



# SA SERIES SSL VPN APPLIANCES (SA2500, SA4500, SA6500)

## Ogólny zarys produktu

Seria SA Urządzeń SSL VPN firmy Juniper Networks przewodzi na rynku SSL VPN dzięki kompletnej ofercie urządzeń zdalnego dostępu, z takimi produktami nowej generacji jak urządzenia Juniper Networks SA2500 SSL VPN, Juniper Networks SA4500 SSL VPN i Juniper Networks SA6500 SSL VPN o wysokiej skalowalności i redundancji, zaprojektowanymi specjalnie z myślą o dużych przedsiębiorstwach i usługodawcach. Seria SA łączy w sobie bezpieczeństwo protokołu SSL i zgodną ze standardami kontrolę dostępu z kreowaniem szczegółowej polityki i niezrównaną elastycznością. Efektem jest zapewnienie wszechobecnej ochrony wszystkich zadań danego przedsięwzięcia z opcją kontroli dostępowej na niezwykle drobiazgowym poziomie, aby zabezpieczać najbardziej wrażliwe aplikacje i dane. Urządzenia SSL VPN z serii SA firmy Juniper Networks gwarantują niższy całkowity koszt utrzymania niż tradycyjne rozwiązania IPsec oraz unikatowe cechy bezpieczeństwa typu „end-to-end”.

## Opis produktu

Juniper Networks przedstawia nową generację wiodących na rynku urządzeń serii SA SSL VPN. Nowe SA2500, SA4500 i SA6500 są urządzeniami SSL VPN, które spełniają wymagania firm każdego rozmiarów. Urządzeniem SA 6500 Juniper potwierdza swoją dominację na rynku, dostarczając wysoko skalowalne rozwiązanie bazujące na rzeczywistych testach wydajnościowych. Urządzenia serii SA używają protokołu SSL, który znaleźć można we wszystkich standardowych przeglądarkach WWW. Użycie SSL likwiduje potrzebę instalacji oprogramowania po stronie klienta lub zmian na wewnętrznych serwerach oraz eliminuje koszty związane z konserwacją i obsługą techniczną stacji końcowych. Urządzenia Juniper Networks serii SA oferują także zaawansowane funkcje partner/klient dla sieci ekstranet, które umożliwiają kontrolę dostępu do użytkowników i ich grup bez konieczności wprowadzania zmian w infrastrukturze, tworzenia stref zdemilitaryzowanych (DMZ) oraz instalowania agentów programowych.

## Architektura i kluczowe komponenty

Model Juniper Networks SA2500 SSL VPN umożliwia małym i średnim przedsiębiorstwom uzyskanie zdalnego dostępu do zasobów sieciowych oraz sieci ekstranet, jak również zapewnia bezpieczeństwo sieci intranet. Użytkownicy mogą łączyć się z siecią przedsiębiorstwa z jakiegokolwiek komputera podłączonego do Internetu. Model SA2500 oferuje wysoką dostępność (HA) oraz płynne funkcjonowanie systemu w razie pojawienia się usterki. Ponieważ urządzenie SA2500 używa dokładnie tego samego oprogramowania co większe modele SA4500 i SA6500, nawet mniejsze organizacje uzyskują tę samą wysoką wydajność, administracyjną elastyczność.

Dzięki modelowi Juniper Networks SA4500 SSL VPN średnie oraz duże przedsiębiorstwa bez większych nakładów finansowych mogą zapewnić dostęp do sieci ekstranet jedynie za pomocą przeglądarki WWW. Jedną z cech urządzeń z serii SA4500 jest wysoka funkcjonalność zarządzania prawami dostępu, która może być wykorzystana przy tworzeniu bezpiecznych sieci ekstranet klient-partner. Ta funkcjonalność pozwala przedsiębiorcy zabezpieczyć również dostęp do sieci intranet, dzięki czemu pracownicy lub goście mogą skorzystać z dokładnie tych zasobów sieci, które są im aktualnie potrzebne, jednocześnie nie naruszając polityki bezpieczeństwa przedsiębiorstwa. Wbudowana kompresja dla wszystkich typów ruchu sieciowego zwiększa wydajność. Dostępna jest również sprzętowa akceleracja SSL dla bardziej wymagających środowisk. Model SA 4500 oferuje również wysoką dostępność (HA) wraz z płynnym funkcjonowaniem systemu w razie pojawienia się usterki.

Model SA6500 SSL VPN przeznaczony jest dla dużych przedsiębiorstw i usługodawców. Charakteryzuje go najlepsza w tej klasie produktów wydajność, skalowalność oraz możliwość budowania konfiguracji nadmiarowych, dzięki czemu sprawdza się w organizacjach mających wyższe wymagania odnośnie bezpiecznego dostępu oraz autoryzacji. SA6500 posiada również wbudowaną kompresję dla Web i plików, oraz najwyższej klasy chipset przyspieszający szyfrowanie SSL, który odciąża procesor z wykonywania procesów szyfrowania i odszyfrowania.

Ponieważ każde z urządzeń Juniper Networks serii SA SSL VPN używa tego samego oprogramowania, nie ma zależności pomiędzy doświadczeniem użytkowników lub administratorów a wyborem urządzenia. Wszystkie urządzenia oferują najwyższą wydajność, stabilność i skalowalność. Dlatego też decyzję co do wyboru urządzenia, które najlepiej spełni potrzeby twojej organizacji łatwo podjąć na podstawie ilości użytkowników, redundancji systemu, możliwości akceleracji na dużą skalę i potrzeb rosnącej populacji użytkowników korzystających ze zdalnego dostępu.

- **SA2500:** Wspiera przedsiębiorstwa małych i średnich rozmiarów jako ekonomiczne rozwiązanie, które bez problemu obsłuży do 100 użytkowników jednocześnie w pojedynczym systemie lub w klastrze składającym się z dwóch węzłów.
- **SA4500:** Umożliwia średnim i dużym organizacjom obsłużyć 1000 użytkowników jednocześnie w pojedynczym systemie. Oferuje opcję przejścia na sprzętową akcelerację SSL dla tych organizacji, które wymagają najwyższej wydajności przy dużym obciążeniu.
- **SA6500:** Zbudowany z myślą o dużych przedsiębiorstwach i usługodawcach, SA6500 zapewnia najlepszą w swojej klasie wydajność, skalowalność i redundancję dla organizacji z wysokimi wymaganiami odnośnie bezpiecznego dostępu i autoryzacji. Obsługuje aż do 10000 użytkowników jednocześnie w pojedynczym systemie lub dziesiątki tysięcy użytkowników jednocześnie w klastrze składającym się z czterech węzłów.

