

Juniper Networks NetScreen-SA seria 1000



Urządzenia VPN SSL NetScreen Secure Access serii 1000 umożliwiają małym i średnim firmom wdrażanie proporcjonalnych do kosztów rozwiązań bezpiecznego zdalnego dostępu w ramach sieci ekstranet i intranet. Użytkownicy mogą uzyskać dostęp do sieci korporacyjnej i aplikacji z poziomu każdej standardowej przeglądarki WWW. W urządzeniach serii NetScreen-SA 1000 wykorzystuje się SSL – protokół zabezpieczeń, który niemal w każdej przeglądarce WWW spełnia rolę mechanizmu transportu z bezpiecznym dostępem. Wykorzystanie SSL eliminuje potrzebę instalowania oprogramowania klienckiego, modyfikacji wewnętrznych serwerów oraz kosztownych czynności konserwacyjnych. Urządzenia NetScreen Secure Access oferują również zaawansowane własności ekstranetu partner-klient, które zapewniają kontrolowany dostęp użytkownikom i grupom o zróżnicowanych prawach bez konieczności zmian w infrastrukturze, instalacji strefy DMZ i agentów programowych. Własność ta umożliwia firmom uzyskanie bezpiecznego dostępu do korporacyjnej sieci intranet. Dzięki temu administratorzy mogą ograniczyć dostęp do zasobów różnym pracownikom, zleceniobiorcom lub gościom, biorąc pod uwagę ich rzeczywiste potrzeby.

Urządzenia NetScreen-SA serii 1000 można zakupić z zestawem funkcji programowych Baseline (podstawowy) lub Advanced (zaawansowany). Oprogramowanie w wersji Baseline to własności najprostsze potrzebne firmom do wdrożenia rozwiązań bezpiecznego zdalnego dostępu, a także podstawowej sieci ekstranet klient-partner lub bezpiecznego intranetu. Produkty w wersji Advanced charakteryzują się dodatkowymi, zaawansowanymi własnościami, które pozwalają na sprostanie potrzebom bardziej złożonych instalacji, dla bardziej zróżnicowanych grup użytkowników oraz przypadków zastosowania.

Podsumowanie korzyści

Obniżenie całkowitego kosztu użytkowania

- Bezpieczny zdalny dostęp bez konieczności instalacji oprogramowania klienckiego lub modyfikacji serwerów oraz praktycznie brak konieczności konserwacji;
- Bezpieczny dostęp do sieci extranet bez konieczności tworzenia stref DMZ, wzmacniania serwera, dublowania zasobów lub dodatkowych instalacji w celu wprowadzenia nowych aplikacji lub użytkowników.

Bezpieczeństwo warstwowe „end-to-end”

- Różnorodne opcje zabezpieczeń od urządzenia użytkownika do danych aplikacyjnych i serwerów.

Bogate możliwości zarządzania prawami dostępu

- Dynamiczny, kontrolowany dostęp na poziomie URL, pliku, aplikacji i serwera na podstawie różnorodnych, specyficznych dla sesji zmiennych włącznie z identyfikatorem użytkownika, urządzenia, kontrolą zabezpieczeń i poziomem zaufania sieci.

Zabezpieczenie według celu

- Trzy różne metody dostępu umożliwiają administratorom dostosowanie poziomu bezpieczeństwa i dostępu dla użytkownika i sesji.

Wysoka dostępność

- Opcja instalacji par klastrów umożliwiająca wdrożenie funkcji wysokiej dostępności w sieciach LAN i WAN.

Uproszczone zarządzanie

- Opcje centralnego zarządzania umożliwiające zunifikowaną administrację;
- Własności samoobsługi użytkowników ulepszają produktywność, a jednocześnie obniżają koszty administracyjne.

Obniżenie całkowitego kosztu użytkowania

Urządzenia NetScreen-SA serii 1000 charakteryzują się bogactwem własności, które umożliwiają znaczne obniżenie całkowitego kosztu użytkowania w porównaniu z tradycyjnymi rozwiązaniami zdalnego dostępu lub dostępu do sieci ekstranet/intranet.

