

Seria PA-4000

Seria PA-4000 obejmuje urządzenia, które zapewniają bezprecedensową przejrzystość oraz kontrolę aplikacji, użytkowników oraz zawartości w sieciach przedsiębiorstw.

IDENTYFIKACJA APLIKACJI:

- Identyfikuje ponad 950 aplikacji, bez względu na port, protokół, szyfrowanie SSL lub mechanizmy unikania identyfikacji.
- Umożliwia efektywne egzekwowanie polityk dotyczących użytkownika aplikacji: akceptuj, blokuj, zaplanuj, skontroluj, zastosuj mechanizmy kształtowania pasma dla ruchu sieciowego.
- Narzędzia graficznego przedstawiania ruchu sieciowego zapewniają prosty podgląd aplikacji wykorzystywanych w sieci.

IDENTYFIKACJA UŻYTKOWNIKA:

- Bazująca na politykach kontrola nad tym, kto korzysta z aplikacji dzięki płynnej integracji z Active Directory, LDAP oraz eDirectory.
- Identyfikuje użytkowników usług terminalowych Citrix oraz Microsoft Terminal Services, zapewniając tym samym przejrzystość i kontrolę użytkowanych przez nich aplikacji.
- Kontrola hostów pracujących na systemach innych niż Windows, dzięki zastosowaniu uwierzytelniania webowego.

IDENTYFIKACJA ZAWARTOŚCI:

- Blokowanie wirusów, oprogramowania typu spyware oraz exploit, limitowanie nieautoryzowanego transferu plików oraz poufnych danych takich jak numery kart kredytowych oraz kontrola aktywności Web niezwiązanej z pracą.
- Architektura oprogramowania typu „pojedyncze skanowanie” umożliwia uzyskanie wielo-gigabitowej przepustowości z zachowaniem niewielkich opóźnień przy jednoczesnym funkcjonowaniu skanowania zawartości.



Seria Palo Alto Networks™ PA-4000 składa się z trzech platform o wysokiej wydajności: PA-4020, PA-4050 oraz PA-4060. Wszystkie przeznaczone są do zastosowań w środowiskach internetowych na poziomie bramy dostępowej w sieciach o dużej prędkości oraz w centrach danych. Seria PA-4000 zarządza przepływem ruchu sieciowego o przepustowości wielu gigabitów, wykorzystując do tego dedykowane zasoby pamięci oraz przetwarzania danych, odpowiedzialne za usługi sieciowe, usługi bezpieczeństwa, usługi ochrony przed zagrożeniami oraz usługi zarządzania.

10 Gb/s w architekturze typu backplane zapewnia płynne połączenie pomiędzy dedykowanymi procesorami, jak również oddziela funkcje przetwarzania danych od funkcji zarządzających. Dzięki temu zapewniony jest stały dostęp do narzędzi zarządzania, bez względu na natężenie ruchu sieciowego. Modele PA-4050 oraz PA-4020 posiadają 24 interfejsy, natomiast PA-4060 obsługuje interfejsy 10Gb/s. Wszystkie platformy serii PA-4000 wykorzystują dedykowane interfejsy do synchronizacji w ramach klastra HA oraz zarządzania.

Komponentem zarządzającym w urządzeniach firewall serii PA-4000 jest PAN-OSTM, system operacyjny skoncentrowany na funkcjach bezpieczeństwa, który zapewnia ścisłą integrację pomiędzy trzema unikalnymi technologiami identyfikacji zagrożeń: App-ID™, User-ID oraz Content-ID z kluczowymi funkcjami firewall, funkcjami sieciowymi oraz zarządzania.

KLUCZOWE PARAMETRY WYDAJNOŚCIOWE

	PA-4020	PA-4050	PA-4060
Przepustowość firewall	2Gb/s	10Gb/s	10Gb/s
Przepustowość systemu zapobiegania zagrożeniom	2Gb/s	5Gb/s	5Gb/s
Przepustowość IPSec VPN	1Gb/s	2Gb/s	2Gb/s
Tunele/interfejsy IPSec VPN	2000	4000	4000
Liczba równoczesnych użytkowników SSL VPN	5000	10000	10000
Liczba nowych sesji na sekundę	60000	60000	60000
Maksymalna liczba sesji	500000	2000000	2000000

Szczegółowa specyfikacja właściwości serii PA-4000 znajduje się na www.paloaltonetworks.com/literature

