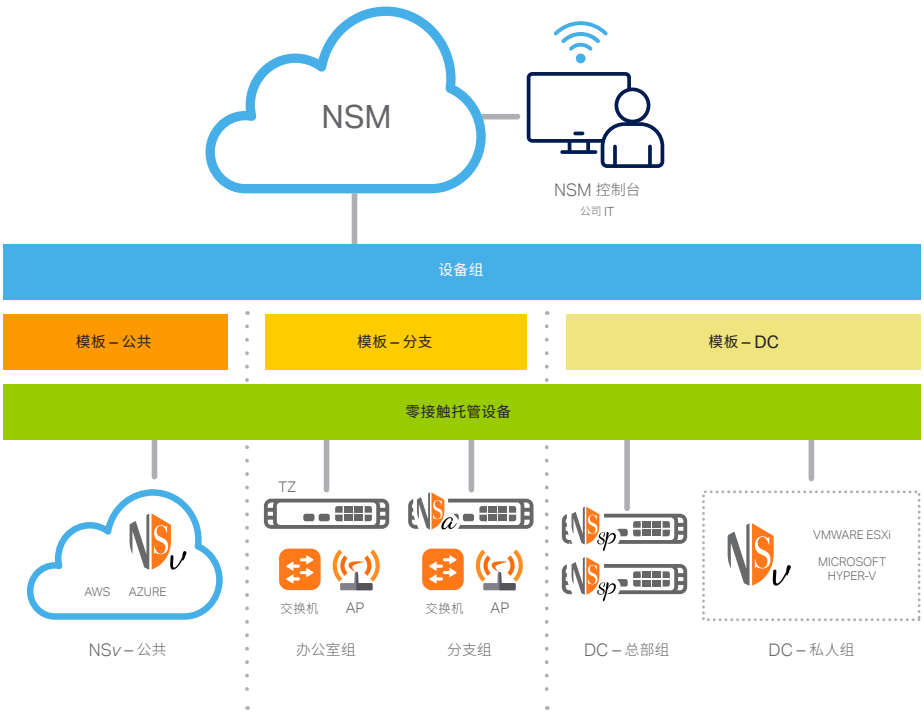
SONICWALL

Network Security Manager

适用于任何环境的统一防火墙管理系统

无论您是要保护小型企业、分布式企业还是多个企业，网络安全都可能会因为运营混乱、隐藏风险和监管要求而变得不堪重负。从以往情况来看，良好的防火墙管理实践主要依赖于稳健而可靠的系统及运营控制措施。然而，对于运营良好的安全运营中心 (SOC) 而言，常见错误、配置错误甚至可能出现违反这些控制措施的情况仍然持续带来挑战。

SonicWall Network Security Manager (NSM) 是一个多租户集中化防火墙管理器，支持通过遵守可审核的工作流程，集中管理所有防火墙操作，避免出现错误。其原生分析引擎提供单一管理平台可见性，支持通过统一和关联所有防火墙的日志，监控和发现威胁。NSM 还提供对每个配置更改和精细报告的完整审核跟踪，从而帮助您保持合规。NSM 可扩展至任何规模的组织，以管理部署在多个地点的成千上万台防火墙设备的网络，只需投入极少的精力和时间即可完成所有工作。



好处：

企业业务

- 减少安全管理开销
- 了解威胁形势和安全态势
- 使用 SaaS 减少资本支出

业务运营

- 无需部署硬件/软件
- 消除防火墙管理孤岛
- 轻松地远程安装任意数量的防火墙
- 了解所有安全操作

安全

- 跨所有环境审核、确认和强制实施一致的安全策略
- 迅速发现问题和风险并做出响应
- 做出明智的安全策略决定

掌控一切：从一个位置编排防火墙操作

NSM 为您提供统一防火墙管理系统所需的一切。它赋予您租户级别可见性、基于组的设备控制和无限制扩展，以集中管理和配置 SonicWall 网络安全操作。这包括部署和管理所有防火墙设备、设备组和租户；通过灵活的本地控制，在您的环境中同步并执行一致的安全策略，以及从一个动态仪表板监控所有内容，并提供详细的报告和分析。NSM 使您能够通过一个对用户友好的云原生控制台完成所有这些工作，该控制台可以使用任何支持浏览器的设备从任何位置访问。

多租户管理

当您的防火墙环境随着复杂的多重云和多地点租户的增长而增长，而这些租户对每个网络分段都有不同的安全需求时，您将需要一个能够与该环境一起扩展的防火墙管理系统。NSM 可以跨所有托管租户提供全面的多租户管理和独立策略控制隔离。这种隔离涵盖为每个租户指示防火墙操作的所有 NSM 管理特性和功能。您可以针对每个租户进行构建，使其拥有自己的用户、组和角色集，以便在所分配的租户帐户边界内执行设备组管理、策略编排和所有其他管理任务。

