www.IDC4.com

高防IP

海量DDoS清洗接入方式
快速便捷的高防解决方案

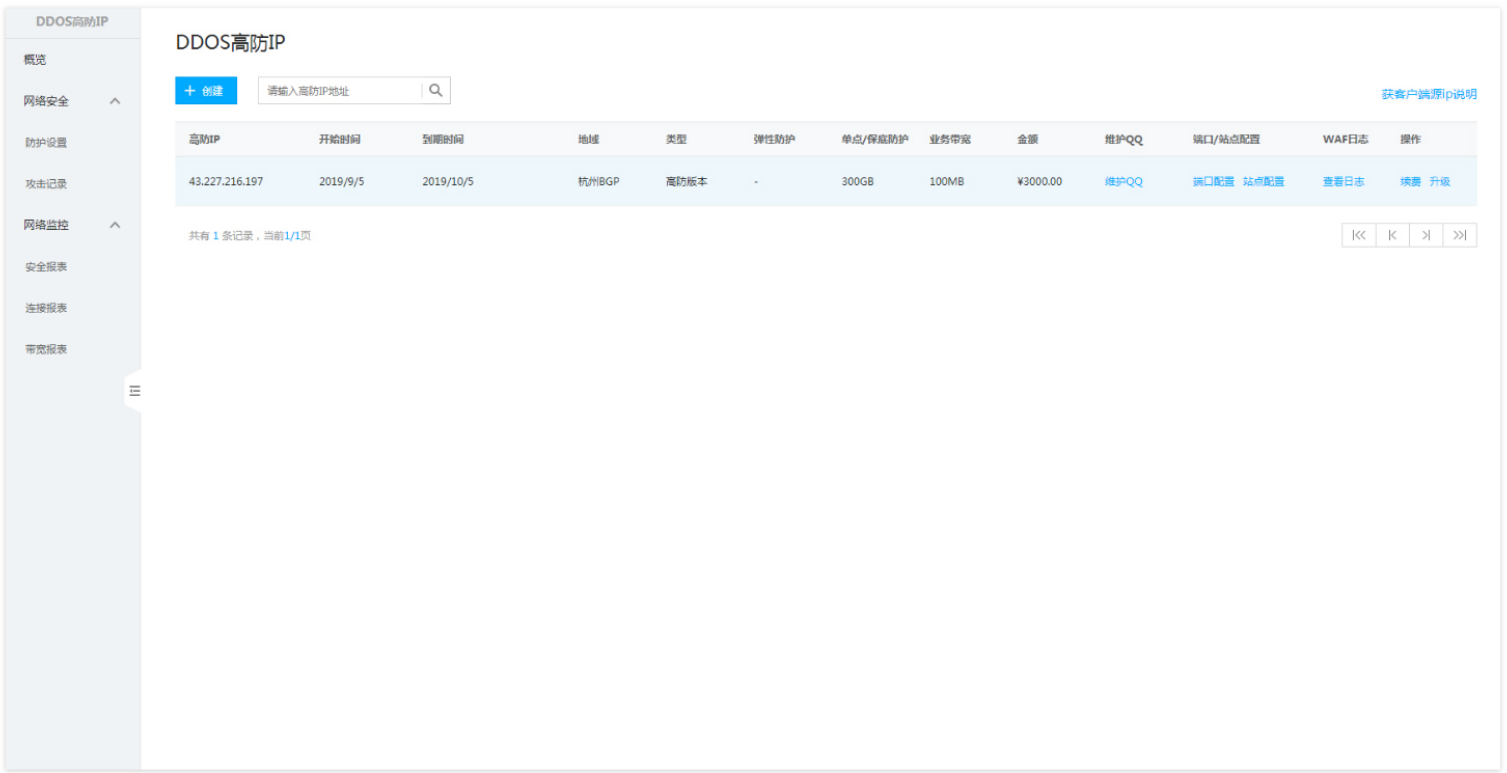
IDC4.COM 德迅

德迅云安全高防IP功能展示

概览

近源清洗多种流量清洗部署方案，无损防御各种DDoS攻击，5s发现恶意请求，10s快速阻断攻击，事前拦截、事后溯源、全方位防黑。

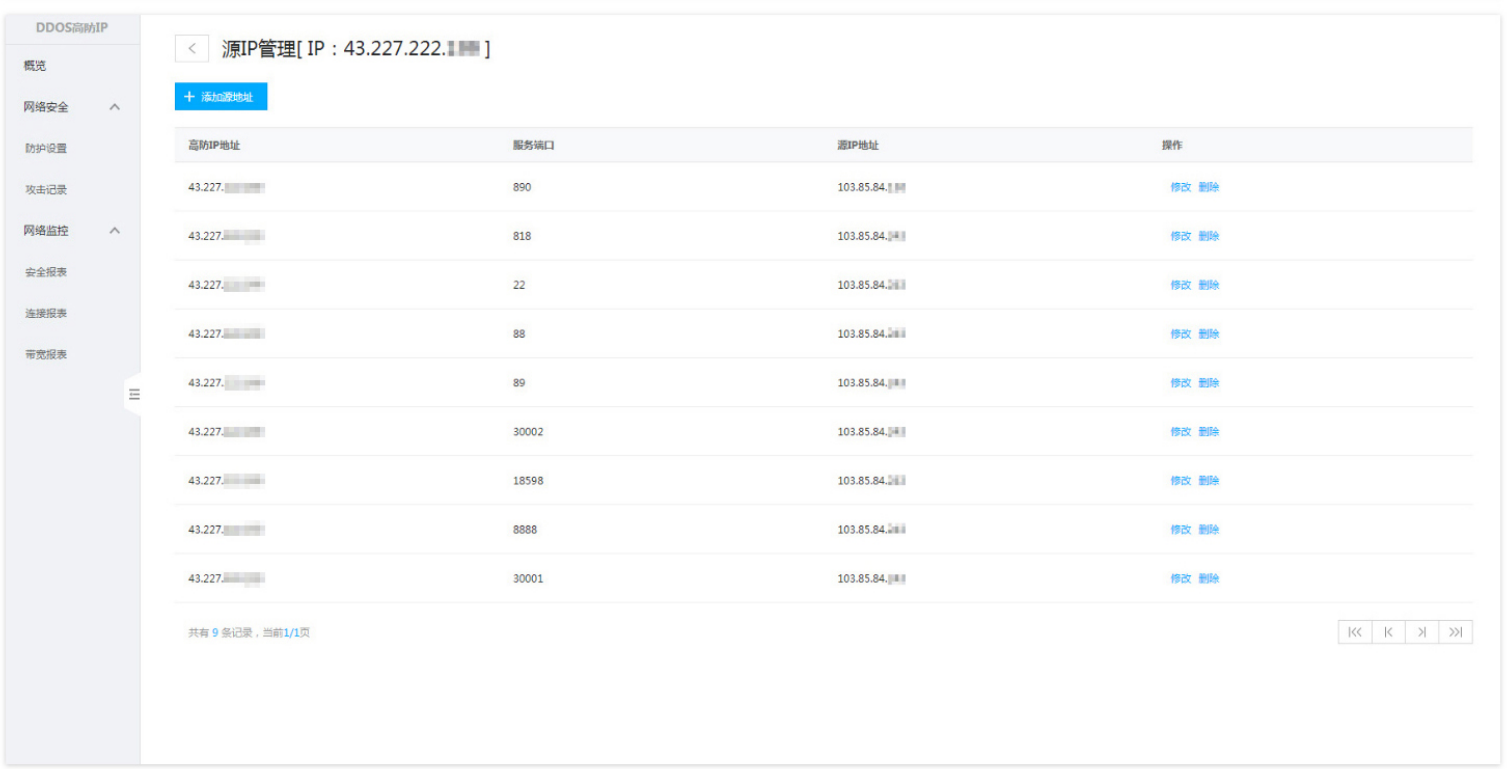
2019-7-18 10:28



源IP设置

可以按指定端口分发,满足单IP多业务模式,为用户提供高质量、低成本的产品。

