华为HiSecEngine USG6600F&USG6700F系列AI防火墙

数字化浪潮正在席卷全球，广泛的连接、爆炸式增长的数据以及蓬勃发展的智能应用正在深刻改变人类的生活和工作方式，企业业务的数字化和云服务化推动着企业网络的变革，同时也给网络安全带来了更大的挑战：威胁增多，未知威胁变异加快且隐蔽度高；用户对安全业务需求逐渐增长，性能和时延成为瓶颈；海量的安全策略和日志，威胁处置和运维耗时巨大。防火墙作为网络边界的“第一道门”是当前企业安全防护的首选，然而传统防火墙通常只能基于签名实现威胁的分析和阻断，该方法对未知威胁无有效的处置方法，同时威胁的实效依赖运维人员的专业度。这种单点、被动、事中防御的方式已经不能有效的解决未知威胁攻击，对于隐匿于加密流量中的威胁更是难以有效的识别。

华为推出HiSecEngine USG6600F&USG6700F系列AI防火墙，通过全新软硬件架构，打造具备智能防御、卓越性能、极简运维三大关键能力的新一代AI防火墙，有效应对挑战。HiSecEngine USG6600F&USG6700F系列使用智能技术赋能边界防御，精准阻断已知和未知威胁；内置多个安全专用加速引擎有效提升转发、内容安全检测、IPSec等关键业务处理性能；通过安全运维平台实现防火墙、入侵防御、抗DDoS等多类安全产品的统一管理和运维，降低安全运维OPEX。

HUAWEI

01 产品亮点

卓越性能

HiSecEngine USG6600F&USG6700F系列AI防火墙使用全新软硬件架构，通过自适应安全引擎（ASE）为业务模块动态分配资源，最大限度提高资源利用率，提升整体业务性能；同时针对核心业务，使用NP（Network Processor）、模式匹配、加解密协处理引擎，有效提升小包转发性能、降低转发时延，增强应用识别和入侵防御检测以及IPSec等业务性能。

智能防御

- 签名1:N恶意文件家族
- 检测速度与签名检测性能相当
- 具有未知威胁检测能力

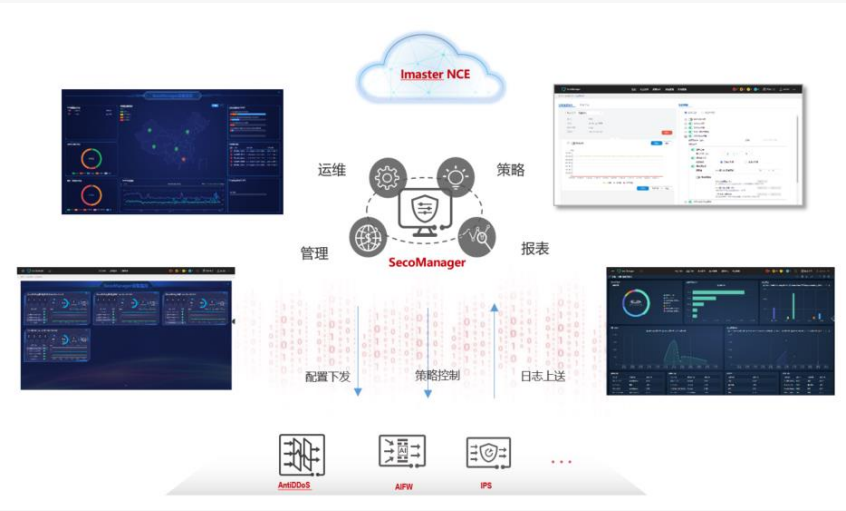
HiSecEngine USG6600F&USG6700F系列AI防火墙提供应用识别、入侵防御（IPS）、反病毒和URL过滤等内容安全相关的功能，有效保证内网服务器和用户免受威胁的侵害。

传统IPS签名生产使用人工分析制作的方式，生产效率低，签名的准确度对专家经验的依赖度高。华为创新地使用智能技术+专家经验赋能，智能云端入侵防御签名生产的方式，签名生产率较人工提升30倍，同时降低人工分析带来的误差，持续提升入侵检测准确度。

