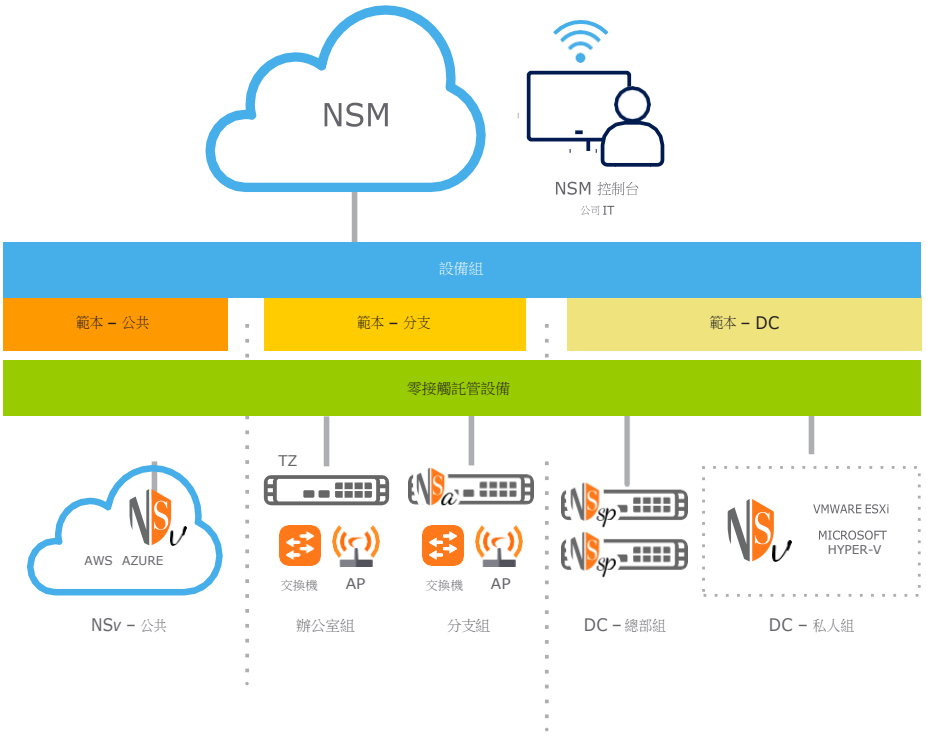
SONICWALL

Network Security Manager

適用於任何環境的防火牆管理系統

無論您是要保護小型企業、分散式企業還是多個企業，網路安全都可能會因為運營混亂、隱藏風險和監管要求而變得不堪重負。從以往情況來看，良好的防火牆管理實踐主要依賴於穩健而可靠的系統及運營控制措施。然而，對於運營良好的安全運營中心 (SOC) 而言，常見錯誤、配置錯誤甚至可能出現違反這些控制措施的情況仍然持續帶來挑戰。

SonicWall Network Security Manager (NSM) 是一個多租戶集中化防火牆管理器，支持通過遵守可審核的工作流程，集中管理所有防火牆操作，避免出現錯誤。其原生分析引擎提供單一管理平台可視性，支持通過統一和關聯所有防火牆的日誌，監控和發現威脅。NSM 還提供對每個配置更改和精細報告的完整審核跟蹤，從而幫助您保持合規。NSM 可擴展至任何規模的組織，以管理部署在多個地點的成千上萬台防火牆設備的網路，只需投入極少的精力和時間即可完成所有工作。



好處：

企業業務

- 減少安全管理開銷
- 瞭解威脅形勢和安全態勢
- 使用 SaaS 減少資本支出

業務運營

- 無需部署硬體/軟體
- 消除防火牆管理孤島
- 輕鬆地遠端安裝任意數量的防火牆
- 瞭解所有安全操作

安全

- 跨所有環境審核、確認和強制實施一致的安全性原則
- 迅速發現問題和風險並做出回應
- 做出明智的安全性原則決定

掌控一切：從一個位置編排防火牆操作

NSM 為您提供統一防火牆管理系統所需的一切。它賦予您租戶級別可見性、基於組的設備控制和無限制擴展，以集中管理和配置 SonicWall 網路安全操作。這包括部署和管理所有防火牆設備、設備組和租戶；通過靈活的本地控制，在您的環境中同步並執行一致的安全性原則，以及從一個動態儀錶板監控所有內容，並提供詳細的報告和分
析。NSM 使您能夠通過一個對用戶友好的雲原生控制台完成所有這些工作，該控制台可以使用任何支援流覽器的設備從任何位置訪問。

