WAF Document

2021-02-24

Contents

Product Description

Introduction

The Web Application Firewall ("WAF") is a Web security protection product provided by Baidu AI Cloud to the users, and can effectively protect against different Web attacks, and assist the users in customizing access rules, and improving the security of business such as the website. The originally-created brand-new WAF technology architecture system can flexibly deploy the WAF instances in each Web business ingress to avoid the embarrassment that hackers bypass the age embarrassment nt to directly attack the source station under the traditional cloud WAF architecture. The integration of big data capabilities in cloud security also enables WAF to better help the customers improve the website security and availability more effectively and quickly.

Core Concepts

WAF

The web application firewall is called as "WAF" for short.

Web attack

Attacks against web applications, including but not limited to the following types of attacks: SQL injection, XSS cross-site, Webshell upload, command injection, illegal HTTP protocol request, unauthorized file access, etc.

Features

It can comprehensively protect the common Web attack threats

IR provides a variety of Web service attack protection functions such as SQL injection, XSS cross-site, Webshell upload, and unauthorized access.

Fast update of high-risk 0day vulnerability

The WAF security operation expert of Baidu AI Cloud acquires different 0day loophole information in the first time, and timely updates the web application firewall rule base, and reduces the impact caused by the 0day loophole attacks.

It supports the bypass observation pattern

The bypass observation mode is set to only record and not block the attacks. The customers can conveniently evaluate the working condition of different rules such as the general definition in the actual business.

Accurate access control

The users can combine and match a variety of HTTP fields to form the custom rules of their own business. The simple logical grammar is supported.

Advantages

Unique innovative cloud architecture

You can easily deploy the WAF instances in your cloud IT network architecture, which can fully avoid the problem of exposure of traditional cloud WAF source station.

Rule strategy is accurate and effective

The WAF policy has gone through the field test by Baidu in multiple businesses, and the rule policy is accurate and effective, with a good protection effect.

Easy to use

It needs no complex domain switch setting for DNS, and its operation is easier.

Events traceable

It can completely record different elements of the attacks, which makes it convenient for customers to analyze and understand the attack status.

Application Scenarios

The WAF (Web Application Firewall) is applied to the Web application security protection of different kinds of websites such as finance, e-commerce, o2o, internet+, game, government, and insurance. The main problems solved include but are not limited to:

- Prevent data leakage, avoid the core of the website from being stolen due to the injection, intrusion and attacks.
- 0day attack protection, providing the rule policies of quick repair in view of the latest vulnerabilities of the system software.

Pricing

Pricing

You can currently purchase the Web application firewall of Baidu AI Cloud by the annual/monthly payment mode.

- Billing items: Charging by the package specification
- Payment Method: prepaid
- Deduction period: Sold monthly/annually from the purchase date of the user.
- Expiration Description: When the protection service purchased by you expires, the configuration of the Web application firewall is retained for 7 days. The protection continues when the user renews the protection within 7 days. After 7 days, the configuration of the Web application firewall is released and the service is unavailable.
- Ensure the account is free from arrears before procurement.

Package price

The package version of WAF is currently sold, including the following parameters:

Product configuration	WAF package
Product price	800 (Yuan/Month)
Business protection of HTTP	Support
Business protection of HTTPS	Support
Number of supported BLB protocol port monitors	1
Number of protected root domains	1
Number of protected subdomains	10, scalable
Number of custom rules	20, scalable
0day fast protection	Support
Number of back-to-origin IPs	2,000

Extended configuration

The WAF instance package supports a maximum of 10 subdomains and 20 custom rules by default. To scale up your configurations, please additionally purchase the following configurations:

Extended configuration	Price
Number of protected subdomains (every 10)	100 (Yuan/Month)
Custom rules (every 20)	100 (Yuan/Month)

Operation Guide

BLB-WAF Overview

BLB is responsible for parsing and forwarding HTTP and HTTPS protocol requests, and WAF is responsible for providing security protection functions. The created WAF instances needs to be bound to the HTTP/HTTPS business on the BLB instances in the same region, so the WAF can provide Web protection for the HTTP/HTTPS business.

> **Note**
>
> When configuring BLB WAF, the user must ensure that the purchased BLB and WAF are in the same region.

Create BLB WAF Instances

1. Log into Baidu AI Cloud Console.
2. After logging in, select "Product Service > Web Application Firewall" to enter the page of BLB WAF list.
3. Click [Purchase WAF Instance] key and select the configuration information:

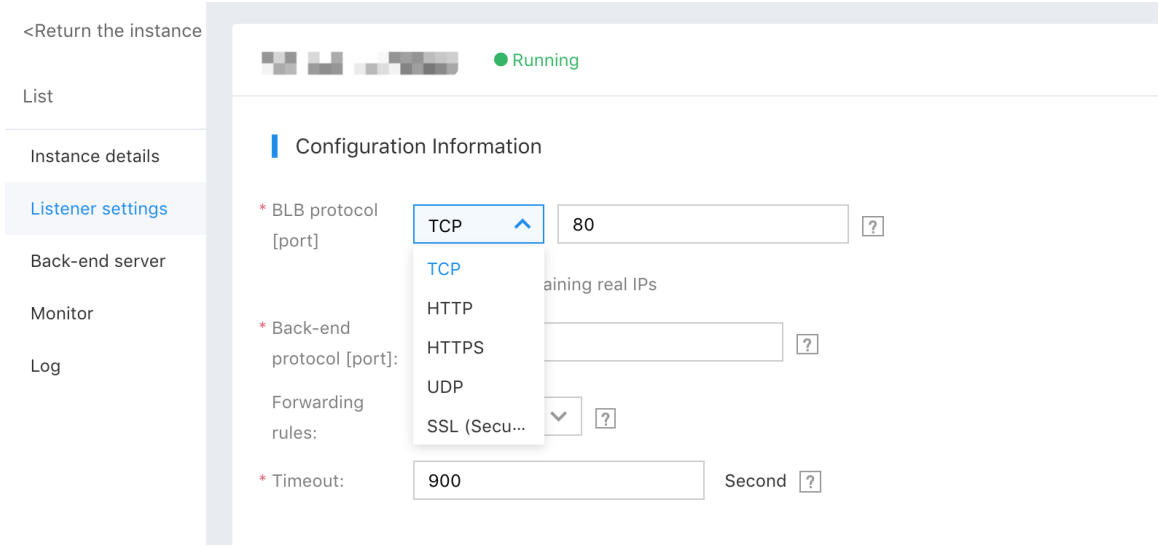
Parameter	Description
Region	Currently, the following regions are supported: North China - Beijing, South China- Guangzhou, East China - Suzhou, "Finance Central China - Shanghai and Hong Kong Zone II.
Number of supported root domains	Each WAF instance protects one root domain.
Number of supported subdomains	The package covers the protection of 10 subdomains by default; according to business requirements, you can also purchase more additional subdomains for protection.
Protocol supported	The package includes two protocol types, HTTP and HTTPS.
Web security protection	The WAF service can automatically update attack vulnerabilities, including different common Web attacks, and 0day attack rules.
Custom access rules	You can realize the control and filtration of your own business by the custom rules. Currently, the matching processing of the following contents is supported: "source IP", "URL address", "Referer" field, "User-Agent" fields of the http request, etc.. The package supports a maximum of 20 custom rules by default; if you need to customize more rules, please purchase additional rules in the console.

4. Select the purchased duration and number of WAF instances, and click [Next] . Confirm the purchase information and complete payment.
5. After payment, the WAF instance is created. You can return to the list page to view.

Configure BLB

Configure BLB Monitoring

1. Select "Product Services > Load Balance" to enter the page of "Instance List".
2. Select the BLB instance requiring configuration of a monitor, and then **Frontend protocol/port** Or **Backend protocol/port** Column, click **Configure** Enter the details page of monitor setting for configuration.
3. Fill in the configuration information.