内置支持基于智能技术的防病毒内容检测引擎（CDE）覆盖亿级病毒样本，结合AI安全检测模型，通过对病毒进行深度分析，快速检测恶意文件、勒索软件等，有效提高威胁检出率。

极简运维

HiSecEngine USG6600F&USG6700F系列提供全新的Web UI界面，以威胁可视化定义新安全界面，直观呈现设备状态、告警、流量、威胁事件等关键信息，实现多维数据钻取，关注客户的使用体验，不断改进易用性，简化运维。



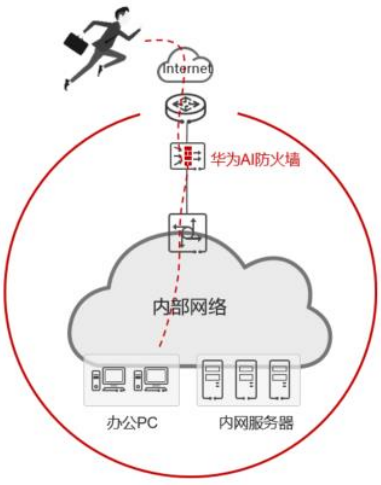
支持安全管理平台SecoManager的统一纳管，实现从单点防御到全网协防。SecoManager提供策略调优和智能运维能力，还可以同步管理入侵防御、抗DDoS等安全产品，全面快速消除网络威胁，提升安全处置效率。

HiSecEngine USG6600F&USG6700F系列也支持通过NCE-Campus纳管，NCE-Campus也可同时支持对交换机、AR、AP、POL、NE以及第三方厂家设备的统一管理和监控。

丰富的网络特性

HiSecEngine USG6600F&USG6700F系列提供VPN、IPv6、智能选路等丰富的网络特性。

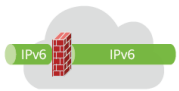
- 提供IPsec VPN、SSL VPN等丰富的VPN特性，支持DES、3DES、AES、SHA、SM2/3/4等多种加密算法，保障数据传输的安全性、可靠性。
- 提供安全丰富的IPv6网络切换能力、策略管控能力、安全防护能力以及业务可视能力，有效帮助政府、媒资、运营商、互联网、金融等行业进行IPv6改造建设。
- 提供基于多出口链路的动/静态智能选路功能，根据管理员设置的链路带宽、权重、优先级选择出接口，按照不同的选路方式转发流量到各条链路上，并根据各条链路的实时状态动态调整分配结果，以此提高链路资源的利用率和用户体验。



