

# PA-500



PA-500

تستهدف سلسلة PA-500 من شركة Palo Alto Networks™ نشر جدار الحماية عالي السرعة لمكاتب أفرع المؤسسات والشركات متوسطة الحجم. إن PA-500 تدير تدفقات نقل البيانات في الشبكة باستخدام مصادر حاسوبية مخصصة 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 الجيل الجديد من جدار الحماية PA-500 هو PAN-OS™، وهو عبارة عن نظام تشغيل مخصص للأمن يسمح للمنظمات بتمكين التطبيقات بشكل آمن باستخدام App-ID و User-ID و Content-ID و GlobalProtect و WildFire.

PA-500	الأداء والقدرات <sup>1</sup>
250 ميجابايت لكل ثانية	سرعة جدار الحماية (App-ID مُمكِن)
100 ميجابايت لكل ثانية	سرعة منع المخاطر
50 ميجابايت لكل ثانية	سرعة VPN - IPSec
7,500	جلسات العمل الجديدة في الثانية
64,000	الحد الأقصى لجلسات العمل
250	واجهات نفق/أنفاق VPN - IPSec
100	المستخدمين المتزامنين لـ GlobalProtect (SSL VPN)
1,000	جلسات فك تشفير SSL
25	شهادات SSL الواردة
3	أجهزة التوجيه الظاهرية
20	مناطق الحماية
1,000	الحد الأقصى لعدد السياسات

<sup>1</sup> يتم قياس الأداء والقدرات تحت ظروف اختبار مثالية باستخدام PAN-OS 5.0.

للحصول على وصف كامل لمجموعة مميزات الجيل الجديد من جدار الحماية PA-500، برجاء زيارة [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature).

## المميزات الرئيسية للجيل الجديد من جدار الحماية PA-500:

- 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 التمكنين الأمن: 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 الأمانة لتشمل أي مستخدم في أي مكان، مع **USER-ID™** و **GLOBALPROTECT™**.
- التكامل بدون وكيل مع خدمات LDAP و Active Directory 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.

## مواصفات الأجهزة

## الإدخال/الإخراج

- (8) 10/100/1000

## 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)

- 180 واط (40 واط/75 واط)

## الحد الأقصى للوحدة الحرارية البريطانية/ساعة

- 256

## جهد الدخل [تردد الإدخال]

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

## الحد الأقصى للاستهلاك الحالي

- 1 أمبير عند 100 فولت تيار متردد

## متوسط الوقت بين الأعطال

- 10-16 عام

## الحد الأقصى لتيار التدفق

- 110 أمبير عن 230 فولت تيار متردد؛ 51 أمبير عند 115 فولت تيار متردد

## الحامل القابل للتثبيت [الأبعاد]

- 1 وحدة، حامل قياسي 19 بوصة (ارتفاع 1.75 x عمق 10 x عرض 17 بوصة)

## الوزن [الجهاز بشكل مستقل/عند الشحن]

- 8 رطل/13 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 ICسا 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: BGP، RIP، OSPF، ثابت
- حجم جدول إعادة التوجيه (المدخلات لكل جهاز/في VR): 1,250/1,250 1000/1000
- 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 802.1q VLAN لكل جهاز/لكل واجهة: 4,094/4,094
- الحد الأقصى للواجهات: 250
- الواجهات المجمعة (802.3ad)

## NAT/PAT

- الحد الأقصى لقواعد NAT: 125
- الحد الأقصى لقواعد (NAT [DIPP]: 125
- ال-IP الديناميكية ومجموعة المنافذ: 254
- مجموعة ال-IP الديناميكية: 16,234
- أوضاع NAT: NAT 1:1 NAT، n:n NAT، m:n NAT
- فائض DIPP (عناوين IP فريدة للوجهة لكل منفذ المصدر و IP): 1
- NAT64

## VIRTUAL WIRE

- الحد الأقصى لخطوط الشبكات الظاهرية: 125
- أنواع الواجهات التي تم تعيينها إلى خطوط الشبكات الظاهرية: الواجهات الفعلية والفرعية

## إعادة توجيه L2

- جهاز/حجم جدول ARP: 500
- جهاز/حجم جدول MAC: 500
- حجم جدول IPv6 المجاور: 500

## 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 يوميا وما يصل إلى 250 تقرير استعلام بواسطة تجزئة الملف في اليوم (الاشتراك مطلوب)

## تصفية 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)

- دمج المستخدم (USER-ID) مع Microsoft Active Directory وNovell eDirectory وSun One وغيرها من الدلائل القائمة على LDAP.
- دمج المستخدم (USER-ID) مع Microsoft Exchange وMicrosoft Windows Server 2003/2008/2008r2 Server 2003/2007/2010
- دمج المستخدم (USER-ID) مع Citrix XenApp وMicrosoft
- واجهة برمجة التطبيقات (API) لـ XML لتسهيل الدمج مع مستودعات المستخدم غير القياسية

## IPSEC VPN (الموقع إلى الموقع)

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

## منع التهديدات (الاشتراك مطلوب)

- الحماية من استغلال الثغرات الأمنية في نظام التشغيل والتطبيقات
- الحماية المعتمدة على التدفق ضد الفيروسات (بما في ذلك، المضمنة في HTML وJavaScript وPDF والملفات المضغوطة) وبرامج التجسس والفيروسات المتنقلة

## تصفية URL (الاشتراك مطلوب)

- تصنيفات URL محددة مسبقا ومخصصة
- التخزين المؤقت على الجهاز لأحدث عناوين URL التي تم الدخول إليها
- تصنيف URL كجزء من معايير التطابق 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 SSL/الوصول البعيد (GLOBALPROTECT)

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

## الإدارة، إعداد التقارير، أدوات الرؤية

- واجهة الويب المنمجة أو CLI أو الإدارة المركزية (Panorama)
- واجهة مستخدم متعددة اللغات
- Syslog وNetflow إصدار 9 وSNMP إصدار 2 أو 3
- واجهة برمجة التطبيقات REST المستندة إلى XML
- ملخص رسومي للتطبيقات وتصنيفات URL والتهديدات والبيانات (ACC)
- عرض وتصفية وتصدير نقل البيانات والتهديدات وWildFire وURL وسجلات تصفية البيانات
- تقارير كاملة التخصيص

للحصول على وصف كامل لمجموعة مميزات الجيل الجديد من جدار الحماية PA-500، برجاء زيارة [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature).

Palo Alto Networks، Inc. يظفون قوقل عيجه ©2012. Palo Alto Networks، Inc. رشنلا قوقل شامل اع يه Panorama و App-ID و PAN-OS و Palo Alto Networks راعشو و Palo Alto Networks راعي غتلل كضردع تانافصول اع عيجه Palo Alto Networks، Inc. ظفرشل ظلولم عيراجت قودب قلد عتي اميف قولي و عيجه يا Palo Alto Networks ظفرش لمجنت الو. قبحس راعشو نود ظفرش ظفنتحت و. ننتسمل اذه يف قنمضتعل تامل عمل شيدحتب ملتلا يا الو. ننتسمل اذه نود قروض يا ب قرضنلا مده لعل اع و. ليوحت و. ليوحت و. بريغت قحج Palo Alto Networks قبحج PAN\_SS\_PA3000\_112512. قبحس راعشو

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](http://www.paloaltonetworks.com)

 **paloalto**  
NETWORKS  
the network security company™