

سلسلة PA-2000



PA-2020

PA-2050

تتكون سلسلة PA-2000 من Palo Alto Networks™ من اثنين من النظم الأساسية عالية الأداء، PA-2020 و PA-2050، يستهدف كل منهما نشر عالي السرعة على بوابة الإنترنت. تدير سلسلة PA-2000 تدفقات نقل البيانات في الشبكة باستخدام معالجة مخصصة وذاكرة للشبكات والأمن ومنع المخاطر المحتملة والإدارة.

يتم تقسيم لوحة التوصيل بالشبكة عالية السرعة إلى بيانات منفصلة ومستويات تحكم، مما يضمن إمكانية إدارة عمليات الدخول بشكل دائم، بغض النظر عن حمل نقل البيانات. العنصر المتحكم في سلسلة PA-2000 هو PAN-OS™، وهو عبارة عن نظام تشغيل مخصص للأمن يسمح للمؤسسات بتمكين التطبيقات بشكل آمن باستخدام App-ID و User-ID و Content-ID و WildFire و GlobalProtect.

المميزات الرئيسية للجيل الجديد من جدار الحماية PA-2000:

تصنيف كافة التطبيقات، على جميع المنافذ، طوال الوقت مع™ APP-ID.

• تحديد التطبيق، بغض النظر عن المنفذ أو التشفير (SSH أو SSL) أو تقنية المراوغة المستخدمة.

• استخدام التطبيق وليس المنفذ كأساس لكافة قرارات سياسة التمكن الآمن: السماح، الرفض، الجدولة، الفحص، تطبيق تشذيب سيل البيانات.

• تصنيف التطبيقات غير المعروفة من أجل التحكم في السياسة أو التحليل الجنائي للمخاطر أو إنشاء App-ID مخصص أو التقاط حزمة لتطوير App-ID.

توسيع سياسات تمكين التطبيقات الآمنة لتشمل أي مستخدم في أي مكان، مع

™ USER-ID و™ GLOBALPROTECT.

• التكامل بدون وكيل مع خدمات Active Directory و LDAP و eDirectory Citrix والخدمات الطرفية من Microsoft.

• التكامل مع NAC و 802.1X اللاسلكي وغيرها من مستودعات المستخدم غير القياسية الأخرى مع XML API.

• نشر السياسات المتسقة بين المستخدمين المحليين والبعدين الذين يقومون بتشغيل النظم الأساسية Microsoft Windows أو Mac OS X أو Linux أو Android أو iOS.

الحماية ضد جميع المخاطر المحتملة – المعروفة وغير المعروفة باستخدام

™ WILDFIRE و™ CONTENT-ID.

• منع مجموعة من المخاطر المعروفة، بما في ذلك الفيروسات المعطلة للأمان والبرامج الضارة وبرامج التجسس، عبر كافة المنافذ، بغض النظر عن أساليب مراوغة التهديدات الشائع استخدامها.

• الحد من النقل غير المرخص للملفات والبيانات الحساسة، والتحكم في تصفح الويب غير المرتبط بالعمل.

• تحديد البرامج الضارة غير المعروفة، وتحليل لأكثر من 100 سلوك ضار، وإنشاء وتسليم توقيع بشكل تلقائي في التحديث التالي المتوفر.

PA-2020	PA-2050	الأداء والقدرات ¹
500 ميجابايت لكل ثانية	1 جيجابايت في الثانية	سرعة جدار الحماية (App-ID مُمكن)
200 ميجابايت لكل ثانية	500 ميجابايت لكل ثانية	سرعة منع المخاطر
200 ميجابايت لكل ثانية	300 ميجابايت لكل ثانية	سرعة VPN لـ IPSec
15,000	15,000	جلسات العمل الجديدة في الثانية
125,000	250,000	الحد الأقصى لجلسات العمل
1,000	2,000	واجهات نفق/اتفاق VPN لـ IPSec
500	1,000	المستخدمين المتزامنين لـ GlobalProtect (SSL VPN)
1,000	1,000	جلسات فك تشفير SSL
25	25	شهادات SSL الواردة
10	10	أجهزة التوجيه الظاهرية
6/1	6/1	الأنظمة الظاهرية (القاعدة/الحد الأقصى ²)
40	40	مناطق الحماية
2,500	5,000	الحد الأقصى لعدد السياسات

¹ يتم قياس الأداء والقدرات تحت ظروف اختبار مثالية باستخدام PAN-OS 5.0.

² إضافة أنظمة ظاهرية للكلمة الأساسية يتطلب ترخيص يتم شراؤه بشكل منفصل.

للحصول على وصف كامل لمجموعة مميزات الجيل الجديد من جدار الحماية PA-2000، برجاء زيارة www.paloaltonetworks.com/literature.

