Seria SonicWall TZ

Wyjątkowa ochrona i znakomita wydajność przy niezwykle niskim TCO

Seria SonicWall TZ rozwiązań UTM (Unified Threat Management) została doskonale dopasowana do wymagań każdej organizacji, która potrzebuje bezpieczeństwa klasy Enterprise.

Firewalle z serii SonicWall TZ zapewniają szerokie spektrum ochrony opartej na zaawansowanych usługach bezpieczeństwa, takich jak lokalna i wykorzystująca chmurę ochrona antymalware i antyspyware, kontrola aplikacyjna, chroniący przed włamaniami system IPS (Intrusion Prevention System) i filtrowanie URL. W odpowiedzi na szybko rosnącą liczbę nowych wykorzystujących szyfrowanie ataków, seria TZ dysponuje odpowiednią mocą obliczeniową do inspekcji zaszyfrowanych połączeń SSL/TLS. Przy połączeniu z przełącznikami Dell X-Series wybrane modele serii TZ mogą bezpośrednio zarządzać bezpieczeństwem tych dodatkowych portów.

Wspierana przez SonicWall Capture Threat Network seria SonicWall TZ zapewnia stałe aktualizacje bezpieczeństwa, oferując zaawansowaną ochronę sieci przed cyberprzestępcami. Firewalle platformy TZ mogą skanować każdy bajt każdego pakietu bez względu na port, protokół i rozmiar plików, przy niemal zerowym opóźnieniu.

Seria SonicWall TZ oferuje porty Gigabit Ethernet, opcjonalną zintegrowaną technologię bezprzewodową 802.11ac*, połączenia VPN IPSec oraz SSL, funkcję failover opartą na łączności 3G/4G, load balancing i segmentację sieci. Rozwiązania UTM z serii TZ zapewniają szybki i bezpieczny dostęp mobilny urządzeniom wielu platform: Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X i Linux.

Rozwiązanie SonicWall Global Management System (GMS) umożliwia centralne wdrażanie i zarządzanie firewallami z serii SonicWall TZ przy użyciu jednego systemu.

Zarządzane bezpieczeństwo dla rozproszonych środowisk

Szkoły, sklepy detaliczne, zdalne lokalizacje, biura oddziałowe i rozproszone przedsiębiorstwa potrzebują rozwiązania, które będzie się integrować z firewallami w ich centralach. Urządzenia z serii SonicWall TZ współdzielą ten sam kod (i tę samą ochronę) z flagowym rozwiązaniem SonicWall - firewallami nowej generacji SuperMassive. Upraszcza to zarzadzanie zdalnymi lokalizacjami, ponieważ każdy administrator ma do dyspozycji ten sam interfejs użytkownika. GMS umożliwia działom IT konfigurowanie, monitorowanie i zarządzanie zdalnymi firewallami SonicWall przy użyciu pojedynczej konsoli. Poprzez dodanie szybkiej i bezpiecznej sieci bezprzewodowej seria SonicWall TZ rozszerza granice chronionego środowiska, dołączając do niego klientów i gości odwiedzających placówkę handlową albo zdalne biuro.

Korzyści:

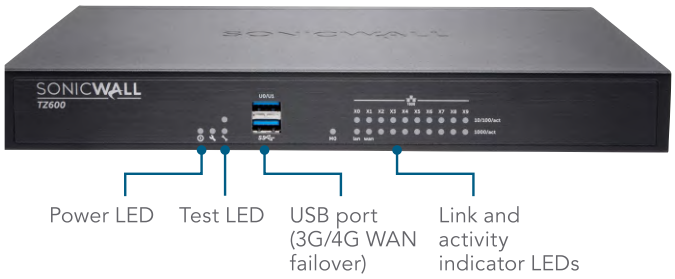
- Ochrona sieciowa klasy Enterprise
- Inspekcja DPI (Deep Packet Inspection) całego ruchu, bez ograniczeń co do rozmiaru plików i protokołu
- Bezpieczna komunikacja bezprzewodowa Secure 802.11ac z wykorzystanie zintegrowanego kontrolera bezprzewodowego lub poprzez zewnętrzne bezprzewodowe punkty dostępowe SonicPoint/SonicWave
- Mobilny dostęp SSL VPN dla urządzeń Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS i Linux
- Możliwość bezpiecznego zarządzania dodatkowymi 100 portami z konsoli TZ przy wdrożeniu łączonym z przełącznikami Dell X-Series

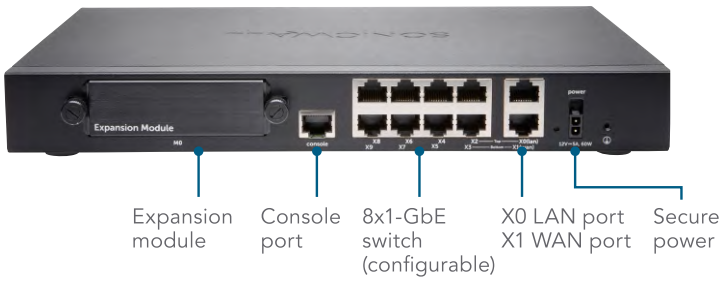
* 802.11ac obecnie niedostępne dla modeli SOHO, obsługujących 802.11a/b/g/n

Seria SonicWall TZ600

Rozwijającym się przedsiębiorstwom, placówkom handlu detalicznego i biurom oddziałowym, poszukującym wydajnej ochrony w atrakcyjnej cenie, firewall nowej generacji SonicWall TZ600 oferuje ochronę sieci z funkcjonalnością klasy Enterprise i wyjątkowymi osiągami.

