★完全公开

奇安信
新一代网络安全领军者

网神 VPN 安全网关系统-NSV1800 产品白皮书

首次创建时间：2022 年 8 月 18 日

地址：北京市西城区西直门外南路26号院1号

邮编：100044

© 奇安信集团 股票简称：奇安信 股票代码：688561

● 版权声明

奇安信集团，保留所有权利。
奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。
对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。
由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输**

延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利：**在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0.0	C	新建	郑金志	郑金志	2022-8-18

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ 数据分级	公开数据（Y）	内部数据（）	普通商秘（）	核心商秘（）

*数据分级标注及说明：

1、文档编写前，应标注数据安全级别，默认为内部；

2、请根据文档内容评估数据安全级别，在对应数据级别（）中填写（Y）；

3、分级 TIPS：

【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；

【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；

【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；

【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。

更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips

目录

1 产品概述 1
1.1 产品简介 1
1.2 产品性能形态 1
2 产品特色功能 3
2.1 智能安全网关 3
2.2 自动安全组网 3
2.3 零配置快部署 3
2.4 广域出口整合 4
2.5 智能路径优选 4
2.6 可视集中管控 4
2.7 全面安全防护 4
2.8 威胁情报加持 4
2.9 小安智能巡检 5
2.10 灵活防封堵 5
2.11 平台网关高可用 5
2.12 CA 证书管理 6
3 产品特点与优势 7
3.1 高智能、高可用 7
3.2 高安全、高效益 7
3.3 高性能、高稳定 7
3.4 全加密、快组网 7

1 产品概述

1.1 产品简介

网神 VPN 安全网关系统 V4.0 系列产品（以下简称“安全网关”）是网神自主创新的新一代安全网关，符合国家密码管理部门要求，支持核准的国密协商模式及 SM1/2/3/4 算法，IPSec VPN 性能吞吐高达 15G。不仅支持多种 VPN 协议，同时集成了基础防火墙、应用与身份识别、应用层安全防护等综合安全防御功能，实现组网与安全策略一体化，能够为电子政务外网、新关基建设提供全面的接入方案。

1.2 产品性能形态

产品名称	网神 VPN 安全网关系统
版本	V4.0
产品型号	NSV1800
整机吞吐	200Gbps
IPSec VPN 新建连接数	50
IPSec VPN 并发连接数	5000
IPSec VPN 最大加密吞吐	15Gbps
SSL VPN 新建连接数	500
SSL VPN 并发连接数	50000
SSL VPN 最大加密吞吐	5Gbps
SFP 千兆光口数量	4
SFP+万兆光口数量	6
带外管理口（MGT）数量	1
HA 接口数量	1
异步串行口数量	1
USB 接口数量	2

机箱规格尺寸（高*宽*深）	3U 133mm*440mm*600mm

2 产品特色功能

2.1 智能安全网关

网神 VPN 安全网关系统支持多种类型的安全网关，产品形态覆盖低端桌面型 CPE、中高端机架型 CPE 和虚拟化 CPE 等多款型号，架构覆盖 ARM，X86 和国产化等不同的平台，可以提供多种类型接口，不同转发性能的安全网关设备，供客户不同的业务场景进行选择。采用的工业级硬件具备防潮、防雷、防高温、高海拔、防电涌等功能，并且集成 VPN、IPS、AV、FW 等功能，是真正多用途，安全一体化的智能网关设备。

2.2 自动安全组网

网神 VPN 安全网关系统支持通过国际算法模板或国密算法模板，由管控平台统一下发 IPSec VPN 组网配置，管理员可根据模板按需下发组网策略，安全网关即可自动建立业务隔离的安全加密隧道，保证业务数据传送的安全性及私密性，整个过程管理员无需对 IPSec VPN 进行配置。

安全网关采用模板化方式下发 VPN 组网且预置模板.在 fullmesh 拓扑下可实现全自动组建 site-to-site 的网络，无需人工配置，在 partial-mesh 及 star 拓扑下，管理员仅需对分支设备要连接哪一个中心节点进行选择，即可完成对网络的编排。同时，网神 VPN 安全网关系统解决方案支持对未注册的设备进行预编排，将配置完整的生成在管控平台中，待安全网关注册上线后，即可立即下发配置加入 SD-WAN 网络。

2.3 零配置快部署

网神 VPN 安全网关系统支持通过无线上线、邮件上线、部署向导上线、批量上线的方式自动注册安全网关并从管控平台获取网络配置和安全策略配置，实现分钟级上线。极大缩短了设备上线时间，降低了开通业务的复杂度，节省了运维实施成本。

2.4 广域出口整合

网神 VPN 安全网关系统支持 Internet、4G、MPLS、MSTP 等多种广域（WAN）出口的统一整合，当其中一个广域网出口出现故障时，可以切换到其他正常的广域网出口，保证业务持续服务不受影响。

2.5 智能路径优选

网神 VPN 安全网关系统支持遥测技术，通过管控平台监测整个企业广域网的端到端服务质量，基于 WKSP 技术支持基于跳数、时延、带宽等多维度的智能选路，实现基于应用的路径优选和质量保证。

2.6 可视集中管控

网神 VPN 安全网关系统提供可视化集中管控能力，支持对全网的安全网关的自动化运维、网络编排、安全编排、业务管理、威胁管理、安全能力按需定制等，支持全网的网络状态、业务数据及网络质量的集中管理和展示，支持一键跳转安全网关管理界面。

2.7 全面安全防护

网神 VPN 安全网关系统支持多种类型的安全防护，如攻击防护、黑白名单、应用级访问控制以及上网 URL 过滤策略防护等。同时通过数据加密传输、身份统一认证、权限集中管控、威胁深度识别的体系化安全保障，提供全面安全防护的组网方案。

