Seria SonicWall Network Security appliance (NSa)

Walidowana branżowo efektywność i wydajność ochrony dla sieci średniej wielkości i rozproszonych przedsiębiorstw.

Seria urządzeń SonicWall Network Security appliance (NS*a*) zapewnia sieciom średniej wielkości, oddziałom firm i rozproszonym przedsiębiorstwom zaawansowaną ochronę przed zagrożeniami opartą na wydajnej platformie bezpieczeństwa. Dzięki innowacyjnym technologiom deep learningu w rozwiązaniu SonicWall Capture Cloud Platform urządzenia NS*a* oferują zautomatyzowaną detekcję i ochronę przed włamaniami w czasie rzeczywistym.

Nowoczesna ochrona przed zagrożeniami o wyjątkowej wydajności

Ataki sieciowe stały się obecnie bardzo wyrafinowane i trudne do wykrycia przy użyciu tradycyjnych metod detekcji. Skuteczna obrona przed nimi wymaga wykorzystania inteligencji z chmury obliczeniowej. Bez niej bramowe rozwiązania bezpieczeństwa nie są w stanie poradzić sobie ze złożonymi zagrożeniami. Seria urządzeń Ns*a*, czyli firewalli nowej generacji (NGFW - next-generation firewalls), integruje zaawansowane technologie bezpieczeństwa w celu zapewniania sieciom skutecznej ochrony. Technologia Real-Time Deep Memory Inspection (RTDMI™), która wkrótce zostanie opatentowana, dopełnia opartą na wielu silnikach usługę SonicWall Capture Advanced Threat Protection (ATP). Mechanizm RTDMI proaktywnie wykrywa i blokuje zagrożenia typu zero-day i nieznany dotąd malware, przeprowadzając kontrolę procesów bezpośrednio w pamięci. Dzięki architekturze czasu rzeczywistego technologia SonicWall RTDMI działa precyzyjnie, z minimalną liczbą fałszywych wykryć (false positives), identyfikując i neutralizując wyrafinowane ataki w czasie krótszym niż 100 nanosekund od ujawnienia złośliwych mechanizmów. W połączeniu z opatentowanym* mechanizmem Reassembly-Free Deep Packet Inspection (RFDPI) egzaminuje każdy bajt każdego pakietu, jednocześnie kontrolując na firewallu zarówno wchodzący, jak i wychodzący ruch. Wykorzystując platformę SonicWall Capture Cloud oraz wbudowane funkcjonalności, takie jak ochrona przed intruzami, antymalware oraz filtrowanie web/URL, seria NS*a* zatrzymuje na bramie sieciowej nawet najbardziej podstępne zagrożenia.

Dodatkowo firewalle SonicWall zapewniają kompletną ochronę, przeprowadzając pełne deszyfrowanie i inspekcję połączeń TLS/SSL i SSH oraz aplikacji, w przypadku których nie da się zastosować proxy, bez względu na rodzaj użytego transportu i protokołu. Firewall zagląda głęboko w każdy pakiet (w nagłówek i dane), poszukując niezgodności z protokołem, zagrożeń, luk zero-day, intruzów, a także zdefiniowanych kryteriów.

Mechanizm DPI (Deep Packet Inspection) wykrywa i chroni przed ukrytymi atakami wykorzystującymi kryptografię, blokuje pobieranie zaszyfrowanego malware'u, ogranicza rozprzestrzenianie się infekcji, uniemożliwia komunikację typu command and control (C&C) oraz eksfiltrację danych. Reguły włączenia i wyłączenia umożliwiają całkowitą kontrolę w dostosowywaniu, który ruch podlega deszyfrowaniu i inspekcji w oparciu o specyficzne standardy w organizacji oraz uregulowania prawne.

Często, gdy organizacja włączy funkcjonalności typu DPI (takie jak IPS, antywirus, antyspyware, dekrypcja/inspekcja TLS/SSL i in.), wydajność sieciowa spada, czasem bardzo wyraźnie. Jednakże urządzenia z serii NSa wykorzystują wielordzeniową architekturę, która opiera się na mikroprocesorach specjalizowanych pod kątem bezpieczeństwa.

W połączeniu z mechanizmami RTDMI i RFDPI ta wyjątkowa architektura zapobiega degradacji wydajności, do której dochodzi w innych firewallach.

Korzyści:

Wyjątkowa ochrona przed zagrożeniami i wydajność

- Oczekująca na opatentowanie technologia RTDMI (Real-Time Deep Memory Inspection)
- Opatentowana technologia RFDPI (reassembly-free deep packet inspection)
- Ochrona przed zagrożeniami oparta na wewnętrznych funkcjonalnościach i chmurze
- Dekrypcja i inspekcja TLS/SSL
- Walidowana przez branżę efektywność bezpieczeństwa
- Wielordzeniowa architektura sprzętowa
- Dedykowany zespół badawczy ds. zagrożeń Capture Labs

Sieciowa kontrola i elastyczność

- System operacyjny SonicOS o wielu możliwościach
- Inteligencja i kontrola aplikacyjna
- Segmentacja sieciowa z VLAN
- Bezpieczeństwo szybkich sieci bezprzewodowych

Łatwość wdrożenia, konfiguracji i bieżącego zarządzania

- Rozwiązanie ściśle zintegrowane
- Scentralizowane zarządzanie
- Skalowalność oparta na wielu platformach sprzętowych
- Niski całkowity koszt posiadania

Sieciowa kontrola i elastyczność

Podstawą działania serii NS*a* jest SonicOS, bogaty w funkcjonalności system operacyjny SonicWall. SonicOS zapewnia organizacjom sieciową kontrolę i elastyczność, oferując inteligencję i kontrolę aplikacyjną, wizualizację w czasie rzeczywistym, zaawansowany technologicznie system IPS (Intrusion Prevention System) z technologią anti-evasion, szybkie sieci VPN (Virtual Private Networking) i inne wydajne funkcjonalności ochrony.

Dzięki wykorzystaniu inteligencji i kontroli aplikacyjnej administratorzy sieciowi mogą identyfikować i oddzielać produktywne aplikacje od tych, które są nieproduktywne i potencjalnie niebezpieczne, oraz kontrolować ruch przy użyciu polityk na poziomie aplikacyjnym wobec zarówno pojedynczych użytkowników, jak i ich grup (włącznie z harmonogramami i listami wykluczeń). Kluczowe dla biznesu aplikacje mogą być priorytetyzowane z przydziałem większego pasma, a mniej istotnym przydzielane jest mniejsze pasmo. Monitoring i wizualizacja w czasie rzeczywistym zapewnia graficzne przedstawienie aplikacji, użytkowników i zużycia pasma, dając granularny wgląd w ruch sieciowy.

Organizacjom wymagającym większej elastyczności w architekturze sieciowej SonicOS oferuje narzędzia do segmentowania sieci przy użyciu technologii wirtualnych LAN-ów (VLAN). Dzięki temu administratorzy sieciowi mogą tworzyć interfejs VLAN, który umożliwia separację sieci na małe grupy logiczne. Mogą ustanawiać reguły, które określają poziom komunikacji z urządzeniami z innych VLAN-ów.

Każdy firewall z serii NS*a* ma wbudowany kontroler sieci bezprzewodowej, który umożliwia organizacjom rozszerzanie granic sieci poprzez wykorzystanie technologii WiFi. Współdziałające ze sobą firewalle SonicWall i punkty dostępowe SonicWave 802.11ac Wave 2 tworzą rozwiązanie bezpieczeństwa sieci bezprzewodowej. Łączy ono wiodącą technologię Next-Generation Firewall z szybką komunikacją bezprzewodową, zapewniając ochronę sieciową i wydajność klasy enterprise w sieciach bezprzewodowych .

