SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

SonicWall SMA to zunifikowana brama bezpieczeństwa dla organizacji stojących przed wyzwaniami dotyczącymi mobilności, BYOD i migracji do chmury.

SonicWall SMA to zunifikowana brama, która zapewnia organizacjom bezpieczny dostęp do krytycznych zasobów korporacyjnych - w każdym momencie, z dowolnego urządzenia i miejsca. Dzięki opartemu na politykach mechanizmowi szczegółowej kontroli dostępu SMA, kontekstowej autoryzacji urządzeń, ochronie VPN na poziomie aplikacji i zaawansowanemu jednokrotnemu logowaniu (SSO) organizacje mogą bez problemu korzystać z BYOD oraz mobilności w hybrydowym środowisku IT.

Mobilność i BYOD
W organizacjach chcących korzystać z zalet BYOD, elastycznego stylu pracy i bezpiecznej współpracy
z niezależnymi podmiotami SMA staje się kluczowym narzędziem do egzekwowania bezpiecznego dostępu.
Rozwiązanie to daje organizacji najlepszą w swojej klasie ochronę, minimalizując zagrożenia m.in. poprzez obsługę najnowszych algorytmów szyfrowania. Wykorzystując SonicWall SMA, administratorzy mogą zapewniać użytkownikom końcowym szybki, łatwy i bezpieczny dostęp mobilny do niezbędnych aplikacji biznesowych, danych i zasobów oraz przyznawać im oparte na rolach uprawnienia. Co więcej, organizacje mogą tworzyć bezpieczne reguły stosowania modelu BYOD w celu ochrony swoich sieci korporacyjnych i danych przed nieautoryzowanym dostępem i złośliwym oprogramowaniem.

Migracja do chmury
Organizacjom rozpoczynającym swoją migrację do chmury SMA oferuje infrastrukturę jednokrotnego logowania (SSO), która korzysta z pojedynczego portalu webowego do uwierzytelniania użytkowników
w hybrydowym środowisku IT. Niezależnie od tego, czy firmowe zasoby są w środowisku lokalnym,
w Internecie czy w hostowanej chmurze, dostęp do nich jest spójny i bezproblemowy. W celu zwiększenia bezpieczeństwa SMA integruje się również z wiodącymi w branży rozwiązaniami uwierzytelniania wieloskładnikowego (MFA).

Dostawcy usług zarządzanych (MSP)
Dla organizacji hostujących własną infrastrukturę, a także dostawców usług zarządzanych SMA to kompleksowe rozwiązanie zapewniające wysoki poziom ciągłości biznesowej oraz dużą skalowalność. Jedno urządzenie SMA jest w stanie obsłużyć do 20 000 jednoczesnych połączeń, a dzięki inteligentnemu klastrowaniu możliwe staje się skalowanie takiego rozwiązania do setek tysięcy użytkowników. Centra danych mogą obniżyć swoje koszty dzięki aktywnemu klastrowaniu i wbudowanemu mechanizmowi dynamicznego równoważenia obciążeń (w zależności od potrzeb użytkowników realokującemu w czasie rzeczywistym globalny ruch do najbardziej zoptymalizowanego data center). Zestawy narzędzi SMA umożliwiają dostawcom świadczenie usług bez przestojów i wywiązywanie się z bardzo rygorystycznych umów SLA. Niezależnie od scenariuszy wykorzystania rozwiązania działy IT mogą przy użyciu SMA zapewniać dostęp, który będzie najbezpieczniejszy i najlepiej obsługiwany.

Rozwiązanie SMA - dostępne jako specjalizowane urządzenie fizyczne albo wydajne wirtualne - bezproblemowo wpasowuje się w istniejącą infrastrukturę IT. Do zapewniania bezpiecznego dostępu pracownikom używającym prywatnych urządzeń lub zewnętrznym firmom organizacje mogą wybrać którąś
z opcji wykorzystujących przeglądarkę internetową, niewymagających programowego klienta (clientless). Mogą też zdecydować się na bardziej tradycyjny i pełny kliencki dostęp VPN, w którym dla kadry kierowniczej stworzone zostaną bezpieczne tunele z wykorzystaniem urządzeń dowolnego typu. Niezależnie od tego, czy organizacje chcą z jednego miejsca zapewnić niezawodny bezpieczny dostęp dla pięciu pracowników, czy skalować ten dostęp do tysięcy użytkowników w globalnie rozproszonych centrach danych, SonicWall SMA jest właściwym rozwiązaniem. Dzięki niemu można korzystać z mobilności i modelu BYOD bez obaw o bezpieczeństwo oraz łatwo przenosić swoje zasoby i aplikacje do chmury. W każdym wariancie SMA oferuje pracownikom organizacji bezpieczną, bezproblemową i spójną usługę dostępową.

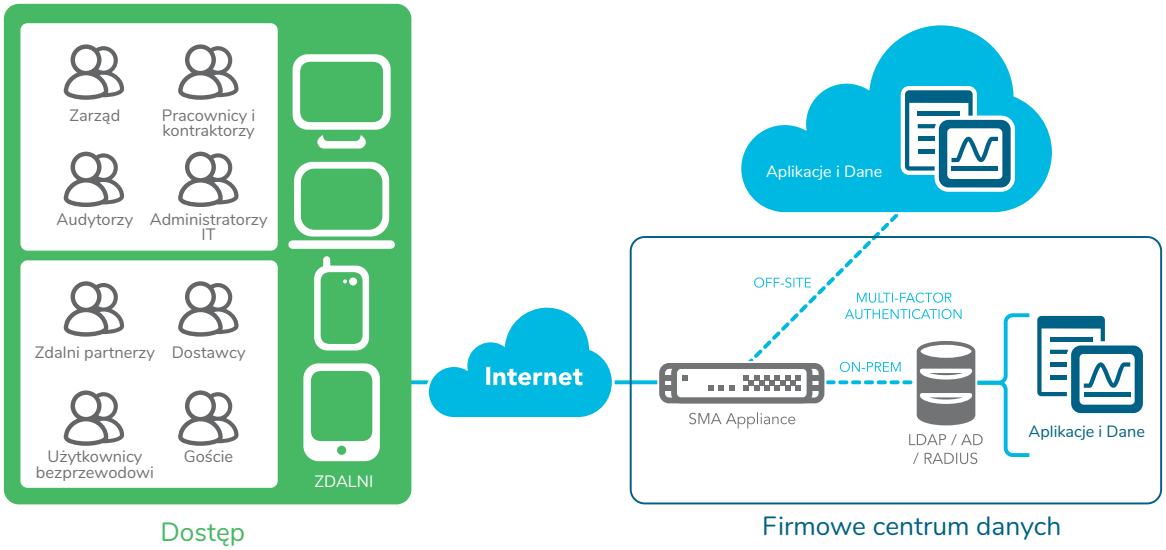
Korzyści z wdrożenia:

