

# 网神 VPN 安全网关系统 产品彩页

地址：北京市西城区西直门外南路26号院1号

邮编：100044

# 1 产品介绍

网神 VPN 安全网关系统是集 VPN 组网，路由转发，硬件加解密以及安全防护功能于一体的安全网关系统。部署在企业网络的边界，在企业的分支机构和总部之间或是各个分支之间建立安全隧道，对通信数据包进行加解密，进而保证数据通信的安全性。相比传统的 VPN 网关，网神 VPN 安全网关系统支持全面的 IPv6 能力及 IPv4/IPv6 过渡技术，同时提供网络和安全策略一体化配置的管理手段。不仅支持国际算法 3DES/AES，同时支持国密算法 SM1/2/3/4。网神 VPN 安全网关系统可以基于应用的流量感知和流量调度，支持可视化的应用分析和展示，实现基于应用及业务视角的数据安全加密、防护。

# 2 产品功能列表

基础组网	部署模式	产品支持路由、透明、交换以及混合模式接入，复杂应用环境的接入需求。
	网络协议	产品支持 4G 接入，并可实现 4G 连接与有线链路之间的互为备份。
		产品支持通过 802.3ad 协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余
	路由协议	产品支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持 RIP v1/v2/ng，OSPFv2/v3，BGP4/4+ 协议；
		支持静态和动态多播路由，支持 IPV4 和 IPV6 协议
		产品支持基于策略的路由负载，支持根据应用和服务进行智能选路
		支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测
		产品支持 ISP 路由负载均衡，支持自定义负载权重，支持基于优先级的 ISP 路由链路备份
	地址转换	产品支持全面的 NAT 转换配置，包括包括一对一，一对多，多对一的源、目的地址转换。
		产品支持在会话的源、目的地址同为 IPv4 地址时，可将目的地址转换至指定服务器地址，同时可探测服务器是否存活

	DNS代理	支持 DDNS 功能。
	IPv6	支持 IPv6 手动及自动的 IP/MAC 探测及绑定；
		产品支持 IPv6 下静态路由及策略路由、动态路由，动态路由应包括 RIPng、OSPFv3、BGP4+。
		产品支持 NAT64、DNS64
		产品支持配置基于 IPv6 地址的安全策略；
		产品支持 IPv6 管理地址
	加密隧道	提供 SM1、SM2、SM3、SM4 国密算法加密隧道
访问控制	访问控制	产品支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。
	应用识别与控制	产品支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 3000 种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类。
	用户识别与认证	产品支持基于用户的访问控制，可与 LDAP/Radius/证书/Active Directory/TACACS+/POP3 等用户认证系统联动。提供自动跳转功能，用户登录后自动弹出默认的应用界面。提供不少于 12 种认证方式，任何 4 种认证方式进行组合，主认证可以自由选择
		产品支持 802.1x 认证，要求支持基于端口和 MAC 两种接入控制方式。
		支持二层 MAC 地址 IP 地址绑定；支持跨三层 MAC 地址 IP 地址绑定。
	流量管理	产品支持多调度类相互嵌套的带宽管理设置。支持设置每 IP 最大或最小带宽，支持对每 IP 进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。
支持配置基于 IP、用户、应用的流量管理规则，且至少支持对 3000 种以上应用定制流量管理规则。		

攻击防护	网络攻击防护	产品支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、日志多种防护措施。
		产品支持 DHCP 协议防护。
		产品支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 PiNg of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、LaNd、WiNNUke、DNS 异常、IP 分片等。
		产品支持防护 IP 地址欺骗攻击。
VPN	IPSec VPN	产品支持 IPv4 IPSec VPN 及 IPv6 IPSec VPN。
		产品支持 IPSec VPN 的主模式（Main Mode）、积极模式（Aggressive Mode）、国密三种协商模式建立的网关-网关加密隧道；国密协商模式经国家密码管理局核准。
		支持主流加密算法，包含国际算法 DES/3DES/AES-128/AES-256、国密算法 SM1/SM2/SM4；支持主流验证算法，包含国际算法 MD5/SHA1/SHA-256、国密算法 SM3；支持独立的硬件加密卡。
		支持 IPSec VPN 穿越 NAT，支持 DPD 探测。
		产品支持 GRE 隧道，支持 GRE over IPSec VPN；
		产品的 IPSec VPN 功能支持无损数据压缩算法
		支持本地 CA 并可为参与 IPSec VPN 隧道建立的设备颁发用于身份认证的证书。
	其他 VPN	产品支持 L2TP、支持 L2TP over IPSec、支持 PPTP，并支持本地认证以及 LDAP/Radius/证书/Active Directory/TACACS+/POP3 等第三方用户认证系统。支持客户端地址分配。
		产品支持 SSL VPN，支持使用 SSL VPN 客户端与安全网关建立 SSL VPN 加密隧道，支持对远程用户进行口令认证或证书认证，或证书认证+口令认证双因素；口令认证支持本地认证以及 LDAP/Radius/证书/Active Directory/TACACS+/POP3 等第三方用户认证系统；支持 USB-key 证书；支持本地 CA 并可为 SSL VPN 客户端颁发用于身份认证的证书。
	运维	运维管理

		产品支持三权分立管理，支持安全管理员、审计管理员、系统管理员三种管理员角色；支持以读写、只读、无权限的方式自定义权限管理，权限管理的范围至少包括策略配置、对象配置、网络配置、系统配置、日志等。
		产品支持启用管理员证书认证功能，通过管理员所持有的电子钥匙内的证书，表征管理员身份，实现管理员双因素认证；管理员证书必须为 SM2 证书，且不同角色管理员必须采用不同的 SM2 证书。
		产品支持将告警信息以 SNMP Trap、邮件、声音、短信等形式通知管理员，
		产品支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器
		产品内置抓包工具，并可通过表达式方便灵活的指定抓包过滤条件
	对接 联调	提供开放接口，实现对接联调

## 3 产品型号与指标

### 3.1 NSV2000

序号	指标	指标详细描述
1	产品型号	NSV2000
2	CPU	国产化飞腾 CPU
3	操作系统	国产化麒麟操作系统
4	接口	千兆电口 6 个
		千兆光口 4 个
		万兆电口 4 个
		扩展插槽 1 个(支持扩展 4 口千兆电口，4 口千兆光口)
5	最大并发数	SM2: 6 万
		SM3: 6 万
		SM4: 6 万
6	最大在线用户数	SM2: 6 万
		SM3: 6 万
		SM4: 6 万
7	每秒新建连接数	SM2: 3 万
		SM3: 3 万
		SM4: 3 万
8	网络吞吐率	SM2: 7000Mbps

	SM3: 7000Mbps
	SM4: 7000Mbps