

# 文档版本

---

2017-12-08

## 变更日志

---

- 2018-05-10
  - Changes
    - DescribeIPFirewallProtect
      - 修复请求Action文档
- 2018-04-23
  - Changes
    - DescribeIPFirewallProtect
      - 修改返回值
    - SetIPFirewallProtect
      - 修改传入值、返回值
- 2017-12-8
  - Changes
    - 查看高防IP的带宽峰值
      - 返回格式调整，参数新增BlackHoleTimes黑洞次数
    - 获取IP的防护组信息
      - 新增参数Package,显示IP是否属于高防包
- 2017-12-2
  - Changes
    - 查看高防IP的带宽信息，传入参数新增PackageID字段
    - 查看高防IP的带宽峰值，传入参数新增PackageID字段
    - 查看高防IP分线路的带宽信息，传入参数新增PackageID字段
- 2017-11-22
  - Changes
    - 查询防火墙防护策略
    - 设置防火墙防护策略
- 2017-11-17
  - Changes
    - 查询系统高防防护包列表
    - 创建高防防护包
    - 查询防护包信息
    - 添加IP到高防防护包
    - 修改高防防护包配置
    - 从高防防护包删除IP
    - 删除高防防护包
    - 延长高防防护包期限
    - 关闭高防防护包弹性防护
    - 开启高防防护包弹性防护

- 
- 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
- 2017-09-17
  - 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
- 2017-07-26
  - Changes
    - 控制防火墙的接口
      - 查询防火墙主机设置集序号
      - 设置防火墙主机状态集序号

- 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
      - 查询防火墙屏蔽列表
      - 重置防火墙屏蔽列表
- 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」
- 2017-06-16
  - New features
    - 「创建高防IP四层防护配置」
    - 「更新高防IP四层防护配置」
    - 「删除高防IP四层防护配置」
    - 「更新高防IP七层防护配置」
    - 「更新高防IP七层防护配置」
    - 「删除高防IP七层防护配置」
- 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_server%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&Urls=%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
&Urls=%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&Urls=%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
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



错误码	错误信息	描述
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	CreateIPFourLayerAntiConfig	创建高防IP四层防护配置	
14	UpdateIPFourLayerAntiConfig	更新高防IP四层防护配置	
15	DeleteIPFourLayerAntiConfig	删除高防IP四层防护配置	
16	CreateIPSevenLayerAntiConfig	创建高防IP七层防护配置	
17	UpdateIPSevenLayerAntiConfig	更新高防IP七层防护配置	
18	DeleteIPSevenLayerAntiConfig	删除高防IP七层防护配置	
19	DescribeIPLineMonitorData	查看高防IP分线路的带宽信息	
20	GetIPMetricInfo	获取高防IP预警信息	
21	DescribeDomainFirewallList	查询域名在防火墙名单	
22	DescribeIPFirewallList	查询IP在防火墙名单	
23	AddDomainWhiteList	添加域名至防火墙白名单	
24	AddIPWhiteList	添加IP至防火墙白名单	
25	DeleteDomainWhiteList	从防火墙白名单中删除域名	
26	DeleteIPWhiteList	从防火墙白名单中删除IP	
27	DescribeBlockList	查询防火墙屏蔽列表	
28	ResetBlockIP	重置防火墙屏蔽列表	
29	DescribeIPFirewallProtect	查询防火墙防护策略	
30	SetIPFirewallProtect	设置防火墙防护策略	
31	DescribeBlackHoleInfo	查看黑洞信息	
32	CreateProtectPackage	创建高防防护包	

序号	名称	描述	备注
33	DescribeProtectPackage	查询防护包信息	
34	AddProtectPackageIP	添加IP到高防防护包	
35	ModifyProtectPackage	修改高防防护包配置	
36	DeleteProtectPackageIP	从高防防护包删除IP	
37	DeleteProtectPackage	删除高防防护包	
38	ExtendProtectPackageDueTime	延长高防防护包期限	
39	ClosePackageElasticAntiDDos	关闭高防防护包弹性防护	
40	OpenPackageElasticAntiDDos	开启高防防护包弹性防护	
41	DescribeIPData	查看IP信息	
42	DescribeUserFirewallWhiteList	查询用户名白名单记录	

# 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
BandwithType	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
RegionNotExit	Region Type is not exist	9402	指定的地域不存在
ZoneNotExit	Zone Type is not exist	9402	指定的可用区不存在
BandwithTypeNotExit	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
BandwidthType	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所属服务包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			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	String		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	IP is not exit.	9403	没有权限查看该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，可查询高防IP与服务包IP。若传递参数PackageID，返回在相应服务包时间内的带宽信息，不传递参数PackageID，返回高防IP不属于服务包时间的带宽信息

