中数国科 VPN 综合安全网关

产品白皮书

（中数国科集团）

【中数国科】

■ 文档编号	■ 密　级
■ 版本编号	■ 日　期
■ 撰 写 人	■ 批 准 人
■	■ @2025 中数国科

■ 版权声明

目录

一、引言

在当今加速演进的数字化时代，企业的运营边界早已突破物理办公场所的限制。远程办公、全球分布式团队、分支互联、混合云及多云架构已成为业务常态。这种无处不在的连接需求在带来灵活性与效率提升的同时，也前所未有地放大了企业网络所面临的安全风险与管理复杂性。

企业网络管理者正深陷多重困境：一方面，必须为分散各地的员工、分支机构和云端应用提供安全、稳定、高性能的网络接入，保障业务连续性；另一方面，却不得不应对日益严峻的网络攻击威胁（如数据泄露、勒索软件、APT 攻击）以及日趋严格的数据安全与合规要求。同时，传统的网络连接与安全解决方案往往呈现“烟囱式”部署——远程访问 VPN、站点间 VPN、防火墙、入侵防御等系统各自为政。这不仅导致管理界面碎片化、策略配置复杂冗长，大幅增加运维负担和出错概率，也常常因性能瓶颈和扩展性不足而难以适应业务快速发展的需求，造成总体拥有成本居高不下。

传统的单一功能 VPN 设备或叠加式安全方案，在应对现代企业复杂、动态且高度互联的环境时，愈发显得力不从心。它们在统一管控、深度安全融合、弹性扩展以及简化用户

体验方面存在显著短板。企业迫切需要一种能够打破孤岛、整合能力、化繁为简的新型基础设施。

正是在这样的背景下，中数国科集团推出了新一代中数国科 VPN 综合安全网关。它并非简单的功能堆砌，而是基于对现代企业网络与安全痛点的深刻洞察，旨在提供一个一体化、智能化、安全融合的连接中枢。中数国科 VPN 综合安全网关集高性能多协议 VPN 连接、深度集成的下一代安全防护能力、统一策略管理于一身，致力于从根本上解决企业在安全互联、简化运维、保障性能和满足合规等方面的核心挑战，为企业构建面向未来的安全网络连接基石。

二、产品概述

2.1.产品简介

中数国科 VPN 综合安全网关（以下简称“综合网关”）是中数国科集团严格按照国家技术规范，利用安全隧道技术，在 IP 层实现互联网网络信息防护的安全设备。产品利用 Internet 或其它公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。

产品遵循国家密码管理局颁发的《GM/T 0022 IPSec VPN 技术规范》、《GM/T 0023 IPSec VPN 产品规范》、《GM/T 0024 SSL VPN 技术规范》和《GM/T 0025 SSL VPN 产品规范》，支持 SM2、SM3、SM4 国密算法；利用基于 SM2 算法的数字证书技术实现数据的传输加密和身份认证。

综合网关支持国密标准的 IPSec 与 SSL 安全传输协议，为用户提供以下核心功能：

(1) 全栈可信接入服务：

综合网关支持国密标准的 SSL 协议，全面支持国密标准规定的数字证书+口令的“双因

子”认证机制。网关深度融合安全隧道技术、TCP 端口代理技术和 HTTP 代理技术，在网络层、传输层以及应用层构建全方位防护体系，能够为 IP 层以上的所有网络服务提供安全、高效的加密接入通道，满足固定办公终端、移动用户及智能终端等不同场景、多平台的可信接入需求。产品采用创新的网络架构设计，支持大并发用户接入与高吞吐量数据传输，保障业务访问体验。

(2) 安全高效组网服务：

中数国科 VPN 安全网关产品采用标准的 IPSec 安全协议，利用安全隧道技术，在 IP 层实现互联网网络信息防护，产品利用 Internet 或其它公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。能兼容绝大多数第三方 IPSec VPN 产品，与其互联互通，实现交叉组网；在工作模式上，除标准模式外，还提供匿名模式，支持任意的 IPSec VPN 以多对一的方式接入，高效解决复杂组网需求。

2.2.产品外观

综合网关为 2U 标准机架式设备，其产品整机及前后面板视图如下所示：

图 2.1 ARM 系列 综合网关整机图

图 2.2 X86 系列 综合网关整机图

2.3.标准规程

- GM/T 0024 SSL VPN 技术规范
- GM/T 0025 SSL VPN 网关产品规范
- GM/T 0022 IPSec VPN 技术规范
- GM/T 0023 IPSec VPN 网关产品规范
- GM/T 0002 SM4 分组密码算法
- GM/T 0003 SM2 椭圆曲线公钥密码算法
- GM/T 0004 SM3 密码杂凑算法
- GM/T 0005 随机性检测规范
- GM/T 0006 密码应用标识规范
- GM/T 0009 SM2 密码算法使用规范
- GM/T 0010 SM2 密码算法加密签名消息语法规范
- GM/T 0015 基于 SM2 密码算法的数字证书格式
- GBT 15843.3 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制

