绿盟黑洞云清洗服务

产品白皮书

【绿盟科技】

■ **文档编号**	黑洞云清洗服务-产品白皮书-V1.0	■ **密级**	完全公开
■ **版本编号**	V1.1	■ **日期**	2018/8/1
■ **撰 写 人**		■ **批准人**	

© 2019 绿盟科技

■ **版权声明**

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ **版本变更记录**

时间	版本	说明	修改人

目录

一. 概述 1
二. 客户价值 1
三. 原理介绍 1
四. 客户价值 3
4.1 安全功能 3
4.2 运营体系 3
4.3 服务交付 4
4.3.1 服务开通 4
4.3.2 用户门户 4
4.4 服务优势 5
4.4.1 零部署，零运维 5
4.4.2 防护硬实力 5
4.4.3 安全专家团队全天候远程支持 5
五. 服务规格 5
5.1 基础防护 6
5.2 弹性防护 6

一. 概述

随着发起 DDoS 攻击的手段愈发普遍和简单以及相关黑色产业链的形成，DDoS 攻击的发生频次和流量峰值逐年增长。据不完全统计，2015 年中国境内共发生 18 万余次有记录的 DDoS 攻击（还有很多 DDoS 攻击并未被检测和统计到），平均每小时 20 多次。2016 年有记录的 DDoS 攻击流量峰值已经突破 600G。

为了协助客户有效缓解 DDoS 攻击，在 ADS 之外绿盟科技推出了黑洞云清洗服务，专门用于解决大流量 DDoS 攻击。当客户遭遇到超过自身出口带宽的 DDoS 大流量攻击时，采用黑洞云清洗服务后，攻击流量将被牵引到绿盟云清洗中心进行清洗，通过清洗后的流量规模将大大缩小，不再对客户链路造成拥堵。清洗后的流量回注给客户，保障客户的正常业务。

黑洞云清洗服务，是应对大流量攻击的有效手段，以最小的经济投入应对大流量 DDoS 攻击，帮助客户有效缓解当前的 DDoS 攻击。

二. 客户价值

黑客通过购买黑产可以轻易发动大流量攻击，攻击流量可以在短时间内打满客户出口带宽，让客户的正常业务无法正常运行。绿盟黑洞云清洗服务产品能够帮助客户以最小的成本有效应对大流量攻击问题。黑洞云清洗服务目前最高可以抵御 300G 的大流量 DDoS 攻击 。

客户购买黑洞云清洗服务后，将同时获取到多节点，多线路的大流量攻击清洗服务。

黑洞云清洗服务购买灵活，可按月消费，可以根据自身业务情况灵活升级。

三. 原理介绍

绿盟黑洞云清洗服务就是把本地部署的 ADS 的功能，通过云服务的方式远程提供给被防护的客户，不需要本地部署和运营。黑洞云清洗服务主要是通过修改 DNS 服务器上域名 IP 信息，将攻击流量牵引到云清洗中心进行清洗。