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
PackageID	String	否	IP所属的服务包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，可查询高防IP与服务包IP。若传递参数PackageID，返回在相应服务包时间内的带宽峰值信息与黑洞次数，不传递参数PackageID，返回高防IP不属于服务包时间的带宽峰值信息

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
PackageID	String	否	IP所属的服务包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. 创建高防IP四层防护配置

#### 描述

地址: /ip

创建高防IP四层防护配置

#### 请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：CreateIPFourLayerAntiConfig
IP	String	是	高防IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
Configs	FourLayerAntiConfig[]	是	四层防护配置，字符串内包含键值对的配置信息，并且需要转义，转义方法同URL，配置示例： "[{'Protocol':'TCP','Port':'8148','SourceIP':'27.148.196.94:8000'}]"

#### FourLayerAntiConfig

参数名	类型	必选	说明
Port	String	是	监听的端口号
Protocol	String	是	接入协议：TCP
SourceIP	String	是	单个的源站IP，如果包含端口号，IP和端口号之间用冒号连接，如：10.1.1.1:3306

返回参数

参数名	类型	说明
FourLayerAntiConfigInfo	FourLayerAntiConfigDataSetType	配置信息FourLayerAntiConfigDataSetType的集合

类型说明

参数名	类型	说明
UUID	String	配置信息的唯一标识符

错误码

无

返回示例

```
{
  "Code": "200",
  "FourLayerAntiConfigInfo": {
    "UUID": "25102260430176407"
  },
  "Message": "Success",
  "RequestId": "5a7f8250-0327-445d-862b-94591dbc593a",
  "Status": "Success",
  "Timestamp": "2017-06-15 16:08:16"
}
```

14. 更新高防IP四层防护配置

描述

地址： /ip

更新高防IP四层防护配置

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值： UpdateIPFourLayerAntiConfig
IP	String	是	高防IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
UUID	String	是	配置信息的唯一标识符
Configs	FourLayerAntiConfig[]	是	四层防护配置，字符串内包含键值对的配置信息，并且需要转义，转义方法同URL，配置示例： "[{'Protocol':'TCP','Port':'8148','SourceIP':'27.148.196.94:8000'}]"

FourLayerAntiConfig

参数名	类型	必选	说明
Port	String	是	监听的端口号
Protocol	String	是	接入协议：TCP
SourceIP	String	是	单个的源站IP，如果包含端口号，IP和端口号之间用冒号连接，如：10.1.1.1:3306

返回参数

无

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "5a7f8250-0327-445d-862b-94591dbc593a",
  "Status": "Success",
  "Timestamp": "2017-06-15 16:08:16"
}
```

15. 删除高防IP四层防护配置

描述

地址： /ip

删除高防IP四层防护配置

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：UpdateIPFourLayerAntiConfig
IP	String	是	高防IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
UUID	String	是	配置信息的唯一标识符

返回参数

无

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "f03e981b-9a17-4eef-8709-528581a2476d",
  "Status": "Success",
  "Timestamp": "2017-06-16 09:54:18"
}
```

## 16. 创建高防IP七层防护配置

### 描述

地址: /ip

创建高防IP七层防护配置

### 请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：CreatelPSevenLayerAntiConfig
IP	String	是	高防IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
Configs	SevenLayerAntiConfig[]	是	七层防护配置，字符串内包含键值对的配置信息，并且需要转义，转义方法同URL，配置示例： "[{'Type':'Site','Domain':'antiddos.api-test.kaopuyun.com','Cname':'antiddos.api-test.kaopuyun.com','Protocol':'Http', 'PublicKey':'PublicKey','PrivateKey':'PrivateKey','Port':'80','SourceIPs':'10.1.1.1:8000'}]"

#### SevenLayerAntiConfig

参数名	类型	必选	说明
Type	String	是	业务类型: Site---网站 App---App
Domain	String	是	域名
Cname	String	否	Cname
Protocol	String	是	接入协议: HTTP HTTPS
PublicKey	String	否	公钥信息，HTTPS协议需要
PrivateKey	String	否	密钥信息，HTTPS协议需要
Port	String	是	端口号，默认情况下HTTP端口号80，HTTPS端口号443
SourceIPs	String	是	源站IP，多个IP之间用逗号分隔，如果包含端口号，IP和端口号之间用冒号连接，如： 10.1.1.1:80,10.1.1.2:80



返回参数

参数名	类型	说明
SevenLayerAntiConfigInfo	SevenLayerAntiConfigDataSetType	配置信息SevenLayerAntiConfigDataSetType的集合

