SONICWALL

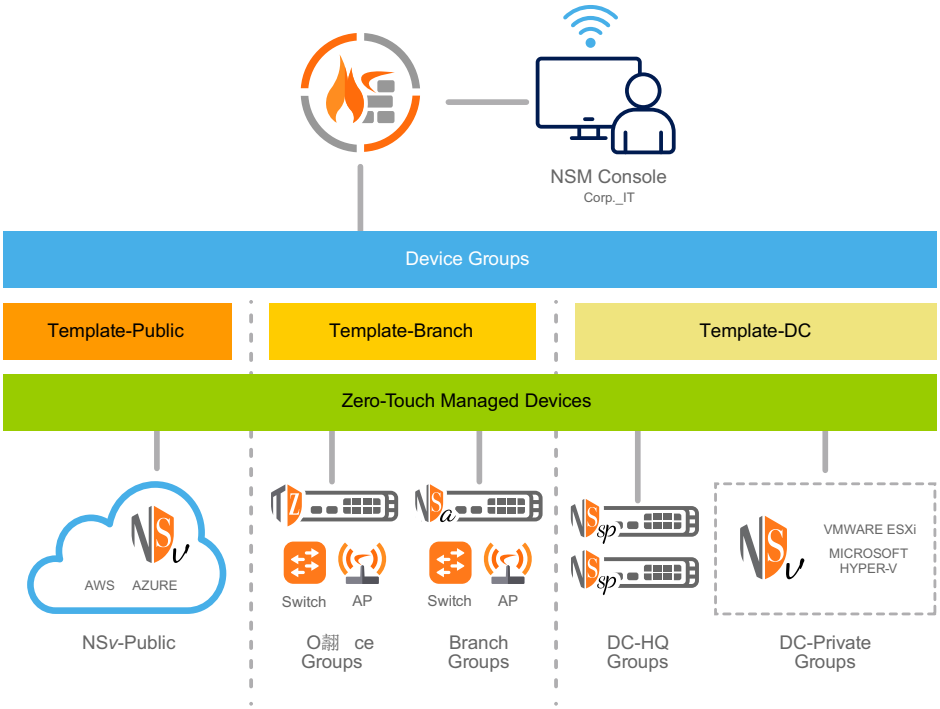
# Network Security Manager

Zunifikowany system zarządzania zaporami sieciowymi, który skaluje się w każdym środowisku

Nieważne, czy pod opieką mamy małą firmę, rozproszone przedsiębiorstwo, wiele organizacji czy zamknięte środowisko, ochronę sieci mogą nam bardzo utrudniać: chaos operacyjny, nieuwzględnione ryzyka oraz wymogi regulacyjne. Tradycyjnie najlepsze praktyki zarządzania firewallem opierały się głównie na sprawdzonych systemach i mechanizmach kontroli operacji. Jednakże nawet w dobrze zarządzanych Centrach Operacji Bezpieczeństwa (SOC) częste błędy, niewłaściwe konfiguracje, a nawet naruszenia posiadanych środków kontroli wciąż pozostają wyzwaniami.

SonicWall Network Security Manager (NSM), to działające w trybie multi-tenant narzędzie, które umożliwia centralne zarządzanie wszystkimi operacjami firewalli. Zastosowanie w nim przepływów pracy podlegających audytowi umożliwia eliminowanie błędów. Funkcje raportowania i analityki[1,2] zapewniają w jednym oknie wgląd w chronione środowisko oraz umożliwiają monitorowanie i wykrywanie zagrożeń, dzięki ujednoliceniu i korelowaniu rejestrów zdarzeń ze wszystkich zapór.

NSM pomaga również zachować zgodność z regulacjami, ponieważ oferuje pełne ścieżki audytu dla każdej zmiany konfiguracji oraz szczegółowe raportowanie. Rozwiązanie daje się skalować w organizacji dowolnej wielkości, umożliwiając zarządzanie sieciami z nawet tysiącami zapór rozmieszczonych w wielu lokalizacjach. NSM robi to wszystko, oszczędzając administratorom wysiłku i czasu.




