EXCLUSIVE NETWORKS

paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS

Öne Çıkan Özellikler

- **Dünyadaki ilk Makine Öğrenimi Destekli Yeni Nesil Güvenlik Duvarı (Machine Learning Supported Next Generation Firewall)**
- **Gartner Ağ Güvenlik Duvarı kategorisinde, Magic Quadrant®'ta 9 Kez Lider**
- **The Forrester Wave™', Q3'20 raporunda Kurumsal Güvenlik Duvarlarında Lider**
- **Kaçakların %100'ünü engellediğinden, 2019 NSS Labs NGFW Test Raporu'nda En Yüksek Güvenlik Etkinliği Puanına sahip**
- **Görünürlüğü ve güvenliği, ek sensöre gerek kalmadan, yönetilmeyen IoT cihazları da dahil tüm cihazları kapsayacak şekilde genişletir.**
- **Aktif/aktif ve aktif/pasif modlarla yüksek kullanılabilirliği destekler.**
- **Şube ve uzaktan çalışanlar için, isteğe bağlı güç kaynağı ile sessiz ve fansız, çevreye duyarlı bir tasarıma sahiptir.**
- **İsteğe bağlı Zero Touch Provisioning (ZTP) ile çok sayıda güvenlik duvarının dağıtımını basitleştirir.**
- **Panorama™ ağ güvenliği yönetimi ile merkezi yönetimi destekler.**

PA-400 Serisi

PA-410, PA-440, PA-450 ve PA-460'dan oluşan Palo Alto Networks PA-400 Serisi, dağınık lokasyonlu şubelere, küçük ve orta ölçekli işletmelere gelişmiş Makine Öğrenimi (Machine Learning- ML) Destekli Yeni Nesil Güvenlik Duvarı (Next Generation Firewall- NGFW) çözümünü sunuyor.

PA-400 Serisi

Dünyanın ilk Makine Öğrenimi Destekli Yeni Nesil Güvenlik Duvarı, bilinmeyen tehditleri önlemenizi, IoT dahil, kullanımdaki her cihazı görmenizi, korumanızı ve otomatik politika önerileriyle hataları azaltmanızı sağlar.

PA-400 Serisi ara yüzü, PAN-OS®, yani tüm Palo Alto Networks Yeni Nesil Güvenlik Duvarlarını çalıştıran yazılımdır. PAN-OS; uygulamalar, olası tehditler ve içerik dahil olmak üzere tüm trafiği kullanıcıya özel olarak sınıflandırır, ardından bu trafiği lokasyona veya cihaz türünden bağımsız olarak kullanıcıya bağlar. Uygulama, içerik ve kullanıcı için, gelişmiş güvenlik altyapısını oluşturur ve daha kısa vaka yanıt süreleri sağlar.

Temel Güvenlik ve Bağlantı Özellikleri

Makine Öğrenimi Destekli Yeni Nesil Güvenlik Duvarı

- Daha önce karşılaşılmayan kimlik avı girişimlerini tespit edip, hemen durdururken; dosya tabanlı saldırılar için, güvenlik duvarının çekirdeğine makine öğrenimini (ML) yerleştirir.
- Zero-delay imzaları ve komutları Yeni Nesil Güvenlik Duvarına göndermek için, bulut tabanlı makine öğreniminden yararlanır.
- Yeni Nesil Güvenlik Duvarında, IoT cihazlarını tespit etmek ve politika önerileri sunmak için, davranış analizinden yararlanır.
- Zaman kazandıran ve insan ihmali olasılığını azaltan politika önerilerini otomatikleştirir.

Layer 7 denetimi ile, her zaman tüm bağlantı noktalarındaki tüm uygulamaları tanımlar ve sınıflandırır.

- Bağlantı noktası, protokol veya şifrelemeden (TLS/SSL) bağımsız olarak ağınızda dolaşan uygulamaları tanımlar.
- Tüm güvenlik kararlarınızın temeli olarak, bağlantı noktasını değil; uygulamayı kullanır: trafik şekillendirmeye izin verme, reddetme, planlama, inceleme ve uygulama gibi.
- Firmaya özel tescilli uygulamalar için, özel App-ID™ etiketleri oluşturma veya Palo Alto Networks'ün yeni uygulamalar için, App-ID (Uygulama Kimliği) geliştirilmesini talep etme özelliğini sunar.
- Kötü amaçlı dosyaları engellemek ve veri hırsızlığı girişimlerini engellemek için, bir uygulama içindeki tüm yük verilerini (örneğin, dosya ve veri modelleri) tanımlar.
- Ağınızdaki tüm onaylanmış ve onaylanmamış SaaS trafiğine ilişkin bilgi sağlayan, hizmet olarak yazılım (SaaS) raporları dahil olmak üzere standart ve özelleştirilmiş uygulama kullanım raporları oluşturur.
- Firmaya özel süreç geliştirme ile eski Layer 4 kümelerinin Uygulama Kimliği tabanlı kurallara güvenli bir şekilde taşınmasını sağlayarak, size daha güvenli ve yönetimi daha kolay bir kural kümesi sunar.

