

Juniper Networks NetScreen-IDP 10/100/500/1000

Urządzenia zabezpieczeń Juniper Networks NetScreen Intrusion Detection and Prevention (NetScreen-IDP) realizują zadania monitorowania aplikacji i sieci oraz wykrywania i przeciwdziałania incydentom i dzięki temu są sprawnym mechanizmem obrony przed najgroźniejszymi atakami. NetScreen-IDP po podłączeniu do sieci skutecznie zatrzymuje ataki na poziomie sieci i aplikacji zanim spowodują one rzeczywiste zniszczenia, dzięki czemu minimalizuje nakłady finansowe i czasowe związane z włamaniami. Urządzenia NetScreen-IDP nie tylko ułatwiają zabezpieczenie sieci przed skutkami ataków, ale dostarczają informacje nt. nieuprawnionych aplikacji i komputerów, które zostały dodane do sieci bez wiedzy administratorów. Posiadanie wiedzy o istnieniu w sieci nieuprawnionych aplikacji takich jak programy peer-to-peer lub komunikatory ułatwia utrzymanie polityki bezpieczeństwa oraz zapewnienie zgodności ze strategią wykorzystania aplikacji w firmie. Scentralizowane, oparte o reguły zarządzanie zapewniające precyzyjną kontrolę nad działaniem systemu informatycznego oraz łatwy dostęp do funkcji rejestrowania zdarzeń, a także tworzenia raportów dostosowanych do potrzeb użytkownika to własności, dzięki którym urządzenia NetScreen-IDP są najlepszym sposobem zabezpieczenia kluczowych zasobów informacyjnych firmy.



Juniper Networks NetScreen-IDP 10/100/500/1000

System zarządzania

Architektura trójwarstwowa		Tak
Interfejs użytkownika GUI	Windows Linux	Tak Tak
Centralny serwer zarządzania	Linux Red Hat 7/8 Red Hat Enterprise Server 3 Solaris 7/8	Tak Tak
Interfejs zarządzania	Aplikacja GUI (Java) Interfejs wiersza poleceń (CLI)	Tak Tak
Liczba użytkowników		nieograniczona
Scentralizowane zarządzanie	Zarządzanie polityką Przeglądanie logów Zarządzanie incydentami	Tak Tak Tak
Rejestrowanie zdarzeń		Ponad 50,000 zapisów na sekundę
Eksportowanie logów		PDF, Postscript, XML, CSV, SNMP, SMTP, Syslog, PostgreSQL
Aktualizacja sygnatur		Uaktualnienia sygnatur minimum raz na tydzień
Raporty generowane w czasie rzeczywistym		Tak
Raporty definiowane przez użytkownika		Tak
Raporty z możliwością eksportu (HTML)		Tak

Urządzenie zabezpieczeń

Metody detekcji ataków (8 metod)	- wykrywanie ataków poprzez pełno-stanowe sygnatury - wykrywanie anomalii protokołów - wykrywanie tylnych wejść - wykrywanie anomalii ruchu - wykrywanie spoofingu IP - wykrywanie ataków (D)DoS - wykrywanie ataków L2 - oszukiwanie intruzów (network honeypot)	Tak Tak Tak Tak Tak Tak Tak Tak
----------------------------------	--	--

Juniper Networks NetScreen-IDP 10/100/500/1000

Sygnatury	Pełno-stanowe (stateful) Analizowane konteksty aplikacji Ataki złożone (sygnatury + anomalie protokołów) Otwarty format sygnatur Definiowane przez użytkownika Równoległe dopasowywanie sygnatur Dekodowane protokoły	Tak 500+ Tak Tak Tak Tak 60+
Interpretacja ruchu	Scalanie pakietów Usuwanie duplikatów Normalizacja danych	Tak Tak Tak
Aktywna reakcja	Zablokowanie pakietu Zablokowanie połączenia	Tak Tak
Pasywna reakcja	TCP Reset Zamknij klienta Zamknij serwer Zamknij połączenia Akcje na adres IP	Tak Tak Tak Tak Tak
Metody powiadamiania	Wbudowana przeglądarka logów SMTP (email) Skrypty użytkownika SNMP SYSLOG	Tak Tak Tak Tak Tak
Zarządzanie pakietami	Zapis sesji ustalany przez użytkownika Wbudowana przeglądarka pakietów Zgodność z przeglądarkami pakietów innych firm	Tak Tak Tak
Tryby pracy	Bridge Router Proxy-ARP Transparent Sniffer (pasywny)	Tak Tak Tak Tak Tak
Sieci korporacyjne	Obsługa sieci VLAN 802.1Q Obsługa SNMP MIB-II	Tak Tak
Narzędzia monitorowania i reagowania na incydenty	Informacje o incydentach poziomu aplikacji (L7) Informacje o incydentach poziomu sieci (L2-L4) Informacje o nieprzebrzeganiu przez pracowników polityki firmy Korelacja informacji o incydentach Wyjaśnianie incydentów (TruSecure)	Tak Tak Tak Tak Tak