## Korzyści

**Biznesowe**

- Mniejsze koszty zarządzania bezpieczeństwem
- Wiedza o stanie zagrożeń i zabezpieczeniach
- Obniżone koszty inwestycyjne (CAPEX) dzięki SaaS

**Operacyjne**

- Wyeliminowanie silosów w zarządzaniu zaporami sieciowymi
- Łatwe zdalne wdrażanie dowolnej liczby firewalli
- Wgląd we wszystkie operacje bezpieczeństwa

**Dotyczące bezpieczeństwa**

- Wyeliminowanie pojedynczego punktu awarii w oparciu o wysoką dostępność (HA)
- Audytowanie, zatwierdzanie i egzekwowanie spójnych polityk bezpieczeństwa we wszystkich środowiskach
- Wykrywanie i szybkie reagowanie na problemy i zagrożenia
- Podejmowanie świadomych decyzji co do polityki bezpieczeństwa
- Zapobieganie nieautoryzowanemu dostępowi, w tym zagrożeniom wewnętrznym

## Utrzymuj kontrolę: koordynuj operacje zapory z jednego miejsca

NSM oferuje wszystko, czego oczekujesz od ujednoliconego systemu zarządzania zaporami sieciowymi. Zapewnia widoczność każdego tenanta, kontrolę urządzeń w oparciu o grupy oraz nieograniczoną skalowalność, umożliwiając centralne zarządzanie i prowadzenie operacji bezpieczeństwa sieci opartej na rozwiązaniach SonicWall. Obejmuje to wdrażanie i zarządzanie wszystkimi firewallami, grupami urządzeń i tenantami oraz synchronizowanie i egzekwowanie spójnych polityk bezpieczeństwa we wszystkich środowiskach - w oparciu o elastyczne lokalne mechanizmy kontroli i monitorowanie wszystkiego przy użyciu jednego dynamicznego interfejsu ze szczegółowymi raportami i analizami. NSM umożliwia zarządzanie wszystkim z poziomu jednej konsoli, do której można uzyskać dostęp z dowolnego miejsca i na dowolnym urządzeniu obsługującym przeglądarkę.

### Zarządzanie w trybie multi-tenant

Środowisko chronione przez zapory będzie z czasem rosło, dlatego potrzebny będzie system zarządzania, który będzie się wraz z nim skalował. NSM oferuje pełne zarządzanie w trybie multi-tenant, zapewniając izolację polityk kontroli na wszystkich zarządzanych tenantach. Separacja obejmuje wszystkie elementy zarządzania NSM oraz funkcje, które określają działanie zapory dla każdego tenanta. Można tworzyć tenanty z własnymi zestawami użytkowników, grup i ról w zarządzaniu urządzeniami, orkiestracją polityk oraz wszystkich innymi zadaniami administracyjnymi w obszarze przypisanego do tenanta konta.

### Zarządzanie grupami urządzeń

Funkcja Device Group oferuje efektywną metodę tworzenia i zarządzania firewallami zebranymi w proste grupy oraz grupy hierarchiczne. Ułatwia ona zatwierdzanie i wdrażanie szablonów konfiguracji w grupach zapór. Umożliwia synchronizację i egzekwowanie polityk, obiektów i ustawień w dowolnie wybranych grupach zapór w sposób spójny i niezawodny. Wszystkie zatwierdzone zmiany polityk w szablonie są automatycznie wdrażane we wszystkich grupach urządzeń skojarzonych z tym szablonem. W celu ułatwienia zarządzania, identyfikowania i tworzenia powiązań, grupy urządzeń można definiować szczegółowo w oparciu o dowolne atrybuty, takie jak: typ sieci, lokalizacja, jednostka biznesowa, struktura organizacyjna (a także ich kombinacje).

