UNIS ACG1000-E-G 国产化应用控制网关产品彩页

产品概述

UNIS ACG1000-E-G 系列是 UNIS 推出的国产化网络审计产品。该产品可以路由模式、透明桥接模式、旁路模式以及混合模式部署在网络的关键节点。其融合了应用控制、行为审计、网络优化等全面功能，为用户提供一个综合、完整的全业务应用场景解决方案。

UNIS ACG1000-E-G 采用海光 3 系多核 CPU 架构。从软件、硬件两部分将信息产业创新政策贯通，打造新一代安全可靠，自主自控的下一代应用控制网关。在硬件部分，从芯片层面掌握安全可信、运行可靠的技术。在软件部分，搭载基于统信国产操作系统，从软件架构、功能研发、漏洞检测、软件发布、技术支持等环节实现全方面自主产权。可深度识别、精准管控和高效审计 IM 聊天软件、P2P 下载软件、炒股软件、网络游戏、流媒体、在线视频等近千种常见应用。

利用智能流控、智能阻断、智能路由等技术使其拥有强大的带宽管理特性。

配合创新的网络应用行为精细化管理功能、清晰易管理日志等功能，为用户提供了最全面、最清晰、最直观上网行为解决方案。

UNIS ACG1000-E-G

产品特点

网络适应性强

UNIS ACG1000-E-G 系列产品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。

全面身份认证

UNIS 以用户需求为导向，实现了丰富的身份认证手段：

- 本地认证：Web 认证、用户名/密码认证、IP/MAC/IP-MAC 绑定、802.1x 认证；
- 单点登录：标准 AD 域，一次登录，多次认证；
- 第三方认证：RADIUS、LDAP 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”并关注微信公众号；
- 短信认证：传统的认证方式，方便快捷；
- 访客二维码认证：连接网络的用户通过审核人员扫描二维码接入网络；
- 混合认证：界面配置选择多种认证方式，用户可根据需要更换认证方式；
- 免认证：用户免认证上线。

细致行为管理

UNIS ACG1000-E-G 系列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。

UNIS ACG1000-E-G 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 网站解密

UNIS ACG1000-E-G 系列提供了 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。

终端行为管理

UNIS ACG1000-E-G 联动终端行为管理客户端提供了一个高效、全面的解决方案。它通过深入的终端行为审计和高效的准入控制机制，帮助企业精确地管理和监控终端设备的使用情况。该产品能够对 PC 行为进行全面关键数据审计以及外接设备全面记录，防止敏感信息的泄露和非法内容的传播，通过 16 种精细化的准入检查规则，确保只有符合企业安全策略的设备才能接入网络，有效防止了恶意软件的威胁和网络资源的滥用。

动态带宽管理

UNIS ACG1000-E-G 系列产品采用智能流控、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。

助力营销推广

UNIS ACG1000-E-G 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。

UNIS ACG1000-E-G 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。

快易安全互联

UNIS ACG1000-E-G 的 VPN 模块具有业界领先技术，在复杂网络环境下大大简化了管理员的维护工作量。配合集中管理和数据分析系统，可实现 VPN 快速零配置上线，隧道接口感兴趣流等无需配置自动协商，整个 VPN 网络全自动收敛，自适应多线路，完美的解决了分支运维能力弱的问题。而独创的主备切换 0 丢包技术，可实现 TCP 业务不中断，完美的解决 HA 切换 VPN 业务不中断。

UNIS ACG1000-E-G 支持 4G 网络并支持 4G IPsecVPN 加密连接，无需改变原有网络架构，在主线路故障时主动承接和中心端的网络加密通信，具备数据完整性、数据传输安全、高性价比、网络无改变等特性，可让管理员高枕无忧。

高级安全防护

UNIS ACG1000-E-G 具备超过 8000+种预定义攻击特征的入侵防御功能和海量病毒特征独特实时病毒拦截技术以及高效引擎的病毒防护功能，实时的对流量进行分析，从数据链路层到应用层有效的阻断网络中的攻击和病毒行为，实时与管理员进行邮件同步攻击事件。UNIS ACG1000-E-G 还具备自定义攻击规则的功能，从而可以防护网络中特有的复杂的攻击，全方位的立体保护用户的关键数据，避免机密文件泄露和经济损失。

翻墙行为防护

UNIS ACG1000-E-G 具备专业的翻墙行为管控能力，针对上网用户实现准入鉴权、权限管理和翻墙管控，构建网络边界安全。ACG1000 内置了 16 种准入鉴别方式、180 种海外应用特征库、5500 海外网站库以及全球 IP 属地控制，配合终端行为管理客户端对用户进程双管齐下，能够对翻墙行为进行快速识别，通过流量回溯定位追踪至实名用户。

AIGC 智能运维

UNIS ACG1000-E-G 融合对话式 AI 技术，将 AI 能力快速落地到应用控制网关，能够提供简单易用的 AI 智能防护和运维能力。ACG1000 系列产品内含大模型通识知识库、网络安全和上网行为管理知识库，融合强大的算力模型，通过启发式交互及下钻式引导，实现策略快速下发、运维保障、场景安全加固、业务敏捷开通等多种智能化运维，让“小白”也能通过对话式，来满足企业的运维合规需求。

行为轨迹分析

通过对用户网络账号、行为动作、上网设备及时间等多维度信息进行关联数据分析，UNIS 上网行为与管理产品真正实现了基于用户的上网行为管理与审计的可视化，将用户的上网行为轨迹清晰直观的加以呈现，有助于网络管理人员制定更有针对性的网络管理策略，保障网络资源的合理有效利用和工作效率提升。

清晰事后审计

UNIS ACG1000-E-G 系列产品支持详细、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。同时，UNIS ACG1000-E-G 产品提供丰富美观的报表，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。

智能行为报表

UNIS ACG1000-E-G 系列产品支持智能的行为管理报表功能，对用户网络行为进行记录与分析。支持小时/天/周为单位的用户流量、应用流量、设备流量趋势图、列表 TOP 统计展示。对于用户的行为的数据留存与分析，即是对国家法律法规的遵从，也是真正管理好企业员工上网，有效利用网络资源的需要。正对用户上网行为以及相关内容查询统计，能够对用户的网络活动进行较长时间的回溯与反查，帮助管理员全面了解网络的使用情况，为改进网络管理提供详实准确的依据。同时 UNIS ACG1000-E-G 产品提供多套内置报表模板，当然也支持管理员自定义报表内容，最大限度的满足各行各业的报表需求。

管理简易安全

UNIS ACG1000-E-G 系列产品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 UNIS ACG1000-E-G 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。UNIS ACG1000-E-G 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。

产品规格

硬件规格

产品型号	ACG1000-E-G
固定业务接口	6 千兆电+ 4 千兆光
扩展卡槽	2
扩展卡	8 电、4 万兆、4 光 4 电（bypass）
Console 口	1
内存	32G
存储	4T
平均无故障时间(MTBF)	≥68869 小时
缺省配置重量	16.1kg
外形尺寸（长×高×深/mm）	435*88*500mm
温度	工作温度 0℃~40℃， 非工作温度-20℃~70℃
湿度	工作 10%-90%非凝露
电源	可选配双电源

最大输入电流	5A
最大功率供给(W)	350W
硬件 bypass	支持 2 对 GE 口（GE2-GE5）

软件规格

一级 SPEC	二级 SPEC	三级 SPEC	四级 SPEC
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
	端口镜像	镜像接口	物理接口支持作为镜像接口和被镜像接口
		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
	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	支持基于路由权重的多链路负载均衡
		策略路由	5元组策略路由+应用+时间
		ISP路由	内置电信、联通、移动、教育网ISP信息，可自定义ISP信息
		RIP	支持v1、v2
		OSPF	支持缺省路由发布、路由重发布
	NAT	通用功能	支持源NAT、目的NAT、静态NAT
			支持一键NAT回流（双向nat）
		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	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）
	地址探测	接口探测	支持PING、TCP、DNS地址监控条目
		地址探测组	支持多个地址探测从属组关系
		路由探测	支持探测路由以确保路由有效性

一级 SPEC	二级 SPEC	三级 SPEC	四级 SPEC
	链路负载均衡	链路负载均衡	支持基于权重、优先级的七元组链路负载均衡
			负载均衡接口支持健康探测
	服务器负载均衡	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
	DDNS	DDNS	支持花生壳ddns客户端以及域名IP绑定
网络优化	APP动态缓存	APP动态缓存	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
	应用缓存	应用缓存	支持文件的应用缓存，支持文件名模糊匹配的文件缓存
	服务质量管理	服务质量管理	支持PING、TCP、DNS探测
			支持自定义间隔时间探测
虚拟路由器	VRF	接口虚拟化	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；
		IP地址重叠	不同vrf下的接口可以配置相同的ip地址
		静态路由	支持静态路由
安全防护	通用功能	黑名单	支持手动配置
			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
	扫描防护	通用	基于接口的配置，支持自动加入黑名单
		扫描方式	端口扫描、IP地址扫描
	异常包防护	异常包类型	Ping of Death；Land-Base；Tear Drop；TCP flag；Winnuke；Smurf；IP选项；IP Spoof；Jolt2
	ARP防护	防ARP攻击	支持ARP学习与主动保护，防ARP Flood攻击
		ARP学习控制	基于接口的ARP学习控制
	Flood防护	支持类型	SYNFlood、UDPFlood、ICMPFlood、DNSFlood
	行为模型	DNS隧道检测	支持DNS隧道检测，检测通用隧道中的恶意流量
	防暴力破解	防暴力破解	支持HTTP、FTP、Telnet、IMAP、SMTP、POP3等等明文协议防暴力破解
	弱密码防护	弱密码防护	支持Telnet、FTP、imap、pop3、smtp等协议弱密码保护
	非法外联防护	非法外联防护	支持配置重要服务器允许外联的设备或终端
		非法外联学习	支持服务器外联自学习
	WEB防护	防护策略	支持规则防护；精确访问控制；防盗链；CSRF攻击防护；CC攻击防护；应用隐藏；网页防篡改。
		规则库	支持：http协议检、通用攻击、SQL注入攻击、XSS攻击、目录遍历、恶意扫描与爬虫、木马攻击、会话劫持、敏感信息泄露、服务器防护、CMS漏洞防护等11中类型
		防篡改网页缓存	支持缓存和清理
	风险扫描	端口扫描	端口扫描仅支持TCP

一级 SPEC	二级 SPEC	三级 SPEC	四级 SPEC
		弱密码扫描	支持显示扫描结果，支持密码字典导入
流量管理	通用功能	配置管理	增删改
	流量控制	线路管理	绑定接口
			支持基于接口的上下行带宽管理
		通道管理	支持高、中、低优先级通道设置
			支持应用、用户、源地址、服务、时间的通道匹配
	排除策略	排除策略	支持用户、地址排除
	限额策略	限额策略	支持基于时长、流量的限额策略
			支持超出限额阈值时进行阻断，流控
解密策略	https网站解密	https网站解密	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
	ssl邮箱解密	ssl邮箱解密	支持ssl加密网页版邮箱的解密
			支持ssl加密客户端版邮箱的解密
防共享上网	防共享上网	防共享上网	支持用户共享网络监测
			支持阻断和限速两种惩罚方式
			支持共享网络用户终端数阀值配置，支持不同终端单独配置
访问控制	IPv4策略	策略	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、服务以及时间和终端类型
			支持应用控制，URL过滤、终端公告推送的策略动作
			基于策略的长连接（老化时间）
	IPv6策略	配置管理	支持用户和应用均为任意的7元组策略
上网行为控制与审计	应用控制	应用控制	支持根据应用配置应用控制策略
		邮件控制	支持针对发件人；收件人；标题&内容；邮件大小；附件个数控制
		web关键字控制	支持搜索引擎；http上传；http页面内容的关键字控制
		虚拟账号	支持针对QQ虚拟账号的黑白名单控制
		URL控制	支持预定义和自定义URL分类过滤
		终端公告	支持根据策略的终端公告内容推送
	应用审计	http审计	支持网页访问；网络社区；网页搜索；http外发文件；http文件下载的审计
		邮件审计	支持发邮件；收邮件；web邮件的收发审计
		即时通讯	支持QQ客户端；微信客户端；网页QQ；网页微信；移动飞信等聊天内容审计
		基础协议	支持FTP；TFTP；TELNET基础网络协议账号，命令等内容的审计

