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**	V1.0	■ **日期**	2016/06/13
■ **撰 写 人**	张鹏	■ **批准人**	

■ **版本变更记录**

时间	版本	说明	修改人
2016/06/13	V1.0	新建	张鹏

目录

一. 引言 1
二. 客户价值 1
三. 原理介绍 2
四. 黑洞云清洗服务产品介绍 4
4.1 产品概述 4
4.2 服务交付 4
4.2.1 服务开通 4
4.2.2 客户自服务 5
4.2.3 清洗服务启动 5
4.2.4 本地网络变更 5
4.2.5 收费模式 5
4.3 客户价值 6
4.3.1 安心 6
4.3.2 省心 6
4.3.3 放心 6
4.3.4 联合 6
4.3.5 省钱 6
4.4 典型部署 7
五. 总结 7

一. 引言

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。另一方面，除了攻击流量越来越大外，攻击复杂度也越来越高，往往是大攻击流量掩护小型复杂攻击流对目标发起攻击。很多客户倒在了大流量和复杂应用层的双层攻击下。

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产品，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，通过粗粒度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，再经过客户本地部署的 ADS 或 WAF 设备细粒度过滤一遍，以防复杂应用层攻击对服务器造成影响。

黑洞云清洗服务定位于本地清洗的备援服务，是应对大流量攻击的关键手段，能够帮助客户突破本地清洗方案的局限，以最小的经济投入应对大流量 DDoS 攻击。黑洞云清洗服务和本地 ADS 或 WAF 组成立体的抗 DDoS 防御体系，形成了绿盟科技完整的抗拒绝服务解决方案，该方案通过云端和本地的混合清洗方式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，只有本地清洗设备的客户将束手无策。绿盟科技黑洞云清洗服务产品能够帮助网络管理人员解决本地清洗方案的硬伤，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，将同时获取到联通和电信的双链路大流量攻击清洗服务。

黑洞云清洗服务购买灵活，按次消费，可以根据自身业务情况灵活购买，服务利用率高，非常适合大流量攻击频率不高以本地清洗为主的客户群体。

三. 原理介绍

在了解黑洞云清洗服务产品功能之前先简要介绍一下黑洞云清洗服务产品的工作原理。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。

如图 1 所示，流量牵引步骤如下：

① DNS 服务器更换对外服务 IP。客户购买黑洞云清洗服务后，将获取到绿盟云清洗中心的防护 IP:VIP1，客户自己在 DNS 服务上把原域名 IP1 更换为 VIP1。如果使用的是阿里 DNS 域名服务，可以进行自动更换。

② 流量完成切换。客户端向源站的访问流量直接流向 VIP1，安全防护由云清洗中心接管。

③ 回源正常用户。回注方式与传统方式不同,传统是要打上 VPN 标签进行回注隔离主机路由，我们采用协议栈更换技术（替换源、目的 IP 地址），把处理完成的流量再送给源站 IP1 实现回注。

