سلسلة VM

المميزات الرئيسية للجيل الجديد من جدار الحماية سلسلة VM:

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

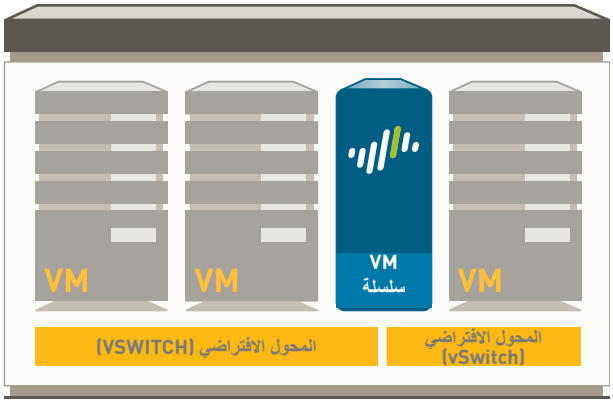
- تحديد التطبيق، بغض النظر عن المنفذ أو التشفير (SSL أو SSH) أو تقنية المراوغة المستخدمة.
- استخدام التطبيق وليس المنفذ كأساس لكافة قرارات سياسة التمكين الآمن: السماح، الرفض، الجدولة، الفحص، تطبيق التحكم في سيل البيانات.
- تصنيف التطبيقات غير المعرّفة من أجل التحكم في السياسة أو التحليل الجنائي للمخاطر أو إنشاء App-ID مخصص أو التقاط حزمة لمزيد من التحقيق.

توسيع سياسات تمكين التطبيقات الآمنة لتشمل أي مستخدم في أي مكان، مع USER-ID™ و GLOBALPROTECT™.

- الدمج بدون وكيل مع خدمات Active Directory وLDAP و eDirectory Citrix والخدمات الطرفية من Microsoft.
- الدمج مع NAC واللاسلكي وغيرها من مستودعات المستخدم غير القياسية الأخرى مع XML API.
- نشر السياسات المتسقة بين المستخدمين الذين يقومون بتشغيل النظم الأساسية Microsoft Windows أو Mac OS X أو Linux أو Android أو iOS، بغض النظر عن الموقع.

الحماية ضد جميع المخاطر المحتملة – المعروفة وغير المعروفة باستخدام CONTENT-ID™ و WILDFIRE™.

- 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 وتوفير الحماية بشكل تلقائي في التحديث التالي المتوفر.



جدار الحماية الافتراضي سلسلة VM

تعمل سلسلة VM من شركة Palo Alto Networks™ على تمديد تمكين التطبيقات بطريقة آمنة داخل البيئات الافتراضية مع معالجة التحديات الأمنية الرئيسية الافتراضية. ويتلخص ذلك في تتبع السياسات الأمنية لحركة الجهاز الافتراضي مع معالجة ديناميكية للأهداف والدمج مع أنظمة التزامن باستخدام واجهة برمجة تطبيقات قوية خاصة بإدارة XML.

تتألف سلسلة VM من ثلاثة نماذج عالية الأداء، نموذج VM-100 ونموذج VM-200 ونموذج VM-300، تستخدم جميعها بنية برمجيات ذات تمرير واحد وذلك لتقليل زمن الوصول لبيئات مراكز البيانات. تم فصل الإدارة عن مستويات البيانات بحيث يمكن للمستخدمين تعيين وحدات معالجة مركزية مخصصة لكل مستخدم، كوسيلة لضمان إمكانية إدارة عمليات الدخول بشكل دائم، بغض النظر عن حمل نقل البيانات. العنصر المتحكم في سلسلة VM هو PAN-OS™، وهو عبارة عن نظام تشغيل مخصص للأمن يسمح للمنظمات بتمكين التطبيقات بشكل آمن باستخدام App-ID وUser-ID وContent-ID و GlobalProtect وWildFire.

القدرات العامة[1]	VM-300	VM-200	VM-100
الحد الأقصى لجلسات العمل	250,000	100,000	50,000
واجهات نفق/أنفاق VPN لـ IPSec	2,000	500	25
المستخدمين المتزامنين لـ GlobalProtect (SSL VPN)	500	200	25
جلسات فك تشفير SSL	1024	1024	1024
شهادات SSL الواردة	25	25	25
أجهزة التوجيه الظاهرية	3	3	3
مناطق الحماية	40	20	10
الحد الأقصى لعدد السياسات	5,000	2,000	250
الأهداف المعالجة	10,000	4,000	2,500
الأداء[1] والمواصفات الافتراضية			
سرعة جدار الحماية (App-ID مُمكن)	1 جيجابايت لكل ثانية		
سرعة منع التهديدات	600 جيجابايت لكل ثانية		
سرعة VPN لـ IPSec	250 جيجابايت لكل ثانية		
جلسات العمل الجديدة في الثانية	8000		

