PA-4000 Series

PA-4000 Series Yeni Nesil Güvenlik Duvarı Temel Özellikleri:

HER PORTTAN HER UYGULAMAYI HER ZAMAN APP-ID™ İLE SINIFLANDIRMA

- Port, protokol, şifreleme (SSL veya SSH) ya da yaygın olarak kullanılan koruma atlatma tekniklerinden bağımsız olarak uygulama tespiti.
- Güvenli ağ ve uygulama erişimini sağlayacak politika temelli karar mekanizlarında ana unsur olarak port değil, uygulamayı kullanma imkanı: izin ver, reddet, zamanla, incele, trafik şekillendirmesini uygula.
- Tanınmayan uygulamaları politika kontrol, forensics amaçlı analiz, özelleştirilmiş App-ID oluşturma veya App-ID geliştirmesi için paket yakalama (packet capture) amaçlı olarak kategorize edebilme imkanı.

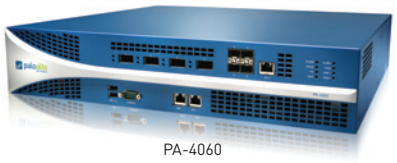
USER-ID VE GLOBALPROTECT SAYESİNDE, GÜVENLİ UYGULAMA ERİŞİMİNİ MÜMKÜN KILAN POLİTİKALARIN HERHANGİ BİR LOKASYONDAKİ HERHANGİ BİR KULLANICI İÇİN BİLE UYGULANABİLECEK ŞEKİLDE GENİŞLETİLEBİLMESİNİ SAĞLAYABİLME.

- Active Directory, LDAP, eDirectory Citrix ve Microsoft Terminal Servisleri ile ajansız entegrasyon.
- XML API kullanarak NAC, 802.1X kablosuz ve diğer standart dışı kullanıcı depolama sistemleri ile entegrasyon.
- Microsoft Windows, Mac OS X, Linux, Android veya iOS platformlarını kullanan yerel ve uzak kullanıcılara loaksyondan bağımsız eşdeğer seviyede güvenlik politikası dağıtma imkanı.

CONTENT-ID™ VE WILDFIRE™ İLE İSTER BİLİNEN İSTER BİLİNMEYEN OLSUN, TÜM TEHDİTLERE KARŞI KORUNMA.

- Hangi yaygın kullanılan güvenlik atlatma taktiği kullanılırsa kullanılsın, tüm portlardan akan trafik için, açıklardan yararlanma, kötücül yazılım ve casus yazılım dahil olmak üzere birçok bilinen tehdidi engelleyin.
- Dosyaların ve hassas verilerin izinsiz aktarımını engelleyin ve iş amaçlı olmayan internette aktivitesini denetim altına alın.
- 100'den fazla kötü amaçlı davranışı analiz ederek bilinmeyen zararlı yazılımları tespit etme ve otomatik olarak imza oluşturup bir sonraki ilk antivirus güncellemesinde koruma sağlama.

paloalto NETWORKS
the network security company™


PA-4060


PA-4050


PA-4020

Palo Alto Networks™ PA-4000 Series, hepsi de yüksek hızlı internet ağ geçidi ihtiyacı olan kurumları hedefleyen, PA-4060, PA-4050 ve PA-4020 adlı üç yüksek hızlı performans platformundan oluşmaktadır. PA-4000 Series, ağ iletişimi, güvenlik, tehdit önleme ve yönetim ana işlev alanları için adanmış işlem ve bellek kullanarak 10 Gbps değerine kadar throughput üretir.

Yüksek hızlı backplane ayrı ayrı veri ve denetim kartlarına bölünmüş olduğundan trafik yüküne bağlı olmaksızın her zaman yönetim erişimi sağlanabilmektedir. PA-4000 serisi yeni nesil güvenlik duvarının ana öğesi, App-ID, User-ID, Content-ID, GlobalProtect ve WildFire kullanarak kurumların güvenli uygulama erişimine sahip olmasını sağlayan güvenlik odaklı ve özel bir güçlendirilmiş işletim sistemi olan PAN-OS™ işletim sistemidir.

PERFORMANS VE KAPASİTE DEĞERLERİ[1]	PA-4060	PA-4050	PA-4020
Güvenlik duvarı throughput (App-ID etkin)	10 Gbps	10 Gbps	2 Gbps
Tehdit önleme throughput	5 Gbps	5 Gbps	2 Gbps
IPSec VPN throughput	2 Gbps	2 Gbps	1 Gbps
Saniyedeki yeni oturum sayısı	60.000	60.000	60.000
Maksimum eşzamanlı oturum sayısı	2.000,000	2.000,000	500.000
IPSec VPN tüneli/tünel arayüzleri	4000	4000	2000
GlobalProtect (SSL VPN) eş zamanlı kullanıcı	10.000	10.000	5000
SSL şifre çözme oturumu	23.000	23.000	7500
Geliş yönlü SSL sertifikalar	300	300	25
Sanal yönlendiriciler	125	125	20
Sanal sistemler (baz/maksimum[2])	25/125	25/125	10/20
Güvenlik bölgeleri	500	500	80
Maksimum politika sayısı	20.000	20.000	10.000

[1] Performans ve kapasiteler PAN-OS 5.0 kullanılarak ideal test koşullarında ölçülmektedir.

