DDoS 防护

快速入门

腾讯云

文档目录

快速入门
DDoS 高防包

最近更新时间：2024-12-20 19:11:43

DDoS 高防包为腾讯云公网 IP 提供更高的 DDoS 防护能力，可支持防护 CVM、CLB、NAT、WAF 等产品和服务。DDoS 高防包接入便捷，无需变更业务 IP，可快速完成防护配置。

前提条件

在绑定防护 IP 前，您需要成功购买 DDoS 高防包（标准版） 或 DDoS 高防包（轻量版）。

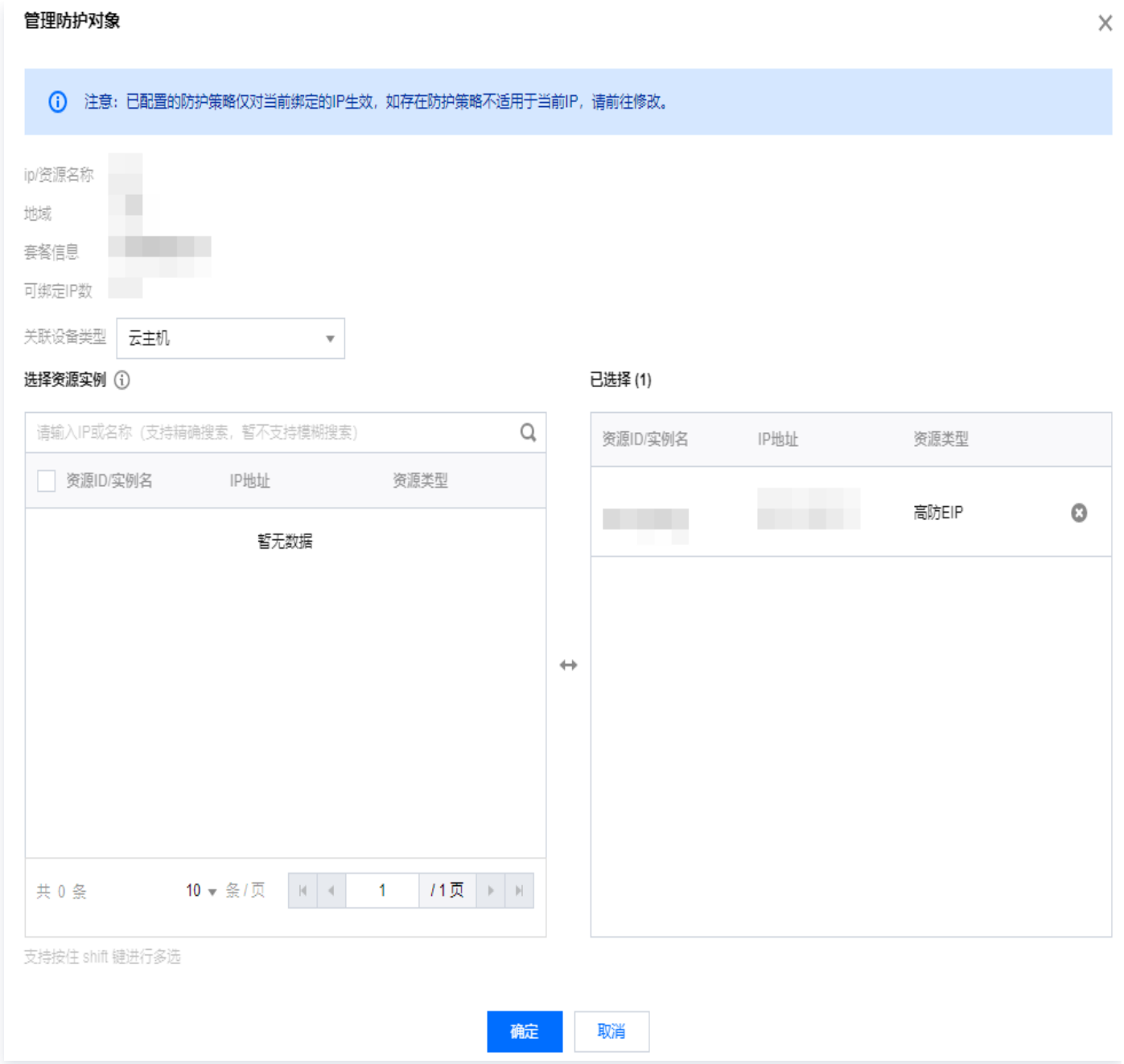
操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航中，单击**云上防护实例**。
2. 在云上防护实例页面，选择目标实例，单击操作列的**管理防护对象**。

