ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

FAQ

Document Version: 20220601

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings> Network> Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.WAF FAQ

This topic provides answers to some frequently asked questions about Web Application Firewall (WAF).

- FAQ about pre-sales consulting
    - Can I use WAF to protect servers that are not deployed on Alibaba Cloud?
    - Does WAF support Cloud Web Hosting instances?
    - Can WAF protect HTTPS services?
    - Does WAF support custom ports?
    - What are the limits for the ports that can be added to WAF?
    - Does the QPS limit that is configured for a WAF instance in the WAF console apply to the entire WAF instance or a single domain name added to the WAF instance?
    - Does WAF support two-way HTTPS authentication?
    - Does WAF support the WebSocket, HTTP/2, and SPDY protocols?
    - Is the origin server affected if you add HTTP/2 services to WAF?
    - Which TLS protocols does WAF support?
    - Can WAF protect websites that use NTLM authentication?
- FAQ about website access configuration
    - Can I use the internal IP address of an ECS instance as an origin IP address in the WAF console?
    - Can WAF protect multiple origin IP addresses for one domain name?
    - How does WAF balance request loads among origin servers?
    - Does WAF support the health check feature?
    - Does WAF support session persistence?
    - Does latency occur when I change an origin IP address in the WAF console?
    - What are the back-to-origin CIDR blocks of WAF?
    - Does WAF automatically add its back-to-origin CIDR blocks to security groups?
    - Do I need to allow access requests from all client IP addresses?
    - Can a WAF instance that uses an exclusive IP address defend against DDoS attacks?
    - Can WAF be deployed with CDN or with Anti-DDoS Pro or Anti-DDoS Premium?
    - Can I deploy WAF with CDN and Anti-DDoS Pro or Anti-DDoS Premium by using different Alibaba Cloud accounts?
    - How does WAF ensure the security of an uploaded certificate and its private key? Does WAF decrypt HTTPS traffic and record the content of HTTPS requests?
    - A domain name is added to WAF. Why am I unable to find the domain name in the domain name list?
- FAQ about website protection configuration
    - How can I use WAF to defend against HTTP flood attacks?
    - How long does it take for configuration modifications in the WAF console to take effect?
    - When I configure custom protection policies (ACL policies) in the WAF console, can I enter CIDR blocks in the IP field?
    - Why does a custom protection policy in which the URL match field contains two forward slashes (//) not take effect?

- FAQ about website protection analysis
    - Can I view the source IP addresses of HTTP flood attacks in the WAF console?
    - How do I query the bandwidth usage of WAF?

Can I use WAF to protect servers that are not deployed on Alibaba Cloud?

Yes, you can use WAF to protect servers that are not deployed on Alibaba Cloud. WAF protects all servers that are accessible over the Internet. These servers can be deployed on Alibaba Cloud or third-party clouds, or in data centers.

> **Notice** If you want to add domain names to a WAF instance in the Chinese mainland, you must complete Internet Content Provider (ICP) filing for the domain names. ICP filing is required by the Ministry of Industry and Information Technology (MIIT). If the domain names do not have ICP filing, the domain names cannot be added to the WAF instance.

Does WAF support Cloud Web Hosting instances?

Yes, all editions of WAF support exclusive Cloud Web Hosting instances. After you activate WAF, you can configure exclusive instances in the WAF console.

Shared Cloud Web Hosting instances use shared IP addresses, which means that multiple users share the same origin server. We recommend that you do not configure WAF for shared instances.

Can WAF protect HTTPS services?

Yes, all editions of WAF can protect HTTPS services. You can add wildcard domain names to WAF.

To protect HTTPS services, you must upload SSL certificates and private key files as prompted. After HTTPS-enabled websites are added to WAF, WAF decrypts access requests, checks request packets, encrypts the requests, and then forwards the requests to origin servers.

Does WAF support custom ports?

The Business and Enterprise editions of WAF support custom non-standard ports. The WAF Business edition supports up to 10 non-standard ports, and the WAF Enterprise edition supports up to 50 non-standard ports.

> **Notice** WAF supports non-standard ports only within a specific port range. The non-standard ports must be within the allowed port range. For more information, see View the allowed port range.

What are the limits for the ports that can be added to WAF?

WAF supports only specific ports. The ports vary based on editions of WAF. For more information, see View the allowed port range.

Security risks may be caused by vulnerable ports, and Internet service providers (ISPs) block service traffic that is destined for the vulnerable ports. Vulnerable TCP ports include ports 42, 135, 137, 138, 139, 445, 593, 1025, 1434, 1068, 3127, 3128, 3129, 3130, 4444, 5554, 5800, 5900, and 9996. If your website that is protected by WAF uses the preceding vulnerable ports, your website may be inaccessible in some regions. Before you add your web service to WAF, make sure that the website does not use the preceding vulnerable ports.

Does the QPS limit that is configured for a WAF instance in the WAF console apply to the entire WAF instance or a single domain name added to the WAF instance?

The queries per second (QPS) limit applies to the entire WAF instance.

For example, if you add three domain names to a WAF instance in the WAF console, the total QPS of these domain names cannot exceed the configured QPS limit. If the total QPS exceeds the limit, WAF triggers throttling and may discard packets at random.

Does WAF support two-way HTTPS authentication?

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

Does WAF support the WebSocket, HTTP/2, and SPDY protocols?

All editions of WAF support WebSocket. WAF Business and higher editions support HTTP/2. WAF does not support SPDY.

Is the origin server affected if you add HTTP/2 services to WAF?

Yes, the origin server is affected. If you add HTTP/2 services to WAF, WAF can handle HTTP/2 requests from clients, but WAF forwards requests to the origin servers only over HTTP 1.0 or 1.1. Therefore, if you want to add HTTP/2 services, HTTP/2 multiplexing cannot work as expected and the clean bandwidth of the origin server increases.

Which TLS protocols does WAF support?

WAF instances that reside in the Chinese mainland support TLS 1.0, TLS 1.1, and TLS 1.2. WAF instances that reside outside the Chinese mainland support TLS 1.1 and TLS 1.2.

If you have personalized requirements, you can customize TLS configurations. For example, you can disable TLS 1.0 and enable TLS 1.3 for your WAF instance. For more information, see Configure custom TLS settings.

Can WAF protect websites that use NTLM authentication?

No, WAF cannot protect websites that use New Technology LAN Manager (NTLM) authentication. If your website uses NTLM authentication, the access requests forwarded by WAF may fail to pass the NTLM authentication of an origin server. As a result, authentication prompts may be repeatedly displayed on the client. We recommend that you use a different authentication method for your website.

Can I use the internal IP address of an ECS instance as an origin IP address in the WAF console?

No, you cannot use the internal IP address of an Elastic Compute Service (ECS) instance as an origin IP address. The reason is that WAF forwards requests to an origin server over the Internet.

Can WAF protect multiple origin IP addresses for one domain name?

Yes, you can enter a maximum of 20 origin IP addresses when you add a domain name in the WAF console.

How does WAF balance request loads among origin servers?

If you configure multiple origin servers, WAF automatically uses the IP hash method to balance request loads among these origin servers. You can also use other load balancing algorithms based on your business requirements. For more information, see Add a domain name.

Does WAF support the health check feature?

Yes, WAF supports the health check feature, which is enabled by default. WAF checks the availability of origin IP addresses. If an origin server is unavailable, WAF forwards the requests to another origin server.

> **Note** If an origin server does not respond, WAF sets a cooldown period for the origin server. During the period, WAF does not forward requests to the origin server but forwards the requests to another origin server. After the period elapses, new requests may be forwarded to the faulty origin server again. For more information about how the health check feature works, see Health check overview.

Does WAF support session persistence?

Yes, WAF supports session persistence, which is disabled by default. If you want to enable session persistence, submit a to contact technical support.

Does latency occur when I change an origin IP address in the WAF console?

Yes, latency occurs when you change an origin IP address. The new IP address requires about 1 minute to take effect.

What are the back-to-origin CIDR blocks of WAF?

You can perform the following operations to query back-to-origin CIDR blocks: Log on to the WAF console and choose **System Management > Product Information**. For more information, see Allow access from back-to-origin CIDR blocks of WAF.

Does WAF automatically add its back-to-origin CIDR blocks to security groups?

No, WAF does not automatically add its back-to-origin CIDR blocks to security groups. If you deploy other firewalls or host protection software for origin servers, we recommend that you add the back-to-origin CIDR blocks of WAF to the required whitelists.

We recommend that you configure specific protection policies for the origin servers. For more information, see Configure protection for an origin server.

Do I need to allow access requests from all client IP addresses?

You can allow access requests from all client IP addresses or only from the back-to-origin CIDR blocks of WAF. To protect web services of origin servers, we recommend that you allow access requests only from the back-to-origin CIDR blocks of WAF.