三、应用场景

综合网关基于高性能基础软硬件平台，全面支持标准的 IPSec 与 SSL 安全协议，并广泛兼容主流第三方 IPSec/SSL VPN 产品，实现便捷的互联互通与交叉组网，有效保护企业网络边界安全。IPSec 功能除标准模式外，创新提供独特的匿名工作模式，显著提升对复杂网络环境的适应性与部署响应速度，充分满足重要行业和领域在异地局域网安全互联、移动办公可信接入、关键平台精细化访问控制等方面的核心需求，为用户提供可信身份认证、端到端数据加密传输等全方位安全保障。

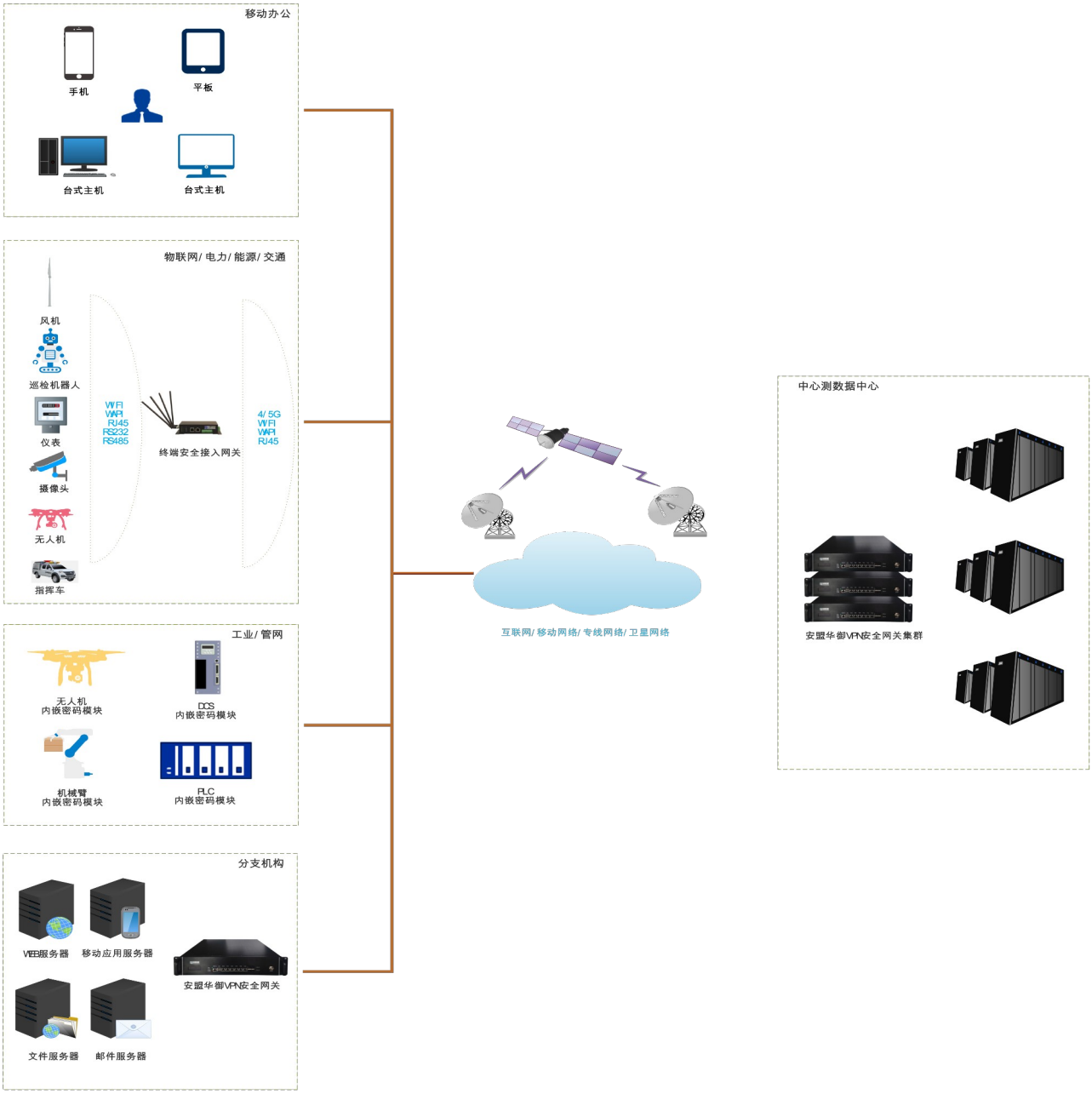

图 3.1 综合网关应用场景

3.1.远程移动安全接入

场景痛点：移动办公、居家办公常态化，员工需随时随地安全访问内网资源（OA、邮件、文件服务器、业务系统），但公网环境风险高，需严防数据泄露和未授权访问。

解决方案：网关提供国密 SSL VPN 接入，支持口令或证书或双因子认证（数字证书+口令）的多种登录认证方式和终端安全检查，为员工建立客户端到网关的加密隧道。支持

隧道模式和代理模式，无缝访问各类应用。高并发设计保障海量员工同时流畅办公。

3.2.异地机构远程互联

场景痛点：分支机构（门店、工厂、办事处）需与总部实时交换业务数据（ERP、CRM、财务），传统专线成本高昂、部署慢；普通互联网连接不安全、质量差。

解决方案：利用国密 IPSec VPN 构建 “网关-网关”加密隧道，通过公共互联网实现安全、稳定、低成本的互联。SM3 加密保障数据完整性，SM4 加密保障数据机密性。高兼容性确保与现有设备互通，匿名模式简化多分支接入总部。

3.3.物联设备安全接入

场景痛点：大量分布式的物联网设备（如监控、传感器、工控设备）需安全接入中心平台进行管理和数据回传，设备资源有限，需轻量级安全协议。

