

PA-500

Cechy i funkcje zapory nowej generacji PA-500:

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-500

Zapora Palo Alto Networks™ PA-500 jest przeznaczona do szybkiego wdrażania w korporacyjnym środowisku z rozproszonymi oddziałami oraz w średnich przedsiębiorstwach. Zapora PA-500 zarządza przepływami ruchu sieciowego za pomocą specjalnych zasobów sprzętowych 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. Zaporą nowej generacji PA-500 steruje system operacyjny PAN-OS™ z zaawansowanymi funkcjami zabezpieczeń, który zapewnia ochronę aplikacji dzięki funkcjom App-ID, User-ID, Content-ID, GlobalProtect oraz WildFire.

WYDAJNOŚĆ I PRZEPUSTOWOŚĆ¹

PA-500

Przepływność zapory (z funkcją App-ID)	250 Mb/s
Przepływność systemu zapobiegania zagrożeniom	100 Mb/s
Przepływność sieci IPSec VPN	50 Mb/s
Liczba nowych sesji na sekundę	7500
Maksymalna liczba sesji	64 000
Liczba tuneli/interfejsów tuneli sieci VPN IPSec	250
Liczba jednoczesnych użytkowników funkcji GlobalProtect (VPN SSL)	100
Liczba sesji odszyfrowywania SSL	1000
Liczba certyfikatów przychodzących SSL	25
Liczba routerów wirtualnych	3
Liczba stref zabezpieczeń	20
Maksymalna liczba zasad	1000

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

Pełny opis funkcji zapory nowej generacji PA-500 znajduje się na stronie www.paloaltonetworks.com/literature.

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

- (8) 10/100/1000

ADMINISTRACYJNE PORTY WE-WY

- (1) autonomiczny port administracyjny 10/100/1000
- (1) port konsoli RJ-45

POJEMNOŚĆ DYSKÓW

- dysk twardy 160 GB

ZASILANIE (ŚREDNI/MAKSYMALNY POBÓR MOCY)

- 180 W (40 W/75 W)

MAKS. BTU/H

- 256

NAPIĘCIE WEJŚCIOWE (CZĘSTOTLIWOŚĆ WEJŚCIOWA)

- 100–240 V AC (50–60 Hz)

MAKS. POBÓR PRĄDU

- 1 A przy 100 V AC

ŚREDNI CZAS MIĘDZY AWARIAMI (MTBF)

- 10,16 roku

MAKS. POCZĄTKOWY PRĄD ROZRUCHOWY

- 110 A przy 230 V AC; 51 A przy 115 V AC

MONTAŻ W SZAFIE (WYMIARY)

- standardowa szafa 1U, 19 cali
- [4,45 cm wys. x 25,4 cm gł. x 43,2 cm szer.]

MASA (SAMO URZĄDZENIE/W OPAKOWANIU TRANSPORTOWYM)

- 3,6 kg/5,9 kg

BEZPIECZEŃSTWO

- UL, CUL, CB

INTERFERENCJA ELEKTROMAGNETYCZNA (EMI)

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

CERTYFIKATY

- FIPS 140 Level 2, Common Criteria EAL2, 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): 1250/1250
- Routing oparty na politykach
- Protokół PPPoE (Point-to-Point Protocol over Ethernet)
- 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: 4,094/4,094
- Maks. liczba interfejsów: 250
- Zagregowane interfejsy (802.3ad)

NAT/PAT

- Maks. liczba polityk trybu NAT: 125
- Maks. liczba polityk trybu NAT (DIPP): 125
- Liczba dynamicznych adresów IP i pula portów: 254
- Pula 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): 1
- NAT64

POŁĄCZENIE WIRTUALNE

- Maks. liczba połączeń wirtualnych: 125
- Typy interfejsów przypisane do połączeń wirtualnych: fizyczne oraz podinterfejsy

PRZEKAZYWANIE L2

- Rozmiar tablicy ARP/urządzenie: 500
- Rozmiar tablicy MAC/urządzenie: 500
- Rozmiar tablicy sąsiednich adresów IPv6: 500

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 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: 4

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 PA-500 znajduje się na stronie www.paloaltonetworks.com/literature.