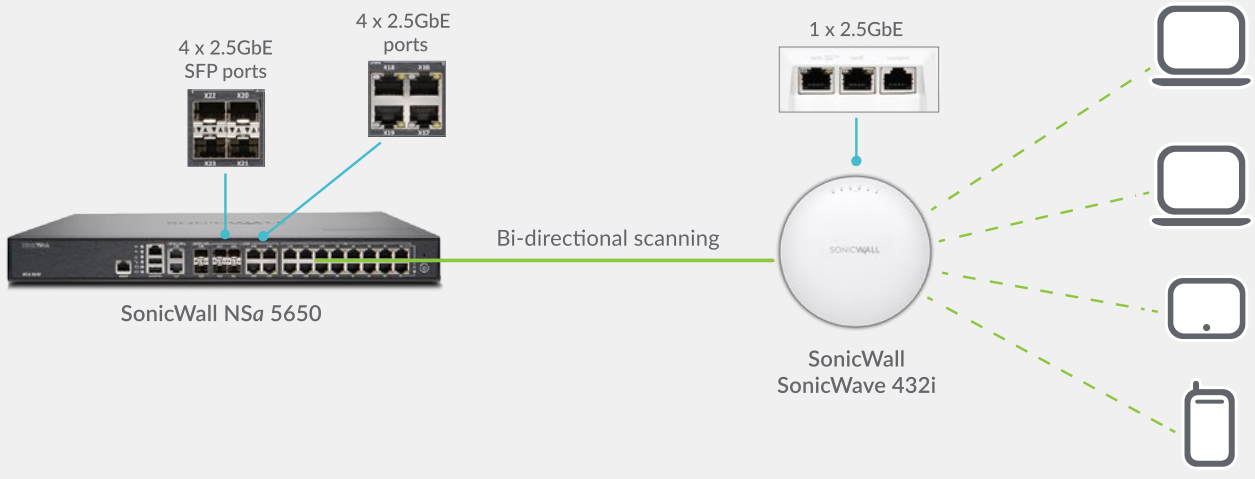
Łatwość wdrożenia, konfiguracji i bieżącego zarządzania

Podobnie jak wszystkie firewalle SonicWall, seria NS*a* ściśle integruje kluczowe technologie bezpieczeństwa, komunikacji i elastyczności w jednym kompleksowym rozwiązaniu. Obejmuje to także bezprzewodowe punkty dostępowe SonicWave oraz serię SonicWall WAN Acceleration Appliance (WXA) – obydwa rozwiązania są automatycznie wykrywane i obsługiwane przez zarządzający firewall NS*a*. Konsolidowanie wielu funkcjonalności eliminuje konieczność zakupu i instalowania produktów „firm trzecich" (Third Party), które nie zawsze dobrze ze sobą współpracują. Mniej jest też pracy przy wdrażaniu rozwiązania w sieci i konfigurowania go, co zaoszczędza czas i pieniądze.

Bieżące zarządzanie, monitoring i raportowanie bezpieczeństwa sieciowego jest przeprowadzane centralnie przez firewall albo poprzez SonicWall Capture Security Center. W ten sposób administratorzy sieciowi mają jedną konsolę do kontroli wszystkich elementów sieci. Uproszczone wdrażanie i konfiguracja oraz ułatwione zarządzanie przekładają się w organizacji na niższy całkowity koszt posiadania oraz większy zwrot z inwestycji.

Bezpieczna i szybka sieć bezprzewodowa

Połączenie firewalli nowej generacji z serii NSa z punktami dostępowymi SonicWall SonicWave 802.11ac Wave 2 tworzy rozwiązanie szybkiej bezpiecznej sieci bezprzewodowej. Zarówno urządzenia Nsa, jak i SonicWave są wyposażone w porty 2,5 GbE, które zapewniają obsługę wielogigabitowej przepustowości bezprzewodowej technologii Wave 2. Firewall skanuje cały bezprzewodowy ruch przychodzący i wychodzący z sieci przy użyciu technologii Deep Packet Inspection, a następnie likwiduje zagrożenia, takie jak malware i próby włamania, nawet w połączeniach szyfrowanych. Można też uruchomić dodatkowe warstwy ochrony sieci WLAN, wykorzystując filtrowanie treści, kontrolę i inteligencję aplikacyjną oraz rozwiązanie Capture Advanced Threat Protection.



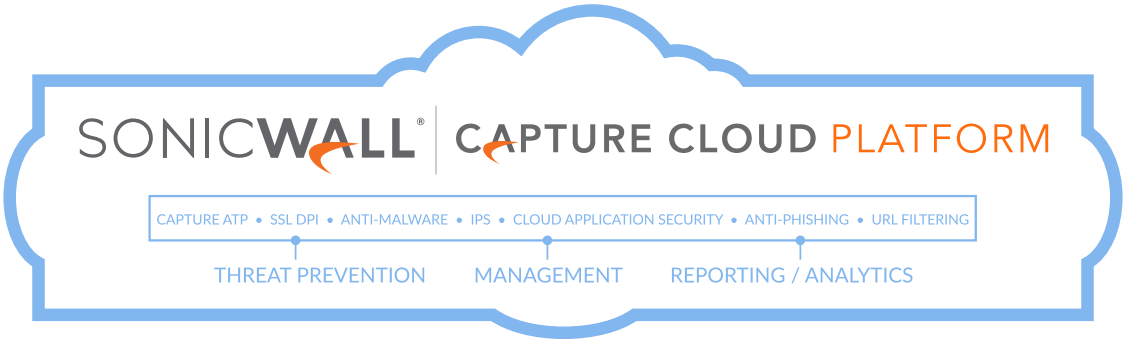
Capture Cloud Platform

Platforma SonicWall Capture Cloud zapewnia organizacjom dowolnej wielkości opartą na chmurze ochronę przed zagrożeniami i zarządzanie siecią, a dodatkowo raportowanie i analitykę. Platforma integruje threat intelligence, czyli zarządzanie informacjami o zagrożeniach zbieranymi z wielu źródeł, w tym z nagradzanej wielosilnikowej usługi sandboxingu - Capture Advanced Threat Protection, a także ponad miliona sensorów SonicWall rozmieszczonych na całym świecie.

Jeśli okaże się, że dane przychodzące do sieci zawierają nieznany wcześniej złośliwy kod, to Capture Labs - dedykowany firmowy zespół badawczy firmy SonicWall, opracowuje sygnaturę, która jest przechowywana w bazie danych Capture Cloud Platform i rozsyłana do firewalli klientów, zapewniając im aktualną ochronę. Nowe aktualizacje działają natychmiast bez restartów i przerw w pracy urządzeń. Sygnatury rezydujące na appliance chronią przed wieloma klasami ataków, przy czym pojedyncza sygnatura odnosi się do dziesiątek tysięcy poszczególnych zagrożeń.

Oprócz mechanizmów obrony dostępnych na urządzeniu firewalle NS*a* mają także stały dostęp do bazy danych Capture Cloud Platform, która rozszerza zasoby sygnaturowe o dziesiątki milionów sygnatur.

Capture Cloud Platform zapewnia nie tylko ochronę przed zagrożeniami, ale także pojedynczą konsolę zarządzania, dzięki której administratorzy mogą łatwo tworzyć raporty o aktywności sieciowej, zarówno w ujęciu czasu rzeczywistego, jak i historycznym.

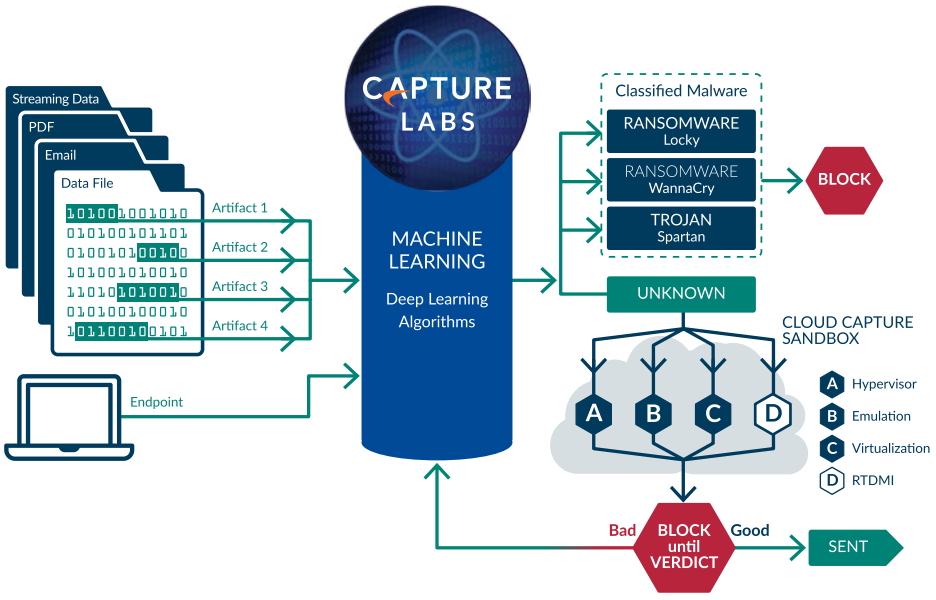


Zaawansowane ochrona przed zagrożeniami

W centrum automatyzowanej ochrony SonicWall przed włamaniami w czasie rzeczywistym działa usługa Capture Advanced Threat Protection, oparty na chmurze wielosilnikowy sandbox, który rozszerza bezpieczeństwo firewalli o wykrywanie i zapobieganie zagrożeniom typu zero-day. Podejrzane pliki są wysyłane do chmury, gdzie są analizowane przy użyciu algorytmów deep learningu, z blokowaniem ich na bramie, dopóki nie zostanie wydany werdykt. Wielosilnikowa platforma sandboxingu, która wykorzystuje technologię Real-Time Deep Memory Inspection, zwirtualizowany sandbox, pełną emulację systemu oraz analizę na poziomie wirtualizatora, uruchamia podejrzany kod i analizuje jego zachowanie. Kiedy plik jest uznawany za złośliwy, jest on blokowany i Capture ATP tworzy natychmiast jego hash. Zaraz potem sygnatura jest wysyłana do firewalli, by zapobiec dalszym atakom.