Can a WAF instance that uses an exclusive IP address defend against DDoS attacks?

Yes, a WAF instance that uses an exclusive IP address can defend against DDoS attacks.

WAF provides exclusive IP addresses for users. Blackhole filtering that defends against DDoS attacks can apply to these IP addresses, similar to the IP addresses of ECS and Server Load Balancer (SLB) instances. The default DDoS mitigation capability provided by the WAF instance that uses an exclusive IP address is the same as the DDoS mitigation capability of an ECS instance in the region where WAF is deployed.

Can WAF be deployed with CDN or with Anti-DDoS Pro or Anti-DDoS Premium?

Yes, WAF is fully compatible with Alibaba Cloud Content Delivery Network (CDN), Anti-DDoS Pro, and Anti-DDoS Premium. If you want to deploy WAF with CDN and Anti-DDoS Pro or Anti-DDoS Premium, we recommend that you deploy the components in the following sequence: client, Anti-DDoS Pro or Anti-DDoS Premium, CDN, WAF, SLB, and origin server.

If you want to deploy WAF with CDN or with Anti-DDoS Pro or Anti-DDoS Premium, set the address of the origin server to the CNAME assigned by WAF when you add a domain name to CDN, Anti-DDoS Pro, or Anti-DDoS Premium. In this case, requests are forwarded by CDN, Anti-DDoS Pro, or Anti-DDoS Premium to WAF and then to the origin server. This way, the origin server is protected. For more information, see Add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF and Use WAF with CDN.

Can I deploy WAF with CDN and Anti-DDoS Pro or Anti-DDoS Premium by using different Alibaba Cloud accounts?

Yes, you can deploy WAF with CDN and Anti-DDoS Pro or Anti-DDoS Premium by using different accounts. This deployment mode allows you to defend against DDoS attacks and web application attacks.

How does WAF ensure the security of an uploaded certificate and its private key? Does WAF decrypt HTTPS traffic and record the content of HTTPS requests?

If you use WAF to protect HTTPS services, you must upload the required SSL certificate and its private key. This way, WAF can decrypt HTTPS traffic to detect attacks and analyze the characteristics of attacks. Alibaba Cloud uses a dedicated key server to store and manage private keys. The key server is based on Alibaba Cloud Key Management Service (KMS) and can ensure the data security, integrity, and availability of both certificates and private keys. This helps meet the requirements for regulation, classified protection, and compliance. For more information about KMS, see What is Key Management Service?.

WAF uses an uploaded certificate and its private key to decrypt HTTPS traffic only in the scenarios when they detect attacks in real time. WAF records only specific content of request payloads. The content is determined based on attack characteristics. Then, WAF can provide attack reports and data statistics based on the content. WAF can record the full content of requests or responses only when WAF is authorized.

WAF has been accredited against authoritative standards, including ISO 9001, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 29151, BS 10012, Cloud Security Alliance (CSA) STAR, MLPS level 3, Service Organization Control (SOC) 1, SOC 2, SOC 3, Cloud Computing Compliance Criteria Catalogue (C5), Green Finance Certification Scheme developed by Hong Kong Quality Assurance Agency (HKQAA), Outsourced Service Providers Audit Report (OSPAR), and Payment Card Industry Data Security Standard (PCI DSS). The standards also include those that prove the effectiveness of WAF across financial sectors in Hong Kong (China). WAF also provides the same security and compliance qualifications as Alibaba Cloud. For more information, visit Alibaba Cloud Trust Center.

Note If you use WAF to protect HTTPS services, you can use a dual-certificate method. This method allows you to independently use a set of certificate and private key on both your WAF instance and the origin server. The two sets of certificates and private keys must be valid. This way, the key server can separately manage the certificates and keys.

A domain name is added to WAF. Why am I unable to find the domain name in the domain name list?

The domain name is automatically removed by WAF. This may be because the ICP filing information of the domain name becomes invalid. You must complete ICP filing for the domain name and add the domain name to WAF again. For more information about ICP filing, see ICP filing application overview.

Notice Before you add a domain name to a WAF instance in the Chinese mainland, make sure that the ICP filing information is up-to-date. To meet the requirements of laws and regulations, WAF removes the domain names whose ICP filing information is invalid on a regular basis.

How can I use WAF to defend against HTTP flood attacks?

WAF provides various protection modes to defend against HTTP flood attacks. You can select a mode based on your business requirements. For more information, see Configure HTTP flood protection.

To achieve better protection and reduce the occurrence of false positives, you can use the WAF Business edition or WAF Enterprise edition in which security experts tailor protection algorithms specific to your business. For more information, see Create a custom protection policy.

How long does it take for configuration modifications in the WAF console to take effect?

In most cases, configuration modifications take effect within 1 minute.

When I configure custom protection policies (ACL policies) in the WAF console, can I enter CIDR blocks in the IP field?

Yes, you can enter CIDR blocks in the IP field when you configure custom protection policies in the WAF console.

Why does a custom protection policy in which the URL match field contains two forward slashes (//) not take effect?

When the rules engine of WAF processes the URL match field, it compresses consecutive forward slashes (/). Therefore, the rules engine cannot match the custom protection policy because the URL match field contains two forward slashes (//).

If you want to define an ACL policy in which the URL match field contains two forward slashes (//), enter a single forward slash (/) instead. For example, if you want to set the URL match field to `//api/sms/request` , enter `/api/sms/request` instead. This way, WAF can implement access control based on the policy.

Can I view the source IP addresses of HTTP flood attacks in the WAF console?

Yes, you can view the source IP addresses of HTTP flood attacks after you enable Log Service of WAF. For more information, see Enable Log Service for WAF and Query logs.

How do I query the bandwidth usage of WAF?

You can query the bandwidth usage of WAF on the **Overview** page in the WAF console.

2.How do I handle the mismatch between a certificate and its private key?

Problem description

After you upload an HTTPS certificate to the Anti-DDoS Pro console, Anti-DDoS Premium console, or WAF console, the message **The certificate and the private key do not match.** is returned.

Cause and solution

Possible cause	Solution

The uploaded certificate and private key do not match in content.	Check whether the MD5 values of the certificate file and the private key file are the same. If the MD5 values are different, the certificate file and the private key file are associated with different domain names.
	You can run the following commands to view the MD5 values of the certificate file and private key file:
	`openssl x509 -noout -modulus -in <Content of the certificate file>|openssl md5`
	`openssl rsa -noout -modulus -in  <Content of the private key file>|openssl md5`
	If the uploaded certificate and private key do not match in content, we recommend that you upload the correct certificate file and private key file.

The Rivest-Shamir-Adleman (RSA) private key is in an invalid format.	Generate a private key and upload the new private key. You can run the following command to generate a new private key: `openssl rsa -in <Content of the original private key file> -out <Content of the new private key file>`

Fix the certificate chain

When you purchase an SSL certificate, the certificate service provider offers you a complete certificate chain. The certificate chain includes an intermediate certificate and a domain name certificate. If no intermediate certificates are provided, we recommend that you use a tool to fix the certificate chain.

You can run the following command on your server to check the integrity of the certificate chain:

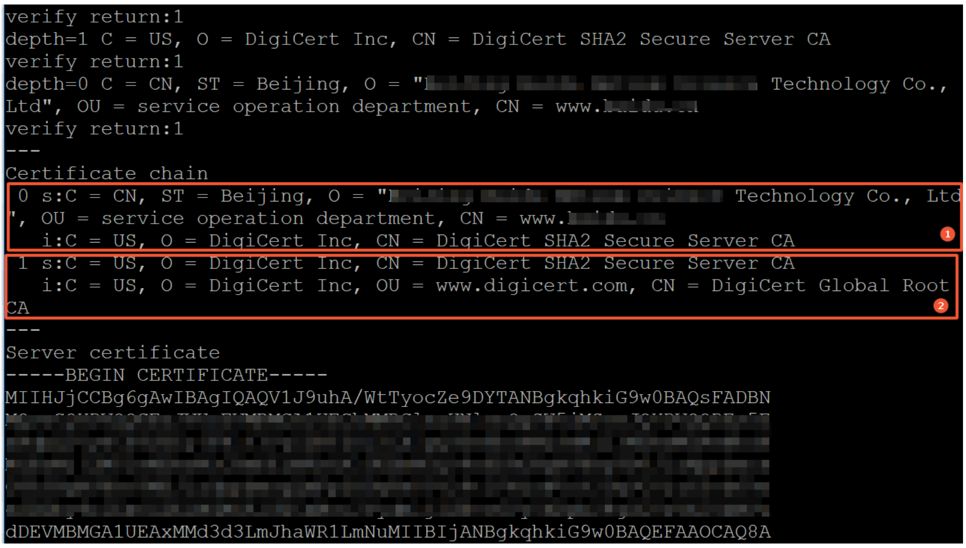
```
openssl s_client -connect <server ip>:443 -servername <domain name>
```

Variables:

- `<server ip>` : Set the value to the IP address of your server.
- `<domain name>` : Set the value to the domain name of the website.

