

# Seria PA-3000

Cechy i funkcje zapory nowej generacji serii PA-3000:

## MOŻLIWOŚĆ STAŁEJ KLASYFIKACJI WSZYSTKICH APLIKACJI NA WSZYSTKICH PORTACH ZA POMOCĄ SYGNATUR APP-ID™.

- Identyfikacja aplikacji niezależnie od portu z szyfrowaniem SSL lub SSH albo z zastosowaniem techniki unikowej.
- Uwzględnianie aplikacji, a nie portów na potrzeby wszelkich decyzji związanych z realizacją polityk zabezpieczeń, takich jak zezwalanie, odmowa, planowanie, inspekcja czy kształtowanie ruchu.
- Kategoryzowanie niezidentyfikowanych aplikacji na potrzeby kontroli polityk, badanie zagrożeń, tworzenie niestandardowych sygnatur App-ID lub przechwytywanie pakietów w celu doskonalenia programowania sygnatur App-ID.

## ROZSZERZENIE POLITYK ZABEZPIECZEŃ APLIKACJI DLA DOWOLNYCH UŻYTKOWNIKÓW W DOWOLNYM MIEJSCU ZA POMOCĄ FUNKCJI USER-ID™ ORAZ GLOBALPROTECT™.

- Integracja z usługami Active Directory, LDAP, eDirectory Citrix oraz usługami terminalowymi firmy Microsoft bez zastosowania agentów.
- Integracja z urządzeniami NAC, bezprzewodowymi urządzeniami 802.1X oraz innymi, niestandardowymi repozytoriami użytkowników z interfejsem XML API.
- Wdrażanie spójnych zasad na potrzeby użytkowników lokalnych i zdalnych korzystających z platform Microsoft Windows, Mac OS X, Linux, Android lub iOS.

## OCHRONA PRZED ZNANYMI I NIEZNANYMI ZAGROŻENIAMI ZA POMOCĄ FUNKCJI CONTENT-ID™ ORAZ WILDFIRE™.

- Blokowanie szerokiego zakresu znanych zagrożeń, takich jak programy wykorzystujące luki, złośliwe oprogramowanie i programy szpiegujące na wszystkich portach, niezależnie od zastosowanej techniki unikowej.
- Ograniczanie nieautoryzowanego transferu plików i danych poufnych oraz kontrola przeglądania stron niezwiązanych z pracą.
- Identyfikowanie nieznanego złośliwego oprogramowania, analizowanie ponad 100 rodzajów złośliwych zachowań, automatyczne tworzenie i dostarczanie pliku sygnatur w kolejnej dostępnej aktualizacji.



PA-3050



PA-3020

Zapora Palo Alto Networks™ serii PA-3000 składa się z dwóch wydajnych platform PA-3050 i PA-3020 przeznaczonych do wdrażania w systemach szybkich bram internetowych. Zapora serii PA-3000 zarządza przepływami ruchu sieciowego za pomocą specjalnych zasobów sprzętowych oraz pamięci przeznaczonych do obsługi sieci, zabezpieczeń, zapobiegania zagrożeniom i zarządzania.

Szybka płyta główna jest podzielona na moduły obsługi danych oraz sterowania, co zapewnia stały dostęp do funkcji zarządzania niezależnie od natężenia ruchu sieciowego. Zapora serii PA-3000 steruje system operacyjny PAN-OSTM z zaawansowanymi funkcjami zabezpieczeń, który zapewnia ochronę aplikacji dzięki funkcjom App-ID, User-ID, Content-ID, GlobalProtect oraz WildFire.

| WYDAJNOŚĆ I PRZEPUSTOWOŚĆ <sup>1</sup>                            | PA-3050  | PA-3020  |
|-------------------------------------------------------------------|----------|----------|
| Przeptywność zapory (z funkcją App-ID)                            | 4 Gb/s   | 2 Gb/s   |
| Przeptywność systemu zapobiegania zagrożeniom                     | 2 Gb/s   | 1 Gb/s   |
| Przeptywność sieci IPSec VPN                                      | 500 Mb/s | 500 Mb/s |
| Liczba nowych sesji na sekundę                                    | 50 000   | 50 000   |
| Maksymalna liczba sesji                                           | 500 000  | 250 000  |
| Liczba tuneli/interfejsów tuneli sieci VPN IPSec                  | 2000     | 1000     |
| Liczba jednoczesnych użytkowników funkcji GlobalProtect (VPN SSL) | 2000     | 1,000    |
| Liczba sesji odszyfrowywania SSL                                  | 15,360   | 7,936    |
| Liczba certyfikatów przychodzących SSL                            | 25       | 25       |
| Liczba routerów wirtualnych                                       | 10       | 10       |
| Liczba systemów wirtualnych (podst./maks.2)                       | 1/6      | 1/6      |
| Liczba stref zabezpieczeń                                         | 40       | 40       |
| Maksymalna liczba zasad                                           | 5000     | 2500     |

<sup>1</sup> Wydajność i przepustowość zmierzone w idealnych warunkach testowania w systemie PAN-OS 5.0.

