

文档版本

2018-06-05

变更日志

- 2018-06-05
 - Changes
 - 查询用户名白名单记录支持返回高防IP
- 2017-12-08
 - Changes
 - 查看高防IP的带宽峰值,新增返回参数BlackHoleTimes
 - 获取IP的防护组信息, 新增返回参数Package
 - 防火墙白名单返回示例修改
- 2017-10-31
 - Changes
 - 查看高防IP的带宽信息
 - 查看高防IP的带宽峰值
 - 查看高防IP分线路的带宽信息
 - 可查询时间范围改为任意时间
- 2017-10-11
 - Changes
 - 获取高防IP预警信息
 - 重新规范IPMetricInfoData返回信息参数
- 2017-09-14
 - Changes
 - 高防IP公共返回参数
 - 新增status字段
- 2017-09-07
 - Changes
 - 从指定防护组删除IP
 - 新增从制定防护组删除IP后, 自动删除所有有关此IP在防火墙的配置, 如白名单, 端口号配置, 如果删除失败, 会提示联系运维人员线下修改
- 2017-09-06
 - Changes
 - 高防IP参数添加至防火墙部分接口

- 添加域名至防火墙白名单
 - 添加IP至防火墙白名单
 - 从防火墙白名单中删除域名
 - 从防火墙白名单中删除IP
- tips: 鉴于现在存在平台和线下都有可能操作的情况, IPUserID目前仍为可选参数, 后期会逐渐变为必选参数 (查询类的仍为可选参数)
- 2017-08-08
 - Changes
 - 高防IP接口
 - 新增传入参数: IPUserID, 传入该IP的二级用户信息
 - **「获取IP的防护组信息」**
 - 新增返回参数: 二级用户信息、开通时间、关闭时间
- 2017-07-27
 - Changes
 - 修改操作防火墙各接口返回状态码判定
- 2017-07-21
 - Changes
 - 控制防火墙的接口
 - 查询域名是否在防火墙名单
 - 查询IP是否在防火墙名单
 - 添加域名至防火墙白名单
 - 添加IP至防火墙白名单
 - 从防火墙白名单中删除域名
 - 从防火墙白名单中删除IP
- 2017-07-05
 - Changes
 - 高防IP接口
 - **「获取高防IP预警信息」**
 - 增加参数「StartTime」、「EndTime」, 预警信息支持自定义时间段获取
- 2017-06-26
 - New features
 - **「获取高防IP预警信息」**
- 2017-06-18
 - New features
 - **「新增分线路查询带宽」**
- 2017-06-12
 - Changes
 - **「查看可用的防护组列表」**

- 删除返回参数「guaranteeValue」

- 2017-06-08

- Changes

- 公共参数

- 统一日期时间格式，在涉及到请求和返回的日期时间信息时，日期和时间合并表示时，采用 **UTC** 时间，遵循 ISO 8601，在两者中间加大写字母 T，在时间之后加大写字母 Z，例如 2017-06-01T23:00:10Z 表示 UTC 时间 2017 年 6 月 1 日 23 点 0 分 10 秒

- 高防 IP 接口

- 「修改 IP 的防护组」

- 新增支持修改保底防护组或弹性防护组，可单独修改其中一项或同时修改两项，对应的生效时间参数是必须的；在生效时间之前如果有多次提交，则以最后一次提交为准
- 参数拼写调整
 - guaranteeProtectGroupId -> GuaranteeProtectGroupId
 - elasticProtectGroupId -> ElasticProtectGroupId
- 增加参数
 - GuaranteeEnableTime

- 2017-06-08

新增文档

API 概述

靠谱云向用户开放所有资源操作相关的 API，我们的 API 是通过 HTTP GET/POST 方式来进行调用的。在调用我们的 API 之前，您需要先联系我们获取 API 密钥 ID (AccessKeyId) 和 API 密钥的私钥 (AccessKeySecret)。API 密钥 ID 将作为参数包含在每一个请求中发送；而 API 密钥的私钥负责生成请求串的签名，API 密钥的私钥需要被妥善保管，请勿外传。

1、服务地址

靠谱云 API 服务接入地址：<http://antiddos.api.kaopuyun.com>。

2、通信协议

支持通过 HTTP 通道进行请求通信。

3、请求方法

同时支持 POST 和 GET 请求，需要注意不能混合使用，即如果使用 GET 方式，则参数均从 Querystring 取得，如果使用 POST 方式，则参数均从 Request Body 中取得，Querystring 中的参数将忽略。两种方式参数格式规则相同，一般使用 GET，当参数字符串过长时使用 POST。

4、字符编码

UTF-8

5、API请求结构

内容	说明
API入口	API调用的webservice入口，详见接口的请求地址说明
公共参数	每个API调用都需要包含公共参数
指令名称	API指令的名称(Action)，例如DescribeIPMonitorData、DescribeProtectGroup等
指令参数	指令参数请参见每个指令的相关文档

公共参数

1、公共请求参数

公共请求参数是指每个接口都需要使用到的请求参数。

参数名	必选	类型	说明
Version	是	string	API版本号，当前版本为:2
AccessKeyId	是	string	靠谱云颁发给用户的访问服务所用的密钥 ID
Signature	是	string	签名结果串，请参见签名机制
Timestamp	是	string	请求的时间戳，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如 2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
SignatureNonce	是	string	唯一随机数，用于防止网络重放攻击。用户在不同请求间要使用不同的随机数值
Action	是	string	每个API都有自己的Action，用来标识所请求指令

