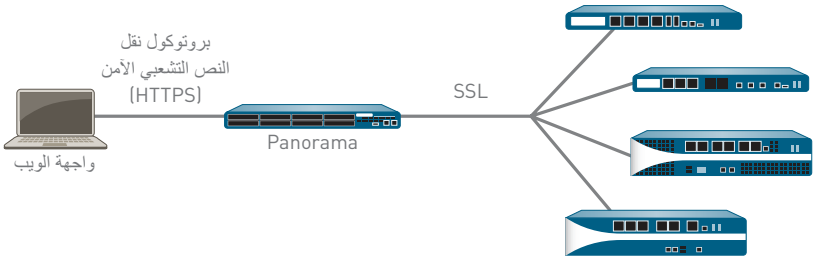
PANORAMA



توفر Panorama إدارة السياسات ولأجهزة مركزيا عبر شبكة جدران حماية من الجيل الجديد من شركة Palo Alto Networks™.

- عرض ملخص رسومي للتطبيقات الموجودة بالشبكة، والمستخدمين المعنيين، والتأثيرات الأمنية المحتملة.
- نشر سياسات الشركات مركزياً لاستخدامها بالاقتران مع السياسات المحلية لتحقيق أقصى قدر من المرونة.
- تفويض مستويات مناسبة من المراقبة الإدارية على مستوى الجهاز أو على الصعيد العالمي مع الإدارة القائمة على أساس الأدوار.
- التحليل والتحقيق وإعداد التقارير مركزيا حول معدل نقل البيانات داخل الشبكة وعن الحوادث الأمنية والتعديلات الإدارية.

عادة ما تحتوي المنظمات الكبيرة على العديد من جدران الحماية المنتشرة في جميع أنحاء شبكاتهم وفي أكثر الأحيان، تكون عملية إدارتها ومراقبتها عملية مرهقة للغاية بسبب التعقيدات والتناقضات بين الأجهزة الفردية. والنتيجة هي زيادة في الجهود الإدارية والتكاليف ذات الصلة.

توفر Panorama إدارة ورؤية مركزية للجيل الجديد من جدران الحماية من شركة Palo Alto Networks. فمن موقع مركزي، يمكن للمسئولين الحصول على معلومات حول التطبيقات والمستخدمين والمحتوى التي تمر عبر جدران الحماية. تزيد معرفة ما يحدث داخل الشبكة، مع وجود سياسات آمنة لتمكين التطبيقات، من الحماية والتحكم بينما يقلل من الجهود الإدارية. يمكن للمسؤولين أن يقوموا بشكل مركزي بإجراء التحليلات وإعداد التقارير وإجراء التحليلات الشرعية للبيانات التي يتم تجميعها على مر الوقت، أو للبيانات المخزنة على جدار الحماية المحلي.