Specyfikacja	Seria TZ600
Firewall - przepustowość	1.5 Gbps
Full DPI - przepustowość	500 Mbps
Antymalware - przepustowość	500 Mbps
IPS - przepustowość	1.1 Gbps
IMIX - przepustowość	900 Mbps
Maks. liczba połączeń	125,000
DPI Nowe połączenia/s	12,000

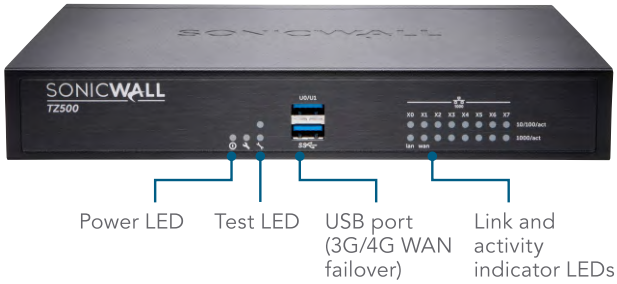




Seria SonicWall TZ500

Rozwijającym się biurom oddziałowym i firmom z sektora MŚP seria SonicWall TZ500 zapewnia wysoce efektywną ochronę pozbawioną kompromisów, wydajność i opcję zintegrowanej technologii bezprzewodowej 802.11ac dual-band.

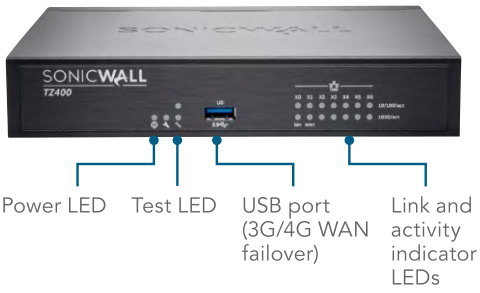
Specyfikacja	Seria TZ500
Firewall - przepustowość	1.4 Gbps
Full DPI - przepustowość	400 Mbps
Antymalware - przepustowość	400 Mbps
IPS - przepustowość	1.0 Gbps
IMIX - przepustowość	700 Mbps
Maks. liczba połączeń DPI	100,000
Nowe połączenia/s	8,000



Seria SonicWall TZ400

W małych firmach, handlu detalicznym i zdalnych biurach seria SonicWall TZ400 zapewnia ochronę klasy Enterprise. Dostępna opcja elastycznej sieci bezprzewodowej 802.11ac dual-band, zintegrowanej z firewallem.

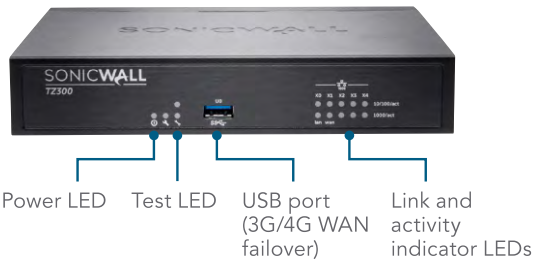
Specyfikacja	Seria TZ400
Firewall - przepustowość	1.3 Gbps
Full DPI - przepustowość	300 Mbps
Antymalware - przepustowość	300 Mbps
IPS - przepustowość	900 Mbps
IMIX - przepustowość	500 Mbps
Maks. liczba połączeń DPI	90,000
Nowe połączenia/s	6,000



Seria SonicWall TZ300

Seria SonicWall TZ300 oferuje rozwiązanie all-in-one, chroniące sieci przed atakami. W odróżnieniu od produktów konsumenckich firewalle SonicWall TZ300 łączą efektywną ochronę przed włamaniami, antymalware i filtrowanie treści/URL z opcjonalną, zintegrowaną technologią bezprzewodową 802.11ac oraz oferują szerokie wsparcie dla platform mobilnych przy obsłudze laptopów, smartfonów i tabletów.

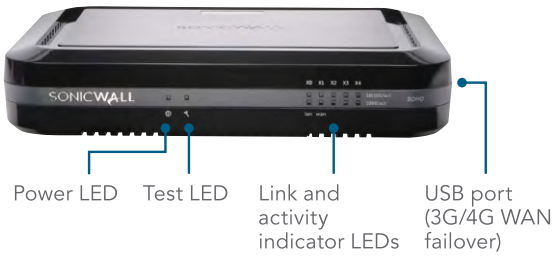
Specyfikacja	Seria TZ300
Firewall - przepustowość	750 Mbps
Full DPI - przepustowość	100 Mbps
Antymalware - przepustowość	100 Mbps
IPS - przepustowość	300 Mbps
IMIX - przepustowość	200 Mbps
Maks. liczba połączeń DPI	50,000
Nowe połączenia/s	5,000

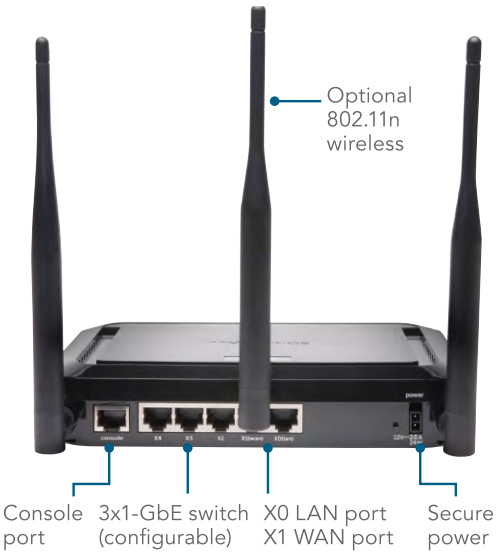


Seria SonicWall SOHO

W przewodowych i bezprzewodowych środowiskach małych i domowych biur seria SonicWall SOHO za przystępną cenę zapewnia ochronę tej samej klasy biznesowej, jakiej wymagają duże organizacje.

