USG9500系列高端防火墙

华为技术有限公司

HUAWEI

USG9520

USG9560

USG9580

产品概述

随着云计算时代的到来，以“虚拟化技术”和“高速网络”为基石的云计算，被视为未来互联网时代发展的重要变革。随着云计算的落地实施，数据安全问题越来越受到人们的关注。IDG的一项调查显示66.7%调查对象认为安全问题是影响企业决策是否将业务切换到云的核心关键要素。

为助力企业和运营商将业务快速安全的迁移到“云”上，华为公司推出了云数据中心安全网关---USG9500系列产品,该系列产品包括USG9520、USG9560、USG9580三款产品。USG9500定位于保护云业务提供商、企业数据中心、以及企业的核心数据网络，它采用分布式软硬件设计，其I/O接口模块（LPU）以及业务处理模块（SPU）相互独立并按需配置，提供连接、保护和管理大型企业、云数据中心网络所必须的各项基本功能，通过将交换、路由、安全服务整合到统一的设备中，提供给用户卓越的性能保证、动态的策略调整、专业的安全防护。

产品说明

USG9500结合专用的多核处理芯片以及分布式硬件平台，采用革命性的“NP+多核＋分布式”架构，突破安全业务处理性能对CPU能力的限制，提供业界领先业务处理能力和业务扩展能力，同时所有部件均采用全冗余技术，提供双NP接口模块、双CPU业务处理模块、双控制模块、双电源、业务板负载等多项技术保证，使得设备达到核心路由器级别的高可靠性，从而进一步保证高速网络环境下的业务连续性。

USG9500采用动态的分布式并行处理技术，业务流量通过接口模块线速分布转发到多个专用业务处理模块，可按需配置，彻底解决不断增长的高速网络环境下的业务处理能力和数据转发能力相互矛盾的问题。该分布式技术在流量转发层面采用线速智能分流技术，所有数据流从首包开始就平均分配给各业务处理模块，无任何处理瓶颈，从而实现业务处理能力真正随业务模块线性倍增，从根本上支撑用户网络长久发展。

USG9500提供多种I/O模块，用户可以根据实际需求来灵活配置，并且I/O模块和业务处理模块采用相同的接口插槽，可通过不同I/O接口模块和业务处理模块的组合，匹配用户实际网络中对接口和性能的组合需求，为用户量身定制安全防护方案。USG9500系列产品包括USG9520、USG9560和USG9580三款产品，USG9580提供业界领先的安全防护性能和扩展能力，支持16个扩展槽位，整机性能随业务板卡增加线形提高。

- 业务处理模块（SPU）是USG9500产品的“心脏”，负责处理所有的业务。SPU采用同样的多核多处理器硬件，通过软件模块实现各种业务特性，SPU板与LPU板之间具有心跳检测机制，SPU板支持互相备份。当其中的一块业务板出现故障后。该业务板承担的所有功能将立即重新分发到其他业务板处理，不会导致后续业务中断。
- I/O接口模块（LPU）是USG9500产品的“手和脚”，负责对外连接和数据传递。LPU板上集成的高速网络处理器赋予了接口板足够的灵活性。防火墙相关的部分功能可以在接口板进行预处理，极大地减轻了SPU的压力。由于网络处理器针对各种报文转发进行了特别设计，比如具有专门的硬件查表协处理器，专门的位操作设计，因此在处理小报文时具有独特的优势，使得USG9500在处理现网混合流量时性能接近线速。通过LPU板和SPU板的配合，使USG9500可以高性能地处理复杂安全业务，同时具有了弹性的资源配置。

优势特性

驾驭云的力量：T级处理平台，最佳真实业务处理性能，运营商级可靠性

T级处理平台 – *弹性资源配备，性能线性倍增*

USG9500采用采用革命性的“NP+多核＋分布式”架构，该架构可以突破安全业务处理性能对CPU能力的限制，提供业界领先的业务处理能力和业务线性扩展能力。无需更换硬件机框，业务处理性能未来可以平滑升级到T级，在提供出色

的性能体验的同时，降低总体拥有成本。该产品采用华为成熟的VRP操作系统，该系统集成了基础的交换、路由、安全功能，在核心网、骨干网络等现网设备中，已积累了大量实践和应用。