示例

```
?Version=2
&AccessKeyId=kpy-test
&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1dgI%3D
&Timestamp=2015-08-06T12:00:00Z
&SignatureNonce=15215528852396
&Action=CdnRefresh
...
```

2、公共返回参数

返回内容为JSON格式。

参数名	说明
Code	请求结果代码，200代表请求成功。
Message	请求结果的说明信息。
RequestId	唯一识别码，用于跟踪和排查问题。
Status	请求结果信息，Success代表请求成功。
服务端获取到时间，北京时间，格式为：YYYY-MM-DD hh:mm:ss	服务端获取到时间，北京时间，格式为：YYYY-MM-DD hh:mm:ss

签名机制

这里介绍API请求中签名 (Signature) 的生成方法。签名需要你先联系我们获取到 AccessKeyId和 AccessKeySecret，这里我们假设

```
AccessKeyId= "afegxgu0VdR5fT7K"  
AccessKeySecret= "b2cd9c1319ea16ec3c5e1f3fee1432b3"
```

例如我们的请求参数如下:

```
AccessKeyId=afegxgu0VdR5fT7K  
Version=2  
Dirs=["http://www.kaopuyun.com/buy/"]  
SignatureNonce=asd  
UrIs=["http://www.kaopuyun.com","http://www.kaopuyun.com/buy/cloud_server"]  
Action=CdnRefresh  
Timestamp=2015-08-25T11:11:11Z
```

签名步骤

1. 按参数名进行升序排列

排序后的参数为:

```
AccessKeyId=afegxgu0VdR5fT7K
Action=CdnRefresh
Dirs=["http://www.kaopuyun.com/buy/"]
SignatureNonce=asd
Timestamp=2015-08-25T11:11:11Z
UrIs=["http://www.kaopuyun.com", "http://www.kaopuyun.com/buy/cloud_server"]
Version:1
```

2. 对参数名称和参数值进行URL编码

注意：空格编码为%20，'/'编码为%2F， '~'不编码 编码后的请求串为：

```
AccessKeyId=afegxgu0VdR5fT7K
Action=CdnRefresh
Dirs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2F%22%5D
SignatureNonce=asd
Timestamp=2015-08-25T11%3A11%3A11Z
UrIs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%22%2C%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2Fcloud_ser
ver%22%5D
Version=2
```

3. 构造URL请求串

参数名和参数值之间用“=”号连接，参数和参数之间用“&”号连接，注意不包括Signature参数，构造后的URL请求为：

```
AccessKeyId=afegxgu0VdR5fT7K&Action=CdnRefresh&Dirs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2F%22%5D&SignatureNonce=asd&Timestamp=2015-08-25T11%3A11%3A11Z&UrIs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%22%2C%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2Fcloud_server%22%5D&Version=1
```

4. 构造被签名串

被签名串的构造规则为：被签名串 = HTTP请求方式 + '&' + uri + '&' + URL请求串。示例使用的cdn刷新接口，uri是/cdn，请求方式采用GET。

```
GET&/cdn&AccessKeyId=afegxgu0VdR5fT7K&Action=CdnRefresh&Dirs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2F%22%5D&SignatureNonce=asd&Timestamp=2015-08-25T11%3A11%3A11Z&UrIs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%22%2C%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2Fcloud_server%22%5D&Version=1
```

5. 计算签名

计算被签名串的签名 Signature。•将API密钥的私钥 (AccessKeySecret) 作为key，生成被签名串的 HMAC-SHA1 签名 •将签名进行 Base64 编码，获得最终的签名串：darDvDsR9igfiZ2f6q/9sWzIY0k= •将签名用于参数 Signature的值。

6. 添加签名

将签名参数附在原有请求串的最后面，进行URL编码后得到最终的请求串

```
AccessKeyId=afegxgu0VdR5fT7K&Action=CdnRefresh&Dirs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2F%22%5D&SignatureNonce=asd&Timestamp=2015-08-25T11%3A11%3A11Z&UrIs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%22%2C%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2Fcloud_server%22%5D&Version=1&Signature=darDvDsR9igfiZ2f6q%2F9sWzIY0k%3D
```

完整的请求URL为(为了查看方便，我们人为地将参数之间用回车分隔开)

```
https://api.kaopuyun.com/cdn?AccessKeyId=afegxgu0VdR5fT7K
&Action=CdnRefresh
&Dirs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2F%22%5D
&SignatureNonce=asd
&Timestamp=2015-08-25T11%3A11%3A11Z
&UrIs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%22%2C%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2Fcloud_server%22%5D
&Version=2
&Signature=darDvDsR9igfiZ2f6q%2F9sWzIY0k%3D
```

实际URL为

```
https://api.kaopuyun.com/cdn?
AccessKeyId=afegxgu0VdR5fT7K&Action=CdnRefresh&Dirs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2F%22%5D&SignatureNonce=asd&Timestamp=2015-08-25T11%3A11%3A11Z&UrIs=%5B%22http%3A%2F%2Fwww.kaopuyun.com%22%2C%22http%3A%2F%2Fwww.kaopuyun.com%2Fbuy%2Fcloud_server%22%5D&Version=2&Signature=darDvDsR9igfiZ2f6q%2F9sWzIY0k%3D
```