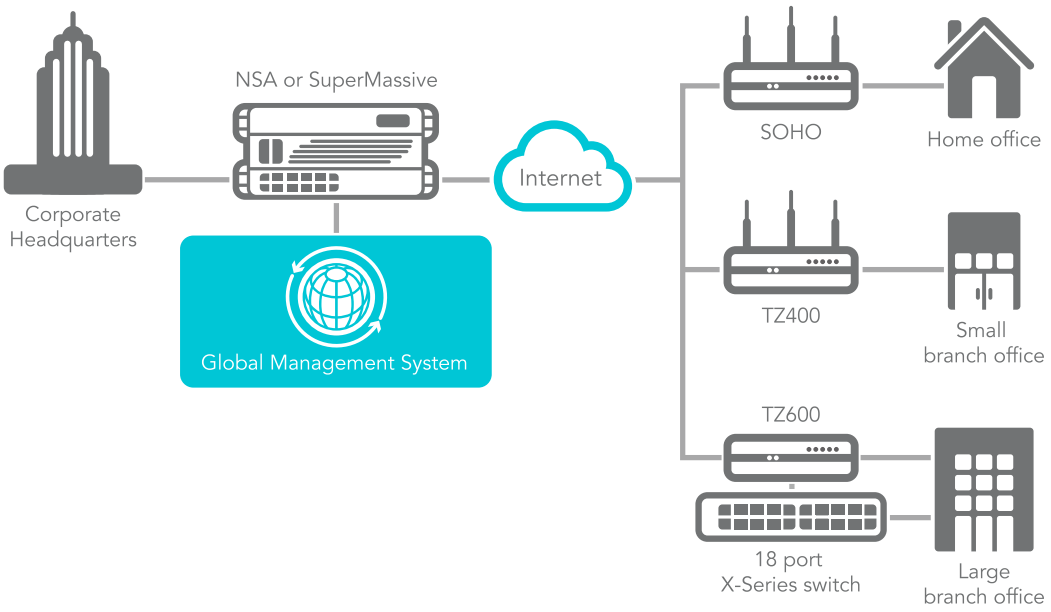
Specyfikacja	Seria SOHO
Firewall - przepustowość	300 Mbps
Full DPI - przepustowość	50 Mbps
Antymalware - przepustowość	50 Mbps
IPS - przepustowość	100 Mbps
IMIX - przepustowość	60 Mbps
Maks. liczba połączeń DPI	10,000
Nowe połączenia/s	1,800





Elastyczna architektura o wyjątkowej skalowalności i wydajności

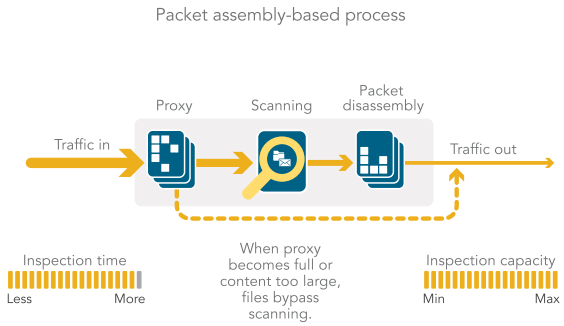
Mechanizm Reassembly-Free Deep Packet Inspection (RFDPI) został stworzony od podstaw z myślą o zapewnieniu skanowania bezpieczeństwa na najwyższym poziomie wydajności, mogącym sprostać ruchowi sieciowemu, który z natury jest równoległy i stale rosnący. W połączeniu z systemami wykorzystującymi wiele rdzeni procesorów ta równoległa architektura programowa doskonale skaluje się, zaspakajając potrzeby w zakresie inspekcji DPI (Deep Packet Inspection) zmasowanego ruchu sieciowego. Platforma SonicWall TZ wykorzystuje procesory, które (w odróżnieniu od x86) są zoptymalizowane pod kątem przetwarzania pakietowego, kryptograficznego i sieciowego, a jednocześnie pozostają elastyczne i programowalne (w odróżnieniu od systemów ASIC). Ta elastyczność ma kluczowe znaczenie, gdy trzeba użyć nowego kodu i zaktualizować działanie firewalli w celu zapewniania ochrony przed nowymi atakami, wymagającymi zastosowania nowych, bardziej zaawansowanych technik detekcji.



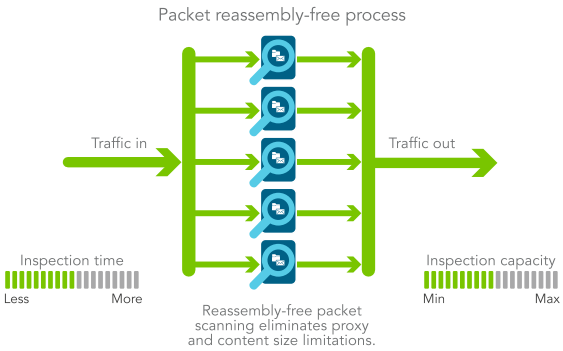
Mechanizm Reassembly-Free Deep Packet Inspection (RFDPI)

Mechanizm RFDPI zapewnia wyjątkową ochronę przed zagrożeniami i kontrolę aplikacji bez wpływu na wydajność. Ten opatentowany 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, próbujących oszukać mechanizmy detekcji i wprowadzić złośliwy kod do sieci.

Kiedy pakiet przechodzi niezbędne wstępne procesowanie, w tym dekrypcję 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 - wtedy uruchamiana jest wcześniej ustalona akcja. Gdy zidentyfikowano malware, firewall SonicWall kończy połączenie zanim dojdzie do jakichkolwiek szkód 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.



