

宙斯盾安全防护

产品简介

产品文档



腾讯云

【版权声明】

©2013-2020 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。

文档目录

产品简介

宙斯盾安全防护概述

DDoS 高防 IP

DDoS 高防包

产品简介

宙斯盾安全防护概述

最近更新时间：2020-04-17 10:23:02

产品简介

腾讯云宙斯盾安全防护（Aegis Anti-DDoS）基于腾讯海量业务十余年安全技术的积累，为业务提供多层次全方位、高性价比的应对 DDoS 攻击威胁的防护方案，能够对各类网络攻击流量进行精准清洗，并将正常业务流量回送到业务服务器，防止 DDoS 攻击造成业务波动、服务中断、用户体验劣化等问题。同时，宙斯盾安全防护具备 T 级防护资源和专属防护集群，并可通过自定义高级安全策略，对特定攻击行为进行针对性防护。

产品划分

宙斯盾安全防护产品划分：需要付费的 [DDoS高防IP](#)、[DDoS高防包](#)；可免费配置的自定义高级安全策略：[DDoS防护高级策略](#)、[HTTP CC防护高级策略](#)、[水印防护](#)。

产品定价

宙斯盾安全防护产品为组合定价，包年包月预付费 + 按天按量后付费进行组合付费。保底防护峰值为包月预付费，弹性防护峰值和业务转发流量为按量后付费，按日结算。腾讯云宙斯盾安全防护产品定价，详情请参见：

- [DDoS 高防 IP 单 IP 定价](#)
- [DDoS 高防 IP 套餐定价](#)
- [DDoS 高防包单 IP 定价](#)
- [DDoS 高防包多 IP 定价](#)

使用方式

腾讯云宙斯盾安全防护是基于 Web 的用户界面（即控制台）的服务，如果您已注册腾讯云账户，您就可以直接登录 [Aegis Anti-DDoS 控制台](#)，进行选购操作。

相关概念

使用 Aegis Anti-DDoS 时，您有可能会涉及到以下概念：

- **DDoS**

分布式拒绝服务攻击（Distributed Denial-of-Service）的首字母缩写，即利用网络资源向特定目标服务器发起服务请求，通过耗尽目标服务器的带宽或其他资源来使正常用户的服务请求无法完成的网络攻击手法。

- **IP 封堵**

当 DDoS 攻击流量超过用户设置的防护峰值时，安全防护系统会在一段时间内屏蔽被攻击目标服务器的所有请求服务。

- **BGP 网络**

使用边界网关协议（Border Gateway Protocol，BGP）与互联网 AS 直接互联的网络类型。腾讯云 BGP 链路对接了 28 家运营商，能够消除跨网时延的困扰，为您提供优质的网络访问体验。

- **三网网络**

电信、联通、移动的非 BGP 网络。提供静态 IP 资源，非本网用户需要跨网访问。

- **转发规则**

配置规则实现业务请求先访问高防 IP 的服务端口，然后转发到源站服务器 IP 地址的源站端口。可以配置端口转发规则，并支持按权重或按最小连接数进行源站轮询。

- **回源出口 IP 地址**

业务请求从高防 IP 转发到源站服务器时使用的出口 IP 地址。源站服务器如果配置了相关的安全策略，需要将源站出口 IP 地址加入到白名单，以免误判为攻击。

- **防护峰值**

分为保底防护峰值和弹性防护峰值。如果选配了弹性防护峰值，则防护峰值为能够防护攻击的最高峰值。若攻击流量超过最高防护峰值，安全系统会将攻击 IP 暂时封堵。

- **区域**

高防 IP 或者高防包提供服务的区域。建议根据源站服务器就近选择。高防包只能绑定同区域的腾讯云公网 IP 地址。

相关服务

- **DDoS 高防 IP**

为腾讯云客户（包括云外主机）提供应对大流量 DDoS 攻击的防护服务。用户将高防 IP 作为业务流量接入的入口，后端防护系统将对流量进行检测，发现 DDoS 攻击时将进行清洗，并将清洗后的正常业务请求转发到业务源站服务器。

- **防护域名**

产品控制台在用户创建业务时免费提供的防护域名。用户可以在自己的主域名配置 CNAME 解析到防护域名，实现便捷接入。防护域名可以开启到高防 IP 的解析开关，根据用户来源智能解析。

- **DDoS 高防包**

为腾讯云客户的云内服务器提供的 DDoS 防护能力提升服务。分为单 IP 和多 IP 两种模式，单 IP 高防包可以绑定一个腾讯云公网 IP 地址，多 IP 高防包可以绑定多个腾讯云公网 IP 地址。

- **弹性流量包**

为DDoS高防包提供弹性防护流量计费模式，当业务发生攻击超过保底防护落入在弹性防护区间时，则会从同区域的已购买弹性流量包中扣除弹性发生的流量。与弹性带宽计费相对，能够花更少的防护成本有效应对波峰式高带宽攻击。