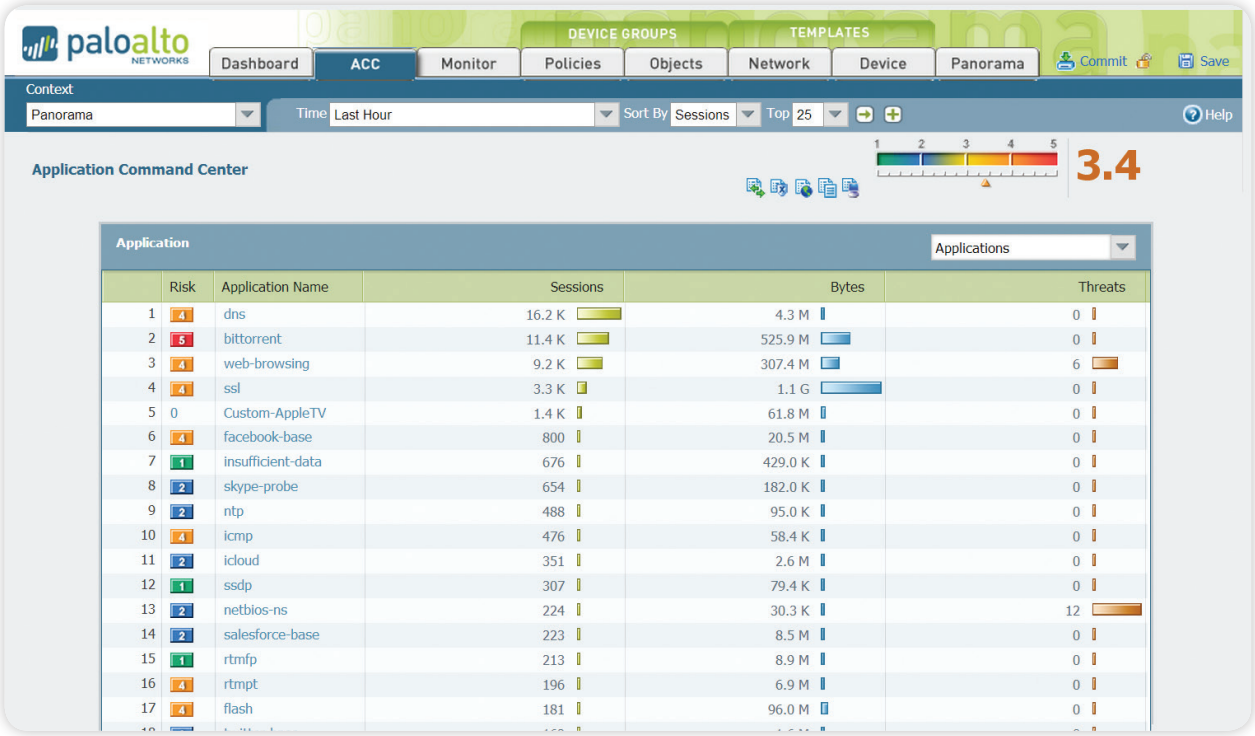
إن كلا من Panorama والأجهزة الفردية لها نفس الشكل والمظهر المستند إلى شبكة الإنترنت، مما يقلل من منحنى التعلم ويقلل كذلك من التأخير في تنفيذ المهمة الحالية. تلتزم شركة Palo Alto Networks بفلسفة الإدارة التي تؤكد على الاتساق، مما يوفر تفوقاً كبيراً على العروض التنافسية.

الرؤية المركزية: مركز قيادة التطبيقات

باستخدام مراقبة وقيادة التطبيقات (ACC) من Panorama سيوفر للمسؤول طريقة عرض رسومية للتطبيقات والـ URL والتهديدات والبيانات (الملفات والنماذج) في كافة أجهزة Palo Alto Networks التي يتم إدرتها. تجلب مراقبة وقيادة التطبيقات (ACC) البيانات بشكل ديناميكي من كل جهاز للتأكد من أن المسئولين لديهم أحدث عرض للتطبيقات في الشبكة، ومن يستخدم هذه الأجهزة والتهديدات المحتملة التي قد يشكلونها. يمكن للمسئولين فحص التطبيقات الجديدة أو غير المألوفة عن طريق نقرة واحدة والتي تعرض وصف للتطبيق وسماته الرئيسية وخصائصه السلوكية ومن يستخدمه.

توفر البيانات الإضافية حول التصنيفات والتهديدات الخاصة بـ URL صورة كاملة عن نشاط الشبكة. تسمح الرؤية المستمدة من مراقبة وقيادة التطبيقات (ACC) للمسئولين باتخاذ قرارات سياسية مستنيرة وتسمح لهم كذلك بالاستجابة السريعة للتهديدات الأمنية المحتملة.

paloalto NETWORKS
the network security company™



مركز قيادة التطبيقات: يوفر مركز قيادة التطبيقات طرق عرض محلية وعالمية لمعدل نقل بيانات التطبيقات، مع إمكانية التنقل للأسفل لمعرفة المزيد عن النشاط الحالي.

مراقبة السياسة العالمية: تمكين التطبيقات بأمان

يعني تمكين التطبيقات بأمان السماح الوصول إلى تطبيقات محددة ذات سياسات معينة مطبقة لمنع التهديدات وتصفية الملفات أو البيانات أو URL. تسهل Panorama التمكين الآمن للتطبيقات عبر شبكة جدران الحماية بالكامل عن طريق السماح للمسئولين بإدارة القواعد من موقع مركزي.

تساعد السياسات المشتركة القائمة على Panorama على ضمان الامتثال للمتطلبات الداخلية أو التنظيمية في حين أن قواعد الأجهزة المحلية تحافظ على الأمن والمرونة. حيث يمكن للجمع بين المراقبة الإدارية المركزية والمحلية على السياسات والأهداف المساعدة في تحقيق التوازن بين الأمن المتسق على المستوى العالمي وبين المرونة على المستوى المحلي.

