response/data loss, and so on.

How to use WAF for defense

1. Log on to the *Web Application Firewall console*.

2. Go to the Management > Website Configuration page.
3. Locate to the domain name to be configured and click Policies.
4. Enable HTTP ACL Policy, and click Settings.
5. Click Add Rule and add the following access control rules respectively.
   - Block the access containing pingback in User-Agent.
     - Rule name: wp1
     - Matching field: User-Agent
     - Logical operator: Includes
     - Matching content: pingback
     - Action: Block
   - Block the access containing WordPress in User-Agent.
     - Rule name: wp2
     - Matching field: User-Agent
     - Logical operator: Includes
     - Matching content: WordPress
     - Action: Block

 Note:
You must add both the rules separately.

2 Protect your origin server

If the IP address of your origin server is disclosed, an attacker may exploit it to bypass Alibaba Cloud WAF and start direct-to-origin attacks against your origin server. To prevent such attacks, you can configure a security group (ECS origins) or whitelist (SLB origins) in your origin server.

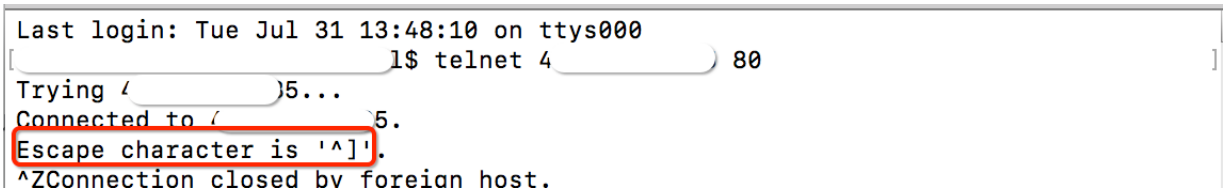
Context

> Note:
> You are not required to do the configuration described in this topic. But we recommend that you do so to eliminate the possible risk arises from IP exposure.

You can verify if such a risk exists in your origin server as follows.

Use Telnet to establish a connection from a non-Alibaba Cloud host to the listener port of your origin server's public IP address. Check if the connection is successful. If the connection succeeds, your origin server faces an exposure risk. Once a hacker obtain the public IP address, he or she can bypass WAF to reach your origin server. If the connection fails, your origin server is secure.

For example, test the connection to port 80 and 800 of your WAF-enabled origin server IP. If the connection is successfully established, your origin server is insecure.



Note

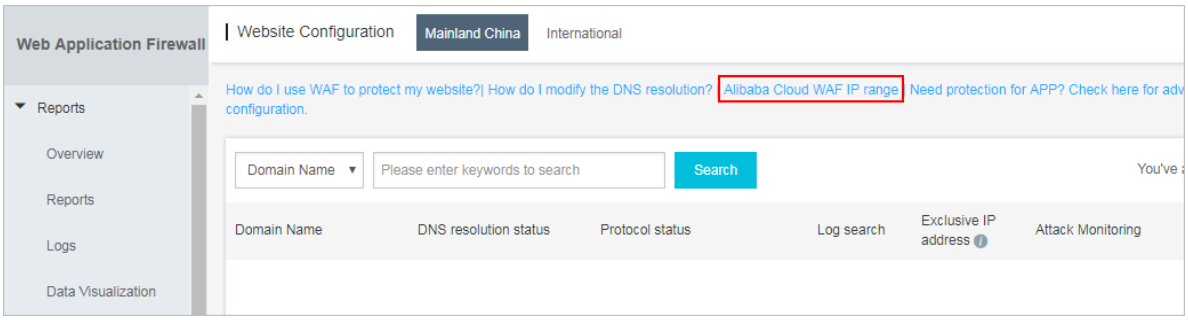
Configuring a security group has certain risks. Consider the following:

- Make sure that all domain names hosted in your origin server (ECS or SLB instance) are deployed with Alibaba Cloud WAF.
- In case of an Alibaba Cloud WAF cluster failure, where the WAF-inspected traffic is returned to origin server through a standby route, the access to your site will be affected if the security group policy is enabled in origin server.

- In case of an expansion of the Alibaba Cloud WAF IP addresses, 5xx error pages may be frequently returned to a visitor if the security group policy is enabled in origin server.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. Go to the Management > Website Configuration page.
3. Click Alibaba Cloud WAF IP range to view the WAF IP addresses.



4. In the Alibaba Cloud WAF IP range dialog box, click Copy IP list.

5. Configure the access control in your origin server to only allow the WAF IP addresses.
   - For an ECS origin
     a. Go to the *ECS instance list*, locate the origin instance, and click Manage.
     b. In the left-side navigation pane, click Security Groups.
     c. Locate to the security group to be operated and click Add Rules.
     d. Click Add Security Group Rule and complete the following configuration to allow the WAF IP addresses with the highest priority.
        - NIC: Internet Network
        - Rule Direction: Ingress
        - Action: Allow
        - Protocol Type: Customized TCP
        - Authorization Type: Ipv4 CIRD Block
        - Port Range: 80/443
        - Authorization Objects: Paste the copied WAF IP addresses in step 4.
        - Priority: 1
     e. Add another security group rule and configure it as follows to block all accesses with the lowest priority.
        - NIC: Internet Network
        - Rule Direction: Ingress
        - Action: Forbid
        - Protocol Type: Customized TCP
        - Port Range: 80/443
        - Authorization Type: Ipv4 CIRD Block
        - Authorization Object: 0.0.0.0/0
        - Priority: 100

 Note:

If the origin instance interacts with other IPs or applications, you must add corresponding rules to allow accesses from them.

- For an SLB origin

  The configuration in an SLB instance is similar as ECS. You add the WAF IP addresses to the whitelist. For more information, see *Configure access control*.

  - Create an access control list
  - Add the WAF IP addresses to the IP whitelist
  - Enable the IP whitelist

3 Get real client IP address

In many cases, a visitor's browser is not directly connected to the server for website access because CDN, WAF, or Anti-DDoS Pro is deployed in between. For example, the following is a common architecture: Client > CDN/WAF/Anti-DDoS Pro > Origin server. Here, how can a server get the real IP address of the client whose initial request passes through multiple layers of acceleration?

When forwarding a user's request to the server next in the chain, a proxy server that is open and transparent adds an X-Forwarded-For record to the HTTP header. This record is used to record the user's real IP address and takes the format of `X-Forwarded-For: user IP`. If multiple proxy servers are involved in the request process, X-Forwarded-For record displays in the following format: `X-Forwarded-For: user's IP address, Proxy 1-IP address, Proxy 2-IP address, Proxy 3-IP address ...`.

Therefore, a common application server can use the X-Forwarded-For record to get a visitor's real IP address. The following content describes the corresponding X-Forwarded-For configuration methods for the Nginx, IIS 6, IIS 7, Apache, and Tomcat servers.

Notice:

Back up your current environment such as the ECS snapshot and web server configuration file before performing the following configuration.

Nginx

1. Install http_realip_module.

As load balancing, Nginx uses http_realip_module to get the real IP address.

You can run the `# nginx -V | grep http_realip_module` command to verify whether or not, this module is installed. If not, recompile Nginx and load this module.

Note:

Nginx installed by the default procedure does not have this module installed.

Use the following code to install the http_realip_module module.

```
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_mod ule -- without
- http - cache -- with - http_ssl_m odule -- with - http_reali
p_module
make
make install
kill - USR2 ` cat / alidata / server / nginx / logs / nginx . pid
`
kill - QUIT ` cat / alidata / server / nginx / logs / nginx . pid
. oldbin `
```

2. Add the WAF IP addresses to the Nginx configuration.

Open `default . conf` and add the following content to `location / {}`:

```
set_real_i p_from ip_range1 ;
set_real_i p_from ip_range2 ;
...
set_real_i p_from ip_rangex ;
real_ip_he ader X - Forwarded - For ;
```

Note:

`ip_range1 , 2 ,..., x` indicates the back-to-source IP addresses of WAF, and multiple entries must be added respectively.

3. Modify log_format.

log_format usually exists under the HTTP configuration in `nginx . conf`. Add the *x - forwarded - for* field in *log_format* to replace the original *remote - address*. After the modification, *log_format* is as follows.

```
log_format main '$ http_x_for warded_for - $ remote_use r
 [$ time_local ] "$ request " ' '$ status $ body_bytes _sent "$
http_refer er " ' '"$ http_user_ agent " ';
```

After the preceding operations are completed, run `nginx - s reload` to restart Nginx and validate the configuration. When the configuration is effective, the Nignx server records the client IP address in the X-Forwarded-For field.

IIS 6

You can get the visitor's real IP address from the IIS 6 log, provided that the *F5XForwardedFor.dll* plug-in has been installed.

1. Copy `F5XForward edFor . dll` from the `x86 \ Release` or `x64 \ Release` directory (according to the OS version of the server) to a specified directory assumed as `C :\ ISAPIFilte rs` , and make sure that the IIS process has the read permission for this directory.
2. Open the IIS manager, find the currently visited website, right-click the website and select Property to open the Property page.
3. Switch to the ISAPI Filter tab page on the Property page and click Add.
4. Set the following parameters in the Add window, and then click OK.
   - Filter name: F5XForwardedFor
   - Executable file: enter the complete path of F5XForwardedFor.dll. In this example, `C :\ ISAPIFilte rs \ F5XForward edFor . dll` .
5. Restart the IIS server and wait for the configuration to be effective.

IIS 7

You can get the visitor’s real IP address through the *F5XForwardedFor* module.

1. Copy `F5XFFHttpM odule . dll` and `F5XFFHttpM odule . ini` from the `x86 \ Release` or `x64 \ Release` directory (according to the OS version of the server) to a specified directory assumed as `C :\ x_forwarde d_for \ x86` and `C :\ x_forwarde d_for \ x64` , and make sure that the IIS process has the read permission for this directory.
2. In IIS Manager, double-click to open Module.
3. Click Configure Local Module.
4. Click Register in the Configure Local Module dialog box, and register the downloaded DLL file.
   - Register the x_forwarded_for_x86 module
     - Name: x_forwarded_for_x86
     - Path: `C :\ x_forwarde d_for \ x86 \ F5XFFHttpM odule . dll`
   - Register the x_forwarded_for_x64 module
     - Name: x_forwarded_for_x64
     - Path: `C :\ x_forwarde d_for \ x64 \ F5XFFHttpM odule . dll`
5. After registration, select the newly registered modules (x_forwarded_for_x86 and x_forwarded_for_x64), and click OK to enable them.