- Zunifikowany i bezpieczny dostęp do wszystkich zasobów sieciowych i chmurowych „w dowolnym czasie, na dowolnym urządzeniu i dla dowolnej aplikacji”
- Możliwość kontroli, kto ma dostęp, do jakich zasobów – poprzez zdefiniowanie szczegółowych polityk
- w ramach niezawodnego mechanizmu kontroli dostępu
- Zwiększenie wydajności pracy, dzięki jednokrotnemu logowaniu (SSO) z pojedynczym adresem URL do dowolnej aplikacji SaaS lub hostowanej
- Niższy całkowity koszt posiadania i ograniczenie złożoności zarządzania dostępem poprzez konsolidację komponentów infrastruktury w hybrydowym środowisku IT
- Wgląd w każde łączące się urządzenie z możliwością przyznawania dostępu w oparciu o polityki i stan ochrony punktu końcowego
- Zapobieganie atakom wykorzystującym złośliwe oprogramowanie poprzez skanowanie wszystkich plików przesłanych do sieci przy użyciu rozwiązania sandbox Capture ATP
- Ochrona się przed atakami internetowymi i możliwość zapewnienia zgodności ze standardem PCI przy użyciu dodatkowego zabezpieczenia Web Application Firewall
- Blokowanie ataków DDoS i zombie dzięki wykrywaniu lokalizacji Geo IP i ochronie przed botnetami
- Zapewnienie bezpiecznego dostępu w oparciu o natywną funkcjonalność agenta w przeglądarce HTML5, bez konieczności instalowania i utrzymywania oprogramowania klienckiego na urządzeniach końcowych (tryb clientless)
- Dostęp do praktycznych informacji niezbędnych w podejmowaniu właściwych decyzji w oparciu
- monitorowanie w czasie rzeczywistym i kompleksowe raportowanie
- Łatwość wdrażania dzięki elastycznym opcjom urządzeń fizycznych i wirtualnych, dostosowanych do potrzeb dowolnej organizacji
- Możliwość dynamicznego przyznawania praw dostępu zgodnie ze zmieniającym się w czasie rzeczywistym zapotrzebowaniem i z automatycznym przekierowywaniem punktów końcowych na połączenia o najwyższej wydajności i najmniejszym opóźnieniu
- Minimalizowanie kosztów eksploatacji dzięki wbudowanemu równoważeniu obciążeń (load balancing), które nie wymaga dodatkowego sprzętu i usług, oraz funkcji przełączania awaryjnego urządzeń o zerowym wpływie na dostępność usługi
- Zabezpieczenie przed zakłóceniami w działalności biznesowej i sezonowymi skokami natężenia ruchu dzięki możliwości natychmiastowego skalowania wydajności

SMA – urządzenia i wdrożenie

Specjalizowana brama oferująca bezpieczny dostęp w każdym momencie, z dowolnego urządzenia i miejsca

SMA jest zaawansowaną bramą bezpieczeństwa zapewniająca bezpieczny dostęp do zasobów sieciowych i chmurowych z dowolnego urządzenia. Jako specjalizowane urządzenie wykorzystujące system Linux, SMA oferuje scentralizowane, szczegółowe, oparte na politykach egzekwowanie zdalnego i mobilnego dostępu do wszelkich zasobów korporacyjnych. Dostępne w formie wzmocnionych urządzeń fizycznych lub wydajnych urządzeń wirtualnych, SMA bezproblemowo wpasowuje się w każdą istniejącą infrastrukturę IT.



Rozwiązanie SMA zapewnia bezpieczny dostęp wszystkim użytkownikom, urządzeniom i aplikacjom.

Elastyczne wdrażanie w oparciu o specjalizowane urządzenia fizyczne i wirtualne
Brama SonicWall SMA może być wdrożona jako specjalizowane, wydajne rozwiązanie sprzętowe lub jako urządzenie wirtualne, które w optymalny sposób wykorzystuje wspólne zasoby obliczeniowe, ułatwia migrację oraz ogranicza wydatki kapitałowe. Urządzenia sprzętowe są zbudowane w oparciu wielordzeniową architekturę, która w zapewnianiu niezawodnego i bezpiecznego dostępu oferuje niezbędną wydajność do akceleracji SSL, uzyskiwania dużej przepustowości VPN i obsługi serwerów proxy. Z myślą o sektorach regulowanych rozwiązanie SMA jest również oferowane z certyfikatem FIPS 140-2 Level 2. Urządzenia wirtualne SMA oferują takie same możliwości bezpiecznego dostępu i mogą być uruchamiane na popularnych platformach wirtualizacyjnych, w tym Microsoft Hyper-V i VMware ESX.

Współdzielone licencje użytkownika dla wielu urządzeń
Organizacje posiadające urządzenia rozproszone na całym świecie mogą zaspokajać zmieniające się lokalnie potrzeby odnośnie licencji, wykorzystując różnice czasowe. Niezależnie od tego, czy korporacja wdraża pełne licencje VPN, czy podstawowe licencje ActiveSync, może ona za pomocą centralnego zarządzania SMA przenosić licencje z tych urządzeń, gdzie zapotrzebowanie spada (skończył się czas pracy), do tych w innym obszarze geograficznym, gdzie potrzeby użytkowników wzrastają (czas pracy się zaczyna) .

Widoczność sieci z kontekstowym profilowaniem urządzeń
Najlepsze w swojej klasie uwierzytelnianie kontekstowe zapewnia dostęp tylko zaufanym urządzeniom i autoryzowanym użytkownikom. Laptopy i komputery stacjonarne są sprawdzane pod kątem posiadanego oprogramowania zabezpieczającego, certyfikatów klienckich oraz identyfikatorów urządzeń. W przypadku urządzeń mobilnych przed udzieleniem dostępu pozyskiwane są niezbędne informacje dotyczące poziomu ochrony, takie jak brak oznak rootowania i jailbreakingu, identyfikatory urządzeń, status certyfikatów oraz wersje systemu operacyjnego. Urządzenia, które nie spełniają wymaganych reguł, nie mają dostępu do sieci, a ich użytkownicy są powiadamiani o niezgodności.