Note You can run the preceding command on your server regardless of whether the website is added.

If the **Certificate chain** section in the returned result includes the domain name certificate and the intermediate Certificate Authority (CA) certificate, the certificate chain is complete. Section 1 shows a domain name certificate, and Section 2 shows an intermediate CA certificate.

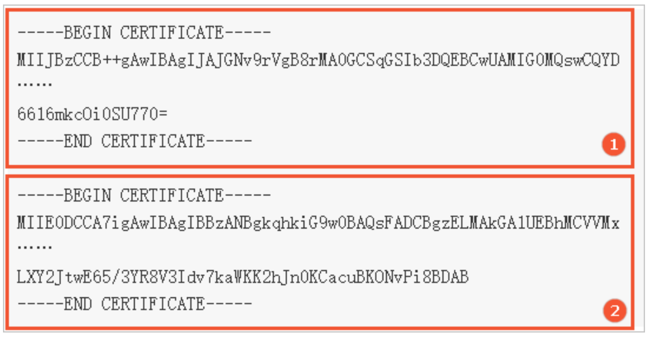


```
verify return:1
depth=1 C = US, O = DigiCert Inc, CN = DigiCert SHA2 Secure Server CA
verify return:1
depth=0 C = CN, ST = Beijing, O = "[redacted] Technology Co.,
Ltd", OU = service operation department, CN = www.[redacted]
verify return:1
---
Certificate chain
 0 s:C = CN, ST = Beijing, O = "[redacted] Technology Co., Ltd
", OU = service operation department, CN = www.[redacted]
   i:C = US, O = DigiCert Inc, CN = DigiCert SHA2 Secure Server CA
 1 s:C = US, O = DigiCert Inc, CN = DigiCert SHA2 Secure Server CA
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root
CA
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIHJjCCBg6gAwIBAgIQAQV1J9uhA/WtTyocZe9DYTANBgkqhkiG9w0BAQsFADBN
[redacted]
dDEVMBMGA1UEAxMMd3d3LmJhaWR1LmNuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
```

If the returned result displays only the domain name certificate, the certificate chain is incomplete. In this case, we recommend that you use a tool to fix the certificate chain. For example, you can use the tool to download the complete certificate chain. Then, you can replace your certificate with the certificate chain that you downloaded.

The following figure shows the content format of the certificate file. Section 1 shows a domain name certificate, and Section 2 shows an intermediate certificate.

Notice The certificate content cannot contain spaces or carriage return characters.



```
-----BEGIN CERTIFICATE-----
MIIJBzCCB++gAwIBAgIJAJGNv9rVgB8rMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYD
......
6616mkcOi0SU770=
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIE0DCCA7igAwIBAgIBBzANBgkqhkiG9w0BAQsFADCBgzELMAkGA1UEBhMCVVMx
......
LXY2JtwE65/3YR8V3Idv7kaWKK2hJn0KCacuBKONvPi8BDAB
-----END CERTIFICATE-----
```

3.FAQ about Log Service for WAF

This topic provides answers to some frequently asked questions about Log Service for Web Application Firewall (WAF).

- How do I enable the Log Service for WAF feature?
- What information is recorded in WAF logs?
- How do I determine the log storage specifications that I need?
- Can I change the log storage period on the Log Service page?

How do I enable the Log Service for WAF feature?

If you use a subscription WAF instance that runs the Pro or higher edition, you can select Yes for Log Service when you purchase the instance. If you do not enable the feature when you purchase the instance, you can upgrade the instance to enable the feature. For more information, see 包年包月实例 Procedure.

What information is recorded in WAF logs?

WAF logs record the HTTP and HTTPS requests that clients send to the domain names protected by WAF. If you enable log collection for a domain name, WAF records logs when it detects requests. If you disable log collection for a domain name, WAF does not record logs on requests.

For information on how to enable and disable log collection for a domain name, see Step 2: Enable the log collection feature.

How do I determine the log storage specifications that I need?

You can specify the log storage capacity based on the log storage configurations and the daily QPS of your website service.

Log storage configurations include the following items:

- Log type: The log types include full logs and attack logs. If you want to store full logs, you must specify a larger storage capacity than the capacity that is required for attack logs.
- Log storage period: A longer storage period requires a larger log storage capacity.
- Fields contained in logs: WAF log fields are classified into required fields and optional fields. If you want to include more optional fields, you must specify a larger log storage capacity.

If you enable the Log Service for WAF feature for the first time, the following default log storage configurations are used: full logs are stored, logs are retained for 180 days, and only required fields are included in logs. You can modify log storage configurations by using the **log settings** feature. For more information, see Modify log settings.

For example, the default log storage configurations are used. The following list provides suggestions on how to select the required log storage capacity based on the daily QPS of your website service:

- If the daily average QPS is not greater than 80, we recommend that you select 3 TB of storage capacity.
- If the daily average QPS ranges from 80 to 120, we recommend that you select 5 TB of storage capacity.
- If the daily average QPS ranges from 120 to 260, we recommend that you select 10 TB of storage capacity.
- If the daily average QPS ranges from 260 to 350, we recommend that you select 15 TB of storage

capacity.

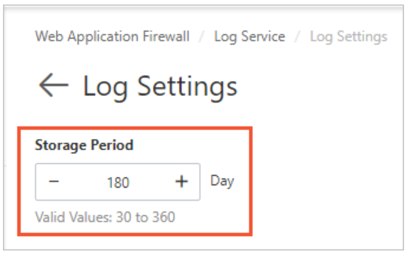
- If the daily average QPS ranges from 350 to 500, we recommend that you select 20 TB of storage capacity.
- If the daily average QPS ranges from 500 to 1,200, we recommend that you select 50 TB of storage capacity.

> **Note** If you want to customize the log storage configurations, you can estimate the required log storage capacity based on the preceding information.

Can I change the log storage period on the Log Service page?

Only subscription WAF instances allow you to change the log storage period within the range of 30 to 360 days. If you use a pay-as-you-go WAF instance, logs are retained only for seven days, and the log storage period cannot be changed.

If you use a subscription WAF instance of the Business or higher edition and the Log Service for WAF feature is enabled, you can perform the following operations to open the Log Service page and change the log storage period: Log on the WAF console. In the left-side navigation pane, choose **Log Management > Log Service** and click **Log Settings**. For more information, see Modify log settings.



Web Application Firewall / Log Service / Log Settings

Log Settings

Storage Period: 180 Day

Valid Values: 30 to 360

4.How do I troubleshoot website access exceptions?

This topic describes how to troubleshoot access exceptions on websites that are protected by Web Application Firewall (WAF).

Instructions

If you cannot access a website that is protected by WAF, you can use the following methods to troubleshoot the exception:

1. Determine whether the origin server is faulty: Bypass WAF and check whether the origin server responds to access requests in an expected manner.
2. Determine whether WAF blocks valid requests: Disable protection modules to check whether WAF blocks access requests.
3. Determine whether the exception is a common exception: Analyze and troubleshoot the exception by following the instructions in the common access exceptions table.

> ? **Note** If the exception persists after troubleshooting, submit a ticket to contact Alibaba Cloud technical support.

For more information about the tools that are used during troubleshooting, see Appendix: Common tools.

Determine whether the origin server is faulty

To bypass WAF and determine whether the origin server responds to access requests in an expected manner, perform the following steps:

1. Disable the security groups, blacklists, whitelists, firewalls, SafeDog, and Yunsuo on the origin server to prevent back-to-origin IP addresses of WAF from being blocked.
2. Modify the *hosts* file in your computer to resolve the domain name to the public IP address of the required Elastic Compute Service (ECS) instance, Server Load Balancer (SLB) instance, or on-premises server. The public IP address is the IP address of the origin server that you add to WAF.
3. Use a browser of your computer to access the domain name of the origin server and check whether the same exception occurs.
    - If you cannot access the origin server, the origin server is faulty. We recommend that you check the working status of the origin server, including processes, CPU utilization, memory, and web logs, and fix the exception.
    - If you can access the origin server, the exception is not due to the origin server. Check whether the exception occurs because WAF blocks the access requests. For more information, see Determine whether WAF blocks valid requests.

Determine whether WAF blocks valid requests

To disable the blocking functions of WAF and determine whether WAF blocks valid access requests, perform the following steps:

1. Disable **RegEx Protection Engine** for the domain name of the origin server to check whether the exception persists. For more information, see Configure the protection rules engine feature.

If you can access the website after you disable this function, we recommend that you set **Protection Rule Group** to **Loose rule group** in the **RegEx Protection Engine** section. By default, **Medium rule group** is selected. Alternatively, you can analyze the URL of the origin server by using Log Service for WAF. Then, add a custom protection policy to WAF to allow all access requests to this URL. For more information, see Create a custom protection policy.

