PA-5400 Serisi

Palo Alto Networks ML (Makine Öğrenimi) - Destekli PA-5400 Serisi

PA-5430, PA-5420 ve PA-5410 'dan oluşan NGFW 'ler yüksek hızdaki veri merkezleri, internet ağ geçitleri ve servis sağlayıcıların konumlandırması için idealdir. PA-5400 Serisinde yer alan cihazlar kriptolu trafik dahil olmak üzere trafiğin tamamını güvence altına alır.

Öne Çıkan Özellikler

- Dünyanın ilk ML- Destekli NGFW ürünü
- Ağ Güvenlik Duvarları kategorisinde Gartner Magic Quadrant™ 'da 10 kez Lider olarak gösterilmiştir.
- Forrester Wave™ tarafında Kurumsal Güvenlik Duvarları alanında Q3 2020 'de Lider olarak gösterilmiştir.
- 2019 NSS Laboratuvarları NGFW Test Raporunda söz konusu cihaz serisine en yüksek Güvenlik Etkinlik Puanı verilmiştir. (Evasion (atlatma) tekniklerinin %100 'ünün engellenmiş olması nedeniyle)
- Servis sağlayıcıların ve kurumların 5G Dönüşümünü ve Çok Erişimli Uç Bilgi İşleme Sürecini (MEC) korumak adına oluşturulmuş 5G 'ye özgü bir güvenlik tesis etmektedir.
- Ek sensörlere gerek duyulmaksızın, yönetilmeyen IoT cihazları da dahil olmak üzere, görünürlüğü ve güvenliği tüm cihazları kapsayacak şekilde genişletmektedir.
- Aktif/ Aktif ve Aktif/ Pasif Mod seçenekleriyle yüksek - kullanılabilirlik (HA) sağlamaktadır.
- Güvenlik hizmetleri ile öngörülebilir performans sağlar.
- Panorama™ Ağ Güvenliği Yönetimi ile merkezi yönetimi destekler.

Dünyanın ilk ML- Destekli Yeni Nesil Güvenlik Duvarı (NGFW), bilinmeyen tehditleri önlemenize, IoT dahil tüm cihazları görmenize, güvence altına almanıza ve otomatik politika önerileriyle hataları azaltmanıza olanak tanımaktadır.

PA-5400 Serisinde de, Palo Alto Networks bünyesindeki NGFW 'ların tamamının işletilmesinde kullanılan aynı yazılım, yani PAN-OS® bulunmaktadır. PAN-OS, uygulamalar, tehditler ve içerik dahil olmak üzere tüm trafiği doğal olarak sınıflandırır, konum veya cihazdan bağımsız olarak bahsedilen bu trafiği kullanıcıya bağlar.

Temel Güvenlik ve Bağlantı Özellikleri

ML - Destekli Yeni Nesil Güvenlik Duvarı

- Daha önce hiç görülmemiş kimlik avı (phishing) girişimlerini belirleyip hemen durdururken , dosya tabanlı saldırılar için, bağlantı içi imzasız (inline signatureless) saldırılara karşı da önleme sağlamak amacıyla güvenlik duvarının çekirdeğine (core) Makine Öğrenimi (ML) özelliğini entegre etmektedir.
- Sıfır gecikmeli imzaları ve talimatları NGFW 'ya geri göndermek için bulut tabanlı ML işlemlerinden yararlanmaktadır.
- IoT cihazlarını tespit etmek ve politika önerilerinde bulunmak için davranış analizi yöntemini kullanır; NGFW üzerinde, bulut üzerinden iletilen, entegre bir hizmettir.
- Zamandan tasarruf sağlayan ve insan hatası olasılığını azaltan politika önerilerini otomatikleştirir.