6. Add the registered DLL in API and CGI restrictions respectively, and change the settings from Restricted to Allowed.
7. Restart the IIS server and wait for the configuration to be effective.

Apache

Windows system

The Apache 2.4 or higher versions have the remoteip_module file (*mod_remoteip.so*) in the installation package. You can use this file to get the real client IP address.

1. Under Apache's configuration file folder *conf/extra/*, create the *httpd-remoteip.conf* file.

   Note:
   Using *remoteip.conf* instead of *httpd.conf* to load the related configuration helps avoid misoperation.

2. In the *httpd-remoteip.conf* file, add the following code.

```
# load mod_remoteip.so
LoadModule remoteip_module modules/mod_remoteip.so
# configure RemoteIPHeader
RemoteIPHeader X-Forwarded-For
# configure WAF back-to-source IP addresses
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. Edit the *conf/httpd.conf* file to insert *httpd-remoteip.conf*.

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

4. In *httpd.conf*, change log format.

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

5. Restart Apache to bring the configuration into effect.

Linux system

You can get the real client IP address by installing the third-party module *mod_rpaf*.

1. Run the following command to install *mod_rpaf* .

```
wget http :// stderr . net / apache / rpaf / download / mod_rpaf
- 0 . 6 . 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. Edit the Apache configuration file */ alidata / server / httpd / conf / httpd . conf* to add the following content at the end of the file.

Note:

`RPAFproxy_ ips` are not the public IP addresses of load balancing. Refer to the Apacha logs for the IP addresses (usually contain two IP addresses).

```
LoadModule rpaf_modul e modules / mod_rpaf - 2 . 0 . so
RPAFenable On
RPAFsethos tname On
RPAFproxy_ ips ip addresses
RPAFheader X - Forwarded - For
```

3. Run the following command to restart Apache and bring the configuration into effect.

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

Configuration example of mod-rpaf

```
LoadModule rpaf_modul e modules / mod_rpaf - 2 . 0 . so
RPAFenable On
RPAFsethos tname On
RPAFproxy_ ips 10 . 242 . 230 . 65 10 . 242 . 230 . 131
RPAFheader X - Forwarded - For
```

Tomcat

You can enable the X-Forwarded-For feature of the Tomcat server as follows.

Open *tomcat / conf / server . xml* and modify the AccessLogValve log record function to the following content:

```
< Valve className =" org . apache . catalina . valves . AccessLogV
alve " 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 " resolveHos ts =" false "/>
```

4 Best practices for Web application protection

This topic describes the best practices for Web application protection based on WAF. The following aspects are covered: scenarios, protection policies, protection effects, and rule updates.

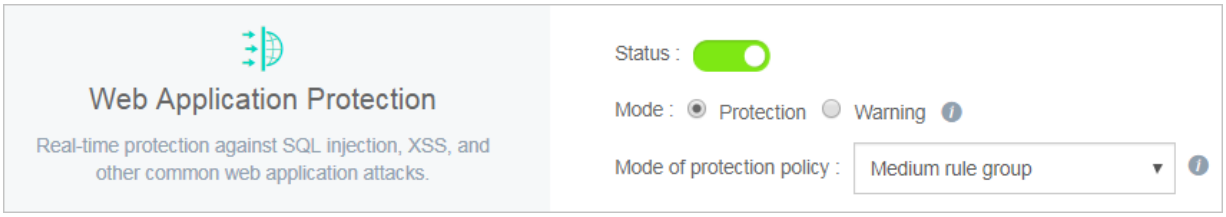
Scenarios

WAF provides protection against Web attacks, such as SQL injection, XSS, remote command execution, and webshell upload. For more information about Web attacks, see *OWASP 2017 Top 10*.

> **Note:**
> Server intrusions caused by security issues in host layers, such as unauthorized access to Redis and MySQL, are not covered by WAF.

Protection policies

After you add your domain to WAF, log on to the *Web Application Firewall console*. In the left-side navigation pane, choose Management > Website Configuration. Select your domain and click Policies to view the protection status of your website, as shown in the following figure:



By default, Web Application Protection is enabled and the normal mode protection is used. The parameters are as follows:

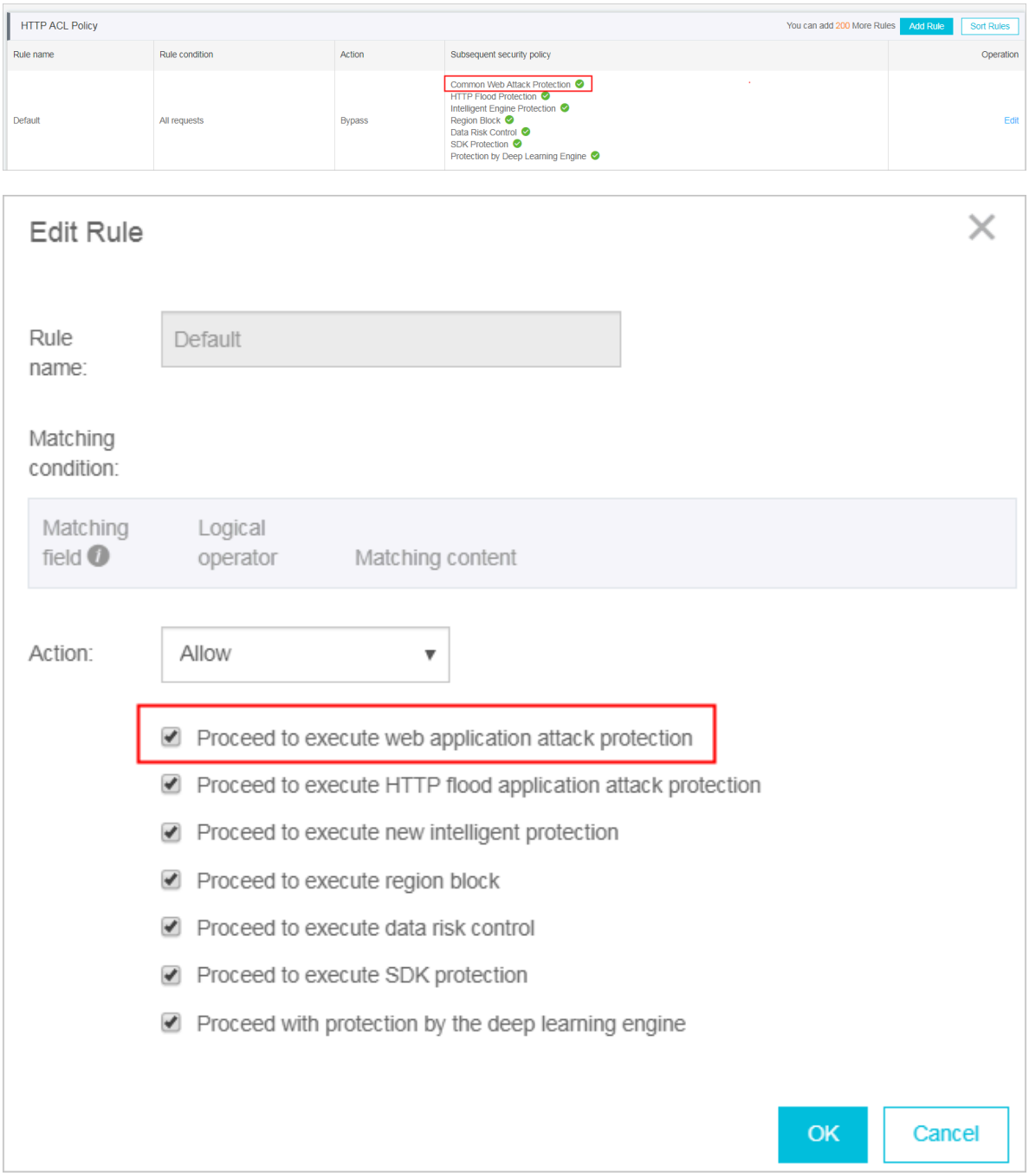
- Status
  - Enabled indicates that Web Application Protection is enabled.
  - Disabled indicates that Web Application Protection is disabled.

- Mode: Two modes are provided: Protection and Warning.
  - The Protection mode indicates that WAF automatically blocks malicious requests and logs attacks when the application is under attack.
  - The Warning mode indicates that WAF does not block malicious requests but logs attacks when the application is under attack.
- Protection Policy: Three protection policies are available when the Protection mode is selected: Loose, Normal, and Strict.
  - Loose: This policy only blocks requests that display typical attack patterns.
  - Normal: This policy blocks requests that display common attack patterns.
  - Strict: This policy blocks crafted requests that display specific types of attack patterns.