2. If the problem persists after you disable **RegEx Protection Engine**, disable **HTTP Flood Protection** for the domain name of the origin server. For more information, see Configure HTTP flood protection.

   If you can access the website after you disable this function, we recommend that you set Mode to **Prevention** in the **HTTP Flood Protection** section. If Mode is already set to **Prevention**, skip this step. Alternatively, you can analyze the URL of the origin server by using Log Service for WAF. Then, add a custom protection policy to WAF to allow all access requests to this URL. For more information, see Create a custom protection policy.

   If the exception persists after you disable **HTTP Flood Protection**, this exception is not due to the blocking functions of WAF. For more information, see Determine whether the exception is a common exception.

Determine whether the exception is a common exception

If the exception disappears after you disable WAF and continues to occur after you enable WAF, troubleshoot the exception by following the instructions in the following table.

Exception	Description	Cause	Solution

Exception	Description	Cause	Solution
Access blocked (405 error)	The error message "405 Method Not Allowed" appears, or the HTTP status code 405 is returned.	The access request is blocked by a custom protection policy or the RegEx Protection Engine.	1. Disable the custom protection policy for the domain name of the origin server and check whether the error message appears. For more information, see Create a custom protection policy. If the error message no longer appears, the custom protection policy blocks the access request. Find the custom protection policy and delete it. 2. If the error message still appears after you disable the custom protection policy, disable **RegEx Protection Engine** for the domain name of the origin server to check whether the exception persists. For more information, see Configure the protection rules engine feature. If you can access the website after you disable this function, we recommend that you set **Protection Rule Group** to **Loose rule group** in the **RegEx Protection Engine** section. By default, **Medium rule group** is selected. Alternatively, you can analyze the URL of the origin server by using Log Service for WAF. Then, add a custom protection policy to WAF to allow all access requests to this URL. For more information, see Create a custom protection policy.
Connection reset (302 error)	The system prompts that the connection is reset. The HTTP status code is 302, and the Set-Cookie header is contained in the response.	Access from an IP address triggers HTTP Flood Protection.	Disable **HTTP Flood Protection** for the domain name of the origin server. For more information, see Configure HTTP flood protection. If you can access the website after HTTP Flood Protection is disabled, the access requests are blocked by the HTTP flood protection rule. We recommend that you set Mode to **Prevention** in the **HTTP Flood Protection** section. If Mode is already set to **Prevention**, skip this step. Alternatively, you can analyze the URL of the origin server by using Log Service for WAF. Then, add a custom protection policy to WAF to allow all access requests to this URL. For more information, see Create a custom protection policy.

Exception	Description	Cause	Solution
HTTPS access exceptions	After a client sends an HTTPS request, the certificate `www.notexist.com` is returned.	WAF requires the browser to support Server Name Indication (SNI), whereas the browser of the client may not support SNI.	By default, macOS and iOS operating systems support SNI. For Windows and Android operating systems, make sure that they are compatible with SNI. For more information, see HTTPS access exceptions arising from SNI compatibility ("Certificate not trusted").
Blank screen (502 error)	When you access a website, a blank screen error occurs and the HTTP status code 502 is returned.	When the origin server such as an ECS or SLB instance or a server experiences a packet loss or becomes unreachable, WAF returns the HTTP status code 502.	1. Check whether the origin server has security software or policies configured, such as a blacklist, the iptables program, a firewall, SafeDog, or Yunsuo. If the origin server has security software or policies configured, stop or uninstall them, clear the blacklist, and check whether the exception is resolved. 2. Bypass WAF to check whether the website can be accessed. For more information, see Determine whether the origin server is faulty. If the exception persists, check the processes, CPU utilization, memory, or web logs of the origin server for errors.
Ping failure of a domain name	The domain name cannot be pinged. A text message is received. The message indicates that WAF experiences DDoS attacks, and blackhole filtering is triggered.	WAF cannot mitigate DDoS attacks.	Activate Anti-DDoS to mitigate DDoS attacks. For more information, see Overview.
Unbalanced server load	The load is unbalanced among multiple ECS instances in the backend.	WAF uses Layer 4 hash algorithms for IP addresses. If Anti-DDoS Pro or Anti-DDoS Premium is deployed together with WAF, or SLB uses Layer 4 forwarding, ECS instances may have unbalanced load.	Configure WAF and ECS instances to directly use SLB to balance the load. Use Layer 7 forwarding and enable cookie session persistence or load balancing.

Exception	Description	Cause	Solution
WeChat or Alipay callback failure	WeChat or Alipay callback fails.	The possible reason is that HTTP flood protection rules block high-frequency requests, or HTTPS callback is used but WeChat or Alipay does not support SNI.	- HTTP Flood Protection: i. Disable **HTTP Flood Protection** for the domain name of the origin server. For more information, see Configure HTTP flood protection. ii. If WeChat or Alipay can be accessed after HTTP Flood Protection is disabled, the access request is blocked by HTTP flood protection rules. We recommend that you set Mode to **Prevention** in the **HTTP Flood Protection** section. If Mode is already set to **Prevention**, skip this step. Alternatively, you can analyze the URL of the origin server by using Log Service for WAF. Then, add a custom protection policy to WAF to allow all access requests to this URL. For more information, see Create a custom protection policy. - SNI: Configure WeChat or Alipay to bypass WAF and directly use the IP address of the ECS or SLB instance. For more information, see HTTPS access exceptions arising from SNI compatibility ("Certificate not trusted").

Appendix: Common tools

- Chrome DevTools: It is provided by Google Chrome. It can be used to view loading status of elements on pages. Press **F12** to open the tool and navigate to the **Network** tab.
- ping: The ping test tool can be used to analyze and determine network faults. This tool is available in Windows and Linux. In Windows, press Win+R and enter cmd to open Command Prompt. Command: `ping domain name or IP address`.
- traceroute for Linux and tracert for Windows: The link tracing tools can be used to detect the hop where the packet loss occurs. In Windows, press Win+R and enter *cmd* to open Command Prompt. Command: `tracert -d domain name or IP address`.
- nslookup: This tool can be used to detect whether domain name resolution is functional. In Windows, press Win+R and enter *cmd* to open Command Prompt. Command: `nslookup domain name`.

5.How do I troubleshoot HTTPS access issues

After a website is added to WAF, the website can be accessed over HTTP, but fails to be accessed over HTTPS. For example, the website may fail to open, the certificate may be untrusted, interfaces may fail to be called, or errors may be reported for devices, OSs, or apps of specific types. This topic describes how to troubleshoot the access issues.

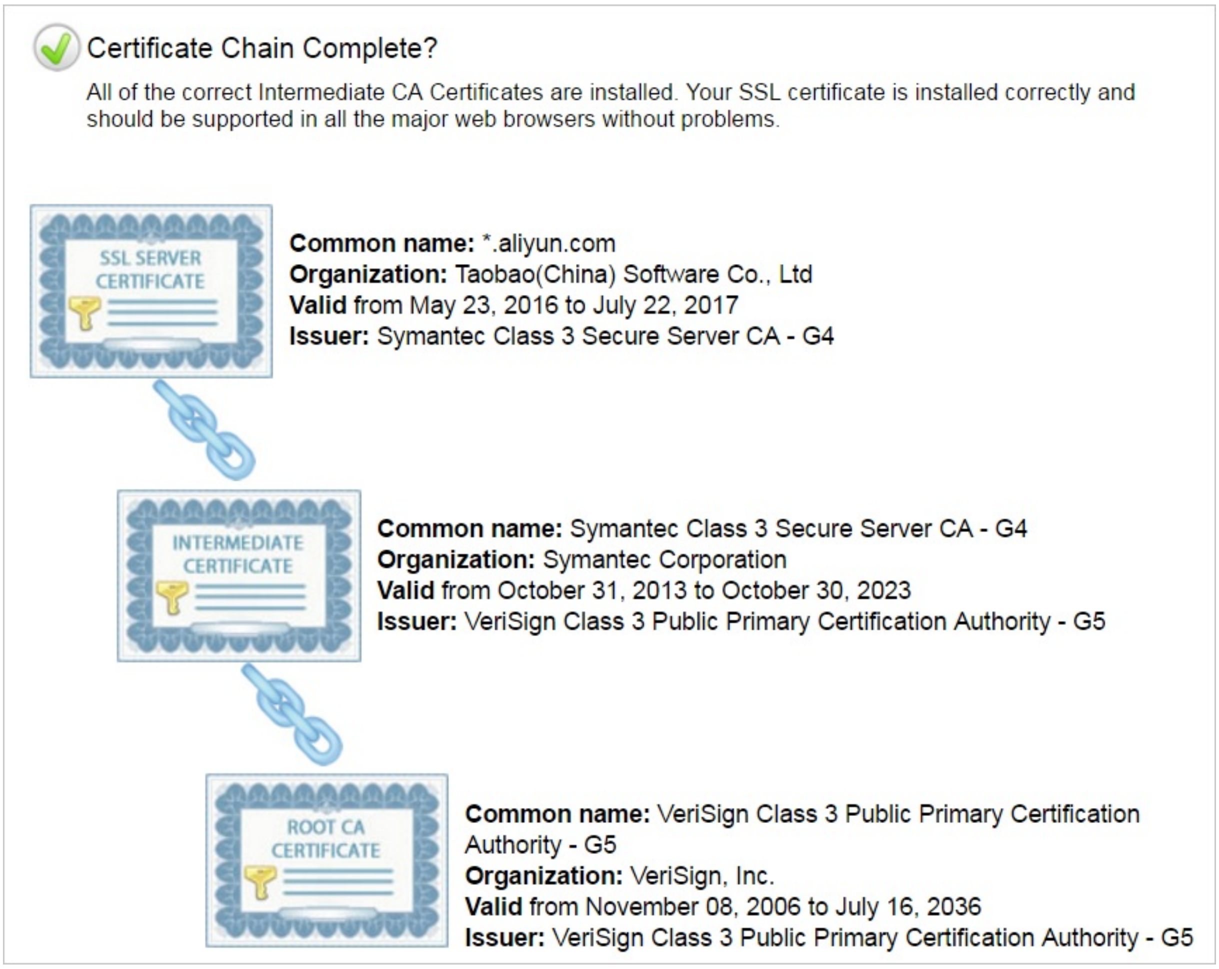
Check whether HTTPS is selected in the WAF console and whether the required certificate is uploaded

