

★完全公开

网神 SecIPS 3600 入侵防御 系统国产化系列 P3300-3680-F 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 产品概述

1.1 产品参数

表 1 产品型号与指标

| | |
|-------------------------|---------------------------------------|
| 产品名称 | 网神 SecIPS 3600 入侵防御系统 |
| 产品型号 | P3300-3680-F |
| 商品编码 | P3300-3680-F-QW |
| 硬件平台 CPU | 国产化飞腾处理器 |
| 操作系统 | 国产化麒麟操作系统 |
| 网络层吞吐 | 40Gbps |
| 应用层吞吐 | 101Gbps |
| 最大并发会话数 | ≥400 万 |
| 每秒新建会话数 | 35 万 |
| 电口 10/100/1000Base-T 个数 | 8 |
| 1000M 光口个数 | 8 |
| 10G 光口个数 | 4 |
| 扩展槽 | 1 |
| 管理接口（电口）个数 | 1 |
| HA 接口（电口）个数 | 1 |
| USB 接口 | 2 |
| RJ45 串口 | 1 |
| 存储 | 1TB |
| 机箱规格&尺寸 | 2U 430mm（宽）×600mm（深）×90mm（高） |
| 机架规格 | 19 寸 |
| 温度和湿度 | 工作温度:0~40℃，存储温度:-25~70℃，相对湿度:5~90%不凝结 |

| | |
|------|--------------------------|
| 电源 | 冗余电源 100-240V 100W |
| 可选模块 | IPS/APP/AV/URL |

2 产品功能

2.1 网络适应能力

| |
|--|
| 产品支持路由模式、透明模式、旁路模式以及混合模式接入，满足复杂应用环境的接入需求。 |
| 支持物理子接口技术，可以虚拟多个逻辑接口（不依靠 VLAN 区分）。 |
| 支持 VLAN 接口，支持 VLAN 子接口产品。 |
| 支持多个纯透明桥，支持桥接口。 |
| 支持聚合接口，聚合接口支持路由和交换两种工作模式，聚合模式（Channel 模式）支持三种：轮询方式、热备方式、802.3ad，其中 802.3ad 方式支持 3 种负载算法：根据源和目的 MAC 地址组合均衡、根据 MAC 地址和 IP 组合均衡、根据 IP 和 TCP/UDP 端口组合均衡。 |
| 支持聚合子接口。 |
| 支持环回接口。 |
| 支持隧道接口。 |
| 支持 ADSL 拨号接口（16 条）。 |
| 支持 MPLS 的透传和控制。 |
| 支持将接口流量镜像到其他物理接口。 |
| 三层接口 IP 地址支持 IPv4 和 IPv6 地址。静态地址支持 float 和 static 类型，通常情况下使用 float 类型。 |
| 支持安全域的配置，包括二层安全域和三层安全域。 |
| 路由模式物理接口、物理子接口、旁路模式物理接口、VLAN 接口、桥接口、路由模式聚合接口、旁路模式聚合接口、聚合子接口、虚拟系统接口支持巨帧（MTU>1518，最大可以支持 9216），支持静态、策略路由、OSPF、BGP4 等动态路由；。 |

| |
|--|
| 支持 802.1d 标准生成树协议，支持 VLAN Trunk 功能。 |
| 支持 IGMP Snooping。 |
| 支持静态 DNS，从指定的入接口或源 ISP 接收到的 DNS 请求，设备会代替 DNS 服务器将指定的域名与 IP 地址对应关系应答给客户端。典型应用环境为内网用户通过公网域名访问内网服务器。 |
| 支持 DDNS 动态域名解析，可实时查看域名、接口及 IP 的更新状态，支持四家服务商，分别为：oray（花生壳动态域名）、pubyun（公云）、changeip、noip，仅支持 ADSL 接口。 |
| 支持 DNS 透明代理，设备收到客户端 DNS 请求报文时，设备会将请求报文中的 DNS 地址替换为设备指定的代理 DNS 地址，帮助其实现 DNS 解析，可配置一个首选两个备选 DNS 代理服务器。 |
| 支持 DHCP Server 和 DHCP Server Client 以及 DHCP 中继，支持 DHCP 地址绑定和 DHCP 域名服务器。 |
| 支持 ARP 代理。（仅命令行支持） |
| 支持添加静态 MAC 地址表和静态 ARP 地址表。 |
| 支持静态路由、策略路由、ISP 路由、动态路由（RIP、RIPng、OSPF、OSPFv3、BGP）、静态多播路由以及动态多播路由。 |
| 支持调整策略路由默认的优先级，可高于直连路由或静态路由。（命令行实现） |

