



IDP SERIES INTRUSION DETECTION AND PREVENTION APPLIANCES (IDP75, IDP250, IDP800, IDP8200)

Ogólny zarys produktu

Zważywszy na stale rosnącą ilość i wyrafinowanie ataków sieciowych, coraz bardziej istotnym dla firm staje się bezpieczeństwo ich sieci. Problem potęguje jeszcze zwiększająca się liczba podatności w aplikacjach oraz systemach operacyjnych, jak również coraz krótszy czas z jakim tworzone są nowe ataki, mające na celu ich wykorzystanie. Seria urządzeń Juniper Networks IDP Intrusion Detection and Prevention oferuje najaktualniejsze możliwości chronienia sieci przed szerokim spektrum ataków dzięki funkcji systemu Intrusion Prevention System (IPS). Wspierane przez Juniper Networks Security Team, urządzenia serii IDP zapewniają również najszybsze w branży czasy reakcji na nowo wykryte zagrożenia.

Opis produktu

Seria urządzeń Juniper Networks IDP Intrusion Detection and Prevention zapewnia wszechstronny i prosty w obsłudze system ochrony, który powstrzymuje ataki na poziomie sieci i aplikacji, nie dając im dokonać szkód, minimalizując jednocześnie czas i koszty poświęcone utrzymaniu bezpiecznego środowiska sieciowego. Korzystając z uznanych w branży technik wykrywania i zapobiegania zagrożeniom, seria IDP od pierwszego dnia użytkowania gwarantuje ochronę przed robakami, trojanami, spyware'em, keyloggerami i innym złośliwym oprogramowaniem, zapobiegając zainfekowaniu przez nie sieci lub ich rozprzestrzenieniu poprzez zarażone wcześniej urządzenia.

Urządzenia z serii Juniper Networks IDP Intrusion Detection and Prevention nie tylko pomagają chronić sieć przed atakami, ale również dostarczają informacji na temat groźnych serwerów czy typów i wersji aplikacji oraz systemów operacyjnych, które mogły zostać dodane do sieci bezwiednie. Usługa sygnatur aplikacji, dostępna w serii IDP, idzie o krok dalej i pozwala na precyzyjne wykrywanie konkretnych aplikacji takich jak programy peer-to-peer czy komunikatory internetowe. Ta właśnie wiedza o konkretnych aplikacjach działających w sieci, umożliwia administratorom łatwiejsze realizowanie polityk bezpieczeństwa przy jednoczesnym pozostawianiu w zgodzie z korporacyjną polityką użytkownika aplikacji. Urządzenia z serii IDP Intrusion Detection and Prevention dają również możliwość korzystania ze znaczników DiffServ, co pozwala ruterom wprowadzać ograniczenia przepustowości łącza dla drugorzędnych aplikacji. Administratorzy są w stanie nie tylko sprawować kontrolę nad dostępem uzyskiwanym przez konkretne aplikacje, ale również zagwarantować aplikacjom o kluczowym znaczeniu dla firmy przewidywalną jakość usługi.

Urządzenia z serii Juniper Networks IDP Intrusion Detection and Prevention są zarządzane przez Juniper Networks Network and Security Manager (NSM), scentralizowane, oparte na regułach rozwiązań administracyjnych, zapewniające szczegółową kontrolę nad zachowaniem systemu. NSM umożliwia również łatwy dostęp do zebranych logów, w pełni konfigurowalną opcję raportowania i obsługę wszystkich urządzeń z serii Juniper Networks firewall/VPN/IDP z poziomu pojedynczego interfejsu użytkownika. Dzięki połączeniu systemów bezpieczeństwa najwyższej klasy, szczegółowej kontroli sieci, przejrzystości oraz scentralizowanemu zarządzaniu, seria IDP jest najlepszym rozwiązaniem dla zabezpieczenia kluczowych zasobów informacji.