مواصفات الأجهزة

الإدخال/الإخراج

- PA-2050: 10/100/1000 (16)، SFP (4) جيجابت ضوئية
- PA-2020: 10/100/1000 (12)، SFP (2) جيجابت ضوئية

إدارة الإدخال/الإخراج

- (1) منفذ إدارة خارج النطاق بسرعة 10/100/1000 (1) منفذ RJ-45 لوحدة التحكم

السعة التخزينية

- HDD بسعة 160 جيجابايت

مصدر الطاقة (المتوسط/الحد الأقصى لاستهلاك الطاقة)

- 250 واط واط (105 واط/120 واط)

الحد الأقصى للوحدة الحرارية البريطانية/ساعة

- 409

جهد الدخل (تردد الإدخال)

- 100-240 فولت تيار متردد (50-60 هرتز)

الحد الأقصى للاستهلاك الحالي

- 1,5 أمبير عند 100 فولت تيار متردد

متوسط الوقت بين الأعطال

- 3-7 عام

الحد الأقصى لتيار التدفق

- 70 أمبير عند 230 فولت تيار متردد؛ 35 أمبير عند 115 فولت تيار متردد

الحامل القابل للتركيب (الأبعاد)

- 1 وحدة، حامل قياسي 19 بوصة (ارتفاع 1.75 x عمق 17 x عرض 17 بوصة)

الوزن (الجهاز بشكل مستقل/عند الشحن)

- 15 رطل/20 رطل

السلامة

- شهادات UL، CB، CUL

EMI

- FCC فئة A و CE فئة A و VCCI فئة A و TUV

الشهادات

- 140 FIPS مستوى 2، معايير مشتركة EAL2 و ICSA و UCAPL

البيئة

- درجة حرارة التشغيل: من 32 إلى 122 درجة فهرنهايت، من 0 إلى 50 درجة مئوية
- درجة الحرارة أثناء عدم التشغيل: من -4 إلى 158 درجة فهرنهايت، من -20 إلى 70 درجة مئوية

الشبكات

أوضاع الواجهة:

- L2 و L3 و Tap و Virtual wire (وضع الشفافية)

التوجيه

- الأوضاع: OSPF، RIP، BGP، ثابت
- حجم جدول إعادة التوجيه (المدخلات لكل جهاز/في VR): (PA-2050) 5,000/2,500 (PA-2020) 2,500/2,500
- إعادة توجيه مستند إلى سياسة
- بروتوكول Point-to-Point عبر الإيثرنت (PPPoE)
- البث المتعدد: PIM-SM و PIM-SSM والإصدار الأول والثاني والثالث من IGMP

التوافر العالي

- الأوضاع: فعال/فعال، فعال/غير فعال
- اكتشاف الخطأ: مراقبة المسار، مراقبة الواجهة

تعيين العنوان

- تعيين عنوان للجهاز: عميل DHCP/PPPoE/ثابت
- تعيين عناوين للمستخدمين: خادم DHCP/ترحيل DHCP/ثابت

IPv6

- L2 و L3 و Tap و خط الشبكة الظاهرية (وضع الشفافية)
- المميزات: App-ID و User-ID و Content-ID و WildFire وفك تشفير SSL

شبكات VLAN

- علامات VLAN لكل جهاز/لكل واجهة: 4,094/4,094
- الحد الأقصى للواجهات: (PA-2020) 1,024 (PA-2050) 2,048
- الواجهات المجمعة (802.3ad)

NAT/PAT

- الحد الأقصى لقواعد NAT: 1,000
- الحد الأقصى لقواعد NAT (DIPP): 200
- الـ IP الديناميكية ومجموعة المنافذ: 254
- مجموعة الـ IP الديناميكية: 16,234
- أوضاع NAT: 1:1 NAT، n:n NAT، m:n NAT
- فائض DIPP (عناوين IP فريدة للوجهة لكل منفذ المصدر وIP): 2
- NAT64

VIRTUAL WIRE

- الحد الأقصى لخطوط الشبكات الظاهرية: (PA-2020) 512 (PA-2050) 1,024
- أنواع الواجهات التي تم تعيينها إلى خطوط الشبكات الظاهرية: الواجهات الفعلية والفرعية

إعادة توجيه L2

- جهاز/حجم جدول ARP: (PA-2020) 1,000 (PA-2050) 2,500
- جهاز/حجم جدول MAC: (PA-2020) 1,000 (PA-2050) 2,500
- حجم جدول IPv6 المجاور: 1,000

الأمان

جدار الحماية

- تحكم في التطبيقات والمستخدمين والمحتوى معتمد على السياسة
- حماية الحزم المجزئة
- حماية بالفحص الاستطلاعي
- الحماية ضد قطع الخدمة (DoS)/القطع الموزع للخدمة (DDos)
- فك التشفير: SSL (الوارد والصادر)، SSH