DDoS 高防 IP

最近更新时间：2019-09-27 11:16:42

什么是 DDoS 高防 IP

DDoS 高防 IP 是互联网业务防御 DDoS 攻击的主要产品，能够有效地应对大流量的 DDoS 攻击。高防 IP 可按区域和线路维度，为您提供丰富的防御资源。您可以根据业务所在地区和网络，选择适合自身的资源。目前可提供大陆 BGP 和三网高防 IP，境外区域包括中国香港、美国西部、日本、韩国、新加坡等地区。腾讯云高防 IP 最高可以应对 T 级的攻击流量。

使用场景

DDoS 高防 IP 服务于腾讯云以及腾讯云以外的所有云服务器。

防护原理

DDoS 高防 IP 通过代理转发模式防护源站服务器，业务流量直接访问高防 IP，然后回源到源站服务器。如果发生 DDoS 攻击，攻击流量在经过高防 IP 时，防护系统会进行过滤清洗，并将清洁业务流量转发回源到业务服务端，以保障业务在 DDoS 攻击场景下的可用性。

为什么选择 DDoS 高防 IP

- 隐藏真实源站 IP
DDoS 高防 IP 通过代理转发模式，将业务流量转发给源站 IP，以隐藏源 IP，攻击流量被清洗，保护源站业务。
- 超大带宽防护
DDoS 高防 IP 可针对云内外服务器提供 T 级防护，轻松抵御大流量 DDoS 攻击和 CC 攻击。

注意：

如需配置更高带宽防护，请联系客服咨询。

- 支持单 IP、套餐购买
DDoS 高防 IP 支持一次性购买一条或多条不同线路 IP，灵活选购，适用各种业务场景使用。业务需求如果主要是某一个运营商线路，可以直接选购单 IP 防护。而套餐提供多线路防护，避免用户跨网访问。
- 灵活计费
按月预付费的保底防护 + 按天后付费的弹性防护，按实际攻击量计费，为您节约成本。详情请参见 [计费说明](#)。

使用时需要注意什么

DDoS 高防 IP 通过将高防 IP 作为业务 IP 对外发布的方式来隐藏源站 IP，以达到防护目的，若用户源站曾被攻击过且源站 IP 已暴露，那么建议购买 DDoS 高防 IP 服务后更换源站 IP，以确保源站 IP 的隐秘性，让攻击者无法直接攻击源站。如果是腾讯云服务器 IP，请参见 [如何更换腾讯云服务器 IP 地址](#)。

如何配置 DDoS 高防 IP

登录 [宙斯盾安全防护控制台](#)，在左侧目录单击【DDoS 高防 IP】，选择【购买高防 IP】。操作详情请参见 [DDoS 高防 IP](#)。

DDoS 高防包

最近更新时间：2019-09-27 12:03:15

什么是 DDoS 高防包

DDoS 高防包是针对互联网业务部署在腾讯云上的、防 DDoS 攻击的主要产品。DDoS 高防包使用简单，在业务不便更改 IP 地址或者有大量 IP 需要防护的场景下，可以快速简单地完成防护配置。目前 DDoS 高防包有单 IP 模式和多 IP 模式。

使用场景

DDoS 高防包仅适用于腾讯云产品，含云服务器、负载均衡、黑石服务器、黑石负载均衡、NAT IP、EIP、GAAP IP 等。

为什么选择 DDoS 高防包

- 无需任何配置，即时生效
购买 DDoS 高防包后，可通过高防包直接绑定云服务产品，无需额外更换源 IP，快速防护。
- 超大带宽防护
DDoS 高防包可针对云内服务器提供 200Gbps 保底防护，400Gbps 弹性防护。

注意：

如需配置高带宽防护，请联系客服咨询。

- 支持单 IP 模式、多 IP 模式
DDoS 高防包支持一次性选购单 IP 或多 IP，灵活选购，适应各种业务场景。多 IP 支持同时绑定多个不同业务 IP，同时配置高防策略。
- 灵活计费
按月预付费的保底防护 + 按天后付费的弹性防护 / 按用量后付款的弹性流量包。当业务攻击带宽超过保底防护峰值且未超过弹性防护峰值时，DDoS 高防包继续防护，超过保底峰值部分按用量后付款，为用户节约成本。详情请参见 [计费说明](#)。
业务攻击带宽超过保底防护峰值时，将按 **弹性带宽峰值/弹性流量包** 计费。弹性流量包按流量计费，与弹性带宽

峰值按带宽计费相对，当业务攻击带宽很高但实际流量不是很多时，弹性流量包能够用较低的防护成本有效应对波峰式高带宽攻击。

如何配置 DDoS 高防包

登录 [宙斯盾安全防护控制台](#)，在左侧目录单击【DDoS 高防包】，选择【购买高防包】。操作详情请参见 [DDoS 高防包](#)。