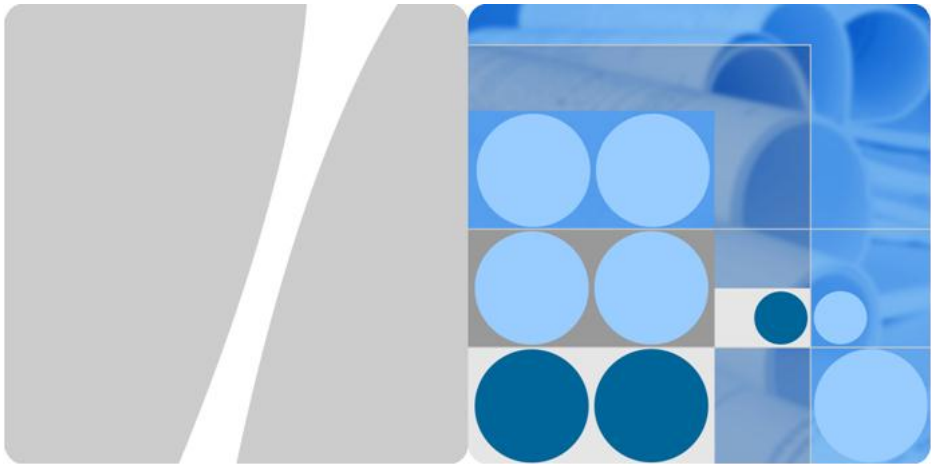

华为ASG2000上网行为管理产品规格清单

华为技术有限公司

商标声明


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： 0755-28560000 4008302118

客户服务传真： 0755-28560111

分类	功能	详细指标	ASG2100	ASG2200	ASG2600	ASG2800
硬件规格	主机自带接口	设备的固定接口	4GE+2Combo	4GE+2Combo	4GE+4Combo	4GE+4Combo
	槽位数量	设备支持槽位数	4MIC+1FIC	4MIC+1FIC	2FIC	2FIC
	接口卡类型	设备支持的扩展插卡类型	MIC-1FE/MIC-5FE/FIC-4GE MIC-WiFi DFIC-X86	MIC-1FE/MIC-5FE/FIC-4GE MIC-WiFi DFIC-X86	FIC-4GE/FIC-8GE/FIC-8GE（光） FIC-4GE Bypass/FIC-2路光口bypass	FIC-4GE/FIC-8GE/FIC-8GE（光） FIC-4GE Bypass/FIC-2路光口bypass DFIC-X86
	USB接口		2	2	2	2
	外型尺寸（W*D*H）	包括机框，外型	442(宽)×420(深)×1U(高)	442(宽)×420(深)×1U(高)	442(宽)×560(深)×1U(高)	442(宽)×560(深)×1U(高)
	重量	设备重量	裸机5.4kg，满配8kg	裸机5.4kg，满配8kg	裸机8.2kg，满配8.9kg	裸机8.2kg，满配8.9kg
	电源	交流电源-额定电压	100～240V 50/60Hz	100～240V 50/60Hz	100～240V 50/60Hz	100～240V 50/60Hz
		直流电源-额定电压	NA	NA	NA	NA
		冗余电源	单电源	单电源	双电源	双电源
	功率	电源最大功率	整机电源100W（12V，不包含POE，支持X86卡）；X86为57W	整机电源100W（12V，不包含POE，支持X86卡）；X86为57W	最大功率150W；X86为57W	最大功率150W；X86为57W
	工作环境温度	运行工作、短期工作的温度	运行：0℃~45℃ 短期：-5℃~55℃	运行：0℃~45℃ 短期：-5℃~55℃	运行：0℃~45℃ 短期：-5℃~55℃	运行：0℃~45℃ 短期：-5℃~55℃
	环境湿度	工作、存储的湿度	工作：5%～95%，不结露	工作：5%～95%，不结露	工作：5%～95%，不结露	工作：5%～95%，不结露
	MTBF/MTTR	平均无故障时间 平均修复时间	MTBF：12.67年 MTTR：0.5小时	MTBF：12.67年 MTTR：0.5小时	MTBF：16.67年 MTTR：0.5小时	MTBF：16.67年 MTTR：0.5小时
性能规格	性能参数	推荐用户规模	400	1,500	5,000	10,000
		转发吞吐量	300Mbps	1Gbps	2.5Gbps	3Gbps