### Zarządzanie, zatwierdzanie i wdrażanie szablonów

Uproszczone przepływy pracy w NSM umożliwiają łatwe i szybkie projektowanie, walidację, audytowanie oraz zatwierdzanie szablonów konfiguracji, bez względu na to, czy zarządza się jedną zaporą, czy tysiącem w wielu lokalizacjach. Szablony z różnymi politykami zapory, ustawieniami i powiązanymi obiektami są definiowane niezależnie od urządzenia. Są one wykorzystywane przez NSM do centralnego i automatycznego wysyłania konfiguracji do pojedynczych urządzeń lub ich grup, wymagających podobnych ustawień.

## Działaj efektywniej: pracuj mądrzej i szybciej, z mniejszym wysiłkiem podejmując działania związane z bezpieczeństwem

NSM to narzędzie zarządzające produktywnością, które umożliwia inteligentniejszą pracę i szybsze podejmowanie działań związanych z bezpieczeństwem przy mniejszym wysiłku. Zostało ono zaprojektowane w oparciu o procesy biznesowe i zasadę upraszczania operacji. Stosuje też automatyzację przepływów pracy w celu osiągnięcia lepszej koordynacji bezpieczeństwa. Pomaga zmniejszyć złożoność, ograniczyć czas i koszty wykonywania codziennych operacji bezpieczeństwa oraz zadań administracyjnych.

### Bezproblemowe wdrażanie w trybie Zero-Touch

Zintegrowana z NSM funkcja Zero-Touch Deployment umożliwia bardzo łatwe wdrażanie i dostosowywanie zapór, przełączników i punktów dostępowych SonicWall w lokalizacjach zdalnych i oddziałach. Cały proces wymaga minimum interwencji użytkownika i jest w pełni zautomatyzowany. Obsługujące funkcję Zero-Touch urządzenia są wysyłane bezpośrednio do miejsc instalacji. Po zarejestrowaniu i podłączeniu do sieci wszystkie natychmiast zaczynają działać, zapewniając bezpieczeństwo i płynną komunikację. Po nawiązaniu łączności z NSM do wszystkich podłączonych urządzeń są automatycznie przesyłane wstępnie skonfigurowane szablony. Ogranicza to czas, koszty i złożoność tradycyjnego procesu lokalnego wdrażania.

### Pozbawione błędów zarządzanie zmianami

NSM oferuje natychmiastowy dostęp do efektywnych i zautomatyzowanych przepływów pracy, które są zgodne z zarządzaniem zmianami polityk firewalli oraz audytowymi wymaganiami centrów SOC.

Zastosowanie szeregu rygorystycznych procedur umożliwia eliminację błędów przy zmianach polityk. Obejmuje to porównanie konfiguracji, walidację i autoryzację przed wdrożeniem. Grupy zatwierdzania są elastyczne, dzięki czemu można je dostosować się do procedur audytu wewnętrznego różnych zespołów funkcyjnych. Dzięki obowiązkowemu procesowi zatwierdzania, NSM umożliwia poprawę efektywności operacyjnej, ogranicza ryzyko i eliminuje błędy w konfiguracji.

### Automatyzacja zarządzania z użyciem RESTful API

Dzięki użyciu interfejsów API RESTful w NSM specjaliści ds. bezpieczeństwa mogą stosować oparte na standardach podejście do programowego zarządzania specyficznymi funkcjami NSM bez konieczności korzystania z interfejsu przeglądarki. Ułatwia to współdziałanie między NSM a konsolami zarządzania innych firm, zwiększając efektywność wewnętrznego zespołu ds. bezpieczeństwa. Usługi API mogą automatyzować operacje firewalli na dowolnych zarządzanych urządzeniach. Obejmuje to typowe codzienne zadania, takie jak zarządzanie grupami urządzeń i tenantami, konfiguracje audytu, przeprowadzanie kontroli stanu systemu itp.