IPv6网络切换能力

- V4/V6双栈
- DSLite 隧道
- 64翻译
- 66翻译

NAT66



对公私网IPv6的地址进行转换，减少内网IPv6发布难度，同时隐藏内部ipv6地址，防止外部攻击

IPv6策略管控能力

- 安全策略
- 应用控制
- 用户管控
- URL过滤

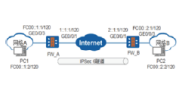
用户认证

将网络流量的IP地址识别为用户，为网络行为控制和网络权限分配提供了基于用户的管理维度，实现精细化的管理

IPv6安全防护能力

- 入侵检测
- 病毒过滤
- 攻击防护
- IPSec6

IPSec6



提高IPv6网络间的通信安全。

IPv6业务可视能力

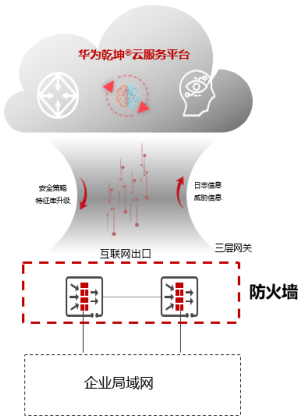
- 设备管理
- 流量监控
- 应用识别
- 日志和报表

报文镜像

在不中断业务的前提下抓取、分析会话报文

可信可控的视频终端安全接入，威胁全网可视

联动华为乾坤安全云服务解决方案



威胁分析

- **自动关联分析**：利用智能技术和知识图谱实现日志的智能聚合分析
- **安全专家分析**：云端运营专家基于取证信息、实时海量情报，实现威胁精准判定

威胁处置

- **黑白名单功能**：人工完成黑白名单设置，保护已知业务，快速阻断威胁
- **威胁自动阻断**：基于智能技术判定准确识别攻击源

安全态势感知

- **定期安全报告**：定期自动生成周报、月报，并通过邮件发送至用户邮箱
- **事件紧急通知**：通过短信、邮件两种方式通知用户

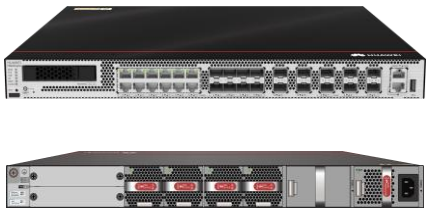
大部分威胁攻击来源于网络流量，通过在本地网络出口部署防火墙与华为乾坤安全云服务联动，实现威胁自动分析处置，在保证内网和外网互通的同时，能够有效拦截流量攻击威胁，针对外部攻击源进行自动化处置，保护企业网络资源。

通过防火墙联动华为乾坤安全云服务，可按需获取边界防护与响应等安全服务，轻量部署、云端统一运维，有效减少硬件产品堆叠，极大降低企业安全投资和运维难度。

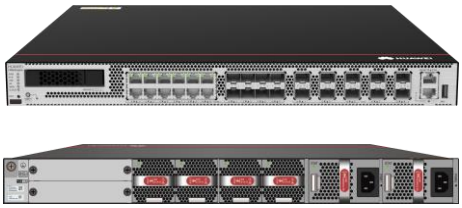
02 产品图

- **丰富接入能力:** 支持Ethernet, 5G RU
- 产品图:

华为HiSecEngine USG6615F/USG6625F

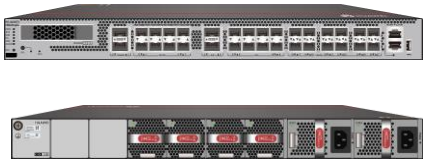


华为HiSecEngine USG6635F/USG6655F/USG6685F



华为HiSecEngine USG6636F/USG6656F/USG6686F

华为HiSecEngine USG6710F/USG6715F



华为HiSecEngine USG6725F

03 产品规格（为方便展示，规格表中采用设备简称）

型号		USG6615F	USG6625F	USG6635F	USG6655F
固定端口	业务口	8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+		8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+	
	USB	1×USB3.0			
Bypass插卡		支持2个电bypass或光bypass插卡			
硬盘		可选配2.5英寸SATA硬盘（240GB/480GB/960GB/1.92TB/3.84TB），可热插拔			
机箱高度		1U			
尺寸(W×D×H) mm		442 × 420 × 43.6			
风扇		3+1			
散热（气流走向）		前面板进，后面板出			
最大功耗		162.4W		179.1W	
电源（AC）输入电压		100 V-240 V, 50 Hz/60 Hz			
电源（AC）冗余		选配双电源		标配双电源	
重量（空配）		6.3kg		7.3kg	
工作环境	温度	0~45℃			
	湿度	5%-95%非凝露			
存储环境	温度	-40℃～70℃			
	湿度	5%～95%			

型号		USG6685F	USG6636F	USG6656F	USG6686F
固定端口	业务口	8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+	2*QSFP28 + 2*QSFP+ + 4*SFP28 + 10*SFP+ + 8GE COMBO[3]		
	USB	1×USB3.0			
Bypass插卡		支持			
硬盘		可选配2.5英寸SATA硬盘（240GB/480GB/960GB/1.92TB/3.84TB），可热插拔	可选配2.5英寸SATA硬盘（240GB/480GB/960GB/1.92TB/3.84TB），可热插拔		
机箱高度		1 U			
尺寸(W×D×H)mm		442×420×43.6			
风扇		1+3	4		
散热（气流走向）		前面板进，后面板出			
最大功耗		179.1 W	183 W		
电源（AC）输入电压		100 V-240 V, 50 Hz/60 Hz			
电源（AC）冗余		标配双电源	1+1		
重量（空配）		7.3kg	8.035kg		
工作环境	温度	0~45℃			
	湿度	5%-95%非凝露			
工作环境	温度	-40℃～70℃			
	湿度	5%～95%			

