ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

Website Access

Document Version: 20201021

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.Tutorial

Web Application Firewall (WAF) can protect your website after you add it to WAF. If you do not add the website, WAF does not protect it.

Add your website to WAF

After you activate WAF, you can add your website to WAF in **CNAME** mode.

After you add the domain name of your website in the WAF console, change the DNS record to redirect the traffic of your website to WAF. Then, WAF filters the traffic and forwards normal traffic to the origin server of the domain name. You can add the domain name by manually adding a website or by configuring WAF to automatically add a website.

In CNAME mode, perform the following operations to add a website:

1. Add domain names: This topic describes how to manually add a website or configure WAF to automatically add a website.

   > Note
   >
   > - If your website uses HTTPS, you must upload a correct and valid HTTPS certificate in the WAF console so that HTTPS requests can be processed as normal. For more information, see Upload HTTPS certificates.
   > - If the origin server uses a port other than port 80 over HTTP and port 443 over HTTPS, you can customize the port in the WAF console. For more information, see Supported custom ports.

2. Allow access from WAF back-to-origin CIDR blocks: WAF uses specified back-to-origin CIDR blocks to forward normal traffic back to the origin server. To allow inbound traffic from the back-to-origin CIDR blocks, you must configure the security software or access control policies of the origin server when you add a website to WAF.
3. Verify domain name settings: This topic describes how to set up a staging environment after a domain name is added and how to check whether the traffic forwarding settings are in effect. You cannot change the DNS record before the settings take effect. Otherwise, your services are interrupted.
4. Change the DNS settings: This topic describes how to manually change the DNS record to redirect the traffic of your website to WAF.

After you add a domain name, WAF forwards access requests to your website for protection. WAF provides multiple protection features to protect your websites against different types of attacks. Among the features, only **RegEx Protection Engine** and **HTTP Flood Protection** are enabled by default. The RegEx Protection Engine feature protects your websites against common web attacks, such as SQL injection, XSS, and webshell upload. The HTTP Flood Protection feature protects your websites against HTTP flood attacks. You need to manually enable other features and configure protection rules. For more information, see Overview.

Best practices

- Configure protection for your origin server: When the origin server is deployed on ECS, you can configure security group policies in ECS or SLB to allow only inbound requests from WAF. This prevents web attackers from bypassing WAF and directly attacking the origin server.

- Retrieve actual IP addresses of clients: After you configure WAF, all requests are forwarded to WAF, and WAF returns the processed requests back to the origin server. You must use X-Forwarded-For to retrieve the actual IP addresses of the sources that initiated these requests.

Connect cloud services to WAF

- Deploy WAF and Anti-DDoS Pro together: You can deploy both WAF and Anti-DDoS Pro or Anti-DDoS Premium to protect against web and DDoS attacks.
- Deploy WAF and CDN together: You can deploy your CDN service and WAF in sequence to speed up your website and protect against web attacks at the same time.

2.Website access with CNAME

2.1. Add domain names

This topic describes how to enable WAF protection for your website in CNAME mode.

Prerequisites

- WAF is activated, and the number of second-level domain names and subdomains that are added to a WAF instance does not reach the upper limit.

  > Note The total number of domain names that can be added to a WAF instance depends on the specifications of the instance and the number of extra domain name packages that you purchase. For more information, see Extra domain quota.

- If your domain name is protected by a WAF instance in mainland China, you must complete ICP filing for your domain name. If you do not complete ICP filing but still add your domain name to WAF, an error may occur and the system prompts you to complete ICP filing.

Context

You can use either of the following methods to add your website configurations:

- Configure WAF to automatically add website configurations: This mode requires you to select the target domain name and network protocol type on the **Add Domain Name** page because WAF automatically reads information about the domain name assets under your Alibaba Cloud account. Then, WAF adds website configurations, such as the domain name, server address, and standard ports (80 and 443), and changes the DNS record of the domain name.

  > Note The account that you use to add domain names must have management permissions on Alibaba Cloud DNS resources. Otherwise, DNS resolution fails. If DNS resolution fails, you can manually change the DNS record of the domain name after the domain name is automatically added.

- Manually add website configurations: This mode requires you to manually add your website configurations, such as the domain name, protocol, server address, and server port. You also need to change the DNS record of the domain name to forward the web requests of the website to WAF for traffic scrubbing.

Configure WAF to automatically add website configurations

The **Add Domain Name** page appears only when an eligible domain name exists. If the page appears, you can select the website that you want to add to WAF. The website is automatically added to WAF.

Eligible domain names contain only valid domain names that are configured in Alibaba Cloud DNS.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.

3. In the left-side navigation pane, choose **Asset Center > Website Access**.
4. On the **Website Access** page, click **Add Domain Name**.
5. On the **Add Domain Name** page, select the target domain name in the **Domain Name** column and the target protocol in the **Protocol Type** column, and click **Add domain protection now**.

> **Note** The **Add Domain Name** page appears only when an eligible domain name exists. If the **Add Domain Name** page does not appear, we recommend that you manually add the website configurations. For more information, see Step 6.

Automatic addition of website configurations

If you select **https**, you must complete certificate verification before you add the website configurations.

Perform the following operations to verify the certificate:

i. Select a domain name and **https** and click **Verify Certificate** in the **HTTPS Certificate** column.

ii. In the **Verify Certificate** dialog box, specify **Upload Type** and upload the HTTPS certificate.For more information, see Update HTTPS certificates.

iii. Click **Confirm** after the HTTPS certificate is uploaded.

- If the certificate verification succeeds, click **Add domain protection now**.
- If the certificate verification fails, verify the certificate again based on the error message, such as **The certificate and key do not match**, until the verification succeeds.

WAF automatically adds the website configurations and changes the DNS record.

> **Note** If you want to add ports other than 80 and 443, manually edit the domain name after the domain name is automatically added. For more information, see References.

Possible issues and solutions:

- **Domain name was added, but you need to manually change the DNS record.**

  Possible causes: The account that you use to add the domain name does not have management permissions on Alibaba Cloud DNS resources, or the uploaded HTTPS certificate does not match your domain name.

  > **Note** Assume that your website supports HTTPS and the certificate verification succeeds. If the uploaded certificate and the website do not match, the certificate detection still fails, and the DNS record is not automatically changed. In this case, you must upload a valid and correct certificate and then manually change the DNS record. For more information, see Upload HTTPS certificates.

  Click **manually access the DNS**. In the **Manual Configuration** dialog box, change the DNS record. For more information, see Change the DNS settings.

- **The maximum number of domain names has been reached.**

  Click **extra domain package** to purchase an extra domain name package. Add the domain name again.

- **No ICP filing records are found for the domain name.**

  If your domain name is protected by a WAF instance in mainland China, you must complete ICP filing for your domain name. Complete ICP filing for your domain name.

Manually add website configurations

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Asset Center > Website Access**.
4. On the **Website Access** page, click **Add Domain Name**.
5. (Optional)On the **Add Domain Name** page, click **Manually Add Other Websites**.

   > **Note** The **Add Domain Name** page appears only when an eligible domain name exists. For more information, see Configure WAF to automatically add website configurations. If the **Add Domain Name** page does not appear, skip this step.

