

PA-2000 Series

Wesentliche Funktionen der PA-2000 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 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, 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.



PA-2050



PA-2020

Die Palo Alto Networks™ PA-2000 Series besteht aus den zwei Hochleistungsplattformen PA-2050 und PA-2020, die für die Bereitstellung von Hochgeschwindigkeits-Internet-Gateways konzipiert wurden. Die PA-2000 Series regelt den Netzwerkdatenfluss mithilfe entsprechender Verarbeitung und Speicher für Netzwerke, Sicherheit, Bedrohungsschutz und Management.

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-2000 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-2050	PA-2020
Firewall-Durchsatz (aktivierte App-ID)	1 Gbit/s	500 Mbit/s
Bedrohungsschutz-Durchsatz	500 Mbit/s	200 Mbit/s
IPSec-VPN-Durchsatz	300 Mbit/s	200 Mbit/s
Neue Sitzungen pro Sekunde	15.000	15.000
Max. Anzahl an Sitzungen	250.000	125.000
IPSec-VPN-Tunnel/Tunnelschnittstellen	2.000	1.000
Gleichzeitige Benutzer von GlobalProtect (SSL VPN)	1.000	500
SSL-Entschlüsselungssitzungen	1.000	1.000
Eingehende SSL-Zertifikate	25	25
Virtuelle Router	10	10
Virtuelle Systeme (Basis/max.2)	1/6	1/6
Sicherheitszonen	40	40
Max. Anzahl an Richtlinien	5.000	2.500

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 Funktionsatzes der PA-2000 Series-Firewall der nächsten Generation finden Sie unter www.paloaltonetworks.com/literature.

HARDWARESPEZIFIKATIONEN**E/A**

- PA-2050: (16) 10/100/1000, (4) SFP optische Gigabit
- PA-2020: (12) 10/100/1000, (2) SFP optische Gigabit

MANAGEMENT-E/A

- (1) 10/100/1000 Out-of-Band-Management-Port, (1) Konsolen-Port RJ-45

SPEICHERKAPAZITÄT

- 160 GB HDD

STROMVERSORGUNG (DURCHSCHN./MAX. STROMVERBRAUCH)

- 250 W (105 W/120 W)

MAX. BTU/H

- 409

EINGANGSSPANNUNG (EINGANGSFREQUENZ)

- 100–240 VAC (50–60 Hz)

MAX. STROMVERBRAUCH

- 3 A @ 100 VAC

MEAN TIME BETWEEN FAILURES (MTBF)

- 7,3 Jahre

MAX. EINSCHALTSTROM

- 70 A @ 230 VAC; 35 A @ 115 VAC

IM RACK MONTIERBAR (ABMESSUNGEN)

- 1 Einheit, 48,26 cm-Standard-Rack (2,54 cm H x 43,18 cm T x 43,18 cm B)

GEWICHT (STAND-ALONE-GERÄT/WIE GELIEFERT)

- 6,8 kg/9 kg

SICHERHEIT

- UL, CUL, CB

EMI

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

ZERTIFIZIERUNGEN

- FIPS 140 Level 2, Common Criteria EAL2, ICOSA, 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): 5.000/2.500 (PA-2050), 2.500/2.500 (PA-2020)
- Richtlinienbasierte Weiterleitung
- PPP over Ethernet (PPPoE)
- 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: 2.048 (PA-2050), 1.024 (PA-2020)
- Aggregatschnittstelle (802.3ad)

NAT/PAT

- Max. Anzahl an NAT-Regeln: 1.000
- Max. Anzahl an NAT-Regeln (DIPP): 200
- 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): 2
- NAT64

VIRTUAL WIRE

- Max. Anzahl an Virtual Wires: 1.024 (PA-2050), 512 (PA-2020)
- Schnittstellentypen auf Virtual Wires abgebildet: physische und Teilschnittstellen

L2-WEITERLEITUNG

- Größe der ARP-Tabelle/Gerät: 2.500 (PA-2050), 1.000 (PA-2020)
- Größe der MAC-Tabelle/Gerät: 2.500 (PA-2050), 1.000 (PA-2020)
- Größe der IPv6-Nachbartabelle: 1.000

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 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 Berichtsfragen 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: 4

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-2000 Series-Firewall der nächsten Generation finden Sie unter www.paloaltonetworks.com/literature.