解决方案：网关可作为 IoT 安全接入中心。结合中数国科自研的 4/5G 终端安全接入网关，为 IoT 设备提供身份认证（如证书/预共享密钥）和数据传输加密。在网关处实施访问控制与威胁检测，防止恶意设备入侵或数据窃取。可广泛应用于电力、能源、油田、管网、光伏、水利、交通、环保、广播站台、无人机等领域。

3.4.大型网络专网搭建

场景痛点：专网非绝对安全，大型行业专网（如政务、金融、能源、医疗专网）虽然相对公网安全，但内部仍存在未授权访问、窃听、内部人员泄露或高级威胁渗透的风险；另外，专网内运行着不同部门和级别的应用系统，其中核心业务数据（如财政支付、社保信息、金融交易、工控指令、敏感病历）安全等级要求极高，有数据分级保护需求。

解决方案：通过 IPSec 隧道在大专网中划分小专网，实现核心系统与专网其他部分的逻辑隔离，严格限制访问权限，仅允许授权端点通过加密隧道访问敏感数据，落实“最小权限”原则。网关还可提供集中策略管理、安全审计日志，满足等保和行业对高等级数据传输的合规审计要求。

3.5.行业专网延伸建设

场景痛点：大型企业多级架构下，省市级专线网络覆盖成熟，但县级/乡级分支面临严峻挑战：一方面，偏远地区专线资源稀缺或部署周期长达数月，无法满足基层业务快速接入需求；另一方面，专线月费高昂且需固定带宽支出，数千个末端节点叠加成本指数级增长。传统方案迫使企业牺牲网络覆盖率，导致末端业务数据脱节、管理盲区扩大，严重制约数字化下沉进程。

解决方案：综合网关以敏捷架构破局：通过加密隧道将公共互联网转化为虚拟专网，解决物理专线覆盖盲区。使企业以轻量化投入构建全层级互联的“超级大网”，实现业务系统向神经末梢的高效延伸。

3.6.数据中心备份容灾

场景痛点：主备数据中心间需实时/定时同步大量业务数据，对传输安全、带宽和稳定性要求极高；需避免专线单点故障。

解决方案：利用高性能国密 IPSec VPN 建立高带宽、低延迟的加密隧道进行数据同步。支持多链路负载均衡与故障切换，保障传输可靠性。大吞吐设计满足海量数据迁移需求。