Usługa analizuje wiele rodzajów systemów operacyjnych oraz typów plików, w tym programów wykonywalnych, DLL, PDF, dokumentów MS Office, archiwów, JAR i APK.

Rozwiązanie SonicWall Capture Client łączy technologię antywirusa nowej generacji z opartym na chmurze i wielu silnikach sandboxingiem, tworząc kompletną ochronę punktów końcowych.

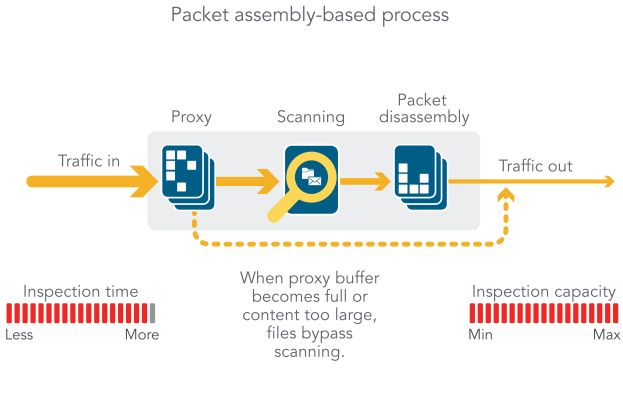


Mechanizm Reassembly-Free Deep Packet Inspection

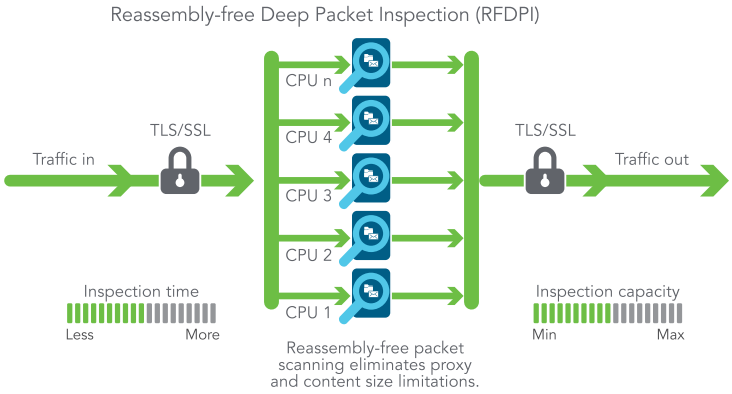
Technologia SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) to cechujący się małym opóźnieniem i działający w trybie single-pass system inspekcji, który przeprowadza opartą na strumieniu, dwukierunkowa analizę ruchu z dużą szybkością i bez użycia technik proxy i buforowania. W ten sposób efektywnie wykrywa próby włamań i pobrania malware'u, jednocześnie identyfikując ruch aplikacyjny bez względu na używany port i protokół. Ten firmowy mechanizm wykorzystuje inspekcję strumieni ruchu do wykrywania zagrożeń w warstwach 3-7 oraz poddaje strumienie szeroko zakrojonej, powtarzanej normalizacji i dekrypcji w celu neutralizowania technik przenikania, które próbują oszukać mechanizmy detekcji i wprowadzić złośliwy kod do sieci.

Kiedy pakiet przechodzi niezbędne wstępne procesowanie, w tym dekrypcję TLS/SSL, jest on analizowany w oparciu o jedną własną reprezentację złożoną z trzech baz danych sygnatur: ataków, malware i aplikacji. Połączenie jest następnie dalej procedowane pod kątem stanu strumienia w odniesieniu do tych baz danych, aż do wykrycia ataku lub innego pasującego przypadku, a wtedy uruchamiana jest wcześniej ustalona akcja.

W większości przypadków połączenie jest zakańczane i tworzone są odpowiednie logi i powiadomienia. Jednakże mechanizm może być także skonfigurowany wyłącznie do inspekcji lub (przy wykrywaniu aplikacji w celu zarządzania pasmem w warstwie 7) do zawiadamiania strumienia aplikacyjnego o zidentyfikowaniu aplikacji.



Competitive proxy-based architecture



SonicWall stream-based architecture

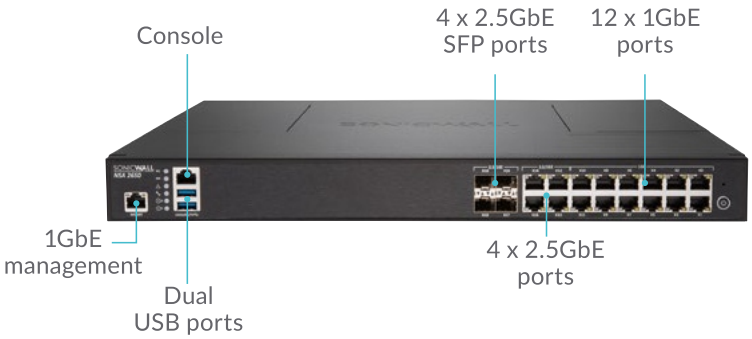
Globalne zarządzanie i raportowanie

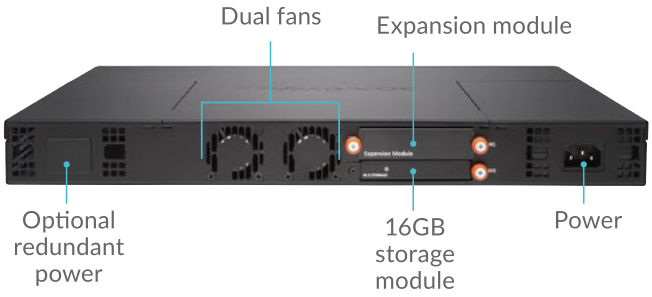
Administratorom w organizacjach w dużym stopniu regulowanym i z tego powodu wymagającym w pełni skoordynowanego zarządzania bezpieczeństwem, zgodnością ze standardami i ryzykiem firma SonicWall zapewnia zunifikowaną, bezpieczną i rozszerzalną platformę do administrowania firewallami SonicWall, bezprzewodowymi punktami dostępowymi i przełącznikami z serii Dell X-Series, udostępniającą skorelowany i audytowalny proces przepływu pracy. Przedsiębiorstwa mogą łatwo konsolidować zarządzanie urządzeniami ochrony, ograniczać złożoność administrowania i diagnostyki oraz kontrolować wszystkie operacyjne aspekty infrastruktury bezpieczeństwa, takie jak: scentralizowane zarządzanie i egzekwowanie polityk; monitorowanie w czasie rzeczywistym; aktywności użytkowników; identyfikowanie aplikacji; analityka przepływu i analiza śledcza; raportowanie pod kątem zgodności i audytów oraz wiele innych. Dodatkowo organizacje dostosowują się do wymaganych zmian w zarządzaniu firewallami, związanymi z automatyzacją przepływu pracy i zapewniającymi elastyczność oraz pewność we wdrażaniu właściwych polityk we właściwym czasie, w zgodzie z obowiązującymi regulacjami.

Rozwiązania do zarządzania i raportowania SonicWall, dostępne w formie on-premise jako SonicWall Global Management System oraz w chmurze jako Capture Security Center, oferują spójny sposób kontroli nad bezpieczeństwem sieciowym pod kątem procesów biznesowych i poziomów usługowych. Znakomicie upraszczają one zarządzanie cyklem życiowym w całym środowisku ochrony (w porównaniu do zarządzania skupionego na poszczególnych urządzeniach).