Protection tips:

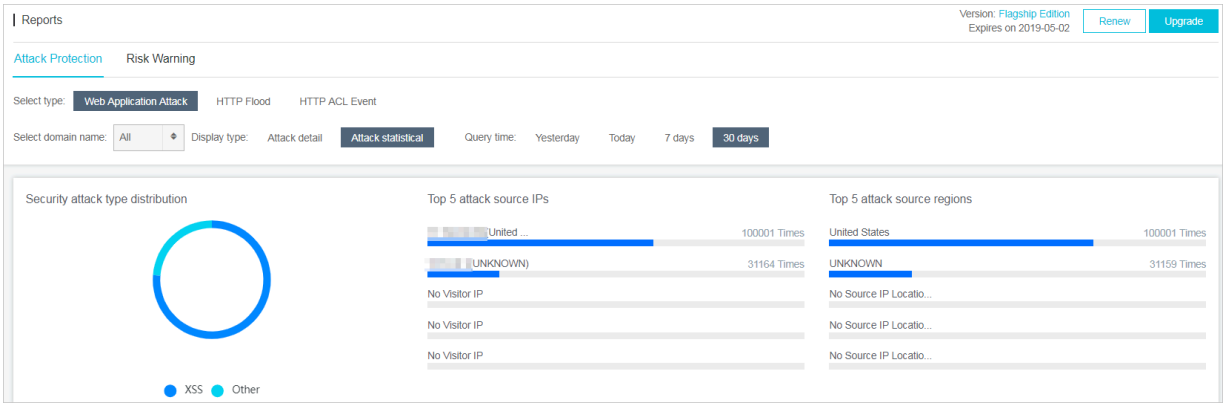
- If you are not clear about your website's traffic patterns, we recommend that you use the Warning mode first. You can observe the traffic flow for one or two weeks and then analyze the attack log.
  - If you do not find any record indicating that normal requests are blocked, you can switch to the Protection mode to enable further protection.
  - If normal requests are found in the attack log, contact customer service to resolve the issue.
- If you add domains of PHPMyAdmin or tech forums to WAF, normal requests may be mistakenly blocked. We recommend that you contact customer service to resolve the issue.
- Note the following points in your operations:
  - Do not pass raw SQL statements or JavaScript code in HTTP requests.
  - Do not use special keywords, such as UPDATE and SET, to define the path in URLs, such as `www . example . com / abc / update / mod . php ? set = 1`.
  - If file uploads are required, restrict the maximum file size to 50 MB. We recommend that you use OSS or other methods to upload files exceeding the size limit.

- After Web Application Protection is enabled, do not disable the All Requests option in the default rule of HTTP ACL Policy, as shown in the following figure:

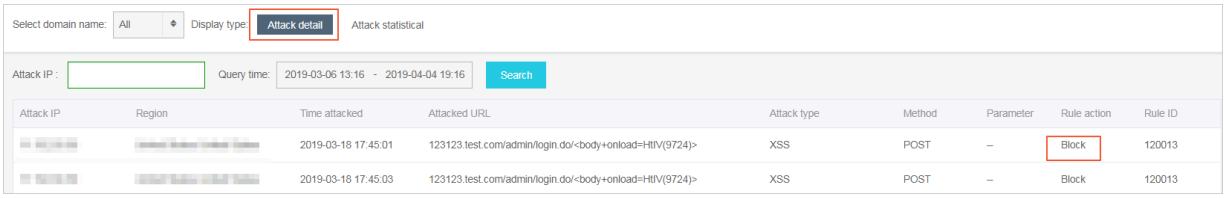


Protection effects

After Web Application Protection is enabled, you can choose Reports > Reports to view details about blocked attacks, as shown in the following figure:



On the Reports page, you can view attack details by time, such as yesterday, today, last seven days, or last month. You can click View Attack Details to view detailed attack information, as shown in the following figure:



The figure displays the details about a SQL injection attack that has been blocked by WAF.

> **Note:**
> If you find that normal requests are mistakenly blocked by WAF, we recommend that you *whitelist* the affected URLs in HTTP ACL policies and then contact customer service to resolve the issue.

Rule updates

When new vulnerabilities are discovered, WAF updates protection rules and releases security bulletins in a timely manner.

Log on to the *Web Application Firewall console*. In the left-side navigation pane, choose Overview > Security to view the latest security bulletins.

> **Note:**
> Web attacks usually have more than one proof of concept (POC). A thorough analysis is conducted to determine the cause of the vulnerability so that the protection rule can prevent all exploits of this vulnerability.

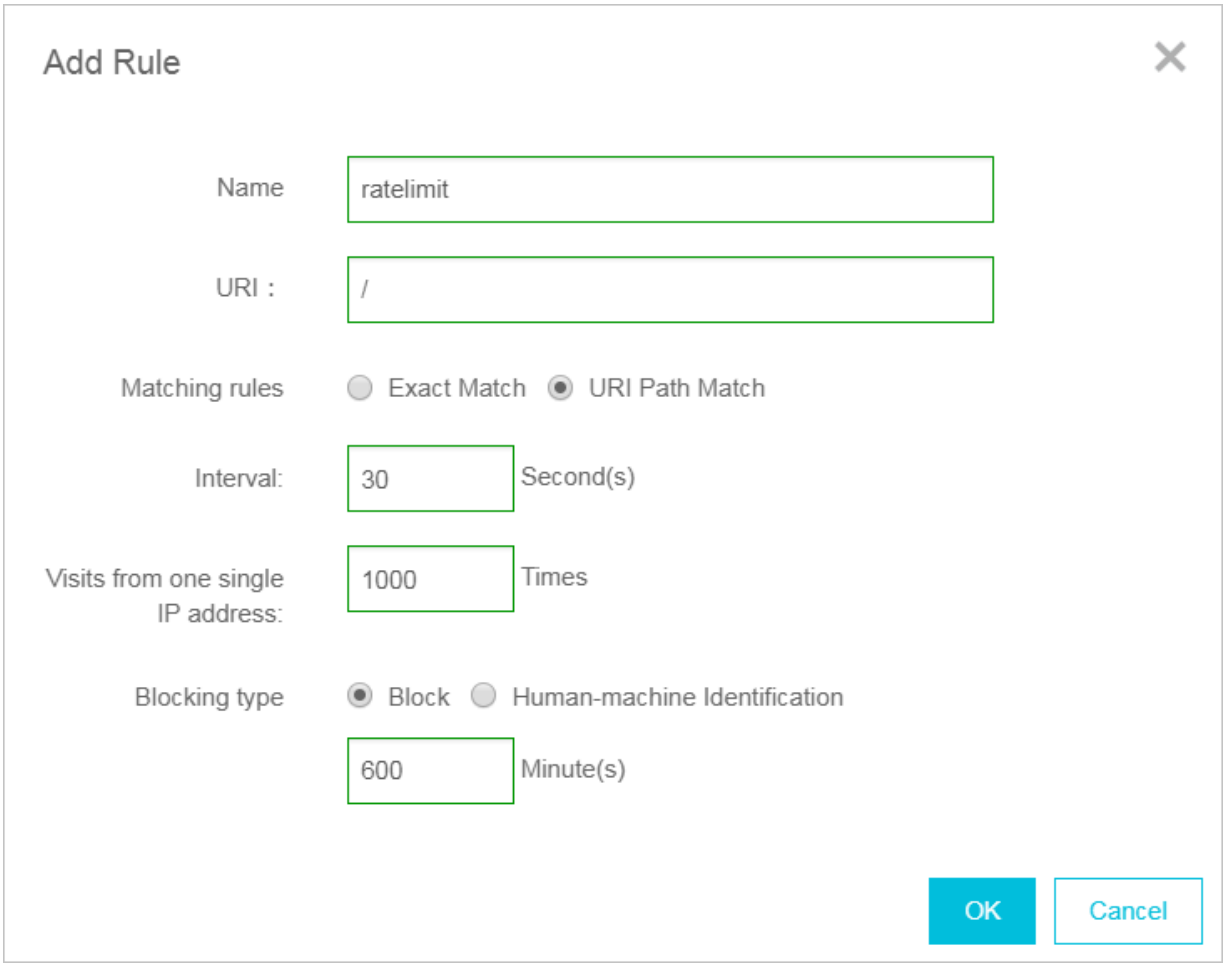
5 Best practices for HTTP flood protection

This topic describes common scenarios of HTTP flood attacks and introduces related protection strategies offered by WAF. By using WAF, you can effectively protect your site from HTTP flood attacks.

Frequent HTTP flood attacks

During HTTP flood attacks, the request rate of a single zombie server is typically far higher than that of a normal user. The most effective way to defend against this type of attack is to restrict the request rate of the source IP.

You can create *custom HTTP flood protection rules* to implement restrictions on the request rate. Example:



This rule uses prefix match to select all paths under the domain. If an IP address sends more than 1,000 requests to the domain within 30 seconds, the IP address is blocked for 10 hours. This rule can be used to protect small and medium-sized websites.

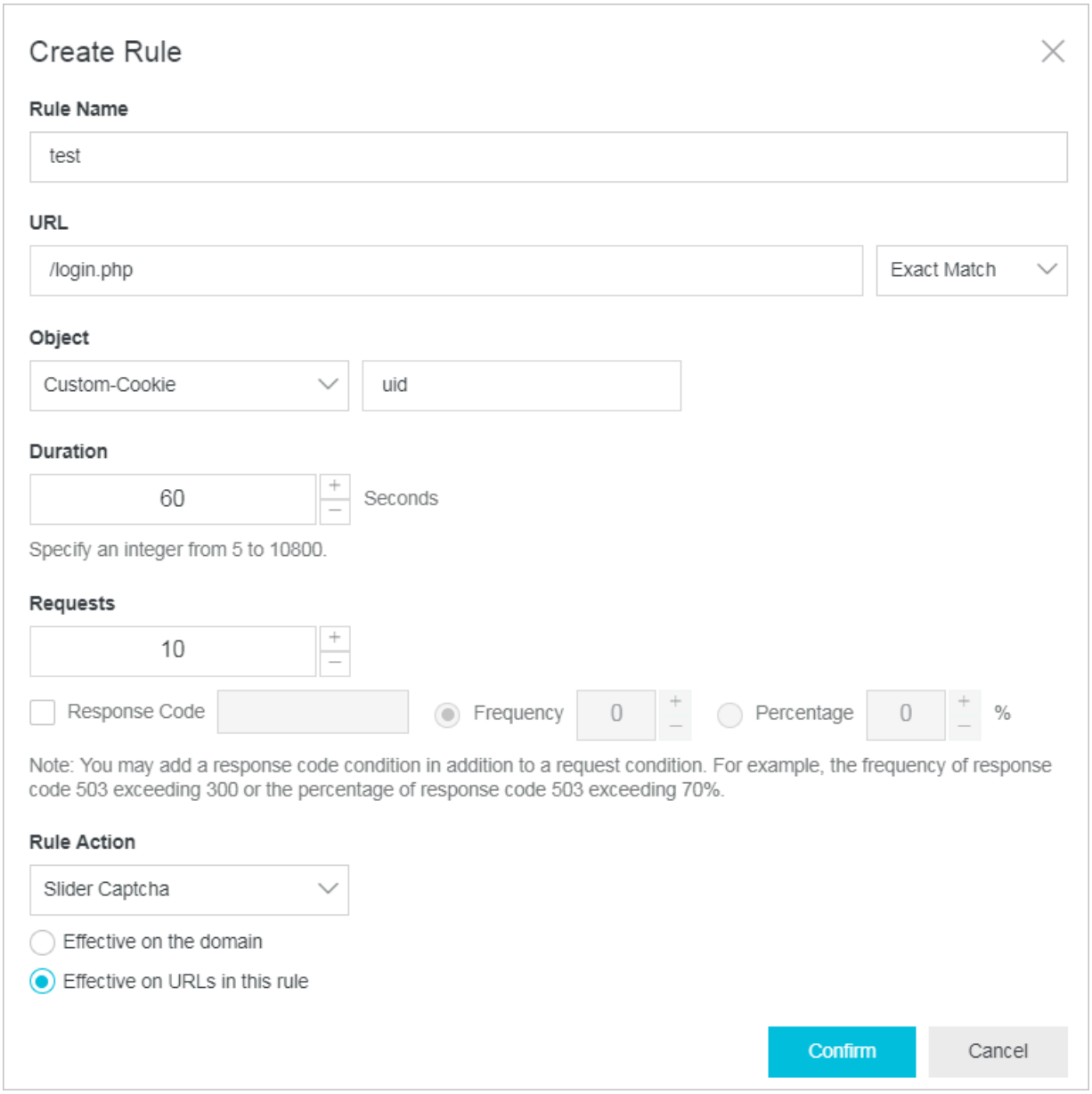
You can modify the protected paths, adjust the blocking threshold, and change the blocking type based on your need to achieve better protection. For example, to prevent user enumeration, you can use prefix match to select the logon path, such as "/login.php", and block IPs that send more than 20 requests to access the path within 60 seconds.