Full Layer 7 Inspection ile Her Zaman , Tüm portlarda, Tüm Uygulamaları Tanımlar ve Sınıflandırır

- Port, Protokol, Kaçınma Teknikleri (evasive) veya Kriptolamadan (TLS/ SSL) bağımsız olarak ağınızdan geçen uygulamaları tanımlar. Buna ek olarak, SaaS Security lisansı aracılığı ile SaaS infilakına (explosion) ayak uydurabilmek için yeni uygulamaları otomatik olarak tespit ve kontrol eder.
- Güvenli etkinleştirme politika kararlarınızın tümünde bağlantı noktasını değil; uygulamayı kullanır: Trafik şekillendirmeye izin verilmesi, izin verilmemesi, trafik şekillendirmenin planlanması, incelenmesi ve uygulanmasını sağlar.
- Özel Uygulamalar için özel App-ID™ etiketlerinin oluşturulması veya Palo Alto Networks'ten yeni uygulamalar için App-ID geliştirilmesinin talep edilmesi olanağı sunar.
- Kötü amaçlı dosyaları ve veri sızdırma girişimlerini engellemek için, uygulama içindeki tüm yük verilerini (payload data) (Örneğin: files and data patterns) tanımlar.
- Ağınızdaki tüm onaylanmış ve onaylanmamış SaaS trafiğine ilişkin bilgi sağlayan SaaS raporları dahil olmak üzere standart ve özelleştirilmiş uygulama kullanım raporları oluşturur.
- Size daha güvenli ve yönetimi daha kolay bir kural seti sunarak, yerleşik Policy Optimizer (Politika Optimize Edici) ile eski Layer 4 Kural Setlerinin App-ID tabanlı kurallara güvenli bir şekilde taşınmasını sağlar.

Kullanıcıya Dayalı Politikayı Uyarlamanın Yanısıra, Herhangi bir Konum/ Cihazdaki Kullanıcılara Yönelik Güvenliği Sağlar.

- Yalnızca IP adreslerini değil, kullanıcı ve grupları da esas alarak görünürlük, güvenlik politikaları, raporlama ve adli bilişim sağlar.
- Kullanıcı bilgilerinden yararlanmak amacıyla çok çeşitli kaynaklara kolayca entegre olur: Kablosuz LAN Denetleyicileri, VPN 'ler, Dizin Sunucuları, SIEM 'ler, PROXY 'ler ve daha fazlası.
- Kullanıcı dizinlerine değişikliklerin uygulanmasını beklemeksizin, zamana bağlı güvenlik eylemleri gerçekleştirmeye yönelik, güvenlik duvarında Dinamik Kullanıcı Grupları (DUG 's) tanımlamanıza olanak tanır.
- Kullanıcıların konumlarından (ofis, ev,mobil vb.) ve cihazlarından (iOS ve Android® Mobil Cihazlar, macOS®, Windows®, Linux Masaüstü Bilgisayarlar, Dizüstü Bilgisayarlar; Citrix ve Microsoft VDI ve Terminal Sunucuları) bağımsız olarak tutarlı politikalar uygular.
- Herhangi bir uygulama değişikliği olmadan, herhangi bir uygulama için, ağ katmanında Çok Faktörlü Kimlik Doğrulamayı (MFA) etkinleştirerek, kurumsal kimlik bilgilerinin herhangi bir web sitesine sızmasını ve çalınan kimlik bilgilerinin yeniden kullanılmasını önler.
- Şüpheli veya kötü niyetli kullanıcıları kısıtlamak amacıyla kullanıcı davranışına dayalı dinamik güvenlik eylemlerini tesis eder.
- Kimlik tabanlı güvenlik için tamamıyla yeni bir bulut tabanlı mimari olan Cloud Identity Engine vasıtası ile Zero Trust güvenlik yaklaşımına hızla geçiş yapmak için, konum ve kullanıcı kimliği depolarının nerede bulunduğundan bağımsız olarak, kullanıcılarınızın kimliğini tutarlı bir şekilde doğrular ve yetkilendirir.