Własność	Korzyści
Wykorzystanie protokołu SSL dostępnego we wszystkich standardowych przeglądarkach WWW	Bezpieczny zdalny dostęp bez konieczności instalacji oprogramowania klienckiego i modyfikacji istniejących serwerów.
Oparte o standardowe protokoły metody zabezpieczeń	Korzyści z inwestycji w urządzenia NetScreen-SA serii 1000 można czerpać w wielu zastosowaniach i zasobach przez długi okres czasu.
Własności samoobsługi użytkownika	Własności, do których należą zintegrowane zarządzanie hasłami oraz pojedyncze logowanie (ang. Web Single Sign-On) zwiększają produktywność użytkowników, upraszczają administrację dużymi i zróżnicowanymi grupami użytkowników i obniżają koszty pomocy technicznej.
Obsługa wielu nazw <i>Zestaw własności programowych Advanced</i>	Możliwość instalowania kilku wirtualnych witryn WWW za pomocą pojedynczego urządzenia NetScreen-SA 1000 pozwala na uzyskanie oszczędności ponieważ nie trzeba ponosić kosztów dodatkowych serwerów. Nakłady związane z zarządzaniem są niższe, a użytkownik uzyskuje wrażenie, jakby odwoływał się do różnych serwerów ponieważ wprowadza różne adresy URL.
Interfejs użytkownika z możliwością dostosowania do indywidualnych potrzeb <i>Zestaw własności programowych Advanced</i>	Umożliwia tworzenie stron logowania dostosowanych do indywidualnych potrzeb. Indywidualny wygląd interfejsu dla specyficznych ról użytkowników, co podnosi ich komfort korzystania z aplikacji.

Bezpieczeństwo warstwowe „end-to-end”

Urządzenia NetScreen-SA serii 1000 zapewniają kompletne zabezpieczenia warstwowe „end-to-end” obejmujące końcowego klienta, urządzenia, dane i zabezpieczenia warstwowe serwera. Należą do nich:

Własność	Korzyści
Wbudowane sprawdzanie węzła zdalnego (Native Host Checker)	Dzięki sumom kontrolnym MD5 umożliwiającym sprawdzanie autentyczności aplikacji, komputery-klienty można sprawdzać na początku i w trakcie trwania sesji. W ten sposób można zweryfikować dopuszczalną postawę bezpieczeństwa sprawdzając rejestry dla predefiniowanych plików, procesów i portów.
Interfejs API funkcji sprawdzania węzła zdalnego (Host Checker API)	Utworzony we współpracy z najlepszymi producentami zabezpieczeń. Funkcje umożliwiają sprawdzenie czy włączono odpowiednie usługi zabezpieczeń zarówno w momencie logowania, jak w trakcie trwania sesji, co zabezpiecza zarówno sieć, jak jej użytkowników.
Wzmocnione urządzenie zabezpieczeń i serwer WWW	Wzmocniona infrastruktura bezpieczeństwa, dla której audyt przeprowadzili eksperci w dziedzinie zabezpieczeń (między innymi firma TruSecure). Skuteczne zabezpieczenie wewnętrznych zasobów i obniżenie całkowitego kosztu użytkownika dzięki zminimalizowaniu konieczności bieżącego instalowania uaktualnień serwerów.
Usługi zabezpieczeń wykorzystują filtrowanie pakietów i bezpieczny routing na poziomie jądra	Pewność, że próby nieautoryzowanych połączeń takich, jak zniekształcone pakiety lub ataki DoS zostaną odfiltrowane
Mechanizm zerowania pamięci podręcznej	Wszystkie pobierane pliki pośrednie i pliki tymczasowo instalowane w czasie logowania są usuwane w momencie wylogowania. W ten sposób uzyskuje się pewność, że po wylogowaniu nie pozostaną żadne dane.
Pułapki dla danych (Data Trap) i kontrola buforów	Uniemożliwienie opuszczenia sieci przez wrażliwe metadane (pliki cookie, nagłówki, formularze, itp.). Przekształcenie treści na taką postać, której buforowanie nie jest możliwe.