错误码表

每次请求服务器会返回代码 (Code) 和信息(Message)等内容，当返回代码不为"Success"时，表示请求未正常执行，返回码也称为错误码，错误码如下表。

错误分为 **服务端错误** 和 **客户端错误** 两种，如果是服务器端错误，说明该错误是由服务器端引起的，这个情况下请及时与我们联系；如果是客户端错误，说明该错误是由用户提交的API引起的。

服务端错误

错误码	错误信息	描述	操作建议	Http 状态 码
InternalServerError	Internal error, please contact us	服务器执行请求过程中遇到未知错误 时，会返回该错误信息	请及时与 我们联系	5xx

客户端错误

错误码	错误信息	描述
9304	DuplicateRequest	修改前后数据没有变化
9400	APIVersionError	API版本参数错误
9400	ParamAbsence	该参数是必须提交的
9400	ParamError	您提交的参数错误
9400	ParamNotPair	参数必须配对使用
9400	NoThisAction	不存在该操作
9400	TimeError	提交时间参数错误
9401	PermissionDenied	您没有权限操作这个IP
9402	ProtectGroupNotExist	防护组id参数不存在
9402	RegionNotExist	指定地域不存在
9402	IPFormatError	IP数据错误
9402	ZoneNotExist	指定区域不存在
9402	BandwidthTypeNotExist	指定带宽类型不存在
9403	IPNotExist	IP不存在
9403	IPError	此IP已被他人配置
9403	DomainError	此域名已被他人配置
9403	IPConflict	指定的IP地址冲突
9403	NotInCorrectStatus	未处于正确的状态
9403	IPNotUsed	IP未在使用中
9405	ParamError	您提交的参数错误
9407	SLBConfCheckFaile	代理配置信息验证失败
9407	SLBConfNotExist	代理配置信息不存在
9407	SLBConfTcpNoSingle	代理配置TCP协议只能拥有一个源站信息
9407	SLBConfDuplicate	代理配置重复
9408	IPAddFail	IP添加防护组失败
9408	ChangeFail	修改失败
9408	QueryFail	查询失败
9408	FirewallConnFail	防火墙连接失败

错误码	错误信息	描述
9408	TimeIntervalTooLong	时间间隔太长,不得超过
9502	RemoteSerConnFaile	远程服务器连接失败
9504	RemoteSerConnTimeout	远程服务器连接超时
9504	RemoteSerAuthFaile	远程服务器认证失败
9504	RemoteSerIOErr	远程服务器IO错误

API列表

序号	名称	描述	备注
1	DescribeProtectGroup	查看可用的防护组列表	
2	AddProtectGroupIP	添加IP到指定的防护组	
3	DescribeIPInfo	获取高防IP的防护组信息	
4	DescribeIPStatus	查看高防IP的防护状态信息	
5	ModifyIPProtectGroup	修改IP的防护组信息	
6	CloseIPElasticAntiDDos	关闭IP的弹性流量服务	
7	OpenIPElasticAntiDDos	开启IP的弹性流量服务	
8	CloseIPAntiDDos	关闭IP的高防服务	
9	OpenIPAntiDDos	开启高防IP的防护	
10	DeleteProtectGroupIP	将指定IP从防护组中删除	
11	DescribeIPMonitorData	查看高防IP的带宽信息	
12	DescribeIPMaxMonitorData	查看高防IP的带宽峰值信息	
13	DescribeIPLineMonitorData	查看高防IP分线路的带宽信息	
14	GetIPMetricInfo	获取高防IP预警信息	
15	DescribeIPFirewallList	查询IP在防火墙名单	
16	AddIPWhiteList	添加IP至防火墙白名单	
17	DeleteIPWhiteList	从防火墙白名单中删除IP	

API接口

高防IP接口

1.查看可用的防护组列表

描述

地址：/ip

查看可用与设置的防护组信息。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeProtectGroup
Region	String	否	地域
Zone	String	否	可用区
BandwidthType	String	否	线路类型： AntiBGP---高防BGP AntiCTC---高防电信 SuperAntiBGP---超防BGP SuperAntiCTC---超防电信

返回参数

参数名	类型	说明
ProtectGroupInfo	ProtectGroupDataSetType	防护组信息ProtectGroupDataSetType的集合

类型说明

ProtectGroupDataSetType节点说明

参数名	类型	说明
BandwithType	String	带宽类型
Region	String	地域
Zone	String	可用区
ProtectGroupID	string	防护组ID，唯一
ProtectGroupName	String	防护组名称
BlackHoleValue	int	黑洞阈值，单位G

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "ProtectGroupInfo":
  [

    {
      "BandwithType": "超防电信",
      "BlackHoleValue": "200",
      "ProtectGroupID": "superantictc_200g",
      "ProtectGroupName": "超防电信_200G",
      "Regio": "靠谱云福州4区",
      "Zone": "cn-fuzhou-4-a"
    },

    .....
    .....

