

华为HiSecEngine AntiDDoS12000 系列产品

卓越性能、毫秒响应、精准防御、智能驾驶

随着互联网的高速发展，黑客攻击手段不断演进，行业内的恶性竞争日趋激烈，促使DDoS攻击强度、频率和复杂度持续提升，DDoS防御面临新的挑战：

- 攻击强度持续攀升，挑战防御成本；
- 大流量攻击呈现Fast Flooding，挑战防御系统响应速度；
- 业务多元化，攻击复杂化，传统防御技术失效。

为应对新的防御挑战，华为推出了AntiDDoS12000系列产品：全流量逐包检测，60+流量模型，毫秒级攻击响应；NP防御加速，单机最高2.4T防御能力，高效阻断网络层攻击；7层智能“滤板”，多维度行为分析及机器学习，精确识别各种复杂CC攻击；独创在线升级防御引擎，快速应对0-day DDoS；防御策略自动调优，防御全程智能驾驶。

产品图



AntiDDoS12004



AntiDDoS12008



AntiDDoS12016



HUAWEI



产品亮点

- **卓越性能**: CPU智能协同NP防御加速, 单机最高2.4T防御能力
- **毫秒响应**: 全流量逐包检测, 60+流量模型, 毫秒级攻击响应, 业务零影响
- **精准防御**: 7层智能“滤板”, 多维度机器学习加持, 逐层过滤L3/4/7攻击; 独创在线升级防御引擎, 快速应对0-day DDoS; 三层防御架构, 秒级应对扫段攻击
- **智能驾驶**: 专家策略模板, 防御效果评估, 防御策略自动调优, 防御全程智能驾驶

方案功能

网络层DDoS防御

- 采用电信级硬件架构, CPU智能协同NP防御加速, 单机防御性能最高2.4T
- 全流量采集, 逐包检测, 60+流量模型, 毫秒级攻击响应, 快速阻断网络层攻击, 保障网络链路带宽可用性

应用层DDoS防御

- 基于多维度行为分析和机器学习, 精准防御HTTP CC&HTTPS CC, 不解密防御加密攻击, 性能更高
- 全面抵御会话层及应用层攻击, 保护网站、APP、API、DNS等关键业务系统

增值运营

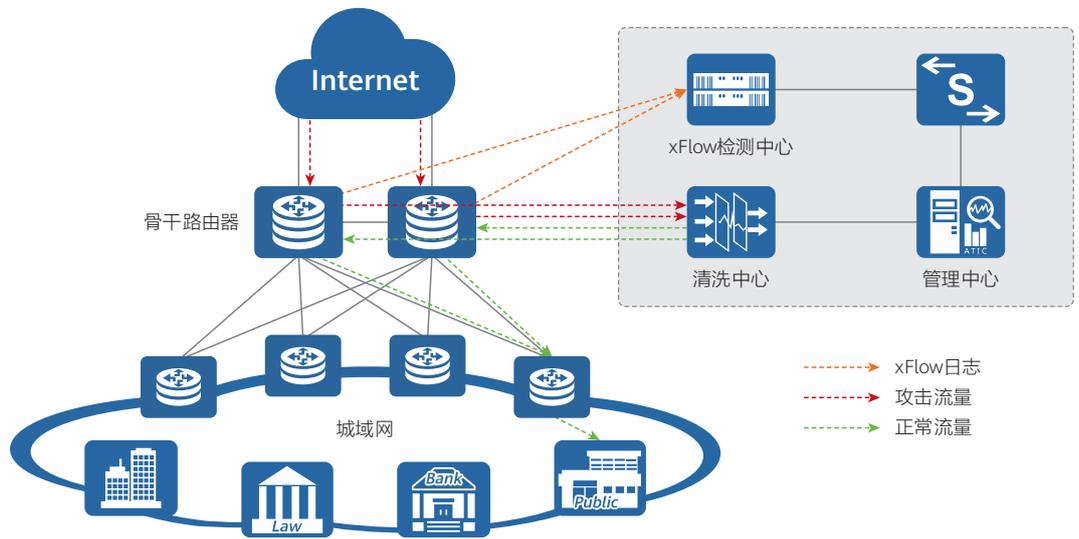
- 基于租户业务、防护带宽提供差异化防护及报表管理
- 开放API、SYSLOG日志满足第三方运营平台防御策略和报表集成

典型场景

城域网防护

随着大流量DDoS攻击泛滥, 挤占运营商网络价值带宽, 企业投诉增多; 同时, 针对DNS系统的DDoS攻击频发, 危及网络基础设施可用性。运营商网络部署DDoS攻击缓解系统, 保护网络管道及基础设施可用性成为刚需。