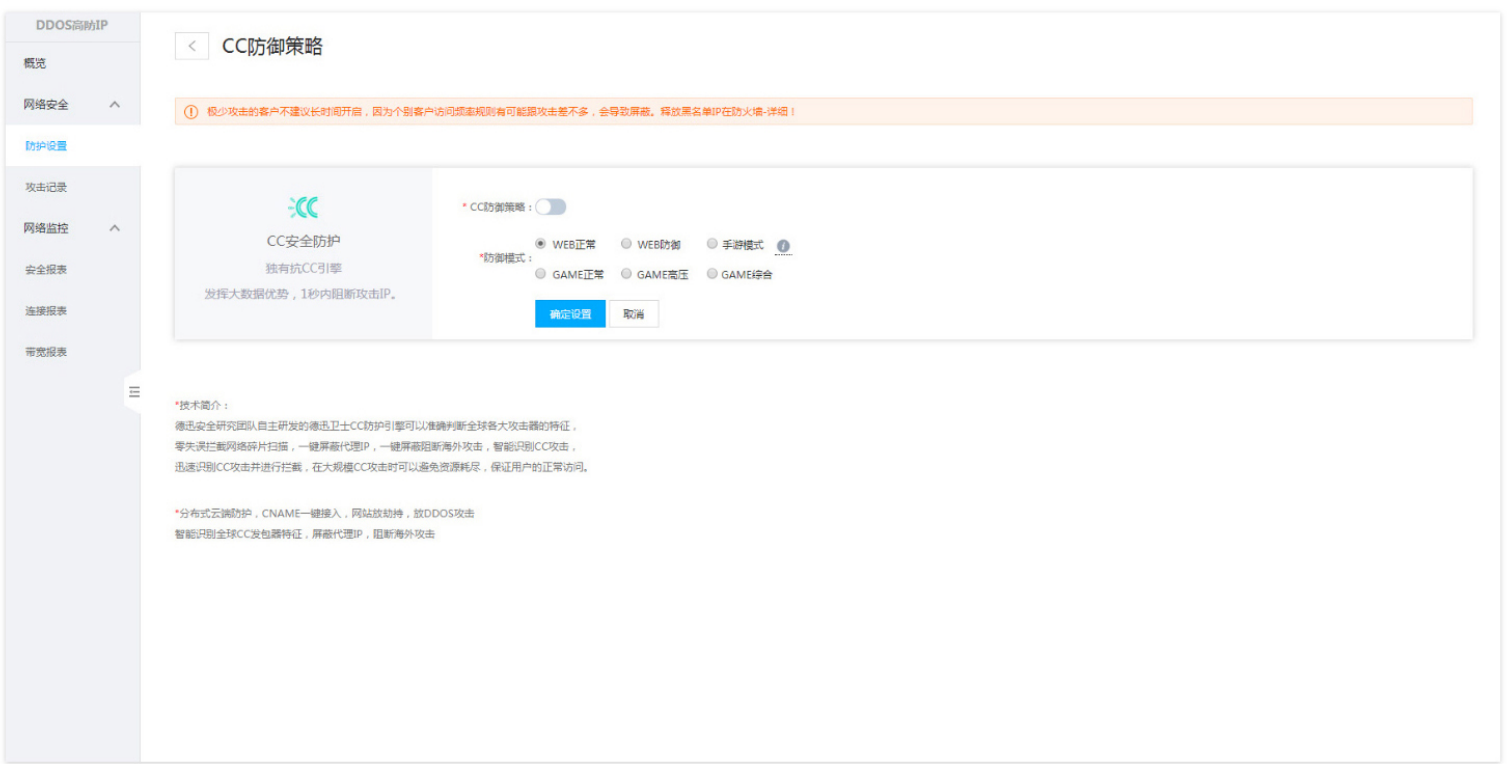
2019-7-18 10:28



防护设置

可自助设置防火墙规则，防护CC不求人。

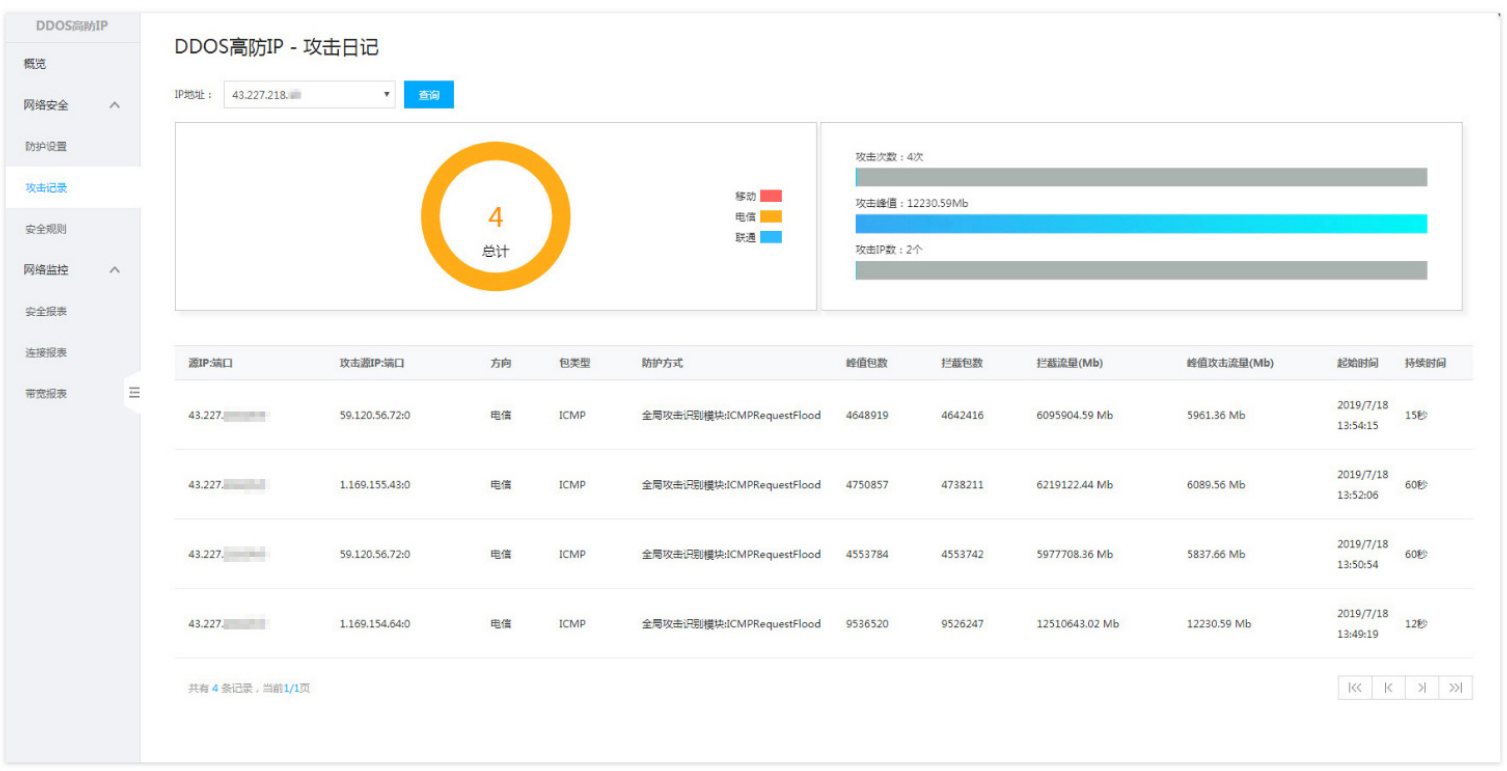
2019-7-18 10:28



攻击记录

可查看服务器被DDOS攻击的记录,攻击类型,攻击大小,攻击时间,攻击源IP。

2019-7-18 10:28



安全情报

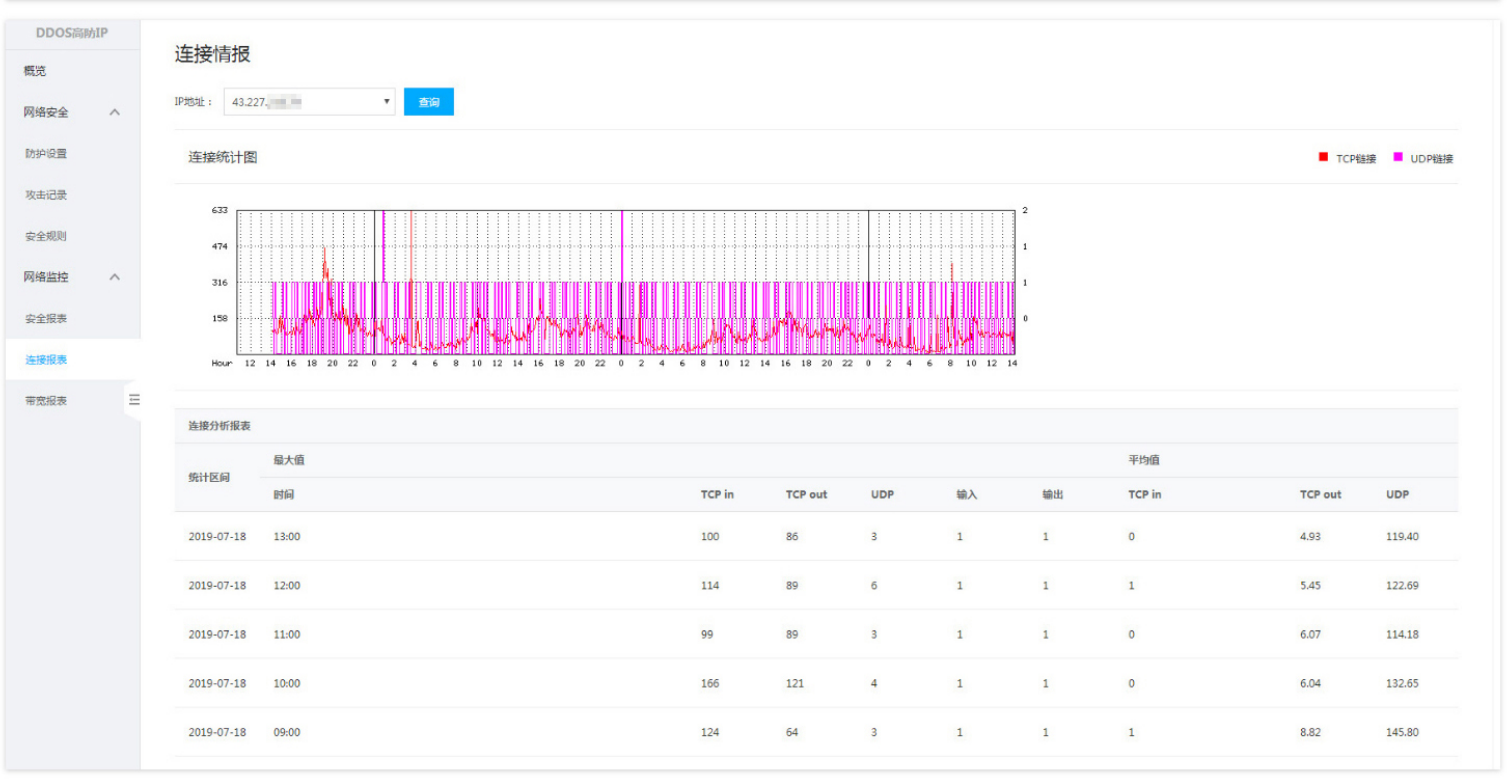
可以详细查看CC攻击连接峰值与占用最大带宽,并且与抛物形图形展示。