Parameter	Description
BLB protocol [Port]	According to the protocol and port of the external service in the user's actual business, select the protocol type of http/https and fill in the port.
Backend protocol [Port]	According to the protocol and port of the external service in the user's actual business, select the protocol type of http/https and fill in the port.

4. The rest functions are available by default. Finally, click **Confirm** Complete the setting of BLB monitor.

BLB Add Backend Servers

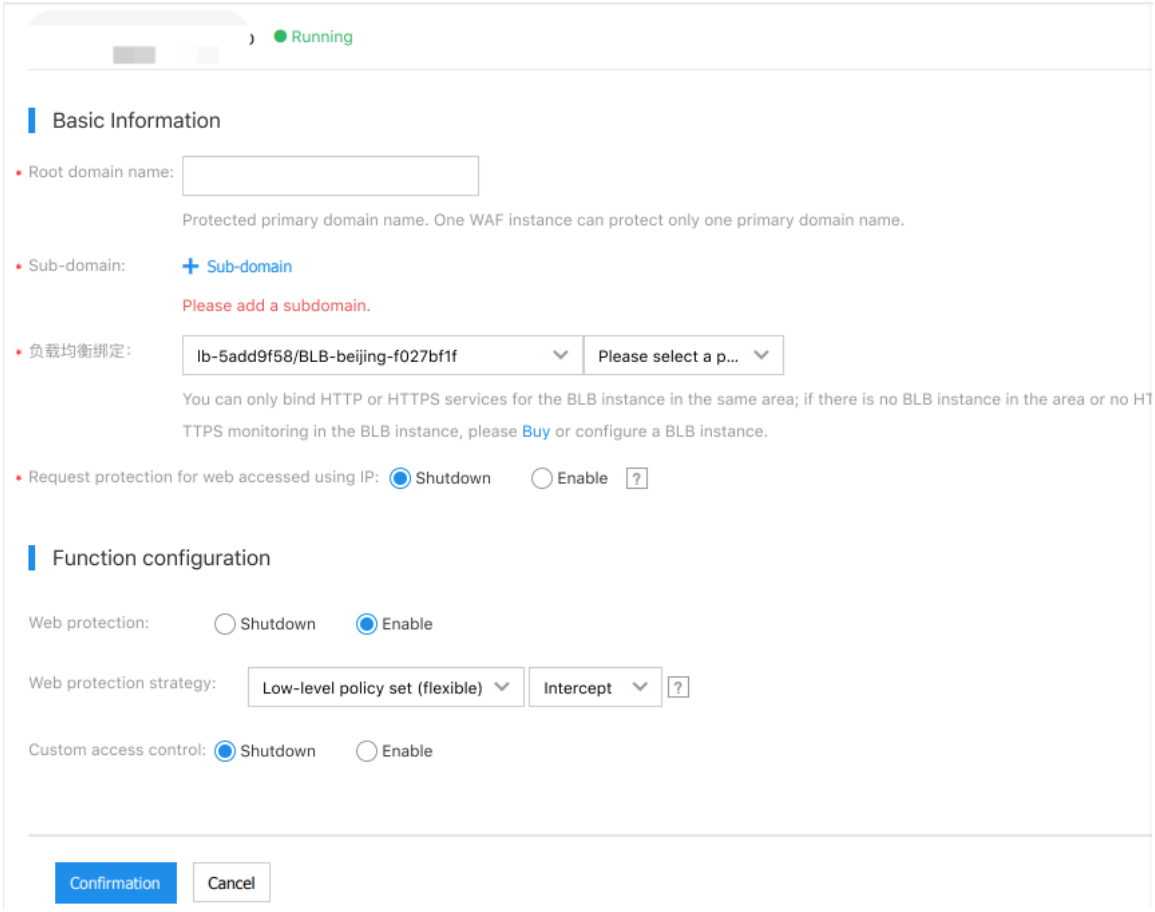
1. Select "Product Services > Load Balance" to enter the page of "Instance List".
2. Select the BLB instance requiring configuration of a monitor, and then **Backend server** Column, click **Configure** Enter the page of back-end server.
3. Click **Add backend server** In the pop-up menu bar, select the server BCC instance to be configured, and click **Next step** Then, set the server weighted value, and finally click "Confirm". Complete the addition of BLB in the back-end server.

Configure WAF

After purchase of the WAF instance, you need to configure the WAF instance to realize the WAF protection capability. The configuration steps are as follows:

1. Select "Product Services > Web Application Firewall" to enter the page of BLB WAF list. Click **Primary domain** under the column **Configure** Enter the details page of configuration.
2. To fill in the basic configuration, you need to fill in the "root domain" and "subdomain" to be protected, and select the bound load balance BLB instance.

   Only the BLB instances which are in the same region with WAF instance can be bound, and only the HTTP/HTTPS protocol is supported. In case of no BLB instances meeting conditions, please go to Console to purchase or re-configure the BLB instance.



3. Enable the Web protection, and select the protection policy level.
   - The set of intermediate policies is enabled by default. The stricter the policies are, the better the security protection effect is. The set of advanced policies means the enablement of strict protection policies, but the error interception may occur; the set of intermediate policies means a set of intermediate and low policies; and the set of low policies means loose protection policies.
   - Each kind of protection policy has the functions of [Intercept] and [Observe] . The interception pattern requests to immediately block an attack when finding it; the observation pattern request to immediately record but not intercept an attack when finding it.
4. (Optional) Enable the custom access control, click [Add] key, and realize the control and filtration of your own business by the custom rules.

Parameter	Description
Name	Name of custom access control rule
Match	Matching processing of the following contents: "source IP", "URL address", "Referer" field, "User-Agent" fields of the http request, etc.
Matched pattern	Select the matched pattern: Prefix, include or postfix.
Match string	Enter the string requiring access control.
Executed action	Blacklist or whitelist strings
Pattern	Intercept: Immediately block an attack when finding it; observe: Immediately record but not intercept an attack when finding it.

5. Click [Confirmation], and complete the BLB binding operation.

Rebind EIP

To realize the WAF protection function of BLB, you need to unbind EIP from the Baidu Cloud Compute, and then bind it to the corresponding BLB. The specific procedures are as follows:

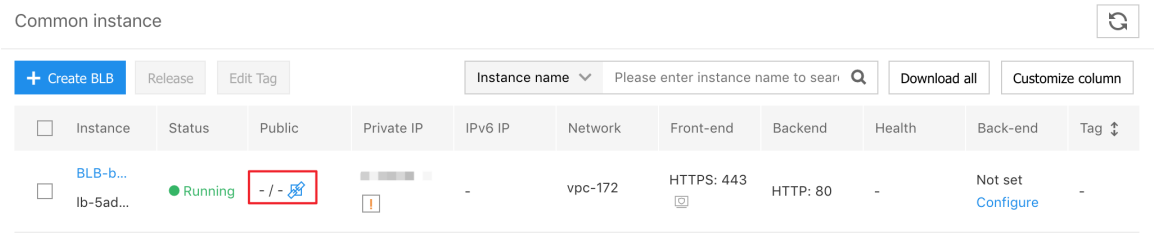
> **Note** In this step, EIP needs to be unbound, which may cause the business interruption. Please reasonably arrange the operation time to reduce the impact on the online business.

Unbind EIP from BCC

1. Select "Product Service > Baidu Cloud Compute" to enter the page of BCC instance list.
2. Click the name of instance from which the EIP is to be unbound, and enter the instance details page of the instance.
3. On **Configuration information** In the contents, click "Unbind EIP", and in the pop-up menu bar, select **Confirm** Unbind the EIP from BCC.

Bind EIP to BLB.

1. Select "Product Service > Load Balance" to enter the page of "BLB Instance List".
2. Select the BLB instance to which EIP is to be bound, and click **Public IP/Bandwidth** The corresponding network symbol in the bar, enter the page of "Bind EIP".



3. From the EIP list, select the EIP which is just unbound from BCC, and then click **Confirm** Bind the EIP to BLB.

CDN-WAF-Overview

The Web Application Firewall is responsible for providing the application security protection function for CDN to effectively defend different common Web attacks such as SQL injection, XSS cross-site script, backdoor upload, and unauthorized access. The user needs to add a domain in CDN for the created WAF instance, and in this way, WAF can provide web protection for your domains.

