华为HiSecEngine AntiDDoS12000系列产品

高效、极速、智能、敏捷

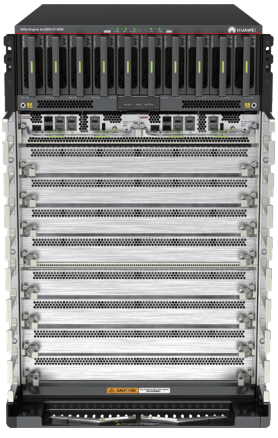
随着互联网的高速发展，黑客攻击手段不断演进，行业内的恶意竞争日趋激烈，促使DDoS攻击强度、频率和复杂度持续提升，企业网络边界防护面临新的挑战：

- 攻击流量越来越大，挑战企业防御成本；
- 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，提供毫秒级攻击响应；NP防御加速，单机T级防御，高效阻断网络层攻击；7层智能“滤板”，多维度行为分析及会话检测，精准识别各位复杂CC攻击；独创在线升级防御引擎，快速应对0-day DDoS。

产品图

AntiDDoS12004



AntiDDoS12008

HUAWEI

产品亮点

- **高效：**CPU协同NP防御加速，单机T级，业界最大
- **极速：**毫秒级攻击响应，业务“0”感知，业界最快
- **智能：**7层智能“滤板”100+攻击，业界最多
- **敏捷：**防御引擎在线升级，快速应对0-day DDoS；防御评估+策略自调优，防御自动驾驶，业界独创

方案功能

网络层DDoS防护

- 采用专业路由器硬件架构，硬件防御全面加速，单机DDoS防御性能最高可达2.4Tbps
- 全流量采集，逐包检测，60+流量模型，攻击响应最快可达毫秒级，快速阻断DDoS攻击，保障企业网络基础设施可用

应用层DDoS防护

- 采用智能防御引擎，7层“滤板”，提供最精准和全面的攻击防御
- 基于多维度行为分析及会话检查，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、DNS等关键业务系统

增值运营

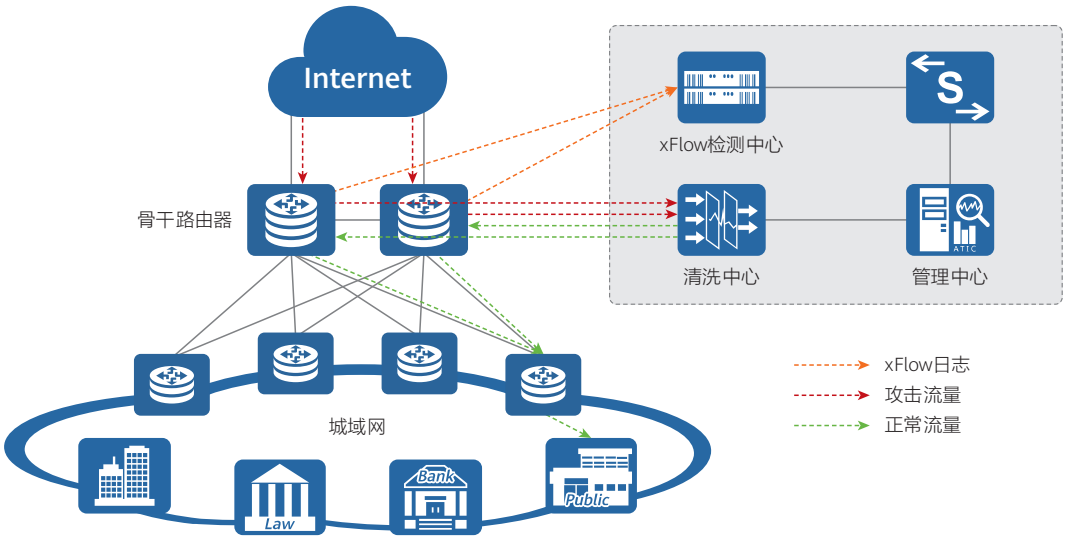
- 基于租户业务、防护带宽提供差异化防护及报表管理
- 开放API、SYSLOG日志满足第三方运营平台防御策略和报表集成

