

华为AntiDDoS8000 DDoS防御系统

T级性能，秒级响应，精准防护，增值运营

随着互联网和物联网的发展，DDoS攻击呈现出新的特点：

- 攻击越来越频繁，流量越来越大，2015年攻击流量峰值高达600Gbps
- 反射放大攻击横扫全球，直接拥塞链路
- 慢速应用型攻击精确打击互联网金融和游戏等业务系统

反射放大和慢速应用攻击日趋流行，分层防御方案成为抗DDoS首选。华为AntiDDoS8000 DDoS防御系统，运用大数据分析技术，针对60多种网络流量进行抽象建模，可以实现T级防护性能，秒级攻击响应速度和超百种攻击的全面防御。通过与华为云清洗中心联动，可以实现分层清洗，为用户提供从网络链路带宽到在线业务的全面防护。

产品图



AntiDDoS8030



AntiDDoS8080



AntiDDoS8160



方案功能

大流量DDoS防护

- 多核分布式硬件架构，结合大数据智能防护引擎，提供T级防护性能
- 秒级攻击响应时延，快速阻断攻击流量

应用型DDoS防护

- 全流量采集和3~7层的逐包分析，针对60多种网络流量进行抽象建模，提供最精准和全面的攻击检测
- 本地会话行为信誉、地理位置信誉和僵尸网络IP信誉等全方位的信誉体系，精确防御僵尸网络发起的应用型DDoS攻击，降低误判，提升用户体验
- 全面防护100多种攻击类型，保护用户Web服务、DNS服务、DHCP服务、VoIP服务等关键业务系统

DDoS防护运营

- 基于租户的自动和手动防护策略，防护手段全面
- 基于租户的独立报表统计和邮件发送，防护管理简单
- 支持租户自助Portal，增加租户粘性
- 支持规模运营，支持10万个租户，差异化运营

IPv4和IPv6双栈DDoS防护

- 支持IPv4和IPv6双栈DDoS防护

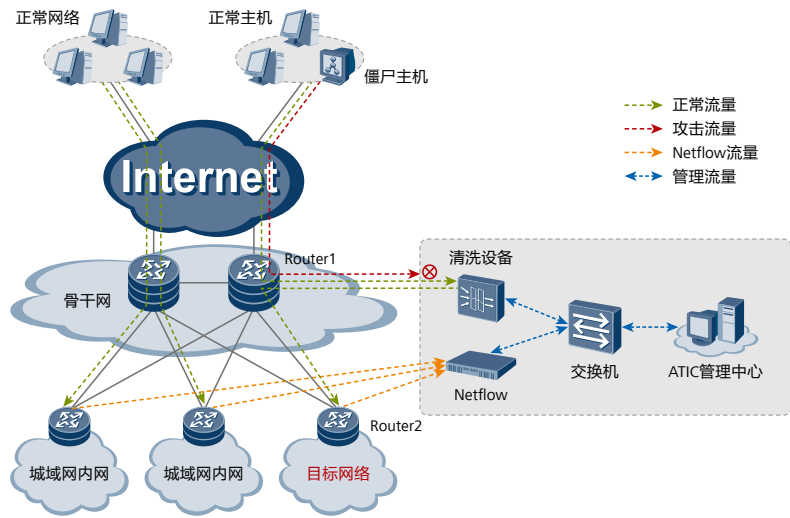
On-premise+Cloud分层DDoS防护

- On-premise设备实时在线，保护用户业务
- 链路拥塞时，On-premise设备可以自动发送云信令，启动云清洗，保护用户链路
- 2T+云清洗能力，全球10+清洗中心智能调度，分钟级攻击响应

