



产品概述

UX600-24GF4T 是优力普自主研发的一款基于先进的 MIPS 嵌入式多核构架的上网行为管理产品，具有 12 千兆电接口数量，支持 12 千兆 SFP 光接口，支持 4 万兆接口总数；接口无路由/交换/LAN/WAN 等固化区

分，均可作为二三层接口使用，支持多桥组部署。

UX600-24GF4T 系列产品面向中小企业、宽带网络边界、网络和数据中心等多个层次开发和设计，通过单路径并行处理的应用识别和安全检测引擎，融合用户上网行为管理、内容审计、上层业务优化等功能，可谓用户提供一个综合和完整的解决方案。

UX600-24GF4T 系列可以工作在路由、桥接、混杂等多种方式部署在网络的关键节点，对应用数据进行 L2-L7 层的全面检测和分析。深度检测、管控和审计千余种 IM 即时聊天、P2P 下载软件、在线视频、VOD 流媒体、购物、炒股、网游等常见应用，支持 BYOD 特征库，可识别 ios 版和安卓版移动互联网软件如腾讯微博、QQ 空间等特征，针对特定无应用指纹的应用：迅雷、P2P 下载支持行为模式的智能识别，并利用智能流控、一键阻断、智能路由等技术提供有效管理。提供 SSH、WEB、集中管理和账户分级等多种交互方式，是广大企业用户提高网络安全的理想选择。

产品特点

● 灵活的场景适应能力

UX600-24GF4T 安全审计网关可适应用户各种复杂网络场景。在满足路由、透明、旁路、混合等部署模式同时，配合 IPv4/IPv6 双协议栈，结合静态路由、动态路由、策略路由、ISP 路由、链路负载均衡和服务器负载均衡等，可在 802.1Q、GRE、RIP、OSPF、VRF、多出口等各种复杂的网络环境中灵活组网。

● 精细的行为管理

UX600-24GF4T 产品控制层面不再局限对网络应用的阻断，更能深入识别应用的内置动作。例如对 QQ 的控制力度不仅仅是登录动作，更可识别到收文件、发文件、语音、视频等动作，对微信也可识别控制多达 11 种行为动作。

UX600-24GF4T 可快速识别“一拖 N”的网络私接行为，精准定位“N”即私接用户数量，并进

行有效精细的针对终端类型进行管控，及时发现非法热点，预防个人用户私接路由，通过对应用的更精细化管理让网络更有序。

- **SSL 内容解密**

UX600-24GF4T 提供了 HTTPS 审计功能，采用特有的加密流量识别技术，能够对主流的加密网站、加密网站搜索记录、加密邮件等进行行为识别。管理员可以采用自定义的方式，定向审计用户和加密网站，保障网络行为清晰的事后审计，有效的防止企业机密外泄。

- **动态带宽管理**

UX600-24GF4T 产品采用智能流控、智能阻断、智能路由等技术，将网络出口带宽划分为逻辑通道，并支持在通道中再划分子通道，完美进行带宽限制和带宽保障。同时支持将类型复杂的网络流量分布到不同的网络出口转发，是企业提升带宽利用率、保护带宽投资的最佳利器。

- **清晰的内容审计**

UX600-24GF4T 产品支持详细、清晰、易用的日志特性，可以全面记录审计用户上网行为、使用流量、访问网站、所用终端系统及设备类型平台等信息；日志支持定制化过滤器，可根据 IP 地址、认证用户、访问应用、访问 URL、发帖内容等要素进行搜索，让事后审计省时省力；可支持对 HTTPS、邮箱类解密策略的配置。以柱状图、饼状图、百分比等形式最直观地体现网络运行状况，让网络管理规划有据可循、有的放矢。

- **配置维护简洁**

UX600-24GF4T 产品具备多面、简单化和安全的管理特性，简化网络运维，降低安全成本，适用于各种网络场景。除支持本地管理之外，可配合网管平台进行快速上线、集中配置下发和日志收集，极大的释放了运维压力；支持拓展云管理，实现大数据分析；双因子 UKey 认证提供双重认证方式，极大的提高了网络的安全性；端口镜像、端口漂移、链路服务质量统计、界面抓包等运维工具，助力运维。

- **全方位的身份认证手段**

本地认证：Web 认证、用户名/密码认证、IP/MAC/IP-MAC 绑定；

单点登录：AD 域、安博通 AAA 系统、第三方系统等；

第三方认证：RADIUS、LDAP、IMC、AAS、SAM 等

APP 认证：不需要借助数据中心软件，无需 APP 修改，避免协调沟通成本；

微信认证：连接商家 WIFI，自动弹出“一键微信连 WIFI”，可强制关注公众号；

混合认证：用户根据需求切换认证方式；

● 营销增值服务

创新的将 APP 缓存在设备本地，当用户下载时直接推送，几十 M 的文件只要几秒钟，极大的提升了带宽利用率的同时大大加速和提升了用户体验；并且支持 iOS 和安卓 APP 的缓存，业界技术领先；在低成本的投入下同时为客户的终端营销推广开辟了新的方向。配合 APP 身份认证，可强制推广商户的 APP，提高商户的 APP 安装率，拥有更多的可转化潜在用户。

