DDoS 防护

故障处理

腾讯云

文档目录

故障处理

配置安全组阻止入站后，仍遭受到 DDoS 攻击

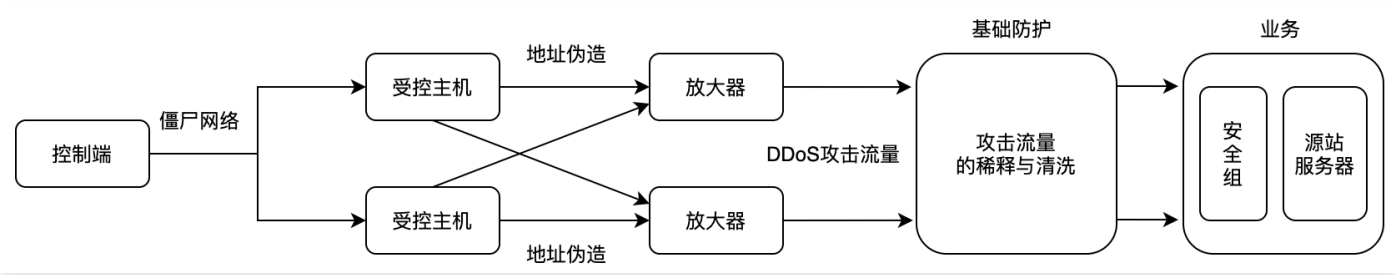
最近更新时间：2024-04-18 15:48:53

现象描述

配置了安全组规则阻止入站后，业务仍遭受到 DDoS 攻击。

可能原因

常见 DDoS 攻击方法包括：攻击网络和带宽资源、攻击系统资源、攻击应用资源等方式。
常见攻击流程如下图所示：



1. 控制端通过僵尸网络等方式控制大量主机，通过放大、反射等方式构造大量 DDoS 流量攻击服务器。
2. 云业务服务提供商会提供一定攻击流量稀释与清洗的 基础防护 。
3. 用户进行安全组的入站策略等配置，只能达到基于 IP 和端口的防护，此时经过基础防护若不能完全将攻击流量进行稀释与清洗，攻击者仍可以达到利用 DDoS 攻击流量占用网络和带宽资源等目的。

解决思路

购买 DDoS 高防包或 DDoS 高防 IP，获得更强的防护能力，抵御大流量 DDoS 攻击。

处理步骤

DDoS 高防包、DDoS 高防 IP 购买方法请参见 购买指引 。

> **说明**
> - 防护对象：
  - DDoS 高防包只针对腾讯云内的用户提供 DDoS 防护能力。
  - DDoS 高防 IP 面向云内外用户，支持网站域名和业务端口接入防护。
- 接入：
  - DDoS 高防包的接入配置更加便捷，无需变更公网 IP 地址。
  - DDoS 高防 IP 需修改 DNS 解析或修改业务 IP 后才能接入防护。

详情请参见 DDoS 防护解决方案对比 。

公网 IP 遭遇 DDoS 攻击

最近更新时间：2023-07-21 10:53:03

现象描述

业务遭受 DDoS 大流量攻击，消耗目标服务器性能/网络带宽，造成服务器无法正常提供服务。

可能原因

用户 IP 遭受的攻击大小，超过了腾讯云赠送的基础防护能力。

解决思路

- **更换公网 IP（攻击停止时，临时方案）**
  攻击者发起 DDoS 攻击是针对具体业务 IP，通过临时更换 IP，只能临时规避被封堵的问题，无法根本解决，攻击者可能随时针对新 IP 发起第二次攻击，产生二次影响。
- **购买高防产品（推荐方案）**
  通过购买 DDoS 高防产品，提升 IP 的防护能力，抵御大流量攻击，如攻击流量超过了高防包所在地域的能力，可按需选择更大防护能力的高防 IP 产品。