2.8 威胁情报加持

网神 VPN 安全网关系统支持基于“TI INSIDE”引擎驱动的威胁情报能力，可以精准检测出多种勒索病毒、挖矿木马、APT 攻击工具等，定位到网络中的失陷主机并进行一键处置。通过管控平台与威胁情报中心的协同联动，最新的威胁

情报可以迅速由管控平台推送至全网所部署的安全网关上，升级全网安全网关的检测能力。

2.9 小安智能巡检

网神 VPN 安全网关系统解决方案 支持小安巡检机器人，支持基础巡检，专家巡检两种模式。基础巡检中对网神 VPN 安全网关系统解决方案网络的互联网、接口、隧道、路由、业务的状态和质量进行实时探测和智能数据分析，支持设备进行 CPU 利用率，内存利用率，硬盘利用率，风扇转速，设备温度，设备巡行时间等设备健康维度进行巡检，支持对设备威胁统计，流量统计，隧道统计，接口信息，许可证等业务健康维度进行巡检。

专家巡检模式下可以对设备异常，设备 CPU packe 剩余百分比，影响性能开关，转发核占用百分比等进行专家模式巡检，发现设备潜在问题。通过不同的巡检模式可以协助用户基于网络和业务全局状态进行故障定位和运维支持，为网神 VPN 安全网关系统解决方案解决方案的 Devops 能力奠定基础。

2.10 灵活防封堵

网神 VPN 安全网关系统基于 PrivateEX 增强隔离技术为企业用户的广域组网提供私密的虚拟专网，采用 UDP 隧道的传输模式，提高传输效率。由于部分运营商会针对 UDP 数据报文进行封堵，SD-WAN 支持智能自动轮询监听端口技术，有效解决端口封堵问题提高网络自适应性。

2.11 平台网关高可用

奇网神 VPN 安全网关系统解决方案整体方案与架构采用控制平面与数据平面分离的设计，控制平面出现故障时，数据平面不会受到影响，提高了整个网络的可靠性。数据平面可以持续传输业务并可继续感知直连链路的故障并进行线路切换。当控制平面恢复时，全网的控制权可由控制平面继续接管，数据平面恢复向控制平面提交链路探测结果，以保证控制平面可以重新计算全网的最优路径。

网神 VPN 安全网关系统解决方案的安全网关及管控平台均支持高可用功能。

安全网关支持系统层级的高可用，设备内可存在连个不同版本的系统，当其中一个系统故障时，可以切换到另一个系统。当安全网关升级失败时，可以使用备份系统启动设备，实现版本回退。安全网关支持保存三份不同的历史配置，当出现误配置导致业务受影响时，可以通过回滚历史配置来修复问题。同时，安全网关支持设备级的高可用。可以实现设备间的会话同步及隧道状态同步，当其中一台设备故障时，会话及业务可以平滑切换到另一设备，确保业务的连续性。

管控平台系统的高可用功能可以实现主备-高可用。当主系统因软件故障、硬件故障或断电等异常情况下导致服务不可用时，备用系统可以无缝接管 SD-WAN 网络和设备，保障网络和业务的持续可用。

2.12 CA 证书管理

安全网关集成 CA 组件，并可对证书进行管理，可作为小型 CA 中心颁发数字证书，支持 RSA 及 SM2 两种非对称算法。同时安全网关支持与第三方 CA 系统进行对接。

当网络中不仅存在安全网关，还同时部署管控平台时，管控平台同样集成 CA 能力，可作为 CA 中心为全网的安全网关自动颁发数字证书，支持支持 RSA 及 SM2 两种非对称算法。同样，管控平台支持与第三方 CA 系统进行对接。

因此，在采用 VPN 进行组网时，选择数字证书认证的方式来确认通讯双方的身份真实性更具安全性。依赖安全网关具备的安全 VPN 网络能力，更能快速实现颁发证书及通过证书认证才能加入加密网络的方案。这样的方案更具安全性、便捷性。

3 产品特点与优势

3.1 高智能、高可用

基于智能选路 WKSP 技术，实现基于业务的最短路径、最小延迟、保障带宽等维度的智能选路，同时支持多路径保护和多路径负载分担；基于遥测技术实现网络状态和质量的实时探测，并针对故障和质量劣化等情况进行智能的路径切换，保障业务的高可用。

3.2 高安全、高效益

基于 PrivateEX 增强隔离技术为企业用户的广域组网提供私密的虚拟专网，在兼容标准的 IPsec VPN 技术的情况下，采用极简的隧道封装，降低隧道技术带来的额外开销，进一步降低企业的带宽成本。

3.3 高性能、高稳定

基于自主研发的第四代 SecOS 操作系统和异步并行处理的专利技术，为安全网关提供高性能的数据转发处理能力，以及高性能的深度应用识别能力。

基于 CPU 专属分配技术，将管理平台和数据转发平面分属不同的 CPU 处理，提升了安全网关的稳定性，同时支持双操作系统和网关的 HA 部署方案以提高方案部署的可靠性。

3.4 全加密、快组网

网神 VPN 安全网关系统解决方案不仅实现了国际标准模式下的全自动组网，同时首创全自动国密模式安全组网能力，实现符合国家密码管理局要求，经商密检测中心核准的国密模式 IPSec VPN 自动组网功能。

支持对接入的安全网关设备进行双向认证，基于 PKI 技术实现一体化证书申请、颁发、安装。并通过网络编排能力实现全网自动化国密模式组网。