一级 SPEC	二级 SPEC	三级 SPEC	四级 SPEC
		娱乐股票	支持股票娱乐账号和评论的审计
		网络应用	支持其他大类网络应用的审计
	策略分析	策略分析	支持分析冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略；支持策略分组，进行区分化管理和运维。
	入侵防御	入侵防御配置	支持预定义的入侵攻击特征类，包含最大事件集、常规事件集、应用事件集、攻击事件集。
		IPS自定义规则	支持协议字段包括：IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等多种协议；支持正则表达式匹配。
	病毒防护	防病毒设定	默认支持20万病毒特征库，高端型号支持拓展至800万特征库；支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀。
		病毒列表	支持展示和搜索病毒特征库
VPN	IPsec VPN	IKE第一阶段协商模式	支持IKEv1
			支持主模式和野蛮模式
		加密/HASH算法	国际标准算法(DES/3DES/AES/MD5/SHA-1)
		IPsec封装	支持ESP和AH封装
		IPsec冷备份	支持IPsec冷备份，主VPN断开，备VPN触发开始建立
	IPsec快速VPN	IPsec快速VPN	支持IPsec快速vpn配置
			支持中心端和客户端方式部署
	SSL VPN	全局配置	支持配置SSL VPN的全局功能
		资源	支持配置SSL VPN发布的网路资源
		用户	支持本地管理SSL VPN的账号，支持对接AD和Radius
		在线用户	支持对SSL VPN用户实时在线监控
		基础防护	支持SSL VPN功能网络的基础防护功能
用户管理	用户同步	snmp同步	支持通过SNMP协议读取网络设备的用户相关信息，将读取的信息录入本地
		AD用户同步	支持通过LDAP协议同步同步读取AD服务器上的用户到本地
			支持单次手动同步和多次自动同步
		ARP扫描	支持通过ARP扫描的方式将扫描到的用户同步到本地
		认证后录入	支持通过各种认证策略之后将已经认证的用户同步录入到本地。作为本地用户供策略调用
	用户结构	用户组织结构	支持标准的树形结构方便管理用管理和调用用户
		临时账号	本地设置的用户账号支持设置用户有效期
	通用功能	伪portal抑制	支持伪portal抑制功能（http-APP）（命令行）
		https弹portal	基于https访问弹出认证portal
	IPv6支持	IPv6用户	用户可绑定IPv6地址
	portal逃生	portal逃生	基于已认证用户逃生

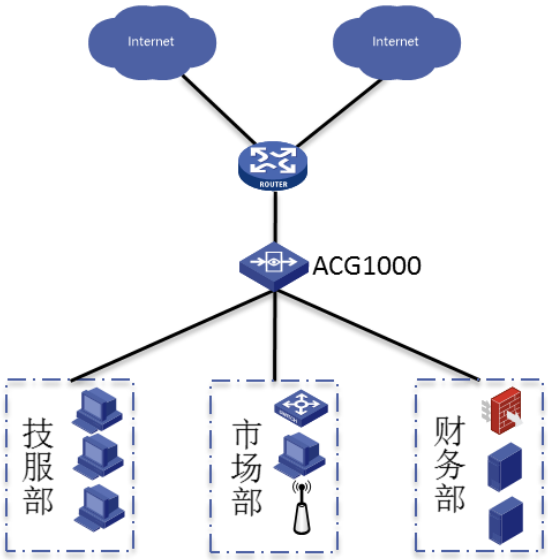
一级 SPEC	二级 SPEC	三级 SPEC	四级 SPEC
			基于全部用户逃生
	IMC联动	与IMC通信	与IMC联动
用户策略	识别相关	识别范围	设置识别的IP地址范围
	重定向	重定向页面	默认重定向页面
	策略	认证策略	匹配项：源接口、源地址、目的接口、目的地址、时间
			支持微信、短信、本地、免认证、portal认证、AD单点登录、二维码认证、混合认证
系统管理	系统管理员	账号管理	登录认证方式支持本地认证、Radius服务器认证、LDAP服务器认证
			支持系统管理员的U-key双因子认证
		管理设定	支持三权分立
			支持账号唯一性检查
	认证服务器	Radius	支持多用户第三方存储远端请求认证
		LDAP	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
		服务器组	Radius/LDAP服务器组，支持主备和集群
		短信认证	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
		AD单点登录	支持AD服务器的单点登录认证方式
		微信认证	支持微信连wifi认证方式
			支持强制关注功能
			支持无感知认证
		混合认证	支持多种认证方式的混合认证
	系统维护设定	诊断工具	Ping、traceroute、TCP SYN探测
		抓包工具	支持按照过滤条件抓取数据报文
			支持将报文下载到本地保存查看
		信息收集	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
	可靠性	硬件bypass	电口断电bypass
			电口启动过程bypass
		软件bypass	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
	双机热备HA	主备、主主模式	支持配置、流、特征库、接口状态、IPsecVPN状态同步
	SNMP	SNMP配置	SNMP代理
			版本：v1、v2、v3

