NSv 270/470/870

SonicWall Network Security virtual NSv 270/470/870 防火墙，提供企业级安全、简化管理、完全可见性、灵活部署，同时为虚拟工作负载提供卓越性能。

虚拟环境中经常发现新漏洞，这些漏洞会产生严重的安全隐患和挑战。但是，保护所有这些安全向量还需要能始终将正确的安全策略应用于正确的网络控制点，因为一些安全故障可能是由无效策略或错误配置所导致。

亮点

公共云、私有云和政府云安全

- 具有自动实时漏洞检测和预防功能的下一代防火墙
- 已获专利的 Real-Time Deep Memory Inspection (RTDMI™) 技术
- 获得专利的免重组深度包检测 (RFDPI) 技术
- 通过统一策略实现完整的端到端可见性和简化管理
- 应用程序智能与控制
- DNS 安全
- 基于信誉的内容过滤服务 (CFS 5.0)
- Wi-Fi 6 防火墙管理
- 网络访问控制与 Aruba ClearPass 集成
- 支持 AWS 和 Azure 美国政府云
- 与 Microsoft Azure Sentinel 集成以实现更快的事件响应
- 支持私有云 (ESXi、Hyper-V、KVM、Nutanix) 和公共云 (AWS、Azure) 平台

虚拟机保护

- 数据保密性
- 防止数据泄露的安全通信
- 流量验证、检查和监控
- 虚拟网络弹性和可用性

数据表

NSv 防火墙系列可以帮助安全团队减少这类安全风险和漏洞，这些安全风险和漏洞会严重干扰您的关键业务服务和运营。它使企业能够控制通过防火墙的动态流量，并提供对不同策略的可见性和洞察力。还能帮助简化管理任务、减少配置错误并加快部署时间，所有这些都有助于改善整体安全状况。

SonicOSX 和安全服务

SonicOSX 架构是 NSv 270/470/870 防火墙的核心。它由功能丰富的 SonicOSX 7 操作系统驱动，具有直观的用户界面 (UI)、高级安全性、联网和管理功能。

SonicOSX 7.0 从头开始构建，具有统一策略，可提供对各种安全策略的集成管理。在每个防火墙的单个规则库中轻松配置第 3 层到第 7 层控制，为配置策略提供一个集中位置。新网络界面提供关键威胁信息的图形可视化，并显示可操作的警报，提示您通过简单的点击操作来配置上下文安全策略。

NSv 进一步集成 SD-WAN、TLS 1.3 支持、实时可视化、高速虚拟专用网络 (VPN) 以及其他强大的安全功能。未知威胁会被发送到 SonicWall 基于云的 Capture Advanced Threat Protection (ATP) 多引擎沙箱进行分析。Capture ATP 利用 SonicWall 已获专利的 Real-Time Deep Memory Inspection (RTDMI) 技术来发现和拦截驻留在内存中的恶意软件和零日威胁。

结合 Capture ATP、RTDMI 技术和安全高级服务，NSv 系列防火墙可在恶意软件进入您的关键系统之前将其拦截在网关处。

部署

1. 云边缘：保护公共云、私有云和政府云

- 保护 Amazon Web Services (AWS) 和 Microsoft Azure 上的工作负载
- 使用集成 VPN、IPS、CFS、AV 等的高级下一代防火墙功能，保护云应用程序和云基础设施免受网络威胁
- 轻松解密加密流量并利用 TLS 1.3 支持提高安全性
- 通过实施威胁防御和分段功能确保符合监管标准
- 使用统一策略获得跨多个区域和可用区域的流量的完整可见性和控制
- 通过从 CAPEX 转向 OPEX 实现成本效益和效率
- 通过部署 NSv 防火墙保护专为美国政府机构及其客户指定的 AWS 和 Azure 云
- 保护虚拟化计算资源和监控程序，以保护 VMware ESXi、Microsoft Hyper-V、Nutanix 和 KVM 上的私有云工作负载
- 通过对虚拟机之间区内主机通信的完全可见性防止威胁
- 确保在整个虚拟环境中适当应用安全策略
- 按应用程序、用户和设备提供安全的应用程序启用规则，无论 VM 的位置如何
- 实施适当的安全性分区和隔离
- 与 Microsoft Azure Sentinel 集成，这是一种可扩展的云原生安全信息事件管理 (SIEM) 和安全编排自动响应 (SOAR) 解决方案，可加快事件响应