    {
      "BandwithType": "超防电信",
      "BlackHoleValue": "400",
      "ProtectGroupID": "superantictc_400g",
      "ProtectGroupName": "超防电信_400G",
      "Regio": "靠谱云福州4区",
      "Zone": "cn-fuzhou-4-a"
    }
  ],
  "RequestId": "5c7f5707-a4bc-469e-b4c2-f05cb38b925c",
  "Status": "Success",
  "Timestamp": "2017-06-12 13:44:11"
}
```

2.添加IP到指定的防护组

描述

地址：/ip

添加指定IP到指定防护组，一个IP只能加入一个防护组。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：AddProtectGroupIP
IP	String	是	IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
guaranteeProtectGroupID	String	是	保底防护组ID，从DescribeProtectGroup接口获取
elasticProtectGroupID	String	是	弹性防护组ID，从DescribeProtectGroup接口获取
Region	String	是	地域
Zone	String	是	可用区
BandwidthType	String	是	线路类型： AntiBGP---高防BGP AntiTele---高防电信 SuperAntiBGP---超防BGP SuperAntiTele---超防电信

返回参数

无

类型说明

无

错误码

错误代码	描述	Http状态码	语义
IPError	You don't have permission to view this IP's data	9403	没有权限查看该IP的信息
IpConflict	IpConflict	9403	IP地址冲突，已在其他防护组
ProtectGroupNotExist	ProtectGroup is not exist	9402	指定的防护组不存在
RegionNotExist	Region Type is not exist	9402	指定的地域不存在
ZoneNotExist	Zone Type is not exist	9402	指定的可用区不存在
BandwithTypeNotExist	Bandwith Type is not exist	9402	指定的带宽类型不存在

返回示例

无

3.获取IP的防护组信息

描述

地址：/ip

获取高防IP的防护组信息。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeIPInfo
IP	String	否	IP地址，支持批量IP，多个IP用逗号（半角）分隔；若参数为空，默认返回所有IP的数据
IPUserID	String	否	IP地址隶属的二级用户ID

返回参数

参数名	类型	说明
ProtectGroupInfo	ProtectGroupDataSetType	防护组信息ProtectGroupDataSetType的集合

类型说明

ProtectGroupDataSetType节点说明

参数名	类型	说明
ip	String	IP地址
IPUserID	String	二级用户ID
Region	String	地域
Zone	String	可用区
BandwithType	String	线路类型: AntiBGP---高防BGP AntiTele---高防电信 SuperAntiBGP---超防BGP SuperAntiTele---超防电信
OpenTimeStamp	String	开通时间，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
CloseTimeStamp	String	关闭时间，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
ProtectGroupType	ProtectGroupTypeSetData	节点类型和数据： 保底带宽 GAURATEE 弹性带宽 ELASTIC
Package	String	IP所属包ID，若不属于包，则为空
Status	String	IP当前使用状态： Open—在用 Close---关闭

ProtectGroupTypeSetData节点说明

参数名	类型	说明
BlackHoleValue	String	黑洞阈值，单位G
ProtectGroupID	String	防护组ID，唯一
ProtectGroupName	String	防护组名称

错误码

无

返回示例

```
{
  "Code":200,
  "Message":"Success",
  "ProtectGroupInfo":
  [
    {
      "BandwithType":"高防BGP",
      "CloseTimeStamp":"2017-12-05T08:03:15Z",
      "ELASTIC":
      {
        "BlackHoleValue":100,
        "ProtectGroupID":"antibgp_100g",
        "ProtectGroupName":"高防BGP_100G"
      },
      "GAURATEE":
      {
        "BlackHoleValue":100,
        "ProtectGroupID":"antibgp_100g",
        "ProtectGroupName":"高防BGP_100G"
      },
      "IPUserID":"mosco",
      "OpenTimeStamp":"2017-12-05T07:22:45Z",
      "Package":"c115eb34-d98c-11e7-88de-50e54919757f",
      "Region":"",
      "Status":"close",
      "Zone":"",
      "ip":"10.2.2.3"
    },
    {
      "BandwithType":"高防BGP",
      "CloseTimeStamp":"",
      "ELASTIC":
      {
        "BlackHoleValue":100,
        "ProtectGroupID":"antibgp_100g",
        "ProtectGroupName":"高防BGP_100G"
      },
      "GAURATEE":
      {
        "BlackHoleValue":60,
        "ProtectGroupID":"antibgp_60g",
        "ProtectGroupName":"高防BGP_60G"
      },
      "IPUserID":"da",
      "OpenTimeStamp":"2017-12-05T08:18:43Z",
      "Package":"",
      "Region":"靠谱云福州4区",
      "Status":"open",
      "Zone":"cn-fuzhou-4-a",
      "ip":"10.2.2.5"
    }
  ]
}
```



```
],  
  "RequestId": "5046d2cd-23dd-4e4d-9d03-a51aef900ba7",  
  "Status": "Success",  
  "Timestamp": "2017-12-06 17:36:37"  
}
```

4. 查看高防IP的状态

描述

地址: /ip

查看高防IP的防护状态信息。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeIPStatus
IP	String	否	IP地址，支持批量IP，多个IP用逗号（半角）分隔；若参数为空，默认返回所有IP的数据
IPUserID	String	否	IP地址隶属的二级用户ID

返回参数

参数名	类型	说明
IPStatusData	IPStatusData[]	IP状态数据集

类型说明

IPStatusData节点说明

参数名	类型	说明
IP	String	IP地址
IPStatus	String	IP的当前黑洞状态，以下值中的一个： Normal---正常 BlackHole---黑洞
protectGroupStatus	String	套餐所处的状态： Close---关闭服务(黑洞阈值为0) Guarantee---保底状态(黑洞阈值为保底带宽) Elastic---弹性峰值状态(黑洞阈值为弹性峰值带宽)
BlackHoleStatus	String	黑洞信息数据
	String	IP对应所在运营商线路的黑洞状态，对应值为： CTC---电信 CMCC---移动 CNC---联通
StartTime	String	进入黑洞的时间，仅当黑洞状态时该值有效，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
EndTime	String	结束黑洞的时间，仅当黑洞状态时该值有效，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒

错误码

错误代码	描述	Http状态码	语义
IPError	You don't have permission to view this IP's data	401	没有权限查看该IP的信息
IPNotExist	IP is not exist.	402	查询的IP不存在

返回示例

