NSv 270/470/870

Die SonicWall Network Security virtual NS*v* 270-/470-/870-Firewalls bieten Enterprise-Class-Sicherheit sowie eine optimierte Verwaltung, umfassende Transparenz und flexible Implementierung. Gleichzeitig gewährleisten sie eine überragende Performance für virtuelle Workloads.

Regelmäßig werden Schwachstellen innerhalb virtueller Umgebungen aufgedeckt, die ernsthafte Herausforderungen und Probleme für die Sicherheit bedeuten. Um all diese Sicherheitsvektoren schützen zu können, müssen die richtigen Sicherheitsregeln konsequent den richtigen Kontrollpunkten im Netzwerk zugeordnet werden. Das ist sehr wichtig, da manche Sicherheitsmängel auf ineffektive Regeln oder falsche Konfigurationen zurückzuführen sind.

HIGHLIGHTS

Sicherheit in Public, Private und Government-Clouds

- Next-Generation-Firewall mit automatisierter Erkennung und Prävention von Sicherheitslücken in Echtzeit
- Patentierte Real-Time Deep Memory Inspection(RTDMI™)-Technologie
- Patentierte Reassembly-Free Deep Packet Inspection(RFDPI)-Technologie
- Umfassende, durchgängige Transparenz und optimierte Verwaltung mit Unified Policy
- Application-Intelligence und Anwendungskontrolle
- DNS-Sicherheit
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- Wi-Fi-6-Firewall-Management
- Integration der Netzwerkzugriffskontrolle mit Aruba ClearPass
- Unterstützt AWS- und Azure-US-Government-Clouds
- Integration mit Microsoft Azure Sentinel für eine schnellere Reaktion auf Vorfälle
- Unterstützung von Private-Cloud-Plattformen (ESXi, Hyper-V, KVM, Nutanix) und Public-Cloud-Plattformen (AWS, Azure)

Schutz virtueller Maschinen

- Vertraulichkeit von Informationen
- Sichere Kommunikation dank Schutz vor Datenlecks
- Validierung, Prüfung und Überwachung des Datenverkehrs
- Stabilität und Verfügbarkeit virtueller Netzwerke

DATENBLATT

Die Firewalls der NS*v* Series unterstützen Ihre Security-Teams im Kampf gegen Sicherheitsrisiken und Schwachstellen, die Ihre geschäftskritischen Services und Prozesse signifikant beeinträchtigen können. Unternehmen können den dynamischen Traffic, der die Firewall passiert, steuern und erhalten einen transparenten Einblick in die verschiedenen Regeln, die im System implementiert sind. Die Firewalls tragen dazu bei, Verwaltungsaufgaben zu vereinfachen, Konfigurationsfehler zu reduzieren und die Implementierungszeit zu verkürzen, sodass insgesamt eine höhere Sicherheit möglich ist.

SonicOSX und Sicherheitsservices

Die SonicOSX-Architektur bildet das Herzstück der NS*v* 270-/470-/870-Firewalls. Sie basiert auf dem Betriebssystem SonicOSX 7, das viele Features wie eine intuitive Benutzeroberfläche (UI) sowie erweiterte Sicherheits-, Netzwerk- und Management-Funktionen umfasst.

SonicOSX 7.0 wurde von Grund auf mit Unified Policy konzipiert, einem Feature, das eine integrierte Verwaltung verschiedener Sicherheitsregeln erlaubt. Durch eine einfache Bereitstellung der Layer-3- bis Layer-7-Kontrollen in einer einzigen Regelbasis für jede Firewall lassen sich Regeln zentral konfigurieren. Die neue Weboberfläche enthält grafische Visualisierungen kritischer Bedrohungsdaten sowie praktische Warnmeldungen, die User dazu auffordern, kontextbezogene Sicherheitsregeln durch einfaches Klicken zu konfigurieren.

Daneben bietet die NS*v* Series integriertes SD-WAN, Unterstützung für TLS 1.3, Echtzeitvisualisierung, ultraschnelles Virtual Private Networking (VPN) und andere robuste Sicherheitsfeatures. Verdächtige Dateien werden zur Analyse an die cloudbasierte SonicWall-Multi-Engine-Sandbox Capture Advanced Threat Protection (ATP) weitergeleitet. Capture ATP nutzt die patentierte SonicWall-Technologie Real-Time Deep Memory Inspection (RTDMI), um Malware und Zero-Day-Bedrohungen im Arbeitsspeicher zu identifizieren und zu blockieren.