工作原理如下图所示：

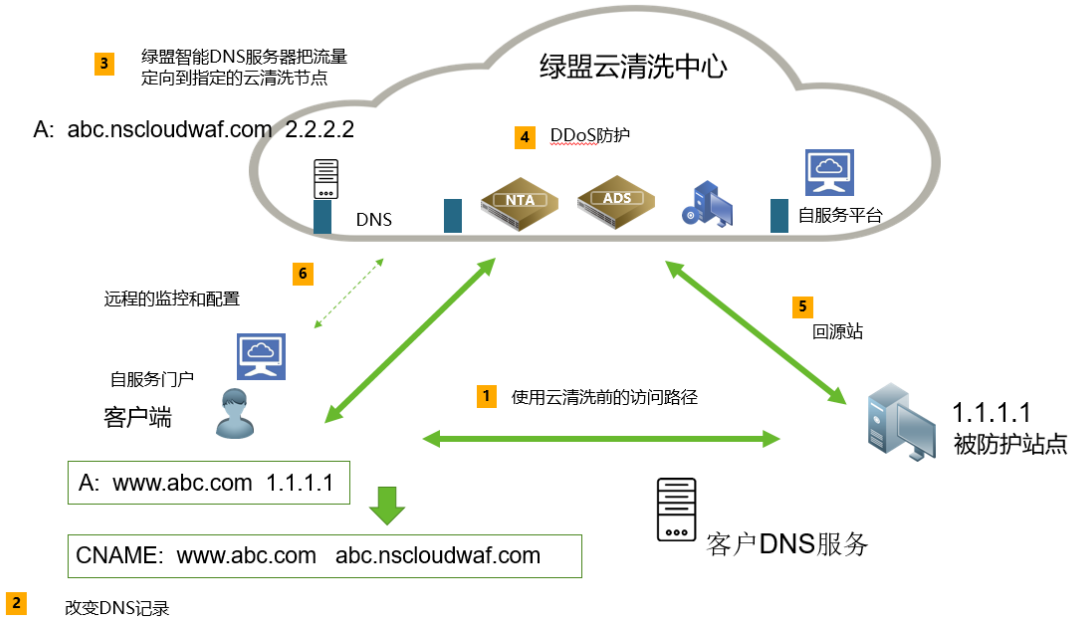


图 3.1 绿盟黑洞云清洗服务工作原理

1) 用户在未使用云清洗服务之前，其终端客户的访问流量通过 DNS 解析直接访问到被防护的网站。本例子中客户的站点为 www.abc.com,其 IP 地址为 1.1.1.1。如路径 1 所示。

2) 当客户启用云清洗的防护，需要修改其授权 DNS 指向。需要增加 CNAME 记录，把原有域名解析到绿盟提供的别名上面，同时需要删除原有 A 记录。本例中绿盟提供的 CNAME 为 abc.nsfocuswaf.com。如图中 2 所示。

3) 绿盟智能 DNS 解析服务器会根据源地址的归属地、所属运营商链路、延时等信息选择把流量定向到对应的云清洗防护节点。本例中是指向了 2.2.2.2 的云清洗地址。如图中 3 所示。

4) 绿盟黑洞云清洗会配置好相应的基础防护模板，并对访问的流量进行防护。云清洗的防护引擎采用的是业界领先的绿盟的实体 ADS 和 NAT 的引擎，对客户的网站进行精准的防护。如图中 4 所示。

5) 云清洗工作在反向代理的模式，所有的客户端的请求都需要由代理向源站请求。图中第 5 部为回源请求。

6) 绿盟黑洞云清洗服务带有客户端的自服务平台，给客户提供可视化的监控和配置界面，查看防护流量和攻击事件的状态。

四. 客户价值

4.1 安全功能

4.1.1 基于数据特征的攻击行为识别

绿盟黑洞云清洗服务可高效防护各类基于网络层、混合型、连接耗尽型等的拒绝服务攻击，如 SYN Flood、UDP Flood、UDP DNS Query Flood、(M)Stream Flood、ICMP Flood、ACK Flood/ DDoS 等攻击。