Politikayı kullanıcıya göre uyarlarken, herhangi bir lokasyonda yada cihazdaki kullanıcılar için güvenlik sağlar.

- Yalnızca IP adreslerine değil, kullanıcılara ve gruplara göre görünürlük, güvenlik politikaları, raporlama ve araştırma sağlar.
- Kullanıcı bilgilerinden yararlanmak için, çok çeşitli kaynaklarla kolayca entegre olur: kablosuz LAN denetleyicileri, VPN'ler, dizin sunucuları, SIEM'ler, proxy'ler ve daha fazlası gibi.
- Değişikliklerin kullanıcı gruplarına uygulanmasını beklemeden zamana bağlı güvenlik aksiyonları gerçekleştirmek için, güvenlik duvarında Dinamik Kullanıcı Grupları (DUG) tanımlamanıza olanak tanır.
- Kullanıcıların lokasyonlarından (ofis, ev, seyahat 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.
- Kurumsal kimlik bilgilerinin 3. taraf web sitelerine sızmasını önler ve herhangi bir uygulama değişikliği olmadan ağ katmanında çok faktörlü kimlik doğrulamasını (MFA) etkinleştirerek çalınan kimlik bilgilerinin yeniden kullanımını önler.
- Şüpheli veya kötü niyetli kullanıcıları engellemek için ,kullanıcı davranışına göre dinamik güvenlik aksiyonları belirler.

Şifrelenmiş, trafikte gizlenmiş kötü niyetli aksiyonları önler.

- TLS 1.3 ve HTTP/2 kullanan trafik dahil olmak üzere, hem gelen hem de giden TLS/SSL şifreli trafiğe yönelik politikayı inceler ve uygular.
- Şifre çözmeden, şifreli trafik miktarı, TLS/SSL sürümleri, şifre paketleri ve daha fazlası gibi TLS trafiği için zengin görünürlük sunar.
- Riskleri azaltmak için, eski TLS protokollerinin, güvenli olmayan şifrelerin ve yanlış yapılandırılmış sertifikaların kullanımı üzerinde kontrol sağlar.
- Kolay şifre çözme dağıtımı sağlar ve sabitlenmiş sertifikalara sahip uygulamalar gibi sorunları gidermek için, mevcut günlükleri kullanmanıza izin verir.
- Gizlilik ve uygunluk amacıyla URL kategorisi, kaynak ve hedef bölge, adres, kullanıcı, kullanıcı grubu, cihaz ve bağlantı noktasına göre şifre çözmeyi esnek bir şekilde etkinleştirmenizi veya devre dışı bırakmanızı sağlar.
- Güvenlik duvarından şifresi çözülmüş trafiğin bir kopyasını oluşturmanıza ve araştırma, geçmiş amaçlar veya veri kaybını önleme (DLP) için trafik toplama araçlarına göndermenizi sağlar.

Merkezi yönetim ve görünürlük sunar.

- Panorama™ ağ güvenliği yönetimi aracılığıyla birden fazla dağıtılmış Palo Alto Networks Yeni Nesil Güvenlik Duvarı (lokasyon ve ölçekten bağımsız) için, tek bir arayüz ile merkezi yönetim, yapılandırma ve görünürlükten yararlanır.
- Panorama aracılığıyla yapılandırma paylaşımını kolaylaştırır ve günlük kaydı ihtiyaçları arttıkça günlük kayıtları ölçeklendirir.
- Kullanıcıların, Uygulama Komuta Merkezi (ACC) aracılığıyla, ağ trafiği ve tehditlere ilişkin derin görünürlük ve kapsamlı bilgiler elde etmesini sağlar.

Bulut tabanlı güvenlik hizmetleriyle gelişmiş tehditleri tespit edin ve önleyin.

Günümüzde, siber saldırıların etki alanı ve sayısı artmıştır; 30 dakika içinde 45.000 varyanta ölçeklenir, kurumunuz içinde kötü amaçlı yükler sağlamak için, birden çok tehdit vektörü veya gelişmiş teknikler kullanırlar. Geleneksel silolara ayrılmış güvenlik çözümleri, kullanıcılarını, cihazlarını ve uygulamalarını

korumaya çalışan firmalar için zordur. Sözkonusu firmalar için, güvenlik açığı oluşturur, güvenlik ekipleri için yönetim yükünü artırır, tutarsız erişim ve görünürlükle verimliliği engeller. Sektör lideri Yeni Nesil Güvenlik Duvarı platformuyla sorunsuz bir şekilde entegre olan Bulutta Sağlanan Güvenlik Hizmetlerimiz, istihbaratı anında koordine etmek ve tüm tehdit vektörleri genelindeki tüm tehditlere karşı koruma sağlamak için, 80.000 müşterinin ağ etkisinden faydalanır. Tüm kurumsal lokasyonlardaki boşlukları ortadan kaldırın ve bir platformda tutarlı olarak sunulan sınıfının en iyisi güvenlikten yararlanın, böylece en gelişmiş ve yakalanması zor tehditlere karşı bile güvende olabilirsiniz!

- **Threat Prevention (TP)—** Performanstan ödün vermeden tek geçişte, tüm trafik genelinde bilinen tüm tehditleri önlemek için geleneksel bir saldırı önleme sisteminin (IPS) ötesinde çözüm sağlar.
- **Advanced URL Filtering—** Sektörün ilk gerçek zamanlı web koruma motoru ve lider kimlik avı koruması ile operasyonel verimliliği en üst düzeye çıkarırken, en iyi web koruması sağlar.
- **WildFire® —** 42.000'den fazla müşteriden sektör lideri bulut tabanlı analiz ve istihbaratla desteklenen bilinmeyen kötü amaçlı yazılımların otomatik olarak algılanması ve önlenmesiyle dosyaların güvende olmasını sağlar.
- **DNS Security —** DNS üzerinden tehditleri gerçek zamanlı olarak tespit etmek ve önlemek için Makine Öğreniminin gücünden yararlanır ve güvenlik personeline politikalar oluşturmak, tehditlere hızlı ve etkili bir şekilde yanıt vermek için istihbarat sağlar.
- **IoT Security —** Tek bir platformda Makine Öğrenimi Destekli görünürlük, önleme ve uygulama sunan, sektörün en kapsamlı IoT güvenlik çözümünü sağlar.
- **DLP —** Hassas verileri ağlar, bulutlar ve kullanıcılar arasında tutarlı bir şekilde koruyan, sektörün ilk bulut tabanlı DLP lisansını sunar.
- **SaaS Security —** Yeni SaaS uygulamalarını tespit etmenize, verileri korumanıza ve en düşük toplam sahip olma maliyetiyle (TCO) zero-day tehditlerini önlemenize olanak tanıyan entegre SaaS güvenliği sağlar.

SD-WAN işlevselliği sağlar.

- SDW-WAN'ı sadece mevcut güvenlik duvarlarınızda etkinleştirerek kolayca kullanabilirsiniz.
- Sektör lideri güvenliğimizle yerel olarak entegre olan SD-WAN'ı güvenle uygulamanızı sağlar.
- Gecikmeyi, titreşimi ve paket kaybını en aza indirerek benzersiz bir kullanıcı deneyimi sunar.

Tek Geçişli Mimari ile, benzersiz bir deneyim sunar.

- Tüm tehditler ve içerik için ağ oluşturma, politika araması, uygulama, kod çözme ve imza eşleştirme işlemini tek geçişte gerçekleştirir. Bu, tek bir güvenlik cihazında birden çok işlevi gerçekleştirmek için, gereken işlem ek yükünü önemli ölçüde azaltır.
- Akış tabanlı, tek tip imza eşleştirmeden faydalanarak tek geçişte tüm imzalar için, trafiği tarayarak gecikmeyi önler.
- Güvenlik abonelikleri etkinleştirildiğinde tutarlı ve öngörülebilir performans sağlar. (Tablo 1'de, "Tehdit Önleme performansı" birden çok abonelik etkinleştirilerek ölçülmüştür.)

Tablo 1: PA-400 Serisi Performans ve Kapasiteler

	PA-460	PA-450	PA-440	PA-410*
Güvenlik duvarı Performans (HTTP/appmix)†	5.2/4.7 Gbps	3.8/3.2 Gbps	3.0/2.4 Gbps	Çok yakında
Tehdit Önleme Performans(HTTP/appmix)‡	2.4/2.6 Gbps	1.6/1.7 Gbps	0.9/1.0 Gbps	Çok yakında
IPsec VPN Performans §	3.1 Gbps	2.2 Gbps	1.6 Gbps	Çok yakında
Maks. Sessions	400,000	300,000	200,000	Çok yakında
Saniye başına yeni session	74,000	52,000	39,000	Çok yakında

Not: Sonuçlar PAN-OS 10.1'de ölçülmüştür

* PA-410 Performans verileri gelecekte eklenecektir.