Kriptolanmış Trafikte Gizlenen Kötü Amaçlı Etkinlikleri Önler

- TLS 1.3 ve HTTP/2 kullanan trafik de dahil olmak üzere, hem gelen hem de giden TLS/ SSL kriptolu trafiği inceler ve bunlara yönelik politika uygular.
- Kriptolanmış trafik miktarı, TLS/ SSL versiyonları, TLS trafiğine şifre çözmeden zengin görünürlük sunar.
- Riskleri azaltmak amacıyla eski TLS protokollerinin, güvenli olmayan şifrelerin ve yanlış yapılandırılmış sertifikaların kullanımı üzerinde kontrol sağlar.
- Kripto çözüm sürecinin düzenlenmesini kolaylaştırarak, sabitlenmiş sertifikalara sahip uygulamalar gibi sorunları gidermek amacıyla, yerleşik logları kullanmanıza olanak tanır.
- Gizliliğin ve regülasyon hükümlerine uyum sağlanması için, URL kategorisine, kaynak ve hedef bölgeye, adrese, kullanıcıya, kullanıcı grubuna, cihaza ve portlara göre esnek bir şekilde kripto çözme sürecini etkinleştirmenize veya devre dışı bırakmanıza imkan sağlar
- Güvenlik duvarından şifresi çözülmüş trafiğin bir kopyasını oluşturmanıza (decryption mirroring) ve adli bilişim, tarihsel amaçlar veya veri kaybının önlenmesi (DLP) amacıyla bu kopyayı trafik toplama araçlarına göndermenizi sağlar.
- Network Packet Broker aracılığı ile tüm trafiği (Kriptosu Çözülmüş TLS, Kriptosu Çözülmemiş TLS ve TLS Olmayan) herhangi bir güvenlik aracına akıllı bir şekilde iletmenizi, ağ performansınızı optimize etmenizi ve maliyet avantajı sağlar.

Merkezi Yönetim ve Görünürlük Olanağı Sunar

- Tek bir birleştirilmiş kullanıcı arayüzüne sahip Panorama sayesinde ağ güvenlik yönetimi aracılığıyla birden çok dağıtılmış Palo Alto Networks NGFW'ları için (konum veya ölçekten bağımsız olarak) merkezi yönetim, yapılandırma ve görünürlükten yararlanır.
- Şablonlar ve cihaz grupları sayesinde Panorama aracılığıyla yapılandırma paylaşımını kolaylaştırıp günlük log ihtiyaçları arttıkça günlük log toplama işlemini ölçeklendirir.
- Uygulama Komuta Merkezi (ACC) aracılığıyla, kullanıcıların ağ trafiği ve tehditleri hakkında derin görünürlük ve kapsamlı bilgiler elde etmelerini sağlar.

AIOps ile Güvenlik Yatırımınızı En Üst Düzeye Çıkarın ve İş Kesintilerini Önleyin

- Güvenlik yaklaşımınızı güçlendirmek ve güvenlik yatırımlarınızdan en iyi şekilde yararlanmanız için, NGFW'a yönelik AIOps, özgün yapınıza göre sürekli özelleştirilmiş en iyi uygulama önerilerini sizlere sunar.
- Gelişmiş telemetri verileriyle desteklenen Makine Öğrenimine (ML) dayalı güvenlik duvarı sağlığı, performans ve kapasite sorunlarını akıllıca tahmin eder. Ayrıca, öngörülen aksaklıkları gidermek için, eyleme dönüştürülebilir öngörüler sunar.

Bulut Tarafından Sağlanan Güvenlik Hizmetleri Sayesinde Gelişmiş Tehditleri Algılar ve Önler

Günümüzün karmaşık siber saldırıları, kötü niyetli yükler (payloads) sağlamak amacıyla birden fazla tehdit vektörü ve gelişmiş teknikler kullanarak 30 dakikada 45.000 varyant oluşturabilmektedir. Güvenlik açıkları oluşturarak, güvenlik ekipleri için ek yükü artırarak, tutarsız erişim ve görünürlükle iş verimliliğini engelleyerek, diğer güvenlik anlayışları ile etkileşim içinde olmayan geleneksel güvenlik anlayışı kurumlar için zorluklara neden olmaktadır.