3. 在管理防护对象窗口中，根据实际防护需求选择“关联设备类型”及“资源实例”。

> **说明：**
> DDoS 高防包支持托管 IP，目前在白名单开放使用中。如用户使用腾讯云的托管 IP，需要接入 DDoS 高防包，请致电4009100100转1（工作日9:00am - 6:00pm）进行咨询，或 提交工单 申请使用。

- 关联设备类型：支持云主机，负载均衡，Web 应用防火墙等公有云具有公网 IP 的资源。
- 选择资源实例：允许多选，“选择资源实例”数量不得超过可绑定 IP 数。



4. 选择完成后，单击**确定**即可。

> **说明：**
> 接入完成后，如需个性化防护可在 防护配置页面 进行个性化配置，详情请参见 防护配置 文档。

DDoS 高防 IP
网站业务接入

最近更新时间：2024-04-25 09:26:21

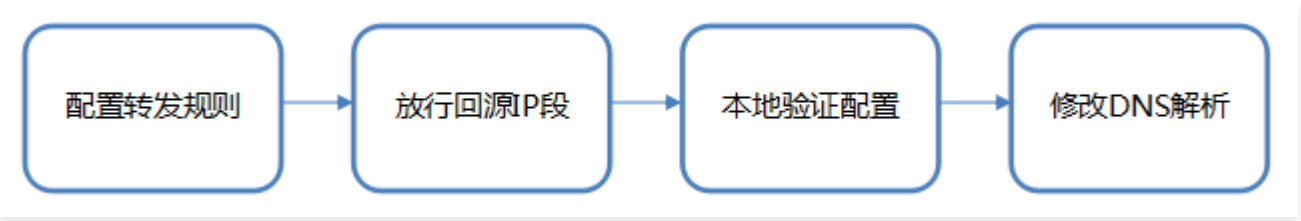
本文档介绍了网站类业务用户将业务接入 DDoS 高防 IP 实例并验证转发配置的详细操作步骤。

> **说明：**
> 网站业务接入和非网站业务接入操作步骤一致，区别在于 本地验证配置 不同。

前提条件

- 在添加转发规则前，您需要成功购买 中国大陆 DDoS 高防 IP 实例 或 境外 DDoS 高防 IP 实例 。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品，例如腾讯云的 DNSPod 。

