

Alibaba Cloud Web Application Firewall

FAQ

Issue: 20190322

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 <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 WAF FAQ.....	1
2 Definitions of common web vulnerabilities.....	7
3 Modify local hosts file to test WAF.....	11
4 DNS resolution status exception.....	13
5 Emergency Mode of HTTP Flood Protection.....	16
6 Why the WAF CNAME address can not be accessed directly?.....	17
7 How do I obtain the real IP of a client?.....	18
8 Product specification for Alibaba Cloud DNS version of WAF.....	20
9 How to fix error 405?.....	22
10 How to fix WAF blackholes?.....	23
11 How to view the WAF back-to-source IP addresses?.....	25
12 HTTPS access exceptions.....	26
13 File upload requests blocked by Alibaba Cloud WAF.....	30
14 How to fix the logon status loss issue?.....	31
15 How to handle ECS intrusion?.....	32
16 HTTPS access exceptions arising from SNI compatibility ("Certificate not trusted").....	35
17 Long connection timeout.....	39
18 WAF troubleshooting manual.....	40
19 WAF back-to-origin CIDR blocks update.....	46

1 WAF FAQ

- *Can servers outside Alibaba Cloud use WAF?*
- *Does WAF support cloud virtual hosts?*
- *How to prevent HTTP flood attacks?*
- *Does WAF support HTTPS?*
- *Does WAF support user-defined ports?*
- *Does the QPS limitation of WAF aim at the QPS summarized by the whole WAF instances or the QPS upper limit for one configured domain name?*
- *Which edition of WAF provides security against malicious SMS?*
- *Can the origin IP address in WAF be set to an internal network IP address of ECS?*
- *Can WAF be connected together with CDN or Anti-DDoS IP?*
- *Can WAF protect IP addresses of multiple origins under one domain name?*
- *How does WAF share load when multiple origins are configured?*
- *Does WAF support health check?*
- *Does WAF support session persistence?*
- *Can there be a delay, when an origin IP address of WAF is being modified?*
- *When does the modified configuration take effect in WAF console?*
- *What is the back-to-source IP address of WAF?*
- *Does WAF automatically add its back-to-source IP addresses to the security group?*
- *Do I need to allow accesses from all client IP addresses to enable WAF back-to-source?*
- *Can the source IP addresses of HTTP flood attacks be viewed in WAF console?*
- *How to query the bandwidth traffic used by WAF?*
- *Does the IP field in HTTP ACL policies of WAF support entry of a network segment?*
- *What are the features of the Anti-DDoS capability provided by WAF?*
- *Does WAF support HTTPS two-way authentication?*
- *Does WAF support Websocket and HTTP 2.0 or SPDY protocol?*
- *Which SSL protocols are supported by WAF?*
- *Can I use different Alibaba Cloud accounts to deploy Alibaba Cloud WAF, CDN, and Anti-DDoS Pro for the same domain name?*
- *Can I use double slashes (//) in the URL matching condition of an HTTP ACL rule?*

- [Can I deploy Alibaba Cloud WAF for websites that enable NTLM \(NT LAN Manager\) authentication?](#)

Can servers outside Alibaba Cloud use WAF?

Yes, WAF can protect any web server/applications that can be accessed through the Internet, whether it is inside or outside Alibaba Cloud. You can protect your web service in AWS, Azure, or any other cloud and data centers.



Note:

Domain names accessed within Mainland China must apply for an ICP license at the Ministry of Industry and Information Technology.

Does WAF support cloud virtual hosts?

The Business and Enterprise editions of WAF support exclusive virtual hosts, which can be configured after WAF is enabled.

Shared hosts use shared IP addresses, which means that the origin is used by multiple users. We recommend that you not to configure WAF separately.

How to prevent HTTP flood attacks?

WAF provides HTTP flood protection in the Normal and Emergency modes. You can switch the protection mode based on the actual situation. For more information, see [Configure the HTTP flood protection mode](#).

For better protection effects and lower false positives rate, you can use the WAF Business Edition or WAF Enterprise Edition, to customize or request the security professional to customize targeted protection policies for you. For more information, see [Customize HTTP flood protection](#).

Does WAF support HTTPS?

Yes, all editions of WAF fully support HTTPS businesses and wildcard domain names.

WAF can handle HTTPS traffic if the SSL certificate and key are uploaded as needed. WAF decrypts the requests, examines the data, and then encrypts them again, before forwarding them back to the origin.

Does WAF support user-defined ports?

The Business and Enterprise editions of WAF support user-defined non-standard ports. The Business version supports up to 10 non-standard ports and the Enterprise version supports up to 50 non-standard ports.

**Note:**

For more information, see [Supported non-standard ports](#).

Does the QPS limitation of WAF aim at the QPS summarized by the whole WAF instances or the QPS upper limit for one configured domain name?

The QPS limitation of WAF is for all WAF instances. For example, if the configuration of your WAF protects three domain names, then the accumulated QPS of the three domain names cannot exceed the upper limit. If the accumulated QPS exceeds the QPS limitation of WAF instances, rate limiting is triggered and packet loss may occur.

Which edition of WAF provides security against malicious SMS?

All editions of WAF provides security against malicious SMS. For more information, see [How to select the WAF edition](#).

Can the origin IP address in WAF be set to an internal network IP address of ECS?

In WAF, traffic is returned to origin through a public network. Direct entry of an internal network IP address is not supported.

Can WAF be connected together with CDN or Anti-DDoS IP?

The WAF is fully compatible with CDN and Anti-DDoS services. Fundamental architecture: Client > Anti-DDoS > CDN > WAF > SLB > Origin

For service combination with Anti-DDoS or CDN, WAF's CNAME must be entered as the origin for Anti-DDoS or CDN. This action turns the traffic towards WAF after it goes through Anti-DDoS or CDN. WAF then returns the traffic to the origin.

For more information, see [Use Anti-DDoS Pro with WAF](#) and [Use CDN with WAF](#).

Can WAF protect IP addresses of multiple origins under one domain name?

Yes. Individual domain protection can hold up to 20 origin IPs. These IPs are separated with commas. If multiple origins are added to one domain, WAF loads balance requests based on the round-robin method, and performs health checks

for all the origins. When WAF fails to get a response from any origin, WAF stops forwarding requests to that origin until it returns to normal.

How does WAF share load when multiple origins are configured?

If you configure multiple origin IP addresses, WAF automatically uses polling to perform a load balance to access requests.

Does WAF support health check?

By default, WAF enables health check. WAF checks the access status of all origin IP addresses. If an origin IP address does not respond, WAF does not forward any requests to the origin IP address until the access status of the IP address is completely recovered.

Does WAF support session persistence?

Yes, WAF supports session persistence. However, you must enable the function by submitting a ticket to the technical support team.

Can there be a delay, when an origin IP address of WAF is being modified?

Not really. Once the origin IP address that is protected by WAF gets modified, the modification is effective within a minute.

When does the modified configuration take effect in WAF console?

Generally, the modified configuration is effective within a minute.

What is the back-to-source IP address of WAF?

You can view the back-to-source IP address on the Management > Website Configuration page of the [Alibaba Cloud WAF console](#). For more information, see [How to View the WAF back-to-source IP address](#).

Does WAF automatically add its back-to-source IP addresses to the security group?

No, WAF does not automatically add its back-to-source IP addresses to the security group. If your origin is deployed with other firewall or host security protection software, we recommend that you manually add the WAF back-to-source IP addresses to the whitelist.

For more information, see [Protect your origin server](#).

Do I need to allow accesses from all client IP addresses to enable WAF back-to-source?

No, because according to your service type you can only allow the WAF back-to-source IP addresses or IP addresses of all clients.

For the Web service, we recommend that you only allow the WAF back-to-source IP addresses to [protect the origin](#).

Can the source IP addresses of HTTP flood attacks be viewed in WAF console?