支持对用户进行广告推送的功能。广告推送作为电子商务营销阶段的应用，具有灵活性、互动性和目标受众准确的特点，极大的降低了广告投放的费用，广告推送为大量的广告主服务，把互联网广告以合适的方式推送给合适的消费者，广告投放的精准性高，转化率高。

● 高度可靠性

UX600-24GF4T 安全审计网关支持双机热备和软硬件 bypass 功能，不会成为网络瓶颈和故障点，确保网络高可靠性。当设备 CPU、内存等参数高于一定阈值时，自动 bypass 设备，让整个设备变为纯透明转发，保证业务不中断。

Bypass 最大功率 300W；内置软件 Bypass 模块，内置一路电口 Bypass；在设备流量异常时，可自动切换到 Bypass 状态，当设备恢复时，可自动切换回工作状态；

产品规格

硬件规格

产品型号	UX600-24GF4T
业务接口	12 个千兆电接口 12 个千兆 SFP 光接口 4 个万兆接口
管理接口	任一业务接口
Console	1 个 RS232/RJ45
扩展插槽	1 个 TF 槽
PoE 供电接口	无
CPU	Cavium CN7020
CPU 主频	800MHz
CPU 核数	2
吞吐量	40Gbps
应用层吞吐量	15Gbps
最大并发连接数	1000 万
新建连接数	60 万
适用带宽	2G

用户数量	2 万人
内存	1GB
FLASH	4GB
硬盘	32G TF
产品性能使用场景推荐	80M 带宽/300 用户
电源	AC 220V 内置
输入额定电压	AC 100~240V
最大输入电流	1A
最大功率(W)	25W
MTBF	≥100000 小时
外形尺寸	320*44*205mm
重量	1.9kg
工作温度	0°C~40°C
工作湿度	5%-90%非凝露
环保认证	符合 Rohs

软件规格

网络功能	部署模式	旁路	单接口监听交换机镜像流量	
		串行	支持透明、路由、混合（透明+路由）、多组桥、多口桥	
		混合	支持旁路和串行混合部署	
	网络接口配置	物理接口	启用/关闭	
			IPv4 地址类型：静态（支持主从）、DHCP 动态获取 IP、PPPoE 动态获取 IP	
			IPv6 地址类型：静态（支持主从）	
			DHCP 下发 DNS	
			接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping	
			协商模式：自动、强制（可设置双工和速率）	
			工作模式：路由模式、桥模式	

		MTU, 修改范围 1280-1500
	子接口	子接口管理 (增删改)
		子接口 ID: 1-4094
		启用/关闭
		IPv4 地址类型: 静态 (支持主从)、DHCP 动态获取 IP、PPPoE 动态获取 IP
		IPv6 地址类型: 静态 (支持主从)
		接口管理方式: HTTPS、HTTP、SSH、Telnet、Ping
		MTU, 修改范围 1280-1500
	桥接口	桥接口管理 (增删改)
		桥接口 ID: 0-255
		启用/关闭
		IPv4 地址类型: 静态 (支持主从)、DHCP 动态获取、PPPoE 动态获取
		IPv6 地址类型: 静态 (支持主从)
		接口管理方式: HTTPS、HTTP、SSH、Telnet、Ping
		MTU, 修改范围 1280-1500
	聚合接口	聚合接口管理 (增删改)
		聚合接口 ID: 0-255
		启用/关闭
		IPv4 地址类型: 静态 (支持主从)、DHCP 动态获取、PPPoE 动态获取

		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	loopback 接口	支持生成、配置 loopback 接口。（命令行支持）
		支持基于 loopback (或指定 IP) 接口地址的管理 (设备管理等) (命令行支持)
	隧道接口 (显示)	隧道模式：IPv6 隧道、IPSec 隧道
		显示项目：接口名称、隧道模式、连接状态、启用状态
	4G 接口	支持联通 4G 上网卡 (推荐：华为 E3372)
	虚拟线	支持虚拟线功能，bypass 部分安全功能和安全策略
		支持虚拟配置
		支持端口联动
		数据传输支持 vlan tag 过滤
	TCP MSS 调整	支持根据业务类型智能调整
		命令行支持接口 TCP MSS 手工调整，支持全局设置和 VPN 单独配置
	端口镜像	镜像接口
镜像功能		支持将多个物理接口的流量镜像到一个接口
		支持基于接口全部流量，上行流量，下行流量的镜像
DHCP	DHCP 服务类型	DHCP 服务器
		DHCP 中继代理
	服务器属性	网络配置：网关、子网、开始结束 IP 地址