Note the following points when you use HTTP flood protection:

- The Human-machine Identification blocking type can verify whether requests are sent from Web browsers or automation scripts. You can use this blocking type to protect Web and HTML5 applications, but not native apps or API services. To protect native apps and API services, set the blocking type to block.
- For APIs or IP addresses that may be mistakenly blocked by HTTP flood protection, you can use *HTTP ACL Policy* to whitelist these source IPs.
- Do not enable the emergency mode for native apps or API services.

We recommend that you use Anti-Bot Service for more targeted protection and flexible handling methods.

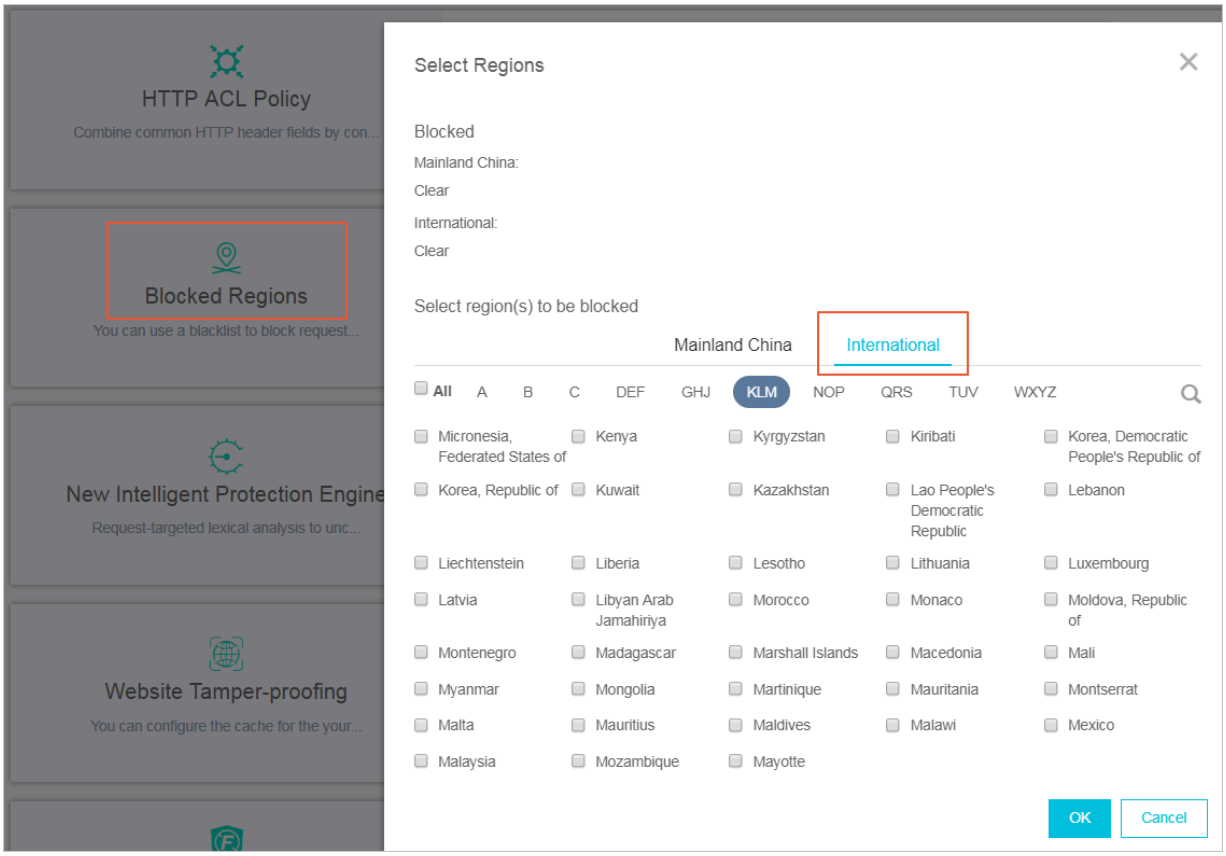
For example, blocking IP addresses may affect NAT. Anti-Bot Service allows you to use cookies or request parameters to calculate the request rate. You can also use slider captcha to verify the identity of the requester. In the following example, the request rate is calculated based on the user's cookie. Slider captcha is used to verify the identity of the user. Assume that the cookie format is as follows: uid=12345.



Attacks originating from international regions and public clouds

A large portion of HTTP flood attacks originate from international regions, data centers, and public clouds. If your website targets Chinese users, you can block requests from international regions to mitigate this attack.

WAF provides the *Blocked Regions* feature for this purpose.



If you need to block IP addresses from data centers or public clouds, such as Alibaba Cloud or Tencent Cloud, contact customer service through DingTalk.

Abnormal or unusual packets

Malicious requests in HTTP flood attacks are arbitrarily constructed and contain abnormal or unusual packets compared with normal requests. Most malicious requests have the following features:

- Abnormal user-agent. For example, the user-agent field shows characteristics of automation tools (such as Python), has an incorrect format (such as Mozilla///), or is obviously exceptional (such as www.baidu.com). Block the request if these features are detected.
- Unusual user-agent. For example, promotional HTML5 pages targeting WeChat users are supposed to be accessed through WeChat. It is unusual if the user-agent field indicates that the request is sent from a Windows desktop browser, such as MSIE 6.0. Block the request if these features are detected.
- Unusual referer. For example, the referer field does not exist or indicates the address of an illegitimate site. We recommend that you block this request.

However, the user may be visiting your home page for the first time. If the page can only be accessed through redirects, it is unusual that the referer field is void.

- Unusual cookie: Similar to the referer field, a normal request usually contains a cookie that is related to the user, unless it is the user's first visit to your site. In many situations, malicious requests in HTTP flood attacks do not contain any cookie information.
- Missing HTTP headers: For example, normal requests usually contain the authorization header while malicious requests usually do not.
- Incorrect request method: For example, if an API has only received POST requests before and is now overwhelmed by GET requests, then you can directly block GET requests.

To handle these requests, you can analyze their features and add *HTTP ACL policies* to block the malicious requests.