操作流程



操作步骤

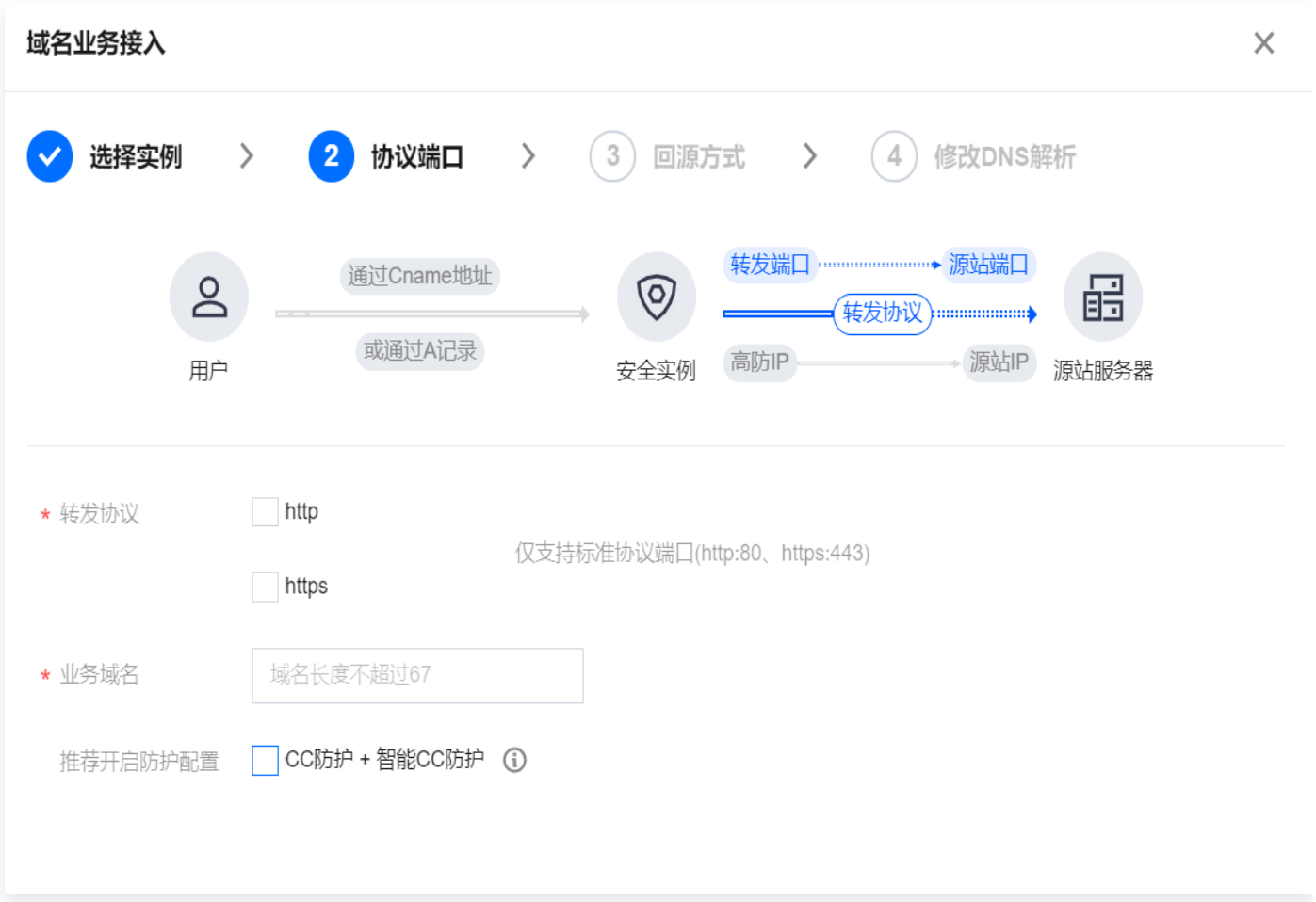
配置转发规则

1. 登录 DDoS 防护（新版）控制台，在左侧目录中，单击**业务接入** > **域名接入**。
2. 在域名接入页面，单击**开始接入**。

3. 在域名业务接入页面，选择关联实例 ID，单击**下一步：协议端口**。

> **说明：**
> 支持多选，多实例同步接入。

4. 选择转发协议和证书，填写业务域名，单击**下一步：回源方式**。



5. 选择回源方式，填写源站 IP+端口或源站域名。单击**下一步：修改 DNS 解析**。

说明：

- 备用源站：当源站转发异常会自动切换转发至备用源站。
- 仅支持标准协议端口 `(http:80、https:443)` 。
- 支持泛域名。

6. 单击**完成**，即可完成接入规则。

说明：

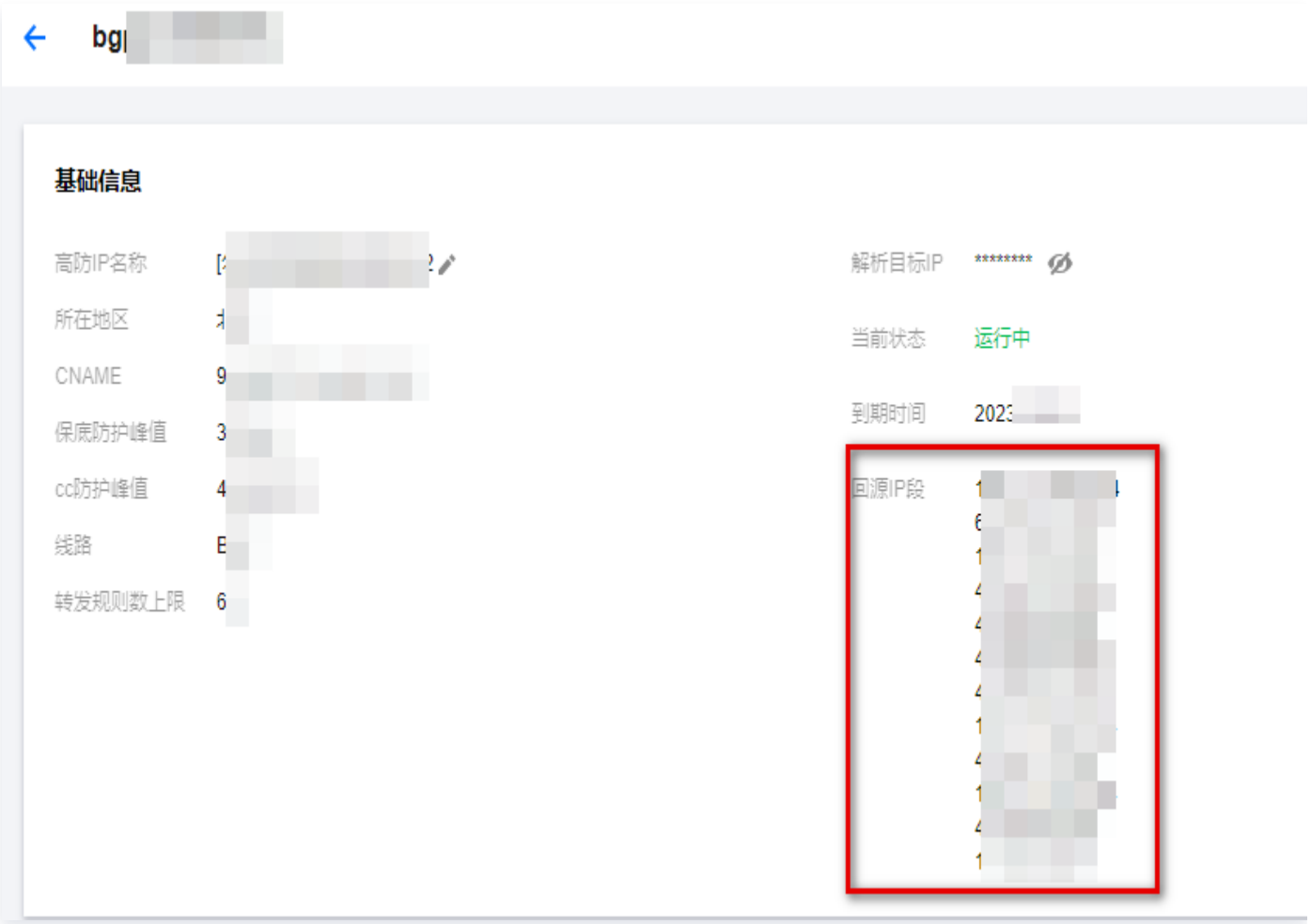
接入完成后，如需个性化防护可在 防护配置页面 进行个性化配置，详情请参见 防护配置 文档。