		租约：无限、有限时长	
		高级属性：DNS 支持 2 个，Wins 支持 2 个，域	
		支持排除地址	
		支持 IP-MAC 绑定	
	DHCP 监视器	显示 IP 地址和 MAC 地址及开始时间、结束时间	
		清除条目	
	IPv4 路由	路由表	显示设备路由信息
		高级路由属性	支持非对称路由
			命令行下支持强制源进源出
		静态路由	增删改
支持基于路由权重的多链路负载均衡			
支持路由优先级			
支持 VRF 配置			
策略路由		增删改、移动	
		5 元组策略路由+时间	
		基于用户的策略路由	
		基于应用的策略路由	
		支持基于路由权重的多链路负载均衡	
ISP 路由		内置电信、联通、移动、教育网 ISP 信息	
		支持自定义 ISP 信息	
		增删改	
RIP		支持 v1、v2	

		支持缺省路由发布和路由重发布	
		支持接口下发送版本和接收版本的设置	
		支持认证方式：字符、MD5、不需要认证	
		OSPF	支持缺省路由发布、路由重发布
			支持 OSPF 网络区域信息的增删改
			支持接口下相关配置
	支持认证方式：字符、MD5、不需要认证		
	NAT	通用功能	支持日志发送
地址池			
源 NAT		支持配置的增删改、移动	
		源地址转换类型：出接口、地址池、不转换	
目的 NAT		支持配置的增删改、移动	
		目的地址转换类型：地址池、转换端口、不转换	
静态 NAT		支持配置的增删改查、移动	
ALG		动态端口支持协议 ALG：H.323、SIP、FTP、TFTP、PPTP	
		FTP、TFTP、SIP 支持非标准端口设置	
会话限制		规则管理	增删改
	功能	支持基于地址对象的限制	
		支持基于 IP 的会话数、每秒新建的限制（如引用地址对象，则对地址对象中的每个 IP 地址进行限制）	
	限制阻断	显示限制信息	
		IP 会话限制内容：IP 地址、连接数、会话限制、每秒新建、每秒新	

		建限制、限制阻断统计、引用地址对象名	
		支持查询过滤和全部显示	
		会话监控	
		实时会话支持多条件多维度筛选，条件支持点击生成，手动编辑	
		会话统计	支持列选择，列排序
		显示当前 IP 地址的连接数	
		支持实时会话，历史会话的趋势图展示	
		支持基于源 IP，目的 IP，目的端口会话数排名	
	地址探测	接口探测	支持 session 状态监控
			支持 ping 地址监控条目
			支持 tcpsyn 地址监控条目
			支持 dns 地址监控条目
		地址探测组	支持接口类型：物理接口，子接口，桥接口，聚合接口，隧道接口
			支持多个地址探测从属组关系
分为严格模式和非严格模式（严格模式即所有探测条目均成功组状态才成功，非严格模式探测条目间为独立状态）			
支持对探测组描述			
路由探测		支持探测路由以确保路由有效性	
支持场景及部署方式		支持静态路由或 ISP 路由联动	
	支持与接口状态联动		
	支持与 HA 联动		
日志说明	可对地址探测失效、恢复有日志记录		
链路负载均衡	链路负载均衡	支持基于权重的链路负载均衡	

衡		支持基于优先级的链路负载均衡
		基于直连网段和特定网段的负载均衡排除
		负载均衡接口支持健康探测
		支持基于负载均衡接口的 dns-dnat 功能
		支持负载连接统计
		基于七元组的链路负载均衡策略
		基于域名的负载均衡策略
		基于接口, 接口组的负载均衡策略
		负载均衡接口支持 pppoe, dhcp, 聚合链路, 物理接口, 等三层接口
服务器负载均衡	服务器负载均衡	支持基于连接权重的服务器负载均衡
		支持基于源地址散列+权重的服务器负载均衡
		支持服务器组服务或服务器健康状态的探测
		支持服务器负载日志的开启关闭
DDNS	DDNS	支持花生壳 ddns 客户端以及域名 IP 绑定
		支持基于接口绑定的 ddns
		支持记录 ddns 更新日志
		支持配置多条 DDNS 更新任务
二层支持	VLAN	vlan 子接口
		子接口都支持 IEEE 802.1Q, 能进行封装和解封。
		支持对报文进行二次基于 802.1Q 封装的 VLAN-VPN 应用。(QinQ)
	生成树协议	支持 802.1d 的 STP 生成树协议。

		报文透传	支持二层解封装和再封装，对上层透明
	IPv6	基础功能	<p>IPv6 地址对象</p> <p>IPv6 IPS 安全防护</p> <p>IPv6 路由通告</p> <p>IPv6 静态路由、OSPFv3</p> <p>支持用户和应用均为任意的 7 元组策略，URL 过滤，病毒防护</p> <p>扩展报文头的逐跳报文的处理、分片报文等的处理</p> <p>隧道支持：手工隧道，6to4 隧道，ISATAP</p> <p>防畸形报文攻击</p> <p>识别终端到特定服务器的 APP 下载，设备自动根据终端的下载地址下载 APP</p> <p>支持文件的应用缓存</p> <p>支持文件名模糊匹配的文件缓存</p> <p>支持 PING、TCP、DNS 探测</p>
网络优化	APP 动态缓存	APP 动态缓存	支持接口探测
	应用缓存	应用缓存	支持针对特定域名的 APP 缓存, 只要是该域名传输的 APP 全部缓存
			支持自定义间隔时间探测
	服务质量管理	服务质量管理	接口默认属于 root，创建 VRF 后可把接口添加到 VRF 内，一个接口只能属于一个 VRF；
			不同 vrf 下的接口可以配置相同的 ip 地址
			支持静态路由