Sektörde lider konumunda olan NGFW'ları ile Palo Alto Networks sorunsuz bir şekilde entegre olan Bulut Tarafından Sağlanan Güvenlik Hizmetleri İLE, istihbaratı anında koordine etmek ve tüm vektörlerdeki tehditlere karşı koruma sağlamak amacıyla 80.000 müşterinin ağ etkisini kullanmaktadır. En gelişmiş ve tespit edilmesi zor tehditlere karşı bile güvende kalmak için, lokasyonlarınızda kapsama boşluklarını ortadan kaldırıp bir platform bünyesinde tutarlı bir şekilde Sınıfının-En-İyisi-Güvenlik çözümünü sunar.

- **Threat Prevention:**- En yüksek düzeyde güvenlik etkinliğine sahip sektörün önde gelen saldırı önleme sistemi (IPS) sayesinde saldırının her aşamasında tehditleri engeller.
- **Gelişmiş Tehdit Önleme** – Kendine özgü derin öğrenme ve makine öğrenimi modelleri doğrultusunda daha önceden bilinmeyen tespit edilmesi zor komuta ve kontrol trafiğini %50'ye varan oranda engellemek amacıyla endüstride sınıfının en iyisi IPS'leri genişletmektedir.
- **WildFire®** - Endüstri lideri bulut tabanlı analiz kanalı ile bilinmeyen kötü amaçlı yazılımları otomatik olarak algılayarak ve önleyerek dosyaların güvende kalmasını sağlar.
- **Advanced URL Filtering** - Bilinen ve bilinmeyen kötü amaçlı web sitelerini kullanıcılarınız ziyaret etmeden önce erişimi engelleyerek internetin güvenli bir şekilde kullanılmasını sağlar
- **DNS Security** - Komuta ve kontrol amacıyla DNS kullanan saldırıları bozar, altyapınızda herhangi bir değişiklik gerektirmeden veri hırsızlığını kesintiye uğratır.
- **IoT Security—** Tek bir platform bünyesinde ML destekli görünürlük, önleme ve uygulama sağlayarak sektörün en kapsamlı IoT güvenlik çözümünü sunmaktadır.
- **Kurumsal DLP** — Tüm kurum genelinde hassas verileri tutarlı bir şekilde belirleyerek güvenli olmayan aktarımları ve kurumsal politika ihlallerini önleyerek veri ihlali risklerini en aza indirir.
- **SaaS Security** — Yeni Nesil Bulut Erişimi Güvenlik Aracısı (CASB), uygulama infilakının (explosion) bir adım önünde olmanızı sağlayarak, tüm SaaS Uygulamalarını otomatik olarak görür ve güvenliğini sağlar.

Tek Geçişli (Single-Pass) Mimari ile Paket İşleme Süreci için Özgün Bir Yaklaşım Sunar

- Tüm tehditler ve içerik için - ağ oluşturma, politika arama, uygulama, kod çözme ve imza eşleştirme işlemlerini tek geçişte gerçekleştirir. Bu, tek bir güvenlik cihazında birden çok işlevi gerçekleştirmek için gereken işlem yükü miktarını önemli ölçüde azaltmaktadır.
- Akış tabanlı, tek tip imza eşleştirme yöntemini kullanarak tüm imzalar için trafiği tek geçişte tarayarak gecikme yaşanmasını önler.
- Güvenlik lisansları etkinleştirildiğinde tutarlı ve öngörülebilir performans sağlar.