分类	功能	详细指标
系统组成	系统组件	1、支持管理中心和设备分离的架构，一个管理中心可以多个设备 2、管理中心可以内置也可以部署到普通PC或服务器上
组网部署	网关模式	1、支持网关模式，支持静态路由（基于优先级和目标的路由）、策略路由(基于ACL、用户的选路）、OSPF 2、支持NAT/NAT-SERVER、DHCP SERVER、DNS/DDNS、组播等功能 3、支持部署为VRRP
	网桥模式	1、支持网桥模式，以透明方式串接在网络中； 2、支持VRRP环境下的部署； 3、支持组播、IPv6透传等功能；
	旁路模式	1、支持旁路模式，无需更改网络配置，实现上网行为审计； 2、支持多路监听
用户管理	组织结构	提供基于部门和账号的分组管理功能: 1、树状组织部门管理架构，满足不同部门、不同账号的差异化安全策略配置要求； 2、部门信息包括：部门名称、描述信息、安全策略； 3、账号信息包括：账号、显示名称、所属部门、描述信息、账号策略和上网策略；
	本地账号策略	本地账号属性包括以下配置参数: 1、允许管理员重置本地账号密码； 2、支持强制用户下次登录修改密码； 3、支持永久账号和账号有效期配置； 4、支持账号冻结，可以实时启用或禁止账号的使用状态； 5、支持账号的多点登录属性可配置，同一时间，可以允许或阻止一个帐号在多台机器上登录； 6、支持账号与机器属性绑定的认证，IP/IP段/MAC/IP+MAC的单向绑定认证，或只允许具体IP/IP段/MAC/IP+MAC使用某个指定账号的双向绑定认证，防止用户使用同一帐号登录不同上网管控级别的机器； 7、支持文件手工导入批量创建账号信息；
	第三方账号数据源同步	1、支持微软AD（Active Directory）数据源同步； 2、支持华为终端安全管理（TSM）数据源同步；
	身份认证方式	支持多种用户身份识别方式，满足不同接入场景需求: 1、主动认证： 通过安装在客户机器的认证代理或WEB认证界面，输入用户名+密码的方式，实现身份识别； 2、单点自动认证： 客户机器上已经完成AD、华为TSM认证的场景下，后台自动联动，实现身份识别； 3、网段自动认证： 通过客户机器接入网络后，自动识别所在网段，实现身份识别；
	认证策略	可强制指定用户、指定IP段的用户必须使用单点登录
	特权用户管理	可设置全局的免监控用户列表，这些用户登录后，不需要做任何审计和控制，只审计用户登录信息
用户策略	策略分类	WAN/LAN/DMZ域间策略（根据五元组、时间段、方向）、 全局排除地址策略（内网用户访问指定目标IP或域时，不受控制和审计）、用户策略（本文未声明均指示此类策略）
	策略分配	支持不同用户及用户组间策略的复用，允许高级别管理员对管辖范围内的用户强制部署策略
	策略生效时段、启用和禁用	生效时段内策略才有效；可以禁用策略，禁用后的策略不会生效
实时监控	运行状态	1、支持首页运行状态展示和运行状态刷新间隔设置； 2、设备资源信息：支持CPU、内存，Flash和SD卡的使用率百分比表盘展示； 3、设备状态图：支持设备外观和端口状态展示； 4、接口流量统计趋势：支持各个接口近60分钟/24小时/30天流入和流出趋势图； 5、当天日志总量统计：支持基于不同类型（HTTP POST、文件外发、邮件外发、URL过滤、入侵事件、病毒事件、垃圾邮件）拦截操作日志和审计操作日志的统计表图； 6、协议会话数统计：支持基于不同协议类型（如TCP、UDP、ICMP、SMTP、HTTP、FTP、RSTP、H323等）的最近流量排行柱状图和表图百分比； 7、系统信息：支持电源状态、环境温度、风扇状态、主备状态、在线管理员数、在线用户数监控；
	安全状态	1、病毒事件TOP10柱状排行； 2、入侵事件TOP10柱状排行； 3、攻击事件TOP10柱状排行； 4、滥用知名端口事件TOP10柱状排行；
	连接监控	监控在线用户域间访问连接，基于用户、所属部门、源IP/Port、目的IP/Port、协议、应用和域间方向详细信息；
	在线用户	支持在线或冻结用户状态列表，用户、所属部门、IP地址、认证方式、登录时间/冻结时间、在线时间/解冻剩余时间、用户状态；
	系统统计	1、支持基于协议的会话统计值柱状图； 2、支持收发报文统计值柱状图； 3、支持被丢弃报文（如SYN Flood/ICMP Flood/UDP Flood/黑名单/超大包等）统计值柱状图；
	接口统计	基于端口的输入/输出报文速率和流量
页面浏览控制	URL过滤策略	基于时间段控制用户浏览页面，可以根据用户对大类和小类进行控制，支持的大类包括：游戏、人文、休闲、博彩、宗教、金融、赌博等
	URL分类库	1、URL分类库大于6500万，11种语言，130+内容分类，支持用户自定义分类，通过华为云安全能力中心，实现云端自动更新 2、URL分类库更新周期小于3天
	灰名单（没有分类）策略	可以定制不能匹配URL分类的是否限制还是放行
应用控制	应用控制策略	根据应用分类进行控制，基于时间段对用户进行控制
	P2P控制	1、支持常见P2P下载软件（BitTorrent，eMule等）、常见P2P视频软件（PPStream、PPLive等）、常见P2SP软件（迅雷、网际快车等）控制 2、支持超过130种的P2P应用
	IM控制	1、支持常见IM控制，包括QQ、MSN、Gtalk（含加密）、雅虎通、飞信等，同时支持根据IM的不同行为属性（DPI小类，如聊天、语音、视频、文件上传下载、远程控制、网络硬盘等）进行控制 2、支持超过70种的IM应用
	其他常规应用控制	1、支持网游、炒股类流量、远程控制、网络存储、FTP、SSL、代理工具、SMTP/POP3、WebMail软件诸类应用的控制，HTTP协议非网页流量（网页视频、网页游戏等）控制 2、支持超过90种的网络存储应用 3、支持超过110中的网络流媒体应用 4、支持超过90种VoIP应用 5、能够识别超过20种的WebMail应用
	知名端口非标协议控制	支持在知名端口（21，25，80，110，443端口）上使用非标准协议的审计