```
{
  "Code": "200",
  "IPStatusData":
  [
    {
      "BlackHoleStatus":
```

```

        {
        },
        "IP": "10.1.1.1",
        "IPStatus": "Normal",
        "protectGroupStatus": "Elastic"
    },

    {
        "BlackHoleStatus":
        {
            "CMCC":
            {
                "EndTime": "2017-06-01T12:38:53Z",
                "StartTime": "2017-06-01T11:08:15Z"
            },
            "CNC":
            {
                "EndTime": "2017-06-01T12:39:53Z",
                "StartTime": "2017-06-01T11:08:13Z"
            }
        },
        "IP": "10.1.1.2",
        "IPStatus": "BlackHole",
        "protectGroupStatus": "Elastic"
    }
],
"Message": "Success",
"RequestId": "65c2fc43-92c5-42ca-a855-ff151832d3e2",
"Status": "Success",
"Timestamp": "2017-06-01 12:03:31"
}

```

5.修改IP的防护组

描述

地址: /ip

修改IP的防护组信息，支持修改保底防护组或弹性防护组，**可单独修改其中一项或同时修改两项**，对应的生效时间参数是必须的；在生效时间之前如果有多次提交，则以最后一次提交为准。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：ModifyIPProtectGroup
IP	String	是	IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
GuaranteeProtectGroupId	String	否	保底高防IP的防护组ID
GuaranteeEnableTime	TimeStamp		高防IP保底流量修改的生效时间，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
ElasticProtectGroupId	String	否	弹性高防IP的防护组ID
ElasticEnableTime	TimeStamp		高防IP弹性流量修改的生效时间，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
Region	String	是	地域
Zone	String	是	可用区
BandwidthType	String	是	线路类型： AntiBGP---高防BGP AntiTele---高防电信 SuperAntiBGP---超防BGP SuperAntiTele---超防电信

返回参数

无

类型说明

无

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "870286df-5228-4246-9e11-927419fb2a0a",
  "Status": "Success",
  "Timestamp": "2017-08-07 17:43:27"
}
```

6.关闭IP的弹性流量服务

描述

地址：/ip

关闭Ip的弹性流量服务，保留保底带宽防护。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：CloseIPElasticAntiDDos
IP	String	是	IP地址
IPUserID	String	否	IP地址隶属的二级用户ID

返回参数

无

类型说明

无

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "07308c64-6b3e-4bf0-9255-1b502785f004",
  "Status": "Success",
  "Timestamp": "2017-08-08 09:46:13"
}
```

7.开启IP的弹性流量服务

描述

地址： /ip

开启IP的弹性流量服务。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：OpenIPElasticAntiDDos
IP	String	是	IP地址
IPUserID	String	否	IP地址隶属的二级用户ID

返回参数

无

类型说明

无

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "07308c64-6b3e-4bf0-9255-1b502785f004",
  "Status": "Success",
  "Timestamp": "2017-08-08 09:46:13"
}
```

8.关闭高防IP防护

描述

地址：/ip

关闭IP的高防服务(将防护组调整为free组别)。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：CloseIPAntiDDos
IP	String	是	IP地址
IPUserID	String	否	IP地址隶属的二级用户ID

返回参数

无

类型说明

无

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "07308c64-6b3e-4bf0-9255-1b502785f004",
  "Status": "Success",
  "Timestamp": "2017-08-08 09:46:13"
}
```

9.开启高防IP防护

描述

地址：/ip

开启高防IP的防护，将其防护状态调整为最近一次关闭高防防护之前的状态。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：OpenIPAntiDDos
IP	String	是	IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
ElasticEnable	Boolean	是	True:开启弹性流量 False:不开启弹性流量

返回参数

无

类型说明

无

错误码

无

返回示例


```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "07308c64-6b3e-4bf0-9255-1b502785f004",
  "Status": "Success",
  "Timestamp": "2017-08-08 09:46:13"
}
```

10.从指定防护组删除IP

描述

地址：/ip

将指定IP从防护组中删除。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DeleteProtectGroupIP
IP	String	是	IP地址
IPUserID	String	否	IP地址隶属的二级用户ID

返回参数

无

类型说明

无

错误码

错误代码	描述	Http状态码	语义
IPError	PermissionDeny.	9403	没有权限修改该IP的信息
CommitFail	Commit Fail	9408	提交修改失败, 请联系运维人员线下修改

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "07308c64-6b3e-4bf0-9255-1b502785f004",
  "Status": "Success",
  "Timestamp": "2017-08-08 09:46:13"
}
```

11. 查看高防IP的带宽信息

描述

地址: /ip

- 1) 查看高防IP的带宽信息
- 2) 带宽信息的精度根据查询的时间段来判断:

```
<=1天: 5分钟一个点
<=3天: 15分钟一个点
<=6天: 30分钟一个点
<=12天: 1小时一个点
<=30天: 3小时一个点
>30天: 以1天为一个点
```