Create a CDN WAF Instance

1. Log into Baidu AI Cloud Console.
2. After logging in, select "Product Service > Web Application Firewall" to enter the page of WAF list.
3. Click [Purchase WAF Instance] key and select the configuration information:

Parameter	Description
Region	global
Number of supported root domains	Each WAF instance protects one root domain.
Number of supported subdomains	The package covers the protection of 10 subdomains by default; according to business requirements, you can also purchase more additional subdomains for protection.
Protocol supported	The package includes two protocol types, HTTP and HTTPS.
Web security protection	The WAF service can automatically update attack vulnerabilities, including different common Web attacks, and 0day attack rules.
Custom access rules	You can realize the control and filtration of your own business by the custom rules. Currently, the matching processing of the following contents is supported: "source IP", "URL address", "Referer" field, "User-Agent" fields of the http request, etc.. The package supports a maximum of 20 custom rules by default; if you need to customize more rules, please purchase additional rules in the console.

4. Select the purchased duration and number of WAF instances, and click [Next] . Confirm the purchase information and complete payment.

5. After payment, the WAF instance is created. You can return to the list page to view.

Associate a CDN Instance

1. Enter the page of CDN WAF list, and click [Configure] key in one operation column of WAF instances.

2. Fill in the "root domain" and "subdomain" to be protected, and select the bound domain.

   Only the main domains existing in the list of CDN domains of Baidu AI Cloud can be bound, and only the HTTP/HTTPS protocol is supported. In case of no domains meeting conditions, please go to Console to purchase or re-configure the domains.

3. Enable the Web protection, and select the protection policy level.

   - The set of intermediate policies is enabled by default. The stricter the policies are, the better the security protection effect is. The set of advanced policies means the enablement of strict protection policies, but the error interception may occur; the set of intermediate policies means a set of intermediate and low policies; and the set of low policies means loose protection policies.

   - Each kind of protection policy has the functions of [Intercept] and [Observe] . The interception pattern requests to immediately block an attack when finding it; the observation pattern request to immediately record but not intercept an attack when finding it.

4. (Optional) Enable the custom access control, click [Add] key, and realize the control and filtration of your own business by

the custom rules.

Parameter	Description
Name	Name of custom access control rule
Match	Matching processing of the following contents: "source IP", "URL address", "Referer" field, "User-Agent" fields of the http request, etc.
Matched pattern	Select the matched pattern: Prefix, include or postfix.
Match string	Enter the string requiring access control.
Executed action	Blacklist or whitelist strings
Pattern	Intercept: Immediately block an attack when finding it; observe: Immediately record but not intercept an attack when finding it.

5. Click [Confirm Validation] , and complete the BLB binding operation.

WAF bound to CDN Instance

1. In the console, select **Content delivery network CDN** Enter the product page, and in the left navigation bar, click **Domain management** Enter the page of CDN domain management list.
2. Click the domain requiring addition of WAF protection, enter the details page of domain, and click **Security configuration** in the left navigation bar. Enter the page of WAF configuration.
3. Click the button next to the WAF configuration, and enter the interface of WAF configuration modification. In the pop-up window, select **Enable** Enable the WAF protection function.

The WAF configuration is closed by default, and can be used only when the user selects "Enable".

4. In the list of WAF instance, select the WAF instance to be bound, and finally click "Save" to bind WAF to CDN instance. If you don't purchase any WAF instance, purchase the CDN WAF instance according to the prompt.

> Note:
> Explanation on the primary domain status: When the list of primary domains displays "Unconfigure", it means that the primary domain is not configured; when the list of primary domains displays bfgdu.com, it means that the primary domains are inconsistent; in the two cases, you can use the WAF function only after you complete the configuration. The number of online configured domains is 20. If the domains exceed the configured number, the temporarily unavailable domains needs to be deleted.

5. (Optional) In the pop-up window, click **Manage my WAF instance**, jump to the page of CDN WAF list. The user can manage and configure the WAF instance here.

View Data Report

In the protection process of web application firewall, the detailed attack information may be intercepted and observed. For the convenience of users to view the attack details, WAF provides the data report function. You can view the data reports by two modes, as shown below:

1. Enter the web application firewall list, click [Data Report] in the operation column, or directly click the WAF instance name, and enter the details page of data report to view the Web attack data and custom blocking events on the day.
2. Enter the operation page of CDN products of the content distribution network, and select WAF protection under the

statistical analysis.

API Reference

Overview

Welcome to use the core security product of Baidu AI Cloud - application firewall (Web Application Firewall). The WAF Open API is open to the public. The WAF API is designed according to the Open Cloud API design specifications and provides Restful API to the public.

If you first call the API of Baidu AI Cloud product, you can watch API Introduction Video Guide to quickly master the API calling method.

WAF API currently provides the following interface types:

Interface type	Interface description
WAF report query interface	The waf report interface can realize the operations including query of waf instance details, query of attack details within a period, and query of the trend of attacks within a period.
BLB-WAF interface description	The BLB-WAF interface can realize the operations including query of list of waf instances purchased by the user, query of list of all blb instances which can be bound by the user, interfaces for binding and unbinding blb, query of number of configurable sub-domains, issuance of waf configuration, and query of waf configuration.
CDN-WAF interface description	The CDN-WAF interface can realize the operations including query of the list of cdn-waf instances of the user, the number of configurable sub-domains of the user and the number of custom rules, and query of waf rule configurations and issued waf rule configuration.

Instructions for Use

Understanding the following contents helps you use API operation WAF service better.

- Signature authentication
- Idempotency
- Time and date
- Typesetting agreement

Signature Authentication

This WAF API will authenticate every access request to ensure security for users. Access Key and request signature mechanism are adopted for security authentication. Access Key consists of an Access Key ID and a Secret Access Key, both of which are strings and are officially issued to users by Baidu AI Cloud. The Access Key ID is used to identify the user, and the Access Key Secret is a key used to encrypt the signature string and the signature verification string on the server side, which shall be kept strictly confidential.

Format of the signature string

```
bce-auth-v{version}/{accessKeyId}/{timestamp}/{expireTime}/{signedHeaders}/{signature}
```

Application Steps

For getting AK/SK, please see Get AK/SK.

Signature Generation Algorithm

For specific introductions to the signature generation algorithm, please see Authentication Certification Mechanism.

Idempotency

If a request timeout or internal server error occurs when the create interface is called, the user may try to resend the request. At this time, the user can avoid creating more resources than expected through the clientToken parameter, that is, to ensure the idempotence of the request.

Idempotency is based on clientToken, an ASCII string no longer than 64 bits usually placed in a query string such as `<http://bss.bj.baidubce.com/open-api/v2/wafStatistics/waf-3a4b5c? clientToken=be31b98c-5e41-4838-9830-9be700de5a20. >`

If the user calls the creation interface with the same clientToken value, the server will return the same request result. Therefore, when the user encounters an error and retries, he can provide the same clientToken value to ensure that only one resource is created. If the user provides a used clientToken, but other request parameters (including queryString and requestBody) are different or even URL path is different, the error code of IdempotentParameterMismatch will be returned.

The clientToken is valid for 24 hours, subject to the last time when the server receives the clientToken. That is, if the client continuously sends the same clientToken, the clientToken will be valid for a long time.

Time and Date

There are various methods to express date and time. For the sake of uniformity, unless it is a convention or a corresponding specification, wherever the date and time is required, UTC time shall be used, ISO 8601 shall be followed , and the following constraints shall be met:

- Fields expressing the date all utilize the YYYY-MM-DD format, e.g.2014-06-01 which means June 1, 2014.
- Fields expressing time all utilize the hh:mm:ss format, with the capital letter Z added at the end, which means UTC time. E.g. 23:00:10Z means UTC time: 23:00:10.
- When the date and time is combined, the capital letter T is added between the two items, e.g. 2014-06-01T23:00:10Z means UTC time: 23:00:10 on June 1, 2014.