6. Complete the **Add Domain Name** wizard.

   i. **Enter your website information.**

Parameter	Description
Domain Name	Enter the domain name that needs WAF protection. ■ WAF supports exact match domains, such as `www.aliyun.com`, and wildcard domains, such as `*.aliyun.com`. ■ If you use a wildcard domain, WAF automatically matches all subdomains of the wildcard domain. ■ If you configure both a wildcard domain and an exact match domain, WAF uses the forwarding rules and protection policies of the exact match domain. ■ Currently, `.edu` domain names are not supported. To add `.edu` domain names, submit a ticket for technical support.
Protection Resource(applicable to only the Exclusive edition)	If you are using the WAF Exclusive edition, select a protection resource. > **Note** This is available only for the WAF Exclusive edition. Valid values: ■ **Shared Cluster**: This is the default value. ■ **Exclusive Cluster**: You can customize an exclusive cluster to deliver business-specific protection. For more information, see Create an exclusive cluster.

Parameter	Description
Protocol Type	Select a protocol type. Valid values: ■ **HTTP** ■ **HTTPS**: If your website supports HTTPS, select **HTTPS** and upload the certificate and private key files after you add the website configurations. For more information, see Upload HTTPS certificates. After you select **HTTPS**, click **Advanced Settings**.  **Advanced Settings** supports the following features: ■ **Enforce HTTPS Routing**: If this feature is enabled, the HTTP requests are delivered through HTTPS port 443. You must clear HTTP before you turn on Enforce HTTPS Routing. If you want a client to access your website by using HTTPS, enable this feature. This enhances access security. **Notice** Before you enable this feature, make sure that your website supports HTTPS services. After this feature is enabled, requests are delivered over HTTPS. ■ **Enable HTTP**: If this feature is enabled, WAF forwards requests over HTTP. The default port is 80. This feature allows WAF to implement HTTPS access without changes to the origin server, which reduces the workload of your website. If your website does not support HTTPS, turn on Enable HTTP. ■ **HTTP2**: This option is available only when you use the WAF Business or Enterprise edition and select **HTTPS**.

Parameter	Description
Destination Server (IP Address)	Enter the address of the origin server. You can select either **IP** or **Destination Server (Domain Name)**. WAF filters and redirects requests to this address. ■ **IP**: Enter the public IP address of the origin server. Separate multiple IP addresses with commas (,). You can enter up to 20 IP addresses. Do not use line breaks. **Note** If you enter multiple IP addresses, WAF automatically performs health checks and load balancing on these addresses before redirecting requests. ■ If the origin server is an Alibaba Cloud ECS instance, enter the public IP address of the instance. ■ If the ECS instance is connected to an SLB instance, enter the public IP address of the SLB instance. ■ If your origin server is not deployed on Alibaba Cloud, we recommend that you ping the domain name to query the public IP address of the origin server, and then enter the public IP address. ■ **Destination Server (Domain Name)**: Enter the domain name of the origin server, such as an OSS bucket. The domain name of the origin server must be different from the protected domain name. **Note** If you enter a domain name of an OSS bucket, you must bind this domain name to the bucket in the OSS console. For more information, see Bind custom domain names.

Parameter	Description
Destination Server Port	Specify the port used to forward website requests. WAF redirects the filtered requests through only the port that you specify. If other ports are enabled, no security threats are posed to the origin server. **Notice** Protocol Type and Destination Server Port must be the protocol and port used by the origin server to provide web services. WAF does not support port translation. For example, if the origin server provides web services through HTTP port 80, HTTP and port 80 must be configured for your domain name. Default ports: ■ **HTTP 80**: This port is used when HTTP is selected. ■ **HTTPS 443**: This port is used when HTTPS is selected. **Note** HTTP/2 uses the same port as HTTPS does. Custom ports: Click **Customize** and configure the HTTP and HTTPS custom ports. Custom ports Click **View Allowed Port Range** to query all supported ports. Separate multiple ports with commas (,). **Note** ■ WAF Enterprise and Exclusive each supports a maximum of 50 different server ports, including ports 80, 8080, 443, and 8443. WAF Pro and Business each supports a maximum of 10 ports, including ports 80, 8080, 443, and 8443. ■ For more information about ports supported by the shared cluster, see Supported custom ports. ■ If you are using the WAF Exclusive edition, you can select ports from only the **Server Ports** section on the **Exclusive Cluster Settings** page. For more information, see Create an exclusive cluster.

Parameter	Description
Load Balancing Algorithm	If multiple origin IP addresses are configured, select a value. Valid values: ■ **IP hash**: Requests from a specific IP address are redirected to the same origin server. This is the default value. Note If the IP addresses of origin servers are not scattered on different network segments when this algorithm is selected, unbalanced loads may occur. ■ **Round Robin**: All requests are distributed to origin servers in turn. ■ **Least time**: You can use the intelligent DNS resolution feature and the upgraded Least-time back-to-origin algorithm to minimize the latency when traffic is forwarded to origin servers. Note You can select **Least time** only when intelligent load balancing is enabled. For more information, see Intelligent load balancing. After the setting takes effect, WAF distributes back-to-origin requests to the IP addresses of multiple origin servers to achieve load balancing.
Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF	Select **Yes** if you need to configure a Layer 7 proxy in front of WAF. Otherwise, WAF cannot obtain the actual IP addresses of clients. For more information, see the following topics: ■ Deploy WAF and Anti-DDoS Pro together ■ Deploy WAF and CDN together Select **No** if you do not need to configure a Layer 7 proxy in front of WAF.
Request Tag	Enter a **Header Field Name** that is not occupied and a custom **Header Field Value** to mark website requests forwarded by WAF. WAF adds the specified header field and value to the filtered requests. This allows your origin server to identify and collect the requests redirected by WAF, which in turn implements precise protection and effect analysis. Notice If a request already contains the specified header field, WAF overwrites the original field value with the specified value.

Parameter	Description
Resource Group	Select the resource group to which the domain name belongs from the resource group list. Note You can use Resource Management to create resource groups and manage resources under your Alibaba Cloud account by department or project. For more information, see Create a resource group.

ii. **Change DNS Settings.**Change the DNS record of the domain name to redirect the website requests to WAF for traffic scrubbing. For more information, see Change the DNS settings.

iii. **Add Completed.**If your server is using a different firewall in addition to WAF, disable the firewall or add the IP address of WAF to the whitelist of the firewall to prevent the firewall from blocking traffic from WAF. For more information, see Allow access from WAF back-to-origin CIDR blocks. If your server does not use other firewalls, no configuration is required.

Click **Completed. Return to the website list.** The Website Access page appears.

What to do next

After you add the domain name, access requests to the website are protected by WAF. You can also configure website protection configurations for better protection.

WAF provides multiple protection features to protect your websites against different types of attacks. Among the features, only **RegEx Protection Engine** and **HTTP Flood Protection** are enabled by default. The RegEx Protection Engine feature protects your websites against common web attacks, such as SQL injection, XSS, and webshell upload. The HTTP Flood Protection feature protects your websites against HTTP flood attacks. You need to manually enable other features and configure protection rules. For more information, see Overview.

Upload HTTPS certificates

If your domain name uses **HTTPS**, you must upload the valid and correct HTTPS certificate associated with the domain name in the WAF console. This ensures that WAF protects HTTPS requests.