Figure 5-1: Example 1: Block requests that do not contain cookies

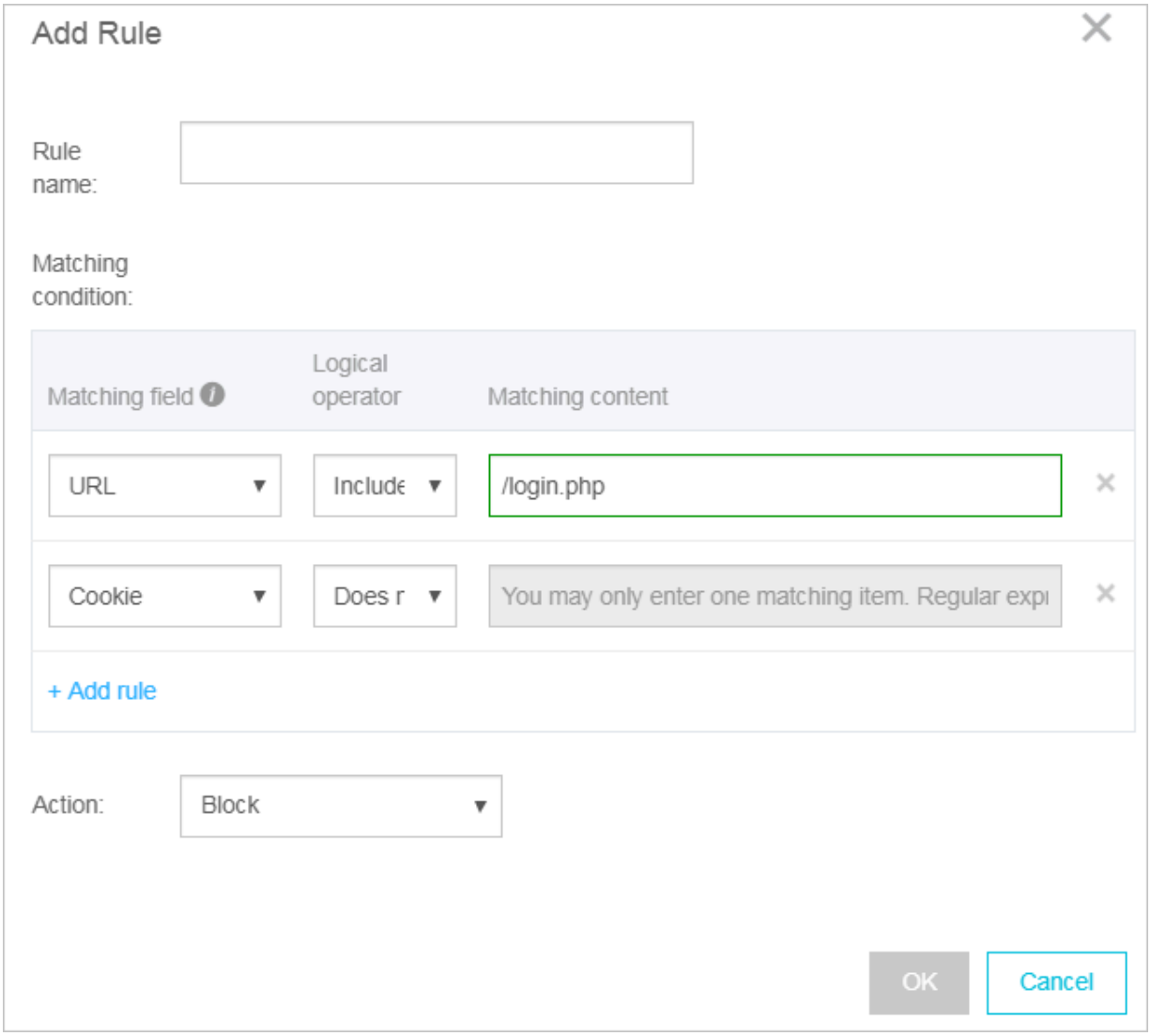
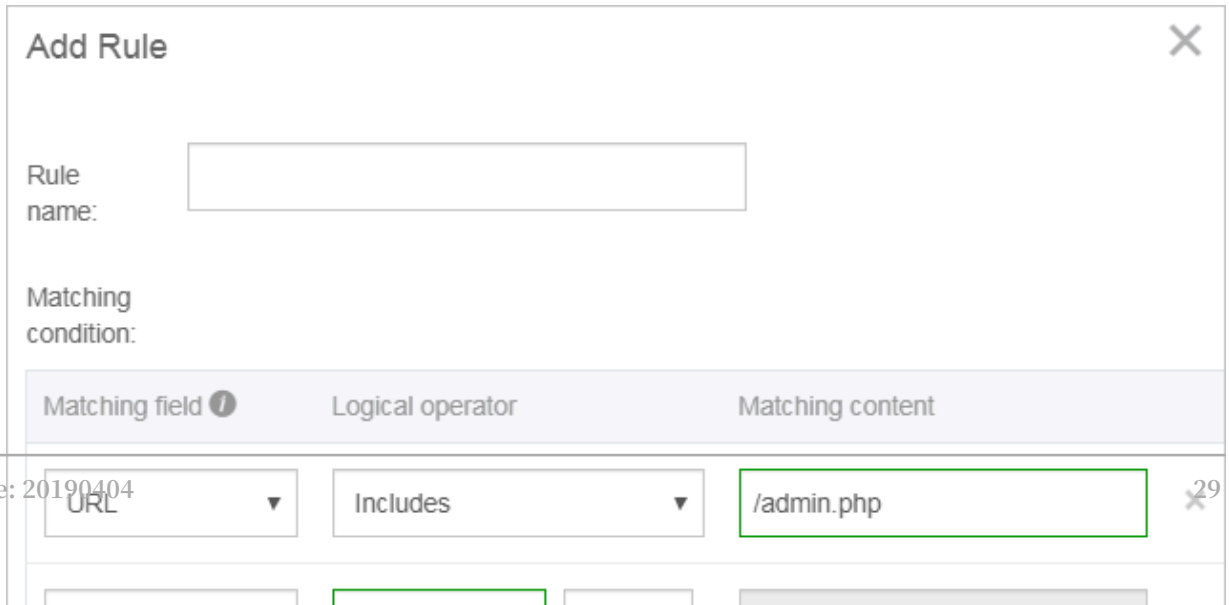


Figure 5-2: Example 2: Block requests that do not contain authorization headers



API abuses

We recommend that you use *Data Risk Control* to protect important APIs from abuses. These APIs include logon, registration, voting, and SMS verification APIs.

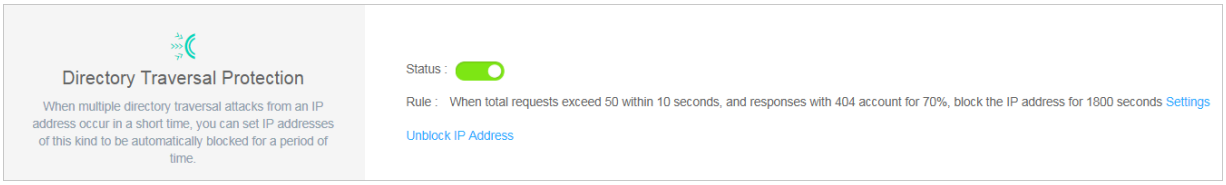
Data Risk Control injects a JavaScript snippet into your webpage and collects information about user behavior and environment variables to determine whether the request is sent from a real user or an automation script. Data Risk Control makes decisions based on human identification. The request rate and source IP address are not taken into account. The service is very effective in mitigating low-frequency attacks.

> **Note:**
> Data Risk Control depends on the authorization headers contained in normal requests to identify malicious requests. The service is not applicable to environments where JavaScript is not supported, such as API services and native apps. To prevent false positives, we recommend that you test out Data Risk Control first before you enable it in the production environment. You can contact customer service for the test methods.

Malicious scans

A large number of malicious scans pose a serious threat to the performance of your servers. Apart from restricting scans based on frequency, you can also use *Malicious IP Blocking* to enhance protection.

Scan requests displaying common attack patterns are automatically blocked by WAF based on default protection rules. Malicious IP Blocking can directly block IP addresses that frequently trigger protection rules.



Fake apps

To protect your business from fake apps, you can use a number of different mitigation s such as custom HTTP flood protection, blocked regions, and HTTP ACL policies . You can also integrate with Alibaba Cloud Security SDK for enhanced protection capability.

After you integrate the SDK with your app, all incoming requests must be verified before they are sent to the server. The device information and request signature are combined to determine if the request is sent from a legitimate app. Requests that do not originate from the official app are automatically blocked. This ensures that only requests from legitimate clients are served. You do not need to analyze the patterns of illegitimate requests.

To use the security SDK, you must activate Anti-Bot Service. For more information, see *SDK instructions*.

Web crawlers

For informational websites offering services such as credit reports, apartment rentals, airline tickets, and e-book reading, Web crawlers can significantly increase bandwidth usage, slow down the server's performance, and even cause data leakage. The aforementioned approaches may not be very effective in preventing Web crawlers. We recommend that you use Anti-Bot Service for more advanced protection.

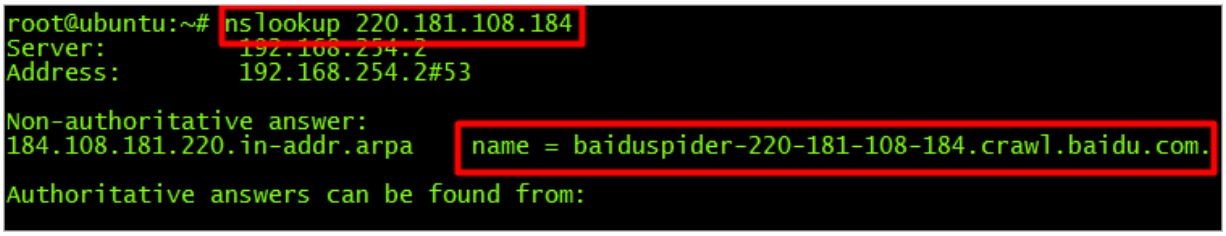
6 Intercept malicious crawlers

This topic explains the features of malicious crawlers and describes how to use WAF to block them.

It is noteworthy that, professional crawlers constantly change their crawling methods to bypass anti-crawling policies set by the website administrators. It is impossible to achieve perfect protection by applying fixed rules. In addition, anti-crawling has a strong association with the characteristics of your own business. Therefore, you must regularly review and update the protection policies to achieve relatively ideal results.

Distinguish malicious crawlers

Normal crawlers are usually labeled with marks similar to xxspider's user-agent. They request in a regular manner, and the URLs and time are relatively scattered. If you perform an inverted nslookup or tracert on a legitimate crawler, you can always find the legitimate source address. For example, a Baidu crawler record is shown in the following figure.

