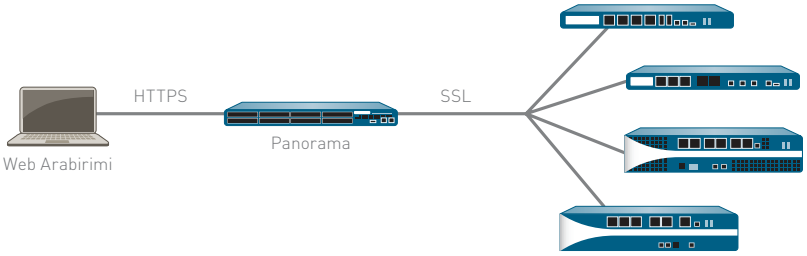
PANORAMA

Panorama, Palo Alto Networks'ün bir ya da birden çok yeni nesil güvenlik duvarı üzerinde merkezileştirilmiş politika ve cihaz yönetimi sağlar.

- Ağ üzerindeki uygulamaların, bunlarla ilgili kullanıcıların ve olası güvenlik etkilerinin grafiksel özeti görüntülenebilir.
- Kurumsal firewall güvenlik politikalarının, maksimum esneklik sağlamak amacıyla yerel politikalarla bağlantılı olarak kullanılabilecek şekilde merkezden dağıtılmasını sağlar.
- Rol tabanlı yönetim sayesinde yönetimsel kontrolün ilgili düzeylerin cihaz seviyesinde veya genel olarak atanmasını sağlayın.
- Ağ trafiğini, güvenlik olaylarını ve yönetimsel değişiklikleri merkezi olarak analiz, araştırma ve raporlama imkanı sunar.



Genel olarak büyük kuruluşların ağlarında birçok güvenlik duvarı kurulu bulunmaktadır ancak, çoğunlukla, ayrı cihazlar arasında oluşan uyuşmazlıklar ve karmaşık durumlar nedeniyle bunların yönetimi ve denetimi sorunlu olmaktadır. Bunun sonucunda da yönetimsel işlemlerde ve ilgili süreçlerde harcanan adam/saat gibi gizli maliyetlerde bir artış gözlenmektedir.

Panorama, Palo Alto Networks gelecek nesil güvenlik duvarlarının merkezileştirilmiş yönetimini ve izlenmesini sağlar. Yöneticiler merkezi bir konumdan uygulamalar, kullanıcılar ve güvenlik duvarlarından geçen içerikler hakkında bilgi edinebilir. Uygulamaların güvenli kullanımını sağlayacak olan politikaların devreye alınmasını sağlamanın yanısıra ağ üzerinde neler olup bittiği hakkında bilgi sahibi olmak, kontrol ve korumayı en üst seviyeye çıkartırken yönetimsel çabaları en aza indirmektedir. Yöneticiler zaman içinde merkezi konumda biriken veya yerel güvenlik duvarlarında depolanan verilerin analizini, raporlamasını ve vaka sonrası incelemelerini merkezi bir konumdan yapabilir.