[1] يتم قياس الأداء والقدرات تحت ظروف اختبار مثالية باستخدام PAN-OS 5.0 و 8 مراكز معالجات لوحدة المعالجة المركزية (CPU).

paloalto NETWORKS
the network security company™

الافتراضي	VM-300	VM-200	VM-100
برنامج مراقبة الأجهزة الافتراضية (HyperVisor)	VMware ESXi 4.1 و ESXi 5.0		
برنامج تشغيل الشبكات	VMXNet3		
مراكز معالجات وحدة المعالجة المركزية (CPU)	2 أو 4 أو 8		
الذاكرة (الحد الأدنى)	4 جيجابايت		
سعة محرك القرص (الحد الأدنى/الحد الأقصى)	40 جيجابايت/2 تيرابايت		

الشبكات

أوضاع الواجهة:

- L2 وL3 وTap وVirtual wire (وضع الشفافية)

التوجيه

- الأوضاع: OSPF، RIP، BGP، ثابت
- حجم جدول إعادة التوجيه (المدخلات لكل جهاز/في VR): 5000/5000 (VM-300), 1,250/1,250 (VM-200), 1000/1000 (VM-100)
- إعادة توجيه مستند إلى سياسة
- البث المتعدد: PIM-SM وPIM-SSM والإصدار الأول والثاني والثالث من IGMP

التوافر العالي

- الأوضاع: فعال/غير فعال مع عدم مزامنة الجلسات
- 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 وL3 وTap وخط الشبكة الظاهرية (وضع الشفافية)
- المميزات: App-ID وUser-ID وContent-ID وWildFire وفك تشفير SSL

شبكات VLAN

- علامات VLAN 802.1q لكل جهاز/لكل واجهة: 4,094/4,094
- الحد الأقصى للواجهات: 2,000 (VM-300), 500 (VM-200), 100 (VM-100)

NAT/PAT

- الحد الأقصى لقواعد NAT: 1,000 (VM-300), 1,000 (VM-200), 125 (VM-100)
- الحد الأقصى لقواعد NAT (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- الـ IP الديناميكية ومجموعة المنافذ: 254
- مجموعة الـ IP الديناميكية: 32,000
- أوضاع NAT: 1:1 NAT, n:n NAT, m:n NAT
- فائض DIPP (عناوين IP فريدة للوجهة لكل منفذ المصدر و IP): 2
- NAT64

VIRTUAL WIRE

- الحد الأقصى لخطوط الشبكات الظاهرية: 1,000 (VM-300), 250 (VM-200), 50 (VM-100)
- أنواع الواجهات التي تم تعيينها إلى خطوط الشبكات الظاهرية: الواجهات الفعلية والفرعية

إعادة توجيه L2

- جهاز/حجم جدول ARP: 2,500 (VM-300), 500 (VM-200), 500 (VM-100)
- جهاز/حجم جدول MAC: 2,500 (VM-300), 500 (VM-200), 500 (VM-100)
- حجم جدول IPv6 المجاور: 1,000 (VM-300), 500 (VM-200), 500 (VM-100)

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 التوقيع
- تقديم تحديث توقيع WildFire في أقل من ساعة مع دمج إنشاء السجلات/الإبلاغ؛ والوصول إلى واجهة برمجة التطبيقات (API) الخاصة بـ WildFire للإرسال البرنامجي لأكثر من 100 عينة يومياً وما يصل إلى 1,000 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)

- Microsoft Active Directory وNovell eDirectory وSun One وغيرها من الدلائل القائمة على LDAP.
- Microsoft Windows Server 2003/2008/2008r2 وMicrosoft Exchange Server 2003/2007/2010
- الخدمات الطرفية من Microsoft وCitrix XenApp
- 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 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 (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 لسياسات 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: (VM-100) 4 ,(VM-300, VM-200) 6

الوصول البعيد/SSL VPN (GLOBALPROTECT)

- بوابة GlobalProtect
- موقع GlobalProtect
- النقل: IPSec مع بديل SSL
- المصادقة: LDAP أو SecurID أو DB محلية
- نظام تشغيل العميل: Mac OS X 10.6، 10.7 (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 و4.0 Android والأحدث، VPNC IPSec لـ Linux

الإدارة، إعداد التقارير، أدوات الرؤية

- واجهة الويب المدمجة 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 سلسلة VM، برجاء زيارة www.paloaltonetworks.com/literature.

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

paloalto NETWORKS
the network security company™