			支持手动配置
虚拟路由	VRF	接口虚拟化	支持触发防攻击规则和 IPS 阻断源地址规则自动进入黑名单
		IP 地址重叠	支持生存时间配置
		静态路由	扫描攻击分析
安全防护	通用功能	黑名单	异常包攻击分析
			Flood 攻击分析
			基于接口的配置
		分析模块	支持自动加入黑名单
			扫描阈值设置
			端口扫描、IP 地址扫描
	扫描防护	通用	Ping of Death; Land-Base; Tear Drop; TCP flag; Winnuke; Smurf; IP 选项; IP Spoof; Jolt2
			启用与关闭
			支持 ARP 学习与主动保护
		扫描方式	可设置 IP-MAC 绑定
	异常包防护	异常包类型	防 ARP Flood 攻击
	ARP 防护	防 ARP 攻击	支持 ARP 表查看、绑定、清除、接口信息
			基于接口的 ARP 学习控制
			一体化配置
			基于目的 IP、IP 范围
支持接口防御			
	ARP 学习控制	阈值设置	

			SYNFlood、UDPFlood、ICMPFlood、DNSFlood
	Flood 防护	通用	增删改
			绑定接口
			支持基于接口的上下行带宽管理
		支持类型	支持高、中、低优先级通道设置
流量管理	通用功能	配置管理	支持应用、用户、源地址、服务、时间的通道匹配
	流量控制	线路管理	保障带宽
			限制带宽
		通道管理	支持针对用户名实现每用户限速
			支持针对终端 IP 实现每 IP 限速
			自动支持流量整形
			支持用户、地址排除
			支持基于时长的限额策略
	支持基于流量的限额策略		
	支持日限额，月限额		
	排除策略	排除策略	支持限额的提醒，可自定义提醒阈值
	限额策略	限额策略	支持超出限额阈值时进行阻断，流控
			支持基于策略的 https 网站解密
支持自定义 https 网站解密			
支持预定义 https 网站解密			
支持 ssl 加密网页版邮箱的解密			
解密策	https 网站	https 网站解密	支持 ssl 加密客户端版邮箱的解密

略	解密		支持解密策略的启用禁用
			支持基于入接口, 源地址, 目的地址多维度的解密策略
	ssl 邮箱解密	ssl 邮箱解密	支持解密后阻断
			支持解密策略排除特定的站点
	解密策略	解密策略	支持用户共享网络监测
			支持共享网络用户终端数阈值配置, 支持不同终端单独配置
			支持共享网络的状态冻结、解锁
			支持阻断的自定义提示
	防共享上网	防共享上网	支持基于 IP 或 IP 网段的共享网络监测白名单
			支持策略增删改查、启用/禁用、移动
支持策略匹配次数清零			
支持修改默认策略动作: 允许/拒绝			
七元组策略匹配条件: 用户、应用、源地址、源接口、目的地址、目的接口、服务			
访问控制	IPv4 策略	配置管理	支持基于时间表的策略配置
			支持应用选择过滤
			支持基于应用的应用类型组选择
	策略	支持策略动作为: 审计、免审计、拒绝	
		基于策略的长连接 (老化时间)	
		支持动作为拒绝的策略进行日志记录	
		支持策略增删改、启用/禁用、移动	
		支持策略匹配次数清零	

	IPv6 策略	配置管理	支持修改默认策略动作：允许/拒绝	
			支持用户和应用均为任意的 7 元组策略	
			支持基于时间表的策略配置	
		策略	支持策略动作为：允许、拒绝	
			支持动作为拒绝的策略进行日志记录	
			增删改	
	防火墙	应用过滤策略	配置管理	支持根据应用行为来区分不同应用的审计内容
				根据应用行为确定审计内容
				支持基于关键字或者数字的内容审计
		策略	支持允许/阻断的策略动作	
			审计日志选项:不记录、紧急、告警、严重、错误、警示、通知、信息	
			增删改	
URL 过滤策略	配置管理	支持预定义和自定义 URL 分类过滤		
		支持恶意 URL 过滤		
		内置 URL 分类库, 策略高达 1230W 条, 支持 56 个 URL 分类, URL 库可在线升级		