Typesetting Agreement

Layout	Meaning
< >	Variable
[ ]	Optional item
{ }	Mandatory item
|	Mutual exclusion relationship
Monospaced font Courier New	Screen output

API Service Domain Name

Service domain names of WAF API:

Region	Endpoint	Protocol
global	bss.bj.baidubce.com	HTTP and HTTPS
Beijing	bss.bj.baidubce.com	HTTP and HTTPS
Guangzhou	bss.gz.baidubce.com	HTTP and HTTPS
Suzhou	bss.su.baidubce.com	HTTP and HTTPS
Finance East China - Shanghai	bss.fsh.baidubce.com	HTTP and HTTPS
Wuhan	bss.fwh.baidubce.com	HTTP and HTTPS
Baoding	bss.bd.baidubce.com	HTTP and HTTPS
Hong Kong	Not open yet	Not open yet
Hong Kong Zone II	Not open yet	Not open yet

Note: WAF API supports two modes of call, i.e. HTTP and HTTPS. HTTPS calling is recommended to improve data security.

Calling Conventions

The data exchange format is JSON, and all request/response body contents are encoded in UTF-8. The IPs used in the URL parameters are expressed in dotted decimal.

Request Parameter

The request parameters include the 4 kinds below:

Parameter Type	Description
URI	Generally used to indicate the operation entity, e.g. PUT / v1/ schedule/{ scheduleId}.
Query parameter	Request parameters carried in URL.
HEADER	Passed by the HTTP header, e.g. x-bce-date.
RequestBody	Request data body organized in JSON format.

API Version Number

Parameter	Type	Parameter position	Description	Required or not
version	String	Url parameter	The current API version is 2.	Yes

Return Value Description

There are two types of return values:

Return Content	Description
HTTP STATUS CODE	E.g. 200,400,403,404, etc.
ResponseBody	Response data body organized in JSON format.

Common Header

Public Request Header

The Table below lists the public headers carried by all waf APIs. The standard header of the HTTP protocol is not listed here.

HEADER	Required or not	Description
Authorization	Yes	Including Access Key and request signature.
Content-Type	Yes	application/json; charset=utf-8
x-bce-date	No	A string representing the date conforms to the BCE API specification
Host	Yes	Represent the domain name of request API

Public Response Header

The Table below lists the public response headers of all Waf APIs. The standard response header of the HTTP protocol is not listed here.

HEADER	Description
Content-Type	Only support JSON format, application/json; charset=utf-8
x-bce-request-id	Waf is backend generated and automatically set to the response header

Error Return

The detailed error information is returned through Response Body in case of a request error, and the following format is followed:

Parameter name	Type	Description
code	String	Error code
message	String	Err description
requestId	String	RequestID of this request

Example:

```
 {
   "requestId" : "ae2225f7-1c2e-427a-a1ad-5413b762957d",
   "code" : "NoSuchKey",
   "message" : "The resource you requested does not exist"
}
```

The error codes are divided into public error codes of Baidu AI Cloud and peculiar error codes of WAF services. The specific error codes are as follows:

BCE Common Error Code

Error return code	Error message	status code	Description
Access Denied	Access denied.	403Forbidden	No permission to access the corresponding resource.
InappropriateJSON	The JSON you provided was well-formed and valid, but not appropriate forthis operation.	400 Bad Request	The JSON format in the request is correct, but doesn't meet the requirements semantically, For example, a required item is missing, or the value type does not match. For consideration of compatibility, all unrecognizable items should be ignored directly, and this error should not be returned.
		500	All other undefined errors should not be utilized when there are

InternalError	We encountered an internal error Please try again.	InternalServerError	All other undefined errors should not be utilized when there are specific corresponding other types of errors (including generic and service customized errors).
InvalidAccessKeyId	The Access Key ID you provided doesnot exist in our records.	403Forbidden	Access key ID does not exist.
InvalidHTTPAuthHeader	The Access Key ID you provided does notexist in our records.	400 BadRequest	Authorization header field format error.
InvalidHTTPRequest	There was an error in the body of your HTTP request.	400 Bad Request	The HTTP body format is wrong. For example, it does not conform to the specified Encoding.
InvalidURI	Could not parse the specified URI.	400 Bad Request	The URI format is incorrect, such as mismatch of some service-defined keywords. For ID mismatch, more specific error codes should be defined, such as NoSuchKey.
MalformedJSON	The JSON you provided was not well-formed.	400 BadRequest	Illegal JSON format.
InvalidVersion	The API version specified was invalid.	404 NotFound	The version number of the URI is illegal.
OptInRequired	A subscription for the service is required.	403Forbidden	No corresponding service has been enabled.
PreconditionFailed	The specified If-Match header doesn ' tmatch the ETag header.	412PreconditionFailed	See Etag for details.
RequestExpired	Request has expired. Timestamp date is <Data>.	400 BadRequest	The request has timed out. Change to x-bce-date. If only Date exists in the request, you need to convert Date to datetime.
IdempotentParameterMismatch	The request uses the same client token asa previous, but non-identical request.	403Forbidden	The API parameters corresponding to clientToken are non-identical.
SignatureDoesNotMatch	The request signature we calculated does not match the signature you provided. Check yourSecret Access Key and signing method. Consultthe service documentation for details.	400 Bad Request	The signature attached in the authorization header field is inconsistent with the server-side verification.

Waf Business Error Code

Error code	Err description	HTTP status code	Semantics
ReadWafDenied	No read waf permission	403	No waf read service permission
OperateWafDenied	No operate waf permission	403	No waf operation permission
WafAdminDenied	No waf admin permission	403	No waf administration permission
UnsupportedWAFOperation	The status of specified waf does not support this operation	400	The status of waf instance doesn't support operation.
WafInterfaceError	The interface not supporte this kind of waf type	400	The called interface doesn't support the passed waf instance type.
WafBindNotFound	The specified waf bind does not exist	404	The blb identifier to be bound is not found.
WafUnBindNotFound	The specified waf unbind does not exist	404	The blb to be unbound is not found.
WafBindRepeatError	The specified waf bind is repetition	400	The blb is bound to waf and not unbound.
InvalidParameter	Invalid Parameters	400	The parameter passed in by the interface is invalid.

WAF Data Report Related Interface

WAF Query Instance Details

Interface description

Query the details of waf instance, including status of waf instance, finish time of waf, number of configured rules, statistics of attacks intercepted by web protection and custom rules in the last days.

- Note that the waf identifier needs to be specified for normal calling.

Request structure

```
 GET /v{version}/wafStatistics/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
payType	String	Payment type
wafName	String	waf name
status	String	Waf instance status: available/paused/pausing/updating/deleting/deleted.
endTime	String	Maturity time
rule	Object	Configured access rules and remaining configurable rules
webAttack	Object	Statistics of web attacks in last days
customAttack	Object	Statistics of custom rule attacks in the last days

Request example

```
 GET /v2/wafStatistics/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Return example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
    "payType": "prepay| postpay",          //Payment type
    "wafName": "WAFNAME",                  //WAF NAME
    "status": "STATUS",                     //WAF instance status: available/paused/pausing/updating/deleting/deleted.
    "endTime": "2017-03-14 16:40:43",      //Finish time: Local time
    "rule": {
        "used": COUNT,                    //Configured access rules, INT type
        "use": INIT,                     //Remaining configurable access rules, INT type
    },
    "webAttack": {
        "today": COUNT,                   //Count of web attacks today, INT type
        "lastWeek": INIT,                //Count of web attacks in last week, INT type
    },
    "customAttack":   {
        "today": COUNT,                   //Count of custom rules today, INT type
        "lastWeek": INIT,                //Count of other custom attacks in last week, INT type
    },
}
```

WAF is Used to Query the Attack Details

Interface description

Query the list of attack details within a period. The attack type needs to be specified, and must be one of whole event, web attack, custom rule blocking event. The start time and finish time needs to be specified, and indicated by time stamps.

Request structure