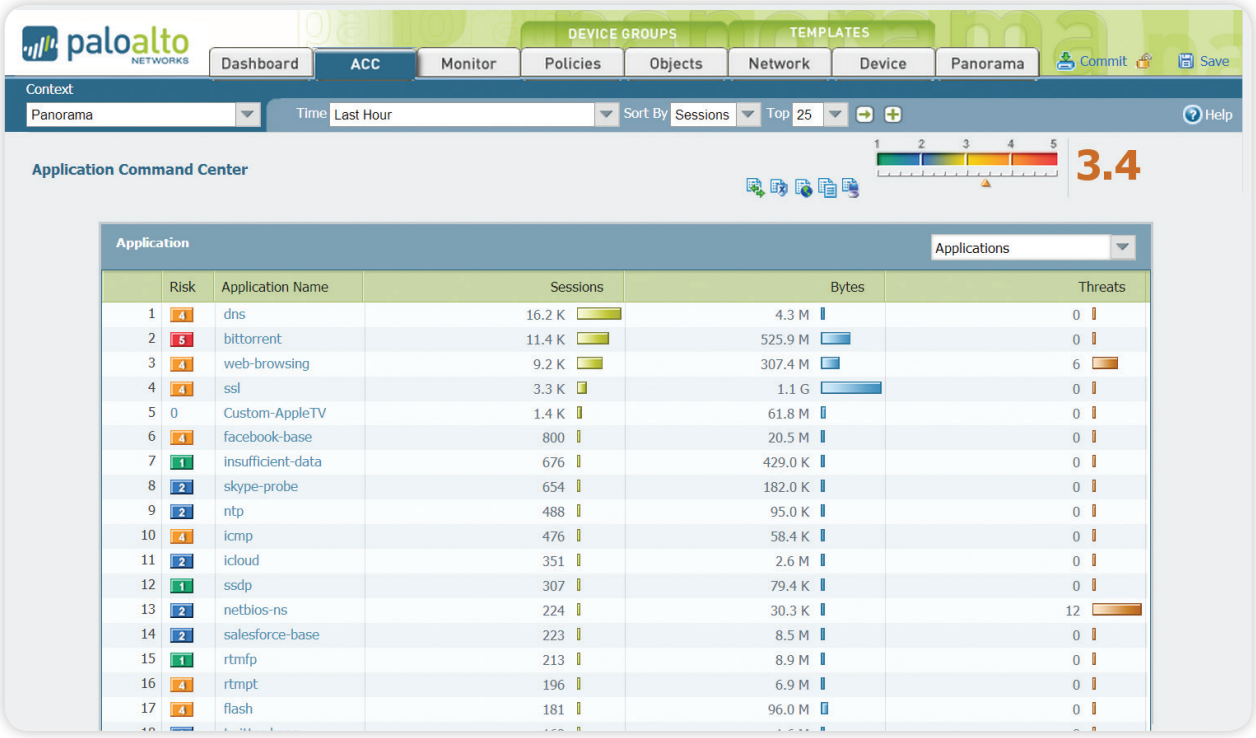
Hem Panorama hem de ayrı ayrı firewall sistemleri aynı web tabanlı görünümü ve kullanımı paylaştığından öğrenme eğrisi en aza indiği gibi, yapılacak işlerde gecikmeyi de önler. Palo Alto Networks, her kademede güvenlik politikalarının tutarlılığına önem veren bir yönetim felsefesine bağlı olduğundan rakiplerin sunduklarına kıyasla önemli avantajlar sağlamaktadır.

Merkezi Görünürlük: Uygulama Komuta Merkezi

Güvenlik yöneticisinin Panorama'nın Uygulama Komuta Merkezi'ni (Application Control Center, ACC) kullanması, yönetimindeki tüm Palo Alto Networks cihazları üzerindeki uygulamaların, URL'lerin, tehdit ve verilerin (dosyalar ve paternler) grafiksel bir görünümünü sağlar. ACC merkezi yönetim altındaki her cihazdan sürekli veri toplayarak güvenlik yöneticilerinin ağlarında dolaşan uygulamalardan, bunları kimlerin kullandığından ve bu uygulamaların beraberinde taşıdıkları olası tehditlerden güncel ve dinamik bir şekilde haberdar olmasını sağlar. Yöneticiler, tek bir tıklamayla söz konusu uygulamaların açıklamalarını, ana özelliklerini, karakteristik davranışlarını ve kimlerin kullandığını görerek yeni veya yabancısı oldukları uygulamaları derinlemesine araştırabilirler.

Erişilen URL kategorileri ve tespit edilen tehditler hakkındaki ilave bilgiler, ağ üzerindeki trafiğin tam bir özet resmini verir. ACC'nin sağladığı görünürlükle yöneticiler bilgiye dayanan politika kararları alabilir ve olası güvenlik tehditlerine daha çabuk yanıt verebilir.

paloalto NETWORKS
the network security company™



Uygulama Komuta Merkezi (ACC), mevcut ağ hareketleri hakkında daha fazla bilgi sahibi olmak için ayrıntılı drill-down kabiliyetleri ile birlikte uygulama trafiğinin yerel ve global görünümlerini sağlar.

Genel Politika Denetimi: Uygulamaları Güvenli Kılma

Uygulamaların güvenli kılınması, belirli uygulamalara erişimin, belirli tehditleri önlemiş olarak ve dosya, veri veya URL filtreleme politikaları uygulanmış olarak sağlanması anlamına gelir. Panorama, güvenlik yöneticilerin kuralları merkezi bir konumdan yönetmesini sağlayarak, uygulamaları güvenlik duvarı ağının bütününde güvenli bir şekilde etkinleştirebilmelerini kolaylaştıran bir bileşendir.