		支持 URL 阻断和审计 (动作: 允许、拒绝)
		URL 日志选项:不记录、紧急、告警、严重、错误、警示、通知、信息
	策略	审计用户名、所在组名
		审计应用名、所在应用类
		审计操作系统、平台、终端、供应商
		审计源 IP 地址、目的 IP 地址、目的端口
应用控制及 审计	通用审计内容	基于帐号的登录控制、黑/白名单
		支持非加密收发消息时的关键字内容审计
		识别迅雷等 P2P 软件
		基于行为 (登录、交易、行情) 的控制和审计
		支持自定义关键字对象
	即时通讯	基于行为的控制和审计
		基础协议
		关键字过滤
	P2P 类	支持邮件内容审计, 不支持附件审计, 提供基于关键的邮件、http 等相关内容的关键字过滤功能。
	股票软件	支持普通版 webmail 审计 (QQ、163、126、新浪、139 邮箱)
	网络游戏	支持论坛 (BBS、博客) 主题过滤 (如果有)
	搜索引擎	论坛 (BBS、博客、微博) 内容过滤
	Webmail	支持以发件人过滤
		支持邮件客户端的主题、内容、附件名过滤

		社区类	支持记录邮件内容，需要带本地硬盘
			支持基于命令和操作的审计
		联系人	论坛上传下载文件名过滤
		非加密邮件	支持基于源、目的、规则集的入侵检测。
			支持 5 种自定义动作
		命令类	支持自定义 IPS 规则
			支持日志合并，符合告警策略后进行告警
IPS	入侵防御	入侵防御	支持网络态势感知
			支持防暴力破解
			支持服务器异常流量学习和非法外联检测
			支持弱密码检测及防护，弱密码扫描
			支持发现内网操作系统，应用，服务等
			支持 IPS 安全报表
			支持软件 bypass (CPU and 内存高于 70%)
			可记录攻击日志和报警。
			支持系统规则库手动、自动升级。
			系统定义超过 4000 条规则，包含 Backdoor, bufferoverflow, dosddos, im, p2p, vulnerability, scan, webcgi, worm, game。
		支持 HTTP, FTP, POP3, SMTP, IMAP 协议的病毒查杀	
		DDOS 防护	查杀邮件正文/附件、网页及下载文件中包含的病毒
		特征库	支持 300 万余种病毒的查杀，病毒库定期与及时更新
			支持启发式扫描查杀未知病毒

			3 年特征库升级服务
AV	防病毒	病毒防护	支持 ZIP/RAR 等压缩文件的病毒查杀
			压缩：默认 5 层，最大 20 层
			支持 TAR 等多种打包文件的病毒查杀
			支持 500+ 条预置 Web 防护规则，包括 SQL 注入，XSS，命令注入等 OWASP Top10 威胁
			支持多个字段匹配访问控制，支持与逻辑，支持匹配后不再继续安全检查
			支持 7 种级别日志记录
			支持全站，指定 URL，指定文件类型的防盗链
Web 防护	防护策略	规则防护	支持配置站点白名单，允许白名单中的网站调用资源
		精准访问控制	支持 7 种级别日志记录
			支持 CSRF 攻击防护，支持配置防护 URL
		防盗链	支持 7 种级别日志记录
			支持全站、指定 URL 的 CC 攻击防护
			支持配置检测时长，访问次数
		CSRF 防护	支持 7 种级别日志记录
			支持隐藏 Server 信息
		CC 攻击防护	支持隐藏 X-Powered-By 信息
			支持替换客户端出错页面
			支持替换服务端出错页面
		应用隐藏	支持 7 种级别日志记录

			支持配置防篡改起始 URL，支持配置例外 URL	
			支持 7 种级别日志记录	
			支持每月更新规则库	
			支持 500+条预置 Web 防护规则，包括 SQL 注入，XSS，命令注入等 OWASP Top10 威胁	
		网页防篡改	支持缓存篡改前的页面	
			支持手动清理缓存	
		规则库	规则库	支持 X.509 V3 数字证书，支持 DER/PEM/PKCS12 多种证书编码。
				支持内置 CA，为其他设备或移动用户签发证书。
		防篡改缓存	防篡改缓存	支持本地 CA 根证书、根私钥的更新。
				支持在线 CRL 列表。
PKI	PKI	证书格式	支持 IKEv1	
		本地 CA	支持主模式和野蛮模式	
			预共享密钥	
			RSA 证书认证	
VPN	IPSec VPN	IKE 第一阶段协商模式	IPSec 支持国密算法	
		国际标准算法(DES/3DES/AES/MD5/SHA-1)		
		IKE 身份认证	支持隧道模式	
			支持 ESP 和 AH 封装	
		国密	网关到网关	
		加密/HASH 算法	远端地址为动态	
		IPSec 封装模式	对端地址为 DNS	