(Tablo 1'de, "Tehdit Önleme verimliliği", birden çok lisans etkinleştirildiğinde ölçülmüştür)

SD-WAN İşlevselliğini Etkinleştirir

- Sektörde lider konumundaki güvenlik yaklaşımımızla kendiliğinden entegre SD-WAN 'ı güvenli bir şekilde uygulamanızı sağlar.
- Gecikme, titreme ve paket kaybını en aza indirmesi nedeniyle benzersiz bir kullanıcı deneyimi sunar.

Tablo 1: PA-5400 Serisi Performans ve Kapasiteler

	PA-5430	PA-5420	PA-5410
Güvenlik Duvarı Verimliliği (HTTP / appmix)*	63/59.4 GBPS	53.7/47.5 GBPS	45.2/36.7 GBPS
Tehdit Önleme Verimliliği (HTTP / appmix)†	37.6/40.9 GBPS	28.8/30.5 GBPS	22/23.5 GBPS
IPsec VPN Verimliliği ‡	42 GBPS	28.7 GBPS	21 GBPS
Maksimum Oturum	8.3M	6.2M	4.1M
Saniye Başına Yeni Oturum Adedi §	366.000	315.000	246.000
Sanal sistemler (taban / maksimum) ‖	25/125	15/65	10/20

Not: Sonuçlar PAN-OS 10.2 bünyesinde ölçülmüştür.

* Güvenlik Duvarı verimliliği, 64 KB HTTP / appmix işlemleri kullanılarak App-ID ve izin verilen log tutma işlemleri vesilesi ile ölçülmüştür.

† * Tehdit Önleme verimliliği, 64 KB HTTP / appmix işlemleri kullanılarak App-ID, IPS, Antivirüs, Casus Yazılım Önleme, WildFire, DNS Güvenlik, Dosya Bloklama ve loglama etkinleştirilerekölçülmüştür.

‡ IPsec VPN verimliliği 64 KB HTTP işlemleri ve loglama işlemleri etkinken ölçülmüştür.

§ Saniyedeki yeni oturum sayısı, 1 bayt HTTP işlemleri kullanılarak, Uygulama Geçersiz Kılma vesilesi ile ölçülür.

‖ Taban miktar üzerinden sanal sistemler eklenmesi ayrı olarak satın alınabilen bir lisansın varlığını gerektirmektedir.

L2, L3, tap, Sanal Kablo (Saydam Mod)

Yönlendirme

Hassas (Kesintisiz) Yeniden Başlatmalı OSPFv2/v3, Hassas (Kesintisiz) Yeniden Başlatmalı BGP, RIP, Statik Yönlendirme

Politikaya Dayalı İletim

Ethernet (PPPoE) ve DHCP Üzerinden Noktadan Noktaya Protokol - Dinamik adres ataması babında desteklenmektedir.

Birden Fazla Noktaya Yayın: PIM-SM, PIM-SSM, IGMP v1, v2 ve v3

Çift Yönlü Yönlendirme Algılama (BFD)

Tablo 2: PA-5400 Serisi Ağ Özellikleri_(devamı)
SD-WAN
Yol Kalitesi Ölçümü (Titreme, Paket Kaybı, Gecikme)
İlk Yol Seçimi (PBF)
Parola Değişimi: Manuel Parola, IKEv1 ve IKEv2 (Önceden Paylaşılmış Parola, Sertifika Tabanlı Kimlik Doğrulama)
IPv6
L2, L3, Çekme Kablo, Sanal Kablo (Saydam Mod)
Özellikler: App-ID (Uygulama ID), User-ID (Kullanıcı ID), Content-ID (İçerik ID), WildFire, ve SSL Kripto Çözme İşlemi
SLAAC
IPsec VPN
Parola Değişimi: Manuel Parola, IKEv1 ve IKEv2 (Önceden Paylaşılmış Parola, Sertifika Tabanlı Kimlik Doğrulama)
Kriptolama: 3DES, AES (128 bit, 192 bit, 256 bit)
Kimlik Doğrulama: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLAN 'lar
Cihaz Başına / Ara Yüz Başına 802.1 Q VLAN Etiketleri: 4,094 /
4,094 Kümeleşme Ara Birimleri (802.3ad), LACP
Ağ Adresi Çevirisi
NAT (Ağ Adresi Çevirisi) Modları (IPv4): Statik IP, Dinamik IP, Dinamik IP ve Bağlantı Noktası (Bağlantı Noktası Adresi Çevirisi) NAT64, NPTv6
Ek NAT (Ağ Adresi Çevirisi) Özellikleri: Dinamik IP Kaydı, Ayarlanabilir Dinamik IP ve Aşırı Bağlantı Noktası Talebi
Yüksek Kullanılabilirlik
Modlar: Aktif/Aktif, Aktif/Pasif, HA Kümeleme
Arıza Tespiti: Yol İzleme, Arayüz İzleme
Mobil Ağ Altyapısı*
5G Güvenlik
5G MEC (Çok Erişimli Uç Bilgi İşleme Süreci) Güvenliği
GTP Güvenliği
SCTP Güvenliği
* Daha fazla bilgi için lütfen 5G 'ye Yönelik ML - Destekli NGFW 'lerimize ait Veri Formuna bakınız.

