BIGBET88 安全防护文档 v1

2021/10/08

目录：

1.防护概述
1-1.防护概述
1-2.防护概念
2.网络流量攻击
2-1.cc 攻击
2-2.Ddos 攻击
3.CDN 厂家
3-1.Google CDN
3-2.G-coreLab CDN
3-3. Cloudflare CDN
3-4.CDN 总体评估对比

1.防护概述

1-1.防护概述

在目前信息化大爆炸时代，网站安全防护是一个令各个 IT 行业最头疼也是最耗费经历的事情。据不完全统计 95%以上的网站受到黑客的攻击，90%以上的网站存在严重的网站安全问题。虽然网络安全的开发商不断增加，网站安全产品也层出不穷，就目前产品来看，都无法根本防护网站安全。由于网站安全的复杂性，安全防护更加复杂，仅依靠单一的产品或者统一的服务无法从根本上解决网站安全问题。需要具有一定的安全意识，针对性的进行防护还是可以解决大部分的安全问题，那么下面就从几个角度讲解下如何进行网站安全防护：

1-2.防护概念

域名解析的安全策略

一般企业或者个人站长都会忽略域名解析的安全性，随意的将域名托管到一些免费域名解析平台上进行解析，经过验证发现大部分域名解析是存在安全隐患的，域名解析生效时间过长、解析出现错误、甚至被别人非法劫持。

网站加速防护策略

如果遇到网站被攻击的情况，很多技术人员会选择一些安全加速类产品，但是目前免费的加速防护基本上被人破解了，有很多绕过检测的方式，而且加速后网站部分会出现各种由于三方安全产品带来的访问问题。所以，在本身技术实现方面也可以做 API 验签/WAF/访问频率限制等安全策略.提高网站本身安全硬实力的等级。

服务器安全防护策略

服务器安全性是网站防护中最重要的一个环节，很多技术人员在产品上线的时候随意开一些端口，无形中就增加了服务器安全风险。这个需要一整套关于安全的整体流程体系去对服务器安全／办公室网络安全等登陆服务器的主机去做相关的安全限制，能够在没有发生问题的时候防患未然。在发生安全问题的时候能够第一时间回溯安全事件并加固安全限制。从根本上防止内部／外部的安全隐患。

网站安全防护策略

服务器安全防护可以保护整个服务器的安全，但是针对每个网站，安全策略肯定不一样，所以这时候如果还会遇到黑客攻击的情况，请针对网站再次进行更深层次的安全防护，例如：定期安全漏洞的扫描、巡检、网站日志深层分析 等。做到安全无小事、安全无死角。

网站代码安全防护

在网站开发的阶段,代码的安全概念就要加入到项目整体管理的模块，在使用某些开源或公用的开发框架、模块的时候，一定要使用最新版本、没有安全漏洞的模块去进行安全开发。代码安全管理方面，要加固代码提交的安全概念。注意代码提交的 review 等，确保提交的网站代码是无恶意后门、无安全漏洞。

网站后台安全防护

关于网站后代的安全更加需要在 登陆验证、登陆 ip 方面、登陆密码等方面的安全限制严格要求并严格执行。防止人为的密码泄漏，做到即使密码泄漏也无法对整体网站后台管理系统照成任何的安全风险。

2.攻击分类

2-1.cc 攻击

概念：CC 攻击的原理就是攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。

防护：对特定的请求类型加入验签、国家区域访问限制和访问频率限制等,能够抑制 95%的 CC 攻击。

2-2.Ddos 攻击

概念：大数据，大流量来压垮网络设备和服务器，要么有意制造大量无法完成的不完全请求来快速耗尽服务器资源

防护：在遇到大规模的流量攻击.一般都是使用第三方的 CDN 防护+流量黑洞模式去做流量的清洗,能够抑制 93%的流量攻击。

2-3.DNS 劫持/中间人攻击

概念: 攻击或伪造 DNS 请求，把目标网站域名解析到错误的 IP 地址从而实现用户要求用户访问指定 IP 地址（网站）的攻击类型

防护: 利用安全签名对 DNS 请求加密或自建 dns 服务器。

注:以上是三种在网站运营过程中遇到最多的攻击方式.其他的攻击方式和防护不再赘述。

3.CDN 厂家

3-1.G-coreLab CDN 防护

每月订阅费用	**基础 € 50/月**	**专业版本€ 140/月**	**企业定制版本**
保证可用性（SLA）	➢ 99.5%	➢ 99.9%	99.9%
在网络和传输层（L，L4）防御 DDos 攻击	没有限制	没有限制	没有限制
在应用层（L7）防御 DDos 攻击	没有限制	没有限制	没有限制
防御资源数量	1	1	1
技术支持	8/5	24/7	24/7
一个补充资源的防御，一个月的价格	**€** 50/月	**€** 50/月	每个请求
保护合法流量	3Mbps	5Mbps	每个请求
资源包超出流量（每 Mbps）	**10€**	**8€**	每个请求
提供 1 个补充 IP 地址，以客户域名的防御	**130€**	**130 €**	每个请求
颁发和支持 SSL 证书，每个证书 1 个月的价格	**2 €**	**2 €**	每个请求
(合法流量的总带宽为启用此选项的资源计算)	**此资源包不可用**	**5 €**	**5 €**
HTTPS 过滤，没有密钥泄露，每个月每个资源的价格	**此资源包不可用**	**115 €**	**115 €**