WILDFIRE

- تحديد وتحليل الملفات المستهدفة وغير المعروفة لأكثر من 100 سلوك ضار
- توليد وتوفير الحماية التلقائية من البرامج الضارة المكتشفة من خلال تحديثات التوقيعات
- تكامل تقديم تحديث توقيع WildFire في أقل من ساعة مع تسجيل الدخول/الإبلاغ؛ والوصول إلى واجهة برمجة التطبيقات (API) الخاصة بـ WildFire للإرسال البرنامجي لأكثر من 100 عينة يومياً وما يصل إلى 250 تقرير استعلام بواسطة تجزئة الملف في اليوم (الإشترار مطلوب)

تصنيفية البيانات والملفات

- نقل الملفات: التحكم ثنائي الاتجاه في أكثر من 60 نوع من الملفات الفريدة
- نقل البيانات: الرقابة ثنائية الاتجاه على النقل غير المصرح به لرقم CC وSSN
- الحماية من التنزيلات غير المقصودة

دمج المستخدم (USER-ID)

- Microsoft Active Directory و Sun One و Novell eDirectory وغيرها من الدلائل القائمة على LDAP.
- Microsoft Windows Server 2003/2008/2008r2
- Microsoft Exchange Server 2003/2007/2010 و
- الخدمات الطرفية من Citrix XenApp و Microsoft
- واجهة برمجة التطبيقات (API) لـ XML لتسهيل الدمج مع مستودعات المستخدم غير القياسية

IPSEC VPN (الموقع إلى الموقع)

- التبادل الرئيسي (Key Exchange): مفتاح يدوي، إصدار 1
- التشفير: 3DES و AES (128 بت، 192 بت، 256 بت)
- المصادقة: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- إنشاء نفق VPN ديناميكي (GlobalProtect)

منع التهديدات (الإشترار مطلوب)

- الحماية من استغلال الثغرات الأمنية في نظام التشغيل والتطبيقات
- الحماية المعتمدة على التدفق ضد الفيروسات (بما في ذلك، المضمنة في HTML و Javascript و PDF والملفات المضغوطة) و برامج التجسس والفيروسات المنتقلة

تصنيفية URL (الإشترار مطلوب)

- تصنيفات URL محددة مسبقاً ومخصصة
- التخزين المؤقت على الجهاز لأحدث عناوين URL التي تم الدخول إليها
- تصنيف URL كجزء من معايير التوافق لسياسيات الأمان
- معلومات عن وقت التصفح

جودة الخدمة (QoS)

- التحكم في نقل البيانات المستند إلى سياسة حسب التطبيق والمستخدم والمصدر والوجهة والواجهة ونفق VPN لـ IPSec والمزيد
- 8 فئات لنقل البيانات مع بارامترات النطاق الترددي المضمون والأقصى وذات الأولوية
- مراقب ذو نطاق ترددي في الوقت الحقيقي
- لكل سياسة ضبط diffserv
- الواجهات الفعلية المدعومة لـ QoS: 4

VPN (GLOBALPROTECT)/الوصول البعيد

- بوابة GlobalProtect
- موقع GlobalProtect
- النقل: IPSec مع بديل SSL
- المصادقة: LDAP أو SecurID أو DB محلية
- نظام تشغيل العميل: 10.7، Mac OS X 10.6، (32/64 بت)، 10.8، (32/64 بت)، Windows XP، Windows Vista (32/64 بت)، Windows 7 (32/64 بت)
- دعم العملاء من جهات خارجية: Apple iOS و Android 4.0 والأحدث، VPN IPSec لـ Linux

الإدارة، إعداد التقارير، أدوات الرؤية

- واجهة الويب المدمجة أو CLI أو الإدارة المركزية (Panorama)
- واجهة مستخدم متعددة اللغات
- Syslog و Netflow إصدار 9 و SNMP إصدار 2 أو 3
- واجهة برمجة التطبيقات REST المستندة إلى XML
- ملخص رسمي للتطبيقات وتصنيفات URL والتهديدات والبيانات (ACC)
- عرض وتصفية وتصدير نقل البيانات والتهديدات و WildFire و URL وسجلات تصفية البيانات
- تقارير كاملة التخصيص

للحصول على وصف كامل لمجموعة مميزات الجيل الجديد من جدار الحماية PA-2000، برجاء زيارة www.paloaltonetworks.com/literature.

Palo Alto Networks، Inc. يتلّفون قوقل عيّمج. ©2012 Palo Alto Networks، Inc. رشنلّا قوقل شاملع يه Panorama و App-ID و PAN-OS و Palo Alto Networks راعشرو Palo Alto Networks، Inc. ظفرشل ظلولم عيبراجت قوقل قوقل عيّمج يه Palo Alto Networks ظفرش لمجنت الو. قيسم راعشرو نود ظفرش ظفتحتو. دن تسجل اذه يف قنمضتجل تامول عمل شيدحتب مازتلا ي الو. دن تسجل اذه نود قروض ياب قرضنلّا مده عمل اعم و ا ليوحت و ا ليدعت و ا بريغت قحج Palo Alto Networks قوسم راعشرو PAN_SS_PA2000_112512.

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



the network security company™