类型说明

参数名	类型	说明
UUID	String	配置信息的唯一标识符

错误码

无

返回示例

```
{
  "Code": "200",
  "FourLayerAntiConfigInfo": {
    "UUID": "SLBSevenLayer-25102260430176431"
  },
  "Message": "Success",
  "RequestId": "6cfb8994-6f80-4535-a622-e2a957a44930",
  "Status": "Success",
  "Timestamp": "2017-06-16 15:07:58"
}
```

17. 更新高防IP七层防护配置

描述

地址：/ip

更新高防IP七层防护配置。

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值： UpdateIPSevenLayerAntiConfig
IP	String	是	高防IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
UUID	String	是	配置信息的唯一标识符
Configs	SevenLayerAntiConfig[]	是	七层防护配置，字符串内包含键值对的配置信息并且需要转义，转义方法同URL 配置示例： "[{'Type':'Site','Domain':'antiddos.api-test.kaopuyun.com','Cname':'antiddos.api-test.kaopuyun.com','Protocol':'Http','PublicKey':'PublicKey','PrivateKey':'PrivateKey','Port':'80','SourceIPs':'10.1.1.1:8000'}]"

SevenLayerAntiConfig

参数名	类型	必选	说明
Type	String	是	业务类型: Site---网站 App---App
Domain	String	是	域名
Cname	String	否	Cname
Protocol	String	是	接入协议: HTTP HTTPS
PublicKey	String	否	公钥信息，HTTPS协议需要
PrivateKey	String	否	密钥信息，HTTPS协议需要
Port	String	是	端口号，默认情况下HTTP端口号80，HTTPS端口号443
SourceIPs	String	是	源站IP，多个IP之间用逗号分隔，如果包含端口号，IP和端口号之间用冒号连接，如： 10.1.1.1:80,10.1.1.2:80

### 返回参数

无

### 类型说明

无

### 错误码

无

### 返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "5a7f8250-0327-445d-862b-94591dbc593a",
  "Status": "Success",
  "Timestamp": "2017-06-15 16:08:16"
}
```

## 18. 删除高防IP七层防护配置

### 描述

地址： /ip

删除高防IP七层防护配置。

### 请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DeleteIPSevenLayerAntiConfig
IP	String	是	高防IP地址
IPUserID	String	否	IP地址隶属的二级用户ID
UUID	String	是	配置信息的唯一标识符

返回参数

无

错误码

无

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "f03e981b-9a17-4eef-8709-528581a2476d",
  "Status": "Success",
  "Timestamp": "2017-06-16 09:54:18"
}
```

19. 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，可查询高防IP与服务包IP。若传递参数PackageID，返回在相应服务包时间内的分线路带宽信息，不传递参数PackageID，返回高防IP不属于服务包时间的分线路带宽信息
- 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
PackageID	String	否	IP所属的服务包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"
}
```

20. 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—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
Code(弃用)	String	预警代码，以逗号分隔的关于预警信息的关键信息的描述,四个字段，分别表示：预警信息类别,预警阈值类别,预警阈值比例（百分比）,线路，例如： BPS,SYS,100,CNC—BPS带宽流量预警,系统阈值,100%,CNC联通线路 BPS,GUARANTEE,100,TOTAL—BPS带宽流量预警,保底阈值,100%,所有线路合并 BPS,ELASTIC,80,TOTAL—BPS带宽流量预警,弹性阈值,80%,所有线路合并

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"
}
```

## 21. 查询域名在防火墙名单

### 描述

地址: /ip

查询域名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：DescribeDomainFirewallList
Operator	String	是	系统规定参数，取值：'ctc','cmcc','cnc','bgp'
Hostname	String	是	可输入需要查询的域名
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
DescribeDomainFirewallList	DescribeDomainFirewallListdata	域名是否在防火墙名单中

### 状态码



查询成功为 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
域名在白名单
域名在黑名单
域名不在名单
防火墙连接超时

返回示例

```
{
  "Code":200,
  "DescribeDomainFirewallList":"bgp:域名不在白名单",
  "Message":"Success",
  "RequestId":"a4f1085b-8635-4f3d-a5d4-ed64b731dad5",
  "Status":"Success",
  "Timestamp":"2017-11-27 16:30:55"
}
```

22. 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 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
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"
}
```

### 23. 添加域名至防火墙白名单

地址: /ip

将域名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：AddDomainWhiteList
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	可输入需要添加的域名
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
AddDomainWhiteList	AddDomainWhiteListtype	防火墙添加域名至白名单成功与否结果

#### 状态码

查询成功为 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
域名添加至白名单
防火墙连接超时
此域名已被他人配置

#### 返回示例

```
{
  "AddDomainWhiteList":"bgp:域名添加至白名单",
  "Code":200,
  "Message":"Success",
  "RequestId":"ce045b5b-2d95-47a3-ac09-84cfce76f279",
  "Status":"Success",
  "Timestamp":"2017-11-27 16:31:32"
}
```

### 24. 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
PackagelD	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ID

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 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
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"
}
```