Spójna obsługa przy użyciu jednego portalu webowego
Użytkownicy nie muszą pamiętać wszystkich adresów URL dla poszczególnych aplikacji i dbać o poszczególne zakładki. SMA zapewnia scentralizowany portal dostępowy, który zapewnia użytkownikom jeden adres URL dający dostęp do wszystkich kluczowych aplikacji przy użyciu standardowej przeglądarki internetowej. Po zalogowaniu się użytkownika w oknie przeglądarki jest wyświetlany dostosowywany portal webowy, który w spójny sposób umożliwia dostęp do dowolnej usługi SaaS lub aplikacji lokalnej. Portal wyświetla tylko łącza i spersonalizowane zakładki właściwe dla konkretnego urządzenia końcowego, użytkownika lub grupy. Portal jest niezależny od platformy sprzętowej i działa ze wszystkimi popularnymi systemami urządzeń końcowych, w tym Windows, Mac OS, Linux, iOS i Android. Obsługuje także szeroką gamę przeglądarek na wszystkich tych urządzeniach.

Federacyjne jednokrotne logowanie (SSO) zarówno do SaaS, jak i lokalnych aplikacji
Możliwe jest wyeliminowanie konieczności stosowania wielu haseł i ograniczenie złych praktyk bezpieczeństwa, takich jak ponowne użycie tego samego hasła. SMA oferuje federacyjne jednokrotne logowanie (SSO) zarówno do aplikacji SaaS, hostowanych w chmurze, jak i tych uruchamianych w lokalnej sieci. W celu zapewniania dodatkowego bezpieczeństwa SMA integruje się z wieloma serwerami AAA (Authentication, Authorization, Accounting) oraz wiodącym

technologiami uwierzytelniania wieloskładnikowego (MFA - Multi-Factor Authentication). Bezpieczne logowanie SSO może być przeprowadzane tylko na autoryzowanych urządzeniach końcowych, po sprawdzeniu przez SMA ich stanu ochrony i zgodności ze standardami. Za sprawą mechanizmu wymuszającego polityki dostępowe użytkownicy mogą widzieć tylko autoryzowane aplikacje, do których po udanym uwierzytelnieniu uzyskują dostęp. Rozwiązanie obsługuje federacyjne logowanie jednokrotne nawet podczas korzystania z klientów VPN, zapewniając użytkownikom bezproblemowe uwierzytelnianie bez względu na to, czy korzystają oni z bezpiecznego dostępu opartego na kliencie, czy bez klienta.

Zapobieganie naruszeniom bezpieczeństwa i zaawansowanym atakom
SonicWall SMA dodaje w organizacji warstwę bezpiecznego dostępu, zwiększając jej ochronę i zmniejszając powierzchnię potencjalnego ataku.

- SMA integruje się z opartym na chmurze wielosilnikowym rozwiązaniem sandboxingu SonicWall Capture ATP, umożliwiając skanowania wszystkich plików przesłanych przez użytkowników z niezarządzanych punktów końcowych lub spoza firmowej sieci. W rezultacie użytkownicy mają zapewniony taki sam poziom ochrony przed zaawansowanymi zagrożeniami (w tym ransomware i złośliwym oprogramowaniem wykorzystującymi luki typu zero-day) bez względu na to czy są w podróży, czy pracują w biurze.[1]
- Usługa SonicWall Web Application Firewall oferuje organizacjom ekonomiczne, dobrze zintegrowane zabezpieczenie wewnętrznych aplikacji webowych. Dzięki niemu firmy mogą zapewnić poufność swoim danym, a wewnętrzne usługi webowe są chronione przed dostępem nieautoryzowanego, złośliwego użytkownika.
- Wykrywanie lokalizacji Geo-IP i ochrona przed botnetami zabezpieczają organizacje przed atakami DDoS oraz skompromitowanymi punktami końcowymi funkcjonującymi jako „zombie".

Bezproblemowy i bezpieczny dostęp w oparciu o przeglądarkę (bez klienta)
SonicWall SMA działa w trybie clientless, dlatego administrator nie musi ręcznie instalować programowego klienta na każdym komputerze, który będzie używany do zdalnego dostępu. W rezultacie ogranicza się koszty działu IT i wszelką zależność od Javy. W takiej rozszerzonej koncepcji zdalnego dostępu nie jest wymagana instalacja lub wstępna konfiguracja punktu końcowego, a autoryzowany pracownik zdalny może usiąść na dowolnym komputerze w wybranym miejscu na świecie i bezpiecznie uzyskać dostęp do swoich zasobów korporacyjnych. W najczystszej postaci bezpieczny dostęp sprowadza się do opartej na HTML5 przeglądarki internetowej, zapewniając użytkownikom bezproblemową i ujednoliconą obsługę.

Obsługa w trybie „Always On"
Aby zapewnić bezproblemową obsługę użytkowników, SMA oferuję funkcję Always On VPN dla zarządzanych urządzeń z systemem Windows. Administratorzy mogą tak skonfigurować ustawienia, aby połączenie VPN było automatycznie nawiązywane za każdym razem, gdy autoryzowany klient punktu końcowego wykryje sieć publiczną lub niezaufaną. Pojedyncze logowanie do urządzenia z systemem Windows zapewnia użytkownikowi bezpieczne połączenie z zasobami firmowymi. Użytkownicy nie muszą logować się do swoich klientów VPN ani używać dodatkowych haseł. Z jednej strony daje to pracownikom mobilnym bezproblemowy dostęp do zasobów o znaczeniu krytycznym – taki, jaki mieliby w w biurze.
Z drugiej strony umożliwia administratorom IT utrzymanie kontroli nad zarządzanymi urządzeniami, podnosząc poziom bezpieczeństwa w organizacji.