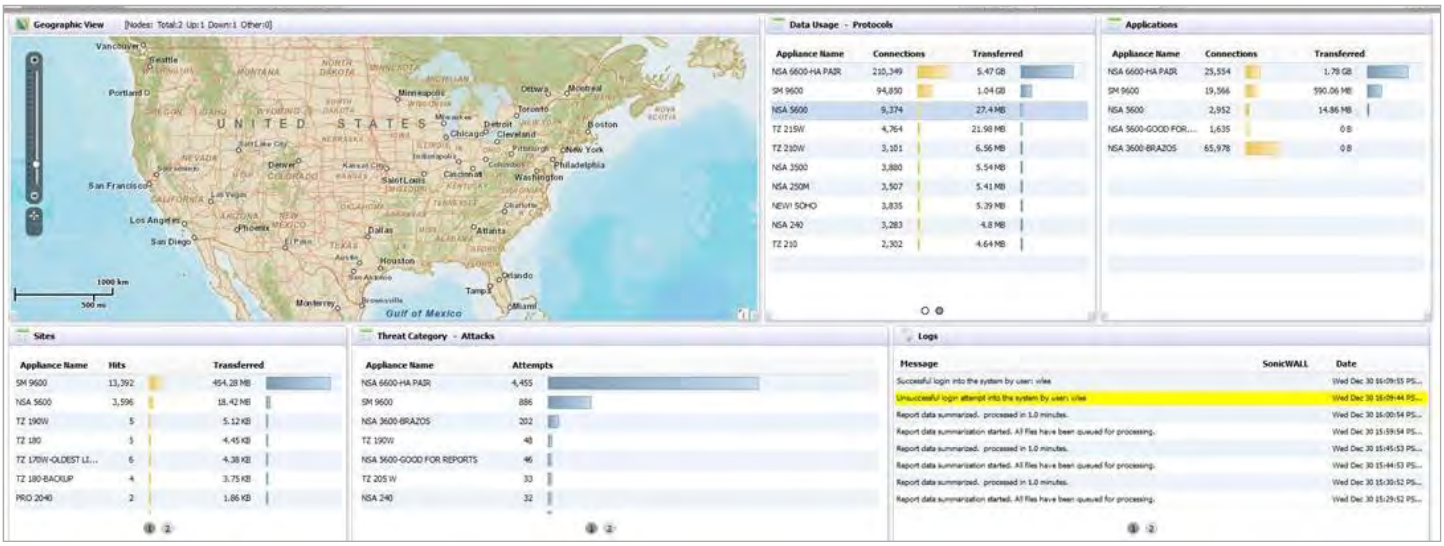
Competitive proxy-based architecture



SonicWall stream-based architecture

Globalne zarządzanie i raportowanie

W przypadku większych, rozproszonych wdrożeń w korporacjach opcjonalny Global Management System (GMS) zapewnia administratorom zunifikowaną, bezpieczną i rozszerzalną platformę do administrowania firewallami SonicWall i przełącznikami z serii Dell X-Series. Dzięki niemu 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. GMS dostosowuje się także do wymaganych zmian w zarządzaniu firewallami, poprzez funkcję automatyzacji przepływu pracy. W rezultacie oferuje lepszy sposób zarządzania bezpieczeństwem sieciowym na poziomie procesów biznesowych i usługowych, znakomicie upraszczając zarządzanie cyklem życiowym w całym środowisku ochrony (w porównaniu do zarządzania skupionego na poszczególnych urządzeniach).



