

# Juniper Networks NetScreen-Security Manager

- Scentralizowane zarządzanie „end-to-end” w całym cyklu życia urządzenia zapewniające szczegółową kontrolę nad konfiguracją urządzenia, ustawieniami sieci i politykami zabezpieczeń.
- Delegowanie ról administratora zapewnia dostęp do informacji tym, którzy ich potrzebują.
- Intuicyjny, graficzny interfejs użytkownika upraszcza wykonywanie skomplikowanych zadań, takich jak konfiguracja urządzeń, definiowanie polityk i instalacja VPN.
- Trójwarstwowa architektura maksymalizuje wydajność i elastyczność.

## Ogólny opis produktu

System Juniper Networks NetScreen-Security Manager, łatwe w użyciu rozwiązanie zarządzające wszystkimi aspektami urządzeń Netscreen włącznie z ich konfiguracją, ustawieniami sieci i polityką zabezpieczeń to nowe podejście do zarządzania bezpieczeństwem. W odróżnieniu od niektórych rozwiązań, w których konieczne jest korzystanie z wielu narzędzi zarządzających dla jednego urządzenia, dzięki systemowi NetScreen-Security Manager dział IT może zarządzać urządzeniem w całym cyklu jego życia posługując się jednym, scentralizowanym systemem. Za pomocą systemu NetScreen-Security Manager technicy, administratorzy sieci i administratorzy zabezpieczeń mogą wspólnie pracować nad poprawą wydajności zarządzania, minimalizacją nakładów pracy i obniżeniem kosztów.

## Delegowanie uprawnień administratora

NetScreen-Security Manager umożliwia działom informatycznym korporacji delegowanie odpowiednich poziomów dostępu administracyjnego, od dostępu „tylko do odczytu” do pełnych praw edycyjnych, dla odpowiednich użytkowników. Dzięki temu, osoby, którym nadano odpowiednie prawa mogą wykonywać różnorodne zadania administracyjne. Korporacje mogą udostępnić lub ograniczyć dostęp do informacji określonym osobom lub komórkom organizacyjnym. Dzięki temu pracownicy mogą podejmować decyzje zgodne z ich rolą w korporacji. Podobnie, dzięki udostępnieniu, lub ograniczeniu, uprawnień systemowych na podstawie umiejętności użytkowników, korporacje mogą stosować administrację na podstawie ról. W takim przypadku prawa i zadania odpowiadają bezpośrednio idealnej strukturze zespołu korporacji. Administrację na podstawie ról można osiągnąć wykorzystując predefiniowane role w systemie NetScreen-Security Manager lub poprzez utworzenie ról użytkownika na podstawie ponad pięćdziesięciu zadań, które można przypisać w systemie. Dodatkowo system NetScreen-Security Manager posiada kilka innych własności, które umożliwiają poprawę skuteczności zespołu pracującego nad zabezpieczeniami:

- Blokowanie obiektów umożliwia równoległe bezpieczne modyfikowanie różnych polityk przez kilku administratorów;
- Pola komentarzy w plikach logów i politykach umożliwiają zespołowi administracyjnemu wyjaśnianie przeznaczenia reguł i stanu incydentów;
- Menedżer zadań umożliwia scentralizowany wgląd w stan wszystkich uaktualnień urządzeń, zarówno w trakcie wykonywania jak zakończonych;

Dzięki stylowi zarządzania w systemach NetScreen korporacje mogą wyposażyć grupy lub osoby odpowiedzialne za poszczególne fazy cyklu życia urządzeń w prawo do podejmowania kluczowych decyzji dotyczących bezpieczeństwa z zachowaniem poufności. W ten sposób poprawiają bezpieczeństwo zapewniając użytkownikom dostęp tylko do tych informacji, do których dostęp jest niezbędny.

## Uproszczone zarządzanie złożonymi zadaniami

Kluczową zasadą filozofii projektowej systemu NetScreen-Security Manager jest uproszczenie złożoności administracji urządzeń zabezpieczeń przy zachowaniu elastyczności pozwalającej na spełnienie różnorodnych potrzeb firm. System NetScreen-Security Manager dostarcza jednolitego, zintegrowanego interfejsu zarządzania, za pomocą którego można kontrolować każdy parametr urządzenia z centralnej lokalizacji. Za pomocą kilku kliknięć myszą administrator może skonfigurować urządzenie, utworzyć politykę zabezpieczeń lub zarządzać uaktualnieniami oprogramowania firmware. Za pomocą systemu NetScreen-Security Manager można zarządzać wszystkimi tymi aspektami urządzenia, którymi można zarządzać za pomocą interfejsu wiersza poleceń. System NetScreen-Security Manager zawiera, między innymi, następujące narzędzia:

- Szablony ról upraszczają tworzenie i zarządzanie uprawnieniami użytkowników;

