华为HiSecEngine AntiDDoS1900系列产品

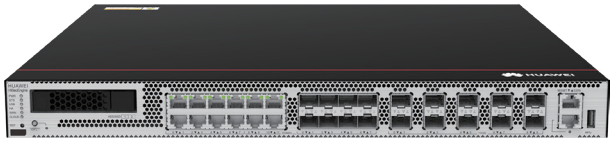
卓越性能、毫秒响应、精准防御、智能驾驶

随着互联网的高速发展，黑客攻击手段不断演进，行业内的恶意竞争日趋激烈，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AntiDDoS1900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，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；防御策略自动调优，防御全程智能驾驶。

产品图



AntiDDoS1905

AntiDDoS1908

HUAWEI

产品亮点

- **卓越性能：**CPU智能协同NP防御加速，高效阻断网络层攻击，防御成本低
- **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
- **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

- 多核分布式硬件架构，CPU智能协同NP防御加速，单G防御成本低
- 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

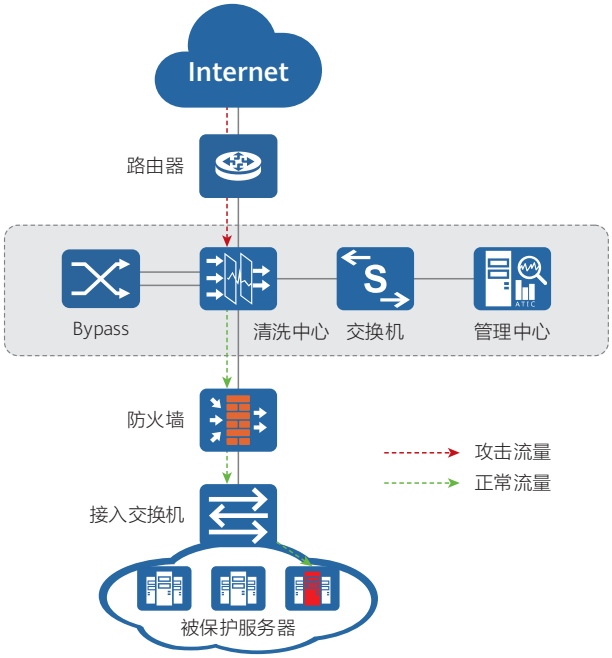
- 基于租户业务、防护带宽提供差异化防护及报表管理
- 开放API、SYSLOG日志满足第三方运营平台防御策略和报表集成

典型场景

企业网络防护

随着数字化转型的不断推进，企业网络面临越来越多的安全威胁，既要抵御网络层攻击，保护网络基础设施；又要防御应用层攻击，保护企业应用的可用性。

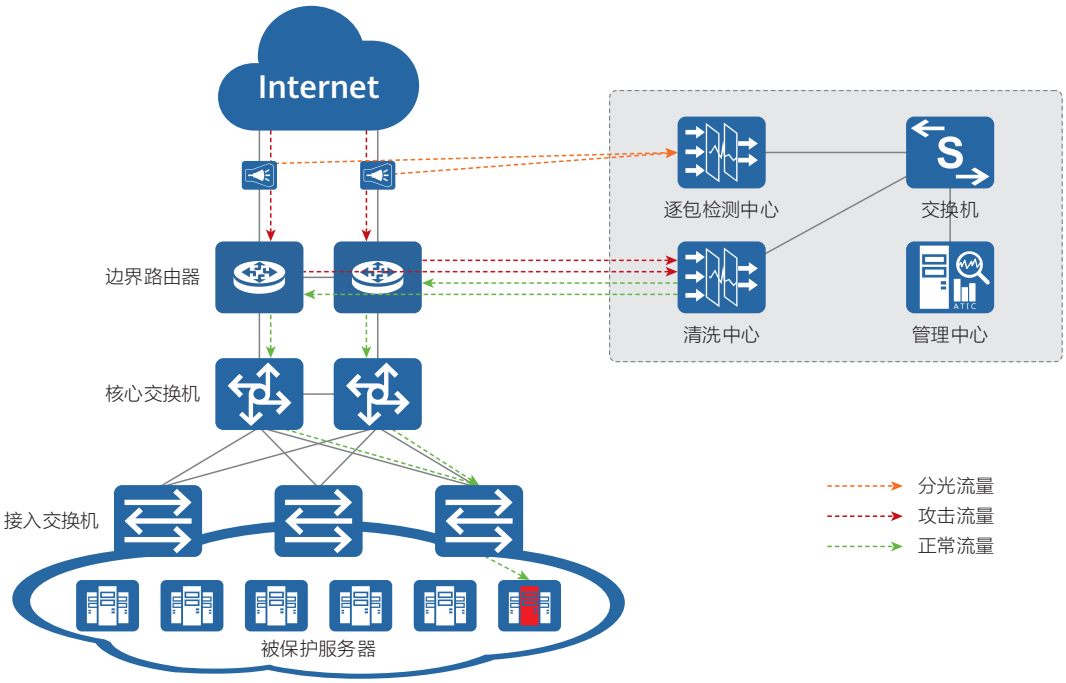
如图所示，清洗设备直路部署在企业网络边界，作为企业的第一道关卡，对进入企业的流量进行实时防御。