Network Security appliance NS*a* 2650

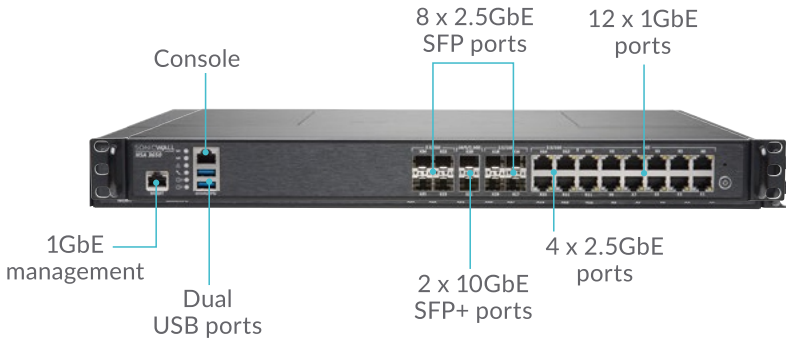
NS*a* 2650 zapewnia wydajną ochronę przed zagrożeniami, obsługując tysiące szyfrowanych połączeń (i wiele więcej nieszyfrowanych) w organizacjach średniej wielkości i rozproszonych przedsiębiorstwach.

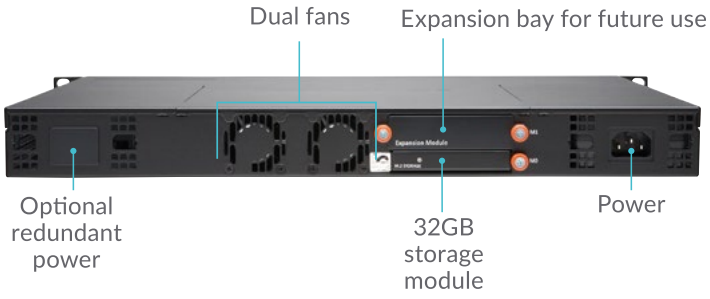




Network Security appliance NS*a* 3650

SonicWall NS*a* 3650 to idealne rozwiązanie dla biur oddziałowych i mniejszych oraz średnich środowisk korporacyjnych, w których ważna jest przepustowość sieci i wydajność.



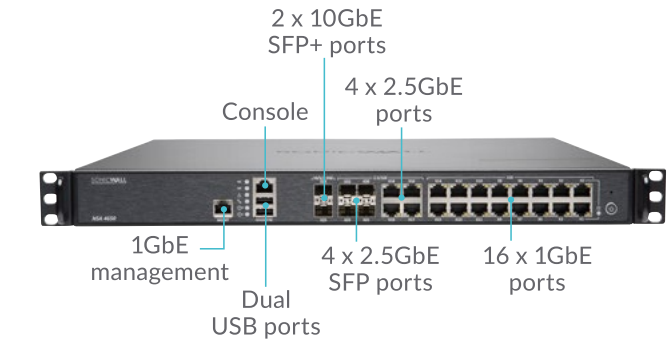


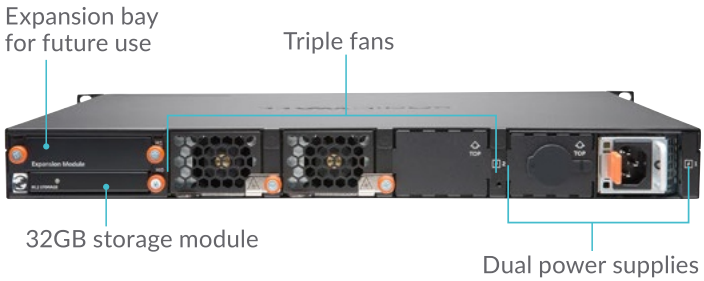
Firewall	NS*a* 2650
Przepustowość firewalla	3.0 Gbps
Przepustowość IPS	1.4 Gbps
Przepustowość antymalware	600 Mbps
Przepustowość Full DPI	600 Mbps
Przepustowość IMIX	700 Mbps
Maks. liczba połączeń DPI	500,000
Nowe połączenia/s	14,000/s
Opis	**SKU**
NS*a* 2650 - tylko firewall	01-SSC-1936
NS*a* 2650 TotalSecure Advanced (1 rok)	01-SSC-1988

Firewall	NS*a* 3650
Przepustowość firewalla	3.75 Gbps
Przepustowość IPS	1.8 Gbps
Przepustowość antymalware	800 Mbps
Przepustowość Full DPI	730 Mbps
Przepustowość IMIX	900 Mbps
Maks. liczba połączeń DPI	750,000
Nowe połączenia/s	14,000/s
Opis	**SKU**
NS*a* 3650 – tylko firewall	01-SSC-1937
NS*a* 3650 TotalSecure Advanced (1 -rok)	01-SSC-4081

Network Security appliance NS*a* 4650

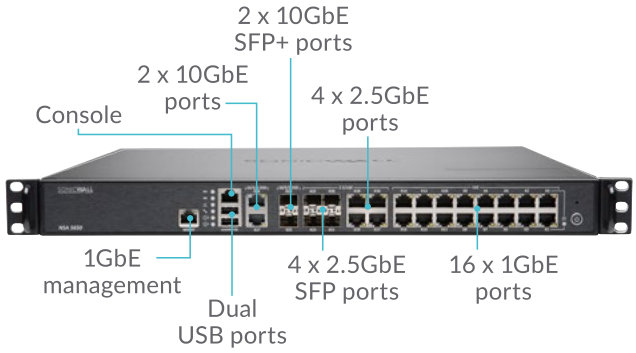
SonicWall NS*a* 4650 chroni rozwijające się organizacje średniej wielkości i biura oddziałowe, zapewniając funkcjonalność klasy Enterprise i bezkompromisową wydajność.

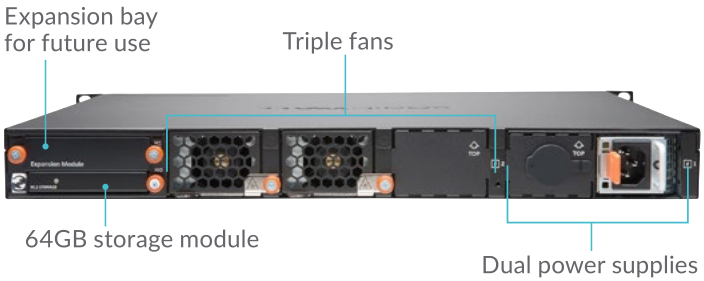




Network Security appliance NS*a* 5650

SonicWall NS*a* 5650 to idealne rozwiązanie dla rozproszonych środowisk korporacyjnych i biur oddziałowych, potrzebujących dużej wydajności i gęstości portów.





Firewall	NS*a* 4650
Przepustowość firewalla	6.0 Gbps
Przepustowość IPS	2.3 Gbps
Przepustowość antymalware	1.25 Gbps
Przepustowość Full DPI	1.2 Gbps
Przepustowość IMIX	1.3 Gbps
Maks. liczba połączeń DPI	1,000,000
Nowe połączenia/s	40,000/s
Description	**SKU**
NS*a* 4650 – tylko fire wall	01-SSC-1938
NS*a* 4650 TotalSecure Advanced (1 rok)	01-SSC-4094

Firewall	NS*a* 5650
Przepustowość firewalla	6.25 Gbps
Przepustowość IPS	3.4 Gbps
Przepustowość antymalware	1.7 Gbps
Przepustowość Full DPI	1.7 Gbps
Przepustowość IMIX	1.45 Gbps
Maks. liczba połączeń DPI	1,500,000
Nowe połączenia/s	40,000/sec
Description	**SKU**
NS*a* 5650 - tylko firewall	01-SSC-1939
NS*a* 5650 TotalSecure Advanced (1 rok)	01-SSC-4342

