NSv 270/470/870

SonicWall Network Security virtual NSv 270/470/870 防火牆，提供企業級安全、簡化管理、完全可見性、靈活部署，同時為虛擬工作負載提供卓越性能。

虛擬環境中經常發現新漏洞，這些漏洞會產生嚴重的安全隱患和挑戰。但是，保護所有這些安全向量還需要能始終將正確的安全性原則應用於正確的網路控制點，因為一些安全故障可能是由無效策略或錯誤配置所導致。

特點

公共雲和私有雲安全

- 具有自動即時漏洞檢測和預防功能的下一代防火牆
- 正在申請專利的 Real-Time Deep Memory Inspection (RTDMI) 技術
- 獲得專利的免重組深度包檢測 (RFDPI) 技術
- 通過統一策略實現完整的端到端可見性和簡化管理
- 應用程式智慧與控制
- 分段安全性和安全性分區
- 跨私有雲 (ESXi、Hyper-V、KVM、Nutanix) 和公共雲 (AWS、Azure) 平台支援

虛擬機器保護

- 數據保密性
- 防止資料外洩的安全通信
- 流量驗證、檢查和監控
- 虛擬網路彈性和可用性
- SonicOSX 7.0

查找適合您企業的 SonicWall 解決方案：

sonicwall.com/NSv

DATASHEET

NSv 防火牆系列可以說明安全團隊減少這類安全風險和漏洞，這些安全風險和漏洞會嚴重干擾您的關鍵業務服務和營運。它使企業能夠控制通過防火牆的動態流量，並提供對不同策略的可見性和洞察力。還能說明簡化管理任務、減少配置錯誤並加快部署時間，所有這些都有助於改善整體安全狀況。

SonicOSX 和安全服務

SonicOSX 架構是 NSv 240/470/870 防火牆的核心。它由功能豐富的 SonicOSX 7.0 作業系統驅動，具有設計現代化的全新使用者介面與使用者體驗 (UX/UI)、高級安全性、聯網和管理功能。

SonicOSX 7.0 從頭開始構建，具有統一策略，可提供對各種安全策略的集成管理。在每個防火牆的單個規則庫中輕鬆配置第 3 層到第 7 層控制，為配置策略提供一個集中位置。新網路介面呈現實用的威脅資訊視覺化，並顯示可操作的警報，提示您通過簡單的點擊操作來配置上下文安全性原則。

NSv 進一步集成 SD-WAN、TLS 1.3 支持、即時視覺化、高速虛擬私人網路 (VPN) 以及其他強大的安全功能。未知威脅會被發送到 SonicWall 基於雲的 Capture Advanced Threat Protection (ATP) 多引擎沙箱進行分析。增強 Capture ATP 是我們正在申請專利的 Real-Time Deep Memory Inspection (RTDMI™) 技術。作為 Capture ATP 的引擎之一，RTDMI 通過直接在記憶體中進行檢查來探測並阻止惡意軟體和零時差攻擊。

通過利用採用 RTDMI 技術的 Capture ATP，除了高級安全服務以外，NSv 系列防火牆還可以在閘道處阻止惡意軟體、勒索軟體和其他高級威脅。

部署

1. Cloud Edge 和資料中心安全公共雲

- 保護 Amazon Web Services (AWS) 和 Microsoft Azure 上的工作負載
- 使用集成 VPN、IPS、CFS、AV 等的高級下一代防火牆功能，保護雲應用程式和雲基礎設施免受網路威脅
- 輕鬆解密/加密流量並利用 TLS 1.3 支持提高安全性
- 通過實施威脅防禦和分段功能確保符合監管標準
- 適當擴展和調整您的基礎設施規模
- 使用統一策略獲得跨多個區域和可用區域的流量的完整可見性和控制
- 通過從 CAPEX 轉向 OPEX 實現成本效益和效率
- 安全私有雲
- 保護虛擬化計算資源和監控程序，以保護 VMware ESXi、Microsoft Hyper-V、Nutanix 和 KVM 上的私有雲工作負載
- 通過對虛擬機器之間區內主機通信的完全可視性防止威脅
- 確保在整個虛擬環境中適當應用安全性原則
- 按應用程式、使用者和設備提供安全的應用程式啟用規則，無論 VM 的位置如何
- 實施適當的安全性分區和隔離
- 使用統一策略獲得跨多個位置和可用區域的流量的完整可見性和簡化配置

2. Internet Edge

- 保護公司資源免受互聯網閘道攻擊。
- 使用先進安全功能保護 Internet Edge免受最高級攻擊並自動阻止威脅
- 通過實施威脅防禦和分段功能確保符合監管標準
- 通過利用 SonicOSX 增強提高業務效率、性能並降低成本
- 分段關鍵 PoS（銷售點）系統，確保業務連續性
- 使用統一策略獲得跨多個區域和可用區域的流量的完整可見性和控制

