

华为 Secoway USG9500 统一安全网关 配置原则

版权所有 © 华为技术有限公司 2012。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <http://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 概述	4
1.1 版本定位和软硬件介绍.....	4
1.2 新增报价项.....	8
1.3 版本配套关系.....	9
2 应用概述	10
3 产品配置	11
3.1 新增报价项的配置原则.....	11
3.2 典型配置及部件切换.....	12
3.3 SBOM 与 BBOM 的对应关系.....	13
3.4 产品配置.....	13
4 版本升级	16
4.1 升级路径.....	16
4.2 USG9500 V100R003 向 V200R001C01 升级.....	16
4.3 USG9500 V200R001C00 向 V200R001C01 升级.....	16

1 概述

1.1 版本定位和软硬件介绍

USG9500 系列高端防火墙,发展到 V2R1C01 软件版本,支持 USG9520、USG9560、USG9580 三种机框,版本定位为 2012 年到 2013 年全球主力销售版本。可以满足最大吞吐到 200G 的不同场景要求。

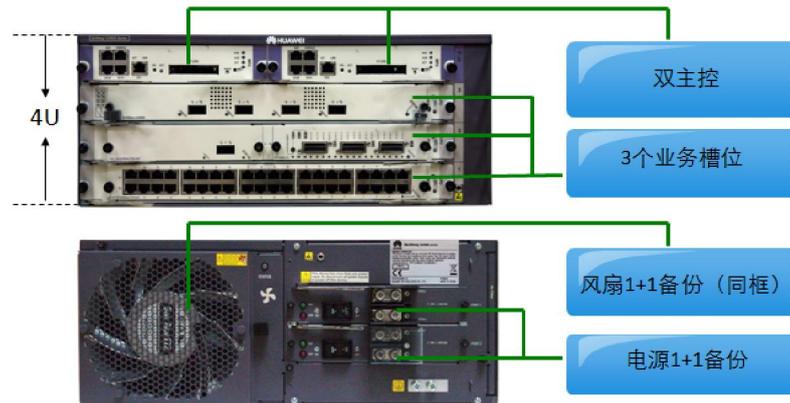


	USG9520	USG9560	USG9580
最大吞吐	40Gbps	100Gbps	200Gbps
槽位	3 x LPU/SPU 2 x MPU	8 x LPU/SPU 2 x SRU 1 x SFU	16 x LPU/SPU 2 x MPU 4 x SFU
高度	4U(DC)/5U(AC)	14U	32U

按照硬件部件介绍:

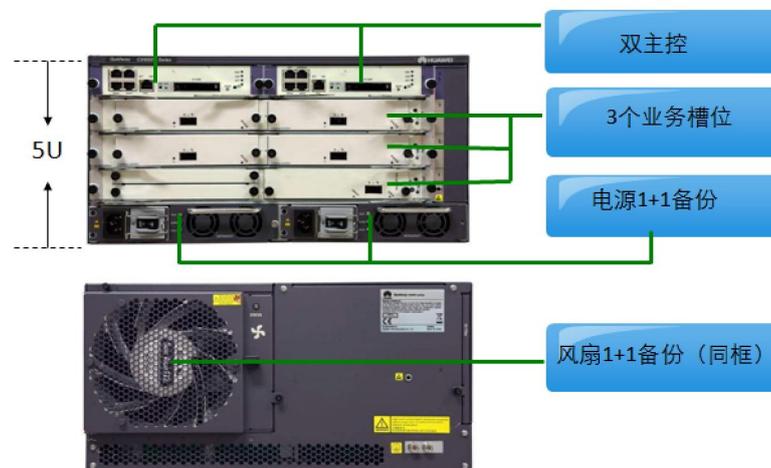
- USG9500 高端防火墙为分布式硬件架构,从报价项的角度来讲,一般包括机箱、主控板、交换板、电源、CF 卡、DDR 内存、接口板、业务板、光模块、光纤、license 等部件。