- Szablony konfiguracji urządzeń pozwalają na zminimalizowanie błędów konfiguracji. Wszystkie aspekty urządzenia lub grupy urządzeń są zarządzane za pośrednictwem szablonu;
- Menedżer VPN przyspiesza instalację VPN poprzez utworzenie niezbędnych reguł po zdefiniowaniu podstawowej topologii;

## Rejestrowanie i tworzenie raportów

System NetScreen-Security Manager zawiera wysokowydajny mechanizm rejestrowania umożliwiający działom informatyki zbieranie i monitorowanie szczegółowych informacji historycznych dotyczących kluczowych kryteriów, takich jak ruch w sieci oraz zdarzenia związane z bezpieczeństwem. Wykorzystując wbudowane możliwości raportowania administratorzy mogą błyskawicznie generować raporty, które można wykorzystać w procesie wyjaśniania przyczyn określonych sytuacji lub sprawdzania, czy użytkownicy postępują zgodnie z obowiązującymi zasadami. W celu wykonania bardziej szczegółowej analizy, pliki logów można wyeksportować do narzędzi wspomagających tworzenie raportów firm zewnętrznych lub bazy danych. Mechanizmy monitorowania czasu rzeczywistego umożliwiają śledzenie stanu sieci VPN oraz włączenia (wyłączenia) urządzeń, a także monitorowanie klastra HA. Logi zapisane za pomocą systemu NetScreen-Security Manager można analizować w następujący sposób.

- Funkcja Log Viewing umożliwia przeglądanie logów zarejestrowanych w systemie w czasie rzeczywistym. Zdefiniowane przez użytkownika filtry umożliwiają administratorowi wykonywanie błyskawicznego analizy stanu zabezpieczeń oraz zachodzących w systemie zdarzeń
- Funkcja Log Investigator zapewnia możliwość skorelowania wysokopoziomowych informacji z logów w celu poszukiwania trendów i anomalii;
- Log Reporting umożliwia administratorowi generowanie, przeglądanie i eksportowanie raportów podsumowujących logi oraz alarmów, których źródłem są zarządzane urządzenia firewall/VPN.

## Architektura

Na architekturę systemu NetScreen-Security Manager składają się: serwer urządzenia (Device Server), serwer graficznego interfejsu użytkownika (GUI Server) oraz interfejs użytkownika (UI). W celu spełnienia różnorodnych potrzeb personelu informatycznego w zakresie zarządzania, a jednocześnie zachowania elastyczności i wysokiej wydajności podjęto fundamentalną decyzję projektową dotyczącą umieszczenia wszystkich funkcji dotyczących urządzenia na serwerze urządzenia (Device server), a wszystkich scentralizowanych funkcji konfiguracyjnych na serwerze graficznego interfejsu użytkownika (GUI server). Oddzielenie serwera urządzenia od serwera graficznego interfejsu użytkownika pozwala na osiągnięcie lepszej wydajności i elastyczności. Komponenty serwera urządzenia i graficznego interfejsu mogą być umieszczone na tym samym serwerze w przypadku, gdy najważniejszą rolę odgrywają koszty i (lub) prostota rozwiązania. Można je również umieścić na oddzielnych serwerach wtedy, kiedy wydajność lub elastyczność instalacji są ważniejsze. Niezależnie od rozmieszczenia serwera urządzenia i serwera GUI, interfejs użytkownika (UI) stanowi dla administratora pojedynczy punkt dostępu do wszystkich informacji i funkcji systemu. Dzięki wykorzystaniu możliwości obliczeniowych serwera GUI dla większej części obciążenia, można zminimalizować obciążenie komputera końcowego użytkownika. Wszystkie warstwy systemu NetScreen-Security Manager są połączone za pomocą kanału komunikacji opartego o protokół TCP zabezpieczonego poprzez szyfrowanie AES oraz uwierzytelnianie SHA-1. Dzięki zastosowaniu w kanale komunikacji mechanizmów zabezpieczeń podobnych do IPSec VPN, łatwo można wdrożyć bezpieczne zarządzanie w większości środowisk sieciowych.

## Przegląd własności

## Konfiguracja

- Szablony urządzeń z możliwością zastępowania wartości domyślnych;
- Konfiguracja wszystkich aspektów urządzenia;
- Możliwość importu kompletnej konfiguracji urządzenia;
- Sprawdzanie poprawności konfiguracji urządzenia;
- Raport różnic w konfiguracji urządzeń;
- Narzędzie modelowania VPN;
- Zarządzanie VPN na podstawie tras lub polityk;
- Topologie VPN typu full mesh, hub & spoke, mieszana;
- Współdzielenie polityk;
- Zarządzanie zabezpieczeniami antywirusowymi oparte o reguły;
- Zarządzanie głęboką inspekcją zapory firewall oparte o reguły;
- Sprawdzanie poprawności polityk;
- Współdzielenie obiektów;