Urządzenie Juniper Networks IDP75 Intrusion Detection and Prevention oferuje małym i średnim przedsiębiorstwom, jak również biurom regionalnym wszelkie możliwości Intrusion Prevention System (IPS). Wbudowana funkcja bypass to także opłacalny sposób na zagwarantowanie ciągłej dostępności sieci. Dzięki konkurencyjnemu i kompletnemu pakietowi IPS o wysoce elastycznych możliwościach, przedsiębiorstwa nie muszą już dłużej oszczędzać na bezpieczeństwie.

Urządzenia Juniper Networks IDP250 i IDP800 Intrusion Detection and Prevention oferują średnim i dużym przedsiębiorstwom, jak również usługodawcom, wiodące na rynku możliwości IPS. Wspierając rozmaite opcje wysokiej dostępności, IDP250 i IDP800 zapewniają stałą ochronę dla sieci należących do przedsiębiorstw czy usługodawców.

Seria Juniper Networks ISG Integrated Security Gateways stanowi elastyczny zintegrowany system bezpieczeństwa dla dużych przedsiębiorstw i usługodawców, z opcją dodawania modułów bezpieczeństwa z serii IDP, seria ISG prezentuje najkorzystniejszą na rynku ofertę, łączącą możliwości firewall'a, IPsec VPN i IPS, w ramach pojedynczego urządzenia.

Właściwości i zalety

Metody wykrywania ruchu sieciowego

Urządzenia Juniper Networks IDP Series Intrusion Detection and Prevention oferują kombinację ośmiu różnych metod służących precyzyjnej identyfikacji zagrożeń przepływających przez sieć. Zapewniając najwyższy stopień elastyczności, zróżnicowane metody wykrywania minimalizują także ilość fałszywych trafień.

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Wykrywanie poprzez sygnatury	Sygnatury są stosowane wyłącznie do odpowiednich partii ruchu sieciowego, określonych przez stosowny kontekst protokołu.	Zminimalizowanie występowania fałszywych trafień.
Wykrywanie nieprawidłowości w protokole	Użycie protokołu niezgodnie z założeniami umieszczonymi w dokumentach RFC jest weryfikowane w celu wykrycia ewentualnych naruszeń czy nadużyć.	Proaktywna ochrona niewykrytych słabych punktów sieci.
Wykrywanie backdoor	Oparta na heurystyce analiza nietypowych szablonów ruchu sieciowego i pakietów umożliwia wykrywanie trojanów i rootkitów.	Zapobieganie rozprzestrzenianiu się oprogramowania złośliwego w momencie, kiedy inne środki bezpieczeństwa zawodzą.
Wykrywanie nieprawidłowości w ruchu sieciowym	Heurystyczne zasady wykrywają niespodziewane szablony ruchu sieciowego, mogące sugerować próbę infiltracji lub ataku.	Aktywne zapobieganie infiltracji bądź atakom typu Distributed Denial of Service (DDoS).
Wykrywanie prób fałszowania adresu IP nadawcy (IP spoofing)	Sprawdzanie prawidłowości dozwolonych adresów wewnątrz i na zewnątrz sieci.	Zezwolenie wyłącznie na autoryzowany ruch sieciowy, podczas gdy dostęp z ukrytych źródeł jest blokowany.
Wykrywanie ataków typu Denial of Service (DoS)	Oparta na mechanizmie SYN cookies ochrona przed atakami typu SYN flood.	Ochrona kluczowych zasobów sieci przed zasypaniem atakami typu SYN flood.
Wykrywanie ataków i podejrzanych działań na poziomie warstwy 2 modelu OSI (Layer 2)	Ataki na poziomie warstwy 2 modelu OSI są wykrywane przy użyciu sugerowanych reguł dotyczących normatywnych ograniczeń dla tabel Address Resolution Protocol (ARP), obsługi fragmentacji, przekroczonej dozwolonych czasów połączenia oraz maksymalnej wielkości/długości dla pakietów danych.	Zapobieganie dalszemu infekowaniu wewnętrznej sieci przez zaatakowanego hosta przy użyciu takich metod jak ARP cache poisoning.
Sieciowy honeypot	Otwarte porty prowadzą do fałszywych zasobów, aby pomagać śledzić podejrzane działania.	Możliwość wglądu w zagrożenia mogące płynąć z sieci zewnętrznej i aktywna ochrona sieci zanim jeszcze jej kluczowe zasoby zostaną zaatakowane.