25. 从防火墙白名单中删除域名

描述

地址： /ip

将域名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：DeleteDomainWhiteList
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	输入需要删除的域名
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
DeleteDomainWhiteList	DeleteDomainWhiteListtype	防火墙从白名单中删除成功与否结果

状态码

查询成功为 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
域名从白名单删除
防火墙连接超时
此域名已被他人配置

返回示例

```
{
  "Code":200,
  "DeleteDomainWhiteList":"bgp:域名从白名单删除",
  "Message":"Success",
  "RequestId":"4b63bab8-ea27-414e-bd02-63c4311c8572",
  "Status":"Success",
  "Timestamp":"2017-11-27 16:47:07"
}
```

26. 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 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
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"
}
```

27. 查询防火墙屏蔽列表

描述

地址：/ip

控制防火墙查询IP是否在屏蔽列表中

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeBlockList
Operator	String	是	系统规定参数，取值：'ctc','cmcc','cnc','bgp'
SourceIP	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

参数名	类型	说明
fb_dict	dict	IP在屏蔽列表中对应的屏蔽地址和时间

状态码

查询成功为 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
查询结果即为fb_dict
防火墙连接超时

返回示例

```
{
  "BlockListData":
  [
    {
      "ctc":
      {
        "27.148.157.86-61.88.231.148": "2842"
      }
    },
    {
      "cmcc":
      {
      }
    },
    {
      "cnc":
      {
      }
    },
    {
      "new":
      {
      }
    }
  ],
  "Code": 200,
  "Message": "Success",
  "RequestId": "2b85b336-3999-4f7c-b82b-ac037c7f8b86",
  "Status": "Success",
  "Timestamp": "2017-11-27 17:56:00"
}
```

28. 重置防火墙屏蔽列表

描述

地址: /ip

重置防火墙对应源IP与目的IP的屏蔽列表

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：ResetBlockIP
Operator	String	是	系统规定参数，取值：'ctc','cmcc','cnc','bgp'
SourceIP	String	是	输入需要重置的源IP
remote_ip	String	是	输入需要重置的目的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
ResetBlockIP	ResetBlockIP	防火墙重置屏蔽列表结果

状态码

查询成功为 <b>Success</b> ，否则为 <b>Fail</b> ； <b>BGP</b> 中当三个防火墙全成功才为 <b>Success</b> ，否则为 <b>Fail</b>
源IP - 目的IP，reset
防火墙连接超时

返回示例

```
{
  "Code": "200",
  "Message": "Success",
  "RequestId": "7fd05fa7-0455-4cd7-a459-1ed776d632c0",
  "Status": "Success",
  "Timestamp": "2017-07-20 02:09:17",
  "cmcc": [
    "27.151.13.9-112.195.126.12, reset"
  ],
  "cnc": [
    "27.151.13.9-112.195.126.12, reset"
  ],
  "ctc": [
    "27.151.13.9-112.195.126.12, reset"
  ]
}
```

29. 查询防火墙防护策略

描述

地址：/ip

查询IP在防火墙内设置的集序号

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeIPFirewallProtect
IP	String	是	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

DescribeIPFirewallProtectData返回参数说明

参数名	类型	说明
GlobalProtectLevel	Int	防火墙防护策略等级，0，1，2数字越大越严格，默认为0
WebProtectLevel	Int	防火墙防护策略等级，0，1，2数字越大越严格，默认为0

状态码

分为宽松，中等，严格三个等级，查询成功为 <b>Success</b>
IP不存在
防火墙连接超时

返回示例

```
{
  "Code":200,
  "DescribeIPFirewallProtectData":
  {
    "GlobalProtectLevel":1,
    "WebProtectLevel":2
  },
  "Message":"Success",
  "RequestId":"e85a81e7-78e1-440a-b6ba-532a22536a53",
  "Status":"Success",
  "Timestamp":"2018-04-23 15:25:31"
}
```

30. 设置防火墙防护策略

描述

地址：/ip

设置IP在防火墙上的防护策略

请求参数



参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：SetIPFirewallProtect
IP	String	是	输入需要查询的IP
IPUserID	String	是	IP地址隶属的二级用户ID
GlobalProtectLevel	String	否	除Web防护外的全局防护策略，0，1，2三个防护等级数字越大越严格，不传则使用原有设定
WebProtectLevel	String	否	Web防护策略，0，1，2三个防护等级数字越大越严格，不传则使用原有设定

返回参数

参数名	类型	说明
SetIPFirewallProtectData	SetIPFirewallProtect type	设置IP在防火墙防护策略

状态码

设置宽松，中等，严格三个等级，成功为 <b>Success</b>
IP不存在
防火墙连接超时

返回示例