放行回源 IP 段

为了避免源站拦截 DDoS 高防 IP 的回源 IP 而影响业务，建议在源站的防火墙、Web 应用防火墙、IPS 入侵防护系统、流量管理等硬件设备上设置白名单策略，将源站的主机防火墙和其他任何安全类的软件（如安全狗等）的防护功能关闭或设置白名单策略，确保高防的回源 IP 不受源站安全策略的影响。

1. 登录 DDoS 防护（新版）控制台，在左侧导航中，单击**云上防护实例**。
2. 在云上防护实例页面，选择目标实例，单击操作列的**实例 ID**。

3. 在基本信息页面，查看回源 IP 段。



本地验证配置

转发配置完成后，DDoS 高防 IP 实例的高防 IP 将按照转发规则将相关端口的报文转发到源站的对应端口。为了最大程度保证业务的稳定，建议在全面切换业务之前先进行本地测试。具体的验证方法如下：

1. 修改本地 hosts 文件，使本地对于被防护站点的请求经过高防。下面以 Windows 操作系统为配置本地 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：

```
<高防 IP 地址> <被防护网站的域名>
```

2. 例如高防 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 文件中绑定的高防 IP 地址时，说明本地 hosts 生效。

> **说明：**
> 若解析到的 IP 地址依然是源站地址，可尝试在 Windows 的命令提示符中运行 `ipconfig /flushdns` 命令刷新本地的 DNS 缓存。

3. 确认 hosts 绑定已经生效后，使用域名进行验证。若能正常访问则说明配置已经生效。

> **说明：**
> 若使用正确的方法显示验证失败，请登录 DDoS 高防 IP 控制台检查配置是否正确。排除配置错误和验证方法不正确后，若问题依然存在，请 提交工单 联系我们协助。

修改 DNS 解析

如需修改 DNS 解析，请参见 配置智能调度 文档的修改 DNS 解析进行操作。

> **注意：**
> 高防资源将提供 CNAME，请将 DNS 解析地址修改为该 CNAME 高防资源。CNAME 解析目的高防 IP 将不定期更换。（不涉及三网资源）。

非网站业务接入

最近更新时间：2024-04-18 16:01:21

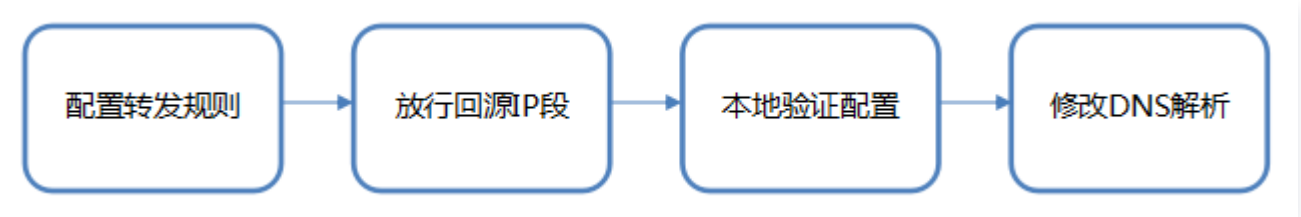
本文档介绍了非网站类业务用户如何将业务接入 DDoS 高防 IP 实例并验证转发配置。

