USG9500系列

USG9500系列T级下一代防火墙

大数据时代，网络流量几何级数增长，网络接入方式灵活多样，全联接已经成为常态，业务形态按需扩展，眼镜、手表、甚至是家庭电器，健康检测产品等终端都在智能化，在与人类的活动建立起数字的联接。

人们足不出户，就可以畅享移动办公带来的效率和便利。但是，传统的安全结构却正在瓦解，联接技术要求更加敏捷和无处不在，同时又需要安全可靠和保护数据隐私，而保障安全可靠和数据隐私防护就要克服泛在化的安全漏洞、风险、防御持续恶意的入侵。安全已经成为ICT世界最重要和迫切的问题。

因此，在云服务提供商、大型数据中心和大型企业园区网络边界，迫切需要更换老的防火墙为高性能多业务的下一代防火墙，任何有类似需求的企业用户都应该尽快评估当前的防火墙设备在功能和性能上是否遇到了瓶颈，未雨绸缪，防患于未然。

产品图

USG9520

USG9560

USG9580

产品说明

USG9500系列产品包括USG9520、USG9560和USG9580三款产品，提供业界领先的安全防护性能和扩展能力，整机最大1.92 Tbps IMIX防火墙吞吐量与1.4 Tbps IPSec吞吐量。

USG9500结合专用的多核处理芯片以及分布式硬件平台，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，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。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接口模块（LPU）**负责对外连接和数据传递。I/O接口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，匹配用户网络对接口和性能的组合需求，量身定制安全防护方案。支持GE、10GE接口、40GE接100GE接口和跨板端口捆绑，可灵活适应大接口容量或高接口密度等不同的应用场景需求。

USG9500**业务处理模块（SPU）**负责处理所有的业务。SPU分为母板和扩展卡两部分，可灵活组合不同性能单板，采用多核多处理器硬件，通过软件模块实现各种业务特性。SPU板与LPU板之间心跳检测机制，SPU板间备份机制，保障业务板出现故障后,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。

优势特性

最精准的访问控制 — *基于ACTUAL的六维一体化防护*

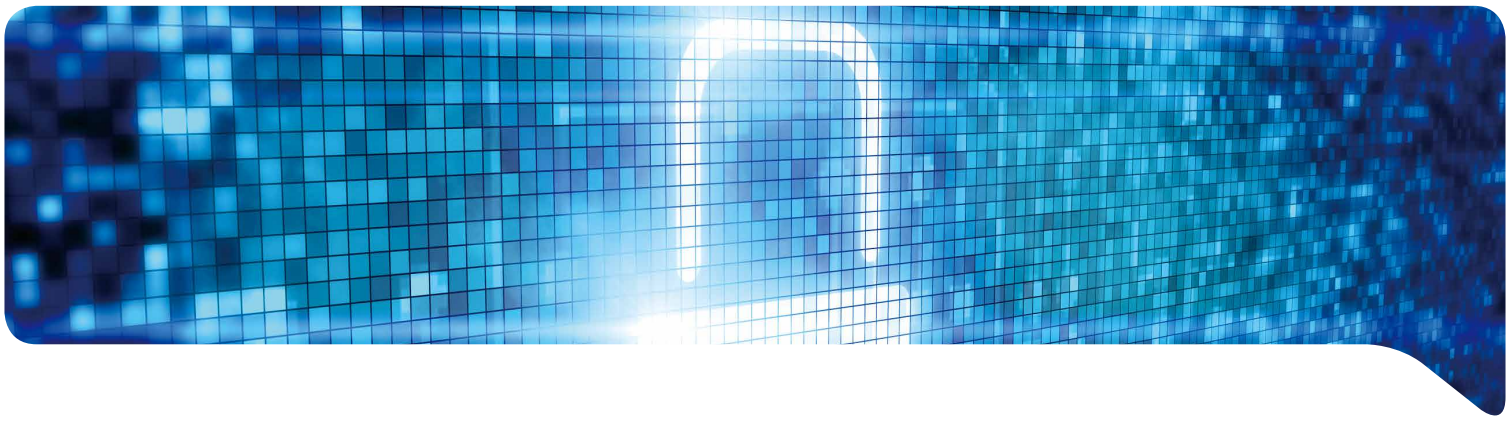
传统防火墙主要通过端口和IP进行访问控制，下一代防火墙的核心功能依然是访问控制。USG9500在控制的维度和精细程度上都有很大的提高：