Funkcje

Mechanizm RFDPI	
Funkcja	Opis
Reassembly-Free Deep Packet Inspection (RFDPI)	Wysokowydajny, firmowy i opatentowany mechanizm inspekcji, który przeprowadza opartą na strumieniu dwukierun kową analizę ruchu (bez użycia P roxy i buforowania) w celu wykrycia prób włamania i m alware oraz identyfikowania ruchu aplikacji bez względu na używane porty.
Dwukierunkowa inspekcja	Skanuje pod kątem zagrożeń jednocześnie ruch wchodzący i wychodzący, by zagwarantować, że sieć nie jest wykorzy stywana do dystrybucji malware i nie stała się platformą do uruchamiania ataków w przypadku, gdy dołączono do niej zainfekowaną maszynę z zewnątrz.
Inspekcja oparta na strumieniu	Technologia inspekcji bez proxy i buforowania, która zapewnia ultra niskie o późnienia badanych przez DPI milionów jednoczesnych strumieni sieciowych. Nie wprowadza ograniczeń wielkości strumieni i może zastosowana w przypadku powszechnie wykorzystywanych protokołów oraz strumieni raw TCP.
Wysoka skalowalność i równoległość	Unikalna budowa mechanizmu RFDPI wykorzystuje wielordzeniową architekturę w celu zapewnienia dużej przepustowości DPI i ekstremalnie dużych prędkości ustanawiania nowych sesji w odpowiedzi na gwałtowne przyrosty ruchu w wymagających sieciach.
Inspekcja single-pass	Architektura single-pass DPI jednocześnie skanuje ruch pod kątem malware, włamań i identyfikacji aplikacji, co przekłada się na znaczne zmniejszenie opóźnień i pewność, że informacje o wszystkich zagrożeniach są korelowane w ramach pojedynczej architektury.
Firewall i networking	
Funkcja	Opis
REST API	Dzięki API firewalle mogą otrzymywać i wykorzystywać wszystkie informacje o zagrożeniach pochodzące ze wszystkich źródeł zewnętrznych w celu ochrony przed zaawansowanymi zagrożeniami, w rodzaju zero -day, wewnętrznych napastników, skompromitowanych danych uwierzytelniających, ransomware i APT (Advanced Persistent Threats).
Stateful Packet Inspection	Cały ruch sieciowy jest kontrolowany, analizowany i doprowadzany do zgodności ze standardami za pomocą po lityk dostępu na firewallach.
High availability/clustering	Seria NS*a* obsługuje tryby: Active/Passive (A/P) z synchronizacją stanu, DPI Active/Active (A/A) oraz wysokodostępny clustering Active/Active. DPI Active/Active odciąża mechanizm deep packet inspec tion na rdzeniach pasywnego appliance w celu zwiększenia przepustowości.
Ochrona przed atakami DDoS/DoS	Zabezpieczenie przed zalewem SYN chroni w przypadku ataku DoS, wykorzystując zarówno technikę Layer 3 SYN proxy, jak i Layer 2 SYN blacklisting. Dodatk owo zabezpiecza przed DoS/DDoS dzięki ochronie przed zalewem UDP/ICMP oraz ograniczaniu szybkości połączeń.
Obsługa IPv6	IPv6 (Internet Protocol version 6) stopniowo zastępuje IPv4. Dzięki SonicOS sprzęt będzie obsługiwał implementacje filtrowani a oraz trybu wire.
Opcje elastycznego wdrażania	Seria NS*a* może być wdrażana w trybach tradycyjnego NAT, Layer 2 bridge, wire i network tap.
WAN load balancing	Równoważy obciążenia na interfejsach WAN przy użyciu metod Round Robin, Spillover i Percentage.
Zaawansowane QoS (quality of service)	Zabezpiecza kluczową komunikację wykorzystująca 802.1p i tagowanie DSCP oraz remapuje ruch VoIP w sieci.
Obsługa H.323 gatekeeper i SIP proxy	Blokuje niechciane połączenia poprzez wymaganie, by wszystkie przychodzące rozmow y były autoryzowane i uwierzytelniane przez rozwiązania H.323 gatekeeper lub SIP proxy.
Zarządzanie pojedynczymi i kaskadowymi przełącznikami Dell X-Series	Zarządza ustawieniami bezpieczeństwa na dodatkowych portach, takich jak Portshield, HA, PoE and PoE +, przy użyciu pojedynczej konsoli wykorzystującej interfejs do zarządzania firewallem w przełącznikach sieciowych Dell X -Series.
Uwierzytelnianie biometryczne	Obsługuje uwierzytelnianie na urządzeniach mobilnych przy użyciu odcisku palca, dzięki czemu da ne uwierzytelniające nie mogą być łatwo powielone lub przekazane, co zwiększa bezpieczeństwo w dostępie do sieci.
Logowanie przez open authentication i serwisy społecznościowe	Umożliwia gościom w sieci wykorzystanie danych uwierzytelniających z serwisów s połecznościowych, takich Facebook, Twitter i Google+ do zalogowania się i uzyskania dostępu do Internetu lub innych usług gościnnych przy użyciu punktów dostępowych WiFi, LAN oraz stref DMZ oraz uwierzytelniania w trybie pass -through.
Zarządzanie i raport owanie	
Funkcja	Opis
Global Management System (GMS)	System GMS umożliwia monitorowanie, konfigurowanie i raportowanie na wielu urządzeniach SonicWall przy użyciu pojedynczej konsoli zarządzania z intuicyjnym interfejsem, ograniczając koszty zarządzania i jego złożoność.
Wydajne zarządzanie pojedynczym urządzeniem	Intuicyjny interfejs webowy umożliwia szybką i wygodną konfigurację (obok kompleksowego interfejsu CLI i obsługi SNMPv2/3).
Raportowanie przepływów aplikacyjnych poprzez IPFIX/NetFlow	Eksportuje analitykę ruchu aplikacyjnego i wykorzystania danych poprzez protokoły IPFIX lub NetFlow, zapewniając monitoring w ujęciu czasu rzeczywistego i historycznym przy użyciu SonicWall Scrutinizer i innych narzędzi obsługujących IPFIX i NetFlow .
Virtual private networking (VPN)	
Funkcja	Opis
Auto-provision VPN	Ułatwia i ogranicza złożoność wdrażania rozproszonych firewalli poprzez automatyzację wstępnego konfigurowania bramy VPN w trybie site-to-site pomiędzy firewallami, w wyniku czego natychmiast i autom atycznie ustanawiana jest ochrona oraz komunikacja.
VPN IPSec dla komunikacji site-to-site	Dzięki wysokowydajnemu rozwiązaniu VPN IPSec seria NS *a* może pracować jako koncentrator VPN dla tysięcy innych dużych lokalizacji, biur oddziałowych i domowych.
Zdalny dostęp przez VPN SSL lub klienta IPSec	Bezklientowa technologia VPN SSL lub prosty w użyciu klient IPSec umożliwiają łatwy dostęp do poczty email, plików, komputerów, serwisów intranetowych oraz aplikacji z różnych platform.
Redundantna brama VPN	Kiedy wykorzystuje się wiele sieci WAN, można skonfigurować główny i zapasowy VPN tak, by zapewniały płynne i automatyczne odzyskiwanie i utrzymanie wszystkich sesji VPN w razie awarii (failover and failback).
Route-based VPN	Możliwość przeprowadzania dynami cznego routingu przez łącza VPN zapewnia stałą dostępność na wypadek czasowego uszkodzenia tunelu VPB (płynny re-routing ruchu między punktami końcowymi przy użyciu tras alternatywnych).

Monitoring treści/kontekstu	
Funkcja	Opis
Śledzenie akty wności użytkowników	Identyfikacja użytkownika i aktywności jest zapewniana poprzez płynną integrację SSO AD/LDAP/Citrix1/Terminal Services, w połączeniu z obszerną informacją dostarczaną przez DPI.
Identyfikacja pochodzenia ruchu poprzez GeoIP	Identyfiku je i kontroluje ruch sieciowy przychodzący i wychodzący do szczególnych krajów w celu ochrony przed atakami ze znanych z zagrożeń i podejrzanych źródeł oraz śledzenia podejrzanego ruchu, który pochodzi z sieci. Możliwe jest samodzielne dodanie krajów i lis t botnetów oraz usunięcie niewłaściwego kraju i tagów botnetu przypisanych do adresów IP. Eliminuje niewłaściwe filtrowanie adresów IP spowodowane złą klasyfikacją.
DPI z filtrowaniem wyrażeń regularnych	Zapobiega wyciekowi danych poprzez identyfikowanie i kontrolowanie treści przechodzących przez sieć metodą dopasowywanie wyrażeń regularnych.