典型场景

场景1：城域网防护

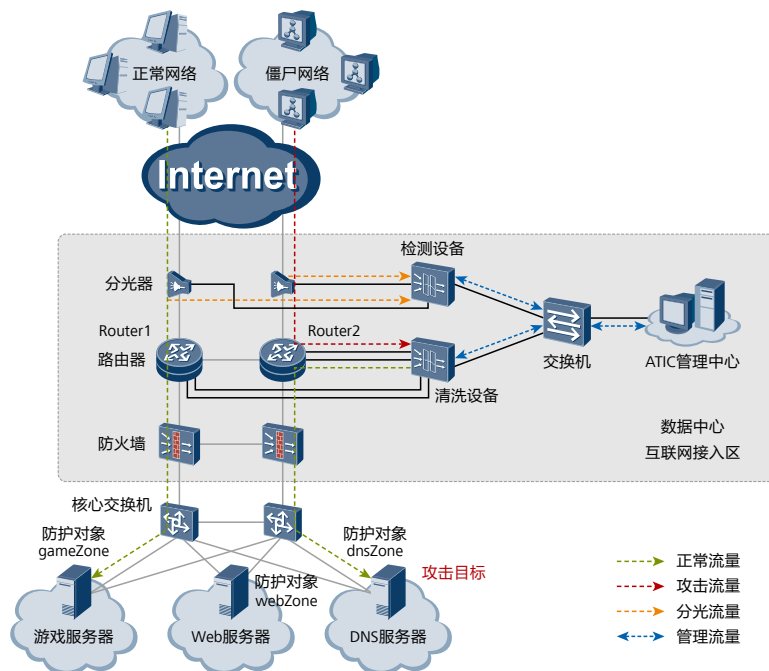
城域网是指在地域上覆盖一个城市范围，为城域多业务提供综合传送平台的网络，主要应用于大中型城市地区。提供通用和公共的网络构架，以高速有效地传输数据、声音、图像和视频等信息，满足用户日新月异的互连网应用需求。



如图所示，Netflow检测设备实时采集路由器Netflow日志，判定网络中的流量是否异常。发生流量异常时，通知清洗设备启动清洗。清洗设备旁路部署在核心路由器Router1上，对到达防护对象的流量进行清洗，清洗完成后，再将正常流量通过MPLS LSP方式回注到原链路Router2，由Router2继续转发，最终将流量送到防护对象。清洗设备仅有一个接口与Router1直连，主接口引流，子接口回注；接口充足的情况也可以其他接口回注。

场景2：数据中心防护与运营

数据中心（Internet Data Center，简称IDC）是网络基础资源的一部分，为互联网内容提供商、企业、媒体和各类网站提供大规模、高质量、安全可靠的数据传输服务和高速接入服务。数据中心主要提供DNS服务器、Web服务器、游戏等业务。近年来，来自外部互联网针对数据中心的DDoS攻击越来越多，包括重要用户服务器遭受攻击，数据中心链路带宽被占用，以及视频、游戏、网游等业务遭受的应用层攻击。



如图所示，清洗设备旁路部署在核心路由器Router1和Router2上，对到达防护对象的流量进行检测和清洗。由于是旁路部署，需要将到达防护对象的下行流量通过BGP引流方式实时牵引至清洗设备进行检测和清洗，清洗完成后，再将正常流量通过策略路由方式回注到原链路Router1和Router2，最终将流量送到防护对象。

ATIC管理中心支持安全运营功能。ATIC管理中心可以根据租户的业务特点，配置防护策略。攻击发生时，ATIC管理中心可以自动启动防护，同时通过邮件等方式发送告警信息。租户可以通过登陆Portal，自助查询攻击与防护情况。数据中心运营商可以基于租户设计商业模式，实现业务增值。