To use WAF to protect HTTPS services, you must select HTTPS in the WAF console and upload the same certificate and private key as the certificate and private key of the origin server. If you use WAF together with other services, such as Anti-DDoS Pro, Anti-DDoS Premium, or Alibaba Cloud CDN, you must upload a certificate and private key to WAF. The certificates and private keys of other services do not take effect on WAF. You must separately upload the certificate and private key of WAF.

> **Note** After a certificate is uploaded in the WAF console, a maximum of 5 minutes are required for the configuration to take effect. During this period, access issues may occur. Before you change the DNS record of your website to WAF, we recommend that you modify the hosts file on your computer and verify domain name settings. After you confirm that the domain name settings are in effect, you can change the DNS record of your website to WAF. For more information, see Verify domain name settings.

Check whether the certificate chain is valid

An invalid certificate chain is a common cause of HTTPS access issues. In most cases, a certificate service provider offers a valid certificate chain that contains one server certificate and one or more root certificate authority (CA) certificates. The following figure shows a certificate chain that contains an Alibaba Cloud SSL certificate.



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 a valid certificate chain is uploaded to WAF. To combine multiple certificates into a certificate chain, concatenate the content of the certificates into a single file. Make sure that the server certificate is at the top level of the certificate chain, followed by root certificates. The following example shows an example of a certificate chain that can be uploaded.

```
-----BEGIN CERTIFICATE-----
......
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
......
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
......
-----END CERTIFICATE-----
```

If a certificate chain is invalid, the browser displays an on-screen message to prompt that the certificate is untrusted. In this case, if the website is accessed from Android mobile phones, specific OSs, or apps of specific types, errors are reported in some environments.

You can use online third-party testing tools, such as SSL Installation Checker, to check whether a certificate chain is valid. For more information, visit SSL Installation Checker.

Note The online third-party testing tools can be used to check the status of the certificate chain only for the destination to which your website is mapped. For example, If your website is mapped to the origin server, instead of WAF, the online third-party testing tools cannot be used to check whether the certificate chain of WAF is valid.

Check whether a server name indication (SNI) compatibility issue occurs

If clients or apps of specific types cannot access your website over HTTPS and the error message "SSL handshake failed/error" or "the certificate cannot be trusted" is displayed, the clients or apps may not support SNI. Clients that use outdated versions of Android and apps that are developed by using outdated versions of Java are incompatible with SNI. Internet Explorer, outdated mobile phones, and callback interfaces for third-party payment systems are incompatible with SNI.

Most browsers, apps, and payment callback interfaces of Alipay and WeChat support SNI. If you can access your website when your website is mapped to the origin server but cannot access your website when your website is mapped to WAF, an SNI compatibility issue occurs. We recommend that you upgrade the client or map your website to the origin server.

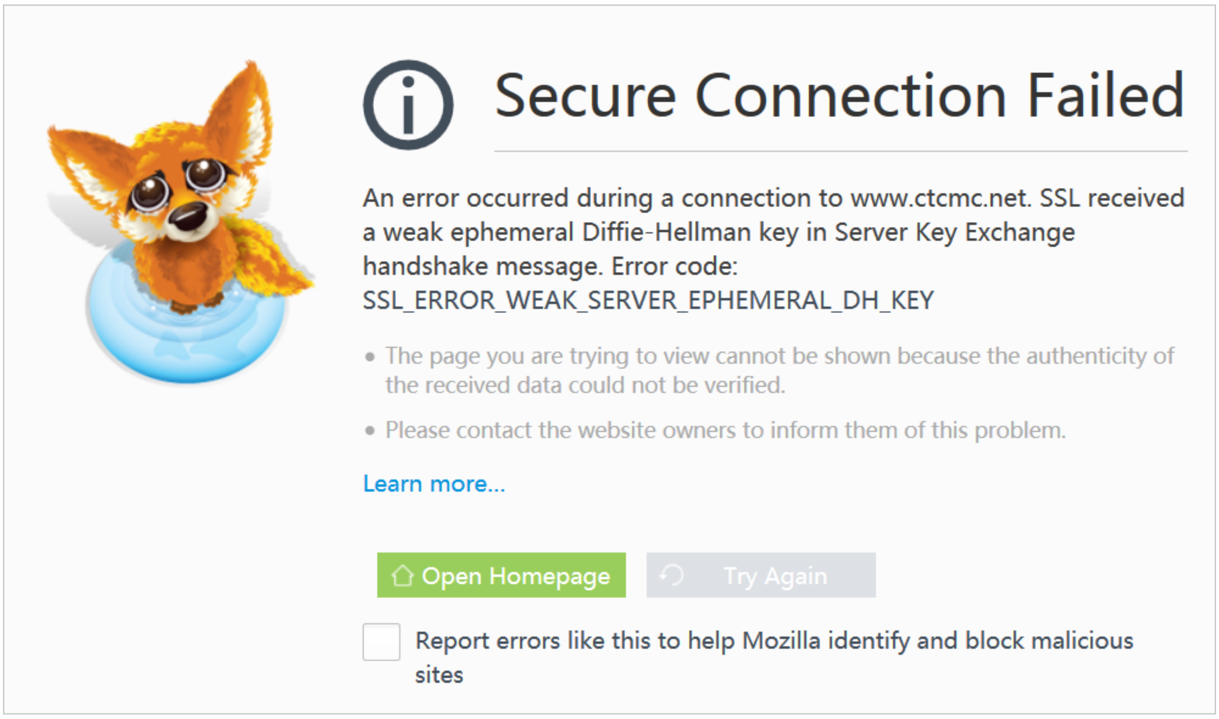
For more information, see HTTPS access exceptions arising from SNI compatibility ("Certificate not trusted").

Check whether your website is hosted on Windows Server 2003 or IIS6 servers

After a website that is hosted on Windows Server 2003 or IIS6 servers is added to WAF, the HTTP 502 status code is returned when the website is accessed over HTTPS. The status code is returned because the TLS version and cipher suite of the system are outdated and do not meet the security requirements. The TLS and cipher suite are incompatible with the default HTTPS back-to-origin algorithm of WAF. The feature that allows you to redirect HTTPS requests to origin servers is not supported for websites that are hosted Windows Server 2003 servers. Microsoft recommends that you do not host your HTTPS website on Windows Server 2003 servers. We recommend that you host your website on servers that run Windows Server 2008 or later to ensure secure communications.

Check whether the Diffie-Hellman (DH) key meets the length requirements

If the DH key is too short to meet the length requirements, the key is not secure. WAF does not support this type of key. If you use a new version of Mozilla Firefox, such as Mozilla Firefox 51.0.1, to access the website that is not protected by WAF, an error message similar to the following message is displayed.



Secure Connection Failed

An error occurred during a connection to www.ctcmc.net. SSL received a weak ephemeral Diffie-Hellman key in Server Key Exchange handshake message. Error code: SSL_ERROR_WEAK_SERVER_EPHEMERAL_DH_KEY

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

□ Report errors like this to help Mozilla identify and block malicious sites

To resolve this issue, upgrade related components, such as the JDK, to ensure that the DH key is 2048-bit long or longer.