## Standardowe właściwości SA6500

- Podwójne dyski twarde o zapisie lustrzanym, w technologii Serial Advanced Technology Attachment (SATA) z możliwością wymiany lub naprawy bez przerywania pracy całego urządzenia,
- Podwójne wentylatory z możliwością wymiany lub naprawy bez przerywania pracy całego urządzenia,
- Zasilacz z możliwością wymiany lub naprawy bez przerywania pracy całego urządzenia ,
- 4 GB SDRAM,
- 4-portowa karta sieciowa 10/100/1000,
- 1-portowy interfejs zarządzający 10/100/1000,
- Sprzętowy moduł akceleracji SSL.

## Opcjonalne właściwości SA 6500

- Drugi zasilacz lub zasilacz prądu stałego DC,
- 4-portowa karta sieciowa typu small form-factor pluggable (SFP).

## Właściwości i zalety

### Wysoka skalowalności w modelu Secure Access 6500 SSL VPN

SA 6500 został stworzony, aby sprostać zwiększającym się potrzebom dużych przedsiębiorstw i usługodawców, w związku z czym posiada możliwość obsługi tysięcy użytkowników zdalnie łączących się z siecią. Poniżej podane zostały dane liczbowe dotyczące ilości użytkowników, którzy mogą być jednocześnie obsługiwani przez platformę SA6500:

- Pojedyncze urządzenie SA6500: obsługuje maksymalnie 10000 użytkowników jednocześnie,
- Klaster złożony z dwóch jednostek SA6500: obsługuje maksymalnie 18000 użytkowników jednocześnie,
- Klaster złożony z trzech jednostek SA6500: obsługuje maksymalnie 26000 użytkowników jednocześnie,
- Klaster złożony z czterech jednostek SA 6500: obsługuje maksymalnie 30000 użytkowników jednocześnie.

Testy wydajności oparte zostały na symulacjach przeprowadzonych w istniejących środowiskach sieciowych.

W przypadku dostępu do rdzenia oznacza to uzyskiwanie dostępu do rzeczywistych aplikacji Web, co niesie za sobą rygorystyczną kontrolę kodu HTML oraz ewaluację polityki przedsiębiorstwa.

## Warstwowa ochrona typu end-to-end

Modele SA 2500, SA 4500 i SA 6500 zapewniają warstwową ochronę typu end-to-end obejmującą klienta końcowego, urządzenia, dane oraz serwery.

**Tabela 1: Warstwowa ochrona typu End-to-End, właściwości i zalety**

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Federacja UAC-SA	Nieprzerwanie dostosowuje sesje użytkownika serii SA do Juniper Networks Unified Access Control w ramach logowania – i odwrotnie (importuje sesje UAC do serii SA). Tożsamość użytkowników jest weryfikowana tylko jeden raz przed zezwoleniem im na dostęp do tego typu środowisk.	Zapewnia użytkownikom – czy to lokalnym czy zdalnym – ciągły dostęp w ramach pojedynczego logowania do korporacyjnych zasobów zabezpieczanych przez reguły kontroli dostępowej UAC lub serii SA. Upraszcza obsługę dla użytkownika końcowego.
Automatyczne naprawy SMS	Automatycznie dostosowuje niezgodne stacje końcowe poprzez aktualizację aplikacji odbiegających od korporacyjnych reguł bezpieczeństwa. Dynamicznie inicjuje aktualizacje tych aplikacji na stacji końcowej przy użyciu protokołu Microsoft SMS.	Zwiększa wydajność zdalnych użytkowników, zapewniając im natychmiastowy dostęp do korporacyjnej sieci bez konieczności oczekiwania na okresowe aktualizacje oprogramowania i gwarantuje zgodność z korporacyjnymi regułami bezpieczeństwa.
Kontroler Hosta (Host Checker)	Klienci mogą być kontrolowani zarówno tuż przed, jak i w trakcie sesji w celu weryfikacji czy dane urządzenie posiada wystarczające zabezpieczenia w postaci odpowiednich aplikacji (oprogramowanie antywirusowe, firewall, itp.). Funkcja ta może być dostosowywana do wymagań i opierać się na weryfikacji portów otwartych/zamkniętych, na sprawdzaniu plików/procesów i weryfikacji ich autentyczności zgodnie z sumami kontrolnymi Message Digest 5 (MD 5), na weryfikacji ustawień rejestru, certyfikatów urządzenia i wielu innych.	Weryfikuje, czy urządzenie końcowe spełnia standardy bezpieczeństwa przedsiębiorstwa przed udzieleniem dostępu, w razie potrzeby dostosowując urządzenie lub poddając użytkownika kwarantannie.
Interfejs API kontrolera hosta	Stworzony przy współpracy z najlepszymi w swojej klasie dostawcami zabezpieczeń stacji końcowych, pozwala przedsiębiorstwom narzucić swoją politykę bezpieczeństwa wobec zarządzanych PC posiadających zainstalowany firewall, oprogramowanie antywirusowe lub inne oprogramowanie zabezpieczające, jednocześnie poddając kwarantannie urządzenia z nią niezgodne.	Podporządkowanie użytkowników i urządzeń zdalnych aktualnej polityce bezpieczeństwa; łatwiejsze zarządzanie.
Obsługa zaufanych połączeń sieciowych (Trusted Network Connect – TNC) na kontrolerze hosta	Umożliwia kooperację z różnorodnymi rozwiązaniami zabezpieczającymi, od oprogramowania antywirusowego, przez zarządzanie poprawkami, po rozwiązania odpowiedzialne za standaryzację.	Pozwala klientom użytkować istniejące systemy bezpieczeństwa stacji końcowej pochodzące od innych dostawców.
Egzekwowanie polityk	Pozwala przedsiębiorstwu ustalić, czy dany host niezgodny z API jest godny zaufania bez potrzeby pisania dedykowanych implementacji API lub blokowania użytkowników zewnętrznych, takich jak klienci lub partnerzy korzystający z innych rozwiązań zabezpieczających.	Umożliwia uzyskanie dostępu do końcowych urządzeń sieci ekstranet, takich jak komputery PC partnerom, którzy mogą korzystać z rozwiązań zabezpieczających odmiennych od tych wykorzystywanych przez przedsiębiorstwo.
Wzmocnione urządzenie zabezpieczające	Zaprojektowany na bazie specjalnie stworzonego systemu operacyjnego.	Urządzenie jest mniej podatne na ataki, ponieważ nie zostało zaprojektowane do wykonywania jakichkolwiek dodatkowych zadań; brak luk typu backdoor, które mogłyby być wykorzystane przez hackerów.
Usługi zabezpieczeń wykorzystujące filtrowanie pakietów i bezpieczne rutowanie na poziomie jądra	Niepożądane pakiety danych są blokowane zanim rozpocznie się ich przetwarzanie przez stos TCP.	Odfiltrowuje niewiarygodne próby połączenia, takie jak zniekształcone pakiety lub ataki typu DOS.
Bezpieczna wirtualna przestrzeń robocza (Secure Virtual Workspace)	Bezpieczne, odseparowane środowisko obsługujące sesje zdalne, w którym szyfrowane są wszystkie dane i kontrolowane są połączenia do urządzeń I/O (drukarki, dyski, itp.).	Gwarantuje, że po zakończonej sesji wszelkie dane należące do przedsiębiorstwa są kasowane z terminali komputerowych lub innych punktów końcowych nie zarządzanych przez systemy przedsiębiorstwa.
Czyszczenie pamięci podręcznej (Cache Cleaner)	Wszystkie pośrednie i tymczasowe pliki zainstalowane podczas sesji są usuwane przy wylogowaniu.	Gwarantuje, że żadne potencjalnie wrażliwe dane wykorzystywane podczas sesji, nie są pozostawiane na urządzeniu końcowym.
Pułapki dla danych i kontrola pamięci podręcznej	Transformacja danych na formaty niebuforowane.	Uniemożliwia opuszczenie sieci poufnym metadaniem (pliki cookie, nagłówki, formularze, itp.).
Zintegrowana ochrona przed złośliwym oprogramowaniem	Wcześniej zainstalowane oprogramowanie sprawdzające chroni użytkowników i urządzenia przed keyloggerami, trojanami oraz aplikacjami zdalnego dostępu.	Pozwala klientom wzmocnić ochronę stacji końcowej.
Skoordynowana kontrola zagrożeń	Umożliwia urządzeniom Juniper SA SSL VPN oraz systemom wykrywania intruzów (IDP) powiązać daną sesję SSL VPN z funkcjami wykrywającymi IDP, podejmując automatyczne działania przeciw użytkownikom odpowiedzialnym za ataki.	Zapewnia skuteczną identyfikację, powstrzymywanie i zapobieganie zagrożeniom, zarówno na poziomie sieci jak i aplikacji, w obrębie sieci zdalnego dostępu.