Sensor Hardware	Juniper Networks NetScreen-IDP 10	Juniper Networks NetScreen-IDP 100	Juniper Networks NetScreen-IDP 500	Juniper Networks NetScreen-IDP 1000	Juniper Networks NetScreen-IDP Bypass
Interfejsy	2 interfejsy miedziane gigabitowe Ethernet i 1 interfejs standardowy 10/100	2 interfejsy miedziane gigabitowe Ethernet i 2 interfejsy standardowe 10/100 ⁽¹⁾	2 interfejsy miedziane gigabitowe Ethernet i 2 światłowodowe gigabitowe ⁽²⁾	2 interfejsy miedziane gigabitowe Ethernet i 2 światłowodowe gigabitowe ⁽²⁾	
Pamięć (RAM)	512 MB	1 GB	4 GB	4 GB	
Maksymalna liczba sesji	10 000	70 000	220 000	500 000	
Przepustowość	do 20 Mb/sek ⁽³⁾	do 200 Mb/sek	do 500 Mb/sek	do 1 Gb/sek ⁽⁴⁾	
Wysoka dostępność					
Standalone failover	Nie	Tak	Tak	Tak	
Klasytry HA	Nie	Tak	Tak	Tak	
Równoważenie obciążenia	Nie	Tak	Tak	Tak	
Zewnętrzne LB	Nie	Tak	Tak	Tak	
Fail Open	Tak ⁽⁵⁾	Tak ⁽⁵⁾	Tak ⁽⁶⁾	Tak ⁽⁶⁾	
Fizyczna redundancja					
Redundantne zasilanie	Nie	Opcjonalnie	Tak	Tak	
RAID	Nie	Opcjonalnie	Tak	Tak	
Parametry fizyczne					
Moc AC	230 Wat	275 Wat	275 Wat	325 Wat	12 Wat
Napięcie AC	100/240 VAC, 2.0-1.0 A, 50/60 Hz	100/240 VAC, 3.9-2.0 A, 50/60 Hz	100/240 VAC, 3.9-2.0 A, 50/60 Hz	110/220 V	90-264 VAC
Bateria systemowa	CR2032 3V	CR2032 3V	CR2032 3V	3V	
Temperatura pracy	50° to 95°F	50° to 95°F	50° to 95°F	50° to 95°F	
Temperatura przechowywania	-40° to 149°F	-40° to 149°F	-40° to 149°F	-40° to 149°F	
Wilgotność względna (praca)	8% to 80%	8% to 80%	8% to 80%	8% to 80%	
Wilgotność względna (przechowywanie)	5% to 95%	5% to 95%	5% to 95%	5% to 95%	
Wysokość (praca)	-50 to 10 000 ft	-50 to 10 000 ft	-50 to 10 000 ft	-50 to 10 000 ft	
Wysokość	-50 to 35 000 ft	-50 to 35 000 ft	-50 to 35 000 ft	-50 to 35 000 ft	
Waga	27 lbs	35,27 lbs	35,27 lbs	35 lbs	1,5 lbs
Wysokość	1,69 cali 1 U	1,69 cali 1 U	1,69 cali 1 U	1,69 cali 1 U	1,35 cali
Szerokość	16,7 cala	19 cali	19 cali	17,61 cali	8 cali
Głębokość	23,1 cala	26,9 cala	26,9 cala	27 cali	5 cali