型号		USG6710F	USG6715F	USG6725F
固定端口	业务口	2*QSFP28 + 2*QSFP+ + 8*ZSFP+ + 20*SFP+ [1]		4*QSFP28 + 16*ZSFP+ + 8*SFP+[2]
	USB	1×USB3.0		
硬盘		可选配2.5英寸SATA硬盘（240GB/480GB/960GB/1.92TB/3.84TB），可热插拔		
机箱高度		1 U		
尺寸(W×D×H)mm		442 x 600 x 43.6		
风扇		3+1		4+1
散热（气流走向）		前面板进，后面板出		
最大功耗		391 W	399 W	445W
电源（AC）输入电压		100 V-240 V, 50 Hz/60 Hz		
电源（AC）冗余		标配双电源		
重量（空配）		10.26kg		10.6kg
工作环境	温度	0~45℃		
	湿度	5%-95%非凝露		
工作环境	温度	-40℃ ~ 70℃		
	湿度	5%-95%非凝露		

注意： 1.USG6710F、USG6715F部分100GE接口与25GE接口互为Combo； 2. USG6725F部分100GE接口与25GE接口互为Combo。3. USG6636F/USG6656F/USG6686F中100GE与40GE光接口互为Combo，25GE/10GE与40GE光接口互为Combo。可配置为：4 * 40G、2 * 100G、1 * 100G+ 2 * 40G、4 * 25G/10G + 1 * 100G、4 * 25G/10G + 2 * 40G。

功能特性	描述
一体化防护	集传统防火墙、VPN、入侵防御、防病毒、带宽管理、Anti-DDoS、URL过滤等多种功能于一身，全局配置视图和一体化策略管理。
应用识别与管控	非基于端口，基于签名、关联识别、行为识别等技术进行识别；预置6000+应用，支持应用细分；支持自定义应用；支持50+的分类和20+的风险标签，可基于分类及标签进行访问控制；并支持应用识别特征库自动升级。
安全策略管理	支持基于VLAN ID、五元组、安全域、地区、应用和时间段等维度对流量进行管控，并同时进行内容安全的一体化检测；支持策略自学习，可对命中的安全策略下的流量聚合，生成子安全策略，实现细分安全策略和精准的流量安全管理。 预置常用防护场景模板，快速部署安全策略，降低学习成本。可与第三方策略管理软件(FireMon，Algosec)对接，方便用户安全运维。
带宽管理	在识别业务应用的基础上，可管理每IP使用的带宽，确保关键业务和关键用户的网络体验。管控方式包括：限制最大带宽或保障最小带宽、修改应用转发优先级等。
入侵防御	第一时间获取最新威胁信息，准确检测并防御针对漏洞的攻击；支持万级CVE漏洞覆盖；支持漏洞攻击(含Windows、Unix/Linux等系统漏洞，数据库、Apache、IIS、Tomcat等软件及中间件漏洞)防护、Web攻击 (如SQL注入、XSS、RCE等)防护、僵尸网络/远控/木马等恶意流量的检测，支持基于用户行为的暴力破解检测；最大支持2.5万+预定义签名，并支持特征库自动更新；支持攻击取证，支持全流抓包(含三次握手信息)及攻击片段高亮展示, 方便运维；支持X-Forwarded-For(XFF)字段提取。
WAF	采用签名、语义分析、机器学习等技术，支持对SQL注入、跨站脚本攻击、RCE、CSRF、反序列化等OWASP Top 10攻击的检测，支持盗链保护、网页防篡改；支持HTTP方法及字段长度控制等。
反病毒	支持HTTP/FTP/SMTP/POP3/IMAP4/NFS/SMB等协议的文件病毒检测； 可检测支持木马、蠕虫、间谍软件、漏洞利用程序、广告软件、黑客工具、Rootkit、后门、灰色软件、僵尸网络程序、勒索软件、钓鱼软件、挖矿软件、勒索软件、Web shell程序等检测，支持Office文档类型、可执行文件（Windows/Linux/MacOS）、脚本文件、Flash文件、PDF文件、RTF文件、网页、图片等各种文件类型病毒检测；支持攻击取证；支持tar/gzip/zip/rar/7z等多种压缩混合及多层压缩检测，最大支持100层压缩文件病毒检测，支持告警、阻断、添加宣告、删除附件等多种响应动作。
高级恶意软件防护	反病毒引擎采用启发式、AI-Based、语义分析、Emulator等检测技术, 辅助情报/信誉等检测, 通过动态模拟沙箱执行，可支持加壳病毒检测, 脚本变形检测, 复合文档内嵌病毒检测；覆盖数十亿级变种病毒检测，并支持特征库自动升级。同时支持联动沙箱，把可疑文件送到本地沙箱或者云沙箱进行进一步的检测，可检测更多的零日恶意软件。