[2] Baz miktara sanal sistemlerin eklenebilmesi için ayrı lisans satın alınmalıdır.

PA-4000 Series yeni nesil güvenlik duvarı özelliklerinin daha detaylı ve tam bir açıklaması için www.paloaltonetworks.com/literature adresini ziyaret edebilirsiniz.

DONANIM ÖZELLİKLERİ

I/O PORT SAYISI

- PA-4060: (4) 10 Gigabit XFP, (4) Gigabit SFP
- PA-4050, PA-4020: (16) 10/100/1000, (8) Gigabit SFP

YÖNETİM AMAÇLI I/O PORT SAYISI

- (2) 10/100/1000 yüksek erişebilirlik, (1) 10/100/1000 bant dışı yönetim, (1) DB9 konsol bağlantı noktası

DEPOLAMA KAPASİTESİ

- 160 GB HDD

GÜÇ KAYNAĞI (ORTALAMA/MAKSİMUM GÜÇ TÜKETİMİ)

- Yedekli 400 W AC (175 W/200 W)

MAKSİMUM BTU/SA

- 682

GİRİŞ VOLTAJI (GİRİŞ FREKANSI)

- 100-240 VAC (50-60 Hz)

MAKSİMUM AKIM TÜKETİMİ

- 2,5 A'de 100 VACc

MTBF

- 7,18 yıl

MAKSİMUM ANİ AKIM TÜKETIMI

- 50 A'de 230 VAC; 30 A'de120 VAC

RAF YERLEŞTİRME BOYUTLARI

- 2U, 48,3 cm standart raf (Y 9 cm x D 42 cm x G 44,5 cm)

AĞIRLIK (TEK BAŞINA CİHAZ/TESLİM EDİLDİĞİ GİBİ)

- 15 kg/18 kg

GÜVENLİK

- UL, CUL, CB

EMI

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

SERTİFİKASYONLAR

- FIPS 140 Düzey 2, Genel Ölçütler EAL2, ICSA, UCAPL

ORTAM

- Çalışma sıcaklığı 0 - 50 C
- Çalışmama sıcaklığı -20 - 70 C

AĞ İLETİŞİMİ

ARAYÜZ MODLARI:

- L2, L3, Tap Mod (sniffer), Sanal Kablo (saydam mod)

YÖNLENDİRME

- Modlar: OSPF, RIP, BGP, Statik
- Yönlendirme tablosu boyutu (cihaz başına/VR başına girdi sayısı): 20.000/20.000 (PA-4060, PA-4050), 10.000/10.000 (PA-4020)
- Politika tabanlı yönlendirme
- Ethernet üzerinden Noktadan Noktaya İletişim (PPPoE)
- Jumbo çerçeveler: Maks çerçeve boyutu 9210 bayt
- Multicast Yönlendirme: PIM-SM, PIM-SSM, IGMP v1, v2 ve v3

YÜKSEK ERİŞİLEBİLİRLİK

- Modlar: Aktif/Aktif, Aktif/Pasif
- Arıza algılaması: Yol izleme, ağ arayüz izleme

ADRES ATAMASI

- Cihaz için adres ataması: DHCP İstemci/PPPoE/Statik
- Kullanıcılar için adres ataması: DHCP Sunucusu/DHCP Aktarıcısı/Statik

IPV6

- L2, L3, Tap Mode, sanal kablo (saydam mod)
- Özellikler: App-ID, User-ID, Content-ID, WildFire ve SSL şifre çözme

VLAN'LAR

- Cihaz başına 802.1q VLAN etiketi/arabirim başına: 4094/4094
- Maksimum arayüz sayısı: 4096 (PA-4060, PA-4050), 2.048 (PA-4020)
- Birleştirilmiş (aggregated) ağ arayüzleri (802.3ad)

NAT/PAT

- Maksimum NAT kuralı: 4000 (PA-4060, PA-4050), 1.000 (PA-4020)
- Maksimum NAT kuralı (DIPP): 250 (PA-4060, PA-4050), 200 (PA-4020)
- Dinamik IP ve port havuzu: 254
- Dinamik IP havuzu: 16.234
- NAT Modları: 1:1 NAT, n:n NAT, m:n NAT
- DIPP çoklu kullanım (oversubscription) (her bir kaynak port ve IP başına benzersiz hedef IP'leri): 8 (PA-4060, PA-4050), 4 (PA-4020)
- NAT64

SANAL KABLO

- Maksimum sanal kablo: 2.048 (PA-4060, PA-4050), 1.024 (PA-4020)
- Sanal kablolarla eşleştirilen arabirim türleri: fiziksel ve alt arabirimler