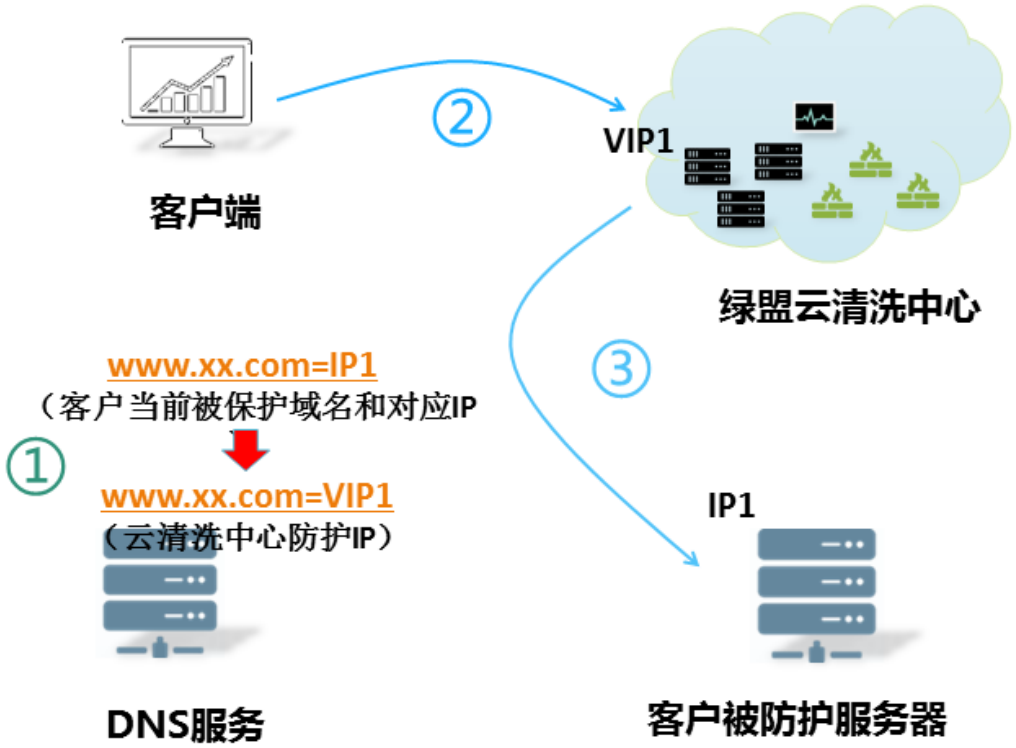


图 1

上述技术原理场景适用于攻击者是按域名解析的方式攻击目标网站（大部分攻击都是采取改方式），但是如果攻击者直接瞄准 IP 进行攻击，则无法防御大流量攻击，有其局限性。

应对直接攻击 IP 的技术方案如图 2 所示：

流量牵引步骤如下：

① DNS 服务器更换对外服务 IP。客户自己在 DNS 服务上把原域名 IP1 更换为 VIP1。如果使用的是阿里 DNS 域名服务，可以进行自动更换。

② 流量完成切换。

③ 回源正常用户，与图 1 不同在于，此时是回源到另外一个没有暴露的 IP2 地址。需要客户在自身的网络中启用备用 IP 地址 IP2，暂时废弃 IP1 地址的应用。

④ 同时联系运营商将去往 IP1 的数据包给黑洞路由丢弃。为了防止 IP2 暴露，如果在该地址之前有安全设备，如防火墙，建议在安全设备上只开放云清洗中心的回源网段。另外，IP2 最好不要跟 IP1 在一个 C 段，在的话有可能被遍历到。

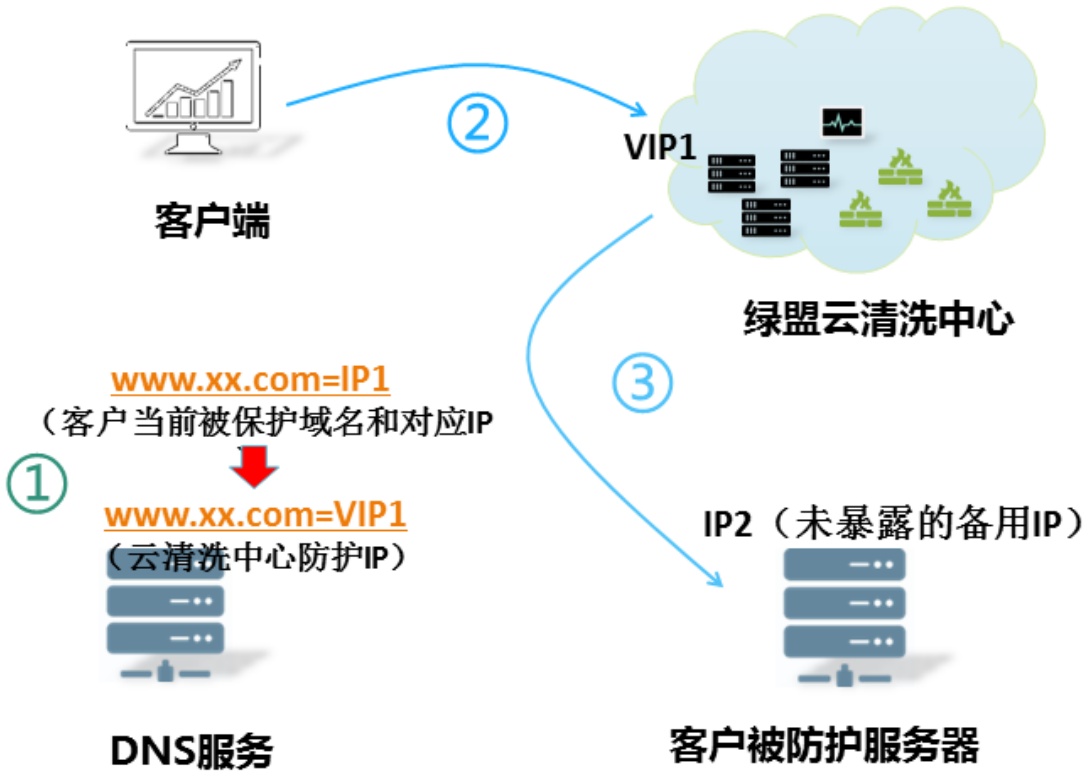


图 2

什么是回源网段？

回源网段的意思是使用云清洗中心的回源网段的 IP 替换原来的访问者 IP，把数据包转发给源站。

建议客户最好能够在其网络边界的安全设备上将回源网段 IP 访问客户对外网站服务的流量加入白名单，其余源 IP 访问客户对外网站服务的流量全部禁止。

四. 黑洞云清洗服务产品介绍

4.1 产品概述

绿盟科技黑洞云清洗服务（Collapsar Cloud-based Scrubbing Service，简称 NSFOCUS CCSS）是一款基于 DNS 智能牵引技术，定位于本地清洗的备援服务，面向政府、金融、教育和企业等客户提供云清洗服务的抗 D 产品。