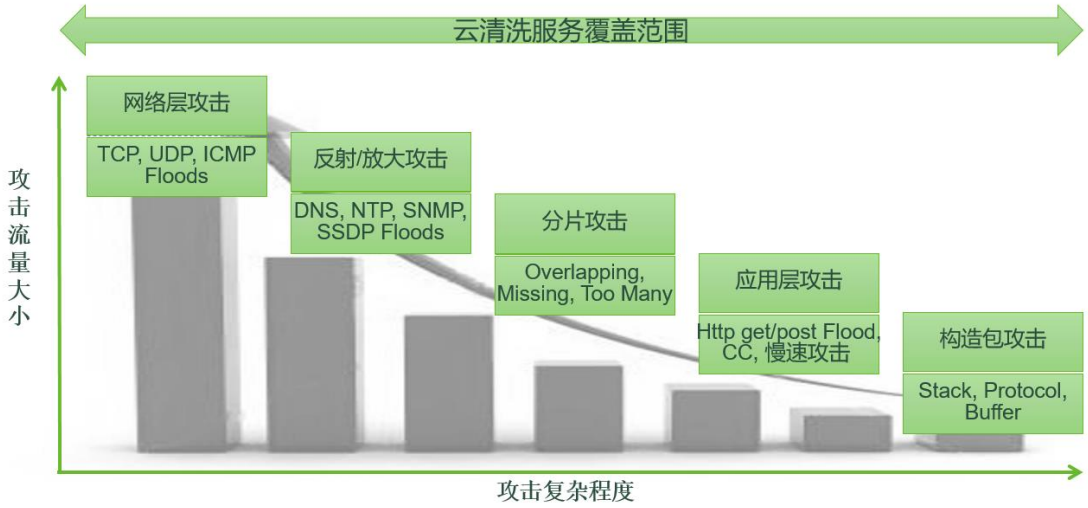


图 4.1 绿盟黑洞云清洗防护能力

4.1.2 基于特征的攻击行为识别

包检查规则允许管理员根据攻击包的源/目的 IP，源/目的协议端口，以及协议类型或 TCP flag/ICMP Type/ICMP Code 等特征字节定义模版，进行快速防护。