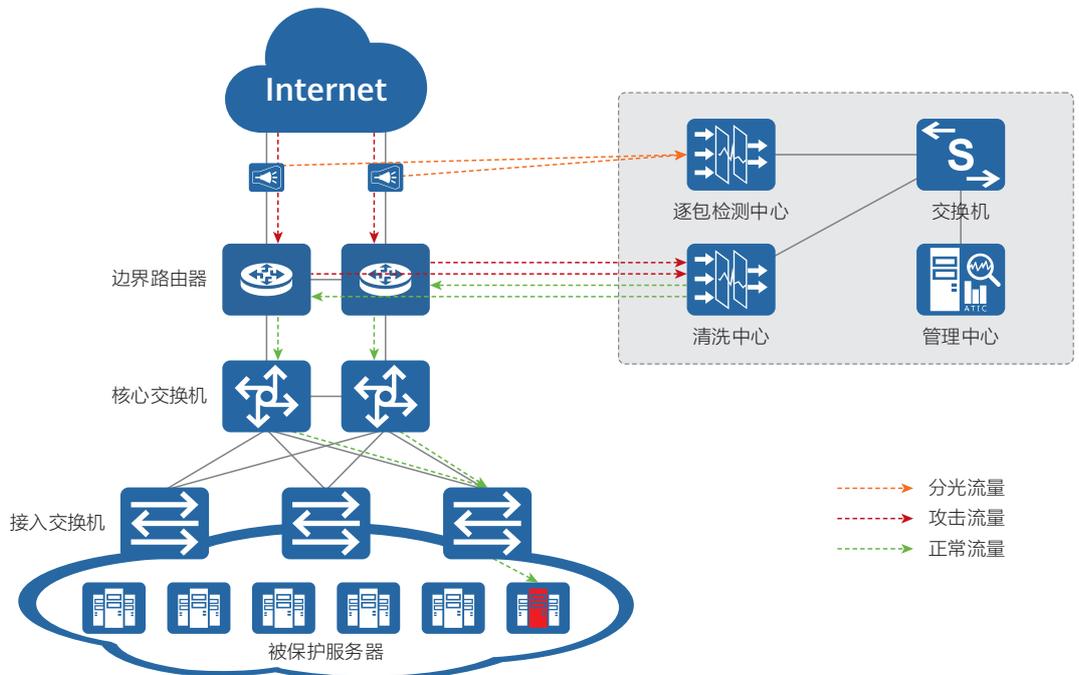
如图所示, xFlow检测设备实时采集和分析路由器产生的xFlow日志, 对防护网络进行DDoS攻击检测。当检测到攻击, 检测中心上报管理中心异常告警, 触发清洗中心对被攻击IP发布引流路由, 流量被牵引至清洗中心进行精细化过滤, 丢弃攻击流量, 干净的业务流量再被回注到原有网络。



数据中心防护

行业内的恶性竞争导致数据中心成为DDoS攻击的重灾区。攻击发生时，不仅被攻击IP的业务不可用；严重时，危及数据中心网络基础设施可用性。网络边界DDoS防御是数据中心必备的第一道安全屏障。

如图所示，AntiDDoS设备旁路部署在网络边界，将防护网络流量1:1分光或镜像到检测中心进行逐包实时检测，一旦发现DDoS攻击，检测中心上报异常告警到管理中心，管理中心触发清洗中心发布引流路由，将被攻击IP的流量牵引到清洗中心。清洗中心过滤掉攻击流量，将干净流量回注到网络。整体方案无单点故障，且仅需要牵引被攻击IP到清洗中心，方案可靠性最高。



增值运营

管理中心支持租户级的DDoS防护服务运营功能。系统基于防护对象进行防御策略配置和报表呈现，防护对象可和租户一一对应，方便ISP基于租户业务类型和防护带宽提供差异化的DDoS防护服务。管理中心支持丰富的Restful API和第三方运营平台实现防御策略对接；并支持多维度的Syslog日志和第三方运营平台对接，提供攻击日志、防御效果报表展示。

规格清单

DDoS防御功能

畸形报文防御：

支持LAND、Fraggle、Smurf、Winnuke、Ping of Death、Tear Drop、TCP Error Flag等攻击防御。

扫描窥探型攻击防御：

支持端口扫描、地址扫描、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攻击防御。

网络泛洪攻击防御：

支持SYN Flood、SYN-ACK Flood、ACK Flood、FIN Flood、RST Flood、TCP Fragment Flood、TCP Malformed Flood、UDP Flood、UDP Malformed、UDP Fragment Flood、IP Flood、ICMP Fragment Flood、ICMP Flood、Other Flood等常见网络层泛洪攻击防御；支持扫段攻击、脉冲攻击防御。