规格清单

DDoS防护功能

<p>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。</p>	<p>Web应用防护功能: HTTP Get Flood; HTTP Post Flood; HTTP Slow Header; HTTP Slow Post; HTTPS Flood; SSL DoS/DDoS; WordPress反射放大攻击; RUDY; LOIC等，支持报文合法性检查。</p>
<p>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。</p>	<p>DNS应用防护功能: DNS Query Flood; DNS Reply Flood; DNS缓存投毒攻击; 支持源限速。</p>
<p>网络型攻击防护功能: SYN Flood; SYN-ACK Flood; ACK Flood; FIN Flood; RST Flood; TCP Fragment Flood; UDP Flood; UDP Fragment Flood; IP Flood; ICMP Flood; TCP连接耗尽攻击; Sockstress; TCP重传攻击; TCP空连接攻击。</p>	<p>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。</p>
<p>UDP反射放大攻击防护功能: NTP反射放大; DNS反射放大; SSDP反射放大; Chargen反射放大; TFTP反射放大; SNMP反射放大; NetBIOS反射放大; QOTD反射放大; Quake Network Protocol反射放大; Portmapper反射放大; Microsoft SQL Resolution Service 反射放大; RIPv1反射放大; Steam Protocol反射放大。</p>	<p>过滤器功能: IP报文过滤器; TCP报文过滤器; UDP报文过滤器; ICMP报文过滤器; DNS报文过滤器; SIP报文过滤器; HTTP报文过滤器。</p> <p>地理位置过滤功能: 支持基于源IP的地理位置进行阻断、限速。</p>
<p>攻击特征库功能: RUDY, slowhttptest, slowloris, LOIC, AnonCannon, RefRef, ApacheKill, ApacheBench, 支持每周自动更新。</p>	<p>IP信誉功能: 全球最活跃的500万僵尸主机，支持每日自动更新，快速阻断攻击; 支持本地业务访问IP信誉，基于本地业务访问会话建立动态IP信誉，快速转发业务访问流量，提升用户体验。</p>

管理与报表功能

<p>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10万个防护对象（租户）；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。</p>	<p>报表功能: 清洗前后流量对比；流量TOPN统计；应用层流量对比和分布；协议类型分布；源IP地理位置流量统计；攻击事件详情；攻击事件TOPN（按照持续时间或报文数）；攻击类型分布；攻击流量趋势；DNS解析成功率；应用层TOPN流量统计（源IP、HTTP URI、HTTP HOST、DNS域名）；支持HTML/PDF/Excel等格式报表下载功能；支持邮件推送报表功能；支持定期生成天报、周报、月报、年报功能；支持租户自助Portal。</p>
--	---

引流与回注功能

<p>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。</p>	<p>回注功能: 支持静态路由回注；MPLS VPN回注；支持MPLS LSP回注；GRE Tunnel；Layer-2 回注；策略路由回注等多种回注方式。</p>
---	---

接口与硬件参数

型号	AntiDDoS8030	AntiDDoS8080	AntiDDoS8160
接口			
扩展槽位	3	8	16
扩展接口板	FW-LPUF-120, 2个子槽位	FW-LPUF-120, 2个子槽位 FW-LPUF-240, 2个子槽位	FW-LPUF-120, 2个子槽位 FW-LPUF-240, 2个子槽位
扩展子卡	24 × GE (SFP); 5 × 10GE (SFP+); 6 × 10GE (SFP+); 12 × 10GE (SFP+); 1 × 40GE (CFP); 1 × 100GE (CFP)		
外形尺寸与重量			
高 × 宽 × 深	DC: 175mm × 442mm × 650 mm (4U) AC: 220mm × 442mm × 650mm (5U)	620mm × 442mm × 650mm (14U)	1420mm × 442mm × 650mm (32U)