```
{
  "Code":200,
  "Message":"Success",
  "RequestId":"b271da08-7ca9-41f1-bdbe-bf93689424dc",
  "SetIPFirewallProtectData":
  [
    "45.126.120.122防护策略已设置"
  ],
  "Status":"Success",
  "Timestamp":"2017-11-21 14:29:35"
}
```

31. 查看IP黑洞信息

描述

地址：/ip

查看IP具体黑洞信息，只能查24小时之内的数据

请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeBlackHoleInfo
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
IPBlockHoleData	IPBlockHoleData[]	IP黑洞信息数据集

### 类型说明

参数名	类型	说明
IP	String	IP地址
Line	String	线路
Createdt	String	日期和时间合并表示时，采用UTC时间
Enddt	String	日期和时间合并表示时，采用UTC时间
Ban_time	String	黑洞时间
Current_value	String	黑洞时的线路值
Threshold_value	String	黑洞阈值
Direction	String	流量方向

### 错误码

无

### 返回示例

```

{
  "Code":200,
  "IPBlockHoleData":
  [
    {
      "ban_time":"00:20:00",
      "createdt":"2017-11-14-T11:30:43Z",
      "current_value":138834000000,
      "direction":"Incoming",
      "enddt":"2017-11-14-T11:50:43Z",
      "ip":"45.126.122.106",
      "line":"ctc",
      "threshold_value":100000000000
    },
    {
      "ban_time":"00:20:00",
      "createdt":"2017-11-14-T11:11:59Z",
      "current_value":170561000000,
      "direction":"Incoming",
      "enddt":"2017-11-14-T11:31:59Z",
      "ip":"45.126.122.106",
      "line":"ctc",
      "threshold_value":100000000000
    },
    {
      "ban_time":"00:20:00",
      "createdt":"2017-11-14-T11:11:54Z",
      "current_value":79635000000,
      "direction":"Incoming",
      "enddt":"2017-11-14-T11:31:54Z",
      "ip":"45.126.122.106",
      "line":"cnc",
      "threshold_value":70000000000
    },
    {
      "ban_time":"00:20:00",
      "createdt":"2017-11-14-T11:11:56Z",
      "current_value":60229000000,
      "direction":"Incoming",
      "enddt":"2017-11-14-T11:31:56Z",
      "ip":"45.126.122.106",
      "line":"cmcc",
      "threshold_value":35000000000
    }
  ],
  "Message":"Success",
  "RequestId":"8ef20dcd-ec25-4b01-b948-81843f4eedde",
  "Status":"Success",
  "Timestamp":"2017-11-16 14:55:01"
}

```

## 32.创建高防防护包

描述

创建高防防护包

请求参数

参数	类型	必选	说明
Action	String	是	系统规定参数，取值：CreateProtectPackage
IPUserID	String	是	IP地址隶属的二级用户ID
PackageName	String	是	防护包名称
GuaranteeProtectGroupID	String	是	防护包保底防护组
ElasticProtectGroupID	String	是	防护包弹性防护组
BandwidthType	String	是	带宽类型，必须是AntiBGP
IPNums	Int	是	防护包IP数量，上限256个
LifeDay	Int	是	防护包开通时长，单位（天）

返回参数

参数	类型	说明
ProtectPackageInfo	ProtectPackageInfoDataSet	防护包信息集

类型说明

参数	类型	说明
Due_Time	timestamp	防护包到期时间
PackageID	String	防护包ID，作为防护包唯一标识

状态码

Code	Message	说明
9402	指定带宽类型不存在	带宽指定只能为AntiBGP
9400	IP数量超过限制	IP数量上限为256个

返回示例

```
{
  "Code":200,
  "Message": "Success",
  "ProtectPackageInfo":
  {
    "Due_Time": "2017-12-07T01:21:20Z",
    "PackageID": "9e1af092-cb35-11e7-8e1b-50e54919757f"
  },
  "RequestId": "6b255d88-0982-4a99-b2d9-a8a89d669c78",
  "Status": "Success",
  "Timestamp": "2017-11-17 09:21:20"
}
```

### 33.查询防护包信息

描述

请求参数

参数	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeProtectPackage
IPUserID	String	否	IP地址隶属的二级用户ID
PackageID	String	否	防护包ID,可查看指定防护包信息，或所有防护包信息

返回参数

参数	类型	说明
ProtectPackageInfo	ProtectPackageInfoDataSet	防护包信息集合

类型说明

参数	类型	说明
CloseTimeStamp	String	关闭时间
DueTime	Timestamp	防护包预计到期时间
ElasticProtect	String	弹性防护组
GuaranteeProtect	String	保底防护组
IPNums	String	防护包IP数量上限
IPNumsUsed	String	防护包已使用IP数量
IPs	String	防护包中已存在的IP
OpenTimeStamp	Timestamp	开通时间
PackageID	String	防护包ID
PackageName	String	防护包名称
ProtectStatus	String	防护状态，保底/弹性/free
Status	String	开关状态：开启/关闭

状态码

无

返回示例