## Niższy całkowity koszt użytkowania

Oprócz szeregu korzyści dla bezpieczeństwa przedsiębiorstwa modele SA2500, SA4500 oraz SA6500 posiadają szereg właściwości, które redukują całkowity koszt ich użytkowania.

Tabela 2: Koszt użytkowania, właściwości i zalety

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Wykorzystuje SSL	Bezpieczne połączenie pomiędzy użytkownikiem zdalnym a wewnętrznym źródłem danych poprzez połączenie Web na poziomie aplikacji.	Bezpieczny dostęp zdalny bez potrzeby wprowadzania oprogramowania klienckiego, bez dodatkowych kosztów związanych z utrzymaniem oraz bez potrzeby wprowadzania zmian w istniejących serwerach. Brak problemów związanych z firewall, proxy czy NAT.
Bazuje na protokołach i metodach zabezpieczających opartych o standardy przemysłowe	Brak potrzeby dodatkowej instalacji wymaganych protokołów standardowych.	Korzyści z inwestycji w urządzenia SA można czerpać w wielu zastosowaniach i zasobach przez długi okres czasu.
Rozległa integracja i współpraca z usługami katalogowymi	Istniejące w sieci usługi katalogowe mogą być dalej wykorzystywane w celu uwierzytelnienia i autoryzacji zapewniając bezpieczeństwo dostępu bez konieczności odtwarzania tych struktur.	Istniejące usługi katalogowe mogą być nadal wykorzystywane bez konieczności zmian infrastruktury; dodatkowy API nie jest wymagany dla integracji z usługami katalogowymi.
Integracja z systemami silnego uwierzytelnienia oraz zarządzania tożsamością i dostępem	Wsparcie dla SecurID, Security Assertion Markup Language (SAML), infrastruktury klucza publicznego (PKI)/certyfikatów cyfrowych.	Wykorzystuje istniejące korporacyjne metody uwierzytelniania w celu uproszczenia zarządzania.
Obsługa wielu nazw hosta	Możliwość instalowania różnych wirtualnych witryn WWW za pomocą pojedynczego urządzenia serii SA SSL VPN.	Niweluje koszt utrzymania dodatkowych serwerów oraz ułatwia zarządzanie. Użytkownik wprowadzając różne URL uzyskuje wrażenie jakby odwoływał się do różnych serwerów.
Interfejs użytkownika dostosowany do indywidualnych potrzeb	Tworzenie stron logowania w pełni dostosowanych do indywidualnych potrzeb.	Pozwala na indywidualne podejście do określonych ról usprawniając użytkowanie.
Juniper Networks Network and Security Manager (NSM)	Intuicyjny webowy interfejs użytkownika pozwalający na konfigurowanie, aktualizację i monitorowanie urządzeń SA w obrębie pojedynczego urządzenia/klastra lub w globalnym rozmieszczeniu klastrów.	Pozwala firmom wygodnie zarządzać, konfigurować i monitorować urządzenia SA z jednej, centralnej lokalizacji.
W razie nagłego niebezpieczeństwa (In Case of Emergency – ICE)	Pozwala na udzielenie licencji na ograniczony okres czasu większej liczbie dodatkowych użytkowników urządzenia SA SSL VPN w razie katastrofy lub epidemii.	Pozwala przedsiębiorstwu na dalsze prowadzenie swojej działalności poprzez podtrzymanie produktywności, utrzymanie kontaktów biznesowych i kontynuację dostarczania usług swoim klientom w wypadku zaistnienia zdarzeń losowych.
Obsługa wielu platform	Możliwość uzyskania dostępu do zasobów przy użyciu różnych platform (np. Windows, Mac, Linux, urządzenia mobilne).	Zapewnia elastyczność, pozwalając użytkownikom na uzyskanie dostępu do zasobów przedsiębiorstwa za pomocą urządzenia i systemu operacyjnego każdego typu.

## Bogate możliwości zarządzania prawami dostępu

Modele SA2500, SA4500 oraz SA6500 pozwalają na dynamiczne zarządzanie prawami dostępu bez wprowadzania zmian w infrastrukturze, opracowywania nowych rozwiązań, wprowadzania i obsługiwanego dodatkowego oprogramowania. Umożliwia to instalację i utrzymanie mechanizmów bezpiecznego dostępu, jak również zabezpieczenie sieci ekstranet i intranet. Kiedy użytkownik loguje się do urządzenia serii SA SSL VPN, musi przejść przez proces wstępnego uwierzytelnienia, a następnie w sposób dynamiczny przydzielony zostaje do określonej roli sesji, w skład której wchodzi ustawienia sieci, urządzenia, tożsamości oraz reguły sesji. Szczegółowe polityki autoryzacji dostępu do zasobów dodatkowo zapewniają dokładne przestrzeganie wymogów bezpieczeństwa.