## Bądź bardziej świadomy: odkrywaj nieznane zagrożenia dzięki aktywnemu monitorowaniu, raportowaniu i analityce [1-2]

Interaktywna konsola NSM zapewnia monitorowanie i raportowanie w czasie rzeczywistym oraz dostarcza dane analityczne. Informacje te pomagają rozwiązywać problemy, badać zagrożenia i podejmować inteligentne działania w zakresie polityki bezpieczeństwa, czego efektem jest bardziej adaptacyjne podejście do ochrony.

### Wgląd wszędzie i we wszystko

NSM w połączeniu z analityką[1-2] zapewnia widoczność 360° przez 7 dni w tygodniu całego ekosystemu zabezpieczeń SonicWall - na poziomie tenanta, grupy lub urządzenia. Oferuje w czasie niemal rzeczywistym statyczną analizę całego ruchu sieciowego i transmisji danych, które przechodzą przez ekosystem zapory sieciowej. Wszystkie dane dziennika są automatycznie rejestrowane, agregowane, kontekstualizowane i przedstawione w zrozumiały, praktyczny i łatwy do wykorzystania sposób. Można następnie odkrywać, interpretować, ustalać priorytety i podejmować odpowiednie działania obronne i naprawcze w oparciu o wgląd wynikający z danych i świadomości sytuacyjnej.

Funkcja planowania raportów umożliwia ich dostosowanie w oparciu o dowolną kombinację danych o ruchu. NSM daje dostęp do rejestrów z 365 dni na poziomie urządzenia w celach analizy historycznej, wykrywania anomalii, ujawniania luk w zabezpieczeniach itp. Pomaga to w śledzeniu, mierzeniu i utrzymaniu efektywności sieci i operacji bezpieczeństwa.

**Znaj swoje ryzyka**

Dzięki dodatkowym funkcjom zagłębiania i obracania można przeprowadzać głębszą analizę i korelowanie danych, aby odkrywać nieznane zagrożenia i problemy z większą dokładnością i pewnością. Korzystając z kombinacji raportów historycznych, analiz opartych na użytkownikach i aplikacjach oraz wglądu w punkty końcowe, można dokładnie przeanalizować różne wzorce i trendy związane z ruchem przychodzącym/wychodzącym, wykorzystaniem aplikacji, dostępem użytkowników i urządzeń, działaniami dotyczącymi zagrożeń itp. Zyskuje się świadomość sytuacyjną oraz cenny wgląd i wiedzę, niezbędne nie tylko do odkrywania zagrożeń bezpieczeństwa, ale także koordynowania działań naprawczych oraz monitorowania i śledzenia wyników. Wszystko to umożliwia spójne egzekwowanie bezpieczeństwa w chronionym środowisku.

**Elastyczne wdrażanie**

Administratorzy mogą wdrażać NSM na różne sposoby, wybierając ten, który najlepiej odpowiada ich wymaganiom operacyjnym, regulacyjnym i budżetowym.

Aby nie martwić się utrzymaniem, mogą postawić na ofertę NSM w formie SaaS, usługi hostowanej przez SonicWall i dostępnej przez Internet. NSM w modelu SaaS można skalować na żądanie, jednocześnie zmniejszając koszty operacyjne. Znikają problemy ze sprzętem i oprogramowaniem do wdrożenia, harmonogramem utrzymania, dostosowywaniem, konfigurowaniem lub aktualizowaniem oprogramowania, przestojami, amortyzacją i kosztami wycofania z użytku. Wszystkie związane z tym wydatki zastępuje jeden niewysoki i przewidywalny koszt rocznej subskrypcji.

W celu uzyskania pełnej kontroli i zgodności systemu można wdrożyć NSM w chmurze publicznej Microsoft Azure lub jako urządzenie wirtualne w chmurze prywatnej, opartej na VMware, Microsoft Hyper-V lub KVM. Takie rozwiązanie zapewnia wszystkie operacyjne i ekonomiczne korzyści płynące z wirtualizacji, w tym skalowalność, zwinność i szybkość udostępniania systemu, proste zarządzanie oraz redukcję kosztów.