```
GET /v{version}/wafEvent/{waf_id}?type={type}&beginTime={time}&endTime={time}&pageNo={pageno}&pageSize={pagesize}&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
type	String	Yes	QUERY parameter	The values of all, webAttack and customAttack respectively represent whole event, web attack, and custom rule blocking event.
beginTime	TIMESTAMP	Yes	QUERY parameter	Time stamp: Select the beginning time of an event.
endTime	TIMESTAMP	Yes	QUERY parameter	Time stamp: Select the finish time of an event.
pageNo	Int	Yes	QUERY parameter	Display the page number of the attack list.
pageSize	Int	Yes	QUERY parameter	Number in each page
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
data	List<AttackEvent>	List of attacks intercepted by WAF
total	Int	Number of attacks

Request example

```
 GET /v2/wafEvent/waf-3a4b5c?
type=webAttack&beginTime=1546963200&endTime=1547625600&pageSize=10&pageNo=1&clientToken=be31b98c-
5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Return example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
    "data": [
        {
            "time": "2017-03-14 19:49:53",            //Event, local time
            "bcc": ["instance_id1", "instance_id2"],   //Affected assets
            "ip": "ip",                              //Attacker IP
            "addr": "USA",                            //Attack value address
            "userAgent": "baidu spider",                 //Attacker camouflage
            "url": "URL",                             //Attacker URL
            "ruleId": "zdy_id",                        //Here is the custom rule name after the user sets a custom rule.
            "ruleName": "sql-0001",                      //Defense mode
            "ruleInfo": "SQL injection",                      //Security event
            "type": "deny| log",                       //Matched pattern
            "body": "body",                           //Match contents
        },
        {...},
    ]
   "total": 1000,                                     //Total
}
```

WAF Is Used to Query the Trend of Attacks within a Period

Interface description

It is used to query the trend map of attack frequency within 24 hours. The attack type needs to be specified, and must be one of whole event, web attack, custom rule blocking event. The finish time of a period needs to be specified, and indicated by a time stamp.

Request structure

```
 GET /v{version}/wafCount/{waf_id}?time={time}&type={type}&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
time	TIMESTAMP	Yes	QUERY parameter	Time stamp: Select the finish time of an event.
type	String	Yes	QUERY parameter	The values of all, webAttack and customAttack respectively represent whole event, web attack, and custom rule blocking event.
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
total	List<PeriodAttackCount>	Array of attacks per hour within a period

Request example

```
 GET /v2/wafCount/waf-3a4b5c?
time=1546963200&type=webAttack&pageSize=10&pageNo=1&clientToken=be31b98c-5e41-4838-9830-
9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Return example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
  "total":[
     {
        "time":00,
        "total":10
     },
     {
        "time":"12",
        "total":"20"
     },
  ]
}
```

BLB-WAF Related Interface

BLB-WAF is Used to Query the List of Waf Instances Purchased by the User in One Region

Interface description

It is used to query the list of waf instances purchased by the user in one region. The pageNo needs to be specified, and pageSize is used for paging query of the list of waf instances.

Request structure

```
GET /v{version}/wafBlbRegionOverview?pageNo=1&pageSize=10&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
pageNo	Int	Yes	Query parameter	Page number of waf list
PageSize	Int	Yes	Query parameter	Number displayed in the waf list page
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
wafList	List<WafResourceInstanceModel>	List of BlbWaf instances
totalCount	Int	Number of waf instances of the user in one region

Request example

```
GET /v2/wafBlbRegionOverview?pageNo=1&pageSize=10&clientToken=be31b98c-5e41-4838-9830-9be700de5a20
HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Return example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
   "wafList": [
      {
         "region": "gz| bj| su| Hk",     //resource region:gz: Guangzhou| bj: Beijing| su: Suzhou| hk: Hong Kong
         "listener": {
            "protocol": "http| https",   //listener protocol:http| https
            "port": 80,                  //listener port, int type: 1-65535
         },
         "wafName": "NAME",          //WAF instance name
         "wafId": "WAFID",           //WAF ID
         "status": "STATUS",         //WAF instance status: available/paused/pausing/updating/deleting/deleted
         "blbName": "BLBNAME",       //Bound BLB instance name
         "blbId": "BLBID",           //Bound BLB ID
         "domain": "test.com",       //Bound primary domain
         "subDomain": {              [This field is not displayed in the page and may not be updated]
            "used": COUNT,           //Configured sub-domain, INT type
            "total": TOTAL,         //All configurable sub-domains, INT type
         },
         "webSwitch":0| 1,           //web protection switch, INT type: 0: Close, 1: Enable
         "customSwitch":0| 1,        //Custom protection switch, INT type: 0: Close, 1: Enable
      },
      {...},
   ],
   "totalCount": 10 // total number of entries
}
```

BLB-WAF is Used to Query the Page of List of All WAF Instances Purchased by the User in All Regions

Description

- The pageNo needs to be specified, and pageSize is used for paging query of the list of waf instances.

Request structure

```
 GET /v{version}/wafBlbAllOverview?pageNo=1&pageSize=10&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
pageNo	Int	Yes	Query parameter	Page number of waf list
PageSize	Int	Yes	Query parameter	Number displayed in the waf list page
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
wafList	List<WafResourceInstanceModel>	List of Blb-Waf instances of the user in all regions
totalCount	Int	Number of Blb-Waf instances of the user in all regions

Request example

```
 GET /v2/wafBlbAllOverview?pageNo=1&pageSize=10&clientToken=be31b98c-5e41-4838-9830-9be700de5a20
HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
    "wafList": [
        {
            "region": "gz| bj| su| Hk",     //resource region:gz: Guangzhou| bj: Beijing| su: Suzhou| hk: Hong Kong
            "listener": {
                "protocol": "http| https",     //listener protocol:http| https
                "port": 80,                  //listener port, int type: 1-65535
            },
            "wafName": "NAME",          //WAF instance name
            "wafId": "WAFID",          //WAF ID
            "status": "STATUS",         //WAF instance status: available/paused/pausing/updating/deleting/deleted
            "blbName": "BLBNAME",       //Bound BLB instance name
            "blbId": "BLBID",          //Bound BLB ID
            "domain": "test.com",       //Bound primary domain
            "webSwitch":0| 1,          //web protection switch, INT type: 0: Close, 1: Enable
            "customSwitch":0| 1,        //Custom protection switch, INT type: 0: Close, 1: Enable
        },
        {...},
    ],
    "totalCount": 10 // total number of entries
}
```

Query All BLB Instances of the User

Description

Query all available blb instances of the user, as well as the protocols and ports bound to blb instances.

- The waf designator needs to be specified

Request structure

```
GET /v{version}/wafBlb/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
blbList	List<BlbInstance>	List of configuration details of blb instances owned by the user

Request example

```
GET /v2/wafBlb/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
  "blbList": [
     {
        "blbId": "ID",                        //BLB ID
        "blongId": "xxxxxxxxxxx",             //BLB Long ID
        "blbName": "NAME",                     //BLB NAME
        "listenerList": [
           {
              "protocol": "http| https",   //listener protocol:http| https
              "port": 80,               //listener port, int type: 1-65535
              "rsList" [
                  "xxxxxx-xxxxxx-xxxxxx-xxxx",        //BCC bound to BLB
                     ]

           },
           {
             ...
           },
        ],
        "bccList": ["instance-1","instance-2"], //BCC bound to BLB
     },
     {...},
  ]
}
```

BLB Bound to WAF Instance

Description

- The following items need to be specified: waf identifier, blb identifier and protocols and monitoring ports bound to blb.