Intuicyjne zarządzanie i kompleksowe raportowanie
SonicWall zapewnia intuicyjną webową platformę zarządzania - Central Management Server (CMS), aby usprawnić administrowanie urządzeniami, zapewniając jednocześnie duże możliwości raportowania. Łatwy w użyciu interfejs GUI zapewnia przejrzystość zarządzania zarówno pojedynczymi, jak i wieloma urządzeniami i politykami. Każda strona pokazuje, jak są skonfigurowane ustawienia na wszystkich zarządzanych komputerach. Ujednolicone zarządzanie politykami ułatwia tworzenie i monitorowanie reguł dostępu i konfiguracji. Pojedyncza polityka może kontrolować dostęp użytkowników, urządzeń i aplikacji do danych, serwerów i sieci. Dział IT może automatyzować rutynowe zadania i zaplanować działania, uwalniając zespoły bezpieczeństwa od wykonywania powtarzalnych czynności. W efekcie mogą one skoncentrować się na strategicznych celach związanych z bezpieczeństwem, takich jak reagowanie na incydenty. Dzięki łatwemu w użyciu raportowaniu i scentralizowanemu rejestrowaniu zdarzeń dział IT może obserwować trendy w dostępie użytkowników i śledzić ogólną kondycję systemu.

Zapewnienie dostępności usług 24/7
Aby zapewnić stały bezpieczny dostęp do aplikacji o znaczeniu krytycznym, organizacje wymagają wysokiego stopnia niezawodności w zakresie utrzymania usług. Urządzenia SMA oferują organizacjom posiadającym pojedyncze centra danych tradycyjnie realizowaną wysoką dostępność (HA) w trybie „active-passive. Natomiast w przypadku lokalnych lub rozproszonych data center dostępna jest globalna funkcja HA w trybie „active-active" lub z klastrowanie „active-standby". Oba modele HA zapewniają użytkownikom bezproblemowe działanie przy niezauważalnym przełączaniu awaryjnym i zachowaniu ciągłości sesji.

Skorzystaj z klienta VPN, który odpowiada Twoim potrzebom

Realizację opartego na politykach bezpiecznego zdalnego dostępu dla różnych punktów końcowych, w tym laptopów, smartfonów i tabletów, ułatwia wybór odpowiedniego rozwiązania spośród szerokiej gamy klientów VPN.

Klient VPN	Obsługiwany OS	Model SMA	Kluczowe cechy
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Wszystkie modele	Biometryczne uwierzytelnianie, VPN na poziomie aplikacji, wymuszanie kontroli punktów końcowych
Connect Tunnel (Thin Client)	Windows, Mac OS i Linux	6200, 6210, 7200, 7210, 8200v	Pełna obsługa „jak w biurze" z zaawansowaną kontrolą punktów końcowych
NetExtender (Thin Client)	Windows i Linux	210, 410, 500v	Wymusza szczegółowe polityki dostępu i rozszerza dostęp sieciowy na natywne klienty

Mniejsze koszty eksploatacji dzięki mechanizmowi równoważenia obciążeń

Wbudowana w urządzenie SMA funkcja load balancingu zapewnia skalowalność na poziomu wymaganym przez średniej wielkości firmy i duże korporacje. Wybrane modele urządzeń SMA oferują mechanizm dynamicznego równoważenia obciążeń w celu inteligentnego rozdziału ruchu związanego z sesjami oraz możliwość alokowania licencji użytkowników w czasie rzeczywistym, zgodnie z aktualnymi potrzebami. Organizacje nie muszą inwestować w zewnętrzne moduły równoważące obciążenia, co ogranicza wydatki kapitałowe.

Ubezpieczenie od nieprzewidzianych zdarzeń

Rozwiązanie Disaster Recovery (DR) oraz zachowanie pełnej ciągłości działania wymagają gotowości do radzenia sobie ze znacznym wzrostem ruchu związanym ze zdalnym dostępem przy jednoczesnym zachowaniu bezpieczeństwa oraz kontroli kosztów. Pakiety licencyjne SonicWall Spike dla SMA to dodatkowe licencje, dzięki którym rozproszone organizacje mogą skalować liczbę użytkowników i natychmiast osiągać maksymalną wydajność, zachowując ciągłości działania. Licencje Spike działają jak polisa ubezpieczeniowa na wypadek wszelkich przyszłych planowanych lub nieplanowanych skoków ruchu, powiększając bieżącą liczbę użytkowników o dziesiątki, a nawet setki dodatkowych.

Funkcje

Zaawansowane uwierzytelnianie

Federacyjne SSO[2]	SMA wykorzystuje uwierzytelnianie SAML 2.0 do obsługi federacyjnego SSO przez pojedynczy portal zapewniający dostęp do zasobów zarówno lokalnych, jak i w chmurze. Wymusza też uwierzytelnianie MFA w celu dodatkowej ochrony.
Uwierzytelnianie wieloskładnikowe (MFA - multifactor authentication)	Cyfrowe certyfikaty X.509 Cyfrowe certyfikaty po stronie serwera i klienta RSA SecurID, Dell Defender, Google Authenticator, Duo Security i inne tokeny z jednorazowymi hasłami/dwoma składnikami uwierzytelniania Common Access Card (CAC) UwierzytelnianieDual lub Stacked Obsługa Captcha, login/hasło
Uwierzytelnianie SAML	SMA może być skonfigurowane jako SAML Identity Provider (IdP), SAML Service Provider (SP) albo proxy dla istniejącego lokalnego IdP – w celu uruchomienia federacyjnego SSO przy użyciu uwierzytelniania SAML 2.0.
Repozytoria uwierzytelniania	SMA zapewnia prostą integrację ze standardowymi repozytoriami w celu łatwego zarządzania kontami użytkowników i hasłami. Grupy użytkowników (w tym zagnieżdżone) mogą być tworzone dynamicznie w oparciu o repozytoria uwierzytelniania RADIUS, LDAP lub Active Directory. W specyficznej autoryzacji oraz weryfikacji zarejestrowanego urządzenia mogą być odpytywane typowe i szczególne atrybuty LDAP.
Aplikacyjne proxy Layer 3-7	SMA oferuje elastyczne opcje proxy, np. dostęp dla dostawcy może być zapewniony przez bezpośrednie proxy, dostęp dla kontraktora przez reverse proxy, a dostęp pracownika do Exchange przez ActiveSync.
Reverse proxy	Rozszerzona usługa reverse proxy z uwierzytelnianiem umożliwia administratorom konfigurowanie portalu i zakładek do dostarczania aplikacji. Dzięki temu użytkownicy mogą bezproblemowo łączyć się zdalnie z aplikacjami i zasobami, w tym RDP i HTTP. Ta funkcja obsługuje wszystkie przeglądarki, w tym IE, Chrome i Firefox.
Ograniczona delegacja Kerberos	SMA zapewnia obsługę uwierzytelniania z wykorzystaniem istniejącej infrastruktury Kerberos, nie wymagając zaufania do usług front-end w celu delegowania usługi.