2019-7-18 10:28

连接监控

可以详细查看CC攻击连接峰值与占用最大带宽,并且与抛物形图形展示。

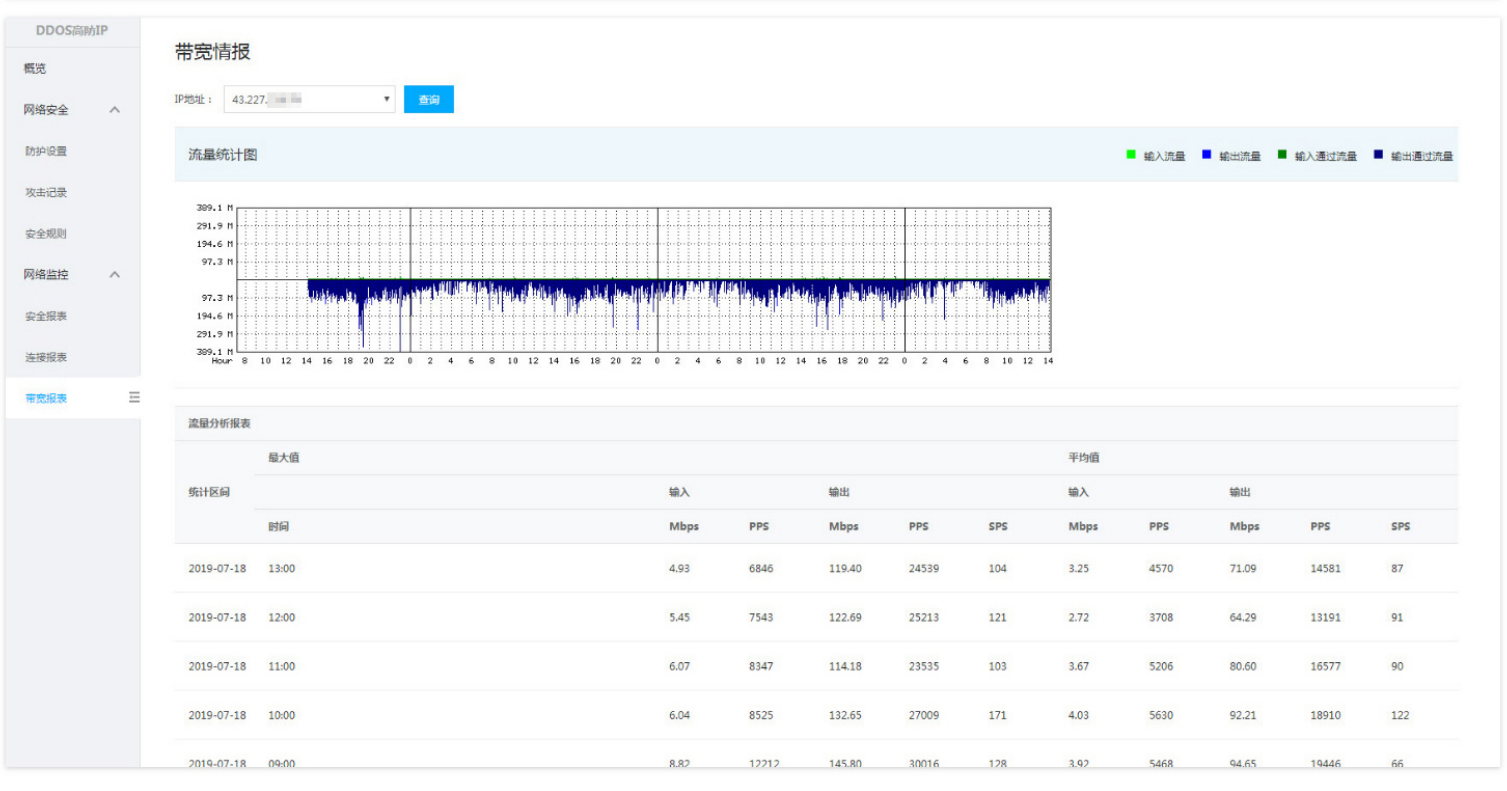
2019-7-18 10:28



带宽监控

可以详细查看CC攻击连接峰值与占用最大带宽,并且与抛物形图形展示。

2019-7-18 10:28



如何在阿里云后台添加高防 IP 白名单

通过设置白名单解决因误判 IP 被拦截问题
若您发现部分正常业务或者 IP 无法访问，有可能是因为攻击误判导致 IP 被拦截,。

背景信息