**Tabela 3: Zarządzanie prawami dostępu, właściwościami i zalety**

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Hybrydowy model polityk oparty o role i zasoby	Administratorzy mogą dostosowywać polityki dostępu użytkowników.	Gwarantuje, że polityka bezpieczeństwa dostosowana jest do zmieniających się wymogów biznesowych.
Wstępne uwierzytelnianie	Atrybuty sieci oraz urządzenia, takie jak kontroler hosta/mechanizm czyszczenia pamięci podręcznej, wyniki skanowania bezpieczeństwa punktu końcowego, źródłowy adres IP, typ przeglądarki oraz certyfikaty cyfrowe mogą być poddane analizie zanim wydane zostanie zezwolenie na zalogowanie.	Wyniki są podstawą dla dynamicznie podejmowanych decyzji wymuszających przyjęcie obowiązującej polityki bezpieczeństwa.
Polityka dynamicznego uwierzytelniania	Pozwala administratorom na ustanowienie dynamicznej strategii uwierzytelniania dla każdej unikatowej sesji.	Wykorzystuje istniejące usługi katalogowe przedsiębiorstwa, PKI oraz silne uwierzytelnianie.
Dynamiczne mapowanie ról	Kombinacja atrybutów sieci, urządzenia oraz sesji pozwalająca na ustalenie, który z trzech różnych typów dostępu ma być udzielony.	Pozwala administratorom dostosowywać konfigurację dla poszczególnych, unikatowych sesji.
Autoryzacja zasobów	Niezwykle szczegółowa kontrola na poziomie URL, serwera lub plików.	Pozwala administratorom na dostosowanie polityki bezpieczeństwa do poszczególnych grup użytkowników, udostępniając jedynie kluczowe dane.
Szczegółowy audyt i gromadzenie logów	Funkcja ta może zostać skonfigurowana tak, by działać na poziomie użytkownika, zasobów lub zdarzeń w celu weryfikacji bezpieczeństwa lub planowania wydajności.	Zapewnia szczegółowe audytowanie i gromadzenie logów o jasnym i łatwym do zrozumienia formacie.
Wyrażenia definiowane przez użytkownika	Umożliwia stosowanie dynamicznych kombinacji atrybutów dla poszczególnych sesji na poziomie definiowania/mapowania reguł oraz polityki autoryzacji zasobów.	Zapewnia większą szczegółowość i możliwość dostosowania roli polityki.

## Samoobsługa użytkownika

Właściwości modeli SA2500, SA4500 oraz SA6500 pozwalają na kompleksowe zarządzanie hasłami. Właściwości te zwiększają produktywność użytkownika końcowego, znacznie upraszczają zarządzanie dużymi i zróżnicowanymi zasobami użytkownika, jak również zdecydowanie redukują liczbę telefonów do centrum obsługi technicznej.

**Tabela 4: Samoobsługa użytkownika, właściwości i zalety**

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Ograniczone delegowanie	Kiedy użytkownik loguje się do serii SA przy użyciu danych logowania, które nie mogą być przekazane do serwera końcowego, urządzenie serii SA wyszuka w imieniu użytkownika bilet Kerberos w infrastrukturze Active Directory. Bilet będzie zachowany w pamięci podręcznej urządzenia w czasie trwania sesji. Kiedy użytkownik będzie usiłował wejść do aplikacji zabezpieczonej przez protokół Kerberos, seria SA użyje danych logowania użytkownika zapisanych w pamięci podręcznej, aby zalogować tego użytkownika do aplikacji bez konieczności podawania przez niego hasła.	Eliminuje konieczność zarządzania przez firmy statycznymi hasłami dostępu, co redukuje czas i koszty administrowania systemem.
Zaawansowane udoskonalenia SSO – wsparcie Kerberos SSO i NTLMv2	Seria SA będzie automatycznie autoryzować zdalnych użytkowników poprzez protokół Kerberos lub NTLMv2, na podstawie danych logowania użytkownika.	Upraszcza obsługę użytkownikom, eliminując potrzebę każdorazowego wprowadzania przez nich danych logowania przy wchodzeniu do różnych aplikacji.
Zintegrowane zarządzanie hasłami	Oparty o standardy interfejs pozwalający na szeroką integrację z politykami dotyczącymi zarządzania hasłami w usługach katalogowych (LDAP, Microsoft Active Directory, NT i inne).	Wykorzystuje istniejące serwery do uwierzytelniania użytkowników; użytkownicy mogą zarządzać swoimi hasłami bezpośrednio poprzez interfejs serii SA.
Webowe pojedyncze logowanie (SSO) i NT LAN Manager (NTLM)	Pozwala użytkownikom na uzyskanie dostępu do innych aplikacji lub zasobów, które chronione są przez odmienne systemy zarządzające dostępem bez potrzeby ponownego wprowadzania danych identyfikacyjnych.	Eliminuje potrzebę wprowadzania i przetrzymywania przez użytkowników końcowych osobnych zestawów danych logowania dla aplikacji webowych oraz Microsoftu.
Webowe pojedyncze logowanie (SSO) bazujące na formularzach, zmiennych nagłówka, SAML	Możliwość wprowadzania nazwy użytkownika, danych uwierzytelniania lub innych atrybutów zdefiniowanych przez użytkownika do formularzy uwierzytelniających innych produktów lub jako zmiennych nagłówka.	Zwiększa produktywność użytkownika i poprawia komfort pracy.

## Wybór dostępu w zależności od zadań

Modele SA2500, SA4500 oraz SA6500 zapewniają trzy różne metody dostępu. Wybór danej metody jest jednym z zadań użytkownika, administrator może uaktywnić odpowiednią metodę dostępu dla poszczególnych sesji, biorąc pod uwagę atrybuty użytkownika, urządzenia oraz sieci w połączeniu z regułami bezpieczeństwa przedsiębiorstwa.