	和协议	Hub Spoke 组网, spoke 之间通过 IPsec 通信
	部署模式	VPN track (可以探测到 VPN peer 地址不可达并将隧道删除)
		客户端远程接入, 支持扩展认证和模式配置
		隧道 VPN
		支持 IPsec 冷备份, 主 VPN 断开, 备 VPN 触发开始建立
		基于安全策略配置/基于路由 (隧道口) 配置
		DPD
		NAT 穿越
	IPsec 冷备份	FQDN
	配置方式	DH 组配置
	其他特性	PFS
		隧道监视器
		支持隧道持续时间统计等
		支持用户强制下线
		支持 IPsec 快速 vpn 配置
	维护手段	支持中心端和客户端方式部署
	流量统计	支持本地传输子网配置
	用户功能	支持 VPN 内网段映射
IPsec 快速 VPN	IPsec 快速 VPN	支持 VPN 链路优先级选择
		支持显示 SSL VPN 在线用户, 支持显示发送接收字节数, 登录时间 在线时长等
		支持在线用户批量冻结, 注销

			支持配置资源 IP, 资源 IP 范围
			支持资源导入导出
SSL VPN	在线用户		支持配置预定义资源类型, 自定义资源类型
			支持配置门户页面, 标题, logo, 公告
	资源		支持配置客户端下载链接
			支持对用户授权资源, 进行访问控制
			支持拨入时间段限制
	门户页面		支持配置强制下线时间
			策略支持导入导出
	策略		支持选择 2 个 SSL VPN 拨入接口
			支持两条链路完成 SSL VPN 功能
			支持配置 SSL VPN 端口, 全局 DNS, 地址池, 默认路由
			支持用户多处登录
			支持防暴力破解功能
	全局配置		支持 OpenSSL 加密库中的 SSLv3/TLSv1 协议函数库
			使用树形展示和管理用户, 基于组织结构和属性两个维度展示用户
			用户支持有效期
			支持初次认证修改密码
SSL VPN 加密类型	SSL VPN 加密 类型		用户、组的导入导出
用户管 理	通用功能	显示	用户、组的新建、删除
		有效期	支持用户组

	修改密码	可以在认证用户、固定 IP 用户、匿名用户之间自由变换
	导入导出	支持用户和用户组的移动功能
	新建、删除	支持单选移动, 多选移动, 全部移动
	用户组	支持批量用户密码设置
	用户种类的改变	支持批量用户启用禁用
	批量操作	支持用户用户组的模糊查询功能
		支持用户用户组的一键全部清除功能
		支持伪 portal 抑制功能 (http-APP) (命令行)
		基于 https 访问弹出认证 portal
	模糊查询	对认证用户、移动用户、第三方认证用户支持超时时间检查
	一键清除	增删改
	伪 portal 抑制	支持 HTTP 登录
	https 弹 portal	本地认证 (支持无感知认证)、认证服务器、静态绑定
	超时检查	锁定时间
认证用户	账号管理	认证用户保活
	认证服务器	支持唯一性检查
	认证方式	登录后重定向页面
	认证设定	绑定多个认证地址
		用户登录和注销界面
		支持移动设备登录页面自适应
		支持 SNMP 同步用户, 支持周期性同步, 支持自动录入用户, 支持 IP/MAC 绑定, 支持下载同步结果

		支持 ARP 扫描同步用户，支持周期性同步，支持自动录入用户，支持 IP/MAC 绑定，支持下载同步结果
	基本功能	支持 LDAP 同步用户，支持周期性同步，支持自动录入用户
		用户可绑定 IPv6 地址
用户同步	SNMP 同步	自动添加用户
	ARP 扫描	内置移动用户组
	LDAP 同步	与 AAS 联动
IPv6 支持	IPv6 用户	基于已认证用户逃生
移动用户	用户	基于全部用户逃生
	移动用户组	支持 portal server 探测
AAS 联动	与 AAS 通信	与 IMC 联动
portal 逃生	portal 逃生	对于未识别出用户的流量，策略将其 web 访问的流量重定向到指定的 portal 页面
		用户认证成功后，记录该用户信息。
		用户认证成功后的访问流量，可识别并定期刷新
IMC 联动	与 IMC 通信	Portal 页面自定义
	用户强制 Portal	对认证用户进行细粒度业务控制
		推送认证页面，接收 Portal 用户的认证信息
		发起用户认证请求以及用户下线通知
		提供用户自服务选项，链接到中央 Radius 服务器提供的自服务页面完成相应功能。
业务控制	强制用户在访问网页时需重定向至指定 portal server 并认证	

		接收 Portal	记录 portal 上用户上下线信息日志
		Server 发起的认证请求	设置识别的 IP 地址范围
		用户认证	匹配项：源接口、源地址、目的接口、目的地址、时间
		用户上下线日志	重定向页面选项（相关行为）
用户策略	识别相关	识别范围	支持微信、短信、本地、免认证、portal 认证、混合认证
	重定向	重定向页面	管理员账号的增删改查
	策略	认证策略	只读管理员查看配置权限（审计员） 登录认证方式支持本地认证、Radius 服务器认证、LDAP 服务器认证 密码复杂度：必须包括数字，英文和字符，8-31 个字符
系统管理	系统管理员	账号管理	支持系统管理员的 U-key 双因子认证
			每帐号可绑定 3 个 IPv4 地址或子网
			支持三权分立
			支持账号唯一性检查
			最大登录重试次数 1-60 次，默认为 5 次
			登录失败阻断间隔 1-3600 秒，默认为 1 分钟
	管理设定	页面超时时间 1-480 分，默认为 10 分钟	
		在线管理员 1-20 个，默认为 20 个	
		支持管理员在线监控和强制下线	
		支持管理员黑名单，阻断用户可监控，可解锁	
			支持用户信息在远端 Radius 服务器存储