Zarządzanie dostępem

Access Control Engine (ACE)	Administratorzy przyznają albo odmawiają dostępu na podstawie polityk i ustalają działania naprawcze dla sesji w kwarantannie. Obiektowa polityka ACE wykorzystuje elementy związane z siecią, zasobem, tożsamością, urządzeniem, aplikacją, datą i czasem.
End Point Control (EPC)	EPC umożliwia administratorowi wymuszanie szczegółowych reguł kontroli dostępu na podstawie kondycji łączącego się urządzenia. Dzięki głębokiej integracji na poziomie OS możliwe jest łączenie wielu elementów w celu klasyfikacji i oceny ryzyka. Odpytywanie EPC ułatwia tworzenie profilu urządzenia – na podstawie kompleksowej, predefiniowanej listy rozwiązań w rodzaju antywirus, osobisty firewall i antyspyware dla platform Windows, Mac i Linux (w tym ich wersji i posiadanych aktualizacji sygnatur).
App Access Control (AAC)	Administratorzy mogą ustalać, które konkretne aplikacje mobilne mogą mieć dostęp do określonych zasobów w sieci poprzez indywidualne tunele aplikacyjne. Polityki AAC są egzekwowane zarówno na kliencie, jak i serwerze, co zapewnia efektywną ochronę obwodową.

Wyjątkowe bezpieczeństwo

Layer 3 SSL VPN	Seria SMA zapewnia funkcje tunelowania layer-3 o dużej wydajności dla szerokiej gamy urządzeń klienckich działających w dowolnym środowisku.
Obsługa szyfrowania	Konfigurowalna długość sesji Szyfrowanie: AES 128 + 256 bit, Triple DES, RC4 128 bit Hashes: SHA-256 Elliptic Curve Digital Signature Algorithm (ECDSA)
Obsługa zaawansowanych algorytmów szyfrowania	Urządzenie SMA zapewnia od razu wysoki poziom bezpieczeństwa zgodny ze standardami, w tym domyślną konfigurację szyfrowania. Administratorzy mogą sami jeszcze bardziej zwiększać jego możliwości w zakresie wydajności, bezpieczeństwa i kompatybilności.
Certyfikaty bezpieczeństwa	Certyfikowane dla: FIPS 140-2 Level 2, ICSA SSL-TLS, In-progress for Common Criteria, UC-APL
Bezpieczne współdzielenie plików	Blokowanie na bramie nieznanych ataków typu zero-day, w tym ransomware, wraz z zautomatyzowanymi działaniami naprawczymi. Pliki przesyłane przez niezarządzane punkty końcowe są w ramach bezpiecznego dostępu do sieci firmowej badane przez oparte na chmurze wielosilnikowe rozwiązanie Capture ATP.
Web Application Firewall (WAF)	Chroni przed opartymi na protokołach i webie atakami, ułatwiając sektorowi finansowemu, ochronie zdrowia, firmom e-commerce i innym organizacjom osiągać zgodność z OWASP Top 10 i PCI.
Detekcja Geo IP i ochrona przed botnetami	Dzięki detekcji Geo IP i ochronnie przed botnetami organizacje mogą przyznawać lub odmawiać dostępu użytkownikom na podstawie ich lokalizacji geograficznej.

Intuicyjna obsługa użytkownika

Always On VPN	Automatycznie ustanawia połączenie zarejestrowanego urządzenia z systemem Windows z firmową siecią. Zapewnia większy wgląd w komunikacje i zgodność z regulacjami
Secure Network Detection (SND)	Klient VPN dla SMA wykrywa, kiedy urządzenie jest poza firmową siecią i automatycznie ustanawia połączenie szyfrowane. Następnie, jeśli urządzenie znowu znajdzie się w zasięgu zaufanej sieci, wyłącza je.
Dostęp do zasobów w trybie clientless	SMA zapewni a bezpieczny dostęp do zasobów bez programowego klienta – poprzez agenty przeglądarki HTML5 i udostępnienie protokołów RDP, ICA, VNC, SSH i Telnet
Portal SSO (Single Sign -On)	Portal WorkPlace oferuje łatwy w użyciu, dostosowywany interfejs dla bezpieczneg o dostępu do dowolnych zasobów w środowisku hybrydowego IT po jednokrotnym logowaniu (SSO)
Tunelowanie Layer 3	W celu uzyskania największej wydajności administratorzy mogą wybierać pomiędzy trybami Split-Tunnel oraz Redirect -All z tunelowaniem SSL/TLS i opcjonalną funkcją ESP fallback.
Przeglądarka plików HTML5	Nowoczesny eksplorator plików daje użytkownikom możliwość łatwego ich współdzielenia poprzez dowolną przeglądarkę internetową.
Integracja mobilnych OS	Funkcjonalność Mobile Connect jest obsługiw ana na wszystkich platformach systemowych, co daje użytkownikom pełną elastyczność w wyborze urządzeń mobilnych.

Niezawodność

Global Traffic Optimizer (GTO)	SMA oferuje globalne równoważenie obciążeń związanych z ruchem, bez wpływu na obsługę użytkowników. Ruch jest przekierowywany do najlepiej zoptymalizowanego i najwydajniejszego w danym momencie data center.
Dynamiczne HA (High Availability) [2]	W zależności od wdrożenia w pojedynczym albo rozproszonym geograficznie data center SMA obsługuje konfiguracje Active/Passive i Active/Active, zapewniając wysoką dostępność (HA).
Universal Session Persistence [1]	Funkcja podtrzymania sesji zapewnia użytkownikom bezproblemową i nieprzerwaną obsługę. W przypadku wyłączenia któregoś z urządzeń inteligentne klastrowanie SMA realokuje użytkowników i dane ich sesji, nie wymagając powtórnego uwierzytelniania.
Skalowalna wydajność	SMA skaluje wykładniczo wydajność poprzez wdrażanie kolejnych urządzeń, co dodatkowo eliminuje pojedynczy punkt awarii. Poziome klastrowanie daje możliwość łączenia fizycznych i wirtualnych urządzeń SMA.
Dynamiczne licencjonowanie	Licencje użytkownika nie muszą już być przypisane do konkretnych urządzeń SMA. Można je dystrybuować i przypisywać dynamicznie pomiędzy zarządzanym urządzeniami, w zależności od bieżących potrzeb.