2.2 双栈支持

| |
|---|
| 支持接口 IPv4、IPv6 地址配置。 |
| 支持使用 IPv6 地址进行设备管理。 |
| 支持 IPv6 邻居的动态管理和静态配置。 |
| 支持 NAT64 和 DNS64。 |
| 支持 IPV6 手动及自动的 IP/MAC 探测及绑定。 |
| 支持 IPV6 的本地认证。 |
| 支持 IPV6 的 SYSLOG、SNMP。 |
| 支持 IPV6 下静态路由、策略路由、动态路由（RIPng、OSPFv3、BGP4+）。 |
| 支持 IPV6 下的漏洞防护、防间谍软件、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及 QoS。 |

支持 IPv6 安全策略、SSL 解密策略。

支持 IPv6 隧道技术（6to4、ISATAP、手工隧道）。

支持 IPv6 地址黑名单。

支持 IPv6 Web 认证。

2.3 访问控制能力

安全策略支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。

支持可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许）进行访问策略配置，能够配置是否生成访问控制策略的会话日志，支持访问控制策略的导入导出；

支持未配置安全策略时，设备执行默认的全禁止策略。支持用户修改默认策略为允许。（命令行实现）

支持冗余策略分析。

支持策略启用，无需编辑策略即可快速启用或禁用策略。

支持对象与策略引用关系的展示及查看，增加易用性。

支持通过一条安全策略引用漏洞防护、防间谍软件、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控配置文件，实现对应功能的高级访问控制。

支持 8 个会话长连接自定义设置，每种长连接可以被任意安全策略引用，实现不同的业务、不同的会话保持时长。

支持会话限制功能，可以根据 IP 地址、安全域（入域、出域、双向）、应用进行会话限制，支持对单个 IP 或所有 IP 的新建和并发连接数进行限制。

支持通过过滤条件对当前的会话进行查询和统计。

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。

支持基于安全域的 IPv4 和 IPv6 的 IP-MAC 绑定，支持 IP-MAC 探测。

支持基于安全域的 IPv4 和 IPv6 的 IP-MAC 未绑定策略，对未绑定到 IP-MAC 绑定列表中的 IP 地址，可自定义允许访问还是禁止。

管理主机的可信主机、可信 MAC 功能支持对管理设备的 IP 地址、MAC 地址进行控制。

2.4 反病毒

| |
|--|
| 提供全面、强劲的病毒检测及防护功能，支持通过对 HTTP、FTP、SMTP、POP3、IMAP、SMB 协议进行病毒扫描，并可以根据扫描结果进行相应的处理。 |
| 支持对多种网盘网页版、网页邮箱、论坛、博客进行病毒扫描，并根据扫描结果进行相应处理。 |
| 支持的压缩文件解压层数，默认为 3。最大支持 6 层。 |
| 搭载 AV 引擎，能免疫 90%以上的加壳和变种病毒。 |
| 支持自定义病毒签名，通过病毒特征的 MD5 码进行自定义病毒识别。 |
| 支持病毒例外，对特定的病毒特征不进行查杀。 |
| 支持病毒样本留存。 |
| 支持 web 浏览病毒推送消息、邮件病毒推送消息和文件传输病毒推送消息。 |
| 支持 AV 特征库自动及手动升级。设备默认的标准库数量超过 3500 万。 |

2.5 漏洞防护和防间谍软件

| |
|---|
| 支持防护的漏洞类型包括：缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、支持抵御 SQL 注入、XSS 注入、webshe11 等多种常见的应用层安全威胁，支持配置 SQL 注入白名单、WEB 攻击、其他未分类攻击、自定义签名。 |
| 支持对 HTTP、FTP、SMTP、IMAP、POP3、TELNET 等服务的隐蔽通信检测和防护，可设置相应警告、阻断动作； |
| 支持抵御 SQL 注入、XSS 注入、webshe11 等多种常见的应用层安全威胁，支持配置 SQL 注入白名单； |
| 支持针对具体的漏洞防护攻击类型进行日志、阻断、放行、重置方式的动作设定。默认给出各个预定义漏洞特征的推荐设置动作。支持查看单个预定义漏洞的 CNNVD 编号或 CVE 编号及详细信息。 |
| 支持防护的间谍软件的类型包括：木马后门、病毒蠕虫、僵尸网络、自定义签名。 |
| 支持对 HTTP、FTP、SMTP、IMAP、POP3、TELNET 等服务的隐蔽通信检测和防护，可设置相应警告、阻断动作； |
| 支持自定义间谍软件签名。支持自定义基于 TCP、UDP、HTTP 协议的间谍软件，并根据各协议的报文结 |