**Możliwości ochrony**

Administracja rządowa, ochrona zdrowia, koncerny farmaceutyczne i inne duże organizacje często wdrażają zamknięte sieci, aby zachować prywatność i izolować aplikacje o znaczeniu krytycznym oraz najbardziej wrażliwe systemy informatyczne, takie jak zasoby dokumentów niejawnych, instalacje SCADA czy laboratoria badawcze. NSM obsługuje zamknięte środowiska sieciowe, dając ich administratorom możliwość implementowania, licencjonowania, łatania i aktualizowania narzędzia i zarządzanych przez nie zapór sieciowych bez konieczności kontaktowania się z SonicWall License Managerem i MySonicWall.

Aby zwiększyć ochronę, NSM wymusza użycie kilku środków kontroli dostępu do kont, zapobiegając nieautoryzowanemu dostępowi do interfejsu zarządzania. Udziela dostępu administracyjnego zgodnie z rolami użytkownika i uruchamia blokadę konta na podstawie określonej liczby nieudanych prób logowania. Dostęp jest udzielany tylko po zalogowaniu się z określonej listy dozwolonych źródłowych adresów IP i zabezpieczony przy użyciu uwierzytelniania dwuskładnikowego (2FA)3.

## Podsumowanie funkcji

**Zarządzanie**

- Tenant and Device Group level management
- Configuration templates
- Device grouping
- Device configuration conversion into template
- Commit and deploy wizard
- Configuration audits
- Config – Diff
- O翻 ine Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of SD-WAN
- Management of Security Services
- High Availability
- Configuration backups
- RESTful API
- Multi-device firmware upgrade
- Role-based administration
- Access Point and Switch Management
- Intelligent Platform Monitoring (IPM)[3]
- Multi-device certificate management

**Monitoring [1,2]**

- Device health and status
- License and support status
- Network/Threat summary
- Alert and notification center
- Event logs
- Topology view

**Analityka [1,2]**

- User-based activities
- Application usage
- Cross-product visibility with Capture Client
- Real-Time Dynamic Visualization
- Drill-down and pivoting capabilities

**Raportowanie[1,2]**

- Scheduled PDF reports - Tenant/Group/Device level
- Customizable reports
- Centralized logging
- Multi-Threat report
- User-Centric report
- Application Usage report
- Bandwidth and Services reports
- Per User Bandwidth Reporting

**Ochrona**

- Closed Network support
- Account lockout
- Account access control
- 2FA support[3]
- Authenticator App TFA support

## Licencje I pakiety

| Funkcja | NSM SaaS Essential | NSM SaaS Advanced | NSM On-Prem |
|---|---|---|---|
| Zarządzanie | Tak | Tak | Tak |
| Raportowanie | 7 dni | 365 dni | Nie[2] |
| Analityka | Nie | Tak | Nie[2] |

| Produkt | SKU |
|---|---|
| NSM ESSENTIAL FOR SOHO 250 1YR | 02-SSC-5219 |
| NSM ADVANCED FOR SOHO 250 1YR | 02-SSC-5213 |
| NSM ESSENTIAL FOR TZ 270 1YR | 02-SSC-7049 |
| NSM ADVANCED FOR TZ 270 1YR | 02-SSC-6977 |
| NSM ESSENTIAL FOR TZ 370 1YR | 02-SSC-7067 |
| NSM ADVANCED FOR TZ 370 1YR | 02-SSC-6989 |
| NSM ESSENTIAL FOR TZ 470 1YR | 02-SSC-7001 |
| NSM ADVANCED FOR TZ 470 1YR | 02-SSC-7073 |
| NSM ESSENTIAL FOR TZ 570 1YR | 02-SSC-4975 |
| NSM ADVANCED FOR TZ 570 1YR | 02-SSC-4963 |
| NSM ESSENTIAL FOR TZ 670 1YR | 02-SSC-5011 |
| NSM ADVANCED FOR TZ 670 1YR | 02-SSC-4999 |
| NSM ESSENTIAL FOR NSa 2700 1YR | 02-SSC-7166 |