Możliwości Serii IDP

Urządzenia Juniper Networks IDP Series Intrusion Detection and Prevention oferują szereg wyjątkowych właściwości, gwarantujących najwyższy poziom bezpieczeństwa sieciowego.

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Dekodowanie protokołu	Wsparcie ponad 60 funkcji dekodujących, co wraz z ponad 500 kontekstami wymusza właściwe użycie protokołów.	Większa dokładność sygnatur dzięki precyzyjnemu kontekstowi protokołów.
Sygnatury ²	Zbiór ponad 5500 sygnatur służących identyfikacji nieprawidłowości, ataków, oprogramowania złośliwego i aplikacji.	Ataki są precyzyjnie identyfikowane, a próby wykorzystania znanych słabych punktów systemu są wykrywane.
Interpretacja ruchu sieciowego	Dostępne są opcje odświeżania, normalizacji i dekodowania protokołów.	Zapobieganie próbom obejścia pozostałych zabezpieczeń IDP poprzez użycie metod zaciemniania.
Identyfikacja i wiedza o aplikacjach	Zawiera kontekst użycia, informacje o protokole i sygnatury, aby umożliwić identyfikację aplikacji na każdym porcie.	Umożliwia oparcie reguł i polityk na przepływie aplikacji zamiast na portach – pozwala na ochronę i nadzorowanie standardowych aplikacji na niestandardowych portach.
Ochrona typu zero-day	Wykrywanie nieprawidłowości w protokole i zabezpieczanie nowo wykrytych słabych punktów systemu w dniu ich znalezienia.	Sieć jest od początku zabezpieczona przed wszystkimi nowymi zagrożeniami.

Rekomendowana polityka	Konkretna grupa sygnatur ataków jest identyfikowana przez Juniper Networks Security Team jako kluczowe dla ochrony danego typu przedsiębiorstwa.	Instalacja i obsługa są uproszczone przy jednoczesnym zagwarantowaniu najwyższego bezpieczeństwa sieci.
------------------------	--	---

¹Właściwości honeypota sieciowego nie są dostępne dla wersji IDP8200.

²Dostępnych jest 5560 sygnatur, ze średnio 10 nowymi dodawanymi cotygodniowo (stan ze stycznia 2008).

Szczegółowa kontrola ruchu sieciowego

Aby sprostać szerokiemu spektrum wymagań branżowych, Urządzenia Juniper Networks IDP Series Intrusion Detection and Prevention oferują szczegółową kontrolę nad przepływem danych w sieci.

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Aktywne reagowanie na ruch	Wspierane są różnorakie metody reagowania, takie jak odrzucenie pakietu, zrywanie połączenia, zamknięcie klienta, zamknięcie serwera oraz zamknięcie klienta/serwera.	Zapewnienie stosownego poziomu reagowania na ataki.
Znakowanie DiffServ/ QoS	Pakiety są znakowane przy użyciu DiffServ code point (DSCP).	Optimalizacja sieci i zapewnienie przepustowości łącza koniecznej do funkcjonowania kluczowych dla firmy aplikacji.
Pasywne reagowanie na ruch sieciowy	Wspierane są takie metody pasywnego reagowania jak reset czy logowanie TCP.	Uzyskanie wglądu w aktualne zagrożenia w sieci z możliwością udaremnienia potencjalnych ataków.
Reguły kontroli VLAN	W odniesieniu do każdego VLAN'a są stosowane unikalne polityki.	Stosowanie unikalnych polityk, zależnych od wymogów działu, klienta i zgodności z regulacjami prawnymi.
Rekomendowane działania	Zespół Juniper Networks Security Team zasugeruje stosowną reakcję sygnatury.	Łatwość utrzymania i obsługi. Administratorzy nie muszą już znać ani samemu poszukiwać właściwej odpowiedzi na każde możliwe zagrożenie.
IPAction	Możliwość wprowadzenia precyzyjnego zakazu dostępu wraz z konfiguracją czasu jego trwania, począwszy od konkretnego host'a, a skończywszy na wybranym ruchu sieciowym.	Blokowanie ataków DDoS (Distributed Denial of Service) wykrytych przez metodę wykrywania nieprawidłowości w ruchu sieciowym, system wykrywania DoS lub przy pomocy sieciowego honeypota.

