★完全公开

网神 SecGate3600 防火墙
NSG5000-TG35M-QYD
产品白皮书

地址：北京市西城区西直门外南路26号院1号

邮编：100044

版权声明

● 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、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。

目录

1. 产品概述 1
1.1 产品简介 1
1.1.1 产品性能及形态 1
2. 产品功能 2
2.1 基础组网功能 2
2.2 精细化访问控制功能 3
2.3 一体化威胁防护功能 4
2.4 可视化智能管理功能 4
2.5 协同防御功能 5
3. 特点与优势 5
3.1 领先的第四代 SecOS 安全协议栈 5
3.2 三重云+五大联动 6
3.3 安全隔离的虚拟系统 6
3.4 智能动态策略快速拦截攻击 7
3.5 应用层综合安全防护技术 7
3.6 完善的内网 DLP（数据防泄漏） 7

1. 产品概述

1.1 产品简介

在信息化飞速发展的今天，网络形势正发生着日新月异的演变，层出不穷的新型威胁冲击着现有的安全防护体系。传统的安全设备，一是以本地规则库为核心，无法有效检测已知威胁；二是没有数据智能，无法感知未知威胁；三是没有联动智能，无法对网络进行协同防御。面对诸如 0-day、APT 及未知威胁等越来越多样化和层次化的攻击，逐渐变得力不从心。归根结底，现在的安全和产品体系还在用单机的、私有的思路来解决网络的、公有的已知威胁。而面对未知的安全威胁，我们不能再孤军作战，而必须是协同共享。

网神 SecGate 3600 防火墙系统是奇安信自主创新的新一代防火墙安全系统，基于奇安信 NDR（基于网络的检测与响应）安全体系。在强劲性能与更先进架构的支撑下，集成了防火墙、VPN、应用与身份识别、防病毒、入侵防御、虚拟系统、行为管理、应用层内容安全防护、威胁情报等综合安全防御功能，并完成了与奇安信天眼、天擎及病毒云、URL 云、应用云、云沙箱、情报云等多项系统的协同防御功能，在扩展了协同防御能力的基础上，由防火墙的分析中心、数据中心、处置中心三大中心实现对威胁的分析、定位、处置一体化过程。是专门为政府、军队、金融、教育、运营商、企业的网络出口打造的基于协同防御体系的新一代安全防御系统。

1.1.1 产品性能及形态

产品名称	网神 SecGate 3600 防火墙系统 v3.6.6.0
产品型号	NSG5000-TG35M-QYD
防火墙吞吐（bps）	20Gbps
标配并发连接数	150 万
每秒新建连接数	5 万
Ipsec 吞吐	2Gbps
虚拟防火墙个数	16

策略数	9000
电口 10/100/1000Base-T 个数	6
SFP 千兆光口个数	8
SFP+万兆光口个数	4
异步串行管理接口	1
带外管理口（MGT）	1
高可用性口（HA）	1
USB 接口	2
机箱规格&尺寸	1U 440mm（宽）×560mm（深）×44.2mm（高）

2. 产品功能

2.1 基础组网功能

1. 部署模式：支持路由模式、透明模式、交换模式、混合模式以及旁路模式接入。

2. 路由特性：默认路由、静态路由、策略路由、支持 RIP、RIPng、OSPF、BGP 等动态路由。

3. IP 协议：支持 IPV4、IPV6 双栈。

4. NAT：支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式。

5. 负载均衡：支持基于 IP、ISP、应用、用户、服务等的多链路负载均衡，支持 DNS 流量的负载均衡，支持基于服务器地址的负载均衡；支持 IPSec VPN 的多链路备份和负载。

6. 网络服务：支持 DHCP 服务器、DNS 透明代理、ARP 代理等网络服务。

7. VPN：支持 IPSec VPN、SSL VPN、L2TP、PPTP、GRE，IPSecVPN 支持国密算法；SSL VPN 支持 Windows 客户端；DS-Lite 支持作为 B4 和 AFTR。

8. 虚拟系统：支持虚拟系统路由、交换、监控、审计、安全、防护等全隔离。

9. 高可靠性：支持双机热备功能，支持路由和透明模式下的“主-备”、“主-主”模式，支持接口联动，链路探测。

2.2 精细化访问控制功能

1. 访问控制：支持基于 IP、安全域、VLAN、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制，支持一条安全策略配置应用控制、入侵防护、URL 过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，并支持安全策略的快速检索，冗余策略分析，命中时间分析和安全策略推荐。