四、主要功能

分类	功能	具体描述
数据安全	数据机密性保护	利用加密算法加密用户数据，即使非授权的用户得到数据也无法获悉真实内容。
	数据完整性保护	保护数据在传输过程中的完整性，有效防止数据被非法用户修改。
	数据的备份和恢复	在系统正常工作时，可以备份设备的配置和管理信息。在系统故障后或用户有需求的情况下，可将配置和管理信息恢复。此功能可减少用户的管理开销。
网络连接	网口自定义	网络接口支持四种模式设置：外网口，内网口，管理口，心跳口。
	网络接入方式	支持静态 IP、动态 IP 以及 PPPoE 等多种网络接入方式。
	VLAN 支持	支持 VLAN 网络，通过自定义 VLAN ID 适应 VLAN 网络环境。
管理安全	三权分立	由系统管理员、安全管理员、安全审计员三员协同管理 VPN 安全网关。
	双因子身份鉴别	管理员采用具有安全功能的智能密码钥匙作为身份认证介质以及用户名口令相结合双因子因素作为管理员用户身份鉴别的方式，增加了安全性。
	IP/MAC 绑定	支持访问限制功能，可基于 IP、MAC 地址限制客户端访问设备管理界面，防止未经允许的管理终端访问设备。
	账号锁定	支持防暴力破解功能，多次登录失败账号进行锁定。
	账号安全	支持账号安全设置，可设置尝试次数、锁定时长及超时退出。
身份认证	证书格式	支持基于 SM2 密码算法的标准 x509 v3 数字证书格式。

	国密支持	支持 SM2、SM3、SM4 国密算法和 RSA、AES、SHA 等主流国际算法。
	双证书支持	支持签名证书和加密证书的双证书认证体系。
	第三方 CA 支持	支持 P10 格式导出证书请求，支持导入第三方 CA 的签发的证书和数字信封。（山西 CA、四川 CA、沃通 CA 等）
	完整模式支持	支持标准的通过双向协商认证建立 IPSec 协议的 VPN 隧道。
	匿名模式支持	可以不提供对端设备网络信息及公钥证书的情况下，提供任意的 IPSec VPN 连接，以多对一方式接入。
	安全用户口令认证	采用基于用户名口令融合密码算法的挑战应答机制的强身份认证方式，解决了用户名口令易枚举爆破的问题。
IPSec VPN 功能	部署方式	支持网关模式和透明模式（网桥）部署，其中透明模式不改变原有的网络拓扑。
	安全报文封装	支持 AH 嵌套 ESP 协议和 ESP 协议。
	工作模式	支持隧道模式和传输模式。
	NAT 穿透	支持单 NAT 和对等双 NAT 网络以适应复杂网络的环境。
隧道管理	隧道流量控制	避免某些接入用户滥用 VPN 带宽，确保各分支能顺畅访问总部，确保访问内网数据的质量。
	隧道状态监控	实时查看隧道各阶段的建立情况以及隧道密通流量使用情况。
	DPD 探测	基于 DPD 机制，可侦测对端 VPN 网关是否正常运行。若 VPN 网关发生掉线，能重建隧道以保证网络畅通。
SS	部署模	VPN 安全网关部署模式支持远程客户端-网关模式和网关-网关模式两

L VPN 功能	式	种。远程客户端-网关模式时客户端产品兼容 Windows 平台、Linux 平台以及 Android 平台，同时支持信创国产 Linux 平台。
	工作模式	支持隧道模式和代理模式，其中使用隧道模式是用来支持基于 IP 的所有应用，使用代理模式的方式用来支持 HTTP 和 TCP 应用。
	卸载功能	支持 SSL 中止、SSL 卸载、SSL 桥接以及站点证书卸载功能。
	访问控制	支持细粒度的访问控制功能，基于用户和角色对资源进行有效控制。其中对网络访问可控制到 IP 地址、端口和协议，对 Web 资源的访问可控制到 URL 或端口，并能根据访问时间进行控制。
	公告管理	支持管理员可定制公告信息并推送给 SSL 客户端。
	SSL 协议	支持 RSA/SM2 证书自适应。根据客户端的算法能力进行自动适应，支持 TLS1.0、TLS1.1、TLS1.2、TLS1.3 和 GMSSL 协议。
	密码算法	支持国际算法（RSA）及国密算法（SM2）。
	密码套件	支持 ECC-SM4-SM3 密码套件和国际主流安全密码套件。
	在线用户	支持实时查看在线用户，审计用户接入行为。
	统一门户	客户端提供统一登录认证和统一门户，使用户访问业务系统更便捷、更安全。
	国密浏览器	兼容 360 国密浏览器、奇安信可信浏览器、赢达信国密浏览器以及密信等主流国内安全浏览器。
	日志审计	隧道模式支持基于五元组级细粒度的日志记录；代理模式支持到 URL 级细粒度的日志记录。
	节点资源池	支持节点资源池功能，可作为业务系统集群的前置负载均衡器。