```
{
  "Code":200,
  "Message":"Success",
  "ProtectPackageInfo":
  [
    {
      "CloseTimeStamp":,
      "DueTime":"2017-12-05T02:49:11Z",
      "ElasticProtect":"高防BGP_60G",
      "GuaranteeProtect":"高防BGP_10G",
      "IPNums":90,
      "IPNumsUsed":4,
      "IPs":"10.1.1.61,10.1.1.45,10.1.1.56,10.1.1.60",
      "OpenTimeStamp":"2017-11-15T02:49:11Z",
      "PackageID":"8f0aa154-c9af-11e7-8aed-50e54919757f",
      "PackageName":"pkg_00312",
      "ProtectStatus":"Elastic",
      "Status":"open"
    },
    {
      "CloseTimeStamp":,
      "DueTime":"2017-12-06T02:17:49Z",
      "ElasticProtect":"高防BGP_100G",
      "GuaranteeProtect":"高防BGP_10G",
      "IPNums":26,
      "IPNumsUsed":0,
      "IPs":",
      "OpenTimeStamp":"2017-11-16T02:17:49Z",
      "PackageID":"577e2768-ca74-11e7-8415-50e54919757f",
      "PackageName":"pkg_00312",
      "ProtectStatus":"Elastic",
      "Status":"open"
    }
  ],
  "RequestId":"f088e904-ea6a-40c5-b942-c6367604006b",
  "Status":"Success",
  "Timestamp":"2017-11-16 14:22:49"
}
```

### 34.添加IP到高防防护包

#### 描述

添加IP到高防防护包

#### 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：AddProtectPackageIP
PackageID	String	是	防护包ID
IP	String	是	要添加的IP，需未在使用状态IP
IPUserID	String	是	IP地址隶属的二级用户ID

#### 返回参数

无

状态码

Code	Message	说明
9403	未处于正确的状态	IP已处于使用状态
9402	指定服务包不存在	指定防护包不存在，IPUserID或PackageID存在问题
9400	服务包IP余量不足	添加IP数量超过防护包上限
9403	服务包不允许该操作:请检查服务包状态	服务包关闭状态下，不允许操作

返回示例

```
{
  "Code":200,
  "Message": "Success",
  "RequestId":"3eda0be4-f73d-4e86-9dd2-f2a2c7d86a42",
  "Status":"Success",
  "Timestamp":"2017-11-16 15:17:39"
}
```

35.修改高防防护包配置

描述

修改高防防护包配置，可修改IP数量，保底防护组，弹性防护组，三者非必须参数，但须至少一个参数。

请求参数

参数	类型	必选	说明
Action	String	是	系统规定参数，取值：ModifyProtectPackage
IPUserID	String	是	IP地址隶属的二级用户ID
GuaranteeProtectGroupID	String	否	防护包保底防护组ID
GuaranteeEnableTime	Timestamp	否	高防包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	防护包弹性防护组ID
ElasticEnableTime	Timestamp	否	高防包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
PackageID	String	是	防护包ID
IPNums	String	否	防护包IP数量上限，不超过256

返回参数

无

状态码

Code	Message	说明
9405	您提交的参数错误:保底防护组需小于弹性防护组	保底防护组需小于弹性防护组
9405	您提交的参数错误:线路类型需为AntiBGP	保底/弹性防护组线路类型只能为AntiBGP
9405	您提交的参数错误: 请检查PackageID,IPUserID	PackageID或IPUserID输入错误
9304	修改前后数据没有变化: ['ipnums与原先相同', '保底防护组与原先相同', '弹性防护组与原先相同']	修改前后数据相同
9403	服务包状态不允许该操作:请检查服务包状态	服务包处于free状态或是关闭状态，不允许修改

返回示例

```
{
  "Code":200,
  "Message": "Success",
  "RequestId": "3eda0be4-f73d-4e86-9dd2-f2a2c7d86af3",
  "Status": "Success",
  "Timestamp": "2017-11-16 15:17:39"
}
```

36.从高防防护包删除IP

描述

从高防防护包删除IP，并删除IP相应防火墙与四七层配置

请求参数

参数	类型	是否必须	说明
Action	String	是	系统规定参数，取值：DeleteProtectPackageIP
PackageID	String	是	防护包ID
IP	IP	是	要操作的IP

返回参数

无

状态码

Code	Message	说明
9403	IP未在使用中: 10.1.1.39,10.1.1.40	IP未在使用
9405	您提交的参数错误: 请检查PackageID,IPUserID	PackageID或IPUserID输入错误
9401	您没有权限进行该操作: IP不属于此服务包	IP不属于此服务包

返回示例