处理步骤

更换公网 IP（攻击停止时，临时方案）

更换公网 IP 相关限制如下：

- 单个账号单个地域不超过3次/天。
- 单台实例仅允许更换1次公网 IP。
- 更换后原公网 IP 将被释放。

更换操作详情，请参见 更换公网 IP 地址 。

购买配置高防产品（推荐方案）

- 购买并配置 DDoS 高防包、 DDoS 高防 IP 请参见 购买指引 和 快速入门 。
- DDoS 高防包和 DDoS 高防 IP 的对比，请参见 DDoS 防护解决方案对比 。

业务被大流量攻击导致封堵

最近更新时间：2024-04-18 15:48:53

现象描述

业务被大流量攻击导致 IP 封堵，业务无法访问。

可能原因

- 超过防护流量阈值，导致被封堵。
- 攻击还在持续，无法进行自动解封。

解决思路

- DDoS基础防护：默认情况下，封堵2~24小时后自动解封（具体封堵时长，请以实际封堵时长为准）。
- DDoS 高防用户每天拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

如解封次数用完：

- 未购买 DDoS 高防包的客户，建议用户购买高防包，首次绑定设备可进行解封。
- 已购买 DDoS 高防包的客户，建议客户升级防护套餐，可提前解除封堵。

处理步骤

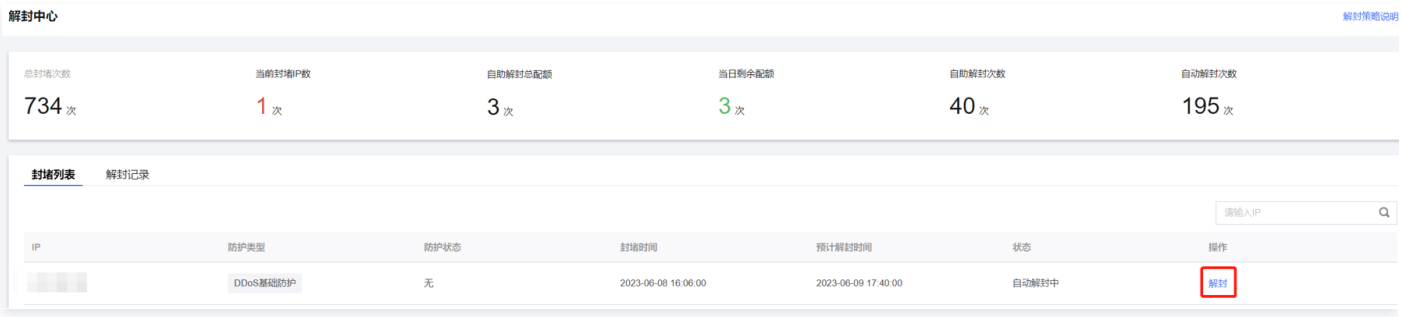
1. 登录 DDoS 防护（新版）控制台，在左侧导航中，选择**解封中心**页面，查看自助解封剩余次数。
   - 若自助解封剩余次数为0，则跳转到 步骤5，或等待自动解封。
   - 若自助解封剩余次数不为0，则跳转到 步骤2。

> **说明：**
> 自动解封时间，请参考 DDoS 防护（新版）控制台 自助解封 > 近期安全事件页面的“预计解封时间”项。

2. 查看攻击是否已停止，请选择防护概览查看。
   - 若是，则跳转到 步骤3。
   - 若否，待攻击停止时，继续执行解封操作，执行 步骤3。

> **说明：**
> 攻击如果持续进行未停止，则无法进行解封，需等待攻击结束自助解封或自动解封。

3. 在左侧导航中，选择**解封中心**，进入解封操作页面。
4. 在解封操作页面，找到状态为“自动解封中”的防护 IP，在右侧操作栏中，单击**解封**。



5. 不同 DDoS 防护产品的用户，对应建议如下：
   - 如果是 DDoS 基础防护用户，建议用户购买高防包（支持防护地域：广州、上海和北京），首次绑定设备 可进行解封。
   - 如果是 DDoS 高防用户，建议用户升级防护套餐（增加防护次数或防护 IP 数），可提前解除封堵。

