华为HiSecEngine AntiDDoS1900系列产品

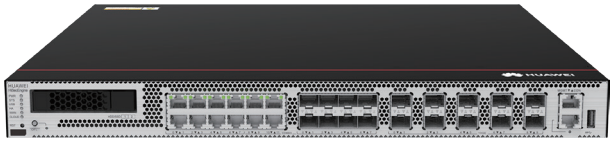
高效、极速、智能、敏捷

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AntiDDoS1900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，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，精准识别各类复杂CC攻击；独创在线升级防御引擎，快速应对0-day DDoS。

产品图



华为HiSecEngine AntiDDoS1905

HUAWEI

产品功能

网络层DDoS防护

- 多核分布式硬件架构，CPU智能协同NP防御加速，单G防御成本最低
- 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
- 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

灵活部署

- 直路部署，bypass插卡提供可靠性保障
- 旁路部署，多样化引流回注，满足多场景需求

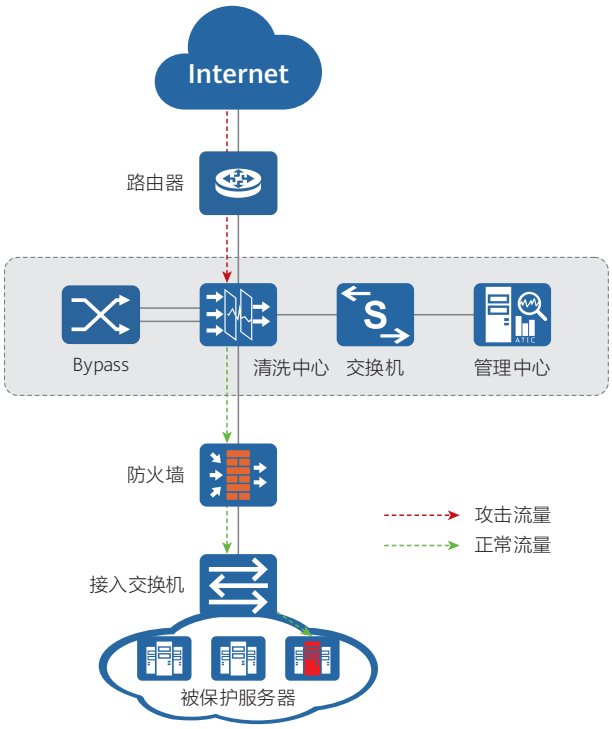
防护能力

- 1U设备，防护能力10-40Gbps，按需订阅

典型场景

场景1：企业网络防护

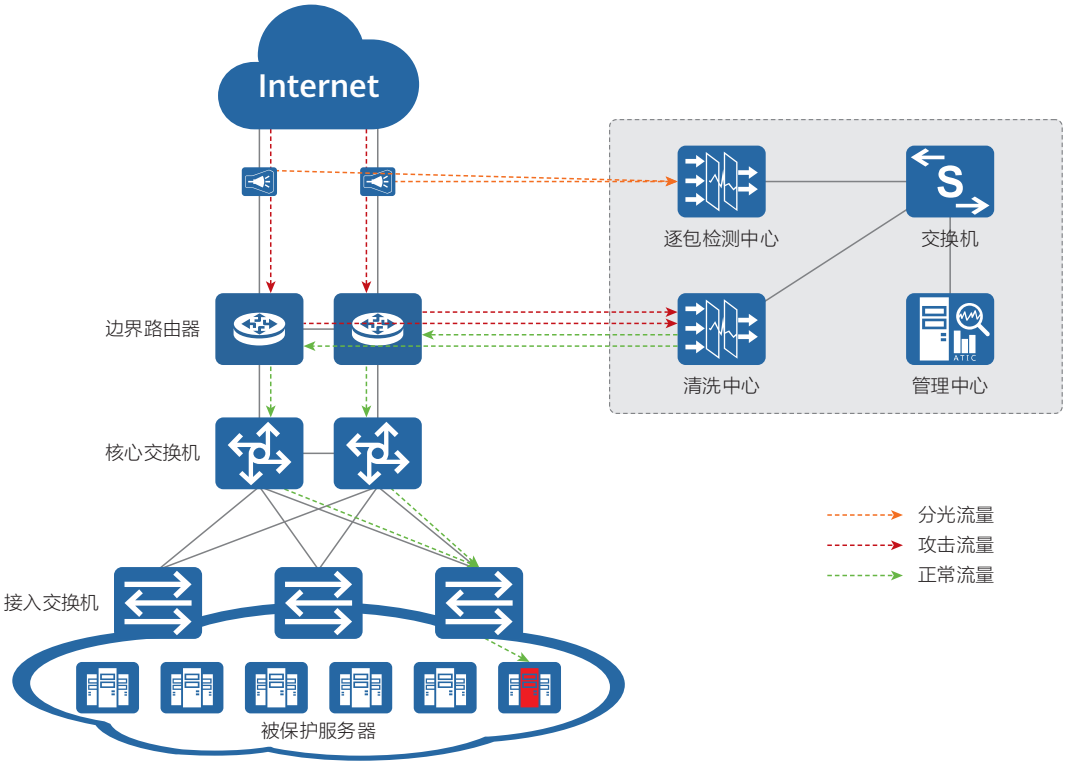
随着数字化转型的不断推进，企业网络面临越来越多的安全威胁，既要抵御网络层攻击，保护网络基础设施；又要防御应用层攻击，保护企业应用的可用性。



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。

场景2：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。

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。

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。

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。

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。

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：
支持通过智能分析进行真实源慢速攻击防御。