USG9520 直流机箱



- NE40E-X3直流机箱高4U
- 主控板、线卡前维护，电源、风扇等后维护

USG9520交流机箱



- USG9520交流机箱高5U
- 主控板、线卡、电源前维护，风扇后维护

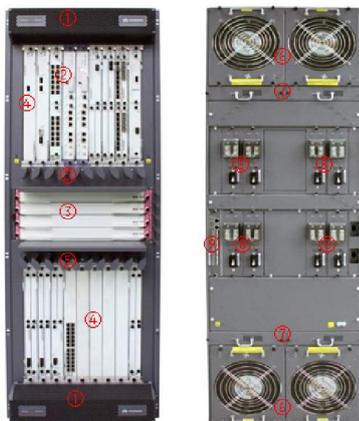
USG9560外观结构



- 高度: 14U
- 背板容量: 15T, 400G/Slot
- 交换容量: 1.44T
- 主控SRU: 1: 1备份
- 交换网: 2+1备份
- 风扇: 1+1备份
- 电源: 分区供电, 2+2备份

序号	模块单元	数量
①	进风口	× 1
②	SRU板	× 2
③	交换板	× 1 (共3块, 其中2块交换网板物理集成在主控板上)
④	接口板+业务板	× 8
⑤	走线区	× 1
⑥	风扇框	× 2
⑦	低频滤波单元	× 2
⑧	系统配电模块	× 4
⑨	独立监控单元	× 1

USG9580 外观结构



- 高度: 32U
- 背板容量: 30T, 400G/Slot
- 交换容量: 2.56T
- 主控MPU: 1: 1备份
- 交换网: 3+1备份
- 风扇: 2+2备份
- 电源: 分区供电, 4+4备份

序号	模块单元	数量
①	进风口	× 2
②	MPU板	× 2
③	交换板	× 4
④	接口板+业务板	× 16
⑤	走线区	× 2
⑥	风扇框	× 4
⑦	低频滤波单元	× 4
⑧	系统配电模块	× 8
⑨	独立监控单元	× 1

- 为了方便配置报价, 各款型号均对基本配置进行了“打包”, 形成 Bundle 模式, 例如 USG9520 交流配置。基本配置中, 包含了机箱, 主控板, 交换板, CF 卡, DDR 内存和电源, 里面的配置数量均按照可以安插的最大数量来配置, 以保证高可靠性和整机性能支撑。这里仅需要选择电源类型: 直流或者交流。
- 对于选择直流电源的情况下, 默认提供 25 米的直流电源线, 包含在报价项中, 不单独报价。但需要根据项目要求, 建议提前工勘, 了解直流机柜、机房放置位置等信息, 裸压端子需要根据现场施工情况制作。
- 接口板

配置接口板需要考虑两方面的因素：接口容量需求和接口类型。对于前者来说，需要和客户沟通对 USG9500 产品的接口容量需求，譬如 2 个万兆接口，4 个千兆接口。接口容量还有一个需求来自于产品自身，譬如双机部署场景，需要预留千兆接口用于双机互联。对于接口类型来说，同样需要和客户确认，与 USG9500 相连接的对端设备接口，是什么样的类型，万兆以太还是万兆 POS，千兆以太网光接口或者电接口。

USG9500 支持两种接口板，LPUF-21（20G 容量）和 LPUF-40（40G 容量），均支持 2 个灵活子卡的槽位；LPUF-21 支持 5 种灵活子卡，LPUF-40 支持 3 种灵活子卡。



注意：两种接口板的灵活子卡不能相互混插。

接口板类型	支持板卡类型	占用子卡槽位数
LPUF-21 (20G 处理能力, 2 子卡槽位)	12×GE 光灵活子卡	1
	12×GE 电灵活子卡	1
	1×10GE 灵活子卡	1
	1×10G POS 灵活子卡	1
	4×10GE 灵活子卡	2
LPUF-40 (40G 处理能力, 2 子卡槽位)	20×GE 光灵活子卡	1
	2×10GE 灵活子卡	1
	4×10GE 灵活子卡	1

● 业务板

配置业务板需要根据业务场景来选择不同的业务处理板，再考虑业务处理容量问题。业务板支持灵活配置，可更加细粒度地满足客户对性能的需求。

采用 LPUF-21 接口板配置时，接口板与业务板的数量比例为 1:1，采用 LPUF-40 接口板配置时，接口板与业务板的数量比例为 1:2。



USG9500 支持三类业务板：FW 板，DDoS 板，IPS 板。三种业务板的硬件形态基本相同。FW 板、DDoS 板有不带子卡的 10G 性能业务板和带子卡的 20G 性能业务板两种硬件形态，IPS 板只有带子卡的 8G 性能业务板一种硬件形态。

