Alibaba Cloud Web应用防火墙

Statistics and Analysis

Issue: 20200704



Legal disclaimer

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

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

- 5. By law, all the 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 include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
- 6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

| Style | Description | Example |
|--------------|--|---|
| 0 | 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. |
| | 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. |
| ! | 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. |
| Ê | 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 listinstanceid Instance_ID |
| [] or [alb] | This format is used for an optional value, where only one item can be selected. | ipconfig [-all -t] |

| Style | Description | Example |
|-------------|--|-----------------------|
| {} or {alb} | This format is used for a required value, where only one item can be selected. | switch {active stand} |

Contents

| Legal disclaimer | . I |
|----------------------------|-------------|
| Document conventions | I |
| 1 View overall information | 1 |
| 2 View security reports | . 11 |
| 3 Data visualization | . 20 |

1 View overall information

This topic describes the Overview page of the Web Application Firewall (WAF) console. The Overview page displays the protection information of websites that are added to WAF, including attack events, emergency vulnerabilities, protection statistics, and request analysis charts. You can obtain the security status of your website and perform security analysis based on the information displayed on this page.

Access the Overview page

- **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 , in which the instance is deployed.
- 3. In the left-side navigation pane, click .
- 4. In the upper-left corner of the **Overview** page that appears, specify the target domain (all domains or a single domain) and the time period (Real-time, Today, 7 Days, 30 Days, or Customize) to view the overall information.

| Over | view | | | |
|----------------------|---------------|----------|---------|--------|
| All | | | | \sim |
| Real-tim Customi: | e Today ze | 7 Days | 30 Days | |
| Events | Vulnerat | oilities | | |

Note:

The overall information for the last 30 days is available. You can customize a time period within the last 30 days.

Overall information

The Overview page includes the following three parts:

- Event list and emergency vulnerability records (area 1 in the figure)
- Protection statistics (area 2 in the figure)
- Request analysis charts (area 3 in the figure)

| Overview | | | | | | | |
|---|---|---|---|--|---|---|------------------------------|
| All Real-time Today 7 Days 30 Days Customize | 2 All 49,341 Times | Web Intrusion Pr 106 Times | HTTP Flood Prot O Times | Scan Protection 75 Times | Access Control | Blocked Bot Attacks 246 Times | |
| Events Vulnerabilities Update FasterXML jackson-databind / Fastjson Remote Code Execution Policy(databind#2704) Updated On: May 8, 2020 Update FasterXML jackson-databind / Fastjson Remote Code Execution Policy(databind#2688) Updated On: Apr 28, 2020 Update FasterXML jackson-databind / Fastjson Remote Code Execution Policy(databind#2689) | Requests QPS E 10,000 8,000 6,000 4,000 2,000 0 Apr 22, 2020 9:00 - All | AM Apr 28, 2020 6: • Web Intrusion Preventio | Code 30 PM May 5, 2020 n — HTTP Flood Protect | 4:00 AM May 11, ion — Scan Protection | 2020 1:30 PM May 17 | 7, 2020 11:00 PM Blocked Bot Attacks | 3 |
| Updated On: Apr 28, 2020 Update FasterXML jackson-databind / Fastjson Remote Code Execution Policy(databind#2698) Updated On: Apr 28, 2020 Update TongDa OA Unauthorized Login | Browser Distribution | Top UserAgents | robot/spider 86.33% | URL Requests | Top IP api/ | | 2,796 1,562 866 857 |
| Updated On: Apr 22, 2020 Update FasterXML jackson-databind / Update FasterXML jackson-databind / Fastjson Remote Code Execution Policy/databind=29(8) | | | downloading tool 3.48% chrome 1.01% firefox 0.21% microsoft edge 0.01% | 5 | onfig.do ıll/order/p plnfo pi/ | pull | 805 637 532 459 |
| Updated On: Apr 28, 2020 Update FasterXML jackson-databind / Fastjson Remote Code Execution Policy(databind#2698) Updated On: Apr 28, 2020 Update TongDa OA Unauthorized Login | Attack Distribution | | | | nch pi/ | | 454 |
| Policy Updated On: Apr 22, 2020 Update FasterXML jackson-databind / Fastijson Remote Code Execution Policy(UC=2020-11113) Updated On: Apr 9, 2020 | | | Tempo | ් rarily no data! | | | |

Event list and emergency vulnerability records

The **Vulnerabilities** tab is displayed by default. You can view the updates to the protection rules for the latest disclosed security vulnerabilities on this tab.