	应用识别特征库	1、支持1200+应用识别，覆盖国内外主流应用，含300+移动智能终端应用，支持自定义应用 2、支持如下分类：P2P文件共享、VoIP、IM、Web浏览、文件访问协议、Web视频、股票、游戏、隧道协议、网络攻击、电子邮件、网络管理、远程连接、新闻组、网络存储、无线协议、Web邮箱、数据库、网络流媒体、P2P网络视频、软件更新、蠕虫、僵尸网络、未知流量等大类 3、支持应用识别特征库自动更新
带宽管理	自定义流量范围	1、支持基于接口、源地址来定义流量范围 2、支持根据用户或部门、应用、用户+应用来定义流量范围 2、支持基于协议端口定义流量范围 3、支持基于目的地址来定义流量范围
	自定义带宽策略	1、支持带宽闲时复用 2、支持带宽整体和单IP限制 3、支持带宽保证 4、支持连接数限制 5、支持展示带宽策略的通过包数和丢弃包数等信息
配额管理	流量配额	可以限制单用户每月/天的流量配额
	上网时长配额	可以限制指定时段内的上网时长，支持不纳入时长计算的例外流量
	并发连接数配额	支持针对每个用户的最大连接数控制
行为审计和分析	行为审计	1. 上网行为查询：审计谁、什么时候、使用某种应用（大类或具体应用），被系统拦截或记录的行为审计记录 2. 上网流量查询：审计谁、什么时候、使用某种应用（大类或具体应用），累计流量 3. 上网时长查询：审计谁、什么时候，使用某种应用（大类或具体应用），累计使用时长 4. 其他性查询：异常行为查询、用户上下线查询、威胁防护查询
	上网时长分析	1、基于部门/人、应用大类/小类分析上网时长，识别主要是那些人、那些应用上网时间比较长，以评估办公效率下降情况 2、可以周期性的生成上述报表，同时支持邮件发送报表
	上网流量分析	1、排行：基于部门/人、应用大类/小类分析上网流量，识别主要是那些用户、那些应用在占用出口带宽，以评估带宽滥用情况 2、趋势：基于部门/人、应用大类或TopN应用，在指定时段内的流量日周月趋势，可以针对上下行和总量进行统计 3、对比：基于办公无关应用、或选定应用、选定部门，统计总体和Top应用的流量、增长数、增长率；同时提供基于各上班时间点的趋势对比；可以跟前一天/周/月进行对比 4、可以周期性的生成上述报表，同时支持邮件发送报表
	上网行为次数分析	1、排行：基于部门/人、应用大类/小类分析上网次数，识别主要是那些用户、那些应用频繁使用网络，以评估应用控制使用情况，辅助调整策略 2、趋势：基于部门/人、指定应用的使用时长日周月趋势 3、对比：基于办公无关应用、或选定应用、选定部门，统计总体和Top应用的使用次数、增长数、增长率；同时提供基于各上班时间点的趋势对比；可以跟前一天/周/月进行对比 4、可以周期性的生成上述报表，同时支持邮件发送报表
	综合分析	提供综合报表，展示用户在办公效率、带宽利用、威胁过滤、合规性方面的总体概况和专项评估情况，以辅助管理和投资决策： 1. 办公效率评估报表，可以基于日期范围、选定用户、选定统计对象（应用分类集），展示主要用户组的时长损失情况、主要办公无关应用的应用时长情况 2. 带宽利用评估报表，可以基于日期范围、选定用户、选定统计对象（应用分类集），展示出口带宽利用率、带宽主要被哪些应用和哪些用户组占用 3. 员工合规性评估表，可以基于日期范围、选定用户、选定统计对象（URL分类集、应用分类集），展示不良网站流量、违规应用（如翻墙软件等逃避措施）方面的情况 4. 整体评估报表，可以基于日期范围、选定用户进行统计，集中展示办公效率、带宽利用、威胁过滤（主要威胁分布、检测和拦击效果）、员工合规性方面的总体概述和专项评估。 5. 上述报表均提供总体概述和专项评估，总体概述说明主要情况，专项评估对主要情况进行展开分析 6. 可自定义分析对象，用于对所关注的应用/应用分类和网站的分析 7. 支持定义报表名称、报表条件等 8. 支持以RTF/HTML/PDF格式导出报表 9. 可以周期性的生成分析报表，同时支持邮件发送报表