设备组管理

设备组为您提供了一种有效的方法，用于以组或分层组的形式创建和管理防火墙设备，以及在防火墙组上确认和部署配置模板。这允许您以一致且可靠的方式在任何选定的防火墙组之间同步并强制实施公共策略、对象和/或设置要求。模板中所有经过批准的策略变更将自动应用于与该模板链接的所有设备组。设备分组可以根据任何特征（例如，网络类型、位置、业务单位、组织结构或相关属性的组合）进行精细定义，以便于管理、识别和关联。

模板管理、确认和部署

NSM 简化了工作流程，使您可以轻松快速地设计、验证、审核和确认配置模板，以便跨多个地理位置管理一个或数千个防火墙设备。具有各种防火墙策略、设置和相关对象的模板将独立于设备进行定义，然后由 NSM 以集中方式自动推送到需要类似配置的设备或设备组。

运作效率更高：更智能地工作、更快地采取安全措施，一切都轻而易举

NSM 是一个可以提高工作效率的管理工具，让您能够更智能地工作、更快地采取安全措施，一切都轻而易举。它的设计以业务流程为指导，秉承简化的原则，在某些情况下自动执行工作流程，以实现更好的安全协调，同时减少执行日常安全操作和管理任务的复杂性、时间和开销。

轻松零接触部署

零接触部署服务集成到 NSM 中，使您可以轻松地在远程和分支机构办公地点部署和操作 SonicWall 防火墙、交换机和接入点。整个过程只需极少的用户干预，并且是完全自动化的。采用零接触的设备直接运送到安装地点。打开包装、注册、连接到网络并通电后，所有连接的设备均可立即运行，安全性和连接性可顺畅实现。与 NSM 建立通信链接后，预配置设备模板将自动推送到所有采用零接触的设备。这样做可以避免执行耗费时间、成本高昂、操作复杂的传统现场安装流程。

无差错变更管理

NSM 提供对功能强大的自动化工作流程的即时访问，这些工作流程符合 SOC 的防火墙策略变更管理和审核要求。在部署之前应用一系列严格的程序来配置、比较、验证、审查和批准防火墙策略，进而实现无差错的策略变更。审批团队非常灵活，能够遵守来自不同类型组织的不同授权和审核程序。NSM 以编程方式部署经过全面验证和审核的安全策略，以提高运营效率、降低风险并消除配置错误和人为错误。

使用 RESTful API 实现管理自动化

NSM RESTful API 为技能熟练的安全操作员提供了一种标准的方法，可以在没有管理 Web 界面的情况下，以编程方式管理 NSM 特定的功能。它促进了 NSM 和第三方管理控制台之间的互操作性，可提高您的内部安全团队的效率。API 服务用于自动执行任何托管设备的防火墙操作。其中包括常见的日常任务，例如租户、设备组和租户管理、审核配置、执行系统运行状况检查等。

增强意识：通过主动监控、报告和分析来调查隐藏风险

NSM 交互式仪表板加载了实时监控、报告和分析数据，可帮助解决问题、调查风险并指导做出明智的安全策略决定和策略行动，以实现更强大的适应性安全态势。

随时随地洞察一切

NSM 报告、分析和风险监控仪表板可在租户、组或设备级别让您长达 7 天 360 度全方位监视整个 SonicWall 安全生态系统。它对通过防火墙生态系统的所有网络流量和数据通信提供静态和接近实时的分析。所有日志数据都会自动记录、汇总、场景化，并以有意义、可操作且易于使用的方式呈现，让您能够根据数据驱动的洞察和情境感知发现、解读、确定优先顺序并采取适当的防御和纠正措施。计划的报告支持使用任意组合的可审核数据完全自定义报告。可在设备级别提供长达 365 天的记录日志，以进行历史分析、异常检测、安全缺口发现等。这将帮助您跟踪、测量和运行有效的网络和安全操作。

了解您的风险

借助增加的向下钻取和透视功能，您可以进一步调查并关联数据，从而更准确和更有信心地全面检查和发现隐藏的威胁和问题。结合使用历史记录报告、基于用户和基于应用程序的分析以及端点可见性，您可以全面分析与入口/出口流量、应用程序使用、用户和设备访问、威胁行为等相关的各种模式和趋势。您将获得情境感知和有价值的洞察和知识，不仅可以发现安全风险，还可以编排补救措施，同时监控和跟踪结果，以促进和推动整个环境中一致的安全强制实施。

功能摘要

管理

- 租户及设备组级别管理
- 配置模板
- 设备分组
- 确认和部署向导
- 配置审核
- 配置 – 差异
- 离线管理和计划
- 安全防火墙策略的管理
- 安全 VPN 策略的管理
- 软件定义的广域网 (SD-WAN) 的管理
- 增值安全服务的管理
- 冗余和高可用性
- 防火墙设备的首选项文件备份
- RESTful API
- 固件升级
- 基于角色的管理
- 接入点和交换机管理

