华为HiSecEngine USG6300E系列AI防火墙（盒式）

随着企业业务不断的数字化、云服务化，网络在企业运营中占据着重要的位置，出于各种目的，网络攻击者通过身份仿冒、网站挂马、恶意软件等多种方式进行网络渗透与攻击，影响企业网络的正常使用。采用防火墙部署网络边界是当前防护企业网络安全的主要方式，但是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，还会引起设备性能的降低。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在不损坏用户隐私的情况下更是无法有效的识别。

华为HiSecEngine USG6300E系列AI防火墙，在提供NGFW能力的基础上，联动其他安全设备，主动积极防御网络威胁，增强边界检测能力，有效防御高级威胁，同时解决性能下降问题。产品提供模式匹配以及加解密业务处理加速能力，使得防火墙处理内容安全检测、IPSec等业务的性能显著提升。

产品图

华为HiSecEngine USG6300E系列AI防火墙（盒式）

HUAWEI

产品亮点

卓越性能

HiSecEngine USG6300E系列AI防火墙内置转发、加密、模式匹配三大协处理引擎，有效将小包转发性能，IPS、AV业务性能以及IPSec业务性能提升2倍。

智能防御

HiSecEngine USG6300E系列AI防火墙内置NGE、CDE威胁防御引擎。NGE作为NGFW检测引擎，提供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。

全新自研CDE（Content-based Detection Engine）病毒检测引擎，用智能技术重新定义恶意文件检测。提供数据深度分析，暴露威胁的细节，快速检测恶意文件，有效提高威胁检出率，帮助客户做到更全面的网络风险评估，有效应对攻击链上的网络威胁，真正实现攻击防御“智”能化。

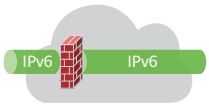
极简运维

融合云管理方案，即插即用，实现极速简易开局。安全控制器组件化融入AC-Campus，实现统一管理，策略下发，有效提升防火墙运维管理。全新的Web UI2.0，以威胁可视化定义新安全界面，大幅提升易用性，简化运维。

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

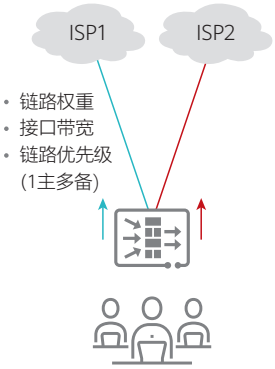
报文镜像

在不中断业务的前提下抓取、分析会话报文

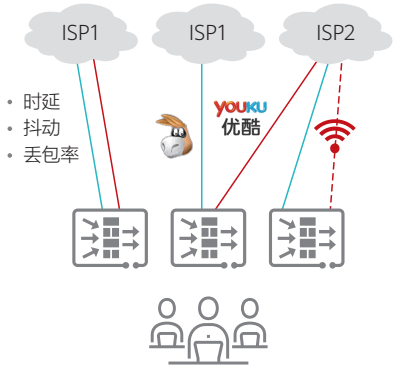
安全丰富的IPv6能力

随着《IPv6行动计划》在各行各业的逐步开展和深入，网络安全行业逐步进入IPv6时代，HiSecEngine USG6300E系列AI防火墙提供安全丰富的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。

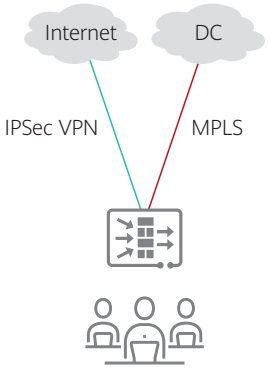
静态智能选路



动态智能选路



支持基于IPSec/internet/Mpls选路



智能选路

HiSecEngine USG6300E系列AI防火墙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、优先级或者自动探测到的链路质量动态地选择出接口，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。

产品规格

型号		HiSecEngine USG6306E-B	HiSecEngine USG6305E	HiSecEngine USG6309E	HiSecEngine USG6315E	HiSecEngine USG6325E
固定端口	业务口	16×GE + 8×GE Combo + 2×10GE (SFP+)	2×10GE (SFP+) + 8×GE Combo			
	Bypass	Y	--			
	WAN	--	2×GE			
	USB	1×USB3.0	1×USB2.0 + 1×USB3.0			
外置存储		选配，支持SSD 240GB/960G、HDD 1TB	选配，支持M.2卡，64G/240G			
产品型态		1U				
尺寸 (W×D×H) mm		442×420×43.6				
整机最大功耗		76.9W	40W			
电源 (AC) 输入电压		100-240V				
电源 (AC) 冗余		选配				
重量 (不含硬盘)		6.25kg	5.8kg			
工作环境	温度	0～45°C				
	湿度	5%-95%非凝露				
存储环境	温度	-40°C～70°C				
	湿度	5%～95%				

