PA-4000 Series

Wesentliche Funktionen der PA-4000 Series-Firewall der nächsten Generation:

KLASSIFIZIEREN SIE MIT APP-ID™ JEDERZEIT SÄMTLICHE ANWENDUNGEN AUF ALLEN PORTS.

- Identifizieren Sie die Anwendung unabhängig vom Port, der Verschlüsselung (SSL oder SSH) oder der eingesetzten Umgehungsmethode.
- Nutzen Sie die Anwendung und nicht den Port als Basis für sämtliche Entscheidungen im Rahmen der Richtlinie zur sicheren Aktivierung: zulassen, ablehnen, planen, prüfen, Traffic-Shaping anwenden.
- Kategorisieren Sie nicht identifizierte Anwendungen für die Richtlinienkontrolle, die Bedrohungsanalyse, die Erstellung benutzerdefinierter App-IDs oder die Datenaufzeichnung für die App-ID-Entwicklung.

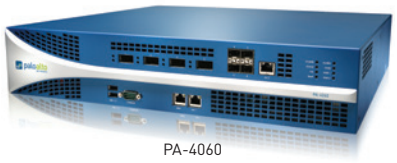
ERWEITERN SIE MIT USER-ID™ UND GLOBALPROTECT™ DIE RICHTLINIEN ZUR SICHEREN ANWENDUNGSAKTIVIERUNG AUF BELIEBIGE BENUTZER UND STANDORTE.

- Agentenlose Integration in Active Directory, LDAP, eDirectory Citrix und Microsoft Terminal Services.
- Integration in NAC, drahtloses 802.1X und andere nicht standardmäßige Benutzer-Repositorys mit einer XML-API.
- Bereitstellung konsistenter Richtlinien für lokale und Remote-Benutzer, die Microsoft Windows-, Mac OS X-, Linux-, Android- oder iOS-Plattformen ausführen.

MIT CONTENT-ID™ UND WILDFIRETM KÖNNEN SIE SICH VOR SÄMTLICHEN BEKANNTEN UND UNBEKANNTEN BEDROHUNGEN SCHÜTZEN.

- Blockieren Sie eine Reihe von bekannten Bedrohungen, einschließlich Ausnutzung von Sicherheitslücken, Malware und Spyware, in allen Ports, unabhängig von den eingesetzten Taktiken zur Vermeidung gängiger Bedrohungen.
- Beschränken Sie die Übertragung von Dateien und sensiblen Daten und kontrollieren Sie die nicht arbeitsbezogene Internetsuche.
- Identifizieren Sie unbekannte Malware und suchen Sie nach über 100 schädlichen Funktionsweisen. Mit dem nächsten verfügbaren Update ist das automatische Erstellen und Bereitstellen einer Signatur möglich.

paloalto NETWORKS
the network security company™


PA-4060


PA-4050


PA-4020

Die Palo Alto Networks™ PA-4000 Series besteht aus den drei Hochleistungsplattformen PA-4060, PA-4050 und PA-4020, die für die Bereitstellung von Hochgeschwindigkeits-Rechenzentren und -Internet-Gateways konzipiert wurden. Die PA-4000 Series stellt durch dedizierte Verarbeitung und Arbeitsspeicher bis zu 10 Gbit/s Durchsatz für die wesentlichen Funktionsbereiche von Netzwerken, Sicherheit, Bedrohungsschutz und Management bereit.

Die Hochgeschwindigkeits-Backplane ist in separate Daten- und Steuerebenen unterteilt, wodurch der Management-Zugriff jederzeit unabhängig von der Höhe des Datenflusses verfügbar ist. Die PA-4000 Series-Firewall wird über PAN-OS™ gesteuert, einem sicherheitsspezifischen Betriebssystem, über das Unternehmen Anwendungen sicher unter Verwendung von App-ID, User-ID, Content-ID, GlobalProtect und WildFire aktivieren können.

LEISTUNG UND KAPAZITÄTEN[1]	PA-4060	PA-4050	PA-4020
Firewall-Durchsatz (aktivierte App-ID)	10 Gbit/s	10 Gbit/s	2 Gbit/s
Bedrohungsschutz-Durchsatz	5 Gbit/s	5 Gbit/s	2 Gbit/s
IPSec-VPN-Durchsatz	2 Gbit/s	2 Gbit/s	1 Gbit/s
Neue Sitzungen pro Sekunde	60.000	60.000	60.000
Max. Anzahl an Sitzungen	2.000.000	2.000.000	500.000
IPSec-VPN-Tunnel/Tunnelschnittstellen	4.000	4.000	2.000
Gleichzeitige Benutzer von GlobalProtect (SSL VPN)	10.000	10.000	5.000
SSL-Entschlüsselungssitzungen	23.000	23.000	7.500
Eingehende SSL-Zertifkate	300	300	25
Virtuelle Router	125	125	20
Virtuelle Systeme (Basis/max.[2])	25/125	25/125	10/20
Sicherheitszonen	500	500	80
Max. Anzahl an Richtlinien	20.000	20.000	10.000

[1] Leistung und Kapazitäten werden unter idealen Testbedingungen mit PAN-OS 5.0 gemessen.