> **说明：**
> 非网站业务接入和网站业务接入操作步骤一致，区别在于 本地验证配置 不同。

前提条件

- 在添加转发规则前，您需要成功购买 中国大陆 DDoS 高防 IP 实例 或 境外 DDoS 高防 IP 实例 。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品，例如腾讯云的 DNSPod 。

操作流程



操作步骤

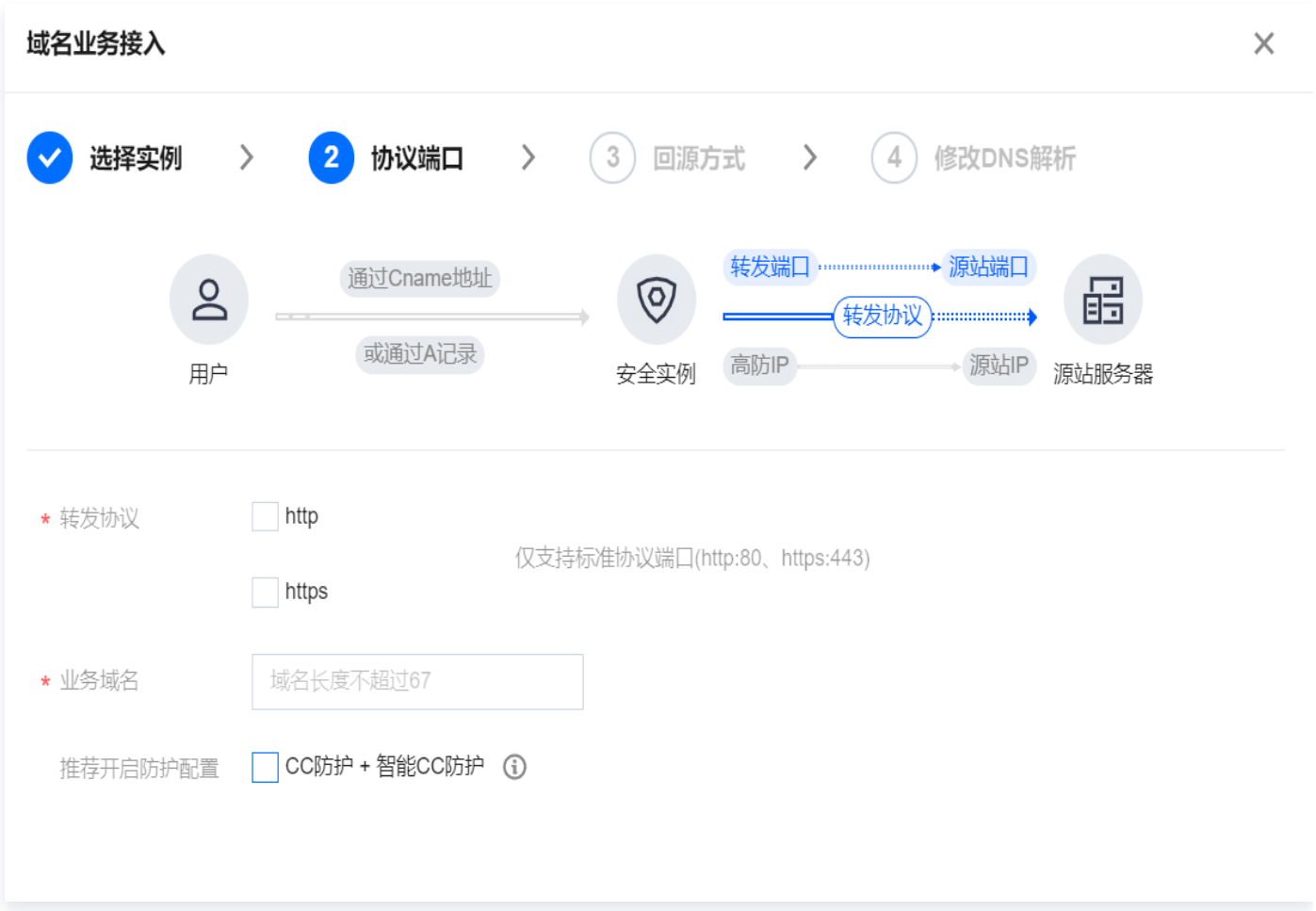
配置转发规则

1. 登录 DDoS 防护（新版）控制台，在左侧目录中，单击**业务接入 > 域名接入**。
2. 在域名接入页面，单击**开始接入**。

3. 在域名业务接入页面，选择关联实例 ID，单击**下一步：协议端口**。

> **说明：**
> 支持多选，多实例同步接入。