数据中心防护

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。

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。

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。

基线学习：
支持动态流量基线学习，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。	**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回注等多种回注方式。

接口与硬件参数

型号	AntiDDoS1905	AntiDDoS1908
接口		
标准接口	8×GE COMBO + 4×GE RJ45 + 4×GE SFP + 6×10GE SFP+	4×100G/40G+16×25G/10G(25G/100G COMBO)+8×10G/GE
功能形态	清洗或检测	
硬件bypass	内置单模光bypass插卡，外置单模多模bypass	外置单模多模bypass
性能		
最大防御吞吐	40 Gbps	80Gbps
最大防御包速率	50 Mpps	120 Mpps
外形尺寸与重量		
宽×深×高	442mm×420mm×43.6mm (1U)	442mm×600mm×43.6mm (1U)
重量	6.3kg (空配)	10.2kg (空配)
电源与运行环境		
供电方式	额定输入电压： • 交流 (AC)：100V～240V，50Hz/60Hz • 高压直流 (HVDC)：240V，DC 输入电压范围： • 交流 (AC)：90V～290V，45Hz～65Hz • 高压直流 (HVDC)：190～290V，DC	
最大功耗	222W	242W
电源冗余	1+1冗余备份	
风扇冗余	N+1冗余备份	
风道	前后风道	
长期工作环境温度	0°C～45°C	
存储温度	-40°C～70°C	
长期工作环境相对湿度	5% RH～95% RH，无冷凝	
存储相对湿度	5% RH～95% RH，无冷凝	
认证		
安全认证	电磁兼容性 (EMC) 认证 CB，CCC，CE-SDOC，ROHS，REACH&WEEE(EU)，C-TICK，ETL，FCC&IC，VCCI，BSMI	

订购信息

型号	描述
主机	
AntiDDoS1905-AC	AntiDDoS1905交流主机(8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+，1交流电源
AntiDDoS1908-AC	AntiDDoS1908-AC-交流主机(4*QSFP28 + 16*ZSFP+ + 8*SFP+，2交流电源)
License	
N1-AntiDDoS1000-F-Lic	N1-AntiDDoS1000基础功能包，每设备
N1-AntiDDoS1000-F-SnS1Y	N1-AntiDDoS1000基础功能包，1年软件订阅与保障年费，每设备
LIC-ADS1905-CLN10G	10G清洗能力(适用于AntiDDoS1905)
LIC-ADS1905-DET10G	10G检测能力(适用于AntiDDoS1905)
LIC-ADS1905-CLN20G	20G清洗能力(适用于AntiDDoS1905)
LIC-ADS1905-DET20G	20G检测能力(适用于AntiDDoS1905)
LIC-ADS1905-CLN40G	40G清洗能力(适用于AntiDDoS1905)
LIC-ADS1905-DET40G	40G检测能力(适用于AntiDDoS1905)
LIC-ADS1908-CLN10G	10G清洗能力(适用于AntiDDoS1908)
LIC-ADS1908-DET10G	10G检测能力(适用于AntiDDoS1908)