功能特性	描述
Web安全	支持Web/URL过滤, 支持基于新闻/游戏/赌博/毒品/恶意网页等130+的分类能力, 云端分类库超过5.6亿, 支持20+语言, 重点分类支持100+语言；URL云端分类查询服务器全球部署，提供高速度、低时延的分类查询服务，同时满足不同国家/地区的管理要求; 支持自定义URL/Host黑白名单过滤；支持HTTPS不解密过滤；支持TLS/SSL解密过滤, 支持HTTP/2及QUIC过滤; 支持批量导入恶意分类URL。支持安全搜索：支持5大知名搜索引擎: YouTube, Bing, Google, Yahoo, Yandex. 强制过滤搜索结果中的不合法内容。支持可以根据不同的用户/组、时间段和安全区域等信息，对用户/组进行URL访问控制，达到精确管理用户上网行为的目的。
模型藏毒检测	基于模型文件内容极速检测，支持onnx/pickle/safetensors/pth/checkpointh等主流模型文件，防护恶意模型加载引发资产窃取和破坏。
提示词攻击防护	支持通过静态规则或自定义正则规则对模型输入内容进行过滤，支持采用语义分析和AI技术对提示词攻击模式进行识别，防止SQL注入、XSS和RCE等注入攻击。
DNS安全	支持联动云端进行DNS恶意域名过滤, 基于海量的威胁信息, 利用AI/知识图谱等技术发现恶意DNS请求，包括C&C（Command-and-Control）、DGA(Domain Generation Algorithm)、失陷站点、挖矿、勒索、钓鱼等恶意域名，本地支持最大200万恶意域名库。 支持基于DNS的分类过滤, 支持DNS安全搜索、支持DNS重定向(Sinkhole)。
反僵尸网络/间谍软件	支持僵尸网络、木马、蠕虫、远控工具、间谍软件等恶意程序软件及相关恶意流量的检测, 对恶意软件进行反病毒和高级恶意软件防护检测, 阻止恶意程序下载; 对于恶意软件产生的恶意流量, 进行基于签名的检测，以及基于AI的加密流量检测技术（ECA），支持C&C流量检测，并可基于IP、恶意域名信誉快速检测；支持僵尸网络攻击日志中通信双方在僵尸网络角色信息显示。
威胁信息	基于华为安全智能中心，通过多AI算法及专家分析，每日生产海量的IP、域名、URL、文件等威胁信息；并通过自动升级同步这些威胁信息到设备进行威胁检测，快速阻断新型攻击；同时支持和第三方的威胁信息源对接，丰富检测规则。
OT/IoT安全	支持Modbus、S7、Profinet、OPC等常见工控协议和摄像头等物联网设备的识别和控制，以及IoT资产风险评估. 支持摄像头等IoT设备、ICS/SCADA等工控软件和协议的漏洞检测。 开启流量探针功能，同时结合HiSec Insight态势感知，可以对IoT资产进行流量行为基线学习，并进行IoT资产风险评估，发现IoT资产风险。 1.OT协议支持列表请参考：https://isecurity.huawei.com/security/wiki/application （商务系统-工业应用）2. 防火墙部署在普渡模型L3.5级以上。
流探针	支持解析并采集流量的元数据Metadata以及攻击取证信息，包括网络层元数据（如IP、端口、报文特征等）、应用层元数据（如HTTP、DNS、TLS、SSH等协议深度解析后的字段信息），并把采集的数据发送至安全态势感知平台HiSec Insight进行更进一步的深度分析，HiSec Insight利用深度学习/机器学习等算法, 可发现网络流量潜在和高级威胁，包括未知威胁。
Anti-DDoS	采用源IP探测、指纹检测、动态限流等技术，支持针对DDoS攻击和单包攻击的防御，防范SYN Flood、UDP Flood、ICMP Flood、HTTP Flood、HTTPS Flood、DNS Flood和SIP Flood等10+种常见DDoS攻击以及20+种单包攻击，支持流量基线自学习，支持IP信誉过滤。
邮件过滤	支持邮件地址、实时黑名单列表、MIME邮件头字段（收发件人，主题等）过滤，支持SMTP发送邮件限速。
数据泄漏防护	支持100+真实文件类型识别，支持自定义文件后缀，并基于文件类型进行上传/下载传输分别控制；支持office文档、网页、代码、TXT等文件的关键字内容过滤，可自定义关键字、支持正则及权重配置，支持对大模型文件类型的识别、支持基于IP、用户、地理位置等对大模型访问控制，防止越权访问与数据泄露等。
SaaS访问控制	支持基于特征、DNS关联、IP信息库的SaaS应用识别和访问控制, 支持基于Top50的SaaS应用IP信息库识别, 可首报文识别SaaS应用, 并基于SaaS应用进行选路, 保证员工SaaS应用使用体验。