典型场景

城域网防护

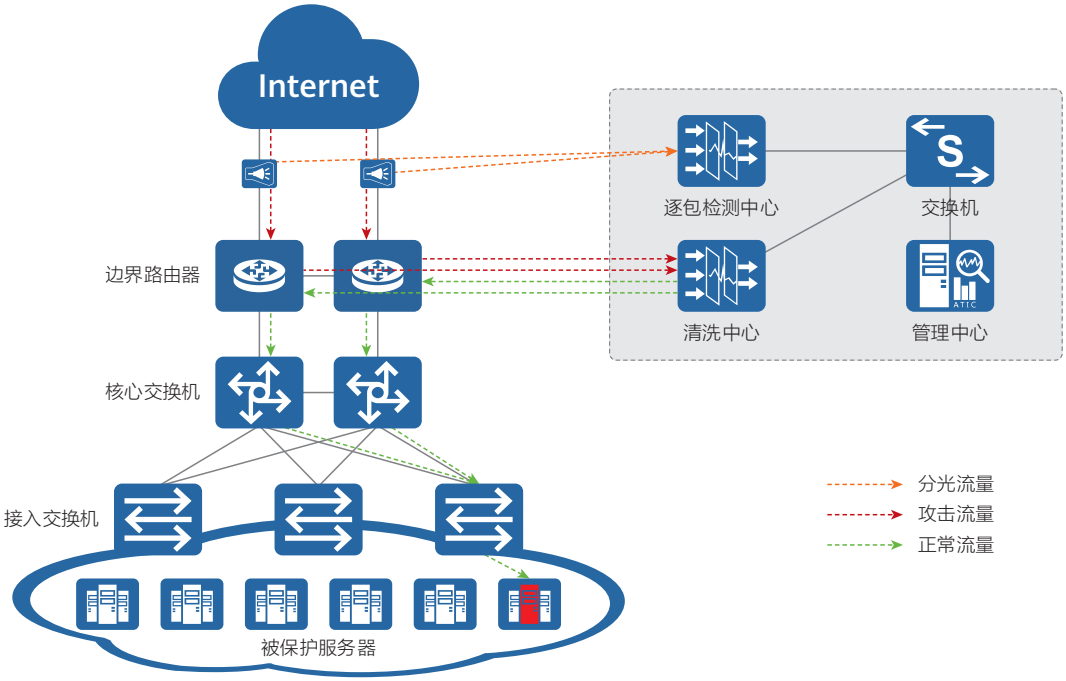
如图所示，xFlow检测设备实时采集和分析路由器产生的xFlow日志，实现防护网络攻击检测。当检测到攻击，通知管理中心触发清洗中心对被攻击IP发布引流路由，被攻击IP的流量被牵引至清洗设备进行精细化过滤，丢弃攻击流量，干净的业务流量再被送回到原有网络。

注：华为Netflow设备仅销售国内运营商市场



数据中心防护与运营

行业内的恶意竞争导致数据中心成为DDoS攻击的重灾区。攻击发生时，不仅导致被攻击的业务不可用；严重时，会使得整体网络瞬间瘫痪，危及所有租户业务系统可用性。DDoS防护成为数据中心网络边界防护刚需。



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，检测中心上报异常事件到管理中心，管理中心触发清洗中心发布引流路由，将被攻击IP的流量动态牵引到清洗中心。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。

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。系统支持丰富的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，和第三方运营平台实现攻击日志、防御效果展示报表对接。

规格清单

DDoS防护功能

协议滥用类攻击防护功能： LAND；Fraggle；Smurf；Winnuke；Ping of Death；Tear Drop；TCP Error Flag等攻击。	**HTTP应用防护功能：** 支持高频HTTP Flood防御； 支持慢速HTTP Slow Header、HTTP Slow Post、RUDY、LOIC、HTTP Multi-Methods、HTTP Range放大攻击、HTTP空连接防御等防御； 支持WordPress反射攻击防御。
扫描窥探型攻击防护功能： 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。	**HTTPS应用/TLS加密应用防护功能：** 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。
网络型攻击防护功能： SYN Flood、SYN-ACK Flood、ACK Flood、FIN Flood、RST Flood、TCP Fragment Flood、TCP Malformed Flood、UDP Flood、UDP Fragment Flood、IP Flood、ICMP Flood等常见网络层泛洪攻击防御； 支持真实源SYN、TCP连接耗尽、Sockstres、TCP空连接等常见会话层攻击防御。	**DNS应用防护功能：** 支持DNS Query Flood、NXDomain Flood、DNS Reply Flood、DNS缓存投毒攻击防御； 支持源限速、域名限速。
UDP反射攻击防护功能： 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。	**静态软件过滤规则：** IP报文过滤器：支持基于源IP、目的IP、报文长度、协议、Payload等IP报文字段过滤流量； TCP报文过滤器：支持基于源IP、目的IP、报文长度、源端口、目的端口、TCP-Flag、Payload等TCP报文字段过滤流量； UDP报文过滤器：支持基于源IP、目的IP、报文长度、源端口、目的端口、Payload等UDP报文字段过滤流量； ICMP报文过滤器：支持基于源IP、目的IP、报文长度、Payload等ICMP报文字段过滤流量； DNS报文过滤器：支持基于源IP、目的IP、报文长度、源端口、domain等DNS报文字段过滤流量； HTTP报文过滤器：支持基于源IP、目的IP、报文长度、源端口、URI、User_Agent等HTTP报文字段过滤流量； SIP报文过滤器：支持基于源IP、目的IP、报文长度、源端口、caller、callee等SIP报文字段过滤流量； 支持基于源IP、目的IP、源端口、目的端口、协议、TCP-Flag、报文长度等创建硬件过滤规则。
TCP反射攻击防护功能： 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。	
TCP回放攻击防护功能： 支持基于网络层特征创建静态过滤规则； 支持动态生成TCP回放攻击过滤规则。	
SIP应用防护功能： SIP Flood/SIP Methods Flood防范，包括：Register Flood，Deregistration Flood，Authentication Flood，Call Flood； 支持源限速。	
共栈防护功能： 支持IPv4/IPv6共栈DDoS攻击防御。	
智能行为分析： 支持通过智能分析技术进行真实源慢速攻击防御。	