		支持多用户第三方存储远端请求认证
	在线用户管理	单服务器认证
	阻断用户	支持用户信息在远端 LDAP 服务器存储
认证服务器	Radius	支持多用户第三方存储远端请求认证
		支持 LDAP 用户、用户组同步认证
		单服务器认证
	LDAP	Radius/LDAP 服务器组，支持主备和集群
		支持无感知认证
		支持短信验证码验证身份实现 wifi 认证上网
		支持 AD 服务器的单点登录认证方式
	服务器组	支持微信连 wifi 认证方式
	短信认证	支持强制关注功能
		支持无感知认证
	AD 单点登录	支持免认证
	微信认证	不同认证方式的 portal 支持内容自定义
		支持多种认证方式的混合认证
		手工设置时间
	免认证	NTP 同步
portal 自定义	设备间同步时间 (通过 NTP 保持一致)	
混合认证	恢复出厂配置	
系统维护设定	系统时间	系统重启
		旁路部署

		许可证
系统重启		配置文件导入导出
		双备份配置
部署方式		系统升级手动、自动、升级历史
授权		支持断点续传
配置文件		动态库升级 (应用、URL、IPS、AV)
		ping 探测
系统升级		traceroute 探测
		TCP SYN 探测
		支持按照过滤条件抓取数据报文
诊断工具		支持将报文下载到本地保存查看
		设置方式: 手动搜集和自动收集
		收集内容操作: 下载、查看、删除
抓包工具		电口断电 bypass
		电口启动过程 bypass
信息收集		IPS 模块软件 bypass: 瞬时 cpu 使用率超过 70%按 10:1 进入检测流程, 命令行可调比例
		支持配置同步
可靠性	硬件 bypass	支持流同步
		支持特征库同步
	软件 bypass	支持接口状态监控
双机热备	主备模式	支持抢占模式

HA		支持备机可管理
		支持 AGG 口作为心跳口，提高心跳口可靠性
		支持 HA 状态监控
		支持认证用户同步
		支持流同步
		支持接口状态监控
		支持地址代理
	主主模式	支持非对称路由
		支持 AGG 口作为心跳口，提高心跳口可靠性
		支持两个或者多个接口状态绑定
		SNMP 代理
		版本：v1、v2、v3
		trap 版本：v1、v2 Notification、v2Inform
接口状态同步组	物理状态同步	trap 地址
SNMP	SNMP 配置	CPU、内存
		增删改查
	trap	认证方式：None、MD5、SHA
		支持 snmp 跨三层取 mac
	私有 mib	支持同时多台交换机跨三层取 mac
	SNMP 用户	支持 snmp V1 V2 V2c 版本
		支持 IPMAC 绑定

		支持 4 个 DNS 服务器
	跨三层取 mac	静态域名 (256 个)
		支持基于出接口的 dns 权重比例透明代理
	IPMAC 绑定	支持基于出接口的 dns 优先级透明代理
域名相关	DNSserver	支持基于出接口的流量权重比例的 DNS 透明代理
		支持静态域名 (支持模糊匹配, 支持优先级匹配)
	DNS 透明代理	支持特定域名特定 dns 服务器解析 (支持模糊匹配)
		支持 dns 透明代理缓存功能的开启关闭
		透明代理链路 dns 主持主备配置
		日志服务器: 地址和端口 (3 组)
		本地日志记录开关、日志服务器日志级别开关
		设备映射表流量、上网行为、系统管理
		各模块 Debug 支持
日志设定	syslog 日志配置	支持多份配置保存
	日志过滤	支持下次启动配置指定
	设备映射表	支持配置拷入, 拷出备份列表
Debug	命令行	支持 U 盘版本升级
配置管理	配置管理	支持 U 盘配置导入
		支持 U 盘的零配置上线
		支持中英文版本的切换
		支持本地中英文 Web 界面管理及命令行管理, 支持基于 SSL 协议的远程安全管理

	U 盘零配置	U 盘零配置	支持管理端口的自定义	
			支持中英文版本的切换	
			支持管理端口的自定义 支持系统资源告警 支持 IPSec 告警	
	中英文版本	中英文版本	支持管理端口的自定义 支持系统资源告警 支持 IPSec 告警 支持邮件和弹窗告警，弹窗告警默认展示最近 10 条告警记录	
	管理端口自定义	管理端口自定义	支持管理端口的自定义 支持系统资源告警 支持 IPSec 告警 支持邮件和弹窗告警，弹窗告警默认展示最近 10 条告警记录 模块支持手动刷新	
	系统告警	系统告警	模块支持 5 秒，10 秒，30 秒，60 秒自动刷新	
			模块支持关闭	
			模块支持显示顺序自定义	
	监控	首页	通用功能	部分模块支持筛选过滤
				支持针对管理员保存风格
支持恢复默认风格				
支持新增会话数，当前会话总数趋势图显示				
支持威胁分类 TOP5 展示，支持图表和表格切换显示				