型号		HiSecEngine USG6335E	HiSecEngine USG6355E	HiSecEngine USG6365E	HiSecEngine USG6385E	HiSecEngine USG6306E-B
固定端口	业务口	2×10GE (SFP+) + 8×GE Combo				16×GE(RJ45) + 8×GE Combo + 2×10GE(SFP+)
	WAN	2×GE				--
	USB	1×USB2.0 + 1×USB3.0				USB3.0

型号		HiSecEngine USG6335E	HiSecEngine USG6355E	HiSecEngine USG6365E	HiSecEngine USG6385E	HiSecEngine USG6306E-B
外置存储		选配，支持M.2卡，64G/240G	选配，支持M.2卡，240G			选配2.5英寸形态硬盘，支持SSD 240GB/HDD 1TB
产品型态		1U				
尺寸 (W×D×H) mm		442×420×43.6				
整机最大功耗		40W				76.9W
电源 (AC) 输入电压		100-240V				
电源 (AC) 冗余		选配				
重量 (不含硬盘)		5.8kg				6.25kg
工作环境	温度	0～45°C				
	湿度	5%-95%非凝露				
存储环境	温度	-40°C～70°C				
	湿度	5%～95%				

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、数据防泄漏、带宽管理、Anti-DDoS、URL过滤、反垃圾邮件等多种功能于一身，全局配置视图和一体化策略管理。
应用识别与管控	可识别6000+应用，访问控制精度到应用功能。应用识别与入侵检测、防病毒、内容过滤相结合，提高检测性能和准确率。
云管理模式	设备自行向云管理平台发起认证注册，实现即插即用，简化网络创建和开局。 远程业务配置管理、设备监控故障管理，实现海量设备的云端管理。
云应用安全感知	可对企业云应用进行精细化和差异化的控制，满足企业对用户使用云应用的管控需求。
入侵防御与Web防护	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。可防护各种针对web的攻击，包括SQL注入攻击和跨站脚本攻击等。
防病毒	病毒库每日更新，可迅速检出超过500万种病毒。
APT防御	与本地/云端沙箱联动，对恶意文件进行检测和阻断。 支持流探针信息采集功能，对流量信息进行全面的信息采集，并将采集的信息发送到HiSec Insight进行分析、评估、识别网络中的威胁和APT攻击。 加密流量无需解密，联动HiSec Insight，实现对加密流量威胁检测。 主动响应恶意扫描行为，并通过联动HiSec Insight进行行为分析，快速发现，记录恶意行为，实现对企业威胁的实时防护。
数据防泄漏	对传输的文件和内容进行识别过滤，可准确识别常见文件的真实类型，如Word、Excel、PPT、PDF等，并对内容进行过滤。
带宽管理	在识别业务应用的基础上，可管理每用户/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。

功能特性	描述
URL过滤	URL分类库超过1.2亿，可对特定类别网站的访问进行加速，保障对高优先级网站的访问体验。 支持DNS过滤，直接根据域名对访问的网页进行过滤。 支持safesearch，对google等搜索引擎的资源进行过滤，保障访问健康网络的资源。
行为和内容审计	可基于用户对访问内容进行审计、溯源。
负载均衡	支持服务器负载均衡和链路负载均衡，充分利用现有网络资源。
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、L2TP VPN、MPLS VPN、GRE等；提供自研的VPN客户端SecoClient，实现SSL VPN、L2TP VPN和L2TP over IPSec VPN用户远程接入。 支持DES、3DES、AES、SHA、SM2/SM3/SM4等多种加密算法。
DSVPN	动态智能VPN，为公网地址动态变化的分支之间建立VPN隧道，降低大量分支间的组网和运维成本。
SSL加密流量检测	检测并防御隐藏在SSL加密流量中的威胁，包括入侵防御、反病毒、内容过滤、URL过滤等应用层防护。
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。
Anti-DDoS	支持DDoS攻击防护，防范SYN flood、UDP flood等10+种常见DDoS攻击。
用户认证	支持多种用户认证方式，包括本地认证、RADIUS、HWTACACS、AD、LDAP等。防火墙支持内置Portal及Portal重定向功能，与 Agile Controller配合可以实现多种认证。
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。
安全策略管理	支持基于VLAN ID、五元组、安全域、地区、应用、URL分类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。 预置常用防护场景模板，快速部署安全策略，降低学习成本。 与FireMon，Algosec公司合作提供安全策略管理解决方案，降低运维成本，减少故障风险。
丰富的报表	可视化多维度报表呈现，支持用户、应用、内容、时间、流量、威胁、URL等多维度呈现报表。 通过华为安全中心平台生成“网络安全分析报告”，对当前网络的安全状态进行评估，并给出相关优化建议。
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。
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