引流与回注功能

引流功能：	回注功能：
支持手动引流；策略路由/BGP路由等多种自动引流方式。	支持静态路由回注；GRE Tunnel；Layer-2回注；策略路由回注等多种回注方式。

接口与硬件参数

型号	AntiDDoS12004	AntiDDoS12008
接口		
主控槽位	2	
扩展槽位	4	8
接口板	24端口10GBase LAN/WAN-SFP+ + 2端口100GBase-QSFP 48端口10GBase LAN/WAN-SFP+	24端口10GBase LAN/WAN-SFP+ + 2端口100GBase-QSFP 48端口10GBase LAN/WAN-SFP+ 18端口100GBase-QSFP
外形尺寸与重量		
高×宽×深	442mm×874mm×438mm (9.8U)	442mm×874mm×703mm (15.8U)
重量	DC机箱：81kg (空机箱) AC机箱：76kg (空机箱)	DC机箱：147.2kg (空机箱) AC机箱：144.6kg (空机箱)
电源与运行环境		
供电方式	额定输入电压： • 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： • 直流(DC)：-40V～-72V • 交流(AC)：176V～290V；45Hz～65Hz • 高压直流(HVDC)：188V～288V/260V～400V	
功率	整机最大功耗：2226W 整机典型功耗：1129W 整机静态功耗：771W	整机最大功耗：8496W 整机典型功耗：5007W 整机静态功耗：3278W
电源冗余	N+1	
工作环境温度	0℃～45℃ (长期)，-5℃～50℃ (短期)	
存储温度	-40℃～70℃	
工作环境相对湿度	5% RH～85% RH，不结露(长期)，5% RH～95% RH，不结露(短期)	
存储相对湿度	0% RH～95% RH	

订购信息

型号	描述
主机	
ADS12004-AC-B02	AntiDDoS12004交流基本配置(含交流机箱，2*MPU，2*交流电源，满配风扇)
ADS12004-DC-B02	AntiDDoS12004直流基本配置(含直流机箱，2*MPU，2*直流电源，满配风扇)
ADS12008-AC-B02	AntiDDoS12008交流基本配置(含交流机箱，2*MPU，4*SFUA，2*交流电源，满配风扇)
ADS12008-DC-B02	AntiDDoS12008直流基本配置(含直流机箱，2*MPU，4*SFUA，2*直电源，满配风扇)
业务处理板模块	
AntiDDoS12000-SPUB-ADS-01	AntiDDoS12000业务处理板1
AntiDDoS12000-SPUB-ADS-02	AntiDDoS12000业务处理板2
AntiDDoS12000-SPCB-ADS-01	AntiDDoS12000防护业务子卡1
AntiDDoS12000-SPCB-ADS-02	AntiDDoS12000防护业务子卡2
线路处理板模块	
LPUA-18CQ	18端口100GBase-QSFP+接口板
LPUA-48XS	48端口10GBase LAN/WAN-SFP+接口板
LPUA-2CQ-24XS	24端口10GBase LAN/WAN-SFP+ + 2端口100GBase-QSFP+接口板
管理软件	
AntiDDoS12000-F-Lic-N1	AntiDDoS12000基础功能包，每设备
AntiDDoS12000-F-SnS1Y	AntiDDoS12000 基础功能包，1年软件订阅与保障年费，每设备