You can upload an HTTPS certificate by using the following methods:

- Manual uploading:

  You must prepare the following files for your website before you upload the certificate:

  - The certificate file in the CRT or PEM format
  - The private key file in the KEY format

- Selecting an existing certificate: You can select certificate that is associated with the domain name. For more information, see SSL Certificates Service.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the

region, **Mainland China** or **International**, in which the instance is deployed.

3. In the left-side navigation pane, choose **Asset Center** > **Website Access**.
4. On the **Website Access** page, find the target domain name and click the

   

   icon next to **HTTPS** in the **Protocol Status** column.

   > **Note** **HTTPS** is displayed in the **Protocol Status** column only when you select HTTPS during the addition of domain names.

   

   If no certificates are uploaded or the uploaded certificate is invalid, the HTTPS status is Abnormal. For example, this occurs if the format of the certificate is invalid or the certificate does not match the domain name. The HTTPS status changes to Normal after a valid certificate is uploaded to the WAF console.
5. In the **Upload Certificate** or **Update Certificate** dialog box, specify **Upload Type** to upload an HTTPS certificate.

   > **Note** If a certificate has been uploaded, the **Update Certificate** dialog box is displayed. The **Update Certificate** and **Upload Certificate** dialog boxes have the same configuration items.

   - **Manual Upload**: Specify **Certificate Name**, copy the content in the certificate file to the **Certificate File** field and the content in the private key file to the **Private Key File** field.

     

     For more information about **Certificate File**, see the following descriptions:

     - If the certificate file is in the PEM, CER, or CRT format, you can use a text editor to open the certificate file and copy its text content.
     - If the certificate file is in another format, such as PFX or P7B, you must covert the certificate file format to PEM. Then, you can use a text editor to open the certificate file and copy its text content. For information about how to convert the format of a certificate file, see How do I convert an HTTPS certificate to the PEM format?.
     - If the target domain name is associated with multiple certificate files, for example, a certificate chain, you must merge the text content in the certificate files and then copy the merged content to the **Certificate File** field.
   - **Select Existing Certificate**: Select the certificate to be uploaded from the **Certificate** drop-down list.

     

     The **Certificate** drop-down list is a collection of certificates that are issued in the SSL Certificates Service console. You can select the certificate associated with the domain name in this list. You can click **Cloud Security - Certificates Service** to go to the SSL Certificates Service console to manage certificates.
   - **Purchase Certificate**: Click **Buy Now** to go to the configuration page of SSL Certificates Service to purchase a certificate for the domain name.

After you purchase the certificate, it is automatically uploaded to WAF.

> **Note** You can purchase only a DV certificate on this page. If you want to purchase a different type of certificate, go to the buy page of SSL Certificates Service. For more information, see Purchase guide.

6. Click **Confirm**.
   After a valid and correct certificate is uploaded, the HTTPS status changes to **Normal**.

References

You can go to the **Website Access** page to view the added domain name in the list and perform the following operations as required:

- Check the DNS resolution status: The **DNS Status** of the domain name is **Normal** only when the DNS record is resolved to the WAF CNAME address and WAF detects access traffic to it. If **DNS Status** is **Abnormal**, click the  icon to query the cause. After the exception is fixed, click the  icon to perform the check again.

  For more information, see DNS resolution status exception.
- Upload HTTPS certificates: If your website supports HTTPS, make sure that the correct certificate and private key files are uploaded to WAF. This ensures that WAF protects HTTPS requests. You can click the  icon next to HTTPS to upload the HTTPS certificate and private key for the domain name.

  For more information, see Upload HTTPS certificates.
- Enable Log Service for WAF: You can enable Log Service for WAF to collect all logs of your website. The logs can be used for query, analysis, dashboard data visualization, and alerting.

  For more information, see Enable log collection.

  > **Note** Log Service for WAF is a value-added service provided by WAF. It is available only after you enable it. For more information, see Enable Log Service for WAF.
- Configure protection resources: Click the  icon in the **Protection Resource** column to configure protection resources for the domain name.

  The following protection resource types are supported:
  - **Shared Cluster and Shared IP**

    > **Note** By default, websites that are automatically added use protection resources of the Shared Cluster and Shared IP type.
  - **Shared Cluster and Exclusive IP** : For more information, see Exclusive IP addresses.

  - **Shared Cluster and Load Balancing Among Multiple WAF Nodes**: For more information, see Intelligent load balancing.
  - **Exclusive Cluster**: For more information, see Create an exclusive cluster.

- View attack monitoring reports: Click **View Report** in the **Attack Monitoring** column to navigate to the **Security report** page to view the protection report of the domain name. For more information, see View security reports.
- Configure protection policies: Click **Config** in the Actions column to navigate to the **Website Protection** page. On the page that appears, you can configure **Web Security**, **Bot Management**, and **Access Control/Throttling** modules. For more information, see Configure the RegEx Protection Engine.
- Edit a domain name: Click **Edit** in the Actions column to modify the website configurations, such as the protocol type, server address, and server port. Domain names cannot be changed.
- Delete a domain name: Click **Delete** in the Actions column to delete a domain name.

> **Warning** Before you delete a domain name, change the DNS record to map the domain name to the IP address of the origin server. Otherwise, traffic to the domain name cannot be forwarded after the domain name is deleted.

FAQ

What do I need to know about migrating website configurations across accounts?

To prevent traffic forwarding errors caused by misoperations during website configuration migration, a 30-minute protection period is configured for your website. To migrate the website configurations to another account, you must delete the website configurations from the current account. Thirty minutes later, you can add the website configurations to the WAF instance of another account.

If you want to immediately migrate the website configurations, submit a ticket or apply for a protection period cancellation for this domain name in the DingTalk customer support group. After the protection period is canceled, you can add the website configurations to the WAF instance of another account.

2.2. Verify domain name settings

After you have added a domain name to the WAF console and before changing the DNS record to redirect requests to WAF for protection, we recommend that you change the DNS record on a local computer to verify WAF domain name settings. This example in this topic is performed on a Windows machine. The example describes how to verify the domain name settings on your local computer.

hosts local access WAF

Prerequisites

The domain name has been added to the WAF console. For more information, see Add domain names.

Context

You can configure address-to-name mapping of your local computer by modifying its *hosts* file. This means the DNS record takes effect on only the local computer. During the verification, you

must resolve the domain name of your website to the IP address of WAF on a local computer. If you can access the domain name added to the WAF console from a local computer, the domain name settings in WAF are correct. The step on a local computer prevents access exceptions caused by incorrect domain name settings.

Procedure

The following procedure describes how to verify domain name settings on a local computer that runs Windows.

1. Open File Server Resource Manager on your local computer.
2. In the address bar, enter *C:\Windows\System32\drivers\etc\hosts* and open the *hosts* file with Notepad or Notepad++.
3. Append the following content to the *hosts* file:

   ```
   <WAF IP address> <Protected domain name>
   ```

   where, `<Protected domain name>` is the domain name that you added to WAF. `<WAF IP address>` is the WAF IP address that is mapped to the domain name. Separate `<WAF IP address>` and `<Protected domain name>` with a space.

   To obtain the WAF IP address, follow these steps:

   i. Log on to the Web Application Firewall console.

   ii. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.

   iii. In the left-side navigation pane, choose **Asset Center** > **Website Access**.

   iv. On the **Website Access** page, move the pointer over the domain name, view and copy the WAF CNAME address of the domain name.

   

   v. Open Command Prompt in Windows.

   vi. Run the following command to obtain the WAF IP address:

   ```
   ping <WAF CNAME address that you have copied>
   ```

   vii. Record the WAF IP address in the command output.

   Assume that you have added the domain name `test.wafqa3.com` to the WAF console and the WAF IP address is `47. ***. ***.213`. Append the following content to the *hosts* file:

   ```
   47.***. ***.213 test.wafqa3.com
   ```

   

4. Save changes to the *hosts* file and run the `ping <Protected domain name>` command to verify that your changes are in effect. If your changes are in effect, the IP address in the command output is the WAF IP address that is mapped to the domain name.

   If the origin IP address is displayed, try refreshing the local DNS cache. You can run the `ipconfig` or `flushdns` command to refresh the DNS cache. Then, run the ping command again until the changes take effect.

5. In the address bar of your local browser, enter the protected domain name.
   - If you can access the website, the domain name settings added to the WAF console are correct. In this case, you can restore the *hosts* file and update the DNS record to redirect traffic to WAF for protection. For more information, see Change the DNS settings.
   - If you are unable to access your website, the domain name settings added may be incorrect. We recommend that you check the domain name settings in the WAF console and perform the verification again after troubleshooting. For more information, see Add domain names.
6. (Optional)Simulate simple web attack commands to verify whether WAF works properly. For example, in your browser's address bar, enter `<Protected domain name>/alert(xss)`, a web attack request, and verify whether WAF blocks the attack.
7. After the verification is complete, delete the record added in Step 3 from the *hosts* file.

> **Notice** Delete the record after the verification is complete. Otherwise, exceptions may occur when the local computer sends requests to the protected domain name.

Contact technical support

If you cannot identify any faults in domain name settings, contact technical support for help with the following ways:

- Log on to the WAF console. At the lower part of the left-side navigation pane, click **Meet Expert**, join the WAF emergency handling DingTalk group by scanning the DingTalk code, and contact Alibaba Cloud security experts for assistance.
- Submit a ticket.

2.3. Change the DNS settings

After you add a domain name to the WAF console, you must use the CNAME address (or IP address) of WAF to change the DNS settings. To ensure website security, requests from your website are then resolved to WAF for traffic scrubbing. This topic describes how to change DNS settings.

Prerequisites

- The website configurations are added to the WAF console. For more information, see Add domain names
- You have the permissions to change DNS records at your DNS service provider.
- (Optional)Requests from WAF back-to-origin CIDR blocks are allowed. For more information, see Allow access from WAF back-to-origin CIDR blocks.

  > **Notice** If you use security software such as FortiGate for your origin server, you must add the WAF back-to-origin CIDR blocks to the whitelist of the software. This prevents normal traffic from being blocked by access control policies.

- (Optional)The forwarding configurations for your website are correct and valid. Before you change the DNS settings, you must verify that the website forwarding configurations are correct. This prevents service interruptions caused by incorrect configurations. For more information, see Verify domain name settings.

> **Warning** If you change the DNS settings before the forwarding configurations for your website take effect, service interruptions may occur.

Context

WAF redirects requests in either one of the following methods:

- CNAME record: resolves the domain name to the WAF CNAME address.

  We recommend that you use the CNAME record method. If an error occurs, such as node failures or failures in a data center, the CNAME record allows WAF to use another WAF IP address or directs the requests to the origin server directly. This ensures business continuity and provides high availability and disaster recovery capabilities.

- A record: resolves the domain name to the WAF IP address.

  We recommend that you use the A record method only when the CNAME record conflicts with the current DNS settings. For example, the CNAME record conflicts with the MX record, and the MX record must be retained.

The following content describes how to configure WAF for a website that does not use proxy services such as CDN and Anti-DDoS Pro. If you need to deploy both WAF and other proxy services, see the following topics:

- Deploy WAF and CDN together
- Deploy WAF and Anti-DDoS Pro together

Obtain the WAF CNAME address and WAF IP address

You must obtain the WAF CNAME address or WAF IP address of your domain name before you change the DNS settings. If you have already obtained the address when you add the domain name, skip the following steps.

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Asset Center** > **Website Access**.
4. On the **Website Access** page, find and move the pointer over the target domain name and copy the WAF CNAME address of the domain name.

   

5. (Optional) Obtain the WAF IP address of the domain name.

   > **Note** Perform this step when you use the A record method. If you use the CNAME record, skip this step.

   i. Open Command Prompt in Windows.

   ii. Run the following command to obtain the WAF IP address:

   ```
   ping <WAF CNAME address that you have copied>
   ```

   iii. Record the WAF IP address in the command output.

Use Alibaba Cloud DNS to change the DNS records

The following example demonstrates how to change the DNS records in Alibaba Cloud DNS. If your domain name is hosted on Alibaba Cloud DNS, perform the following steps to change the DNS records. If your domain name is not hosted on Alibaba Cloud DNS, refer to the following steps to change the DNS records at your DNS service provider.

1. Log on to Alibaba Cloud DNS console.
2. On the **Manage DNS** page, find the target domain name and click **Configure** in the Actions column.
3. On the **DNS Settings** page, find the target record in the **Host** column and click **Edit** in the Actions column. In the following example, `aliyun.com` is used:
   - **www**: used to select domain names that begin with www, such as `www.aliyun.com`.
   - **@**: matches the root domain name, for example, `aliyun.com`.
   - *: matches all wildcard domain names including root domain names and subdomain names, such as `blog.aliyun.com`, `www.aliyun.com`, and `aliyun.com`.
4. In the **Edit Record** dialog box, select either the CNAME record or the A record to change the record.
   - **CNAME record**: Set **Type** to **CNAME** and **Value** to the WAF CNAME address and keep other settings unchanged.

     > **Note** We recommend that you set the TTL to 10 minutes. The greater the TTL is, the longer it takes to synchronize and change the DNS records.

     Note the following descriptions about conflicts:

     - You can specify only one CNAME record for each host record. Set Value to the WAF CNAME address.
     - Different record types conflict with each other. For example, a CNAME record, an A record, an MX record, and a TXT record cannot exist at the same time under the same host record. If you cannot change the record type, delete all conflicting records, and then add a new CNAME record.

       > **Warning** You must delete all conflicting records and add the new CNAME record. This must be completed in a short period of time. Otherwise, your domain name becomes inaccessible.

     - If you must retain the MX record, we recommend that you use the A record method to resolve the domain name to the WAF IP address.
   - **A record**: Set **Type** to **A** and **Value** to the WAF IP address and keep other settings unchanged.

     > **Note** We recommend that you set the TTL to 10 minutes. The greater the TTL is, the longer it takes to synchronize and change the DNS records.

5. Click **OK** and wait for the DNS records to take effect
6. Verify the DNS settings. You can ping the website domain name or use a DNS detection tool to verify whether the DNS records take effect.

> **Note** It takes some time for the DNS records to take effect. If the verification fails, verify the DNS records again in 10 minutes.

7. Check the DNS resolution status.
   i. Log on to the Web Application Firewall console.
   ii. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
   iii. In the left-side navigation pane, choose **Asset Center** > **Website Access**.
   iv. On the **Website Access** page, find the added domain name and view its **DNS Status**.