For the WAF Enterprise edition, you can view the full logs of source IP addresses of HTTP flood attacks on the service analysis page.

How to query the bandwidth traffic used by WAF?

You can view query the used bandwidth traffic on the overview page in the WAF console.

Does the IP field in HTTP ACL policies of WAF support entry of a network segment?

Yes, WAF supports the entry of an IP network segment in the IP field of HTTP ACL policies.

What are the features of the Anti-DDoS capability provided by WAF?

- WAF provides independent IP addresses to each user. These IP addresses are also subject to Anti-DDoS blackhole policies, and are consistent with ECS and Server Load Balancer.
- The blackhole threshold for WAF is the same as the ECS default threshold in the current region.

You can purchase [Anti-DDoS Pro](#) to protect your website against DDoS attacks.

Does WAF support HTTPS two-way authentication?

No. WAF does not support HTTPS two-way authentication.

Does WAF support Websocket and HTTP 2.0 or SPDY protocol?

WAF is already supporting the WebSocket protocol. However, it currently does not support HTTP 2.0 or SPDY protocol.

Which SSL protocols are supported by WAF?

Supported SSL protocols:

- TLSv1

- TLSv1.1
- TLSv1.2

Example of SSL_ciphers suite:

```
" ECDHE - RSA - AES256 - GCM - SHA384 : ECDHE - RSA - AES128 - GCM  
- SHA256 : DHE - RSA - AES256 - GCM - SHA384 : DHE - RSA - AES128 -  
GCM - SHA256 : ECDHE - RSA - AES256 - SHA384 : ECDHE - RSA - AES128  
- SHA256 : ECDHE - RSA - AES256 - SHA : ECDHE - RSA - AES128 - SHA :  
DHE - RSA - AES256 - SHA256 : DHE - RSA - AES128 - SHA256 : DHE - RSA  
- AES256 - SHA : DHE - RSA - AES128 - SHA : ECDHE - RSA - DES - CBC3  
- SHA : EDH - RSA - DES - CBC3 - SHA : AES256 - GCM - SHA384 : AES128  
- GCM - SHA256 : AES256 - SHA256 : AES128 - SHA256 : AES256 - SHA :  
AES128 - SHA : DES - CBC3 - SHA : HIGH :! aNULL :! eNULL :! EXPORT  
:! DES :! MD5 :! PSK :! RC4 "
```

Can I use different Alibaba Cloud accounts to deploy Alibaba Cloud WAF, CDN, and Anti-DDoS Pro for the same domain name?

Yes. You can deploy Alibaba Cloud WAF, CDN, and Anti-DDoS Pro for the same domain name by using different Alibaba Cloud accounts. For example, you can use Alibaba Cloud account A to deploy Alibaba Cloud WAF for your domain name and use another Alibaba Cloud account B to deploy Anti-DDoS Pro for the same domain name to protect against Web attacks and DDoS attacks.

Can I use double slashes (//) in the URL matching condition of an HTTP ACL rule?

No. The Alibaba Cloud WAF HTTP ACL rule processing engine compresses double or multiple forward slashes into a single slash for standard purposes. Therefore, URL matching conditions with double slashes cannot be correctly matched.

We recommend that you replace the double slash in the URL matching condition with a single slash (/). For example, use `/ api / sms / request` instead of `// api / sms / request` to let WAF inspect web requests that contain this URI.

Can I deploy Alibaba Cloud WAF for websites that enable NTLM (NT LAN Manager) authentication?

No. We recommend that you do not deploy Alibaba Cloud WAF for websites that support NTLM authentication. Since the valid web request forwarded by WAF cannot pass the NTLM authentication of the origin server, the client encounters repeated authentication requests.

We recommend that you use other authentication methods for your website.

2 Definitions of common web vulnerabilities

Cross-site attack

Description

Cross-site scripting (XSS) usually occurs at the client's end. Hackers use it to steal private information and passwords, for phishing, and to transmit malicious codes. HTML, JavaScript, VBScript, and ActionScript are the technologies most likely to be hit by the XSS attacks.

An attacker inputs the code that harms the client to the server and uses code to forge a webpage. When a user opens the webpage, the malicious code is injected into the user's browser to mount attacks. The attacker can then steal the session cookies to obtain the user's private information, including passwords and other sensitive information.

Threat

XSS attacks generate no direct harms to web servers, but the attacks spread across the websites to steal the users' sensitive account information and passwords. In this case, it can create severe damage to the websites too. XSS attacks may cause the following damages:

- **Phishing:** The most typical attacks include using the reflexive cross-site scripting vulnerability of the target website to redirect website users to a phishing website, injecting phishing JavaScript to monitor the input of forms on the target website, and mounting more advanced DHTML-based phishing attacks.
- **Hanging Trojans on websites:** Typical attacks include embedding hidden malicious websites through IFrame during cross-site access, redirecting victims to malicious websites, and displaying dialog boxes for malicious websites.
- **Identity theft:** Cookie is used for authenticating the identity of a user when the user loads a specified website. XSS can be exploited to steal the user's cookie and obtain the user's permission to perform operations on the website. If the cookie of a website administrator is stolen, the website will be exposed to severe threats.
- **Stealing website users' information:** After stealing a user's cookie to obtain the user's identity, the attacker can further obtain the user's permission to perform operations on the website and view the user's private information.

- **Spamming:** XSS vulnerabilities are exploited to send lots of unwanted information on behalf of the victim to target user groups in an SNS community.
- **Hijacking of users' web behaviors:** An advanced type of XSS attack hijacks a user's web behaviors to monitor the user's browsing history and sent/received data.
- **XSS worm:** XSS worms can be used to place advertisements, generate traffic, embed Trojan virus on websites, play pranks, corrupt online data, and mount DDoS attacks.

CRLF attack

Description

HTTP response splitting is also called a CRLF injection attack. CR and LF correspond to the carriage return and line feed characters.

An HTTP header consists of multiple lines that are separated by combinations of CRLF characters. Each line is in the structure of "Key: Value". If the CRLF characters are injected into a portion of the value input by the user, the HTTP header structure may change.

Threat

By injecting self-defined HTTP header information (such as session cookie or HTML code), the attacker can start XSS attacks or session fixation vulnerability attacks.

Web SQL injection

Description

Web SQL injection is a security vulnerability that occurs at the database layer of apps. It is widely used to obtain the website control permission illegally.

Poorly designed apps may overlook the check on SQL instructions in input strings. As a result, these instructions are falsely treated as normal SQL instructions and run by the database. When this happens, the database is subject to attacks, leading to data theft, modification, and deletion, or even insertion of malicious code and backdoors into websites.

Threat

SQL injection attacks may cause the following damages:

- Confidential data may be stolen.
- Core business data may be tampered with.

- Web pages may be defaced.
- Database servers may be turned into zombie hosts by attacks, or the enterprise website may even be attacked.

Webshell attack

Description

A webshell attack is an attack structured to write webpage-based Trojan virus into website servers in an attempt to control the servers.

Threat

An attacker may write web-based Trojan backdoors into websites to operate files and run commands on these websites.

Local file inclusion

Description

Local file inclusion is a type of vulnerability that occurs when the app code fails to implement strict control over the processing of include files. As a result, attackers are allowed to run uploaded static files or website log files as code.

Threat

Attackers may exploit this vulnerability to run commands on servers to get server operation permission, causing a series of negative consequences such as malicious deletion of websites and tampering of user and transaction data.

Remote file inclusion

Description

Remote file inclusion is a type of vulnerability that occurs when the app code fails to implement strict control over the processing of include files. As a result, attackers are allowed to construct parameters including remote code for execution on servers.

Threat

Attackers may exploit this vulnerability to run commands on servers to get the server operation permission, causing a series of negative consequences such as malicious deletion of websites and tampering of user and transaction data.