3-2.Google CDN 防护

	标准级别	Plus 级别
计费模式	按量	订阅
订阅价格	N/a	3000 美元 / 月（包括最多 100 个受保护的资源）
受保护的资源	N/a	初始 100 美元后每月 30 美元 / 受保护资源
WAF HTTP 请求	每百万个请求 0.75 USD	包括
WAF 安全策略	每个安全策略每月 5 美元	包括
WAF 规则	买个规则每月 1 美元	包括
数据处理费用	N/a	收取，请参见下面文档
时间承诺	N/a	一年
Google Cloud Armor 机器人管理(预览版)	N/a	N/a

受保护的资源包括每个注册项目中以下负载均衡器类型的所有后端服务：

- 外部 HTTP(S) 负载平衡器
- SSL 代理负载均衡器
- TCP 代理负载均衡器

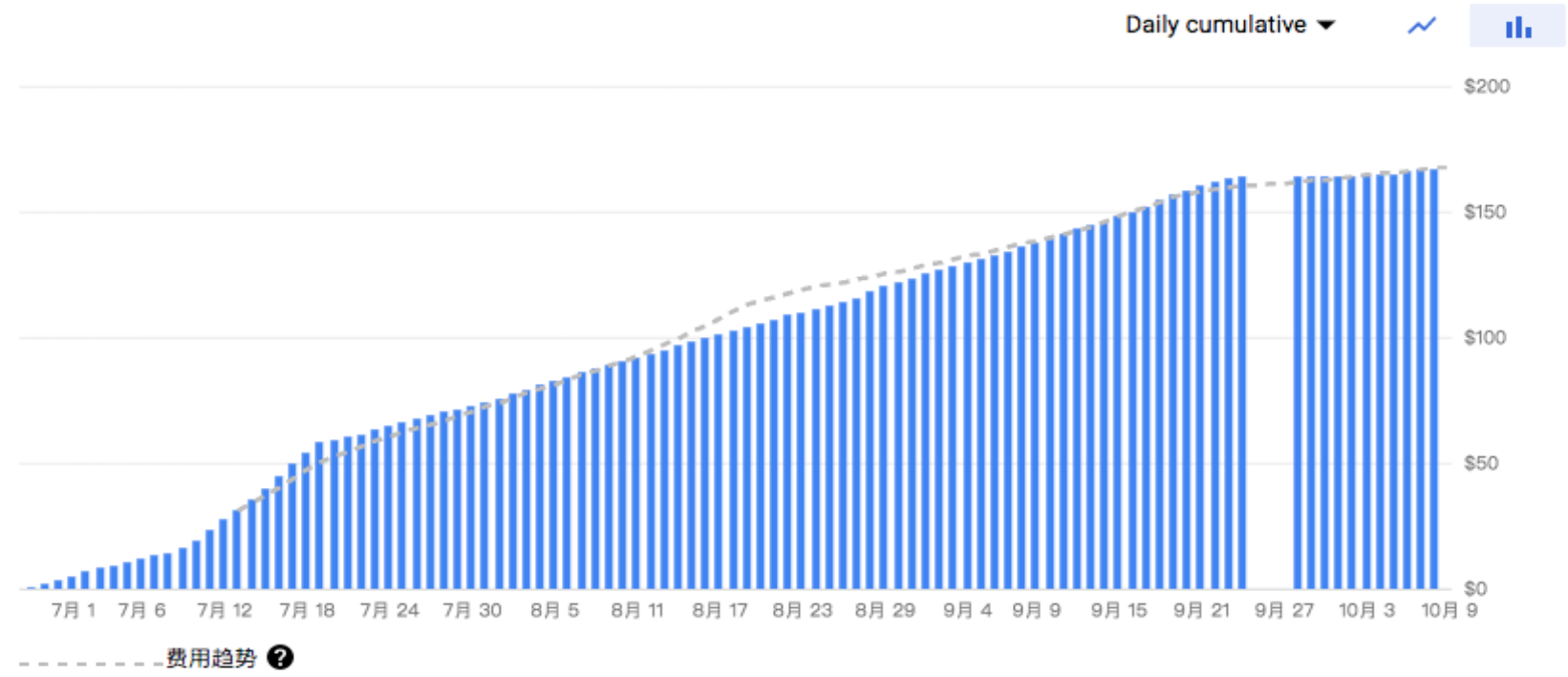
Google 云 数据处理费用收费方案

TB 输出	Cloud Load Balancing, internet, and Cloud Interconnect	Clould CDN	Clould DNS
0 – 100	$0.05	$0.025	包含
101 – 500	$0.04	$0.020	包含
500 - 1000	$0.03	$0.015	包含
1001 +	联系销售团队	$0.010	包含