目前阿里云服务器默认都有一层云盾防护，如有 IP 数据包输送过大，频率过高很容易会被云盾拦截，导致业务运营停止。

我们只要在云盾后台添加高防 IP 白名单，就能解决被云盾误拦截的问题。

操作步骤

打开云盾后台控制面板

地址：https://yundunnext.console.aliyun.com/?p=sc

说明 您也可以在登录阿里云控制台后，将鼠标移至右上角的账户图标打开用户菜单，并单击 **安全管控**，进入云盾安全管控平台管理控制台。

1. 在面板左侧 定位到**白名单管理 > 访问白名单**页面，单击**添加**。
2. 选择对象类型，输入源 IP（非当前云账户名下的 IP），在左侧列表中选择当前云账号名下的对象 IP（例如 ECS 云服务器公网 IP），单击右箭头按钮，将选中的 IP 加入右侧待添加列表，单击**确定**。即将所输入的访问源 IP 加入所添加的对象 IP 的访问白名单，所有来自该源 IP 对于您云账户名下的目标 IP 的访问都将不受任何安全管控限制。
选择对象类型，输入源 IP（非当前云账户名下的 IP），在左侧列表中选择当前云账号名下的对象 IP（例如 ECS 云服务器公网 IP），单击右箭头按钮，将选中的 IP 加入右侧待添加列表，单击**确定**。