Tabela 5: Wybór dostępu w zależności od zadań, właściwości i zalety

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Dostęp webowy nie wymagający instalacji oprogramowania po stronie klienta	Dostęp do aplikacji webowych, takich jak złożone JavaScript, XML lub aplikacje Flash oraz aplety Java, które wymagają połączenia sieciowego, jak również do standardowych aplikacji e-mail, takich jak Outlook Web Access (OWA), współdzielonych plików Windows i UNIX, aplikacji dla usług telnet/SSH, usług terminalowych, emulacji terminali i innych.	Zapewnia najprostszą formę dostępu do aplikacji oraz zasobów z różnorodnych urządzeń końcowych, łącznie z urządzeniami mobilnymi, jak również umożliwia niezwykle szczegółową kontrolę zabezpieczeń. Metoda ta całkowicie eliminuje potrzebę istnienia oprogramowania klienta wykorzystując jedynie przeglądarkę WWW.
Secure Application Manager (SAM)	Pobranie niewielkiego kodu Javy lub aplikacji umożliwia uzyskanie dostępu do aplikacji klient/serwer.	Umożliwia uzyskanie dostępu do aplikacji klient/serwer używając jedynie przeglądarki WWW; zapewnia również dostęp do aplikacji natywnych na serwerze terminalowym bez konieczności uprzedniego instalowania klienta.
Network Connect (NC)	Zapewnia kompletne połączenie sieciowe pomiędzy wieloma platformami; integracja Windows Logon/Gina z pojedynczym logowaniem (SSO) do domeny; usługi instalacyjne zmniejszające potrzebę posiadania praw administratorских. Daje możliwość rozdzielnego tunelowania.	Użytkownicy potrzebują jedynie przeglądarki WWW; Network Connect dokonuje klarownej selekcji pomiędzy dwiema możliwymi metodami transportu, aby automatycznie zapewnić najwyższą możliwą wydajność dla każdego środowiska sieciowego; używany razem z Juniper Installer Services nie wymaga praw administratorских, aby zainstalować, obsługiwać i aktualizować Network Connect; dostępna jest również opcjonalna, osobna instalacja. Możliwość rozdzielnego tunelowania daje dowolność w określaniu, które hosty czy podsieci włączyć lub wykluczyć z tunelowania.

## Opcje produktu

Urządzenia SA2500, SA4500 oraz SA6500 występują w różnych opcjach licencyjnych dla zapewnienia jeszcze większej funkcjonalności.

### Licencja użytkownika

Wraz z pojawieniem się modeli SA2500, SA4500 oraz SA6500, zakup urządzeń został uproszczony dzięki połączeniu właściwości, które niegdyś były dostępne wyłącznie jako osobne aktualizacje. Obecnie aby rozpocząć użytkowanie, potrzebna jest tylko jedna licencja: licencja użytkownika. Również obecni użytkownicy starszej generacji urządzeń (SA2000, SA4000 i SA6000) skorzystają z tych zmian po aktualizacji ich systemów do nowszej wersji oprogramowania (6.1 lub wyższej).

Licencje użytkownika zapewniają funkcjonalność, która umożliwia użytkownikom zdalnym, ekstranetowym i intranetowym dostęp do sieci. W pełni spełniają potrzeby zarówno podstawowych jak i kompleksowych wdrożeń z różnorodnymi odbiorcami i sposobami wykorzystania. Wymagają niewielkiej ilości oprogramowania po stronie klienta, zmian serwera, modyfikacji DMZ czy wdrożeń agentów programowych lub nie wymagają ich wcale. Dla łatwego zarządzania ilością licencji użytkownika, każda licencja dopuszcza tylu użytkowników, ilu było określonych w licencji z możliwością dodania kolejnych. Na przykład, jeśli oryginalnie zakupiono licencje na 100 użytkowników, ale liczba użytkowników w ciągu ostatniego roku wzrosła i wyczerpała pulę z licencji, wystarczy dokupić licencje na kolejnych 100 użytkowników i wówczas system umożliwi obsługę do 200 użytkowników jednocześnie. Kluczowe właściwości zawarte w ramach tej licencji to:

- Secure Application Manager (SAM) oraz Network Connect (NC) zapewniają funkcjonujące na różnych platformach wsparcie aplikacji klient/serwer dzięki użyciu SAM, jak również pełnego dostępu do wszystkich warstw sieci dzięki użyciu dwóch adaptacyjnych metod transportu, które znaleźć można w NC. Połączenie SAM i NC z dostępem webowym zapewni bezpieczny dostęp dla praktycznie

wszystkich użytkowników i klientów, od zdalnie pracujących/ mobilnych pracowników po partnerów i klientów korzystających z różnorodnych urządzeń, w jakiegokolwiek sieci.

- Wybór dostępu w zależności od zadań wykracza poza bazującą na rolach kontrolę dostępu i pozwala administratorom właściwie, dokładnie i dynamicznie zbalansować wymagania bezpieczeństwa z wymaganiami dostępu,
- Zaawansowane wsparcie dla PKI to możliwość importowania wielu głównych i pośrednich CA, weryfikacji wielu certyfikatów serwerów z wykorzystaniem protokołu Online Certificate Status Protocol (OCSP),
- Usługa samoobsługi użytkownika daje użytkownikom możliwość tworzenie własnych, ulubionych zakładek, w tym dostęp do ich własnych stacji roboczych ze zdalnej lokalizacji, a nawet zmianę swojego hasła kiedy już wygaśnie,
- Wsparcie dla wielu nazw hostów (na przykład, <https://employees.company.com>, <https://partners.company.com> i <https://employees.company.com/engineering>). Te wszystkie strony są widoczne jako jedyne, z osobnymi stronami logowania i z dostosowanym wyglądem tak, aby trafiać w potrzeby i wymagania odbiorców,
- Interfejs użytkownika dostosowany do potrzeb użytkownika i delegowanych ról administracyjnych,
- Zaawansowana kontrola stacji końcowych przy pomocy narzędzi takich jak: Host Checker, Cache Cleaner i Secure Virtual Workspace pilnuje, aby użytkownicy w sposób dynamiczny uzyskiwali dostęp do systemów i zasobów, ale tylko w stopniu, na jaki pozwala polityka bezpieczeństwa organizacji. Dane pozostałe po realizacji usługi są usuwane z dysków tak, aby nie pozostał żaden ślad,
- Wsparcie dla VLAN (do 240 sieci VLAN).

## Licencja na zabezpieczenie spotkań Secure Meeting (opcjonalnie)

Licencja na aktywowanie Juniper Networks Secure Meeting rozszerza możliwości urządzeń serii SA SSL VPN niskim kosztem, umożliwiając w każdym czasie i miejscu skuteczną ochronę konferencji webowych oraz zdalną kontrolę dostępu do PC. Secure Meeting umożliwia współdzielenie aplikacji w czasie rzeczywistym, co pozwala autoryzowanym pracownikom i partnerom w prosty sposób wyznaczać spotkania online lub aktywować spotkania w danej chwili dzięki intuicyjnemu interfejsowi webowemu, którego obsługa nie wymaga przeprowadzania dodatkowych szkoleń lub wdrożeń. Personel obsługi klienta może służyć pomocą każdemu użytkownikowi lub klientowi zdalnie kontrolując jego PC bez wymogu instalowania przez użytkownika jakiegokolwiek dodatkowego oprogramowania. Najlepsze w swojej klasie możliwości protokołu AAA umożliwiają przedsiębiorstwom w prosty sposób zintegrować Secure Meeting z wykorzystywaną już przez nie wewnętrzną infrastrukturą uwierzytelniającą. Przewodząca na rynku, zoptymalizowana i posiadająca certyfikaty Common Criteria architektura urządzenia SSL VPN Junipera oraz zabezpieczenia transferu danych SSL/HTTPS dla wszystkich typów ruchu sieciowego, gwarantuje zgodność tego rozwiązania z najsurowszymi wymogami bezpieczeństwa przedsiębiorstwa.