最佳的真实业务处理性能 – *有效保障用户关键业务*

大型企业、数据中心的网络环境中，由于业务量剧增，高性能是基本的要求。USG9500采用了革命性的系统架构，在防火墙吞吐量、每秒新建连接数、最大并发连接数三个主要指标上处于领先地。由于USG9500采用了专有的分流技术，整机性能随SPU的配置数量线性倍增。当配置N块SPU时，USG9500最大防火墙吞吐量可达到N倍于单板的性能，防火墙性能指标业界领先， VPN吞吐量业界最高，DDoS防护种类业界最全、防护性能业界最佳。

在Internet混合业务流量模型（IMIX）下，USG9500仍然可达到惊人的200Gbps防火墙吞吐能力，随着下一代业务板卡的问世，整机IMIX吞吐量达到1T级别， 最大并发数达到9.6亿的天文数字，再次实现业界高端旗舰防火墙产品的历史性的突破。

运营商级可靠性 – *分层管理，全冗余，保障用户业务永续*

网络的安全一直都是企业运行的关键所在。为保证高速网络环境下的业务持续，USG9500采用独特的管理/监控/数据分层管理技术，提供物理元器件级可靠性保证；支持主/备、主/主组网、端口聚合、VPN冗余、业务板负载均衡等关键技术，提供网络可靠性保证；提供业界独有的双主控主备倒换技术，将防火墙的可靠性提高到高端路由器级别，保证关键节点可靠性一致。USG9500整机平均无故障时间长达二十五年，故障倒换时间小于1秒，真正保障业务持续稳定运行。

保护云的智慧 – 专业插板承载安全业务，超过1000种应用程序识别，持续的更新升级保障

专业插板承载安全业务 – *Anti-DDoS、IPS有效保护*

网络威胁、攻击始终影响着大企业、数据中心内部的网络安全。USG9500采用独立的Anti-DDoS插板和IPS插板，可以对内部网络做到有效防护。独立的Anti-DDoS插板，可以提供“七层净化”技术，秒级防御流量型、应用型和畸形报文等各种DoS/DDoS攻击，通过丰富的报表呈现，轻松管理Anti-DDoS业务。独立的IPS插板，基于赛门铁克专业的IPS引擎和先进的漏洞检测技术，可以实现业界领先的高检出率和低误报率。

由于独立插板的形态，IPS业务和Anti-DDoS业务并不影响普通防火墙的转发，可以有选择性的配置策略，对需要做检测的流量送到专业插板处理，实现智能保护的同时，保障业务的流畅运行。

超过1000种应用程序识别能力 – *应用安全可视可控*

数据中心海量业务应用，如何实现数据中心的网络数据的透明可视，进而实现可疑风险的控制，显得至关重要。USG9500的应用感知技术采用数据包协议分析和特征匹配技术，对网络层到应用层的数据进行全面分析，可以准确识别蠕虫流量、僵尸工具流量，同时支持P2P、VoIP、聊天、视频、游戏、股票等超1000种应用程序识别，帮助云计算数据中心客户清晰地了解进出流量的成份和比例，为流量策略调整提供参考；基于时间、应用、用户、带宽、连接数的多方位调控手段，可有效保障关键业务带宽，提升带宽利用率，阻断僵尸流量，防止蠕虫感染，让应用安全可视可控。

持续的更新升级保障 – *自动升级最新知识库*

华为专业的知识库研究和维护团队，实时研究包含移动终端应用在内的最新应用，每月数次更新知识库，用户可自由选择远程手工、自动更新，或者本地手工更新知识库，实现应用识别知识库持续更新升级。

适应云的敏捷：全面的虚拟化技术，支持NAT策略动态飘移

全面的虚拟化技术 – *支持更多的虚拟化*

数据中心在运营过程中，越来越多的从物理服务器往虚拟服务器迁徙、从单一数据中心到租用给多个租户的发展问题。USG9500系列产品，可以快速部署在数据中心出口，全面解决多用户数据安全隔离和互访的需求，同时可以基于动态策略，调整个各虚拟系统的带宽和会话业务资源。单台物理设备可虚拟为业界最大规模的4096台设备，所有的策略配置和管理可以基于每一个虚拟设备为单位调整。该产品支持虚拟系统下的Anti-DDoS攻击防御、IPS攻击防御保护、IPv6安全访问等，大大提高了业务组网能力，为数据中心创造定制化的部署策略，满足不同用户/租户的安全防护需求，可实现数据中心对安全业务的精细化管理。