- 3) 返回的数据点中必须包含时间段中的峰值
- 4) 如果EndTime - StartTime<300S, 则只返回 StartTime 一个点的数据。
- 5) StartTime不为整5分钟的情况, 则向下取整5分钟 (如2016-10-28 11:12:00则转为2016-10-28 11:10:00)
- 6) EndTime范围内无数据的节点, 则不返回该节点数据
- 7) 带宽信息只提供入流量的数据

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeIPMonitorData
IP	String	是	IP地址，支持批量IP，多个IP用逗号（半角）分隔
IPUserID	String	否	IP地址隶属的二级用户ID
StartTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
EndTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
Region	String	否	地域
Zone	String	否	可用区
BandwidthType	String	否	带宽类型

返回参数

参数名	类型	说明
IPMonitorData	IPMonitorDataSetType	实例的监控数据IPMonitorDataSetType数据集合。

类型说明

IPMonitorDataSetType节点参数说明

参数名	类型	说明
IP	String	IP地址
KBPS	Integer	相应时间精度内，kbps均值
PPS	Integer	相应时间精度内，pps均值
KBPS_MAX	Integer	相应时间精度内，kbps最大值
PPS_MAX	Integer	相应时间精度内,pps最大值
TimeStamp	String	数据对应的时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒

错误码

错误代码	描述	Http状态码	语义
IPError	You don't have permission to view this IP's data	401	没有权限查看该IP的信息
TimeError	The time you entered is incorrect	9400	输入的时间范围有误

返回示例

```
{
  "Code": "200",
  "IPMonitorData": [
    {
      "Data": [
        {
          "KBPS": "4",
          "KBPS_MAX": "41",
          "PPS": "5",
          "PPS_MAX": "61",
          "TimeStamp": "2016-11-29 20:15:00"
        },
        {
          "KBPS": "3",
          "KBPS_MAX": "22",
          "PPS": "4",
          "PPS_MAX": "29",
          "TimeStamp": "2016-11-29 20:35:00"
        },
        {
          "KBPS": "7",
          "KBPS_MAX": "29",
          "PPS": "8",
          "PPS_MAX": "37",
          "TimeStamp": "2016-11-29 20:40:00"
        },
        {
          "KBPS": "6",
          "KBPS_MAX": "29",
          "PPS": "8",
          "PPS_MAX": "37",
          "TimeStamp": "2016-11-29 20:45:00"
        },
        {
          "KBPS": "6",
          "KBPS_MAX": "28",
          "PPS": "8",
          "PPS_MAX": "36",
          "TimeStamp": "2016-11-29 20:50:00"
        }
      ]
    },
  ],
}
```

```

    {
      "KBPS": "8",
      "KBPS_MAX": "64",
      "PPS": "10",
      "PPS_MAX": "87",
      "TimeStamp": "2016-11-29 20:55:00"
    },
    {
      "KBPS": "8",
      "KBPS_MAX": "35",
      "PPS": "10",
      "PPS_MAX": "37",
      "TimeStamp": "2016-11-29 21:00:00"
    },
    {
      "KBPS": "4",
      "KBPS_MAX": "27",
      "PPS": "5",
      "PPS_MAX": "37",
      "TimeStamp": "2016-11-29 21:05:00"
    },
    {
      "KBPS": "4",
      "KBPS_MAX": "24",
      "PPS": "6",
      "PPS_MAX": "34",
      "TimeStamp": "2016-11-29 21:10:00"
    },
    {
      "KBPS": "5",
      "KBPS_MAX": "23",
      "PPS": "7",
      "PPS_MAX": "32",
      "TimeStamp": "2016-11-29 21:15:00"
    }
  ],
  "ip": "125.77.30.212"
},
{
  "Data": [],
  "ip": "45.126.122.14"
}
],
"Message": "Success",
"RequestId": "044a02e1-6439-4fdb-a063-94fab9f327c5",
"Status": "Success",
"Timestamp": "2016-12-02 17:30:11"
}

```

12.查看高防IP的带宽峰值与黑洞次数

描述

地址: /ip

- 1) 查看高防IP的带宽峰值信息
- 2) 返回的数据点中必须包含时间段中的峰值 3) 如果EndTime - StartTime<300S，则只返回 StartTime 一个点的数据。 4) StartTime不为整5分钟的情况，则向下取整5分钟（如2016-10-28 11:12:00则转为2016-10-28 11:10:00）
- 5) EndTime范围内无数据的节点，则不返回该节点数据 6) 带宽信息只提供入流量的数据

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeIPMaxMonitorData
IP	String	是	IP地址，支持批量IP，多个IP用逗号（半角）分隔
IPUserID	String	否	IP地址隶属的二级用户ID
StartTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
EndTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
Region	String	否	地域
Zone	String	否	可用区
BandwidthType	String	否	带宽类型

返回参数

参数名	类型	说明
IPMaxMonitorData	IPMaxMonitorDataSetType[]	带宽峰值的峰值与黑洞次数

类型说明

参数名	类型	说明
IP	String	IP
KBPS_MAX	Integer	相应时间精度内，KBPS峰值
PPS_MAX	Integer	相应时间精度内，PPS峰值
BlackHoleTimes	Integer	查询时间段内，IP为高防IP（非处于服务包期间）的黑洞次数，若传递参数PackageID，则为在服务包内的黑洞次数