Możliwości zarządzania prawami dostępu

Urządzenia NetScreen-SA serii 1000 zawierają mechanizmy dynamicznego zarządzania prawami dostępu, które nie wymagają zmian w infrastrukturze, tworzenia kodu oraz wdrażania (konserwacji) oprogramowania. Dzięki temu instalacja i utrzymanie mechanizmów bezpiecznego zdalnego dostępu, a także bezpiecznych sieci extranet i intranet jest łatwiejsza.

Użytkownicy, którzy logują się do urządzenia NetScreen-SA 1000 przechodzą przez wstępną ocenę przed procesem uwierzytelniania, w wyniku czego są dynamicznie przydzielani do roli sesji, na którą składają się ustawienia sieci, urządzenia, tożsamości i polityki sesji. Dokładne przestrzeganie rygorów bezpieczeństwa dodatkowo zapewniają szczegółowe polityki autoryzacji dostępu do zasobów.

Własność	Korzyści
Hybrydowy model polityki w oparciu o role i zasoby	Możliwość dynamicznego definiowania praw dostępu pozwalająca na zapewnienie zgodności polityki bezpieczeństwa z dynamicznymi wymaganiami biznesowymi.
Wstępna ocena przed uwierzytelnianiem	Jeszcze przed zalogowaniem można sprawdzić takie atrybuty sieci i urządzenia, jak status funkcji sprawdzającej hosta (Host Checker), mechanizmu czyszczenia pamięci podręcznej (Cache Cleaner), źródłowy adres IP, typ przeglądarki oraz certyfikaty cyfrowe. Wyniki tego sprawdzenia można wykorzystać do podjęcia dynamicznych decyzji zmierzających do wymuszenia przestrzegania obowiązującej polityki.
Polityka dynamicznego uwierzytelniania	Wykorzystanie istniejących w korporacji usług katalogowych, PKI oraz mechanizmów silnego uwierzytelniania w celu ustanowienia dynamicznej polityki uwierzytelniania dla każdej sesji użytkownika.
Dynamiczne mapowanie ról	Połączenie atrybutów sieci, urządzenia i sesji w celu określenia jednego z trzech typów dostępu. W ten sposób administrator może tworzyć specyficzne konfiguracje dla każdej niepowtarzalnej sesji.
Autoryzacja zasobów	Umożliwia niezwykle szczegółową kontrolę dostępu na poziomie adresu URL, serwera lub pliku. W ten sposób można tworzyć politykę zabezpieczeń dla poszczególnych zasobów.
Szczegółowy audyt i rejestrowanie	Możliwość wykorzystania do celów bezpieczeństwa lub planowania wydajności przejrzystych i zrozumiałych wyników audytu i rejestrowania na poziomie użytkownika, zasobu lub zdarzenia.
Wyrażenia definiowane przez użytkownika <i>Zestaw własności oprogramowania Advanced</i>	Możliwość stosowania dynamicznych kombinacji atrybutów dla poszczególnych sesji na poziomie definiowania/mapowania reguł ról oraz definiowania polityki autoryzacji zasobów.
Pojedyncze logowanie – Uwierzytelnianie BASIC Auth i NTLM	Użytkownicy nie muszą utrzymywać i wprowadzać wielu zestawów danych identyfikacyjnych w aplikacjach webowych i firmy Microsoft.
Pojedyncze logowanie wykorzystanie formularzy oraz zmiennych nagłówka <i>Zestaw własności programowych Advanced</i>	Oprócz uwierzytelniania BASIC Auth oraz NTLM SSO, w zaawansowanym zestawie własności istnieje możliwość wprowadzania nazwy użytkownika, hasła i innych atrybutów zdefiniowanych przez użytkownika w formularzu uwierzytelniania innych produktów lub jako zmienne nagłówkowe. W ten sposób zwiększa się produktywność użytkownika i poprawia komfort jego pracy.

