Seria PA-5000

Cechy i funkcje zapory nowej generacji serii PA-5000:

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, analiza zagrożeń, tworzenie niestandardowych reguł App-ID lub przechwytywanie pakietów do dalszych badań.

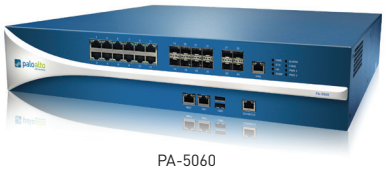
ROZSZERZENIE POLITYK ZABEZPIECZEŃ APLIKACJI DLA DOWOLNYCH UŻYTKOWNIKÓW W DOWOLNYM MIEJSCU ZA POMOCĄ FUNKCJI USER-ID™ ORAZ GLOBALPROTECT™.

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

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 nad przeglądaniem stron niezwiązanych z pracą.
- Identyfikowanie nieznanego złośliwego oprogramowania, analizowanie ponad 100 rodzajów złośliwych zachowań, automatyczne tworzenie i dostarczanie zabezpieczeń w kolejnej dostępnej aktualizacji.

paloalto NETWORKS
the network security company™



PA-5060

PA-5050

PA-5020

Zapora Palo Alto Networks™ serii PA-5000 składa się z trzech wydajnych modeli PA-5060, PA-5050 i PA-5020 przeznaczonych do wdrażania w systemach szybkich centrów danych i bram internetowych.

Zapora serii PA-5000 zapewnia maksymalnie 20 Gb/s przepływności dzięki specjalnym zasobom sprzętowym oraz pamięciom przeznaczonym do obsługi sieci, zabezpieczeń, zapobiegania zagrożeniom i zarządzania. Pozwala to na stały dostęp do funkcji zarządzania niezależnie od natężenia ruchu sieciowego, a moduły obsługi danych oraz sterowania są fizycznie podzielone. Zaporą serii PA-5000 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[1]	PA-5060	PA-5050	PA-5020
Przepływność zapory (z funkcją App-ID)	20 Gb/s	10 Gb/s	5 Gb/s
Przepływność systemu zapobiegania zagrożeniom	10 Gb/s	5 Gb/s	2 Gb/s
Przepływność sieci IPSec VPN	4 Gb/s	4 Gb/s	2 Gb/s
Maksymalna liczba sesji	4 000 000	2 000 000	1 000 000
Liczba nowych sesji na sekundę	120 000	120 000	120 000
Liczba tuneli/interfejsów tuneli sieci VPN IPSec	8000	4000	2000
Liczba jednoczesnych użytkowników funkcji GlobalProtect (VPN SSL)	20 000	10 000	5000
Liczba sesji odszyfrowywania SSL	90 000	45 000	15 000
Liczba certyfikatów przychodzących SSL	1000	300	100
Liczba routerów wirtualnych	225	125	20
Liczba systemów wirtualnych (podst./maks.2)	25/225*	25/125*	10/20*
Liczba stref zabezpieczeń	900	500	80
Maksymalna liczba zasad	40 000	20 000	10 000

[1] Wydajność i przepustowość zmierzone w idealnych warunkach testowania w systemie PAN-OS 5.0.

[2] Dodanie systemów wirtualnych do liczby podstawowej wymaga zakupu osobnej licencji.

Pełny opis funkcji zapory nowej generacji serii PA-5000 znajduje się na stronie visit www.paloaltonetworks.com/literature.

DANE TECHNICZNE SPRZĘTU

PORTY WE-WY

- PA-5060, PA-5050: (12) gniazd 10/100/1000, (8) gigabitowych portów optycznych SFP, (4) 10-gigabitowych portów optycznych +
- PA-5020: (12) gniazd 10/100/1000, (8) gigabitowych portów optycznych SFP

ADMINISTRACYJNE PORTY WE-WY

- (2) porty o wysokiej dostępności 10/100/1000, (1) port do zarządzania pozapasmowego 10/100/1000, (1) port konsoli RJ45

OPCJE PAMIĘCI MASOWEJS

- pojedynczy lub podwójny dysk SSD

POJEMNOŚĆ DYSKÓW

- 120 GB, 240 GB SSD, RAID 1

ZASILANIE (ŚREDNI/MAKSYMALNY POBÓR MOCY)

- PA-5060: nadmiarowy 450 W AC (330 W/415 W)
- PA-5050, PA-5020: nadmiarowy 450 W AC (270 W/340 W)

MAKS. BTU/H

- PA-5060: 1,416
- PA-5050, PA-5020: 1,160

NAPIĘCIE WEJŚCIOWE (CZĘSTOTLIWOŚĆ WEJŚCIOWA)

- 100–240 V AC (50–60 Hz), od -40 do -72 V DC

MAKS. POBÓR PRĄDU

- 8 A przy 100 V AC, 14 A przy 48 V DC

MAKS. POCZĄTKOWY PRĄD ROZRUCHOWY

- 80 A przy 230 V AC; 40 A przy 120 V AC; 40 A przy 48 V DC

ŚREDNI CZAS MIĘDZY AWARIAMI (MTBF)

- 6,5 roku

MONTAŻ W SZAFIE (WYMIARY)

- standardowa szafa 1U, 19 cali (8,9 cm wys. x 53,3 cm gł. x 44,5 cm szer.)

MASA (SAMO URZĄDZENIE/W OPAKOWANIU TRANSPORTOWYM)

- 18,6 kg/25 kg

BEZPIECZEŃSTWO

- UL, CUL, CB

INTERFERENCJA ELEKTROMAGNETYCZNA (EMI)

- FCC — klasa A, CE — klasa A, VCCI — klasa A

CERTYFIKATY

- NEBS Level 3, Common Criteria EAL2, FIPS level 2, ICSA, UCAPL

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): 64,000/64,000
- 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/przekaźnik 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: 4,094/4,094
- Maks. liczba interfejsów: 4 096 (PA-5060, PA-5050), 2 048 (PA-5020)
- Zagregowane interfejsy (802.3ad)

NAT/PAT

- Maks. liczba polityk trybu NAT: 8000 (PA-5060), 4000 (PA-5050), 1000 (PA-5020)
- Maks. liczba polityk trybu NAT (DIPP): 450 (PA-5060), 250 (PA-5050), 200 (PA-5020)
- Liczba dynamicznych adresów IP i pula portów: 254
- Pula dynamicznych adresów IP: 32 000
- Tryby NAT: 1:1 NAT, n:n NAT, m:n NAT
- Nadsubskrypcja DIPP (unikatowe docelowe adresy IP przypadające na źródłowy port i adres IP): 8 (PA-5060, PA-5050), 4 (PA-5020)
- NAT64

POŁĄCZENIE WIRTUALNE

- Maks. liczba połączeń wirtualnych: 12
- Typy interfejsów przypisane do połączeń wirtualnych: fizyczne oraz podinterfejsy

PRZEKAZYWANIE L2

- Rozmiar tablicy ARP/urządzenie: 32 000 (PA-5060, PA-5050), 20 000 (PA-5020)
- Rozmiar tablicy MAC/urządzenie: 32 000 (PA-5060, PA-5050), 20 000 (PA-5020)
- Rozmiar tablicy sąsiednich adresów IPv6: 5000 (PA-5060, PA-5050), 2000 (PA-5020)

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 nowo wykrytych złośliwych programów dzięki aktualizacjom pliku 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 urządzenia 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: 12

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-5000 znajduje się na stronie www.paloaltonetworks.com/literature.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com