	信息传递	支持信息传递功能，用户访问 HTTP 应用时，系统在完成相应的身份监别后，把验证结果、用户的基本信息插入到 HTTP 请求中传送给后台的应用系统，应用系统通过标准的 HTTP 操作即可获取信息，并基于该信息作相应的访问控制以及进行相应的业务审计。获取的信息包括：用户 IP 地址，用户证书的关键信息。
终端安全	**终端绑定**	支持客户端终端绑定功能。即只允许特定用户仅在指定终端设备使用。
	客户端安全	支持完整性的自校验功能，通过对客户端软件的进行签名，以保护客户端软件的完整性。
	客户端主机安全检查	支持客户端主机安全检查功能。客户端在连接网关时，根据网关下发的客户端安全策略检查用户操作系统环境的安全性，不符合安全策略的用户将无法使用 VPN 接入内网。
密钥安全	**自动密钥协商**	在系统启动或者在用户指定的特定条件下，通信的双方自动完成密钥协商，网络通信的安全用新协商密钥保护；用户可自定义设置工作密钥和会话密钥更换周期。
	密钥更新	安全管理员可自定义设置设备密钥的密钥更换周期。
	密钥销毁	支持在紧急情况下远程通过软件的方式进行密码资源销毁，支持在紧急情况下通过异形钥匙硬件手动密码资源销毁，支持在未授权情况下非法窥探密码设备内部，非法开盖后密码资源随即销毁，全面保障密钥安全，密码资源销毁时提供多种人机交互方式：蜂鸣器、告警灯以及液晶显示屏方式告警。
	密钥备份和恢复	在系统正常工作时，可以备份设备中的密钥和证书；当密钥丢失或损坏时可以快速恢复。
网络防护	**集成防火墙**	基于包过滤的防火墙功能，支持网络访问控制，防止外部网络用户对 VPN 的攻击。
	防重放	避免因中间人攻击，网络传输的数据包被非法用户修改后重放，接收

	攻击	方能识别并丢弃被非法篡改的数据包。
	攻击防御	实时防御 Synflood、Icmpflood、Udp Flood、Ping of death、Icmp-Smurf、Tcp-Land、Icmp-Unreachable、ARP Flood、Udp-Teardrop 等多种攻击。
高可用	双机热备	支持双机热备，同时提供自动回切、策略同步等功能。
	硬件 Bypass	支持硬件 Bypass 功能，在网关出现故障或异常时，可以迅速响应，避免用户网络中断。
	定制系统	自研嵌入式密码安全操作系统，通过对安全操作系统进行裁剪、加固和制作内存文件系统，并从设备启动、设备运行、设备通信、设备资源存储、设备升级、设备日志审计等环节均采用密码技术进行安全防护的嵌入式密码安全操作系统，除操作系统基于密码技术的内生安全外，其制作的内存文件系统相对于磁盘文件系统，更大程度上保障了断电等异常情况下操作系统的高可靠性。
	系统冗余	冗余系统支持，冗余系统可用于紧急情况下的系统修复，提高系统的高可用性。
系统监控	实时监控	支持设备资源监控，可实时查看 CPU、内存以及磁盘使用状态。
	SNMP 远程监控	支持 SNMP 远程监控，支持 V1/V2c/V3 版本，可设置共同体并可限制访问源。
系统管理	日志外发	支持 SYSLOG 功能，可将日志发送至第三方日志服务器。
	SSH 安全管理	支持 SSH 安全管理。
	日志管理	支持安全日志查看、导出、审计以及日志防篡改功能。
	告警管	支持邮件、短信、SNMP TRAP 以及 SYSLOG 告警，管理员可通过告

	理	警类型（系统日志、管理日志、安全防护、安全接入）、自定义告警级别、自定义告警间隔的方式进行告警。
	自动校时	支持自动校时功能，可从时间服务器自动同步设备时间，支持设置校时间隔时长。
	诊断工具	支持 ping、traceroute、抓包分析等功能，方便管理员运维诊断使用。
	恢复出厂设置	系统具有恢复默认设置功能，方便使用。
	软件修复	通过本地升级来修复软件。
	集中管控	支持统一接入自研密码设备管理平台和密码应用监测平台。

五、产品规格

产品型号		VPN3000		
整体说明		ARM 系列	X86 系列	信创系列
性能参数		中低端	中高端	中高端
IPSec VPN	加解密吞吐率	460Mbps	-	-
	加解密时延	0.157ms	-	-
	每秒新建隧道数	40 个	-	-
	最大并发隧道数	4000 个	-	-
SSL	加解密吞	282Mbps	-	-

