

★完全公开



# 网神 SecDDoS 3600 抗拒绝服务系统 V4.0 F3300-U008P 产品白皮书

首次创建时间：2024 年 8 月 1 日  
最新修改时间：2025 年 7 月 16 日

地址：北京市西城区西直门外南路26号院1号

邮编：100044

# 1 产品概述

网神 SecDDoS 3600 抗拒绝服务系统主要职责就是抵御 DDoS 攻击行为，通过对流量的分析和识别，检测流量中的各种 DDoS 攻击行为，使用阈值限制，流量算法、识别验证等多种方式识别 DDoS 流量，高效的抵御 DDoS 攻击和保障用户网络的完整性和可靠性。

## 2 产品功能

### 2.1 极速处理能力

网神 SecDDoS 3600 抗拒绝服务系统实现极速的流量处理能力，从低端千兆到万兆高端产品均为 64 字节小包限速能力，极速的小包处理能力可以完全处理大流量 DDoS 攻击。网神 SecDDoS 3600 抗拒绝服务系统从软件到网卡驱动都做了大量的优化，因 DDoS 攻击行为主要是流量型攻击，因此对于网神 SecDDoS 3600 抗拒绝服务系统来说 64 字节小包的性能要求尤为重要。

### 2.2 双协议栈识别

随着 IPv6 的高速普及，网神 SecDDoS 3600 抗拒绝服务系统支持双协议栈过滤，通过对 IP 地址的识别，自动区分是 IPv4 还是 IPv6 协议。快速适应网络的高速发展需求和 DDoS 防御需求。

### 2.3 自主防御算法

网神 SecDDoS 3600 抗拒绝服务系统具备自主开发的独立防护算法，包含连接代理、数据转发、内核防护、数据挖掘等防护算法。防护算法主要是抵御来自网络层、应用层的 DDoS 攻击。

- **独特的连接代理防护算法**，针对 SYN 攻击，采用 SYN Proxy 连接代理防护模式，以代理模式处理客户端与服务器之间的连接，同时完成攻击报文

的过滤，即使在海量攻击下仍然可以保证 99.99% 的新建连接的成功率。

- **高效的连接数据转发算法**，采用自主研发的 TCP Fast Rechecksum 技术，高效的处理来自 TCP 的连接数据及其校验和，并进行快速转发，而无需重新统计报文数据，对 TCP 反射攻击进行防护，针对 SYNACK 攻击报文进行精准过滤，支持对 TCP、UDP、ICMP 分片报文进行限速控制。
  - **模块化的内核防护算法**，采用了 Kernel Protection Plugin For Linux & Windows 技术，将特定的防护算法以模块的形式实现，简化了核心代码，优化了系统构架，并具有良好的扩展性。
  - **基于数据挖掘的通用防护算法**，采用 Generic Protection Based On Data Mining 技术即基于数据挖掘的通用防护算法，对于开启保护的服务器，防护模块会自动对客户端与服务器端的通信进行数据统计与挖掘，察觉恶意流量并加以过滤，有效率高达 97.3% 以上。

## 2.4 应用层防御

网神 SecDDoS 3600 抗拒绝服务系统针对应用层的 CC 攻击时，使用切入页面防护手段进行防御。僵尸网络、CC 攻击器都是电脑系统，无法输入验证码、验证页面等内容。网神 SecDDoS 3600 抗拒绝服务系统就是，采用 Web Protection Based On Page Injection 即基于页面插入式 Web 防护算法。对于开启防护的 Web 服务器，防护模块会主动插入 Web 页面，客户端可无察觉的自动完成验证过程，已达到高效的防御 Web 类连接攻击的目的。另外，也可以通过验证服务器辅助来加强防护级别。

## 2.5 阈值限制

网神 SecDDoS 3600 抗拒绝服务系统也使用标准的“阈值”设置。针对 TCP、UDP、ICMP 等协议进行数据包流量限制。通过对流量限制、报文限制、连接限制等多维度的阈值限制来保障带宽的有效使用。

## 2.6 规则匹配

网神 SecDDoS 3600 抗拒绝服务系统有规则匹配防御方式，通过对协议、端口号、标识位等多元素的正则匹配过滤方式，通过对 TCP、UDP、ICMP 等协议数据包的多维度字符的过滤来有效抵御 DDoS 攻击行为

## 2.7 端口保护

网神 SecDDoS 3600 抗拒绝服务系统的端口保护功能，主要基于重要应用业务的，通过端口来识别应用业务，例如 FTP、POP3、FTP、POP3、SSH、HTTP、DNS、SMTP 等。通过设置延迟提交、验证 TTL 值、支持对 DNS 查询防护以及 DNS 响应防护的能力。支持 DNS 协议防护的检测和清洗。同步连接等多种处理方式来抵御针对应用业务的 DDoS 攻击行为

## 2.8 旁路防御

网神 SecDDoS 3600 抗拒绝攻击系统支持旁路抵御模式，支持 BGP 旁路牵引防护模式。支持在设备上直接查看抓包文件，并根据抓包内容快速关联防护策略，一键配置下发；产品提供手工牵引、自动牵引模式。当没有 DDoS 攻击时，流量不经过网神 SecDDoS 3600 抗拒绝攻击系统。减少网络设备。当发现 DDoS 攻击，流量牵引进入网神 SecDDoS 3600 抗拒绝攻击系统进行流量过滤。

## 2.9 流量分析器

网神 SecDDoS 3600 抗拒绝攻击系统有配套产品——流量分析器。流量分析器主要针对网络层、应用层流量进行分析，发现 DDoS 攻击流量。支持傀儡机防护，通过对源 IP 的 URL 访问比例进行统计防护傀儡攻击。与网神 SecDDoS 3600 抗拒绝服务系统形成组合方案并旁路部署在网络中。当 DDoS 攻击流量出现，流量分析器除了进行分析流量也同时把流量自动牵引至抗拒绝服务系统进行流量过滤。

## 2.10 扩展集群方式

网神 SecDDoS 3600 抗拒绝服务系统支持扩展集群方式，针对流量不断扩展的同时，与老旧设备形成集群扩展部署方式，旧设备与新设备形成一个整体的防御体系。采用 Extensible Firewall Cluster Mode 即可扩展的集群模式，通过领先的数据分流技术，使得若干设备可组合形成更大的防护主体，提供海量攻击的防护解决方案。

## 2.11 数据综合分析

网神 SecDDoS 3600 抗拒绝攻击系统支持多维度的数据分析功能，提供基于攻击主机、攻击类型、流量分析、性能分析、连接分析、数据报文捕捉等多种数据分析。并为多种数据塑造成线形、饼型等分析方式。

# 3 产品参数

## 3.1 性能指标

产品型号	F3300-U008P
CPU	国产化 CPU 飞腾 D2000
操作系统	国产化麒麟操作系统
64 字节小包处理能力	860 万/pps
吞吐	8G
处理能力	240 万
混合报文抗攻击能力	2Gbps
主机防护数量	30 万/个
新建连接数	56 万/秒

并发连接数	1800 万
延迟	<20us

## 3.2 硬件规格

产品型号	F3300-U008P
串行配置管理接口 (个)	1
独立管理口	1
独立 HA 口	1
接口	6 个电口+4 个万兆光口
机箱	2U
BYPASS	2 对