Request structure

```
 PUT /v{version}/wafBind/{waf_id}?clientToken={clientToken}  HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
   "blbId": "ID",                    //BLB identifier
   "listener": {
      "protocol": "http| https",      //listener protocol:http| https
      "port": 80,                    //listener port, int type: 1-65535
   }
}
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
blbId	String	Yes	Request Body parameters	Blb identifier to be bound
listener	Object	Yes	Request Body parameters	Protocol and port monitored by blb
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

No special return parameters

Request example

```
 PUT /v2/wafBind/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
    "blbId": "lb-ecfca910"
    "listener": {
        "protocol": "http",
        "port": 80,
    }
}
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
```

BLB Unbound from WAF Instance

Interface description

- The following items need to be specified: waf identifier, blb identifier and protocols and monitoring ports bound to blb.

Request structure

```
 PUT /v{version}/wafUnbind/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
    "blbId": "ID",                    //BLB ID
    "listener": {
        "protocol": "http| https",     //listener protocol:http| https
        "port": 80,                    //listener port, int type: 1-65535
    }
}
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
blbId	String	Yes	Request Body parameters	Blb identifier to be bound
listener	Object	Yes	Request Body parameters	Protocol and port monitored by blb
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

No special return parameters

Request example

```
 PUT /v2/wafUnbind/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
    "blbId": "lb-ecfca910"
    "listener": {
        "protocol": "http",
        "port": 80,
    }
}
```

Response example

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
```

Query the Number of Configurable Sub-domains and the Number of Custom Rules

Interface description

- Return the number of configurable sub-domains of the user and the number of custom rules.
- The waf designator needs to be specified

Request structure

```
GET /v{version}/wafRules/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
domainSum	Int	Number of sub-domains
ruleSum	Int	Number of rules

Request example

```
GET /v2/wafRules/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
{
    "domainSum": 20, //number of sub-domains, int type: 10| 20| 30| 40| 50
    "ruleSum": 40,         //number of rules, int type: 20| 40| 60| 80| 100
}
```

Configuration of Rules Issued by BLB-WAF

Interface description

- The waf designator needs to be specified
- Configurations requiring to pass waf and blb

Request structure

```
 PUT /v{version}/wafConfig/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
    "domain": "test.com",                 //Primary domain: without http and https heads, only supporting upper and lower
case letters, numbers, and -._.
    "subDomain": [
        "DOMAIN1", "DOMAIN2", "DOMAIN3",
    ],                                    //Subdomain, the number of subdomains should be obtained according to config sum query.
    "webSwitch": 0| 1,                    //web protection switch, INT type: 0: Close, 1: Enable
    "webModel": {
        "policy": "high| middle| low",    //Policy level: high, middle, low
        "type": "log| deny",              //Executed policy: log: observation pattern, deny: interception pattern
    },
    "customSwitch": 0| 1,                 //Custom protection switch, INT type: 0: Close, 1: Enable
    "customModel": [
        {
            "name": "NAME",               //Policy name: only supports 1-65 numbers, upper and lower case letters, -/_., and
must start with letters.
            "type": "log| deny| pass",    //Executed action: log: observation pattern, deny: interception pattern, pass: trusted
traffic
            "conditions": [               //A maximum of three items allowed
                {
                    "key": "KEY",         //Matches, only supporting the several models: uri| ip| referer| user_agent|
get_param
                    "match": ": MATCH",   //Matched pattern: prefix| include| suffix| equal| not_equal| not_include
                    "value": "xxx",       //Match contents: not supporting Chinese, supporting numbers, upper and lower
case letters, -._.
                },
            ]
        },
    ],
}
```

Request header

There are no other special headers except the public headers.

Request parameter

- For the BLB-WAF configuration, refer to wafConfig for details.

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
domain	String	Yes	Request Body parameters	Primary domain: without http and https heads, only supporting upper and lower case letters, and numbers.
subDomain	List	Yes	Request Body parameters	List of sub-domains
webSwitch	Int	Yes	Request Body parameters	web protection switch, INT type: 0: Close, 1: Enable
webModel	Object	Yes	Request Body parameters	Configuration of interception policy of waf
customSwitch	Int	Yes	Request Body parameters	Custom protection switch, INT type: 0: Close, 1: Enable
customModel	List<BlbCustomRule>	Yes	Request Body parameters	Custom rules when the custom rule protection is enabled.
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

No special return parameters

Request example

```
 PUT /v2/wafConfig/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
   "domain": "test.com",                 //Primary domain: without http and https heads, only supporting upper and lower
case letters, numbers, and -._.
   "subDomain": [
      "aa.test.com", "bb.test.com", "cc.test.com",
   ],                                    //Subdomain, the number of subdomains should be obtained according to config sum query.
   "webSwitch": 1,                       //web protection switch, INT type: 0: Close, 1: Enable
   "webModel": {
      "policy": "high",      //Policy level: high, middle, low
      "type": "deny",               //Executed policy: log: observation pattern, deny: interception pattern
   },
   "customSwitch": 1,                  //Custom protection switch, INT type: 0: Close, 1: Enable
   "customModel": [
      {
         "name": "test111",              //Policy name: only supports 1-65 numbers, upper and lower case letters, -/_., and
must start with letters.
         "type": "pass",      //Executed action: log: observation pattern, deny: interception pattern, pass: trusted traffic
         "conditions": [               //A maximum of three items allowed
            {
               "key": "ip",               //Matches, only supporting the several models: uri| ip| referer| user_agent| get_param
               "match": "equal",           //Matched pattern: prefix| include| suffix| equal| not_equal| not_include
               "value": "192.168.1.1",              //Match contents: not supporting Chinese, supporting numbers, upper
and lower case letters, -._.
            },
         ]
      },
   ],
}
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
```

BLB-WAF is Used to Query the Rule Configuration

Interface description

- The waf designator needs to be specified

Request structure

```
 GET /v{version}/wafConfig/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
waf_id	String	Yes	URL parameter	waf identifier
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

- For the BLB-WAF configuration, refer to WafConfig for details.

Parameter name	Type	Description
domain	String	Primary domain: without http and https heads, only supporting upper and lower case letters, and numbers.
subDomain	List	List of sub-domains
webSwitch	Int	web protection switch, INT type: 0: Close, 1: Enable
webModel	Object	Configuration of interception policy of waf
customSwitch	Int	Custom protection switch, INT type: 0: Close, 1: Enable
customModel	List<BlbCustomRule>	Custom rules when the custom rule protection is enabled.

Request example

```
 GET /v2/wafConfig/waf-3a4b5c? clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
{
    "domain": "test.com",                //Primary domain: without http and https heads, only supporting upper and lower case letters, numbers, and -._, with the upper limit of length of 256.
    "subDomain": [
        "aa.test.com", "bb.test.com", "cc.test.com",
    ],                                   //Subdomain, the number of subdomains should be obtained according to config sum query.
    "blbId": "BLBID",                    //Bound  BLB  instance name
    "status": "available",         //WAF instance status: available/paused/pausing/updating/deleting/deleted
    "listener": {
        "protocol": "http",        //listener protocol:http| https
        "port": 80,                    //listener port, int type: 1-65535
    },
    "webSwitch": 1,                    //web protection switch, INT type: 0: Close, 1: Enable
    "webModel": {
        "policy": "high",       //Policy level: high, middle, low
        "type": "log",                //Executed policy: log: observation pattern, deny: interception pattern
    },
    "customSwitch": 1,//Custom protection switch, INT type: 0: Close, 1: Enable
    "customModel": [
        {
            "name": "test111",              //Policy name: only supports 1-65 numbers, upper and lower case letters, -/_., and must start with letters.
            "type": "pass",       //Executed action: log: observation pattern, deny: interception pattern, pass: trusted traffic
            "conditions": [               //A maximum of three items allowed
                {
                    "key": "ip",               //Matches, only supporting the several models: uri| ip| referer| user_agent| get_param
                    "match": "equal",           //Matched pattern: prefix| include| suffix| equal| not_equal| not_include
                    "value": "192.168.1.1",              //Match contents: not supporting Chinese, supporting numbers, upper and lower case letters, -._.
                },
            ]
        },
    ],
}
```

CDN-WAF-API

Query All Cdn-waf Instances of the User

Description

- Query cdn-waf instances of the user

Request structure

```
 GET /v{version}/cdnwaf/overview?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
wafList	List<CdnWafInstance>	List of all cdn-waf instances of the user