<sup>2</sup> Dodanie systemów wirtualnych do liczby podstawowej wymaga zakupu osobnej licencji.

Pełny opis funkcji zapory nowej generacji serii PA-3000 znajduje się na stronie [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature)

**DANE TECHNICZNE SPRZĘTU****PORTY WE-WY**

- PA-3050, PA-3020: {12} gniazd 10/100/1000, {8} gigabitowe porty optyczne SFP

**ADMINISTRACYJNE PORTY WE-WY**

- {1} autonomiczny port administracyjny 10/100/1000, {2} porty o wysokiej dostępności 10/100/1000, {1} port konsoli RJ-45

**POJEMNOŚĆ DYSKÓW**

- 120 GB SSD

**ZASILANIE (ŚREDNI/MAKSYMALNY POBÓR MOCY)**

- 250 W (150/200)

**MAKS. BTU/H**

- 683

**NAPIĘCIE WEJŚCIOWE (CZĘSTOTLIWOŚĆ WEJŚCIOWA)**

- 100–240 V AC (50–60 Hz)

**MAKS. POBÓR PRĄDU**

- 2 A przy 100 V AC

**MONTAŻ W SZAFIE (WYMIARY)**

- standardowa szafa 1U, 19 cali (4,45 cm wys. x 42,5 cm gł. x 43,2 cm szer.)

**MASA (SAMO URZĄDZENIE/W OPAKOWANIU TRANSPORTOWYM)**

- 6,8 kg/9 kg

**BEZPIECZEŃSTWO**

- UL, CUL, CB

**INTERFERENCJA ELEKTROMAGNETYCZNA (EMI)**

- FCC klasa A, CE klasa A, VCCI klasa A, TUV

**CERTYFIKATY**

- ICSA

**ŚRODOWISKO**

- Temperatura pracy: od 0 do 50°C
- Temperatura podczas przechowywania: od -20 do 70°C

**URZĄDZENIA SIECIOWE****TRYBY INTERFEJSU:**

- L2, L3, Tap, połączenie wirtualne (tryb transparentny)

**ROUTING**

- Tryby: OSPF, RIP, BGP, adres statyczny
- Rozmiar tablicy przekazywania (liczba wpisów na urządzenie/VR): 5000/2500 (PA-3050), 2500/2500 (PA-3020)
- Routing oparty na politykach
- Protokół PPPoE (Point-to-Point Protocol over Ethernet)
- Duże ramki: maks. wielkość ramki 9210 bajtów
- Multicasting: PIM-SM, PIM-SSM, IGMP v1, v2 i v3

**WYSOKA DOSTĘPNOŚĆ**

- Tryby: aktywny/aktywny, aktywny/pasywny
- Wykrywanie usterek: monitorowanie ścieżek i interfejsów

**PRZYDZIELANIE ADRESÓW**

- Przydzielanie adresów do urządzeń: klient DHCP/PPPoE/adres statyczny
- Przydzielanie adresów do użytkowników: serwer DHCP/przełącznik DHCP/adres statyczny

**IPv6**

- L2, L3, Tap, połączenie wirtualne (tryb transparentny)
- Funkcje: App-ID, User-ID, Content-ID, WildFire i rozszyfrowywanie SSL

**WIRTUALNE SIECI LAN (VLAN)**

- Liczba znaczników 802.1q sieci VLAN na urządzenie/interfejs: 4094/4094
- Maks. liczba interfejsów: 2048 (PA-3050), 1024 (PA-3020)
- Zagregowane interfejsy (802.3ad)

**NAT/PAT**

- Maks. liczba polityk trybu NAT: 1000
- Maks. liczba polityk trybu NAT (DIPP): 200
- Liczba dynamicznych adresów IP i puła portów: 254
- Puła dynamicznych adresów IP: 16 234
- Tryby NAT: 1:1 NAT, n:n NAT, m:n NAT
- Nadsubskrypcja DIPP (unikatowe docelowe adresy IP przypadające na źródłowy port i adres IP): 2
- NAT64

**POŁĄCZENIE WIRTUALNE**

- Maks. liczba połączeń wirtualnych: 10
- Typy interfejsów przypisane do połączeń wirtualnych: fizyczne oraz podinterfejsy

**PRZEKAZYWANIE L2**

- Rozmiar tablicy ARP/urządzenie: 2500 (PA-3050), 1500 (PA-3020)
- Rozmiar tablicy MAC/urządzenie: 2500 (PA-3050), 1500 (PA-3020)
- Rozmiar tablicy sąsiednich adresów IPv6: 2500 (PA-3050), 1500 (PA-3020)