The **Events** tab displays historical security events. WAF aggregates the blocked attacks into events so that you can quickly identify attacks and threats to your website.



Note:

If you select all domains, the total numbers of attacks and events on all domains are displayed. You can also select a specific domain to view the relevant events.

Web Application Firewall classifies the attacks into events based on the attack type, severity, frequency, and time. The events are classified into the following types: invalid request blocking, HTTP flood attack blocking, web attack blocking, request blocking based on precise access control, request blocking based on region blocking policies, and request blocking based on continuous attack protection.

| @ 116811Attacks | 18 days ago |
|-----------------|-------------|
| 55615Attacks | 18 days ago |
| 38310Attacks | 19 days ago |
| 🧟 69941Attacks | 19 days ago |
| ⓓ 69941Attacks | 19 days ago |
| 5380Attacks | 19 days ago |
| 💮 97817Attacks | 19 days ago |

You can click an event to view information of the event and the related data of the event type. For example, in the HTTP Flood Protection area, you can view the top 5 source IP addresses that initiate the most attacks, user agents, referrers, and requested URLs of the attacks. You can also view the number of attacks that are blocked for each of these items. You can also view the protection suggestions provided below the data.

| HTTP Flood Protection | | | |
|---|-------------------------|------------------------|--------|
| May 30, 2019 10:49 AM → May 30, 2019 10: | 57 AM | | |
| Requests Blocked Attacks 157256 Times 116811 Time | Peak Q es 391 | PS | |
| Attack Source IP | | UserAgent | |
| 1 Shanghai | 34920 | python-requests/2.18.4 | 116811 |
| 1 Shanghai | 29580 | No data | 0 |
| 57) Afghanistan | 29286 | No data | 0 |
| 2 Sichuan | 28976 | No data | 0 |
| 103. Australia | 28969 | No data | 0 |
| Referer | | URL | |
| | 116811 | No data | 0 |
| No data | 0 | No data | 0 |
| No data | 0 | No data | 0 |
| No data | 0 | No data | 0 |
| No data | 0 | No data | 0 |
| Suggestion We recommend the following sol | lutions: | | |

Protection statistics

This area displays the number of **all** received requests and the numbers of the following types of protection requests, including **Web Intrusion Prevention**, **HTTP Flood Protection**, **Scan Protection**, **Access Control**, and **Blocked Bot Attacks**.



The Blocked Bot Attacks module is available only in the new protection engine. For more information, see **#unique_4**.



You can click the number of requests under each protection module to go to the corresponding **Security report** page to view data details. For more information, see View security reports.

You can click the drop-down icon in the lower part of this area to display the trend charts of the requests in each module.



Note:

If you select all domains, the top 5 domains with the most data volume and their data are displayed.

| All 49,341 Times | Web Intrusion Pr | HTTP Flood Prot O Times | Scan Protection 75 Times | Access Control | Blocked Bot Attacks 246 Times |
|---------------------|------------------|-----------------------------------|---------------------------------|----------------|-------------------------------|
| | | | | | |
| 45,511 | 6 4 | No data 0 | ,,c 75 | | |
| 1,549 | 3 28 | No data 0 | No data 0 | . 28 | No data 0 |
| 609 | B 7 | No data 0 | No data 0 | . 9 | No data 0 |
| . 445 | 6 | No data 0 | No data 0 | No data 0 | No data 0 |
| . 308 | 1 | No data 0 | No data 0 | No data 0 | No data 0 |
| | | | ~ | | |

Request analysis charts

• Trends: displays the trends of **Requests**, **QPS**, **Bandwidth**, and **Response Code** within a specified period. The minimum time granularity is one minute.



- You can click a legend item below the trend chart to hide or show the relevant records.

- The Blocked Bot Attacks module is available only in the new protection engine. For more information, see #unique_4.
- Requests: displays the total number of requests, the number of web intrusion prevention times, the number of HTTP flood protection times, the number of scan protection times, the number of access control hits, and the number of bot protection times.



- **QPS**: displays the queries per second (QPS) of all requests, the QPS of web intrusion prevention, the QPS of HTTP flood protection, the QPS of scan protection, the QPS of access control, and the QPS of bot protection.