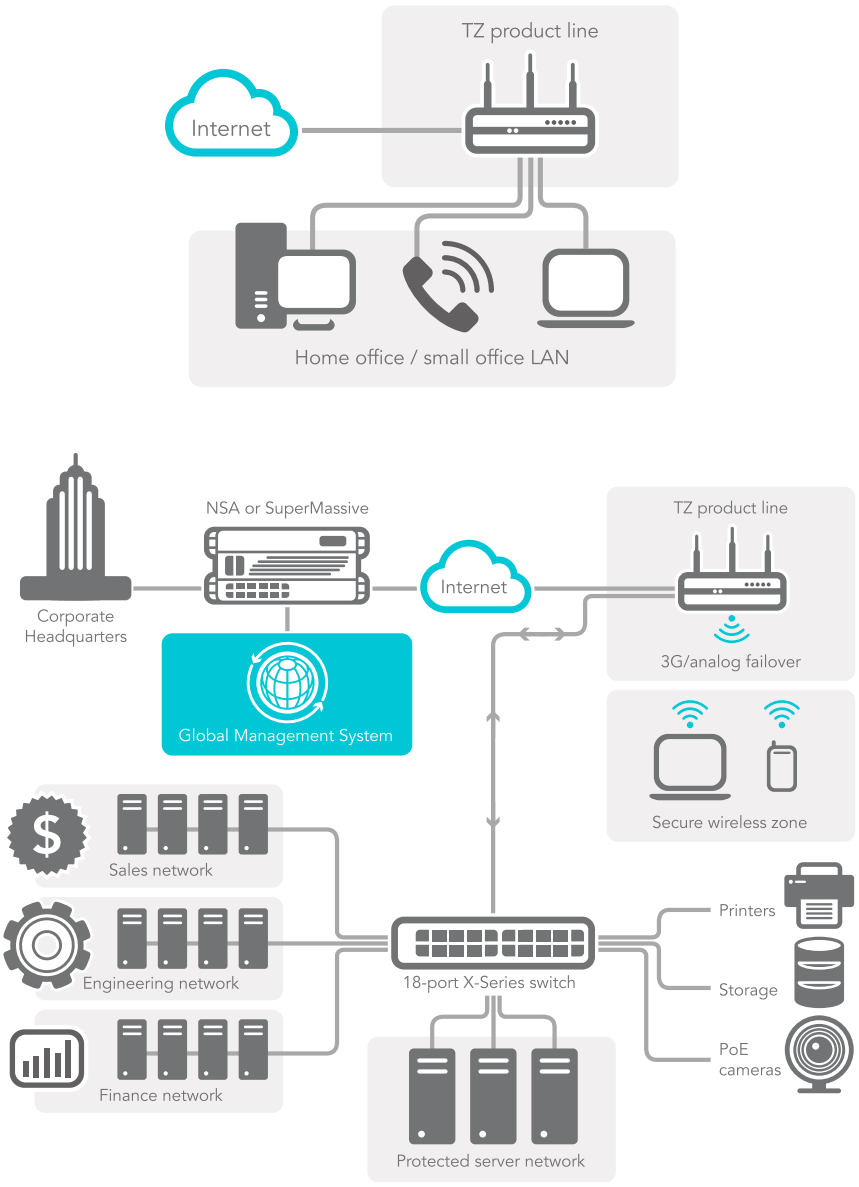
SONICWALL

Bezpieczeństwo i ochrona

Capture Labs - dedykowany firmowy zespół badawczy firmy SonicWall opracowuje zabezpieczenia, które są następnie wdrażane na firewallach w ramach stale aktualizowanej ochrony. Zespół wykorzystuje ponad milion sensorów rozmieszczonych na całym świecie do zbieranie próbek złośliwego kodu oraz telemetrycznych informacji zwrotnych dotyczących ostatnich zagrożeń, które są następnie wykorzystywane do tworzenia ochrony przed włamaniami i antymalware oraz detekcji aplikacji. Klienci korzystający z firewall'i SonicWall z aktualną subskrypcją otrzymują ciągłe aktualizacje ochrony przed zagrożeniami, które działają natychmiast, bez potrzeby restartu lub przerwy w pracy urządzeń.
Sygnatury w urządzeniach chronią przed szerokim spektrum rodzajów ataków, a jedna sygnatura obejmuje dziesiątki tysięcy poszczególnych zagrożeń. Oprócz własnych mechanizmów ochrony urządzenia mają dostęp do SonicWall CloudAV – chmury, która rozszerza bazę sygnatur na firewallach o ponad 20 mln sygnatur (ta liczba stale rośnie). Aby wzmocnić inspekcję dokonaną przez urządzanie, firewall łączy się przy użyciu firmowego lekkiego protokołu z bazą danych CloudAV. Dzięki funkcjonalności Geo-IP i filtrowania botnetów firewalle nowej generacji SonicWall mogą blokować ruch z niebezpiecznych domen i całych rejonów geograficznych, redukując poziom ryzyka w sieci.

Inteligencja i kontrola aplikacyjna

Inteligencja aplikacyjna daje wgląd administratorom w przepływający przez sieć ruch związany z aplikacjami. W efekcie mogą stosować środki kontroli według priorytetów biznesowych, ograniczać pasmo dla nieproduktywnych aplikacji i blokować takie, które mogą być niebezpieczne. Wizualizacja w czasie rzeczywistym identyfikuje anomalie w zachowaniu aplikacji, umożliwiając natychmiastowe reagowanie na potencjalne ataki przychodzące i wychodzące z sieci albo na tworzące się wąskie gardła. Analityka ruchu aplikacyjnego SonicWall oferuje granularny wgląd w ruch związany z aplikacjami, wykorzystanie pasma i zagrożenia dla bezpieczeństwa, a także zaawansowaną diagnostykę i funkcje przydatne w analizie śledczej. Dodatkowo bezpieczna funkcjonalność SSO (single sign-on) ułatwia obsługę użytkowników, zwiększając ich produktywność i ograniczając wezwania wsparcia. Dzięki intuicyjnemu interfejsowi web'owemu zarządzanie inteligencją i kontrolą aplikacyjną nie jest skomplikowane.



Elastyczna i bezpieczna sieć bezprzewodowa

Dostępna opcjonalnie szybka technologia bezprzewodowa 802.11ac* w połączniu z firewallami nowej generacji SonicWall tworzy bezpieczne rozwiązanie, które zapewnia kompleksową ochronę zarówno przewodowym jak i bezprzewodowym sieciom.
Dzięki wydajnej komunikacji bezprzewodowej klasy enterprise wyposażone w technologię WiFi urządzenia mogą łączyć się z większej odległości i wykorzystywać aplikacje mobilne wymagające połączeń o dużej przepustowości (takich jak wideo i głos), bez degradacji sygnału w środowiskach o dużej gęstości.

**802.11ac obecnie niedostępne dla modeli SOHO, obsługujących 802.11a/b/g/n*

Funkcje

Mechanizm RFDPI	
Funkcja	Opis
Reassembly-Free Deep Packet Inspection (RFDPI)	Wysokowydajny, firmowy i opatentowany mechanizm inspekcji, który przeprowadza opartą na strumieniu dwukierunkową analizę ruchu (bez użycia proxy i buforowania) w celu wykrycia prób włamania i malware'u 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 wykorzystywana do dystrybucji malware'u i nie stała się platformą do uruchamiania ataków w przypadku, gdy dołączono do niej zainfekowaną maszynę z zewnątrz.
Inspekcja single-pass	Architektura single-pass DPI jednocześnie skanuje ruch pod kątem malware'u, włamań i identyfikacji aplikacji, co przekłada się na znaczne zmniejszenie opóźnień i pewność, że informacje o wszystkich zagrożeniach są korelowane w ramach pojedynczej architektury.
Inspekcja oparta na strumieniu	Technologia inspekcji bez proxy i buforowania, która zapewnia ultraniskie opóźnienia badanych przez DPI milionów jednoczesnych strumieni sieciowych. Nie wprowadza ograniczeń wielkości strumieni i może być zastosowana w przypadku powszechnie wykorzystywanych protokołów oraz strumieni raw TCP.
Technologia DPI-SSH (Deep Packet Inspection of Secure Socket Shell)	Technologia DPI-SSH wykrywa i zapobiega zaawansowanym atakom wykorzystującym SSH, blokuje pobieranie malware'u, zapobiega rozprzestrzenianiu się infekcji, uniemożliwia komunikację typu command and control (C&C) oraz eksfiltrację danych.
Capture Advanced Threat Protection	
Funkcja	Opis
Wielosilnikowy sandboxing	Wielosilnikowa platforma sandboxingu, 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.
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 sygnatur bramy antywirusowej, IPS, bazy URL, IP oraz reputacji domen zostają zaktualizowane w ciągu 48 godz.
Blokowanie do werdyktu	Aby zapobiec przedostawaniu się do sieci potencjalnie złośliwego oprogramowania, wysyłane do chmury w celu analizy pliki są przetrzymywane na bramie aż do momentu wydania werdyktu o ich szkodliwości.
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'm, włamaniami i wyciekiem danych. Korzysta z polityk aplikacyjnych, kontroli URL i treści, by chronić przed zagrożeniami ukrywającymi się w ruchu zaszyfrowanym. Wchodzi w skład subskrypcji ochrony dla wszystkich modeli serii oprócz SOHO (dla tego modelu trzeba zakupić oddzielną licencję).
Inspekcja SSH	Technologia DPI-SSH (Deep Packet Inspection of SSH) przeprowadza dekrypcję i inspekcję danych przechodzących przez tunel SSH, chroniąc przed atakami wykorzystującymi takie połączenia.
Ochrona przed włamaniami	
Funkcja	Opis
Ochrona oparta na przeciwdziałaniu	Ściśle zintegrowany system IPS (Intrusion Prevention System) wykorzystuje sygnatury i inne mechanizmy obrony do skanowania pakietów pod kątem luk i exploit'ów, 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 kategorii 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 włamaniami. 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, dekodowanie 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 oraz wewnętrzny pod kątem wirusów, Trojanów, key loggerów i innego rodzaju malware'u w plikach o nieograniczonej długości i rozmiarze na wszystkich portach i strumieniach TCP.
Ochrona przed malware CloudAV	Nieustannie aktualizowana baza danych z dziesiątkami milionów sygnatur zagrożeń, rezydująca na chmurowych serwerach SonicWall, jest referencją dla lokalnych baz sygnatur, zwiększając ochronę i możliwości mechanizmu RFDPIw zwalczaniu zagrożeń.
Ciągłe aktualizacje bezpieczeństwa	Nowe aktualizacje zagrożeń są automatycznie przekazywane firewallom z aktywnymi usługami bezpieczeństwa i zaczynają działać natychmiast, bez potrzeby restartu czy przerwy w pracy urządzeń.