[2] Zum Hinzufügen von virtuellen Systemen zur Basismenge muss eine separate Lizenz erworben werden.

Eine vollständige Beschreibung des Funktionssatzes der PA-4000 Series-Firewall der nächsten Generation finden Sie unter www.paloaltonetworks.com/literature.

HARDWARESPEZIFIKATIONEN

E/A

- PA-4060: (4) 10 Gigabit XFP, (4) Gigabit SFP
- PA-4050, PA-4020: (16) 10/100/1000, (8) Gigabit SFP

MANAGEMENT-E/A

- (2) 10/100/1000 hohe Verfügbarkeit, (2) 10/100/1000 Out-of-Bound-Management, (1) Konsolen-Port DB9

SPEICHERKAPAZITÄT

- 160 GB HDD

STROMVERSORGUNG (DURCHSCHN./MAX. STROMVERBRAUCH)

- Redundant 400 W AC (175 W/200 W)

MAX. BTU/H

- 682

EINGANGSSPANNUNG (EINGANGSFREQUENZ)

- 100–240 VAC (50–60 Hz)

MAX. STROMVERBRAUCH

- 2,5 A @ 100 VAC

MEAN TIME BETWEEN FAILURES (MTBF)

- 7,18 Jahre

MAX. EINSCHALTSTROM

- 50 A @ 230 VAC; 30 A @ 115 VAC

IM RACK MONTIERBAR (ABMESSUNGEN)

- 2 Einheiten, 48,26 cm-Standard-Rack (7,62 cm H x 53.34 cm T x 43,18 cm B)

GEWICHT (STAND-ALONE-GERÄT/WIE GELIEFERT)

- 14,9 kg/18,1 kg

SICHERHEIT

- UL, CUL, CB

EMI

- FCC-Klasse A, CE-Klasse A, VCCI-Klasse A, TUV

ZERTIFIZIERUNGEN

- FIPS 140 Level 2, Common Criteria EAL2, ICSA, UCAPL

UMGEBUNG

- Betriebstemperatur 0 bis 50 °C
- Temperatur bei Nichtbetrieb -20 bis 70 °C

NETZWERK

SCHNITTSTELLENMODI:

- L2, L3, TAP, Virtual Wire (transparenter Modus)

ROUTING

- Modi: OSPF, RIP, BGP, Static
- Größe der Weiterleitungstabelle (Einträge pro Gerät und VR): 20.000/20.000 (PA-4060, PA-4050), 10.000/10.000 (PA-4020)
- Richtlinienbasierte Weiterleitung
- PPP over Ethernet (PPPoE)
- Jumbo Frames: 9.210 Byte max. Frame-Größe
- Multicase: PIM-SM, PIM-SSM, IGMP v1, v2 und v3

HOHE VERFÜGBARKEIT

- Modi: Aktiv/Aktiv, Aktiv/Passiv
- Fehlererkennung: Pfadüberwachung, Schnittstellenüberwachung

ADRESSZUWEISUNG

- Adresszuweisung für Gerät: DHCP-Client/PPPoE/Static
- Adresszuweisung für Benutzer: DHCP-Server/DHCP Relay/Static

IPV6

- L2, L3, TAP, Virtual Wire (transparenter Modus)
- Funktionen: App-ID, User-ID, Content-ID, WildFire und SSL-Entschlüsselung

VLANS

- 802.1q VLAN-Tags pro Gerät und Schnittstelle: 4,094/4,094
- Max. Anzahl an Schnittstellen: 4.096 (PA-4060, PA-4050), 2.048 (PA-4020)
- Aggregatschnittstelle (802.3ad)

NAT/PAT

- Max. Anzahl an NAT-Regeln: 4.000 (PA-4060, PA-4050), 1.000 (PA-4020)
- Max. Anzahl an NAT-Regeln (DIPP): 250 (PA-4060, PA-4050), 200 (PA-4020)
- Pool dynamischer IP-Adressen und Ports: 254
- Pool dynamischer IP-Adressen: 16.234
- NAT-Modi: 1:1 NAT, n:n NAT, m:n NAT
- DIPP-Überbelegung (Eindeutige Ziel-IPs pro Quell-Port und IP): 8 (PA-4060, PA-4050), 4 (PA-4020)
- NAT64