   

   The **DNS Status** of the domain name is **Normal** only when it is resolved to the CNAME address of WAF and WAF detects access traffic to it.

   v. (Optional)If **DNS Status** is **Abnormal**, click the  icon to query the cause.

   Common causes include **No traffic through the CNAME is detected** and **No Traffic**. After the exception is fixed, click the  icon to perform the check again.

   If you confirm that the DNS settings are correct, check the DNS resolution status again in an hour or troubleshoot the errors. For more information, see DNS resolution status exception.

   > **Note** The DNS resolution status only indicates whether you have correctly configured WAF for your website. It does not indicate whether your website is accessible.

References

- Protect the origin server.

  If the IP address of your origin server is exposed, attackers may bypass WAF and directly attack your origin server. To avoid such attacks, we recommend that you configure an ECS security group or SLB whitelist policy to block malicious requests. For more information, see Configure protection for your origin server.

- Retrieve actual IP addresses of clients.

  After you configure WAF for your website, all requests are forwarded to WAF, and WAF returns the processed requests back to the origin server. In this case, you need to use the `X-Forwarded-For` request header to retrieve the actual IP addresses of clients. For more information, see Retrieve actual IP addresses of clients.

2.4. Configure protection for your origin server

After you add your website to the WAF console, you can configure access control policies for your origin server to allow inbound traffic from only WAF back-to-origin CIDR blocks. This protects you from direct-to-origin attacks. This topic describes how to configure security group rules and whitelist policies for an origin server that is deployed on ECS and SLB instances.

Prerequisites

- The origin server is deployed on the ECS and SLB instances. All domain names deployed on those instances are added to and protected by WAF. For more information, see Add domain names.
- The traffic to the website has been resolved to WAF for protection. This means the DNS resolution status of the domain name is normal in the WAF console. For more information, see Check the DNS resolution status.

Precautions

After you add your website to the WAF console for protection, the traffic is always be forwarded, regardless of whether you configure protection for your origin server. If the IP address of your origin server is exposed, malicious parties can bypass WAF and launch direct-to-origin attacks. This function can prevent such attacks. For more information about how to determine whether the IP address of your origin server is exposed, see FAQ.

Risks may arise when you configure the access control policies on the origin server. Take note of the following items before you configure protection for the origin server:

- Make sure that all domain names whose origin servers are deployed on ECS and SLB instances are added to the WAF console.
- If a WAF cluster fails, requests may be forwarded to the origin server in bypass mode to avoid service interruptions. In this case, if you have configured the ECS security group or SLB whitelist policies for the origin server, users may not be able to access your origin server from the Internet.
- If back-to-origin CIDR blocks are added after WAF cluster scale-out and you have configured the ECS security group and SLB whitelist policies for the origin server, HTTP 5xx errors may be frequently reported.

Obtain WAF back-to-origin CIDR blocks

> **Notice** The WAF back-to-origin CIDR blocks are updated on a regular basis. Pay attention to update notifications and make sure that you add the updated back-to-origin CIDR blocks to the security group and whitelist policies in a timely manner to avoid service interruption.

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **System Management** > **Product Information**.

4. In the lower part of the **Product Information** page, find the **WAF IP Segments** section and click **Copy All IPs**.The **WAF IP Segments** section displays the latest back-to-origin CIDR blocks.

Configure ECS security group rules

If your origin server is deployed on an ECS instance, you must configure security group rules for the ECS instance after obtaining the WAF back-to-origin CIDR blocks. These security group rules only allow inbound traffic from the WAF back-to-origin CIDR blocks.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images** > **Instances**.
3. In the top navigation bar, select the resource group and region of the ECS instance.
4. In the **Instances** section, find the target instance and choose **More** > **Network and Security Group** > **Configure Security Group** in the Actions column.
5. Find the security group that you want to configure and click **Add Rules** in the Actions column.
6. Click **Add Security Group Rule**.
7. In the **Add Security Group Rule** dialog box, specify the required parameters and click **OK**.

Parameter	Description
NIC Type	The default NIC type is the same as the network type of the ECS instance. ○ When the network type of the ECS instance is VPC, the default value is **Internal**. ○ When the network type of the ECS instance is a classic network, set **NIC Type** to **Public**.
Rule Direction	Select **Inbound**.
Action	Select **Allow**.
Protocol Type	Select **Custom TCP**.
Port Range	Enter **80/443**.
Priority	Enter **1**, which indicates the highest priority.
Authorization Type	Select **IPv4 CIDR Block**.

Parameter	Description
Authorization Object	Paste the copied back-to-origin CIDR blocks. CIDR blocks follow the 10.x.x.x/32 format. Separate multiple CIDR blocks with commas (,). You can add up to 10 CIDR blocks to each security group rule. Note We recommend that you put all WAF back-to-origin CIDR blocks into multiple security groups and add multiple security group rules for authorization.
Description	The description of the security group rule. Example: Allow inbound traffic from the WAF back-to-origin CIDR blocks.

The security group rule that you added takes the highest priority and allows all inbound traffic from the WAF back-to-origin CIDR blocks.

Warning Make sure that you add all WAF back-to-origin CIDR blocks to the security group rules. Otherwise, access exceptions may occur.

8. Add another security group rule with the lowest priority and configure it as follows to block all accesses.

The following table lists the specific rule configurations.

Parameter	Description
NIC Type	The default NIC type is the same as the network type of the ECS instance. ○ When the network type of the ECS instance is VPC, the default value is Internal. ○ When the network type of the ECS instance is a classic network, set NIC Type to Public.
Rule Direction	Select Inbound.
Authorization Type	Select Forbid.
Protocol Type	Select Custom TCP.
Port Range	Enter 80/443.
Priority	Enter 100, which indicates the lowest priority.
Authorization Type	Select IPv4 CIDR block.
Authorization Object	Enter 0.0.0.0/0, which indicates all CIDR blocks.

Parameter	Description
Description	The description of the security group rule. Example: Block all inbound traffic, with a priority of 100.

Note If your origin server communicates with other IP addresses or applications, you must add another security group rule to allow access from them. Alternatively, you can add a security group rule to allow access from all ports and set it to the lowest priority.

Configure SLB access control policies

If your origin server is deployed with SLB, you must obtain the WAF back-to-origin CIDR blocks and configure an access control policy (whitelist) for the SLB instance. The policy allows only the inbound traffic from the WAF back-to-origin CIDR blocks.

1. Log on to the SLB console.
2. In the left-side navigation pane, click **Access Control**.
3. Click **Create Access Control List**.
4. On the **Create Access Control List** page, configure the following policy group and click **OK**.

Parameter	Description
Access Control List Name	The name of the custom policy group. Example: WAF back-to-origin CIDR block
Resource Group	Select the resource group to which the policy group belongs.
IP Version	Select IPv4.
Add Multiple Addresses and Descriptions	Paste all WAF back-to-origin IP addresses. Enter one entry in each line. Start a new line by pressing Enter. Note All copied WAF back-to-origin CIDR blocks are separated by commas (,). When you copy those IP addresses, we recommend that you use a text editor that supports extension replacement, such as Notepad or Word, to replace the commas (,) with line breaks (\n).