- ⁽¹⁾ Każdy interfejs 10/100 można zastąpić opcjonalną kartą z czterema interfejsami 10/100/1000. W sumie 2 standardowe interfejsy 10/100 można zastąpić ośmioma interfejsami 10/100/1000.
- ⁽²⁾ Każdy interfejs światłowodowy (Base-SX) można zastąpić opcjonalną kartą z czterema interfejsami 10/100/1000. W sumie 2 standardowe interfejsy światłowodowe (Base-SX) można zastąpić ośmioma interfejsami 10/100/1000. Uwaga: światłowodowe karty gigabitowe są przystosowane wyłącznie dla łącz wielo-modowych SC (Base-SX). Jeśli jest potrzebne łącze jedno-modowe użytkownik powinien zastosować konwerter.
- ⁽³⁾ Urządzenie IDP-10 obsługuje ciągle przepustowość 20 MB/Sec, choć może obsłużyć przepustowość pełnej szybkości łącza.
- ⁽⁴⁾ Zgodnie z testami dla oprogramowania IDP 3.0.
- ⁽⁵⁾ Wymaga modułu NetScreen-IDP Bypass, który zakupuje się oddzielnie.
- ⁽⁶⁾ Wymaga zastosowania urządzenia Bypass dostarczanego przez firmy zewnętrzne.

Serwer zarządzania

Oprogramowanie zarządzające IDP działa w systemie Solaris 7/8 lub Linux RedHat 7.2/8 albo RedHat Enterprise Server 3. Zalecany procesor: 1GHZ (Linux), 400 MHz (Solaris). Zalecane parametry sprzętowe: 1GB RAM, 18 GB miejsca na dysku.

Produkt

NetScreen-IDP 10 Intrusion Detection and Prevention Appliance
 NetScreen-IDP 100 Intrusion Detection and Prevention Appliance
 NetScreen-IDP 500 Intrusion Detection and Prevention Appliance
 NetScreen-IDP 1000 Intrusion Detection and Prevention Appliance

Produkt

NS-IDP-10
 NS-IDP-100-002
 NS-IDP-500-002
 NS-IDP-1000

Kliencka aplikacja zarządzająca z graficznym interfejsem użytkownika

Aplikacja kliencka to program w Javie działający w systemach Windows 2000, NT, XP oraz Linux RedHat 8 lub RedHat Enterprise Server 3. Środowisko wykonawcze Javy w wersji 1.4.1 jest dołączone. Wymagania miejsca na dysku: 128 MB. Wymagania RAM: 256 MB (IDP 2.1), 512 MB (IDP 3.0)

Akcesoria

NetScreen-IDP Bypass Fail-Open Device (tylko IDP-10 i IDP-100)
 Karty NetScreen-IDP Fiber Gigabit (zestaw 2 kart)*
 Poczwórna karta NetScreen-IDP 10/100/1000**
 Nadmiarowy twardy dysk NetScreen-IDP (tylko IDP 100)
 Zasilacz AC NetScreen-IDP (tylko IDP 100)
 NetScreen-IDP Rapid Rail Kit
 NetScreen-IDP Chatsworth Rail Kit
 *wyłącznie dla urządzenia NetScreen-IDP 100
 **wyłącznie dla urządzeń NetScreen-IDP 100/500/1000



1194 North Mathilda Avenue Sunnyvale, CA 94089 USA
 Tel: 888-JUNIPER (888 -586-4737) lub 408-745-2000
 Faks: 408-745-2100

Copyright © 2004 Juniper Networks, Inc. Wszystkie prawa zastrzeżone. Juniper Networks, logo Juniper Networks, NetScreen, NetScreen Technologies, GigaScreen oraz logo NetScreen to zarejestrowane znaki handlowe firmy Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC oraz NetScreen ScreenOS to zarejestrowane znaki handlowe firmy Juniper Networks, Inc. Wszystkie pozostałe znaki handlowe oraz zarejestrowane znaki handlowe należą do ich prawowitych właścicieli.
 Numer części: 110010-001 kwiecień 2004

Dystrybucja w Polsce:



CLICO Sp. z o.o.
 30-063 Kraków, Al. 3-go Maja 7
 tel. (12) 632-51-66
 tel. (12) 292-75-22 ... 25
 fax (12) 632-36-98
 e-mail: info@netscreen.pl
 www.netscreen.pl

CLICO Oddział Katowice
 40-555 Katowice, ul. Rolna 43
 tel. (32) 203-92-35
 tel. (32) 609-80-50
 tel. (32) 609-80-51
 fax (32) 203-92-24
 e-mail: katowice@clico.pl

CLICO Oddział Warszawa
 03-738 Warszawa, ul. Kijowska 1
 tel. (22) 518-02-70...72
 fax (22) 518-02-73
 e-mail: warszawa@clico.pl