功能特性	描述
行为审计	支持对用户常见的上网行为进行审计，规范用户上网，包括FTP(上传/下载/命令等)、HTTP(发帖/搜索/浏览等)、DNS、Telnet、SNMP、邮件收发等行为的记录。
业务智能选路	支持基于业务的策略路由，在多出口场景下可根据多种负载均衡算法（如带宽比例、链路健康状态、地理位置等）进行智能选路。
VPN加密	支持丰富高可靠性的VPN特性，如IPSec VPN、SSL VPN、GRE等；支持DES、3DES、AES、SHA、SM2/SM3/SM4等多种加密算法。
SSL加密流量检测	检测并防御隐藏在TLS/SSL（IPv4，IPv6）加密流量中的威胁，可对TLS/SSL（IPv4，IPv6）流量解密后进行入侵防御、反病毒、内容过滤、URL过滤等应用层防护，基于URL分类的白名单例外。
SSL卸载	替代服务器实现SSL加解密，有效降低服务器负载，并实现HTTP流量的负载均衡。
丰富的报表	可视化多维度报表呈现，支持IP地址、应用、时间、流量、威胁等多维度呈现报表。 支持报表查看，包括流量报表、威胁报表、邮件过滤报表、带宽管理报表、系统报表、命中策略报表、文件过滤报表、内容过滤报表、URL报表，支持报表定制与订阅。
安全虚拟化	支持多种安全业务的虚拟化，包括防火墙、入侵防御、反病毒、VPN等。不同用户可在同一台物理设备上进行隔离的个性化管理。
路由特性	全面支持IPV4/IPV6下的多种路由协议，如RIP、OSPF、BGP、IS-IS、RIPng、OSPFv3、BGP4+、IPv6 IS-IS等。
IP组播	支持IPv4三层组播协议，如：IGMP、MSDP、PIM，提供点对多点的服务模式，降低带宽消耗。
部署及可靠性	透明、路由、混合部署模式，支持主/主、主/备 HA特性。
服务器负载均衡	全面支持IPv6，支持L4/L7层服务器负载分担，支持基于源IP、HTTP Cookie等多种会话保持方法；支持SSL卸载和加密；服务和安全策略结合，有效提升服务的安全性；支持基于多种协议如TCP、Radius、DNS、HTTP的健康检查用于及时感知服务器状态变化。
安全中心	基于内置的资产识别模块，可识别Windows、Linux、Android、iOS、摄像头等资产，并支持将威胁日志与资产进行关联分析，呈现资产的风险评估结果，以及资产失陷攻击链过程。
SRv6	支持IS-IS for SRv6、BGP for SRv6、SRv6 BE、SRv6 TE Policy、SRv6中间节点保护、SRv6防微环、SRv6 OAM、SRv6 SRH压缩、SRv6 TI-LFA FRR、EVPN L3VPN。
安全SD-WAN	内置安全SD-WAN解决方案，构建低成本、商业级互联网链接； ZTP一键式部署（邮件），零技能要求，设备分钟级开通； 支持FEC，视频报文30%丢包率不花屏卡顿，基于链路质量选路，链路实时切换，保证关键应用体验； 多链路选路/双CPE灵活组网，保证站点业务不掉线；端到端IPSec加密，设备安全可信，保障业务安全传输。
用户认证	上网用户支持多种用户认证方式，包括本地Portal认证和单点登录。本地Portal认证支持推送设备内置的Portal页面，并将上网用户在Portal页面输入的账号密码推送到本地数据库或RADIUS、HWTACACS、AD、LDAP认证服务器进行认证。单点登录包含RADIUS单点登录和Agile Controller（NCE-Campus）单点登录两种方式。
运维能力	支持telemetry，自动读取硬件（风扇/电源/光模块/以太端口等）、温度传感器、驱动信息 ，设备主动向采集器上送设备的接口流量统计、CPU和内存使用率。
PPPoE	支持作为PPPoE客户端提供上网服务，包括用户的认证授权，动态IP地址分配的能力。
SSL VPN支持Posture合规检查	支持操作系统版本检查、操作系统补丁检查、杀毒软件检查、防火墙检查、运行进程检查、文件安全检查、注册表检查、端口检查、防截屏、防二次跳转。
正向代理	可作为内网终端设备的代理服务器，终端用户完成用户认证和安全策略检查后通过设备代理上网（支持HTTP、HTTPS协议），管理员也可通过代理设备管理终端用户的上网行为并发送日志给日志服务器。
WebMaster	WebMaster内嵌网管，提供可视化、一键化人机操作界面，包括整网可视、网络级业务一键发放、网元管理等；提供网络自动化管理能力，如自开局、自诊断、自排障等。