单块防火墙业务板吞吐量最大 20G (大包),新建 50 万/秒,并发 800 万。单块 IPS 业务性能为 8G (UDP 大包,实际业务能力低于此值)。单块 DDOS 业务板的防御能力为 20G (UDP 大包)。可根据性能需要线性叠加配置,即 N 块业务板性能为单块业务板性能的 N 倍。

业务板配置使用时,有部分限制,请注意不同机框槽位数限制等。

下列业务可能涉及软件 License 支持:

板卡	功能	指标	备注
FW 板	IPSec	6G/12G	涉及 VPN 规模 license
	CGN	NAT64、DS-Lite、6RD	涉及 CGN 功能 license, NAT64、DS-Lite、6RD 需要分别申请
IPS 板	IPS	8G	当配置 IPS 板时,至少需要一块 FW 板才能使用
Anti-DDoS 板	清洗/检测	10G/20G	当 DDoS 与 FW 业务板混插时,无需检测板。DDOS 板使用时需购买 license

详细销售指导信息请参阅销售指导。

1.2 新增报价项

USG9500 V200R001C01 版本新增如下硬件报价项:

编码	型号	描述	说明
0305G07W	E8KE-X-21-4X10GE-XFP	4 端口 10GBase WAN/LAN-XFP 灵活子卡(占用两个子槽位)	该子卡用于 LPUF-21 接口板, 请注意区分
0305G07X	E8KE-X-40-4X10GE-XFP	4 端口 10GBase LAN/WAN-XFP 灵活插卡 (P40)	该子卡用户 LPUF-40 接口板, 请注意区分

0305G08N	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	200G 交换网板替换 40G 交换网板, 一般不单独报价
0305G08P	E8KE-X8-SFUC-200	X8 200Gbps 交换网单元 C-含 HS 通用安全平台软件	仅作为典型配置中组件备货, 不单独销售
0305G08Q	E8KE-X16-SFUC-200	X16 200Gbps 交换网单元 B-含 HS 通用安全平台软件	仅作为典型配置中组件备货, 不单独销售

USG9500 V200R001C01 版本新增如下软件报价项:

编码	型号	描述	说明
8270G9DD	LIC-VSYS-2000-E8KE	虚拟防火墙数(2000 Vsys)	原最大虚拟防火墙数报价项为 1000
8270G9DE	LIC-VSYS-4000-E8KE	虚拟防火墙数(4000 Vsys)	同上

1.3 版本配套关系

USG9500 V200R001C01 版本的配套关系如下表:

设备形态	版本
eLog 日志服务器	eLog V100R003C00SPC200
VSM 管理中心服务器安装软件	VSM V200R001C00
网管系统 U2000	U2000V100R006C02 以及兼容该版本的更高版本

2 应用概述

USG9500 应用场景主要有：

- GPRS 网络 PS 域防护，主要部署在 Gi 口进行安全防护，以及大规模地址换。
- 国际关口局
- 城域网 DDoS 防护
- DDoS流量清洗
- IDC 数据中心应用层防护
- IPv6 迁移（CGN）
- 海量 VPN 网关
- LTE无线传输回传网络加密

具体见 USG9500 防火墙销售指导

3 产品配置

3.1 新增报价项的配置原则

USG9500 V200R001C01 新增报价项详见本文 1.2 章节。

■ 0305G07W 的配置原则

0305G07W	E8KE-X-21-4X10GE-XFP	4 端口 10GBase WAN/LAN-XFP 灵活子卡 (占用两个子槽位)	该子卡用于 LPUF-21 接口板, 请注意区分
----------	----------------------	---	--------------------------

相比 0305G052 (1 端口 10GBase WAN/LAN XFP 灵活子卡), 0305G07W 的主要变化为占用了 2 个子槽位, 即 LPUF-21 接口板配置了一块该子卡后, 需要把中间挡板拆除, 不能再插入新的子卡。