Remote code execution

Description

Remote code execution is a high-risk security vulnerability. It allows an attacker to exploit a server code vulnerability to input and run malicious code on the server.

Threat

Attackers may exploit this vulnerability to run assembled code on servers.

FastCGI attack

Description

FastCGI attack is a severe security vulnerability in Nginx. By default, the FastCGI module may cause servers to incorrectly parse any file types in PHP mode.

Threat

Malicious attackers may destroy a Nginx server that supports PHP.

3 Modify local hosts file to test WAF

Location of the hosts file

C : \ Windows \ System32 \ drivers \ etc \ hosts

Hosts file functionality

The hosts file specifies the correspondence between the domain name and IP address . If a domain name has an IP address specified in the hosts file, the system will not resolve its IP address through the domain name system (DNS) when accessing this domain name, but will directly access the specified IP address instead.

Therefore, if your website is deployed with Anti-DDoS Pro or WAF services, you can modify the local hosts file to direct the website to the WAF without changing the online business flow. This allows you to test whether or not the business services work normally after they pass through WAF.

Procedure

1. Find the IP address allocated by WAF.

When the domain name is configured, WAF generates a CNAME record for resolution purposes. Use the ping command to get the IP address of the CNAME record, and this IP address is the WAF IP. Use `www.abc.com` as an example.

- a. Log on to the [Alibaba Cloud WAF console](#) and go to the Management > Website Configuration page to view the WAF CNAME address.



- b. Use the ping command to get the IP address of the CNAME record.

```
Pinging kg1m0d16s0h7d4hniqdesz5m7ac1ts.aliyuncs.com [112.124.157.116] with
32 bytes of data:
Reply from 112.124.157.116: bytes=32 time=9ms TTL=108
Reply from 112.124.157.116: bytes=32 time=6ms TTL=108
Reply from 112.124.157.116: bytes=32 time=7ms TTL=108
Reply from 112.124.157.116: bytes=32 time=12ms TTL=108
```

2. Locate to the `C : \ Windows \ System32 \ drivers \ etc \` folder.
3. Open the hosts file in Notepad, and point the domain name to the WAF IP address.

The hosts file format is `< IP > < domain name >`. For example, point

`www.abc.com` to `xx . xx . xx . xxx . xx . xx . xx . xxx www . abc . com .`

4. Save the modified hosts file to the `C : \ Windows \ System32 \ drivers \ etc \` folder.

4 DNS resolution status exception

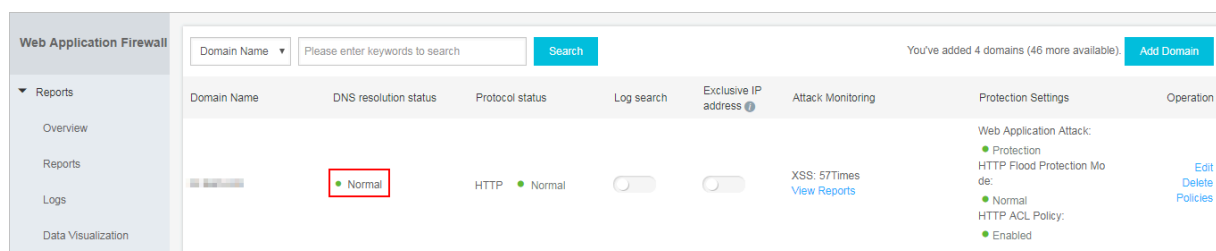
When a website configuration is created in Alibaba Cloud WAF, WAF automatically performs the following checks:

- **Domain to CNAME:** Performed every hour to detect whether the domain name has been resolved to the WAF CNAME address.
- **Web traffic:** Performed every several minutes to detect whether the web traffic to the domain name passes through WAF.

When one of the checks is ok, the DNS resolution status is **Normal**, which indicates that Alibaba Cloud WAF is perfectly implemented for the website.

To view the DNS resolution status, log on to the [Alibaba Cloud WAF console](#) and go to the **Management > Website Configuration** page.

The Normal status displays as follows.



If the DNS resolution status is **Exception**, then Alibaba Cloud WAF may not be correctly configured. This topic explains how does WAF determine the DNS resolution status and lists common exception statuses.

How does WAF determine the DNS resolution status

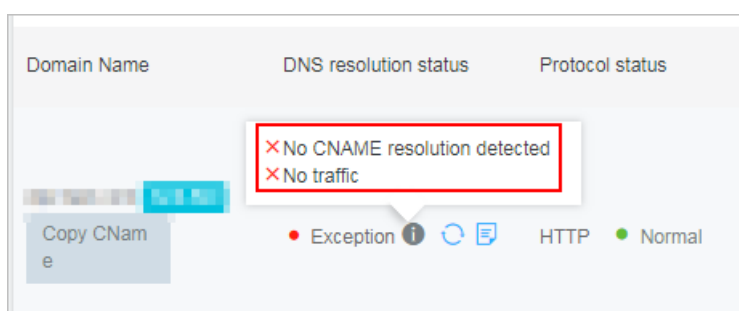
Alibaba Cloud WAF determines the DNS resolution status by the following conditions. When one of the conditions is met, the DNS resolution status is normal.

- **Condition A:** The domain name is resolved to the WAF CNAME address.
- **Condition B:** Web traffic of the domain name passes through WAF. When at least 10 requests are detected in the last five seconds, it is ok. Two or three requests per minute are regarded as no traffic. To view the history of web traffic, you can check the Attack protection report of HTTP flood. For more information, see [Attack protection reports](#).

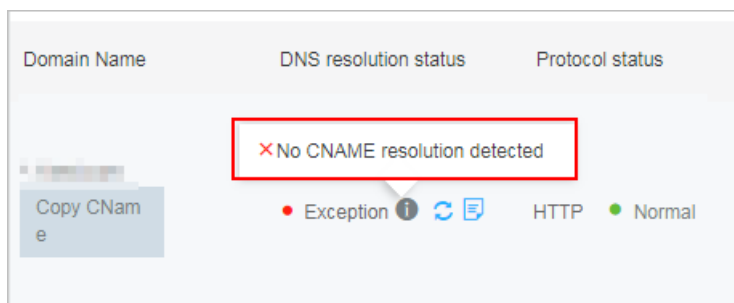
We recommend that you use a CNAME record to redirect web traffic to WAF. Using CNAME supports node switch or even redirecting traffic back to the origin in case of node failure or machine failure, which improves your business' s availability and failure recovery capacity. If CNAME record conflicts with your current DNS settings, you can use an A record to do traffic redirection.

Common exception statues

- For a fully qualified domain name (FQDN, such as example.abc.com), if both the Domain to CNAME and Web traffic checks fail, the exception status displays as follows.



- For a wildcard domain name (for example, *.abc.com), the exception status displays as follows.



- When the website is deployed with CDN or other proxy servers in front of WAF, the domain name is resolved to CDN and other proxy servers rather than WAF. As a result, the Domain to CNAME check fails. In addition, the CDN-returned traffic received by WAF is low, which may result in the Web traffic check fails. In this case, the exception message does not definitely indicate that WAF is ill-configured.

For more information about how to deploy WAF and CDN together, see [Deploy WAF and CDN together](#).

Manually test if WAF is working

- Visit a domain name that is configured in Alibaba Cloud WAF, for example, `www.aliyundemo.cn`. The webpage can be accessed normally.

2. Add the `/ alert (xss)` string to the end of the domain name to assemble a testing URL and visit this URL (in this example, `www . aliyundemo . cn / alert (xss)`). If you receive a 405 page telling you that this request is blocked by Alibaba Cloud WAF, then WAF is protecting the website.

