



Juniper Networks Secure Access 2500, 4500 i 6500

Opis produktu

Juniper Networks przedstawia nową generację swoich wiodących na rynku urządzeń Secure Access SSL VPN. Nowe SA 2500, SA 4500 i SA 6500 są urządzeniami SSL VPN, które spełniają wymagania firm każdego rozmiaru. Urządzeniem SA 6500, Juniper potwierdza swoją dominację na rynku, dostarczając wysoko skalowalne rozwiązanie bazujące na rzeczywistych testach wydajnościowych. Urządzenia Secure Access 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 Secure Access SSL VPN 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 oraz kluczowe komponenty

Model Juniper Networks SA 2500 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 SA 2500 oferuje wysoką dostępność (HA) oraz płynne przełączanie sesji użytkowników w razie pojawienia się usterki. Ponieważ SA 2500 używa dokładnie tego samego oprogramowania co większe SA 4500 i SA 6500, nawet mniejsze organizacje uzyskają tę samą wysoką wydajność, administracyjną elastyczność i wygodę użytkownika.

Dzięki modelowi Juniper Networks SA 4500 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 SA 4500 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 aktualnie są im 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 przełączaniem sesji użytkowników w razie pojawienia się usterki.

Model Juniper Networks SA 6500 przeznaczony jest dla dużych przedsiębiorstw i dostawców usług. Jego cechy to najlepsza wydajność w tej klasie produktów, skalowalność oraz nadmiarowość, dzięki czemu sprawdza się w organizacjach mających większe wymagania odnośnie bezpiecznego dostępu oraz autoryzacji. Ponadto model SA 6500 oferuje wysoką dostępność (HA) oraz zapewnia przełączanie sesji użytkowników w razie pojawienia się usterki. SA 6500 posiada również wbudowaną kompresję dla Web i plików, oraz najwyższej klasy chipset przyspieszający szyfrowanie SSL, który odciąża procesor przy wykonywaniu procesów szyfrowania i odszyfrowania.

Ponieważ każde z urządzeń Juniper Networks Secure Access SSL VPN używa tego samego oprogramowania, nie ma problemu wyboru urządzenia w zależności od umiejętności użytkowników lub administratorów. Wszystkie urządzenia oferują najwyższą wydajność, stabilność i skalowalność. Dlatego decyzję, które urządzenie najlepiej spełni potrzeby twojej organizacji, łatwo uzależnić od ilości użytkowników, redundancji systemu, możliwości akceleracji i potrzeb rosnącej populacji użytkowników korzystających ze zdalnego dostępu.

Produkty z serii Juniper Networks Secure Access SSL VPN przewodzą na rynku wirtualnych sieci prywatnych SSL (SSL VPN) tworząc kompletną ofertę urządzeń zdalnego dostępu, w tym Secure Access 2500 (SA 2500), Secure Access 4500 (SA 4500) i Secure Access 6500 (SA 6500). SA 6500 jest urządzeniem nowej generacji z wysoką skalowalnością i redundancją, zaprojektowane zostało specjalnie dla dużych przedsiębiorstw i dostawców usług. Urządzenia z serii Juniper Networks Secure Access łączą bezpieczeństwo SSL z bazującą na standardach kontrolą dostępu, szczegółowym tworzeniem reguł zachowań oraz bezkonkurencyjną elastycznością. Otrzymany rezultat zapewnia danemu przedsiębiorstwu kompleksową ochronę bez względu na zadania, które muszą zostać wykonane oraz umożliwia przechodzenie na coraz bardziej rygorystyczne poziomy kontroli dostępu, aby ochronić najbardziej cenne aplikacje i dane. Urządzenia z serii Juniper Networks Secure Access SSL VPN zapewniają niższy całkowity koszt utrzymania w porównaniu z tradycyjnymi rozwiązaniami IPSec oraz unikają cechy bezpieczeństwa typu „End-to-End”.

- **SA 2500:** Wspiera biznes małych i średnich rozmiarów (SMB) jako ekonomiczne rozwiązanie, które bez problemu obsłuży do 100 użytkowników jednocześnie w pojedynczym systemie lub w dwu-jednostkowym klastrze.
- **SA 4500:** Umożliwia średnim i dużym organizacjom obsługę 1000 użytkowników jednocześnie w pojedynczym systemie. Oferuje opcję migracji do sprzętowej akceleracji SSL dla tych organizacji, które wymagają największej wydajności przy dużym obciążeniu.
- **SA 6500:** Zbudowany z myślą o dużych przedsiębiorstwach i dostawcach usług, SA 6500 zapewnia najlepszą w swojej klasie wydajność, skalowalność i redundancję dla organizacji z wysokimi wymaganiami odnośnie bezpiecznego dostępu i autoryzacji. Obsługuje aż 10 000 użytkowników jednocześnie w pojedynczym systemie lub dziesiątki tysięcy w 4-jednostkowym klastrze.

