华为AntiDDoS1000系列

华为技术有限公司

HUAWEI

FROST & SULLIVAN

Dear Huawei Employees,

Heartiest Congratulations to the Huawei team for the successful vision and ingenuity demonstrated in attaining the Product Innovation Award for its anti-DDOS solutions in Network Security Market in the Middle East.

Huawei received this Award for its leadership and accomplishments displayed in the network security space. It has been able to achieve it due to its technology innovation, dedicated workforce, a well stratified channel structure and a strategic focus towards developing a cost effective and efficient security product offering in the form of its anti-DDOS solution.

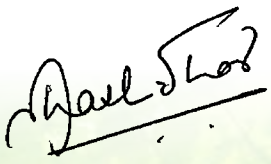
The Award is an accomplishment to be truly proud of, as this recognition stems from an in-depth analysis of the Network Security space by our experienced industry research team.

Frost & Sullivan is a global growth consulting company with more than fifty years of research and consulting experience. We take great pride in rewarding those few companies who exhibit excellence in their growth strategies.

Our expert analysts confer Frost & Sullivan Awards upon companies in each market sector that demonstrate exceptional leadership, successful customer acquisition and service strategies, and sound execution in business plans, in addition to other critical marketing factors.

On behalf of everyone at Frost & Sullivan, I would like to congratulate you all on this outstanding achievement. We are proud to present you the Frost & Sullivan 2012 Middle East New Product Innovation Award in Network Security Market.

Yours Sincerely,



Y S. Shashidar
Managing Director
Frost & Sullivan
Middle East, North Africa and South Asia

背景与挑战

分布式拒绝服务（DDoS——Distributed Denial of Service）攻击随着IT及网络的发展演进至今，早已脱离了早期纯粹黑客行为的范畴，进而形成了完整的黑色产业链，其危害更是远超以往。

DDoS攻击形势愈加严峻

当前DDoS攻击防御形势更加严峻，单次攻击流量超过500G的案例已经发生，攻击数量较2007难增加20倍，全球僵尸主机规模已经超过3000万台……随处可以获得的攻击工具，庞大的僵尸网络群体，发动一次DDoS攻击不再需要任何黑客技术门槛，只需要3步（下载攻击工具、购买僵尸主机，发动攻击）即可完成一次攻击。

DDoS攻击由流量型攻击转向应用型和移动型攻击

过去DDoS攻击以Flood型攻击为主，更多的针对运营商的网络和基础架构；而当前的DDoS攻击越来越多的是针对具体应用和业务，如：针对某个移动APP应用、企业门户应用、在线购物、在线视频、在线游戏、DNS、Email等，攻击的目标更加广泛，单次攻击流量小成本低，移动型智能终端攻击传统防御方式影响正常业务、攻击行为更为复杂和仿真，造成DDoS攻击检测和防御更加困难。

业务中断影响企业正常运营

业务系统频遭DDoS攻击将企业推向两难境地，严重的影响着企业业务的正常运营。一方面，业务中断造成企业的形象受损，客户流失，收益降低等，尤其是对电商、网游、门户类小型互联网企业；另一方面，企业若自己建设DDoS防护系统，会给这些“小本经营”企业带来巨大投资和维护压力，严重的影响着企业业务的正常运营。

DDoS攻击造成IDC客户流失

一个业务系统遭受DDoS攻击，攻击流量挤占整个IDC带宽资源，影响其他租户的业务系统；数据中心中服务器被黑客控制，沦为僵尸，恶意流量充斥着数据中心的带宽资源，甚至给数据中心带来法律风险；安全问题导致IDC租户流失，竞争力下降、运营成本增加等一系列的负面影响，严重的影响IDC业务运营和收益。

产品特点

产品概述

基于多年来对客户需求的深刻理解和在安全方面的专业研究，华为公司推出的AntiDDoS1000系列产品，面向金融、政府、ICP服务商、及数据中心等关键在线业务系统，提供专业的DDoS攻击防护解决方案。

华为AntiDDoS1000系列在防护传统流量型DDoS攻击的基础上，重点加强了对应用层攻击的防护、IPv4-v6双栈防护、僵木蠕防护等功能，真正保护用户业务安全永续。

华为的AntiDDoS1000在管理配置上，采用GUI图形化管理方式，对流量模型进行学习、自动推荐防护策略、灵活的告警和精细化报表呈现等功能，满足IDC和企业IT安全、简单、便捷的管理要求。