2. Internet Edge

- 保护公司资源免受互联网网关攻击。
- 使用先进安全功能保护 Internet Edge 免受最高级攻击并自动阻止威胁
- 通过实施威胁防御和分段功能确保符合监管标准
- 通过利用 SonicOSX 增强提高业务效率、性能并降低成本
- 分段关键 PoS（销售点）系统，确保业务连续性
- 使用统一策略获得跨多个区域和可用区域的流量的完整可见性和控制

NSv 系列系统规格

防火墙一般信息	NSv 270	NSv 470	NSv 870
操作系统	SonicOSX[11]		
支持的虚拟机监控程序	VMware ESXi v5.5/v6.0/v6.5/v6.7/v7.0/v8.0、Microsoft Hyper-V、KVM Ubuntu 16.04 / CentOS 7、Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[10]		
支持的政府云[12]	AWS 和 Azure（美国东部和西部地区）		
支持的 AWS 实例类型	c5.large c5n.large c5d.large m5.large m5n.large	c5.xlarge c5n.xlarge c5d.xlarge m5.xlarge m5n.xlarge	c5.2xlarge c5n.2xlarge c5d.2xlarge m5.2xlarge m5n.2xlarge
支持的 Azure 实例类型	Standard D2 v2 Standard_B2ms Standard_D2V4 Standard_D2ds_V4 Standard_D2s_v4	Standard D3 v2 Standard_B4ms Standard_DS3_v2 Standard_D2ds_V4	Standard D4 v2 Standard_A8_v2 Standard_F8 Standard_F8s Standard_D8_v4 Standard_D8_v3 Standard_D8s_v3
许可	BYOL、PAYG[1]		
支持的最大 vCPU	2	4	8
接口计数 (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)	8/8/8/8/8/8	8/8/8/8/8/8	8/8/8/8/8/8
最大管理/DataPlane 核心	1/1	1/3	1/7
最小内存[2]	4GB	8GB	10GB
最大内存[3]	6GB	10GB	14GB
支持的 IP/节点	无限制		
最小存储	60GB		
SSO 用户	500	10000	15000
日志记录	分析器、本地日志、Syslog		
高可用性	主动/被动[4]		

防火墙/VPN 性能[5,7]	NSv 270	NSv 470	NSv 870
防火墙检查吞吐量	6 Gbps	9 Gbps	14 Gbps
威胁防御吞吐量	1.6 Gbps	2.9 Gbps	8 Gbps
IPS 吞吐量	4 Gbps	6 Gbps	8 Gbps
TLS/SSL DPI 吞吐量	800 Mbps	2 Gbps	4 Gbps
VPN 吞吐量[8]	1.4 Gbps	3.5 Gbps	8 Gbps
每秒连接数	13760	37270	75640
最大连接数 (SPI)	225000	1.5M	3M
最大连接数 (DPI)	125000	1.5M	2M
TLS/SSL DPI 连接数	8000	20000	30000
VPN	**NSv 270**	**NSv 470**	**NSv 870**
站点到站点 VPN 隧道	75	6000	10000
IPSec VPN 客户端[13] （最大）	50(1000)	2000(4000)	2000(6000)
包括 SSL VPN 客户端[6]	2	2	2
SSL VPN 客户端最大数量[6]	100	200	300
加密/身份验证	DES、3DES、AES（128、192、256 位）/MD5、SHA-1、Suite B、通用访问卡 (CAC)		
密钥交换	Diffie Hellman 组 1、2、5、14v		
基于路由的 VPN	RIP、OSPF、BGP		
联网	**NSv 270**	**NSv 470**	**NSv 870**
IP 地址分配	静态、DHCP、内部 DHCP 服务器[9]、DHCP 中继[9]		
NAT 模式	一对一、多对一、一对多、灵活的 NAT（重叠 IP）、PAT		
逻辑 VLAN 和隧道接口（最大）[7]	128	128	128
路由协议	BGP、OSPF、RIPv1/v2、静态路由、基于策略的路由		
QoS	带宽优先级、最大带宽、有保障带宽、DSCP 标记、802.1p		
身份验证	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部用户数据库、终端服务、Citrix		
本地用户数据库	250	2500	3200