يمكن للمسئولين نشر سياسات تتيح التمكين الآمن التطبيقات أو وظائف التطبيقات المعتمدة على المستخدمين عبر دمج خدمات الدليل في أثناء قيام البرامج المانعة للتهديدات محددة التطبيقات بحماية المحتوى والشبكة. إن القدرة على تحديد سياسة واحدة يمكنها تمكين التطبيقات بأمان المعتمدة على المستخدم – وليس عناوين الـ IP – تسمح للمؤسسات بالحد بشكل كبير من عدد السياسات المطلوبة. ويعد الانخفاض الكبير في الحمل الإداري المرتبط بإضافة ونقل وتغيير الموظفين، والذي قد يحدث بصورة يومية – تظل السياسات الأمنية مستقرة بينما ينتقل الموظفين من مجموعة إلى أخرى – هو أحد الفوائد المضافة من دمج خدمات الدليل.

مراقبة معدل نقل البيانات: التحليلات والتقارير والتحليلات الشرعية

تستخدم Panorama نفس المجموعة القوية لأدوات المراقبة والإبلاغ المتاحة على مستوى إدارة الأجهزة المحلية وتضيف الرؤية عن طريق توفير عرض مجمع للأنشطة. وحين يقوم المسئولين بإجراء استعلامات للسجلات وإنشاء تقارير، تسحب Panorama بشكل ديناميكي أحدث البيانات مباشرة من جدران الحماية المدارة أو من السجلات المرسلة إلى Panorama. يسمح الوصول إلى أحدث المعلومات عبر كافة الأجهزة للمسئولين بمعالجة الحوادث الأمنية فضلاً عن اتخاذ موقف استباقي لحماية أصول الشركة.

- **عارض السجلات:** بالنسبة للأجهزة الفردية، أو جميع الأجهزة، يمكن لمسئولي Panorama عرض أنشطة السجلات بسرعة باستخدام تصفية ديناميكية للسجلات عن طريق النقر على قيمة الخلية و/أو استخدام منشيء التعبيرات لتحديد معايير الفرز. يمكن حفظ النتائج للاستعلامات المستقبلية أو تصديرها لمزيد من التحليلات.
- **إنشاء التقارير المخصصة:** يمكن استخدام التقارير المعرفة مسبقاً كما هي أو تخصيصها أو تجميعها معاً كتقرير واحد من أجل ملائمة متطلبات معينة.
- **تقارير نشاط المستخدم:** من Panorama، يُظهر تقرير نشاط المستخدم، التطبيقات التي تم استخدامها وتصنيفات URL ومواقع الويب التي تم زيارتها وكافة عناوين URL التي تم زيارتها على مدى فترة من الوقت محددة للمستخدمين الفرديين. تنشيء Panorama تقارير باستخدام طريقة عرض مجمعة لنشاط المستخدم، بغض النظر عن جدار الحماية الذي يحمي هذه الأنشطة، أو نوع الـ IP أو الجهاز الذي يستخدمونه.