You can click **Average** and **Peak** in the upper-right corner of the chart to switch between the average QPS and peak QPS.



- Bandwidth: displays the inbound bandwidth and outbound bandwidth in bit/s.



- **Response Code**: displays the trends of the numbers of HTTP error codes, such as 5XX, 405, 499, 302, and 444.

Note:

You can click **WAF to Client** and **Origin Server to WAF** in the upper-right corner of the trend chart to view the distributions of response codes from the WAF instance to the client and those from the origin server to the WAF instance.



• **Browser Distribution** tab: On this tab, a pie chart shows the distribution of browsers used by the request sources.



• **Top UserAgents** tab: On this tab, the most often used user agents and corresponding requests are displayed.

| Browser Distribution Top UserAgents | |
|---|--------|
| python-requests/2.20.0 | 44,021 |
| - | 1,506 |
| curl/7.54.0 | 1,494 |
| PostmanRuntime/7.24.1 | 1,289 |
| curl/7.68.0 | 236 |
| Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) Ap | 227 |
| Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) Ap | 203 |
| mozilla/5.0 (compatible; baiduspider/2.0; http://ww | 167 |
| Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) | 92 |
| Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) Ap | 68 |

• URL Requests tab: On this tab, the URLs that are often requested and the number of requests are displayed.

| URL Requests | Top IP | |
|--------------|---------------------------|-------|
| | /collect/log | 2,796 |
| · | /mile-video-api/ | 1,562 |
| | /api | 866 |
| | /loggw/logUpload.do | 857 |
| 1, 1,1 | /loggw/logConfig.do | 805 |
| | /co-order-pull/order/pull | 637 |
| 1 ji i i ji | /service/getlpInfo | 532 |
| | /mile-user-api/ | 459 |
| | /v1/lead/launch | 454 |
| · . · · | /mile-task-api/ | 425 |

• **Top IP** tab: On this tab, source IP addresses that initiate the most access requests and the number of requests are displayed.

| URL Requests Top IP | |
|---------------------|-----|
| Beijing | 565 |
| Beijing | 556 |
| Australia | 483 |
| Beijing | 456 |
| Australia | 442 |
| undefined | 243 |
| Beijing | 181 |
| l Zhejiang | 163 |
| Zhejiang | 160 |
| Zhejiang | 157 |

• Attack Distribution area: In this area, the distribution of attack events is displayed.



You can click an event to view information of the event and related data of the event type.

2 View security reports

Web Application Firewall (WAF) provides security reports to display the protection records of each protection module. You can view the web security, bot management, and access control and throttling records on domains that are added to WAF. This allows you to analyze business security.

! Notice:

This topic describes security reports in the WAF console released in January 2020. If your WAF instance was created before this date, see **#unique_6**.

Prerequisites

- A Web Application Firewall instance is available. For more information, see #unique_7.
- The website is associated with the Web Application Firewall instance. For more information, see #unique_8.

Access the security report page

- 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 , in which the instance is deployed.
- **3.** In the left-side navigation pane, click .
- On the Security report page that appears, click any of the following tabs to view the reports of required types: Web Security, Bot Management, and Access Control/ Throttling.

Web Security tab

The **Web Security** tab displays protection records of the following modules: **Web Intrusion Prevention**, **Data Leakage Prevention**, **Account Security**, and **Positive Security Model**.

• Web Intrusion Prevention: displays all web application attacks blocked by WAF. This tab consists of two areas: attack statistics (area 1 in the figure) and attack details (area 2 in

| the figure). You can specify a domain and query time period to search for correspondi | ng |
|---|----|
| data. | |