Centralne zarządzanie i monitoring

Central Management System (CMS)	CMS zapewnia scentralizowane, oparte na przeglądarce zarządzanie wszystkimi funkcjonalnościami SMA.
Alerty użytkownika	Alerty można skonfigurować w oparciu o pułapki SNMP, które są monitorowane przez każdy system NMS (Network Management System) w infrastrukturze IT. Administratorzy mogą także skonfigurować alerty dla skanowania plików przez Capture ATP oraz dla wykorzystania dysków.
Pulpit czasu rzeczywistego	Działający w czasie rzeczywistym i dostosowywany pulpit umożliwia administratorom szybkie i łatwe diagnozowanie problemów z dostępem.
Integracja SIEM	Dzięki przekazywaniu w czasie rzeczywistym danych do systemów SIEM zespoły ds. bezpieczeństwa mogą korelować związane ze zdarzeniami działania i określać pełen przepływ pracy dla konkretnego użytkownika lub aplikacji. Ma to duże znaczenie w zarządzaniu incydentami bezpieczeństwa oraz w analizie śledczej.
Harmonogram	Można tworzyć harmonogram dla zadań utrzymania, takich jak: ustalanie polityk, powielanie ustawień konfiguracyjnych i restartowanie urządzeń - które nie będą następnie wymagać czynności manualnych.

Rozbudowa rozwiązania

API do zarządzania	Interfejsy API do zarządzania dają pełną programistyczną i administracyjną kontrolę nad wszelkimi obiektami w ramach pojedynczego środowiska SMA lub globalnego CMS.
API użytkownika końcowego	Interfejsy API użytkownika końcowego dają pełna kontrolę nad logowaniem, uwierzytelnianiem i przepływem pracy dotyczącym punktów końcowych.
Dwuskładnikowe uwierzytelnianie (2FA)	SMA zapewnia uwierzytelnianie 2FA poprzez integrację z popularnymi rozwiązaniami czasowych haseł jednorazowych (TOTP - time-based one-time password), takimi jak Google Authenticator, Microsoft Authenticator, Duo security itp.
Integracja MDM	SMA integruje się z popularnymi rozwiązaniami EMM (Enterprise Mobile Management), takimi jak np. Airwatch i Mobile Iron.
Dodatkowe integracje z niezależnymi rozwiązaniami	Aby zapewnić zaawansowaną ochronę przed zagrożeniami, SMA integruje się z wiodącymi w branży producentami, takimi jak OPSWAT.

[1] *Dostępne z systemem SMA OS 12.1 lub nowszym*

[2] *Rozszerzone w SMA 12.1*

Zestawienie funkcjonalności (według modelu SMA)

Kategoria	Funkcja	210	410	500v	6210	7210	8200v
Przepustowość	Maks. liczba jednoczesnych sesji użytkowników	50	250	250	2,000	10,000	5,000
	Maks. przepustowość SSL/TLS	560 Mb/s	844 Mb/s	186 Mb/s	800 Mb/s	5.0 Gb/s	1.58 Gb/s
Dostęp kliencki	Layer 3 tunnel	•	•	•	•	•	•
	Split-tunnel and redirect-all	•	•	•	•	•	•
	Always On VPN	•	•	•	•	•	•
	Auto ESP encapsulation	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Secure Network Detection	–	–	–	•	•	•
	File browser (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	On Demand tunnel	–	–	–	•	•	•
	Chrome/Firefox extensions	–	–	–	•	•	•
	CLI tunnel support	–	–	–	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	Net Extender (Windows,Linux)	•	•	•	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
Dostęp mobilny	Per app VPN	–	–	–	•	•	•
	App control enforcement	–	–	–	•	•	•
	App ID validation	–	–	–	•	•	•
Portal użytkownika	Branding	•	•	•	•	•	•
	Customization	–	–	–	•	•	•
	Localization	•	•	•	•	•	•
	User defined bookmarks	•	•	•	•	•	•
	Custom URL support	•	•	•	•	•	•
	SaaS application support	–	–	–	•	•	•
Bezpieczeństwo	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	–	–	–	•	•	•
	Suite B ciphers	–	–	–	•	•	•
	Dynamic EPC interrogation	•	•	•	•	•	•
	Role Based Access Control (RBAC)	–	–	–	•	•	•
	Endpoint registration	•	•	•	•	•	•
	Secure File Share (Capture ATP)	•	•	•	•	•	•
	Endpoint quarantine	•	•	•	•	•	•
	OSCP CRL validation	–	–	–	•	•	•
	Cipher selection	–	–	–	•	•	•
	PKI and client certificates	•	•	•	•	•	•
	Geo IP filter	•	•	•	–	–	–
	Botnet filter	•	•	•	–	–	–
	Forward proxy	•	•	•	•	•	•
	Reverse proxy	•	•	•	•	•	•
Uwierzytelnianie i usługi oparte na tożsamości	SAML 2.0	–	–	–	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML Identity Provider (IdP)	–	–	–	•	•	•
	Biometric device support	•	•	•	•	•	•
	Face ID support for iOS	•	•	•	•	•	•
	Two-factor authentication (2FA)	•	•	•	•	•	•
	Multi-factor authentication (MFA)	–	–	–	•	•	•

Zestawienie funkcjonalności (według modelu SMA) cd.

Kategoria	Funkcja	210	410	500v	6210	7210	8200v
Uwierzytelnianie i usługi oparte na tożsamości cd.	Chained authentication	–	–	–	●	●	●
	One Time Passcode(OTP) via email or SMS	●	●	●	●	●	●
	Common Access Card (CAC) support	–	–	–	●	●	●
	X.509 certificate support	●	●	●	●	●	●
	Captcha integration	–	–	–	●	●	●
	Remote password change	●	●	●	●	●	●
	Forms based SSO	●	●	●	●	●	●
	Federated SSO	–	–	–	●	●	●
	Session persistence	–	–	–	●	●	●
	Auto logon	●	●	●	●	●	●
Kontrola dostępu	Group AD	●	●	●	●	●	●
	LDAP attributes	●	●	●	●	●	●
	Geolocation policies	●	●	●	–	–	–
	Continual endpoint monitoring	●	●	●	●	●	●
Zarządzanie	Management interface (ethernet)	–	–	–	●	●	●
	Management interface (console)	–	–	–	●	●	●
	HTTPS administration	●	●	●	●	●	●
	SSH administration	–	–	–	●	●	●
	SNMP MIBS	●	●	●	●	●	●
	Syslog and NTP	●	●	●	●	●	●
	Usage monitoring	●	●	●	●	●	●
	Configuration rollback	●	●	●	●	●	●
	Centralized management	–	–	–	●	●	●
	Centralized reporting	–	–	–	●	●	●
	Management REST APIs	–	–	–	●	●	●
	Authentication REST APIs	–	–	–	●	●	●
	RADIUS accounting	–	–	–	●	●	●
	Scheduled tasks	–	–	–	●	●	●
	Centralized session licensing	–	–	–	●	●	●
	Event-driven auditing	–	–	–	●	●	●
Sieć	IPv6	●	●	●	●	●	●
	Global load balancing	–	–	–	●	●	●
	Server load balancing	●	●	●	–	–	–
	TCP state replication	●	●	●	●	●	●
	Cluster state failover	–	–	–	●	●	●
	Active/passive high availability	–	●	●	●	●	●
	Active/active high availability	–	–	–	●	●	●
	Horizontal scalability	–	–	–	●	●	●
	Single or multiple FQDNs	–	–	–	●	●	●
	L3-7 smart tunnel proxy	●	●	●	●	●	●
	L7 application proxy	●	●	●	●	●	●
Integracja	2FA TOTP support	●	●	●	●	●	●
	EMM and MDM product support	–	–	–	●	●	●
	SIEM product support	–	–	–	●	●	●
	TPAM password vault	–	–	–	●	●	●
	ESX hypervisor support	–	–	●	–	–	●
	Hyper-V hypervisor support	–	–	●	–	–	●
Opcje licencyjne	Subscription based license	–	–	–	●	●	●
	Perpetual license with support	●	●	●	●	●	●
	Web Application Firewall (WAF)	●	●	●	–	–	–
	Spike licensing	●	●	●	●	●	●
	Tiered licensing	–	–	–	●	●	●
	Virtual assist	●	●	●	–	–	–

** Więcej informacji o klientach VPN na stronie: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

SONICWALL®

Korzyści z migracji na urządzenia klasy high end

Wyższa wydajność | Większa przepustowość | Zaawansowane funkcje | Większa skalowalność

Specyfikacje urządzeń

Wybierz spośród wielu specjalnie zaprojektowanych urządzeń zapewniających bezpieczny mobilny dostęp (SMA). Skorzystaj z elastycznych opcji wdrażania, zapewnianych przez wirtualne i fizyczne urządzenia.

Specyfikacje urządzeń fizycznych

Wydajność	SMA 210	SMA 410	SMA 6210	SMA 7210
Jednoczesne sesje/użytkownicy	do 50	do 250	do 2,000	do 10,000
Przepustowość SSL VPN* (przy maks. CCU)	560 Mb/s	844 Mb/s	do 800 Mb/s	do 5.0 Gb/s
Obudowa	1U	1U	1U	1U
Wymiary	16.92 x 10.23 x 1.75 in (43x26x4.5cm)	16.92 x 10.23 x 1.75 in (43x26x4.5cm)	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)
Waga	11 lbs (5 kg)	11 lbs (5 kg)	17.7 lbs (8 kg)	18.3 lbs (8.3 kg)
Akceleracja szyfrowania danych (AESNI)	NIE	NIE	TAK	TAK
Dedykowany port zarządzania	NIE	NIE	TAK	TAK
Akceleracja SSL	NIE	NIE	TAK	TAK
Storage	4GB (Flash Memory)	4GB (Flash Memory)	2 x 1TB SATA; RAID 1	2 x 1TB SATA; RAID 1
Interfejsy	(2) GB Ethernet, (2)USB, (1) console	(4) GB Ethernet, (2)USB, (1) console	(6)-port 1GE, (2) USB, (1) console	(6)-port 1GE, (2)-port 10Gb SFP+, (2) USB, (1) console
Pamięć	4GB	8GB	8GB DDR4	16GB DDR4
Czip TPM	NIE	NIE	TAK	TAK
Procesor	4 rdzenie	8 rdzeni	4 rdzenie	4 rdzenie
MTBF (@ 25°C lub 77°F) w godz.	61,815	60,151	70,127	129,601
Operacje i zgodność	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
Zasilanie	Fixed power supply	Fixed power supply	Fixed power supply	Dual power supply, hot swappable
Parametry zasilania	100-240VAC, 50-60MHz	100-240VAC, 50-60MHz	100-240 VAC, 1.1 A	100-240 VAC, 1.79 A
Zużycie energii	26.9 W	31.9 W	77 W	114 W
Odprowadzanie ciepła	92 BTU	109 BTU	264 BTU	389 BTU
Certyfikaty środowiskowe	WEEE, EU RoHS, China RoHS			
Odporność na wstrząsy	110 g, 2 ms			
Emisja	FCC, ICES, CE, C-Tick, VCCI; MIC			
Bezpieczeństwo	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme			
Zakres temperatury	0°C do 40°C (32°F do 104° F)			
Certyfikacja FIPS	NIE	NIE	FIPS 140-2 Level 2 with anti-tamper protection	

**Przepustowość może zależeć od warunków wdrożenia i łączności. Publikowane wyniki są oparte na pomiarach wykonanych w laboratorium*

Specyfikacje urządzeń wirtualnych

Specyfikacje	SMA 500v (ESX/ESXi/HyperV)	SMA 8200v (ESX/ESXi/HyperV)
Jednoczesne sesje	do 250 użytkowników	do 5000
Przepustowość SSL VPN* (przy maks. CCU)	do 186 Mb/s	do 1.58 Gb/s
Alokowana pamięć	2GB	8 GB
Procesor	1 rdzeń	4 rdzenie
Akceleracja SSL	NIE	TAK
Zastosowana pojemność dyskowa	2GB	64 GB (default)
Zainstalowany system operacyjny	Linux	Hardened Linux
Dedykowany portzarządzania	NIE	TAK

