

PA-500

PA-500 to firewall nowej generacji, który zapewnia bezprecedensową przejrzystość i 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 i intuicyjny podgląd aplikacji wykorzystywanych w sieci.

IDENTYFIKACJA UŻYTKOWNIKA:

- Bazująca na politykach kontrola nad tym, kto korzysta z aplikacji dzięki integracji z Active Directory, LDAP oraz eDirectory.
- Identyfikuje użytkowników usług terminalowych Citrix oraz Microsoft Terminal Services, zapewniając tym samym 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 oraz przy jednoczesnym funkcjonowaniu skanowania zawartości.



PA-500

Firewall Palo Alto Networks PA-500 przeznaczony jest do zastosowań w środowiskach internetowych na poziomie bramy dostępowej w sieciach o dużej prędkości w oddziałach przedsiębiorstw oraz firmach średniej wielkości. PA-500 zarządza przepływem ruchu sieciowego, wykorzystując do tego dedykowane zasoby odpowiedzialne za usługi sieciowe, usługi bezpieczeństwa, usługi ochrony przed zagrożeniami oraz usługi zarządzania.

Architektura typu backplane zapewnia płynne połączenie pomiędzy 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. Interfejsy dostępne w PA-500 obejmują osiem portów 10/100/1000 ruchu sieciowego oraz dedykowany port zarządzania.

Komponentem zarządzającym w urządzeniach firewall serii PA-500 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-500

Przepustowość firewall	250Mb/s
Przepustowość systemu zapobiegania zagrożeniom	100Mb/s
Przepustowość IPSec VPN	50Mb/s
Tunele/interfejsy IPSec VPN	250
Liczba równoczesnych użytkowników SSL VPN	100
Liczba nowych sesji na sekundę	7 500
Maksymalna liczba sesji	64 000

Szczegółowa specyfikacja platformy firewall następnej generacji PA-500 znajduje się na www.paloaltonetworks.com/literature.

Specyfikacja i funkcje dodatkowe PA-500

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: 1000

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 ubezpieczenia społecznego, 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-bit, 192-bit, 256-bit)
- 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 OS: 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
- Protokół Point-to-Point Protocol over Ethernet (PPPoE)
- Rozpoznawanie aplikacji IPv6, kontrola i pełny wgląd w zawartość (tylko dla trybu virtual wire)
- Strefy bezpieczeństwa: 20
- Rutery wirtualne: 3

SYSTEM ZAPOBIEGANIA ZAGROŻENIOM (WYMAGA SUBSKRYPCJI)

- Wykrywanie i blokowanie prób wykorzystania słabych punktów aplikacji (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 ZAPEWNIAJĄCE 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

SPECYFIKACJA SPRZĘTOWA**PA-500**

Porty wejścia/wyjścia	(8) 10/100/1000
Port zarządzania	(1) 10/100/1000 port zarządzania „poza pasmem”, (1) port konsoli RJ-45
Zasilanie (średnie/maksymalne zużycie mocy)	180W (10W/75W)
Napięcie wejściowe (częstotliwość wejściowa)	100-240Vac (50-60Hz)
Współczynnik mocy	0.997 do 0978
Maksymalne parametry prądu wejściowego	110A@230Vac; 1A@115Vac
Parametry montażu w racku (wymiar)	1U, standardowy rack 19-calowy (1.75"W x 17"G x 17"SZ)
Bezpieczeństwo	UL, CUL, CB
EMI	FCC Class A, CE Class A, VCCI Class A, TUV
MTBF	10,16 lata (PA-2050, PA-2020)

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-500**

Platforma	PAN-PA-500
Roczna subskrypcja systemu zapobiegania zagrożeniom	PAN-PA-500-TP
Roczna subskrypcja filtrowania URL	PAN-PA-500-URL2

Dodatkowe informacje dotyczące właściwości urządzenia PA-500 znajdują się na stronie www.paloaltonetworks.com/literature.