Standardowe cechy SA 6500

- podwójne dyski twarde o zapisie lustrzanym w technologii Serial Advanced Technology Attachment (SATA), wymienne „na gorąco”
- podwójne wentylatory „hot swap”
- zasilacz „hot swap”
- 4 GB SDRAM,
- 4-portowa karta sieciowa 10/100/1000,
- interfejs zarządzający 10/100/1000,
- sprzętowy moduł akceleracji SSL.

Opcjonalne cechy SA 6500

- drugi zasilacz lub zasilacz prądu stałego DC,
- 4-portowa karta sieciowa Small Form-factor Pluggable (SFP).

Właściwości i zalety

Wysoka skalowalność w modelu Secure Access 6500 SSL VPN

SA 6500 został stworzony, aby sprostać zwiększającym się potrzebom dużych przedsiębiorstw i dostawców usług, dzięki czemu 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 SA 6500:

- pojedynczy SA 6500: obsługuje maks. 10 000 użytkowników jednocześnie,
- klastr z złożony z dwóch jednostek SA 6500: obsługuje maks. 18 000 użytkowników jednocześnie,
- klastr z złożony z trzech jednostek SA 6500: obsługuje maks. 26 000 użytkowników jednocześnie,
- klastr z złożony z czterech jednostek SA 6500: obsługuje maks. 30 000 użytkowników jednocześnie.

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

W przypadku Core Access oznacza to uzyskiwanie dostępu do rzeczywistych aplikacji Web, co niesie za sobą dokładne przepisywanie kodu HTML oraz ewaluację skonfigurowanych reguł polityki.

Warstwowa ochrona danych End-to-End

Modele SA 2000, SA 4000 i SA 6000 zapewniają warstwową ochronę danych End-to-End obejmującą klienta końcowego, urządzenia, dane oraz serwery.

Tabela 1: Warstwowa ochrona danych End-to-End, właściwości i zalety.

Właściwości	Opis właściwości	Zalety
Kontroler Hosta (Host Checker)	Klienci mogą być kontrolowani zarówno tuż przed jak i podczas 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 (MD5), na weryfikacji ustawień rejestru, certyfikatów urządzenia i wielu innych.	Weryfikuje/gwarantuje, że urządzenie końcowe spełnia standardy bezpieczeństwa przedsiębiorstwa przed udzieleniem dostępu, w razie potrzeby dostosowując urządzenie lub poddając użytkownika kwarantannie.
Interfejs API kontrolera hosta (Host Checker API)	Pozwala przedsiębiorstwom narzucić swoją politykę bezpieczeństwa wobec zarządzanych PC posiadających zainstalowaną zaporę ogniową, oprogramowanie antywirusowe lub inne oprogramowanie zabezpieczające, jednocześnie poddając kwarantannie urządzenia z nią niezgodne.	Podporządkowanie użytkowników i urządzeń zdalnych aktualnej polityce bezpieczeństwa; łatwiejsze zarządzanie.
Obsługa interfejsu zgodnego z Trusted Network Connect (TNC) na kontrolerze hosta	Umożliwia kooperację z różnorodnymi rozwiązaniami zabezpieczającymi, od oprogramowania antywirusowego przez zarządzanie patch'ami po rozwiązania odpowiedzialne za standaryzację.	Pozwala klientom użytkować istniejące systemy bezpieczeństwa punktu końcowego pochodzące od innych dostawców.
Egzekwowanie polityk	Pozwala przedsiębiorstwu ustalić czy dany host nie obsługujący z API jest godny zaufania bez potrzeby pisania dedykowanych API lub blokowania użytkowników zewnętrznych, takich jak klienci lub partnerzy korzystający z innych rozwiązań zabezpieczających.	Umożliwia uzyskanie dostępu przez końcowe urządzenia sieci ekstranet, takie jak komputery PC partnerów, którzy mogą korzystać z rozwiązań zabezpieczających odmiennych od wykorzystywanych przez przedsiębiorstwo.
Urządzenie o wzmocnionej konfiguracji bezpieczeństwa	Zaprojektowany na bazie dedykowanego systemu operacyjnego.	Urządzenie jest mniej podatne na ataki, jako że nie zostało zaprojektowane do wykonywania jakichkolwiek dodatkowych zadań; brak ogólnie znanych luk typu backdoor, które mogłyby być wykorzystane przez hackerów.