防火墙联动华为乾坤安全云服务解决方案	
服务项	描述
边界防护与响应服务	入侵检测防御：基于已知攻击防护签名拦截来自外网的应用层攻击，阻拦钓鱼邮件、恶意软件（如病毒、木马）的传输行为，监测发现内网问题主机并切断问题主机外联行为，有效保护客户业务的安全、稳定性。
	事件自动分析：利用智能分析结合专家人工手段对防护节点检测到的安全事件进行分析确认，保障攻击拦截以及安全告警的准确性，及时优化攻击识别规则，提升现网防护效果。
	黑白名单功能：客户可基于Portal、APP快速人工完成黑白名单设置，保护已知业务，快速阻断威胁。
	定期安全报告：基于安全防护事件，定期生成周报、月报，并通过邮件发送至用户邮箱。
	事件紧急通知：基于安全防护事件，提取紧急事件，并同时通过短信、邮件两种方式通知用户。

04 订购信息

- 说明：（为方便展示，以下均采用设备简称）
  - **USG6625F/USG6635F/USG6655F/USG6685F/ USG6636F/ USG6656F/ USG6686F的订购信息同USG6615F;**
  - **USG6710F/USG6715F的订购信息同USG6725F。**

产品	型号	描述
USG6615F	USG6615F-AC	USG6615F交流主机(8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+)
USG6725F	USG6725F-AC	USG6725F交流主机(4*QSFP28 + 16*ZSFP+ + 8*SFP+)
基本License		
虚拟防火墙	LIC-USG6KE-VSYS	虚拟防火墙功能
SSL VPN并发用户数	LIC-USG6KF-SSLVPN-100	SSL VPN并发用户数(100个)
	LIC-USG6KF-SSLVPN-200	SSL VPN并发用户数(200个)
	LIC-USG6KF-SSLVPN-500	SSL VPN并发用户数(500个)
	LIC-USG6KF-SSLVPN-1000	SSL VPN并发用户数(1000个)
	LIC-USG6KF-SSLVPN-2000	SSL VPN并发用户数(2000个)
	LIC-USG6KF-SSLVPN-5000	SSL VPN并发用户数(5000个)
NGFW License		
IPS特征库升级服务	LIC-USG6615F-IPS-1Y	IPS特征库升级每年(适用于USG6615F)
	LIC-USG6725F-IPS-1Y	IPS特征库升级每年(适用于USG6725F)
URL远程查询升级服务	LIC-USG6615F-URL-1Y	URL远程查询升级每年(适用于USG6615F)
	LIC-USG6725F-URL-1Y	URL远程查询升级每年(适用于USG6725F)
AV升级服务	LIC-USG6615F-AV-1Y	AV特征库升级每年(适用于USG6615F)
	LIC-USG6725F-AV-1Y	AV特征库升级每年(适用于USG6725F)
威胁防护年数(包含IPS，URL，AV，Web防护)	LIC-USG6615F-TP-1Y	威胁防护功能包每年(适用于USG6615F)
	LIC-USG6725F-TP-1Y	威胁防护功能包每年(适用于USG6725F)
恶意流量AI检测升级服务	LIC-USG6615F-MTAI	恶意流量AI检测升级每年(适用于USG6615F)
恶意流量AI检测升级服务	LIC-USG6725F-MTAI	恶意流量AI检测升级每年(适用于USG6725F)