Oparte na subskrypcji usługi ochrony przed włamaniami

Capture Advanced Threat Protection	
Funkcja	Opis
Wielosilnikowy sandboxing	Wielosilnikowa platforma sandb oxingu, która obejmuje zwirtualizowany sandbox, emulację pełnego systemu oraz analizę na poziomie wirtualizatora, wykonuje podejrzany kod i bada jego zachowanie, zapewniając kompleksowy wgląd w złośliwą aktywność.
Real-Time Deep Memory Inspection (RTDMI)	Oczekująca na opatentowanie technologia oparta na chmurze wykrywa i blokuje malware, który nie przejawia złośliwej aktywności i ukrywa się poprzez szyfrowanie. Poprzez zmuszenie malware do ujawnienia swoich złośliwych mechanizmów arsenału w pamięci operacy jnej mechanizm RTDMI proaktywnie wykrywa i blokuje nieznane dotąd zagrożenia typu zero -day.
Blokowanie do werdyktu	Aby zapobiec przedostawaniu się do sieci potencjalnie złośliwego oprogramowania, wysyłane do chmury w celu analizy pliki są przetrzymywane n a bramie aż do momentu wydania werdyktu o ich szkodliwości.
Analiza wielu rodzajów i rozmiarów plików	Analizowanie wielu rodzajów plików, w tym: programów wykonywalnych, DLL, PDF, dokumentów MS Office, archiwów, JAR i APK, oraz wielu systemów operacyjnych , takich jak: Windows, Android, Mac OS X i środowiska wielu przeglądarek.
Szybkie wdrażanie sygnatur	Kiedy plik jest identyfikowany jako złośliwy, natychmiast jego sygnatura jest wdrażana na firewallach w ramach subskrypcji SonicWall Capture ATP, a bazy s ygnatur bramy antywirusowej, IPS, baz URL, IP oraz reputacji domen zostają zaktualizowane w ciągu 48 godz.
Capture Client	Capture Client to zunifikowana platforma kliencka, która zapewnia wiele funkcji bezpieczeństwa punktów końcowych, w tym zaawansowaną ochronę przed malware oraz obsługę wglądu w ruch zaszyfrowany. Wykorzystuje technologie ochrony warstwowej, kompleksowe raportowanie i egzekwowanie ochrony punktów końcowych.
Ochrona przed atakami wykorzystującymi szyfrowanie	
Funkcja	Opis
Dekrypcja i inspekcja TLS/SSL	Dokonuje dekrypcji i inspekcji zaszyfrowanego ruchu TLS/SSL w locie i bez proxy, chroniąc przed malware, włamaniami i wyciekiem danych. Korzysta z polityk aplikacyjnych, kontroli URL i treści, by chronić przed zagrożeniami ukrywającymi si ę w ruchu zaszyfrowanym. Wchodzi w skład subskrypcji ochrony dla wszystkich modeli serii NS *a*.
Inspekcja SSH	Technologia DPI -SSH (Deep Packet Inspection of SSH) przeprowadza dekrypcję i inspekcję danych przechodzących przez tunel SSH, chroniąc przed atakam i wykorzystującymi takie połączenia.
Ochrona przed włamaniami	
Funkcja	Opis
Ochrona oparta na przeciwdziałaniu	Ściśle zintegrowany system IPS (iIntrusion Prevention System) wykorzystuje sygnatury i inne mechanizmy obrony do skanowania pakietów pod kąt em luk i exploitów, obejmując szerokie spektrum ataków i podatności.
Automatyczne aktualizacje sygnatur	SonicWall Threat Research Team stale opracowuje i wdraża aktualizacje dla obszernego zestawu mechanizmów obrony w IPS, przygotowanego dla ponad 50 kat egorii ataków. Nowe aktualizacje zaczynają działać natychmiast, bez potrzeby restartu czy przerwy w pracy urządzenia.
Ochrona IPS intra -zone	Zwiększa bezpieczeństwo wewnętrzne poprzez segmentację sieci na wiele stref bezpieczeństwa z ochroną przed właman iami. Zapobiega propagacji zagrożeń poza granice stref.
Detekcja oraz blokowanie botnetów i ruchu command and control (C&C)	Identyfikuje i blokuje ruch C&C pochodzący z botnetów w sieci lokalnej do domen i adresów IP, które są zidentyfikowane jako rozpowszechniające malware lub znane jako ośrodki C&C.
Anomalie i nadużycia protokołów	Identyfikuje i blokuje ataki, które wykorzystują protokoły, aby przeniknąć przez system IPS.
Ochrona zero -day	Chroni sieć przed atakami zero -day, korzystając z ciągłych aktualizacji dotyczących nowych metod wykorzystania exploitów oraz technik zabezpieczających przed tysiącami rodzajów exploitów.
Technologia anti -evasion	Ekstensywna normalizacja strumienia, dekod owanie i inne mechanizmy zapobiegają przedostaniu się do sieci zagrożeń stosujących techniki utrudniające ich wykrycie w warstwach 2 -7.
Ochrona przed zagrożeniami	
Funkcja	Opis
Brama antymalware	Mechanizm RFDPI skanuje cały ruch wchodzący, wychodzący o raz wewnętrzny pod kątem wirusów, Trojanów, key loggerów i innego rodzaju malware w plikach o nieograniczone długości i rozmiarze ma wszystkich portach i strumieniach TCP.
Ochrona przed malware Capture Cloud	Nieustannie aktualizowana baza danych z dzies iątkami milionów sygnatur zagrożeń, rezydująca na chmurowych serwerach SonicWall, jest referencją dla lokalnych baz sygnatur, zwiększając ochronę i możliwości mechanizmu RFDPI w zwalczaniu zagrożeń.
Ciągłe aktualizacje bezpieczeństwa	Nowe aktualizacje zag rożeń są automatycznie przekazywane firewallom z aktywnymi usługami bezpieczeństwa i zaczynają działać natychmiast, bez potrzeby restartu czy przerwy w pracy urządzeń.
Dwukierunkowa inspekcja raw TCP	Mechanizm RFDPI może skanować strumienie raw TCP dwuki erunkowo na dowolnym porcie, zapobiegając atakom, które wykorzystują przestarzałe systemy bezpieczeństwa, chroniące tylko wybrane, dobrze znane porty.
Obszerne wsparcie dla protokołów	Identyfikuje powszechnie wykorzystywane protokoły, takie jak HTTP/S, FT P, SMTP, SMBv1/v2 oraz inne, które nie przesyłają danych w raw TCP. Dekoduje ruch w celu inspekcji malware, nawet jeśli nie są wykorzystywane standardowe, dobrze znane porty.

Inteligencja i kontrola aplikacyjna	
Funkcja	Opis
Kontrola aplikacyjna	Kontroluje aplikacje lub poszczególne ich funkcje, które zostały zidentyfikowane przez mechanizm RFDPI na podstawie stale uzupełnianej bazy tysięcy sygnatur aplikacyjnych, zwiększając bezpieczeństwo i wydajność sieci.
Identyfikacja własnych aplikacji	Kontrola własnych aplikacji przez tworzenie sygnatur w oparciu w specyficzne parametry i unikalne wzory w komunikacji sieciowej aplikacji, w celu zwiększenia kontroli nad siecią.
Zarządzanie pasmem aplikacji	Granularna alokacja i regulacja dostępnego pasma dla kluczowych aplikacji lub kategorii aplikacji przy spowalnianiu mniej istotnego ruchu.
Kontrola granularna	Kontrola aplikacji lub specyficznych komponentów aplikacji w oparciu o harmonogramy, grupy użytkowników, listy wykluczeń i wybór działań, z pełną identyfikacją SSO użytkownika poprzez integrację z usługami LDAP/AD/Terminal Services/Citrix.
Filtrowanie treści	
Funkcja	Opis
Filtrowanie treści	Realizuje przy użyciu usług Content Filtering Service polityki wykorzystania WWW i blokuje dostęp do stron internetowych zawierających informacje bądź grafiki, które są niewłaściwe bądź nieproduktywne.
Enforced Content Filtering Client	Rozszerza egzekwowanie polityk, blokując treści internetowe na urządzeniach Windows, Mac OS, Android i Chrome OS, znajdujących się poza granicą chronioną przez firewall.
Kontrola granularna	Blokuje treści na podstawie predefiniowanych kategorii lub ich dowolnej kombinacji. Filtrowanie może być ustalone według pór dnia, takich jak godziny pracy bądź nauki, i stosowane w odniesieniu do poszczególnych użytkowników bądź ich grup.
Web caching	Klasyfikacja URL jest przechowywana lokalnie w pamięci firewalli SonicWall, więc czas odpowiedzi dotyczący dostępu do odwiedzanych stron lub jego braku to ułamki sekund.
Antywirus i antyspyware	
Funkcja	Opis
Ochrona wielowarstwowa	Wykorzystuje funkcjonalności firewalla jako pierwszą warstwę obrony granicznej w połączeniu z ochroną punktów końcowych do blokowania złośliwego oprogramowania przedostającego się do sieci z laptopów, pamięci USB i innych niechronionych systemów.
Opcja automatycznego egzekwowania	Zapewnia, by każdy komputer uzyskujący dostęp do sieci dysponował odpowiednim oprogramowaniem antywirusowym i/lub zainstalowanym i aktywnym certyfikatem DPI-SSL, co ogranicza koszty typowych działań w zarządzaniu ochroną antywirusową.
Opcja automatycznego wdrażania i instalacji	Wdrażanie i instalacja klientów antywirusowych i antyspyware na kolejnych maszynach następują automatycznie w całej sieci, co redukuje pracę administratorów.
Antywirus nowej generacji	Capture Client wykorzystuje mechanizm statycznej sztucznej inteligencji (AI) do wykrywania zagrożeń, zanim zaczną być aktywne oraz umożliwia przywracanie systemu do poprzedniego stanu przed infekcją.
Ochrona przed spyware	Wydajna ochrona antyspyware skanuje i blokuje instalowanie szerokiego spektrum programów szpiegowskich na komputerach stacjonarnych i laptopach, zanim zaczną one transmitować poufne dane.