DDoS 攻击未达到阈值业务 IP 被封堵

最近更新时间：2024-04-18 15:48:53

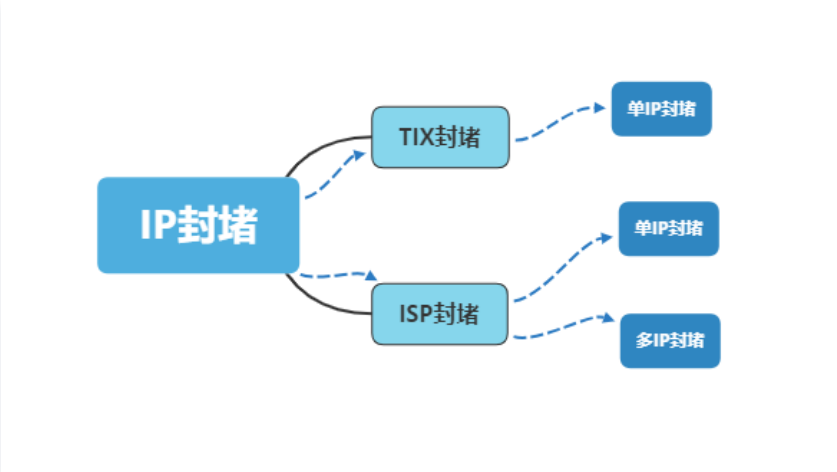
现象描述

攻击流量没有达到购买封堵阈值，但 IP 被封堵。

可能原因

已购买 DDoS 高防包，所有出网口的攻击流量总和未达到购买阈值便进行封堵。 计算方式：所有出网口的攻击流量与购买阈值对比。

1. 根据封堵的节点位置分为两种封堵。
   - TIX 封堵：为腾讯的出口网关进行封堵，封堵的阈值是可调控的。
   - ISP 封堵：为运营商封堵，封堵的阈值基本固定的。
2. 在 ISP 封堵的情况下分为两种方式封堵。
   - 单 IP 封堵：当一个 IP 的流量达到某个出口单 IP 封堵阈值（根据出口带宽设置）时封堵。
   - 多 IP 封堵：当某个检测区间 IDC 的总流量（攻击流量 + 业务流量）超过多 IP 封堵阈值。



解决思路

等待攻击结束后进行自助解封或者自动解封。

处理步骤

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择**自助解封**页面，查看自助解封剩余次数。
   - 若自助解封剩余次数为0，则跳转到 步骤5，或等待自动解封。
   - 若自助解封剩余次数不为0，则跳转到 步骤2。

> **说明：**
> 自动解封时间，请参考控制台 解封中心 页面的“预计解封时间”项。

2. 查看攻击是否已停止，请选择 防护概览 查看。
   - 若是，则跳转到 步骤3。
   - 若否，待攻击停止时，继续执行解封操作，执行 步骤3。

> **说明：**
> 攻击如果持续进行未停止，则无法进行解封，需等待攻击结束自助解封或自动解封。

3. 在左侧导航中，选择**解封中心**，进入解封操作页面。
4. 在解封操作页面，找到状态为“自动解封中”的防护 IP，在右侧操作栏中，单击**解封**。

5. 不同 DDoS 防护产品的用户，对应建议如下：
   - 如果是 DDoS 基础防护用户，建议用户购买高防包（支持防护地域：广州、上海和北京），首次绑定设备 可进行解封。
   - 如果是 DDoS 高防用户，建议用户升级防护套餐（增加防护次数或防护 IP 数），可提前解除封堵。

使用高防 IP，业务访问出现502报错

最近更新时间：2024-04-18 15:48:53

现象描述

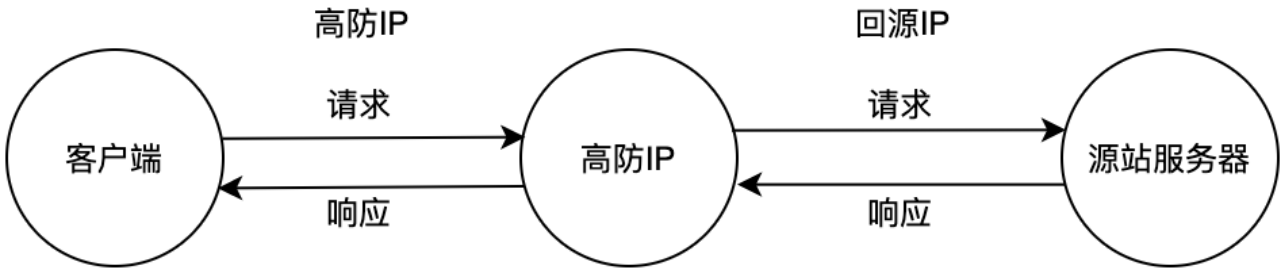
使用高防 IP 之后，访问业务出现502报错：Bad Gateway，如图所示：