Panorama tabanlı paylaşılan politikalar, yerel cihaz kuralları güvenliği ve esnekliği sağlarken, kurum içi düzenlemelerle veya yasal düzenlemelerle uyum içinde olunmasına yardımcı olur. Politikalar ve nesneler üzerindeki merkezileştirilmiş kontrol imkanları ile yerel kontrol imkanlarının birleştirilmesi, global seviyede tutarlı güvenlikle yerel düzeydeki esneklik arasında bir denge oluşturulabilmesini sağlar.

Uygulamaya özgü tehdit önleme, içerikleri ve ağı korurken yöneticiler, dizin hizmetleri entegrasyonu üzerinden kullanıcıları esas alarak uygulamaların ve uygulama işlevlerinin güvenle etkinleştirilmesini sağlayan politikaların dağıtımını yapabilir. IP adresi yerine kullanıcı tabanlı olarak uygulamaların güvenli kılınmasını sağlayan tek bir politika belirleyebilme yeteneği, kurumlar için gerekli olan politika sayısını önemli ölçüde azaltmaktadır. Dizin hizmetlerinin entegrasyonunun getirdiği ek bir avantaj da, çalışan sayısının artması, çalışanların tayin olmaları veya görev değişiklikleri gibi hemen hergün karşılaşılabilecek durumlar ile güvenlikle ilgili yönetimsel iş yükünde önemli düşüşlere neden olmasıdır. Kullanıcılar bir gruptan diğerine geçtikleri durumda bile güvenlik politikaları aynı stabil hallerinde kalmaktadır.

Trafik İzleme: Analiz Etme, Raporlama ve Olay Sonrası İncelemeleri

Panorama, yerel cihaz yönetimi seviyesinde kullanılan güçlü izleme ve raporlama araçlarının aynısını kullanmanızı sağlar ve ağ üzerindeki hareketlerin toplu bir görünümünü sağlayarak detaylı bir görünürlük sunar. Yöneticiler log dosyaları sorgulamalarıyla raporlar oluştururken Panorama, geçerli verilerin çoğunu dinamik olarak doğrudan merkezi yönetim kontrolündeki güvenlik duvarlarından veya Panorama'ya iletilen log dosyalarından alır. Tüm cihazlardaki en son bilgilere erişimlerinin olması, yöneticilerin güvenlik olaylarına müdahale edebilmelerinin yanı sıra kurum varlıklarını korumak için etkileşimli bir pozisyon alabilmelerini de sağlar.

- **Log Dosyası Görüntüleyicisi:** Panorama yöneticileri tek bir cihaz veya tüm cihazlarla ilgili olarak sıralama ölçütlerini tanımlamak için bir hücre değerini ve/veya ifade oluşturucusunu tıklatıp dinamik günlük filtrelemesini kullanarak log etkinliklerini hızla görüntüleyebilir. Sonuçlar daha sonraki sorgulamalar için kaydedilebilir veya daha ayrıntılı analiz için dışa aktarılabilir.
- **Özel Raporlama:** Önceden tanımlanan raporlar, ihtiyaca göre, olduğu gibi, özelleştirilmiş biçimde veya birlikte gruplanarak tek bir rapor şeklinde kullanılabilir.
- **Kullanıcı Etkinliği Raporları:** Panorama'daki kullanıcı etkinliği raporu, kullanılan uygulamaları, ziyaret edilen URL kategorilerini, web sitelerini ve her kullanıcı için belirli bir zaman diliminde ziyaret edilen tüm URL'leri gösterir. Panorama, raporları hangi güvenlik duvarıyla korunduklarından ya da hangi IP adresini ya da cihazı kullandıklarından bağımsız olarak, kullanıcıların etkinliklerinin toplu görünümünden yararlanarak oluşturur.