Właściwości	Opis właściwości	Zalety
Usługi zabezpieczeń wykorzystujące filtrowanie pakietów i bezpieczny ruting na poziomie jądra	Niepożądane pakiety są blokowane zanim rozpocznie się ich przetwarzanie przez stos TCP.	Odfiltrowuje nieuprawnione 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.
Paupki 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	Preinstalowane oprogramowanie sprawdzające użytkowników i urządzenia pod kątem keyloggerów, trojanów oraz aplikacji zdalnego dostępu.	Pozwala klientom wzmocnić ochronę punktu końcowego.
Skoordynowana kontrola zagrożeń (Coordinated Threat Control)	Umożliwia urządzeniu 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.	Skuteczna identyfikacja, powstrzymanie i zapobieganie zagrożeniom, zarówno na poziomie sieci jak i aplikacji, w obrębie sieci zdalnego dostępu.

Niższy całkowity koszt użytkowania

Oprócz szeregu korzyści związanych z bezpieczeństwem przedsiębiorstwa, modele SA 2500, SA 4500 oraz SA 6500 posiadają szereg właściwości, które redukują koszt ich użytkowania.

Tabela 2: Koszt użytkowania, właściwości i zalety.

Właściwości	Opis właściwości	Zalety
Wykorzystanie 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.
Protokoły i metody zabezpieczające oparte o standardy przemysłowe	Brak potrzeby instalacji wymaganych protokołów nie 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 – wsparcie dla nich jest wbudowane.
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 obsługi różnych wirtualnych witryn WWW za pomocą pojedynczego urządzenia SA.	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 dostosowanych do indywidualnych potrzeb.	Pozwala na indywidualne podejście do określonych ról usprawniając użytkowanie.
Juniper Networks Central Manager	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.
Obsługa sytuacji nadzwyczajnych (In case of emergency – ICE)	Pozwala na udzielenie licencji na ograniczony okres czasu większej liczbie dodatkowych użytkowników urządzenia SA SSL VPN w razie katastrofy, epidemii lub innych sytuacji nadzwyczajnych.	Pozwala przedsiębiorstwu na dalsze prowadzenie swojej działalności poprzez podtrzymanie produktywności, utrzymanie kontaktów biznesowych i kontynuację dostarczania usług swoim klientom w wypadku zaistnienia zdarzeń losowych poprzez umożliwienie zdalnej pracy większej liczbie pracowników.
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 wielu typów.

Bogate możliwości zarządzania prawami dostępu

Modele SA 2500, SA 4500 oraz SA 6500 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 SA, 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.

Właściwości	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.
Wstępna ocena stanu bezpieczeństwa	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 zgodność z obowiązującą polityką bezpieczeństwa.
Polityka dynamicznego uwierzytelniania	Pozwala administratorom na ustanowienie dynamicznej strategii uwierzytelniania unikalnej dla każdej 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 przyznany.	Pozwala administratorom przypisywać unikalną konfigurację dla poszczególnych sesji.
Autoryzacja zasobów	Niezwykle szczegółowa kontrola na poziomie URL, serwera lub plików.	Pozwala administratorom na dostosowanie polityki bezpieczeństwa do poszczególnych grup użytkowników, udostępniając jedynie niezbędne dane.
Szczegółowy audyt i logowanie	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 w 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 SA 2500, SA 4500 oraz SA 6500 pozwalają na kompleksowe zarządzanie hasłami. Właściwości te zwiększają produktywność użytkownika końcowego, znacznie upraszczają zarządzanie dużymi i zróżnicowanymi zasobami użytkowników, jak również w dużym stopniu redukują liczbę zgłoszeń do centrum obsługi technicznej.

Właściwości	Opis właściwości	Zalety
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 SA.
Pojedyncze logowanie (SSO) i NT LAN Manager (NTLM) przez Web	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 Microsoft.
Pojedyncze logowanie (SSO) bazujące na formularzach, zmiennych nagłówka, SAML przez Web	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 metody dostępu w zależności od zadań

Modele SA 2500, SA 4500 oraz SA 6500 zapewniają trzy różne metody dostępu. Selekcja danej metody jest jednym z elementów roli użytkownika, administrator może uaktywnić odpowiednią metodę dostępu dla poszczególnych sesji biorąc pod uwagę atrybuty użytkownika, urządzenia oraz sieci w połączeniu z politykami bezpieczeństwa przedsiębiorstwa.