4. 选择转发协议和证书，填写业务域名，单击**下一步：回源方式**。



5. 选择回源方式，填写源站 IP+端口或源站域名。单击**下一步：修改 DNS 解析**。

说明：

- 备用源站：当源站转发异常会自动切换转发至备用源站。
- 支持泛域名。

6. 单击**完成**，即可完成接入规则。

说明：

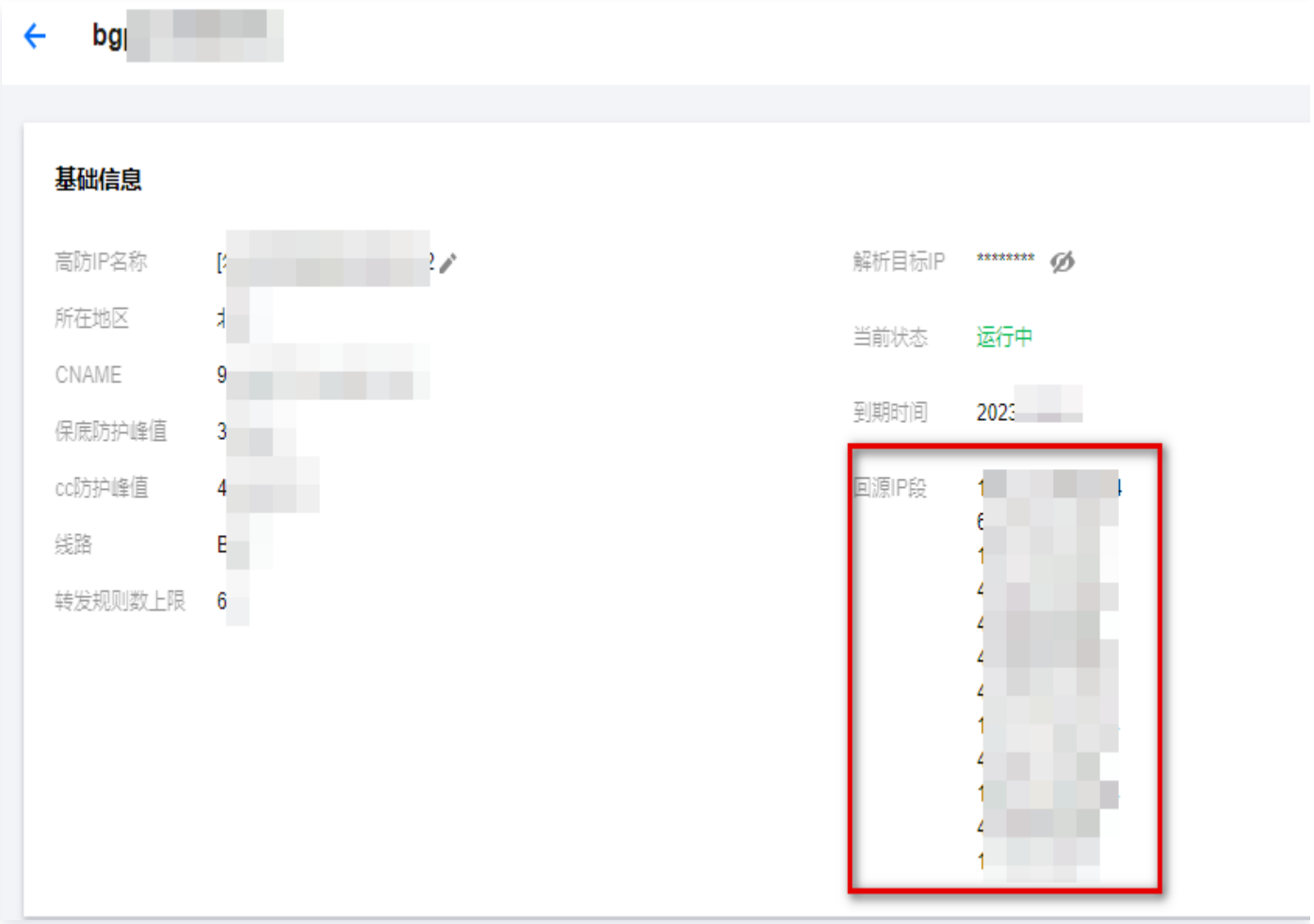
接入完成后，如需个性化防护可在防护配置页面进行个性化配置，详情请参见 防护配置 文档。

放行回源 IP 段

为了避免源站拦截 DDoS 高防 IP 的回源 IP 而影响业务，建议在源站的防火墙、Web 应用防火墙、IPS 入侵防护系统、流量管理等硬件设备上设置白名单策略，将源站的主机防火墙和其他任何安全类的软件（如安全狗等）的防护功能关闭或设置白名单策略，确保高防的回源 IP 不受源站安全策略的影响。