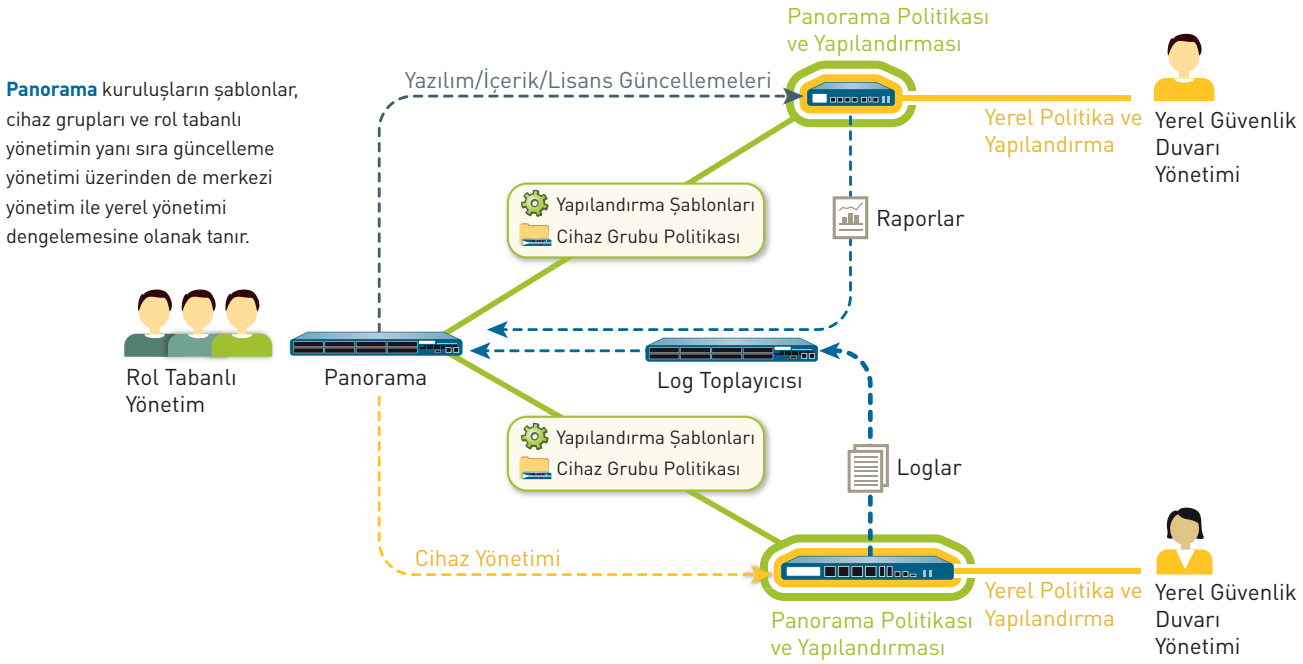
Panorama Yönetim Mimarisi

Panorama hem merkezi gözetim, hem de yerel denetim sağlayan bir model kullanarak kuruluşların Palo Alto Networks güvenlik duvarlarını yönetmelerine olanak tanımaktadır. Panorama merkezi yönetim için birçok araç sağlar:

- **Şablonlar:** Panorama ortak cihaz ve ağ yapılandırmalarını şablonlar üzerinden yönetir. Yapılandırmayı merkezi olarak yönetmek için şablonlar kullanılabilir ve ardından değişiklikler yönetilen tüm güvenlik duvarlarına dağıtılır. Bu yaklaşım, aynı güvenlik duvarı değişikliğinin tekrar tekrar birçok cihazda yinelenmesini önler. Bu tür kullanımın bir örneği, ortak DNS ve NTP sunucusu ayarlarının her cihazda tek tek gerçekleştirilmesi yerine yüzlerce güvenlik duvarına dağıtılmasıdır.
- **Cihaz Grupları:** Panorama, ortak politikaları ve nesneleri, cihaz grupları üzerinden yönetir. Ortak gereksinimleri olan birçok cihazın kural esaslarını merkezi olarak yönetmek için cihaz grupları kullanılır. Cihazların gruplandırılmasına örnek olarak coğrafi konumlarının (ör., Avrupa ve Kuzey Amerika) veya işlevlerinin (ör., dış çevre firewall'u veya veri merkezi firewall'u olmaları gibi) kullanılması gösterilebilir. Cihaz grupları içinde sanal sistemler, fiziksel güvenlik duvarlarıyla aynı düzeyde ayrı cihazlar olarak işlem görür. Bu, cihazdaki farklı sanal sistemler arasında ortak kural tabanının paylaşılmasını sağlar.