[1]PAYG 目前仅在 AWS 上可用

[2]禁用巨型帧的内存。

[3]启用巨型帧的内存。巨型帧需要额外的内存。Azure 和 AWS 不支持巨型帧。

[4]在 VMware ESXi 平台、KVM、Azure、Microsoft Hyper-V 和 Nutanix 上提供高可用性。NSv 270 通过使用 D3v2 VM 大小支持 HA。AWS 上不支持高可用性。Azure 上的高可用性要求服务器大小支持三个或更多接口。

[5]发布的性能数据符合规格，实际性能可能会因基础硬件、网络条件、防火墙配置和已激活的服务而异。性能和容量也可能会因基础虚拟化基础设施而异，我们建议在您的环境中进行其他测试，以确保满足您的性能和容量要求。使用运行带有 VMware vSphere 7.0 的 SonicOS 7.0.1 的 Intel Xeon 处理器（Platinum 8268 @2.9GHz、3.9GHz Turbo、37.5M 缓存）观察到的性能指标

[6]可用于 MSSP 计划的 SSL VPN 客户端在 NSv 270 上为 50 个，在 NSv 470 上为 75 个。增加的 SSL VPN 编号仅可从 SonicOS 6.5.4.4-44v-21-723 固件及更高版本获得。

[7]Azure 和 AWS 上不支持 VLAN 接口。

测试方法：基于 RFC 2544 的最大性能（用于防火墙）。使用行业标准的 Keysight HTTP 性能测试工具对威胁防御/网关 AV/反间谍软件/IPS 吞吐量进行测量。通过多个端口对使用多个流量进行测试。通过由默认防火墙设置启用的网关 AV、反间谍软件、IPS 和应用程序控制对威胁防御吞吐量进行测量。根据 RFC 2544，使用 1418 字节数据包大小的 AESGMAC16-256 加密 UDP 流量对 VPN 吞吐量进行测量。所有规格、功能和可用性均可能随时更改。

[8]所有性能参数均使用带 SR-IOV 和 Turbo boost 的 Dell R740 进行测试。

[9]在私有云上受支持，在公共云平台上不受支持。

[10]运行 SonicOSX 7.0.0 及更高版本固件的 SonicWall NSv 270/470/870 支持 Nutanix AHV。

[11]SonicOSX 7.0.1 及更高版本的用户将能够在经典/全局和策略模式之间进行选择和切换。

[12]政府云只能通过 BYOL 提供

[13]可用于 MSSP 计划的 GVC 客户端在 NSv 270 上为 25 个，在 NSv 470 上为 50 个

SonicOSX 7.0 功能摘要

防火墙

- 有状态数据包检查
- 免重组深度数据包检查
- DDoS 攻击防护（UDP/ICMP/SYN 泛洪攻击）
- IPv4/IPv6 支持
- 面向远程访问的生物身份验证
- DNS 代理
- REST API
- SonicWall 交换机集成[1]
- SonicWall Wi-Fi 6 AP 集成
- 基于信誉的内容过滤服务 (CFS 5.0)
- DNS 过滤
- SD-WAN
  - SD-WAN 可扩展性
  - SD-WAN 可用性向导
- API
  - 全面 API 支持
- 多租户[3]
  - 多租户支持
  - 租户视图和每个租户的固件支持
- 在经典/全局和策略模式之间切换[4]