	报表任务	提供报表任务，自动生成指定条件的报表： 1. 定制普通和综合报表任务，在指定周期和指定时间内生成相应报表 2. 已生成报表查看：可以浏览通过报表任务生成的报表，可以下载
内容控制和审计	文件外发控制	基于文件类型和大小控制文件通过http/ftp外发
	Web提交内容大小控制	可以限制用户通过HTTP POST提交的内容的大小，支持完全禁止POST
	Web提交内容关键字控制	基于关键字控制WEB提交内容，包括网络发帖（如知名/常用的BBS、blog、wiki、微博等http应用）
	邮件外发控制	基于源目邮件地址（地址或地址后缀黑白名单）、内容关键字（标题和内容）、邮件大小、SMTP附件个数和附件类型控制外发邮件，邮件包括SMTP和WebMail（http协议）
	IM文件外发控制	基于文件类型和大小控制通过主流IM（QQ、MSN、阿里旺旺、飞信、雅虎通、Gtalk（含加密））外发文件
	IM审计	1、审计主流IM（QQ、MSN、阿里旺旺、飞信、雅虎通、Gtalk（含加密））的聊天内容、双方帐号和文件属性，对于外发文件还可还原外发文件内容
	文件下载审计	记录通过http下载文件的行为和文件属性（文件名、大小、类型），无需保存文件
上网安全	威胁过滤	提供上网安全防护，降低用户由于WEB使用、跟外网的文件传输导致的对内和对外安全风险。包括 1）漏洞利用检测，如基于浏览器、常用办公软件（Ms Office/pdf等）、插件脚本（ActiveX/JavaScript/VBScript等）、流媒体（Quick Time/Flash Player/Real Play/Windows Media/VLC等）等漏洞利用； 2）恶意行为和代码检测，包括后门/间谍/僵尸软件、黑客工具、键盘记录软件、零日攻击、木马蠕虫、系统补丁等其他安全漏洞； 3）基于漏洞的入侵攻击特征库数量≥1800+种，攻击检测率≥90%； 4）对于检测到的不同级别的威胁（高中低），可进行差别处理，处理方式有阻断和告警 4）支持HTTP/FTP/POP3/SMTP等常用协议的文件病毒扫描功能，病毒库数量≥500万种，病毒检测率≥90%；支持对文件真实类型的有效识别；支持对各种压缩格式及多层压缩文件进行病毒扫描；支持对加壳病毒的脱壳扫描；可设置病毒扫描等级；响应方式支持病毒文件的删除，返回页面警告，邮件标记警告，日志记录等；可设置扫描的等级（高中低），扫描等级越高，检测率越高，但是性能会较低 5）扫描例外: 可设定源地址或目标地址，对这些地址不进行威胁检测和病毒扫描
	恶意URL过滤	支持过滤恶意URL页面的访问，包括恶意网站、钓鱼网站、恶意软件网站
	反垃圾邮件过滤	1. 支持跟RBL（Real-time Black List, 实时黑名单）服务器进行联动检测垃圾邮件，可以添加RBL服务器查询集合 2. 支持本地黑白名单，对接收到白名单内的邮件不做控制，对接收到黑名单内的邮件直接认为是垃圾邮件