Właściwość	Opis właściwości	Zalety
Clientless Care Web Access	Dostęp do aplikacji webowych, zawierających złożone elementy typu JavaScript, XML lub aplikacje Flash oraz aplety Java, które wymagają dostępu do socket'u, jak również do standardowych aplikacji e-mail, takich jak Outlook Web Access (OWA), współdzielonych zasobów plików Windows i UNIX, aplikacji telnet/SSH, emulacji terminali, SharePoint 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 instalowania dodatkowego 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 natywnych aplikacji 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.	Użytkownicy potrzebują jedynie przeglądarki WWW; Network Connect dokonuje przezroczystej selekcji pomiędzy dwiema możliwymi metodami transportu, aby automatycznie zapewnić najwyższą możliwą wydajność dla każdego środowiska sieciowego; korzystanie z Juniper Installer Services nie wymaga praw administratorских aby zainstalować, obsługiwać i aktualizować Network Connect; dostępny jest również opcjonalny samodzielny instalator.

Opcje produktu

Modele SA 2500, SA 4500 oraz SA 6500 występują w różnych opcjach licencyjnych w celu dostosowania funkcjonalności do potrzeb.

Licencje użytkownika

Wraz z pojawieniem się SA 2500, 4500 oraz 6500, proces zamawiania urządzeń został uproszczony dzięki kombinacji opcji, które można wprowadzać niezależnie od siebie. Obecnie w wariantach podstawowym potrzebna jest tylko jedna licencja: licencja na liczbę użytkowników. Również obecni użytkownicy starszej generacji urządzeń (SA 2000, 4000 i 6000) skorzystają z tych zmian, gdyż ich systemy zostaną uaktualnione do nowszej wersji oprogramowania (6.1 lub wyższej), czyli do nowego sposobu licencjonowania.

Licencje użytkownika dostarczają funkcjonalności, 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 zmian oprogramowania po stronie klienta, lub serwera, przebudowy strefy DMZ, wdrożeń agentów programowych lub nie wymagają ich wcale. Dla łatwego zarządzania ilością licencji użytkownika, każda licencja dopuszcza tytuł 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 licencję na kolejnych 100 użytkowników i wówczas system umożliwi obsługę do 200 użytkowników jednocześnie. Kluczowe cechy zawarte w ramach tej licencji to:

- Secure Application Manager (SAM) oraz Network Connect (NC) zapewniają funkcjonujące na różnych platformach wsparcie dla aplikacji klient/serwer dzięki użyciu SAM, jak również pełnego dostępu do wszystkich warstw sieci dzięki użyciu dwóch adaptacyjnych metod transportu, które są dostępne 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 opartą na rolach kontrolę dostępu i pozwala administratorom właściwie, dokładnie i dynamicznie równoważyć wymagania bezpieczeństwa z wymaganiami dostępu,
- zaawansowane wsparcie dla PKI to możliwość importowania wielu głównych i pośrednich CA, wsparcia protokołu Online Certificate Status Protocol (OCSP) oraz wielu certyfikatów serwerów,
- usługa samoobsługi użytkownika daje możliwość tworzenia własnych, ulubionych zakładek, w tym dostęp do ich własnych stacji roboczych ze zdalnej lokalizacji, a nawet zmianę swojego hasła kiedy już wygaśnie,
- wsparcie dla serwisów z wieloma nazwami (na przykład, <https://employees.company.com>, <https://partners.company.com> and <https://employees.company.com/engineering>). Każdy z nich może sprawiać wrażenie, jakby był jedynym serwisem obsługiwanym przez system, z osobnymi stronami logowania i z dostosowanym wyglądem tak, aby trafiać w potrzeby i przyzwyczajenia odbiorców,
- interfejs użytkownika dostosowany do potrzeb użytkownika i delegowanych ról administracyjnych,

- zaawansowana kontrola bezpieczeństwa stacji końcowych przy pomocy narzędzi takich jak: Host Checker, Cache Cleaner i Secure Virtual Workspace zapewnia, aby użytkownicy w sposób dynamiczny uzyskiwali dostęp do systemów i zasobów, ale tylko w stopniu, na który 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 Advanced Endpoint Defense zintegrowana z ochroną przed złośliwym oprogramowaniem (opcjonalnie)

Advanced Endpoint Defense: moduł ochrony przed złośliwym oprogramowaniem jest oprogramowaniem zintegrowanym z Host Checker'em zapewniającym ochronę przed niebezpieczeństwami, takimi jak konie trojańskie oraz key loggery znajdujące się na punkcie końcowym, z którego użytkownik ma zamiar rozpocząć zdalną sesję dostępu. Moduł chroniący przed złośliwym oprogramowaniem konfigurowany jest jako moduł kontrolera hosta i w sposób dynamiczny dostarczany jest do komputera PC użytkownika końcowego, bez potrzeby uprzedniego instalowania dodatkowego oprogramowania. Wszystkie urządzenia Secure Access SSL VPN dostarczane są razem z bezpłatną licencją dla 25 jednocześnie działających użytkowników. W celu zwiększenia tej liczby klienci powinni zamówić dodatkową licencję.