Scentralizowane zarządzanie

Scentralizowane zarządzanie urządzeniami Juniper Networks IDP Series Intrusion Detection and Prevention i produktami typu firewall jest możliwe poprzez Network and Security Manager (NSM). NSM cechuje się ścisłą integracją pomiędzy wieloma różnymi platformami, co pozwala na proste i intuicyjne zarządzanie bezpieczeństwem całej sieci.

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
Administracja oparta na rolach	Ponad 100 różnych czynności może być przyporządkowanych jako unikalne uprawnienia, właściwe różnym administratorom.	Usprawnienie operacji biznesowych przez logiczny podział ról i narzucenie ich różnym administratorom.
Planowe aktualizacje systemu bezpieczeństwa	Automatyczne aktualizowanie urządzeń serii IDP o nowe sygnatury/potencjalne obiekty ataku.	Najwyższe aktualizacje bezpieczeństwa są wprowadzane bez konieczności manualnej ingerencji użytkownika.
Domeny	Możliwość logicznego rozdziału urządzeń, polityk, raportów i innych czynności administracyjnych.	Przystosowanie do operacji biznesowych poprzez grupowanie urządzeń oparte na sposobie prowadzenia interesów.
Blokowanie obiektów	Możliwość bezpiecznej równoczesnej modyfikacji konfiguracji.	Uniknięcie niewłaściwej konfiguracji jako efektu nadpisania ustawień konfiguracyjnych.
Regularne wykonywanie kopii zapasowych bazy danych	Zapewnienie wykonywania automatycznych kopii zapasowych bazy danych NSM.	Zapewnienie redundancji danych konfiguracyjnych.
Menadżer zadań	Wgląd w trwające i zakończone zadania.	Uproszczenie aktualizacji wielu zadań i urządzeń serii IDP.

Gromadzenie logów, raportowanie i powiadamianie

Połączenie urządzeń serii IDP Juniper Networks i menadżera NSM zapewnia szeroki wachlarz możliwości gromadzenia logów i raportowania.

WŁAŚCIWOŚĆ	OPIS WŁAŚCIWOŚCI	ZALETY
IDP Reporter	Prekonfigurowane raportowanie w czasie rzeczywistym, dostępne w każdym urządzeniu serii IDP.	Otrzymywanie szczegółowych raportów od każdego urządzenia serii IDP zainstalowanego w sieci, bez obciążania infrastruktury IT.
Profiler ³	Precyzyjne wychwytywanie szczegółów dotyczących profilu ruchu sieciowego w określonym przedziale czasowym.	Otrzymywanie szczegółowych informacji na temat napotykanego zagrożenia, jak również przepływu różnych aplikacji w sieci.
Security Explorer	Interaktywny i dynamiczny interfejs graficzny zapewnia kompleksowy wgląd w różne warstwy sieci i aplikacji.	Ogromne uproszczenie zrozumienia funkcjonowania ruchu sieciowego, jak również szczegółów dotyczących ataków.

³Funkcja profiler'a nie jest dostępna dla wersji IDP8200.