5 Emergency Mode of HTTP Flood Protection

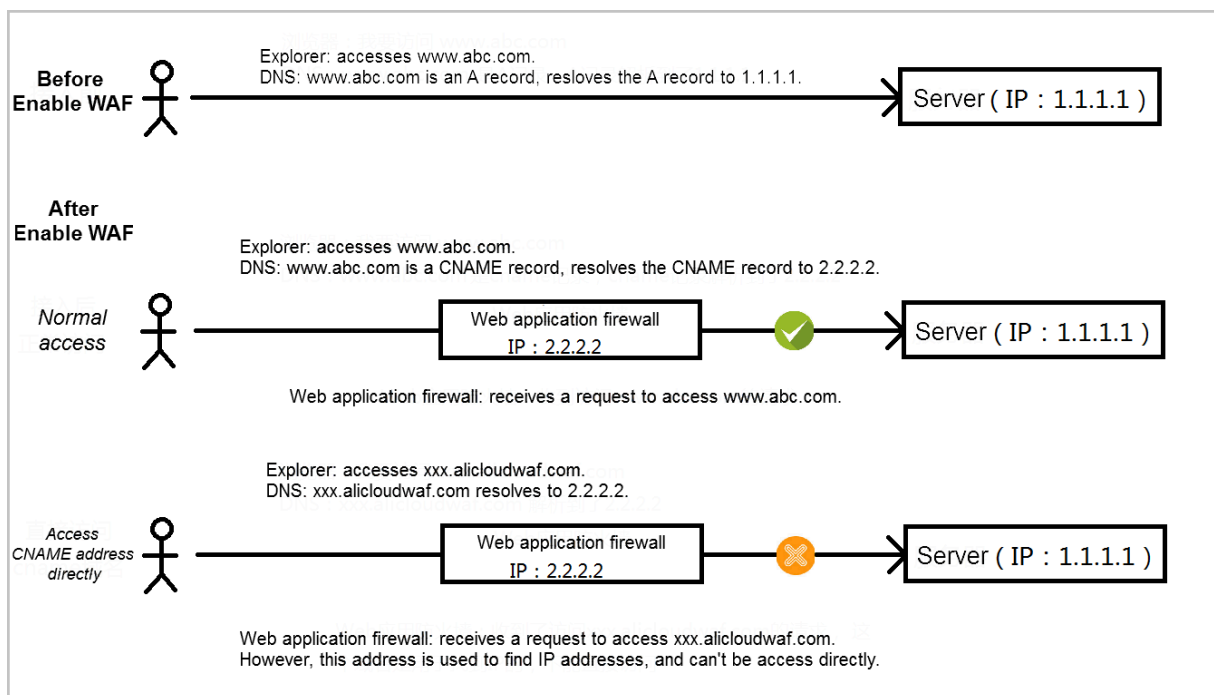
When normal mode fails to mitigate a large-volume and sophisticated HTTP flood, you can enable the emergency mode of HTTP flood protection.

By default, HTTP flood protection is set to the normal mode in protection against common HTTP floods. WAF then mitigates HTTP floods normally. In case the origin CPU rises, or loses response from the database or application, you must activate the emergency mode.

The Emergency mode may cause false positives to legitimate traffic. We recommend that you choose the Business or Enterprise Plan for the customized HTTP flood protection policies.

6 Why the WAF CNAME address can not be accessed directly?

The CNAME domain name generated by WAF or Anti-DDoS Pro is used for DNS resolution and cannot be directly accessed.



If you access the CNAME directly, a 504 error page may occur.

7 How do I obtain the real IP of a client?

When an HTTP request goes through a layer-7 proxy, the source IP of this packet is modified with the proxy IP, instead of the real IP of the client (client IP). Practically, the client IP is often written into the x-forwarded-for field in the HTTP head field, as shown in the following figure.

The Alibaba Cloud WAF works as follows.

Suppose that WAF protects the domain “www.abc.com”. Generally, packets from the client follow the Client browser > WAF > Origin server (Apache/Nginx/IIS and so on) path. In this architecture, WAF acts as a reverse proxy between the client and the origin server.

However, in a network architecture containing multiple proxies (for example, CDN and Anti-DDoS Pro), multiple IP addresses get added to the x - forwarded - for field. This is because each proxy adds on the client IP, or the last proxy IP.

Therefore, the x - forwarded - for field may appear as X - Forwarded - For : Client IP , Proxy 1 , Proxy 2 , Proxy 3 , ... However, the client IP still occupies the first address position in the x-forwarded-for field.

Procedure

Follow these steps to obtain the real IP address of a client:

1. Send a request command for the x - forwarded - for field content.

The following are examples of request commands for several common languages.

- For ASP

```
Request . ServerVariables (" HTTP_X_FORWARDED_FOR ")
```

- For ASP.NET(C#)

```
Request . ServerVariables [" HTTP_X_FORWARDED_FOR "]
```

- For PHP

```
$ _SERVER [" HTTP_X_FORWARDED_FOR "]
```

- For JSP

```
request . getHeader (" HTTP_X_FORWARDED_FOR ")
```

2. Separate the output `x - forwarded - for` with commas. The first derived IP address is the client IP.

8 Product specification for Alibaba Cloud DNS version of WAF

The following table lists product specifications for the Alibaba Cloud DNS version of WAF:

Product parameter	Description	DNS version
HTTP	Supports HTTP (80) port	Supported
HTTPS	Supports HTTPS (443) port	Not supported
Data centers outside cloud	Supports websites outside Alibaba Cloud	Supported
Basic Web application protection	Protects against common Web attacks such as SQL injection and command execution	Supported
0day vulnerability defense	Quickly protects against the latest Web vulnerabilities	Supported
Service availability	Protects the data center where the server is deployed	Supports single data center
Custom Web protection policies	Customizes Web protection policies for websites	Not supported
Custom HTTP flood protection policies	Provides security professionals to customize protection rules for specific service interfaces	Not supported
HTTP flood protection threshold	Maximum attack requests per second that can be defended	1,000
HTTP ACL policies	Number of rules for access control that can be added	5 (IP/URL)
Number of protected domain names	Number of domain names that can be protected	2
Daily QPS threshold	Normal requests per second	100

Bandwidth threshold	Maximum bandwidth per second (Mbps)	10 (origins outside Alibaba Cloud) 200 (origins inside Alibaba Cloud)
Number of back-to-source IP addresses	Maximum number of IP addresses that are passed back to the origin at the same time for the same domain name	2
Custom requirement	Supports various custom requirements	Not supported

If the product specifications of the DNS version cannot fit your requirements, you can upgrade the service in the console.

9 How to fix error 405?

Once you deploy WAF, a 405 error is reported if you try to access any URL that can pose a security threat to your website and access to that URL is denied.

However, if you confirm the access to a few URLs is a normal business request, you can [Configure HTTP ACL policy](#) to add access rules. This allows access for specific URLs or source IP addresses.

10 How to fix WAF blackholes?

What is a blackhole

When Web Application Firewall (WAF) suffers heavy-traffic DDoS attack that is beyond the free-protection capability of Anti-DDoS Basic, WAF is thrown into a blackhole.

After a WAF IP address is thrown into the blackhole, all traffic that flows through WAF (normal access or attack) is blocked, which means that during the blackhole period, you cannot access any domain names protected by the WAF instance.



Note:

If a site is thrown into a blackhole, it can only be recovered after the blackhole period is over. The default blackhole period lasts for 150 minutes. The WAF blackhole threshold is the same as the default threshold of the region where the ECS is located.

For more information about the blackhole and blackhole policies, see [Alibaba Cloud blackhole policies](#).

How to avoid a blackhole

By default, each WAF instance allocates an exclusive IP address to you. Once this WAF IP address is thrown into the black hole, none of the domain names protected by this WAF instance can be accessed during the black hole period. To avoid this, you can purchase an additional [Exclusive IP](#) address for an important domain name. In this case, this important domain name is not affected by other domain names under DDoS attacks.



Note:

The best solution to heavy-traffic DDoS attacks is to use [Anti-DDoS Pro](#) to protect your domain names.