Opcja Secure Meeting dostępna jest dla modeli SA2500, SA4500 oraz SA6500.

## Licencja Instant Virtual System (opcjonalnie)

Opcja Juniper Networks Instant Virtual System (IVS) opracowana została, aby umożliwić administratorom obsługę 240 logicznie niezależnych bram SSL VPN w obrębie jednego urządzenia/klastra. Pozwala to dostawcom usług na dostarczanie wielu klientom usług sieciowych zarządzanych przez SSL VPN z jednego urządzenia lub klastra, jak również umożliwia przedsiębiorstwom na całkowite segmentowanie ruchu w sieci SSL VPN pomiędzy wieloma grupami użytkowników. IVS umożliwia całkowite odseparowanie klientów i zapewnia segregację ruchu w sieci pomiędzy wieloma klientami, korzystając ze szczegółowego, bazującego na rolach tagowania VLAN (802.1Q). Pozwala to na bezpieczne segregowanie użytkowników końcowych, nawet w przypadku gdy dwoje klientów posiada ten sam adres IP i umożliwia dostosowanie konkretnego VLAN do różnych użytkowników, takich jak pracownicy zdalni lub partnerzy klientów.

Domain Name Service (DNS)/Windows Internet Name Service (WINS), AAA, serwery log/accounting oraz serwery aplikacji, takie jak poczta Web, współdzielone pliki, itp. mogą być przechowywane w sieciach intranet klienta lub w sieci usługodawcy. Usługodawcy mogą dostosować ogólną liczbę jednocześnie pracujących użytkowników dla poszczególnego klienta z możliwością rozszerzenia o kolejnych użytkowników, takich jak pracownicy zdalni przedsiębiorstwa, kontrahenci, partnerzy i inni. Seria SA rozszerza wsparcie programowe konfiguracji i zarządzania IVS. Umożliwia to usługodawcom zintegrowanie zarządzania IVS z ich własnymi systemami wsparcia operacyjnego (OSS). Pozwala to również przedsiębiorstwom korzystającym z IVS na zastosowanie możliwości importowania i/lub eksportowania XML w zarządzaniu indywidualnymi systemami wirtualnymi.

Opcja IVS dostępna jest dla modeli SA4500 i SA6500.

## Opcja wysokiej dostępności (HA)

Juniper Networks opracował różnorodne opcje klastrowania HA dla urządzeń serii SA, zapewniając nadmiarowość i płynne funkcjonowanie systemu w rzadkich przypadkach awarii. Te opcje klastrowania umożliwiają również skalowalność wydajności w celu spełnienia wymogów najbardziej wymagających środowisk. Modele SA2500

i SA4500 mogą zostać zakupione w postaci klastrów złożonych z dwóch jednostek, a model SA6500 w postaci klastrów złożonych z dwóch lub wielu jednostek, co zapewnia całkowitą nadmiarowość oraz szeroką skalowalność użytkowania.

Zarówno klastry złożone z wielu jednostek jak i klastry złożone z dwóch jednostek pozwalają na monitorowanie stanów i płynne funkcjonowanie całej sieci LAN i WAN w razie mało prawdopodobnej awarii jednej z jednostek. Wówczas konfiguracje systemu (takie jak konfiguracja serwera uwierzytelniającego, grup autoryzacji, zakładek, itp.), ustawienia profilu użytkownika (np. zdefiniowanie przez użytkownika zakładek, pliki cookie, itp.) oraz sesje użytkowników zostaną zachowane. Przejęcie pracy przez drugą jednostkę jest płynne, co pozwala uniknąć przerw w pracy użytkownika/przedsiębiorstwa, bez potrzeby ponownego logowania się użytkowników oraz przestoju. Klastry złożone z wielu jednostek działają w automatycznym trybie Aktywny-Aktywny, podczas gdy klastry złożone z dwóch jednostek mogą być przestawiane pomiędzy trybami Aktywny-Aktywny i Aktywny-Pasywny.

Licencje wysokiej dostępności pozwalają na współdzielenie licencji pomiędzy dwoma lub większą ilością urządzeń serii SA (w zależności od platformy) bez możliwości łączenia ilości obsługiwanych użytkowników. Na przykład, jeżeli klient posiada licencje na 100 użytkowników dla SA4500 a następnie zakupi kolejny SA4500 z licencją klastrową na 100 użytkowników, to sumarycznie będzie miał możliwość współdzielenia pomiędzy tymi urządzeniami obsługi 100 użytkowników.

Opcja HA dostępna jest dla modeli SA2500, SA4500 oraz SA6500.

## Licencja ICE (opcjonalnie)

SSL VPN może pomóc w funkcjonowaniu przedsiębiorstwa utrzymując połączenia nawet w przypadku zaistnienia najmniej spodziewanych zdarzeń losowych, takich jak huragany, ataki terrorystyczne, strajki pracowników służb transportowych, pandemii lub epidemii, czyli zdarzeń, które wiążą się z izolacją całych regionów lub skupisk ludzkich na dłuższy okres czasu. Wraz z odpowiednim zbalansowaniem ryzyka i kosztów, opcja ICE dla urządzeń Juniper Networks serii SA zapewnia rozwiązanie mogące sprostać dramatycznej potrzebie uzyskania zdalnego dostępu, które zapewniłoby kontynuowanie działalności przedsiębiorstwa w razie katastrofalnych w skutkach zdarzeń losowych. ICE pozwala na udzielenie licencji dla większej ilości dodatkowych użytkowników pracujących na pojedynczych urządzeniach serii SA SSL VPN na ograniczony okres czasu.

Dzięki ICE przedsiębiorstwa mogą:

- Podtrzymać wydajność zapewniając pracownikom ogólny dostęp do aplikacji i danych z dowolnego miejsca, o dowolnym czasie i za pomocą dowolnego urządzenia,
- Podtrzymać kontakty biznesowe dzięki całodobowemu dostępowi do aplikacji i usług w czasie rzeczywistym, jednocześnie zapewniając bezpieczeństwo i ochronę zasobów,
- Kontynuować dostarczanie usług najwyższej jakości klientom oraz partnerom, z którymi utrzymywana jest współpraca online,
- Zachować zgodność z federalnymi i rządowymi normami prawnymi COOP (Continuity of Operations),
- Zbalansować ryzyko i skalowalność niskimi kosztami i prostotą wdrożenia,
- Licencja ICE dostępna jest dla modeli SA4500 oraz SA6500 i zawiera następujące właściwości:
  - Zestaw podstawowy (Baseline),
  - Secure Meeting.