由于为收敛子卡, 限于 LPUF-21 接口板母板 20G 处理能力限制, 4 端口万兆子卡最终会收敛到最大处理 20G 业务流量。在端口密度有要求且单板业务流量不超过 20G 时, 可以使用此板卡, 请注意区分。

■ 0305G07X 的配置原则

0305G07X	E8KE-X-40-4X10GE-XFP	4 端口 10GBase LAN/WAN-XFP 灵活插卡 (P40)	该子卡用户 LPUF-40 接口板, 请注意区分
----------	----------------------	-------------------------------------	--------------------------

相比 0305G075 (2 端口 10GBase LAN/WAN-XFP 灵活插卡(P40)), 该子卡同样占用了 1 个子槽位, 主要变化为由 2 端口提高到了 4 端口, LPUF-40 接口板可以插入 2 块该子卡, 形成单接口板 8 个万兆接口的高密度接口板。

由于为收敛子卡，限于 LPUF-40 接口板母板 40G 处理能力限制，4 端口万兆子卡最终会收敛到最大处理 20G 业务流量。在端口密度有要求且单板业务流量不超过 40G 时，可以使用此板卡，请注意区分。

对于既要 4 万兆接口，又需要多个千兆接口的场景，可以采用 LPUF-40 接口板上，插入 1 块 0305G07X（4 万兆收敛子卡）加 0305G076（20 端口 GE 灵活插卡）应对。

3.2 典型配置及部件切换

3.2.1 典型配置

国内版华为 Secospace 配置器将从 2012.11 月开始支持 USG9500 V200R001C01 产品 USG9560、USG9580 200G 交换网的主机 Bundle 直流典型配置，默认采用原 40G 交换网的主机 Bundle 直流典型配置。典型配置国内和海外采用不同的编码，共有 4 种，海外配置原则请参考 USG9500 配置原则海外版，与 40G 交换网的典型配置关系为：

新增局点全部默认采用 200G 交换网直流或交流主机 Bundle 典型配置；

扩容局点需要选择区分升级前版本和升级后版本，当有低级别版本升级到 V200R001C01 版本时，需要给出提示：“一线需确认现网的 C 版本，如果是在 C00 版本扩容收敛子卡，需要向客户报单次项目升级费用”。

有变动的基本配置说明如下：

编码	型号	描述	说明
0235G6XT	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	该典型配置所含交换网板，由 40G 升级为 200G，编码不变
0235G7EF	USG9580-BASE-DC-02	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	同上

0235G6XU	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	删除此交流基本配置,采用直流基本配置 0235G6XT 和一个交流电源模块 0231G5C2 实现,配置器上自动计算配置
----------	--------------------	--	--

注: USG9580 也仅有直流基本配置 0235G7EF (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)。如果采购 USG9580 交流机框,采用直流基本配置 0235G7EF 和两个交流电源模块 0231G5C2 实现。配置器上自动计算配置。

老 40G 典型配置不再推荐使用,新发布的配置器上新建局点时不再考虑保留。

3.2.2 部件切换

请参考 3.2.1 节典型配置切换,原 40G 交换网典型配置在 C01 版本全部推荐切换到 200G 交换网典型配置,现网 C00 版本如果是 40G 交换网,如果直接升级到 C01 版本,不影响设备正常使用。

3.3 SBOM 与 BBOM 的对应关系

不涉及。

3.4 产品配置

3.4.1 软件及 License 配置

版本	V200R001C01 (默认)
虚拟防火墙	支持创建 1 个虚拟防火墙
IPSec	支持 100 条 IPSec 隧道
GTP	不支持
IPS	不支持
DS-Lite	行业网不销售
NAT64	行业网不销售
6RD	行业网不销售

版本	V200R001C01 （默认）
DDoS	不支持

VFW 个数，按照用户需要的数量规模配置，可选择项有 5、10、25、50、100、200、500、1000、2000、4000。其中 2000 和 4000 资源项为 V2R1C01 版本新增。

VPN 隧道，按照用户需要的数量规模配置，可选择项有 100、500、1000、2000、5000、1 万、2 万、8 万。

IPS 性能 License 在 Unistar 配置器上已经作为 SBOM（S4025166）整体体现，无需单独配置。购买后默认不支持升级服务，仅有基础 IPS 库。