型号	AntiDDoS8030	AntiDDoS8080	AntiDDoS8160
重量	DC机箱: 15kg (空机箱), 30.7 kg (满配置) AC机箱: 25kg (空机箱), 40.7 kg (满配置)	43.2 kg (空机箱), 112.9 kg (满配置)	94.4 kg (空机箱), 233.9 kg (满配置)
电源与运行环境			
供电方式	额定输入电压: DC: -48 V AC: 175 V to 264 V; 50/60 Hz 最大输入电压范围: DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz	额定输入电压: DC: -48 V AC: 175 V to 264 V; 50/60 Hz 最大输入电压范围: DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz	额定输入电压: DC: -48 V AC: 175 V to 264 V; 50/60 Hz 最大输入电压范围: DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz
功率	1 × FW-LPUF-120 + 2 × ADS-SPUC-B + 2 × ADS-SPC-80-01: DC: 1066 W (典型), 1272 W (最大) AC: 1185 W (典型), 1414 W (最大)	3 × FW-LPUF-240 + 5 × ADS-SPUD-B + 10 × ADS-SPC-80-01: DC: 4025 W (典型), 4823 W (最大) AC: 4282 W (典型), 5132 W (最大)	6 × FW-LPUF-240 + 9 × ADS-SPUD-B + 18 × ADS-SPC-80-01: DC: 7387 W (典型), 8930 W (最大) AC: 7858 W (典型), 9500 W (最大)
电源冗余	DC: 双电源, 支持热插拔 AC: 双电源, 支持热插拔	DC: 4个PEM模块, 支持热插拔 AC: 4个PEM模块+1个外置交流电源框	DC: 8个PEM模块, 支持热插拔 AC: 8个PEM模块+2个外置交流电源框
工作环境温度	0°C ~ 45°C (长期), -5°C ~ 50°C (短期)		
存储温度	-40°C ~ 70°C		
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		
认证			
安全认证	电磁兼容性 (EMC) 认证 CB, Rohs, FCC, MET, C-tick, VCCI 认证		



订购信息

型号	描述
主机	
ADS8030-BASE-DC-01	AntiDDoS8030直流基本配置(含X3直流机箱, 2*MPU)
ADS8030-BASE-AC-01	AntiDDoS8030交流基本配置(含X3交流机箱, 2*MPU)
ADS8080-BASE-DC-01	AntiDDoS8080 200G直流基本配置(含X8直流机箱, 2*SRU200A, 1*SFU200C)
ADS8160-BASE-DC-01	AntiDDoS8160 200G直流基本配置(含X16直流机箱, 2*MPU, 4*SFU200B)
业务处理板模块	
ADS-SPUC-B	AntiDDoS8030业务处理板(基础板)
ADS-SPUD-B	AntiDDoS8080&AntiDDoS8160业务处理板(基础板)
ADS-SPC-20-00	20G DDoS防护业务子卡
ADS-SPC-40-00	40G DDoS防护业务子卡
ADS-SPC-80-00	80G DDoS防护业务子卡
线路处理板模块	
FW-LPUF-120	灵活插卡线路处理板(LPUF-120, 2个子槽位)
FW-LPUF-240	灵活插卡线路处理板(LPUF-240, 2个子槽位)
FW-6X10G-SFP+	6端口10GBase LAN/WAN-SFP+灵活插卡A
FW-1X100G-CFP	1端口100GBase-CFP灵活插卡A
FW-12X10G-SFP+	12端口10GBase LAN/WAN-SFP+ 灵活插卡A(P120-A)
E8KE-X-101-5X10GE-SFP+	5端口10GBase LAN/WAN-SFP+灵活插卡A(P101, 1/2宽, 占用两个子槽位)
E8KE-X-101-24XGE-SFP	24端口100/1000Base-X-SFP 灵活插卡(P101, 1/2宽, 占用两个子槽位)
E8KE-X-101-1X40GE-CFP	1端口40GBase LAN-CFP 灵活插卡(P100, 1/2宽, 占两个子卡槽位)
管理软件	
LIC-ADS-NOFA00	AntiDDoS管理中心基础功能汇总项

关于本文档

本文档仅供参考, 不构成任何承诺或保证。本文档中的商标、图片、标识均归华为技术有限公司或拥有合法权利的第三方所有。

版权所有 ©华为技术有限公司 2016。保留一切权利。