产品功能

基于业务的防护策略

本方案能够针对防护对象的业务流量进行持续的周期性的学习和分析，勾勒出业务流量正常曲线，针对不同的业务流量类型、同一业务不同时段，采取不同的防御防护类型和防护策略，实现精细化防护。

精准的异常流量清洗

华为AntiDDoS1000采用大数据分析技术，从60多种维度对流量进行模型学习，一旦某个维度出现流量异常立即启动防护。防护采用七层过滤、行为分析、会话监控等多种技术手段，能精确防护各种Flood类攻击流量、web应用类攻击流量、DNS攻击流量、SSL DoS/DDoS类攻击流量和协议栈漏洞类攻击流量，保护应用服务器安全。

DNS流量智能Cache

华为AntiDDoS1000不但能够精确防护针对DNS服务器的各种漏洞攻击、应用攻击、和Flood类攻击，还可提供DNS Cache功能，缓解DNS服务器大流量下的性能压力。

流行僵木蠕防护

黑客通过木马蠕虫感染网络中的大量主机，分层控制组成僵尸网络，以便其发动各种攻击行为，因此可谓僵尸网络是黑客发起DDoS攻击的温床。华为AntiDDoS1000系列能够支持全球最流行200+种僵尸工具/木马/蠕虫流量识别与阻断，从而达到摧毁僵尸网络的目的。

完善的IPv4-v6双栈防护

2011年2月，IANA宣告IPv4地址分配告罄，企业面临无新的v4地址使用局面，纷纷将IPv6网络建设纳入网络

规划建设议程。华为Anti-DDoS解决方案独有的IPv4-v6双栈合一技术，能够同时防御IPv6，IPv4组网内的DDoS攻击，满足双栈DDoS防御需求，帮助用户无忧过渡到下一代网络。

灵活的组网部署方式

AntiDDoS1000系列作为对已有网络的保护措施，必须能够适应客户多种不同的网络环境，并满足客户不同的业务等级要求。

正是基于此，华为AntiDDOS1000系列为客户提供了直路和旁路等多种网络部署方式，客户可以根据业务需要和网络结构灵活选择，具体包括如下方式：

直路接入模式：将清洗检测模块串接在客户需要保护的网络中，直接对客户流量进行检测和清洗。华为基于高性能多核硬件平台，在高效的保证检测和清洗的准确性的同时，也将处理时延做到最小。此外，华为AntiDDOS1000支持Bypass板卡模块，当出现意外时，流量自动透传清洗模块，避免为客户引入新的故障点。

旁路引流模式：将清洗模块部署在客户网络旁路上，对客户流量进行旁路检测，一旦发现DDOS攻击流量，清洗检测中心可以根据客户在管理中心上制定的检测清洗策略执行相应的动作。

产品特点

华为AntiDDoS1000系列产品主要特点：

高效快速：5Gbps防护性能、秒级防护响应

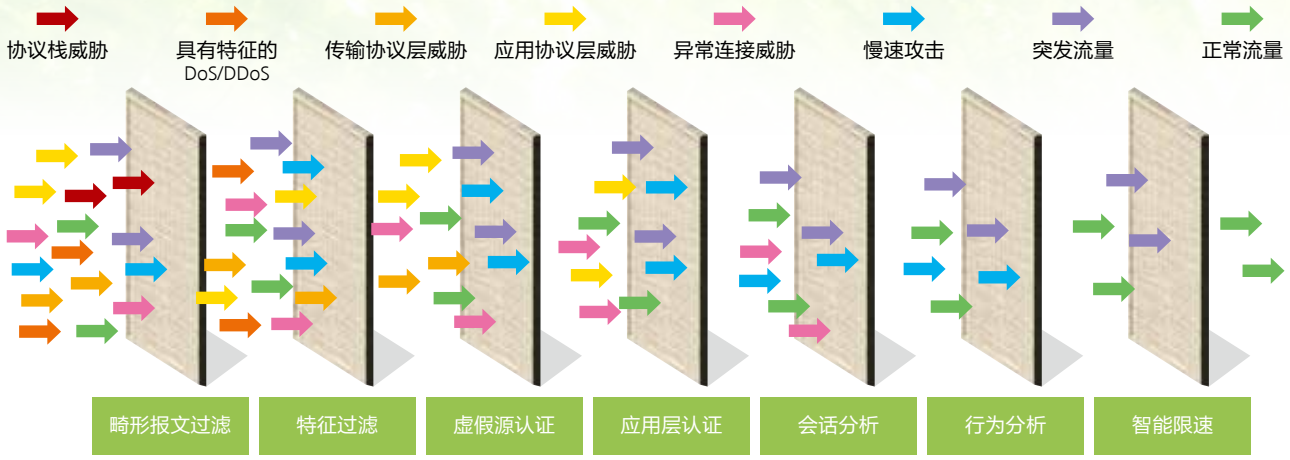
- 基于高性能多核CPU，提供5Gbps的防护性能，满足企业DDoS防护性能需求，轻松应对各种规模应用型DDoS攻击
- 采用业务模型流量自学习和逐包深度检测技术，一旦发现流量和报文异常，自动触发防护策略，从攻击发生到防御启动时延小于2秒钟