DDoS安全防护上，USG9500采用基于内容感知技术的检测机制，深入分析报文的每个字节，精心打造的“七层净化”架构可以有效识别流量型攻击、应用型攻击、扫描窥测型攻击和畸形包攻击等多种类型。同时支持秒级攻击响应速度，业界最高的防御能力，轻松防御各种规模DDoS攻击。

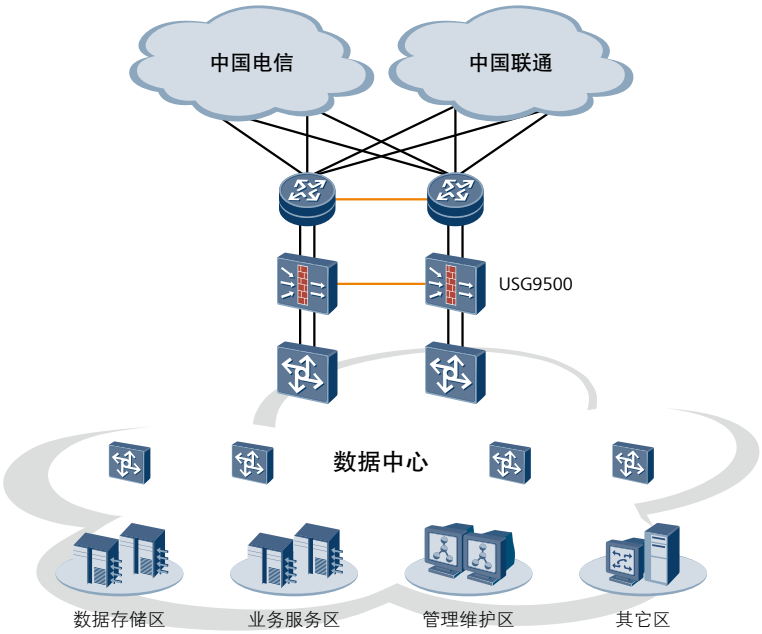
IPS攻击防御保护上，USG9500 采用了赛门铁克公司先进的IPS检测引擎和签名库，可以对系统漏洞、未授权自动下载、欺骗类应用软件、间谍/广告类软件、异常协议、P2P异常等多种威胁进行防护。其基于“漏洞”的签名规则，单条规格可以覆盖上千种攻击，并借助赛门铁克公司全球部署的蜜罐系统，实时捕获最新的攻击、蠕虫、木马等威胁，为产品提供于零日攻击的防御能力。为进一步提高IPS特性的实用性，USG9500采用内部旁路和专板专用的技术，将需要进行入侵防护的业务流量内部分流到专用业务处理模块处理，一方面提高业务处理能力，一方面使得这部分业务不会影响防火墙基本业务，保证业务持续稳定。

IPv6安全访问上，USG9500支持IPv6路由，IPv6 ACL策略访问控制，IPv6 DDoS攻击防御，IPv6 IPSec安全接入，为用户成功向IPv6网络迁移提供安全的解决方案。同时提供全面的IPv4向IPv6过渡技术如：NAT44(4)、DS-Lite、6RD和NAT64，确保用户网络演进及业务过渡提供高效、灵活、节省、放心。

支持NAT策略动态飘移 – *支持更灵活的策略调整*

为满足IDC弹性地址分配，以及虚拟机飘移后安全策略能够随之动态调整需求，USG9500支持NAT策略动态调整技术（与华为管理平台配合），实现虚拟动态环境下安全防护。

应用场景



背景与挑战：

近年来随着企业数据规模大幅度膨胀，企业的核心关键业务转向数据中心，同时成为了黑客攻击的新焦点。数据中心在云计算时代，从早期的业务大集中到目前基于虚拟化技术的服务器整合，这些变化对数据中心的安全带来了新的挑战。针对数据中心安全事件频繁的现象，其安全性已经成为数据中心能否提供高效、可用服务的关键。

客户需求：

大型数据中心业务有服务虚拟化、计算资源按需分配、数据访问量不断增大、出口带宽不断增长的特点，同时随着数据中心的不断整合，导致支撑业务的服务器、虚拟机数量不断增加，在发展为“云”数据中心后，业务访问海量增长，远程访问规模不断膨胀，不同业务或者租户需要提供独立的安全业务平面，数据中心内流量监控管理更加复杂，同时也吸引了更多非法访问和攻击。这种趋势导致早期的出口安全设备在性能和功能上已经无法满足新的需求，成为数据中心的瓶颈。