Mithilfe von Capture ATP, der RTDMI-Technologie und erweiterten Sicherheitsservices sind die Firewalls der NS*v* Series in der Lage, Malware direkt am Gateway zu stoppen – bevor sie in Ihre kritischen Systeme gelangen kann.

Implementierungsoptionen

1. Cloud Edge: sichere Public, Private und Government-Clouds

- Sichere Workloads auf Amazon Web Services (AWS) und Microsoft Azure
- Schutz von Cloud-Anwendungen und -Infrastrukturen vor Cyberbedrohungen mit hoch entwickelten Next-Generation-Firewall-Features inklusive VPN, IPS, CFS, AV etc.
- Einfache Entschlüsselung von verschlüsseltem Verkehr sowie höhere Sicherheit dank TLS-1.3-Unterstützung
- Einhaltung gesetzlicher Vorgaben durch die Implementierung von Funktionen zur Bedrohungsabwehr und Segmentierung
- Umfassende Transparenz und Kontrolle über den Traffic über verschiedene Regionen und Verfügbarkeitszonen hinweg dank Unified Policy
- Kostenvorteile und Effizienz durch eine Umgliederung von CapEx in OpEx
- Schutz von AWS- und Azure-Clouds für US-Behörden und deren Kunden durch die Implementierung der NS*v*-Firewalls
- Schutz von virtualisierten Rechenressourcen und Hypervisoren, um die Sicherheit von Private-Cloud-Workloads auf VMware ESXi, Microsoft Hyper-V, Nutanix und KVM zu gewährleisten
- Verhinderung von Bedrohungen durch einen umfassenden Einblick in die Intra-Host-Kommunikation zwischen virtuellen Maschinen
- Angemessene Anwendung von Sicherheitsregeln in der gesamten virtuellen Umgebung
- Regeln für ein sicheres Application-Enablement nach Anwendung, Benutzer und Inhalt unabhängig vom VM-Standort
- Implementierung geeigneter Sicherheitszonen sowie Isolierung
- Integration mit Microsoft Azure Sentinel, einer skalierbaren, cloudnativen Security-Information-Event-Management(SIEM)- und Security-Orchestration-Automated-Response(SOAR)-Lösung für eine schnellere Reaktion auf Vorfälle

2. Internet-Edge

- Schutz von Unternehmensressourcen vor Angriffen am Internet-Gateway
- Schutz des Internet-Edge vor den raffiniertesten Angriffen mithilfe erweiterter Sicherheitsfeatures und automatische Blockierung von Bedrohungen
- Einhaltung gesetzlicher Vorgaben durch die Implementierung von Funktionen zur Bedrohungsabwehr und Segmentierung
- Optimierung der betriebswirtschaftlichen Effizienz und Performance sowie Kostenreduzierung dank SonicOSX-Verbesserungen
- Segmentierung kritischer Point-of-Sale(POS)-Systeme zur Gewährleistung der Geschäftskontinuität
- Umfassende Transparenz und Kontrolle über den Traffic über verschiedene Regionen und Verfügbarkeitszonen hinweg dank Unified Policy

NSv Series – Systemdaten

Firewall allgemein	NSv 270	NSv 470	NSv 870
Betriebssystem	SonicOSX[11]		
Unterstützte Hypervisoren	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]		
Unterstützte Government-Clouds[12]	AWS und Azure (in den Regionen Osten und Westen der USA)		
Unterstützte AWS-Instanztypen	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
Unterstützte Azure-Instanztypen	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
Lizenzierung	BYOL, PAYG[1]		
Maximal unterstützte Anzahl von vCPUs	2	4	8
Anzahl der Schnittstellen (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
Maximale Anzahl von Management-/Data-Plane-Kernen	1/1	1/3	1/7
Minimaler Arbeitsspeicher[2]	4 GB	8 GB	10 GB
Maximaler Arbeitsspeicher[3]	6 GB	10 GB	14 GB
Unterstützte IP/Nodes	Unbegrenzt		
Mindestspeicher	60 GB		
SSO-Benutzer	500	10.000	15.000
Protokollierung	Analyzer, lokale Logdatei, Syslog		
Hochverfügbarkeit	Aktiv/Passiv[4]		

