

# PA-5000 Series

## Wesentliche Funktionen der PA-5000 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 eine weitere Prüfung.

### ERWEITERN SIE MIT USER-ID™ UND GLOBALPROTECT™ DIE RICHTLINIEN ZUR SICHEREN ANWENDUNGS-AKTIVIERUNG 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-Repositories mit einer XML-API.
- Bereitstellung konsistenter Richtlinien für Benutzer, die Microsoft Windows-, Mac OS X-, Linux-, Android- oder iOS-Plattformen ausführen.

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

- Blockieren Sie eine Reihe von bekannten Bedrohungen, einschließlich Ausnutzung von Sicherheitslücken, Malware und Spyware – auf 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 von Schutz möglich.



PA-5060



PA-5050



PA-5020

Die Palo Alto Networks™ PA-5000 Series besteht aus den drei Hochleistungsmodellen PA-5060, PA-5050 und PA-5020, die für die Bereitstellung von Hochgeschwindigkeits-Rechenzentren und -Internet-Gateways konzipiert wurden.

Die PA-5000 Series stellt durch dedizierte Verarbeitung und Arbeitsspeicher bis zu 20 Gbit/s Durchsatz für die wesentlichen Funktionsbereiche Netzwerk, Sicherheit, Bedrohungsschutz und Management bereit. Die Daten- und Steuerungsebenen sind physisch voneinander getrennt, um sicherzustellen, dass der Management-Zugriff unabhängig von der Höhe des Datenflusses stets verfügbar ist. Die PA-5000 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 <sup>1</sup>	PA-5060	PA-5050	PA-5020
Firewall-Durchsatz (aktivierte App-ID)	20 Gbit/s	10 Gbit/s	5 Gbit/s
Bedrohungsschutz-Durchsatz	10 Gbit/s	5 Gbit/s	2 Gbit/s
IPSec-VPN-Durchsatz	4 Gbit/s	4 Gbit/s	2 Gbit/s
Max. Anzahl an Sitzungen	4.000.000	2.000.000	1.000.000
Neue Sitzungen pro Sekunde	120.000	120.000	120.000
IPSec-VPN/IPSec-VPN-Tunnel/ Tunnelschnittstellen	8.000	4.000	2.000
Gleichzeitige Benutzer von GlobalProtect (SSL VPN)	20.000	10.000	5.000
SSL-Entschlüsselungssitzungen	90.000	45.000	15.000
Eingehende SSL-Zertifikate	1.000	300	100
Virtuelle Router	225	125	20
Virtuelle Systeme (Basis/max. <sup>2</sup> )	25/225*	25/125*	10/20*
Sicherheitszonen	900	500	80
Max. Anzahl an Richtlinien	40.000	20.000	10.000

<sup>1</sup> Leistung und Kapazitäten werden unter idealen Testbedingungen mit PAN-OS 5.0 gemessen.

<sup>2</sup> Zum Hinzufügen von virtuellen Systemen zur Basismenge muss eine separate Lizenz erworben werden.

**HARDWARESPEZIFIKATIONEN****E/A**

- PA-5060, PA-5050: (12) 10/100/1000, (8) Gigabit SFP, (4) 10 Gigabit SFP+
- PA-5020: (12) 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 RJ45

**SPEICHEROPTIONEN**

- Ein oder zwei SSD-Laufwerke

**SPEICHERKAPAZITÄT**

- 120 GB, 240 GB SSD, RAID 1

**STROMVERSORGUNG (DURCHSCHN./MAX. STROMVERBRAUCH)**

- PA-5060: Redundant 450 W AC (330 W/415 W)
- PA-5050, PA-5020: Redundant 450 W AC (270 W/340 W)

**MAX. BTU/H**

- PA-5060: 1,416
- PA-5050, PA-5020: 1,160

**EINGANGSSPANNUNG (EINGANGSFREQUENZ)**

- 100–240 VAC (50–60 Hz); -40 bis -72 VDC

**MAX. STROMVERBRAUCH**

- 8 A @ 100 VAC, 14 A @ 48 VDC

**MAX. EINSCHALTSTROM**

- 80 A @ 230 VAC; 40 A @ 120 VAC; 40 A @ 48 VDC

**MEAN TIME BETWEEN FAILURES (MTBF)**

- 6,5 Jahre

**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)**

- 18,6 kg/ca. 25 kg

**SICHERHEIT**

- UL, CUL, CB

**EMI**

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

**ZERTIFIZIERUNGEN**

- NEBS Level 3, Common Criteria EAL2, FIPS level 2, ICESA, UCAPL

**UMGEBUNG**

- Betriebstemperatur: 0 bis 50 °C
- Temperatur bei Nichtbetrieb: -4 bis 158 F, -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):  
64.000/64.000
- Richtlinienbasierte Weiterleitung
- PPP over Ethernet (PPPoE)
- Jumbo Frames: 9.210 Byte max. Frame-Größe
- Multicast: 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-5060, PA-5050),  
2.048 (PA-5020)
- Aggregatschnittstelle (802.3ad)

**NAT/PAT**

- Max. Anzahl an NAT-Regeln: 8.000 (PA-5060), 4.000 (PA-5050),  
1.000 (PA-5020)
- Max. Anzahl an NAT-Regeln (DIPP): 450 (PA-5060), 250 (PA-5050), 200  
(PA-5020)
- Pool dynamischer IP-Adressen und Ports: 254
- Pool dynamischer IP-Adressen: 32.000
- NAT-Modi: 1:1 NAT, n:n NAT, m:n NAT
- DIPP-Überbelegung (Eindeutige Ziel-IPs pro Quell-Port und IP): 8
- NAT64

**VIRTUAL WIRE**

- Max. Anzahl an Virtual Wires: 2.048 (PA-5060, PA-5050), 1.024 (PA-5020)
- Auf Virtual Wires abgebildete Schnittstellen: physische und  
Teilschnittstellen

**L2-WEITERLEITUNG**

- Größe der ARP-Tabelle/Gerät: 32.000 (PA-5060, PA-5050),  
20.000 (PA-5020)
- Größe der MAC-Tabelle/Gerät: 32.000 (PA-5060, PA-5050),  
20.000 (PA-5020)
- Größe der IPv6-Nachbartabelle: 5.000 (PA-5060, PA-5050),  
2.000 (PA-5020)

## SICHERHEIT

### FIREWALL

- Richtlinienbasierte Steuerung von Anwendungen, Benutzern und Inhalt
- Schutz fragmentierter Pakete
- Schutz vor Auskunftschaftung
- 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 unbekanntem 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 Berichtsabfragen 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-Repositories

### 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, Netflow v9 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

Eine vollständige Beschreibung des Funktionssatzes der PA-5000 Series-Firewall der nächsten Generation finden Sie unter [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature).