



PA-3410



PA-3430



PA-3420



PA-3440

# PA-3400 Serisi

## Palo Alto Networks ML (Makine Öğrenimi) - Destekli PA-3400 Serisi

PA-3440, PA-3430, PA-3420 ve PA-3410'dan oluşan NGFW 'ler, yüksek hızdaki internet ağ geçidine sahip dağıtık yapıdaki organizasyonlara yöneliktir. PA-3400 Serisinde yer alan cihazlar trafiğin tamamını güvence altına alır.

### Öne Çıkan Özellikler

- Dünyanın ilk ML- Destekli NGFW ürünü
- Ağ Güvenlik Duvarı Kategorisinde Gartner Magic Quadrant™ 'da 10 defa üst üste Lider olarak gösterilmiştir.
- Forrester Wave™ tarafında Kurumsal Güvenlik Duvarları alanında, Q3 2020 'de Lider olarak gösterilmiştir.
- 2019 NSS Laboratuvarları NGFW Raporunda, PA-3400 serisine en yüksek Güvenlik Etkinlik Puanı verilmiştir. (Evasion (atlatma) tekniklerinin % 100 'ünün engellenmiş olması nedeniyle)
- Ek sensöre gerek duyulmaksızın, yönetil(e)meyen 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.
- Sıfır Dokunma Sağlama (ZTP) sayesinde çok sayıda güvenlik duvarının konuşlandırılmasını daha kolay hale getirmektedir.
- Panorama™ Ağ Güvenliği Yönetimi ile merkezi yönetimi destekler.

Dünyanın ilk ML- Destekli Yeni Nesil Güvenlik Duvarı (NGFW), bilinmeyen tehditleri önlemenize, IoT cihazları da dahil tüm cihazları görmenize, güvence altına almanıza ve otomatik politika önerileri kanalıyla hataları azaltmanıza imkan tanır.

PA-3400 Serisinde kontrolü Palo Alto Networks bünyesindeki NGFW'ların tamamında kullanılan yazılım, yani PAN-OS® sağlar. PAN-OS, uygulamalar, tehditler ve içerik dahil olmak üzere tüm trafiği doğal olarak sınıflandırır; konum veya cihaz türünden 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 'a 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 ağımdan 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 tümü için, 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.
- Ağımdaki 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.

### Kullanıma Dayalı Politika Uyarıların Yanısıra, Herhangi bir Konum/ Cihazdaki Kullanıcılara da Güvenlik 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 dışarıdaki 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 sunar.
- 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 tesis edilmesi ve regülasyon hükümlerine uyum sağlanması adına, 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 olanak tanır.
- 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) dışarıda herhangi bir güvenlik aracına akıllı bir şekilde iletmenizi, ağ performansınızı optimize etmenizi ve maliyetlerinizi azaltmanıza yardımcı olur.

## Merkezi Yönetim ve Görünürlük Olanakları Sunar

- Tek bir birleştirilmiş kullanıcı arabirimi bünyesinde Panorama 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 artırtıkça 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 ile, 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 adına eyleme dönüştürülebilir öngörüler sunar.

## Bulutta Sağlanan Güvenlik Hizmetleri Sayesinde Gelişmiş Tehditleri Algular 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, tutsuz 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 'larımızla sorunsuz bir şekilde entegre olan Bulut tarafından sağlanan güvenlik hizmetlerimiz, 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 tarafınıza sunulan bu Sınıfının-En-İyisi-Güvenlik çözümünden yararlanınız.

- **Threat Prevention** - En yüksek düzeyde güvenlik etkinliğine sahip sektörün önde gelen saldırı önleme sistemi (IPS) vasıtası ile saldırının her aşamasında tehditleri engeller.
- **Gelişmiş Tehdit Önleme** - Kendine özgü derin öğrenme ve makine öğrenimi modelleri doğrultusunda daha öncelerde bilinmeyen tespit edilmesi zor komuta ve kontrol trafiğini %50 'ye varan oranda önlemek 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 yeni 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 engeller.

- **IoT Security** — Tek bir platform üzerinde ML destekli görünürlük, koruma ve uygulama sağlayan, sektörün en kapsamlı IoT güvenlik çözümünü sunmaktadır.
- **Kurumsal DLP** — Tüm kurum genelinde hassas verileri tutarlı bir şekilde tespit ederek, 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 Mimari (Single-Pass) ile Paket İşleme Süreci için Özgün Bir Yaklaşım Sunar

- Tüm tehditler ve içerik için- ağ oluşturma, politika arama, uygulama, şifre 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 gecikmeyi önler.
  - Güvenlik lisansları etkinleştirildiğinde tutarlı ve öngörülebilir performans sağlar.
- (Tablo 1'de, "Tehdit Önleme verimliliği", birden çok abonelik etkinleştirildiğinde ölçülmüştür)

### SD-WAN İşlevselliğini Etkinleştirir

- Sektörde lider konumundaki güvenlik yaklaşımımız, entegre çalışan SD-WAN 'ı güvenli bir şekilde uygulamanızı sağlar.
- Gecikme, titreme ve paket kaybını en aza indirerek, benzersiz bir son kullanıcı deneyimi sunar.

**Tablo 1: PA-3400 Serisi Performans ve Kapasiteler**

	PA-3440	PA-3430	PA-3420	PA-3410
Güvenlik Duvarı Verimliliği (HTTP / appmix)*	27.5/24 GBPS	23.8/19.6 GBPS	19.1/16.5 GBPS	13.1/11.3 GBPS
Tehdit Önleme Verimliliği (HTTP / appmix)†	10.5/12.7 GBPS	8.7/10.2 GBPS	7.4/8.8 GBPS	5.1/5.9 GBPS
IPsec VPN Verimliliği ‡	14.5 GBPS	12.2 GBPS	9.9 GBPS	6.8 GBPS
Maksimum Oturum	3M	2.5M	2M	1.4M
Saniye Başına Yeni Oturum Adedi §	250.000	222.000	190.000	130.000
Sanal sistemler (taban / maksimum)	1/11	1/11	1/11	1/11

Not: Sonuçlar PAN-OS 10.2 ile, 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 Güvenliği, Dosya Bloklama ve loglama etkinleştirilerek ölçülmüştür.

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

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

|| Taban miktar üzerinden sanal sistemler eklenmesi ayrı olarak satın alınabilen bir lisans gerektirmektedir.

**Tablo 2: PA-3400 Serisi Ağ Özellikleri**

#### Arayüz Modları

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

#### Yönlendirme

Hassas (Kesintisiz) Yeniden Başlatılabilir OSPFv2/v3, Hassas (Kesintisiz) Yeniden Başlatılabilir BGP, RIP, Statik Yönlendirme Politikaya Dayalı İletim

Ethernet (PPPoE) Üzerinden Noktadan Noktaya Protokol

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

Çift Yönlü Yönlendirme Algılama (BFD)

**Tablo 2: PA-3400 Serisi Ağ Özellikleri (devamı)****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

**Tablo 3: PA-3400 Serisi Donanım Özellikleri****I/O**

PA-3440: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSPF+/QSFP28 (2)

PA-3430: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSPF+/QSFP28 (2)

PA-3420: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)

PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)

**Yönetim I/O**

100/1000 Bant Dışı Yönetim Bağlantı Noktası (1),

100/1000 Yüksek Kullanılabilirlik (2), 10G SFP + Yüksek Kullanılabilirlik (1)

RJ-45 Konsol Bağlantı Noktası (1), Mikro USB (1)

**Depolama Kapasitesi**

480 GB SSD

**Güç Kaynağı (Ortalama/Maksimum Enerji Tüketimi)**

Yedekli 450 WATT AC (155W/190W)

**Maksimum BTU/Saat**

650

**Giriş Voltajı Frekansı**

AC: 100–240 VAC (50–60Hz)

**Maksimum Amper Tüketimi**

AC: 1.9 A @ 100 VAC, 0.8 A @ 240 VAC

### Tablo 3: PA-3400 Serisi Donanım Özellikleri (devamı)

#### Arızalar Arasındaki Ortalama Süre (MTBF)

22 Yıl

#### Raf Montaj Boyutları

1U, 19" Standart Raf 14.15" x 17.15" x 1.70"

#### Ağırlık (Bağımsız Cihaz / Sevk Edildiği Şekliyle)

15.5 LBS / 25 LBS

#### Güvenlik

cTUVus, CB

#### EMI

FCC Sınıf A, CE Sınıf A, VCCI Sınıf A

#### Sertifikalar

[paloaltonetworks.com/company/certifications.html](http://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-3400 Serisinin özellikleri ile ilgili detaylı bilgi sahibi olmak ve demo talebinde bulunmak için, [PanSales\\_TR@exclusive-networks.com](mailto:PanSales_TR@exclusive-networks.com) adresinden satış ekibimizle iletişime geçebilirsiniz.