注意：边缘安全政策的计费方式与后端安全政策相同，但存在以下例外情况：在 Managed Protection Plus 层级中，因 CDN 出站流量而产生数据处理费用

Google 从 2021/06/27 – 2021/10/08 CDN 使用费用

2021/6/27 – 2021/10/8（总费用）		2021/6/27 – 2021/10/8（预测的总费用）	
US$166.42	↑ –	US$167.63	↑ –
包含 US$0.00 的赠金	US$166.42 对比 2021/3/15 – 2021/6/26	包含 US$0.00 的赠金	US$167.62 对比 2021/3/15 – 2021/6/26



	项目	项目 ID	项目编号	费用	折扣	促销及其他	↓ 小计
●	yiy-rich	yiy-rich	535776018317	$166.42	$0.00	–	$166.42

3-3. Cloudflare CDN 防护

免费版本 Free	专业版本 $20/月	商业版本 $200/月	企业定制版本 销售询价
快速易用的 DNS	快速易用的 DNS	专业版本中包含的所用功能	商业版本中包含的所有功能
免费自动的 SSL 证书	免费自动的 SSL 证书	Web 应用程序防火墙	Web 应用程序防火墙
全球内容分发网络	全球内容分发网络	具有共享或单个自定义上传的 SSL / TLS 1.2 和 1.3	具有共享或单个自定义上传的 SSL / TLS 1.2 和 1.3
容量高达 100Tbps 的攻击防护	容量高达 100Tbps 的攻击防护	自动程序分析与高级缓解	自动程序分析与高级缓解
多达 10 万个 Workers 请求和 30 个脚本	多达 10 万个 Workers 请求和 30 个脚本	50 个页面规则	125 个页面规则
3 个页面规则	20 个页面规则	最小边缘缓存到期 TTL（在 30 分钟时）	最小边缘缓存到期 TTL（在 30 秒或更短时间内）
	Web 应用程序防火墙增强安全	分析时间范围（在 15 分钟范围）	具有目标集成的审核日志和 Enterprise 原始日志
	机器人报告和基本缓解	全天候优先客户支持：聊天和电子邮件	分析时间范围（在 1 分钟范围）
	DDoS 警报	100% 正常运行时间 SLA	全天候优先客户支持：电话、聊天和电子邮件支持
	无损图像优化	等候室流量管制	100% 正常运行时间，高达 25 倍补偿 SLA
	加快移动页面加载速度		基于角色的帐户控制
	隐私之上的分析		单点登陆支持
			网络优先顺序
			Enterprise Bot Management
			采用 Magic Transit 的第 3 层网络 DDoS 保护*
			Spectrum（针对 TCP/UDP）
			SSL/TLS For SaaS
			中国网络节点访问加速

注:目前使用的是商业版本 200$/月.

Cloudflare CDN 从 2021/06/27 – 2021/10/08 使用费用

发票

Cloudflare 不为单笔付款逐一提供收据。您将在完成订单后 24 小时内看到合并的发票。

对于任何未列出的历史发票，请发送电子邮件至 billing@cloudflare.com。

发票日期	发票编号	发票金额	状态
2021年10月3日	CFUSA3290226	US$5.00	已支付
2021年9月3日	CFUSA3146524	US$205.00	已支付
2021年8月3日	CFUSA3005640	US$205.00	已支付
2021年7月8日	CFUSA2891192	US$4.35	已支付
2021年7月3日	CFUSA2868496	US$200.00	已支付
2021年6月4日	CFUSA2738522	US$250.00	已支付

3-4.CDN 总体评估对比

CDN 厂商列表	目前使用套餐/月	流量 G	防护能力	防护能力套餐	备注
Google CDN	按使用量	$0.09/G	N/a(未开通)	**每月 3,000 美元或 按使用付费**	支持 ipv6
G-coreLab	€50	1.5T	N/a(未开通)	**€ 140 /月 包括合法流量 5M 或 使用企业定制**	支持 ipv6
Cloudflare	200$	100G	10T	**企业级别需要联系官方销售**	支持 ipv6
VN CDN	260$	5T	N/a(未开通)	**无防护能力**	不支持 ipv6