Seria VM

Cechy i funkcje zapory nowej generacji serii VM:

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™.

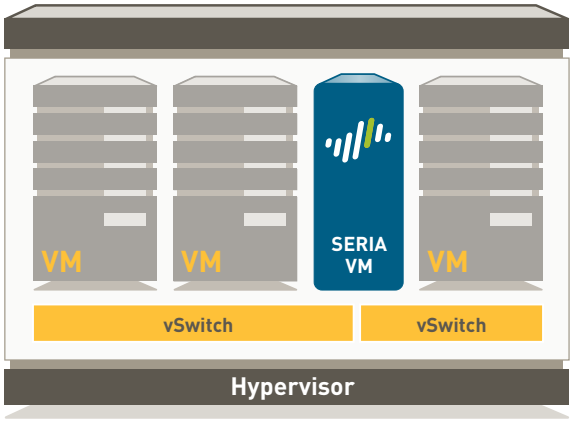
- Integracja z usługami Active Directory, LDAP, eDirectory Citrix oraz usługami terminalowymi firmy Microsoft bez zastosowania agentów.
- Integracja z urządzeniami NAC, urządzeniami bezprzewodowymi oraz innymi niestandardowymi repozytoriami użytkowników z interfejsem XML API.
- Wdrażanie spójnych zasad 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™



Wirtualna zapora serii VM

Zapory Palo Alto Networks™ serii VM rozszerzają bezpieczne korzystanie z aplikacji na środowiska wirtualne, zapewniając jednocześnie rozwiązanie następujących najważniejszych kwestii z zakresu bezpieczeństwa platform wirtualizacji: śledzenie zasad zabezpieczeń ruchu kierowanego do maszyny wirtualnej z obiektami adresów dynamicznych oraz integracja z systemami aranżacji przy użyciu zaawansowanego interfejsu API do zarządzania opartego na kodzie XML.

Seria VM składa się z trzech wydajnych modeli VM-100, VM-200 oraz VM-300 z jednoprzebiegową architekturą oprogramowania, która gwarantuje minimalne opóźnienia w środowiskach centrów danych. Elementy służące do zarządzania i przetwarzania danych są rozdzielone, więc użytkownicy mogą przydzielać określoną moc procesora do określonych zadań, zapewniając jednocześnie dostęp do funkcji zarządzania niezależnie od natężenia ruchu sieciowego. Zaporą serii VM steruje system operacyjny opracowany pod kątem bezpieczeństwa PAN-OS™, który zapewnia ochronę aplikacji dzięki funkcjom App-ID, User-ID, Content-ID, GlobalProtect oraz WildFire.

OGÓLNE PARAMETRY WYDAJNOŚCIOWE[1]	VM-300	VM-200	VM-100
Maksymalna liczba sesji	250 000	100 000	50 000
Liczba tuneli/interfejsów tuneli sieci VPN IPSec	2000	500	25
Liczba jednoczesnych użytkowników funkcji GlobalProtect (VPN SSL)	500	200	25
Liczba sesji odszyfrowywania SSL	1024	1024	1024
Liczba certyfikatów przychodzących SSL	25	25	25
Liczba routerów wirtualnych	3	3	3
Liczba stref zabezpieczeń	40	20	10
Maksymalna liczba zasad	5000	2000	250
Liczba obiektów adresów	10000	4000	2500
PRZEPŁYWNOŚĆ I WIRTUALIZACJA[1]			
Przepływność zapory (z funkcją App-ID)	1 Gb/s		
Przepływność systemu zapobiegania zagrożeniom	600 Gb/s		
Przepływność sieci IPSec VPN	250 Gb/s		
Liczba nowych sesji na sekundę	8000		

[1] Parametry wydajnościowe zmierzone w idealnych warunkach testowania w systemie PAN-OS 5.0 przy użyciu 8 rdzeni procesora.

WIRTUALIZACJA	VM-300	VM-200	VM-100
Hypervisor	VMware ESXi 4.1 i ESXi 5.0		
Sterownik sieci	VMXNet3		
Liczba rdzeni procesora	2, 4 lub 8		
Pamięć RAM (min.)	4 GB		
Pojemność dysku twardego (min./maks.)	40 GB/2 TB		

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): 1000/1000
- Routing oparty na politykach
- Multicasting: PIM-SM, PIM-SSM, IGMP v1, v2 i v3

WYSOKA DOSTĘPNOŚĆ

- Tryby: tryb aktywny/pasywny bez synchronizacji sesji
- 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: 4094/4094
- Maks. liczba interfejsów: 1024 (VM-300), 288 (VM-200), 100 (VM-100)

NAT/PAT

- Maks. liczba polityk trybu NAT: 1000 (VM-300), 1000 (VM-200), 125 (VM-100)
- Maks. liczba polityk trybu NAT (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- 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): 2
- NAT64

POŁĄCZENIE WIRTUALNE

- Maks. liczba połączeń wirtualnych: 500 (VM-300), 100 (VM-200), 40 (VM-100)
- Typy interfejsów przypisane do połączeń wirtualnych: fizyczne oraz podinterfejsy

PRZEKAZYWANIE L2

- Rozmiar tablicy ARP/urządzenie: 1000 (VM-300), 500 (VM-200), 500 (VM-100)
- Rozmiar tablicy MAC/urządzenie: 1000 (VM-300), 500 (VM-200), 500 (VM-100)
- Rozmiar tablicy sąsiednich adresów IPv6: 1000 (VM-300), 500 (VM-200), 500 (VM-100)

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 1000 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 SSN
- 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: 6 (VM-300, VM-200), 4 (VM-100)

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 VM znajduje się na stronie visit 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