Zabezpieczenia według celu

Urządzenia NetScreen-SA serii 1000 zapewniają trzy różne metody dostępu. Metody te można zdefiniować jako część roli użytkownika. Dzięki temu administrator może zdefiniować odpowiedni rodzaj dostępu dla konkretnej sesji biorąc pod uwagę konto użytkownika, urządzenie oraz atrybuty sieci w połączeniu ze politykami zabezpieczeń obowiązującymi w firmie.

Własność	Korzyści
Dostęp webowy bez klienta (Clientless core Web access)	Dostęp do aplikacji webowych takich, jak złożone aplikacje JavaScript i aplety Javy wymagające połączenia do gniazdka, a także do standardowych aplikacji e-mailowych, plików oraz aplikacji dla usług telnet i SSH. Najłatwiejszy dostęp do aplikacji i zasobów umożliwiając stosowanie niezwykle dokładnych opcji kontroli zabezpieczeń.
Secure Application Manager (SAM)	Pobranie niewielkiego kodu Javy lub aplikacji umożliwia uzyskanie dostępu dla aplikacji klient-serwer za pomocą wyłącznie przeglądarki WWW.
Połączenie sieciowe (Network Connect)	Kompletne połączenie warstwy sieci realizowane za pomocą automatycznie pobieranej z poziomu przeglądarki WWW aplikacji, dla tych użytkowników, którzy tego potrzebują.

Wysoka dostępność

Urządzenia NetScreen-SA serii 1000 zawierają szereg własności zapewniających dostępność i nadmiarowość cechy wymagane do zagwarantowania dostępu do funkcji o kluczowym znaczeniu.

Własność	Korzyści
Monitorowanie stanów (Stateful peering)	Jednostki wchodzące w skład klastra synchronizują dane o stanie systemu, profilu użytkownika i sesji w ramach grupy urządzeń w klastrze zapewniając w ten sposób bezproblemowe wznowienie pracy w przypadku awarii przy minimalnym czasie niedostępności sieci i obniżeniu produktywności.
Klastry	Klastry zwielokrotniają skumulowaną przepustowość umożliwiając obsługę niespodziewanych skoków w ruchu a także aplikacji wymagających wielu zasobów. Można je wykorzystywać w trybie Aktywny-Pasywny lub Aktywny-Aktywny, a także w pojedynczym ośrodku lub pomiędzy kilkoma punktami POP (Point of Presence). Klastry można instalować w sieci LAN lub sieci WAN w zależności od liczby licencji użytkowników, co zapewnia skalowalność w przypadku rozszerzenia się bazy użytkowników.

Uproszczone zarządzanie i administracja

Urządzenia NetScreen-SA serii 1000 zawierają szereg własności dostępnych z centralnej konsoli zarządzania, których zastosowanie wymaga jedynie kliknięcia odpowiedniego przycisku. Korzyści te można rozszerzyć na urządzenia wewnątrz klastra poprzez zainstalowanie systemu NetScreen-SA Central Manager produktu o rozbudowanych możliwościach wyposażonego w intuicyjny, graficzny, webowy interfejs użytkownika opracowany w celu ułatwienia zadań konfiguracji, uaktualniania i monitorowania urządzeń NetScreen Secure Access zarówno w obrębie pojedynczego klastra jak w globalnej instalacji złożonej z wielu klastrów.