502 Bad Gateway

nginx/1.18.0

可能原因

使用高防 IP 后的业务流量走向图：



原因一：回源 IP 被源站拦截或限速

在配置高防 IP 后，源站服务器的 IP 被高防 IP 在中间代理而被隐藏。所有经过高防 IP 服务访问的客户端源 IP 都会变成高防 IP 的回源 IP。源站服务器接收到的访问请求都是来自高防 IP 回源段，而高防 IP 回源段的 IP 数量有限，分摊过后每个回源 IP 访问源站服务器的请求量较大。

若源站服务器配置了 DDoS 攻击等相关安全防护策略，将有机率触发 DDoS 防护策略，导致将回源 IP 限速甚至拦截。

原因二：源站本身异常，导致响应高防的请求超时

导致异常的可能原因：

1. 在使用高防 IP 之前，源站 IP 暴露，被恶意攻击导致故障。
2. 源站服务器机房物理故障。
3. 服务器内存、CPU 占用过高，导致性能降低。
4. 源站服务器中 Apache、Nginx 等 Web 程序异常。
5. 公网转发至源站服务器间链路出现故障。

原因三：网络抖动或者链路故障

公网网络质量不佳造成的业务访问不稳定，提示502报错。

解决思路

原因一：解决思路

通过腾讯云拨测平台对源站 IP 和高防 IP 进行拨测，对比源站 IP 和高防 IP 的访问情况，拨测方式可以参考 腾讯云拨测使用说明。
如源站 IP 正常、高防 IP 大范围异常，则可以判断为高防回源 IP 被源站服务器拦截或限速导致，建议进行高防回源IP加白操作。

详细处理步骤请参见 原因一：处理步骤。

原因二：解决思路

通过将本地主机的解析结果修改为源站来验证源站本身是否正常，首先修改本地 hosts 文件，确认 hosts 绑定已经生效之后，使用域名进行验证源站是否可以正常访问，如不能正常访问，可以尝试做如下处理：

1. 源站 IP 保护。详情步骤请参见 处理措施1。
2. 请相关人员进行机房故障检查，修复物理故障。详情步骤请参见 处理措施2。
3. 确认 Web 服务是否正常并修复。详情步骤请参见 处理措施3。
4. 检查服务器进程占用，内存占用等性能参数是否正常并恢复至正常状态。详情步骤请参见 处理措施4。
5. 查看网络层面进行排查或者源站链路监控设备监控到的链路状态，也可通过更换链路测试进行验证与规避。详情步骤请参见 处理措施5。

详细处理步骤请参见 原因二：处理步骤。

原因三：解决思路

确定是否存在链路故障情况并联系网络服务商进行修复。

详细处理步骤请参见 原因三：处理步骤。

处理步骤

原因一：处理步骤

将高防 IP 回源段添加至防火墙、主机安全防护软件的白名单中进行放行，下面以 CentOS 6.5 操作系统的防火墙添加白名单为例：

1. 执行如下命令，查看 Linux 防火墙的状态。

```
service iptables status
```

如果控制台提示 Chain INPUT、Chain FORWARD 以及 Chain OUTPUT 项下没有任何规则条目，说明防火墙还未开启。

service iptables status

```
[root@localhost /]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

2. 执行如下命令，查看防火墙配置文件。

```
cat /etc/sysconfig/iptables
```

根据业务需求，确保防火墙没有额外的黑白名单设置后，将防火墙开启，防止直接打开防火墙之后对业务造成影响。

3. 执行如下命令，开启防火墙。