错误码

无

返回示例

```
{
  "Code":200,
  "IPMaxMonitorData":
  [
    {
      "BlackHoleTimes":0,
      "IP":"45.126.120.122",
      "KBPS_MAX":0,
      "PPS_MAX":0,
      "TimeStamp":"2017-10-31T05:50:00"
    },
    {
      "BlackHoleTimes":0,
      "IP":"10.1.1.88",
      "KBPS_MAX":665,
      "PPS_MAX":56,
      "TimeStamp":"2017-10-31T05:50:00"
    }
  ],
  "Message":"Success",
  "RequestId":"a5cbc894-0f30-4c7d-a62f-743cf512d5a5",
  "Status":"Success",
  "Timestamp":"2017-12-13 17:37:48"
}
```

13. 查看高防IP分线路的带宽信息

描述

地址： /ip

- 1) 查看高防IP分线路的带宽信息
- 2) 带宽信息的精度根据查询的时间段来判断:

<=1天： 5分钟一个点
<=3天： 15分钟一个点
<=6天:30分钟一个点
<=12天:1小时一个点
<=30天:3小时一个点
>30天： 以1天为一个点

- 3) 返回的数据点中必须包含时间段中的峰值
- 4) 如果EndTime - StartTime<300S， 则只返回 StartTime 一个点的数据。
- 5) StartTime不为整5分钟的情况， 则向下取整5分钟（如2016-10-28 11:12:00则转为2016-10-28 11:10:00）
- 6) EndTime范围内无数据的节点， 则不返回该节点数据
- 7) 带宽信息只提供入流量的数据

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeIPLineMonitorData
IP	String	是	IP地址，支持批量IP，多个IP用逗号（半角）分隔
IPUserID	String	否	IP地址隶属的二级用户ID
StartTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
EndTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
Region	String	否	地域
Zone	String	否	可用区
BandwidthType	String	否	带宽类型

返回参数

参数名	类型	说明
IPLineMonitorData	IPLineMonitorDataSetType	实例的监控数据IPLineMonitorDataSetType数据集合。

类型说明

IPLineMonitorDataSetType节点参数说明

参数名	类型	说明
IP	String	IP地址
Line	String	线路
KBPS	Integer	5分钟内, kbps均值
PPS	Integer	5分钟内, pps均值
KBPS_MAX	Integer	5分钟内, kbps最大值
PPS_MAX	Integer	5分钟内,pps最大值
TimeStamp	String	数据对应的时间点, 日期和时间合并表示时, 采用UTC时间, 遵循ISO 8601, 在两者中间加大写字母T, 在时间之后加大写字母Z, 例如2017-06-01T23:00:10Z 表示UTC时间2017年6月1日23点0分10秒

错误码

错误代码	描述	Http状态码	语义
IPError	You don't have permission to view this IP's data	401	没有权限查看该IP的信息
TimeError	The time you entered is incorrect	9400	输入的时间范围有误

返回示例

```
{
  "Code": "Success",
  "IPMonitorData": [
    {
      "Data": [
        {
          "KBPS": "4",
          "KBPS_MAX": "41",
          "PPS": "5",
          "PPS_MAX": "61",
          "TimeStamp": "2016-11-29 20:15:00"
        },
        {
          "KBPS": "3",
          "KBPS_MAX": "22",
```

```

        "PPS": "4",
        "PPS_MAX": "29",
        "TimeStamp": "2016-11-29 20:35:00"
    },
    {
        "KBPS": "5",
        "KBPS_MAX": "23",
        "PPS": "7",
        "PPS_MAX": "32",
        "TimeStamp": "2016-11-29 21:15:00"
    }
],
"Line": "CTC",
"ip": "125.77.30.212"
},
{
    "Data": [],
    "Line": "CTC",
    "ip": "45.126.122.14"
}
],
"Message": "Success",
"RequestId": "044a02e1-6439-4fdb-a063-94fab9f327c5",
"Status": "Success",
"Timestamp": "2016-12-02 17:30:11"
}

```

14. 获取高防IP预警信息

描述

地址: /ip

获取高防IP预警信息。

开始时间和结束时间为可选参数，如果不提供这两个参数，则获取最新一次获取之后的所有预警信息；开始时间和结束时间间隔上限600秒。

预警信息生命周期为1天。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：GetIPMetricInfo
IP	String	否	IP地址，支持批量IP，多个IP用逗号（半角）分隔；若参数为空，默认返回所有IP的数据
IPUserID	String	否	IP地址隶属的二级用户ID
StartTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
EndTime	String	是	获取数据的起始时间点，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒

返回参数

参数名	类型	说明
IPMetricInfoData	IPMetricInfoData[]	预警信息数据集

类型说明

IPMetricInfoData节点说明

参数名	类型	说明
Name	String	预警名称： BPS一带宽流量预警，单位GB
IP	String	IP地址
Timestamp	String	预警触发时间，日期和时间合并表示时，采用UTC时间，遵循ISO 8601，在两者中间加大写字母T，在时间之后加大写字母Z，例如2017-06-01T23:00:10Z表示UTC时间2017年6月1日23点0分10秒
Current	String	当前值
Threshold	String	预警阈值
Type	String	预警阈值类别，取值：'SYS','GUARANTEE','ELASTIC',分别对应系统级别、保底级别、峰值级别
Ratio	String	预警阈值比例（百分比）
Line	String	线路信息，取值：'CTC','CMCC','CNC','TOTAL'
Msg	String	预警信息