VPN	吐率			
	每秒新建连接数	170	-	-
	最大并发用户数	2000	-	-
	最大并发连接数	2000	-	-
SSL 卸载	加解密吞吐率	350Mbps	-	-
	每秒新建连接数	260	-	-
	最大并发用户数	6000	-	-
	最大并发连接数	6000	-	-
硬件配置	CPU（颗*核*线程）	瑞芯微 ARM64，1*4*1	Intel i7-6700，1*4*2	飞腾 D2000,1*8*1
	CPU 主频	2.0GHz	3.4GHz	2.3GHz
	内存	8G DDR4	16G DDR4	16G DDR4
	硬盘	32GB eMMC	64G SSD	64G SSD
接口配置	管理网口	1GE	1GE	1GE
	业务网口	5GE，2SFP	4GE，4SFP	4GE，4SFP
	心跳网口	1GE	1GE	1GE
	USB 接口	3 个 USB2.0	2 个 USB2.0	2 个 USB2.0
	console 串口	1 个 RJ45 串口	1 个 RJ45 串口	1 个 RJ45 串口
	网口扩展槽	不支持	2 个 PCIE 网口扩展槽	不支持

安全配置	机箱锁	支持	支持	支持
	开盖销毁	支持	支持	支持
	手动销毁	支持	支持	支持
显示配置	指示灯	1 个电源灯，3 个工作状态灯，1 个报警灯	1 个电源灯，2 个工作状态灯，1 个报警灯	1 个电源灯，2 个工作状态灯，1 个报警灯
	蜂鸣器	支持	支持	支持
	液晶屏显	支持	支持	支持
电源	插电自启	支持	支持	支持
	是否冗余	支持	支持	支持
	整机功耗	<200W	350W	<200W
	额定工作电压	220V	100~240V 47~63	220V±10% 50Hz±2%
机箱	尺寸(长 x 宽 x 高(mm))	440 x 560 x 89（不含把手及电源）	440 x 560 x 89（不含把手及电源）	440 x 560 x 89（不含把手及电源）
	规格	2U	2U	2U
	净重	12Kg	12Kg	12Kg
工作环境	工作温度	0~40℃	0~40℃	0~50℃
	工作相对湿度	5%～95%RH	10%～90%RH	20%～90%RH
	大气压力	86～106KPa	86～106KPa	86～106KPa

六、特点优势

6.1.安全合规

6.1.1.标准规范

综合网关符合《GM/T 0024 SSL VPN 技术规范》、《GM/T 0025 SSL VPN 网关产品规范》、《GM/T 0022 IPSec VPN 技术规范》、《GM/T 0023 IPSec VPN 网关产品规范》《GM/T 0028 密码模块安全技术要求安全二级》，全面符合国家密码管理法规，确保产品的安全性与合规性，满足政府、金融、能源等关键行业需求。

6.1.2.物理防护

综合网关配置三重物理防护体系，保障密码设备硬件与数据安全：配备带钥匙的旋钮式机箱物理锁，有效抵御非法物理接触。内置持续开盖监测开关，实时侦测非法开盖行为，并自动触发敏感数据紧急擦除机制。紧急情况下支持手动立即销毁密钥等密码资源。物理散热通道覆盖高密度防窥视防尘网，严防针对设备硬件的物理窥探与破坏。

6.1.3.身份认证

通过硬件级加密通道构建零信任运维体系：采用基于智能密码钥匙的硬件数字证书实现双向强身份鉴别，确保远程运维场景中管理员身份真实性及管理指令传输安全，有效防御中间人攻击与数据窃取，满足等保 2.0 三级远程管控要求。

采用基于密码算法融合用户名口令的挑战-应答机制强身份认证方式，从根本上解决弱口令爆破风险，提升认证强度。

6.1.4.密钥安全

构建多层级密钥防护体系：支持用户自主定义设备业务工作密钥及会话密钥的更换周期，确保密钥全生命周期的动态安全。支持密钥备份恢复，保障密钥全生命周期安全。

6.1.5.网络防护

综合网关集成防火墙功能，实时阻断 Synflood、Icmpflood、Udp Flood、Ping of death、Icmp-Smurf、Tcp-Land、Icmp-Unreachable、ARP Flood、Udp-Teardrop 等多种攻击，保障业务连续性。

6.1.6.日志安全

采用国密 SM2 算法对管理员操作日志实施数字签名，确保日志完整性、操作不可抵赖性及司法取证有效性，符合《网络安全法》审计留存要求。

6.2.智能融合

6.2.1.三位一体

综合网关将 IPSecVPN、SSLVPN、SSL 卸载三大核心功能深度融合，打造一体化平台，实现统一管理，灵活适配多种应用场景。

6.2.2.动态可视

综合网关提供全方位可视化管理能力，实现网络状态透明可览、用户行为可追溯、安全事件可预警。支持实时监控隧道建立的状态、流量实时统计展示；支持实时查看在线用户，审计用户接入行为；能够定制公告信息并推送给 SSL 客户端。