一级 SPEC	二级 SPEC	三级 SPEC	四级 SPEC
		trap	trap版本：v1、v2 Notification、v2Inform
	域名相关	DNSserver	支持4个DNS服务器
		DNS透明代理	支持基于出接口的dns 权重比例、优先级透明代理
	配置管理	配置管理	支持多份配置保存
			支持下次启动配置指定
			支持配置拷入，拷出备份列表
	U盘零配置	U盘零配置	支持U盘版本升级
			支持U盘配置导入
			支持U盘的零配置上线
	中英文版本	中英文版本	支持中英文版本的切换
	管理端口自定义	管理端口自定义	支持管理端口的自定义
	系统告警	系统告警	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
	无线非经	非经SDK	支持非经SDK方式对接无线非经平台；

典型组网

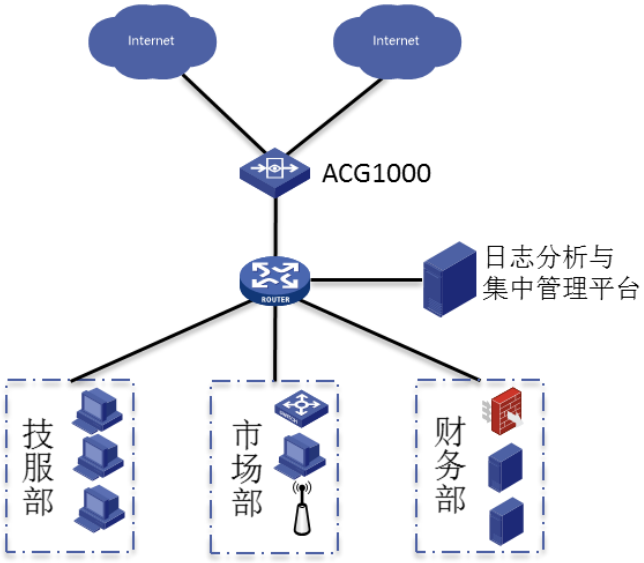
透明部署

- 适用于数据中心机房，可灵活的以串行路由或者透明方式部署于数据中心机房出口，根据实际网络环境署简单；
- 提供身份认证功能，验证上网用户身份合法性；
- 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽；
- 支持设备本地日志记录，日志也可发送到集中管理和数据分析中心处理，并可进行数据分析。



路由部署

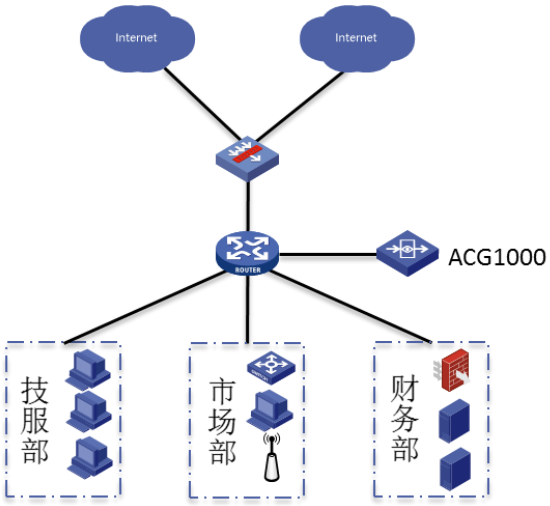
- 适用于大中型企业用户，以网关方式在线部署于网络出口；
- 提供诸如 NAT、负载均衡等出口特性；
- 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽；
- 支持 VPN/MPLS/ VLAN/PPPoE 等复杂网络环境；
- 支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理。



旁挂部署

- 适用于不改变网络拓扑，仅做行为审计的场景，一般部署于核心层；
- 针对用户上网行为进行分析和审计；

- 提供日志记录、日志导出功能。



紫光恒越技术有限公司

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-62166890
传真：010-51652020-116
版本：

www.unisyue.com

客户服务热线
400-910-9998