VM-Series

VM-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.

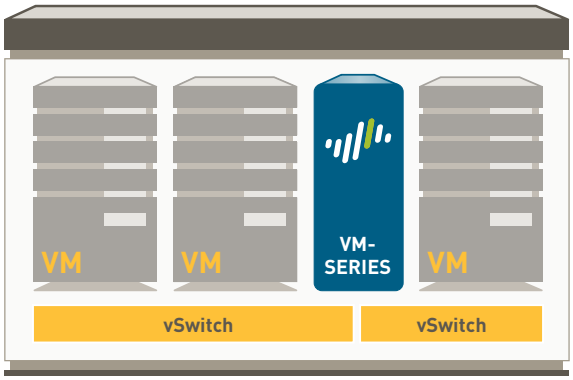
- Active Directory, LDAP, eDirectory Citrix ve Microsoft Terminal Servisleri ile ajansız entegrasyon.
- XML API kullanarak NAC, kablosuz ve diğer standart dışı kullanıcı depolama sistemleri ile entegrasyon.
- Microsoft Windows, Mac OS X, Linux, Android veya iOS platformlarını kullanan yerel ve uzak kullanıcılara 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™



VM-Series Virtual Firewall

Palo Alto Networks™ VM-Series, sunduğu dinamik adres nesneleri sayesinde kurumsal firewall güvenlik politikalarının yer değiştiren sanal makinelere göre dinamik olarak adapte edilmesi ve güçlü bir XML yönetim API sayesinde orkestrasyon sistemlerine entegrasyon gibi sanallaştırmaya ilişkin ana güvenlik sorunlarını çözerken güvenli uygulama kullanımını sanal ortamlara taşır:

VM-Series, veri merkezi ortamlarında gecikme süresini en aza indirmek için tek geçişli yazılım mimarisi kullanan yüksek performanslı 3 modelden oluşur: VM-100, VM-200 ve VM-300. Trafik yükü ne olursa olsun her zaman yönetim erişiminin olması amacıyla kullanıcıların her birine adanmış CPU'lar atayabilmeleri için yönetim ve veri kartları ayrılmıştır. VM-Series 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

GENEL KAPASİTE DEĞERLERİ[1]	VM-300	VM-200	VM-100
Maksimum oturum sayısı	250,000	100,000	50,000
IPSec VPN tüneli/tünel arabirimleri	2,000	500	25
GlobalProtect (SSL VPN) eş zamanlı kullanıcı sayısı	500	200	25
SSL şifre çözme oturumu	1024	1024	1024
Geliş yönlü SSL sertifikalar	25	25	25
Sanal yönlendiriciler	3	3	3
Güvenlik bölgeleri	40	20	10
Maksimum politika sayısı	5,000	2,000	250
Adres nesneleri	10,000	4,000	2,500
PERFORMANS[1]			
Güvenlik duvarı throughput (App-ID Etkin)	1 Gbps		
Tehdit önleme throughput	600 Gbps		
IPSec VPN throughput	250 Gbps		
Saniye başına yeni oturum	8,000 Gbps		

[1] Performans ve kapasiteler PAN-OS 5.0 ve 8 CPU çekirdekleri kullanılarak ideal test koşullarında ölçülmektedir.

SANALLAŞTIRMA	VM-300 VM-200 VM-100
HyperVisor	VMware ESXi 4.1 ve ESXi 5.0
Ağ sürücüsü	VMXNet3
CPU çekirdekleri	2, 4 veya 8
Bellek (Minimum)	4GB
Disk sürücü kapasitesi (Minimum/Maksimum)	40 GB/2 TB

AĞ İLETİŞİMİ

ARAYÜZ MODLARI:

- L2, L3, Tap Mod, Sanal kablo (saydam mod)

YÖNLENDİRME

- Modlar: OSPF, RIP, BGP, Statik
- Yönlendirme tablosu boyutu (cihaz/VR başına girdi sayısı): 1000/1000
- Politika tabanlı yönlendirme
- Multicast yönlendirme: PIM-SM, PIM-SSM, IGMP v1, v2 ve v3

YÜKSEK ERİŞİLEBİLİRLİK

- Modlar: Oturum eşitlemesi olmadan 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, virtual wire (transparent mode)
- Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption

VLAN'LAR

- Cihaz/arayüz başına 802.1q VLAN etiketi: 4.094/4.094
- Maksimum arayüz sayısı: 1024 (VM-300), 288 (VM-200), 100 (VM-100)

NAT/PAT

- Maksimum NAT kuralı: 1.000 (VM-300), 1.000 (VM-200), 125 (VM-100)
- Maksimum NAT kuralı (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- Dinamik IP ve port havuzu: 254
- Dinamik IP havuzu: 32.000
- NAT Modları: 1:1 NAT, n:n NAT, m:n NAT
- DIPP çoklu kullanım (oversubscription) (Kaynak port ve IP başına benzersiz hedef IP'leri): 2
- NAT64

SANAL KABLO

- Maksimum sanal kablo: 500 (VM-300), 100 (VM-200), 40 (VM-100)
- Sanal kablolarla eşleştirilen arabirim türleri: fiziksel ve alt arabirimler

L2 İLETİM

- Cihaz başına ARP tablosu boyutu: 1.000 (VM-300), 500 (VM-200), 500 (VM-100)
- Cihaz başına MAC tablosu boyutu: 1.000 (VM-300), 500 (VM-200), 500 (VM-100)
- IPv6 komşuluk tablosu boyutu: 1.000 (VM-300), 500 (VM-200), 500 (VM-100)

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 WildFire imza güncellemesi; entegre günlükleme (loglama)/raporlama; günde 100 örneğe kadar dosya yükleme imkanı ve günde 1.000 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: 6 (VM-300, VM-200), 4 (VM-100)

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, Netflow v9 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

VM-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