增值功能	网络	1、支持IPv4协议，允许IPv6透传 2、支持静态路由（基于优先级和目标、出接口和/或下一跳IP的路由，预置国内常见的ISP选路规则）、动态路由（OSPF）、策略路由（基于ACL、用户的选路） 3、支持基本网络服务，如DHCP/DNS/DDNS、组播 4、支持802.3ad链路聚合，可以将多个物理端口捆绑成一个逻辑端口以提升带宽，最多可捆绑4条链路，当其中某一条链路中断时可自动将流量分担到其他链路中，提高可靠性；
	NAT（网关模式）	1. 支持NAT 2. 支持NAT-SERVER，通过端口映射，将内部服务器映射为公网可以访问
	WLAN	可扩展无线办公电脑的无线接入服务
	安全防护	1. 攻击防范（流量/应用层泛洪攻击、扫描、畸形报文、特殊报文控制），能够抵御各种DoS攻击和DDoS攻击，包括：SYN Flood攻击、UDP Flood攻击、ICMP Flood攻击、DNS Flood攻击、ARP攻击、IP Spoofing攻击、LAND攻击、Smurf攻击、Fraggle攻击、Winnuke攻击、Ping of Death攻击、Tear Drop攻击、Http get攻击、CC攻击等； 2. 支持黑名单（静态或动态生成黑名单列表，设备丢弃来自黑名单中的IP地址的报文）、白名单功能
管理功能	管理员权限	1. 管理员具有级别，具有策略权限时，不同级别的管理员可以管理低于等于其级别的策略 2. 设备各功能模块查看/配置权限支持授予不同管理员，不同管理员负责不同部门的业务管理； 3. 管理中心超级管理员可以配置所有设备，不同日志管理员负责不同部门的日志管理；
	管理方式	本地或远程支持WEB管理，支持通过telnet/ssh/console协议进行管理，设备忘记密码或IP也无需重置
	集中管理	1、管理员可以通过管理中心管理多台ASG设备，并且支持不同管理员只能查看管辖部门内指定类别的日志和报表 2、支持多设备集中配置管理、集中查看日志和报表不需要选择具体设备来查看 3、实时汇总各设备日志
可靠性	软件Bypass	启用软件bypass后，设备直通（相当于普通转发设备），不做业务控制
	硬件Bypass	当设备断电、设备重启、设备业务异常时启用Bypass，Bypass开启后，相当于网线直通
	设备HA	支持两台主备和主主两种方式。发生切换时终端用户无需再次认证。透明、路由、旁路均支持
	引擎失效保护	业务引擎失效后，不会导致业务中断
	引擎过载保护	业务引擎过载后，不会导致业务中断
	多线路接入	最大支持8条线路接入互联网（负载均衡和备份），可以同时使用不同运营商线路，支持智能选择最优线路等多种负载均衡策略
	业务隔离设计	不管是否内置或外置日志中心，日志查询和输出报表均不影响设备性能
可维护性	特征库升级	管理中心超级管理员可以指定升级计划，对选定的ASG设备的特征库（IPS/AV/DPI/ULR）进行自动升级；也支持自动或手工方式（在线或离线）对单台设备升级上述升级项，同时支持失败回退
	版本和补丁升级	提供版本和补丁的一键式升级
	灾备还原配置	提供配置备份和恢复功能，以防设备异常时是恢复到最近备份的配置
	远程抓包分析	将报文发送到特定的主机，在远程主机上对报文进行分析
	业务诊断和设备信息采集	以WEB方式提供网页无法打开、设备重启、Ping、Tracerts等诊断功能，同时提供设备信息采集功能
	日志备份	支持自动定时备份
其他	多语言支持	支持简体中文和英文
	Syslog事件外发接口	ASG设备支持以Syslog方式外送选定系统异常类的事件，如网络、引擎、系统负载、CPU/MEM/DISK资源占用过大等异常事件
	SNMP接口	提供SNMP查询设备状态和SNMP Trap外发设备事件
	告警管理	1. 支持对设备异常或业务异常的告警 2. 支持显示当前和历史告警，当前告警可确认、历史告警可查询，均支持告警导出 3. 支持显示所有事件，根据条件查询事件，支持导出 4. 对于指定类型的告警，可以通过邮件和短信方式发送通知；对不同级别的告警，可以分别启用声音告警