Firewall-/VPN-Performance[5,7]	NSv 270	NSv 470	NSv 870
Firewall-Inspection-Durchsatz	6 GBit/s	9 GBit/s	14 GBit/s
Threat-Prevention-Durchsatz	1,6 GBit/s	2,9 GBit/s	8 GBit/s
IPS-Durchsatz	4 GBit/s	6 GBit/s	8 GBit/s
TLS-/SSL-DPI-Durchsatz	800 MBit/s	2 GBit/s	4 GBit/s
VPN-Durchsatz[8]	1,4 GBit/s	3,5 GBit/s	8 GBit/s
Verbindungen pro Sekunde	13.760	37.270	75.640
Max. Anzahl von Verbindungen (SPI)	225.000	1,5 Mio.	3 Mio.
Max. Anzahl von Verbindungen (DPI)	125.000	1,5 Mio.	2 Mio.
TLS-/SSL-DPI-Verbindungen	8.000	20.000	30.000
VPN	**NSv 270**	**NSv 470**	**NSv 870**
Site-to-Site-VPN-Tunnel	75	6.000	10.000
IPSec-VPN-Clients[13] (max.)	50 (1.000)	2.000 (4.000)	2.000 (6.000)
Enthaltene SSL-VPN-Clients[6]	2	2	2
Max. Anzahl von SSL-VPN-Clients[6]	100	200	300
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256 Bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)		
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v		
Routenbasiertes VPN	RIP, OSPF, BGP		
Netzwerk	**NSv 270**	**NSv 470**	**NSv 870**
IP-Adresszuweisung	Statisch, DHCP, interner DHCP-Server[9], DHCP-Relay[9]		
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT		
Logische VLAN- und Tunnel-Schnittstellen (max.)[7]	128	128	128
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing		
QoS	Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p		
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix		
Lokale Benutzerdatenbank	250	2.500	3.200

[1] PAYG ist momentan nur auf AWS verfügbar.
[2] Speicher mit deaktiviertem Jumbo-Frame.
[3] Speicher mit aktiviertem Jumbo-Frame. Für Jumbo-Frames ist zusätzlicher Speicher erforderlich. Jumbo-Frames werden auf Azure und AWS nicht unterstützt.
[4] Hochverfügbarkeit (HV) auf VMware-ESXi-Plattform, KVM, Azure, Microsoft Hyper-V und Nutanix möglich. NSv 270 unterstützt HV durch Nutzung von D3v2 VM. HV wird nicht auf AWS unterstützt. HV auf Azure erfordert eine Servergröße, die mindestens drei Schnittstellen unterstützt.
[5] Bei den aufgeführten Performancezahlen handelt es sich um die Höchstwerte. Die tatsächliche Performance kann je nach Hardware, Netzwerkbedingungen, Firewall-Konfiguration und aktivierten Diensten variieren. Performance und Kapazitäten können auch je nach Virtualisierungsinfrastruktur variieren. Wir empfehlen zusätzliche Tests innerhalb Ihrer Umgebung, um sicherzustellen, dass Ihre Performance- und Kapazitätsanforderungen erfüllt werden. Die Performancekennzahlen wurden unter Verwendung eines Intel-Xeon-Prozessors (Platinum 8268 mit 2,9 GHz, 3,9 GHz Turbo, 37,5 MB Cache) mit SonicOS 7.0.1 mit VMware vSphere 7.0 ermittelt.
[6] Für das MSSP-Programm sind 50 SSL-VPN-Clients für die NSv 270 und 75 für die NSv 470 erhältlich. Eine höhere SSL-VPN-Anzahl ist nur ab SonicOS-Firmware 6.5.4.4-44v-21-723 erhältlich.
[7] VLAN-Schnittstellen werden auf Azure und AWS nicht unterstützt.
Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Der Threat-Prevention-/Gateway-AV-/Anti-Spyware-/IPS-Durchsatz wurde mit Keysight-HTTP-Leistungstesttools nach Branchenstandard gemessen. Die Tests wurden mit mehreren Datenströmen über mehrere Portpaare durchgeführt. Der Threat-Prevention-Durchsatz wurde bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle mit Standard-Firewall-Einstellungen gemessen. Der VPN-Durchsatz wurde bei UDP-Verkehr mit 1.418 Bytes pro Paket und AESGMAC16-256-Verschlüsselung gemäß RFC 2544 gemessen. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.
[8] Alle Performance-Parameter werden unter Verwendung von Dell R740 mit SR-IOV und Turbo-Boost getestet.
[9] Unterstützung auf Private-Cloud-, aber nicht auf Public-Cloud-Plattformen.
[10] Nutanix AHV wird auf SonicWall NSv 270/470/870 mit SonicOSX-Firmware 7.0.0 und höher unterstützt.
[11] Nutzer von SonicOSX 7.0.1 und höher können zwischen den Modi Classic/Global und Policy wählen und wechseln.
[12] Government-Cloud ist nur über BYOL verfügbar.
[13] Für das MSSP-Programm sind 25 GVC-Clients für die NSv 270 und 50 für die NSv 470 erhältlich.