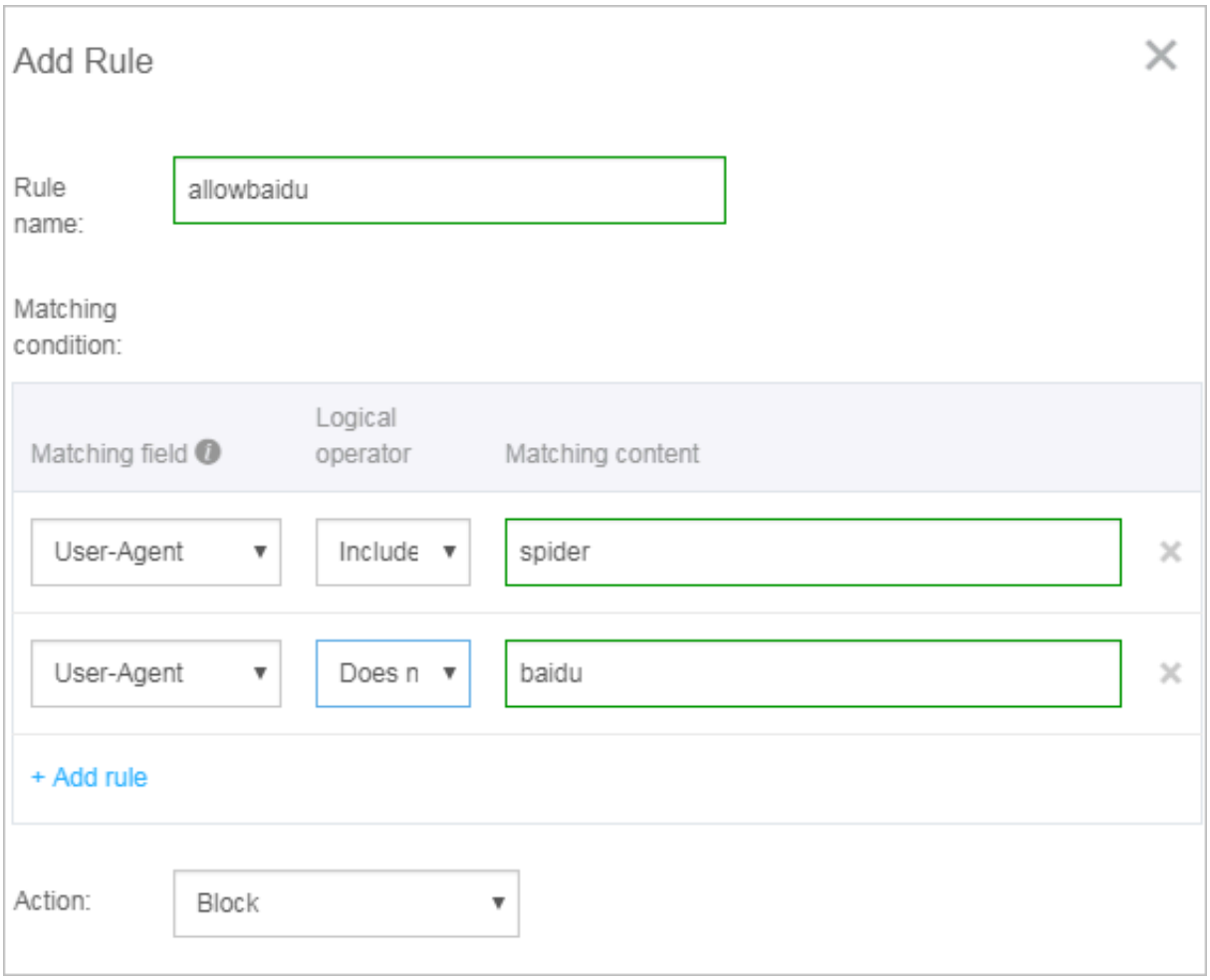


However, malicious crawlers may send a large number of requests to a specific URL/interface of a domain name during a specific period of time. It may be an HTTP flood attack disguised as a crawler, or a crawler that crawls targeted sensitive information disguising as a third party. When the number of requests sent by a malicious crawler is large enough, it can usually cause a sharp rise in CPU usage, failure to open the website, and service interruptions.

WAF performs *Risk warning* against malicious crawlers, and alerts you about yesterday's crawler requests. You can configure one or more of the following rules based on your actual business situation, to block the corresponding crawler requests.

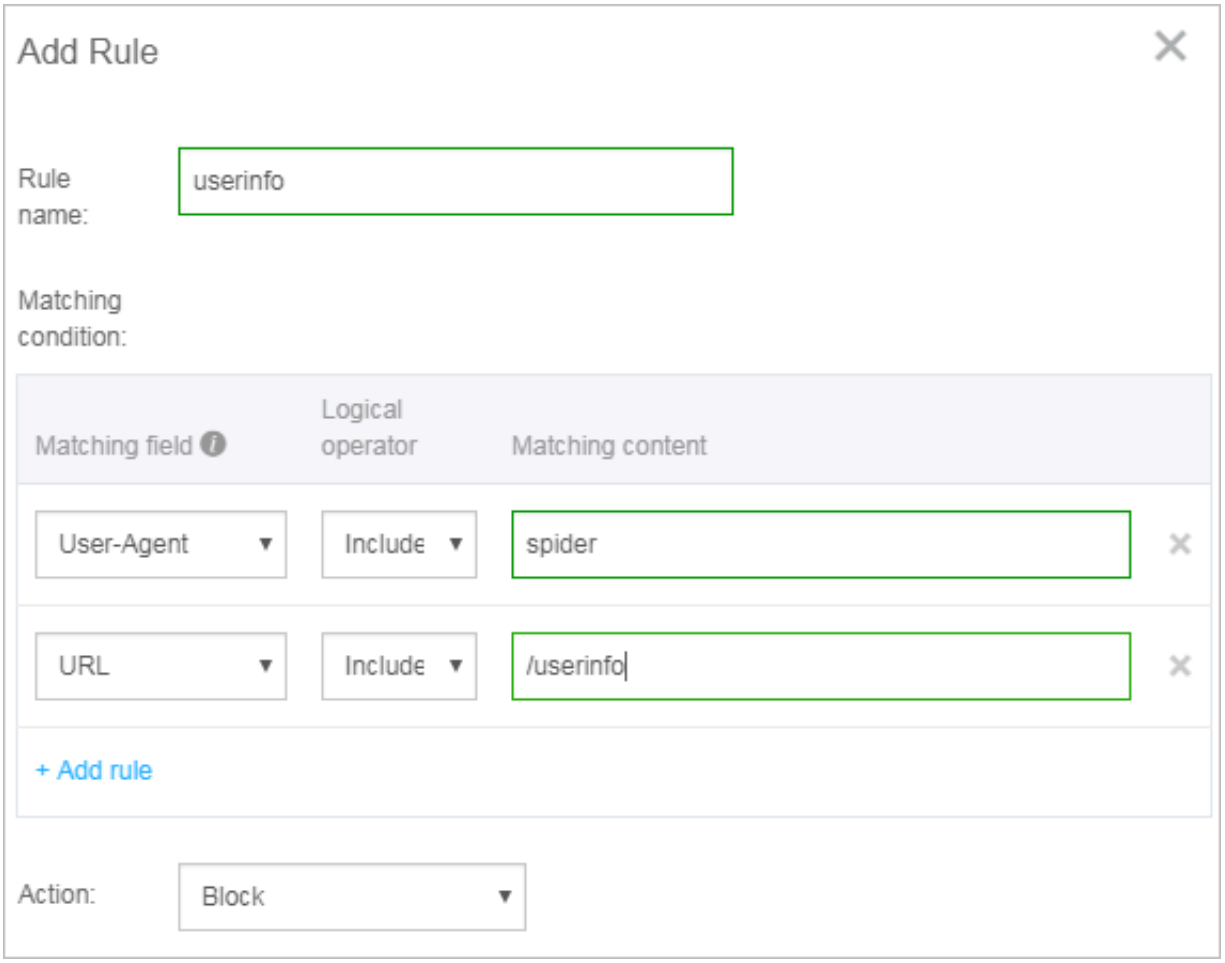
Configure HTTP ACL policy to block specific crawlers

You can *configure the HTTP ACL policy* to use user-agent, URL, and other keywords to filter out malicious crawler requests. For example, the following configuration only allows Baidu crawler, and filters out other crawlers (keywords are not case-sensitive).



Note:
Multiple conditions in a rule are connected by the "AND" logical relationship, that is, a request must satisfy all conditions of a rule for the rule to be effective.

You can use the following configurations to prevent all crawlers from accessing contents under the `/ userinfo` directory.



Configure custom HTTP flood policies to block malicious requests

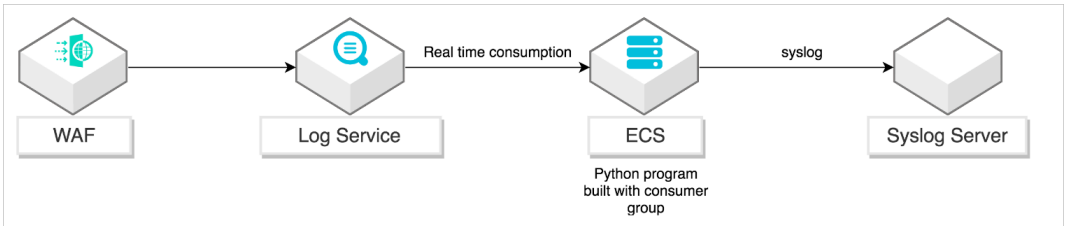
Using *custom HTTP flood protection rules* allows you to set a few specific URLs blocking rules under certain access frequency.

7 Integrate Alibaba Cloud WAF log with syslog

This topic describes how to integrate Alibaba Cloud WAF log with syslog to guarantee all compliance, auditing, and other related logs can be ingested into your Security Operation Center.

Overview

The following figure illustrates the syslog integration architecture:



Alibaba Cloud Log Service is a one-stop service for log data. Log Service experiences massive big data scenarios of Alibaba Group. Log Service (LOG or SLS) allows you to quickly complete the collection, consumption, shipping, query, and analysis of log data without the need for development, which improves the Operation & Maintenance (O&M) efficiency and the operational efficiency, and builds the processing capabilities to handle massive logs in the DT (data technology) era. For more information, see *Log Service Production Introduction*.

Python Program is a program running on ECS to deliver WAF log to a syslog server. The consumer library is an advanced mode of log consumption in Log Service, and provides the consumer group concept to abstract and manage the consumption end. Compared with using SDKs directly to read data, you can only focus on the business logic by using the consumer library, without caring about the implementation details of Log Service, or the load balancing or failover between consumers. For more information, see *Consumer group introduction*.

Syslog Server is a centralize log message management server to receive multiple syslog sources.

Prerequisites

Before you begin, make sure of the following:

- You have purchased Alibaba Cloud WAF business edition or above to protect your website. For more information, see *Purchase Alibaba Cloud WAF* and *Implement Alibaba Cloud WAF*.
- You have a Linux ECS server with the following recommended hardware spec:
  - Operating System with Ubuntu
  - 8 vCPUs with 2.0+ GHz
  - 32GB Memory
  - at least 2GB available disk space (10GB or more is suggested)
- You have a syslog server with UDP port 514 enabled to receive syslog.