VIRTUAL WIRE

- Max. Anzahl an Virtual Wires: 2.048 (PA-4060, PA-4050), 1.024 (PA-4020)
- Auf Virtual Wires abgebildete Schnittstellen: physische und Teilschnittstellen

L2-WEITERLEITUNG

- Größe der ARP-Tabelle/Gerät: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- Größe der MAC-Tabelle/Gerät: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- Größe der IPv6-Nachbartabelle: 5.000 (PA-4060, PA-4050), 2.000 (PA-4020)

SICHERHEIT

FIREWALL

- Richtlinienbasierte Steuerung von Anwendungen, Benutzern und Inhalt
- Schutz fragmentierter Pakete
- Schutz vor Auskundschaftung
- Schutz vor Denial of Service (DoS)/Distributed Denial of Services (DDoS)
- Entschlüsselung: SSL (eingehend und ausgehend), SSH

WILDFIRE

- Identifizieren und analysieren Sie über 100 schädliche Funktionsweisen in zielgerichteten und unbekannten Dateien.
- Generieren Sie Schutz für neu entdeckte Malware und stellen Sie diesen automatisch über Signatur-Updates bereit.
- Bereitstellung des Signatur-Updates in weniger als einer Stunde, integrierte Protokollierung/Berichterstellung, Zugriff auf WildFire-API für programmatische Eingabe von bis zu 100 Mustern und bis zu 250 Berichtsanfragen nach Datei-Hash pro Tag (Abonnement erforderlich)

DATEI- UND DATENFILTERUNG

- Dateiübertragung: Bidirektionale Steuerung von über 60 eindeutigen Dateitypen
- Datenübertragung: Bidirektionale Steuerung von nicht autorisierter Übertragung von CC-Nr. und SSN
- Schutz vor unbeabsichtigtem Herunterladen

BENUTZERINTEGRATION (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One und andere LDAP-basierte Verzeichnisse
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML-API für die Integration in nicht standardmäßige Benutzer-Repositorys

IPSEC-VPN (STANDORT-ZU-STANDORT)

- Schlüsselaustausch: Manueller Schlüssel, IKE v1
- Verschlüsselung: 3DES, AES (128-Bit, 192-Bit, 256-Bit)
- Authentifizierung: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamische VPN-Tunnelerstellung (GlobalProtect)

BEDROHUNGSSCHUTZ (ABONNEMENT ERFORDERLICH)

- Anwendung, Schutz vor Ausnutzung von Sicherheitslücken im Betriebssystem
- Stream-basierter Virenschutz (einschließlich Viren in HTML, Javascript, PDF und komprimierten Dateien), Spyware, Würmer

URL-FILTERUNG (ABONNEMENT ERFORDERLICH)

- Vordefinierte und benutzerdefinierte Kategorien
- Geräte-Cache für die zuletzt aufgerufenen URLs
- URL-Kategorie als Teil der Übereinstimmungskriterien für Sicherheitsrichtlinien
- Informationen zur Surfzeit

QUALITY-OF-SERVICE (QOS)

- Richtlinienbasiertes Traffic-Shaping nach Anwendung, Benutzer, Quelle, Zielort, Schnittstelle, IPSec-VPN-Tunnel und mehr
- 8 Traffic-Klassen mit garantierten, maximalen und priorisierten Bandbreitenparametern
- Bandbreitenüberwachung in Echtzeit
- Diffserv-Markierung pro Richtlinie
- Unterstützte physische Schnittstellen für QoS: 12

SSL-VPN/REMOTE-ZUGRIFF (GLOBALPROTECT)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec mit SSL-Fallback
- Authentifizierung: LDAP, SecurID oder lokale DB
- Client-Betriebssystem: Mac OS X 10.6, 10.7 (32/64 Bit), 10.8 (32/64 Bit), Windows XP, Windows Vista (32/64 Bit), Windows 7 (32/64 Bit)
- Client-Support von Drittanbietern: Apple iOS, Android 4.0 und höher, VPNC-IPSec für Linux

MANAGEMENT, BERICHTE, TRANSPARENZ-TOOLS

- Integrierte Webschnittstelle, CLI oder zentrale Verwaltung (Panorama)
- Mehrsprachige Benutzeroberfläche
- Syslog und SNMP v2/v3
- XML-basierte REST-API
- Grafische Zusammenfassung aller Anwendungen, URL-Kategorien, Bedrohungen und Daten (ACC)
- Protokolle zu Traffic, Bedrohung, WildFire, URL und Datenfilterung anzeigen, filtern und exportieren
- Vollständig anpassbare Berichte

Zusätzliche Informationen zum Funktionssatz der PA-4000 Series-Firewall der nächsten Generation finden Sie unter 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