统一策略

- 统一策略整合了第 3 层到第 7 层的规则：
  - 来源/目标 IP/端口/服务
  - 应用程序控制
  - CFS/Web 僵尸网络/Geo-IP
  - 规则图
  - 单通道安全服务强制实施 – IPS/GAV/AS/Capture ATP
  - 用于端点安全/BWM/QoS/CFS/入侵防御的基于配置文件的对象
- 安全/DoS 规则的操作配置文件
- 规则管理：
  - 克隆
  - 影子规则分析
  - 单元格内编辑
  - 规则导出
  - 群组编辑
- 管理视图
  - 已使用/未使用的规则
  - 活动/活动中的规则
  - 分区/自定义分组
  - 可定制网格/布局

TLS/SSL/SSH 解密和检查

- TLS 1.3
- 支持具有增强安全性的 TLS 1.3
- 针对 TLS/SSL/SSH 的深度数据包检查
- 包含/排除对象、群组或主机名
- SSL 控制
- 按区域或规则精细控制 DPI-SSL

Capture 高级威胁防护[2]

- Real-Time Deep Memory Inspection
- 云端多引擎分析
- 虚拟化沙箱
- 虚拟机监控程序级分析
- 全系统模拟
- 广泛的文件类型检查
- 自动和手动提交
- 实时威胁情报更新
- 在裁决前进行阻止
- Capture Client

入侵防御[2]

- 基于签名的扫描
- 网络访问控制与 Aruba ClearPass 集成
- 自动签名更新
- 双向检查引擎
- 精细的 IPS 规则功能
- GeoIP 强制实施
- 利用动态列表过滤僵尸网络
- 正则表达式匹配

反恶意软件[2]

- 基于数据流的恶意软件扫描
- 网关防病毒
- 网关反间谍软件
- 双向检查
- 不限制文件大小
- 云端恶意软件数据库

应用程序识别[2]

- 应用程序控制
- 应用程序带宽管理
- 创建定制的应用程序签名
- 防止数据泄露
- 通过 NetFlow/IPFIX 进行应用程序报告
- 综合式应用程序签名数据库

流量可视化和分析

- 用户活动
- 应用程序/带宽/威胁使用情况
- 云端分析

HTTP/HTTPS Web 内容过滤[2]

- URL 过滤
- 代理规避
- 关键字拦截
- 基于信誉的内容过滤服务 (CFS 5.0)
- DNS 过滤
- 基于策略的过滤（排除/包含）
- HTTP 标头插入
- 带宽管理 CFS 评级类别
- 带有应用程序控制的统一策略模型
- 内容过滤客户端

VPN

- 安全 SD-WAN
- 自动配置 VPN
- 用于站点到站点连接的 IPSec VPN
- SSL VPN 和 IPSec 客户端远程访问
- 冗余的 VPN 网关
- Mobile Connect for iOS、Mac OS X、Windows、Chrome、Android 和 Kindle Fire
- 基于路由的 VPN (RIP/OSPF/BGP)

增强仪表板

- 增强设备视图
- 顶级流量和用户摘要
- 对威胁的洞察
- 通知中心
- 增强数据包监控
- UI 上的 SSH 终端
- 新设计/模板
- 行业与全球平均值比较

联网

- PortShield[1]
- 巨型帧
- 路径 MTU 发现
- 增强日志记录
- VLAN 中继
- 端口镜像（NSa 2650 及更高版本）
- 第 2 层 QoS
- 端口安全
- 动态路由 (RIP/OSPF/BGP)
- SonicWall 无线控制器[1]
- 基于策略的路由（ToS/metric 和 ECMP）
- NAT
- DHCP 服务器
- 带宽管理
- 链路聚合[1]（静态和动态）
- 端口冗余性[1]
- 主动/被动 (A/P) 高可用性（包括状态同步）
- A/A 集群[1]
- 入站/出站负载平衡
- L2 桥接、[1]有线/虚拟有线模式、分接模式、NAT 模式
- 3G/4G WAN 故障转移[1]
- 非对称路由
- 通用访问卡 (CAC) 支持
- SonicCoreX 和 SonicOS 容器化