هيكل إدارة Panorama

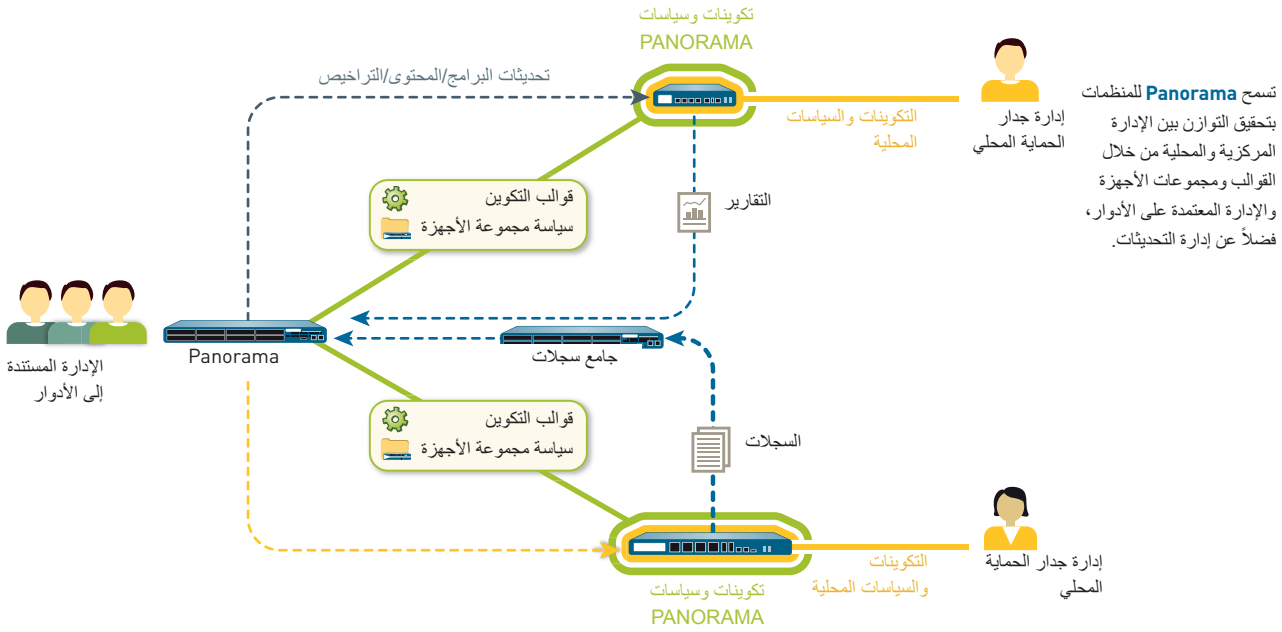
تُمكِّن Panorama المؤسسات من إدارة جدران الحماية من Palo Alto Net-works الخاصة بهم باستخدام نموذج يوفر كلاً من الإشراف المركزي والرقابة المحلية. توفر Panorama عدد من الأدوات للإدارة المركزية:

- **القوالب:** تدير Panorama تكوينات الأجهزة والشبكات المشتركة من خلال القوالب. يمكن استخدام القوالب لإدارة التكوينات بشكل مركزي ثم تطبيق التغييرات على كافة جدران الحماية التي يتم إدارتها. هذا النهج يعمل على تجنب تكرار نفس التغيير بجدار الحماية الفردي عبر العديد من الأجهزة. أحد الأمثلة على هذا الاستخدام هو تطبيق إعدادات خادم DNS و NTP المشتركة عبر مئات من جدران الحماية، بدلاً من تنفيذ نفس التغيير على جهاز تلو الآخر.
- **مجموعات الأجهزة:** تدير Panorama الأهداف والسياسات المشتركة من خلال مجموعات الأجهزة. تُستخدم مجموعات الأجهزة لإدارة أسس القواعد بشكل مركزي للعديد من الأجهزة ذات المتطلبات المشتركة. أحد الأمثلة على تجميع الأجهزة في مجموعات الأجهزة قد تكون حسب الناحية الجغرافية (مثل، أوروبا وأمريكا الشمالية) أو الناحية الوظيفية (مثل، المحيط أو مركز البيانات). يتم التعامل، داخل مجموعات الأجهزة، مع الأنظمة الافتراضية كأجهزة الفردية، عند نفس المستوى كجدار حماية فعلي. وهذا يسمح بمشاركة أساس القاعدة المشتركة عبر مختلف الأنظمة الافتراضية في الجهاز.

يمكن للمنظمات استخدام السياسات المشتركة للمراقبة المركزية مع الاستمرار في توفير مسئول جدار الحماية بالاستقلالية لإجراء تعديلات محددة للمتطلبات المحلية. في مستوى مجموعة الأجهزة، يمكن للمسئولين إنشاء سياسات مشتركة يتم تعريفها على أنها أول مجموعة من القواعد (قواعد أولية) وآخر مجموعة من القواعد (قواعد نهائية) ليتم تقييمها في مقابل معايير التطابق. يمكن عرض القواعد الأولية والنهائية على جدار الحماية الذي يتم إدارته، ولكن لا يمكن تعديلها إلا من Panorama ضمن سياق محتوى الأدوار الإدارية التي تم تعريفها. يمكن تعديل قواعد الجهاز المحلية (تلك التي بين القواعد الأولية والنهائية) بواسطة إما المسئول المحلي، أو بواسطة مسئول Panorama الذي قام بالتحويل إلى سياق جدار حماية محلي. وبالإضافة إلى ذلك، يمكن للمنظمة استخدام الأهداف المشتركة التي تم تعريفها بواسطة مسئول Panorama، والتي يمكن الرجوع إليها عن طريق قواعد الجهاز التي يتم إدارتها محليا.