Procedure

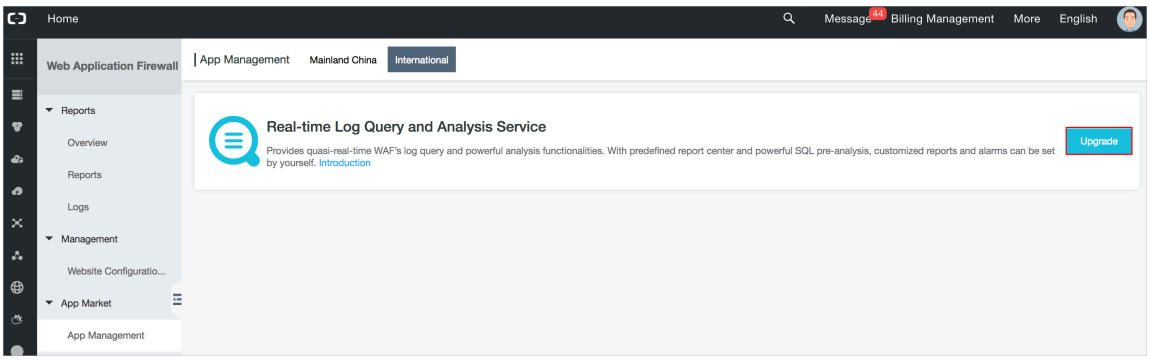
1. Enable Alibaba Cloud WAF logging.

   Follow these steps to enable Alibaba Cloud WAF logging in the WAF console:

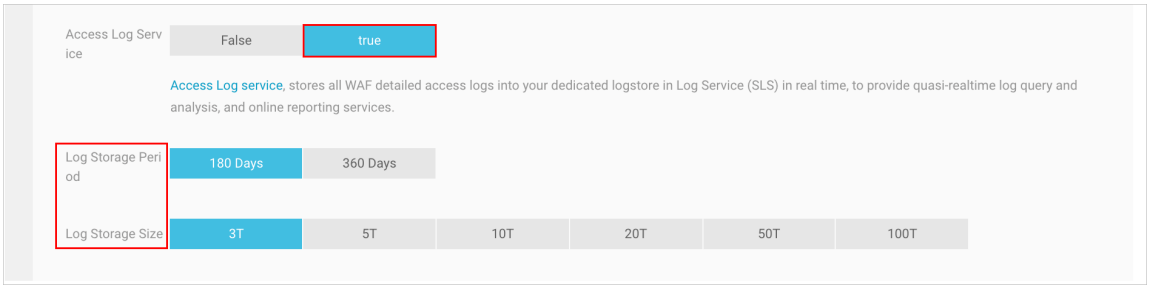
   a. Log on to the *Alibaba Cloud WAF console*.

   b. In the left-side navigation pane, selectApp Market > App Management.

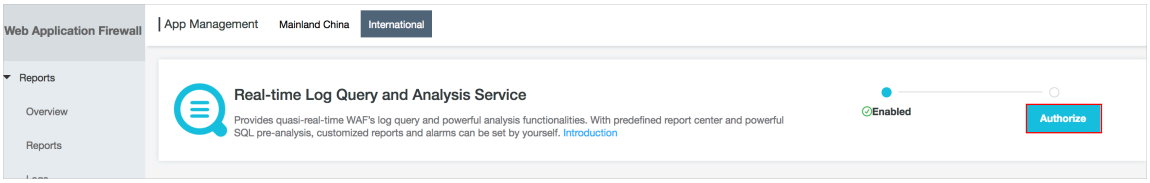
   c. Under Real-time Log Query and Analysis Service, click Upgrade.



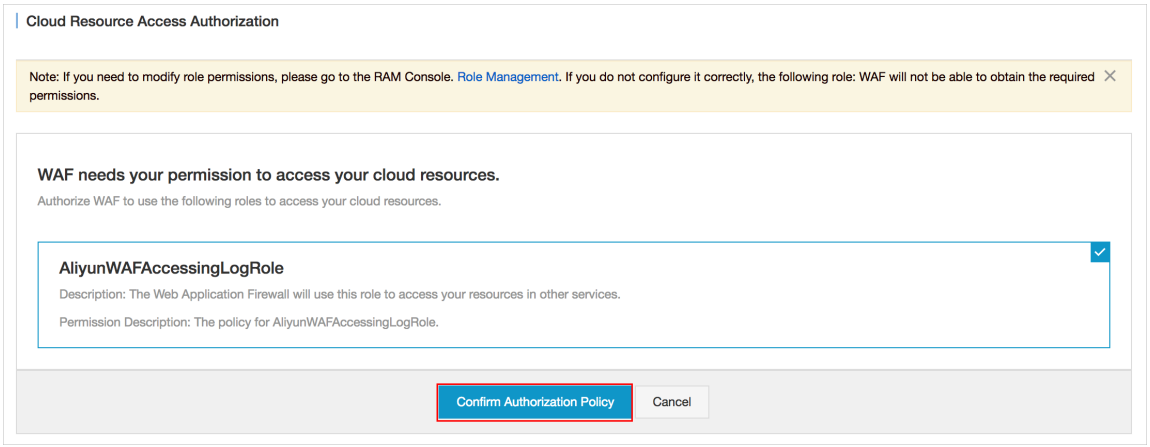
   d. On the Update page, enable Access Log Service and select Log Storage Period and Log storage Size accordingly.



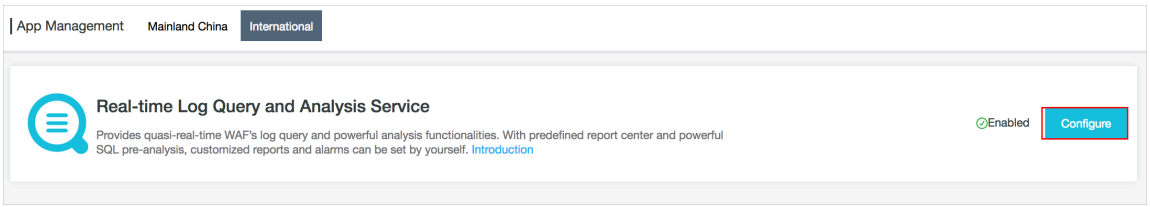
   e. After activating Log service, click Authorization under Real-time Log Query and Analysis Service.



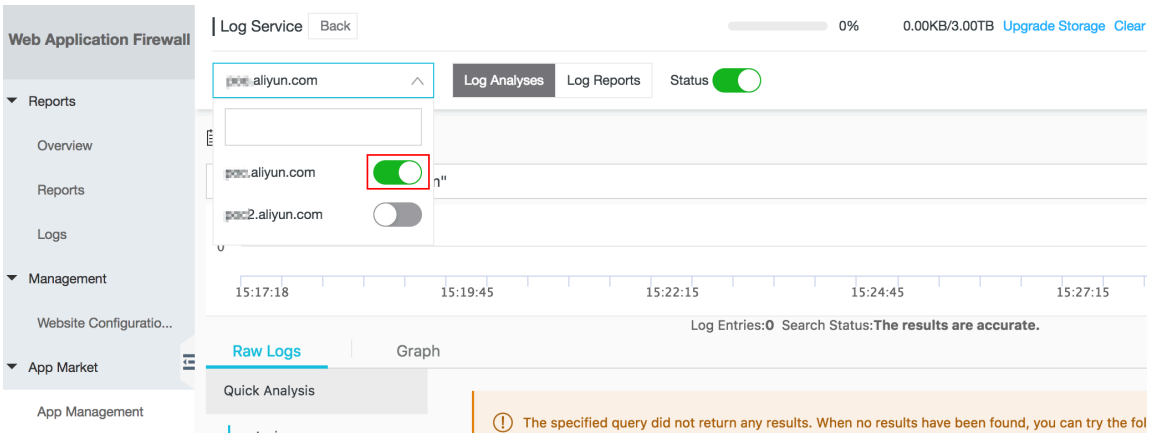
   f. On the Cloud Resource Access Authorization page, click Confirm Authorization Policy.



g. Under Real-time Log Query and Analysis Service, click Configure.



h. In the domain name drop-down box, enable the website you want to enable Log service.



2. Set up the Python environment in ECS.

   Follow these steps to install the Log Service Python SDK in ECS:

   a. Log on to the ECS instance through SSH or the console. For more information, see *Connect to an ECS instance*.

   b. Install Python3, pip and Python SDK of Log Service. For more information on Log Service Python SDK, see *User Guide*.

```
apt - get   update
apt - get   install  - y   python3 - pip   python3 - dev
cd  / usr / local / bin
ln  - s  / usr / bin / python3   python
pip3   install  -- upgrade   pip
```

```
pip install aliyun-log-python-sdk
```

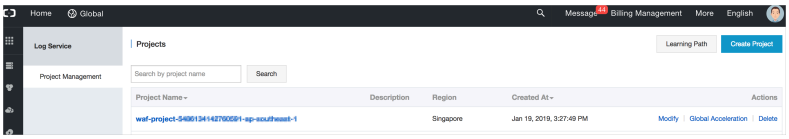
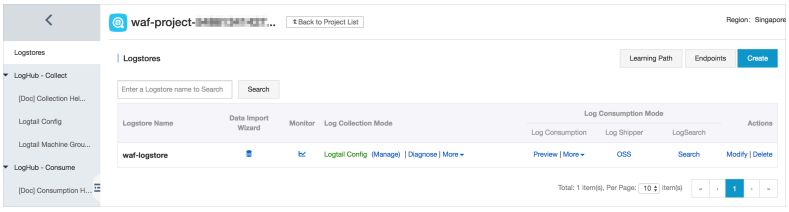
3. Configure Python program to send logs to the syslog server.