Ochrona przed zagrożeniami cd.	
Funkcja	Opis
Dekrypcja i inspekcja SSL	Dokonuje dekrypcji i inspekcji zaszyfrowanego ruchu SSL w locie i bez proxy, chroniąc przed malware'm, włamaniami i wyciekiem danych. Korzysta z polityk aplikacyjnych, kontroli URL i treści, by chronić przed zagrożeniami ukrywającymi się w ruchu zaszyfrowanym. Wchodzi w skład subskrypcji ochrony dla wszystkich modeli z wyjątkiem SOHO (dla tego modelu jest oddzielnie sprzedawana licencja).
Dwukierunkowa inspekcja raw TCP	Mechanizm RFDPI może skanować strumienie raw TCP dwukierunkowo 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, FTP, SMTP, SMBv1/v2 oraz inne, które nie przesyłają danych w raw TCP. Dekoduje ruch w celu inspekcji malware'u, 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 o 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.
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.
YouTube dla szkól	Daje nauczycielom możliwość wyboru spośród tysięcy darmowych edukacyjnych treści wideo w serwisie YouTube EDU, które są zorganizowane według przedmiotów i klas oraz odpowiadają powszechnym standardom edukacyjnym.
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 firewall'a 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.
Ciągła, automatyczna ochrona antywirusowa	Częste aktualizacje antywirusowe i antyspyware są dostarczane transparentnie na wszystkie komputery i serwery plików, co zwiększa produktywność użytkowników końcowych i redukuje zarządzanie bezpieczeństwem.
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.
Firewall i networking	
Funkcja	Opis
Stateful Packet Inspection	Cały ruch sieciowy jest kontrolowany, analizowany i doprowadzany do zgodności ze standardami za pomocą polityk dostępu na firewallach.
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. Dodatkowo 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 filtrowania oraz trybu wire.
Opcje elastycznego wdrażania	Seria SonicWall TZ może być wdrażana w trybach tradycyjnego NAT, Layer 2 bridge, wire i network tap.
Uwierzytelnianie biometryczne	Obsługuje uwierzytelnianie na urządzeniach mobilnych przy użyciu odcisku palca, dzięki czemu dane uwierzytelniające nie mogą być łatwo powielone lub przekazane, co zwiększa bezpieczeństwo w dostępie do sieci.
Integracja z przełącznikami Dell X-Series	Zarządza ustawieniami bezpieczeństwa na dodatkowych portach, takich PoE and PoE+, przy użyciu pojedynczej konsoli wykorzystującej interfejs do zarządzania firewallem w przełącznikach sieciowych Dell X-Series (niedostępna dla modelu SOHO)

Firewall i networking cd.	
Funkcja	Opis
High Availability	Modele SonicWall TZ500 i SonicWall TZ600 obsługują funkcję wysokiej dostępności z synchronizacją stanu. Modele SonicWall TZ300 i SonicWall TZ400 obsługują HA bez synchronizacji Active/Standby. Modele SonicWall SOHO nie oferują funkcji HA.
Threat 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).
Bezpieczeństwo sieci bezprzewodowej	Technologia bezprzewodowa IEEE 802.11ac może zapewnić przepustowość WiFi do 1,3 Gb/s, większy zasięg i niezawodność. Dostępna w modelach do SonicWall TZ600 do SonicWall TZ300. Opcja 802.11 a/b/g/n dostępna dla modeli SonicWall SOHO.
Zarządzanie i raportowanie	
Funkcja	Opis
Global Management System (GMS)	System SonicWall GMS umożliwia monitorowanie, konfigurowanie i raportowanie na wielu urządzeniach SonicWall i przełącznikach Dell X-Series 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 GMSFlow Server 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 automatycznie ustanawiana jest ochrona oraz komunikacja.
VPN IPSec dla komunikacji site-to-site	Dzięki wysokowydajnemu rozwiązaniu VPN IPSec seria SonicWall TZ 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 dynamicznego routingu przez łącza VPN, które zapewnia stałą dostępność na wypadek czasowego uszkodzenia tunelu VPN (płynny re-routing ruchu między punktami końcowymi przy użyciu tras alternatywnych).
Monitoring treści/kontekstu	
Funkcja	Opis
Śledzenie aktywności użytkowników	Identyfikacja użytkownika i jego 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	Identyfikuje oraz 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.
DPI z filtrowaniem wyrażeń regularnych	Zapobiega wyciekowi danych poprzez identyfikowanie i kontrolowanie treści przechodzących przez sieć metodą dopasowywania wyrażeń regularnych.

