Alibaba Cloud
Web Application Firewall

Best Practices

Issue: 20190212

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 informatio n, 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 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.

```
Last login: Tue Jul 31 13:48:10 on ttys000
[                                    1$ telnet 4                  80                    ]
Trying                    5...
Connected to                    5.
Escape character is '^]'.
^ZConnection closed by foreign host.
```

Note

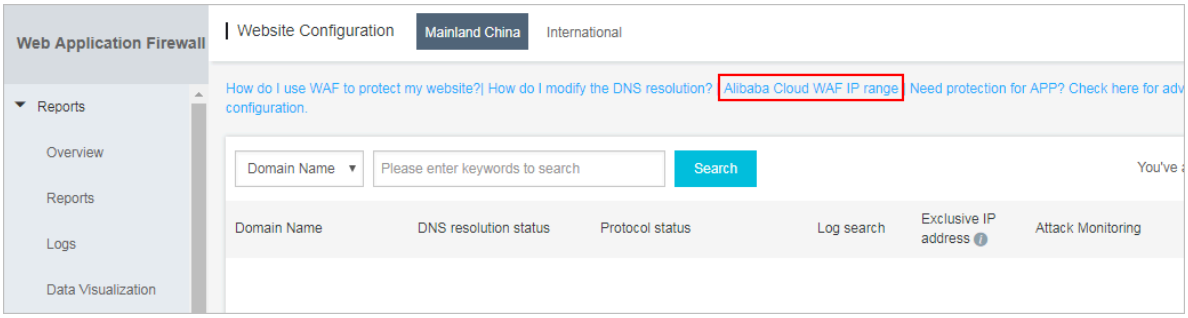
Configuring a security group has certain risks. Consider the following:

- 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

2 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_module --without-http-cache --with-http_ssl_m
odule --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

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

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

```
set_real_ip_from ip_range1;
set_real_ip_from ip_range2;
...
set_real_ip_from ip_rangex;
real_ip_header    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_forwarded_for - $remote_user [$time_local
] "$request" ' '$status $body_bytes_sent "$http_referer" ' '"$
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 *`F5XForwardedFor.dll`* from the *`x86\Release`* or *`x64\Release`* directory (according to the OS version of the server) to a specified directory assumed as *`C:\ISAPIFilters`*, 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:\ISAPIFilters\F5XForwardedFor.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 `F5XFFHttpModule.dll` and `F5XFFHttpModule.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_forwarded_for\x86` and `C:\x_forwarded_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_forwarded_for\x86\F5XFFHttpModule.dll`
   - Register the x_forwarded_for_x64 module
     - Name: x_forwarded_for_x64
     - Path: `C:\x_forwarded_for\x64\F5XFFHttpModule.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

Follow these steps to obtain the visitor's real IP address in Apache.

1. Run the following code to install the third-party module *mod_rpaf* for Apache.

```
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. Modify the Apache configuration file `/alidata/server/httpd/conf/httpd.conf` and add the following information at the end.

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

   Where `RPAFproxy_ips ip address` is not the public IP address provided by Server Load Balancer. You can obtain the specific IP address from the Apache log. Usually two IP addresses are included.

3. Run the following command to restart Apache once you add the IP address.

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

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.AccessLogValve" directory
="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T
" resolveHosts="false"/>
```