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。

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。

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。

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。

管理与报表功能

管理功能： 支持账号管理和权限分配功能；提供基于防护对象的防御策略配置和报表呈现；支持设备性能监控功能；支持抓包溯源与指纹提取功能；支持短信/声音/邮件告警功能；支持日志转储功能；支持动态流量基线学习。	**报表功能：** 清洗前后流量对比；流量TOPN统计；协议类型分布；攻击事件详情；攻击事件TOPN；攻击类型分布；攻击流量趋势；支持PDF等格式报表导出功能。

部署模式与引流回注

部署模式： 支持直路部署；支持旁路部署。	**引流回注：** 引流功能：支持手动引流；策略路由/BGP路由等多种自动引流方式。 回注功能：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	AntiDDoS1905
接口	
标准接口	8×GE COMBO + 4×GE RJ45 + 4×GE SFP + 6×10GE SFP+
部署模式	直路部署；旁路部署(静态引流)；旁路部署(动态引流)
功能形态	清洗或检测，使用命令行切换
Bypass插卡	支持
外形尺寸与重量	
尺寸(W×D×H)mm	442×420×43.6
重量	9.3kg
电源与运行环境	
供电方式	额定输入电压： AC：100 V to 240 V，50 Hz/60 Hz 最大输入电压范围： AC：90 V to 290 V，47 Hz to 63 Hz
功率	242W
电源冗余	AC：1+1冗余电源
工作环境温度	0°C～45°C (长期)，-5°C～55°C (短期)
存储温度	-40°C～70°C
工作环境相对湿度	5% RH～95% RH，不结露

型号	AntiDDoS1905
存储相对湿度	5% RH～95% RH，不结露
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 + 10*10GE SFP+，双电源)
管理中心	
AntiDDoS1000-F-Lic-N1	AntiDDoS1000基础功能包，每设备
AntiDDoS1000-F-SnS1Y-N1	AntiDDoS1000基础功能包，1年软件订阅与保障年费, 每设备
License	
LIC-ADS1905-CLN10G	AntiDDoS1905产品10G清洗能力
LIC-ADS1905-DET10G	AntiDDoS1905产品10G检测能力