SONICWALL

Die SonicOSX-7.0-Funktionen im Überblick

Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Schutz vor DDoS-Angriffen (UDP-/ICMP-/SYN-Flood)
- IPv4-/IPv6-Unterstützung
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- REST-APIs
- SonicWall-Switch-Integration[1]
- Integration mit SonicWall-Wi-Fi-6-AP
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- DNS-Filterung
- SD-WAN
  - SD-WAN-Skalierbarkeit
  - SD-WAN-Usability-Assistent
- API
  - Umfassende API-Unterstützung
- Mandantenfähigkeit[3]
  - Unterstützung mehrerer Nutzer
  - Nutzer-Ansicht mit Firmware-Support pro Nutzer
- Wechsel zwischen den Modi Classic/Global und Policy[4]

Unified Policy

- Unified Policy umfasst Regeln für die Schichten 3 bis 7:
  - Quell-/Ziel-IP/Port/Service
  - Anwendungskontrolle
  - CFS/Web-Botnet/Geo-IP
  - Regeldiagramm
  - Durchsetzung von Single-Pass-Sicherheitsservices – IPS/GAV/AS/Capture ATP
  - Profilbasierte Objekte für Endpoint-Security / BWM / QoS / CFS / Intrusion-Prevention
- Aktionsprofile für Sicherheits-/DoS-Regeln
- Regelmanagement:
  - Cloning
  - Shadow-Rule-Analyse
  - Zelleninterne Bearbeitung
  - Export von Regeln
  - Gruppenbearbeitung
- Verwaltung von Ansichten
  - Verwendete/Nicht verwendete Regeln
  - Aktive/Inaktive Regeln
  - Abschnitte / Benutzerdefinierte Gruppen
  - Einstellbares Grid/Layout

TLS-/SSL-/SSH-Entschlüsselung und -Prüfung

- TLS 1.3
- Unterstützung von TLS 1.3 mit verbesserter Sicherheit
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Granulare DPI-SSL-Steuerung nach Zone oder Regel

Capture Advanced Threat Protection[2]

- Real-Time Deep Memory Inspection
- Cloudbasierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Übermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client

Intrusion-Prevention[2]

- Signaturbasierte Scans
- Integration der Netzwerkzugriffskontrolle mit Aruba ClearPass
- Automatische Signatur-Updates
- Bidirektionale Prüf-Engine
- Granulare IPS-Regeln
- Geo-IP-Durchsetzung
- Botnet-Filterung mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[2]

- Streambasierte Malware-Scans
- Virenschutz am Gateway
- Spyware-Schutz am Gateway
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloudbasierte Malware-Datenbank

Anwendungsidentifizierung[2]

- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellung benutzerdefinierter Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungssignaturendatenbank

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloudbasierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten[2]

- URL-Filterung
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- DNS-Filterung
- Regelbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Rating-Kategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

VPN

- Sicheres SD-WAN
- Auto-Provisioning für VPNs
- IPSec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPSec-Client
- Redundantes VPN-Gateway
- Mobile Connect für iOS, Mac OS X, Windows, Chrome, Android und Kindle Fire
- Routenbasiertes VPN (RIP/OSPF/BGP)

Verbessertes Dashboard

- Optimierte Geräteansicht
- Überblick über den häufigsten Traffic und die häufigsten Nutzer
- Einblick in Bedrohungen
- Benachrichtigungszentrale
- Erweiterte Paketüberwachung
- SSH-Terminal auf der Benutzeroberfläche
- Neues Design/Template
- Vergleich mit Branchen- bzw. weltweitem Durchschnitt

Netzwerk

- PortShield[1]
- Jumbo-Frames
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung (NS*a* 2650 und höher)
- Layer-2-QoS

- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller[1]
- Regelbasiertes Routing (ToS/ metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Link-Aggregation[1] (statisch und dynamisch)
- Port-Redundanz[1]
- Hochverfügbarkeitsmodus A/P mit State-Sync
- A/A-Clustering[1]
- Lastausgleich für ein- und ausgehenden Datenverkehr
- L2-Bridge-[1], Wire-/Virtual-Wire-, Tap-, NAT-Modus
- 3G-/4G-WAN-Failover[1]
- Asymmetrisches Routing
- Unterstützung von Common Access Card (CAC)
- SonicCoreX- und SonicOS-Containerisierung

Entschlüsselungsrichtlinie

- Unified Policy für SSL-/TLS-Traffic

DoS-Richtlinie

- Unified Policy zur Verhinderung von DoS-/DDoS-Angriffen

VoIP

- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- H.323-Gatekeeper- und SIP-Proxy-Unterstützung

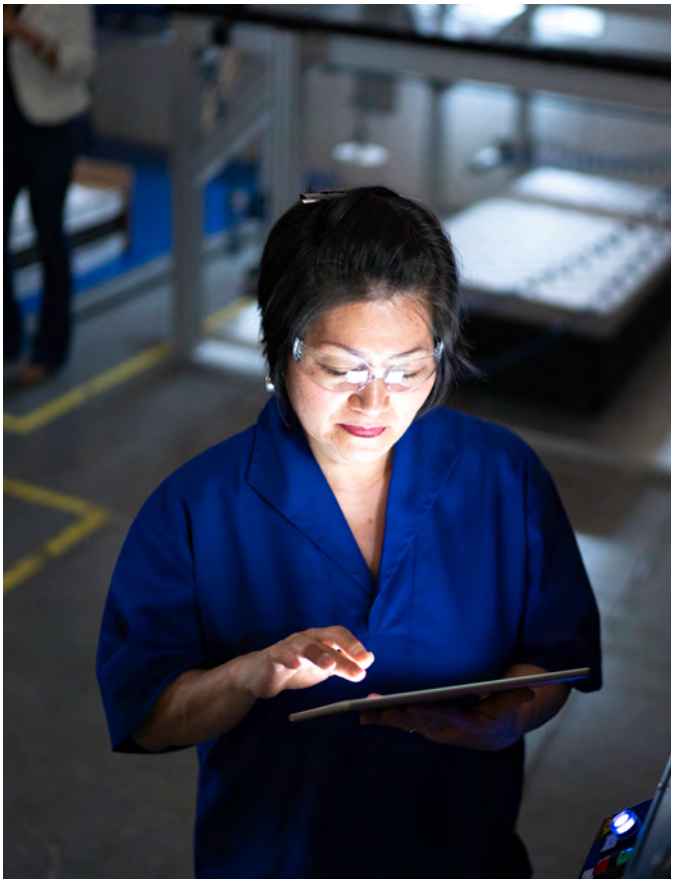
Verwaltung und Überwachung

- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Vollautomatische Registrierung und Implementierung
- Unterstützung der mobilen SonicExpress-App
- SNMPv2/v3
- Zentrales Management und Reporting mit Network Security Manager (NSM)[2]
- Protokollierung
- NetFlow-/IPFIX-Export
- Cloudbasiertes Konfigurationsbackup
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- Externes Reporting (Scrutinizer)
- LCD-Bildschirm[1]
- Dell N-Series- und X-Series-Switch-Verwaltung mit hintereinander geschalteten Switches[1]
- Reporting mit Network Security Manager

Wireless-Bereich[1]

- SonicWave-AP-Cloud- und -Firewall-Management
- WIDS/WIPS
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- 802.11s-Mesh-Networking
- Automatische Kanalauswahl
- Analyse des HF-Spektrums
- Floor Plan View
- Topology View
- Bandsteering
- Beamforming
- AirTime-Fairness
- Bluetooth Low Energy
- MiFi-Extender
- Zyklische Quote für Gastbenutzer
- LHM-Gast-Portal

[1] Wird nicht auf Firewalls der NS*v* Series unterstützt.
[2] Erfordert zusätzliches Abo.
[3] Nur für NSsp-Firewalls verfügbar.
[4] Verfügbar ab SonicOSX 7.0.1.



PARTNER ENABLED SERVICES

Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Die SonicWall-Advanced-Services-Partner unterstützen Sie mit erstklassigen Professional Services. Weitere Informationen:

www.sonicwall.com/PES

Erfahren Sie mehr über die SonicWall NSv 270/470/870 Series

www.sonicwall.com/NSv

Über SonicWall

SonicWall ermöglicht eine stabile, skalierbare und nahtlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-NSv-270-470-870-JK-9963