NSv 系列系統規格

防火牆一般資訊	NSv 270	NSv 470	NSv 870
作業系統	SonicOSX[12]		
支持的虛擬機器監控程序	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7、Microsoft Hyper-V、KVM Ubuntu 16.04 / CentOS 7、Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[11]		
支援的公共雲平台（實例類型）[1]	AWS (c5.large)、Azure (Std D2 v2)	AWS (c5.xlarge)、Azure (Std D3 v2)	AWS (c5.2xlarge)、Azure (Std D4 v2)
許可	BYOL、PAYG[2]		
支援的最大 vCPU	2	4	8
介面計數 (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)	8/8/8/2/2	8/8/8/4/4	8/8/8/8/8
最大管理/DataPlane 核心	1/1	1/3	1/7
最小記憶體[3]	6 GB	8 GB	10 GB
最大記憶體	6 GB	10 GB	14 GB
支持的 IP/節點	無限制		
最小存儲	60 GB		
SSO 用戶	500	10,000	15,000
日誌記錄	分析器、本地日誌、Syslog		
高可用性	主動/被動5		
防火牆/VPN 性能[6,8]	**NSv 270**	**NSv 470**	**NSv 870**
防火牆檢查輸送量	6 Gbps	9 Gbps	14 Gbps
威脅防禦輸送量	1.6 Gbps	2.9 Gbps	8 Gbps
IPS 輸送量	4 Gbps	6 Gbps	8 Gbps
TLS/SSL DPI 輸送量	800 Mbps	2 Gbps	4 Gbps
VPN 輸送量	1.4 Gbps	3.5 Gbps	8 Gbps
每秒連接數	13,760	37,270	75,640
最大連接數 (SPI)	225,000	1.5M	3M
最大連接數 (DPI)	125,000	1.5M	2M
TLS/SSL DPI 連接數	8,000	20,000	30,000
VPN	**NSv 270**	**NSv 470**	**NSv 870**
網站到網站 VPN 隧道	75	6000	10,000
IPSec VPN 用戶端（最大）	50(1000)	2000(4000)	2000(6000)
包括 SSL VPN 用戶端[7]	2	2	2
SSL VPN 用戶端最大數量[7]	100	200	300
加密/身份驗證	DES、3DES、AES（128、192、256 位）/MD5、SHA-1、Suite B、通用訪問卡 (CAC)		
金鑰交換	Diffie Hellman 組 1、2、5、14v		
基於路由的 VPN	RIP、OSPF、BGP		
聯網	**NSv 270**	**NSv 470**	**NSv 870**
IP 地址分配	靜態、DHCP、內部 DHCP 伺服器[10]、DHCP 中繼[10]		
NAT 模式	一對一、多對一、一對多、靈活的 NAT（重疊 IP）、PAT		
最大 VLAN[9]	128	128	128
路由式通訊協定	BGP、OSPF、RIPv1/v2、靜態路由、基於策略的路由		
QoS	頻寬優先順序、最大頻寬、有保障頻寬、DSCP 標記、802.1p		
身份驗證	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、內部使用者資料庫、終端服務、Citrix		

[1]可用性待定。
[2]PAYG 目前僅在 AWS 上可用。
[3]禁用巨型幀的記憶體。
[4]啟用巨型幀的記憶體。巨型幀需要額外的內存。Azure 和 AWS 不支持巨型幀。
[5]在 VMware ESXi 平台、KVM、Azure、Microsoft Hyper-V 和 Nutanix 上提供高可用性。AWS 上不支援高可用性。
[6]發佈的性能資料符合規格，實際性能可能會因基礎硬體、網路條件、防火牆配置和已啟動的服務而異。性能和容量也可能會因基礎虛擬化基礎設施而異，我們建議在您的環境中進行其他測試，以確保滿足您的性能和容量要求。使用運行帶有 VMware vSphere 6.5 的 SonicOSv 6.5.0.2 的 Intel Xeon W 處理器（W-2195 2.3GHz、4.3GHz Turbo、24.75M 緩存）觀察到的性能指標。
[7]增加的 SSL VPN 編號僅可從 SonicOS 6.5.4.4-44v-21-723 韌體及更高版本獲得。
[8]Azure 和 AWS 上不支持 VLAN 介面。測試方法：基於 RFC 2544 的最大性能（用於防火牆）。使用行業標準的 Keysight HTTP 性能測試工具對威脅防禦/閘道 AV/反間諜軟體/IPS 輸送量進行測量。通過多個埠對使用多個流量進行測試。通過由默認防火牆設置啟用的閘道 AV、反間諜軟體、IPS 和應用程式控制對威脅防禦輸送量進行測量。根據 RFC 2544，使用 1418 位元組資料包大小的 AESGMAC16-256 加密 UDP 流量對 VPN 輸送量進行測量。所有規格、功能和可用性均可能隨時更改。
[9]所有性能參數均使用帶 SR-IOV 和 Turbo boost 的 Dell R740 進行測試。
[10]在私有雲上受支援，在公共雲平台上不受支援。
[11]運行 SonicOSX 7.0.0 及更高版本韌體的 SonicWall NSv 270/470/870 支持 Nutanix AHV。
[12]SonicOSX 7.0.1 及更高版本的用戶將能夠在經典/全域和策略模式之間進行選擇和切換。