Tablo 3: PA-5400 Serisi Donanım Özellikleri
1/O
PA-5430: 1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 25G SFP28 (4), 40G/100G QSPF+/QSFP28 (4)
PA-5420: 1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 25G SFP28 (4), 40G/100G QSPF+/QSFP28 (4)
PA-5410: 1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 25G SFP28 (4), 40G/100G QSPF+/QSFP28 (4)
Yönetim I/O
1G SFP Bant Dışı Yönetim Bağlantı Noktası (1), 1G SFP Yüksek Kullanılabilirlik (2), 40G QSFP + Yüksek Kullanılabilirlik (1), RJ-45 Konsol Bağlantı Noktası (1), Mikro USB
Depolama Kapasitesi
480 GB SSD Çifti, Sistem Depolama

Tablo 3: PA-5400 Serisi Donanım Özellikleri_(devamı)
Güç Kaynağı (Ortalama/Maksimum Enerji Tüketimi)
630/760 W
Maksimum BTU/Saat
1638
Güç Kaynakları (Taban/Maksimum)
1:1 Tam Yedekli (2/2)
AC Giriş Voltajı (Giriş Hz)
100–240 VAC (50–60 Hz)
AC Güç Kaynağı Çıkışı
1,200 WATT/Güç Kaynağı
Maksimum Amper Tüketimi
AC: 7 A @ 100 VAC, 3 A @ 240 VAC DC: 15 A @ -48 VDC, 12 A @ -60 VDC
Maksimum Ani Akım
AC: 50 A @ 230 VAC, 50 A @ 120 VAC DC: 200 A @ 72 VDC
Arızalar Arasındaki Ortalama Süre (MTBF)
22 Yıl
Raf Montaj Boyutları
2U, 19" Standart Raf (3.45" Yükseklik x 22.5" Derinlik x 17.34" Genişlik)
Ağırlık (Bağımsız Cihaz / Sevk Edildiği Şekliyle)
35.2 LBS/48.8 LBS
Güvenlik
cTUVus, CB
EMI
FCC Sınıf A, CE Sınıf A, VCCI Sınıf A
Sertifikalar
Bakınız paloaltonetworks.com/company/certifications.html
Ortam
Çalışma Sıcaklığı: 32° ila 122° F, 0° ila 50° C Çalışmadığı Zamanlarda Dayanabileceği Azami Sıcaklık: -4° ila 158° F, -20° ila 70° C Nem Toleransı: %10 ila %90 Maksimum Yükseklik: 10,000 FT/3,048 M Hava Akımı: Önden Arkaya Doğru

PA-5400 Serisinin özellikleriyle ilgili detaylı bilgi almak ve demo talebinde bulunmak için, PanSales_TR@exclusive-networks.com adresinden satış ekibimiz ile iletişime geçebilirsiniz.