  Kuruluşlar, güvenlik duvarı yöneticisinin yerel gereksinimlere göre ayarlamalar yapabilmelerine olanak sağlarken, merkezi kontrol için paylaşılan politikaları kullanabilir. Cihaz grubu düzeyinde yöneticiler, ilk kurallar kümesi (kurallar öncesi) olarak tanımlanabilecek paylaşılan politikalar ve eşleşme ölçütlerine göre değerlendirilecek son kurallar kümesi (kurallar sonrası) oluşturabilirler. Kurallar öncesi ve sonrası, yönetilen güvenlik duvarında görüntülenebilir fakat yalnızca tanımlanmış idari roller bağlamında Panorama'dan düzenlenebilir. Yerel cihaz kuralları (kurallar öncesi ile sonrası arasındakiler) ya yerel yönetici ya da yerel güvenlik duvarı bağlamına geçirilmiş Panorama yöneticisi tarafından düzenlenebilir. Buna ilaveten bir kuruluş, yerelden yönetilen cihaz kurallarında kullanmak suretiyle, Panorama yöneticisi tarafından tanımlanmış paylaşılan nesneleri kullanabilir.
- **Rol Tabanlı Yönetim:** Kuruluşlar rol tabanlı yönetimi, çeşitli personele özellik düzeyinde yönetici erişimi (etkin, salt okunur, devre dışı ve görüntülenemez) atamak için kullanabilir. Belirli yöneticilere, bazı erişimler için görüntüleyemez veya salt okuyabilir erişimi sağlanırken işlerine ilişkin görevlere uygun erişimler verilebilir. Bu tür erişim denetiminin nasıl kullanılacağına örnek olarak, kuruluş genelinde farklı görevleri olan personele güvenlik yöneticisi veya ağ yöneticisi gibi farklı roller tanımlanması gösterilebilir. Yönetici tarafından yapılan tüm değişiklikler, yapıldıkları saati, yöneticiyi, kullanılan yönetim arabirimi (Web, UI, CLI, Panorama), komutu veya yapılan işlemi gösterir biçimde loglara kaydedilir.
- **Yazılım, İçerik ve Lisans Güncelleme Yönetimi:** Birçok kuruluş, organizasyonlarının boyutu büyüdükçe, güncellemelerin sahadaki kutularına düzenli bir biçimde gönderilmesini ister. Örneğin, güvenlik ekipleri bir yazılım güncellemesinin Panorama üzerinden tüm üretim güvenlik duvarlarına bir kerede dağıtılmasından önce merkezi olarak denetlemesini tercih edebilir. Panorama kullanılarak güncelleme süreci, yazılım güncellemeleri, içerik (uygulama güncellemeleri, antivirüs imzaları, tehdit imzaları, URL filtreleme veri tabanı, vs) ve lisanslar merkezi olarak yönetilebilir.

Kuruluşlar; şablonları, cihaz gruplarını, rol tabanlı yönetimi ve güncelleme yönetimini kullanarak, uygun erişim yetkilerini, görselleştirme araçlarını, politika oluşturma, hem genel hem yerel düzeyde raporlama ve log dosyalarına kaydetme gibi tüm yönetim işlevlerini ihtiyaçlarına göre ilgili kişilere delege edebilirler.



Dağıtım Esnekliği

Kuruluşlar Panorama'yı donanımsal appliance veya sanal appliance olarak dağıtabilir.

Donanımsal Appliance

Panorama'yı yüksek performanslı ayrılmış donanım olarak dağıtmayı tercih eden veya Panorama yönetimini ve büyük hacimleri loga kaydetme işlevlerini ayırmak isteyen kuruluşlar, gereksinimlerini karşılamak için M-100 donanımsal appliance kullanabilir. M-100'de çalışan Panorama aşağıdaki yollarla dağıtılabilir:

- **Merkezi olarak:** Bu senaryoda bütün Panorama yönetimi ve log kaydetme işlevleri tek bir cihazda birleştirilir (yüksek kullanılabilirlik seçeneğiyle).
- **Dağıtılmış olarak:** Kurumlar yönetim ve log kaydetme işlevlerini birden fazla cihaza ayırmak isteyebilir. Bu yapılandırmada işlevler yönetici appliance'lar ile log toplayıcı appliance'lar arasında ayrılır.
  - **Panorama Yöneticisi:** Panorama yöneticisi, yönetilen cihazların tümünde politika ve cihaz yapılandırmasına ilişkin görevlerin yapılmasından sorumludur. Yönetici appliance log verilerini yerel olarak depolamaz ve bunun yerine log verilerinin işlenmesi için ayrı log toplayıcı appliance'lar kullanır. Yönetici appliance, merkezi raporlama için log toplayıcılarda depolanan verileri analiz eder.
  - **Panorama Log Toplayıcısı:** Log kayıt hacmi yüksek ve bunları uzun süre depolama gereksinimi olan kuruluşlar, yönetilen birden fazla güvenlik duvarından alınan log bilgilerini toplayan adanmış Panorama log toplayıcısı cihazlarının dağıtımını yapabilir.