构，指定一个或多个字段的特征值，这些特征值可以被以文本的形式或正则表达式的形式进行匹配，同时支持是否按顺序对这些特征值进行匹配检测。支持自定义间谍软件的源端口范围及目的端口范围。

支持针对具体的间谍软件类型进行日志、阻断、放行、重置方式的动作设定。默认给出各个预定义间谍软件的推荐设置动作。支持查看单个预定义间谍软件的详细信息。

产品具有内置 4000 种 IPS 的攻击特征，可检测包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等攻；

2.6 本地威胁情报检测

支持威胁情报库自动及手动升级。设备威胁情报库数量为 4 万以上。

2.7 高可用性

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。

支持配置同步和动态信息同步。

支持抢占模式和非抢占模式。

支持非抢占模式的强制主备切换。

支持透明模式下的非对称主主部署。

支持接口联动。

支持 HA 接口监控。

2.8 抗攻击能力

支持基于安全域的攻击防护配置。

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。

支持对 DNS Flood 攻击进行 5 种处理动作：警告、丢弃、普通防护、增强防护及授权服务器防护。

| |
|--|
| 支持对 HTTP Flood 攻击进行 4 种处理动作：警告、丢弃、普通防护、增强防护。 |
| 支持 TC 反弹技术和 NS 重定向技术。 |
| 支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护，可以防止局域网内广播和多播数据包泛滥，保障网络正常通信。 |
| 支持 DHCP 防护，可进行 DHCP 服务器检查、DHCP 请求检查和 DHCP 请求限速等功能。 |
| 支持 SYN Cookie 设置。 |
| 支持 IP 安全域关联，指定 IP 或网段从特定的安全域访问，防止 IP 欺骗。 |

2.9 日志审计能力

| |
|---|
| 支持日志的中文本土化展示，日志分为流量日志、威胁日志、域名日志、URL 过滤日志、邮件过滤日志、内容日志、行为日志、即时通讯日志、配置日志和事件日志。 |
| 日志支持模糊搜索和按精确策略条件搜索，协助定位异常行为，并通过带条件跳转实现指定行为在分析中心中的关联活动展示，确认异常行为是否具有威胁。 |
| 支持设置查询日志的时间。 |
| 支持对日志进行分析，输出网络活动、威胁活动、阻止的活动等分析结果。支持自定义分析活动。 |
| 事件日志可按功能模块进行分级、分类记录和查看和外发到日志服务器。分级包括：紧急、警报、严重、错误、告警、通知、信息和调试。 |
| 可提供自有品牌管理软件对日志进行收集、分析，并能提供详尽日志统计报表。 |
| 支持针对配置变更、病毒事件、攻击事件、异常事件、启动事件及 CPU 温度、CPU 风扇转速、NAT 端口池利用率、CPU 利用率、内存利用率、硬盘利用率、接口带宽比等系统资源等进行邮件告警。 |

2.10 监控

| |
|--|
| 支持会话监控，支持断开指定的会话或断开设备全部会话。 |
| 支持基于 IP、端口、安全域、应用、安全策略等信息对会话进行高级查询。 |
| 支持系统监控。包括对 CPU 利用率、CPU 温度、CPU 风扇转速进行监控。 |
| 支持隧道监控，可对 IPSec VPN 两阶段的基本信息、隧道状态、超时时间、流量大小进行实时统计。 |
| 支持服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非 |

法外联行为并告警；

支持服务器监控和终端监控功能显示。基于安全域纬度监控网络中的服务器、PC 终端用户及手持移动终端用户等资产类型的监控及统计, 并对访问服务器的 IP 及登入用户名进行记录, 并关联相关用户信息。

支持路由监控。包括 IPv4 路由监控、IPv6 路由监控、策略路由监控、ISP 路由监控、多播转发表监控。

多种响应方式, 包括: 告警、阻断、IP 隔离、抓包等需求。

2.11 报表

带硬盘的设备支持添加报表任务。支持每天、每周、每月生成报表。报表支持本地保存、FTP 服务器上传、邮件发送（发送后处置）。

支持下载已生成报表。

支持自定义报表模板。模板下默认支持威胁汇总、流量汇总、应用程序汇总子类型。

2.12 安全诊断能力

表 33 安全诊断能力

支持在 Web、CLI 下的在线抓包。

支持在 CLI 下的调试工具。