1. 登录 DDoS 防护（新版）控制台，在左侧导航中，单击**云上防护实例**。
2. 在云上防护实例页面，选择目标实例，单击操作列的**实例 ID**。

3. 在基本信息页面，查看回源 IP 段。



本地验证配置

转发配置完成后，DDoS 高防 IP 实例的高防 IP 将按照转发规则将相关端口的报文转发到源站的对应端口。为了最大程度保证业务的稳定，建议在全面切换业务之前先进行本地测试。具体的验证方法如下：

- **使用 IP 访问的业务**

  对于直接通过 IP 进行交互的业务（如游戏业务），可通过 telnet 命令访问高防 IP 端口，查看是否能连通。若能在本地客户端直接填写服务器 IP，则直接填入高防 IP 进行测试，查看本地客户端是否可以正常连接。
  例如高防 IP 为10.1.1.1，转发端口为1234，源站 IP 为10.2.2.2，源站端口为1234。本地通过telnet命令访问10.1.1.1:1234，telnet命令能连通则说明转发成功。

- **使用域名访问的业务**

  对于需要通过域名访问的业务，可通过修改本地 hosts 来验证配置是否生效。

1. 修改本地 hosts 文件，使本地对于被防护站点的请求经过高防。下面以 Windows 操作系统为配置本地 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：

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

   例如高防 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 文件中绑定的高防 IP 地址时，说明本地 hosts 生效。

   > **说明：**
   > 若解析到的 IP 地址依然是源站地址，可尝试在 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 绑定已经生效后，使用域名进行验证。若能正常访问则说明配置已经生效。

   > **说明：**
   > 若使用正确的方法显示验证失败，请登录 DDoS 高防 IP 控制台检查配置是否正确。排除配置错误和验证方法不正确后，若问题依然存在，请 提交工单 联系我们协助。

修改 DNS 解析

如需修改 DNS 解析，请参见 配置智能调度 文档的修改 DNS 解析进行操作。

> **注意：**
> 高防资源将提供 CNAME，请将 DNS 解析地址修改为该 CNAME 高防资源。CNAME 解析目的高防 IP 将不定期更换。（不涉及三网资源）。

DDoS 高防 IP（境外企业版）

最近更新时间：2024-04-18 16:01:21

DDoS 高防 IP（境外企业版）是针对业务部署在腾讯云内境外地区的用户，以提升 DDoS 境外防护能力的付费产品。

- DDoS 高防 IP（境外企业版）可以独立购买和持有的公网 IP 地址资源。
- DDoS 高防 IP（境外企业版）绑定云资源后，云资源可以通过 DDoS 高防 IP（境外企业版）与公网通信。

本文以 DDoS 高防 IP（境外企业版）关联云资源为例介绍 DDoS 高防 IP（境外企业版）的使用生命周期。

背景信息

DDoS 高防 IP（境外企业版）的使用生命周期包括购买 DDoS 高防 IP（境外企业版）、DDoS 高防 IP（境外企业版）实例配置防护规则、DDoS 高防 IP（境外企业版）配置业务规则，DDoS 高防 IP（境外企业版）销毁。

1. 购买 DDoS 高防 IP（境外企业版）：根据实际使用需求，购买 DDoS 高防 IP（境外企业版）资源。
2. DDoS 高防 IP（境外企业版）实例 配置防护规则：配置贴合业务的防护策略。
3. DDoS 高防 IP（境外企业版）配置业务规则：将 DDoS 高防 IP（境外企业版）的实例关联到需防护的云上资源。
4. DDoS 高防 IP（境外企业版）销毁：将 DDoS 高防 IP（境外企业版）与云资源取消关联后，您可以将该 DDoS 高防 IP（境外企业版）与其他云资源关联。取消关联操作可能会导致对应云资源的网络不通，且未绑定云资源的 DDoS 高防 IP（境外企业版）会产生 IP 资源费。

操作步骤

购买 DDoS高防IP（境外企业版）

1. 登录 DDoS 高防 IP（境外企业版）控制台。
2. 参考上文 购买指引 进行套餐购买。
3. 单击控制台**云上防护实例**，即可查看已购买的 DDoS 高防 IP（境外企业版），此时处于未绑定状态。

> **说明：**
> 建议您及时为处于未绑定状态的 DDoS 高防 IP（境外企业版）绑定云资源，节省 IP 资源费。IP 资源费按小时计费，精确到秒级，不足一小时，按闲置时间占比收取费用，因此请及时绑定云资源。详细标准可参考 计费概述 。