```
{
  "Code":200,
  "Message":"Success",
  "RequestId":"6614ea20-e5bf-41fd-bbd6-32b8b4c24d23",
  "Status":"Success",
  "Timestamp":"2017-11-16 17:29:32"
}
```

### 37.删除高防防护包

#### 描述

删除高防防护包，并删除相应防火墙配置

#### 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：DeleteProtectPackage
IPUserID	String	是	IP地址隶属的二级用户ID
PackageID	String	是	防护包ID

#### 返回参数

无

#### 状态码

Code	Message	说明
9402	指定服务包不存在	服务包不存在，查看IPUserID或PackageID
9403	服务包状态不允许该操作:请检查服务包状态	服务包已关闭，不能重复操作

#### 返回示例

```
{
  "Code":200,
  "Message":"Success",
  "RequestId":"4e2f63ac-ee1c-489a-a699-9639c2d50967",
  "Status":"Success",
  "Timestamp":"2017-11-16 18:23:56"
}
```

### 38.延长高防防护包期限

#### 描述

延长高防防护包期限，如果提前续费，则在原到期时间上添加相应天数。若延期续费，则从当前时间开始计算，添加相应天数。

#### 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：ExtendProtectPackageDueTime
IPUserID	String	是	IP地址隶属的二级用户ID
PackageID	String	是	防护包ID
LifeDay	Int	是	防护包需要延长的天数，单位（天）

### 返回参数

参数	类型	说明
Due_Time	timestamp	防护包到期时间
PackageID	String	防护包ID，作为防护包唯一标识

### 状态码

Code	Message	说明
9402	指定服务包不存在	服务包不存在，请查看IPUserID或PackageID

### 返回示例

```
{
  "Code": 200,
  "Message": "Success",
  "ProtectPackageInfo": {
    "Due_Time": "2019-01-09T05:33:33Z",
    "PackageID": "855d723a-c9c6-11e7-96a6-50e54919757f"
  },
  "RequestId": "7fcf6aaf-586a-40db-adcf-a7384a956ce1",
  "Status": "Success",
  "Timestamp": "2017-11-17 09:22:51"
}
```

## 39.关闭高防防护包弹性防护

### 描述

关闭高防防护包弹性防护，相应包下的IP弹性防护也关闭

### 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：ClosePackageElasticAntiDDos
IPUserID	String	是	IP地址隶属的二级用户ID
PackageID	String	是	防护包ID

### 返回参数

无

状态码

Code	Message	说明
9402	指定服务包不存在	服务包不存在，请查看IPUserID或PackageID
9403	未处于正确的状态	服务包处于保底或free状态

返回示例

```
{
  "Code":200,
  "Message": "Success",
  "RequestId": "3434a8de-33b2-40df-b133-97c3d2701111",
  "Status": "Success",
  "Timestamp": "2017-11-17 10:43:48"
}
```

40.开启高防防护包弹性防护

描述

开启高防防护包弹性防护，相应包下的IP弹性防护也开启

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：OpenPackageElasticAntiDDos
IPUserID	String	是	IP地址隶属的二级用户ID
PackageID	String	是	防护包ID

返回参数

无

状态码

Code	Message	说明
9402	指定服务包不存在	服务包不存在，请查看IPUserID或PackageID
9403	未处于正确的状态	服务包已处于开启状态

返回示例

```
{
  "Code":200,
  "Message": "Success",
  "RequestId": "3434a8de-33b2-40df-b133-97c3d2701111",
  "Status": "Success",
  "Timestamp": "2017-11-17 10:43:48"
}
```

41.查询普通IP流量信息，状态信息

描述

查询IP在所查询时间内，IP为普通IP时间段内的流量信息，状态信息

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：DescribeNormalIPData
IP	String	是	只支持单个IP，可输入高防IP，普通IP，但返回数据为该IP为普通IP时间段数据
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	类型	说明
IPDataInfo	IPDataInfoDataSet	IPDataInfo信息集合

类型说明

参数	类型	说明
IPDataInfo	IPDataInfoDataSet	IP数据集包含 MonitorData 和MonitorDataMax
MonitorData	MonitorDataDataSet	流量数据，规则参考DescribeIPMonitorData
MonitorDataMax	MonitorDataMaxDataSet	流量峰值数据，规则参考DescribeIPMaxMonitorData

状态码

错误代码	描述	说明
9400	时间参数有错	时间参数错误

返回示例