解决方案：

如图所示，可以通过部署2台USG9500在大型IDC/VDC网络的入口，可以一台设备虚拟为多台设备，分配个不同的租户，且每个虚拟系统的带宽、会话资源可以按需个性化定制，每个虚拟系统隔离，外部网络和内部网络安全隔离。随着对数据量访问性能的要求增加，可以按需扩展业务板卡，而无需购买新的设备，降低每G功耗，实现业务平滑扩容。通过深度业务感知、流量日志溯源，与eLog日志系统配合，可以对安全日志分析，提供强大的日志报表功能，方便企业对于网络安全状况的了解和取证。通过扩展入侵防御板卡、Anti-DDoS板卡，可以阻止外部网络的病毒、攻击进入IDC内部网络。为了保证系统级的运行稳定性，可在出口处部署2台设备，可以采用Active-Active或者Active-Standby两种双机部署方案，提供毫秒级的业务倒换。

产品规格

项目	USG9520	USG9560	USG9580
扩展及I/O			
扩展槽位	3 (SPU+LPU)	8 (SPU+LPU)	16 (SPU+LPU)
主控槽位	2		
SPU类型	防火墙业务板、IPS业务板、Anti-DDoS业务板等		
接口模块类型	以太网：24 × GE / 2 × 10GE / 12 × GE / 4 × 10GE POS：OC192		
防火墙基本特性			
工作模式	透明模式、路由模式、混合模式		
应用层包过滤 (ASPF)	支持		
访问控制	支持		
状态合法性检测	支持		
黑白名单	支持		
虚拟防火墙	支持		
安全域划分	支持		
负载均衡	支持		
应用层协议识别	支持		
地址转换			
目的地NAT/PAT	支持		
目的地NAT位于作为入口处接口IP的相同子网中	支持		
目的地地址对应一个地址 (M:1)	支持		
目的地地址对应另一组地址 (M:M)	支持		
NO-PAT方式的地址转换	支持		
PAT方式的地址转换	支持		
源NAT-IP地址持久性	支持		
源地址池分组	支持		
源IP地址在接口子网范围外	支持		
NAT Server	支持		
双向NAT	支持		
NAT-ALG	支持		
无限地址扩展	支持		
基于策略的目的NAT	支持		
三元组NAT	支持		
DDoS攻击防护			
双向防护	支持		
SYN Flood	支持		
SYN-ACK Flood	支持		
FIN/RST Flood	支持		
UDP Flood	支持		
DNS Query Flood	支持		
HTTP Flood	支持		
ICMP flood	支持		
入侵防御			
状态协议特征	支持		
零配置 IPS	支持		
攻击检测机制	协议异常、流量异常、模式匹配		
攻击响应机制	丢弃连接、关闭连接、日志、电子邮件		
蠕虫防护	支持		
防御零日攻击	支持		
特洛伊木马防护	支持		
广告软件/键盘记录软件防护	支持		
Web/工具栏攻击	支持		
Web2.0攻击	支持		
下载所驱动的攻击	支持		
僵尸网络	支持		
防止受感染的系统散播攻击	支持		
侦听防护	支持		
复合攻击防护	支持		
基于漏洞的特征签名库	支持		
支持多级压缩文件	支持		
独立PDF检测引擎	支持		