> **Note** The length of the key is determined by the server encryption algorithm that is used. The length is irrelevant to the configurations of the certificate. If you are unable to resolve this issue, contact your origin server developer or search for relevant solutions. You can search for relevant solutions based on the following error message: `SSL routines:ssl3_check_cert_and_algorithm:dh key too small` .

Check whether HTTP is selected

If you enable the feature that redirects HTTP requests to HTTPS requests on the origin server, you must select HTTP and HTTPS in the WAF console. If you select only HTTP or HTTPS in this situation, WAF cannot forward HTTPS requests to the origin server, and errors are reported.

6.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” .

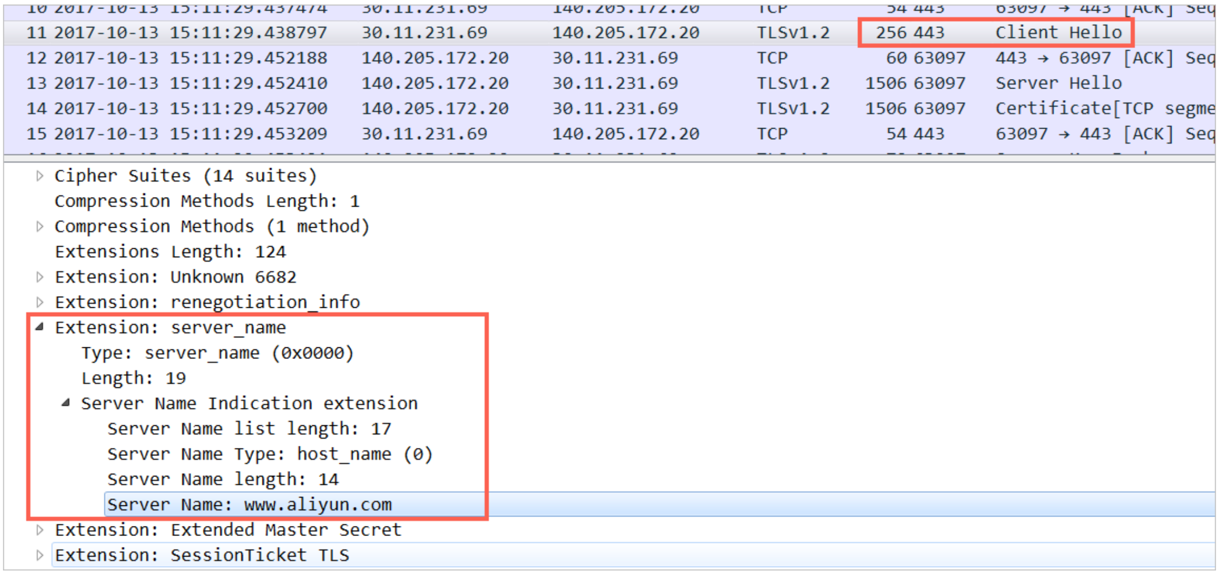
If the client does not support SNI, the following symptoms may occur:

- 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

7.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.

8.What do I do if blackhole filtering is triggered for my WAF instance?

If a Web Application Firewall (WAF) instance is under DDoS attacks, blackhole filtering may be triggered for the instance. This topic describes the impact after blackhole filtering is triggered and the solution.

Impact

If a Web Application Firewall (WAF) instance is under DDoS attacks and the peak attack traffic exceeds the free DDoS mitigation capability provided by the instance, blackhole filtering is triggered for the instance. Then, the traffic destined for the default exclusive IP address of the WAF instance is routed to an IP address that does not exist. In this case, you can receive notifications on the **Overview** page of the WAF console.

After blackhole filtering is triggered, all the traffic redirected to the WAF instance is discarded. This includes both normal and attack traffic. During blackhole filtering, all the domain names added to the WAF instance are inaccessible.

Methods to deactivate blackhole filtering and mitigate DDoS attacks

Blackhole filtering is automatically deactivated after a specific period. By default, blackhole filtering is deactivated 150 minutes after it is triggered. The threshold to trigger blackhole filtering for the WAF instance is the same as the default threshold at which Alibaba Cloud triggers blackhole filtering in the region of your Elastic Compute Service (ECS) instance. For more information about blackhole filtering policies, see Blackhole filtering policy of Alibaba Cloud.

> **Note** By default, each WAF instance has an exclusive IP address. If blackhole filtering is triggered for a default exclusive IP address, all the domain names added to the WAF instance become inaccessible. To prevent an important domain name from being affected by DDoS attacks on other domain names that are protected by the same WAF instance, we recommend that you purchase an exclusive IP address for the important domain name. For more information about exclusive IP addresses, see Exclusive IP addresses.

If you want to mitigate DDoS attacks, we recommend that you use Anti-DDoS Pro or Anti-DDoS Premium to protect your domain name. If you have deployed WAF with Anti-DDoS Pro or Anti-DDoS Premium but blackhole filtering is still triggered for WAF, submit a to contact the after-sales team.

FAQ about WAF for which blackhole filtering is triggered

- Blackhole filtering is triggered for my WAF instance. Can it be immediately deactivated?

  No, blackhole filtering cannot be immediately deactivated after it is triggered. Blackhole filtering is purchased by Alibaba Cloud from Internet service providers (ISPs). The ISPs have strict limits on the time and frequency to deactivate blackhole filtering. Therefore, you cannot manually deactivate blackhole filtering. You must wait until blackhole filtering is automatically deactivated.

  > **Note** Even if you can immediately deactivate blackhole filtering, it is triggered again if the WAF instance is still under DDoS attacks.

- Multiple domain names are added to my WAF instance. How do I check which domain name is under attack?

Attackers can resolve a domain name that is added to WAF to obtain the IP address of the WAF instance. Then, the attackers launch DDoS attacks on the IP address. DDoS attacks target the default exclusive IP address of a WAF instance. You cannot determine which domain name is under attack based on attack traffic.

However, you can change the DNS records of domain names to determine the attacked domain name. For example, you can resolve some domain names to WAF and the rest of the domain names to other services, such as ECS, Alibaba Cloud CDN, or Server Load Balancer (SLB). If blackhole filtering is no longer triggered after this operation, the attacked domain name is among the domain names that you resolve to the other services. However, this method is complicated and may cause some assets, such as the IP address of the origin server, to be exposed on the Internet. More serious security issues may arise. Therefore, we recommend that you do not use this method to determine the attacked domain name.

- Blackhole filtering is triggered for my WAF instance. Can I prevent this issue by changing the IP address of my WAF instance?

  No, you cannot prevent blackhole filtering by changing the IP address. If attackers target your domain name, they can ping your domain name to obtain the IP address of your WAF instance regardless of whether you change the IP address.

- What is the difference between DDoS attacks and HTTP flood attacks? Why is WAF unable to defend against DDoS attacks?

  DDoS attacks are common at Layer 4, and HTTP flood attacks are common at Layer 7. HTTP flood attacks may use HTTP GET or POST requests. WAF can defend against HTTP flood attacks. To defend against DDoS attacks, WAF must be able to receive a huge volume of traffic before it can scrub the traffic. However, WAF cannot provide sufficient bandwidth in this case. Therefore, we recommend that you use Anti-DDoS Pro or Anti-DDoS Premium to defend against DDoS attacks.

9.Supported domain suffixes

Web Application Firewall (WAF) supports the majority of domain suffixes. This topic shows the domain suffixes supported by WAF.

Note If the domain suffix you want to configure is not supported, to contact us.

0~9

2000.hu	5xsoft.com

a

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

b

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

c

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

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

d

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

e

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

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

f

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

g

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

h

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

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

i

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

j

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

k

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

l

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

m

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

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

n

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

o

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

p

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

q

qa	qh.cn	qou.cn			

r

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

s

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

t

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

u

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

v

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

w

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

x

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

y

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

z

za.net	za.org	zhangkj.co	zj.cn	zone	

10.If my website receives requests over an unconfigured port, is the origin server threatened?

Web Application Firewall (WAF) protects websites by filtering and forwarding requests to the websites. However, it forwards requests over only the HTTP and HTTPS ports that you configure when you add your website to WAF.

If your website receives requests over an unconfigured port, WAF does not forward the requests to the origin server regardless of whether the port is enabled. This does not pose any security risks or threats to the origin server.

11.WAF access traffic flow

This topic describes the access traffic flow of Web Application Firewall (WAF).

Access traffic flow description:

> **Note** IP addresses of WAF instances are all deployed on the cloud. You can use a virtual IP address that is configured for a WAF instance to view traffic over Banff. A WAF instance that is configured with a virtual IP address is an LVS cluster. The virtual IP address is similar to a virtual IP address of an SLB instance. You can view the virtual IP address of the WAF instance and the IP address of a WAF engine at the backend in SLB/VPC Operations and Maintenance System.