Podsumowanie funkcjonalności SonicOS

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- Ochrona przed DDoS (UDP/ICMP/SYN flood)
- Obsługa IPv4/IPv6
- Biometryczne uwierzytelnianie w zdalnym dostępie
- DNS proxy
- REST APIs

Dekrypcja i inspekcja TLS/SSL/SSH[1]

- Deep packet inspection dla TLS/SSL/SSH
- Włączanie/wyłączanie obiektów, grup lub nazw hostów
- Kontrola TLS/SSL

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- Oparta na chmurze wielosilnikowa analiza
- Zwirtulizowany sandboxing
- Analiza na poziomie wirtualizatora
- Emulacja pełnego systemu
- Sprawdzanie wielu typów plików
- Zautomatyzowane albo ręczne dodawanie
- Aktualizacje threat intelligence w czasie rzeczywistym
- Blokowanie do werdyktu
- Capture Client

Ochrona przed włamaniami[1]

- Skanowanie sygnaturowe
- Automatyczne aktualizacje sygnatur
- Inspekcja dwukierunkowa
- Granularne reguły IPS
- Ochrona z GeoIP
- Filtrowanie botnetów i dynamiczne listy
- Dopasowywanie wyrażeń regularnych

Antymalware[1]

- Skanowanie malware oparte na strumieniu
- Brama antywirusowa
- Brama antyspyware
- Inspekcja dwukierunkowa
- Bez ograniczeń wielkości plików
- Chmurowa baza danych malware

Identyfikacja aplikacji[1]

- Kontrola aplikacji
- Zarządzanie pasmem aplikacji
- Własne tworzenie sygnatur aplikacji
- DLP (Data Leakage Prevention)
- Raportowanie aplikacji przez NetFlow/IPFIX
- Kompleksowa baza sygnatur aplikacji

Wizualizacja i analityka ruchu

- Aktywność użytkownika
- Wykorzystanie aplikacji
- Analityka oparta na chmurze

Web content filtering[1]

- Filtrowanie URL
- Technologia anti-proxy
- Blokowanie słów kluczowych
- Wprowadzanie nagłówków HTTP
- Zarządzanie pasmem na podstawie kategorii ratingu CFS
- Ujednolicony model polityk w kontroli aplikacji
- Content Filtering Client

VPN

- Auto-provisioning VPN
- IPSec VPN dla komunikacji site-to-site
- SSL VPN i klient zdalnego dostępu IPSec
- Redundantna brama VPN
- Mobile Connect dla iOS, Mac OS X, Windows, Chrome, Android i Kindle Fire
- Route-based VPN (OSPF, RIP, BGP)

Networking

- PortShield
- Ramki Jumbo
- Rozszerzone logowanie
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Port mirroring
- Layer-2 QoS
- Bezpieczeństwo portów
- Dynamiczny routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DNS/DNS proxy
- Serwer DHCP
- Zarządzanie pasmem
- Link aggregation (static and dynamic)
- Redundancja portów
- A/P high availability i state sync
- A/A clustering
- load balancing inbound/outbound
- L2 bridge, wire/virtual wire mode, tap mode
- failover 3G/4G WAN
- Asymetryczny routing
- Obsługa Common Access Card (CAC)

Wireless

- WIDS/WIPS
- Analiza spektrum RF
- Ochrona przed rogue AP
- Widok planu piętra
- Widok topologii
- Band steering
- Beamforming
- AirTime fairness
- Extender MiFi
- Guest cyclic quota
- Portal gościnny LHM

VoIP

- Granularna kontrola QoS
- Zarządzanie pasmem
- Transformacja SIP i H.323 według reguł dostępu
- Obsługa H.323 gatekeeper i SIP proxy

Zarządzanie i monitoring

- Capture Security Center, GMS, Web UI, CLI, REST APIs, SNMPv2/v3
- Logowanie
- Eksportowanie Netflow/IPFix
- Oparty na chmurze backup konfiguracji
- BlueCoat Security Analytics Platform
- Zarządzanie punktami dostępowymi SonicWall
- Zarządzanie przełącznikami Dell X-Series, także kaskadami

[1] *Wymaga dodatkowej subskrypcji*

SONICWALL

Specyfikacje serii NS*a*

Firewall	NS*a* 2650	NS*a* 3650	NS*a* 4650	NS*a* 5650
Operating system	SonicOS 6.5.1			
Security processing cores	4	4	10	10
Interfaces	4 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 8 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console
Expansion	1 Expansion Slot (Rear)*			
Built-in storage	16 GB	32 GB	32 GB	64 GB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs			
SSO users	40,000	50,000	60,000	70,000
Maximum access points supported	48	96	128	192
Logging	Analyzer, Local Log, Syslog			
Firewall/VPN Performance	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
Firewall inspection throughput [1]	3.0 Gbps	3.75 Gbps	6.0 Gbps	6.25 Gbps
Full DPI throughput [2]	600 Mbps	730 Mbps	1.2 Gbps	1.7 Gbps
Application inspection throughput [2]	1.4 Gbps	2.1 Gbps	3.0 Gbps	4.25 Gbps
IPS throughput [2]	1.4 Gbps	1.8 Gbps	2.3 Gbps	3.4 Gbps
Anti-malware inspection throughput [2]	600 Mbps	800 Mbps	1.25 Gbps	1.7 Gbps
IMIX throughput	700 Mbps	900 Mbps	1.3 Gbps	1.45 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL) [2]	250 Mbps	300 Mbps	500 Mbps	800 Mbps
VPN throughput [3]	1.3 Gbps	1.5 Gbps	3.0 Gbps	3.5 Gbps
Connections per second	14,000/sec	14,000/sec	40,000/sec	40,000/sec
Maximum connections (SPI)	1,000,000	2,000,000	3,000,000	4,000,000
Maximum connections (DPI)	500,000	750,000	1,000,000	1,500,000
Maximum connections (DPI SSL)	18,000	24,000	30,000	37,000
Default connections (DPI/DPI SSL) [4]	500,000/12,000	625,000/15,000	750,000/18,000	1,000,000/19,000
VPN	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
Site-to-site tunnels	1,000	3,000	4,000	6,000
IPSec VPN clients (max)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN NetExtender clients (max)	2 (350)	2 (500)	2 (1,000)	2 (1,500)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256 -bit)/MD5, SHA-1, Suite B Cryptography			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF, BGP			
Networking	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
IP address assignment	Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode			
VLAN interfaces	256	256	400	500
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy -based routing			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications (in progress)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL, USGv6, CsFC			
High availability	Active/Passive with State Sync	Active/Passive with State Sync Active/Active Clustering		Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering
Hardware	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
Power supply	Dual, redundant 120W (one included)		Dual, redundant 350W (one included)	
Fans	Dual, Fixed		Triple, Removable	
Input power	100-240 VAC, 60-50 Hz			
Maximum power consumption (W)	37.2	46.0	93.6	103.6
[illegible]	162,231	156,681	154,529	153,243
MTBF @25°C in years	18.5	17.9	17.6	17.5
Form factor	1U Rack Mountable			
Dimensions	16.9 x 12.8 x 1.8 in (43 x 32.5 x 4.5 cm)		16.9 x 16.3 x 1.8 in (43 x 41.5 x 4.5 cm)	
Weight	11.5 lb (5.2 kg)	11.7 lb (5.3 kg)	15.2 lb (6.9 kg)	15.2 lb (6.9 kg)
WEEE weight	12.1 lb (5.5 kg)	12.3 lb (5.6 kg)	19.6 lb (8.9 kg)	19.6 lb (8.9 kg)
Shipping weight	17.0 lb (7.7 kg)	17.2 lb (7.8 kg)	24.9 lb (11.3 kg)	24.9 lb (11.3 kg)
Major regulatory	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI			
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)			
Humidity	10-90% non-condensing			

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] Full DPI/GatewayAV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. DPI SSL performance measured on HTTPS traffic with IPS enabled.
[3] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.
[4] For every 125,000 DPI connections reduced, the number of available DPI SSL connections increases by 3,000.
**Future use. All specifications, features and availability are subject to change.*

Specyfikacja serii NSA (starszej)

