Anti-DDoS解决方案

方案概述

分布式拒绝服务（DDoS——Distributed Denial of Service）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。

当前DDoS单次攻击带宽已突破100G，较2007年增长10倍，DDoS攻击数量增加了 20倍，僵尸主机规模已经超过3000万台……，给网络带宽带来巨大压力，而且攻击工具越来越智能，攻击行为越来越隐蔽和仿真，尤其是面向IDC应用的攻击层出不穷，使得客户当前部署的防御手段基本失效。

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Anti-DDoS解决方案，面向运营商、企业、数据中心和ICP服务商（门户网站、游戏服务商、在线视频、DNS服务商、CDN服务等）提供专业DDoS防护，在传统流量型Anti-DDoS基础上重点加强了对应用层攻击的防护，和IPv6-v4混合组网下攻击的防护能力，真正保护用户业务永续无忧。

方案特点

高效快速：200Gbps防护性能、秒级防护响应

- 基于高性能多核CPU，提供2G-200G的全系列Anti-DDoS产品；
- 采用业务模型流量自学习和逐包检测技术，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："V-ISA"信誉安全体系，可防御百余种攻击防护

- 独有的“V-ISA”信誉安全体系，可防御100+种DDoS攻击，防护类型业界最多；
- 支持全球最新 200+种僵木蠕防护，保护用户远离黑客控制；
- IPv4/IPv6双栈合一，首家全面支持IPv6攻击防御的方案；
- 终端识别技术，提供非法客户端精准判别，降低误判。

运营增值：十万租户保护、多样自助服务

- “租户”可实现自助配置防护策略、生成独立安全报表，让客户的客户对防护效果一目了然；
- 支持攻击特征自助提取，帮助客户实现紧急防御，有效“抵御零日”攻击 。

产品规格

	AntiDDoS1000系列			AntiDDoS8000系列		
型号	**AntiDDoS1520**	**AntiDDoS1550**	**AntiDDoS1500-D**	**AntiDDoS8030**	**AntiDDoS8080**	**AntiDDoS8160**
固定接口	4×GE（RJ45）+4×GE（combo）			无		
扩展槽位	2×FIC	2×FIC	2×FIC	3	8	16
扩展接口卡	2×10GE（SFP+）； 2×10GE（SFP+）+8GE（RJ45）； 8×1GE（SFP）； 8×1GE（RJ45）；			1×10GE（XFP）； 2×10GE（XFP）； 1×10G POS（XFP）； 12×1GE（SFP）； 20×1GE（SFP）；		
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；			无		
外型尺寸（W×D×H）	442×560×43.6	442×560×43.6	442×560×43.6	442×650×175（直流） 442×650×220（交流）	442×650×620（直流） 442×650×709（交流）	442×650×1420（直流） 442×650×1598（交流）
最大功耗	150W	150W	150W	1330W（直流） 1368W（交流）	3038W（直流） 3231W（交流）	5824W（直流） 6195W（交流）
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；Fast flux僵尸网络等					
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					