## Rejestrowanie

- Zintegrowane logi czasu rzeczywistego i historyczne;
- Pełne możliwości filtrowania;
- Zapisywanie widoków dla poszczególnych użytkowników;
- Oznaczanie logów, wprowadzanie komentarzy pomocnych przy koordynacji pracy zespołowej;

## Administracja

- Administracja w oparciu o reguły;
- Blokowanie obiektów;
- Logowanie i audyt;
- Domeny;
- Zautomatyzowane nadawanie wersji domen;
- Menedżer zadań umożliwiający śledzenie statusu aktualizacji;
- Integracja z narzędziami firm zewnętrznych;
- Serwer Syslog na podstawie reguł;
- SNMP na podstawie reguł;

## Monitorowanie w czasie rzeczywistym

- Zapory firewall;
- Sieci VPN;
- Klastry NSRP (HA);
- Wykorzystanie procesora dla serwera GUI;
- Wykorzystanie procesora dla serwera urządzenia;

## Raportowanie

- Raporty dotyczące zapory firewall;
- Raporty głębokiej inspekcji (ataki);
- Raporty ekranowania (ataki);
- Raporty administracyjne;
- Eksport do HTML;
- Log Investigator umożliwiający korelowanie informacji zapisanych w logach;

## Bezpieczna komunikacja

- Bezpieczna komunikacja we wszystkich warstwach;
- Mechanizm komunikacji w oparciu o protokół TCP;
- Szyfrowanie: AES, 256 bitów;
- Uwierzytelnianie: SHA-1;

## Minimalne wymagania systemowe

|  |  |
|--|--|
| Interfejs użytkownika  |  |
| Obsługa systemów operacyjnych  | Microsoft Windows 2000, Windows NT, Windows XP             |
| Minimalny procesor Pentium II  | 400 MHz lub odpowiednik                                    |
| Minimalna ilość pamięci RAM  | 256 MB, zalecana 512 MB                                    |
| Minimalna ilość dostępnego miejsca na dysku                          | 100 MB   |
| Minimalna przepustowość łącza do serwera                             | 384kb/sek (DSL) lub LAN                                    |
| Serwer zarządzania (serwer GUI w połączeniu z serwerem urządzenia)   |  |
| Minimalna częstotliwość procesora                                    | 1 GHz*   |
| Minimalna ilość pamięci RAM  | 1 GB*  |
| Minimalne wymagania dotyczące twardego dysku:                        | 10K rpm i co najmniej 18GB                                 |
| wolnego miejsca (każdy zapis w logu to mniej więcej 100 bajtów)*     |  |
| Minimalna szybkość karty sieciowej                                   | 100 Mb/sek*  |
| Obsługa systemów operacyjnych  | Solaris 8, Solaris 9, Red Hat Linux 8.0, Red Hat Linux 9.0 |
| Maksymalna liczba zarządzanych urządzeń przypadająca na serwer: 1000 |  |

\*Urządzenia Global Pro lub Global Pro Express są również obsługiwane

## Obsługa urządzeń

|                                 |
|---------------------------------|
| Juniper Networks NetScreen-5XP  |
| Juniper Networks NetScreen-5XT  |
| Juniper Networks NetScreen-5GT  |
| Juniper Networks NetScreen-204  |
| Juniper Networks NetScreen-208  |
| Juniper Networks NetScreen-500  |
| Juniper Networks NetScreen-25   |
| Juniper Networks NetScreen-50   |
| Juniper Networks NetScreen-100  |
| Juniper Networks NetScreen-5200 |
| Juniper Networks NetScreen-5400 |

## Obsługa systemu operacyjnego NetScreen ScreenOS

|   |
|---|
| Juniper Networks ScreenOS 4.0.0                 |
| Juniper Networks ScreenOS 4.0.0 DIAL2           |
| Juniper Networks ScreenOS 4.0.1                 |
| Juniper Networks ScreenOS 4.0.3                 |
| Juniper Networks ScreenOS 5.0.0 i wersje nowsze |

## Informacje o zamówieniach

| Produkt  | Oznaczenie produktu |
|--|---------------------|
| Juniper Networks NetScreen-Security Manager, 10 urządzeń   | NS-SM-10            |
| Juniper Networks NetScreen-Security Manager, 25 urządzeń   | NS-SM-25            |
| Juniper Networks NetScreen-Security Manager, 50 urządzeń   | NS-SM-50            |
| Juniper Networks NetScreen-Security Manager, 100 urządzeń  | NS-SM-100           |
| Juniper Networks NetScreen-Security Manager, 200 urządzeń  | NS-SM-200           |
| Juniper Networks NetScreen-Security Manager, 500 urządzeń  | NS-SM-500           |
| Juniper Networks NetScreen-Security Manager, 1000 urządzeń | NS-SM-1000          |



1194 North Mathilda Avenue Sunnyvale, CA 94089 USA  
Phone: 888-JUNIPER (888-586-4737) or 408-745-2000  
Fax: 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 wersji: 110018-001 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: support@clico.pl  
www.clico.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