1. A client sends a request to access the virtual IP address of a WAF instance.
2. The WAF instance forwards the request to backend server A of an LVS cluster.
3. Server A parses request packets to Layer 7 and checks whether this request is a malicious access request or an attack.
    - If this request is a normal access request, server A forwards it to an origin server.
    - If this request is a malicious access request, server A blocks the request and returns the parsed packet information to the client. The traffic flow ends.
4. The origin server processes the forwarded request and returns processing results to server A.

    > **Note** Server A has different roles in Step 3 and Step 4.
    >
    > - For the client, server A acts as a server.
    > - For the origin server, server A acts as a client.

5. Server A returns packet information to the client by using the IP address of the LVS cluster. The traffic flow ends.

12.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.

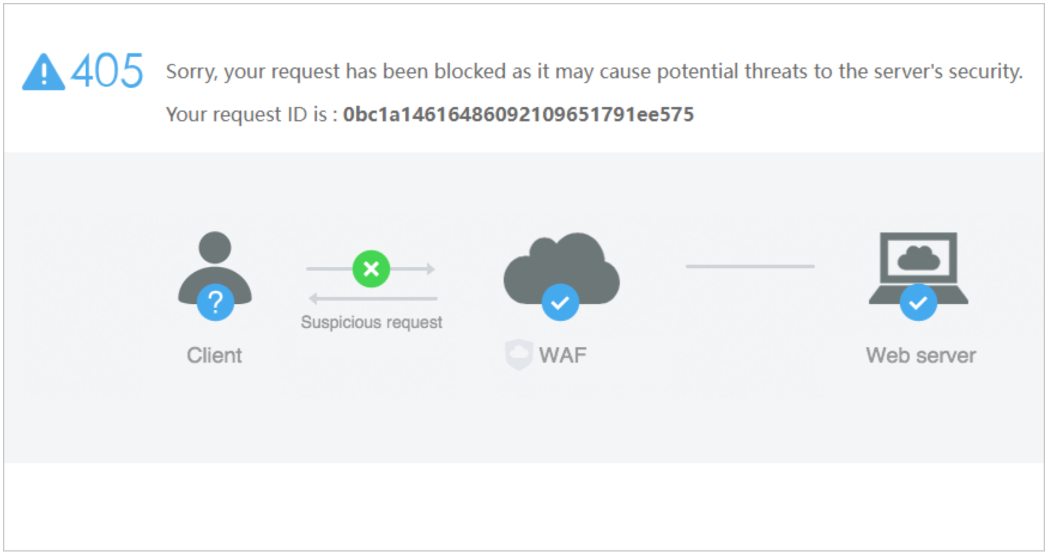
By default, HTTP flood protection is set to the normal mode in protection against common HTTP floods. WAF then mitigates HTTP floods normally. In case the origin CPU rises, or loses response from the database or application, you must activate the emergency mode.

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.

13.How do I troubleshoot 405 errors?

Problem description

After a website is added to Web Application Firewall (WAF), an HTTP 405 status code is returned when access requests are sent to a URL that may pose a threat to the website. The HTTP 405 status code indicates that WAF blocks the access requests.



405 Sorry, your request has been blocked as it may cause potential threats to the server's security.

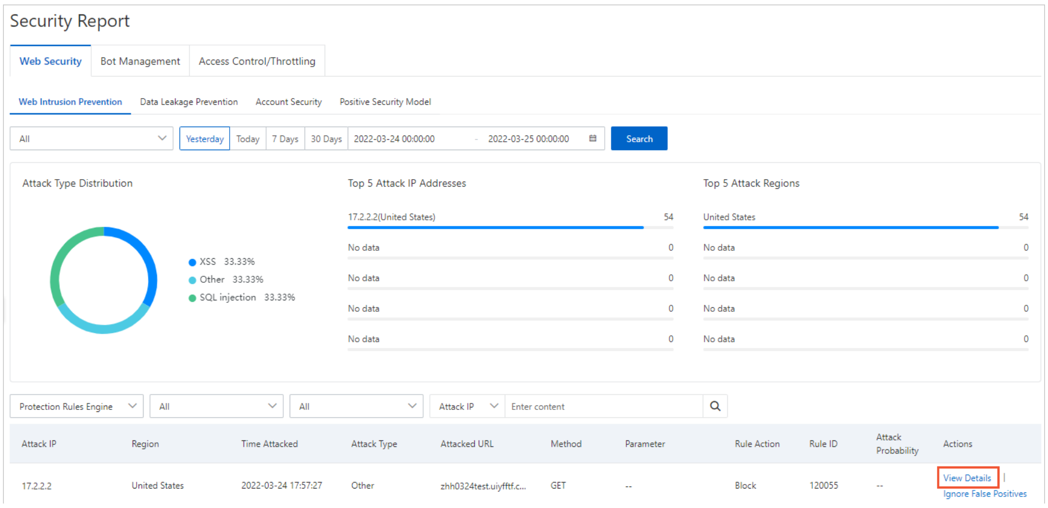
Your request ID is : **0bc1a14616486092109651791ee575**

Solution

If an HTTP 405 status code is returned, you can use one of the following methods to query attack details:

- Log on to the . In the left-side navigation pane, click **Security Report**. On the **Web Security** tab, click **Web Intrusion Prevention**. On the Web Intrusion Prevention tab, you can view the records of attacks that are blocked by WAF and obtain the attack details. For more information, see View Security Reports.

> **Notice** On the **Security Report** page, you can query the details about only attacks that are blocked by Protection Rules Engine and Deep Learning Engine.



Security Report

Web Security | Bot Management | Access Control/Throttling

Web Intrusion Prevention | Data Leakage Prevention | Account Security | Positive Security Model

All | Yesterday | Today | 7 Days | 30 Days | 2022-03-24 00:00:00 - 2022-03-25 00:00:00 | Search

Attack Type Distribution

- XSS 33.33%
- Other 33.33%
- SQL injection 33.33%

Top 5 Attack IP Addresses

17.2.2.2(United States)	54
No data	0
No data	0
No data	0
No data	0

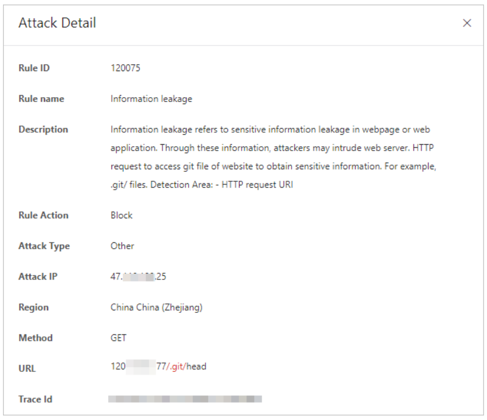
Top 5 Attack Regions

United States	54
No data	0
No data	0
No data	0
No data	0

Protection Rules Engine | All | All | Attack IP | Enter content

Attack IP	Region	Time Attacked	Attack Type	Attacked URL	Method	Parameter	Rule Action	Rule ID	Attack Probability	Actions
17.2.2.2	United States	2022-03-24 17:57:27	Other	zhh0324test.uiyfftf.c...	GET	--	Block	120055	--	View Details | Ignore False Positives

The following figure shows an example of attack details.



Attack Detail

Rule ID	120075
Rule name	Information leakage
Description	Information leakage refers to sensitive information leakage in webpage or web application. Through these information, attackers may intrude web server. HTTP request to access git file of website to obtain sensitive information. For example, .git/ files. Detection Area: - HTTP request URI
Rule Action	Block
Attack Type	Other
Attack IP	47.[redacted].25
Region	China China (Zhejiang)
Method	GET
URL	120[redacted]77/.git/head
Trace Id	[redacted]

- If you have enabled log collection for the domain name of your website, we recommend that you query attack details on the Log Service page. On the Log Service page, you can view the details about attacks that are blocked by all protection features of WAF.

  To query the details about an attack, obtain the ID of the attack request from the block page that is returned by WAF. Then, log on to the . In the left-side navigation pane, click **Log Service**. On the **Log Query** tab, query logs by using the advanced search feature. For more information, see Query logs.

  Notice The Log Service for WAF feature is a paid feature. You must activate Log Service and enable log collection for a domain name before you can query the logs of the domain name. For more information, see Enable Log Service for WAF and Step 2: Enable the log collection feature.

  Log Service

If logs show that WAF blocks normal requests, you can use one of the following methods to resolve the issue:

- On the **Security Report** page, click the **Web Security** tab. Then, click **Web Intrusion Prevention**. On the Web Intrusion Prevention tab, find the rules that block normal requests and click **Ignore False Positives**.

  For more information, see View security reports on the Web Security tab.

Notice You can click **Ignore False Positives** only for the built-in protection rules of Protection Rules Engine and the protection rules that are automatically generated by Deep Learning Engine. If a custom protection rule blocks normal requests, you must delete the rule. For example, if an access control list (ACL) rule or HTTP flood protection rule that you configured in the Custom Protection Policy feature blocks normal requests, you must delete the rule.