Licencja Advanced Endpoint Defense dostępna jest dla modeli SA 2500, SA 4500, oraz SA 6500.

Licencja Secure Meeting (opcjonalnie)

Licencja na aktywowanie Secure Meeting rozszerza możliwości urządzeń Juniper Networks Secure Access SSL VPN umożliwiając skuteczną ochronę konferencji webowych w dowolnym czasie i miejscu oraz zdalną kontrolę dostępu do PC. Secure Meeting umożliwia współdzielenie aplikacji w czasie rzeczywistym, co pozwala uprawnionym 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 AAA umożliwiają przedsiębiorstwom w prosty sposób zintegrować Secure Meeting z wykorzystywaną już przez nie wewnętrzną infrastrukturą uwierzytelniającą. Wiodąca na rynku, zoptymalizowana i posiadająca certyfikaty Common Criteria architektura urządzenia SSL VPN Junipera oraz zabezpieczenia transferu danych SSL/HTTPS dla wszystkich typów ruchu sieciowego gwarantują zgodność tego rozwiązania z najsurowszymi wymogami bezpieczeństwa przedsiębiorstwa.

Opcja Secure Meeting dostępny jest dla modeli SA 2500, SA 4500, and SA 6500.

Licencja Instant Virtual System (opcjonalnie)

Opcja Juniper Networks Instant Virtual System (IVS) opracowana została, aby umożliwić administratorom obsługę 255 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 tagowania VLAN (802.1Q) bazującego na rolach. Pozwala to na bezpieczne segregowanie ruchu użytkowników końcowych, nawet w przypadku gdy dwóch klientów posiada ten sam adres IP i umożliwia przypisanie konkretnego VLAN'u dla różnych klas 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 znajdować się w sieciach intranet klienta lub w sieci dostawcy usługi. Dostawcy mogą dostosować ogólną liczbę jednocześnie pracujących użytkowników dla poszczególnego klienta z możliwością rozszerzenia liczby kolejnych kategorii użytkowników, takich jak pracownicy zdalnych przedsiębiorstwa, kontrahentów, partnerów, i innych.

Opcja IVS dostępna jest dla modeli SA 4500 and SA 6500.

Opcja wysokiej dostępności (HA)

Juniper Networks opracowało różnorodne opcje klastrowania HA dla urządzeń Secure Access, zapewniając nadmiarowość i płynne funkcjonowanie systemu w potencjalnych przypadkach awarii. Te opcje klastrowania umożliwiają również skalowalność wydajności w celu spełnienia wymogów najbardziej wymagających środowisk. Modele Secure Access 2500 i 4500 mogą zostać zakupione w postaci klastrów złożonych z dwóch jednostek, a model Secure Access 6500 w postaci klastrów złożonych z dwóch lub wielu jednostek (Multi-Unit), co zapewnia całkowitą nadmiarowość oraz szeroką skalowalność użytkowania. Zarówno klastry Multi-Unit jak i klastry złożone z dwóch jednostek pozwalają na monitorowanie stanów i płynne funkcjonowanie całej sieci LAN i WAN w razie potencjalnej awarii jednej z jednostek. Wówczas konfiguracje systemu (takie jak konfiguracja serwera uwierzytelniającego, grup autoryzacji, zakładek, itp.), ustawienia profilu użytkownika (takie jak zdefiniowane przez użytkownika zakładki, pliki cookie, itp.) oraz sesje użytkowników zostaną zachowane. Przejęcie pracy przez drugą jednostkę jest płynne, co pozwala uniknąć przerw w produktywności użytkownika/przedsiębiorstwa, 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 Secure Access (w zależności od platformy) bez możliwości łączenia licencji na ilość obsługiwanych użytkowników. Na przykład jeżeli klient posiada licencje na 100 użytkowników dla SA 4500 a następnie zakupi kolejny SA 4500 z licencją klastrową na 100 użytkowników, to w ramach licencji wysokiej dostępności będzie miał możliwość współdzielenia pomiędzy tymi urządzeniami 100 użytkowników.

Opcja HA dostępna jest dla modeli SA 2500, SA 4500 oraz SA 6500.