解密策略

- SSL/TLS 流量的统一策略

DoS 策略

- DoS/DDoS 攻击防御的统一策略

VoIP

- 精细 QoS 控制
- 带宽管理
- 用于 VoIP 流量的 DPI
- H.323 Gatekeeper 和 SIP 代理支持

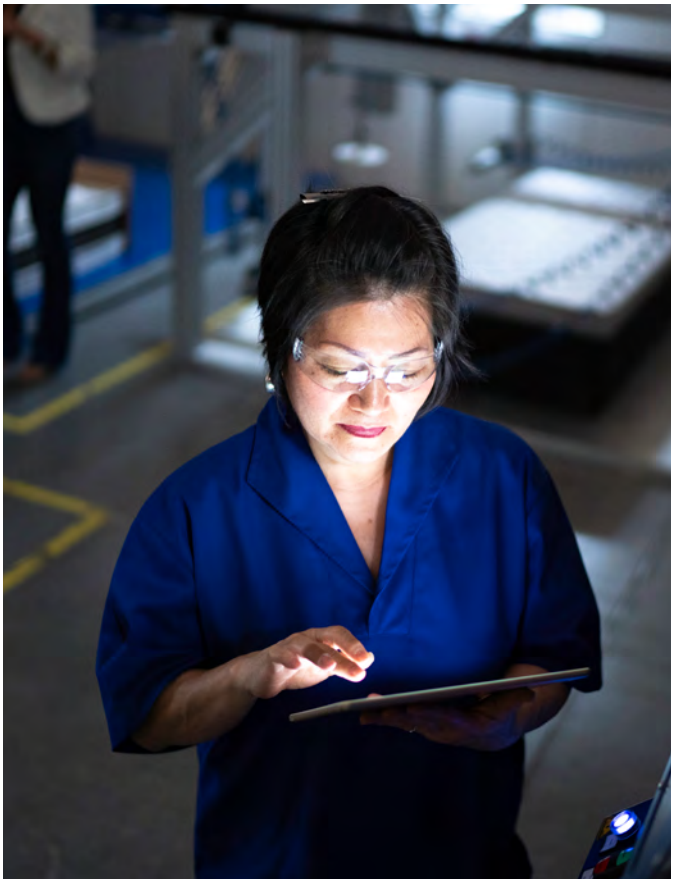
管理和监控

- Web 图形用户界面
- 命令行界面 (CLI)
- 零接触注册与配置
- SonicExpress 移动应用程序支持
- SNMPv2/v3
- 利用 Network Security Manager (NSM)[2] 进行集中化管理和报告
- 日志记录
- Netflow/IPFix 导出
- 云端配置备份
- 应用程序和带宽可视化工具
- IPv4 和 IPv6 管理
- 机外报告 (Scrutinizer)
- LCD 管理屏幕[1]
- Dell N 系列和 X 系列交换机管理，包括级联交换机[1]
- Network Security Manager 报告

无线[1]

- SonicWave AP 云和防火墙管理
- WIDS/WIPS
- 恶意 AP 预防
- 快速漫游 (802.11k/r/v)
- 802.11s 网状网络
- 自动信道选择
- RF 频谱分析
- 楼层平面图
- 拓扑视图
- 频段引导
- 波束赋形
- 无线传输公平性
- 低功耗蓝牙技术
- MiFi 扩展器
- 访客循环配额
- LHM 访客门户

[1] NSv 系列防火墙对此不提供支持
[2] 需要额外订阅
[3] 仅在 NSsp 防火墙上可用
[4] 在 SonicOSX 7.0.1 及更高版本上可用



合作伙伴支持服务

需要帮助规划、部署或优化 SonicWall 解决方案吗？SonicWall 高级服务合作伙伴接受过培训，可为您提供世界一流的专业服务。了解更多：

www.sonicwall.com/PES

深入了解 SonicWall NSv 270/470/870 系列

www.sonicwall.com/NSv

关于 SonicWall

SonicWall 为超分布式时代和每个人都远程办公、每个人都移动办公、每个人都不太安全的工作现实提供了稳定、可扩展、无缝的网络安全。通过了解未知、提供实时可见性并实现经济学突破，SonicWall 为世界各地的大型企业、政府和中小企业弥补了网络安全业务缺口。有关详情，请访问www.sonicwall.com。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有关详情，请访问我们的网站。
www.sonicwall.com