6.2.3.精细控制

提供用户/角色双维度资源控制体系：网络层可精准管控 IP、端口及协议，Web 层可细化至 URL 级访问权限，并支持时间策略动态约束。

通过主机安全检查引擎动态验证操作系统环境合规性，阻断非安全终端接入，并结合

客户端-设备唯一绑定机制，确保用户仅限授权终端访问，完美适配企业异构终端生态。

6.2.4.全密防护

综合网关从设备启动、设备运行、设备通信、设备资源存储、设备升级、设备日志审计等环节均采用密码技术进行安全防护，保证设备整体的安全。

6.3.便捷高效

6.3.1.泛适组网

实时可视化监测隧道建立全阶段状态及流量分布，支持基于 IP 粒度的隧道流量管控。全面兼容 ESP 协议及国密标准的 AH 嵌套 ESP 报文封装协议，满足多样化安全传输需求。

综合网关创新性采用净载荷封装技术，实现网络链路端到端透明加解密，业务系统零改造接入，彻底突破传统 VPN 要求保护子网必须异构的组网限制，同时安全策略支持全网加密、定向加密以及定向透传策略组合的方式，使得部署安装灵活便捷。

综合网关提供匿名工作模式，显著提升对复杂网络环境的适应性与部署响应速度。

6.3.2.终端兼容

通过主机安全检查引擎动态验证操作系统环境合规性，阻断非安全终端接入；结合客户端-设备唯一绑定机制，确保用户仅限授权终端访问，完美适配企业异构终端生态。产品兼容 Windows 平台、Linux 平台以及 Android 平台，同时支持信创国产 Linux 平台，充分支持 PC、移动终端、物联网设备的接入。

6.3.3.即时响应

提供多维度可定义告警策略：支持按系统日志、管理日志、安全防护、安全接入四类事件类型触发告警，允许管理员自定义告警级别与告警周期，通过邮件、SYSLOG、短信、SNMPTRAP 等方式推送通知，实时触达管理员终端。通过精准的阈值-响应联动机制，确保关键安全事件实时触达，实现安全问题早发现、早处理，降低安全风险与业务影响。

6.3.4.统一端口

产品客户端基于 HTTP 代理实现 SSL 远程访问，对浏览器和操作系统无特殊要求；综合网关代理转发时服务端支持单端口代理配置，单端口代理配置避免传统多端口代理的 SSL VPN 部署于防火墙后侧时正/反向代理策略调整时必须动态调整防火墙策略的劣势。

6.3.5.传输高效

综合网关网络报文转发时相对于传统的 IP OVER SSL 技术，我们采用多网络报文包组装后统一加密封装后传输，大大提高了设备整体加解密吞吐量。

采用创新的 IPSec 专用链式运算技术，使得同一份数据报文数据完整性和机密性同时运算，使得隧道加解密吞吐率大幅提升。

6.4.稳定可靠

6.4.1.系统加固与裁剪

基于操作系统进行裁剪加固并制作内存文件系统，相对于磁盘文件系统，移除了冗余组件，降低了系统复杂性与攻击面，更大程度上保障了断电等异常情况下操作系统的高可靠性。优化系统资源占用，确保高负载下稳定运行。

6.4.2.冗余系统与电源

在默认系统外提供非业务冗余系统，可用于紧急情况下的系统修复，提高系统的高可用性。

采用双模块冗余电源供电，保证电源的稳定可靠。当一个模块出现故障时，能自动切换到另一个模块供电，不会影响系统正常工作。电源支持热拔插，可以在线更换故障电源，不必断电，有效地提高了综合网关的可用性，保证系统的连续运行。