5. In the left-side navigation pane, choose **Instances > Server Load Balancers**.
6. In the **Server Load Balancers** page, find the target instance and click its ID.
7. On the **Listener** tab, find the target listener and choose > **Set Access Control**.
8. On the Access Control Settings page, turn on **Enable Access Control**, configure the following parameters, and click **OK**.

Parameter	Description
Access Control Method	Select Whitelist to allow specified IP addresses to access the SLB instance.
Access Control List	Select the access control list that you created for the WAF back-to-origin IP addresses.

What to do next

After you configure the ECS security group and SLB whitelist policies, test whether the origin IP address can be connected through ports 80 and 8080 to check whether the protection configurations are in effect.

If the origin server cannot be connected through these ports but your service is running normally, it indicates that the protection configurations are in effect.

FAQ

How can I confirm that the IP address of the origin server remains concealed?

Use Telnet to establish a connection from a host that is not deployed on Alibaba Cloud to the service port of the public IP address of your origin server.

- If the connection is established, the IP address of your origin server may be exposed. Malicious parties that obtain the public IP address can bypass WAF and launch attacks on your origin server.
- If the connection fails, your origin server is secure.

For example, test the connectivity of ports 80 and 8080 of the origin server that is protected by WAF. If the connectivity is normal, your origin server is insecure.

Reachable port of WAF

2.5. Allow access from WAF back-to-origin CIDR blocks

WAF uses specified back-to-origin CIDR blocks to forward normal traffic back to an origin server. To allow inbound traffic from the back-to-origin CIDR blocks, you must configure security software or access control policies of the origin server when you add a website to the WAF console.

Context

If you use security software such as FortiGate for your origin server, you must add the WAF back-to-origin CIDR blocks to a whitelist of the software. This prevents normal traffic forwarded by WAF to the origin server from being blocked by access control policies.

For security purposes, we recommend that you configure access control policies for the origin server to allow only inbound traffic from the WAF back-to-origin CIDR blocks. This prevents attackers from bypassing WAF and directly attacking the origin server. For more information, see Configure protection for your origin server.

Back-to-origin CIDR blocks added on April 30, 2020

On April 30, 2020, the following back-to-origin CIDR blocks were added after WAF clusters were scaled out.

- Regions in mainland China: `39.96.158.0/24,47.110.182.0/24,120.77.139.0/25,47.102.187.0/25`
- Regions outside mainland China: `47.56.50.0/24,161.117.161.0/25,147.139.22.0/25,8.209.192.0/25`

> **Warning** If your origin server has an IP address whitelist or a security group that is configured to allow only WAF back-to-origin CIDR blocks to access your origin server, you must add the new WAF back-to-origin CIDR blocks to the whitelist. Otherwise, the back-to-origin traffic forwarded by WAF may be blocked by the access control policies of the origin server, and the access may be denied.

We recommend that you add the new back-to-origin CIDR blocks to the IP address whitelist in a timely manner.

Obtain the WAF back-to-origin CIDR blocks

You can obtain the back-to-origin CIDR blocks from the following table based on the region of your WAF instance, or follow the following steps to obtain the latest back-to-origin CIDR blocks from the WAF console.

Region of the WAF instance	Back-to-origin CIDR block
Regions in mainland China	`121.43.18.0/24,120.25.115.0/24,101.200.106.0/24,120.55.177.0/24,120.27.173.0/24,120.55.107.0/24,123.57.117.0/24,120.76.16.0/24,182.92.253.32/27,60.205.193.64/27,60.205.193.96/27,120.78.44.128/26,118.178.15.0/24,39.106.237.192/26,106.15.101.96/27,47.101.16.64/27,47.106.31.0/24,47.98.74.0/25,47.97.242.96/27,112.124.159.0/24,39.96.130.0/24,39.96.119.0/24,47.99.20.0/24,47.104.53.0/26,47.108.23.192/26,39.104.199.128/26,39.96.158.0/24,47.110.182.0/24,120.77.139.0/25,47.102.187.0/25`
Regions outside mainland China	`47.89.1.160/27,47.89.7.192/26,47.88.145.96/27,47.88.250.0/24,47.52.120.0/24,47.254.217.32/27,47.88.74.0/24,47.89.132.224/27,47.91.69.64/27,47.91.54.128/27,47.74.160.0/24,47.91.113.64/27,149.129.211.0/27,149.129.140.0/27,8.208.2.192/27,47.56.50.0/24,161.117.161.0/25,147.139.22.0/25,8.209.192.0/25` **Note** If the origin server of the website is deployed in Japan, add the `8.209.192.0/25` back-to-origin CIDR block.

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **System Management** > **Product Information**.
4. In the lower part of the **Product Information** page, find the **WAF IP Segments** section and click **Copy All IPs**.The **WAF IP Segments** section displays the latest back-to-origin CIDR blocks.

What to do next

After you obtain the WAF back-to-origin CIDR blocks, you can add them to the IP address whitelist of your origin security software.

> **Warning** If you do not add the WAF back-to-origin CIDR blocks to the IP address whitelist of the origin server, normal requests sent by WAF may be rejected. This may cause a service interruption.

3.Connect cloud services to WAF

3.1. Deploy WAF and CDN together

You can deploy Alibaba Cloud WAF and CDN (Content Delivery Network) together to speed up your website and protect against web attacks at the same time. We recommend that you use the following architecture: CDN (entry layer, website speed up) > WAF (intermediate layer, web attacks protection) > Origin.

Procedure

Suppose you use Alibaba Cloud CDN. Follow these steps to deploy WAF and CDN together:

1. See Get started with Alibaba Cloud CDN to implement a CDN for your domain name.
2. Create a website configuration in Alibaba Cloud WAF.
   - **Domain name**: Enter the CDN-enabled domain name. Wildcard is supported.
   - **Server address**: Enter the public IP address of the ECS/Server Load Balancer instance, or the external server IP address of the origin server.
   - **Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?**: Check **yes**.

   For more information, see Website configuration.
3. When the website configuration is successfully created, WAF generates a dedicated CNAME address for it.

   > **Note** For more information about how to view the WAF CNAME address, see WAF deployment guide.
4. Modify the CDN configuration to change the origin site address to the WAF CNAME address.
   i. Log on to the Alibaba Cloud CDN console.
   ii. Go to the **Domain Names** page, select the domain to be configured, and click **Configure**.
   iii. Under **Origin site settings**, click **Modify**.
   iv. Modify origin site information.
      - **Type**: Select **Origin Site**.
      - **Origin site address IP**: Enter the WAF CNAME address.
      - **Use the same protocol as the back-to-source protocol**: Select Enable.
   v. Under **Back-to-Source Settings**, make sure that **Back-to-Source host** is disabled.

After the operation is complete, the traffic goes through CDN, and the dynamic content continues to be checked and protected by WAF.

3.2. Deploy WAF and Anti-DDoS Pro together

Alibaba Cloud WAF and Anti-DDoS Pro and are fully compatible. You can use the following architecture to deploy WAF and Anti-DDoS Pro together: Anti-DDoS Pro (entry layer, DDoS attack protection) > WAF (intermediate layer, web attack protection) > Origin.