多租戶管理

當您的防火牆環境隨著複雜的多重雲和多地點租戶的增長而增長，而這些租戶對每個網路分段都有不同的安全需求時，您將需要一個能夠與該環境一起擴展的防火牆管理系統。NSM 可以跨所有託管租戶提供全面的多租戶管理和獨立策略控制隔離。這種隔離涵蓋為每個租戶指示防火牆操作的所有 NSM 管理特性和功能。您可以針對每個租戶進行構建，使其擁有自己的用戶、組和角色集，以便在所分配的租戶帳戶邊界內執行設備組管理、策略編排和所有其他管理任務。

設備組管理

設備組為您提供了一種有效的方法，用於以組或分層組的形式創建和管理防火牆設備，以及在防火牆組上確認和部署配置範本。這允許您以一致且可靠的方式在任何選定的防火牆組之間同步並強制實施公共策略、對象和/或設置要求。範本中所有經過批准的策略變更將自動應用於與該範本連結的所有設備組。設備分組可以根據任何特徵（例如，網路類型、位置、業務單位、組織結構或相關屬性的組合）進行精細定義，以便於管理、識別和關聯。

範本管理、確認和部署

NSM 簡化了工作流程，使您可以輕鬆快速地設計、驗證、審核和確認配置範本，以便跨多個地理位置管理一個或數千個防火牆設備。具有各種防火牆策略、設置和相關物件的範本將獨立于設備進行定義，然後由 NSM 以集中方式自動推送到需要類似配置的設備或設備組。

運作效率更高：更智慧地工作、更快地採取安全措施，一切都輕而易舉

NSM 是一個可以提高工作效率的管理工具，讓您能夠更智慧地工作、更快地採取安全措施，一切都輕而易舉。它的設計以業務流程為指導，秉承簡化的原則，在某些情況下自動執行工作流程，以實現更好的安全協調，同時減少執行日常安全操作和管理任務的複雜性、時間和開銷。

輕鬆零接觸部署

零接觸部署服務集成到 NSM 中，使您可以輕鬆地在遠端和分支機構辦公地點部署和操作 SonicWall 防火牆、交換機和接入點。整個過程只需極少的用戶干預，並且是完全自動化的。採用零接觸的設備直接運送到安裝地點。打開包裝、註冊、連接到網路並通電後，所有連接的設備均可立即運行，安全性和連線性可順暢實現。與 NSM 建立通訊連結後，預配置設備範本將自動推送到所有採用零接觸的設備。這樣做可以避免執行耗費時間、成本高昂、操作複雜的傳統現場安裝流程。

無差錯變更管理

NSM 提供對功能強大的自動化工作流程的即時訪問，這些工作流程符合 SOC 的防火牆策略變更管理和審核要求。在部署之前應用一系列嚴格的程式來配置、比較、驗證、審查和批准防火牆策略，進而實現無差錯的策略變更。審批團隊非常靈活，能夠遵守來自不同類型組織的不同授權和審核程序。NSM 以程式設計方式部署經過全面驗證和審核的安全性原則，以提高運營效率、降低風險並消除配置錯誤和人為錯誤。

使用 RESTful API 實現管理自動化

NSM RESTful API 為技能熟練的安全操作員提供了一種標準的方法，可以在沒有管理 Web 介面的情況下，以程式設計方式管理NSM 特定的功能。它促進了 NSM 和協力廠商管理主控台之間的互通性，可提高您的內部安全團隊的效率。API 服務用於自動執行任何託管設備的防火牆操作。其中包括常見的日常任務，例如租戶、設備組和租戶管理、審核配置、執行系統運行狀況檢查等。