SonicOSX 7.0 功能摘要

防火牆

- 有狀態資料包檢查
- 免重組深度資料包檢查
- DDoS 攻擊防護（UDP/ICMP/SYN 泛洪攻擊）
- IPv4/IPv6 支持
- 面向遠端存取的生物身份驗證
- DNS 代理
- REST API
- SonicWall 交換機集成[1]
- SD-WAN
  - SD-WAN 可擴產性
  - SD-WAN 可用性嚮導
- API
  - 全面 API 支持
- 多租戶3
  - 多租戶支持
  - 租戶視圖和每個租戶的韌體支援
- 在經典/全域和策略模式之間切換4

統一策略

- 統一策略整合了第 3 層到第 7 層的規則：
  - 來源/目標 IP/埠/服務
  - 應用程式控制
  - CFS/Web 僵屍網路/Geo-IP
  - 規則圖
  - 單通道安全服務強制實施 - IPS/GAV/AS/Capture ATP
  - 用於端點安全/BWM/QoS/CFS/入侵防禦的基於設定檔的對象
- 安全/DoS 規則的操作設定檔
- 規則管理：
  - 克隆
  - 影子規則分析
  - 儲存格內編輯
  - 規則匯出
  - 群組編輯
- 管理視圖
  - 已使用/未使用的規則
  - 活動/活動中的規則
  - 分區/自訂分組
  - 可定制網格/佈局

TLS/SSL/SSH 解密和檢查

- TLS1.3
- 支持具有增強安全性的 TLS 1.3
- 針對 TLS/SSL/SSH 的深度資料包檢查
- 包含/排除對象、群組或主機名稱
- SSL 控制
- 按區域或規則精細控制 DPI-SSL

Capture 高級威脅防護[2]

- Real-Time Deep Memory Inspection
- 雲端多引擎分析
- 虛擬沙箱
- 虛擬機器監控程序級分析
- 全系統類比
- 廣泛的檔案類型檢查
- 自動和手動提交
- 即時威脅情報更新
- 在裁決前進行阻止
- Capture Client

入侵防禦[2]

- 基於簽名的掃描
- 自動簽名更新
- 雙向檢查引擎
- 精細的 IPS 規則功能
- GeoIP 強制實施
- 利用動態清單過濾僵屍網路
- 規則運算式匹配

反惡意軟體[2]

- 基於資料流程的惡意軟體掃描
- 網關防病毒
- 閘道反間諜軟體
- 雙向檢查
- 不限制檔案大小
- 雲端惡意軟體資料庫

應用程式識別[2]

- 應用程式控制
- 應用程式頻寬管理
- 創建定制的應用程式簽名
- 防止資料洩露
- 通過 NetFlow/IPFIX 進行應用程式報告
- 綜合式應用程式簽名資料庫

流量視覺化和分析

- 用戶活動
- 應用程式/頻寬/威脅使用情況
- 雲端分析

HTTP/HTTPS Web 內容過濾[2]

- URL 過濾
- 代理規避
- 關鍵字攔截
- 基於策略的過濾（排除/包含）
- HTTP 標頭插入
- 頻寬管理 CFS 評級類別
- 帶有應用程式控制的統一策略模型
- 內容過濾用戶端

VPN

- 安全 SD-WAN
- 自動配置 VPN
- 用於網站到網站連接的 IPSec VPN
- SSL VPN 和 IPSec 用戶端遠端存取
- 冗餘的 VPN 閘道
- Mobile Connect for iOS、Mac OS X、Windows、Chrome、Android 和 Kindle Fire
- 基於路由的 VPN (RIP/OSPF/BGP)

增強儀錶板

- 增強設備視圖
- 頂級流量和用戶摘要
- 對威脅的洞察
- 通知中心
- 增強資料包監控
- UI 上的 SSH 終端
- 新設計/範本
- 行業與全球平均值比較