## Specyfikacja techniczna

	SA2500	SA4500	SA6500
<b>Wymiary i zasilanie</b>			
Wymiary (Szerokość × Wysokość × Głębokość)	43.8 × 4.4 × 36.8 cm (17.26 × 1.75 × 14.5 in)	43.8 × 4.4 × 36.8 cm (17.26 × 1.75 × 14.5 in)	43.8 × 8.8 × 45 cm (17.26 × 3.5 × 17.72 in)
Waga	6.6 kg (14.6 lb) bez opakowania	7.1 kg (15.6 lb) bez opakowania	12 kg (26.4 lb) bez opakowania
Opcja do montażu w racku	Tak, 1U	Tak, 1U	Tak, 2U, 19 cali
Zasilanie prądem zmiennym (A/C)	100-240 VAC, 50-60 Hz, 2.5 A Maks. 200 W	100-240 VAC, 50-60 Hz, 2.5 A Maks. 300 W	100-240 VAC, 50-60 Hz, 2.5 A Maks. 400 W
Bateria	Bateria litowa CR2032 3 V	Bateria litowa CR2032 3 V	Bateria litowa CR2032 3 V
Wydajność	Min. 80% przy pełnym obciążeniu	Min. 80% przy pełnym obciążeniu	Min. 80% przy pełnym obciążeniu
Materiał	Stal walcowana na zimno, grubość 18 (.048)	Stal walcowana na zimno, grubość 18 (.048)	Stal walcowana na zimno, grubość 18 (.048)
MTBF	75 000 godzin	72 000 godzin	98 000 godzin
Wentylatory	Trzy wiatraki na łożyskach kulkowych 40 mm, jeden wentylator jednostki zasilania na łożysku kulkowym 40 mm	Trzy wiatraki na łożyskach kulkowych 40 mm, jeden wentylator jednostki zasilania na łożysku kulkowym 40 mm	Dwa wiatraki na łożyskach kulkowych 80 mm Hot Swap, jeden wentylator jednostki zasilania na łożysku kulkowym 40 mm
<b>Panel przedni</b>			
Dioda LED zasilania, aktywności dysku twardego, sygnalizacja HW	Tak	Tak	Tak
Dioda LED aktywności dysku twardego i błędu kieszeni HD	Nie	Nie	Tak
<b>Porty</b>			
Ruch sieciowy	Dwa porty RJ-45 Ethernet 10/100/1000, full or half duplex (autonegocjacja)	Dwa porty RJ-45 Ethernet 10/100/1000, full or half duplex (autonegocjacja)	Cztery porty RJ-45 Ethernet, full or half duplex, Opcjonalnie moduł SFP
Zarządzanie	Brak	Brak	Jeden RJ-45 Ethernet 10/100/1000 full or half duplex (z autonegocjacją)
Fast Ethernet	Zgodny z IEEE 802.3u	Zgodny z IEEE 802.3u	Zgodny z IEEE 802.3u
Gigabit Ethernet	Zgodny z IEEE 802.3z lub IEEE 802.3ab	Zgodny z IEEE 802.3z lub IEEE 802.3ab	Zgodny z IEEE 802.3z lub IEEE 802.3ab
Konsola	Jeden szeregowy port RJ45	Jeden szeregowy port RJ45	Jeden szeregowy port RJ45

## Specyfikacja techniczna (ciąg dalszy)

	SA2500	SA4500	SA6500
<b>Parametry środowiskowe</b>			
Temperatura w trakcie pracy	5° to 40° C (41° to 104° F)	5° to 40° C (41° to 104° F)	5° to 40° C (41° to 104° F)
Temperatura przechowywania	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)
Względna wilgotność (w trakcie pracy)	8% do 90% bez kondensacji	8% do 90% bez kondensacji	8% do 90% bez kondensacji
Względna wilgotność (przechowywanie)	5% do 95% bez kondensacji	5% do 95% bez kondensacji	5% do 95% bez kondensacji
Wysokość n.p.m. (w trakcie pracy)	Maksymalnie 3000 m (10000 ft)	Maksymalnie 3000 m (10000 ft)	Maksymalnie 3000 m (10000 ft)
Wysokość n.p.m. (przechowywanie)	Maksymalnie 12192 m (40000 ft)	Maksymalnie 12192 m (40000 ft)	Maksymalnie 12192 m (40000 ft)
<b>Certyfikacje</b>			
Certyfikaty bezpieczeństwa	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 Nr. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 Nr. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 Nr. 60950-1-03, IEC 60950-1:2001
Certyfikaty emisji	FCC Klasa A, EN 55022 Klasa A, EN 55024 odporność, EN 61000-3-2, VCCI Klasa A	FCC Klasa A, EN 55022 Klasa A, EN 55024 odporność, EN 61000-3-2, VCCI Klasa A	FCC Klasa A, EN 55022 Klasa A, EN 55024 odporność, EN 61000-3-2, VCCI Klasa A
Gwarancja	90 dni; może zostać przedłużona w ramach dodatkowej umowy	90 dni; może zostać przedłużona w ramach dodatkowej umowy	90 dni; może zostać przedłużona w ramach dodatkowej umowy

## Usługi optymalizacji wydajności i wsparcie

Juniper Networks jest liderem w dziedzinie usług zwiększania wydajności i wsparcia z nimi związanego. Usługi te są zaprojektowane specjalnie, aby przyspieszać, rozszerzać i optymalizować działanie wysokowydajnej sieci. Nasze produkty zapewniają generujące zyski możliwości, co ułatwia wprowadzanie na rynek nowych modeli biznesowych i przedsięwzięć, a także poszerza zasięg rynku, podczas gdy poziom zadowolenia klienta stale wzrasta. Jednocześnie Juniper Networks gwarantuje doskonałą sprawność działania dzięki optymalizacji sieci w taki sposób, by utrzymywała wymagane poziomy wydajności, niezawodności i dostępności. Bardziej szczegółowe informacje dostępne są na stronie [www.juniper.net/products-services](http://www.juniper.net/products-services).