Procedure

1. Create a website configuration for your website in Alibaba Cloud WAF.
   - **Server address**: Check **IP** and enter the public IP address of the ECS instance/Server Load Balancer instance or external server IP address.
   - **Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?**: Check **yes**.

   For more information, see Website configuration.
2. Create a web service access configuration for your website in Anti-DDoS Pro. The procedure is as follows:
   i. On the **Access > Web Service** page, click **Add Domain**.
   ii. In the **Fill in the domain name information** task, do the following:
      - **Domain name**: Enter the domain name to be protected.
      - **Protocol**: Check the supported protocol.
      - **Origin IP/Domain**: Check **Origin site domain** and enter the WAF CNAME address.

        Note For more information about how to view the WAF CNAME address, see WAF deployment guide.

   iii. Click **Next**.
   iv. Complete the **Please choose Instance and ISP Line** task.
3. Update the DNS settings of your domain name. Log on to the DNS host's system and add a CNAME record to redirect web traffic to the Anti-DDoS Pro CNAME address.

   For more information, see Access Anti-DDoS Pro through a CNAME record.

Result

All web requests to your website are redirected to Anti-DDoS Pro for cleanup and then redirected to WAF for inspection before they reach your origin server.

4.Supported custom ports

Web Application Firewall (WAF) protects services at specific non-standard ports and services at standard HTTP ports 80 and 8080 and HTTPS ports 443 and 8443. If your origin server uses ports other than 80 and 443, you must customize server ports when you configure WAF. Then, WAF redirects traffic for your website at the custom server ports.

Prerequisites

- Your website is added to the WAF console. For more information, see Add domain names.

  Note This topic describes how to customize server ports by editing an existing domain name in the WAF console. Alternatively, you can customize server ports when you manually add a website to the WAF console for protection. For more information, see Manually add website configurations.

- To use ports other than 80, 8080, 443, and 8443, you must make sure that the WAF instance that you purchased meets the following specification requirements:
  -

Context

WAF forwards traffic only on specified ports of the origin server. For ports that are not configured, WAF does not forward any traffic on these ports.

Limits

Ports

If you use WAF Business or Enterprise, the following ports are available:

Note The query results displayed in the WAF console prevail. For more information, see Allowed Port Range.

- HTTP-compliant

  80, 81, 82, 83, 84, 86, 87, 88, 89, 97, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9999, 10000, 10001, 10080, 12601, 28080, 33702, and 48800

  Notice Only the WAF instances deployed in the regions in mainland China support port 48800.

- HTTPS-compliant

  443, 4443, 5443, 6443, 7443, 8443, 8553, 8663, 9443, 9553, 9663, and 18980

> **Notice** Only the WAF instances deployed in the regions in mainland China support port 18980.

Port quantity

The total number of ports that can be used by each WAF instance for all websites has the following limits:

- A WAF Business instance on a subscription basis supports a maximum of 10 ports, including ports 80, 8080, 443, and 8443.
- A WAFEnterprise instance on a subscription basis supports a maximum of 50 ports, including ports 80, 8080, 443, and 8443.

> **Note** A WAF Exclusive instance supports more non-standard ports. You can use HTTP ports, HTTPS ports, and HTTP/2 ports as back-to-origin ports. For more information, see Create an exclusive cluster.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Asset Center** > **Website Access**.
4. On the **Website Access** page, find the target domain name and click **Edit** in the Actions column.
5. On the **Edit** page, click **Customize** in the **Destination Server Port** section.
6. Click the required protocol type (valid values: **HTTP** and **HTTPS**), enter the ports that you want to add, and click **Save**.

   > **Note** The ports that you entered must be within the allowed port range. Otherwise, the settings cannot be saved. You can click **View Allowed Port Range** to check whether the specified ports are within the allowed port range.

7. Click **Confirm**.

5.Retrieve actual IP addresses of clients

If you deploy proxy servers, such as CDN, Anti-DDoS Premium, Anti-DDoS Pro, or WAF, on your website, the origin server can use the X-Forwarded-For header in back-to-origin requests to retrieve actual IP addresses of clients. This topic describes how to configure web application servers, such as NGINX, IIS 6, IIS 7, Apache, and Tomcat servers, and Kubernetes containers to retrieve the IP addresses of clients.

Background information

In most scenarios, access requests initiated from the browsers of clients (visitors) are not directly sent to the origin server of a website. Instead, the access requests may pass through intermediate proxy servers, such as CDN, Anti-DDoS Premium, Anti-DDoS Pro, or WAF. During the process, these access requests are forwarded through multiple proxies for security and acceleration. This increases the difficulty in retrieving the actual IP addresses of the clients that initiated the requests.

To address the issue, the X-Forwarded-For header is implemented to record the actual IP addresses of the clients. The transparent proxy adds the X-Forwarded-For header to the HTTP request header before forwarding the access requests to the next-hop server. The header is in the `X-Forwarded-For:Client IP address` format. If the access requests pass through multiple intermediate proxy servers, the X-Forwarded-For header records the actual IP addresses of the clients and IP addresses of intermediate proxy servers. The header records multiple IP addresses separated by a comma (,), such as `X-Forwarded-For:Client IP address, IP address of Proxy Server 1, IP address of Proxy Server 2, IP address of Proxy Server 3, ...` .

Therefore, common web application servers can use the X-Forwarded-For header to retrieve the actual IP addresses of the clients.

The following content demonstrates how to configure the X-Forwarded-For header on the NGINX, IIS 6, IIS 7, Apache, and Tomcat servers, as well as on the Kubernetes containers.

> **Notice** Before you start, make sure that you have backed up the existing environment, including ECS instance snapshots and configuration files of the web application servers.

Configure NGINX servers

The NGINX servers use an http_realip_module module to retrieve the actual IP addresses of the clients.

1. Install the http_realip_module module. Run the `# nginx -V | grep http_realip_module` command on the NGINX server to check whether the module is installed. If the module is not installed, recompile NGINX and load the module.

   > **Note** This module is not installed when NGINX is installed by using a quick installation package.

   Install the http_realip_module module by using the following method:

```
wget http://nginx.org/download/nginx-1.12.2.tar.gz
tar zxvf nginx-1.12.2.tar.gz
cd nginx-1.12.2
./configure --user=www --group=www --prefix=/alidata/server/nginx --with-http_stub_status_mo
dule --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

2. Modify the configuration file of NGINX.
   i. Open the `default.conf` configuration file.
   ii. Add the following content to `location / {}` :

```
set_real_ip_from <ip_range1>;
set_real_ip_from <ip_range2>;
...
set_real_ip_from <ip_rangex>;
real_ip_header X-Forwarded-For;
```

   where, `<ip_range1>` , `<ip_range2>` , and `<ip_rangex>` are the back-to-origin IP addresses of WAF. For more information about the back-to-origin CIDR blocks of WAF, see Allow access from WAF back-to-origin CIDR blocks.

   Enter one back-to-origin IP address in each line. If the back-to-origin IP addresses of the proxy servers include 10.0.0.1, 10.0.0.2, and 10.0.0.3, use the format similar to:

```
set_real_ip_from 10.0.0.1;
set_real_ip_from 10.0.0.2;
set_real_ip_from 10.0.0.3;
real_ip_header X-Forwarded-For;
```

3. Modify the log format.
   i. Open the `nginx.conf` configuration file. `log_format` is typically located in the HTTP configuration.
   ii. In `log_format` , replace the `remote-address` field with the `x-forwarded-for` field.The modified log_format is as follows:

```
log_format  main  '$http_x_forwarded_for - $remote_user [$time_local] "$request" ' '$status $
body_bytes_sent "$http_referer" ' '"$http_user_agent" ';
```

4. Run the `nginx -s reload` command to restart NGINX.
   The configurations take effect after the restart. The NGINX server records the actual IP addresses of the clients by using the X-Forwarded-For header.

Configure IIS 6 servers

You must install the `F5XForwardedFor.dll` plug-in to retrieve the actual IP addresses of the clients from the access log recorded by an IIS 6 server.

1. Depending on your server OS version, copy the `F5XForwardedFor.dll` file from the `x86\Release` or `x64\Release` directory to a custom directory, such as `C:\ISAPIFilters`.

   > **Note** Make sure that the IIS process has read and write permissions on the custom directory.

   If the plug-in is unavailable from the directory, click F5XForwardedFor.dll to download it.
2. Open Internet Information Services (IIS) Manager, find the website, right-click the website, and select **Properties**.
3. In the **Default Web Site Properties** dialog box that appears, click the **ISAPI Filters** tab and click **Add**.
4. In the Add ISAPI Filter dialog box, set the following parameters and click **OK**.
   - **Filter name**: Enter `F5XForwardedFor`.
   - **Executable**: Enter the complete path of `F5XForwardedFor.dll`, for example, `C:\ISAPIFilters\F5XForwardedFor.dll`.
5. Restart the IIS server for the configurations to take effect.

Configure IIS 7 servers

You can install the F5XForwardedFor module to retrieve the actual IP addresses of the clients from the access log recorded by an IIS 7 server.

1. Depending on your server OS version, copy the `F5XFFHttpModule.dll` and `F5XFFHttpModule.ini` files from the `x86\Release` or `x64\Release` directory to a custom directory, such as `C:\x_forwarded_for\x86` or `C:\x_forwarded_for\x64`.

   > **Note** Make sure that the IIS process has read and write permissions on the custom directory.

   If the files are unavailable from the directory, click F5XForwardedFor to download it.
2. In the **IIS Server** section, double-click **Module**.
3. Click **Configure Local Module**.
4. In the **Configure Local Module** dialog box, click **Register** to register the DLL file.
   - Register the x_forwarded_for_x86 module in a 32-bit system.
     - **Name**: Enter `x_forwarded_for_x86`.
     - **Path**: Enter the full path of the `F5XFFHttpModule.dll` module, for example `C:\x_forwarded_for\x86\F5XFFHttpModule.dll`.
   - Register the x_forwarded_for_x64 module in a 64-bit system.

- **Name**: Enter `x_forwarded_for_x64`.
- **Path**: Enter the full patch of the `F5XFFHttpModule.dll` module, for example *C:\x_forwarded_for\x64\F5XFFHttpModule.dll*.

5. In the **Configure Local Module** dialog box, select the newly registered x_forwarded_for_x86 or x_forwarded_for_x64 module and click **OK**.
6. In the **ISAPI and CGI Restrictions** section, add the registered DLL file and set **Restriction** to **Allow**.
7. Restart the IIS server and wait for the configurations to take effect.

Configure Apache servers

Configure Apache servers in Windows.

The installation packages of Apache 2.4 and later provide the remoteip_module module file (`mod_remoteip.so`). You can use this module to retrieve the actual IP addresses of clients.

1. Create a configuration file named `httpd-remoteip.conf` in the extra configuration folder of Apache (`conf/extra/`).

   > **Note** You can load the related configurations by importing the `remoteip.conf` configuration file. This reduces the number of times that you modify the `httpd.conf` file and avoids service exceptions due to misoperations.

2. Add the following content to the `httpd-remoteip.conf` configuration file:

   ```
   # Load the mod_remoteip.so module.
   LoadModule remoteip_module modules/mod_remoteip.so
   # Set the RemoteIPHeader header.
   RemoteIPHeader X-Forwarded-For
   # Set the back-to-origin IP addresses.
   RemoteIPInternalProxy <ip_range1> <ip_range2> ..... <ip_rangex>
   ```

   where, `<ip_range1>`, `<ip_range2>`, and `<ip_rangex>` are the back-to-origin IP addresses of WAF. For more information about the back-to-origin CIDR blocks of WAF, see Allow access from WAF back-to-origin CIDR blocks.

   Separate multiple back-to-origin IP addresses with spaces. If the IP addresses of the proxy servers include 10.0.0.1, 10.0.0.2, and 10.0.0.3, use the format similar to:

   ```
   RemoteIPInternalProxy 10.0.0.1 10.0.0.2 10.0.0.3
   ```

3. Add the following content to the *conf/httpd.conf* configuration file:

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

   The preceding content inserts the `httpd-remoteip.conf` configuration file into *conf/httpd.conf*.

4. Modify the log format in the `httpd.conf` configuration file.

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

5. Restart Apache for the configurations to take effect.

Configure Apache servers in Linux.

Follow the preceding steps to add the remoteip_module module (`mod_remoteip.so`) and configure the log format to retrieve the actual IP addresses of clients. This module is included in Apache 2.4 and later.

If the version of Apache is earlier than 2.4, install mod_rpaf (third-party module) to retrieve the actual IP addresses of clients.

1. Install the mod_rpaf module.

```
wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

2. Append the following content to the `/alidata/server/httpd/conf/httpd.conf` configuration file of Apache:

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

where, `<rpaf IP address>` is the IP address of the mod_rpaf module. You can query the specific IP addresses in the Apache log. Do not use the IP addresses of the proxy servers. Typically, two IP addresses are included, as shown in the following example:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 10. ***. ***.65 10. ***. ***.131
RPAFheader X-Forwarded-For
```

3. Restart Apache for the configurations to take effect.

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

For more information about the Apache modules, see Apache help document.

Configure Tomcat servers

Take the following steps to allow the Tomcat servers to retrieve the actual IP addresses of clients by using the X-Forwarded-For header.

1. Open the `tomcat/conf/server.xml` configuration file.
2. Modify the AccessLogValve logging function as follows:

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T" resolveHosts="fal
se"/>
```

Configure Kubernetes containers

If your ECS instance is deployed on Kubernetes, Kubernetes records the actual IP addresses of clients in the X-Original-Forwarded-For field and the back-to-origin IP addresses of WAF in the X-Forwarded-For field. To obtain the actual IP addresses of clients, you must modify the container configuration file to enable an Ingress controller to add them to the X-Forwarded-For field.

You can modify the container configuration file by performing the following steps:

1. Run the following command to modify the `kube-system/nginx-configuration` configuration file:

```
kubectl -n kube-system edit cm nginx-configuration
```

2. Add the following content to the configuration file:

```
compute-full-forwarded-for: "true"
forwarded-for-header: "X-Forwarded-For"
use-forwarded-headers: "true"
```

3. Save the configuration file.
   The configurations take effect immediately after you save the configuration file. Then, the Ingress controller adds the actual IP addresses of clients to the X-Forwarded-For field.
4. Change the field you use to obtain the actual IP addresses of clients to the X-Original-Forwarded-For field.