WAF black hole FAQ

My WAF is thrown into a blackhole. Can you recover it immediately?

The blackhole is a service that Alibaba Cloud purchases from the operator who imposes strict restrictions on the time and frequency to trigger a blackhole.

Therefore, you cannot manually deactivate the blackhole state, rather you have to patiently wait for the system to automatically free the server.

In fact, even if the blackhole is deactivated immediately, it gets triggered again if the WAF is still under heavy-traffic DDoS attack.

How do I know the specific domain name that is under attack when the WAF is configured with multiple domain names?

Generally, the hacker resolves a WAF protected domain name to obtain the WAF instance's IP address, and then starts the DDoS attack against this IP address. Heavy-traffic DDoS attacks are targeting at a WAF IP address. We cannot figure out the domain name that is under attack, based on the traffic.

However, you can use the domain name split method to find out the domain name that is under attack. For example, you can resolve some of the domain names to WAF, and the rest to some other places (ECS origin, CDN, or SLB). If the WAF is no longer in the blackhole, it means that the hacker's target lies in the domain names that are resolved to other places. However, this operation is relatively complex and may expose the origin and other assets, which may lead to a greater security issue. Unless necessary, do not use this method to find the domain name that is under attack.

Can you help change the WAF IP address so that my WAF is not thrown into the blackhole?

Changing the WAF IP address does not resolve the problem. A hacker can obtain your new IP address by pinging your domain name and can start another DDoS attack. So, changing your IP address will not be of much help.

Is there any difference between a DDoS attack and an HTTP flood attack? Why cannot WAF defend against DDoS attacks?

Heavy-traffic DDoS attacks are layer 4 attacks against IP addresses; while HTTP flood attacks are layer 7 attacks (for example, HTTP GET/POST Flood).

WAF can defend against HTTP flood attacks. However, in the case of heavy-traffic DDoS attacks, it requires sufficient bandwidth resources to take over all traffic to perform the traffic cleaning. Therefore, you can only count on protection from Anti-DDoS Pro.

11 How to view the WAF back-to-source IP addresses?

To avoid your WAF's back-to-source IP addresses from being blocked or slowed down by the origin, you can add the WAF's back-to-source IP addresses to the whitelist of your origin's security group, firewall, or other host security protection software.

Follow these steps to view the WAF's back-to-source IP address segment.

1. Log on to the [Web Application Firewall console](#).
2. Go to the Management > Website Configuration page.
3. Click Alibaba Cloud WAF IP range in the upper corner of the page.

You can add the WAF back-to-source IP address segment to the whitelist of your origin server's security group, firewall or other host security protection software, to deploy protection for your origin server. For more information, see [Protect origin](#).

12 HTTPS access exceptions

This topic provides troubleshooting methods for HTTPS access exceptions after the website is connected to WAF (HTTP access is normal). The symptoms include failure to open the page, the system prompts that the certificate cannot be trusted, failure to call some ports, and access errors for certain machine types, operation systems, and Apps.

HTTPS enabled and certificate uploaded?

When using WAF to protect HTTPS services, you must select HTTPS in the WAF console and upload the certificate/key that is exactly the same as that of the server. Even when WAF is used in sync with Anti-DDoS Pro, SLB, CDN, and other products, you must upload the certificate/key in the WAF console. WAF certificate is independent of other products.



Note:

Once you upload the certificate in the console, it may take up to five minutes for the configuration to be effective. During this period, you may still encounter access exceptions. You can [bind hosts](#), and switch DNS resolution once WAF is configured and effective.

Is certificate chain complete?

In most cases, the certificate service provider provides you with multiple certificates (including the server certificate and one or more CA root certificates), which together form a complete certificate chain. Taking Alibaba Cloud certificate as an example, the certificate chain you may receive is shown in the following figure.

 **Certificate Chain Complete?**

All of the correct Intermediate CA Certificates are installed. Your SSL certificate is installed correctly and should be supported in all the major web browsers without problems.



Common name: *.aliyun.com
Organization: Taobao(China) Software Co., Ltd
Valid from May 23, 2016 to July 22, 2017
Issuer: Symantec Class 3 Secure Server CA - G4

↓



Common name: Symantec Class 3 Secure Server CA - G4
Organization: Symantec Corporation
Valid from October 31, 2013 to October 30, 2023
Issuer: VeriSign Class 3 Public Primary Certification Authority - G5

↓



Common name: VeriSign Class 3 Public Primary Certification Authority - G5
Organization: VeriSign, Inc.
Valid from November 08, 2006 to July 16, 2036
Issuer: VeriSign Class 3 Public Primary Certification Authority - G5

Make sure that you upload the complete certificate chain in WAF (as shown in the preceding figure). Also, pay attention to the sequence of the certificate when you upload them. Such as the server certificate must be at the top, and the root certificate must be at the bottom and, combine text content of the multiple certificates. The following is an example of the certificate content you need to upload.

```
----- BEGIN    CERTIFICAT  E -----
MIIFdDCCBF      ygAwIBAgIQ  Fmr88Z0mn6  rEleGaC6UV  EzANBgkqhki
iG9w0BAQsF      ADCB
Obc3E + 7h0u6cUXaQ  AmFNZ2a ...
----- END    CERTIFICAT  E -----
----- BEGIN    CERTIFICAT  E -----
MIIFYjCCBE      qqAwINMTYw  NjA3MDAwMD  AwmLTaWduL  CBJbmMuMRL
nN5bWNiLmN      vbS9
wY2EzLWc1L      m1hbnRlY1B  LSS0yLTU ...
----- END    CERTIFICAT  E -----
----- BEGIN    CERTIFICAT  E -----
MIIG / TCCBeWgAwI  BAGIQLMUH0  3pBzhUCrOR  0SsKM + DANBgkqhki
G9w0BAQsFA      DB +
NzIDMgUHVi      bGljIFByaW  1 ...
----- END    CERTIFICAT  E -----
```

If the certificate chain is incomplete, the page may prompt that the certificate cannot be trusted, and some Android mobile phones, operation systems, or Apps

may encounter access errors or exceptions (the access may be normal in some environments).

You can also use third-party inspection tools available on the Internet (for example, [GeoCerts™ SSL Checker](#)) to check if the current certificate chain is complete.



Note:

This method can only check the domain name status that can be resolved. If you already resolve the domain name to the origin rather than WAF, you cannot check the certificate status in WAF.

SNI Problem

If only some specified clients or applications cannot normally access the HTTPS service, the system prompts “SSL handshake failed/error” , or “the certificate cannot be trusted” , it may be because the client does not support SNI. These clients or applications may be old Android devices, calling programs (especially programs using SSL protocol) developed with an older version of JAVA, IE browser running on a Windows XP, some old version mobile phones, and some third-party payment callback interfaces.

Currently, most browsers, applications, and WeChat and Alipay callback interfaces support SNI. It may be the SNI compatibility problem if the access returns to normal when you resolve the domain name to the origin, and you encounter exceptions if you resolve the domain name to the WAF. You can upgrade the client, or directly resolve the callback interface to the origin.