Yönetimle log toplamanın ayrılması, kuruluşların ölçeklenebilirlik, kurumsal veya coğrafi gereksinimlerini karşılamak için dağıtımları optimize edebilmesine olanak sağlar.

Sanal Araç

Kuruluşların sanallaştırma insiyatiflerini desteklemelerine ve veri merkezlerinde bazen sınırlı ve pahalı olabilen raf alanını birleştirmelerine olanak sağlamak için Panorama, VMware ESX(i) üzerinde sanal araç olarak dağıtılabilir. Sanal appliance iki yolla dağıtılabilir:

- **Merkezi olarak.** Bütün Panorama yönetimi ve log kaydetme işlevleri tek bir sanal araçta birleştirilir (yüksek kullanılabilirlik seçeneğiyle).
- **Dağıtılmış olarak:** Panorama log toplayıcı, donanımsal ve sanal appliance'ların karışımını destekler.
  - **Panorama Yöneticisi:** Sanal appliance Panorama yöneticisi olarak hizmet verebilir ve yönetilen cihazların tümünde politika ve cihaz yapılandırmasına ilişkin görevlerin yapılmasından sorumludur.
  - **Panorama Log Toplayıcısı:** Panorama log toplayıcıları yoğun log toplamanın yükünü azaltmaktan ve görevlerin yerine getirilmesinden sorumludur ve M-100 kullanılarak dağıtılabilir. Sanal appliance Panorama log toplayıcısı olarak kullanılamaz.

Panorama işlevlerini birleştirme veya ayırma seçeneğinin yanı sıra donanım veya sanal platform seçeneği sunmak kuruluşlara, dağıtılmış ağ ortamındaki birden fazla Palo Alto Networks güvenlik duvarının yönetilmesinde maksimum esneklik sağlamaktadır.

PANORAMA ÖZELLİKLERİ

Desteklenen cihaz sayısı	1.000 adete kadar
Yüksek Kullanılabilirlik	Aktif/Pasif
Yönetici doğrulaması	Yerel veri tabanı
	RADIUS

M-100 MERKEZİ YÖNETİM APPLIANCE ÖZELLİKLERİ

I/O

- (1) 10/100/1000, (3) 10/100/1000 (ileride kullanılmak için), (1) DB9 Konsolu seri bağlantı noktası

DEPOLAMA (2 SEÇENEK)

- M-100 1TB RAID: 1TB RAID Depolama için 2 x 1TB RAID Onaylı HDD
- M-100 4TB RAID: 4TB RAID Depolama için 8 x 1TB RAID Onaylı HDD

GÜÇ KAYNAĞI/MAKSİMUM GÜÇ TÜKETİMİ

- 500 W/500 W

MAKSİMUM BTU/SA

- 1.705 BTU/sa

GİRİŞ VOLTAJI (GİRİŞ FREKANSI)

- 100-240 VAC (50-60 Hz)

MAKSİMUM AKIM TÜKETİMİ

- 10 A'da 100 VAC

MTBF

14,5 yıl

RAFA YERLEŞTİRİLME BOYUTLARI

- 1U, 48,3 cm standart raf (Y 4,5 cm x D 58,4 cm x G 44 cm)

AĞIRLIK (TEK BAŞINA CİHAZ/TESLİM EDİLDİĞİ GİBİ)

- 12,1kg/ 15,9 kg

GÜVENLİK

- UL, CUL, CB

EMI

- FCC A Sınıfı, CE A Sınıfı, VCCI A Sınıfı

ORTAM

- Çalışma sıcaklığı 5 - 40 C
- Çalışmama sıcaklığı: -40 - -65 C

SANAL APPLIANCE ÖZELLİKLERİ

MİNİMUM SUNUCU GEREKSİNİMLERİ

- 40 GB Sabit Sürücü
- 4 GB RAM
- Quad-Core CPU (2GHz+)

VMWARE DESTEĞİ

- VMware ESX 4.1 veya daha yenisi

TARAYICI DESTEĞİ

- IE v7 veya daha yenisi
- Firefox v3.6 veya daha yenisi
- Safari v5.0 veya daha yenisi
- Chrome v11.0 veya daha yenisi

LOG DEPOLAMA

- VMware Sanal +Disk: 2TB maksimum
- 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