项目	USG9520	USG9560	USG9580
自定义攻击特征	支持		
攻击编辑 (端口范围等)	支持		
流特征	支持		
状态协议特征	支持		
Overload protection	支持		
可防御攻击数量	8000+		
IPSec VPN			
DES/3DES/AES加密	支持		
MD-5和SHA-1验证	支持		
手动密钥、PKI (X.509)、IKEv2	支持		
完美前向保密性 (DH组群)	1, 2, 5		
防重放攻击	支持		
远程接入VPN	支持		
支持EAP认证	支持		
冗余VPN网关	支持		
高可用性			
主/备、主/主	支持		
配置同步	支持		
防火墙和IPSec VPN的会话同步	支持		
设备故障检测	支持		
链路故障检测	支持		
双主控业务倒换	支持		
用户身份验证和接入控制			
固有的(内部)数据库	支持		
RADIUS记账	支持		
基于Web进行验证	支持		
公共密钥基础架构 (PKI) 支持			
PKI 证书要求(PKCS 10)	支持		
支持证书颁发机构	支持		
自签署的证书	支持		
路由			
BGP路由	支持		
BGP对等体	支持		
BGP实例	支持		
OSPF路由	支持		
OSPF实例	支持		
RIP v2路由表	支持		
RIP v1/v2实例	支持		
动态路由	支持		
静态路由	支持		
基于策略的路由	支持		
FIB	支持		
路由叠代	支持		
IPv6			
状态过滤	支持		
OSPFv3	支持		
BGP4+	支持		
ISIS6	支持		
IPv6 ACL Standard	支持		
IPv6 ACL Extended	支持		
IPv6 接口统计	支持		
IPv6邻居发现安全 (SEND)	支持		
DS-Lite	支持		
NAT64	支持		
6RD	支持		
虚拟化			
最多安全区数	根FW：32个，虚拟FW：8个		
最多虚拟防火墙数	4096		
每个接口支持的最多VLAN数	4094		
虚拟防火墙带宽预分配	支持		

项目	USG9520	USG9560	USG9580
虚拟防火墙会话预分配	支持		
负载均衡			
根据路由权重负载分担	支持		
根据链路带宽负载分担	支持		
管理			
WebUI (HTTP和HTTPS)	支持		
命令行接口 (控制台)	支持		
命令行接口 (远程登录)	支持		
命令行接口 (SSH)	支持		
U2000及VSM网管系统	支持		
分级管理员	支持		
软件升级	支持		
配置回退	支持		
日志记录/监控			
结构化系统日志	支持		
SNMP (v2)	支持		
二进制日志	支持		
路由跟踪	支持		
日志服务器配套(eLog)	支持		
尺寸、电源、运行环境			
尺寸 (W×H×D)	442×650×175 (直流) 442×650×220 (交流)	442×650×620 (直流) 442×650×709 (交流)	442×650×1420 (直流) 442×650×1598 (交流)
重量	空机箱15kg (直流) 满　配32kg (直流) 空机箱25kg (交流) 满　配42kg (交流)	空机箱43.2kg (直流) 满　配113kg (直流) 空机箱64.4kg (交流) 满　配134.2kg (交流)	空机箱94.4kg (直流) 满　配229kg (直流) 空机箱136.8kg (交流) 满　配271.4kg (交流)
电源AC	90VAC~275VAC；推荐175VAC~275VAC		
电源DC	-72V～-38V，额定-48V		
最大功耗	1330W (直流) 1368W (交流)	3038W (直流) 3231W (交流)	5824W (直流) 6195W (交流)
工作环境温度	长期工作：0°C 至 45°C 短期工作：-5°C 至 55°C 存储：-40°C 至 70°C		
环境湿度	长期：5%RH ～ 85%RH，无凝结 短期：5%RH ～ 95%RH，无凝结 存储：0%RH ～ 95%RH，无凝结		
认证			
安全性认证	支持		
电磁兼容性 (EMC) 认证	支持		
CB认证	支持		
Rohs	支持		
FCC	支持		
MET	支持		
C-tick	支持		
VCCI	支持		

订购信息

USG9520主机	
USG9520-BASE-DC-02	USG9520直流基本配置(含X3直流机箱，2*MPU)-含HS通用安全平台软件
USG9520-BASE-AC-02	USG9520交流基本配置(含X3机箱，2*MPU，2交流电源)-含HS通用安全平台软件
FWCD00MPUD01	X3 主处理板(含2*CF和1*DDR DRAM)-含HS通用安全平台软件
USG9520-CHAS-AC-02	一体化交流机箱组件-5U
USG9520-CHAS-DC-02	一体化直流机箱组件-4U
USG9560主机	
USG9560-BASE-DC-02	USG9560直流基本配置(含X8机箱，2*SRU，1*SFU，4直流电源)-含HS通用安全平台软件
USG9560-BASE-AC-02	USG9560交流基本配置(含X8机箱，2*SRU，1*SFU，4交流电源)-含HS通用安全平台软件
USG9560-CHAS-DC-02	一体化直流机箱组件-14U(含两块电源滤波单元和四块直流电源)
E8KE-X8-SRUA-200	X8 200Gbps路由交换板A(含2*CF卡和1*DDR DRAM)-含HS通用安全平台软件
E8KE-X8-SFUC-200	X8 200Gbps交换网单元C-含HS通用安全平台软件