| Produkt | SKU |
|---|---|
| NSM ADVANCED FOR NSa 2700 1YR | 02-SSC-7160 |
| NSM ESSENTIAL FOR NSa 3600/NSa 3650 1YR | 02-SSC-5299 |
| NSM ADVANCED FOR NSa 3600/NSa 3650 1YR | 02-SSC-5293 |
| NSM ESSENTIAL FOR NSa 4600/NSa 4650 1YR | 02-SSC-5325 |
| NSM ADVANCED FOR NSa 4600/NSa 4650 1YR | 02-SSC-5319 |
| NSM ESSENTIAL FOR NSa 5600/NSa 5650 1YR | 02-SSC-5347 |
| NSM ADVANCED FOR NSa 5600/NSa 5650 1YR | 02-SSC-5341 |
| NSM ESSENTIAL FOR NSa 6600/NSa 6650 1YR | 02-SSC-5365 |
| NSM ADVANCED FOR NSa 6600/NSa 6650 1YR | 02-SSC-5359 |
| NSM MANAGEMENT ON-PREM BASE LICENSE - 5 NODES 1YR | 02-SSC-6873 |
| NSM ON-PREM MANAGEMENT - 1 NODE ADD-ON 1YR | 02-SSC-6874 |
| NSM ON-PREM MANAGEMENT - 10 NODE ADD-ON 1YR | 02-SSC-6875 |
| NSM ON-PREM MANAGEMENT - 25 NODE ADD-ON 1YR | 02-SSC-6876 |
| NSM ON-PREM MANAGEMENT - 100 NODE ADD-ON 1YR | 02-SSC-6877 |
| NSM ON-PREM MANAGEMENT - 250 NODE ADD-ON 1YR | 02-SSC-6878 |

*Dostępne są również wieloletnie SKU i umowy pomocy technicznej. Aby uzyskać ich pełną listę, skontaktuj się z wybranym resellerem lub działem* SonicWall Sales.

[1] NSM SaaS obejmuje funkcje raportowania i analizy.
[2] NSM On-Prem wymaga odzielnej instalacji i licencji SonicWall Analytics On-Prem dla funkcji raportowania i analizy.
[3] Dostępne tylko w NSM On-Prem.
[4] Nie uwzględnia 365 dni raportowania i 30 dni analityki.

### Przeglądarki internetowe

- Microsoft Internet Explorer 11.0 lub nowszy i ostatnie wersje Microsoft Edge, Mozilla Firefox, Google Chrome i Safari

### Wymagania systemowe NSM On-Prem

- Wirtualizator: ESXi 7.0, 6.7, 6.5 oraz Hyper-V 2016, 2019
- Minimalne zasoby: 4 vCPU, 16GB RAM, 250GB na dysku

### Zarządzane urządzenia

- NSsp 15700, NSsp 12000 Series4, SuperMassive 9000 Series4, E-Class NSA, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Brak wsparcia dla urządzeń i firmware Generation 5, w tym przewodowego sprzętu SOHO z systemem SonicOS 5.9.
- SonicWall Network Security Virtual Appliances: NSv Series
- SonicWall SonicWave, SonicPoint
- SonicWall Switch

### O firmie SonicWall

W erze hiper-rozproszonego środowiska pracy, gdy wszyscy są zdalni, mobilni i niechronieni, SonicWall konsekwentnie wprowadza w życie swoją koncepcję Boundless Cybersecurity. Zapewniając wgląd w czasie rzeczywistym i niezwykle ekonomiczne podejście do ochrony, SonicWall wypełnia luki w zabezpieczeniach w przedsiębiorstwach, instytucjach rządowych oraz małych i średnich firmach na całym świecie. Aby uzyskać więcej informacji, odwiedź stronę www.sonicwall.com oraz śledź nas w serwisach Twitter, LinkedIn, Facebook I Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Dodatkowe informacje na stronie.
www.sonicwall.com



Datasheet-NSM-US-VG-3836