```
service iptables start
```

service iptables start

```
[root@localhost /]# service iptables start
iptables: Applying firewall rules:                         [  OK  ]
```

4. 执行如下命令，再次查看防火墙状态。

```
service iptables status
```

如果控制台提示 Chain INPUT、Chain FORWARD 以及 Chain OUTPUT 任意项显示规则条目，证明防火墙已经打开。

```
[root@localhost /]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,
ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp
dpt:22
5    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with ic
mp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with ic
mp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

5. 执行如下命令，设置 IP 白名单，将回源 IP 段加入防火墙白名单中。

```
Iptables -A INPUT -s 回源IP -j ACCEPT
```

6. 执行如下命令，查看添加的白名单策略，是否成功添加到了防火墙配置中。

```
iptables -nL --line-number
```

如果看到添加的防火墙规则在输出内容内，则代表添加成功。

7. 执行如下命令，保存防火墙配置。

```
service iptables save
```

```
[root@localhost /]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

8. 执行如下命令，重启防火墙，使配置生效。

```
service iptables restart
```

```
[root@localhost /]# service iptables restart
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

原因二：处理步骤

将本地主机的解析结果修改为源站，来验证源站本身是否正常，首先修改本地 hosts 文件，具体操作如下：

1. 修改本地hosts文件，使本地对业务高防域名的请求到达源站 IP，下面以 Windows 操作系统为例，配置本地 hosts 文件：
   打开本地计算机 `C:\Windows\System32\drivers\etc` 路径下的 hosts 文件，在文末添加如下内容：

   ```
   <源站 IP 地址> <被防护网站的域名>
   ```

   例如源站 IP 为10.1.1.1，域名为 `www.qqq.com` ，则添加：

   ```
   10.1.1.1        www.qqq.com
   ```

   保存 hosts 文件，在本地计算机对被防护的域名运行 ping 命令。
   当解析到的 IP 地址是 hosts 文件中绑定的源站 IP 地址时，说明本地 hosts 生效。若没有解析到源站 IP，在 Windows 的命令提示符中运行 `ipconfig /flushdns` 命令，刷新本地的 DNS 缓存。
2. 确认 hosts 绑定已经生效之后，使用域名进行验证：源站是否可以正常访问，如不能正常访问，针对可能原因对应做如下处理。

处理措施1：源站 IP 保护

查看源站流量、请求量是否有大量增长，同时对比高防 IP 管理控制台中的监控。服务器本身流量监控以 CentOS 系统为例，具体操作如下：

1. 常见 Linux 服务器网络流量使用情况可以使用 iftop 进行查看：

   ```
   执行命令：iftop [-i interface]（参数 -i 后跟的 interface 表示网络接口名，如 eth0、eth1 ）
   ```

输出如下：

```
                 25.0Kb            50.0Kb            75.0Kb            100Kb        125Kb
n1m7l3ilyinf41          => 1[redacted]                    97.3Kb  34.1Kb  29.7Kb
                        <=                                18.9Kb  16.2Kb  32.5Kb
n1m7l3ilyinf41          => 1[redacted]                    8.70Kb  8.06Kb  8.07Kb
                        <=                                8.41Kb  7.73Kb  8.67Kb
n1m7l3ilyinf41          => 1[redacted]                    1.55Kb  1.55Kb  1.55Kb
                        <=                                9.50Kb  9.50Kb  9.50Kb
n1m7l3ilyinf41          => 2[redacted]                    1.48Kb  1.66Kb  1.94Kb
                        <=                                 160b    160b    178b
n1m7l3ilyinf41          => 1[redacted]                     0b     194b    242b
                        <=                                 0b     110b    138b

TX:             cumm:   279KB   peak:   109Kb          rates:   109Kb  45.6Kb  41.5Kb
RX:                     310KB           206Kb                   37.0Kb  33.7Kb  50.9Kb
TOTAL:                  589KB           311Kb                   146Kb   79.3Kb  92.5Kb
```

