

DDoS 防护 快速入门



腾讯云

【 版权声明 】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

快速入门

DDoS 高防包

DDoS 高防 IP

网站业务接入

非网站业务接入

DDoS 高防 IP (境外企业版)

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。

管理防护对象
✕

注意：已配置的防护策略仅对当前绑定的IP生效，如存在防护策略不适用于当前IP，请前往修改。

ip/资源名称

地域

套餐信息

可绑定IP数

关联设备类型 云主机

选择资源实例 ⓘ

请输入IP或名称 (支持精确搜索, 暂不支持模糊搜索)

<input type="checkbox"/> 资源ID/实例名	IP地址	资源类型
暂无数据		

共 0 条 10 条 / 页

已选择 (1)

资源ID/实例名	IP地址	资源类型
		高防EIP ✕

确定
取消

支持按住 shift 键进行多选

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。

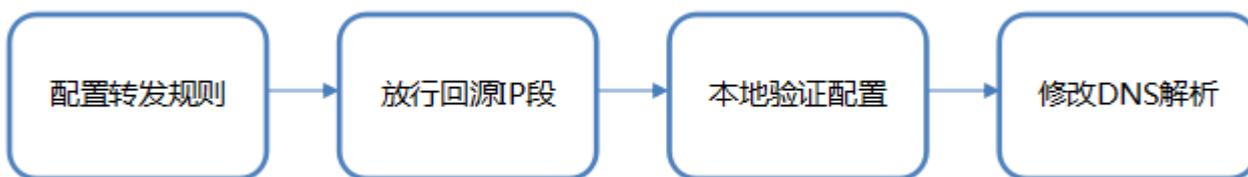
说明：

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

- 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**。
- 在域名接入页面，单击**开始接入**。



- 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。

域名业务接入 ×

1 选择实例 > 2 协议端口 > 3 回源方式 > 4 修改DNS解析

用户 通过Cname地址 安全实例 转发端口 源站端口
或通过A记录 转发协议 源站服务器
高防IP 源站IP

* 关联实例ID

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。

域名业务接入 ×

✓ 选择实例 > 2 协议端口 > 3 回源方式 > 4 修改DNS解析

用户 通过Cname地址 安全实例 转发端口 源站端口
或通过A记录 转发协议 源站服务器
高防IP 源站IP

* 转发协议 http 仅支持标准协议端口(http:80、https:443)
 https

* 业务域名

推荐开启防护配置 CC防护 + 智能CC防护 ⓘ

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。

域名业务接入
✕

✓ 选择实例 >
✓ 协议端口 >
3 回源方式 >
④ 修改DNS解析

用户 → (通过Cname地址 / 或通过A记录) → 安全实例 → (转发端口 ↔ 源站端口) / (转发协议) → 源站服务器

高防IP ↔ 源站IP

* 回源方式

IP回源

域名回源

回源方式：清洗后的干净业务流量可通过IP、域名两种方式访问源站服务器

* 源站IP+端口

源站IP	源站端口
<input style="width: 90%;" type="text" value="示例：1.1.1.1, 请根据实际源站填写"/>	<input style="width: 90%;" type="text" value="示例：80"/> 删除
+ 添加	

注意：请输入源站IP+端口，最多支持16个

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**。

实例ID/名称/标签	实例类型	IP协议	接入资源	业务规格	防护规格	操作
	DDoS高防IP	IPv4	CNAME:	线路: 业务带: 弹性业务带宽:	保底峰值: 弹性峰值: CC峰值: 4	防护配置 升级 续费
	DDoS高防IP	IPv4	CNAME:	线路: B 业务带宽: 弹性业务带宽:	保底峰值: 弹性峰值: CC峰值: 4	防护配置 升级 续费

3. 在基本信息页面，查看回源 IP 段。

← bgi

基础信息

高防IP名称		解析目标IP	*****
所在地区		当前状态	运行中
CNAME	9	到期时间	2023
保底防护峰值	3	回源IP段 	
cc防护峰值	4		
线路	E		
转发规则数上限	6		