- **الإدارة المستندة إلى الأدوار:** يمكن للمنظمات استخدام الإدارة المستندة إلى الأدوار لتفويض مستوى الوصول الإداري (مُمكن أو للقراءة فقط أو معطل ومخفى من العرض) للخاصية لموظفين مختلفين. يمكن إعطاء الحق لمسئولين محددين للوصول إلى المهام المتعلقة بعملهم مع جعل حق الوصول إلى مهام أخرى مخفية أو للقراءة فقط. أحد الأمثلة على الطريقة التي يمكن استخدام هذا النوع من التحكم في الوصول هي تحديد أدوار مختلفة للموظفين المسئولين عن مهام مختلفة عبر المؤسسة، مثل مدراء الأمن مقابل مدراء الشبكة. يتم تسجيل جميع التغييرات التي يقوم بها أي المسئول، حيث يظهر وقت وقوعها، **والمسئول، وواجهة الإدارة** المستخدمة (Web UI، CLI، Panorama)، والأمر أو الإجراء المتخذ.
- **إدارة تحديث البرمجيات والمحتوى والتراخيص:** وحيث تزداد عمليات النشر في الحجم، ترغب العديد من المنظمات في التأكد من أنه يتم إرسال التحديثات إلى مربعات انتقال البيانات من الخادم بطريقة منظمة. على سبيل المثال، قد تفضل فرق الأمن تأهيل تحديث البرنامج بشكل مركزي قبل أن يتم تسليمه عبر Panorama لكافة جدران حماية الإنتاج في آن واحد. باستخدام Panorama، يمكن إدارة عملية التحديث مركزياً لتحديث البرامج، والمحتوى (تحديث التطبيقات، وتوقيعات برامج مكافحة الفيروسات، وتوقيعات التهديدات وقاعدة بيانات تصفية URL، وغير ذلك) والتراخيص.

باستخدام القوالب ومجموعات الأجهزة والإدارة المستندة إلى الأدوار وإدارة التحديثات يمكن للمنظمات تفويض حق وصول مناسب لكافة وظائف الإدارة؛ ومنها أدوات الرؤية وإنشاء سياسة وإعداد التقارير والسجلات على المستويين العالمي والمحلي.



مرونة النشر

يمكن للمنظمات نشر Panorama سواء كجهاز مادي أو جهاز افتراضي.

جهاز مادي

إن المنظمات التي تفضل نشر Panorama كجهاز مادي مخصص عالي الأداء، أو ترغب في فصل إدارة Panorama ووظائف التسجيل لكميات كبيرة من بيانات السجلات، يمكنها استخدام الجهاز المادي M-100 لتلبية احتياجاتهم. يمكن نشر Panorama التي تعمل على جهاز M-100 بالطرق التالية:

- **مركزيا:** في هذا السيناريو، يتم توحيد جميع وظائف الإدارة والتسجيل في Panorama داخل جهاز واحد (مع خيار إمكانية التوافر العالي).
- **موزعا:** قد تفضل بعض المنظمات فصل وظائف الإدارة والتسجيل عبر أجهزة متعددة. وبموجب هذا التكوين، يتم تقسيم الوظائف بين المديرين وجامعي السجلات.
  - **مدير Panorama:** إن مدير Panorama مسئول عن التعامل مع المهام المرتبطة بتكوين السياسات والأجهزة في جميع الأجهزة التي يتم إدارتها. لا يقوم المدير بتخزيم بيانات السجلات محلياً، ولكنه يستخدم جامعي السجلات المنفصلة للتعامل مع بيانات السجل. يحلل المدير البيانات المخزنة في مجمعات السجلات لإعداد تقارير مركزية.
  - **جامع سجلات Panorama:** يمكن للمنظمات التي تمتلك تسجيلات ذات أحجام كبيرة ومتطلبات استبقاء نشر أجهزة جامع سجلات Panorama مخصصة والتي تعمل على تجميع معلومات السجلات من العديد من جدران الحماية التي يتم إدارتها.