监控

- 设备运行状况和状态
- 许可证和支持状态
- 网络/威胁摘要
- 警报和通知中心
- 事件日志
- 拓扑视图

分析

- 基于用户的活动
- 应用程序使用
- 利用 Capture Client 实现跨产品可见性
- 实时动态可视化
- 向下钻取和透视功能

报告

- 计划的 PDF 报告 – 租户/组/设备级别
- 可自定义的报告
- 集中式日志记录
- 多威胁报告
- 以用户为中心的报告
- 应用程序使用报告
- 带宽和服务报告
- 每个用户带宽报告

许可和包装

功能特性	基础版	高级版
每个租户管理数百台设备	是	是
多租户管理	是	是
设备清单	是	是
在组级别推动策略	是	是
设备组	是	是
模板	是	是
确认与部署	是	是
配置审核	是	是
配置差异	是	是
工作流程自动化	是	是
API	是	是
零接触部署	是	是
任务计划	是	是

功能特性	基础版	高级版
备份/还原	是	是
固件升级	是	是
接入点和交换机管理	是	是
报告数据天数	7 天	365 天
组/租户级别仪表板	是	是
Capture ATP（设备级别）	是	是
捕获威胁评估（设备级别）	是	是
组级别可见性和报告	是	是
计划的报告（设备组级别）	是	是
基于用户的分析	否	是
应用程序分析	否	是
威胁分析	否	是
向下钻取和透视	否	是

产品	SKU
NSM ESSENTIAL FOR SOHO 250 1 年	02-SSC-5219
NSM ADVANCED FOR SOHO 250 1 年	02-SSC-5213
NSM ESSENTIAL FOR TZ 350 1 年	02-SSC-5239
NSM ADVANCED FOR TZ 350 1 年	02-SSC-5231
NSM ESSENTIAL FOR TZ 400 1 年	02-SSC-5263
NSM ADVANCED FOR TZ 400 1 年	02-SSC-5257
NSM ESSENTIAL FOR TZ 500 1 年	02-SSC-5183
NSM ADVANCED FOR TZ 500 1 年	02-SSC-5177
NSM ESSENTIAL FOR TZ 570 1 年	02-SSC-4975
NSM ADVANCED FOR TZ 570 1 年	02-SSC-4963
NSM ESSENTIAL FOR TZ 600 1 年	02-SSC-5201
NSM ADVANCED FOR TZ 600 1 年	02-SSC-5195
NSM ESSENTIAL FOR TZ 670 1 年	02-SSC-5011
NSM ADVANCED FOR TZ 670 1 年	02-SSC-4999
NSM ESSENTIAL FOR NS*a* 2600/NS*a* 2650 1 年	02-SSC-5281
NSM ADVANCED FOR NS*a* 2600/NS*a* 2650 1 年	02-SSC-5275
NSM ESSENTIAL FOR NS*a* 3600/NS*a* 3650 1 年	02-SSC-5299
NSM ADVANCED FOR NS*a* 3600/NS*a* 3650 1 年	02-SSC-5293
NSM ESSENTIAL FOR NS*a* 4600/NS*a* 4650 1 年	02-SSC-5325
NSM ADVANCED FOR NS*a* 4600/NS*a* 4650 1 年	02-SSC-5319
NSM ESSENTIAL FOR NS*a* 5600/NS*a* 5650 1 年	02-SSC-5347
NSM ADVANCED FOR NS*a* 5600/NS*a* 5650 1 年	02-SSC-5341
NSM ESSENTIAL FOR NS*a* 6600/NS*a* 6650 1 年	02-SSC-5365
NSM ADVANCED FOR NS*a* 6600/NS*a* 6650 1 年	02-SSC-5359

还提供多年 SKU 和支持合同。有关完整列表，请联系您的首选经销商或 SonicWall 销售部门。

互联网浏览器

- Microsoft® Internet Explorer 11.0 或更高版本，以及 Microsoft Edge、Mozilla Firefox、Google Chrome 和 Safari 的最新版本。

NSM 的托管设备[1]

- SonicWall 网络安全设备：SuperMassive 9000 系列[2]、E-Class NSA、NS*sp* 12000 系列[2]、NS*a* 系列、TZ 系列、SOHO-W、SOHO 250、SOHO 250W
- SonicWall Network Security Virtual 设备：NSv 系列
- SonicWall SonicWave、SonicPoint
- SonicWall 交换机

[1] 支持运行 SonicOS 6.x 或 7.x 版本的防火墙。
[2] 不支持 365 天报告和 30 天分析。

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 Boundless Cybersecurity。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

Datasheet-NSM-US-COG-2114