	风格保存	支持攻击趋势图显示
		支持显示系统日志
	会话数	支持显示 IPS 日志, AV 日志, 安全日志
	威胁分布	设备序列号、主机名称、产品型号、系统版本、APP 版本、授权信息
	攻击趋势	系统时间、日志汇总 (访问网站、收发邮件、论坛与微博、IM 聊天)、运行时间
	系统日志	基于物理口的上下行流量统计 bps (10 分钟 120 个点)
	威胁日志	整机总流量统计 Kbps/Mbps/Gbps
	系统信息	接口状态
		接口详细信息
	实时流量 (设备)	支持图表和表格显示方式切换
		Top 20
	接口信息状态	CPU、内存
		显示所有用户
	用户、应用流量	显示移动用户
	排名	支持列选择, 列排序
系统资源	按网段查询, 支持模糊搜索	
在线用户	全部用户	冻结、解冻
	移动用户	离线
	列操作	支持基于 IP 及 IP 段配置白名单
	查询	支持 基于用户、MAC、终端数量的监控

		管理	支持状态监控、解锁操作	
			应用统计总览可视	
	防私接防共享	防私接防共享	应用比例图呈现	
			应用统计趋势图总览	
			应用统计详细信息展现	
	流量监控	统计集	应用流量统计	应用与用户维度耦合
				应用 TOP11 统计
				支持实时应用流量统计
				用户统计总览
				支持用户统计柱状呈现
用户统计详细信息总览与应用维度耦合				
支持查看单个用户的应用趋势及应用 TOP 列表				
用户流量统计		用户 TOP15 统计		
		支持实时用户流量统计		
		支持接口上下行统计, 包含每小时、每天、每周		
		支持设备转发数据历史的可视化		
		支持每个接口收发数据历史的可视化		
流量监控		接口流量统计	支持将客户多种审计条件统一管理查看	
			支持对设备转发流量统计, cpu 使用率, 内存、会话、转发流量 4 项统计趋势图	
			支持时间选项查阅历史使用情况	

		用户信息中心	增删改查, 支持批量删除
			支持子网、地址范围、主机的地址添加方式
		健康统计	支持排除地址
			增删改查, 支持批量删除
资源管理	地址	IPv4 地址对象	支持子网、地址范围、主机的地址添加方式
			增删改查, 支持批量删除
			支持组嵌套
		IPv6 地址对象	支持 89 种预定义服务
			增删改查, 支持批量删除
		地址组对象	支持协议类型: TCP、UDP、ICMP、其他协议号
	增删改查, 支持批量删除		
	服务	预定义服务	支持预定义自定义服务添加
		自定义服务	支持组嵌套
			非标准端口 ALG (FTP、TFTP、SIP)
		服务组	支持应用自定义功能
	支持基于地址, 端口, 域名或 URL 的应用自定义		
	显示预定义分类, 支持 18 个分类		
	非标准端口配置	显示分类下应用的属性: 中英文名称、平台、风险级别、流行度、描述	
	应用	应用自定义	增删改查
支持修改识别模式以达到对应识别目的			
预定义应用		智能模式: 应用引擎将尽可能多的方法识别应用流量	

		快速模式：应用引擎关闭部分智能分析以提高性能
	应用组	关闭模式：应用引擎关闭
	识别模式	增删改查，支持批量删除
		内置任何时间条目：any
		日计划、周计划、月计划
		计时器
时间表	通用	支持对恶意 URL 手工排除
		查看预定义 URL 分类
	时间类型	增删改查，支持批量删除
		支持预定义 https 解密 URL
URL	恶意 URL 白名单	支持自定义 https 解密 URL
	预定义	支持统计用户的 URL 标签，上送 IMC
	自定义	支持 URL 阻断提示的自定义
	https 界面对象	增删改查，支持批量删除
		支持基于策略的广告推送功能
	URL 用户标签	支持策略的启用禁用
	阻断提示	支持基于广告对象的策略引用
关键字	自定义	支持外部广告服务器
广告设置	广告设置	最多支持三套广告模板
		分类记录
		日志存储空间耗尽后，可滚动覆盖
		系统关键事件日志，支持中文显示，支持日志导出

			管理员操作日志，支持中文显示，支持日志导出
日志查询	数据库	嵌入式数据库	攻击防护日志，支持中文显示，支持日志导出
			IPS 日志
	日志记录	系统日志	AV 日志
		操作日志	
		安全防护日志	
		IPS 日志	
		AV 日志	

订购信息

产品名称	产品信息
UX600-24GF4T	UX600-24GF4T 上网行为管理 (12 个千兆以太网电口, 12 个千兆 SFP 光口, 4 个万兆接口、网络吞吐能力 1Gbps、自带 32G 存储空间)