| Web Security | Bot Management | Access Control/Th | rottling | | | | | | | | | |
|------------------------|---------------------|--------------------------|-----------------|---------------------------|------------------|------------------------|------------|--------------|---------------|--------------------|--------------|------|
| Web Intrusion Pre | evention Data Leak | kage Prevention A | ccount Security | y Positive Security Model | | | | | | | | |
| All | ~ | Yesterday Today 7 | 7 Days 30 Da | Apr 21, 2020 00:00 | - May | / 21, 2020 15:50 | 🛗 Sea | rch | | | | |
| 1 Security attack t | type distribution | | | Top 5 attack source ips | | | | Top 5 attack | source region | 15 | | |
| | | | | (Beijing) | | | 28 | Australia | | | | 64 |
| | | webshell 60.38% | | (Australia) | | | 24 | Beijing | | | | 41 |
| | | Other 38.68% | | I(Australia) | | _ | 21 | Shanxi1 | | | | 1 |
| | | 100 0.5470 | | (Australia) | | | 11 | No data | | | | 0 |
| | | | | (Australia) | | | 8 | No data | | | | 0 |
| | | | | | | | | | | | | |
| Regular Protection | on 🗸 All | ~ | Attack IP | Search | 1 | | | | | | | |
| 2 Attack IP | Region | Time Attacked | Attack Type | Attacked URL | Method | Parameter | Rule A | ction | Rule ID | Attack Probability | Actions | |
| | China Beijing | May 20, 2020 1:37 PM | Other | "''' n/ | GET | | Block | | 200054 | | View Details | |
| | China Beijing | May 20, 2020 1:37 PM | Other | n/ | GET | | Block | | 200054 | | View Details | |
| | China Beijing | May 20, 2020 1:37 PM | Other | n/ | GET | | Block | | 200054 | | View Details | |
| | China Beijing | May 20, 2020 1:37 PM | Other | n/ | GET | | Block | | 200054 | | View Details | |
| | China Beijing | May 20, 2020 1:37 PM | Other | n/ | GET | | Block | | 200054 | | View Details | |
| | China Beijing | May 20, 2020 1:37 PM | Other | n/ | GET | | Block | | 200054 | | View Details | |
| | China Beijing | May 20, 2020 1:37 PM | Other | n/ | GET | | Block | | 200054 | | View Details | |
| | China Beijing | May 20, 2020 1:37 PM | Other | n/ | GET | | Block | | 200054 | | View Details | |
| | Australia Australia | May 20, 2020 12:02 PM | webshell | /t | GET | | Block | | 117028 | | View Details | |
| | Australia Australia | May 20, 2020 12:02 PM | webshell | /t | GET | | Block | | 117028 | | View Details | |
| | Australia Australia | May 20, 2020 12:02 PM | webshell | /t | GET | | Block | | 117028 | | View Details | |
| | Australia Australia | May 20, 2020 12:02 PM | webshell | , /t | GET | | Block | | 117028 | | View Details | |
| | | | | Total: | 106 items, Per P | age: 10 items ltems pe | er Page 10 | 50 10 | 0 < Previ | ous 1 2 3 4 | 11 Ne | xt > |

- The attack statistics area includes **Security attack type distribution**, **Top 5 attack source ips**, and **Top 5 attack source regions**.
- The attack details area displays the following information: Attack IP, Region, Time Attacked, Attack Type, Attacked URL, Method, Parameter, Rule Action, Rule ID, and Attack Probability. You can specify the following information to search for the records that you want to view: protection module (valid values: Regular Protection and Deep

learning), attack type (valid values: SQL injection, XSS, Code execution, CRLF, Local file inclusion, Remote file inclusion, webshell, CSRF, and Other), and attack IP address.

You can click **View Details** in the Actions column that corresponds to a record to access the **Attack Detail** pane.

| Attack Detai | I |
|--------------|---------------|
| Rule ID | 200054 |
| Rule Action | Block |
| Attack Type | Other |
| Attack IP | |
| Region | China Beijing |
| Method | GET |
| URL | /1.mdb |
| Trace Id | |

For more information about how to configure web intrusion prevention, see the following topics:

- #unique_9
- #unique_10
- Data Leakage Prevention: displays the records of web requests that triggered data leakage prevention rules. The following information is provided: Attack IP, Region, Time Attacked, Attacked URL, Method, Parameter, Rule Action, Rule ID, and

Attack Probability. You can specify a domain and query time period to search for

corresponding data.

| Web Security | Bot Mana | gement | Access Control/ | Throttling | | | | | | |
|-----------------|-----------|---------|------------------|------------------|-----------------------|-----------------|--------------|---------|--------------------|---------|
| Web Intrusion P | revention | Data Le | akage Prevention | Account Security | Positive Security Mod | lel | | | | |
| All | | ~ | Yesterday Today | 7 Days 30 Days | Apr 21, 2020 00:00 | - May 21, | 2020 16:56 🗎 | Search | | |
| Attack IP | Region | | Time Attacked | Attacked URL | Method | Parameter | Rule Action | Rule ID | Attack Probability | Actions |
| | | | | | No c | data available. | | | | |

You can click **View Details** in the Actions column that corresponds to a record to access the **Attack Detail** pane.

For more information about how to configure data leakage prevention, see **#unique_11**.

 Account Security: displays the records of risk events that occurred at the specified endpoint during the configuration of account security. The following information is provided: Domain, Endpoint, Malicious Requests Occurred During, Blocked Requests/ Total Requests, and Alert Triggered By. You can specify a domain, endpoint, and query time period to search for corresponding data.

| Security | Security report | | | | | | | | | |
|-----------------|--|---------------------------|------------------------------------|------------------------------------|--------------------|--|--|--|--|--|
| Web Security | Bot Management Access Control/Throttling | | | | | | | | | |
| Web Intrusion P | revention Data Leal | kage Prevention Account S | ecurity Positive Security Model | | | | | | | |
| All | All Yesterday Today 7 Days 30 Days | | | | | | | | | |
| Domain | E | ndpoint | Malicious Requests Occurred During | Blocked Requests/Total Requests | Alert Triggered By | | | | | |
| | | | No data available. | | | | | | | |

For more information about how to configure account security, see **#unique_12**.

• **Positive Security Model**: displays the records of web application attacks that triggered automatically-generated positive security model rules. The following information is provided: **Attack IP**, **Region**, **Time Attacked**, **Attacked URL**, **Method**, **Rule Action**, **Rule**

ID, and **Attack Probability**. You can specify a domain and query time period to search for corresponding data.

| Web Security | Bot Management | Access Control/Throttling | J | | | | | |
|-----------------|--------------------|---------------------------|-------------------|------------------|----------------------|---------|--------------------|---------|
| Web Intrusion P | Prevention Data Le | akage Prevention Account | Security Positive | e Security Model | | | | |
| All | ~ | Yesterday Today 7 Days | 30 Days Apr 21 | , 2020 00:00 | - May 21, 2020 16:59 | | | |
| Attack IP | Region | Time Attacked | Attacked URL | Method | Rule Action | Rule ID | Attack Probability | Actions |
| | | | | No data av | vailable. | | | |

You can click **View Details** in the Actions column that corresponds to a record to access the **Attack Detail** pane.

For more information about how to configure a positive security model, see **#unique_13**.

Bot Management tab

The **Bot Management** tab displays the monitoring data of access requests of crawlers generated in websites. This tab consists of two sections: **Data Trends** and **Real-time Monitoring in Last 10 Minutes**. You can specify a domain and query time period to search for corresponding data.

| Web Securit | y Bot Mana | agement | Access | Control/T | hrottling | | | | | | | | | | |
|-----------------|----------------------|------------|--------------|-----------|-----------|-----------|-------------------|-----------|-----------------|-----------------|------------|------------|------------|-------------|------------|
| All | | \sim | Yesterday | Today | 7 Days | 30 Days | Apr 21, 2020 00:0 | DO | - May | 21, 2020 16:59 | Ē | Search | | | |
| Data Trends | ; | | | | | | | | | | | | | | |
| Overview | Interceptic | on Analysi | s | | | | | | | | | | | | |
| (times/5 min |) | | | | | | | | | | | | | | Statistics |
| 1,800 | | | | | | | | | | | | | | | |
| 1,500 | | | | | | | | | 1 | | | | | | |
| 1,200 | | | | | | | | | | | | | | | |
| 900 | | | | | | | | | | | | | | | |
| 600 | | | | | | | | | | | | | | | |
| 300 | | | | | | | | | | | | | | | |
| 0 Apr 21, 20 | 20 12-00 AM | Apr | 25 2020 10 | 55 DM | Åpr | 20 2020 0 | 50 PM M- | w 5 2020 | 2:45 DM | I May 10, 20 | 20 7-40 PM | May 15, 20 | 20.6-25 PM | J | 20.5-20.PM |
| Apr 21, 20 | 20 12:00 AM | Abis | 20, 2020 10. | .55 P W | Api | QPS | App Protection | Threa | at Intelligence | Algorithm | n Model | Way 15, 20 | 20 0.35 PW | Way 20, 20, | 20 5.50 PW |
| | | | | | | | | | | | | | | | |
| Real-time N | lonitoring i | n Last 1(| 0 Minute | s | | | | | | | | | | | |
| Domain Na me | Protection Module | Policy Na | ame Statu | 15 | 16:58 | | 16:57 16:5 | 56 | 16:55 | 16:54 | 16:53 | 16:52 | 16:51 | 16:50 | 16:49 |
| | | | | | | | No | data is a | vailable | | | | | | E |

• Data Trends: includes two tabs: Overview and Interception Analysis. The Overview tab displays the trend chart of total requests and access requests of crawlers that triggered

the protection rules under different protection modules. The **Interception Analysis** tab displays the trend chart of requests and blocked requests.

 Real-time Monitoring in Last 10 Minutes: displays the records of access requests of crawlers that triggered the protection rules under different protection modules in the last 10 minutes.

For more information about how to configure bot management, see the following topics:

- #unique_14
- #unique_15
- #unique_16

Access Control/Throttling tab

The **Access Control/Throttling** tab displays the records of web requests that triggered the protection rules under the following protection modules: **HTTP Flood Protection**, **Scan Protection**, and **Access Control**. You can specify a domain and query time period to search for corresponding data. You can also query data-related logs with one click.

HTTP Flood Protection: displays the trend of HTTP flood protection. The following information is provided: Total QPS, Alerts on Custom Rule Hit, Blocking on Custom Rule Hit, and Blocking on System Rule Hit. This tab also displays the data of No. of matches

for different rule types (valid values: Alerts on Custom Rule Hit, Blocking on Custom Rule Hit, and Blocking on System Rule Hit).

| Web Security | Bot Management | Access Control/ | Throttling | | | | | | |
|--|--|-----------------|----------------------|---|--|--|-------------------------|--|--|
| HTTP Flood Prot | HTTP Flood Protection Scan Protection Access Control | | | | | | | | |
| All | ~ | Yesterday Today | 7 Days 30 Days | Apr 21, 2020 00:00 | - May 21, 2020 | 17:00 🗰 Search | | | |
| 6 5 4 3 2 1 0 0 7 21, 2020 12:00 A | M Apr 25, 20. | 20 3:30 PM | Apr 30, 2020 7:00 Al | M May 4, 2020 10:3 n Custom Rule Hit — Blo | D PM May 9, 2020 kking on Custom Rule Hit | 2:00 PM May 14, 2020 5:30 / Blocking on System Rule Hit | AM Møy 18, 2020 9:00 PM | | |
| Rule Type | | | | | No. of matches | | | | |
| Alerts on Custom | Rule Hit | | | | 0 | | | | |
| Blocking on Custo | om Rule Hit | | | | 0 | | | | |
| Blocking on Syste | m Rule Hit | | | | 0 | | | | |

You can click the value of **No. of matches** for a rule type to access the **Log Service** page. The system automatically enters the query statements of the logs related to HTTP flood protection on this page to facilitate log query. For more information, see **#unique_17**.

| Status C This domain has Log Service enabled. You can manage domain settings on the Website Configurations page. |
|--|
| Log Query Log Analysis |
| @ waf-logstore |
| <pre>1 matched_host:" and block_action: tmd</pre> |
| |
| |
| |

For more information about how to configure HTTP flood protection, see **#unique_18**.

For more information about how to customize HTTP flood protection rules, see #unique_19.

 Scan Protection: displays the trend of scan protection. The following information is provided: Total QPS, Directory Traversal Protection, Collaborative Protection, Highfrequency Web Attack Protection, and Scan Tool-based Blocking. This tab also displays the data of No. of matches for different rule types (valid values: Directory Traversal

Protection, **Collaborative Protection**, **High-frequency Web Attack Protection**, and **Scan Tool-based Blocking**).

| Web Security | Bot Manageme | nt Access | Control/Throttling | | | | | | | |
|--|--------------------|----------------------------|-----------------------------------|-----------|----------------------|--|--|--------------------------------------|--|--|
| HTTP Flood Prot | ection Scan Pr | otection Ac | cess Control | | | | | | | |
| All | ~ | Yesterday | Today 7 Days | 30 Days | Apr 21, 2020 00:00 | - May 21, 2020 17:02 | 🗰 Search | | | |
| 6 5 4 3 2 1 0 pr 21, 2020 12:00 A | M Apr 25, | 2020 3:30 PM otal QPS [| Apr 30, 20 Directory Traversal | 0 7:00 AM | May 4, 2020 10:30 PM | May 9, 2020 2:00 Pl High-frequency Web At | M May 14, 2020 5:30 AM tack Protection — Scan Tool-ba | May 18, 2020 9:00 PM sed Blocking | | |
| Rule Type | | | | | No | o. of matches | | | | |
| Directory Traversal Protection 53 | | | | | | | | | | |
| Collaborative Pro | tection | | | | 0 | 0 | | | | |
| High-frequency V | Veb Attack Protect | tion | | | 22 | | | | | |
| Scan Tool-based | Blocking | | | | 0 | | | (E | | |

You can click the value of **No. of matches** for a rule type to access the **Log Service** page. The system automatically enters the query statements of the logs related to scan protection on this page to facilitate log query. For more information, see **#unique_17**.

| Status 🜑 This domain has Log Service enabled. You can manage domain settings on the Website Configurations page. |
|--|
| Log Query Log Analysis |
| @ waf-logstore |
| <pre>1 matched_host:" and block_action: antiscan</pre> |
| |

For more information about how to configure scan protection, see **#unique_20**.

Access Control: displays the trend of access control. The following information is provided: Total QPS, Blocking by ACL Policy, Alerts by ACL Policy, and Blocking by Blacklisting. This tab also displays the number of matches for custom rules.

| Web Security | Bot Management | Access Control/Thrott | ling | | | | | |
|--|---------------------|-----------------------|-------------------------|---|--|----------------------|----------------------|---|
| HTTP Flood Pro | tection Scan Protec | ction Access Control | | | | | | |
| All | \sim | Yesterday Today 7 Da | iys 30 Days | Apr 21, 2020 00:00 | - May 21, 2020 17:04 | 🗰 Search | | |
| 6 5 4 3 2 1 0 pr 21, 2020 12:00 / | AM Apr 25, 202 | 10 3:30 PM Apr 30 | 2020 7:00 AN tal QPS | May 4, 2020 10:30 Ph Blocking by ACL Policy — Al | 1 May 9, 2020 2:00 P arts by ACL Policy — Block | May 14, 2020 5:30 AM | May 18, 2020 9:00 PM | I |
| Rule ID | | Domain Na | me | D | escription | No. of ma | atches | |
| 1417218 | | | | - | | 57 | | |
| 1417231 | | | | - | | 15 | | |
| 1858257 | | | n | c | : | 9 | | |
| 1883577 | | , | | w | ww | 28 | | |

You can click the ID of a custom rule to view and modify the configurations of this rule in the **Edit Rule** dialog box that appears. For more information, see Create a custom protection policy.

You can click the value of **No. of matches** for a custom rule to access the **Log Service** page. The system automatically enters the query statements of the logs related to access control on this page to facilitate log query. For more information, see **#unique_17**.

| · · · · · | Status 🜑 This domain has Log Service enabled. You can manage domain settings on the Website Configurations page. |
|------------------------|--|
| Log Query Log Analysis | |
| ∅ waf-logstore | |
| 1 matched_host:" | and block_action: acl |
| | |

For more information about how to configure access control, see **#unique_19**.

For more information about how to configure an IP address blacklist, see **#unique_21**.

3 Data visualization

Based on the detailed website logs collected by WAF, WAF provides the data visualization service. By converting the data into a visual big screen, you can monitor and understand the real-time attack and defense situations of your website. This provides you with visual and transparent data analysis and decision-making capabilities to keep your website security.

Features

Currently, the WAF data visualization service provides the following two visual screens for your choice:

More WAF data visualization screens are coming.



Note:

Because of the particularity of visual screens, only Google Chrome browser 56 and a later version is supported.

WAF Real-time Attack and Defense Situation Screen

WAF real-time attack and defense situation screen is updated every second. It displays current day's website visit and overall interception situations for all your websites that protected by WAF. This screen focus on displaying the stability of the website service and the quality of the network service.



Note:

The data range on this screen is from 0:00 to the current time of today.

| Display item | Description | |
|-----------------------|---|--|
| Inbound Bandwidth | Inbound bandwidth traffic (Unit: bps). | |
| Outbound Bandwidth | Outbound bandwidth traffic (Unit: bps). | |
| QPS | Current website traffic (Unit: QPS). | |
| Interception Ratio | The percentage of the website requests that are intercepted by WAF. | |
| Today's Interceptions | The number of the website requests that are intercepted by WAF. | |

| Display item | Description | |
|-----------------------------------|---|--|
| Mobile OS Distribution | OS distribution for the visit requests from mobile clients. | |
| PC Browser Distribution | Browser distribution for the visit requests from PC clients. | |
| Top 10 Source IPs | The top 10 source IPs that have most visits and their visit volumes. | |
| Top 5 Visited URLs | The top 5 URLs that is visited and their visit volumes. | |
| Exception Monitoring | The exception HTTP response status code returned and their occurrences. | |
| Visit Statistics (Mainland China) | The visit statistics heat map shows the source distribution of the visit requests in the last hour. | |
| Request | Shows the visit request trending (Unit: QPS). Additionally, this chart shows the trend in the number of requests intercepted by WAF, including precise access control interception, anti-fraud interception, web attack interception and HTTP flood attack interception. | |
| Bandwidth | Shows the inbound and outbound bandwidth trending (Unit: bps). | |

The white points on the earth in the middle of the screen show the global WAF server room.



WAF Security Data Platform Screen

WAF security data platform screen displays security information about web attacks, HTTP flood attack, and precise access control interceptions.



By clicking the Domains to be Monitored area at the lower-left corner of the screen, you can choose the domains that you want to monitor. You can also choose to monitor all the domains.

| Display item | Description | |
|--------------------------|--|--|
| Total Visits | The number of total visits of the selected domains on the day. | |
| Web Attacks | The number of web attacks intercepted by WAF for the selected domains on the day. | |
| HTTP Flood Attacks | The number of HTTP flood attacks intercepted by WAF for the selected domains on the day. | |
| Precise Access Control | The number of requests intercepted by the WAF precise access control rules for the selected domains on the day. | |
| Top Web Attack Source IP | Top attack source IPs, the region of the IPs, and their attack volumes. Additionally, hover the mouse over the top attack source IP to view the web attack type distribution and the tags of the source IP. | |
| Regional heat map | The regional heat map on the upper-right corner shows the distribution of the regions that the attack source belongs to. | |



The radar chart in the middle of the WAF security data platform screen shows the visits, web attack interception, HTTP flood attack interception, and precise access control interceptions every 15 minutes as an interval. Additionally, you can select a time period in the radar chart, and click the floating window, to view detailed security data information for that time period.



Note:

Click the date at the bottom of the large screen to select to display the security data for the specified date.

| Display item | Description | |
|--------------------------|--|--|
| Visits | Website visits (Unit: QPS). | |
| Web Attacks | The number of web attacks intercepted by WAF. | |
| HTTP Flood Attacks | The number of HTTP flood attacks intercepted by WAF . | |
| Precise Access Control | The number of requests intercepted by precise access control rules in WAF. | |
| Top Web Attack Source IP | Top attack source IPs, the region of the IPs, and their attack volumes. Additionally, hover the mouse over the top attack source IP to view the web attack type distribution and the tags of the source IP. | |
| Web Attack Types | The distribution of web attack types intercepted. | |
| Top Attack Regions | The top 5 attack source regions. | |
| Top Hit Rules | The top 5 WAF protection rules that were hit. | |



Enable the Data Visualization service

To enable the Data Visualization service, follow these steps:

- 1. Log on to the Alibaba Cloud Security WAF management console.
- 2. Go to Reports > Data Visualization, select the region of your WAF instance, and click
 Purchase Now。



If the region of your WAF instance is International, you must upgrade it to the Business or Enterprise version.



3. On the WAF instance upgrade page, select **Single Screen** or **Multiple Screens**.

| Options | Description | Pricing |
|-----------------|---|---------------|
| Single Screen | Only one data visualization screen is supported. | USD 300/month |
| Multiple Screen | All WAF data visualization screens are supported. | USD 600/month |

Note:

The Data Visualization service inherits the expiration time of your current WAF instance. According to the service option you selected and the expiration time of the current WAF instance, the system automatically calculates the payment for you. After you enable the Data Visualization service, you have to renew the Data Visualization service when you renew your WAF instance.

- 4. Click to select the Web Application Firewall Service of Terms, and click Pay.
- **5.** On the **Data Visualization**page, click one data visualization screen to enjoy the WAF Data Visualization service.

Note:

If you purchased the Single Screen service, select one data visualization screen, and click **Enable Now**.