- **一体化防护：**从应用、用户、内容、时间、威胁、位置6个维度进行一体化的管控和防御。内容层的防御与应用识别深度结合，一体化处理。例如：识别出Oracle的流量，进而针对性地进行对应的入侵防御，效率更高，误报更少。
- **基于应用：**运用多种技术手段，准确识别包括移动应用及Web应用内的6000+应用协议及应用的不同功能，继而进行访问控制和业务加速。例如：区分微信的语音和文字后采取不同的控制策略。
- **基于用户：**通过Radius、LDAP、AD等8种用户识别手段集成已有用户认证系统简化管理。基于用户进行访问控制、QoS管理和深度防护。
- **基于位置：**与全球位置信息结合，识别流量发起的位置信息；掌控应用和攻击发起的位置，第一时间发现网络异常情况。根据位置信息可以实现对不同区域访问流量的差异化控制。支持根据IP自定义位置。

最实用NGFW特性 — *一台顶多台设备，大幅降低TCO*

越来越多的信息资产连接到了互联网上，网络攻击和信息窃取形成巨大的产业链，这对下一代防火墙的防护范围提出了更高要求。USG9500具备全面的防护功能：

- **一机多能：**集传统防火墙、VPN、入侵防御、防病毒、数据防泄漏、带宽管理、上网行为管理等功能于一身，简化部署，提高管理效率。
- **入侵防护（IPS）：**超过5000种漏洞特征的攻击检测和防御。支持Web攻击识别和防护，如跨站脚本攻击、SQL注入攻击等。
- **防病毒（AV）：**高性能病毒引擎，可防护500万种以上的病毒和木马，病毒特征库每日更新。
- **数据防泄漏：**对传输的文件和内容进行识别过滤。可识别120+种常见文件类型，防止通过修改后缀名的病毒攻击。能对Word、Excel、PPT、PDF、RAR等30+文件进行还原和内容过滤，防止企业关键信息通过文件泄露。



- **SSL解密：**作为代理，可对SSL加密流量进行应用层安全防护，如IPS、AV、数据防泄漏、URL过滤等。
- **Anti-DDoS：**可以识别和防范SYN flood、UDP flood等10+种DDoS攻击，识别500多万种病毒。
- **上网行为管理：**采用基于云的URL分类过滤，预定义的URL分类库已超过8500万，阻止员工访问恶意网站带来的威胁。并可对员工的发帖、FTP等上网行为进行控制。可对上网记录进行审计。
- **安全互联：**丰富的VPN特性，确保企业总部和分支间高可靠安全互联。支持IPSec VPN、L2TP VPN、MPLS VPN、GRE等。
- **QoS管理：**基于应用灵活的管理流量带宽的上限和下限，可基于应用进行策略路由和QoS标签着色。支持对URL分类的QoS标签着色，例如：优先转发对财经类网站的访问。
- **负载均衡：**支持服务器间的负载均衡。对多出口场景，可按照链路质量、链路带宽比例、链路权重基于应用进行负载均衡。

最领先的“NP＋多核＋分布式”架构 *— 性能线性倍增，突破传统性能瓶颈*

USG9500采用核心路由器硬件平台，提供模块化部件，接口模块基于双NP处理器，保证接口流量线速转发；业务处理模块（SPU）基于多核多线程架构，每颗CPU都有应用加速引擎，结合华为对海量会话的并发处理优化技术，可确保NAT、VPN等多种业务高速并行处理，处理能力不受CPU处理性能的限制。LPU和SPU各司其职，通过部署多块SPU，实现整机性能线性倍增，为保护高速网络环境提供无以伦比的扩展性和灵活性，确保用户前期低成本投入，后期顺利扩容。

由于采用了革命性的系统架构，USG9500在防火墙吞吐量、最大并发连接数等主要指标上是目前业界性能最高的安全网关。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。USG9500最大防火墙整机吞吐量达到业界领先的1.92Tbps，最大并发连接数为25.6亿，虚拟防火墙数量可高达4095个，足以满足广电、政府、能源、教育等高端用户的高性能需求。

最稳定可靠的安全网关产品 *— 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在支持主-备、主-主组网、端口聚合、VPN冗余、业务板负载均衡等关键技术的同时，还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20万小时，故障倒换时间小于1秒，真正保障业务持续稳定运行。

最丰富的虚拟化 *— 应对云网络部署*

随着云计算时代的到来，以“虚拟化技术”和“高速网络”为基石的云计算面临安全的挑战。USG9500具有高吞吐量性能的同时提供了丰富的虚拟系统功能，支持资源虚拟化、配置虚拟化、转发虚拟化等多维度虚拟化功能，为云网络用户提供个性化的网络安全需求。资源虚拟化提供定制化的虚拟资源，不同虚拟系统可按需分配不同资源；管理虚拟化提供各虚拟防火墙独立配置个性化策略，日志管理和审计功能，提供按照租户要求的管理策略；转发虚拟化提供定制化的业务处理流程，各虚拟系统之间转发平面隔离，一个虚拟系统资源耗尽不影响其他虚拟系统正常运行，且逻辑隔离，确保各虚拟系统内部租户的数据安全。