Specyfikacja i funkcje dodatkowe serii PA-4000

APP-ID

- Identyfikacja i kontrola ponad 950 aplikacji
- Deszyfrowanie SSL (dla ruchu wchodzącego i wychodzącego)
- Edytowalne właściwości aplikacji
- Własne aplikacje HTTP i SSL

FIREWALL

- Bazująca na politykach kontrola dostępu na podstawie aplikacji, kategorii aplikacji, podkategorii, technologii, czynnika ryzyka lub charakterystyki
- Kontrola funkcji aplikacji
- Ochrona pofragmentowanych pakietów
- Ochrona z zastosowaniem skanowania rozpoznawczego
- Ochrona przed atakami Denial of Service (DoS)/Distributed Denial of Service (DDoS)
- Maksymalna liczba polityk: (PA-4020) 10,000 (PA-4050) 20,000, (PA-4060)

USER – ID

- Kontrola na podstawie użytkownika, grupy oraz adresu IP
- Active Directory, LDAP, eDirectory, Citrix oraz Microsoft Terminal Services
- XML API (integracja z zewnętrznymi repozytoriami użytkowników)
- Funkcje WMI i NetBios polling
- Maksymalna liczba równoczesnych instancji mapowanych użytkowników/IP: 64000

FILTROWANIE DANYCH

- Kontrola nieautoryzowanego transferu danych (numerów NIP, numerów kart kredytowych, danych zgodnych ze zdefiniowanym wzorcem)
- Kontrola nieautoryzowanego transferu ponad 50 typów plików

FILTROWANIE URL (WYMAGA SUBSKRYPCJI)

- 76 kategorii, zintegrowana baza danych zawierająca 20 milionów URLi
- Edytowalna baza cache o pojemności 1 miliona URLi (na podstawie bazy danych zawierającej 180 milionów URLi)
- Edytowalne strony blokujące oraz kategorie URL

IPSEC VPN (SITE-TO-SITE)

- Klucz manualny, IKE v1
- Szyfrowanie 3DES, AES (128 bitów, 192 bity, 256 bitów)
- Uwierzytelnianie SHA1, MD5

SSL VPN (DOSTĘP ZDALNY)

- Transport IPSec z funkcją SSL fall-back
- Egzekwowanie polityk dedykowanych ruchowi SSL VPN
- Włączanie/wyłączanie rozdzielnego tunelowania w celu kontroli dostępu klienta
- Uwierzytelnianie LDAP, SecurID lub lokalnych DB
- System operacyjny klienta: Windows XP, Windows Vista (32 oraz 64 bity), Windows 7 (32 oraz 64 bity)

WYSOKA DOSTĘPNOŚĆ

- Mechanizm failover typu active/passive
- Synchronizacja konfiguracji i sesji
- Sprawdzanie „heartbeat”
- Monitorowanie łącza i trasy w poszukiwaniu anomalii

FUNKCJE SIECIOWE

- Ruting dynamiczny (BGP, OSPF oraz RIPv2)
- Tryb „tap”, virtual wire, warstwa 2, warstwa 3
- Network address translation (NAT)
 - Translacja adresu wyjściowego i docelowego
 - Pula dynamicznych adresów IP i portów: 254
 - Pula dynamicznych adresów IP: 16234
- Serwer DHCP/DHCP relay: do 3 serwerów
- Obsługa 802.1Q VLAN 4,094
- Przesył bazujący na politykach
- Agregacja łączy 802.3ad
- Protokół Point-to-Point Protocol over Ethernet (PPPoE)
- Rozpoznawanie aplikacji IPv6, kontrola i pełny wgląd w zawartość (tylko dla trybu virtual wire)
- Ramki Jumbo
- Rutery wirtualne: (PA-4020) 20, (PA-4050) 125, (PA-4060) 125
- Strefy bezpieczeństwa: (PA-4020) 80, (PA-4050) 500, (PA-4060) 500
- Systemy wirtualne (bazowo/maksymalnie): (PA-4020) 10/20*, (PA-4050) 25/125*, (PA-4060) 25/125*

SYSTEM ZAPOBIEGANIA ZAGROŻENIOM (WYMAGA SUBSKRYPCJI)

- Wykrywanie i blokowanie prób wykorzystania słabych punktów aplikacji (system IPS)
- Strumieniowa ochrona przed wirusami, oprogramowaniem spyware oraz robakami
- Ochrona antywirusowa HTML/Javascript
- Kontrola skompresowanych plików wykorzystujących algorytmy Zip, Gzip itd.
- Sygnatury zagrożeń oraz antyspyware
- Aktualizacje zawartości: codziennie (malware), tygodniowo (sygnatury zagrożeń), w sytuacji awaryjnej (wszystkie komponenty)

