DDOS 云防御

一、云防御简介

DDoS 云防御（DDoS Cloud Defense）-随着 Internet 互联网的不断普及，网络带宽的增加，高速广泛连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。更为严峻的是，利用 DDos 攻击恶意竞争、敲诈勒索已经形成了一条完善的黑客产业链！而且，发动 DDoS 攻击成本极低，在网上可以随便搜索到很多 DDoS 攻击器，技术要求也越来越低。相反的是，专业防御 DDos 攻击的价格十分昂贵，而且对于攻击源的追查难度极大，防护成本远远大于攻击成本，导致 DDoS 攻击事件正在成上升趋势。出于商业竞争、打击报复和网络敲诈等多种因素，很多 IDC 托管机房、商业站点、游戏服务器、聊天网络等网络服务商长期以来一直被 DDoS 攻击所困扰，随之而来的是客户投诉、同虚拟主机用户受牵连、法律纠纷、商业损失等一系列问题，因此，解决 DDoS 攻击问题成为网络服务商必须考虑的头等大事。在现有单一的安全防护体系及被动的策略难以有效应对时，云盾集成所有已部署的 DDoS 防御资源形成强大的云防御系统，为用户提供高效的整体网络安全解决方案，让您以最少的投资可获得最大的安全回报。

二、云防御技术

云盾云防御系统是一个多层面、多角度、多结构的多元立体系安全防护体系。他是由云盾的多个安全产品整合而成的一个全新一代的防护体系。他们的组成部份分成高防服务器、高防智能 DNS、高防服务器集群（高防服务器集群集成了国内外高防服务器、CDN 防御主机、BGP 防御主机）、集群式防火墙架构、网络监控系统、高防智能路由体系、而形成组合的一套智能的、完善的、快速响应

机制的云安全防护架构。形成终极的 CC/DDOS 的防护架构。架构全球领先的安全防护方案！为您业务保架护航、业务永续！

云盾 DDoS 云防御采用是的以防御为主的分布式集群防御。管理员可通过网络监控系统的访问行为进行严密检测及安全评估。一旦发现问题，智能 DNS 解析系统能针对不同的网络应用服务设置检测端口 ,在遭受攻击使能自动切换成另一节点，保证用户的正常访问。云盾对每个节点服务器都配置了多个 IP 地址，真实数据所在的服务器 IP 不对外公布，网络攻击者难以检测到真实服务器 IP。而值得一提的是，为了防御大规模的 DDoS 攻击， 云盾组建的分布式集群防御网络每个节点都能承受不低于 10G 的 DDoS 攻击，并可根据用户需要增加节点来无限扩展防御能力。在遭受 DDoS 攻击之后，云盾 的宕机检测系统会快速更换，在保证网站恢复正常的同时还能将攻击者的数据包返回发送点，使攻击源变成瘫痪状态，从而将攻击的损失降为最小。

三、DDOS 攻击的形式

SYN/ACK Flood 攻击

这种攻击方法是经典最有效的 DDOS 方法，可通杀各种系统的网络服务，主要是通过向受害主机发送大量伪造源 IP 和源端口的 SYN 或 ACK 包，导致主机的缓存资源被耗尽或忙于发送回应包而造成拒绝服务 ,由于源都是伪造的故追踪起来比较困难，缺点是实施起来有一定难度，需要高带宽的僵尸主机支 持。少量的这种攻击会导致主机服务器无法访问，但却可以 Ping 的通，在服务器上用 Netstat -na 命令会观察到存在大量的 SYN_RECEIVED 状态，大量的这种攻击会导致 Ping 失败、TCP/IP 栈失效，并会出现系统凝固现象，即不响应键 盘和鼠标。普通防火墙大多无法抵御此种攻击。

TCP 全连接攻击

这种攻击是为了绕过常规防火墙的检查而设计的，一般情况下，常规防火墙大多具备过滤 TearDrop、Land 等 DOS 攻击的能 力，但对于正常的 TCP 连接是放过的，殊不知很多网络服务程序（如：IIS、Apache 等 Web 服务器）能接受的 TCP 连接数是 有限的，一旦有大量的 TCP 连接，即便是正常的，也会导致网站访问非常缓慢甚至无法访问 ,TCP 全连接攻击就是通过许多僵尸主机不断地与受害服务器建立大量的 TCP 连接，直到 服务器的内存等资源被耗尽而被拖跨，从而造成拒绝服务，这种攻击的特点是可绕过一般防火墙的防护而达到攻击目的，缺点是需要找很多僵尸主机，并且由于僵尸 主机的 IP 是暴露的，因此容易被追踪。

刷 Script 脚本攻击

这种攻击主要是针对存在 ASP、JSP、PHP、CGI 等脚本程序， 并 调用 MSSQLServer、 MySQLServer、Oracle 等数据库的网站系统而设计的，特征是和服务器建立正常的 TCP 连接，并不断的向脚本程序提交查询、列表等大量耗费数 据库资源的调用 ,典型的以小博大的攻击方法。一般来说 ,提交一个 GET 或 POST 指令对客户端的耗费和带宽的占用是几乎可以忽略的 ,而服务器为处理此请求 却可能要从上万条记录中去查出某个记录，这种处理过程对资源的耗费是很大的，常见的数据库服务器很少能支持数百个查询指令同时执行，而这对于客户端来说却 是轻而易举的，因此攻击者只需通过 Proxy 代理向主机服务器大量递交查询指令，只需数分钟就会把服务器资源消耗掉而导致拒绝服务，常见的现象就是网站慢 如蜗牛、ASP 程序失效、PHP 连接数据库失败、数据库主程序占用 CPU 偏高。这种攻击的特点是可以完全绕过普通的防火墙防护，轻松找一

些 Proxy 代理 就可实施攻击 ,缺点是对付只有静态页面的网站效果会大打折扣，并且有些 Proxy 会暴露攻击者的 IP 地址。

四、云防御特点

-具有强大的攻击检测和防护能力，可以抗 200G 以上流量的攻击

-对已知和未知的攻击都可以完美的防御

-所具备其他防火墙不具备的海量 DDoS 防御，在一定压力测试下对强大的 DDoS 攻击可以做到完美的防御

-采用透明模式，在不改变网络拓扑图的前提下，拥有强大的网络部署能力

-拥有丰富的管理能力，用户可以远程通过 IE 浏览器、或远程桌面跳转登录后台

-详细的攻击数据分析系统，有利于对流量进行统计分析

-运用智能负载均衡系统保证网站在线服务不中断

-只需要把被攻击的网站或者服务器 IP 地址接到云端网络，就可以立即实现抗攻击功能

-云防御服务器的规模可以动态伸缩，满足应用和用户规模增长的需要

-不按带宽收费，不加收任何初始配置费用，按照攻击流量计费，比硬件防火墙可节省 50 倍成本每年

五、防御流程

一：接入云盾云防御系统

A：针对 WEB 攻击-将被攻击网站的域名提交给云盾

B：针对服务器攻击-将被攻击服务器的 IP 地址提交给云盾

二：配置云防御系统

后端的云防御系统配置策略交由云盾完成。

三：完成配置，接受攻击