2. 应用识别：可精确识别 5000 余种互联网应用，700 余种移动应用，支持应用云识别。

3. 行为管控：支持对 HTTP、SMTP、POP3、IMAP、FTP、TELNET 协议进行细粒度的控制，过滤不受信任的网络行为。

4. 用户认证：支持基于 web 的无客户端方式的用户认证，具备集成 AD 活动目录、LDAP、RADIUS 的第三方认证。

5. 文件过滤：不基于后缀名方式实现对文档、压缩、归档三大类共 30 多种常用文档类型过滤。

6. 邮件过滤：支持对邮件收发件人进行过滤，基于 RBL 黑名单及自定义 IP 地址黑名单两种方式的反垃圾邮件支持。

7. URL 过滤：预置 133 类 URL 资源库，可手动离线或自动在线进行更新升级，支持 URL 云查询，支持云端 URL 查询分析，支持自定义 URL 过滤。

8. 内容过滤：实现 HTTP、FTP、POP3、SMTP、IMAP 五种应用协议的双向内容传输过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义。

9. 带宽管理：支持根据 IP 地址、用户、服务、应用、时间等信息划分虚拟 QoS 通道进行带宽管理，支持多层级调度类嵌套的最大带宽限制和最小带宽保证。

10. 黑名单：支持地址白名单;支持基于时间维度的 IP 或 MAC 的黑名单设置；支持域名黑白名单。

2.3 一体化威胁防护功能

1. 攻击防护：支持攻击防护类型包括：Flood（SYN Flood、ICMP Flood、UDP Flood、IP Flood）、恶意扫描（禁止 tracert、IP 地址扫描攻击、端口扫描）、欺骗防护（IP 欺骗、DHCP 监控辅助检查）、异常包攻击（Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片）、ICMP 管控（禁止 ICMP 分片、禁止路由重定向报文、禁止不可达报文、禁止超时报文、ICMP 报文大小限制）、应用层 Flood（DNS Flood、HTTP Flood）SYN Cookie。

2. 病毒防护：搭载人工智能引擎，能免疫 90%以上的加壳和变种病毒，并支持病毒云查杀技术对 HTTP、FTP、SMTP、POP3 和 IMAP 流量进行病毒查杀。

3. 本地威胁情报检测：支持威胁情报库自动及手动升级，防火墙威胁情报数量为 4 万以上。

4. 入侵防御：目前可识别并阻断 7000 余种漏洞入侵和间谍软件，该数量后续会持续增加；支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL 注入、WEB 攻击、弱口令扫描等入侵行为防御，支持生成动态策略。

2.4 可视化智能管理功能

1. 设备管理：支持 Web 界面（Http、Https）和命令行界面（SSH、Console、CLI）。

2. 管理权限：支持超级管理员、策略管理员和审计管理员三权分立管理，支持自定义管理员权限。

3. 日志输出：支持流量日志、威胁日志、域名日志、URL 过滤日志、邮件过滤日志、行为日志等多维度中文可视化分析和日志外发，并支持基于 IP、用户、接口、地区、应用等多达 90 多种过滤条件模糊搜索自定义时间段内的历史日志。

4. 统计分析：支持按应用、IP、用户等类型对相应类型的字节数、会话数进行在指定时间范围内进行排序，支持基于接口、安全域的新建连接数、并

发连接数的历史统计。支持基于网络中的流量趋势及增长应用、下降应用、带宽消耗、威胁的排行统计。并支持威胁地图，帮助用户了解网络中威胁基于地理位置的分布的风险。

5. 监控分析：支持会话监控、用户监控、资产监控、路由监控、系统资源监控。

2.5 协同防御功能

1. 终端联动：智慧防火墙可以与奇安信天擎终端安全管理系统进行联动，增强防火墙对应用特征及木马特征的识别。

2. 天眼联动：支持与天眼系统联动，防火墙支持发送常用协议头部信息给天眼，支持加密传输方式，天眼可以向防火墙下发域名、URL、恶意 IP 等处置策略，支持自动处置和人工处置。

3. 天眼沙箱联动：防火墙支持与天眼威胁文件鉴定器（沙箱）联动，进行文件静态检测和动态检测，从而可以识别出未知威胁文件。

4. 奇安信安全云联动：防火墙支持与奇安信安全云联动，通过奇安信安全云，云防进行病毒云查杀、URL 云识别、云沙箱、应用云识别、威胁情报云检测，奇安信安全云应急响应通知，支持防火墙向奇安信安全云，云镜上传日志，并通过云端威胁情报进行威胁检测。