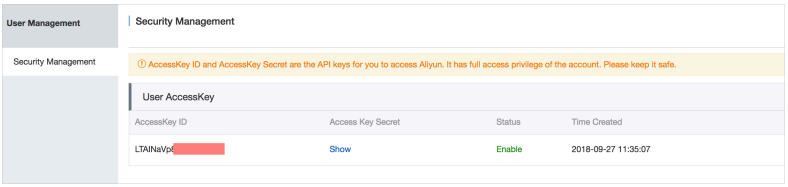
   Follow these steps to configure Python Program to ship WAF logs to the syslog server:

   a. Download the latest example of integration code from *GitHub*:

   ```
   wget https://raw.githubusercontent.com/aliyun/aliyun-log-python-sdk/master/tests/consumer_group_examples/sync_data_to_syslog.py
   ```

   b. Replace Log Service and syslog related settings in Python Program, including:

Parameter	Meaning	Description
SLS Project	Log Service project name	Project is Log Service's resource management unit, used to isolate and control resources. You can find the Project Name in the *Alibaba Cloud Log Service console*. 
SLS Endpoint	Log Service Endpoint	Log Service Endpoint is a URL used to access a project and logs within the project, and is associated with the Alibaba Cloud region where the project resides and the project name. You can find the Endpoint URL in *Service endpoint*.
SLS Logstore	Logstore	Logstore is a unit in Log Service for the collection, storage, and query of log data. Each Logstore belongs to a project, and each project can create multiple Logstores. You can find the Logstore Name under your Log Service Project in the *Alibaba Cloud Log Service console*: 

Parameter	Meaning	Description
SLS accessKeyId and accessKey	AccessKey	AccessKey is a "secure password" designed for you to access your cloud resources by using APIs (not the console). You can use the AccessKey to sign API request content to pass the security authentication in Log Service. For more information, see *AccessKey Introduction*. You can find your Accesskey in the *User Management console*: 
Syslog Host	Syslog Host	Syslog host is same as the IP address/Hostname you access syslog server.
Syslog Port	Syslog Port	Syslog port is a port to receive syslog. UDP uses port 514 and TCP uses port 1468.
Syslog protocol	Syslog protocol	You can specify UDP or TCP to receive syslog, depending on your syslog server setting.
Syslog separator	Syslog separator	Syslog separator is used to separate syslog key-value pairs.

The following is the sample setting in Python Program:

- Log Services

```
endpoint = os . environ . get (' SLS_ENDPOI NT ', ' http
:// ap - southeast - 1 . log . aliyuncs . com ')
accessKeyI d = os . environ . get (' SLS_AK_ID ', ' replace
to your accessid ')
accessKey = os . environ . get (' SLS_AK_KEY ', ' replace
to your accesskey ')
project = os . environ . get (' SLS_PROJEC T ', ' waf -
project - 5486134142 76 ****- ap - southeast - 1 ')
logstore = os . environ . get (' SLS_LOGSTO RE ', ' waf -
logstore ')
consumer_g roup = os . environ . get (' SLS_CG ', ' WAF -
SLS ')
```

- Syslog

```
settings = {
                " host ": " 1 . 2 . 3 . 4 ",
                " port ": 514 ,
                " protocol ": " udp ",
                " sep ": ",",
                " cert_path ": None ,
                " timeout ": 120 ,
                " facility ": syslogclie nt . FAC_USER ,
```

```
                " severity ":  syslogclie  nt . SEV_INFO ,
                " hostname ":  None ,
                " tag ":  None
            }
```

c. Run Python Program. Suppose the Python program is saved as "sync_data_to_syslog.py". You can launch it as:

```
python   sync_data_  to_syslog . py
```

The Python program log shows successfully sent log to remote syslog server.

```
***  start   to   consume   data ...
 consumer   worker  " WAF - SLS - 1 "  start
 heart   beat   start
 heart   beat   result : []  get : [ 0 ,  1 ]
 Get   data   from   shard   0 ,  log   count :  6
 Complete   send   data   to   remote
 Get   data   from   shard   0 ,  log   count :  2
 Complete   send   data   to   remote
 heart   beat   result : [ 0 ,  1 ]  get : [ 0 ,  1 ]
```

You are able to search the WAF log in syslog server now.

8 Use custom rule groups to prevent false positives

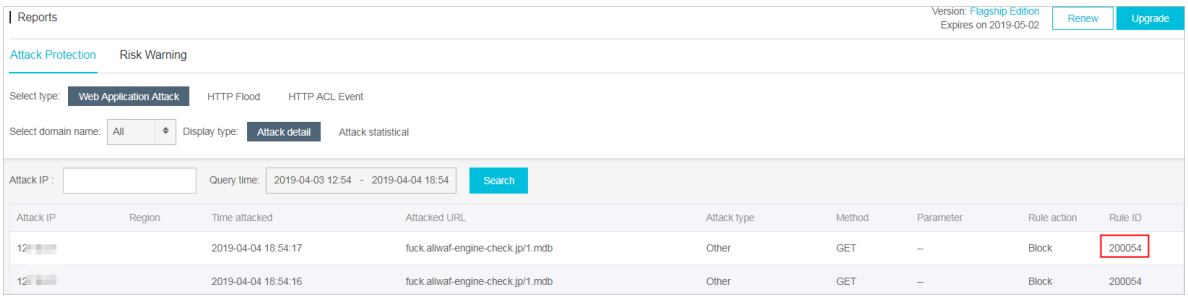
When you find that normal requests to your site are mistakenly blocked by WAF, you can set custom rule groups to prevent this issue.

When a normal request to your site is blocked by WAF, you can identify the rule that causes the issue and create a custom rule group for the affected domain. You can then remove the specified rule to resolve the issue.

> **Note:**
> Before you remove a rule, make sure that the requests blocked according to this rule are normal requests.

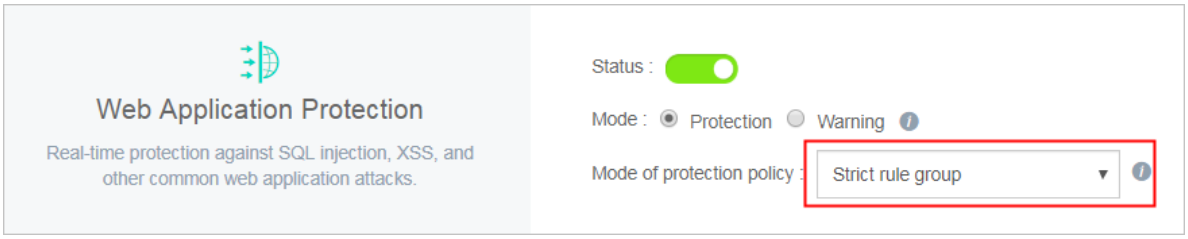
Identify the ID of the protection rule that causes false positives

1. Log on to the *Web Application Firewall console*.
2. Select Mainland China or International.
3. In the left-side navigation pane, choose Reports > Reports and click Attack Protection.
4. Click Web Application Attack and select the affected domain from the drop-down list. Then click Attack Details.
5. You can select a time range or source IP to search for records you are interested in. The record contains the ID of the protection rule that causes false positives.



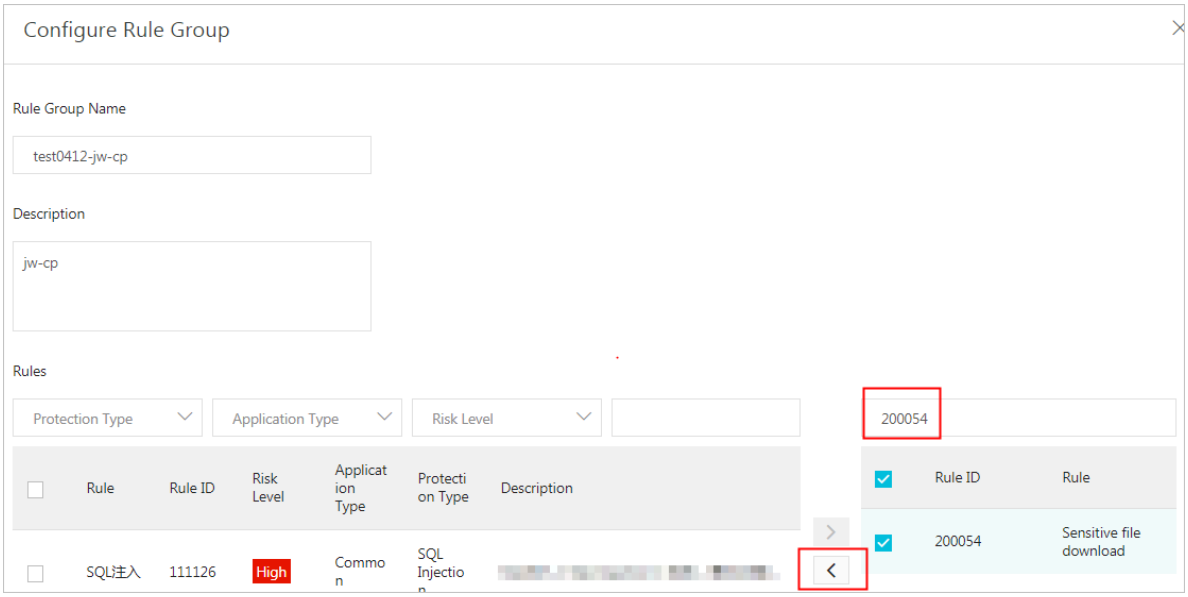
Create custom group rules for a domain

1. In the left-side navigation pane, choose Management > Website Configuration. Select the affected domain and click Policies to view the protection configuration of this domain.



2. In the left-side navigation pane, choose Settings > Custom Rule Groups. Select the rule group associated with the affected domain and click Copy.
3. Enter a rule group name and description. Click OK to create a custom rule group.
4. Select the newly created rule group and click Edit.
5. In the Configure Rule Group dialog box that appears, select the rule that has caused false positives from the rules list on the right side. Click  to remove this rule from the rule group and click Confirm.

> **Note:**
> All protection rules are listed on the left side, and rules in the specified custom rule group are listed on the right side.



6. On the Custom Rule Groups page, select the new rule group, click Apply to Website, and select the affected domain.

After the custom rule group is changed for the affected domain, the same requests sent to your domain are no longer blocked.

Note:
If requests are still blocked, make sure you have identified the right ID of the protection rule that causes false positives and remove this rule from the custom rule group.