即将所输入的访问源 IP 加入所添加的对象 IP 的访问白名单，所有来自该源 IP 对于您云账户名下的目标 IP 的访问都将不受任何安全管控限制。

如果您想要放行所有对该对象 IP 的访问，在 **源 IP** 框中输入 0.0.0.0 即可放行所有 IP 对该目标 IP 的访问。


添加
添加0.0.0.0表示放行所有IP
对象类型:
云服务器ECS
* 源IP:
0.0.0.0
选择所有
已选(0 个)
全部选择
输入服务器IP/名称进行搜索
i-bp1iw4hobozjjhv54zuf (
47.11)
i-bp1as iflfe (
121. .105)
i-2zej4i raxwy (
4.126)
afwmie8j (
47.100.
已选(0 个)
全部选择
仅支持IP精确查询
e3k4uafwmie8j (
.145)
«
‹
1
›
»
GO
重置
确定

高防 IP 获取客户端真实 IP

业务请求经过高防 IP 的 4 层转发后，业务服务器端接收到报文后，其看到的源 IP 地址是高防 IP 的出口 IP 地址。为了让服务器端能够获取到用户端实际的 IP 地址，可以使用如下 TOA 的方案。在业务服务的 Linux 服务器上，安装对应的 TOA 内核包，并重启服务器后。业务侧就可以获取到用户端实际的 IP 地址。