إن الفصل بين الإدارة وجامع السجلات يُمكّن المنظمات من تحسين نشرها من أجل تلبية متطلبات القياس والمتطلبات التنظيمية والجغرافية.

جهاز افتراضي

يمكن نشر Panorama كجهاز افتراضي على VMware ESX(i)، مما يسمح للمنظمات بدعم مبادراتها الافتراضية ودمج مساحة الحامل التي تكون في بعض الأحيان محدودة أو مكلفة في مركز البيانات. يمكن نشر الجهاز الافتراضي بطريقتين:

- **مركزيا.** يتم توحيد جميع وظائف الإدارة والتسجيل في Panorama داخل جهاز افتراضي واحد (مع خيار إمكانية التوافر العالي).
- **موزعا:** تدعم مجموعة سجلات Panorama الموزعة مزيج من الأجهزة المادية والافتراضية.
  - **مدير Panorama:** يمكن أن يعمل الجهاز الافتراضي كمدير Panorama، وهو مسئول عن التعامل مع المهام المرتبطة بتكوين السياسات والأجهزة في جميع الأجهزة التي يتم إدارتها.
  - **جامع سجلات Panorama:** إن جامعات سجلات Panorama مسئولة عن تفريغ جامع السجلات المكثف ومعالجة المهام، ويمكن نشره باستخدام جهاز M-100. لا يمكن استخدام الجهاز الافتراضي كجامع سجلات Panorama.

إن توفير الاختيار بين المنصة المادية والافتراضية، فضلاً عن الاختيار بين جمع أو فصل وظائف Panorama، يوفر للمنظمات الحد الأقصى من المرونة لإدارة جدران حماية Palo Alto Networks متعددة ضمن بيئة الشبكات الموزعة.

مواصفات PANORAMA

عدد الأجهزة المدعومة	ما يصل إلى 1000
التوافر العالي	فعال/غير فعال
مصادقة المسئول	قاعدة بيانات محلية
	RADIUS

مواصفات جهاز الإدارة M-100

الإدخال/الإخراج

- (1) 10/100/1000، (3) 10/100/1000 (للاستخدام المستقبلي)، (1) منفذ تسلسلي DB9 لوحدة التحكم

التخزين (خياران)

- M-100 1 تيرابايت RAID: 2 x 1 تيرابايت RAID، وHDD معتمد لـ 1 تيرابايت بتخزين RAID
- M-100 4 تيرابايت RAID: 8 x 1 تيرابايت RAID، وHDD معتمد لـ 4 تيرابايت بتخزين RAID

مورد الطاقة/الحد الأقصى لاستهلاك الطاقة

- 500 واط/500 واط

الحد الأقصى للوحدة الحرارية البريطانية/ساعة

- 1705 وحدة حرارية بريطانية/ساعة

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 (MTBF)

Years 14.5

الحامل القابل للتركيب (الأبعاد)

- 1 وحدة، حامل قياسي 19 بوصة (ارتفاع 1.75 x عمق 23 x عرض 17.2 بوصة)

الوزن (الجهاز بشكل مستقل/عند الشحن)

- 26.7 رطل/يحدد لاحقاً رطل

السلامة

- شهادات UL، CUL، CB

EMI

- FCC فئة A وCE فئة A وVCCI فئة A

البيئة

- درجة حرارة التشغيل: من 40 إلى 104 درجة فهرنهايت، من 5 إلى 40 درجة مئوية
- درجة الحرارة أثناء عدم التشغيل: من -40 الى 149 درجة فهرنهايت، من -40 إلى 65 درجة مئوية

مواصفات الجهاز الافتراضي

الحد الأدنى لمواصفات الخادم

- قرص صلب 40 جيجابايت
- ذاكرة وصول عشوائي 4 جيجابايت
- Quad-Core CPU 2GHz+

دعم برنامج VMWARE

- VMware ESX، 4.1 الإصدار 7 أو أحدث

دعم المستعرض

- IE الإصدار 7 أو أحدث
- Firefox الإصدار 3.6 أو أحدث
- Safari الإصدار 5.0 أو أحدث
- Chrome الإصدار 11.0 أو أحدث

تخزين السجلات

- قرص افتراضي لـ VMware: حد أقصى 2 تيرابايت
- NFS

paloalto NETWORKS
the network security company™

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