产品规格

参数 \ 型号	USG9520	USG9560	USG9580
性能和容量			
防火墙吞吐量 (1518字节)	120Gbps	960Gbps	1.92Tbps
防火墙吞吐量 (IMIX混合流量)	120Gbps	960Gbps	1.92Tbps
最大并发会话数	1.6亿	12.8亿	25.6亿
IPsec VPN 性能 (AES)	120Gbps	700Gbps	1400Gbps
IPsec VPN 并发隧道	25.6万	100万	100万
扩展及I/O			
接口类型	支持 GE，10GE，40GE，100GE等常见接口		
业务板	防火墙业务板，应用安全业务板等		
尺寸、电源、运行环境			
尺寸 (W × D × H：mm)	442 × 650 × 175 (4U直流) 442 × 650 × 220 (5U交流)	442 × 650 × 620 (14U)	442 × 650 × 1420 (32U)
重量	空机箱15kg，直流 满配30.7kg，直流 空机箱25kg，交流 满配40.7kg，交流	空机箱43.2kg 满配112.9kg	空机箱94.4kg 满配233.9kg
电源AC	90VAC～264VAC；推荐175VAC～264VAC		
电源DC	-72V～-38V，额定-48V		
功耗	典型直流(DC)：1066W 典型交流(AC)：1185W 最大直流(DC)：1272W 最大交流(AC)：1414W	典型直流(DC)：4520W 典型交流(AC)：4282W 最大直流(DC)：4823W 最大交流(AC)：5132W	典型直流(DC)：7387W 典型交流(AC)：7858W 最大直流(DC)：8930W 最大交流(AC)：9500W
工作环境温度	长期工作：0°C 至 45°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		

注：性能数据是在理想环境下测试得出，实际情况会因现网情况不同而出现变化。

安全特性

基本防火墙功能
路由/透明/混合模式
状态检测
黑名单、白名单
访问控制
ASPF应用层包过滤
安全域划分

出站负载均衡
基于ISP的路由
智能出站探测
出站透明DNS代理
基于用户的流控
基于应用的流控
基于链路的流控
基于时间的流控

入站负载均衡
入站智能DNS
服务器负载均衡
基于应用的Qos

URL过滤
8500万URL地址库
80+分类
基于用户、IP、分类、次数等趋势和TOPN统计
URL过滤日志查询

虚拟私有网络(VPN)
DES，3DES，和AES加密
MD5和SHA-1认证
手工配置密钥，PKI (X 509) 以及IKEv2
前向安全性 PFS (DH组)
防重放攻击
支持传输模式、隧道模式
IPSec NAT穿越
DPD探测
EAP认证
EAP-SIM、EAP-AKA
VPN网关冗余
IPSec V6，IPSec 4 over 6，IPSec 6 over 4
L2TP隧道
GRE隧道

Anti-DDoS
SYN-flood，ICMP-flood，TCP-flood，UDP-flood，
DNS-flood攻击防御
Port-scan，Smurf，Tear-drop，IP-Sweep攻击防御
IPv6扩展头攻击防护
TTL 检测
TCP-mss检测
攻击日志输出

高可靠性
跨数据中心集群
主-主，主-备模式
双机热备切换 (华为冗余协议)
配置同步备份
框内业务板间备份
防火墙及IPSec VPN会话同步备份
设备故障检测
链路故障检测
双主控切换

管理
WebUI (HTTP和HTTPS)
命令行接口 (控制台)
命令行接口 (远程登录)
命令行接口 (SSH)
U2000及VSM网管系统
分级管理员
软件升级

配置回退
STelnet、SFTP

支持认证

安全性认证
电磁兼容性 (EMC) 认证
CB，Rohs，FCC，MET，C-tick，VCCI认证
ICSA实验室五大安全认证：Firewalls，IPS，IPSec，SLL-TLS，Anti-Virus

NAT/CGN

目的NAT/PAT
NAT NO-PAT
源NAT-IP address persistency
源IP地址池组
NAT Server
双向NAT
NAT-ALG
不受限IP地址扩展
基于策略的目的NAT
端口范围预分配
发夹访问模式
SMART NAT
NAT64
DS-Lite
6RD (IPv6快速部署)

业务感知

识别和控制超过6000种协议：
P2P，即时通讯，游戏，股票，VoIP，视频，流媒体，邮件，移动电话，网页浏览，远程接入，网络管理，以及新闻等。

AV防病毒

500万种病毒检测
基于流检测，性能更高
加密流量检测
按照病毒家族趋势和TOPN统计

PKI

在线获取CA证书
在线获取CRL
多级CA证书
支持PKCS#10证书协议
CA认证
SCEP、OCSP、CMPv2协议支持
自签名证书

入侵检测防御IPS

异常协议检测
自定义签名
知识库自动更新
零日攻击防御
蠕虫、木马、恶意软件攻击防御

网络和路由

POS/GE/10GE链路支持
DHCP中继/服务器
基于策略的路由
IPv4/IPv6 动态路由 (RIP/OSPF/ISIS/BGP)
域间/Vlan间路由
多链路聚合 (Eth-trunk，LACP)