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. Przy odpowiednim zbalansowaniu ryzyka i kosztów, opcja ICE dla urządzeń Juniper Networks Secure Access zapewnia rozwiązanie mogące sprostać nagłej potrzebie uzyskania zdalnego dostępu, co 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 Secure Access SSL VPN na ograniczony okres czasu.

Dzięki ICE przedsiębiorstwa mogą:

- utrzymać wydajność zapewniając pracownikom ogólny dostęp do aplikacji i danych z dowolnego miejsca, w 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,
- zbalansować ryzyko i skalowalność niskimi kosztami i prostotą wdrożenia.

Licencja ICE dostępna jest dla modeli SA4500 oraz SA6500 i zawiera wszystkie poniższe opcje i zestawy opcji:

- Baseline,
- Secure Meeting.

Specyfikacje

	SA 2500	SA 4500	SA 6500
Wymiary i zasilanie			
Wymiary (Szerokość × wysokość × głębokość)	17.26 × 1.75 × 14.5 in (43.8 × 4.4 × 36.8 cm)	17.26 × 1.75 × 14.5 in (43.8 × 4.4 × 36.8 cm)	17.26 × 3.5 × 17.72 in (43.8 × 8.8 × 45 cm)
Waga	6.6 kg	7.1 kg	12 kg
Montowanie w szafie rack	Tak, 1U	Tak, 1U	Tak, 2U, 19"
Zasilanie A/C	100-240 VAC, 50-60 Hz, 2.5 A Maks. 200 Wat	100-240 VAC, 50-60 Hz, 2.5 A Maks. 300 Wat	100-240 VAC, 50-60 Hz, 2.5 A Maks. 400 Wat
Bateria systemowa	CR2032 3 V litowa	CR2032 3 V litowa	CR2032 3 V litowa
Efektywność	min. 80% przy pełnym obciążeniu	min. 80% przy pełnym obciążeniu	min. 80% przy pełnym obciążeniu
Materiał	blacha stalowa walcowana na zimno o grubości 18 gauge (0,048")	blacha stalowa walcowana na zimno o grubości 18 gauge (0,048")	blacha stalowa walcowana na zimno o grubości 18 gauge (0,048")
Wentylatory	3 wentylatory o łożysku kulkowym 40 mm, wentylator jednostki zasilania o łożysku kulkowym 40 mm	3 wentylatory o łożysku kulkowym 40 mm, wentylator jednostki zasilania o łożysku kulkowym 40 mm	2 wentylatory typu hot-swap o łożysku kulkowym 80 mm, wentylator jednostki zasilania o łożysku kulkowym 40 mm

Wyświetlacz

Dioda LED zasilania, aktywności HD, awarii HW	Tak	Tak	Tak
Dioda aktywności HD i dioda awarii na kieszeni HD	Nie	Nie	Tak

Porty

Sieciowe	Dwa RJ-45 Ethernet 10/100/1000 half- lub full-duplex (z autonegociacją)	Dwa RJ-45 Ethernet 10/100/1000 half- lub full-duplex (z autonegociacją)	Cztery RJ-45 Ethernet lub half- lub full-duplex Opcjonalnie moduł SFP
Zarządzania	Brak	Brak	Jeden RJ-45 Ethernet 10/100/1000 half- lub full-duplex (z autonegociacją)
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	1 szeregowy port RJ45	1 szeregowy port RJ45	1 szeregowy port RJ45

Parametry środowiskowe

Temperatura pracy	41° do 104° F (5° do 40° C)	41° do 104° F (5° do 40° C)	41° do 104° F (5° do 40° C)
Temperatura przechowywania	-40° do 158° F (-40° do 70° C)	-40° do 158° F (-40° do 70° C)	-40° do 158° F (-40° do 70° C)
Wilgotność względna (praca)	8% do 90% bez kondensacji	8% do 90% bez kondensacji	8% do 90% bez kondensacji
Wilgotność względna (przechowywanie)	5% do 95% bez kondensacji	5% do 95% bez kondensacji	5% do 95% bez kondensacji
Wysokość (praca)	maksymalnie 10,000 ft (3,000 m)	maksymalnie 10,000 ft (3,000 m)	maksymalnie 10,000 ft (3,000 m)
Wysokość (przechowywanie)	maksymalnie 40,000 ft (12,192 m)	maksymalnie 40,000 ft (12,192 m)	maksymalnie 40,000 ft (12,192 m)

	SA 2500	SA 4500	SA 6500
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 kontraktem supportowym	90 dni, może zostać przedłużona kontraktem supportowym	90 dni, może zostać przedłużona kontraktem supportowym