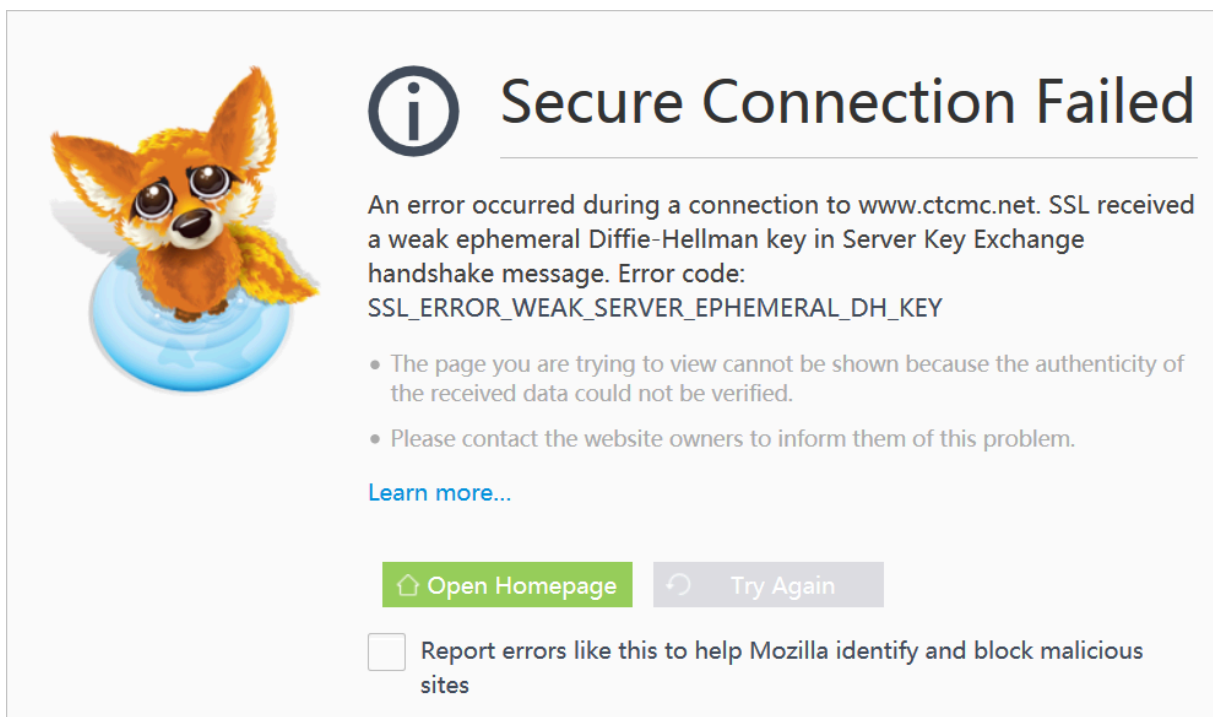
For more information, see [HTTPS access exceptions arising from SNI compatibility \(Certificate not trusted\)](#).

Windows Server 2003/IIS6 server

Access HTTPS service from Windows Server 2003 or IIS6 server that is connected to WAF may cause a white screen or 502 error. Because the TLS version and encryption suite of these systems are too old, the security performance is too weak, and it is not compatible with WAF’ s default HTTPS back-to-source algorithm. WAF does not support HTTPS back-to-source requests for Windows Server 2003, and Microsoft officially suggests not to use Windows Server 2003 to build HTTPS sites. For your communication security, we recommend that you upgrade your operating system to Windows Server 2008 or later.

Link failure caused by short DH key

Short DH (Diffie-Hellman) keys are known for security problems. WAF does not support short keys anymore. Likewise, you can see similar errors when you use a later version of the Firefox browser (for example, 51.0.1) to access the origin, even when you are not using WAF.



We recommend that you upgrade the related components (such as JDK version), to make sure that the server's DH key algorithm is 2048 bits or more.



Note:

Length of a key is determined by the server's encryption algorithm, and has nothing to do with the certificate. If you do not know how to operate, contact your server developer, or search for the related solutions. You can find the related solutions based on the following error messages: `SSL routines : ssl3_check_cert_and_algorithm : dh key too small`.

HTTP enabled for services requiring HTTP redirect?

If you have set on the origin to force redirect HTTP access requests to HTTPS, then you must select both HTTP and HTTPS in WAF. Otherwise, these HTTP requests cannot be normally forwarded to the origin after they are redirected to WAF, and the system throws an error.

13 File upload requests blocked by Alibaba Cloud WAF

Symptoms

When a client uses the POST method to upload files from a browser, they may receive the 405 error telling that the request was blocked by Alibaba Cloud WAF.

Causes

When a client uses the POST method to upload a file, the file content will be transcoded and added to the POST body. Therefore, Alibaba Cloud WAF also inspects the file content. In case the file content contains sensitive keywords, Alibaba Cloud WAF regards the request as malicious code and intercepts the request.

Resolution

Currently, no active measure is available to avoid such false positives caused by transcoded files. We recommend that you create an HTTP ACL rule to allow the client request.

14 How to fix the logon status loss issue?

Symptoms

Some sites may encounter loss of logon status or other exceptions related to the logon status when using WAF. Root causes of these exceptions include the following:

- The domain name has multiple origins (ECS), but does not synchronize the sessions, especially in architectures where an SLB is attached after WAF.
- Failure to obtain the real IP address from X-forwarded-for for validation.

Resolution

- Configure session synchronization for the server.
- If the WAF is connected to an SLB, you can use the layer-7 HTTP method to forward the traffic, and enable the cookie-based session persistence.
- Obtain the real IP address from x-forwarded-for.

For more information, see [Obtain the visitor's real IP address](#).

15 How to handle ECS intrusion?

The ECS instances can still encounter intrusion, even after being protected by WAF. It may be caused because of the following:

No.	Causes	Resolution
1	The ECS instance is intruded before it is connected to WAF. In this case , you must first clean up the ECS instance.	Perform a server cleanup as described in the following sections.
2	When the DNS resolution is not updated once WAF is configured. This makes the traffic flow directly to ECS, without letting it pass through WAF.	Make sure that DNS resolution is updated so that the website is under the protection of WAF. For more information, see Implement Alibaba Cloud WAF .
3	Before WAF is used, the IP address of the ECS instance is disclosed and no security group is configured. As a result, hackers directly attack the ECS instance through its IP address.	Configure a security group to prevent attacks that can bypass WAF. For more information, see Protect your origin server .
4	Other sites that are not protected by WAF exist on the ECS instance. The ECS instance is consequently affected by attacks targeting these sites.	Make sure that all HTTP services on the ECS instance are protected by WAF.
5	The ECS instance encounters non-Web-attack intrusions, such as the brute crack of the ssh password.	Make sure that the ECS instance and database adopt strong passwords.



Notice:

Before clearing Trojans and viruses, first [Create a snapshot](#) to back up data to avoid data loss arising from operation mistakes.

Clear Trojans and viruses

1. Check the network connection by using `netstat` and analyze if any suspicious requests exist. If yes, stop the ECS instance.
2. Use antivirus software to scan and clean viruses.

Run the following command to clear Trojans in Linux.

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

Check and fix vulnerabilities for your ECS instance

1. Check if the server account is normal. If the server account is abnormal, stop the ECS and delete the abnormal account.
2. Check if the remote logon to ECS exists. If yes, set up a strong logon password that contains more than 10 characters and consists of uppercase and lowercase alphabets, digits, and special characters.
3. Confirm that the backend passwords of Jenkins, Tomcat, PhpMyadmin, WDCP, and Weblogic are strong passwords. You can disable the management port 8080, if the services are not in use.
4. Check for vulnerabilities for Web applications, such as struts and Elasticsearch. Make sure that the website is protected by WAF. We recommend that you use Server Guard for Trojans and viruses clearing and patches installation.
5. Check if the following vulnerability exists: the Jenkins administrator runs commands remotely without using a password. If yes, set a password or close the page for managing the 8080 port.
6. Check if the following vulnerability exists: files can be written on Redis without using a password. Check if SSH logon key files created by hackers exist under /root/. If the files exist, delete the files. Modify Redis to make users access Redis using passwords and configure stronger passwords. If access to public networks is not required, use `bind 127.0.0.1` to only allow local access.
7. Check MySQL, SQLServer, FTP, and Web management backend for which passwords are set and make sure you set strong passwords.

Enable Alibaba Cloud Security services

- Make sure that WAF is enabled for all websites on the ECS instance.

- Use Alibaba Cloud Security Threat Detection Service for host scanning, Trojans scanning and clearing, and fixing vulnerabilities.