回显结果说明：

- 第一行：带宽使用情况显示。
- 中间部分为外部连接列表，即记录了哪些 IP 正在和本机的网络连接。
- 中间部分靠右侧部分是实时流量信息，分别是该访问 IP 连接到本机2秒、10秒和40秒的平均流量。
- => 代表发送数据，<= 代表接收数据 。
- 底部三行：
  - 第一列：TX 表示发送流量，RX 表示接收流量，TOTAL 表示总流量。
  - 第二列 cumm：表示第一列各种情况的总流量。
  - 第三列 peak：表示第一列各种情况的流量峰值。
  - 第四列 rates：表示第一列各种情况2秒、10秒、40秒内的平均流量。

2. 查看高防 IP 管理控制台的业务流量监控，参考 防护概览（总览）。
   如果源站遭到大流量攻击，但高防IP管理控制台显示无异常，则有可能是攻击绕过高防IP直接攻击源站。此种源 IP 暴露的处理方法参考 源站 IP 暴露的解决方法。

处理措施2：请相关人员进行机房故障检查，修复物理故障

对服务器硬件状态进行自查：查看源站服务器机房是否出现断电、网卡、 驱动、内存以及接线等物理硬件故障情况，及时更新或修复。

处理措施3：确认 Web 服务是否正常并修复

查看源站服务器的相关监控，CPU/内存的使用率、带宽的使用率等情况。

> **说明：**
> - 通常情况下 CPU 或者内存的使用率长时间超过90%，即可判断为状态异常。
> - 带宽使用需要对比业务正常时期业务进程占用情况，查看是否有明显增长，可以参照 云服务器带宽使用率过高。

如有异常，进一步处理请您联系相关的技术人员或机房负责人员协助排查问题。

处理措施4：检查服务器进程占用，内存占用等性能参数是否正常并恢复至正常状态

对服务器 Web 程序状态进行自查：使用 `ps -C nginx -o pid` 命令查看服务器 nginx 进程是否正常运行。
如有异常需要联系服务器技术人员，针对源站服务器中 Apache、Nginx 等服务进行修复至业务正常状态水平。

处理措施5：查看网络层面进行排查或者源站链路监控设备监控到的链路状态，也可通过更换链路测试进行验证与规避

对公网网络至源站服务器间链路质量，链路连通情况，中间网络设备转发情况等全面进行自查，确保此段链路连通性正常。

原因三：处理步骤

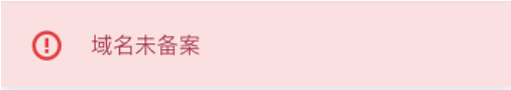
通过腾讯云拨测平台中的站点质量监控对源站 IP 和高防 IP 分别进行公网网络质量的检测和监控。监控方式可以参考 腾讯云拨测使用说明。
如果有公网网络质量不佳的情况，进一步需要联系所属运营商进行反馈处理。

域名接入高防 IP，提示未备案

最近更新时间：2024-04-23 14:52:01

现象描述

域名接入高防 IP，提示未备案。



可能原因

域名未在工信部备案

根据国务院令第292号《互联网信息服务管理办法》和《非经营性互联网信息服务备案管理办法》规定，国家对经营性互联网信息服务实行许可制度，对非经营性互联网信息服务实行备案制度。未获取许可或者未履行备案手续的，不得从事互联网信息服务，否则属于违法行为。

因此，所有对中国大陆境内提供服务的网站都必须先进行 ICP 备案，备案成功并获取通信管理局下发的 ICP 备案号后，才能开通访问。

备案信息未及时同步

若您接入域名已经在工信部备案成功，接入高防 IP 时提示域名未备案，可能是因为工信部备案信息还未同步腾讯云 ICP 备案系统。

处理步骤

域名未在工信部备案

您可以使用腾讯云 ICP 备案系统进行备案，备案成功并获取通信管理局下发的 ICP 备案号后，即可使用域名接入高防 IP。详情请参见：备案概述。

> **说明：**
> 若您在其他备案接入商进行备案，详情请咨询您的备案接入商。

备案信息未及时同步

备案完成后，一般工信部信息同步以及腾讯云备案管理系统的信息拉取均需要一定周期，请您等待24小时后再进行接入。