5. NGSOC 联动：支持与 NGSOC 联动，防火墙支持发送日志 NGSOC，NGSOC 可以向防火墙下发处置策略，支持人工处置。

3. 特点与优势

3.1 领先的第四代 SecOS 安全协议栈

具备完全自主知识产权的网神第四代 SecOS 操作系统，在第三代 SecOS 带来的高安全性、高开放性、高扩展性和高可移植性基础之上，重点加强了防火墙的协同防御能力、数据生成能力、数据分析能力、数据处置能力，让防火墙具备多端联动、风险信息全方位展示、拦截已知威胁、定位未知威胁、一键处置威胁行

为的能力，弥补了传统防火墙重配置轻管理的缺点，并能提供多维度的有效信息帮助用户完成日常维护工作。

3.2 三重云+五大联动

三重云

木马云：木马云查杀功能，可以有效补充本地木马库不足，解决无法抵御未知木马问题。

病毒云：病毒云查杀功能，可第一时间拦截新病毒、未知病毒，并将病毒库扩充到 20 亿。

URL 云：URL 云查询功能，可极大扩充本地 URL 库，解决本地 URL 库分类少，资源不足问题。

五大联动

情报威胁：防火墙可以接收来自奇安信安全云的威胁情报，根据情报生成动态策略，以此确认未知数据是正常数据还是恶意数据，并根据结果进行下一步的阻断或者放行处理。防范以多种形态出现的新恶意软件和 DDoS 攻击，以及 APT、0-day 等攻击所带来的日益增长的威胁。

终端协同：通过与天擎终端安全管理平台联动，防火墙可以实现应用识别的增强，更加精准的完成对应用的限流、阻断、过滤功能。

天眼联动：支持与天眼系统联动。防火墙支持发送常用协议头部信息给天眼。支持加密传输方式。天眼可以向防火墙下发域名、URL、恶意 IP 等处置策略。

NGSOC 联动：防火墙支持发送日志 NGSOC。NGSOC 可以向防火墙下发处置策略。支持人工处置。

沙箱联动：进行文件静态检测和动态检测，从而可以识别出未知威胁文件。

3.3 安全隔离的虚拟系统

虚拟系统功能可以将网神 SecGate 3600 防火墙系列虚拟成多个相互隔离并独立运行的虚拟系统，每一个虚拟系统都可以为用户提供定制化的安全防护功能，并可配备独立的管理员账号。在用户网络不断扩展时，通过虚拟系统功能不仅能

有效降低用户网络的复杂度，还能提高网络的灵活性。当这些相互隔离并独立运行的虚拟防火墙系统需要通讯时，可以通过网神 SecGate 3600 防火墙系列提供的虚拟接口实现，而不需要通过物理链路将它们进行连接。

3.4 智能动态策略快速拦截攻击

网神 SecGate 3600 防火墙系列配备智能动态策略机制，当入侵防护、木马专项防护、防弱口令扫描等模块对异常流量进行过滤识别后，防火墙会提取攻击特征并生成智能动态策略，当攻击持续不断流入防火墙时，攻击特征被记录的异常流量会直接命中动态策略，快速拦截在防火墙之外。在目前攻击手法越来越偏向混合攻击+大流量攻击组合进攻的当下，智能动态策略可以为防火墙节省大量资源用来应对大流量混合攻击，并保证正常数据的通过。

3.5 应用层综合安全防护技术

网神 SecGate 3600 防火墙系列不仅提供多达 23 种普遍的基于网络层的攻击防护，并配备入侵防护、病毒检测、地址黑白名单、域名黑白名单功能。针对 HTTP、DNS、DHCP 协议提供针对性、多级别、适用于不同场景的应用层安全防护，更提供木马专项查杀、防弱口令扫描、局域网多播广播防护等功能，覆盖用户内外网安全。

3.6 完善的内网 DLP（数据防泄漏）

网神 SecGate 3600 防火墙系列具有邮件过滤，文件过滤，内容过滤功能，其中邮件过滤支持基于 RBL 黑名单以及自定义本地黑白名单的邮件过滤、同时能够基于收发件人关键字进行邮件过滤；文件过滤支持针对 HTTP、SMTP、POP3、IMAP、FTP 协议传输的文件进行过滤，主要包含 3 大类：文档类、压缩类、归档类；内容过滤支持针对 HTTP、SMTP、POP3、IMAP、FTP 协议内容进行过滤，支持预定义关键字，包含身份证号、手机号等 5 类，支持基于内容过滤的页面推送功能，支持自定义添加关键字，可以正则匹配或者完全匹配。