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.qq.com`，则添加：

```
10.1.1.1 www.qq.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。

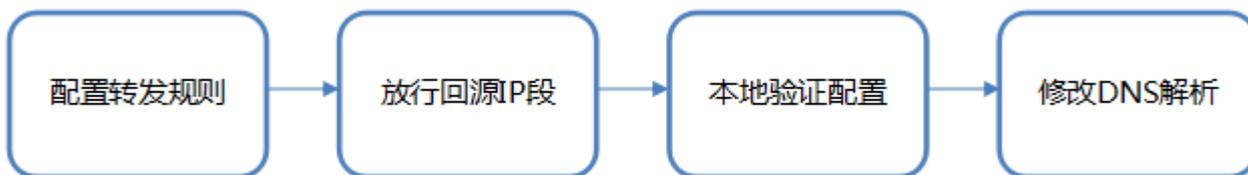
说明：

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

- 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**。
- 在域名接入页面，单击**开始接入**。



- 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。

域名业务接入 ✕

1 选择实例 > 2 协议端口 > 3 回源方式 > 4 修改DNS解析

用户 通过Cname地址 安全实例 转发端口 源站端口
或通过A记录 转发协议 源站服务器
高防IP 源站IP

* 关联实例ID b[redacted]

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。

域名业务接入 ✕

✓ 选择实例 > 2 协议端口 > 3 回源方式 > 4 修改DNS解析

用户 通过Cname地址 安全实例 转发端口 源站端口
或通过A记录 转发协议 源站服务器
高防IP 源站IP

* 转发协议 http 仅支持标准协议端口(http:80、https:443)
 https

* 业务域名 域名长度不超过67

推荐开启防护配置 CC防护 + 智能CC防护 ⓘ

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。

域名业务接入
✕

✓ 选择实例 >
 ✓ 协议端口 >
 3 回源方式 >
 4 修改DNS解析

用户

通过Cname地址
或通过A记录

安全实例

转发端口 ↔ 源站端口

转发协议

高防IP ↔ 源站IP

源站服务器

* 回源方式

IP回源

域名回源

回源方式：清洗后的干净业务流量可通过IP、域名两种方式访问源站服务器

* 源站IP+端口

源站IP	源站端口
<input style="width: 90%;" type="text" value="示例：1.1.1.1, 请根据实际源站填写"/>	<input style="width: 90%;" type="text" value="示例：80"/> 删除
+ 添加	

注意：请输入源站IP+端口，最多支持16个

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**。

实例ID/名称/标签	实例类型	IP协议	接入资源	业务规格	防护规格	操作
	DDoS高防IP	IPv4	CNAME:	线路: 业务带: 弹性业务带宽:	保底峰值: 弹性峰值: CC峰值: 4	防护配置 升级 续费
	DDoS高防IP	IPv4	CNAME:	线路: B 业务带宽: 弹性业务带宽:	保底峰值: 弹性峰值: CC峰值: 4	防护配置 升级 续费

3. 在基本信息页面，查看回源 IP 段。

← bgi

基础信息

<p>高防IP名称: </p> <p>所在地区: </p> <p>CNAME: </p> <p>保底防护峰值: 3</p> <p>cc防护峰值: 4</p> <p>线路: E</p> <p>转发规则数上限: 6</p>	<p>解析目标IP: </p> <p>当前状态: 运行中</p> <p>到期时间: 2023-</p> <p>回源IP段: </p>
---	---

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.qq.com`，则添加：

```
10.1.1.1 www.qq.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。

① 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。

① 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

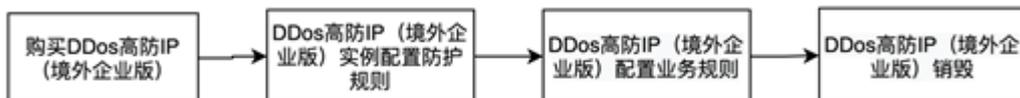
DDoS 高防 IP（境外企业版）是针对业务部署在腾讯云内境外地区的用户，以提升 DDoS 境外防护能力的付费产品。

- 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](#)。

ID/名称/标签	IP协议	高防IP	业务规格	防护规格	运行状态	最近7天攻击	日期	自动续费	操作
未命名 / 无	IPv4		线路: Anycast 业务带宽上限: 100Mbps 套餐信息: 企业版	防护次数: 无限次 防护能力: 全力防护	防护状态: 运行中 绑定状态: 已绑定	0次	购买时间: 2022-02-21 到期时间: 2022-05-21	<input type="checkbox"/>	防护配置 查看报表
未命名 / 无	IPv4		线路: Anycast 业务带宽上限: 100Mbps 套餐信息: 企业版	防护次数: 无限次 防护能力: 全力防护	防护状态: 运行中 绑定状态: 已绑定	0次	购买时间: 2022-01-27 到期时间: 2024-04-27	<input type="checkbox"/>	防护配置 查看报表

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](#)。

ID/名称/标签	IP协议	高防IP	业务规格	防护规格	运行状态	最近7天攻击	日期	自动续费	操作
未命名 / 无	IPv4		线路: Anycast 业务带宽上限: 100Mbps 套餐信息: 企业版	防护次数: 无限次 防护能力: 全力防护	防护状态: 运行中 绑定状态: 已绑定	0次	购买时间: 2022-02-21 到期时间: 2022-05-21	<input type="checkbox"/>	防护配置 查看报表
未命名 / 无	IPv4		线路: Anycast 业务带宽上限: 100Mbps 套餐信息: 企业版	防护次数: 无限次 防护能力: 全力防护	防护状态: 运行中 绑定状态: 已绑定	0次	购买时间: 2022-01-27 到期时间: 2024-04-27	<input type="checkbox"/>	防护配置 查看报表

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。

IP接入 ✕

关联Anycast高防IP

云主机 负载均衡

实例ID/名称	可用区	内网IP	已绑定普通公网IP
<input checked="" type="radio"/> lt-xxxx	中国香港	10.10.10.10	10.10.10.10
<input type="radio"/> lt-xxxx	中国香港	10.10.10.10	10.10.10.10

共 2 条 10 条 / 页

解绑云资源绑定

1. 在 IP接入页面，选择所需实例，单击操作列的删除。

实例ID名称	Anycast高防IP	防护资源类型	防护资源ID名称	防护状态	绑定状态	修改时间	操作
bgpip-C-xxxx	xxxx	xxxx	xxxx	运行中	已绑定	2022-02-21 15:26:31	删除
bgpip-C-xxxx	xxxx	xxxx	xxxx	运行中	已绑定	2022-01-27 19:38:29	删除
bgpip-C-xxxx	xxxx	xxxx	xxxx	运行中	已绑定	2022-01-14 14:48:07	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。