如图 3 所示超过 10G 的大流量 DDoS 攻击属于小概率事件（20%以内），80%的客户在考虑成本投入的情况下大多不会为了应对这类 20%的攻击而购买大量本地清洗设备、出口带宽或购买长时间的云清洗服务。虽然大流量攻击发生概率小，但只要遇到其所遭受的损失是客户无法承受的。

绿盟黑洞云清洗服务就是针对这类小概率大流量 DDoS 攻击应运而生的服务产品，该服务产品与绿盟 ADS 或 WAF 设备一起使用效果最佳。其中本地设备用于应对经常发生的 10G 以下的 DDoS 攻击。为了便于理解，以医疗保险为例，其一般由日常门诊和大病保险组成，本地设备相当于日常门诊，绿盟云清洗服务相当于大病保险，双管齐下以最经济的投入保障客户业务的健康运行。

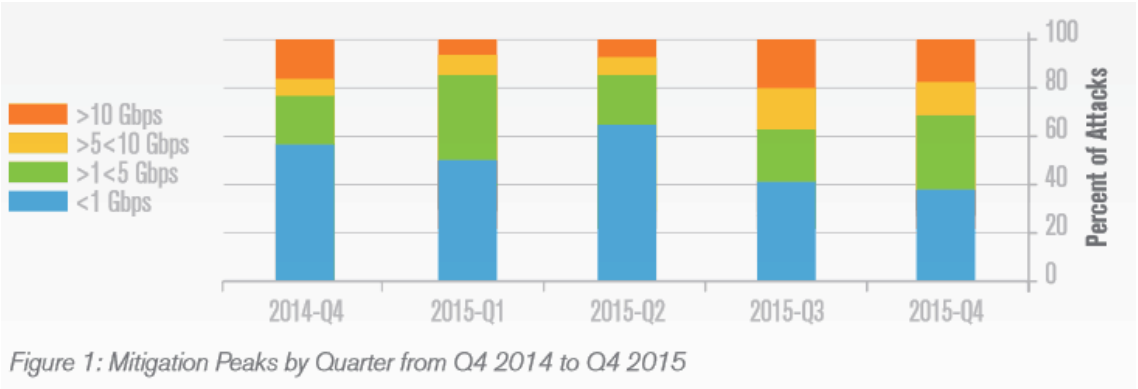


图 3

4.2 服务交付

4.2.1 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自服务系统的访问地址（该自服务系统集成在绿盟云上）、账号信息和绿盟云清洗中心防护 IP 等关键信息。

4.2.2 客户自服务

客户可登录黑洞云清洗自服务系统进行黑洞云清洗服务的管理和运维。管理和运维工作简单明了且工作量极少，前期完成一次性配置后，后期查看清洗报表即可。客户按照说明进行简单几步操作即可正式使用黑洞云清洗服务，真正做到“我的清洗服务，我做主”。

4.2.3 清洗服务启动

当客户遇到大流量攻击时，如果客户决定启用黑洞云清洗服务，客户只需完成一步，即可启动黑洞云清洗服务。对于网站类业务防护，客户需要进行 DNS 修改，将被防护域名解析成云清洗中心防护 IP。对于非网站类业务防护，则需要在客户端中更改服务器的地址为云清洗中心防护 IP。

4.2.4 本地网络变更

如果启用备用 IP，需要在防火墙处修改公网地址为备用 IP，原 IP 弃用，并通知运营商协助阻断发往原 IP 的流量。同时建议客户最好将云清洗中心的回源网段到备用 IP 的网站访问流量设置成允许通过，其它源到备用 IP 的网站访问流量禁止通过。

4.2.5 收费模式

黑洞云清洗服务按次收费，每次服务最长持续时间为 24 小时。黑洞云清洗服务按可抵御的最大攻击峰值划分成不同服务类型，目前共有 20G，100G，200G 和 300G 共 4 档服务。假如客户只购买了最大清洗峰值为 20G 的清洗服务，当其遭受到峰值超过 20G 的攻击，云清洗中心继续为客户进行清洗服务半小时，同时通知客户当前攻击情况及提醒客户购买相应攻击峰值的清洗服务。如果客户不再升级服务，则半小时后将停止清洗服务。