Specyfikacja techniczna

	IDP75	IDP250	IDP800	IDP8200
Wymiary i zasilanie				
Wymiary (szerokość × wysokość × głębokość)	43.2 × 4.3 × 38.1 cm (17 × 1.69 × 15 in)	43.2 × 4.3 × 38.1 cm (17 × 1.69 × 15 in)	43.2 × 8.6 × 48.3 cm (17 × 3.4 × 19 in)	43.2 × 8.6 × 48.3 cm (17 × 3.4 × 19 in)
Waga	15 lb	16.5 lb	27 lb	41 lb
Zasilanie A/C	100 – 240 VAC, 50 – 60 Hz 4.0 – 2.0 A maksimum 200 W	100 – 240 VAC, 50 – 60 Hz 5.0 – 1.5 A Cold Swappable, maksimum 300 W	100 – 240 VAC, 50 – 60 Hz 6.0 – 2.0 A Hot Swappable, nadmiarowy – podwójny, maksimum 400W	100 – 240 VAC, 50 – 60 Hz 10.0 – 4.0 A Hot Swappable, nadmiarowy – podwójny, maksimum 700W
Zasilanie D/C	brak	brak	(opcjonalnie) 36 V – 75 VDC, 24 – 11 A, Hot Swappable, nadmiarowy – podwójny, maksimum 710 W	(opcjonalnie) 36 V – 75 VDC, 24 – 11 A, Hot Swappable, nadmiarowy – podwójny, maksimum 710 W
Mean Time Between Failures (MTBF)	75000 godzin	73000 godzin	108000 godzin	73000 godzin
Pamięć	1 GB	2 GB	4 GB	16 GB
Dysk twardy	80 GB	80 GB	2 × 74 GB nadmiarowy RAID 1	2 × 74 GB nadmiarowy RAID 1
Porty				
Stałe porty I/O	Dwa porty RJ-45 Ethernet 10/100/1000 z bypassem	Osiem portów RJ-45 Ethernet 10/100/1000 z bypassem	Dziesięć portów RJ-45 Ethernet 10/100/1000 z bypassem	brak
Modularne sloty I/O	0	0	2	4
Modularne karty I/O	brak	brak	4-port GE miedziany z bypassem 4-port GE Fiber SFP 4-port GE SX-bypass	4-port GE miedziany z bypassem 4-port GE Fiber SFP 4-port GE SX-bypass 2-port 10GE bez bypassu 2-port 10 GE SR-bypass
Zarządzanie	Jeden port RJ-45 Ethernet 10/100/1000	Jeden port RJ-45 Ethernet 10/100/1000	Jeden port RJ-45 Ethernet 10/100/1000	Jeden port RJ-45 Ethernet 10/100/1000
Wysoka dostępność (HA)	brak	Jeden port RJ-45 Ethernet 10/100/1000	Jeden port RJ-45 Ethernet 10/100/1000	Jeden port RJ-45 Ethernet 10/100/1000
Wydajność⁴				
Maksymalna ilość sesji	10000	70000	500000	5 milionów
Przepustowość	150 Mbps	300 Mbps	1 Gbps	10 Gbps

⁴ Wydajność, przepustowość i inne cechy wyszczególnione powyżej oparte są na osiągnięciach systemów używających oprogramowania serii IDP w wersji 4.2r1 dla urządzenia IDP8200 i w wersji 4.1r2a dla urządzeń IDP75, IDP250 i IDP800. Pomiary przedstawiają najwyższe wartości otrzymane w standardowych warunkach testowych przy stosowaniu się do sugerowanej polityki, jeżeli nie zaznaczono inaczej. Faktyczne wyniki mogą się różnić w zależności od wersji oprogramowania serii IDP i zastosowania. Pełna lista wspieranego oprogramowania serii IDP dla urządzeń IDP75, IDP250, IDP800 i IDP8200 znajduje się na stronie Juniper Networks Customer Support Center (Centrum Obsługi Klienta Juniper Networks) pod adresem <http://www.juniper.net/customers/support/>

Specyfikacja techniczna (ciąg dalszy)