增強意識：通過主動監控、報告和分析來調查隱藏風險

NSM 互動式儀錶板載入了即時監控、報告和分析資料，可說明解決問題、調查風險並指導做出明智的安全性原則決定和策略行動， 以實現更強大的適應性安全態勢。

隨時隨地洞察一切

NSM 報告、分析和風險監控儀錶板可在租戶、組或設備級別讓您長達 7 天 360 度全方位監視整個 SonicWall 安全生態系統。它對通過防火牆生態系統的所有網路流量和資料通信提供靜態和接近即時的分析。所有日誌資料都會自動記錄、匯總、場景化，並以有意義、可操作且易於使用的方式呈現，讓您能夠根據資料驅動的洞察和情境感知發現、解讀、確定優先順序並採取適當的防禦和糾正措施。計畫的報告支援使用任意組合的可審核資料完全自訂報告。可在設備級別提供長達 365 天的記錄日誌，以進行歷史分析、異常檢測、安全缺口發現等。這將說明您跟蹤、測量和運行有效的網路和安全操作。

瞭解您的風險

借助增加的向下鑽取和透視功能，您可以進一步調查並關聯資料，從而更準確和更有信心地全面檢查和發現隱藏的威脅和問題。結合使用歷史記錄報告、基於使用者和基於應用程式的分析以及端點可見性，您可以全面分
析與入口/出口流量、應用程式使用、使用者和設備訪問、威脅行為等相關的各種模式和趨勢。您將獲得情境感知和有價值的洞察和知識，不僅可以發現安全風險，還可以編排補救措施，同時監控和跟蹤結果，以促進和推動整個環境中一致的安全強制實施。

功能摘要

管理

- 租戶及設備組級別管理
- 配置範本
- 設備分組
- 確認和部署嚮導
- 配置審核
- 配置 – 差異
- 離線管理和計畫
- 安全防火牆策略的管理
- 安全 VPN 策略的管理
- 軟體定義的廣域網路 (SD-WAN) 的管理
- 增值安全服務的管理
- 冗餘和高可用性
- 防火牆設備的首選項檔案備份
- RESTful API
- 韌體升級
- 基於角色的管理
- 接入點和交換機管理

監控

- 設備運行狀況和狀態
- 許可證和支援狀態
- 網路/威脅摘要
- 警報和通知中心
- 事件日誌
- 拓撲視圖

分析

- 基於用戶的活動
- 應用程式使用
- 利用 Capture Client 實現跨產品可見性
- 即時動態視覺化
- 向下鑽取和透視功能

報告

- 計畫的 PDF 報告 – 租戶/組/設備級別
- 可自訂的報告
- 集中式日誌記錄
- 多威脅報告
- 以用戶為中心的報告
- 應用程式使用報告
- 頻寬和服務報告
- 每個用戶頻寬報告

許可和包裝

功能特性	基礎版	高級版
每個租戶管理數百台設備	是	是
多租戶管理	是	是
設備清單	是	是
在組級別推動策略	是	是
設備組	是	是
範本	是	是
確認與部署	是	是
配置審核	是	是
配置差異	是	是
工作流程自動化	是	是
API	是	是
零接觸部署	是	是
任務計畫	是	是

功能特性	基礎版	高級版
備份/還原	是	是
韌體升級	是	是
接入點和交換機管理	是	是
報告資料天數	7 天	365 天
組/租戶級別儀錶板	是	是
Capture ATP（設備級別）	是	是
捕獲威脅評估（設備級別）	是	是
組級別可見性和報告	是	是
計畫的報告（設備組級別）	是	是
基於用戶的分析	否	是
應用程式分析	否	是
威脅分析	否	是
向下鑽取和透視	否	是

產品	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

互聯網流覽器

- 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 On-Prem 系統需求

- 支援虛擬系統：ESXi 7.0, 6.7, 6.5 and Hyper-V 2016, 2019
- 虛擬系統資源：4 vCPUs, 16GB記憶體 , 250GB 儲存空間

[1] 支援運行 SonicOS 6.x 或 7.x 版本的防火牆。
[2] 不支持 365 天報告和 30 天分析。

NSM 的託管設備[1]

- SonicWall 網路安全設備：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 設備：NS*v* 系列
- SonicWall SonicWave、SonicPoint
- SonicWall 交換機

關於 SonicWall

SonicWall 為超分散式時代和每個人都遠端辦公、每個人都移動辦公、每個人都不太安全的工作現實提供了 Boundless Cybersecurity。通過瞭解未知、提供即時可見性並實現經濟學突破，SonicWall 為世界各地的大型企業、政府和中小企業彌補了網路安全業務缺口。有關詳情，請訪問 www.sonicwall.com。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有關詳情，請訪問我們的網站。
www.sonicwall.com

 Datasheet-NSM-US-COG-2114

SONICWALL®