4.3 客户价值

4.3.1 安心

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每条链路最高 300G 的清洗服务。

有效应对大流量和应用层混合攻击，让客户无论遭遇何种 DDoS 攻击都高枕无忧。客户遇到小流量复杂应用层攻击或脉冲攻击时，直接通过本地 ADS 或 WAF 清洗。遇到大流量攻击时，联动黑洞云清洗服务，生效速度快，通过云清洗服务的粗粒度过滤，清洗到绝大部分攻击流量，剩下的“漏网之鱼”通过 ADS 或 WAF 的细粒度防御算法进行过滤。再复杂的组合型 DDoS 攻击都将无功而返。

4.3.2 省心

交付简单，在线实施，零运维。需要清洗时享受一键清洗服务，事后在线随时查看清洗报表，对攻击及其清洗情况了如指掌。

4.3.3 放心

只有大流量攻击时才牵引，大部分时间流量只过本地，流量仍然在客户的有效掌控之中。客户可以放心使用该服务产品，不用担心自身业务的私密性安全。

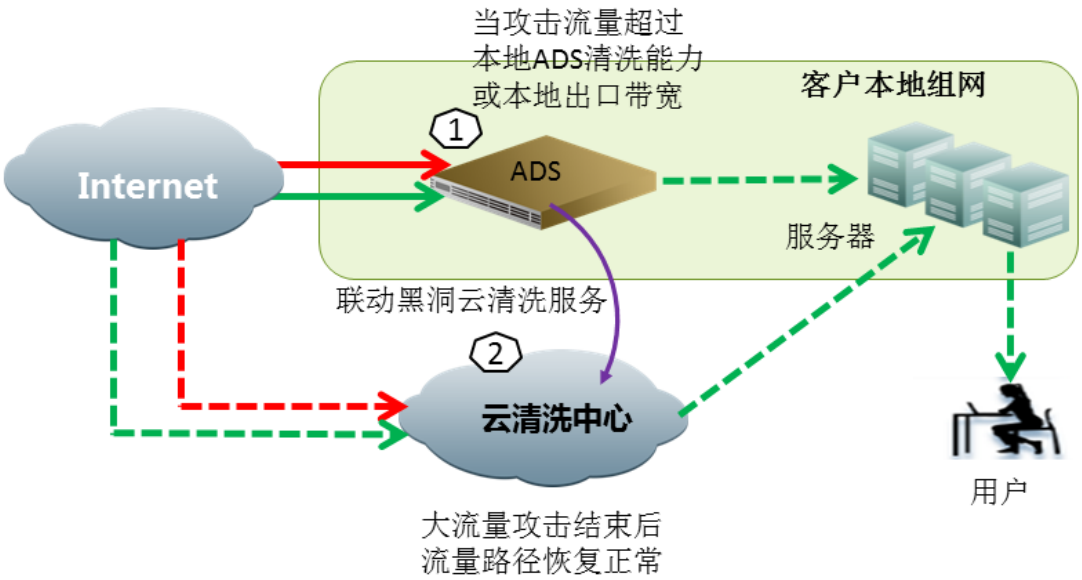
4.3.4 联合

本地清洗时，本地清洗设备（ADS 或 WAF）进行实时检测和清洗。当攻击流量超过本地设备设置阈值后，本地设备（ADS 或 WAF）自动联动云清洗中心进行黑洞云清洗服务，秒级响应。

4.3.5 省钱

基于 DDoS 攻击历史统计数据，10G 以上大流量攻击仅占全部攻击的 20%以内，推出灵活的按次清洗服务，避免客户承担昂贵的包月或包年的云清洗服务。客户根据自身遭受的攻击情况，灵活购买服务，将服务利用率最大化。

4.4 典型部署



1 本地清洗设备有效应对中小规模流量攻击（以复杂应用层攻击为主，占所遇攻击数量的 80%以上，精细过滤攻击流量）。

2 遇到超大流量攻击时可以自动联动云清洗中心进行黑洞云清洗（简单粗暴型攻击为主，占所遇攻击数量的 20%以下，粗过滤攻击流量）。

3 该服务可单独购买，需要清洗的时候修改自身 DNS 域名信息指向云清洗中心防御 IP 并确保自身网站的源站 IP 与黑洞云清洗服务所配置的源站 IP 保持一致（边界安全设备上启用过滤规则，仅允许清洗中心的回源网段访问自身网站服务）。该服务也可以跟本地 ADS 或 WAF 设备联合使用，当本地设备感知到攻击超过设定阈值后，可以联动云清洗中心进行黑洞云清洗服务。

五. 总结

黑洞云清洗服务产品联合本地 ADS 或 WAF 清洗打造绿盟科技最强抗 D 方案，黑洞云清洗服务进行粗粒度过滤，过滤掉大部分攻击流量；本地 ADS 或 WAF 进行细粒度过滤，过滤

掉复杂的应用层攻击或脉冲攻击，二者结合形成立体防护方案让 DDoS 攻击无法影响客户业务的正常运行。最后总结一句话：联合的抗 D 才是最强的抗 D！