精确全面：百余种攻击防御和IPv6防护

- 独有大数据分析技术，提供“V-ISA”信誉安全体系，可精确防御100+种DDoS攻击，防御类型业界最多
- 可提供全球最新 200+种僵木蠕防护，保护用户远离黑客网络
- 智能IPv4-v6双栈合一，率先全面支持IPv6攻击防御，首家的同时支持IPv4-v6攻击同时防护的方案
- 独有的终端识别技术，可精确识别客户端类型，如：智能终端、机顶盒、普通客户端等，不同客户端采用不同的防护技术，确保不对正常用户产生误判

简单易用：管理简单、报表丰富

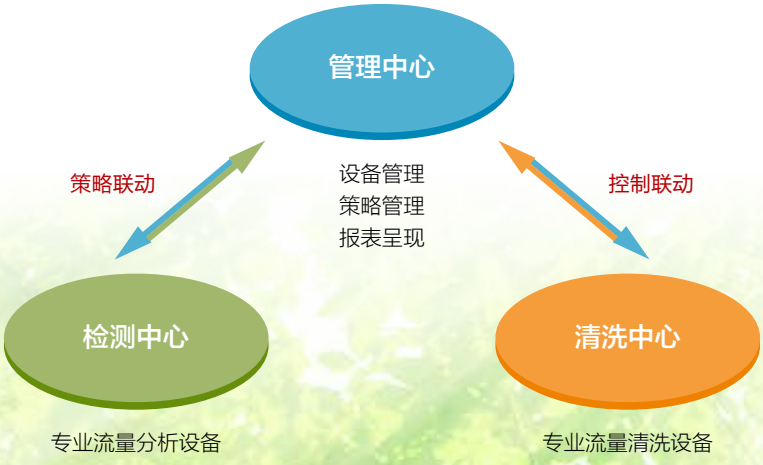
- GUI的图形化管理界面，基于业务的管理和防护模板，简单方便



- 业务流量模型、攻击趋势分析、多种告警模式、丰富的报表功能，让管理人员对业务安全态势了如指掌
- 支持攻击报文抓取，进而提取攻击特征，支持攻击特征自定义过滤技术，可实现紧急情况下DDoS攻击防御，有效“抵御零日”攻击

方案组成

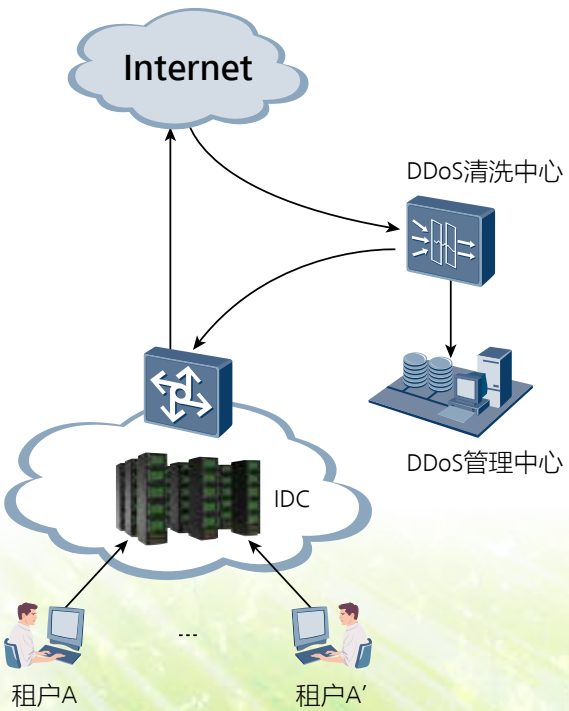
如下图所示，华为AntiDDOS1000系列由AntiDDoS1500-D、AntiDDoS1520、AntiDDoS1550三款产品组成。其中AntiDDoS1500-D为检测设备，其它2款AntiDDoS1520、AntiDDoS1550均为清洗设备，因客户防护性能不同，在使用时选其一即可。华为的Anti-DDoS解决方案由三部分组成：检测中心即AntiDDoS1500-D、清洗中心（AntiDDoS1520或者AntiDDoS1550）和管理中心（ATIC管理中心软件）。三者通过策略联动和控制联动最终为客户提供管理简单、部署灵活等专业防DDOS解决方案。



- 检测中心：作为整个解决方案的“触角”，检测中心设备接受管理中心的下发检测策略，并根据该策略实现对网络中DDOS流量的识别和检测，并将检测结果反馈给管理中心。
- 清洗中心：作为整个解决方案的“响应执行者”，清洗中心根据管理中心下发的控制指令，完成对网络流量中的DDOS攻击流量清洗。
- 管理中心：作为整个解决方案的“大脑”，用户通过管理中心制定检测策略和清洗策略，并下发至检测中心设备和清洗中心设备上，来控制整个检测和清洗过程。同时，用户还可以通过管理中心生成和查看攻击报表和清洗记录。
- *注（1）：实际方案部署中，检测中心可以是逐包检测技术的检测设备，也可以是Netflow抽样检测设备；*
- *注（2）：清洗中心也可以直路串接在用户网络中（无需配置检测中心），起到全面双向防护作用，具体组网可根据用户的实际需求，实现灵活配置。*

典型应用场景

企业IDC安全安全应用场景



将华为的Anti-DDoS解决方案部署在IDC出口处，能够帮助客户解决一下攻击防护：

1、防御针对DNS服务器的各类攻击，如：DNS协议栈漏洞攻击、DNS反射攻击、DNS Flood攻击、DNS CacheMiss攻击等，同时能够提供DNS Cache功能，缓解大流量DNS服务器压力。

2、防护针对web服务器类攻击，如：SYN Flood攻击、http Flood攻击、CC攻击、慢速连接类攻击等。

3、防护针对网游类攻击，如：UDP Flood攻击、SYN Food、TCP类攻击等。

4、防护针对https服务器的SSL DoS/DDoS类攻击等。

5、支撑IDC将DDoS防护作为安全业务做运营，可对客户提供资助策略配置和自助报表功能。

产品照片

AntiDDoS1000系列

规格参数

型号	AntiDDoS1520	AntiDDoS1550	AntiDDoS1500-D
固定接口	4×GE（RJ45）+4×GE（combo）		
扩展槽位	2×FIC	2×FIC	2×FIC
扩展接口卡	2×10GE（SFP+）；2×10GE（SFP+）+8GE（RJ45）；8×1GE（SFP）；8×1GE（RJ45）；		
Bypass卡	4×1GE（RJ45）；2链路LC/UPC多模光接口；2链路LC/UPC单模光接口；		
外型尺寸（W×D×H）	442×560×43.6	442×560×43.6	442×560×43.6
最大功耗	150W	150W	150W
IPv4威胁防御类型			
异常过滤	黑名单/基于HTTP协议字段的过滤/TCP/UDP/other协议负载特征过滤		
协议漏洞威胁防护	IP Spoofing；LAND攻击；Fraggle攻击；Smurf攻击；Winnuke攻击；Ping of Death攻击；Tear Drop攻击；IP Option控制攻击；IP分片控制报文攻击；TCP标记合法性检查攻击；超大ICMP控制报文攻击；ICMP重定向控制报文攻击；ICMP不可达控制报文攻击等		
传输层威胁防护	SYN flood攻击；ACK flood攻击；SYN-ACK flood攻击；FIN/RST flood攻击；TCP fragment flood攻击；UDP flood攻击；UDP fragment flood攻击；ICMP flood等		
扫描窥探型威胁防护	端口扫描攻击；地址扫描攻击；TRACERT控制报文攻击；IP源站选路选项攻击；IP时间戳选项攻击；IP路由记录选项攻击等		
DNS威胁防护	虚假源DNS query flood攻击；真实源DNS query flood攻击；DNS reply flood攻击；DNS缓存投毒攻击；DNS协议漏洞攻击等		
Web威胁防护	HTTP get /post flood攻击；CC 攻击；HTTP slow header/post攻击；HTTPS flood攻击；SSL DoS/DDoS攻击；TCP连接耗尽攻击；Sockstress攻击；TCP重传攻击；TCP空连接攻击等		
VOIP威胁防护	SIP flood		
僵木蠕威胁防护	200+流行僵尸木马蠕虫防护，如：LOIC、HOIC、Slowloris、Pyloris、HttpDosTool、Slowhttptest、Thc-ssl-dos、傀儡僵尸、猎鹰DDOS、风云白金、小鱼重装等主流僵尸网络工具		
IPv6威胁防御类型			
IPv6威胁防御类型	ICMP Fragment报文攻击；黑名单过滤；基于HTTP协议字段的过滤；支持TCP/UDP/other协议负载特征过滤；SYN flood攻击；ACK flood攻击；SYN-ACK flood攻击；FIN/RST flood攻击；TCP fragment flood攻击；UDP flood攻击；UDP fragment flood攻击；ICMP flood攻击；虚假源DNS query flood攻击；真实源DNS query flood攻击；DNS reply flood攻击；DNS缓存投毒攻击；DNS协议漏洞攻击；Fast flux僵尸网络；HTTP get /post flood 攻击；CC 攻击；HTTP slow header/post攻击；HTTPS flood攻击；SSL DoS/DDoS攻击；TCP连接耗尽攻击；Sckstress攻击；TCP重传攻击；TCP空连接攻击；SIP flood等		
IPv4/IPv6双栈防御	支持		