```
{
  "Code":200,
  "IPDataInfo":
  [
    {
      "MonitorData":
      [
        {
          "KBPS":5505,
          "KBPS_MAX":5505,
          "PPS":8192,
          "PPS_MAX":8192,
          "TimeStamp":"2017-10-27T09:15:00Z"
        },
        {
          "KBPS":944,
          "KBPS_MAX":944,
          "PPS":1000,
          "PPS_MAX":1000,
          "TimeStamp":"2017-10-27T12:30:00Z"
        },
        {
          "KBPS":552,
          "KBPS_MAX":688,
          "PPS":1000,
          "PPS_MAX":1000,
          "TimeStamp":"2017-10-27T13:45:00Z"
        },
        {
          "KBPS":528,
          "KBPS_MAX":528,
          "PPS":1000,
          "PPS_MAX":1000,
          "TimeStamp":"2017-10-28T03:00:00Z"
        }
      ],
      "MonitorDataMax":
      [
        {
          "KBPS":528,
          "KBPS_MAX":528,
          "PPS":1000,
          "PPS_MAX":1000,
          "TimeStamp":"2017-10-28T03:00:00Z"
        }
      ]
    }
  ],
  "Message":"Success",
  "RequestId":"6753f3e4-e480-416f-8749-8e260c8a93da",
  "Status":"Success",
  "Timestamp":"2017-11-22 16:47:59"
}
```

## 42.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
PackageID	String	否	高防包ID，传则显示这个包名下白名单，不传显示用户名下白名单
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
Domain	Bool	否	True显示域名白名单，False显示IP白名单，不传域名IP都显示

/

### 返回参数

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

### 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":
  [
    "test.cc",
    "10.10.10.10",
    "10.1.1.82"
  ]
}
```

## 43.查看普通IP黑洞信息

### 描述

查看普通IP当前黑洞信息

### 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：DescribeNormalIPBlackHoleInfo
IP	String	是	普通IP

返回参数

参数	类型	说明
IPBlackHoleData	IPBlackHoleDataSet	黑洞数据集,“Normal”状态数据都为空

类型说明

参数名	类型	说明
IP	String	IP地址
IPState	String	IP状态，“Normal”为正常，“BlackHole”处于黑洞
Createdt	String	黑洞开始时间，采用UTC时间
Enddt	String	黑洞理论结束时间，如无手工解除的理论结束时间，采用UTC时间
Ban_time	String	黑洞持续时间
Current_value	String	黑洞时的线路值
Threshold_value	String	黑洞阈值
Direction	String	流量方向

错误码

无

状态码

无

返回示例

```
{
  "Code":200,
  "IPBlackHoleData":
  [
    {
      "IP":"125.77.29.221",
      "IPState":"BlackHole",
      "Ban_time":"00:20:00",
      "Createdt": "2017-11-28T04:31:00"
      "Current_value":"130729",
      "Direction":"Incoming ",
      "Enddt":"2017-11-28T04:51:00",
      "Threshold_value":"100000"
    },
    {
      "IP":"125.77.29.256",
      "IPState":"Normal",
      "Ban_time":"",
      "Createdt": ""
      "Current_value":"",
      "Direction":"",
      "Enddt":"",
      "Threshold_value":""
    }
  ],
  "Message": "Success",
  "RequestId": "3c6e2675-3a93-4cf8-abe0-0242b3639f0d",
  "Status": "Success",
  "Timestamp": "2017-11-28 12:42:43"
}
```

## 44.查看普通IP峰值信息与黑洞次数

### 描述

查看普通IP相应时间段内的峰值信息和黑洞次数

### 请求参数

参数名	类型	必选	说明
Action	String	是	系统规定参数，取值：DescribeNormalIPMaxData
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
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
DataSet	IPDataSet	IP黑洞信息数据集

类型说明

参数名	类型	说明
IP	String	IP地址
BlackHoleTimes	Int	查询时间段内黑洞次数
MonitorDataMax	String	峰值数据集
KBPS_MAX	String	查询时间段内，且IP为普通IP时，BPS最大值
PPS_MAX	String	查询时间段内，且IP为普通IP时，PPS最大值
TimeStamp	String	峰值出现时间点

错误码

无

返回示例

```
{
  "Code":200,
  "DataSet":
  [
    {
      "BlackHoleTimes":0,
      "IP":"45.126.122.174",
      "MonitorDataMax":
      {
        "KBPS_MAX":0,
        "PPS_MAX":0,
        "TimeStamp":"2017-10-30T03:00:00Z"
      }
    }
  ],
  "Message":"Success",
  "RequestId":"72b36d8b-4389-4f53-978d-9a44662b5cd6",
  "Status":"Success",
  "Timestamp":"2017-12-08 11:42:06"
}
```