错误码

错误代码	描述	Http状态码	语义
IPError	You don't have permission to view this IP's data	401	没有权限查看该IP的信息
IPNotExist	IP is not exist.	402	查询的IP不存在

返回示例

```
{
  "Code": "200",
  "IPMetricsInfoData": [
    {
      "Current": "0.23",
      "IP": "10.1.1.2",
      "Line": "CNC",
      "Msg": "Exceeds the Sys threshold[CNC]",
      "Name": "metric_bps",
      "Ratio": "100%",
      "Threshold": "0.0098",
      "Timestamp": "2017-07-04 14:16:40",
      "Type": "SYS"
    }
  ],
  "Message": "Success",
  "RequestId": "768c23a3-d5a7-4267-9d13-153afbb69e79",
  "Status": "Success",
  "Timestamp": "2017-07-04 14:23:18"
}
```

15. 查询IP在防火墙名单

描述

地址: /ip

查询IP是否在防火墙黑白名单中

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeIPFirewallList
Operator	String	是	系统规定参数，取值：'ctc','cmcc','cnc','bgp'
Hostname	String	是	可输入需要查询的IP
IPUserID	String	否	IP地址隶属的二级用户ID

返回参数说明

参数名	类型	说明
DescribeIPFirewallList	DescribeIPFirewallListdata	IP是否在防火墙名单中

状态码

查询成功为Success，否则为Fail；BGP中当三个防火墙全成功才为Success，否则为Fail
IP在白名单
IP不在名单
防火墙连接超时

返回示例

```
{
  "Code":200,
  "DescribeIPFirewallList":"bgp:IP不在白名单",
  "Message":"Success",
  "RequestId":"f2ab5ff6-5b4c-4863-af8e-048827d775d5",
  "Status":"Success",
  "Timestamp":"2017-11-27 16:09:58"
}
```

16. 添加IP至防火墙白名单

描述

地址：/ip

将IP添加到防火墙白名单中

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：AddIPWhiteList
PackageID	String	否	高防包ID
IP	String	否	高防IP地址
Operator	String	是	系统规定参数，取值：'ctc','cmcc','cnc','bgp'
Hostname	String	是	可输入需要添加的IP
IPUserID	String	是	IP地址隶属的二级用户

返回参数

参数名	类型	说明
AddIPWhiteList	AddIPWhiteListtype	防火墙添加IP至白名单成功与否结果

状态码

查询成功为Success，否则为Fail；BGP中当三个防火墙全成功才为Success，否则为Fail
IP添加至白名单
防火墙连接超时
此IP已被他人配置

返回示例

```
{
  "AddIPWhiteList": "bgp:IP添加至白名单",
  "Code": 200,
  "Message": "Success",
  "RequestId": "b4997cf7-ba8b-45fe-9d19-11c4f44b5652",
  "Status": "Success",
  "Timestamp": "2017-11-27 16:22:37"
}
```

17. 从防火墙白名单中删除IP

描述

地址： /ip

将IP从防火墙白名单中删除

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DeleteIPWhiteList
PackageID	String	否	高防包ID
IP	String	否	高防IP地址
Operator	String	是	系统规定参数，取值：'ctc','cmcc','cnc','bgp'
Hostname	String	是	输入需要删除的IP
IPUserID	String	是	IP地址隶属的二级用户ID

返回参数

参数名	类型	说明
DeleteIPWhiteList	DeleteIPWhiteListtype	防火墙从白名单中删除成功与否结果

状态码

查询成功为Success，否则为Fail；BGP中当三个防火墙全成功才为Success，否则为Fail
IP从白名单删除
防火墙连接超时
此IP已被他人配置

返回示例

```
{
  "Code":200,
  "DeleteIPWhiteList":"bgp:IP从白名单删除",
  "Message":"Success",
  "RequestId":"ca57acb1-dce7-4bfe-9dc5-6a4bea04e7f5",
  "Status":"Success",
  "Timestamp":"2017-11-27 16:22:57"
}
```

18.查询用户名白名单记录

描述

查询查询用户名下白名单明细

请求参数

参数	类型	是否必选	说明
Action	String	是	系统规定参数，取值：DescribeUserFirewallWhiteList
IPUserID	String	是	IP地址隶属的二级用户ID
IP	String	否	高防IP，传则显示这个IP名下白名单，不传则显示用户名下白名单

返回参数

参数	类型	说明
UserWhiteListData	UserWhiteListDataType	用户白名单信息集合

类型说明

参数	类型	说明
高防IP：[白名单IP，白名单IP...]	Dict	用户白名单信息高防IP-白名单IP键值对

状态码

Code	Message	说明
9403	FirewallConnFail	防火墙连接失败

返回示例


```
{
  "Code":200,
  "Message":"Success",
  "RequestId":"67a8aa03-ac16-4d89-bda1-b97630fa17d1",
  "Status":"Success",
  "Timestamp":"2017-11-27 10:11:53",
  "UserWhiteListData":
  [
    {
      "45.126.122.93":
      [
        "10.10.10.10",
        "10.1.1.82"
      ]
    }
  ]
}
```