QUALITY OF SERVICE (QOS)

- Bazujące na politykach kształtowanie pasma dla ruchu sieciowego na podstawie aplikacji, użytkownika, źródła, punktu docelowego, interfejsu, tunelu IPSec VPN i innych
- 8 klas ruchu sieciowego z parametrami dla gwarantowanej, maksymalnej i priorytetowej przepustowości
- Monitorowanie przepustowości w czasie rzeczywistym
- Znaczniki diffserv dla każdej polityki

NARZĘDZIA ZARZĄDZANIA

- Zintegrowany interfejs webowy
- Interfejs wiersza poleceń (CLI)
- Administracja na podstawie ról
- Narzędzia Syslog i SNMPv2
- Edytowalna formatka logowania administratora
- Architektura REST API bazująca na XML
- Scentralizowane zarządzanie (Panorama)
- Centralnie zarządzane aktualizacje systemu PAN-OS oraz zawartości (Panorama)
- Współdzielone polityki (Panorama)

NARZĘDZIA ZAPEWNIĄCE PRZEJRZYŚĆ I RAPORTOWANIE

- Graficzne podsumowanie aplikacji, kategorii URL, zagrożeń oraz danych (ACC)
- Przegląd, filtrowanie oraz eksportowanie logów ruchu sieciowego, zagrożeń, URL oraz filtrowania danych
- W pełni edytowalne raportowanie
- Narzędzia śledzenia sesji

* Dodawanie systemów wirtualnych do ilości bazowej wymaga wykupienia osobnej licencji.

SPECYFIKACJA SPRZĘTOWA

	PA-4060	PA-4050/ PA-4020
Porty wejścia/wyjścia	(4) 10 Gigabit XFP + (4) Gigabit SFP	(16) 10/100/1000 + (8) Gigabit SFP
Porty zarządzania	(2) 10/100/1000 wysoka dostępność, (1) 10/100/1000 zarządzanie poza pasmem, (1) DB9 port konsoli	(2) 10/100/1000 wysoka dostępność, (1) 10/100/1000 zarządzanie poza pasmem, (1) DB9 port konsoli
Zasilanie (średnie/maksymalne zużycie mocy)	Redundantne 400W AC (175W/200W)	
Napięcie wejściowe (częstotliwość wejściowa)	100-240Vac (50-60Hz)	
Współczynnik mocy	0.93 do 0.95 (PA-4060, PA-4050, PA-4020)	
Maksymalne parametry prądu wejściowego	50A@230Vac; 30A@120Vac	
Parametry montażu w racku (wymiar)	2U, standardowy rack 19-calowy (3.5"W x 16.5"G x 17.5"SZ)	
Bezpieczeństwo	UL, CUL, CB	
EMI	FCC Class A, CE Class A, VCCI Class A, TUV	
MTBF	7,18 lata (PA-4060, PA-4050, PA-4020)	

PARAMETRY ŚRODOWISKOWE

Temperatura w trakcie pracy	0° to 50° C, 32° to 122° F
Temperatura przechowywania	-20° to 70° C, -4° do 158° F

INFORMACJE DOTYCZĄCE ZAMÓWIEŃ

	PA-4060	PA-4050	PA-4020
Platforma	PAN-PA-4060	PAN-PA-4050	PAN-PA-4020
Roczna subskrypcja systemu zapobiegania zagrożeniom	PAN-PA-4060-TP	PAN-PA-4050-TP	PAN-PA-4020-TP
Roczna subskrypcja filtrowania URL	PAN-PA-4060-URL2	PAN-PA-4050-URL2	PAN-PA-4020-URL2
Rozszerzenie systemów wirtualnych (10 dodatkowych)	---	---	PAN-PA-4020-VSYS-10
Rozszerzenie systemów wirtualnych (50 dodatkowych)	PAN-PA-4060-VSYS-50	PAN-PA-4050-VSYS-50	---
Rozszerzenie systemów wirtualnych (100 dodatkowych)	PAN-PA-4060-VSYS-100	PAN-PA-4050-VSYS-100	---

Dodatkowe informacje dotyczące właściwości oprogramowania serii PA-2000 znajdują się na stronie www.paloaltonetworks.com/literature.