会话层攻击防御：

支持真实源SYN Flood、真实源ACK Flood、TCP连接耗尽、Sockstress、TCP空连接等常见会话层攻击防御。

UDP反射攻击防御：

支持NTP、DNS、SSDP、CLDAP、Memcached、Chargen、SNMP、WSD等常见UDP反射放大攻击静态过滤规则；支持动态生成过滤规则防御新型UDP反射放大攻击。

TCP反射攻击防御：

支持基于网络层特征创建静态过滤规则；
支持动态生成TCP反射攻击过滤规则。

WEB、APP、API应用层攻击/HTTP CC攻击防御：

支持基于行为分析防御高频HTTP应用攻击/HTTP CC；
支持基于机器学习防御低频HTTP应用攻击/HTTP CC；
支持基于行为分析防御慢速HTTP攻击，包括HTTP Slow Header、HTTP Slow Post、RUDY、LOIC、HTTP Multi-Methods、HTTP Range放大、HTTP空连接等。

WEB、APP、API加密应用层攻击/HTTPS CC/TLS加密攻击/QUIC Flood防御：

支持高频HTTPS/TLS加密攻击防御；
支持慢速TLS不完整会话及空连接防御；
支持QUIC Flood防御。

DNS应用攻击防御：

支持DNS Malformed、DNS Query Flood、NXDomain Flood、DNS Reply Flood、DNS缓存投毒防御；
支持源限速、域名限速。

SIP应用攻击防御：

支持SIP Flood/SIP Methods Flood防御，包括：Register Flood、Deregistration Flood、Authentication Flood、Call Flood等攻击防御；
支持源限速。

自定义过滤规则：

支持自定义本地软件及硬件过滤规则，支持自定义BGP flowspec过滤规则执行远端过滤，可定义的字段包括：源/目的IP、报文长度、IP协议、IP载荷、源/目的端口、TCP-Flag、TCP载荷、UDP载荷、ICMP载荷、DNS域名、HTTP URI、HTTP User-Agent字段、SIP caller字段、SIP callee字段等。

地理位置过滤:

阻断策略支持自定义, 海外到国家, 国内到省。

共栈防御:

支持IPv4/IPv6共栈DDoS攻击防御。

防御策略智能调优:

支持攻击流量快照及防御效果评估;

支持防御策略自动调优;

支持攻击自动取证;

支持云端策略模板同步。

基线学习:

支持动态流量基线学习, 支持智能降噪, 避免基线污染, 学习周期可配。

抓包取证:

支持基于攻击事件自动抓包和自定义ACL抓包, 支持抓包文件在线解析分析、溯源及下载本地分析。

管理与报表功能

管理功能:

- 支持多台AntiDDoS设备统一策略管理、性能监控、告警管理;
- 支持分权分域管理用户权限;
- 支持攻击事件通过短信、声音、邮件通知;
- 支持日志审计及发送第三方转储。

报表功能:

- 支持多维度的流量统计分析, 包括流量对比、流量TOPN、协议分布等;
- 支持多维度的攻击事件分析, 包括攻击详情、攻击TOPN、攻击事件TOPN等;
- 支持多维度的攻击态势分析, 包括攻击类型分布、流量峰值分布、持续时间分布等;
- 支持扫段攻击防御效果报表查询;
- 支持攻击源报表查询;
- 支持报表导出。

增值运营:

- 支持自定义防护对象, 配置客户化防护地址段和防护带宽;
- 支持客户化防御策略;
- 支持客户化报表;
- 支持租户级portal。

第三方平台对接:

- 支持基于syslog实现日志和报表对接;
- 支持基于Restful API实现防御策略对接。

部署模式与引流回注

部署模式:

- 支持直路部署、旁路静态引流部署、旁路逐包检测动态引流部署、旁路xFlow检测动态引流部署。

引流回注:

- 引流功能: 支持基于策略路由、BGP等方式的静态引流; 支持基于BGP的动态引流。
- 回注功能: 支持Layer-2回注、静态路由回注、策略路由回注、GRE Tunnel回注、SRv6回注、MPLS LSP/VPN回注等多种回注方式。

接口与硬件参数

型号	AntiDDoS12004	AntiDDoS12008	AntiDDoS12016
接口			
主控槽位	2		
扩展槽位	4	8	16
接口板	<ul style="list-style-type: none"> 24端口10GBase-SFP+ + 2端口40G/100GBase-QSFP28 48端口10GBase-SFP+ 	<ul style="list-style-type: none"> 24端口10GBase-SFP+ + 2端口40G/100GBase-QSFP28 48端口10GBase-SFP+ 4端口400GBase-QSFP 12端口40G/100GBase-QSFP28+24端口10GBase-SFP+ (注: 默认开放4个接口, 如需更多接口容量, 请购买100G接口扩容RTU进行扩容, 最大支持扩容2个100GE接口)	<ul style="list-style-type: none"> 24端口10GBase-SFP+ + 2端口40G/100GBase-QSFP28 48端口10GBase-SFP+ 4端口400GBase-QSFP 12端口40G/100GBase-QSFP28+24端口10GBase-SFP+ (注: 默认开放4个接口, 如需更多接口容量, 请购买100G接口扩容RTU进行扩容, 最大支持扩容2个100GE接口)
防御性能			
最大防御性能	400 Gbps	1.2 Tbps	2.4 Tbps
最大防御包速率	300 Mpps	900 Mpps	1800 Mpps
外形尺寸与重量			
宽×深×高	442mm×874mm×438mm (9.8U)	442mm×874mm×703mm (15.8U)	442mm×1033mm×1436mm (32.3U)
重量	DC机箱: 82.8kg (空机箱) AC机箱: 77.8kg (空机箱)	DC机箱: 101.8kg (空机箱) AC机箱: 95.8kg (空机箱)	DC机箱: 233.6kg (空机箱) AC机箱: 222.6kg (空机箱)
电源与运行环境			
供电方式	额定输入电压: <ul style="list-style-type: none"> 直流(DC): -48V/-60V 交流(AC): 220V; 50Hz/60Hz 高压直流(HVDC): 240V/380V 最大输入电压范围: <ul style="list-style-type: none"> 直流(DC): -40V ~ -72V 交流(AC): 176V ~ 290V; 45Hz ~ 65Hz 高压直流(HVDC): 188V ~ 288V/260V ~ 400V 		
最大功耗	4696W	10917W	21834W
电源冗余	N+1		
风扇冗余	N+1		
风道	前后风道		
长期工作环境温度	0°C ~ 40°C		
存储温度	-40°C ~ 70°C		
长期工作环境相对湿度	5% RH ~ 85% RH, 非凝露		
存储相对湿度	5% RH ~ 85% RH, 非凝露		

订购信息

型号	描述
主机	
ADS12004-AC-B04	AntiDDoS12004交流基本配置 (含交流机箱, 2*MPUD, 2*交流电源, 满配风扇)
ADS12004-DC-B04	AntiDDoS12004直流基本配置 (含直流机箱, 2*MPUD, 2*直流电源, 满配风扇)
ADS12008-AC-B04	AntiDDoS12008交流基本配置 (含交流机箱, 2*MPUD, 4*SFUA, 2*交流电源, 满配风扇)
ADS12008-DC-B04	AntiDDoS12008直流基本配置 (含直流机箱, 2*MPUD, 4*SFUA, 2*直流电源, 满配风扇)
ADS12016-AC-B00	AntiDDoS12016交流基本配置 (含交流机箱, 2*MPUB, 4*SFU16A, 4*交流电源, 满配风扇)
ADS12016-DC-B00	AntiDDoS12016直流基本配置 (含直流机箱, 2*MPUB, 4*SFU16A, 5*直流电源, 满配风扇)
业务处理板模块	
SPUB-ADS-01	AntiDDoS12000业务处理板B-01
SPUB-ADS-02	AntiDDoS12000业务处理板B-02
SPCB-ADS-01	AntiDDoS12000防护业务子卡B-01
SPCB-ADS-02	AntiDDoS12000防护业务子卡B-02
线路处理板模块	
LPUA-4DQ	4端口400GBase-QSFP-DD接口板
LPUA-12CQ24XS	12端口100GBase-QSFP28+24端口10GBase-SFP+接口板 注: 默认开放4个接口, 如需更多接口容量, 请购买100G接口扩容RTU进行扩容, 最大支持扩容2个100GE接口
LPUA-48XS	48端口10GBase-SFP+接口板
LPUA-2CQ-24XS	24端口10GBase-SFP+ + 2端口100GBase-QSFP28接口板
软件	
N1-AntiDDoS12000-F-Lic	N1-AntiDDoS12000 基础功能包, 每设备
N1-AntiDDoS12000-F-SnS1Y	N1-AntiDDoS12000 基础功能包, 1年软件订阅与保障年费, 每设备
LIC-ADS12000-DET	AntiDDoS12000检测License(10G)
LIC-ADS12000-CLN	AntiDDoS12000清洗License(10G)
LIC-ADS12000-LPU-400G	1*AntiDDoS400G接口扩容License(适用于4*400GE接口板)
LIC-ADS12000-LPU-100G	1*AntiDDoS100G接口扩容License(适用于12*100GE接口板)

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,华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息,恕不另行通知。

版权所有 © 华为技术有限公司 2023。保留一切权利。