6.4.3.业务连续与高可用

支持多机相互热备技术，综合网关出现故障时，主、备机实现无缝切换，提供策略同步功能，确保用户业务不间断运行，增强用户网络健壮性。

提供灾备恢复机制，确保极端情况下的业务可用性。

业务网口支持硬件 Bypass 功能，在网关出现故障或异常时，可以迅速响应，避免用户网络中断或性能下降。

七、产品部署

7.1 远程客户端-网关（网关式）

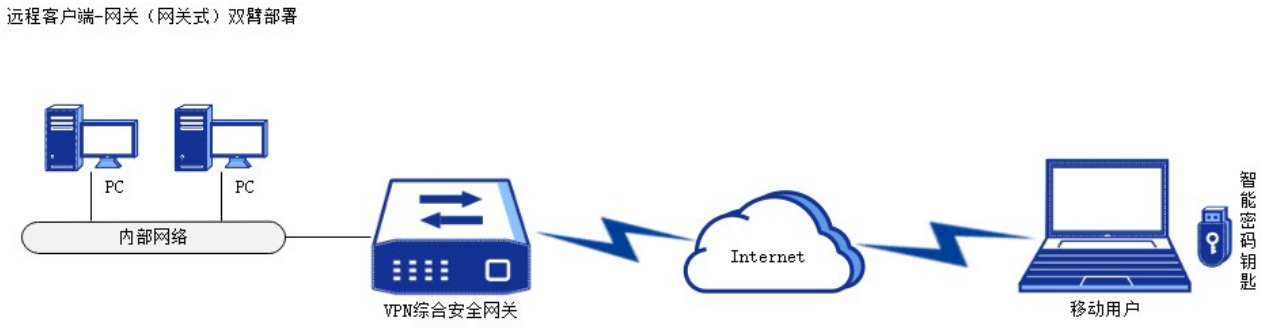

图 7.1 远程客户端-网关（网关式）双臂部署图

7.2 远程客户端-网关（旁路式）

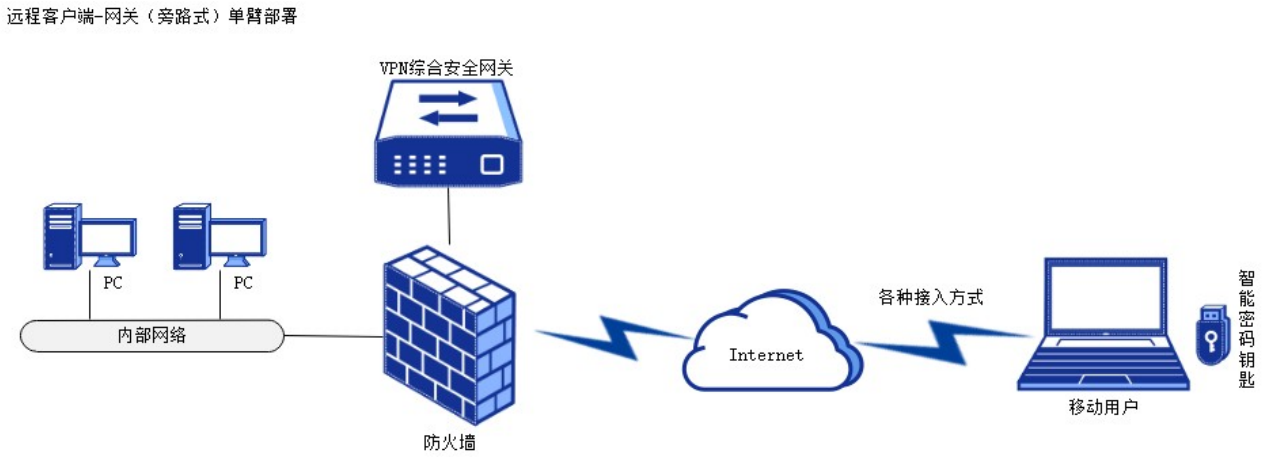

图 7.2 远程客户端-网关（旁路式）单臂部署图

7.3 网关-网关

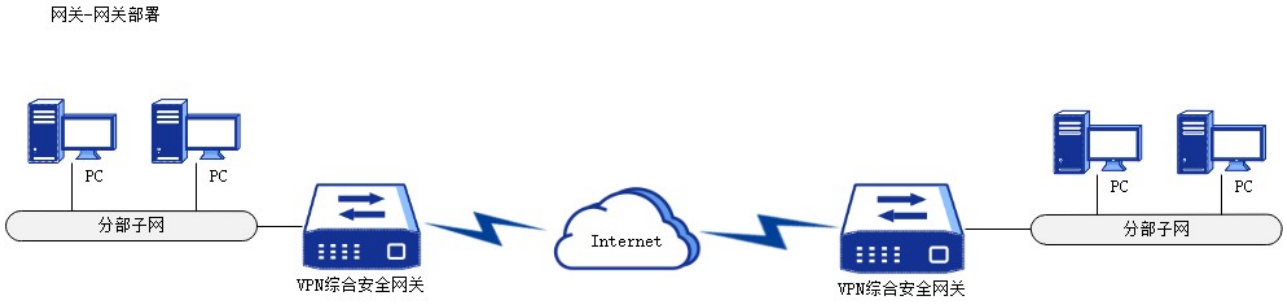

图 7.3 网关-网关部署图