- On the **Website Protection** page, configure whitelist rules for different protection features. You can configure custom match conditions and specify the protection features or protection rules whose checks are bypassed when the specified match conditions are met. You can use the URL field to configure a custom match condition.

  For more information, see Configure a website whitelist.

14.What do I do if services on non-standard ports cannot be added to WAF of the Pro edition?

Problem description

WAF of the Pro edition protects only website services that use standard HTTP ports 80 or 8080 or HTTPS ports 443 or 8443. If your services use non-standard ports, the services cannot be added to WAF of the Pro edition.

Solution

- WAF of the Business edition or higher supports specific non-standard ports. For more information, see View the allowed port range. If your services use ports within the port range that is supported by WAF, upgrade your WAF instance to the Business edition or higher. For more information, see Renewal and upgrade.
- If your services use ports that are not supported by WAF, you can deploy an SLB instance that serves as a proxy. The services are deployed in the following sequence: WAF, SLB, and ECS.

  If you deploy an SLB instance that serves as a proxy, you can configure HTTPS services in WAF. By default, port 443 is used. If you deploy an HTTPS listener on the SLB instance, the frontend port is port 443 and the backend port is the service port.

  > Note If you deploy services as described in this section, you must upload HTTPS certificate files to both the WAF and SLB instances. Otherwise, requests cannot be forwarded to origin servers.

15.What do I do if “The HTTPS private key format is invalid” appears when I upload an HTTPS certificate file?

Problem description

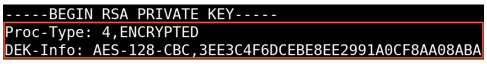
The system prompts "The HTTPS private key format is invalid" when you upload an HTTPS certificate file to WAF.

Cause

The private key of the certificate may be encrypted. WAF cannot identify the encrypted private key.

Solution

1. View the private key file. If the private key file contains the content that is marked in the red box in the following figure, the private key is encrypted.

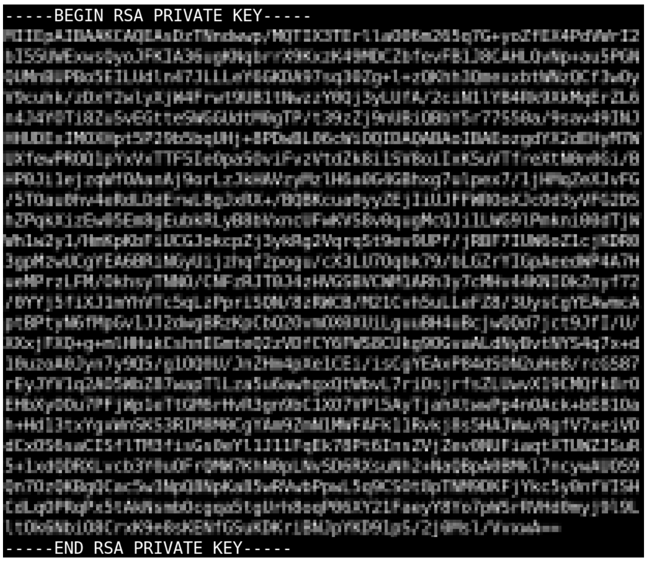
   

   ```
   -----BEGIN RSA PRIVATE KEY-----
   Proc-Type: 4,ENCRYPTED
   DEK-Info: AES-128-CBC,3EE3C4F6DCEBE8EE2991A0CF8AA08ABA
   ```

2. Run the following command and enter a password to decrypt the private key:

   ```
   openssl rsa -in [$keyName] -text
   #[$keyName] indicates the name of the private key file.
   ```

   If the following result is returned, the private key is decrypted.

   ```
   -----BEGIN RSA PRIVATE KEY-----
   [redacted]
   -----END RSA PRIVATE KEY-----
   ```

3. Re-upload the decrypted private key file to WAF.

16.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.

17.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.

18.What do I do if a persistent connection times out?

This topic describes how to resolve the issue that a persistent connection between a client and a server times out. The server is protected by Web Application Firewall (WAF).

Problem description

In some business scenarios, a server requires more than 60 seconds to process a client request. Before the server returns the response, it does not exchange data with the client.

For example, you upload an Excel file on a web page for the server to process. The server requires about 3 minutes to process the data and does not exchange data with the client over HTTP or TCP within 120 seconds. In this case, WAF returns a 504 Gateway Timeout error to the client and terminates the connection.

WAF does not maintain a persistent connection that lasts more than 120 seconds without data exchange.

Solution

- If you use a WAF exclusive cluster to protect your website, you can configure a connection timeout period. A custom timeout period can range from 120 seconds to 3,600 seconds. You can separately configure connection timeout periods for both read and write connections. For more information, see Create an exclusive cluster.
- If you use a WAF shared cluster to protect your website, the connection timeout period cannot be modified.

19.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.

20.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

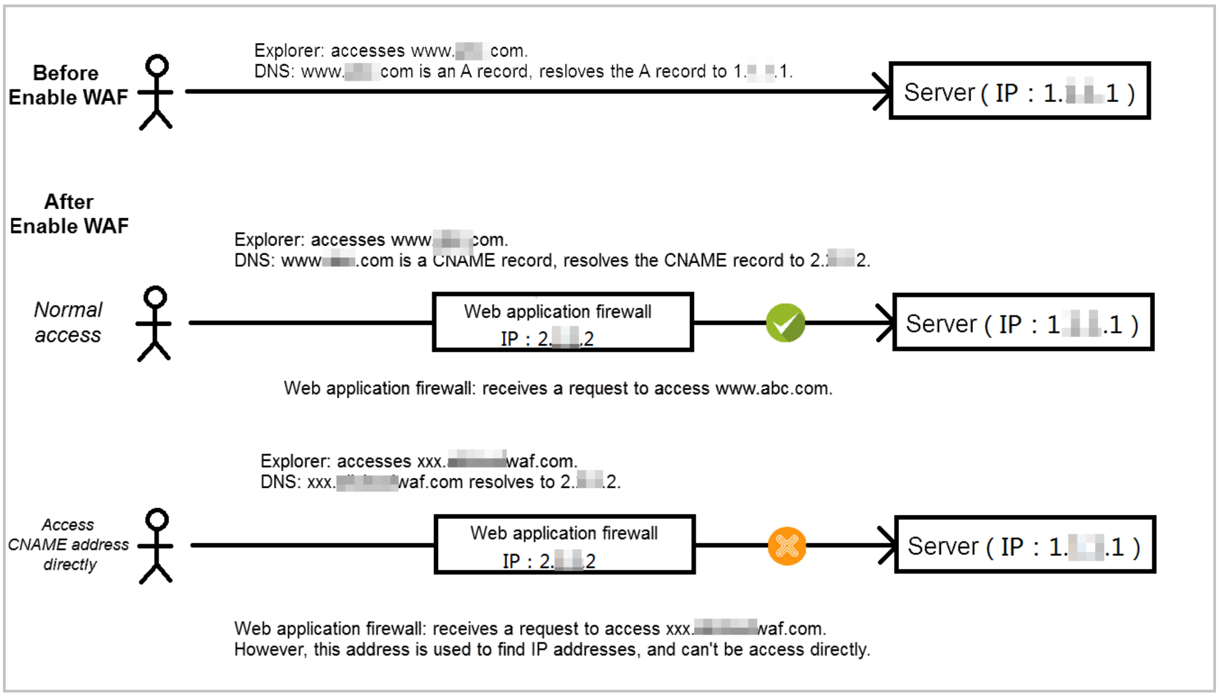
FastCGI attack is a severe security vulnerability in Nginx. By default, the FastCGI module may cause servers to incorrectly parse any file types in PHP mode.

Threat

Malicious attackers may destroy a Nginx server that supports PHP.

21.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.



Before Enable WAF
Explorer: accesses www.[redacted] com.
DNS: www.[redacted] com is an A record, resloves the A record to 1.[redacted].1.
Server (IP : 1.[redacted].1)
After Enable WAF
Explorer: accesses www[redacted]com.
DNS: www[redacted].com is a CNAME record, resolves the CNAME record to 2.[redacted]2.
Normal access
Web application firewall
IP : 2.[redacted].2
Server (IP : 1[redacted].1)
Web application firewall: receives a request to access www.abc.com.
Explorer: accesses xxx.[redacted]waf.com.
DNS: xxx.[redacted]waf.com resolves to 2.[redacted].2.
Access CNAME address directly
Web application firewall
IP : 2.[redacted]2
Server (IP : 1.[redacted].1)
Web application firewall: receives a request to access xxx.[redacted]waf.com.
However, this address is used to find IP addresses, and can't be access directly.

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