L2 İLETİM

- Cihaz başına ARP tablosu boyutu: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- Cihaz başına MAC tablosu boyutu: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- IPv6 komşuluk tablosu boyutu: 5000 (PA-4060, PA-4050), 2000 (PA-4020)

GÜVENLİK

GÜVENLİK DUVARI

- Uygulamaların, kullanıcıların ve içeriğin politika tabanlı denetimi
- Parçalanmış (fragmented) paket koruması
- Keşif taraması koruması
- Hizmet Reddi (DoS)/Dağıtılmış Hizmet Redleri (DDoS) koruması
- Şifre Çözme: SSL (giriş yönünde ve çıkış yönünde), SSH

WILDFIRE

- Hedefli ve bilinmeyen dosyaları 100'den fazla kötü amaçlı davranışa karşı tarama ve 0ncı gün ataklarına yönelik tespit
- Yeni bulunan zararlı yazılımlara karşı imza güncellemeleri sayesinde koruma üretilmesi ve otomatik olarak dağıtılması
- 1 saatten daha az sürede imza güncellemesi; entegre günlükleme (loglama)/raporlama; günde 100 örneğe kadar dosya yükleme imkanı ve günde 1000 adede kadar dosya hash değeri bazlı rapor sorgulama imkanı sağlayan WildFire API erişimi (Abonelik Gerektirir)

DOSYA VE VERİ FİLTRELEME

- Dosya aktarımı: 60'tan fazla farklı dosya türünde iki yönlü denetim
- Veri aktarımı: CC# ve SSN değerlerinin izinsiz aktarımında iki yönlü denetim
- Drive-by-download koruması

KULLANICI ENTEGRASYONU (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One ve diğer LDAP tabanlı dizinler
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Hizmetleri, Citrix XenApp
- Standart dışı kullanıcı depolarıyla tümleştirmeyi sağlamak için XML API

IPSEC VPN (SITE-TO-SITE)

- Anahtar Değişimi: Manüel anahtar, IKE v1
- Şifreleme: 3DES, AES (128 bit, 192 bit, 256 bit)
- Kimlik Doğrulaması: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dinamik VPN tüneli oluşturma (GlobalProtect)

TEHDİT ÖNLEME (ABONELİK GEREKTİRİR)

- Uygulama ve işletim sistemi güvenlik açıklarından yararlanma koruması
- Virüslere (HTML, Javascript, PDF'lere katıştırılmış olanlar ve sıkıştırılmışlar dahil), casus yazılımlara, solucanlara karşı akış tabanlı koruma

URL FİLTRELEME (ABONELİK GEREKTİRİR)

- Ön-tanımlı ve özelleştirilebilir URL kategorileri
- En son erişilen URL'ler için cihaz üzerinde önbellekleme
- SSL/SSH decryption, QoS, erişim kontrol gibi çeşitli güvenlik politikaları için eşleşme ölçütlerinin bileşeni olarak URL kategorisi
- Internet üzerinde dolaşım (browse) süresi bilgileri

HİZMET KALİTESİ (QOS)

- Uygulamaya, kullanıcıya, kaynağa, hedefe, arabirime, IPSec VPN tüneline ve daha pek çok şeye göre ilke tabanlı trafik şekillendirmesi
- Garanti edilen, maksimum ve öncelikli bant genişliği parametreleriyle 8 trafik sınıfı
- Gerçek zamanlı bant genişliği izleme
- Politika tabanlı Diffserv işaretleme
- QoS için desteklenen fiziksel arabirimler: 12

SSL VPN/UZAK ERİŞİM (GLOBALPROTECT)

- GlobalProtect Ağ Geçidi
- GlobalProtect Portalı
- Taşıma: SSL geri dönüşüyle IPSec
- Kimlik Doğrulaması: LDAP, SecurID veya yerel DB
- İstemci İşletim Sistemi: Mac OS X 10.6, 10.7 (32/64 bit), 10.8 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Üçüncü taraf istemci desteği: Apple iOS, Android 4.0 ve daha yenisi, Linux için VPNC IPSec

YÖNETME, RAPORLAMA, GÖRÜNÜRLÜK ARAÇLARI

- Tümleşik web arabirimi, CLI veya merkezi yönetim (Panorama)
- Çok dilli kullanıcı arabirimi
- Syslog ve SNMP v2/v3
- XML tabanlı REST API
- Uygulamaların, URL kategorilerinin, tehditlerin ve verilerin (ACC) grafik özeti
- Trafik, tehdit, WildFire, URL ve veri filtreleme günlük dosyalarını görüntüleme, filtreleme ve dışa aktarma
- Tam olarak özelleştirilebilir raporlama

PA-4000 Series yeni nesil güvenlik duvarı özelliklerinin daha detaylı ve tam bir açıklaması için www.paloaltonetworks.com/literature adresini ziyaret edebilirsiniz.

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