Firewall general	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Operating system	SonicOS 6.5.1				
Security processing cores	4	6	8	10	24
Interfaces	8 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 4 x 1-GbE SFP, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 4 x 1-GbE SFP, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 4 x 1-GbE SFP, 12 x 1-GbE, 1 GbE Management, 1 Console	4 x 10-GbE SFP+, 8 x 1-GbE SFP, 8 x 1-GbE, 1 GbE Management, 1 Console
Expansion	1 Expansion Slot (Rear)*, SD Card*				
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs				
SSO users	30,000	40,000	50,000	60,000	70,000
Maximum access points supported	32	48	64	96	128
Logging	Analyzer, Local Log, Syslog				
Firewall/VPN Performance	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Firewall inspection throughput[1]	1.9 Gbps	3.4 Gbps	6.0 Gbps	9.0 Gbps	12.0 Gbps
Full DPI throughput[2]	300 Mbps	500 Mbps	800 Mbps	1.6 Gbps	3.0 Gbps
Application inspection throughput[2]	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
IPS throughput[2]	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
Anti-malware inspection throughput[2]	400 Mbps	600 Mbps	1.1 Gbps	1.7 Gbps	3.0 Gbps
IMIX throughput	600 Mbps	900 Mbps	1.6 Gbps	2.4 Gbps	3.5 Gbps
TLS/SSL decryption and inspection (DPI SSL)[2]	200 Mbps	300 Mbps	500 Mbps	800 Mbps	1.3 Gbps
VPN throughput[3]	1.1 Gbps	1.5 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps
Connections per second	15,000/sec	20,000/sec	40,000/sec	60,000/sec	90,000/sec
Maximum connections (SPI)	500,000	750,000	1,000,000	1,500,000	1,500,000
Maximum connections (DPI)[4]	250,000	375,000	500,000	1,000,000	1,000,000
Default/Maximum connections (DPI SSL)[4]	1,000/1,000	2,000/2,750	3,000/4,500	4,000/8,500	6,000/10,500
VPN	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Site-to-site VPN tunnels	250	1,000	3,000	4,000	6,000
IPSec VPN clients (max)	10 (250)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN NetExtender clients (max)	2 (250)	2 (350)	2 (500)	2 (1,000)	2 (1,500)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v				
Route-based VPN	RIP, OSPF, BGP				
Networking	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
IP address assignment	Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay				
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode				
VLAN interfaces	256	256	256	400	500
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing				
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p				
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)				
VoIP	Full H323-v1-5, SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certifications	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL				
High availability	Active/Passive with State Sync	Active/Passive with State Sync Active/Active Clustering		Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering	
Hardware	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Power supply	Single, Fixed 200W	Single, Fixed 250W			
Fans	Dual, Fixed				Dual, redundant, hot swappable
Input power	100-240 VAC, 60-50 Hz				
Maximum power consumption (W)	49.4	74.3	86.7	90.9	113.1
MTBF @25°C in hours	176,540	146,789	139,783	134,900	116,477
MTBF @25°C in years	20.15	16.76	15.96	15.40	13.30
Form factor	1U Rack Mountable				
Dimensions	1.75 x 10.25 x 17 in (4.5 x 26 x 43 cm)	1.75 x 19.1 x 17 in (4.5 x 48.5 x 43 cm)			
Weight	10.1 lb (4.6 kg)	13.56 lb (6.15 kg)			14.93 lb (6.77 kg)
WEEE weight	11.0 lb (5.0 kg)	14.24 lb (6.46 kg)			19.78 lb (8.97 kg)
Shipping weight	14.3 lb (6.5 kg)	20.79lb (9.43 kg)			26.12 lb (11.85 kg)
Major regulatory	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI, CU				
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)				
Humidity	10-90% non-condensing				

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] Full DPI/GatewayAV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs.
[3] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.
[4] For every 125,000 DPI connections reduced, the number of available DPI SSL connections increases by 750.
**Future use. All specifications, features and availability are subject to change.*

Informacje do zamówień serii NS*a*

NS*a* 2650	SKU
NS*a* 2650 TotalSecure Advanced Edition (1 rok)	01-SSC-1988
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS*a* 2650 (1 rok)	01-SSC-1783
Capture Advanced Threat Protection for NS *a* 2650 (1 rok)	01-SSC-1935
Threat Prevention –Intrusion Prevention, Gateway Anti -Virus, Gateway Anti -Spyware, Cloud Anti -Virus for NS*a* 2650 (1 rok)	01-SSC-1976
24x7 Support for NS*a* 2650 (1 rok)	01-SSC-1541
Content Filtering Service for NS *a* 2650 (1 rok)	01-SSC-1970
Enforced Client Anti -Virus & Anti -Spyware	Based on user count
Comprehensive Anti -Spam Service for NS *a* 2650 (1 rok)	01-SSC-2001
NS*a* 3650	**SKU**
NS*a* 3650 TotalSecure Advanced Edition (1 rok)	01-SSC-4081
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *a* 3650 (1 rok)	01-SSC-3451
Capture Advanced Threat Protection for NS *a* 3650 (1 rok)	01-SSC-3457
Threat Prevention –Intrusion Prevention, Gateway Anti -Virus, Gateway Anti -Spyware, Cloud Anti -Virus for NS*a* 3650 (1 rok)	01-SSC-3632
24x7 Support for NS *a* 3650 (1 rok)	01-SSC-3439
Content Filtering Service for NS *a* 3650 (1 rok)	01-SSC-3469
Enforced Client Anti -Virus & Anti -Spyware	Based on user count
Comprehensive Anti -Spam Service for NS *a* 3650 (1 rok)	01-SSC-4030
NS*a* 4650	**SKU**
NS*a* 4650 TotalSecure Advanced Edition (1 rok)	01-SSC-4094
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filter ing and 24x7 Support for NS *a* 4650 (1 rok)	01-SSC-3493
Capture Advanced Threat Protection for NS *a* 4650 (1 rok)	01-SSC-3499
Threat Prevention –Intrusion Prevention, Gateway Anti -Virus, Gateway Anti -Spyware, Cloud Anti -Virus for NS*a* 4650 (1 rok)	01-SSC-3589
24x7 Support for NS *a* 4650 (1 rok)	01-SSC-3487
Content Filtering Service for NS *a* 4650 (1 rok)	01-SSC-3583
Enforced Client Anti -Virus & Anti -Spyware	Based on user count
Comprehensive Anti -Spam Service for NS *a* 4650 (1 rok)	01-SSC-4062
NS*a* 5650	**SKU**
NS*a* 5650 TotalSecure Advanced Edition (1 rok)	01-SSC-4342
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *a* 5650 (1 rok)	01-SSC-3674
Capture Advanced Threat Protection for NS *a* 5650 (1 rok)	01-SSC-3680
Threat Prevention – Intrusion Prevention, Gateway Anti -Virus, Gateway Anti -Spyware, Cloud Anti -Virus for NS*a* 5650 (1 rok)	01-SSC-3698
24x7 Support for NS *a* 5650 (1 rok)	01-SSC-3660
Content Filtering Service for NS *a* 5650 (1 rok)	01-SSC-3692
Enforced Cli ent Anti -Virus & Anti -Spyware	Based on user count
Comprehensive Anti -Spam Service for NS *a* 5650 (1 rok)	01-SSC-4068
Moduły i akcesoria*	**SKU**
10GBASE -SR SFP+ Short Reach Module	01-SSC-9785
10GBASE -LR SFP+ Long Reach Module	01-SSC-9786
10GBASE SFP+ 1M Twi nax Cable	01-SSC-9787
10GBASE SFP+ 3M Twinax Cable	01-SSC-9788
1000BASE -SX SFP Short Haul Module	01-SSC-9789
1000BASE -LX SFP Long Haul Module	01-SSC-9790
1000BASE -T SFP Copper Module	01-SSC-9791

**Pełna lista obsługiwanych modułów SFP i SFP+ u lokalnego przedstawiciela SonicWall*

Numery modeli:

NS*a* 2650 - 1RK38-0C8
NS*a* 3650 - 1RK38-0C7
NS*a* 4650 - 1RK39-0C9
NS*a* 5650 - 1RK39-0CA

O firmie

SonicWall od ponad 27 lat zapobiega cyberprzestępstwom, broniąc małe i średnie przedsiębiorstwa oraz korporacje na całym świecie. Połączony potencjał produktów i partnerów tworzy ochronę w czasie rzeczywistym, dostosowaną do indywidulanych potrzeb ponad 500 tys. firm z przeszło 200 krajów. Z SonicWall można bez obaw rozwijać swój biznes.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-NetworkSecurityAppliance-US-KJ-MKTG1745

SONICWALL