Request example

```
  GET /v2/cdnwaf/overview?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
{
    "wafList": [
        {
            "wafName": "NAME",          //WAF instance name
            "wafId":  "WAFID",         //WAF ID
            "status": "STATUS",         //WAF instance status: available/paused/pausing/updating/deleting/deleted
            "domain": "test.com",       //Bound primary domain
            "subDomain": {
                "used": COUNT,          //Configured sub-domain, INT type
                "total": TOTAL,         //All configurable sub-domains, INT type
            },
            "subDomainList": [
                "DOMAIN1", "DOMAIN2", "DOMAIN3",
            ]:                      //List of sub-domains
            "webSwitch":0| 1,           //web protection switch, INT type: 0: Close, 1: Enable
            "customSwitch":0| 1,        //Custom protection switch, INT type: 0: Close, 1: Enable
        },
        {...},
    ]
}
```

Get All the Primary Domains of the User

Interface description

- Return to the list of all primary domains of the user

Request structure

```
GET /v{version}/cdnwaf/domainList?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
domainList	List	List of primary domains

Request example

```
GET /v2/cdnwaf/domainList?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Response example

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
{
    "domainList": [
        {
            Primary domain in "domain": "test.com",       //cdn
        },
        {...},
    ]
}
```

Query the List of Available Sub-domains

Interface description

- Sub-domains which comply with the primary domain and are not added to other waf instances, or the sub-domains bound to the waf instance

Request structure

```
 PUT /v{version}/cdnwaf/querySubDomainList/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
   Primary domain in "domain": "test.com",            //cdn
}
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
domain	String	Yes	Request Body parameters	Domain name
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
subDomainList	List	Return to the list of available sub-domains of the user. The subDomain is the subdomain name and status is the subdomain status.

Request example

```
   PUT /v2/cdnwaf/querySubDomainList/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20
HTTP/1.1
 HOST bss.{region}.baidubce.com
   Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
   {
       "domain": "test.com",
   }
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
{
    "subDomainList": [
        {
            "subDomain": "a.test.com",        //Sub-domain in cdn
            "status": 0| 1,                   //Sub-domain status, INT type: 0: No addition, 1: Added to the waf instance,
        },
        {...},
    ]
}
```

Query the Configurable Sub-domains and the Number of Custom Rules

Interface description

- The waf designator needs to be specified
- The primary domain of cdn needs to be specified.

Request structure

```
 GET /v{version}/cdnwaf/cdnWafRules/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
    Primary domain in "domain": "test.com",              //cdn
}
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
domainSum	Int	Number of subdomains
ruleSum	Int	Number of rules

Request example

```
 GET /v2/cdnwaf/cdnWafRules/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Response example

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
{
    "domainSum": DOMAINSUM,      //Number of subdomains, int type: 10| 20| 30| 40| 50
    "ruleSum": RULESUM,          //Number of rules, int type: 20| 40| 60| 80| 100
}
```

Configuration of WAF Rules Issued by CDN-WAF

Interface description

Configuration of rules for issuing WAF

Request structure

```
 PUT /v2/cdnwaf/cdnWafConfig/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
    "domain": "test.com",                //Primary domain: without http and https heads, only supporting upper and lower case letters, numbers, and -._.
    "subDomain": [
        "DOMAIN1", "DOMAIN2", "DOMAIN3",
    ],                                   //Subdomain, the number of subdomains should be obtained according to config sum query.
    "webSwitch": 0| 1,                   //web protection switch, INT type: 0: Close, 1: Enable
    "webModel": {
        "policy": "high| middle| low",       //Policy level: high, middle, low
        "type": "log| deny",                 //Executed policy: log: observation pattern, deny: interception pattern
    },
    "customSwitch": 0| 1,                //Custom protection switch, INT type: 0: Close, 1: Enable
    "customModel": [
        {
            "name": "NAME",              //Policy name: only supports 1-65 numbers, upper and lower case letters, -/_., and must start with letters.
            "pattern": "black| white",       //Executed action: black: intercept, white: pass
            "type": "log| deny",             //Policy type: Log: observation pattern, deny: interception pattern. When the pattern is white, the type can be only log observation pattern.
            "key": "KEY",                //Matches, only supporting the several models: uri, ip, referer, user_agent, get_param
            "match": ": MATCH",              //Matched pattern: prefix| include| suffix
            "value": "xxx",              //Match contents: not supporting Chinese, supporting numbers, upper and lower case letters, -._.
        },
    ],
}
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence
domain	String	Yes	Request Body parameters	Primary domain: without http and https heads, only supporting upper and lower case letters, and numbers.
subDomain	List	Yes	Request Body parameters	List of sub-domains
webSwitch	Int	Yes	Request Body parameters	web protection switch, INT type: 0: Close, 1: Enable
webModel	Object	Yes	Request Body parameters	Configuration of interception policy of waf
customSwitch	Int	Yes	Request Body parameters	Custom protection switch, INT type: 0: Close, 1: Enable
customModel	List<CdnCustomRule>	Yes	Request Body parameters	Custom rules when the custom rule protection is enabled.

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

No special return parameters

Request example

```
PUT /v2/cdnwaf/cdnWafConfig/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20
Host bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
    "domain": "test.com",                //Primary domain: without http and https heads, only supporting upper and lower case letters, numbers, and -._.
    "subDomain": [
        "DOMAIN1", "DOMAIN2", "DOMAIN3",
    ],                                   //Subdomain, the number of subdomains should be obtained according to config sum query.
    "webSwitch": 0| 1,                   //web protection switch, INT type: 0: Close, 1: Enable
    "webModel": {
        "policy": "high| middle| low",       //Policy level: high, middle, low
        "type": "log| deny",             //Executed policy: log: observation pattern, deny: interception pattern
    },
    "customSwitch": 0| 1,                //Custom protection switch, INT type: 0: Close, 1: Enable
    "customModel": [
        {
            "name": "NAME",              //Policy name: only supports 1-65 numbers, upper and lower case letters, -/_., and must start with letters.
            "pattern": "black| white",       //Executed action: black: intercept, white: pass
            "type": "log| deny",         //Policy type: Log: observation pattern, deny: interception pattern. When the pattern is white, the type can be only log observation pattern.
            "key": "KEY",                //Matches, only supporting the several models: uri, ip, referer, user_agent, get_param
            "match": ": MATCH",          //Matched pattern: prefix| include| suffix
            "value": "xxx",              //Match contents: not supporting Chinese, supporting numbers, upper and lower case letters, -._.
        },
    ],
}
```

Response example

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
```

CDN-WAF is Queried to Query WAF Rule Configuration

Interface description

Configuration of rules for querying CDN-WAF

Request structure

```
GET /v2/cdnwaf/cdnWafConfig/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

Request header

There are no other special headers except the public headers.

Request parameter

Parameter name	Type	Required or not	Parameter position	Description
version	String	Yes	URL parameter	API version number (the current value is 2)
clientToken	String	Yes	Query parameter	Idempotence, for details, please see Idempotence

Return status code

"200" for return successful and Error Code for return failed.

Return header

There are no other special headers except the public headers.

Return parameter

Parameter name	Type	Description
domain	String	Primary domain: without http and https heads, only supporting upper and lower case letters, and numbers.
subDomain	List	List of sub-domains
webSwitch	Int	web protection switch, INT type: 0: Close, 1: Enable
webModel	Object	Configuration of interception policy of waf
customSwitch	Int	Custom protection switch, INT type: 0: Close, 1: Enable
customModel	List<CdnCustomRule>	Custom rules when the custom rule protection is enabled.