Własność	Korzyści
Central Manager	Bezproblemowe zarządzanie klastrami z poziomu zintegrowanej centralnej konsoli zarządzania, dzięki której administracja staje się wygodna i wydajna. System Central Manager umożliwia administratorom śledzenie metryk klastra, modyfikowanie konfiguracji i instalację uaktualnień oraz stanowi mechanizm awaryjnego odtwarzania dla urządzeń lokalnych oraz umieszczonych w klastrze.
Delegowanie na podstawie roli <i>Zestaw własności oprogramowania Advanced</i>	Szczegółowe delegowanie na podstawie roli pozwala zminimalizować niedobory personelu IT dzięki umożliwieniu administratorom delegowania kontroli nad różnymi wewnętrznymi i zewnętrznymi populacjami użytkowników do odpowiednich osób. W ten sposób można dobrać poziom kontroli do potrzeb geograficznych biznesowych i funkcjonalnych.
Łatwa edycja odwzorowań ról oraz polityki autoryzacji zasobów	Administratorzy mogą kopiować i wielokrotnie wykorzystywać istniejące polityki, co upraszcza proces konfigurowania złożonych polityk składających się z wielu zmiennych oraz administrację wieloma typami grup (ról).
Możliwość dostosowania danych audytu (logu) do indywidualnych potrzeb	Dzięki produktowi NetScreen-SA Central Manager dane logów można zestawiać w standardowych formatach takich, jak W3C lub WELF, a także przygotowywać jako dane wejściowe do pakietów przetwarzania raportów firm zewnętrznych.
SNMP	Ulepszone monitorowanie dzięki opartej na standardach integracji z systemami zarządzania firm zewnętrznymi.

Specyfikacje

Opcje aktualizacji

- Secure Application Manager
- Network Connect
- Klastry wysokiej dostępności
- Secure Meeting

Specyfikacje techniczne

- NetScreen-SA 1000 - obudowa
- Wymiary: Szer: 17,72"; Wys: 1,74"; Głęb: 19"
- (Szer: 45,00 cm; Wys: 4,41 cm; Głęb: 48,26 cm)
- Waga: 18,5lb 8,3916 (kg) typowo (bez kartonu)
- Materiał: blacha stalowa walcowana na zimno o grubości 18 gauge (0,048")
- Wentylatory: wypychające z 4 łożyskami kulkowymi plus 1 wentylator chłodzący procesor

Wyświetlacz

- Wyłącznik panelu przedniego
- Dioda LED zasilania

Porty

Sieciowe

- Dwa RJ-45: Ethernet
- 10/100 duplexowe lub półduplexowe (z autonegociacją)
- zgodne z IEEE 802.3

Konsola

- 1 9-stykowy szeregowy port konsoli

Zasilanie

- Napięcie wejściowe i prąd 90-264 VAC w pełnym zakresie
- 6A (RMS) - 115 VAC
- 3A (RMS) - 230 VAC
- Częstotliwość wejściowa 47 - 63 Hz
- Wydajność min 65% przy pełnym obciążeniu
- Natężenie uderzenia prądowego: maksymalnie 60 A dla 115 VAC
- Natężenie uderzenia prądowego: maksymalnie 90 A dla 230 VAC
- Moc wyjściowa 350 W
- 2 wentylatory z łożyskami kulkowymi wypychające
- Średni czas pomiędzy awariami dla zasilacza 100 000 godzin w temperaturze 25°C

Parametry środowiskowe

- Zakres temperatur pracy: 5°C do 30°C (41°F do 86°F)
- Krótkotrwała praca: 0°C do 50°C (32°F do 122°F)
- Przechowywanie: -30°C do 60°C (-22°F do 140°F)
- Wilgotność względna (praca): 20% do 80%
- Wilgotność względna (przechowywanie): 5% do 95%
- Wysokość: do 3 000 m (10 000 ft)
- Odporność na wstrząsy (praca): 2G przez 11ms
- Odporność na wstrząsy (przechowywanie): 30G przez 11ms

Certyfikaty bezpieczeństwa i emisji

- Bezpieczeństwo: CB do IEC 60950: 1999, 3 edycja; TUV GS EN60950: 2000; TUV C-US do UL60950: 2000; CAN/CSA-C22.2
- Nr 60950: 2000
- Emisja: FCC klasy B, VCCI klasy B, CE klasy B

Gwarancja

- 90 dni - możliwość przedłużenia w umowie pomocy technicznej



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: 110005-001 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