## Informacje dotyczące zamówień

NUMER MODELU	OPIS
<b>SA2500</b>	
System bazowy SA2500	System bazowy SA2500
Licencje użytkownika	
SA2500-ADD-10U	Dodaje 10 jednocześnie pracujących użytkowników dla modelu SA2500
SA2500-ADD-25U	Dodaje 25 jednocześnie pracujących użytkowników dla modelu SA2500
SA2500-ADD-50U	Dodaje 50 jednocześnie pracujących użytkowników dla modelu SA2500
SA2500-ADD-100U	Dodaje 100 jednocześnie pracujących użytkowników dla modelu SA2500
Licencje opcji dodatkowych	
SA2500-MTG	Zabezpieczenie spotkań Secure Meeting dla SA2500
Licencje klastrowania	
SA2500-CL-10U	Klastrowanie: Pozwala na dzielenie dodatkowych 10 użytkowników z kolejnego urządzenia SA2500
SA2500-CL-25U	Klastrowanie: Pozwala na dzielenie dodatkowych 25 użytkowników z kolejnego urządzenia SA2500
SA2500-CL-50U	Klastrowanie: Pozwala na dzielenie dodatkowych 50 użytkowników z kolejnego urządzenia SA2500
SA2500-CL-100U	Klastrowanie: Pozwala na dzielenie dodatkowych 100 użytkowników z kolejnego urządzenia SA2500
<b>SA4500</b>	
System bazowy SA4500	System bazowy SA4500
Licencje użytkownika	
SA4500-ADD-50U	Dodaje 50 jednocześnie pracujących użytkowników dla modelu SA4500
SA4500-ADD-100U	Dodaje 100 jednocześnie pracujących użytkowników dla modelu SA4500
SA4500-ADD-250U	Dodaje 250 jednocześnie pracujących użytkowników dla modelu SA4500
SA4500-ADD-500U	Dodaje 500 jednocześnie pracujących użytkowników dla modelu SA4500
SA4500-ADD-1000U	Dodaje 1000 jednocześnie pracujących użytkowników dla modelu SA4500
Licencje opcji dodatkowych	
SA4500-MTG	Secure Meeting dla SA4500
SA4500-IVS	Instant Virtual System dla SA4500
SA4500-ICE	Licencja ICE dla SA4500
SA4500-ICE-CL	Licencja klastrowania ICE License dla SA4500
Licencje klastrowania	
SA4500-CL-50U	Klastrowanie: Pozwala na dzielenie dodatkowych 50 użytkowników z kolejnego urządzenia SA4500
SA4500-CL-100U	Klastrowanie: Pozwala na dzielenie dodatkowych 100 użytkowników z kolejnego urządzenia SA4500
SA4500-CL-250U	Klastrowanie: Pozwala na dzielenie dodatkowych 250 użytkowników z kolejnego urządzenia SA4500
SA4500-CL-500U	Klastrowanie: Pozwala na dzielenie dodatkowych 500 użytkowników z kolejnego urządzenia SA4500

NUMER MODELU	OPIS
<b>SA6500</b>	
System bazowy SA6500	System bazowy SA6500
Licencje użytkownika	
SA6500-ADD-100U	Dodaje 100 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-250U	Dodaje 250 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-500U	Dodaje 500 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-1000U	Dodaje 1000 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-2500U	Dodaje 2500 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-5000U	Dodaje 5000 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-7500U	Dodaje 7500 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-10000U	Dodaje 10000 jednocześnie pracujących użytkowników dla modelu SA6500
SA6500-ADD-12500U*	Dodaje 10000 jednocześnie pracujących użytkowników dla modelu SA6500S
A6500-ADD-15000U*	Dodaje 15000 jednocześnie pracujących użytkowników dla modelu SA6500
A6500-ADD-20000U*	Dodaje 20000 jednocześnie pracujących użytkowników dla modelu SA6500
A6500-ADD-25000U*	Dodaje 25000 jednocześnie pracujących użytkowników dla modelu SA6500
Licencje opcji dodatkowych	
SA6500-MTG	Secure Meeting dla SA6500
SA6500-IVS	Instant Virtual System dla SA6500
SA6500-ICE	Licencja ICE dla SA6500
SA6500-ICE-CL	Licencja klastrowania ICE dla SA6500
Licencje klastrowania	
SA6500-CL-100U	Klastrowanie: Pozwala na dzielenie dodatkowych 100 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-250U	Klastrowanie: Pozwala na dzielenie dodatkowych 250 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-500U	Klastrowanie: Pozwala na dzielenie dodatkowych 500 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-1000U	Klastrowanie: Pozwala na dzielenie dodatkowych 1000 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-2500U	Klastrowanie: Pozwala na dzielenie dodatkowych 2500 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-5000U	Klastrowanie: Pozwala na dzielenie dodatkowych 5000 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-7500U	Klastrowanie: Pozwala na dzielenie dodatkowych 7500 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-10000U	Klastrowanie: Pozwala na dzielenie dodatkowych 10000 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-12500U	Klastrowanie: Pozwala na dzielenie dodatkowych 12500 użytkowników z kolejnego urządzenia SA6500

SA6500-CL-15000U	Klastrowanie: Pozwala na dzielenie dodatkowych 15000 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-20000U	Klastrowanie: Pozwala na dzielenie dodatkowych 20000 użytkowników z kolejnego urządzenia SA6500
SA6500-CL-25000U	Klastrowanie: Pozwala na dzielenie dodatkowych 25000 użytkowników z kolejnego urządzenia SA6500

#### Akcesoria

UNIV-CRYPTO	Moduł akceleratora SSL dla SA 4500
UNIV-PS-400W-AC	Zapasy zasilacz 400W dla SA6500
UNIV-80G-HDD	Zamienny dysk twardy 80GB dla SA6500
UNIV-MR2U-FAN	Zapasy wentylator do urządzenia SA6500
UNIV-MR1U-RAILKIT	Zestaw do montażu w racku urządzeń SA2500 i SA4500
UNIV-MR2U-RAILKIT	Zestaw do montażu w racku urządzenia SA6500
UNIV-SFP-FSX	Transceiver mini-GBIC światłowodowy SX dla SA6500
UNIV-SFP-FLX	Transceiver mini-GBIC światłowodowy LX dla SA 6500
UNIV-SFP-COP	Transceiver mini-GBIC miedziany dla SA6500
SA6500-IOC	Karta GBIC I/O

\*Wymaga dodatkowych urządzeń SA6500

## O Juniper Networks

Juniper Networks, Inc. jest liderem w dziedzinie wysokowydajnych rozwiązań sieciowych. Juniper zapewnia wysoce wydajną infrastrukturę sieciową, która stwarza elastyczne i godne zaufania środowisko, aby przyspieszać wdrażanie usług i aplikacji do pojedynczej sieci. Służy to napędzaniu przedsięwzięć o dużym potencjale rozwoju. Więcej informacji znaleźć można na stronie [www.juniper.net](http://www.juniper.net)

## Dystrybucja w Polsce:



CLICO Sp. z o.o.  
Budynek CC Oleandry  
30-063 Kraków, ul. Oleandry 2  
tel. 012 378-37-00  
tel. 012 632-51-66  
tel. 012 292-75-22 ... 24  
fax 012 632-36-98  
e-mail: sales@clico.pl  
www.clico.pl

CLICO Oddział Katowice  
40-568 Katowice, ul. Ligocka 103  
tel. 032 444-65-11  
tel. 032 203-92-35  
tel. 32 609-80-50...51  
fax 032 203-97-93  
e-mail: katowice@clico.pl

CLICO Oddział Warszawa  
Budynek Centrum Milenium  
03-738 Warszawa, ul. Kijowska 1  
tel. 022 201-06-88  
tel. 022 518-02-70...75  
fax 022 518-02-73  
e-mail: warszawa@clico.pl

© 2009 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.