产品	型号	描述
NGFW License		
工控安全功能	LIC-USG6615F-ICS-1Y	工控安全每年(适用于USG6615F)
	LIC-USG6725F-ICS-1Y	工控安全每年(适用于USG6725F)
DDoS防御增强功能	LIC-USG6700F-AntiDDoS	DDoS防御增强功能（适用于USG6700F)
	LIC-USG6600F-AntiDDoS	DDoS防御增强功能（适用于USG6600F)
IPv6+功能	LIC-USG6600F-IPv6+-LIC	IPv6+功能 (含SRv6,信道化子接口,iFit)（适用于USG6600F)
	LIC-USG6700F-IPv6+-LIC	IPv6+功能 (含SRv6,信道化子接口,iFit)（适用于USG6700F)
N1 License		
USG6615F	N1-USG6615F-F-Lic	N1-USG6615F基础功能包，每设备
	N1-USG6615F-F-SnS1Y	N1-USG6615F基础功能包，每年软件订阅与保障年费，每设备
	N1-USG6615F-A-Lic	N1-USG6615F高级功能包,每设备
	N1-USG6615F-A-SnS1Y	N1-USG6615F高级功能包，每年软件订阅与保障年费，每设备
USG6725F	N1-USG6725F-F-Lic	N1-USG6725F基础功能包,每设备
	N1-USG6725F-F-SnS1Y	N1-USG6725F基础功能包,每年软件订阅与保障年费,每设备
	N1-USG6725F-A-Lic	N1-USG6725F高级功能包,每设备
	N1-USG6725F-A-SnS1Y	N1-USG6725F高级功能包,每年软件订阅与保障年费,每设备
乾坤安全云服务License		
USG6615F	N1-C-USG6615F-F-Lic	云部署模式-基础功能包，每设备,每年
	LIC-USG6615F-BA-1Y	边界防护服务-威胁自动阻断(适用于USG6615F)，每设备，每年
	LIC-USG6615F-TP-1Y	威胁防护每年(适用于USG6615F)
USG6725F	N1-C-USG6725F-F-Lic	云部署模式-基础功能包，每设备,每年
	LIC-USG6725F-BA-1Y	边界防护服务-威胁自动阻断(适用于USG6725F)，每设备，每年
	LIC-USG6725F-TP-1Y	威胁防护每年(适用于USG6725F)
iMaster NCE-HisecInsight		
USG6615F	LIC-USG6615F-TP-1Y	威胁防护每年(适用于USG6615F)
USG6725F	LIC-USG6725F-TP-1Y	威胁防护每年(适用于USG6725F)
SASE分支互联License		
USG6615F	N1-USG6615F-S-S-Lic	N1 SASE分支互连标准包（适用于USG6615F)
	N1-USG6615F-S-S-S1Y	N1 SASE分支互连标准包（适用于USG6615F），软件订阅与保障年费，每设备，1年
云沙箱检测服务		
USG6615F	LIC-USG6615F-CS-1Y	云沙箱检测服务每年(适用于USG6615F)
USG6725F	LIC-USG6725F-CS-1Y	云沙箱检测服务每年(适用于USG6725F)

华为技术有限公司
深圳龙岗区坂田华为基地
电话：+86 755 28780808
邮编：518129 www.huawei.com