Informacje do zamówień

Numer modelu	Opis
Secure Access 2500: system podstawowy	
SA2500	Secure Access 2500 Base System
Secure Access 2500: licencje na liczbę użytkowników	
SA2500-ADD-10U	Dodaje 10 jednocześnie pracujących użytkowników dla modelu SA 2500
SA2500-ADD-25U	Dodaje 25 jednocześnie pracujących użytkowników dla modelu SA 2500
SA2500-ADD-50U	Dodaje 50 jednocześnie pracujących użytkowników dla modelu SA 2500
SA2500-ADD-100U	Dodaje 100 jednocześnie pracujących użytkowników dla modelu SA 2500
Secure Access 2500: licencje opcji dodatkowych	
SA2500-MTG	Secure Meeting dla SA 2500
SA-AED-ADD-50U	ZAdvanced Endpoint Defense: Malware Protection – dodaje 50 równocześnie pracujących użytkowników
SA-AED-ADD-100U	Advanced Endpoint Defense: Malware Protection – dodaje 100 równocześnie pracujących użytkowników
Secure Access 2500: licencje klastrowania	
SA2500-CL-10U	Klastrowanie: Pozwala na dzielenie dodatkowych 10 użytkowników z kolejnego urządzenia SA 2500
SA2500-CL-25U	Klastrowanie: Pozwala na dzielenie dodatkowych 25 użytkowników z kolejnego urządzenia SA 2500
SA2500-CL-50U	Klastrowanie: Pozwala na dzielenie dodatkowych 50 użytkowników z kolejnego urządzenia SA 2500
SA2500-CL-100U	Klastrowanie: Pozwala na dzielenie dodatkowych 100 użytkowników z kolejnego urządzenia SA 2500
Secure Access 4500: system podstawowy	
SA4500	Secure Access 4500 Base System
Secure Access 4500: licencje na liczbę użytkowników	
SA4500-ADD-50U	Dodaje 50 jednocześnie pracujących użytkowników dla modelu SA 4500
SA4500-ADD-100U	Dodaje 100 jednocześnie pracujących użytkowników dla modelu SA 4500
SA4500-ADD-250U	Dodaje 250 jednocześnie pracujących użytkowników dla modelu SA 4500
SA4500-ADD-500U	Dodaje 500 jednocześnie pracujących użytkowników dla modelu SA 4500
SA4500-ADD-1000U	Dodaje 1000 jednocześnie pracujących użytkowników dla modelu SA 4500
Secure Access 4500: licencje opcji dodatkowych	
SA4500-MTG	Secure Meeting dla SA 4500
SA4000-IVS	Instant Virtual System dla SA 4000
SA4500-ICE	Licencja ICE dla SA 4500
SA4500-ICE-CL	Licencja klastrowania ICE dla SA 4500

Numer modelu	Opis
SA-AED-ADD-50U	Advanced Endpoint Defense: Malware Protection – dodaje 50 równocześnie pracujących użytkowników
SA-AED-ADD-100U	Advanced Endpoint Defense: Malware Protection – dodaje 100 równocześnie pracujących użytkowników
SA-AED-ADD-250U	Advanced Endpoint Defense: Malware Protection – dodaje 250 równocześnie pracujących użytkowników
SA-AED-ADD-500U	Advanced Endpoint Defense: Malware Protection – dodaje 500 równocześnie pracujących użytkowników
Secure Access 4500: licencje klastrowania	
SA4500-CL-50U	Klastrowanie: Pozwala na dzielenie dodatkowych 50 użytkowników z kolejnego urządzenia SA 4500
SA4500-CL-100U	Klastrowanie: Pozwala na dzielenie dodatkowych 100 użytkowników z kolejnego urządzenia SA 4500
SA4500-CL-250U	Klastrowanie: Pozwala na dzielenie dodatkowych 250 użytkowników z kolejnego urządzenia SA 4500
SA4500-CL-500U	Klastrowanie: Pozwala na dzielenie dodatkowych 500 użytkowników z kolejnego urządzenia SA 4500
SA4500-CL-1000U	Klastrowanie: Pozwala na dzielenie dodatkowych 1000 użytkowników z kolejnego urządzenia SA 4500
Secure Access 6500: system podstawowy	
SA6500	Secure Access 6500 Base System
Secure Access 6500: licencje na liczbę użytkowników	
SA6500-ADD-100U	Dodaje 100 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-250U	Dodaje 250 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-500U	Dodaje 500 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-1000U	Dodaje 1000 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-2500U	Dodaje 2500 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-5000U	Dodaje 5000 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-7500U*	Dodaje 7500 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-10000U*	Dodaje 10000 jednocześnie pracujących użytkowników dla modelu SA 6500
SA6500-ADD-12500U*	Dodaje 10000 jednocześnie pracujących użytkowników dla modelu SA 6500S
SA6500-ADD-15000U*	Dodaje 15000 jednocześnie pracujących użytkowników dla modelu SA 6500