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
- Threat APIs

Dekrypcja i inspekcja TLS/SSL/SSH[1]

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

Capture Advanced Threat Protection1

- 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
- Funkcja Auto-Block

Ochrona przed włamaniami[1]

- Skanowanie sygnaturowe
- Automatyczne aktualizacje sygnatur
- Inspekcja dwukierunkowa
- Granularne reguły IPS
- Ochrona z GeoIP/filtrowanie botnetów
- Dopasowywanie wyrażeń regularnych

Antymalware[1]

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

Identyfikacja aplikacji

- Kontrola aplikacji
- Wizualizacja aplikacji[2]
- Blokowanie komponentów aplikacji
- Zarządzanie pasmem aplikacji
- Własne tworzenie sygnatur aplikacji
- DLAP (Data Leakage Prevention)
- Raportowanie aplikacji przez NetFlow/IPFIX
- Śledzenie aktywności użytkownika (SSO)
- Kompleksowa baza sygnatur aplikacji

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
- Rozszerzone logowanie
- Layer-2 QoS
- Bezpieczeństwo portów
- Dynamiczny routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and

ECMP)

- Asymmetric routing
- Serwer DHCP
- NAT
- Zarządzanie pasmem
- High availability - Active/Standby with state sync[3]
- Inbound/outbound load balancing
- L2 bridge mode, NAT mode
- 3G/4G WAN failover
- Obsługa Common Access Card (CAC)

Zarządzanie i monitoring

- Web GUI
- Command line interface (CLI)
- SNMPv2/v3
- Centralne zarządzanie i raportowanie przy użyciu SonicWall GMS
- Logging
- Eksportowanie Netflow/IPFix
- Backup konfiguracji oparty na chmurze
- Wizualizacja aplikacji i pasma
- Zarządzanie IPv4 i IPv6
- Zarządzanie przełącznikami Dell X-Series, także kaskadami

Zintegrowana sieć bezprzewodowa

- Dual-band (2.4 GHz i 5.0 GHz)
- Technologie bezprzewodowe 802.11 a/b/g/n/ac[2]
- Wireless intrusion detection/prevention
- Bezprzewodowe usługi gościnne
- Lightweight hotspot messaging
- Segmentacja wirtualnych punktów dostępowych
- Captive portal
- Cloud ACL

[1] *Wymaga dodatkowe subskrypcji*
[2] *Niedostępne w modelach SOHO*
[3] *State sync high availability tylko dla modeli SonicWall TZ500 i SonicWall TZ600*

Specyfikacje systemowe SonicWall TZ

Hardware overview	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Operating system	SonicOS				
Security processing cores	2	2	4	4	4
Interfaces	5x1GbE, 1 USB, 1 Console	5x1GbE, 1 USB, 1 Console	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, 1 Expansion Slot
Expansion	USB	USB	USB	2 USB	Expansion Slot (Rear)*, 2 USB
Single Sign-On (SSO) Users	250	500	500	500	500
VLAN interfaces	25	25	50	50	50
Access points supported (maximum)	2	8	16	16	24
Dell X-Series switch models supported	Not available	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Firewall/VPN performance	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Firewall inspection throughput[1]	300 Mbps	750 Mbps	1,300 Mbps	1,400 Mbps	1,500 Mbps
Full DPI throughput[2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Application inspection throughput[2]	-	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
IPS throughput[2]	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
Anti-malware inspection throughput[2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
IMIX throughput	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
IPSec VPN throughput[3]	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
Connections per second	1,800	5,000	6,000	8,000	12,000
Maximum connections (SPI)	10,000	50,000	100,000	125,000	150,000
Maximum connections (DPI)	10,000	50,000	90,000	100,000	125,000
Maximum connections (DPI SSL)	100	500	500	750	750
VPN	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Site-to-site VPN tunnels	10	10	20	25	50
IPSec VPN clients (maximum)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
SSL VPN licenses (maximum)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual assist bundled (maximum)	-	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1, Suite B Cryptography				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14				
Route-based VPN	RIP, OSPF				
Certificate support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to- SonicWall VPN, SCEP				
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN				
Global VPN client platforms supported	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10				
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)				
Security services	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL				
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists				
Enforced Client Anti-Virus and Anti-Spyware	McAfee®				
Comprehensive Anti-Spam Service	Supported				
Application Visualization	No	Yes	Yes	Yes	Yes
Application Control	Yes	Yes	Yes	Yes	Yes
Capture Advanced Threat Protection	No	Yes	Yes	Yes	Yes

SONICWALL™

Specyfikacje systemowe SonicWall TZ cd.