Reinitialize the cloud disk

If the preceding methods cannot help you fix the problem, we recommend that you reinitialize your cloud disk to restore the system disk or the data disk to the status when they were created.

For more information, see [Reinitialize a cloud disk](#).



Notice:

Before re-initializing the cloud disk, download and back up the data on the system disk and data disk to your local storage. After initialization, perform antivirus for the data and then upload it to your cloud storage.

When the cloud disk is reinitialized, perform the preceding cleanup and enable Alibaba Cloud Security.

16 HTTPS access exceptions arising from SNI compatibility ("Certificate not trusted")

Background

The objective of introducing virtual host on the HTTP server is to make the multiple domain names reuse one IP address to balance the supply of IPv4 addresses. The server can allocate requests to different domain names (virtual hosts) to process according to the hosts specified in client requests. On an HTTPS server where the IP address is shared by multiple domain names (virtual hosts), when the browser accesses an HTTPS site, an SSL connection is established first with the server. The first step to establish an SSL connection is to request a certificate from the server. The server sends a certificate irrespective of the domain names. This is because the server cannot determine the domain name accessed by the browser.

Server name indication (SNI) is an SSL/TLS extension that is used to resolve the issue of a single server using multiple domain names and certificates. Before the server is connected to establish an SSL connection, the domain name (host name) of the site to be accessed is sent first, so that the server returns an appropriate certificate based on the domain name.

Now, most operating systems and browsers support SNI extension. This function is embedded in OpenSSL 0.9.8 and Nginx of the new version also supports SNI.

Symptoms

When the client does not support SNI, the HTTPS access may become abnormal when you access WAF.

When a browser that does not support SNI is used to access a website that uses WAF, the WAF does not know the domain name requested by the client therefore, it cannot retrieve the corresponding virtual host certificate to exchange with the client. The Web application firewall can only use an embedded default certificate to perform the handshake with the client. In this case, the browser of the client displays a message “Certificate not trusted” .

If the client does not support SNI, the following symptoms may occur:

- On the mobile App client, the iOS client can be normally accessed but the Android client cannot be normally opened.
- The browser displays a message indicating the certificate is untrusted after a Web page is opened.

Resolution

Capture the SSL handshake packet on the client to determine whether the client supports SNI. Assume that the Chrome browser is used to access the official website of Alibaba Cloud.

If SNI extension can be seen in the Client Hello packet as illustrated in the following figure, the client supports SNI extension.

10	2017-10-13	15:11:29.437474	30.11.231.69	140.205.172.20	TCP	54 443	63097 → 443 [ACK] Seq
11	2017-10-13	15:11:29.438797	30.11.231.69	140.205.172.20	TLSv1.2	256 443	Client Hello
12	2017-10-13	15:11:29.452188	140.205.172.20	30.11.231.69	TCP	60 63097	443 → 63097 [ACK] Seq
13	2017-10-13	15:11:29.452410	140.205.172.20	30.11.231.69	TLSv1.2	1506 63097	Server Hello
14	2017-10-13	15:11:29.452700	140.205.172.20	30.11.231.69	TLSv1.2	1506 63097	Certificate[TCP segme
15	2017-10-13	15:11:29.453209	30.11.231.69	140.205.172.20	TCP	54 443	63097 → 443 [ACK] Seq


```

  > Cipher Suites (14 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 124
  > Extension: Unknown 6682
  > Extension: renegotiation_info
  > Extension: server_name
    Type: server_name (0x0000)
    Length: 19
    > Server Name Indication extension
      Server Name list length: 17
      Server Name Type: host_name (0)
      Server Name length: 14
      Server Name: www.aliyun.com
  > Extension: Extended Master Secret
  > Extension: SessionTicket TLS
  
```

Otherwise, the client does not support SNI extension. For clients that do not support SNI,

- We recommend that you upgrade the browser or try using later version of the browsers such as Chrome and Firefox.
- For third-party callbacks from WeChat and Alipay, use the IP address of the origin to bypass the Web application firewall.

SNI compatibility



Note:

SNI is compatible with TLS1.0 and later versions but not supported by SSL.

- SNI supports the following desktop browsers:
 - Chrome 5 and later versions
 - Chrome 6 and later versions (Windows XP)
 - Firefox 2 and later versions
 - IE 7 and later versions (running in Windows Vista/Server 2008 and later versions , IE of any version in Windows XP OS not supporting SNI)
 - Konqueror 4.7 and later versions
 - Opera 8 and later versions
 - Safari 3.0 in Windows Vista/Server 2008 and later versions or Mac OS X 10.5.6 and later versions
- SNI supports the following libraries:
 - GNU TLS
 - Java 7 and later versions (serving as the client only)
 - HTTP client 4.3.2 and later versions
 - libcurl 7.18.1 and later versions
 - NSS 3.1.1 and later versions
 - OpenSSL 0.9.8j and later versions
 - OpenSSL 0.9.8f and later versions (flags must be configured)
 - QT 4.8 and later versions
 - Python3, Python 2.7.9 and later versions
- SNI supports the following mobile browsers:
 - Android Browser on 3.0 Honeycomb and later versions
 - iOS Safari on iOS 4 and later versions
 - Windows Phone 7 and later versions
- SNI supports the following servers:
 - Apache 2.2.12 and later versions
 - Apache Traffic Server 3.2.0 and later versions
 - HAProxy 1.5 and later versions
 - IIS 8.0 and later versions
 - lighttpd 1.4.24 and later versions
 - LiteSpeed 4.1 and later versions
 - Nginx 0.5.32 and later versions

- **SNI supports the following command lines:**
 - **cURL 7.18.1 and later versions**
 - **wget 1.14 and later versions**

17 Long connection timeout

Symptoms

In some service scenarios, when a client submits a request, the server returns a response after more than 60s for processing. The server does not exchange any data with the client during the processing.

For example, you upload an Excel file on the Web page, requiring the server to process data in the file (the processing time is about 3 minutes). Within 120s after the file is submitted, no data (HTTP or TCP packet) is exchanged between the client and the server. In this case, WAF returns a 504 timeout response to the client and disconnects the connection.

This is because WAF does not maintain a long connection that lasts more than 120s (without any data exchange) and this Layer 7 timeout interval (120s) cannot be modified.

Resolution

We recommend that you modify the exchange mode of the request so that some data (such as Ack packet, heartbeat packet, and keep-alive packet that can maintain the session) can be exchanged for long connections within 60s.

Considering the diversity of user scenarios, code-level modification suggestions are not provided. You must make adjustments according to your service features.

18 WAF troubleshooting manual

This topic describes the symptoms, issues and provides the solution for the critical problems that arise when a domain name that accesses WAF encounters any abnormal access.

Tools

- **Chrome browser - Developer tool:** The developer tool provided by the Chrome browser can be conveniently used to view loading of page elements. Press F12 to open the tool and switch to the Network tab.
- **ping:** The ping test tool provided by Windows and Linux operating systems can be used to analyze and determine network faults. In the Windows OS, you can press Win+R and enter CMD to open the tool. Usage: `ping domain name / IP address`.
- **tracert (Linux)/tracert (Windows):** The link tracing tool can be used to detect the hop where the data loss occurs. In the Windows OS, press CTRL+R and enter cmd to open the tool. Usage: `tracert - d domain name / IP address`.
- **nslookup:** This tool can be used to detect whether domain name resolution is functional. In the Windows OS, press CTRL+R and enter cmd to open the tool. Usage: `nslookup domain name`.

Troubleshooting methods

Check if the origin is normal

Follow these steps to bypass WAF and verify if the problem lies in the origin.

1. Disable the security group, blacklist, whitelist, firewall, dongle, and cloud lock on the origin to prevent the WAF IP address from being added in the blacklist.
2. Modify the local hosts file and direct the domain name to the public network IP address (the origin IP address specified on WAF) of the corresponding ECS, SLB, or server.
3. Check if the problem still occurs without WAF.