Request example

```
GET /v2/cdnwaf/cdnWafConfig/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20

Host bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

Response example

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
{
    "domain": "test.com",                //Primary domain: without http and https heads, only supporting upper and lower case letters, numbers, and -._, with the upper limit of length of 256.
    "subDomain": [
        "DOMAIN1", "DOMAIN2", "DOMAIN3",
    ],                                   //Subdomain, the number of subdomains should be obtained according to config sum query.
    "status": "STATUS",          //WAF instance status: available/paused/pausing/updating/deleting/deleted
    "webSwitch": 0| 1,                   //web protection switch, INT type: 0: Close, 1: Enable
    "webModel": {
        "policy": "high| middle| low",       //Policy level: high, middle, low
        "type": "log| deny",                 //Executed policy: log: observation pattern, deny: interception pattern
    },
    "customSwitch": 0| 1,                //Custom protection switch, INT type: 0: Close, 1: Enable
    "customModel": [
        {
            "name": "NAME",                  //Policy name: only supports 16 numbers, upper and lower case letters, -/_.
            "type": "log| deny",             //Policy type: log: observation pattern, deny: interception pattern
            "pattern": "black| white",       //Executed action: black: intercept, white: pass
            "key": "KEY",                    //Matches, only supporting the several models: uri, ip, referer, user_agent, get_param
            "match": ": MATCH",              //Matched pattern: prefix| include| suffix
            "value": "xxx",                  //Match contents: not supporting Chinese, supporting numbers, upper and lower case letters, -._.
        },
    ]
}
```

Appendix

Model Object Definition

WafResourceInstanceModel

Parameter name	Type	Description
region	Region	Region where the resource is located
listener	Object	The listener object has 2 elements, and protocol and port respectively represent the protocol and port monitored by blb.
wafName	String	Waf instance name
wafId	String	waf identifier
status	InstanceStatus	Waf instance status
blbName	String	Blb instance name
blbId	String	Blb identifier
domain	String	Primary domain bound to waf
webSwitch	Int	web protection switch, INT type: 0: Close, 1: Enable
customSwitch	Int	Custom protection switch, INT type: 0: Close, 1: Enable

BlbListener

Parameter name	Type	Description
protocol	String	Only https or http types
port	Int	listener port, int type: 1-65535
rsList	List	List of bcc bound to blb

InstanceStatus

Code	Description
available	Instance available
paused	The instance expires and is suspended.
pausing	The instance expires and is being processed.
updating	The instance is being updated.
deleting	The instance is being deleted.
deleted	The instance is deleted.

Region

Code	Description
bj	Beijing
gz	Guangzhou
su	Suzhou
fsh	Shanghai
hkg	Hong Kong
hk02	Hong Kong Zone II

AttackEvent

Parameter name	Type	Description
time	String	Occurrence time of attack
bcc	List	List of affected assets
ip	String	Attacker ip
addr	String	Attacker address
userAgent	String	Attacker camouflage ua
url	String	Attack request url
ruleId	String	When the user sets a custom rule, RuleId represents the identifier of the custom rule.
ruleName	String	When the user sets a custom rule, RuleId represents the name of the custom rule.
ruleInfo	String	Contents of the custom rule set by the user
type	String	Web protection strategy, deny or log modes
body	String	Details of attack request

PeriodAttackCount

Parameter name	Type	Description
time	Int	Value characterizing a time point, value range, [00-24]
total	Int	Number of attacks at this time point

BlbInstance

Parameter name	Type	Description
blbName	String	Blb instance name
blbId	String	Blb identifier
longId	String	Long id of blb
listenerList	List<BlbListener>	List of protocols monitored by blb

BlbCustomRule

Parameter name	Type	Description
name	String	Policy name: only supports 1-65 numbers, upper and lower case letters, -/_ ., and must start with letters.
type	String	Action executed by the custom rule: log: observation pattern, deny: interception pattern, pass: trusted traffic
conditions	List<CustomCondition>	Custom rule conditions contained in the custom rule, a maximum of 3 items

CustomCondition

Parameter name	Type	Description
key	String	Matches, only supporting the several models: uri, ip, referer, user_agent, get_param
match	String	Matched pattern: prefix, include, suffix, equal, not_equal, not_include.
value	String	Match contents: not supporting Chinese, supporting numbers, upper and lower case letters-._

CdnWafInstance

Parameter name	Type	Description
wafName	String	Waf instance name
wafId	String	waf identifier
status	InstanceStatus	Waf instance status
domain	String	Primary domain bound to waf
subdomain	SubDomainCount	Statistics of sub-domains configured by waf
subDomainList	List	List of names of protected subdomains
webSwitch	Int	web protection switch, INT type: 0: Close, 1: Enable
customSwitch	Int	Custom protection switch, INT type: 0: Close, 1: Enable

CdnCustomRule

Parameter name	Type	Description
name	String	Policy name: only supports 1-65 numbers, upper and lower case letters, -/_ ., and must start with letters.
type	String	Action executed by the custom rule: log: observation pattern, deny: interception pattern, pass: trusted traffic
patten	String	Executed action: black: intercept, white: pass
key	String	Matches, only supporting the several models: uri, ip, referer, user_agent, get_param
match	String	Matched pattern: prefix, include, suffix, equal, not_equal, not_include.
value	String	Match contents: not supporting Chinese, supporting numbers, upper and lower case letters-._

Update History

2019-01-24

- API document online

FAQs

Web Attack Classification Description

Web malicious scanning

Before launching attacks, hackers always use tools to detect the vulnerabilities of different WEB application systems and different typical applications (such as SQL injection, Cookie injection, XPath injection, LDAP injection, cross-site script, code injection, form bypassing, weak password, sensitive file and directory, management background, sensitive data) so as to gather information for subsequent attacks.

Cross-site script attack

It is also known as XSS, and uses the website vulnerabilities to maliciously steal information from users. In order to gather the user information, the attackers often insert JavaScript, VBScript, ActiveX or Flash in the vulnerable programs to deceive users. Once they steal the user information, the attackers can steal user accounts, modify user settings, steal/pollute cookies, and make advertisements, etc. A great deal of malicious codes of XSS attacks appear every day.

Remote file control

Some careless developers deploy the codes on the server, and the parameter settings can call and read the server system files. The remote attackers can call these system files for operation by the malicious parameters to cause threats of varying degrees to the WEB services and user privacy.

Remote backdoor execution

Backdoor programs generally refer to those program methods which bypass the security control to acquire the program or system access right. At the development stage of software, the programmers often create a backdoor program in the software to modify the defects in the program design. However, if these backdoors are known by others, or the backdoor programs are not deleted before the software is released, the backdoors become security risks and are easily attacked by hackers as vulnerabilities.

Malicious file upload

Some forum websites often allow users to upload files. The reason causing the vulnerability is that the author doesn't check or strictly filter the data submitted by the visitors, and the visitors can directly commit the modified data to bypass the check of extension name. The submitted malicious program can be executed as a remote backdoor.

Exception file reference

The web development programmers may reference external files in the codes, and the exception file reference allows the attacker to use the "dynamic file inclusion" mechanism realized in the target application. This may enable the contents of output file to cause the code execution on the Web server. Other attacks such as site script code execution may be caused in the client JavaScript, etc.

Exception file resolution

Some web server vulnerabilities allow the modified script files to be resolved according to the common picture file extension name but still execute the contents of script files. Combined with the malicious file upload attacks, this can generally bypass the extension name limits to commit backdoor files.

System vulnerability

It refers to the susceptibility or defect of a system, and its severity is generally high. The attackers can use the vulnerabilities to directly bypass the relevant security protection mechanisms of the system.

Invalid HTTP version

The HTTP protocol has a variety of versions and is identified as (major) and (minor), such as version 0.9 , 1.0 or 1.1 . An invalid HTTP version means that the attackers use the unsupported http version number to construct a data packet request to attack the web server.

Denial-of-service attack

The denial-of-service attack means that the attackers manage to let the target machine stop providing services, and it one of the common attack means of the hackers. In fact, the consumptive attacks on the network bandwidth only occupy a small part of denial-of-service attack. As long as the attacks can cause troubles to the target, suspension of some services and even host crash, these attacks are denial-of-service attacks.

How to get the last 6 months attack intercept log

How to get the last 6 months attack intercept log

Users can browse the interception log information within 180 through the data statistics page.