† Güvenlik duvarı verimi, 64 KB HTTP/appmix işlemleri kullanılarak Uygulama Kimliği ve günlük kaydı etkinleştirilerek ölçülür.

‡ Tehdit Önleme verimi, 64 KB HTTP/appmix işlemleri kullanılarak Uygulama Kimliği, IPS, antivirüs, casus yazılım önleme, WildFire, dosya engelleme ve günlük kaydı etkinleştirilerek ölçülür.

§ IPsec VPN verimi, 64 KB HTTP işlemleri ve etkin günlüğe kaydetme ile ölçülür.

|| Saniye başına yeni oturumlar, 1 baytlık HTTP işlemleri kullanılarak uygulama geçersiz kılma ile ölçülür.

Tablo 2: PA-400 Serisi Ağ Özellikleri
Arabirim Modları
L2, L3, tap, sanal kablo (şeffaf mod)
Routing
Yeniden başlatma ile OSPFv2/v3, yeniden başlatma ile BGP, RIP, statik yönlendirme
Politikaya dayalı iletme
Ethernet üzerinden noktadan noktaya protokol (PPPoE)
Çok noktaya yayın: PIM-SM, PIM-SSM, IGMP v1, v2 ve v3
SD-WAN
Yol kalitesi ölçümü (titreme, paket kaybı, gecikme)
İlk yol seçimi (PBF)
Dinamik yıl değişikliği
IPv6
L2, L3, tap, sanal kablo (şeffaf mod)
Özellikler: App ID, User ID, Content ID, WildFire ve SSL Decryption
SLAAC
IPsec VPN
Anahtar değişimi: manüel anahtar, IKEv1 ve IKEv2 (önceden paylaşılan anahtar, sertifika tabanlı kimlik doğrulama)
Şifreleme: 3DES, AES (128 bit, 192 bit, 256 bit)
Kimlik DOğrulama: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLAN'lar
Cihaz başına/arabirim başına 802.1Q VLAN etiketi: 4.094/4.094

Tablo 3: PA-400 Serisi Donanım Özellikleri
G/Ç
PA-460, PA-450, PA-440: 10/100/1000 (8) RJ45 PA-410: 10/100/1000 (7) RJ45
Yönetim G/Ç
10/100/1000 bant dışı yönetim bağlantı noktası (1), RJ45 konsol bağlantı noktası (1), USB bağlantı noktası (1), Micro USB bağlantı noktası (1)
Depolama Kapasitesi
PA-460, PA-450, PA-440: 128 GB eMMC PA-410: 64 GB eMMC

Tablo 3: PA-400 Serisi Donanım Özellikleri (devamı)
Güç Kaynağı (Ort./Maks. Güç Tüketimi)
PA-460, PA-450: 33/41 W PA-440: 29/34 W PA-410: 17/18 W
Maks. BTU/sa
PA-460, PA-450: 141 PA-440: 117 PA-410: 78
Giriş Voltajı (Giriş Frekansı)
100–240 VAC (50–60 Hz)
Maks. Akım Tüketimi
PA-460, PA-450: 3.4 A @ 12 VDC PA-440: 2.9 A @ 12 VDC PA-410: 1.5 A @ 12 VDC
Maks. Ani Akım
PA-460, PA-450: 4.2 A PA-440: 3.3 A PA-410: 2.1 A
Boyutlar
PA-460, PA-450, PA-440: 1.74" Y x 8.83" D x 8.07" G PA-410: 1.63" Y x 6.42" D x 9.53" G
Ağırlık (Bağımsız Cihaz/Sevk Edildiği Haliyle)
PA-460, PA-450, PA-440: 5.0 lb / 7.8 lb PA-410: 3.1 lb/ 5.9 lb
Güvenlik
cTUVus, CB
EMI
FCC Sınıf B, CE Sınıf B, VCCI Sınıf B
Sertifikalar
Bkz.: paloaltonetworks.com/company/certifications.html
Çevre
Çalışma sıcaklığı: 32° ila 104° F, 0° ila 40° C Çalışma dışı sıcaklık: -4° ila 158° F, -20° ila 70° C Pasif soğutma

PA-400 Serisinin özellikleri ve ilgili kapasiteleri hakkında daha fazla bilgi edinmek için lütfen paloaltonetworks.com/net-work-security/next-generation-firewall/pa-400 adresini ziyaret edin.

paloalto NETWORKS

Exclusive Networks Türkiye
Karaman Çiftliği Yolu Kar Plaza No: 47/1 İçerenköy/ Ataşehir /İstanbul
PanSales_TR@exclusive-networks.com

EXCLUSIVE NETWORKS