订购信息

AntiDDoS1000系列产品订购信息

AntiDDoS1000系列订购信息		
AntiDDoS1500-D主机基本配置		
AntiDDoS1500D-AC	AntiDDoS1500 D-SUBZ31UAH-AMS1500-D交流主机-含HW通用安全平台软件	二选一
AntiDDoS1500D-DC	AntiDDoS1500 D-SUBZ31UDH-AMS1500-D直流主机-含HW通用安全平台软件	
AntiDDoS1520主机基本配置		
AntiDDoS1520-AC	AntiDDoS1520-SUBZ11UAH-AMS1520交流主机-含HW通用安全平台软件	二选一
AntiDDoS1520-DC	AntiDDoS1520-SUBZ11UDH-AMS1520直流主机-含HW通用安全平台软件	
AntiDDoS1550主机基本配置		
AntiDDoS1550-AC	AntiDDoS1550-SUBZ21UAH-AMS1550交流主机-含HW通用安全平台软件	二选一
AntiDDoS1550-DC	AntiDDoS1550-SUBZ21UDH-AMS1550直流主机-含HW通用安全平台软件	
AntiDDoS1000系列接口模块集合		
FIC-2SFP+&8GE	2*10GE光口+8GE电口卡-含HW通用安全平台软件	选配
FIC-8GE	8GE电口卡-含HW通用安全平台软件	选配
FIC-2SFP+	2*10GE光口FIC卡-含HW通用安全平台软件	选配
FIC-8SFP	8GE光口FIC卡-含HW通用安全平台软件	选配
FIC-8SFP	8GE光口FIC卡-含HW通用安全平台软件	选配
FIC-2LINE-M-BYPASS	2链路LC/UPC多模光接口Bypass保护卡-含HW通用安全平台软件	选配
FIC-2LINE-S-BYPASS	2链路LC/UPC单模光接口Bypass保护卡-含HW通用安全平台软件	选配
DDOS功能组件		
ADSCT001WIN01	Windows中文运行平台(交流服务器，硬盘，加载Windows中文系统及补丁软件)-含操作系统License	选配
ADSCT001WIN03	Windows中文运行平台(直流服务器，硬盘，加载Windows中文系统及补丁软件)-含操作系统License	选配
NS19MKM00	键盘&鼠标(USB)-19英寸液晶显示器	选配
AntiDDoS管理中心		
LIC-ADS-NOFA00	AntiDDoS管理中心-基础功能汇总项-含HW通用安全平台软件	必配

商标声明

、**HUAWEI、华为**、是华为技术有限公司的商标或者注册商标。

在本手册中以及本手册描述的产品中，出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

华为技术有限公司

深圳市龙岗区坂田华为基地

电话: (0755) 28780808

邮编: 518129

版本号: M3-036926-20150116-C-1.0

www.huawei.com