USG9580主机	
USG9580-CHAS-DC-02	一体化直流机箱组件-32U(含八块直流电源)
FWCD00MPUB00	X16 主处理板(含2*CF卡和1*DDR DRAM)-含HS通用安全平台软件
FWCD00SFU40B	X16 40Gbps交换网单元B-含HS通用安全平台软件
E8KE-X16-SFUC-200	X16 200Gbps交换网单元B-含HS通用安全平台软件
USG9580-BASE-DC-200	Secoway USG9580-SU9Z8DCBC-USG9580直流基本配置(含X16机箱，2*SRU，1*SFU，4直流电源)-含HS通用安全平台软件
USG9500通用业务板	
FWCD00SPUA01	业务处理单板-双CPU-含HS通用安全平台软件
FWCD00SPUA02	业务处理单板-四CPU-含HS通用安全平台软件
FWCD00SPCA01	业务处理插卡-双CPU-含HS通用安全平台软件
FWCD000IPS00	8G性能IPS业务板
LPUF-21灵活插卡线路板	
FWCD0LPUKD01	灵活插卡线路处理板(LPUF-21，两个子槽位) B-含HS通用安全平台软件
FWCD00L1XX01	1端口10GBase WAN/LAN XFP灵活子卡
FWCD00EBGF01	12端口100/1000Base-X SFP灵活子卡
FWCD00EBGE01	12端口10/100/1000Base-TX RJ45灵活子卡
FWCD0P1XBZ01	1端口OC-192c/STM-64c POS-XFP灵活插卡
E8KE-X-21-4X10GE-XFP	4端口10GBase WAN/LAN-XFP灵活子卡(占用两个子槽位)
LPUF-40灵活插卡线路板	
FWCD0LPUF40A01	灵活插卡线路处理板(LPUF-40，两个子槽位) A-含HS通用安全平台软件
FWCD00L2XX01	2端口10GBase LAN/WAN-XFP灵活插卡(P40)
FWCD00EFGF01	20端口100/1000Base-X-SFP灵活插卡(P40)
E8KE-X-40-4X10GE-XFP	4端口10GBase LAN/WAN-XFP灵活插卡(P40)
IPS特征库升级服务时间	
FWCS000IPS00	IPS特征库升级服务1年License-含HS通用安全平台软件
FWCS000IPS01	IPS特征库升级服务3年License-含HS通用安全平台软件
FWCS08GIPS00	IPS特性业务处理板数量-含HS通用安全平台软件
防火墙特性	
FWCS010GFW00	防火墙10G性能License-含HS通用安全平台软件
FWCS020GFW01	防火墙20G性能License-含HS通用安全平台软件
FWCS1T2GSW01	防火墙10G升级至20G性能License-含HS通用安全平台软件
DDOS管理中心	
FWCS10GDDD00	DDOS 检测10G性能License-含HS通用安全平台软件
FWCS10GDDC00	DDOS清洗10G性能License-含HS通用安全平台软件
FWCS20GDDD00	DDOS 检测20G性能License-含HS通用安全平台软件
FWCS20GDDC00	DDOS清洗20G性能License-含HS通用安全平台软件
FWCS10GDDU00	DDOS检测10G升级到20G性能License-含HS通用安全平台软件
FWCS10GDCU00	DDOS清洗10G升级到20G性能License-含HS通用安全平台软件
配套设备	
CR52-22-D	2.2m路由器双开门总装机柜
CR5M000CMU60	集中监控模块
FWCT001WIN00	Windows中文运行平台(服务器,加载Windows中文系统及补丁软件)-含操作系统License
NS19MKM00	服务器其它配件-键盘&鼠标(USB)-19英寸液晶显示器-最大象素1280*1024/75Hz 100~240VAC电源-无资料-黑色
CR52-PWRA-AC-DF	机柜用交流配电盒-2路或6路输入-6路(双3路)输出(6路20A双极空开)
USG9500-PWR-AC	交流电源模块
DDoS管理中心（非运营版）	
FWCS00NOFA00	DDOS管理中心-非运营版功能汇总项-含HS通用安全平台软件

华为技术有限公司

深圳市龙岗区坂田华为基地

电话: (0755) 28780808

邮编: 518129

版本号: M3-035027-20121203-C-1.0

www.huawei.com