## BEZPIECZEŃSTWO

### ZAPORA

- Kontrola aplikacji, użytkowników i zawartości oparta na politykach
- Ochrona pofragmentowanych pakietów
- Ochrona przed skanowaniem rozpoznawczym
- Ochrona przed atakami typu odmowa usługi (DoS)/rozproszona odmowa usługi (DDoS)
- Odszyfrowywanie: SSL (połączenia przychodzące i wychodzące), SSH

### WILDFIRE

- Ukierunkowane identyfikowanie i analizowanie nieznanych plików pod względem ponad 100 rodzajów złośliwych zachowań
- Generowanie i automatyczne zapewnianie ochrony przed nowo wykrytym złośliwym oprogramowaniem za pomocą aktualizacji sygnatur
- Aktualizacja pliku sygnatur WildFire w czasie poniżej godziny, zintegrowane funkcje rejestrowania/raportowania; dostęp do interfejsu API funkcji WildFire, umożliwiającego przekazywanie w sposób automatyczny do 100 próbek oraz 250 zapytań raportów dziennie (wymagana subskrypcja)

### FILTROWANIE PLIKÓW I DANYCH

- Przesyłanie plików: dwukierunkowa kontrola ponad 60 typów plików
- Przesyłanie danych: dwukierunkowa kontrola nieautoryzowanych transferów numerów kart kredytowych i SNN
- Ochrona przed niepożądanym pobieraniem plików

### INTEGRACJA UŻYTKOWNIKÓW (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One i inne usługi katalogowe oparte na protokole LDAP
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- Interfejs API XML zapewniający integrację z niestandardowymi repozytoriami użytkowników

### SIEĆ VPN IPSEC (MIĘDZY LOKACJAMI)

- Wymiana kluczy: ręczna wymiana kluczy, IKE v1
- Szyfrowanie: 3DES, AES (128-bitowe, 192-bitowe, 256-bitowe)
- Uwierzytelnianie: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamiczne tworzenie tuneli sieci VPN (GlobalProtect)

### ZAPOBIEGANIE ZAGROŻENIOM (WYMAGANA SUBSKRYPCJA)

- Ochrona przed wykorzystywaniem luk w aplikacjach i systemie operacyjnym
- Ochrona antywirusowa oparta na przesyłaniu strumieniowym (także elementów wbudowanych w plikach HTML, Javascript, PDF oraz plikach skompresowanych), ochrona przed programami szpiegującymi i robakami

### FILTROWANIE ADRESÓW URL (WYMAGANA SUBSKRYPCJA)

- Wstępnie zdefiniowane i niestandardowe kategorie adresów URL
- Bufor urzędzenia na potrzeby obsługi ostatnio odwiedzanych adresów URL
- Kategorie adresów URL jako część kryteriów wyszukiwania zasad zabezpieczeń
- Informacje o czasie przeglądania

### JAKOŚĆ USŁUG (QOS)

- Oparte na politykach kształtowanie ruchu dla aplikacji, użytkowników, źródeł, elementów docelowych, interfejsów, tuneli sieci VPN IPsec i innych elementów
- 8 klas ruchu z gwarantowanymi, maksymalnymi i priorytetowymi parametrami przepustowości
- Monitorowanie przepustowości w czasie rzeczywistym
- Oznaczanie na potrzeby architektury DiffServ wg polityk
- Liczba interfejsów fizycznych dla funkcji QoS: 6

### SIEĆ VPN SSL/DOSTĘP ZDALNY (GLOBALPROTECT)

- Brama GlobalProtect
- Portal GlobalProtect
- Transport: IPsec z szyfrowaniem SSL
- Uwierzytelnianie: LDAP, SecurID lub lokalna baza danych
- System operacyjny klienta: Mac OS X 10.6, 10.7 (32-/64-bitowy), 10.8 (32-/64-bitowy), Windows XP, Windows Vista (32-/64-bitowy), Windows 7 (32-/64-bitowy)
- Obsługa klientów innych firm: Apple iOS, Android 4.0 lub nowszy, VPNC IPsec dla systemu Linux

### NARZĘDZIA DO ZARZĄDZANIA, RAPORTOWANIA I INSPEKCJI

- Zintegrowany interfejs graficzny, wiersza poleceń (CLI) i centralne zarządzanie (Panorama)
- Wielojęzyczny interfejs użytkownika
- Narzędzia Syslog, Netflow v9 i SNMP v2/v3
- Interfejs API w architekturze REST oparty na kodzie XML
- Graficzne podsumowanie aplikacji, kategorii adresów URL, zagrożeń i danych (ACC)
- Wyświetlanie, filtrowanie i eksportowanie dzienników ruchu, zagrożeń, funkcji WildFire, adresów URL i filtrowania danych
- Raporty w pełni dostosowywane do potrzeb użytkownika

Pełny opis funkcji zapory nowej generacji serii PA-3000 znajduje się na stronie [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature).