

# Juniper Networks NetScreen-SA Central Manager



## Uproszczona administracja

- Centralne zarządzanie urządzeniami NetScreen Secure Access SSL VPN firmy Juniper Networks;
- Wysoko wydajna i skalowalna architektura umożliwia elastyczne zarządzanie zmieniającą się w czasie infrastrukturą.

## Zoptymalizowana wydajność

- Statystyki czasu rzeczywistego systemu/klastr; a
- Automatyczne aktualizacje oprogramowania urządzeń;
- Kopie zapasowe i funkcje odtwarzania umożliwiające błyskawiczne przywracanie systemu po awarii.

## Zapewnienie spójnego obrazu polityki bezpieczeństwa

- Funkcje synchronizacji pozwalają na automatyzację propagacji zmian w obrębie klastra;
- Technologia „Push” eliminuje braki w przestrzeganiu polityki bezpieczeństwa poprzez wysyłanie informacji do innych bram lub klastrów.

## Wszystostronne raportowanie umożliwiające szybkie reagowanie

- Bogate możliwości filtrowania umożliwiające szybkie wyszukiwanie zdarzeń o kluczowym znaczeniu;
- Szczegółowe archiwai umożliwiające łatwe wykonywanie porównań.

Rodzina urządzeń NetScreen Secure Access firmy Juniper Networks konsekwentnie przewodzi na rynku urządzeń SSL VPN zapewniając bezpieczny dostęp mobilnym pracownikom, partnerom biznesowym oraz klientom. Wraz z rozwojem instalacji SSL VPN, zarówno w wymiarze wielkości użytkowanych klastrów, jak i ich zasięgu geograficznego, wzrastają potrzeby zapewnienia prostego i skutecznego nimi zarządzania. Firma Juniper Networks znacznie rozszerzyła swoje kompetencje na rynku urządzeń SSL VPN poprzez opracowanie oprogramowania NetScreen-SA Central Manager produktu o rozbudowanych możliwościach, wyposażonego w intuicyjny, graficzny, webowy interfejs użytkownika. Opracowany on został w celu ułatwienia zadań konfiguracji, uaktualniania i monitorowania urządzeń NetScreen Secure Access, zarówno w obrębie pojedynczego klastra urządzeń jak w globalnej instalacji złożonej z wielu klastrów. Dzięki umożliwieniu skalowalnej, scentralizowanej konfiguracji i konserwacji doskonałych urządzeń NetScreen Secure Access firmy Juniper Networks korporacje mogą korzystać z ich własności łatwiej i w sposób bardziej ekonomiczny.

## Wylimitowanie powtarzających się zadań administracyjnych w procesie zapewniania przestrzegania zasad polityki bezpieczeństwa

Jednym z podstawowych wymagań skutecznej polityki bezpieczeństwa jest jej jednolite wdrożenie w całej korporacji. „Ręczne” zarządzanie polityką bezpieczeństwa oraz jej czasochłonna replikacja zadania sprzyjające popełnianiu błędów mogą znacząco popsuć efekty zastosowania urządzeń bezpiecznego dostępu, niezależnie od tego, jak łatwe są we wdrożeniu. NetScreen SA-Central Manager ułatwia zachowanie spójnego przestrzegania polityki bezpieczeństwa dzięki zautomatyzowaniu wielu powtarzających się zadań. System doskonale sprawdza się jako pomoc w wykonywaniu zadań administracyjnych w korporacji rozbudowującej swoje instalacje SSL VPN na wielu rozproszonych użytkownikach. W systemie NetScreen SA-Central Manager zastosowano zaawansowane technicznie mechanizmy synchronizacji pomiędzy urządzeniami NetScreen Secure Access umożliwiające propagację reguł bezpiecznego dostępu, uwierzytelniania i autoryzacji użytkowników, a także konfiguracji urządzeń w obrębie klastra. System ten ułatwia także wykonywanie automatycznych uaktualnień oprogramowania, co pozwala na maksymalizację czasu dostępności systemu.

## Poprawienie wydajność infrastruktury dzięki sprawnemu planowaniu wykorzystania zasobów sieciowych

Przy użyciu systemu NetScreen-SA Central Manager administratorzy uzyskują dostęp do szczegółowych informacji dotyczących zajętości sieci i jej

wydajności. Za pośrednictwem graficznej konsoli użytkownika system umożliwia uzyskanie w czasie rzeczywistym informacji w postaci wykresów o wykorzystaniu zasobów sieciowych, ja również o innych metrykach systemowych. Dzięki temu administratorzy mogą zidentyfikować wzorce wykorzystania systemu i lepiej planować jego rozwój. Możliwość wykonania obrazu stanu systemu ułatwia archiwizację jego konfiguracji oraz umożliwia wgląd w jego historyczne stany.

## Wbudowany lokalny i globalny system odtwarzania po awarii

W przypadku awarii urządzeń NetScreen SA (która de facto jest mało prawdopodobna), system Central Manager, obok rozbudowanych możliwości odtwarzania konfiguracji samych urządzeń Secure Access, zapewnia dodatkową funkcjonalność. Funkcje tworzenia lokalnych kopii awaryjnych i odtwarzania dają administratorom możliwość zapisywania pełnej konfiguracji dla wszystkich urządzeń zarządzanych przez Central Manager lub tylko wybranego fragmentu. Dzięki temu, w przypadku awarii można szybko przywrócić pojedyncze urządzenie lub cały klaster do stanu pierwotnego. Ponadto możliwe jest śledzenie historii zmian konfiguracji oraz dostępu do urządzeń z uprawnieniami administratora. Funkcja deterministycznego odtwarzania klastra (Deterministic Cluster Recovery) optymalizuje żywotność systemu. Dzięki przypisaniu odpowiednich priorytetów do poszczególnych węzłów klastra administratorzy mogą zapewnić, że w klastrze obowiązuje najbardziej pożądana jego konfiguracja. W przypadku zakłóceń w komunikacji pomiędzy elementami składowymi klastra, po przywróceniu komunikacji węzeł o najwyższym priorytecie propaguje do pozostałych węzłów poprawny stan klastra.

## Kosztowo efektywna funkcjonalność centralnego zarządzania

NetScreen SA-Central Manager jest wdrażany jako aktualizacja oprogramowania w istniejących klastrach, a nie jako osobny serwer (taka architektura o wiele bardziej nadaje się do zastosowania w sieciach o dużej skali z wieloma klastrami). Również mało rozbudowane systemy mogą skorzystać z zalet centralnego zarządzania bez potrzeby dokonywania jakichkolwiek zmian w infrastrukturze. Central Manager działa jako nakładka na istniejącą aplikację zarządzania urządzeniami Secure Access (Administrator Console) dodając wiele nowych funkcji, które dostępne są poprzez znany, webowy interfejs użytkownika. Aplikacja NetScreen SA-Central Manager bezproblemowo integruje się z oprogramowaniem urządzeń Secure Access oraz Secure Meeting tworząc jedną z najbardziej rozbudowanych aplikacji zarządzających w segmencie urządzeń SSL VPN.

## 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