S4025166	8G 性能 IPS 业务板
0303G046	IPS 特性业务处理板数量-含 HS 通用安全平台软件
8270G889	业务处理单板-四 CPU-含 HS 通用安全平台软件

IPS 升级服务有 1 年和 3 年两种报价项，推荐选择其一购买。否则 IPS 防御效果无法保证最新的攻击能够防御成功。

8270G744	IPS 特征库升级服务 1 年 License-含 HS 通用安全平台软件
8270G745	IPS 特征库升级服务 3 年 License-含 HS 通用安全平台软件

Anti-DDoS 性能 License 分为 10G 性能、20G 性能、10G 升 20G 性能 3 种。已作为 SBOM 包含在单板选择中。需要根据防御攻击的流量大小配置不同性能的 License。

S4025227	10G 性能检测业务处理板-含 HS 通用安全平台软件 业务处理单板-双 CPU-含 HS 通用安全平台软件
	DDOS 检测 10G 性能 License-含 HS 通用安全平台软件
S4025228	10G 性能清洗业务处理板-含 HS 通用安全平台软件 业务处理单板-双 CPU-含 HS 通用安全平台软件
	DDOS 清洗 10G 性能 License-含 HS 通用安全平台软件
S4025254	20G 性能检测业务处理板-含 HS 通用安全平台软件 业务处理单板-四 CPU-含 HS 通用安全平台软件
	DDOS 检测 20G 性能 License-含 HS 通用安全平台软件
S4025255	20G 性能清洗业务处理板-含 HS 通用安全平台软件 业务处理单板-四 CPU-含 HS 通用安全平台软件
	DDOS 清洗 20G 性能 License-含 HS 通用安全平台软件
S4025258	10G 性能升级至 20G 性能 DDOS 检测插板-含 HS 通用安全平台软件 业务处理插卡-双 CPU-含 HS 通用安全平台软件

	DDOS 检测 10G 升级到 20G 性能 License-含 HS 通用安全平台软件
S4025259	10G 性能升级至 20G 性能 DDOS 清洗插板-含 HS 通用安全平台软件
	业务处理插卡-双 CPU-含 HS 通用安全平台软件
	DDOS 清洗 10G 升级到 20G 性能 License-含 HS 通用安全平台软件

3.4.2 外部报价电缆/光纤配置

配套交流电源时免工勘，配套直流电源时请咨询当地华为工程师，提前工勘，确定实际所需电缆长度。光纤配置，与光模块数量匹配，单模多模选择，请根据实际传输距离确定。

如有疑问，请咨询华为工程师。

3.4.3 光模块配置

当配置的接口板为光接口时，需要配置光模块部件，请注意区分万兆规格（XFP）和千兆规格（SFP 或 eSFP），还需向客户询问光模块的模式、波长、传输距离等指标。

如有疑问，请咨询华为工程师。

4 版本升级

4.1 升级路径

具体升级需求需要联系产品 LMT 确定。

升级前的版本 \ 目标版本	USG9500 V200R001C01
USG9500 V200R001C00	√
USG9500 V100R003	√

4.2 USG9500 V100R003 向 V200R001C01 升级

V200R001 版本继承 V100R003 版本的所有硬件及软件特性并在此基础上增强。

由于 V100R003 版本为单纯防火墙版本，不支持 DDOS，因此需支持 DDOS 特性时推荐升级到 V200R001C01 版本。

注意：

- 1) 配套网管、eLog、VSM 版本请参考 1.3 节描述升级。
- 2) USG9310、USG9320 机框 2012 年年底在网络 BU 计划 EOM。

4.3 USG9500 V200R001C00 向 V200R001C01 升级

V200R001 版本继承 V100R003 版本的所有硬件及软件特性并在此基础上增强。

注意：

- 3) 配套网管、eLog、VSM 版本请参考 1.3 节描述升级。
- 4) USG9310、USG9320 机框 2012 年年底在网络 BU 计划 EOM。
- 5) V200R001C00 版本只有在升级到 C01 版本后才能够支持收敛子卡、200G 交换网板以及 200G 直流/交流典型配置。
- 6) C00 版本相对 C01 版本新增了软件 License, 具体升级策略请参考 3.1 节进行配置。