**Przepustowość może zależeć od warunków wdrożenia i łączności. Publikowane wyniki są oparte na pomiarach wykonanych w laboratorium. SMA 8200v na Hyper-V skaluje się do 5000 jednoczesnych sesji i zapewnia przepustowość SSL-VPN do 1.58 Gb/s (z systemem SMA OS 12.1 i Windows Server 2016)*

informacje dotyczące zamówień

SKU	SONICWALL SECURE MOBILE ACCESS (SMA) APPLIANCE
02-SSC-2800	SMA 210 with 5 user license
02-SSC-2801	SMA 410 with 25 user license
01-SSC-8469	SMA 500v with 5 user license
02-SSC-0978	SMA 7210 with administrator test license
02-SSC-0976	SMA 6210 with administrator test license
01-SSC-8468	SMA 8200v (virtual appliance)
SKU	**SONICWALL SMA USER LICENSES**
01-SSC-9182	SMA 500V add 5 user (Also available for SMA 210)
01-SSC-2414	SMA 500V add 100 user (Also available for SMA 410)
01-SSC-7856	SMA 5 user license- stackable for 6210, 7210, 8200v
01-SSC-7860	SMA 100 user license- stackable for 6210, 7210, 8200v
01-SSC-7865	SMA 5000 user license- stackable for 7210, 8200v
SKU	**SONICWALL SMA SUPPORT CONTRACT**
01-SSC-9191	24X7 support for SMA 500V up to 25 user 1yr (Also available for SMA 210 & 410)
01-SSC-2326	24X7 support for SMA 6210 100 user 1yr stackable
01-SSC-2350	24X7 support for SMA 7210 500 user 1yr stackable
01-SSC-8434	24X7 support for SMA 8200V 5 user 1yr stackable (Also available for SMA 6210, 7210)
01-SSC-8446	24X7 support for SMA 8200V 100 user 1yr stackable (Also available for SMA 6210, 7210)
01-SSC-7913	24X7 support for SMA 8200V 5000 user 1yr stackable (Also available for SMA 6210, 7210)
SKU	**CENTRAL MANAGEMENT FOR 6210, 7210, 8200V**
CMS appliance license	
01-SSC-8535	CMS base + 3 appliance license (Free- for Trials and use with subscription user licenses)
01-SSC-8536	CMS 100 appliances license1yr (for use with subscription user licenses)
01-SSC-3369	CMS base + 3 appliances (Free- for use with perpetual user licenses)
01-SSC-3402	CMS 100 appliance license 1yr (for use with perpetual user licenses)
Central user licenses (subscription)	
01-SSC-2298	CMS pooled license 10 user 1yr
01-SSC-8539	CMS pooled license 1000 user 1yr
01-SSC-5339	CMS pooled license 50000 user 1yr
Central user licenses (perpetual)	
01-SSC-2053	CMS perpetual license 10 user
01-SSC-2058	CMS perpetual license 1000 user
01-SSC-2063	CMS perpetual license 50000 user
Support for central user licenses (perpetual)	
01-SSC-2065	CMS 24x7 support 1yr 10 user
01-SSC-2070	CMS 24x7 support 1yr 1000 user
01-SSC-2075	CMS 24x7 support 1yr 50000 user
Central ActiveSync licenses (subscription)	
01-SSC-2088	CMS pooled email license 10 user 1yr
01-SSC-2093	CMS pooled email license 1000 user 1yr
01-SSC-2087	CMS pooled email license 50000 user 1yr

informacje dotyczące zamówień cd.

Central spike licenses	
01-SSC-2111	CMS spike 1000 user 5days
01-SSC-2115	CMS spike 50000 user 5days
Capture add-on (subscription)	
Skontaktuj się ze swoim resellerem ** Licencje subskrypcji obejmują wsparcie 24X7*	
SKU	**SONICWALL SMA ADD-ONS**
01-SSC-2406	SMA 7210 FIPS add-on
01-SSC-2405	SMA 6210 FIPS add-on
01-SSC-9185	SMA 500V Web Application Firewall 1 YR (Also available for SMA 210 & 410)
SKU	**SONICWALL SMA SECURE UPGRADE**
02-SSC-2794	SMA 210 Secure Upgrade Plus, 5 User Bundle with 24X7 support up to 25 users 1yr
02-SSC-2795	SMA 210 Secure Upgrade Plus, 5 User Bundle with 24X7 support up to 25 users 3yr
02-SSC-2798	SMA 410 Secure Upgrade Plus, 25 User Bundle with 24X7 support up to 100 users 1yr
02-SSC-2799	SMA 410 Secure Upgrade Plus, 25 User Bundle with 24X7 support up to 100 users 3yr
02-SSC-2893	SMA 6210 Secure Upgrade Plus, 24X7 support up to 100 users 1yr
02-SSC-2894	SMA 6210 Secure Upgrade Plus, 24X7 support up to 100 users 3yr
02-SSC-2895	SMA 7210 Secure Upgrade Plus, 24X7 support up to 250 users 1yr
02-SSC-2896	SMA 7210 Secure Upgrade Plus, 24X7 support up to 250 users 3yr
SKU	**SPIKE LICENSE FOR SMA (INCREMENTAL NEEDED TO REACH CAPACITY)**
01-SSC-2240	SMA 210 10 day 50 user spike license (Also available for SMA 410 and 500v)
01-SSC-7873	SMA 8200v 10 day 5-2500 user spike license (Also available for SMA 6210, 7210)

**Dostępne również wieloletnie SKUs i umowy wsparcia. Pełną listę SKU posiada reseller lub dział handlowy*

Potrzebujecie pomocy w planowaniu, wdrażaniulub optymalizacji rozwiązania SonicWall? Partnerzy działający w ramach SonicWall Advanced Services zapewnią Wam światowej klasy usługi profesjonalne. Więcej informacji na stronie www.sonicwall.com/PES

O firmie

SonicWall od ponad 28 lat zapobiega cyberprzestępstwom, broniąc małe i średnie przedsiębiorstwa oraz korporacje i instytucje rządowe na całym świecie. Wsparta przez SonicWall Capture Labs, wielokrotnie nagradzane firmowe rozwiązanie do wykrywania i zapobiegania naruszeniom bezpieczeństwa w czasie rzeczywistym, zabezpiecza ponad milion sieci, pocztę e-mail, aplikacje i dane w ponad 215 krajach i terytoriach. Chronione organizacje działają wydajniej i mniej się obawiają się o swoje bezpieczeństwo. Aby uzyskać więcej informacji, odwiedź stronę www.sonicwall.com lub śledź nas na Twitterze, LinkedIn, Facebooku i Instagramie.

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

Datasheet-SecureMobileAccess-US-VG-1385