Check if the access request is intercepted falsely

Follow these steps to adjust the protection policy to check if the access request is intercepted falsely.

1. Log on to the [Alibaba Cloud WAF console](#).
2. Go to the Management > Website Configuration page.
3. Find the domain name with abnormal access and click policies under the Operation list.
4. Disable Web Application Protection and check if the problem persists. If the problem disappears,
 - We recommend that you [Configure the Web Application Protection policy](#) to Loose.
 - You can also analyze the URL, and use [HTTP ACL Policy](#) to add a new rule to allow access from normal URLs.
5. If the problem still exists, disable HTTP Flood Protection and check if the problem persists. If the problem disappears,
 - We recommend that you [Configure the HTTP Flood Protection mode](#) to Normal.
 - You can also analyze the URL or IP address, and use [HTTP ACL Policy](#) to add a new rule to allow access from normal URLs or IP addresses.

Common problems about WAF

If the problem continues to appear when WAF is connected and discontinues when WAF is disconnected, the following procedure can troubleshoot such issues.

Access blocked (405 error)

Symptoms

The page indicating the access is blocked is displayed and 405 is returned in the response.

Causes

Possible causes include:

- The access is blocked because of HTTP ACL policy.
- The access is blocked because of Web Application Protection.

Resolution

1. Log on to the [Web Application Firewall console](#).
2. Go to the Management > Website Configuration page.
3. Find the domain name with abnormal access and click policies under the Operation list.

4. Disable HTTP ACL Policy and check if the page (405) is still displayed. If the page is no longer displayed, the access is intercepted because of the ACL rule. You can resolve the problem by deleting the rule.
5. If the problem appears even after you disable HTTP ACL Policy, you must try disabling Web Application Protection and check if the problem continues to occur. If the problem disappears,
 - We recommend that you [Configure the Web Application Protection policy](#) to Loose.
 - You can also analyze the URL, and use [HTTP ACL Policy](#) to add a new rule to allow access from normal URLs.

Connection reset (302 error)

Symptoms

When some IP addresses are used to access the website, a message “the connection is reset” is displayed and 302 is returned in the response. Set-cookie is also sent.

Causes

Access based on an IP address triggers HTTP Flood protection rules.

Resolution

1. Log on to the [Alibaba Cloud WAF console](#).
2. Go to the Management > Website Configuration page.
3. Find the domain name with abnormal access and click policies under the Operation list.
4. Disable HTTP Flood Protection and check if access recovers. If access recovers after HTTP Flood protection is disabled, the access is intercepted because of HTTP Flood Protection rules.
 - You can set [HTTP ACL Policy](#) to add a new rule to allow access from normal URLs or IP addresses.
 - If the HTTP Flood Protection mode is Emergency, we recommend that you [Configure the HTTP Flood Protection mode](#) to Normal.

HTTPS access abnormal

Symptoms

After an HTTPS request is sent, the certificate `www . notexist . com` is returned.

Causes

WAF requires the browser to support SNI. Generally, iOS primitively supports SNI . For Windows and Android operation systems, you must confirm that they are compatible with SNI.

Resolution

See [HTTPS access exceptions arising from SNI compatibility \(Certificate not trusted\)](#).

White screen (502 error)

Symptoms

During access to the website, white screen occurs and 502 is returned in the response.

Causes

When packet loss occurs on the origin (ECS, SLB, or server) or the origin becomes unreachable, WAF returns white screen.

Resolution

- Check if security software or policies such as blacklist, iptables, firewall, dongle , and cloud lock are set for the origin. If yes, stop or uninstall the related service, clear the blacklist, and check if the problem disappears.
- See [Troubleshooting methods](#). Access by bypassing WAF and check if the access is normal. If access is still abnormal, check if the processes, CPU, memory, and Web logs of the origin are abnormal.

Ping failure and black hole triggered

Symptoms

Pinging a domain name fails. In addition, a short message is received, indicating that WAF encounters a DDoS attack and enters the black hole.

Causes

The DDoS attack is not in the protection scope of WAF.

Resolution

Enable [Anti-DDoS Pro](#) to defend against DDoS attacks.

The load of multiple servers in the backend is unbalanced

Causes

WAF uses Layer 4 IP address hash algorithm. Therefore,

- When Anti-DDoS Pro is connected to WAF, the load on the ECS may not be balanced
-
- When the SLB uses Layer 4 forwarding, the load on the ECS may not be balanced.

Resolution

Set WAF and ECS to directly use SLB to balance load, that is, enable Layer 7 forwarding, cookie session persistence, and load balancing.

WeChat or Alipay callback failure

Symptoms

WeChat or Alipay callback fails.

Causes

- High-frequency access is intercepted by HTTP Flood Protection.
- HTTPS is used for callback and WeChat and Alipay do not support SNI. For more information about SNI, see [HTTPS access exceptions arising from SNI compatibility \(Certificate not trusted\)](#).

Resolution

- HTTP Flood Protection
 1. Log on to the [Alibaba Cloud WAF console](#).
 2. Go to the Management > Website Configuration page.
 3. Find the domain name with abnormal access and click policies under the Operation list.
 4. Disable HTTP Flood Protection and check if access recovers. If access recovers once HTTP Flood protection is disabled, the access is intercepted because of the HTTP Flood Protection rules.
 - You can set [HTTP ACL Policy](#) to add a new rule to allow access from normal URLs or IP addresses.
 - If the HTTP Flood Protection mode is Emergency, we recommend that you [Configure the HTTP Flood Protection mode](#) to Normal.

- **SNI compatibility**

Set WeChat or Alipay to make it directly call the IP address of the ECS or SLB, without going through WAF.

19 WAF back-to-origin CIDR blocks update

To provide better web application protection for you, Alibaba Cloud Web Application Firewall (WAF) expands the capacity of the global WAF server rooms to further improve service capabilities. After the expansion of the capacity, WAF's WAF back-to-origin CIDR blocks are expanded.

If your origin servers have IP whitelist or security group settings for access control, to only allow accesses from WAF back-to-origin CIDR blocks, you must add the following new WAF back-to-origin CIDR blocks into the whitelist. Otherwise, traffic forwarded by WAF to the origin servers can be blocked by access control policies, and your website cannot be visited as expected.



Note:

Besides adding new back-to-origin CIDR blocks, some existing CIDR blocks are also updated this time. Please verify the new CIDR blocks carefully.

New WAF back-to-origin CIDR blocks for the mainland China instances

121.43.18.0/24, 120.25.115.0/24, 101.200.106.0/24, 120.55.177.0/24, 120.27.173.0/24, 120.55.107.0/24, 123.57.117.0/24, 120.76.16.0/24, 182.92.253.32/27, 60.205.193.64/27, 60.205.193.96/27, 120.78.44.128/26, 118.178.15.0/24, 39.106.237.192/26, 106.15.101.96/27, 47.101.16.64/27, 47.106.31.0/24, 47.98.74.0/25, 47.97.242.96/27, 112.124.159.0/24, 39.96.130.0/24, 39.96.119.0/24, 47.99.20.0/24, 47.104.53.0/26, 47.108.23.192/26

New WAF back-to-origin CIDR blocks for the International instances

47.89.1.160/27, 47.89.7.192/26, 47.88.145.96/27, 47.88.250.0/24, 47.52.120.0/24, 47.254.217.32/27, 47.88.74.0/24, 47.89.132.224/27, 47.91.69.64/27, 47.91.54.128/27, 47.74.160.0/24, 47.91.113.64/27, 149.129.211.0/27, 149.129.140.0/27, 47.89.7.224/27, 8.208.2.192/27

You can also log on to the Web Application Firewall management console, and go to the Management > Website Configuration page, to check the latest WAF back-to-origin CIDR blocks.