	IDP75	IDP250	IDP800	IDP8200
Nadmiarowość				
Redundantne zasilanie	Nie	Nie	Tak	Tak
Prąd stały (DC)	Nie	Nie	Tak	Tak
RAID	Nie	Nie	Tak	Tak
Wbudowany bypass	Tak	Tak	Tak	Tak
Parametry środowiskowe				
Temperatura pracy	5° do 40° C (41° do 104° F)	5° do 40° C (41° do 104° F)	5° do 40° C (41° do 104° F)	5° do 40° C (41° do 104° F)
Temperatura przechowywania	-40° do 70° C (-40° do 158° F)	-40° do 70° C (-40° do 158° F)	-40° do 70° C (-40° do 158° F)	-40° do 70° C (-40° do 158° F)
Względna wilgotność (w trakcie pracy)	8% do 90% bez kondensacji	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	5% do 95% bez kondensacji
Wysokość n.p.m. (w trakcie pracy)	3048 m (10000 ft)	3048 m (10000 ft)	3048 m (10000 ft)	3048 m (10000 ft)
Wysokość n.p.m. (przechowywanie)	12192 m (40000 ft)	12192 m (40000 ft)	12192 m (40000 ft)	12192 m (40000 ft)

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 wysoko wydajnej sieci. Nasze produkty zapewniają generujące zyski możliwości, co ułatwia wprowadzanie na rynek nowych modeli biznesowych i przedsięwzięć, a także poszerza zasięg rynku. 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

Informacje dotyczące zamówień

NUMER MODELU	OPIS
Urządzenia IDP Juniper Networks	
IDP75	IDP75 Intrusion Detection and Prevention Appliance
IDP250	IDP250 Intrusion Detection and Prevention Appliance
IDP800	IDP800 Intrusion Detection and Prevention Appliance
IDP8200	IDP8200 Intrusion Detection and Prevention Appliance
Moduły I/O dla IDP800 i 8200	
IDP-10GE-2SR-BYP	IDP 2-porty 10GE z bypass (SR) (wyłącznie dla IDP8200)
IDP-10GE-2XFP	IDP 2-porty 10GE (SR/LR) (wyłącznie dla IDP8200)
IDP-1GE-4COP-BYP	IDP 4-porty z bypass
IDP-1GE-4SFP	IDP 4-porty SFP (bez bypass)
IDP-1GE-4SX-BYP	IDP 4-porty fiber z bypass (SX)
UNIV-SFP-COP	IDP miedziany SFP
UNIV-SFP-FLX	IDP światłowodowy SFP LX
UNIV-SFP-FSX	IDP światłowodowy SFP SX
UNIV-SFP-FSR	Transceiver XFP światłowodowy krótkiego zasięgu
UNIV-SFP-FLR	Transceiver XFP światłowodowy długiego zasięgu
Zarządzanie*	
NS-SM-S-BSE	Oprogramowanie Network and Security Manager (NSM) z licencją na obsługę 25 urządzeń
NS-SM-ADD-50D	Licencja na dodatkowe 50 urządzeń
NS-SM-ADD-100D	Licencja na dodatkowe 100 urządzeń
Dostępne są dodatkowe opcje licencyjne NSM	

NUMER MODELU	OPIS
Akcesoria	
UNIV-74G-HDD	Zamienny HDD dla IDP800 i IDP8200
UNIV-PS-710W-DC	Zasilacz DC dla IDP800 i IDP8200
UNIV-PS-400W-AC	Zasilacz AC dla IDP800
UNIV-PS-700W-AC	Zasilacz AC dla IDP8200
UNIV-PS-300W-AC	Zasilacz AC dla IDP250
IDP-FLASH	Pakiet instalacyjny dla IDP75, IDP250 i IDP800
IDP-FLASH-8200	Pakiet instalacyjny dla IDP8200
UNIV-MR2U-FAN	Zapasy wentylator do urządzenia IDP800
UNIV-HE2U-FAN	Zapasy wentylator do urządzenia IDP8200
UNIV-HE2U-RAILKIT	Zestaw do montażu w rack'u urządzenia IDP8200 (zawiera szyny)
UNIV-MR2U-RAILKIT	Zestaw do montażu w rack'u urządzenia IDP 800 (zawiera szyny)
UNIV-MR1U-RAILKIT	Zestaw do montażu w rack'u urządzeń IDP250 i IDP75 (zawiera szyny)

* Każde zakupione urządzenie z serii IDP posiada oryginalnie licencję na obsługę pięciu urządzeń.

O Juniper Networks

Juniper Networks, Inc. jest liderem w dziedzinie wysoko wydajnych 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.

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.