聯網

- PortShield1
- 巨型幀
- 路徑 MTU 發現
- 增強日誌記錄
- VLAN 中繼
- 埠鏡像（NSa 2650 及更高版本）
- 第 2 層 QoS
- 埠安全
- 動態路由 (RIP/OSPF/BGP)
- SonicWall 無線控制器[1]
- 基於策略的路由（ToS/metric 和 ECMP）
- NAT
- DHCP 伺服器
- 頻寬管理

- 鏈路聚合1（靜態和動態）
- 埠冗餘性[1]
- 主動/被動 (A/P) 高可用性（包括狀態同步）
- A/A 集群[1]
- 入站/出站負載平衡
- L2 橋接、1有線/虛擬有線模式、分接模式、NAT 模式
- 3G/4G WAN 容錯移轉[1]
- 非對稱路由
- 通用訪問卡 (CAC) 支持
- SonicCoreX 和 SonicOS 容器化

解密策略

- SSL/TLS 流量的統一策略

DoS 策略

- DoS/DDoS 攻擊防禦的統一策略

VoIP

- 精細 QoS 控制
- 頻寬管理
- 用於 VoIP 流量的 DPI
- H.323 Gatekeeper 和 SIP 代理支援

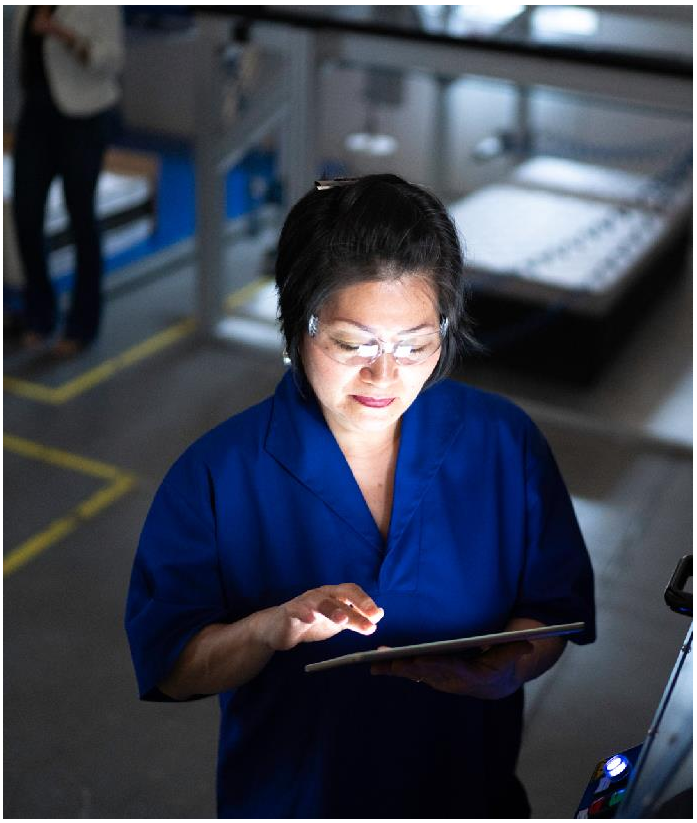
管理和監控

- Web 圖形化使用者介面
- 命令列介面 (CLI)
- 零接觸註冊與配置
- SonicExpress 移動應用程式支援
- SNMPv2/v3
- 利用 Network Security Manager (NSM)2 進行集中化管理和報告
- 日誌記錄
- Netflow/IPFix 匯出
- 雲端配置備份
- BlueCoat 安全分析平台
- 應用程式和頻寬視覺化工具
- IPv4 和 IPv6 管理
- 機外報告 (Scrutinizer)
- LCD 管理螢幕[1]
- CSC 簡單報告

無線1

- SonicWave AP 雲管理
- WIDS/WIPS
- 惡意 AP 預防
- 快速漫遊 (802.11k/r/v)
- 802.11s 網狀網路
- 自動通道選擇
- RF 頻譜分析
- 樓層平面圖
- 拓撲視圖
- 頻段引導
- 波束賦形
- 無線傳輸公平性
- 低功耗藍牙技術
- WiFi 擴展器
- 訪客迴圈配額
- LHM 訪客門戶

[1] NSv 系列防火牆對此不提供支援
[2] 需要額外訂閱
[3] 僅在 NSsp 防火牆上可用
[4] 在 SonicOSX 7.0.1 及更高版本上可用



合作夥伴支援服務

需要幫助規劃、部署或優化 SonicWall 解決方案嗎？SonicWall 高級服務合作夥伴接受過培訓，可為您提供世界一流的專業服務。瞭解更多：

www.sonicwall.com/PES

深入瞭解 SonicWall NSv 240/470/870 系列

www.sonicwall.com/NSv

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。有關更多資訊，請訪問 www.sonicwall.com 或在 Twitter、LinkedIn、Facebook 和 Instagram 上關注我們。

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

SONICWALL