TOA 原理

高防转发后，数据包同时会做 SNAT 和 DNAT，数据包的源地址和目标地址均修改。
TCP 协议下，为了将客户端 IP 传给服务器，会将客户端的 IP，port 在转发时放入了自定义的 tcp option 字段。

```
#define TCPOPT_ADDR    200

#define TCPOLEN_ADDR 8    /* |opcode|size|ip+port| = 1 + 1 + 6 */



/*

*insert client ip in tcp option, now only support IPV4,

*must be 4 bytes alignment.

*/

struct ip_vs_tcpo_addr {

__u8 opcode;

__u8 opsize;

__u16 port;

__u32 addr;

};
```

Linux 内核在监听套接字收到三次握手的 ACK 包之后，会从 SYN_REVC 状态进入到 TCP_ESTABLISHED 状态。这时内核会调用 tcp_v4_syn_recv_sock 函数。 Hook 函数 tcp_v4_syn_recv_sock_toa 首先调用原有的 tcp_v4_syn_recv_sock 函数，然后调用 get_toa_data 函数从 TCP OPTION 中提取出 TOA OPTION，并存储在 sk_user_data 字段中。

然后用 inet_getname_toa hook inet_getname，在获取源 IP 地址和端口时，首先调用原来的 inet_getname，然后判断 sk_user_data 是否为空，如果有数据从其中提取真实的 IP 和 port，替换 inet_getname 的返回。

客户端程序在用户态调用 getpeername，返回的 IP 和 port 即为客户端的原始 IP。

内核包安装步骤

Centos 6.x/7.x

安装步骤

下载安装包
(1) Centos 6.x 下载
(2) Centos 7.x 下载

安装包文件

```
Centos 6 安装命令：rpm -hiv kernel-2.6.32-220.23.1.el6.toa.x86_64.rpm --force
```

```
Centos 7 安装命令：rpm -hiv kernel-3.10.0-693.el7.centos.toa.x86_64.rpm --force  如果提示冲突报错安装下面依赖组件

Centos 7 安装依赖组件：yum -y install dracut linux-firmware xfsprogs kmod kexec-tools
```

安装完成之后重启主机

```
reboot
```

执行命令检查 toa 模块是否加载成功

```
lsmod | grep toa
```

没有加载的话手工开启

```
modprobe toa
```

可用下面的命令开启自动加载 toa 模块

```
echo modprobe toa >> /etc/rc.d/rc.local
```

Ubuntu 16.04

下载安装包：
(1) 内核包下载
(2) 内核 header 包下载
安装步骤：

```
dpkg -i linux-image-4.4.87.toa_1.0_amd64.deb
```

Headers 包可不装，如需要做相关开发则安装。
安装完成之后重启主机，然后 `lsmod | grep toa` 检查 toa 模块是否加载 没有加载的话 `modprobe toa` 开启。
可用下面的命令开启加载 toa 模块

```
echo modprobe toa >> /etc/rc.d/rc.local
```

Debian 8

(1) 内核包下载
(2) 内核 header 包下载

安装方法与 Ubuntu 相同。

请根据业务服务器 Linux 操作系统的类型和版本下载对应的内核包，按如下步骤操作。如果没有和用户操作系统一致的内核包，用户还可以参考下面 TOA 源代码安装指引操作。

TOA 源代码内核安装指引

源码安装

下载打好 toa 补丁 的源码包，单击 toa 补丁即可下载安装包。

解压。

编辑 .config，将 `CONFIG_IPV6=M` 改成 `CONFIG_IPV6=y`。

如果需要加上一些自定义说明，， 可以编辑 Makefile。

make -jn (n 为线程数)。

`make modules_install`。

`make install`。

修改 /boot/grub/menu.lst 将 default 改为新安装的内核（title 顺序从 0 开始）。

Reboot 重启后即为 toa 内核。

`lsmode | grep toa` 检查 toa 模块是否加载 没有加载的话 `modprobe toa` 开启。