Numer modelu	Opis
A6500-ADD-20000U*	Dodaje 20000 jednocześnie pracujących użytkowników dla modelu SA 6500
A6500-ADD-25000U*	Dodaje 25000 jednocześnie pracujących użytkowników dla modelu SA 6500
A6500-ADD-50000U*	Dodaje 50000 jednocześnie pracujących użytkowników dla modelu SA 6500

*Wymaga dodatkowych urządzeń SA 6500

Secure Access 6500: licencje opcji dodatkowych

SA6500-MTG	Secure Meeting dla SA 6500
SA6500-IVS	Instant Virtual System dla SA 6500
SA6500-ICE	Licencja ICE dla SA 6500
SA6500-ICE-CL	Licencja klastrowania ICE dla SA 6500
SA-AED-ADD-50U	Advanced Endpoint Defense: Malware Protection – dodaje 50 równocześnie pracujących użytkowników
SA-AED-ADD-100U	Advanced Endpoint Defense: Malware Protection – dodaje 100 równocześnie pracujących użytkowników
SA-AED-ADD-250U	Advanced Endpoint Defense: Malware Protection – dodaje 250 równocześnie pracujących użytkowników
SA-AED-ADD-500U	Advanced Endpoint Defense: Malware Protection – dodaje 500 równocześnie pracujących użytkowników
SA-AED-ADD-1000U	Advanced Endpoint Defense: Malware Protection – dodaje 1000 równocześnie pracujących użytkowników
SA-AED-ADD-2500U	Advanced Endpoint Defense: Malware Protection – dodaje 2500 równocześnie pracujących użytkowników

Secure Access 6500: licencje klastrowania

SA6500-CL-100U	Klastrowanie: Pozwala na dzielenie dodatkowych 100 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-250U	Klastrowanie: Pozwala na dzielenie dodatkowych 250 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-500U	Klastrowanie: Pozwala na dzielenie dodatkowych 500 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-1000U	Klastrowanie: Pozwala na dzielenie dodatkowych 1000 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-2500U	Klastrowanie: Pozwala na dzielenie dodatkowych 2500 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-5000U	Klastrowanie: Pozwala na dzielenie dodatkowych 5000 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-7500U	Klastrowanie: Pozwala na dzielenie dodatkowych 7500 użytkowników z kolejnego urządzenia SA 6500

Numer modelu	Opis
SA6500-CL-10000U	Klastrowanie: Pozwala na dzielenie dodatkowych 10000 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-12500U	Klastrowanie: Pozwala na dzielenie dodatkowych 12500 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-15000U	Klastrowanie: Pozwala na dzielenie dodatkowych 15000 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-20000U	Klastrowanie: Pozwala na dzielenie dodatkowych 20000 użytkowników z kolejnego urządzenia SA 6500
SA6500-CL-25000U	Klastrowanie: Pozwala na dzielenie dodatkowych 25000 użytkowników z kolejnego urządzenia SA 6500

Akcesoria

SA4500-CRYPTO	Wymienny moduł akceleratora SSL dla SA 4500
SA6500-PS	Wymienny nadmiarowy moduł zasilania dla SA 6500
SA6500-HD	Wymienny dysk twardy dla SA 6500
SA6500-FAN	Wymienny wentylator dla SA 6500
SA2500-4500-ACC-RKMT-1U	Rack Mount Kit do Secure Access and Infranet Controller – 1U
SA6500-ACC-RKMT-2U	Rack Mount Kit do Secure Access and Infranet Controller – 2U
SA6500-GBIC-FSX	Moduł GBIC Fiber SX dla SA 6500
SA6500-GBIC-FLX	Moduł GBIC Fiber LX dla SA 6500
SA6500-GBIC-COP	TModuł GBIC Copper dla SA 6500
SA6500-IOC	Karta GBIC I/O

Informacje o Juniper Networks

Juniper Networks Inc. jest liderem wysokowydajnych rozwiązań sieciowych. Juniper oferuje wysokowydajną infrastrukturę sieciową, tworzącą elastyczne i zaufane środowisko przyspieszające wdrażanie serwisów i aplikacji wewnątrz sieci. Wszystko to napędza biznes o dużym potencjale rozwoju. Więcej informacji można znaleźć na 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