4.2 运营体系

1. 运维监控

支持全网流量安全监控，如业务流量采集、监控和分析、安全事件告警、攻击源动态监控等；可视化专业报表呈现，如流量报表、攻击报表和清洗报表。

2. 误报漏报响应

误报、漏洞处理，最终客户可以选择通过用户门户自助处理，也可以通过拨打绿盟科技 7×24 小时服务热线，发起专家支持。

3. 主动优化

主动发现漏报、潜在风险、错误的配置，主动帮助客户进行优化。

4.3 服务交付

4.3.1 服务开通

黑洞云清洗服务开通后，客户会收到服务开通通知，并通过该通知获取到黑洞云清洗用户门户的访问地址、账号信息等关键信息。

4.3.2 用户门户

客户可登录黑洞云清洗用户门户进行黑洞云清洗服务的管理和运维。可通过门户获取报表：流量报表、攻击报表和清洗报表。

客户可实时监控流量和告警，如被攻击 IP 地址、攻击类型、攻击状态、攻击开始和结束时间、清洗情况、攻击期间流量趋势图和告警动态。

客户可通过门户在线配置防护组、防护策略、例外规则等。

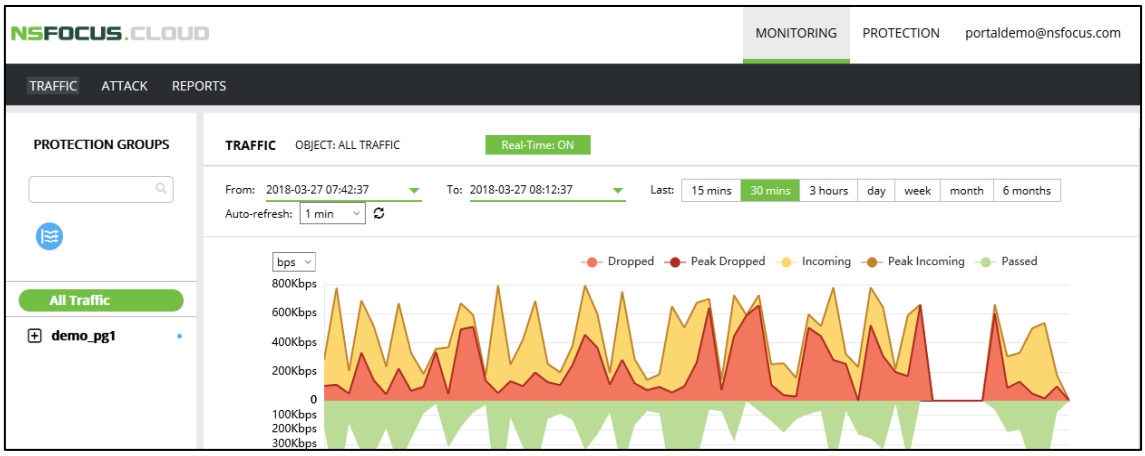


图 4.2 绿盟黑洞云清洗服务用户门户监控图

4.4 服务优势

4.4.1 零部署，零运维

客户部署云清洗的操作非常方便，只需要更改其 DNS 授权域名服务器的 DNS 解析记录，不需要对客户网站进行任何网络结构调整、也无需在客户生产服务器上安装程序。

客户拥有专属的云清洗门户，在线随时查看清洗情况，报表丰富，对攻击及其清洗情况了如指掌。

4.4.2 防护硬实力

突破本地清洗的带宽局限，可抵御高达 300G 的大流量 DDoS 攻击，客户再也不用担心本地出口被攻击恶意堵死而束手无策。联通和电信的双链路客户不用购买两次服务，购买一次服务即可享受两条链路的清洗服务。

云清洗的防护引擎采用的是业界领先的绿盟的实体 ADS 和 NAT 的引擎，对客户的网站进行精准的防护。有效应对大流量和全协议层攻击，让客户无论遭遇何种 DDoS 攻击都高枕无忧。

4.4.3 安全专家团队全天候远程支持

绿盟安全专家团队拥有多名具有行业认证和产品认证资格的安全专家（CISSP、CISP、ISO 27001LA 等），具备丰富的安全专业知识、技能和实战经验。绿盟安全专家团队已主导和参与多年的抗 DDos 攻击应急响应与防护工作。

绿盟安全专家团队提供 7x24 小时全时服务，快速响应客户反馈。

五. 服务规格

绿盟黑洞云清洗服务提供种付费模式：

1. 基础防护（按月预付费）
2. 组合防护（按年预付费）

5.1 基础防护

基础防护的规格指标见下表：

服务名称		绿盟黑洞云清洗服务（基础防护按月预付费）					
服务规格		高级版（10G）	高级版（20G）	高级版（30G）	高级版（40G）	高级版（50G）	高级版（100G）
功能	网络层 DDoS 防护	√	√	√	√	√	√
	应用层 DDoS 防护	√	√	√	√	√	√
	CC 防御	√	√	√	√	√	√
	高防 IP	√	√	√	√	√	√
	清洗能力动态扩展	√	√	√	√	√	√
	防护报表	√	√	√	√	√	√
性能	DDoS 防护能力峰值	10Gbps	20Gbps	30Gbps	40Gbps	50Gbps	100Gbps
	业务带宽峰值	20Mbps	20Mbps	20Mbps	20Mbps	20Mbps	20Mbps
	CC 防护能力峰值	40000pps	80000pps	120000pps	160000pps	200000pps	400000pps
	防护域名个数	50	50	50	50	50	50
	高防 IP 数	1	1	1	1	1	1
服务	远程技术支持服务	√	√	√	√	√	√
	产品系统升级服务	√	√	√	√	√	√
	产品规则升级服务	√	√	√	√	√	√
	安全专家运营服务	√	√	√	√	√	√

5.2 组合防护

按次防护的规格指标见下表：

服务名称	绿盟黑洞云清洗服务（按年预付费）
服务规格	DDoS 攻击防御峰值
高级版（20G3 次 200G1 次）	20Gbps*3+200Gbps*1
高级版（20G10 次 200G2 次）	20Gbps*10+200Gbps*2
高级版（50G3 次 200G1 次）	50Gbps*3+200Gbps*1
高级版（50G10 次 200G2 次）	50Gbps*10+200Gbps*2

5.3 弹性防护

在基础防护的基础上，通过弹性防护让客户能够应对突发的、超大流量的 DDoS 攻击，根据使用情况付费，基础防护结合弹性防护极大降低客户成本。

弹性防护的规格指标见下表：

服务名称	绿盟黑洞云清洗服务（弹性防护按天后付费）
服务规格	DDoS 攻击防御峰值
高级版（20G 天）	20Gbps
高级版（30G 天）	30Gbps
高级版（40G 天）	40Gbps
高级版（50G 天）	50Gbps
高级版（60G 天）	60Gbps
高级版（80G 天）	80Gbps
高级版（90G 天）	90Gbps
高级版（100G 天）	100Gbps
高级版（150G 天）	150Gbps
高级版（200G 天）	200Gbps