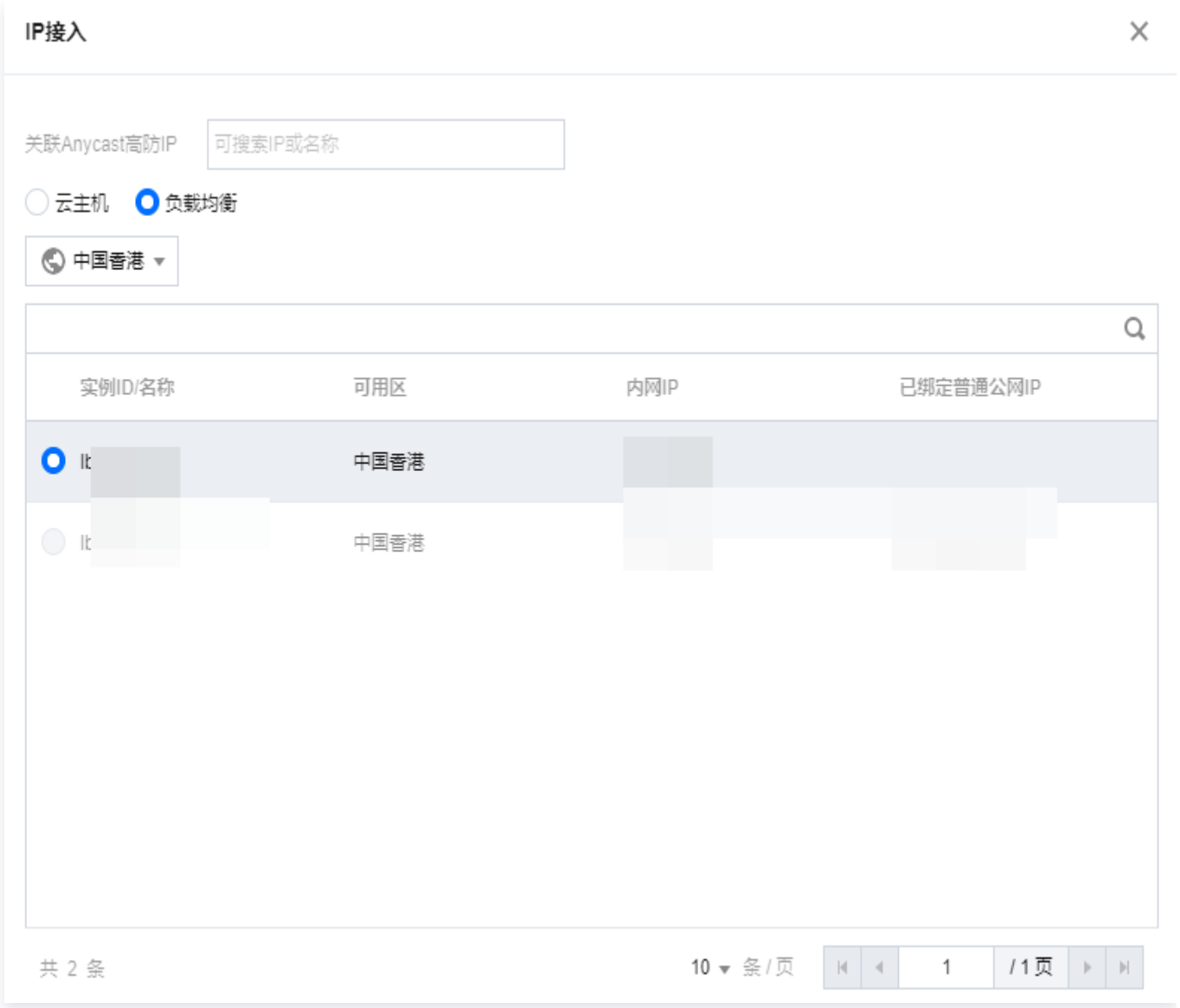
配置防护规则

1. 登录 DDoS 防护（新版）控制台，在左侧导航中，单击**云上防护实例**。
2. 选择对应 DDoS 高防 IP（境外企业版）实例，单击**防护配置**，配置方式可参考 配置防护规则 。

关联云资源

1. 登录 DDoS 防护（新版）控制台，单击**业务接入 > IP 接入**。
2. 在 IP 接入页面，单击**开始接入**。
3. 在 IP 接入页面，“关联 Anycast 高防 IP”处选择 DDoS 高防 IP（境外企业版）实例，单击**确定**，即可完成与云资源的绑定。

> **说明：**
> 已绑定公网 IP 或 Anycast IP 的资源不能重复绑定。



解除云资源绑定

1. 在 IP接入页面，选择所需实例，单击操作列的**删除**。

2. 在解除绑定弹窗中，单击**确定**，即可取消关联。

> **注意：**
> 解除绑定可能导致您的云资源网络不通，请谨慎操作。解绑后，您可以将该资源绑定其他云资源。