Networking	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
IP address assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay				
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode				
Routing protocols[4]	BGP[4], OSPF, RIPv1/v2, static routes, policy-based routing				
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)				
Authentication	LDAP (wiele domen), XAUTH/ RADIUS, SSO, Novell, wewnętrzna baza użytkowników user database	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix			
Local user database	150			250	
VoIP	Full H.323v1-5, SIP				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certifications	FIPS 140-2 (with Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus				
Certifications pending	Common Criteria NDPP				
Common Access Card (CAC)	Supported				
High availability	No	Active/standby	Active/standby	Active/standby with stateful synchronization	Active/standby with stateful synchronization
Hardware	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Form factor	Desktop				
Power supply (W)	24W external	24W external	24W external	36W external	60W external
Maximum power consumption (W)	6.4 / 11.3	6.9 / 12.0	9.2 / 13.8	13.4 / 17.7	16.1
Input power	100 to 240 VAC, 50-60 Hz, 1 A				
Total heat dissipation	21.8 / 38.7 BTU	23.5 / 40.9 BTU	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
Dimensions	3.6x14.1x19cm	3.5x13.4x19cm	3.5x13.4x19cm	3.5x15x22.5cm	3.5x18x28cm
Weight	0.34 kg / 0.75lbs 0.48 kg / 1.06lbs	0.73 kg / 1.61lbs 0.84 kg / 1.85lbs	0.73 kg / 1.61lbs 0.84 kg / 1.85lbs	0.92 kg / 2.03lbs 1.05 kg / 2.31lbs	1.47 kg / 3.24 lbs
WEEE weight	0.80 kg / 1.76lbs 0.94 kg / 2.07lbs	1.15 kg / 2.53lbs 1.26 kg / 2.78lbs	1.15 kg / 2.53lbs 1.26 kg / 2.78lbs	1.34 kg / 2.95lbs 1.48 kg / 3.26lbs	1.89 kg /4.16 lbs
Shipping weight	1.20 kg / 2.64lbs 1.34 kg / 2.95lbs	1.37 kg / 3.02lbs 1.48 kg / 3.26lbs	1.37 kg / 3.02lbs 1.48 kg / 3.26lbs	1.93 kg / 4.25lbs 2.07 kg / 4.56lbs	2.48 kg / 5.47 lbs
MTBF (years)	58.9/56.1 (wireless)	56.1	54.0	40.8	18.4
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)				
Humidity	5-95% non-condensing				
Regulatory	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Regulatory model (wired)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Major regulatory compliance (wired models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, BSMI, KCC/MSIP	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL cUL, TUV/ GS, CB, Mexico CoC by UL,WEEE, REACH, KCC/MSIP
Regulatory model (wireless)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Major regulatory compliance (wireless models)	FCCClassB,FCC RFICESClassB, IC RFCE(R&TTE, EMC,LVD,RoHS), RCM, VCCI Class B,MIC/TELEC,UL, cUL, TUV/GS,CB, Mexico CoC by UL, WEEE , REACH	FCCClassB,FCC RFICESClassB, IC RFCE(R&TTE, EMC,LVD,RoHS), RCM, VCCI Class B,MIC/TELEC,UL, cUL, TUV/GS,CB, Mexico CoC by UL, WEEE , REACH	FCCClassB,FCC RFICESClassB, IC RFCE(R&TTE, EMC,LVD,RoHS), RCM, VCCI Class B,MIC/TELEC,UL, cUL, TUV/GS,CB, Mexico CoC by UL, WEEE , REACH	FCCClassB,FCC RFICESClassB, IC RFCE(R&TTE, EMC,LVD,RoHS), RCM, VCCI Class B,MIC/TELEC,UL, cUL, TUV/GS,CB, Mexico CoC by UL, WEEE , REACH	-

Specyfikacje systemowe SonicWall TZ cd.

Integrated Wireless	SOHO series	TZ300, TZ400, TZ500 series	TZ600
Standards	802.11 a/b/g/n	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS	-
Frequency bands[5]	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz;	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz; 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz	-
Operating Channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64;	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48,Japan 36-48, Spain 36-48/52-64	-
Transmit output power	Based on the regulatory domain specified by the system administrator	Based on the regulatory domain specified by the system administrator	-
Transmit power control	Supported	Supported	-
Data rates supported	802.11a: 6, 9, 12, 18,24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15,30, 45, 60, 90, 120, 135, 150 Mbps per channel;	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15,30, 45, 60, 90, 120, 135, 150 Mbps per channel; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Mbps per channel	-
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM)	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	-

*Future use.
[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] BGP is available only on SonicWall TZ400, TZ500 and TZ600.
[5] All TZ integrated wireless models can support either 2.4GHz or 5GHz band. For dual-band support, please use SonicWall's wireless access points products (SonicPoints)

Seria SonicWall TZ - informacje do zamówień

Produkt	SKU
SonicWall SOHO with 1-year TotalSecure	01-SSC-0651
SonicWall SOHO Wireless-N with 1-year TotalSecure	01-SSC-0653
SonicWall TZ300 with 1-year TotalSecure Advanced Edition	01-SSC-1702
SonicWall TZ300 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1703
SonicWall TZ400 with 1-year TotalSecure Advanced Edition	01-SSC-1705
SonicWall TZ400 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1706
SonicWall TZ500 with 1-year TotalSecure Advanced Edition	01-SSC-1708
SonicWall TZ500 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1709
SonicWall TZ600 with 1-year TotalSecure Advanced Edition	01-SSC-1711
High availability options (each unit must be the same model)	
SonicWall TZ500 High Availability	01-SSC-0439
SonicWall TZ600 High Availability	01-SSC-0220

Seria SonicWall TZ - informacje do zamówień cd.

Usługi	SKU
For SonicWall SOHO Series	
Comprehensive Gateway Security Suite 1-year	01-SSC-0688
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0670
Content Filtering Service 1-year	01-SSC-0676
Comprehensive Anti-Spam Service 1-year	01-SSC-0682
24x7 Support 1-year	01-SSC-0700
For SonicWall TZ300 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ300 (1-year)	01-SSC-1430
Capture Advanced Threat Protection for TZ300 (1-year)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0602
Content Filtering Service 1-year	01-SSC-0608
Comprehensive Anti-Spam Service 1-year	01-SSC-0632
24x7 Support 1-year	01-SSC-0620
For SonicWall TZ400 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ400 (1-year)	01-SSC-1440
Capture Advanced Threat Protection for TZ400 (1-year)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0534
Content Filtering Service 1-year	01-SSC-0540
Comprehensive Anti-Spam Service 1-year	01-SSC-0561
24x7 Support 1-year	01-SSC-0552
For SonicWall TZ500 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ500 (1-year)	01-SSC-1450
Capture Advanced Threat Protection for TZ500 (1-year)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0458
Content Filtering Service 1-year	01-SSC-0464
Comprehensive Anti-Spam Service 1-year	01-SSC-0482
24x7 Support 1-year	01-SSC-0476
For SonicWall TZ600	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ600 (1-year)	01-SSC-1460
Capture Advanced Threat Protection for TZ600 (1-year)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0228
Content Filtering Service 1-year	01-SSC-0234
Comprehensive Anti-Spam Service 1-year	01-SSC-0252
24x7 Support 1-year	01-SSC-0246

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.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-TZ Series-US-VG-MKTG658

SONICWALL™