虚拟系统

4095虚拟系统 (VSYS) 定义
VLAN虚拟化
安全域虚拟化
自定义虚拟资源
VFW间路由
基于虚拟系统的流量CAR
管理虚拟化
多租户虚拟资源隔离

日志记录/监控

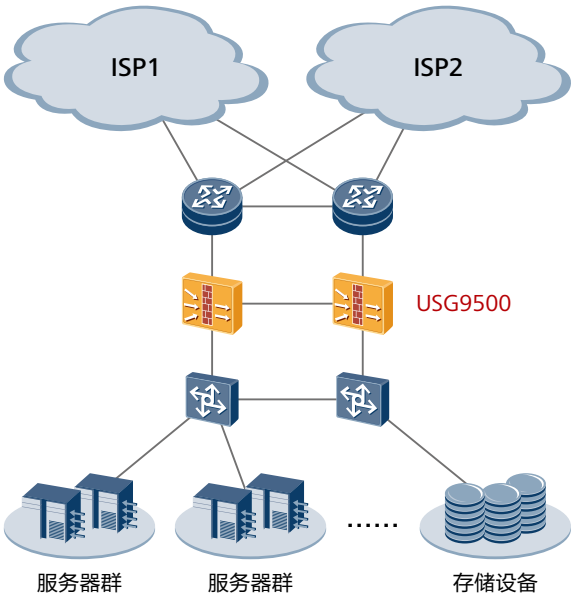
结构化系统日志
SNMP (V1/V2/V3)
二进制日志
路由跟踪
日志服务器配套 (LogCenter)

用户身份验证和接入控制

固有的 (内部) 数据库
RADIUS记账
基于Web进行验证

注：上述列举特性在USG9500系列产品中根据具体版本支持程度略有不同。具体信息请咨询华为工程师。

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/企业网络的入口，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LogCenter安全事件管理中心配合，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。

订购信息

	主机
USG9520-BASE-AC-51	USG9520交流基本配置(含X3交流机箱，2*MPU)
USG9520-BASE-DC-51	USG9520直流基本配置(含X3直流机箱，2*MPU)
USG9560-BASE-DC-51	USG9560直流基本配置(含X8直流机箱，2*SRU，1*SFU)
USG9580-BASE-DC-51	USG9580直流基本配置(含X16直流机箱，2*MPU，4*SFU)
	USG9500通用业务板
SPU-X3-40-E8KE	40G性能X3防火墙业务板
SPU-X8X16-80-E8KE	80G性能X8&X16防火墙业务板
SPC-S-40-E8KE	40G性能防火墙业务处理子卡
SPC-D-80-E8KE	80G性能防火墙业务处理子卡
SPU-X3-B	X3业务处理板(基础板)
SPU-X8X16-B	X8&X16业务处理板(基础板)
SPUA-H	增强型防火墙业务板A-60&80
SPUB-H	增强型防火墙业务板B-60&80
SPUA-M	增强型防火墙业务板A-20
SPUB-M	增强型防火墙业务板B-20
SPCA-H&M	增强型防火墙业务处理子卡A
SPCB-H&M	增强型防火墙业务处理子卡B
SPC-APPSEC-FW	应用安全业务处理子卡-含华为通用安全平台软件
SPCA-APPSEC-FW	增强型应用安全业务处理子卡A
SPCB-APPSEC-FW	增强型应用安全业务处理子卡B
SPU-X3-B2	X3业务处理板2(基础板)
	USG9500灵活插卡线路板
E8KE-X-LPUF-101	灵活插卡线路处理板(LPUF-101，四个子槽位)
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)
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)
FW-LPUF-120	灵活插卡线路处理板(LPUF-120，2个子槽位)-含华为通用安全平台软件
FW-LPUF-240	灵活插卡线路处理板(LPUF-240，2个子槽位)-含华为通用安全平台软件
FW-6X10G-SFP+	6端口10GBase LAN/WAN-SFP+灵活插卡A
FW-12X10G-SFP+	12端口10GBase LAN/WAN-SFP+灵活插卡A(P120-A)
FW-1X100G-CFP	1端口100GBase-CFP灵活插卡A
FW-20X1G-RJ45	20端口10/100/1000Base-RJ45灵活插卡
FW-3X40G-SFP	3端口40GBase-QSFP+灵活插卡

注：以上订购信息只是产品部分部件信息，具体信息请联系当地华为工程师。